社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（23）
2008／7／25

電子署名文書管理システム構築における課題と考察

高尾美由紀　林　紘一郎

情報セキュリティ大学院大学 〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
E-mail: {mgs063504, koichiro.hayashi}@iisec.ac.jp,

あらまし　電子署名法が施行されて７年が経過しているが、電子署名の普及は官公庁、建設業など特定の分野に留まっており、期待通りには進んでいない。普及を阻む原因のひとつとして「電子署名は解りにくい」との指摘がある。[1]本論文では一般の企業が電子署名文書の管理システムを構築する際に遭遇する問題点と解決策を分析し、電子署名普及のための課題について検討する。
また、本論文で分析の対象としている「一般ユーザ」とは一般企業におけるシステム企画担当・業務設計担当・システム運用設計担当を指し、これらのユーザに対して電子署名の理解を普及させるするための方策を検討する。

キーワード　電子署名文書、普及、購買、業務運用設計、一般ユーザー向けガイドライン、
ユーザーインターフェース

Examination of the issues in designing of electronic signature – documentation system

Miyuki TAKAO　Koichiro HAYASHI

Institution of Information Security　2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-shi, Kanagawa, 221-0835 Japan
E-mail: {mgs063504, koichiro.hayashi}@iisec.ac.jp

Abstract　Electronic signature and Digital timestamp are new technologies which provide high level integrity to digital data. But unfortunately, they are not well developed as expected.

They say one of the reason is both technologies are hard to understand for general users and there is not proper users guide. Governments and industry standards body promote several guidelines and about them. But most of guidelines are engineering guideline or operating rules for CA(Certificate Authority). They are not proper guideline for public users. In this thesis, first of all, I examine issues hard to understand about electronic signature and digital timestamp for general users. Key issues are as follows.

From above examination, I will contrive System Development Guideline for users which explain designing concept of operating rule in electronic signature documentation system. My proposal is add control items to ISO27001 Control Items Exhibit A. These items are management requirement about electronic signature and digital timestamp.

Keyword　Electronic Signature Document, Diffusion, Purchase, Designing Business Opereration, Implementation Guide for Users, User Interface

1. はじめに

筆者は電子署名関連業務を担当して約８年となる。この間に電子署名法、IT一括書面法、e-文書法などが施行されているが、電子署名の普及状況は当初期待された通りには普及していない。普及されている業種は官公庁・建設業と限られており、筆者の担当業種である金融業や一般事業法人においては普及率は低い。しかし電子署名に関する様々な照会は少なからず受けており、普及率が低

[1] 「電子署名普及に向けた調査検討報告書」H18.3 次世代電子商取引推進協議会

い業種においても電子署名に対する関心はそれなりにある。

では普及を阻害する要因は何か。様々な指摘がされているが、阻害要因の一つとして「電子署名はわかりにくい」との指摘がある。

筆者の過去の業務経験を通じても、このような意見は非常に多かった。この点は解決するべき最優先課題だと考えている。ではこの状況を改善するためにはどのようにしたら良いか。

対応策を検討するために、一般ユーザにとってわかりにくい点を次項から検証する。

2. 【現状分析１】一般ユーザにとって難解な点

電子署名があまり普及していない業種の企業が電子署名文書管理システムを構築する際に、第一に直面する問題が「何をしたら良いかわからない」「電子署名文書の管理システム構築と、通常の電子文書の管理システム構築との違いがわからない」という点である。

これらの漠然とした疑問を分析していくと、難解な点は以下のように整理される。

(1)購買
- ・何を購入しなければならないか
- ・システム開発は誰に、何を依頼すればよいか
- ・電子証明書とは何か、どこから入手するのか

(2)業務運用設計
- ・電子署名、電子証明書の管理方法
- ・電子署名文書の管理方法
- （通常の電子文書との違い）

次項以降、それぞれの点について考慮するべき点、検討点を分析する。

2.1. 購買

電子署名文書管理システムを構築する場合、購買は次の５点について検討が必要となる。（図 1:電子署名文書管理システム構築における購買）

(1)システム構築　（証明書インターフェース、電子署名／タイムスタンプの付与・検証、電子文書の作成、業務システムとのインターフェース）
(2)ハードウェア（HSM、セキュアサーバ）
(3)ソフトウェア（署名検証エンジン、署名ソフトウェア）
(4)媒体・周辺機器（IC カード、セキュア USB、リーダ／ライター）
(5)証明書（電子署名用、タイムスタンプ用）

