



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 の規準 v2.2.2 \(the WebTrust Principles and Criteria for Certification Authorities v2.2.2\)](#) に準拠して、2023 年 10 月 16 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 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、鍵ライフサイクル管理と証明書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。

付録 A の「対象 CA の識別情報」に記載されている CA#12-CA#15 及び CA#17-CA#19 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。

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。

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、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鍵と証明書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、2023 年 10 月 16 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 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。

以上

付録 A

対象 CA

Root CAs
CA#1: SecureSign Root CA16
CA#2: SecureSign Root CA15
CA#3: SecureSign Root CA14
CA#4: SecureSign Root CA12
CA#5: SecureSign RootCA11
OV SSL Issuing CAs
CA#6: Cybertrust Japan SureServer CA G8
CA#7: Cybertrust Japan SureServer CA G7
CA#8: JCSI TLSSign Public CA
EV SSL Issuing CAs
CA#9: Cybertrust Japan SureServer EV CA G9
CA#10: Cybertrust Japan SureServer EV CA G8
CA#11: Cybertrust Japan SureServer EV CA G7
Non-EV Code Signing Issuing CAs
CA#12: Cybertrust Japan SureCode CA G4
CA#13: Cybertrust Japan SureCode CA G3
EV Code Signing Issuing CAs
CA#14: Cybertrust Japan SureCode EV CA G4
CA#15: Cybertrust Japan SureCode EV CA G3
Secure Email (S/MIME) CAs
CA#16: Cybertrust Japan SureMail CA G9
CA#17: Cybertrust Japan SureMail CA G8
Timestamp CAs
CA#18: Cybertrust Japan SureTime CA G4
CA#19: Cybertrust Japan SureTime CA G3



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 = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C204EE8D72977C85027A25A27DD2DF2CB	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年4月8日16:06:19	2045年4月8日16:06:19	0693A30A5E286937AA611DEBEBFC2D6F23E4F3A0	(SHA1) DD50C0F779B3642E74A2B89D9FD340DDBBF0F24F (SHA256) 4B009C1034494F9AB56BBA3BA1D62731FC4D20D8955ADCEC10A925607261E338	—
4	1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AFEC251B4ED5397E6E682C32B1C9016	rsaEncryption	2048Bits	sha256WithRSAEncryption	2020年4月8日14:36:46	2040年4月8日14:36:46	5734F374CF044BD525E6F140B62C4CD92DE9A0AD	(SHA1) 7A221E3DDE1B06AC9EC84770168E3CE5F76B06F4 (SHA256) 3F034BB5704D44B2D08545A02057DE93EBF3905FCE721ACBC730C06DDAEE904E	—



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
5	1	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	01	rsaEncryption	2048Bits	sha1WithRSAEncryption	2009年4月8日 13:56:47	2029年4月8日 13:56:47	5BF84D4FB2A586D43AD2F1639AA0BE09F657B7DE	(SHA1) 3BC49F48F8F373A09C1EBDF85BB1C365C7D811B3 (SHA256) BF0FEEFB9E3A581AD5F9E9DB7589985743D261085C4D314F6F5D7259AA421612	—
6	1	CN = Cybertrust Japan SureServer CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	4D8247384ADF541F88340F4928553224B6C48FE2	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日 18:45:15	2030年6月22日 18:45:15	3DD29719E5391699EE6BB01B7AC6F3FACAF5F703	(SHA1) A07043D2965389E4EF90EBEAEA319996A9877819 (SHA256) 93D931D5F95411998705B148532F4E16FBCF00F3318DFF9B6A0765ED749C8FD0	2.23.140.1.2.2
7	1	CN = Cybertrust Japan SureServer CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	167DDD4E7ABD348B6A105BC9CA24ACE745F2B6CB	rsaEncryption	2048Bits	sha256WithRSAEncryption	2020年6月22日 16:42:05	2030年6月22日 16:42:05	8E3C286393A4E4850F5489DD69B23C52674AB5A4	(SHA1) F9DDEC1E1FCF62CE4FAD04EDC44109A9504F4784 (SHA256) A2E2C3D73CFF96451325712E212FA15C40FD4F2C3F143C1BB619385365304C02	2.23.140.1.2.2
8	1	CN = JCSI TLSSign Public CA O = Cybertrust Japan Co.,Ltd. C = JP	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	7540ACF59D071D7A7ECAF2FB965A7D11415CD53	rsaEncryption	2048Bits	sha256WithRSAEncryption	2018年10月11日 10:36:33	2029年4月8日 13:56:47	D3342FDDF84C99DE843F051DB9D9F440D9C08BB1	(SHA1) 5E2ED0EDD013B5EF5EB2203FAAB6F876452FCEC2 (SHA256) 9253BFB668F3E743A525E48B5F750A8A66035F806297C25F8134DC8AC9635BD8	2.23.140.1.2.2



