2019年度
実務者説明会(説明会資料抜粋)

日時：2020年2月17日(月) 14時～16時

場所：六本木ファーストビル１階（第１～3会議室）

（東京都港区六本木1丁目9番9号）

一般財団法人日本情報経済社会推進協会

電子署名・認証センター

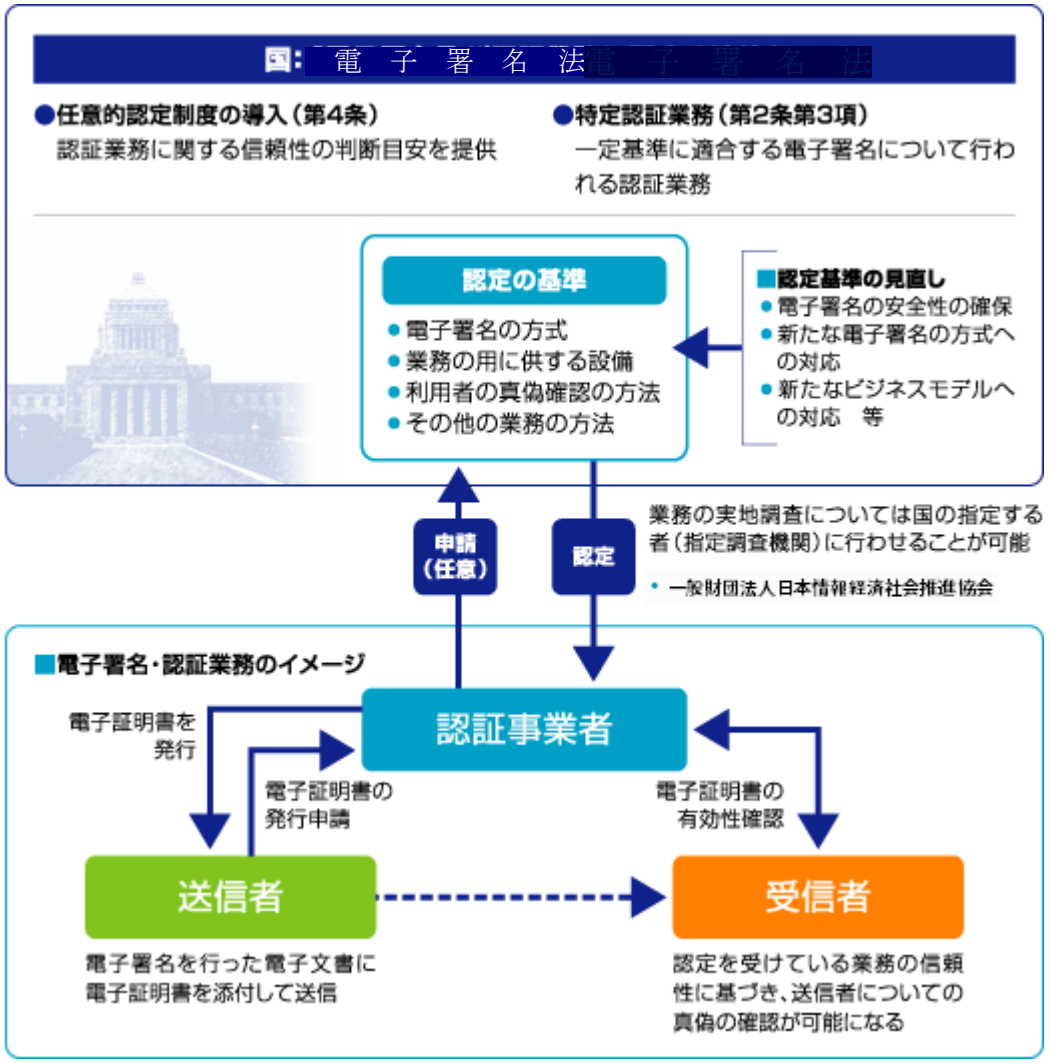
JIPDEC

目次

1. 電子署名法と変更認定

(1) 電子署名法第3条の「電磁的記録の真正な成立の推定」を支える特定認証業務に関する認定の制度
(2) 認定の基準に関する電子署名法等の条文
(3) 変更認定に関する電子署名法等の条文
(4) 変更認定の考え方
(5) 変更認定の実施、及び問合せ状況
(6) 変更認定が不要となった事例