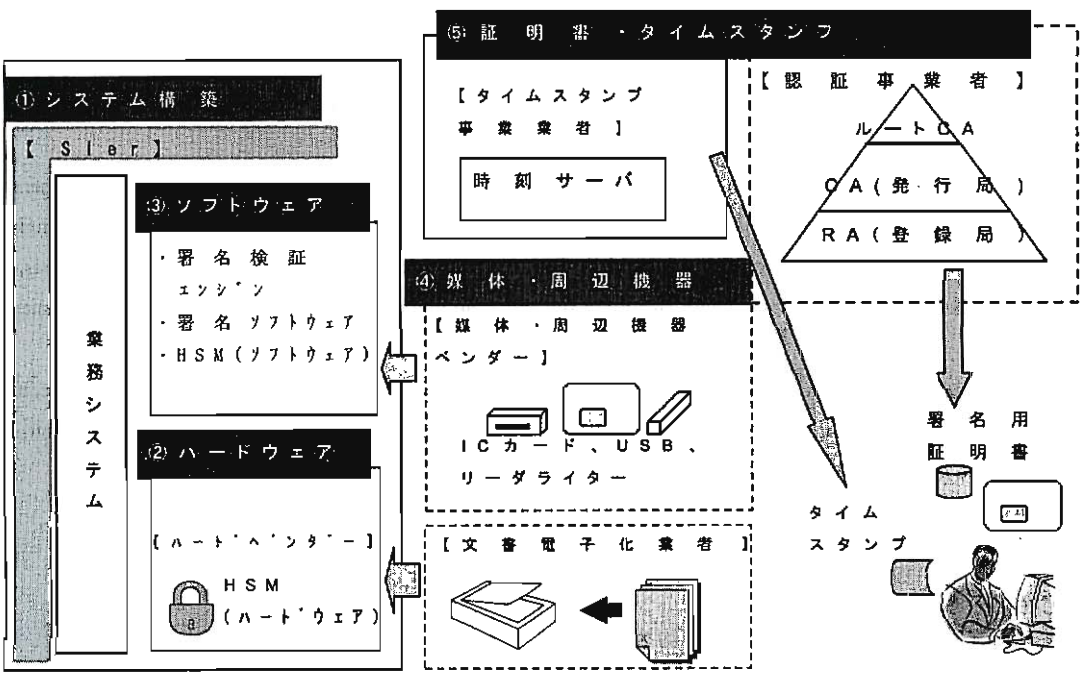

図　1：電子署名文書管理システム構築における購買

2.1.1. システム構築

電子署名文書管理システムを構築する場合、機能はユーザーとのインターフェース部分から「証明書インターフェース」「電子署名／タイムスタンプの付与・検証」「電子文書の作成」「業務システムとのインターフェース」の４点に分類される。そしてそれぞれの機能についてパッケージ購入要否、開発担当（専門ベンダー・自社）などについて適切に選定する必要がある。PKI 技術と一口に言ってもその分野は広く、それぞれの詳細分野に専門のベンダーがいる。さらに各専門ベンダーは専門分野に特化しており、システム全体の観点から各技術を適切に選定するのはユーザー自身がしなければならない。なぜならば、PKI 技術を総合的に利用するためのアドバイスができるベンダーや技術者は少ないからである。

2.1.2. ハードウェア

電子署名を利用する場合、通常のサーバ類などの機器に加えて HSM(Hardware Security Module)*とセキュアサーバも購買検討の対象となる。いずれも耐タンパ性（外部からの情報読取行為に対する耐性）に優れたハードウェアで、証明書の秘密鍵や重要な情報を格納するために使用する。

*：HSM にはハードウェアとソフトウェアの２種類がある。

耐タンパ性の強度の認定基準としては FIPS140-2 などがあり、認定認証局や WebTrust 規準を取得している認証局は同基準のレベル３あるいは４の製品を利用しているのが一般的であるが、価格が高いという難点がある。高価格のために HSM を利用せずに、秘密鍵を通常のフォルダに格納した一般ユーザーの例を知っている。せっかくの PKI 技術も秘密鍵を通常のフォルダに格納したのでは、技術自体の存在意義が失われる。しかし一般ユーザーが機器類に対して認定認証局と同じように費用をかけるのは無理である。様々なレベルのユーザに対して、適切なセキュリティレベルを提供する HSM の製品ラインアップ拡充が必要である。

