KPMG あずさ監査法人

有限責任 あずさ監査法人
東京都新宿区津久戸町 1 番 2 号
あずさセンタービル 〒162-8551

Telephone 03 3266 7500
Fax 03 3266 7600
Internet http://www.kpmg.com/jp/azsa
period of time

独立した監査法人の認証局のための WebTrust-EV 保証報告書

2020 年 2 月 14 日

サイバートラスト株式会社
技術統括
PKI 技術本部
プロダクトマネジメント部
坂本 勝 殿

有限責任 あずさ監査法人
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 v1.6.8（the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.8）に基づいて、2018 年 12 月 11 日から 2019 年 12 月 10 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 EV 認証局（以下「CA」という。）Cybertrust Japan EV CA G2（札幌）のサービス（以下「EV-CA サービス」という。）の提供について記載された「経営者の記述書」について検証を行った。 なお、当該 CA は、2019 年 9 月 30 日から 2019 年 12 月 10 日までの期間において、加入者証明書を発行しておらず、証明書の失効情報のみを提供していた。

経営者の記述書によれば、サイバートラスト株式会社は EV-CA サービスについて、下記事項を実施していた。

1. 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 EV 証明書を提供するためのコミットメントを含む EV 証明書のライフサイクル管理実務と手続を当社のウェブサイトで「Cybertrust Japan EV CA Certification Practice Statement（EVC 認証局運用規程）Version 4.2 （2019 年 6 月 24 日改訂）」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. 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。
   - EV 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）適切に収集、認証、検証されていたこと。
   - 管理する鍵と EV 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。

記述書に対する経営者の責任

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 v1.6.8 に基づいて、EV-CA サービスの提供が記述書に記載されたとおりにされていることの合理的保証を提供するための有効な内部統制を維持し、当該事実を記載した経営者の記述書を適正に作成することにある。

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結論を報告することにある。当監査法人の検証は、ＩＴ委員会実務指針第２号「Trust サービスに係る実務指針（中間報告）」に準拠して実施され、(1)サイバートラスト株式会社の EV-CA サービスの鍵と EV 証明書のライフサイクル管理のビジネス実務及び鍵と EV 証明書のインテグリティ、EV 加入者情報の認証に関する内部統制を理解し、(2) サイバートラスト株式会社が開示した鍵と EV 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し、(3)内部統制の運用状況の有効性をテスト、評価し、(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したことを含んでいる。

当監査法人は、検証の結果として結論を報告するための合理的な基礎を得たと判断している。

サイバートラスト株式会社の EV-CA 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、彼らの内部統制への相互作用、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 v1.6.8 に基づいて、2018 年 12 月 11 日から 2019 年 12 月 10 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。

強調事項

この保証報告書は、認証局のための WebTrust-EV 保証規準 v1.6.8 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 EV-CA サービスの品質についての何ら結論を報告するものではなく、又、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 EV-CA サービスの適合性についても何ら結論を報告するものではない。

サイバートラスト株式会社の Web サイト上の認証局のための 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。

利害関係

サイバートラスト株式会社と当監査法人又はパートナーとの間には、公認会計士法の規定に準じて記載すべき利害関係はない。

以上

経営者の記述書

2020 年 2 月 14 日

サイバートラスト株式会社
技術統括
PKI技術本部
プロダクトマネジメント部
坂本 勝

当社は、Extended Validation（以下「EV」という。）認証局（以下「CA」という。）（札幌）のサービス（以下「EV-CAサービス」という。）を付録Aに記載されたCAを通じて提供している。

当社の経営者は、当社の Web サイトで公開している EV-CA ビジネス実務の開示、及び鍵と EV 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-CA サービスの運用について、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。したがって、有効な内部統制といえども、当社の EV-CA サービス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、EV-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、2018年12月11日から2019年12月10日までの期間において、EV-CAサービスの提供に関して、認証局のためのWebTrust-EV保証規準v1.6.8（the WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL v1.6.8）に準拠して、下記の事項を実施した。なお、当該CAは、2019年9月30日から2019年12月10日までの期間において、加入者証明書を発行しておらず、証明書の失効情報のみを提供していた。

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 証明書を提供するためのコミットメントを含む EV 証明書のライフサイクル管理実務と手続を当社のウェブサイトで「Cybertrust Japan EV CA Certification Practice Statement（EVC 認証局運用規程）Version 4.2 （2019 年 6 月 24 日改訂）」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。
   - EV 加入者情報は、（当社が行う登録業務のため）適切に収集、認証、検証されていたこと。
   - 管理する鍵と EV 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。

