# 電子署名活用ガイド

## –デジタル化社会の信頼性確保のために–

第 3 版

2025 年 4 月 24 日

電子認証局会議

## 改訂履歴

| 版数 | 日付 | 内容 |
|---|---|---|
| 初版 | 2009 年 4 月 | ・初版発行 |
| 第 2 版 | 2013 年 9 月 | ・最新事例の追加<br>・「経営者」「実務者」「システム担当者」と章立てを分割 |
| 第 3 版 | 2025 年 4 月 | ・最新事例の追加 |

## はじめに

電子署名及び認証業務に関する法律（平成 12 年5月 31 日法律第 102 号、以下「電子署名法」）が制定され早くも 25 年になります。

世界の多くの国家でも電子署名制度が確立され、今後は国際取引においても電子署名が必須となる時代になるでしょう。

我が国でも民間の業務のペーパーレス化、電子化が進んだものの、未だに紙の利用は残存しており、電子的な仕組みでもセキュリティ対策は、ID・パスワードの利用にとどまっているケースも多いのが現状です。こうした中、紙の紛失による個人情報漏えい事故や、営業秘密にかかる電子データの漏えい事故などが頻発しています。 現在、企業では主要な課題として内部統制の確立が求められ、業務の透明化、さらに業務改善による効率化の推進があげられています。これら課題改善のためにもまず業務の実態を知る必要があります。さらに点検、監査の視点からは、監査対象の明確化、監査対象業務の記録が必須とされています。

企業が情報管理を適切に実施し、業務改善を進め、点検・監査を的確に行うためには IT の力を利用するとともに、その**ベースとして電子署名制度を利用した安全確実な運用体制を確立することが重要**です。

そこで我が国の認定認証業務を行う事業者が一堂に会し、電子署名・認証制度の普及促進を目的として活動を始め、2009 年から『電子署名活用ガイド』を公開いたしました。

本ガイドは電子署名法認定認証事業者が自ら執筆し、まとめております。どうぞご活用ください。

2025 年 4 月

**電子認証局会議**

# 図中に使用したアイコンの説明表

| アイコン | 意　味 | アイコン | 意　味 |
|---|---|---|---|
| | 未押印の紙文書 | | 電子証明書 |
| | 押印済の文書 | | 秘密鍵 |
| | 紙の証明書 | | タイムスタンプ |
| | 未署名の電子文書 | | CRL（失効情報） |
| | 電子署名済の<br>電子文書 | | 認証局 |
| | 電子署名＋<br>タイムスタンプ済の<br>電子文書 | | タイムスタンプ局 |

# 目 次

**改訂履歴** ..... **2**

**1. 経営者の皆さんへ** ..... **7**

1.1 デジタル化社会の脆弱性と信頼性 ..... 7
1.2 「紙」文書から「電子」文書へ ..... 7
1.3 電子化によるメリットとは？ ..... 8
1.4 戦略的法務とは ..... 8
1.5 電子化を進めた企業像（全従業員が電子証明書を所持） ..... 13

**2. 実務者の皆さんへ** ..... **15**

2.1 電子署名の法的有効性 ..... 15
2.2 電子化を進めた企業例 ..... 21
2.3 先行事例に学ぶ戦略的活用法 ..... 21
2.3.1 **メールへの電子署名** ..... 21
2.3.2 メールの暗号化 ..... 22
2.3.3 電子取引関係文書への電子署名 ..... 23
2.3.4 稟議書への電子署名 ..... 27
2.3.5 電子申請 ..... 28
2.3.6 電子入札 ..... 29
2.3.7 会社法（取締役会議事録） ..... 30
2.3.8 公開文書への電子署名 ..... 32
2.3.9 PL 法対応と先使用権保護 ..... 32
2.3.10 営業日報、業務記録 ..... 33
2.3.11 社内機密情報の暗号化 ..... 36
2.3.12 業務システムへの本人認証 ..... 37
2.3.13 国税関係帳簿・証憑類の電子保存 ..... 38
2.3.14 医療関連文書の電子保存 ..... 39
2.3.15 士業の電子申請 ..... 40
2.4 電子署名に用いる電子証明書とは ..... 41
2.5 電子署名の運用のポイント ..... 44

**3. システム担当の皆さんへ** ..... **49**

3.1 電子証明書利用時の操作方法 ..... 49
3.2 電子署名の技術的対策のポイント ..... 52
3.2.1 電子署名とは、どのような技術なのか？ ..... 52
3.2.2 署名形式について ..... 55
3.2.3 複数署名について ..... 56
3.2.4 署名とタイムスタンプ ..... 56
3.2.5 長期署名の必要性 ..... 57
3.2.6 電子証明書暗号アルゴリズムの移行計画 ..... 60
3.3 電子認証局について ..... 60

**4. 用語集** ..... **66**

**5. 関係法令とガイドライン** ..... **72**

**6. 付録 ..... 75**

6.1 電子認証局会議について ..... 75
6.2 認証局のサービスガイド ..... 75

# 1. 経営者の皆さんへ

## 1.1 デジタル化社会の脆弱性と信頼性

インターネットの普及により、生活やビジネスの場はサイバー空間に広がっています。ネットで簡単に購入やサービス利用申込が可能となり、チケットや搭乗券はスピーディーに予約でき、ネットから銀行振込やクレジットカード決済が簡単にできるなど、ネット上の情報が信頼でき、適切に利用可能な場合は、大変便利な世の中になりました。ビジネスの場でも、取引先や顧客との電子取引や、自社 Web ページを通じての情報公開、マーケティングなど、今やネットはビジネスにとって大変重要なインフラとなっています。

ところが、もしネットで繋がっている相手が、あなたが思っている相手でなかったとしたらどうでしょう？

- クレジットカードの番号を入力したサイトが本物でなかったら…？
- ネットバンキングから送られてきたメールに従ってアクセスしたサイトが本物でなかったら…？
- 電子取引で発行した注文書が不正に改ざん、流用されたとしたら…？

現在の企業活動は、電子情報の信頼性のもとに機能しています。一旦その信頼が崩れてしまうと機能不全に陥りかねません。

あなたがインターネットを通じて繋がっている**相手が、間違いなく本人であることを確認できる**ことも、電子取引で発行した注文書が本物で、改ざんされていないことを確認できることも、我々電子認証事業者が発行する電子証明書によって実現されています。電子証明書は、デジタル社会の脆弱性を克服し、信頼できるビジネスインフラとしてインターネットを機能させる上で、必要不可欠な社会基盤であります。

“電子認証局会議”に集う我々、電子認証事業者の役割は、電子認証サービスを通じて、そこで飛び交う電子情報の信頼性を担保し、デジタル社会のビジネスに信頼をもたらすことにあります。

## 1.2 「紙」文書から「電子」文書へ

企業活動を円滑で効率的に進める上で、ネット上のサイバー空間に繋がれた現代の社会は今までにない変革の機会にあります。“電子情報の信頼性”が確保できれば、従来、紙ベースで運用していた様々な業務を電子化しペーパーレスとすることで、より効率的で低コストな事業インフラを実現できます。

即ち、従来の紙ベースの業務をいかに電子化していくかが、経営課題の一つといえるでしょう。

では、どのような業務が“電子情報の信頼性”を前提に電子化できるでしょうか？ 以下の事例が報告されています。

- 顧客、取引先、従業員への通知、連絡

電子メール、公開文書

- 電子取引や取引情報の電子保存

見積、発注、契約、納品、請求、領収など

- 業務記録の電子保存

生産記録、品質管理記録、実施記録

PL 法対応、民訴法対応記録

- 国税関係文書、医療関係文書の電子保存
- 電子申請

官公庁などへの電子申請、電子入札、電子申告など

具体的に“電子情報の信頼性”を確保する技術的対策は**信頼される電子証明書を取得して電子情報に“電子署名”を付与することで実現**できますが、その法的裏付けとしては、2001 年に施行された「電子署名法」があります。本人により電子署名が付与された電子文書は、訴訟時の証拠としても紙と同等な証拠能力があるとされています。2005 年に施行された e-文書法で国税関係文書、医療関係文書など様々な文書の電子保存への道が開け、その利用が広がっています。

本書では「2-3 先行事例に学ぶ戦略的活用法」で詳しい事例をご紹介しています。

## 1.3 電子化によるメリットとは？

これまでの情報システムでは、記名押印が必要な文書を電子化できなかったが故に、どうしても書面による通知や保管といった業務プロセスが残ってしまいました。例えば顧客や取引先からの「申込書」や「契約書」は、今まで書面での受領が当たり前で、それが必要な仕事だと漫然と考えられているのが実態だと思われます。

しかしながら実は、そういった業務にこそ電子化の光を当て、紙を電子に置き換えてペーパーレス化することにより、さらなる効率化・大幅なコスト削減の余地が存在することに気づくはずです。

電子証明書の電子署名機能を導入し、紙を電子に置き換えた事例では、次のようなメリットが多数報告されています。

● 業務プロセスの効率化・スピードアップ

書類作成、仕分け・配送、受領、分類、ファイリング・保存、書類の検索、参照、廃棄など、いわゆる文書のライフサイクル管理に係る一連のプロセスの効率化、顧客対応などビジネスのスピードアップ。

● コスト削減

上記効率化に伴う人件費、印刷費、配送費、保管費などの経費削減。

また、契約書などの電子化の場合は、印紙税が削減可能。

● セキュリティ向上

電子文書の一元管理や、改ざん検知が可能となることによるセキュリティの向上、監査性、管理性向上、すなわち内部統制管理のレベルアップにより企業ガバナンスが向上。

電子署名の導入による全社的なペーパーレス化の推進は、今後の情報化投資を考える上で、情報化戦略の一つとして経営判断が求められる重要なテーマであるといえます。

## 1.4 戦略的法務とは

― 弁護士視点からの経営者への提言 ―

弁護士 牧野 二郎

**■戦わずして勝つ準備**

裁判は、費用もかかる上、結果の予想が確実に立てられないため、ビジネスとして捕らえることは大変困難です。もし、予め裁判を避けることができるならば、それは大変合理的といえるでしょう。以下にその方法を紹介します。

① トラブルの原因を作らないこと

裁判に繋がりかねないトラブルはさまざまです。

発注者と受注者の認識がずれていることに気づかず、漫然と作業を進めると、結果として出来上がったものが発注者の意図と全く違うものになり、これがこじれると損害賠償問題に発展します。

さらに要求仕様が変化し、それに漫然と現場が対応して、当初の内容とずれて、スケジュールに影響し、作業にかかるコストが大きく変化して、最後にこじれて、トラブルになることもあります。

また、単純に請負人側の任務の怠慢、担当者のスキル不足、下請けが事故を起こした場合など、事業の遂行において受注者側の一方的なミスが発生することもあります。

我が国では、契約が成立したら、一般に、現場が優秀なこともあり、決められた作業は常に順調に進み、予定通り終わってきたという認識がその基礎にあるようです。

ところが現実は必ずしもそうではありません。状況が急速に変化するため、企画した内容が数ヶ月で変更を余儀なくされるということもあります。

また、委託内容が複雑であるため、未熟な下請けが理解できないまま進んでいるということも起きるのです。

② 契約締結段階の注意

まず、契約段階から要求仕様や機能要件について、発注者と受注者とが、徹底した議論を行い、発注者の希望内容を精査して、内容を明確にし、かつ可能な限り言葉にして、相互の理解を確認し合うことが必要になります。

一般に発注者は「素人」ですから、イメージだけで語ることも多いものです。それに対して受注者は特定の分野の専門家ですが、相手が素人だということを忘れて、相手の言葉を自分の経験値や既存の専門技術に当てはめ、勝手に解釈し、理解したつもりになるのです。こうした行き違いを起こさないためには、まず、発注者側は自分のイメージを正確に表現し、伝え、伝わっているかを確認しておくことが重要です。受注者も、発注者の意味を解釈しながら、具体例を示しながら、何度も発注者の意図を確認、検証すべきなのです。

③ 契約遂行段階での注意

次に、契約後の契約管理が重要になります。契約は締結したら完成というものではありません。契約は、その後の作業に関する「基本合意」に過ぎない、と肝に銘じるべきなのです。契約が進行するに連れて、詳細を打ち合わせる必要が出てくるはずなのです。

契約を実施し、作業が進む中で、予想外の事態が発生し、発注者のイメージが実現されていないことが鮮明になることがあります。契約の実施によって、発注者のイメージが形になっていく中で、イメージと実際の成果物とのズレが現実問題として見えてくるわけです。できるだけズレが小さい早期の段階で修正を重ね、あるいは早期にズレを発見して、認識合わせを行い、必要なときは契約の修正を実施する必要があります。

このように、契約締結は終着点ではなく、むしろ「キックオフ」、作業開始の GO サインなのであって、そこからが本当の仕事が始まる、と理解すべきなのです。

契約は変化するものと理解して、それを動く契約として把握し、まとめきるのがプロジェクトマネージャーといわれる事業の管理責任者になります。

マネージャーは、作業の変化やスケジュールの調整をしながら、両当事者のズレや齟齬を明確にして、変化を修正する作業を担当して、当事者の満足する成果物を作成するという役割を果たすのです。

**■戦うなら、確実に勝つために**

契約を締結し、実施作業の管理に疎漏がない場合でも、トラブルが起きて、問題となることが

あります。発注者が次々と仕様を変更し、受注者に対して過度の負荷を与える事態が生じたり、当初の費用を変更しないなど我がままであったり、反対に、受注者が不誠実で、技量が著しく劣っていたような場合などもあります。

こうした場合には、早期に契約を解消する必要が出てきます。しかし目的が達成できていないのですから、発注者は契約の際約束された代金全額を支払おうとはしませんし、反対に、受注者は指定された作業をしていますので、その分を支払うよう求めます。こうして、支払いをめぐってトラブルが起きます。

戦うならば勝たなければなりません。勝つべき場合に、確実に勝つという意味であって、自分の側に責任がある場合は早期に認めて、早期に撤収するのが賢明です。

勝つべき場合に勝つこと、絶対に負けないためには、水掛け論を極力排し、当初から物事を正確に記録して、相手方とも合意しておくことが必須です。

トラブルの原因を明確にして、責任の所在まではっきりするような記録が必要です。この場合も、業務記録がものをいうことになります。

本来の有利な立場を維持して、不当に不利な立場とならないようにするためには、徹底して業務を記録し、本当の事実、内容を明確にする努力をして、それを相手に確認してもらい、記録にして確定させることが重要です。すなわち、電子的に記録や合意文書を作成する場合は、その真正性に一点の曇りも無いよう電子署名を付与するなどの対策が重要な役割を果たすことになります。もし、相手が事実を事実として認めないならば、相手方の不誠実さが鮮明になるような事実関係が指摘されているか（質問に対して回答しない、クレームばかり言うだけで解決しようとしない、など）とか、自分の方は誠実に徹底して対応した事実が残っているか、を立証するということになります。

**■裁判官の心証をわしづかみにするために**

裁判官の心証形成を理解しておくと、何をすべきか自ずと見えてきます。

裁判官は、トラブルの事象に常に精通しているわけではありません。仮に既に何件かトラブル解決を経験したとしても、それらとは事案が異なることを意識しており、経験だけに依存するような判断はしないはずです。

そこで裁判に当たって必要なのが、明確なストーリーと証拠を持つことです。当事者の関係、当事者の特質、それを踏まえて、何が起きたのか、原因はなにか、を明確に提示します。単純明快なストーリーと、それをしっかり裏付けるような証拠を準備して、提出します。裁判官は、信頼できる証拠（やり取りが記載された電子メールなど）があれば、事実認定も安心してできます。

訴訟の早期の段階で、裁判官が争点を把握しようとしている段階でしっかりと証拠固めすることが裁判官の心証をわしづかみにする方法なのです。

以前の訴訟では、重要証拠は隠しておき、証人尋問などで逃げ場をふさいだ上で劇的に提出して立ち往生させる、といった技巧を好み、また、弁護士の依頼者も相手を騙すことばかりに関心を持ち、裏をかかれないように証拠の後出しを露骨に要求してきました。

これは映画やテレビの影響で、劇的な意外性のあるストーリー展開を見せるための工夫に過ぎないのですが、素人は、それが現実に起きると思い込んでいるため、現実の場面でも同様に行動することを求めるのです。

ところが、実際の裁判は劇的でもなければ、意外性があるなどということもありません。むしろ地味で、淡々と証拠を積み上げていくだけなのです。

だまし討ちなどは利きませんし、証拠の後出しは「時機に後れた攻撃防御」として否定されます。必要な情報は早期に出して攻防を尽くすというのが、フェアな議論として尊重されているのです。

また訴訟の実務では、事前準備、準備手続が積極的に活用され、法廷での議論は激減して

います。法廷は主張の整理や、証拠調べ、証人尋問などで利用され、通常は裁判官室か、円卓のある部屋で全員同席して争点整理が進められます。しかも、証拠は隠さず早期に出すよう求められ、裁判官は早い段階で心証形成をしているのが実態です。

このような仕組みや実際の運用を理解した上で、信頼性の高い証拠を用意しておき、否定されない、偽造できない証拠として活用できるように電子署名などを付与した記録を作り、安全に保管・確保しておくことが重要なのです。

**■相手の手持ち証拠に期待しない**

ドラマなどでは、相手が証拠を隠して最後の場面でそれを暴くことで劇的に逆転勝利するといったストーリーが作られることがあります。サスペンスものの、いわば定番といえるでしょう。

刑事事件では、犯人の持っている証拠を強制的に捜索して確保するということが可能なのですが、民事事件ではそうした証拠の確保はできません。もし、相手が提出を拒否している証拠をどうしても取りたいという場合には、証拠保全、あるいは証拠提出命令などを求めることがありますが、実際には多くの限界があります。

証拠保全とは、裁判官に立ち会ってもらい、相手方の事務所や自宅に赴いて証拠を収集する作業です。米国では「ディスカバリー」という仕組みがあり、網羅的な証拠確保が行われ、意外な証拠が出てくることもありますが、我が国ではそうしたディスカバリー制度は採用されておらず、極めて限定的に証拠保全が認められるだけです。

証拠保全手続は、既に明らかな証拠を保全するだけで、それ以上の意味はありません。

ここから言えるのは、やはり、「自ら業務記録を丹念につけることで、訴訟の準備を進めるのが望ましい形であって、相手方の手元証拠に期待するのは意味のないこと」だ、という事実の理解が重要であるということです。

＜コラム＞

**電子データの証拠性が認められた判例**

ネットの普及により、裁判においても電子データが証拠として重要な位置を占めるようになってきています。

電子署名そのものではありませんが、電子署名に用いられる「ハッシュ関数」と呼ばれる技術が、裁判で証拠として扱われる事件がありました。

ファイル交換ソフト（WinMX）により、個人情報を含む電子データが流失し、プライバシーを侵害されたとする原告が、インターネットサービスプロバイダに対して、発信者情報の開示を求める請求を行った事件です。

（東京地判 H16.6.8　発信者情報開示請求事件　 判例タイムズ No.1212297 頁）

ハッシュ関数とは、電子データを決められた長さのまったく異なる文字列（ハッシュ値）に変換する技術で、2つの電子データのハッシュ値を比較し、それが等しければ、その電子データ同士は同一のものであることを証明できます。なお、ハッシュ関数は電子署名で、「公開鍵暗号方式」と共に用いられ、電子データが改ざんされていないかを検知するために利用されています。

この事件では、個人情報を含む電子データが、実際に発信者のパソコンから流失したものかが争点となりましたが、ファイルの同一性の証拠としてハッシュ値が用いられ、ハッシュ値の一致により個人情報を含む電子データが発信者のパソコンから流失したものであるという事実が認められ、原告の発信者情報の開示を求める請求が認められました。

このように、実際の裁判においても電子データが証拠として扱われるケースが出てきており、電子データに法的証拠性を与える電子署名の重要性がますます高まっていくと思われます。

＜コラム＞

**ある判例：合理的な情報収集・管理は経営者の責任**

取締役の責任が問われた事件で、裁判所が「情報の取り扱い」について明確な判断をしました。長銀事件の一つ、東京地方裁判所平成 16 年3月 25 日判決です。

この事件は、長銀がノンバンクに対して行った5つの融資が、取締役の善管注意義務違反及び忠実義務違反だとして、株主が当時の取締役などに損害賠償請求を行った事案で、東京地裁は、銀行の融資判断と取締役の情報管理責任に触れて、次のように判示ました。

「支援をしない場合と支援を行う場合に見込まれる損失を幅広く情報収集・分析、検討した上で、後者が前者よりも小さい場合、すなわち支援により負担する損失を上回るメリットが得られる場合にのみ、支援を行うことが許されるものというべきである。」

「このような判断は、情報の非対称と多数の経済主体間の複雑な相互依存関係の中において、これを取り巻く諸情勢を踏まえた専門的かつ総合的判断であることから、情勢分析と衡量判断の当否は、意思決定の時点において一義的に定まるものではなく、取締役の経営判断に属する事項としてその裁量が認められるべきであり、いわゆる経営判断の原則が妥当する。」

とした上で、さらに、

「取締役の責任を問うためには、取締役の判断に許容された裁量の範囲を超えた善管注意義務違反があったか否か、すなわち、意思決定が行われた当時の状況下において、原告と同程度の規模を有する大銀行の取締役に一般的に期待される水準に照らして、当該判断をするためになされた情報収集・分析、検討が合理性を欠くものであったか否か、これらを前提とする判断の推論過程及び内容が明らかに不合理なものであったか否かが問われなければならない。」

と判断したのです。

すなわち、最後に示されたように、

① 取締役の情報収集・分析、検討が「合理的」であったか否か

② その後の判断が「明らかに不合理」なものであったか否か

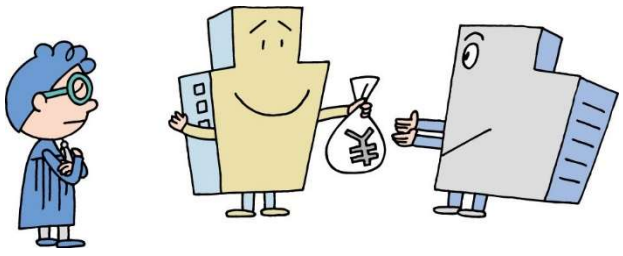
を問題とすべきだ、としました。

情報収集は、徹底して行い、合理的に収集しなければならない、と言うわけです。

ただし、二段目は、取締役の専門的判断を尊重して、その判断基準を「不合理な判断ではなかったこと」というように変えて、著しく不合理であって、とうてい説明ができないほどの不合理判断でなければ、責任を問わないとしたわけです。

こうして、経営者、取締役は、可能な限り合理的な情報収集をしなければならないし、その点の責任はあるけれども、そこをしっかりしておれば、その後の判断は専門家として尊重する、責任を問わないとしたのです。

情報収集、情報管理の必要性を明確にしてくれた、名判断といえる判決です。

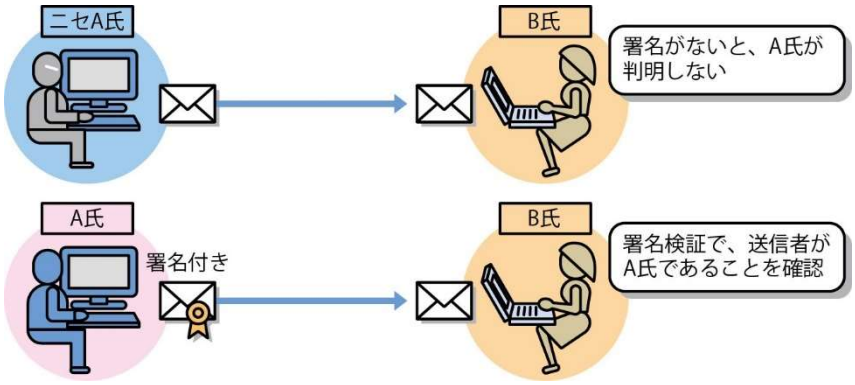


## 1.5　電子化を進めた企業像（全従業員が電子証明書を所持）

電子証明書が普及した社会・企業ではあらゆる業務を、効率よく、スピーディーに、かつ安全確実に実施できるだけでなく、大幅なコスト削減をも実現することが可能になります。また、電子署名された情報は、客観的な情報として第三者に提示することも可能になります（「2-1 電子署名の法的有効性」）。

**■電子情報のやり取り（メール利用などにおいて）**

お互いのメール送信時や、電子文書を用いて情報を発信する際には、情報元の確認が可能な『電子署名』を付与することで、悪意の第三者による「なりすまし」や「改ざん」を未然に防止できます。




また、特定の相手にしか解読できない電子文書を作成することも可能ですので、『電子親展文書』として機密文書や利用明細などの授受もインターネット上で可能になります。

対象となる書類
電子メール、稟議／決裁文書、利用明細など、機密文書　etc.

