H12－認証・公証WG－1

電子署名利用者システムの
構築・利用ガイドライン

平成13年3月

電子商取引推進協議会
認証・公証WG
Ｅジャパン協　議　会

目　　次

図　表　目　次

はじめに

21 世紀を迎えた今、インターネットは広汎な個人や企業により、普段の生活や経済活動で活用されている。様々な分野の、大量の、かつ新鮮な情報が手軽に入手できる点で生活が便利になり、取引や手続きもネットワーク上で行うことができるので、従来に加えて利用効率が高まった。音楽やプログラムなどのディジタル商品は、それ自体がネットワーク上で流通している。

このような利便性や利用効率の向上とは裏腹に、インターネットを利用する際の不具合も読者は現実に経験しているのではないだろうか。例えば、インターネット・ショッピングに不安を感じることもあるかもしれない。あるいは、普段面識のない企業から商品などの紹介が電子メールで送られて来て、プライバシー保護の点で懸念を抱くこともあるのではないだろうか。

平成 13 年 4 月 1 日より電子署名法が施行されるが、これを契機として、産業界全体での電子商取引の普及拡大にさらに拍車がかかることは間違い無く、それに牽引されて電子署名の社会全般への普及も急速に進展すると考えられる。

電子商取引の普及･発展に向けては、電子署名技術、さらには電子認証システムに対する社会全体の信頼感を現行の印鑑制度と同レベルにまで高めていくことが必要不可欠である。

そのためには、より信頼性が高くて、導入し易く、相互運用性が高い電子認証システムを構築することが必要である。

所謂、電子署名法における特定認証業務の基準に合致した認証機関が、適切な本人認証および安全な認証業務を遂行したとしても、消費者、サイバーショップ､企業従業員などの認証システム利用者が使用するハード､ソフト及び運用が電子署名の安全性を保証できなければ､信頼できる電子認証・電子署名が成り立たず､安心して電子商取引が行なえない。

このように、電子署名の実務での本格的利用のためには、「利用者システムをどのように構築し、利用するかという点について、遵守すべきルール」が必要であり、その点を本ガイドラインでは対象とし、セキュリティ要件ならびに考慮点を列挙している。

本ガイドラインの主題は、インターネットの利用における安全性の確保である。また、そのための仕組みである「電子署名」あるいは「署名」と呼ばれる技術を、インターネットの利用者の観点から、また電子署名を実現するソフトウェア開発者の観点から検討する。

①　利用者と電子署名

インターネットの利用者は、通信や取引を安全に行うために電子署名が利用できる。ただし、安全性を得るには、ソフトウェア等の取り扱いに関して最低限の留意事項を守ることが求められる。本ガイドラインでは、利用者が電子署名を扱う場面や手順と、その留意事項を提示する。本ガイドラインにおける利用者とは、通信や取引における電子署名の利用者であり、また、電子署名の裏付けとなる電子認証サービスを受ける利用者でもある。

②　開発者と電子署名

安全性を確保するためには、電子署名を行うソフトウェアは、悪用等による不正を許すものであってはならない。この観点から、本ガイドラインでは電子署名を行うソフトウェアの開発者向けに、安全性確保に求められる要件を提示する。この成果は来年度の認証・公証ＷＧへ引き継ぎ、当該ソフトウェアに関する安全性基準を Common Criteria (ＩＳO/ＩＥＣ 15408、ＪＩＳ5070) に基づく Protection Profile として成果をまとめることを想定している。Protection Profile への準拠は、利用者がソフトウェアの安全性を判断する際の一つの指針となるものである。

また、電子署名を行うソフトウェアやそれを利用するアプリケーション・プログラムは、安全性の側面を重視する結果、ともすると利用者に不親切なものとなりがちであった。パソコンに表示する通知や指示が技術者以外には分かりづらく、利便性の点で課題がある場合である。利便性を確保することは、利用上の誤りを防ぎ、運用も含めた安全性確保に重要である。本ガイドラインでは利便性確保のためのソフトウェア開発者への指針もあわせて提示している。

本ガイドラインは、4 部で構成されており、読者との対応は次のとおりである。

- 個人利用者‥‥‥第Ⅰ部および第Ⅱ部
- 企業での利用者‥‥‥第Ⅰ部および第Ⅲ部
- ソフトウェア開発者‥‥‥第Ⅳ部

第Ⅰ部では、個人および企業の利用者を対象に、電子署名に関する基本的な事項を、専門知識を前提とせずにできるだけ平易に説明している。本ガイドラインの導入部である。

第Ⅱ部は、電子メールとインターネット・ショッピングを例に、個人の利用者を対象として、安全性を確保するための留意事項と対策を平易に記述している。

第Ⅲ部は、企業間電子商取引における企業での利用を対象に、安全性を確保するための留意事項と対策を記述している。企業間電子商取引においては不正な取引の影響が個人の場合よりも大きいが、その一方では対策により多くの費用を充てることができ、またシステム部門が電子署名に関する知識を持つこともできるので、留意事項と対策を詳細に記述している。

第Ⅳ部は、開発者向けの留意事項である。利用者システム—電子署名を扱うソフトウェアとアプリケーション・ソフトウェア—の開発者を対象とする、安全性と利便性の両方の観点を含むガイドラインである。

本ガイドラインで扱う電子署名は公開鍵暗号基盤 (ＰＫＩ：public key infrastructure) と呼ばれる技術を利用している。そこで、電子署名に関する留意事項と対策を理解する上で必要なＰＫＩの基本的な事項は、本ガイドラインの中で説明するように努めた。ＰＫＩの詳細について興味のある読者は、関連する書物も活用されたい。

参考文献

- 『電子署名・認証ハンドブック　パーソナルユース編』

  http://www.jipdec.or.jp/esac/personal.pdf
- 『電子署名・認証ハンドブック　ビジネスユース編』

  http://www.jipdec.or.jp/esac/business.pdf

  平成１３年３月、電子署名・認証センター

電子署名について前提知識を想定せずに平易に解説したハンドブックである。
本ガイドラインの理解に、特に第Ｉ部とあわせて参照することを推奨する。

今回の報告書内容を元にして、来年度は活動するため、来年度末の報告書をより実践的なものとする為に、各界各方面から忌憚の無いご意見を頂きたいと考えております。ご意見等ございます方は下記連絡先までお寄せ頂くようお願い申し上げます。

連絡先

電子商取引推進協議会（ＥＣＯＭ）
認証・公証ＷＧ
〒 135-8073
東京都江東区青海 2-45　タイム 24 ビル 10 階
TEL. 03-5500-3600
FAX. 03-5500-3660
Ｅ-mail： info@ecom.or.jp
http://www.ecom.or.jp/

第Ⅰ部　電子署名の利用

電子署名は、インターネットを利用して通信や取引を行う際に、安全性を確保するための仕組みである。

本第Ⅰ部では、以降の各部を理解するための前提として、

- 電子署名が必要な背景
- 電子署名の効果
- 電子署名の仕組み
- 電子署名の安全性とは何か
- 電子署名の利便性とは何か
- 本ガイドラインで扱うアプリケーション

を概観する。

1　電子署名が必要な背景

インターネットを利用した通信や取引には様々な脅威が伴う。そのため、安全性を確保する仕組みとして電子認証と電子署名が利用される。様々な脅威の中でも、本ガイドラインでは、不正につながり得る脅威とその対策を採り上げている。

1.1　インターネット利用における脅威

インターネットが通信や取引に日常的に利用され、人々の生活や企業活動の道具として定着している。その一方で、インターネットを不用意に利用すると様々な問題を引き起こすことから、個人や企業は安全性を確保するために必要な対策を講じることが要請され、また、その負担も含めてインターネットの価値を評価すべきことも認識されるようになっている。

では、どのような問題がありうるのだろうか。店頭での売買のようなインターネットによらない取引等と対比して具体的に考えてみる。

まず、個人が店に出向いて買い物をする場面を考える。買い物客は現金やカードで代金を支払い、それと引き換えに商品を受け取るので、客も店も取引に関して特に不安を持たない。また、従来の企業間の商取引においては、契約書は取引相手から郵送されてくる。契約書には代表者の捺印(押印)があるのでそれが真正のものであると分かるし、印鑑証明書も添付されていれば、その印に関して第三者による証明も得られる。これらの例は、当事者同士が直接に対面し、あるいは紙を媒体として行う、従来の形の取引である。

これに対して、インターネットによる通信や取引では、状況が異なる。インターネット・ショッピングでは、個人は自宅にいながらパソコンに表示される商品を選択し、やはりパソコンを操作して自分の銀行口座から代金の振り込み指示をすることもできる。しかし、店員と顔をあわせるわけでもなく、客は商品が確かに届くかとの不安を持つこともあるだろう。また、店の立場では、商品を先に発送すると不払いを心配しなければならない。

企業間の電子商取引においては、例えば、契約書や取引明細が電子的な文書ファイルの形で電子メールに添付されてくる。そして、不特定多数の人が利用するインターネットを媒体とする限り、これが本来の相手方から送付された真正の文書であるとの確証は持てない。誰かが悪意を持って偽の電子文書を送りつけているのではないか、という懸念がどうしても残るのである。

オープンなネットワークに依存して相手と対面せず、取引に時間差があり、また紙と印

鑑も使わないことが、インターネットの利用で問題を生じうる理由である。利用者である個人や企業にとって避けられない脅威が、問題の原因となりうる。

1.2　脅威の種類と対策

様々な脅威の中で、本ガイドラインでは、通信や取引における不正という観点からの脅威を採り上げる。これには、次の３種類がある。

- なりすまし

  他人になりすまして不正な通信や取引を行うこと。

- 改ざん

  通信や取引の内容を不当に変更すること。一方の当事者が相手方から受信した情報を変更したり、第三者が変更したりする場合が考えられる。

- 否認

  通信や取引を行った後に、その行為をしたこと自体を否定する不正行為。送信者による送信の否認と、受信者による受信の否認がある。事後否認とも呼ぶ。

不正につながるこれらの脅威への対抗策の一つが、電子署名である。特に、電子署名の利用にあたり利用者が留意すべき事項と、電子署名を行うソフトウェアの開発者向けの留意事項が、本ガイドラインの主題である。

本ガイドラインの範囲を明確にするために、関連する脅威のうち、本ガイドラインでは対象としないものにも触れておきたい。

代表的なものは、盗聴である。通信や取引の内容を第三者が知る脅威で、個人のプライバシーの侵害や、企業秘密の暴露につながるものである。盗聴への対抗策は、情報の暗号化である。第三者が情報を盗んでも、暗号化されていれば解読されない。対抗策として利用する技術が共通であることから、盗聴は、先に挙げたなりすまし、改ざんおよび否認とあわせて採り上げられることが多い。しかし、通信や取引における不正に直ちにつながるものではなく、本ガイドラインでは盗聴とその対策は対象に含めていない。

ハッカーがインターネットから個人や企業のコンピュータに侵入し、データを破壊するなどの脅威も重要であるが、これも他の報告や書物に譲る。また、システムやサービスが利用したいときに利用できるという観点からの指標は、信頼性である。これも利用者の重要な関心事であるが、本ガイドラインでは扱わない。

2　電子署名の効果

電子署名は電子文書の通信に適用される仕組みであり、契約書等を紙でやりとりする場合の捺印と同様の効果を持つ。電子署名は、送信側で作成されて本文とあわせて転送され、受信側で正当性の確認を受ける。電子文書に対する送信側と受信側におけるこの処理は、書類の作成者が書類に捺印し、受領者が印影を照合する手続きと似ている。

2.1　電子署名の役割

電子署名は、通信や取引の安全性確保を目的として電子文書に付加される電子的な情報であり、次の働きをする。

- 通信の途中などで電子文書が改ざんされた場合に、その事実を受信側で検出する（改ざんの検出）。
- 受信側で情報の送信者を特定する（なりすましの防止、否認の防止）。

すなわち、電子署名は、紙の文書における印影と同様の効果を持つのである（図-Ⅰ-2-1）。

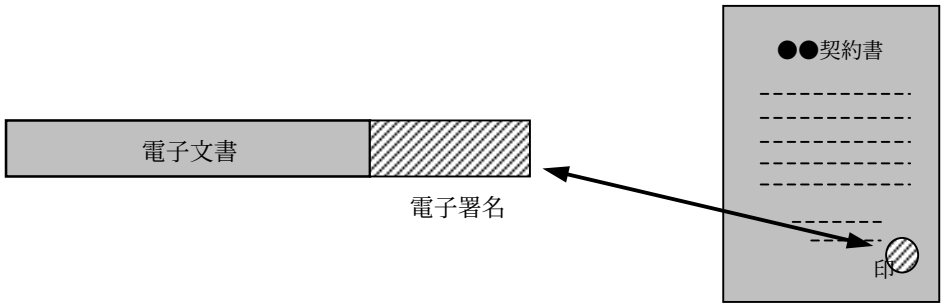

図-Ⅰ-2-1　電子署名と印影

電子署名が印影と対比できることから、その利用における留意事項も、捺印に対応づけて考えることができる。重要な契約書などの文書に捺印をする場合に、何に留意するだろうか。契約の内容に応じた責任と義務を負い、また権利を確保することを意識して、内容をよく確認した上で捺印する。このことは、インターネットの利用においても同様である。個人や企業の担当者が電子署名を行う際には、送信する情報の内容をよく承知していることが求められる。電子署名により、その情報に関する自身の責任と義務ならびに権利を表

明することになるからである。

このような意味を持つ電子署名に関して、法律の整備も進められている。電子署名に関連する法律として、『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）』があり、平成１３年４月 1 日から施行される。通称「電子署名法」である。この法律においては、「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」とされており、技術的に安全性を確保する仕組みである電子署名が、法的にも印影と同等の効力を持つものとなるのである。

ただし、電子署名の効果が相手方や第三者から認められるためには、電子署名を行うパソコンやソフトウェアが適正に管理されていることが前提となる。すなわち、自身の電子署名を有効なものとするには、他人が勝手にパソコンを使って電子署名を悪用し得るようなパソコンの管理は適切とは言えない。また、安全性が確認されたソフトウェアを利用することも重要である。これは、印鑑の管理にも対比できるものである。本ガイドラインでは、電子署名の利用に関するパソコン等の安全な管理の内容を具体的に示す。

「電子署名」という用語は、狭義および広義の用法がある点に注意する必要がある。本ガイドラインでは、電子署名を狭義に用いている。これに対して広義には、指紋や手書き署名を電子的に扱い署名のはたらきを持たせることも、「電子署名」に含める。これらを区別するために、広義の電子署名に対する狭義の用語として「ディジタル署名」を用いることも多い。

また、本書では電子署名を署名とも呼ぶ。

2.2　署名生成とは

電子署名は、送信する情報に対してある計算を施すことにより作成される情報である。例えば送信情報が

認証・公証ＷＧ

であれば、その電子署名は計算の結果

07ab 5f16 879d b738 2491 76b4 10ef 77cd
b3e8 b574 cdb2 0cf8 d5c4 7ab2 7e1f d5a5
0980 4868 8044 76f2 8a93 0705 f3ae fe50
d709 42f9 f42f 8caf 9431 3b0c 421d 2fdd
de6d f809 9bbc 52f2 cc27 ff1f 14a0 2851

4bbc bcf7 aead 250f 54f0 3995 d9d2 0ed4

8d7b 3f6a 4bdc 6005 72d0 2537 6837 322c

ca6f ecf3 52ec 3f75 8c96 caf9 d925 7db0

などとなる。普段われわれが使う単語や文とは異なる記号である。

電子署名は、ソフトウェアやハードウェアが計算をして作成する。計算を実行し、その結果である電子署名を元の電子文書に規定の形式で付加することを、署名生成と呼ぶ。この計算は複雑なものであるが、利用者は、その計算式の詳細を知る必要はない。機械的あるいは電気的な仕組みを知らなくとも自動車が運転でき、家電製品も活用できるのと同様である。

では、電子署名は、利用者から見てどの時点でなされるのだろうか。パソコンのメール用ソフトウェアで、「署名」ボタンを持つものがある。これを選択すると、メールの送信時に電子署名が生成され、電子メールに付け加えられる。また、電子商取引に専用のアプリケーション・プログラムでは、利用者がパソコンの画面上で「署名」を指示するのではなく、あるデータの送信や回送を行う際には常にその利用者の署名を付加するようにできているものも多い。いずれの場合にも、電子署名は前述のように紙の文書への捺印に相当するものであり、電子署名を付加する署名生成の操作は捺印と同様の意味を持つことに十分に留意する必要がある。

なお、電子文書に対する電子署名と、電子文書の内容の秘匿を目的とした暗号化を区別することが重要である。電子商取引用のアプリケーション・プログラムで例えば通信を安全に（セキュアに）行う、との選択ができるものもある。これは、通信の暗号化の要否を選択するものであり、電子署名の利用有無ではないことが多い。

2.3　署名検証とは

次に、電子署名が付加された電子文書（署名付き電子文書）を受信する場合を考える。

受信した電子署名に対して送信側で行った署名生成とは逆の計算を行い、その計算結果が受信した本文と同一であることを確認することにより、データに対する改ざんがないこと、また送信者が意図した相手であることを確認できるのである。（実際の計算手順を簡略化して説明している。）

この計算を行い電子署名を確認することを、署名検証という。署名検証により受信情報の正当性が確認できるので、受信側の当事者は、不正な取引による被害などを防ぐことが

できる。署名検証は、紙と印鑑を用いる従来の取引における印影の照合に対応する手続きである。

前節で述べた署名生成と同様に、署名検証の計算も電子メールや電子商取引用のソフトウェアが行う。ここでも、利用者は計算式や技術の詳細を知る必要はなく、署名検証の結果がそのソフトウェアから通知される。署名検証に失敗した場合、すなわち安全性が確認できなかった場合には、送信者や取引内容のどこかに疑念があるので、利用者は、その取引を中止すべきであると分かるのである。

3　電子署名の仕組み

3.1　電子署名の仕組み

前章では、電子署名とは、署名対象となる電子文書に対してある計算を行うことによって生成されたものであることを説明した。本章では、その仕組みについてもう少し詳しく説明する。

電子署名を生成する際の計算には、電子文書に加えて、「秘密鍵」と呼ばれる情報も利用する。電子文書を入力として秘密鍵で加工した結果が電子署名である。一方、電子文書と電子署名が伝達されると、受け取り側では署名検証を行う。署名検証では、「公開鍵」と呼ばれる情報を利用して電子署名に対して計算を施し、この計算結果と元の電子文書とが一致しているかどうかを確認する。

より技術的には、電子署名は、公開鍵暗号方式を用いて実現される。公開鍵暗号方式では、電子文書を暗号化する際に使用する鍵と暗号文を復号する際に使用する鍵とが異なる。公開鍵暗号方式の利用者は、どちらか一方の鍵を広く一般に開示し、もう一方の鍵は秘密に保管しておく。前者が公開鍵であり、後者が秘密鍵である。この公開鍵と秘密鍵とは１対１対応であって、どちらか一方の鍵で暗号化した情報はもう一方の鍵でしか復号できない。また、公開鍵から秘密鍵を算出することも非常に困難となっている（つまり、正しい秘密鍵を知っているのは利用者本人だけである）。

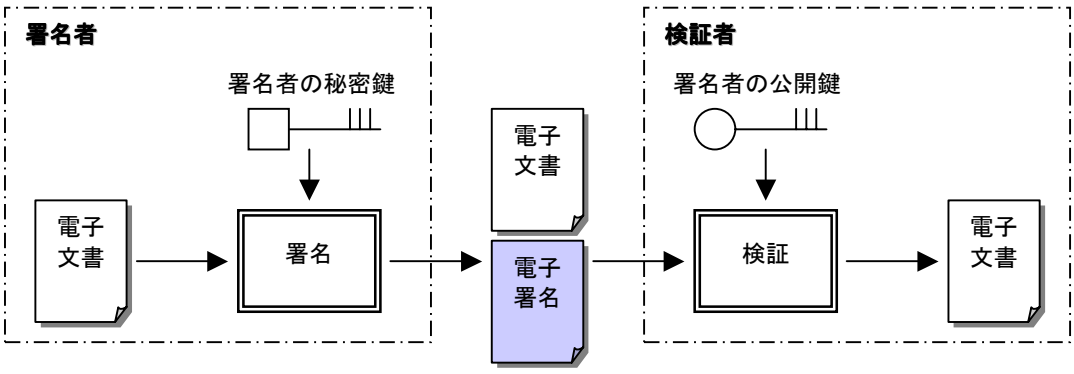

図-Ⅰ-3-1 電子署名の仕組み

図-Ⅰ-3-1は、電子署名の仕組みの具体的な例である。ある電子文書に対して署名者（電子文書に対して自己の電子署名を付与する利用者）が電子署名を付け、それを検証者に送

る場合、署名者は自分の秘密鍵で情報を暗号化し、電子文書と暗号文（電子署名）とを組にして検証者に送る。検証者は、受け取った電子署名を署名者の公開鍵で復号し、その復号結果と署名者より受け取った電子文書とを比較する。もし、それら２つのデータが一致していれば、受け取った電子署名は署名者の秘密鍵で暗号化されていることになる。前記のとおり、署名者の秘密鍵を知っているのは署名者本人しかいないはずなので、検証者は、当該署名者が署名したということ、および電子情報が何ら改ざんされていないということを確認することができる。しかし、一般に公開鍵暗号方式には処理速度が遅いという欠点がある。そのため、実際に電子署名を行うときには、予め電子文書を一定の大きさまで圧縮し、その圧縮結果に対して署名するようにする。この圧縮方法をハッシュ関数、ハッシュ関数の出力結果であるビット列を、ハッシュ値、あるいはメッセージダイジェストなどと呼ぶ。

このような電子署名は、

- 秘密鍵を安全に管理しておけば、第三者が電子署名を偽造することはできない。
- 電子文書と電子署名とは１対１対応であり、別の文書と組にしても比較時に一致しないため不正を検出できる。
- 正しい電子署名を作ることができるのは署名者本人しかいないので、電子文書と電子署名の組を保管しておけば、当該署名者は署名事実を事後否認できない。

などといった特性を備えており、ネットワークを介して離れた相手と通信したり取引を行ったりするようなシステムにおいて、安全性を確保するための重要な技術の一つとなっている。ただし、電子署名を適切に利用するためには、署名者が自己の秘密鍵を他人に知られたり、無断で使われたりしないようにきちんと管理することが必要である。

秘密鍵や電子署名などと従来の印鑑などとの対比を表-Ⅰ- 3-1に示す。

表-Ⅰ- 3-1 秘密鍵と印鑑との対比

秘密鍵	印鑑
電子署名	文書に付された印影
署名生成	捺印
署名検証	印影照合
公開鍵	印影照合のための正しい印影
秘密鍵の安全な管理	印鑑の安全な保管

3.2　電子署名の利用環境

本ガイドラインで想定している電子署名の利用環境を図-Ⅰ- 3-2に示す。図-Ⅰ- 3-2も含め、公開鍵暗号を利用して各種情報通信システムの安全性を確保するための一連の技術およびサービスをＰＫＩ（Public Key Infrastructure）と呼ぶ。

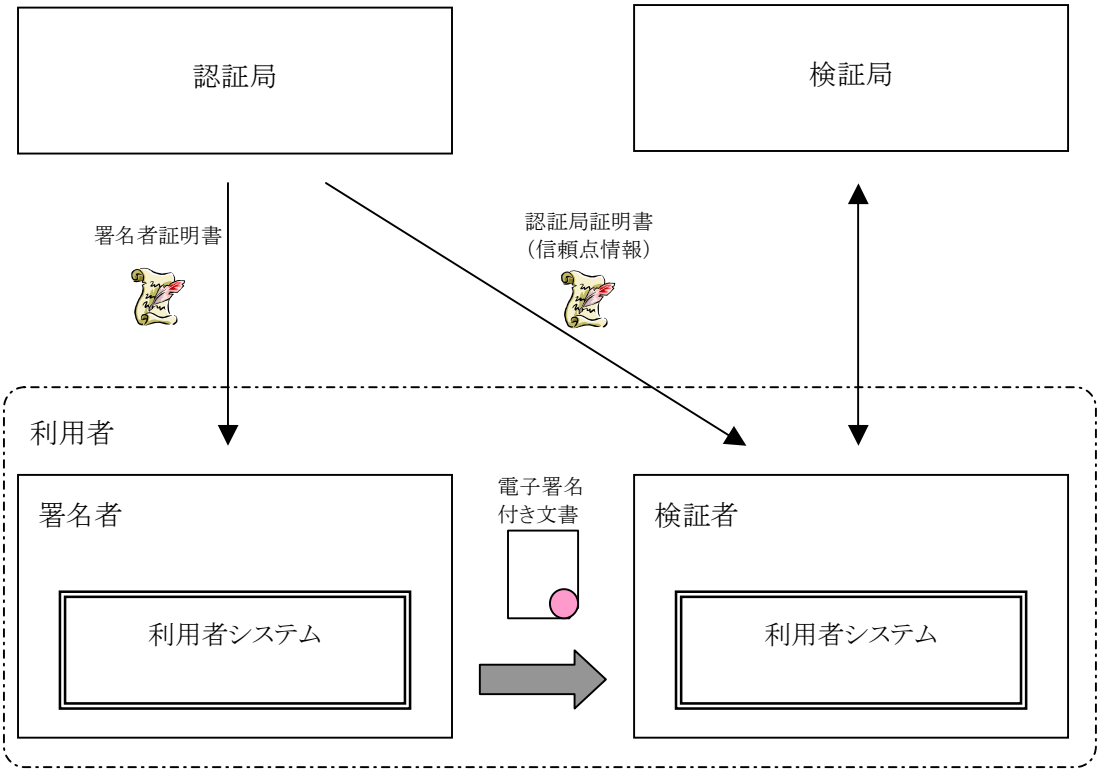

図-Ⅰ- 3-2 電子署名利用環境の全体

3.2.1　証明書と認証局

電子署名の検証においては、署名者の公開鍵を用いるため、検証者は署名者の正しい公開鍵を知っていることが必要である。

例えば、不正者Ｃが利用者Ａになりすまそうとする場合を考える。まず、不正者Ｃは「自分が利用者Ａである」と詐称すると共に、使用する公開鍵と秘密鍵の組を生成し、その公開鍵を「自分(利用者Ａ)の公開鍵だ」と偽って提示する。次に、その公開鍵に対応した秘密鍵で電子文書に署名し、それを利用者Ｂに送る。利用者Ｂが、不正者Ｃが開示した偽の公開鍵を利用者Ａの公開鍵だと考え、その公開鍵で署名の検証を行うと、不正者Ｃを利用者

Ａだと誤認してしまうことになる。このように、電子署名を利用するシステムでは、各利用者とその利用者の公開鍵との対応関係がきちんと保証されていなければならない。

このような不正を防ぐために、認証局（ＣＡ：Certification Authority）と呼ぶ信頼できる第三者機関（ＴＴＰ：Trusted Third Party）を利用する認証の枠組みが、国際電気通信連合（ＩＴＵ）の勧告Ｘ．５０９で規定されている。認証局とは、公開鍵とその所有者とを対応づけるために証明書（Certificate）と呼ぶ電子データを発行する機関である。認証局では、各利用者から証明書の発行依頼を受けた場合に、それら利用者の本人確認を行った後、正しい利用者からの依頼であった場合にのみ証明書を発行する。認証局が発行した証明書には所有者の識別情報や公開鍵などが記載されており、それらの情報に認証局が電子署名を施すことによって第三者が改ざんできないようになっている。

これにより、認証局の正しい認証局証明書（信頼点情報）だけを事前に入手しておけば、当該認証局が発行した証明書をもつ全ての利用者を認証することができる。このようなやり方は、市役所が印鑑証明書を発行することによって個人の印鑑が本物であることを保証しているのと同じ考え方に基づくものである。ただし、印鑑証明書とは異なり、証明書には有効期限（印鑑証明書自体には有効期限はないが、受取手が発行日（例えば、３ヶ月以内に発行されたもの等）を指定する場合が多い）がある。

以上のように、認証局証明書は、署名者証明書の正当性を確認する上での信頼の要となっている。そのため、検証者が信頼する（署名者証明書の正当性を確認する際に使用する）認証局証明書を信頼点、または信頼点情報と呼ぶ。検証者は、当該認証局が信頼するに足るものであるかを判断するために、認証局によって公開される認証局運用規定（ＣＰＳ：Certification Practice Statement）と呼ばれる、認証の実施における手続きや遵守事項等を文書化したものなどを参照することが求められる。

3.2.2　証明書の有効性と検証局

証明書は、それに対応する秘密鍵の紛失などの理由により、有効期限内であっても失効（無効化）されることがある。そのため、証明書を用いて署名検証を行う場合、当該証明書がその時点で失効されているかどうか（証明書の有効性）を確認する必要がある。証明書が失効されているかどうかを確認する方法としては、当該証明書が、認証局が発行する証明書失効リスト（ＣＲＬ：Certificate Revocation Lists）に記載されているかどうか調べる方法や、検証局（ＶＡ：Validation Authority）と呼ばれる第三者機関にオンラインで問

い合わせる方法などがある。この検証局への問い合わせには、ＯＣＳＰ（Online Certificate Status Protocol）等が利用される。そのため、検証局のことをＯＣＳＰ Responder と呼ぶこともある。

3.2.3　利用者システム

本ガイドラインにおいて、利用者システムとは、ＰＫＩ技術に基づく電子署名を利用する利用者（署名者ならびに検証者）が、電子署名の生成あるいは検証を行うために用いるシステムであって、アプリケーションと署名プログラムとからなる。

4　電子署名の安全性とは何か

利用者が利用する証明書を発行する認証局が安全性確保のために種々のセキュリティ対策を実施することはもちろん重要であるが、利用者が自分の秘密鍵と利用者システムを用いて電子署名する場合、また他人の証明書等と利用者システムを用いて電子署名の検証を行う場合も、安全性を確保するために種々のセキュリティ対策を実施することが重要である。

本章では、利用者システムにおいても安全性確保が必要であり、そのために種々のセキュリテイ対策を実施することが重要であることを示す。また、そのセキュリティ対策は、利用者による運用面の対策と、利用者システムの処理系におけるセキュリティ対策の両面の対策が重要であることを示す。

4.1　署名生成と署名検証の安全性

利用者が自分の秘密鍵と利用者システムを用いて電子署名する場合、また他人の証明書等と利用者システムを用いて電子署名の検証を行う場合、例えば次のような脅威が想定される。

- 署名生成時

(1) **署名が可能な状態で自席を離れた隙に、他人が自分になりすまして不正に署名する。**

(2) **利用者システム及び秘密鍵を使用可能にするための認証情報（パスワード等）を書き留めたメモを見た人が、自分の利用者システムにアクセスし、自分になりすまして不正に署名する。または、認証情報が類推されやすいものであったために他人に認証情報を見破られ、他人が自分の利用者システムをアクセスし、自分になりすまして不正に署名する。**

(3) **利用者システムのハードディスク上の秘密鍵を、知らない間に他人にコピーされた。（ネットワークを介してか、席を離れた隙にか、またはコンピュータを修理に出している間にコピーされた。）あるいは、秘密鍵を格納してあるＩＣカードを盗まれた。このような場合でかつ、上記のように他人が認証情報を知り得た場合、他人が別のコンピュータから自分になりすまして不正に署名する。**

- 署名検証時

(4) **利用者システムが適切でないために、署名検証エラーになるべきケースに署名検証が成功してしまう。あるいは逆に署名検証が成功すべきケースに署名検証エラーに**

なってしまう。（つまり、信頼してはいけないものを信頼し、信頼すべきものを信頼しないという問題が起こる。）

ここで、利用者システムが適切でないケースとして、例えば利用者システムを構成するソフトウェアが不適切であったり、証明書の最新の失効情報をオンラインで入手できる環境設定でなかったり、コンピュータの日時設定が正しくなかったりするケースが想定される。

利用者システムで署名生成又は署名検証する場合、これらの脅威を始めとして種々の脅威が想定されるので、利用者システムにおいても安全性確保が必要であり、そのためにいくつかのセキュリテイ対策を実施することが重要である。

そのセキュリティ対策は、セキュリティ対策を実施した信頼できるソフトウェア及びハードウェアで利用者システムを構築するだけでは十分でない。利用者による運用面のセキュリティ対策が併せて重要である。セキュリティ対策は、物理的設置環境、ネットワーク環境、運用管理などに亙って、トータルなセキュリティ・システムとして対策を講じることが肝要である。

以下の節で、利用者による運用面の対策と、利用者システムの対策について示す。

4.2　利用者システムの安全な運用

利用者システムの利用者が運用面で実施すべきセキュリティ対策として、例えば次のような対策が必要である。

(1) **離席時には、利用者システムからログアウトするか、利用者システムをシャットダウンする。秘密鍵をＩＣカードに保管・使用している場合には、そのＩＣカードを携行する。**

(2) **利用者システム及び秘密鍵を使用可能にするための認証情報（パスワード等）はメモせずに暗記する。あるいは、書き留めたメモを安全に管理するか携行する。他人から何らかの理由で教えてくれと言われても、認証情報は教えない。また、認証情報は、類推されにくいものにする。**

(3) **自分の大切な秘密鍵を保管・使用する媒体は、耐タンパ媒体（ＩＣカード等）を採用することが望ましい。**

(4) **利用者システムを構成するソフトウェア及びハードウェアは、セキュリティ対策が**

実施された信頼できる製品を採用する。また証明書は、信頼できる認証局から発行してもらう。

(5) **利用者システムのコンピュータの日時を正確に設定する。**

利用者システムの利用者が運用面で実施すべきセキュリティ対策としては、これらの対策を始めとしていくつかの対策が必要である。電子メールとインターネット・ショッピングをモデルケースとした対策を、第Ⅱ部「個人による電子署名の利用」に示すので参照されたい。また、企業間電子商取引システムをモデルケースとした対策を、第Ⅲ部「企業における電子署名の利用」に示すので併せて参照されたい。

