

電子署名・認証の利用状況調査

平成 14年 3月



電子商取引推進協議会
PKI 連携推進フォーラム

はじめに	1
1 PKIの動向	2
1.1 政府における電子署名・認証の推進と取り組み	2
1.1.1 PKIの必要性	2
1.1.2 電子署名及び認証業務に関する法律	5
1.1.3 電子政府構想におけるGPKIの推進状況	9
1.1.4 GPKIの課題 - 認証局が要求する証明書のフォーマット	16
1.2 商業登記に基礎を置く電子認証制度の概要と今後の展望	17
1.2.1 商業登記制度の意義	17
1.2.2 電子認証制度のあらまし	18
1.2.3 電子認証制度の展望と課題	23
1.3 電子認証サービスの現状について	26
1.3.1 電子認証サービスの現状	26
1.3.2 電子認証サービスの将来像	31
1.3.3 ユビキタス・ネットワークと認証	35
1.3.4 リアル社会とサイバー社会の接点	37
2 電子署名・認証の利用形態と利用動向（アンケート調査）	41
2.1 電子署名・認証の利用形態	41
2.1.1 用途	41
2.1.2 認証局形態	42
2.2 電子署名・認証の利用動向	44
2.2.1 アンケート調査実施概要	44
2.2.2 アンケート調査票回収企業の概要	44
2.2.3 アンケート調査結果	46
2.2.3.1 商取引におけるインターネットの普及状況	46
2.2.3.2 情報システムの導入とセキュリティ対策	48
2.2.3.3 インターネット導入とセキュリティ対策に関する分析	61
2.2.3.4 PKIの利用実態	64
2.3 電子署名・認証の普及課題	70

2.3.1	PKI 利用企業の課題評価.....	70
2.3.2	PKI 非導入企業の非導入理由.....	71
2.3.3	PKI の課題分析.....	72
参考文献	74
・メンバーリスト	74

はじめに

国内におけるPKI推進活動は、これまで政府、各地方公共団体、各業界団体、ユーザ企業等の組織ごとに進められており、必ずしも統一的な方針、さらには、多くのユーザの意見を集めた接続性、運用性を重視したものになっては無く、かつ、PKI推進にかかわる情報の流通も十分ではないといった課題がある。

日本のPKI推進の連携を進めるためには、広くPKI推進にかかわる団体が集まり、各団体の成果・課題、等の情報を収集・蓄積・共有し、PKI相互運用性の確保などの共通課題についてはユーザの視点で検討を行える場を提供するとともに、蓄積された各団体の成果、検討結果の普及、啓発活動に取り組む組織の設立に向け具体的な検討を進める必要がある。

PKI連携推進フォーラムでは、PKIの普及広報を目的に平成13年10月1日に情報化月間特別シンポジウム「電子署名・認証でどう変わる電子商取引 - 電子認証基盤・サービスの現状と展望」を開催した。（この概要はECOM Journal 第3号で紹介した。）また、我が国では、PKIに関して、その技術や制度の標準化、実装評価、認証サービス等に様々な団体が関与しているが、これらの団体がそれぞれの活動を活かしながら連携する場の構築を目指す、「電子署名・認証利用パートナーシップ（仮称）」設立のための準備会を立ち上げた。（この概要はECOM Journal 第4号で紹介した。）

それと並行して、「電子署名と電子認証の現状及び将来像調査」を行い、その中でECOM会員に対するアンケート調査を行った。この調査については、別途報告書の形で公開する予定である。

本報告は、本フォーラムの活動を紹介する目的で、以上の活動を報告書としてまとめたものである。

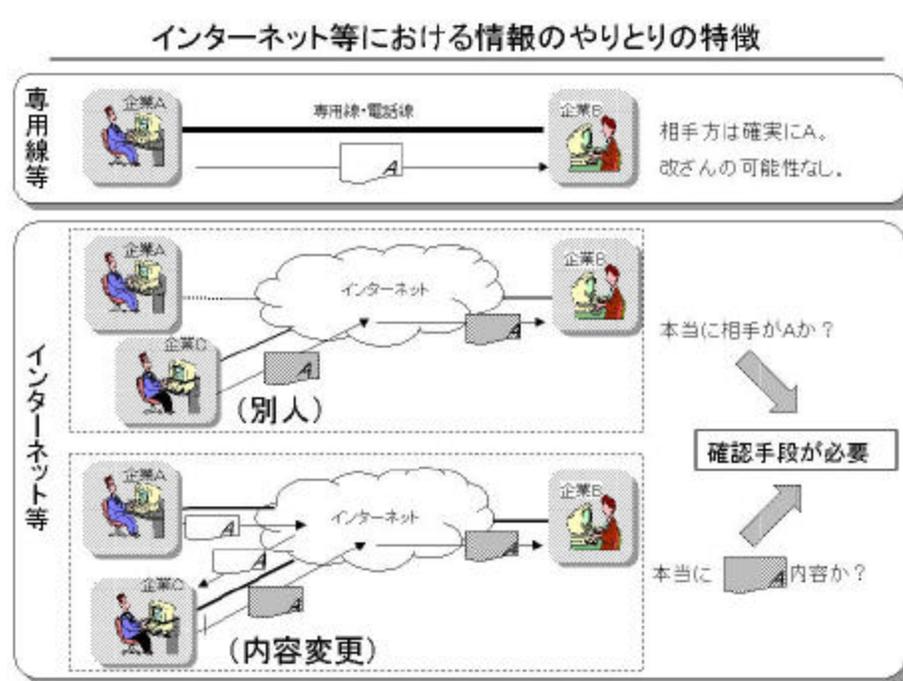
1 P K Iの動向

1.1 政府における電子署名・認証の推進と取り組み

1.1.1 P K Iの必要性

(1) サイバー空間の特質

サイバー空間の特質のためP K I（公開鍵基盤）の必要性が出てくる。すなわち、従来専用線で行われていた情報交換においては、情報の流れは完全に管理をされて、情報のやりとりは信頼ができるもの、他者が改ざんする余地がないものとして運用が進められてきた。しかし、インターネットの普及によって、通信経路に誰も管理していない部分が現れた。このため、受け手側は、送られてきた情報が相手のものなのか、あるいは相手の情報が正しいものなのかについては、このサイバー空間（インターネット空間）において、何の保証や確認ができないことになる。その結果、なりすましとか、情報の改ざんなどの詐欺ができるようになる。



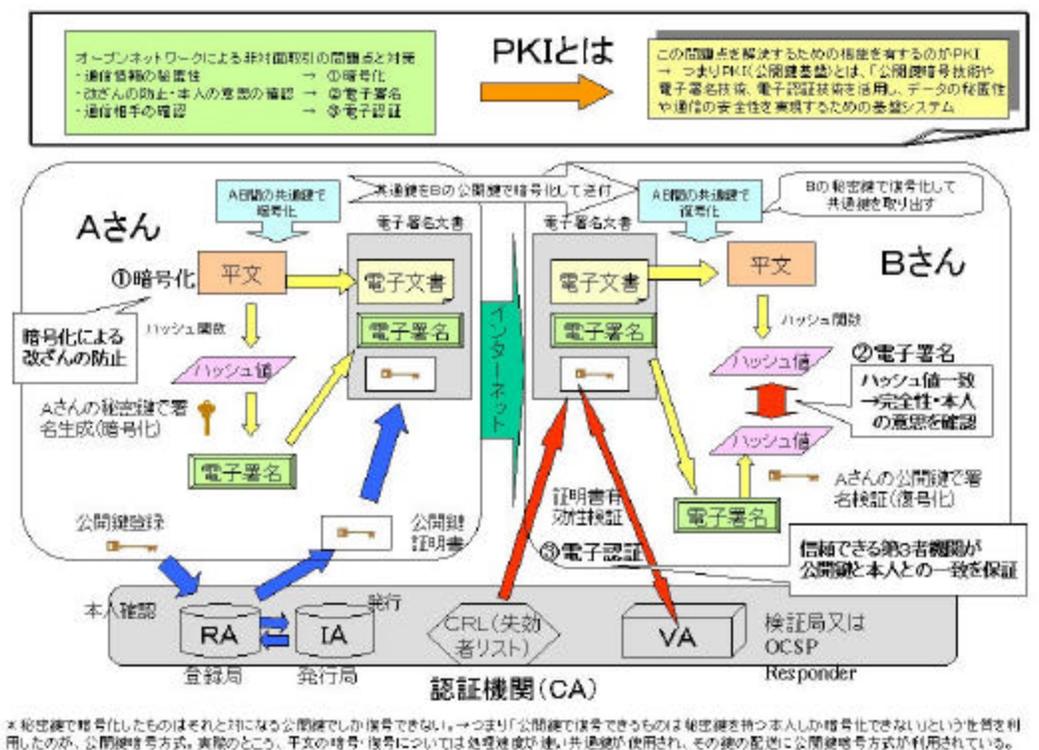
出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-1 インターネット等における情報のやり取りの特徴

すなわち、図 1-1 に示すとおり、専用線の際には、B さんから見れば相手方は確

実に A さんであり、改ざんの可能性はない。しかしながら、インターネットを用いた場合には、A さんからの情報として、A さんは情報を流していないにもかかわらず、別人が A さんの名前をかたって流したり、あるいは、A さんは実際に情報を流しているけれども、途中で内容の変更が行われる可能性がある。これらの課題について、インターネット上は何も保証されない。したがって確認手段としてこの P K I が必要になる。

(2) P K I のビジネスでの利用



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-2 PKIのビジネスでの利用

PKIとして実際にビジネスで利用されている方法を図 1-2 に示す。オープンネットワークによる非対面取引の問題点と対策として、通信情報の秘匿性をどのように確保するのか、改ざんの防止、本人の意思の確認をどのように行うか、および、通信相手の確認をどのように行うかがある。

この3つの確認を解決する手段としてPKIがある。

秘匿性については暗号化が有効である。

改ざんの防止等については、電子署名が有効である。

通信相手の確認については電子認証が有効である。

具体的な取引の中で、「それでは文書のやりとりをしよう」とした場合には、

ステップ 1

Aさんは、平文を暗号化してBさんに送る。共通鍵を用いてこの文書を暗号化する場合、AB間で、共通鍵をBさんの公開鍵で暗号化して送る。すなわち、共通鍵をBの公開鍵で暗号化して送り、受けたBさんはその共通鍵で暗号文書を復号化する。

ステップ 2

Aさんは、平文にハッシュ関数をかけてハッシュ値を得る。次にそのハッシュ値をAさんの秘密鍵を使って暗号化する。これが電子署名であり、この電子署名を文書に添付して送る。

ステップ 3

Aさんは、この電子署名文書をつくるにあたり、電子認証をするときの認証機関に対しあらかじめ公開鍵を登録する。登録は、本人確認をしたのちこの認証機関が「その公開鍵がAさんのものである」ことを示す証明書を出す。その証明書を、Aさんは自分の文書の添付してBさんに送る。

ステップ 4

受け取ったBさんは、送られてきているBさんの公開鍵で共通鍵を復号化して、この送られてきた電子文書を平文化する。そして、この平文にハッシュ関数を用いてハッシュ値を得る。つぎに、送られてきた文書に添付されている電子署名を公開鍵を使って復号化してハッシュ値を得、この2つのハッシュ値一致していれば、この文書が改ざんされていないことがわかる。

つぎに、認証機関に対し、証明書とこの文書が本当にAさんのものか、送られてきた公開鍵と本人との一致を検証してもらう。その検証がなされて初めて、これはAさんがつくった真正な電子文書であることが確認される。

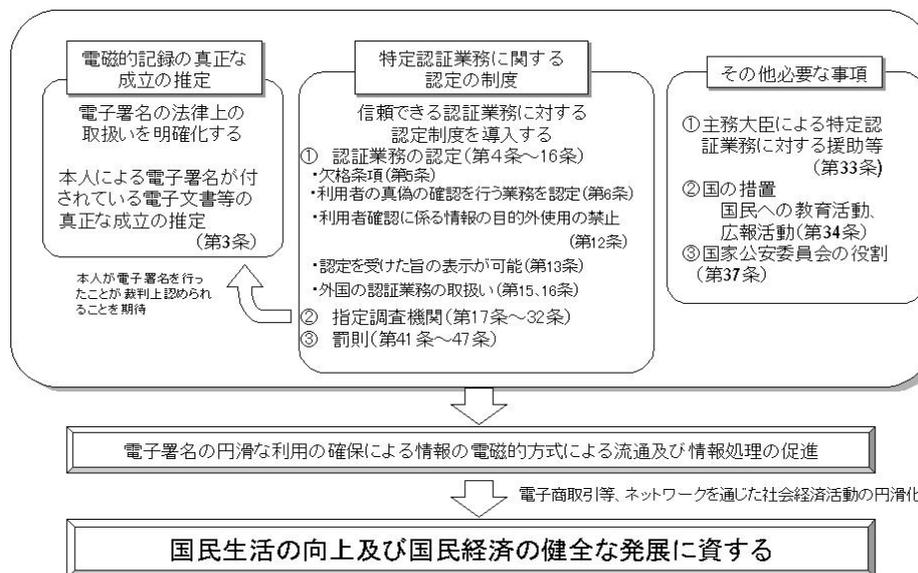
これが一連のPKIを利用した処理の流れである。

1.1.2 電子署名及び認証業務に関する法律

(1) 法律の構成

2001年4月から電子署名認証法が施行している。図1-3にこの法律の構成を示す。この法律上は、大きく分けると2つの内容からなっている。一つが「電磁的記録の真正な成立の推定」である。まず、電子署名の法律上の取り扱いを明確化し、本人による電子署名が付されている電子文書等の真正な成立の推定をしていくものである。電子署名がついていると、その文書が真正なものであることの推定効が働く。

電子署名及び認証業務に関する法律の構成



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-3 電子署名及び認証業務に関する法律の構成

もう一つが、「特定認証業務に関する認定の制度」である。これは、ボランティアな認定制度であり、本人の署名であることを証明する証明書を発行したり検証したりする機関の認定を行うものである。ただ、この認定がないと認証業務をできないのではなく、認定を得れば業務の信頼性の証明になり、非常に質の高い業務を行っていることを政府として認定する制度である。

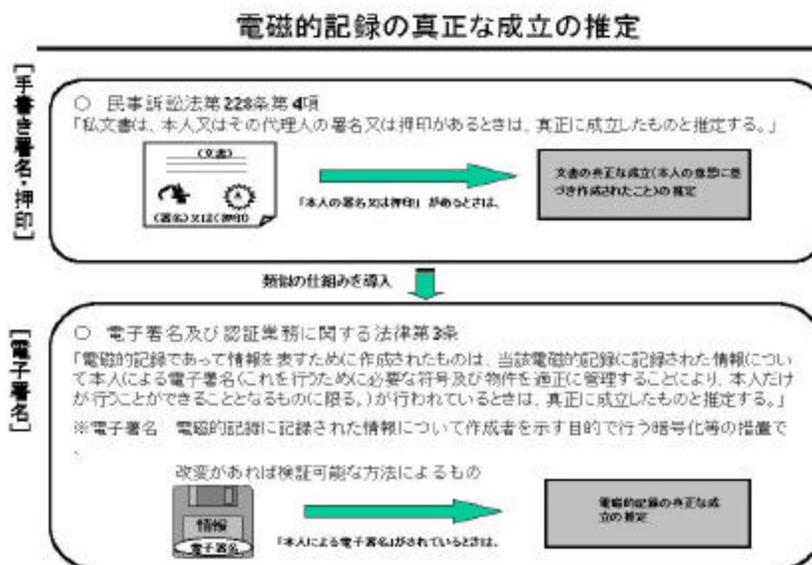
この2つの制度により、「電子署名の円滑な利用の確保による情報の電磁的方式による流通及び情報処理の促進をする」目的で、電子商取引あるいは電子署名の利用を

促進していこうとしている。

(2) 電磁的記録の真正な成立の推定

「電磁的記録の真正な成立の推定」は現在の民事訴訟法に規定がある。民事訴訟手続において、電子署名がいわゆる手書きの署名と同様の取り扱いをしてもらうことがこの規定の趣旨であり、取引において電子署名が、実印と同じ取り扱いになる（図 1-4 参照）。

民事訴訟法上は、「私文書は、本人またはその代理人の署名または押印があるときには、真正に成立したものと推定する」という扱いになる。また、電子署名の場合にも、「電磁的記録であって情報を表すために作成されたものは、当該電磁的記録に記録された情報について本人による電子署名が行われているときは、真正に成立したものと推定する」という規定が 3 条にある。これは、電子署名が実際の手書きの署名、押印、などと同様に扱われることを意味する。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

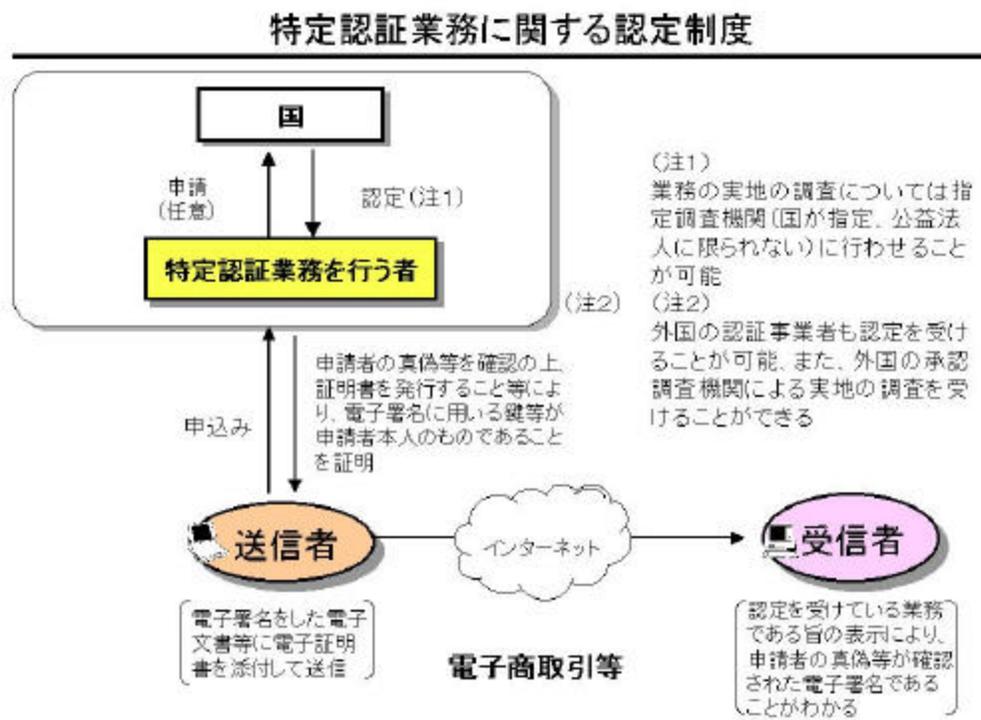
図 1-4 電磁的記録の真正な成立の推定

(3) 特定認証業務

「特定認証業務」は、国が認証業務を行っている会社について、その業務が一定のレベルの質を持ったものであることが確認できれば認定をするものである。図 1-5 に概要を示す。その認定は、実際に調査の上国が認定をしてもいいが指定調査機関が認

定をしてもよく、現在は日本品質保証機構（JQA）が指定調査をしている。

また、法律上は、この特定認証業務、認証業務を特定する行為については、外国の同様の制度との相互承認の制度がある。したがって、外国においてもこの相互承認をするためには二国間で取り決めをする必要がある。日本で特定認証業務の認定を得ている場合は、取り決めをした相手の国においても同様な取り扱いを受ける仕組みである。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-5 特定認証業務に関する認定制度

認定を受けるための要件

特定認証業務の認定を受けるにあたっての要件として以下の3項目がある。

ただし、禁錮以上の刑や本法違反による刑に処せられた者又は認定を取り消された者等は、一定の期間認定を受けられない。

A.業務の用に供する設備

- 認証業務に利用する秘密鍵の厳重な保管

- 安全・信頼性を有する設備の使用 等

B.利用者の真偽の確認の方法

- 公的機関の発行する証明書の提示を求める 等

C.その他の業務方法

- 業務管理規定を定め適当な権限分散を図っていること
- 失効リストの適切な開示 等

認定の効果

認定の効果は、一定のサービスの質があることが確認されることであり、法律上の規定としては「当該業務が認定を受けている旨の表示が可能である」ことによつて受信者の信頼の目安になる。

A.当該業務が認定を受けている旨の表示が可能

- 受信者の信頼の目安
- 裁判上、本人が行った電子署名であると認められることを期待

認定認証事業者の義務

義務については、いわゆる帳簿の保存の義務や「利用者確認に係る情報の目的外使用の禁止」の規定がある。

利用者の真偽の確認資料等の保存義務（帳簿保存義務）

利用者確認に係る情報の目的外使用の禁止罰則利用者が認定認証事業者等に対し不実の証明をさせる行為についての罰則（3年以下の懲役又は200万円以下の罰金）等

(4) 相互承認

「我が国の認定制度に類する外国の制度に基づいて、外国にある事業所により認定業務を行っている場合に、我が国の認定を受ける際の特例を定めるものである」であり、認定の審査手続の簡素化、具体的には指定調査機関の調査が省略される。

背景

ネットワークを利用した情報のやりとりはグローバルな性格を持つものであり、日本の認証事業者の証明に係るもののみならず、外国の認証事業者の証明に係るものも出てくることが予想される。

