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 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®の規準」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。

1. 総務省の CA が実施するビジネス、鍵のライフサイクル管理と証明書のライフサイクル管理及び CA 環境の内部統制の実務を GPKI の Web サイトで公開している「アプリケーション認証局2（Root）CP/CPS（平成 27 年 9 月 7 日改定、平成 29 年 6 月 23 日改定）」及び「アプリケーション認証局2（Sub）CP/CPS（平成 27 年 9 月 7 日改定、平成 29 年 6 月 23 日改定、平成 29 年 9 月 8 日改定）」にて開示していた。

2. 総務省は、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。
   - 総務省の「アプリケーション認証局2（Root）CP/CPS（平成 27 年 9 月 7 日改定、平成 29 年 6 月 23 日改定）」及び「アプリケーション認証局2（Sub）CP/CPS（平成 27 年 9 月 7 日改定、平成 29 年 6 月 23 日改定、平成 29 年 9 月 8 日改定）」に準拠してサービスを提供していたこと。

3. 総務省は、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。
   - 総務省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。
   - 総務省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、総務省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 証明書申請は、正確で、認証され、承認されていたこと。

4. 総務省は、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 システムとデータへの論理的、物理的アクセスは許可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。

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®の規準」に基づいて、CA サービスの提供が記述書に記載されたとおりにされていることの合理的保証を提供するため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「経営者の記述書」に対する結論を報告することにある。

総務省は、そのビジネス実務として開示しているとおり、加入者登録業務のために外部登録局（府省 LRA）を使用している。外部登録局（府省 LRA）における内部統制は、当監査法人による検証の範囲外である。

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) 総務省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

(2) 総務省が開示した鍵と証明書のライフサイクル管理のビジネス実務に従って実施された取引を試査により検証

(3) 内部統制の運用の有効性のテスト及び評価

(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

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。

総務省の 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、個々の加入者及び信頼者の存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

内部統制の固有の限界のため、誤り又は不正が発生し、それらが発見されないことがある。さらに、(1) システム又は内部統制に対する変更、(2) 処理要件の変更、(3) 時間の経過により要求された変更及び(4) ポリシー又は手続への準拠性の程度の低下のため、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®の規準」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

総務省の Web サイト上の認証局のための 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。

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、総務省の 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総務省の 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

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。）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
- 証明書ステータス情報の処理

総務省は、そのビジネス実務として開示しているとおり、加入者登録業務のために外部登録局（府省LRA）を使用している。

総務省のマネジメントは、総務省のWebサイトで公開している「アプリケーション認証局2（Root）CP/CPS（平成27年9月7日改定、平成29年6月23日改定）」及び「アプリケーション認証局2（Sub）CP/CPS（平成27年9月7日改定、平成29年6月23日改定、平成29年9月8日改定）」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（鍵及び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総務省の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とられる。

内部統制には誤謬及び内部統制の迂回また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、総務省の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。

総務省のマネジメントは、総務省のCAの運用に関する内部統制を評価した。その評価に基づく総務省の意見では、総務省は、「認証局のためのWebTrust®の規準」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、CAサービスの提供に関して、下記事項を実施した。

1. 総務省のCAが実施する鍵及び証明書のライフサイクル管理、個人情報保護の実務について、総務省のCAのWebサイトにおける「アプリケーション認証局2（Root）CP/CPS（平成27年9月7日改定、平成29年6月23日改定）」及び「アプリケーション認証局2（Sub）CP/CPS（平成27年9月7日改定、平成29年6月23日改定、平成29年9月8日改定）」にて開示した。

2. 下記について合理的な保証を提供する有効な内部統制を維持していた。
   - 総務省の「アプリケーション認証局2（Root）CP/CPS（平成27年9月7日改定、平成29年6月23日改定）」及び「アプリケーション認証局2（Sub）CP/CPS（平成27年9月7日改定、平成29年6月23日改定、平成29年9月8日改定）」に準拠してサービスを提供していたこと。

3. 下記について合理的な保証を提供する有効な内部統制を維持していた。
   - 総務省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。
   - 総務省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、総務省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、物理的アクセスは許可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。

総務省が準拠した「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 ビジネス実務の管理

認証局運用規程の管理

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

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管理

加入者鍵ライフサイクル管理の内部統制

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

以上

(Translation)

WebTrust for Certification Authorities
Independent Auditors' 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 of the examination

We have examined the assertion by the management of Ministry of Internal Affairs and Communications (the "management's assertion") that in providing its certification 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-

1. disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Application CA2 (Root) CP/CPS (dated September 7, 2015 and Jun 23, 2017) and Application CA2 (Sub) CP/CPS (dated September 7, 2015, Jun 23, 2017 and September 8, 2017) on Ministry of Internal Affairs and Communications's website

