

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

		変更履歴あり			整形版	備考
Version History					Version History	
Version Number	Date	Description	Version Number	Date	Description	
1.00	2019.06.17	Publication of the first version	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	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 an administrator"			additional information of "general e-mail address indicating an administrator"	
1.20	2020.04.01	Revision due to Mozilla Root Store Policy (v2.7)	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"	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"	2.00	2020.07.22	Revision of "7. Certificate, CRL, and OCSP Profiles"	
2.10	2020.08.20	Revision of the maximum validity period of certificate	2.10	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"	2.20	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	2.21	2021.04.01	Revision of the date and version	
2.22	2021.04.28	Revision due to Mozilla Root Store Policy (v2.7.1)	2.22	2021.04.28	Revision due to Mozilla Root Store Policy (v2.7.1)	
2.23	2021.05.27	 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". 	2.23	2021.05.27	 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	Revision of "3.2.2.4.18 Agreed-Upon Change to Website v2"	2.30	2021.11.18	• Revision of "3.2.2.4.18 Agreed-Upon Change to Website v2"	
		Sunset of "subject:organizationalUnitName"			Sunset of "subject:organizationalUnitName"	
3.00	2021.12.08	Revisions due to new service provision	3.00	2021.12.08	\cdot Revisions due to new service provision	
3.10	2022.03.02	\cdot Add a reference to the new terms and conditions	3.10	2022.03.02	\cdot Add a reference to the new terms and conditions	
3.11	2022.04.01	\cdot Revision of the date and version	3.11	2022.04.01	\cdot Revision of the date and version	
3.20	2022.09.30	Revision of "6.3 Other Aspects of Key Pair Management"	3.20	2022.09.30	• Revision of "6.3 Other Aspects of Key Pair Management"	
		\cdot Add description of Revocation Reason Code to be applied in this CA.			\cdot Add description of Revocation Reason Code to be applied in this CA.	
3.30	2023.04.24	\cdot Revision of the maximum validity period of certificate	3.30	2023.04.24	\cdot Revision of the maximum validity period of certificate	
3.40	2023.06.08	Revision of "1.1 Overview"	3.40	2023.06.08	Revision of "1.1 Overview"	
		Revision of "7.3 OCSP Profile"			· Revision of "7.3 OCSP Profile"	
3.50	2023.08.28	Revision of description to clarify compliance with Baseline Requirements	3.50	2023.08.28	Revision of description to clarify compliance with Baseline Requirements	
3.60	2024.02.22	Revision of "7. Certificate, CRL, and OCSP Profiles"	3.60	2024.02.22	Revision of "7. Certificate, CRL, and OCSP 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 "4.2.4 Check of CAA Records"	3.71	2024.06.05	Revision of "1.6 Definitions and Acronyms" and "4.2.4 Check of CAA Records"	
3.72	2024.08.26	Revision of "4.2.1 Performing Identification and Authentication Functions"	3.72	2024.08.26	Revision of "4.2.1 Performing Identification and Authentication Functions"	
<u>3.73</u>	2024.11.07	Revision of " 4.3.1 CA Actions during Certificate Issuance", " 4.9.1 Circumstances	3.73	2024.11.07	Revision of " 4.3.1 CA Actions during Certificate Issuance", " 4.9.1 Circumstances	改訂履歴の追記
		for Certificate Revocation" and "8.4 Topics Covered by Assessment"			for Certificate Revocation" and "8.4 Topics Covered by Assessment"	

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.

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

整形版

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.

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
	TLS Server Certificate		Issuance and Management of Pu
			- Trusted TLS Server Certificat
		•	Apple Root Certificate Program
		•	Chrome Root Program Policy
		•	Microsoft Trusted Root Program
		•	Mozilla Root Store Policy

ublicly	
tes	
l	
n	

備考

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 operation, this CP shall be revised, as needed, in order to reflect such developments 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

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 to 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> and 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 (inclulimited to, this CP, the CPS, the Terms and Conditions, and the related do Baseline Requirements, Baseline Requirements take precedence over these do

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 a operation, this CP shall be revised, as needed, in order to reflect such de 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") assign 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.
JPRS CA Certification Practice Statement (CPS)	1.3.6.1.4.1.53827

1.3 PKI Participants

1.3.1 CA

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

1.3.2 RA

"RA" stands for "Registration Authority," an entity that mainly performs re the existence and validate the identities of applicants who apply for th revocation of certificates, registers information necessary for issuing ce

	備考
and Conditions, those of this CP PS. Also, if any nd the English on. In the event luding, but not locuments) and documents.	
ture Certificate framework for	
technologies or evelopments or	
gned by the CA	
.1.1.4	
7.1.2.4	
s and revokes	
mation on the	
; generates and	
eviews to verify	
he issuance or	
ertificates, and	

変更履歴あり	整形版	備考
requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.	requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.	
1.3.3 Subscribers	1.3.3 Subscribers	
"Subscribers" means an individual, corporation, or organization that has been issued a	"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	certificate by the CA and uses the certificate. "Subscriber Certificate" means the certificate	
issued by the CA to the Subscribers.	issued by the CA to the Subscribers.	
1.3.4 Relying Parties	1.3.4 Relying Parties	
A "Relying Party" means an individual, corporation, or organization that verifies the	A "Relying Party" means an individual, corporation, or organization that verifies the	
validity of certificates issued by the CA.	validity of certificates issued by the CA.	
1.3.5 Other Participants	1.3.5 Other Participants	
No stipulation.	No stipulation.	
1.4 Certificate Usage	1.4 Certificate Usage	
1.4.1 Appropriate Certificate Uses	1.4.1 Appropriate Certificate Uses	
Certificates issued by the CA are used to encrypt information for server authentication and	Certificates issued by the CA are used to encrypt information for server authentication and	
on communication pathways.	on communication pathways.	
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	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/	<u>https://jprs.jp/pubcert/f_mail/</u>	
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

ACME (Automated Certificate Management Environment)

"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 issuance. This Protocol is specified in RFC 8555.

Archive

"Archive" means information acquired for the purpose of keeping a history for any legal or other reason.

Audit Log

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 unauthorized operations of, Certification Authority systems.

Authorization Domain Name

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)

CAA (Certificate Authority Authorization)

"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.

<u>Authority</u> <u>CA (Certification Authority)</u> <u>CA (Certification Authority)</u> <u>CA (Certification Authority)</u> <u>CA (Certification Authority)</u>

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 to prevent "CAA" stands for "Certificate Authority Authorization," a functi

整形版

1.6 Definitions and Acronyms

ACME (Automated Certificate Management Environment)

"ACME" stands for "Automated Certificate Management Environment", a CA and an applicant can use to automate the process of verification issuance. This Protocol is specified in RFC 8555.

Archive

"Archive" means information acquired for the purpose of keeping a histo or other reason.

<u>Audit Log</u>

An "Audit Log" is a log of actions, accesses, and other histories pertaining Authority systems that are recorded for the purpose of monitoring ac unauthorized operations of, Certification Authority systems.

Authorization Domain Name

The Domain Name used to obtain authorization for certificate issuance for The CA may use the FQDN returned from a DNS CNAME lookup as the purposes of domain validation. If the FQDN contains a wildcard character MUST remove all wildcard labels from the left most portion of requested I 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.

	備考
, a protocol that and certificate	
ory for any legal	
to Certification	
r a given FQDN. e FQDN for the cer, 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	

整形版

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.

CP (Certificate Policy)

"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)

"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.

ECDSA (Elliptic Curve Digital Signature Algorithm)

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

<u>Escrow</u>

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

unintended erroneous issuance of certificates from unauthorized Certificat in connection with the authority to use a domain by adding information to t in order to specify the Certification Authority authorized to issue a cer 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 set 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)

"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) if 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.

ECDSA (Elliptic Curve Digital Signature Algorithm)

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

<u>Escrow</u>

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

	備考
tion Authorities	כ מוע
the DNS record	
rtificate for the	
tilleate for the	
• • • • • • • • • • • • • • • • • • • •	
icies regarding	
ervers for which	
pplying for the	
that sets forth	
procedures and	
out certificates	
changes in the	
Keys.	
6962 to register	
for the purpose	
ossessed by the	
red by a digital	
widely used as	
control of an	
control of all	

<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 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

<u>A process in which the content of digitally signed data such as a Precertificate [RFC 6962]</u>, 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.

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)

"OIDs" stands for "Object Identifiers," numerals registered in international registration institutions as unique IDs among global networks within a framework for maintaining

<u>FIPS 140-2</u>

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

整形版

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 of maintaining security.

JPRS Partners

"JPRS Partners" mean business enterprises authorized by JPRS in connu 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 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

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>

"OIDs" stands for "Object Identifiers," numerals registered in internation institutions as unique IDs among global networks within a framework for

	ملد مللخ
	備考
raphic modules nd Technology). efined.	
in the Internet	
yption device to for the purpose	
nection with the	
in a public key	
ertificate [RFC ata-to-be-signed) is checked for nents.	用語定義の追加
ynchronize the	
for providing	
nal registration	
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.

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.

Repository

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 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.

整形版

and administering the connectivity of networks and the uniqueness of serv

<u>PKI (Public Key Infrastructure)</u>

"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.

Private Key

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."

Public Key

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 perforverify the existence and validate the identities of applicants who apply for revocation of certificates, registers information necessary for issuing c 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

<u>Repository</u>

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

RFC 3647 (Request for Comments 3647)

"RFC 3647" stands for "Request for Comments 3647," a document framework for CP and CPS published by the IETF (Internet Engineering 7 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.

	備考
vices or the like.	U田 ペマ
g the encryption nologies such as	
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 Task Force), an	
ning the public ce), an industry	

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

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

整形版

<u>RSA</u>

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

<u>SHA-1 (Secure Hash Algorithm 1)</u>

"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 bit 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 h (summarization functions) used in digital signing. The bit length is two hu (256) bits. The algorithm works to detect any alterations in an original mes 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 Subju-Names in the Certificate.

Wildcard Domain Name

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

2. Publication and Repository Responsibilit

2.1 Repository

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

2.2 Publication of Information

	備考
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	
me twenty-four wever, that the nance or other	

The CA shall publish the CRLs, this CP, and the CPS on the Repository to allow online That 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

The Distinguished Name (DN) format of the X.500 series shall stipulate 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 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 th revised. The CA describes to the CP and the CPS in detail how the CA implemversion 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 Television 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 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 property right to the The CA does not verify whether an applicant holds any intellectual property

to allow online	備考
ne Repository as ments the latest	
ublished on the	
Relying Parties a general Web	
the CA shall be e X.500 series ecommunication	
communication	
ngs are specified	
be issued by the	
te the rules for	
to be issued by	
S	
rty 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

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

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;

Subsequent sections 3.2.2.4.1-20 correspond to the section numbers of the methods specified 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

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 of 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 signed verifying Request (hereinafter referred to as "CSR") and of 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 c the same manner as set forth in "3.2.2.1 Authentication of Organization Iden

3.2.2.4 Validation of Domain Authorization or Control

The CA SHALL confirm that prior to issuance, the CA has validated each FG 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 me by BR.

Jame" is | The CA doesn't issue certificates if "RFC 7686 - The ".onion" Special-Use Dom

	備考
t to the CA a	
any third party.	
nection with a	
te or settle the	
or to revoke an	
gnature on the	
confirming that	
ley contained in	
or alteration or	
ts issued by, or	
entity, or using	
atabases of any	
' in a certificate	
as set forth in	
certificate to in	
ntity."	
QDN listed in	
ethods specified	
main Name" is	

included in the certificates.

The CA SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Not applicable

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 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.

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 remain valid for use in a confirming response for no more than 25 days from its creation.

3.2.2.4.3 Phone Contact with Domain Contact

Not applicable

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by

- Sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign (""@""), followed by the Authorization Domain Name; and
- 2. including a Random Value in the email; and
- 3. receiving a confirming response utilizing the Random Value.

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 creation.

3.2.2.4.5 Domain Authorization Document

Not applicable

3.2.2.4.6 Agreed-Upon Change to Website

Not applicable

3.2.2.4.7 DNS Change

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.

3.2.2.4.8 IP Address

Not applicable

included in the certificates.

The CA SHALL maintain a record of which domain validation method, includ BR version number, they used to validate every domain.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Not applicable

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 Rame email and then receiving a confirming response utilizing the Randor Random Value MUST be sent to an email address listed in the WHOIS The CA does not use fax, SMS, or postal mail to send a Random Value The Random Value SHALL be unique in each email. The Random remain valid for use in a confirming response for no more than 25 creation.

3.2.2.4.3 Phone Contact with Domain Contact

Not applicable

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the FQDN by

- Sending an email to one or more addresses created by 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as followed by the at-sign (""@""), followed by the Authorization and
- 2. including a Random Value in the email; and
- 3. receiving a confirming response utilizing the Random Value.

The Random Value SHALL be unique in each email. The Random remain valid for use in a confirming response for no more than 25 creation.

3.2.2.4.5 Domain Authorization Document

Not applicable

3.2.2.4.6 Agreed-Upon Change to Website

Not applicable

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the 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 for 25 days from its creation.

3.2.2.4.8 IP Address

Not applicable

13/59

	備考
ıding relevant	
ndom Value via dom Value. The S record. es. n Value SHALL 5 days from its	
using 'admin', the local part, Domain Name;	
n Value SHALL 5 days from its	
ne presence of a n Name that is	
e request. The or no more than	

変更履歴あり	整形版
3.2.2.4.9 Test Certificate	3.2.2.4.9 Test Certificate
Not applicable	Not applicable
3.2.2.4.10 TLS Using a Random Value	3.2.2.4.10 TLS Using a Random Value
Not applicable	Not applicable
3.2.2.4.11 Any Other Method	3.2.2.4.11 Any Other Method
Not applicable	Not applicable
3.2.2.4.12 Validating Applicant as a Domain Contact	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	Confirming the Applicant's control over the FQDN by validating the Ap
registrant of the domain name. This method may only be used if the CA is also the	registrant of the domain name. This method may only be used if the O
Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.	Domain Name Registrar, or an Affiliate of the Registrar, of the Base Dom
3.2.2.4.13 Email to DNS CAA Contact	3.2.2.4.13 Email to DNS CAA Contact
Not applicable	Not applicable
3.2.2.4.14 Email to DNS TXT Contact	3.2.2.4.14 Email to DNS TXT Contact
Not applicable	Not applicable
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 us
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" directed
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.
• Redirects MUST be the result of a 301, 302, or 307 HTTP status code	• Redirects MUST be the result of a 301, 302, or 307 HTT
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.
• Redirects MUST be to the final value of the Location HTTP response	• 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.

