CA Certificate Policy 新旧対照表 JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy(整形版)	備考 凡例: <u>赤字(下線付き)</u> :追加
JPRS CA Certificate Policy Version 3. <u>6</u> 50	JPRS CA Certificate Policy Version 3.60	<u>青字(取消線付き)</u> : 削除 バージョンの更新
<u>FebruaryAugust 2228</u> , 202 <mark>43</mark> Japan Registry Services Co., Ltd.	February 22, 2024 Japan Registry Services Co., Ltd.	実施日を修正

	JIKO	CA Certificate Policy(変更履歴付) Version History		JP	RS CA Certificate Policy(整形版) Version History	備考
Version Number	Date	Description	Version Number	Date	Description	
.00	2019.06.17	Publication of the first version	1.00	2019.06.17	Publication of the first version	
.10	2019.09.25	Revision of "3.2.2.4 Validation of Domain Authorization or	1.10	2019.09.25	Revision of "3.2.2.4 Validation of Domain Authorization or	
		Control" (adding the additional information of "general e-			Control" (adding the additional information of "general e-	
		mail address indicating an administrator"			mail address indicating an administrator"	
.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)	
.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"	
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"	
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	
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"	
21	2021.04.01	Revision of the date and version	2.21	2021.04.01	Revision of the date and version	
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)	
23	2021.05.27	 Clarification of "3.2.2.4 Validation of Domain Authorization or Control" Delete the description of invalid Subordinate CAs from 	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".			"7. Certificate, CRL, and OCSP Profiles".	
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"	
00	2021.12.08	Sunset of "subject:organizationalUnitName" Revisions due to new service provision	3.00	2021.12.08	Sunset of "subject:organizationalUnitName" Revisions due to new service provision	
10	2021.12.08	Add a reference to the new terms and conditions	3.10	2021.12.08	Add a reference to the new terms and conditions	
10	2022.03.02	Revision of the date and version	3.11	2022.03.02	Revision of the date and version	
20	2022.09.30	 Revision of "6.3 Other Aspects of Key Pair Management" Add description of Revocation Reason Code to be applied in this CA. 	3.20	2022.09.30	 Revision of "6.3 Other Aspects of Key Pair Management" Add description of Revocation Reason Code to be applied in this CA. 	
30	2023.04.24	• Revision of the maximum validity period of certificate	3.30	2023.04.24	• Revision of the maximum validity period of certificate	
40	2023.06.08	 Revision of "1.1 Overview" Revision of "7.3 OCSP Profile"	3.40	2023.06.08	 Revision of "1.1 Overview" Revision of "7.3 OCSP Profile"	
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	
. <u>60</u>	2024.02.22	Revision of "7. Certificate, CRL, and OCSP Profiles"	3.60	2024.02.22	Revision of "7. Certificate, CRL, and OCSP Profiles"	改訂履歴の追記
eferred t he Japai oes not	o as the "JPRS' rese texts of the guarantee the	te Policy" of Japan Registry Services Co., Ltd. (hereinafter) is an unofficial translation provided as reference, and only e statement have legal effect. Please kindly note that JPRS accuracy of this English translation in comparison to the Japanese language. JPRS may provide the revised English				記載を削除
olicy." If		e of revision for the same version of "JPRS CA Certificate on of "JPRS CA Certificate Policy" is published, please stop cument.				
able of _{中略)}	Contents		Table of (中略)	Contents		

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 RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." Table 1 1 List of Stands

Table	<u>1.1 List of Standards</u>
Types of certificates issued	Standards to comply with
by the CA	
	Baseline Requirements for the
	Issuance and Management of Publicly
	- Trusted TLS Server Certificates
TLS Server Certificate	Apple Root Certificate Program
	Chrome Root Program Policy
	Microsoft Trusted Root Program
	Mozilla Root Store Policy

If any inconsistency is found among the provisions of this CP, the Terms and Conditions, and the CPS, the provisions of the Terms and Conditions shall prevail over those of this CP and the CPS, and the provisions of this CP shall prevail over those of the CPS. Also, if any inconsistency is found among the provisions of the Japanese version and the English version of this CP, the English version shall prevail over the Japanese version. 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.

1.

1.1

TPRS CA Certi	ficate Policy(整形版)	備考
		UT S
1 Overview is document, the JPRS CA Certific pulates policies regarding the usages, rtificates to be issued by Japan Reg PRS") as a Certification Authority (he oviding the JPRS Digital Certificate ervices"). rious procedures regarding the opera e JPRS CA Certification Practice Stat certificate for one-way and mutual c mmunication RootCA2, Security Con ot CA 2024, a Certification Author	発行を受ける認証局を追加	
ereinafter referred to as "SECOM Trust Systems"), and the CA is authorized to issue rtificates to Subscribers. ertificates issued by the CA are used for encrypting information for server authentication d on communication pathways. "The Terms and Conditions of JPRS Digital Certificate suance Services" and "The Terms and Conditions of JPRS Digital Certificate Issuance rvices for ACME" (hereinafter, both will be referred to as the "Terms and Conditions") pulate the servers to be covered by the issuance of such certificates. the person who intends to have a certificate issued by the CA is required to consider the erms and Conditions, this CP, and the CPS in light of his/her/its own purposes of use, and en 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 anagement of Publicly-Trusted TLS Server Certificates" (hereinafter referred to as the aseline Requirements") published by CA/Browser Forum at https://www.cabforum.org/, d the Application Software Supplier Standards published."		Baseline Requirementsの正式名 称変更に合わせ修正
Types of certificates issued	.1 List of Standards Standards to comply with	当認証局が準拠するべき規準に関 する記載を追記
by the CA TLS Server Certificate	 Baseline Requirements for the Issuance and Management of Publicly Trusted TLS Server Certificates Apple Root Certificate Program Chrome Root Program Policy Microsoft Trusted Root Program Mozilla Root Store Policy 	
any inconsistency is found among the d the CPS, the provisions of the Term d the CPS, and the provisions of this consistency is found among the pro- rsion of this CP, the English version ent of any inconsistency between the t limited to, this CP, the CPS, the T d Baseline Requirements, Baselin cuments.	英語版が優先して適用される旨を 追記	
	ternet X.509 Public Key Infrastructure Certificate nework" advocated by the IETF as a framework for s.	
3/18		

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 requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.

1.3.3 Subscribers

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

1.3.4 Relying Parties

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

1.3.5 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

1.4.2 Prohibited Certificate Uses

Certificates issued by the CA may be used solely as set forth in "1.4.1 Appropriate Certificate Uses," and may not be used for any other purposes.

1.5 Policy Administration

IDPS CA Contificate Deliev	(教武氏)	備考
JPRS CA Certificate Policy With any developments or improvements pertaining to t		佣石
operation, this CP shall be revised, as needed, in orde improvements.		
1.2 Document Name and Identification The official name of this CP is the "JPRS CA Certificate I		
Following are an Object Identifier (hereinafter referred under this CP, and an OID of the CPS referenced by this	0	
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 certificates, discloses revocation information, provides certificate status using the OCSP (Online Certificate Stat protects the CA's own Private Keys, and registers Subscr	s and stores information on the tus Protocol) server, generates and	
1.3.2 RA		
"RA" stands for "Registration Authority," an entity that mainly performs reviews to verify the existence and validate the identities of applicants who apply for the issuance or revocation of certificates, registers information necessary for issuing certificates, and requests the CA to issue certificates, among the operations of the CA. The CA acts as an RA.		
1.3.3 Subscribers		
"Subscribers" means an individual, corporation, or organization that has been issued a certificate by the CA and uses the certificate. "Subscriber Certificate" means the certificate issued by the CA to the Subscribers.		
1.3.4 Relying Parties		
A "Relying Party" means an individual, corporation, validity of certificates issued by the CA.		
1.3.5 Other Participants		
No stipulation.		
1.4 Certificate Usage		
1.4.1 Appropriate Certificate Uses		
Certificates issued by the CA are used to encrypt information for server authentication and on communication pathways.		
1.4.2 Prohibited Certificate Uses		
Certificates issued by the CA may be used solely as Certificate Uses," and may not be used for any other purp		
1.5 Policy Administration		

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy(整形版)
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: Contact: Inquiries contact office, Japan Registry Services Co., Ltd. Address: Chiyoda First Bldg. East <u>13F</u> , 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101-0065 JAPAN	Inquiries concerning this CP should be directed to: Contact: Inquiries contact office, Japan Registry Services Co., Ltd. Address: Chiyoda First Bldg. East, 3-8-1 Nishi-Kanda, Chiyoda-ku, Tokyo 101
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 certificate issued by the CA is revealed, please notify via the following webform: <u>https://jprs.jp/pubcert/f_mail/</u>	If a compromise or unauthorized use of any Private Key or any other trouble a certificate issued by the CA is revealed, please notify via the following webfor <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 C
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
 1.6 Definitions and Acronyms <u>ACME (Automated Certificate Management Environment)</u> <u>"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.</u> <u>Archive</u> <u>"Archive" means information acquired for the purpose of keeping a history for any legal or other reason.</u> <u>Audit Log</u> 	 1.6 Definitions and Acronyms <u>ACME (Automated Certificate Management Environment)</u> "ACME" stands for "Automated Certificate Management Environment", a a CA and an applicant can use to automate the process of verification a issuance. This Protocol is specified in RFC 8555. <u>Archive</u> "Archive" means information acquired for the purpose of keeping a history or other reason. <u>Audit Log</u>
 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. <u>Authorization Domain Name</u> 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.	An "Audit Log" is a log of actions, accesses, and other histories p Certification Authority systems that are recorded for the purpose of monito to, and unauthorized operations of, Certification Authority systems. <u>Authorization Domain Name</u> The Domain Name used to obtain authorization for certificate issuance FQDN. The CA may use the FQDN returned from a DNS CNAME lookup for the purposes of domain validation. If the FQDN contains a wildcard ch the CA MUST remove all wildcard labels from the left most portion of requ The CA may prune zero or more labels from left to right until encount Domain Name and may use any one of the intermediate values for the purp validation.
<u>Base Domain Name</u> <u>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. <u>"example.co.uk" or "example.com"</u>). 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.</u>	<u>Base Domain Name</u> The portion of an applied-for FQDN that is the first domain name node left controlled or public suffix plus the registry-controlled or public "example.co.uk" or "example.com"). For FQDNs where the right-most doma is a gTLD having ICANN Specification 13 in its registry agreement, the gT be used as the Base Domain Name.
<u>CA (Certification Authority)</u> <u>"CA" stands for "Certification Authority," an entity that mainly issues, renews, and revokes certificates, discloses information on certificate revocation, provides and stores</u>	<u>CA (Certification Authority)</u> "CA" stands for "Certification Authority," an entity that mainly issues, revokes certificates, discloses information on certificate revocation, provid

	lite -tw
	加石
01-0065 JAPAN	住所を修正
le pertaining to oform:	
Conference.	
on Conference.	
a protocol that and certificate	記載順の見直し
ory for any legal	
pertaining to itoring accesses	
nce for a given p as the FQDN character, then quested FQDN. ntering a Base rpose of domain	
eft of a registry- ic suffix (e.g. nain name node gTLD itself may	
es, renews, and ides and stores	

information on the status of certificates using the OCSP (Online Certificate Status Protocol) server, generates and protects the CA's own Private Keys, and registers Subscribers.

CAA (Certificate Authority Authorization)

<u>"CAA" stands for "Certificate Authority Authorization," a function to prevent</u> <u>unintended erroneous issuance of certificates from unauthorized Certification</u> <u>Authorities in connection with the authority to use a domain by adding information to</u> <u>the DNS record in order to specify the Certification Authority authorized to issue a</u> <u>certificate for the domain. This function is stipulated in RFC 6844.</u>

CP (Certificate Policy)

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

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)

<u>"CT" stands for "Certificate Transparency," a scheme stipulated in RFC 6962 to register</u> 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

<u>A "Digital Certificate" means digital data certifying that a Public Key is possessed by the</u> 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.

Escrow

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

<u>FIPS 140-2</u>

<u>"FIPS 140-2" are a set of security accreditation criteria for cryptographic modules</u> 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)

<u>A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.</u>

<u>HSM (Hardware Security Module)</u> <u>"HSM" stands for "Hardware Security Module," a tamper-resistant encryption device to</u>

JPRS CA Certificate Policy (整形版)

information on the status of certificates using the OCSP (Online Cer Protocol) server, generates and protects the CA's own Private Keys, Subscribers.

CAA (Certificate Authority Authorization)

"CAA" stands for "Certificate Authority Authorization," a function unintended erroneous issuance of certificates from unauthorized Authorities in connection with the authority to use a domain by adding the DNS record in order to specify the Certification Authority authoric certificate for the domain. This function is stipulated in RFC 6844.

CP (Certificate Policy)

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

CPS (Certification Practices Statement)

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

CRL (Certificate Revocation List)

"CRL" stands for "Certificate Revocation List," a list of information abrevoked during their period of validity for any reason, including cl particulars described in the certificates or the compromise of any Private H

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) to 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 assursignature 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.

<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

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

	備老
rtificate Status , and registers	Umity
ion to prevent d Certification g information to rized to issue a	
licies regarding ervers for which pplying for the	
that sets forth onal procedures	
bout certificates changes in the Keys.	
6962 to register for the purpose	
possessed by the red by a digital	
s widely used as	用語定義の追加
control of an	
raphic modules nd Technology). lefined.	
in the Internet	
yption 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>

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

NTP (Network Time Protocol)

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

OCSP (Online Certificate Status Protocol)

<u>"OCSP" stands for "Online Certificate Status Protocol," a protocol for providing</u> 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 and administering the connectivity of networks and the uniqueness of services or the like.

PKI (Public Key Infrastructure)

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

Private Key

<u>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.</u> <u>A Private Key may be referred to as a "secret key."</u>

Public Key

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

RA (Registration Authority)

<u>"RA" stands for "Registration Authority," an entity that mainly performs reviews to</u> 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)

<u>"RFC 3647" stands for "Request for Comments 3647," a document defining the</u> framework for CP and CPS published by the IETF (Internet Engineering Task Force), an

JPRS CA Certificate Policy (整形版)

be used for generating, storing, using, or otherwise handling Private purpose of maintaining security.

JPRS Partners

"JPRS Partners" mean business enterprises authorized by JPRS in conne 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 is cryptosystem.

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.

OID (Object Identifier)

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

PKI (Public Key Infrastructure)

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

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 A Private Key may be referred to as a "secret key."

<u>Public Key</u>

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

RA (Registration Authority)

"RA" stands for "Registration Authority," an entity that mainly perfor verify the existence and validate the identities of applicants who apply for or revocation of certificates, registers information necessary for issuing cor 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

Repository

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 T

e Keys for the	備考
nection with the	
in a public key	
synchronize the	
l for providing	
nal registration for maintaining services or the	
g the encryption nologies such as	
stem. A Private son in question.	
ystem. A Public other party to	
orms reviews to for the issuance certificates, and	
f entropy.	
and others are	
nt defining the 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.

<u>RSA</u>

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

SHA-1 (Secure Hash Algorithm 1)

<u>"SHA-1" stands for "Secure Hash Algorithm 1," one of the hash functions</u> (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)

<u>"SHA-256"</u> 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

<u>A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.</u>

Wildcard Domain Name

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

(1) "あ" ~ "ん"

<u>アーカイブ (Archive)</u>

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

エスクロー (Escrow)

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

鍵ペア (Key Pair)

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

<u>監査ログ (Audit Log)</u>

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

JPRS CA Certificate Policy (整形版)

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.

<u>RSA</u>

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

SHA-1 (Secure Hash Algorithm 1)

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

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 n its 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 Subject 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.

	備老
	via - J
ning the public ce), an industry	
idely used as a	
hash functions a computation pit length is one s in an original cansmitted and	
hash functions undred fifty-six message during	
n, for example, g.	
ject Alternative	
P) immediately	

公開鍵 (Public Key) A "Public Key" means a key of a Key Pair used in a public key cryptosystem. A Public Key corresponds to a cortain Private Key and is disclosed to the other party to communication. 指定事業者 (IPRS Partners) "JPRS Partners" mean business enterprises authorized by JPRS in connection with the Digital Certificate Issuance Services to be provided by JPRS. 私有鏈 (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." タイムスタンプ (Time Stamp) "Time Stamp" means recorded data indicating dates and times when, for example, electronic files have been prepared and a system has performed processing. 電子証明書 (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. ランダム値 (Random Value) A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy. リポジトリ (Repository) The "Repository" means the database in which CA certificates, CRLs, and others are stored and published. ワイルドカード証明書 (Wildcard Cortificate) A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate. ワイルドカードドメイン名 (Wildcard Domain Name) A string starting with "*." (U+002A ASTERISK, U+002E FULL STOP) immediately followed by a Fully-Qualified Domain Name. (2) "A" ~ "Z" 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. **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.

JPRS CA Certificate Policy (変更履歴付)

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.

備考

Base Domain Name

The portion of an applied-for FQDN that is the first domain name node left of a registrycontrolled or public suffix plus the registry-controlled or public suffix (e.g.

"example.co.uk" or "example.com"). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

CA (Certification Authority)

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

CAA (Certificate Authority Authorization)

"CAA" stands for "Certificate Authority Authorization," a function to prevent unintended erroneous issuance of certificates from unauthorized Certification Authorities in connection with the authority to use a domain by adding information to the DNS record in order to specify the Certification Authority authorized to issue a certificate for the domain. This function is stipulated in RFC 6844.

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

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

CPS (Certification Practices Statement)

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

CRL (Certificate Revocation List)

"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.

FIPS 140-2

"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.

備考

JPRS CA Certificate Policy (整形版)

NTP (Network Time Protocol)

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

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 and administering the connectivity of networks and the uniqueness of services or the like.

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.

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.

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.

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.

<u>RSA</u>

"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.

備考
L]

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

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

2.3 Time or Frequency of Publication

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

The frequency of CRL issuance is specified in Section 4.9.7.