2.1.3. ソフトウェア

DBMS やミドルウェアに加えて、電子署名専用ソフトウェアが必要となる。専用ソフトウェアとしては、署名検証エンジン（単独文書、大量文書向け）と署名ソフトウェアがある。

それぞれのソフトウェアは利用実績やサポート体制の観点から製品を選択する必要がある。

これらの製品が提供する機能を自社開発する選択肢もあるが、昨今 ECOM の実証実験で各社製品の相互運用性が確認されている上、開発には PKI 技術に習熟している必要があることから、専用製品を利用した方が得策である。

2.1.4. 媒体・周辺機器

電子署名に特有な媒体・周辺機器としては「電子証明書を格納する媒体（IC カード、セキュア USB）」「リーダー・ライター」の２種類がある。

ここで留意するべき点は PC との親和性である。IC カードやリーダー・ライターは、ドライバー導入時に問題が発生する場合が多く、導入時のサポート工数が大きな負担となる。

従って PC との親和性や他社での導入実績、ベンダーサポート体制の観点から「媒体＋リーダー・ライター＋各種ドライバー」をセットにして適切な製品を選択する必要がある。

2.1.5. 証明書（署名用・タイムスタンプ用）

購買において一番理解しづらいのが証明書である。電子署名文書管理システムにおいては電子署名用とタイムスタンプ用の２種類を調達する必要がある。調達にあたっては以下の 5 点について検討し、認証事業者などと具体的な調達について決定する必要がある。

(1)事前検討項目
- ①証明書の利用目的（電子入札用、電子文書への署名、電子メールへの署名、SSL 通信、Web サイト本人認証）
- ②利用形態（利用者の単位[個人単位、役職単位]、利用者数、タイムスタンプ数、電子文書保管期間）
- ③優先項目（セキュリティ、費用対効果、操作性など）

(2)署名用証明書　調達先
- ①法的観点からの判断（電子署名法準拠要否）　　文書の保管
- ②認証局経営体（自社で認証局を構築、外部認証局［認定認証事業者、それ以外の認証事業者］、官公庁）

(3)タイムスタンプ調達先
- ①技術方式（リンキング方式、電子証明書方式、アーカイビング方式）
- ②発行体（自社でタイムスタンプ局を構築、タイムスタスタンプ認定事業者）

(4)証明書特有のリスク
- ①内容確認（電子署名用証明書の場合、CN 確認は必須）
- ②認証局／タイムスタンプ局　運用規定リスク（認定認証事業者／タイムスタンプ事業者への規制法制がない、主務官庁の監督権限が曖昧、賠償責任が法律で未整備、認証局／タイムスタンプ局のデータ保管期間）
- ③認証局／タイムスタンプ局　経営リスク（認証局休廃止時の業務引継が法律では保証されていない、同休廃止時の過去の検証データの引継ぎが法律で保証されていない、認証局休廃止の事前通知が義務付けられていない）
- ④認証局オペレーショナルリスク（操作ミス、システム障害）

(5)秘密鍵格納方法
- ①安全な格納方法の具体例・基準（耐タンパ性）
- ②セキュアな格納装置（HSM など）の価格

2.2. 業務設計

電子署名文書管理では通常の電子文書管理における業務に加えて、「電子署名文書のライフサイクル管理」と「電子証明書のライフサイクル管理」の2点について検討する必要がある。

2.2.1. 電子文書ライフサイクル管理

通常の電子文書においても文書のライフサイクル管理は存在する。(文書作成、保管、廃棄)

電子署名文書の場合は、電子署名に利用した電子証明書の有効期限とタイムスタンプの有効期限の2つの観点を勘案してライフサイクルのイベント実施タイミングを決定する必要がある。(図 2:電子署名文書のライフサイクル)

