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 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

当監査法人は、認証局のための WebTrust の規準 v2.2（the WebTrust Principles and Criteria for Certification Authorities v2.2）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認証局（以下「CA」という。）Cybertrust Japan Public CA G3（札幌）のサービス（以下「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 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が実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及びCA環境の内部統制の実務をサイバートラスト株式会社のウェブサイトで「Cybertrust Japan Public CA Certification Practice Statement（認証局運用規程）Version 8.9（2019年6月24日改訂）」にて開示していた。
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。
   - サイバートラスト株式会社の「Cybertrust Japan Public CA Certification Practice Statement（認証局運用規程）Version 8.9（2019年6月24日改訂）」に準拠してサービスを提供していたこと。
3. 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。
   - サイバートラスト株式会社が管理する鍵と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。

- サイバートラスト株式会社が管理する加入者鍵と加入者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。
- 加入者の情報は、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。
- 下位CAの証明書申請は、正確で、認証され、承認されていたこと。

4. 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。

- 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システムの開発、保守及び運用が適切に承認され、実施されていたこと。

サイバートラスト株式会社は、CAの鍵を寄託せず、加入者鍵の生成及び証明書の一時停止サービスを提供しない。従って、当監査法人の手続は、それらの規準に関連する内部統制を含んでいない。

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 の規準 v2.2 に基づいて、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鍵と証明書のライフサイクル管理のビジネス実務及び鍵と証明書のインテグリティ、加入者と信頼者情報の認証と個人情報保護、鍵と証明書のライフサイクル管理に係る運用の継続性、システムインテグリティの開発、保守、及び運用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 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 の規準 v2.2 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 の規準 v2.2 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 CA サービスの品質について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 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 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、付録Aに記載された認証局（以下「CA」という。）を通じて、次の認証局（札幌）のサービス（以下「CAサービス」という。）を提供している。

- 加入者の登録
- 証明書の更新
- 証明書の再生成
- 証明書の発行
- 証明書の配送
- 証明書の失効
- 証明書の審査

当社の経営者は、当社のWebサイトで公開している「Cybertrust Japan Public CA Certification Practice Statement（認証局運用規程）Version 8.9（2019年6月24日改訂）」におけるCAビジネス実務の開示、サービスのインテグリティ（鍵と証明書のライフサイクル管理を含む。）及びCA環境の内部統制を含む当社の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。したがって、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CAの運用に関する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の規準v2.2（the WebTrust Principles and Criteria for Certification Authorities v2.2）に準拠して、2018年12月11日から2019年12月10日までの期間において、CAサービスの提供に関して、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. 当社のCAが実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及びCA環境の内部統制の実務を当社のWebサイトにおける「Cybertrust Japan Public CA Certification Practice Statement（認証局運用規程）Version 8.9（2019年6月24日改訂）」にて開示していた。

2. 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。
   - 当社は、「Cybertrust Japan Public CA Certification Practice Statement（認証局運用規程）Version 8.9（2019年6月24日改訂）」に準拠してサービスを提供していたこと。
3. 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。
   - 当社が管理する鍵と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。
   - 当社が管理する加入者鍵と加入者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。
   - 加入者の情報は、当社が行う登録業務のため、適切に認証されていたこと。
   - 下位CAの証明書申請は、正確で、認証され、承認されていたこと。
4. 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。
   - 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システムの開発、保守及び運用が適切に承認され、実施されていたこと。

当社が準拠した認証局のための WebTrust の規準 v2.2 には、以下が含まれる。

CAビジネス実務の開示

CAのビジネス実務管理

- 認証局運用規程（CPS）の管理

サービスのインテグリティ

CA鍵ライフサイクル管理の内部統制

- CA鍵の生成
- CA鍵のストレージ、バックアップと復旧
- CA公開鍵の配送
- CA鍵の使用法
- CA鍵の保存及び破壊
- CA鍵の危殆化
- CAの暗号化ハードウェアライフサイクルの管理

下位CAの証明書ライフサイクル管理の内部統制

- 下位CA証明書ライフサイクル管理

証明書ライフサイクル管理の内部統制

- 加入者の登録
- 証明書の更新
- 証明書の再生成
- 証明書の発行
- 証明書の配送
- 証明書の失効
- 証明書の審査

CA環境の内部統制

- セキュリティ管理
- 資産の分類と管理
- 人員のセキュリティ
- 物理的・環境的セキュリティ
- 運用管理
- システムアクセス管理
- システム開発と保守
- ビジネス継続性の管理
- モニタリングと遵守
- 監査ログの取得