	備考
the Applicant is the if the CA is also the ase Domain Name.	
g that the Random	
uest used to retrieve	
he request (meaning	
d directory, and e, and	
7 HTTP status code a 308 HTTP status	
ion HTTP response	

- 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).

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.

For Certificates issued on or after 2021-11-18, this method is not applicable for validating Wildcard Domain Names.

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.

3.2.2.4.20 TLS Using ALPN

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 Certificate is "registry-controlled" or is a "public suffix" (e.g. "*.com", "*.co.uk", see RFC

2. Redirects MUST be to resource URLs with either the "h scheme.

3. Redirects MUST be to resource URLs accessed via port 80 (https).

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.

For Certificates issued on or after 2021-11-18, this method is not validating Wildcard Domain Names.

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 "I scheme.
- 3. Redirects MUST be to resource URLs accessed via port 8 (https).

This method is not applicable for validating Wildcard Domain Names.

- 3.2.2.4.20 TLS Using ALPN
- 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 Certificate is "registry-controlled" or is a "public suffix" (e.g. "*.com", "*.co

	備考
uttp" or "https"	
0 (http) or 443	
e request. The or no more than	
applicable for	
applicable for	
in control of the 8.3 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. nttp" or "https"	
30 (http) or 443	
5.	
a documented	
n Name in the	
o.uk", see RFC	

変更履歴あり	整形版	備考
6454 Section 8.2 for further explanation).	6454 Section 8.2 for further explanation).	
If the FQDN portion of any Wildcard Domain Name is "registry-controlled" or is a "public	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	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	entire Domain Namespace. (e.g. CAs MUST NOT issue "*.co.uk" or "*.local", but MAY issue	
"*.example.com" to Example Co.).	"*.example.com" to Example Co.).	
Determination of what is "registry-controlled" versus the registerable portion of a Country	Determination of what is "registry-controlled" versus the registerable portion of a Country	
Code Top-Level Domain Namespace is accordance with Baseline Requirements.	Code Top-Level Domain Namespace is accordance with Baseline Requirements.	
3.2.2.7 Data Source Accuracy	3.2.2.7 Data Source Accuracy	
Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the	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	source for its reliability, accuracy, and resistance to alteration or falsification. The CA	
considers the following during its evaluation:	considers the following during its evaluation:	
1. The age of the information provided,	1. The age of the information provided,	
2. The frequency of updates to the information source,	2. The frequency of updates to the information source,	
3. The data provider and purpose of the data collection,	3. The data provider and purpose of the data collection,	
4. The public accessibility of the data availability, and	4. The public accessibility of the data availability, and	
5. The relative difficulty in falsifying or altering the data.	5. The relative difficulty in falsifying or altering the data.	
3.2.2.8 CAA Records	3.2.2.8 CAA Records	
As part of the Certificate issuance process, the CA MUST retrieve and process 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.	the CAA record, or 8 hours, whichever is greater.	
When processing CAA records, the CA MUST process the issue, issuewild, and iodef	When processing CAA records, the CA MUST process the issue, issuewild, and iodef	
property tags as specified in RFC 8659, although the CA does not act on the contents of the	property tags as specified in RFC 8659, although the CA does not act on the contents of the	
iodef property tag. Where are additional property tags are supported, the CA MUST NOT	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.	conflict with or supersede the mandatory property tags set out in Baseline Requirements.	
The CA MUST respect the critical flag and not issue a certificate if they encounter an	The CA MUST respect the critical flag and not issue a certificate if they encounter an	
unrecognized property tag with this flag set.	unrecognized property tag with this flag set.	
The CA permitted to treat a record lookup failure as permission to issue if:	The CA permitted to treat a record lookup failure as permission to issue if:	
- the failure is outside the CA's infrastructure; and	- the failure is outside the CA's infrastructure; and	
- the lookup has been retried at least once; and	- the lookup has been retried at least once; and	
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.	- the domain's zone does not have a DNSSEC validation chain to the ICANN root.	

The CA shall log any actions taken as part of its processing practices.

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

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.

整形版

The CA shall log any actions taken as part of its processing practices.

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 red domain name to be described in the certificate or has been granted an exclusion the 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

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 Subscribt 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 cl following;

- 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 Requeprivate key of the account granted to the subscriber.
- 3. The certificate issued under ACME protocol and the Revocation Requiprivate key of the certificate.

	備考
egistrant of the	
sive right to use	
thority to apply	
verified by any	
entication of an	
CA by Security	
COM TLS RSA	
ts	
per at a rekey in	
quest	
check one of the	
nated Business	
issuance of the	
lest is signed by	
uest is signed by	

変更履歴あり	整形版
4. Certificate Life-Cycle Operational Requirements	4. Certificate Life-Cycle Operational Requirements
4.1 Certificate Application	4.1 Certificate Application
4.1.1 Who Can Submit a Certificate Application	4.1.1 Who Can Submit a Certificate Application
(1) Domain Validation	(1) Domain Validation
A person who is a registrant of the domain name to be described in a certificate or has been	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	granted an exclusive right to use the domain name by the registrant may apply for the
certificate.	certificate.
(2) Organization Validation	(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.	unincorporated, may apply for the certificate.
4.1.2 Enrollment Process and Responsibilities	4.1.2 Enrollment Process and Responsibilities
Each person who may apply for a certificate and intends to do so shall apply for the	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	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.	the Certificate Application submitted to the CA is accurate.
4.2 Certificate Application Processing	4.2 Certificate Application Processing
4.2.1 Performing Identification and Authentication Functions	4.2.1 Performing Identification and Authentication Functions
The CA shall review application information by considering the information in the manner	The CA shall review application information by considering the information in the manner
set forth in "3.2 Initial Identity Validation" of this CP.	set forth in "3.2 Initial Identity Validation" of this CP.
The certificate request MAY include all factual information about the Applicant to be	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	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	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.	the Certificate by the Applicant.
Applicant information MUST include, but not be limited to, at least one Fully-Qualified	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.	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.	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	The CA MAY use the documents and data provided in Section 3.2 of this CP to verify

変更履歴あり	整形版	備考
certificate information, or may reuse previous validations themselves, provided that the CA	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	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.	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,	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.	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	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	validation was obtained more than the maximum time permitted for reuse of the data or	
locument prior to issuing the Certificate.	document prior to issuing the Certificate.	
After the change to any validation method specified in the Baseline Requirements, the CA	After the change to any validation method specified in the Baseline Requirements, the CA	
nay continue to reuse validation data or documents collected prior to the change, or the	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 n a ballot.	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	The CA SHALL develop, maintain, and implement documented procedures that identify	
and require additional verification activity for High Risk Certificate Requests prior to the	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	Certificate's approval, as reasonably necessary to ensure that such requests are properly	
verified under these Requirements.	verified under these Requirements.	
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	
he issuance registration of the certificate.	the issuance registration of the certificate.	
f 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	
he 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		
he 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	In reviewing the application information, the CA shall check the CAA records in accordance	
with RFC 8659. The domain of the CA to be described in the CAA records shall be "jprs.jp."	with RFC 8659. The domain of the CA to be described in the CAA records shall be "jprs.jp."	
	The Certificate Subscribers who want to grant the authority to issue certificates to the	
FQDN must include the value of "jprs.jp" in the property "issue" of the CAA record for each		
DNS zone.	DNS zone.	
4.3 Certificate Issuance	4.3 Certificate Issuance	

4.3.1 CA Actions during Certificate Issuance

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 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.

4.3.1.1 Manual authorization of certificate issuance for Root CAs

No stipulation.

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.

4.3.1.3 Linting of issued Certificates

The CA MAY use a Linting process to test each issued Certificate.

4.3.2 Notification to Subscriber of Certificate Issuance

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

整形版

4.3.1 CA Actions during Certificate Issuance

After completing a review of a certificate application, the CA shall register in is based on the application information and necessary for the issuance of a c CT log server operated by a third party and prescribed by the CA, and certificate. The information to be registered on the CT log server shall be a "7.1 Certificate Profile" of this CP.

4.3.1.1 Manual authorization of certificate issuance for Root CA No stipulation.

4.3.1.2 Linting of to-be-signed Certificate content

The CA confirms whether the certificate to be issued technically conform Requirements for some items by the pre-certificate linting function and refuse does not meet the requirements.

4.3.1.3 Linting of issued Certificates

The CA MAY use a Linting process to test each issued Certificate.

4.3.2 Notification to Subscriber of Certificate Issuance

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 subscriber page 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 of 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 Enterissuance of certificates.

4.5 Key Pair and Certificate Usage

	備考
nformation that certificate, on a then issue the as described in	
IS	Baseline Requirementsへの準 拠を明確にするための追記
ms to Baseline ses to issue if it	
an e-mail to the te issued under	
e following time; criber-only web	
protocol and the d under ACME	
ther than 1 and	
• Entities terprises) of the	

変更履歴あり	整形版	備考
4.5.1 Subscriber Private Key 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	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.	communication pathways, and not for any other usage.	
4.5.2 Relying Party Public Key and Certificate 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	
ane CPS before verifying the reliability of certificates issued by the CA and relying on the	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	4.6 Certificate Renewal A "certificate renewal" means the issuance of a new certificate to a Subscriber without any	
hange 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.	CA recommends that the Subscriber generate a new Key Pair.	
4.6.1 Circumstances for Certificate Renewal	4.6.1 Circumstances for Certificate Renewal	
A certificate may be renewed without involving rekey when the certificate is about to expire.	A certificate may be renewed without involving rekey when the certificate is about to expire.	
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	
correspondingly.	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	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall	
pply correspondingly.	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 correspondingly.	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	The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply	
correspondingly.	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	The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of	
this CP shall apply correspondingly.	this CP shall apply correspondingly.	

変更履歴あり	整形版	備考
4.7 Certificate Re-key A "certificate re-key" means the issuance of a new certificate to a Subscriber after generating a new Key Pair.	4.7 Certificate Re-key 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 expire.	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	
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.	
4.7.3 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 correspondingly.	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.	
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate	4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate	
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 CP shall apply 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 CP shall apply 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 Entities	
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 Other Entities" of 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 (excluding the common 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 CP shall apply 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	The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply	

変更履歴あり	整形版	
correspondingly.	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	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall	
apply correspondingly.	apply correspondingly.	
4.8.5 Conduct Constituting Acceptance of Modified Certificate	4.8.5 Conduct Constituting Acceptance of Modified Certificate	
The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply	The provisions of "4.4.1 Conduct Constituting Certificate Acceptance" of this CP shall apply	
correspondingly.	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	The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply	
correspondingly.	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 Entities	
The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of	The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of	
this CP shall apply correspondingly.	this CP shall apply correspondingly.	
4.9 Certificate Revocation and Suspension	4.9 Certificate Revocation and Suspension	
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 CA to have 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, including theft, loss,	
leakage, or unauthorized use thereof;any of the particulars described in the certificate or its purposes of use are incorrect;	leakage, or unauthorized use thereof;any of the particulars described in the certificate or its purposes of use are incorrect;	
 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, or is included 	
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 "3.1.1 Types of	
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 corresponding CRLReason	
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 CRLreason, that the CA	1. The Subscriber requests in writing, without specifying a CRLreason, that the CA	
revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode	revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode	
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 was not	
authorized and does not retroactively grant authorization (CRLReason #9,	authorized and does not retroactively grant authorization (CRLReason #9,	
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 corresponding to the	

Public Key in the Certificate suffered a Key Compromise (CRLReason #1, keyCompromise);

- 4. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate <u>, including</u> <u>but not limited to those identified in the Baseline Requirements Section 6.1.1.3(5),</u> <u>CPS "6.1.1 Key Pair Generation"(such as a Debian weak key,</u> <u>see https://wiki.debian.org/SSLkeys)</u> (CRLReason #1, keyCompromise);
- 5. The CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).

The CA SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days and use the corresponding CRLReason if one or more of the following occurs:

- 6. The Certificate no longer complies with the requirements of <u>Section</u>
 <u>6.1.5</u> and <u>Section 6.1.6</u> of Baseline Requirements (CRLReason #4, superseded);
- The CA obtains evidence that the Certificate was misused (CRLReason #9, privilegeWithdrawn);
- 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

整形版

Public Key in the Certificate suffered a Key Compromise (CRLReaso keyCompromise);

- 4. The CA is made aware of a demonstrated or proven method that can of the Subscriber's Private Key based on the Public Key in the Certificat but not limited to those identified in the Baseline Requirements Section CPS "6.1.1 Key Pair Generation" (CRLReason #1, keyCompromise);
- 5. The CA obtains evidence that the validation of domain authorization any Fully-Qualified Domain Name or IP address in the Certificate sh relied upon (CRLReason #4, superseded).

