KPMG あずさ監査法人

有限責任 あずさ監査法人
〒162-8551
東京都新宿区津久戸町 1 番 2 号
あずさセンタービル
Telephone 03 3266 7500
Fax 03 3266 7600
Internet home.kpmg/jp/azsa

独立業務実施者の保証報告書

2025 年 8 月 5 日

株式会社日本レジストリサービス
代表取締役社長　東田 幸樹　殿

有限責任 あずさ監査法人
東京事務所
パートナー　公認会計士 紫垣昌利

範囲

当監査法人は、認証局のための WebTrust-SSL 基本要件保証規準 v2.8（the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8）に準拠して、2024 年 6 月 7 日から 2025 年 6 月 6 日までの期間において、付録 A に記載された株式会社日本レジストリサービスの認証局（以下「CA」という。）のサービス（東京）（以下「SSL CA サービス」という。）に関する経営者の記述書について合理的保証業務を行った。

経営者の記述書によれば、株式会社日本レジストリサービスは SSL CA サービスについて、下記事項を実施していた。

1. 株式会社日本レジストリサービスは、CA ブラウザフォーラムガイドラインに準拠して SSL 証明書を提供するためのコミットメントを含む SSL 証明書ライフサイクル管理のビジネス実務を株式会社日本レジストリサービスのウェブサイトで付録 B に記載された認証局運用規程及び証明書ポリシーにて開示し、当該開示された実務に従ってサービスを提供していた。

2. 株式会社日本レジストリサービスは、下記について合理的な保証を提供するための有効な内部統制を維持していた。
   - 管理する鍵と SSL 証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
   - SSL 加入者情報は、（株式会社日本レジストリサービスが行う登録業務のため）適切に認証されていたこと。

3. 株式会社日本レジストリサービスは、下記について合理的な保証を提供するための有効な内部統制を維持していた。
   - CA システムとデータへの論理的、物理的アクセスは、承認された個人に制限されていたこと。
   - 鍵と証明書の管理に関する運用の継続性が維持されていたこと。

KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

・ CA システムのインテグリティを維持するため、CA システムに係る開発、保守及び運用は適切に承認され、実施されていたこと。

認証局の責任

株式会社日本レジストリサービスの経営者の責任は、認証局のための WebTrust-SSL 基本要件保証規準 v2.8 に準拠して、経営者の記述書を適正に作成すること、及び、記述書に記載されたサービスを提供することにある。

業務実施者の職業倫理、独立性及び品質管理

当監査法人は、誠実性、客観性、職業的専門家としての能力及び正当な注意、守秘義務及び職業的専門家としての行動に関する基本原則を基礎とする国際会計士倫理基準審議会の職業会計士のための国際倫理規程（国際独立性基準を含む。）（国際倫理規程）の独立性及びその他の職業倫理に関する規定を遵守した。

また、当監査法人は、国際品質マネジメント基準第１号「財務諸表の監査若しくはレビュー又はその他の保証若しくは関連サービス業務を行う事務所の品質マネジメント」を適用しており、これは、職業倫理に関する規定、職業的専門家としての基準及び適用される法令等の要求事項の遵守に関する方針と手続を含む、品質マネジメントシステムをデザイン、適用及び運用することを要求している。

業務実施者の責任

当監査法人の責任は、当監査法人の実施した手続に基づいて経営者の記述書に対して意見を表明することにある。

当監査法人は、国際監査・保証基準審議会が公表した国際保証業務基準 3000「過去財務情報の監査又はレビュー以外の保証業務」に準拠して業務を実施した。当該指針は、当監査法人に、すべての重要な点において、経営者の記述書が適正に表示されているかどうかについて、合理的な保証を得るための手続を計画し実施することを求めている。従って、手続には、(1)株式会社日本レジストリサービスの SSL 証明書の発行、更新、失効にわたる関連する内部統制を含む SSL 証明書ライフサイクル管理のビジネス実務を理解すること、(2)株式会社日本レジストリサービスが開示した SSL 証明書ライフサイクル管理のビジネス実務に従って実施された取引を試査によりテストすること、(3)内部統制の運用評価手続を実施し評価すること、(4)当監査法人が状況に応じて必要と認めたその他の手続を実施することを含んでいる。