電子署名及び認証業務に関する法律第15条第3項

我が国の認定制度に類する外国の制度に基づいて、外国にある事業所により認証

業務を行っている場合に、我が国の認定を受ける際の特例（認定の審査手続の簡素化等）を定めるものである。

相互承認の推進状況

日・シンガポール新時代経済連携協定（JSEPA）締結に向けた協議の中で、電子署名法に係る認定の相互承認について議論している。

認定の相互承認が行われた場合、シンガポールの電子取引法における認証機関に対するライセンスがあれば、日本の電子署名法における特定認証業務の認定を受ける手続が簡素化される。（逆に、日本の認定を受けていれば、シンガポールのライセンスを取得する手続も簡素化される。）

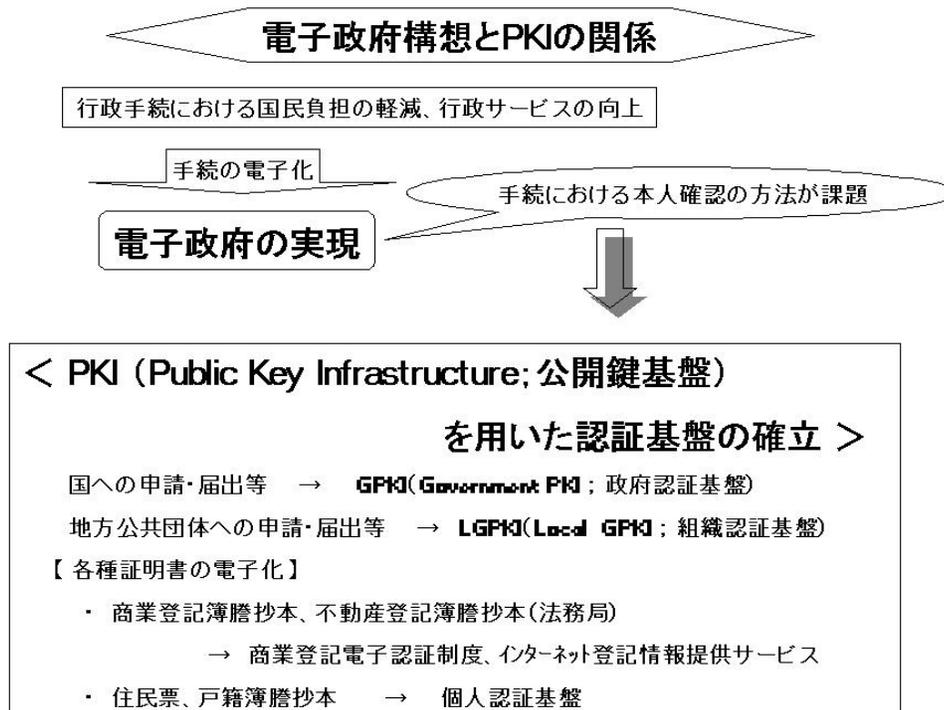
この認定の相互承認が行われる場合には、シンガポールの電子取引法による認証機関に対するライセンスを持っていれば、日本の電子署名法における特定認証業務の認定を受ける手続が簡素化される。これは逆もしかりで、日本の認証機関がシンガポールでライセンスを取得する場合にも、手続の簡素化が行われる。

1.1.3 電子政府構想におけるGPKIの推進状況

(1) 電子政府構想とPKI

電子政府における認証は図 1-6 に示すとおり、PKIを採用している。「行政手続における国民負担の軽減、行政サービスの向上」を目的に、2003年の電子政府の実現を目指して進めてきている。

国への申請や届出等について、GPKI（Government PKI；政府認証基盤）をつくる。そして、地方公共団体等の申請・届出等については、地方でも同様に認証基盤をつくらうとしている。また、各種証明書の電子化を図るために、商業登記簿の謄本であるとか、不動産の登記簿の抄本を認証するサービス・制度や情報提供サービスを作ろうとしている。また、住民票、戸籍簿の謄抄本についても、公的個人認証基盤を作っていく。これは住民票に代わるものである。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

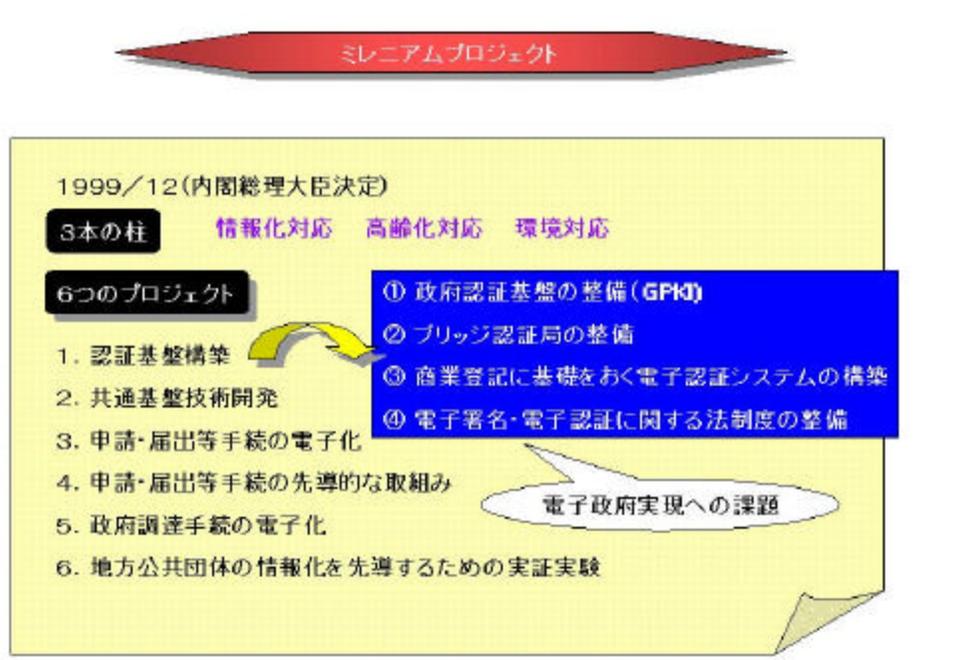
図 1-6 電子政府構想とPKIの関係

政府のIT関連の大きな計画としては、ミレニアムプロジェクトとIT重点化計画、情報化のe-Japan重点計画、及びe-Japan重点計画の14年度の施策をまとめたe-Japan2002プログラム、が基本的な計画として動いている。

(2) ミレニアムプロジェクト

情報化対応、高齢化対応、環境対応の3つの柱のうちの情報化対応のプロジェクトとして、図1-7に示すとおり6つのプロジェクトが挙げられている。その中の認証基盤の構築が、政府のPKI構築に係る部分である。その中身は、政府の認証基盤の整備、ブリッジ認証局の整備（政府の認証基盤は、各府省が認証局をつくり、それを束ねて対外的な外部との認証をする機関として、ブリッジ認証局を置く考え方）、商業登記に基礎を置く電子認証システムの構築、電子署名・電子認証に関する法制度の整

備、がある。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

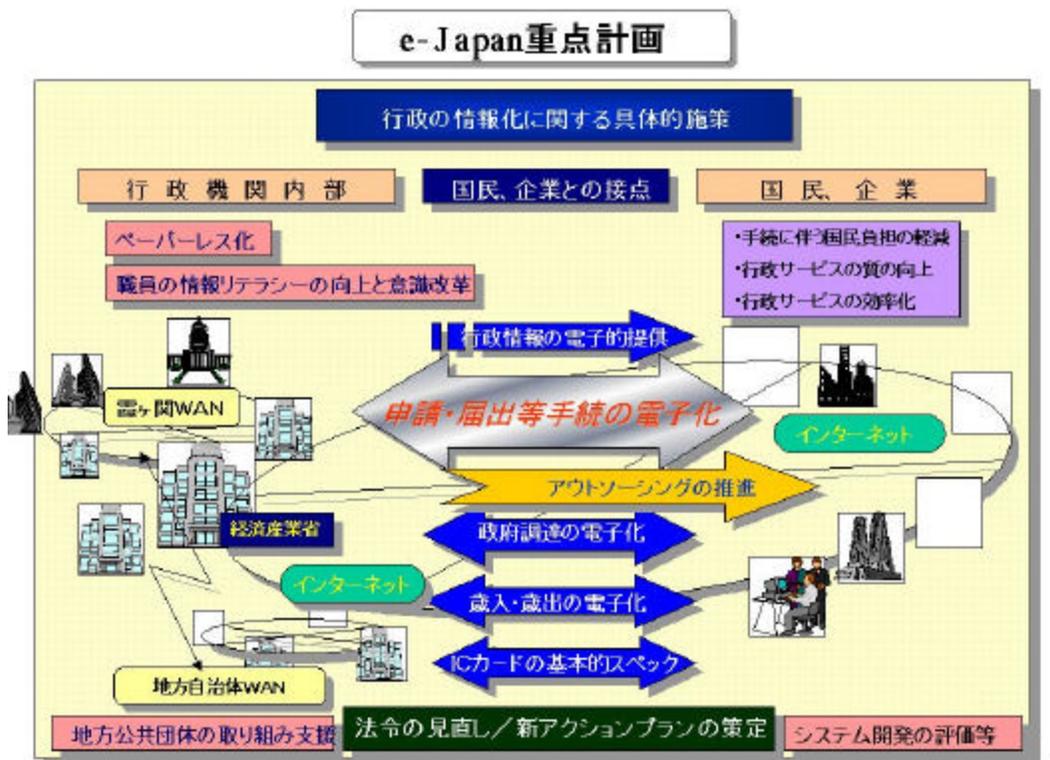
図 1-7 ミレニアムプロジェクト

(3) e-Japan 重点計画

行政の情報化に関する具体的な施策が5本ある。そのうち、電子認証、PKIに係る部分が「申請・届出等の手続の電子化」である。そこに、「国民と行政の間の実質的にすべての申請・届出等手続を、2003年度までのできるだけ早期にインターネット等で行うようにする」等とあり、そのための具体的な施策は以下のとおりである。また、e-Japan 重点計画の全体像を図 1-8 に示す。

- ・ 国民等と行政の間の実質的に全ての申請・届出等手続を、2003年度までのできる限り早期にインターネット等で行えるようにする。
 - ・ 各府省は、申請・届出等手続の電子化に関わる共通基盤システム（府省認証システム、複数の手続の受付・結果通知等について汎用的に利用できるシステム（以下「汎用受付等システム」という。））を2002年度までに整備する。（全府省）
- このため、行政情報化推進各省庁連絡会議において、汎用受付等システムの整備に

あたって、府省間で整合性を図る必要があるものについて、2001年度早期に基本的な仕様を取りまとめる。(総務省及び全府省)



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-8 e-Japan 重点計画

(4) 2002 プログラム

e-Japan 重点計画は 2001 年 3 月につくられている。2002 プログラムはその後、6 月か 7 月に取りまとめられて、平成 14 年度の施策として動いている。

以下、行政の情報化及び公共分野における情報通信技術の活用の推進内容を示す。

- ・ 行政情報の電子的提供：行政組織、制度等に関する基礎的な情報、予算及び決算に関する情報等の電子的提供。
- ・ 申請・届出等手続の電子化：認証システム、汎用受付等システム、手数料納付システム、文書管理システム等の整備。
- ・ 公的個人認証基盤の構築：住民基本台帳のデータを活用した地方公共団体による

公的個人認証システムの整備。

- ・政府調達の電子化：非公共事業における入札・開札システムの整備、一部公共事業における電子調達システムの整備。

- ・ペーパーレス化：本省と地方支分部局等のLAN間接続、国と地方公共団体等を通ずるネットワークの整備推進

- ・地方公共団体への取組支援：国の行政情報化と歩調を合わせた地方公共団体の情報化支援

- ・地方公共団体による広域的なシステム整備：複数の地方公共団体による広域的なシステム構築

- ・地方選挙における電子投票：地方公共団体の選挙における電子投票の試行を可能とするための取組

- ・システム開発に係る評価指標の策定・普及：ソフトウェア開発・調達プロセス評価指標モデルの普及

- ・公共分野における情報化の推進：科学技術・保健・医療・福祉・環境・防災・公共交通分野等の情報化等

- ・効率的な施策の推進：通信サービスの多様化、技術の進展等に応じた効率的なシステムの構築、施策の整合性確保

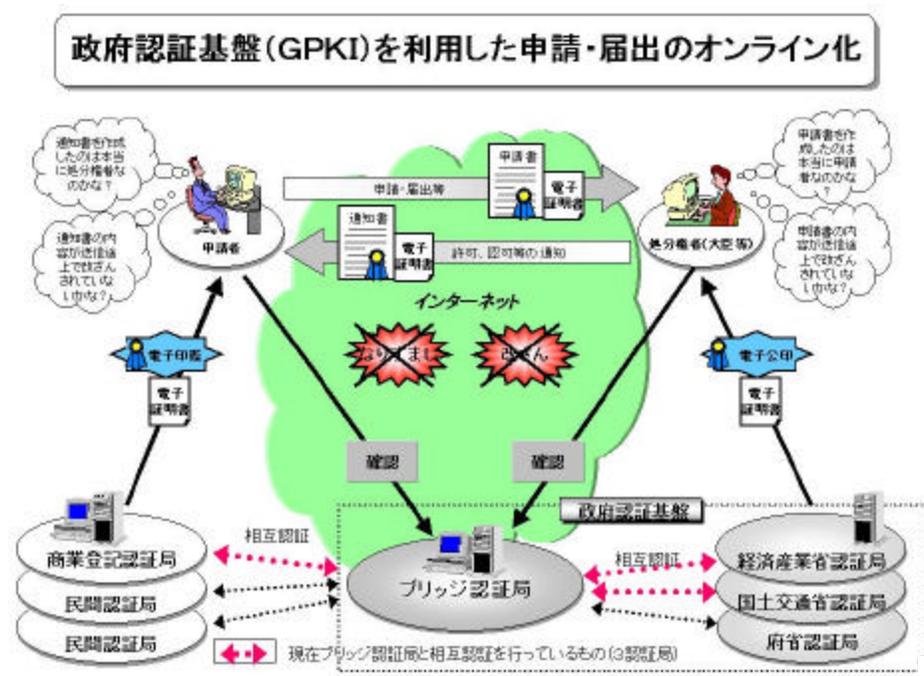
ここで、PKIの関係は、2番目の「申請・届出等手続の電子化」があり、認証システム、汎用受付等システム、手数料納付システム、文書管理システム等の整備を行うことと、LGPKIでは、公的個人認証基盤の構築として、住民基本台帳のデータを活用した地方公共団体による公的個人認証サービスの認証システムの整備がある。そのほか、電子化の関係では、情報の電子的な提供、政府調達の電子化、あるいは、地方選挙における電子投票などがある。

政府の認証基盤については、各府省の認証局とブリッジ認証局の仕組み・制度で構築していこうとしている。図1-9に示す。

これが政府が構築中の認証基盤であり、各府省の認証局とブリッジ認証局の間で相互の認証を行い、外部との相互認証はこのブリッジ認証局が行う。

基本的な電子認証の仕方は、PKIの仕組みと基本的には同じである。まず申請者が申請をし、処分権者は、その申請者からの申請書や届出が真正なものであるかどうか、あるいは本人のものであるか確認をする。次に、許認可等の通知を受けて、申請

者はこのブリッジ認証局に、これが真正なものであるかどうかを確認する。



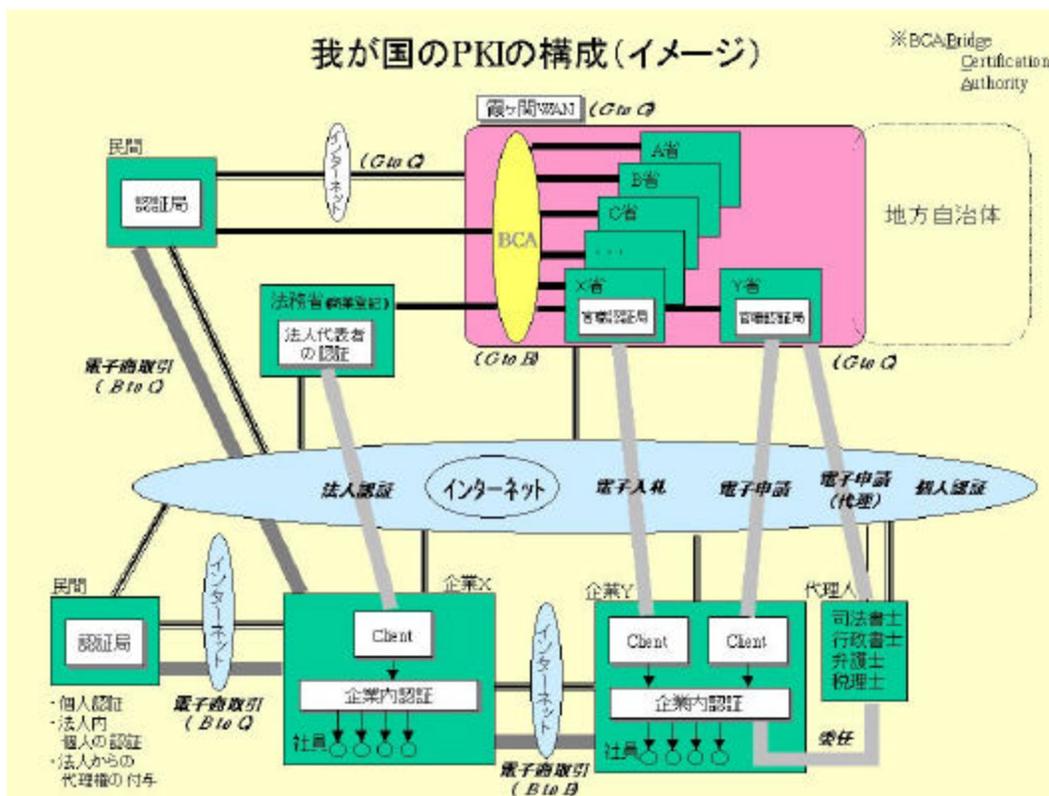
出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-9 政府認証基盤 (GPKI)を利用した申請、届出のオンライン化

ブリッジCAについては、府省CAの最上位のCAについてだけブリッジCAが機能する。そして、一方、府省CAについては、ブリッジCAを介して民間の認証局等と相互認証をしていこうとしている。そして、セキュリティの実施手順、その他運営に必要な諸規定については、ブリッジCAも府省CAも定めることになっている。

(5) 我が国のPKIの構成

図 1-10 に政府の霞ヶ関のPKIの姿を示す。これ以外に地方自治体のLGPKIが別途ある。また、民間の認証局との間で相互認証を行うことになる。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-10 わが国のPKIの構成イメージ

(6) 経済産業省電子公文書システム

経済産業省では、2001年6月18日に第1号の電子公文書の発出した。

まず、経済産業省では、大臣等の電子的署名の証明書を発行できる経済産業省の認証局を構築しており、2001年5月末から稼働を開始をしている。民間との間のインターネット上での申請等を電子的にやりとりできる汎用電子申請システムや電子的に受け取った文書についてペーパーレスで決裁できる電子決裁システムを構築している。

このシステムを使い、2001年6月18日に先行的に大臣による公文書の発出をした。このシステムを使うと、申請をインターネットで受け付けて、電子決裁をして承認を行うため、その間に紙を使う必要がない。あとは、担当官も一度も席を離れることなく手続が完了でき、業務の効率化にもつながる。

このシステムの特徴としては、完全ペーパーレスのシステムである。次に、汎用性のあるシステムであり、この汎用電子申請システムは経済産業省の手続のみならず将来的には他省庁の手続も対応可能である。そして3つ目は、インターネットを利用した安全なシステムである。つまり、強固な暗号を利用した通信を行う。4つ目が、商業登記認証局等の電子証明書の最大限に活用したもので、GPKIと相互認証した商業登記認証局等の電子証明書を一つ取得すれば、複数手続に対し電子申請が可能である。

具体的なプロセスを以下に示す。

申請者から、経済産業大臣あて電子公文書が送信される（汎用電子申請システムを利用）。

経済省側は、この申請を受信し、審査した上で、電子的に決裁する（電子決裁システムを利用）。

決裁終了後、施行文に大臣が電子署名し、大臣名の電子公文書（経済省認証局が発行した電子証明書が付く）を作成する（経済省認証局及び汎用電子申請システムを利用）。

この電子公文書を申請者へ送信する（汎用電子申請システムを利用）。

1.1.4 GPKIの課題 - 認証局が要求する証明書のフォーマット

電子証明書のフォーマットは国際電気通信連合が定めている X.509 の version3 で定められている。このフォーマットの中には、基本領域と拡張領域があって、基本領域の記入項目は規定されているが、拡張領域は認証局が使用できる。この拡張領域について政府内に取り決めがない。したがって、政府の各省庁はそれぞれ認証局を立てるため、その認証局ごとに拡張領域に情報を書くことができる。

各省庁が独自に決めると、証明書のプロファイルが各省ごとに乱立することになり、さらに、それぞれ手続ごとにこの拡張領域を使用すると、さらに手続ごとのプロファイルが乱立する。そうになると、証明書の汎用性はなくなる。

