

独立業務実施者の保証報告書

2021年12月8日

サイバートラスト株式会社
認証・セキュリティ事業部
PKI 技術本部
プロダクトマネジメント部
部長
坂本 勝 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

小松博明 

範囲

当監査法人は、[認証局のための WebTrust-EV 保証規準 v1.7.3 \(the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.7.3\)](#) に準拠して、2020年12月11日から2021年10月15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 証明書の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上で[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有効な内部統制を維

持していた。

- 管理する鍵及び 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 v1.7.3](#) 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、秘密保持、並びに職業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、国際品質管理基準の第 1 号を適用しており、従って、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して文書化した方針と手続を含む、包括的な品質管理システムを保持している。

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、EV SSL 加入者情報の認証に関する内部統制を理解すること、(2)サイバートラスト株式会社が開示した EV SSL 証明書の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)内部統制の運用状況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の経営者は、CA ブラウザフォーラムを構成するインターネットブラウザのオンラインフォーラムである Bugzilla のサイトで公開された情報を記載した[付録C](#)を当監査法人に開示した。当監査法人は、これらの情報を考慮して評価手続及び評価範囲を決定している。

内部統制の相対的有効性

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

内部統制の性質や固有の限界のため、先に述べた規準に適合するためのサイバートラスト株式会社の能力に影響を及ぼす可能性がある。例えば、内部統制により誤謬又は不正、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、修正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から将来を予測することは、変更が生ずることにより、その結論の妥当性を失うリスクがある。

意見

当監査法人は、[経営者の記述書](#)が、[認証局のための WebTrust-EV 保証規準 v1.7.3](#)に基づいて、2020年12月11日から2021年10月15日までの期間において、全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 v1.7.3](#)が対象としている範囲を越えて、サイバートラスト株式会社のCA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CA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 CA12
CA#2:	SecureSign Root CA14
CA#3:	SecureSign Root CA15
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 #	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
1	CN SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	=CN SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	=66F9C7C1AF ECC251B4ED 5397E6E682 C32B1C9016	rsaEncryption	(2048Bits)	sha256WithRSAEncryption	2020年4月8日 14:36:46	2040年4月8日 14:36:46	5734F374CF04 4BD525E6F140 362C4CD92DE9 A0AD	(SHA1) 7A221E3DDE1B06 AC9EC84770168E 3CE5F76B06F4 (SHA256) 3F034BB5704D44 B2D08545A02057 DE93EBF3905FCE 721ACBC730C06D DAEE904E
2	CN SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	=CN SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	=64DB5A0C20 4EE8D72977 C85027A25A 27DD2DF2CB	rsaEncryption	(4096Bits)	Sha384WithRSAEncryption	2020年4月8日 16:06:19	2045年4月8日 16:06:19	0693A30A5E28 6937AA611DEB EBFC2D6F23E4 F3A0	(SHA1) DD50C0F779B364 2E74A2B89D9FD3 40DDBBF0F24F (SHA256) 4B009C1034494F 9AB56BBA3BA1D6 2731FC4D20D895 5ADCEC10A92560 7261E338
3	CN SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	=CN SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	=1615C7C3D8 49A7BE690C 8A88EDF070 F9DDB73E87	id-ecPublicKey	(384Bits)	ecdsa-with-SHA384	2020年4月8日 17:32:56	2045年4月8日 17:32:56	EB41C8AEFC5 9E5148F5BD8B F4872093412B D3F4	(SHA1) CBBA83C8C15A5D F1F9736FCAD7EF 2813064A077D (SHA256) E778F0F095FE84 3729CD1A008217 9E5314A9C29144 2805E1FB1D8FB6 B8886C3A
4	CN Cybertrust Japan SureServer EVD CA G9 O = Cybertrust Japan Co., Ltd. C = JP	=CN SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	=756AA35ABA 8847DD5103 C33A37B168 FA13A4F715	rsaEncryption	(4096Bits)	Sha384WithRSAEncryption	2020年6月22日 17:50:22	2030年6月22日 17:50:22	EDB8FA2F3D7D 25BEE354B165 CE54A8833B92 F0C7	(SHA1) EDEC2820E5CD08 CB234D3B2417FE 0DCDB51D238B (SHA256) 93397E182492A7 E7C582BADFE043 48E6FA985CBA19 AFDE16FD740FF0 3857367C

