# JPRS CA Certificate Policy Version <u>3.74<mark>3.80</u></u></mark>

変更履歴あり

JPRS CA Certificate Polic Version 3.80

整形版

MarchMay 27<u>20</u>, 2025 Japan Registry Services Co., Ltd. May 20, 2025 Japan Registry Services Co., L

	備考
	凡例 : <u>赤字(下線付き)</u> : 追加 <del>青字(取消線付き)</del> : 削除
ЭУ	バージョンの更新
td.	改訂日の更新

		Version History
Version Number	Date	Description
1.00	2019.06.17	Publication of the first version
1.10	2019.09.25	Revision of "3.2.2.4 Validation of Domai Authorization or Control" (adding the additional information of "general e-mail address indicatin an administrator"
1.20	2020.04.01	Revision due to Mozilla Root Store Policy (v2.7)
1.30	2020.07.10	Revision of "7.1.2 Subordinate CA Certificat Profile"
2.00	2020.07.22	Revision of "7. Certificate, CRL, and OCS Profiles"
2.10	2020.08.20	Revision of the maximum validity period of certificate
2.20	2020.10.06	Revision of "3.2.2.4 Validation of Domai Authorization or Control"
2.21	2021.04.01	Revision of the date and version
2.22	2021.04.28	Revision due to Mozilla Root Store Policy (v2.7.1)
2.23	2021.05.27	<ul> <li>Clarification of "3.2.2.4 Validation of Domain Authorization or Control"</li> <li>Delete the description of invalid Subordinate CA from "7. Certificate, CRL, and OCSP Profiles".</li> </ul>
2.30	2021.11.18	<ul> <li>Revision of "3.2.2.4.18 Agreed-Upon Change to Website v2"</li> <li>Sunset of "subject:organizationalUnitName"</li> </ul>
3.00	2021.12.08	Revisions due to new service provision
3.10	2022.03.02	Add a reference to the new terms and conditions
3.11	2022.04.01	Revision of the date and version
3.20	2022.09.30	<ul> <li>Revision of "6.3 Other Aspects of Key Pair Management"</li> <li>Add description of Revocation Reason Code to b applied in this CA.</li> </ul>
3.30	2023.04.24	Revision of the maximum validity period of certificate
3.40	2023.06.08	<ul> <li>Revision of "1.1 Overview"</li> <li>Revision of "7.3 OCSP Profile"</li> </ul>
3.50	2023.08.28	Revision of description to clarify compliance wit

		整形版
		Version History
Version	Date	Description
Number		-
1.00	2019.06.17	Publication of the first version
1.10	2019.09.25	Revision of "3.2.2.4 Validation of Domain
		Authorization or Control" (adding the additional
		information of "general e-mail address indicating
1.00	2020.04.01	an administrator"
1.20	2020.04.01	Revision due to Mozilla Root Store Policy (v2.7)
1.30	2020.07.10	Revision of "7.1.2 Subordinate CA Certificate Profile"
2.00	2020.07.22	Revision of "7. Certificate, CRL, and OCSP
		Profiles"
2.10	2020.08.20	Revision of the maximum validity period of
		certificate
2.20	2020.10.06	Revision of "3.2.2.4 Validation of Domain
		Authorization or Control"
2.21	2021.04.01	Revision of the date and version
2.22	2021.04.28	Revision due to Mozilla Root Store Policy (v2.7.1)
2.23	2021.05.27	$\cdot$ Clarification of "3.2.2.4 Validation of Domain
		Authorization or Control"
		Delete the description of invalid Subordinate CAs
		from "7. Certificate, CRL, and OCSP Profiles".
2.30	2021.11.18	$\cdot$ Revision of "3.2.2.4.18 Agreed-Upon Change to
		Website v2"
		Sunset of "subject:organizationalUnitName"
3.00	2021.12.08	Revisions due to new service provision
3.10	2022.03.02	Add a reference to the new terms and conditions
3.11	2022.04.01	Revision of the date and version
3.20	2022.09.30	• Revision of "6.3 Other Aspects of Key Pair
		Management"
		Add description of Revocation Reason Code to be
		applied in this CA.
3.30	2023.04.24	Revision of the maximum validity period of
2.42		certificate
3.40	2023.06.08	• Revision of "1.1 Overview"
2 50	2022 00 20	Revision of "7.3 OCSP Profile"
3.50	2023.08.28	Revision of description to clarify compliance with

		変更履歴あり			整形版
		Baseline Requirements			Baseline Requirements
3.60	2024.02.22	Revision of "7. Certificate, CRL, and OCSP	3.60	2024.02.22	Revision of "7. Certificate, CRL, and
		Profiles"			Profiles"
3.70	2024.04.11	Revision of Table 7.1-2 and Table 7.1-3	3.70	2024.04.11	Revision of Table 7.1-2 and Table 7.1-3
3.71	2024.06.05	Revision of "1.6 Definitions and Acronyms" and	3.71	2024.06.05	Revision of "1.6 Definitions and Acrony
		"4.2.4 Check of CAA Records"			"4.2.4 Check of CAA Records"
3.72	2024.08.26	Revision of "4.2.1 Performing Identification and	3.72	2024.08.26	Revision of "4.2.1 Performing Identification
		Authentication Functions"			Authentication Functions"
3.73	2024.11.07	Revision of " 4.3.1 CA Actions during Certificate	3.73	2024.11.07	Revision of " 4.3.1 CA Actions during C
		Issuance", " 4.9.1 Circumstances for Certificate			Issuance", " 4.9.1 Circumstances for C
		Revocation" and " 8.4 Topics Covered by			Revocation" and " 8.4 Topics Cov
		Assessment"			Assessment"
3.74	2025.03.27	Revision of "4.2.4 Check of CAA Records"	3.74	2025.03.27	Revision of "4.2.4 Check of CAA Records"
<u>3.80</u>	2025.05.20	Revision of "1.6 Definitions and Acronyms",	3.80	2025.05.20	Revision of "1.6 Definitions and Acronym
		<u>"3.2.2.4 Validation of Domain Authorization or</u>			"3.2.2.4 Validation of Domain Authorizat
		Control", "3.2.2.8 CAA Records" and "7.1			Control", "3.2.2.8 CAA Records" and "7.1
		Certificate Profile"			Certificate Profile"
		Add "3.2.2.9 Multi-Perspective Issuance			Add "3.2.2.9 Multi-Perspective
		Corroboration"			Corroboration"

## 1. Introduction

#### 1.1 Overview

This document, the JPRS CA Certificate Policy (hereinafter referred to as "this CP"), stipulates policies regarding the usages, purposes of use, scope of application, etc. of Digital Certificates to be issued by Japan Registry Services Co., Ltd. (hereinafter referred to as "JPRS") as a Certification Authority (hereinafter referred to as the "CA"), for the purpose of providing the JPRS Digital Certificate Issuance Services (hereinafter referred to as the "Services").

Various procedures regarding the operation and maintenance of the CA are stipulated in the JPRS CA Certification Practice Statement (hereinafter referred to as the "CPS").

A certificate for one-way and mutual certification has been issued to the CA by Security Communication RootCA2, Security Communication ECC RootCA1 or SECOM TLS RSA Root CA 2024, a Certification Authority operated by SECOM Trust Systems Co., Ltd (hereinafter referred to as "SECOM Trust Systems"), and the CA is authorized to issue certificates to Subscribers.

## 1. Introduction

## 1.1 Overview

This document, the JPRS CA Certificate Policy (hereinafter referred to stipulates policies regarding the usages, purposes of use, scope of application Certificates to be issued by Japan Registry Services Co., Ltd. (hereinafter "JPRS") as a Certification Authority (hereinafter referred to as the "CA"), fo providing the JPRS Digital Certificate Issuance Services (hereinafter ref. "Services").

Various procedures regarding the operation and maintenance of the CA and the JPRS CA Certification Practice Statement (hereinafter referred to as the A certificate for one-way and mutual certification has been issued to the Communication RootCA2, Security Communication ECC RootCA1 or SEC Root CA 2024, a Certification Authority operated by SECOM Trust Sys (hereinafter referred to as "SECOM Trust Systems"), and the CA is auth certificates to Subscribers.

	備考
and OCSP	
nyms" and	
cation and	
Certificate	
Certificate	
overed by	
s"	
ms", ation or	改訂履歴の追記
1	
1	
Issuance	
as "this CP")	
n, etc. of Digita	
r referred to as r the purpose o	
erred to as the	
re stipulated ir	1
e "CPS").	
CA by Security	
COM TLS RSA	
stems Co., Ltd	
orized to issue	

#### 整形版

Certificates issued by the CA are used for encrypting information for server authentication and on communication pathways. "The Terms and Conditions of JPRS Digital Certificate Issuance Services" and "The Terms and Conditions of JPRS Digital Certificate Issuance Services for ACME" (hereinafter, both will be referred to as the "Terms and Conditions") stipulate the servers to be covered by the issuance of such certificates.

Each person who intends to have a certificate issued by the CA is required to consider the Terms and Conditions, this CP, and the CPS in light of his/her/its own purposes of use, and then to consent to the Terms and Conditions, this CP, and the CPS.

The CA conforms to the current version of "Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates" (hereinafter referred to as the "Baseline Requirements") published by CA/Browser Forum at https://www.cabforum.org/, and the Application Software Supplier Standards published."

Table1.1 List of Standards

Types of certificates issued by	Standards to comply with
the CA	
	• Baseline Requirements for the
	Issuance and Management of Publicly
	- Trusted TLS Server Certificates
TLS Server Certificate	• Apple Root Certificate Program
	Chrome Root Program Policy
	Microsoft Trusted Root Program
	Mozilla Root Store Policy

If any inconsistency is found among the provisions of this CP, the Terms and Conditions, and the CPS, the provisions of the Terms and Conditions shall prevail over those of this CP and the CPS, and the provisions of this CP shall prevail over those of the CPS. Also, if any inconsistency is found among the provisions of <u>the Japanese version</u> and the English version of this CP, the English version shall prevail over <u>the Japanese version</u>. In the event of any inconsistency between the documents established by the CA (including, but not limited to, this CP, the CPS, the Terms and Conditions, and the related documents) and Baseline Requirements, Baseline Requirements take precedence over these documents.

This CP conforms to the RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" advocated by the IETF as a framework for the operation of Certification Authorities.

With any developments or improvements pertaining to the CA in terms of technologies or With any developments or improvements o

Certificates issued by the CA are used for encrypting information for server and on communication pathways. "The Terms and Conditions of JPRS Dig Issuance Services" and "The Terms and Conditions of JPRS Digital Certif Services for ACME" (hereinafter, both will be referred to as the "Terms and stipulate the servers to be covered by the issuance of such certificates. Each person who intends to have a certificate issued by the CA is required

Terms and Conditions, this CP, and the CPS in light of his/her/its own purportion then to consent to the Terms and Conditions, this CP, and the CPS.

The CA conforms to the current version of "Baseline Requirements for th Management of Publicly-Trusted TLS Server Certificates" (hereinafter ref "Baseline Requirements") published by CA/Browser Forum at https://www and the Application Software Supplier Standards published."

Table	able1.1 List of Standards		
Types of certificates issued by	Standards to comply with		
the CA			
	• Baseline Requirements for the		
	Issuance and Management of P		
	- Trusted TLS Server Certifica		
TLS Server Certificate	• Apple Root Certificate Program		
	Chrome Root Program Policy		
	Microsoft Trusted Root Program		
	Mozilla Root Store Policy		

If any inconsistency is found among the provisions of this CP, the Terms a and the CPS, the provisions of the Terms and Conditions shall prevail over t and the CPS, and the provisions of this CP shall prevail over those of the CP inconsistency is found among the provisions of <u>the Japanese version</u> ar version of this CP, the English version shall prevail over <u>the Japanese version</u> of any inconsistency between the documents established by the CA (incl limited to, this CP, the CPS, the Terms and Conditions, and the related d Baseline Requirements, Baseline Requirements take precedence over these of

This CP conforms to the RFC 3647 "Internet X.509 Public Key Infrastruct Policy and Certification Practices Framework" advocated by the IETF as a the operation of Certification Authorities.

With any developments or improvements pertaining to the CA in terms of to operation, this CP shall be revised, as needed, in order to reflect such de

		備考
authent	cication	
gital Cer	tificate	
ificate Is	suance	
nd Condi	itions")	
to consid	der the	
oses of u	se, and	
e Issuan	ce and	
ferred to		
v.cabforu	m.org/,	
	1	
Publicly		
ates		
1		
m		
	J	
and Cond	litions	
those of t		
PS. Also		
nd the English		
on. In the event		
luding, but not		
locuments) and		
documents.		
ture Certificate		
framew	ork for	
technolo	gies or	
evelopme	ents or	

#### improvements.

#### **1.2 Document Name and Identification**

The official name of this CP is the "JPRS CA Certificate Policy."

Following are an Object Identifier (hereinafter referred to as "OID") assigned by the CA under this CP, and an OID of the CPS referenced by this CP:

Name	OID	
JPRS CA Certificate Policy (CP)	1.3.6.1.4.1.53827.1.1.4	
JPRS CA Certification Practice Statement (CPS)	1.3.6.1.4.1.53827.1.2.4	

#### **1.3 PKI Participants**

#### 1.3.1 CA

"CA" stands for "Certification Authority," an entity that mainly issues and revokes certificates, discloses revocation information, provides and stores information on the certificate status using the OCSP (Online Certificate Status Protocol) server, generates and protects the CA's own Private Keys, and registers Subscribers.

#### 1.3.2 RA

"RA" stands for "Registration Authority," an entity that mainly performs reviews to verify the existence and validate the identities of applicants who apply for the issuance or revocation of certificates, registers information necessary for issuing certificates, and requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.

#### 1.3.3 Subscribers

"Subscribers" means an individual, corporation, or organization that has been issued a certificate by the CA and uses the certificate. "Subscriber Certificate" means the certificate issued by the CA to the Subscribers.

#### **1.3.4 Relying Parties**

A "Relying Party" means an individual, corporation, or organization that verifies the validity of certificates issued by the CA.

#### **1.3.5 Other Participants**

No stipulation.

#### **1.4 Certificate Usage**

#### **1.4.1 Appropriate Certificate Uses**

Certificates issued by the CA are used to encrypt information for server authentication and on communication pathways.

<b>教</b> 政告		) 一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
improvements.		備考
1.2 Document Name and Identification		
The official name of this CP is the "JPRS CA Certificate I		
Following are an Object Identifier (hereinafter referred		
under this CP, and an OID of the CPS referenced by this	CP.	
Name	OID	
JPRS CA Certificate Policy (CP)	1.3.6.1.4.1.53827.1.1.4	
JPRS CA Certification Practice Statement (CPS)	1.3.6.1.4.1.53827.1.2.4	
1.3 PKI Participants		
1.3.1 CA		
"CA" stands for "Certification Authority," an entity	that mainly issues and revokes	
certificates, discloses revocation information, provides	-	
certificate status using the OCSP (Online Certificate Sta	tus Protocol) server, generates and	
protects the CA's own Private Keys, and registers Subscr	ibers.	
1.3.2 RA		
"RA" stands for "Registration Authority," an entity that	mainly performs reviews to verify	
the existence and validate the identities of applicant	s who apply for the issuance or	
revocation of certificates, registers information necess	sary for issuing certificates, and	
requests the CA to issue certificates, among the operation	is of the CA. The CA acts as an RA.	
1.3.3 Subscribers		
"Subscribers" means an individual, corporation, or org	anization that has been issued a	
certificate by the CA and uses the certificate. "Subscriber	r Certificate" means the certificate	
issued by the CA to the Subscribers.		
1.3.4 Relying Parties		
A "Relying Party" means an individual, corporation,	or organization that verifies the	
validity of certificates issued by the CA.		
1.3.5 Other Participants		
No stipulation.		
1.4 Certificate Usage		
1.4.1 Appropriate Certificate Uses		
Certificates issued by the CA are used to encrypt information	ation for server authentication and	
on communication pathways.		

変更履歴あり	整形版
1.4.2 Prohibited Certificate Uses	1.4.2 Prohibited Certificate Uses
Certificates issued by the CA may be used solely as set forth in "1.4.1 Appropriate	
Certificate Uses," and may not be used for any other purposes.	Certificate Uses," and may not be used for any other purposes.
1.5 Policy Administration	1.5 Policy Administration
1.5.1 Organization Administering the Document	1.5.1 Organization Administering the Document
This CP shall be maintained and administered by the CA.	This CP shall be maintained and administered by the CA.
1.5.2 Contact Information	1.5.2 Contact Information
Inquiries concerning this CP should be directed to:	Inquiries concerning this CP should be directed to:
Contact: Inquiries contact office, Japan Registry Services Co., Ltd.	Contact: Inquiries contact office, Japan Registry Services Co., Ltd.
Address: Chiyoda First Bldg. East, 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101-0065 JAPAN	Address: Chiyoda First Bldg. East, 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101-0065 JAPAN
E-mail: <u>info@jprs.jp</u>	E-mail: <u>info@jprs.jp</u>
If a compromise or unauthorized use of any Private Key or any other trouble pertaining to a	If a compromise or unauthorized use of any Private Key or any other trouble pertaining to a
certificate issued by the CA is revealed, please notify via the following webform:	certificate issued by the CA is revealed, please notify via the following webform:
https://jprs.jp/pubcert/f_mail/	https://jprs.jp/pubcert/f_mail/
1.5.3 Person Determining CP Suitability as Policy	1.5.3 Person Determining CP Suitability as Policy
The details of this CP shall be determined by the CA's Certificate Operation Conference.	The details of this CP shall be determined by the CA's Certificate Operation Conference.
1.5.4 Approval Procedures	1.5.4 Approval Procedures
This CP shall come into effect upon approval of the CA's Certificate Operation Conference.	This CP shall come into effect upon approval of the CA's Certificate Operation Conference.
1.6 Definitions and Acronyms	1.6 Definitions and Acronyms
ACME (Automated Certificate Management Environment)	ACME (Automated Certificate Management Environment)
"ACME" stands for "Automated Certificate Management Environment", a protocol that	"ACME" stands for "Automated Certificate Management Environment", a protocol that
a CA and an applicant can use to automate the process of verification and certificate	a CA and an applicant can use to automate the process of verification and certificate
issuance. This Protocol is specified in RFC 8555.	issuance. This Protocol is specified in RFC 8555.
Archive	Archive
"Archive" means information acquired for the purpose of keeping a history for any legal	"Archive" means information acquired for the purpose of keeping a history for any legal
or other reason.	or other reason.
Audit Log	Audit Log
An "Audit Log" is a log of actions, accesses, and other histories pertaining to Certification	An "Audit Log" is a log of actions, accesses, and other histories pertaining to Certification
Authority systems that are recorded for the purpose of monitoring accesses to, and	Authority systems that are recorded for the purpose of monitoring accesses to, and
unauthorized operations of, Certification Authority systems.	unauthorized operations of, Certification Authority systems.
Authorization Domain Name	Authorization Domain Name
The Domain Name used to obtain authorization for certificate issuance for a given FQDN.	The Domain Name used to obtain authorization for certificate issuance for a given FQDN.

# The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

#### Base Domain Name

The portion of an applied-for FQDN that is the first domain name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

#### CA (Certification Authority)

"CA" stands for "Certification Authority," an entity that mainly issues, renews, and revokes certificates, discloses information on certificate revocation, provides and stores information on the status of certificates using the OCSP (Online Certificate Status Protocol) server, generates and protects the CA's own Private Keys, and registers Subscribers.

#### CAA (Certificate Authority Authorization)

"CAA" stands for "Certificate Authority Authorization," a function to prevent unintended erroneous issuance of certificates from unauthorized Certification Authorities in connection with the authority to use a domain by adding information to the DNS record in order to specify the Certification Authority authorized to issue a certificate for the domain. This function is stipulated in RFC 8659.

#### <u>CP (Certificate Policy)</u>

"CP" stands for "Certificate Policy," a document that sets forth policies regarding certificates to be issued by the CA, such as the types of certificates, the servers for which certificates may be issued, the usages of certificates, procedures for applying for the issuance of certificates, and the criteria for such issuance.

#### CPS (Certification Practices Statement)

"CPS" stands for "Certification Practice Statement," a document that sets forth provisions to be followed in operating the CA, such as various operational procedures and security standards.

#### CRL (Certificate Revocation List)

#### 整形版

The CA may use the FQDN returned from a DNS CNAME lookup as the purposes of domain validation. If the FQDN contains a wildcard charact MUST remove all wildcard labels from the left most portion of requested may prune zero or more labels from left to right until encountering a Base and may use any one of the intermediate values for the purpose of domain

#### **Base Domain Name**

The portion of an applied-for FQDN that is the first domain name registry-controlled or public suffix plus the registry-controlled or public "example.co.uk" or "example.com"). For FQDNs where the right-most dom is a gTLD having ICANN Specification 13 in its registry agreement, the g be used as the Base Domain Name.

#### CA (Certification Authority)

"CA" stands for "Certification Authority," an entity that mainly issue revokes certificates, discloses information on certificate revocation, prov information on the status of certificates using the OCSP (Online Cer Protocol) server, generates and protects the CA's own Private Keys, Subscribers.

#### CAA (Certificate Authority Authorization)

"CAA" stands for "Certificate Authority Authorization," a function unintended erroneous issuance of certificates from unauthorized Certificate in connection with the authority to use a domain by adding information to in order to specify the Certification Authority authorized to issue a cert domain. This function is stipulated in RFC 8659.

#### <u>CP (Certificate Policy)</u>

"CP" stands for "Certificate Policy," a document that sets forth policertificates to be issued by the CA, such as the types of certificates, the second certificates may be issued, the usages of certificates, procedures for approximate of certificates, and the criteria for such issuance.

#### CPS (Certification Practices Statement)

"CPS" stands for "Certification Practice Statement," a document t provisions to be followed in operating the CA, such as various operational security standards.

#### CRL (Certificate Revocation List)

備考 e FQDN for the ter, then the CA FQDN. The CA e Domain Name n validation.	
node left of a blic suffix (e.g. nain name node gTLD itself may	
es, renews, and vides and stores ertificate Status , and registers	
ion to prevent tion Authorities the DNS record rtificate for the	
licies regarding ervers for which applying for the	
that sets forth procedures and	

#### "CRL" stands for "Certificate Revocation List," a list of information about certificates revoked during their period of validity for any reason, including changes in the particulars described in the certificates or the compromise of any Private Keys.

#### CT (Certificate Transparency)

"CT" stands for "Certificate Transparency," a scheme stipulated in RFC 6962 to register and publish information about certificates on a log server (CT log server) for the purpose of monitoring and auditing information about issued certificates.

#### **Digital Certificates**

A "Digital Certificate" means digital data certifying that a Public Key is possessed by the party specified in the data. The validity of a Digital Certificate is assured by a digital signature of the relevant CA affixed to the Digital Certificate.

#### DNS TXT Record Email Contact

The email address included in the TXT resource record in the DNS zone of the FQDN prefixed with the "\_validation-contactemail" label, as defined in Appendix A.2.1 of Baseline Requirements.

#### ECDSA (Elliptic Curve Digital Signature Algorithm)

"ECDSA" is one of the most standard encryption technologies. ECDSA is widely used as a public key cryptosystem.

#### Escrow

"Escrow" means the placement (entrustment) of an asset in the control of an independent third party.

#### <u>FIPS 140-2</u>

"FIPS 140-2" are a set of security accreditation criteria for cryptographic modules developed by the United States NIST (National Institute of Standards and Technology). Four levels, from Level 1 (the lowest) to Level 4 (the highest), have been defined.

#### FQDN (Fully-Qualified Domain Name)

A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

#### HSM (Hardware Security Module)

"HSM" stands for "Hardware Security Module," a tamper-resistant encryption device to be used for generating, storing, using, or otherwise handling Private Keys for the purpose

#### 整形版

"CRL" stands for "Certificate Revocation List," a list of information aborevoked during their period of validity for any reason, including cliparticulars described in the certificates or the compromise of any Private F

#### CT (Certificate Transparency)

"CT" stands for "Certificate Transparency," a scheme stipulated in RFC 6 and publish information about certificates on a log server (CT log server) is of monitoring and auditing information about issued certificates.

#### **Digital Certificates**

A "Digital Certificate" means digital data certifying that a Public Key is poparty specified in the data. The validity of a Digital Certificate is assurs signature of the relevant CA affixed to the Digital Certificate.

#### DNS TXT Record Email Contact

The email address included in the TXT resource record in the DNS zone prefixed with the "\_validation-contactemail" label, as defined in App Baseline Requirements.

#### ECDSA (Elliptic Curve Digital Signature Algorithm)

"ECDSA" is one of the most standard encryption technologies. ECDSA is a public key cryptosystem.

#### Escrow

"Escrow" means the placement (entrustment) of an asset in the independent third party.

#### FIPS 140-2

"FIPS 140-2" are a set of security accreditation criteria for cryptogr developed by the United States NIST (National Institute of Standards ar Four levels, from Level 1 (the lowest) to Level 4 (the highest), have been de

#### FQDN (Fully-Qualified Domain Name)

A Domain Name that includes the Domain Labels of all superior nodes Domain Name System.

#### HSM (Hardware Security Module)

"HSM" stands for "Hardware Security Module," a tamper-resistant encry be used for generating, storing, using, or otherwise handling Private Keys

	備考
oout certificates changes in the Keys.	UTH
6962 to register for the purpose	
oossessed by the red by a digital	
ne of the FQDN bendix A.2.1 of	用語定義の追加
s widely used as	
control of an	
raphic modules nd Technology). lefined.	
in the Internet	
yption device to	
for the purpose	
ior one purpose	

of maintaining security.

#### JPRS Partners

"JPRS Partners" mean business enterprises authorized by JPRS in connection with the Digital Certificate Issuance Services to be provided by JPRS.

#### <u>Key Pair</u>

A "Key Pair" means a pair consisting of a Private Key and Public Key in a public key cryptosystem.

#### Linting

A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, Certificate Revocation List, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.

#### Multi-Perspective Issuance Corroboration (MPIC)

<u>A process by which the determinations made during domain validation and CAA checking</u> by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

#### Network Perspective

<u>Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted</u> <u>server instance) or collection of network components (e.g., a VPN and corresponding</u> <u>infrastructure) for sending outbound Internet traffic associated with a domain control</u> <u>validation method and/or CAA check. The location of a Network Perspective is</u> <u>determined by the point where unencapsulated outbound Internet traffic is typically first</u> <u>handed off to the network infrastructure providing Internet connectivity to that</u> <u>perspective.</u>

#### NTP (Network Time Protocol)

"NTP" stands for "Network Time Protocol," a protocol designed to synchronize the internal clocks of computers over a network.

#### OCSP (Online Certificate Status Protocol)

"OCSP" stands for "Online Certificate Status Protocol," a protocol for providing information on the status of a certificate in real time.

OID (Object Identifier)

of maintaining security.

#### JPRS Partners

"JPRS Partners" mean business enterprises authorized by JPRS in conn Digital Certificate Issuance Services to be provided by JPRS.

整形版

#### Key Pair

A "Key Pair" means a pair consisting of a Private Key and Public Key i cryptosystem.

#### Linting

A process in which the content of digitally signed data such as a Prece 6962], Certificate, Certificate Revocation List, or OCSP response, or da object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) conformance with the profiles and requirements defined in these Requirem

#### <u>Multi-Perspective Issuance Corroboration (MPIC)</u>

A process by which the determinations made during domain validation and by the Primary Network Perspective are corroborated by other Networ before Certificate issuance.

#### Network Perspective

Related to Multi-Perspective Issuance Corroboration. A system (e.g., a server instance) or collection of network components (e.g., a VPN and infrastructure) for sending outbound Internet traffic associated with a o validation method and/or CAA check. The location of a Network determined by the point where unencapsulated outbound Internet traffic is handed off to the network infrastructure providing Internet connec perspective.

#### NTP (Network Time Protocol)

"NTP" stands for "Network Time Protocol," a protocol designed to sy internal clocks of computers over a network.

#### OCSP (Online Certificate Status Protocol)

"OCSP" stands for "Online Certificate Status Protocol," a protocol information on the status of a certificate in real time.

<u>OID (Object Identifier)</u>

	備考
nection with the	
in a public key	
ertificate [RFC ata-to-be-signed ) is checked for nents.	
d CAA checking rk Perspectives	用語定義の追加
a cloud-hosted l corresponding domain control Perspective is is typically first ctivity to that	用語定義の追加
ynchronize the	
for providing	

#### "OIDs" stands for "Object Identifiers," numerals registered in international registration institutions as unique IDs among global networks within a framework for maintaining and administering the connectivity of networks and the uniqueness of services or the like.

#### PKI (Public Key Infrastructure)

"PKI" stands for "Public Key Infrastructure," an infrastructure for using the encryption technology known as a public key cryptosystem to realize security technologies such as digital signatures, encryption, and certification.

#### Primary Network Perspective

The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es).

#### Private Key

A "Private Key" means a key of a Key Pair used in a public key cryptosystem. A Private Key corresponds to a certain Public Key and is possessed only by the person in question. A Private Key may be referred to as a "secret key."

#### Public Key

A "Public Key" means a key of a Key Pair used in a public key cryptosystem. A Public Key corresponds to a certain Private Key and is disclosed to the other party to communication.

#### RA (Registration Authority)

"RA" stands for "Registration Authority," an entity that mainly performs reviews to verify the existence and validate the identities of applicants who apply for the issuance or revocation of certificates, registers information necessary for issuing certificates, and requests the CA to issue certificates, among the operations of the CA.

