



有限責任 あずさ監査法人

〒162-8551

東京都新宿区津久戸町 1 番 2 号

あずさセンタービル

Telephone 03 3266 7500

Fax 03 3266 7600

Internet home.kpmg/jp/azsa
period of time

独立業務実施者の保証報告書

2023 年 2 月 16 日

サイバートラスト株式会社
PKI 技術本部
パブリック証明書マネジメント部
部長
坂本 勝 殿

有限責任 あずさ監査法人
東京事務所
パートナー 公認会計士

紫垣昌利

範囲

当監査法人は、[認証局のための WebTrust の規準 v2.2.2 \(the WebTrust Principles and Criteria for Certification Authorities v2.2.2\)](#) に準拠して、2021 年 12 月 11 日から 2022 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。）のサービス（北海道及び東京）（以下「CA サービス」という。）に関する[経営者の記述書](#)について合理的保証業務を行った。

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

- サイバートラスト株式会社は、CA 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[付録 B](#) に記載された認証局運用規程及び証明書ポリシーにて開示していた。
- 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認証局運用規程は、証明書ポリシーと整合していたこと。
 - サイバートラスト株式会社は、証明書ポリシー及び認証局運用規程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及び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 システム及びデータへの論理的、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、証明書の一時的停止サービス及び下位 CA 証明書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。

認証局の責任

サイバートラスト株式会社の経営者の責任は、[認証局のための WebTrust の規準 v2.2.2](#) に準拠して、経営者の記述書を適正に作成すること、及び、記述書に記載されたサービスを提供することにある。

職業倫理、独立性及び品質管理

当監査法人は、誠実性、客観性、職業的専門家としての能力及び正当な注意、秘密保持並びに職業的専門家としての行動に関する基本原則を基礎とする国際会計士倫理基準審議会の職業会計士のための国際倫理規程（国際独立性基準を含む。）（国際倫理規程）の独立性及びその他の職業倫理に関する規定を遵守した。

また、当監査法人は、国際品質管理基準の第 1 号「過去財務情報の監査及びレビュー、その他の保証業務及び関連サービス業務を実施する会計事務所の品質管理」を適用しており、従って、職業倫理に関する規定、職業的専門家としての基準及び適用される法令等の要求事項の遵守に関して文書化した方針と手続を含む、包括的な品質管理システムを保持している。

業務実施者の責任

当監査法人の責任は、当監査法人の実施した手続に基づいて経営者の記述書に対して意見を表明することにある。

当監査法人は、国際監査・保証基準審議会が公表した国際保証業務基準 3000「過去財務情報の監査又はレビュー以外の保証業務」に準拠して業務を実施した。当該指針は、当監査法人に、すべての重要な点において、経営者の記述書が適正に表示されているかどうかについて、合理的な保証を得るための手続を計画し実施することを求めている。従って、手続には、(1) サイバートラスト株式会社の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機密保持、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すること、(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



すること、(3)内部統制の運用評価手続を実施し評価すること、(4)当監査法人が状況に応じて必要と認めたその他の手続を実施することを含んでいる。

当監査法人は、意見表明の基礎となる十分かつ適切な証拠を入手したと判断している。

サイバートラスト株式会社における特定の内部統制の相対的な有効性と重要性、及び加入者と信頼者の内部統制リスクの評価に与える影響は、内部統制との相互作用、及び個々の加入者と信頼者の所在場所において現れるその他の要因に依存している。当監査法人は個別の加入者と信頼者の所在場所における内部統制の有効性を評価するための手続を実施していない。

内部統制の限界

内部統制の有効性には、人為的なミスの可能性や内部統制の回避など、固有の限界がある。例えば、その性質により、内部統制は、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の将来への予測は、内部統制が無効になる可能性があるというリスクの影響を受ける。

意見

当監査法人は、サイバートラスト株式会社の経営者の記述書が、[認証局のための WebTrust の規準 v2.2.2](#)に基づいて、2021 年 12 月 11 日から 2022 年 12 月 10 日までの期間において、すべての重要な点において適正に表示されているものと認める。

この保証報告書は、[認証局のための WebTrust の規準 v2.2.2](#)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表明するものではない。また、いかなる顧客の意図する目的に対するサイバートラスト株式会社のサービスの適合性についても何ら表明するものではない。

