3 システム担当の皆さんへ

3-1 電子証明書利用時の操作方法

■署名検証の方法

もし、あなたが電子署名付きの電子文書を手に入れたら、何を確認したらよいでしょうか。

電子署名に利用された電子証明書が信頼できるか、以下の項目を確認しましょう(署名検証)。

- 信頼された認証局から発行されているか
- 有効期間内か
- 失効されていないか

また、電子文書自体が電子署名後に変更されていないか確認することも重要です。

本節では、Adobe Reader X、Adobe Acrobat X(以下、Acrobat Xと記載)を用いて、上記の項目を最初に確認する方法を紹介します。

★電子署名付きPDFを手に入れたら～Acrobat X編～
電子認証局会議ホームページ内にある、電子認証局会議会則(http://www.c-a-c.jp/pdf/us/CAC_kaisoku.pdf)を題材に、署名の確認を行います。

【電子署名の確認】

まず、PDFに電子署名が付いているかどうかを確認します。PDFファイルをAcrobat Xで開きます。

署名が付いている場合、**図3-1**のように、上部に電子署名に関する情報(アイコン、メッセージなど)が表示がされます。

電子署名の状態を表すアイコンは、**表3-1**に示す通り5種類があり、表示されているアイコンの種類によって、電子署名に利用された電子証明書の信

図3-1　電子署名の有無確認

頼性を確認することができます。①であれば、まったく問題はありませんが、それ以外の場合は詳しく確認する必要があります。

具体的な確認方法については、電子認証局会議のWebページ「**★電子署名付きPDFを手に入れたら～Acrobat X編～**」を参照してください。

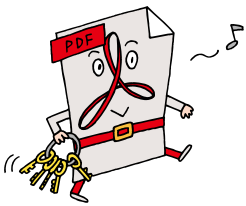


表3-1　電子署名状態アイコンの信頼について

アイコンおよびメッセージ	電子署名に利用された電子証明書は			電子文書に対する電子署名後の変更有無
	信頼済認証局が発行か	有効期間内か	失効されていないか	
 ①署名済みであり、全ての署名が有効。	○（信頼済）	○（有効）	○（未失効）	○（変更なし）
 ②署名済みであり、すべての署名が有効。ただし、最終署名の後に署名されていない変更あり。	○（信頼済）	○（有効）	○（未失効）	×（変更あり）
 ③少なくとも１つの署名に問題があり。	？（確認必要）	？（確認必要）	？（確認必要）	？（確認必要）
 ④無効な署名があり。	○（信頼済）	○（有効）	×（失効済み）	？（確認必要）
 ⑤検証が必要な署名があります。	？（確認必要）	？（確認必要）	？（確認必要）	？（確認必要）

3-2 電子署名の技術的対策のポイント

本節では、ビジネスシーンにおいて電子署名を導入する際に考慮すべき「技術的な考え方」や「対策上のポイント」について解説します。

なお電子署名の利用にあたっては、「技術」とともに「運用」の理解が大切です。運用要件は「2-5 電子署名の運用のポイント」をご確認ください。

3-2-1 電子署名とは、どのような技術なのか？

Q 電子署名とは、どのような技術なのか？

A 電子データに、紙文書における記名・押印と同等な証拠能力を持たせる技術です。電子署名法*1により、電子署名を付与した電子記録は"真正に成立したものと見なす"ことができ、電子記録に証拠性を持たせることが可能となります。

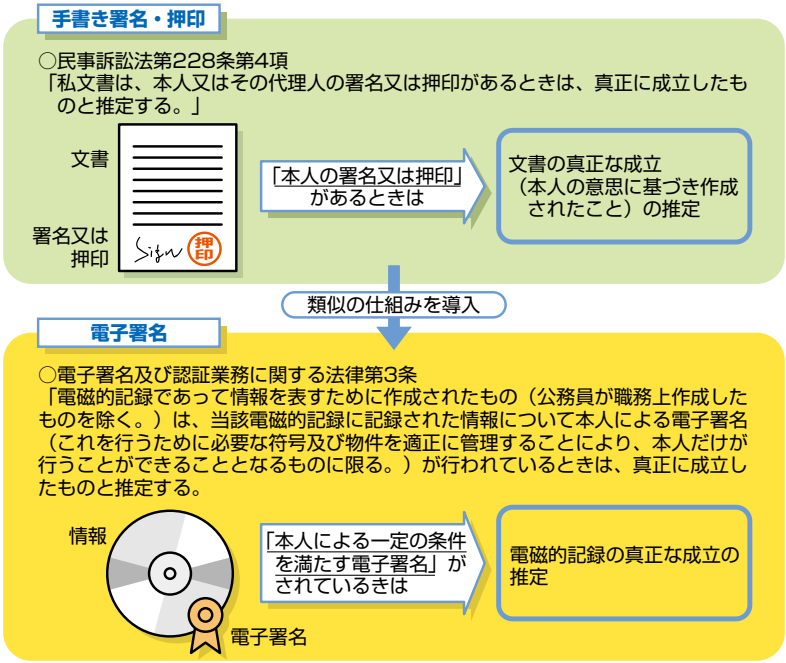


図3-2 民事訴訟法第228条第4項と電子署名法第3条

＊1「電子署名及び認証業務に関する法律」2001年4月施行

電子署名には、信頼できる第三者機関となる電子認証局から署名者に対して発行された電子証明書（公開鍵証明書）と秘密鍵（私有鍵）のペアが必要となります。署名者自身が唯一の所有者である秘密鍵を用いて、署名対象文書に対して暗号技術を用いた署名処理を行い、署名データを生成します。署名データを受け取った署名検証者は、署名データが正しいことを確認するために、

