新日本有限責任監査法人
東京都千代田区内幸町二丁目２番３号
日比谷国際ビル
〒100-0011

Tel: +81 3 3503 3500
Fax: +81 3 3503 1966
www.eyjapan.jp

Building a better working world

独立した監査法人の認証局のためのWebTrust－SSL基本要件保証報告書

平成29年12月22日

総務省
行政管理局行政情報システム企画課
情報システム管理室長
小髙　久義　殿

新日本有限責任監査法人

シニアパートナー　公認会計士　遊 馬 正 美

範囲

当監査法人は、「認証局のための WebTrust®－SSL 基本要件保証規準」に基づいて、平成 28 年 10 月 1 日から平成 29 年 9 月 30 日までの期間において、総務省の政府認証基盤（GPKI）アプリケーション認証局 2（Root）、アプリケーション認証局 2（Sub）、及び共用 LRA による電子認証サービス（以下「認証局」を「CA」といい、これらのサービスを総称して「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。ただし、共用 LRA は、本年稼働したシステムであるため、システム稼働後の平成 29 年 2 月 1 日から平成 29 年 9 月 30 日までの期間を対象とし検証を行った。

- 総務省は、証明書実務及び手続並びにCAブラウザフォーラムガイドラインに準拠してSSL証明書を提供するためのコミットメントを開示していた。
- 総務省は、次の事項に関する合理的な保証を提供する有効な内部統制を保持していた。
  - 加入者情報が（総務省が実施する登録業務によって）適切に収集、認証、検証されている。
  - 管理する鍵及び証明書のインテグリティが確立されており、そのライフサイクルを通じて保護されている。
  - 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る。
  - 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る。
  - 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、実施されている。

記述書に対する経営者の責任

総務省のマネジメントの責任は、「認証局のための WebTrust®－SSL 基本要件保証規準」に基づいて、総務省の CA の有効な内部統制を維持し、当該事実を記載した「経営者の記述書」を作成することにある。

業務実施者の責任

当監査法人の責任は、当監査法人の実施した手続に基づいて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）」に準拠して次の事項を実施した。

(1) SSL証明書の発行、更新、失効を含む総務省のSSL証明書ライフサイクル管理実務と手続に関して理解

(2) 開示されたSSL証明書ライフサイクル管理実務に従って実行された取引の選択によるテスト

(3) 内部統制の運用状況の有効性のテスト及び評価

(4) 状況に応じて必要と認めた他の手続

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。

内部統制の限界

内部統制の固有の限界のため、誤り又は不正、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が発生し、それらが発見されないことがある。当監査法人の結論から将来を予想することにはリスクがある。

意見

当監査法人は、「経営者の記述書」が、「認証局のための WebTrust®－SSL 基本要件保証規準」に基づいて、平成 28 年 10 月 1 日から平成 29 年 9 月 30 日までの期間（ただし、共用 LRA は、平成 29 年 2 月 1 日から平成 29 年 9 月 30 日）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

総務省における特定の内部統制の相対的有効性と重要性及び加入者と依拠する当事者のための統制リスクの評価における効果は、個々の加入者や依拠する当事者の所在によって統制の相互関係や他の要因によって異なる場合がある。当監査法人は、個々の加入者及び依拠する当事者の所在に関する内部統制の有効性を評価するような手続は何ら行っていない。

この報告書は、「認証局のための WebTrust®－SSL 基本要件保証規準」で対象とした範囲を越えた総務省のサービスの品質についての表現を含んでおらず、又、いかなる顧客の意図する目的のための総務省のサービスの適合性についても同様である。

総務省の Web サイト上の WebTrust®－SSL 基本要件シールは、この保証報告書の内容を象徴的に表示しているが、この保証報告書の変更又は追加的な保証を提供することを意図したものではなく、そのような解釈をすべきではない。

利害関係

　総務省と当監査法人又はシニアパートナーとの間には、公認会計士法の規定に準じて記載すべき利害関係はない。

以上

経営者の記述書

平成29年12月22日

新日本有限責任監査法人　殿

総務省
行政管理局行政情報システム企画課
情報システム管理室長
小髙　久義

総務省は、政府認証基盤（GPKI）アプリケーション認証局2（Root）、アプリケーション認証局2（Sub）、及び共用LRAによる電子認証サービス（以下「認証局」を「CA」といい、これらのサービスを総称して「CAサービス」という。）に係る内部統制を評価した。その評価に基づき、平成28年10月1日から平成29年9月30日までの期間（ただし、共用LRAは、平成29年2月1日から平成29年9月30日）において、所在地東京（日本）における総務省のCAサービスは、総務省のマネジメントの意見では、「認証局のためのWebTrust®－SSL基本要件保証規準」に従って、下記事項を実施した。