図 2の通り、ライフサイクルイベントの保管、廃棄やアーカイブ実施時期などについて、電子証明書とタイムスタンプの有効期限を勘案してタイミングを決定する。

電子署名文書における法的効力を勘案すると電子署名、タイムスタンプのどちらかが有効である場合は、「効力が証明されている状態」であるが両方とも有効期限切れの場合は効力が保証されていない状態となる。従って両方とも有効期限切れとなった場合は、速やかに廃棄処分とする運用とした方が適切である。

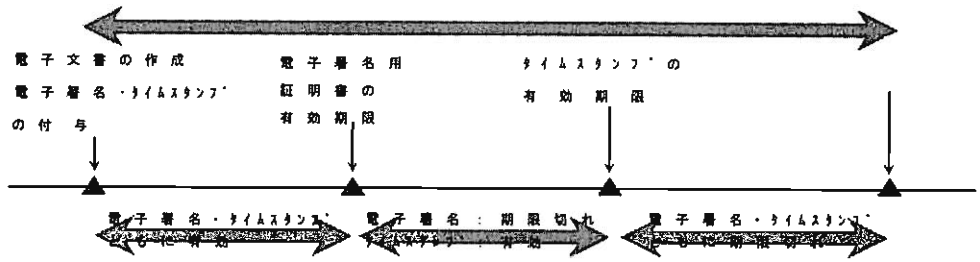

図 2:電子署名文書のライフサイクル

2.2.2. 証明書ライフサイクル管理

システム運用などにおいては購買や ID 管理などが運用フェーズで発生する。(例:システム保守契約の更新、備品の購買、人事異動によるユーザーID 更新)

ライフサイクルのきっかけとなるイベントと運用設計上の主な留意点として次に述べる。

いずれも検討対象となる業務は購買、印章取扱、電子署名文書管理業務、同システム運用業務であり、該当する規定を修正する必要がある。

(1)発行

購買、印章取扱、電子署名文書管理システム運用などの規定に対して、記述するべき項目としては以下の例がある。

①購買:手続開始時期、証明書調達先、承認手順など

②印章取扱:証明書利用に必要な職階・職務権限、人事異動の際の取扱手順、社内システムへの証明書登録手順

認定認証事業者から証明書を調達する場合は、銀行届出印・正式な会社印と同様の扱いで規定類を整備する必要がある。

(2)更新

記述するべき項目は発行作業で記述した内容に加えて、以下の2点についても検討が必要である。

①購買:手続き開始時期と証明書有効期限の関係

②印章取扱:新旧証明書並存期間の取扱方法、有効期限切れ証明書の取扱

(3)失効

失効については利用者からの要請に基づくものと、認証局が必要と判断して実施する失効がある。しかし対応手順は両方のケースとも同じであることから、利用者からの要請に基づくケースで業務設計を行うことで十分である。

失効は発行・更新とは違い、以下の観点で業務設計を行う必要がある。

①失効申請の緊急度:紛失などによる失効と、人事異動に伴う失効では作業開始可能時期や承認手順、作業内容が違う。

②失効後の証明書の取扱:過去に署名した文書の取扱、過去に実施した署名有効性検証情報の取扱など

(4)鍵の危殆化

鍵の危殆化の分類としては(表 1)のようになる。

それぞれの場合において、実施するべき手順を検討する必要がある。

事例 対象	鍵の漏えい・紛失・盗難	鍵の弱体化	鍵のｱﾙｺﾞﾘｽﾞﾑの弱体化	鍵の消失・破損
利用者の秘密鍵	即時失効が必要	即時失効する必要はない。しかしIPAなど官公庁・関連団体からの暗号関連評価に関する発表を逐次確認し、対応方法と対応時期について決定する必要がある。		即時失効する必要はない。しかし新規証明書を速やかに発行してもらい、切り替える。
電子認証局の秘密鍵				
ﾀｲﾑｽﾀﾝﾌﾟの秘密鍵				
ﾀｲﾑｽﾀﾝﾌﾟ局の秘密鍵				

