

WebTrustの保証報告書等の記載に係る研究文書

2021年2月2日
改正 2021年12月28日
最終改正 2022年10月13日
日本公認会計士協会
監査・保証基準委員会
(研究文書：第10号)

目次

I	はじめに	1
II	WebTrustの保証報告書等の記載例	1
	1. 認証局のためのWebTrustの保証報告書（無限定適正、期間評価）の記載例	1
	2. 認証局のためのWebTrustの経営者の記述書（期間評価）の記載例	5

《Ⅰ はじめに》

従来、WebTrust 保証業務については、カナダ勅許職業会計士協会（CPA Canada）とのライセンス契約に基づき実施される業務であり、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）」では、日本公認会計士協会が CPA Canada とライセンス契約を締結し、業務を行う国内監査法人が日本公認会計士協会とサブライセンスを締結することとしていた。しかし、当該ライセンス契約は、2020年12月末をもって終了したため、WebTrust 保証業務を実施する監査法人は個別に CPA Canada とライセンス契約を締結する等の対応が必要となる。

WebTrust 保証業務において、保証報告書等を作成するに際しては、CPA Canada が報告書等の雛型を提供しているため、それを参照して作成することになる。当該雛型については、カナダ基準、米国基準又は国際基準（ISAE3000）で業務を実施する場合について、それぞれ提供されている。

本研究文書は、CPA Canada が公表しているひな型に関して、国際基準に基づく場合における日本語による報告書の記載例（一部）を参考として提供するものである。なお、CPA Canada に日本語による報告書を提出する際には、英文による翻訳も併せて添付して提出することが必要になるため、留意することが求められる。

本研究文書は、会員が遵守すべき基準等に該当しない。また、2021年12月28日時点の最新情報に基づいている。

《Ⅱ WebTrust の保証報告書等の記載例》

《1. 認証局のための WebTrust の保証報告書（無限定適正、期間評価）の記載例》

独立した監査法人の認証局のための WebTrust 保証報告書

×年×月×日

〇〇〇〇株式会社

代表取締役社長 〇〇 〇〇 殿 [適切な宛先とする]

〇〇監査法人

〇〇事務所

代表社員 公認会計士 〇〇〇〇

社 員 公認会計士 〇〇〇〇

(注)

範囲

当監査法人は、認証局のための WebTrust の規準 v×.× (the WebTrust Principles and Criteria for Certification Authorities v×.×) に準拠して、×年×月×日から×年×月×日までの期間において、付録 A に記載された〇〇〇〇株式会社の認証局（以下「CA」という。）のサービス（場所）（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、〇〇〇〇株式会社は CA サービスについて、下記事項を実施してい

た。

1. ○○○○株式会社は、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「○○○○○○認証局運用規程 Version×」及び「証明書ポリシー Version×」[該当する場合]にて開示していた。
2. ○○○○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。
 - ・ ○○○○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[該当する場合]。
 - ・ ○○○○株式会社は、証明書ポリシー[該当する場合]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. ○○○○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。
 - ・ ○○○○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。
 - ・ ○○○○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、(○○○○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. ○○○○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。

[外部の登録局を利用している場合]○○○○株式会社は、○○○○株式会社のビジネス実務において開示された特定の加入者登録活動のため外部の登録局を利用している。当監査法人の手続は、これらの外部の登録局により実施される内部統制を含んでいない。

○○○○株式会社は、CA の鍵を寄託せず、加入者鍵の生成サービス及び証明書の一時停止サービスを提供しない[提供していないサービスのみ記載]。したがって、当監査法人の手続は、こ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

○○○○株式会社の経営者の責任は、認証局のための WebTrust の規準 v×. × 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、秘密保持並びに

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、国際品質管理基準の第1号を適用しており、したがって、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して文書化した方針と手続を含む、包括的な品質管理システムを保持している。