すなわち、ある省で使ったものと同じ証明書を、ほかの省で使えるか、電磁的にそれが読めるかどうか保証は全くない。すると、省庁へ手続ごとの証明書を別途それぞれ対応して作成する可能性が出てくる。したがって、拡張領域の使い方に対して、政府として決めていくことが必要である。

1.2 商業登記に基礎を置く電子認証制度の概要と今後の展望

1.2.1 商業登記制度の意義

(1) 商業登記とは

商業登記とは、会社その他の商人に関する事項を登記簿に記載することで、取引の安全と円滑を図り、商人・会社自身の信用の保持を図る制度である。「会社その他の商人」とは、個人商店も商人であり商号の登記をすることにより商業登記ができる。また、厳密には会社ではないが、外国会社も商業登記の中に入る。そこで、合名会社、合資会社、有限会社、株式会社、及び外国会社、その他の商号に関する事項を記載する。

管轄の登記所は、その営業所の所在地を管轄する法務局、及び法務局の支局・出張所で対応しており、全国に768ヶ所ある(2001年10月1日時点)。取り扱っている会社・法人の数は約350万社である。ここで、会社・法人あるが、商業登記は商法に基づく登記である。法人の登記は別にあり、例えば財団法人、社団法人、学校法人、宗教法人、社会福祉法人といった法人と名がつくものの登記は法人登記と呼ばれている。

(2) 登記事項証明書

登記簿自体は紙である。昔ながらの登記簿を基本にして登記業務を行っている登記所と、コンピュータに全ての登記事項をデータベース化して扱っている登記所と2種類ある。この登記事項証明書は、コンピュータで登記事務を取り扱っている庁の発行するもので、商号、本店、目的、役員等々が記録されている。これに法務局登記官のハンコがついて証明書が出る。

(3) 印鑑証明書

印鑑証明制度は、登記を受け付けるときに、その登記をする権限がある人であることを確認するための手段である。ある会社の登記がされると、その会社で、例えば「目的を変更する」、「商号を変更する」、「本店を移転する」あるいは「支店をつくる」など登記事項に変更がある場合に登記の申請をしなければならない。その登記の申請をする権限がある人かどうかを確認するためのハンコが、登記所に届け出た印鑑である。設立の登記をする際に、この印鑑を届け、印鑑簿と照合して、それに対応する印鑑を持っている人にこの印鑑証明書を発行する。この印鑑証明書には、商号と住所、代

表取締役名、及び代表者の生年月日が書いてある。

(4) 商業登記の役割

役割としては、以下のとおりである。

- ・会社は、登記により法人格を取得（設立、合併、会社分割の成立要件）。
- ・登記事項に変更があれば、遅滞なく変更登記をする義務。
- ・登記すべき事項は、登記しなければ善意の第三者に対抗できない。
- ・故意過失により不実の登記をした者は、善意の第三者に対抗できない。

(5) 登記内容の正確性確保のための手段

登記内容の正確性確保のための手段として、以下の規定があり、これらの規定全体によって登記内容の正確性が担保される。

- ・申請書には添付書面が必要（定款、議事録、市区町村長の印鑑証明など）。
- ・会社代表者の印鑑提出の制度（印鑑証明書）。
- ・無効・取消しの原因があると、登記申請を却下。
- ・登記を怠ると過料の制裁。
- ・虚偽の登記申請には刑事罰（公正証書原本不実記載罪）。

1.2.2 電子認証制度のあらまし

商業登記に基づく電子認証制度について以下に述べる。

(1) 信頼性の高い電子認証制度

信頼性の高い電子認証制度として、ネットワーク社会において商業登記情報を活用することができる。また、印鑑証明書、資格証明書と同等の機能を有する電子認証制度を提供することにより、抽象的に言えば、商業登記に基づく電子認証制度で、法人格の存在の証明、代表権限の証明、本人性の証明、が担保される。

(2) 電子証明書の取得

取得方法を図 1-11 を用いて説明する。商業登記に基づく電子認証制度自体は、2000 年の 4 月に商業登記法の改正法が国会で成立し、10 月から運用を開始している。東京法務局の本局と前橋地方法務局の 2 ヶ所でスタートしたが、その後鋭意全国展開を図り、2001 年 10 月時点で、全国で 61 ヶ所の登記所で運用している。全国に 350 万法人があるが、法人全体の約 40%がこの時点でカバーされている。2001 年度末までには、95 ヶ所の登記所で運用を開始する予定であり、全体の約 55%の法人がカバーされる予

定である。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-11 電子証明書の取得まで

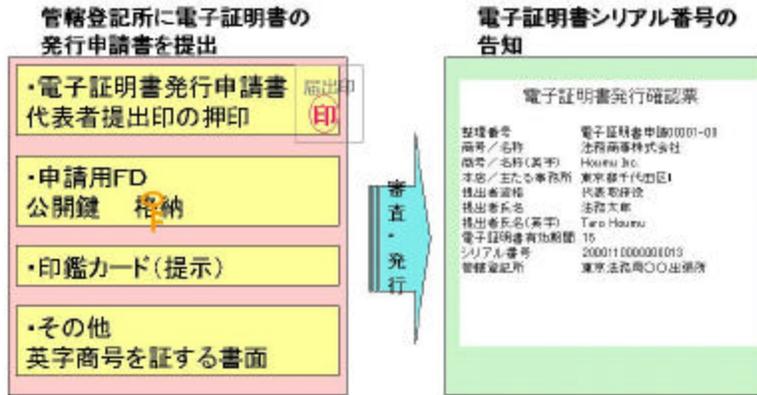
利用の流れを図 1-12 に示す。この「商業登記に基づく電子認証制度」は、商業登記所が商業登記情報に基づいて運営するもので、それ以外のサービスの部分は最小限になっている。

申請する場合、まず、市販の専用ソフトを申請者の側で購入・準備して、自分の秘密鍵と公開鍵のペアをつくる。この申請自体は、オフラインの申請であり、会社の代表者が自分の会社を管轄する登記所あるいは支局・出張所に行くか、郵送する。その際には、紙ベースの申請書に記入し、その申請書に会社の実印を押す。その実印を押した申請書と、専用ソフトでつくった公開鍵と電子証明書の記載事項等を記録したフロッピーディスクを一緒に提出する。

次に、管轄登記所では、本人からの申請に間違いがないか印鑑を確認することにより確認する。次に、フロッピーに記載された、電子証明書に書くべき、会社の本店所在地、商号、あるいは代表者氏名など、登記情報の確認を行う。確認後、受け取ったフロッピーの内容を、専用回線で電子認証登記所に送る。

電子証明書発行申請

管轄登記所に申請を行うと、審査が行われます。電子認証登記所で電子証明書が発行されると、管轄登記所の窓口で、そのシリアル番号が告知されます。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-12 電子証明書発行申請

電子認証登記所（東京に1ヶ所ある）に鍵管理装置等があり、登記官の秘密鍵によって電子署名をして証明書を発行する。申請窓口で電子証明書のシリアル番号を教え、発行した証明書はインターネットでアクセスしシリアル番号を入力することにより電子証明書が送信される。

以上で説明したように、このシステムでは鍵を管理しないため、秘密鍵の管理は代表者自身の責任で行う。

登記官作成の電子証明書の例を図 1-13 に示す。

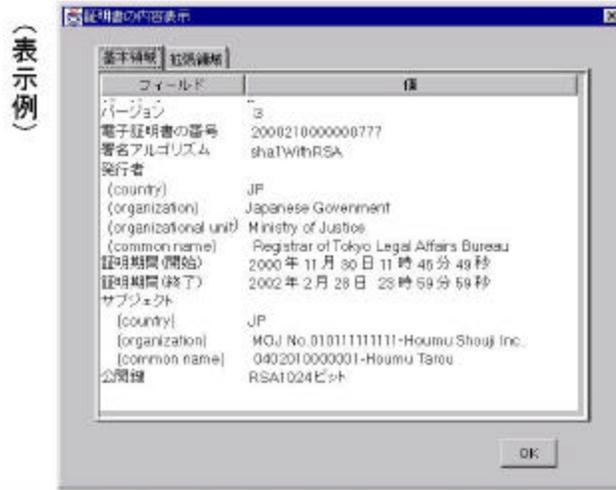
これは X . 509 の version3 に準拠してつくられたものである。

発行者は Ministry of Justice、common name が Register of Tokyo Legal Affairs Bureau であり、公開鍵は RSA1024 ビットである。

次に拡張領域部分を図 1-14 に示す。

この図において、登記官の証明書情報、登記官名、登記情報として商号または営業主、会社法人等番号（それぞれの登記所ごとに会社法人に番号を振っている）、本店の所在地、印鑑提出者の氏名、印鑑提出者の資格、登記所、などが記入されている。

登記官作成の電子証明書(標準領域部分)



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-13 登記官作成の電子証明書(標準領域部分)

登記官作成の電子証明書(拡張領域部分)



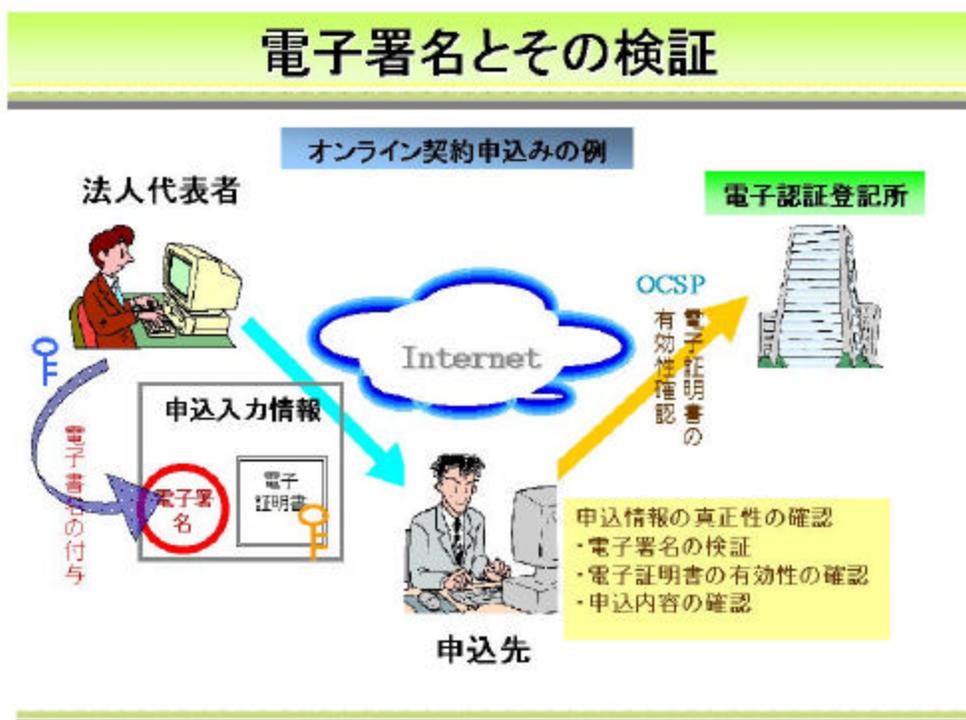
出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-14 登記官作成の電子証明書(拡張領域部分)

(3) 電子署名とその検証

有効性確認について、図 1-15 を用いて説明する。

電子署名をして相手方に送るまでは一般の電子署名の使い方と同じである。しかし、商業登記に基づくものは有効性確認に特徴がある。電子証明書の拡張領域部分に「サービスへのアクセス」があり、メソッドはOCSP (Online Certificate Status Protocol)、ロケーション等、記入されている。ここでこの電子証明書の失効情報、保留情報などのステータスがわかる仕組みになっている。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-15 電子署名とその検証

ここまでは普通のOCSPと同じだが、この「電子認証登記所」は、この先にある管轄登記所と連携しており、管轄登記所で登記情報の変更があるとその登記情報の変更がここに送られる。したがって会社代表者の交代、商号の変更、場合によっては破産した場合には、登記情報として管轄登記所で登記情報に変更が加わり、発行した電子証明書の事項に変更が生じている場合には、直ちに管轄登記所から電子認証登記所

に連絡が行く。このように、商業登記の電子認証は、商業登記情報をリアルタイムに反映した有効性確認ができる仕組みが特徴である。

1.2.3 電子認証制度の展望と課題

当面予定される動きについて述べる。

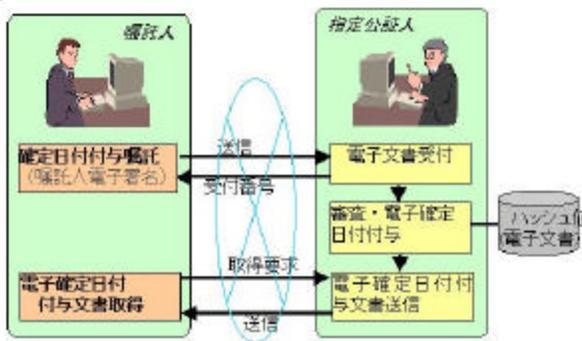
(1) 「公証制度に基礎を置く電子公証制度」との制度的連携

図 1-16 に示すとおり「公証制度に基礎を置く電子公証制度」は、2000 年の 4 月に成立した商業登記法等の一部を改正する法律の際に合わせて公証人法が改正されて、公証人が電子的な手段で確定日付を付与する「電子確定日付の付与」制度が導入された。この制度は、インターネットで情報を送信して、公証人が電子確定日付を付して送る制度である。

公証制度に基礎を置く電子公証制度(1)

1. 電子確定日付の付与

- ① 電子確定日付の付与を囑託する情報をインターネットで指定公証人に送信し、受付番号を受信
- ② 指定公証人は内容確認後、電子署名を行い、そのハッシュ値を保管
- ③ 囑託人は受付番号を指定して、電子確定日付付与文書を取得



電子確定日付付与文書には、法律上「確定日付アル証書」と同一の効果が認められる。 → 「完全ナル証拠力」

出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-16 公証制度に基礎を置く電子公証制度(1)

「電磁的記録（電子私署証書）の認証」は、図 1-17 の説明では、「公証人によって電子文書に行った電子署名の真正が証明される」となっているが、ここに言う認証とは、電子認証の認証とは違い、公証人法の「公証人の面前で電子署名をしたことを認証する」で使われる認証である。電子の世界とオフラインの世界とが入り混じったものだが、ニーズとしては、外国に公証人の認証のある文書を送る場合、今までは紙の公証人の認証文書しかできないが、この電磁的な認証制度によると、署名は公証人の所に行く必要があるが、電子的な公正証書ができるため、海外等に送る際には非常に便利な制度である。

「ハッシュ値または同一情報の保存と内容の証明」は、公証人の業務として、ハッシュ値の保存と存在証明をしたり、同一情報の保存と謄本の提供をしたりする仕組みである。この電子公証制度は、平成 14 年度導入の予定である。

公証制度に基礎を置く電子公証制度(2)

2. 電磁的記録(電子私署証書)の認証

公証人によって、電子文書に行った電子署名の真正が証明される。

3. ハッシュ値又は同一情報の保存と内容の証明

3-1. ハッシュ値の保存と存在証明(情報の同一性の証明)

電子確定日付付与文書、電子私書証書は、ハッシュ値が保存される。



電子確定日付付与や認証が公証人によってなされたものであること(同一性)の証明を請求できる。

←オンライン又はオフラインいずれも対応

3-2. 同一情報の保存と謄本の提供

電子確定日付付与文書、電子私書証書そのもの(同一情報)の保存を請求できる。



電子確定日付付与文書、電子私書証書の同一情報(謄本)を取得できる。

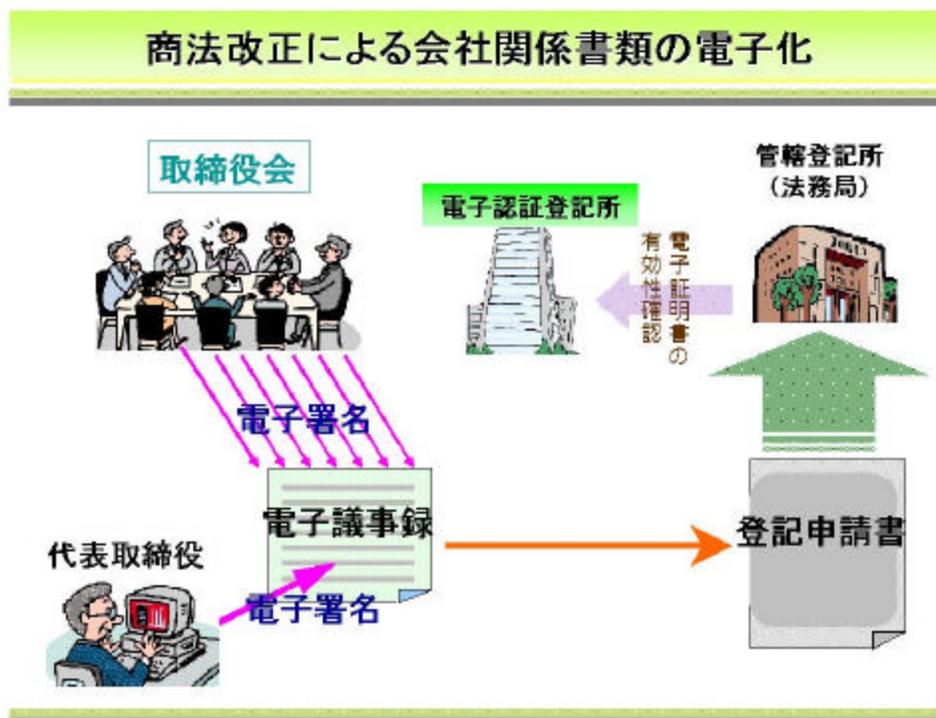
←オンライン又はオフラインいずれも対応

出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-17 公証制度に基礎を置く電子公証制度(2)

(2) 「商法改正による会社関係書類の電子化」

図 1-18 に示す「商法改正による会社関係書類の電子化」は、商法ではこれまで株主総会の招集通知などは書面でなければならなかったが電子的に作成することができるようにしたものである。この中では、特に定款とか議事録、株主総会議事録、取締役会議事録、さらに貸借対照表等の計算書類を電子的に作成し、その電子情報に電子署名をすることにより、定款、あるいは議事録とすることができる制度である。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.E.COM.or.jp/>

図 1-18 商法改正による会社関係書類の電子化

(3) 今後の取り組みと課題

この商業登記に基づく電子認証制度を幅広く、多くの場面で利用して、電子政府の実現、あるいは電子取引社会の実現に役立てるためには以下の課題がある。

電子認証制度の運用の早期全国展開

- ・「電子政府」の実現に向けたスケジュールとの整合
公開鍵暗号方式による「電子署名」の普及と利用環境の拡大
- ・情報通信セキュリティの手段 署名・押印に代わる利用
利用手数料の見直し
- ・電子商取引・電子申請の普及を牽引
- ・中小企業にも利用しやすい料金設定の要請 など

1.3 電子認証サービスの現状について

1.3.1 電子認証サービスの現状

(1) PKIとID/PW

PKIと簡易な認証方式であるID/PW方式について比較検討を行う。

当然それぞれ一長一短あり、ID/PW方式は、セキュリティが低い。ただしPKI方式は、その導入コストが高く、教育、あるいは管理運用面で非常に煩雑なところがある。一般的にはどの程度のセキュリティが要求されるか、などによって、ID/PWと言うのを完全否定するものではない。図1-19に比較結果を載せる。

	PKI方式	ID/PW方式
コスト	○ - 新規システムやICカードなどの導入コストが必要 - 教育コストも必要	● - 既存のシステムでほぼ対応済み
集中管理	● - 証明書のDBは集中管理されている - 登録・失効管理は煩雑	● - 複数のリソースに複数のユーザが複数のID/PWでアクセスしている
使い勝手	○ - 高度なセキュリティを要するプロセスでも利用者は簡単に利用可能 - 認証失敗の原因がわかりづらい	○ - セキュリティの高さに比例して、利便性が悪くなる(文字列を長くする、多重化するなど)
安全性	● - ハッキングの可能性はほぼゼロ	○ - ハッキング可能

・ コスト面ではID/PW方式に分があるものの、管理や利便性、セキュリティ面ではPKIに優位性があり、使い分けが求められる

出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-19 PKI vs ID / PW方式

(2) PKIの導入例

PKIの導入例を図1-20に示す。一番多いのは、B to Bの取引におけるもの、あるいは社内のネットワークへのアクセスへの採用が第一に進んでいる。

対象	企業名	用途	目的	効果
営業用パソコン	ソニーマーケティング (2001年～)	営業社員のパソコンに指紋認証システムとPKIを導入	盗難、紛失時および外部からのネットワーク接続の際の内部情報漏洩防止	どこからでも、安全に社内サーバへのログインが可能となり、機動力ある営業活動が可能となった
グループ経営管理システム	日商岩井 (1999年10月～)	書類もしくはVANで行っていたデータ交換業務をインターネットに移行	連結決済情報の収集	大幅なコスト削減が可能になる(具体的な数値は不明)
対顧客機密情報交換	J.P.モルガン (1998年頃～)	インターネットを通じた機密情報の交換にPKIを導入	交渉過程における最高機密情報の漏洩、改竄、否認防止	カスタマイズド・ハードウェア暗号機が不要になったことで100万ドルのコスト削減が可能となった 平均3週間を要した取引条件交渉が3日で終わるようになった
情報のオンライン提供	帝国データバンク (1999年10月～)	企業データのオンライン提供にPKIを導入	アクセス者の管理	電子商取引が円滑に進行