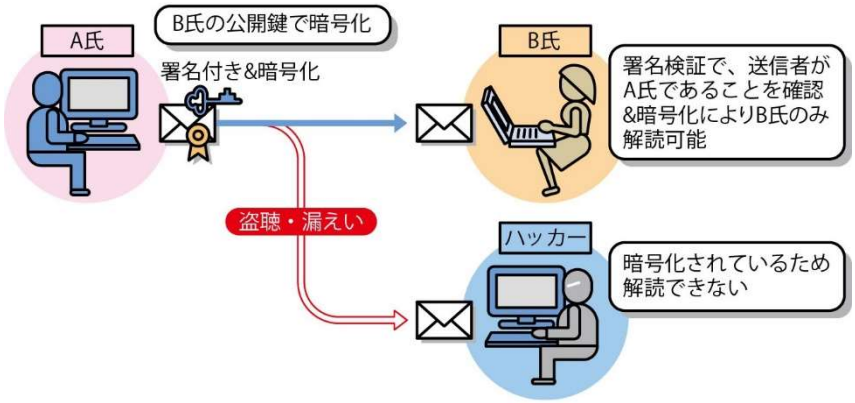



図1-2　電子親展文書の送信

**■営業において**

営業報告はもとより、交通費請求などの社内申請手続きも電子署名を使うことで、社内外からすべて電子的なやり取りで完結させることができます。

営業はその分、客先での商談時間を創出し、営業活動の効率を上げることができます。

対象となる書類
営業報告書（日報、週報、月報 など）、各種社内届（休暇届、出張届、欠勤届、遅刻・早退届など）、出張旅費精算書、各種契約書、見積書 etc.

**■経理において**

電子署名が付与された電子文書の利用が普及した世界では、仕事の効率アップ、経費の削減などの効果が最も期待できる分野です。請求書などの伝票類がすべて電子化され、管理コストの大幅な削減とともに、紙であれば当然かかっていた印刷費・郵送費・保管費をほぼゼロにすることができます。

対象となる書類
請求書、納品書、仮払精算書、出金伝票、入金伝票、振替伝票、仕入伝票、発注伝票、売上伝票、出荷伝票、決算報告書（貸借対照表、損益計算書 など）、元帳 etc.

**■製造（or サービス提供）において**

製造やサービス提供の現場で働く人たちは、手持ちの端末から作成した業務報告書に電子署名を付与し、管理者に素早く送ることができます。しかも、管理者が遠隔地で離れていても、当然何の問題もありません。さらに、顧客との間で何らかのトラブルが発生した際には、電子署名が付与された報告済みの業務報告書を証拠として取り扱うことも可能です。（電子署名法）

対象となる書類
業務報告書、図面、設計書、現場写真 etc.

**■研究・開発において**

製品開発に携わる研究者等は、研究や製品設計等に関するすべての電子記録に対し、電子署名・タイムスタンプを付与をしたうえで保存することで、知財における先使用権を確保しつつ、また、PL 法対応上の電子記録の真正性を確保できています。実験データ、実験の様子を撮影した写真や動画、会議の録音内容、メモ帳に走り書きしたアイデア、最終的な報告書、製品図面などを、数十年の長期にわたり証拠性が担保される方式で保存し、いつでも検索・確認が可能となります。

対象となる書類
研究ノート、研究開発レポート、研究完了報告書、技術成果報告書、研究月報、研究移管書、発明提案書、実験データ、設計図 etc.

# 2. 実務者の皆さんへ

## 2.1 電子署名の法的有効性

【文責】弁護士 牧野 二郎

本節では、電子署名の法的な意味について検討することにします。

これまで紙に印刷した契約書などに、署名・押印、または記名・捺印をしてきたわけですが、情報化の時代に果たして紙のままで良いのか、印章の管理や使用方法はこのままで良いのかを、真剣に検討すべき時期にあるといえます。

情報化の中で、我が国の産業の更なる効率化が強く求められています。少子高齢化による働き手の減少という事実に直面していることから、契約書や契約実務の中にも IT の技術を活かした対応が求められるでしょう。また、国際競争力の強化が求められており、その面からも効率的、合理的な契約実務、契約書作成が必要となっているのです。

### なぜ電子署名なのか？契約書の役割の変化

**＜契約管理の意味と重要性＞**

これまでの一般的な認識によれば、契約書の作成というのは、契約交渉のまとめとして、交渉の最終段階のまとめの意味であり、これで条件や内容が確定したもの、といわれてきました。契約書が完成しますと、社長や総務部長がこれを管理して、トラブルが起きたら出してくる、問題が発生したときにはじめて検討する、という類のものでした。通例では問題は起きず、その履行をじっくりと待てばよいわけです。営業面での売上も、契約した時点で確定したとされて、それがひとつの区切りとなっていたわけです。

そのため契約書は、契約違反に厳しく、罰則や、解除条項がしっかり書かれているのが重要といわれてきたのです。

ところが、情報化の時代、そして急速な環境の変化の中では、こうした契約書の持つ意味合いも変わってきています。情報化の持つ機能は多様ですが、特徴的なものだけ見ても次の3点が挙げられます。

● 第一に、情報化により時代の変化が激しくなり、それに応じて機敏、迅速な対応が求められてきたこと（高速化）

● 第二に、情報交換が頻繁に行われるため、情報の管理が重要になってきたこと（情報管理）

● 第三に、効率化の促進で、アウトソーシングが活用され、関係企業が増加し、それらの契約、契約実施、サービス管理などが重要となってきたこと（品質管理）

こうした主要な変化は今やどの職場にも見られるものです。電子メールや各種のファイルのやり取りなくして業務は進まなくなってきているのです。

こうした大きな流れの中で、契約書、契約実務もまた高速化、情報管理、品質管理など様々な面から、変化することが求められているのです。

こうした時代の背景の変化は、内部統制という形で法的な要請にもなってきました（会社法、金融商品取引法）。多くの企業が内部統制を進めるなかで、契約書の意味合いが大きく変化してきています。

これまでの契約が、交渉の「まとめ」として認識されてきたのに対して、内部統制時代の契約書、契約実務では、まとめではなく「スタート」という認識になりつつあるのです。すなわち内部統制の

ポイントは業務管理であり、製品やサービスの品質を正確に適正に管理することが求められるわけですが、それを実行するには、アウトソーシング先企業の業務内容の点検も必要となるのです。業務を管理するということは、外部の企業に任せている業務も管理するということを意味するのです。ここから、契約書の最も重要なポイントは、ペナルティ条項だけではなく、むしろ、業務管理の方法を明記して、契約の履行、契約に従った業務遂行が確認できるような内容になっていないといけない、ということになってきているのです。

こうして契約書は、業務内容を管理する指針、基本方針を示すものとなり、その付随書類として求められるものに業務の基準を定める「仕様書」、そして契約当事者が互いに業務の内容を点検できるように合意した「品質合意書（サービスレベル・アグリーメント：SLA など）」が必要となるのです。仕様書や SLA は、責任者が机の中にしまっておくものではなく、日常の業務遂行を管理するために、点検表、確認のための基準書として日常的に、かつ現場で使われるものなのです。

**＜電子契約という要請＞**

では、こうした契約書、契約実務に対する変化は、契約書作成、契約実務にどのように影響するのでしょうか。日常的な情報交換が電子メールなどにより、電子的に行われていることから、契約の交渉も電子メールにより行われ、契約書の案文が添付ファイルとしてやり取りされています。契約当事者が相互の要求を指摘しながら、現実に最も適合した契約とすべく、修正を繰り返すという形になってきています。これまでのような活字印刷した契約書を一方的に押し付けるというものではなく、合理的な契約交渉、的確な契約の作成が求められているのです。こうして、契約交渉の電子化が進んでいるのです。

次に、契約書そのものは紙に印刷して、各自署名押印を、という作業がいまだに多く行われています。その結果、類似した契約に関する検討に際して、最終決着した契約書を参照するためには担当者にその契約書を探してもらい、その都度コピーし、郵送してもらうなど、不便な状況にあります。これを回避するため、起案段階の不確かな契約書案を利用したり、最初からすべてやり直すなどの不経済な作業が繰り返されているのです。大量の契約が行われている企業では、類似契約を探すことすらできない状況にあるようで。これでは業務の効率化は図れません。

さらに、内部監査や監査法人による業務点検の際に、必要となる契約書の確認や関連書類の確認などを遠隔で行うことができず、つねに契約書を保管している現地事務所に出向かなければならず、監査費用の高額化を招いているのです。

しかし、これまで紙による対応をしてきましたので、電子的な処理が進んだとしても、そのことから決定的な支障が生じたわけではありません。紙による処理が基本であったことから、紙の処理に対応した商慣行が確立してきたともいえるのです。たとえそれが不適切、不経済でも、ともかく動くものであり、ゆっくりとした時代には合理的な仕組みとして機能していたのです。

問題は情報化の中で、そうした旧態依然とした制度のみに依存して、効率化が図れるのか、競争力は出るのか、ということなのです。企業の周辺で電子化が急速に進み、諸外国にあっても急速な電子化が進められているわけであり、その流れは押し留めることができないものであり、かつますます高度化し、高速度化していくのですから、その環境変化に対応することが必要となるのです。現状肯定だけでは、環境変化に対応できなかったマンモスのようなってしまうでしょう。

企業を取り巻く、急速な環境の変化に対応せず、「今のままで支障がないじゃないか」と言っている法務対応の体質では、そうした企業は環境に見放され、熾烈な競争のなか、競争力を失い、マンモスのように淘汰され、自滅してゆく運命にあるといってよいでしょう。

契約の世界だけを見た場合、特段、今の紙の世界、紙を活用した仕組みに欠陥があるわけではないのです。ただ問題は、情報活用ができず、効率化の大きな支障となり、様々な非効率的な対応が求められる結果、企業全体によどんだ業務処理を残してしまう危険性が指摘されてい

るのです。

**証拠としての有効性**

電子契約は果たして証拠として認めてもらえるのだろうか、という疑問をもたれる方は多いと思います。これまでのような署名押印で、判子の印影が赤く出ていないと認められなかったという体験からは、電子的なものでは赤い判子の印影がなく、否定されると思いがちなのです。この反面、従来は赤い印影があればよいとばかりに、三文判が大量に売り出され、誰でも自由に文房具屋で購入して利用することができ、それでも赤い印影がついていることで、なぜか許容されるというものでした。

そこで我が国の法制度における契約の形態を見てみますと、興味深いことがわかります。まず、契約は意思の合致により成立するとされていますので、口頭での契約があります。株式の売買などは多く電話での意思確認だけで進めていますので、その典型ともいえるでしょう。小額の契約もまた口頭だけで成立し、実行されています。こうした口頭契約も契約として、確かに成立し、

有効であり、かつ証拠として認められるのです。ただ、立証方法の点で紙での契約に比べて困難な点があるという問題があるわけです。そこで、録音やメモをとるといった方法で争いを防止しているのです。その点、契約内容を紙に書いて互いに判子を押すという手法であれば、同一内容を両当事者が検討して、確認して押印したと考えられることから、口頭契約よりも安心感があり、かつ立証も比較的容易となるわけです。ただ、この場合でも第三者が勝手に三文判を購入して利用した場合などは、他人に成りすますことができますので、争いがないわけではありません。また、内容の偽造も可能であることから、成立した契約に合意以外の事項を付記したり、金額を変えたりするといった行為が行われて争いになることもあります。

紙の契約書の場合は、その紙の契約書の存在が争われると、関係者の証人尋問や関連証拠の検証などが行われ、総合的に判断することになります。そのため、実印を使用した契約書への押印と印鑑証明書を添付するといった方法で、こうした争いを可能な限り未然に防止するという対策が採られるわけです。

**＜では、電子契約はどうでしょうか＞**

電子契約にも口頭契約にほぼ同様といえるメールによる意思の合致や、書面と同様に一定の判子同様の電子的サイン（簡易な電子署名など）を行うことも可能です。さらに、公的に認められた認証局が発行する電子証明書を利用して正確に署名し、契約するという方法が提供されています。

電子契約であれば、紙の契約以上の絶対的な効果があるか、といえばそうではありません。紙でやるか、電子でやるのかは方法論（技術）の違いであって、法的な効果としてはまったく差がないというのが本当のところです。

まず、電子メールなどで交渉して、契約が成立した場合ですが、電子メール自体が証拠になります。ほとんどの場合電子メールそのものが正しく成立したものとして立証に利用され、偽造の主張で争われることはきわめて少ないようです。したがって、電子メールだけでも証拠として利用できるのです。

ただ、争われた場合に困難な事態になる危険があるので、CC（同報）を行うなの対策も必要とされています。

次に簡易な方法で電子証明書を利用して契約することができます。電子証明書にも様々な用途に従い、多様なものが用意されています。それらを利用してサイン（電子署名）することができます。電子署名は、暗号技術に基づき改ざん検知が可能ですので、原則として偽造、変造の主張を防ぐことができます。ただし、実際にサイン（電子署名）したものが、そこに表意者として表示された本人であるかについて争われた場合（自己否認をした場合）にはその署名の際に利用し

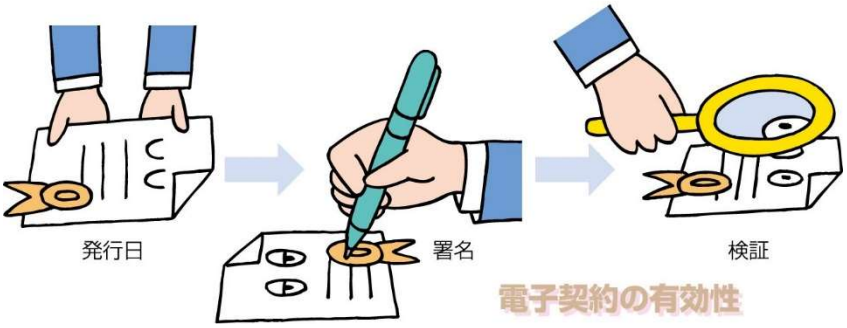
た電子証明書とその秘密鍵が本人のものであり、かつ本人が管理し、利用していたものであるとの主張立証が必要となる場合があります。

この点所定の認定認証局から発行される電子証明書は、その基礎に戸籍制度や住民登録制度、印鑑証明制度を置き、それらに基づく証明方法を事前に確認して作成しているため、本人のものとして本人が作成したことが厳格に確認され、証明されるものとなっています。なお、実印と同様に所定の秘密鍵を適正に管理しておくことが必要です。

### 電子契約の成立及びその確認（検証）

電子契約、特に認定認証局の発行する電子証明書、秘密鍵を利用して署名（電子署名）した契約の場合には、どのようにその成立などが確認されるのでしょうか。電子証明書の有効性などとの関係はどうなるのでしょうか。

まず、契約自体は口頭でも成立しますが、その確かな成立の証拠としては電子署名法に基づく電子署名の付与および電子署名の検証が必要です。この点、印鑑証明書の場合には、契約時点でのその内容の正確性は確認できません。ただ、印鑑証明書の提出先側で期限を設け、発行された日から例えば、3ヶ月以内のものを要求しているというだけです。一般に不動産売買の際には、不動産移転登記申請する場合に印鑑証明書を提出しますが、その時点では住民票の変更が同時進行するため、交付された時点ではすでに表記された内容が現実とは一致していないことが多いのですが、その点を含めて問題とはしていません。ただ単に、その発行のときに確かにその住所を持っていたため、その時点で本人であったとの確認をした、という事実をもって本人性を確認しているというわけです。




電子署名の場合には、実はさらに電子証明書の厳格な管理という視点から、発行日に有効であるだけではなく、その後、相手方が確認する場合にも、正しく電子署名がなされたことを検証できることが求められます。もし、署名時にすでに失効届けがなされて電子証明書が失効している、または有効期限が切れているということになりますと、検証ができない事態となり、電子証明書の有効性に問題があるということが判明するため、契約者に注意喚起することができるようになっています。

こうして電子署名は、署名に用いる電子証明書がいったん発行された後にも、その電子証明書が失効していないか確認する仕組み（検証）が用意されていることで、その信頼性が確保されているのです。

#### ＜電子証明書の失効と契約の有効性＞

電子証明書には有効期間があり、その期間内であれば署名もできますし、検証によってその電子証明書の有効性の確認が可能です。しかし、有効期間を経過しますと署名時点の有効性が確認できなくなります。

署名の検証ができない場合でも、契約当事者間で検証できないことに同意しており、その同

意が後に争えないように記載されるなどしていれば、ひとまず問題はないといえそうです。しかし、後日そうした同意の存在自体まで否定されたときには、元も子もありません。

結局、所定の電子証明書の検証ができず、失効の有無が確かめられない場合や、仮にそれを知って同意していたとしても、後にその同意自体の存在を争われたりすれば、結局、電子署名の効果を主張できなくなりますので、電子署名が無いのと同じものとして、すなわち電子メールなどで契約したときのように、電子契約としてその契約書の成立を立証しなければならなくなります。

したがって、たとえ信頼性の高い電子署名方式を採用したとしても、その信頼は署名検証が可能であることが前提となっていますので、電子証明書の有効期間を越えた場合の署名検証を有効にする手段を確保するか、有効期間中の署名検証結果を明示する情報を添付する方法が確保されるべきでしょう。

### 印紙税はかからないのか？

電子署名による契約のメリットの1つとして、印紙税がかからないことが挙げられます。これは印紙税法が税の支払いを免除しているわけではなく、法律の規定によれば紙の契約書に対して、所定の金額の印紙を貼付して納付するとしているために、電子的な手続きではそうした「貼付」が現実にはできないため、納付方法がない、というのが現実なのです。

印紙税法では、次のように規定しています。

「課税文書の作成者は……（中略）……当該課税文書にはり付ける方法により、印紙税を納付しなければならない。」「……当該課税文書に印紙をはり付ける場合には……当該課税文書と印紙の彩紋とにかけ、判明に印紙を消さなければならない」（印紙税法第8条）と、規定して、印紙は文書に貼り付け、その貼り付けた印紙を印鑑で消して、再利用できないようにしなければならないとしているのです。

したがって電子文書には貼り付ける場所もなく、貼り付ける方法もないため、事実上免税になるという結果になります。

この点については、福岡国税局の以下の回答で確認できます。

「注文請書の調製行為を行ったとしても、注文請書の現物の交付がなされない以上、たとえ注文請書を電磁的記録に変換した媒体を電子メールで送信したとしても、ファクシミリ通信により送信したものと同様に、課税文書を作成したことにはならないから、印紙税の課税原因は発生しないものと考える。

ただし、電子メールで送信した後に本注文請書の現物を別途持参するなどの方法により相手方に交付した場合には、課税文書の作成に該当し、現物の注文請書に印紙税が課されるものと考える。」

https://www.nta.go.jp/about/organization/fukuoka/bunshokaito/inshi_sonota/081024/02.htm#a03

『福岡国税局＞文書回答事例＞印紙税その他の間接税＞請負契約に係る注文請書を電子的記録に変換して電子メールで送信した場合の印紙税の課税関係について』

したがって、電子メールなどによってやり取りする限りでは、印紙税の課税原因がないとするのが、公式見解と考えられます。

＜コラム＞

**電子文書の証拠能力、証明力**

**■設計図などを紙に代えて電子データで保管することでよいでしょうか？**

e-文書法（民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法

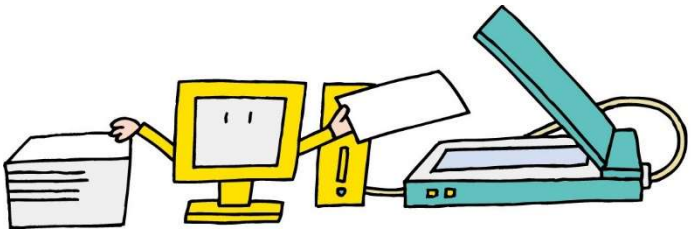
律）は所轄官庁の指定により電子データを紙の書類に代えて保管することを可能にしたのですが、e-文書法の対応となっていないものも数多くあります。たとえば製造物責任法の場合、事業者は各種の設計図などを保管しておく必要があり、保管期間は 10 年と長期になります。

そのため、製品ごとに紙の書類すべてを保存することになるのですが、保存には安全な保管場所や多額の管理費用、管理人員などが必要となります。

もし、電子データで保管できれば、こうした経費を削減できるため、経団連などから電子データの保管を認めるように要請が出されています。

電子データの保管を考えた場合、電子データと紙の書類との信頼性、長期保存性、見読性の確保について多くの議論がありました。デジタルデータや、電子証明書、それらを記録する媒体の安全性などの議論も進んでいます。その成果から見ますとこの点ではほとんど問題となることはありません。したがって、技術的には電子データの保存は、紙の書類の保管とほぼ同等の機能、信頼性を持っているといっていいのです。この点からは、電子データは証拠としての十分な意味、信頼性があるといえるでしょう。

問題は、電子データと他の証拠、人の記憶などとの関係付けです。電子データの最大の特徴は媒体から開放され電子信号となるため、コピーや送信が自由に行える点です。その結果、電子データと物、他の証拠との関係性が大変希薄になるという問題があります。



例えば、電子メールには筆跡がないので、書き手を特定することができません。紙であれば筆跡の他、筆圧、使われた紙、インクの色やにじみ、風化の状況など、様々な情報と関連付けられているのです。こうした違いから、電子データを証拠として利用するためには、ある工夫が重要になります。