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
9	1	CN = Cybertrust Japan SureServer EV CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	756AA35ABA8847DD5103C33A37B168FA13A4F715	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年6月22日 17:50:22	2030年6月22日 17:50:22	EDB8FA2F3D7D25BEE354B165CE54A8833B92F0C7	(SHA1) EDEC2820E5CD08CB234D3B2417FE0DCDB51D238B (SHA256) 93397E182492A7E7C582BADFE04348E6FA985CBA19AFDE16FD740FF03857367C	2.23.140.1.1
10	1	CN = Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	7CA3593373BD43AA87416AB0439DAC5D0361D803	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日 18:39:21	2030年6月22日 18:39:21	AEE4FDC16E22F8DFB71383F8E2D143B696B93AC8	(SHA1) FBF4B414FBA71E4F10AA57CF8C47697489D59ED1 (SHA256) 70C4002E0DF2FF51E691654903BE742D09D5A74A84B15B68FBCDA320FBF3DC6B	2.23.140.1.1
11	1	CN = Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	2C77F85B12969E757EAC8921C7155089AE35F418	rsaEncryption	2048Bits	sha256WithRSAEncryption	2020年6月22日 16:34:38	2030年6月22日 16:34:38	7483319BF875CD0DCF8E84E6D28E9AA6794C2AA6	(SHA1) 99865D3428D04DEF0D3FA29DEFB D5905A0B040A7 (SHA256) 76648FBC40CC4164CEA02422A09EB4EAD29C67F5E7DD74F691B7FA08043472C5	2.23.140.1.1
12	1	CN = Cybertrust Japan SureCode CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	2141B3AAF2EFD0F09FC1CBE2C6A8AB4E966DA06F	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日 19:02:43	2036年6月22日 19:02:43	A56FC7383B5B24E8D03FF1E60804858BCDCA8CCF	(SHA1) 7F466C2F01734A4034024DBD9E460515D3B80C76 (SHA256) 42A7E8F7E06F2FC1CE417B26AC6F724E7BCC520A3B64ED506C7AA0B6DA25D63E	2.23.140.1.4.1



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
13	1	CN = Cybertrust Japan SureCode CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	605809FFFD7A D23CC7793CFC 3181DE152DFE 1C19	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年6月22日 17:37:47	2036年6月22日 17:37:47	47F78166565D8C5DEF9 DF481260F8557884168A 8	(SHA1) A50C5F28193A2F2971517BE5DD3C 2212AAEE5376 (SHA256) A2383AF3FDE129CCFB7865D057D 40A1A4BDA70E1E45C53E8BB5868 1AF62E1B4B	2.23.140.1.4.1
14	1	CN = Cybertrust Japan SureCode EV CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	3067E8FBFB22 01DE04917E3A E9701115A580F 9D1	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日 18:56:51	2036年6月22日 18:56:51	2FE1DE06415D92B9F78 BB34C20C7043726DF72 EB	(SHA1) 542AA69A5F38DFD4CD9C41B0304 8B7BCE10124A7 (SHA256) AEEDAB7F871504EE07CEB3ED93A F034394548B1E655F7C759B9646AB 78F0CEBB	2.23.140.1.3
15	1	CN = Cybertrust Japan SureCode EV CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	401C0824BBCE A63303FB626F7 D613BFF01241 FF6	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年6月22日 17:31:36	2036年6月22日 17:31:36	3D5C4FB323D4C83BD0 1CC593D5577BB849906 AC4	(SHA1) 6261D96B51BFF7807F38B4A52E415 5D89EFEF71E (SHA256) 87CC9D3EDF3F8517D922944AA114 A5576AB4FD8DF09E35D10FF314C8 EA172619	2.23.140.1.3
16	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	rsaEncryption	4096Bits	sha256WithRSAEncryption	2024年7月30日 17:11:33	2034年7月29日 17:10:15	83486A284E149A7D1A C5F2EA05D43E72BE60 0EA7	(SHA1) D3FA22289481BA615E9A688CEE92 A2F103D8114E (SHA256) DF722167C475B964E39C2536D87E6 94A160F65C43F62DAC8764EA051D 5783AAA	2.23.140.1.5.2.3



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
17	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
18	1	CN = Cybertrust Japan SureTime CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	3E745100E3A15C5D0288B4475F408E516A8337B5	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2021年9月9日 11:41:04	2037年9月9日 11:41:04	160378BECDE5F52B490829E4D21143A6CAD6C489	(SHA1) F95B7E1CA40A890941A5039DAD81463D92B3A4B7 (SHA256) 5022E703CD525D1D45F8CAB522C00B8D371891C9995D28F36E12906B8D1E9EBE	2.23.140.1.4.2
19	1	CN = Cybertrust Japan SureTime CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	47C05BCA232CA403ABA01603F0584B6B150ACFFB	rsaEncryption	4096Bits	Sha384WithRSAAEncryption	2021年9月9日 11:28:53	2037年9月9日 11:28:53	DDB89D9132793721A466BB0CDB0C84ECAC1BA029	(SHA1) 3C050F28F197CE9BBE16EE6551C9530D838D9AD5 (SHA256) F8D976C1190F85B54EBD88B45986FCF475D1A58F8CFD1D70B0E40A6346BBA4A6	2.23.140.1.4.2



付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#5, CA#8	JCSI Certificate Policy (JCSI 証明書ポリシー)	3.5	2023/9/13
	JCSI Certificate Policy (JCSI 証明書ポリシー)	3.6	2024/3/15
	JCSI Certificate Policy (JCSI 証明書ポリシー)	3.7	2024/7/30
CA#1 ～ CA#4, CA#6, CA#7, CA#9 ～ CA#19	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#19	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、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
- ・ 下位 CA の相互認証

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、証明書ライフサイクル管理の内部統制、及び下位 CA の証明書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場合がある。

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、2023年10月16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. 当社のCAが実施するビジネス、鍵ライフサイクル管理と証明書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ための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ための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 ビジネス実務の管理

- ・ 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
- ・ IC カードライフサイクル管理



- ・ 加入者鍵管理の要件

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

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

当社は、CA の鍵を寄託せず、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 の「対象 CA の識別情報」に記載されている CA#12-CA#15 及び CA#17-CA#19 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
CA#3: SecureSign Root CA14
CA#4: SecureSign Root CA12
CA#5: SecureSign RootCA11
OV SSL Issuing CAs
CA#6: Cybertrust Japan SureServer CA G8
CA#7: Cybertrust Japan SureServer CA G7
CA#8: JCSI TLSSign Public CA
EV SSL Issuing CAs
CA#9: Cybertrust Japan SureServer EV CA G9
CA#10: Cybertrust Japan SureServer EV CA G8
CA#11: Cybertrust Japan SureServer EV CA G7
Non-EV Code Signing Issuing CAs
CA#12: Cybertrust Japan SureCode CA G4
CA#13: Cybertrust Japan SureCode CA G3
EV Code Signing Issuing CAs
CA#14: Cybertrust Japan SureCode EV CA G4
CA#15: Cybertrust Japan SureCode EV CA G3
Secure Email (S/MIME) CAs
CA#16: Cybertrust Japan SureMail CA G9
CA#17: Cybertrust Japan SureMail CA G8
Timestamp CAs
CA#18: Cybertrust Japan SureTime CA G4
CA#19: Cybertrust Japan SureTime CA G3