・ PKI非導入企業は、情報漏洩の被害者となった場合でも、企業としての義務を果たしていないとみなされ、大きな損失を被る可能性がある

出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図1-20 PKI導入例

(3) PKIの自社構築とアウトソーシング

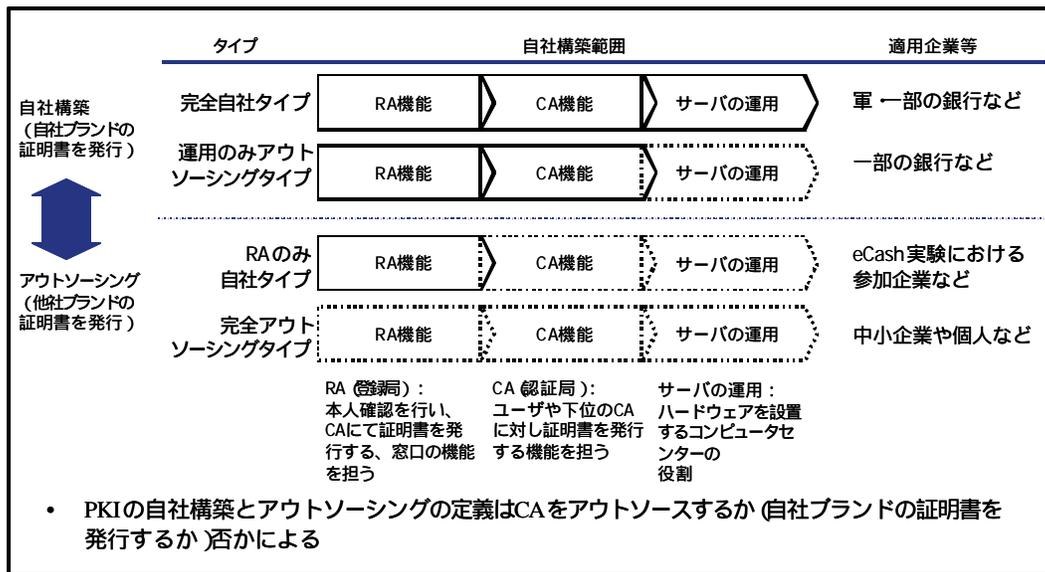
PKI導入において、PKIを自社で構築するかアウトソーシングするかが問題となる。一般的にどちらがいいということはなく、何に使うか、そしてどういう設備、どのぐらいのコストをかけられるかで決まってくる。

図1-21にその比較を示す。

完全自社タイプでは、サーバの運用、RAからサーバの運用まで一貫してやるが、しっかりした目的と用途がないと、コスト面でも運用面でも負荷が多い。比較的多いのがサーバの運用だけをアウトソースして、RAとCAについては自社でやるタイプである。

もう一段下がると、RA機能だけは自分でやるが、あとはアウトソースするタイプである。RAは当然自分の所でどのように登録するか、何を認めて何を登録するかが一番重要になる部分である。

完全アウトソーシングタイプは、比較的小さい企業であるとか、個人向けのものなどに限られる。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-21 PKIの自社構築とアウトソーシング

(4) PKIシステム構築における留意点

PKIシステム構築における留意点として、情報システムとしての面、あるいはセキュリティ強化の面が議論されがちである。しかし、PKIシステムはエンド・トゥ・エンドの全体で考えなければいけない。特に議論がされないのがPKIの利用範囲の特定である。また、CAの数と役割、証明書のライフサイクル管理、認証局運用規定(CPS)である。

(5) PKI構築の事例と特性

例えば完全自社タイプでは、運営主体が全ての責任を持つことになり、自由度は非常に高い。しかし、管理等が非常に大変である。完全アウトソーシングタイプはその逆であり、自由度は低い、比較的簡易に気軽にできる。そこで、誰が認証したかブランドが重要になる場合は、完全自社タイプか運用のみアウトソースするタイプになる。表にまとめたものを図 1-22 に示す。

タイプ	特徴	適用範囲	利用例	自由度
完全自社タイプ	- 完全に運営主体がすべて責任を持つ	- ログイン認証 - メールの署名・暗号化 - 電子決裁 - ファイルの暗号化	- 組織内での利用 - 金融機関の顧客	大
運用のみアウトソーシングタイプ	- センター施設や運用ノウハウの面で不安が有る場合	- ログイン認証 - メールの署名・暗号化 - 電子決裁 - ファイルの暗号化	- 組織内での利用 - 金融機関の顧客	中
RAのみ自社タイプ	- 他の企業が作成した認証ドメインに参加し、自主的に自らの提供するサービスについて自主的に認証する必要がある場合 - 証明書のブランドは自社ブランドではない	- 認証ドメインの中で、権限が与えられた範囲についてのログイン認証のコントロール - メールの署名・暗号化 - ファイルの暗号化	- 社内の一部部署が独自に発行するケースやグループ企業が発行する形態をとる場合に用いられることがある - ごく限られた利用範囲において採用	中
完全アウトソーシングタイプ	- コンシューマパッケージソフトの多くがこの形態 - 機能的には劣っていないが、証明書の身分証明力はきわめて低いことが多い	- コンシューマパッケージソフトの多くがこの形態 - ログイン認証 - メールの署名・暗号化 - ファイルの暗号化	- 広く消費者を対象とできるが、証明書の証明力は比較的弱く、実効性に乏しい - 対象は大きい、実売数・実利用数は小さい	小

出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-22 PK構築の事例と特性

(6) PKI 関連の法整備の動向

重要と考えられる法律について、図 1-23 に示す。

名称	内容	PKIとの関連
電子署名法 「電子署名および認証業務に関する法律」 2001年4月施行	- 手書きの署名や、紙への押印と同じ法的効力を電子署名にも認める - 一定の水準を満たしている民間の認証機関を国が認定する	- PKIがもっとも安価で確実な認証方法
IT書面一括法 「書面の交付等に関する情報通信の技術の利用のための関係法律の整備に関する法律」 2001年4月施行	- 従来、紙で交付することを義務付けている書面を、電子的手段で代替することを認めるもの - この法律で、訪問販売法、証券取引法、旅行業法など50の法律の改正を一括して行う	- PKIがもっとも安価で確実な認証方法
電子契約法 「電子消費者契約及び電子承諾通知に関する民法の特例に関する法律」 第151回通常国会で成立	- 電子契約の成立時期を承諾の通知の発信主義から到達主義へ転換 - クリックミスなどによる電子的意思表示について錯誤無効が認められる要件を明確化	- 紛争の際の証拠として成立させるためにPKIは重要
個人情報保護法 「個人情報の保護に関する法律」 第151回国会提出 衆議院で閉会中審査	- 一定以上の規模の個人情報データベースを持っている事業者は、本人からの情報開示や訂正、利用停止の求めに応じる義務が罰則付きで定められる。	- ID/PWでは情報漏洩の可能性が高く、法的責任を問われる可能性が高い(PKIの導入が必要)

• ネット上での取引の増大を睨んだ法制度が急ピッチで整備されつつある

出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-23 PKI 関連の法整備の動向

「IT書面一括法」は、紙で交付することを義務づけている書面を電子的手段で代

替することができる。「電子契約法」は、発信主義から到達主義へ転換するという
ことで、例えば時刻認証のようなものの重要性が増していく。

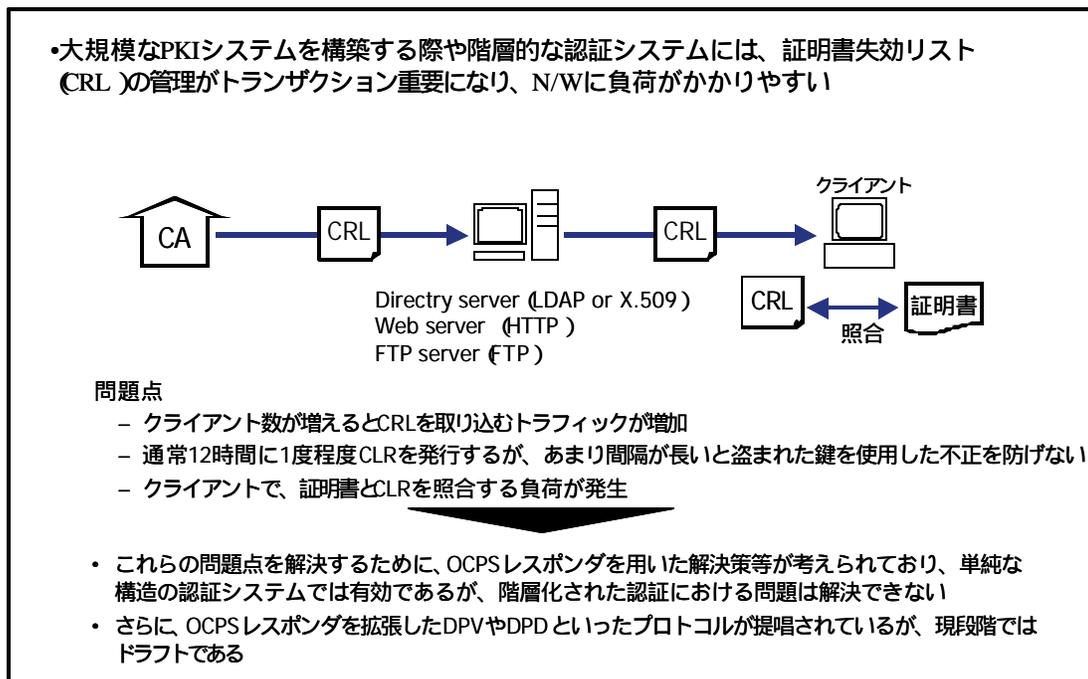
「個人情報保護法」は、情報の管理の問題であり、サーバに個人情報が平文で置い
てあり、そのままそっくり盗まれた場合の罰則、あるいは別の目的で集めた個人情報
を勝手に使う場合の罰則である。

(7) P K I 普及における課題

一つ目の課題は、複数の証明書、鍵の管理である。

各企業なり組織は一つのグループにしか属していないわけではなく、関係が錯綜し
てくる。そこで、いくつか解決の方法は提示されて実現に向けて動いている。

もう一つの課題は、認証システムを運用管理する場合、一番問題になるのは、失効
リスト(CRL)の管理である。これがトランザクション上、非常に重要になってく
る。失効の問い合わせ、照会の間隔を長くすると、失効したのがわからない、あるい
は鍵を盗まれたのを勝手に使われてしまうリスクがあるし、間隔を非常に短くすると、
今度はトラフィックが非常に増える。この関係を図 1-24 に示す。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-24 C R L 管理方法

(8) B to B 取引における発展形態

企業を中心とした企業グループ、あるいは業界内の垂直統合であるとか、業界横断の水平統合のような取引群がある。例えばGM社とフォード社のそれぞれの取引グループが、Covicint社という形で統合されたように、こういった形が一形態である。また、B to Bで同じソフトウェアを使うことにより、簡単に統合できる。例えばCommerce One社はそれを売りにしていた。このように、どのプラットフォームを用いているかにより、B to Bの取引のグループが大きくなっていくかに影響する方向が見られる。

(9) セキュリティ事件とそのインパクト

PKIを使って鍵が盗まれたとか、大きな事件は起きていない。広い意味でのセキュリティだと、事故が起こるのはヒューマンエラーによるものが多い。いくらシステムを強固にして管理を強固にしても、そのヒューマンエラー（故意と故意ではないもの両方含む）の教育、管理体制とがこれまで以上に重要になってくる。

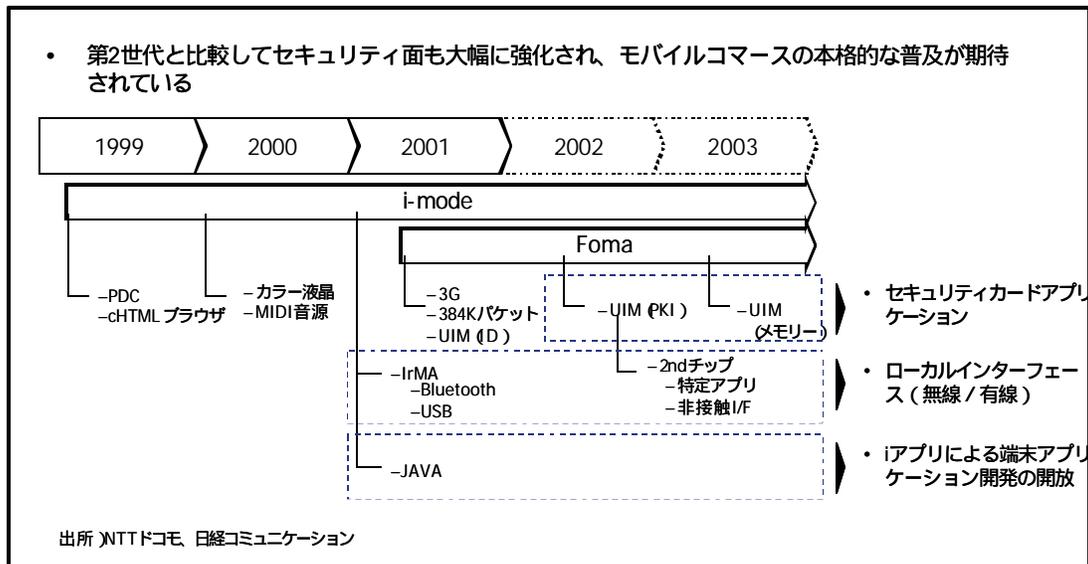
1.3.2 電子認証サービスの将来像

一つは第3世代の携帯電話である。図 1-25 に第3世代の携帯電話の技術ロードマップを示す。第2世代と比較して、セキュリティ面も非常に大幅に強化されて、モバイルコマースの本格的な普及が期待される。2001年10月からFOMA、ドコモの第3世代が始まり、2002年、2003年に向けて、UIMにPKIが導入される。あるいはセカンドスロットで非接触のインターフェースを持つとか、あるいはIrMAとかBluetoothなどのインターフェースを持つことが予定されている。

UIMは、ICカードのICチップ部分が携帯電話に入ったもので、ICカードと同じことがUIMでもできるようになり、電話番号と電話帳が入っている以外の部分を、セキュリティであるとか、通常のICカードアプリケーションに開放する動きがある。

携帯電話による認証であるが、UIM内に秘密鍵、公開鍵、Root CAの証明書を入れる。この場合、認証局の管理の問題がある。一つは大手の認証機関（VeriSign、エントラスト、等）あるいはコンテンツプロバイダーや金融機関が認証局を管理する場合である。もう一つは、移動体事業者自身が認証局を管理することが考えられる。ただし、現在の携帯電話のプロセッサだと、エンコード、デコード等全部携帯電話でやるのは性能から見て負担が重い。

もう一つは携帯電話であるが、無線インターフェースが採用されると無線区間でも認証が必要になる。例えば、駅の改札口をICカードの代わりに、携帯電話で通るであるとか、コンビニのレジで電子マネーで決済するであるとか、電子チケットとしてコンサート会場でゲートを通るであるなどである。こういった所では、当然高額なお金が絡み、個人情報問題もあり認証が必要になる。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-25 第3世代の携帯電話の技術ロードマップ

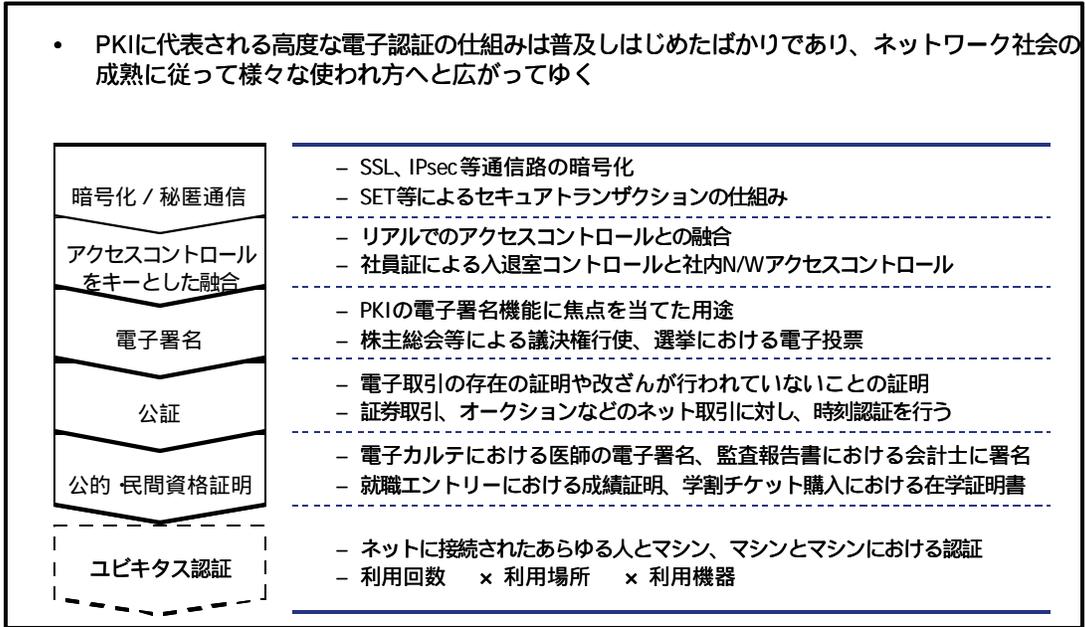
ただし、ネットの認証の場合は、ある程度時間がかかっても許される面はあるが、リアルにおいては、1秒よりもっと短い時間で処理しなければいけない。これはプロセッサ速度と供給電力の問題等々あるが、現状では、今のPKIの仕組みだと実現は困難である。

(1) 電子認証の進展

電子認証の進展を図 1-26 に示す。

暗号化や秘匿通信は既に利用されている。アクセスコントロールをキーとした融合（例えば、社員証がICカードになっていて、入退館の管理のカードになっている）したものをICカードに統合して管理する等ICカードを中心とした統合の動きがある。

PKIの使われ方として、今後は電子署名部分の部分に焦点が当たっていく。例として、商法改正によって、電子メールやホームページ上で、決算報告であるとか株主総会の招集通知をできるようになった。要するに、総会に出席しない株主が事前に電子的に議決権を行使、あるいは委任することができる。こういった公証・電子署名の使い方が増えてくるとネットで活動している個人株主も、まとまって大きなパワーを持って経営に物申すことが可能になる。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-26 電子認証の進展

もう一つ、広義の公証であるが、取引時刻の認証が重要になってくる。特に金融では非常に重要になるが、秒単位で非常に大きな利益やロスが出るため、その取引時刻が何時何分何秒であったかを公証する。これはNTTデータ社の「Secure Seal」、セイコーインスツルメント(SII)社の「タイムスタンプサービス」がある。

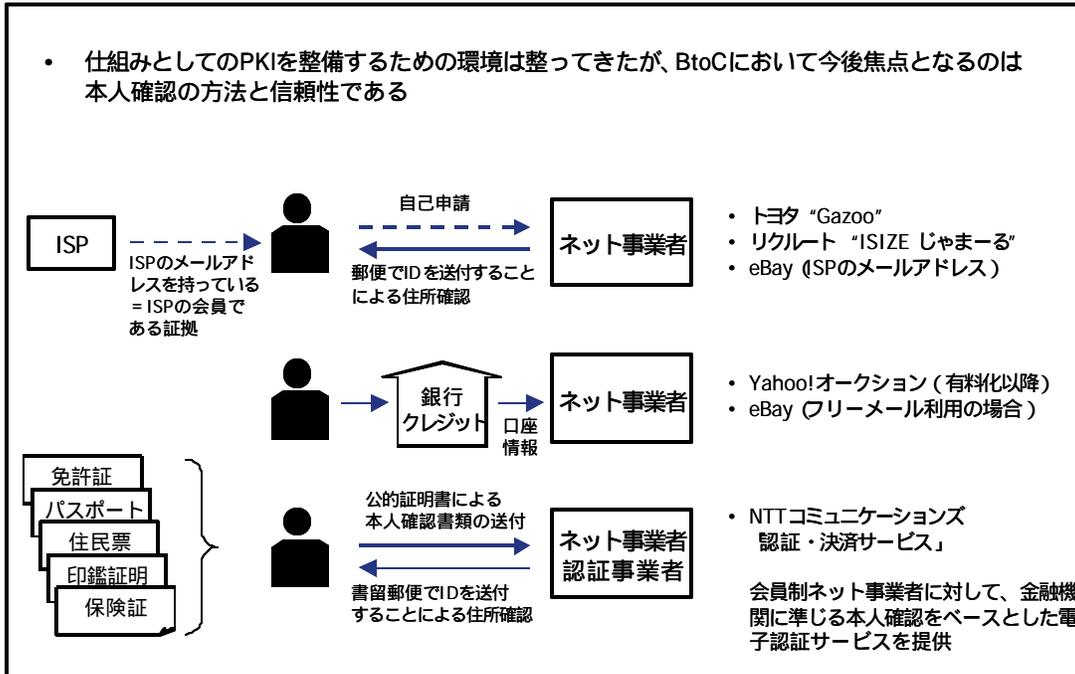
また、資格の証明による電子化の発展に関し、電子政府や e-Japan の絡みで関係ある部分だが、例えば、生命保険に入るために診断書は紙で書いて提出することになっているが、例えば電子的な診断書を発行してもらい、そこに医師に電子署名をしてもらい、これを、厚生省の認証局に照合して、この人は本当に医者かどうかを問い合わせ