**■電子データを作成する際の工夫**

電子データを作成する際には、作成者と電子データを関連付ける工夫が必要です。電子データに作成者の電子署名を付与することでデータと作成者の関連付けが図れますが、その場合にも電子署名というデジタルデータが本人の意思によって作成署名され、利用保管されたことを示す必要があります。電子データを作成する際の規則の制定、規則に従って作成したことの記録、通し番号、製品とデータとの関係を示す情報などが作成されている必要があります。具体的にはどのような文書に電子署名をつけるか、その際の電子署名はどのようなものか、その署名に利用する電子証明書はどのように保管され使用されるのか、などを定めた「電子署名利用規則」、作成された電子データを保管管理するための「電子文書管理規則」といったものが必要でしょう。

**■電子データを証拠として利用する場合の工夫**

電子データを再現して、利用する際にも注意が必要です。どのような状態で電子データが保存されていたか、誰が管理していたか、管理に関する規則はどうか、管理状態はどうであったか、といった情報が重要です。こうした情報がその電子データの価値を大きく左右することがあります。また、電子データを見えるようにするためにプリントする際にも、プリントの条件や環境などを記録しておく必要があります。

こうして電子データを証拠として利用する場合には、単に CAD データや PDF ファイルなどを

単体で提出するのではなく、その電子データのもともとの作成経緯や作成者との関連、証拠化した際の状況などの情報とともに示すことが有効です。

以上の工夫をして電子データを保管すれば、様々な場面で利用することができ、必要な情報を大量の紙で保管するのに代えて電子データと関連書類だけに集約することも十分に可能となります。

## 2.2 電子化を進めた企業例

全従業員が電子証明書を持ち、企業内のあらゆる部署、場面で電子署名が使われています。取締役会議事録などの各種議事録、業務や営業の結果を記録報告する営業日報や業務記録、IR 文書のように広く一般に公開する各種文書、研究開発での成果や報告などの研究ノートや図面、官公庁などへ提出申請する各種文書、顧客や取引先との契約書、などなど。これによって、コストの削減、仕事の効率化が進み、社員はそれぞれの仕事に、より専念できるようになります。

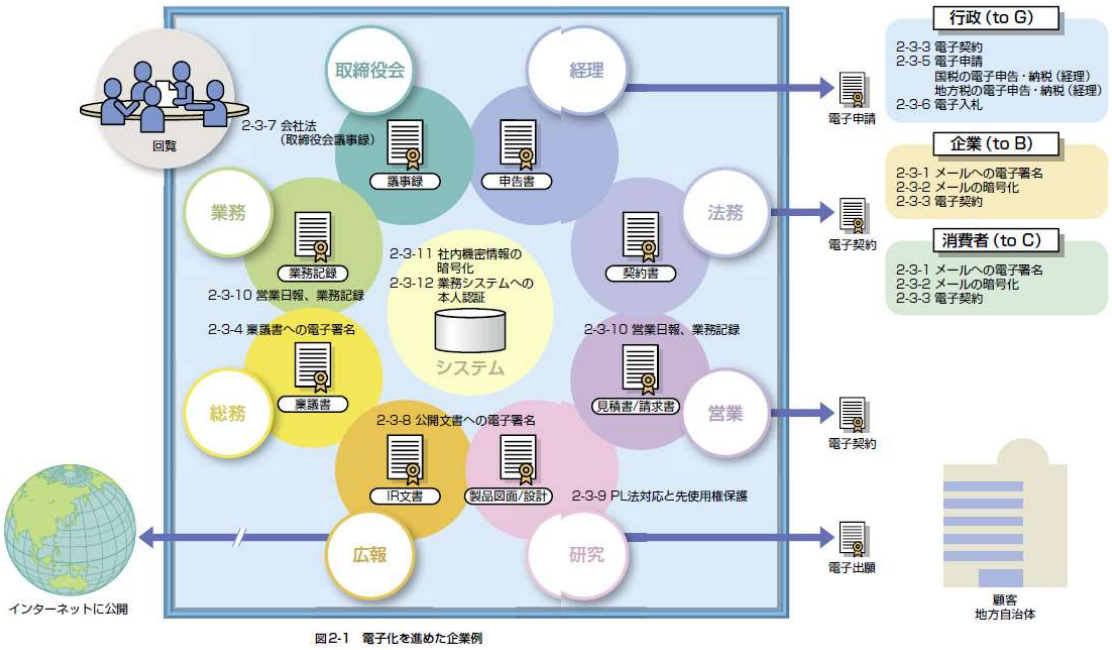



図2-1 電子化を進めた企業例

## 2.3 先行事例に学ぶ戦略的活用法

### 2.3.1 メールへの電子署名

電子メールの差出人の書き換えは意外に簡単にできてしまいます。つまり現在のネット上では、多くのなりすまし電子メールが飛び交っています。このため、差出人の表示のみを信頼した結果、フィッシングサイトへ誘導され、ウィルス感染されたファイルによる被害が発生するという事例も多数報告されています。

また、自社の名前をかたった不審なメールを送付されてしまい、お客さまや取引先に損害を生じさせる事例も多数報告されています。

電子メールが自社の発信であり、その内容が改ざんされていないことが確認でき、受信者が

安心して対応いただけるようにすることが必要です。
そのためには、**電子証明書を用いた“電子署名”が有効です。**

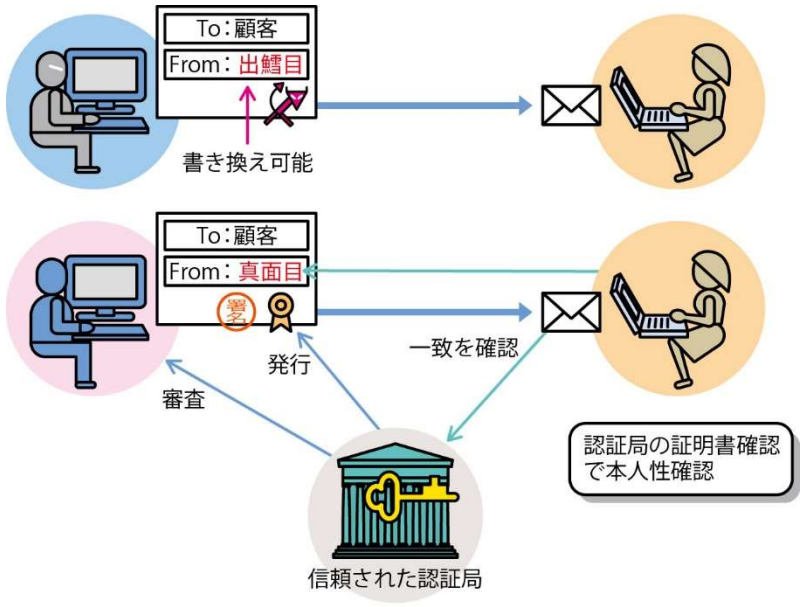
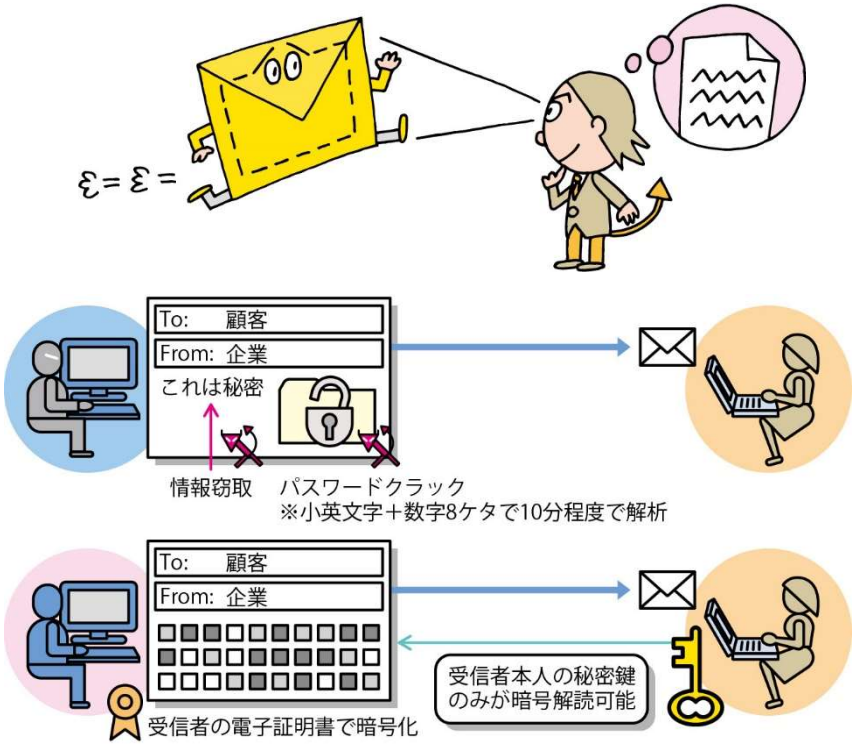



図2-2　メールへの電子署名付与による本人性確認

事例
◆業種：企業全般　金融機関では平成 17 年度に取組実施
◆対象業務：お客さまや取引先への連絡
◆導入メリット：
お客さまや取引先が
● 自社を語るなりすましメールでないことが判断できる。
● 自社からの連絡内容が改ざんされていないことを判断できることにより、大切なお客さまや取引先をフィッシングやウィルス被害などの被害を未然に防止します。
また、Outlook や Thunderbird など一般的なメールソフトで利用できます。

### 2.3.2　メールの暗号化

電子メールの送信データは、送信経路上で第三者が情報を取得することが簡単にでき、メールの題名や本文の記載内容が読み取れてしまいます。また、添付ファイルについて、暗号化していない場合はそのまま読み取れてしまいます。仮に zip などのパスワードにより暗号化したとしても、別のメールでパスワードを伝達したのでは、経路上で窃取される危険性が高いことからセキュリティは低下してしまいます。口頭で伝えるとしてもパスワードの長さは限られてしまい、高いセキュリティは実現できません。




受信者の電子証明書による電子メール暗号化（S/MIME）では、メールの受信者本人にしか開けない強力な暗号化を施します。開くための鍵はメール送信者でも知りえない情報ですので、**受信者本人しか開けません。**

事例
◆業種：企業全般
◆対象業務：個人情報を扱う業務、新技術情報やその仕様のやり取り
◆導入メリット：
● 個人情報や新技術情報などの機密情報を含むような依頼および回答内容でも安全に送信できます。
● 受信者の電子証明書（公開情報ですので、秘密ではありません。）を事前に入手する必要がありますが、パスワードのやり取りは事前にも事後にも必要ありません。
● 受信者本人のみが暗号を解くことが可能であり、万一第三者にメールデータを窃取されても、暗号を解くことができないため、秘匿したデータが漏えいすることがありません。万が一、宛先を誤ってしまっても、同様に内容は、秘匿できます。
● パスワードよりもはるかに強固な暗号化が施されます。
● Outlook や Thunderbird など一般的なメールソフトで利用できます。

### 2.3.3 電子取引関係文書への電子署名

**■電子契約**

従来、紙文書での交付や手続き、保存が義務付けられていた書面を、2001 年の IT 書面一括法の施行により、送付される側の同意を条件として電子メールなど電子的な手段で交付することが可能となりました。電子契約とは従来、書面により取り交わしていた契約書を、電子ファイルで作成し、当事者双方の電子署名を付与して保存する電子的な契約方法です。

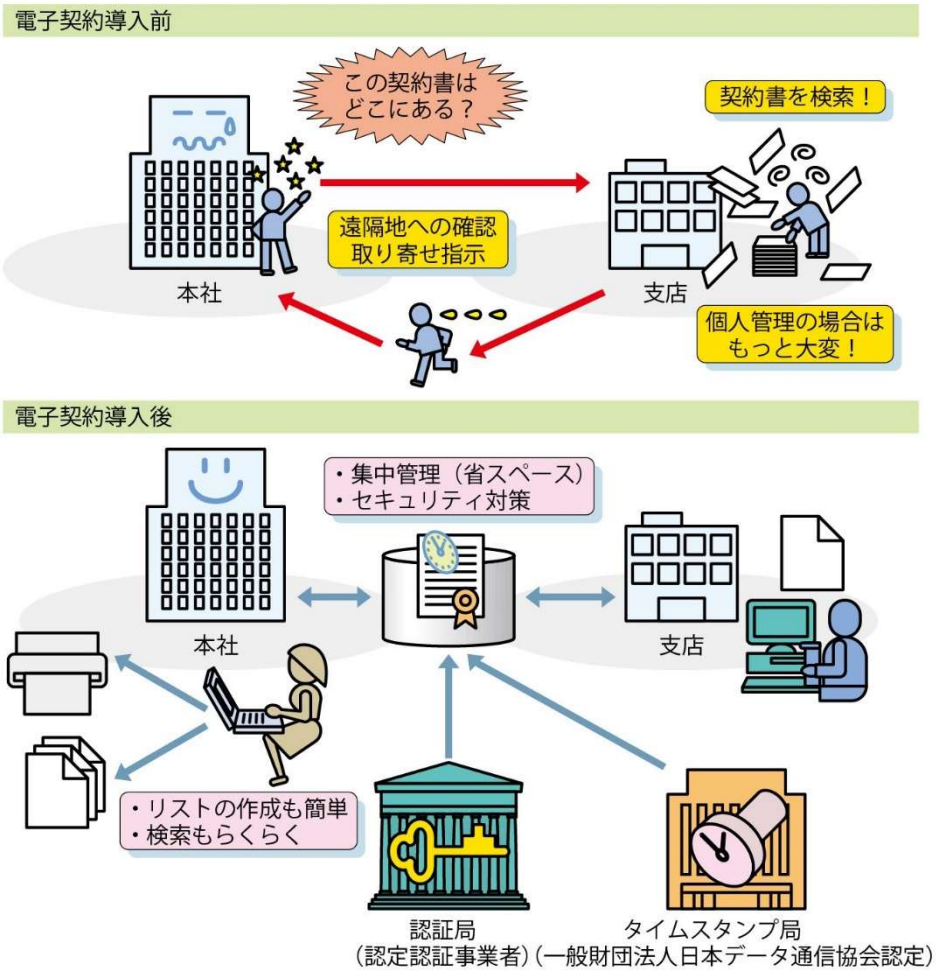



図2-4　電子契約導入前後の比較

事例
◆業種：企業全般
◆対象業務：契約業務
◆業務内容：電子契約書の作成、契約の締結、電子契約書の管理、電子契約書の電子保存
◆導入メリット：
(1) 印紙税が不要
● 電子データによる契約締結が可能となり、電子データは非課税「2-1 電子署名の法的有効性」の「印紙税はかからないのか？」参照
(週間税務通信 No.2672 より、以下記事要約)
【記事要約】
IT 書面一括法が今年(2001 年)4 月より施行されたことより、問題となるのが印紙税の取扱である。
(中略)本誌では、この IT 書面一括法施行後も従来通り電子データによるやり取りを、印紙税の課税文書とみなさない旨当局に確認した。
すなわち、ネット上を行き交う電子データは、印紙税法上の文書として認識されない、印紙税課税そのものが及ばないことになる。
(2) 事務コストの削減
● 契約書管理事務に携わる、人員のコスト削減
● 通信・交通費の削減
● 契約書の郵送などによる通信費用が不要
● 文書保管に関わる費用が削減
● 保管場所の省スペース化が可能
(3) 契約管理の徹底
会社法ならびに金融商品取引法において内部統制が求められている現在、取引の正当性を証明するのは契約書です。
契約書を紙から電子データにすることにより、確実かつ効率的な契約管理が実現可能となります。

**■請求書などの電子化**

2001 年の「電子署名法」の施行により、書面に記名、押印して作成される書類を、電子的に作成する場合、本人の電子署名があれば、法的に書面に記名、押印して作成される書類と同等の証拠能力を有すことになりました。

これを、電子取引に応用すると、電子的に作成した発注書や請求書などに、作成責任者の電子署名を付与すれば、紙の発注書や請求書などと同等の証拠性を有した電子文書が作成可能になります。

また、2005 年4月の「e-文書法」の施行に伴い「電子帳簿保存法」の一部が改定され、“国税関係書類のスキャニング保存”と、“電子取引情報の電子保存”が容認されました。なお、両者ともに「電子帳簿保存法」で示された要件を満たす必要がありますが、電子取引情報を“電子保存”する際には税務署などへの届出までは必要としていません。

これら2つの法律に基づき、近年、請求書などを電子的に作成、配信すると共にそのまま電子保存を行う事例が増えてきています。

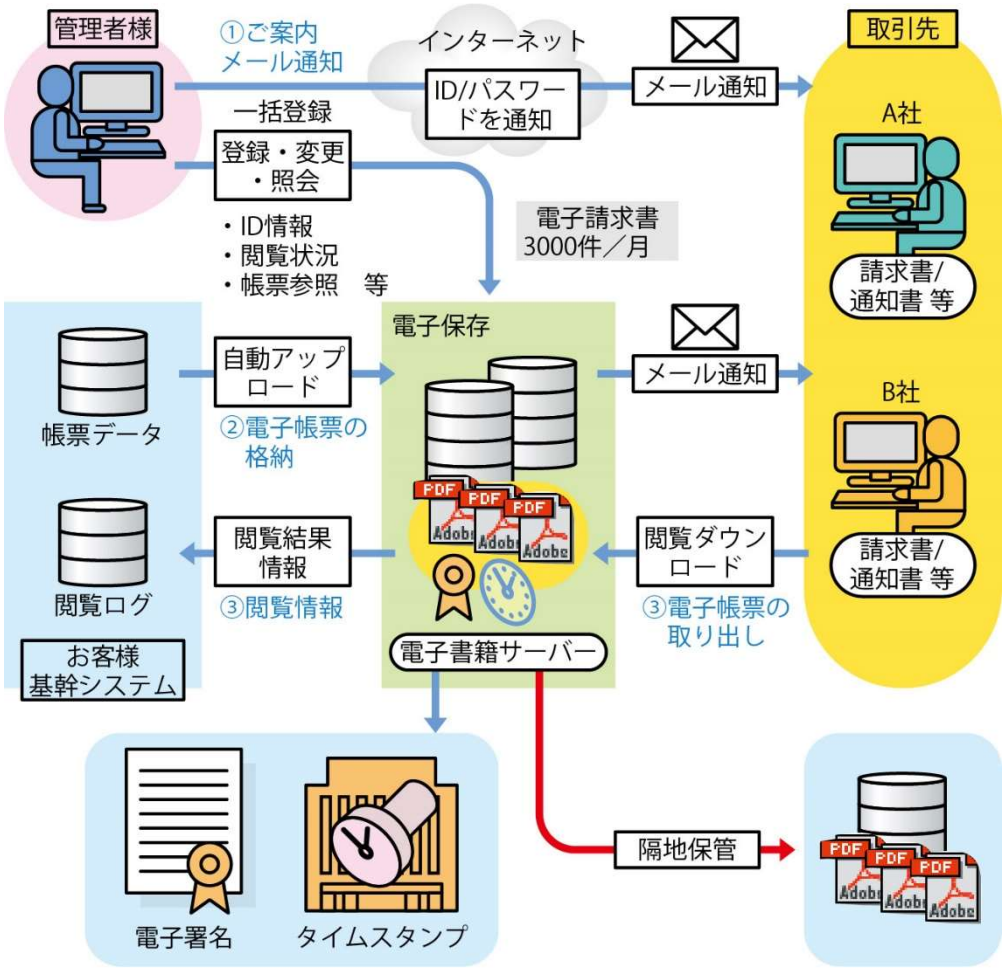



図2-5　請求書電子化の例

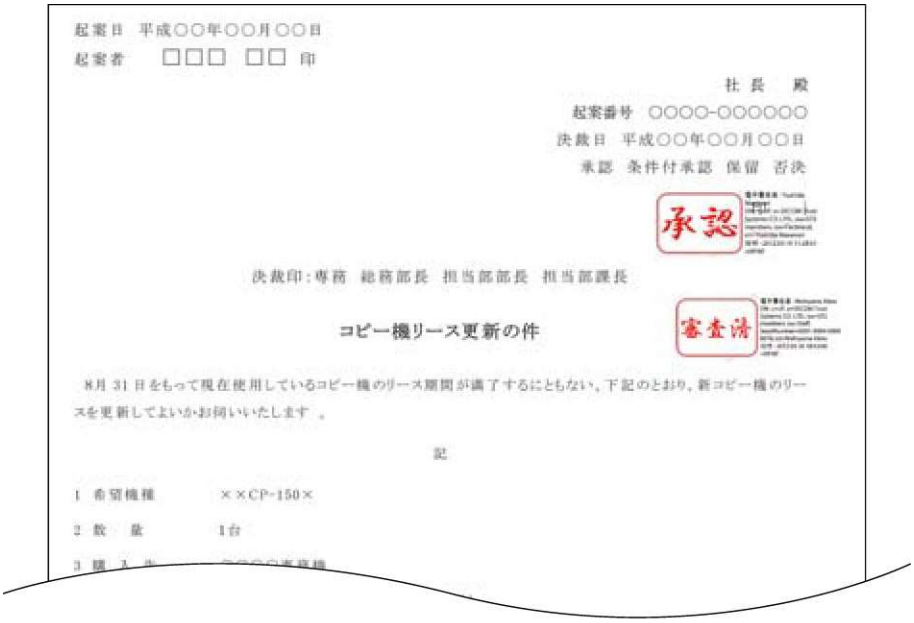
事例
◆業種：製造業、サービス業、流通業など、企業一般
◆対象業務：請求書の発行、送付、保存業務
◆業務内容：従来、基幹システムのデータで作成した請求書をプリントアウトして、顧客別に仕分け、発送作業を行っていたが、請求書の電子データに電子署名とタイムスタンプを付与した上で電子配信し、そのまま電子保存する。
◆導入メリット：
(1) コスト削減
● 印刷コスト、郵送コスト、保管コストなどの削減
● 紙の原本のファイリング業務など、紙さばきのための管理人件費の削減
(2) 業務の効率化
● 請求額の問い合わせ対応業務がなくなり業務の効率化を実現
●請求額がすぐに確定でき取引先からも高評価を獲得
●従来の書類保管スペースを、別の目的に有効利用可能
(3) リスク対応力の強化
●原本が電子データとなり、原本バックアップが可能
(4) 地球環境への配慮
●請求書や明細書類のプリントアウトがなくなり、紙を節約

### 2.3.4 稟議書への電子署名

従来、紙文書にて手続を行ってきた稟議書の回議に、電子署名を活用することで内部統制の強化および経費削減効果が期待できます。

事例
◆導入メリット：
(1) 承認者の証明および非改ざん証明
承認者および承認された情報が第三者に改ざんされていないことを証明できます。
(2) 経費削減
ペーパーレスよって紙媒体、印刷、保管などに係る経費の大幅な節約が可能になります。