4.3　安全性の高い利用者システムの実装

利用者は、利用者システムを構成するソフトウェア及びハードウェアとして、セキュリティ対策が実施された信頼できる製品を採用する必要がある。利用者システムを構成するソフトウェアは、鍵管理機能、署名生成機能及び署名検証機能等を実現する「署名プログラム」と、署名プログラムを利用する「アプリケーション・プログラム」とに大別されるが、それぞれに対してセキュリティ対策が必要である。

署名プログラムを提供する開発者が実施すべきセキュリティ対策として、例えば次のような対策が必要である。

(1) **利用者の認証**

利用者が本人であることを確認するための認証情報を用いて、利用者認証を行い、利用者認証が成功しないと署名プログラムを利用できないようにする。

(2) **データ保護（暗号化と改ざん検知）**

秘密鍵や利用者認証情報を固定ディスク上のファイルとして保管する場合は、暗号化して保管するとともに、改ざん検知可能な仕組みのもとに保管する。

また、秘密鍵や利用者認証情報は、ファイルとして保管できるだけでなく、耐タンパ媒体（ＩＣカード等）に保管して利用できるようにすることが望ましい。

(3) **十分な強度を有する暗号アルゴリズムと鍵長の使用**

十分な強度を有すると評価されている暗号アルゴリズムと鍵長を使用可能とする。

また、アプリケーション・プログラムを提供する開発者が実施すべきセキュリティ対策と

して、例えば次のような対策が必要である。

(4) **再確認するユーザインタフェース**

利用者の指示に従って秘密鍵や利用者認証情報の、変更、削除等を行う際には、実行して良いかどうかを問い合わせるユーザインタフェースによって、利用者に再確認した上で実行する。

安全性の高い利用者システムを実現するためには、署名プログラム開発者及びアプリケーション・プログラム開発者が、これらのセキュリティ対策を始めとして種々の対策を実施する必要がある。署名プログラム開発者及びアプリケーション・プログラム開発者が安全性の高い信頼される製品を開発するためのセキュリティ対策指針を第Ⅳ部「電子署名利用者システム開発の指針」に示すので、参照されたい。利用者は、安全性の高い利用者システムを構築するために、この指針に適合するソフトウェアを採用することが望ましい。

5　電子署名の利便性とは何か

電子署名および署名システムに関連する利用者・システム管理者は、セキュリティを侵害するような操作を行わないように、誤操作の防止と、簡易な操作で利用者が目的の操作を遂行できるという利便性が充分に考慮されているシステムを利用することが望ましい。

5.1　誤操作の防止

利用者が要求する操作が引き起こすセキュリティ上の影響範囲を明白に利用者に通知することが必要である。このためには電子署名システムとして以下の対策をとらなければならない。

(1) 適切な操作ガイドライン文書

利用者を、一般利用者やシステム管理者など対象者ごとに分類し、それぞれの操作によるセキュリティ上の影響範囲を明示する文書（オンラインマニュアルを含む）を提供しなければならない。電子署名生成・検証システムにおいては、署名操作をするためにどのような操作が必要かを明示し、また検証システムにおいては、署名検証のための操作を明示する必要がある。これらの操作のための管理操作（信頼点の追加や、利用者の登録など）についても、セキュリティ上の影響範囲を明示したガイドライン文書を提供すべきである。これらによって、利用者が知らずにアンセキュアな状況に陥ることを防ぐ。

(2) 適切で容易に理解できる表現による表示

利用者に対して、提供する情報については、適切で容易に理解できる表現が望ましい。例えばエラーメッセージなどを表示する場合は、エラーの原因やその後の対応方針を利用者が容易に理解できなければならない。電子署名生成・検証システムにおいては特に、認証局の信頼性についての情報を簡単に知ること、証明書の内容について利用者が理解できることが必要とされる。

5.2　簡易な操作

一般に簡易な操作（運用）はセキュリティの維持と相反関係にあるとされる。しかしながら、特に一般利用者は、ＰＫＩ技術について深い知識を持たない場合が多く、従ってセキュリティを維持しつつ可能な限り簡易な操作を提供しなければならない。このためには電子署名システムとして以下の対策をとらなければならない。

(1) ワンタッチオペレーション

複数の機能を一度の操作で実現可能であるものをまとめること。署名検証については望ましい。ただし、署名生成については、利用者の署名意思の確認などが必要となるため、本操作を提供しないほうが望ましい

5.3　その他の利便性に関連する対策

電子署名システムにおけるその他の利便性対策については、利用者にストレスを感じさせない性能、汎用性（多様な業務への対応）などがある。

6　本ガイドラインで扱うアプリケーション

本ガイドラインでは、電子署名を利用する様々なアプリケーションの中から、安全対策や利便性を検討する上で典型的であると考えられる個人間の電子メール、インターネット・ションピング、および企業間電子商取引を採り上げる。

6.1　多様なアプリケーション

電子署名を利用する様々なアプリケーションは、いくつかの側面から分類できる。

(1) 個人的、私的な利用と、ビジネスあるいは公的な利用の分類

- Ｃ to Ｃ (consumer to consumer)

  個人間の私的な電子メール利用、コンテンツ配信、インターネット・オークションなどである。

- Ｂ to Ｃ (business to consumer)

  インターネット・ショッピング。商品展示・選択、注文、支払いのすべてをインターネット上で行う方法や、支払いは店頭で商品と引き換えに行う方法など、いくつかの方式がある。また、音楽や画像など商品も電子情報として表現できるものは、商品配送もインターネットで行う。

- Ｂ to Ｂ (business to business)

  企業間電子商取引。部品や原材料を調達する企業が中心になる形態や、供給する企業が中心となる形態、あるいは、貿易業務など特定の業務を関係する企業が電子化する形態などがある。

- Ｇ to Ｃ (government to consumer)、Ｇ to Ｂ (government to business)

  政府や自治体に対する申請・届け出、許認可、調達・応札などである。

インターネットや電子署名を導入する場合には、安全性や前提となる技術についてある範囲の知識が必要である。一般に、ビジネスあるいは公的な利用の場合には、その組織の中に専門の部署を置き、そこで前提知識を持つこともできる。これに対して、個人には前提知識を多く期待することはできない。本ガイドラインでは、前提知識に関する相違を意識して留意事項等を整理している。

(2) 取引金額や価値の大きさによる分類

取引金額や価値が大きければ、不正取引に伴う損害も大きい。従って、安全策により多くの費用を投じることが合理的である。

(3) 機器による分類

- 個人のパソコン
- 個人の携帯電話
- 街頭のＫＩＯＳＫ端末
- 企業内のパソコン
- 行政機関のパソコン　など

機器により、電子署名に関するソフトウェアの環境が、安全性の観点から異なる。従って、とるべき対策も異なるものとなる。

6.2　本ガイドラインで扱う事例

前節にあげた多様なアプリケーションの中から、本ガイドラインでは代表的と考えられる３種類のアプリケーションを題材としている。

- 個人間の電子メール
- インターネット・ショッピング
- 企業間電子商取引

これらを通して、利用者が安全性確保のための技術的知識を持つ場合と持たない場合の両方を検討する。また、企業であればその内部で専門知識を持たないエンドユーザとそれを持つシステム管理部門があり、これらを区別して検討する。また、不正による影響の大小も異なる。一般には、企業では高額な、あるいは信頼関係の基本に係わる取引を行うので、個人よりもはるかに多額の安全対策投資を行う必要があり、それが可能でもある。

特徴の異なる３つのアプリケーションについてそれぞれ適切な留意事項と安全対策を検討することにより、様々な他のアプリケーションにも応用でき、留意事項と安全対策が読み取れるガイドラインを目指している。

第Ⅱ部　個人による電子署名の利用

本ガイドラインでは、代表的なアプリケーションとして、３つのアプリケーションを取り上げているが、第Ⅱ部では、その内の２つ、個人間の電子メール及びインターネット・ショッピングを例題として記述する。

第Ⅰ章は、「電子メール」利用時の利用場面及び利用手順について、

第Ⅱ章は、「インターネット・ショッピング」利用時の利用場面及び利用手順について、

第Ⅲ章は、両方のアプリケーションに共通する個人による電子署名の利用にあたっての「留意事項と安全対策」について記述している。

1　電子メール

電子メールは、基本的に 1 対 1 の通信であるが、プライバシー確保や差し出し人、受取人が郵便ほど、確実に保証されているわけではない。インターネットの特性から、メールの内容を盗み見られたり、その内容を書き換えられたり、また、送信者、受信者の本人性（なりすまし）等を心配しなければならない。そこで、情報の真正性（改ざんされていないこと）の保証や差し出し人の証明等の機能を有した電子署名が必要となる。

本章では、個人による電子メール利用者が電子署名を利用することを想定し、署名をすることの意味や方法、署名付文書を受け取ったときの対処方法、また署名のための秘密鍵、証明書の管理方法等について、利用場面、利用手順の観点から記述している。

電子メールに対して電子署名を行える市販ソフトウェア群をここでは広くセキュアメールと呼ぶ。図-Ⅱ- 1-1にセキュアメールのシステム構成例（概念図）を示す。

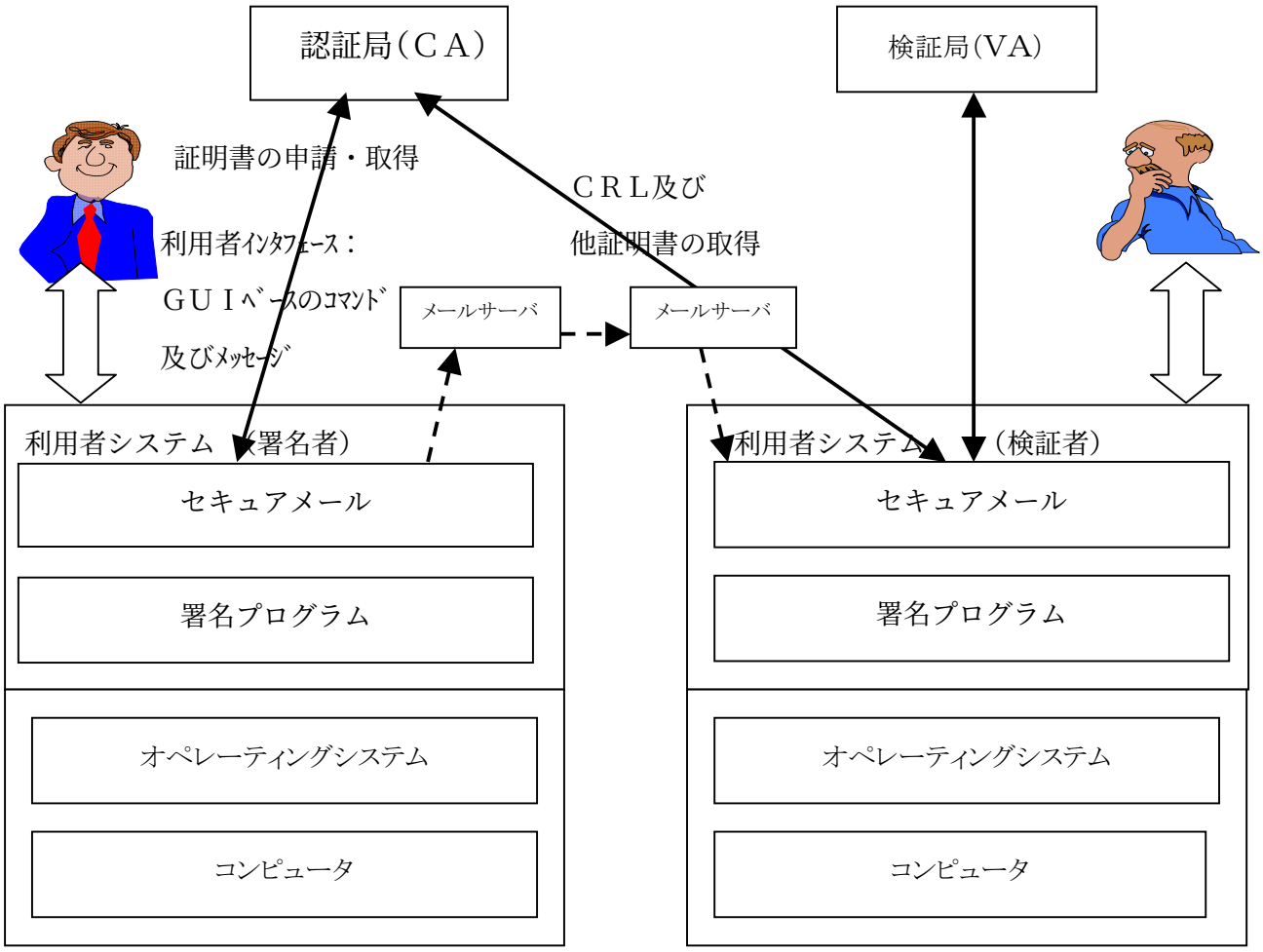

図-Ⅱ- 1-1　セキュアメールのシステム構成例(概念図)

図-Ⅱ- 1-1セキャメールのシステム構成例（概念図）は、認証局については、単一認証局を想定して一個としているが、複数の認証局に亙って複数存在する場合もありうる。また、通信には、一般にインターネットを利用することを想定し、ファイアウォール等のネットワーク構成については省略している。

1.1　利用場面

個人による電子メール利用者が、セキュアメールを利用して署名・検証を行う場面には以下の様なケースが考えられる。

セキュアメール利用者が電子メールに署名を行う場合

- 利用者が送信する電子メールの真正性を証明する。
- 利用者が送信する電子メールが利用者自身から送信されたことを証明する。

セキュアメール利用者が電子メールの署名の検証を行う場合

- 利用者が受信した電子メールの真正性を確認する。
- 利用者が受信した電子メールが送信者として名乗っている本人から送信されたことを確認する。

1.1.1　署名の対象

電子メールが署名対象となる。特定の個人が作成したこと、内容が改ざんされていないことを証明したい電子メールについて署名を付ける。また、電子メールの添付ファイルへの署名も対象とする。

1.1.2　利用アプリケーション

利用アプリケーションとしては、セキュアメールに対応したメールソフトウェアを利用する。電子署名に使用する秘密鍵の生成、証明書の申請及び取得、署名の生成、検証等の基本機能を有するものとする。

1.1.3　証明書の発行者

証明書の発行者には、セキュアメール利用者が署名付き電子メールを交換する利用者間

で、共通に信頼できる同一の認証局の場合とお互いに異なる認証局の場合がある。

なお、後者の利用形態においては、利用時にお互いの証明書が信頼して利用できるか否かを確認する必要がある。信頼して利用可能な場合は信頼する認証局とすることで、署名の検証が可能となる。

1.1.4　認証対象

セキュアメール利用者個人が認証の対象となる。

1.1.5　鍵の生成

セキュアメール利用者が、利用に先立って秘密鍵・公開鍵ペアを生成し認証局に対して証明書の申請書を提出する必要がある。この際に作成する鍵ペアはセキュアメールに付属する鍵ペア生成ツールによって生成する。

1.1.6　署名鍵と検証

セキュアメール利用者は署名生成を行う場合には秘密鍵を使用する。また、署名の検証を行う場合は署名者の証明書を使用する。

1.1.7　鍵管理媒体

秘密鍵はセキュアメール利用者が使用するパーソナルコンピュータ（ＰＣ）のハードディスク（ＨＤ）上に格納される。秘密鍵に対しては不正使用、不正コピーなどの脅威に対するセキュリティ対策が必要である。セキュリティ対策としては、秘密鍵の暗号化とアクセス制御とする。

なお、鍵管理媒体として耐タンパ性を考慮したＩＣカード等が考えられるが、セキュアメール利用ではＰＣのＨＤ上に格納し管理されるのが一般的と考えられる。

1.1.8　鍵のアクセス管理

秘密鍵を使用する際には、秘密鍵に対するアクセスを制限するためにパスワードを設定する。パスワードの付与のルールやパスワードの管理についてはセキュリティ上十分注意する必要がある。

1.2　利用手順

セキュアメールを利用する手順例を、鍵・証明書のライフサイクルに沿って、準備、利用、廃棄の各フェーズの順に記述する。

なお、セキュアメール及びその利用手順は、本項で記述する内容以外にも想定されるが、典型的な実現例を基にした記述としている。

1.2.1　準備

鍵・証明書を保持していない利用者が、これらを取得する手順ならびにこの証明書を発行する認証局証明書を取得する手順を記述する。

1.2.1.1　証明書の申請・取得

(1) 自分で申請・取得する場合

証明書の申請・取得は、セキュアメールの証明書申請に相当する機能を使用する。認証局の選択／指定、申請項目入力、秘密鍵保護パスワード入力、鍵ペア生成のためのランダムなキーストローク（又はランダムなマウス操作等）等の操作を行うことによって、証明書の申請書を生成し、生成した申請書を認証局へ送付する。申請書の送付方法は、一般にＦＤ等の媒体に格納してオフラインで送付する方法、セキュアメールの機能に応じてオンライン（ＨＴＴＰ通信、メール通信）で送付する方法がある。いずれの方法にせよ、生成された鍵ペア、特に秘密鍵は、電子署名用の鍵として申請者本人のみ取り扱えるものとして他人に漏洩しないような厳密な管理がこの段階から必要である。 上記、秘密鍵保護パスワードの設定管理もその一つである。

認証局から電子メール等で証明書の発行通知を受け取った後、セキュアメールの証明書の取得に相当する機能を使用し、自分の証明書（及びルート認証局の証明書等一式）を取得・検証し、自ＰＣのＨＤ等の秘密鍵／証明書保管媒体に保管する。この段階で、申請時に生成された公開鍵は、公開鍵証明書として秘密鍵と対応付けられて保管される。また、公開鍵証明書は 公開鍵とその所有者(利用者)を結びつけるものであるため、証明書に記載される所有者の検証は必須である。検証の結果、所有者本人を表わしていなければ 失効及び新規発行の手順を踏むことになる。

(2) 組織から秘密鍵・証明書を配付される場合

組織が一括して認証局による公開鍵生成、証明書発行及び秘密鍵、証明書の保管媒

体（ＩＣカード等）への格納を実施するケースもある。

秘密鍵及び証明書がＩＣカードのようにポータブルな媒体に保管されている場合には不要だが、ファイルの形でＦＤに格納されている場合等では、セキュアメールの秘密鍵・証明書のインポートに相当する機能を使用し、ＦＤ中の秘密鍵及び証明書を自ＰＣのＨＤにインポートする。インポートした秘密鍵は、前述の如く厳密な管理が必要である。

(3) 他の目的で申請・取得した証明書の場合

セキュアメール利用以外の目的で、すでに秘密鍵及び証明書を取得し、かつセキュアメールを利用した電子メールへの署名を行う場合は、その秘密鍵及び証明書が利用するセキュアメールに適合するか否かを付属の説明書等で確認する必要がある。また、当該証明書を発行した認証局の認証局運用規定に記述されている証明書の使用条件等についても確認する必要がある。確認の結果、使用可能な場合は、前記（1）又は（2）による証明書の取得は不要となる。

1.2.1.2　信頼点とする証明書の登録

自分の信頼点となる証明書がセキュアメールに予め登録されていない場合には、セキュアメールから信頼する認証局の証明書登録に相当する機能を使用し、自分の信頼点となる証明書を登録する。また、電子メールをやり取りする相手のルート認証局が自分のルート認証局と異なっていても相手のルート認証局を信用する場合には、必要に応じて相手のルート認証局証明書を同様の操作で登録する。（なお、相手の認証局又は上位認証局が自分の認証局又は上位認証局と相互認証しており、かつセキュアメールが相互認証下の証明書検証機能を有している場合には、相手のルート認証局の証明書登録は不要となる。）

信頼点として良いか否かの確たる判断基準がなく、個々人が適切に判断することは難しいが、「第３章 留意事項と安全対策」の信頼点に関する記述を参照に行うことを推奨する。

1.2.1.3　証明書失効情報（ＣＲＬ）の入手

セキュアメール利用者が、署名検証に伴う証明書検証の都度、証明書発行認証局からＣＲＬをリアルタイムにリポジトリからオンラインで入手する場合もある。セキュアメールがオンラインでＣＲＬを入手可能なものならば、該当機能にそのように設定しておくのが望ましい。

1.2.2　利用

秘密鍵を使用した電子メールへの署名とその検証方法について記述する。

1.2.2.1　セキュアメールの署名生成と発信

セキュアメールの署名に相当する機能を使用して、電子メールに署名する。署名する際には、パスワード入力要求に応えて自分の秘密鍵保護対応のパスワードを入力する。最後に、電子メールの発信操作を行う。

1.2.2.2　署名付電子メールの受信と署名検証

受信した電子メールに対して、セキュアメールの署名検証に相当する機能を選択し実行する。署名検証実行後、署名検証結果（署名者及び検証の正／不正）を確認する。

署名検証において、相手のルート認証局証明書が「信頼点とする証明書」として予めセキュアメールに登録されていない場合には、「この証明書は信頼できる証明書として確認できないが、信用するか／しないか？」という趣旨のメッセージによる確認が行われることがある。

また、署名検証に伴って一般に証明書検証及び失効情報の取得がセキュアメールによって自動的に実行されるが、失効情報取得を実施する場合には、予め次のように利用者がセキュアメールに対してその方法についての設定を行う。

(1) **ＣＲＬファイル入力の場合**

定期的に又は受信した電子メールの署名検証に先立って、ＣＲＬ ファイルを何らかの方法で入手する。セキュアメールのＣＲＬ ファイル入力に 相当する機能を使用し、ＣＲＬ ファイルを入力しておく。（当ケースは、ＣＲＬ に即時性が乏しくＣＲＬ の新鮮さが問題になる可能性があるので、一般的には推奨しない。適用システムへの適合性を良く吟味する必要がある。）

(2) **ＣＲＬのオンライン入力の場合**

ＣＲＬ を署名検証に伴う証明書検証の都度、リアルタイムにリポジトリからオンラインで入手する場合には、予め準備フェーズにて記述したごとくセキュアメールにＣＲＬ をオンライン入力できるように設定しておく。

1.2.2.3　秘密鍵・証明書の更新

秘密鍵と対応する証明書は、認証局運用規定に従って（証明書の有効期限が切れる前に）定期的に更新する。また、証明書の失効に伴って、新しい秘密鍵と対応する証明書が必要になる場合もある。その際には、証明書の申請・取得と同様な手順で（ただし、更新モードで）、秘密鍵・証明書を更新する。

なお、一般には、秘密鍵を変更しないで証明書の有効期限が延長された証明書が取得できるケースや、自動的に秘密鍵・証明書の更新動作を実行してくれるケースなどもありうる。

秘密鍵・証明書の更新は、認証局の認証局運用規定に依存していくつかの方式が存在する。このことが、利用者から見ると分かり難く、運用の混乱を招きかねない。しかし利用者は、証明書には有効期限があることを認識し、証明書を期間連続的に利用するためには新たなる証明書をいずれかの方式で取得しなければならないことを念頭におく必要がある。

1.2.2.4　パスワードの管理

自分の秘密鍵保護用パスワードは自分だけの秘密にしておく。また、ある期間を経たら、適宜新しいパスワードに変更する。セキュアメールのパスワード変更に相当する機能を使用し、現行パスワード及び新パスワードを入力することによってパスワード変更する。

1.2.2.5　証明書の失効要求

秘密鍵の格納媒体（ＩＣカード等）を紛失した場合、パスワードが漏洩した場合、その他秘密鍵が危殆化した場合、利用者が自分の証明書を無効にしたい場合がある。これらの場合には、利用者から認証局に対して、自分の証明書の失効を要求する。証明書を発行した認証局の認証局運用規定に従って、オフライン又はオンラインで失効要求する。

証明書の失効要求は、現在はオフラインによる方法が一般的と考えられる。なお、オンラインで要求するためには、セキュアメール及び認証局に該当機能が装備されている必要がある。

1.2.3　廃棄

業務を終了する場合、退会する場合など、自分の秘密鍵をもはや使用しなくなった場合は、証明書を発行した認証局の認証局運用規定に従いセキュアメールの該当機能を用いて、

失効手続きを行った後、確実に自分の秘密鍵を廃棄する。（又は、ＩＣカードを運用管理者に返却して、運用管理者が一括して廃棄する。）

　また、自マシンのセキュアメール及び動作環境上から、混乱をきたさないよう、自他の証明書を削除しておくことが望ましい。

2　インターネット・ショッピング

現在、インターネットを利用したオンラインショッピングやオークションが盛んになっている。ネットワーク上で行う商取引は、店舗に出かけることの煩わしさがないことや、通信販売よりも即座に手軽に受発注できることなど優れた点が多く、今後も大いに普及するものと思われる。

しかし、相手を確認できないインターネットの取引では不安が大きく、受発注に用いる電子文書に対し信頼性を付与する必要がある。本章では、注文文書とそれに対する確認文書に対する電子署名の利用について述べる。

図-Ⅱ- 2-1は想定するショッピングの手続きを示す。

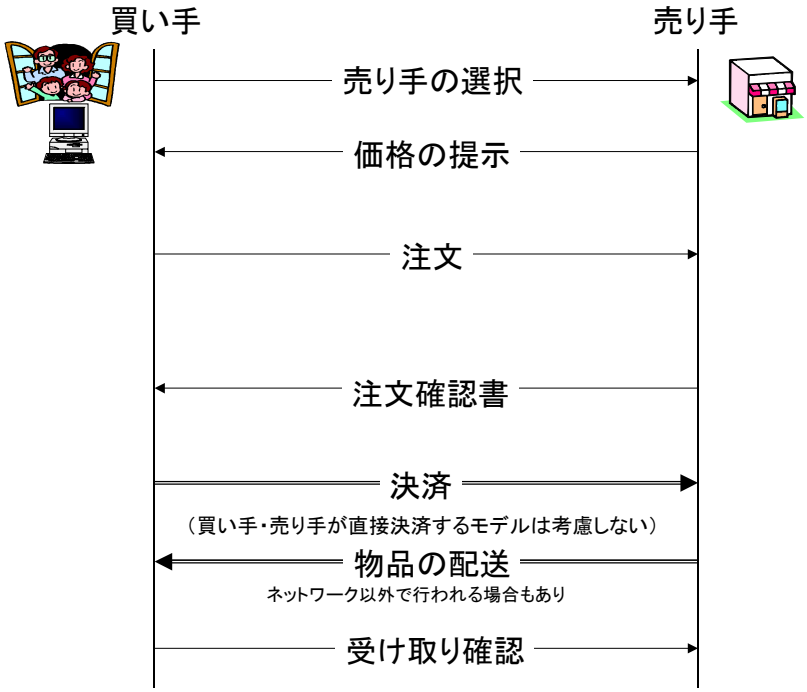

図-Ⅱ- 2-1　想定するショッピングの手続き

1. 売り手の選択

　買い手は、商品を購入する売り手を選択する。

2. 価格の提示

　売り手は、買い手に対し価格を提示する。

3. 注文

　買い手は商品を発注する。注文書が売り手に送信される。

4. 注文確認

　売り手は、注文内容を記載した確認書を買い手に送信する。

5. 決済

　買い手から売り手に代金が支払われる。方法は特記しない。

6. 物品の配送

　売り手から買い手に商品が配送される。方法は特記しない。

7. 受取確認

　買い手は、売り手に対し商品を受け取った旨を通知する。

上記の手続きのうち、「3. 注文」における買い手の電子署名と売り手の署名検証、および「４．注文確認」における売り手の電子署名と買い手の署名検証が対象になる。なお、買い手の側からすれば、簡単になりすましが可能なインターネット上においての売り手との取引は、きわめて危険である。現状のインターネット・ショッピングにおいては、ＳＳＬサーバ認証により売り手を認証し、セキュリティを確保する方法がよく用いられている。

2.1　利用場面

本章で想定するインターネット・ショッピング（注文と注文確認）においてのセキュリティ要件を述べる。

売り手の側では、以下の要件があると考えられる。

- 信頼できる買い手であることを確認できる。
- 買い手が自らの意思で注文したことを確認できる。

一方、買い手の側では、以下の要件があると考えられる。

- 信頼できる売り手であることを確認できる。
- 売り手が注文を正しく受けたことを確認できる。
- 買い手の情報が他人に漏洩することがない。

上記に対して、買い手が作成する注文書、および、売り手が作成する注文確認書に対して電子署名を行えば、以下の効果が得られる。

- 買い手・売り手が作成した注文書・確認書の真正性を証明する。
- 注文書・確認書が買い手・売り手自身から送信されたことを証明する。

このとき、受信した注文書および確認書に対し、売り手・買い手が署名の検証を行えば、上記の事象に対する確認が行える。

2.1.1　署名の対象

注文書および確認書が署名対象となる。特定の個人が作成したこと、内容が改ざんされていないことを証明するために署名を付ける。

2.1.2　利用アプリケーション

利用アプリケーションとしては、インターネット・ショッピングに対応した発注プログラム（個人）および受注プログラム（サイト）を利用する。これらのプログラムは、電子署名に使用する秘密鍵の生成、証明書の申請及び取得、署名の生成、検証等の基本機能を有するものとする。

2.1.3　証明書の発行者

証明書の発行者には、売り手・買い手が共通に信頼できるパブリック認証局の場合とお互いに信頼関係を持たない認証局の場合がある。後者の利用形態においては、利用時に信頼できる認証局か否かを確認する必要があり、信頼する認証局として登録することで、署名の検証が可能となる。また、インターネット・ショッピングでは会員制のサービス形態をとることも考えられる。この場合、認証局は売り手側から指定されるプライベート認証局となることも考えられる。

2.1.4　認証対象

インターネット・ショッピング利用者個人及びインターネット・ショッピングサイトが認証対象となる。ただし、本章では、ＳＳＬ等による相手認証については対象外である。

2.1.5　鍵の生成

インターネット・ショッピング利用者が、利用に先立って秘密鍵・公開鍵ペアを生成し認証局に対して証明書の申請書を提出する必要がある。この際に作成する鍵ペアは発注・受注ソフトウェアに付属する鍵ペア生成ツールによって生成する場合と、認証局が生成したものを配布する場合とがある。後者の場合、受注・発注プログラムに対して秘密鍵・公

開鍵ペアを登録する必要がある。

2.1.6　署名鍵と検証

インターネット・ショッピング利用者は署名生成を行う場合には個人の秘密鍵を使用する。また、署名の検証を行う場合は署名者の証明書を使用する。この時、署名者の証明書が正当なものであるか否かを検証するために、認証局の公開鍵証明書を使用する。この認証局の公開鍵証明書は、認証局同士が相互認証している場合が、複数存在する場合もありこれらを信頼点（認証局）として署名検証ソフトウエアに登録を要する。

2.1.7　鍵管理媒体

秘密鍵はインターネット・ショッピング利用者が使用するパーソナルコンピュータ（ＰＣ）のハードディスク（ＨＤ）上に格納される場合と、耐タンパ性を考慮した暗号演算付きＩＣカードが考えられる。秘密鍵に対しては不正使用、不正コピーなどの脅威に対するセキュリティ対策が必要であるが、ＰＣ利用者は不正に秘密鍵を入手できないような運用管理をすべきである。また、署名プログラムは、鍵の格納に対するアクセス制御機能を提供しなければならない。

2.1.8　鍵のアクセス管理

秘密鍵に対するアクセスを制限するためにパスワードを設定する場合は、パスワードの付与のルールやパスワードの管理についてはセキュリティ上十分注意する必要がある。ＩＣカードに格納する場合利用者は、ＰＩN(Personal　Identification　Number)の管理を責任を持って行わなければならない。

2.2　利用手順

2.2.1　準備

2.2.1.1　証明書の申請・取得

証明書の申請・取得等の手続きについては、認証局が準備する、認証局運用規定または運用規定に規定される。申請・取得については、個人で鍵生成を行い申請する場合と、組

織（サイト）を通して申請する場合（この場合鍵生成は、組織（サイト）・センター側で行われることが多い）とがある。ここでは、個人で申請・取得する手順を紹介する。

(1) 売り手・買い手側の申請・取得

証明書の申請・取得は、受発注プログラムに付随する証明書申請に相当する機能を使用する。鍵ペア生成のためのランダムなキーストローク（又はランダムなマウス操作等）等の操作を行うことによって、鍵ペアを生成し、鍵の格納時に用いる保護パスワードの設定を行う。次に認証局を選択／指定し、必要な申請項目を入力することで、プログラムにより認証局への証明書の申請書が生成され、この申請書を認証局へ送付する。申請書の送付方法は、一般にＦＤ等の媒体に格納してオフラインで送付する方法、オンライン（ＨＴＴＰ通信、メール通信）で送付する方法がある。生成された鍵ペア、特に秘密鍵は、電子署名用の鍵として申請者本人のみ取り扱えるものとして他人に漏洩しないような厳密な管理がこの段階から必要となる。 上記、秘密鍵保護パスワードの設定管理もその一つである。

認証局から電子メール等で証明書の発行通知を受け取った後、受発注プログラムの証明書の登録に相当する機能を使用し、自分の証明書（及びルート認証局の証明書等一式）を取得・検証し、自ＰＣのＨＤ等の秘密鍵／証明書保管媒体に保管する。この段階で、申請時に生成された公開鍵は、プログラム内部で、公開鍵証明書として秘密鍵と対応付けられて保管されるケースが多い。また、公開鍵証明書は 公開鍵とその所有者(利用者)を結びつけるものであるため、発行された証明書に記載された所有者を確認する必要がある。確認の結果所有者本人を表していなければ 失効及び新規発行の手順を踏むことになる。

(2) サイトから秘密鍵・証明書を配付される場合

サイトが一括してセンター側における公開鍵・秘密鍵ペア生成、証明書発行及び秘密鍵、証明書の保管媒体（ＩＣカード等）への格納を実施するケースもある。証明書発行対象である利用者は、手交、書留の信頼できる方法でその媒体を受領する。受領後、受領証へ確認のためにサイン／押印することが望ましい。