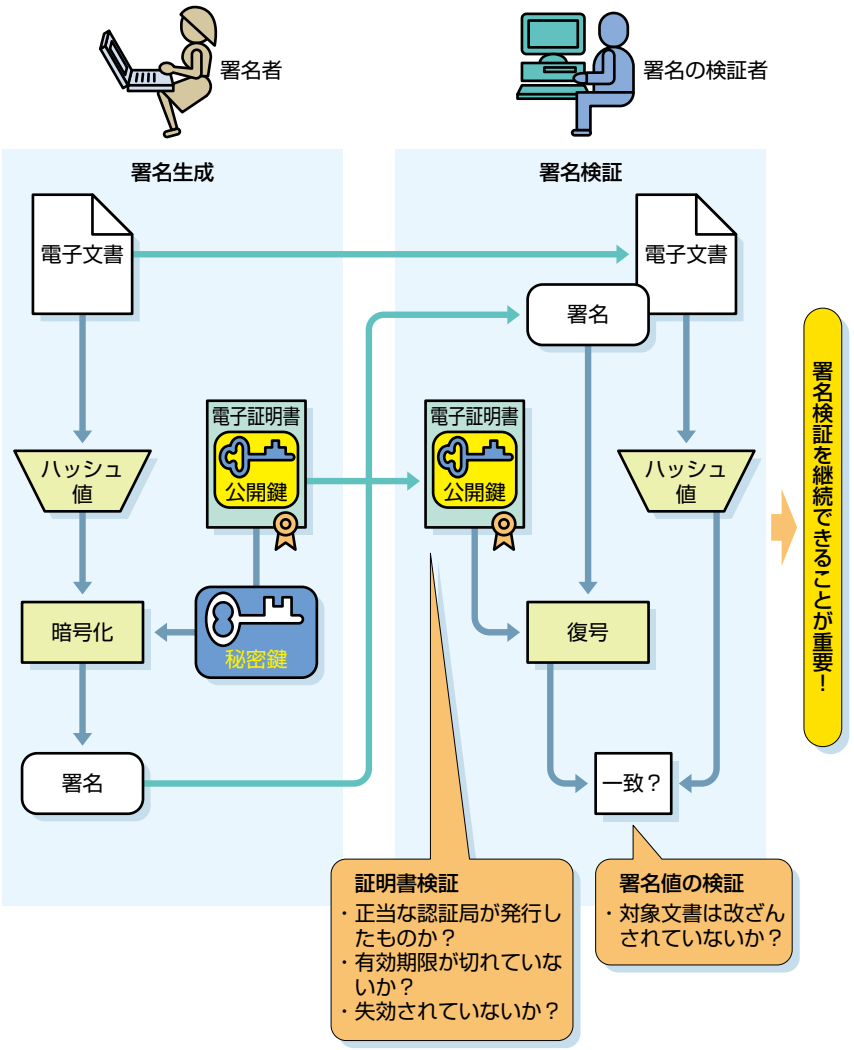


図3-3　電子署名および検証の具体的方法

まず署名者の電子証明書が本物であることを確認し、電子証明書の中の公開鍵を用いて署名データに含まれる暗号部分を復号します。正しく復号できれば、本人が間違いなく電子署名したものであることが確認できます。

Q 電子署名と署名検証の要件とは？

A 表3-2のとおりであり、電子署名の真正性を保つために極めて重要です。

表3-2は、極めて重要です。紙に記名・押印されたものは目で見て確認できますが、電子署名そのものは電子データであるため、検証可能なシステムにおいて内容を確認・検証して初めて有効性が確認できることになります。

表3-2　電子署名および署名検証の要件

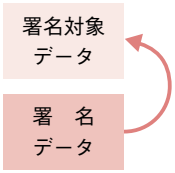
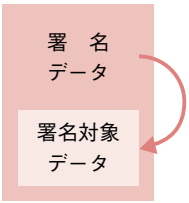
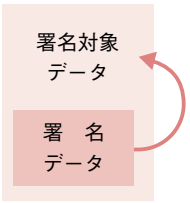
	要件概要	要件詳細	
1.電子署名の要件	有効な電子証明書を用いて電子署名すること	A	正当な（信頼できる）認証局から発行されたもの
		B	有効期限が切れていない
		C	失効していない
2.署名検証の要件	署名対象文書の有効性を維持したい期間、電子署名が正しく検証できるようにする。	D	正当な認証局から発行された本人の電子証明書であったか？
		E	署名当時に電子証明書の有効期限が切れていなかったか？
		F	署名当時に電子証明書は失効していなかったか？
		G	署名対象データは改ざんされていないか？