(1)電子署名法第3条の「電磁的記録の真正な成立の推定」を支える特定認証業務に関する認定の制度



特定認証業務の認定を受けるためには、どのような技術・設備水準が必要なのか示されており、電子署名の方式や業務の用に供する設備、利用者の真偽確認の方法等が定められ、こうした認定を受けた認証局が発行する電子証明書は、一定レベルの信頼性を保ったものだと判断される。

(2) 認定の基準に関する電子署名法等の条文

電子署名法第四条（認定）

特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。

2　前項の認定を受けようとする者は、主務省令で定めるところにより、次の事項を記載した申請書その他主務省令で定める書類を主務大臣に提出しなければならない。

一　氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

二　申請に係る業務の用に供する設備の概要

三　申請に係る業務の実施の方法

電子署名法第六条（認定の基準）

主務大臣は、第四条第一項の認定の申請が次の各号のいずれにも適合していると認めるときでなければ、その認定をしてはならない。

一　申請に係る業務の用に供する設備が主務省令で定める基準に適合するものであること。

二　申請に係る業務における利用者の真偽の確認が主務省令で定める方法により行われるものであること。

三　前号に掲げるもののほか、申請に係る業務が主務省令で定める基準に適合する方法により行われるものであること。

※ 解説

電子署名法第六条で定められた「認定の基準」は、さらに施行規則や指針・方針に落ちてきて、より具体的で細かな判断基準が定められ、事業者が実施している業務一つ一つに展開されている。

＜凡例＞

○設備の要件・・青字で記載

○真偽確認方法・・マゼンタで記載

○業務の方法・・緑字で記載

(3) 変更認定に関する電子署名法等の条文

電子署名法 第九条（変更の認定等）

認定認証事業者は、第四条第二項第二号又は第三号の事項を変更しようとするときは、主務大臣の認定を受けなければならない。
ただし、主務省令で定める軽微な変更については、この限りでない。