当監査法人は、意見表明の基礎となる十分かつ適切な証拠を入手したと判断している。

株式会社日本レジストリサービスにおける特定の内部統制の相対的な有効性と重要性、及び加入者と信頼者の内部統制リスクの評価に与える影響は、内部統制との相互作用、及び個々の加入者と信頼者の所在場所において現れるその他の要因に依存している。当監査法人は個別の加入者と信頼者の所在場所における内部統制の有効性を評価するための手続を実施していない。

内部統制の限界

内部統制の有効性には、人為的なミスの可能性や内部統制の回避など、固有の限界がある。例えば、その性質により、内部統制は、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反を防止、発見することができないことがある。又、当監査法人の発見事項に基づく結論の将来への予測は、内部統制が無効になる可能性があるというリスクの影響を受ける。

KPMG

意見

当監査法人は、株式会社日本レジストリサービスの経営者の記述書が、認証局のための WebTrust-SSL 基本要件保証規準 v2.8 に基づいて、2024 年 6 月 7 日から 2025 年 6 月 6 日までの期間において、すべての重要な点において適正に表示されているものと認める。

この保証報告書は、認証局のための WebTrust-SSL 基本要件保証規準 v2.8 が対象としている範囲を超えて、株式会社日本レジストリサービスのサービスの品質について何ら表明するものではない。また、いかなる顧客の意図する目的に対する株式会社日本レジストリサービスのサービスの適合性についても何ら表明するものではない。

WebTrust シールの使用

株式会社日本レジストリサービスの認証局のための WebTrust-SSL シールの使用は、この保証報告書の内容を象徴的に表示しているが、この保証報告書の変更又は追加的な保証を提供することを意図したものではなく、そのような解釈をすべきではない。

付録 A

対象 CA

OV SSL Issuing CAs
CA#1: JPRS Organization Validation Authority - G4
CA#2: JPRS OV RSA CA 2024 G1
CA#3: JPRS OV ECC CA 2024 G1
Other CAs
CA#4: JPRS Domain Validation Authority - G4
CA#5: JPRS DV RSA CA 2024 G1
CA#6: JPRS DV ECC CA 2024 G1

対象CAの識別情報

CA #	Cert #	サブジェクト	発行者	シリアル番号	キーアルゴリズム	キーサイズ	ダイジェストアルゴリズム	有効期限の開始	有効期限の終了	サブジェクト キー識別子	拇印	ポリシーオブジェクト識別子
1	1	CN = JPRS Organization Validation Authority - G4 O = Japan Registry Services Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B17E7B3B17E9FEE430280C2C2F59	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 22 10:23:28 2020 GMT	May 29 05:00:39 2029 GMT	D535AEC4D4326E8029152AD4001CB4ED23B92B38	801C522D3AD138E4F05D467EA369C1CC276078BF284018D0525EBBBC5342C836	2.23.140.1.2.2
2	1	CN = JPRS OV RSA CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911EF8E1B63325130A546BDC62E8	rsaEncryption	4096bit	sha384WithRSAEncryption	Apr 4 05:05:41 2024 GMT	Jan 12 00:00:00 2039 GMT	F5B655E3DBDC66D6A031C170DD22C7D1BDCAF25D	DAFA254E0173F0FD793A92ECFDF2C72C53EA5A761A73B7A3394C49182EA90933	2.23.140.1.2.2
3	1	CN = JPRS OV ECC CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA46F91F30C80CCC1CC1DCFDD294	id-ecPublicKey	384bit	ecdsa-with-SHA384	Apr 4 05:53:50 2024 GMT	Jun 16 00:00:00 2031 GMT	7E9E2AAE6A8D400A7BB211666055F1BFAF6CEC18	9C280369D072F89D9C9B62640BBF2F28D2F30ECEE9759854031D5C5C53E8D1B6	2.23.140.1.2.2
4	1	CN = JPRS Domain Validation Authority - G4 O = Japan Registry Services Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B17F05E48A55E6F5EF198802FFB9	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 22 10:40:53 2020 GMT	May 29 05:00:39 2029 GMT	7C24CE0DA4382DC7B3635EA7787A8D1D4C2EC715	F19D55CD08A3EA42BD91508073823174DD92370213C177F82531756DA7508A51	2.23.140.1.2.1