#### Random Value

A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

#### <u>Repository</u>

The "Repository" means the database in which CA certificates, CRLs, and others are stored and published.

#### RFC 3647 (Request for Comments 3647)

"RFC 3647" stands for "Request for Comments 3647," a document defining the

#### 整形版

"OIDs" stands for "Object Identifiers," numerals registered in internation institutions as unique IDs among global networks within a framework for and administering the connectivity of networks and the uniqueness of serv

#### PKI (Public Key Infrastructure)

"PKI" stands for "Public Key Infrastructure," an infrastructure for using technology known as a public key cryptosystem to realize security techno digital signatures, encryption, and certification.

#### Primary Network Perspective

The Network Perspective used by the CA to make the determination authority to issue a Certificate for the requested domain(s) or IP address Applicant's authority and/or domain authorization or control of the reque or IP address(es).

#### <u>Private Key</u>

A "Private Key" means a key of a Key Pair used in a public key cryptosys Key corresponds to a certain Public Key and is possessed only by the person Private Key may be referred to as a "secret key."

#### <u>Public Key</u>

A "Public Key" means a key of a Key Pair used in a public key cryptosystem corresponds to a certain Private Key and is disclosed to the other party to c

#### RA (Registration Authority)

"RA" stands for "Registration Authority," an entity that mainly perfor verify the existence and validate the identities of applicants who apply for revocation of certificates, registers information necessary for issuing correquests the CA to issue certificates, among the operations of the CA.

#### Random Value

A value specified by a CA to the Applicant that exhibits at least 112 bits of

#### <u>Repository</u>

The "Repository" means the database in which CA certificates, CRLs, a stored and published.

#### RFC 3647 (Request for Comments 3647)

e "RFC 3647" stands for "Request for Comments 3647," a document

onal registration for maintaining vices or the like.	備考
g the encryption nologies such as	
of 1) the CA's s(es) and 2) the ested domain(s)	用語定義の追加
stem. A Private on in question. A	
m. A Public Key communication.	
orms reviews to the issuance or certificates, and	
f entropy.	
and others are	
nt defining the	

framework for CP and CPS published by the IETF (Internet Engineering Task Force), an industry group that establishes technical standards for the Internet.

#### RFC 5280 (Request for Comments 5280)

"RFC 5280" stands for "Request for Comments 5280," a document defining the public key infrastructure published by the IETF (Internet Engineering Task Force), an industry group that establishes technical standards for the Internet.

#### RSA

"RSA" is one of the most standard encryption technologies. RSA IS widely used as a public key cryptosystem.

#### SHA-1 (Secure Hash Algorithm 1)

"SHA-1" stands for "Secure Hash Algorithm 1," one of the hash functions (summarization functions) used in digital signing. A hash function is a computation technique for generating a fixed-length bit string from a given text. The bit length is one hundred sixty (160) bits. The algorithm works to detect any alterations in an original message during its transmission by comparing the hash values transmitted and received.

#### SHA-256 (Secure Hash Algorithm 256)

"SHA-256" stands for "Secure Hash Algorithm 256," one of the hash functions (summarization functions) used in digital signing. The bit length is two hundred fifty-six (256) bits. The algorithm works to detect any alterations in an original message during its transmission by comparing the hash values transmitted and received.

#### <u>Time Stamp</u>

"Time Stamp" means recorded data indicating dates and times when, for example, electronic files have been prepared and a system has performed processing.

#### Wildcard Certificate

A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

#### Wildcard Domain Name

A string starting with "\*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name.

## 2. Publication and Repository Responsibilities

#### 整形版

framework for CP and CPS published by the IETF (Internet Engineering industry group that establishes technical standards for the Internet.

#### RFC 5280 (Request for Comments 5280)

"RFC 5280" stands for "Request for Comments 5280," a document define key infrastructure published by the IETF (Internet Engineering Task Force group that establishes technical standards for the Internet.

#### RSA

"RSA" is one of the most standard encryption technologies. RSA IS we public key cryptosystem.

#### SHA-1 (Secure Hash Algorithm 1)

"SHA-1" stands for "Secure Hash Algorithm 1," one of the h (summarization functions) used in digital signing. A hash function is technique for generating a fixed-length bit string from a given text. The b hundred sixty (160) bits. The algorithm works to detect any alterations message during its transmission by comparing the hash values transmitte

#### SHA-256 (Secure Hash Algorithm 256)

"SHA-256" stands for "Secure Hash Algorithm 256," one of the l (summarization functions) used in digital signing. The bit length is two he (256) bits. The algorithm works to detect any alterations in an original mest transmission by comparing the hash values transmitted and received.

#### <u>Time Stamp</u>

"Time Stamp" means recorded data indicating dates and times when electronic files have been prepared and a system has performed processing

#### Wildcard Certificate

A Certificate containing at least one Wildcard Domain Name in the Subj Names in the Certificate.

#### Wildcard Domain Name

A string starting with "\*." (U+002A ASTERISK, U+002E FULL STOI followed by a Fully-Qualified Domain Name.

## 2. Publication and Repository Responsibilit

	<b>供</b> 孝
Task Force), an	備考
ning the public ce), an industry	
idely used as a	
hash functions a computation bit length is one s in an original ed and received.	
hash functions undred fifty-six ssage during its	
n, for example, g.	
ject Alternative	
P) immediately	
ties	

#### 2.1 Repository

The CA shall maintain and manage the Repository to allow access to the same twenty-four (24) hours a day, three hundred sixty-five (365) days a year. Note, however, that the Repository may be temporarily unavailable at times for system maintenance or other reasons.

#### 2.2 Publication of Information

The CA shall publish the CRLs, this CP, and the CPS on the Repository to allow online access by Subscribers and Relying Parties.

## 2.3 Time or Frequency of Publication

This CP and the CPS shall be revised at least annually and published on the Repository as revised. The CA describes to the CP and the CPS in detail how the CA implements the latest version of Baseline Requirements.

The frequency of CRL issuance is specified in Section 4.9.7.

#### 2.4 Access Controls on Repositories

The CA does not exercise any specific access control over information published on the Repository. The CA's CRLs shall be made available to Subscribers and Relying Parties through the Repository. Access to the Repository shall be granted through a general Web interface.

## 3. Identification and Authentication

#### 3.1 Naming

#### 3.1.1 Types of Names

The name of each Subscriber to be described in certificates to be issued by the CA shall be configured according to the Distinguished Name (DN) format for the X.500 series recommendations (recommendations formulated by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T)).

#### 3.1.2 Need for Names to Be Meaningful

The information included in certificates issued by the CA and their meanings are specified in Section 7.1.1.

#### 3.1.3 Anonymity or Pseudonymity of Subscribers

No name identical to any anonym or pseudonym used in any certificate to be issued by the CA may be registered.

#### 3.1.4 Rules for Interpreting Various Name Forms

整形版

#### 2.1 Repository

The CA shall maintain and manage the Repository to allow access to the san (24) hours a day, three hundred sixty-five (365) days a year. Note, how Repository may be temporarily unavailable at times for system maintenreasons.

#### 2.2 Publication of Information

The CA shall publish the CRLs, this CP, and the CPS on the Repository access by Subscribers and Relying Parties.

## 2.3 Time or Frequency of Publication

This CP and the CPS shall be revised at least annually and published on the revised. The CA describes to the CP and the CPS in detail how the CA implements of Baseline Requirements.

The frequency of CRL issuance is specified in Section 4.9.7.

## 2.4 Access Controls on Repositories

The CA does not exercise any specific access control over information pur Repository. The CA's CRLs shall be made available to Subscribers and F through the Repository. Access to the Repository shall be granted through interface.

## 3. Identification and Authentication

#### 3.1 Naming

#### 3.1.1 Types of Names

The name of each Subscriber to be described in certificates to be issued by the configured according to the Distinguished Name (DN) format for the recommendations (recommendations formulated by the International Teleor Union Telecommunication Standardization Sector (ITU-T)).

#### 3.1.2 Need for Names to Be Meaningful

The information included in certificates issued by the CA and their meaning in Section 7.1.1.

#### 3.1.3 Anonymity or Pseudonymity of Subscribers

No name identical to any anonym or pseudonym used in any certificate to b CA may be registered.

#### 3.1.4 Rules for Interpreting Various Name Forms

The Distinguished Name (DN) format of the X.500 series shall stipulate the rules for The Distinguished Name (DN) format of the X.500 series shall stipulat

	備考
ume twenty-four wever, that the mance or other	
to allow online	
ne Repository as ments the latest	
ublished on the Relying Parties a general Web	
the CA shall be e X.500 series ecommunication	
igs are specified	
be issued by the	
the rules for	

interpreting various name forms and shall be complied with accordingly.

#### 3.1.5 Uniqueness of Names

The attribute of a Distinguished Name (DN) to be described in a certificate to be issued by the CA shall be unique to the server covered by the issuance.

#### 3.1.6 Recognition, Authentication, and Roles of Trademarks

The CA does not verify whether an applicant holds any intellectual property right to the name described in a certificate application. No Subscriber may submit to the CA a certificate application with any registered trademark or associated name of any third party. If any dispute arises between a Subscriber and any third party in connection with a registered trademark or the like, the CA will not undertake to arbitrate or settle the dispute. The CA is entitled to reject a Subscriber's certificate application or to revoke an issued certificate on account of such a dispute.

#### **3.2 Initial Identity Validation**

#### 3.2.1 Method to Prove Possession of a Private Key

A Subscriber's possession of a Private Key is proved by verifying the signature on the relevant Certificate Signing Request (hereinafter referred to as "CSR") and confirming that the CSR has been signed with the Private Key corresponding to the Public Key contained in the CSR.

#### 3.2.2 Authentication of Organization and Domain Identity

The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

#### 3.2.2.1 Authentication of Organization Identity

(1) Domain Validation

The CA does not verify the existence of organizations.

(2) Organization Validation

The CA shall verify the existence of organizations by using public documents issued by, or Web pages or Web page databases of, the relevant country or local public entity, or using inquiries made by any third party that is deemed reliable by the CA, or the databases of any such third party.

#### 3.2.2.2 DBA/Tradename

If a DBA/tradename is described as the "Organization (organization name)" in a certificate to be issued by the CA, the CA shall verify the information same manner as set forth in "3.2.2.1 Authentication of Organization Identity (2) Organization Validation."

#### 3.2.2.3 Verification of a Country

整形版

interpreting various name forms and shall be complied with accordingly.

#### 3.1.5 Uniqueness of Names

The attribute of a Distinguished Name (DN) to be described in a certificate the CA shall be unique to the server covered by the issuance.

#### 3.1.6 Recognition, Authentication, and Roles of Trademarks

The CA does not verify whether an applicant holds any intellectual propert name described in a certificate application. No Subscriber may submit certificate application with any registered trademark or associated name of a If any dispute arises between a Subscriber and any third party in comregistered trademark or the like, the CA will not undertake to arbitrate dispute. The CA is entitled to reject a Subscriber's certificate application or issued certificate on account of such a dispute.

#### **3.2 Initial Identity Validation**

#### 3.2.1 Method to Prove Possession of a Private Key

A Subscriber's possession of a Private Key is proved by verifying the sig relevant Certificate Signing Request (hereinafter referred to as "CSR") and c the CSR has been signed with the Private Key corresponding to the Public Key the CSR.

#### 3.2.2 Authentication of Organization and Domain Identity

The CA SHALL inspect any document relied upon under this Section for falsification.

#### 3.2.2.1 Authentication of Organization Identity

(1) Domain Validation

The CA does not verify the existence of organizations.

(2) Organization Validation

The CA shall verify the existence of organizations by using public document Web pages or Web page databases of, the relevant country or local public e inquiries made by any third party that is deemed reliable by the CA, or the da such third party.

#### 3.2.2.2 DBA/Tradename

If a DBA/tradename is described as the "Organization (organization name)" to be issued by the CA, the CA shall verify the information same manner "3.2.2.1 Authentication of Organization Identity (2) Organization Validation."

#### 3.2.2.3 Verification of a Country

The CA shall verify the information on the "Country (country name)" in a certificate to in The CA shall verify the information on the "Country (country name)" in a certificate to in

	備老
	備考
-	
to be issued by	
5	
rty right to the	
t to the CA a	
any third party.	
nection with a e or settle the	
or to revoke an	
gnature on the	
confirming that	
ey contained in	
r alteration or	
ts issued by, or	
entity, or using	
atabases of any	
in a certificate	
as set forth in	
"	

変更履歴あり	整形版	備考
the same manner as set forth in "3.2.2.1 Authentication of Organization Identity."	the same manner as set forth in "3.2.2.1 Authentication of Organization Identity."	
3.2.2.4 Validation of Domain Authorization or Control	3.2.2.4 Validation of Domain Authorization or Control	
The CA SHALL confirm that prior to issuance, the CA has validated each FQDN listed in	The CA SHALL confirm that prior to issuance, the CA has validated each FQDN listed in	
the Certificate using at least one of the methods listed below;	the Certificate using at least one of the methods listed below;	
Subsequent sections 3.2.2.4.1-20 correspond to the section numbers of the methods specified	Subsequent sections 3.2.2.4.1-20 correspond to the section numbers of the methods specified	
by BR.	by BR.	
The CA doesn't issue certificates if "RFC 7686 - The ".onion" Special-Use Domain Name" is	The CA doesn't issue certificates if "RFC 7686 - The ".onion" Special-Use Domain Name" is	
included in the certificates.	included in the certificates.	
The CA SHALL maintain a record of which domain validation method, including relevant	The CA SHALL maintain a record of which domain validation method, including relevant	
BR version number, they used to validate every domain.	BR version number, they used to validate every domain.	
3.2.2.4.1 Validating the Applicant as a Domain Contact	3.2.2.4.1 Validating the Applicant as a Domain Contact	
Not applicable	Not applicable	
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact	3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact	
Confirming the Applicant's control over the FQDN by sending a Random Value via	Confirming the Applicant's control over the FQDN by sending a Random Value via	
email and then receiving a confirming response utilizing the Random Value. The	email and then receiving a confirming response utilizing the Random Value. The	
Random Value MUST be sent to an email address listed in the WHOIS record.	Random Value MUST be sent to an email address listed in the WHOIS record.	
The CA does not use fax, SMS, or postal mail to send a Random Values.	The CA does not use fax, SMS, or postal mail to send a Random Values.	
The Random Value SHALL be unique in each email. The Random Value SHALL	The Random Value SHALL be unique in each email. The Random Value SHALL	
remain valid for use in a confirming response for no more than 25 days from its	remain valid for use in a confirming response for no more than 25 days from its	
creation.	creation.	木籾訂士社の担併数了たっい
For certificates issued on or after 2025-7-10, this method will no longer be applicable.	For certificates issued on or after 2025-7-10, this method will no longer be applicable.	本認証方法の提供終了について 追記
3.2.2.4.3 Phone Contact with Domain Contact	3.2.2.4.3 Phone Contact with Domain Contact	て但記
Not applicable	Not applicable	
3.2.2.4.4 Constructed Email to Domain Contact	3.2.2.4.4 Constructed Email to Domain Contact	
Confirm the Applicant's control over the FQDN by	Confirm the Applicant's control over the FQDN by	
1. Sending an email to one or more addresses created by using 'admin',	1. Sending an email to one or more addresses created by using 'admin',	
'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part,	'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part,	
followed by the at-sign (""@""), followed by the Authorization Domain Name;	followed by the at-sign (""@""), followed by the Authorization Domain Name;	
and	and	
2. including a Random Value in the email; and	2. including a Random Value in the email; and	
3. receiving a confirming response utilizing the Random Value.	3. receiving a confirming response utilizing the Random Value.	
The Random Value SHALL be unique in each email. The Random Value SHALL	The Random Value SHALL be unique in each email. The Random Value SHALL	
remain valid for use in a confirming response for no more than 25 days from its	remain valid for use in a confirming response for no more than 25 days from its	
creation.	creation.	
3.2.2.4.5 Domain Authorization Document	3.2.2.4.5 Domain Authorization Document	
Not applicable	Not applicable	
3.2.2.4.6 Agreed-Upon Change to Website	3.2.2.4.6 Agreed-Upon Change to Website	
Not applicable	Not applicable	
3.2.2.4.7 DNS Change	3.2.2.4.7 DNS Change	

#### 整形版

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value in a DNS TXT record of the Authorization Domain Name that is prefixed with a Domain Label that begins with "\_acme-challenge".

The CA MUST provide a Random Value unique to the certificate request. The Random Value MUST remain valid for use in a confirming response for no more than 25 days from its creation.

The CA performing validations using this method MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same Random Value as the Primary Network Perspective.

#### 3.2.2.4.8 IP Address

Not applicable

#### 3.2.2.4.9 Test Certificate

Not applicable

3.2.2.4.10 TLS Using a Random Value

Not applicable

#### 3.2.2.4.11 Any Other Method

Not applicable

#### 3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the registrant of the domain name. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

#### 3.2.2.4.13 Email to DNS CAA Contact

Not applicable

#### 3.2.2.4.14 Email to DNS TXT Contact

Not applicable Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact for the Authorization Domain Name selected to validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email. The email MAY be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 25 days from its creation.

This method will be applicable for certificates issued on or after 2025-5-29.

Confirming the Applicant's control over the FQDN by confirming th Random Value in a DNS TXT record of the Authorization Domain prefixed with a Domain Label that begins with "\_acme-challenge".

The CA MUST provide a Random Value unique to the certificate Random Value MUST remain valid for use in a confirming response fo 25 days from its creation.

The CA performing validations using this method MUS Multi-Perspective Issuance Corroboration as specified in Section 3.2.2 corroborating, a Network Perspective MUST observe the same Rando Primary Network Perspective.

#### 3.2.2.4.8 IP Address

Not applicable

3.2.2.4.9 Test Certificate

Not applicable

3.2.2.4.10 TLS Using a Random Value

Not applicable

3.2.2.4.11 Any Other Method

Not applicable

#### 3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the A registrant of the domain name. This method may only be used if the Domain Name Registrar, or an Affiliate of the Registrar, of the Name.3.2.2.4.13 Email to DNS CAA Contact

Not applicable

#### 3.2.2.4.14 Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Ran email and then receiving a confirming response utilizing the Rand Random Value MUST be sent to a DNS TXT Record Email Con-Authorization Domain Name selected to validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided the address is DNS TXT Record Email Contact for each Authorization being validated. The same email MAY be sent to multiple recipients recipients are DNS TXT Record Email Contacts for each Authorization Name being validated.

The Random Value SHALL be unique in each email. The email MAY be entirety, including the re-use of the Random Value, provided that its and recipient(s) SHALL remain unchanged. The Random Value SHAL for use in a confirming response for no more than 25 days from its creat This method will be applicable for certificates issued on or after 2025-

ne presence of a n Name that is	備考
request. The or no more than	
ST implement 2.9. To count as om Value as the	Baseline Requirements改訂 に伴う追記
Applicant is the CA is also the Base Domain	
ndom Value via lom Value. The contact for the	本認証方法について追記
hat each email Domain Name s as long as all azation Domain	
be re-sent in its entire contents LL remain valid ation. 5-29.	

敷Ŧ	钐	版

The CA performing validations using this method MUST implement	The CA performing validations using this method MUST
Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as	Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9
corroborating, a Network Perspective MUST observe the same selected contact	corroborating, a Network Perspective MUST observe the same sele
address used for domain validation as the Primary Network Perspective.	address used for domain validation as the Primary Network Perspective
3.2.2.4.15 Phone Contact with Domain Contact	3.2.2.4.15 Phone Contact with Domain Contact
Not applicable	Not applicable
3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact	3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact
Not applicable	Not applicable
3.2.2.4.17 Phone Contact with DNS CAA Phone Contact	3.2.2.4.17 Phone Contact with DNS CAA Phone Contact
Not applicable	Not applicable
3.2.2.4.18 Agreed-Upon Change to Website v2	3.2.2.4.18 Agreed-Upon Change to Website v2
Confirming the Applicant's control over the FQDN by verifying that the Random	Confirming the Applicant's control over the FQDN by verifying that
Value is contained in the contents of a file.	Value is contained in the contents of a file.
1. The entire Random Value MUST NOT appear in the request used to retrieve	1. The entire Random Value MUST NOT appear in the request use
the file, and	the file, and
2. the CA MUST receive a successful HTTP response from the request (meaning	2. the CA MUST receive a successful HTTP response from the requ
a 2xx HTTP status code must be received).	a 2xx HTTP status code must be received).
The file containing the Random Value:	The file containing the Random Value:
1. MUST be located on the Authorization Domain Name, and	1. MUST be located on the Authorization Domain Name, and
2. MUST be located under the "/.well-known/pki-validation" directory, and	2. MUST be located under the "/.well-known/pki-validation" director
3. MUST be retrieved via either the "http" or "https" scheme, and	3. MUST be retrieved via either the "http" or "https" scheme, and
4. MUST be accessed over port 80 (http) or 443 (https).	4. MUST be accessed over port 80 (http) or 443 (https).
If the CA follows redirects, the following apply:	If the CA follows redirects, the following apply:
1. Redirects MUST be initiated at the HTTP protocol layer.	1. Redirects MUST be initiated at the HTTP protocol layer.
$\cdot$ Redirects MUST be the result of a 301, 302, or 307 HTTP status code	$\cdot$ Redirects MUST be the result of a 301, 302, or 307 HTTE
response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status	response, as defined in RFC 7231, Section 6.4, or a 308
code response, as defined in RFC 7538, Section 3.	code response, as defined in RFC 7538, Section 3.
$\cdot$ Redirects MUST be to the final value of the Location HTTP response	$\cdot$ Redirects MUST be to the final value of the Location HT
header, as defined in RFC 7231, Section 7.1.2.	header, as defined in RFC 7231, Section 7.1.2.
2. Redirects MUST be to resource URLs with either the "http" or "https"	2. Redirects MUST be to resource URLs with either the "http
scheme.	scheme.
3. Redirects MUST be to resource URLs accessed via port 80 (http) or 443	3. Redirects MUST be to resource URLs accessed via port 80 (
(https).	(https).
The CA MUST provide a Random Value unique to the certificate request. The	The CA MUST provide a Random Value unique to the certificate r
Random Value MUST remain valid for use in a confirming response for no more than	Random Value MUST remain valid for use in a confirming response for
25 days from its creation.	25 days from its creation.
For Certificates issued on or after 2021-11-18, this method is not applicable for	For Certificates issued on or after 2021-11-18, this method is not a
validating Wildcard Domain Names.	validating Wildcard Domain Names.
Except for Onion Domain Names, the CA performing validations using this method	Except for Onion Domain Names, the CA performing validations using

16/63

	備考
ST implement	
2.9. To count as	
elected contact	
ive.	
at the Random	
used to retrieve	
quest (meaning	
ctory, and	
d	
u	
TP status code	
98 HTTP status	
HTTP response	
ttp" or "https"	
-	
0 (http) or 443	
- (p, 01 110	
roquest The	
e request. The	
or no more than	
<b>.</b>	
t applicable for	
ing this method	Baseline Requirements改訂

# MUST implement Multi-Perspective Issuance Corroboration as specified in Section 3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same Random Value as the Primary Network Perspective.

#### 3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

- 1. The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).
- 2. The CA MUST provide a Random Value unique to the certificate request. The Random Value MUST remain valid for use in a confirming response for no more than 25 days from its creation.
- 3. If the CA follows redirects, the following apply:
  - $1.\,Redirects\,MUST$  be initiated at the HTTP protocol layer.
    - Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3.
    - Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
  - 2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
  - 3. Redirects MUST be to resource URLs accessed via port 80 (http) or 443 (https).

This method is not applicable for validating Wildcard Domain Names.

Except for Onion Domain Names, the CA performing validations using this method <u>MUST implement Multi-Perspective Issuance Corroboration as specified in Section</u> <u>3.2.2.9. To count as corroborating, a Network Perspective MUST observe the same</u> Random Value as the Primary Network Perspective.

#### 3.2.2.4.20 TLS Using ALPN

Not applicable

3.2.2.4.21 DNS Labeled with Account ID - ACME

Not applicable

#### 3.2.2.5 Authentication for an IP Address

The CA does not issue any certificate to grant certification to any IP Address.

#### 3.2.2.6 Wildcard Domain Validation

Before issuing a Wildcard Certificate, the CA MUST establish and follow a documented procedure that determines if the FQDN portion of any Wildcard Domain Name in the MUST implement Multi-Perspective Issuance Corroboration as speci 3.2.2.9. To count as corroborating, a Network Perspective MUST obs Random Value as the Primary Network Perspective.

整形版

#### 3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain FQDN using the ACME HTTP Challenge method defined in Section 8. The following are additive requirements to RFC 8555.

- 1. The CA MUST receive a successful HTTP response from (meaning a 2xx HTTP status code must be received).
- 2. The CA MUST provide a Random Value unique to the cert The Random Value MUST remain valid for use in a confirmin no more than 25 days from its creation.
- 3. If the CA follows redirects, the following apply:
  - 1. Redirects MUST be initiated at the HTTP protocol layer.
    - Redirects MUST be the result of a 301, 302, or 30 code response, as defined in RFC 7231, Section HTTP status code response, as defined in RFC 753
    - Redirects MUST be to the final value of the L response header, as defined in RFC 7231, Section
  - 2. Redirects MUST be to resource URLs with either the "h scheme.
  - 3. Redirects MUST be to resource URLs accessed via port 80 (https).

This method is not applicable for validating Wildcard Domain Names.

Except for Onion Domain Names, the CA performing validations usin MUST implement Multi-Perspective Issuance Corroboration as specif 3.2.2.9. To count as corroborating, a Network Perspective MUST obs Random Value as the Primary Network Perspective.

#### 3.2.2.4.20 TLS Using ALPN

Not applicable

3.2.2.4.21 DNS Labeled with Account ID - ACME

Not applicable

#### 3.2.2.5 Authentication for an IP Address

The CA does not issue any certificate to grant certification to any IP Address

#### 3.2.2.6 Wildcard Domain Validation

Before issuing a Wildcard Certificate, the CA MUST establish and follow procedure that determines if the FQDN portion of any Wildcard Domain

ified in Section	備考 に伴う追記
serve the same	
n control of the	
3.3 of RFC 8555.	
m the request	
tificate request.	
ng response for	
07 HTTP status	
n 6.4, or a 308 38, Section 3.	
Location HTTP	
7.1.2. http" or "https"	
30 (http) or 443	
ng this method	Baseline Requirements改訂
fied in Section	
serve the same	
	Baseline Requirements改訂
	に伴う追記
5.	
a documented n Name in the	

Certificate is "registry-controlled" or is a "public suffix" (e.g. "\*.com", "\*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public suffix", CAs MUST refuse issuance unless the Applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs MUST NOT issue "\*.co.uk" or "\*.local", but MAY issue '\*.example.com" to Example Co.).

Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is accordance with Baseline Requirements.

#### 3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA considers the following during its evaluation:

- 1. The age of the information provided,
- 2. The frequency of updates to the information source,
- 3. The data provider and purpose of the data collection,
- 4. The public accessibility of the data availability, and
- 5. The relative difficulty in falsifying or altering the data.

#### 3.2.2.8 CAA Records

As part of the Certificate issuance process, the CA MUST retrieve and process CAA records in accordance with RFC 8659 for each dNSName in the subjectAltName extension that does not contain an Onion Domain Name. If the CA issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

Some methods relied upon for validating the Applicant's ownership or control of the subject domain(s) (see Section 3.2.2.4) to be listed in a certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see Section 3.2.2.9). To corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue regardless of whether the responses from both Perspectives are byte-for-byte identical Additionally, the CA MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

When processing CAA records, the CA MUST process the issue, issuewild, and iddef When processing CAA records, the CA MUST process the issue, issuew property tags as specified in RFC 8659, although the CA does not act on the contents of the

Certificate is "registry-controlled" or is a "public suffix" (e.g. "\*.com", "\*.com", "\*.com"). 6454 Section 8.2 for further explanation).

If the FQDN portion of any Wildcard Domain Name is "registry-controlled" suffix", CAs MUST refuse issuance unless the Applicant proves its rightful entire Domain Namespace. (e.g. CAs MUST NOT issue "\*.co.uk" or "\*.local". '\*.example.com" to Example Co.).

Determination of what is "registry-controlled" versus the registerable portio Code Top-Level Domain Namespace is accordance with Baseline Requirement

#### 3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, the CA SHAL source for its reliability, accuracy, and resistance to alteration or falsific considers the following during its evaluation:

- 1. The age of the information provided,
- 2. The frequency of updates to the information source,
- 3. The data provider and purpose of the data collection,
- 4. The public accessibility of the data availability, and
- 5. The relative difficulty in falsifying or altering the data.

#### 3.2.2.8 CAA Records

As part of the Certificate issuance process, the CA MUST retrieve and proce in accordance with RFC 8659 for each dNSName in the subjectAltName exte not contain an Onion Domain Name. If the CA issues, they MUST do so wit the CAA record, or 8 hours, whichever is greater.