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 = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C204EE8D72977C85027A25A27DD2DF2CB	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年4月8日16:06:19	2045年4月8日16:06:19	0693A30A5E286937AA611DEBEBFC2D6F23E4F3A0	(SHA1) DD50C0F779B3642E74A2B89D9FD340DDBBF0F24F (SHA256) 4B009C1034494F9AB56BBA3BA1D62731FC4D20D8955ADCEC10A925607261E338	—
4	1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AFEC251B4ED5397E6E682C32B1C9016	rsaEncryption	2048Bits	sha256WithRSAEncryption	2020年4月8日14:36:46	2040年4月8日14:36:46	5734F374CF044BD525E6F140B62C4CD92DE9A0AD	(SHA1) 7A221E3DDE1B06AC9EC84770168E3CE5F76B06F4 (SHA256) 3F034BB5704D44B2D08545A02057DE93EBF3905FCE721ACBC730C06DDAEE904E	—



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
5	1	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	01	rsaEncryption	2048Bits	sha1WithRSAEncryption	2009年4月8日 13:56:47	2029年4月8日 13:56:47	5BF84D4FB2A586D43AD2F1639AA0BE09F657B7DE	(SHA1) 3BC49F48F8F373A09C1EBDF85BB1C365C7D811B3 (SHA256) BF0FEEFB9E3A581AD5F9E9DB7589985743D261085C4D314F6F5D7259AA421612	—
6	1	CN = Cybertrust Japan SureServer CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	4D8247384ADF541F88340F4928553224B6C48FE2	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日 18:45:15	2030年6月22日 18:45:15	3DD29719E5391699EE6BB01B7AC6F3FACAF5F703	(SHA1) A07043D2965389E4EF90EBEAEA319996A9877819 (SHA256) 93D931D5F95411998705B148532F4E16FBCF00F3318DFF9B6A0765ED749C8FD0	2.23.140.1.2.2
7	1	CN = Cybertrust Japan SureServer CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	167DDD4E7ABD348B6A105BC9CA24ACE745F2B6CB	rsaEncryption	2048Bits	sha256WithRSAEncryption	2020年6月22日 16:42:05	2030年6月22日 16:42:05	8E3C286393A4E4850F5489DD69B23C52674AB5A4	(SHA1) F9DDEC1E1FCF62CE4FAD04EDC44109A9504F4784 (SHA256) A2E2C3D73CFF96451325712E212FA15C40FD4F2C3F143C1BB619385365304C02	2.23.140.1.2.2
8	1	CN = JCSI TLSSign Public CA O = Cybertrust Japan Co.,Ltd. C = JP	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	7540ACF59D071D7A7ECAFC2FB965A7D11415CD53	rsaEncryption	2048Bits	sha256WithRSAEncryption	2018年10月11日 10:36:33	2029年4月8日 13:56:47	D3342FDDDF84C99DE843F051DB9D9F440D9C08BB1	(SHA1) 5E2ED0EDD013B5EF5EB2203FAAB6F876452FCEC2 (SHA256) 9253BFB668F3E743A525E48B5F750A8A66035F806297C25F8134DC8AC9635BD8	2.23.140.1.2.2



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
9	1	CN = Cybertrust Japan SureServer EV CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	756AA35ABA8847DD5103C33A37B168FA13A4F715	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年6月22日17:50:22	2030年6月22日17:50:22	EDB8FA2F3D7D25BEE354B165CE54A8833B92F0C7	(SHA1) EDEC2820E5CD08CB234D3B2417FE0DCDB51D238B (SHA256) 93397E182492A7E7C582BADFE04348E6FA985CBA19AFDE16FD740FF03857367C	2.23.140.1.1
10	1	CN = Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	7CA3593373BD43AA87416AB0439DAC5D0361D803	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日18:39:21	2030年6月22日18:39:21	AEE4FDC16E22F8DFB71383F8E2D143B696B93AC8	(SHA1) FBF4B414FBA71E4F10AA57CF8C47697489D59ED1 (SHA256) 70C4002E0DF2FF51E691654903BE742D09D5A74A84B15B68FBCDA320FBF3DC6B	2.23.140.1.1
11	1	CN = Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	2C77F85B12969E757EAC8921C7155089AE35F418	rsaEncryption	2048Bits	sha256WithRSAEncryption	2020年6月22日16:34:38	2030年6月22日16:34:38	7483319BF875CD0DCF8E84E6D28E9AA6794C2AA6	(SHA1) 99865D3428D04DEF0D3FA29DEFB D5905A0B040A7 (SHA256) 76648FBC40CC4164CEA02422A09EB4EAD29C67F5E7DD74F691B7FA08043472C5	2.23.140.1.1
12	1	CN = Cybertrust Japan SureCode CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	2141B3AAF2EFD0F9FC1CBE2C6A8AB4E966DA06F	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日19:02:43	2036年6月22日19:02:43	A56FC7383B5B24E8D03FF1E60804858BCDCA8CCF	(SHA1) 7F466C2F01734A4034024DBD9E460515D3B80C76 (SHA256) 42A7E8F7E06F2FC1CE417B26AC6F724E7BCC520A3B64ED506C7AA0B6DA25D63E	2.23.140.1.4.1