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 fol

- The Certificate no longer complies with the requirements of <u>Section</u>
 <u>6.1.5</u> and <u>Section 6.1.6</u> of Baseline Requirements (CRLReason #4, sup
- 7. The CA obtains evidence that the Certificate was misused (CRLReas privilegeWithdrawn);
- 8. The CA is made aware that a Subscriber has violated one or more of a obligations under the Subscriber Agreement or Terms of Use (CRLRe privilegeWithdrawn);
- 9. The CA is made aware of any circumstance indicating that use of a F 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 C(RLReason #5, cessationOfOperation);
- 10. The CA is made aware that a Wildcard Certificate has been used to a fraudulently misleading subordinate FQDN (CRLReason #9, privilegenergy).
- 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 accordan 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 cont maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)"

	備考
on #1,	
easily compute	
ate , including	Baseline Requirementsへの準
tion 6.1.1.3(5),	拠を明確にするための追記
or control for	
nould not be	
xe a Certificate	
llowing occurs:	
perseded);	
son #9,	
its material	
eason #9,	
QDN in the	
as revoked a	
it licensing or	
pplicant has	
Domain Name)	
.1	
authenticate a	
geWithdrawn);	
ined in the	
nce with these	
pearing in the	
· · · ·	
pires or is	
ntinue " which results	
winch 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 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

整形版

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 follor 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 compromised, he/she/it must promptly file the Revocation Request of the cert The CA SHALL maintain a continuous 24x7 ability to accept and respond requests and Certificate Problem Reports.

4.9.5 Time within Which the CA Shall Process the Revocation

Upon accepting a valid Revocation Request of a certificate, the CA shall protected the Revocation Request and reflect the relevant information in the certificate Within 24 hours after receiving a Certificate Problem Report, the CA SHA the facts and circumstances related to a Certificate Problem Report a preliminary report on its findings to both the Subscriber and the entity Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the any entity reporting the Certificate Problem Report or other revocation-reestablish whether or not the certificate will be revoked, and if so, a date where we certificate. The period from receipt of the Certificate Problem Report or other certificate to published revocation MUST NOT exceed the terms of terms of the terms of the terms of terms

	備考
tion Practice	
by this section	
h results in no	
oses the	
hat the specific	
,	
application for	
application for	
owing way, and	
4.	
been or may be	
tificate.	
d to revocation	
on Request	
comptly process	
e on the CRL.	
ALL investigate	
and provide a	
who filed the	
Subscriber and	
elated notice to	
nich the CA will	
lem Report or	
time frame set	

変更履歴あり	整形版	備考
forth in Section 4.9.1.1 of this CP.	forth in Section 4.9.1.1 of this CP.	
4.9.6 Revocation Checking Requirement for Relying Parties	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.	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	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	verify the validity of the certificate by checking the CRL. CRLs do not contain information	
on certificates that have expired.	on certificates that have expired.	
4.9.7 CRL Issuance Frequency	4.9.7 CRL Issuance Frequency	
The CA SHALL update and reissue CRLs at least once every seven days, and the value of	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	the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate	
field.	field.	
4.9.8 Maximum Latency for CRLs	4.9.8 Maximum Latency for CRLs	
The CA shall forthwith reflect an issued CRL in the Repository.	The CA shall forthwith reflect an issued CRL in the Repository.	
4.9.9 On-line Revocation/Status Checking Availability	4.9.9 On-line Revocation/Status Checking Availability	
Information on the certificate status shall be provided online via the OCSP server.	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	OCSP responses MUST conform to RFC 6960 and/or RFC 5019. OCSP responses MUST	
either:	either:	
1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or	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.	2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.	
the Certificate whose revocation status is being thetked.	the Certificate whose revocation status is being checked.	
In the latter case, the OCSP signing Certificate MUST contain an extension of	In the latter case, the OCSP signing Certificate MUST contain an extension of	
type id-pkix-ocsp-nocheck, as defined by RFC 6960.	type id-pkix-ocsp-nocheck, as defined by RFC 6960.	
4.9.10 On-line Revocation/Status Checking Requirements	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	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	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	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	Repository, the Relying Party shall check the information on the certificate status provided	
through the OCSP server.	through the OCSP server.	
OCSP responders operated by the CA SHALL support the HTTP GET method, as described	OCSP responders operated by the CA SHALL support the HTTP GET method, as described	
in RFC 6960 and/or RFC 5019.	in RFC 6960 and/or RFC 5019.	
The validity interval of an OCSP response is the difference in time between	The validity interval of an OCSP response is the difference in time between	
the this $Update\ and\ next Update\ field,\ inclusive.$ For purposes of computing differences,	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	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.	shall be equal to one day, ignoring leap-seconds.	
For the status of Subscriber Certificates:	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</u> 7.1.2.3 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.

The OCSP responder MAY provide definitive responses about "reserved" certificate serial numbers, as if there was a corresponding Certificate that matches the Precertificate [RFC 6962].

A certificate serial number within an OCSP request is one of the following three options:

- "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
- "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>Section</u>
 <u>7.1.2.4</u>, associated with the Issuing CA; or
- 3. "unused" if neither of the previous conditions are met.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

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:

https://jprs.jp/pubcert/f_mail/

Please include either of the following information in your report.

- The compromised private key itself
- A CSR signed by the compromised private key

- 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, t SHALL update the information provided via an Online Certificate Sta prior to one-half of the validity period before the nextUpdate.
- 4. For OCSP responses with validity intervals greater than or equal to s then the CA SHALL update the information provided via an Online O Status Protocol at least eight hours prior to the nextUpdate, and no la 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" a requests.

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

The OCSP responder MAY provide definitive responses about "reserved" centre numbers, as if there was a corresponding Certificate that matches the Prece 6962].

A certificate serial number within an OCSP request is one of the following th

- 1. "assigned" if a Certificate with that serial number has been issued by CA, using any current or previous key associated with that CA subject
- "reserved" if a Precertificate [RFC 6962] with that serial number has

 a. the Issuing CA; or b. a Precertificate Signing Certificate, as defined
 <u>7.1.2.4</u>, associated with the Issuing CA; or
- 3. "unused" if neither of the previous conditions are met.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Regarding Key Compromise

If a compromise of any Private Key pertaining to a certificate issued by the please notify via the following webform:

https://jprs.jp/pubcert/f_mail/

Please include either of the following information in your report.

- The compromised private key itself
- \cdot A CSR signed by the compromised private key

	備考
l to eight hours;	
ten days;	
then the CA	
tatus Protocol	
sixteen hours,	
Certificate	
later than four	
later tilan lour	
number that is	
us. If the OCSP	
ne with <u>Section</u>	
status for such	
rial numbers as	
ertificate serial	
certificate [RFC	
hree options:	
_	
y the Issuing	
ct; or	
s been issued by	
ed in <u>Section</u>	
9	
CA is moved and	
CA is revealed,	

変更履歴あり	整形版	備考
(A CSR must contain a string indicating that a private key has been compromised in the	(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")	"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.	shall revoke the certificate within 24 hours from the time of confirmation.	
4.9.13 Circumstances for Suspension	4.9.13 Circumstances for Suspension	
Not applicable.	Not applicable.	
4.9.14 Who Can Request Suspension	4.9.14 Who Can Request Suspension	
Not applicable.	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	
Subscribers and Relying Parties may check information on the status of a certificate	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	Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the	
Expiry Date of the revoked Certificate.	Expiry Date of the revoked Certificate.	
4.10.2 Service Availability	4.10.2 Service Availability	
The CA shall manage the OCSP server to allow Subscribers and Relying Parties to check	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	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	sixty-five (365) days a year. However, the OCSP server may be temporarily unavailable at	
times for maintenance or other reasons.	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.	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	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.	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	
enforcement 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.	

変更履歴あり	整形版
No stipulation.	No stipulation.
4.11 End of Subscription (Registration)	4.11 End of Subscription (Registration)
f a Subscriber ceases to use his/her/its certificate, or cancels the Services, the Subscriber	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 cerminate.	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.	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.
4.12.2 Session Key Encapsulation and Recovery Policy and Practices	4.12.2 Session Key Encapsulation and Recovery Policy and Practices
Not applicable.	Not applicable.
5. Facility, Management, and Operational Controls	5. Facility, Management, and Operational Controls
5.1 Physical Security Controls	5.1 Physical Security Controls
Stipulated in the CPS.	Stipulated in the CPS.
5.2 Procedural Controls	5.2 Procedural Controls
Stipulated in the CPS.	Stipulated in the CPS.
5.3 Personnel Controls	5.3 Personnel Controls
Stipulated in the CPS.	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
Stipulated 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

変更履歴あり	整形版	備考
Stipulated 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.	Stipulated in the CPS.	
5.4.6 Audit Log Collection System	5.4.6 Audit Log Collection System	
Stipulated in the CPS.	Stipulated in the CPS.	
5.4.7 Notification to Event-Causing Subject	5.4.7 Notification to Event-Causing Subject	
Stipulated in the CPS.	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: this CP; documents prepared under this CP stipulating the business operations of the 	 "5.5 Records Archival" of the CPS: this CP; documents prepared under this CP stipulating the business operations of the 	
Certification Authority;	Certification Authority;	
 records and audit reports on the results of audits; and information on applications from Subscribers and the histories thereof. 	 records and audit reports on the results of audits; and 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) years: this CP; documents prepared under this CP stipulating the business operations of the Certification Authority; records and audit reports on the results of audits; and information on applications from Subscribers and the histories thereof. 	 Stipulated in the CPS. The CA shall archive the following information for at least seven (7) years: this CP; documents prepared under this CP stipulating the business operations of the Certification Authority; records and audit reports on the results of audits; and information on applications from Subscribers and the histories thereof. 	
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	

30/59

Stipulated in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Stipulated in the CPS.

5.6 Key Changeover

Before the validity period of a certificate relevant to the CA's own Private Key becomes 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. Once the new Private Key has been generated, the CA shall issue certificates and CRLs using the new Private Key.

5.7 Compromise and Disaster Recovery

Stipulated in the CPS.

5.8 CA or RA Termination

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 set forth in "9.11 Individual Notices and Communications with Participants."

6. Technical Security Controls

6.1 Key Pair Generation and Installation

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.

6.1.2 Private Key Delivery to Subscriber

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.

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 his/her/its certificate. The communication pathways for such delivery shall be encrypted by the TLS.

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.

6.1.5 Key Sizes

When issuing a TLS server certificate that complies with Baseline Requirements, the following confirmation need to be done:

Stipulated in the CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

Stipulated in the CPS.

5.6 Key Changeover

Before the validity period of a certificate relevant to the CA's own Private shorter than the maximum validity period of certificates issued to Subs Private Key for the CA shall be generated and a certificate relevant thereto s Once the new Private Key has been generated, the CA shall issue certificate using the new Private Key.

5.7 Compromise and Disaster Recovery

Stipulated in the CPS.

5.8 CA or RA Termination

If the CA is required to suspend its operations as a Certification Authority of Authority, the CA shall notify Subscribers to that effect in advance by any of forth in "9.11 Individual Notices and Communications with Participants."

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

"6.1.1 Generation of Key Pairs" of the CPS stipulates a policy on Private Key

6.1.2 Private Key Delivery to Subscriber

Each Subscriber's Private Key shall be generated by the Subscriber himse. The CA does not generate or deliver the Private Keys of Subscribers to Subsc

6.1.3 Public Key Delivery to the Certificate Issuer

A Subscriber shall deliver his/her/its Public Key to the CA online when his/her/its certificate. The communication pathways for such delivery shall b the TLS.

6.1.4 CA' Public Key Delivery to Relying Parties

Relying Parties may obtain Public Keys of the CA by accessing the CA's Repo

6.1.5 Key Sizes

When issuing a TLS server certificate that complies with Baseline Requirem following confirmation need to be done:

	備考
e Key becomes scribers, a new shall be issued. eates and CRLs	
or Registration f the means set	
ys of the CA.	
elf/herself/itself. cribers.	
en applying for be encrypted by	
ository.	
ients, the	

r RSA key pairs the CA SHA	変更履歴な	59			整形	版	備考
i Kon key pans the en sing	LL:		Fo	or RSA key pairs the CA SHA	LL:		
• Ensure that the modulu	ıs size, when encoded	, is at least 2048 bits, and;		• Ensure that the modulu	s size, when encod	ed, is at least 2048 bits, and;	
• Ensure that the module	ıs size, in bits, is even	ly divisible by 8.		• Ensure that the modulu	s size, in bits, is ev	enly divisible by 8.	
r ECDSA key pairs the CA	SHALL:		Fo	or ECDSA key pairs the CA	SHALL:		
		point on the NIST P-256 or NIST P				d point on the NIST P-256 or NIST P-384	
elliptic curve.	1			elliptic curve.	. r		
o other algorithms or key si	zes are permitted.		No	o other algorithms or key siz	zes are permitted.		
.1.6 Public Key Parar	neters Generatio	on and Quality Checking	6	6.1.6 Public Key Paran	neters Generat	tion and Quality Checking	
ipulated in the CPS. No po	olicy is stipulated or	the generation and quality inspection	n of Sti	ipulated in the CPS. No po	licy is stipulated	on the generation and quality inspection of	
e Public Key parameters of	Subscribers.		the	e Public Key parameters of	Subscribers.		
.1.7 Key Usage Purpo	oses		6	6.1.7 Key Usage Purpo	ses		
		ys intended by the CA and by certific				keys intended by the CA and by certificates	
sued by the CA:	usugoo or no			sued by the CA:			
·				·			
	Table 6.1 Key Usa	age Purposes			Table 6.1 Key U	Jsage Purposes	
	the CA	Certificates issued by the			the CA	Certificates issued by the	
		CA				CA	
digitalSignature	—	yes		digitalSignature	—	yes	
nonRepudiation	—	—		nonRepudiation	—	—	
keyEncipherment	—	yes		keyEncipherment	—	yes	
		(except for certificates				(except for certificates	
		issued by using ECDSA				issued by using ECDSA	
		key)				key)	
dataEncipherment	—	—		dataEncipherment	—	—	
keyAgreement	—	—		keyAgreement		—	
	yes			keyCertSign	yes		
keyCertSign	yes	—		cRLSign	yes		
keyCertSign cRLSign	0			encipherOnly		_	
		—		1 0			

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 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.

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 Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking of this CP.

The CA SHALL generate non-sequential Certificate serial numbers greater than zero (0) 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)

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 stipulate Subscriber Certificates issued on or after 1 September 2020 MUST NOT has period greater than 398 days. Subscriber Certificates issued prior to 1 Septem a validity period of 825 days or less.