Some methods relied upon for validating the Applicant's ownership or control domain(s) (see Section 3.2.2.4) to be listed in a certificate require CAA retrieved and processed from additional remote Network Perspectives bet issuance (see Section 3.2.2.9). To corroborate the Primary Network Perspe Network Perspective's CAA check response MUST be interpreted as perm regardless of whether the responses from both Perspectives are byte-for Additionally, the CA MAY consider the response from a remote Network corroborating if one or both of the Perspectives experience an acceptable CAA failure, as defined in this section.

property tags as specified in RFC 8659, although the CA does not act on the

#### 整形版

	備考
o.uk", see RFC	V田 <del>ハ</del> ウ
" or is a "public Il control of the , but MAY issue	
on of a Country nts.	
L evaluate the cation. The CA	
ess CAA records ension that does thin the TTL of	
ol of the subject A records to be fore Certificate ective, a remote hission to issue, -byte identical. Perspective as A record lookup	Baseline Requirements改訂 に伴う追記
wild, and iodef contents of the	

変更履歴あり	整形版
iodef property tag. Where are additional property tags are supported, the CA MUST NOT conflict with or supersede the mandatory property tags set out in Baseline Requirements.	iodef property tag. Where are additional property tags are supported, the CA conflict with or supersede the mandatory property tags set out in Baseline Rec
The CA MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property tag with this flag set.	The CA MUST respect the critical flag and not issue a certificate if they ourrecognized property tag with this flag set.
<ul> <li>The CA is permitted to treat a record lookup failure as permission to issue if:</li> <li>the failure is outside the CA's infrastructure; and</li> <li>the lookup has been retried at least once; and</li> <li>the domain's zone does not have a DNSSEC validation chain to the ICANN root.</li> </ul>	<ul> <li>The CA is permitted to treat a record lookup failure as permission to issue if:</li> <li>the failure is outside the CA's infrastructure; and</li> <li>the lookup has been retried at least once; and</li> <li>the domain's zone does not have a DNSSEC validation chain to the ICA</li> </ul>
The CA shall log any actions taken as part of its processing practices.	The CA shall log any actions taken as part of its processing practices.
<u>3.2.2.9 Multi-Perspective Issuance Corroboration</u> On or after 2025-3-15, the CA implements Multi-Perspective Issuance Corroboration in accordance with section 3.2.2.9 of the Baseline Requirements.	<b>3.2.2.9 Multi-Perspective Issuance Corroboration</b> On or after 2025-3-15, the CA implements Multi-Perspective Issuance Corraccordance with section 3.2.2.9 of the Baseline Requirements.
<ul> <li><u>Before Certificate issuance, the CA will corroborate the following determinations made by the Primary Network Perspective from multiple remote Network Perspectives:</u> <ul> <li>the presence of the expected 1) Random Value, 2) Request Token, 3) Contact Address as specified in this CP "3.2.2.4 Domain Authentication"</li> <li>the CA's authority to issue to the requested domain(s), as specified in this CP "3.2.2.8 CAA Records"</li> </ul> </li> </ul>	<ul> <li>Before Certificate issuance, the CA will corroborate the following determinate the Primary Network Perspective from multiple remote Network Perspectives</li> <li>the presence of the expected 1) Random Value, 2) Request Token, 3) Corras specified in this CP "3.2.2.4 Domain Authentication"</li> <li>the CA's authority to issue to the requested domain(s), as specified in the CAA Records"</li> </ul>
The "Quorum Requirements" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If the CA does NOT rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements MUST be met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.	The "Quorum Requirements" Table describes quorum requirements Multi-Perspective Issuance Corroboration. If the CA does NOT rely on the Network Perspectives for both Domain Authorization or Control and CAA Re the quorum requirements MUST be met for both sets of Network Perspec Domain Authorization or Control set and the CAA record check set). Network are considered distinct when the straight-line distance between them is at 1 Network Perspectives are considered "remote" when they are distinct from Network Perspective and the other Network Perspectives represented in a quo
The CA MAY reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives MAY omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days. <u>Table 3.2.2.9-1 Quorum Requirements</u>	The CA MAY reuse corroborating evidence for CAA record quorum comp maximum of 398 days. After issuing a Certificate to a domain, remote Network MAY omit retrieving and processing CAA records for the same domain or its su subsequent Certificate requests from the same Applicant for up to a maximum Table 3.2.2.9-1 Quorum Requirements
<u># of Distinct Remote Network</u> <u># of Allowed non-Corroborations</u>	# of Distinct Remote Network # of Allowed non-Corroborations

Perspectives Used

	備考
CA MUST NOT	
equirements.	
y encounter an	
:	
CANN root.	
orroboration in	Baseline Requirements改訂 に伴う追記
ations made by es:	
ontact Address	
this CP "3.2.2.8	
ts related to he same set of Record checks, ectives (i.e.,the rk Perspectives t least 500 km. m the Primary uorum.	
mpliance for a rk Perspectives subdomains in im of 398 days.	

	変更履歴あり			整刑	<b>彩版</b>	
<u>2-5</u>	<u>1</u>		2-5		1	
<u>6+</u>	2		6+		2	

#### Phased Implementation Timeline:

- On or after 2025-3-15, the CA implements Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. The CA MAY proceed with certificate issuance if the number of remote Network Perspectives that do not corroborate the determinations made by the Primary Network Perspective ("non-corroborations") is greater than allowed in the Quorum Requirements table.
- On or after 2025-09-15, the CA MUST implement Multi-Perspective Issuance Corroboration using at least five (5) remote Network Perspectives. The CA MUST ensure that the requirements defined in the Quorum Requirements Table are satisfied, and the remote Network Perspectives that corroborate the Primary Network Perspective fall within the service regions of at least two (2) distinct Regional Internet Registries. If the requirements are not satisfied, then the CA MUST NOT proceed with issuance of the Certificate.

#### 3.2.3 Authentication of Individual Identity

The CA does not issue any certificate to grant certification to any individual.

#### 3.2.4 Non-Verified Subscriber Information

(1) Domain Validation

The CA stipulates no policies on non-verified information on Subscribers. (2) Organization Validation

The CA stipulates no policies on non-verified information on Subscribers.

#### 3.2.5 Validation of Authority

(1) Domain Validation

When issuing a certificate, the CA shall verify that the Subscriber is a registrant of the domain name to be described in the certificate or has been granted an exclusive right to use the domain name by the registrant.

(2) Organization Validation

The CA shall verify that an applicant for a certificate has the legitimate authority to apply for a certificate by making contact with a contact person that may be verified by any document, database, or other information source to be used for "3.2.2. Authentication of an Organization's Identity and Domain Name" of this CP.

3.2.6 Criteria for Interoperation

#### Phased Implementation Timeline:

On or after 2025-3-15, the CA implements Multi-Perspective Issuance using at least two (2) remote Network Perspectives. The CA MAY certificate issuance if the number of remote Network Perspectives corroborate the determinations made by the Primary Networ ("non-corroborations") is greater than allowed in the Quorum Requirement

On or after 2025-09-15, the CA MUST implement Multi-Perspector Corroboration using at least five (5) remote Network Perspectives. The ensure that the requirements defined in the Quorum Requirements Table and the remote Network Perspectives that corroborate the Print Perspective fall within the service regions of at least two (2) distinct Rep Registries. If the requirements are not satisfied, then the CA MUST NO issuance of the Certificate.

#### 3.2.3 Authentication of Individual Identity

The CA does not issue any certificate to grant certification to any individual.

#### **3.2.4 Non-Verified Subscriber Information**

(1) Domain Validation

The CA stipulates no policies on non-verified information on Subscribers.

(2) Organization Validation

The CA stipulates no policies on non-verified information on Subscribers.

#### 3.2.5 Validation of Authority

#### (1) Domain Validation

When issuing a certificate, the CA shall verify that the Subscriber is a redomain name to be described in the certificate or has been granted an exclusthe domain name by the registrant.

(2) Organization Validation

The CA shall verify that an applicant for a certificate has the legitimate aut for a certificate by making contact with a contact person that may be v document, database, or other information source to be used for "3.2.2. Author Organization's Identity and Domain Name" of this CP.

#### 3.2.6 Criteria for Interoperation

	備考
e Corroboration	
Y proceed with	
es that do not	
rk Perspective	
ients table.	
ective Issuance	
The CA MUST	
ole are satisfied,	
mary Network	
egional Internet	
OT proceed with	
egistrant of the	
sive right to use	
thority to apply	
verified by any	
entication of an	

#### A certificate for one-way mutual certification has been issued to the CA by Security Communication RootCA2, Security Communication ECC RootCA1 or SECOM TLS RSA Root CA 2024, a Certification Authority operated by SECOM Trust Systems.

#### 3.3 Identification and Authentication for Re-key Requests

The CA shall perform validate and authenticate the identity of any Subscriber at a rekey in the same manner as set forth in "3.2 Initial Identity Validation" of this CP.

## 3.4 Identification and Authentication for Revocation Request

The CA shall validate an identity in order to accept Revocation Request by check one of the following;

- 1. The Revocation Request from any Subscriber through the Designated Business Enterprise that has acted as an agent in the application for issuance of the certificate or use of services.
- 2. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the account granted to the subscriber.
- 3. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate.

## 4. Certificate Life-Cycle Operational Requirements

#### 4.1 Certificate Application

#### 4.1.1 Who Can Submit a Certificate Application

#### (1) Domain Validation

A person who is a registrant of the domain name to be described in a certificate or has been granted an exclusive right to use the domain name by the registrant may apply for the certificate.

#### (2) Organization Validation

A person who is a sole proprietor having his/her address within Japan, or an organization having its head office or principal office, branch office or subdivision, place of business, or other equivalent permanent place to the foregoing within Japan, whether incorporated or unincorporated, may apply for the certificate.

#### 4.1.2 Enrollment Process and Responsibilities

Each person who may apply for a certificate and intends to do so shall apply for the certificate after consenting to the provisions of the Terms and Conditions, this CP, and the CPS. Each person applying for a certificate must assure that the information provided in the Certificate Application submitted to the CA is accurate.

#### 4.2 Certificate Application Processing

A certificate for one-way mutual certification has been issued to the C Communication RootCA2, Security Communication ECC RootCA1 or SEC Root CA 2024, a Certification Authority operated by SECOM Trust Systems.

#### 3.3 Identification and Authentication for Re-key Request

The CA shall perform validate and authenticate the identity of any Subscribe the same manner as set forth in "3.2 Initial Identity Validation" of this CP.

#### 3.4 Identification and Authentication for Revocation Req

The CA shall validate an identity in order to accept Revocation Request by carfollowing;

- 1. The Revocation Request from any Subscriber through the Design Enterprise that has acted as an agent in the application for is certificate or use of services.
- 2. The certificate issued under ACME protocol and the Revocation Requ private key of the account granted to the subscriber.
- 3. The certificate issued under ACME protocol and the Revocation Requ private key of the certificate.

## 4. Certificate Life-Cycle Operational Require

#### 4.1 Certificate Application

#### 4.1.1 Who Can Submit a Certificate Application

#### (1) Domain Validation

A person who is a registrant of the domain name to be described in a certificar granted an exclusive right to use the domain name by the registrant may certificate.

#### (2) Organization Validation

A person who is a sole proprietor having his/her address within Japan, or a having its head office or principal office, branch office or subdivision, place other equivalent permanent place to the foregoing within Japan, whether is unincorporated, may apply for the certificate.

#### 4.1.2 Enrollment Process and Responsibilities

Each person who may apply for a certificate and intends to do so shall certificate after consenting to the provisions of the Terms and Conditions, the CPS. Each person applying for a certificate must assure that the information the Certificate Application submitted to the CA is accurate.

#### 4.2 Certificate Application Processing

#### 整形版

	備考
CA by Security	
COM TLS RSA	
i.	
ts	
per at a rekey in	
quest	
check one of the	
check one of the	
nated Business	
issuance of the	
uest is signed by	
lest is signed by	
ements	
cate or has been	
y apply for the	
an organization	
e of business, or	
incorporated or	
ll apply for the	
this CP, and the	
tion provided in	

#### 4.2.1 Performing Identification and Authentication Functions

The CA shall review application information by considering the information in the manner set forth in "3.2 Initial Identity Validation" of this CP.

The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information MUST include, but not be limited to, at least one Fully-Qualified Domain Name or IP address to be included in the Certificate's subjectAltName extension.

Section 6.3.2 of this CP limits the validity period of Subscriber Certificates.

The CA MAY use the documents and data provided in Section 3.2 of this CP to verify certificate information, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 of this CP or completed the validation itself no more than 825 days prior to issuing the Certificate.

For validation of Domain Names according to Section 3.2.2.4 of this CP, any data, document, or completed validation used MUST be obtained no more than 398 days prior to issuing the Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

After the change to any validation method specified in the Baseline Requirements, the CA may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this section unless otherwise specifically provided in a ballot.

The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

#### 4.2.1 Performing Identification and Authentication Function

The CA shall review application information by considering the information set forth in "3.2 Initial Identity Validation" of this CP.

The certificate request MAY include all factual information about the A included in the Certificate, and such additional information as is necessary obtain from the Applicant in order to comply with these Requirements Certificate Policy and/or Certification Practice Statement. In cases where request does not contain all the necessary information about the Applicant, robtain the remaining information from the Applicant or, having obtained it findependent, third-party data source, confirm it with the Applicant. The stablish and follow a documented procedure for verifying all data requested the Certificate by the Applicant.

Applicant information MUST include, but not be limited to, at least one I Domain Name or IP address to be included in the Certificate's subjectAltNam

Section 6.3.2 of this CP limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 of thi certificate information, or may reuse previous validations themselves, provid obtained the data or document from a source specified under Section 3.2 completed the validation itself no more than 825 days prior to issuing the Ce

For validation of Domain Names according to Section 3.2.2.4 of this CP, any d or completed validation used MUST be obtained no more than 398 days prior Certificate.

In no case may a prior validation be reused if any data or document use validation was obtained more than the maximum time permitted for reuse document prior to issuing the Certificate.

After the change to any validation method specified in the Baseline Require may continue to reuse validation data or documents collected prior to the validation itself, for the period stated in this section unless otherwise specif in a ballot.

The CA SHALL develop, maintain, and implement documented procedure and require additional verification activity for High Risk Certificate Request Certificate's approval, as reasonably necessary to ensure that such request verified under these Requirements.

#### 整形版

	備考
IS	
n in the manner	
Applicant to be by for the CA to a and the CA's the certificate the CA SHALL from a reliable, 'he CA SHALL for inclusion in	
Fully-Qualified me extension.	
is CP to verify ded that the CA 2 of this CP or ertificate.	
data, document, or to issuing the	
ed in the prior e of the data or	
ements, the CA change, or the fically provided	
es that identify ests prior to the sts are properly	

変更履歴あり	整形版
4.2.2 Approval or Rejection of a Certificate Application	4.2.2 Approval or Rejection of a Certificate Application
On approving any certificate application as a result of the review, the CA shall proceed to	On approving any certificate application as a result of the review, the CA shall proceed to
the issuance registration of the certificate.	the issuance registration of the certificate.
If any certificate application is not complete, the CA shall reject the application and request	If any certificate application is not complete, the CA shall reject the application and request
the person who has submitted the application to submit an application again after	the person who has submitted the application to submit an application again after
correction or addition.	correction or addition.
4.2.3 Time to Process Certificate Applications	4.2.3 Time to Process Certificate Applications
After approving a certificate application, the CA shall proceed to the issuance registration of	After approving a certificate application, the CA shall proceed to the issuance registration of
the certificate in a timely manner.	the certificate in a timely manner.
4.2.4 Check of CAA Records	4.2.4 Check of CAA Records
In reviewing the application information, the CA shall check the CAA records in accordance	
with RFC 8659. The domain name of the CA to be described in the CAA records shall be	with RFC 8659. The domain name of the CA to be described in the CAA records shall be
"jprs.jp" or "acme.jprs.jp".	"jprs.jp" or "acme.jprs.jp".
The Certificate Subscribers who want to grant the authority to issue certificates to the FQDN must include one of the following domain names in the property "issue" or	FQDN must include one of the following domain names in the property "issue" or
"issuewild" of the CAA record for each DNS zone.	"issuewild" of the CAA record for each DNS zone.
jprs.jp (for certificates issued without using the ACME protocol)	jprs.jp (for certificates issued without using the ACME protocol)
acme.jprs.jp (for certificates issued using the ACME protocol)	acme.jprs.jp (for certificates issued using the ACME protocol)
4.3 Certificate Issuance	4.3 Certificate Issuance
4.3.1 CA Actions during Certificate Issuance	4.3.1 CA Actions during Certificate Issuance
After completing a review of a certificate application, the CA shall register information that	After completing a review of a certificate application, the CA shall register information that
is based on the application information and necessary for the issuance of a certificate, on a	is based on the application information and necessary for the issuance of a certificate, on a
CT log server operated by a third party and prescribed by the CA, and then issue the	
	certificate. The information to be registered on the CT log server shall be as described in
"7.1 Certificate Profile" of this CP.	"7.1 Certificate Profile" of this CP.
4.3.1.1 Manual authorization of certificate issuance for Root CAs	4.3.1.1 Manual authorization of certificate issuance for Root CAs
No stipulation.	No stipulation.
4.3.1.2 Linting of to-be-signed Certificate content	4.3.1.2 Linting of to-be-signed Certificate content
	The CA confirms whether the certificate to be issued technically conforms to Baseline
	Requirements for some items by the pre-certificate linting function and refuses to issue if it
does not meet the requirements.	does not meet the requirements.
4.3.1.3 Linting of issued Certificates	4.3.1.3 Linting of issued Certificates
The CA MAY use a Linting process to test each issued Certificate.	The CA MAY use a Linting process to test each issued Certificate.
4.3.2 Notification to Subscriber of Certificate Issuance	4.3.2 Notification to Subscriber of Certificate Issuance

#### 整形版

The CA shall notify a Subscriber of the issuance of a certificate by sending an e-mail to the Designated Business Enterprise or the Subscriber. However, if the certificate issued under ACME protocol, no notification sending an e-mail.

#### 4.4 Certificate Acceptance

#### 4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber shall be deemed to have accepted the certificate at any of the following time;

- 1. When the Subscriber requests to get the certificate from the subscriber-only web page and the CA responses the Certificate.
- 2. When the subscriber requests to get the certificate under ACME protocol and the CA responses the Certificate. However, only for certificates issued under ACME protocol.
- 3. When the subscriber installs the certificate obtained by a method other than 1 and 2 into his/her/its server.

#### 4.4.2 Publication of the Certificates by the CA

The CA does not publish certificates of Subscribers.

#### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CA does not notify any third party (excluding Designated Business Enterprises) of the issuance of certificates.

#### 4.5 Key Pair and Certificate Usage

#### 4.5.1 Subscriber Private Key and Certificate Usage

Each Subscriber may use his/her/its certificate issued by the CA and the corresponding Private Key solely for encrypting information for server authentication and on communication pathways, and not for any other usage.

#### 4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties may verify the reliability of certificates issued by the CA by using such certificates. Relying Parties shall understand and consent to the provisions of this CP and the CPS before verifying the reliability of certificates issued by the CA and relying on the same.

#### 4.6 Certificate Renewal

A "certificate renewal" means the issuance of a new certificate to a Subscriber without any change in his/her/its Public Key. When a Subscriber has his/her/its certificate renewed, the CA recommends that the Subscriber generate a new Key Pair.

#### 4.6.1 Circumstances for Certificate Renewal

A certificate may be renewed without involving rekey when the certificate is about to expire.

The CA shall notify a Subscriber of the issuance of a certificate by sending a Designated Business Enterprise or the Subscriber. However, if the certificat ACME protocol, no notification sending an e-mail.

#### 4.4 Certificate Acceptance

#### 4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber shall be deemed to have accepted the certificate at any of the

- 1. When the Subscriber requests to get the certificate from the subspage and the CA responses the Certificate.
- 2. When the subscriber requests to get the certificate under ACME process the Certificate. However, only for certificates issued protocol.
- 3. When the subscriber installs the certificate obtained by a method ot 2 into his/her/its server.

#### 4.4.2 Publication of the Certificates by the CA

The CA does not publish certificates of Subscribers.

#### 4.4.3 Notification of Certificate Issuance by the CA to Other

The CA does not notify any third party (excluding Designated Business Ent issuance of certificates.

#### 4.5 Key Pair and Certificate Usage

#### 4.5.1 Subscriber Private Key and Certificate Usage

Each Subscriber may use his/her/its certificate issued by the CA and the Private Key solely for encrypting information for server authentics communication pathways, and not for any other usage.

#### 4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties may verify the reliability of certificates issued by the CA certificates. Relying Parties shall understand and consent to the provisions the CPS before verifying the reliability of certificates issued by the CA and same.

#### 4.6 Certificate Renewal

A "certificate renewal" means the issuance of a new certificate to a Subscrib change in his/her/its Public Key. When a Subscriber has his/her/its certificat CA recommends that the Subscriber generate a new Key Pair.

#### 4.6.1 Circumstances for Certificate Renewal

A certificate may be renewed without involving rekey when the certificate is a

	備考
an e-mail to the	
te issued under	
e following time;	
criber-only web	
protocol and the	
d under ACME	
ther than 1 and	
r Entities	
terprises) of the	
terprises/ or the	
1.	
e corresponding	
cation and on	
A by using such	
s of this CP and	
d relying on the	
ber without any	
te renewed, the	
about to ovning	
about to expire.	

変更履歴あり	整形版	備考
4.6.2 Who May Request Renewal	4.6.2 Who May Request Renewal	
The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	
4.6.3 Processing Certificate Renewal Requests	4.6.3 Processing Certificate Renewal Requests	
The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply orrespondingly.	The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.	
4.6.4 Notification of New Certificate Issuance to Subscriber	4.6.4 Notification of New Certificate Issuance to Subscriber	
The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall pply correspondingly.	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate	4.6.5 Conduct Constituting Acceptance of a Renewal Certificate	
The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply orrespondingly.	The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.	
4.6.6 Publication of the Renewal Certificate by the CA	4.6.6 Publication of the Renewal Certificate by the CA	
The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply orrespondingly.	The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	
4.6.7 Notification of Certificate Issuance by the CA to Other Entities	4.6.7 Notification of Certificate Issuance by the CA to Other Entities	
The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of his CP shall apply correspondingly.	The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.	
<b>I.7 Certificate Re-key</b> A "certificate re-key" means the issuance of a new certificate to a Subscriber after generating a new Key Pair.	<b>4.7 Certificate Re-key</b> A "certificate re-key" means the issuance of a new certificate to a Subscriber after generating a new Key Pair.	
4.7.1 Circumstances for Certificate Re-key	4.7.1 Circumstances for Certificate Re-key	
A certificate may be renewed without involving re-key when the certificate is about to xpire.	A certificate may be renewed without involving re-key when the certificate is about to expire.	
4.7.2 Who May Request Certification of a New Public Key	4.7.2 Who May Request Certification of a New Public Key	
"he provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply orrespondingly.	The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	
4.7.3 Processing Certificate Re-keying Requests	4.7.3 Processing Certificate Re-keying Requests	
The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply prrespondingly.	The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.	
4.7.4 Notification of New Certificate Issuance to Subscriber	4.7.4 Notification of New Certificate Issuance to Subscriber	
The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	

変更履歴あり	整形版
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate	4.7.5 Conduct Constituting Acceptance of a Re-keyed Certifi
The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.	The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this correspondingly.
4.7.6 Publication of the Re-keyed Certificates by the CA	4.7.6 Publication of the Re-keyed Certificates by the CA
The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	The provisions of "4.4.2 Publication of the Certificates by the CA" of this C correspondingly.
4.7.7 Notification of Certificate Issuance by the CA to Other Entities	4.7.7 Notification of Certificate Issuance by the CA to Other
The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.	The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Oth this CP shall apply correspondingly.
4.8 Certificate Modification	4.8 Certificate Modification
4.8.1 Circumstances for Certificate Modification	4.8.1 Circumstances for Certificate Modification
If a need arises to modify any registered information in a certificate (excluding the common name used in the certificate), the certificate shall be modified.	If a need arises to modify any registered information in a certificate (excludin name used in the certificate), the certificate shall be modified.
4.8.2 Who May Request Certificate Modification	4.8.2 Who May Request Certificate Modification
The provisions of "4.1.1 Who Can Submit a Certificate Application" of this CP shall apply correspondingly.	The provisions of "4.1.1 Who Can Submit a Certificate Application" of this Correspondingly.
4.8.3 Processing Certificate Modification Requests	4.8.3 Processing Certificate Modification Requests
The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.1 CA Actions during Certificate Issuance" of this C correspondingly.
4.8.4 Notification of New Certificate Issuance to Subscriber	4.8.4 Notification of New Certificate Issuance to Subscriber
The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall apply correspondingly.	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of apply correspondingly.
4.8.5 Conduct Constituting Acceptance of Modified Certificate	4.8.5 Conduct Constituting Acceptance of Modified Certifica
The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply correspondingly.	The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this correspondingly.
4.8.6 Publication of the Modified Certificate by the CA	4.8.6 Publication of the Modified Certificate by the CA
The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	The provisions of "4.4.2 Publication of the Certificates by the CA" of this C correspondingly.
4.8.7 Notification of Certificate Issuance by the CA to Other Entities	4.8.7 Notification of Certificate Issuance by the CA to Other
The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of this CP shall apply correspondingly.	The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Oth this CP shall apply correspondingly.
4.9 Certificate Revocation and Suspension	4.9 Certificate Revocation and Suspension

	備考
ficate	
s CP shall apply	
CD shall apply	
CP shall apply	
r Entities	
ther Entities" of	
ing the common	
ing the common	
CP shall apply	
CP shall apply	
of this CP shall	
ate	
s CP shall apply	
CP shall apply	
r Entities	
ther Entities" of	

#### 変更履歴あり 整形版 4.9.1 Circumstances for Certificate Revocation 4.9.1 Circumstances for Certificate Revocation If any one of the following events occurs, the Subscriber must apply to the CA to have the If any one of the following events occurs, the Subscriber must apply to the corresponding certificate revoked: corresponding certificate revoked: • the information described in the certificate has changed; • the information described in the certificate has changed; • the Private Key has been or may be compromised for any reason, including theft, loss • the Private Key has been or may be compromised for any reason, include leakage, or unauthorized use thereof; leakage, or unauthorized use thereof; • any of the particulars described in the certificate or its purposes of use are incorrect; • any of the particulars described in the certificate or its purposes of use • the Subscriber finds that an improper string has been designated for, or is included • the Subscriber finds that an improper string has been designated for, of in, a value set in any information in the certificate (as set forth in "3.1.1 Types of in, a value set in any information in the certificate (as set forth in "3.1. Names" of this CP) (for Organization Validation only); or Names" of this CP) (for Organization Validation only); or • the Subscriber stops using the certificate. • the Subscriber stops using the certificate. The CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason The CA SHALL revoke a Certificate within 24 hours and use the correspond if one or more of the following occurs: if one or more of the following occurs: 1. The Subscriber requests in writing, without specifying a CRL reason, that the CA 1. The Subscriber requests in writing, without specifying a CRL reason, revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode revoke the Certificate (CRLReason "unspecified (0)" which results in extension being provided in the CRL); extension being provided in the CRL); 2. The Subscriber notifies the CA that the original certificate request was not 2. The Subscriber notifies the CA that the original certificate request w authorized and does not retroactively grant authorization (CRLReason #9, authorized and does not retroactively grant authorization (CRLRease privilegeWithdrawn); privilegeWithdrawn); 3. The CA obtains evidence that the Subscriber's Private Key corresponding to the 3. The CA obtains evidence that the Subscriber's Private Key correspond Public Key in the Certificate suffered a Key Compromise (CRLReason #1, Public Key in the Certificate suffered a Key Compromise (CRLReaso keyCompromise); keyCompromise); 4. The CA is made aware of a demonstrated or proven method that can easily compute 4. The CA is made aware of a demonstrated or proven method that can the Subscriber's Private Key based on the Public Key in the Certificate, including the Subscriber's Private Key based on the Public Key in the Certifica but not limited to those identified in the Baseline Requirements Section 6.1.1.3(5), but not limited to those identified in the Baseline Requirements Section and CPS "6.1.1 Key Pair Generation" (CRLReason #1, keyCompromise); and CPS "6.1.1 Key Pair Generation" (CRLReason #1, keyCompromis 5. The CA obtains evidence that the validation of domain authorization or control for 5. The CA obtains evidence that the validation of domain authorization any Fully-Qualified Domain Name or IP address in the Certificate should not be any Fully-Qualified Domain Name or IP address in the Certificate sh relied upon (CRLReason #4, superseded). relied upon (CRLReason #4, superseded). The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate The CA SHOULD revoke a certificate within 24 hours and MUST revok within 5 days and use the corresponding CRLReason if one or more of the following occurs: within 5 days and use the corresponding CRLReason if one or more of the fol 6. The Certificate no longer complies with the requirements of <u>Section</u> 6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6 of Baseline Requirements (CRLReason #4, superseded); 6.1.5 and Section 6.1.6 of Baseline Requirements (CRLReason #4, su 7. The CA obtains evidence that the Certificate was misused (CRLReason #9, 7. The CA obtains evidence that the Certificate was misused (CRLReas privilegeWithdrawn); privilegeWithdrawn);

	備考
CA to have the	
ding theft, loss,	
e are incorrect;	
or is included	
.1 Types of	
ing CRLReason	
that the CA	
no reasonCode	
as not	
on #9,	
iding to the	
n #1,	
easily compute	
te , including	
tion 6.1.1.3(5), se);	
or control for	
nould not be	
ke a Certificate	
llowing occurs:	
perseded);	
on #9,	

- 8. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use (CRLReason #9, privilegeWithdrawn);
- 9. The CA is made aware of any circumstance indicating that use of a FQDN in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name (CRLReason #5, cessationOfOperation);
- 10. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN (CRLReason #9, privilegeWithdrawn);
- 11. The CA is made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn);
- 12. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's CP or CPS(CRLReason #4, superseded);
- 13. The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
- 14. The CA's right to issue Certificates under Baseline Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
- 15. Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement for a reason that is not otherwise required to be specified by this section 4.9.1.1 of Baseline Requirements (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL); or
- 16. The CA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

#### 4.9.2 Who Can Request Revocation

The following can request the Revocation Request;

- 1. The Subscriber
- 2. Designated Business Enterprise that has acted as an agent in the application for issuance of the certificate or use of services.
- 3. Owner of the private key for the Certificate.