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
13	1	CN = Cybertrust Japan SureCode CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	605809FFFD7A D23CC7793CFC 3181DE152DFE 1C19	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年6月22日 17:37:47	2036年6月22日 17:37:47	47F78166565D8C5DEF9 DF481260F8557884168A 8	(SHA1) A50C5F28193A2F2971517BE5DD3C 2212AAEE5376 (SHA256) A2383AF3FDE129CCFB7865D057D 40A1A4BDA70E1E45C53E8BB5868 1AF62E1B4B	2.23.140.1.4.1
14	1	CN = Cybertrust Japan SureCode EV CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	3067E8FBFB22 01DE04917E3A E9701115A580F 9D1	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2020年6月22日 18:56:51	2036年6月22日 18:56:51	2FE1DE06415D92B9F78 BB34C20C7043726DF72 EB	(SHA1) 542AA69A5F38DFD4CD9C41B0304 8B7BCE10124A7 (SHA256) AEEDAB7F871504EE07CEB3ED93A F034394548B1E655F7C759B9646AB 78F0CEBB	2.23.140.1.3
15	1	CN = Cybertrust Japan SureCode EV CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	401C0824BBCE A63303FB626F7 D613BFF01241 FF6	rsaEncryption	4096Bits	Sha384WithRSAEncryption	2020年6月22日 17:31:36	2036年6月22日 17:31:36	3D5C4FB323D4C83BD0 1CC593D5577BB849906 AC4	(SHA1) 6261D96B51BFF7807F38B4A52E415 5D89EFEF71E (SHA256) 87CC9D3EDF3F8517D922944AA114 A5576AB4FD8DF09E35D10FF314C8 EA172619	2.23.140.1.3
16	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	rsaEncryption	4096Bits	sha256WithRSAEncryption	2024年7月30日 17:11:33	2034年7月29日 17:10:15	83486A284E149A7D1A C5F2EA05D43E72BE60 0EA7	(SHA1) D3FA22289481BA615E9A688CEE92 A2F103D8114E (SHA256) DF722167C475B964E39C2536D87E6 94A160F65C43F62DAC8764EA051D 5783AAA	2.23.140.1.5.2.3



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
17	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
18	1	CN = Cybertrust Japan SureTime CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	3E745100E3A15C5D0288B4475F408E516A8337B5	id-ecPublicKey	384Bits	ecdsa-with-SHA384	2021年9月9日 11:41:04	2037年9月9日 11:41:04	160378BECDE5F52B490829E4D21143A6CAD6C489	(SHA1) F95B7E1CA40A890941A5039DAD81463D92B3A4B7 (SHA256) 5022E703CD525D1D45F8CAB522C00B8D371891C9995D28F36E12906B8D1E9EBE	2.23.140.1.4.2
19	1	CN = Cybertrust Japan SureTime CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	47C05BCA232CA403ABA01603F0584B6B150ACFFB	rsaEncryption	4096Bits	Sha384WithRSAAEncryption	2021年9月9日 11:28:53	2037年9月9日 11:28:53	DDB89D9132793721A466BB0CDB0C84ECAC1BA029	(SHA1) 3C050F28F197CE9BBE16EE6551C9530D838D9AD5 (SHA256) F8D976C1190F85B54EBD88B45986FCF475D1A58F8CFD1D70B0E40A6346BBA4A6	2.23.140.1.4.2

付録 B

証明書ポリシー

CA	CP 名	Version	日付
CA#5, CA#8	JCSI Certificate Policy (JCSI 証明書ポリシー)	3.5	2023/9/13
	JCSI Certificate Policy (JCSI 証明書ポリシー)	3.6	2024/3/15
	JCSI Certificate Policy (JCSI 証明書ポリシー)	3.7	2024/7/30
CA#1 ～ CA#4, CA#6, CA#7, CA#9 ～ CA#19	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#19	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



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 Japan Co., Ltd.. ("CTJ") that for its Certification Authority (CA) operations at Hokkaido and Tokyo, Japan, throughout the period October 16, 2023 to August 23, 2024 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;
 - the Subscriber information is properly authenticated (for the registration activities performed by CTJ); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
4. maintained effective controls to provide reasonable assurance that:



(Translation)

- 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](#).

Appendix A, CA#12-CA#15 and CA#17-CA#19 were revoked on August 20, 2024. Those CAs did not issue certificates throughout the period August 20, 2024 to August 23, 2024 and was maintained online to provide revocation status information only.

CTJ does not escrow its CA keys, and does not provide certificate suspension 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 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 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;



(Translation)

- (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.

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 October 16, 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 v2.2.2](#).

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 v2.2.2](#), 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 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.)

APPENDIX A

List of CAs in Scope

Root CAs
CA#1: SecureSign Root CA16
CA#2: SecureSign Root CA15
CA#3: SecureSign Root CA14
CA#4: SecureSign Root CA12
CA#5: SecureSign RootCA11
OV SSL Issuing CAs
CA#6: Cybertrust Japan SureServer CA G8
CA#7: Cybertrust Japan SureServer CA G7
CA#8: JCSI TLSSign Public CA
EV SSL Issuing CAs
CA#9: Cybertrust Japan SureServer EV CA G9
CA#10: Cybertrust Japan SureServer EV CA G8
CA#11: Cybertrust Japan SureServer EV CA G7
Non-EV Code Signing Issuing CAs
CA#12: Cybertrust Japan SureCode CA G4
CA#13: Cybertrust Japan SureCode CA G3
EV Code Signing Issuing CAs
CA#14: Cybertrust Japan SureCode EV CA G4
CA#15: Cybertrust Japan SureCode EV CA G3
Secure Email (S/MIME) CAs
CA#16: Cybertrust Japan SureMail CA G9
CA#17: Cybertrust Japan SureMail CA G8
Timestamp CAs
CA#18: Cybertrust Japan SureTime CA G4
CA#19: Cybertrust Japan SureTime CA G3