2. maintained effective controls to provide reasonable assurance that:
   –Ministry of Internal Affairs and Communications provided its services in accordance with its Application CA2 (Root) CP/CPS (dated September 7, 2015 and Jun 23, 2017) and Application CA2 (Sub) CP/CPS (dated September 7, 2015, Jun 23, 2017 and September 8, 2017)

3. maintained effective controls to provide reasonable assurance that:
   –the integrity of keys and certificates it manages was established and protected throughout their life cycles;
   –the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
   –the Subscriber information was properly authenticated (for the registration activities performed by Ministry of Internal Affairs and Communications); and
   –subordinate CA certificate requests were accurate, authenticated, and approved

4. maintained effective controls to provide reasonable assurance that:
   –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 Trust Services Criteria for Certification Authorities.

Management's responsibility for its assertion

Ministry of Internal Affairs and Communication's management is responsible for maintaining effective internal controls based on the WebTrust Principles and Criteria for Certification Authorities, and making the management's assertion.

Independent Accountants' responsibility

Our responsibility is to express an opinion on management's assertion based on our examination.

Ministry of Internal Affairs and Communications makes use of external registration authorities (registration authorities at ministries, etc.) for specific subscriber registration activities as disclosed in Ministry of Internal Affairs and Communications's business practice disclosures.

Our examination did not extend to the controls exercised by the external registration authorities.

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 Ministry of Internal Affairs and Communication'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 life cycle management operations, and over the development, maintenance, and operation of systems integrity;

(2) selectively testing transactions executed in accordance with Ministry of Internal Affairs and Comunications's disclosed key and certificate life cycle 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 our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at the CA services of Ministry of Internal Affairs and Communications 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 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 October 1, 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 Trust Services Criteria for Certification Authorities

Emphasis

Ministry of Internal Affairs and Communications's use of the WebTrust® for Certification Authorities Seal on Ministry of Internal Affairs and Communications's website 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.

This report does not include any representation as to the quality of Ministry of Internal Affairs and Communications's services beyond those covered by the Trust Services Criteria for Certification Authorities,

nor the suitability of any of Ministry of Internal Affairs and Communications’s services for any customer's intended purpose.

Other matter
Ernst & Young ShinNihon LLC and 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 assertion 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") provides the following services (the "CA services") through its certification authorities (CA), the Government Public Key Infrastructure (GPKI) Application Certification Authority2 (Root) and Application Certification Authority2 (Sub) and a Local Registration Authority (the "shared LRA"):

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate status information processing

MIC makes use of external registration authorities (local registration authorities at ministries, etc.) for specific subscriber registration activities as disclosed in MIC's business practice disclosures.

Management of MIC is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure in its Application CA2 (Root) CP/CPS , dated September 7, 2015 and Jun 23, 2017 and Application CA2 (Sub) CP/CPS , dated September 7, 2015, Jun 23, 2017 and September 8, 2017 on MIC'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 MIC'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 MIC's Management's opinion, in providing the CA services through the Application Certification Authority2 (Root) and Application Certification Authority2 (Sub) 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 –

1. disclosed its Business, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control practices in its Application CA2(Root) CP/CPS , dated September 7, 2015 and Jun 23, 2017 and Application CA2 (Sub) CP/CPS , dated September 7, 2015, Jun 23, 2017 and September 8, 2017 on MIC's website

2. maintained effective controls to provide reasonable assurance that:
   - MIC provided its services in accordance with its Application CA2 (Root) CP/CPS , dated September 7, 2015 and Jun 23, 2017 and Application CA2 (Sub) CP/CPS , dated September 7, 2015, Jun 23, 2017 and September 8, 2017

3. maintained effective controls to provide reasonable assurance that:
   - the integrity of keys and certificates it manages was established and protected throughout their life cycles;
   - the integrity of subscriber keys and certificates it manages was established and protected throughout their life cycles;
   - the Subscriber information was property authenticated (for the registration activities performed by MIC); and
   - subordinate CA certificate requests were accurate, authenticated, and approved

4. maintained effective controls to provide reasonable assurance that:
   - 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 Trust Services Criteria for Certification Authorities including the following:

CA Business Practices Disclosure

- Certification Policy / Certification Practice Statement

CA Business Practices Management

- Certification Policy / Certification Practice Statement Management

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 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

Subscriber Key Life Cycle Management Controls

- Requirements for Subscriber Key Management

Certificate Life Cycle Management Controls

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

Subordinate CA Certificate Life Cycle Management Controls

- Subordinate CA Certificate Life Cycle Management

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