#### 4.9.3 Procedures for Revocation Request

The CA SHALL accept the Revocation Request received in one of the following way, and The

#### 8. The CA is made aware that a Subscriber has violated one or more of i obligations under the Subscriber Agreement or Terms of Use (CRLRe privilegeWithdrawn);

整形版

- 9. The CA is made aware of any circumstance indicating that use of a F<sup>4</sup> Certificate is no longer legally permitted (e.g. a court or arbitrator ha Domain Name Registrant's right to use the Domain Name, a relevant services agreement between the Domain Name Registrant and the Ap terminated, or the Domain Name Registrant has failed to renew the I (CRLReason #5, cessationOfOperation);
- 10. The CA is made aware that a Wildcard Certificate has been used to a fraudulently misleading subordinate FQDN (CRLReason #9, privileg
- 11. The CA is made aware of a material change in the information contain Certificate (CRLReason #9, privilegeWithdrawn);
- 12. The CA is made aware that the Certificate was not issued in accorda Requirements or the CA's CP or CPS(CRLReason #4, superseded);
- 13. The CA determines or is made aware that any of the information app Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
- 14. The CA's right to issue Certificates under Baseline Requirements exp revoked or terminated, unless the CA has made arrangements to commaintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" in no reasonCode extension being provided in the CRL);
- 15. Revocation is required by the CA's Certificate Policy and/or Certificate Statement for a reason that is not otherwise required to be specified b 4.9.1.1 of Baseline Requirements (CRLReason "unspecified (0)" which reasonCode extension being provided in the CRL); or
- 16. The CA is made aware of a demonstrated or proven method that expo Subscriber's Private Key to compromise or if there is clear evidence the method used to generate the Private Key was flawed (CRLReason #1, keyCompromise).

#### 4.9.2 Who Can Request Revocation

The following can request the Revocation Request;

- 1. The Subscriber
- 2. Designated Business Enterprise that has acted as an agent in the issuance of the certificate or use of services.
- 3. Owner of the private key for the Certificate.

#### 4.9.3 Procedures for Revocation Request

The CA SHALL accept the Revocation Request received in one of the follow

	備考
its material	
eason #9,	
QDN in the	
as revoked a	
t licensing or	
pplicant has	
Domain Name)	
authenticate a	
geWithdrawn);	
ined in the	
nce with these	
ince with these	
accenter at the	
pearing in the	
•••••	
pires or is	
itinue " which results	
which results	
tion Dupation	
tion Practice	
by this section h results in no	
II Tesuits III IIo	
a a a a tha	
oses the	
that the specific	
-,	
application for	
1	
owing way, and	

revoke the certificate after verification the Revocation Request by section 3.4.

- 1. Request through Designated Business Enterprise
- 2. Request under ACME protocol

#### 4.9.4 Revocation Request Grace Period

If someone who can request revocation determines that the Private Key has been or may be compromised, he/she/it must promptly file the Revocation Request of the certificate.

The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

#### 4.9.5 Time within Which the CA Shall Process the Revocation Request

Upon accepting a valid Revocation Request of a certificate, the CA shall promptly process the Revocation Request and reflect the relevant information in the certificate on the CRL. Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1 of this CP.

#### 4.9.6 Revocation Checking Requirement for Relying Parties

A URL in which the CRL is stored shall be described in a certificate to be issued by the CA. Before placing trust in and using a certificate issued by the CA, the Relying Party must verify the validity of the certificate by checking the CRL. CRLs do not contain information on certificates that have expired.

#### 4.9.7 CRL Issuance Frequency

The CA SHALL update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

#### 4.9.8 Maximum Latency for CRLs

The CA shall forthwith reflect an issued CRL in the Repository.

#### 4.9.9 On-line Revocation/Status Checking Availability

Information on the certificate status shall be provided online via the OCSP server. OCSP responses MUST conform to RFC 6960 and/or RFC 5019. OCSP responses MUST either:

#### 整形版

revoke the certificate after verification the Revocation Request by section 3.4

- 1. Request through Designated Business Enterprise
- 2. Request under ACME protocol

#### 4.9.4 Revocation Request Grace Period

If someone who can request revocation determines that the Private Key has been or may be compromised, he/she/it must promptly file the Revocation Request of the certificate. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

#### 4.9.5 Time within Which the CA Shall Process the Revocation Request

Upon accepting a valid Revocation Request of a certificate, the CA shall promptly process the Revocation Request and reflect the relevant information in the certificate on the CRL. Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1 of this CP.

#### 4.9.6 Revocation Checking Requirement for Relying Parties

A URL in which the CRL is stored shall be described in a certificate to be issued by the CA. Before placing trust in and using a certificate issued by the CA, the Relying Party must verify the validity of the certificate by checking the CRL. CRLs do not contain information on certificates that have expired.

#### 4.9.7 CRL Issuance Frequency

The CA SHALL update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

#### 4.9.8 Maximum Latency for CRLs

The CA shall forthwith reflect an issued CRL in the Repository.

#### 4.9.9 On-line Revocation/Status Checking Availability

Information on the certificate status shall be provided online via the OCSP server. OCSP responses MUST conform to RFC 6960 and/or RFC 5019. OCSP responses MUST either:

L		
┡		
•	٠	

備考

- 1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
- 2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

#### 4.9.10 On-line Revocation/Status Checking Requirements

Before placing trust and using a certificate issued by the CA, the Relying Party must verify the validity of the certificate. If any Relying Party does not confirm whether or not the revocation of the certificate has been registered by checking the CRL included in the Repository, the Relying Party shall check the information on the certificate status provided through the OCSP server.

OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

- 1. OCSP responses MUST have a validity interval greater than or equal to eight hours;
- 2. OCSP responses MUST have a validity interval less than or equal to ten days;
- 3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
- 4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with <u>Section 7.1.2.3</u> or <u>Section 7.1.2.5</u>, the responder MUST NOT respond with a "good" status for such requests.

The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

#### 整形版

- 1. Be signed by the CA that issued the Certificates whose revocation statchecked, or
- 2. Be signed by an OCSP Responder whose Certificate is signed by the the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an type id-pkix-ocsp-nocheck, as defined by RFC 6960.

#### 4.9.10 On-line Revocation/Status Checking Requirements

Before placing trust and using a certificate issued by the CA, the Relying Pa the validity of the certificate. If any Relying Party does not confirm whet revocation of the certificate has been registered by checking the CRL in Repository, the Relying Party shall check the information on the certificate s through the OCSP server.

OCSP responders operated by the CA SHALL support the HTTP GET method in RFC 6960 and/or RFC 5019.

The validity interval of an OCSP response is the difference in the thisUpdate and nextUpdate field, inclusive. For purposes of comput a difference of 3,600 seconds shall be equal to one hour, and a difference of shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

- 1. OCSP responses MUST have a validity interval greater than or equal
- 2. OCSP responses MUST have a validity interval less than or equal to
- 3. For OCSP responses with validity intervals less than sixteen hours, a SHALL update the information provided via an Online Certificate St prior to one-half of the validity period before the nextUpdate.
- 4. For OCSP responses with validity intervals greater than or equal to a then the CA SHALL update the information provided via an Online O Status Protocol at least eight hours prior to the nextUpdate, and no l days after the thisUpdate.

If the OCSP responder receives a request for the status of a certificate serial "unused", then the responder SHOULD NOT respond with a "good" status responder is for a CA that is not Technically Constrained in line 7.1.2.3 or Section 7.1.2.5, the responder MUST NOT respond with a "good" strengests.

The CA SHOULD monitor the OCSP responder for requests for "unused" ser part of its security response procedures.

	備考
atus is being	
CA that issued	
n extension of	
arty must verify	
ether or not the	
included in the	
status provided	
-	
od, as described	
time between	
ting differences,	
86,400 seconds	
l to eight hours;	
o ten days;	
then the CA	
tatus Protocol	
sixteen hours,	
Certificate	
later than four	
l number that is	
as. If the OCSP	
ne with <u>Section</u>	
status for such	
rial numbers as	

変更履歴あり	整形版
The OCSP responder MAY provide definitive responses about "reserved" certificate serial	The OCSP responder MAY provide definitive responses about "reserved" cert
numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC 6962].	numbers, as if there was a corresponding Certificate that matches the Precer 6962].
A certificate serial number within an OCSP request is one of the following three options:	A certificate serial number within an OCSP request is one of the following three
<ol> <li>"assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject; or</li> <li>"reserved" if a Precertificate [RFC 6962] with that serial number has been issued by a. the Issuing CA; or b. a Precertificate Signing Certificate, as defined in <u>Section</u> <u>7.1.2.4</u>, associated with the Issuing CA; or</li> <li>"unused" if neither of the previous conditions are met.</li> </ol>	<ol> <li>"assigned" if a Certificate with that serial number has been issued by the CA, using any current or previous key associated with that CA subject;</li> <li>"reserved" if a Precertificate [RFC 6962] with that serial number has been issued by the Issuing CA; or b. a Precertificate Signing Certificate, as defined in <u>7.1.2.4</u>, associated with the Issuing CA; or</li> <li>"unused" if neither of the previous conditions are met.</li> </ol>
4.9.11 Other Forms of Revocation Advertisements Available	4.9.11 Other Forms of Revocation Advertisements Available
Not applicable.	Not applicable.
4.9.12 Special Requirements Regarding Key Compromise	4.9.12 Special Requirements Regarding Key Compromise
If a compromise of any Private Key pertaining to a certificate issued by the CA is revealed, please notify via the following webform: <u>https://jprs.jp/pubcert/f_mail/</u> Please include either of the following information in your report. • The compromised private key itself • A CSR signed by the compromised private key (A CSR must contain a string indicating that a private key has been compromised in the "CN" field. e.g. CN="This key is compromised") The CA shall verify whether any of the certificates issued by the CA use the presented private key. Upon confirmation of a certificate that uses the presented private key, the CA shall revoke the certificate within 24 hours from the time of confirmation.	"CN" field. e.g. CN="This key is compromised") The CA shall verify whether any of the certificates issued by the CA use the
4.9.13 Circumstances for Suspension	4.9.13 Circumstances for Suspension
Not applicable.	Not applicable.
<b>4.9.14 Who Can Request Suspension</b> Not applicable.	<b>4.9.14 Who Can Request Suspension</b> Not applicable.
4.9.15 Procedures for Suspension Request	4.9.15 Procedures for Suspension Request
Not applicable.	Not applicable.
4.9.16 Limits on Suspension Period	4.9.16 Limits on Suspension Period
Not applicable.	Not applicable.
4.10 Certificate Status Services	4.10 Certificate Status Services
4.10.1 Operational Characteristics	4.10.1 Operational Characteristics
	31/63

	備考
ertificate serial	
certificate [RFC	
nree options:	
in of opping	
y the Issuing	
ct; or	
been issued by	
d in <u>Section</u>	
9	
CA is revealed,	
promised in the	
e the presented	
ate key, the CA	

	整形版 Subscribers and Relying Parties may check information on the status of a certificate
through the OCSP server.	through the OCSP server.
Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.	Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.
4.10.2 Service Availability	4.10.2 Service Availability
information on the status of a certificate twenty-four (24) hours a day, three hundred sixty-five (365) days a year. However, the OCSP server may be temporarily unavailable at times for maintenance or other reasons. The CA SHALL operate and maintain its CRL and OCSP capability with resources	The CA shall manage the OCSP server to allow Subscribers and Relying Parties to check information on the status of a certificate twenty-four (24) hours a day, three hundred sixty-five (365) days a year. However, the OCSP server may be temporarily unavailable at times for maintenance or other reasons. The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.
The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.	The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.
The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority	The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority
Certificate Problem Report, and where appropriate, forward such a complaint to law	Certificate Problem Report, and where appropriate, forward such a complaint to law
nforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.	enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.
4.10.3 Optional Features	4.10.3 Optional Features
lo stipulation.	No stipulation.
4.11 End of Subscription (Registration)	4.11 End of Subscription (Registration)
If a Subscriber ceases to use his/her/its certificate, or cancels the Services, the Subscriber shall request for revocation of his/her/its certificate. If a Subscriber fails to carry procedures for certificate renewal and his/her/its certificate expires, the certificate registration shall terminate.	If a Subscriber ceases to use his/her/its certificate, or cancels the Services, the Subscriber shall request for revocation of his/her/its certificate. If a Subscriber fails to carry procedures for certificate renewal and his/her/its certificate expires, the certificate registration shall terminate.
However, the CA may treat a Subscriber who has been issued a certificate under ACME protocol differently from the above. Other details regarding the cancellation of the Service by the Subscriber are specified in the Terms and Conditions.	However, the CA may treat a Subscriber who has been issued a certificate under ACME protocol differently from the above. Other details regarding the cancellation of the Service by the Subscriber are specified in the Terms and Conditions.
4.12 Key Escrow and Recovery	4.12 Key Escrow and Recovery
4.12.1 Key Escrow and Recovery Policy and Practices	4.12.1 Key Escrow and Recovery Policy and Practices
The CA does not escrow the Private Keys of Subscribers.	The CA does not escrow the Private Keys of Subscribers.
<b>4.12.2 Session Key Encapsulation and Recovery Policy and Practices</b> Not applicable.	<b>4.12.2 Session Key Encapsulation and Recovery Policy and Practices</b> Not applicable.

変更履歴あり	整形版
5. Facility, Management, and Operational Controls	5. Facility, Management, and Operational Controls
5.1 Physical Security Controls Stipulated in the CPS.	<b>5.1 Physical Security Controls</b> Stipulated in the CPS.
5.2 Procedural Controls Stipulated in the CPS.	<b>5.2 Procedural Controls</b> Stipulated in the CPS.
5.3 Personnel Controls tipulated in the CPS.	<b>5.3 Personnel Controls</b> Stipulated in the CPS.
5.4 Audit Logging Procedures	5.4 Audit Logging Procedures
5.4.1 Types of Events Recorded	5.4.1 Types of Events Recorded
Stipulated in the CPS.	Stipulated in the CPS.
5.4.2 Frequency of Processing Audit Log	5.4.2 Frequency of Processing Audit Log
Stipulated in the CPS.	Stipulated in the CPS.
5.4.3 Retention Period for Audit Log	5.4.3 Retention Period for Audit Log
tipulated in the CPS. Audit Logs on the RA system shall be archived for at least seven (7)	Stipulated in the CPS. Audit Logs on the RA system shall be archived for at least seven (7)
ears.	years.
5.4.4 Protection of Audit Log	5.4.4 Protection of Audit Log
tipulated in the CPS.	Stipulated in the CPS.
5.4.5 Audit Logs Backup Procedure	5.4.5 Audit Logs Backup Procedure Stipulated in the CPS.
5.4.6 Audit Log Collection System	5.4.6 Audit Log Collection System Stipulated in the CPS.
5.4.7 Notification to Event-Causing Subject Stipulated in the CPS.	<b>5.4.7 Notification to Event-Causing Subject</b> Stipulated in the CPS.
5.4.8 Vulnerability Assessments	5.4.8 Vulnerability Assessments
Stipulated in the CPS.	Stipulated in the CPS.
5.5 Records Archival	5.5 Records Archival
5.5.1 Types of Records Archived	5.5.1 Types of Records Archived
The CA shall archive the following information in addition to the information prescribed in	
"5.5 Records Archival" of the CPS:	"5.5 Records Archival" of the CPS:
• this CP;	• this CP;
documents prepared under this CP stipulating the business operations of the	• documents prepared under this CP stipulating the business operations of the

変更履歴あり	整形版	備考
Certification Authority;	Certification Authority;	
<ul> <li>records and audit reports on the results of audits; and</li> </ul>	• records and audit reports on the results of audits; and	
<ul> <li>information on applications from Subscribers and the histories thereof.</li> </ul>	• information on applications from Subscribers and the histories thereof.	
5.5.2 Retention Period for Archive	5.5.2 Retention Period for Archive	
Stipulated in the CPS. The CA shall archive the following information for at least seven (7	(7) Stipulated in the CPS. The CA shall archive the following information for at least seven (7)	
/ears:	years:	
• this CP;	• this CP;	
• documents prepared under this CP stipulating the business operations of th		
<ul><li>Certification Authority;</li><li>records and audit reports on the results of audits; and</li></ul>	<ul><li>Certification Authority;</li><li>records and audit reports on the results of audits; and</li></ul>	
<ul> <li>information on applications from Subscribers and the histories thereof.</li> </ul>	<ul> <li>information on applications from Subscribers and the histories thereof.</li> </ul>	
5.5.3 Protection of Archive	5.5.3 Protection of Archive	
Stipulated in the CPS.	Stipulated in the CPS.	
5.5.4 Archive Backup Procedures	5.5.4 Archive Backup Procedures	
Stipulated in the CPS.	Stipulated in the CPS.	
5.5.5 Requirements for Time-Stamping of Records	5.5.5 Requirements for Time-Stamping of Records	
Stipulated in the CPS.	Stipulated in the CPS.	
5.5.6 Archive Collection System	5.5.6 Archive Collection System	
Stipulated in the CPS.	Stipulated in the CPS.	
5.5.7 Procedures to Obtain and Verify Archive Information	5.5.7 Procedures to Obtain and Verify Archive Information	
Stipulated in the CPS.	Stipulated in the CPS.	
5.6 Key Changeover	5.6 Key Changeover	
Before the validity period of a certificate relevant to the CA's own Private Key become		
shorter than the maximum validity period of certificates issued to Subscribers, a new	w shorter than the maximum validity period of certificates issued to Subscribers, a new	
Private Key for the CA shall be generated and a certificate relevant thereto shall be issued	Private Key for the CA shall be generated and a certificate relevant thereto shall be issued.	
Once the new Private Key has been generated, the CA shall issue certificates and CRL		
asing the new Private Key.	using the new Private Key.	
5.7 Compromise and Disaster Recovery	5.7 Compromise and Disaster Recovery	
Stipulated in the CPS.	Stipulated in the CPS.	
5.8 CA or RA Termination	5.8 CA or RA Termination	
f the CA is required to suspend its operations as a Certification Authority or Registratio	If the CA is required to suspend its operations as a Certification Authority or Registration	
Authority, the CA shall notify Subscribers to that effect in advance by any of the means se	t Authority, the CA shall notify Subscribers to that effect in advance by any of the means set	
orth in "9.11 Individual Notices and Communications with Participants."	forth in "9.11 Individual Notices and Communications with Participants."	

変更履歴あり	整形版	備考
6. Technical Security Controls	6. Technical Security Controls	
6.1 Key Pair Generation and Installation	6.1 Key Pair Generation and Installation	
6.1.1 Key Pair Generation	6.1.1 Key Pair Generation	
6.1.1 Generation of Key Pairs" of the CPS stipulates a policy on Private Keys of the CA.	"6.1.1 Generation of Key Pairs" of the CPS stipulates a policy on Private Keys of the CA.	
6.1.2 Private Key Delivery to Subscriber	6.1.2 Private Key Delivery to Subscriber	
Each Subscriber's Private Key shall be generated by the Subscriber himself/herself/itself.	Each Subscriber's Private Key shall be generated by the Subscriber himself/herself/itself.	
The CA does not generate or deliver the Private Keys of Subscribers to Subscribers.	The CA does not generate or deliver the Private Keys of Subscribers to Subscribers.	
6.1.3 Public Key Delivery to the Certificate Issuer	6.1.3 Public Key Delivery to the Certificate Issuer	
A Subscriber shall deliver his/her/its Public Key to the CA online when applying for	A Subscriber shall deliver his/her/its Public Key to the CA online when applying for	
his/her/its certificate. The communication pathways for such delivery shall be encrypted by		
the TLS.	the TLS.	
6.1.4 CA' Public Key Delivery to Relying Parties	6.1.4 CA' Public Key Delivery to Relying Parties	
Relying Parties may obtain Public Keys of the CA by accessing the CA's Repository.	Relying Parties may obtain Public Keys of the CA by accessing the CA's Repository.	
6.1.5 Key Sizes	6.1.5 Key Sizes	
When issuing a TLS server certificate that complies with Baseline Requirements, the	When issuing a TLS server certificate that complies with Baseline Requirements, the	
Collowing confirmation need to be done:	following confirmation need to be done:	
For RSA key pairs the CA SHALL:	For RSA key pairs the CA SHALL:	
• Ensure that the modulus size, when encoded, is at least 2048 bits, and;	• Ensure that the modulus size, when encoded, is at least 2048 bits, and;	
• Ensure that the modulus size, in bits, is evenly divisible by 8.	• Ensure that the modulus size, in bits, is evenly divisible by 8.	
For ECDSA key pairs the CA SHALL:	For ECDSA key pairs the CA SHALL:	
• Ensure that the key represents a valid point on the NIST P-256 or NIST P-384	• Ensure that the key represents a valid point on the NIST P-256 or NIST P-384	
elliptic curve.	elliptic curve.	
No other algorithms or key sizes are permitted.	No other algorithms or key sizes are permitted.	
6.1.6 Public Key Parameters Generation and Quality Checking	6.1.6 Public Key Parameters Generation and Quality Checking	
Stipulated in the CPS. No policy is stipulated on the generation and quality inspection of	Stipulated in the CPS. No policy is stipulated on the generation and quality inspection of	
the Public Key parameters of Subscribers.	the Public Key parameters of Subscribers.	
6.1.7 Key Usage Purposes	6.1.7 Key Usage Purposes	
The following table summarizes the usages of keys intended by the CA and by certificates	The following table summarizes the usages of keys intended by the CA and by certificates	
ssued by the CA:	issued by the CA:	

	Table 6.1 Key U	
	the CA	Certificates issued by th
		CA
digitalSignature	_	yes
nonRepudiation	_	—
keyEncipherment	—	yes
		(except for certificate
		issued by using ECDS.
		key)
dataEncipherment		—
keyAgreement	_	—
keyCertSign	yes	—
cRLSign	yes	—
encipherOnly	—	—
decipherOnly	_	_

## 6.2 Private Key Protection and Cryptographic Module Engineering 6.2 Controls

Stipulated in the CPS.

#### 6.3 Other Aspects of Key Pair Management

#### 6.3.1 Public key archival

Stipulated in the CPS.

#### 6.3.2 Certificate operational periods and key pair usage periods

The Validity period of the key pair and CA certificate of the CA is stipulated in the CPS. Subscriber Certificates issued on or after 1 September 2020 MUST NOT have a validity period greater than 398 days. Subscriber Certificates issued prior to 1 September 2020 have a validity period of 825 days or less.

For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time For greater than this, including fractional seconds and/or leap seconds, shall represent an additional day.

6.4 Activation Data Stipulated in the CPS.

6.5 Computer Security Controls Stipulated in the CPS.

6.6 Life Cycle Technical Controls Stipulated in the CPS.

	整形版	反	備考
	Table 6.1 Key Us		
	the CA	Certificates issued by the	
		CA	
digitalSignature	—	yes	
nonRepudiation	—		
keyEncipherment	—	yes	
		(except for certificates	
		issued by using ECDSA	
		key)	
dataEncipherment	—	—	
keyAgreement	—	—	
keyCertSign	yes		
cRLSign	yes	_	
encipherOnly		—	
decipherOnly	_	—	
	_	igement	
<b>3.1 Public key archiv</b> ulated in the CPS.	al	gomont	
ulated in the CPS.		and key pair usage periods	
ulated in the CPS. <b>3.2 Certificate operat</b> Validity period of the ke scriber Certificates issue	t <b>ional periods a</b> by pair and CA cert d on or after 1 Sep Subscriber Certific		alidity
ulated in the CPS. <b>3.2 Certificate operat</b> Validity period of the ke scriber Certificates issue od greater than 398 days. lidity period of 825 days of the purpose of calculation	tional periods a ey pair and CA cert d on or after 1 Sep Subscriber Certific or less. ns, a day is measur	and key pair usage periods tificate of the CA is stipulated in the ptember 2020 MUST NOT have a va	alidity ) have f time
ulated in the CPS. <b>3.2 Certificate operat</b> Validity period of the ke scriber Certificates issue od greater than 398 days. lidity period of 825 days of the purpose of calculation ter than this, including tional day.	tional periods a ey pair and CA cert d on or after 1 Sep Subscriber Certific or less. ns, a day is measur	and key pair usage periods tificate of the CA is stipulated in the ptember 2020 MUST NOT have a va cates issued prior to 1 September 2020 red as 86,400 seconds. Any amount o	alidity ) have f time
ulated in the CPS. <b>3.2 Certificate operat</b> Validity period of the ke scriber Certificates issue od greater than 398 days. lidity period of 825 days of the purpose of calculation ter than this, including tional day. <b>Activation Data</b>	tional periods a ey pair and CA cert d on or after 1 Sep Subscriber Certific or less. ns, a day is measur	and key pair usage periods tificate of the CA is stipulated in the ptember 2020 MUST NOT have a va cates issued prior to 1 September 2020 red as 86,400 seconds. Any amount o	alidity ) have f time
ulated in the CPS. <b>3.2 Certificate operat</b> Validity period of the ke scriber Certificates issue od greater than 398 days. lidity period of 825 days of the purpose of calculation ter than this, including tional day. <b>Activation Data</b> ulated in the CPS.	tional periods a ey pair and CA cert d on or after 1 Sep Subscriber Certific or less. ns, a day is measur fractional seconds	and key pair usage periods tificate of the CA is stipulated in the ptember 2020 MUST NOT have a va cates issued prior to 1 September 2020 red as 86,400 seconds. Any amount o	alidity ) have f time
ulated in the CPS. <b>3.2 Certificate operat</b> Validity period of the ke scriber Certificates issue od greater than 398 days. lidity period of 825 days of the purpose of calculation ter than this, including	tional periods a ey pair and CA cert d on or after 1 Sep Subscriber Certific or less. ns, a day is measur fractional seconds	and key pair usage periods tificate of the CA is stipulated in the ptember 2020 MUST NOT have a va cates issued prior to 1 September 2020 red as 86,400 seconds. Any amount o	alidity ) have f time
ulated in the CPS. <b>3.2 Certificate operat</b> Validity period of the ke scriber Certificates issue od greater than 398 days. lidity period of 825 days of the purpose of calculation ter than this, including tional day. <b>Activation Data</b> ulated in the CPS. <b>Computer Security</b>	tional periods a ey pair and CA cert d on or after 1 Sep Subscriber Certific or less. ns, a day is measur fractional seconds	and key pair usage periods tificate of the CA is stipulated in the ptember 2020 MUST NOT have a va cates issued prior to 1 September 2020 red as 86,400 seconds. Any amount o	alidity ) have f time

## Co

Stip

## 6.3

#### 6.3

Stip

#### 6.3

6.4 Stip

6.5 Stip

6.6 Stip

## 6.7 Network Security Controls

Stipulated in the CPS.

## 6.8 Time Stamping

Stipulated in the CPS.

# 7. Certificate, CRL, and OCSP Profiles

## 7.1 Certificate Profile

The CA SHALL meet the technical requirements set forth in Section 2.2 - Publication of T Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Ir Generation and Quality Checking of this CP.

The CA SHALL generate non-sequential Certificate serial numbers greater than zero (0) T and less than 2^159 containing at least 64 bits of output from a CSPRNG.

Certificates issued by the CA conform to RFC 5280, the profile of which are indicated in the tables below.