2.4 Access Controls on Repositories

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

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

3.1.2 Need for Names to Be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

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 does not verify whether an applicant holds any intellectual property right to the name described in a certificate application. No Subscriber may submit to the CA a certificate application with any registered trademark or associated name of any third certificate application with any registered trademark or associated name

JPRS CA Certificate Policy (整形版)

2. Publication and Repository Responsibilit

2.1 Repository

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

2.2 Publication of Information

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

2.3 Time or Frequency of Publication

This CP and the CPS shall be revised at least annually and published on the revised. The CA describes to the CP and the CPS in detail how the CA i 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 pu Repository. The CA's CRLs shall be made available to Subscribers and 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 configured according to the Distinguished Name (DN) format for the recommendations (recommendations formulated by the International Tele 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 meanin 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 stipulat 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 prope name described in a certificate application. No Subscriber may submi

	備考
ties	
ame twenty-four wever, that the enance or other	
to allow online	
ne Repository as implements the	
ublished on the Relying Parties a general Web	
the CA shall be e X.500 series ecommunication	
ags are specified	
be issued by the	
te the rules for	
to be issued by	
S	
erty right to the it to the CA a ne of any third	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy(整形版)	備考
party. If any dispute arises between a Subscriber and any third party in connection with a	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	
ispute. The CA is entitled to reject a Subscriber's certificate application or to revoke an	dispute. The CA is entitled to reject a Subscriber's certificate application or to revoke an	
ssued certificate on account of such a dispute.	issued certificate on account of such a dispute.	
8.2 Initial Identity Validation	3.2 Initial Identity Validation	
3.2.1 Method to Prove Possession of a Private Key	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	
elevant Certificate Signing Request (hereinafter referred to as "CSR") and confirming that	relevant Certificate Signing Request (hereinafter referred to as "CSR") and confirming that	
he CSR has been signed with the Private Key corresponding to the Public Key contained	the CSR has been signed with the Private Key corresponding to the Public Key contained	
n the CSR.	in the CSR.	
3.2.2 Authentication of Organization and Domain Identity	3.2.2 Authentication of Organization and Domain Identity	
	The CA SHALL inspect any document relied upon under this Section for alteration or	
alsification.	falsification.	
3.2.2.1 Authentication of Organization Identity	3.2.2.1 Authentication of Organization Identity	
1) Domain Validation	(1) Domain Validation	
The CA does not verify the existence of organizations.	The CA does not verify the existence of organizations.	
2) Organization Validation by CA shall verify the existence of organizations by using public documents issued by or	(2) Organization Validation The CA shall verify the existence of organizations by using public documents issued by or	
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 <u>using</u>	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 <u>using</u>	
equiries made by any third party that is deemed reliable by the CA, or the databases of	inquiries made by any third party that is deemed reliable by the CA, or the databases of	
ny such third party.	any such third party.	
3.2.2.2 DBA/Tradename	3.2.2.2 DBA/Tradename	
	If a DBA/tradename is described as the "Organization (organization name)" in a certificate	
o be issued by the CA, the CA shall verify the information same manner as set forth in	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."	"3.2.2.1 Authentication of Organization Identity (2) Organization Validation."	
3.2.2.3 Verification of a Country	3.2.2.3 Verification of a Country	
	The CA shall verify the information on the "Country (country name)" in a certificate to in	
he same manner as set forth in "3.2.2.1 Authentication of Organization Identity."	the same manner as set forth in "3.2.2.1 Authentication of Organization Identity."	
3.2.2.4 Validation of Domain Authorization or Control	3.2.2.4 Validation of Domain Authorization or Control	
The CA SHALL confirm that prior to issuance, the CA has validated each FQDN listed in	The CA SHALL confirm that prior to issuance, the CA has validated each FQDN listed in	
he Certificate using at least one of the methods listed below;	the Certificate using at least one of the methods listed below;	
Subsequent sections 3.2.2.4.1-20 correspond to the section numbers of the methods pecified by BR.	Subsequent sections 3.2.2.4.1-20 correspond to the section numbers of the methods specified by BR.	
'he 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	
ncluded in the certificates.	included in the certificates.	
The CA SHALL maintain a record of which domain validation method, including relevant	The CA SHALL maintain a record of which domain validation method, including relevant	
BR version number, they used to validate every domain.	BR version number, they used to validate every domain.	
3.2.2.4.1 Validating the Applicant as a Domain Contact	3.2.2.4.1 Validating the Applicant as a Domain Contact	
Not applicable	Not applicable	
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact Confirming the Applicant's control over the FQDN by sending a Random Value via	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	email and then receiving a confirming response utilizing the Random Value. The	
Random Value MUST be sent to an email address listed in the WHOIS record.	Random Value MUST be sent to an email address listed in the WHOIS record.	
The CA does not use fax, SMS, or postal mail to send a Random Values.	The CA does not use fax, SMS, or postal mail to send a Random Values.	
The Random Value SHALL be unique in each email. The Random Value SHALL	The Random Value SHALL be unique in each email. The Random Value SHALL	
remain valid for use in a confirming response for no more than 25 days from its	remain valid for use in a confirming response for no more than 25 days from its	
creation.	creation.	
3.2.2.4.3 Phone Contact with Domain Contact Not applicable	3.2.2.4.3 Phone Contact with Domain Contact Not applicable	
3.2.2.4.4 Constructed Email to Domain Contact	3.2.2.4.4 Constructed Email to Domain Contact	

Confirm the Applicant's control over the FQDN by 1. 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 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. 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 3.2.2.4.9 Test Certificate Not applicable 3.2.2.4.10 TLS Using a Random ValueNumber Not applicable Not applicable 3.2.2.4.11 Any Other Method Not applicable 3.2.2.4.12 Validating Applicant as a Domain Contact Confirming the Applicant's control over the FQDN by validating the Applicant is the registrant of the domain name. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name. 3.2.2.4.13 Email to DNS CAA Contact Not applicable 3.2.2.4.14 Email to DNS TXT Contact Not applicable Not applicable 3.2.2.4.15 Phone Contact with Domain Contact Not applicable 3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact Not applicable 3.2.2.4.17 Phone Contact with DNS CAA Phone Contact Not applicable 3.2.2.4.18 Agreed-Upon Change to Website v2 Confirming the Applicant's control over the FQDN by verifying that the Random Value is contained in the contents of a file. 1. The entire Random Value MUST NOT appear in the request used to retrieve the file, and 2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received). The file containing the Random Value: 1. MUST be located on the Authorization Domain Name, and 2. MUST be located under the "/.well-known/pki-validation" directory, and 3. MUST be retrieved via either the "http" or "https" scheme, and 4. MUST be accessed over port 80 (http) or 443 (https).

If the CA follows redirects, the following apply:

JPRS CA Certificate Policy (整形版)

Confirm the Applicant's control over the FQDN by

- 1. 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
- 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

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 than 25 days from its creation.

3.2.2.4.8 IP Address

Not applicable

3.2.2.4.9 Test Certificate

- Not applicable
- 3.2.2.4.10 TLS Using a Random Value

3.2.2.4.11 Any Other Method

Not applicable

3.2.2.4.12 Validating Applicant as a Domain Contact

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

3.2.2.4.13 Email to DNS CAA Contact

Not applicable

3.2.2.4.14 Email to DNS TXT Contact

- 3.2.2.4.15 Phone Contact with Domain Contact Not applicable
- 3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact Not applicable
- 3.2.2.4.17 Phone Contact with DNS CAA Phone Contact Not applicable

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that Value is contained in the contents of a file.

- 1. The entire Random Value MUST NOT appear in the request u the file, and
- 2. the CA MUST receive a successful HTTP response from the rec a 2xx HTTP status code must be received).

The file containing the Random Value:

- 1. MUST be located on the Authorization Domain Name, and
- 2. MUST be located under the "/.well-known/pki-validation" direct
- 3. MUST be retrieved via either the "http" or "https" scheme, and
- 4. MUST be accessed over port 80 (http) or 443 (https).
- If the CA follows redirects, the following apply:

	備考
using 'admin', the local part, Domain Name;	
1 Value SHALL 5 days from its	
C.	
ne presence of a n Name that is	
e request. The ise for no more	
	Baseline Requirementsの表記変 更に合わせ修正
Applicant is the e CA is also the Domain Name.	
at the Random	
used to retrieve	
quest (meaning	
ctory, and d	

- 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).

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 6454 Section 8.2 for further explanation).

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

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

3.2.2.7 Data Source Accuracy

JPRS CA Certificate Policy (整形版)

1. Redirects MUST be initiated at the HTTP protocol layer.

- Redirects MUST be the result of a 301, 302, or 307 HT response, as defined in RFC 7231, Section 6.4, or a 308 code response, as defined in RFC 7538, Section 3.
- Redirects MUST be to the final value of the Location H header, as defined in RFC 7231, Section 7.1.2.
- 2. Redirects MUST be to resource URLs with either the "ht 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 responthan 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 I response header, as defined in RFC 7231, Section
 - 2. Redirects MUST be to resource URLs with either the "h scheme.
 - 3. Redirects MUST be to resource URLs accessed via port 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 6454 Section 8.2 for further explanation).

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

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

3.2.2.7 Data Source Accuracy

	備考
TTP status code 08 HTTP status	
HTTP response	
http" or "https"	
0 (http) or 443	
e request. The use for no more	
t applicable for	
in control of the 8.3 of RFC 8555.	
m the request	
tificate request. ing response for	
07 HTTP status n 6.4, or a 308 338, Section 3. Location HTTP 7.1.2. http" or "https" 80 (http) or 443	
5.	
y a documented n Name in the co.uk", see RFC	
" or is a "public ıl control of the , but MAY issue	
on of a Country nts.	

JPRS CA Certificate Policy (変更履歴付) JPRS CA Certificate Policy (整形版) Prior to using any data source as a Reliable Data Source, the CA SHAL 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 falsific 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 proce in accordance with RFC 8659 for each dNSName in the subjectAltName extension that in accordance with RFC 8659 for each dNSName in the subjectAltName does not contain an Onion Domain Name. If the CA issues, they MUST do so within the does not contain an Onion Domain Name. If the CA issues, they MUST do TTL of the CAA record, or 8 hours, whichever is greater. TTL of 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, issuew 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 iddef property tag. Where are additional property tags are supported, the CA MUST NOT iodef property tag. Where are additional property tags are supported, the C 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 R 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 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 IC The CA shall log any actions taken as part of its processing practices. The CA shall log any actions taken as part of its processing practices. 3.2.3 Authentication of Individual Identity 3.2.3 Authentication of Individual Identity The CA does not issue any certificate to grant certification to any individual. The CA does not issue any certificate to grant certification to any individual. 3.2.4 Non-Verified Subscriber Information 3.2.4 Non-Verified Subscriber Information (1) Domain Validation (1) Domain Validation The CA stipulates no policies on non-verified information on Subscribers. The CA stipulates no policies on non-verified information on Subscribers. (2) Organization Validation (2) Organization Validation The CA stipulates no policies on non-verified information on Subscribers, however, an The CA stipulates no policies on non-verified information on Subscribers. does not assure the accuracy of information described in the "Organizational Univ (organizational unit name)" (OU). 3.2.5 Validation of Authority 3.2.5 Validation of Authority (1) Domain Validation (1) Domain Validation When issuing a certificate, the CA shall verify that the Subscriber is a registrant of the When issuing a certificate, the CA shall verify that the Subscriber is a re domain name to be described in the certificate or has been granted an exclusive right to domain name to be described in the certificate or has been granted an exc use the domain name by the registrant. use the domain name by the registrant. (2) Organization Validation (2) Organization Validation The CA shall verify that an applicant for a certificate has the legitimate aut

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 A certificate for one-way mutual certification has been issued to the C Communication RootCA2, Security Communication ECC RootCA1 or SECOM TLS RSA Communication RootCA2, Security Communication ECC RootCA1 or SEC

	准去
JPRS CA Certificate Policy (整形版) Prior to using any data source as a Reliable Data Source, the CA SHALL evaluate the	備考
source for its reliability, accuracy, and resistance to alteration or falsification. The CA	
considers the following during its evaluation:	
 The age of the information provided, The frequency of updates to the information source, 	
3. The data provider and purpose of the data collection,	
4. The public accessibility of the data availability, and	
5. The relative difficulty in falsifying or altering the data.	
3.2.2.8 CAA Records	
As part of the Certificate issuance process, the CA MUST retrieve and process CAA records	
in accordance with RFC 8659 for each dNSName in the subjectAltName extension that	
does not contain an Onion Domain Name. If the CA issues, they MUST do so within the	
TTL of the CAA record, or 8 hours, whichever is greater.	
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	
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.	
The CA MUST respect the critical flag and not issue a certificate if they encounter an	
unrecognized property tag with this flag set.	
The CA permitted to treat a record lookup failure as permission to issue if	
 the failure is outside the CA's infrastructure; 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 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	訂明書。の回道日の記書は成正文
The CA stipulates no policies on non-verified information on Subscribers.	証明書へのOU項目の記載は廃止済 みのため記載を削除
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	発行を受ける認証局を追加

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版)	備考
Root CA 2024, a Certification Authority operated by SECOM Trust Systems.	Root CA 2024, a Certification Authority operated by SECOM Trust Systems.	加中有
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.	3.3 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 account granted to the subscriber. 	 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 account granted to the subscriber. 3. The certificate issued under ACME protocol and the Revocation Request is signed by private key of the certificate. 	
4. Certificate Life-Cycle Operational Requirements	4. 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 A person who is a registrant of the domain name to be described in a certificate or has been granted an exclusive right to use the domain name by the registrant may apply for the certificate. (2) Organization Validation A person who is an sole proprietor individual 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. 	 granted an exclusive right to use the domain name by the registrant may apply for the certificate. (2) Organization Validation A person who is a sole proprietor having his/her address within Japan, or an organization having its head office or principal office, branch office or subdivision, place of business, or	
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 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.	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	
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 set forth in "3.2 Initial Identity Validation" of this CP. The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.	set forth in "3.2 Initial Identity Validation" of this CP. The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. The CA SHALL	
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.	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.	

4

4.

4

(1)

ce (2)

4

4.

4

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy(整形版)	備考
The CA MAY use the documents and data provided in Section 3.2 of this CP to verify certificate information, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 of this CP or	Section 6.3.2 of this CP limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 of this CP to verify certificate information, or may reuse previous validations themselves, provided that the CA obtained the data or document from a source specified under Section 3.2 of this CP or completed the validation itself no more than 825 days prior to issuing the Certificate.	
document, or completed validation MUST be obtained no more than 398 days prior to issuing the Certificate. In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or	For validation of Domain Names according to Section 3.2.2.4 of this CP, any reused data, document, or completed validation MUST be obtained no more than 398 days prior to issuing the Certificate. In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.	
and require additional verification activity for High Risk Certificate Requests prior to the	The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.	
4.2.2 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 the issuance registration of the certificate.	On approving any certificate application as a result of the review, the CA shall proceed to the issuance registration of the certificate.	
	If any certificate application is not complete, the CA shall reject the application and request the person who has submitted the application to submit an application again after 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 the certificate in a timely manner.	
4.2.4 Check of CAA Records	4.2.4 Check of CAA Records	
The Certificate Subscribers who want to grant the authority to issue certificates to the		
4.3 Certificate Issuance	4.3 Certificate Issuance	
4.3.1 CA Actions during Certificate Issuance	4.3.1 CA Actions during Certificate Issuance	
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	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.	
4.3.2 Notification to Subscriber of Certificate Issuance	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.	
F		

4.4.1 Conduct Constituting 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;	The Subscriber shall be deemed to have accepted the certificate at any o time;
 When the Subscriber requests to get the certificate from the subscriber-only web page and the CA responses the Certificate. 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. 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	4.4.2 Publication of the Certificates by the CA
The CA does not publish certificates of Subscribers.	The CA does not publish certificates of Subscribers.
4.4.3 Notification of Certificate Issuance by the CA to Other Entities	4.4.3 Notification of Certificate Issuance by the CA to Other
The CA does not notify any third party (excluding Designated Business Enterprises) of the issuance of certificates.	The CA does not notify any third party (excluding Designated Business Ensuance of certificates.
4.5 Key Pair and Certificate Usage	4.5 Key Pair and Certificate Usage
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 Private Key solely for encrypting information for server authentication and on communication pathways, and not for any other usage.	Each Subscriber may use his/her/its certificate issued by the CA and the Private Key solely for encrypting information for server authentic 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 the CPS before verifying the reliability of certificates issued by the CA and relying on the same.	Relying Parties may verify the reliability of certificates issued by the CA certificates. Relying Parties shall understand and consent to the provisions the CPS before verifying the reliability of certificates issued by the CA and same.
4.6 Certificate Renewal	4.6 Certificate Renewal
A "certificate renewal" means the issuance of a new certificate to a Subscriber without any change in his/her/its Public Key. When a Subscriber has his/her/its certificate renewed, the CA recommends that the Subscriber generate a new Key Pair.	
4.6.1 Circumstances for Certificate Renewal	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 certific 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 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.	The provisions of "4.3.1 CA Actions during Certificate Issuance" of this 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 apply correspondingly.	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" apply correspondingly.
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate	4.6.5 Conduct Constituting Acceptance of a Renewal Certif

JPRS CA Certificate Policy(整形版)

	備考
of the following	
criber-only web	
protocol and the d under ACME	
ther than 1 and	
r Entities	
terprises) of the	
e corresponding cation and on	
A by using such s of this CP and d relying on the	
ber without any te renewed, the	
ate is about to	
CP shall apply	
CP shall apply	
of this CP shall	
icate	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy(整形版)	備考
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 correspondingly.	The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.	
4.6.7 Notification of Certificate Issuance by the CA to Other Entities	4.6.7 Notification of Certificate Issuance by the CA to Other Entities	
The provisions of "4.4.3 Notification of Certificate Issuance by the CA to Other Entities" of 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.	
4.7 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	

	JPRS CA Certificate Policy (整形版) The provisions of "4.3.1 CA Actions during Certificate Issuance" of this CP shall apply correspondingly.
4.8.4 Notification of New Certificate Issuance to Subscriber	4.8.4 Notification of New Certificate Issuance to Subscriber
he provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall 's oply correspondingly.	The provisions of "4.3.2 Notification to Subscriber of Certificate Issuance" of this CP shall 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 correspondingly.
4.8.6 Publication of the Modified Certificate by the CA	4.8.6 Publication of the Modified Certificate by the CA
	The provisions of "4.4.2 Publication of the Certificates by the CA" of this CP shall apply correspondingly.
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 this CP shall apply correspondingly.
I.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 corresponding certificate revoked: the information described in the certificate has changed; 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; 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 Names" of this CP) (for Organization Validation only); or the Subscriber stops using the certificate.
The CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:	The CA SHALL revoke a Certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:
1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);	1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);	2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn);
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);	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 (such as a Debian weak key, see <u>https://wiki.debian.org/SSLkeys</u>) (CRLReason #1,	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 (such as a Debian weak key, see <u>https://wiki.debian.org/SSLkeys</u>) (CRLReason #1, keyCompromise);
keyCompromise);	

within 5 days and use the corresponding CRLR eason 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);
- 7. 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 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

- 17. 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, su
- 18. The CA obtains evidence that the Certificate was misused (CRLRease privilegeWithdrawn);
- 19. The CA is made aware that a Subscriber has violated one or more of i obligations under the Subscriber Agreement or Terms of Use (CRLRe privilegeWithdrawn);
- 20. The CA is made aware of any circumstance indicating that use of a Fe 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 b (CRLReason #5, cessationOfOperation);
- 21. The CA is made aware that a Wildcard Certificate has been used to a fraudulently misleading subordinate FQDN (CRLReason #9, privileg
- 22. The CA is made aware of a material change in the information contai Certificate (CRLReason #9, privilegeWithdrawn);
- 23. The CA is made aware that the Certificate was not issued in accordan Requirements or the CA's CP or CPS(CRLReason #4, superseded);
- 24. The CA determines or is made aware that any of the information app Certificate is inaccurate (CRLReason #9, privilegeWithdrawn);
- 25. 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)" in no reasonCode extension being provided in the CRL);
- 26. Revocation is required by the CA's Certificate Policy and/or Certificate Statement for a reason that is not otherwise required to be specified 1 4.9.1.1 of Baseline Requirements (CRLReason "unspecified (0)" which reasonCode extension being provided in the CRL); or
- 27. 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 t 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 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 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 be compromised, he/she/it must promptly file the Revocation Request of the of The CA SHALL maintain a continuous 24x7 ability to accept and respond

JPRS CA Certificate Policy (整形版) within 5 days and use the corresponding CRLReason if one or more of the fo

	備考
ollowing occurs:	
perseded);	
son #9,	
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
its material	
eason #9,	
FQDN in the	
as revoked a	
nt licensing or Applicant has	
Domain Name)	
authenticate a	
geWithdrawn);	
ined in the	
• • • • •	
ince with these	
pearing in the	
pearing in the	
pires or is	
itinue	
" which results	
tion Practice	
by this section h results in no	
n results in no	
oses the	
that the specific	
l,	
the application	
owing way and	
owing way, and 4.	
1.	
,	
as been or may	
certificate. Id to revocation	
in to revolation	

requests and Certificate Problem Reports.