図2-6　稟議書回議の電子化メリット


起案日　平成○○年○○月○○日
起案者　□□□　□□　印

社長　殿
起案番号　○○○○-○○○○○○
決裁日　平成○○年○○月○○日
承認　条件付承認　保留　否決

承認

決裁印:専務　総務部長　担当部部長　担当部課長

審査済

コピー機リース更新の件

8月31日をもって現在使用しているコピー機のリース期間が満了するにともない、下記のとおり、新コピー機のリースを更新してよいかお伺いいたします。

記

1　希望機種　××CP-150×
2　数　量　1台

図2-7　稟議書サンプル

### 2.3.5　電子申請

e-Japan 構想のもと、官公庁や自治体などへの電子申請が広がっています。

電子申請では、申請書を電子データのままでインターネットを利用して、自宅や職場から 24 時間申請することが可能になります。

ただし、便利な反面、対面確認が行われないため、重要な個人データや資産について、あいまいな認証では、身に覚えのない申請がされる危険性があります。そのため、これらに利用できる電子証明書は本人確認を厳密に行う自治体や電子認証登記所とともに民間では認定認証事

業者が発行するものが使われています。

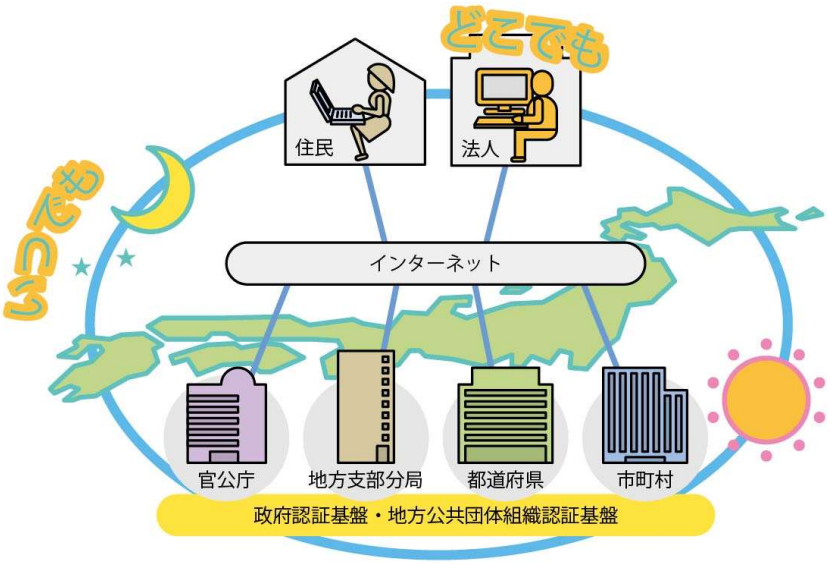



図2-8　電子申請のメリット

事例
◆業種：届出、許可申請などを行う企業及び個人
◆対象業務：官公庁や自治体などへの届出、許可申請など
◆導入メリット：
● 申請窓口の対応時間外でも申請・確認が可能
● 申請窓口に出向くことなく会社事務所から申請が可能
● 申請にエラーチェックが実施され、計算ミスなどの防止が可能
● 手数料や税が軽減される場合もあり、移動や待ち時間がかからず、費用の削減も可能
※ 現在利用できる官公庁関係の電子申請に関しては、以下をご参照ください。
e-Gov 電子申請システム
https://shinsei.e-gov.go.jp/
各地方自治体などについては、それぞれの自治体などのホームページで確認してください。

### 2.3.6　電子入札

e-Japan 構想のもと、官公庁や自治体などへの電子入札が広がっています。

応札者側の事務手続きや移動に伴う費用の削減により、入札の機会が拡大し競争性が確保され、発注金額の低減も可能になります。

なお、官公庁や自治体の公募案件は金額も大きく、入札における本人性および本人の意思確認については厳重かつ公正に行われる必要があります。そのため、これらに利用できる電子証明書は本人確認を厳密に行う認定認証事業者が発行するものが使われています。

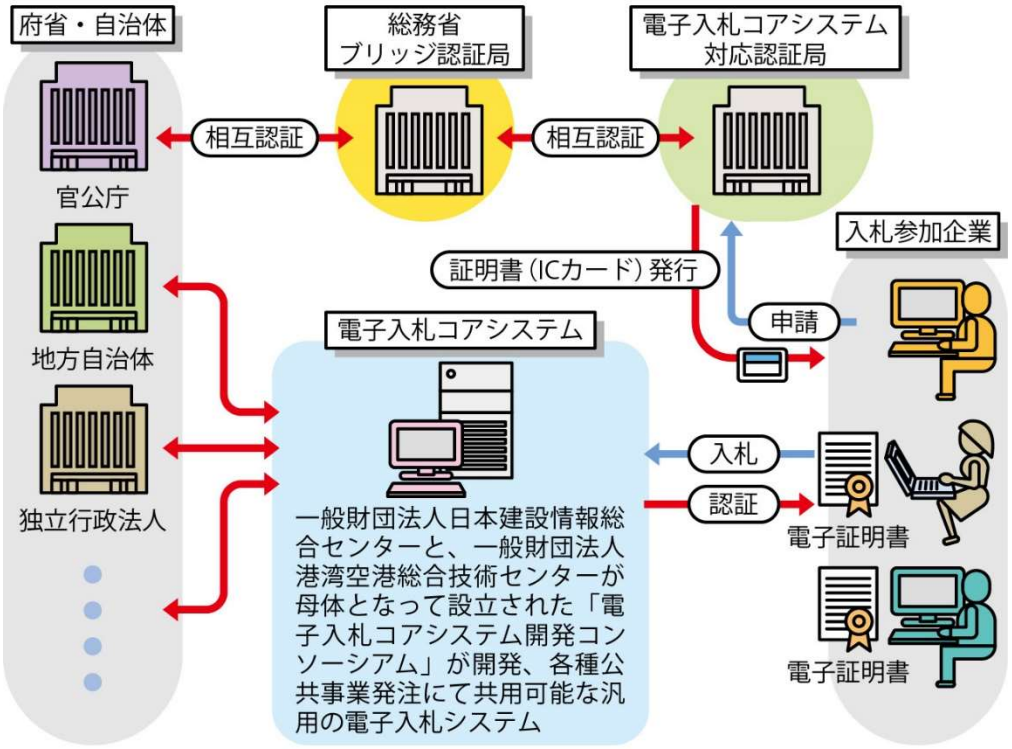



図2-9　電子入札コアシステム概略図

事例
◆業種：電子入札行う企業及び個人事業主
◆対象業務：官公庁や自治体への電子入札
◆導入メリット：
● 本人性の確認を中立公正な第三者機関である認定認証局によって実施
● より多くの案件に応札する機会が拡大することによる競争性の確保、受注機会の拡大
● 応札者が発注者のもとへ出向くための移動回数の大幅削減
● 入札に伴う書類の作成、送付業務が自動化されることによる効率化
※ 現在利用できる電子入札に関しては、以下をご参照ください。
電子入札コアシステム開発コンソーシアム
https://www.cals.jacic.or.jp/coreconso/

### 2.3.7　会社法（取締役会議事録）

取締役会議事録などの承認において、従来は直接承認者本人に事務方が押印をお願いしてきました。それを電子化することより、議事録書類の持ち回りなどの煩雑な事務手続きから開放されます。

事例

◆業種：企業全般（遠隔地に在住の取締役・社外取締役が多い企業には特に有効です）

◆対象業務：取締役会議事録など

◆業務内容：取締役会議事録などの承認者が電子署名を付与して電子保存

◆導入メリット：時間、経費などの大幅な節約が可能になります。

特徴

（1）役員は、それぞれ、事前に電子証明書を取得します。

＊ オンライン登記申請などの添付書類として取締役会議事録などを電子的に作成して提出する場合、使用できる電子証明書は法務省の「登記・供託オンライン申請システム登記ねっと供託ねっと（ https://www.touki-kyoutaku-online.moj.go.jp/）」の Web ページなどでご確認ください。

（2）取締役会議事録などを電子化（PDF）して各役員が電子署名を施します。

（3）電子署名した電子ファイルをメールへの添付として次の役員に回覧します。

（4）データベース化された電子ファイルは、アクセス制御された各役員から閲覧が可能となります。

注）平成 13 年 11 月の商法改正において会社関係書類が電磁的記録をもって作成できることとされ、電磁的記録には「署名に代わる措置」すなわち電子署名が必要とされた。また商業登記法第 19 条の 2 により、登記の申請書に添付すべき定款、議事録もしくは最終の貸借対照表が電磁的記録で作成されているとき、もしくは登記の申請書に添付すべき書面につきその作成に代えて電磁的記録の作成がされているときは、当該電磁的記録に記録された情報の内容を記録した電磁的記録を当該申請書に添付すべきこととされた。

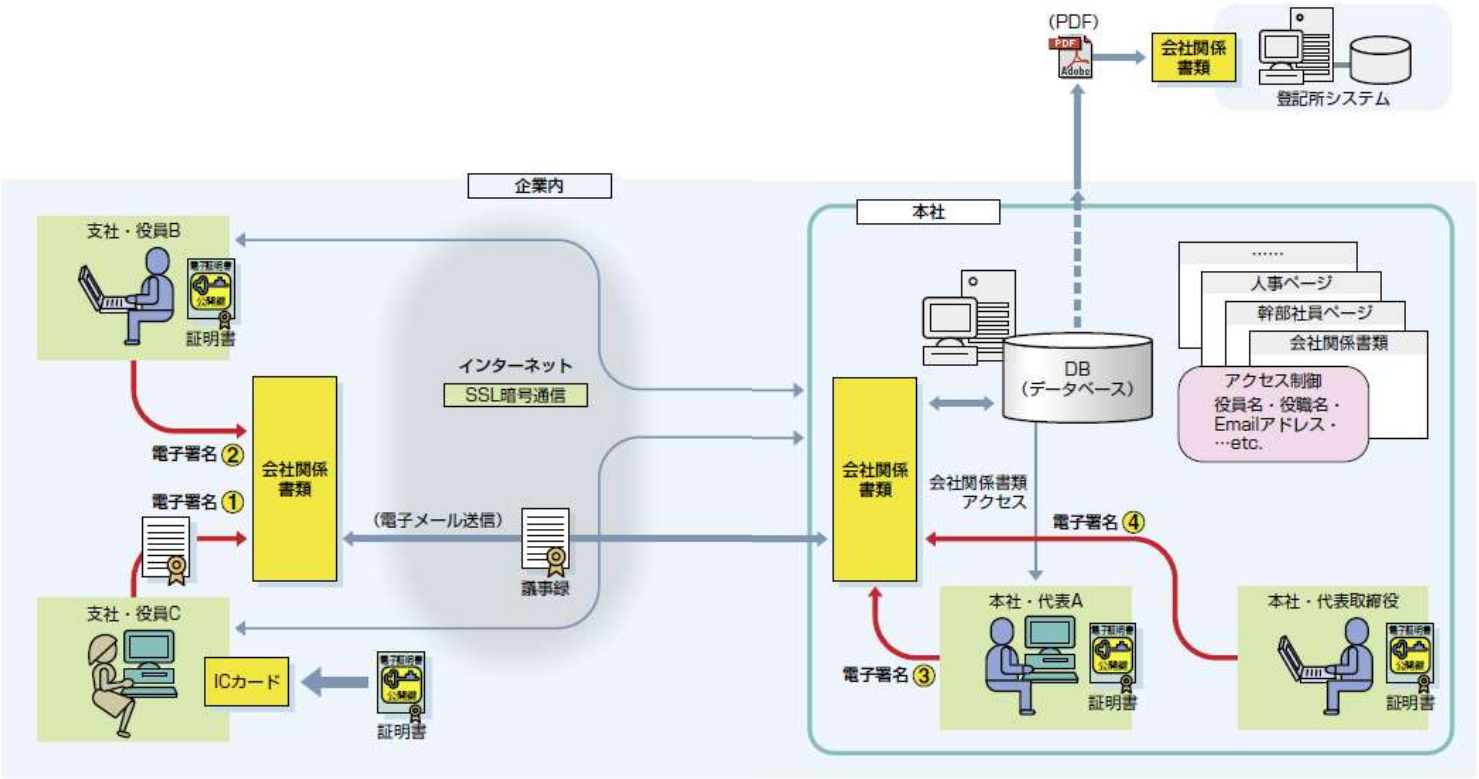



図2-10 取締役会議事録への電子署名

### 2.3.8　公開文書への電子署名

企業などの公開情報において、電子署名を活用することで発信元や公開情報の非改ざん性を証明することができ、企業や組織の信頼性の向上が期待できます。

事例

◆業種:企業全般

◆対象業務: IR 文書などのコンプライアンス性の高い情報やニュース、新着情報などの発信元の信頼性担保が重要な情報の公開

◆導入メリット:

(1) 公開情報の所有者の証明および非改ざん証明

公開情報の発信元および発信された情報が第三者に改ざんされていないことを証明できます。

(2) 二次配布時の真正性

公開情報が二次配布された際に作成責任の所在を明確化できます。

電子認証局会議　会則

（平成22年10月22日）

電子署名者：TATSUTO KODANI
DN：o=Japan Digital Notarization Authority, Inc., ou=Japan Digital Notarization Authority (PROVE CA, ou=Group - JNI, ou=General - 10377-01, cn=TATSUTO KODANI, email=tkodani@jnotary.com
日付：2012.11.09 10:50:40 +09'00'

電子認証局会議　会則

第1章 総 則

（名称）
第1条 本会は、「電子認証局会議」と称する。
2 英語名は、CERTIFICATION AUTHORITY CONFERENCE（略称：CAC）と称する。

（目的）
第2条 電子認証局会議（以下「本会」という。）は、広く関係団体などと連携・協力し、電子署名・電子認証の活用の場を広げ、その有用性について社会的理解を深めるために活動する。さらに、電子署名・電子認証の仕組みの理解を促進するとともに、事業活動や経済活動に利用される安全で便利なセキュリティ基盤となるよう、公開鍵認証基盤の健全な発展に寄与する。

（事業）[注1]
第3条 本会は、前条の目的を達成するため、次の活動を行う。
(1) 電子認証局ならびに関連事業者との情報交流、情報提供に関する活動
(2) 電子認証業務およびその認定に対する政策提言、法制度改正提言に関する活動
(3) 電子署名・電子認証の利活用拡大、オンライン手続の利用促進に関する活動
(4) 電子署名・電子認証の普及啓発促進に関する活動
(5) 電子署名・電子認証の広報宣伝活動に関する活動
(6) 政府関係機関、他関係諸団体との渉外、連絡、意見交流に関する活動

図2-11　公開文書への電子署名サンプル

### 2.3.9　PL 法対応と先使用権保護

知的財産保護に関する特許庁のガイドライン「先使用権制度の円滑な活用に向けて―戦略的なノウハウ管理のために―」が 2006 年6月に公開され、先使用権の立証手段の1つとして電子化された知財情報へ電子署名やタイムスタンプを付与することが例示されました。一方、PL 法や民法上の製造物責任への対応の側面からも知財情報や製品図面の証拠性を担保して長期に保管管理する必要があります。したがって電子署名やタイムスタンプにより電子情報の証拠性

が担保されるため、メーカー各社で実施している製品図面の管理・保存も電子化できる事になり、図面や知財情報の電子管理の利用が加速しています。知財情報の流出事件が頻発する昨今、電子署名法に基づく真正な成立の推定が働く電子署名とタイムスタンプを併用することで、作成責任と作成時期が明確になり、証拠性が高まります。

事例
◆業種：製造業など
◆対象業務：製品図面、研究ノートなどの研究情報の電子保存
◆業務内容：設計工程で確定となった製品図面に承認者が電子署名とタイムスタンプを付与して電子保存
研究者が研究ノート、実験データなどに電子署名とタイムスタンプを付与して電子保存
◆導入メリット：
紙の原図を取り扱わなくて済み、図面管理コストの低減が図れる。先使用権保護対策として、

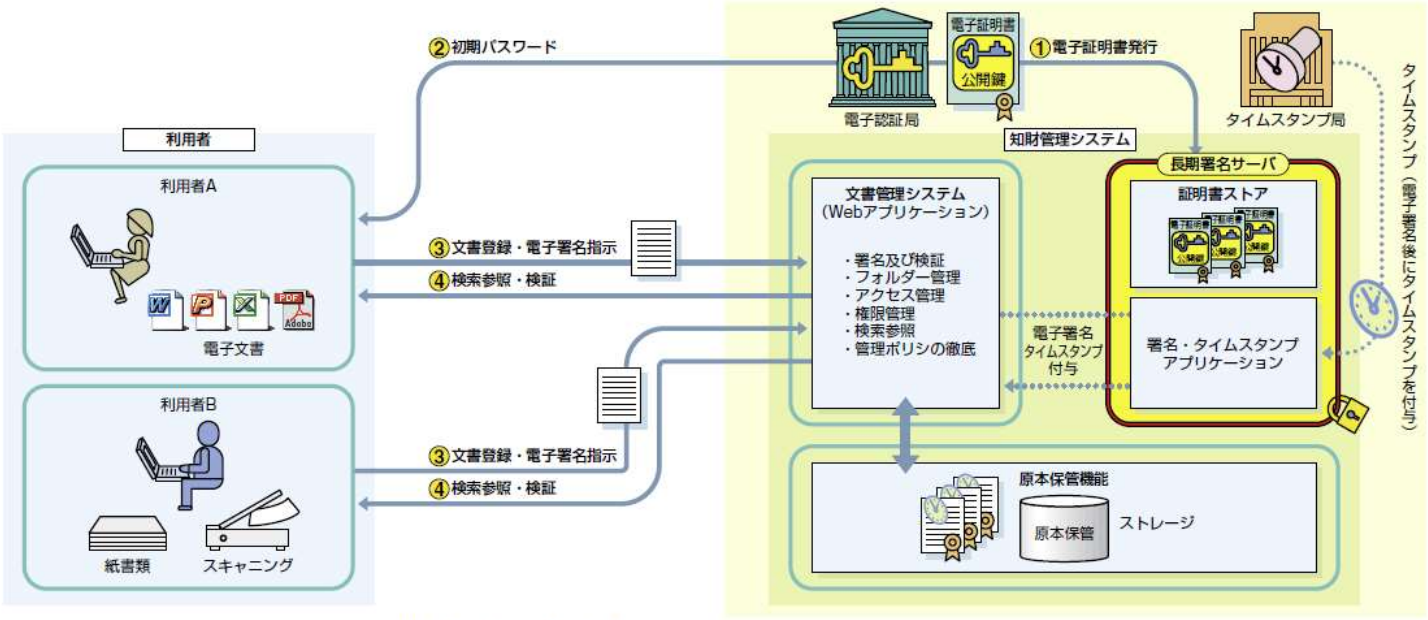



図2-12　PL法対応と先使用権保護

従来、知財情報を収集、公証人役場へ持ち込み確定日付を押してもらう工程を経ていたが、電子的に収集、署名・タイムスタンプで済むため、知財管理にかかる手間を省ける。

### 2.3.10　営業日報、業務記録

各企業で様々な業務フローを電子化、効率アップを追求しているなかで、従来、法的証拠能力の確保が困難なために電子化が遅れていた“業務記録”も、事例が報告されています。記録の作成者や承認者が電子署名を付与することで作成責任の所在が明確になり、記録の改ざんがないことが保証されるとともに、電子署名法により法的証拠能力も確保可能となります。

今後、このように生産管理記録や図面、業務履行状況の記録など、様々な分野で記録を電子的に作成、電子署名を付与した後で保存することにより、さらなるコスト削減を実現することが可能となります。

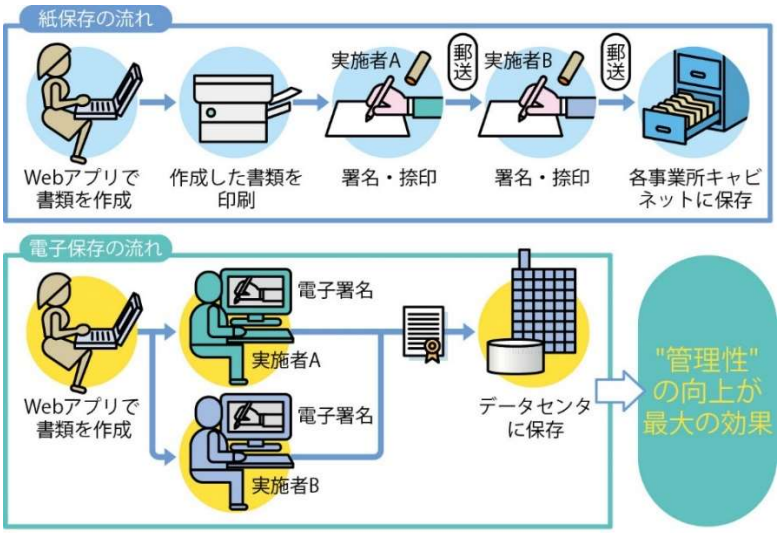



図2-13　電子保存による管理性の向上

業務記録の電子化として、以下のような例があります。

事例

◆業種：警備業

◆対象業務：教育実施記録の電子化

◆業務内容：警備会社では警備員に対する定期的な教育実施が法律により義務付けられ、その実施記録を営業所で保管することが定められている。従来は教育実施者の記名、押印が必要なことから紙で作成、保存していました。

〈紙保存による問題点〉

● プリンタによる打ち出し、署名・捺印、送付、ファイリングなど紙ベースの運用負荷が大きかった。

● 書類整備の実施管理、完了確認に手間がかかっていた。

● 複数の教育実施者などに配布、押印し回収するため、時間がかかり、書類紛失リスクもあった。

● 紙での保存の為、本当に存在するかは現地でないと確認できなかった。

● 書類の差し替え忘れなど、更新不備があっても気づかなかった。

● 手書きによる作成のため、作成された日付に保証がなかった。

〈解決手法〉

教育実施者に対して電子証明書を発行。教育実施記録を電子的に作成、電子署名とタイムスタンプを付与し電子保存する運用とした。なお、教育実施記録の法定保存期間は2年だが、保存期間中に教育実施者の退職などの理由により電子証明書の取り消し処理を行った場合に、署名検証ができなくなることから、長期署名形式を採用し、署名後に署名者の電子証明書が取消処理されたとしても、電子署名の検証が継続して可能な状態を維持する運用を実施しています（詳細は「3-2-5 長期署名の必要性」も併せて参照）。

