



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
period of time

独立業務実施者の保証報告書

2024 年 10 月 31 日

サイバートラスト株式会社
PKI 事業本部
執行役員本部長
田村 光義 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-EV 保証規準 v1.8 \(the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8\)](#) に準拠して、2023 年 10 月 16 日から 2024 年 8 月 23 日までの期間において、[付録 A](#) に記載されたサイバートラスト株式会社の認証局（以下「CA」という。）のサービス（北海道及び東京）（以下「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、サイバートラスト株式会社は CA サービスについて、下記事項を実施していた。

- サイバートラスト株式会社は、CA ブラウザフォーラムガイドラインに準拠して Extended Validation SSL（以下「EV SSL」という。）証明書を提供するためのコミットメントを含む EV SSL 証明書ライフサイクル管理のビジネス実務を、サイバートラスト株式会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。
- サイバートラスト株式会社は、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 EV 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。
 - EV SSL 加入者情報は、（サイバートラスト株式会社が行う登録業務のため）適切に認証されていたこと。



認証局の責任

サイバートラスト株式会社の経営者の責任は、認証局のための [WebTrust-EV 保証規準 v1.8](#) 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。

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) サイバートラスト株式会社の EV 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 EV 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) サイバートラスト株式会社が開示した EV SSL 証明書ライフサイクル管理の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。

サイバートラスト株式会社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。

意見

当監査法人は、サイバートラスト株式会社の経営者の記述書が、認証局のための [WebTrust-EV 保証規準 v1.8](#) に基づいて、2023 年 10 月 16 日から 2024 年 8 月 23 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-EV 保証規準 v1.8](#) が対象としている範囲を超えて、サイバートラスト株式会社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サイバートラスト株式会社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

サイバートラスト株式会社の認証局のための WebTrust-EV 保証規準シールの使用は、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

Root CAs
CA#1: SecureSign Root CA15
CA#2: SecureSign Root CA14
CA#3: SecureSign Root CA12
EV SSL Issuing CAs
CA#4: Cybertrust Japan SureServer EV CA G9
CA#5: Cybertrust Japan SureServer EV CA G8
CA#6: Cybertrust Japan SureServer EV CA G7



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	署名アルゴリズム	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 = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D849A7BE690C8A88EDF070F9DDDB73E87	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年4月8日 17:32:56	2045年4月8日 17:32:56	EB41C8AEFCD59E5148F5BD8BF4872093412BD3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179E5314A9C291442805E1FB1D8FB6B8886C3A	—
2	1	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C204EE8D72977C85027A25A27DD2DF2CB	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年4月8日 16:06:19	2045年4月8日 16:06:19	0693A30A5E286937AA611DEBEBFC2D6F23E4F3A0	(SHA1) DD50C0F779B3642E74A2B89D9FD340DDBBF0F24F (SHA256) 4B009C1034494F9AB56BBA3BA1D62731FC4D20D8955ADCEC10A925607261E338	—
3	1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AFEC251B4ED5397E6E682C32B1C9016	rsaEncryption	2048Bits	sha256WithRSAEncryption	2020年4月8日 14:36:46	2040年4月8日 14:36:46	5734F374CF044BD525E6F140B62C4CD92DE9A0AD	(SHA1) 7A221E3DDE1B06AC9EC84770168E3CE5F76B06F4 (SHA256) 3F034BB5704D44B2D08545A02057DE93EBF3905FCE721ACBC730C06DDAEE904E	—
4	1	CN = Cybertrust Japan SureServer EV CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	756AA35ABA8847DD5103C33A37B168FA13A4F715	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年6月22日 17:50:22	2030年6月22日 17:50:22	EDB8FA2F3D7D25BEE354B165CE54A8833B92F0C7	(SHA1) EDEC2820E5CD08CB234D3B2417FE0DCDB51D238B (SHA256) 93397E182492A7E7C582BADFE04348E6FA985CBA19AFDE16FD740FF03857367C	2.23.140.1.1