表 1：鍵の危殆化の事例と対応作業例

3.【現状分析２】一般利用者向けの整備状況

2. で利用者にとって難解な点を検証したが、このような点を解決する指針となる規定・ガイドラインの状況はどうなっているか。この点について検証してみる。

現在、日本で知られている PKI・電子署名に関連した主な標準規格・ガイドラインは以下の通りである。

(1)認定認証局向け管理基準
(2)WebTrust 基準
(3)ISO 規格（金融機関向け　認証局管理基準）
(4)JIS 規格（JISZ6016、JISA6017、JIS X 5092、JIS X 5093）
(5)デファクト基準（RFC3126、3161、3280、3467 など）
(6)官公庁発行の規定、ガイドライン、報告書
　①医療情報システムの安全管理に関するガイドライン
　②電子帳簿保存法通達
　③文書の電磁的保存等に関する検討委員会報告書
(7)ECOM 報告書、ガイドライン
　①電子署名利用システムの構築・利用ガイドライン
　②電子署名文書長期保存に関するガイドライン
　③タイムスタンプサービスの利用ガイドライン　ほか

このうち、一般の利用者向けに記載されているのは(6)①～③と(7)①であり、大半は IT ベンダーや認証事業者向けとなっている。

また、先に挙げた一般利用者向けの規定・ガイドラインもシステム構築全般を俯瞰したものではなく、2であげたユーザーにとっての疑問に対して、十分に答えた内容となっていない。一般ユーザーがシステム構築を行うための総合的な導入ガイドラインの整備が必要である。

4. 電子署名文書の普及のために

4.1. 方向性（「わかりにくさ」の解消）

電子署名という言葉や、「電子署名とは印鑑・署名のデジタル版」という理解は広く普及している。

しかし、いざこの技術を利用してシステム構築や利用を検討する際、単純に印鑑を電子に置き換えれば良いわけではない。電子署名や PKI 技術には特有の特徴があり、ユーザーはその点を踏まえて利用する必要があり、ここがユーザーの利用意欲の大きな障壁となっている。

電子署名を広く普及されるためには、電子署名や PKI 技術を意識することなく利用できるように、ユーザーインターフェースを向上させる必要があるが、残念ながらまだそこまで環境が整備されていない。現時点では電子署名を利用する場合、ユーザーが電子署名や PKI 技術の各要素技術を取捨選択し、業務運用の大半を自分で設計していく必要がある。

2の現状分析で挙げた点を見てもユーザーが考慮するべき点が多すぎるのは明らかである。一企業が勉強してシステム構築するには負担が重過ぎる。電子署名を普及されるためには、PC を利用できる程度のユーザーが CP,CPS,CRL などといった PKI 技術の知識がなくても、利用できる状況にする必要がある。

いくら良い技術でも簡単かつ安全に利用できなければ淘汰されてしまう。PC やインターネットが 90 年代に社会基盤として認知されていった歴史を見れば、それは明らかである。

4.2. 利用者向けガイドライン整備

前項で、電子署名を普及させるためには PC やインターネットと同様に、特別な知識がなくても利用できるようにユーザーインターフェースを向上させる必要があると述べた。

しかしこれは最終的な到達目標であり、ここに至るまでには時間が必要である。そこで直近の方策として、一般ユーザー向けのシステム構築ガイドラインを整備し、電子署名の理解をサポートする必要がある。

ここでは電子署名文書管理システム構築ガイドラインの内容について提案する。

4.2.1. ガイドラインの考え方

電子署名文書システムを構築・管理する場合、システム構築の基本的な部分は通常の電子文書管理システムと同じである。電子署名という言葉がつくと特殊な留意点が多いのではないかと懸念するユーザーも多いが、特別に考慮するべき点は電子証明書や電子署名の部分であり、この点を通常のシステム構築の留意点に対して追加すれば良い。

従って準拠するべき規格・参考にするべき規格類は広く知られている ISO9000、27000 などが該当する。しかしこれらの規格類は電子証明書・電子署名についての記述が不足していることから、2に上げた難解な点を解説するこの部分に追加するべき管理項目を検討することで、電子署名文書システム構築ガイドラインの要件が満たされる。

電子署名文書システム用の特別なガイドラインを一から作成する必要はない。以上の考え方を踏まえて、追加するべき管理項目について検討する。この項目については以下の規定をもとに検討した。