◆導入メリット：

● コスト削減

書類の作成、整備状況の管理にかかる管理人件費の削減

● 業務の効率化

電子化された書類作成、複数の電子署名ワークフローにより効率化が実現。

書類の作成に複数の営業所を経由していたため、整備までに時間が掛かっていたが、書類整備までの時間が劇的に短縮した。

タイムスタンプが付与され作成日時が明確となったことから、早期の作成を促されるようになった。

従来の書類保管スペースを、別の目的に有効利用できた。

● 書類の管理性の向上

全国の営業所での保管義務のある書類の整備状況がワンクリックで確認可能となり、管理性が向上できた。

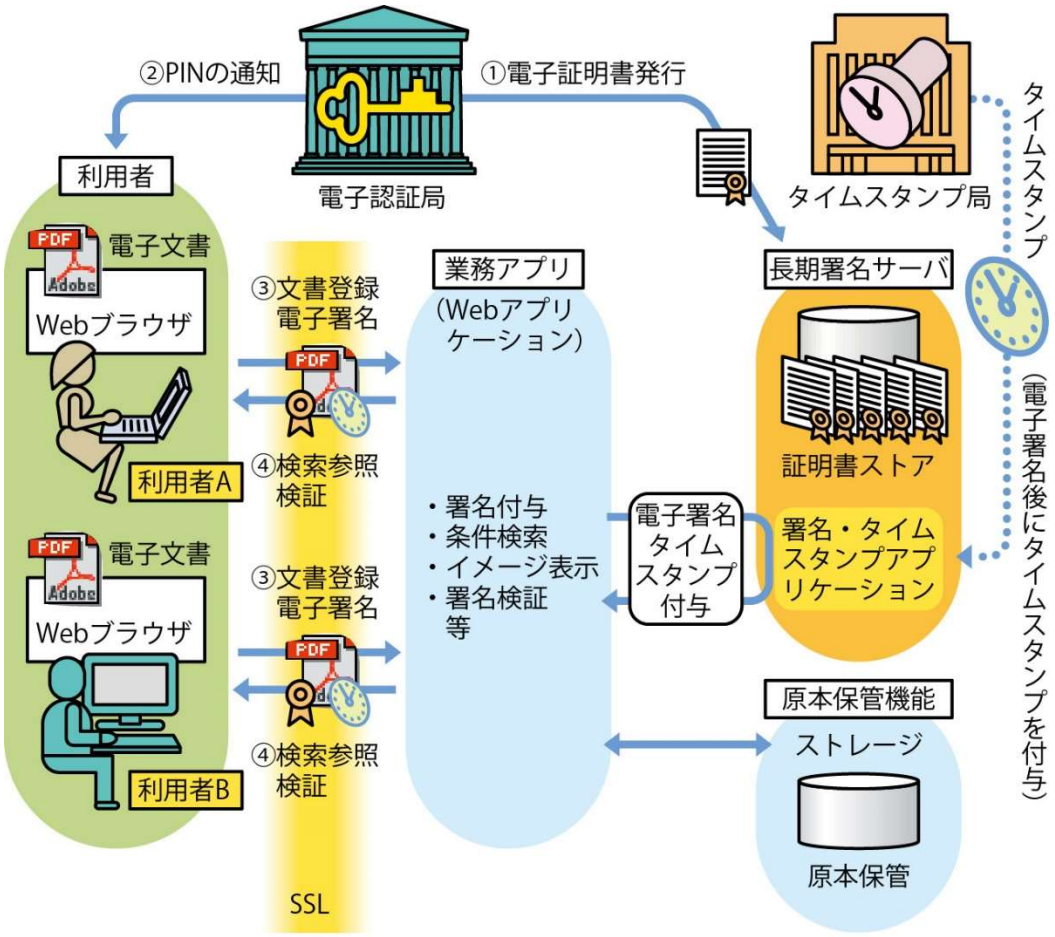



図2-14　電子署名／タイムスタンプを利用した電子化例

### 2.3.11　社内機密情報の暗号化

**■通信経路の暗号化**

社内では、個人情報をはじめ機密情報を取り扱う業務が増えており、これまで以上に情報漏えい防止の重要性が高まっています。暗号化通信により、インターネットを介したシステムとの通信において盗聴による通信内容の情報漏えいを未然に防止できます。

事例

◆業種：企業全般

◆対象業務：機密情報などを取り扱う業務

◆業務内容：インターネットを利用したシステムにおいて、機密情報の送受信が必要となる業務

◆導入メリット：

通信経路の暗号化によりデータを暗号化するため、機密情報なども安全にやり取りができます。万一、第三者に盗聴されても、中身の解読が困難であるため情報漏えい防止が可能です。

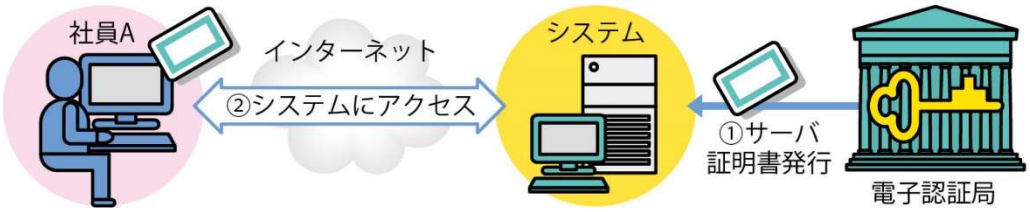



図2-15　社内機密情報の暗号化

**■ファイルの暗号化**

パソコンの不正使用や盗難・紛失、コンピュータウイルスによる情報漏えいがマスコミをにぎわす昨今、社内機密情報や人目に触れては困るファイルをお持ちの方も多いことでしょう。

そこで、ひとつの防衛手段としてファイルの暗号化があります。暗号化手法にも色々ありますが、例えば、パソコンでは、見られては困る大事なファイルを電子証明書の鍵によって意味不明な内容(暗号文)に変換しておき、電子証明書の鍵が分からないと暗号文は元に戻せない手法を利用すれば、安全性が高まり、万が一の企業内での不正使用や盗難・紛失に備えることができます。

事例
◆業種：企業全般
◆対象業務：機密情報を取り扱う業務全般
◆業務内容：社内で機密文書の取り扱いが必要となる業務
◆導入メリット：
ファイルを暗号化することで、機密情報などを安全に取り扱うことができ情報漏えい防止になります。

図2-16　電子証明書を利用したファイルの暗号化

### 2.3.12　業務システムへの本人認証

社内業務システムなどにおいて、社員または特定の要員にのみアクセスを許可したい場合、従来のユーザーID ／パスワードに加え、クライアント証明書(個人用証明書)による本人確認などを組み合わせることによって、よりセキュリティレベルの高いアクセス制御ができ、不正アクセスを防止することができます。

事例
◆業種：企業全般
◆対象業務：業務システム全般
◆業務内容：業務システムへのアクセスを制限したい業務
◆導入メリット：不正アクセス防止

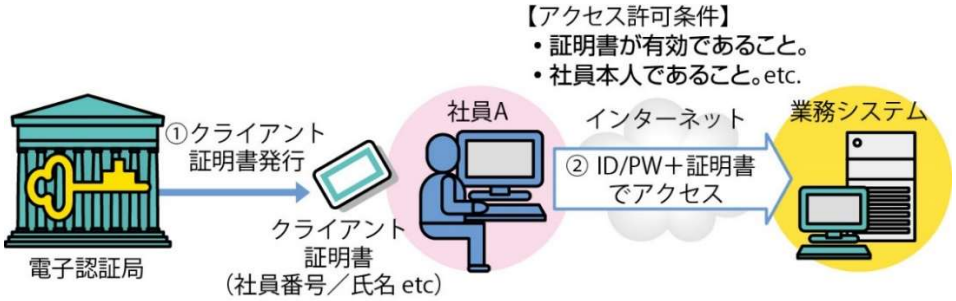



図 2-17　電子証明書を利用した本人認証

### 2.3.13　国税関係帳簿・証憑類の電子保存

国税関連書類では、2008 年頃から大手金融機関を中心に、コスト削減戦略の中で電子証明書を活用し、顧客サービスやセキュリティの向上を図りながら、コスト削減も実現する事例が出てきています。

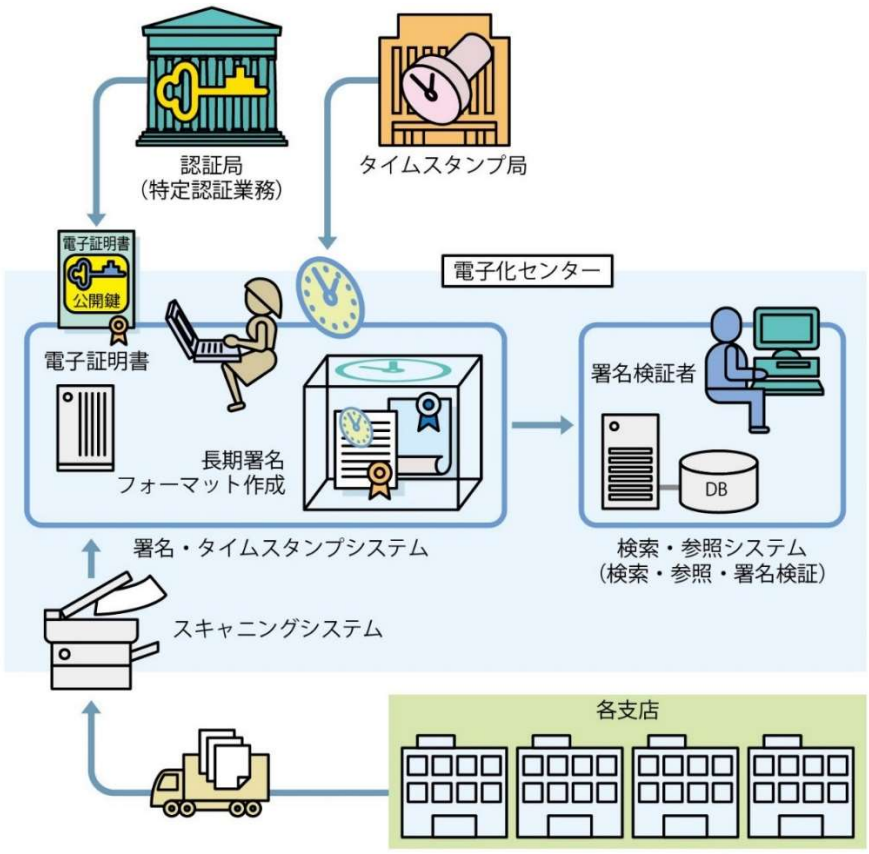



図 2-18　国税関連書類の電子化例

さまざまな業種で導入が進んでいますが、具体的な事例としては次のとおりです。

事例

◆業種：都市銀行

◆対象業務：口座振替依頼書の電子保存

◆業務内容：全国から送られてくる口座振替依頼書をセンターにて一括してスキャニング、電子署名とタイムスタンプを付与して電子保存

※2015 年度の電子帳簿保存法改正に伴い、「入力者または監督者に関する情報の確認」は電子署名以外の方法でも認められるようになりましたが、証拠性を確保するうえで、電子署名が最も適切であると考えられています。

◆導入メリット：

（1）顧客対応力の強化と人件費削減を両立

問い合わせ時、照会時の検索性が飛躍的向上しました。従来は、該当するマイクロフィルムを探し、コマ検索して参照。原本が必要となる場合は倉庫保管の紙ファイルを取り寄せていました。電子化後は、スキャニング画像そのものが証拠性を持ち、事務端末で即時に検索可能となりました。

（2）ローコストで個人情報保護を強化

全国の支店で分散管理し定期的に保管個数チェックをしていたフィルムと書類を、セキュリティ管理が行き届いているデータセンターでの一括管理に切り替えることが可能となりました。少ない工数で以前より強固な個人情報管理が可能となり、漏洩リスクの減少がはかられました。

### 2.3.14　医療関連文書の電子保存

厚生労働省（以下、「厚労省」という。）では 2005 年3月に「医療情報システムの安全管理に関するガイドライン」を公開し、医療分野での電子保存の要件が示され、2010 年2月には第 4.1 版に更新され、一定の要件を満たす場合は医療情報を医療機関以外で外部保存することも認められました。

電子カルテなどの導入が進んでいる医療機関でも、紙記録との二重管理を余儀なくされていました。近年、e-文書法への対応製品のリリースが進む中、厚生労働省のガイドラインも技術的に満たすことが容易となり、紙記録の電子化が進んでいます。

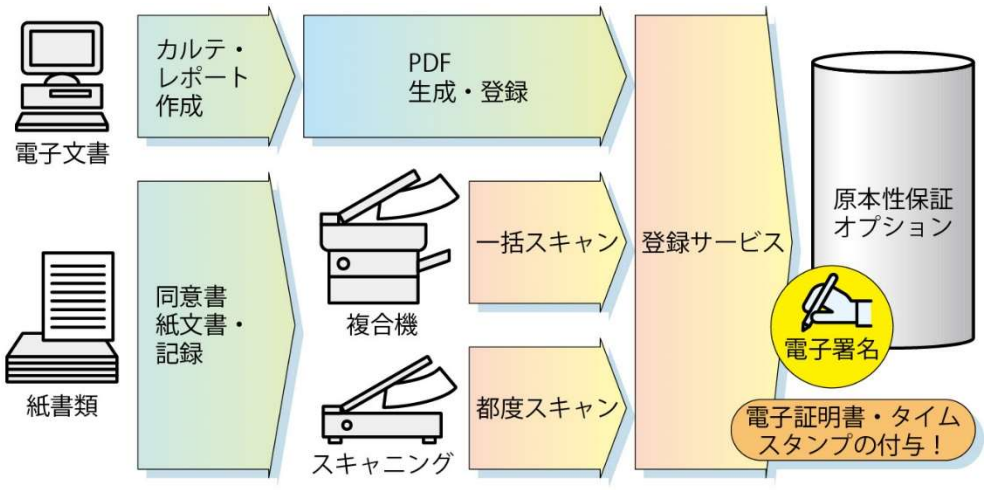



図 2-19　医療関連文書の電子化

事例
◆業種：地域中核病院
◆対象業務：診療記録の電子保存
◆業務内容：診療過程で発生する紙ベースの諸記録をスキャニングし電子署名とタイムスタンプを付与して電子保存。診療過程で発生する電子作成された諸記録に電子署名とタイムスタンプを付与して電子保存。
◆導入メリット：
一般的に電子カルテの導入が進み診療業務の中で IT 化は進行しつつあります
が、どうしても紙ベースの記録が残り、電子と紙の二重管理を余儀なくされていました。一部の先進的な病院では、厚労省のガイドラインが提示される以前から、紙の記録と電子作成された記録を統合管理することにより管理コストの軽減を実現していましたが、一部の記録に関しては紙管理の状態にありました。厚労省のガイドラインに準拠することで紙の廃棄を実現し、管理コストのさらなる軽減をはかることができました。くわえて診療記録の電子保存に関するコンプライアンスも確立することができ、さまざまな病院で導入が進んでいます。

### 2.3.15 士業の電子申請

士業関係で使用される電子証明書は、行政情報化時代における各種電子申請において、申請を行う国民の負担軽減、利便性の向上に資するものとなっています。

■全国社会保険労務士会連合会
e-Gov 電子申請システム(厚生労働省関連)
労働社会保険関係手続
全国健康保険協会電子申請システム
健康保険関係手続の一部
■日本司法書士会連合会
登記・供託オンライン申請システム
不動産登記関係手続
商業・法人登記関係手続
動産譲渡登記関係手続
債権譲渡登記関係手続
供託関係手続
電子公証関係手続
■日本税理士会連合会
国税電子申告・納税システム
地方税ポータルシステム
■日本土地家屋調査士会連合会
登記・供託オンライン申請システム
不動産表示登記関係手続
■日本行政書士会連合会
自動車保有関係手続のワンストップサービスシステム
登記・供託オンライン申請システム
電子公証手続
■弁理士
特許庁への電子出願

## 2.4　電子署名に用いる電子証明書とは

### ■電子署名利用の背景

従来からビジネスの場では、紙に記載された文書などは内容の改ざんが容易に確認できることや、商習慣などにより押印を確認できれば、本人が作成したものと推定することができるため、契約書など、多くの文書において書面に記名、押印した文書を取り交わし、保存する運用が広く行われてきました。このことは、民事訴訟法（以下、「民訴法」という。）第228条4項において、「紙に記載され、押印もしくは、署名された文書（契約書、議事録など）は、真正に成立すると推定される」と規定され、法的に裏付けられています。

一方、電子メール、送付されたワープロで作成された契約書などの文書、表計算ソフトで作成された各種の電子的な情報は、内容の変更が容易で、改ざんや差し替えなどを検知することができず、信頼性が認められないため、従来、書面で行っていた業務において、にわかに使用することができませんでした。しかしながら、こうした電子情報は、近年、社会・経済活動において不可欠のものとなっているばかりか、電子情報の流通は、社会・経済活動の効率化、迅速化などのために急速に増大しています。

もし、こうした電子情報に対して、紙に記名・押印したものと同等の効力があればどうでしょう？ビジネスのスピードは飛躍的にアップし、紙を扱う手間から開放されコストも大幅に削減できます。そのためには、電子情報に「署名・押印」に相当するものを電子的に付与し、紙に記名・押印された文書と同等の法的効力を与えることが必要になります。

### ■電子署名と電子署名法

「電子署名法」（電子署名及び認証業務に関する法律：法律第百二号）が平成 12 年5月 31 日に制定、これにより電子署名が定義されて、電子署名に法的な有効性を与えました。電子署名法は、

（1） 電磁的記録の真正な成立の推定（第3条）

（2） 特定認証業務に関する認定制度（第4条から第 16 条）

の2本柱からなっており、情報の電磁的方式による流通及び情報処理の促進を図ることを目的としています。

この法律で「電子署名」は、電磁的記録（当該情報）に対して以下の要件を満たして行われる“措置“と定義されています。（第2条1項）

（1） 当該情報が、当該措置を行った者の作成に係るものであることを示すためのものであること（本人性）

（2） 当該情報について改変が行われていないかどうかを確認することができるものであること（非改ざん性）

とされています。

また、電磁的記録について、本人による電子署名が行われているときは、真正に成立したものと推定するとしています。（第3条）

これは“紙に、押印もしくは、署名された文書が、真正に成立すると推定される”とした「民訴法」第 228 条4項に対応する内容となっており、電子文書に本人の電子署名があれば、紙に記名・押印したものと同等の法的証拠性が与えられることになりました。

なお、電子署名は、目で確認することができないため、電子署名を行うソフトウェアには、電子署名が本物であることを確認する“署名検証”機能が用意されているのが通例です。

■認定認証業務

電子署名法では「特定認証業務」の中でもさらに厳格な基準をクリアした場合に与えられる認定制度が定められています。

(1) 認証業務に使用する設備が主務省令で定める基準に適合するもの
(2) 認証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って行われるもの
(3) 認証業務が主務省令で定める基準に適合する方法によって行われるもの

上記3点の適合が認められる認証業務については、主務大臣(内閣総理大臣及び法務大臣)による「特定認証業務」の認定を受けることができます。通常、認定を受けた「特定認証業務」を「認定認証業務」と呼びます。

「特定認証業務」の認定を受けるためには、前記の要件を満たしているかについて、国(及び指定調査機関)の実地調査を受ける必要があります。認定の有効期間は政令で定められています。認定を継続して受けるためには、認定の有効期間が終わるまでに、国(及び実地調査を実施する指定調査機関)による実地調査を受ける必要があります。電子署名法では「認定認証業務」を行う事業者を「認定認証事業者」といい、一般的には「認定認証局」と呼称しています。

認定を受けることにより「認定認証局」は、厳格な基準を満たして運用していることが国によって確認されていると言えます。

図2-20　電子署名法における認証業務の定義

■電子証明書の選定

電子証明書を購入する場合の選定ポイントを列挙します。

(1) 用途を確認
(2) 法令やガイドラインの確認
(3) 電子証明書の選定
(4) 専用ソフトウェアの要否およびパソコン要件を確認
(5) 発行対象を確認

**(1) 用途を確認**

電子証明書の用途は、「署名・暗号・認証」の3種類があります。メールの暗号化であれば、「メールの暗号化が可能な電子証明書」を用意する必要があります。

**(2) 法令やガイドラインの確認**

電子証明書を利用する業務に関係する法令やガイドラインにおいて、電子証明書に対してどのような要件があるか確認を行います。

### (3) 電子証明書の選定

電子証明書は、「認証局」から発行されます。この認証局の役割は、「**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**」ことです。そのため、認証局は、電子証明書の発行や失効の基準・ルールを明確に定め、証明書ポリシー（以下、CP）運用規程（以下、CPS）に記載しています。

認証局の種類は、国の認定を受けた民間企業が運営する「認定認証局」や、一般的なブラウザーに予め組み込まれている自身の電子証明書を発行している「信頼されたルート認証局」、インターネットなどに公開せずグループや企業内でのやり取りに限定した「プライベート認証局」などがあります。

表2-1　主な認証局の種類

| 種　類 | 特　徴 |
|---|---|
| 認定認証局 | 電子署名法施行規則で定める一定基準を満たし、国の認定を受けた認証局 |
| 信頼された<br>ルート認証局 | OSやWebブラウザーベンダーが示す基準を満たした認証局<br>電子証明書は予めOSやWebブラウザーに格納される |
| プライベート認証局 | 企業や個人が自由に設計、運用を行うことができる認証局 |

次に、電子証明書を購入する認証局を選定します。

「価格」や「有効期間」、「付加サービス」などで違いがあります。電子証明書は、現実の世界の「実印と印鑑登録証明書」に相当する効力を持ちます。電子証明書を購入する際は、認証局が信頼できるかどうかが重要になりますので、以下をポイントにご確認ください。

1） 目的の用途の電子証明書を提供しているか確認

認証局により、発行や失効の基準・ルールや取り扱う電子証明書の種類が異なりますので、用途に応じた電子証明書を提供しているか確認します。

2） 認証局の「運用体制」が信頼できるか確認

認証局がどのような運用体制で電子証明書を発行しているかを確認します。

3） 認証局の業務手続きが信頼できるか確認

認証局が電子証明書を発行する際にどのような手続きで「本人確認」「意思確認」を行っているか。

上記3点は通常、CP/CPS で確認できます。

我々電子認証局会議を構成する各認証局は、認定認証業務として国の認定を受けており、信頼性は最も高いものといえます。

### (4) 専用ソフトウェアの要否およびパソコン要件を確認

電子証明書の利用にあたり、専用ソフトウェアが必要な場合があります。

電子証明書の購入先で、パソコン要件（OS、メモリ、ブラウザーなど）が案内されていますので、購入前に必ず確認します。

専用ソフトウェアは、通常「電子署名」する機能と「電子署名を検証」する機能を備えています。

電子証明書をブラウザー（ Microsoft Edge など）やメーラー（Outlook など）に組み込むなど、専用ソフトウェアが不要な場合もありますが、その場合でもパソコン要件が決まっていることが一般的です。

**(5) 発行対象を確認**

認定認証局は、発行対象(通常は「自然人」)を認証して電子証明書を発行しており、電子証明書には、発行対象の名前が記載されます。

官公庁・地方自治体の電子入札用電子証明書のように、発行対象を「企業の代表者」「入札・見積・契約権限を委任されている支店長」などに制限している場合がありますので、確認の必要があります。

## 2.5 電子署名の運用のポイント

本節では、実際に電子署名を使う場合の留意点として、実世界の「印章」に相当する「秘密鍵」および、実世界の印鑑登録証明書に相当する秘密鍵の所有者を証明する「電子証明書」の管理、運用について解説します。

実際の会社における印章と秘密鍵の特性を対比した表を以下に示します。

印および電子の世界も、管理・運用は基本的には同様と考えられます。

表 2-2 印章と秘密鍵の特性比較

| 項目 | 印章 | 秘密鍵 |
|---|---|---|
| 所有者証明 | 印鑑登録証明書 | 電子証明書 |
| 利用者 | 管理部門 | 本人(代理人) |
| 保管者 | 管理部門 | 本人(代理人) |
| 保管場所 | ロッカー、金庫など | サーバーや PC(パスワード管理)もしくは IC カードなど |
| 複製 | 不可 | 技術的には<br>・電子ファイル形式では可<br>・IC タイプでは不可<br>運用上の制限が必要 |
| 対象文書 | 紙 | 電子ファイル(PDF、XML、イメージファイルなど) |
| 履歴管理 | 押印請求書で承認回覧 | ワークフローや電子署名付きメールなどでの申請も可能 |