秘密鍵及び証明書がＩＣカードのようにポータブルな媒体に保管されている場合には不要だが、ファイルの形でＦＤに格納されている場合等では、受発注プログラムの秘密鍵・証明書のインポートに相当する機能を使用し、ＦＤ中の秘密鍵及び証明書を自ＰＣのＨＤにインポートする。インポートした秘密鍵は、前述の如く厳密な管理が

必要である。なお、ＦＤなどに秘密鍵が格納される場合、暗号化は必須である。

(3) 他の目的で申請・取得した証明書の場合

インターネット・ショッピング利用以外の目的で、すでに秘密鍵及び証明書を取得し、かつインターネット・ショッピングを利用する場合は、その秘密鍵及び証明書が利用する受・発注プログラムに適合するか否かを付属の説明書等で確認する必要がある。また、当該証明書を発行した認証局の運用規定に記述されている証明書の使用条件等についても確認する必要がある。確認の結果、使用可能な場合は、前記（１）又は（２）による証明書の取得は不要となる。

2.2.1.2　信頼点とする証明書の登録

自分の信頼点となる証明書（通常は自分のルート認証局の証明書）が受・発注プログラムに予め登録されていない場合には、受・発注プログラムから信頼点登録に相当する機能を使用し、自分の信頼点となる証明書を登録する。また、受・発注をやり取りする相手のルート認証局が自分のルート認証局と異なっていても相手のルート認証局を信用する場合には、必要に応じて相手のルート認証局証明書を信頼点として、同様の操作で登録する。（なお、相手の認証局又は上位認証局が自分の認証局又は上位認証局と相互認証しており、かつ受・発注プログラムが相互認証下の証明書検証機能を有している場合には、相手のルート認証局の証明書登録は不要となる。）

信頼点として良いか否かの確たる判断基準がないため、個々人が適切に判断することは難しい。第Ⅱ部 第 3 章 留意事項と安全対策の信頼点に関する記述を参照することを推奨する。

2.2.1.3　証明書失効情報（ＣＲＬ）の入手または、オンライン状態検索

受・発注プログラム利用者が、署名検証に伴う証明書検証の都度、証明書発行認証局からＣＲＬをリアルタイムにリポジトリ（一般的にはディレクトリシステム）からオンラインで入手する場合もある。また、証明書状態をオンラインで検索するサービスを提供している認証局もある。受・発注プログラムがこれらの情報を入手可能、または状態検索問い合わせが可能である場合は、該当機能にそのように設定しておくのが望ましい。

2.2.2　利用

2.2.2.1　買い手による注文

(1) 売り手を選択し、価格提示を受ける

(2) 注文する（署名付き注文書を送信する）

注文内容を確認するとともに、発注プログラムにより、「売り手が信頼する認証局から発行された公開鍵証明書と対応する秘密鍵による署名を付与すること」を通知される。発注プログラムは、利用する秘密鍵を選択するために秘密鍵に対応する公開鍵証明書（証明書・鍵にフレンドリー名をつけるか、証明書内の、明示可能な領域）等を列挙する。利用者は、選択した公開鍵証明書に対応した秘密鍵によって「注文内容に対して署名を生成」する。買い手は、売り手に対して「署名付き注文書」を送信する。

(3) 署名付き注文書を保存

利用者は、発注プログラムの機能により、事後否認での利用を考慮して「署名付き注文書」を保存する。このとき、発注プログラムは、どの鍵を利用して署名したかが判断できる情報を付加する。

(4) 「署名付き注文確認書」を検証する。

送信した「署名付き注文書」と、受信した「署名付き注文確認書」が発注プログラムにより表示され、利用者は内容に相違がないかを目視などで確認する。また、署名付き注文確認書が、売り手によって作成されたものかを売り手の公開鍵証明書によって検証する。この時、売り手の公開鍵証明書を発行した認証局の公開鍵証明書や信頼点の公開鍵証明書を利用する。

2.2.2.2　売り手による注文の確認

(1) 買い手から受注・署名の検証

予め決められた手順で相手を認証した後、署名付き注文書（受注）を受け付ける。「署名付き注文書」に付与された電子署名を検証し、買い手および注文内容を確認する。署名検証するためには、買い手に対して公開鍵証明書を発行した認証局の公開鍵証明書と、それに関連する信頼点の公開鍵証明書を利用する。また、公開鍵証明書が失効されていないか、有効期限内であるか、なども検証する。失効確認については、

オンライン確認手段がある場合は、これを利用する場合もある。検証によって、買い手本人の注文であることと、注文内容が改ざんされていないことを確認することになる。

(2) **注文確認書を作成**

買い手に対して、受注を受け付けた内容を明示した注文確認書を送付する。この時売り手の秘密鍵を利用して電子署名を生成し、「署名付き注文確認書」を作成する。

2.2.2.3　秘密鍵･証明書の更新

秘密鍵に対応する公開鍵証明書は、認証局の認証局運用規定（または実施規定）において更新手順が規定される。例えば、重複期間を設け、この期間は２種類の証明書を利用できる場合や、新証明書を利用した際に旧証明書を失効させる、など複数の方式が考えられる。これらの手順が正しく利用者に伝わることが必要で、また利用者は、証明書には有効期限が有ることを認識し、証明書を期間連続的に利用するためには新たなる証明書を取得しなければならないことを念頭に置く必要がある。

2.2.2.4　パスワードの管理

自分の秘密鍵保護用パスワードは自分だけの秘密にしておく。また、ある期間を経たら、適宜新しいパスワードに変更する。受・発注プログラムはパスワード変更に相当する機能を提供し、現行パスワード及び新パスワードを入力することによってパスワード変更を可能としなければならない。

2.2.2.5　公開鍵証明書の履歴管理

後日において、なされた署名が正当なものであるかを検証するために、有効期限が切れた後においても署名の検証を可能とするため公開鍵証明書の履歴管理機能をもつ受・発注プログラムが存在する。利用者は、公開鍵証明書の更新、失効後の新規発行などの際に、これらの機能を提供する受・発注プログラムへの保管操作を行う。

2.2.2.6　証明書の失効要求

秘密鍵の格納媒体（ＩＣカード）を紛失した場合、パスワードが漏洩した場合、その他秘密鍵が危殆化したと考えられる場合、さらに利用者がサイトへの参加資格を喪失した場

合など、利用者またはサイトが公開鍵証明書を無効にしたい場合がある。これらの場合には、利用者から認証局に対して、証明書の失効を要求する。証明書の失効操作は、厳密には認証局の認証局運用規定（または実施規定）において、主体者および責任者などが規定される。失効が利用者以外の主体によって行われる場合、利用者との間で失効に関する委任がなされなければならない。証明書の失効要求は、現在はオンラインまたはオフラインによる方法が考えられる。失効された公開鍵証明書情報は、失効リスト（ＣＲＬ）として発行され、証明書有効性検証において利用される。また、オンライン有効性検証機能を提供するサービスが提供されている場合、失効が発生した事象は、当該サービスへ通知される。

2.2.3　廃棄

業務を終了する場合、退会する場合など、自分の秘密鍵をもはや使用しなくなった場合は、証明書を発行した認証局の認証局運用規定に従い、失効手続きを行った後、確実に自分の秘密鍵を(又はＩＣカード)を廃棄する。

また、自マシンの受・発注プログラム及び動作環境上から、自他の証明書を削除しておくことが望ましい。

3　留意事項と安全対策

本章では、個人が利用する「電子メール」及び「インターネット・ショッピング」における電子署名の生成と検証に関する留意事項と安全対策について記述する。

3.1　準備

個人による利用者が電子署名を利用するにあたり、準備段階での留意事項と安全対策について記述する。

3.1.1　電子署名の理解

電子署名の利用者は安全な運用が行えるよう、予め電子署名について理解しておく必要がある。

電子署名を理解するための情報源の例としては、「電子署名法あるいはその解説書」や「電子署名を使用するアプリケーションソフトウェア文書（マニュアルなど）」などが挙げられる。

3.1.2　適正なソフトウェアの利用

ソフトウェア自体のセキュリティホールからシステム全体の安全が脅かされる恐れもあるので、セキュリティ対策が施された信頼できるソフトウェアを利用する必要がある。

ソフトウェアの選択に際しては、既存の評価基準や認定基準などを参考にすると良い。ソフトウェアの選択基準の例としては、「セキュリティ評価基準(ＩＳO15408)準拠の製品」や「本ガイドラインの第Ⅳ部に適合した製品」などが挙げられる。

また、古いバージョンのソフトウェアには、セキュリティ上の問題点がある場合もあり、適切なバージョンのソフトウェアを取得する必要がある。

3.1.3　ソフトウェアの適正な入手

不正なプログラムと差し替えられることがないよう、ソフトウェアは適正な手段で入手し安全に保管管理する必要がある。

適正な入手手段の例としては「正規の販売ルートによる購入」などが挙げられる。

また、インターネット・ショッピングの受注者側が利用するソフトウェアについては、「評価プロダクトと実際に利用する製品は分離して管理する」などが挙げられる。

3.1.4　セキュリティ情報の入手

利用するアプリケーションやオペレーティングシステム等のセキュリティ情報（セキュリティホール、関連ウィルス情報等）を入手し、自分のシステム内にセキュリティホールを残さないようにする必要がある。

セキュリティ情報の入手手段の例としては「ベンダーが公表する情報の定期的な確認」や「情報処理振興事業協会等の第三者機関が発表する情報の定期的な確認」などが挙げられる。

3.1.5　ウィルスチェックの実施

コンピュータウィルスの感染により利用しているソフトウェアあるいはシステム全体のセキュリティが脅かされる恐れもあるので、ウィルスの感染防止と早期発見のために定期的な監視などの対策をとる必要がある。

ウィルス対策の例としては、「ウィルス対策ソフトウェアの導入」や「ウィルス情報ファイルの定期更新」などが挙げられる。

3.1.6　信頼できる認証局の選定

証明書の発行申請・取得にあたっては、認証局の信頼性について充分理解し、利用目的（電子メール、インターネット・ショッピング等）に応じた信頼できる認証局を選定することが必要である。

信頼される認証局の例としては、「『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）』（電子署名法）に基づく特定認証業務の認定を受けている認証局」、「電子署名を利用するアプリケーション（電子メール、インターネット・ショッピング等）を提供する組織で選定された認証局」、「運用実績のある認証局」、「認証局運用規定を公開し、かつ適切に運用している認証局」などが挙げられる。

3.1.7　証明書の適切な申請・取得

認証局から証明書を申請し取得する場合は、適切で信頼できる方法で行う必要がある。適切な申請・取得方法の例としては、「利用目的（電子メール、インターネット・ショッピング等）に応じた認証局の選定と選定した認証局の認証局運用規定に記載された申請・

取得方法に従う」などが挙げられる。

また、手段としてオンラインまたはオフラインの方法があるが、これらについても認証局の認証局運用規定に従った選択をする。

3.1.8　証明書の記載事項の確認

証明書は本人認証のよりどころとなると同時に他人に配布するものであるため、発行された証明書の記載事項を表示ツール等の使用が可能であれば確認することを推奨する。

確認する項目の例としては、「発行対象者名が申請内容と一致しているか」や「プライバシー情報が記載されていないか」などが挙げられる。

3.1.9　コンピュータシステム内日時合わせ

電子署名を利用する際の日時は、電子署名を利用するマシンの内部時計（システム日時）が使用されるため、署名側と署名検証側との日時が異なると、証明書の有効期限検証を含む日時に関連する署名検証が正しく行われないことにつながる。これを防ぐため、システム日時を正しく設定し維持することが大切である。

システム日時合わせの例としては、「使用するマシンの“日付と時刻設定”ツールにより適時確認する」などが挙げられる。

3.2　鍵及び本人識別情報（パスワード）の管理

鍵及び本人識別情報の管理について留意事項と安全対策について記述する。

3.2.1　秘密鍵の鍵長の選定

決済を伴うインターネット・ショッピング等の電子署名に使用する秘密鍵についは、適切な鍵長を選定することが有効である。

鍵長の例としては、「ＲＳＡ鍵の場合は、１０２４bit」などが挙げられる。

3.2.2　秘密鍵の管理

決済を伴うインターネット・ショッピング等の電子署名に使用する秘密鍵は、安全な媒体に格納することで鍵が不正にコピーされないよう留意する必要がある。

安全な保管媒体の例として、「耐タンパ媒体（署名機能付ＩＣカード等）」を推奨する。

また、「使用するマシン等に格納する」場合は、秘密鍵へのアクセス制御を充分にし、利用者本人以外が利用できない措置を講じる。この場合、当該マシン等の故障による修理依頼で他人へ渡す際においても十分な管理を推奨する。

推奨する例としては、「暗号化された秘密鍵をバックアップし、当該マシン等に格納されている秘密鍵を消去した後に修理担当業者等へ引き渡す」などが挙げられる。

なお、修理返却後秘密鍵の復元を行った後は、速やかにバックアップ用の秘密鍵の消去を行う必要がある。

3.2.3　本人識別情報（パスワード）の管理

電子署名に使用する秘密鍵は、パスワードによるアクセス制御が行われ利用者本人以外の使用を制限している。このため、鍵利用のためのパスワードは安全に管理する必要がある。

安全な管理方法の例としては、「他人に類推されにくいパスワードの設定（生年月日、電話番号等は使用しない）」、「パスワードを利用者本人だけの秘密にする（備忘用のメモ等には充分な注意が必要である）」、「パスワードを定期的に変更する」などが挙げられる。

3.2.4　秘密鍵複製の制限

秘密鍵の複製は、その重要性からバックアップも含め行わないこととする。（バックアップについては、秘密鍵保管媒体マシンの修理等特別な場合を除く。）

3.3　署名生成（電子署名の利用）

電子署名の生成（利用）する際の留意事項と安全対策について記述する。

3.3.1　離席時の処置

電子署名で使用しているマシン等からの離席時に、署名文書の改ざんが行われないよう留意する必要がある。

離席時の留意事項の例としては、「秘密鍵保管媒体がＩＣカードの場合は、ＩＣカードを抜き取り携帯する」、「使用マシン等に保管されている場合は、関連するアプリケーションを利用できないように、ログアウトまたはシャットダウン等の手段でマシン等の使用

を制限する」などが挙げられる。

3.3.2　電子署名操作ログの管理

電子署名を利用する利用者が、決済を伴うインターネット・ショッピング等の注文受注者（売り手）の場合、注文否認を含む操作ミスまたは不正等による注文発注者（買い手）との齟齬等が発生した場合への対応として、操作の履歴（ログ）を保存し定期的に確認する必要がある。

操作ログの運用管理の例としては、「操作ログが採取できるソフトウェアを利用する」、「操作ログ改ざん検出のため、署名を行った上で保管する」、「署名に関する操作のログファイルを定期的にバックアップ及びアーカイブし管理する」などが挙げられる。

3.3.3　電子署名の意味の伝達

電子署名を行う際には、署名検証者が表記を確認することにより、署名の意味（目的）の理解が可能となるよう、署名対象文書に署名の意味を表記する。

電子署名の意味の表記例としては、「文責」、「照査」、「検認」、「承認」、「決済」、「契約締結・領収」などが挙げられる。

3.3.4　電子署名付文書の管理

電子署名を利用する利用者が、決済を伴うインターネット・ショッピング等の注文発注者（買い手）及び受注者（売り手）の場合は、両者間で発生する紛争等への対応を考慮しておく必要がある。

万一の紛争等への対応の例としては、「両者で取り交わした署名付文書を検証に用いる証明書とともに保管する」などが挙げられる。

3.4　鍵及び証明書の更新

鍵及び証明書の更新についての留意事項と安全対策について記述する。

3.4.1　秘密鍵及び証明書の更新

秘密鍵及び証明書は、有効期限が設定され期限内での使用のみ有効と判断される。そのため、引き続き証明書の利用及び電子署名（秘密鍵）の利用を必要とする場合は、有効期

限内に新しい証明書の更新を当該認証局へ申請する。

証明書の更新に伴う申請及び取得に際しての留意事項と対策は、「3.1 準備」の項目と同様である。

3.5　鍵及び証明書の廃棄

鍵及び証明書の廃棄についての留意事項と安全対策について記述する。

3.5.1　証明書の失効

証明書は、対応する秘密鍵の安全性が確保されているといった条件の範囲内で使用されるものであるが、秘密鍵の不正コピー、秘密鍵保管媒体の盗難、紛失などが発生し鍵の安全性が保証できなくなった場合は、証明書を無効にする処置として「証明書の失効」を行う必要がある。証明書の失効手続きについては、「証明書を発行した認証局の認証局運用規定に記載された手続き」に従い実施する必要がある。

実施する作業の例としては、「証明書を発行した認証局への速やかな失効申請」、「引き続き証明書の利用及び電子署名の利用を必要とする場合は、新しい証明書の再発行要求」などが挙げられる。

3.5.2　秘密鍵の廃棄

「証明書の失効」で記述した状況等により証明書を失効した場合、あるいは秘密鍵や証明書の利用をやめる場合などは、保管している秘密鍵を速やかにかつ完全に廃棄する必要がある。

廃棄する手段の例として、鍵保管媒体がＩＣカードの場合は「利用者個人が物理的に破壊する」、「組織等から配布を受けている場合は、組織等の運用管理者へ返却し廃棄処理を依頼する」などが挙げられる。また、鍵保管媒体がＨＤ等の場合は「ＨＤのフォーマットを行う」が挙げられる。

3.6　署名検証（信頼点の管理）

署名検証を行う際、信頼点となる認証局の管理について留意事項と安全対策について記述する。

3.6.1　信頼点の操作

署名検証（証明書検証）のよりどころとなる信頼点に関する操作は、不正な追加や変更などが行われないように利用者本人自らが行う。

3.6.2　信頼点証明書の追加

信頼点の証明書を追加する場合は、その証明書に対する署名検証、有効性確認及び失効状況等に問題が無いことを確認した上で行う。

証明書の確認方法の例としては、「雑誌や新聞などで広報された証明書の内容と一致していることを確認する」などが挙げられる。

3.6.3　信頼点の確認

信頼する信頼点の情報を定期的に確認し、信頼点リストに不審な信頼点が追加されていないことを確認する。

第III部　企業における電子署名の利用

企業間電子商取引（いわゆるＢｔｏＢ）のための情報システムは、これまで紙媒体で行われていた商取引の様々なフェーズの電子化を推進する。電子化された商取引では、捺印された文書（紙媒体）に相当する、信頼し得る電子文書の存在が必須となる。

現状の企業間電子商取引はＷｅｂ（WWW）技術に基づくもの、すなわちＷｅｂサーバとブラウザによって行われるものが多数を占めている。その場合、Ｗｅｂサイトに掲示公開（または相手を限定して開示）される情報、ダウンロードされる情報、およびブラウザからのフォーム入力情報は、いずれもこの電子文書としての信頼性に欠けるものがある。電磁記録であるがゆえに、情報提供側からすれば受取側による改ざんが可能と考えられ、また受取側からすれば提供側のなりすましや提供後の原本改ざんの可能性があるからである。

この信頼を得るには、文書の改ざん、文書作成者のなりすましなどを排除することが必要である。そのために、企業間電子商取引をサポートするシステムにおいて、標準化の進んでいる電子署名技術が、多用されると考えられている。

企業間電子商取引を実現するための電子署名には、企業の代表者印などに相当するもの、社内でのみ意味を持つもの、などの様々な署名が考えられる。本第Ⅲ部では、想定する利用場面と利用手順を１章で記述し、次に、そこで求められる留意事項、安全対策を２章で検討する。また、「1.2 利用手順」で記述する利用手順を、「付録２　企業間電子商取引おける電子署名の利用手順」で一覧にまとめている。

1　企業間電子商取引システム

ここでは、本第Ⅲ部で検討する企業間電子商取引の形態や、処理の手順を記述する。電子商取引において部品等を調達する企業の主導の下に複数の供給側企業がこれに参加する調達ＥＤＩを題材にしている。企業内には電子署名を利用するエンドユーザ部門と、これを技術および運用の面で支援するシステム管理部門が存在するものとする。また、エンドユーザ部門の利用者はＩＣカードを持ち、秘密鍵を格納して認証に利用すること、などを想定している。

次の２章で電子署名の利用における留意事項と対策を検討する際に、本章における利用場面と利用手順の設定が前提となる。

1.1　利用場面

1.1.1　利用場面の概要

企業間電子商取引には、販売ＥＤＩ、調達ＥＤＩなどの様々な取引形態が考えられる。従来、特定の取引相手との間に専用線などを敷設して実施していたＥＤＩがオープンなネットワークに移行するばかりでなく、販売、調達のオープン化、すなわち不特定多数との間での販売、調達などの試みも始まっている。特定のＥＤＩ専用ソフトウェアを利用するものもあれば、電子メールソフトウェアなどの汎用ソフトウェアによるものもある。

本第Ⅲ部では、企業間電子商取引の例として部品の調達ＥＤＩを取り上げる。ある企業が自社の新たな製品を製造するために必要な部品を新たに調達するという例である。ここでは調達先として広範囲の企業からの公募を想定した。そして応募に基づいて調達先を絞り込み、より詳細な要求仕様を提示し、最終的に見積り、契約先の決定、契約と進むものとした。そしてこの例では、これらのやりとりが、後述する基本契約を除き全て電子文書により行われると想定している。

このような電子調達では、例えば調達仕様書、見積書など、多くの文書が調達側と供給側の間で授受され、その内容に基づいて双方の手続きが進む。したがってその内容の真正性が疑わしい状況では、企業は次の段階へ進むにあたってリスクテーキング（またはリスクヘッジ）を強いられることになる。電子署名は電子文書の内容の真正性を保つための技術として、このリスクを軽減するために用いられる。

本ガイドラインの利用場面では、特に以下の各項を想定している。

- 電子署名の信頼性

調達の各段階で一方から他方に供給される主要な電子文書は、相手方の次のアクションに必要な信頼を得るために、電子署名が付与される（署名生成）。この信頼のレベルとして、企業代表者印に相当する高いレベルと、文書の改ざん防止を主目的とする、「人」とその権限、責任についての要請の高くないレベルとが想定される。前者は契約書などの重要文書、および仕様書や見積書の提供側に、後者は詳細資料などの文書、および仕様書や見積書の受領側の署名（受付印）などに使われると考えられる。

- 秘密鍵とその証明

署名生成をなしうる「人」は、信頼された第三者機関、もしくは合意された当事者の一方が運営する認証機関により、識別され認証され、その秘密鍵に対して証明書が発行される。前述のように「人」にはその署名の権限と責任が伴うが、そのレベルにより認証機関の要件も変化すると想定される。

なお、権限の付与方法、およびその表示方法については、本ガイドラインの対象外とする。また、「人」が介在することなくアプリケーション・プログラム内で自動的に行われる署名生成も、本ガイドラインの対象外である。

- 複数の署名

同一の文書について、複数の当事者が電子署名を付与することがある。契約書などでは調達側、供給側の双方の電子署名が行われると想定される。また企業内で複数当事者が署名する可能性もある。例えば文書作成担当と責任者による署名、もしくは複数部門の関係者がそれぞれ関係箇所に責任をもつための署名などである。この場合、通常はまず既になされた署名を検証した上で、自分も署名を付与するものと想定される。

- 電子署名の行為者と支援組織

一般に企業内において、商取引の専門家は電子署名行為に習熟しているとは限らない。例えば企業の代表者にＰＫＩに関する充分な知識を要求することは困難かもしれない。一方、電子署名を行うソフトウェア、ハードウェアは、セキュリティ保持の観点からそれらの運用について一定の制約、規定された手順の遵守が求められる。このギャップを埋める支援組織として、企業内に「システム管理部門」の存在を想定する。「システム管理部門」は電子署名を利用する「エンドユーザ部門」が使用するシステムを選択し、その具体的方法を指導し、同時に秘密鍵の漏洩防止などを含むセキュリ

ティ上の規定を遵守させる役割を担う。

1.1.2　利用者システムと処理の流れ

前項で述べた部品の調達ＥＤＩで想定される調達側、供給側両システムの一例を図-Ⅲ-1-1に示す。

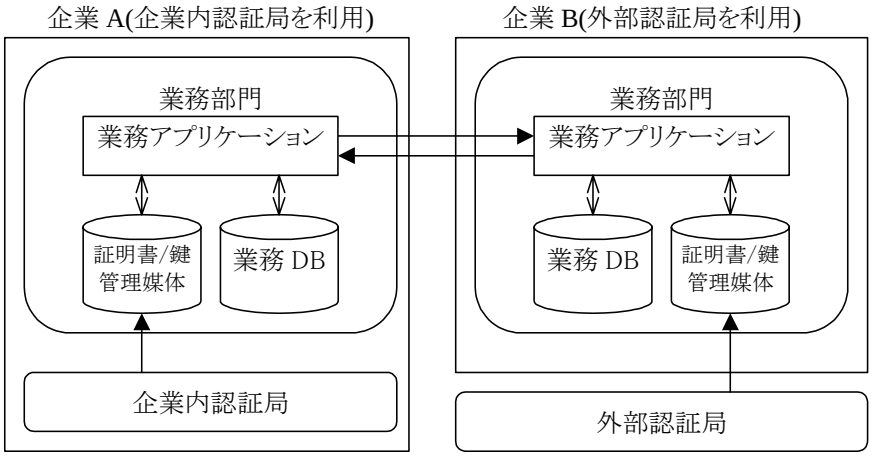

図-Ⅲ- 1-1　企業間電子商取引のシステム構成例

図-Ⅲ- 1-1の例では、Ａ、Ｂ両企業の利用者への証明書の発行機関として、「企業内認証局を用いる例」と「外部認証局を用いる例」を挙げている。企業内認証局では、その証明書の発行者（証明書に記載される発行名義人）がその企業自身である。また、外部認証局では、信頼された第三者機関としての認証機関が証明書の発行者となる。

証明書を受け取り検証する側から見れば「利用者を誰が証明しているか、その証明した人は信頼できるか」が大きな問題となる。この例のように、お互いの証明書が異なる認証局から発行されている場合は、以下のような方法で信頼関係を結ぶ必要がある。

(ア) 互いの業務担当者が相手の発行者を信頼する。

（取引相手の証明書を発行者した認証局の証明書を、信頼点として利用者システムの署名検証プログラムに登録する）

(イ) 互いの発行者が相手の発行者を信頼する。

（発行者同士が相互認証を結ぶ）

上の例のように企業内認証局から発行された証明書が用いられる場合、（ア）の方法では相手企業（企業Ｂ）の個々の業務担当者（署名検証を行う者）が、企業Ａの企業内認証

局を自身の署名検証プログラムに信頼点として加えなければならない。この行為は、企業Ａ、Ｂ間での何らかの合意に基づいて、企業Ｂの「システム管理部門」の指導により行われることになる。企業Ｂの外部認証局は、予め信頼された第三者機関として署名検証プログラムの信頼点に加えられている場合がある。（イ）の方法は企業Ａの発行者が企業Ｂの発行者を（自企業内に向けて）証明し、また企業Ｂの発行者が企業Ａの発行者を証明する、いわゆる相互認証である。この場合、企業内の業務担当者は自企業の証明書発行者だけを予め信頼点に加えておけばよいことになる。

本ガイドラインでは、図-Ⅲ- 1-1の業務部門の間で、以下の処理を想定している。

- 調達側が調達概要をＷｅｂで公開。
- 供給側が応募の意思表示を行う。
- 調達側が初期調査により数社に絞込み、さらに詳細な調達仕様を提示する。

（アクセス制御されたＷｅｂページで公開）

- 調達仕様書はＸＭＬで記述され、これを取り込んだ「見積書入力フォーム」も合わせて公開する。
- 供給側は見積書入力フォームに見積り内容を記述し、調達側に返信する。
- 調達側は、見積内容を検討の上、契約先を決定する。
- 基本契約を締結後、調達側が発注契約を行う。
- 供給側は発注契約に対し、受注確認書を返信する。

上記の業務フローの概要を図-Ⅲ- 1-2に示す。

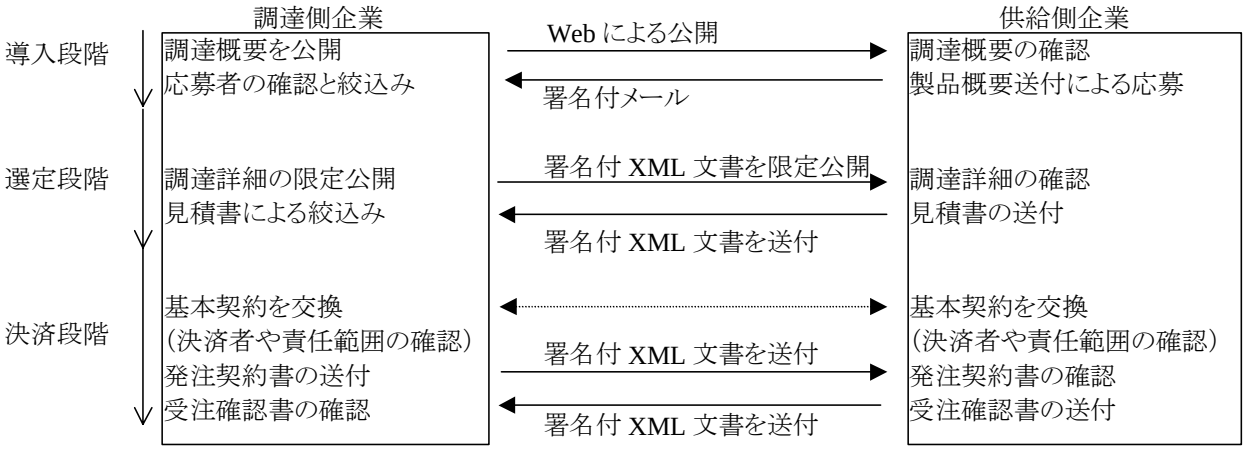

図-Ⅲ- 1-2　企業間電子商取引（調達ＥＤＩ）における業務フロー例

調達ＥＤＩの一連の処理の中でも、その段階に応じて、署名生成・署名検証に求められる安全性の水準が異なると考えられる。以下、順に述べる。

①　導入段階

調達側企業は、公募等により供給側企業を募る。この段階では、取引相手を広い範囲から選定する目的から、対象は必ずしも限定されない。また、この段階での改ざんやなりすましは後の段階で検出されるので、それによる被害は軽微なものであることが想定できる。

調達概要は例えばＷｅｂで公開される文書である。この文書の真正性を電子署名により保証すべきか否かは、上記により議論の分かれるところである。例えばＷｅｂサーバに予め認証機関から（ＳＳＬサーバ認証の）証明書を得て運用することで、供給側企業に対してＷｅｂサーバのなりすましがないことを保証すれば済むかもしれない。ただしＳＳＬは、掲示された個々の文書の真正性については何も約束しない。もし調達側企業が自身の企業内認証局の発行したＳＳＬサーバ認証の証明書（このＷｅｂサーバは確かに当社の特定部門が運用している、という意味になるだろう）を使用するならば、この時点で調達側企業の認証局（発行者）は供給側企業に信頼されていなければならない。

供給側企業は、調達概要を見て自社製品により応募すると決めた場合、例えば電

子メールにより調達側企業に応募の意思を伝える。この電子メールに、例えば自社製品のカタログなど（公開情報）を添付することも考えられる。この電子メールには発信元のなりすましがないこと、通信路上での改ざんがないことを保証するために、供給側企業の業務担当者がＳ／ＭＩＭＥなどで規定する電子署名を付与することが考えられる。その場合、この電子署名に用いられる業務担当者の秘密鍵に対する証明書は、供給側企業の認証局（例では外部認証局）から発行されたものである。この時点で供給側企業の認証局（発行者）は予め調達側企業に信頼されているか、電子メールを受け取った時点で調達側企業が個別に信頼するか否かを決定することになる。これは調達側企業による供給側企業の信用調査などと合わせて行われるかもしれない。

なお本ガイドラインの範疇外だが、もしこの段階で既に機密情報を含む応募が行われるならば、供給側企業からの電子メールは調達側企業の業務担当者宛にＳ／ＭＩＭＥなどで暗号化されて送付されるべきであろう。

②　選定段階

①の応募内容に基づいて調達側企業は、調達交渉を続けるべき供給側企業候補を絞る。続いて絞り込んだ供給側企業に対して調達の詳細（いわゆる調達仕様）を開示し、見積りを求めることになる。供給側企業は調達仕様に基づいて検討し、見積書を提出する。

この段階では、調達仕様書、見積書ともに、その真正性が必須となる。すなわち、調達仕様書については、調達側企業の業務担当者についてなりすましがないことと、その内容に改ざんがないことが、また見積書についても、供給側企業の業務担当者についてなりすましがないことと、その内容に改ざんがないことが、それぞれ求められる。したがって選定段階からは、授受される文書は原則として電子署名の付与された文書となる。

電子署名に使用される業務担当者の秘密鍵は、相手方企業から信頼された認証局（発行者）により証明されていなければならない。この段階で、必要ならば冒頭で述べた認証局の信頼に関する合意が、他の取り決め（例えば機密保持契約など）と合わせて行われるかもしれない。この合意に基づいて業務担当者はそれぞれ、相手企業の認証局の証明書を信頼点へ追加することになるだろう。もし、ある企業の業

務担当者の署名プログラムや秘密鍵のセキュリティ管理が十分なものでなければ、相手企業は電子署名による真正性の保証が得られないおそれがある。企業の「システム管理部門」は相手認証局および業務担当者のセキュリティ・ポリシーを充分吟味しなければならない。また一方で、自認証局および業務担当者のセキュリティ・ポリシーを、文書化された一定レベルに保たなければならない。

文書への電子署名は、例えばＸＭＬのような標準に基づいて行われる。調達側企業から調達仕様書が、例えばＸＭＬ文書として作成され、署名生成がなされて、各供給側企業候補に送付される。受取側はその電子署名を検証し、真正性を確認した上で、その内容に基づいて見積りを出すか否か、価格、納期などを検討する。供給側企業は最終的に見積書を、やはりＸＭＬ文書として作成および署名生成を行い、調達側企業に送付する。受取側となる調達側企業ではその電子署名を検証し、真正性を確認した上で、その内容を見ることになる。また、この間、質問書／回答書などの補助的文書が授受されることがある。これらも、必要とされる真正性の度合いによっては、電子署名付きＸＭＬ文書となると考えられる。