・RFC3467

・ISO27000

その結果、電子署名文書管理を行う上で規定などで追加するべき管理項目として以下のようになる。

(1)電子文書の種類と重要度分析

(2)電子文書の管理規定

以下の内容を反映した管理規定を作成

①電子文書の種類（電子契約書、電子化した契約書、電子取引証憑、電子操作履歴（＝ログファイル）など)。

②情報の重要度（社内で規定した分類における該当レベル、問題が発生した場合の経営への影響度など)。

③保存期間

④電子文書の作成プロセス

⑤使用する証明書の種類

⑥使用するタイムスタンプの種類。

⑦準拠するべきCPS・タイムスタンプ局運用規定

⑧準拠性監査（内部監査・外部監査)。

⑨当該規定決裁権限者

⑩本業務の関係者

・認証局

・タイムスタンプ局

・当該業務に係る第三者

・証明書利用者

・当社

⑪準拠する社内規定

(3)証明書・タイムスタンプ購買

以下を明記した購買規定を作成する。

①使用する証明書、タイムスタンプの種類、調達先

②証明書名義人の職務要件

③購入時の調達先への情報開示項目、証明書名義人への情報開示同意取得

④購買が発生する業務イベント（初期購入、人事異動、証明書更新、再発行、情報変更）

⑤認証局、タイムスタンプ局への費用が発生しない要件（有効性検証、先方要件による再発行など）

⑥認証局、タイムスタンプ局への手続きが発生するその他の事項

（失効、証明書停止、停止解除、鍵の再生成、契約解除）

⑦証明書、タイムスタンプの購買にかかる当方作業と事業者側の作業の手順

(4)証明書・タイムスタンプの管理

以下の内容を盛り込んだ証明書・タイムスタンプ管理規定を作成する。

①証明書・タイムスタンプの種類、利用用途

調達先

②証明書・タイムスタンプのCP・CPSの名称、格納場所（URL）

③証明書・タイムスタンプのCP・CPS改訂に対する情報収集手段と改訂内容のリスク分析と対応方法

④使用する証明書・タイムスタンプに格納されている重要な情報項目（ユーザ側の指定で設定される項目、そのほかユーザが知らなければならない項目、誤った情報が設定された場合のリスク）

⑤証明書・タイムスタンプのリスクと対応方法

（証明書そのものに対するリスクと認証局の責任、対応方法）

⑥有効性検証のための参照先

⑦有効性検証におけるリスクと対応方法

⑧証明書・タイムスタンプとその秘密鍵の格納先と格納先のセキュリティ要件

⑨証明書・タイムスタンプの運用上のイベントと各イベント時の作業手順（初期購入、人事異動、証明書更新、再発行、情報変更時のシステムやアーカイブ類などへの作業項目とその手順）

⑩CRL管理（バージョン、拡張手順）

（証明書に格納する氏名の文字形式（アルファベット、非許容文字、名前・苗字の順番）

(4)証明書の鍵管理

以下を明記した購買規定を作成する。

①鍵ペアの生成と導入

・鍵の目的と用途の定義

・公開鍵・秘密鍵の鍵ペアを生成する担当者の定義

・認証局から鍵を受け取る手順

・鍵ペアの生成手順と生成場所（ハードウェア、ソフトウェア）

②秘密鍵の管理

・管理者の単位（専用管理者の設置、証明書所有者毎の管理）

・秘密鍵を寄託されている場合の寄託先、エスクローシステムのセキュリティ管理

・バックアップの有無、その方式、バックアップ担当者、バックアップ形式（平文、暗号化、分割鍵）

・バックアップシステムのセキュリティ管理

の内容
・アーカイブ有無、方式、担当者、形式
・アーカイブシステムのセキュリティ管理方法
・秘密鍵活性化の担当者とその職務要件、活性化の手順、方法
・非活性化の担当者、手順、方法
・秘密鍵のシステム内保管方法
・秘密鍵破棄（実施可能な担当者、手順）
・暗号モジュールの能力定義
③公開鍵の管理（アーカイブ有無、方式、担当者、形式、アーカイブシステムのセキュリティ管理の内容）
④その他データの管理（PIN、パスワードなどの管理手順を策定）