秘密鍵の運用にあたっては、特性を理解しながら、印章と同様な運用・管理規則(手順)の策定が必要です。

したがって、秘密鍵や電子署名の管理・運用に係わるルールとして、上表のような項目を「利用規程」などに定め、秘密鍵所有者に開示、同意を得ることが望まれます。

＜コラム＞

**電子証明書の保管、使用方法**

**■代表者の「電子証明書」(IC カード)を、担当部署で管理してもよいでしょうか？**

電子証明書を、印章同様に管理組織として預かり、管理したい、というご希望があるようです。

現在の社会実態として、会社の社長印は社長室長などで、銀行印は経理部で保管し、規則や指示によって使用している例が多くみられます。弁護士事務所でも印章は2つあることが多く、弁護士が持ち歩くものと事務局長が管理しているものとがあるようです。

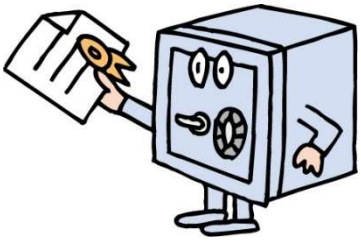
印鑑を使う必要性に応じて印章の保管利用について実用的な対応がなされています。

さて、電子証明書の場合はどうでしょうか。

電子証明書は、必ず本人が持ち、本人以外が使ってはならない、といわれてきたこともあり、そうした厳格な運用が実用的な利用を制限しているようです。代表者が自分の手で使用しなければならない、とすれば事務手続きまで代表者に強要するようなものです。それではあまりに実情に反し、使い難くなり、リアルな印章のほうがよほど便利で合理的、ということになります。

電子署名法3条では、電子署名は「当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）」とされています。この場合の「本人だけが行うことができることとなるもの」とは、本人の意思に従っているという意味であって、他人が勝手に利用できる仕組みであってはならない、という意味です。そのため、前段に書かれているように「適正な管理」が必要になるわけです。「適正な管理」というのは、自分の手で持っているとか、自分の手で電子証明書（IC カード）を使用しなければならないといったことをいうのではなく、管理形態を意味するわけです。

管理がきちんとしていれば、個人的事情には法は介入しないのです。



印鑑登録証明書を発行する場合も家族や付添い人に発行を依頼することがあります。本人の指示で印鑑登録証（カード）を持って発行を依頼するときは「使者」として行動することになります。その法律効果はすべて本人に帰属するとされています。また、実印の保管にあたって自宅に置くよりも銀行に預けるほうが安全であれば貸し金庫を利用します。この場合も自らの支配、管理下にある状態ということになります。こうした「使者」の利用、組織的な管理も法的には認められるものなのです。電子証明書の保管や使用においても同様です。

たとえば、行政組織では長の電子証明書（カード）は、表 2-3 のような管理規則に従って管理課が管理するとされています。また、表 2-4 に示すような利用規程を定め適切に管理することが重要になります。

表2-3　電子証明書の管理規則例

| 電子署名に用いる職名など | 当該電子署名に係るカード管理者 |
|---|---|
| 市　長 | 行財政局行政部庶務課長 |
| 市　長(各事務専用) | 各事務主管課長 |
| 収入役 | 会計室会計課長 |
| 危機管理監 | 危機管理室長 |
| 観光監 | 国際文化観光局文化観光部文化交流課長 |
| 神戸市事務分掌条例(平成15年10月条例第19号)第1条に規定する局又は室の長 | 当該局又は室の庶務担当課長 |
| 会計室長 | 会計室会計課長 |
| 区　長 | 当該区役所まちづくり推進部総務課長 |

このように厳格な規程で、管理体制ができていて、利用する場合のルールが決まっていれば、本人が利用した、本人の正当な意思表示であると取り扱うことになります。

会社や組織で電子証明書を管理する場合には、誰が見ても「適正な管理」と評価できるようなルール作り、組織作りと管理を行うことが求められます。

具体的には組織内に利用者のための「電子署名利用規則」、そして管理者のための「電子署名管理規則」、「電子証明書使用に関する規則」といったものを作成し、確実に実施することが考えられます。こうした体制があれば、今までの印章のときと同様に電子証明書を担当部署に預けて活用することができるのです。

表2-4　電子証明書の利用規程例

| | | |
|---|---|---|
| 1 | 利用用途 | どのような業務の、どんな書類に電子署名するのか？ |
| 2 | 発行対象(署名者) | 発行対象者(署名者)は誰にするのか？ |
| 3 | 各種ルール | 発行・更新・取消などの申請手続きは、何に基づき、誰が、どのように実施するのか？ |
| 4 | 秘匿管理 | 秘密鍵の格納方法、パスワード設定など、秘密鍵が不正に漏えいしない対策を定め、利用者の秘密鍵に対する適切な管理を行うよう指導する。<br>・秘密鍵の管理主体（電子証明書所有者、代理人を指定する場合は、代理人を定義）の明確な規定<br>・秘密鍵の正当なバックアップ目的以外の複製禁止<br>・秘密鍵を紛失した場合の失効申請方法 |
| 5 | 代理人と署名申請 | 代理人への署名委任、電子署名申請や電子証明書管理などを定めた運用ルールが必要(詳しくは、「2-4 電子署名に用いる電子証明書とは」を参照) |
| 6 | 記録の保管 | 電子証明書発行・更新・失効申請の記録や署名申請など、記録の保管ルールを定める |
| 7 | 電子証明書所有者の同意 | 上記「1」で定めた電子証明書利用用途や、CP/CPS、本利用規程などへの電子証明書所有者の同意 |

＜コラム＞

**電子認証局の本人確認方法について**

「現実の世界」、「デジタルの世界」の二つの世界を比較しながら説明してみます。

現実の世界では、大事な書類や契約書へ記名・捺印する場合に使用する「印章」は、「実印」を使うと思います。それではいったい誰があなたの使っている「実印」を本物であるということを証明してくれているのでしょうか。そうです役所です。役所に「実印」として印鑑登録を行い、それを公的に証明してくれるものが「印鑑登録証明書」であることは、みなさんよくご存知のとおりです。

なぜ大事な書類や契約書に「実印」を使うのかというと、印影を印鑑登録して、この印影は「自分のものですよ」と役所に証明してもらい、あとで争いごとが起きた場合に備えることができるというのが大きな理由ではないでしょうか。

デジタルの世界では印章（ハンコそのもの）は存在しませんので、印章に相当するものを作らなければいけません。但し、その“電子の印章に相当するもの”は役所に持っていっても印鑑登録してくれません。従って、その“電子の印章に相当するもの”が間違いなく本人のものであることを証明してくれる信頼の置ける第三者が必要になります。この第三者機関が「電子認証局」になります。

「電子認証局」の役割として、電子証明書の申請者へ、

①「秘密鍵と公開鍵からなる1対の電子的な鍵ペア」

②「電子証明書」

を発行します。

「電子的な鍵ペア」の実体は0と1の記号のかたまりであり、デジタルの世界ではこの「秘密鍵」が印章に相当します。一方、「公開鍵」の方は所有者の「電子証明書」の中に入れられて、発行認証局の電子署名が付与されます。この電子証明書は役所が発行する「印鑑登録証明書」に相当します。

即ち、認証局がその公開鍵が本人のもので有ることを保証するわけです。

認証局は、住民票や在籍証明書等により申請者の実在性を証明し、対となる秘密鍵が間違いなく本人が所有するものであることを確認することにより、電子証明書所有者の本人性を証明します。

いわば「現実の世界」の「役所」の役割を果たしているわけです。ここで秘密鍵と公開鍵という聞きなれない言葉がでてきました。これは、日本政府が電子政府構想において文書の流通や申請・届出の電子化を推進していますが、その中でも採用している暗号化技術であり、PKI（PKI：Public KeyInfrastructure 公開鍵暗号基盤）と呼ばれています。

この電子的な鍵ペアは、電子情報の暗号化と復号を行うための一対の情報（施行規則等では符号と定義されています。）で、この一対の片方を秘密鍵（Private Key）、もう片方を公開鍵（Public Key）と呼んでいます。

デジタルの世界では、「記名・捺印（自筆で署名＋実印で押印）」をすることができないので、本人の秘密鍵（印章に相当する）を用いて電子契約書などに対し「電子署名」を行います。また、電子署名を確認する（署名検証といいます）ためには本人の公開鍵を必要とします。「電子署名」を行った人が確かに「本人」であることを確認できるようにするため、本人の公開鍵が格納された電子証明書を添付し相手へ渡すわけです。

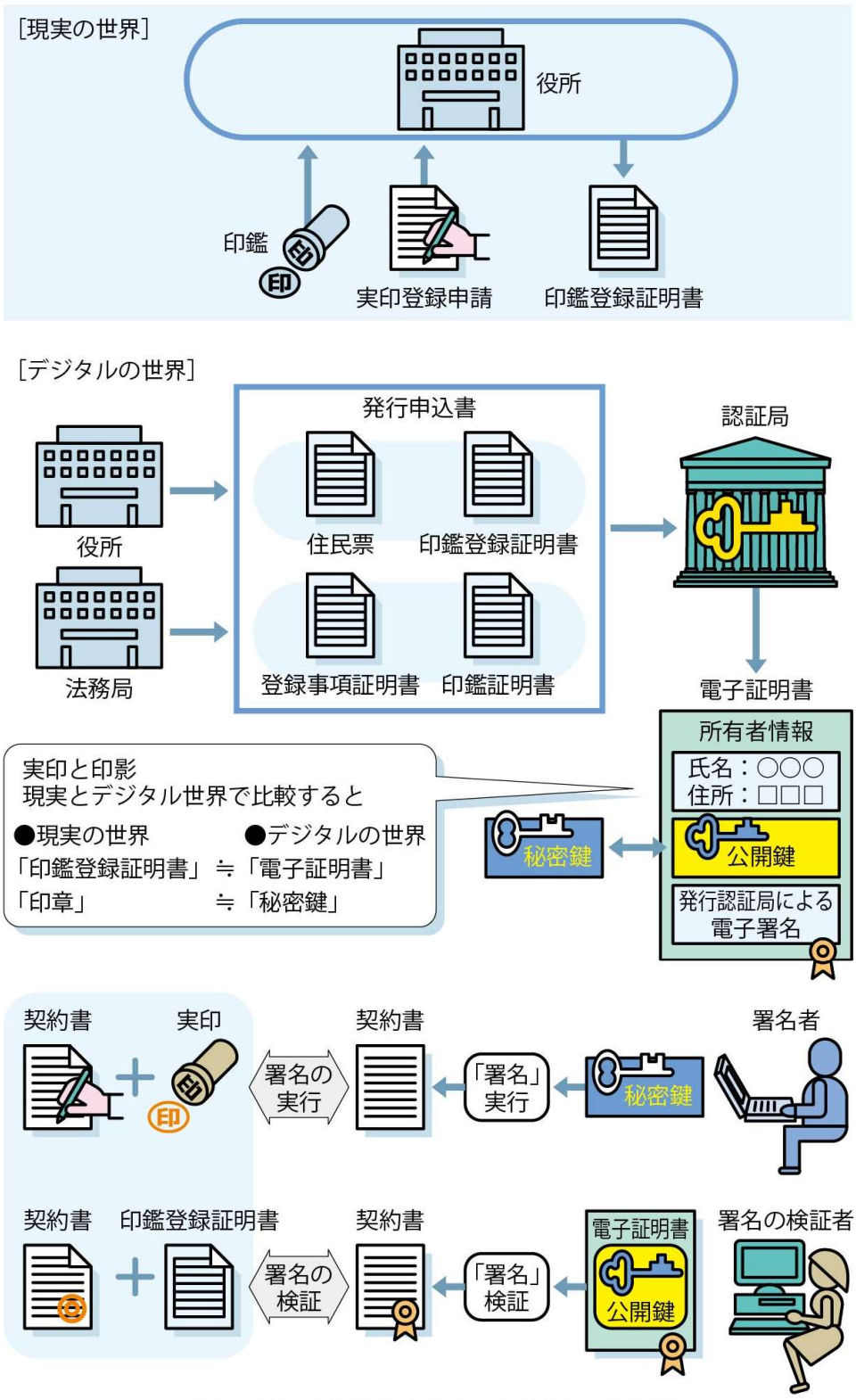



図2-21　現実とデジタル世界の本人確認方法比較

# 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( https://www.c-a-c.jp/assets/document/us/02CAC_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。

図 3-1　電子署名の有無確認

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「電子署名の検証方法」（ https://www.c-a-c.jp/case/verification.html ）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。

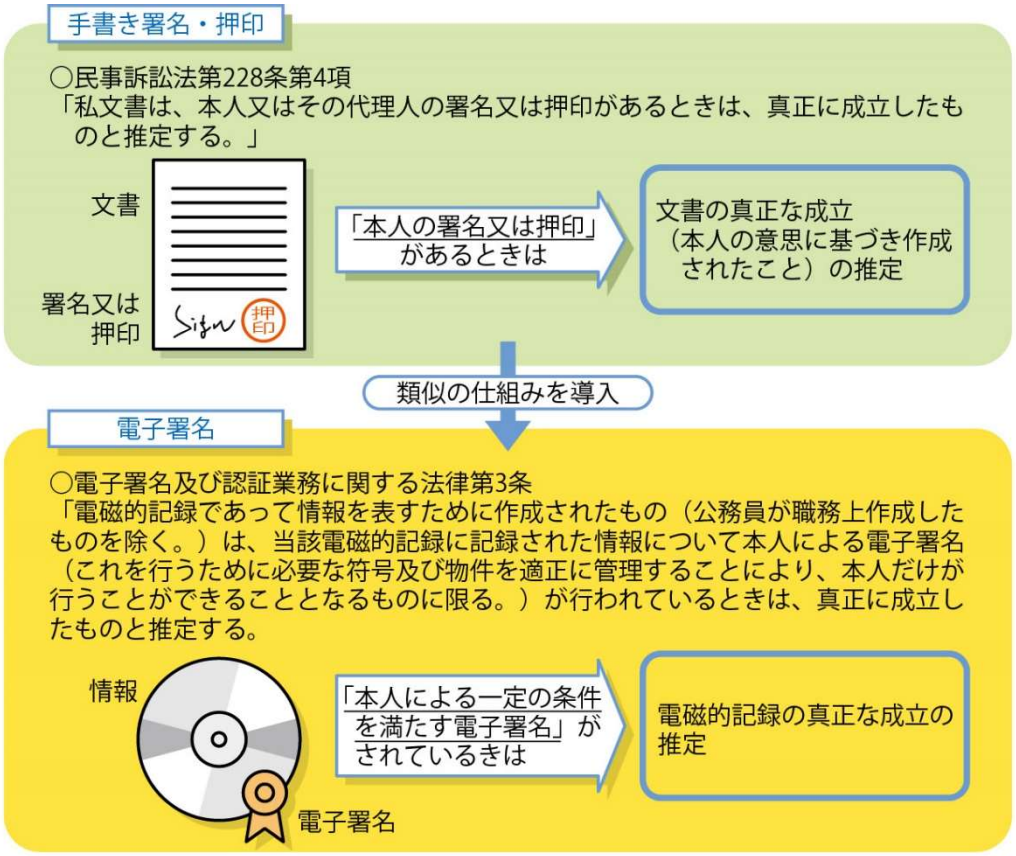



図 3-2　民事訴訟法第 228 条第 4 項と電子署名法第 3 条

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、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を検証します。正しく検証できれば、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。

1 「電子署名及び認証業務に関する法律」2001 年 4 月施行

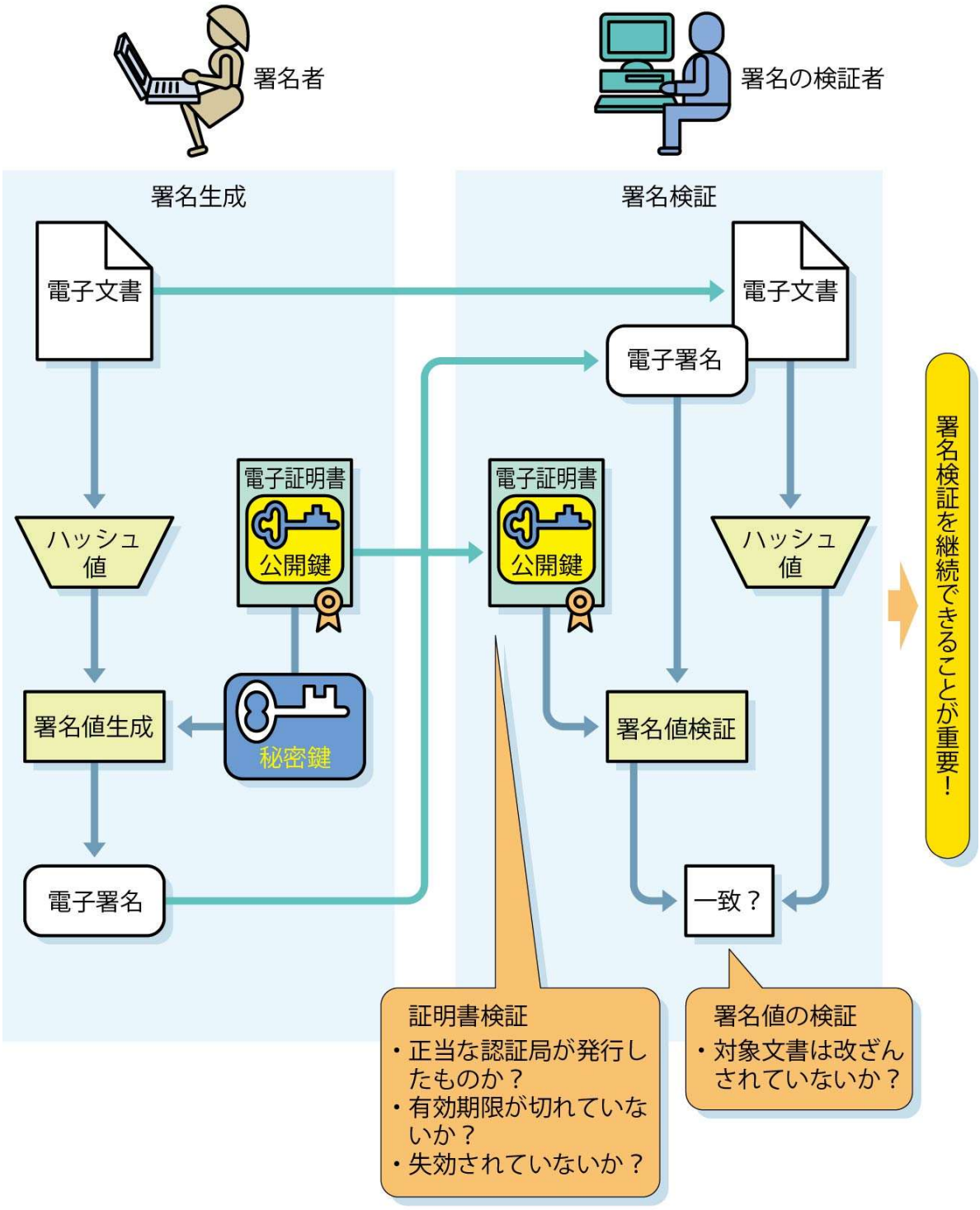



図3-3　電子署名および検証の具体的方法

**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**

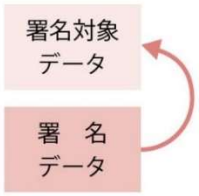
| | 要件概要 | 要件詳細 | |
|---|---|---|---|
| 1.電子署名の要件 | 有効な電子証明書を用いて電子署名すること | A | 正当な（信頼できる）認証局から発行されたもの |
| | | B | 有効期限が切れていない |
| | | C | 失効していない |
| 2.署名検証の要件 | 署名対象文書の有効性を維持したい期間、電子署名が正しく検証できるようにする。 | D | 正当な認証局から発行された本人の電子証明書であったか？ |
| | | E | 署名当時に電子証明書の有効期限が切れていなかったか？ |
| | | F | 署名当時に電子証明書は失効し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

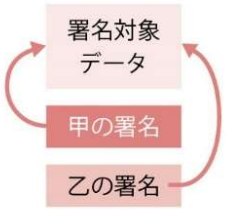
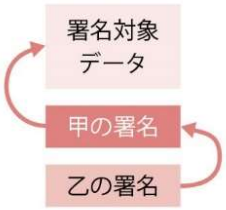
| (1) 分離形式<br>(Detached 型) | (2) 内包形式<br>(Enveloping 型) | (3) 包含形式<br>(Enveloped 型) |
|---|---|---|
|  <br>署名対象データと独立して、署名データを作成 | <br>署名データの中に署名対象データを格納(内包)して作成 | <br>署名データを署名対象データの中に含む（包含）形で作成する場合 |
| ・署名対象データの形式を問わず、あらゆるファイル形式に署名データを作成可能<br>・既存アプリで署名対象データを取り扱う場合など、アプリ側への影響が僅少<br>・署名対象データと署名データの紐づけ管理が必要 | ・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<br>・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<br>・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<br>• 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<br>• 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[1]は、なぜ必要なのか？**

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。

**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。

[1] 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。

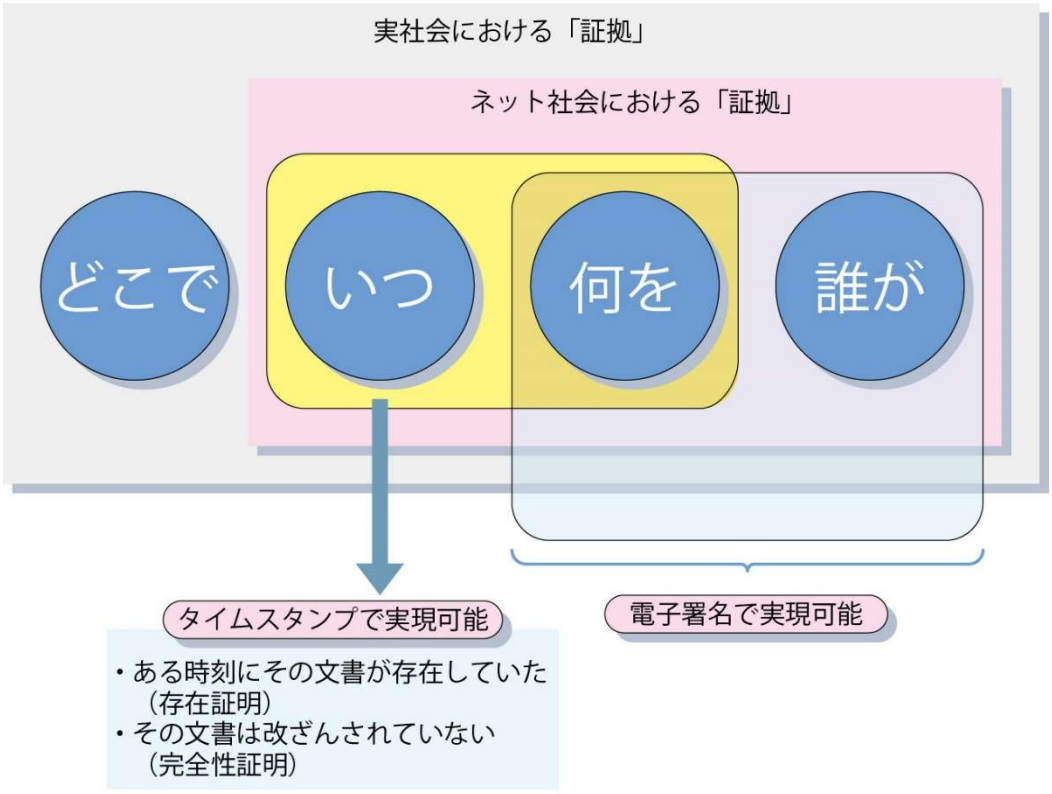



図3-4　タイムスタンプで実現される内容

### 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、かつて電子署名に用いられていた最も一般的な暗号アルゴリズムである SHA-1、RSA1024 は脆弱化が進むことが予測されたことから、