なおこれらの文書について一般には真正性と共に、業務担当者（署名生成者）の資格、権限が問題になるが、その扱いは本ガイドラインでは触れていない。また、文書の真正性は、その授受時点で確認されるものとしている。電子署名付文書の長期保存（電子署名の有効性の長期継続に基づく長期間経過後の文書の真正性確認）も本ガイドラインの対象外である。

③　決済段階

決済段階では、特定の相手であることが最も確実に保証されなければならない。この段階での改ざんやなりすましは、金額的にも、企業にとっての信用面でも、重大な問題を引き起こすからである。

したがって、ここで交わされる契約書、発注書、受注確認書などの文書については、選定段階以上に厳密な署名生成と署名検証が必要とされる。②で述べた業務担当者（署名生成者）の資格、権限の確認を含む、別途の基本契約などが交わされた上で、個別案件の文書の署名が行われるかもしれない。また、そのための秘密鍵は特に厳重な管理下におかれていなければならない。署名プログラムはパスワードなどではなく生体認証などで守られていなければならないかもしれない。また、少な

くとも契約終了時点まで証明書が有効であることが必要かもしれない。

文書と署名は②と同様、標準化されたＸＭＬ技術などが使われると考えられる。文書によっては、調達側企業と供給側企業の双方が電子署名（多重署名）することになるかもしれない。

1.1.3　利用場面の詳細

企業間電子商取引に関して、以下の想定を置く。

(1) 取引の形態

企業間電子商取引の様々な形態を取引の場の主体で分類すると、調達ＥＤＩ、販売ＥＤＩなどがある。本第Ⅲ部では、調達ＥＤＩを検討対象とする。検討結果は、電子署名の利用という観点からは販売ＥＤＩにも準用できる。

(2) 取引の公開性と段階

調達側の企業は、供給側の企業を広く公募する場合（オープン参加）と、随意契約のように特定の取引相手を予め決めている場合がある。また、その中間の場合で、事前に登録されているメンバを対象に調達仕様を提示する場合もある。ここではオープン参加の場合を例に採り上げる。その上で、契約企業を決定する過程は、前項に記述した「導入段階」「選定段階」および「決裁段階」の３段階を踏むものとした。

(3) 取引の当事者

取引に参加する当事者から見ると、取引形態は以下のようなものが考えられる。

- 調達側と供給側の２者間による取引
- 公証局や電子商取引市場運営者などが介在する３者間による取引

ここでは２者間の取引を想定する。

(4) 取引額や取引の価値

小額の取引や真正性要求の程度が低い情報（導入段階でやり取りされる情報など）の場合は、改ざん防止などを主目的として担当者レベルの署名のみでよいかもしれない。また、高額の場合は担当者と決裁者の双方の署名が必要になることも考えられる。

ここでは、より高い運用レベルが要求される高額の取引を想定する。この想定は、「(10)署名用と暗号化用の鍵ペア」「(11)鍵管理媒体」「(12)鍵認証の方法」など、運用管理面の想定に反映される。

(5) 署名の対象

署名が必要となる文書の内容としては、契約書、情報公開、応募、問い合わせ／回答、仕様書、見積書など、企業間電子商取引で交わされる文書全般を対象とする。

文書の形式としては、Word や Text 等の一般ファイル、ＸＭＬ文書などを対象とする。特に、文書の一部分への署名や、一方の企業内における担当者と決済者の階層的な署名、契約書への双方の企業の署名などに適した構造を持つＸＭＬ文書は、企業間電子商取引における典型的な文書形式として想定する。

(6) 利用アプリケーション

メーラ、ブラウザ、汎用ＸＭＬブラウザなど、各種アプリケーションを対象とする。

なお、業務処理対応に開発されたアプリケーション・プログラムを利用する場合には、アプリケーション・プログラムで署名生成や署名検証の手続を実現したり、支援したりすることもあり、本ガイドラインで提示する留意事項と対策はそのままでは適用できない。

(7) 証明書の発行者

互いの発行者を利用者が信頼することが前提となるが、信頼関係確立は以下の場合を想定する。

- 利用者間で同一の発行者による証明書を利用している場合。具体的には調達者側企業により提供された証明書を利用する場合など。
- 互いの発行者は異なるが、発行者間で相互認証が行われている場合。
- 互いの発行者は異なるが、自社の基準に照らして、信頼に値すると判断した場合。

(8) 認証対象（取引の当事者）

認証対象は企業内個人とする。

エンドユーザ部門やその個人には、ＰＫＩに関する専門知識を要求しない。エンドユーザ部門を支援する組織として、ＰＫＩの知識を持つシステム管理部門の存在を想定する。システム管理部門は、電子署名を利用するエンドユーザ部門が使用するシステムを選択し、その具体的利用方法を指導し、同時に秘密鍵の漏洩防止などを含むセキュリティ上の規定を遵守させる役割を担うものとする。

(9) 鍵の生成

鍵の生成は、利用者システムにて行う方法と、認証局などで生成して利用者に配布する方法がある。ここでは、利用者システムにて鍵を生成することを想定する。

(10) 署名用と暗号化用の鍵ペア

利用者は、電子署名を利用するために鍵ペアを持つ。また、電子文書等の秘匿も行うのであれば、暗号化用の鍵ペアも持つ。これらの二組の鍵ペアは、一組のものを共通に使うことはせず、別のものを使用する。

企業間電子商取引では高い安全性が求められることから、署名用の秘密鍵はバックアップをせず、紛失したら再発行すべきである。これに対して、暗号用の鍵ペアは復号を行うために安全な運用のもとでバックアップをする運用が基本となるためである。

(11) 鍵管理媒体

秘密鍵は、企業間電子商取引で要求される安全性を実現するため、ＩＣカードに格納するものとする。

(12) 鍵認証の方法

前項に加えて、ここでは秘密鍵を格納したＩＣカードをＰＩＮ（Personal Identification Number、暗証番号）で認証するものとする。

1.2　利用手順

「1.1　利用場面」で想定した調達ＥＤＩの一連の手順において、調達側企業は、電文の送信に際して署名生成を、また受信時には署名検証を行う。署名生成に関して、利用者は、「準備」「鍵の管理」「署名生成」「鍵の更新」及び「鍵の廃棄」を行う。また、署名検

証に関連して、「準備」及び「署名検証」を行う。

なお、供給側企業においても署名生成および署名検証のための利用手順は類似しており、同様の留意事項と安全対策が必要とされる。

また、以降で記述する「エンドユーザ部門」および「システム管理部門」は、それぞれ下記の意味として使用している。

- 「エンドユーザ部門」：相手企業と調達仕様書や契約書のやりとりなど電子署名を必要とする業務を行う担当部門。
- 「システム管理部門」：エンドユーザ部門を支援し、システムの設置と管理、電子署名に関する指導、企業内認証局の管理などの役割をもつ部門。

1.2.1　準備

1.2.1.1　鍵ペアの生成

利用者が電子署名に用いる鍵ペア（秘密鍵と公開鍵）を生成する。一般的には、アプリケーション・プログラムに付属する鍵生成ツールによって生成される。

1.2.1.2　鍵の格納

生成した鍵ペアを鍵管理媒体に格納する。ここでは、鍵管理媒体はＩＣカードである。一般的にはアプリケーション・プログラムが鍵管理媒体との接続インタフェースを持つ。エンドユーザ部門の担当者がアプリケーション・プログラムの機能を用いて鍵管理媒体に鍵を格納する。

1.2.1.3　信頼点の登録

署名検証に必要な信頼点（相手企業の証明書を発行した認証局の証明書）を、署名プログラムに登録する。信頼点の確認はシステム管理部門によって行われる。システム管理部門は、基本契約または相手企業が公に公開している認証局証明書のフィンガープリントを確認し、適切な方法で相手企業認証局の証明書を入手し、エンドユーザ部門担当者に配布する。エンドユーザ部門担当者は、システム管理部門から提供される相手企業認証局証明書のみを署名プログラムに登録する。

1.2.1.4　証明書の申請と証明書の取得

エンドユーザ部門の担当者は、アプリケーション・プログラムの機能を用いて企業内認証局に対して証明書発行申請を行い、企業内認証局から証明書を取得する。システム管理部門はエンドユーザ部門担当者が正しい申請者であることを認証するために、エンドユーザ部門担当者自身とシステム管理部門しか知りえないＰＩＮなどをエンドユーザ部門担当者に安全な方法で配布する。エンドユーザ部門の担当者は、ＰＩＮ、自分自身を証明する申請項目と秘密鍵保護パスワードを入力して証明書の申請書を生成し企業内認証局に送付する。申請書の送付方法はフロッピー・ディスクなどに格納してオフラインで送付する方法とＨＴＴＰＳなど安全な通信手段を用いたオンラインで送付する方法がある。企業内認証局により生成された証明書も申請書と同様な手段で返送される。

証明書は、企業内認証局のルート証明書まで含んだ証明書チェインの形式と企業内認証局のルート証明書を含まない形式がある。ルート証明書を含まない形式の場合はシステム管理部門が安全な方法でルート認証局の証明書をエンドユーザ部門担当者に公開しエンドユーザ部門担当者自身が適切な方法でアプリケーション・プログラムに取り込む必要がある。取得した証明書はアプリケーション・プログラムを用いて鍵ペア(秘密鍵と公開鍵)チェックなどの検証を行い、証明書管理媒体に安全に保管する。

1.2.2　鍵の管理

1.2.2.1　鍵格納媒体の保管

エンドユーザ部門の担当者は秘密鍵を不正に使用されないために、ＩＣカードに保護パスワードの設定を正しく行い、厳重に保管管理する。システム管理部門は保護パスワードの設定方法のガイドラインを作成し、エンドユーザ部門の担当者に対して簡単に推測されないパスワードの設定や定期的なパスワードの変更を指導する。

1.2.2.2　信頼点リストの維持

システム管理部門は正しい信頼点（信頼する相手企業認証局の証明書）をエンドユーザ部門に適切な方法で通知する。エンドユーザ部門担当者はシステム管理部門から通知された信頼点のみ署名プログラムに登録し、不当な信頼点の登録を防ぐために信頼点のリストを定期的に維持管理する。

1.2.2.3　鍵のバックアップ

安全のため、秘密鍵のバックアップは行わない。

1.2.2.4　有効期限後の鍵の保管

証明書と鍵の有効期限が切れた場合は、その証明書と鍵を格納したままのＩＣカードを引き続き保持することはせず、システム管理部門が定める規定に従ってＩＣカードを廃棄あるいは返却などする。

1.2.3　署名生成

1.2.3.1　署名対象部分の作成

電子文書のうち、署名対象とする部分を作成する。

例えば、調達仕様書において調達側企業が詳細仕様を記述する部分と、供給側企業が見積り内容を記述する部分が、一つのＸＭＬ文書に記載されている場合を想定する。その詳細仕様部分など、該当部分を作成する。

1.2.3.2　秘密鍵の活性化

エンドユーザ部門の担当者は、ＩＣカード内の秘密鍵を利用するためにＰＩＮを入力する。尚、ＰＩＮはシステム管理部門から発行されるガイドラインに従い、エンドユーザ部門の担当者が定期的に変更する必要がある。

1.2.3.3　署名生成と署名文書の送信

エンドユーザ部門にて署名生成を行い、署名付文書を相手方企業へ送信する。

例えば、エンドユーザ部門担当者が、適切な責任者に詳細仕様の内容の確認を依頼し署名実施の許可を得た後、調達仕様書の仕様記述部分にアプリケーション・プログラムを用いて署名を施し、送信する。また、必要があれば、署名付電子文書をＳＳＬなどにより通信路の秘匿性を保持した環境で送信する。

1.2.4　鍵の更新

1.2.4.1　証明書と鍵ペアの更新

エンドユーザ部門担当者は、証明書の有効期限が切れる前に認証局に証明書の更新申請を行い、新しい証明書を取得する。システム管理部門が適切な更新対象エンドユーザ部門担当者であることを認証する手段として次の２つの方法が考えられる。

- システム管理部門が更新対象エンドユーザ部門担当者にその本人とシステム管理部門のみが知りえる更新確認用ＰＩＮを安全に配布し、証明書更新申請受付時にＰＩＮを確認して更新対象者を認証する方法
- エンドユーザ部門担当者がアプリケーション・プログラムを利用して既存の秘密鍵で更新申請書に電子署名を施し、認証局が証明書更新申請書の署名検証を行うことにより既存の認証済み証明書保持者であることを認証する方法

後者の場合には、次の手順を踏む。

エンドユーザ部門担当者は更新前の秘密鍵を利用するＰＩＮを入力して、新しく鍵ペアを生成する。エンドユーザ部門担当者は自分自身を証明する申請項目と生成した秘密鍵で更新申請書を生成して認証局に送付する。認証局は申請書を検証し新しい証明書を返信する。申請書の送付及び証明書の取得方法などについては「1.2.1.4　証明書の申請と証明書の取得」と同様である。

1.2.5　鍵の廃棄

1.2.5.1　証明書の失効

秘密鍵の危殆化（紛失、盗難など）やＩＣカード等の破損などにより証明書が使用不可能となった場合、エンドユーザ部門担当者は速やかにシステム管理部門に既存証明書の失効依頼を行う。システム管理部門は認証局運用規定に従い既存証明書の失効手続きを行う。エンドユーザ部門の担当者の変更が発生した場合も、エンドユーザ部門担当者はシステム管理部門に前担当者の証明書の失効依頼を行う。

1.2.5.2　鍵の廃棄

秘密鍵の危殆化（紛失、盗難など）の発生や証明書の有効期限が切れた場合、エンドユ

ーザ部門担当者は、ＩＣカードの初期化処理を行い、鍵ペアを使用不可能とする。

1.2.6　署名検証

1.2.6.1　署名付文書の入手

相手方企業から署名付文書を入手する。

例えば、調達側企業が供給側企業の記述した署名付ＸＭＬ文書を入手すると、調達仕様書の見積り内容記述部分に供給側企業の署名がなされている。

1.2.6.2　証明書の検証

エンドユーザ部門の担当者は、証明書の検証をアプリケーション・プログラムに指示する。

アプリケーション・プログラムは、次の処理を行う。

(1) **有効期限や** KeyUsage **等の確認**

証明書に記載されている有効期限や KeyUsage 項目に記載されている内容に従った利用が行われているかの確認を行う。

(2) **証明書発行者の確認**

証明書チェーンを正しくたどり署名生成者の証明書が事前にアプリケーション・プログラムに登録されている信頼点（署名生成者の証明書の発行認証局）であるか確認する。正しく確認できない場合は、アプリケーション・プログラムからその旨の通知が利用者になされる。

(3) **失効確認（ＣＲＬ／ＯＣＳＰ）**

アプリケーション・プログラムは署名生成者の証明書を発行した認証局から証明書の失効情報を取得し、署名生成者の証明書が有効であるかどうかの確認を行う。一般的にＣＲＬとＯＣＳＰを用いた失効確認方法がある。ＣＲＬを用いる場合はＣＲＬの更新間隔やＣＲＬデータの取得間隔を十分考慮する必要がある。

1.2.6.3　署名生成者の確認

企業間電子商取引において決済段階での署名生成者が取引の権限者であるかの確認は、オフラインで行われる基本契約時に権限者の証明書のフィンガープリントを交換すること

で確認するものと想定する。調達仕様書の見積り仕様部分に施される署名の署名生成者の確認は既にアプリケーション・プログラムに登録されている信頼点（相手企業認証局）から発行された証明書に対応する秘密鍵で署名されていることの確認とその証明書のフィンガープリントがオフラインで事前に交換された証明書のフィンガープリントと同一であるかの確認を行う。

1.2.6.4　署名検証（非改ざん確認）

エンドユーザ部門担当者はアプリケーション・プログラムを用いて、調達仕様書の見積り仕様部分に施された署名が信頼点（相手企業認証局）から発行された証明書に対応する秘密鍵で署名されていることを検証し、内容が改ざんされていないことを確認する。

1.2.6.5　信頼点の追加

システム管理部門は新たな取引企業が追加される度に適切な信頼点をエンドユーザ部門担当者に通知する。

1.2.6.6　内容の確認

エンドユーザ部門担当者はアプリケーション・プログラムの機能を用いて、電子文書の署名範囲を明確に認識して、相手側が保証する記述内容を確認する。

2　留意事項と安全対策

本章では、１章で記述した利用場面と利用手順を前提として、電子署名の生成と検証に関する留意事項と安全対策を「エンドユーザ部門」、「システム管理部門」のそれぞれを対象にまとめる。

2.1　エンドユーザ部門

2.1.1　準備

以下に、この段階でエンドユーザ部門担当者が作業する際の留意事項と対策を示す。

(1) 電子署名の理解

電子署名の利用者は安全な運用が行えるよう、予め電子署名について理解しておく必要がある。

電子署名を理解するための情報源の例としては、「電子署名法あるいはその解説書」や「電子署名を使用するアプリケーションソフトウェア文書（マニュアルなど）」、「社内システム管理部門が配布する手引書」などが挙げられる。

(2) 適正なソフトウェアの利用

ソフトウェア自体のセキュリティホールからシステム全体の安全が脅かされる恐れもあるので、セキュリティ対策が施された信頼できるソフトウェアを利用する必要がある。

ソフトウェアの選択に際しては、既存の評価基準や認定基準などを参考にするとよい。ソフトウェアの選択基準の例としては、「セキュリティ評価基準(ＩＳO15408)準拠の製品」や「本ガイドラインの第Ⅳ部に適合した製品」などが挙げられる。

また、古いバージョンのソフトウェアには、セキュリティ上の問題点がある場合もあり、適切なバージョンのソフトウェアを取得する必要がある。

(3) ソフトウェアの適正な入手

不正なプログラムと差し替えられることがないよう、ソフトウェアは適正な手段で入手し安全に保管管理する必要がある。

適正な入手手段の例としては「正規の販売ルートによる購入」や「社内システム管理部門からの入手」などが挙げられる。

(4) セキュリティ情報の入手

利用するアプリケーションやＯＳ等のセキュリティ情報（セキュリティホール、関連ウィルス情報等）を入手し、自分のシステム内にセキュリティホールを残さないようにする必要がある。

セキュリティ情報の入手手段の例としては「ベンダーが公表する情報の定期的な確認」や「情報処理振興事業協会等の第三者機関が発表する情報の定期的な確認」、「社内システム管理部門からの通達の実施」などが挙げられる。

(5) ウィルスチェックの実施

コンピュータウィルスの感染により利用しているソフトウェアあるいはシステム全体のセキュリティが脅かされる恐れもあるので、ウィルスの感染防止と早期発見のために定期的な監視などの対策をとる必要がある。

ウィルス対策の例としては、「ウィルス対策ソフトウェアの導入」や「ウィルス情報ファイルの定期更新」、「ウィルス感染監視の自動化」などが挙げられる。

(6) 信頼できる認証局の選定

証明書の発行申請・取得にあたっては、認証局の信頼性について充分理解し、利用目的に応じた信頼できる認証局を選定する必要がある。

信頼される認証局の例としては、「社内システム管理部門が指定した認証局」、「『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）』（電子署名法）に基づく特定認証業務の認定を受けている認証局」、「電子署名を利用するアプリケーションを提供する組織（取引業界団体など）で選定された認証局」、「運用実績のある認証局」、「認証局運用規定を公開し、かつ適切に運用している認証局」などが挙げられる。

(7) 証明書の適切な申請・取得

認証局から証明書を申請し取得する際は、適切で信頼できる方法で行う必要がある。

適切な申請・取得方法の例としては、「社内システム管理部門が指定した手段に従う」、「選定した認証局の運用規定に記載された申請・取得方法に従う」などが挙げられる。

(8) 証明書の記載事項の確認

証明書は本人認証のよりどころとなると同時に他者に配布するものであるため、発行された証明書の記載事項を表示ツール等により確認する必要がある。

確認する項目の例としては、「発行対象者名や証明書用途などが申請内容と一致し

ているか」や「プライバシー情報が記載されていないか」などが挙げられる。

(9) コンピュータシステム内日時合わせ

電子署名を利用する際の日時は、電子署名を利用するマシンの内部時計（システム日時）が使用されるため、署名生成側と署名検証側との日時が異なると、証明書の有効期限検証を含む日時に関連する署名検証が正しく行われないことにつながる。これを防ぐため、システム日時を正しく設定し維持する必要がある。

システム日時の設定と維持の方法の例としては、「ＧＰＳを利用した時刻同期」や「時刻同期サーバ（ＮＴＰサーバ）の利用」などが挙げられる。

2.1.2　鍵および本人識別情報の管理

以下に、この段階でエンドユーザ部門担当者が作業する際の留意事項と対策を示す。

(1) 秘密鍵の保管媒体

決済を伴う電子署名に使用する秘密鍵は、安全な媒体を利用することで鍵が不正にコピーされたりしないよう留意する必要がある。

安全な保管媒体の例としては、「耐タンパ媒体（ＩＣカード等）」などが挙げられる。

(2) 秘密鍵保管媒体の管理

秘密鍵保管媒体は、紛失や不正持ち出しが起きないように安全に保管する必要がある。

安全な保管方法の例としては、「ＩＣカードを鍵つきの引き出しに保管」や「ＩＣカードの常時携帯」、「入退出記録や利用記録の採取と定期的な確認」、「秘密鍵をハードディスクに保存している場合は、マシン修理時に秘密鍵を完全に消去してからマシンを持ち出す」などが挙げられる。

(3) 本人識別情報（パスワード）の管理

秘密鍵が他人に不正利用されないよう、鍵利用のための本人識別情報（パスワード）は安全に管理する必要がある。

安全な管理方法の例としては、「他人に類推されにくいパスワードを設定」や「パスワードを暗記（メモなどに記録しない）」、「他人に教えない」などが挙げられる。

(4) 秘密鍵複製の制限

秘密鍵が不正にコピーされないよう、予めバックアップも含め複製は行わないよう

に規定しておく必要がある。

2.1.3　署名生成

以下に、この段階でエンドユーザ部門担当者が作業する際の留意事項と対策を示す。

(1) 作成中データの改ざん防止

作成段階（署名前段階）においてデータが改ざんされないよう、作成途中のデータもアクセス管理対象ファイルとして取り扱う必要がある。

アクセス管理方法の例としては、「作成途中のデータの更新権限を”本人のみ”とする」や「更新履歴が残るツールを利用する」などが挙げられる。

(2) 離席時の処置

離籍時に不正なデータの更新などが行われないよう運用する必要がある。

離籍時の運用の例としては、「離席時には署名用ＩＣカードを携行する」や「離席時にはアプリケーションを利用できないように、ログアウト、シャットダウン、または何らかの手段でロックする」、「作業場所は施錠した上、許可を持つもののみ入室可能とする」などが挙げられる。

(3) 操作ログの管理

不正な利用の発見のために、操作の履歴を保存し定期的に確認する必要がある。

操作ログの運用の例としては、「操作ログが採取できるソフトウェアを利用する」や「操作ログの改ざん検出のために、署名を行った上で保管する」、「操作ログの改ざん防止のために、ＣＤ－Ｒなどの書き換えできない媒体に保管する」などが挙げられる。

(4) 電子署名の意味の伝達

電子署名を行う際には、署名検証者が表記を確認することにより署名の意味（目的）の理解が可能となるよう、署名対象文書に署名の意味を表記する必要がある。

署名の意味の表記例としては、「文責」、「照査」、「検認」、「承認」、「決済」、「契約締結・領収」などが挙げられる。

(5) 電子署名の範囲の確認

ＸＭＬ署名などで部分署名を行う場合は、署名範囲が適切であることを確認する必要がある。

2.1.4　鍵および証明書の更新

以下に、この段階でエンドユーザ部門担当者が作業する際の留意事項と対策を示す。

(1) 証明書の更新

証明書は有効期間が設定されその期間内での使用のみ有効と判断されるため、引き続き証明書の利用及び電子署名の利用を必要とする場合は、有効期限内に新しい証明書の更新を当該認証局へ申請する必要がある。

証明書の更新に伴う申請および取得に際しての留意事項と対策は、「2.1.1 準備」の項目と同様である。

2.1.5　鍵および証明書の廃棄

以下に、この段階でエンドユーザ部門担当者が作業する際の留意事項と対策を示す。

(1) 証明書の失効

証明書はそれに対応する鍵の安全性が確保されているといった条件の範囲内で使用されるものであるが、秘密鍵の不正コピー、秘密鍵保管媒体の盗難、紛失などが発生し鍵の安全性が保証できなくなった場合は、証明書を無効にする処置として「証明書の失効」を行う必要がある。

証明書の失効手続きについては、「認証局の運用規定に記載された手続き」や「社内システム管理部門が定めた手順」などに従い実施する必要があるが、実施する作業の例としては、「認証局への速やかな証明書の失効申請」や「新しい証明書の再発行要求」などが挙げられる。

(2) 秘密鍵の廃棄

「証明書の失効」で記述した状況等により証明書を失効した場合、あるいは鍵や証明書の利用をやめる場合などの際には、保管している秘密鍵を速やかにかつ完全に廃棄する必要がある。

廃棄する手段の例としては、「ＩＣカードを物理的に破壊する」や「ＩＣカードを社内システム管理部門へ返却し廃棄処理を依頼する」、「ＨＤ等へ保管している場合は、フォーマットした上で無意味なデータを繰り返し上書きしておく」などが挙げられる。

2.1.6　署名検証

以下に、この段階でエンドユーザ部門担当者が作業する際の留意事項と対策を示す。

(1) 信頼点の操作

署名検証（証明書検証）のよりどころとなる信頼点に関する操作は、不正な追加や変更などが行われないよう利用者本人自らあるいは権限を持つもの（社内システム管理部門）が行う必要がある。

(2) 信頼点証明書の追加

信頼点の証明書を追加する場合は、その証明書に対する署名検証、有効性確認及び失効状況等に問題が無いことを確認した上で行う、あるいは、運用規定などで定められた手段で確認した上で追加操作を行う必要がある。

証明書の確認方法の例としては、「雑誌や新聞などで広報された証明書のフィンガープリントと一致していることを確認する」などが挙げられる。

(3) 信頼点の確認

信頼する信頼点の情報を定期的に確認し、信頼点リストに不審な信頼点が追加されていないことを確認する必要がある。

(4) 署名範囲の確認

ＸＭＬ署名などの部分署名がされている文書を検証する場合は、真正性を必要とする部分が署名対象範囲に含まれていることを確認する。

(5) 署名付文書の保管

受け取った署名付文書は、否認拒否の対応など再検証に備えて保管することがある。この場合、正しく検証ができるよう、署名付文書と併せて「署名検証に用いる証明書」「その証明書のその時点の失効情報（ＣＲＬやＯＣＳＰ応答など)」「その時点の信頼点情報」とを、保管する必要がある。

2.2　システム管理部門

2.2.1　準備

以下に、この段階でシステム管理部門担当者が作業する際の留意事項と対策を示す。

(1) 電子署名の理解

電子署名の利用者（エンドユーザ部門担当者）が安全な運用が行えるよう、予め電

子署名について理解しておく必要がある。また、必要に応じて安全な運用を行うための手引書などを作成しエンドユーザ部門に配布することも有効である。

電子署名を理解するための情報源の例としては、「電子署名法あるいはその解説書」や「電子署名を使用するアプリケーションソフトウェア文書（マニュアルなど）」などが挙げられる。

(2) 適正なソフトウェアの利用

ソフトウェア自体のセキュリティホールからシステム全体の安全が脅かされる恐れもあるので、セキュリティ対策が施された信頼できるソフトウェアを選定する必要がある。

ソフトウェアの選択に際しては、既存の評価基準や認定基準などを参考にするとよい。ソフトウェアの選択基準の例としては、「セキュリティ評価基準(ＩＳO15408)準拠の製品」や「本ガイドラインの第Ⅳ部に適合した製品」などが挙げられる。

また、古いバージョンのソフトウェアには、セキュリティ上の問題点がある場合もあり、適切なバージョンのソフトウェアを取得する必要がある。

(3) ソフトウェアの適正な入手

不正なプログラムと差し替えられることがないよう、ソフトウェアは適正な手段で入手し安全に保管管理する必要がある。

適正な入手手段の例としては「正規の販売ルートによる購入し、エンドユーザ部門担当者へ直接提供する」「評価プロダクトと実際に利用する製品は分離して管理する」などが挙げられる。

(4) セキュリティ情報の入手

利用するアプリケーションやＯＳ等のセキュリティ情報（セキュリティホール、関連ウィルス情報等）を入手し、自分のシステム内にセキュリティホールを残さないようにする必要がある。また、入手したセキュリティ情報は、必要に応じて整理したり対策方法を併記するなどして、エンドユーザ部門に配布することも有効である。

セキュリティ情報の入手手段の例としては「ベンダーが公表する情報の定期的な確認」や「情報処理振興事業協会等の第三者機関が発表する情報の定期的な確認」などが挙げられる。

(5) ウィルスチェックの実施

コンピュータウィルスの感染により利用しているソフトウェアあるいはシステム全

体のセキュリティが脅かされる恐れもあるので、ウィルスの感染防止と早期発見のために定期的な監視などの対策をとる必要がある。また、あわせてエンドユーザ部門に対しても、同様の指導をすることも有効である。

ウィルス対策の例としては、「ウィルス対策ソフトウェアの導入」や「ウィルス情報ファイルの定期更新」、「ウィルス感染監視の自動化」などが挙げられる。

(6) 信頼できる認証局の選定

証明書の発行申請・取得にあたっては、認証局の信頼性について充分理解し、利用目的に応じた信頼できる認証局を選定する必要がある。また、必要に応じて社内認証局を構築し安全に管理・運営した上で、エンドユーザ部門へ証明書を発行することも有効である。

信頼される認証局の例としては、「『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）』（電子署名法）に基づく特定認証業務の認定を受けている認証局」、「電子署名を利用するアプリケーションを提供する組織（取引業界団体など）で選定された認証局」、「運用実績のある認証局」、「認証局運用規定を公開し、かつ適切に運用している認証局」などが挙げられる。

(7) 証明書の適切な申請・取得

認証局から証明書を申請し取得する際は、適切で信頼できる方法で行う必要がある。必要に応じてエンドユーザ部門に対して「認証局の運用規定を明示する」などして、具体的な手順を示すことも有効である。

適切な申請・取得方法の例としては、「選定した認証局の運用規定に記載された申請・取得方法に従う」などが挙げられる。

(8) 証明書の記載事項の確認

証明書は本人認証のよりどころとなると同時に他者に配布するものであるため、発行された証明書の記載事項を表示ツール等により確認する必要がある。また、その旨をエンドユーザ部門へ指導することも有効である。

確認する項目の例としては、「発行対象者名や証明書用途などが申請内容と一致しているか」や「プライバシー情報が記載されていないか」などが挙げられる。

(9) コンピュータシステム内日時合わせ

電子署名を利用する際の日時は、電子署名を利用するマシンの内部時計（システム日時）が使用されるため、署名生成側と署名検証側との日時が異なると、証明書の有

効期限検証を含む日時に関連する署名検証が正しく行われないことにつながる。これを防ぐため、システム日時を正しく設定し維持する必要がある。また、その旨をエンドユーザ部門へ指導することも有効である。

システム日時の設定と維持の方法の例としては、「ＧＰＳを利用した時刻同期」や「時刻同期サーバ（ＮＴＰサーバ）の利用」などが挙げられる。

2.2.2　鍵および本人識別情報の管理

以下に、この段階でシステム管理部門担当者が作業する際の留意事項と対策を示す。

(1) 秘密鍵の鍵長の選定

エンドユーザ部門が電子署名に使用する秘密鍵について、業務要件や利用アプリケーションなどを考慮し、適切な鍵長を選択し指導することが有効である。

鍵長の例としては、「ＲＳＡ鍵の場合は、1024bit」などが挙げられる。

(2) 秘密鍵の保管媒体

決済を伴う電子署名に使用する秘密鍵の保管媒体として、鍵が不正にコピーされたりしないよう安全な媒体を選定し、エンドユーザ部門に対して指導することが有効である。

安全な保管媒体の例としては、「耐タンパ媒体（ＩＣカード等）」などが挙げられる。

(3) 秘密鍵保管媒体の管理

秘密鍵保管媒体は、紛失や不正持ち出しが起きないように安全に保管する必要があり、その旨をエンドユーザ部門に対して指導することが有効である。

安全な保管方法の例としては、「ＩＣカードを鍵つきの引き出しに保管」や「ＩＣカードの常時携帯」、「入退出記録や利用記録の採取と定期的な確認」などが挙げられる。

(4) 秘密鍵複製の制限

秘密鍵が不正にコピーされないよう、予めバックアップも含め複製は行わないように規定しておく必要がある。

2.2.3　署名生成

以下に、この段階でシステム管理部門担当者が作業する際の留意事項と対策を示す。

(1) **作業場所の入退室管理**

署名データを作成する場所に不正な入退出がないよう、入退出者の管理を行う必要がある。

入退出管理方法の例としては、「作業場所は施錠した上、許可を持つもののみ入室可能とする」や「ハードウェアトークンによる認証機構を備えた扉を設置し許可された人しか入室させない」、「入退出履歴を記録として保管し、定期的に確認する」などが挙げられる。

(2) **操作ログの管理**

不正な利用の発見のために、操作の履歴を保存し定期的に確認する必要がある。

操作ログの運用の例としては、「操作ログが採取できるソフトウェアを利用する」や「操作ログの改ざん検出のために、署名を行った上で保管する」、「操作ログの改ざん防止のために、ＣＤ－Ｒなどの書き換えできない媒体に保管する」などが挙げられる。

2.2.4　鍵および証明書の更新

以下に、この段階でシステム管理部門担当者が作業する際の留意事項と対策を示す。

(1) **証明書の更新**

証明書は有効期間が設定されその期間内での使用のみ有効と判断されるため、引き続き証明書の利用及び電子署名の利用を必要とする場合は、有効期限内に新しい証明書の更新を当該認証局へ申請する必要がある。システム管理部門が、エンドユーザ部門の証明書を管理している場合は、有効期間の終了前にエンドユーザ部門担当者に更新を促す連絡を行うことも有効である。