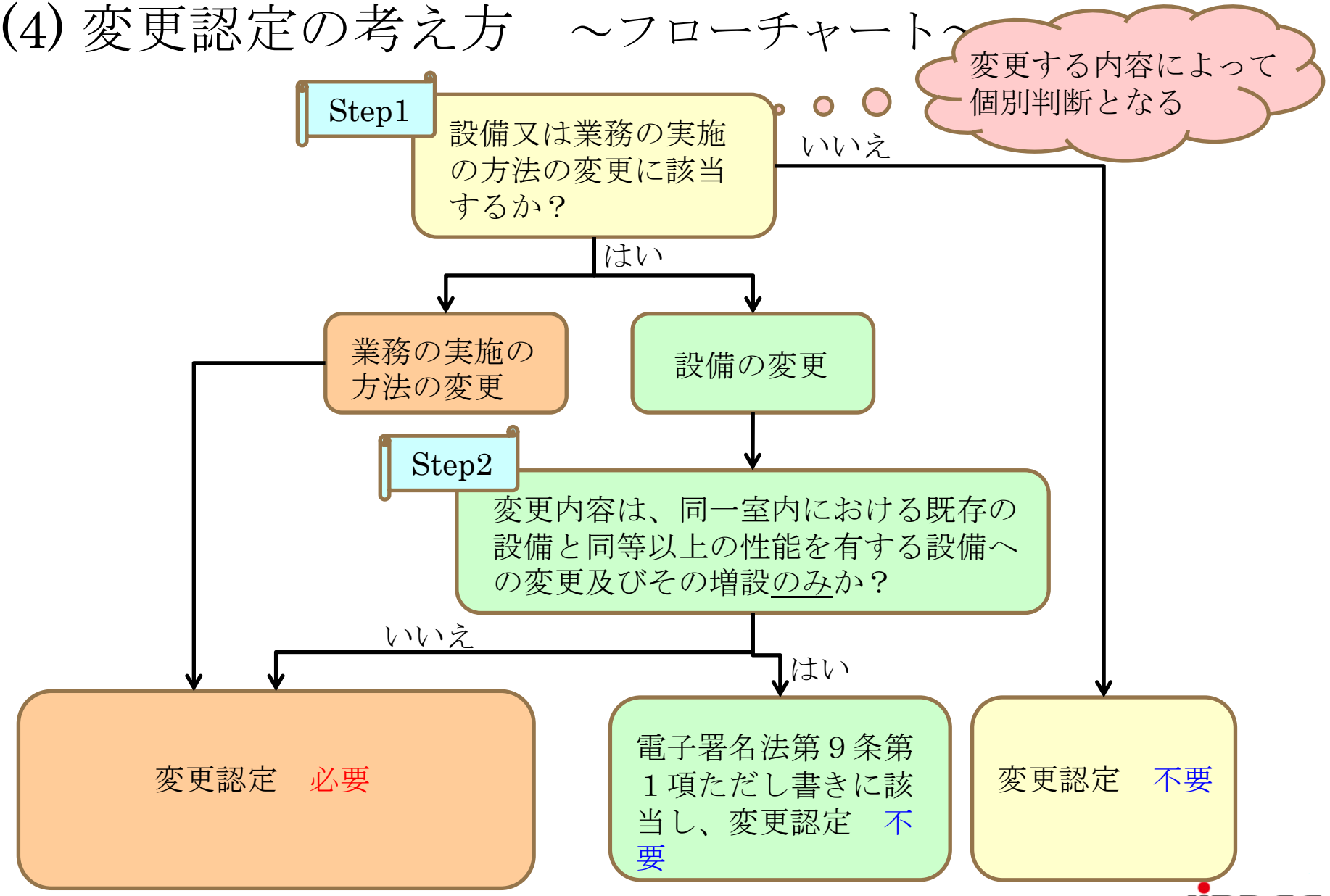
電子署名法 第四条第二項第二号又は第三号

二　申請に係る業務の用に供する設備の概要
三　申請に係る業務の実施の方法

施行規則 第九条（軽微な変更）

電子署名法第九条第一項ただし書の主務省令で定める軽微な変更は、同一室内における既設の設備と同等以上の性能を有する設備への変更及びその増設とする。

(4) 変更認定の考え方　～フローチャート～



(5) 変更認定の実施、及び問合せ状況

- 実施状況（2019年度）
  - 業務の実施方法変更に伴う変更認定0件
  - 設備の変更に伴う変更認定1件

- 問合せ状況（2019年2月1日～2020年1月31日）
  - 認定認証事業者からの全問合せの内、変更認定に関する問合せの割合は約53%

(6) 変更認定が不要となった事例

昨年(2019年2月)の実務者説明会以降の問合せで、事業者が特定されず、かつ汎用的に参考となる事例を抽出し、変更認定は不要であると判断された事例を紹介する。

なお、施行規則第十二条第一項第四号ホに基づき、認証業務用設備及び施行規則第四条各号（変更の対象となる設備や装置等が該当する号）の基準に適合するために必要な設備の維持管理に関する記録を作成、保存し、更改後の更新調査時に指定調査機関による確認を受ける。

＜業務系＞

① 電子委任状法対応 (電子署名法に関する業務の方法の変更がない場合)

② 暗号アルゴリズム移行完了に伴う措置等

③ CPSに記載の連絡先窓口の部署名等の変更

＜設備系＞

④ 登録用端末設備の設置場所変更

⑤ HSMの更改

(6)変更認定が不要となった事例　－業務関係－

① 電子委任状法対応 (電子署名法に関する業務の方法の変更がない場合)

（質問）
　電子委任状の普及の促進に関する法律への対応として、電子証明書に代理権に関する項目を属性として記載することは、変更認定に該当するか。

（回答）
　電子署名法第四条第二項第三号の事項についての変更に当たらないのであれば、変更の認定は不要である。具体的な内容について、指定調査機関に相談して欲しい。
　なお、CP/CPSに記述する電子委任状法に対応していることを示すための事項については、電子署名法による認定の対象外であるが、不明瞭であったり他の記述と齟齬のある記述であったりすると認証業務に対する信頼性を損なうおそれを否定できないため、明確かつ適切に記述して欲しい。