Table 7.1-1 Subscriber Certificate Profile (applicable to certificates issued by JPRS Domain Validation Authority - G4 or JPRS Organization Validation Authority - G4)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Num	ber	An integral serial number to be	-
		assigned by the CA to the certificate	
Signature A	lgorithm	sha256 with RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN=JPRS Domain Validation Authority	
		- G4	
		(2) Organization Validation	
		CN=JPRS Organization Validation	
		Authority – G4	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-

## 6

## 7

6.7 Netwo Stipulated in	ork Security Connumber of the CPS.	ntrols		
<b>5.8 Time</b> Stipulated i	<b>Stamping</b> n the CPS.			
7. Certi	ificate, CRL,	and OCSP Profiles		
	icate Profile			
		cal requirements set forth in Section 2.2 -		
		ey Sizes, and Section 6.1.6 - Public Ke	ey Parame	eters
	and Quality Checking	g of this CP. quential Certificate serial numbers greater	then zor	م س
	-	t least 64 bits of output from a CSPRNG.		5 (0)
	-	form to RFC 5280, the profile of which are in	ndicated in	h the
ables below	-			
Table 7.1-1	Subscriber Certificat	e Profile (applicable to certificates issued by	JPRS Dor	nain
		e Profile (applicable to certificates issued by RS Organization Validation Authority – G4)		nain
	Authority – G4 or JPI			nain
Validation	Authority – G4 or JPI	RS Organization Validation Authority – G4)           Description of setting           Version 3		nain
Validation . Basic field	Authority – G4 or JPI 1	RS Organization Validation Authority – G4) Description of setting		nain
Validation Basic field Version	Authority – G4 or JPI 1	RS Organization Validation Authority – G4)           Description of setting           Version 3		nain
Validation Basic field Version Serial Nu	Authority – G4 or JPI 1	RS Organization Validation Authority – G4)          Description of setting         Version 3         An integral serial number to be assigned by the CA to the certificate         sha256 with RSA Encryption		nain
Validation Basic field Version Serial Nu	Authority – G4 or JPI d mber Algorithm Country	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> </ul>		nain
Validation Basic field Version Serial Nu Signature	Authority – G4 or JPl d mber Algorithm Country Organization	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> <li>O=Japan Registry Services Co., Ltd.</li> </ul>		
Validation Basic field Version Serial Nu Signature	Authority – G4 or JPI d mber Algorithm Country	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> <li>O=Japan Registry Services Co., Ltd.</li> <li>(1) Domain Validation</li> </ul>		
Validation Basic field Version Serial Nu Signature	Authority – G4 or JPl d mber Algorithm Country Organization	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> <li>O=Japan Registry Services Co., Ltd.</li> <li>(1) Domain Validation</li> <li>CN=JPRS Domain Validation Authority</li> </ul>		nain
Validation Basic field Version Serial Nu Signature	Authority – G4 or JPl d mber Algorithm Country Organization	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> <li>O=Japan Registry Services Co., Ltd.</li> <li>(1) Domain Validation</li> <li>CN=JPRS Domain Validation Authority</li> <li>- G4</li> </ul>		
Validation Basic field Version Serial Nu Signature	Authority – G4 or JPl d mber Algorithm Country Organization	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> <li>O=Japan Registry Services Co., Ltd.</li> <li>(1) Domain Validation</li> <li>CN=JPRS Domain Validation Authority</li> <li>- G4</li> <li>(2) Organization Validation</li> </ul>		
Validation Basic field Version Serial Nu Signature	Authority – G4 or JPl d mber Algorithm Country Organization	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> <li>O=Japan Registry Services Co., Ltd.</li> <li>(1) Domain Validation</li> <li>CN=JPRS Domain Validation Authority</li> <li>- G4</li> <li>(2) Organization Validation</li> <li>CN=JPRS Organization Validation</li> </ul>		
Validation Basic field Version Serial Nu Signature Issuer	Authority – G4 or JPI	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> <li>O=Japan Registry Services Co., Ltd.</li> <li>(1) Domain Validation</li> <li>CN=JPRS Domain Validation Authority</li> <li>- G4</li> <li>(2) Organization Validation</li> <li>CN=JPRS Organization Validation</li> <li>Authority – G4</li> </ul>		
Validation Basic field Version Serial Nu Signature	Authority – G4 or JPl d mber Algorithm Country Organization	<ul> <li>RS Organization Validation Authority – G4)</li> <li>Description of setting</li> <li>Version 3</li> <li>An integral serial number to be assigned by the CA to the certificate</li> <li>sha256 with RSA Encryption</li> <li>C=JP</li> <li>O=Japan Registry Services Co., Ltd.</li> <li>(1) Domain Validation</li> <li>CN=JPRS Domain Validation Authority</li> <li>- G4</li> <li>(2) Organization Validation</li> <li>CN=JPRS Organization Validation</li> </ul>		

		変更履歴あり				整形版		備考
ubject	Country	(1) Domain Validation	-	Subject	Country	(1) Domain Validation	-	
		No description				No description		
		(2) Organization Validation				(2) Organization Validation		
		C=JP as the address of the Subscriber				C=JP as the address of the Subscriber		
		(country)				(country)		
	State or Province	(1) Domain Validation	-		State or Province	(1) Domain Validation	-	
		No description				No description		
		(2) Organization Validation				(2) Organization Validation		
		Address of the Subscriber (prefecture				Address of the Subscriber (prefecture		
		name) (mandatory)				name) (mandatory)		
	Locality	(1) Domain Validation	-		Locality	(1) Domain Validation	-	
		No description				No description		
		(2) Organization Validation				(2) Organization Validation		
		Address of the Subscriber (city, town, or				Address of the Subscriber (city, town, or		
		village name) (mandatory)				village name) (mandatory)		
	Organization	(1) Domain Validation	-		Organization	(1) Domain Validation	-	
		No description				No description		
		(2) Organization Validation				(2) Organization Validation		
		Name of the Subscriber (mandatory)				Name of the Subscriber (mandatory)		
	Organizational	(1) Domain Validation	-		Organizational	(1) Domain Validation	-	
	Unit	No description			Unit	No description		
		(2) Organization Validation				(2) Organization Validation		
		Business division name of the				Business division name of the		
		Subscriber (optional ).				Subscriber (optional ).		
		However, this item will not be included				However, this item will not be included		
		in certificates issued on or after 18				in certificates issued on or after 18		
		November 2021.				November 2021.		
		• A string comprising symbols only or				• A string comprising symbols only or		
		spaces only may not be designated,				spaces only may not be designated,		
		and any of the following strings				and any of the following strings		
		may not be included:				may not be included:		
		<ul> <li>any name, company name, trade name, or trademark that</li> </ul>				<ul> <li>any name, company name, trade name, or trademark that</li> </ul>		
		is likely to cause others to				is likely to cause others to		
		misconstrue that the relevant				misconstrue that the relevant		
		information is the information of any organization other than				information is the information of any organization other than		
		the applicant organization;				the applicant organization;		
		<ul> <li>any string indicating a legal personality, such as "Co., Ltd";</li> </ul>				<ul> <li>any string indicating a legal personality, such as "Co., Ltd";</li> </ul>		
		<ul> <li>any string referring to a</li> </ul>				any string referring to a		
		<ul><li>specific natural person;</li><li>any string indicating an</li></ul>				<ul><li>specific natural person;</li><li>any string indicating an</li></ul>		

	変更履歴あり				整形版	
Commo	address; • any phone number; • any domain name or IP address; or • any string meaning "blank", "not applicable" or the like ("null", "N/A" or the like)	-		Common Name	address; any phone number; any domain name or IP address; or any string meaning "blank", "not applicable" or the like ("null", "N/A" or the like) A host name used in the DNS of the server in which the certificate is scheduled to be installed (mandatory) - The value must be encoded as a	-
	character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically.				character-for-character copy of the dNSName entry value from the Subject Alternative Name extension. Specifically.	
Subject Public Key I	· · ·	-		Subject Public Key Info	The subject's Public Key (RSA 2048 bits)	-
Extended field	Description of setting	critical		Extended field	Description of setting	critical
KeyUsage	digitalSignature, keyEncipherment	У	-	KeyUsage	digitalSignature, keyEncipherment	У
ExtendedKeyUsage	TLS Web Server Authentication	n	-	ExtendedKeyUsage	TLS Web Server Authentication	n
Subject Alt Name	dNSName= name(s) of the server(s)	n	_	Subject Alt Name	dNSName= name(s) of the server(s)	n
CertificatePolicies	<ul> <li>[1] Certificate Policy</li> <li>1.3.6.1.4.1.53827.1.1.4</li> <li>CPS</li> <li>http://jprs.jp/pubcert/info/repository/</li> <li>[2] Certificate Policy</li> <li>(1) Domain Validation</li> <li>2.23.140.1.2.1</li> <li>(2) Organization Validation</li> </ul>	n		CertificatePolicies	<ul> <li>[1] Certificate Policy</li> <li>1.3.6.1.4.1.53827.1.1.4</li> <li>CPS</li> <li>http://jprs.jp/pubcert/info/repository/</li> <li>[2] Certificate Policy</li> <li>(1) Domain Validation</li> <li>2.23.140.1.2.1</li> <li>(2) Organization Validation</li> </ul>	n
	2.23.140.1.2.2				2.23.140.1.2.2	
CRL Distribution Po		n		CRL Distribution Points	<ul> <li>(1) Domain Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/dv</li> <li>ca_g4/fullcrl.crl</li> <li>(2) Organization Validation</li> <li>http://repo.pubcert.jprs.jp/sppca/jprs/ovc</li> <li>a_g4/fullcrl.crl</li> </ul>	n
Authority Informatio	n Access [1] ocsp (1.3.6.1.5.5.7.48.1) (1) Domain Validation http://dv.g4.ocsp.pubcert.jprs.jp (2) Organization Validation http://ov.g4.ocsp.pubcert.jprs.jp	n		Authority Information Access	<ul> <li>[1] ocsp (1.3.6.1.5.5.7.48.1)</li> <li>(1) Domain Validation</li> <li>http://dv.g4.ocsp.pubcert.jprs.jp</li> <li>(2) Organization Validation</li> <li>http://ov.g4.ocsp.pubcert.jprs.jp</li> </ul>	n

	変更履歴あり	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	(1) Domain Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/dv	
	ca_g4/JPRS_DVCA_G4_DER.cer	
	(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc	
	a_g4/JPRS_OVCA_G4_DER.cer	
Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n
	(160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's Public Key	n
	(160 bits)	
Certificate Transparency	Value of an OCTET STRING containing	n
Timestamp List	the encoded	
(1.3.6.1.4.1.11129.2.4.2)	${f SignedCertificateTimestampList}$	

Table 7.1-2 Subscriber Certificate Profile (applicable to certificates issued by JPRS DV RSA CA 2024 G1 or JPRS OV RSA CA 2024 G1)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Number		An integral serial number to be	-
<u> </u>		assigned by the CA to the certificate	
0	Algorithm	sha256 with RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN= JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
		CN= JPRS OV RSA CA 2024 G1	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	(1) Domain Validation	-
		No description	
		(2) Organization Validation	
		C=JP as the address of the Subscriber	
		(country)	
	State or Province	(1) Domain Validation	-
		No description	
		(2) Organization Validation	
		Address of the Subscriber (prefecture	

		整形版		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		(1) Domain Validation		
		http://repo.pubcert.jprs.jp/sppca/jprs/dv		
		ca_g4/JPRS_DVCA_G4_DER.cer		
		(2) Organization Validation		
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc		
		a_g4/JPRS_OVCA_G4_DER.cer		
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n	
		(160 bits)		
Certificate	Transparency	Value of an OCTET STRING containing	n	
Timestam	p List	the encoded		
(1.3.6.1.4)	.1.11129.2.4.2)	SignedCertificateTimestampList		
		/		
able 7.1-2	Subscriber Certificat	te Profile (applicable to certificates issued	by JPRS	S DV
RSA CA 202	24 G1 or JPRS OV RS	A CA 2024 G1)		_
RSA CA 202 <mark>Basic field</mark>		A CA 2024 G1) Description of setting	critical	
Basic field			critical -	
		Description of setting	critical -	-
<mark>Basic field</mark> Version		Description of setting       Version 3	critical - -	_
<mark>Basic field</mark> Version	nber	Description of settingVersion 3An integral serial number to be	critical - -	-
Basic field Version Serial Nun Signature	nber	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificate	-	-
Basic field Version Serial Nun Signature	nber Algorithm	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA Encryption	-	
Basic field Version Serial Nun Signature	nber Algorithm Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JP	-	-
Basic field Version Serial Nun	nber Algorithm Country Organization	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.	-	-
Basic field Version Serial Nun Signature	nber Algorithm Country Organization	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation	-	
Basic field Version Serial Nun Signature	nber Algorithm Country Organization	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV RSA CA 2024 G1	-	
Basic field Version Serial Nun Signature Issuer	nber Algorithm Country Organization	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV RSA CA 2024 G1(2) Organization Validation	-	
Basic field Version Serial Nun Signature Issuer	nber Algorithm Country Organization Common Name	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV RSA CA 2024 G1(2) Organization ValidationCN= JPRS OV RSA CA 2024 G1	-	
Basic field Version Serial Num Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV RSA CA 2024 G1(2) Organization ValidationCN= JPRS OV RSA CA 2024 G1E.g.) 2008/3/1 00:00:00 GMT	-	
Basic field Version Serial Num Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV RSA CA 2024 G1 (2) Organization Validation CN= JPRS OV RSA CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT	-	
Basic field Version Serial Nun Signature	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV RSA CA 2024 G1 (2) Organization Validation CN= JPRS OV RSA CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain Validation	-	
Basic field Version Serial Num Signature . Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV RSA CA 2024 G1(2) Organization ValidationCN= JPRS OV RSA CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description	-	
Basic field Version Serial Num Signature A Issuer	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV RSA CA 2024 G1(2) Organization ValidationCN= JPRS OV RSA CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization Validation	-	
Basic field Version Serial Num Signature . Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV RSA CA 2024 G1(2) Organization ValidationCN= JPRS OV RSA CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationCaliforniaCaliforniaCaliforniaCN=JPRS OV RSA CA 2024 G1E.g.) 2009/3/1 00:00:00 GMTCALCALCALCONSCAL </td <td>-</td> <td></td>	-	
Basic field Version Serial Num Signature . Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV RSA CA 2024 G1(2) Organization ValidationCN= JPRS OV RSA CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber (country)	-	
Basic field Version Serial Num Signature . Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingVersion 3An integral serial number to be assigned by the CA to the certificatesha256 with RSA EncryptionC=JPO=Japan Registry Services Co., Ltd.(1) Domain ValidationCN= JPRS DV RSA CA 2024 G1(2) Organization ValidationCN= JPRS OV RSA CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT(1) Domain ValidationNo description(2) Organization ValidationC=JP as the address of the Subscriber (country)(1) Domain Validation	-	

		整形版		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		(1) Domain Validation		
		http://repo.pubcert.jprs.jp/sppca/jprs/dv		
		ca_g4/JPRS_DVCA_G4_DER.cer		
		(2) Organization Validation		
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc		
		a_g4/JPRS_OVCA_G4_DER.cer		
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n	
,e	<i></i>	(160 bits)		
Certificate	Transparency	Value of an OCTET STRING containing	n	
Timestam	1 0	the encoded		
-	(1.11129.2.4.2)	SignedCertificateTimestampList		
able 7.1-2	Subscriber Certifica	te Profile (applicable to certificates issued	by JPRS	DV
	4 G1 or JPRS OV RS		U	
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Nun	nber	An integral serial number to be	-	
		assigned by the CA to the certificate		
Signature	Algorithm	sha256 with RSA Encryption	-	
Issuer	Country	C=JP	-	
	Organization	O=Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN= JPRS DV RSA CA 2024 G1		
		(2) Organization Validation		
		CN= JPRS OV RSA CA 2024 G1		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
U	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	
Subject	Country	(1) Domain Validation	-	
j.		No description		
		(2) Organization Validation		
		C=JP as the address of the Subscriber		
		(country)		
	State or Province	(1) Domain Validation	-	
		No description		
		(2) Organization Validation		
		Address of the Subscriber (prefecture		
		inarios of the Subscriber (prefecture		

	変更履歴あり			整形版		備考
	name) (mandatory)			name) (mandatory)		
Locality	(1) Domain Validation	-	Locality	(1) Domain Validation	-	
	No description			No description		
	(2) Organization Validation			(2) Organization Validation		
	Address of the Subscriber (city, town, or			Address of the Subscriber (city, town, or		
	village name) (mandatory)			village name) (mandatory)		
Organization	(1) Domain Validation	-	Organization	(1) Domain Validation	-	
	No description			No description		
	(2) Organization Validation			(2) Organization Validation		
	Name of the Subscriber (mandatory)			Name of the Subscriber (mandatory)		
Common Name		-	Common Name	A host name used in the DNS of the	-	
	server in which the certificate is			server in which the certificate is		
	scheduled to be installed (mandatory)			scheduled to be installed (mandatory)		
	- The value must be encoded as a			- The value must be encoded as a		
	character-for-character copy of the			character-for-character copy of the		
	dNSName entry value from the			dNSName entry value from the		
	Subject Alternative Name extension.			Subject Alternative Name extension.		
	Specifically.			Subject Internative Plane extension.		
Subject Public Key Info	The subject's Public Key (RSA 4096 bits,		Subject Public Key Info	The subject's Public Key (RSA 4096 bits,		
Subject I ublic Key Illio	RSA3072 bits or RSA 2048 bits)		Subject I ublic Key Illio	RSA3072 bits or RSA 2048 bits)		
Extended field	Description of setting	critical	Extended field	Description of setting	critical	
KeyUsage	· · ·		KeyUsage			
ReyUsage	digitalSignature,	У	KeyUsage	digitalSignature,	У	
	keyEncipherment			keyEncipherment		
ExtendedKeyUsage	TLS Web Server Authentication.	n	ExtendedKeyUsage	TLS Web Server Authentication,	n	
	TLS Web Client Authentication			TLS Web Client Authentication		プロファイルの修正
	<u>(optional)</u>			(optional)		
Subject Alt Name	dNSName= name(s) of the server(s)	n	Subject Alt Name	dNSName= name(s) of the server(s)	n	
CertificatePolicies	Certificate Policy	n	CertificatePolicies	Certificate Policy	n	
	(1) Domain Validation			(1) Domain Validation		
	2.23.140.1.2.1			2.23.140.1.2.1		
	(2) Organization Validation			(2) Organization Validation		
	2.23.140.1.2.2			2.23.140.1.2.2		
CRL Distribution Points	(1) Domain Validation	n	CRL Distribution Points	(1) Domain Validation	n	
	http://repo.pubcert.jprs.jp/sppca/jprs/dv			http://repo.pubcert.jprs.jp/sppca/jprs/dv		
	ca_rsa2024g1/fullcrl.crl			ca_rsa2024g1/fullcrl.crl		
	(2) Organization Validation			(2) Organization Validation		
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc			http://repo.pubcert.jprs.jp/sppca/jprs/ovc		
	a_rsa2024g1/fullcrl.crl			a_rsa2024g1/fullcrl.crl		
		1	Authority Information Access			

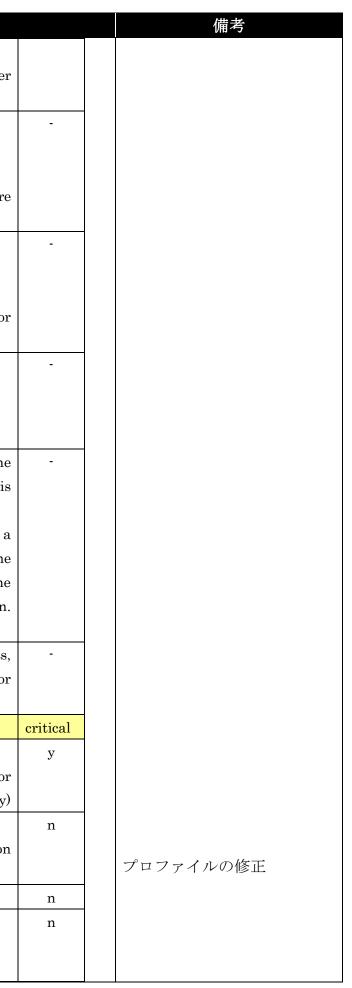
	変更履歴あり			整形版
	(1) Domain Validation			(1) Domain Validation
	http://dv.rsa2024g1.ocsp.pubcert.jprs.jp			http://dv.rsa2024g1.ocsp.pubce
	(2) Organization Validation			(2) Organization Validation
	http://ov.rsa2024g1.ocsp.pubcert.jprs.jp			http://ov.rsa2024g1.ocsp.pubcer
	[2] ca issuers (1.3.6.1.5.5.7.48.2)			[2] ca issuers (1.3.6.1.5.5.7.48.2
	(1) Domain Validation			(1) Domain Validation
	http://repo.pubcert.jprs.jp/sppca/jprs/dv			http://repo.pubcert.jprs.jp/sppc
	ca_rsa2024g1/JPRS_DVCA_RSA2024G			ca_rsa2024g1/JPRS_DVCA_RS
	1_DER.cer			1_DER.cer
	(2) Organization Validation			(2) Organization Validation
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc			http://repo.pubcert.jprs.jp/sppc
	a_rsa2024g1/JPRS_OVCA_RSA2024G1			a_rsa2024g1/JPRS_OVCA_RSA
	_DER.cer			_DER.cer
Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n	Authority Key Identifier	SHA-1 hash for the issuer's P
	(160 bits)			(160 bits)
Subject Key Identifier	SHA-1 hash for the subject's Public Key	n	Subject Key Identifier	SHA-1 hash for the subject's P
	(160 bits)			(160 bits)
Certificate Transparency	Value of an OCTET STRING containing	n	Certificate Transparency	Value of an OCTET STRING c
Timestamp List	the encoded		Timestamp List	the
(1.3.6.1.4.1.11129.2.4.2)	${\bf SignedCertificateTimestampList} (option$		(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampLi
	al).			al).

Table 7.1-3 Subscriber Certificate Profile (applicable to certificates issued by JPRS DV	
ECC CA 2024 G1 or JPRS OV ECC CA 2024 G1)	

Basic field		Description of setting	critical
Version		Version 3	-
Serial Nu	mber	An integral serial number to be	-
		assigned by the CA to the certificate	
Signature	Algorithm	ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN= JPRS DV ECC CA 2024 G1	
		(2) Organization Validation	
		CN= JPRS OV ECC CA 2024 G1	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
NotAfter		E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	(1) Domain Validation	-
		No description	

		整形版		
		(1) Domain Validation		
		http://dv.rsa2024g1.ocsp.pubcert.jprs.jp		
		(2) Organization Validation		
		http://ov.rsa2024g1.ocsp.pubcert.jprs.jp		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		(1) Domain Validation		
		http://repo.pubcert.jprs.jp/sppca/jprs/dv		
		ca_rsa2024g1/JPRS_DVCA_RSA2024G		
		1_DER.cer		
		(2) Organization Validation		
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc		
		a_rsa2024g1/JPRS_OVCA_RSA2024G1		
		_DER.cer		
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
-		(160 bits)		
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n	1
		(160 bits)		
Certificate	Transparency	Value of an OCTET STRING containing	n	
Timestamp	o List	the encoded		
(1.3.6.1.4.1.11129.2.4.2)		SignedCertificateTimestampList(option		
		al).		
			1	1
$F_{ablo}$ 7 1-9	Cash a suit an Castifica	te Profile (applicable to certificates issued	by JPRS	DV
rable 1.1-3	Subscriber Certifica	te i follie (applicable to certificates issued		
	24 G1 or JPRS OV E			
			critical	
ECC CA 202		CC CA 2024 G1)	critical -	
ECC CA 202 <mark>Basic field</mark>	24 G1 or JPRS OV E4	CC CA 2024 G1) Description of setting	critical	
ECC CA 202 Basic field Version	24 G1 or JPRS OV E4	CC CA 2024 G1) Description of setting Version 3	critical - -	
ECC CA 202 Basic field Version	24 G1 or JPRS OV E4	CC CA 2024 G1) Description of setting Version 3 An integral serial number to be	critical - -	
ECC CA 202 Basic field Version Serial Nun	24 G1 or JPRS OV E4	CC CA 2024 G1) Description of setting Version 3 An integral serial number to be assigned by the CA to the certificate	critical - - -	
ECC CA 202 Basic field Version Serial Nun Signature A	24 G1 or JPRS OV E4 nber Algorithm	CC CA 2024 G1) Description of setting Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384	critical - - - - -	
ECC CA 202 Basic field Version Serial Nun Signature A	24 G1 or JPRS OV Events of the second	CC CA 2024 G1) Description of setting Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP	critical	
ECC CA 202 Basic field Version Serial Nun Signature A	24 G1 or JPRS OV Events of the second	CC CA 2024 G1)  Description of setting  Version 3  An integral serial number to be assigned by the CA to the certificate  ecdsa-with-SHA384  C=JP  O=Japan Registry Services Co., Ltd.	critical - - - - - - - - -	
ECC CA 202 Basic field Version Serial Nun Signature A	24 G1 or JPRS OV Events of the second	CC CA 2024 G1)  Description of setting  Version 3  An integral serial number to be assigned by the CA to the certificate  ecdsa-with-SHA384  C=JP  O=Japan Registry Services Co., Ltd.  (1) Domain Validation	critical - - - - - - - - -	
ECC CA 202 Basic field Version Serial Nun Signature A	24 G1 or JPRS OV Events of the second	CC CA 2024 G1) Description of setting Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1	critical - - - - - -	
ECC CA 202 Basic field Version Serial Nun Signature A	24 G1 or JPRS OV Events of the second	CC CA 2024 G1)Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation	critical	
ECC CA 202 Basic field Version Serial Nun Signature A Issuer	24 G1 or JPRS OV Events of the second	CC CA 2024 G1) Description of setting Version 3 An integral serial number to be assigned by the CA to the certificate ecdsa-with-SHA384 C=JP O=Japan Registry Services Co., Ltd. (1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1	critical	
ECC CA 202 Basic field Version Serial Nun Signature A Issuer	24 G1 or JPRS OV Events of the second	CC CA 2024 G1)Description of settingVersion 3An integral serial number to be assigned by the CA to the certificateecdsa-with-SHA384C=JPO=Japan Registry Services Co., Ltd.(1) Domain Validation CN= JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT	critical         -	

		変更履歴あり					整形版
		(2) Organization Validation					(2) Organization Validation
		C=JP as the address of the Subscriber					C=JP as the address of the Subscribe
		(country)					(country)
S	State or Province	(1) Domain Validation	-			State or Province	(1) Domain Validation
		No description					No description
		(2) Organization Validation					(2) Organization Validation
		Address of the Subscriber (prefecture					Address of the Subscriber (prefectur
		name) (mandatory)					name) (mandatory)
]	Locality	(1) Domain Validation	-			Locality	(1) Domain Validation
		No description					No description
		(2) Organization Validation					(2) Organization Validation
		Address of the Subscriber (city, town, or					Address of the Subscriber (city, town, o
		village name) (mandatory)					village name) (mandatory)
(	Organization	(1) Domain Validation	-			Organization	(1) Domain Validation
		No description					No description
		(2) Organization Validation					(2) Organization Validation
		Name of the Subscriber (mandatory)					Name of the Subscriber (mandatory)
(	Common Name	A host name used in the DNS of the	-			Common Name	A host name used in the DNS of th
		server in which the certificate is					server in which the certificate i
		scheduled to be installed (mandatory)					scheduled to be installed (mandatory)
		- The value must be encoded as a					- The value must be encoded as
		character-for-character copy of the					character-for-character copy of th
		dNSName entry value from the					dNSName entry value from the
		Subject Alternative Name extension.					Subject Alternative Name extension
		Specifically.					Specifically.
Subject Publi	c Key Info	The subject's Public Key (RSA 4096 bits,	-		Subject Pu	ublic Key Info	The subject's Public Key (RSA 4096 bits
		RSA 3072 bits, RSA 2048 bits, P-256 or					RSA 3072 bits, RSA 2048 bits, P-256 o
		P-384)					P-384)
Extended fiel	d	Description of setting	critical		Extended	field	Description of setting
KeyUsage		digitalSignature,	У		KeyUsage		digitalSignature,
		keyEncipherment (except for					keyEncipherment (except fo
		certificates issued by using ECDSA key)					certificates issued by using ECDSA key
ExtendedKey	Usage	TLS Web Server Authentication,	n		Extended	KeyUsage	TLS Web Server Authentication,
		TLS Web Client Authentication					TLS Web Client Authentication
		<u>(optional)</u>					(optional)
Subject Alt N	ame	dNSName= name(s) of the server(s)	n	]	Subject Al	t Name	dNSName= name(s) of the server(s)
CertificatePol	licies	Certificate Policy	n		Certificate	Policies	Certificate Policy
		(1) Domain Validation					(1) Domain Validation
		2.23.140.1.2.1					2.23.140.1.2.1



	変更履歴あり			整形版	
	(2) Organization Validation			(2) Organization Validation	
	2.23.140.1.2.2			2.23.140.1.2.2	
CRL Distribution Points	(1) Domain Validation	n	CRL Distribution Points	(1) Domain Validation	n
	http://repo.pubcert.jprs.jp/sppca/jprs/dv			http://repo.pubcert.jprs.jp/sppca/jprs/dv	
	ca_ecc2024g1/fullcrl.crl			ca_ecc2024g1/fullcrl.crl	
	(2) Organization Validation			(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc			http://repo.pubcert.jprs.jp/sppca/jprs/ovc	
	a_ecc2024g1/fullcrl.crl			a_ecc2024g1/fullcrl.crl	
Authority Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n	Authority Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n
	(1) Domain Validation			(1) Domain Validation	
	http://dv.ecc2024g1.ocsp.pubcert.jprs.jp			http://dv.ecc2024g1.ocsp.pubcert.jprs.jp	
	(2) Organization Validation			(2) Organization Validation	
	http://ov.ecc2024g1.ocsp.pubcert.jprs.jp			http://ov.ecc2024g1.ocsp.pubcert.jprs.jp	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)			[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	(1) Domain Validation			(1) Domain Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/dv			http://repo.pubcert.jprs.jp/sppca/jprs/dv	
	ca_ecc2024g1/JPRSDVCA_ECC2024G1			ca_ecc2024g1/JPRSDVCA_ECC2024G1	
	_DER.cer			_DER.cer	
	(2) Organization Validation			(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc			http://repo.pubcert.jprs.jp/sppca/jprs/ovc	
	a_ecc2024g1/JPRS_OVCA_ECC2024G1			a_ecc2024g1/JPRS_OVCA_ECC2024G1	
	_DER.cer			_DER.cer	
Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n	Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n
	(160 bits)			(160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's Public Key	n	Subject Key Identifier	SHA-1 hash for the subject's Public Key	n
	(160 bits)			(160 bits)	
Certificate Transparency	Value of an OCTET STRING containing	n	Certificate Transparency	Value of an OCTET STRING containing	n
Timestamp List	the encoded		Timestamp List	the encoded	
(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampLi		(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampLi	
	st (optional)			st (optional)	

Basic fie	Basic field Description of setting		critical
Version	Version Version 3		-
Serial N	Serial Number     An integral serial number to basigned by the CA to the certificate		-
Signatu	re Algorithm	sha256 With RSA Encryption	-
Issuer	Country	C=JP	-