当社は、CAの鍵を寄託せず、加入者鍵の生成及び証明書の一時停止サービスを提供しない。従って、当社の記述書には、それらの規準に関連する内部統制を含んでいない。

付録 A

対象 CA

- Cybertrust Japan Public CA G3

対象 CA の情報

- Cybertrust Japan Public CA G3

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 Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 87 28	rsaEncryption	2048bit	sha1, sha256	2013年5月 9日 1:04:33	2020年6月 9日 1:03:31	73 a8 08 53 29 B8 15 fb 99 80 e5 c5 37 d8 f8 39 7B a4 13 06	(SHA1) 17FF892373 5A98082365 50488F96C5 3098212543 (SHA256) 5EDD31887 B72455B409 4005273ED7 508B7175E9 2DEF395BD 1F7ADB210 079DF21
2	CN = Cybertrust Japan Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 9c a5	rsaEncryption	2048bit	sha1, sha256	2014年1月 23日 3:45:54	2020年6月 10日 2:44:46	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) 7E41DF13E 9A50BFA148 D0C9482BB 424B73D7B6 DF (SHA256) C39C3F6190 57DD59903C 62F8BC1C86 8C668E0F45 1A79A55230 A248BE16B E10FF
3	CN = Cybertrust Japan Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 a2 76	rsaEncryption	2048bit	sha1, sha256	2014年2月 28日 3:09:27	2020年6月 10日 2:07:29	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) 421176A7C4 E864A7C879 5977ED0379 FAE0F7495C (SHA256) CFB93C1B3 98F5884E69 8DCEB02FC 4300FBFFF3

										824A03B43A89D7AE56CC401204
4	CN = Cybertrust Japan Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	05 43 40 d0 a2 c4 cc 81 11 fa a8 37 7d 46 e0 6f	rsaEncryption	2048bit	sha1, sha256	2016 年 11 月 15 日 21:03:31	2025年5月 10 日 21:00:00	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) C05265396B57CA49CCB2B03C9C59CD76BC5D9157 (SHA256) EB57F205113A581147E0F1D97328274FB030EC69EEC89CA297DCF55A3FB4463C

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 for Certification Authorities

Independent Accountant's 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 certification authority (CA), Cybertrust Japan Public CA G3, services at Sapporo, Japan (the "CA services") 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 Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Cybertrust Japan Public CA Certification Practice Statement Version 8.9, dated June 24, 2019 on Cybertrust Japan Co., Ltd.'s website;
2. maintained effective controls to provide reasonable assurance that:
   - Cybertrust Japan Co., Ltd. provided its services in accordance with its Cybertrust Japan Public CA Certification Practice Statement Version 8.9, dated June 24, 2019;
3. maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
   - the integrity of subscriber keys and certificates it manages was established and protected

(Translation)

throughout their life cycles;
- the Subscriber information was properly authenticated (for the registration activities performed by Cybertrust Japan Co., Ltd.); and
- subordinate CA certificate requests were accurate, authenticated, and approved;

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

based on the WebTrust Principles and Criteria for Certification Authorities v2.2.

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.

Cybertrust Japan Co., Ltd. does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

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 v2.2.

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 certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity

(Translation)

of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and 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 CA services 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, during 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 v2.2.

Emphasis

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 v2.2, 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 Seal on Cybertrust

(Translation)

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 Certification Authority Operations During the Period 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") provides the following certification authority (CA) services (the "CA services") through its CAs as enumerated in Appendix A:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate Validation

The management of Cybertrust is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in its Cybertrust Japan Public CA Certification Practice Statement Version 8.9, dated June 24, 2019 on Cybertrust's website, service integrity (including key and certificate life cycle management controls), and CA environmental 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 internal control can provide only reasonable assurance with respect to Cybertrust's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

The management of Cybertrust has assessed the controls over its CA operations. Based on that

(Translation)

assessment, in Cybertrust's Management's opinion, in providing the CA services at Sapporo, Japan, during the period December 11, 2018 through December 10, 2019, Cybertrust has:

1. disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Cybertrust Japan Public CA Certification Practice Statement Version 8.9, dated June 24, 2019 on Cybertrust's website;
2. maintained effective controls to provide reasonable assurance that:
   - Cybertrust provided its services in accordance with its Cybertrust Japan Public CA Certification Practice Statement Version 8.9, dated June 24, 2019;
3. maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
   - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
   - the Subscriber information was properly authenticated (for the registration activities performed by Cybertrust); and
   - subordinate CA certificate requests were accurate, authenticated, and approved;
4. maintained effective controls to provide reasonable assurance that:
   - logical and physical access to CA systems and data was restricted to authorized individuals;
   - the continuity of key and certificate management operations was maintained; and
   - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities v2.2 including the following:

CA Business Practices Disclosure

CA Business Practices Management

- Certification Practice Statement Management

Service Integrity

CA Key Life Cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution

- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

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.

Cybertrust does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion did not extend to controls that would address those criteria.