4.9.5 Time within Which the CA Shall Process the Revocation Request

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

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

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-line Revocation/Status Checking Availability

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

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

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

4.9.10 On-line Revocation/Status Checking Requirements

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

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

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

4.9.5 Time within Which the CA Shall Process the Revocation

Upon accepting a valid Revocation Request of a certificate, the CA shall pr 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 s any entity reporting the Certificate Problem Report or other revocation-re establish whether or not the certificate will be revoked, and if so, a date whi revoke the certificate. The period from receipt of the Certificate Probl revocation-related notice to published revocation MUST NOT exceed the t forth in Section 4.9.1.1 of this CP.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

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

4.9.8 Maximum Latency for CRLs

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

4.9.9 On-line Revocation/Status Checking Availability

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

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

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

4.9.10 On-line Revocation/Status Checking Requirements

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

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

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

JPRS CA Certificate Policy (整形版) requests and Certificate Problem Reports.

	備考
on Request	
romptly process te on the CRL. ALL investigate and provide a y who filed the	
e Subscriber and related notice to hich the CA will blem Report or time frame set	
S	
osued by the CA. Ving Party must tain information	
and the value of le value of the	
server. esponses MUST	
tatus is being	
CA that issued	
nsion of type id-	
arty must verify ether or not the included in the status provided	
od, as described	
time between ting differences, f 86,400 seconds	

		14 ×
JPRS CA Certificate Policy (変更履歴付) shall be equal to one day, ignoring leap-seconds.	JPRS CA Certificate Policy (整形版) shall be equal to one day, ignoring leap-seconds.	備考
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;	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;	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.	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.	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.	If the OCSP responder receives a request for the status of a certificate serial number that is "unused", then the responder SHOULD NOT respond with a "good" status. If the OCSP responder is for a CA that is not Technically Constrained in line with <u>Section 7.1.2.3</u> or <u>Section 7.1.2.5</u> , the responder MUST NOT respond with a "good" status for such requests.	
The CA SHOULD monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.	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].	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:	A certificate serial number within an OCSP request is one of the following three options:	
1. "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	1. "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 a. the Issuing CA; or b. a Precertificate Signing Certificate, as defined in <u>Section</u> <u>7.1.2.4</u>, associated with the Issuing CA; or 	 "reserved" if a Precertificate [RFC 6962] with that serial number has been issued by a. the Issuing CA; or b. a Precertificate Signing Certificate, as defined in <u>Section</u> <u>7.1.2.4</u>, associated with the Issuing CA; or 	
3. "unused" if neither of the previous conditions are met.	3. "unused" if neither of the previous conditions are met.	
4.9.11 Other Forms of Revocation Advertisements Available	4.9.11 Other Forms of Revocation Advertisements Available	
Not applicable.	Not applicable.	
4.9.12 Special Requirements Regarding Key Compromise	4.9.12 Special Requirements Regarding Key Compromise	
If a compromise of any Private Key pertaining to a certificate issued by the CA is revealed, please notify via the following webform: <u>https://jprs.jp/pubcert/f_mail/</u> Please include either of the following information in your report.	If a compromise of any Private Key pertaining to a certificate issued by the CA is revealed, please notify via the following webform: <u>https://jprs.jp/pubcert/f_mail/</u> Please include either of the following information in your report.	
 The compromised private key itself A CSR signed by the compromised private key (A CSR must contain a string indicating that a private key has been compromised in the "CN" field. e.g. CN="This key is compromised") 	 The compromised private key itself A CSR signed by the compromised private key (A CSR must contain a string indicating that a private key has been compromised in the "CN" field. e.g. CN="This key is compromised") 	
The CA shall verify whether any of the certificates issued by the CA use the presented private key. Upon confirmation of a certificate that uses the presented private key, the CA shall revoke the certificate within 24 hours from the time of confirmation.		
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.	

JPRS CA Certificate Policy(変更履歴付)	JPRS CA Certificate Policy (整形版) 備考
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.
1.10 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 chrough the OCSP server. Revocation entries on a CRL or OCSP Response MUST NOT be removed until after the Expiry Date of the revoked Certificate.	through the OCSP server.
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 information on the status of a certificate twenty-four (24) hours a day, three hundred sixty- five (365) days a year. However, the OCSP server may be temporarily unavailable at times for maintenance or other reasons. The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.	information on the status of a certificate twenty-four (24) hours a day, three hundred sixty- five (365) days a year. However, the OCSP server may be temporarily unavailable at times for maintenance or other reasons. The CA SHALL operate and maintain its CRL and OCSP capability with resources
The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.	The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.
The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority 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.	
4.10.3 Optional Features	4.10.3 Optional Features
lo stipulation.	No stipulation.
4.11 End of Subscription (Registration) If a Subscriber ceases to use his/her/its certificate, or cancels the Services, the Subscriber shall request for revocation of his/her/its certificate. If a Subscriber fails to carry procedures for certificate renewal and his/her/its certificate expires, the certificate registration shall terminate. 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.	 shall request for revocation of his/her/its certificate. If a Subscriber fails to carry procedures for certificate renewal and his/her/its certificate expires, the certificate registration shall terminate. However, the CA may treat a Subscriber who has been issued a certificate under ACME
1.12 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
he 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 lot applicable.	4.12.2 Session Key Encapsulation and Recovery Policy and Practices Not applicable.
5. Facility, Management, and Operational Controls	5. Facility, Management, and Operational Controls
5.1 Physical Security Controls	5.1 Physical Security Controls

JPRS CA Certificate Policy(変更履歴付) Stipulated in the CPS.	JPRS CA Certificate Policy (整形版) 備考 Stipulated in the CPS.
5.2 Procedural Controls	5.2 Procedural Controls Stipulated in the CPS.
5.3 Personnel Controls	5.3 Personnel Controls 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.
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) years.	Stipulated in the CPS. Audit Logs on the RA system shall be archived for at least seven (7) years.
5.4.4 Protection of Audit Log	5.4.4 Protection of Audit Log
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
"5.5 Records Archival" of the CPS:this CP;	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 Certification Authority; records and audit reports on the results of audits; and information on applications from Subscribers and the histories thereof. 	 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.
5.5.2 Retention Period for Archive	5.5.2 Retention Period for Archive
years:this CP;documents prepared under this CP stipulating the business operations of the	 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. 	 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

Stipulated in the CPS.

5.5.4 Archive Backup Procedures

Stipulated in the CPS.

5.5.5 Requirements for Time-Stamping of Records

Stipulated in the CPS.

5.5.6 Archive Collection System

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:

JPRS CA Certificate Policy (整形版)

5.5.3 Protection of Archive

Stipulated in the CPS.

5.5.4 Archive Backup Procedures

Stipulated in the CPS.

5.5.5 Requirements for Time-Stamping of Records

Stipulated in the CPS.

5.5.6 Archive Collection System

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 so 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
te Key becomes	
scribers, a new shall be issued.	
cates and CRLs	
or Registration of the means set	
ys of the CA.	
elf/herself/itself. scribers.	
cribers.	
en applying for be encrypted by	
~ · · · · · · · · · · · · · · · · · · ·	
ository.	
nents, the	

For RSA key pairs the CA SHALL:

- Ensure that the modulus size, when encoded, is at least 2048 bits, and;
- Ensure that the modulus size, in bits, is evenly divisible by 8. •

For ECDSA key pairs the CA SHALL:

• Ensure that the key represents a valid point on the NIST P-256 or NIST P-384 elliptic curve.

No other algorithms or key sizes are permitted.

6.1.6 Public Key Parameters Generation and Quality Checking

Stipulated in the CPS. No policy is stipulated on the generation and quality inspection of the Public Key parameters of Subscribers.

6.1.7 Key Usage Purposes

The following table summarizes the usages of keys intended by the CA and by certificates issued by the CA:

	Table 6.1 Key Usage I	Purposes
	the CA	Certificates issued by the CA
digitalSignature	—	yes
nonRepudiation	—	—
keyEncipherment	_	yes <u>(except for certificates</u> <u>issued by using ECDSA</u> <u>key)</u>
dataEncipherment	—	—
keyAgreement	—	—
keyCertSign	yes	—
cRLSign	yes	—
encipherOnly	—	—
decipherOnly	—	—

6.2 Private Key Protection and Cryptographic Module Engineering 6.2 Controls

Stipulated in the CPS.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

Stipulated in the CPS.

6.3.2 Certificate operational periods and key pair usage periods

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

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

For

For

No

6.

6.

						/## 	
n F	JPRS C RSA key pairs the CA SHA	A Certificate F	ollcy(叠形版)			備考	
r 1	toA key pairs the CA SITA						
•	Ensure that the modulu	us size, when encod	ded, is at least 2048 bits, and;				
٠	Ensure that the modulu	us size, in bits, is e	venly divisible by 8.				
r F •	ECDSA key pairs the CA S Ensure that the key re elliptic curve.		point on the NIST P-256 or NIST	5 P-384	ECDSA 追加	(ECC)に同	関する記載の
o of	ther algorithms or key size	es are permitted.					
.1	.6 Public Key Parame	eters Generatio	on and Quality Checking				
-	ulated in the CPS. No poli Public Key parameters of S	-	n the generation and quality inspec	ction of			
.1	.7 Key Usage Purpos	ses					
			eys intended by the CA and by cert	ificates			
	ed by the CA:	ine usages of Ke	eys intended by the OA and by cert	lineates			
		Table 6.1 Key Usa the CA	age Purposes Certificates issued by the				
		the CA	CA				
	digitalSignature	—	yes				
	nonRepudiation	—	—				
	keyEncipherment		yes (except for certificates issued by using ECDSA key)		ECDSA 追加	(ECC)に目	関する記載の
	dataEncipherment	—	—				
	keyAgreement	—	—				
	keyCertSign	yes	—				
	cRLSign	yes	—				
	encipherOnly	—					
	decipherOnly	—	—				
or ipt	Private Key Protect Introls Inlated in the CPS. Other Aspects of Ka		otographic Module Engine gement	ering			
.3	.1 Public key archiva	I					
ipυ	ulated in the CPS.						
.3	.2 Certificate operation	onal periods a	nd key pair usage periods				
bs rio	criber Certificates issued	on or after 1 Sep Subscriber Certi	ificate of the CA is stipulated in the tember 2020 MUST NOT have a ficates issued prior to 1 September	validity			
eat			ed as 86,400 seconds. Any amount and/or leap seconds, shall repres				
	20/10						

Co

Stip

6.3

6.

Stip

6.

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 | T 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) T and less than 2¹⁵⁹ 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 - G4on or after July 29 2020)

Basic field	l	Description of setting	critical				
Version		Version 3	-				
Serial Nur	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=Japan Registry Services Co., Ltd.	-				
	Common Name	(1) Domain Validation	-				
		CN=JPRS Domain Validation Authority					
		- G4					
		(2) Organization Validation					
		CN=JPRS Organization Validation					
		Authority – G4					
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-				
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-				
Subject	Country	(1) Domain Validation	-				
		No description					
		(2) Organization Validation					
		C=JP as the address of the					
		Subscriberorganization or individual					
		(country)					
	State or Province	(1) Domain Validation	-				
		No description					
		(2) Organization Validation					
		Address of the <u>Subscriberorganization</u>					

	JPRS CA C	ertificate Policy(整形版)			備考
6.4 Activat					
6.5 Compu	uter Security Co the CPS.	ontrols			
6.6 Life Cy Stipulated in	/cle Technical C the CPS.	Controls			
6.7 Networ Stipulated in	rk Security Con the CPS.	trols			
6.8 Time S Stipulated in					
7. Certif	icate, CRL, a	and OCSP Profiles			
The CA SHAI Information, Generation ar The CA SHAI and less than	Section 6.1.5 - Key nd Quality Checking LL generate non-seq 2^159 containing at	al requirements set forth in Section 2.2 - y Sizes, and Section 6.1.6 - Public Ke of this CP. uential Certificate serial numbers greater least 64 bits of output from a CSPRNG. orm to RFC 5280, the profile of which are in	y Parame than zero	eters o (0)	
Table 7.1-1		ate Profile (applicable to certificates iss 4 or JPRS Organization Validation Authori		\mathbf{PRS}	プロファイルの適用対象の記載を 修正
Basic field		Description of setting	critical	1	
Version		Version 3	-		
Serial Num		An integral serial number to be assigned by the CA to the certificate	-		
Signature A		sha256 with RSA Encryption	-	-	
Issuer	Country	C=JP	-	-	
	Organization Common Name	O=Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation Authority – G4	-		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-		
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	1	
Subject	Country	 (1) Domain Validation No description (2) Organization Validation C=JP as the address of the Subscriber (country) 	-		表現の修正(以後、同様)
	State or Province	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture) 	-		

JPRS CA Co	ertificate Policy(変更履歴付)			JPRS CA	Certificate Policy(整形版)	備考	
	or individual (prefecture name)				name) (mandatory)		
	(mandatory)						
Locality	(1) Domain Validation	-		Locality	(1) Domain Validation	-	
Hocarry	No description			Locality	No description		
	(2) Organization Validation				(2) Organization Validation		
	Address of the <u>Subscriberorganization</u>				Address of the Subscriber (city, town, or		
	or individual (city, town, or village				village name) (mandatory)		
	name) (mandatory)				vinage name/ (manuatory)		
Organization	(1) Domain Validation	-		Organization	(1) Domain Validation	-	
	No description				No description		
	(2) Organization Validation				(2) Organization Validation		
	Name of the Subscriber or the				Name of the Subscriber (mandatory)		
	Subscriber's organization (mandatory)						
Organizational	(1) Domain Validation	-		Organizational	(1) Domain Validation	-	
Unit	No description			Unit	No description		
	(2) Organization Validation				(2) Organization Validation		
	Business division name of the				Business division name of the		
	Subscriber (<u>optional voluntary</u>).				Subscriber (optional).		
	However, this item will not be included				However, this item will not be included	表現の修正	
	in certificates issued on or after 18				in certificates issued on or after 18		
	November 2021.				November 2021.		
	 A string comprising symbols only 				 A string comprising symbols only 		
	or spaces only may not be				• A string comprising symbols only or spaces only may not be		
	designated, and any of the				designated, and any of the		
	following strings may not be				following strings may not be		
	included:				included:		
	• any name, company name,				• any name, company name,		
	trade name, or trademark that				trade name, or trademark that		
	is likely to cause others to				is likely to cause others to		
	misconstrue that the relevant				misconstrue that the relevant		
	information is the information				information is the information		
	of any organization other than				of any organization other than		
	the applicant organization;				the applicant organization;		
	• any string indicating a legal				• any string indicating a legal		
	personality, such as "Co., Ltd";				personality, such as "Co., Ltd";		
	• any string referring to a				• any string referring to a		
	specific natural person;				specific natural person;		
	any string indicating an				any string indicating an		
	address;				address;		
	any phone number;				• any phone number;		
	any domain name or IP				any domain name or IP		
	address; or				address; or		
	• any string meaning "blank",				• any string meaning "blank",		
	"not applicable" or the like				"not applicable" or the like		
	("null", "N/A" or the like)				("null", "N/A" or the like)		
Common Name	A host name used in the DNS of the	<u> </u>		Common Name	A host name used in the DNS of the		
Common Name		-		Common Name			
	server in which the certificate is				server in which the certificate is		
	scheduled to be installed (mandatory)				scheduled to be installed (mandatory)		
	- The value must be encoded as a				- The value must be encoded as a		
	character-for-character copy of the				character-for-character copy of the		
	dNSName entry value from the				dNSName entry value from the		
	Subject Alternative Name extension.				Subject Alternative Name extension.		
	Specifically.				Specifically.		
oject Public Key Info	The subject's Public Key (RSA 2048	-	Subject Pu	ublic Key Info	The subject's Public Key (RSA 2048	-	
-	bits)			-	bits)		
tended field	Description of setting	critical	Extended	field	Description of setting c	ritical	

JPRS CA Ce	rtificate Policy(変更履歴付)		JPRS CA (Certificate Policy(整形版)
KeyUsage	digitalSignature, keyEncipherment	У	KeyUsage	digitalSignature, keyEncipherment
ExtendedKeyUsage	TLS Web Server Authentication	n	ExtendedKeyUsage	TLS Web Server Authentication
Subject Alt Name	dNSName= name(s) of the server(s)	n	Subject Alt Name	dNSName= name(s) of the server(s)
CertificatePolicies	 [1] Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/ [2] Certificate Policy (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation 	n	CertificatePolicies	 [1] Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/ [2] Certificate Policy (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation
	2.23.140.1.2.2			2.23.140.1.2.2
CRL Distribution Points	 (1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_g4/fullcrl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc a_g4/fullcrl.crl 	n	CRL Distribution Points	 (1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_g4/fullcrl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ove a_g4/fullcrl.crl
Authority Information Access	 [1] ocsp (1.3.6.1.5.5.7.48.1) (1) Domain Validation http://dv.g4.ocsp.pubcert.jprs.jp (2) Organization Validation http://ov.g4.ocsp.pubcert.jprs.jp [2] ca issuers (1.3.6.1.5.5.7.48.2) (1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_g4/JPRS_DVCA_G4_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc a_g4/JPRS_OVCA_G4_DER.cer 	n	Authority Information Access	 [1] ocsp (1.3.6.1.5.5.7.48.1) (1) Domain Validation http://dv.g4.ocsp.pubcert.jprs.jp (2) Organization Validation http://ov.g4.ocsp.pubcert.jprs.jp [2] ca issuers (1.3.6.1.5.5.7.48.2) (1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_g4/JPRS_DVCA_G4_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ove a_g4/JPRS_OVCA_G4_DER.cer
Authority Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n	Authority Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)
Subject Key Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n	Subject Key Identifier	SHA-1 hash for the subject's Public Key (160 bits)
Certificate Transparency Timestamp List (*) (1.3.6.1.4.1.11129.2.4.2)	Value of an OCTET STRING containing the encoded SignedCertificateTimestampList	n	Certificate Transparency Timestamp List (1.3.6.1.4.1.11129.2.4.2)	Value of an OCTET STRING containing the encoded SignedCertificateTimestampList

operated by a third party and prescribed by the CA at the time of certificate issuance. Other information in the profile of certificates_(table 7.1-3 defined as Precertificate) shall be registered on the CT log server.