WebTrust シールの使用

サイバートラスト株式会社の認証局のための WebTrust 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。

その他の情報

サイバートラスト株式会社の経営者は、CA ブラウザフォーラムを構成するインターネットブラウザのオンラインフォーラムである Bugzilla のサイトで公開された情報を記載した[付録 C](#)を当監査法人に開示している。



付録 A

対象 CA

OV SSL Issuing CAs
CA#1: Cybertrust Japan SureServer CA G4
EV SSL Issuing CAs
CA#2: Cybertrust Japan SureServer EV CA G3
Secure Email (S/MIME) CAs
CA#3: Cybertrust Japan SureMail CA G4



対象CAの識別情報

CA #	Cert #1	サブジェクト	発行者	シリアル番号	キーアルゴリズム	キーサイズ	署名アルゴリズム	有効期限の開始	有効期限の終了	サブジェクトキー識別子	拇印
1	1	CN = Cybertrust Japan SureServer CA G4 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b1630cecb43c2e	rsaEncryption	2048bit	sha256WithRSAEncryption	2019年9月27日 10:54:23	2029年5月29日 14:00:39	62a7d2dade85b692f185b cf6e8959d75a0fa4e1f	(SHA1) F695C5B4037AE8EAE51EA943A4F54D750E0DA609 (SHA256) 0207056D172C80BDFB6DC45BE9E5808846078D1E6EEF1B6ED70259AB332A64C1
2	1	CN = Cybertrust Japan SureServer EV CA G3 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b16488bce695fc	rsaEncryption	2048bit	sha256WithRSAEncryption	2019年9月27日 11:04:20	2029年5月29日 14:00:39	826c755d53f54569bc252 da44c89e6b2b74187a3	(SHA1) A88503F53FA02D0B2C4D1437BCD1BD6AA111539D (SHA256) FEC99ADA7AA49D4FEA9EFF123542095A880C004FD6933F9364B02B2E3574EA38
3	1	CN = Cybertrust Japan SureMail CA G4 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b1655c8e69915b	rsaEncryption	2048bit	sha256WithRSAEncryption	2019年9月27日 11:14:09	2029年5月29日 14:00:39	fcc6dafec7add55ace48dec ffde828c5a3ba8f11	(SHA1) BACAF A90E4A81408FF7B1245B7E973213C83488C (SHA256) 73609E68EEAA8B52808CB503FB8EA64EDD38923DA9C55AE788051AB416DD759E

付録 B

CA	証明書ポリシー及び認証局運用規程	ウェブサイト
Cybertrust Japan SureServer CA G4	- サイバートラスト認証局運用規程 v1.3 (発効日：2022年05月13日) - サイバートラスト認証局運用規程 v1.4 (発効日：2022年09月05日) - サイバートラスト SureServer 証明書ポリシー v1.9 (発効日：2022年06月23日) - サイバートラスト SureServer 証明書ポリシー v2.0 (発効日：2022年09月05日)	https://www.cybertrust.ne.jp/ssl/repository/
Cybertrust Japan SureServer EV CA G3	- サイバートラスト認証局運用規程 v1.3 (発効日：2022年05月13日) - サイバートラスト認証局運用規程 v1.4 (発効日：2022年09月05日) - サイバートラスト SureServer EV 証明書ポリシー v2.0 (発効日：2022年06月23日) - サイバートラスト SureServer EV 証明書ポリシー v2.1 (発効日：2022年09月05日)	https://www.cybertrust.ne.jp/ssl/repository/
Cybertrust Japan SureMail CA G4	- サイバートラスト認証局運用規程 v1.3 (発効日：2022年05月13日) - サイバートラスト認証局運用規程 v1.4 (発効日：2022年09月05日) - サイバートラスト SureMail 証明書ポリシー v2.0 (発効日：2022年06月23日) - サイバートラスト SureMail 証明書ポリシー v2.1 (発効日：2022年09月05日)	https://www.cybertrust.ne.jp/ssl/repository/



付録 C

#	開示内容	公開リンク
1	SECOM: Failed an annual update of Cybertrust Japan (CTJ) CPS	https://bugzilla.mozilla.org/show_bug.cgi?id=1769222