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

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 - I Information, Section 6.1.5 - Key Sizes, and Section 6.1.6 - Public Key Generation and Quality Checking of this CP.

The CA SHALL generate non-sequential Certificate serial numbers greater 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 in 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)



	進去
	備考
ods	
ed in the CPS.	
ave a validity	
ber 2020 have	
mount of time	
represent an	
Publication of	
y Parameters	
than zero (0)	
ndicated in the	
JPRS Domain	

		変更履歴あり			
Basic field		Description of setting	critical	Basic field	
Version		Version 3	-	Version	
Serial Nur	nber	An integral serial number to be	-	Serial Nur	nber
		assigned by the CA to the certificate			
Signature	Algorithm	sha256 with RSA Encryption	-	Signature	Algorithm
Issuer	Country	C=JP	-	Issuer	Country
	Organization	O=Japan Registry Services Co., Ltd.	-		Organization
	Common Name	(1) Domain Validation	-		Common Name
		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	-	Validity	NotBefore
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-		NotAfter
Subject	Country	(1) Domain Validation	-	Subject	Country
		No description			
		(2) Organization Validation			
		C=JP as the address of the Subscriber			
		(country)			
	State or Province	(1) Domain Validation	-		State or Province
		No description			
		(2) Organization Validation			
		Address of the Subscriber (prefecture			
		name) (mandatory)			
	Locality	(1) Domain Validation	-		Locality
		No description			
		(2) Organization Validation			
		Address of the Subscriber (city, town,			
		or village name) (mandatory)			
	Organization	(1) Domain Validation	-		Organization
		No description			
		(2) Organization Validation			
		Name of the Subscriber (mandatory)			
	Organizational	(1) Domain Validation	-		Organizational
	Unit	No description			Unit
		(2) Organization Validation			
		Business division name of the			
		Subscriber (optional).			

		整形版	
sic field		Description of setting	critical
sion		Version 3	-
ial Nui	nber	An integral serial number to be	-
		assigned by the CA to the certificate	
nature	Algorithm	sha256 with RSA Encryption	-
ıer	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	
idity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-
ject	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	
		name) (mandatory)	
	Locality	(1) Domain Validation	-
		No description	
		(2) Organization Validation	
		Address of the Subscriber (city, town,	
		or village name) (mandatory)	
	Organization	(1) Domain Validation	-
		No description	
		(2) Organization Validation	
		Name of the Subscriber (mandatory)	
	Organizational	(1) Domain Validation	-
	Unit	No description	
		(2) Organization Validation	
		Business division name of the	
		Subscriber (optional).	

	変更履歴あり			整形版		備考
	However, this item will not be			However, this item will not be		
	included in certificates issued on or			included in certificates issued on or		
	after 18 November 2021.			after 18 November 2021.		
	• A string comprising symbols only			• A string comprising symbols only		
	or spaces only may not be			or spaces only may not be		
	designated, and any of the following			designated, and any of the following		
	strings may not be included:			strings may not be included:		
	 any name, company name, trade name, or trademark that is likely to cause others to misconstrue that the relevant information is the information of any organization other than the applicant organization; any string indicating a legal personality, such as "Co., Ltd"; any string referring to a specific natural person; any string indicating an 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) 			 any name, company name, trade name, or trademark that is likely to cause others to misconstrue that the relevant information is the information of any organization other than the applicant organization; any string indicating a legal personality, such as "Co., Ltd"; any string referring to a specific natural person; any string indicating an 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	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.	-	Common Name	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.	-	
Subject Public Key Info	The subject's Public Key (RSA 2048 bits)	-	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	[1] Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/	n	CertificatePolicies	[1] Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/	n	

	変更履歴あり			整形版	
	[2] Certificate Policy			[2] Certificate Policy	
	(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/			http://repo.pubcert.jprs.jp/sppca/jprs/	
	dvca_g4/fullcrl.crl			dvca_g4/fullcrl.crl	
	(2) Organization Validation			(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/			http://repo.pubcert.jprs.jp/sppca/jprs/	
	ovca_g4/fullcrl.crl			ovca_g4/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.g4.ocsp.pubcert.jprs.jp			http://dv.g4.ocsp.pubcert.jprs.jp	
	(2) Organization Validation			(2) Organization Validation	
	http://ov.g4.ocsp.pubcert.jprs.jp			http://ov.g4.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/			http://repo.pubcert.jprs.jp/sppca/jprs/	
	dvca_g4/JPRS_DVCA_G4_DER.cer			dvca_g4/JPRS_DVCA_G4_DER.cer	
	(2) Organization Validation			(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/jprs/			http://repo.pubcert.jprs.jp/sppca/jprs/	
	ovca_g4/JPRS_OVCA_G4_DER.cer			ovca_g4/JPRS_OVCA_G4_DER.cer	
Authority Key Identifier	SHA-1 hash for the issuer's Public	n	Authority Key Identifier	SHA-1 hash for the issuer's Public	n
	Key (160 bits)			Key (160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's Public	n	Subject Key Identifier	SHA-1 hash for the subject's Public	n
	Key (160 bits)			Key (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)	SignedCertificateTimestampList		(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampList	

Basic field	asic 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			

		変更履歴あり				整形版		備考
	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 DV RSA CA 2024 G1				CN= JPRS DV RSA CA 2024 G1		
		(2) Organization Validation				(2) Organization Validation		
		CN= JPRS OV RSA CA 2024 G1				CN= JPRS OV RSA CA 2024 G1		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
-	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-		NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	
Subject	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				C=JP as the address of the		
		Subscriber (country)				Subscriber (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				Address of the Subscriber		
		(prefecture name) (mandatory)				(prefecture name) (mandatory)		
	Locality	(1) Domain Validation	-		Locality	(1) Domain Validation	-	
		No description			, i i i i i i i i i i i i i i i i i i i	No description		
		(2) Organization Validation				(2) Organization Validation		
		Address of the Subscriber (city,				Address of the Subscriber (city,		
		town, or village name)				town, or village name)		
		(mandatory)				(mandatory)		
	Organization	(1) Domain Validation	-		Organization	(1) Domain Validation	-	
		No description				No description		
		(2) Organization Validation				(2) Organization Validation		
		Name of the Subscriber				Name of the Subscriber		
		(mandatory)				(mandatory)		
	Common Name	A host name used in the DNS of	-		Common Name	A host name used in the DNS of	-	
		the server in which the certificate				the server in which the certificate		
		is scheduled to be installed				is scheduled to be installed		
		(mandatory)				(mandatory)		
		- The value must be encoded as				- The value must be encoded as		
		a character-for-character copy				a character-for-character copy		
		of the dNSName entry value				of the dNSName entry value		
		from the Subject Alternative				from the Subject Alternative		
		Name extension. Specifically.				Name extension. Specifically.		
Subiect Pi	ublic Key Info	The subject's Public Key (RSA	-	Subject P	ublic Key Info	The subject's Public Key (RSA	-	
		4096 bits, RSA3072 bits or		2		4096 bits, RSA3072 bits or		

	変更履歴あり		
	RSA 2048 bits)		
Extended field	Description of setting	critical	Extend
KeyUsage	digitalSignature,	У	KeyUsa
	keyEncipherment		
ExtendedKeyUsage	TLS Web Server Authentication	n	Extend
	TLS Web Client Authentication		
Subject Alt Name	dNSName= name(s) of the server(s)	n	Subject
CertificatePolicies	Certificate Policy	n	Certifie
	(1) Domain Validation		
	2.23.140.1.2.1		
	(2) Organization Validation		
	2.23.140.1.2.2		
CRL Distribution Points	(1) Domain Validation	n	CRL D
	http://repo.pubcert.jprs.jp/sppca/		
	jprs/dvca_rsa2024g1/fullcrl.crl		
	(2) Organization Validation		
	http://repo.pubcert.jprs.jp/sppca/		
	jprs/ovca_rsa2024g1/fullcrl.crl		
Authority Information	[1] ocsp (1.3.6.1.5.5.7.48.1)	n	Author
Access	(1) Domain Validation		Access
	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/dvca_rsa2024g1/JPRS_DV		
	CA_RSA2024G1_DER.cer		
	(2) Organization Validation		
	http://repo.pubcert.jprs.jp/sppca/		
	jprs/ovca_rsa2024g1/JPRS_OV		
	CA_RSA2024G1_DER.cer		
Authority Key Identifier	SHA-1 hash for the issuer's	n	Author
	Public Key (160 bits)		
Subject Key Identifier	SHA-1 hash for the subject's	n	Subject
	Public Key (160 bits)		
Certificate Transparency	Value of an OCTET STRING containing	n	Certific