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

Basic field		Description of setting	<u>critical</u>
Version		Version 3	- 1
Serial Number		An integral serial number to be assigned by the CA to the certificate	- 1
Signature Algorithm		sha256 with RSA Encryption	- 1
Issuer	Country	<u>C=JP</u>	- 1
	Organization	<u>O=Japan Registry Services Co., Ltd.</u>	-
	<u>Common Name</u>	(1) Domain Validation <u>CN= JPRS DV RSA CA 2024 G1</u> (2) Organization Validation <u>CN= JPRS OV RSA CA 2024 G1</u>	11
Validity	<u>NotBefore</u>	E.g.) 2008/3/1 00:00:00 GMT	-

	JPRS CA C	ertificate Policy(整形版)			備考
KeyUsage		digitalSignature, keyEncipherment	У		
ExtendedKeyU	Jsage	TLS Web Server Authentication	n		
Subject Alt Na		dNSName= name(s) of the server(s)	n		
CertificatePoli		[1] Certificate Policy	n		
		1.3.6.1.4.1.53827.1.1.4			
		CPS			
		http://jprs.jp/pubcert/info/repository/			
		[2] Certificate Policy			
		(1) Domain Validation			
		2.23.140.1.2.1			
		(2) Organization Validation			
		2.23.140.1.2.2			
CRL Distributi	ion Points	(1) Domain Validation	n		
		http://repo.pubcert.jprs.jp/sppca/jprs/dv			
		ca_g4/fullcrl.crl			
		(2) Organization Validation			
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc			
Anth ority Info	mation Accord	a_g4/fullcrl.crl [1] ocsp (1.3.6.1.5.5.7.48.1)			
Authority Inio	rmation Access	(1) Domain Validation $(1.3.6.1.3.5.7.48.1)$	n		
		http://dv.g4.ocsp.pubcert.jprs.jp			
		(2) Organization Validation			
		http://ov.g4.ocsp.pubcert.jprs.jp			
		[2] ca issuers (1.3.6.1.5.5.7.48.2)			
		(1) Domain Validation			
		http://repo.pubcert.jprs.jp/sppca/jprs/dv			
		ca_g4/JPRS_DVCA_G4_DER.cer			
		(2) Organization Validation			
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc			
		a_g4/JPRS_OVCA_G4_DER.cer			
Authority Key	Identifier	SHA-1 hash for the issuer's Public Key	n		
~		(160 bits)			
Subject Key Id	lentifier	SHA-1 hash for the subject's Public Key	n		
		(160 bits)			
Certificate Tra		Value of an OCTET STRING containing	n		
Timestamp Lis		the encoded			
(1.3.6.1.4.1.1)	1129.2.4.2)	SignedCertificateTimestampList			
					表 7.1-7と重複のため削除
Fable 7.1-2 Sub	oscriber Certificat	e Profile (applicable to certificates issued	l by JPRS	DV	中間CA証明書の追加に伴うプロ
	1 or JPRS OV RS.				ファイルの追加
Basic field		Description of setting	critical		
Version		Version 3	-		
Serial Number	ſ	An integral serial number to be	-		
		assigned by the CA to the certificate			
Signature Algo	orithm	sha256 with RSA Encryption	-		
	ountry	C=JP	-		
	rganization	O=Japan Registry Services Co., Ltd.	-		
~	ommon Name	(1) Domain Validation	-		
C	011111011 1 (41110				
C		CN= JPRS DV RSA CA 2024 G1			
		(2) Organization Validation			
	lotBefore				

	TPRS CA Cer	tificate Policy(変更履歴付)			TPRS CA	Certificate Policy(整形版)	
	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	-
Bubject		No description	-	Subject		No description	
		(2) Organization Validation				(2) Organization Validation	
		C=JP as the address of the Subscriber				C=JP as the address of the Subscriber	
		(country)				(country)	
	State or Province	(1) Domain Validation			State or Province	(1) Domain Validation	_
	State of 1 rovince	No description	-		State of 1 founde	No description	
		(2) Organization Validation				(2) Organization Validation	
		Address of the Subscriber (prefecture				Address of the Subscriber (prefecture	
		name) (mandatory)				name) (mandatory)	
	T				T 1:4	(1) Domain Validation	
	<u>Locality</u>	(1) Domain Validation	<u> </u>		Locality		-
		No description				No description	
		(2) Organization Validation				(2) Organization Validation	
		Address of the Subscriber (city, town, or				Address of the Subscriber (city, town, or	
		<u>village name) (mandatory)</u>	<u> </u>			village name) (mandatory)	
	<u>Organization</u>	(1) Domain Validation			Organization	(1) Domain Validation	-
		No description				No description	
		(2) Organization Validation				(2) Organization Validation	
		Name of the Subscriber (mandatory)	<u> </u>			Name of the Subscriber (mandatory)	
	<u>Common Name</u>	A host name used in the DNS of the			Common Name	A host name used in the DNS of the	-
		server in which the certificate is				server in which the certificate is	
		scheduled to be installed (mandatory)				scheduled to be installed (mandatory)	
		- The value must be encoded as a				- The value must be encoded as a	
		character-for-character copy of the				character-for-character copy of the	
		dNSName entry value from the				dNSName entry value from the	
		Subject Alternative Name extension.				Subject Alternative Name extension.	
		Specifically.				Specifically.	
Subject Pub	<u>lic Key Info</u>	The subject's Public Key (RSA 4096	<u> </u>	Subject Pu	blic Key Info	The subject's Public Key (RSA 4096	-
		bits-, RSA3072 bits or RSA 2048 bits)			20 7 7	bits, RSA3072 bits or RSA 2048 bits)	
Extended field	<u>eld</u>	Description of setting	<u>critical</u>	Extended f	ïeld	Description of setting	critical
<u>KeyUsage</u>		digitalSignature.	У	KeyUsage		digitalSignature,	У
.		keyEncipherment	<u> </u>			keyEncipherment	
ExtendedKe	<u>eyUsage</u>	TLS Web Server Authentication	<u>n</u>	Extended	leyUsage	TLS Web Server Authentication	n
		TLS Web Client Authentication				TLS Web Client Authentication	
Subject Alt		<u>dNSName= name(s) of the server(s)</u>	<u>n</u>	Subject Alt		dNSName= name(s) of the server(s)	n
<u>CertificateP</u>	<u>Policies</u>	[1] Certificate Policy	<u>n</u>	Certificate	Policies	[1] 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	
		[2] Certificate Policy				[2] Certificate Policy	
		$\underline{1.3.6.1.4.1.53827.1.1.4}$				1.3.6.1.4.1.53827.1.1.4	
CRL Distrib	oution Points	(1) Domain Validation	<u>n</u>	CRL Distr	bution Points	(1) Domain Validation	n
		http://repo.pubcert.jprs.jp/sppca/jprs/dv				http://repo.pubcert.jprs.jp/sppca/jprs/dv	
		<u>ca_rsa2024g1/fullcrl.crl</u>				ca_rsa2024g1/fullcrl.crl	
		(2) Organization Validation				(2) Organization Validation	
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc				http://repo.pubcert.jprs.jp/sppca/jprs/ovc	
		<u>a rsa2024g1/fullcrl.crl</u>				a_rsa2024g1/fullcrl.crl	
<u>Aut</u> hority In	nformation Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	<u>n</u>	Authority	Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	n
		(1) Domain Validation				(1) Domain Validation	
		http://dv.rsa2024g1.ocsp.pubcert.jprs.jp				http://dv.rsa2024g1.ocsp.pubcert.jprs.jp	
		(2) Organization Validation				(2) Organization Validation	
		http://ov.rsa2024g1.ocsp.pubcert.jprs.jp				http://ov.rsa2024g1.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	
							1

JPRS CA Cer	tificate Policy(変更履歴付)	
	http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_rsa2024g1/JPRS_DVCA_RSA2024G 1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc a_rsa2024g1/JPRS_OVCA_RSA2024G1 _DER.cer	
<u>Authority Key Identifier</u>	SHA-1 hash for the issuer's Public Key (160 bits)	<u>n</u>
Subject Key Identifier	SHA-1 hash for the subject's Public Key (160 bits)	<u>n</u>
Certificate Transparency <u>Timestamp List</u> (1.3.6.1.4.1.11129.2.4.2)	Value of an OCTET STRING containingtheencodedSignedCertificateTimestampList(optional).	<u>n</u>

	JPRS CA C	Certificate Policy(整形版)			備考
		http://repo.pubcert.jprs.jp/sppca/jprs/dv			
		ca_rsa2024g1/JPRS_DVCA_RSA2024G			
		1 DER.cer			
		(2) Organization Validation			
		http://repo.pubcert.jprs.jp/sppca/jprs/ovc			
		a_rsa2024g1/JPRS_OVCA_RSA2024G1			
A 1 1	T7 T1 + · @·	_DER.cer			
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)			
Certificate	Transparency	Value of an OCTET STRING containing	n		
Timestam	p List	the encoded			
(1.3.6.1.4)	(.1.11129.2.4.2)	SignedCertificateTimestampList(option			
		al).			
				-	
		te Profile (applicable to certificates issued	l by JPRS	DV	中間CA証明書の追加に伴うプ
	24 G1 or JPRS OV EC				ファイルの追加
Basic field		Description of setting	critical	1	
Version		Version 3	-	-	
Serial Nur	nhor	An integral serial number to be	-		
	IIDEI	assigned by the CA to the certificate			
C :	A 1				
0	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	-	-	
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	(1) Domain Validation No description	-	-	
	State or Province	(1) Domain Validation	-	-	
	State or Province	(1) Domain Validation No description	-	-	
	State or Province	(1) Domain ValidationNo description(2) Organization Validation	-		
		 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) 	-	-	
	State or Province	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation 	-	-	
		 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description 	-	-	
		 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation 	-	-	
		 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or 	-	-	
	Locality	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) 	-	-	
		 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation 	-	-	
	Locality	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (1) Domain Validation No description No description 	-		
	Locality	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation 	-	-	
	Locality Organization	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation 	-		
	Locality	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation 	-		
	Locality Organization	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation 	-		
	Locality Organization	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation Name of the Subscriber (mandatory) A host name used in the DNS of the server in which the certificate is 	- -	-	
	Locality Organization	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation Name of the Subscriber (mandatory) A host name used in the DNS of the server in which the certificate is scheduled to be installed (mandatory) 	-	-	
	Locality Organization	 (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (prefecture name) (mandatory) (1) Domain Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation No description (2) Organization Validation Address of the Subscriber (city, town, or village name) (mandatory) (1) Domain Validation No description (2) Organization Validation Name of the Subscriber (mandatory) A host name used in the DNS of the server in which the certificate is 	- -		

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

Basic field		Description of setting	<u>critical</u>
Version		Version 3	-
Serial Nu	<u>mber</u>	<u>An integral serial number to be</u> <u>assigned by the CA to the certificate</u>	-
Signature	<u>Algorithm</u>	ecdsa-with-SHA384	<u>_</u>
<u>Issuer</u>	<u>Country</u>	<u>C=JP</u>	-
	Organization	<u>O=Japan Registry Services Co., Ltd.</u>	-
	Common Name	(1) Domain Validation	_
		<u>CN= JPRS DV ECC CA 2024 G1</u>	
		(2) Organization Validation	
		<u>CN= JPRS OV ECC CA 2024 G1</u>	
<u>Validity</u>	<u>NotBefore</u>	<u>E.g.) 2008/3/1 00:00:00 GMT</u>	_
	<u>NotAfter</u>	<u>E.g.) 2009/3/1 00:00:00 GMT</u>	<u>_</u>
<u>Subject</u>	Country	(1) Domain Validation	<u>_</u>
		<u>No description</u>	
		(2) Organization Validation	
		<u>C=JP as the address of the Subscriber</u>	
		(country)	
	State or Province	(1) Domain Validation	1
		<u>No description</u>	
		(2) Organization Validation	
		Address of the Subscriber (prefecture	
		<u>name) (mandatory)</u>	
	Locality	(1) Domain Validation	1
		No description	
		(2) Organization Validation	
		Address of the Subscriber (city, town, or	
		village name) (mandatory)	
	<u>Organization</u>	(1) Domain Validation	1
		No description	
		(2) Organization Validation	
		Name of the Subscriber (mandatory)	
	<u>Common Name</u>	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	

	JPRS CA C	Certificate Policy(整形版)			備考
		http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_rsa2024g1/JPRS_DVCA_RSA2024G 1_DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc			
		a_rsa2024g1/JPRS_OVCA_RSA2024G1 _DER.cer			
	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		
Timestam	e Transparency p List 4.1.11129.2.4.2)	Value of an OCTET STRING containing the encoded SignedCertificateTimestampList(option al).	n		
ECC CA 202	24 G1 or JPRS OV EC		-	DV	中間CA証明書の追加に伴うプロ ファイルの追加
Basic field		Description of setting	critical		
Version Serial Nur	mber	Version 3An integral serial number to be assigned by the CA to the certificate	-		
Signature	Algorithm	ecdsa-with-SHA384	-		
Issuer	Country	C=JP	-		
155401	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	-		
vanaity	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 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	-		

b 22 Extended field <u>KeyUsage</u> <u>d</u> <u>k</u> <u>c</u> ExtendedKeyUsage	Subject Alternative Name extension. Specifically.Specifically.The subject's Public Key (RSA 4096 pits, RSA 3072 bits, RSA 2048 bits, P- 256 or P-384)Description of setting ligitalSignature, xeyEncipherment (except for certificates issued by using ECDSA key)	- <u>critical</u> X	Subject Public Key Info Extended field	Subject Alternative Name extension. Specifically.The subject's Public Key (RSA 4096 bits, RSA 3072 bits, RSA 2048 bits, P-	-	
b 22 Extended field <u>KeyUsage</u> <u>d</u> <u>k</u> <u>c</u> ExtendedKeyUsage	bits, RSA 3072 bits, RSA 2048 bits, P- 256 or P-384) Description of setting digitalSignature, xeyEncipherment (except for certificates issued by using ECDSA key)	<u>critical</u>		bits, RSA 3072 bits, RSA 2048 bits, P-	-	
Extended field I KeyUsage d keyUsage d keyUsage I ExtendedKeyUsage I	Description of settingligitalSignature,keyEncipherment(exceptforcertificates issued by using ECDSA key)		Extended field	256 or P-384)		
KeyUsage d k k c k ExtendedKeyUsage T	ligitalSignature, xeyEncipherment (except for xertificates issued by using ECDSA key)				critical	
			KeyUsage	digitalSignature, keyEncipherment (except for certificates issued by using ECDSA key)	У	
	<u>FLS Web Server Authentication</u> FLS Web Client Authentication	<u>n</u>	ExtendedKeyUsage	TLS Web Server Authentication TLS Web Client Authentication	n	
Subject Alt Name d	lNSName= name(s) of the server(s)	<u>n</u>	Subject Alt Name	dNSName= name(s) of the server(s)	n	
	1] Certificate Policy 1) Domain Validation 2.23.140.1.2.1 2) Organization Validation 2.23.140.1.2.2 2] Certificate Policy 1.3.6.1.4.1.53827.1.1.4	<u>n</u>	CertificatePolicies	 [1] Certificate Policy (1) Domain Validation 2.23.140.1.2.1 (2) Organization Validation 2.23.140.1.2.2 [2] Certificate Policy 1.3.6.1.4.1.53827.1.1.4 	n	
	1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_ecc2024g1/fullcrl.crl 2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc a_ecc2024g1/fullcrl.crl	<u>n</u>	CRL Distribution Points	 (1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_ecc2024g1/fullcrl.crl (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc a_ecc2024g1/fullcrl.crl 	n	
	1] ocsp (1.3.6.1.5.5.7.48.1) 1) Domain Validation http://dv.ecc2024g1.ocsp.pubcert.jprs.jp 2) Organization Validation http://ov.ecc2024g1.ocsp.pubcert.jprs.jp 2] ca issuers (1.3.6.1.5.5.7.48.2) 1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_ecc2024g1/JPRSDVCA_ECC2024G1 DER.cer 2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc a_ecc2024g1/JPRS_OVCA_ECC2024G1 DER.cer	<u>n</u>	Authority Information Access	 [1] ocsp (1.3.6.1.5.5.7.48.1) (1) Domain Validation http://dv.ecc2024g1.ocsp.pubcert.jprs.jp (2) Organization Validation http://ov.ecc2024g1.ocsp.pubcert.jprs.jp [2] ca issuers (1.3.6.1.5.5.7.48.2) (1) Domain Validation http://repo.pubcert.jprs.jp/sppca/jprs/dv ca_ecc2024g1/JPRSDVCA_ECC2024G1 _DER.cer (2) Organization Validation http://repo.pubcert.jprs.jp/sppca/jprs/ovc a_ecc2024g1/JPRS_OVCA_ECC2024G1 _DER.cer 	n	
	SHA-1 hash for the issuer's Public Key 160 bits)	<u>n</u>	Authority Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n	
	SHA-1 hash for the subject's Public Key 160 bits)	<u>n</u>	Subject Key Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n	
Certificate TransparencyVTimestamp List(1.3.6.1.4.1.11129.2.4.2)	Value of an OCTET STRING containing the encoded SignedCertificateTimestampLi st (optional)	<u>n</u>	Certificate Transparency Timestamp List (1.3.6.1.4.1.11129.2.4.2)	Value of an OCTET STRING containing the encoded SignedCertificateTimestampLi st (optional)	n	
Table 7.1-42 Subordinate CA Cert Security Communication RootCA2000 Control of Contro of Contro of Contro of Control of Control of Contro of Control of	tificate Profile (applicable to certificat	tes issued by	Table 7.1-4 Subordinate CA C Security Communication RootCA	Certificate Profile (applicable to certificat	es issued	by プロファイルの適用対象の記載を 修正
	Description of setting	critical	Basic field	Description of setting	critical	
	Version 3	-	Version	Version 3	-	
Serial Number A a	An integral serial number to be assigned by the CA to the certificate sha256 With RSA Encryption	-	Serial Number Signature Algorithm	An integral serial number to be assigned by the CA to the certificate sha256 With RSA Encryption	-	
	C=JP		Issuer Country	C=JP		