CA #	Cert #	サブジェクト	発行者	シリアル番号	キーアルゴリズム	キーサイズ	ダイジェストアルゴリズム	有効期限の開始	有効期限の終了	サブジェクト キー識別子	拇印	ポリシーオブジェクト識別子
5	1	CN = JPRS DV RSA CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911DF50A9BCFBACCC94B6211D57F	rsaEncryption	4096bit	sha384WithRSAEncryption	Apr 4 04:50:03 2024 GMT	Jan 12 00:00:00 2039 GMT	A21DF57FCA6D049184686DB817EA184A9AA8CAFD	52361A6ABC835E7AD4B375F2165055303169DDE9FBEB4FAAF588ED532DDC2DCB	2.23.140.1.2.1
6	1	CN = JPRS DV ECC CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA4500ACA26353B09C3F0C6B6EBF	id-ecPublicKey	384bit	ecdsa-with-SHA384	Apr 4 05:30:34 2024 GMT	Jun 16 00:00:00 2031 GMT	587C1D2586486AEC293ABAEF5E4D7DABF44050BF	1B901D550A5A51F6737279C6021445F051BD293015612A5BAA3F8588829EE69A	2.23.140.1.2.1

付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 CA#2	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.80	2025/5/20
CA#3 CA#4	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.74	2025/3/27
CA#5 CA#6	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.73	2024/11/7
	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.72	2024/8/26
	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.71	2024/6/5

運用規程

CA	CPS 名	Version	日付
CA#1 CA#2	JPRS サーバー証明書認証局運用規程（Certification Practice Statement）	1.54	2025/5/20
CA#3 CA#4	JPRS サーバー証明書認証局運用規程（Certification Practice Statement）	1.53	2024/11/7
CA#5 CA#6	JPRS サーバー証明書認証局運用規程（Certification Practice Statement）	1.52	2024/8/26
	JPRS サーバー証明書認証局運用規程（Certification Practice Statement）	1.51	2024/6/5

以上

経営者の記述書

2025 年 8 月 5 日

株式会社日本レジストリサービス

代表取締役社長 

当社は、付録 A に記載された認証局（以下「CA」という。）を運営し、SSL 認証局サービス（以下「SSL CA サービス」という。）を提供している。

当社の経営者は、当社の Web サイトで公開している SSL CA ビジネス実務の開示、SSL 鍵ライフサイクル管理の内部統制、SSL 証明書ライフサイクル管理の内部統制を含む当社の SSL CA の運用について、有効な内部統制を確立し、維持することに責任がある。これらの内部統制はモニタリングの仕組みを含んでおり、識別された欠陥を修正するための行動が取られる。

内部統制には、人為的なミスの可能性や内部統制の回避など、固有の限界がある。従って、有効な内部統制といえども、当社の CA の運用について合理的な保証を提供するものでしかない。さらに、状況の変化により、内部統制の有効性は時間とともに変化する場合がある。

当社の経営者は、当社の SSL CA サービス（東京）に係る証明書実務の開示と内部統制を評価した。その評価に基づく当社の経営者の意見では、当社は、認証局のための WebTrust-SSL 基本要件保証規準 v2.8（the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8）に準拠して、2024 年 6 月 7 日から 2025 年 6 月 6 日までの期間において、SSL CA サービスの提供に関して、下記の事項を実施した。

1. CA ブラウザフォーラムガイドラインに準拠して SSL 証明書を提供するためのコミットメントを含む SSL 証明書ライフサイクル管理のビジネス実務を、当社のウェブサイトで付録 B に記載された認証局運用規程及び証明書ポリシーにて開示し、当該開示された実務に従ってサービスを提供していた。

2. 下記について合理的な保証を提供するための有効な内部統制を維持していた。
   - 管理する鍵と SSL 証明書のインテグリティが確立され、そのライフサイクルを通じて保護されていたこと。
   - SSL 加入者情報は、（当社が行う登録業務のため）適切に認証されていたこと。