証明書の更新に伴う申請および取得に際しての留意事項と対策は、「2.2.1　準備」の項目と同様である。

2.2.5　鍵および証明書の廃棄

以下に、この段階でシステム管理部門担当者が作業する際の留意事項と対策を示す。

(1) **証明書の失効**

証明書はそれに対応する鍵の安全性が確保されているといった条件の範囲内で使用されるものであるが、秘密鍵の不正コピー、秘密鍵保管媒体の盗難、紛失などが発生

し鍵の安全性が保証できなくなった場合は、証明書を無効にする処置として「証明書の失効」を行う必要がある。必要に応じて、エンドユーザ部門に対して、失効すべき状態を説明した上で、そのような事態が発生した場合は速やかに失効手続きをとるよう指導することも有効である。

証明書の失効手続きについては、「認証局の運用規定に記載された手続き」などに従い実施する必要があるが、実施する作業の例としては、「認証局への速やかな証明書の失効申請」や「新しい証明書の再発行要求」などが挙げられる。

(2) **秘密鍵の廃棄**

「証明書の失効」で記述した状況等により証明書を失効した場合、あるいは鍵や証明書の利用をやめる場合などの際には、保管している秘密鍵を速やかにかつ完全に廃棄する必要がある。必要に応じて、エンドユーザ部門に対して鍵の廃棄方法を指導することも有効である。

廃棄する手段の例としては、「ＩＣカードを物理的に破壊する」や「ＩＣカードを社内システム管理部門へ返却し廃棄処理を依頼する」、「ＨＤ等へ保管している場合は、フォーマットした上で無意味なデータを繰り返し上書きしておく」などが挙げられる。

2.2.6　署名検証

以下に、この段階でシステム管理部門担当者が作業する際の留意事項と対策を示す。

(1) **信頼点の操作の制限**

署名検証（証明書検証）のよりどころとなる信頼点に関する操作は、不正な追加や変更などが行われないよう利用者本人自らあるいは権限を持つもの（社内システム管理部門）が行う必要がある。必要に応じて、エンドユーザ部門に対してその旨を指導することも有効である。

(2) **信頼点証明書の追加**

信頼点の証明書を追加する場合は、その証明書に対する署名検証、有効性確認及び失効状況等に問題が無いことを確認した上で行う、あるいは、運用規定などで定められた手段で確認した上で追加操作を行う必要がある。必要に応じて、エンドユーザ部門に対してその旨を指導することも有効である。

証明書の確認方法の例としては、「雑誌や新聞などで広報された証明書のフィンガ

ープリントと一致していることを確認する」などが挙げられる。

(3) 信頼点リストの管理

信頼する信頼点の情報を定期的に確認し、信頼点リストに不審な信頼点が追加されていないことを確認する必要がある。必要に応じて、エンドユーザ部門に対してその旨を指導することも有効である。

(4) 署名付文書の保管

受け取った署名付文書は、否認拒否の対応など再検証に備えて保管することがある。この場合、正しく検証ができるよう、署名付文書と併せて「署名検証に用いる証明書」「その証明書のその時点の失効情報（ＣＲＬやＯＣＳＰ応答など）」「その時点の信頼点情報」とを、保管する必要がある。

第Ⅳ部　電子署名利用者システム開発の指針

電子署名の生成・検証機能を提供するプログラムは、ソフトウェアベンダー等の開発者などが作成したものを利用者が使用するというケースが一般的である。そのため、利用者が安全に電子署名を行うために、ソフトウェア開発者は、安全性や利便性を考慮したソフトウェアを提供する必要がある。

ここでは、PKIライブラリなどの「署名プログラム」及びセキュアメール、インターネット・ショッピング、EDI等の電子署名を使用した、「アプリケーション・プログラム」の開発者に対するガイドラインを示す。「署名プログラム」や「アプリケーション・プログラム」を開発するにあたり、利便性を向上させる上で配慮すべきポイントと、安全性を確保するための留意事項及び対策について説明する。

1　利便性向上のための配慮

電子署名生成・検証や関連するシステム管理・運用を利用者が容易に、かつ確実に行うことを支援する為にアプリケーション及び電子署名生成・検証ソフトウェアの開発者が考慮すべき利便性向上のための事項をまとめる。

1.1　目的

利便性には、誤操作に対する対策、簡易性（利用者の理解を深める解説、処理手順の自動化・ＧＵＩの分かり易さ）、汎用性（色々な業務、方式への対応性）、その他の配慮がある。

誤操作に対する対策と簡易性・汎用性の間には、一方を強化すると、他方が低下する関係があり、アプリケーションの性質により、どちらを優先するかを考慮する必要がある。

また利便性向上の為の配慮と利用者の留意事項と対策（第Ⅱ部第 3 章、第Ⅲ部第 2 章）は、密接な関係にあり、利便性を向上する為には、利用者の留意事項を解説、マニュアル化しなければならない。

なお、アプリケーション、電子署名生成、検証ソフトウェアの技術的なセキュリティ機能は、ここでは記述せず次章で記述している。配慮事項の網羅性については、メール・インターネット・ショッピング、企業間電子商取引のケースをモデルとして抽出し、重要と思われる項目を上げている。アプリケーション構築時にこれらの項目を参考にされたい。

以下では、項目毎に、具体的な対策を記述し、対策毎に、メール・インターネット・ショッピング・企業間電子商取引の利用者システムを構築する上で必要かどうかの根拠・解説を付加している。ここでの各モデル（メール・インターネット・ショッピング・企業間電子商取引）の違いは、取り扱う情報資産価値の違いを主な項目の採否の観点としている。

※下記の解説では、必要な対策に関する文章を断定的に記述しているが、必ず必要な要件の項目としてではなく、検討が必要な項目として参考にされたい。表-付録 3- 2に利便性向上のために、開発者が配慮すべき事項の一覧表を付加している。

1.2　誤操作に対する配慮

1.2.1　証明書内容の分かり易い表示

証明書内容を表示する場合に「定義された用語」で、容易に理解できる説明を表示す

る。署名生成時は、利用者が、署名に利用する秘密鍵を特定するために対応する証明書内容を表示する。また署名検証時は、利用者が署名検証した相手証明書内容を知りたい時、署名検証する相手証明書の信頼点の証明書を信頼するかを判断するために以下の配慮が必要となる。

(1) **平易な表現での証明書内容表示**

証明書の内容は、非常に重要な情報である為、全てのサービス（メール・インターネット・ショッピング・企業間電子商取引）で必要である。

(2) **証明書の解説書／ヘルプ機能の装備**

取り扱う情報資産の価値が高く、企業間取引である企業間電子商取引では、必要である。

(3) **証明書の発行者の情報表示**

(2)　と同様。

(4) **証明書内容について、重要度の表示**

証明書の基本領域については、必ず表示する。また、拡張領域において、重要（critical）とされている領域について、判別できるように表示する。

［備考］相手のルート認証局の証明書が信頼できるかどうかは、個々人が判断することは難しい。モデル（メール、インターネット・ショッピング、企業間電子商取引）毎に判断の基準を作ることが望ましい。

1.2.2　認証局情報の容易な入手

利用者が信頼する（証明書を要求する）認証局の選択時、または相手のルート認証局の証明書が信頼できるか判断する時に認証局情報を容易に入手可能なこと。

(1) **証明書ポリシー及び認証局の評価／認定情報を入手するための支援機能**

取り扱う情報資産の価値が高く、企業間取引である企業間電子商取引で必要である。

1.2.3　署名検証結果の分かり易い表示

利用者がその後の動作を判断できるように署名検証結果を分かり易く表示すること。特に検証失敗である場合には、その理由ととるべき動作が表示されるとよい。

(1) **署名の正否とともに、誰の署名であるかを証明書のサブジェクト名を基に正確かつ分かり易く表示**

署名検証は、基本機能である為、全てのモデル（メール、インターネット・ショッピング、企業間電子商取引）で必要である。

(2) **検証時に、相手の発行者の情報を表示**

取り扱う情報資産の価値が高く、企業間取引である企業間電子商取引で必要である。

1.2.4　親切なエラーメッセージ

(1) **利用者がとるべき動作について理解できるよう、エラー処置方法を明示することが望ましい**

署名・署名検証に関するエラーメッセージは、全てのモデル（メール、インターネット・ショッピング、企業間電子商取引）で必要である。

1.2.5　秘密鍵・証明書の選択支援

秘密鍵・証明書を選択するために、そのペアに対して利用者が命名できる等、選択のための支援を提供すること。

(1) **用途（適用ドメイン／アプリケーション、署名の意味等）など利用者が鍵ペアを区別するための情報を選択画面に記入でき、選択時にこれを表示する。**

1.2.6　利用者の遵守事項のガイド表示

秘密鍵・証明書に関して、利用者が守らなければならない事項についての該当操作を利用者が実行する場合に、表示すること。

取り扱う資産の価値が高く、企業間取引である企業間電子商取引では、必要な場合もある。

1.2.7　署名の意思確認の為のＧＵＩ

利用者が意思を持って署名したことを確認できるＧＵＩとすること。

(1) **明示的に署名をすることを示すメッセージ又は署名アイコン**

署名は、基本機能である為、全てのモデル（メール、インターネット・ショッピング、企業間電子商取引）で必要である。

1.2.8　パスワードの設定支援

パスワードは、秘密鍵保管やＩＣカードの所持者認証のために利用するが、パスワード設定について制限がある場合に設定支援を提供すること。

(1) **パスワード設定ガイド**

パスワードによる認証機能は、全てのモデル（メール、インターネット・ショッピング、企業間電子商取引）で必須であるが、パスワードの設定制限については、企業間電子商取引では必要と想定できる為、その設定ガイドも必要とする。

(2) **パスワード確認**

パスワードを設定する場合、再度パスワードを入力させるなど設定時の誤動作に関しての支援である。

(3) **パスワード更新**

初期パスワードなどが存在する場合、パスワード更新を促進するなどである。

1.2.9　署名の意味の表示・伝達

(1) **署名の付帯情報として、署名の意味（文責、照査、検認、認証等）情報を表示・伝達**

自分の署名の意味を表示伝達したい場合に、署名の付帯情報として署名の意味情報を表示・伝達できること。（現実世界で稟議書への文責、照査、検認、認証、の意味で署名する、著作物への著作者明示の意味で署名するなど）

1.2.10　ポータブルな秘密鍵

利用者の署名行為については固定場所で行うことに限定しないことが望ましい。

(1) **秘密鍵保管媒体として、ＩＣカード等の可搬媒体を採用**

秘密鍵は、全てのモデル（メール、インターネット・ショッピング、企業間電子商取引）で可搬媒体を利用することが望ましい。

(2) **カードを限定しない、オープンなインタフェースでのアクセス**

セキュリティ面から独自プロトコルを利用しても良いとも考えられる為、必要事項ではない。

1.3　汎用性に関する配慮

1.3.1　信頼点証明書更新時の利用者秘密鍵の継続使用

証明書を発行した認証局世代が異なる利用者間でも、それらの認証局証明書の有効期限が切れていない限り、お互いに署名検証可能とする手法である。

(1) **ＣＡ秘密鍵有効期限＜ＣＡ証明書有効期限とし、ＣＡ秘密鍵有効期限に合わせてＣＡの世代を交代**

かつ、

(2) **ＣＡ世代間で相互に証明書を発行（NewWithOld、OldWithNew の証明書も発行）し、ＣＡ世代間の認証パスを検証**

取り扱う資産の価値が高く、企業間取引である企業間電子商取引では、必要である。

1.3.2　署名付きであることの表示

利用者が一目で署名つきか否かを判断するために、表示できること。

(1) **署名付きであることを、アイコン、印影イメージ等によって明示**

基本機能の為、全てのモデル（メール、インターネット・ショッピング、企業間電子商取引）で必要である。

(2) **誰の署名であるかを証明書のサブジェクト名を基に正確かつ分かり易く表示**

基本機能の為、全てのモデル（メール、インターネット・ショッピング、企業間電子商取引）で必要である。

(3) **部分署名の場合は、署名範囲の表示**

企業間電子商取引では、部分的な署名も考えられ、取り扱う情報資産価値も高い為、必要である。逆に簡易性は損なわれる。

1.3.3　ワンタッチ・オペレーション

署名検証操作を簡易に行えるために（署名生成については、行わない）操作が簡便であること。

(1) **署名検証をできるだけワンタッチで実行**

(2) **パスワード入力を（１セッション単位につき）１回で済ませることを可能とすること**

業務内容が決定し、署名に必要な情報が事前に決定していれば、処理の自動化を行うことができる。また誤操作をなくす為にも、処理をできるだけ自動化する必要がある。簡易性は高くなるが、アプリケーションとの結合性が高くなる為、汎用性は低くなる。今回のモデル（メール、インターネット・ショッピング、企業間電子商取引）では必要としていない。

1.3.4　相互運用性及び保守性

他認証ドメインの証明書保持者との相互運用性を実現するために、相互認証認証局が発行した証明書について認証パスを構築することを可能とすること。

(1) **他のＣＡドメインに属する人とのやり取りが可能**

相互認証、又は他のＣＡドメインのルートＣＡ証明書を信頼点の一つとして登録

(2) **認証ポリシーに応じて、同一秘密鍵を複数アプリケーションで利用**

汎用性の観点からは、これらの項目はあってもよいが、逆に簡易性は低くなる。

1.4　その他の配慮

1.4.1　複数人でのマシンの共用

マシン数が少ない、などの理由によって複数人でのマシン共用が想定される場合があるが、この場合でも秘密鍵は個人で保持することとする。

(1) **同一マシン内での複数人の秘密鍵を管理（ＨＤ又は秘密鍵管理装置上）**

個人認証が厳密に行われるという条件下での利用が想定できる。

(2) **ＩＣカード等のポータブルな秘密鍵保管媒体を採用**

取り扱う資産の価値が高く、企業間取引である企業間電子商取引では、必要である。

2　安全性確保のための留意事項と対策

本章では、利用者システムの論理モデルを明確にするとともに、利用者システムに対する脅威を分析し、その対策をまとめる。

2.1　利用者システムの論理モデル

2.1.1　想定環境

利用者システムの論理モデルを構築する際に想定した環境を図-Ⅳ- 2-1に示す。

ただし、以降で詳述する論理モデルは、別環境においても適用可能なモデルである。

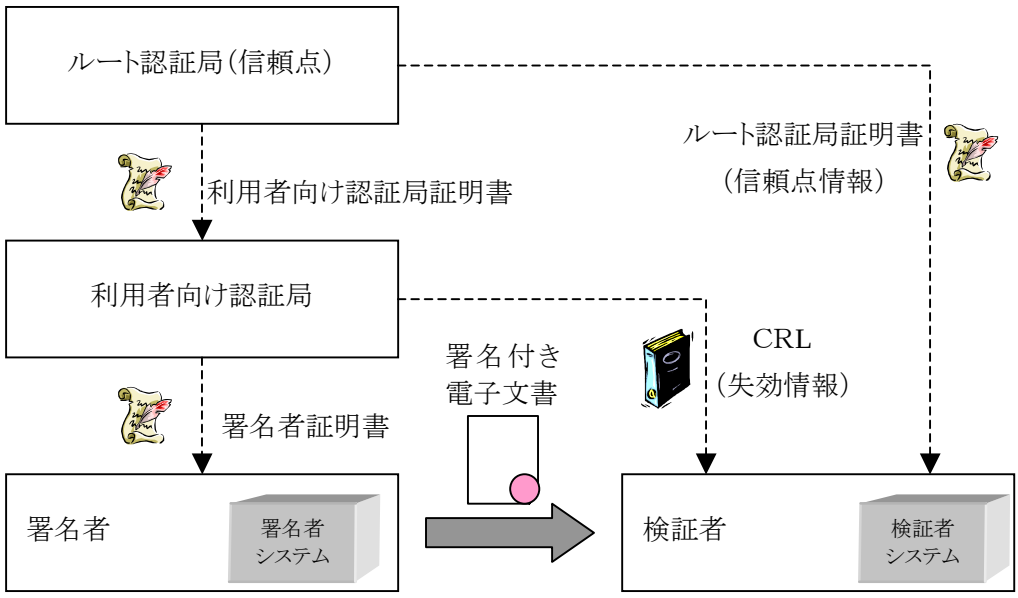

図-Ⅳ- 2-1　想定環境

2.1.2　概要

図-Ⅳ- 2-2は、利用者システムの論理モデルの概観を示す図である。図-Ⅳ- 2-2において、ＰＫＩアプリケーションとは、署名生成や署名検証を行うために、後述の署名プログラムを利用するアプリケーション・プログラム（例えば、電子メールソフトやＥＤＩプログラ

ム等）のことである。また、署名プログラムは、Basic　Function 部と Procedure 部からなる。Basic Function 部は、署名生成／署名検証等に関係する各種処理を実現する、アプリケーション非依存で単機能なプログラムの集合体である。Procedure 部は、ＰＫＩアプリケーションと Basic Function 部との間に介在し、Basic Function 部が提供する複数の機能をまとめた形でＰＫＩアプリケーションから利用可能とする。

一方、機能面で考えた場合、利用者システムは、電子署名生成に係わる鍵管理と署名生成、電子署名検証に係わる証明書管理と署名検証、および、利用者システム自体の運用管理に係わる利用者管理と監査ログ管理、といった 6 つのコンポーネントからなる。以降では、監査ログ管理を除く機能に関してより詳細に記述する。

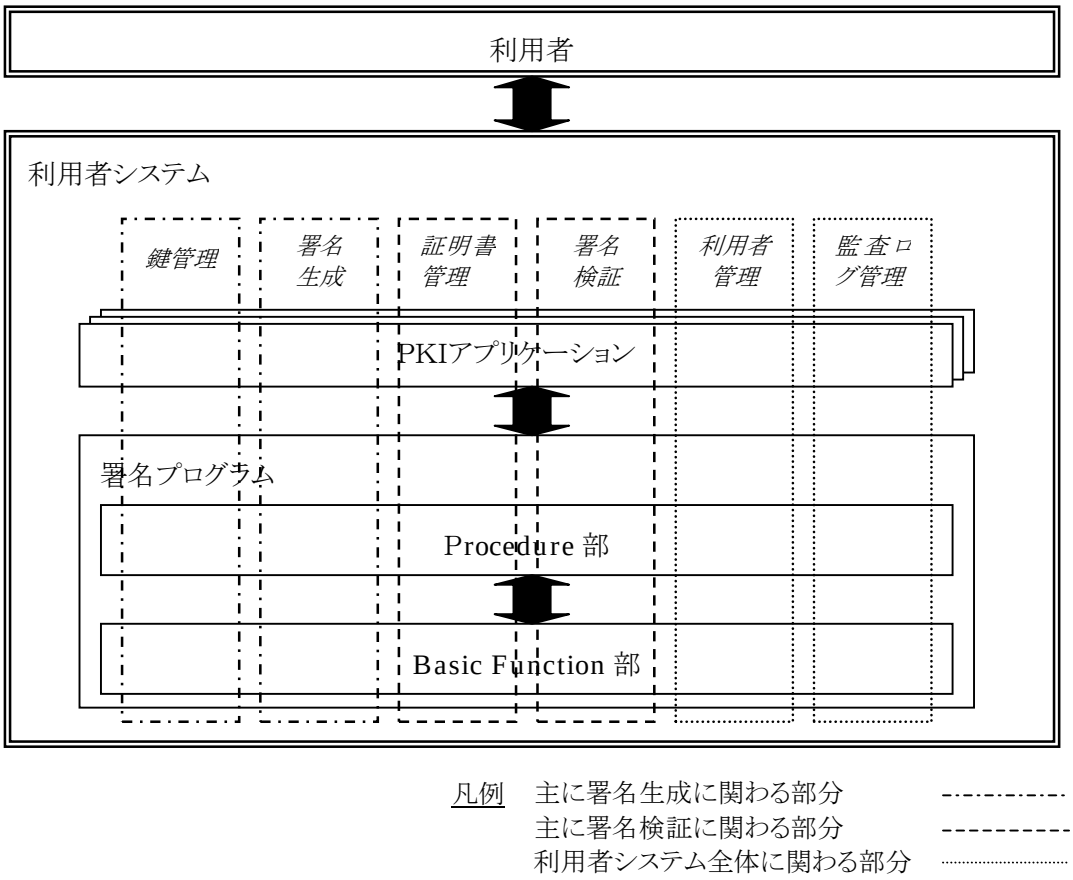

図-Ⅳ- 2-2　利用者システムの論理モデルの概観

2.1.3　利用者システムの使用手順

2.1.3.1　署名者の手順

署名者が利用者システムを使用する際の手順例を以下に示す。ただし、下記手順は、あくまでも一つの例であり、必ずしも全ての利用者システムがこの手順に従うものではない。

(1) **利用者システムの使用開始**

①　利用者の登録

利用者システムに自己の情報（ＩＤ、パスワード等）を登録する。

(2) **鍵ペア／証明書の新規作成**

①　ログイン

利用者システムにログインする。

②　鍵ペアの生成

自分用の鍵ペアを生成、保管する。

③　利用者向け認証局への公開鍵の登録

利用者向け認証局への署名者証明書の発行申請書を作成／送付し、利用者向け認証局から署名者証明書を発行してもらう。

④　ログアウト

利用者システムからログアウトする。

(3) **署名付き電子文書の生成／送付**

①　ログイン

利用者システムにログインする。

②　電子文書の作成

署名対象となる電子文書を作成する。

③　署名の生成

自分の秘密鍵を用いて上記電子文書に署名する。

④　ログアウト

利用者システムからログアウトする。

⑤　署名付き電子文書の送付

検証者に署名付き電子文書を送付する。

(4) **鍵ペア／証明書の更新（有効期限による更新、鍵漏洩による更新など）**

①　ログイン

利用者システムにログインする。

②　利用者向け認証局への署名者証明書の失効申請（鍵漏洩による更新の場合のみ）

前公開鍵を含む署名者証明書が有効期限内である場合には、利用者向け認証局への署名者証明書失効申請書を作成／送付する。

③　鍵ペアの廃棄

前鍵ペアを廃棄する。

④　鍵ペアの生成

自分用の新しい鍵ペアを生成、保管する。

⑤　利用者向け認証局への新公開鍵の登録

新公開鍵に関する利用者向け認証局への署名者証明書の発行申請書を作成／送付し、利用者向け認証局から新しい署名者証明書を発行してもらう。

⑥　ログアウト

利用者システムからログアウトする。

(5) **利用者システムの使用終了**

①　ログイン

利用者システムにログインする。

②　利用者向け認証局への署名者証明書の失効申請

署名者証明書が有効期限内である場合には、利用者向け認証局への署名者証明書失効申請書を作成／送付する。

③　鍵ペアの廃棄

鍵ペアを廃棄する。

④　ログアウト

利用者システムからログアウトする。

⑤　利用者の削除

利用者システムから自己の情報を削除する。

2.1.3.2　検証者の手順

検証者が利用者システムを使用する際の手順例を以下に示す。

(1) 利用者システムの使用開始

①　利用者の登録

利用者システムに自己の情報（ＩＤ、パスワード等）を登録する。

(2) 信頼ポイントの設定

①　ログイン

利用者システムにログインする。

②　信頼点情報の設定

自分の信頼するルート認証局証明書（信頼点情報）や証明書の失効リスト（ＣＲＬを利用する場合のみ）等を利用者システムに設定する（信頼点情報を後述の署名付き電子文書を検証するときに設定する場合もある）。

③　ログアウト

利用者システムからログアウトする。

(3) 署名付き電子文書の検証

①　署名付き電子文書の受取

署名者より署名付き電子文書を受け取る。

②　ログイン

利用者システムにログインする。

③　署名の検証

署名付き電子文書の署名を検証する。なお、署名検証を行う際には、署名者証明書および信頼点までの経路上の利用者向け認証局証明書が必要となる。それらの証明書は、署名付き電子文書とともに送られてくる場合もあるし、ディレクトリ等から検証者自身が入手する場合もある。

④　有効性の検証

上記署名検証に利用した署名者証明書および利用者向け認証局証明書が有効な（失効されていない）証明書であるか確認する。

⑤　ログアウト

利用者システムからログアウトする。

⑥　署名付き電子文書の閲覧

署名付き電子文書を閲覧する。

(4) 利用者システムの使用終了

①　利用者の削除

利用者システムから自己の情報を削除する。

2.1.4　アプリケーション－署名プログラム間のインタフェース

前章で記載した利用者システムの使用手順, および、ある利用者と他の利用者との識別、使用機器の変更などを考慮すると、アプリケーション－署名プログラム間のインタフェース（一部外部システムとのインタフェースも含む）は以下のようなものとなる。ただし、本インタフェースはあくまでも実装の一例でありアプリケーションや署名プログラムの仕様を限定するものではない。また、必ずしも全ての機能を備えている必要はない（以降のフロー図において、実線は基本機能を点線はオプション機能をそれぞれ表している）。

2.1.4.1　利用者管理インタフェース

(1)　利用者情報登録機能

利用者システムを使用する利用者の情報を登録する機能。利用者の名前や認証情報（パスワードや生体情報）などを入力すると、それら情報が利用者システム内のログイン情報や設定情報に追加され、その結果が利用者に通知される。本機能は、他機能に先立って利用されるものである。

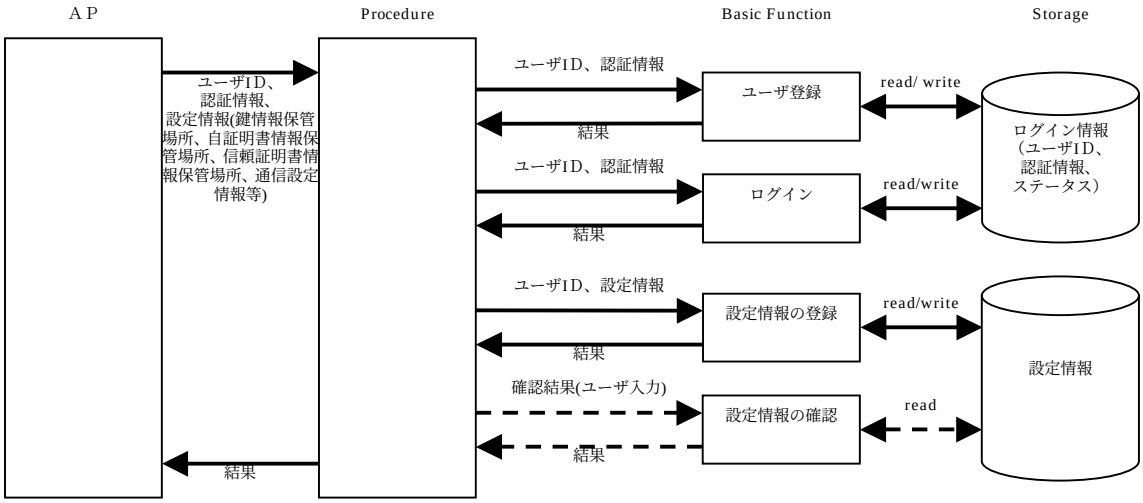

図-Ⅳ- 2-3　利用者情報登録機能

(2) 利用者情報修正機能

すでに登録されている利用者の情報を修正する機能。修正したい利用者の名前や認証情報などを入力して本人確認処理を行った後、修正情報を入力すると、利用者システム内のログイン情報や設定情報が修正され、その結果が利用者に通知される。

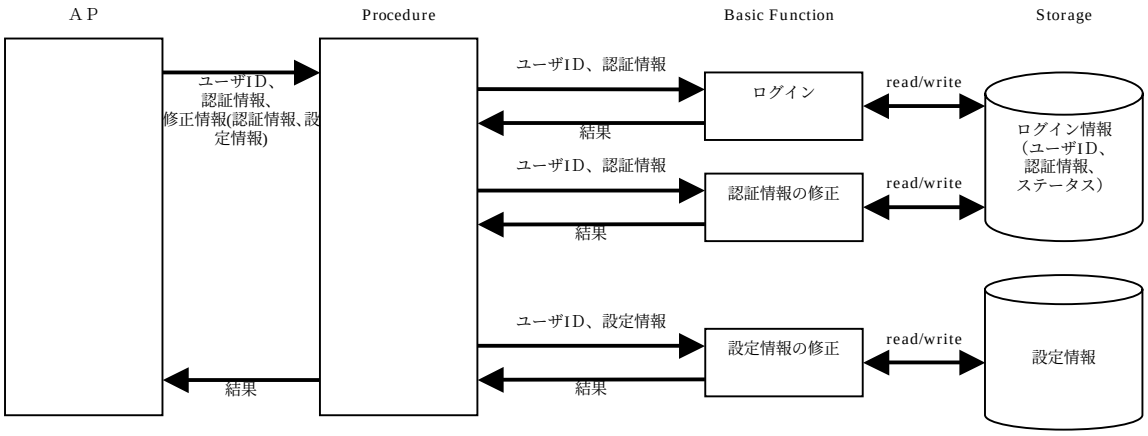

図-Ⅳ- 2-4　利用者情報修正機能

(3) 利用者情報削除機能

すでに登録されている利用者の情報を削除する機能。削除したい利用者の名前や認証情報などを入力して本人確認処理を行った後、利用者システム内のログイン情報や設定情報の当該項目が削除され、その結果が利用者に通知される。

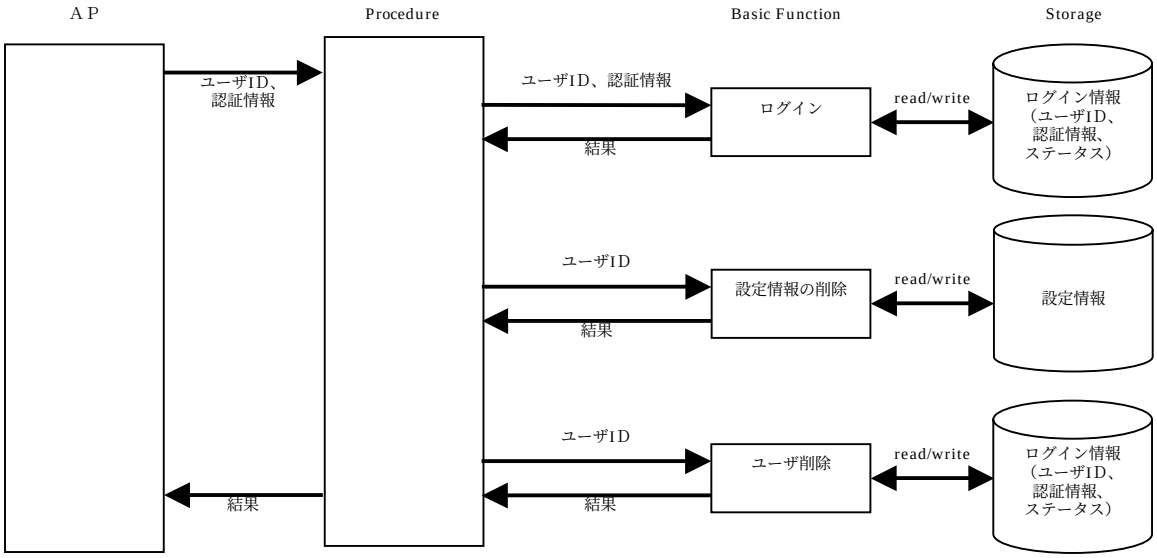

図-Ⅳ- 2-5　利用者情報削除機能

(4) ログイン機能

すでに登録されている利用者が利用者システムの使用を開始する機能。利用者の名前や認証情報などを入力すると、本人確認処理が行われ、その結果が利用者に通知される。本機能によって本人確認処理が正しく行われた場合にのみ、利用者管理インタフェース以外のインタフェースを利用することが可能となる。

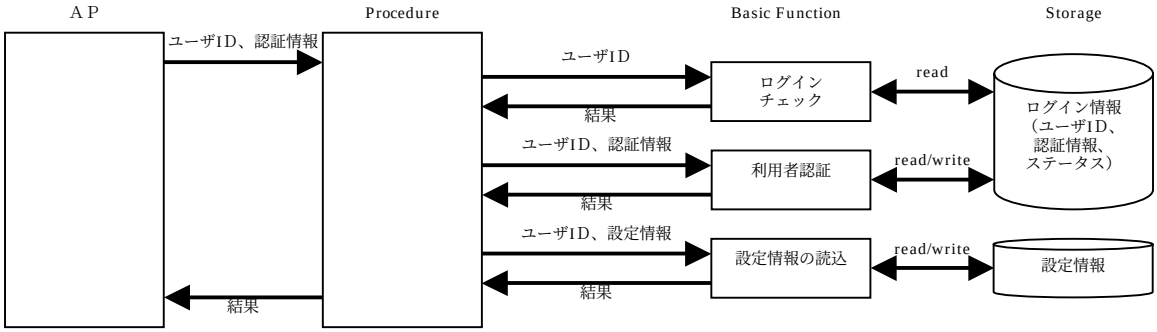

図-Ⅳ- 2-6　ログイン機能

(5) ログアウト機能

すでにログインしている利用者が利用者システムの使用を終了する機能。本機能は、すでにログインしている利用者がいるときにのみ使用可能な機能であり、本機能を実行するとその結果が利用者に通知される。