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、全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。したがって、手続には、(1)〇〇〇〇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機密保持、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すること、(2) 〇〇〇〇株式会社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。

内部統制の相対的有効性

〇〇〇〇株式会社の 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、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〇〇〇〇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。また、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 v×. ×に基づいて、×年×月×日から×年×月×日までの期間において、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。

この保証報告書は、認証局のための WebTrust の規準 v×. ×が対象としている範囲を超えて、〇〇〇〇株式会社の CA 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〇〇〇〇株式会社の CA 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

〇〇〇〇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

(注) 受託会社監査人が電子署名を行う場合には、保証報告書にその氏名を表示すると考えられる。

付録 A

対象 CA

Root CAs
CA # CA名
OV SSL Issuing CAs
CA # CA名
EV SSL Issuing CAs
CA # CA名
Private Trust Issuing CAs
CA # CA名
Non-EV Code Signing Issuing CAs
CA # CA名
EV Code Signing Issuing CAs
CA # CA名
Secure Email (S/MIME) CAs
CA # CA名
Document Signing CAs
CA # CA名
Adobe CAs
CA # CA名
Timestamp CAs
CA # CA名

Other CAs										
CA #	CA名									
対象 CA の識別情報										
No.	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	ダイジェストアルゴリズム	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
1										
										以 上

《 2. 認証局のための WebTrust の経営者の記述書（期間評価）の記載例》

<u>経営者の記述書</u>	
	×年×月×日
	○○○○株式会社 代表取締役○○○○ ○○担当取締役○○○○ [適切な責任者とする]
<p>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。</p> <ul style="list-style-type: none"> ・ 加入者の登録 ・ 証明書更新 ・ 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 ・ 証明書の一時停止 	

- ・ 証明書の審査
- ・ 加入者鍵の生成と管理
- ・ 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。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可能性がある。

当社の経営者は、当社の CA（場所）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 v×. ×（the WebTrust Principles and Criteria for Certification Authorities v×. ×）に準拠して、×年×月×日から×年×月×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「○○○○○○認証局運用規程 Version×」及び「証明書ポリシー-Version×」[該当する場合]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有効な内部統制を維持していた。
 - ・ 当社の（各 CA 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、（各 CA の）証明書ポリシー[該当する場合]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 v×. ×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 (該当する場合)

CA のビジネス実務管理

- ・ 証明書ポリシー管理 (該当する場合)
- ・ 認証局運用規程の管理
- ・ CP 及び CPS の一貫性 (該当する場合)

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
- ・ CA 鍵の寄託 (該当する場合)

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 (サポートされている場合)
- ・ CA が提供する鍵保存及び復旧サービス (サポートされている場合)
- ・ IC カードライフサイクル管理 (サポートされている場合)
- ・ 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
- ・ 証明書更新 (サポートされている場合)
- ・ 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
- ・ 証明書の一時停止（サポートされている場合）
- ・ 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、加入者鍵の生成サービス及び証明書の一時停止サービスを提供しない[提供していないサービスのみ記載]。したがって、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

対象 CA

Root CAs
CA # CA名
OV SSL Issuing CAs
CA # CA名
EV SSL Issuing CAs
CA # CA名
Private Trust Issuing CAs
CA # CA名
Non-EV Code Signing Issuing CAs
CA # CA名
EV Code Signing Issuing CAs
CA # CA名
Secure Email (S/MIME) CAs
CA # CA名
Document Signing CAs
CA # CA名
Adobe CAs
CA # CA名
Timestamp CAs
CA # CA名
Other CAs
CA # CA名

対象 CA の識別情報

No.	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	ダイジェストアルゴリズム	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
1										

以 上

以 上

- 本研究文書（2022年10月13日改正）は、次の公表物の公表に伴う修正を反映している。
 - － 保証業務実務指針（序）「保証業務実務指針及び専門業務実務指針並びに関連する公表物の体系及び用語」（2022年7月21日公表）