5	CN Cybertrust Japan SureServer EVO CA G8 O = Cybertrust Japan Co., Ltd. Ltd. C = JP	=CN SecureSign Root CA15 Cybertrust Japan Co., Ltd. C = JP	=7CA3593373 BD43AA8741 5AB0439DAC 5D0361D803	id- ecPublicKey)	(384Bits	ecdsa- with- SHA384	2020年6月 22日 18:39:21	2030年6月 22日 18:39:21	AEE4FDC16E22 F8DFB71383F8 E2D143B696B9 3AC8	(SHA1) FBF4B414FBA71E 4F10AA57CF8C47 697489D59ED1 (SHA256) 70C4002E0DF2FF 51E691654903BE 742D09D5A74A84 B15B68FBCDA320 FBF3DC6B
6	CN Cybertrust Japan SureServer EVO CA G7 O = Cybertrust Japan Co., Ltd. Ltd. C = JP	=CN SecureSign Root CA12 Cybertrust Japan Co., Ltd. C = JP	=2C77F85B12 969E757EAC 8921C71550 89AE35F418	rsaEncryption n)	(2048Bit	sha256Wi thRSAEnc ryption	2020年6月 22日 16:34:38	2030年6月 22日 16:34:38	7483319BF875 CD0DCF8E84E6 D28E9AA6794C 2AA6	(SHA1) 99865D3428D04D EF0D3FA29DEFBD 5905A0B040A7 (SHA256) 76648FBC40CC41 64CEA02422A09E B4EAD29C67F5E7 DD74F691B7FA08 043472C5

付録B

対象の認証局運用規程及び証明書ポリシー

認証局運用規程

文書名	バージョン	改定日	備考
サイバートラストルート 認証局運用規程	1.07	2021年4月30日	
サイバートラストルート 認証局運用規程	1.08	2021年9月9日	2021年10月14日に「サイバートラスト認証局運用規程」に統合。

文書名	バージョン	改定日	備考
サイバートラスト 認証局運用規程	1.00	2021年10月14日	

証明書ポリシー

文書名	バージョン	改定日	備考
サイバートラストルート 認証局証明書ポリシー	1.07	2021年4月30日	
サイバートラストルート 認証局証明書ポリシー	1.08	2021年6月30日	
サイバートラストルート 認証局証明書ポリシー	1.09	2021年9月9日	
サイバートラスト 証明書ポリシー	1.10	2021年10月14日	2021年10月14日に証明書ポリシー名称を「サイバートラスト証明書ポリシー」に変更。

付録C

公開されている情報

#	開示内容	公開リンク
1	Cybertrust Japan: Root CRLs exceed maximum validity period by one second	https://bugzilla.mozilla.org/show_bug.cgi?id=1737242

以上

経営者の記述書

2021年12月8日

サイバートラスト株式会社
認証・セキュリティ事業部
PKI技術本部
プロダクトマネジメント部
部長



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、Extended Validation（以下「EV SSL」という。）認証局サービス（以下「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証明書の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。

内部統制には誤謬及び内部統制の迂回又は無視を含む固有の限界がある。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可能性がある。

当社の経営者は、EV SSL CAサービス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、2020年12月11日から2021年10月15日までの期間において、EV SSL CAサービス（北海道及び東京）の提供に関し、[認証局のためのWebTrust-EV保証規準v1.7.3 \(the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.7.3\)](#) に準拠して、以下の事項を実施した。

1. 当社は、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 証明書の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. 当社は、下記について合理的な保証を提供する有効な内部統制を維持していた。
 - 管理する鍵及び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。



当社は、CA ブラウザフォーラムを構成するインターネットブラウザのオンラインフォーラムである Bugzilla のサイトで公開されている情報を[付録 C](#)に記載している。



付録 A

対象 CA

Root CAs	
CA#1:	SecureSign Root CA12
CA#2:	SecureSign Root CA14
CA#3:	SecureSign Root CA15
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