(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

- Cybertrust Japan Public CA G3

CA Identifying Information for in Scope CAs

- Cybertrust Japan Public CA G3

No	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Fingerprint
1	CN = Cybertrust Japan Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 87 28	rsaEncryption	2048bit	sha1, sha256	May 9, 2013 1:04:33	June 9, 2020 1:03:31	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) 17FF8923735A9808236550488F96C53098212543 (SHA256) 5EDD31887B72455B4094005273ED7508B7175E92DEF395BD1F7ADB210079DF21
2	CN = Cybertrust Japan Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 9c a5	rsaEncryption	2048bit	sha1, sha256	January 23, 2014 3:45:54	June 10, 2020 2:44:46	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) 7E41DF13E9A50BFA148D0C9482BB424B73D7B6DF (SHA256) C39C3F619057DD59903C62F8BC1C868C668E0F451A79A55230A248BE16BE10FF
3	CN = Cybertrust Japan Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 a2 76	rsaEncryption	2048bit	sha1, sha256	February 28, 2014 3:09:27	June 10, 2020 2:07:29	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) 421176A7C4E864A7C8795977ED0379FAE0F7495C (SHA256) CFB93C1B398F5884E698DCEB02FC4300FBFFF3824A03B43A89D7AE56CC401204
4	CN = Cybertrust Japan Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	05 43 40 d0 a2 c4 cc 81 11 fa a8 37 7d 46 e0 6f	rsaEncryption	2048bit	sha1, sha256	November 15, 2016 21:03:31	May 10, 2025 21:00:00	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) C05265396B57CA49CCB2B03C9C59CD76BC5D9157 (SHA256) EB57F205113A581147E0F1D97328274FB030EC69EEC89CA297DCF55A3FB4463C

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 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 の規準 v2.2（the WebTrust Principles and Criteria for Certification Authorities v2.2）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認証局（以下「CA」という。）Cybertrust Japan EV CA G2（札幌）のサービス（以下「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 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が実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及びCA環境の内部統制の実務をサイバートラスト株式会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。
   - サイバートラスト株式会社の「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）」に準拠してサービスを提供していたこと。
3. 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。
   - サイバートラスト株式会社が管理する鍵と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。

- サイバートラスト株式会社が管理する加入者鍵と加入者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。
- 加入者の情報は、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。
- 下位CAの証明書申請は、正確で、認証され、承認されていたこと。

4. 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。
   - 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システムの開発、保守及び運用が適切に承認され、実施されていたこと。

サイバートラスト株式会社は、CAの鍵を寄託せず、加入者鍵の生成及び証明書の一時停止サービスを提供しない。従って、当監査法人の手続は、それらの規準に関連する内部統制を含んでいない。

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 の規準 v2.2 に基づいて、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鍵と証明書のライフサイクル管理のビジネス実務及び鍵と証明書のインテグリティ、加入者と信頼者情報の認証と個人情報保護、鍵と証明書のライフサイクル管理に係る運用の継続性、システムインテグリティの開発、保守、及び運用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 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 の規準 v2.2 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 の規準 v2.2 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 CA サービスの品質について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 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 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、付録Aに記載された認証局（以下「CA」という。）を通じて、次の認証局（札幌）のサービス（以下「CAサービス」という。）を提供している。

- 加入者の登録
- 証明書の更新
- 証明書の再生成
- 証明書の発行
- 証明書の配送
- 証明書の失効
- 証明書の審査

当社の経営者は、当社のWebサイトで公開している「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）」におけるCAビジネス実務の開示、サービスのインテグリティ（鍵と証明書のライフサイクル管理を含む。）及びCA環境の内部統制を含む当社の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。したがって、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CAの運用に関する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の規準v2.2（the WebTrust Principles and Criteria for Certification Authorities v2.2）に準拠して、2018年12月11日から2019年12月10日までの期間において、CAサービスの提供に関して、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. 当社のCAが実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及びCA環境の内部統制の実務を、当社のWebサイトにおける「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）」にて開示していた。

2. 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。
   - 当社は、「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）」に準拠してサービスを提供していたこと。
3. 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。
   - 当社が管理する鍵と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。
   - 当社が管理する加入者鍵と加入者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。
   - 加入者の情報は、当社が行う登録業務のため、適切に認証されていたこと。
   - 下位CAの証明書申請は、正確で、認証され、承認されていたこと。
4. 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。
   - 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システムの開発、保守及び運用が適切に承認され、実施されていたこと。

当社が準拠した認証局のための WebTrust の規準 v2.2 には、以下が含まれる。

CAビジネス実務の開示

CAのビジネス実務管理

- 認証局運用規程（CPS）の管理

サービスのインテグリティ

CA鍵ライフサイクル管理の内部統制

- CA鍵の生成
- CA鍵のストレージ、バックアップと復旧
- CA公開鍵の配送
- CA鍵の使用法
- CA鍵の保存及び破壊
- CA鍵の危殆化
- CAの暗号化ハードウェアライフサイクルの管理