	整形版	
	(2) Organization Validation	
	2.23.140.1.2.2	
CRL Distribution Points	(1) Domain Validation	n
	http://repo.pubcert.jprs.jp/sppca/jprs/dv	
	ca_ecc2024g1/fullcrl.crl	
	(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc	
	a_ecc2024g1/fullcrl.crl	
Authority Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n
	(1) Domain Validation	
	http://dv.ecc2024g1.ocsp.pubcert.jprs.jp	
	(2) Organization Validation	
	http://ov.ecc2024g1.ocsp.pubcert.jprs.jp	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	(1) Domain Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/dv	
	ca_ecc2024g1/JPRSDVCA_ECC2024G1	
	_DER.cer	
	(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc	
	a_ecc2024g1/JPRS_OVCA_ECC2024G1	
	_DER.cer	
Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n
	(160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's Public Key	n
	(160 bits)	
Certificate Transparency	Value of an OCTET STRING containing	n
Timestamp List	the encoded	
(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampLi	
. ,	st (optional)	
Table 7.1-4 Subordinate CA Cert	ificate Profile (applicable to certificates issu	ed by Secu
Communication RootCA2)		U
Basic field	Description of setting	critical
Version	Version 3	-
Serial Number	An integral serial number to be	-
	assigned by the CA to the certificate	
Signature Algorithm	sha256 With RSA Encryption	-
Issuer Country	C=JP	
issuer Country		

		変更履歴あり			
	Organization	O=SECOM Trust Systems CO.,LTD.	-		
	Common Name	OU=Security Communication RootCA2	-		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-		
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-		
Subject	Country	C=JP	-		
	Organization	O=Japan Registry Services Co., Ltd.	-		
	Common Name	(1) Organization Validation	-		
		<b>CN=JPRS</b> Organization Validation			
		Authority - G4			
		(2) Domain Validation			
		CN=JPRS Domain Validation Authority			
		- G4			
Subject Pu	ıblic Key Info	The subject's Public Key (RSA 2048 bits)	-		
Extended	field	Description of setting	critica		
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n		
		(160 bits)			
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key			
		(160 bits)			
KeyUsage		Certificate Signing	У		
		Off-line CRL Signing			
		CRL Signing (06)			
Certificate	Policies	Certificate Policy	n		
		1.2.392.200091.100.901.4			
		CPS			
		http://repository.secomtrust.net			
		/SC-Root2/			
Basic Cons	straints	Subject Type=CA	У		
		Path Length Constraint=0			
Extended	KeyUsage	TLS Web Server Authentication	n		
CRL Distr	ibution Points	http://repository.secomtrust.net/SC-Roo	n		
		t2/SCRoot2CRL.crl			
Authority	Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n		
		http://scrootca2.ocsp.secomtrust.net			
		[2] ca issuers (1.3.6.1.5.5.7.48.2)			
		http://repository.secomtrust.net/SC-Roo			
		t2/SCRoot2ca.cer			

		整形版	
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	OU=Security Communication RootCA2	-
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Organization Validation	-
		<b>CN=JPRS</b> Organization Validation	
		Authority - G4	
		(2) Domain Validation	
		CN=JPRS Domain Validation Authority	
		- G4	
Subject Pu	blic Key Info	The subject's Public Key (RSA 2048 bits)	-
Extended f	ïeld	Description of setting	critical
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n
		(160 bits)	
KeyUsage		Certificate Signing	У
		Off-line CRL Signing	
		CRL Signing (06)	
Certificate	Policies	Certificate Policy	n
		1.2.392.200091.100.901.4	
		CPS	
		http://repository.secomtrust.net	
		/SC-Root2/	
Basic Cons	straints	Subject Type=CA	У
		Path Length Constraint=0	
ExtendedK	KeyUsage	TLS Web Server Authentication	n
CRL Distri	bution Points	http://repository.secomtrust.net/SC-Roo	n
		t2/SCRoot2CRL.crl	
Authority	Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n
		http://scrootca2.ocsp.secomtrust.net	
		[2] ca issuers (1.3.6.1.5.5.7.48.2)	
		http://repository.secomtrust.net/SC-Roo	
		t2/SCRoot2ca.cer	

Table 7.1-5 Subordinate CA Certificate Profile (applicable to certificates issued by SECOM TLS RSA Root CA 2024)

		変更履歴あり	
Basic field		Description of setting	critica
Version		Version 3	-
Serial Nu	nber	An integral serial number to be	-
		assigned by the CA to the certificate	
Signature	Algorithm	Sha384 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems Co., Ltd.	-
	Common Name	CN= SECOM TLS RSA Root CA 2024	-
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Organization Validation	-
		CN= JPRS OV RSA CA 2024 G1	
		(2) Domain Validation	
		CN= JPRS DV RSA CA 2024 G1	
Subject Public Key Info		The subject's Public Key (RSA 4096 bits)	-
Extended field		Description of setting	critica
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key	
		(160 bits)	
KeyUsage		Certificate Signing	У
		Off-line CRL Signing	
		CRL Signing (06)	
Certificate	Policies	[1] Certificate Policy	n
		(1) Domain Validation	
		2.23.140.1.2.1	
		(2) Organization Validation	
		2.23.140.1.2.2	
		[2] Certificate Policy	
		1.2.392.200091.100.901.11	
Basic Con	straints	Subject Type=CA	У
		Path Length Constraint=0	
Extended	KeyUsage	TLS Web Server Authentication	n
		TLS Web Client Authentication	
CRL Distr	ibution Points	http://repo1.secomtrust.net/root/tlsrsa/tl	n
		srsarootca2024.crl	
Authority	Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n

		整形版	
Basic field		Description of setting	critical
Version		Version 3	-
Serial Nun	nber	An integral serial number to be	-
		assigned by the CA to the certificate	
Signature	Algorithm	Sha384 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems Co., Ltd.	-
	Common Name	CN= SECOM TLS RSA Root CA 2024	-
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Organization Validation	-
		CN= JPRS OV RSA CA 2024 G1	
		(2) Domain Validation	
		CN= JPRS DV RSA CA 2024 G1	
Subject Pu	blic Key Info	The subject's Public Key (RSA 4096 bits)	-
		Description of setting	critical
Extended field Authority Key Identifier		SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject Key Identifier		SHA-1 hash for the subject's Public Key	n
		(160 bits)	
KeyUsage		Certificate Signing	У
		Off-line CRL Signing	
		CRL Signing (06)	
Certificate	Policies	[1] Certificate Policy	n
		(1) Domain Validation	
		2.23.140.1.2.1	
		(2) Organization Validation	
		2.23.140.1.2.2	
		[2] Certificate Policy	
		1.2.392.200091.100.901.11	
Basic Cons	traints	Subject Type=CA	У
		Path Length Constraint=0	
ExtendedK	KeyUsage	TLS Web Server Authentication	n
		TLS Web Client Authentication	
CRL Distri	bution Points	http://repo1.secomtrust.net/root/tlsrsa/tl	n
		srsarootca2024.crl	
Authority 3	Information Access	[1]  ocsp (1.3.6.1.5.5.7.48.1)	n

変更履歴あり	整形版
http://tlsrsarootca2024.ocsp.secom-cert.j	http://tlsrsarootca2024.ocsp.secom-cert.
р	p
[2] ca issuers (1.3.6.1.5.5.7.48.2)	[2] ca issuers (1.3.6.1.5.5.7.48.2)
http://repo2.secomtrust.net/root/tlsrsa/tl	http://repo2.secomtrust.net/root/tlsrsa/t
srsarootca2024.cer	srsarootca2024.cer

Table 7.1-6 Subordinate CA Certificate Profile (applicable to certificates issued by Security	
Communication ECC RootCA1)	

Basic field	l	Description of setting	critical
Version		Version 3	-
Serial Nu	nber	An integral serial number to be assigned by the CA to the certificate	-
Signature	Algorithm	ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Security Communication ECC RootCA1	-
Validity NotBefore E.g.) 2008/3/1 00:00:0		E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	-	
	Common Name	(1) Organization Validation	-
		CN= JPRS OV ECC CA 2024 G1	
		(2) Domain Validation	
		CN= JPRS DV ECC CA 2024 G1	
Subject Pu	ıblic Key Info	The subject's Public Key (384 bits)	-
Extended	field	Description of setting	critical
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n
KeyUsage		Certificate Signing	У
		Off-line CRL Signing	
		CRL Signing (06)	
Certificate	Policies	[1] Certificate Policy	n
		(1) Domain Validation	
		2.23.140.1.2.1	
		(2) Organization Validation	
		2.23.140.1.2.2	

		整形版	
		http://tlsrsarootca2024.ocsp.secom-cert.j	
		p	
		[2] ca issuers (1.3.6.1.5.5.7.48.2)	
		http://repo2.secomtrust.net/root/tlsrsa/tl	
		srsarootca2024.cer	
		·	
Cable 7.1-6	Subordinate CA Cert	ificate Profile (applicable to certificates issu	ed by Secu
Communica	ation ECC RootCA1)		
Basic field		Description of setting	critical
Version		Version 3	-
Serial Nur	nber	An integral serial number to be	-
		assigned by the CA to the certificate	
Signature	Algorithm	ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O=SECOM Trust Systems CO.,LTD.	-
	Common Name	CN=Security Communication ECC	-
		RootCA1	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
Subject	Country	C=JP	-
	Organization	O=Japan Registry Services Co., Ltd.	-
	Common Name	(1) Organization Validation	-
		CN= JPRS OV ECC CA 2024 G1	
		(2) Domain Validation	
		CN= JPRS DV ECC CA 2024 G1	
Subject Pu	ıblic Key Info	The subject's Public Key (384 bits)	-
Extended	field	Description of setting	critical
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key	n
		(160 bits)	
KeyUsage		Certificate Signing	у
		Off-line CRL Signing	
		CRL Signing (06)	
Certificate	Policies	[1] Certificate Policy	n
		(1) Domain Validation	
		2.23.140.1.2.1	
		(2) Organization Validation	
		2.23.140.1.2.2	

	変更履歴あり	
	[2] Certificate Policy	
	1.2.392.200091.100.902.1	
Basic Constraints	Subject Type=CA	У
	Path Length Constraint=0	
ExtendedKeyUsage	TLS Web Server Authentication	n
	TLS Web Client Authentication	
CRL Distribution Points	http://repository.secomtrust.net/SC-EC	n
	C-Root1/SCECCRoot1CRL.crl	
Authority Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n
	http://sceccrootca1.ocsp.secomtrust.net	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	http://repository.secomtrust.net/SC-EC	
	C-Root1/SCECCRoot1ca.cer	

		整形版		
		[2] Certificate Policy		
		1.2.392.200091.100.902.1		
Basic Cons	traints	Subject Type=CA	у	
		Path Length Constraint=0		
ExtendedK	TeyUsage	TLS Web Server Authentication	n	
		TLS Web Client Authentication		
CRL Distri	bution Points	http://repository.secomtrust.net/SC-EC	n	
		C-Root1/SCECCRoot1CRL.crl		
Authority ]	Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n	
		http://sceccrootca1.ocsp.secomtrust.net		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		http://repository.secomtrust.net/SC-EC		
		C-Root1/SCECCRoot1ca.cer		
Table 7.1-7 1 Basic field	Precertificate Profile (	applicable to certificates issued on or after Description of setting	July 29, 2 critical	020)
Version		Encoded value MUST be byte-for-byte	-	
, 01 01011		identical to the same field of the		
		Subuscriber Certificate.		
Serial Nun	ıber	Same as above	-	-
Signature		Same as above	-	
Issuer	Country	Same as above	-	
	Organization	Same as above	-	
	Common Name	Same as above	-	
Validity	NotBefore	Same as above	-	
0	NotAfter	Same as above	-	
Subject	Country	Same as above	-	
-	State or Province	Same as above	-	
	Locality	Same as above	-	
	Organization	Same as above	-	
	Organizational	Same as above	-	
	Unit			
	Common Name	Same as above	-	
Subject Pu	blic Key Info	Same as above	-	
Extended f	ïeld	Description of setting	critical	
Precertifica	ate Poison	extnValue OCTET STRING which is	У	
		exactly the hex-encoded bytes 0500, the		
		encoded representation of the ASN.1		
		NULL value, as specified in RFC 6962,		

## Table 7.1-7 Precertificate Profile (applicable to certificates issued on or after July 29, 2020)

Basic field		Description of setting	critical
Version		Encoded value MUST be byte-for-byte	-
		identical to the same field of the	
		Subuscriber Certificate.	
Serial Nu	nber	Same as above	-
Signature	Algorithm	Same as above	-
Issuer	Country	Same as above	-
	Organization	Same as above	-
	Common Name	Same as above	-
Validity	NotBefore	Same as above	-
	NotAfter	Same as above	-
Subject	Country	Same as above	-
	State or Province	Same as above	-
	Locality	Same as above	-
	Organization	Same as above	-
	Organizational	Same as above	-
	Unit		
	Common Name	Same as above	-
Subject Pu	ıblic Key Info	Same as above	-
Extended	field	Description of setting	critical
Precertific	ate Poison	extnValue OCTET STRING which is	у
		exactly the hex-encoded bytes 0500, the	
		encoded representation of the ASN.1	
		NULL value, as specified in RFC 6962,	

		整形版		
		[2] Certificate Policy		
		1.2.392.200091.100.902.1		
Basic Cons	straints	Subject Type=CA	у	
		Path Length Constraint=0	-	
Extended	KeyUsage	TLS Web Server Authentication	n	
		TLS Web Client Authentication		
CRL Distri	ibution Points	http://repository.secomtrust.net/SC-EC	n	
		C-Root1/SCECCRoot1CRL.crl		
Authority	Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n	
		http://sceccrootcal.ocsp.secomtrust.net		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		http://repository.secomtrust.net/SC-EC		
		C-Root1/SCECCRoot1ca.cer		
able 7.1-7	Precertificate Profile	applicable to certificates issued on or after	July 29, 2	020)
Basic field		Description of setting	critical	
Version		Encoded value MUST be byte-for-byte	-	
		identical to the same field of the		
		Subuscriber Certificate.		
Serial Nur	nber	Same as above	-	
Signature	Algorithm	Same as above	-	
Issuer	Country	Same as above	-	
	Organization	Same as above	-	
	Common Name	Same as above	-	
Validity	NotBefore	Same as above	-	
	NotAfter	Same as above	-	
Subject	Country	Same as above	-	
	State or Province	Same as above	-	
	Locality	Same as above	-	
	Organization	Same as above	-	
	Organizational	Same as above	-	
	Unit			
	Common Name	Same as above	-	
Subject Pu	ıblic Key Info	Same as above	-	
Extended f	field	Description of setting	critical	
Precertific	ate Poison	extnValue OCTET STRING which is	У	
		exactly the hex-encoded bytes 0500, the		
		encoded representation of the ASN.1		
		NULL value, as specified in RFC 6962,		
	10 /62	- ,	1	1

	変更履歴あり	
	Section 3.1.	
KeyUsage	Encoded value MUST be byte-for-byte	У
	identical to the same field of the	
	Subuscriber Certificate.	
ExtendedKeyUsage	Same as above	n
Subject Alt Name	Same as above	n
CertificatePolicies	Same as above	n
CRL Distribution Points	Same as above	n
Authority Information Access	Same as above	n
Authority Key Identifier	Same as above	n
Subject Key Identifier	Same as above	n

%If the Precertificate Poison extension is removed from the Precertificate, and the Signed Certificate Timestamp List is removed from the Subscriber certificate, the contents of the extensions field MUST be byte-for-byte identical to the Subscriber Certificate.

Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS Domain Validation Authority – G4 or JPRS Organization Validation Authority – G4)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Nur	nber	Non-sequential values greater than zero	-
		(0) and less than $2^{159}$ containing 64	
		bits of output from a CSPRNG	
Signature	Algorithm	sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN=JPRS Domain Validation Authority	
		- G4	
		(2) Organization Validation	
		CN=JPRS Organization Validation	
		Authority – G4	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-
Subject	Country	C=JP (fixed value)	-
	Organization	Japan Registry Services Co., Ltd. (fixed	-
		value)	
	Common Name	Name of the OCSP server (mandatory)	-
Subject Pu	ıblic Key Info	The subject's Public Key (RSA 2048 bits)	-
Extended	field	Description of setting	critical

		整形版		
		Section 3.1.		
KeyUsage		Encoded value MUST be byte-for-byte	у	
		identical to the same field of the		
		Subuscriber Certificate.		
ExtendedKeyU	Jsage	Same as above	n	
Subject Alt Na	ime	Same as above	n	
CertificatePoli	icies	Same as above	n	
CRL Distribut	ion Points	Same as above	n	
Authority Info	ormation Access	Same as above	n	
Authority Key	Identifier	Same as above	n	
Subject Key Id	lentifier	Same as above	n	
f the Precertif	ficate Poison exter	ision is removed from the Precertificate, a	nd the Sig	med
ctificate Times	stamp List is remo	oved from the Subscriber certificate, the c	ontents of	the
ensions field I	MUST be byte-for-	byte identical to the Subscriber Certificate		
main Validatio	-	rtificate Profile (Applicable to certificates is or JPRS Organization Validation Authority	y – G4)	
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Number	r	Non-sequential values greater than zero	-	
		(0) and less than $2^{159}$ containing 64		
: A1		bits of output from a CSPRNG		
		sha256 With RSA Encryption	-	
ssuer C	Country	sha256 With RSA Encryption C=JP	-	
ssuer C O	Country Organization	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd.	-	
ssuer C	Country	sha256 With RSA EncryptionC=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation	-	
ssuer C O	Country Organization	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority	-	
lssuer C O	Country Organization	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4	-	
0	Country Organization	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation	-	
ssuer C	Country Organization	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation	-	
Issuer C O C	Country Organization	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation	-	
ssuer C O C	Country Organization Common Name	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4	-	
ssuer C O C 7alidity N N	Country Organization Common Name NotBefore	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4 E.g.) 2008/3/1 00:00:00 GMT	- - - - - - -	
Issuer C O C Validity N Subject C	Country Organization Common Name IotBefore NotAfter	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT	- - - - - - - - -	
Issuer C O C Validity N Subject C	Country Organization Common Name NotBefore NotAfter Country	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value)	- - - - - - - - -	
Issuer C O C Validity N Subject C O	Country Organization Common Name NotBefore NotAfter Country	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed	- - - - - - - - -	
Issuer C O C Validity N Subject C O	Country Organization Common Name NotBefore NotAfter Country Organization Common Name	sha256 With RSA Encryption C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value)	- - - - - - - - - -	

Section 3.1.         Section 3.1.           KeyUsage         Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.         y           ExtendedKeyUsage         Same as above         n           Subject Alt Name         Same as above         n           CertificatePolicies         Same as above         n           CRL Distribution Points         Same as above         n           Authority Information Access         Same as above         n           Subject Key Identifier         Nome sequential to the Subscriber certificate.         suged           Table 7.1*8 OCSP Responder Certificate Profile (Applicable to certificates)         sued by JP			整形版		
KeyUsage         Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.         y           ExtendedKeyUsage         Same as above         n           Subject Alt Name         Same as above         n           CertificatePolicies         Same as above         n           CRI Distribution Points         Same as above         n           Authority Information Access         Same as above         n           Authority Key Identifier         Same as above         n           Subject Norsequential values greater than zero         o         0					
identical to the same field of the Subuscriber Certificate.         ExtendedKeyUsage       Same as above       n         Subject Alt Name       Same as above       n         CertificatePolicies       Same as above       n         CRI. Distribution Points       Same as above       n         Authority Information Access       Same as above       n         Authority Key Identifier       Same as above       n         Subject Key Identifier       Same as above       n         Subject Key Identifier       Same as above       n         Subject Key Identifier       Same as above       n         If the Precertificate Poison extension is removed from the Precertificate, and the Signed ortificate Timestamp List is removed from the Subscriber certificate.       n         Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificate issued by JPRS omain Validation Authority – G4 or JPRS Organization Validation Authority – G4)       Basic field       Description of setting       critical         Version       Version 3       -       -       -       -         Signature Algorithm       sha256 With RSA Encryption       -       -       -         Issuer       Country       C=JP       -       -       -       -       -       -       -       -       -	KeyUsage			V	
ExtendedKeyUsage         Same as above         n           Subject Alt Name         Same as above         n           CertificatePolicies         Same as above         n           CRL Distribution Points         Same as above         n           Authority Information Access         Same as above         n           Authority Information Access         Same as above         n           Authority Key Identifier         Same as above         n           Subject Key Identifier         Organization Version 3         c           Subject Number         Non sequential value				0	
Subject Alt Name         Same as above         n           CertificatePolicies         Same as above         n           CRL Distribution Points         Same as above         n           Authority Information Access         Same as above         n           Authority Information Access         Same as above         n           Authority Key Identifier         Same as above         n           Subject Methods         Description of setting         certificate           Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS omain Validation Authority – G4         Description of setting         critical           Version 3         -			Subuscriber Certificate.		
CertificatePolicies       Same as above       n         CRL Distribution Points       Same as above       n         Authority Information Access       Same as above       n         Authority Information Access       Same as above       n         Authority Key Identifier       Same as above       n         Subject Key Identifier       Same as above       n         Subject Key Identifier       Same as above       n         If the Precertificate Poison extension is removed from the Precertificate, and the Signed artificate Timestamp List is removed from the Subscriber certificate, the contents of the tensions field MUST be byte-for-byte identical to the Subscriber Certificates.         Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS omain Validation Authority – G4       Operativation Variation Variation Variation Variation Authority – G4         Version       Version 3       -         Serial Number       Non-sequential values greater than zero       -         (0) and less than 2^159 containing 64       bits of output from a CSPRNG       -         Signature Algorithm       sha256 With RSA Encryption       -         Issuer       Country       C=JP       -         Organization       Operativation Validation       -         CN=JPRS       Organization Validation       -	ExtendedK	KeyUsage	Same as above	n	
CRL Distribution Points       Same as above       n         Authority Information Access       Same as above       n         Authority Key Identifier       Same as above       n         Subject Key Identifier       Same as above       n         Subject Key Identifier       Same as above       n         If the Precertificate Poison extension is removed from the Precertificate, and the Signed ertificate Timestamp List is removed from the Subscriber certificate, the contents of the tensions field MUST be byte-for-byte identical to the Subscriber Certificates.         Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS print Validation Authority – G4 or JPRS Organization Validation Authority – G4         Version       Version 3       -         Serial Number       Non'sequential values greater than zero       -         (0) and less than 2^159 containing 64       bits of output from a CSPRNG       -         Signature Algorithm       sha256 With RSA Encryption       -         Issuer       Country       C=JP       -         Organization       O=Japan Registry Services Co., Ltd.       -         Common Name       (1) Domain Validation       -         (2) Organization Validation       -       -         Organization       C=JP       -       -         NotAfter       E.g.) 20	Subject Alt	Name	Same as above	n	
Authority Information Access         Same as above         n           Authority Key Identifier         Same as above         n           Subject Key Identifier         Same as above         n           Subject Key Identifier         Same as above         n           If the Precertificate Poison extension is removed from the Precertificate, and the Signed retrificate Timestamp List is removed from the Subscriber Certificate, the contents of the tensions field MUST be byte-for-byte identical to the Subscriber Certificate succed by JPRS organization Validation Authority – G4           Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS organization Validation Authority – G4         Pescription of setting         critical           Basic field         Description of setting         critical         version 3         -           Serial Number         Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG         -           Signature Algorithm         sha256 With RSA Encryption         -           Issuer         Country         C=JP         -           Organization         O= Japan Registry Services Co., Ltd.         -           Validity         NotBefore         E.g.) 2008/3/1 00:00:00 GMT         -           Validitiy         NotAfter         E.g.) 2008/3/1 00:00:00 GMT         -           Subject	Certificate	Policies	Same as above	n	
Authority Key Identifier         Same as above         n           Subject Key Identifier         Same as above         n           Subject Key Identifier         Same as above         n           If the Precertificate Poison extension is removed from the Precertificate, and the Signed ertificate Timestamp List is removed from the Subscriber Certificate, the contents of the tensions field MUST be byte-for-byte identical to the Subscriber Certificates issued by JPRS organin Validation Authority – G4 or JPRS Organization Validation Authority – G4)           Basic field         Description of setting         critical           Version         Version 3         -           Serial Number         Non-sequential values greater than zero         -           (0) and less than 2^159 containing 64         bits of output from a CSPRNG         -           Signature Algorithm         sha256 With RSA Encryption         -           Issuer         Country         C=JP         -           Organization         O= Japan Registry Services Co., Ltd.         -           Common Name         (1) Domain Validation         -           Childity         NotBefore         E.g.) 2008/3/1 00:00:00 GMT         -           Validity         NotAfter         E.g.) 2008/3/5 00:00:00 GMT         -           Subject         Country         C=JP         -         -	CRL Distri	bution Points	Same as above	n	
Subject Key Identifier         Same as above         n           If the Precertificate Poison extension is removed from the Precertificate, and the Signed rrtificate Timestamp List is removed from the Subscriber Certificate, the contents of the tensions field MUST be byte-for-byte identical to the Subscriber Certificates issued by JPRS omain Validation Authority – G4 or JPRS Organization Validation Authority – G4)           Basic field         Description of setting         critical           Version         Version 3         -           Serial Number         Non-sequential values greater than zero         -           (0) and less than 2^159 containing 64         bits of output from a CSPRNG         -           Signature Algorithm         sha256 With RSA Encryption         -           Issuer         Country         C=JP         -           Organization         0= Japan Registry Services Co., Ltd.         -           Common Name         (1) Domain Validation         -           Country         C4         (2) Organization Validation         -           Validity         NotBefore         E.g.) 2008/3/1 00:00:00 GMT         -           Subject         Country         C=JP         -           Organization         Japan Registry Services Co., Ltd.         -           Common Name         Solo8/3/1 00:00:00 GMT         -	Authority l	Information Access	Same as above	n	
If the Precertificate Poison extension is removed from the Precertificate, and the Signed errificate Timestamp List is removed from the Subscriber certificate, the contents of the tensions field MUST be byte-for-byte identical to the Subscriber Certificate.         Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS omain Validation Authority – G4 or JPRS Organization Validation Authority – G4)         Basic field       Description of setting       critical         Version       Version 3       -         Serial Number       Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG       -         Signature Algorithm       sha256 With RSA Encryption       -         Issuer       Country       C=JP       -         Organization       O= Japan Registry Services Co., Ltd.       -         Common Name       (1) Domain Validation       -         Cultority – G4       (2) Organization Validation       -         Validity       NotBefore       E.g.) 2008/3/1 00:00:00 GMT       -         Validity       NotAfter       E.g.) 2008/3/5 00:00:00 GMT       -         Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed       -         Validity       NotAfter       E.g.) 2008/3/5 00:00:00 GMT       -	Authority l	Key Identifier	Same as above	n	
ertificate Timestamp List is removed from the Subscriber certificate, the contents of the tensions field MUST be byte-for-byte identical to the Subscriber Certificate. Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS omain Validation Authority – G4 or JPRS Organization Validation Authority – G4) Basic field Description of setting critical Version Version 3 - Serial Number Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG Signature Algorithm sha256 With RSA Encryption - Issuer Country C=JP - Organization O= Japan Registry Services Co., Ltd Common Name (1) Domain Validation CN=JPRS Organization Validation CN=JPRS Organization Validation CN=JPRS Organization Validation CN=JPRS Organization Validation Authority – G4 Validity NotBefore E.g.) 2008/3/1 00:00:00 GMT - Subject Country C=JP (fixed value) - Organization Japan Registry Services Co., Ltd. (fixed value) Common Name Name of the OCSP server (mandatory) - Subject Public Key Info The subject's Public Key (RSA 2048 bits) -	Subject Ke	y Identifier	Same as above	n	
tensions field MUST be byte-for-byte identical to the Subscriber Certificate. Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS omain Validation Authority – G4 or JPRS Organization Validation Authority – G4) Basic field Version Version 3 critical Version 3 critical Version 3 critical Version 3 critical Signature Algorithm Subgert Ham Subscriber Certificates issued by JPRS Country C=JP Country C=JP Country C=JP Common Name (1) Domain Validation CN=JPRS Organization Validation CN=JPRS Subject Country C=JP (fixed value) Country C=JP (fixed value) Common Name Name of the OCSP server (mandatory) Charlee Subject Public Key Info The subject's Public Key (RSA 2048 bits)	If the Prec	ertificate Poison exte	ension is removed from the Precertificate, a	nd the Sig	med
Table 7.1-8 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS omain Validation Authority – G4 or JPRS Organization Validation Authority – G4)Basic field Description of setting criticalVersionVersion 3-Serial NumberNon-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGSignature Algorithmsha256 With RSA Encryption-IssuerCountryC=JP-OrganizationO= Japan Registry Services Co., LtdCommon Name(1) Domain Validation CN=JPRS Organization Validation Authority – G4-ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/5 00:00:00 GMT-SubjectCountryC=JP-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-	Certificate Ti	imestamp List is ren	noved from the Subscriber certificate, the c	ontents of	the
Demain Validation Authority – G4 or JPRS Organization Validation Authority – G4       Critical         Basic field       Description of setting       critical         Version       Version 3       -         Serial Number       Non-sequential values greater than zero       -         (0) and less than 2^159 containing 64       bits of output from a CSPRNG       -         Signature Algorithm       sha256 With RSA Encryption       -         Issuer       Country       C=JP       -         Organization       O= Japan Registry Services Co., Ltd.       -         Common Name       (1) Domain Validation       -         CN=JPRS       Organization       -         Validity       NotBefore       E.g.) 2008/3/1 00:00:00 GMT       -         Validity       NotAfter       E.g.) 2008/3/5 00:00:00 GMT       -         Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed       -         NotAfter       E.g.) 2008/3/1 00:00:00 GMT       -       -         Subject       Country       C=JP (fixed value)       -       -         Organization       Japan Registry Services Co., Ltd. (fixed       -       -         NotAfter       E.g.) 2008	extensions fie	eld MUST be byte-for	r-byte identical to the Subscriber Certificate		
Demain Validation Authority – G4 or JPRS Organization Validation Authority – G4         Basic field       Description of setting       critical         Version       Version 3       -         Serial Number       Non-sequential values greater than zero       -         (0) and less than 2^159 containing 64       bits of output from a CSPRNG       -         Signature Algorithm       sha256 With RSA Encryption       -         Issuer       Country       C=JP       -         Organization       O= Japan Registry Services Co., Ltd.       -         Common Name       (1) Domain Validation       -         CM       Common Name       (2) Organization Validation       -         Validity       NotBefore       E.g.) 2008/3/1 00:00:00 GMT       -         Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed       -         Validity       NotBefore       E.g.) 2008/3/1 00:00:00 GMT       -         Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed       -         Value)       Common Name       Name of the OCSP server (mandatory)       -					
Basic field       Description of setting       critical         Version       Version 3       -         Serial Number       Non-sequential values greater than zero       -         (0) and less than 2^159 containing 64       bits of output from a CSPRNG       -         Signature Algorithm       sha256 With RSA Encryption       -         Issuer       Country       C=JP       -         Organization       O= Japan Registry Services Co., Ltd.       -         Common Name       (1) Domain Validation       -         (2) Organization Validation       -       -         Country       C=JP       -         Validity       NotBefore       E.g.) 2008/3/1 00:00:00 GMT       -         Validity       NotAfter       E.g.) 2008/3/5 00:00:00 GMT       -         Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed       -         Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed       -         Organization       Japan Registry Services Co., Ltd. (fixed       -         Value)       Common Name       Name of the OCSP server (mandatory)       -		-		-	PRS
Version       Version 3       .         Serial Number       Non-sequential values greater than zero       .         (0) and less than 2^159 containing 64       bits of output from a CSPRNG       .         Signature Algorithm       sha256 With RSA Encryption       .         Issuer       Country       C=JP       .         Organization       O= Japan Registry Services Co., Ltd.       .         Common Name       (1) Domain Validation       .         (2) Organization Validation       .       .         Country       C=JPRS       .         Validity       NotBefore       E.g.) 2008/3/1 00:00:00 GMT       .         Validity       NotAfter       E.g.) 2008/3/5 00:00:00 GMT       .         Subject       Country       C=JP (fixed value)       .         Organization       Japan Registry Services Co., Ltd. (fixed value)       .         Subject       Country       C=JP (fixed value)       .         Subject       Common Name       Name of the OCSP server (mandatory)       .         Subject Public Key Info       The subject's Public Key (RSA 2048 bits)       .	Domain Valid	lation Authority – G	4 or JPRS Organization Validation Authority	y – G4)	1
Serial Number       Non-sequential values greater than zero       -         (0) and less than 2^159 containing 64       bits of output from a CSPRNG         Signature Algorithm       sha256 With RSA Encryption       -         Issuer       Country       C=JP       -         Organization       O= Japan Registry Services Co., Ltd.       -         Common Name       (1) Domain Validation       -         CM       (2) Organization Validation       -         CN=JPRS Domain Validation       -       -         CM       (2) Organization Validation       -         CN=JPRS Organization Validation       -       -         Validity       NotBefore       E.g.) 2008/3/1 00:00:00 GMT       -         Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed value)       -         Subject       Country       C=JP (fixed value)       -         Subject Public Key Info       Name of the OCSP server (mandatory)       -         Subject Public Key Info       The subject's Public Key (RSA 2048 bits)       -	Basic field			critical	
Signature Algorithmsha256 With RSA EncryptionSignature Algorithmsha256 With RSA EncryptionIssuerCountryC=JPOrganizationO= Japan Registry Services Co., Ltd.Common Name(1) Domain ValidationCN=JPRS Domain Validation Authority-G4(2) Organization ValidationCN=JPRS Organization ValidationAuthority - G4ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMTNotAfterE.g.) 2008/3/5 00:00:00 GMTSubjectCountryClappen Registry Services Co., Ltd. (fixed value)OrganizationJapan Registry Services Co., Ltd. (fixed value)OrganizationSubject Public Key InfoThe subject's Public Key (RSA 2048 bits)	Version		Version 3	-	
Signature Algorithmbits of output from a CSPRNGSignature Algorithmsha256 With RSA EncryptionIssuerCountryC=JPOrganizationO= Japan Registry Services Co., Ltd.OrganizationO= Japan Registry Services Co., Ltd.Common Name(1) Domain Validation(1) Domain Validation-CN=JPRS Domain Validation Authority-G4(2) Organization Validation-CN=JPRS Organization Validation-Authority - G4-ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMTNotAfterE.g.) 2008/3/5 00:00:00 GMT-SubjectCountryC=JP (fixed value)-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Common NameName of the OCSP server (mandatory)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-	Serial Num	nber	Non-sequential values greater than zero	-	
Signature Algorithmsha256 With RSA Encryption-IssuerCountryC=JP-OrganizationO= Japan Registry Services Co., LtdCommon Name(1) Domain Validation-CN=JPRS Domain Validation Authority - G4-(2) Organization Validation-CN=JPRS Organization Validation Authority - G4-ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/1 00:00:00 GMT-SubjectCountryC=JP (fixed value)-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Common NameName of the OCSP server (mandatory)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-			(0) and less than $2^{159}$ containing 64		
IssuerCountryC=JP-OrganizationO= Japan Registry Services Co., LtdCommon Name(1) Domain Validation-Common Name(1) Domain Validation-Common Name(2) Organization Validation-CN=JPRS Organization ValidationCN=JPRS Organization ValidationCN=JPRS Organization Validation-CN=JPRS Organization Validation-NotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/5 00:00:00 GMT-SubjectCountryC=JP (fixed value)-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Common NameName of the OCSP server (mandatory)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-			bits of output from a CSPRNG		
OrganizationO= Japan Registry Services Co., Ltd.OrganizationO= Japan Registry Services Co., Ltd.Common Name(1) Domain ValidationCN=JPRS Domain Validation Authority- G4(2) Organization ValidationCN=JPRS Organization ValidationAuthority – G4ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/5 00:00:00 GMTSubjectCountryOrganizationJapan Registry Services Co., Ltd. (fixed value)Common NameName of the OCSP server (mandatory)Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)	Signature	Algorithm		-	
Common Name(1) Domain ValidationCommon Name(1) Domain ValidationCN=JPRS Domain Validation Authority- G4(2) Organization ValidationCN=JPRS Organization ValidationAuthority – G4ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMTNotAfterE.g.) 2008/3/5 00:00:00 GMTSubjectCountryC=JP (fixed value)OrganizationJapan Registry Services Co., Ltd. (fixed value)Common NameName of the OCSP server (mandatory)Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)	Issuer	Country	C=JP	-	
CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority - G4ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/5 00:00:00 GMT-SubjectCountryC=JP (fixed value)-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Common NameName of the OCSP server (mandatory)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-		Organization	O= Japan Registry Services Co., Ltd.	-	
-G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMTNotAfterE.g.) 2008/3/5 00:00:00 GMTSubjectCountryC=JP (fixed value)OrganizationJapan Registry Services Co., Ltd. (fixed value)Common NameName of the OCSP server (mandatory)Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)		Common Name	(1) Domain Validation	-	
(2) Organization Validation CN=JPRS Authority – G4(2) Organization Validation CN=JPRS Organization Validation Authority – G4ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/5 00:00:00 GMT-SubjectCountryC=JP (fixed value)-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Common NameName of the OCSP server (mandatory)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-			CN=JPRS Domain Validation Authority		
CN=JPRS Authority – G4Organization Authority – G4ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/5 00:00:00 GMT-SubjectCountryC=JP (fixed value)-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Common NameName of the OCSP server (mandatory)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-			- G4		
Authority – G4ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/5 00:00:00 GMT-SubjectCountryC=JP (fixed value)-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Common NameName of the OCSP server (mandatory)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-					
ValidityNotBeforeE.g.) 2008/3/1 00:00:00 GMT-NotAfterE.g.) 2008/3/5 00:00:00 GMT-SubjectCountryC=JP (fixed value)-OrganizationJapan Registry Services Co., Ltd. (fixed value)-Common NameName of the OCSP server (mandatory)-Subject Public Key InfoThe subject's Public Key (RSA 2048 bits)-			CN=JPRS Organization Validation		
NotAfter       E.g.) 2008/3/5 00:00:00 GMT       -         Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed value)       -         Common Name       Name of the OCSP server (mandatory)       -         Subject Public Key Info       The subject's Public Key (RSA 2048 bits)       -			Authority – G4		
Subject       Country       C=JP (fixed value)       -         Organization       Japan Registry Services Co., Ltd. (fixed value)       -         Common Name       Name of the OCSP server (mandatory)       -         Subject Public Key Info       The subject's Public Key (RSA 2048 bits)       -	Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
Organization       Japan Registry Services Co., Ltd. (fixed value)         Common Name       Name of the OCSP server (mandatory)         Subject Public Key Info       The subject's Public Key (RSA 2048 bits)		NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-	
value)     value)       Common Name     Name of the OCSP server (mandatory)       Subject Public Key Info     The subject's Public Key (RSA 2048 bits)	Subject	Country	C=JP (fixed value)	-	
Common Name       Name of the OCSP server (mandatory)       -         Subject Public Key Info       The subject's Public Key (RSA 2048 bits)       -		Organization	Japan Registry Services Co., Ltd. (fixed	-	
Subject Public Key Info       The subject's Public Key (RSA 2048 bits)       -			value)		
		Common Name	Name of the OCSP server (mandatory)	-	
Extended field Description of setting critical	Subject Pu	blic Key Info	The subject's Public Key (RSA 2048 bits)	-	
	Extended f	ïeld	Description of setting	critical	