3-2-2　署名形式について

Q　電子署名の形式には、どのようなものがあるか？

A　**表3-3**の３つに大別でき、利用形態に応じて選択します。

表3-3　電子署名の形式種別

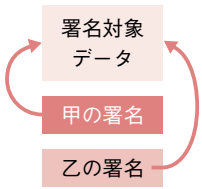
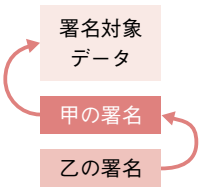
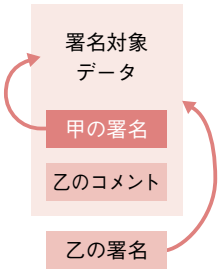
(1) 分離形式 (Detached 型)	(2) 内包形式 (Enveloping 型)	(3) 包含形式 (Enveloped型)
 署名対象データと独立して、署名データを作成	 署名データの中に署名対象データを格納(内包)して作成	 署名データを署名対象データの中に含む（包含）形で作成する場合
・署名対象データの形式を問わず、あらゆるファイル形式に署名データを作成可能 ・既存アプリで署名対象データを取り扱う場合など、アプリ側への影響が僅少 ・署名対象データと署名データの紐づけ管理が必要	・署名対象ファイルと署名データが1ファイルとなり取り扱いが容易 ・アプリなどで署名対象データを利用する場合、署名データから署名対象データの取得が必要	・(2) と同様に1ファイルを管理すればよく、取り扱いが容易 ・署名対象データのファイル形式が、電子署名のサポートを必要とし、作成可能ファイル形式に制限あり（PDF、XMLなど）

3-2-3　複数署名について

Q　契約書や議事録など、複数の署名者が署名する場合はどうするのか？

A　複数人の署名が付与されるケースは、署名対象文書の性格上、**表3-4**の3つの分類に大別できます。利用目的に応じて適切に選択ください。

表3-4　複数署名の種別

（1）並列署名	（2）直列署名	（3）直列署名の応用形
同一の文書を署名対象として、各自がそれぞれ署名するケース	第1の署名者の署名データに対して第2の署名者が署名するケース	第1の署名者が署名した文書に、第2の署名者がコメントを追記し署名するケース
		
議事録への署名など、同一文書を署名者全員が同意した際などに付与する署名	署名に対して署名を重ねて行くことにより作成	署名対象データと第1の署名者の署名データ、および自ら追記したコメント全体を対象として第2の署名を付与
・個々の署名は独立しているため、誰かの署名データを消去されても痕跡が残らない場合があるので注意が必要 ・全員の署名付きデータを安全に保管する必要あり	・報告書の承認のように署名の連鎖があるような場合に適用	・社内の稟議書で審査者が署名した文書へ、決裁者がコメントして署名を付与するような場合への適用 ・実務的には最終決裁者の署名があればよい場合もあり

3-2-4　署名とタイムスタンプ

Q　電子署名の必要性は理解できるが、タイムスタンプ*2は、なぜ必要なのか？

A　タイムスタンプは何時（以前に）署名したものか、電子署名時刻の証拠性を補完してくれるものです。

Q　では電子署名に記録される時刻は何か？

A　例えばパソコンで電子署名した場合、当該パソコンの設定時刻が付与されるに過ぎません。設定を自由に変えることができるパソコンの時間が記録されたところで、証拠になり得ないのは自明です。