(6)変更認定が不要となった事例　－業務関係－

② 暗号アルゴリズム移行完了に伴う措置等

（質問）
　暗号アルゴリズムの移行について、SHA-1withRSAで署名された全ての利用者電子証明書の有効期限が切れるため、CP/CPS及び規程類の修正を行うが、変更認定に該当するか。

（回答）
　業務において発行された「SHA-1withRSAで署名された利用者電子証明書」の有効期間がすべて満了を迎える場合、実情に即してCP/CPS及び規程類の記述を修正することについては、業務の実施方法の変更とまでは言えず、変更認定は不要である。

(6)変更認定が不要となった事例　－業務関係－

③ CPSに記載の連絡先窓口の部署名等の変更

（質問）
　CPSに記載の連絡先窓口の組織名称等を変更することとなった場合、変更認定に該当するか。

（回答）
　法人名称の変更であれば、法第九条第四項のとおり、主務大臣への届け出が必要となる。また、規則第六条第一項第十三号に基づき、指針第十二条第一項第一号では「認証業務の実施に関する規程」の掲載事項として、事業者の名称及び連絡先の規定を求めている。したがって、CPSに記載されている事業者の名称に変更があった場合、CPSの該当箇所を修正する必要があるが、業務の実施方法の変更とまでは言えず、変更認定は不要である。

(6)変更認定が不要となった事例　－設備関係－

④ 登録用端末設備の設置場所変更

（質問）
　登録用端末設備の設置場所を変更することは、変更認定に該当するか。
　なお、新しい設置場所は、現在の設置場所同様、指針第四条第二号に規定されている「関係者以外が容易に登録用端末設備又は利用者識別設備に触れることができないようにするための施錠等の措置」が講じられる。

（回答）
　登録用端末設備の設置場所変更のみの場合は、設備の概要の変更に該当しないため、変更認定は不要である。
　ただし、設置場所変更に伴って、設備を増設したり、不正なアクセス等を防止する措置を変更したりする場合は変更認定が必要になるため、あらかじめ変更認定の必要性を問い合わせること。

(6)変更認定が不要となった事例　－設備関係－

⑤ HSMの更改

（質問）
　HSMの老朽化に伴い、現在のHSMと同等以上の性能をもつHSMに更改することは、変更認定に該当するか。

（回答）
　現在のHSMと同等以上の性能をもつ装置に変更することは、電子署名法第９条第１項ただし書きの軽微な変更に該当するため、変更認定は不要である。
　ただし、HSMの変更に伴い、発行者署名符号の生成手順を変更する場合や、複数の者による発行者署名符号の作成及び管理その他当該発行者署名符号の漏えいを防止するために必要な措置を変更する場合など、他の要件を変更する場合は変更認定が必要になるため、あらかじめ変更認定の必要性を問い合わせること。

2. 認定認証業務の品質維持等に向けた情報共有

2.1 業務関係

(1) 規程・手順の適切な作成と遵守
(2) 誤発行等の事例紹介
(3) 遅滞なく失効すべき事例
(4) 電子証明書の重複発行（失効漏れ）
(5) 失効通知
(6) 帳簿書類の保存状況
(7) 更新調査中、更新の認定前のCP/CPS改定、公開

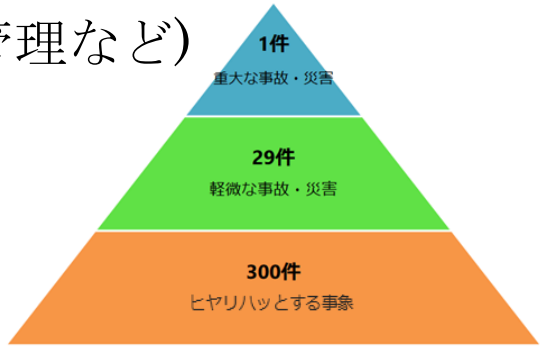
2.2 設備関係

(1) ログ欠損
(2) 不適切な権限設定
(3) 設備更改時の設定漏れ

2.3 障害時の対応

(1) 規程・手順の適切な作成と遵守(1/2)

