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

独立した監査法人の認証局のための WebTrust-SSL 基本要件保証報告書

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ーSSL 基本要件保証規準 v2.2（the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.2）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 SSL 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、「SSL-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。

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SSL証明書を提供するためのコミットメントを含む証明書実務と手続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、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ための有効な内部統制を維持していた。
   - 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。

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ための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システムに係る開発、保守及び運用は適切に承認され、実施されていたこと。
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ための有効な内部統制を維持していた。
   - CAブラウザフォーラムが定めるNetwork and Certificate System Security Requirementsに適合していたこと。

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ーSSL 基本要件保証規準 v2.2 に基づいて、SSL-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 SSL-CA サービスの鍵と SSL 証明書のライフサイクル管理のビジネス実務及び鍵と SSL 証明書のインテグリティ、鍵と SSL 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 SSL 証明書のライフサイクル管理のビジネス実務に従って実施された取引を試査によりテストし、(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 SSL-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－SSL 基本要件保証規準 v2.2 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－SSL 基本要件保証規準 v2.2 で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 SSL-CA サービスの品質についての何らの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のためのサイバートラスト株式会社のサービスの適合性についても何らの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－SSL 基本要件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

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、SSL認証局（以下「CA」という。）サービス（以下「SSL-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、当社のネットワークと証明書のセキュリティシステムの内部統制、Webサイトで公開しているSSL-CAビジネス実務の開示、及び鍵と証明書のライフサイクル管理の内部統制を含む当社のSSL-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SSL-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、SSL-CAサービスに係る証明書実務の開示と内部統制を評価した。その評価に基づく当社の経営者の意見では、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、SSL-CAサービス（札幌）の提供に関し、認証局のためのWebTrust-SSL基本要件保証規準v2.2（the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.2）に準拠して、下記の事項を実施した。

1. 当社は、CAブラウザフォーラムガイドラインに準拠してSSL証明書を提供するためのコミットメントを含む証明書実務と手続を当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、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ための有効な内部統制を維持していた。
   - 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。

3. 当社は、下記について合理的な保証を提供するための有効な内部統制を維持していた。
   - 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システムに係る開発、保守及び運用は適切に承認され、実施されていたこと。
4. 当社は、下記について合理的な保証を提供するための有効な内部統制を維持していた。
   - CAブラウザフォーラムが定めるNetwork and Certificate System Security Requirementsに適合していたこと。

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:F7:31:98:18:57:88:26:5C: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:40:94:00:52:73:ED:75:08:B7:17:5E:92:DE:F3:95: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	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) 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: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	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) 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	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) 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

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-SSL Baseline Requirements for Certification Authorities
Independent Accountants' 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 SSL certificate authority (CA) services at Sapporo, Japan (the "SSL-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 Certificate practices and procedures in its Certification Practice Statement Version 8.2, dated October 19, 2017 on Cybertrust Japan Co., Ltd.'s website, including its commitment to provide SSL 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:
   - subscriber information was properly collected, authenticated (for the registration activities performed by Cybertrust Japan Co., Ltd.) and verified;
   - the integrity of keys and certificates it manages was established and protected throughout their life cycles;

3. 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

4. maintained effective controls to provide reasonable assurance that:

(Translation)

- it met the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

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 – SSL Baseline with Network Security 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 Practical 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 SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and SSL 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 SSL 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 SSL-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 for Certification Authorities – SSL Baseline with Network Security v2.2.

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 for Certification Authorities – SSL Baseline with Network Security 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 – SSL Baseline with Network Security 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") operates its SSL certification authority (CA) services (the "SSL-CA services") through its CAs as enumerated in Appendix A.

The management of Cybertrust is responsible for establishing and maintaining effective controls over its SSL- CA services operations, including its network and certificate security system controls, its SSL-CA business practices disclosure on its website, key lifecycle management controls, and 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 internal control can provide only reasonable assurance with respect to Cybertrust's SSL-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 SSL−CA services. Based on that assessment, in Cybertrust Management's opinion, in providing its SSL-CA services at Sapporo, Japan during the period from December 11, 2016 through December 10, 2017 through the Cybertrust Japan Public CA G2, and the Cybertrust Japan Public CA G3, Cybertrust has:

1. disclosed its Certificate practices and procedures in its Certification Practice Statement Version 8.2, dated October 19, 2017 on Cybertrust's website, including its commitment to provide SSL 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:
   - subscriber information was properly collected, authenticated (for the registration activities performed by Cybertrust) and verified;
   - the integrity of keys and certificates it manages was established and protected throughout their life cycles;

(Translation)

3. 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
4. maintained effective controls to provide reasonable assurance that:
    - it met the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust for Certification Authorities – SSL Baseline with Network Security v2.2.

(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 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:E0:20:AB:92:6D:16:23:F7:31:98:18:57:88:26:5C:43:56:6A:D0:92:28:F3:14:ED:64:E8:34:4A:AF

- Cybertrust Japan Public CA G3

No	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:31:88:7B:72:45:5B:40:94:00:52:73:ED:75:08:B7:17:5E:92:DE:F3:95: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: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	CN = Baltimore CyberTrust Root OU = CyberTrust	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	(SHA1) 42 11 76 a7 c4 e8 64 a7 c8 79 59 77 ed 03 79 fa e0 f7 49 5c

	Japan Co., Ltd. C = JP	O = Baltimore C = IE							f8 39 7b a4 13 06	(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	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

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

独立した監査法人の認証局のための WebTrust-SSL 基本要件保証報告書

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ーSSL 基本要件保証規準 v2.2（the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.2）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 SSL 認証局（以下「CA」という。）Cybertrust Japan EV CA G2（札幌）サービス（以下、「SSL-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。