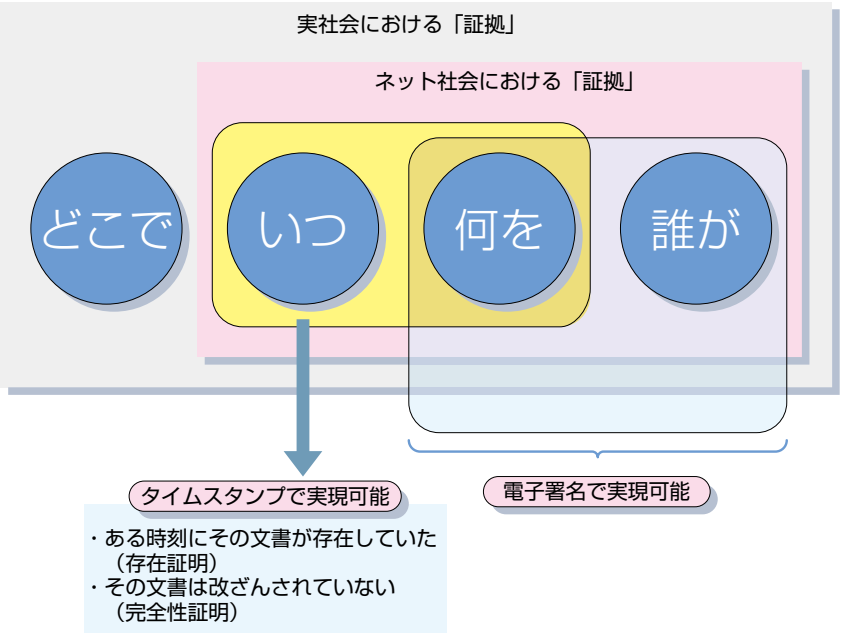


図3-4　タイムスタンプで実現される内容

＊2 ここでいうタイムスタンプは、日本標準時間に同期した日付時間を使用してタイムスタンプの発行業務を行うTSA局から発行されたもののことです。

3-2-5　長期署名の必要性

Q　紙は2000年の歴史があるが、電子署名の効力はそんなに長く持つのか？

A　法定保存期間や商習慣を考えた場合、例えば国税関連書類は7年、会社法関連では10年間の保存義務があります。また、PL法や民法上の訴訟リスクに対応して製品図面などを保存する場合、民法上の時効期間を考えると20年間程度は保存する必要があります。

このように実務的には数十年程度の期間、電子署名の検証を継続させる必要がありますが、電子署名のみでは電子証明書の有効期限(電子署名法では最長5年まで)を超えて署名および署名検証することができません。

したがって、タイムスタンプを組合せた長期署名を付与することにより署名検証を維持、継続する必要があります。

Q　タイムスタンプでなぜ署名検証を維持、継続する必要があるのか？

2つの理由があります。

A　①“電子署名当時”にその公開鍵が有効であったかどうかを確認するため

表3-2のとおり、「有効な電子証明書を用いて電子署名していたか」を後日、検証の際に確認できる必要があります。

つまり、“電子署名当時”にその公開鍵が有効であったかどうかを確認するために、そもそも「いつ電子署名されたか」を明確にする必要があるわけです。電子署名された日時の証拠があれば、電子証明書の有効期限を見て、当該日時に電子証明書が有効期限切れでなかったことを確認し、かつ電子署名当時の失効情報を保管することにより、電子署名当時、その電子証明書は失効していなかったことが確認できればよいのです。

A　②電子署名に用いた暗号技術が脆弱化した場合でも、署名検証を可能とするため

長期署名では、「署名対象データ」と、「署名データ」、「それに関連する電子

証明書」、「失効情報」の全体にタイムスタンプを付与します。これにより署名データや検証に必要な情報等がタイムスタンプの暗号アルゴリズムで保護された形となります。タイムスタンプの暗号アルゴリズムは個人の電子署名に用いられる暗号アルゴリズムより強固な暗号アルゴリズムを利用しますので、署名暗号アルゴリズムが脆弱化した後でも、電子署名の有効性が維持できることになります。

ちなみに、2013年現在、電子署名に用いられる最も一般的な暗号アルゴリズムであるSHA-1、RSA1024、は将来、脆弱化が進むことが予測されており、

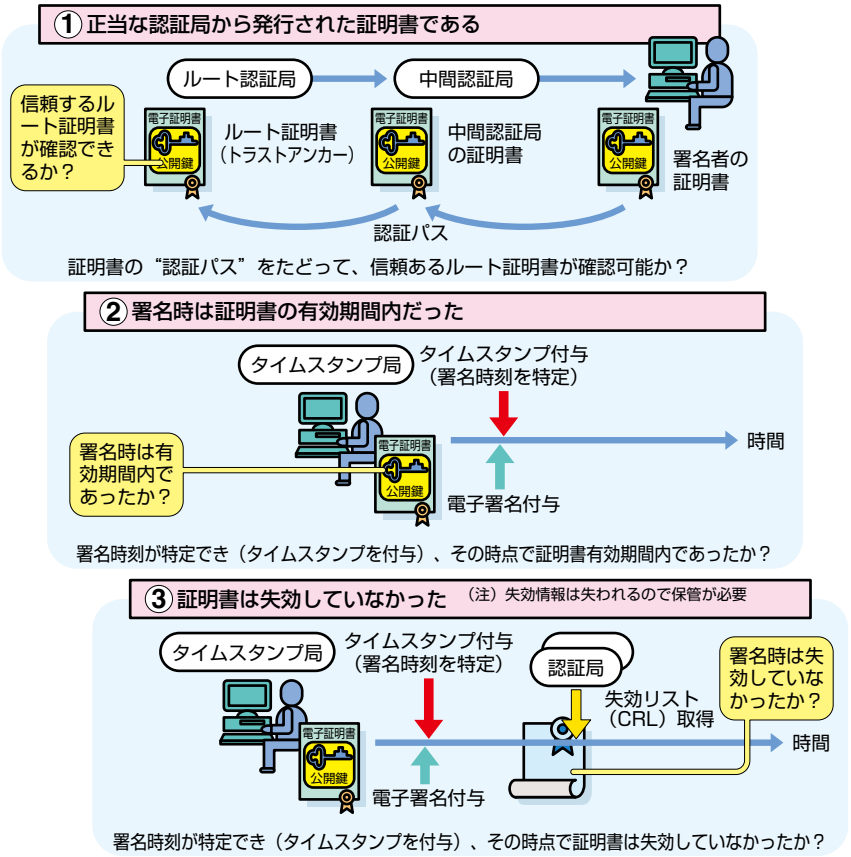


図3-5　長期署名の技術解説

2014年９月以降、政府の情報システムでは、より強固な暗号アルゴリズムへの移行が予定されています*3。長期署名は、このような署名暗号アルゴリズムの脆弱化が起こった後でも電子署名の有効性を維持できるよう開発された技術です。