yUsage digitalSignature, y keyEncipherment y tendedKeyUsage TLS Web Server Authentication n TLS Web Client Authentication n tLS Web Client Authentication n tLS Web Client Authentication n trificatePolicies Certificate Policy n (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation 2.23.140.1.2.2 L Distribution Points (1) Domain Validation n http://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/fuller1.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fuller1.crl (2) Organization Validation n http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fuller1.crl (2) Organization Validation n http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fuller1.crl (1) Domain Validation http://ov.rsa2024g1.ocsp.pubcert jprs.jp (2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert jprs.jp (2) Organization Validation http://ov.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/dvca_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/spca/ jprs/dvca_rsa2024g1.JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/spca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer (2) Organizatio		整形版	
yUsage digitalSignature, keyEncipherment y tendedKeyUsage TLS Web Server Authentication n TLS Web Client Authentication n bject Alt Name dNSName= name(s) of the server(s) n rtificatePolicies Certificate Policy n (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation 2.23.140.1.2.2 1 1 L Distribution Points (1) Domain Validation n http://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/fullcrl.crl n (2) Organization Validation n n http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fullcrl.crl n thority Information [1] ocsp (1.3.6.1.5.5.7.48.1) n thtp://dv.rsa2024g1.ocsp.pubcert jprs.jp (2) Organization Validation n http://repo.pubcert.jprs.jp/sppca/ jprs.jp (2) Organization Validation n http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1.ocsp.pubcert n (2) Organization Validation n ntp://repo.pubcert.jprs.jp/sppca/ n (2) Organization Validation n ntp://repo.pubcert.jprs.jp/sppca/		RSA 2048 bits)	
keyEnciphermenttendedKeyUsageTLS Web Server AuthenticationnTLS Web Client Authenticationbject Alt NamedNSName= name(s) of the server(s)nntificatePoliciesCertificate Policyn(1) Domain Validation2.23.140.1.2.1(2) Organization Validation2.23.140.1.2.21L Distribution Points(1) Domain Validationnhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/fullerl.crl(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullerl.crlthorityInformation11 J oesp (1.3.6.1.5.5.7.48.1)n(1) Domain Validationnhttp://dv.rsa2024g1.ocsp.pubcert.jprs.jp(2) Organization Validationhttp://ovrsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://ovrsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/spca/.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/spca/.jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/spca/.jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/spca/.jprs/ovca_rsa2024g1/JPRS_OVC	Extended field	Description of setting	critical
tendedKeyUsageTLS Web Server AuthenticationnTLS Web Client Authenticationnbject Alt NamedNSName= name(s) of the server(s)ntificatePoliciesCertificate Policyn(1) Domain Validation2.23.140.1.2.1(2) Organization Validation2.23.140.1.2.2(1) Domain Validation2.23.140.1.2.2L Distribution Points(1) Domain Validationnhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/fullerl.crl(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullerl.crlnthorityInformation[1] cosp (1.3.6.1.5.5.7.48.1)n(1) Domain Validationhttp://dv.rsa2024g1.ocsp.pubcertjprs.jpthey.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)1) Domain Validationhttp://ov.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://ov.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)1) Domain Validationhttp://ov.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)1) Domain Validationinhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationnhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA·1 hash for the subject'sn	KeyUsage	digitalSignature,	У
TLS Web Client Authenticationbject Alt NamedNSName= name(s) of the server(s)ntrificatePoliciesCertificate Policyn(1) Domain Validation2.23,140,1.2.1(2) Organization Validation2.23,140,1.2.21L Distribution Points(1) Domain Validationnhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/fullerl.crln(2) Organization Validationnnhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullerl.crln(2) Organization Validationnnhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/ousp.pubcertnthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)ntess(1) Domain Validationnnhttp://dv.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)1(1) Domain Validationhttp://ov.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)11(1) Domain Validationhttp://ov.rsa2024g1.jPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/spca/jprs/dvca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationnhttp://repo.pubcert.jprs.jp/spca/jprs/ovca_rsa2024g1/JPRS_OVnCA_RSA2024G1_DER.cervistovca_rsa2024g1/JPRS_OVnthority Key IdentifierSHA-1 hash for the issuer'snpublic Key (160 bits)vistovca_rsa2024g1/JPRS_OVn		keyEncipherment	
bject Alt Name dNSName= name(s) of the server(s) n rtificatePolicies Certificate Policy n (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation 2.23.140.1.2.2 L Distribution Points (1) Domain Validation n ttp://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/fullerl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fullerl.crl (2) Organization Validation http://dv.rsa2024g1/fullerl.crl (2) Organization Validation http://dv.rsa2024g1/ousp.pubcert jprs.jp (2) Organization Validation http://dv.rsa2024g1.ocsp.pubcert jprs.jp (2) Organization Validation http://ov.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/dvca_rsa2024g1.JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer thority Key Identifier SHA-1 hash for the issuer's n Public Key (160 bits) bject Key Identifier SHA-1 hash for the subject's n	ExtendedKeyUsage	TLS Web Server Authentication	n
rtificatePoliciesCertificate Policy (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation 2.23.140.1.2.2nL Distribution Points(1) Domain Validation 2.23.140.1.2.2nL Distribution Points(1) Domain Validation http://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/fullerl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fullerl.crlthorityInformation[1] cesp (1.3.6.1.5.5.7.48.1)nthorityInformation[1] cesp (1.3.6.1.5.5.7.48.1)nthetp://dv.rsa2024g1.ocsp.pubcert .jprs.jpn(2) Organization Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jpn(1) Domain Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jpn(2) Organization Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jpn(2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ .jprs/dvca_rsa2024g1/JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/spca/ .jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cernthority Key IdentifierSHA-1 hash for the issuer's Public Key (160 bits)n		TLS Web Client Authentication	
(1) Domain Validation2.23.140.1.2.1(2) Organization Validation2.23.140.1.2.2L Distribution Points(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/fullerl.crl(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullerl.crl(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullerl.crlthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)n(1) Domain Validationhttp://dv.rsa2024g1.ocsp.pubcertjprs.jp(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/spca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/spca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA·1 hash for the issuer'snpublic Key (160 bits)bject Key IdentifierSHA·1 hash for the subject'sn	Subject Alt Name	dNSName= name(s) of the server(s)	n
2.23.140.1.2.1 (2) Organization Validation 2.23.140.1.2.2Image: constant of the subject's problem of the subject'	CertificatePolicies	Certificate Policy	n
(2) Organization Validation 2.23.140.1.2.2L Distribution Points(1) Domain Validation http://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/fullerl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fullerl.crlthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)n(1) Domain Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jp(2) Organization Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jp(2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert .jprs.jp(2) Organization Validation http://ov.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/dvca_rsa2024g1/JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer's SUA-1 hash for the subject's		(1) Domain Validation	
2.23.140.1.2.2L Distribution Points(1) Domain Validationnhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/fullerl.crl(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullerl.crl(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullerl.crl(1) Domain ValidationthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)nthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)ntherein (1) Domain Validationhttp://dv.rsa2024g1.ocsp.pubcertjprs.jp(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationinhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVinCA_RSA2024G1_DER.cer(2) Organization Validationininhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_DVinCA_RSA2024G1_DER.cer(2) Organization Validationininhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OViniprs/ovca_rsa2024g1/JPRS_OVinininiprs/ovca_rsa2024g1/JPRS_OVinininiprs/ovca_rsa2024g1_JPRS_OVinininiprs/ovca_rsa2024g1_JPRS_OVinininiprs/ovca_rsa2024g1_JPRS_OVinininiprs/ovca_rsa2024g1_OER.cerinininiprs/ovca_rsa2024g1_JPRS_OVinininiprs/ovca_rsa2024g1_		2.23.140.1.2.1	
L Distribution Points(1) Domain Validationnhttp://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/fullerl.crln(2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fullerl.crlnthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)ntess(1) Domain Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jpn(2) Organization Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jpn(2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert .jprs.jp1(2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert .jprs.jp1(1) Domain Validation http://repo.pubcert.jprs.jp/sppca/ .jprs.jp1(2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ .jprs/ovca_rsa2024g1/JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ 		(2) Organization Validation	
http://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/fullcrl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fullcrl.crlthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)nthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)nthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)nthority[1] ocsp (1.3.6.1.5.5.7.48.1)nthority[2] Organization Validation1http://dv.rsa2024g1.ocsp.pubcert[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validation1http://ov.rsa2024g1.ocsp.pubcert[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validation1http://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validation1http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'snpublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn		2.23.140.1.2.2	
jprs/dvca_rsa2024g1/fullcrl.crl(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/fullcrl.crlthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)n(1) Domain Validationhttp://dv.rsa2024g1.ocsp.pubcert.jprs.jp(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://ov.rsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'snPublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn	CRL Distribution Points	(1) Domain Validation	n
(2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fullcrl.crlthorityInformation(1) Domain Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jpn(2) Organization Validation http://dv.rsa2024g1.ocsp.pubcert .jprs.jp1(2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert .jprs.jp1(2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert .jprs.jp1(2) Organization Validation http://ov.rsa2024g1.ocsp.pubcert .jprs.jp1(2) Organization Validation http://repo.pubcert.jprs.jp/spca/ jprs/dvca_rsa2024g1/JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/spca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer1thority Key IdentifierSHA-1 hash for the issuer's SHA-1 hash for the subject'sn	RL Distribution Points	http://repo.pubcert.jprs.jp/sppca/	
http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/fullerl.crlInthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)ntess(1) Domain Validationhttp://dv.rsa2024g1.ocsp.pubcertjprs.jp(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://ov.rsa2024g1.ocsp.pubcertjprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVca RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'snn.public Key (160 bits)		jprs/dvca_rsa2024g1/fullcrl.crl	
jprs/ovca_rsa2024g1/fullcrl.crlthorityInformation[1] ocsp (1.3.6.1.5.5.7.48.1)n(1) Domain Validationnhttp://dv.rsa2024g1.ocsp.pubcert.jprs.jp(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/[2] organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'snPublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn		(2) Organization Validation	
thority Information [1] ocsp (1.3.6.1.5.5.7.48.1) n (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/dvca_rsa2024g1/JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer thority Key Identifier SHA-1 hash for the issuer's n Public Key (160 bits) bject Key Identifier SHA-1 hash for the subject's n		http://repo.pubcert.jprs.jp/sppca/	
cess(1) Domain Validationhttp://dv.rsa2024g1.ocsp.pubcert.jprs.jp(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'snPublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn		jprs/ovca_rsa2024g1/fullcrl.crl	
http://dv.rsa2024g1.ocsp.pubcert.jprs.jp(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'snPublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn	Authority Information	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n
.jprs.jp(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'snPublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn	Access		
(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'spublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn		http://dv.rsa2024g1.ocsp.pubcert	
(2) Organization Validationhttp://ov.rsa2024g1.ocsp.pubcert.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'snPublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn			
.jprs.jp[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'spublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn			
[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'spublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn		http://ov.rsa2024g1.ocsp.pubcert	
[2] ca issuers (1.3.6.1.5.5.7.48.2)(1) Domain Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/dvca_rsa2024g1/JPRS_DVCA_RSA2024G1_DER.cer(2) Organization Validationhttp://repo.pubcert.jprs.jp/sppca/jprs/ovca_rsa2024g1/JPRS_OVCA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer'spublic Key (160 bits)bject Key IdentifierSHA-1 hash for the subject'sn		.jprs.jp	
http://repo.pubcert.jprs.jp/sppca/ jprs/dvca_rsa2024g1/JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer thority Key Identifier SHA-1 hash for the issuer's n Public Key (160 bits) n			
jprs/dvca_rsa2024g1/JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer thority Key Identifier SHA-1 hash for the issuer's n Public Key (160 bits) n		(1) Domain Validation	
jprs/dvca_rsa2024g1/JPRS_DV CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer thority Key Identifier SHA-1 hash for the issuer's n Public Key (160 bits) n		http://repo.pubcert.jprs.jp/sppca/	
CA_RSA2024G1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer thority Key Identifier SHA-1 hash for the issuer's Public Key (160 bits) bject Key Identifier NHA-1 hash for the subject's n			
http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer's Public Key (160 bits)nbject Key IdentifierSHA-1 hash for the subject'sn			
http://repo.pubcert.jprs.jp/sppca/ jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.certhority Key IdentifierSHA-1 hash for the issuer's Public Key (160 bits)nbject Key IdentifierSHA-1 hash for the subject'sn			
jprs/ovca_rsa2024g1/JPRS_OV CA_RSA2024G1_DER.cer thority Key Identifier SHA-1 hash for the issuer's Public Key (160 bits) bject Key Identifier SHA-1 hash for the subject's			
CA_RSA2024G1_DER.cer thority Key Identifier SHA-1 hash for the issuer's Public Key (160 bits) bject Key Identifier SHA-1 hash for the subject's			
thority Key IdentifierSHA-1 hash for the issuer's Public Key (160 bits)nbject Key IdentifierSHA-1 hash for the subject'sn			
Public Key (160 bits) bject Key Identifier SHA-1 hash for the subject's n	Authority Key Identifier		n
bject Key Identifier SHA-1 hash for the subject's n			
	Subject Key Identifier	-	n
=	<u> </u>		
	Certificate Transparency	-	n

	変更履歴あり				整形別	反
Timestamp List	the	encoded		Timestamp List	the	encoded
(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTime	estampList(optional).		(1.3.6.1.4.1.11129.2.4.2)	SignedCertific	ateTimestampList(optional).

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

Basic field	l	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	
		(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 name) (mandatory)	
	Locality	(1) Domain Validation	-
		No description	
		(2) Organization Validation	
		Address of the Subscriber (city,	
		town, or village name) (mandatory)	
	Organization	(1) Domain Validation	-
		No description	
		(2) Organization Validation	
		Name of the Subscriber	
		(mandatory)	
	Common Name	A host name used in the DNS	-

		整形版		
Timestamp	List	the encoded		
	1.11129.2.4.2)	SignedCertificateTimestampList(optional).		
				1
Fable 7.1-3 \$	Subscriber Certifica	te Profile (applicable to certificates issued	l by JPRS	DV
ECC CA 202	4 G1 or JPRS OV E	CC CA 2024 G1)		
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	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		
		(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 name) (mandatory)		
	Locality	(1) Domain Validation	-	
		No description		
		(2) Organization Validation		
		Address of the Subscriber (city,		
		town, or village name) (mandatory)		
	Organization	(1) Domain Validation	-	
		No description		
		(2) Organization Validation		
		Name of the Subscriber		
		(mandatory)		
	Common Name	A host name used in the DNS	-	

	変更履歴あり			整形版	
	of the server in which the certificate			of the server in which the certificate	
	is scheduled to be installed			is scheduled to be installed	
	(mandatory)			(mandatory)	
	- The value must be encoded as			- The value must be encoded as	
	a character-for-character copy			a character-for-character copy	
	of the dNSName entry value			of the dNSName entry value	
	from the Subject Alternative			from the Subject Alternative	
	Name extension. Specifically.			Name extension. Specifically.	
Subject Public Key Info	The subject's Public Key (RSA	-	Subject Public Key Info	The subject's Public Key (RSA	-
	4096 bits, RSA 3072 bits, RSA			4096 bits, RSA 3072 bits, RSA	
	2048 bits, P-256 or P-384)			2048 bits, P-256 or P-384)	
Extended field	Description of setting	critical	Extended field	Description of setting	critical
KeyUsage	digitalSignature,	у	KeyUsage	digitalSignature,	У
	keyEncipherment (except for			keyEncipherment (except for	
	certificates issued by using			certificates issued by using	
	ECDSA key)			ECDSA key)	
ExtendedKeyUsage	TLS Web Server Authentication	n	ExtendedKeyUsage	TLS Web Server Authentication	n
	TLS Web Client Authentication			TLS Web Client Authentication	
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/			http://repo.pubcert.jprs.jp/sppca/	
	jprs/dvca_ecc2024g1/fullcrl.crl			jprs/dvca_ecc2024g1/fullcrl.crl	
	(2) Organization Validation			(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/			http://repo.pubcert.jprs.jp/sppca/	
	jprs/ovca_ecc2024g1/fullcrl.crl			jprs/ovca_ecc2024g1/fullcrl.crl	
Authority Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n	Authority Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n
	(1) Domain Validation			(1) Domain Validation	
	http://dv.ecc2024g1.ocsp.pubcert			http://dv.ecc2024g1.ocsp.pubcert	
	.jprs.jp			.jprs.jp	
	(2) Organization Validation			(2) Organization Validation	
	http://ov.ecc2024g1.ocsp.pubcert			http://ov.ecc2024g1.ocsp.pubcert	
	.jprs.jp			.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	

	変更履歴あり	
	http://repo.pubcert.jprs.jp/sppca/	
	jprs/dvca_ecc2024g1/JPRSDV	
	CA_ECC2024G1_DER.cer	
	(2) Organization Validation	
	http://repo.pubcert.jprs.jp/sppca/	
	jprs/ovca_ecc2024g1/JPRS_OV	
	CA_ECC2024G1_DER.cer	
Authority Key Identifier	SHA-1 hash for the issuer's	n
	Public Key (160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's	n
	Public Key (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)	${f SignedCertificateTimestampLi}$	
	st (optional)	

Table 7.1-4 Subordinate CA Certificate Profile (applicable to certificates issued by Security	
Communication Root(A2)	

Basic field	l	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	sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	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	-
		CN=JPRS 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	critical

		整形版		
		http://repo.pubcert.jprs.jp/sppca/		
		jprs/dvca_ecc2024g1/JPRSDV		
		CA_ECC2024G1_DER.cer		
		(2) Organization Validation		
		http://repo.pubcert.jprs.jp/sppca/		
		jprs/ovca_ecc2024g1/JPRS_OV		
		CA_ECC2024G1_DER.cer		
Authority	Key Identifier	SHA-1 hash for the issuer's		_
Authority I	Xey Identifier	Public Key (160 bits)	n	
Subject Key Identifier		SHA-1 hash for the subject's		-
		Public Key (160 bits)	n	
Contificato	The second second	-		-
	Transparency	Value of an OCTET STRING containing	n	
Timestamp		the encoded		
(1.3.6.1.4.	1.11129.2.4.2)	SignedCertificateTimestampLi		
		st (optional)		
Basic field		Description of setting	critical	
Version		Version 3	-	_
Serial Num	iber	An integral serial number to be	-	
		assigned by the CA to the certificate		_
a .				
	-	sha256 With RSA Encryption	-	_
	Country	sha256 With RSA Encryption C=JP	-	-
	Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.	-	-
Issuer	Country Organization Common Name	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2	-	-
Issuer	Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.	- - - -	
ssuer	Country Organization Common Name	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2	- - - - -	
Issuer Validity	Country Organization Common Name NotBefore	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMT	- - - - - -	
Issuer Validity	Country Organization Common Name NotBefore NotAfter	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT	- - - - - - -	
Issuer Validity	CountryOrganizationCommon NameNotBeforeNotAfterCountry	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JP	- - - - - - - - - - - -	
Issuer Validity	Country Organization Common Name NotBefore NotAfter Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.	- - - - - - - -	
Issuer Validity	Country Organization Common Name NotBefore NotAfter Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization Validation	- - - - - - - -	
Issuer Validity	Country Organization Common Name NotBefore NotAfter Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization Validation	- - - - - - - -	
Issuer Validity	Country Organization Common Name NotBefore NotAfter Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization ValidationAuthority	- - - - - - - -	
Issuer Validity	Country Organization Common Name NotBefore NotAfter Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization ValidationAuthority- G4	- - - - - - - -	
Issuer Validity	Country Organization Common Name NotBefore NotAfter Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization ValidationAuthority- G4(2) Domain Validation	- - - - - - - -	
Signature 4 Issuer Validity Subject Subject Pu	Country Organization Common Name NotBefore NotAfter Country Organization	sha256 With RSA EncryptionC=JPO=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization ValidationAuthority- G4(2) Domain ValidationCN=JPRS Domain Validation Authority	- - - - - - - -	