3. 下記について合理的な保証を提供するための有効な内部統制を維持していた。
   - CA システムとデータへの論理的、物理的アクセスは、承認された個人に制限されていたこと。
   - 鍵と証明書の管理に関する運用の継続性が維持されていたこと。
   - CA システムのインテグリティを維持するため、CA システムに係る開発、保守及び運用は適切に承認され、実施されていたこと。

付録 A

対象CA

OV SSL Issuing CAs
CA#1: JPRS Organization Validation Authority - G4
CA#2: JPRS OV RSA CA 2024 G1
CA#3: JPRS OV ECC CA 2024 G1
Other CAs
CA#4: JPRS Domain Validation Authority - G4
CA#5: JPRS DV RSA CA 2024 G1
CA#6: JPRS DV ECC CA 2024 G1

対象 CA の識別情報

CA #	Cert #	サブジェクト	発行者	シリアル番号	キーアルゴリズム	キーサイズ	ダイジェストアルゴリズム	有効期限の開始	有効期限の終了	サブジェクト キー識別子	拇印	ポリシーオブジェクト識別子
1	1	CN = JPRS Organization Validation Authority - G4 O = Japan Registry Services Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B17E7B3B17E9FEE430280C2C2F59	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 22 10:23:28 2020 GMT	May 29 05:00:39 2029 GMT	D535AEC4D4326E8029152AD4001CB4ED23B92B38	801C522D3AD138E4F05D467EA369C1CC276078BF284018D0525EBBBC5342C836	2.23.140.1.2.2
2	1	CN = JPRS OV RSA CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911EF8E1B63325130A546BDC62E8	rsaEncryption	4096bit	sha384WithRSAEncryption	Apr 4 05:05:41 2024 GMT	Jan 12 00:00:00 2039 GMT	F5B655E3DBDC66D6A031C170DD22C7D1BDCAF25D	DAFA254E0173F0FD793A92ECFDF2C72C53EA5A761A73B7A3394C49182EA90933	2.23.140.1.2.2
3	1	CN = JPRS OV ECC CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA46F91F30C80CCC1CC1DCFDD294	id-ecPublicKey	384bit	ecdsa-with-SHA384	Apr 4 05:53:50 2024 GMT	Jun 16 00:00:00 2031 GMT	7E9E2AAE6A8D400A7BB211666055F1BFAF6CEC18	9C280369D072F89D9C9B62640BBF2F28D2F30ECEE9759854031D5C5C53E8D1B6	2.23.140.1.2.2
4	1	CN = JPRS Domain Validation Authority - G4 O = Japan Registry Services Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B17F05E48A55E6F5EF198802FFB9	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 22 10:40:53 2020 GMT	May 29 05:00:39 2029 GMT	7C24CE0DA4382DC7B3635EA7787A8D1D4C2EC715	F19D55CD08A3EA42BD91508073823174DD92370213C177F82531756DA7508A51	2.23.140.1.2.1

CA #	Cert #	サブジェクト	発行者	シリアル番号	キーアルゴリズム	キーサイズ	ダイジェストアルゴリズム	有効期限の開始	有効期限の終了	サブジェクト キー識別子	拇印	ポリシーオブジェクト識別子
5	1	CN = JPRS DV RSA CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911DF50A9BCFBACCC94B6211D57F	rsaEncryption	4096bit	sha384WithRSAEncryption	Apr 4 04:50:03 2024 GMT	Jan 12 00:00:00 2039 GMT	A21DF57FCA6D049184686DB817EA184A9AA8CAFD	52361A6ABC835E7AD4B375F2165055303169DDE9FBEB4FAAF588ED532DDC2DCB	2.23.140.1.2.1
6	1	CN = JPRS DV ECC CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA4500ACA26353B09C3F0C6B6EBF	id-ecPublicKey	384bit	ecdsa-with-SHA384	Apr 4 05:30:34 2024 GMT	Jun 16 00:00:00 2031 GMT	587C1D2586486AEC293ABAEF5E4D7DABF44050BF	1B901D550A5A51F6737279C6021445F051BD293015612A5BAA3F8588829EE69A	2.23.140.1.2.1

