KPMG

あずさ監査法人

有限責任 あずさ監査法人
東京都新宿区津久戸町１番２号
あずさセンタービル 〒162-8551

Telephone 03 3266 7500
Fax 03 3266 7600
Internet http://www.kpmg.com/jp/azsa

独立した監査法人の認証局のための Trust サービス保証報告書

平成 26 年 7 月 31 日

サイバートラスト株式会社
技術本部
プロダクトマネジメント部
プロダクト・マネージャー
坂本 勝　殿

有限責任 あずさ監査法人
パートナー　公認会計士　岩下 廣美 印

範囲

当監査法人は、認証局のための WebTrust®の規準＊１に基づいて、平成 26 年 6 月 30 日現在において、サイバートラスト株式会社の認証局 SecureSign RootCA11 サービス（札幌）（以下、「CA サービス」という。）の提供について下記の事項が記載された「経営者の記述書」について検証を行った。

1. サイバートラスト株式会社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「JCSI ルート認証局 Certification Practice Statement （認証局運用規程） Version 1.0 （平成26年6月30日）」にて開示していた。
2. サイバートラスト株式会社は下記について合理的な保証を提供する適切な内部統制を設計していた。
   - サイバートラスト株式会社の「JCSI ルート認証局 Certification Practice Statement （認証局運用規程） Version 1.0 （平成 26 年 6 月 30 日）」に準拠してサービスを提供すること。
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適切な内部統制を設計していた。
   - 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ること。
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適切な内部統制を設計していた。
   - 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ること。

・ 鍵と証明書の管理に関する運用の継続性が維持されること。
・ 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、実施されること。

経営者の責任

経営者の記述書の作成責任は、サイバートラスト株式会社の経営者にある。

業務実施者の責任

当監査法人の責任は、当監査法人の実施した手続に基づいて経営者の記述書に対する結論を報告することにある。

当監査法人の検証は、ＩＴ委員会実務指針第２号「Trust サービスに係る実務指針(中間報告)」に準拠して実施され、(1)サイバートラスト株式会社の鍵と証明書のライフサイクル管理のビジネス実務及び鍵と証明書のインテグリティ、加入者と信頼者情報の認証と個人情報保護、鍵と証明書のライフサイクル管理に係る運用の継続性、システムインテグリティの開発、保守、及び運用に関する内部統制を理解し、(2)内部統制の設計の適合性をテスト、評価し、(3)当監査法人が状況に応じて必要と認めたその他の手続を実施したことを含んでいる。

当監査法人は、検証の結果として結論を報告するための合理的な基礎を得たと判断している。

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

内部統制の限界

内部統制の性質や固有の限界のため、先に述べた規準に適合するためのサイバートラスト株式会社の能力に影響を及ぼす可能性がある。例えば、内部統制により誤謬又は不正、システムや情報への未承認のアクセス、社内及び外部のポリシーや要求への遵守性違反を防止、発見、修正することができないことがある。又、当監査法人の発見事項に基づく結論から将来を予測することは、変更が生ずることにより、その結論の妥当性を失うリスクがある。

意見

当監査法人は、経営者の記述書が、認証局のための WebTrust®の規準に基づいて、平成26年6月30日現在において、全ての重要な点において適正に表示されているものと認める。

強調事項

経営者は認証局（CA）のサービスを稼働していないため、システム導入前に内部統制の設計に対して追加的な変更を行う場合がある。当監査法人は、いずれの期間についても内部統制の運用状況の有効性を評価する手続を実施していない。したがって、当監査法人は個別の、又は全体のサイバートラスト株式会社の内部統制のいかなる側面の有効性に関する意見も表明しない。

この保証報告書は、認証局のための WebTrust®の規準が対象としている範囲を超えて、サイバートラスト株式会社の CA サービスの品質について何ら結論を報告するものではなく、又、いかなる顧客の意図する目的に対するサイバートラスト株式会社の CA サービスの適合性についても何ら結論を報告するものではない。

