

## 独立した監査法人の認証局のための WebTrust 保証報告書

平成 30 年 2 月 13 日

サイバートラスト株式会社  
認証・セキュリティ事業部  
技術統括部 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  
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 v2.0 \(the WebTrust Principles and Criteria for Certification Authorities v2.0\)](#) に基づいて、平成 28 年 12 月 11 日から平成 29 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 G2 及び Cybertrust Japan Public CA G3（札幌）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。

[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「[Certification Practice Statement \(認証局運用規程\) Version 8.2 \(平成29年10月19日改定\)](#)」にて開示していた。
- 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。
  - サイバートラスト株式会社の「[Certification Practice Statement \(認証局運用規程\) Version 8.2 \(平成29年10月19日改定\)](#)」に準拠してサービスを提供していたこと。
- 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 v2.0](#) 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 v2.0](#)に基づいて、平成 28 年 12 月 11 日から平成 29 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 v2.0](#) 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

平成 30 年 2 月 13 日

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

坂本 勝

当社は、[付録A](#)に記載された認証局（以下「CA」という。）Cybertrust Japan Public CA G2及びCybertrust Japan Public CA G3（札幌）を通じて、次のサービス（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「[Certification Practice Statement（認証局運用規程）Version 8.2（平成29年10月19日改定）](#)」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可能性がある。

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v2.0](#)（the WebTrust Principles and Criteria for Certification Authorities v2.0）に準拠して、平成28年12月11日から平成29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。

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「[Certification Practice Statement（認証局運用](#)

[規程\) Version 8.2 \(平成29年10月19日改定\)](#)」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、「[Certification Practice Statement \(認証局運用規程\) Version 8.2 \(平成29年10月19日改定\)](#)」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 v2.0](#)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 G2
- Cybertrust Japan Public CA G3

対象 CA の情報

- Cybertrust Japan Public CA G2

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 キー識別子	拇印
1	CN = Cybertrust Japan Public CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 5c 26	rsaEncryption	(2048bit)	sha1, sha256	2011年8月19日 3:36:33	2018年8月10日 3:35:49	1b e4 8d ef 3a 71 6b 12 65 68 cf b6 91 bc 39 43 01 8d 75 c9	(SHA1) 9f 2e 43 11 21 d8 7d 20 53 e3 2d a3 fa 16 a9 70 af 58 41 52  (SHA256) 00:DC:F6:E0: 20:AB:92:6D: 16:23:F7:31:9 8:18:57:88:26 :5C:43:56:6A :D0:92:28:F3: 14:ED:64:E8: 34:4A:AF

- 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 キー識別子	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) 17 ff 89 23 73 5a 98 08 23 65 50 48 8f 96 c5 30 98 21 25 43  (SHA256) 5E:DD:31:88: 7B:72:45:5B: 40:94:00:52:7 3:ED:75:08:B 7:17:5E:92:D E:F3:95:BD:1 F:7A:DB:21: 00:79:DF:21
2	CN = Cybertrust Japan	CN = Baltimore CyberTrust	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	(SHA1) 7e 41 df 13 e9 a5 0b fa 14 8d

	Public CA G3 O = Cybertrust Japan Co., Ltd. C = JP	Root OU = CyberTrust O = Baltimore C = IE							15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	0c 94 82 bb 42 4b 73 d7 b6 df  (SHA256) C3:9C:3F:61: 90:57:DD:59: 90:3C:62:F8: BC:1C:86:8C :66:8E:0F:45: 1A:79:A5:52: 30:A2:48:BE: 16:BE:10:FF
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	rsaEncr yption	(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) 42 11 76 a7 c4 e8 64 a7 c8 79 59 77 ed 03 79 fa e0 f7 49 5c  (SHA256) CF:B9:3C:1B :39:8F:58:84: E6:98:DC:EB :02:FC:43:00: FB:FF:F3:82: 4A:03:B4:3A: 89:D7:AE:56: CC:40:12:04
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	rsaEncr yption	(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) c0 52 65 39 6b 57 ca 49 cc b2 b0 3c 9c 59 cd 76 bc 5d 91 57  (SHA256) EB:57:F2:05: 11:3A:58:11: 47:E0:F1:D9: 73:28:27:4F: B0:30:EC:69: EE:C8:9C:A2 :97:DC:F5:5 A:3F:B4:46:3 C

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>

(Translation)

**WebTrust for Certification Authorities  
Independent Accountant's Report**

February 13, 2018

To Mr. Masaru Sakamoto  
Senior Manager  
Product Management Department  
Technology Unit  
Certificate Authority & Security Technical Division  
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 G2 and the Cybertrust Japan Public CA G3 services at Sapporo, Japan (the “CA services”) during the period December 11, 2016 through December 10, 2017 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 [Certification Practice Statement Version 8.2, dated October 19, 2017](#) 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 [Certification Practice Statement Version 8.2, dated October 19, 2017](#);
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;



(Translation)

- 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 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 v2.0](#).