付録 A

対象 CA

- Cybertrust Japan EV CA G2

対象の CA の情報

No	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	拇印アルゴリズム	有効期限の開始	有効期限の終了	サブジェクトキー識別	拇印
1	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Cybertrust Global Root O = Cybertrust, Inc	04 00 00 00 00 01 3a e5 37 ed 9e	rsaEncryption	2048bit	sha1, sha256	2012 年 11月9日 17:00:00	2019年12月 9 日 17:00:00	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) B5D17FE3 BDC03F80 B7A81FFC B63FCB58 32268ABD (SHA256) 8917FCCC 50424C56C 985BC0B35 2F53B0CC 9A8E4B776 3242EA988 C9D1CD05 27F0
2	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Cybertrust Global Root O = Cybertrust, Inc	04 00 00 00 00 01 43 72 03 34 9a	rsaEncryption	2048bit	sha1, sha256	2014年1月 8 日 17:00:00	2019年12月 10 日 17:00:00	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) 15C936AD CA01CA4C F31F0FC11 37FA60C11 0EBFD7 (SHA256) BD45B252 C72F3D6D 94A57BD6 F73154129 762880396 E74417AC F51257932 969C6
3	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Cybertrust Global Root O = Cybertrust, Inc	04 00 00 00 00 01 44 6e 19 52 e6	rsaEncryption	2048bit	sha1, sha256	2014年2月 26 日 17:00:00	2019年12月 10 日 17:00:00	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) 9902D1D15 C5A162881 2C2E23A38 4C2BB4E1 DA370 (SHA256) 87D9130F0 DB2627814 E486AF7F E1954C1FE 4E3CBFA1 93D0F66A

										A1157CC9 EE08C
4	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Cybertrust Global Root O = Cybertrust, Inc	0a a1 58 96 a4 d1 af 80 0d a1 69 0e f4 a3 af b4	rsaEncryption	2048bit	sha1, sha256	2017年7月 13日 21:19:28	2021年 12月 14 日 21:00:00	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) E3D9D219 C4ED5136 69F5EF3FA1 5A8DE127 8F2927 (SHA256) 400E5E852 4F3559879 8576312E7 5A545140A 4E4B7314C 1C8C53FD 7EC820E77 B5

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 http://www.kpmg.com/jp/azsa

period of time

(Translation)

WebTrust-EV for Certification Authorities
Independent Accountants' Report

February 14, 2020

To Mr. Masaru Sakamoto
Product Management Department
PKI Technology Division
Technology Unit
Cybertrust Japan Co., Ltd.

KPMG AZSA LLC
Partner
Certified Public Accountant
Hiroaki Komatsu

Scope of the examination
We have examined the assertion by the management of Cybertrust Japan Co., Ltd. (the "management's assertion") that in providing its Cybertust Extended Validation certification authority (CA), Cybertrust Japan EV CA G2, services at Sapporo, Japan (the "EV-CA service") during the period December 11, 2018 through December 10, 2019 for its CAs as enumerated in Appendix A, Cybertrust Japan Co., Ltd. has:

1. disclosed its EV certificate life cycle management practices and procedures in its Cybertrust Japan EV CA Certification Practice Statement Version 4.2, dated June 24, 2019 on Cybertrust Japan Co., Ltd.'s website, including its commitment to provide EV Certificates in conformity with the applicable CA/Browser Forum Guidelines, and provided such services in accordance with its disclosed practices
2. maintained effective controls to provide reasonable assurance that:
   - EV Subscriber information was properly collected, authenticated (for the registration activities performed by Cybertrust Japan Co., Ltd.) and verified; and
   - the integrity of keys and EV certificates it manages was established and protected throughout their life cycles

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8.

The CAs did not issue certificates during the period September 30, 2019 through December 10, 2019 and were maintained online to provide revocation status information only.

Management's responsibility
Cybertrust Japan Co., Ltd.'s management is responsible for its assertion, including the fairness of its presentation, and maintaining effective controls to provide reasonable assurance of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8.

Independent Accountants' responsibility
Our responsibility is to express an opinion on management's assertion based on our examination. Our examination was conducted in accordance with IT Committee Practice

Guidelines No.2 established by the Japanese Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Cybertrust Japan Co., Ltd.'s key and EV certificate lifecycle management business practices and its controls over key and EV certificate integrity, over the authenticity of subscriber information; (2) selectively testing transactions executed in accordance with disclosed key and EV certificate life cycle 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 our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at Cybertrust Japan Co., Ltd.'s EV-CA service 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.

