平成29年度
実務者説明会(説明会資料抜粋)

日時：平成30年2月23日(金) 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

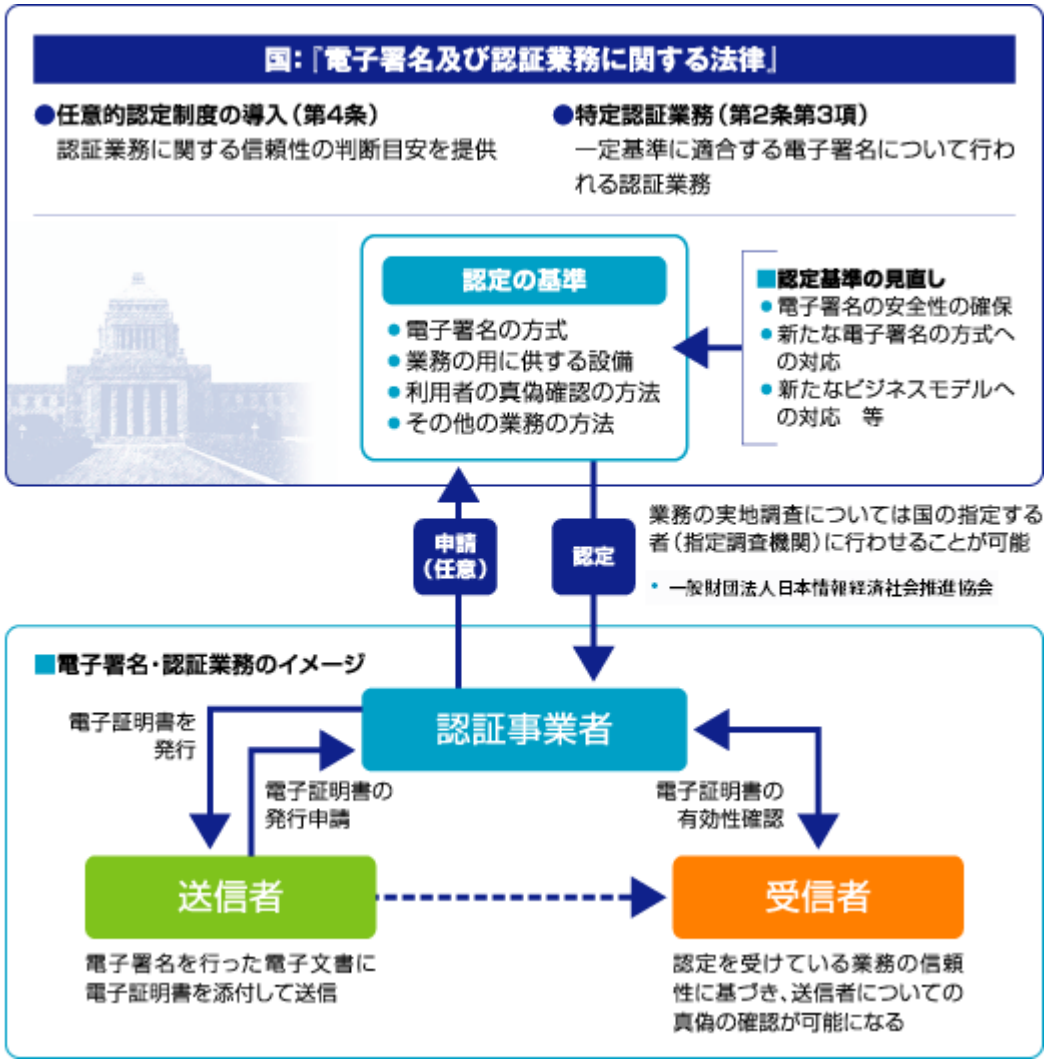
電子署名・認証センター

目次

1. 電子署名法と変更認定

(1) 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令等の条文
(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) 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令等の条文