- 電子署名法に対する不適合の予防
  - 規程・手順の遵守、業務の実態に即した見直し
  - 業務の実施記録の帳簿には、実施日付、実施者、責任者（＊）
- (参考) ハインリッヒの法則 (労働災害、品質管理など)
  - 重大事故・災害1件の陰に
    - 29件の軽微な事故・災害
    - 300件のヒヤリハット
      (事故にいたらない、ヒヤリ ハッとする事象)
  - **重大事故の防止には、ヒヤリハットの撲滅**



＊責任者を記録する必要がある帳簿
（調査項番4106、4108、4109、4204、4301～4305、4404～4407）

(1) 規程・手順の適切な作成と遵守(2/2)

- 電子署名法に対する不適合の予防:
  - 規程・手順の遵守、業務の実態に即した見直し、情報共有
    - 規程・手順の見直しの意図、理由、背景を共有し検討する。
    - 規程・手順の教育では、関連する施行規則や指針等の条文を提示し、電子署名法を遵守する重要性を認証業務全体で共有する。
    - 日常的、定期的に、違反には至らなかった「ヒヤリハット事例」を収集し、共有(朝礼・終礼・小集団活動など)
    - 規程・手順が不明瞭であったり、要員が理解し辛かったりした場合等、規定された内容が適切に共有、認識されるよう迅速に検討し改訂する。
    - リスク検出を容易にするために、チェック項目の追加や表現形式の変更等により、作業記録様式を改善する。
  - 業務の実施記録の帳簿には実施日付、担当者、責任者を記録
    - 担当者に対する責任者の管理・監督
      - 実施前の可否判断
      - 実施後の可否判断
      - 規定された記録の保存場所の徹底

(2) 誤発行等の事例紹介

- 誤発行のリスク要因と原因例
  - データベースの修正ミス
    - 利用者が入力したデータに基づく利用申込書に、手書きの訂正が2個所あるときに、1箇所のみをデータベースに反映
    - 利用申込書の手書き訂正をデータベースに反映する際、別文字も誤削除
  - 規定遵守の軽視
    - 利用者の真偽の確認日において、真偽確認用の住民票の写しが、CP/CPSに規定した発行を受けてから3ヶ月を経過していることに気付きながらも、再提出を求めることなく電子証明書を発行
  - 計算による法人番号
    - 個人事業主について商号の登記事項証明書の「会社法人等番号」をもとに「法人番号」を計算して、電子証明書に記録
- その他のリスク要因と原因例
  - 住民票の写しのマイナンバーの墨塗り忘れ
    - 事務取扱要領等に規定したがチェックリストに無く見落とし

- 間違いやすい文字の例

漢字変換誤りや類似文字の選択誤り

娑 ⇒ 裟、 弍 ⇒ 弐、 紘 ⇒ 絋、 予 ⇒ 与、
進 ⇒ 新、 奬 ⇒ 獎、 瑞 ⇒ 端、 舗 ⇒ 舗

利用者氏名/住所ローマ字等の誤り (実例)

Higashimiya-machi ⇒ Higashimiyamachi　Kasai-shi ⇒ Kosai-shi
Oaza- ⇒ Oza　Ikuo ⇒ Ikuko　jo ⇒ joh
プランニンブ ⇒ プランニング　ピーアンドージー ⇒ ピーアンドジー
○ジィコート ⇒ ○ジィーコート　○ニーブル ⇒ ○ニブール
下馬 ⇒ 下場　睦○ ⇒ 陸○　○夫 ⇒ ○男　○弘 ⇒ ○広　○並 ⇒ ○波
明 ⇒ 昭　常盤 ⇒ 常磐　教会 ⇒ 協会　貨物 ⇒ 貸物
Taro Yamada□ (□:タブ文字) ⇒Taro Yamada　サーベー(べが平仮名)⇒サーベー
○○ ⇒ ○・○（建物名）　○丁目○番○号 ⇒ ○丁○番○号（一部地域）
○○@○○1g.jp ⇒ ○○@○○lg.jp

(3) 遅滞なく失効すべき事例

- 発生した事象:

事象1: 3か月以上前に発行した電子証明書について記録内容誤りの通知があり、当日中に誤りを確認したが、失効申請書の提出を待って、通知受信の22日後に失効

事象2: 新規発行の電子証明書について記録内容誤りの通知があり、当日中に誤りを確認したが、受領書(記載内容誤りの通知) の提出を待って、通知受信の7日後に失効

- 適切な対応:
  - 上記のように、電子証明書の記録内容が事実と異なることを認証局が確認できた場合
    - 施行規則第六条第十号に従い、「電子証明書に記録された事項に事実と異なるものが発見されたとき」と判断し、認証局事由によって失効

(4) 電子証明書の失効漏れ

- 電子証明書に属性情報を記録している場合
  - 属性情報が変更となるときには利用者が失効申請書を提出することが必要
  - 利用者が、この場合に該当するにもかかわらず失効申請書を提出せずに、新たな利用申込書を提出
    - 利用者の住所が変更されていたために、認証局が、当該利用者に対して発行済みであることを検出できず、新たな属性情報が記録された電子証明書を発行

(5) 失効通知

- 失効事由の誤り(失効通知に記載する場合)
  - CRLには、失効事由に応じてReason Codeが記録されることとなっており、誤った内容の記録となった。
  - CRLの訂正は改ざんに該当し望ましくないとされていることから訂正はしていない。

- 失効通知の送付

  施行規則第六条第十二号

  第十号の規定により電子証明書の失効に関する情報を記録した場合においては、遅滞なく当該電子証明書の利用者にその旨を通知すること。

  – 通知方法の規定はないが、通知しないで良い例外規定はない。

(6) 帳簿書類の保存状況

- 調査の観点
  - 施行規則第六条第十五号へ(調査表項番3C51～3C56)
  - 施行規則第十二条(調査表項番4101～4407)

- 認証局外で保存している帳簿書類の保存場所の移転
  - 認証局外の本社組織等が管理している場合であっても、認証局として、適切に移転、保存されていることを確認すること
- 電磁的記録による帳簿書類を保存した設備の設置場所、アクセス制限の状況等
  - 従来紙で保管していた帳簿を、電磁的記録に変更する際には、当該保存場所（文書サーバの実際の保存場所やアクセス制御の状況等）について、更新調査時に実地調査が行われることに留意すること

(7) 更新調査中、主務大臣通知前のCP/CPS改定、公開

- 事象
  - 調査期間中、主務大臣通知を実施する前に、指定調査機関が調査した内容と異なる改訂を行ったCP/CPSを公開した。
- 問題点
  - 認定の更新に際しては、提出された最新のCP/CPSと共に、調査結果を主務大臣に通知している。主務省では当該通知に基づいて認定の更新について判断している。調査した内容と異なるCP/CPSが公開されると、指定調査機関からの通知内容と差異が発生し、適合の判断根拠が不明瞭になる。また、指定調査機関が虚偽の内容を主務大臣に通知したことにもなり、調査結果の通知の信頼性が揺らぐ。
- お願い事項
  - 更新調査中、主務大臣通知前（調査完了通知書によるご連絡前）の改訂が必要となった場合は、必ず早めに指定調査機関にご相談ください。

2.2 設備関係

(1) ログ欠損(1/4)

- 事象
  - 認定更新日の6カ月前に作成したWindowsのイベントログが欠損
  - 認定更新日の10カ月前に作成したＩＣカード 発行 ログが欠損
- 問題点

  施行規則第十二条第一項第四号ハに規定されている認証業務用設備の動作に関する記録である、Windowsのイベントログ及びＩＣカード 発行 ログが、施行規則第十二条第三項に規定されている期間保存されていなかった。
- 関係法令、適合例
  - 施行規則第十二条第一項第四号ハ

    認証業務用設備の動作に関する記録
  - 施行規則第十二条第三項

    第一項第四号に掲げる帳簿書類は、作成した日から認定の更新の日まで保存しなければならない。

2.2 設備関係

(1) ログ欠損(2/4)