このように、「タイムスタンプ」を「電子署名」と適切に組み合わせることにより、電子証明書が失効されたり、有効期限が切れた以降でも、電子署名当時、当該電子証明書が有効であったことを継続して確認することが可能となります。

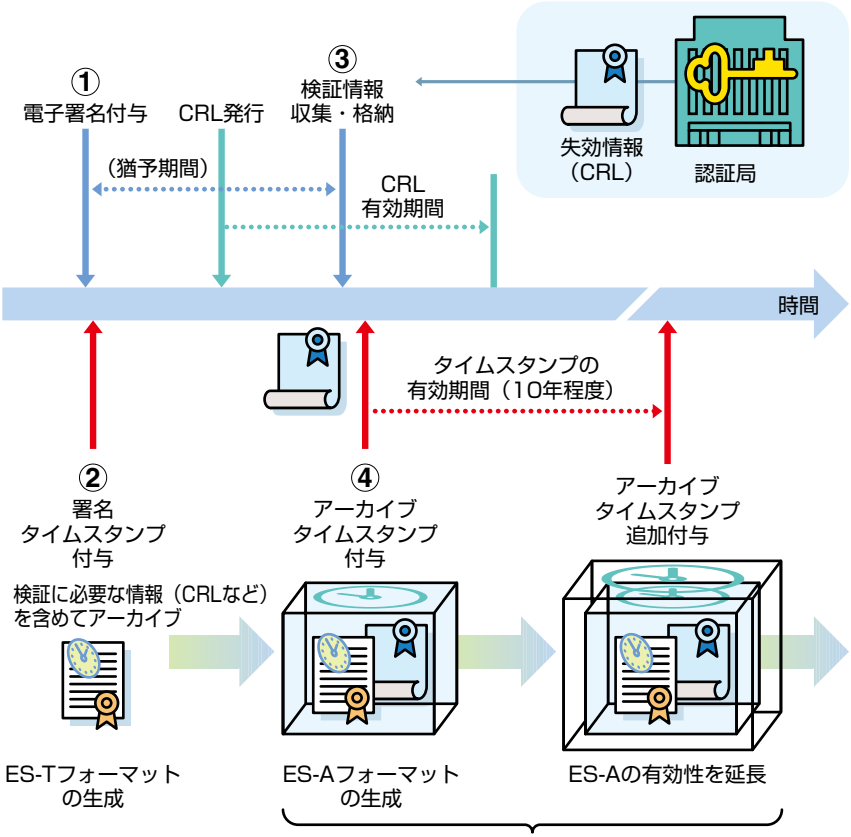


図3-6　タイムスタンプ付与の概要

＊3「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」内閣官房情報セキュリティセンター（2008年4月、2012年10月改定）

通常、電子認証局は電子証明書の有効期間を超えて失効情報の公開はしないので、有効期間を過ぎると電子証明書の有効性確認ができません。すなわち、署名検証を継続する必要がある場合は、失効情報を確保しておく必要があります。

したがって、**長期署名に関するJIS規格やISO**などの標準仕様（「５ 関係法令とガイドライン」を参照）を満たすためには、電子証明書の有効性検証に必要な失効情報などのデータを合わせて保存し、タイムスタンプを付与することが必要となります。その手順の概要を以下に示します。

①電子署名対象データ全体に対して電子署名を付与
②電子署名後すみやかに「署名タイムスタンプ」を付与し、その時刻に電子署名が存在していたことを証明できるようにしておく
（これをES-Tフォーマットといいます）
③電子証明書検証に必要となる、以下の検証情報を収集格納する。
タイムスタンプ局の電子証明書、電子署名者の電子証明書、認証パス上の電子認証局の電子証明書*4
上記のすべての電子認証局の失効情報
④上記の署名対象文書や署名値、検証情報全体に対して「アーカイブタイムスタンプ」を付与（これをES-Aフォーマットといいます）

ここで、各タイムスタンプの役割は、下表のとおりです。すなわち、タイムスタンプによりその時刻に署名が存在していたことを確認し、有効な電子証明書を用いて電子署名したことを後日検証可能とします。