		整形版		
		http://repo.pubcert.jprs.jp/sppca/		
		jprs/dvca_ecc2024g1/JPRSDV		
		CA_ECC2024G1_DER.cer		
		(2) Organization Validation		
		http://repo.pubcert.jprs.jp/sppca/		
		jprs/ovca_ecc2024g1/JPRS_OV		
		CA_ECC2024G1_DER.cer		
Authority]	Key Identifier	SHA-1 hash for the issuer's	n	
		Public Key (160 bits)		
Subject Key Identifier		SHA-1 hash for the subject's	n	
		Public Key (160 bits)		
Certificate	Transparency	Value of an OCTET STRING containing	n	
Timestamp		the encoded		
-		SignedCertificateTimestampLi		
(1.3.6.1.4.1.11129.2.4.2)		st (optional)		
Communica Basic field	tion RootCA2)	Description of setting	critical	
Version		Version 3	-	
Serial Nun	ıber	An integral serial number to be	-	
		assigned by the CA to the certificate		
Signature	Algorithm	sha256 With RSA Encryption	-	
Issuer				
TOOUGI	Country	C=JP	-	
TODUCI	Country Organization	C=JP O=SECOM Trust Systems CO.,LTD.	-	
199461			- - -	
Validity	Organization	O=SECOM Trust Systems CO.,LTD.	- - - -	
	Organization Common Name	O=SECOM Trust Systems CO.,LTD. OU=Security Communication RootCA2	- - - -	
	Organization Common Name NotBefore	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMT	- - - - -	
Validity	Organization Common Name NotBefore NotAfter	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMT	- - - - - -	
Validity	Organization Common Name NotBefore NotAfter Country	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JP	- - - - - - -	
Validity	Organization Common Name NotBefore NotAfter Country Organization	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.	- - - - - - -	
Validity	Organization Common Name NotBefore NotAfter Country Organization	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization Validation	- - - - - - -	
Validity	Organization Common Name NotBefore NotAfter Country Organization	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization Validation	- - - - - -	
Validity	Organization Common Name NotBefore NotAfter Country Organization	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization ValidationAuthority	- - - - -	
Validity	Organization Common Name NotBefore NotAfter Country Organization	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization ValidationAuthority- G4	- - - - - -	
Validity	Organization Common Name NotBefore NotAfter Country Organization	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization ValidationAuthority- G4(2) Domain Validation	- - - - - -	
Validity Subject	Organization Common Name NotBefore NotAfter Country Organization	O=SECOM Trust Systems CO.,LTD.OU=Security Communication RootCA2E.g.) 2008/3/1 00:00:00 GMTE.g.) 2009/3/1 00:00:00 GMTC=JPO=Japan Registry Services Co., Ltd.(1) Organization ValidationCN=JPRS Organization ValidationAuthority- G4(2) Domain ValidationCN=JPRS Domain Validation Authority	- - - - - -	

	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	Certificate Signing	У
	Off-line CRL Signing	
	CRL Signing (06)	
CertificatePolicies	Certificate Policy	Ν
	1.2.392.200091.100.901.4	
	CPS	
	http://repository.secomtrust.net/	
	SC-Root2/	
Basic Constraints	Subject Type=CA	У
	Path Length Constraint=0	
ExtendedKeyUsage	TLS Web Server Authentication	n
CRL Distribution Points	http://repository.secomtrust.net/SC-	n
	Root2/SCRoot2CRL.crl	
Authority Information Access	[1] 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-	
	Root2/SCRoot2ca.cer	

		整形版		
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	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	
	ibution Points	http://repository.secomtrust.net/SC-	n	
		Root2/SCRoot2CRL.crl		
Authority	Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n	
C C		http://scrootca2.ocsp.secomtrust.net		
		[2] ca issuers (1.3.6.1.5.5.7.48.2)		
		http://repository.secomtrust.net/SC-		
		Root2/SCRoot2ca.cer		
Table 7.1-5	Subordinate CA Cert	ificate Profile (applicable to certificates issu	ed by SEC	СОМ
TLS RSA R	oot CA 2024)			
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	Sha384 With RSA Encryption	-	
Issuer	Country	C=JP	-	
	Organization	O=SECOM Trust Systems Co., Ltd.	-	1
	Common Name	CN= SECOM TLS RSA Root CA 2024	-	
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	1
.0	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		

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

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	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	Organization O=Japan Registry Services Co., Ltd.	
	Common Name	(1) Organization Validation	-
		CN= JPRS OV RSA CA 2024 G1	

		整形版		
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		
Extended	KeyUsage	TLS Web Server Authentication	n	
CRL Distri	ibution Points	http://repository.secomtrust.net/SC-	n	
		Root2/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-		
		Root2/SCRoot2ca.cer		
		ificate Profile (applicable to certificates issu	ed by SEC	OM
	oot CA 2024)		1	
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		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		
	42/59			

	変更履歴あり	
	(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	n
	Key (160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's Public	n
	Key (160 bits)	
KeyUsage	Certificate Signing	у
	Off-line CRL Signing	
	CRL Signing (06)	
CertificatePolicies	[1] Certificate Policy	Ν
	(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 Constraints	Subject Type=CA	У
	Path Length Constraint=0	
ExtendedKeyUsage	TLS Web Server Authentication	n
	TLS Web Client Authentication	
CRL Distribution Points	http://repo1.secomtrust.net/root/tlsrsa/	n
	tlsrsarootca2024.crl	
Authority Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n
	http://tlsrsarootca2024.ocsp.	
	secom-cert.jp	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	http://repo2.secomtrust.net/root/	
	tlsrsa/tlsrsarootca2024.cer	

	整形版	
	(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	critical
Authority Key Identifier	SHA-1 hash for the issuer's Public	n
	Key (160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's Public	n
	Key (160 bits)	
KeyUsage	Certificate Signing	у
	Off-line CRL Signing	
	CRL Signing (06)	
CertificatePolicies	[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 Constraints	Subject Type=CA	у
	Path Length Constraint=0	, i i i i i i i i i i i i i i i i i i i
ExtendedKeyUsage	TLS Web Server Authentication	n
v c	TLS Web Client Authentication	
CRL Distribution Points	http://repo1.secomtrust.net/root/tlsrsa/	n
	tlsrsarootca2024.crl	
Authority Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n
	http://tlsrsarootca2024.ocsp.	
	secom-cert.jp	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	http://repo2.secomtrust.net/root/	
	tlsrsa/tlsrsarootca2024.cer	
able 7.1-6 Subordinate CA Certi	ficate Profile (applicable to certificates issu	ied by Seci
ommunication ECC RootCA1)		-
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	ecdsa-with-SHA384	-

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

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	ecdsa-with-SHA384	-

	整形版	
	(2) Domain Validation	
	CN= JPRS DV RSA CA 2024 G1	
Subject Public Key Info	The subject's Public Key (RSA 4096	
Subject Fublic Key IIIo	bits)	
Extended field		critical
	Description of setting SHA-1 hash for the issuer's Public	
Authority Key Identifier		n
	Key (160 bits)	
Subject Key Identifier	SHA-1 hash for the subject's Public	n
	Key (160 bits)	
KeyUsage	Certificate Signing	У
	Off-line CRL Signing	
	CRL Signing (06)	
CertificatePolicies	[1] Certificate Policy	Ν
	(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 Constraints	Subject Type=CA	У
	Path Length Constraint=0	
ExtendedKeyUsage	TLS Web Server Authentication	n
	TLS Web Client Authentication	
CRL Distribution Points	http://repo1.secomtrust.net/root/tlsrsa/	n
	tlsrsarootca2024.crl	
Authority Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n
	http://tlsrsarootca2024.ocsp.	
	secom-cert.jp	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	http://repo2.secomtrust.net/root/	
	tlsrsa/tlsrsarootca2024.cer	
Cable 7.1-6 Subordinate CA Certi	ificate Profile (applicable to certificates issu	ued by Secu
Communication ECC RootCA1)		
Basic field	Description of setting	critical
Version	Version 3	-
VEISIOII		
Serial Number	An integral serial number to be	-
	An integral serial number to be assigned by the CA to the certificate	-

		変更履歴あり	
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 f	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	Ν
		(1) Domain Validation	
		2.23.140.1.2.1	
		(2) Organization Validation	
		2.23.140.1.2.2	
		[2] Certificate Policy	
		1.2.392.200091.100.902.1	
Basic Cons	straints	Subject Type=CA	У
		Path Length Constraint=0	
Extended	KeyUsage	TLS Web Server Authentication	n
		TLS Web Client Authentication	
CRL Distr	ibution Points	http://repository.secomtrust.net/SC-	n
		ECC-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-	
		ECC-Root1/SCECCRoot1ca.cer	

		整形版	
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 Pub	olic Key Info	The subject's Public Key (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	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)	
CertificateF	Policies	[1] Certificate Policy	Ν
		(1) Domain Validation	
		2.23.140.1.2.1	
		(2) Organization Validation	
		2.23.140.1.2.2	
		[2] Certificate Policy	
		1.2.392.200091.100.902.1	
Basic Const	traints	Subject Type=CA	У
		Path Length Constraint=0	
ExtendedKe	eyUsage	TLS Web Server Authentication	n
		TLS Web Client Authentication	
CRL Distrik	bution Points	http://repository.secomtrust.net/SC-	n
		ECC-Root1/SCECCRoot1CRL.crl	
Authority In	nformation 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-	
		ECC-Root1/SCECCRoot1ca.cer	

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 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	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,	
		Section 3.1.	
KeyUsage		Encoded value MUST be byte-for-byte	У
		identical to the same field of the	
		Subuscriber Certificate.	
Extended	KeyUsage		n
Extended Subject Al		Subuscriber Certificate.	n n
	t Name	Subuscriber Certificate. Same as above	
Subject Al Certificate	t Name	Subuscriber Certificate. Same as above Same as above	n
Subject Al Certificate CRL Distr	t Name Policies	Subuscriber Certificate.Same as aboveSame as aboveSame as above	n n
Subject Al Certificate CRL Distr Authority	t Name Policies ibution Points	Subuscriber Certificate.Same as aboveSame as aboveSame as aboveSame as above	n n n
Subject Al Certificate CRL Distr Authority Authority	t Name Policies ibution Points Information Access	Subuscriber Certificate.Same as aboveSame as aboveSame as aboveSame as aboveSame as aboveSame as above	n n n n
Subject Al Certificate CRL Distr Authority Authority Subject Ke	t Name Policies ibution Points Information Access Key Identifier ey Identifier	Subuscriber Certificate.Same as aboveSame as aboveSame as aboveSame as aboveSame as aboveSame as aboveSame as above	n n n n n n

		整形版		
Fable 7.1-7 1 Basic field	Precertificate Profile	applicable to certificates issued on or after Description of setting	July 29, 20 critical)20)
Version		Encoded value MUST be byte-for-byte	-	
10101011		identical to the same field of the		
		Subuscriber Certificate.		
Serial Nun	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	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,		
		Section 3.1.		
KeyUsage		Encoded value MUST be byte-for-byte	У	
		identical to the same field of the		
		Subuscriber Certificate.		
ExtendedK	KeyUsage	Same as above	n	
Subject Alt	Name	Same as above	n	
Certificate	Policies	Same as above	n	
CRL Distri	bution Points	Same as above	n	
Authority	Information Access	Same as above	n	
Authority]	Key Identifier	Same as above	n	
Subject Ke	y Identifier	Same as above	n	
If the Prec	ertificate Poison exte	nsion is removed from the Precertificate, a	nd the Sig	ned
ertificate Ti	imestamp List is rem	oved from the Subscriber certificate, the c	ontents 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 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 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	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		digitalSignature	У
ExtendedK	KeyUsage	OCSPSigning	Ν
OCSP No (Check	null	Ν

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 Number	Non-sequential values greater than zero	-

tensions fie	eld MUST be byte-for	r-byte identical to the Subscriber Certificate	•	
T-11-716				
	-	ertificate Profile (Applicable to certificates is	-	RS
Basic field	-	4 or JPRS Organization Validation Authorit Description of setting	y – G4) critical	
Version		Version 3	-	
Serial Nun	nhor	Non-sequential values greater than zero		
Serial Null	liber	(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	-	
ubject	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 2048 bits)	-	
Extended f	field	Description of setting	critical	
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n	
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n	
KeyUsage		digitalSignature	у	
Extended	KeyUsage	OCSPSigning	N	
DCSP No (Check	null	N	
) OCSP Responder Co 2024 G1 or JPRS OV	ertificate Profile (Applicable to certificates is RSA CA 2024 G1)	ssued by JF	PRS
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Nun	nhor	Non-sequential values greater than zero	-	

	-	ertificate Profile (Applicable to certificates is	-	PF
	lation Authority – G	4 or JPRS Organization Validation Authority		1
Basic field		Description of setting	critical	
Version		Version 3	-	
Serial Nun	ıber	Non-sequential values greater than zero	-	
		(0) and less than 2^{159} containing 64		
<u>C:</u>	A 1	bits of output from a CSPRNG		-
Signature A	_	sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	-
	Organization Common Name	O= Japan Registry Services Co., Ltd. (1) Domain Validation	-	
	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	-	
C C	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-	
Subject	Country	C=JP (fixed value)	-	1
	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 2048 bits)	-	
Extended f	ïeld	Description of setting	critical	
Authority 3	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	leyUsage	OCSPSigning	Ν	
OCSP No (Check	null	Ν	
Table 7.1-9	OCSP Responder C	ertificate Profile (Applicable to certificates is	ssued by J	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	-	1