せる。

あるいは学割で購入するのに、現在、学校で学割を発行しているが、申し込みの時に、その学生の電子署名をつけ、大学の認証局で確かにうちの学生であることを認証して返すといった資格証明が出てくる可能性も高い。

(2) 高まる本人確認の重要性

B to Cにおける本人確認の例を図 1-27 に示す。例えば、一般のネット事業者であると、ISPのメールアドレスを持っていることで、確かにいる人であろうということで本人確認をしたり、あるいはトヨタ社の「Gazoo」やリクルート社の「じゃまーる」のように、ID / PWであるが、それをわざわざ郵送して住所確認をして本人確認をする場合もある。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-27 高まる本人確認の重要性

また、Yahoo! オークションや eBay は、クレジットカードや銀行の口座を持っていることで本人確認を行っている。

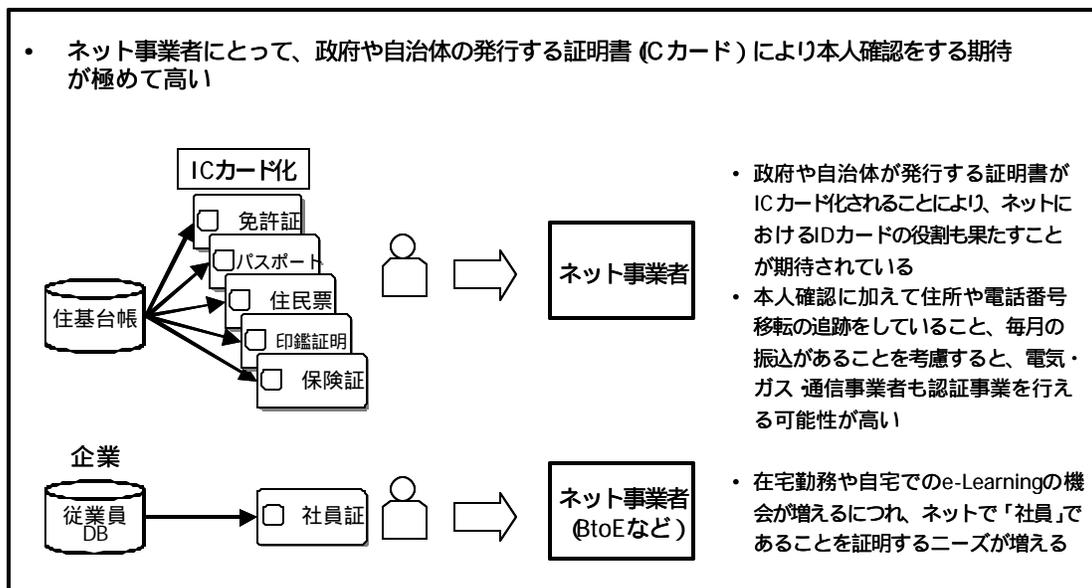
また、ネット事業者自体で、金融機関の各種証明書のように、実際に送ってもらって本人確認をするサービスが出てくる。NTTコミュニケーションズの「認証・決済

サービス」はこれである。これで本人確認をして、それをベースとした本人認証を他のネット事業者に提供するサービスも出てきている。

(3) 政府や自治体が発行する証明書の利用

図 1-28 に示す。政府や自治体が発行する証明書についてはネット事業者からの期待が非常に高い。基本は住基台帳になるが、保険証、パスポートなどがICカード化され、これを使ってネット事業者は本人確認をしたいと期待している。

また、この人が本当にこの企業の社員かどうかを知りたいといったニーズがある。例えば、ある会社の社員だったらチケットは何割引にするとか、家族も対象になるので、どの会社の社員であるという認証は期待されている。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-28 政府や自治体が発行する証明書の利用

また、金融機関は、本人確認の役割が減ることはなく、与信の機能が非常に重要である。金融機関だけではなく、帝国データバンク社のように、会社情報を蓄積しているところの役割が非常に重要になってくる。

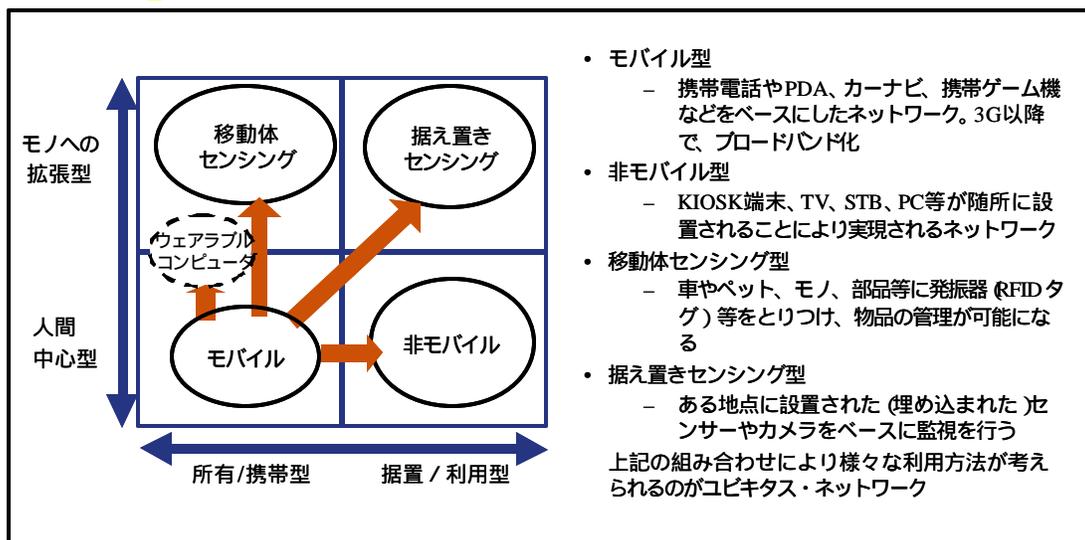
1.3.3 ユビキタス・ネットワークと認証

(1) ユビキタス

ユビキタス (Ubiquitous) とは至る所にある、遍在するという意味で、神様は至る

ところにいる、遍在することから来ている。

ネットワークが使われる範囲が物への拡張、あるいはその場所への拡張とが進んでいくと考えられる。この2つの軸によって分類したユビキタス・ネットワークのタイプを図 1-29 に示す。



出典：情報化月間特別シンポジウム「電子署名 認証でどう変わる電子商取引」(ECOM)
<http://WWW.ECOM.or.jp/>

図 1-29 ユビキタス・ネットワークのタイプ

(2) アグリゲーション

IDアカウンターアグリゲーションは、各種金融機関、特に銀行、証券及びクレジットなどで、ID/PWを代理人として預かり、それで自分自身のアグリゲーションサービス事業者のID/PWに置き換えて、金融機関に一括してログインして、ログインしたときに表示させる自分の口座情報を、HTMLを解析して、読んで、情報をとってきて、一画面に表示する(スクレーピング)サービスである。

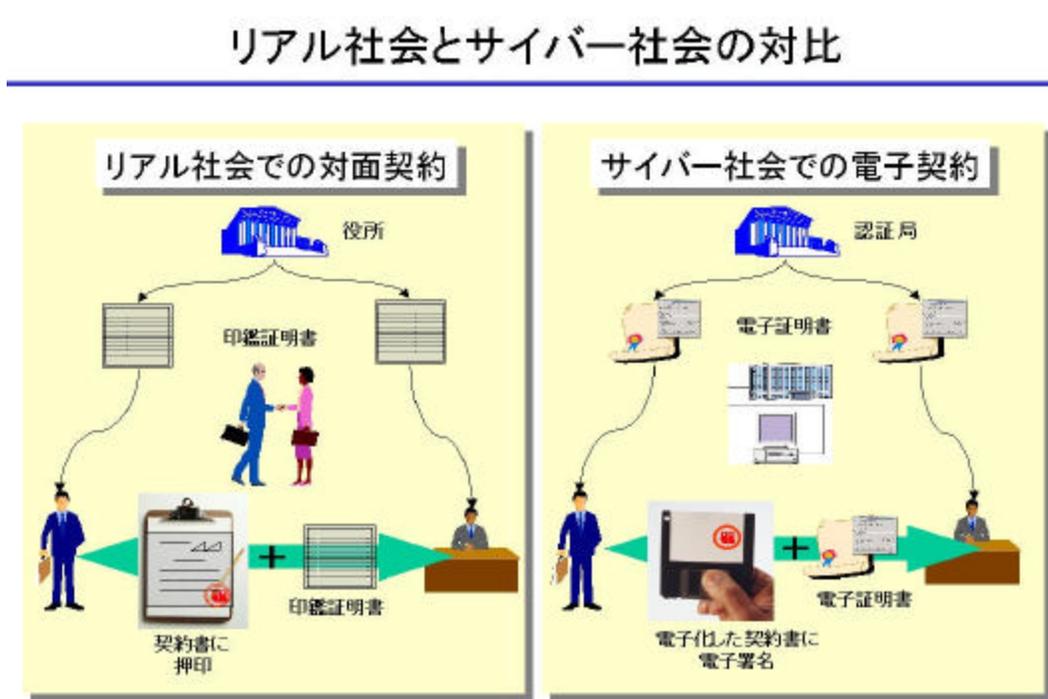
ほとんどの金融機関が提供しているが、当初はID/PWは、その顧客個人に渡したものであって、これを勝手に預かるとはけしからんということで、アグリゲーションを阻止する動きがあった。結局ユーザから見ると非常に便利なサービスであり、このときに初めてID/PWは誰のものかを議論した。結局これをやらないと競争力が低下する可能性があり、また、ユーザに非常に評判がいいので、多くの金融機関がこのサービスを開始している。

PKIに基づいて電子認証についても、セキュリティを高くすれば利便性はやはり

下がるといったトレードオフの関係にあり、かつ、多様なセキュリティ、認証が出てくると、使い勝手の面でも問題があり、電子認証においてもアグリゲーションサービスを検討する余地がある。

1.3.4 リアル社会とサイバー社会の接点

リアル社会における対面契約とサイバー社会における電子契約をハンコと電子署名との関係として対比したのが図 1-30 である。いわゆるハンコが電子署名に対応し、印鑑証明書が電子証明書に対応するという対比関係を示している。



出典 :Japan PKI Partnership 設立準備会資料
<http://WWW.ECOM.or.jp/JPKIP/>

図 1-30 リアル社会とサイバー社会との対比

人と社会システムの視点からみると、電子署名の役割は、リアル社会で個人が所有するハンコに対応しており、本人性の確認と改ざんの検出が電子署名の基本機能（図 1-31）になっている。

発行する電子情報にデジタル署名（=電子署名）を付加すること、つまりハンコを押す

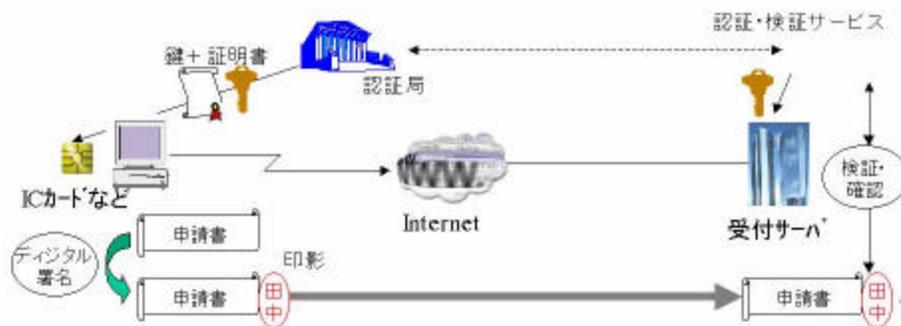
ことで情報を発行した個人を確認することができる。しかし、ハンコは本人が所有し、本人の意思で押印しているといった社会的コンセンサスがあるのに対し、電子署名は、その行為は特別な操作でないため記憶にも残りにくい面もあり、まだ社会的コンセンサスが確立されていない。ここがリアル社会との違いのポイントであり、リアル社会でサイバー社会の電子証明書がどのように受け入れられるが課題である。

また、電子署名は電子媒体である場合に意味があり、紙に印刷すると署名の意味がなくなるため、電子媒体のままのライフサイクル(起案、契約、保存、廃棄)確立が必要である。

人と社会システムの視点(電子署名の役割)

- 電子署名=本人性の確認と改ざんの検出
- 個人認証のための基本技術
→金融機関や電子政府で採用されているPKI(公開鍵基盤)
- (個人の印鑑)によるデジタル署名(押印)
- 個人と印鑑の結びつきを証明するものが証明書(印鑑証明)
- 発行する情報(例えば申請書)にデジタル署名を付加(押印)することで、その情報を発行した個人を確認(押印確認)することができる

*PKI:Public Key Infrastructure



出典 Japan PKI Partnership 設立準備会資料
<http://WWW.ECOM.or.jp/JPKIP/>

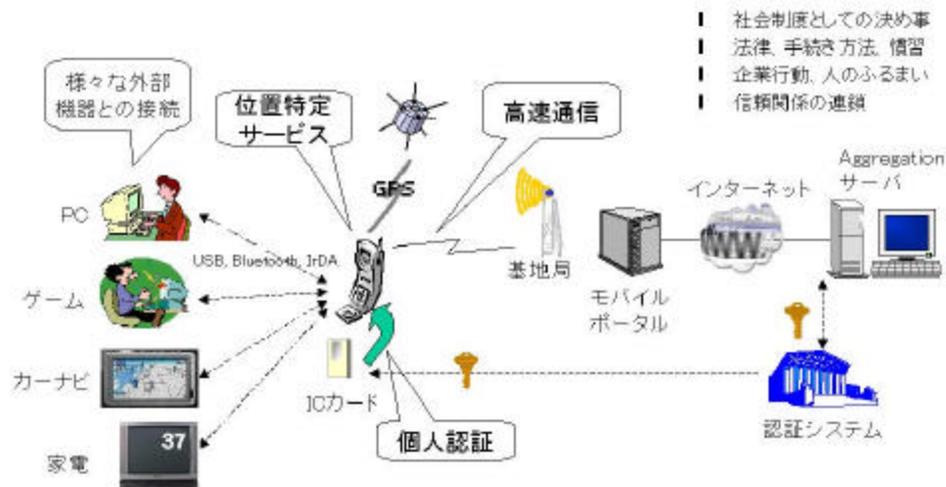
図 1-31 人と社会システムの視点

日常生活において、例えば携帯電話にICカードやICチップがつく状況で個人は認証を意識せずに使う(図 1-32)。ところが、その裏にあるPKIを使った認証、信頼の連鎖の確認は、人は当然のこととして信頼をしている。社会システムとしてそれが確立されていなければ、安心して使うことはできない。社会制度として、人があるいはコミュニティ

がそれを受け入れ、一定のコンセンサスを持って行動するようになることが重要である。

受容とコンセンサス(サイバー社会の認知)

携帯電話は、いつでもどこでも使え、個人を認証可能なデバイスとして活用されていく



出典 :Japan PKI Partnership 設立準備会資料
<http://WWW.ECOM.or.jp/JPKIP/>

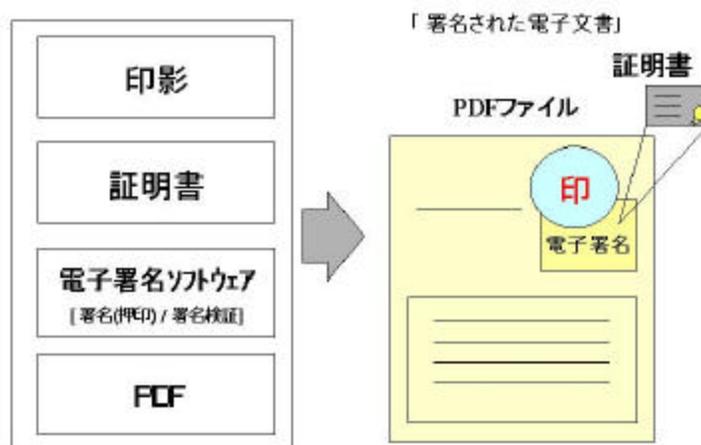
図 1-32 受容とコンセンサス

紙文書に近づいた電子文書として、PDFで実現した例を示す(図 1-33)。

これはハンコのイメージを用いて、デジタル署名で信頼性が担保される例である。実際に紙の文書をつくるときと同様に、電子的にハンコを文書上に押す。ハンコはICカードの中に入っていて、ハンコのイメージを文書上に貼り付ける操作と同時にデジタル署名が添付され信頼性が得られる。

電子署名の検証は、証明書を発行した認証局に確認に行く。その結果は、実際に目で見えるように表示して、これは真正なハンコであるということ、デジタル署名であるということ、を分かりやすく示す。人とのインターフェースをつくることが普及のためには重要なポイントとなる。

事例：紙文書に近づいた電子文書



出典 :Japan PKI Partnership 設立準備会資料
<http://WWW.ECOM.or.jp/JPKIP/>

図 1-33 紙文化に近づいた電子署名

2 電子署名・認証の利用形態と利用動向（アンケート調査）

本章では、PKI を中心とする電子署名・認証の利用形態を整理すると共に、電子署名・認証の先進ユーザを対象としたアンケート調査を実施することで、利用状況や導入検討状況を定量的に把握する。また、電子署名・認証を利用する上での阻害要因を整理する。

2.1 電子署名・認証の利用形態

ここでは、PKI の利用形態を利用用途、認証対象、認証局形態の観点から整理し、その特徴をまとめる。

2.1.1 用途

PKI は、コミュニケーションを含む各種の商取引がインターネット上で安全に行われるようにするためのインフラである。その利用用途を、電子商取引に係わるプレーヤの特性と取引形態という観点から整理すると表 2-1のようにまとめられる。

表 2-1 PKI の用途

分野	取引形態		想定される情報システムの例
B2G	1	規則に準拠した都度取引	電子入札
	2	規則に準拠した都度手続き	電子申請
B2B	3	特定企業間の固定的取引	インターネットEDI
	4	特定企業間の都度取引	電子調達
	5	不特定企業との都度取引	e マーケットプレイス
	6	不特定相手との非定型情報交換	電子メール
	7	特定ユーザとの都度取引	金融取引（ネットバンキング/トレーディング）
企業内	8	社内における情報へのアクセス	イントラネット
	9	社内における業務システム利用	社内業務システム
	10	社外からのイントラネットアクセス	リモートアクセス
B2C	11	社外の業務システムへのアクセス	ASP による業務システム
	12	特定ユーザへのサービス提供	会員制ネットサービス（e ラーニング等）
	13	不特定ユーザとの都度取引	ネットショッピング
	14	不特定ユーザへのサービス提供	ダウンロードサービス
	15	不特定ユーザ間の都度取引仲介	ネットオークション

一方、PKI の利用形態を、機能と利用シーンならびに利用する技術やツールという観点から整理すると表 2-2のようにまとめられる。PKI の機能は利用シーンや目的に合わせて組み合わせて利用されているが、その適用範囲は情報システムを構成する機器（クライアント、サーバ、通信機器）、通信経路、伝送するコンテンツをカバーしている。しかし、認証機能の適用範囲はクライアントを利用するユーザの本人性までは保証しておらず、安全性を高めるには IC カードやバイオメトリクス認証などの組み合わせが必要となる。

表 2-2 PKIの機能と利用

機能	利用シーン	ツール例	技術				
			S S L / T S L	S / M I M E	ジ エ ス ト メ ッ セ ー ジ ダ イ	V P N	S S O
暗号	ネゴシエーション時に利用 電子封筒の役割	VPN 機器 ソフトウェア					
署名	改ざん防止のための署名 印鑑の役割（意思表示）	メールクライアント Acrobat					
認証	サーバ・クライアント認証 機器認証	Web サーバ ブラウザ					

2.1.2 認証局形態

PKIにおける認証局（CA）の機能は、登録（RA）と発行（IA）の2つに大別される。この機能をどのように運用するかによって、認証局の形態は表 2-3および図 2-1に示す完全内部運営方式、発行局外部委託運営方式、完全外部委託運営方式の3つに分類される。一般に、大量に証明書を発行する場合には内部に認証局を持つケースが多く、少量の証明書を発行する場合には認証局を外部化するケースが多いと言われている。

表 2-3 認証局の運営形態別の特徴

	利点	欠点
完全内部 運営方式	証明書発行業務管理を自前で行える 登録時の検査を自前で行える 証明書発行に伴うコストを抑えられる	全て自前で用意するため初期投資が高くなる 運営要員を自前で用意する必要がある 運営に携わる要員の教育が必要になる
発行局外 部委託運 営方式	登録時の検査を自前で行える 発行機関構築の初期投資を抑えられる 電子証明書の発行という定型作業を外 部化することでコストを抑えられる	発行機関を外部化するため運用費用が相対 的に高くなる 登録業務要員を自前で用意する必要がある 電子証明書の発行には（通常）発行枚数に 比例したコストが発生する
完全外部 委託運営 方式	認証局業務全体を外部化するため初 期投資を抑えられる	認証局業務全体を外部化するため運用費用 が相対的に高くなる 電子証明書の発行には（通常）発行枚数に 比例したコストが発生する