表3-5　各タイムスタンプの方式と役割

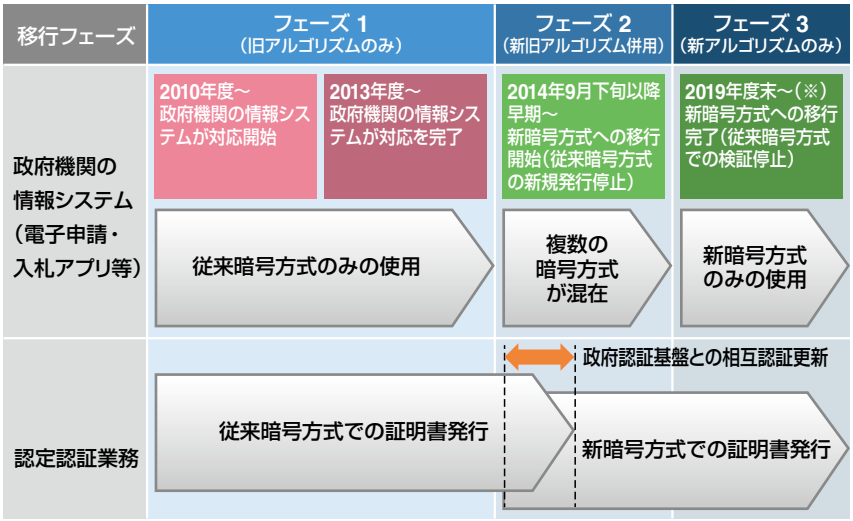
方　式	役　割
署名タイムスタンプ	電子署名時刻の信頼性を確保する
アーカイブタイムスタンプ	署名文書と失効情報をタイムスタンプの暗号アルゴリズムにより保護し、長期に渡り電子署名の真正性を継続する

＊4 認証パス上の認証局は、署名者の電子証明書を発行する認証局とタイムスタンプ局に電子証明書を発行する認証局の２つの認証局パス上の認証局となることに留意が必要です。

3-2-6　電子証明書暗号アルゴリズムの移行計画

内閣官房情報セキュリティセンター（NISC）が2008年４月に「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針」を公開、電子政府などで使用する電子証明書とその利用システムが強固な新暗号方式（SHA-2及びRSA2048）へ対応する発表を行いました。その後2012年10月にスケジュールの変更が発表され、政府機関、電子署名法に基づく認定認証事業者、そして署名アプリケーションを運用する組織が協調し、2014年９月下旬以降早期に認定認証事業者は新暗号方式の電子証明書の発行を開始し、従来暗号方式の電子証明書の発行を停止予定です。政府機関の利用システムは新暗号方式へ移行し、従来暗号及び新暗号の電子証明書の双方が2019年度末頃までは利用可能とすることで、スムースに暗号移行が可能なように移行計画が進められています。

政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針（平成24年11月１日 情報セキュリティ政策会議資料）
http://www.nisc.go.jp/conference/seisaku/dai31/pdf/31shiryou0302.pdf



＊暗号の安全性が急速に低下した場合の緊急時対応計画も作成しています。

図3-7　暗号移行スケジュール

3-3 電子認証局について

■電子証明書発行の仕組み

本節では、認証局や電子証明書の種類、機能について説明します。電子証明書を発行できる仕組みという意味での認証局は、利用範囲から大別すると「パブリック認証局」、「プライベート認証局」そして「電子証明書発行サーバ」に分けることができます。それぞれの違いは電子証明書が広く社会一般に利用されているのか、あるいはある企業グループ内やサービスの中でのみ利用されるのか、または企業内で試用的に利用されるのか、の違いです。認証局の役割は、「電子証明書がまちがいなく本人のものであることを保証する」ことにあります。そのために本人と電子証明書をしっかり紐付けるための電子証明書発行や失効の基準、電子証明書を作る際に重要な認証局の秘密鍵を漏らさないようなルールを明確に定めた上でCP/CPSに記載しています。電子証明書の発行は、各々の認証局が基本的には同一レベルの技術を使用して構築できるため、CP/CPSの規定や運用レベルの差が最大の違いともいえます。一般的にいわれているそれぞれの認証局の特徴は以下のとおりです。

■パブリック認証局

パブリック認証局の最大の特徴は、その信頼性が広く社会に受け入れられている点です。たとえば、民間企業が運営する国の認定を受けた認定認証局や法務省の商業登記認証局、また一般的なブラウザ（Internet Explorerなど）に、予め組み込まれている「信頼されたルート認証局」から電子証明書の発行を受けた認証局など、複数存在します。また、CP/CPSが公開されており、相手方の電子証明書を提示された場合には、そのCP/CPSの内容を確認して、信頼できるものかを判断することが可能となるため、見知らぬ相手とのやり取りを行う場合に有効です。

信頼されたルート認証局としてブラウザに組み込まれるためには、一定の基準を満たす必要があり、パブリック認証局は客観的な審査基準による外部監査を受けているため、発行された電子証明書の信頼性は高くなります。