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

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

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。

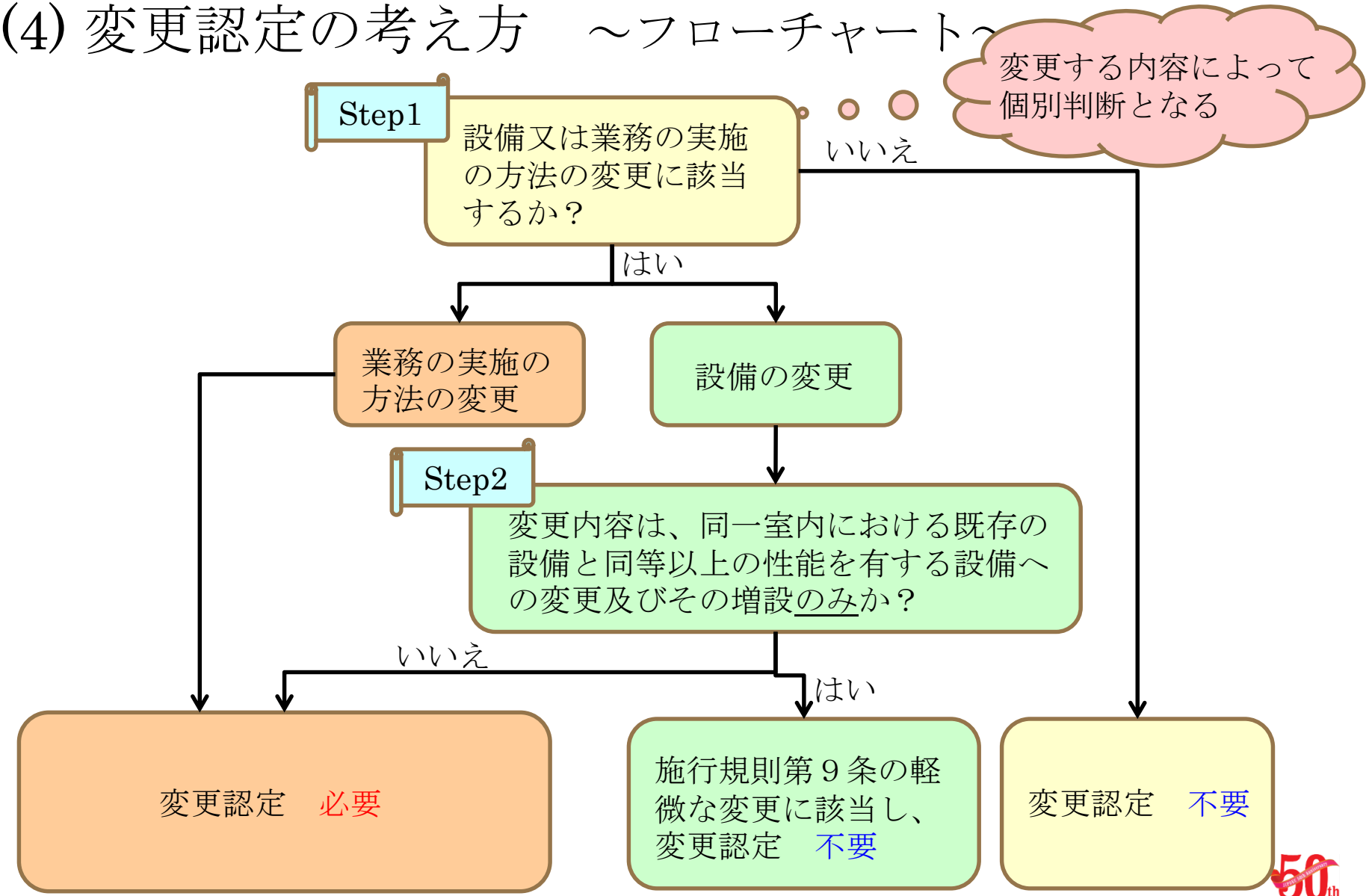
電子署名法 第四条第二項第二号又は第三号

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

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（2017年度）

・業務の実施方法変更に伴う変更認定2件

・設備の変更に伴う変更認定1件

○問合せ状況（2017年2月1日～2018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50%

分類	種類	変更認定に関する問合せの件数
業務	法人番号関連	6
	委託先の合併、事業譲渡等	4
	帳簿保管場所の移動・増設	3
設備	機器・設定変更	8
	部屋移動・変更	4