対象の CA の識別情報

CA #	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
1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AF ECC251B4ED 5397E6E682 C32B1C9016	rsaEncryption	(2048Bits)	sha256WithRSAEncryption	2020年4月8日 14:36:46	2040年4月8日 14:36:46	5734F374CF04 4BD525E6F140 B62C4CD92DE9 A0AD	(SHA1) 7A221E3DDE1B06 AC9EC84770168E 3CE5F76B06F4 (SHA256) 3F034BB5704D44 B2D08545A02057 DE93EBF3905FCE 721ACBC730C06D DAEE904E
2	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C20 4EE8D72977 C85027A25A 27DD2DF2CB	rsaEncryption	(4096Bits)	Sha384WithRSAEncryption	2020年4月8日 16:06:19	2045年4月8日 16:06:19	0693A30A5E28 6937AA611DEB EBFC2D6F23E4 F3A0	(SHA1) DD50C0F779B364 2E74A2B89D9FD3 40DDBBF0F24F (SHA256) 4B009C1034494F 9AB56BBA3BA1D6 2731FC4D20D895 5ADCEC10A92560 7261E338
3	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D8 49A7BE690C 8A88EDF070 F9DDB73E87	id-ecPublicKey	(384Bits)	ecdsa-with-SHA384	2020年4月8日 17:32:56	2045年4月8日 17:32:56	EB41C8AEFCD5 9E5148F5BD8B F4872093412B D3F4	(SHA1) CBB83C8C15A5D F1F9736FCAD97EF 2813064A077D (SHA256) E778F0F095FE84 3729CD1A008217 9E5314A9C29144 2805E1FB1D8FB6 B8886C3A
4	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	756AA35ABA 8847DD5103 C33A37B168 FA13A4F715	rsaEncryption	(4096Bits)	Sha384WithRSAEncryption	2020年6月22日 17:50:22	2030年6月22日 17:50:22	EDB8FA2F3D7D 25BEE354B165 CE54A8833B92 FOC7	(SHA1) EDEC2820E5CD08 CB234D3B2417FE 0DCDB51D238B (SHA256) 93397E182492A7 E7C582BADFE043 48E6FA985CBA19 AFDE16FD740FF0 3857367C



5	CN Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	=CN SecureSign Root CA15 Cybertrust Japan Co., Ltd. C = JP	=7CA3593373 BD43AA8741 6AB0439DAC 5D0361D803	id- ecPublicKey	(384Bits	ecdsa- with- SHA384	2020年6月 22日 18:39:21	2030年6月 22日 18:39:21	AEE4FDC16E22 F8DFB71383F8 E2D143B696B9 3AC8	(SHA1) FBF4B414FBA71E 4F10AA57CF8C47 697489D59ED1 (SHA256) 70C4002E0DF2FF 51E691654903BE 742D09D5A74A84 B15B68FBCDA320 FBF3DC6B
6	CN Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	=CN SecureSign Root CA12 Cybertrust Japan Co., Ltd. C = JP	=2C77F85B12 969E757EAC 8921C71550 89AE35F418	rsaEncryption	(2048Bits	sha256With RSAEncryption	2020年6月 22日 16:34:38	2030年6月 22日 16:34:38	7483319BF875 CD0DCF8E84E6 D28E9AA6794C 2AA6	(SHA1) 99865D3428D04D EF0D3FA29DEFBD 5905A0B040A7 (SHA256) 76648FBC40CC41 64CEA02422A09E B4EAD29C67F5E7 DD74F691B7FA08 043472C5

付録B

対象の認証局運用規程及び証明書ポリシー

認証局運用規程

文書名	バージョン	改定日	備考
サイバートラストルート 認証局運用規程	1.07	2021年4月30日	
サイバートラストルート 認証局運用規程	1.08	2021年9月9日	2021年10月14日に「サイバートラスト認証局運用規程」に統合。

文書名	バージョン	改定日	備考
サイバートラスト 認証局運用規程	1.00	2021年10月14日	

証明書ポリシー

文書名	バージョン	改定日	備考
サイバートラストルート 認証局証明書ポリシー	1.07	2021年4月30日	
サイバートラストルート 認証局証明書ポリシー	1.08	2021年6月30日	
サイバートラストルート 認証局証明書ポリシー	1.09	2021年9月9日	
サイバートラスト 証明書ポリシー	1.10	2021年10月14日	2021年10月14日に証明書ポリシー名称を「サイバートラスト証明書ポリシー」に変更。



付録C

公開されている情報

#	開示内容	公開リンク
1	Cybertrust Japan: Root CRLs exceed maximum validity period by one second	https://bugzilla.mozilla.org/show_bug.cgi?id=1737242

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

December 8, 2021

To Mr. Masaru Sakamoto
Senior Manager
Product Management Department
PKI Technology Division
Certification & Security Business
Cybertrust Japan Co., Ltd.