下位CAの証明書ライフサイクル管理の内部統制

- 下位CA証明書ライフサイクル管理

証明書ライフサイクル管理の内部統制

- 加入者の登録
- 証明書の更新
- 証明書の再生成
- 証明書の発行
- 証明書の配送
- 証明書の失効
- 証明書の審査

CA環境の内部統制

- セキュリティ管理
- 資産の分類と管理
- 人員のセキュリティ
- 物理的・環境的セキュリティ
- 運用管理
- システムアクセス管理
- システム開発と保守
- ビジネス継続性の管理
- モニタリングと遵守
- 監査ログの取得

当社は、CAの鍵を寄託せず、加入者鍵の生成及び証明書の一時停止サービスを提供しない。従って、当社の記述書には、それらの規準に関連する内部統制を含んでいない。

付録 A

対象 CA

- Cybertrust Japan EV CA G2

対象 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) 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	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) 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	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) 9902D1D15C5A1628812C2E23A384C2BB4E1DA370 (SHA256) 87D9130F0DB2627814E486AF7FE1954C1FE4E3CBFA193D0F66AA1157CC9EE08C

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) E3D9D219C4ED513669F5EF3FA15A8DE1278F2927 (SHA256) 400E5E8524F35598798576312E75A545140A4E4B7314C1C8C53FD7EC820E77B5

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 for Certification Authorities

Independent Accountant's 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 certification authority (CA), Cybertrust Japan EV CA G2, services at Sapporo, Japan (the "CA services") 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 Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Cybertrust Japan EV CA Certification Practice Statement Version 4.2, dated June 24, 2019, on Cybertrust Japan Co., Ltd.'s website;
2. maintained effective controls to provide reasonable assurance that:
   - Cybertrust Japan Co., Ltd. provided its services in accordance with its Cybertrust Japan EV CA Certification Practice Statement Version 4.2, dated June 24, 2019;
3. maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
   - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;

(Translation)

- the Subscriber information was properly authenticated (for the registration activities performed by Cybertrust Japan Co., Ltd.); and
- subordinate CA certificate requests were accurate, authenticated, and approved;

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

based on the WebTrust Principles and Criteria for Certification Authorities v2.2.

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.

Cybertrust Japan Co., Ltd. does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

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 v2.2.

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 certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over the development, maintenance,

(Translation)

and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and 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 CA services 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, during 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 v2.2.

Emphasis

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 v2.2, 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 Seal on Cybertrust Japan Co., Ltd.'s website constitutes a symbolic representation of the contents of this report and

(Translation)

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 Certification Authority Operations During the Period 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”) provides the following certification authority (CA) services (the “CA services”) through its CAs as enumerated in Appendix A:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate Validation

The management of Cybertrust is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in its Cybertrust Japan EV CA Certification Practice Statement Version 4.2, dated June 24, 2019 on Cybertrust’s website, service integrity (including key and certificate life cycle management controls), and CA environmental 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 internal control can provide only reasonable assurance with respect to Cybertrust's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

(Translation)

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

1. disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Cybertrust Japan EV CA Certification Practice Statement Version 4.2, dated June 24, 2019 on Cybertrust's website
2. maintained effective controls to provide reasonable assurance that:
   - Cybertrust provided its services in accordance with its Cybertrust Japan EV CA Certification Practice Statement Version 4.2, dated June 24, 2019
3. maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
   - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
   - the Subscriber information was properly authenticated (for the registration activities performed by Cybertrust); and
   - subordinate CA certificate requests were accurate, authenticated, and approved
4. maintained effective controls to provide reasonable assurance that:
   - logical and physical access to CA systems and data was restricted to authorized individuals;
   - the continuity of key and certificate management operations was maintained; and
   - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities v2.2 including the following:

CA Business Practices Disclosure

CA Business Practices Management

- Certification Practice Statement Management

Service Integrity

CA Key Life Cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery

- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Validation

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

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.

Cybertrust does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our assertion did not extend

to controls that would address those criteria.

(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) 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	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) 15C936AD CA01CA4C F31F0FC11 37FA60C11 0EBFD7 (SHA256) BD45B252 C72F3D6D 94A57BD6 F7315412 9762880396 E74417AC F5125793 2969C6
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) 9902D1D15 C5A16288 12C2E23A38 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	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 8d 5f	(SHA1) E3D9D219 C4ED51366 9F5EF3FA1 5A8DE127 8F2927 (SHA256) 400E5E852 4F3559879 8576312E7

(Translation)

										5A545140A 4E4B7314C 1C8C53FD 7EC820E77 B5