原因	対策例
ログサイズ見積誤り	・適切なログサイズの見積とログサイズ設定 ・ログのアーカイブ出力 ・定期的（1～2週間ごと）なログのバックアップ、ログ内容の確認
人為的ミス	・操作手順書の整備 人為的ミスを減らすための明確かつ適切な手順の記述、チェックシートの効果的利用 ・定期的（1～2週間ごと等）に記録内容を実際に確認し、直近の作業記録が遺漏なくログとして残されているか確認 ・複数人による作業・確認 ・定期的な教育 ・自動化
ディスク障害	・定期的（1～2週間ごと）なログのバックアップ ・ログをRAID構成のディスクで管理
Windows Updateによるログ欠損（Windows10）	・Windows Update前のバックアップ ・操作手順書の整備

2.2 設備関係

(1) ログ欠損(3/4)

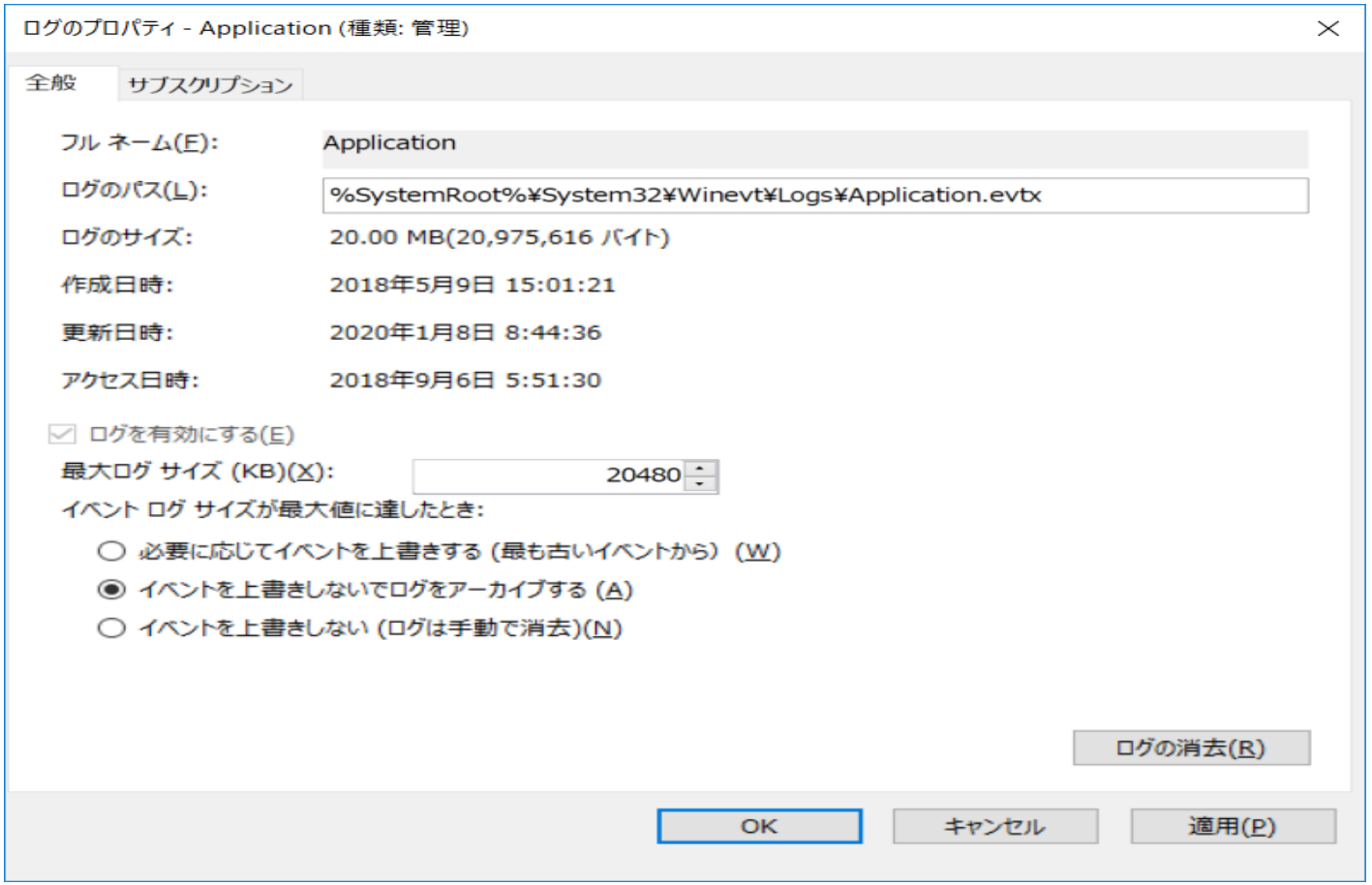
原因	対策例
原因不明のイベントログ記録停止（Windows10） ・ログをアーカイブするタイミングで、ログ記録停止（再現性なし） ・Windowsのイベントログを大量に出力する際のOSのバグと考えられるが詳細不明	・可能な限りログサイズを大きくする。 ・適切にログが取られていることを一定期間確認 ・ログインまたはログアウト時にログを別サーバへ飛ばす。