付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 CA#2 CA#3 CA#4 CA#5 CA#6	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.80	2025/5/20
	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.74	2025/3/27
	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.73	2024/11/7
	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.72	2024/8/26
	JPRS サーバー証明書認証局証明書ポリシー（Certificate Policy）	3.71	2024/6/5

運用規程

CA	CPS 名	Version	日付
CA#1 CA#2 CA#3 CA#4 CA#5 CA#6	JPRS サーバー証明書認証局運用規程（Certification Practice Statement）	1.54	2025/5/20
	JPRS サーバー証明書認証局運用規程（Certification Practice Statement）	1.53	2024/11/7
	JPRS サーバー証明書認証局運用規程（Certification Practice Statement）	1.52	2024/8/26
	JPRS サーバー証明書認証局運用規程（Certification Practice Statement）	1.51	2024/6/5

以上

KPMG AZSA LLC
AZSA Center Building
1-2 Tsukudo-cho, Shinjuku-ku
Tokyo 162-8551, Japan
Telephone +81 (3) 3266 7500
Fax +81 (3) 3266 7600
Internet home.kpmg/jp/azsa

(Translation)

INDEPENDENT ASSURANCE REPORT

August 5, 2025

To Mr. Koki Higashida
President
Japan Registry Services Co., Ltd.

KPMG AZSA LLC
Tokyo Office
Partner, Certified Public Accountant
Masatoshi Shigaki

Scope

We have been engaged, in a reasonable assurance engagement, to report on the management's assertion of Japan Registry Services Co., Ltd. ("JPRS") that for its Certification Authority (CA) operations at Tokyo, Japan, throughout the period June 7, 2024 to June 6, 2025, for its CAs as enumerated in Appendix A, JPRS has:

1. disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in Appendix B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the JPRS website, and provided such services in accordance with its disclosed practices

2. maintained effective controls to provide reasonable assurance that:

   - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
   - SSL subscriber information is properly authenticated (for the registration activities performed by JPRS)

3. maintained effective controls to provide reasonable assurance that:

   - logical and physical access to CA systems and data is restricted to authorized individuals;
   - the continuity of key and certificate management operations is maintained; and
   - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.

KPMG

(Translation)

Certification authority's responsibilities
JPRS's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

Our independence and quality management
We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Management 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements, which requires the firm to design, implement and operate a system of quality management including policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities
Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

(1) obtaining an understanding of JPRS's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management business practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at JPRS and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

(Translation)

In our opinion, throughout the period June 7, 2024 to June 6, 2025, JPRS management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

This report does not include any representation as to the quality of JPRS's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline 2.8, nor the suitability of any of JPRS's services for any customer's intended purpose.

Use of the WebTrust seal
JPRS's use of the WebTrust for Certification Authorities – SSL Baseline Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

(The above represents a translation, for convenience only, of the original report issued in the Japanese language.)

(Translation)

APPENDIX A

List of CAs in Scope

OV SSL Issuing CAs
CA#1: JPRS Organization Validation Authority - G4
CA#2: JPRS OV RSA CA 2024 G1
CA#3: JPRS OV ECC CA 2024 G1
Other CAs
CA#4: JPRS Domain Validation Authority - G4
CA#5: JPRS DV RSA CA 2024 G1
CA#6: JPRS DV ECC CA 2024 G1

KPMG

(Translation)

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
1	1	CN = JPRS Organization Validation Authority - G4 O = Japan Registry Services Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B17E7B3B17E9FEE430280C2C2F59	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 22 10:23:28 2020 GMT	May 29 05:00:39 2029 GMT	D535AEC4D4326E8029152AD4001CB4ED23B92B38	801C522D3AD138E4F05D467EA369C1CC276078BF284018D0525EBBBC5342C836	2.23.140.1.2.2
2	1	CN = JPRS OV RSA CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911EF8E1B63325130A546BDC62E8	rsaEncryption	4096bit	sha384WithRSAEncryption	Apr 4 05:05:41 2024 GMT	Jan 12 00:00:00 2039 GMT	F5B655E3DBDC66D6A031C170DD22C7D1BDCAF25D	DAFA254E0173F0FD793A92ECFDF2C72C53EA5A761A73B7A3394C49182EA90933	2.23.140.1.2.2
3	1	CN = JPRS OV ECC CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA46F91F30C80CCC1CC1DCFDD294	id-ecPublicKey	384bit	ecdsa-with-SHA384	Apr 4 05:53:50 2024 GMT	Jun 16 00:00:00 2031 GMT	7E9E2AAE6A8D400A7BB211666055F1BFAF6CEC18	9C280369D072F89D9C9B62640BBF2F28D2F30ECEE9759854031D5C5C53E8D1B6	2.23.140.1.2.2
4	1	CN = JPRS Domain Validation Authority - G4 O = Japan Registry Services Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B17F05E48A55E6F5EF198802FFB9	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 22 10:40:53 2020 GMT	May 29 05:00:39 2029 GMT	7C24CE0DA4382DC7B3635EA7787A8D1D4C2EC715	F19D55CD08A3EA42BD91508073823174DD92370213C177F82531756DA7508A51	2.23.140.1.2.1