KPMG AZSA LLC
Tokyo Office
Partner, Certified Public Accountant
Hiroaki Komatsu

Scope

We have been engaged, in a reasonable assurance engagement, to report on the [management's assertion](#) of Cybertrust Japan Co., Ltd. that for its Certification Authority (CA) operations at Hokkaido and Tokyo, Japan, throughout the period December 11, 2020 to October 15, 2021 for its CAs as enumerated in [Appendix A](#), Cybertrust Japan Co., Ltd. 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 Cybertrust Japan Co., Ltd.’s 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 Cybertrust Japan Co., Ltd.)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.7.3](#).

Certification Authority’s responsibilities

Cybertrust Japan Co., Ltd.’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 v1.7.3](#).

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 Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor’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 Cybertrust Japan Co., Ltd.’s EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates and its controls over the authenticity of subscriber information;



(Translation)

- (2) selectively testing transactions executed in accordance with disclosed EV 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.

Cybertrust Japan Co., Ltd.'s management has disclosed to us the information enumerated in [Appendix C](#), that have been posted publicly on Bugzilla's site which is the online forums of individual internet browsers that comprise the CA/Browser Forum. We have considered the nature of these information in determining the nature, timing and extent of our procedures.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at Cybertrust Japan Co., Ltd. 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

Because of the nature and inherent limitations of controls, Cybertrust Japan Co., Ltd.'s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, throughout the period December 11, 2020 to October 15, 2021, the [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 v1.7.3](#).



(Translation)

This report does not include any representation as to the quality of Cybertrust Japan Co., Ltd.'s services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.7.3](#), nor the suitability of any of Cybertrust Japan Co., Ltd.'s CA services for any customer's intended purpose.

Use of the WebTrust seal

Cybertrust Japan Co., Ltd.'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 CA12
CA#2:	SecureSign Root CA14
CA#3:	SecureSign Root CA15
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 #	Subject	Issuer	Serial	Key Algorithm	Key Size	Signature Algorithm	Not Before	Not After	SKI	Fingerprint
1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1 AFECC251 B4ED5397 E6E682C3 2B1C9016	RsaEncryption	(2048Bits)	sha256WithRSAEncryption	April 8, 2020 14:36:46	April 8, 2040 14:36:46	5734F374CF 044BD525E6 F140B62C4 CD92DE9A0 AD	(SHA1) 7A221E3DDE 1B06AC9EC84 770168E3CE5 F76B06F4 (SHA256) 3F034BB5704 D44B2D08545 A02057DE93E BF3905FCE72 1ACBC730C06 DDAEE904E
2	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C 204EE8D7 2977C8502 7A25A27D D2DF2CB	RsaEncryption	(4096Bits)	Sha384WithRSAEncryption	April 8, 2020 16:06:19	April 8, 2045 16:06:19	0693A30A5E 286937AA61 1DEBEBFC 2D6F23E4F 3A0	(SHA1) DD50C0F779E 3642E74A2B8 9D9FD340DD BBF0F24F (SHA256) 4B009C103449 4F9AB56BBA 3BA1D62731F C4D20D8955A DCEC10A9256 07261E338
3	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3 D849A7BE 690C8A88 EDF070F9 DDB73E87	id-ecPublicKey	(384Bits)	ecdsa-with-SHA384	April 8, 2020 17:32:56	April 8, 2045 17:32:56	EB41C8AEF CD59E5148 F5BD8BF48 72093412BD 3F4	(SHA1) CBBA83C8C1 5A5DF1F9736 FCAD7EF281 3064A077D (SHA256) E778F0F095F E843729CD1A 0082179E5314 A9C291442805 E1FB1D8FB6 B8886C3A



(Translation)