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	署名アル 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 = Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	7CA3593373BD 43AA87416AB0 439DAC5D0361 D803	id- ecPublic Key	384Bits	ecdsa-with- SHA384	2020年6月22日 18:39:21	2030年6月22日 18:39:21	AEE4FDC16E22F8DFB7 1383F8E2D143B696B93 AC8	(SHA1) FBF4B414FBA71E4F10AA57CF8C4 7697489D59ED1 (SHA256) 70C4002E0DF2FF51E691654903BE7 42D09D5A74A84B15B68FBCDA320 FBF3DC6B	2.23.140.1.1
6	1	CN = Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	2C77F85B12969 E757EAC8921C 7155089AE35F4 18	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	2020年6月22日 16:34:38	2030年6月22日 16:34:38	7483319BF875CD0DCF8 E84E6D28E9AA6794C2 AA6	(SHA1) 99865D3428D04DEF0D3FA29DEFB D5905A0B040A7 (SHA256) 76648FBC40CC4164CEA02422A09E B4EAD29C67F5E7DD74F691B7FA0 8043472C5	2.23.140.1.1



付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 ～ CA#6	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.18	2023/8/24
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.19	2024/3/15
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.20	2024/4/15
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.21	2024/7/30
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.22	2024/8/20

運用規程

CA	CPS 名	Version	日付
CA#1 ～ CA#6	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.07	2023/8/24
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.08	2024/3/15
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.09	2024/4/15
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.10	2024/7/30
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.11	2024/8/20

以上

経営者の記述書

2024 年 10 月 31 日

サイバートラスト株式会社
PKI事業本部
執行役員本部長
田村 光義



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、Extended Validation SSL（以下「EV SSL」という。）CA サービスを提供している。

当社の経営者は、当社の Web サイトで公開している EV SSL CA ビジネス実務の開示、EV SSL 鍵のライフサイクル管理の内部統制、及び EV SSL 証明書ライフサイクル管理の内部統制を含む当社の EV 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 EV SSL CA サービス（北海道及び東京）に関す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、認証局のための [WebTrust-EV 保証規準 v1.8 \(the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.8\)](#) に準拠して、2023 年 10 月 16 日から 2024 年 8 月 23 日までの期間において、EV 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 EV SSL 証明書を提供するためのコミットメントを含む EV 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は[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 EV 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。
 - ・ EV 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。



付録 A

対象CA

Root CAs
CA#1: SecureSign Root CA15
CA#2: SecureSign Root CA14
CA#3: SecureSign Root CA12
EV SSL Issuing CAs
CA#4: Cybertrust Japan SureServer EV CA G9
CA#5: Cybertrust Japan SureServer EV CA G8
CA#6: Cybertrust Japan SureServer EV CA G7



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	署名アルゴリズム	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 = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D849A7BE690C8A88EDF070F9DDB73E87	id-ecPublic Key	384Bits	ecdsa-with-SHA384	2020年4月8日 17:32:56	2045年4月8日 17:32:56	EB41C8AEFCD59E5148F5BD8BF4872093412BD3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179E5314A9C291442805E1FB1D8FB6B8886C3A	—
2	1	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C204EE8D72977C85027A25A27DD2DF2CB	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年4月8日 16:06:19	2045年4月8日 16:06:19	0693A30A5E286937AA611DEBEBFC2D6F23E4F3A0	(SHA1) DD50C0F779B3642E74A2B89D9FD340DDBBF0F24F (SHA256) 4B009C1034494F9AB56BBA3BA1D62731FC4D20D8955ADCEC10A925607261E338	—
3	1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AFEC251B4ED5397E6E682C32B1C9016	rsaEncryption	2048Bits	sha256WithRSAEncryption	2020年4月8日 14:36:46	2040年4月8日 14:36:46	5734F374CF044BD525E6F140B62C4CD92DE9A0AD	(SHA1) 7A221E3DDE1B06AC9EC84770168E3CE5F76B06F4 (SHA256) 3F034BB5704D44B2D08545A02057DE93EBF3905FCE721ACBC730C06DDAEE904E	—
4	1	CN = Cybertrust Japan SureServer EV CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	756AA35ABA8847DD5103C33A37B168FA13A4F715	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年6月22日 17:50:22	2030年6月22日 17:50:22	EDB8FA2F3D7D25BEE354B165CE54A8833B92F0C7	(SHA1) EDEC2820E5CD08CB234D3B2417FE0DCDB51D238B (SHA256) 93397E182492A7E7C582BADFE04348E6FA985CBA19AFDE16FD740FF03857367C	2.23.140.1.1