以上

経営者の記述書

2023 年 2 月 16 日

サイバートラスト株式会社
PKI 技術本部
パブリック証明書マネジメント部
部長



当社は、[付録 A](#)に記載された認証局（以下「CA」という。）を運営し、次の認証局サービス（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
- ・ 加入者鍵の生成

当社の経営者は、当社の Web サイトで公開している CA ビジネス実務の開示、CA ビジネス実務の管理、CA 環境の内部統制、CA 鍵のライフサイクル管理の内部統制、加入者鍵ライフサイクル管理の内部統制及び証明書のライフサイクル管理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、人為的なミスの可能性や内部統制の回避など、固有の限界がある。従って、有効な内部統制といえども、当社の CA の運用について合理的な保証を提供するものでしかない。さらに、状況の変化により、内部統制の有効性は時間とともに変化する可能性がある。

当社の経営者は、当社の CA（北海道及び東京）の運用に関するビジネス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、当社は、[認証局のための](#)



[WebTrust の規準 v2.2.2 \(the WebTrust Principles and Criteria for Certification Authorities v2.2.2\)](#) に準拠して、2021 年 12 月 11 日から 2022 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 サイトで[付録 B](#)に記載された認証局運用規程及び証明書ポリシーにて開示していた。
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。
 - ・ 当社の証明書ポリシーと認証局運用規程が整合していたこと。
 - ・ 当社は、証明書ポリシー及び認証局運用規程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。
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 v2.2.2](#)には、以下が含まれる。

CA ビジネス実務の開示

- ・ 認証局運用規程 (CPS)
- ・ 証明書ポリシー (CP)

CA のビジネス実務管理

- ・ 証明書ポリシー管理
- ・ 認証局運用規程の管理
- ・ CP および CPS の一貫性

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

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

加入者鍵ライフサイクル管理の内部統制

- ・ CA が提供する加入者鍵生成サービス

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

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

当社は、CA の鍵を寄託せず、証明書の一時的停止サービス及び下位 CA 証明書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

OV SSL Issuing CAs
CA#1: Cybertrust Japan SureServer CA G4
EV SSL Issuing CAs
CA#2: Cybertrust Japan SureServer EV CA G3
Secure Email (S/MIME) CAs
CA#3: Cybertrust Japan SureMail CA G4



対象 CA の識別情報

CA #	Cert #	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	ダイジェストアルゴリズム	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	1	CN = Cybertrust Japan SureServer CA G4 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b1630cecb43c2e	rsaEncryption	2048bit	sha256WithRSAEncryption	2019年9月27日10:54:23	2029年5月29日14:00:39	62a7d2dade85b692f185bcf6e8959d75a0fa4e1f	(SHA1) F695C5B4037AE8EAE51EA943A4F54D750E0DA609 (SHA256) 0207056D172C80BDFB6DC45BE9E5808846078D1E6EEF1B6ED70259AB332A64C1
2	1	CN = Cybertrust Japan SureServer EV CA G3 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b16488bce695fc	rsaEncryption	2048bit	sha256WithRSAEncryption	2019年9月27日11:04:20	2029年5月29日14:00:39	826c755d53f54569bc252da44c89e6b2b74187a3	(SHA1) A88503F53FA02D0B2C4D1437BCD1BD6AA111539D (SHA256) FECE9ADA7AA49D4FEA9EFF123542095A880C004FD6933F9364B02B2E3574EA38
3	1	CN = Cybertrust Japan SureMail CA G4 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b1655c8e69915b	rsaEncryption	2048bit	sha256WithRSAEncryption	2019年9月27日11:14:09	2029年5月29日14:00:39	fcc6dafec7add55ace48deeffde828c5a3ba8f11	(SHA1) BACAFA90E4A81408FF7B1245B7E973213C83488C (SHA256) 73609E68EEAA8B52808CB503FB8EA64EDD38923DA9C55AE788051AB416DD759E