(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 30, 2044 15:55:40	186E34B6 DB99556 448A5864 9B89E4B 93F70E2B 0F	(SHA1) D17917EC45E2A0CAD774513010A4C65CAAB33C49 (SHA256) 4C1CCD24F17E950FC18536B33CAFE32293CFC33E8467B41E1C6930 55D7F513BF	—
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	EB41C8A EFCDD59E 5148F5B D8BF487 2093412B D3F4	(SHA1) CBBAB3C8C15A5DF1F9736FCAD7EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179E5314A9C291442805E1FB1D8FB 6B8886C3A	—
3	1	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C204E E8D72977C8502 7A25A27DD2D F2CB	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	April 8, 2020 16:06:19	April 8, 2045 16:06:19	0693A30 A5E28693 7AA611D EBEBFC2 D6F23E4 F3A0	(SHA1) DD50C0F779B3642E74A2B89D9FD340DDBBF0F24F (SHA256) 4B009C1034494F9AB56BBA3BA1D62731FC4D20D8955ADCEC10A9 25607261E338	—
4	1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AFEC C251B4ED5397 E6E682C32B1C 9016	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	April 8, 2020 14:36:46	April 8, 2040 14:36:46	5734F374 CF044BD 525E6F14 0B62C4C D92DE9A 0AD	(SHA1) 7A221E3DDE1B06AC9EC84770168E3CE5F76B06F4 (SHA256) 3F034BB5704D44B2D08545A02057DE93EBF3905FCE721ACBC730C 06DDAEE904E	—



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
5	1	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	01	rsaEncr yption	2048Bit s	sha1WithRS AEncryption	April 8, 2009 13:56:47	April 8, 2029 13:56:47	5BF84D4 FB2A586 D43AD2F 1639AA0 BE09F657 B7DE	(SHA1) 3BC49F48F8F373A09C1EBDF85BB1C365C7D811B3 (SHA256) BF0FEEFB9E3A581AD5F9E9DB7589985743D261085C4D314F6F5D72 59AA421612	—
6	1	CN = Cybertrust Japan SureServer CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	4D8247384ADF 541F88340F492 8553224B6C48F E2	id-ecPublic Key	384Bits	ecdsa-with- SHA384	June 22, 2020 18:45:15	June 22, 2030 18:45:15	3DD2971 9E539169 9EE6BB0 1B7AC6F 3FACAF5 F703	(SHA1) A07043D2965389E4EF90EBEAEA319996A9877819 (SHA256) 93D931D5F95411998705B148532F4E16FBCF00F3318DFF9B6A0765E D749C8FD0	2.23.140.1.2.2
7	1	CN = Cybertrust Japan SureServer CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	167DDD4E7AB D348B6A105BC 9CA24ACE745F 2B6CB	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	June 22, 2020 16:42:05	June 22, 2030 16:42:05	8E3C2863 93A4E485 0F5489D D69B23C 52674AB 5A4	(SHA1) F9DDEC1E1FCF62CE4FAD04EDC44109A9504F4784 (SHA256) A2E2C3D73CFF96451325712E212FA15C40FD4F2C3F143C1BB61938 5365304C02	2.23.140.1.2.2
8	1	CN = JCSI TLSSign Public CA O = Cybertrust Japan Co.,Ltd. C = JP	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	7540ACF59D07 1D7A7ECAF2 FB965A7D1141 5CD53	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	October 11, 2018 10:36:33	April 8, 2029 13:56:47	D3342FD DF84C99 DE843F0 51DB9D9 F440D9C 08BB1	(SHA1) 5E2ED0EDD013B5EF5EB2203FAAB6F876452FCEC2 (SHA256) 9253BFB668F3E743A525E48B5F750A8A66035F806297C25F8134DC8 AC9635BD8	2.23.140.1.2.2



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
9	1	CN = Cybertrust Japan SureServer EV CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	756AA35ABA8 847DD5103C33 A37B168FA13A 4F715	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	June 22, 2020 17:50:22	June 22, 2030 17:50:22	EDB8FA2 F3D7D25 BEE354B 165CE54 A8833B9 2F0C7	(SHA1) EDEC2820E5CD08CB234D3B2417FE0DCDB51D238B (SHA256) 93397E182492A7E7C582BADFE04348E6FA985CBA19AFDE16FD740 FF03857367C	2.23.140.1.1
10	1	CN = Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	7CA3593373BD 43AA87416AB0 439DAC5D0361 D803	id- ecPublic Key	384Bits	ecdsa-with- SHA384	June 22, 2020 18:39:21	June 22, 2030 18:39:21	AEE4FD C16E22F8 DFB7138 3F8E2D1 43B696B9 3AC8	(SHA1) FBBF4B414FBA71E4F10AA57CF8C47697489D59ED1 (SHA256) 70C4002E0DF2FF51E691654903BE742D09D5A74A84B15B68FBCDA 320FBF3DC6B	2.23.140.1.1
11	1	CN = Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	2C77F85B12969 E757EAC8921C 7155089AE35F4 18	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	June 22, 2020 16:34:38	June 22, 2030 16:34:38	7483319B F875CD0 DCF8E84 E6D28E9 AA6794C 2AA6	(SHA1) 99865D3428D04DEF0D3FA29DEFBD5905A0B040A7 (SHA256) 76648FBC40CC4164CEA02422A09EB4EAD29C67F5E7DD74F691B7F A08043472C5	2.23.140.1.1
12	1	CN = Cybertrust Japan SureCode CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	2141B3AAF2EF DF0F9FC1CBE2 C6A8AB4E966 DA06F	id- ecPublic Key	384Bits	ecdsa-with- SHA384	June 22, 2020 19:02:43	June 22, 2036 19:02:43	A56FC73 83B5B24 E8D03FF 1E608048 58BCDC A8CCF	(SHA1) 7F466C2F01734A4034024DBD9E460515D3B80C76 (SHA256) 42A7E8F7E06F2FC1CE417B26AC6F724E7BCC520A3B64ED506C7A A0B6DA25D63E	2.23.140.1.4.1