	変更履歴あり	
Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n
	(160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's Public Key	n
	(160 bits)	
KeyUsage	digitalSignature	У
ExtendedKeyUsage	OCSPSigning	n
OCSP No Check	null	n

Table 7.1-9 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS DV RSA CA 2024 G1 or JPRS OV RSA CA 2024 G1)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Nu	nber	Non-sequential values greater than zero	-
	(0) and less than $2^{159}$ containing 64		
		bits of output from a CSPRNG	
Signature	Algorithm	sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN=JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
		CN= JPRS OV RSA CA 2024 G1	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-
Subject	Country	C=JP (fixed value)	-
	Organization	Japan Registry Services Co., Ltd. (fixed	-
		value)	
	Common Name	Name of the OCSP server (mandatory)	-
Subject Pı	ıblic Key Info	The subject's Public Key (RSA 4096	-
		bits , RSA 3072 bits or RSA 2048 bits)	
Extended	field	Description of setting	critical
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key	n
		(160 bits)	
KeyUsage		digitalSignature	У
Extended	KeyUsage	OCSPSigning	n
OCSP No	Check	null	n

		整形版		備考
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Key Identifier KeyUsage		SHA-1 hash for the subject's Public Key	n	
		(160 bits)		
		digitalSignature	У	
ExtendedK	KeyUsage	OCSPSigning	n	
OCSP No (	Check	null	n	
Table 7.1-9	OCSP Responder C	ertificate Profile (Applicable to certificates is	sued by JI	PRS
V RSA CA 2	2024 G1 or JPRS OV	RSA CA 2024 G1)		
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Nun	nber	Non-sequential values greater than zero	-	
		(0) and less than $2^{159}$ containing 64		
		bits of output from a CSPRNG		
Signature	Algorithm	sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	
	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN=JPRS DV RSA CA 2024 G1		
		(2) Organization Validation		
		CN= JPRS OV RSA CA 2024 G1		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-	
Subject	Country	C=JP (fixed value)	-	
	Organization	Japan Registry Services Co., Ltd. (fixed	-	
		value)		
	Common Name	Name of the OCSP server (mandatory)	-	
Subject Pu	blic Key Info	The subject's Public Key (RSA 4096	-	
		bits , RSA 3072 bits or RSA 2048 bits)		
Extended f	ïeld	Description of setting	critical	
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n	
		(160 bits)		
KeyUsage		digitalSignature	У	
T · 1 1T	KeyUsage	OCSPSigning	n	
OCSP No (				

		整形版		
Authority F	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Key	y Identifier	SHA-1 hash for the subject's Public Key	n	
		(160 bits)		
KeyUsage		digitalSignature	У	
ExtendedK	eyUsage	OCSPSigning	n	
OCSP No C	check	null	n	
		-		J
Table 7.1-9	OCSP Responder C	ertificate Profile (Applicable to certificates is	sued by J	PRS
V RSA CA 2	024 G1 or JPRS OV	RSA CA 2024 G1)		_
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Num	lber	Non-sequential values greater than zero	-	
		(0) and less than $2^{159}$ containing 64		
		bits of output from a CSPRNG		
Signature A	Algorithm	sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	
	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN=JPRS DV RSA CA 2024 G1		
		(2) Organization Validation		
		CN= JPRS OV RSA CA 2024 G1		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-	
Subject	Country	C=JP (fixed value)	-	
	Organization	Japan Registry Services Co., Ltd. (fixed	-	
		value)		
	Common Name	Name of the OCSP server (mandatory)	-	
Subject Pub	olic Key Info	The subject's Public Key (RSA 4096	-	
		bits , RSA 3072 bits or RSA 2048 bits)		
Extended fi	ield	Description of setting	critical	
Authority F	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Key	y Identifier	SHA-1 hash for the subject's Public Key	n	
		(160 bits)		
KeyUsage		digitalSignature	У	
ExtendedK	eyUsage	OCSPSigning	n	
ExtendedKeyUsage OCSP No Check				

	Table 7 1-1	OCCD Beenenden C	変更履歴あり antificate Drafile (Annliashle to contificates	issued by
J		-	ertificate Profile (Applicable to certificates S OV ECC CA 2024 G1)	issued by
	Basic field		Description of setting	critical
	Version		Version 3	-
	Serial Num	ber	Non-sequential values greater than zero	-
			(0) and less than $2^{159}$ containing 64	
			bits of output from a CSPRNG	
	Signature A	lgorithm	ecdsa-with-SHA384	-
	Issuer	Country	C=JP	-
		Organization	O= Japan Registry Services Co., Ltd.	-
		Common Name	(1) Domain Validation	-
			CN=JPRS DV ECC CA 2024 G1	
			(2) Organization Validation	
			CN= JPRS OV ECC CA 2024 G1	
	Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
		NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-
	Subject	Country	C=JP (fixed value)	-
		Organization	Japan Registry Services Co., Ltd. (fixed	-
			value)	
		Common Name	Name of the OCSP server (mandatory)	-
	Subject Pub	olic Key Info	The subject's Public Key (256 bits or 384	-
			bits)	
	Extended fi	eld	Description of setting	critical
	Authority K	Key Identifier	SHA-1 hash for the issuer's Public Key	n
			(160 bits)	
	Subject Key	v Identifier	SHA-1 hash for the subject's Public Key	n
			(160 bits)	
	KeyUsage		digitalSignature	У
	ExtendedK	eyUsage	OCSPSigning	n
	OCSP No C	heck	null	n

## 7.1.1 Version Number(s)

The CA applies version 3.

## 7.1.2 Certificate Extension

Extensions of the Certificate issued by the CA is specified Section 7.1 of this CP.

## 7.1.3 Algorithm Object Identifier

The algorithm OID used in this service is as follows:

Table 7 1-1		整形版	
	-	Certificate Profile (Applicable to certificates	issued by
		RS OV ECC CA 2024 G1)	
Basic field		Description of setting	critical
Version	_	Version 3	-
Serial Nun	nber	Non-sequential values greater than zero	-
		(0) and less than 2^159 containing 64	
~		bits of output from a CSPRNG	
Signature		ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN=JPRS DV ECC CA 2024 G1	
		(2) Organization Validation	
		CN= JPRS OV ECC CA 2024 G1	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-
Subject	Country	C=JP (fixed value)	-
	Organization	Japan Registry Services Co., Ltd. (fixed value)	-
	Common Name	Name of the OCSP server (mandatory)	-
Subject Pu	blic Key Info	The subject's Public Key (256 bits or 384	-
		bits)	
Extended f	ïeld	Description of setting	critical
Authority l	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	n
		(160 bits)	
KeyUsage		digitalSignature	у
ExtendedK	KeyUsage	OCSPSigning	n
	Check	null	n

変更	履歴あり
Algorithm	Object Identifier
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1
sha384 With RSA Encryption	1.2.840.113549.1.1.12
id-ecPublicKey	1.2.840.10045.2.1
ecdsa-with-SHA384	1.2.840.10045.4.3.3

## 7.1.4 Name Format

The CA uses the Distinguished Name specified in RFC 5280.

For every valid Certification Path (as defined by RFC 5280, Section 6), for each Certificate in the Certification Path, the encoded content of the Issuer Distinguished Name field of a Certificate SHALL be byte-for-byte identical with the encoded form of the Subject Distinguished Name field of the Issuing CA certificate.

By issuing the Certificate, the CA represents that it followed the procedure set forth in its CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. The CA SHALL NOT include a Domain Name in a Subject attribute except as specified in Baseline Requirements Section 3.2.2.4.

Distinguished Names MUST NOT contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

The CA will not issue a certificate with a Subject Alternative Name extension or "common name" field that contains a reserved IP address or internal name.

If the "common name" value is a fully qualified domain name or a wildcard domain name, the "common name" value is encoded as a character-for-character copy of the dNSName entry value in the Subject Alternative Name extension. Specifically, all Domain Labels in the FQDN part of a fully qualified domain name or wildcard domain name are encoded as LDH Labels, and P-Labels does not convert to Unicode.

## 7.1.5 Name Constraints

Not set in the CA.

## 7.1.6 Certificate Policy Object Identifier

The OID of the certificate issued by the CA is as described in this CP "1.2 Document Name" and Identification".

The following Certificate Policy identifiers are reserved for use by the CA as an optional means of assertaing that a Certificate complies with Baseline Requirements.

[For DV certificate ] {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificatepolicies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1)

· · · · · · · · · · · · · · · · · · ·	<b>ě形版</b>
Algorithm	Object Identifier
sha256 With RSA Encryption	1.2.840.113549.1.1.11
RSA Encryption	1.2.840.113549.1.1.1
sha384 With RSA Encryption	1.2.840.113549.1.1.12
id-ecPublicKey	1.2.840.10045.2.1
ecdsa-with-SHA384	1.2.840.10045.4.3.3

## 7.1.4 Name Format

The CA uses the Distinguished Name specified in RFC 5280.

For every valid Certification Path (as defined by RFC 5280, Section 6), for a in the Certification Path, the encoded content of the Issuer Distinguished I Certificate SHALL be byte-for-byte identical with the encoded form a Distinguished Name field of the Issuing CA certificate.

By issuing the Certificate, the CA represents that it followed the procedure CP and/or CPS to verify that, as of the Certificate's issuance date, all Information was accurate. The CA SHALL NOT include a Domain Nam attribute except as specified in Baseline Requirements Section 3.2.2.4.

Distinguished Names MUST NOT contain only metadata such as '.', '-', an characters, and/or any other indication that the value is absent, inco applicable.

The CA will not issue a certificate with a Subject Alternative Name extension name" field that contains a reserved IP address or internal name.

If the "common name" value is a fully qualified domain name or a wildcard the "common name" value is encoded as a character-for-character copy of entry value in the Subject Alternative Name extension. Specifically, all Do the FQDN part of a fully qualified domain name or wildcard domain name LDH Labels, and P-Labels does not convert to Unicode.

## 7.1.5 Name Constraints

Not set in the CA.

## 7.1.6 Certificate Policy Object Identifier

The OID of the certificate issued by the CA is as described in this CP "1.2 D and Identification".

The following Certificate Policy identifiers are reserved for use by the CA means of assertaing that a Certificate complies with Baseline Requirements

[ For DV certificate ] {joint-iso-itu-t(2) international-or ca-browser-forum(140) certificatepolicies(1) baseline-requirements(2) doma (2.23.140.1.2.1)

	備考
each Certificate	
Name field of a	
of the Subject	
e set forth in its	
of the Subject	
ne in a Subject	
nd ' ' (i.e. space)	
omplete, or not	
ion or "common	
d domain name,	
f the dNSName	
omain Labels in	
are encoded as	
Ocument Name	
as an optional	
3.	
manipations(23)	
rganizations(23) iin-validated(1)}	
(III vanaatta)	

		変更履歴あり				整形版	
For O	V certificate ]	{joint-iso-itu-t(2) international-org	anizations(23)	[ For O	V certificate	{joint-iso-itu-t(2) international-or	ganizations(23
a-browser-fo	rum(140)	certificatepolicies(1) baseline-re	quirements(2)	ca-browser-for	rum(140)	certificatepolicies(1) baseline-r	equirements(2
rganization-	validated(2)} (2.23.14	40.1.2.2)		organization	validated(2)} (2.23.14	40.1.2.2)	
7.1.7 Use	of Policy Constr	aint Extensions		7.1.7 Use	of Policy Constr	aint Extensions	
lot set.				Not set.			
7.1.8 Polic	cy Qualifier Synt	ax and Semantics		7.1.8 Polic	y Qualifier Synt	ax and Semantics	
or the policy	qualifier, the URI of	f the Web page that publishes this CP and G	CPS is stored.	For the policy	qualifier, the URI o	f the Web page that publishes this CP and	CPS is stored.
7.1.9 How	to interpret Criti	ical Certificate Policy Extensions		7.1.9 How	to interpret Crit	ical Certificate Policy Extensions	
lot set.				Not set.		<b>,</b>	
	rofilo				rofilo		
<b>'.2 CRL P</b>		y the CA shall be as described in the followi	ng tabla:	7.2 CRL P		y the CA shall be as described in the follow	ing table.
ne prome or	UTLS to be issued by	y the OA shall be as described in the followi	iig table.		UTILS to be issued b	y the OA shan be as described in the follow	ing table.
Table 7.2.1 (	Deleted)			Table 7.2.1 (	Deleted)		
Table 7.2.2 (	CRL Profile (applicab	ole to certificates issued by JPRS DV RSA C	A 2024 G1 or	Table 7.2.2 C	RL Profile (applicat	ole to certificates issued by JPRS DV RSA (	CA 2024 G1 or
PRS OV RSA	A CA 2024 G1)			JPRS OV RSA	A CA 2024 G1)		
Basic field		Description of setting	critical	Basic field		Description of setting	critical
Version		Version 2	-	Version		Version 2	-
Signature A	Algorithm	SHA256 with RSAEncryption	-	Signature A	lgorithm	SHA256 with RSAEncryption	-
Issuer	Country	C=JP	-	Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-		Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-		Common Name	(1) Domain Validation	-
		CN=JPRS Domain Validation Authority				CN=JPRS Domain Validation Authority	
		- G4				- G4	
		(2) Organization Validation				(2) Organization Validation	
		CN=JPRS Organization Validation				CN=JPRS Organization Validation	
		Authority – G4				Authority – G4	
This Updat	e	E.g.) 2008/3/1 00:00:00 GMT	-	This Updat	e	E.g.) 2008/3/1 00:00:00 GMT	-
Next Updat	te	E.g.) 2008/3/5 00:00:00 GMT	-	Next Updat	e	E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-	Revoked	Serial Number	E.g.) 0123456789	-
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
s	Reason Code	Revocation Reason Code (*)	-	s	Reason Code	Revocation Reason Code (*)	-
Extended fi	ield	Description of setting	critical	Extended fi	eld	Description of setting	critical
CRL Numb	er	CRL number	n	CRL Numb	er	CRL number	n
Authority F	Key Identifier	SHA-1 hash for the issuer's Public Key	n	Authority K	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)				(160 bits)	
*: The "Rea	ason Code" field is se	et one of the Revocation Reason code specifi	ed in the table	*: The "Rea	ason Code" field is se	et one of the Revocation Reason code specif	ied in the tabl
		on Code is "#0 unspecified", the "Reason C	1 22 62 1 1 1			on Code is "#0 unspecified", the "Reason (	

not appear in the CRL profile.

Table 7.2.3 CRL Profile (applicable to certificates issued by JPRS DV RSA CA 2024 G1 or
JPRS OV RSA CA 2024 G1)

Basic field		Description of setting	critical
Version		Version 2	-
Signature A	lgorithm	SHA384 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN= JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
		CN=JPRS OV RSA CA 2024 G1	
This Update	9	E.g.) 2008/3/1 00:00:00 GMT	-
Next Updat	e	E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
s	Reason Code	Revocation Reason Code (*)	-
Extended fi	eld	Description of setting	critical
CRL Numb	er	CRL number	n
Authority K	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	

\*: The "Reason Code" field is set one of the Revocation Reason code specified in the table 7.2.2.1. If the Revocation Reason Code is "#0 unspecified", the "Reason Code" field does not appear in the CRL profile.

Table 7.2.4 CRL Profile (applicable to certificates issued by JPRS DV ECC CA 2024 G1 or JPRS OV ECC CA 2024 G1)

Basic field		Description of setting	critical
Version		Version 2	-
Signature	Algorithm	ecdsa-with-SHA384	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN= JPRS DV ECC CA 2024 G1	
		(2) Organization Validation	
		CN=JPRS OV ECC CA 2024 G1	
This Upda	te	E.g.) 2008/3/1 00:00:00 GMT	-
Next Upda	ate	E.g.) 2008/3/5 00:00:00 GMT	-

		整形版	
not appear	in the CRL profile.		
fable 7.2.3 C	RL Profile (applical	ole to certificates issued by JPRS DV RSA C	A 2024 G
	A CA 2024 G1)		
Basic field		Description of setting	critical
Version		Version 2	-
Signature A	lgorithm	SHA384 with RSAEncryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	(1) Domain Validation	-
		CN= JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
		CN=JPRS OV RSA CA 2024 G1	
This Update	e	E.g.) 2008/3/1 00:00:00 GMT	-
Next Updat	e	E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
S	Reason Code	Revocation Reason Code (*)	-
Extended fi	eld	Description of setting	critical
	0.14	CRL number	n
CRL Numbe	er		11
	Key Identifier	SHA-1 hash for the issuer's Public Key	n
Authority K	Key Identifier	SHA-1 hash for the issuer's Public Key	n
Authority K The "Reaso	Key Identifier n Code" field is set	SHA-1 hash for the issuer's Public Key (160 bits)	n ed in the t
Authority K The "Reaso 2.2.1. If the	Key Identifier n Code" field is set	SHA-1 hash for the issuer's Public Key (160 bits) one of the Revocation Reason code specifie	n ed in the t
Authority K The "Reaso 2.2.1. If the	Key Identifier n Code" field is set Revocation Reason	SHA-1 hash for the issuer's Public Key (160 bits) one of the Revocation Reason code specifie	n ed in the t
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical	SHA-1 hash for the issuer's Public Key (160 bits) one of the Revocation Reason code specifie	n ed in the t ' field does
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C PRS OV ECC	Key Identifier n Code" field is set Revocation Reason CRL profile.	SHA-1 hash for the issuer's Public Key (160 bits) one of the Revocation Reason code specific Code is "#0 unspecified", the "Reason Code"	n ed in the t ' field does
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical	SHA-1 hash for the issuer's Public Key (160 bits) one of the Revocation Reason code specific Code is "#0 unspecified", the "Reason Code"	n ed in the t ' field does
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C PRS OV ECC	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical	SHA-1 hash for the issuer's Public Key (160 bits) one of the Revocation Reason code specific Code is "#0 unspecified", the "Reason Code" ole to certificates issued by JPRS DV ECC C	n ed in the t ' field does CA 2024 G
Authority K The "Reaso 2.2.1. If the ppear in the Fable 7.2.4 C PRS OV ECC Basic field	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical C CA 2024 G1)	SHA-1 hash for the issuer's Public Key (160 bits)         one of the Revocation Reason code specific         Code is "#0 unspecified", the "Reason Code"         ole to certificates issued by JPRS DV ECC C         Description of setting	n ed in the t ' field does CA 2024 G
Authority K The "Reaso 2.2.1. If the ppear in the Fable 7.2.4 C PRS OV ECC Basic field Version	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical C CA 2024 G1)	SHA-1 hash for the issuer's Public Key (160 bits)         one of the Revocation Reason code specified         Code is "#0 unspecified", the "Reason Code"         ole to certificates issued by JPRS DV ECC C         Description of setting         Version 2	n ed in the t ' field does CA 2024 G
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C PRS OV ECC Basic field Version Signature A	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical C CA 2024 G1)	SHA-1 hash for the issuer's Public Key (160 bits)         one of the Revocation Reason code specific         Code is "#0 unspecified", the "Reason Code"         ole to certificates issued by JPRS DV ECC C         Description of setting         Version 2         ecdsa-with-SHA384	n ed in the t ' field does CA 2024 G
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C PRS OV ECC Basic field Version Signature A	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical C CA 2024 G1)	SHA-1 hash for the issuer's Public Key (160 bits)         one of the Revocation Reason code specific         Code is "#0 unspecified", the "Reason Code"         ole to certificates issued by JPRS DV ECC C         Description of setting         Version 2         ecdsa-with-SHA384         C=JP	n ed in the t ' field does CA 2024 G
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C PRS OV ECC Basic field Version Signature A	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical C CA 2024 G1) Igorithm Country Organization	SHA-1 hash for the issuer's Public Key (160 bits)         one of the Revocation Reason code specifie         Code is "#0 unspecified", the "Reason Code"         ole to certificates issued by JPRS DV ECC C         Description of setting         Version 2         ecdsa-with-SHA384         C=JP         O= Japan Registry Services Co., Ltd.	n ed in the t ' field does CA 2024 G
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C PRS OV ECC Basic field Version Signature A	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical C CA 2024 G1) Igorithm Country Organization	SHA-1 hash for the issuer's Public Key (160 bits)         one of the Revocation Reason code specifie         Code is "#0 unspecified", the "Reason Code"         ole to certificates issued by JPRS DV ECC C         Description of setting         Version 2         ecdsa-with-SHA384         C=JP         O= Japan Registry Services Co., Ltd.         (1) Domain Validation	n ed in the t ' field does CA 2024 G
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C PRS OV ECC Basic field Version Signature A	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical C CA 2024 G1) Igorithm Country Organization	SHA-1 hash for the issuer's Public Key (160 bits)         one of the Revocation Reason code specifie         Code is "#0 unspecified", the "Reason Code"         ble to certificates issued by JPRS DV ECC C         Description of setting         Version 2         ecdsa-with-SHA384         C=JP         O= Japan Registry Services Co., Ltd.         (1) Domain Validation         CN= JPRS DV ECC CA 2024 G1	n ed in the t ' field does CA 2024 G
Authority K The "Reaso 2.2.1. If the opear in the Fable 7.2.4 C PRS OV ECC Basic field Version Signature A	Key Identifier n Code" field is set Revocation Reason CRL profile. CRL Profile (applical C CA 2024 G1) Igorithm Country Organization Common Name	SHA-1 hash for the issuer's Public Key (160 bits)         one of the Revocation Reason code specific         Code is "#0 unspecified", the "Reason Code"         ole to certificates issued by JPRS DV ECC C         Description of setting         Version 2         ecdsa-with-SHA384         C=JP         O= Japan Registry Services Co., Ltd.         (1) Domain Validation         CN= JPRS DV ECC CA 2024 G1         (2) Organization Validation	n ed in the t ' field does CA 2024 G

		整形版		
not appear	in the CRL profile.			
	F			
Table 7.2.3 C	CRL Profile (applicat	ole to certificates issued by JPRS DV RSA C	A 2024 G1	or
PRS OV RSA	A CA 2024 G1)			
Basic field		Description of setting	critical	
Version		Version 2	-	
Signature A	lgorithm	SHA384 with RSAEncryption	-	
Issuer	Country	C=JP	-	
	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN= JPRS DV RSA CA 2024 G1		
		(2) Organization Validation		
		CN=JPRS OV RSA CA 2024 G1		
This Update	e	E.g.) 2008/3/1 00:00:00 GMT	-	
Next Updat	ce	E.g.) 2008/3/5 00:00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
s	Reason Code	Revocation Reason Code (*)	-	
Extended fi	eld	Description of setting	critical	
CRL Numbe	er	CRL number	n	
Authority K	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
The "Reaso	n Code" field is set	one of the Revocation Reason code specifie	ed in the t	able
.2.2.1. If the	Revocation Reason	Code is "#0 unspecified", the "Reason Code"	' field does	not
ppear in the	CRL profile.			
		ole to certificates issued by JPRS DV ECC C	CA 2024 G1	or
	C CA 2024 G1)			1
Basic field		Description of setting	critical	
Version		Version 2	-	
Signature A	-	ecdsa-with-SHA384	-	
Issuer	Country	C=JP	-	
	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN= JPRS DV ECC CA 2024 G1		
		(2) Organization Validation		
		CN=JPRS OV ECC CA 2024 G1		
This Update	e	E.g.) 2008/3/1 00:00:00 GMT	-	

		変更履歴あり	
Revoked	Serial Number	E.g.) 0123456789	-
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
s	Reason Code	Revocation Reason Code (*)	-
Extended field		Description of setting	critical
CRL Number		CRL number	n
Authority Key Identifier		SHA-1 hash for the issuer's Public Key	n
		(160 bits)	

\*: The "Reason Code" field is set one of the Revocation Reason code specified in the table 7.2.2.1. If the Revocation Reason Code is "#0 unspecified", the "Reason Code" field does not appear in the CRL profile.