(6) 変更認定が不要となった事例

昨年(2017年)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法人番号を電子証明書に追加

②委託先の合併、事業譲渡

③IA,RAと異なる保管場所の変更、追加

＜設備系＞

④認証業務用設備のリプレース

⑤認証設備室の監視室の移転

(6)変更認定が不要となった事例

①法人番号を電子証明書に追加

(質問)

電子証明書に国税庁が発番する法人番号を格納するように変更するが、変更認定の対象か

(回答)

法人番号は、施行規則第六条第八号に規定された「利用者の役職名その他の利用者の属性」であり、電子署名法の認定の対象外であるため、変更認定は不要である。
ただし、業務の手順が変更になる場合に、その程度によっては、施行規則第六条第十五号イにより変更認定が必要になることもありうる。

(6)変更認定が不要となった事例

②委託先の合併、事業譲渡

(質問)
委託先企業のA社がＢ社に事業譲渡することとなったが、この場合変更認定は必要か

(回答)
業務の一部を委託する場合については施行規則第六条第十五号ハに規定するとおり、委託の範囲などを明確かつ適切に定め、実施する必要がある。
特定認証事業者から受託している業務に関連する事業に係る権利・義務の全部をＢ社が承継し，Ａ社と特定認証事業者が締結している委託業務契約の内容や委託元の指示の遵守及び責任分担，並びに委託元への定期的な報告等に変更が生じないのであれば、法第四条第二項第三号に規定する業務の実施の方法の変更には該当せず、基本的に変更の認定は要しないと思われる。
ただし、事業譲渡等の詳細によっては改めて検討する必要がある。

(6)変更認定が不要となった事例

③IA,RAと異なる保管場所の変更、追加

（質問）
帳簿書類について、RAやIAの立地とは異なる別の場所に移したいが、変更認定に該当するか。
なお、調査表項番3C56の要件（施錠可能な出入口、火災対策、直射日光対策等）は満たしており、また、運搬時も帳簿の漏洩、滅失毀損防止の対策を講じる。

（回答）
帳簿書類の保管方法に変更がなく、保管場所のみの変更であれば、法第四条第二項第三号に規定する業務の実施の方法の変更には該当せず、変更認定は不要である。

(6)変更認定が不要となった事例

④認証業務用設備のリプレース

(質問)
認証業務用設備の老朽化に伴い、現行の設備と同等以上の性能の、CAサーバ、RA端末、ネットワーク機器のリプレース、及びソフトウェアのバージョンアップを予定している。変更認定は必要であるか。

(回答)
CAサーバ、RA端末、ネットワーク機器等の認証業務用設備もしくは規則第四条第二号の基準に適合するために必要な設備のリプレース、及び当該設備に係るソフトウエアのバージョンアップは、現行のものと同等以上の性能を有している場合、施行規則第九条で定める軽微な変更に該当するため、変更認定は不要である。

(6)変更認定が不要となった事例

⑤認証設備室の監視室の移転

(質問)

認証設備室の不正侵入等を監視している監視室の移転、及び監視室の機器の移設を考えている。移設時は認証設備室に入室権限者２名以上を在室させ異常がないことを確認する。変更認定は必要であるか。

(回答)

移設した監視室及び機器は、現行のものと同等以上の性能を有している場合、施行規則第九条で定める軽微な変更に該当するため、変更認定は不要である。

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) 規程の適切な作成と遵守
(2) 誤発行の事例紹介
(3) 受領書(電子)のデータ消失とその対応
(4) CP/CPSにおける電子証明書プロファイルの記述
(5) 電子証明書の有効期間の開始日

2.2 設備関係

(1)調査時の指摘事項
(2)障害対応時の留意事項

(1)規程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
  - 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1件の陰に
    - 29件の軽度事故
    - 300件のヒヤリハット
      (事故に至らない、ひやり、はっとする事象)
  - **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)規程の適切な作成と遵守 (まとめ) (2/2)

- 電子署名法に対する不適合の予防:
  - 手順の遵守、業務の実態に即した見直し、情報共有
    - 手順の見直しの意図、理由、背景を共有し検討する。
    - 手順規程教育では、関連する施行規則や指針等の条文を提示し、法律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)
    - 手順が不明瞭ならば、迅速に検討し改訂する。
  - 業務の実施記録の帳簿には実施日付、担当者、責任者
    - 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(記録内容を精査の上で承認)
      - 規定された記録の保管場所の徹底