利害関係

サイバートラスト株式会社と当監査法人又はパートナーとの間には、公認会計士法の規定に準じて記載すべき利害関係はない。

以上

＊1　認証局のための WebTrust®の規準(the Trust Services Criteria for Certification Authorities)は、米国公認会計士協会／カナダ勅許職業会計士協会の知的財産であり、日本公認会計士協会が著作権法に従って翻訳している。

cybertrust

経営者の記述書

平成 26 年 7 月 31 日

サイバートラスト株式会社
技術本部
プロダクトマネジメント部
プロダクト・マネージャー
坂本 勝

当社は、認証局SecureSign RootCA11（札幌）を通じて、次のサービス（以下「CAサービス」という。）の提供を準備している。

- 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
- 証明書ステータス情報の処理（オンラインリポジトリーを使用）

当社の経営者は、当社のWebサイトで公開している「JCSI ルート認証局 Certification Practice Statement（認証局運用規程） Version 1.0 （平成26年6月30日）」におけるCAビジネス実務の開示、サービスのインテグリティ（鍵と証明書のライフサイクル管理を含む。）及びCA環境の内部統制を含む当社のCAの運用について、有効な内部統制を確立することに責任がある。これらの内部統制はモニタリングの仕組みを含んでおり、識別された欠陥を修正するための行動が取られる。

内部統制には誤謬及び内部統制の迂回又は無視を含む固有の限界がある。したがって、有効な内部統制といえども、当社の CA の運用について合理的な保証を提供するものでしかない。さらに、状況の変化により、内部統制の有効性は時間とともに変化する場合がある。

当社の経営者は、当社のCAの運用に関する内部統制を評価した。その評価に基づく当社の経営者の意見では、当社は、認証局のためのWebTrust®の規準(the Trust Services Criteria for Certification Authorities)に準拠して、平成26年6月30日現在において、CAサービスの提供に関して、下記の事項を実施した。

1. 当社が実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及びCA環境の内部統制の実務を、当社のWebサイトにおける「JCSI ルート認証局 Certification Practice Statement（認証局運用規程） Version 1.0 （平成26年6月30日）」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適切な内部統制を設計していた。
   - 当社の「JCSI ルート認証局 Certification Practice Statement（認証局運用規程） Version 1.0

（平成 26 年 6 月 30 日）」に準拠してサービスを提供すること。

3. 下記について合理的な保証を提供する適切な内部統制を設計していた。
   - 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ること。

4. 下記について合理的な保証を提供する適切な内部統制を設計していた。
   - 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ること。
   - 鍵と証明書の管理に関する運用の継続性が維持されること。
   - 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、実施されること。

当社が準拠した認証局のための WebTrust®の規準には、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）

CAのビジネス実務管理

- 認証局運用規程（CPS）の管理

サービスのインテグリティ

CA鍵ライフサイクル管理の内部統制

- CA鍵の生成
- CA鍵のストレージ、バックアップと復旧
- CA公開鍵の配送
- CA鍵の使用法
- CA鍵の保存及び破壊
- CA鍵の危殆化
- CAの暗号化ハードウェアライフサイクルの管理

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

以上

KPMG AZSA LLC
AZSA Center Building
1-2, Tsukudo-cho, Shinjuku-ku
Tokyo 162-8551, Japan

Telephone +81 (3) 3266 7500
Fax +81 (3) 3266 7600
Internet http://www.kpmg.com/jp/azsa

(Translation)

Trust Service for Certification Authorities

Independent Accountant's Report

July 31, 2014

To Mr. Masaru Sakamoto
Product Manager
Product Management Department
Technology Division
Cybertrust Japan Co., Ltd.