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 v2.0](#).

#### 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



(Translation)

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, 2016 through December 10, 2017, the [management's assertion](#) is fairly stated, in all material respects, based on the [WebTrust Principles and Criteria for Certification Authorities v2.0](#).

#### 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 v2.0](#), nor the suitability of any of Cybertrust Japan Co., Ltd.'s services for any customer's intended purpose.



(Translation)

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 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,  
2016 through December 10, 2017**

February 13, 2018

Masaru Sakamoto  
Senior Manager  
Product Management Department  
Technology Unit  
Certificate Authority & Security Technical Division  
Cybertrust Japan Co., Ltd.

Cybertrust Japan Co., Ltd. (“Cybertrust”) provides the following 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 [Certification Practice Statement Version 8.2, dated October 19, 2017](#) 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 assessment, in Cybertrust's Management's opinion, in providing the CA services at Sapporo, Japan, through Cybertrust Japan Public CA G2 and Cybertrust Japan Public CA G3, during the period December 11, 2016 through December 10, 2017, Cybertrust has

1. disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its [Certification Practice Statement Version 8.2, dated October 19, 2017](#) on Cybertrust's website;
2. maintained effective controls to provide reasonable assurance that:
  - Cybertrust provided its services in accordance with its [Certification Practice Statement Version 8.2, dated October 19, 2017](#);
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 v2.0](#) 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

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.)



## Appendix A

## List of CAs in Scope

- Cybertrust Japan Public CA G2
- Cybertrust Japan Public CA G3

## CA Identifying Information for in Scope CAs

- Cybertrust Japan Public CA G2

No	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Fingerprint
1	CN = Cybertrust Japan Public CA G2 O = Cybertrust Japan Co., Ltd. C = JP	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 5c 26	rsaEncryption	(2048bit)	sha1, sha256	Aug 19 3:36:33 2011	Aug 10 3:35:49 2018	1b e4 8d ef 3a 71 6b 12 65 68 cf b6 91 bc 39 43 01 8d 75 c9	(SHA1) 9f 2e 43 11 21 d8 7d 20 53 e3 2d a3 fa 16 a9 70 af 58 41 52  (SHA256) 00:DC:F6:E 0:20:AB:92: 6D:16:23:F7 :31:98:18:57 :88:26:5C:43 :56:6A:D0:9 2:28:F3:14:E D:64:E8:34: 4A:AF

- 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 1:04:33 2013	Jun 9 1:03:31 2020	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) 17 ff 89 23 73 5a 98 08 23 65 50 48 8f 96 c5 30 98 21 25 43  (SHA256) 5E:DD:31:8 8:7B:72:45:5 B:40:94:00:5 2:73:ED:75: 08:B7:17:5E :92:DE:F3:9 5:BD:1F:7A: DB:21:00:79 :DF:21
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	Jan 23 3:45:54 2014	Jun 10 2:44:46 2020	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) 7e 41 df 13 e9 a5 0b fa 14 8d 0c 94 82 bb 42 4b 73 d7 b6 df  (SHA256) C3:9C:3F:61 :90:57:DD:5 9:90:3C:62:F 8:BC:1C:86: 8C:66:8E:0F :45:1A:79:A 5:52:30:A2:4 8:BE:16:BE: 10:FF
3	CN = Cybertrust Japan Public CA G3 O = Cybertrust Japan Co., Ltd.	CN = Baltimore CyberTrust Root OU = CyberTrust O = Baltimore C = IE	07 27 a2 76	rsaEncryption	(2048bit)	sha1, sha256	Feb 28 3:09:27 2014	Jun 10 2:07:29 2020	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4	(SHA1) 42 11 76 a7 c4 e8 64 a7 c8 79 59 77 ed 03 79 fa e0 f7 49 5c  (SHA256) CF:B9:3C:1

(Translation)