(2) 誤発行の事例紹介

- リスク要因と原因例
  - 外字、同音異語
  - 外部データの活用 (利用者による入力データなど)
  - データ入力誤りの訂正漏れ
    - 漢字氏名の誤入力を修正したが、ローマ字氏名の誤入力を修正忘れ
  - PIN印字不鮮明
    - ドットインパクトプリンタ印字時における圧力設定忘れ
  - システムテスト後の設定誤り
    - 電子証明書プロファイル変更時にテスト環境で発行者名称を“○○ TEST CA”としてテストを実施、本番環境にプロファイルをそのままコピー
  - 真偽確認に使用すべき公的書類の不備の見逃し
    - 有効期限、「印鑑登録証明書」と「印鑑証明書」の誤認
- 対策案:
  - 手順を適切に規定
    - システム変更時の手順検討も適切に実施
  - 規定された手順に従って愚直、厳格に実施
    - 真偽確認書類との目視照合

- 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⇒紘、 予⇒与、
進⇒新、 奨⇒奬、 瑞⇒端

利用者氏名/住所ローマ字等の入力誤り (実例)

Higashimiya-machi⇒Higashimiyamachi　Kasai-shi⇒Kosai-shi
Oaza-⇒Oza　Ikuo⇒Ikuko　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　常盤⇒常磐　教会⇒協会　貨物⇒貸物

- 対策案
  - 読合せの読み上げ方の検討
  - 間違いやすい文字についてノウハウの蓄積
  - 拡大表示
    - ルーペ利用、他のアプリにコピペし大フォントで表示など

(3) 受領書(電子)のデータ消失とその対応

- 事象
  - 受領書データを受領後、①～③の処理を個別のスクリプトで実施していた事例
    - ①データ転送、②バックアップ、③受領ポイントから削除
  - 上記①～③の処理を停止する必要が生じた際に、①②のみを停止し、③の停止を漏らした。このため、数日分の受領書データが消失した。
- 対応
  - 指定調査機関に相談の上、専門業者と守秘義務契約を締結してHDDからのデータ復旧を依頼 → 復旧できず
  - 受領書データを受信していたサーバのログから、送信者を特定し、該当する利用者に再送信を依頼 → 全員から受領書を再受領
- 再発防止策
  - スクリプトの構成やバックアップの保存方法と手順を見直し、教育実施

(4) CP/CPSにおける電子証明書プロファイルの記述

(a) プロファイルを変更した際（証明書記載事項に法人番号、住所等を追加等）には、新しいプロファイルによる電子証明書の発行開始時期を明記する

✓ 追加したプロファイルが記載されていない有効な電子証明書について、CP/CPSとの不整合を防止する

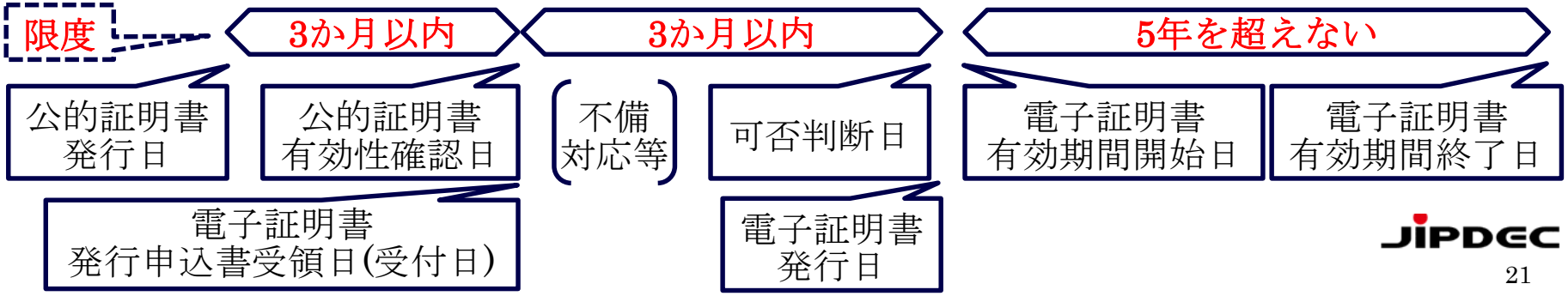
(b) URLの記載誤りの事例

- URLのpath部分は、大文字小文字が区別される
  (修正前) https://example.jp/**NINTEI**
  - ✓ (修正後無効) https://example.jp/**nintei**
- “https://～”とすべきところを“http://～” と記述し、電子証明書の記録内容と不整合