(Translation)

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
5	1	CN = JPRS DV RSA CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911DF50A9BCFBACCC94B6211D57F	rsaEncryption	4096bit	sha384WithRSAEncryption	Apr 4 04:50:03 2024 GMT	Jan 12 00:00:00 2039 GMT	A21DF57FCA6D049184686DB817EA184A9AA8CAFD	52361A6ABC835E7AD4B375F2165055303169DDE9FBEB4FAAF588ED532DDC2DCB	2.23.140.1.2.1
6	1	CN = JPRS DV ECC CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA4500ACA26353B09C3F0C6B6EBF	id-ecPublicKey	384bit	ecdsa-with-SHA384	Apr 4 05:30:34 2024 GMT	Jun 16 00:00:00 2031 GMT	587C1D2586486AEC293ABAEF5E4D7DABF44050BF	1B901D550A5A51F6737279C6021445F051BD293015612A5BAA3F8588829EE69A	2.23.140.1.2.1

(Translation)

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 CA#2 CA#3 CA#4 CA#5 CA#6	JPRS CA Certificate Policy	3.80	May 20, 2025
	JPRS CA Certificate Policy	3.74	March 27, 2025
	JPRS CA Certificate Policy	3.73	November 7, 2024
	JPRS CA Certificate Policy	3.72	August 26, 2024
	JPRS CA Certificate Policy	3.71	June 5, 2024

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 CA#2 CA#3 CA#4 CA#5 CA#6	JPRS CA Certification Practice Statement	1.54	May 20, 2025
	JPRS CA Certification Practice Statement	1.53	November 7, 2024
	JPRS CA Certification Practice Statement	1.52	August 26, 2024
	JPRS CA Certification Practice Statement	1.51	June 5, 2024

(Translation)

JPRS Management's Assertion

August 5, 2025

Koki Higashida
President
Japan Registry Services Co., Ltd.

Japan Registry Services Co., Ltd. ("JPRS") operates the Certification Authority (CA) services for its CAs as enumerated in Appendix A and provides SSL CA services.

The management of JPRS is responsible for establishing and maintaining effective controls over its SSL CA operations, including its SSL CA business practices disclosure on its website, SSL key lifecycle management controls, and SSL certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to JPRS's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

JPRS management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in JPRS management's opinion, in providing its SSL CA services at Tokyo, Japan, throughout the period June 7, 2024 to June 6, 2025, JPRS has:

1. disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statements and Certificate Polices enumerated in Appendix B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the JPRS website, and provided such services in accordance with its disclosed practices

2. maintained effective controls to provide reasonable assurance that:

- the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
- SSL subscriber information is properly authenticated (for the registration activities performed by JPRS)

3. maintained effective controls to provide reasonable assurance that:
   - logical and physical access to CA systems and data is restricted to authorized individuals;
   - the continuity of key and certificate management operations is maintained; and
   - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline v2.8.

(The above represents a translation, for convenience only, of the original assertion issued in the Japanese language.)