		変更履歴あり	
		(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	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
			ı

		整形版	
		(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	field	Description of setting	critical
Authority I	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
OCSP No (Check	null	n
PRS DV EC	-	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1)	
Basic field		Description of setting	critical
Version	1	Version 3	-
Serial Nun	nber	Non-sequential values greater than zero	-
		(0) and less than 2^{159} containing 64	
a .	A1 ···1	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	

Table 7.1-10 OCSP Responder Certificate Profile (Applicable to certificates issued by JPRS DV ECC CA 2024 G1 or JPRS OV ECC CA 2024 G1)

Basic fiel	d	Description of setting	critical
Version		Version 3	-
Serial Nu	ımber	Non-sequential values greater than zero	-
		(0) and less than 2^{159} containing 64	
		bits of output from a CSPRNG	
Signatur	e 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	

		整形版	
		(0) and less than 2^{159} containing 64	
		bits of output from a CSPRNG	
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 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	eld	Description of setting	critical
Authority K	ley 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
ExtendedK	eyUsage	OCSPSigning	n
OCSP No C	heck	null	n
PRS DV ECO	-	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1)	- -
Basic field		Description of setting	critical
Version	1	Version 3	-
Serial Num	ber	Non-sequential values greater than zero	-
		(0) and less than 2^159 containing 64	
<u> </u>	11	bits of output from a CSPRNG	
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	
	47/59	(2) Organization Validation	

		変更履歴あり	
		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	ublic Key Info	The subject's Public Key (256 bits or 384	-
		bits)	
Extended	field	Description of setting	critica
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key	n
		(160 bits)	
Subject K	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

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:

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

			ند منه ۲۰ ال المنه ال المنه		
			至形版		
			PRS OV ECC CA 2024 G1		-
Validity	NotBefore		08/3/1 00:00:00 GMT	-	
	NotAfter		08/3/5 00:00:00 GMT	-	
Subject	Country		(fixed value)	-	-
	Organization	-	Registry Services Co., Ltd. (fixed	-	
		value)			
	Common Name	Name o	f the OCSP server (mandatory)	-	_
Subject Pub	olic Key Info	The sub bits)	ject's Public Key (256 bits or 384	-	
Extended fi	eld	Descrip	tion of setting	critical	
Authority K	Xey Identifier	SHA-1 (160 bit	hash for the issuer's Public Key s)	n	
Subject Key	y Identifier	SHA-1	hash for the subject's Public Key	n	1
		(160 bit	s)		
KeyUsage		digitalS	ignature	У	
ExtendedKe	eyUsage	OCSPS	igning	n	
OCSP No C	heck	null		n	
Extensions of 7.1.3 Algor	rithm Object Iden	ed by the (tifi er	CA is specified Section 7.1 of this C	CP.	
The algorithm	n OID used in this se	ervice is as			T
	Algorithm		Object Identifier		_
sha256 With	RSA Encryption		1.2.840.113549.1.1.11		
RSA Encrypt			1.2.840.113549.1.1.1		_
sha384 With	RSA Encryption		1.2.840.113549.1.1.12		
id-ecPublicK	ley		1.2.840.10045.2.1		
ecdsa-with-S	SHA384		1.2.840.10045.4.3.3		
7.1.4 Nam	e Format				
The CA uses t	the Distinguished N	ame specif	ied in RFC 5280.		
For every vali	id Certification Path	n (as define	ed by RFC 5280, Section 6), for ea	ach Certifi	icate
n the Certific	cation Path, the end	coded conte	ent of the Issuer Distinguished N	ame field	of a
Certificate SI	HALL be byte-for-	byte iden	···· 1 ··· 1 ··· 1 · 1 · 1 · · · · · ·	f the Sub	oject
	J	~	tical with the encoded form of		
Distinguished	l Name field of the I	-		the but	

		整形版		
		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	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		digitalSignature	У	
Extended	KeyUsage	OCSPSigning	n	
OCSP No (Check	null	n	
ne CA appli	sion Number(s) ies version 3.	2		
he CA appli 7.1.2 Cert xtensions o 7.1.3 Algo	ies version 3. t ificate Extensio f the Certificate issu prithm Object Iden	aed by the CA is specified Section 7.1 of this ntifier	CP.	
he CA appli 7.1.2 Cert xtensions o 7.1.3 Algo	ies version 3. tificate Extension f the Certificate issu prithm Object Iden m OID used in this s	ned by the CA is specified Section 7.1 of this ntifier service is as follows:	CP.	٦
ne CA appli 7.1.2 Cert atensions of 7.1.3 Algo ne algorithm	ies version 3. tificate Extension f the Certificate issu- prithm Object Iden m OID used in this so Algorithm	ned by the CA is specified Section 7.1 of this ntifier service is as follows: Object Identifier	CP.	
ne CA appli 7.1.2 Cert atensions of 7.1.3 Algo ne algorithm ha256 With	ies version 3. tificate Extension of the Certificate issues or the Object Iden of OID used in this se Algorithm h RSA Encryption	and by the CA is specified Section 7.1 of this ntifier service is as follows: Object Identifier 1.2.840.113549.1.1.11	СР.	
ne CA appli 7.1.2 Cert atensions of 7.1.3 Algo ne algorithm ha256 With RSA Encryp	ies version 3. tificate Extension f the Certificate issue orithm Object Iden m OID used in this se Algorithm h RSA Encryption option	ned by the CA is specified Section 7.1 of this ntifier service is as follows: Object Identifier 1.2.840.113549.1.1.11 1.2.840.113549.1.1.1	СР.	
ne CA appli 7.1.2 Cert xtensions of 7.1.3 Algo ne algorithm ha256 With RSA Encryp ha384 With	ies version 3. tificate Extension f the Certificate issue or the Object Iden m OID used in this se Algorithm h RSA Encryption otion h RSA Encryption	aed by the CA is specified Section 7.1 of this ntifier service is as follows: Object Identifier 1.2.840.113549.1.1.11 1.2.840.113549.1.1.1 1.2.840.113549.1.1.1 1.2.840.113549.1.1.1	CP.	
ne CA appli 7.1.2 Cert xtensions of 7.1.3 Algo ne algorithm ha256 With SA Encryp ha384 With d-ecPublich	ies version 3. tificate Extension of the Certificate issues or the Object Iden on OID used in this se Algorithm h RSA Encryption otion h RSA Encryption Key	aed by the CA is specified Section 7.1 of this htifier service is as follows: Object Identifier 1.2.840.113549.1.1.11 1.2.840.113549.1.1.1 1.2.840.113549.1.1.1 1.2.840.113549.1.1.12 1.2.840.113549.1.1.12	CP.	
ne CA appli 7.1.2 Cert xtensions of 7.1.3 Algo ne algorithm ha256 With SA Encryp ha384 With d-ecPublich	ies version 3. tificate Extension of the Certificate issues or the Object Iden on OID used in this se Algorithm h RSA Encryption otion h RSA Encryption Key	aed by the CA is specified Section 7.1 of this ntifier service is as follows: Object Identifier 1.2.840.113549.1.1.11 1.2.840.113549.1.1.1 1.2.840.113549.1.1.1 1.2.840.113549.1.1.1	CP.	
ne CA appli 7.1.2 Cert ctensions of 7.1.3 Algo ne algorithm ha256 With CSA Encryp ha384 With d-ecPublich cdsa-with-	ies version 3. tificate Extension of the Certificate issues or the Object Iden on OID used in this se Algorithm h RSA Encryption otion h RSA Encryption Key	aed by the CA is specified Section 7.1 of this htifier service is as follows: Object Identifier 1.2.840.113549.1.1.11 1.2.840.113549.1.1.1 1.2.840.113549.1.1.1 1.2.840.113549.1.1.12 1.2.840.113549.1.1.12	CP.	
he CA appli 7.1.2 Cert xtensions of 7.1.3 Algo he algorithm sha256 With sha256 With sha384 With id-ecPublich ecdsa-with- 7.1.4 Nam he CA uses or every value	ies version 3. tificate Extension f the Certificate issues orithm Object Iden in OID used in this second Algorithm h RSA Encryption otion h RSA Encryption Key SHA384 he Format the Distinguished M lid Certification Pat	aed by the CA is specified Section 7.1 of this htifier service is as follows: Object Identifier 1.2.840.113549.1.1.11 1.2.840.113549.1.1.1 1.2.840.113549.1.1.1 1.2.840.113549.1.1.12 1.2.840.113549.1.1.12	ach Certif	
he CA appli 7.1.2 Cert xtensions of 7.1.3 Algo he algorithm sha256 With sha256 With sha384 With d-ecPublich ecdsa-with- f.1.4 Nam he CA uses or every value	ies version 3. tificate Extensio f the Certificate issue orithm Object Identificate m OID used in this second Algorithm h RSA Encryption otion h RSA Encryption Otion h RSA Encryption Key SHA384 he Format the Distinguished M lid Certification Path, the en-	and by the CA is specified Section 7.1 of this htifier service is as follows: Object Identifier 1.2.840.113549.1.1.11 1.2.840.113549.1.1.12 1.2.840.113549.1.1.12 1.2.840.10045.2.1 1.2.840.10045.4.3.3 Name specified in RFC 5280. h (as defined by RFC 5280, Section 6), for example.	ach Certif Name field	of
he CA appli 7.1.2 Cert xtensions of 7.1.3 Algo he algorithm sha256 With RSA Encryp sha384 With d-ecPublich ecdsa-with- 7.1.4 Nam he CA uses or every value the Certificate S	ies version 3. tificate Extension f the Certificate issues orithm Object Iden in OID used in this series Algorithm h RSA Encryption otion h RSA Encryption otion h RSA Encryption SHA384 the Distinguished N lid Certification Path ication Path, the encryption SHALL be byte-for	And by the CA is specified Section 7.1 of this htifier service is as follows: Object Identifier 1.2.840.113549.1.1.11 1.2.840.113549.1.1.12 1.2.840.113549.1.1.12 1.2.840.10045.2.1 1.2.840.10045.4.3.3 Name specified in RFC 5280. h (as defined by RFC 5280, Section 6), for expected on the Issuer Distinguished I	ach Certif Name field	of

変更履歴あり	整形版	備考
CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Subject	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	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.	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)	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	characters, and/or any other indication that the value is absent, incomplete, or not	
applicable.	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.	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.	LDH Labels, and P-Labels does not convert to Unicode.	
7.1.5 Name Constraints	7.1.5 Name Constraints	
Not set in the CA.	Not set in the CA.	
7.1.6 Certificate Policy Object Identifier	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	The OID of the certificate issued by the CA is as described in this CP "1.2 Document Name	
and Identification".	and Identification".	
The following Certificate Policy identifiers are reserved for use by the CA as an optional	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.	means of assertaing that a Certificate complies with Baseline Requirements.	
[For DV certificate] {joint-iso-itu-t(2) international-organizations(23)	[For DV certificate] {joint-iso-itu-t(2) international-organizations(23)	
$ca\-browser\-forum(140)\ certificate policies(1)\ baseline\-requirements(2)\ domain\-validated(1)\}$	$ca\-browser\-forum(140)\ certificate policies(1)\ baseline\-requirements(2)\ domain\-validated(1)\}$	
(2.23.140.1.2.1)	(2.23.140.1.2.1)	
[For OV certificate] {joint-iso-itu-t(2) international-organizations(23)	[For OV certificate] {joint-iso-itu-t(2) international-organizations(23)	
ca-browser-forum(140) certificatepolicies(1) baseline-requirements(2)	ca-browser-forum(140) certificatepolicies(1) baseline-requirements(2)	
organization-validated(2)} (2.23.140.1.2.2)	organization-validated(2)} (2.23.140.1.2.2)	
7.1.7 Use of Policy Constraint Extensions	7.1.7 Use of Policy Constraint Extensions	
Not set.	Not set.	
7.1.8 Policy Qualifier Syntax and Semantics	7.1.8 Policy Qualifier Syntax and Semantics	
For the policy qualifier, the URI of the Web page that publishes this CP and CPS is stored.	For the policy qualifier, the URI of the Web page that publishes this CP and CPS is stored.	
7.1.9 How to interpret Critical Certificate Policy Extensions	7.1.9 How to interpret Critical Certificate Policy Extensions	
Not set.	Not set.	
7.2 CRL Profile	7.2 CRL Profile	
The profile of CRLs to be issued by the CA shall be as described in the following table:	The profile of CRLs to be issued by the CA shall be as described in the following table:	

Table 7.2.1 (Deleted)

Table 7.2.2 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 Al	gorithm	SHA256 with RSAEncryption	-
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	
This Update		E.g.) 2008/3/1 00:00:00 GMT	-
Next Update	9	E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-
Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
	Reason Code	Revocation Reason Code (*)	-
Extended fie	Extended field Description of setting		critical
CRL Numbe	r	CRL number	n
Authority Ke	ey 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 7.2.3 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 Al	gorithm	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	

			整形版		
,	Гаble 7.2.1 (D	eleted)			
r	Гable 7.2.2 CI	RL Profile (applicable	e to certificates issued by JPRS DV RSA C.	A 2024 G1	or
J	PRS OV RSA	CA 2024 G1)	-		
	Basic field		Description of setting	critical	
	Version		Version 2	-	
	Signature Al	gorithm	SHA256 with RSAEncryption	-	
	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		
-	This Update		E.g.) 2008/3/1 00:00:00 GMT	-	
	Next Update		E.g.) 2008/3/5 00:00:00 GMT	-	
	Revoked	Serial Number	E.g.) 0123456789	-	
	Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
		Reason Code	Revocation Reason Code (*)	-	
-	Extended fie	ld	Description of setting	critical	
	CRL Number	r	CRL number	n	
	Authority Ke	ey Identifier	SHA-1 hash for the issuer's Public Key	n	
			(160 bits)		
	*: The "Reas	son Code" field is set	one of the Revocation Reason code specifie	ed in the t	able
			n Code is "#0 unspecified", the "Reason Co	ode" field o	loes
	not appear i	in the CRL profile.			
			e to certificates issued by JPRS DV RSA C.	A 2024 G1	or
J I	PRS OV RSA	CA 2024 G1)			
ļ	Basic field		Description of setting	critical	
	Version		Version 2	-	
ļ	Signature Al		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		