4	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	756AA35A BA8847DD 5103C33A 37B168FA 13A4F715	RsaEncryption (4096Bits)	Sha384 WithRSA Encryption	June 22, 2020 17:50:22	June 22, 2030 17:50:22	EDB8FA2F3 D7D25BEE3 54B165CE54 A8833B92F0 C7	(SHA1) EDEC2820E5 CD08CB234D 3B2417FE0DC DB51D238B (SHA256) 93397E182492 A7E7C582BA DFE04348E6F A985CBA19A FDE16FD740 FF03857367C
5	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	7CA35933 73BD43AA 87416AB0 439DAC5D 0361D803	id- ecPublicKey (384Bits)	ecdsa- with- SHA384	June 22, 2020 18:39:21	June 22, 2030 18:39:21	AEE4FDC16 E22F8DFB7 1383F8E2D1 43B696B93A C8	(SHA1) FBF4B414FB A71E4F10AA5 7CF8C476974 89D59ED1 (SHA256) 70C4002E0DF 2FF51E69165 4903BE742D0 9D5A74A84B1 5B68FBCDA3 20FBF3DC6B
6	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	2C77F85B 12969E757 EAC8921C 7155089A E35F418	RsaEncryption (2048Bits)	sha256W ithRSAE ncryption	June 22, 2020 16:34:38	June 22, 2030 16:34:38	7483319BF8 75CD0DCF8 E84E6D28E 9AA6794C2 AA6	(SHA1) 99865D3428D 04DEF0D3FA 29DEFBD5905 A0B040A7 (SHA256) 76648FBC40C C4164CEA024 22A09EB4EA D29C67F5E7D D74F691B7FA 08043472C5



(Translation)

APPENDIX B

Certification Practice Statements and Certificate Policies in Scope

Certification Practice Statements

Document Name	Version	Effective Date	Remarks
Cybertrust Japan Root CA Certification Practice Statement	1.07	April 30, 2021	
Cybertrust Japan Root CA Certification Practice Statement	1.08	September 9, 2021	Integrated into "Cybertrust Japan Certification Practice Statement" on October 14, 2021.

Document Name	Version	Effective Date	Remarks
Cybertrust Japan Certification Practice Statement	1.00	October 14, 2021	

Certificate Policies

Document Name	Version	Effective Date	Remarks
Cybertrust Japan Root CA Certificate Policy	1.07	April 30, 2021	
Cybertrust Japan Root CA Certificate Policy	1.08	June 30, 2021	
Cybertrust Japan Root CA Certificate Policy	1.09	September 9, 2021	
Cybertrust Japan Certificate Policy	1.10	October 14, 2021	Document name was changed to "Cybertrust Japan Certificate Policy" on October 14, 2021.



(Translation)

APPENDIX C

Publicly Disclosed Information

#	Disclosure	Publicly Disclosed Link
1	Cybertrust Japan: Root CRLs exceed maximum validity period by one second	https://bugzilla.mozilla.org/show_bug.cgi?id=1737242

Cybertrust Management's Assertion

December 8, 2021

Masaru Sakamoto
Senior Manager
Product Management Department
PKI Technology Division
Certification & Security Business
Cybertrust Japan Co., Ltd.

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

The management of Cybertrust 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 Cybertrust's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Cybertrust management has assessed its disclosures of its certificate practices and controls over its EV SSL CA service. Based on that assessment, in Cybertrust management's opinion, in providing its EV SSL CA services at Hokkaido and Tokyo, Japan, throughout the period December 11, 2020 to October 15, 2021, Cybertrust has:

1. disclosed its EV SSL certificate lifecycle management 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 Cybertrust's 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 Cybertrust)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.7.3](#).

Cybertrust has enumerated the information to [Appendix C](#), that have been posted publicly on Bugzilla's site which is the online forums of individual internet browsers that comprise the CA/Browser Forum.

(Translation)



(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 CA12
CA#2:	SecureSign Root CA14
CA#3:	SecureSign Root CA15
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