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
13	1	CN = Cybertrust Japan SureCode CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	605809FFFD7A D23CC7793CFC 3181DE152DFE 1C19	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	June 22, 2020 17:37:47	June 22, 2036 17:37:47	47F78166 565D8C5 DEF9DF4 81260F85 57884168 A8	(SHA1) A50C5F28193A2F2971517BE5DD3C2212AAEE5376 (SHA256) A2383AF3FDE129CCFB7865D057D40A1A4BDA70E1E45C53E8BB58 681AF62E1B4B	2.23.140.1.4.1
14	1	CN = Cybertrust Japan SureCode EV CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	3067E8FBFB22 01DE04917E3A E9701115A580F 9D1	id-ecPublic Key	384Bits	ecdsa-with- SHA384	June 22, 2020 18:56:51	June 22, 2036 18:56:51	2FE1DE0 6415D92 B9F78BB 34C20C70 43726DF7 2EB	(SHA1) 542AA69A5F38DFD4CD9C41B03048B7BCE10124A7 (SHA256) AEEDAB7F871504EE07CEB3ED93AF034394548B1E655F7C759B9646 AB78F0CEBB	2.23.140.1.3
15	1	CN = Cybertrust Japan SureCode EV CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	401C0824BBCE A63303FB626F7 D613BFF01241 FF6	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	June 22, 2020 17:31:36	June 22, 2036 17:31:36	3D5C4FB 323D4C8 3BD01CC 593D5577 BB849906 AC4	(SHA1) 6261D96B51BFF7807F38B4A52E4155D89EFEF71E (SHA256) 87CC9D3EDF3F8517D922944AA114A5576AB4FD8DF09E35D10FF31 4C8EA172619	2.23.140.1.3
16	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	83486A28 4E149A7 D1AC5F2 EA05D43 E72BE60 0EA7	(SHA1) D3FA22289481BA615E9A688CEE92A2F103D8114E (SHA256) DF722167C475B964E39C2536D87E694A160F65C43F62DAC8764EA0 51D5783AAA	2.23.140.1.5.2.3



(Translation)

Cert #	Subject	Issuer	Serial	Key Algorithm	Key Size	Digest Algorithm	Not Before	Not After	SKI	Fingerprint	Policy identifiers
17	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
18	CN = Cybertrust Japan SureTime CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	3E745100E3A15C5D0288B4475F408E516A8337B5	id-ecPublicKey	384Bits	ecdsa-with-SHA384	September 9, 2021 11:41:04	September 9, 2037 11:41:04	160378BECDE5F52B490829E4D21143A6CAD6C489	(SHA1) F95B7E1CA40A890941A5039DAD81463D92B3A4B7 (SHA256) 5022E703CD525D1D45F8CAB522C00B8D371891C9995D28F36E12906B8D1E9EBE	2.23.140.1.4.2
19	CN = Cybertrust Japan SureTime CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	47C05BCA232CA403ABA01603F0584B6B150ACFFB	rsaEncryption	4096Bits	Sha384WithRSAAEncryption	September 9, 2021 11:28:53	September 9, 2037 11:28:53	DD89D9132793721A466BB0CDB0C84ECAC1BA029	(SHA1) 3C050F28F197CE9BBE16EE6551C9530D838D9AD5 (SHA256) F8D976C1190F85B54EBD88B45986FCF475D1A58F8CFD1D70B0E40A6346BBA4A6	2.23.140.1.4.2



(Translation)

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#5, CA#8	JCSI Certificate Policy	3.5	September 13, 2023
	JCSI Certificate Policy	3.6	March 15, 2024
	JCSI Certificate Policy	3.7	July 30, 2024
CA#1 — CA#4, CA#6, CA#7, CA#9 — CA#19	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#19	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



(Translation)

CTJ MANAGEMENT'S ASSERTION

October 31, 2024

Mitsuyoshi Tamura
Corporate Officer General Manager
PKI 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
- Subordinate CA cross-certification

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, certificate lifecycle management controls, and subordinate CA 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

(Translation)

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 Certification Authority (CA) services at Hokkaido and Tokyo, Japan, throughout the period October 16, 2023 to August 23, 2024, 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;
 - subscriber information is properly authenticated (for the registration activities performed by CTJ); and
 - subordinate CA certificate requests are accurate, authenticated, and approved
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:

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
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

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

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Appendix A, CA#12-CA#15 and CA#17-CA#19 were revoked on August 20, 2024. Those CAs did not issue certificates throughout the period August 20, 2024 to August 23, 2024 and was maintained online to provide revocation status information only.

CTJ does not escrow its CA keys, and does not provide certificate suspension 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.)

APPENDIX A

List of CAs in Scope

Root CAs
CA#1: SecureSign Root CA16
CA#2: SecureSign Root CA15
CA#3: SecureSign Root CA14
CA#4: SecureSign Root CA12
CA#5: SecureSign RootCA11
OV SSL Issuing CAs
CA#6: Cybertrust Japan SureServer CA G8
CA#7: Cybertrust Japan SureServer CA G7
CA#8: JCSI TLSSign Public CA
EV SSL Issuing CAs
CA#9: Cybertrust Japan SureServer EV CA G9
CA#10: Cybertrust Japan SureServer EV CA G8
CA#11: Cybertrust Japan SureServer EV CA G7
Non-EV Code Signing Issuing CAs
CA#12: Cybertrust Japan SureCode CA G4
CA#13: Cybertrust Japan SureCode CA G3
EV Code Signing Issuing CAs
CA#14: Cybertrust Japan SureCode EV CA G4
CA#15: Cybertrust Japan SureCode EV CA G3
Secure Email (S/MIME) CAs
CA#16: Cybertrust Japan SureMail CA G9
CA#17: Cybertrust Japan SureMail CA G8
Timestamp CAs
CA#18: Cybertrust Japan SureTime CA G4
CA#19: Cybertrust Japan SureTime CA G3