付録 B

CA	証明書ポリシー及び認証局運用規程	ウェブサイト
Cybertrust Japan SureServer CA G4	- サイバートラスト認証局運用規程 v1.3 (発効日：2022年05月13日) - サイバートラスト認証局運用規程 v1.4 (発効日：2022年09月05日) - サイバートラスト SureServer 証明書ポリシー v1.9 (発効日：2022年06月23日) - サイバートラスト SureServer 証明書ポリシー v2.0 (発効日：2022年09月05日)	https://www.cybertrust.ne.jp/ss/repository/
Cybertrust Japan SureServer EV CA G3	- サイバートラスト認証局運用規程 v1.3 (発効日：2022年05月13日) - サイバートラスト認証局運用規程 v1.4 (発効日：2022年09月05日) - サイバートラスト SureServer EV 証明書ポリシー v2.0 (発効日：2022年06月23日) - サイバートラスト SureServer EV 証明書ポリシー v2.1 (発効日：2022年09月05日)	https://www.cybertrust.ne.jp/ss/repository/
Cybertrust Japan SureMail CA G4	- サイバートラスト認証局運用規程 v1.3 (発効日：2022年05月13日) - サイバートラスト認証局運用規程 v1.4 (発効日：2022年09月05日) - サイバートラスト SureMail 証明書ポリシー v2.0 (発効日：2022年06月23日) - サイバートラスト SureMail 証明書ポリシー v2.1 (発効日：2022年09月05日)	https://www.cybertrust.ne.jp/ss/repository/



付録 C

#	開示内容	公開リンク
1	SECOM: Failed an annual update of Cybertrust Japan (CTJ) CPS	https://bugzilla.mozilla.org/show_bug.cgi?id=1769222

以上



KPMG AZSA LLC
AZSA Center Building
1-2 Tsukudo-cho, Shinjuku-ku
Tokyo 162-8551, Japan
Telephone +81 (3) 3266 7500
Fax +81 (3) 3266 7600
Internet home.kpmg/jp/azsa
period of time

(Translation)

INDEPENDENT ASSURANCE REPORT

February 16, 2023

To Mr. Masaru Sakamoto
Manager
Public Certificate Management Department
PKI Technology Business Unit
Cybertrust Japan Co., Ltd.

KPMG AZSA LLC
Tokyo Office
Partner, Certified Public Accountant
Masatoshi Shigaki

Scope

We have been engaged, in a reasonable assurance engagement, to report on the [management's assertion](#) of Cybertrust Japan Co., Ltd.. ("CTJ") that for its Certification Authority (CA) operations at Hokkaido and Tokyo, Japan, throughout the period December 11, 2021 to December 10, 2022 for its CAs as enumerated in [Appendix A](#), CTJ has:

1. disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#) on CTJ website
2. maintained effective controls to provide reasonable assurance that:
 - The Certification Practice Statements of CTJ are consistent with its Certificate Policies; and
 - CTJ provides its services in accordance with its Certificate Policies and Certification Practice Statements
3. maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
 - the Subscriber information is properly authenticated (for the registration activities performed by CTJ)
4. maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity



(Translation)

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

CTJ does not escrow its CA keys, and does not provide certificate suspension services, and does not provide subordinate CA certificate services. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

CTJ's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

Our independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (including International Independence Standards) (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Control 1, *Quality Control for Firms that Perform Audits and Reviews of Historical Financial Information, and Other Assurance and Related Services Engagements*, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Practitioner's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

- (1) obtaining an understanding of CTJ'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 lifecycle management operations, and over the development, maintenance and operation of systems integrity;
- (2) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business practices;
- (3) testing and evaluating the operating effectiveness of the controls; and
- (4) performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at CTJ and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other



(Translation)

factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

Opinion

In our opinion, throughout the period December 11, 2021 to December 10, 2022, CTJ management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#).

This report does not include any representation as to the quality of CTJ's CA services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), nor the suitability of any of CTJ's CA services for any customer's intended purpose.

Use of the WebTrust seal

CTJ's use of the WebTrust for Certification Authorities Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Other Matters

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

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



(Translation)

APPENDIX A

List of CAs in Scope

OV SSL Issuing CAs
CA#1: Cybertrust Japan SureServer CA G4
EV SSL Issuing CAs
CA#2: Cybertrust Japan SureServer EV CA G3
Secure Email (S/MIME) CAs
CA#3: Cybertrust Japan SureMail CA G4



(Translation)