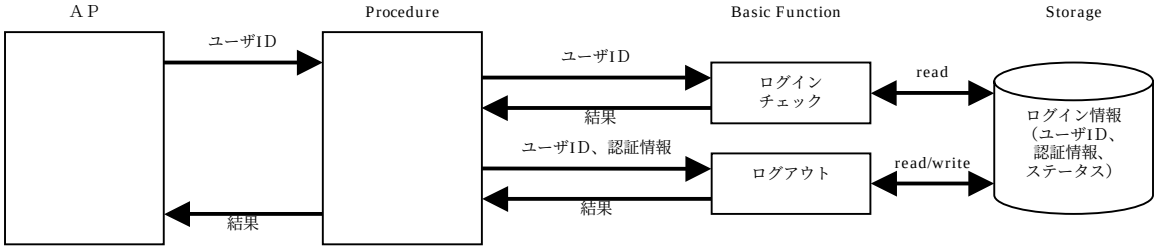

図-Ⅳ- 2-7　ログアウト機能

2.1.4.2　鍵管理インタフェース

(1) 鍵生成機能

現在ログインしている利用者用の鍵ペアを利用者システム内部で生成する機能。本機能を実行すると、利用者システム内に鍵ペアが生成され、その結果が利用者に通知される。

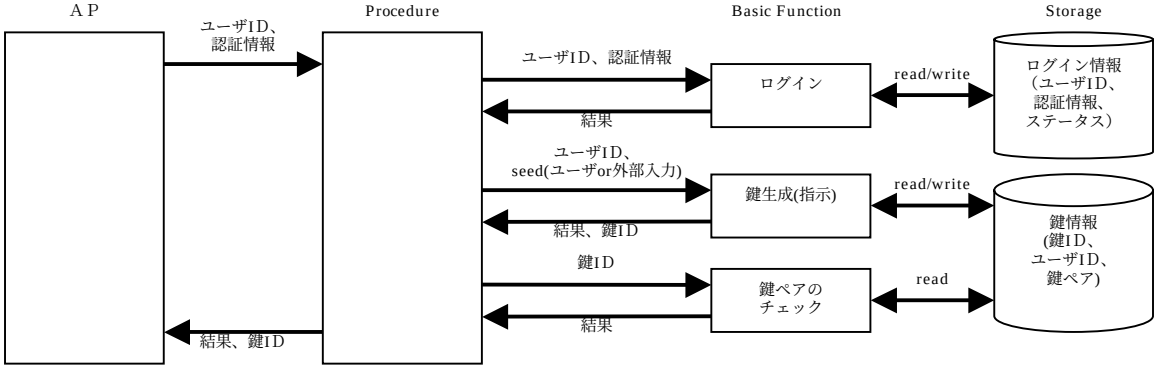

図-Ⅳ- 2-8　鍵生成機能

(2) 鍵入力機能

現在ログインしている利用者用の鍵ペアを利用者システム内部へインポートする機能。他の利用者システムで生成した鍵ペア（機器の変更等による鍵ペアの移動など）や利用者システム以外で生成した鍵ペア（管理部門による鍵ペアの一括した生成など）を入力すると、利用者システム内に鍵ペアがインポートされ、その結果が利用者に通知される。

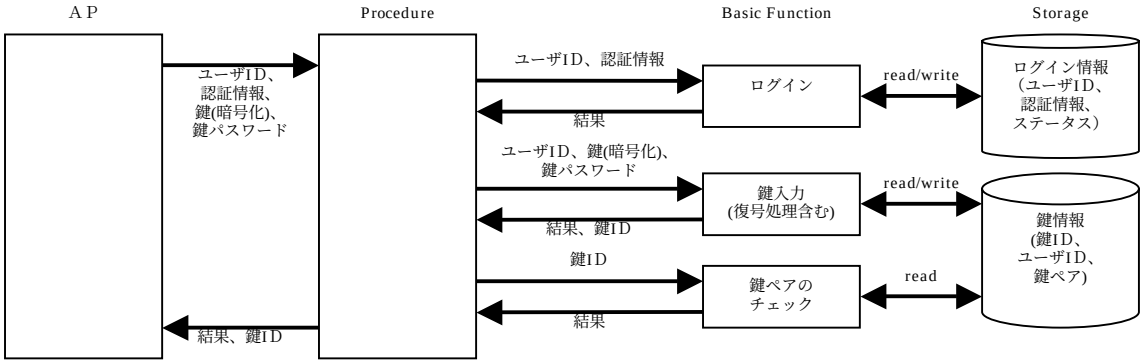

図-Ⅳ- 2-9　鍵入力機能

(3) 鍵出力機能

現在ログインしている利用者用の鍵ペアを利用者システム外部へエクスポートする機能。本機能を実行すると、利用者システム内にある鍵ペアが利用者システム外にエクスポートされ、その結果が利用者に通知される。

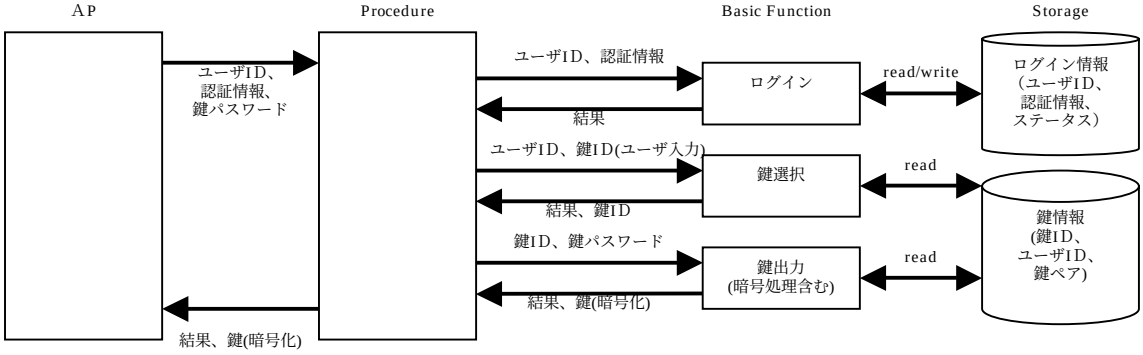

図-Ⅳ- 2-10　鍵出力機能

(4) 鍵廃棄機能

現在ログインしている利用者用の鍵ペアを利用者システム内部から削除する機能。本機能を実行すると、利用者システム内にある鍵ペアが削除され、その結果が利用者に通知される。

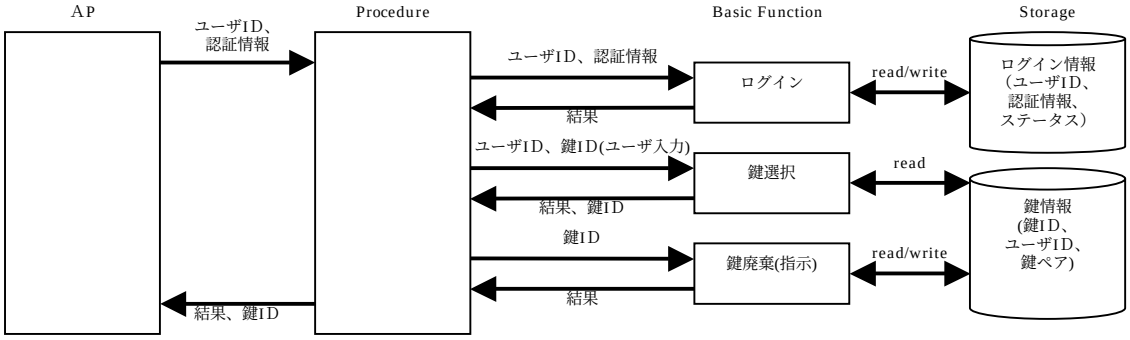

図-Ⅳ- 2-11　鍵廃棄機能

2.1.4.3　証明書管理インタフェース

(1) 署名者証明書オフライン取得（発行申請書作成）機能

現在ログインしている利用者用の署名者証明書をオフラインで取得するために必要な発行申請書を生成する機能。本機能を実行すると、署名者証明書発行に必要なデータ（利用者向け認証局への発行申請書）が生成され、その結果が利用者に通知される。

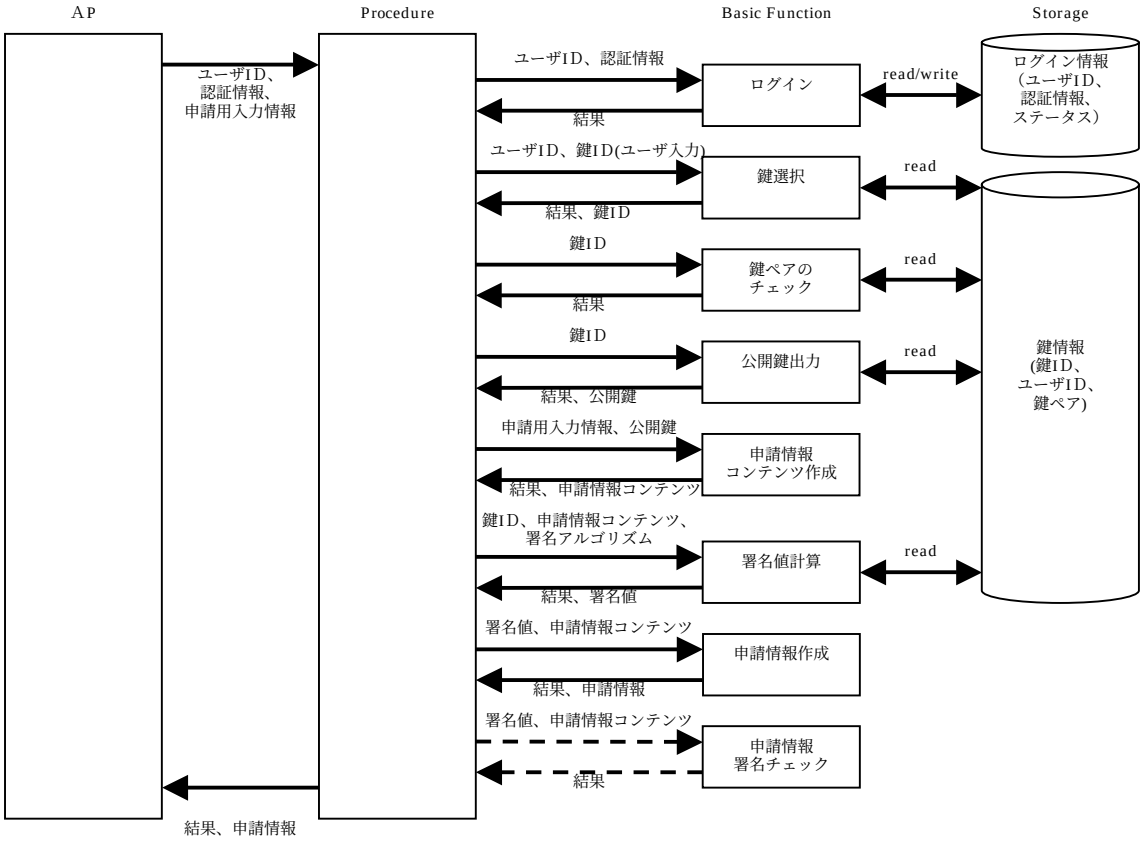

図-Ⅳ- 2-12署名者証明書オフライン取得機能

(2) 署名者証明書オンライン取得機能

現在ログインしている利用者用の署名者証明書をオンラインで取得する機能。本機能を実行すると、まず、署名者証明書発行に必要なデータ（利用者向け認証局への発行申請書）が生成される。次に、利用者向け認証局とオンラインで各種データのやり取りして、署名者証明書ならびに認証局証明書（利用者向け認証局証明書、ルート認証局証明書）が取得され、証明者証明書情報や認証局証明書情報に追加される。

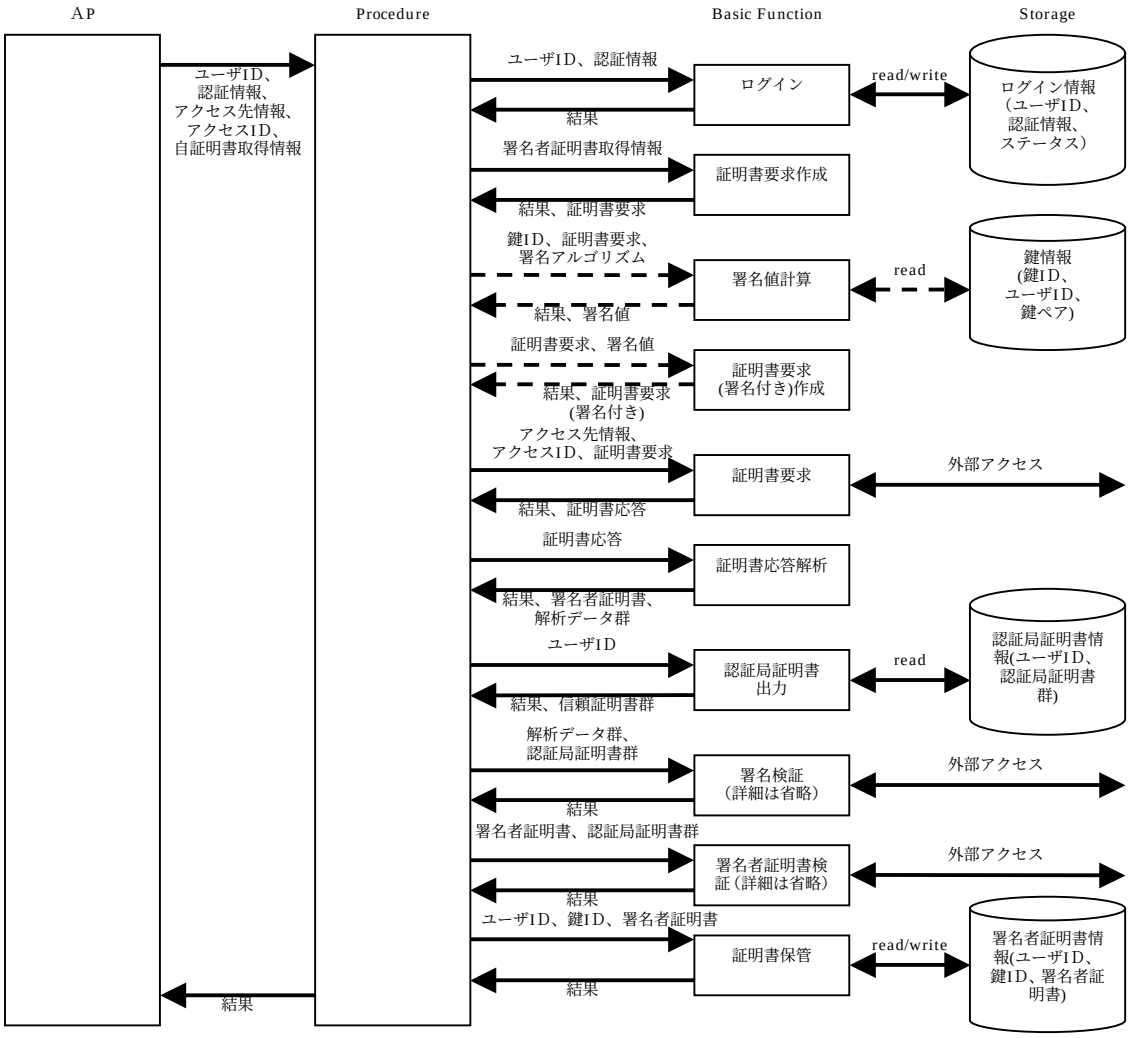

図-Ⅳ- 2-13　署名者証明書オンライン取得機能

(3)　署名者証明書入力機能

現在ログインしている利用者用の署名者証明書を利用者システム内部へインポートする機能。オフラインで入手した署名者証明書や、他の利用者システムで生成した署名者証明書、利用者システム以外で生成した署名者証明書などを入力すると、利用者システム内に当該利用者用の署名者証明書としてインポートされ、その結果が利用者に通知される。

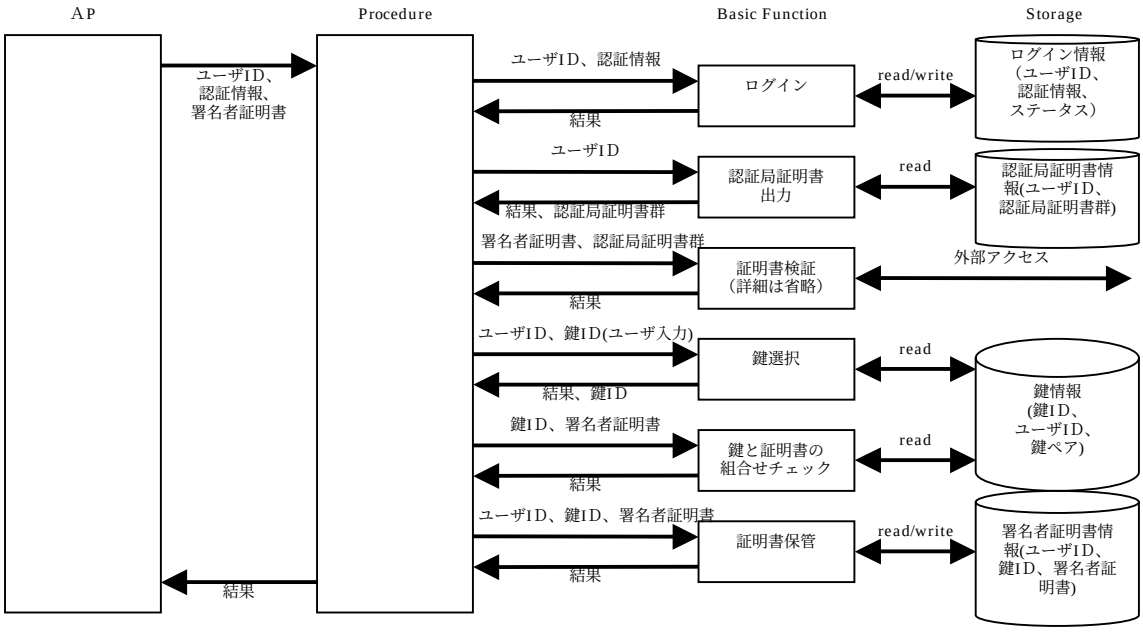

図-Ⅳ- 2-14　署名者証明書入力機能

(4) 署名者証明書出力機能

現在ログインしている利用者用の署名者証明書を利用者システム外部へエクスポートする機能。本機能を実行すると、利用者システム内にある当該利用者用の署名者証明書が利用者システム外にエクスポートされ、その結果が利用者に通知される。

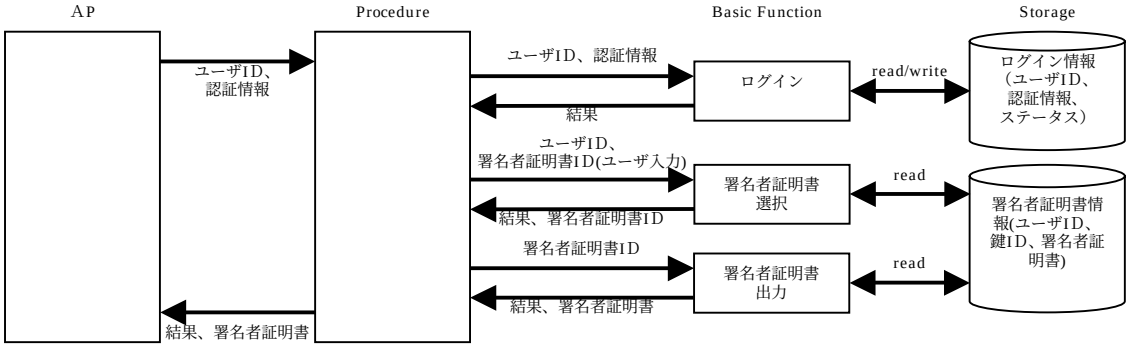

図-Ⅳ- 2-15　署名者証明書出力機能

(5) 署名者証明書削除機能

現在ログインしている利用者用の署名者証明書を利用者システム内部から削除する機能。本機能を実行すると、利用者システム内にある署名者証明書が削除され、その結果が利用者に通知される。

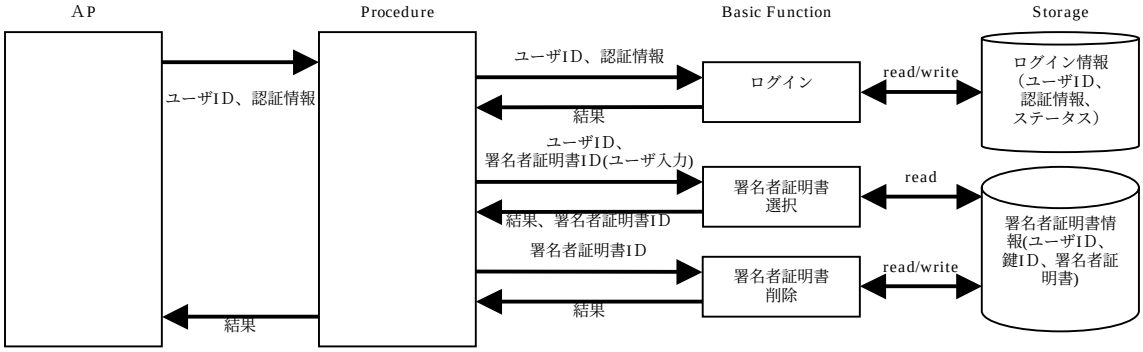

図-Ⅳ- 2-16　署名者証明書削除機能

(6) 署名者証明書オンライン失効機能

現在ログインしている利用者用の署名者証明書をオンラインで失効するための機能。本機能を実行すると、利用者システム内にある署名者証明書を失効するための処理が行われ、その結果が利用者に通知される。

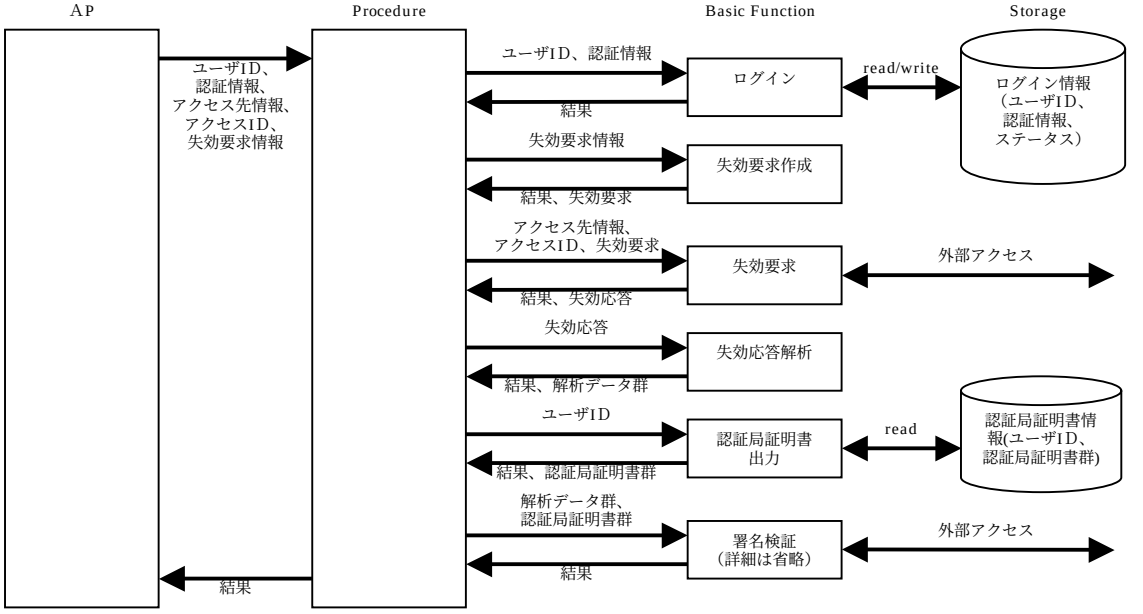

図-Ⅳ- 2-17　署名者証明書オンライン失効機能

(7) 認証局証明書オンライン取得機能

現在ログインしている利用者用の認証局証明書をオンラインで取得する機能。認証局証明書の取得先を入力すると、オンラインで認証局証明書が取得され、利用者システム内の認証局証明書情報に追加されるとともに、その結果が利用者に通知される。

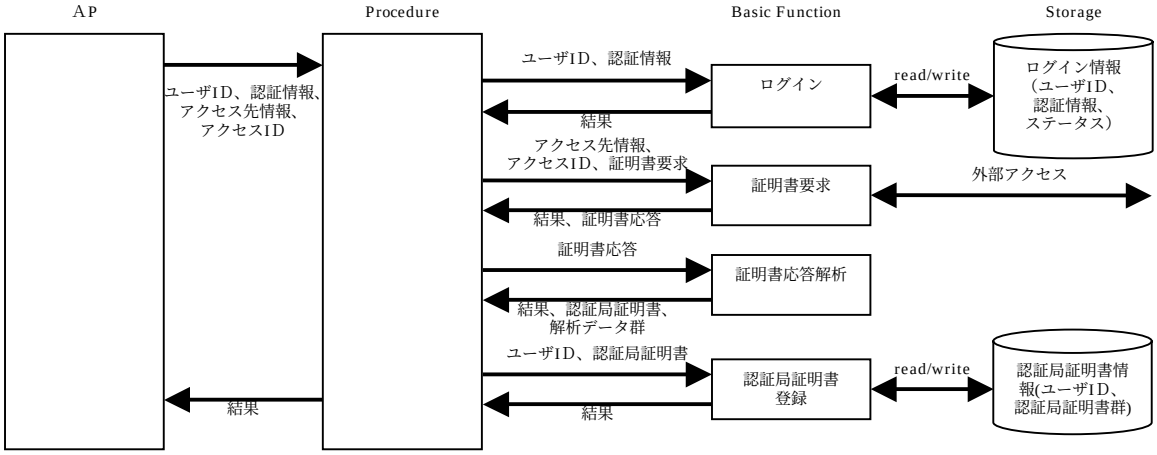

図-Ⅳ- 2-18　認証局証明書オンライン取得機能

(8) 認証局証明書登録機能

現在ログインしている利用者が信頼する認証局証明書を利用者システム内部へインポートする機能。認証局証明書を入力すると、それら情報が利用者システム内の認証局証明書情報に追加され、その結果が利用者に通知される。

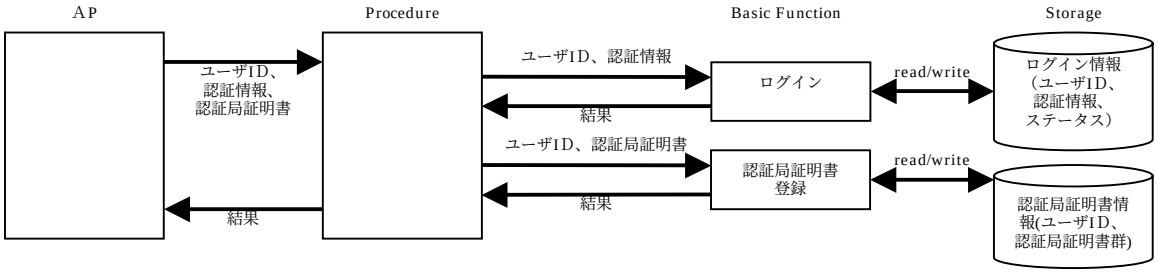

図-Ⅳ- 2-19　認証局証明書登録機能

(9) 認証局証明書削除機能

現在ログインしている利用者が信頼する認証局証明書を利用者システム内部から削除する機能。本機能を実行すると、利用者システム内にある認証局証明書が削除され、その結果が利用者に通知される。

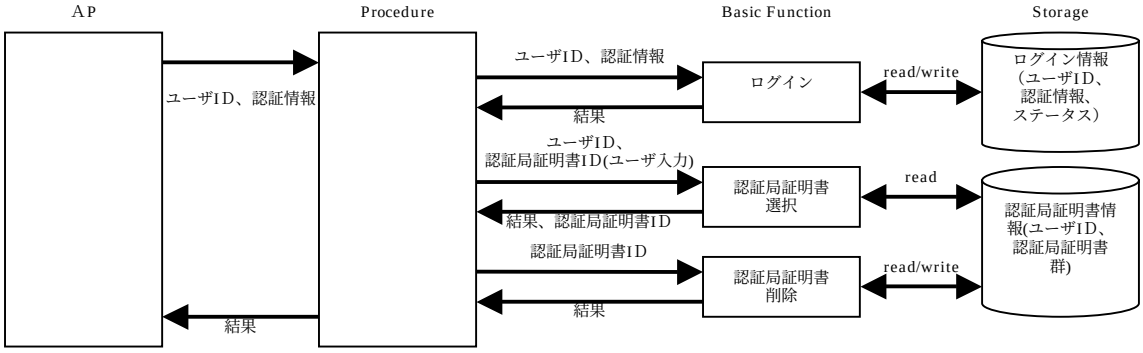

図-Ⅳ- 2-20　認証局証明書削除機能

(10) ＣＲＬオンライン取得機能

現在ログインしている利用者用のＣＲＬをオンラインで取得する機能。ＣＲＬの取得先を入力すると、オンラインでＣＲＬが取得され、利用者システム内のＣＲＬ情報に追加されるとともに、その結果が利用者に通知される。

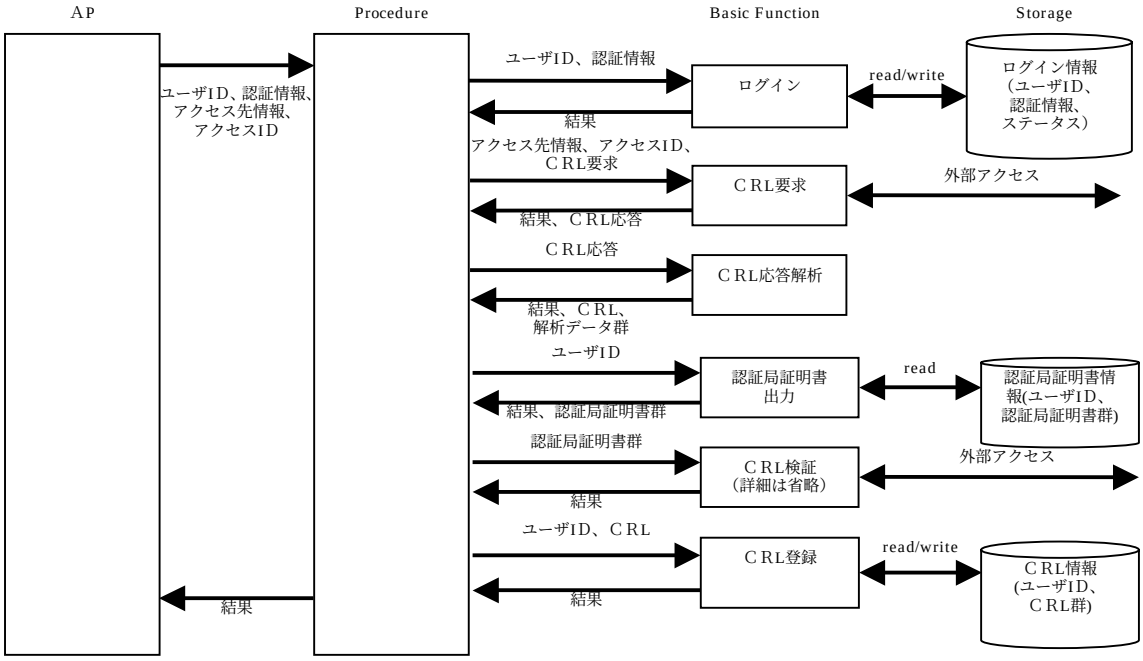

図-Ⅳ- 2-21　CRLオンライン取得機能

(11) ＣＲＬ登録機能

現在ログインしている利用者用のＣＲＬを利用者システム内部へインポートする機能。ＣＲＬを入力すると、それら情報が利用者システム内のＣＲＬ情報に追加され、その結果が利用者に通知される。

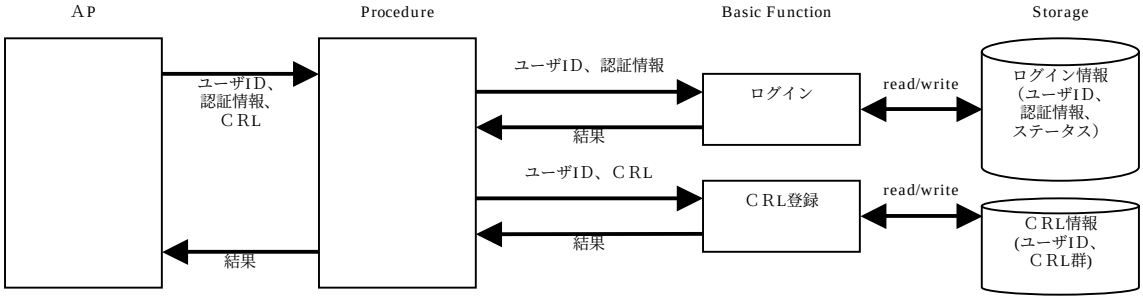

図-Ⅳ- 2-22　CRL登録機能

(12) ＣＲＬ削除機能

現在ログインしている利用者用のＣＲＬを利用者システム内部から削除する機能。本機能を実行すると、利用者システム内にあるＣＲＬが削除され、その結果が利用者に通知される。

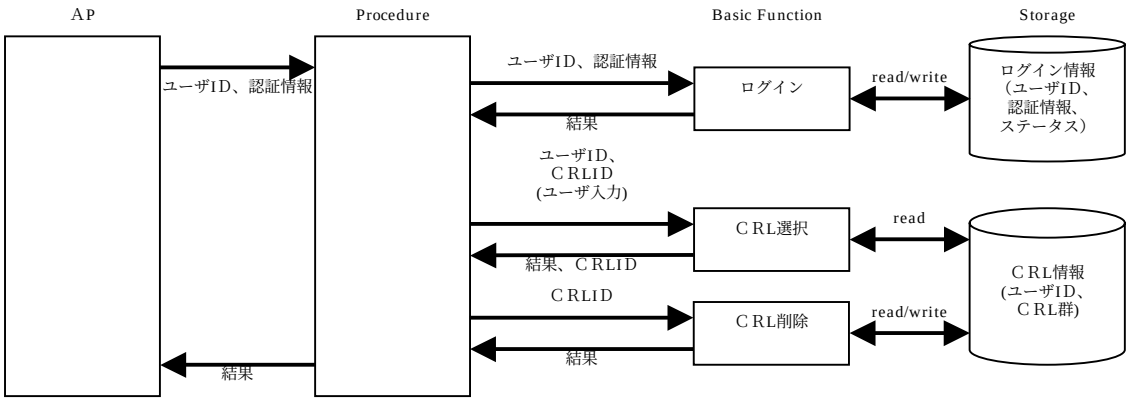

図-Ⅳ- 2-23 CRL削除機能

2.1.4.4　署名生成インタフェース

(1) 署名生成機能

現在ログインしている利用者の電子署名を生成する機能。電子署名を施す対象となる電子文書を指定すると、当該電子文書に対して利用者の電子署名が施されたのち、当該利用者の署名者証明書が添付され、署名付き電子文書が生成されて、その結果が利用者に通知される。