(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 30, 2044 15:55:40	186E34B6 DB99556 448A5864 9B89E4B 93F70E2 B0F	(SHA1) D17917EC45E2A0CAD774513010A4C65CAAB33C49 (SHA256) 4C1CCD24F17E950FC18536B33CAFE32293CFC33E8467B41E1C693 055D7F513BF	—
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- ecPubli cKey	384Bits	ecdsa-with- SHA384	April 8, 2020 17:32:56	April 8, 2045 17:32:56	EB41C8A EFCDD59E 5148F5B D8BF487 2093412B D3F4	(SHA1) CBBA83C8C15A5DF1F9736FCAD7EF2813064A077D (SHA256) E778F0F095FE843729CD1A0082179E5314A9C291442805E1FB1D8F B6B8886C3A	—
3	1	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	64DB5A0C204E E8D72977C850 27A25A27DD2 DF2CB	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	April 8, 2020 16:06:19	April 8, 2045 16:06:19	0693A30 A5E2869 37AA611 DEBEBF C2D6F23 E4F3A0	(SHA1) DD50C0F779B3642E74A2B89D9FD340DDBBF0F24F (SHA256) 4B009C1034494F9AB56BBA3BA1D62731FC4D20D8955ADCEC10A 925607261E338	—
4	1	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	66F9C7C1AFE CC251B4ED539 7E6E682C32B1 C9016	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	April 8, 2020 14:36:46	April 8, 2040 14:36:46	5734F374 CF044BD 525E6F14 0B62C4C D92DE9A 0AD	(SHA1) 7A221E3DDE1B06AC9EC84770168E3CE5F76B06F4 (SHA256) 3F034BB5704D44B2D08545A02057DE93EBF3905FCE721ACBC730C 06DDAEE904E	—



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
5	1	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	01	rsaEncr yption	2048Bit s	sha1WithRS AEncryption	April 8, 2009 13:56:47	April 8, 2029 13:56:47	5BF84D4 FB2A586 D43AD2F 1639AA0 BE09F65 7B7DE	(SHA1) 3BC49F48F8F373A09C1EBDF85BB1C365C7D811B3 (SHA256) BF0FEEFB9E3A581AD5F9E9DB7589985743D261085C4D314F6F5D7 259AA421612	—
6	1	CN = Cybertrust Japan SureServer CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	4D8247384ADF 541F88340F492 8553224B6C48F E2	id- ecPubli cKey	384Bits	ecdsa-with- SHA384	June 22, 2020 18:45:15	June 22, 2030 18:45:15	3DD2971 9E539169 9EE6BB0 1B7AC6F 3FACAF5 F703	(SHA1) A07043D2965389E4EF90EBEAEA319996A9877819 (SHA256) 93D931D5F95411998705B148532F4E16FBCF00F3318DFF9B6A0765E D749C8FD0	2.23.140.1.2.2
7	1	CN = Cybertrust Japan SureServer CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	167DDD4E7AB D348B6A105B C9CA24ACE74 5F2B6CB	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	June 22, 2020 16:42:05	June 22, 2030 16:42:05	8E3C2863 93A4E48 50F5489D D69B23C 52674AB 5A4	(SHA1) F9DDEC1E1FCF62CE4FAD04EDC44109A9504F4784 (SHA256) A2E2C3D73CFF96451325712E212FA15C40FD4F2C3F143C1BB61938 5365304C02	2.23.140.1.2.2
8	1	CN = JCSI TLSSign Public CA O = Cybertrust Japan Co.,Ltd. C = JP	CN = SecureSign RootCA11 O = Japan Certification Services, Inc. C = JP	7540ACF59D07 1D7A7ECAF2 FB965A7D1141 5CD53	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	October 11, 2018 10:36:33	April 8, 2029 13:56:47	D3342FD DF84C99 DE843F0 51DB9D9 F440D9C 08BB1	(SHA1) 5E2ED0EDD013B5EF5EB2203FAAB6F876452FCEC2 (SHA256) 9253BFB668F3E743A525E48B5F750A8A66035F806297C25F8134DC 8AC9635BD8	2.23.140.1.2.2



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
9	1	CN = Cybertrust Japan SureServer EV CA G9 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	756AA35ABA8 847DD5103C33 A37B168FA13A 4F715	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	June 22, 2020 17:50:22	June 22, 2030 17:50:22	EDB8FA2 F3D7D25 BEE354B 165CE54 A8833B9 2F0C7	(SHA1) EDEC2820E5CD08CB234D3B2417FE0DCDB51D238B (SHA256) 93397E182492A7E7C582BADFE04348E6FA985CBA19AFDE16FD74 0FF03857367C	2.23.140.1.1
10	1	CN = Cybertrust Japan SureServer EV CA G8 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	7CA3593373BD 43AA87416AB0 439DAC5D0361 D803	id- ecPubli cKey	384Bits	ecdsa-with- SHA384	June 22, 2020 18:39:21	June 22, 2030 18:39:21	AEE4FD C16E22F 8DFB713 83F8E2D 143B696 B93AC8	(SHA1) FBF4B414FBA71E4F10AA57CF8C47697489D59ED1 (SHA256) 70C4002E0DF2FF51E691654903BE742D09D5A74A84B15B68FBCDA 320FBF3DC6B	2.23.140.1.1
11	1	CN = Cybertrust Japan SureServer EV CA G7 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA12 O = Cybertrust Japan Co., Ltd. C = JP	2C77F85B12969 E757EAC8921C 7155089AE35F4 18	rsaEncr yption	2048Bit s	sha256With RSAEncrypt ion	June 22, 2020 16:34:38	June 22, 2030 16:34:38	7483319B F875CD0 DCF8E84 E6D28E9 AA6794C 2AA6	(SHA1) 99865D3428D04DEF0D3FA29DEFBD5905A0B040A7 (SHA256) 76648FBC40CC4164CEA02422A09EB4EAD29C67F5E7DD74F691B7 FA08043472C5	2.23.140.1.1
12	1	CN = Cybertrust Japan SureCode CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	2141B3AAF2EF DF0F9FC1CBE 2C6A8AB4E966 DA06F	id- ecPubli cKey	384Bits	ecdsa-with- SHA384	June 22, 2020 19:02:43	June 22, 2036 19:02:43	A56FC73 83B5B24 E8D03FF 1E608048 58BCDC A8CCF	(SHA1) 7F466C2F01734A4034024DBD9E460515D3B80C76 (SHA256) 42A7E8F7E06F2FC1CE417B26AC6F724E7BCC520A3B64ED506C7A A0B6DA25D63E	2.23.140.1.4.1



