



あずさ監査法人

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

2024 年 10 月 31 日

サイバートラスト株式会社
PKI事業本部
執行役員本部長
田村 光義 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-S/MIME 保証規準 v1.0.1 \(the WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.0.1\)](#) に準拠して、2023 年 8 月 24 日から 2024 年 8 月 23 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[付録 A](#) に記載された 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 ブラウザフォーラムガイドラインに準拠して S/MIME 証明書を提供するためのコミットメントを含む S/MIME 証明書ライフサイクル管理のビジネス実務を、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、当該開示された実務に従ってサービスを提供していた。
- 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ための有効な内部統制を維持していた。
 - 管理する鍵と S/MIME 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。
 - S/MIME 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）適切に認証されていたこと。

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。

付録 A の「対象 CA の識別情報」に記載されている CA#4 は 2024 年 8 月 20 日に廃止された。また、2024 年 8 月 20 日から 2024 年 8 月 23 日までの期間において、証明書を発行しておらず、失効情報を提供するためにのみオンラインで維持されていた。

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-S/MIME 保証規準 v1.0.1](#) 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、守秘義務及び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、国際品質マネジメント基準第 1 号「財務諸表の監査若しくはレビュー又はその他の保証若しくは関連サービス業務を行う事務所の品質マネジメント」を適用しており、これは、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する方針と手続を含む、品質マネジメントシステムをデザイン、適用及び運用することを要求している。

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 S/MIME 証明書の発行、更新、失効にわたる関連する内部統制を含む S/MIME 証明書ライフサイクル管理のビジネス実務を理解すること、(2) サイバートラスト株式会社が開示した S/MIME 証明書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-S/MIME 保証規準 v1.0.1](#)に基づいて、2023 年 8 月 24 日から 2024 年 8 月 23 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-S/MIME 保証規準 v1.0.1](#)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-S/MIME 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。

以上



付録 A

対象 CA

Root CAs
CA#1: SecureSign Root CA16
CA#2: SecureSign Root CA15
Secure Email (S/MIME) CAs
CA#3: Cybertrust Japan SureMail CA G9
CA#4: Cybertrust Japan SureMail CA G8



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	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	ポリシーオブジェクト識別子
1	1	CN=SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	547B8DAB53110077A81803AEA12B1129AB42E045	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2024年7月30日 16:08:11	2044年7月29日 15:55:40	186E34B6DB99556448A58649B89E4B93F70E2B0F	(SHA1) D17917EC45E2A0CAD774513010A4C65CAAB33C49 (SHA256) 4C1CCD24F17E950FC18536B33CAF E32293CFC33E8467B41E1C693055D7F513BF	—
2	1	CN=SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D849A7BE690C8A88EDF070F9DDB73E87	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年4月8日 17:32:56	2045年4月8日 17:32:56	EB41C8AEFCD59E5148F5BD8BF4872093412BD3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179E5314A9C291442805E1FB1D8FB6B8886C3A	—
3	1	CN=Cybertrust Japan SureMail CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN=SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	143D38AEE7BEA7D577D96AA346B5581E0A651915	rsaEncryption	4096Bits	sha256WithRSAEncryption	2024年7月30日 17:11:33	2034年7月29日 17:10:15	83486A284E149A7D1AC5F2EA05D43E72BE600EA7	(SHA1) D3FA22289481BA615E9A688CEE92A2F103D8114E (SHA256) DF722167C475B964E39C2536D87E694A160F65C43F62DAC8764EA051D5783AAA	2.23.140.1.5.2.3
4	1	CN = Cybertrust Japan SureMail CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1FA4C422EADA4D67BE7EC31B75024A2DB55C0015	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2023年8月21日 12:08:29	2030年6月22日 18:50:52	9FBFE09859F1DBD24E84B093408BA9D5A141026F	(SHA1) 113F753E0D47D761623FC92FC561931D335746B4 (SHA256) 8FBD048775F6F4C486CF4960A7BB8B807225E37C74935E5B99CBA9E41383FECA	2.23.140.1.5.2.1



付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 ～ CA#4	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.18	2023/8/24
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.19	2024/3/15
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.20	2024/4/15
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.21	2024/7/30
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.22	2024/8/20

運用規程

CA	CPS 名	Version	日付
CA#1 ～ CA#4	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.07	2023/8/24
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.08	2024/3/15
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.09	2024/4/15
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.10	2024/7/30
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.11	2024/8/20

経営者の記述書

2024 年 10 月 31 日

サイバートラスト株式会社
PKI事業本部
執行役員本部長



田村 光義

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、S/MIME 認証局サービス（以下「CA サービス」という。）を提供している。