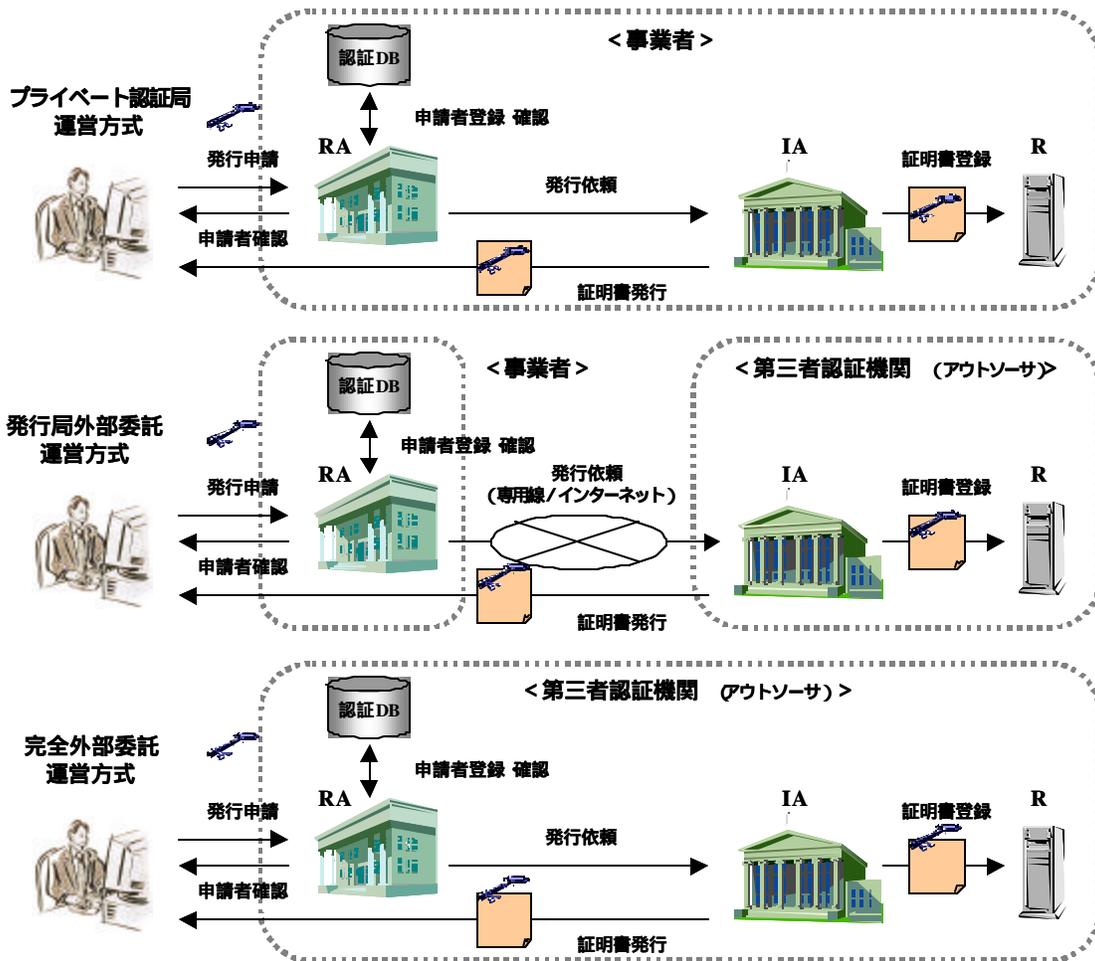


図 2-1 認証局の運営形態別のスキーム

2.2 電子署名・認証の利用動向

ここでは、電子署名・認証の利用動向を定量的に把握するため、先進ユーザを対象に実施したアンケート調査の概要をまとめる。

2.2.1 アンケート調査実施概要

アンケート調査の実施要領を表 2-4に示す。アンケート調査は、2002 年 2 月 5 日に電子メールで ECOM 会員企業のうち、308 社に質問票を送信し、2002 年 2 月 22 日に回収することで実施した。回収調査票は 60 票であり、それを集計対象票とした。

表 2-4 アンケート調査の実施要領

項目	実施要領
調査対象	・ECOM 会員企業
調査方法	・調査票は、Microsoft Word ファイルで作成 ・調査票発送は、上記ファイルを電子メール送信により実施 ・調査票回収は、電子メール受信、郵送回収、FAX 回収など複数の方法で対応
回収数	・有効回答数 60 (= 回収数)
調査時期	・2002 年 2 月 5 日 ~ 2002 年 2 月 22 日

2.2.2 アンケート調査票回収企業の概要

調査対象企業の属性を図 2-2 ~ 図 2-5に示す。業種別では、製造業が 33%であり、そのうち電気機械器具製造業が 15%と最も高い比率を占めている。一方、サービス業は 67%となっており、そのうち情報サービス・調査・印刷・出版業が 27%と最も高い比率を占めている。常雇用従業員規模、資本金、売上高、情報化投資額（2001 年）については、それぞれ 5000 人以上が 51%、50 億円以上が 64%、1000 億円以上が 66%、10 億円以上が 56%を占めており、大企業の比率の高いサンプルになっていることが分かる。

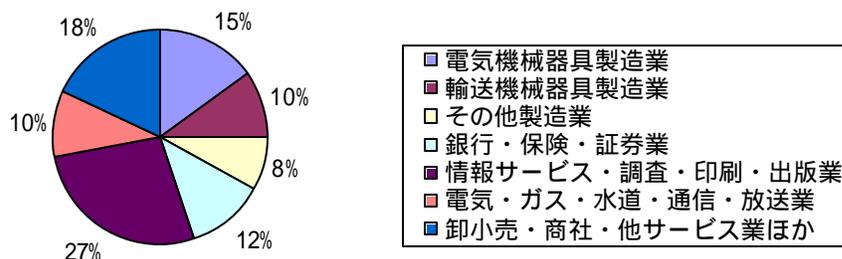


図 2-2 業種 (n = 60)

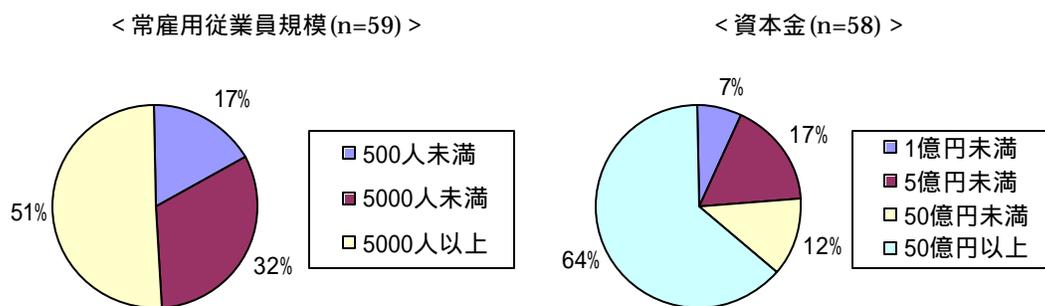


図 2-3 常雇用従業員規模と資本金

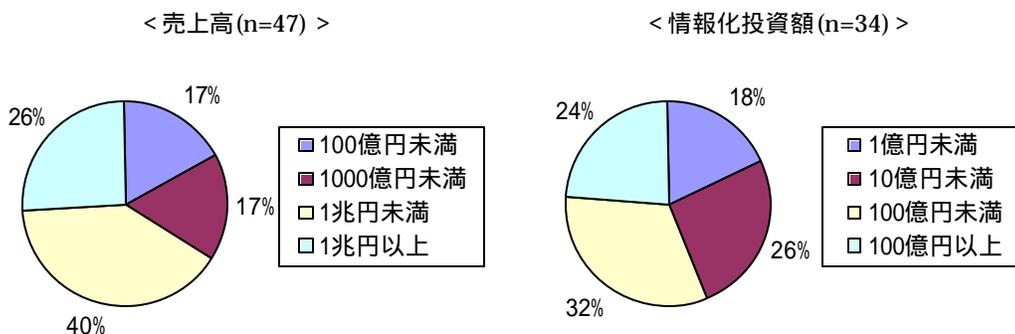


図 2-4 2001 年の売上高と情報化投資額

情報化投資額に占めるセキュリティ対策費については 3%未満が 49%と約半数を占めており、その絶対額は今後とも増加傾向にあるとの見通しを持つユーザが 65%を占めている。

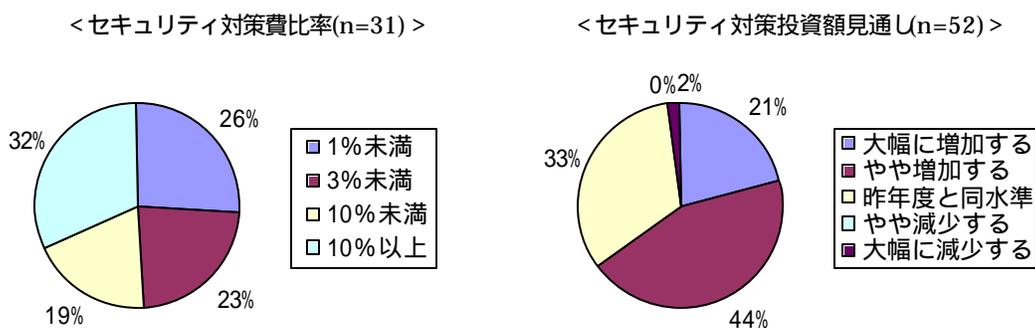


図 2-5 情報化投資額に占めるセキュリティ対策費比率と今後の投資額見通し

2.2.3 アンケート調査結果

ここでは、ECOM 会員企業向けに実施したアンケート調査より、PKI の利用動向に関する分析結果を中心に取り上げまとめるものとする。

2.2.3.1 商取引におけるインターネットの普及状況

PKI の利用用途と想定される各種商取引において、インターネットの普及状況を調査したところ、図 2-6に示す結果を得た。

既に導入済みの情報システムについては、電子メールやイントラネットなど企業内業務の効率化を目的としたシステムの導入比率が高く、B2G 分野の商取引における情報システムの導入比率が低いことが分かる。

また、今後導入が期待される情報システム（あるいは商取引）としては、電子申請や電子入札といった B2G 分野のシステムと、B2B 分野におけるインターネット EDI や電子調達、企業内情報システムのリモートアクセスが挙げられる。

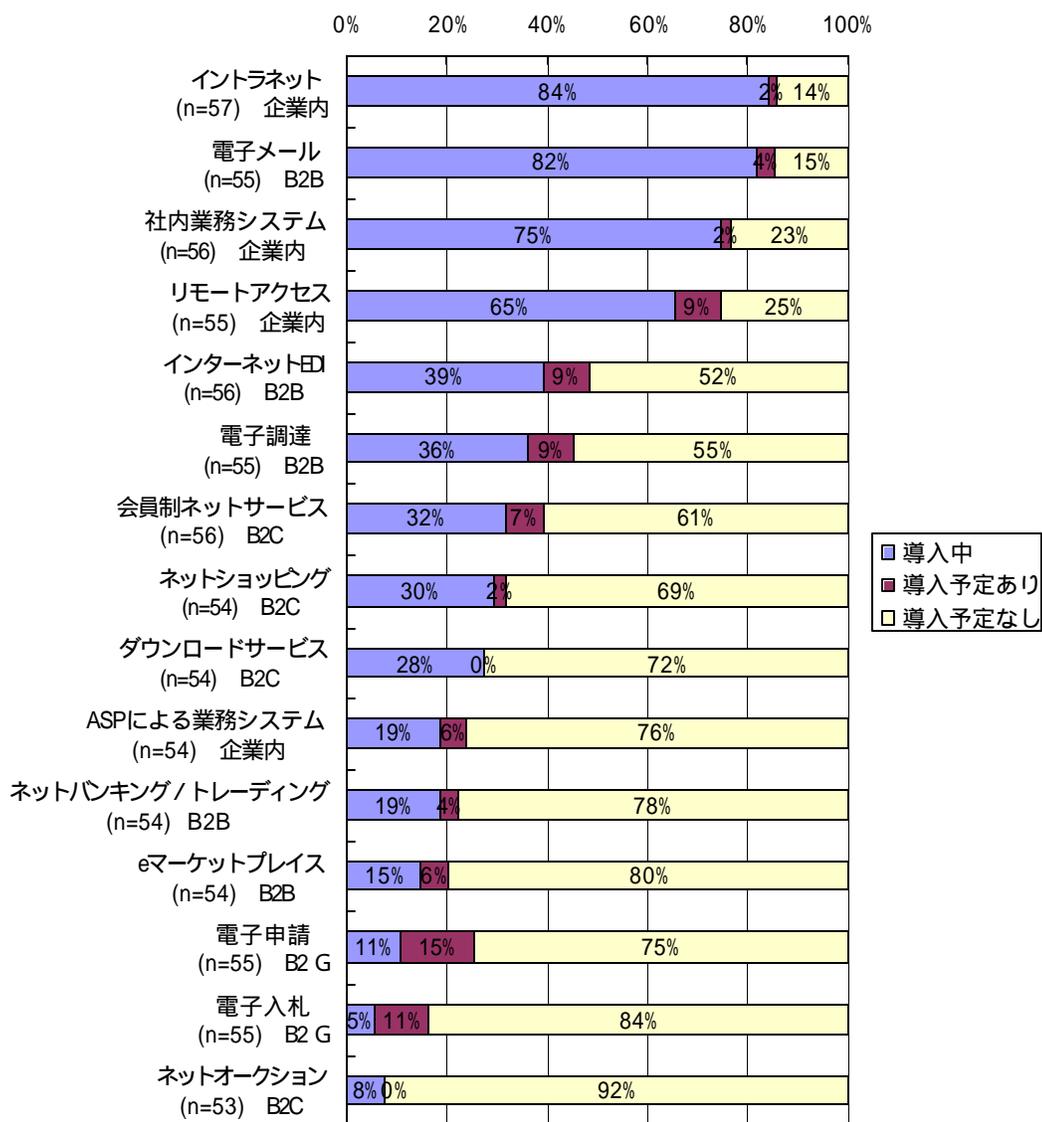


図 2-6 商取引におけるインターネットの普及状況

2.2.3.2 情報システムの導入とセキュリティ対策

(1) インターネット導入に伴う被害の可能性と大きさに関する評価

インターネットの導入に伴う被害の可能性と大きさについて、情報システムのセキュリティが破られる可能性（危険性）と、セキュリティが破られた場合の被害の大きさ（ダメージ）をどのように評価したかについて尋ねたところ、図 2-7の結果を得た。

可能性の大小に係わらず、被害が大きいと評価されているシステムは、第 1 位「eマーケットプレイス」82%、第 2 位「電子入札」80%、第 3 位「リモートアクセス」となっており、続いて「ネットショッピング」75%、「ネットバンキング/トレーディング」70%、「インターネット EDI」67%、「ダウンロードサービス」60%、「電子調達」58%と続いている。

このうち、導入率が比較的高いのはリモートアクセス、インターネット EDI、電子調達であり、その他のシステムの導入率は 30%以下と低いものとなっている。

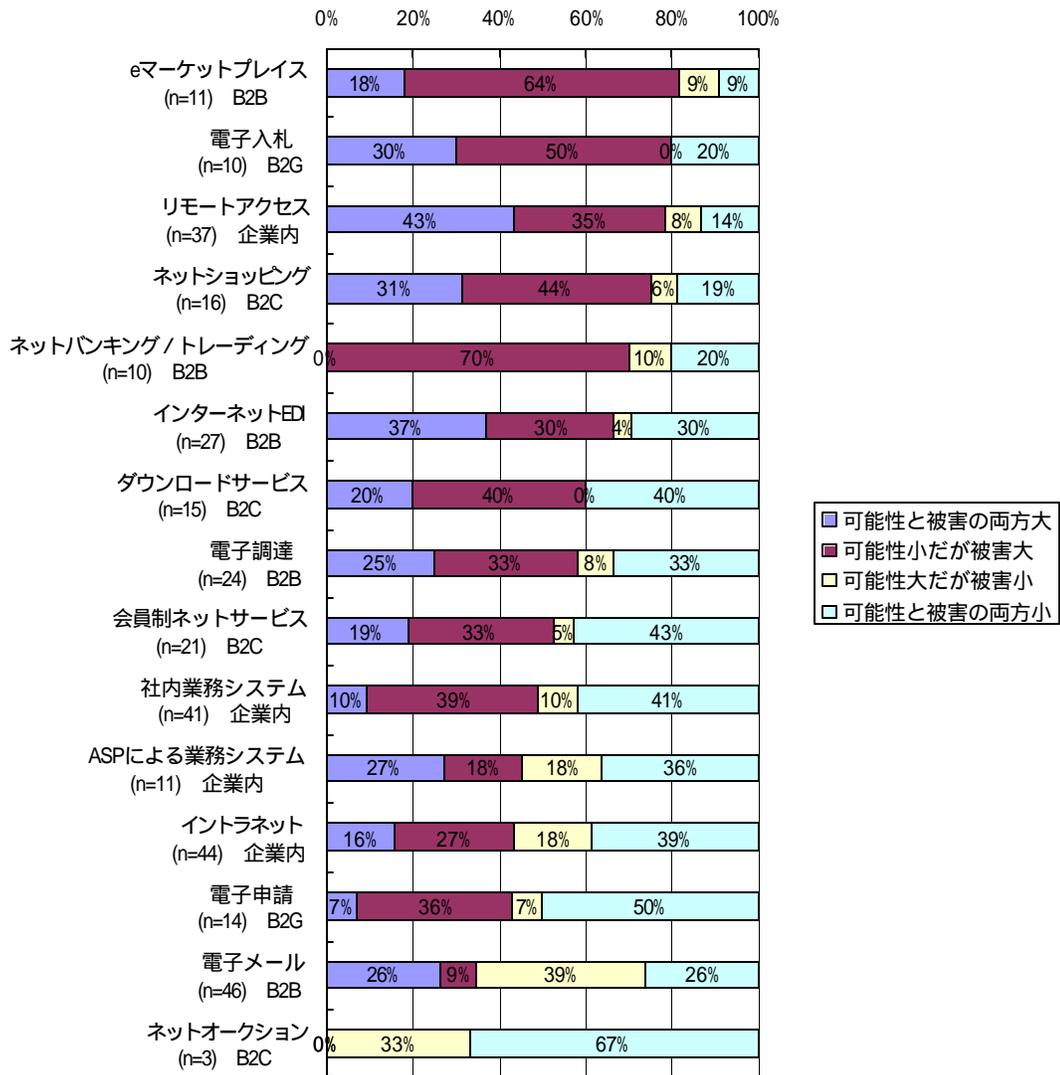


図 2-7 インターネット導入に伴う被害の可能性と大きさ

(2) インターネットを導入する業務プロセスのリスク内容

インターネットの導入リスクを商取引毎に業務プロセスレベルで分析したところ、図 2-8に示す結果を得た。最もリスクの高い業務プロセスについては、e マーケットプレイスやネットバンキング/トレーディング/インターネット EDI/ネットショッピングなど決済を含む情報システムでは、直接大きな被害を被る可能性が高い「決済」を指摘する比率が高いのが特徴である。その他では、「相手の確認」および「契約・受発注・受理」にリスクの高さを指摘する比率が高い。

また、図 2-8の各商取引について最もリスクが高いと評価された業務プロセスにおける具体的なリスクの内容を調査したところ、表 2-5に示す結果を得た。なお、表中の記号の定義は、「指摘率 70%以上」、「指摘率 50~70%」、「指摘率 30~50%」、記号無し「指摘率 30%未満」となっている。

これを見ると、B2B 分野では、データ送受信の否認、データ内容の否認、データの改ざん、データの盗聴など、ネットワーク上を流れるデータに関するリスクを指摘する比率が高いのに対して、企業内分野では、本人の権限および本人性というシステムの利用者に関わるリスクを指摘する比率が高い。一方、B2C 分野では、データおよび利用者に関わるリスクの双方を指摘する比率が高い傾向がある。また、B2G 分野では企業の実在性に関するリスクを指摘する比率が高いのが特徴といえる。