Basic fiel	d	Description of setting	critical	
Version	vision Version 3			
Serial Nu	umber	An integral serial number to be assigned by the CA to the certificate	-	
Signature Algorithm		sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	

Subject Public Key Info Extended field KeyUsage	ertificate Policy (整形版) Subject Alternative Name extension. Specifically. The subject's Public Key (RSA 4096			備考
Extended field	Specifically. The subject's Public Key (RSA 4096			
Extended field	The subject's Public Key (RSA 4096			
Extended field				
	$h_{i+\alpha}$ DCA 2079 $h_{i+\alpha}$ DCA 2048 $h_{i+\alpha}$ D-	_		
	bits, RSA 3072 bits, RSA 2048 bits, P- 256 or P-384)			
		omitical		
KOVIJSOCO	Description of setting	critical		
ney Usage	digitalSignature,	У		
	keyEncipherment (except for			
	certificates issued by using ECDSA key)			
ExtendedKeyUsage	TLS Web Server Authentication	n		
	TLS Web Client Authentication			
Subject Alt Name	dNSName= name(s) of the server(s)	n		
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			
	1.3.6.1.4.1.53827.1.1.4			
CRL Distribution Points	(1) Domain Validation	n		
	http://repo.pubcert.jprs.jp/sppca/jprs/dv			
	ca_ecc2024g1/fullcrl.crl			
	(2) Organization Validation			
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc			
	a_ecc2024g1/fullcrl.crl			
Authority Information Accord	$[1] \operatorname{ocsp}(1.3.6.1.5.5.7.48.1)$			
Authority Information Access	(1) Domain Validation	n		
	http://dv.ecc2024g1.ocsp.pubcert.jprs.jp			
	(2) Organization Validation			
	http://ov.ecc2024g1.ocsp.pubcert.jprs.jp			
	[2] ca issuers (1.3.6.1.5.5.7.48.2)			
	(1) Domain Validation			
	http://repo.pubcert.jprs.jp/sppca/jprs/dv			
	ca_ecc2024g1/JPRSDVCA_ECC2024G1			
	_DER.cer			
	(2) Organization Validation			
	http://repo.pubcert.jprs.jp/sppca/jprs/ovc			
	a_ecc2024g1/JPRS_OVCA_ECC2024G1			
	_DER.cer			
Authority Key Identifier	SHA-1 hash for the issuer's Public Key	n		
	(160 bits)			
Subject Key Identifier	SHA-1 hash for the subject's Public Key	n		
	(160 bits)			
Certificate Transparency	Value of an OCTET STRING containing	n		
Timestamp List	the encoded			
(1.3.6.1.4.1.11129.2.4.2)	SignedCertificateTimestampLi			
(1.0.0.1.1.1.111=0.=.1.=)	st (optional)			
Pable 71-4 Subordinato CA Co	ertificate Profile (applicable to certificat	he issued	hv	プロファイルの適用対象の記載を
Security Communication RootCA2		.co 100ueu	IJу	修正
Basic field	Description of setting	critical		
Version		critical		
	Version 3	-		
Serial Number	An integral serial number to be	-		
	assigned by the CA to the certificate			
Signature Algorithm	sha256 With RSA Encryption	-		
Issuer Country	C=JP	-		

	JPRS CA Cer	tificate Policy(変更履歴付)	
	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	blic Key Info	The subject's Public Key (RSA 2048 bits)	-
Extended f		Description of setting	critica
Authority	Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n
KeyUsage		Certificate Signing Off-line CRL Signing CRL Signing (06)	У
Certificate	Policies	Certificate Policy 1.2.392.200091.100.901.4 CPS http://repository.secomtrust.net	N
Basic Cons	straints	/SC-Root2/ Subject Type=CA Path Length Constraint=0	У
Extended	KeyUsage	TLS Web Server Authentication	n
	ibution Points	http://repository.secomtrust.net/SC- Root2/SCRoot2CRL.crl	n
Authority	Information Access	 [1] ocsp (1.3.6.1.5.5.7.48.1) 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 	n

	JPRS CA (Certificate Policy(整形版)		۲. The second	帯考
	Organization	O=SECOM Trust Systems CO.,LTD.	-		
	Common Name	OU=Security Communication RootCA2	-		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-		
, allaloj	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-		
Subject	Country	C=JP	-		
ie insjere	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 Pul	blic Key Info	The subject's Public Key (RSA 2048	-		
		bits)			
Extended fi		Description of setting	critical		
Authority I	Key Identifier	SHA-1 hash for the issuer's Public Key	n		
~ 1	T 1	(160 bits)			
Subject Key	y Identifier	SHA-1 hash for the subject's Public Key	n		
17 11		(160 bits)			
KeyUsage		Certificate Signing	У		
		Off-line CRL Signing			
Certificatel		CRL Signing (06) Certificate Policy	N		
Certificatei	Policies	1.2.392.200091.100.901.4	IN		
		CPS			
		http://repository.secomtrust.net			
		/SC-Root2/			
Basic Cons	traints	Subject Type=CA	у		
		Path Length Constraint=0	5		
ExtendedKeyUsage		TLS Web Server Authentication	n		
	bution Points	http://repository.secomtrust.net/SC-	n		
		Root2/SCRoot2CRL.crl			
Authority I	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			
			11 050		
	oot CA 2024)	ificate Profile (applicable to certificates issu	ed by SEC		の追加に伴うプロ
	001 CA 2024)	Description of setting	critical	ファイルの追加	
		Version 3	-		
			_		
Version	hor	An integral conial number to be			
Basic field Version Serial Num	nber	An integral serial number to be			
Version Serial Num		assigned by the CA to the certificate	-		
Version Serial Num Signature A	Algorithm	assigned by the CA to the certificate Sha384 With RSA Encryption	-		
Version Serial Num Signature A	Algorithm Country	assigned by the CA to the certificate Sha384 With RSA Encryption C=JP	-		
Version Serial Num Signature A	Algorithm Country Organization	assigned by the CA to the certificate Sha384 With RSA Encryption C=JP O=SECOM Trust Systems Co., Ltd.	- - - -		
Version Serial Num Signature A Issuer	Algorithm Country Organization Common Name	assigned by the CA to the certificate Sha384 With RSA Encryption C=JP O=SECOM Trust Systems Co., Ltd. CN= SECOM TLS RSA Root CA 2024	- - - -		
Version Serial Num Signature A Issuer	Algorithm Country Organization Common Name NotBefore	assigned by the CA to the certificate Sha384 With RSA Encryption C=JP O=SECOM Trust Systems Co., Ltd. CN= SECOM TLS RSA Root CA 2024 E.g.) 2008/3/1 00:00:00 GMT	- - - - -		
Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter	assigned by the CA to the certificate Sha384 With RSA Encryption C=JP O=SECOM Trust Systems Co., Ltd. CN= SECOM TLS RSA Root CA 2024 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT	- - - - - - -		
Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country	assigned by the CA to the certificate Sha384 With RSA Encryption C=JP O=SECOM Trust Systems Co., Ltd. CN= SECOM TLS RSA Root CA 2024 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT C=JP	- - - - - - - -		
Version	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization	assigned by the CA to the certificate Sha384 With RSA Encryption C=JP O=SECOM Trust Systems Co., Ltd. CN= SECOM TLS RSA Root CA 2024 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT C=JP O=Japan Registry Services Co., Ltd.	- - - - - - - - - - - -		
Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country	assigned by the CA to the certificate Sha384 With RSA Encryption C=JP O=SECOM Trust Systems Co., Ltd. CN= SECOM TLS RSA Root CA 2024 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2009/3/1 00:00:00 GMT C=JP	- - - - - - - - - - - -		

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

	JPRS CA	Certificate Policy(整形版)			備考
	Organization	O=SECOM Trust Systems CO.,LTD.	-		
	Common Name	OU=Security Communication RootCA2	-		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-		
valiality	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-		
Subject	Country	C=JP	-		
Subject	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 Pul	blic Key Info	The subject's Public Key (RSA 2048	-		
		bits)			
Extended fi		Description of setting	critical		
Authority I	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			
	D 1: :	CRL Signing (06)	N	-	
Certificate	Policies	Certificate Policy	Ν		
		1.2.392.200091.100.901.4 CPS			
		http://repository.secomtrust.net			
		/SC-Root2/			
Basic Cons	traints	Subject Type=CA	у		
20010 00110		Path Length Constraint=0	5		
ExtendedK	leyUsage	TLS Web Server Authentication	n		
	bution Points	http://repository.secomtrust.net/SC-	n		
		Root2/SCRoot2CRL.crl			
Authority I	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			
		······································			
	oot CA 2024)	ificate Profile (applicable to certificates issu	ed by SEC		中間CA証明書の追加に伴うプロ
Basic field	001 CA 2024)	Description of setting	critical	1	ファイルの追加
Version		Version 3	-		
Serial Num	bor	An integral serial number to be	-		
Serial Null	IDEL	assigned by the CA to the certificate			
Signature A	Algorithm	Sha384 With RSA Encryption	-		
Issuer	Country	C=JP	-		
155001	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	-		
ranany	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-		
Subject	Country	C=JP	-		
Subject	Organization	O=Japan Registry Services Co., Ltd.	-		
	Common Name	(1) Organization Validation	-		
		CN= JPRS OV RSA CA 2024 G1			
		(2) Domain Validation			
	1		1		

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

Basic field		Description of setting	<u>critical</u>
Version		Version 3	- 1
Serial Number		An integral serial number to be	
		assigned by the CA to the certificate	
Signature	<u>Algorithm</u>	Sha384 With RSA Encryption	-
Issuer	Country	<u>C=JP</u>	-
	Organization	O=SECOM Trust Systems Co., Ltd.	- 1
	Common Name	CN= SECOM TLS RSA Root CA 2024	- 1
Validity	<u>NotBefore</u>	<u>E.g.) 2008/3/1 00:00:00 GMT</u>	- 1
	NotAfter	<u>E.g.) 2009/3/1 00:00:00 GMT</u>	- 1
Subject	Country	<u>C=JP</u>	-
	Organization	<u>O=Japan Registry Services Co., Ltd.</u>	- 1
	Common Name	(1) Organization Validation	- 1
		<u>CN= JPRS OV RSA CA 2024 G1</u>	
		(2) Domain Validation	

TPRS CA Cer	tificate Policy(変更履歴付)	
Jind on oor	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 Key	<u>n</u>
	<u>(160 bits)</u>	
Subject Key Identifier	SHA-1 hash for the subject's Public Key	<u>n</u>
	<u>(160 bits)</u>	
<u>KeyUsage</u>	Certificate Signing	<u>y</u>
	Off-line CRL Signing	
	<u>CRL Signing (06)</u>	
<u>CertificatePolicies</u>	[1] Certificate Policy	<u>N</u>
	(1) Domain Validation	
	<u>2.23.140.1.2.1</u>	
	(2) Organization Validation	
	2.23.140.1.2.2	
	[2] Certificate Policy	
	<u>1.2.392.200091.100.901.11</u>	
Basic Constraints	Subject Type=CA	У
	Path Length Constraint=0	
<u>ExtendedKeyUsage</u>	TLS Web Server Authentication	<u>n</u>
	TLS Web Client Authentication	
CRL Distribution Points	http://repol.secomtrust.net/root/tlsrsa/tl	<u>n</u>
	srsarootca2024.crl	
<u>Authority Information Access</u>	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	<u>n</u>
	http://tlsrsarootca2024.ocsp.secom-	
	cert.jp	
	[2] ca issuers (1.3.6.1.5.5.7.48.2)	
	http://repo2.secomtrust.net/root/tlsrsa/tl	
	<u>srsarootca2024.cer</u>	

	JPRS CA (Certificate Policy(整形版)			備考
		CN= JPRS DV RSA CA 2024 G1			
Subject Pu	iblic Key Info	The subject's Public Key (RSA 4096 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 (160 bits)	n		
KeyUsage		Certificate Signing Off-line CRL Signing	У		
~	D 11 1	CRL Signing (06)		-	
Certificate	Policies	[1] Certificate Policy(1) Domain Validation2.23.140.1.2.1	Ν		
		(2) Organization Validation2.23.140.1.2.2[2] Certificate Policy			
\mathbf{D} · \mathbf{C}		1.2.392.200091.100.901.11		-	
Basic Cons		Subject Type=CA Path Length Constraint=0	У	_	
Extended		TLS Web Server Authentication TLS Web Client Authentication	n		
CRL Distr	ibution Points	http://repo1.secomtrust.net/root/tlsrsa/tl srsarootca2024.crl	n		
Authority Information Access		[1] ocsp (1.3.6.1.5.5.7.48.1) http://tlsrsarootca2024.ocsp.secom- cert.jp	n		
		[2] ca issuers (1.3.6.1.5.5.7.48.2) http://repo2.secomtrust.net/root/tlsrsa/tl srsarootca2024.cer			
	Subordinate CA C mmunication ECC R	Certificate Profile (applicable to certificat	es issued	l by	中間CA証明書の追加に伴うプ ファイルの追加
Basic field		Description of setting	critical		2 月 7 200 追加
Version		Version 3	-		
Serial Nur	nber	An integral serial number to be assigned by the CA to the certificate	-		
Signature	Algorithm	ecdsa-with-SHA384	-		
Issuer	Country	C=JP	-	1	
-	Organization	O=SECOM Trust Systems CO.,LTD.	-	1	
	Common Name	CN=Security Communication ECC RootCA1	-		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	1	
v	NotAfter	E.g.) 2009/3/1 00:00:00 GMT	-	1	
a 1 · ·	Country	C=JP	-]	
Subject	Organization	O=Japan Registry Services Co., Ltd.	-	1	
Subject	8	(1) Organization Validation	-		
Subject	Common Name	CN= JPRS OV ECC CA 2024 G1			
Subject	Common Name	CN= JPRS OV ECC CA 2024 G1 (2) Domain Validation			
-		CN= JPRS OV ECC CA 2024 G1 (2) Domain Validation CN= JPRS DV ECC CA 2024 G1	-		
Subject Pu	ıblic Key Info	CN= JPRS OV ECC CA 2024 G1 (2) Domain Validation CN= JPRS DV ECC CA 2024 G1 The subject's Public Key (384 bits)		-	
Subject Pu Extended	ıblic Key Info	CN= JPRS OV ECC CA 2024 G1 (2) Domain Validation CN= JPRS DV ECC CA 2024 G1	- critical n	-	

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

Security Co	<u>mmunication ECC Ro</u>	otCAI)	
Basic field		Description of setting	<u>critical</u>
Version		<u>Version 3</u>	-
<u>Serial Nun</u>	<u>nber</u>	An integral serial number to be	- 1
		assigned by the CA to the certificate	
Signature Algorithm		ecdsa-with-SHA384	- 1
<u>Issuer</u>	Country	<u>C=JP</u>	<u>_</u>
	Organization	<u>O=SECOM Trust Systems CO.,LTD.</u>	<u>_</u>
	Common Name	CN=Security Communication ECC	_
		RootCA1	
<u>Validity</u>	<u>NotBefore</u>	E.g.) 2008/3/1 00:00:00 GMT	-
	<u>NotAfter</u>	E.g.) 2009/3/1 00:00:00 GMT	-
<u>Subject</u>	Country	<u>C=JP</u>	-
	Organization	<u>O=Japan Registry Services Co., Ltd.</u>	-
	Common Name	(1) Organization Validation	<u>_</u>
		CN= JPRS OV ECC CA 2024 G1	
		(2) Domain Validation	
		<u>CN= JPRS DV ECC CA 2024 G1</u>	
<u>Subject Public Key Info</u>		The subject's Public Key (384 bits)	-
Extended f	field	Description of setting	<u>critical</u>
Authority	<u>Key Identifier</u>	SHA-1 hash for the issuer's Public Key	<u>n</u>
		<u>(160 bits)</u>	
Subject Ke	y Identifier	SHA-1 hash for the subject's Public Key	<u>n</u>