当社の経営者は、当社の Web サイトで公開している S/MIME CA ビジネス実務の開示、S/MIME 鍵ライフサイクル管理の内部統制、S/MIME 証明書ライフサイクル管理の内部統制を含む当社の S/MIME 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場合がある。

当社の経営者は、当社の CA サービス（北海道及び東京）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、当社は、[認証局のための WebTrust-S/MIME 保証規](#)
[準 v1.0.1 \(the WebTrust Principles and Criteria for Certification Authorities - S/MIME](#)
[Certificates v1.0.1\)](#) に準拠して、2023 年 8 月 24 日から 2024 年 8 月 23 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. CA ブラウザフォーラムガイドラインに準拠して S/MIME 証明書を提供するためのコミットメントを含む S/MIME 証明書ライフサイクル管理のビジネス実務を、当社のウェブサイト[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、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. 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。
 - ・ 管理する鍵と S/MIME 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。
 - ・ S/MIME 加入者情報は、（当社が行う登録業務のため）適切に認証されていたこと。

3. 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。

付録 A の「対象 CA の識別情報」に記載されている CA#4 は 2024 年 8 月 20 日に廃止された。また、2024 年 8 月 20 日から 2024 年 8 月 23 日までの期間において、証明書を発行しておらず、失効情報を提供するためにのみオンラインで維持されていた。

付録 A

対象CA

Root CAs
CA#1: SecureSign Root CA16
CA#2: SecureSign Root CA15
Secure Email (S/MIME) CAs
CA#3: Cybertrust Japan SureMail CA G9
CA#4: Cybertrust Japan SureMail CA G8

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	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	署名	ポリシーオブジェクト識別子
1	1	CN=SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	547B8DAB53110077A81803AEA12B1129AB42E045	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2024年7月30日16:08:11	2044年7月29日15:55:40	186E34B6DB99556448A58649B89E4B93F70E2B0F	(SHA1) D17917EC45E2A0CAD774513010A4C65CAAB33C49 (SHA256) 4C1CCD24F17E950FC18536B33CAF E32293CFC33E8467B41E1C693055D7F513BF	—
2	1	CN=SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D849A7BE690C8A88EDF070F9DDB73E87	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年4月8日17:32:56	2045年4月8日17:32:56	EB41C8AEFCD59E5148F5BD8BF4872093412BD3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179E5314A9C291442805E1FB1D8FB6B8886C3A	—
3	1	CN=Cybertrust Japan SureMail CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN=SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	143D38AEE7BEA7D577D96AA346B5581E0A651915	rsaEncryption	4096Bits	sha256WithRSAEncryption	2024年7月30日17:11:33	2034年7月29日17:10:15	83486A284E149A7D1AC5F2EA05D43E72BE600EA7	(SHA1) D3FA22289481BA615E9A688CEE92A2F103D8114E (SHA256) DF722167C475B964E39C2536D87E694A160F65C43F62DAC8764EA051D5783AAA	2.23.140.1.5.2.3
4	1	CN = Cybertrust Japan SureMail CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1FA4C422EADA4D67BE7EC31B75024A2DB55C0015	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2023年8月21日12:08:29	2030年6月22日18:50:52	9FBFE09859F1DBD24E84B093408BA9D5A141026F	(SHA1) 113F753E0D47D761623FC92FC561931D335746B4 (SHA256) 8FBD048775F6F4C486CF4960A7BB8B807225E37C74935E5B99CBA9E41383FECA	2.23.140.1.5.2.1

付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#1 ～ CA#4	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.18	2023/8/24
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.19	2024/3/15
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.20	2024/4/15
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.21	2024/7/30
	Cybertrust Japan Certificate Policy (サイバートラスト証明書ポリシー)	1.22	2024/8/20

運用規程

CA	CPS 名	Version	日付
CA#1 ～ CA#4	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.07	2023/8/24
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.08	2024/3/15
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.09	2024/4/15
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.10	2024/7/30
	Cybertrust Japan Certification Practice Statement (サイバートラスト認証局運用規程)	1.11	2024/8/20

以上



あずさ監査法人

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

October 31, 2024

To Mr. Mitsuyoshi Tamura
Corporate Officer General Manager
PKI 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 Co., Ltd. ("CTJ") that for its Certification Authority (CA) operations at Hokkaido and Tokyo, Japan, throughout the period August 24, 2023 to August 23, 2024 for its CAs as enumerated in [Appendix A](#), CTJ has:

1. disclosed its S/MIME certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#), including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the CTJ website, and provided such services in accordance with its disclosed practices
2. maintained effective controls to provide reasonable assurance that:
 - the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
 - S/MIME subscriber information is properly authenticated (for the registration activities performed by CTJ)
3. 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 - S/MIME Certificates v1.0.1](#).