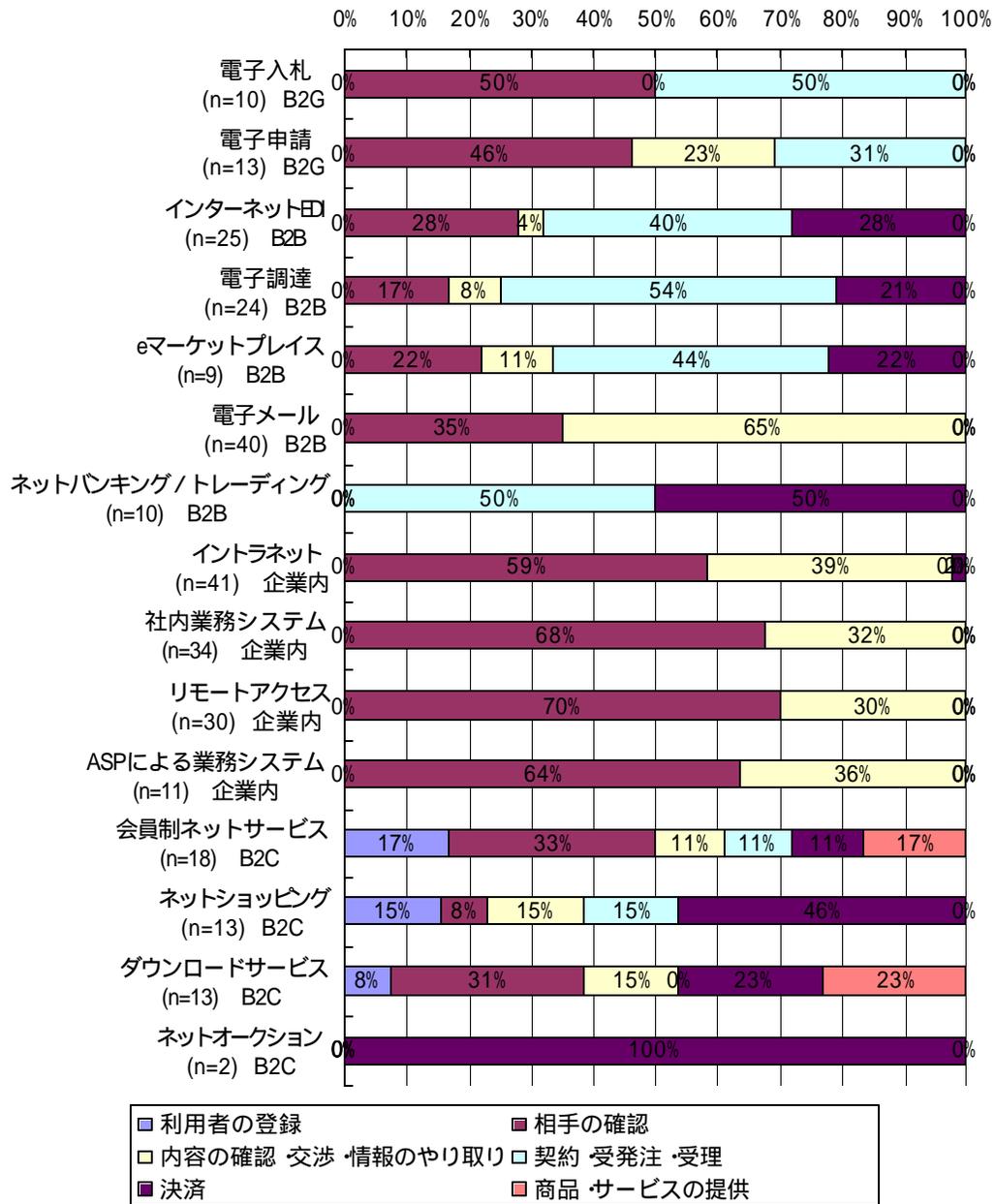


図 2-8 インターネット導入に際して最もリスクの高い業務プロセス

表 2-5 具体的なリスクの内容

分野	取引形態	最もリスクの高い 業務プロセス	具体的なリスクの内容							
			データ送受信の否認	データ内容の否認	データの改ざん	データの盗聴	本人の権限	本人性	個人の実在性	企業の与信
B2G	電子入札 電子申請	相手の確認 相手の確認								
B2B	インターネットEDI 電子調達 e マーケットプレイス 電子メール ネットバンキング等	契約・受発注・受理 契約・受発注・受理 契約・受発注・受理 内容の確認 交渉等 契約・受発注・受理								
企業内 B2C	イントラネット 社内業務システム リモートアクセス ASP 業務システム 会員制ネットサービス ネットショッピング ダウンロードサービス ネットオークション	相手の確認 相手の確認 相手の確認 相手の確認 相手の確認 決済 相手の確認 決済								

(3) インターネット導入時の業務プロセスにおけるセキュリティ対策方針

各商取引においてインターネットを導入する場合、個別の業務プロセスにおけるセキュリティ対策方針を調査した。その結果を、業務プロセス毎にまとめる。

利用者の登録

「利用者の登録」のプロセスを含む以下の情報システムのうち、会員制ネットサービス、ネットショッピング、ダウンロードサービスについては、「全面的にインターネットを採用し、セキュリティ技術で安全性を確保する」という企業が50%を超えるか、それに近い比率を占めていることが分かる。

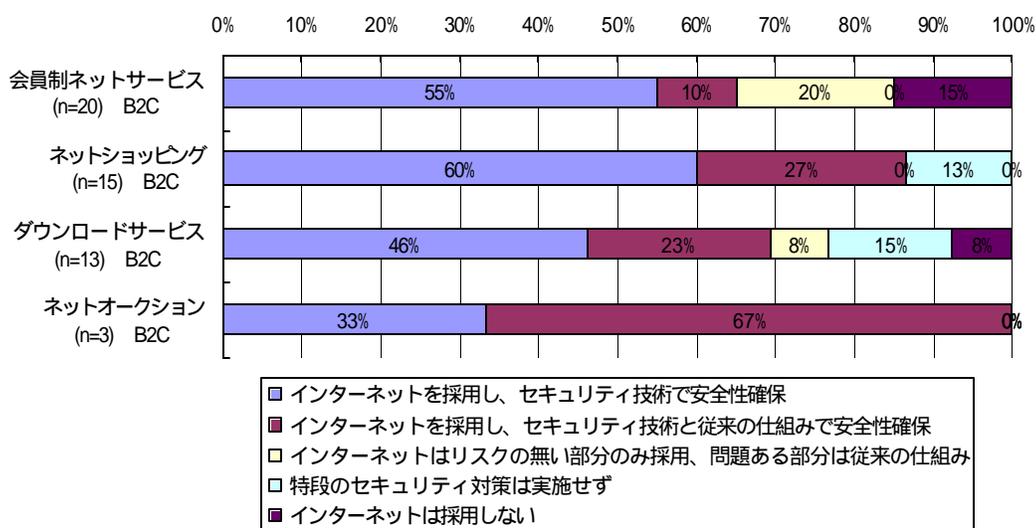


図 2-9 利用者の登録におけるセキュリティ対策方針

相手の確認

「相手の確認」のプロセスを含む、以下の15システムでは、「全面的にインターネットを採用し、セキュリティ技術で安全性を確保する」あるいは「インターネットを採用するが、セキュリティ技術と共に従来の仕組み（専用線の採用、取引先の限定など）も一部取り入れて、安全性を確保する」という企業の比率が大部分を占めている。システム別では、電子メール、eマーケットプレイス、ダウンロードサービスにおいて「特段のセキュリティ対策は実施しない」とする比率が高く、イントラネットと社内業務システムにおいて「インターネットは採用しない」とする比率が高いのが特徴である。

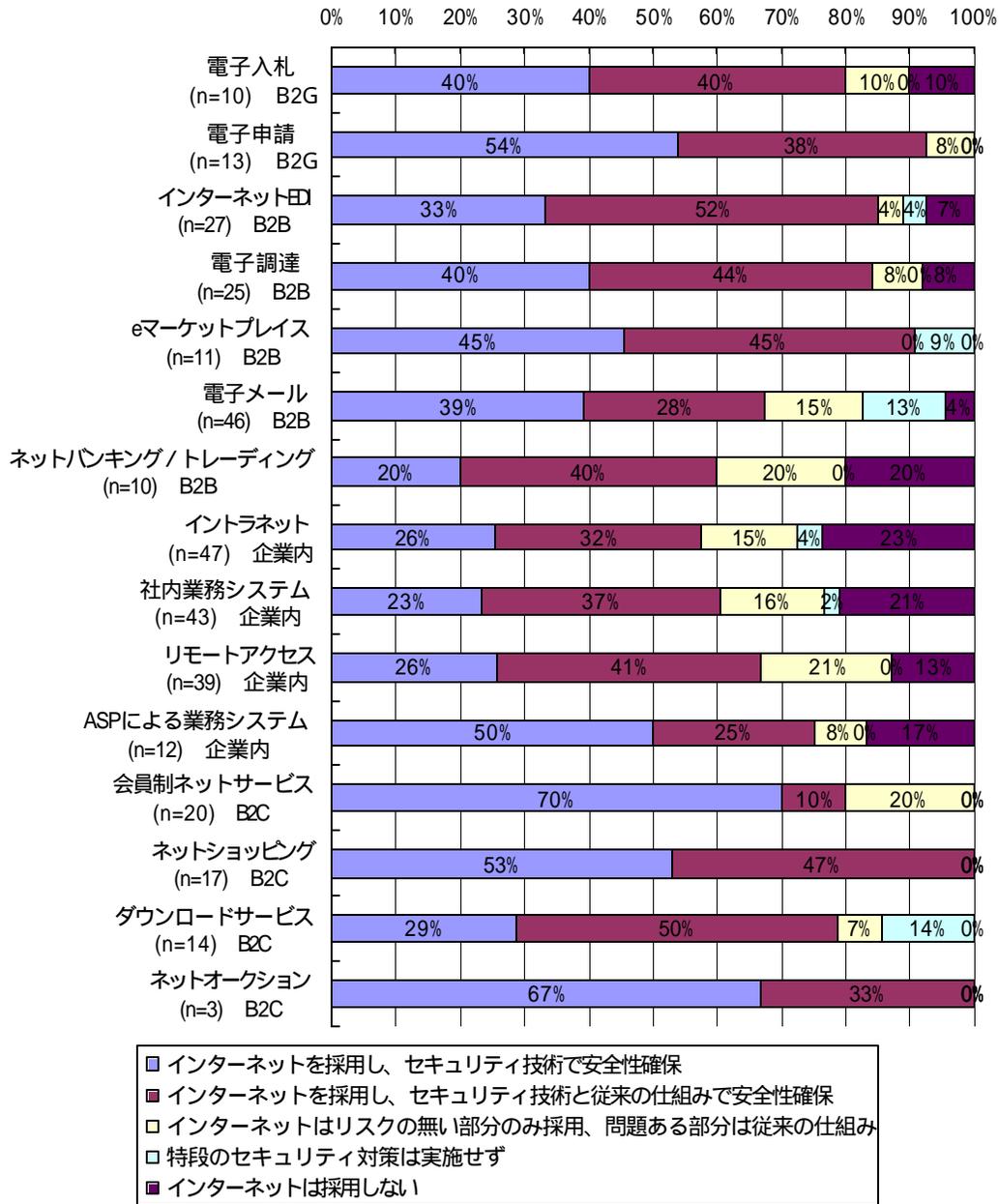


図 2-10 相手の確認におけるセキュリティ対策方針

内容の確認・交渉・情報のやり取り

「内容の確認・交渉・情報のやり取り」のプロセスを含む、以下の15システムでは、前項の「相手の確認」の場合とほぼ同様の傾向が見られるが、「インターネットは採用しない」とする企業の比率が高いのが特徴である。

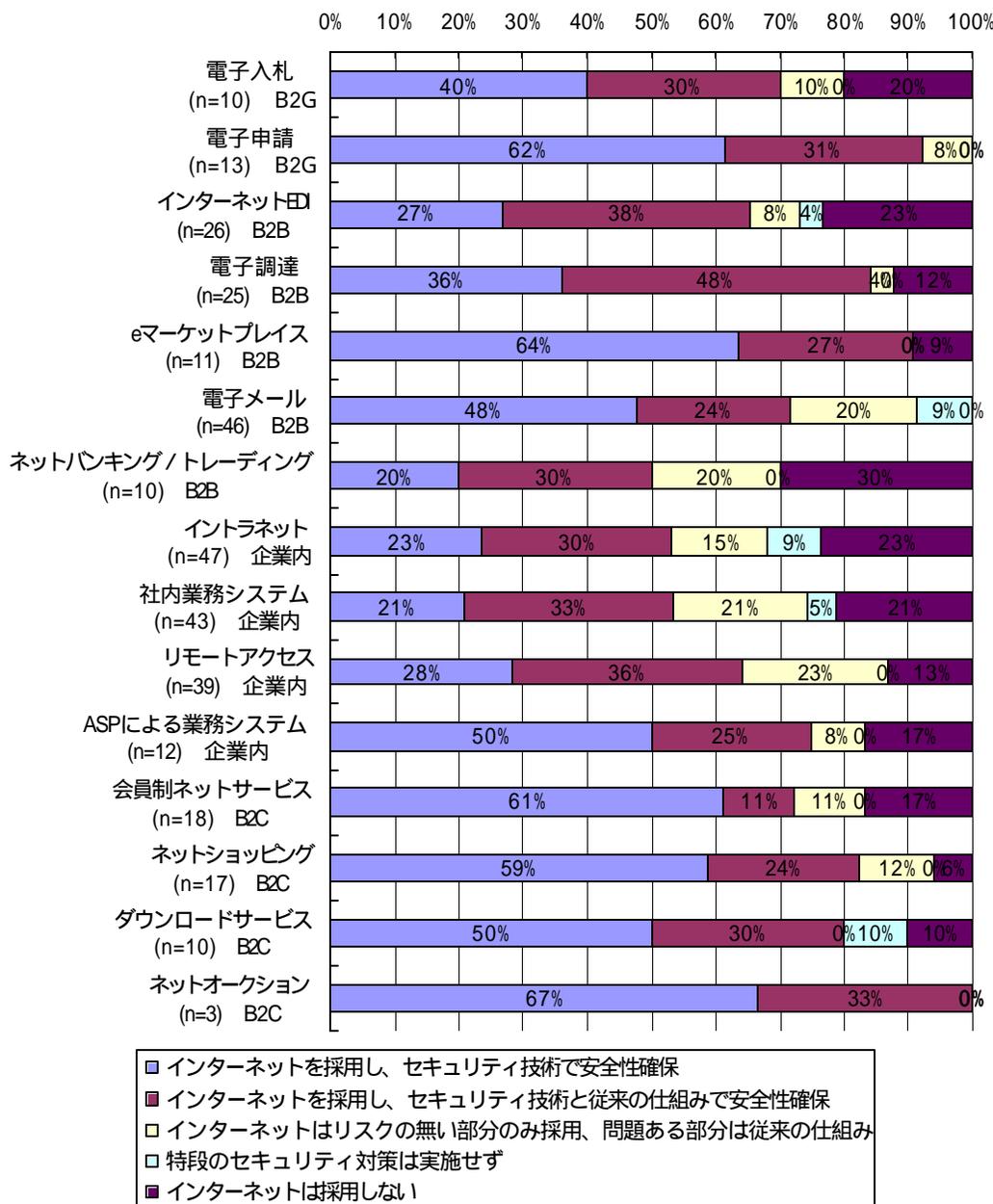


図 2-11 内容の確認・交渉・情報のやり取りにおけるセキュリティ対策方針

契約・受発注・受理

「契約・受発注・受理」のプロセスを含む、以下の10システムでも、前項の「相手の確認」および「内容の確認・交渉・情報のやり取り」の場合とほぼ同様の傾向が見られる。しかし、電子入札、ネットバンキング/トレーディング、会員制ネットサービスでは、「問題がある部分は従来の仕組みで安全性を確保し、インターネットはリスクのない部分にのみ採用する」という比率が高い点が特徴となっている。

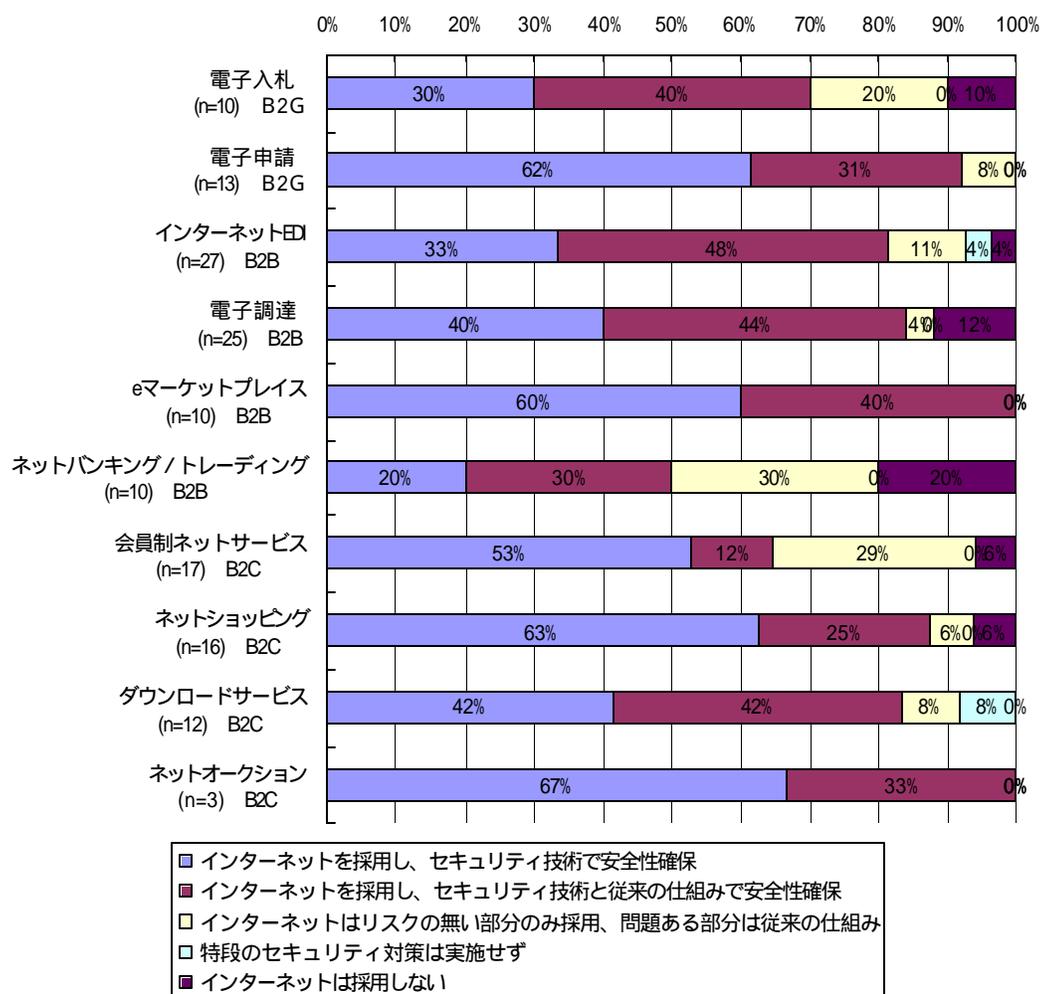


図 2-12 契約・受発注・受理におけるセキュリティ対策方針

決済

「決済」のプロセスを含む、以下の 8 システムでも、「全面的にインターネットを採用し、セキュリティ技術で安全性を確保する」あるいは「インターネットを採用するが、セキュリティ技術と共に従来の仕組みも一部取り入れて安全性を確保する」を合わせた比率が 50%に近いが、それ以上の値となっており、インターネットの採用に積極的であることが分かる。しかし、他の項目に比べて、「インターネットは採用しない」とする企業の比率が高く、想定されるリスクの高さが反映されたものと推察される。

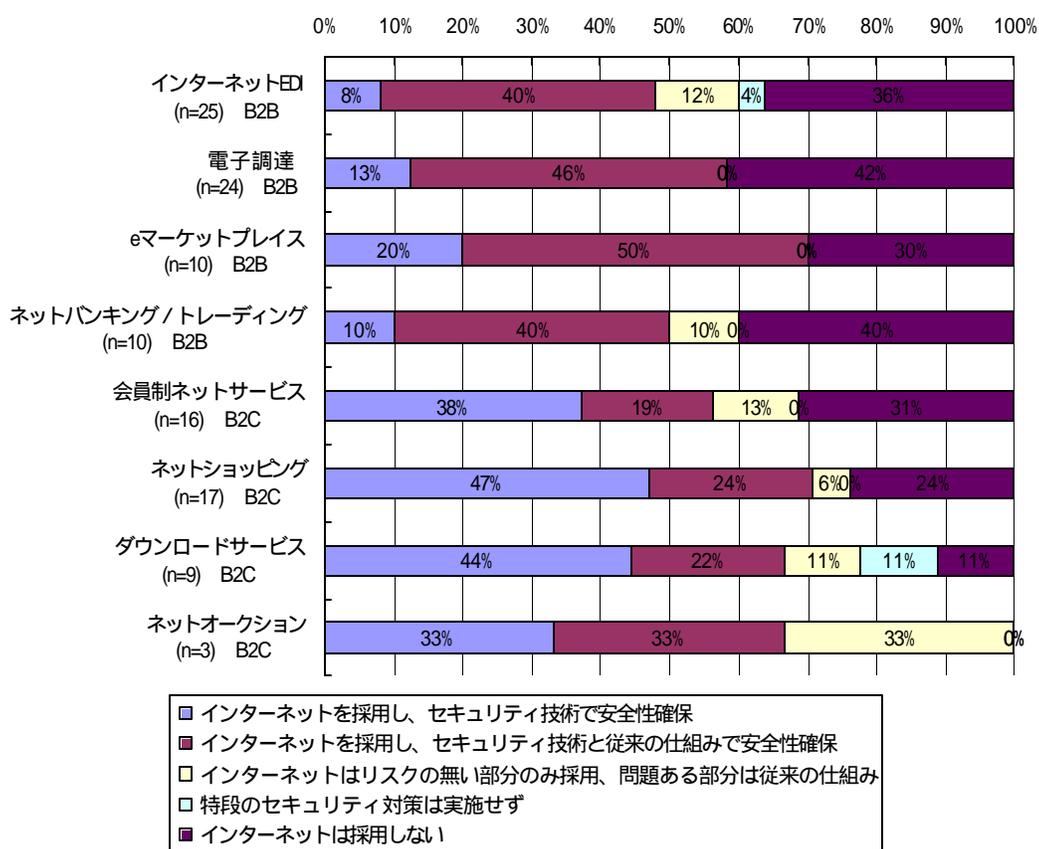


図 2-13 決済におけるセキュリティ対策方針

商品・サービスの提供

「商品・サービスの提供」のプロセスを含む、以下の2システムでも、「全面的にインターネットを採用し、セキュリティ技術で安全性を確保する」あるいは「インターネットを採用するが、セキュリティ技術と共に従来の仕組みも一部取り入れて安全性を確保する」を合わせた比率が80%に近いが、それ以上の値となっており、インターネットの採用に積極的であることが分かる。