■プライベート認証局

パブリック認証局とは異なり、CP/CPSをインターネットなどに公開せずに認証局を運営している場合もあります。これは特定の相手とのやり取りであれば、特に部外者（第三者）から信頼される必要がないためです。例えば、社員証への組み込み、グループ企業内でのやり取り、認証局を運営する企業の取引先とのやり取りなどに利用されています。プライベート証明書を外部の方に提示しても、受け取った相手は信頼できる認証局なのかを確認することができません。このため、不特定多数とのやり取りには不向きな電子証明書になります。プライベート認証局の導入方法としては、専門事業者からソフトウェアを購入した上で、独自のルールを設けて運用することが可能になります。反面、自ら定めたルールに基づいて、電子証明書の発行や失効といった業務を行う必要があります。電子証明書の信頼性のレベルを、その利用用途に応じて任意に設定し、CP/CPSを作成することができます。したがって、手軽な運用で電子証明書を発行して利用することも可能ですが、その電子証明書を利用する集団の中では、非常に信頼性の高いレベルのポリシを作成して厳密に運用することも可能で、実際にそのような運用がなされている場合もあります。

■証明書発行サーバ

認証局とは異なり、CP/CPSを定めず運用するサーバです。単に技術的に電子証明書を発行するサーバもこちらに該当します。これは正確には認証局とは呼べません。なぜなら、「電子証明書がまちがいなく本人のものであることを保証する」運用を行っていないためです。Windows 2000以降のマイクロソフトサーバーOSに備わっている“証明書サービス”で認証機関を構築、或いはOpen_SSLの機能を使用して、比較的簡単に認証局を構築し、一応の機能を持った電子証明書を発行することができるため、簡単に電子証明書を利用することができます。ただし、このような認証局を独自に構築して利用する場合、CP/CPSや相手との合意もないので、不特定多数とのやり取りにはまったく向かず、試用レベルの利用しかできないので注意が必要です。

表3-6　認証局の種類

	信頼性	運用コスト	柔軟性
パブリック認証局	◎	○	△
プライベート認証局	△	○	○
証明書発行サーバー	×	◎	◎

※それぞれ一般的な評価を示すもので、プライベート認証局にも信頼性の高いものを構築することも可能である。

■電子証明書の機能と種類

電子証明書には①電子署名、②認証、③暗号化の３つの機能があります。

①電子署名

電子署名には、実印のように厳密に用い、後日、「自分の署名ではない」などと否認されないよう、否認防止機能があるものと、認め印のように簡易的に用いる否認防止機能がないものの２つがあります。

否認防止機能がある厳密な署名に用いる電子証明書(**秘密鍵**：Private Key)は、認証や暗号化などに用いることは機能的にもできないので、署名のみに使用します。例えば、認定認証事業者の発行する電子証明書や公的個人認証証明書などはこれに該当し、署名にしか使えません。これは秘密鍵を署名以外の目的に使用した場合、悪意を持った者に盗まれないようにするためです。

たとえば認証システムは“その場限りでランダムな値”へ署名させ、その結果を検証することによって本人であることを確認しています。認証システムに不正なプログラムを仕掛けられ、“その場限りでランダムな値”の代わりに“100万円の借用証”に署名させられてはかなわないので、厳密な署名に用いる秘密鍵は認証や他の目的には使わないのです。

②認証

電子証明書は絶対に公開してはいけない「秘密鍵」と、公開してもかまわない「**公開鍵**（Public Key）」の２つがペアになって構成されています。ある秘密鍵で署名された電子文書は、ペアとなる公開鍵でのみ検証することが可能です。つまり公開鍵で検証できたということは、ペアとなる秘密鍵を持つ人が電子署名を付与したことになり、相手先を認証することが可能となります。その他、電子証明書を発行する際、電子証明書の中にユニークな情報を持たせておくことでも相手先の認証を行うことが可能です。インターネット上の商取引スペースの認証に電子証明書を用いることで、ログインIDとパスワードよりも安全な認証が行えます。

③暗号化

電子証明書があれば相手先の認証が可能となると同時に、相手先とやり取りをするファイルの暗号化を行うことも可能となります。「認証」の際にも用いた秘密鍵と公開鍵の一方で暗号化を行うと、ペアとなる鍵でしか暗号を解く（復号する）ことができないという特長が電子証明書にはあります。安全なファイルのやり取りを行いたい場合、相手方に公開してもかまわない公開鍵を渡しておき、その鍵で暗号化したファイルを自分に送ってもらいます。公開鍵で暗号化したファイルは自分しか持っていない秘密鍵でしか復号することができませんので、万が一、暗号化したファイルが漏えいしてしまったとしても、秘密鍵が漏えいしていなければ安全だといえます。

コラム

認定認証局の認証設備室について

電子認証局は、その認証局秘密鍵を安全に管理するために高いセキュリティを持つ部屋に設置することが求められます。この部屋を認証設備室と呼びますが、さらに認定認証業務においては、認証設備室の設置基準が明確に定められており、「認証設備室への入室には、入室する複数人による生体認証装置(身体的特徴を識別する装置)の操作が必要である。」との指針が定められています。例えば以下のような生体認証装置が入退室管理装置として使用されます。