Appendix A, CA#4 were revoked on August 20, 2024. That CA did not issue certificates throughout the period August 20, 2024 to August 23, 2024 and was maintained online to provide revocation status information only.

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 - S/MIME Certificates v1.0.1](#).

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 Management 1, Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements, which requires the firm to design, implement and operate a system of quality management including 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 S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates;
- (2) selectively testing transactions executed in accordance with disclosed S/MIME 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 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.



(Translation)

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 August 24, 2023 to August 23, 2024, 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 - S/MIME Certificates v1.0.1](#).

This report does not include any representation as to the quality of CTJ's services beyond those covered by the [WebTrust Principles and Criteria for Certification Authorities - S/MIME Certificates v1.0.1](#), nor the suitability of any of CTJ's services for any customer's intended purpose.

Use of the WebTrust seal

CTJ's use of the WebTrust for Certification Authorities – S/MIME Certificates 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.

(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

Root CAs
CA#1: SecureSign Root CA16
CA#2: SecureSign Root CA15
Secure Email (S/MIME) CAs
CA#3: Cybertrust Japan SureMail CA G9
CA#4: Cybertrust Japan SureMail CA G8



(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	Policy identifiers
1	1	CN = SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	547B8DAB5311 0077A81803AE A12B1129AB42 E045	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	July 30, 2024 16:08:11	July 29, 2044 15:55:40	186E34B6DB99556448A 58649B89E4B93F70E2B 0F	(SHA1) D17917EC45E2A0CAD774513010A4 C65CAAB33C49 (SHA256) 4C1CCD24F17E950FC18536B33CAF E32293CFC33E8467B41E1C693055D 7F513BF	—
2	1	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D849 A7BE690C8A88 EDF070F9DDB 73E87	id- ecPublic Key	384Bits	ecdsa-with- SHA384	April 8, 2020 17:32:56	April 8, 2045 17:32:56	EB41C8AEFCD59E5148 F5BD8BF4872093412BD 3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7 EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179 E5314A9C291442805E1FB1D8FB6B 8886C3A	—
3	1	CN=Cybertrust Japan SureMail CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN=SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	143D38AEE7BE A7D577D96AA 346B5581E0A65 1915	rsaEncr yption	4096Bit s	sha256With RSAEncrypt ion	July 30, 2024 17:11:33	July 29, 2034 17:10:15	83486A284E149A7D1A C5F2EA05D43E72BE60 0EA7	(SHA1) D3FA22289481BA615E9A688CEE92 A2F103D8114E (SHA256) DF722167C475B964E39C2536D87E6 94A160F65C43F62DAC8764EA051D 5783AAA	2.23.140.1.5.2.3
4	1	CN = Cybertrust Japan SureMail CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1FA4C422EAD A4D67BE7EC31 B75024A2DB55 C0015	id- ecPublic Key	384Bits	ecdsa-with- SHA384	August 21, 2023 12:08:29	June 22, 2030 18:50:52	9FBFE09859F1DBD24E 84B093408BA9D5A1410 26F	(SHA1) 113F753E0D47D761623FC92FC5619 31D335746B4 (SHA256) 8FBD048775F6F4C486CF4960A7BB 8B807225E37C74935E5B99CBA9E4 1383FECA	2.23.140.1.5.2.1



(Translation)

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 — CA#4	Cybertrust Japan Certificate Policy	1.18	August 24, 2023
	Cybertrust Japan Certificate Policy	1.19	March 15, 2024
	Cybertrust Japan Certificate Policy	1.20	April 15, 2024
	Cybertrust Japan Certificate Policy	1.21	July 30, 2024
	Cybertrust Japan Certificate Policy	1.22	August 20, 2024

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 — CA#4	Cybertrust Japan Certification Practice Statement	1.07	August 24, 2023
	Cybertrust Japan Certification Practice Statement	1.08	March 15, 2024
	Cybertrust Japan Certification Practice Statement	1.09	April 15, 2024
	Cybertrust Japan Certification Practice Statement	1.10	July 30, 2024
	Cybertrust Japan Certification Practice Statement	1.11	August 20, 2024

CTJ MANAGEMENT'S ASSERTION

October 31, 2024

Mitsuyoshi Tamura
Corporate Officer General Manager
PKI Business Unit
Cybertrust Japan Co., Ltd.