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
13	1	CN = Cybertrust Japan SureCode CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	605809FFFD7A D23CC7793CF C3181DE152DF E1C19	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	June 22, 2020 17:37:47	June 22, 2036 17:37:47	47F78166 565D8C5 DEF9DF4 81260F85 57884168 A8	(SHA1) A50C5F28193A2F2971517BE5DD3C2212AAEE5376 (SHA256) A2383AF3FDE129CCFB7865D057D40A1A4BDA70E1E45C53E8BB5 8681AF62E1B4B	2.23.140.1.4.1
14	1	CN = Cybertrust Japan SureCode EV CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	3067E8FBFB22 01DE04917E3A E9701115A580F 9D1	id- ecPubli cKey	384Bits	ecdsa-with- SHA384	June 22, 2020 18:56:51	June 22, 2036 18:56:51	2FE1DE0 6415D92 B9F78BB 34C20C7 043726DF 72EB	(SHA1) 542AA69A5F38DFD4CD9C41B03048B7BCE10124A7 (SHA256) AEEDAB7F871504EE07CEB3ED93AF034394548B1E655F7C759B964 6AB78F0CEBB	2.23.140.1.3
15	1	CN = Cybertrust Japan SureCode EV CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	401C0824BBCE A63303FB626F 7D613BFF0124 1FF6	rsaEncr yption	4096Bit s	Sha384With RSAEncrypt ion	June 22, 2020 17:31:36	June 22, 2036 17:31:36	3D5C4FB 323D4C8 3BD01CC 593D5577 BB84990 6AC4	(SHA1) 6261D96B51BFF7807F38B4A52E4155D89EFEF71E (SHA256) 87CC9D3EDF3F8517D922944AA114A5576AB4FD8DF09E35D10FF3 14C8EA172619	2.23.140.1.3
16	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	143D38AEE7B EA7D577D96A A346B5581E0A 651915	rsaEncr yption	4096Bit s	sha256With RSAEncrypt ion	July 30, 2024 17:11:33	July 30, 2034 17:10:15	83486A28 4E149A7 D1AC5F2 EA05D43 E72BE60 0EA7	(SHA1) D3FA22289481BA615E9A688CEE92A2F103D8114E (SHA256) DF722167C475B964E39C2536D87E694A160F65C43F62DAC8764EA0 51D5783AAA	2.23.140.1.5.2.3



(Translation)

C A #	Cert #	Subject	Issuer	Serial	Key Algor ithm	Key Size	Digest Algorith m	Not Before	Not After	SKI	Fingerprint	Policy identifiers
17	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 A4D67BE7EC3 1B75024A2DB5 5C0015	id- ecPubli cKey	384Bits	ecdsa-with- SHA384	August 21, 2023 12:08:29	June 22, 2030 18:50:52	9FBFE09 859F1DB D24E84B 093408B A9D5A14 1026F	(SHA1) 113F753E0D47D761623FC92FC561931D335746B4 (SHA256) 8FBD048775F6F4C486CF4960A7BB8B807225E37C74935E5B99CBA 9E41383FECA	2.23.140.1.5.2.1
18	1	CN = Cybertrust Japan SureTime CA G4 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA15 O = Cybertrust Japan Co., Ltd. C = JP	3E745100E3A1 5C5D0288B447 5F408E516A833 7B5	id- ecPubli cKey	384Bits	ecdsa-with- SHA384	September 9, 2021 11:41:04	September 9, 2037 11:41:04	160378BE CDE5F52 B490829E 4D21143 A6CAD6 C489	(SHA1) F95B7E1CA40A890941A5039DAD81463D92B3A4B7 (SHA256) 5022E703CD525D1D45F8CAB522C00B8D371891C9995D28F36E1290 6B8D1E9EBE	2.23.140.1.4.2
19	1	CN = Cybertrust Japan SureTime CA G3 O = Cybertrust Japan Co., Ltd. C = JP	CN = SecureSign Root CA14 O = Cybertrust Japan Co., Ltd. C = JP	47C05BCA232C A403ABA01603 F0584B6B150A CFFB	rsaEncr yption	4096Bits	Sha384With RSAEncrypt ion	September 9, 2021 11:28:53	September 9, 2037 11:28:53	DDB89D 91327937 21A466B B0CDB0 C84ECA C1BA029	(SHA1) 3C050F28F197CE9BBE16EE6551C9530D838D9AD5 (SHA256) F8D976C1190F85B54EBD88B45986FCF475D1A58F8CFD1D70B0E40 A6346BBA4A6	2.23.140.1.4.2

APPENDIX B

Certificate Policy

CA	Policy Name	Version	Date
CA#5, CA#8	JCSI Certificate Policy	3.5	September 13, 2023
	JCSI Certificate Policy	3.6	March 15, 2024
	JCSI Certificate Policy	3.7	July 30, 2024
CA#1 — CA#4, CA#6, CA#7, CA#9 — CA#19	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#19	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