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	署名アルゴリズム	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 = Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	7CA3593373BD43AA87416AB0439DAC5D0361D803	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日 18:39:21	2030年6月22日 18:39:21	AEE4FDC16E22F8DFB71383F8E2D143B696B93AC8	(SHA1) FBF4B414FBA71E4F10AA57CF8C47697489D59ED1 (SHA256) 70C4002E0DF2FF51E691654903BE742D09D5A74A84B15B68FBCDA320FBF3DC6B	2.23.140.1.1
6	1	CN = Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	2C77F85B12969E757EAC8921C7155089AE35F418	rsaEncryption	2048Bits	sha256WithRSAAEncryption	2020年6月22日 16:34:38	2030年6月22日 16:34:38	7483319BF875CD0DCF8E84E6D28E9AA6794C2AA6	(SHA1) 99865D3428D04DEF0D3FA29DEFB D5905A0B040A7 (SHA256) 76648FBC40CC4164CEA02422A09EB4EAD29C67F5E7DD74F691B7FA08043472C5	2.23.140.1.1



付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 ～ CA#6	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.18	2023/8/24
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.19	2024/3/15
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.20	2024/4/15
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.21	2024/7/30
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.22	2024/8/20

運用規程

CA	CPS 名	Version	日付
CA#1 ～ CA#6	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.07	2023/8/24
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.08	2024/3/15
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.09	2024/4/15
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.10	2024/7/30
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.11	2024/8/20

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
period of time

(Translation)

INDEPENDENT ASSURANCE REPORT

October 31, 2024

To Mr. Mitsuyoshi Tamura
Corporate Officer General Manager
PKI Business Unit
Cybertrust Japan 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 Cybertrust Co., Ltd. ("CTJ") that for its Certification Authority (CA) operations at Hokkaido and Tokyo, Japan, throughout the period October 16, 2023 to August 23, 2024 for its CAs as enumerated in [Appendix A](#), CTJ has:

1. disclosed its extended validation SSL ("EV SSL") certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the CTJ 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 EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by CTJ)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#).

Certification authority's responsibilities

CTJ'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 – Extended Validation SSL v1.8](#).



(Translation)

Our independence and quality control

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 CTJ's EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
- (2) selectively testing transactions executed in accordance with disclosed EV SSL certificate lifecycle management 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 CTJ 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.



(Translation)

Opinion

In our opinion, throughout the period October 16, 2023 to August 23, 2024, CTJ 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 – Extended Validation SSL v1.8](#).

This report does not include any representation as to the quality of CTJ's CA services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8](#), nor the suitability of any of CTJ's services for any customer's intended purpose.

Use of the WebTrust seal

CTJ's use of the WebTrust for Certification Authorities – Extended Validation SSL 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

Root CAs
CA#1: SecureSign Root CA15
CA#2: SecureSign Root CA14
CA#3: SecureSign Root CA12
EV SSL Issuing CAs
CA#4: Cybertrust Japan SureServer EV CA G9
CA#5: Cybertrust Japan SureServer EV CA G8
CA#6: Cybertrust Japan SureServer EV CA G7



(Translation)

CA Identifying Information for in Scope CAs

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
1	1	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D849 A7BE690C8A88 EDF070F9DDB 73E87	id- ecPublic Key	384Bits	ecdsa-with- SHA384	April 8, 2020 17:32:56	April 8, 2045 17:32:56	EB41C8AEFCD59E5148 F5BD8BF4872093412BD 3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7 EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179 E5314A9C291442805E1FB1D8FB6B 8886C3A	—
2	1	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C204E E8D72977C8502 7A25A27DD2D F2CB	rsaEncr yption	4096Bits	Sha384With RSAEncrypt ion	April 8, 2020 16:06:19	April 8, 2045 16:06:19	0693A30A5E286937AA6 11DEBEBFC2D6F23E4F 3A0	(SHA1) DD50C0F779B3642E74A2B89D9FD3 40DDBBF0F24F (SHA256) 4B009C1034494F9AB56BBA3BA1D 62731FC4D20D8955ADCEC10A9256 07261E338	—
3	1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AFEC C251B4ED5397 E6E682C32B1C 9016	rsaEncr yption	2048Bits	sha256With RSAEncrypt ion	April 8, 2020 14:36:46	April 8, 2040 14:36:46	5734F374CF044BD525E 6F140B62C4CD92DE9A 0AD	(SHA1) 7A221E3DDE1B06AC9EC84770168E 3CE5F76B06F4 (SHA256) 3F034BB5704D44B2D08545A02057 DE93EBF3905FCE721ACBC730C06 DDAEE904E	—
4	1	CN = Cybertrust Japan SureServer EV CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	756AA35ABA8 847DD5103C33 A37B168FA13A 4F715	rsaEncr yption	4096Bits	Sha384With RSAEncrypt ion	June 22, 2020 17:50:22	June 22, 2030 17:50:22	EDB8FA2F3D7D25BEE 354B165CE54A8833B92 F0C7	(SHA1) EDEC2820E5CD08CB234D3B2417F E0DCDB51D238B (SHA256) 93397E182492A7E7C582BADFE043 48E6FA985CBA19AFDE16FD740FF 03857367C	2.23.140.1.1