	JPRS CA (Certificate Policy(整形版)			備考
		CN= JPRS DV RSA CA 2024 G1			Ì
Subject Pu	ıblic 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 Key (160 bits)	n		
Subject Ke	ey Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n		
KeyUsage		Certificate Signing Off-line CRL Signing CRL Signing (06)	У		
Certificate	Policies	 [1] Certificate Policy (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 	N		
Basic Cons	straints	Subject Type=CA Path Length Constraint=0	У		
Extended	KeyUsage	TLS Web Server Authentication TLS Web Client Authentication	n		
CRL Distribution Points		http://repol.secomtrust.net/root/tlsrsa/tl srsarootca2024.crl	n		
Authority Information Access		 [1] ocsp (1.3.6.1.5.5.7.48.1) http://tlsrsarootca2024.ocsp.secom- cert.jp [2] ca issuers (1.3.6.1.5.5.7.48.2) http://repo2.secomtrust.net/root/tlsrsa/tl srsarootca2024.cer 	n		
	5 Subordinate CA C mmunication ECC R	Certificate Profile (applicable to certificate	tes issued	l by	中間CA証明書の追加に伴うプロ
Basic field		Description of setting	critical	1	ファイルの追加
Version	L	Version 3	-	_	
Serial Nur	mher	An integral serial number to be	-		
	liber	assigned by the CA to the certificate			
Signature	Algorithm	ecdsa-with-SHA384	-		
Issuer	Country	C=JP	-		
	Organization	O=SECOM Trust Systems CO.,LTD.	-		
	Common Name	CN=Security Communication ECC RootCA1	-		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-		
	NotAfter	E.g.) 2009/3/1 00:00:00 GMT			
Subject	Country	C=JP	-		
-	Organization	O=Japan Registry Services Co., Ltd.	-	_	
-		(1) Organization Validation	-	1	
-	Common Name	CN= JPRS OV ECC CA 2024 G1 (2) Domain Validation			
-		CN= JPRS OV ECC CA 2024 G1 (2) Domain Validation CN= JPRS DV ECC CA 2024 G1	-	-	
Subject Pu	ıblic Key Info	CN= JPRS OV ECC CA 2024 G1 (2) Domain Validation CN= JPRS DV ECC CA 2024 G1 The subject's Public Key (384 bits)		-	
Subject Pu Extended	ıblic Key Info	CN= JPRS OV ECC CA 2024 G1 (2) Domain Validation CN= JPRS DV ECC CA 2024 G1	- critical n	-	

JPRS CA Cer	tificate Policy(変更履歴付)	
	<u>(160 bits)</u>	
KeyUsage	Certificate Signing	У
	Off-line CRL Signing	
	<u>CRL Signing (06)</u>	
<u>CertificatePolicies</u>	[1] Certificate Policy	<u>N</u>
	(1) Domain Validation	
	<u>2.23.140.1.2.1</u>	
	(2) Organization Validation	
	2.23.140.1.2.2	
	[2] Certificate Policy	
	$\underline{1.2.392.200091.100.902.1}$	
Basic Constraints	Subject Type=CA	У
	<u>Path Length Constraint=0</u>	
<u>ExtendedKeyUsage</u>	TLS Web Server Authentication	<u>n</u>
	TLS Web Client Authentication	
CRL Distribution Points	http://repository.secomtrust.net/SC-	<u>n</u>
	ECC-Root1/SCECCRoot1CRL.crl	
Authority Information Access	$[1] \operatorname{ocsp} (1.3.6.1.5.5.7.48.1)$	<u>n</u>
	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	

	JPRS CA C	Certificate Policy(整形版)		-1
		(160 bits)		1
KeyUsage		Certificate Signing	У	
		Off-line CRL Signing		
KeyUsage CertificatePolicies Basic Constraints ExtendedKeyUsage CRL Distribution Points Authority Information Acces Authority Information Acces able 7.1-7 Precertificate Pr D20) Basic field Version Serial Number Signature Algorithm Issuer Country Organization		CRL Signing (06)		
KeyUsage CertificatePolicies Basic Constraints ExtendedKeyUsage CRL Distribution Points Authority Information Access able 7.1-7 Precertificate Pro		[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		
		1.2.392.200091.100.902.1		
Basic Cons	straints	Subject Type=CA	у	
		Path Length Constraint=0		
Extended	KevUsage	TLS Web Server Authentication	n	
	- J J -	TLS Web Client Authentication		
CRL Distr	ibution Points	http://repository.secomtrust.net/SC-	n	1
	~	ECC-Root1/SCECCRoot1CRL.crl		1
Authority	Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n	1
		http://sceccrootca1.ocsp.secomtrust.net		1
		[2] ca issuers $(1.3.6.1.5.5.7.48.2)$		1
		http://repository.secomtrust.net/SC-		1
		ECC-Root1/SCECCRoot1ca.cer		
090)			-	-
		Description of setting	critical	
Basic field		Description of settingEncoded value MUST be byte-for-byte	critical -	
020) <mark>Basic field</mark> Version			critical -	
Basic field		Encoded value MUST be byte-for-byte	critical -	
<mark>Basic field</mark> Version		Encoded value MUST be byte-for-byte identical to the same field of the	critical -	-
Basic field Version Serial Nur	nber	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.	critical	-
Basic field Version Serial Nur Signature	nber Algorithm	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above	critical	-
Basic field Version Serial Nur Signature	nber Algorithm Country	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above Same as above	critical	-
Basic field Version Serial Nur Signature	nber Algorithm Country Organization	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above Same as above Same as above	critical	
Basic field Version Serial Nur Signature Ssuer	nber Algorithm Country	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above Same as above	critical	
Basic field Version Serial Nur Signature ssuer	nber Algorithm Country Organization Common Name NotBefore	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above Same as above Same as above Same as above	critical	
Basic field Version Serial Nur Signature ssuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - -	
Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - -	
Basic field Version Serial Nur Signature ssuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - -	
Basic field Version Serial Nur Signature Ssuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization	 Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above 	- - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Ssuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Ssuer Validity Subject Subject Pu	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name iblic Key Info	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Ssuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name iblic Key Info	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate.Same as aboveSame as above	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Ssuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended Precertific	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field cate Poison	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same as above	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended Precertific	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field cate Poison	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field cate Poison	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended Precertific KeyUsage	mber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organization Organization Organizational Unit Common Name iblic Key Info field ate Poison	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same	- - - - - - - - - - - - - - - - - - -	
Basic field Version Serial Nur Signature Issuer Validity Subject Subject Pu Extended Precertific	mber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organization Organization Organizational Unit Common Name ablic Key Info field cate Poison	Encoded value MUST be byte-for-byte identical to the same field of the Subuscriber Certificate. Same as above Same	- - - - - - - - - - - - - - - - - - -	

Table 7.1-<u>7</u>³ Precertificate Profile (applicable to certificates issued on or after July 29, 2020)

Basic field		Description of setting	critical
Version		Encoded value MUST be byte-for-byte	-
		identical to the same field of the	
		Subuscriber Certificate.	
Serial Nu	nber	Same as above	-
Signature Algorithm		Same as above	-
Issuer	Country	Same as above	-
	Organization	Same as above	-
	Common Name	Same as above	-
Validity	NotBefore	Same as above	-
-	NotAfter	Same as above	-
Subject	Country	Same as above	-
-	State or Province	Same as above	-
	Locality	Same as above	-
	Organization	Same as above	-
	Organizational	Same as above	-
	Unit		
	Common Name	Same as above	-
Subject Pu	ıblic Key Info	Same as above	-
Extended	field	Description of setting	critical
Precertific	ate Poison	extnValue OCTET STRING which is	у
		exactly the hex-encoded bytes 0500, the	-
		encoded representation of the ASN.1	
		NULL value, as specified in RFC 6962,	
		Section 3.1.	
KeyUsage		Encoded value MUST be byte-for-byte	У
		identical to the same field of the	
		Subuscriber Certificate.	
Extended	KeyUsage	Same as above	n
Subject Al	t Name	Same as above	n

	TPRS_CA_C	Certificate Policy(整形版)			備考
	<u>ji 10</u> 011 0	(160 bits)			
leyUsage		Certificate Signing	N7		
ley Osage		Off-line CRL Signing	У		
Cartificante Daliaira		CRL Signing (06)	N		
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			
		1.2.392.200091.100.902.1			
asic Cons	straints	Subject Type=CA	у		
		Path Length Constraint=0	5		
vtondodk	KeyUsage	TLS Web Server Authentication	n		
vicinacul	soy obage	TLS Web Client Authentication	11		
21 Diata	ibution Points		n		
IL DIST	IDULIOII FOIIILS	http://repository.secomtrust.net/SC-	n		
.1	те	ECC-Root1/SCECCRoot1CRL.crl			
athority	Information Access	[1] ocsp (1.3.6.1.5.5.7.48.1)	n		
		http://sceccrootca1.ocsp.secomtrust.net			
		[2] ca issuers (1.3.6.1.5.5.7.48.2)			
		http://repository.secomtrust.net/SC-			
		ECC-Root1/SCECCRoot1ca.cer			
20)	Precertificate Profile		critical	1	
asic field		Description of setting	critical		
		Description of settingEncoded value MUST be byte-for-byte	critical		
asic field		Description of settingEncoded value MUST be byte-for-byteidentical to the same field of the	critical -		
<mark>asic field</mark> ersion		Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.	critical		
ersion ersion erial Nur	nber	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as above	critical -		
ersion ersion erial Nur gnature	nber Algorithm	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical - - -		
usic field prsion prial Nur gnature	nber Algorithm Country	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as aboveSame as aboveSame as above	critical - - - - -		
ersion ersion erial Nur gnature	nber Algorithm Country Organization	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as aboveSame as aboveSame as aboveSame as aboveSame as aboveSame as above	critical - - - - - -		
asic field ersion erial Nur ignature suer	nber Algorithm Country Organization Common Name	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical - - - - - - - - - -		
asic field ersion erial Nur gnature suer	nber Algorithm Country Organization Common Name NotBefore	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical - - - - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity	nber Algorithm Country Organization Common Name NotBefore	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	critical - - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity	nber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - -		
asic field ersion erial Nur gnature suer llidity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - -		
asic field ersion erial Nur gnature suer llidity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - -		
asic field ersion erial Nur gnature suer	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - -		
asic field ersion erial Nur ignature suer alidity	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity abject	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity abject ubject Pu	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name iblic Key Info	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - - - - - - - - - - -		
isic field rsion rial Nur gnature suer lidity ibject ibject Pu ttended f	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above	- - - - - - - - - - - - - - - - - - -		
sic field rsion rial Nur gnature suer lidity bject bject Pu tended f	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name iblic Key Info	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
isic field rsion rial Nur gnature suer lidity ibject ibject Pu ttended f	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur ignature suer alidity ubject ubject Pu xtended f	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity abject ubject Pu xtended f	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur ignature ssuer alidity ubject ubject Pu <u>xtended f</u> recertific	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur ignature suer alidity ubject ubject Pu xtended f	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity abject ubject Pu stended for recertific	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur gnature suer alidity abject ubject Pu <u>xtended f</u> recertific	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ablic Key Info field	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
asic field ersion erial Nur gnature suer llidity abject ubject Pu ctended for eccertific	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name ate Poison	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		
sic field rsion rrial Nur gnature suer llidity lbject lbject Pu ctended for eccrtific	nber Algorithm Country Organization Common Name NotBefore NotAfter Country State or Province Locality Organization Organizational Unit Common Name iblic Key Info field ate Poison	Description of settingEncoded value MUST be byte-for-byteidentical to the same field of theSubuscriber Certificate.Same as aboveSame as above<	- - - - - - - - - - - - - - - - - - -		

JPRS CA Cer	tificate Policy(変更履歴付)		
CertificatePolicies	Same as above	n	
CRL Distribution Points	Same as above	n	
Authority Information Access	Same as above	n	
Authority Key Identifier	Same as above	n	
Subject Key Identifier	Same as above	n	

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

Table 7.1-<u>84</u> OCSP Responder Certificate Profile (Applicable to certificates issued <u>by</u> JPRS Domain Validation Authority - G4 or JPRS Organization Validation Authority -<u>G4on or after July 29, 2020</u>)

Basic field		Description of setting	critical
Version		Version 3	-
Serial Nur	nber	Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	-
Signature	Algorithm	sha256 With RSA Encryption	-
Issuer	Country	C=JP	-
	Organization	O= Japan Registry Services Co., Ltd.	-
	Common Name	 (1) Domain Validation CN=JPRS Domain Validation Authority - G4 (2) Organization Validation CN=JPRS Organization Validation 	-
		Authority – G4	
Validity NotBefore		E.g.) 2008/3/1 00:00:00 GMT	-
~ 1.	NotAfter E.g.) 2008/3/5 00:00 GMT vicet Country C=IP (fixed value)		-
Subject	Country	C=JP (fixed value)	-
	Organization	Japan Registry Services Co., Ltd. (fixed value)	-
	Common Name	Name of the OCSP server (mandatory)	-
Subject Pu	ıblic Key Info	The subject's Public Key (RSA 2048 bits)	-
Extended	field	Description of setting	critical
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
CortificatePolicies (*)		Certificate Policy 1.3.6.1.4.1.53827.1.1.4 CPS http://jprs.jp/pubcert/info/repository/	n
Extended	KevUsage	OCSPSigning	n
OCSP No	• •	null	n
	······································		

*: The "CertificatePolicies" field appears in the OCSP profile if the CA required. However, this field does not appear in the OCSP profile on or after 15 September 2023.

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	<u>critical</u>
Version	Version 3	<u>-</u>
Serial Number	Non-sequential values greater than	<u>-</u>
	zero (0) and less than 2 ¹⁵⁹ containing	

		Certificate Policy(整形版)			備考
Certificate		Same as above	n		
	ibution Points	Same as above	n		
, e	Information Access	Same as above	n		
Authority Key Identifier		Same as above	n		
	ey Identifier	Same as above	n		
		ension is removed from the Precertificate, a	-		
		moved from the Subscriber certificate, the or r-byte identical to the Subscriber Certificate		the	
	-	ertificate Profile (Applicable to certificates is ty – G4 or JPRS Organization Validation Au	-	34)	プロファイルの適用対象の記載る 修正
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	-		
LISSUEL	Organization	O= Japan Registry Services Co., Ltd.	_		
	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	-		
	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-		
Subject	Country	C=JP (fixed value)	-		
U	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		
	Key Identifier	SHA-1 hash for the issuer's Public Key (160 bits)	n		
	ey Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n		
KeyUsage		digitalSignature	У		
Extended	XevUsage	OCSPSigning	n		
OCSP No (null	n		
		nun		1	記載が必要な期間が終了したの [、] 削除
	-	ertificate Profile (Applicable to certificates is RS OV RSA CA 2024 G1)	ssued by		中間CA証明書の追加に伴うプ ファイルの追加
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	-		

a		Certificate Policy(整形版)			備考
Certificate		Same as above	n		
	ibution Points	Same as above	n		
	Information Access	Same as above	n		
v	Key Identifier	Same as above	n		
	ey Identifier	Same as above	n		
		ension is removed from the Precertificate, a	0	-	
		moved from the Subscriber certificate, the c		the	
	-	r-byte identical to the Subscriber Certificate ertificate Profile (Applicable to certificates i			
PRS Domai		ty – G4 or JPRS Organization Validation Au	thority – (G4)	プロファイルの適用対象の記載る 修正
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		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)	-		
	blic Key Info	The subject's Public Key (RSA 2048 bits)	-		
Extended f		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		
ExtendedK		OCSPSigning	n		
OCSP No (Uheck	null	n		記載が必要な期間が終了したの
	-	ertificate Profile (Applicable to certificates i	ssued by		削除 中間CA証明書の追加に伴うプロ
	A CA 2024 G1 or JPI	RS OV RSA CA 2024 G1)		,	ファイルの追加
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	-		

	JPRS CA	Certificate Policy(整形版)		備考
Certificate		Same as above	n	
	ibution Points	Same as above	n	
	Information Access	Same as above	n	
	Key Identifier	Same as above	n	
Subject Key Identifier		Same as above	n	
	v	ension is removed from the Precertificate, a	nd the Signe	d
tensions fi Table 7.1-8	eld MUST be byte-for 8 OCSP Responder C	noved from the Subscriber certificate, the o r-byte identical to the Subscriber Certificate ertificate Profile (Applicable to certificates i ty – G4 or JPRS Organization Validation Au	ssued by	プロファイルの適田対色の記載を
Desie fell		Description of activity	:	
Basic field		Description of setting	critical	
Version	1	Version 3	-	
Serial Nur	nber	Non-sequential values greater than zero (0) and less than 2^159 containing C4 bits of extract from a CCDDNC	-	
<u>Q:</u>	A 1	64 bits of output from a CSPRNG		
<u>Signature.</u> Issuer		sha256 With RSA Encryption		
issuer	Country	C=JP	-	
	Organization Common Name	O= Japan Registry Services Co., Ltd. (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)	-	
	ıblic 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	ey Identifier	SHA-1 hash for the subject's Public Key (160 bits)	n	
KeyUsage		digitalSignature	У	
T. (7. 11	OCCEPC:		
Extended	• •	OCSPSigning	n	
OCSP No (Uheck	null	n	記載が必要な期間が終了したので 削除
	-	ertificate Profile (Applicable to certificates i RS OV RSA CA 2024 G1)	ssued by	中間CA証明書の追加に伴うプロ ファイルの追加
Basic field		Description of setting	critical	
Version		Version 3	-	
~	nber	Non-sequential values greater than	-	

	JPRS CA Cei	tificate Policy(変更履歴付)	
		<u>64 bits of output from a CSPRNG</u>	
Signature	<u>e Algorithm</u>	sha256 With RSA Encryption	-
Issuer	Country	<u>C=JP</u>	-
	Organization	<u>O= Japan Registry Services Co., Ltd.</u>	-
	Common Name	(1) Domain Validation	<u> </u>
		CN=JPRS DV RSA CA 2024 G1	
		(2) Organization Validation	
		<u>CN= JPRS OV RSA CA 2024 G1</u>	
<u>Validity</u>	<u>NotBefore</u>	<u>E.g.) 2008/3/1 00:00:00 GMT</u>	-
	<u>NotAfter</u>	<u>E.g.) 2008/3/5 00:00:00 GMT</u>	-
<u>Subject</u>	Country	<u>C=JP (fixed value)</u>	<u> </u>
	Organization	Japan Registry Services Co., Ltd. (fixed	_
		<u>value)</u>	
	Common Name	Name of the OCSP server (mandatory)	-
Subject P	<u>ublic Key Info</u>	The subject's Public Key (RSA 4096	<u>-</u>
		bits, RSA 3072 bits or RSA 2048 bits)	
Extended	<u>l field</u>	Description of setting	<u>critical</u>
Authority	<u> Key Identifier</u>	SHA-1 hash for the issuer's Public Key	<u>n</u>
		<u>(160 bits)</u>	
Subject K	<u>Key Identifier</u>	SHA-1 hash for the subject's Public Key	<u>n</u>
		<u>(160 bits)</u>	
KeyUsag	<u>e</u>	<u>digitalSignature</u>	у
Extended	<u>lKeyUsage</u>	OCSPSigning	<u>n</u>
OCSP No	<u>Check</u>	null	<u>n</u>