(5)その他の法的な対応手順
①責任範囲の明記、問題が発生する場合、発生時の責任範囲
②個人情報の取り扱い
・認証局などに提出する個人情報の一覧
・認証局など提出先との個人情報取り扱い取り決め内容
・個人情報の範囲と、対象外で認証局に提供している情報
・個人と会社との間での個人情報提供に関する取り決め
③CP、CPS、契約書上で定義されている認証局、当方、関係者の瑕疵となる場合と対応方法
④先方および当方の免責事項一覧
・CP、CPS、対顧契約などで定義されている免責事項一覧
・関係者の責任の制限、責任に関する合意事項
⑤補償
・CP、CPS、対顧契約などで定義されている補償事項一覧
・関係者の責任の制限、責任に関する合意事項
⑥認証局で保管する資料類と保存期間
・電子文書の法的効力裏付けとなる認証局側の有効性検証や証明書発行の証跡の項目、保存期間
・認証局が廃業、引継ぎが発生した場合の証跡類の取り扱い内容
⑦関係者間の通知内容と通知方法
（認証局などからやってくる通知内容と通知方法－CP、CPSの変更、危殆化）
⑧紛争解決手続き・準拠法
（電子署名付文書を外部企業と交換いる場合などで問題が発生した場合の解決手続きや、準拠法を明記）
⑨その他の法的留意事項（知的財産権ほか）

(6)その他
①関連規定・ルール類の見直し（見直しの頻度、手続、改訂に対する評価）

4.3. ユーザーインターフェース向上

前項では一般ユーザ向けのガイドライン類について検討したが、最終的にはユーザーインターフェースを大幅に向上させ、誰でも簡単に利用可能な状況にする必要がある。

具体的に向上するべき点は何か。それは2であげた一般ユーザーにとって難解な点や、管理項目として盛り込むべき点がシステムやサービス内容に盛り込まれることである。

PCが誕生した頃、ユーザーはPCに対してコマンドを一つ一つ入力して実行させて、作業を進めていた。そのためには、ユーザーはコンピューターの知識があることが前提となり、様々な条件や制約を踏まえてコマンドを発行する必要があった。しかし技術が進むと、要求される知識レベルのハードルは低くなり、Windowsや MacOSにおいてはアイコンをクリックするだけで、PCは文字の入力、計算、画像の再生まで様々なことを行う。現在、多くのPCユーザーはMS-DOSや機械語などの知識を持たずに利用している。

電子署名も同様である。

先に挙げた難解な点のうち、購買については PCの周辺機器のように、ハードウェア、ソフトウェア、媒体・周辺機器・証明書などは専用周辺機器類として予めユーザーに提示したり、システム構築についても構築するべき項目をメニュー化する工夫が必要である。

また、業務設計においてはシステム側で証明書や電子署名文書のライフサイクル管理などを行い、ユーザーはPINなどの更新作業程度に留めれば、難解な印象が緩和される。

5. 今後の研究方針

本論文では、利用者向けに電子署名を理解を促進するための方法の一つとして、利用者向けガイドライン案の項目を中心に検討を行い、同ガイドライン案を提案した。今後はユーザーインターフェース向上のために必要な業務アプリケーションの機能と、電子文書における法的な環境について研究を行う予定である。電子署名は電子データの法的効力を補完するために、登場した技術である。したがって、この点における電子署名の優位性を、一般利用者にアピールする必要し、電子署名普及に貢献していきたい。

文　献

[1] 「電子署名普及に向けた調査報告書」H18.3 次世代電子商取引推進協議会
[2] 「RFC3647　インターネットX.509 PKI：証明書ポリシ

ーと認証実施フレームワーク」(Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) IPA（独立行政法人　情報処理推進機構）

[3] 「JIS Q 13335-1:2006（ISO/IEC 13335-1:2004） 情報技術－セキュリティ技術－情報通信技術セキュリティマネジメント－第 1 部：情報通信技術セキュリティマネジメントの概念及びモデル」（財） 日本規格協会

[4] 「JIS Q 27001:2006（ISO/IEC 27001:2005） 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」（財） 日本規格協会

[5] 「JIS Q 27002:2006（ISO/IEC 17799:2005） 情報技術－セキュリティ技術－情報セキュリティマネジメント実践のための規範」（財） 日本規格協会

[6] JIS X 5092:2008 「CMS 利用電子署名(CAdES)の長期署名プロファイル 」（財） 日本規格協会

[7] JIS X 5093:2008 「XML 署名利用電子署名(XAdES)の長期署名プロファイル」（財） 日本規格協会