(5)電子証明書の有効期間の開始日

「電子署名法研究会（平成26 年度第4 回）-議事要旨」より抜粋
http://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/h26_04_giji.html

- 公的証明書の有効期間を3ヶ月以内とすることである程度歯止めがかかる
- ずっと電子証明書の発行を溜め込んでいて、1年後に発行するというのはいけないが、3ヶ月というのがリーズナブルな範囲
- 発行の申請を受け付けて、実際に電子証明書を発行するまでに、いくら期間が空いていてもよいわけではない
- 有効期間の起算点というのは、様々な考え方があるため、5年を超えないという5年をどこで判断するのかというのは、電子証明書に記載されている発行日から最大5年を超えていなければよしとする



2.2 設備関係

(1) 調査時の指摘事項

①ログ欠損（6件）

②不適切な権限設定（2件）

③不適切なパスワード管理（1件）

(1) 調査時の指摘事項　－指摘に関連する法令－

指摘事項	施行規則	
①ログ欠損	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を保存しなければならない。
②不適切な権限設定	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。
③不適切なパスワード管理	同上	同上

(1) 調査時の指摘事項　－状況－

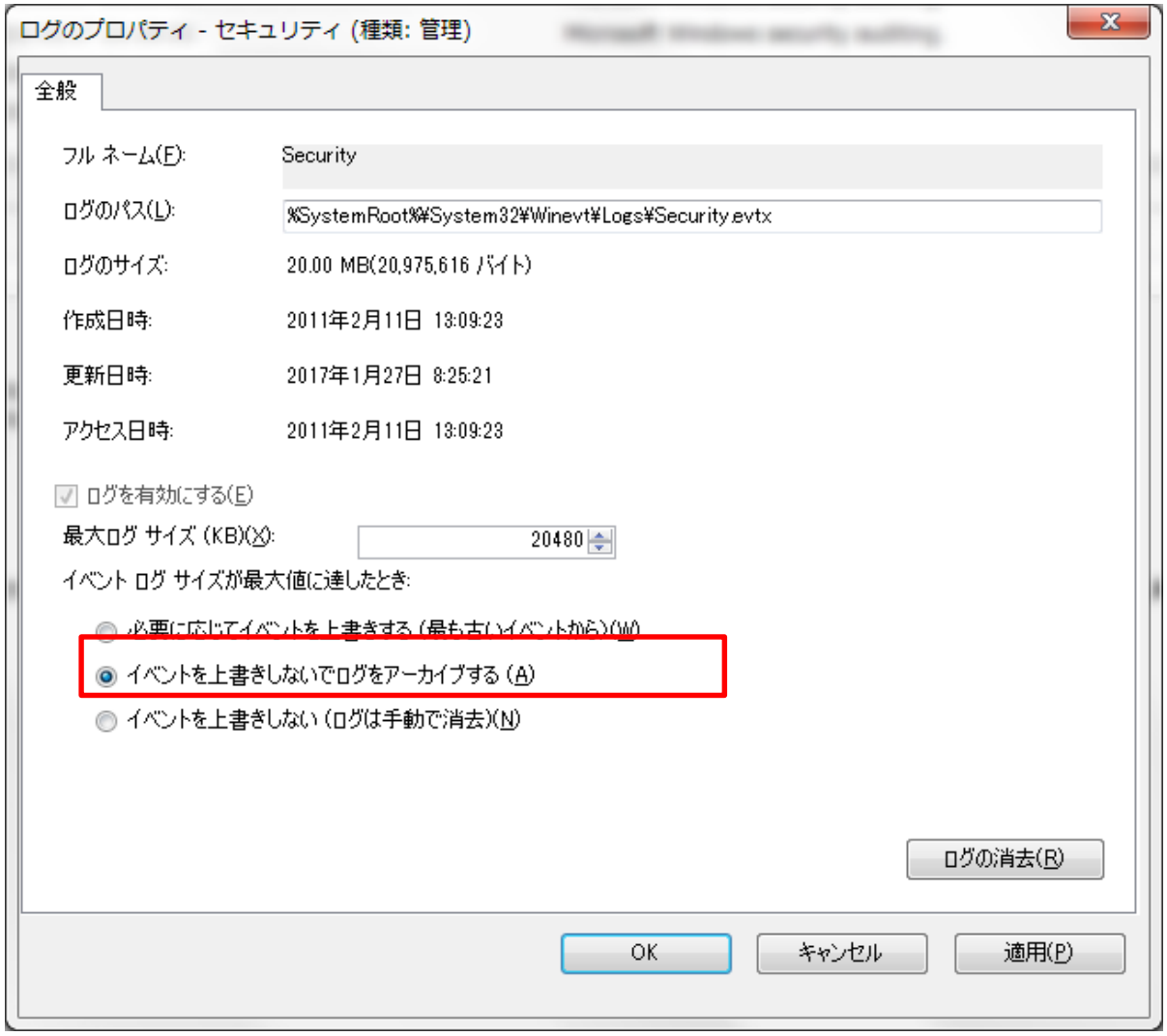
指摘事項	件数	期間	原因
①ログ欠損	6	数日～10ヶ月	・ログサイズ見積もり誤り ・人為的ミス ・ディスク障害
②不適切な権限設定	2	数ヶ月～1年	・権限変更時の設定漏れ
③不適切なパスワード管理	1	調査時の1日	・規程の遵守・理解不足