Limitations in controls
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, for the period December 11, 2018 through December 10, 2019, the management's assertion is fairly stated, in all material respects, based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8.

Emphasis
This report does not include any representation as to the quality of Cybertrust Japan Co., Ltd.'s certification services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8, nor the suitability of any of Cybertrust Japan Co., Ltd.'s services for any customer's intended purpose.

Cybertrust Japan Co., Ltd.'s use of the WebTrust for Certification Authorities – Extended Validation SSL Seal on Cybertrust Japan Co., Ltd.'s website 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.

Other matter
KPMG AZSA LLC and engagement partners have no interest in Cybertrust Japan Co., Ltd., which should be disclosed pursuant to the provisions of the Certified Public Accountants Law of Japan.

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

(Translation)

Assertion by Management
as to its Disclosure of its Business Practices and its Controls
Over its Extended Validation Certification Authority Operations
during the period from December 11, 2018 through December 10, 2019

February 14, 2020

Masaru Sakamoto
Product Management Department
PKI Technology Division
Technology Unit
Cybertrust Japan Co., Ltd.

Cybertrust Japan Co., Ltd. ("Cybertrust") operates its Extended Validation ("EV") certification authority (CA) services (Sapporo, Japan) services (the "EV-CA services") through its CAs as enumerated in Appendix A.

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

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to Cybertrust's EV-CA services operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of Cybertrust has assessed the disclosure of its certificate practices and its controls over its EV- CA service. Based on that assessment, in Cybertrust Management's opinion, in providing its EV-CA services at Sapporo, Japan during the period December 11, 2018 through December 10, 2019, Cybertrust has:

1. disclosed its EV certificate life cycle management practices and procedures in its Cybertrust Japan EV CA Certification Practice Statement Version 4.2, dated June 24, 2019 on Cybertrust's website, including its commitment to provide EV Certificates in conformity with the CA/Browser Forum Guidelines, and provided such services in accordance with its disclosed practices;
2. maintained effective controls to provide reasonable assurance that:
   - EV Subscriber information was properly collected, authenticated (for the registration activities performed by Cybertrust) and verified; and
   - the integrity of keys and EV certificates it manages was established and protected throughout their life cycles

based on the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6.8.

The CAs as enumerated in Appendix A did not issue certificates during the period September 30, 2019 through December 10, 2019 and were maintained online to provide revocation status information only.

(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

- Cybertrust Japan EV CA G2

CA Identifying Information for in Scope CAs

No	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Fingerprint
1	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Cybertrust Global Root O = Cybertrust, Inc	04 00 00 00 00 01 3a e5 37 ed 9e	rsaEncryption	2048bit	sha1, sha256	November 9, 2012 17:00:00	December 9, 2019 17:00:00	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) B5D17FE3BDC03F80B7A81FFCB63FCB5832268ABD (SHA256) 8917FCCC50424C56C985BC0B352F53B0CC9A8E4B7763242EA988C9D1CD0527F0
2	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Cybertrust Global Root O = Cybertrust, Inc	04 00 00 00 00 01 43 72 03 34 9a	rsaEncryption	2048bit	sha1, sha256	January 8, 2014 17:00:00	December 10, 2019 17:00:00	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) 15C936ADCA01CA4CF31F0FC1137FA60C110EBFD7 (SHA256) BD45B252C72F3D6D94A57BD6F73154129762880396E74417ACF51257932969C6
3	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Cybertrust Global Root O = Cybertrust, Inc	04 00 00 00 00 01 44 6e 19 52 e6	rsaEncryption	2048bit	sha1, sha256	February 26, 2014 17:00:00	December 10, 2019 17:00:00	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) 9902D1D15C5A1628812C2E23A384C2BB4E1DA370 (SHA256) 87D9130F0DB2627814E486AF7FE1954C1FE4E3CBFA193D0F66AA1157CC9EE08C
4	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd.	CN = Cybertrust Global Root O = Cybertrust, Inc	0a a1 58 96 a4 d1 af 80 0d a1 69 0e f4 a3 af b4	rsaEncryption	2048bit	sha1, sha256	July 13, 2017 21:19:28	December 14, 2021 21:00:00	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b	(SHA1) E3D9D219C4ED513669F5EF3FA15A8DE1278F2927 (SHA256)

	C = JP								8d 5f	400E5E85 24F35598 798576312 E75A5451 40A4E4B7 314C1C8C 53FD7EC 820E77B5