(Translation)

APPENDIX A

List of CAs in Scope

OV SSL Issuing CAs
CA#1: JPRS Organization Validation Authority - G4
CA#2: JPRS OV RSA CA 2024 G1
CA#3: JPRS OV ECC CA 2024 G1
Other CAs
CA#4: JPRS Domain Validation Authority - G4
CA#5: JPRS DV RSA CA 2024 G1
CA#6: JPRS DV ECC CA 2024 G1

(Translation)

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
1	1	CN = JPRS Organization Validation Authority - G4 O = Japan Registry Services Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B17E7B3B17E9FEE430280C2C2F59	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 22 10:23:28 2020 GMT	May 29 05:00:39 2029 GMT	D535AEC4D4326E8029152AD4001CB4ED23B92B38	801C522D3AD138E4F05D467EA369C1CC276078BF284018D0525EBBBC5342C836	2.23.140.1.2.2
2	1	CN = JPRS OV RSA CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911EF8E1B63325130A546BDC62E8	rsaEncryption	4096bit	sha384WithRSAEncryption	Apr 4 05:05:41 2024 GMT	Jan 12 00:00:00 2039 GMT	F5B655E3DBDC66D6A031C170DD22C7D1BDCAF25D	DAFA254E0173F0FD793A92ECFDF2C72C53EA5A761A73B7A3394C49182EA90933	2.23.140.1.2.2
3	1	CN = JPRS OV ECC CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA46F91F30C80CCC1CC1DCFDD294	id-ecPublicKey	384bit	ecdsa-with-SHA384	Apr 4 05:53:50 2024 GMT	Jun 16 00:00:00 2031 GMT	7E9E2AAE6A8D400A7BB211666055F1BFAF6CEC18	9C280369D072F89D9C9B62640BBF2F28D2F30ECEE9759854031D5C5C53E8D1B6	2.23.140.1.2.2
4	1	CN = JPRS Domain Validation Authority - G4 O = Japan Registry Services Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22B9B17F05E48A55E6F5EF198802FFB9	rsaEncryption	2048bit	sha256WithRSAEncryption	Jul 22 10:40:53 2020 GMT	May 29 05:00:39 2029 GMT	7C24CE0DA4382DC7B3635EA7787A8D1D4C2EC715	F19D55CD08A3EA42BD91508073823174DD92370213C177F82531756DA7508A51	2.23.140.1.2.1

(Translation)

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	SHA256 Fingerprint	Policy identifiers
5	1	CN = JPRS DV RSA CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = SECOM TLS RSA Root CA 2024 O = SECOM Trust Systems Co., Ltd. C = JP	47A5911DF50A9BCFBACCC94B6211D57F	rsaEncryption	4096bit	sha384WithRSAEncryption	Apr 4 04:50:03 2024 GMT	Jan 12 00:00:00 2039 GMT	A21DF57FCA6D049184686DB817EA184A9AA8CAFD	52361A6ABC835E7AD4B375F2165055303169DDE9FBEB4FAAF588ED532DDC2DCB	2.23.140.1.2.1
6	1	CN = JPRS DV ECC CA 2024 G1 O = Japan Registry Services Co., Ltd. C = JP	CN = Security Communication ECC RootCA1 O = SECOM Trust Systems CO.,LTD. C = JP	1DAFAA4500ACA26353B09C3F0C6B6EBF	id-ecPublicKey	384bit	ecdsa-with-SHA384	Apr 4 05:30:34 2024 GMT	Jun 16 00:00:00 2031 GMT	587C1D2586486AEC293ABAEF5E4D7DABF44050BF	1B901D550A5A51F6737279C6021445F051BD293015612A5BAA3F8588829EE69A	2.23.140.1.2.1

(Translation)

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 CA#2 CA#3 CA#4 CA#5 CA#6	JPRS CA Certificate Policy	3.80	May 20, 2025
	JPRS CA Certificate Policy	3.74	March 27, 2025
	JPRS CA Certificate Policy	3.73	November 7, 2024
	JPRS CA Certificate Policy	3.72	August 26, 2024
	JPRS CA Certificate Policy	3.71	June 5, 2024

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 CA#2 CA#3 CA#4 CA#5 CA#6	JPRS CA Certification Practice Statement	1.54	May 20, 2025
	JPRS CA Certification Practice Statement	1.53	November 7, 2024
	JPRS CA Certification Practice Statement	1.52	August 26, 2024
	JPRS CA Certification Practice Statement	1.51	June 5, 2024