2.2 設備関係

(1) ログ欠損(4/4)

- ログのアーカイブ出力設定

イベントログの設定画面



2.2 設備関係

(2) 不適切な権限設定(1/2)

- 事象
  - 退職により認証設備室の入退室権限がなくなった者が、認証設備室の入退室管理装置に登録された設定のままであった。

- 問題点
  - 認証設備室に入退室権限がない者が、入退室できることから、施行規則第六条第十六号で規定される「認証業務用設備が設置された室への立入り」に関する許諾が適切に行われていなかった。

- 関係法令、適合例
  - 施行規則第六条第十六号

    認証業務用設備により行われる業務の重要度に応じて、当該認証業務用設備が設置された室への立入り及びその操作に関する許諾並びに当該許諾に係る識別符号の管理が適切に行われていること。

2.2 設備関係

(2) 不適切な権限設定(2/2)

原因	対策例
権限変更時の設定漏れ	・権限変更時、複数人による設定変更確認 ・定期的な権限設定確認 ・設定確認時、最新の体制表と権限設定の整合性確認

2.2 設備関係

(3) 設備更改時の設定漏(1/2)

- 事象
  - CAサーバとDBサーバ間の通信の暗号化で使われるハッシュ関数が、設計書に規定されていたSHA-256ではなくMD5が使用されていた。
- 問題点

  指針第五条第二号に基づく適合例1221に「事務取扱要領等に明確かつ適切に規定し、その規定を満たす認証業務用設備を設置」とあり、ハッシュ関数が規定されていた設計書の設定（SHA-256）とCAサーバの設定（MD5）に齟齬があった。
- 関係法令、適合例
  - 適合例1221

    (1) 以下の(2)、(3)の事項に関して、事務取扱要領等に明確かつ適切に規定し、その規定を満たす認証業務用設備を設置している。
  - 適合例1222

    (2) 認証業務用設備が２以上の部分から構成され（例えば、発行業務に用いる設備と登録業務に用いる設備に分かれている場合）、外部ネットワークを経由して接続されている場合、当該設備間の通信に関して、各設備の誤認並びに通信内容の盗聴及び改変を防止する措置を講じている。

2.2 設備関係

(3) 設備更改時の設定漏(2/2)

原因	対策例
サーバ更改時の設定漏れ	• サーバの設定書の作成 • 設定変更時の設定書への反映 • 更改時、複数人で設定書の内容をサーバに設定

2.3 障害時の対応

1. 障害報告書提出

①経緯（いつ、誰が、何を、どのように）

②直接的原因～動機的原因(直接的原因を見逃した理由)

– 「なぜなぜ分析」

  - 問題を起こした要因に対し、さらにその要因に対する要因を問うことを繰り返し対策の効果を検証する

③障害期間中、問題ないことの確認内容

– 障害期間中、不正操作がなかったことをログ、作業記録等を使って説明(更新調査で詳細に確認する場合があります)

④類似事故、障害の可能性検討、問題のないことの確認内容

⑤是正の手順、再発防止策

– 対策（いつからを含む）
  再発の可能性が高い事象には、発生時の対応手順作成

– 教育の実施状況

⑥規程、手順、マニュアル等の改定内容（改定日含む）

2.改定された規程、手順、マニュアル等の提出

3.教育記録の提出 (いつ、だれに、何を教育したかの記録提出)