CA Identifying Information for in Scope CAs

CA #	Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Fingerprint
1	1	CN = Cybertrust Japan SureServer CA G4 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b1630cecb43c2e	rsaEncryption	2048bit	sha256WithRSAEncryption	September 27, 2019 10:54:23	May 29, 2029 14:00:39	62a7d2dade85b692f185bcf6e8959d75a0fa4e1f	(SHA1) F695C5B4037AE8EAE51EA943A4F54D750E0DA609 (SHA256) 0207056D172C80BDFB6DC45BE9E5808846078D1E6EEF1B6ED70259AB332A64C1
2	1	CN = Cybertrust Japan SureServer EV CA G3 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b16488bce695fc	rsaEncryption	2048bit	sha256WithRSAEncryption	September 27, 2019 11:04:20	May 29, 2029 14:00:39	826c755d53f54569bc252da44c89e6b2b74187a3	(SHA1) A88503F53FA02D0B2C4D1437BCD1BD6AA111539D (SHA256) FECE9ADA7AA49D4FEA9EFF123542095A880C004FD6933F9364B02B2E3574EA38
3	1	CN = Cybertrust Japan SureMail CA G4 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b1655c8e69915b	rsaEncryption	2048bit	sha256WithRSAEncryption	September 27, 2019 11:14:09	May 29, 2029 14:00:39	fcc6dafec7add55ace48decffde828c5a3ba8f11	(SHA1) BACAF A90E4A81408FF7B1245B7E973213C83488C (SHA256) 73609E68EEAA8B52808CB503FB8EA64EDD38923DA9C55AE788051AB416DD759E

APPENDIX B

CA	CP/CPS	Website
Cybertrust Japan SureServer CA G4	• Cybertrust Japan Certification Practice Statement version 1.3 (Effective Date : May 13, 2022) • Cybertrust Japan Certification Practice Statement version 1.4 (Effective Date : September 5, 2022) • Cybertrust Japan SureServer Certificate Policy v1.9 (Effective Date : June 23, 2022) • Cybertrust Japan SureServer Certificate Policy v2.0 (Effective Date : September 5, 2022)	https://www.cybertrust.ne.jp/ssl/repository/
Cybertrust Japan SureServer EV CA G3	• Cybertrust Japan Certification Practice Statement version 1.3 (Effective Date : May 13, 2022) • Cybertrust Japan Certification Practice Statement version 1.4 (Effective Date : September 5, 2022) • Cybertrust Japan SureServer EV Certificate Policy v2.0 (Effective Date : June 23, 2022) • Cybertrust Japan SureServer EV Certificate Policy v2.1 (Effective Date : September 5, 2022)	https://www.cybertrust.ne.jp/ssl/repository/
Cybertrust Japan SureMail CA G4	• Cybertrust Japan Certification Practice Statement version 1.3 (Effective Date : May 13, 2022) • Cybertrust Japan Certification Practice Statement version 1.4 (Effective Date : September 5, 2022) • Cybertrust Japan SureMail Certificate Policy v2.0 (Effective Date : June 23, 2022) • Cybertrust Japan SureMail Certificate Policy v2.1 (Effective Date : September 5, 2022)	https://www.cybertrust.ne.jp/ssl/repository/



(Translation)

APPENDIX C

#	Disclosure	Publicly Disclosed Link
1	SECOM: Failed an annual update of Cybertrust Japan (CTJ) CPS	https://bugzilla.mozilla.org/show_bug.cgi?id=1769222



(Translation)

CTJ MANAGEMENT'S ASSERTION

February 16, 2023

Masaru Sakamoto
Manager
Public Certificate Management Department
PKI Technology Business Unit
Cybertrust Japan Co., Ltd.

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

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate validation
- Subscriber key generation

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

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to CTJ's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.



(Translation)

CTJ management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in CTJ Management's opinion, in providing its Certification Authority (CA) services at Hokkaido and Tokyo, Japan, throughout the period December 11, 2021 to December 10, 2022, CTJ has:

1. disclosed its business, key lifecycle management, certificate lifecycle management, and CA environmental control practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#) on CTJ's website
2. maintained effective controls to provide reasonable assurance that:
 - The Certification Practice Statements of CTJ are consistent with its Certificate Policies; and
 - CTJ provides its services in accordance with its Certificate Policies and Certification Practice Statements
3. maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
 - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles; and
 - subscriber information is properly authenticated (for the registration activities performed by CTJ)
4. maintained effective controls to provide reasonable assurance that:
 - logical and physical access to CA systems and data is restricted to authorized individuals;
 - the continuity of key and certificate management operations is maintained; and
 - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

in accordance with the [WebTrust Principles and Criteria for Certification Authorities v2.2.2](#), including the following:



(Translation)

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

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

CA Key Lifecycle 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 Lifecycle Management

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services



(Translation)

Certificate Lifecycle Management Controls

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

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

CTJ does not escrow its CA keys, and does not provide certificate suspension services, and does not provide subordinate CA certificate services. Accordingly, our assertion does 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

OV SSL Issuing CAs
CA#1: Cybertrust Japan SureServer CA G4
EV SSL Issuing CAs
CA#2: Cybertrust Japan SureServer EV CA G3
Secure Email (S/MIME) CAs
CA#3: Cybertrust Japan SureMail CA G4



(Translation)

CA Identifying Information for in Scope CAs

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint
1	1	CN = Cybertrust Japan SureServer CA G4 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b1630cecb4 3c2e	rsaEncr yption	2048bit	sha256With RSAEncrypt ion	September 27, 2019 10:54:23	May 29, 2029 14:00:39	62a7d2dade85b692f185 bcf6e8959d75a0fa4e1f	(SHA1) F695C5B4037AE8EAE51EA943A4F54D750E0DA609 (SHA256) 0207056D172C80BDFB6DC45BE9E5808846078D1E6EEF1B6ED70259AB332A64C1
2	1	CN = Cybertrust Japan SureServer EV CA G3 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b16488bce6 95fc	rsaEncr yption	2048bit	sha256With RSAEncrypt ion	September 27, 2019 11:04:20	May 29, 2029 14:00:39	826c755d53f54569bc2 52da44c89e6b2b74187 a3	(SHA1) A88503F53FA02D0B2C4D1437BCD1BD6AA111539D (SHA256) FEC9ADA7AA49D4FEA9EFF123542095A880C004FD6933F9364B02B2E3574EA38
3	1	CN = Cybertrust Japan SureMail CA G4 O = Cybertrust Japan Co., Ltd. C = JP	OU = Security Communication RootCA2 O = SECOM Trust Systems CO.,LTD. C = JP	22b9b1655c8e69 915b	rsaEncr yption	2048bit	sha256With RSAEncrypt ion	September 27, 2019 11:14:09	May 29, 2029 14:00:39	fcc6dafec7add55ace48d ecffde828c5a3ba8f11	(SHA1) BACAF90E4A81408FF7B1245B7E973213C83488C (SHA256) 73609E68EEAA8B52808CB503FB8EA64EDD38923DA9C55AE788051AB416DD759 E

APPENDIX B

CA	CP/CPS	Website
Cybertrust Japan SureServer CA G4	• Cybertrust Japan Certification Practice Statement version 1.3 (Effective Date : May 13, 2022) • Cybertrust Japan Certification Practice Statement version 1.4 (Effective Date : September 5, 2022) • Cybertrust Japan SureServer Certificate Policy v1.9 (Effective Date : June 23, 2022) • Cybertrust Japan SureServer Certificate Policy v2.0 (Effective Date : September 5, 2022)	https://www.cybertrust.ne.jp/ss/repository/
Cybertrust Japan SureServer EV CA G3	• Cybertrust Japan Certification Practice Statement version 1.3 (Effective Date : May 13, 2022) • Cybertrust Japan Certification Practice Statement version 1.4 (Effective Date : September 5, 2022) • Cybertrust Japan SureServer EV Certificate Policy v2.0 (Effective Date : June 23, 2022) • Cybertrust Japan SureServer EV Certificate Policy v2.1 (Effective Date : September 5, 2022)	https://www.cybertrust.ne.jp/ss/repository/
Cybertrust Japan SureMail CA G4	• Cybertrust Japan Certification Practice Statement version 1.3 (Effective Date : May 13, 2022) • Cybertrust Japan Certification Practice Statement version 1.4 (Effective Date : September 5, 2022) • Cybertrust Japan SureMail Certificate Policy v2.0 (Effective Date : June 23, 2022) • Cybertrust Japan SureMail Certificate Policy v2.1 (Effective Date : September 5, 2022)	https://www.cybertrust.ne.jp/ss/repository/



(Translation)

APPENDIX C

#	Disclosure	Publicly Disclosed Link
1	SECOM: Failed an annual update of Cybertrust Japan (CTJ) CPS	https://bugzilla.mozilla.org/show_bug.cgi?id=1769222