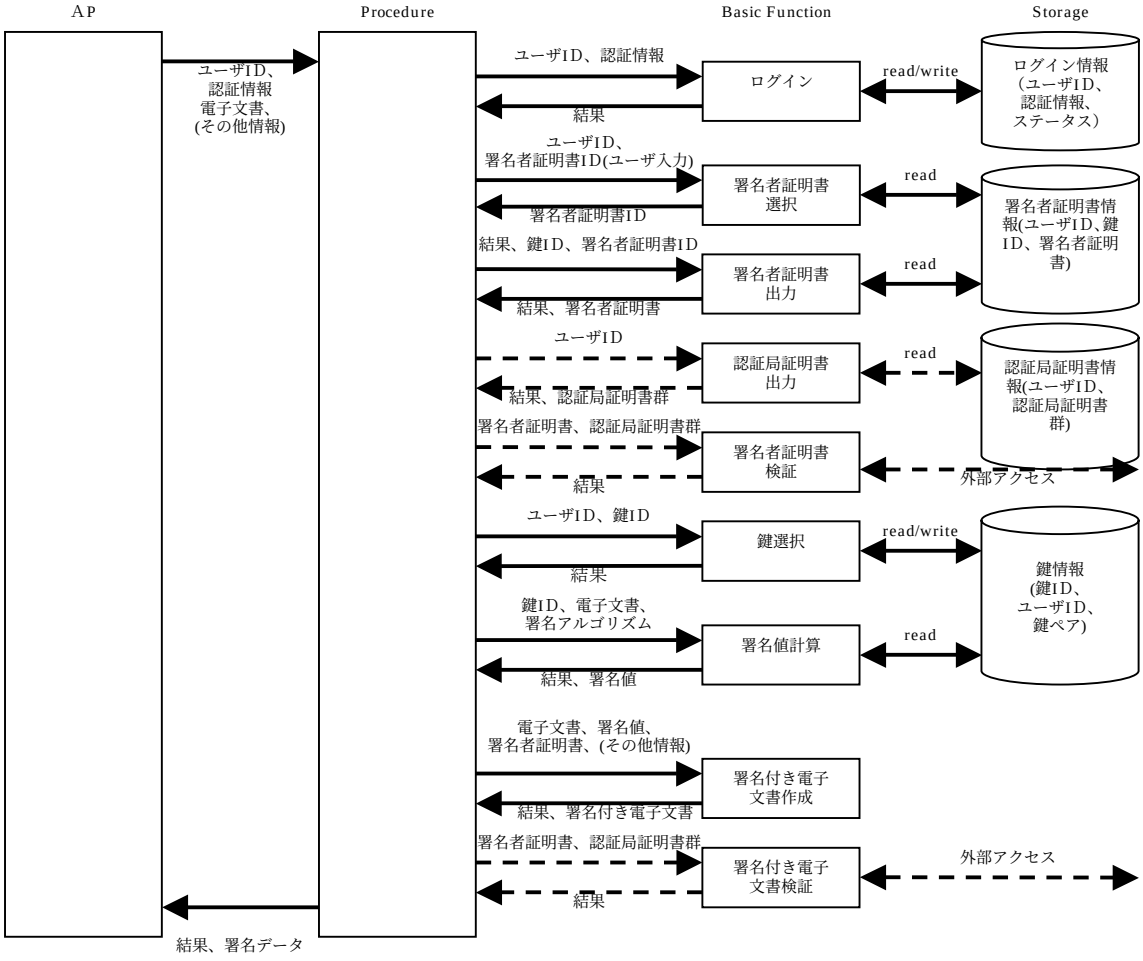

図-Ⅳ- 2-24　署名生成機能

2.1.4.5　署名検証インタフェース

(1) 署名検証機能

署名付き電子文書に含まれる署名者の署名者証明書と、現在ログインしている利用者の信頼点情報（認証局証明書情報内のルート認証局証明書）などに基づいて電子署名を検証する機能。電子署名の検証を行う対象となる署名付き電子文書を指定すると、署名付き電子文書に含まれる署名者の署名者証明書と当該利用者の信頼点情報などに基づいて電子署名の検証が行われ、その結果が利用者に通知される。

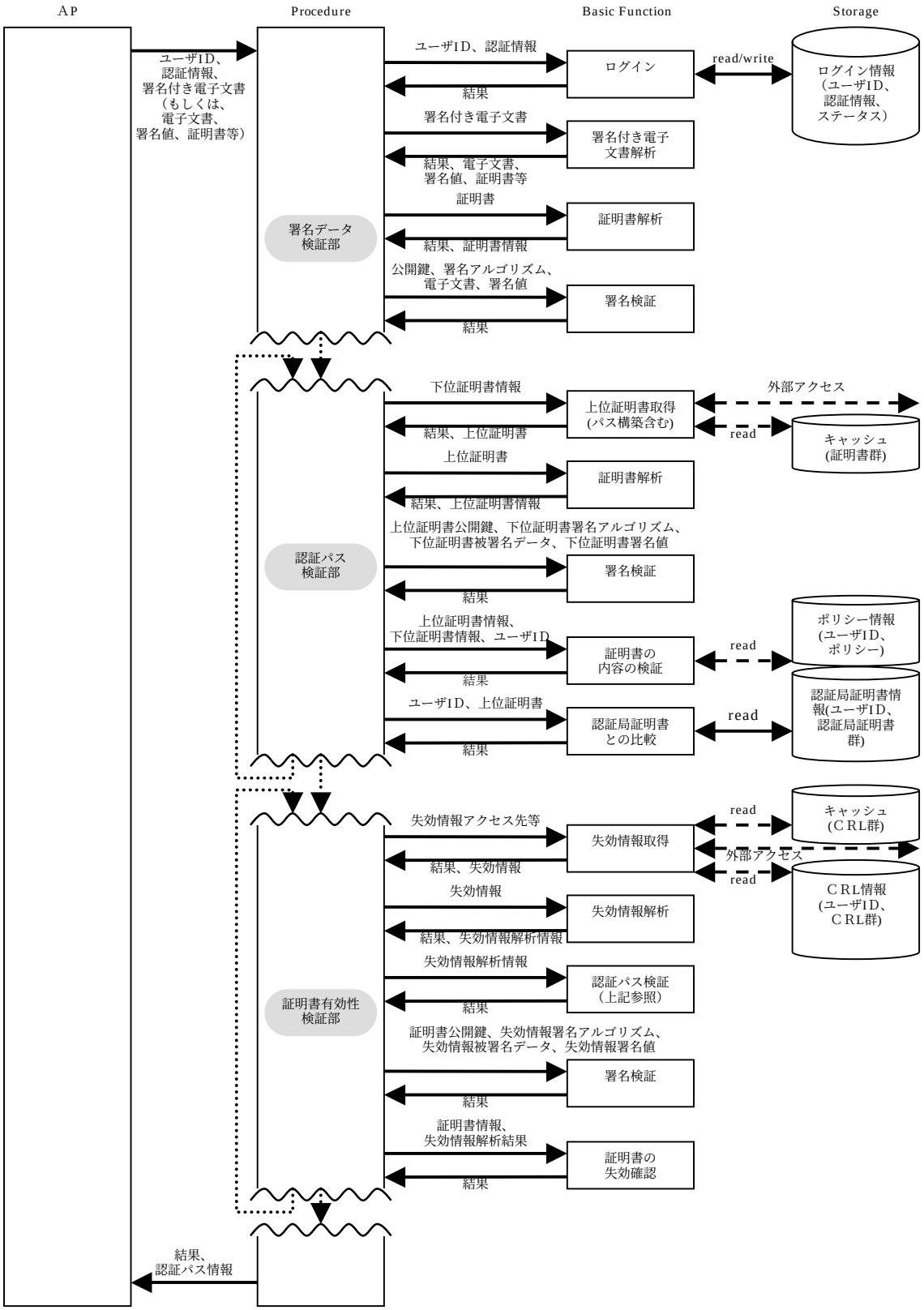

図-Ⅳ- 2-25　署名検証機能

2.2　脅威分析

本節では、利用者システムを使用する上で想定される脅威について記述する。

2.2.1　前提条件

利用者システムでの脅威を分析するにあたり、前提とする対象範囲や条件を示す。

図-Ⅳ- 2-26は、本ガイドラインで考察する脅威分析の対象範囲を示している。すなわち、本ガイドラインでは、署名プログラム自体および署名プログラムが取り扱う重要なデータ（例えば、秘密鍵など）を保護すべき対象とし、アプリケーション・プログラムやアプリケーション・プログラムが取り扱うデータ（例えば、電子署名された電子文書など）は、対象外とする。

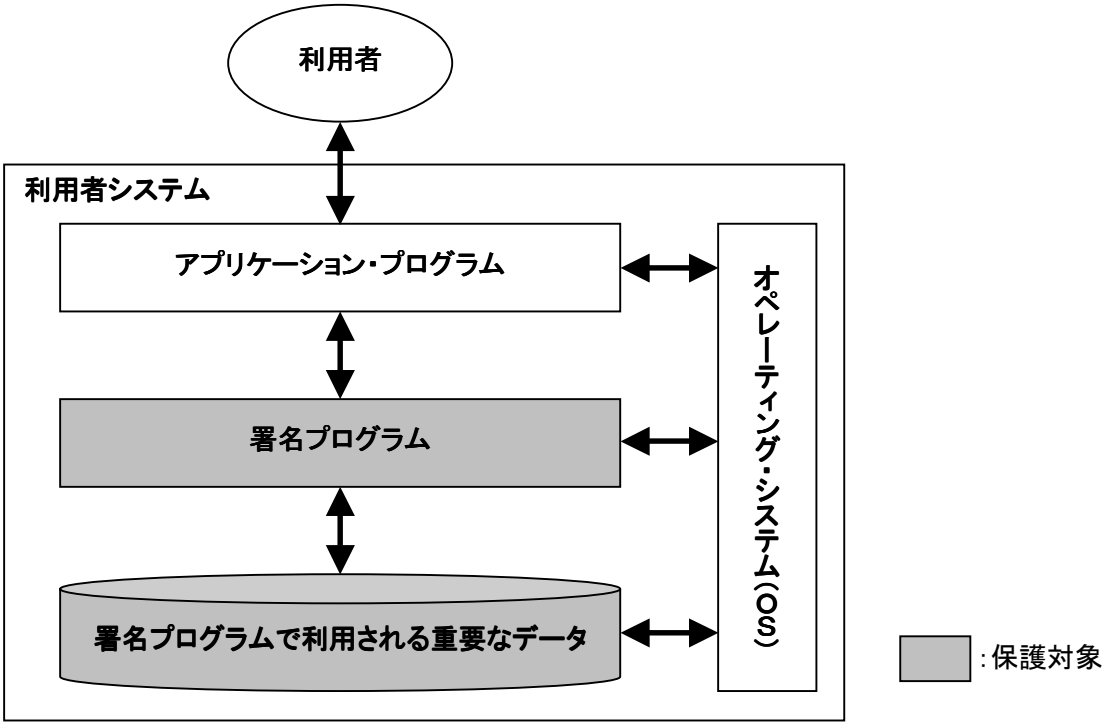

図-Ⅳ- 2-26　脅威分析の対象範囲

以降では、以下のような条件のもと、脅威分析を行っている。

- 正当な利用者は、本人の不利益となるような不正行為を意図的には行わないものとする。
- アプリケーション・プログラムと署名プログラムの間のデータ転送は、高信頼なものとする。

2.2.2　保護資産

利用者システムにおいて保護しなければならない資産として、以下のものが挙げられる。

①　利用者の秘密鍵

秘密鍵とは、電子署名を行うために必要なデータであり、本人確認や否認防止は当該データを利用者本人しか所有していないという前提に基づいて実現されている。従って、秘密鍵を他人に使用させたり、秘密鍵の情報が漏洩したりしないようにしなければならない。

②　本人識別情報および認証情報

本人識別情報とは、ユーザＩＤなど、利用者個人をユニークに特定するための情報であり、認証情報とは、パスワードや生体情報など、本人を認証するために必要な情報である。秘密鍵や署名プログラムの機能等のセキュリティは、これらの情報によって確保されているため、特に、認証情報は漏洩しないようにしなければならない。

③　セキュリティ属性情報

セキュリティ属性情報とは、利用者の証明書、利用者の信頼点情報、利用者が管理する他の証明書及びＣＲＬ、認証局／リポジトリ等へのアクセスポイント情報、利用者が検証時に必要なポリシー情報、アクセス権制御情報など、電子署名の生成処理や検証処理におけるセキュリティを確保するためのデータである。これらのデータが不正であった場合、正当な電子署名の生成や検証が行うことができないので、セキュリティ属性情報は不正に変更されないようにしなければならない。

④　証明書申請情報

証明書申請情報とは、利用者が認証局に証明書を発行してもらう際の申請手続きに必要なデータであり、その中に個人情報等のプライバシーに関わる情報が含まれている場合もある。個人情報等のプライバシーを保護しなければならない場合には、証明書申請情報が漏洩しないようにしなければならない。

⑤　署名プログラム設定情報

署名プログラム設定情報とは、署名プログラムを正常に動作させるための環境情報を設定・記録しておく情報である。従って、署名プログラム設定情報は不正に改変されないようにしなければならない。

⑥　作業用ファイル

作業用ファイルとは、署名プログラムの実行中に、当該プログラムが特定の処理を行うために一時的に作成するファイルである。署名プログラムの実行中に、このファイルが不正に書き換えられると、署名プログラムの出力結果が不正なものとなる恐れがあるため、作業用ファイルは不正に改変されないようにしなければならない。

⑦　監査ログ情報

本ガイドラインでは、セキュリティ属性情報へのアクセス時、及び、アプリケーション・プログラムからの操作時に、署名プログラムが出力するイベントの記録を監査ログ情報と呼ぶことにする。監査ログ情報では、これらのイベント発生時に、「いつ」、「どのサブジェクト（アプリケーション・プログラム）が」、「どのオブジェクト（データ）に対して」、「どのような操作を行い」、「その結果成功したのか？失敗したのか？」というような内容が記録される。

この情報は、監査時などに、セキュリティ属性情報への不正なアクセスや署名プログラム機能の不正な利用がないことを確認するための証拠として使用されるので、一度生成された監査ログ情報は、変更されないようにしなければならない。また、署名プログラムが出力した監査ログ情報と、アプリケーション・プログラムが出力した監査ログ情報との対応関係を比較し、不正な行為がなされていないかどうかを確認する必要もあるため、アプリケーション・プログラムも監査ログ情報を取得する必要がある。

⑧　署名プログラム

署名プログラムとは、利用者が電子署名の生成や検証を行うために使用するプログラムである。従って、それ自体が変更されないようにしなければならない。

2.2.3　脅威

前節で挙げた、保護資産に対して想定される脅威に関し、「誰が攻撃エージェントであり」、「どのような攻撃方法によって」、「どの保護資産が脅威にさらされるのか」を以下に記述する。

- 権限を有していない者が、コンピュータ内の秘密鍵、本人識別・認証情報、セキュリティ属性情報、署名プログラム設定情報、作業用ファイル、監査ログ情報、署名

プログラムにアクセスし、情報の追加・変更・削除をする。

- 権限を有していない者が、コンピュータ内の秘密鍵、認証情報、証明書申請情報を参照・複製する。
- 権限を有していない者が、利用者の離席時などに、コンピュータ内の秘密鍵、本人識別・認証情報、セキュリティ属性情報を不正に追加、変更、削除、使用する。
- 権限を有していない者が、不正なプログラム等で署名プログラムのセキュリティ機能を迂回することによって、コンピュータ内部の秘密鍵、本人識別・認証情報、セキュリティ属性情報を追加、変更、削除、不正使用する。
- 権限を有していない者が、コンピュータ内で削除された残存情報／廃棄された秘密鍵の格納媒体から秘密鍵を参照する。
- 正当な利用者が、過失（操作ミス等）によって、秘密鍵、本人識別・認証情報、セキュリティ属性情報、監査ログ情報を変更・削除する、あるいは、不正な情報をセキュリティ属性情報として登録する。
- 権限を有していない者が、秘密鍵の格納媒体を不正に持ち出し、秘密鍵を参照する。
- 権限を有していない者が、本人識別・認証情報を推測することによって、秘密鍵、本人識別・認証情報、セキュリティ属性情報を参照、変更、削除、不正使用する。
- 権限を有していない者が、暗号アルゴリズムを解読することによって、秘密鍵を暴露する。
- 権限を有していない者が、監査ログ情報の格納媒体を一時的に持ち出し、その内部にある監査ログ情報を追加・変更・削除する。
- 権限を有していない者が、故意にコンピュータのリソースを不足させる、あるいは、正当な利用者が、過失によってコンピュータのリソースを不足させることにより、署名プログラムが監査ログ情報を出力できないようにしてしまう。

2.3　セキュリティ対策

2.2 の脅威に対して行わなければならない対策を、署名プログラム開発者、アプリケーション・プログラム開発者、それ以外という３つの立場から別々に記述する。ここで記述する内容は、セキュリティ対策上実施すべき事項のみでなく、実施することが望ましい事項も含んでおり、これらの詳細な切り分けについては、付録２を参照すること。

2.3.1　署名プログラムが行うべき対策

署名プログラムに要求されるセキュリティ対策を記述する。

①　秘密鍵の保全

秘密鍵の消失や漏洩を防止するための対策を以下に記述する。

- 署名機能を有する耐タンパ性保管媒体（ＩＣカード、ハードウェアセキュリティモジュール等）を用いて秘密鍵を管理するための機能を有すること。
- 秘密鍵をハードディスクに保管する場合やシステム外部に出力する場合には、暗号化すること。
- ハードディスク内に秘密鍵を保管する場合には、アクセス制御を行うこと。
- 署名プログラム（又は秘密鍵）の利用時に、本人識別情報（ユーザＩＤ等）、及び認証情報（パスワード、生体情報等）を用いて、本人を識別・認証する機能を有すること。
- 署名プログラムに登録されている本人識別･認証情報が改ざんされたかどうかを検知する機能を有すること。
- 署名プログラムで使用する本人識別・認証情報を、耐タンパ性保管媒体（ＩＣカード、ハードウェアセキュリティモジュール等）に登録・保管するための機能を有すること。
- （秘密鍵をハードディスクに保管している状態でコンピュータを修理しなければならない等の特別な場合、）秘密鍵を別の装置・保管媒体に退避する機能を有すること。

②　署名プログラムの保護

署名プログラムに対する不正な改変を防止するための対策を以下に記述する。

- 署名プログラムを構成している情報に対するハッシュ値の取得機能と､当該プログラム利用時に、事前に取得しておいたハッシュ値と、実際に使用しようとしている当該プログラムのハッシュ値が一致するかどうかをチェックする機能を有することが望ましい。
- 署名プログラムの設定を変更する権限に対するアクセス制御を行うこと。
- 署名プログラムの設定情報の漏洩を防止するために暗号化すること。

③　失効事象発生時の処置

失効事象が発生した場合、不要となった秘密鍵の悪用を防止するための対策を以

下に記述する。

- 失効した証明書に対応する秘密鍵を完全に抹消すること。

④　セキュリティ属性情報の保護

セキュリティ属性情報に対する不正な改ざんや漏洩を防止するための対策を以下に記述する。

- セキュリティ属性情報に対するアクセス制御、署名、及び暗号化を行うための機能を有すること。
- セキュリティ属性情報へのアクセスに関する監査ログを取得すること。
- セキュリティ属性情報へのアクセスに関する監査ログが、改ざんされたかどうかを検知する機能を有すること。

⑤　安易な信頼点登録の防止

信頼点の不正な登録を防止するための対策を以下に記述する。

- 署名プログラムのインストーラには、一般に信頼できると評価されている信頼点情報を事前に組み込んでおくことが望ましい。
- 信頼点情報の変更に対するアクセス制御を行うこと。

⑥　無許可実行の防止

離席時などに利用者の許可なくプログラムが実行されることを防止するための対策を以下に記述する。

- 署名プログラム利用者の本人識別･認証及びその結果に基づくアクセス制御を行うこと。
- 監査ログを取得すること。

⑦　監査ログの保全

取得した監査ログの改ざん・消失を検知するための対策を以下に記述する。

- 監査ログが改ざんされたかどうかを検知する機能を有すること。
- （削除権限保持者や監査ログビューア利用権限保持者を限定するなどして、）監査ログに対するアクセス制御を行うこと。
- 監査ログ格納領域（監査ログを格納するための領域）の記憶容量が不足しないように、監査ログ格納領域の記憶容量を確認・管理すること。
- 監査ログを定期的に退避する機能を有すること。

⑧　証明書申請情報の秘匿

証明書の発行申請時に作成する証明書申請情報のプライバシー保護に関する対策を以下に記述する。

- 証明書申請情報を出力する際に暗号化することが望ましい。

⑨　信頼できる暗号アルゴリズムの採用

不正者に暗号アルゴリズムを解読され、秘密鍵を暴露されてしまうことを防止するための対策を以下に記述する。

- 一般に信頼できると評価されている暗号アルゴリズム（公開鍵暗号アルゴリズム、共通鍵暗号アルゴリズム、署名アルゴリズム等）と鍵長を使用すること。
- 暗号アルゴリズムが切り替え可能な仕組みとすること。
- 暗号アルゴリズムの鍵長を選択・変更できる仕組みとすること。

⑩　使用済みデータの抹消

使用されなくなったデータが残存し、権限を有していない者によって盗難・悪用されることを防止するための対策を以下に記述する。

- 使用済みのデータが残存しないよう、秘密鍵の廃棄時やユーザの抹消時に、秘密鍵や認証情報を完全に抹消すること。

⑪　バイパスの対策

権限を有していない者が、署名プログラムのセキュリティ機能を迂回し、不正なアクセスルートによって、秘密鍵、認証情報、利用データの不正な追加、変更、削除、使用を防止するための対策を記述する。

- 署名プログラムのセキュリティ機能を迂回できないようなインターフェースを実装することが望ましい。場合によっては、この対策をＯＳで実装してもよい。

⑫　データの退避

セキュリティ属性情報の改ざん・消失を防止するための対策を以下に記述する。

- セキュリティ属性情報を退避する機能を有すること。

2.3.2　アプリケーション・プログラムが行うべき対策

アプリケーション・プログラムに要求されるセキュリティ対策を記述する。

①　秘密鍵の保全

秘密鍵の消失や漏洩を防止するための対策を以下に記述する。

- 認証情報を定期的に変更する機能、および、類推しにくいパスワードであるこ

とをチェックする機能を有することが望ましい。

- 本人識別・認証情報の入力画面等における盗み見を防止すること（パスワードを非表示にする等）。

②　本人識別・認証情報の忘却時の処理

本人識別・認証情報（ユーザＩＤやパスワード等）を忘れてしまった場合の対策を以下に記述する。

- 証明書の更新または再発行に伴って、認証情報を再設定すること。

③　失効事象発生時の処置

秘密鍵の紛失・危殆化した場合、あるいは、証明書の内容変更・使用中止を行う場合、利用者の望まない電子署名付きの電子文書が出回らないようにするための対策を以下に記述する。

- 証明書の失効申請をするための機能を有すること（場合によっては、人間系によるオフラインで対応すること）。
- 証明書（及び秘密鍵）の更新を行う機能を有すること。

④　無許可実行の防止

離席時などに利用者の許可なくプログラムが実行されることを防止するための対策を以下に記述する。

- アプリケーション・プログラム利用者の本人識別・認証及びそれに基づいたアクセス制御を行うこと。
- 監査ログを取得すること。

⑤　監査ログの保全

取得した監査ログの改ざん・消失を検知するための対策を以下に記述する。

- 監査ログが改ざんされたかどうかを検知する機能を有すること。
- （削除権限保持者や監査ログビューア利用権限保持者を限定するなどして、）監査ログに対するアクセス制御を行うこと。
- 監査ログ格納領域（監査ログを格納するための領域）の記憶容量が不足しないように、監査ログ格納領域の記憶容量を確認・管理すること。
- 監査ログを定期的に退避する機能を有すること。

⑥　使用済みデータの抹消

使用されなくなったデータが残存し、権限を有していない者によって盗難・悪用

されることを防止するための対策を以下に記述する。

- 使用済みのデータが残存しないよう、証明書の更新時やユーザ抹消時に、認証情報等を完全に抹消すること。

⑦　再確認するユーザインタフェース

正当な利用者の操作ミスによって重要なデータの改変等を防止するための対策を以下に記述する。

- 秘密鍵、認証情報、セキュリティ属性情報の追加、変更、削除を行う際に、処理の実行を再確認するユーザインタフェースを提供すること。

2.3.3　その他の対策

2.2 の脅威に対して、署名プログラム及びアプリケーション・プログラム以外に要求されるセキュリティ対策を記述する。

①　秘密鍵の保全

秘密鍵の消失や漏洩を防止するための対策を以下に記述する。

- 利用者は、署名機能を有する耐タンパ性保管媒体（ＩＣカード、ハードウェアセキュリティモジュール等）を用いて秘密鍵を管理すること。
- 利用者は、署名プログラムで照合用として使用される本人識別・認証情報を耐タンパ性保管媒体（ＩＣカード、ハードウェアセキュリティモジュール等）に保管すること。
- 秘密鍵をハードディスクに保管している状態で、コンピュータを修理しなければならない等の特別な場合において、利用者は、秘密鍵を別の装置・保管媒体に退避すること。

②　署名プログラムの保護

署名プログラムに対する不正な改変を防止するための対策を以下に記述する。

- 署名プログラムに対して署名付与・署名検証することのできるＯＳを使用することが望ましい。

③　失効事象発生時の処置

秘密鍵の紛失・危殆化した場合、あるいは、証明書の内容変更・使用中止を行う場合、利用者の望まない電子署名付きの電子文書が出回らないようにするための対

策を以下に記述する。

- 利用者は、秘密鍵の紛失・危殆化時、あるいは、証明書の内容変更・使用中止時など場合には、証明書の失効申請をすること。
- 利用者は、秘密鍵の紛失・危殆化時、あるいは、証明書の内容変更時など場合には、証明書を再発行すること（秘密鍵を新規生成すること）。

④　ＯＳによる利用者の認証とファイル管理

権限を有していない者が、利用者システム内の秘密鍵、本人認証・認証情報、セキュリティ属性情報、署名プログラム設定情報、作業用ファイル、監査ログ情報、署名プログラムに不正にアクセスし、それらの情報の参照、追加、変更、削除を防止するための対策を以下に記述する。

- 利用者を個別に識別・認証し、ファイルごとに利用者のアクセス権限を付与できるＯＳを使用すること。また、秘密鍵、本人認証・認証情報、セキュリティ属性情報、署名プログラム設定情報、作業用ファイル、監査ログ情報、署名プログラムに対しては、個別利用者のみ（当該利用者の起動したプログラムも含む）がアクセス可能とすること（ただし、認証情報や署名プログラム等を複数の利用者で共有する場合には、ＯＳがこれらの情報にアクセスしたことを監査ログとして記録するなどの対策が必要となる）。

⑤　データの退避

署名プログラム、セキュリティ属性情報、監査ログ情報の改ざん・消失を防止・回復するための対策を以下に記述する。

- 利用者は、署名プログラム、セキュリティ属性情報、監査ログ情報は、保管媒体に退避して、安全な場所に保管すること。

付録

付録では、本文中で述べた内容を体系立ててまとめ直し、実践の場で活用しやすいように以下のものを表形式にまとめると共に、用語集をつけている。

付録１　利用者の留意事項と対策

付録２　企業間電子商取引おける電子署名の利用手順

付録３　開発者の留意事項と対策

付録 3.1 安全性確保のための開発者の留意事項

付録 3.2 利便性向上のための開発者の留意事項

付録 4　用語集

付録１　利用者の留意事項と対策

電子署名生成・検証が目的とする安全な取引や情報を確保するために、利用者に求められる留意事項と対策についてまとめたものである。

電子署名を利用するアプリケーションの中から本ガイドラインが取り上げた３種類の例（個人による電子メール、インターネット・ショッピング及び企業間電子商取引）の相場観を対比した表としてまとめている。

対象とする読者としては、電子メール、インターネット・ショッピング及び企業間電子商取引などのアプリケーションを通して「電子署名・検証を行う利用者」を想定している。

- 個人による電子メールの利用者
- インターネット・ショッピングの利用者（発注者（買い手）、受注者（売り手））
- 企業間電子商取引の利用者（エンドユーザ部門、システム管理部門）

記号の意味

○：当該アプリケーション利用者の必須事項

―：当該アプリケーション利用者の参考となる留意事項

表-付録 1- 1 利用者の留意事項と対策

通番	留意事項	対　　策	個人による電子メール	インターネット・ショッピング		企業間電子商取引	
				発注者(買い手)	受注者(売り手)	エンドユーザ	システム管理者
1	電子署名の理解	利用者は電子署名の意味を理解する。	○	○	―	○	○
2	ソフトウェアの管理	適正な手段で入手した信頼できる製品、バージョンを利用する。	○	○	○	○	○
		セキュリティ・ホール情報を入手する。	―	○	―	○	○
		ウィルスチェックを定期的に実施する。	○	○	―	○	○

通番	留意事項	対策	個人による電子メール	インターネット・ショッピング		企業間電子商取引	
				発注者(買い手)	受注者(売り手)	エンドユーザ	システム管理者
		(暗号アルゴリズムが解読される危険が生じた場合)暗号アルゴリズム、又はソフトウェアを変更する。	—	—	—	—	—
		評価プロダクトと実際に利用する製品は分離して管理する。	—	—	○	—	○
3	証明書の申請・取得	認証局の信頼性について充分に理解するとともに、評価・認定されたCA、組織で選定したCA、実績のあるCA、又は適切な認証ポリシーに則ったCAから信頼できる方法で証明書を取得する。	○	○	—	○	○
		利用目的に応じたCA及び申請・取得方法を理解し、適切に選択する。また、申請・取得方法は、認証局の運用規定に従う。	○	○	—	○	○
		証明書を取得したら、表示ツール等によってその記載内容を確認することが望ましい(サブジェクト名が正しいか、プライバシー情報が記載されていないことなどを確認)。	○	○	—	○	○
4	コンピュータのシステム日時合わせ	使用するコンピュータ(PC/WS等)のシステム日時を正しく設定・維持する。	○	○	○	○	○
5	秘密鍵及び保管媒体の安全保管	必要に応じて鍵長を選択する。	—	○	○	—	○
		秘密鍵は可能な限り、(ICカードなどの)耐タンパ媒体で管理する。ICカードは、署名機能付きカードが望ましい。	—	○	—	○	○
		やむを得ず、HD等に秘密鍵を保管する場合には、入退出管理等を含め、本人以外がその鍵にアクセスできないようにアクセス制御を行う。 また、保管媒体に対してもアクセス制御を行う。	—	—	—	○	○

通番	留意事項	対策	個人による電子メール	インターネット・ショッピング		企業間電子商取引	
				発注者(買い手)	受注者(売り手)	エンドユーザ	システム管理者
6	マシン修理時の処置	マシンを修理に出す際に、暗号化された秘密鍵をバックアップした上で削除する(確実な消去のためには、HDのフォーマットが必要)。修理されて戻って来たら秘密鍵をリストアする。(秘密鍵保管媒体がHDの場合) [注]HD自身が故障した場合には、バックアップ及びフォーマットができない。万全を期すには、HDを破壊処置する。 [備考]秘密鍵保管媒体としては、HDよりもICカードが適切であろう。	○	○	○	○	○
7	本人識別情報(パスワード)の管理	類推されにくいパスワードを設定する。	○	○	—	○	—
		パスワードを自分だけの秘密にする。	○	○	—	○	—
		パスワードを定期的に変更する。	—	○	—	○	—
8	秘密鍵複製の制限	原則として秘密鍵の複製は行わない。マシンの移行などに伴い、一時的に秘密鍵の複製を作成した場合には、もとの秘密鍵を削除することが望ましい。	○	○	—	○	○
9	作成中データの改ざん防止	作成途中データのアクセス管理対象ファイルへの退避	—	—	—	○	—
10	離席時の処置	離席時にはICカードを携行する。(秘密鍵保管媒体がICカードの場合)	○	○	—	○	—
		離席時にはアプリケーションを利用できないように、ログアウト、シャットダウン、または何らかの手段でロックする。(秘密鍵保管媒体がHDの場合)	○	○	—	○	—
11	入退室管理	扉へ施錠する、ハードウェア・トークンによる認証機構を備えた扉を設置するなどによって、許可された人しか入室させない。	—	—	—	—	○
		入退室記録をとる。	—	—	—	—	○
12	ログの管理	署名に関する操作のログファイルを定期的に待避する。	—	—	○	○	○