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

<u>or no dv eo</u>	<u>U UA 2024 UI 01 01 1</u>	<u>(S UV ECC CA 2024 GI)</u>	
Basic field		Description of setting	<u>critical</u>
Version		Version 3	<u>-</u>
Serial Nun	<u>nber</u>	Non-sequential values greater than	1.1
		zero (0) and less than 2 ¹⁵⁹ containing	
		<u>64 bits of output from a CSPRNG</u>	
Signature	<u>Algorithm</u>	ecdsa-with-SHA384	<u>-</u>
Issuer	<u>Country</u>	<u>C=JP</u>	-
	Organization	<u>O= Japan Registry Services Co., Ltd.</u>	-
	Common Name	(1) Domain Validation	1.1
		CN=JPRS DV ECC CA 2024 G1	
		(2) Organization Validation	
		<u>CN= JPRS OV ECC CA 2024 G1</u>	
<u>Validity</u>	<u>NotBefore</u>	<u>E.g.) 2008/3/1 00:00:00 GMT</u>	<u> </u>
	<u>NotAfter</u>	<u>E.g.) 2008/3/5 00:00:00 GMT</u>	<u> </u>
Subject	<u>Country</u>	<u>C=JP (fixed value)</u>	2
	Organization	Japan Registry Services Co., Ltd. (fixed	1.1
		<u>value)</u>	
	Common Name	Name of the OCSP server (mandatory)	<u>-</u>
Subject Pu	<u>blic Key Info</u>	The subject's Public Key (256 bits or	11
		<u>384 bits)</u>	
Extended f	<u>ield</u>	Description of setting	<u>critical</u>
Authority]	<u>Key Identifier</u>	SHA-1 hash for the issuer's Public Key	<u>n</u>
		<u>(160 bits)</u>	
Subject Ke	<u>y Identifier</u>	SHA-1 hash for the subject's Public Key	<u>n</u>
		<u>(160 bits)</u>	
<u>KeyUsage</u>		<u>digitalSignature</u>	У
ExtendedK	KeyUsage	OCSPSigning	<u>n</u>
OCSP No (Check	null	<u>n</u>

	JPRS CA	Certificate Policy(整形版)		備考
		64 bits of output from a CSPRNG		
-	Algorithm	sha256 With RSA Encryption	-	
lssuer	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		
7 1. 1.		CN= JPRS OV RSA CA 2024 G1		
Validity	NotBefore	E.g.) 2008/3/1 00:00:00 GMT	-	
N 1	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	
	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 K	KevUsage	OCSPSigning	n y	
DCSP No (• •	null	n	
fable 7.1-1 RS DV EC	0 OCSP Responder	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1)		中間CA証明書の追加に伴うプ ファイルの追加
Fable 7.1-1 RS DV EC <mark>Basic field</mark>	0 OCSP Responder	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting	critical	
Fable 7.1-1 RS DV EC <mark>Basic field</mark> Version	0 OCSP Responder 0 C CA 2024 G1 or JP	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3		
Fable 7.1-1 RS DV EC <mark>Basic field</mark>	0 OCSP Responder 0 C CA 2024 G1 or JP	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than	critical	
Fable 7.1-1 RS DV EC <mark>Basic field</mark> Version	0 OCSP Responder 0 C CA 2024 G1 or JP	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing	critical	
Fable 7.1-1 RS DV EC <mark>Basic field</mark> Version Serial Nun	0 OCSP Responder (C CA 2024 G1 or JP) nber	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG	critical	
Cable 7.1-1 RS DV EC <mark>Basic field</mark> Jersion Serial Nun Signature J	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384	critical	
Fable 7.1-1 RS DV EC <mark>Basic field</mark> Version Serial Nun Signature J	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP	critical	
Sable 7.1-1 RS DV EC Basic field Jersion Serial Nun Signature J	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384	critical - - -	
Fable 7.1-1 RS DV EC <mark>Basic field</mark> Version	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd.	critical - - -	
Fable 7.1-1 RS DV EC <mark>Basic field</mark> Version Serial Nun Signature J	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation	critical - - -	
Fable 7.1-1 RS DV EC <mark>Basic field</mark> Version Serial Nun Signature J	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1	critical - - -	
Fable 7.1-1 RS DV EC <mark>Basic field</mark> Version Serial Nun Serial Nun Signature A	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation	critical - - -	
Fable 7.1-1 RS DV EC Basic field Version Serial Nun Serial Nun Signature J Ssuer	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT	critical - - - - - -	
Fable 7.1-1 RS DV EC Basic field Version Serial Nun Serial Nun Signature J Ssuer	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT	critical - - - - - -	
Fable 7.1-1 RS DV EC Basic field Version Serial Nun Serial Nun Signature J Ssuer	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT	critical - - - - - -	
Cable 7.1-1 RS DV EC Basic field Version Serial Nun Serial Nun Signature J ssuer	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter Country	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed	critical - - - - - -	
Fable 7.1-1 RS DV EC Basic field Version Serial Nun Signature 2 Signature 2 Subject	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value)	critical	
Fable 7.1-1 RS DV EC Basic field Version Serial Nun Signature A Signature A Subject Pu Subject Pu	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or	critical	
Fable 7.1-1 RS DV EC Basic field Version Serial Nun Signature 2 Signature 2 Subject Pu Subject Pu Extended f	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key	critical -	
Fable 7.1-1 RS DV EC Basic field Version Serial Num Signature 2 Issuer Validity Subject Subject Pu Extended f Authority 1	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN=JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits) SHA-1 hash for the subject's Public Key	critical -	
Fable 7.1-1 RS DV EC Basic field Version Serial Nun Signature A Subject Pu Subject Pu Extended f Authority I Subject Ke	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info Field Key Identifier	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN=JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits)	critical -	
Fable 7.1-1 RS DV EC Basic field Version Serial Num Signature 2 Subject Pu Subject Pu Extended f Authority 1	0 OCSP Responder 0 C CA 2024 G1 or JP nber Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info field Key Identifier	Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1) Description of setting Version 3 Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384 C=JP O= Japan Registry Services Co., Ltd. (1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN=JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value) Japan Registry Services Co., Ltd. (fixed value) Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits) Description of setting SHA-1 hash for the issuer's Public Key (160 bits) SHA-1 hash for the subject's Public Key	critical -	

	TPRS CA	Certificate Policy(整形版)		備考
	<u> </u>	64 bits of output from a CSPRNG		
Signature A	Algorithm	sha256 With RSA Encryption	-	
Issuer	Country	C=JP	-	
155401	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	-	
vanaity	NotAfter	E.g.) 2008/3/5 00:00:00 GMT	-	
Subject	Country	C=JP (fixed value)	-	
Bubjeet	Organization	Japan Registry Services Co., Ltd. (fixed		
	Organization	value)		
	Common Name	Name of the OCSP server (mandatory)	-	
Subject Pul	blic Key Info	The subject's Public Key (RSA 4096	-	
		bits, RSA 3072 bits or RSA 2048 bits)		
Extended fi	ield	Description of setting	critical	
	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
		(160 bits)		
Subject Key	v Identifier	SHA-1 hash for the subject's Public Key	n	
,)	(160 bits)		
KeyUsage		digitalSignature	у	
ExtendedK	evUsage	OCSPSigning	n	
OCSP No C	· · · · · · · · · · · · · · · · · · ·	null	n	
		Certificate Profile (Applicable to certificates RS OV ECC CA 2024 G1)	issued by	中間CA証明書の追加に伴うプロ
Basic field		Description of setting	critical	ファイルの追加
Basic field Version			critical -	ファイルの追加
		Description of setting	critical - -	ファイルの追加
Version		Description of settingVersion 3	critical - -	ファイルの追加
Version		Description of settingVersion 3Non-sequential values greater than	critical - -	ファイルの追加
Version	ıber	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing	critical - - -	ファイルの追加
Version Serial Num	ıber	Description of settingVersion 3Non-sequential values greater thanzero (0) and less than 2^159 containing64 bits of output from a CSPRNG	critical - - - -	ファイルの追加
Version Serial Num Signature A	ıber Algorithm	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNG ecdsa-with-SHA384	critical - - - - - -	ファイルの追加
Version Serial Num Signature A	iber Algorithm Country	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JP	<u>critical</u> - - - - - - -	ファイルの追加
Version Serial Num Signature A	aber Algorithm Country Organization	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1	critical - - - - - - -	ファイルの追加
Version Serial Num Signature A	aber Algorithm Country Organization	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation	critical - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer	Algorithm Country Organization Common Name	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1	critical - - - - - -	ファイルの追加
Version Serial Num Signature A	Algorithm Country Organization Common Name NotBefore	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT	critical - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity	aber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2008/3/5 00:00:00 GMT	critical - - - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer	Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value)	critical - - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity	aber Algorithm Country Organization Common Name NotBefore NotAfter	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2008/3/5 00:00:00 GMT	critical -	ファイルの追加
Version Serial Num Signature A Issuer Validity	Algorithm Country Organization Common Name NotBefore NotAfter Country	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMTC=JP(fixed value)Japan Registry Services Co., Ltd. (fixed	critical - - - - - - - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity Subject	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value)Japan Registry Services Co., Ltd. (fixed value)Name of the OCSP server (mandatory) The subject's Public Key (256 bits or	- - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity Subject	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value)Japan Registry Services Co., Ltd. (fixed value)Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits)	- - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity Subject Subject Pub Extended fi	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value)Japan Registry Services Co., Ltd. (fixed value)Name of the OCSP server (mandatory) The subject's Public Key (256 bits or	- - - - - - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity Subject Subject Pub Extended fi	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1 E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value)Japan Registry Services Co., Ltd. (fixed value)Name of the OCSP server (mandatory) The subject's Public Key (256 bits or 384 bits)Description of setting	- - - - - - - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity Subject Subject Pub Extended fi	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info ield Key Identifier	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT C=JP (fixed value)Japan Registry Services Co., Ltd. (fixed value)Name of the OCSP server (mandatory)The subject's Public Key (256 bits or 384 bits)Description of setting SHA-1 hash for the issuer's Public Key (160 bits)SHA-1 hash for the subject's Public Key	- - - - - - - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity Subject Subject Pub Extended fi Authority K Subject Key	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info ield Key Identifier	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2008/3/5 00:00:00 GMTC=JP (fixed value)Japan Registry Services Co., Ltd. (fixed value)Name of the OCSP server (mandatory)The subject's Public Key (256 bits or 384 bits)Description of settingSHA-1 hash for the issuer's Public Key (160 bits)SHA-1 hash for the subject's Public Key (160 bits)	- - - - - - - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity Subject Subject Pub Extended fi Authority K Subject Key KeyUsage	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info ield Key Identifier y Identifier	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1(2) Organization Validation CN=JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2008/3/5 00:00:00 GMTC=JP (fixed value)Japan Registry Services Co., Ltd. (fixed value)Name of the OCSP server (mandatory)The subject's Public Key (256 bits or 384 bits)Description of settingSHA-1 hash for the issuer's Public Key (160 bits)SHA-1 hash for the subject's Public Key (160 bits)digitalSignature	- - - - - - - - - - - - - - - - - - -	ファイルの追加
Version Serial Num Signature A Issuer Validity Subject Subject Pub Extended fi Authority K Subject Key	Algorithm Country Organization Common Name NotBefore NotAfter Country Organization Common Name blic Key Info ield Key Identifier y Identifier	Description of settingVersion 3Non-sequential values greater than zero (0) and less than 2^159 containing 64 bits of output from a CSPRNGecdsa-with-SHA384C=JPO= Japan Registry Services Co., Ltd.(1) Domain Validation CN=JPRS DV ECC CA 2024 G1 (2) Organization Validation CN= JPRS OV ECC CA 2024 G1E.g.) 2008/3/1 00:00:00 GMTE.g.) 2008/3/5 00:00:00 GMTC=JP (fixed value)Japan Registry Services Co., Ltd. (fixed value)Name of the OCSP server (mandatory)The subject's Public Key (256 bits or 384 bits)Description of settingSHA-1 hash for the issuer's Public Key (160 bits)SHA-1 hash for the subject's Public Key (160 bits)	- - - - - - - - - - - - - - - - - - -	ファイルの追加

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	$\underline{1.2.840.113549.1.1.12}$
<u>id-ecPublicKey</u>	<u>1.2.840.10045.2.1</u>
ecdsa-with-SHA384	$\underline{1.2.840.10045.4.3.3}$

7.1.4 Name Format

The CA uses the Distinguished Name specified in RFC 5280.

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

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

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

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

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

7.1.5 Name Constraints

Not set in the CA.

7.1.6 Certificate Policy Object Identifier

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

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

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

[For OV certificate] {joint-iso-itu-t(2) international-organizations(23) ca-browserforum(140) certificatepolicies(1) baseline-requirements(2) organization-validated(2)} (2.23.140.1.2.2)

JPRS CA Certific	ate Policy (整形版)	備考
 7.1.1 Version Number(s) The CA applies version 3. 7.1.2 Certificate Extension Extensions of the Certificate issued by the 7.1.3 Algorithm Object Identifier The algorithm OID used in this service is a Algorithm sha256 With RSA Encryption RSA Encryption sha384 With RSA Encryption id-ecPublicKey ecdsa-with-SHA384 7.1.4 Name Format The CA uses the Distinguished Name specifier For every valid Certification Path (as define in the Certification Path, the encoded content Certificate SHALL be byte-for-byte ident Distinguished Name field of the Issuing CA By issuing the Certificate, the CA represent CP and/or CPS to verify that, as of the Information was accurate. The CA SHAII attribute except as specified in Baseline Replication applicable. The CA will not issue a certificate with a State of the content of the content	CA is specified Section 7.1 of this CP. s follows:	備考 本サービスで用いるアルゴリズム の追加
name" field that contains a reserved IP add If the "common name" value is a fully qua the "common name" value is encoded as entry value in the Subject Alternative Nat the FQDN part of a fully qualified domain	lress or internal name. lified domain name or a wildcard domain name, a character-for-character copy of the dNSName me extension. Specifically, all Domain Labels in name or wildcard domain name are encoded as	
LDH Labels, and P-Labels does not convert 7.1.5 Name Constraints	to Unicode.	
Not set in the CA.		
7.1.6 Certificate Policy Object Ide	ntifier	
The OID of the certificate issued by the CA and Identification". The following Certificate Policy identifiers means of assertaing that a Certificate comp		
-	2) international-organizations(23) ca-browser- seline-requirements(2) domain-validated(1)}	
	2) international-organizations(23) ca-browser- ne-requirements(2) organization-validated(2)}	

7.1.7 Use of Policy Constraint Extensions

Not set.

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.

7.1.9 How to interpret Critical Certificate Policy Extensions

Not set.

7.2 CRL Profile

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 Glon or after July 29, 2020)

Basic field		Description of setting	critical
Version		Version 2	-
Signature A	lgorithm	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	E.g.) 2008/3/1 00:00:00 GMT	-
Next Updat	e	E.g.) 2008/3/5 00:00:00 GMT	-
Revoked	Serial Number	E.g.) 0123456789	-
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-
s	Reason Code	Revocation Reason Code (*)	-
Extended field		Description of setting	critical
CRL Number		CRL number	n
Authority K	Ley 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.