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

The management of CTJ is responsible for establishing and maintaining effective controls over its S/MIME CA operations, including its S/MIME CA business practices disclosure on its website, S/MIME key lifecycle management controls, and S/MIME 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.

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 S/MIME CA services at Hokkaido and Tokyo, Japan, throughout the period August 24, 2023 to August 23, 2024, CTJ has:

1. disclosed its S/MIME certificate lifecycle management business practices in its Certification Practice Statements and Certificate Policies enumerated in [Appendix B](#), including its commitment to provide S/MIME certificates in conformity with the CA/Browser Forum Requirements on the CTJ's website, and provided such services in accordance with its disclosed practices
2. maintained effective controls to provide reasonable assurance that:

- the integrity of keys and S/MIME certificates it manages is established and protected throughout their lifecycles; and
- S/MIME subscriber information is properly authenticated (for the registration activities performed by CTJ)

3. 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 - S/MIME Certificates v1.0.1.](#)

Appendix A, CA#4 was revoked on August 20, 2024. That CA did not issue certificates throughout the period August 20, 2024 to August 23, 2024 and was maintained online to provide revocation status information only.

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

APPENDIX A

List of CAs in Scope

Root CAs
CA#1: SecureSign Root CA16
CA#2: SecureSign Root CA15
Secure Email (S/MIME) CAs
CA#3: Cybertrust Japan SureMail CA G9
CA#4: Cybertrust Japan SureMail CA G8

(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	Policy identifiers
1	1	CN = SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	547B8DAB53110077A81803AEA12B1129AB42E045	rsaEncryption	4096Bits	Sha384WithRSAEncryption	July 30, 2024 16:08:11	July 29, 2044 15:55:40	186E34B6DB99556448A58649B89E4B93F70E2B0F	(SHA1) D17917EC45E2A0CAD774513010A4C65CAAB33C49 (SHA256) 4C1CCD24F17E950FC18536B33CAF E32293CFC33E8467B41E1C693055D7F513BF	—
2	1	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1615C7C3D849A7BE690C8A88EDF070F9DDB73E87	id-ecPublicKey	384Bits	ecdsa-with-SHA384	April 8, 2020 17:32:56	April 8, 2045 17:32:56	EB41C8AEFCD59E5148F5BD8BF4872093412BD3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179E5314A9C291442805E1FB1D8FB6B8886C3A	—
3	1	CN=Cybertrust Japan SureMail CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN=SecureSign Root CA16 O = Cybertrust Japan Co., Ltd. C = JP	143D38AEE7BEA7D577D96AA346B5581E0A651915	rsaEncryption	4096Bits	sha256WithRSAEncryption	July 30, 2024 17:11:33	July 29, 2034 17:10:15	83486A284E149A7D1AC5F2EA05D43E72BE600EA7	(SHA1) D3FA22289481BA615E9A688CEE92A2F103D8114E (SHA256) DF722167C475B964E39C2536D87E694A160F65C43F62DAC8764EA051D5783AAA	2.23.140.1.5.2.3
4	1	CN = Cybertrust Japan SureMail CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	1FA4C422EADA4D67BE7EC31B75024A2DB55C0015	id-ecPublicKey	384Bits	ecdsa-with-SHA384	August 21, 2023 12:08:29	June 22, 2030 18:50:52	9FBFE09859F1DBD24E84B093408BA9D5A141026F	(SHA1) 113F753E0D47D761623FC92FC561931D335746B4 (SHA256) 8FBD048775F6F4C486CF4960A7BB8B807225E37C74935E5B99CBA9E41383FECA	2.23.140.1.5.2.1

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#1 — CA#4	Cybertrust Japan Certificate Policy	1.18	August 24, 2023
	Cybertrust Japan Certificate Policy	1.19	March 15, 2024
	Cybertrust Japan Certificate Policy	1.20	April 15, 2024
	Cybertrust Japan Certificate Policy	1.21	July 30, 2024
	Cybertrust Japan Certificate Policy	1.22	August 20, 2024

Certification Practice Statement

CA	Policy Name	Version	Date
CA#1 — CA#4	Cybertrust Japan Certification Practice Statement	1.07	August 24, 2023
	Cybertrust Japan Certification Practice Statement	1.08	March 15, 2024
	Cybertrust Japan Certification Practice Statement	1.09	April 15, 2024
	Cybertrust Japan Certification Practice Statement	1.10	July 30, 2024
	Cybertrust Japan Certification Practice Statement	1.11	August 20, 2024