		整形版		
Table 7.2.1 (D	eleted)			
Table 7.2.2 CI	RL Profile (applicabl	e to certificates issued by JPRS DV RSA C	A 2024 G1	or
PRS OV RSA	CA 2024 G1)			1
Basic field		Description of setting	critical	
Version		Version 2	-	
Signature Al		SHA256 with RSAEncryption	-	
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		
///1.1.1.1.		Authority – G4		
This Update		E.g.) 2008/3/1 00:00:00 GMT	-	
Next Update	ſ	E.g.) 2008/3/5 00:00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
E (1. 1 C .	Reason Code	Revocation Reason Code (*)	-	
Extended fie		Description of setting	critical	
CRL Number		CRL number	n	
Authority Ke	ey Identifier	SHA-1 hash for the issuer's Public Key	n	
*· //l //D	Q. 1. " (°. 11 :	(160 bits)	. 1	. 1. 1 .
		t one of the Revocation Reason code specific on Code is "#0 unspecified", the "Reason Co		
	in the CRL profile.	in Code is #0 unspecified, the Reason Co	oue menu (loes
not appear	in the Chil prome.			
Fable 7.2.3 CI	RI. Profile (applicabl	e to certificates issued by JPRS DV RSA C	A 2024 G1	or
PRS OV RSA		e to tertificates issued by 91 hb DV hbA 0.	A 2024 01	01
Basic field		Description of setting	critical	
Version		Version 2	-	
Signature Al	gorithm	SHA384 with RSAEncryption	-	
Issuer	Country	С=ЈР	-	
1000001	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		
	0/50			

		変更履歴あり	
This Update		E.g.) 2008/3/1 00:00:00 GMT	-
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-
Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
	Reason Code	Revocation Reason Code (*)	-
Extended fie	ld	Description of setting	critical
CRL Numbe	r	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.

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 Al	gorithm	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.g.) 2008/3/1 00:00:00 GMT	-
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-
Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
	Reason Code	Revocation Reason Code (*)	-
Extended field CRL Number		Description of setting	critical
		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.

		整形版			備考	
This Update		E.g.) 2008/3/1 00:00:00 GMT	-			
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-			
Revoked	Serial Number	E.g.) 0123456789	-			
Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-			
	Reason Code	Revocation Reason Code (*)	-			
Extended fie		Description of setting	critical			
CRL Number		CRL number	n			
Authority Ke		SHA-1 hash for the issuer's Public Key	n			
		(160 bits)				
: The "Reason	Code" field is set o	ne of the Revocation Reason code specifie	d in the t	able		
appear in the C	CRL profile. RL Profile (applicable	ode is "#0 unspecified", the "Reason Code" e to certificates issued by JPRS DV ECC C				
Basic field		Description of setting	critical			
Version		Version 2	-			
Signature Al	gorithm	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.g.) 2008/3/1 00:00:00 GMT	-			
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-			
Revoked	Serial Number	E.g.) 0123456789	-			
Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-			
	Reason Code	Revocation Reason Code (*)	-			
Extended fie	ld	Description of setting	critical			
CRL Number	c	CRL number	n			
Authority Ke	ey Identifier	SHA-1 hash for the issuer's Public Key	n			
		(160 bits)				
: The "Reason	Code" field is set o	ne of the Revocation Reason code specifie	ed in the t	able		
.2.2.1. If the F	Revocation Reason C	ode is "#0 unspecified", the "Reason Code"	field does	not		
ppear in the C	CRL profile.					
7.2.1 Versio	on Number(s)					

		整形版		
This Update Next Update		E.g.) 2008/3/1 00:00:00 GMT	-	
		E.g.) 2008/3/5 00:00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
·	Reason Code	Revocation Reason Code (*)	-	
Extended fiel	ld	Description of setting	critical	
CRL Number	 ۲	CRL number	n	
Authority Ke	y Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
The "Reason	Code" field is set o	one of the Revocation Reason code specifie	ed in the t	able
2.2.1. If the R	Revocation Reason C	Code is "#0 unspecified", the "Reason Code"	field does	not
ppear in the C	CRL profile.			
Гable 7.2.4 СF	RL Profile (applicabl	e to certificates issued by JPRS DV ECC C	A 2024 G1	or
PRS OV ECC	CA 2024 G1)			
Basic field		Description of setting	critical	
Version		Version 2	-	
Signature Al	gorithm	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.g.) 2008/3/1 00:00:00 GMT	-	
Next Update		E.g.) 2008/3/5 00:00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificates	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
	Reason Code	Revocation Reason Code (*)	-	
Extended fiel	ld	Description of setting	critical	
CRL Number	c	CRL number	n	
Authority Ke	ey Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
The "Reason	Code" field is set o	one of the Revocation Reason code specifie	ed in the t	able
2.2.1. If the R	Revocation Reason C	Code is "#0 unspecified", the "Reason Code"	field does	not
ppear in the C	CRL profile.			
721Vorein	on Number(s)			

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
	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.

	整形版	備考
The CA applies CRL version 2.		
7.2.2 CRL Entry Extensi	ons	
Use the CRL extension field iss		
reasonCode (OID 2.5.29.21)	-	
	n the reasonCode extension of the CRL entry correspond	ling
	t is revoked after July 15, 2023, unless the CRLReaso	
"unspecified (0)".		
The CA set one of the Revocat	tion Reason Code specified in the following table, with	the
exception of "unspecified (0)".		
Table 7.2.2.1 Revocation Reas	on 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	
#0 privilageWithdrown	discontinuing their website.	
#9 privilegeWithdrawn	When the Subscriber has not upheld their material obligations under the Terms and Conditions.	
	obligations under the ferms and conditions.	
7.3 OCSP Profile		
7.3.1 Version Number(s)		
The CA shall apply OCSP Versi	ion 1.	
7.3.2 OCSP Extensions		
Refer to Section 7.1 of this CP.		
The singleExtensions of an O	CSP response MUST NOT contain the reasonCode (DID
2.5.29.21) CRL entry extension		

7

変更履歴あり	整形版	備考
8. Compliance Audit and Other Assessments	8. Compliance Audit and Other Assessments	
JPRS shall perform audits at least once a year to verify whether or not the CA is operated in	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.	
Compliance audits shall be performed by auditors who are adequately experienced in auditing.	8.2 Identity/Qualifications of AssessorCompliance 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:	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 Auditors shall be operationally independent of the auditee divisions, except in matters related to the audits.	
8.4 Topics Covered by Assessment	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 	Baseline Requirementsへの準 拠を明確にするための修正
The CA shall promptly take necessary corrective actions with respect to any deficiencies	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

Stipulated in the CPS.

9.3.2 Information not within the Scope of Confidential Information

Stipulated in the CPS.

9.3.3 Responsibility to Protect Confidential Information

Stipulated in the CPS.

9.4 Privacy of Personal Information

Stipulated in the CPS.

9.5 Intellectual Property Rights

Unless separately agreed, all intellectual property rights pertaining to the following information shall belong to JPRS:
• certificates and site seals issued by the CA, as well as information on certificate

整形版

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 serperforming self audits on at least a quarterly basis against a randomly selected sa three percent of the Certificates issued by it during the period commencing imthe 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

Stipulated in the CPS.

9.3.2 Information not within the Scope of Confidential Inform Stipulated in the CPS.

9.3.3 Responsibility to Protect Confidential Information Stipulated in the CPS.

9.4 Privacy of Personal Information Stipulated in the CPS.

9.5 Intellectual Property Rights

Unless separately agreed, all intellectual property rights pertaining to information shall belong to JPRS:

- certificates and site seals issued by the CA, as well as information on \boldsymbol{c}

	備考	
ined to displace		
ired to disclose greement with		
cate Operation		
cate Operation		
a specific site		
a optimie and		
• • • •		
rvice quality by		
ample of at least		
nmediately after		
operating and		
operating and		
nation		
the following		
ertificate		

revocation;

- this CP, the CPS, and related documents;
- · Public Keys and Private Keys of the CA; and
- software provided by JPRS.

This CP is published under the Creative Commons license Attribution- NoDerivatives (CC-BY-ND) 4.0 International.



(<u>https://creativecommons.org/licenses/by-nd/4.0/</u>)

9.6 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:

- securely generate and manage the CA's Private Keys;
- accurately manage certificate issuance and revocation based on applications from the RA;
- monitor and operate the CA's system at work; and
- issue and publish the CRLs.

9.6.2 RA Representations and Warranties

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;
- accurately communicate information to the CA in processing applications for certificate issuance and revocation;
- promptly communicate information to the CA during operating hours in processing applications for certificate revocation; and
- maintain and administer the Repository.

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:

1. 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

- revocation;
- this CP, the CPS, and related documents;
- · Public Keys and Private Keys of the CA; and
- · software provided by JPRS.

This CP is published under the Creative Commons license Attribution-(CC-BY-ND) 4.0 International.



(<u>https://creativecommons.org/licenses/by-nd/4.0/</u>)

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The CA shall bear the following obligations in performing its business operat

- securely generate and manage the CA's Private Keys;
- accurately manage certificate issuance and revocation based on applica RA;
- monitor and operate the CA's system at work; and
- issue and publish the CRLs.

9.6.2 RA Representations and Warranties

The CA shall bear the following obligations in performing its business operation

- · install registration terminals in a secure environment and operate the
- accurately communicate information to the CA in processing application certificate issuance and revocation;
- promptly communicate information to the CA during operating hours i applications for certificate revocation; and
- · maintain and administer the Repository.

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 imposing Applicant itself (or made by the Applicant on behalf of its principal or agent under subcontractor or hosting service relationship) the following obligations and warra

1. Accuracy of Information: An obligation and warranty to provide accurate information at all times to the CA, both in the certificate request and as o requested by the CA in connection with the issuance of the Certificate(s)

整形版

	備考
NoDerivatives	
tions as the CA:	
ations from the	
tions as an RA:	
em;	
ons for	
in processing	
in processing	
se, that the	
efit of the CA	
on the	
er a	
anties:	
and a	
e and complete otherwise	
) to be supplied	
, 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.
- 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

by the CA;

- 2. **Protection of Private Key**: An obligation and warranty by the Applicant to reasonable measures to assure control of, keep confidential, and properly times the Private Key that corresponds to the Public Key to be included in Certificate(s) (and any associated activation data or device, e.g. password
- 3. Acceptance of Certificate: An obligation and warranty that the Subscriber and verify the Certificate contents for accuracy;
- Use of Certificate: An obligation and warranty to install the Certificate or that are accessible at the subjectAltName(s) listed in the Certificate, and Certificate solely in compliance with all applicable laws and solely in acco Subscriber Agreement or Terms of Use;
- 5. **Reporting and Revocation**: An obligation and warranty to: a. promptly rerevocation of the Certificate, and cease using it and its associated Private any actual or suspected misuse or compromise of the Subscriber's Private with the Public Key included in the Certificate, and b. promptly request r the Certificate, and cease using it, if any information in the Certificate is incorrect or inaccurate;
- 6. **Termination of Use of Certificate**: An obligation and warranty to prompth of the Private Key corresponding to the Public Key included in the Certificate for reasons of Key Compromise.
- 7. **Responsiveness**: An obligation to respond to the CA's instructions concer Compromise or Certificate misuse within a specified time period.
- 8. Acknowledgment and Acceptance: An acknowledgment and acceptance t entitled to revoke the certificate immediately if the Applicant were to viol the Subscriber Agreement or Terms of Use or if revocation is required by 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 2 assume all responsibilities therefor.

9.6.5 Representations and Warranties of Other Participants No stipulation.

9.7 Disclaimer of Warranties

整形版

	備考
to take all protect at all in the requested d or token);	
er will review	
nly on servers to use the ordance with the	
equest e Key, if there is e Key associated revocation of or becomes	
tly cease all use ficate upon	
rning Key	
that the CA is late the terms of y the CA's CP,	
of this CP. If Party shall	

整形版

The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential damage arising in | The CA is not liable for any indirect, special, incidental, or consequential, special, incidental, or consequential, special, incidental, special, 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
- · 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

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 of 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 us or any other cause not attributable to the CA;
- any damage resulting from a failure of a Subscriber to perform any of h 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 the 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 caus 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
- · any or all damage arising concomitantly with, or in connection with, re publication on the CT log server of information necessary for certificate

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 Condit policy on indemnification to Subscribers for damage.

9.10 Term and Termination

9.10.1 Term

	備考
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	
0 0	
ıch as business	
oint in time, in	
vare;	
ations due to a	
hquake,	
ivil commotion	
egistration and	
e issuance.	
the CA or any	
ng, and trusting	
abilities include	
ormance, or any	
ions stipulate a	

整形版

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.

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.

This CP shall come into effect upon approval by the CA's Certificate Operat This CP shall not lose its effect under any circumstances before its termina 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 i 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 shereof 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 verse which shall be deemed to be a notification thereof to Subscribers.

9.12.3 Circumstances under Which OID Must Be Changed

No stipulation.

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

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

9.15 Compliance with Applicable Laws

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

	備考
ion Conference.	
ation stipulated	
n "9.10.3 Effect	
II 9.10.5 Effect	
en a Subscriber	
should survive	
ribers, Relying	
ipants	
its Web site, by	
revised version	
Conference.	
sion of this CP,	
e, seeks to file a	
st the CA, such	
t shall have the	
irst instance.	
of Japan shall	
of a certificate.	
l law applicable	
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.

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

備考