JPRS OV RSA CA 2024 G1)				
Basic field		Description of setting	<u>critical</u>	
Version		<u>Version 2</u>	-	
Signature A	<u>Algorithm</u>	SHA384 with RSAEncryption	-	
Issuer	Country	<u>C=JP</u>	-	
	Organization	<u>O= Japan Registry Services Co., Ltd.</u>	-	
	Common Name	(1) Domain Validation	-	
		<u>CN= JPRS DV RSA CA 2024 G1</u>		
		(2) Organization Validation		
		<u>CN=JPRS OV RSA CA 2024 G1</u>		
This Updat	<u>e</u>	<u>E.g.) 2008/3/1 00:00:00 GMT</u>	-	
Next Upda	te	<u>E.g.) 2008/3/5 00:00:00 GMT</u>	-	
Revoked	Serial Number	<u>E.g.) 0123456789</u>	-	
<u>Certificate</u>	Revocation Date	<u>E.g.) 2008/3/1 00:00:00 GMT</u>	-	

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

	JPRS CA Certificate Policy (整形版) 備考					
717100						
	of Policy Constra					
Not set.						
7.1.8 Polic	y Qualifier Synta	ax and Semantics				
For the policy	qualifier, the URI of	the Web page that publishes this CP and C	CPS is stored.			
719How	to interpret Criti	cal Certificate Policy Extensions				
	to interpret onti					
Not set.						
7.2 CRL Pi	ofile					
The profile of	CRLs to be issued by	v the CA shall be as described in the followi	ng table:			
Table 7.9.1 (1	Deleted			プロファイルの適用対象の記載を		
Table 7.2.1 (I Table 7.2.2 C		le to certificates issued by JPRS Domain Va	alidation	修正		
		tion Validation Authority $-G4$)				
Basic field		Description of setting	critical			
Version	1	Version 2	-			
Signature A Issuer	-	SHA256 with RSAEncryption C=JP	-			
issuer	Country 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 Updat		E.g.) 2008/3/5 00:00:00 GMT	-			
Revoked	Serial Number	E.g.) 0123456789	-			
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-			
S	Reason Code	Revocation Reason Code (*)	-			
Extended fi		Description of setting	critical			
CRL Numbe	er Tey Identifier	CRL number SHA-1 hash for the issuer's Public Key	n n			
Authority is	ey identilier	(160 bits)	11			
*: The "Rea	son Code" field is se	t one of the Revocation Reason code specifi	ed in the tabl	e		
		on Code is "#0 unspecified", the "Reason C	ode" field doe	28		
not appear	in the CRL profile.					
Table 7.2.3 C	RL Profile (applicab	le to certificates issued by JPRS DV RSA C	A 2024 G1 or			
JPRS OV RSA				中間CA証明書の追加に伴うプロ		
Basic field		Description of setting	critical	ファイルの追加		
Version		Version 2	-			
Signature A	-	SHA384 with RSAEncryption	-			
Issuer	Country Organization	C=JP O= Japan Registry Services Co., Ltd.	-			
	Common Name	(1) Domain Validation	-			
		CN= JPRS DV RSA CA 2024 G1				
		(2) Organization Validation				
		CN=JPRS OV RSA CA 2024 G1				
This Update		E.g.) 2008/3/1 00:00:00 GMT	-			
Next Updat Revoked	e Serial Number	E.g.) 2008/3/5 00:00:00 GMT E.g.) 0123456789				
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-			
	11 / 10					

	JPRS CA (Certificate Policy (整形版)		備考
7471100	of Dolioy Constr			
	of Policy Constr			
Not set.				
7.1.8 Polic	y Qualifier Synt	ax and Semantics		
		f the Web page that publishes this CP and (CPS is stored.	
	-			
7.1.9 How	to interpret Crit	ical Certificate Policy Extensions		
Not set.				
7.2 CRL Pi	ofile			
-		y the CA shall be as described in the followi	ng tahle:	
The profile of	CITES to be issued by	y the Crishan be as described in the following	ing table.	
Table 7.2.1 (I				プロファイルの適用対象の記載を
		ble to certificates issued by JPRS Domain Va	alidation	修正
Authority – G Basic field	4 or JPRS Organiza	tion Validation Authority – G4)	anitical	
Version		Description of settingVersion 2	critical -	
Signature A	lgorithm	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	E.g.) 2008/3/1 00:00:00 GMT	-	
Next Updat		E.g.) 2008/3/5 00:00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
S East and a d.C.	Reason Code	Revocation Reason Code (*)	-	
Extended field		Description of setting CRL number	critical	
	key Identifier	SHA-1 hash for the issuer's Public Key	n n	
11001101109 11		(160 bits)		
		et one of the Revocation Reason code specifi		
		on Code is "#0 unspecified", the "Reason C	ode" field doe	s
not appear	in the CRL profile.			
Table 7 2 3 C	RL Profile (applicab	le to certificates issued by JPRS DV RSA C	A 2024 G1 or	
	A CA 2024 G1)			中間CA証明書の追加に伴うプロ
Basic field		Description of setting	critical	ファイルの追加
Version		Version 2	-	
Signature Algorithm		SHA384 with RSAEncryption	-	
Issuer	Country	C=JP	-	
	Organization Common Name	O= Japan Registry Services Co., Ltd. (1) Domain Validation		
		CN= JPRS DV RSA CA 2024 G1		
		(2) Organization Validation		
		CN=JPRS OV RSA CA 2024 G1		
This Update		E.g.) 2008/3/1 00:00:00 GMT	-	
Next Updat		E.g.) 2008/3/5 00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	

	JPRS CA (Certificate Policy(整形版)		備考
7471100				
	of Policy Constr	aint Extensions		
Not set.				
7.1.8 Polic	cy Qualifier Synt	ax and Semantics		
		f the Web page that publishes this CP and (CPS is stored	
	-		51 6 15 5torea.	
7.1.9 How	to interpret Crit	ical Certificate Policy Extensions		
Not set.				
7.2 CRL P	rofilo			
-		y the CA shall be as described in the followi	ng tahle:	
rite profile of	CILLS to be issued b.	y the Crishan be as described in the following	ing table.	
Table 7.2.1 (プロファイルの適用対象の記載を
		ble to certificates issued by JPRS Domain Va	alidation	修正
	4 or JPRS Organiza	tion Validation Authority – G4)		
Basic field Version		Description of settingVersion 2	critical -	
Signature A	Algorithm	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 Updat	ie	E.g.) 2008/3/1 00:00:00 GMT	-	
Next Updat	te	E.g.) 2008/3/5 00:00:00 GMT	-	
Revoked	Serial Number	E.g.) 0123456789	-	
Certificate	Revocation Date	E.g.) 2008/3/1 00:00:00 GMT	-	
s Extended fi	Reason Code	Revocation Reason Code (*) Description of setting	critical	
CRL Numb		CRL number	n	
	Key Identifier	SHA-1 hash for the issuer's Public Key	n	
	C C C C C C C C C C C C C C C C C C C	(160 bits)		
		et one of the Revocation Reason code specifi		
	the Revocation Reas r in the CRL profile.	on Code is "#0 unspecified", the "Reason C	ode" field does	
not appear	r in the CIL prome.			
Table 7.2.3 (CRL Profile (applicat	le to certificates issued by JPRS DV RSA C	A 2024 G1 or	
	A CA 2024 G1)			中間CA証明書の追加に伴うプロ
Basic field		Description of setting	critical	ファイルの追加
Version Signature Algorithm		Version 2	-	
Issuer	Country	SHA384 with RSAEncryption C=JP	-	
155001	Organization	O= Japan Registry Services Co., Ltd.	-	
	Common Name	(1) Domain Validation	-	
		CN= JPRS DV RSA CA 2024 G1		
		(2) Organization Validation		
This II- 1 -		CN=JPRS OV RSA CA 2024 G1		
This Updat Next Updat		E.g.) 2008/3/1 00:00:00 GMT E.g.) 2008/3/5 00:00:00 GMT		
		E.g.) 22008/3/3 00:00:00 GM1 E.g.) 0123456789	-	
Revoked Serial Number				

JPRS CA Certificate Policy(変更履歴付)			
<u>s</u>	Reason Code	Revocation Reason Code (*)	-
Extended field	<u>eld</u>	Description of setting	critical
CRL Number		<u>CRL number</u>	<u>n</u>
Authority Key Identifier		SHA-1 hash for the issuer's Public Key	<u>n</u>
		<u>(160 bits)</u>	

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

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

7.2.1 Version Number(s)

The CA applies CRL version 2.

7.2.2 CRL Entry Extensions

Use the CRL extension field issued by the CA. reasonCode (OID 2.5.29.21)

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

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

Table 7.2.2.1 Revocation Reason Code

Revocation Reason Code	Circumstances for setting this Revocation Reason	
	Code	
#0 unspecified	When the reason codes below do not apply to the	
	revocation request.	
#1 keyCompromise	When the Subscriber have reasons to believe that	
	the private key of their certificate has been or may	
	be compromised,	

		JPRS CA Ce	ertificate Policy(整形版)
	s	Reason Code	Revocation Reason Code (*)
	Extended field		Description of setting
CRL Number		er	CRL number
	Authority Key Identifier		SHA-1 hash for the issuer's Public Key
			(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 I	ECC (
JPRS OV ECC CA 2024 G1)	

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

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

7.2.1 Version Number(s)

The CA applies CRL version 2.

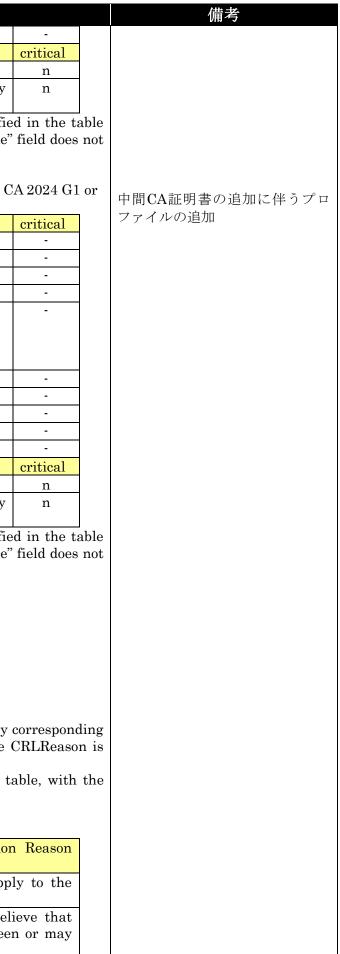
7.2.2 CRL Entry Extensions

Use the CRL extension field issued by the CA. reasonCode (OID 2.5.29.21)

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

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

Revocation Reason Code	Circumstances for setting this Revocation	
	Code	
#0 unspecified	When the reason codes below do not app	
	revocation request.	
#1 keyCompromise	When the Subscriber have reasons to bel	
	the private key of their certificate has bee	
	be compromised,	



JPRS CA Certificate Policy(変更履歴付)		
#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.

8. Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

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

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

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

8.3 Assessor's Relationship to Assessed Entity

Auditors shall be operationally independent of the auditee divisions, except in matters related to the audits.

8.4 Topics Covered by Assessment

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

JPRS CA	Certificate Policy(整形版)	備考
#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 Versio	n 1.	
7.3.2 OCSP Extensions		
Refer to Section 7.1 of this CP.	CSP response MUST NOT contain the reasonCode (O	
2.5.29.21) CRL entry extension.	of response most not contain the reasoncode (O	
8. Compliance Auc	lit and Other Assessments	
8.1 Frequency and Circu	umstances of Assessment	
		tod
in compliance with this CP and t	ast once a year to verify whether or not the CA is operative the CPS	ieu
in compliance with this Or allu (
8.2 Identity/Qualification	ns of Assessor	
	rformed by auditors who are adequately experienced	in
auditing.		
	the WebTrust certification shall be performed by au	dit
corporations with the following of	qualifications and skills:	
- Independence from the s	ubject 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 Infrastructur	e
technology, information s	ecurity tools and techniques, information technology and	
security auditing, and th	e third-party attestation function;	
- licensed by WebTrust;		
- Bound by law, governmen		
- Except in the case of an I		
Professional Liability/Er		
one million US dollars in		
0 2 Annon aria Delettor	ohin to Accord Entity	
8.3 Assessor's Relation	• •	
Auditors shall be operationally independent of the auditee divisions, except in matters		
related to the audits.		
8.4 Topics Covered by Assessment		
Audits shall be performed mainly to verify whether or not the CA is operated in compliance		
-	CA shall undergo WebTrust in accordance with one of t	

following schemes: - WebTrust for CAs - WebTrust for CAs SSL Baseline with Network Security	following schemes: - WebTrust for CAs - WebTrust for CAs SSL Baseline with Network Security
8.5 Actions Taken as a Result of Deficiency The CA shall promptly take necessary corrective actions with respect to any deficiencies pointed out in an audit report.	8.5 Actions Taken as a Result of Deficiency The CA shall promptly take necessary corrective actions with respect to a pointed out in an audit report.
 8.6 Communication of Results Auditors shall report the audit results to the CA. The CA will not externally disclose the audit results unless the CA is 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. 	 8.6 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 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 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.	8.7 Self-Audits The CA shall monitor adherence this CP, the CPS, and strictly control its sep performing self audits on at least a quarterly basis against a randomly self at least three percent of the Certificates issued by it during the period immediately after the previous self-audit sample was taken.
9. Other Business and Legal Matters	9. Other Business and Legal Matters
9.1 Fees To be separately stipulated.	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.	9.2 Financial Responsibility The CA shall maintain a sufficient financial foundation required for maintaining the CA.
9.3 Confidentiality of Business Information	9.3 Confidentiality of Business Information
9.3.1 Scope of Confidential Information	9.3.1 Scope of Confidential Information
Stipulated in the CPS.	Stipulated in the CPS.
9.3.2 Information not within the 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.	9.3.3 Responsibility to Protect Confidential Information Stipulated in the CPS.
9.4 Privacy of Personal 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 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- 	 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 crevocation; 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- NoD
	44/48

JPRS CA Certificate Policy(整形版)

JPRS CA Certificate Policy(変更履歴付)

	備考
1. 6	
any deficiencies	
aired to disclose agreement with	
icate Operation	
a specific site	
rvice quality by ected sample of	
od commencing	
operating and	
mation	
mation	
o the following	
certificate	
Derivatives (CC-	

BY-ND) 4.0 International.



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

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 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;

JPRS CA Certificate Policy (整形版)

BY-ND) 4.0 International.



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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The CA shall bear the following obligations in performing its business oper CA:

- 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 operat

- 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 imposi Applicant itself (or made by the Applicant on behalf of its principal or agent subcontractor or hosting service relationship) the following obligations and w

- 1. Accuracy of Information: An obligation and warranty to provide accur complete information at all times to the CA, both in the certificate reotherwise requested by the CA in connection with the issuance of the to be supplied by the CA;
- 2. **Protection of Private Key**: An obligation and warranty by the Applica reasonable measures to assure control of, keep confidential, and propall times the Private Key that corresponds to the Public Key to be inc requested Certificate(s) (and any associated activation data or device, or token);
- 3. Acceptance of Certificate: An obligation and warranty that the Subscrive review and verify the Certificate contents for accuracy;
- 4. **Use of Certificate**: An obligation and warranty to install the Certificat servers that are accessible at the subjectAltName(s) listed in the Certuse the Certificate solely in compliance with all applicable laws and s accordance with the Subscriber Agreement or Terms of Use;

	備考
erations as the	
ations from the	
tions as an RA: m;	
ons for	
in processing	
in processing	
se, that the	
efit of the CA	
ing on the under a	
warranties:	
rate and	
equest and as e Certificate(s)	
, UCI 1111001E(B)	
ant to take all	
perly protect at	
cluded in the e, e.g. password	
, 5.8. passion	
criber will	
ate only on	
rtificate, and to	
solely in	

- 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

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

9.8 Limitations of Liability

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

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

JPRS CA Certificate Policy (整形版)

- 5. **Reporting and Revocation**: An obligation and warranty to: a. promptly revocation of the Certificate, and cease using it and its associated Pri there is any actual or suspected misuse or compromise of the Subscrift Key associated with the Public Key included in the Certificate, and by request revocation of the Certificate, and cease using it, if any inform Certificate is or becomes incorrect or inaccurate;
- 6. **Termination of Use of Certificate**: An obligation and warranty to pror use of the Private Key corresponding to the Public Key included in th upon revocation of that Certificate for reasons of Key Compromise.
- 7. **Responsiveness**: An obligation to respond to the CA's instructions con Compromise or Certificate misuse within a specified time period.
- 8. Acknowledgment and Acceptance: An acknowledgment and acceptance is entitled to revoke the certificate immediately if the Applicant were terms of the Subscriber Agreement or Terms of Use or if revocation is the CA's CP, CPS, or these Baseline Requirements.

9.6.4 Relying Party Representations and Warranties

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

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimer of Warranties

The CA is not liable for any indirect, special, incidental, or consequential dan 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 oth consequential 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 cause reason not attributable to the CA;
- any or all damage arising in connection with the use of a certificate, su debts;
- any damage caused by an improvement, beyond expectations at this po the cryptographic algorithm decoding capabilities of hardware or softw
- any or all damage caused by the suspension of the CA's business operation force majeure event, including, but not limited to, any act of God, earth volcanic eruption, fire, tsunami, flood disaster, lightning strike, war, cities and the suspension of the transmission of transmission of the transmission of the transmission of transmission of the transmission of the transmission of the transmission of the transmission of transmission o

	備考
ly request ivate Key, if iber's Private o. promptly nation in the	
mptly cease all ne Certificate	
ncerning Key	
ace that the CA e to violate the s required by	
of this CP. If Party shall	
i	
mage arising in sentations and her indirect or	
rranties" of this	
se, negligence,	
his/her/its	
's system; he hardware or	
e CRL, for any	
sed by any	
uch as business	
oint in time, in vare; ations due to a hquake, ivil 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 Each Subscriber shall become liable to indemnify and hold harmless t organizations or other entities related to the CA, upon applying for, receiving, and trusting certificates issued by the CA. The events to be covered by the foregoing liabilities include any loss, damage, lawsuit, mistake, omission, act, delay of, or failure in performance, or any other event that may incur cost burdens of any kind. The Terms and Conditions stipulate a policy on indemnification to Subscribers for damage.

9.10 Term and Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

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

9.12.3 Circumstances under Which OID Must Be Changed

No stipulation.

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

JPRS CA Certificate Policy (整形版)

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 certificat

9.9 Indemnities

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 p any other event that may incur cost burdens of any kind. The Terms a stipulate a policy on indemnification to Subscribers for damage.

9.10 Term and Termination

9.10.1 Term

This CP shall come into effect upon approval by the CA's Certificate 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 Relving Parties on e-mail, in writing, or by other means.

9.12 Amendments

9.12.1 Procedure for Amendment

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

9.12.2 Notification Mechanism and Period

If the CA amends this CP, the CA shall promptly publish the amended vers 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 certifica a lawsuit, refer the dispute to arbitration, or take any other legal action a such party shall notify the CA to that effect in advance. The Tokyo Distr have the agreed exclusive jurisdiction over all disputes involving the Servi instance.

9.14 Governing Law

Regardless of the respective addresses of the CA and Subscribers, the laws of Japan shall | Regardless of the respective addresses of the CA and Subscribers, the laws

	備考
egistration and e issuance.	
the CA or any ng, and trusting abilities include performance, or and Conditions	
ion Conference. ation stipulated	
in "9.10.3 Effect	
en a Subscriber should survive cribers, Relying	
;ipants its Web site, by	
revised version Conference.	
rsion of this CP,	
ate, seeks to file against the CA, rict Court shall ices in the first	
s of Japan shall	

apply to any dispute over the interpretation or validity of this CP, or the use of a apply to certificate.

9.15 Compliance with Applicable Laws

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

9.16 Miscellaneous Provisions

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

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

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

9.17 Other Provisions Not applicable.

JPRS CA Certificate Policy (整形版)

apply to any dispute over the interpretation or validity of this CP, or certificate.

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

9.16 Miscellaneous Provisions

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

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

Any modification to the CA practice enabled under this section MUST be and when the Law no longer applies, or these Requirements are modifipossible to comply with both them and the Law simultaneously. An appropripractice, modification to the CA's CPS and a notice to the CA/Browser Ford above, MUST be made within 90 days.

9.17 Other Provisions Not applicable.

	備考
r the use of a	
l law applicable operates.	
or government ues certificates, ressary to make o operations or ne CA SHALL nent) include in modification of tion to these	
irement) notify S by sending a been posted to s available at d links as the ble revisions to	
discontinued if ied to make it riate change in um, as outlined	