通番	留意事項	対策	個人による電子メール	インターネット・ショッピング		企業間電子商取引	
				発注者(買い手)	受注者(売り手)	エンドユーザ	システム管理者
13	署名の意味の伝達	署名者は、署名対象文書に署名の意味を表記する。署名検証者は、その表記を確認して署名の意味を理解する。 ＜署名の意味の例＞ 文責、照査、検認、承認、決裁、契約締結、領収、…	○	○	—	○	—
14	署名の生成	署名対象に正しく署名されたことを、自ら署名検証することによって、確認することが望ましい。	—	—	—	—	—
15	署名範囲の確認	XML 署名などで部分署名がされている文書を検証する場合は、真正性を必要とする部分が署名対象範囲に含まれていることを確認する。	—	—	—	○	—
16	署名付き文書の管理	署名付き文書は、検証に用いる証明書とともに保管する。	—	○	○	○	○
17	証明書の更新	証明書の有効期間が満了する前に、証明書の更新申請を行う。	○	○	○	○	○
18	証明書の失効	秘密鍵の不正コピー、秘密鍵保管媒体の盗難／紛失など、証明書を失効すべき事態が生じたら、速やかに証明書の失効申請を行う。そして、必要に応じて証明書（及び秘密鍵）の更新申請を行う。	○	○	○	○	○
		確実に失効処理されたことを、自ら署名検証することによって確認することが望ましい。	—	—	—	—	—
19	秘密鍵の廃棄	退会、秘密鍵漏洩などに伴って証明書が失効した場合、又はマシンを廃棄する場合、秘密鍵を次のように速やかに廃棄処置する。 ＜秘密鍵保管媒体がHDの場合＞ 秘密鍵を削除する。（確実な消去のためには、HDのフォーマットが必要） ＜秘密鍵保管媒体がICカードの場合＞ ICカードを破壊する。又は組織の運用管理者に返却し、運用管理者がまとめて再フォーマット又は破壊処置する。	○	○	○	○	○

通番	留意事項	対策	個人による電子メール	インターネット・ショッピング		企業間電子商取引	
				発注者(買い手)	受注者(売り手)	エンドユーザ	システム管理者
20	信頼点(Trust Point)の管理	信頼点の操作については、本人のみが行う。	○	○	—	○	○
		信頼点の証明書を追加する場合は、署名検証、有効性確認、失効していないかを確認の上追加する。	○	○	—	○	○
		信頼する信頼点の情報を定期的に確認する。信頼点リストに、不審な信頼点が追加されていないことを定期的に確認する。	○	○	○	○	○
		検証者が新しい証明書を信頼点として追加する場合は、別途公開されている情報を利用して、確認した上で行う。	—	—	—	—	○
		相手の証明書を信頼する場合でも、必要がなければ、その発行者を信頼点リストに追加しない。	—	—	—	○	—
		信頼点の変更などの際に使用するアクセスコントロール情報(パスワードなど)を正しく管理する。	—	—	—	○	—

付録２　企業間電子商取引おける電子署名の利用手順

本ガイドライン第Ⅲ部で、企業間電子商取引における電子署名を採り上げた。本付録 3 は、その「1.2 利用手順」に記述した内容から、調達側企業での手順を一覧にまとめたものである。

本付録の内容は本ガイドラインにおいて想定した例である。

表-付録 2- 1 企業間電子商取引における電子署名の利用手順

フェーズ	利用場面・利用手順		
	導入段階 （調達側企業が公募等により供給側企業を募る段階。この段階では、取引相手を広い範囲から選定する目的から、対象は必ずしも限定されない）	**選定段階** （応募内容に基づいて供給側企業候補を絞る段階。続いて絞り込んだ供給側企業に対して調達仕様を開示し見積もりを求める。供給側企業は調達仕様に基づいて検討し見積書を提出する。この段階では、調達仕様書、見積書ともに、その真正性が必須となる）	**決済段階** （取引相手と契約を交わし決済まで行う段階。この段階での改ざんやなりすましは、金額的にも企業にとっての信用面でも重大な問題を引き起こすため、特定の相手であることが最も確実に保証されなければならない）
準備 電子署名に関連した事項の確認 (ポリシー、契約事項、など)	*事前確認不要* *（この段階での改ざんやなりすましは後の段階で検出されるので、それによる被害は軽微なものであること想定できるから）*	調達仕様の開示に先立ち、機密保持契約などの取り決めを交わし、この中で、 ・企業内認証局の証明書 ・上記証明書の失効に伴う責任の明確化 などを確認しておく。	取引に先立ち、基本契約を交わし、 ・決済者の特定 ・決済者の証明書 ・企業内認証局の証明書 ・上記証明書の失効に伴う責任の明確化 などを確認しておく。
・業務要件に応じた取引相手の証明書のレベルを選定（発行者や発行条件等）	相手の会社が確認できればよい *（必ずしも署名である必要はないが、どの会社から送付されているかが確認できればよい）*	発行者を確認できる証明書を担当者の証明書として信頼することとする。 ただし、発行者の正当性を、別途公開されている証明書のFingerprint等により確認できることが必要。	予め、契約時に取り交わした相手の発行者の証明書と決済者の証明書を入手し信頼することとする。
・相手側発行者の確認	*事前確認不要* *（業務の段階で、個別に確認）*	相手の発行者の情報と、その証明書を特定する情報を確認する。 （例：証明書のFingerprint等）	相手の発行者の情報と、その証明書を特定する情報を確認する。 （例：証明書のFingerprint等）
・相手側業務権限者の確認	*事前確認不要*	事前確認不要 （取り決めを結んだ会社の社員であることさえ分かればよい）	予め入手した決済者の証明書を「決済権限者証明書ＤＢ」に登録する。
・失効情報取得方法の確認	*事前確認不要*	有効期限内では、キャッシュしている失効情報を利用することとする。	検証時に、常に最新の失効情報を取得することとする。
鍵ペアの生成	*準備不要* *（導入段階では調達側は署名を行わないと想定する）*	証明書申請に使用するツールの機能を用いて、鍵を生成する。	証明書申請に使用するツールの機能を用いて、鍵を生成する。
鍵の格納	*準備不要* *（導入段階では調達側は署名を行わないと想定する）*	証明書申請に使用するツールの機能を用いて、ＩＣカードに格納する。	証明書申請に使用するツールの機能を用いて、ＩＣカードに格納する。
信頼点の登録	*事前設定不要* *（業務の段階で、個別に確認）*	事前取り決めで指定された発行者情報を確認した上で、相手の発行者の証明書を信頼点して登録する。 あるいは、業務の段階で個別に確認する。	基本契約書に記載された発行者情報を確認した上で、相手の発行者の証明書を信頼点として登録する。
証明書の申請	*準備不要* *（導入段階では調達側は署名を行わないと想定する）*	証明書申請に使用するツールの機能を用いて、企業内ＣＡに対し、証明書の発行を依頼する。	証明書申請に使用するツールの機能を用いて、企業内ＣＡに対し、証明書の発行を依頼する。

	証明書の取得	*準備不要* *（導入段階では調達側は署名を行わないと想定する）*	証明書申請に使用するツールの機能を用いて、発行された証明書を取得し保存する。	証明書申請に使用するツールの機能を用いて、発行された証明書を取得し保存する。
管理	鍵格納媒体の保管	*準備不要* *（導入段階では調達側は署名を行わないと想定する）*	調達担当者がＩＣカードを安全な場所に保管し、他者への貸し出しは行わない。	決済担当者がＩＣカードを安全な場所に保管し、他者への貸し出しは行わない。
	信頼点リストの維持	・端末の他の利用者を含めて、不用意な信頼点を登録しないよう注意する。 ・不用意な信頼点が登録されていないことを確認する。	・端末の他の利用者を含めて、不用意な信頼点を登録しないよう注意する。 ・不用意な信頼点が登録されていないことを確認する。	・端末の他の利用者を含めて、不用意な信頼点を登録しないよう注意する。 ・不用意な信頼点が登録されていないことを確認する。
	鍵のバックアップ	*なし* *（導入段階では調達側は署名を行わないと想定する）*	（署名鍵のバックアップはしない）	（署名鍵のバックアップはしない）
	有効期限後の鍵の保存	*なし* *（導入段階では調達側は署名を行わないと想定する）*	有効期限後や失効後は、ＩＣカードを管理部門に返却する。(鍵を破棄する)	有効期限後や失効後は、ＩＣカードを管理部門に返却する。(鍵を破棄する)
利用（署名生成）	署名対象部分の作成	調達概要を作成 *（ただし、導入段階では調達側は署名を行わないと想定する）*	詳細な調達仕様をXMLで記述する。また、これを取り込んだ形式の見積書の雛形(入力フォーム)を作成する。	発注担当者が、発注契約書をXMLで記述する。
	署名鍵の活性化	*なし* *（導入段階では調達側は署名を行わないと想定する）*	ＩＣカードをセットし、ＰＩＮを入力する。	ＩＣカードをセットし、ＰＩＮを入力する。
	署名生成	*なし* *（調達概要には署名を行わないと想定する）*	見積書の雛形のうち、調達仕様部分について、調達担当者が署名を行う。	発注契約書に発注担当者が署名をした上で、決済担当者が署名を行う。
	署名文書を送付	調達概要をWebで公開。 供給側がサーバ認証できるよう、PublicＣＡが発行した証明書を用い、ＳＳLで公開する。	XML形式の見積書雛型(署名付の調達仕様を含む)をＳＳLで公開する。 返信先のアドレスを公開するとともに、相手がメールを暗号化できるようにメール用証明書も公開する。	暗号して、メールで送付する。
利用（署名検証）	署名文書を入手	供給側企業から、応募の意思を示す文書を署名付メールを受信	XMLで記述された見積書を署名付メールで受信。	契約文書を署名付メールで受信。
	証明書の検証	（以下の検証をメーラが行う）	（以下の検証をXMLブラウザが行う）	（以下の検証をメーラが行う）
	・有効期限やUsage等の確認	証明書に設定されている項目に従った利用がされているかを確認する。	証明書に設定されている項目に従った利用がされているかを確認する。	証明書に設定されている項目に従った利用がされているかを確認する。
	・発行者の確認	証明書チェーンが正しくたどれるかを確認する。信頼点に達しない場合は、その旨を利用者に通知する。	証明書チェーンが正しくたどれるかを確認する。信頼点に達しない場合は、その旨を利用者に通知する。	証明書チェーンが正しくたどれるかを確認する。信頼点に達しない場合は、その旨を利用者に通知する。
	・失効確認(ＣRL/0ＣＳＰ)	有効期限内では、キャッシュしている失効情報を利用する。 有効期限外あるいはキャッシュされていない場合はＣRLを取得する。	有効期限内では、キャッシュしている失効情報を利用する。 有効期限外あるいはキャッシュされていない場合はＣRLを取得する。	ＣRLをその都度最新のものに更新して確認する。 あるいは、0ＣＳＰを利用して確認する。
	署名者の確認	証明書の発行者が相手側の企業内認証局であるため、相手側が公開している企業内認証局証明書のFingerprint等を確認し「このメールの検証においてのみ信頼する」こととする。	証明書の発行者が相手側の企業内認証局であるため、相手側が公開している企業内認証局証明書のFingerprint等を確認する。	予め、登録されている決済者であることを確認する。
	署名検証（非改ざん確認）	メールの内容が改ざんされていないことを検証する。 （メーラが行う）	見積書の内容が改ざんされていないことを検証する。 （XMLブラウザが行う）	受注確認書の内容が改ざんされていないことを検証する。 （XMLブラウザが行う）

	信頼点の追加(必要ならば)	その都度、発行者を確認することとして、送付された企業内認証局証明書は、信頼点として登録しない。	その都度、発行者を確認することとして、送付された企業内認証局証明書は、信頼点として登録しない。 ただ、見積もりの変更など対応頻度が多いことが予想される場合は、検証した上で相手の企業内認証局証明書を信頼点としておいてもよい。	予め、登録されている発行者のみ信頼する。
	内容の確認	送付された製品概要や提供側企業の情報などを基に、詳細仕様を提示してもかまわない企業の絞込みを行う。	見積書に示された条件を検討し、発注を行う企業を選定する。	受注確認書の内容を確認し、発注内容との整合性を確認する。
更新	鍵ペアの更新	*なし* *(導入段階では調達側は署名を行わないと想定する)*	有効期限が切れる前に、証明書申請に使用するツールの機能を用いて、鍵を生成する。	有効期限が切れる前に、証明書申請に使用するツールの機能を用いて、鍵を生成する。
	証明書の更新	*なし* *(導入段階では調達側は署名を行わないと想定する)*	有効期限が切れる前に、証明書申請に使用するツールの機能を用いて、証明書を申請し取得する。	有効期限が切れる前に、証明書申請に使用するツールの機能を用いて、証明書を申請し取得する。
	PIN の更新	*なし* *(導入段階では調達側は署名を行わないと想定する)*	PIN は、定期的に変更する。	PIN は、定期的に変更する。
廃棄	証明書の失効	*なし* *(導入段階では調達側は署名を行わないと想定する)*	・所有者が鍵の危殆化に気づいたときやICカードの破損等により使用不可となった場合は、所有者が発行者に失効を依頼する。 ・調達担当者が変更になった場合などは、発行者が失効手続きを行う。	・所有者が鍵の危殆化に気づいたときやICカードの破損等により使用不可となった場合は、所有者が発行者に失効を依頼する。 ・決済担当者が変更になった場合などは、発行者が失効手続きを行う。
	鍵の廃棄	*なし* *(導入段階では調達側は署名を行わないと想定する)*	有効期限後は、初期化するなどして、鍵を使用しようできないようにする。	有効期限後は、初期化するなどして、鍵を使用しようできないようにする。

付録３　開発者の留意事項と対策

本付録は、第Ⅱ部、第Ⅲ部および第Ⅳ部の留意事項と対策を、個人による電子メール、インターネット・ショッピング、企業間電子商取引それぞれにおける、開発者（アプリケーションプログラムおよび利用者システム）が留意すべき項目をそれぞれ比較できるよう、一覧表にまとめた。
また、「第Ⅳ部　1. 利便性向上のための配慮」に対する開発者の留意事項についても、各アプリケーションプログラムの特性に従って一覧表とした。

付録 3.1 安全性確保のための開発者の留意事項

記号の意味

○　　：当該アプリケーションに求められる機能
●　　：署名プログラムに求められる機能
―：当該アプリケーションおよび署名プログラムに参考となる留意事項

表-付録 3- 1 安全性確保の為の開発者の留意事項

通番	留意事項	対策案	個人による電子メール	インターネット・ショッピング		企業間電子商取引
				発注者	受注者	
1	秘密鍵保全（消失防止・漏洩防止）	署名機能を有するICカードを用いた鍵管理（注 1）	●	●	―	●
		秘密鍵の暗号化	●	●	●	●
		アクセス制御管理（HDに保管する場合）	●	●	●	●
		本人認証情報（パスワードによる）	●	●	●	●
		本人認証情報の定期的な変更	●	●	●	●
		本人識別・認証（生体情報）	―	―	―	―
		本人認証情報管理（パスワードチェックおよび類推しにくいパスワード）	―	―	―	―
		システム内における本人識別・認証のために登録された情報の改ざん検知	―	―	●	●
		システム内における本人識別・認証のために登録された情報をICカード・HSMなどの保管媒体に保管	―	●	―	●
		本人識別・認証情報情報の画面等における盗視防止（パスワード非表示）	○	○	○	○
		（秘密鍵保管媒体の修理等の特別な場合における）秘密鍵の退避・エクスポート。ただし、HDに保管する場合のみ。	●	●	●	●
2	本人識別・認証情報の忘却時処理	証明書更新・再発行に伴う認証情報再設定	○	○	○	○
3	セキュリティ機能の保護（プログラムの不正な改変への対策）	プログラムへの署名・署名検証	―	―	―	―
		プログラムの構成情報に対するハッシュ値の一致チェック	―	―	―	―
		プログラムの設定変更権限に対するアクセス制御	―	―	―	●
		プログラム設定情報の暗号化による漏洩防止	―	―	―	●

通番	留意事項	対策案	個人による電子メール	インターネット・ショッピング		企業間電子商取引
				発注者	受注者	
4	失効事象発生時処置	証明書の失効申請(人間系によるオフラインを含む)	○	○	○	○
		証明書(及び秘密鍵)の更新	○	○	○	○
		失効した証明書に対応する秘密鍵の完全抹消	●	●	●	●
6	セキュリティ機能の保護(セキュリティ属性の改ざん防止・秘匿)	セキュリティ属性のアクセス管理・署名・暗号化 [セキュリティ属性:アクセス権制御情報・証明書管理情報(信頼点登録情報等)、鍵管理情報、失効管理情報、本人識別情報等を保持したファイル・データベース]	●	●	●	●
		監査ログの取得	—	●	●	●
		監査ログの改ざん防止	—	●	●	●
7	安易な信頼点登録の防止	インストーラへの信頼点組み込み	—	—	—	—
		信頼点の変更に関するアクセス制御	—	—	—	●
8	無許可実行の防止	ソフトウェア利用者の識別・認証およびアクセス制御	○ ●	○ ●	○ ●	○ ●
		監査ログの取得	—	● ●	○ ●	○ ●
9	監査ログの保全(改ざん検知・消失防止・ログファイルの管理)	監査ログの改ざん検知機能の提供	—	○ ●	○ ●	○ ●
		監査ログへのアクセス管理(削除権限保持者の限定。監査ログビューア権限の限定)	—	—	○ ●	○ ●
		監査ログ情報格納領域の記憶容量の確認・管理	—	—	○ ●	○ ●
		監査ログの定期的退避・アーカイブ保存	—	—	○ ●	○ ●
10	証明書申請情報の秘匿(プライバシー保護)	証明書申請情報の暗号化	—	—	—	—
11	信頼できる暗号アルゴリズムの採用	一般に信頼できると評価されている暗号アルゴリズム(公開鍵アルゴリズム、共通鍵アルゴリズム、署名アルゴリズム等)と鍵長を使用	●	●	●	●
		暗号アルゴリズムの切替機構	—	—	—	●
		鍵長の選択・変更機構	—	—	—	●
12	使用済みデータの抹消	使用済みデータが残存し、悪意の第三者によって盗難されることがないよう、秘密鍵の廃棄時やユーザ抹消時に秘密鍵や認証情報を完全に抹消する	○ ●	○ ●	○ ●	○ ●

通番	留意事項	対策案	個人による電子メール	インターネット・ショッピング		企業間電子商取引
				発注者	受注者	
12	誤操作による秘密鍵・認証データおよび利用者データの保全消失・追加・変更防止	秘密鍵、認証情報、利用者データの追加、変更、削除を行う際に処理実行を再確認するユーザインタフェース	○	○	○	○
13	バイパス対策	処理がバイパスされることがないように、処理系システムのセキュリティ機能に対するアクセス制御を行うこと	—	—	—	—
14	ユーザ識別・認証機能を保有し、ファイルごとのアクセス権限を付与できるOSであること	ユーザ識別・認証機能を保有するOSであること。ファイルごとのユーザのアクセス権限を付与できること（作業用ファイルなど）	—	○	○ OS機能	○ OS機能
15	データの退避	署名プログラム・利用者データを退避保管すること	—	●	●	○ ●

（注 1）製品動向において、ICカードを接続可能なプラットフォームは、Windows 系である。UNIX系の場合のICカードの利用については、今後検討を要する。

付録 3.2 利便性向上のための開発者の留意事項

記号の意味

分類（A：誤操作の防止　B:簡易な操作　C：その他）

関連フェーズ（ア：準備、イ：管理、ウ：利用（署名）、エ：利用（検証）、オ：更新、カ：廃棄、キ：全行程）

○：　利用者アプリケーションに求められる機能

●：　署名プログラムに求められる機能

表-付録 3- 2 利便性向上のための配慮一覧

通番	配慮事項	対策案	分類	個人による電子メール	インターネット・ショッピング	企業間電子取引	関連フェーズ
1	証明書内容の分かり易い表示	平易な表現での証明書内容表示	A	○	○	○	エ
		証明書の解説書／ヘルプ機能の装備	A			○	エ
		証明書の発行者情報の表示	A			○	エ
2	認証局情報の容易な入手	認証ポリシー及びＣＡ評価／認定情報の入手の支援機能	A			○	イ、エ
3	署名検証結果の分かり易い表示	署名検証結果は、署名の正否とともに、誰の署名であるかを証明書のサブジェクト名を基に正確かつ分かり易く表示	A	○	○	○	エ
		検証時に、相手の発行者の情報も表示	A			○	エ
4	親切なエラーメッセージ	利用者がどうしたら良いかが分かるように、エラー処置方法を明示	A	○	○	○	キ
5	秘密鍵・証明書の選択支援と管理ガイド	用途(適用ドメイン／アプリケーション、署名の意味等）を選択画面に記入／表示	A、			○	ウ、エ
		利用者の遵守事項のガイド表示	C			○	ウ、エ
6	署名のためのＧＵＩ	明示的に署名することを示すメッセージ又は署名アイコン	A、B	○	○	○	ウ
7	秘密鍵パスワードの設定支援	秘密鍵パスワードの設定ガイド	A、B			○	ア
8	署名の意味の表示・伝達	署名の付帯情報として、署名の意味（文責、照査、検認、承認等）情報を保持・表示	A	○	○	○	ウ、エ
9	ポータブルな秘密鍵	秘密鍵保管媒体として、ＩＣカード等の可搬媒体を採用	B、	○	○	○	ア、イ
10	ＣＡ証明書更新時の利用者秘密鍵の継続使用	ＣＡ秘密鍵有効期限＜ＣＡ証明書有効期限として、ＣＡ秘密鍵有効期限に合わせてＣＡの世代を交代 かつ、 ・ＣＡ世代間で相互に証明書を発行	C C			● ●	オ オ

通番	配慮事項	対策案	分類	個人による電子メール	インターネット・ショッピング	企業間電子取引	関連フェーズ
		（NewWithOld、OldWithNew の証明書も発行）し、ＣＡ世代間の認証パスを検証 ［補足］ 証明書を発行してもらったＣＡ世代が異なる利用者間でも、それらのＣＡ証明書の有効期限が切れていない限り、お互いに署名検証可能とする。					
１１	署名付きであることの表示	署名付きであることを、アイコン、印影イメージ等によって明示	A、B	○	○	○	エ
		誰の署名であるかを証明書のサブジェクト名を基に正確かつ分かり易く表示	A	○	○	○	エ
１２	ワンタッチ・オペレーション化	署名生成／署名検証をできるだけワンタッチで実行	B				ウ、エ
		パスワード入力を（１セッション単位につき）１回で済ませるモード、又はシングルサインオンを安全に行える	B				ウ、エ
１３	相互運用性及び保守性	他のＣＡドメインに属する人とのやり取りが可能（相互認証、又は他のＣＡドメインのルートＣＡ証明書を信頼点の一つとして登録）	C			○	イ、エ
		認証ポリシーに応じて、同一秘密鍵を複数アプリケーションで利用	C			○	キ
１４	複数人でのマシン共用	同一マシン内での複数人の秘密鍵を管理（ＨＤ又は秘密鍵管理装置上）	C				ア、イ
		ＩＣカード等のポータブルな秘密鍵保管媒体を採用	C			●	ア、イ

付録４　用語集

1. ＣＲＬ（Certificate Revocation List）
   証明書失効リスト。認証局が発行するデータで、有効期限内に失効された証明書のシリアル番号の一覧が記載されている。ＣＲＬは、認証局の電子署名によって改ざんできない形式となっている。
2. ＯＣＳＰ（Online Certificate Status Protocol）
   検証局等に対して、証明書が失効されているかどうかという確認をオンラインで問い合わせるためのプロトコル。
3. ＰＫＩ（Public Key Infrastructure）
   公開鍵暗号を利用して各種情報通信システムの安全性を確保するための一連の技術およびサービス。
4. 改ざん(改竄)
   データを自分の都合のいいように改変する不正行為。
5. 鍵ペア
   公開鍵暗号方式で利用する組となる二つの鍵。公開鍵と秘密鍵とからなる。
6. 危殆化
   秘密鍵等の秘密情報が盗難、漏洩、解読などといった様々な原因によって、その機密性を失うこと（失ったものと想定されること）。
7. 検証局
   証明書が失効されているかどうかという検証者からの問い合わせを受け付け、応答する機関。ＶＡ（Validation Authority）やＯＣＳＰ Responderとも呼ぶ。
8. 検証者
   署名検証を行う人。
9. 公開鍵
   公開鍵暗号方式で利用する鍵ペアのうち、広く一般に開示する鍵。検証者が署名検証を行う際に使用する。
10. 公開鍵暗号方式
    電子文書を暗号化する際に使用する鍵と、暗号文を復号する際に使用する鍵とが異なる暗号方式。公開鍵暗号方式には、どちらか一方の鍵からもう一方の鍵を算出することが

非常に困難であるという性質と、二つの鍵は１対１対応であって、どちらか一方の鍵で暗号化したデータはもう一方の鍵でのみ復号可能であるという性質とがある。公開鍵暗号方式は、電子署名を実現する手段として利用される。

11.証明書

公開鍵とその所有者（署名者、または認証局）とを対応付けるために、認証局が生成する電子データ。認証書、電子証明書、あるいは公開鍵証明書などとも呼ぶ。証明書は、認証局の電子署名によって改ざんできない形式となっており、所有者の名前や公開鍵の値だけでなく、発行した認証局の名前や有効期限や利用目的などといった情報も含まれている。市区町村役場や登記所で発行される印鑑証明書に相当する。

12.証明書の失効

秘密鍵の危殆化等のため、有効期間内の証明書の効力を失わせる行為。証明書の所有者（署名者、または認証局）の指示に基づいて行われる。

13.証明書の有効性確認

検証者が、署名検証に使用する証明書が失効されていないかを確認する行為。確認の方法として、ＣＲＬに記載されているかどうか調べる方法や、検証局にＯＣＳＰでオンライン問い合わせをする方法などがある。

14.証明書ポリシー

認証局が証明書を発行するにあたって設定するサービスや運用等に関する方針や規定。ＣＰ（Certificate Policy）とも呼ぶ。

15.署名検証

署名付き電子文書を、署名者証明書に含まれる署名者の公開鍵を用いて復号することにより、当該電子署名の正当性（署名者によって生成された電子署名であることや、署名付き電子文書が改ざんされていないこと）を検証する行為。紙の文書に付された印影を印鑑証明書等に記された正しい印影を用いて照合する場合に相当する。

16.署名者

署名生成を行う人。

17.署名生成

電子文書に対して、署名者の秘密鍵を用いて暗号化することにより電子署名を施し、署名付き電子文書を生成する行為のこと。紙の文書に捺印する場合に相当する。

18.信頼点、信頼点情報

利用者が信頼する認証局の証明書。通常は、自分の証明書を取得した認証局のルート認証局であることが多い。信頼点は、検証者が署名者証明書の正当性を確認する際に利用される。

19.耐タンパ性

装置を分解するなどして、中にある秘密情報等を不正に入手しようとする行為（Tamper）に対する耐性。

20.電子署名

署名対象となる電子文書、あるいはそのハッシュ値を秘密鍵で暗号化したもの。一般には、タブレット等によって入力された手書きサインも含めて電子署名と呼び、前記秘密鍵で暗号化したものをディジタル署名と呼びわける場合もあるが、本ガイドラインでは、公開鍵暗号方式に基づいて生成されたものだけを電子署名、あるいは単に署名と呼んでいる。

21.電子署名法

平成１３年４月より施行される「電子署名および認証業務に関する法律（平成 12 年 5 月 31 日法律第 102 号）」の略称。電子署名に対して印鑑と同等の推定効を与えている法律。

22.電子認証システム

電子署名を用いて、通信相手の確認や通信メッセージの改ざんチェックなどを行うシステム、および証明書の発行など、電子署名を正しく利用するために必要な処理を行うシステム。なりすましや改ざん、否認などといった不正を防ぐ目的で用いられる。

23.なりすまし

他者のふりをする不正行為。

24.認証局

公開鍵とその所有者とを対応付けるために、署名者または他の認証局に対して証明書を発行する機関。ＣＡ（Certification Authority）とも呼ぶ。また、自己の証明書を自分自身で発行する認証局をルート認証局とも呼ぶ。

25.認証局運用規定

証明書ポリシーに基づいて、認証の実施における手続きや遵守事項等を文書化したもの。ＣＰＳ（Certification Practice Statement）とも呼ぶ。一般に、利用者等に対して開示

される。

26.認証情報

ある利用者を他の利用者と区別するために用いられる情報。パスワードや生体情報等。

27.ハッシュ関数

電子文書に電子署名を施す際などに、その電子文書をある一定の大きさまで圧縮するための計算手順。ハッシュ関数の計算結果である圧縮データをハッシュ値、あるいはメッセージダイジェストと呼ぶ。ハッシュ関数には、あるハッシュ値が与えられたときに、それと同じハッシュ値となるような電子文書を求めることが困難であるという性質（一方向性）と、同じハッシュ値となる二つの異なる電子文書を探し出すことが困難であるという性質（衝突回避性）がある。

28.否認

取引などを行った後に、当該取引に関与したことそのものを否定する不正行為。事後否認とも呼ぶ。

29.秘密鍵

公開鍵暗号方式で利用する鍵ペアのうち、署名者自身が秘密に保持する鍵。署名生成時に使用する。

30.リポジトリ

証明書やＣＲＬ等を保管しておき、利用者からの要求に応じてそれら情報を配布する仕組み。

31.利用者

電子署名技術を利用する人。署名者と検証者に区分される。

索引

（用語集関連）

た

て

な

に

は

ひ

り

メンバーリスト

事務局

菅　知之	電子商取引推進協議会（ECOM）	主席研究員
紙田　政典	電子商取引推進協議会（ECOM）	主席研究員
米倉　早織	電子商取引推進協議会（ECOM）	主席研究員

編集メンバー

役割	氏名	会社名	TF1	TF2	備考
	荻原　利彦	NTTコミュニケーションズ株式会社	○	○	
	鈴木　優一	エントラスト・ジャパン株式会社	○	○	
	保倉　豊	グローバルフレンドシップ株式会社	○	○	
	松山　科子	ソニー株式会社	○		
	二村　朝康	株式会社 NTTデータ	○		
	青野　徳弘	株式会社ソリトンシステムズ	○		
	村上　繁	株式会社ソリトンシステムズ	○		
	中原　康	株式会社東芝		○	
	笈川　光浩	株式会社日立製作所	○	○	＊
	洲崎　誠一	株式会社日立製作所	○	○	＊
リーダー	手塚　悟	株式会社日立製作所	○		
	青木　尚	三菱電機株式会社	○		＊
	田中　稔	三菱電機株式会社	○		＊
ｻﾌﾞﾘｰﾀﾞｰ	佐伯　正夫	三菱電機株式会社		○	
	荒木　義晴	日本ベリサイン株式会社	○	○	
	北村　裕司	日本ボルチモアテクノロジーズ株式会社	○		
	山岡　誉侍	日本電気株式会社　NECｿﾘｭｰｼｮﾝｽﾞ	○	○	＊
ｻﾌﾞﾘｰﾀﾞｰ	小松　文子	日本電気株式会社　NECｿﾘｭｰｼｮﾝｽﾞ	○	○	
	今枝　直彦	日本電信電話株式会社	○	○	
	本間　史夫	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		○	
	栗田　享佳	富士通株式会社	○		＊
	冨高　政治	富士通株式会社		○	＊
リーダー	山下　真	富士通株式会社		○	
	近藤　英幸	富士電機株式会社	○		＊
	柳原　秀明	富士電機株式会社		○	
	米倉　昭利	財団法人　日本情報処理開発協会	○	○	

（注）TF１：電子署名生成システム検討タスクフォース
TF２：電子署名検証システム検討タスクフォース
＊：オブザーバー

電子認証システム仕様検討サブワーキング (SWG1)メンバー

氏名	会社名	備考
八束　啓文	RSAセキュリティ株式会社	
岸本　輝昭	電子商取引安全技術研究組合	
杉山　喜広	株式会社エヌジェーケー	
河田　悦生	NTTドコモ株式会社	
関野　公彦	NTTドコモ株式会社	*
荻原　利彦	NTTコミュニケーションズ株式会社	
中村　逸一	株式会社 NTTデータ	
杉本　則高	株式会社FFC	
上甲　　徹	沖電気工業株式会社	
保倉　　豊	グローバルフレンドシップ株式会社	
高崎　政嗣	グローバルフォーカス株式会社	
宮下　　毅	コンピュータ･アソシエイツ株式会社	
土屋　雄三	Eジャパン協議会	
木下　　剛	株式会社三和銀行	
信濃　義朗	昌栄印刷株式会社	
伊藤　　昇	情報処理振興事業協会	
松山　科子	ソニー株式会社	
正木　淳雄	株式会社ソリトンシステムズ	
星野　　理	株式会社帝国データバンク	
西川　和比古	株式会社東海銀行	
中原　　康	株式会社東芝	
西岡　誠治	財団法人日本建設情報総合センター	
小野　千秋	株式会社日本ｼｽﾃﾑﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ	
浜岡　周作	日本信販株式会社	
小松　文子	日本電気株式会社　NECｿﾘｭｰｼｮﾝｽﾞ	
山岡　誉侍	日本電気株式会社　NECｿﾘｭｰｼｮﾝｽﾞ	*
西本　浩文	日本電子計算株式会社	
今枝　直彦	日本電信電話株式会社	
町田　　陽	日本認証サービス株式会社	
本間　史夫	日本認証サービス株式会社	*
荒木　義晴	日本ベリサイン株式会社	
北村　裕司	日本ボルチモアテクノロジーズ株式会社	
玉山　　恭	株式会社日立情報システムズ	
手塚　　悟	株式会社日立製作所	
洲崎　誠一	株式会社日立製作所	*

氏名	会社名	備考
笈川　光浩	株式会社日立製作所	＊
飯塚　光二	富士重工業株式会社	
山下　　真	富士通株式会社	
冨高　政治	富士通株式会社	＊
栗田　享佳	富士通株式会社	＊
柳原　秀明	富士電機株式会社	
近藤　英幸	富士電機株式会社	＊
及川　卓也	ﾏｲｸﾛｿﾌﾄ　ﾌﾟﾛﾀﾞｸﾄ　ﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ　ﾘﾐﾃｯﾄﾞ	
佐伯　正夫	三菱電機株式会社	
田中　稔	三菱電機株式会社	＊
青木　尚	三菱電機株式会社	＊
米倉　昭利	財団法人　日本情報処理開発協会	
萩原　　隆	財団法人　日本情報処理開発協会	

(注)＊：オブザーバ

平成13年3月発行

発行:電子商取引推進協議会

東京都江東区青海2－45

タイム24ビル10階

Tel　　03-5500-3600

E-mail　info@ecom.or.jp