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SSL証明書を提供するためのコミットメントを含む証明書実務と手続を当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、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ための有効な内部統制を維持していた。
   - 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。
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ための有効な内

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システムに係る開発、保守及び運用は適切に承認され、実施されていたこと。

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ための有効な内部統制を維持していた。
   - CAブラウザフォーラムが定めるNetwork and Certificate System Security Requirementsに適合していたこと。

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ーSSL 基本要件保証規準 v2.2 に基づいて、SSL-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 SSL-CA サービスの鍵と SSL 証明書のライフサイクル管理のビジネス実務及び鍵と SSL 証明書のインテグリティ、鍵と SSL 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 SSL 証明書のライフサイクル管理のビジネス実務に従って実施された取引を試査によりテストし、(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 SSL-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－SSL 基本要件保証規準 v2.2 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－SSL 基本要件保証規準 v2.2 で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 SSL-CA サービスの品質についての何らの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のためのサイバートラスト株式会社のサービスの適合性についても何らの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－SSL 基本要件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

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、SSL認証局（以下「CA」という。）Cybertrust Japan EV CA G2（札幌）サービス（以下「SSL-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、当社のネットワークと証明書のセキュリティシステムの内部統制、Webサイトで公開しているSSL-CAビジネス実務の開示、及び鍵と証明書のライフサイクル管理の内部統制を含む当社のSSL-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SSL-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、SSL-CAサービスに係る証明書実務の開示と内部統制を評価した。その評価に基づく当社の経営者の意見では、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、SSL-CAサービス（札幌）の提供に関し、認証局のためのWebTrust-SSL基本要件保証規準v2.2（the WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security v2.2）に準拠して、下記の事項を実施した。

1. 当社は、CAブラウザフォーラムガイドラインに準拠してSSL証明書を提供するためのコミットメントを含む証明書実務と手続を当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、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ための有効な内部統制を維持していた。
   - 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。

3. 当社は、下記について合理的な保証を提供するための有効な内部統制を維持していた。
   - 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システムに係る開発、保守及び運用は適切に承認され、実施されていたこと。
4. 当社は、下記について合理的な保証を提供するための有効な内部統制を維持していた。
   - CAブラウザフォーラムが定めるNetwork and Certificate System Security Requirementsに適合していたこと。

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:F7:31:54:12:97:62:88:03:96:E7:44:17:AC: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	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) 99 02 d1 d1 5c 5a 16 28 81 2c 2e 23 a3 84 c2 bb 4e 1d a3 70 (SHA256) 87:D9:13:0F:0D:B2:62:78:14:E4:86:AF:7F:E1:95:4C:1F:E4:E3:CB:FA:19:3D:0F

										:66:AA:11:57:CC:9E:E0:8C
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	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) 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:F3:55:98:79:85:76:31:2E: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-SSL Baseline Requirements for Certification Authorities
Independent Accountants' 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 SSL certificate authority (CA) services as Cybertrust Japan EV CA G2 services at Sapporo, Japan (the "SSL-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 Certificate practices and procedures in its Extended Validation Certificate Certification Practice Statement Version 3.7, dated October 19, 2017 on Cybertrust Japan Co., Ltd.'s website, including its commitment to provide SSL 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:
   - subscriber information was properly collected, authenticated (for the registration activities performed by Cybertrust Japan Co., Ltd.) and verified;
   - the integrity of keys and certificates it manages was established and protected throughout their life cycles;

3. 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

4. maintained effective controls to provide reasonable assurance that:

(Translation)

- it met the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

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 – SSL Baseline with Network Security 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 Practical 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 SSL certificate life cycle management business practices and its controls over key and SSL certificate integrity, over the continuity of key and SSL 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 SSL 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 SSL-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 – SSL Baseline with Network Security v2.2.

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 – SSL Baseline with Network Security 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 – SSL Baseline with Network Security 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") operates its SSL certification authority (CA) services as Cybertrust Japan EV CA G2 services at Sapporo, Japan (the "SSL-CA services") through its CAs as enumerated in Appendix A.

The management of Cybertrust is responsible for establishing and maintaining effective controls over its SSL- CA services operations, including its network and certificate security system controls, its SSL-CA business practices disclosure on its website, key lifecycle management controls, and 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 internal control can provide only reasonable assurance with respect to Cybertrust's SSL-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 SSL−CA services. Based on that assessment, in Cybertrust Management's opinion, in providing its SSL-CA services at Sapporo, Japan during the period from December 11, 2016 through December 10, 2017, Cybertrust has:

1. disclosed its Certificate practices and procedures in its Extended Validation Certificate Certification Practice Statement Version 3.7, dated October 19, 2017 on Cybertrust's website, including its commitment to provide SSL 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:
   - subscriber information was properly collected, authenticated (for the registration activities performed by Cybertrust) and verified;

- the integrity of keys and certificates it manages was established and protected throughout their life cycles;

3. 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

4. maintained effective controls to provide reasonable assurance that:
   - it met the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

(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 Berfore	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 17:00:00 2012	Dec 9 17:00:00 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: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	Jan 8 17:00:00 2014	Dec 10 17:00:00 2019	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:F7:31:54:12:97:62:88:03:96:E7:44:17:AC: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 17:00:00 2014	Dec 10 17:00:00 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:D9:13:0F:0D:B2:62:78:14:E4:86:AF:7F:E1:95:4C:1F:E4:E3:CB:FA:19:3D:0F:66:AA:11:57:CC:9E:E0:8C
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	rsaEncryption	(2048bit)	sha1, sha256	Jul 13 21:19:28 2017	Dec 14 21:00:00 2021	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:F3:55:98:79:85:76:31:2E:75:A5:45:14:0A:4E:4B:73:1

										4:C1:C8:C5:3F:D7:EC:82:0E:77:B5