	C = JP								13 06	B:39:8F:58:84:E6:98:DC:EB:02:FC:43:00:FB:FF:F3:82:4A:03:B4:3A:89:D7:AE:56:CC:40:12:04
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	Nov 15 21:03:31 2016	May 10 21:00:00 2025	73 a8 08 53 29 b8 15 fb 99 80 e5 c5 37 d8 f8 39 7b a4 13 06	(SHA1) c0 52 65 39 6b 57 ca 49 cc b2 b0 3c 9c 59 cd 76 bc 5d 91 57  (SHA256) EB:57:F2:05:11:3A:58:11:47:E0:F1:D9:73:28:27:4F:B0:30:EC:69:EE:C8:9C:A2:97:DC:F5:5A:3F:B4:46:3C

## 独立した監査法人の認証局のための WebTrust 保証報告書

平成 30 年 2 月 13 日

サイバートラスト株式会社  
認証・セキュリティ事業部  
技術統括部 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  
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 v2.0 \(the WebTrust Principles and Criteria for Certification Authorities v2.0\)](#) に基づいて、平成 28 年 12 月 11 日から平成 29 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）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。[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「[Extended Validation Certificate Certification Practice Statement \(EVC認証局運用規程\) Version 3.7 \(平成29年10月19日改定\)](#)」にて開示していた。
- 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。
  - サイバートラスト株式会社の「[Extended Validation Certificate Certification Practice Statement \(EVC認証局運用規程\) Version 3.7 \(平成29年10月19日改定\)](#)」に準拠してサービスを提供していたこと。
- 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 v2.0](#) 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 v2.0](#)に基づいて、平成 28 年 12 月 11 日から平成 29 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 v2.0](#) 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

平成 30 年 2 月 13 日

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

坂本 勝

当社は、[付録A](#)に記載された認証局（以下「CA」という。）Cybertrust Japan EV CA G2（札幌）を通じて、次のサービス（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「[Extended Validation Certificate Certification Practice Statement \(EVC認証局運用規程\) Version 3.7 \(平成29年10月19日改定\)](#)」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可能性がある。

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v2.0](#)（the WebTrust Principles and Criteria for Certification Authorities v2.0）に準拠して、平成28年12月11日から平成29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。

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「[Extended Validation Certificate](#)

[Certification Practice Statement \(EVC認証局運用規程\) Version 3.7 \(平成29年10月19日改定\)](#)」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、「[Extended Validation Certificate Certification Practice Statement \(EVC認証局運用規程\) Version 3.7 \(平成29年10月19日改定\)](#)」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 v2.0](#)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 キー識別子	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) b5 d1 7f e3 bd c0 3f 80 b7 a8 1f fc b6 3f cb 58 32 26 8a bd (SHA256) 89:17:FC: CC:50:42: 4C:56:C9: 85:BC:0B: 35:2F:53: B0:CC:9A :8E:4B:77: 63:24:2E: A9:88:C9: D1:CD:05: 27:F0
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) 15 c9 36 ad ca 01 ca 4c f3 1f 0f c1 13 7f a6 0c 11 0e bf d7 (SHA256) BD:45:B2: 52:C7:2F: 3D:6D:94: A5:7B:D6: F7:31:54:1 2:97:62:88 :03:96:E7: 44:17:AC: F5:12:57:9 3:29:69:C 6
3	CN = Cybertrust Japan EV CA G2 O = Cybertrust Japan Co., Ltd.	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	(SHA1) 99 02 d1 d1 5c 5a 16 28 81 2c 2e 23 a3 84 c2 bb 4e 1d a3 70

	C = JP								2a 2b 8d 5f	(SHA256) 87:D9:13: 0F:0D:B2: 62:78:14:E 4:86:AF:7 F:E1:95:4 C:1F:E4:E 3:CB:FA:1 9:3D:0F:6 6:AA:11:5 7:CC:9E:E 0:8C
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	rsaEncr yption	(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) e3 d9 d2 19 c4 ed 51 36 69 f5 ef 3f a1 5a 8d e1 27 8f 29 27  (SHA256) 40:0E:5E: 85:24:F3:5 5:98:79:85 :76:31:2E: 75:A5:45: 14:0A:4E: 4B:73:14: C1:C8:C5: 3F:D7:EC: 82:0E:77: 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>

(Translation)

**WebTrust for Certification Authorities  
Independent Accountant's Report**

February 13, 2018

To Mr. Masaru Sakamoto  
Senior Manager  
Product Management Department  
Technology Unit  
Certificate Authority & Security Technical Division  
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, 2016 through December 10, 2017 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 [Extended Validation Certificate Certification Practice Statement Version 3.7, dated October 19, 2017](#), 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 [Extended Validation Certificate Certification Practice Statement Version 3.7, dated October 19, 2017](#);
3. maintained effective controls to provide reasonable assurance that:



(Translation)

- 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 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 v2.0](#).