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
5	1	CN = Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	7CA3593373BD 43AA87416AB0 439DAC5D0361 D803	id- ecPublic Key	384Bits	ecdsa-with- SHA384	June 22, 2020 18:39:21	June 22, 2030 18:39:21	AEE4FDC16E22F8DFB7 1383F8E2D143B696B93 AC8	(SHA1) FBF4B414FBA71E4F10AA57CF8C4 7697489D59ED1 (SHA256) 70C4002E0DF2FF51E691654903BE7 42D09D5A74A84B15B68FBCDA320 FBF3DC6B	2.23.140.1.1
6	1	CN = Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	2C77F85B12969 E757EAC8921C 7155089AE35F4 18	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	June 22, 2020 16:34:38	June 22, 2030 16:34:38	7483319BF875CD0DCF8 E84E6D28E9AA6794C2 AA6	(SHA1) 99865D3428D04DEF0D3FA29DEFB D5905A0B040A7 (SHA256) 76648FBC40CC4164CEA02422A09E B4EAD29C67F5E7DD74F691B7FA0 8043472C5	2.23.140.1.1



(Translation)

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 — CA#6	Cybertrust Japan Certificate Policy	1.18	August 24, 2023
	Cybertrust Japan Certificate Policy	1.19	March 15, 2024
	Cybertrust Japan Certificate Policy	1.20	April 15, 2024
	Cybertrust Japan Certificate Policy	1.21	July 30, 2024
	Cybertrust Japan Certificate Policy	1.22	August 20, 2024

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 — CA#6	Cybertrust Japan Certification Practice Statement	1.07	August 24, 2023
	Cybertrust Japan Certification Practice Statement	1.08	March 15, 2024
	Cybertrust Japan Certification Practice Statement	1.09	April 15, 2024
	Cybertrust Japan Certification Practice Statement	1.10	July 30, 2024
	Cybertrust Japan Certification Practice Statement	1.11	August 20, 2024



(Translation)

CTJ MANAGEMENT'S ASSERTION

October 31, 2024

Mitsuyoshi Tamura
Corporate Officer General Manager
PKI Business Unit
Cybertrust Japan Co., Ltd.

Cybertrust Co., Ltd. ("CTJ") operates the Certification Authority (CA) services for its CAs as enumerated in [Appendix A](#) and provides Extended Validation SSL ("EV SSL") CA services.

The management of CTJ is responsible for establishing and maintaining effective controls over its EV SSL CA operations, including its EV SSL CA business practices disclosure on its website, EV SSL key lifecycle management controls, and EV 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 CTJ's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

CTJ management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in CTJ management's opinion, in providing its EV SSL CA services at Hokkaido and Tokyo, Japan, throughout the period October 16, 2023 to August 23, 2024, CTJ has:

1. disclosed its EV SSL certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Guidelines on the CTJ website, and provided such services in accordance with its disclosed practices



(Translation)

2. maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and EV SSL certificates it manages is established and protected throughout their lifecycles; and
 - EV SSL subscriber information is properly authenticated (for the registration activities performed by CTJ)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.8.](#)