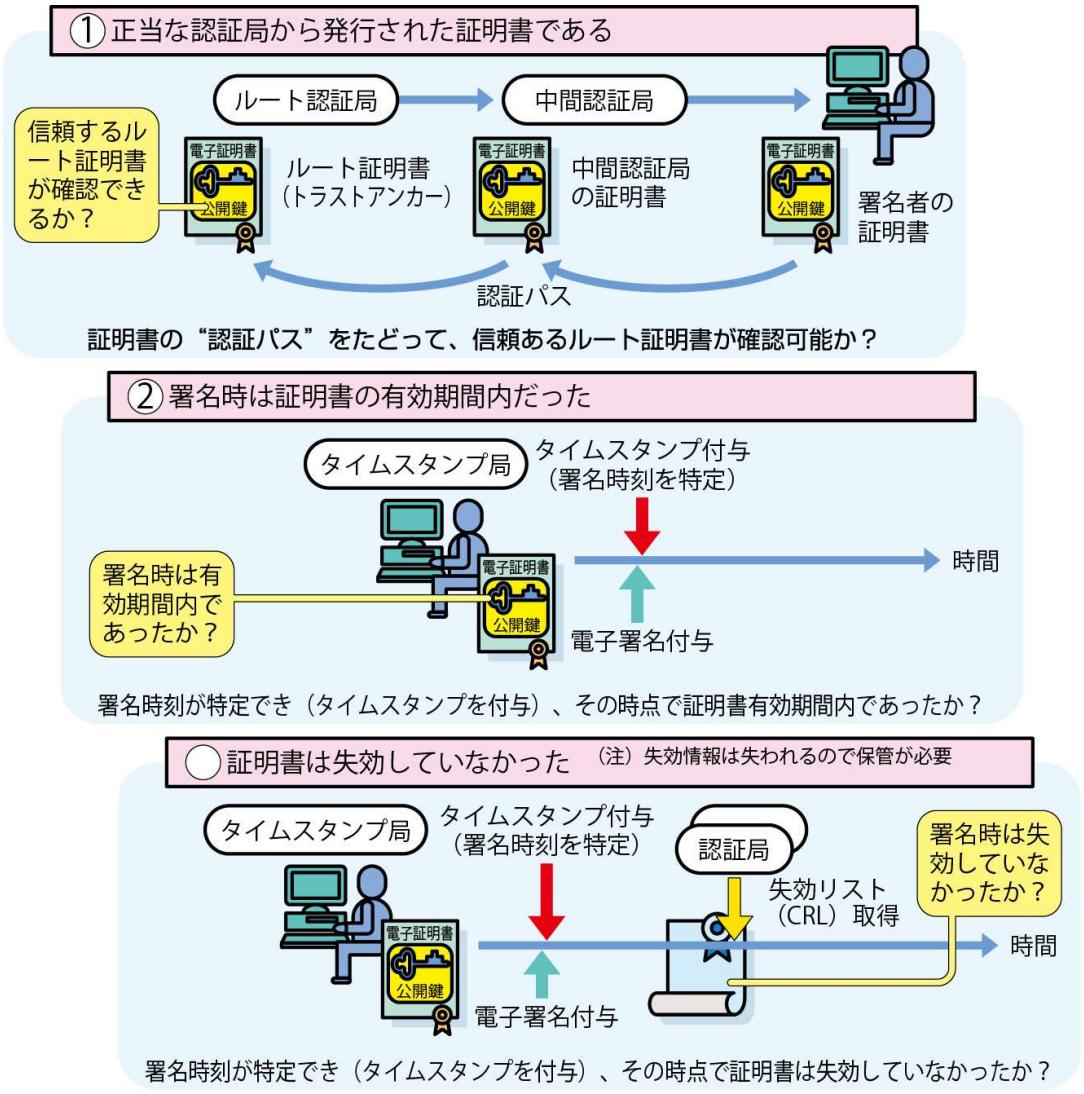



図 3-5　長期署名の技術解説

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実施されました[1]。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

1 「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）

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。

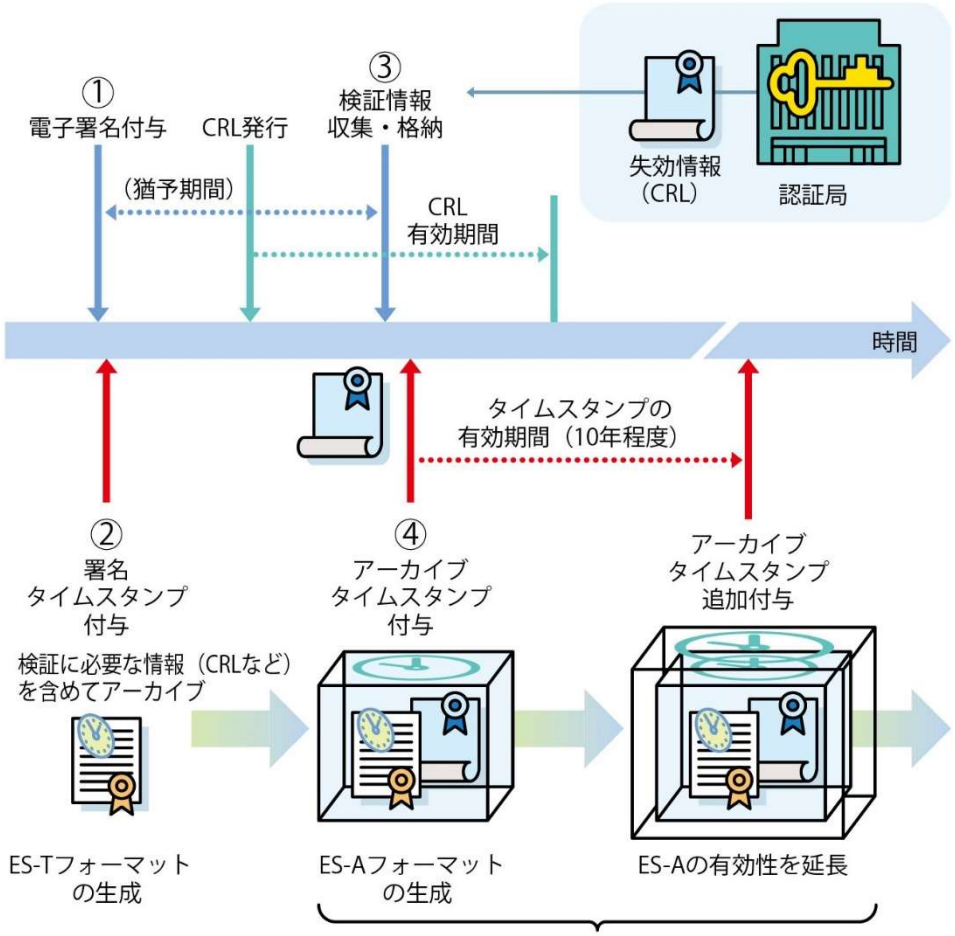



図3-6　タイムスタンプ付与の概要

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[1]
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 |

### 3.2.6 電子証明書暗号アルゴリズムの移行計画

電子署名法の主務官庁であるデジタル庁および法務省から「特定認証業務の基準の改正スケジュール等の周知について[2]」が公表されました(2024 年 5 月 15 日、同年 6 月 11 日更新)。
2028 年に政府認証基盤(BCA)が実施する暗号移行[3]に合わせ、認定認証事業者も暗号移行を順次実施予定です。
電子認証局会議では移行にあたり、利用者の皆さまや署名検証者各位へスムースな移行を可能とするよう、関係各所と調整を実施していきます。
「2028 年暗号移行に関する説明(電子認証局会議)[4]」 も、ご参照ください。

## 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「認定認証局」、「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ー」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。

---

1 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。
2https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/614eb74c-d84f-4945-8293-8f36d3a2d4c7/4cf07134/20240611_digitalsign_law_01.pdf
3 https://www.gpki.go.jp/documents/gov.html
4 https://www.c-a-c.jp/download/cmsassets/20250318_cryptomigration2028.pdf

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。

**■認定認証局**

認定認証局は、民間企業が運営する電子署名法に基づく国の特定認証業務の認定を受けた民間認証局のことです。電子証明書利用者の真偽の確認が主務省令で定める方法に基づいて厳格に実施されることが求められ、実施内容は CP/CPS に規定、公開されます。日本国内での利用に於いては、利用者を正確に特定でき、その信頼性が広く社会に受け入れられており、国や地方自治体の電子入札や電子申請などで活用されています。行政機関が運営する認証局ではありますが、会社・法人の代表者等を対象として電子証明書を発行する法務省の商業登記認証局、そして一般市民を対象として電子証明書（マイナンバーカード）を発行する公的個人認証サービスの認証局等も同じ証明書ポリシーを持ちます。

**■パブリック認証局**

パブリック認証局とは、広義の意味では、一つの組織やシステムに捉われず、広く利用されるための認証局です。そのため、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。

特に主要なブラウザー（ Microsoft Edge など）に、予め組み込まれている「信頼されたルート認証局」をパブリック認証局と呼ぶことが多くあります。この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は CP/CPS が公開され、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。

また、Adobe 社の PDF 閲覧用ソフトウェアに組み込まれている Adobe Approved Trust List(AATL)に掲載された認証局も、重要なパブリック認証局といえます。

Adobe 社が開発した PDF は、国際標準化された仕様（ISO 32000）として企業や官公庁などの電子文書の標準形式として電子署名も可能であり、電子契約にも活用されています。電子署名済み PDF を開く際に Adobe 社の Adobe Acrobat や Adobe Acrobat Reader で開くと、Adobe Approved Trust List(AATL)によってあらかじめ信頼された認証局の証明書リストを参照することで自動的に電子署名を検証可能とする仕組みを持ちます。

**■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ー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。

**■証明書発行サーバー**

認証局とは異なり、CP/CPS を定めず運用するサーバーです。単に技術的に電子証明書を発行するサーバー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。マイクロソフト Windows 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 |
|---|---|---|---|
| 認定認証局 | ◎ | ○ | △ |
| 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でも利用するコミュニティ内で非常に信頼性の高いものを構築する場合もある。

**■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の署名用電子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

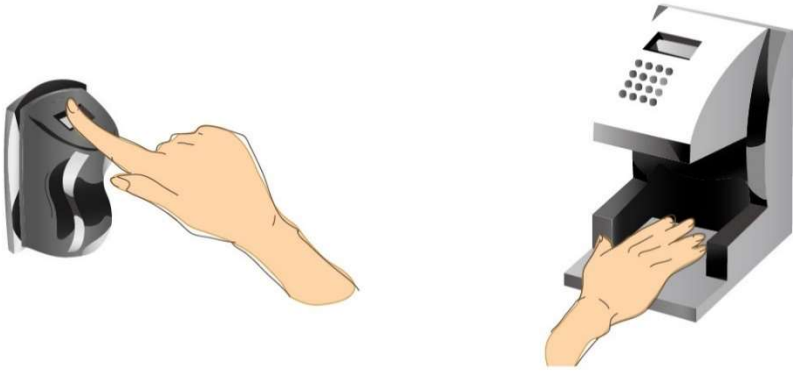
電子証明書があれば相手先の認証が可能となると同時に、相手先とやり取りをするファイルの暗号化を行うことも可能となります。安全なファイルのやり取りを行いたい場合、相手方に公開してもかまわない公開鍵を渡しておき、その鍵で暗号化したファイルを自分に送ってもらいます。公開鍵で暗号化したファイルは自分しか持っていない秘密鍵でしか復号することができませんので、万が一、暗号化したファイルが漏えいしてしまったとしても、秘密鍵が漏えいしていなければ安全だといえます。

〈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



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。

株式会社トインクス

# 4. 用語集

| 通番 | 用語 | 解説 |
|---|---|---|
| 1 | CP/CPS（Certificate Policy/Certification Practice Statement） | 認証局の運用方式、信頼性・安全性を対外的に示す文書のこと。CPは認証局が電子証明書を発行する際の運用方針を定めた証明書ポリシーを指し、CPS は運用方針の実施手順を定めた認証局運用規程を指す。 |
| 2 | e-文書法 | “e-Japan 重点計画 2004”での「IT 規制改革の推進」政策を受け、2005 年に施行された規制緩和の法律。従来、書面による保存が義務付けられていた書類を、原則、電子で保存することを容認した法律。関連分野は、税務、医療、建築、会社法など広範囲に及び、300 本以上の法律が関係するが、特に、国税、医療関連文書などのスキャナー保存の容認が有名。通則法となる「民間事業者などが行う書面の保存などにおける情報通信の技術の利用に関する法律」と、その整備などに関する法律の2本からなる。「電子文書法」ともいう。 |
| 3 | IT 基本法 | 正式名称を「高度情報通信ネットワーク社会形成基本法」といい、情報施策に対する国および地方公共団体の責務を定めた法律。 |
| 4 | IT 書面一括法 | 正式名称を「書面の交付などに関する情報通信の技術の利用のための関係法律の整備に関する法律」といい、書面の交付や書面による手続きを義務付けている法律を改正し、電子的手段（電子メールやWeb など）も認めることで電子商取引の促進を狙った法律。ただし、特定の法律（公正証書が必要なものなど）については従来どおり書面を必要とする規制が残っているものもある。 |
| 5 | PDF（Portable Document Format） | アドビ社が開発したファイルフォーマット。作成したドキュメントを異なるパソコン環境で元のレイアウトどおりに表示・印刷可能な特性を持つ。2008 年7月に国際規格（ISO32000-1）として認定されている。 |
| 6 | PL 法 | 正式名称を「製造物責任法」といい、製造物の欠陥により人の生命、身体又は財産に係る被害が生じた場合における製造業者などの損害賠償の責任について定めた法律。 |
| 7 | RSA1024/RSA2048 | 公開鍵暗号方式である RSA 暗号において処理の際に用いる鍵のデータ長の規格の一つ。鍵のデータ長が長いほど暗号の強度が高く安全とされ、RSA1024 から RSA2048 への移行が実施された。 |
| 8 | S/MIME | 公開鍵暗号方式による電子メールの暗号化と電子署名に関する標準規格。 |
| 9 | SHA-1/SHA-2 | 暗号処理の際に使用されるハッシュ関数（一方向関数）の一つ。SHA-1 の生成するハッシュ値は 160 ビット、SHA-2 の場合は224～512ビットである。一般的にハッシュ値が長いほど安全とされ、SHA-1 から SHA-2 への移行が実施された。なお、SHA-2 は SHA-224、SHA-256、SHA-384、SHA-512 の4種類の総称である。 |

| | | |
|---|---|---|
| 10 | SSL/TLS | インターネット上でデータを暗号化して通信する技術、取り決め。通信者は電子証明書を参照することによって通信先を確認することができ、通信データは電子証明書による暗号化通信によって第三者からの盗聴や改ざんから守られる。 |
| 11 | XML （ Extensible Markup Language） | 属性と値で構成された論理性と拡張性に優れたファイルフォーマット。コンピュータ側で処理することに適した特性を持つ。 |
| 12 | クライアント証明書 | 特定の個人や機器などに発行される電子証明書。ユーザー認証や電子署名の付与、データの暗号化などに利用される。 |
| 13 | サーバー証明書 | サーバーを対象に発行される電子証明書。サーバー証明書によって、サーバーの正当性を証明するとともに、サーバーとクライアント PC 間で情報を送信する際の暗号化通信にも利用される。Web サイトで利用される SSL サーバー証明書が代表例。 |
| 14 | タイムスタンプ | ある時刻にある電子データが存在していたことを証明する「存在証明」と、ある時刻以降電子データの内容が改ざんされていないことを証明する「完全性証明」を実現する仕組みのこと。この証明となる電子データをタイムスタンプトークンというが、これをタイムスタンプと略して呼ぶことも多い。「時刻認証」ともいう。 |
| 15 | タイムスタンプ局 | 電子署名などの手段でタイムスタンプの付与およびタイムスタンプの有効性を保証する機関。電子データの「存在証明」と「完全性証明」を実現する上で重要な役割を果たす。「時刻認証局」ともいう。 |
| 16 | ハッシュ値 | 数値や文字列のデータをハッシュ関数によって一定の長さに変換した値。ハッシュ関数とは擬似乱数を生成する一方向関数で、ハッシュ値の逆算や偽造は極めて困難とされる。 |
| 17 | パブリック認証局／パブリック証明書 | 不特定多数の広範囲に電子証明書を発行する電子認証局のこと。利用者または電子証明書を受け取った相手は公開されているCP/CPSの内容を確認し、信頼できる電子認証局か判断し利用する。通常、主要なブラウザーの「信頼されたルート認証局」にトラストアンカーが予め組み込まれており、Webtrust 制度など外部機関の監査を受けることで電子認証局としての信頼性は高くなる。 |
| 18 | フィンガープリント | 電子証明書の正当性を証明するデータ。電子証明書内のフィンガープリント（拇印）と別途認証局側で公開しているフィンガープリントを照合し一致すれば正しい証明書と確認できる。 |

| | | |
|---|---|---|
| 19 | プライベート認証局／プライベート証明書 | 企業内などの限られた場所や特定の相手など限られた範囲に電子証明書を発行する電子認証局のこと。対象者内でルールを守って利用されればよいため CP/CPS を公開しない場合もある。 |
| 20 | ブリッジ認証局 | 政府認証基盤（GPKI）を構成する認証局の一つで、行政機関側認証局と外部の認証局との中間に位置し、それぞれと相互認証することで橋渡しを行う電子認証局のこと。 |
| 21 | ヘルスケア PKI | 厚生労働省が保健医療福祉分野で用いる電子証明書を標準化するために推進する公開鍵基盤。医療従事者の国家資格属性を証明書に記入することができるので、“医師が電子署名したもの”であることなどが検証可能となる。 |
| 22 | リポジトリ | 電子認証局を構成する要素の一つであり、CP/CPS や失効リストなどの情報公開を行うサービス。 |
| 23 | ルート証明書（自己署名証明書） | ルート認証局が自身の正当性を証明するために発行する電子証明書で自己署名証明書ともいう。利用者の電子証明書内部にはルート証明書への経路情報が存在し、利用者の電子証明書の信頼性を確認する場合にルート証明書によって確認する。なお、この時信頼の起点となるルート証明書のことをトラストアンカーと呼ぶ。 |
| 24 | ルート認証局 | 他の上位の認証局から証明書を受けない最上位の認証局。利用者の証明書の認証パスの最上位に位置し、トラストアンカーとなるルート証明書を発行したり、他の中間認証局に対して証明書を発行する。ルート認証局は利用者証明書の信頼の拠り所になるため、信頼するに足りるセキュリティの高い運用を行い、その基準を CP/CPS などで開示して証明書利用者の信頼を得る必要がある。なお、Microsoft Edge などのブラウザーに証明書が格納されているルート認証局をパブリックルート認証局と呼ぶこともある。 |
| 25 | 暗号アルゴリズム | 暗号化する際の手順・方式。 |
| 26 | 原本性保証 | 複製ではなく本人が作成し以後改ざんされていない原本であることを保証すること。電子文書においては電子署名とタイムスタンプを組み合わせることにより、本人が作成し以後改ざんされていないことを証明できる。 |
| 27 | 公開鍵 | 公開鍵暗号方式で使用される一対の鍵の一つで、一般に公開される鍵。公開鍵は秘密鍵とは異なり、他人に知られても悪用されるおそれはない。秘密鍵で電子署名されたデータは一対の公開鍵でのみ検証可能となる。一方、公開鍵で暗号化されたデータは一対の秘密鍵でのみ復号可能となるので、特定の人にだけデータを渡す際の暗号化に用いられる。 |

| | | |
|---|---|---|
| 28 | 公的個人認証サービス(JPKI) | 住民基本台帳に記載されている者を対象に、各地方公共団体からマイナンバーカードに格納される形で電子証明書が発行される。電子証明書は政府機関や各地方公共団体への電子申請・届出などの行政手続に利用できる。 |
| 29 | 公的個人認証法 | 正式名称を「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」といい、申請・届出などの行政手続をオンラインでできるようにするための公的個人認証サービス(JPKI)制度を規定した法律。 |
| 30 | 失効リスト | 電子証明書の失効情報を掲載するリストで「ARL(Authority Revocation List)」と「CRL(Certificate Revocation List)」の2種類ある。ARL は認証局自身の電子証明書の失効情報を掲載し、CRL は認証局が発行した電子証明書の失効情報を掲載する。 |
| 31 | 商業登記電子証明書 | 法人を対象に、法務省の電子認証登記所の登記官から発行される電子的な証明書。従来の印鑑証明書・資格証明書によって確認している「本人性」、「法人格の存在」、「代表権限の存在」に代わるもので、印鑑登録された社印と同等の法的有効性が認められている。 |
| 32 | 商業登記法 | 商法や会社法の規定されている登記すべき事項の手続について定めた法律。2000 年4月に商業登記に基づく電子認証制度のための改正が行われた。 |
| 33 | 署名検証 | 電子署名の有効性を確認する行為。「電子署名が付与された電子データが改ざんされていないこと」「電子証明書が有効であること」「電子証明書の信頼性が確認されていること」などを確認する。狭義の意味では、「電子署名が付与された電子データが改ざんされていないこと」のみ確認することを指し、「電子証明書が有効であること」「電子証明書の信頼性が確認されていること」は証明書検証として分けて扱われる。 |
| 34 | 政府認証基盤(GPKI) | 政府が運用する認証基盤で、官職認証局、日本政府認証局、ブリッジ認証局の3つの電子認証局から構成される。各認証局からは官職証明書、文書等署名用官職証明書、相互認証証明書などがそれぞれ発行される。 |
| 35 | 耐タンパ性 | 内部情報を不正に読み取られる・改ざんされることに対する耐性のこと。IC カードなど耐タンパ性が高い媒体は不正アクセスに対する強度が高いといえる。 |
| 36 | 地方公共団体組織認証基盤(LGPKI) | 地方公共団体の認証基盤で、地方公共団体職員の職責者に対して職責証明書を発行している。ブリッジ認証局と相互認証している。 |

| | | |
|---|---|---|
| 37 | 中間認証局 | ルート認証局が発行する電子証明書にて自身の正当性を証明する認証局。認証局としての信頼性がルート証明書によって示される点でルート認証局と異なる。 |
| 38 | 長期署名フォーマット | 電子署名とタイムスタンプを組み合わせることで電子署名の検証期間を長期間に渡り維持する仕組み。署名対象毎に「CAdES（CMS Advanced Electronic Signatures）」、「XAdES（XML Advanced Electronic Signatures）」、「PAdES（PDF Advanced Electronic Signatures）」などがあり、それぞれ ISO14533-1、ISO14533-2、ISO 14533-3 として国際規格化が進められている。 |
| 39 | 電子証明書 | 利用者の公開鍵が本人に帰属していることを証明するために認証局が発行する電子的な証明書。「公開鍵証明書」ともいう。 |
| 40 | 電子署名 | 電子証明書を利用した暗号技術により、本人が作成したことを表し、かつ改ざんの有無が確認できるよう本人の秘密鍵により生成された電子的な署名データ。 |
| 41 | 電子署名法 | 正式名称を「電子署名及び認証業務に関する法律」といい、電子署名の定義、電磁的記録の真正な成立の推定、特定認証業務の認定制度について定めた法律。電子文書に対する電子署名が紙文書に対する署名や押印と同等の法的効力を持つと規定されている。 |
| 42 | 電子帳簿保存法 | 正式名称を「電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律」といい、従来紙での保存が義務付けられていた国税関係帳簿書類を、一定の要件を満たすことによって電子データとして保存することを容認した法律。 |
| 43 | 電子認証 | インターネット等ネットワークを利用したやり取りにおいて、電子証明書を用いて本人性を証明する技術のこと。 |
| 44 | 電子認証局（CA） | 電子証明書の発行と失効を行う機関のことで、「CA（Certificate Authority）」ともいう。登録局（RA）、発行局（IA）、リポジトリなどから構成される。 |
| 45 | 登録局（RA） | 電子認証局を構成する要素の一つであり、電子証明書発行のための審査・登録を行う機関のことで、「RA（Registration Authority）」ともいう。 |
| 46 | 特定認証業務 | 電子署名法上の技術的基準に準拠した認証業務のこと。 |
| 47 | 認証パス | 利用者の電子証明書からルート証明書までの信頼の経路。 電子署名の有効性を検証する場合、この経路を元に電子証明書の信頼性を確認する。 |
| 48 | 認定認証業務 | 電子署名法上の技術的基準、設備基準、業務方法に関する基準などをクリアし、国が指定した調査機関の審査を受け認定された認証業務のこと。 |

| | | |
|---|---|---|
| 49 | 発行局(IA) | 電子認証局を構成する要素の一つであり、電子証明書を発行する機関のことで、「IA(Issuing Authority)」ともいう。 |
| 50 | 秘密鍵 | 公開鍵暗号方式で使用される一対の鍵の一つで、利用者本人のみが保有し一般に公開されない鍵。秘密鍵が他人に知られると悪用されるおそれがあるため、厳重に管理する必要がある。秘密鍵は本人のみが所持するものなので電子署名に用いられる。「私有鍵」ともいう。 |
| 51 | 復号 | 暗号化された暗号文を解いて元の平文に戻すこと。 |