(1) 調査時の指摘事項　－対策例－

指摘事項	原因	対策例
①ログ欠損	・ログサイズ見積もり誤り	・適切なログサイズの見積もりとログサイズ設定 ・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構成のサーバで管理
②不適切な権限設定	・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
③不適切なパスワード管理	・規程の遵守・理解不足	・法令及び規定内容の定期的な教育

(1) 調査時の指摘事項　－ログのアーカイブ出力設定－

イベントログの設定画面

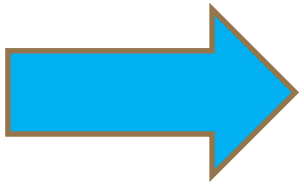


(2) 障害対応時の留意事項

①事前に定められた障害発生時対応手順書等に従って対応

②障害報告書の内容

- 状況
- （真の）原因
- 影響範囲



5W1H（いつ、どこで、誰が、何を、なぜ、どのように）を記述

ログ欠損や不適切な権限設定の期間に、不正操作がないことの確認

- 対応
- 再発防止策（教育含む）

3.非常事態発生時の情報共有手段の整備

○目的

非常事態（大規模災害、暗号アルゴリズム等危殆化）発生時の特定認証業務の状況を、迅速・的確に情報共有する。

○目標

大規模災害発生、3日後、2週間後、3ヵ月後の被害状況・復旧状況を把握できること

○対応内容

指定調査機関：

・特定認証事業者の緊急連絡先の管理
・特定認証事業者への被害状況・復旧状況連絡依頼
・被害状況・復旧状況連絡受付、情報整理
・主務省への被害状況・復旧状況連絡

特定認証事業者：

・指定調査機関への被害状況・復旧状況連絡

○今年度の訓練実施と結果概要

想定時間	特定認証事業者	指定調査機関	主務省
		①メール送付 趣旨説明、訓練の協力依頼、 代替連絡先の提供依頼	
①の翌営業日	②受信確認メール		
①の1週間後	③代替連絡先メール （通常の連絡手段が使用できない場合の連絡先）		
		④訓練終了結果メール	

経過日数	0	1	2	3	4	5	6	7
累計	7	7	7	8				

経過日数	0	1	2	3	4	5	6	7
累計	4	6	6	7	7	7	8	

○訓練結果の評価

　情報共有のための連絡先確認が行えた。また、レスポンスもおおむね当初想定どおりであった。