(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

Root CAs
CA#1: SecureSign Root CA15
CA#2: SecureSign Root CA14
CA#3: SecureSign Root CA12
EV SSL Issuing CAs
CA#4: Cybertrust Japan SureServer EV CA G9
CA#5: Cybertrust Japan SureServer EV CA G8
CA#6: Cybertrust Japan SureServer EV CA G7



(Translation)

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Fingerprint	Policy identifiers
1	1	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D849A7BE690C8A88EDF070F9DDB73E87	id-ecPublicKey	384Bits	ecdsa-with-SHA384	April 8, 2020 17:32:56	April 8, 2045 17:32:56	EB41C8AEFCD59E5148F5BD8BF4872093412BD3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179E5314A9C291442805E1FB1D8FB6B8886C3A	—
2	1	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C204EE8D72977C85027A25A27DD2DF2CB	rsaEncryption	4096Bits	Sha384WithRSAEncryption	April 8, 2020 16:06:19	April 8, 2045 16:06:19	0693A30A5E286937AA611DEBEBFC2D6F23E4F3A0	(SHA1) DD50C0F779B3642E74A2B89D9FD340DDBBF0F24F (SHA256) 4B009C1034494F9AB56BBA3BA1D62731FC4D20D8955ADCEC10A925607261E338	—
3	1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AFEC251B4ED5397E6E682C32B1C9016	rsaEncryption	2048Bits	sha256WithRSAEncryption	April 8, 2020 14:36:46	April 8, 2040 14:36:46	5734F374CF044BD525E6F140B62C4CD92DE9A0AD	(SHA1) 7A221E3DDE1B06AC9EC84770168E3CE5F76B06F4 (SHA256) 3F034BB5704D44B2D08545A02057DE93EBF3905FCE721ACBC730C06DDAE904E	—
4	1	CN = Cybertrust Japan SureServer EV CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	756AA35ABA8847DD5103C33A37B168FA13A4F715	rsaEncryption	4096Bits	Sha384WithRSAEncryption	June 22, 2020 17:50:22	June 22, 2030 17:50:22	EDB8FA2F3D7D25BEE354B165CE54A8833B92F0C7	(SHA1) EDEC2820E5CD08CB234D3B2417FE0DCDB51D238B (SHA256) 93397E182492A7E7C582BADFE04348E6FA985CBA19AFDE16FD740FF03857367C	2.23.140.1.1



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
5	1	CN = Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	7CA3593373BD 43AA87416AB0 439DAC5D0361 D803	id- ecPublic Key	384Bits	ecdsa-with- SHA384	June 22, 2020 18:39:21	June 22, 2030 18:39:21	AEE4FDC16E22F8DFB7 1383F8E2D143B696B93 AC8	(SHA1) FBF4B414FBA71E4F10AA57CF8C4 7697489D59ED1 (SHA256) 70C4002E0DF2FF51E691654903BE7 42D09D5A74A84B15B68FBCDA320 FBF3DC6B	2.23.140.1.1
6	1	CN = Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	2C77F85B12969 E757EAC8921C 7155089AE35F4 18	rsaEncr yption	2048Bits	sha256With RSAEncrypt ion	June 22, 2020 16:34:38	June 22, 2030 16:34:38	7483319BF875CD0DCF8 E84E6D28E9AA6794C2 AA6	(SHA1) 99865D3428D04DEF0D3FA29DEFB D5905A0B040A7 (SHA256) 76648FBC40CC4164CEA02422A09E B4EAD29C67F5E7DD74F691B7FA0 8043472C5	2.23.140.1.1

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 — CA#6	Cybertrust Japan Certificate Policy	1.18	August 24, 2023
	Cybertrust Japan Certificate Policy	1.19	March 15, 2024
	Cybertrust Japan Certificate Policy	1.20	April 15, 2024
	Cybertrust Japan Certificate Policy	1.21	July 30, 2024
	Cybertrust Japan Certificate Policy	1.22	August 20, 2024

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 — CA#6	Cybertrust Japan Certification Practice Statement	1.07	August 24, 2023
	Cybertrust Japan Certification Practice Statement	1.08	March 15, 2024
	Cybertrust Japan Certification Practice Statement	1.09	April 15, 2024
	Cybertrust Japan Certification Practice Statement	1.10	July 30, 2024
	Cybertrust Japan Certification Practice Statement	1.11	August 20, 2024