# 5. 関係法令とガイドライン

■主務省

●デジタル庁（ https://www.digital.go.jp/）

>電子署名

https://www.digital.go.jp/policies/digitalsign/

>電子委任状法

https://www.digital.go.jp/policies/digitalpoa/

●法務省（ https://www.moj.go.jp/）

>電子署名法の概要と認定制度について

https://www.moj.go.jp/MINJI/minji32.html

■電子署名・電子認証に関わる法律一覧

●電子署名法関係

>電子署名及び認証業務に関する法律(電子署名法)

https://laws.e-gov.go.jp/law/412AC0000000102

>電子署名及び認証業務に関する法律施行規制(電子署名法施行規則)

https://laws.e-gov.go.jp/law/413M60000418002

●電子委任状法関係

>電子委任状の普及の促進に関する法律(電子委任状法)

https://laws.e-gov.go.jp/law/429AC0000000064

>電子委任状の普及の促進に関する法律施行規則(電子委任状法施行規則)

https://laws.e-gov.go.jp/law/429M60000408001

●IT 基本法

>高度情報通信ネットワーク社会形成基本法

https://laws.e-gov.go.jp/law/412AC0000000144/20210901_503AC0000000035

●IT 書面一括法

>書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律

https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/15020001127126.htm

●e-文書法関係

>通則法：民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律

https://laws.e-gov.go.jp/law/416AC0000000149

>整備法：民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律

https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/16120041201150.htm

●電子帳簿保存法関係

（ https://www.nta.go.jp/law/joho-zeikaishaku/sonota/jirei/index.htm ）

>電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律（電子帳簿保存法）

https://laws.e-gov.go.jp/law/410AC0000000025

>電子計算機を使用して作成する国税関係帳簿書類の保存方法等に関する法律施行規則（電子帳簿保存法施行規則）

https://laws.e-gov.go.jp/law/410M50000040043

>電子帳簿保存法 Q&A

https://www.nta.go.jp/law/joho-zeikaishaku/sonota/jirei/4-1.htm

●公的個人認証関係

>電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律(公的個人認証法)

https://laws.e-gov.go.jp/law/414AC0000000153

●商業登記に基づく電子認証制度関係

>商業登記法

https://laws.e-gov.go.jp/law/338AC0000000125

●厚生労働省関係

>厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令

https://www.mhlw.go.jp/topics/2005/03/tp0328-1a.html

>医療情報システムの安全管理の関するガイドライン

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

●国土交通省関係

>建設業法施行規則第 13 条の2第2項に規定する「技術的基準」に係るガイドライン

https://www.mlit.go.jp/pubcom/01/kekka/pubcomk06/pubcomk06-1_.html

■電子署名に関連する団体

●一般財団法人　日本情報経済社会推進協会(JIPDEC)( https://www.jipdec.or.jp/)

>電子署名法に基づく特定認証業務の調査

https://www.jipdec.or.jp/project/designated-investigative-organization.html

●一般社団法人　デジタルトラスト協議会(JDTF)( https://jdtf.or.jp/)

>ホワイトペーパー

https://jdtf.or.jp/report/whitepaper/

●日本トラストテクノロジー協議会(JT2A)( http://www.jt2a.org/)

>リモート署名ガイドライン

https://www.jnsa.org/result/jt2a/2020/index.html

●一般財団法人　日本データ通信協会( https://www.dekyo.or.jp/)

>認定タイムスタンプを利用する事業者に関する登録制度

https://www.dekyo.or.jp/touroku/

>総務大臣認定制度による認定時刻認証業務の一覧

https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html

●次世代電子商取引推進協議会(ECOM)

※ 2010 年 3 月 31 日をもって解散しており、日本情報経済社会推進協会(JIPDEC)Web サイトにてアーカイブスが公開されています。

>電子文書の長期保存と見読性に関するガイドライン

https://www.jipdec.or.jp/archives/publications/J0004225

●一般社団法人　保健医療福祉情報システム工業会(JAHIS)( https://www.jahis.jp/)

>ヘルスケア PKI を利用した医療文書に対する電子署名規格

https://www.jahis.jp/standard/detail/id=167

>JAHIS 保存が義務付けられた診療録等の電子保存ガイドライン

https://www.jahis.jp/standard/detail/id=87?contents_type=33

●公益社団法人　日本文書情報マネジメント協会（JIIMA）（ https://www.jiima.or.jp/）
　>政策提言・ガイドライン
　https://www.jiima.or.jp/activity/policy/
●一般社団法人　日本建設業連合会（ https://www.nikkenren.com/）
　>情報セキュリティに関するガイドライン・教育資料集
　https://www.nikkenren.com/kenchiku/ict/security/guideline.html
●特定非営利活動法人　日本ネットワークセキュリティ協会（JNSA）（ https://www.jnsa.org/）

# 6. 付録

## 6.1 電子認証局会議について

■組織名称: 電子認証局会議
(英語名称:CERTIFICATION AUTHORITY CONFERENCE)
■設立年月日: 2006 年 9 月 11 日
■事 業 内 容:
(1) 電子認証局ならびに関連事業者との情報交流、情報提供に関する活動
(2) 電子認証業務およびその認定に対する政策提言、法制度改正提言に関する活動
(3) 電子署名・電子認証の利活用拡大、オンライン手続の利用促進に関する活動
(4) 電子署名・電子認証の普及啓発促進に関する活動
(5) 電子署名・電子認証の広報宣伝活動に関する活動
(6) 政府関係機関、他関係諸団体との渉外、連絡、意見交流に関する活動
(7) 上記各号に掲げた事業に付帯する活動
■ URL:https://www.c-a-c.jp/
■メールアドレス:info@c-a-c.jp

## 6.2 認証局のサービスガイド

電子認証局会議の会員が提供するサービスをご紹介いたします。
記載内容に関するお問合せは、各社の問合せ先までご連絡ください。
【記 載 例】
認証局運営組織名:認証局を運営する主体組織名を記載しています。
URL:認証局の主たる Web ページを記載しています。
【サービス名】主たるサービス名を記載しています。
【概　　要】サービスの概要を記載しています。
【問合せ先】サービスにかかわる問合せ先を記載しています。

| | |
|---|---|
| 組織名 | NTTビジネスソリューションズ株式会社 |
| URL | https://www.e-probatio.com/ |
| サービス名 | e-Probatio PS2 サービス |
| 概要 | 主に電子入札、電子契約、電子納税などの業務において利用される電子証明書(IC カード)を発行するサービスです。 |
| 問合せ先 | https://www.e-probatio.com/contact/<br>上記 URL よりお問い合わせください。<br>TEL:0120-851-240(フリーダイヤル) |

| | |
|---|---|
| 組織名 | 株式会社サイバーリンクス |
| URL | https://mynatrust.jp/service/e-loa/geps/index.html |
| サービス名 | マイナトラスト電子委任状[委任者記録ファイル方式]<br>マイナトラスト電子委任状[取扱事業者記録ファイル方式] |
| 概要 | サイバーリンクスの電子委任状サービス「マイナトラスト電子委任状」は、マイナンバーカードに搭載された電子証明書を、電子的に作成された委任状に関連付けることで、受任者本人が手続を行う権限を有することを簡易かつ確実に証明します。<br>・国及び地方公共団体の調達における電子入札等の手続<br>・行政機関に対する電子申請等の手続<br>・企業間で行われる電子契約、申込み等の手続 |
| 問合せ先 | https://www.cyber-l.co.jp/mynatrust-geps_contact/<br>上記 URL よりお問合せください。<br>TEL:073-488-3787 |

| | |
|---|---|
| 組織名 | セコムトラストシステムズ株式会社 |
| URL | https://www.secomtrust.net |
| サービス名 | 認証サービス |
| 概要 | e-Tax、eLTAX や e-Gov などに対応した電子証明書を発行する「セコムパスポート for G-ID」、日本で初めて Webtrust に適合し、信頼されたパブリックルート認証局として、高度なセキュリティ水準を誇るサーバー証明書を発行する「セコムパスポート for Web」、サービス事業者向けにタイムスタンプ、リモート署名などを、ひとつのプラットフォームで提供する「セコムパスポート Plus」など幅広いサービスを提供します。 |
| サービス名 | 文書電子化サービス |
| 概要 | e-文書法対応をはじめ、様々な文書の電子化保存に必要な電子証明書、タイムスタンプ、長期署名システムなどをワンストップで提供します。タイムスタンプは電子帳簿保存法等で求められる「認定タイムスタンプ」を利用しています。 |
| 問合せ先 | https://www.secomtrust.net/contact/form.html<br>上記 URL よりお問合せください。<br>TEL:0120-39-0756 |

| | |
|---|---|
| 組織名 | 株式会社帝国データバンク |
| URL | https://www.tdb.co.jp/typeA/ |
| サービス名 | TDB 電子認証サービス TypeA |
| 概要 | 電子入札コアシステムを導入する国土交通省や地方自治体など公共発注機関の電子入札に利用できる電子証明書です。政府電子調達システム（GEPS）や一部省庁の電子申請、国税電子申告・電子納税システム（e-Tax）、地方税ポータルシステム（eLTAX）など、幅広い電子申請システムでご利用可能です。組織代表者から委任された代理権内容を予め電子証明書に格納する電子委任状にも対応しています。<br>電子証明書は「4 種類の有効期間」をご用意、「入札情報の無料配信」などの利便性の高いサービスを提供しています。また、電子証明書の破損や紛失、記載事項の変更等に伴う買い直し時に利用できる割引制度や、各地の商工会議所・商工会に所属する会員様向けのお得な割引制度もございます。 |
| 問合せ先 | 電子認証局ヘルプデスク<br>TEL：0570-011999<br>e-mail：certinfo@mail.tdb.co.jp |

| | |
|---|---|
| 組織名 | 株式会社トインクス |
| URL | https://www.toinx.net/ebs/info.html |
| サービス名 | TOiNX 電子入札対応認証サービス |
| 概要 | 当社では、国・地方自治体・公共団体などが提供している電子入札、電子申請、電子申告・納税といった電子行政サービスを利用するために必要となる、電子証明書をご提供しております。当サービスは、専任スタッフによるヘルプデスクサポートや記載内容変更時割引、更新割引などの各種割引制度の充実とともに、東北電力企業グループとして安心・安全をご提供いたします。 |
| 問合せ先 | 株式会社トインクス　電子認証センター<br>e-mail：toinx.cert@toinx.co.jp<br>TEL：022-799-5566<br>FAX：022-799-5565 |

| | |
|---|---|
| 組織名 | 日本行政書士会連合会 |
| URL | https://www.gyosei.or.jp/ |
| サービス名 | セコムパスポート for G-ID 行政書士電子証明書 |
| 概要 | 行政書士電子証明書を、行政書士資格を証明できる電子証明書として行政書士に推奨しています。<br>行政書士電子証明書は電子定款に多く利用されており、また、行政自動車保有関係手続のワンストップサービス（OSS）にも対応しています。 |
| 問合せ先 | https://www.secomtrust.net/sts/contact/entry.html （セコムトラストシステムズ社）<br>電子証明書の取得に関する事項は上記 URL よりお問い合わせください。<br>日本行政書士会連合会　登録課<br>TEL　03-6435-7330 |

| | |
|---|---|
| 組織名 | 日本司法書士会連合会 |
| URL | https://ca3.nisshiren.jp/repository/ |
| サービス名 | セコムパスポート for G-ID 司法書士電子証明書 |
| 概要 | 日本司法書士会連合会が提供する情報に基づき発行する司法書士法施行規則第 28 条第 2 項で法務大臣が指定した電子証明書です。司法書士会の会員が司法書士業務として行うオンライン登記申請等に用いるための電子証明書です。発行の対象は司法書士会の会員のみです。 |
| 問合せ先 | セコムトラストシステムズ株式会社<br>CAサポートセンター 司法書士電子証明書担当<br>E-mail: gid-shiho@secom.co.jp<br>TEL: 0570-020-213<br>※ナビダイヤルへ発信できない場合、050-3786-2782 をご利用ください。受付時間:9:00～12:00 13:00～17:00(土日・祝日及び年末年始を除く) |

| | |
|---|---|
| 組織名 | 日本税理士会連合会 |
| URL | https://www.nichizeiren.or.jp/ |
| 概要 | 日本税理士会連合会では、国税及び地方税の電子申告に対応するための電子証明書の発行に関する事務を税理士会員に対して行っています。 |
| 問合せ先 | TEL:03-5435-0940<br>FAX:03-5435-0941 |

| | |
|---|---|
| 組織名 | 日本電子認証株式会社 |
| URL | https://www.ninsho.co.jp |
| サービス名 | AOSign サービス、法人認証カードサービスなど |
| 概要 | 当社は、建設企業・前払金保証事業会社などにより設立されました。電子入札のほか、電子申請、電子申告など多彩な利用用途に対応し、お客様のニーズにあった電子認証サービスをご提供いたします。<br>AOSign サービスは、電子入札コアシステム対応の電子証明書(IC カード)を発行するサービスです。<br>法人認証カードサービスは、「商業登記に基づく電子証明書」を IC カードに格納してお届けするセキュリティサービスです。 |
| 問合せ先 | 上記 URL の「お問い合わせ」をご利用ください。<br>フリーダイヤルのヘルプデスクにて、きめ細かくサポートいたします。 |

| | |
|---|---|
| 組織名 | 日本土地家屋調査士会連合会 |
| URL | https://www.chosashi.or.jp/members/repository/ |
| サービス名 | セコムパスポート for G-ID 土地家屋調査士電子証明書 |
| 概要 | 土地家屋調査士は、他人の依頼を受けて不動産の表示に関する登記に必要な調査・測量を行い、その位置・形状を明確にし、登記の申請手続等を行う国家資格者です。<br>当連合会では、土地家屋調査士会員に発行される電子証明書の登録局に係る事務の一部を行っています。 |
| 問合せ先 | 日本土地家屋調査士会連合会　事務局　電子認証担当<br>e-mail:ca-info@chosashi.or.jp<br>TEL:03-3292-0050 |

| | |
|---|---|
| 組織名 | my FinTech株式会社 |
| URL | https://www.myfintech.co.jp/ |
| サービス名 | my 電子証明書 |
| 概要 | 当社は、デジタル ID 事業において、「安全・安心なデジタル ID の提供」を実現すべく設立された会社になります。my 電子証明書は、当社が提供するデジタル ID をスマートフォンベースで提供するべく開発された、認証基盤サービスとなります。my 電子証明書を基盤とするデジタル ID は、犯罪収益移転防止法や携帯電話不正利用防止法を始めとした本人確認において、認定の効力を発揮することができます。また、デジタル ID に紐づけられた個人情報についても、連携先の事業者及び連携するタイミングを利用者自身の意思で決定でき、かつ当該意思決定には、紙における署名や記名押印と同等の法的効力を持つことが可能となります。本サービスは、群馬県前橋市・北海道江別市・長崎県大村市様にご導入いただいており、他の自治体様や事業者様につきましても、ご導入を検討頂いております。 |
| 問合せ先 | [電話]<br>・代表電話:03-6878-5530<br>・サービスヘルプデスク:0120-059-745<br><br>[問い合わせフォーム]<br>・企業問い合わせフォーム<br>(https://www.myfintech.co.jp/お問い合わせフォーム)<br>・my 電子証明書お問い合わせフォーム<br>(https://www.myfintechtrust.jp/support/contact_form.html) |

| | |
|---|---|
| 組織名 | 三菱電機デジタルイノベーション株式会社 |
| URL | https://www.mind.co.jp/service/diacert.html |
| サービス名 | DIACERT サービス（電子申請用電子証明書） |
| 概要 | ファイル形式の電子証明書を USB メモリに格納して提供するサービスです。e-Gov、e-Tax 等の国や地方の電子申請、電子納税等のお手続きや e-文書法に基づく保存義務のある文書への電子署名に利用可能です。 |
| URL | https://www.mind.co.jp/service/diacert-plus.html |
| サービス名 | DIACERT-PLUS サービス（電子入札用電子証明書） |
| 概要 | 中央省庁や地方自治体などの公共発注機関に対する電子入札に使用する IC カードタイプの電子証明書を提供するサービスです。<br>DIACERT／DIACERT-PLUS サービスは「電子署名及び認証業務に関する法律」（電子署名法）に基づく特定認証業務の認定を取得しています。 |
| URL | https://www.mind.co.jp/service/eppcert.html |
| サービス名 | Enterprise Premium 電子証明書発行サービス（EPPCERT） |
| 概要 | 企業内・企業間で利用する電子証明書を提供するサービスです。人物や組織の認証用途、電子データへの電子署名用途の電子証明書を提供可能です。提供方法としてダウンロード形式、ならびに CD、USB トークンへの格納のラインナップを揃えています。 |
| 問合せ先 | ホームページの「お問い合わせ」を利用ください。<br>https://www.mind.co.jp/contact/index.html |

電子署名活用ガイド編集委員

【初　版】

●ワーキンググループ

| | |
|---|---|
| セコムトラストシステムズ株式会社 | 西　山　　晃（WG リーダー） |
| 株式会社帝国データバンク | 浅海　輝一 |
| 株式会社帝国データバンク | 小嶋　一隆 |
| 株式会社日本電子公証機構 | 小谷　達人 |
| 日本電子認証株式会社 | 高　橋　　章 |
| 日本電子認証株式会社 | 石山　敏雄 |
| 日本電子認証株式会社 | 平　尾　　仁 |
| 日本認証サービス株式会社 | 町　田　　陽 |
| 日本認証サービス株式会社 | 森岡　照善 |

●監修

| | |
|---|---|
| 弁護士 | 牧野　二郎 |

【第 2版】

| | |
|---|---|
| 株式会社エヌ・ティ・ティ ネオメイト | 新　井　　聡 |
| ジャパンネット株式会社 | 中村　克巳 |
| セコムトラストシステムズ株式会社 | 西　山　　晃 |
| セコムトラストシステムズ株式会社 | 佐藤　順之 |
| セコムトラストシステムズ株式会社 | 吉田　昌徳 |
| 株式会社帝国データバンク | 辻　　博之 |
| 株式会社帝国データバンク | 伊藤　政章 |
| 株式会社帝国データバンク | 小田嶋 昭浩 |
| 東北インフォメーション・システムズ株式会社 | 五十嵐 和成 |
| 株式会社日本電子公証機構 | 小谷　達人 |
| 株式会社日本電子公証機構 | 牛川　智晴 |
| 日本電子認証株式会社 | 高　橋　　章 |
| 日本電子認証株式会社 | 福田　義浩 |
| 日本電子認証株式会社 | 平　尾　　仁 |

●オブザーバー

経済産業省　商務情報政策局　情報セキュリティ政策室

●監　修

| | |
|---|---|
| 牧野総合法律事務所弁護士法人 | 牧野　二郎 |

【第３版】

| | |
|---|---|
| ＮＴＴビジネスソリューションズ株式会社 | 新 井　　聡 |
| 株式会社サイバーリンクス | 本 多　祐 一 |
| セコムトラストシステムズ株式会社 | 岡 本　昭 彦 |
| 株式会社帝国データバンク | 小田嶋 昭浩 |
| 株式会社トインクス | 浅野 みゆき |
| 日本電子認証株式会社 | 大 塚　崇 博 |
| フューチャー・トラスト・ラボ | 西　山　　晃 |
| my FinTech 株式会社 | 林　　昌 孝 |
| 三菱電機デジタルイノベーション株式会社 | 中 村　克 巳 |

●監　修

| | |
|---|---|
| 牧野総合法律事務所弁護士法人 | 牧 野　二 郎 |

（敬称略、社名五十音順。各版の発行当時の組織名・氏名を記載しています。）

電子署名活用ガイド　第3版
発行者：電子認証局会議
発　行：2025 年 4 月
URL：https://www.c-a-c.jp/
問合せ：info@c-a-c.jp
Copyright © 2025 電子認証局会議 All rights reserved.
本書の全部または一部について、無断で変更、加工等を行うことを禁じます。