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 v2.0](#).

#### 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



(Translation)

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, 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, 2016 through December 10, 2017, the [management's assertion](#) is fairly stated, in all material respects, based on the [WebTrust Principles and Criteria for Certification Authorities v2.0](#).

#### 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 v2.0](#), nor the suitability of any of Cybertrust Japan Co., Ltd.'s services for any customer's intended purpose.



(Translation)

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 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,  
2016 through December 10, 2017**

February 13, 2018

Masaru Sakamoto  
Senior Manager  
Product Management Department  
Technology Unit  
Certificate Authority & Security Technical Division  
Cybertrust Japan Co., Ltd.

Cybertrust Japan Co., Ltd. (“Cybertrust”) provides the following 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 [Extended Validation Certificate Certification Practice Statement Version 3.7, dated October 19, 2017](#) 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, through Cybertrust Japan EV CA G2, during the period December 11, 2016 through December 10, 2017, Cybertrust has:

1. disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its [Extended Validation Certificate Certification Practice Statement Version 3.7, dated October 19, 2017](#) on Cybertrust's website;
2. maintained effective controls to provide reasonable assurance that:
  - Cybertrust provided its services in accordance with its [Extended Validation Certificate Certification Practice Statement Version 3.7, dated October 19, 2017](#);
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 v2.0](#) 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

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.)

## 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	Nov 9 17:00:0 0 2012	Dec 9 17:00:0 0 2019	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) b5 d1 7f e3 bd c0 3f 80 b7 a8 1f fc b6 3f cb 58 32 26 8a bd  (SHA256) 89:17:FC:C C:50:42:4C: 56:C9:85:B C:0B:35:2F: 53:B0:CC:9 A:8E:4B:77 :63:24:2E:A 9:88:C9:D1: CD:05:27:F 0
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	Jan 8 17:00:0 0 2014	Dec 10 17:00:0 0 2019	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) 15 e9 36 ad ca 01 ca 4c f3 1f 0f c1 13 7f a6 0c 11 0e bf d7  (SHA256) BD:45:B2:5 2:C7:2F:3D :6D:94:A5: 7B:D6:F7:3 1:54:12:97: 62:88:03:96 :E7:44:17:A C:F5:12:57: 93:29:69:C6
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	Feb 26 17:00:0 0 2014	Dec 10 17:00:0 0 2019	91 43 05 ec b4 6a 15 4f dc e1 ee 86 56 5c 11 d0 2a 2b 8d 5f	(SHA1) 99 02 d1 d1 5c 5a 16 28 81 2c 2e 23 a3 84 c2 bb 4e 1d a3 70  (SHA256) 87:D9:13:0 F:0D:B2:62 :78:14:E4:8 6:AF:7F:E1 :95:4C:1F:E 4:E3:CB:FA :19:3D:0F:6 6:AA:11:57: CC:9E:E0:8 C
4	CN = Cybertrust Japan EV CA G2 O = Cybertrust	CN = Cybertrust Global Root O = Cybertrust,	0a a1 58 96 a4 d1 af 80 0d a1 69 0e	rsaEncryption	(2048bit)	sha1, sha256	Jul 13 21:19:2 8 2017	Dec 14 21:00:0 0 2021	91 43 05 ec b4 6a 15 4f dc e1 ee 86	(SHA1) e3 d9 d2 19 c4 ed 51 36 69 f5 ef 3f a1 5a 8d e1 27 8f 29 27

(Translation)

	Japan Co., Ltd. C = JP	Inc	f4 a3 af b4						56 5c 11 d0 2a 2b 8d 5f	(SHA256) 40:0E:5E:8 5:24:F3:55: 98:79:85:76 :31:2E:75:A 5:45:14:0A: 4E:4B:73:1 4:C1:C8:C5 :3F:D7:EC: 82:0E:77:B 5
--	------------------------------	-----	----------------	--	--	--	--	--	----------------------------------	---