## 7.2.1 Version Number(s)

The CA applies CRL version 2.

#### 7.2.2 CRL Entry Extensions

Use the CRL extension field issued by the CA.

reasonCode (OID 2.5.29.21)

CRLReason must be included in the reasonCode extension of the CRL entry corresponding to a Subscriber Certificate that is revoked after July 15, 2023, unless the CRLReason is "unspecified (0)".

The CA set one of the Revocation Reason Code specified in the following table, with the exception of "unspecified (0)".

#### Table 7.2.2.1 Revocation Reason Code

Revocation Reason Code	Circumstances for setting this Revocation Reason
	Code
#0 unspecified	When the reason codes below do not apply to the
	revocation request.
#1 keyCompromise	When the Subscriber have reasons to believe that the
	private key of their certificate has been or may be
	compromised,
#3 affiliationChanged	When the name of subscriber's organization or other
	organizational information in the certificate has
	changed.
#4 superseded	When the Subscriber requests a new certificate to
	replace their existing certificate.
#5 cessationOfOperation	When the Subscriber no longer owns all of the
	domain names in the certificate or when they will no
	longer be using the certificate because they are

		整形版		
Revoked	Serial Number	E.g.) 0123456789	-	
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
s	Reason Code	Revocation Reason Code (*)	-	
Extended fi		Description of setting	critical	-
CRL Numb		CRL number	n	
	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
	·	(160 bits)		
: The "Reaso	on Code" field is se	t one of the Revocation Reason code specifie	ed in the t	able
.2.2.1. If the	Revocation Reason	1 Code is "#0 unspecified", the "Reason Code"	' field does	not
ppear in the	CRL profile.			
7.2.1 Vers	ion Number(s)			
	es CRL version 2.			
7.2.2 CRL	Entry Extensio	ons		
Jse the CRL	extension field issu	ed by the CA.		
reasonCoo	de (OID 2.5.29.21)			
CRLReason n	nust be included in	the reasonCode extension of the CRL entry $% \left( {{{\left( {{{{\rm{CRL}}}} \right)}_{\rm{cl}}}} \right)$	correspon	ding
		is revoked after July 15, 2023, unless the	CRLReaso	n is
unspecified (	0)".			
		on Reason Code specified in the following ta	able, with	the
exception of "	unspecified (0)".			
	D D			
	Revocation Reason		D	1
Revocation	Reason Code	Circumstances for setting this Revocation	n Reason	
	a 1	Code		-
#0 unspecif	fied	When the reason codes below do not app	ly to the	
		revocation request.		-
#1 keyCom	promise	When the Subscriber have reasons to believe		
		private key of their certificate has been or	r may be	
		compromised,		
#3 affiliatio	onChanged	When the name of subscriber's organization	n or other	
		organizational information in the certifi	cate has	
		changed.		-
#4 superse	ded	When the Subscriber requests a new cert	ificate to	
		replace their existing certificate.		_
		• 0		
#5 cessation	nOfOperation	When the Subscriber no longer owns a	ll of the	
#5 cessatio	nOfOperation			

		整形版			備考
Revoked	Serial Number	E.g.) 0123456789	-		
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-		
s	Reason Code	Revocation Reason Code (*)	-		
Extended fi	eld	Description of setting	critical		
CRL Numb	er	CRL number	n		
Authority K	Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n		
L *: The "Reaso	n Code" field is se	t one of the Revocation Reason code specifie	d in the t	able	
		Code is "#0 unspecified", the "Reason Code"			
appear in the					
11	1				
7.2.1 Versi	ion Number(s)				
The CA applie	es CRL version 2.				
7.2.2 CRL	Entry Extensio	ns			
Use the CRL o	extension field issu	ed by the CA.			
reasonCod	le (OID 2.5.29.21)				
CRLReason n	nust be included in	the reasonCode extension of the CRL entry $% \left( {{{\left( {{{{\rm{CRL}}}} \right)}_{\rm{cl}}}} \right)$	correspond	ling	
to a Subscrib	er Certificate that	is revoked after July 15, 2023, unless the	CRLReaso	n is	
"unspecified (	0)".				
The CA set of	ne of the Revocati	on Reason Code specified in the following ta	able, with	the	
exception of "v	unspecified (0)".				
Table 7.9.9.1	Revocation Reason	a Cada			
	Reason Code		Descer		
Revocation	Reason Code	Circumstances for setting this Revocation Code	i Keason		
#0	čed		ler to the		
#0 unspecif	led	When the reason codes below do not app revocation request.	ly to the		
#1 keyCom	nromise	When the Subscriber have reasons to believe	that the		
	promise	private key of their certificate has been or			
		compromised,	i illay be		
#3 affiliatio	onChanged	When the name of subscriber's organization	or other		
	C	organizational information in the certifi			
		changed.			
#4 supersed	led	When the Subscriber requests a new cert	ificate to		
		replace their existing certificate.			
#5 cessation	nOfOperation	When the Subscriber no longer owns a	ll of the		
	• • • • • • • • •	domain names in the certificate or when the			
		longer be using the certificate because	-		
<u> </u>			v	11	

	変更履歴あり		
	discontinuing their website.		
#9 privilegeWithdrawn	When the Subscriber has not upheld their material		#
	obligations under the Terms and Conditions.		

## 7.3 OCSP Profile

## 7.3.1 Version Number(s)

The CA shall apply OCSP Version 1.

## 7.3.2 OCSP Extensions

Refer to Section 7.1 of this CP.

The singleExtensions of an OCSP response MUST NOT contain the reasonCode (OID 2.5.29.21) CRL entry extension.

# 8. Compliance Audit and Other Assessments

## 8.1 Frequency and Circumstances of Assessment

JPRS shall perform audits at least once a year to verify whether or not the CA is operated in compliance with this CP and the CPS.

## 8.2 Identity/Qualifications of Assessor

Compliance audits shall be performed by auditors who are adequately experienced in auditing.

Audits required for obtaining the WebTrust certification shall be performed by audit corporations with the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- licensed by WebTrust;
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an Internal Government Auditing Agency, maintains
   Professional Liability/Errors & Omissions insurance with policy limits of at least
   one million US dollars in coverage

## 8.3 Assessor's Relationship to Assessed Entity

	整形版
	discontinuing their website.
#9 privilegeWithdrawn	When the Subscriber has not upheld their
	obligations under the Terms and Conditions

## 7.3 OCSP Profile

## 7.3.1 Version Number(s)

The CA shall apply OCSP Version 1.

## 7.3.2 OCSP Extensions

Refer to Section 7.1 of this CP.

The singleExtensions of an OCSP response MUST NOT contain the real 2.5.29.21) CRL entry extension.

# 8. Compliance Audit and Other Assessment

## 8.1 Frequency and Circumstances of Assessment

JPRS shall perform audits at least once a year to verify whether or not the CA compliance with this CP and the CPS.

## 8.2 Identity/Qualifications of Assessor

Compliance audits shall be performed by auditors who are adequately auditing.

Audits required for obtaining the WebTrust certification shall be performed to corporations with the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in Audit Scheme
- Employs individuals who have proficiency in examining Public Key In technology, information security tools and techniques, information techniques, and the third-party attestation function;
- licensed by WebTrust;
- Bound by law, government regulation, or professional code of ethics;
- Except in the case of an Internal Government Auditing Agency, main Professional Liability/Errors & Omissions insurance with policy limit one million US dollars in coverage

# 8.3 Assessor's Relationship to Assessed Entity

Auditors shall be operationally independent of the auditee divisions, except in matters Auditors shall be operationally independent of the auditee divisions, except in matters

	備考
r material	
s.	
asonCode (OID	
S	
A is operated in	
A is operated in	
experienced in	
experienceu in	
rmed by audit	
n an Eligible	
nfrastructure	
chnology and	
and	
tains	
ts of at least	
ept in matters	

related to the audits.

## 8.4 Topics Covered by Assessment

Audits shall be performed mainly to verify whether or not the CA is operated in compliance with this CP and the CPS. The CA shall undergo WebTrust in accordance with one of the following schemes:

- WebTrust for CAs
- WebTrust for CAs SSL Baseline
- WebTrust for CAs Network Security

## 8.5 Actions Taken as a Result of Deficiency

The CA shall promptly take necessary corrective actions with respect to any deficiencies pointed out in an audit report.

## 8.6 Communication of Results

Auditors shall report the audit results to the CA.

The CA will not externally disclose the audit results unless the CA is required to disclose the same under any law, or by an associated organization based on an agreement with JPRS, or unless such disclosure has been approved by the CA's Certificate Operation Conference.

Reports on validation under the WebTrust shall be made referable in a specific site according to the provisions of the respective guidelines of the WebTrust.

## 8.7 Self-Audits

The CA shall monitor adherence this CP, the CPS, and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

# 9. Other Business and Legal Matters

## 9.1 Fees

To be separately stipulated.

## 9.2 Financial Responsibility

The CA shall maintain a sufficient financial foundation required for operating and maintaining the CA.

## 9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

related to the audits.

## 8.4 Topics Covered by Assessment

Audits shall be performed mainly to verify whether or not the CA is operated with this CP and the CPS. The CA shall undergo WebTrust in accordance v following schemes:

- WebTrust for CAs
- WebTrust for CAs SSL Baseline
- WebTrust for CAs Network Security

## 8.5 Actions Taken as a Result of Deficiency

The CA shall promptly take necessary corrective actions with respect to a pointed out in an audit report.

## 8.6 Communication of Results

Auditors shall report the audit results to the CA.

The CA will not externally disclose the audit results unless the CA is require the same under any law, or by an associated organization based on an a JPRS, or unless such disclosure has been approved by the CA's Certific Conference.

Reports on validation under the WebTrust shall be made referable in according to the provisions of the respective guidelines of the WebTrust.

## 8.7 Self-Audits

The CA shall monitor adherence this CP, the CPS, and strictly control its ser performing self audits on at least a quarterly basis against a randomly select least three percent of the Certificates issued by it during the period immediately after the previous self-audit sample was taken.

# 9. Other Business and Legal Matters

**9.1 Fees** To be separately stipulated.

## 9.2 Financial Responsibility

The CA shall maintain a sufficient financial foundation required for maintaining the CA.

## 9.3 Confidentiality of Business Information

#### 9.3.1 Scope of Confidential Information

### 整形版

	備考
d in compliance with one of the	
any deficiencies	
aired to disclose agreement with acate Operation a specific site	
rvice quality by ted sample of at od commencing	
operating and	

変更履歴あり	整形版
Stipulated in the CPS.	Stipulated in the CPS.
9.3.2 Information not within the Scope of Confidential Information	9.3.2 Information not within the Scope of Confidential Information
Stipulated in the CPS.	Stipulated in the CPS.
9.3.3 Responsibility to Protect Confidential Information	9.3.3 Responsibility to Protect Confidential Information
Stipulated in the CPS.	Stipulated in the CPS.
9.4 Privacy of Personal Information	9.4 Privacy of Personal Information
Stipulated in the CPS.	Stipulated in the CPS.
9.5 Intellectual Property Rights	9.5 Intellectual Property Rights
Jnless separately agreed, all intellectual property rights pertaining to the following	
nformation shall belong to JPRS:	information shall belong to JPRS:
• certificates and site seals issued by the CA, as well as information on certificate	• certificates and site seals issued by the CA, as well as information on certificate
revocation;	revocation;
• this CP, the CPS, and related documents;	• this CP, the CPS, and related documents;
• Public Keys and Private Keys of the CA; and	Public Keys and Private Keys of the CA; and
<ul> <li>software provided by JPRS.</li> </ul>	• software provided by JPRS.
This CP is published under the Creative Commons license Attribution- NoDerivatives	This CP is published under the Creative Commons license Attribution- NoDerivatives
(CC-BY-ND) 4.0 International.	(CC-BY-ND) 4.0 International.
(https://creativecommons.org/licenses/by-nd/4.0/)	( <u>https://creativecommons.org/licenses/by-nd/4.0/</u> )
6 Representations and Warranties	9.6 Representations and Warranties
9.6.1 CA Representations and Warranties	9.6.1 CA Representations and Warranties
The CA shall bear the following obligations in performing its business operations as the CA:	The CA shall bear the following obligations in performing its business operations as the CA:
<ul> <li>securely generate and manage the CA's Private Keys;</li> </ul>	<ul> <li>securely generate and manage the CA's Private Keys;</li> </ul>
$\boldsymbol{\cdot}$ accurately manage certificate issuance and revocation based on applications from the	$\cdot$ accurately manage certificate issuance and revocation based on applications from the
RA;	RA;
<ul> <li>monitor and operate the CA's system at work; and</li> </ul>	<ul> <li>monitor and operate the CA's system at work; and</li> </ul>
• issue and publish the CRLs.	• issue and publish the CRLs.
9.6.2 RA Representations and Warranties	9.6.2 RA Representations and Warranties
The CA shall bear the following obligations in performing its business operations as an RA:	The CA shall bear the following obligations in performing its business operations as an RA:
• install registration terminals in a secure environment and operate them;	• install registration terminals in a secure environment and operate them;
+ accurately communicate information to the CA in processing applications for	$\cdot$ accurately communicate information to the CA in processing applications for
certificate issuance and revocation;	certificate issuance and revocation;
$\cdot$ promptly communicate information to the CA during operating hours in processing	$\cdot$ promptly communicate information to the CA during operating hours in processing
applications for certificate revocation; and	applications for certificate revocation; and
<ul> <li>maintain and administer the Repository.</li> </ul>	<ul> <li>maintain and administer the Repository.</li> </ul>

#### 9.6.3 Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
- 2. **Protection of Private Key**: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
- 3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- 4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- 5. **Reporting and Revocation**: An obligation and warranty to: a. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and b. promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- 6. **Termination of Use of Certificate**: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- 7. **Responsiveness**: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.

#### 整形版

#### 9.6.3 Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber Agreement or Terms of Us Applicant make the commitments and warranties in this section for the bene and the Certificate Beneficiaries.

The Subscriber Agreement or Terms of Use MUST contain provisions imposi Applicant itself (or made by the Applicant on behalf of its principal or agent subcontractor or hosting service relationship) the following obligations and v

- 1. Accuracy of Information: An obligation and warranty to provide accur complete information at all times to the CA, both in the certificate reotherwise requested by the CA in connection with the issuance of the to be supplied by the CA;
- 2. **Protection of Private Key**: An obligation and warranty by the Applica reasonable measures to assure control of, keep confidential, and prop all times the Private Key that corresponds to the Public Key to be inc requested Certificate(s) (and any associated activation data or device or token);
- 3. Acceptance of Certificate: An obligation and warranty that the Subscreview and verify the Certificate contents for accuracy;
- 4. **Use of Certificate**: An obligation and warranty to install the Certificat servers that are accessible at the subjectAltName(s) listed in the Cert use the Certificate solely in compliance with all applicable laws and s accordance with the Subscriber Agreement or Terms of Use;
- 5. **Reporting and Revocation**: An obligation and warranty to: a. promptly revocation of the Certificate, and cease using it and its associated Pri there is any actual or suspected misuse or compromise of the Subscrib Key associated with the Public Key included in the Certificate, and b request revocation of the Certificate, and cease using it, if any inform Certificate is or becomes incorrect or inaccurate;
- 6. **Termination of Use of Certificate**: An obligation and warranty to proruse of the Private Key corresponding to the Public Key included in the upon revocation of that Certificate for reasons of Key Compromise.
- 7. **Responsiveness**: An obligation to respond to the CA's instructions cor Compromise or Certificate misuse within a specified time period.

	備考
se, that the	
efit of the CA	
ing on the	
under a	
warranties:	
irate and	
equest and as	
e Certificate(s)	
ant to take all	
perly protect at	
cluded in the	
e, e.g. password	
criber will	
ate only on	
rtificate, and to	
solely in	
U	
ly request	
rivate Key, if	
iber's Private	
o. promptly	
nation in the	
mptly cease all	
he Certificate	
ncerning Key	

8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by the CA's CP, CPS, or these Baseline Requirements.

#### 9.6.4 Relying Party Representations and Warranties

Each Relying Party warrants that he/she/it will comply with the provisions of this CP. If any Relying Party fails to comply with any provision of this CP, the Relying Party shall assume all responsibilities therefor.

#### 9.6.5 Representations and Warranties of Other Participants

No stipulation.

#### 9.7 Disclaimer of Warranties

The CA is not liable for any indirect, special, incidental, or consequential damage arising in connection with any of the warranties stipulated in "9.6.1 CA Representations and Warranties" of this CP, or for lost profits, loss of data, or any other indirect or consequential damage whatsoever.

### 9.8 Limitations of Liability

The CA is not liable for the provisions of "9.6.1 CA Representations and Warranties" of this CP if damage falling under any of the following occurs:

- any or all damage arising from any unlawful conduct, unauthorized use, negligence, or any other cause not attributable to the CA;
- any damage resulting from a failure of a Subscriber to perform any of his/her/its obligations;
- any or all damage arising from any cause attributable to a Subscriber's system;
- any damage arising from any defect or malfunction, or operation, of the hardware or software of the CA or a Subscriber;
- any damage caused by any information published in a certificate or the CRL, for any reason not attributable to the CA;
- any or all damage incurred by a failure in normal communication caused by any reason not attributable to the CA;
- any or all damage arising in connection with the use of a certificate, such as business debts;
- any damage caused by an improvement, beyond expectations at this point in time, in the cryptographic algorithm decoding capabilities of hardware or software;
- any or all damage caused by the suspension of the CA's business operations due to a force majeure event, including, but not limited to, any act of God, earthquake, volcanic eruption, fire, tsunami, flood disaster, lightning strike, war, civil commotion or terrorism; or

#### 整形版

8. Acknowledgment and Acceptance: An acknowledgment and acceptance is entitled to revoke the certificate immediately if the Applicant were terms of the Subscriber Agreement or Terms of Use or if revocation is the CA's CP, CPS, or these Baseline Requirements.

#### 9.6.4 Relying Party Representations and Warranties

Each Relying Party warrants that he/she/it will comply with the provisions of any Relying Party fails to comply with any provision of this CP, the Relying Party assume all responsibilities therefor.

## **9.6.5 Representations and Warranties of Other Participants** No stipulation.

No stipulation.

#### 9.7 Disclaimer of Warranties

The CA is not liable for any indirect, special, incidental, or consequential dar connection with any of the warranties stipulated in "9.6.1 CA Repres Warranties" of this CP, or for lost profits, loss of data, or any other indirect or damage whatsoever.

#### 9.8 Limitations of Liability

The CA is not liable for the provisions of "9.6.1 CA Representations and War CP if damage falling under any of the following occurs:

- any or all damage arising from any unlawful conduct, unauthorized use or any other cause not attributable to the CA;
- any damage resulting from a failure of a Subscriber to perform any of l obligations;
- any or all damage arising from any cause attributable to a Subscriber's
- any damage arising from any defect or malfunction, or operation, of th software of the CA or a Subscriber;
- any damage caused by any information published in a certificate or the reason not attributable to the CA;
- any or all damage incurred by a failure in normal communication cause reason not attributable to the CA;
- any or all damage arising in connection with the use of a certificate, su debts;
- any damage caused by an improvement, beyond expectations at this po the cryptographic algorithm decoding capabilities of hardware or softw
- any or all damage caused by the suspension of the CA's business opera force majeure event, including, but not limited to, any act of God, earth volcanic eruption, fire, tsunami, flood disaster, lightning strike, war, ci or terrorism; or

	備考
nce that the CA	
e to violate the	
s required by	
is required by	
of this CP. If	
Party shall	
mage arising in	
sentations and	
or consequential	
rranties" of this	
se, negligence,	
his/her/its	
's system;	
e hardware or	
e CRL, for any	
sed by any	
uch as business	
and as submood	
aint in time is	
oint in time, in	
vare;	
ations due to a	
hquake,	
ivil commotion	

• any or all damage arising concomitantly with, or in connection with, registration and publication on the CT log server of information necessary for certificate issuance.

#### 9.9 Indemnities

Each Subscriber shall become liable to indemnify and hold harmless the CA or any organizations or other entities related to the CA, upon applying for, receiving, and trusting certificates issued by the CA. The events to be covered by the foregoing liabilities include any loss, damage, lawsuit, mistake, omission, act, delay of, or failure in performance, or any other event that may incur cost burdens of any kind. The Terms and Conditions stipulate a policy on indemnification to Subscribers for damage.

#### 9.10 Term and Termination

#### 9.10.1 Term

This CP shall come into effect upon approval by the CA's Certificate Operation Conference. This CP shall not lose its effect under any circumstances before its termination stipulated in "9.10.2 Termination" herein.

#### 9.10.2 Termination

This CP shall lose its effect upon termination of the CA, except as provided in "9.10.3 Effect of Termination and Survival" herein.

#### 9.10.3 Effect of Termination and Survival

Even in the event of termination of an agreement on use or the like between a Subscriber and the CA, or termination of the CA itself, any provisions of this CP that should survive such termination, by the nature thereof, shall continue to apply to Subscribers, Relying Parties, and the CA, regardless of the reason of such termination.

## 9.11 Individual Notices and Communications with Participants

JPRS shall provide necessary notices to Subscribers and Relying Parties on its Web site, by e-mail, in writing, or by other means.

#### 9.12 Amendments

#### 9.12.1 Procedure for Amendment

This CP may be revised at the discretion of the CA, as appropriate, and the revised version hereof shall come into effect upon approval of the CA's Certificate Operation Conference.

#### 9.12.2 Notification Mechanism and Period

If the CA amends this CP, the CA shall promptly publish the amended version of this CP, which shall be deemed to be a notification thereof to Subscribers.

#### 9.12.3 Circumstances under Which OID Must Be Changed

No stipulation.

• any or all damage arising concomitantly with, or in connection with, republication on the CT log server of information necessary for certificate

整形版

### 9.9 Indemnities

Each Subscriber shall become liable to indemnify and hold harmless t organizations or other entities related to the CA, upon applying for, receivin certificates issued by the CA. The events to be covered by the foregoing lia any loss, damage, lawsuit, mistake, omission, act, delay of, or failure in perfo other event that may incur cost burdens of any kind. The Terms and Conditi policy on indemnification to Subscribers for damage.

#### 9.10 Term and Termination

#### 9.10.1 Term

This CP shall come into effect upon approval by the CA's Certificate Operation This CP shall not lose its effect under any circumstances before its termination in "9.10.2 Termination" herein.

#### 9.10.2 Termination

This CP shall lose its effect upon termination of the CA, except as provided in of Termination and Survival" herein.

#### 9.10.3 Effect of Termination and Survival

Even in the event of termination of an agreement on use or the like betwee and the CA, or termination of the CA itself, any provisions of this CP that such termination, by the nature thereof, shall continue to apply to Subsc Parties, and the CA, regardless of the reason of such termination.

## 9.11 Individual Notices and Communications with Partic

JPRS shall provide necessary notices to Subscribers and Relying Parties on e-mail, in writing, or by other means.

#### 9.12 Amendments

#### 9.12.1 Procedure for Amendment

This CP may be revised at the discretion of the CA, as appropriate, and the hereof shall come into effect upon approval of the CA's Certificate Operation

#### 9.12.2 Notification Mechanism and Period

If the CA amends this CP, the CA shall promptly publish the amended version which shall be deemed to be a notification thereof to Subscribers.

## **9.12.3 Circumstances under Which OID Must Be Changed** No stipulation.

	備考
egistration and	011
e issuance.	
is issuance.	
the CA or any	
ng, and trusting	
abilities include	
ormance, or any	
cions stipulate a	
tion Conference.	
ation stipulated	
in "9.10.3 Effect	
en a Subscriber	
should survive	
cribers, Relying	
cipants	
its Web site, by	
revised version	
Conference.	
sion of this CP,	

#### 9.13 Dispute Resolution Provisions

If any party, for the purpose of resolving a dispute over the use of a certificate, seeks to file a lawsuit, refer the dispute to arbitration, or take any other legal action against the CA, such party shall notify the CA to that effect in advance. The Tokyo District Court shall have the agreed exclusive jurisdiction over all disputes involving the Services in the first instance.

## 9.14 Governing Law

Regardless of the respective addresses of the CA and Subscribers, the laws of Japan shall apply to any dispute over the interpretation or validity of this CP, or the use of a certificate.

### 9.15 Compliance with Applicable Laws

The CA SHALL issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates.

### 9.16 Miscellaneous Provisions

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which the CA operates or issues certificates, the CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA's CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to the CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

**9.17 Other Provisions** Not applicable.

#### 整形版

#### 9.13 Dispute Resolution Provisions

If any party, for the purpose of resolving a dispute over the use of a certificate, seeks to file a lawsuit, refer the dispute to arbitration, or take any other legal action against the CA, such party shall notify the CA to that effect in advance. The Tokyo District Court shall have the agreed exclusive jurisdiction over all disputes involving the Services in the first instance.

## 9.14 Governing Law

Regardless of the respective addresses of the CA and Subscribers, the laws of Japan shall apply to any dispute over the interpretation or validity of this CP, or the use of a certificate.

## 9.15 Compliance with Applicable Laws

The CA SHALL issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates.

## 9.16 Miscellaneous Provisions

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which the CA operates or issues certificates, the CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA's CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to the CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

**9.17 Other Provisions** Not applicable.

## 備考

ĺ		
	変更履歴あり	整形版

備考