KPMG AZSA LLC
Partner
Certified Public Accountant
Hiromi Iwashita

Scope of the examination

We have examined the assertion by the management of Cybertrust Japan Co., Ltd. (the "management's assertion") that in providing its certification authority (CA) services as the SecureSign RootCA11 services (the "CA services") at Sapporo, Japan as of June 30, 2014, Cybertrust Japan Co., Ltd. has -

1. disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its JCSI Root CA Certification Practice Statement Version 1.0, dated June 30, 2014 on Cybertrust Japan Co., Ltd.'s website.
2. designed suitable controls to provide reasonable assurance that:
   - Cybertrust Japan Co., Ltd. provides its services in accordance with its JCSI Root CA Certification Practice Statement Version 1.0, dated June 30, 2014;
3. designed suitable controls to provide reasonable assurance that:
   - the integrity of keys and certificates it manages is established and protected throughout their life cycles, and
4. designed suitable 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

KPMG

(Translation)

- CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

based on the Trust Services Criteria for Certification Authorities.

Management's responsibility
Cybertrust Japan Co., Ltd.'s management is responsible for its assertion.

Independent Accountants' responsibility
Our responsibility is to express an opinion on management's assertion based on our examination. Our examination was conducted in accordance with IT Committee Practice Guidelines No.2 established by the Japanese Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of Cybertrust Japan Co., Ltd.'s key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the continuity of key and certificate life cycle management operations, and over the development, maintenance, and operation of systems integrity; (2) testing and evaluating the suitability of the design of the controls; and (3) performing such other procedures as we considered necessary in the circumstances.
We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls on the CA services at Cybertrust Japan Co., Ltd. and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Limitations in controls
Because of the nature and inherent limitations of controls, Cybertrust Japan Co., Ltd.'s ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any

KPMG

(Translation)

conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

Opinion

In our opinion, as of June 30, 2014, the management's assertion is fairly stated, in all material respects, based on the Trust Services Criteria for Certification Authorities.

Emphasis

Management has not placed its Certification Authority (CA) services in operation and, therefore, additional changes may be made to the design of the controls before the system is implemented. We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of Cybertrust Japan Co., Ltd.'s controls, individually or in the aggregate.

This report does not include any representation as to the quality of Cybertrust Japan Co., Ltd.'s services beyond those covered by the Trust Services Criteria for Certification Authorities, nor the suitability of any of Cybertrust Japan Co., Ltd.'s services for any customer's intended purpose.

Other matter

KPMG AZSA LLC and engagement partners have no interest in Cybertrust Japan Co., Ltd., which should be disclosed pursuant to the provisions of the Certified Public Accountants Law of Japan.

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

cybertrust

(Translation)

Assertion by Management
as to its Disclosure of its Business Practices and its
Controls Over its Certification Authority Operations as of June 30

July 31, 2014

Masaru Sakamoto
Product Manager
Product Management Department
Technology Division
Cybertrust Japan Co., Ltd.

Cybertrust Japan Co., Ltd. ("Cybertrust") provides the following services (the "CA services") through its certification authorities (CA), the SecureSign RootCA11 at Sapporo, Japan:

- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing (using an online repository)

Management of Cybertrust is responsible for designing suitable controls over its CA operations, including CA business practices in its JCSI Root CA Certification Practice Statement Version 1.0, dated June 30, 2014 on Cybertrust's website, service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

Controls have inherent limitations, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective internal control can provide only reasonable assurance with respect to Cybertrust's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in Cybertrust's Management's opinion, in providing the CA services as of June 30, Cybertrust has

–

cybertrust

(Translation)

1. disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its JCSI Root CA Certification Practice Statement Version 1.0, dated June 30, 2014 on Cybertrust's website
2. designed suitable controls to provide reasonable assurance that:
   - Cybertrust provides its services in accordance with its JCSI Root CA Certification Practice Statement Version 1.0, dated June 30, 2014;
3. designed suitable controls to provide reasonable assurance that:
   - the integrity of keys and certificates it manages is established and protected throughout their life cycles;
4. designed suitable 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 Trust Services Criteria for Certification Authorities including the following:

CA Business Practices Disclosure

- Certification Practice Statement

CA Business Practices Management

- Certification Practice Statement Management

Service Integrity

CA Key Life Cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Life Cycle Management

CA Environmental Controls

- Security Management

cybertrust

(Translation)

- 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

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