①指紋照合装置　　②掌形照合装置

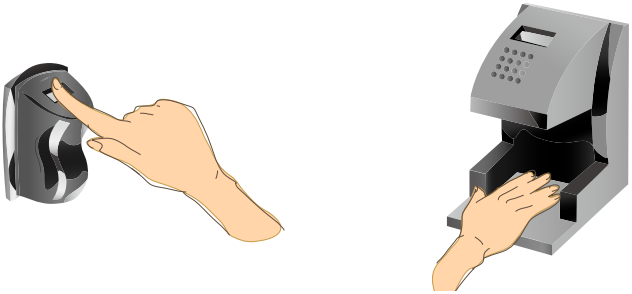


図3-8　認証設備室に設置される生体認証装置の例

このような入退室管理装置を設置し、しかも１人での入室は認められず、２人以上の要員がこの生体認証装置を操作した上で相互に牽制した中で入室することが義務付けられています。例えば、スパイ映画の中などで登場する厳重なコンピュータルームや金庫室などでしか見られないような設備が現実に使用されているのです。また、入室した認証設備室内には、監視カメラが

③固定型監視カメラ　　④全方位型監視カメラ

図3-9　認証設備室に設置される監視カメラ例

設置されており、その映像も記録されています。さらに夜間などに要員が退室した後で無人のはずの部屋の中で動きがあった場合には動体センサが作動して、警報が発せられるシステムが導入されています。

認定認証事業者は、このような高セキュリティの認証局エリアを構築して、さらに、この認証局秘密鍵をハードウェアセキュリティモジュール（HSM）と呼ばれる特殊な専用のハードウェアに格納することが求められます。このHSMは、耐タンパと呼ばれる機能を有し、その内部のデータを取り出そうとして、チップ上の電気信号を読みとろうとしたり、HSMをコンピュータのスロットから抜き取ろうとしたり、あるいはそのボードの蓋をこじ開けようとした場合に内部のデータを自動的に破壊する機能を持っています。このような厳重で高いセキュリティの認証設備室の中に、さらに耐タンパの機能を持つハードウェアを使用して格納することで、電子証明書の発行に使用する認証局秘密鍵を厳重に保管・管理しています。

コラム

東日本大震災から学んだこと

東日本大震災は、2011年（平成23年）3月11日14時46分18秒（日本時間）、三陸沖を震源として発生した日本における観測史上最大規模の大地震で、マグニチュード9.0を記録し最大震度は7、場所によっては波高10m以上にも上る大津波が発生し各種ライフラインも断たれ、東北地方と関東地方の太平洋沿岸部に壊滅的な被害をもたらしました。

当時私は、東京での会合のために会社の後輩と一緒にあるビルの5階にいたのですが、東京にいても相当な揺れを感じたことを覚えています。建物はぐらぐらと横に揺れ、窓のブラインドもそれに呼応するように激しく揺れていました。そんな中、震源地が三陸沖であることを知り、すぐさま会社に連絡してみたのですが携帯電話は繋がりません。当然、その日の新幹線は不通、宿はどこも一杯で結局帰宅難民となってしまったのですが、幸いにも東京の取引先の方々に大変親切にしていただき、その取引先の会議室で一晩を過ごすことができました。

会合のあったビルを出たあと取引先にたどり着くまでの間、テレビから繰り返し流れる火災や津波の映像は、目を疑うほどのすさまじい光景で、一刻も早く会社や親族と連絡をとらなければとの思いから、その後も会社と連絡をとり続け何とかメールで連絡がとれるようになり、職場の状況も少しずつ見えるようになってきました。

職場では、もちろん電気、ガス、水道は使えなかったのですが、幸い机上の資料などがくずれた程度で、社員にも怪我はありませんでした。また、認証局に係る設備は、然るべき地震対策を講じているため問題ないだろうと考えていましたが、津波が来ていたらどうなっていたかわかりません。あとから聞いた話ですが、認証設備の非常用発電機の燃料があと１日遅れたら…という非常に厳しい状況にもなっていたようです。

お客さまにはご迷惑をお掛けしましたが、最終的な認証サービスへの影響は、震災当日の郵便送達遅延による影響のみで事なきをえました。
今回の大震災から学んだことは、運用面での課題は幾つかありますが、何よりも、震災以降、お客さまから問合せをいただいた際に「震災は大丈夫でしたか。頑張ってくださいね。」と温かい言葉をかけていただいたことがとても心の励みになり、今後、お客さまには今まで以上に感謝の気持ちを込めて、丁寧なサポートしなければならないことを再認識いたしました。

ちなみに私と後輩が帰宅できたのは、震災発生から４日後の３月15日でした。その間、ご支援ご協力いただいた方々に心から感謝申し上げます。

最後になりましたが、このたびの東日本大震災により、亡くなられた方々のご冥福をお祈り申し上げますとともに、被災された地域の皆さまとそのご家族の方々に心よりお見舞い申し上げます。

東北インフォメーション・システムズ株式会社