- 総務省は、証明書実務及び手続並びにCAブラウザフォーラムガイドラインに準拠してSSL証明書を提供するためのコミットメントを開示し、当該開示された実務に従ってサービスを提供している。
- 総務省は、次の事項に関する合理的な保証を提供する有効な内部統制を保持していた。
  - 加入者情報が（総務省が実施する登録業務によって）適切に収集、認証、検証されている。
  - 管理する鍵及び証明書のインテグリティが確立されており、そのライフサイクルを通じて保護されている。
  - 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る。
  - 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る。
  - 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、実施されている。

以上

(Translation)

WebTrust -SSL Baseline Requirements for Certification Authorities

Independent Accountants' Report

December 22, 2017

To Mr. Hisayoshi Kodaka
Director of Information Systems Management Office
Government Information Systems Planning Division
Administrative Management Bureau
Ministry of Internal Affairs and Communications

Ernst & Young ShinNihon LLC
Senior Partner
Certified Public Accountant
Masami Asuma

Scope

We have examined the assertion by the management of Ministry of Internal Affairs and Communications (the "management's assertion") that in providing its SSL Certificate Authority (CA) services as the Government Public Key Infrastructure (GPKI) Application Certification Authority2 (Root), Application Certification Authority2 (Sub) (CA) services and the Shared LRA (collectively referred to as the "CA services") during the period October 1, 2016 through September 30, 2017(Since the Shared LRA is a system that started operations in this year, we have examined during the period February 1, 2017 through September 30, 2017), Ministry of Internal Affairs and Communications has –

- disclosed its SSL certificate life cycle management business practices to provide SSL certificates in conformity with the CA/Browser Forum,
- maintained effective controls to provide reasonable assurance that:

- SSL subscriber information was properly collected, authenticated and examined (by its registration activities);
- the integrity of keys and SSL certificates it manages was established and protected throughout its life cycles;
- logical and physical access to CA systems and data was restricted to authorized individuals;
- the continuity of key and certificate management operations was maintained; and
- CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline.

Management's responsibility for its assertion

Ministry of Internal Affairs and Communications's management is responsible for maintaining effective internal controls based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline, and making the management's 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 Practical Guidelines No.2 established by the Japanese Institute of Certified Public Accountants, and accordingly, included

(1) obtaining an understanding of Ministry of Internal Affairs and Communications's SSL certificate life cycle management business practices,

(2) selectively testing transactions executed in accordance with disclosed SSL certificate life cycle management practices;

(3) testing and evaluating the operating effectiveness of the controls; and

(4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

Limitations in controls

Because of inherent limitations of controls, errors or fraud may occur and not be detected. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required due to the time passage, or (4) deterioration of compliance with the policies or procedures may alter the validity of such conclusions.

Opinion

In our opinion, during the period October1, 2016 through September 30, 2017 (Regarding the Shared LRA, during the period February 1, 2017 through September 30, 2017), the management's assertion is fairly stated, in all material respects, based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline.

Emphasis

The relative effectiveness and significance of specific controls at Ministry of Internal Affairs and Communications's SSL-CA services and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

This report does not include any representation as to the quality of Ministry of Internal Affairs and Communications's certification services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline, nor the suitability of any of Ministry of Internal Affairs and Communications's services for any customer's intended purpose.

Ministry of Internal Affairs and Communications's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Other Matter

Ernst & Young ShinNihon LLC and the Senior Partner have no interest in Ministry of Internal Affairs and Communications, which should be disclosed pursuant to the provisions of the Certified Public Accountants Law of Japan.

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

(Translation)

Assertion by Management
as to its Disclosure of its Business Practices and its
Controls Over its Certification Authority Operations During the Period February 1, 2017
through September 30, 2017

December 22, 2017

Mr. Hisayoshi Kodaka
Director of Information Systems Management Office
Government Information Systems Planning Division
Administrative Management Bureau
Ministry of Internal Affairs and Communications

Ministry of Internal Affairs and Communications. ("MIC") has evaluated the internal control over the Government Public Key Infrastructure (GPKI) Application Certification Authority2 (Root), Application Certification Authority2 (Sub) (CA) services and the Shared LRA (collectively referred to as the "CA services"). Based on that evaluation, in MIC management's opinion, in providing its CA services at Tokyo (Japan), during the period October 1, 2016 through September 30, 2017 (Regarding the Shared LRA, during the period February 1, 2017 through September 30, 2017), MIC has–

- disclosed its SSL certificate life cycle management business practices to provide SSL certificates in conformity with the CA/Browser Forum, and provided such services in accordance with its disclosed practices.
- maintained effective controls to provide reasonable assurance that:
  - SSL subscriber information was properly collected, authenticated and examined (by its registration activities);
  - the integrity of keys and SSL certificates it manages was established and protected throughout its life cycles;
  - logical and physical access to CA systems and data was restricted to authorized individuals;
  - the continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity

in accordance with the WebTrust®-SSL Basic Requirements for Certification Authority Criteria for Certification Authorities.