CA Identifying Information for in Scope CAs

CA #	Subject	Issuer	Serial	Key Algorithm	Key Size	Signature Algorithm	Not Before	Not After	SKI	Fingerprint
1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1A FECC251B4 ED5397E6E 682C32B1C 9016	rsaEncryption	(2048Bits)	sha256WithRSAEncryption	April 8, 2020 14:36:46	April 8, 2040 14:36:46	5734F374CF0 44BD525E6F1 40B62C4CD9 2DE9A0AD	(SHA1) 7A221E3DDE 1B06AC9EC84 770168E3CE5 F76B06F4 (SHA256) 3F034BB5704D 44B2D08545A0 2057DE93EBF3 905FCE721ACB C730C06DDAE E904E
2	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C 204EE8D72 977C85027 A25A27DD 2DF2CB	rsaEncryption	(4096Bits)	Sha384WithRSAEncryption	April 8, 2020 16:06:19	April 8, 2045 16:06:19	0693A30A5E2 86937AA611 DEBEBFC2D 6F23E4F3A0	(SHA1) DD50C0F779E 3642E74A2B8 9D9FD340DD BBF0F24F (SHA256) 4B009C103449 4F9AB56BBA 3BA1D62731F C4D20D8955A DCEC10A9256 07261E338
3	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D 849A7BE69 0C8A88ED F070F9DDE 73E87	id-ecPublicKey	(384Bits)	ecdsa-with-SHA384	April 8, 2020 17:32:56	April 8, 2045 17:32:56	EB41C8AEFC D59E5148F5B D8BF4872093 412BD3F4	(SHA1) CBBA83C8C1 5A5DF1F9736 FCAD7EF281 3064A077D (SHA256) E778F0F095F E843729CD1A 0082179E5314 A9C291442805 E1FB1D8FB6 B8886C3A
4	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	756AA35A BA8847DD 5103C33A3 7B168FA13 A4F715	rsaEncryption	(4096Bits)	Sha384WithRSAEncryption	June 22, 2020 17:50:22	June 22, 2030 17:50:22	EDB8FA2F3D 7D25BEE354 B165CE54A8 833B92F0C7	(SHA1) EDEC2820E5 CD08CB234D 3B2417FE0DC DB51D238B (SHA256) 93397E182492 A7E7C582BA DFE04348E6F A985CBA19A FDE16FD740 FF03857367C



5	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	7CA359337 3BD43AA8 7416AB043 9DAC5D03 61D803	id- ecPublicKey	(384Bits)	ecdsa- with- SHA384	June 22, 2020 18:39:21	June 22, 2030 18:39:21	AEE4FDC16E 22F8DFB7138 3F8E2D143B6 96B93AC8	(SHA1) FBBF4B414FB A71E4F10AA5 7CF8C476974 89D59ED1 (SHA256) 70C4002E0DF 2FF51E69165 4903BE742D0 9D5A74A84B1 5B68FBCDA3 20FBF3DC6B
6	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	2C77F85B1 2969E757E AC8921C71 55089AE35 F418	rsaEncryption	(2048Bits)	sha256With RSAEncryption	June 22, 2020 16:34:38	June 22, 2030 16:34:38	7483319BF87 5CD0DCF8E8 4E6D28E9AA 6794C2AA6	(SHA1) 99865D3428D 04DEF0D3FA 29DEFBD5905 A0B040A7 (SHA256) 76648FBC40C C4164CEA024 22A09EB4EA D29C67F5E7E D74F691B7FA 08043472C5



APPENDIX B

Certification Practice Statements and Certificate Policies in Scope

Certification Practice Statements

Document Name	Version	Effective Date	Remarks
Cybertrust Japan Root CA Certification Practice Statement	1.07	April 30, 2021	
Cybertrust Japan Root CA Certification Practice Statement	1.08	September 9, 2021	Integrated into "Cybertrust Japan Certification Practice Statement" on October 14, 2021.

Document Name	Version	Effective Date	Remarks
Cybertrust Japan Certification Practice Statement	1.00	October 14, 2021	

Certificate Policies

Document Name	Version	Effective Date	Remarks
Cybertrust Japan Root CA Certificate Policy	1.07	April 30, 2021	
Cybertrust Japan Root CA Certificate Policy	1.08	June 30, 2021	
Cybertrust Japan Root CA Certificate Policy	1.09	September 9, 2021	
Cybertrust Japan Certificate Policy	1.10	October 14, 2021	Document name was changed to "Cybertrust Japan Certificate Policy" on October 14, 2021.



APPENDIX C

Publicly Disclosed Information

#	Disclosure	Publicly Disclosed Link
1	Cybertrust Japan: Root CRLs exceed maximum validity period by one second	https://bugzilla.mozilla.org/show_bug.cgi?id=1737242