インターネット導入のメリットを最大限に活用できる業務プロセスであるため、業務効率化、コスト削減、新規事業の提供など多くの観点から採用に積極的であるものと推察される。

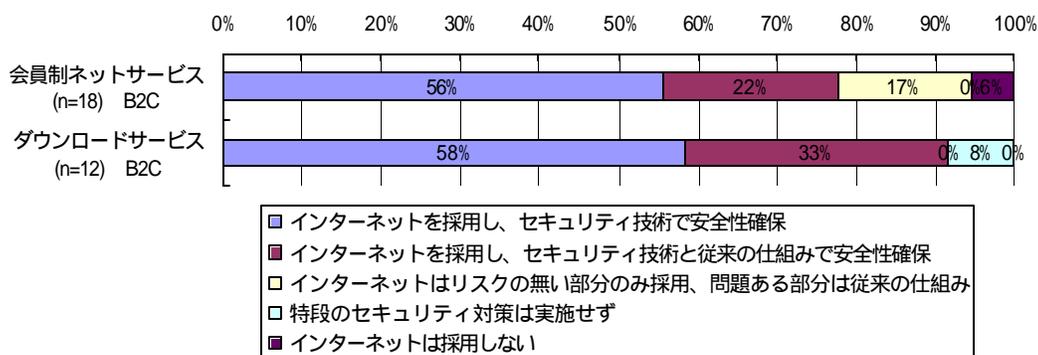


図 2-14 セキュリティ対策方針

(4) 情報システムの導入に伴って実施したセキュリティ対策

情報システムの導入に伴って実施したセキュリティ対策について調査したところ、表 2-6に示す結果を得た。ここで、図表下段の記号は、それぞれ「導入率と平均値の差（導入率 - 平均値）が 20%以上」、「導入率と平均値の差が 10%以上 20%未満」、「導入率と平均値の差が 0%以上 10%未満」を表している。

表 2-6 具体的なセキュリティ対策

	B2G		B2B					企業内					B2C				値 導 入 率 の 平 均
	B1 電 子 入 札	B2 電 子 申 請	B3 ト イ ン タ ー ネ ッ	B4 電 子 調 達	B5 プ レ イ マ イ ス ケ ッ ト	B6 電 子 メ ー ル	B7 ネ ッ ト バ ン キ	B8 ト イ ン ト ラ ネ ッ	B9 社 内 業 務 シ ス テ ム	B10 セ リ ス ト ア ク シ ョ ン	B11 S P 業 務 シ ス テ ム	B12 サ イ バ ン ク シ ョ ン	B13 サ イ バ ン ク シ ョ ン	B14 サ イ バ ン ク シ ョ ン	B15 サ イ バ ン ク シ ョ ン		
回答数	(9)	(14)	(27)	(25)	(11)	(47)	(12)	(49)	(43)	(41)	(13)	(22)	(17)	(15)	(4)		
a. ユーザの確認/アクセス制御	89%	79%	85%	80%	91%	60%	58%	84%	86%	88%	77%	82%	65%	47%	50%	75%	
b. 情報のやり取りの安全性確保	89%	71%	81%	76%	91%	57%	50%	51%	60%	66%	46%	68%	82%	53%	50%	66%	
c. 決済における安全性確保	-	-	48%	32%	55%	-	33%	-	12%	-	-	23%	59%	27%	50%	38%	
d. その他	56%	71%	74%	56%	73%	70%	50%	69%	65%	80%	69%	68%	71%	60%	25%	64%	
a. ユーザの確認/アクセス制御	9	14	27	25	11	47	12	49	43	41	13	22	17	15	4		
1. ID パスワード認証	44%	43%	78%	80%	73%	60%	50%	88%	91%	88%	77%	82%	65%	40%	50%	67%	
2. ワンタイムパスワード認証	0%	0%	7%	8%	0%	6%	0%	16%	9%	46%	15%	0%	0%	0%	0%	7%	
3. バイOMETRICS認証	0%	0%	0%	0%	0%	2%	0%	2%	0%	2%	0%	5%	0%	0%	0%	1%	
4. デジタル署名 証明書	89%	57%	48%	32%	36%	23%	33%	20%	19%	17%	38%	23%	6%	13%	0%	30%	
b. 情報のやり取りの安全性確保	9	14	27	25	11	47	12	49	43	41	13	22	17	15	4		
1. デジタル署名 証明書	78%	64%	56%	44%	45%	23%	42%	22%	23%	17%	31%	41%	24%	33%	0%	36%	
2. 暗号化メール	22%	7%	15%	8%	9%	38%	0%	18%	19%	10%	23%	0%	12%	13%	0%	13%	
3. 暗号化通信	44%	57%	78%	68%	73%	19%	33%	37%	40%	46%	31%	59%	94%	47%	50%	52%	
4. VPN	11%	0%	30%	12%	0%	11%	25%	33%	28%	41%	38%	9%	6%	0%	0%	16%	
5. 回線監視	0%	7%	26%	20%	27%	17%	17%	20%	19%	27%	23%	14%	18%	7%	0%	16%	
6. 電子公証	11%	7%	7%	4%	9%	2%	0%	2%	0%	2%	0%	5%	0%	0%	0%	3%	
c. 決済における安全性確保	0	0	27	25	11	0	12	0	43	0	0	22	17	15	4		
1. SET	-	-	7%	4%	9%	-	8%	-	0%	-	-	0%	12%	7%	0%	5%	
2. SSL	-	-	48%	36%	36%	-	33%	-	12%	-	-	32%	71%	27%	50%	38%	
3. 電子マネー	-	-	0%	0%	0%	-	0%	-	0%	-	-	5%	6%	0%	0%	1%	
d. その他	9	14	27	25	11	47	12	49	43	41	13	22	17	15	4		
1. ファイヤウォール	56%	57%	78%	68%	64%	70%	50%	71%	65%	83%	77%	68%	82%	73%	25%	66%	
2. ウィルス対策	56%	43%	59%	44%	45%	81%	33%	71%	67%	73%	62%	59%	65%	53%	0%	54%	
3. その他	11%	14%	11%	8%	9%	2%	0%	6%	5%	10%	15%	5%	0%	0%	0%	6%	
a. ユーザの確認/アクセス制御																	
b. 情報のやり取りの安全性確保																	
c. 決済における安全性確保																	
d. その他																	
a. ユーザの確認/アクセス制御																	
1. ID パスワード認証																	
2. ワンタイムパスワード認証																	
3. バイOMETRICS認証																	
4. デジタル署名 証明書																	
b. 情報のやり取りの安全性確保																	
1. デジタル署名 証明書																	
2. 暗号化メール																	
3. 暗号化通信																	
4. VPN																	
5. 回線監視																	
6. 電子公証																	
c. 決済における安全性確保																	
1. SET																	
2. SSL																	
3. 電子マネー																	
d. その他																	
1. ファイヤウォール																	
2. ウィルス対策																	
3. その他																	

15 システムに共通して導入率が高いのは、ID・パスワード認証、ファイヤウォール、ウィルス対策、暗号化通信である。一方、デジタル署名・証明書の導入率は、平均で30%台と比較的高い比率となっている。

ID・パスワード認証を除いて、具体的なセキュリティ対策の実施状況を情報システム別に見ると、B2G 分野の電子入札および電子申請でデジタル署名・証明書の導入率が高く、インターネット EDI と eマーケットプレイスでは暗号化通信、電子メールではウィルス対策と暗号化メール、リモートアクセスではワンタイムパスワード認証と VPN、ASP による業務システムでは VPN、ネットショッピングでは暗号化通信と SSL の導入率が特に高いことが分かる。

上記セキュリティ対策導入の相関性を評価するためクラスタ分析を行い、図 2-15 に示す結果を得た。これを見ると、デジタル署名・証明書と暗号化メール、VPN とワンタイムパスワード認証、ウィルス対策とファイヤウォールならびに ID・パスワード認証等の相関性の高いことが分かる。また、バイオメトリクス認証と電子公証については、サンプル数が少ないため偶然近いグループになったものと考えられる。

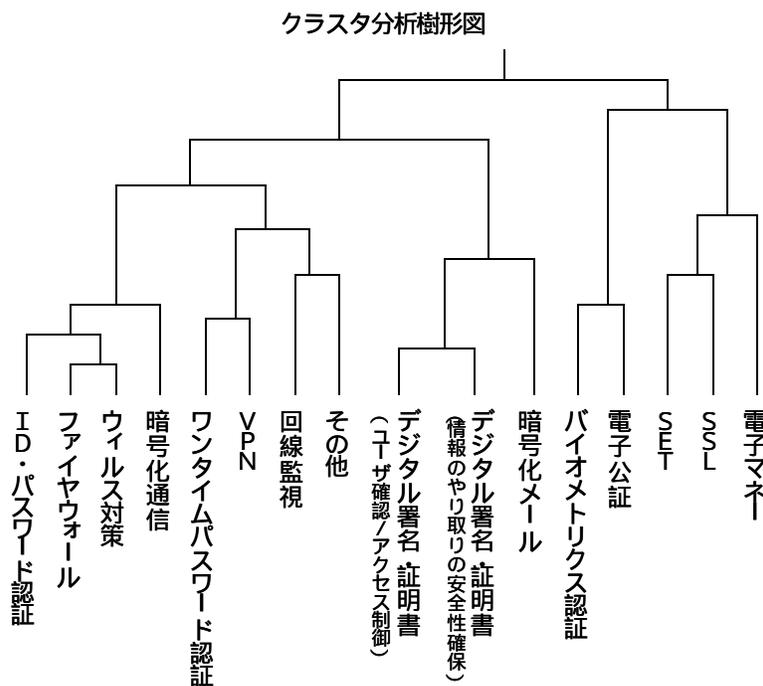


図 2-15 セキュリティ対策のクラスタ分析結果

2.2.3.3 インターネット導入とセキュリティ対策に関する分析

商取引におけるインターネット導入率と、インターネットの導入に伴うリスクの高さに関する評価を分析した結果を図 2-16に示す。図中横軸は、図 2-6に示した商取引におけるインターネットの導入状況のうち、「導入中」比率と「導入予定あり」比率の合計値であり、インターネット導入率のポテンシャル比率を表している。一方、図中縦軸は、図 2-97に示したインターネット導入に伴う被害の可能性と大きさのうち、「可能性と被害の両方が大きい」比率と「可能性は小さいが被害は大きい」比率の合計値であり、インターネット導入に伴う潜在的な被害の大きさ（被害の発生可能性は問わない）を表している。

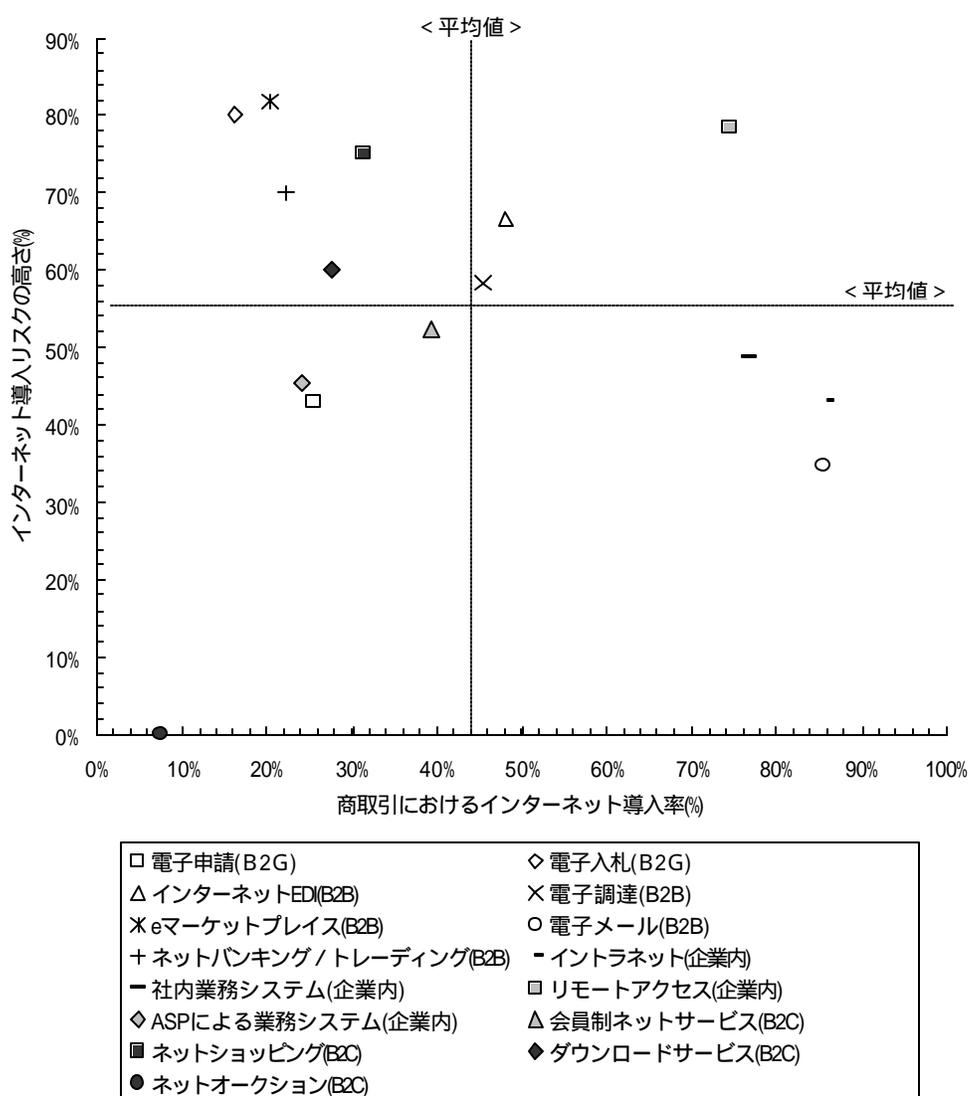


図 2-16 インターネット導入リスクとインターネット導入率に関する分析

これを見ると、インターネット導入リスクが高い（平均値以上）にも係わらず、インターネット導入率が高い（平均値以上）ものとして、以下の3つが挙げられる。

- ・インターネット EDI (B2B)
- ・電子調達 (B2B)
- ・リモートアクセス (企業内)

また、インターネット導入リスクが高く（平均値以上）、しかもインターネット導入が低い（平均値以下）ものとして以下の5つが挙げられる。

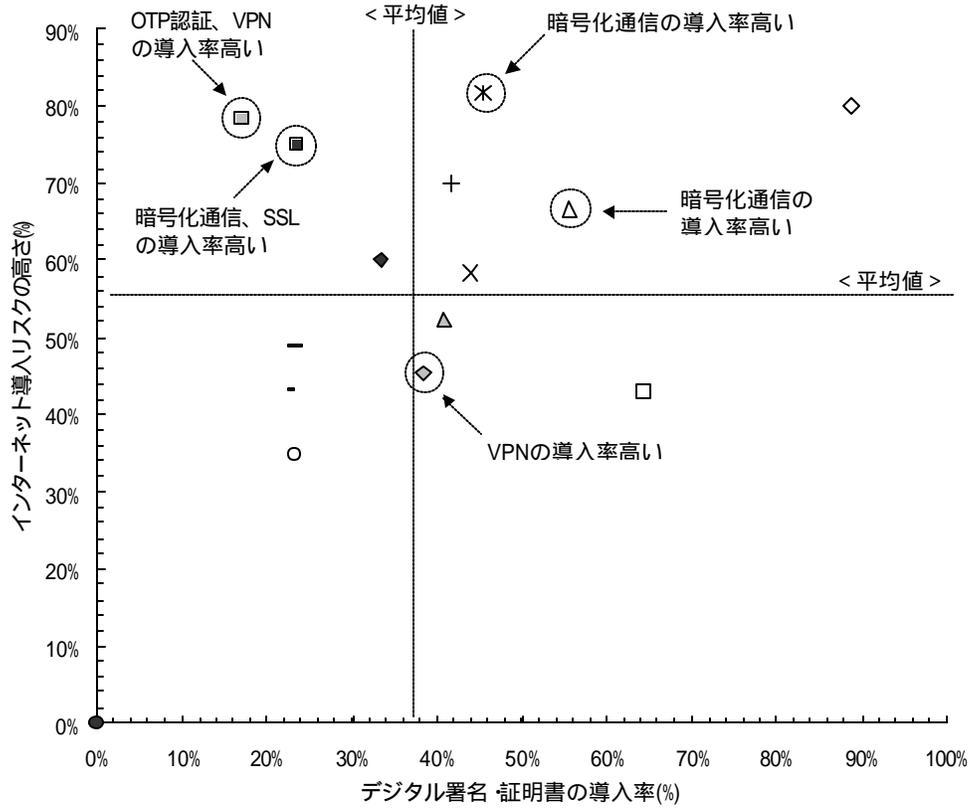
- ・電子入札 (B2G)
- ・e マーケットプレイス (B2B)
- ・ネットバンキング/トレーディング (B2B)
- ・ネットショッピング (B2C)
- ・ダウンロードサービス (B2C)

また、図 2-7 は、インターネット導入リスクとデジタル署名・証明書の導入率の関係を示したものである。図中横軸は、表 2-6 に示した具体的なセキュリティ対策のうち、デジタル署名・証明書の導入率を採用したものである。なお、デジタル署名・証明書の導入率は、ユーザの確認/アクセス制御と情報のやり取りの安全性確保という2つの目的別に調査結果が出ているが、ここでは双方のうち大きい方の比率を採用している。また、図中には、デジタル署名・証明書以外に、全体平均値と比べて特に導入率が高いと評価されたセキュリティ対策のうち、特徴的なものについてコメントを追加している。

これを見ると、図 2-16 でインターネット導入リスクが高いと評価された、8つの商取引のうち、デジタル署名・証明書の導入率が高い（平均値以上）のは以下の5つであり、インターネット導入リスクに対する具体策として、デジタル署名・証明書を導入する効果が比較的高いと評価されている商取引であると考えられる。

- ・電子入札 (B2G)
- ・インターネット EDI (B2B)
- ・電子調達 (B2B)
- ・e マーケットプレイス (B2B)
- ・ネットバンキング/トレーディング (B2B)

これに対して、リモートアクセスではワンタイムパスワード認証とVPN、ネットショッピングでは暗号化通信とSSLの導入率が高い点に特徴があり、デジタル署名・証明書の導入率は平均値よりも低くなっている。これらの商取引では、インターネット導入リスクに対応するため、デジタル署名・証明書以外の方法が主に採用されていることが分かる。



□ 電子申請(B2G)	◇ 電子入札(B2G)
△ インターネットEDI(B2B)	× 電子調達(B2B)
* eマーケットプレイス(B2B)	○ 電子メール(B2B)
+ ネットバンキング/トレーディング(B2B)	- イン트라ネット(企業内)
- 社内業務システム(企業内)	□ リモートアクセス(企業内)
◇ ASPによる業務システム(企業内)	△ 会員制ネットサービス(B2C)
■ ネットショッピング(B2C)	◆ ダウンロードサービス(B2C)
● ネットオークション(B2C)	

図 2-17 インターネット導入リスクとデジタル署名・証明書の導入率に関する分析

2.2.3.4 PKIの利用実態

ここでは、PKI に焦点を絞り、その利用実態について分析した。

(1) PKI の利用状況

PKI を現在利用している企業は、全体の約半数に当たる 48%となっている。PKI の導入可能性を最大限考慮すると、PKI を将来的に導入する可能性のある企業の比率は約 80%となる。

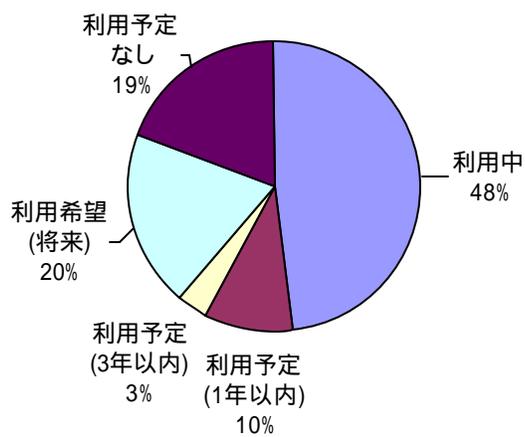


図 2-18 PKI の利用状況 (n=56)

(2) PKI の利用理由

PKI を利用している理由については、「セキュリティ対策上の要件を満足している」84%と「今後の世の中のインフラ技術になると判断した」69%を指摘する比率が特に高く、セキュリティ技術としての機能／性能および将来の普及可能性を評価した結果が導入に結びついているものと考えられる。

また、「現状採り得る方策として最良のものである」45%、「信頼性／安全性等の自社アピールになる」43%となっており、競合技術が無いことを理由に、またユーザに対するアピールを目的として、PKI を導入している比率が高いことが特筆される。

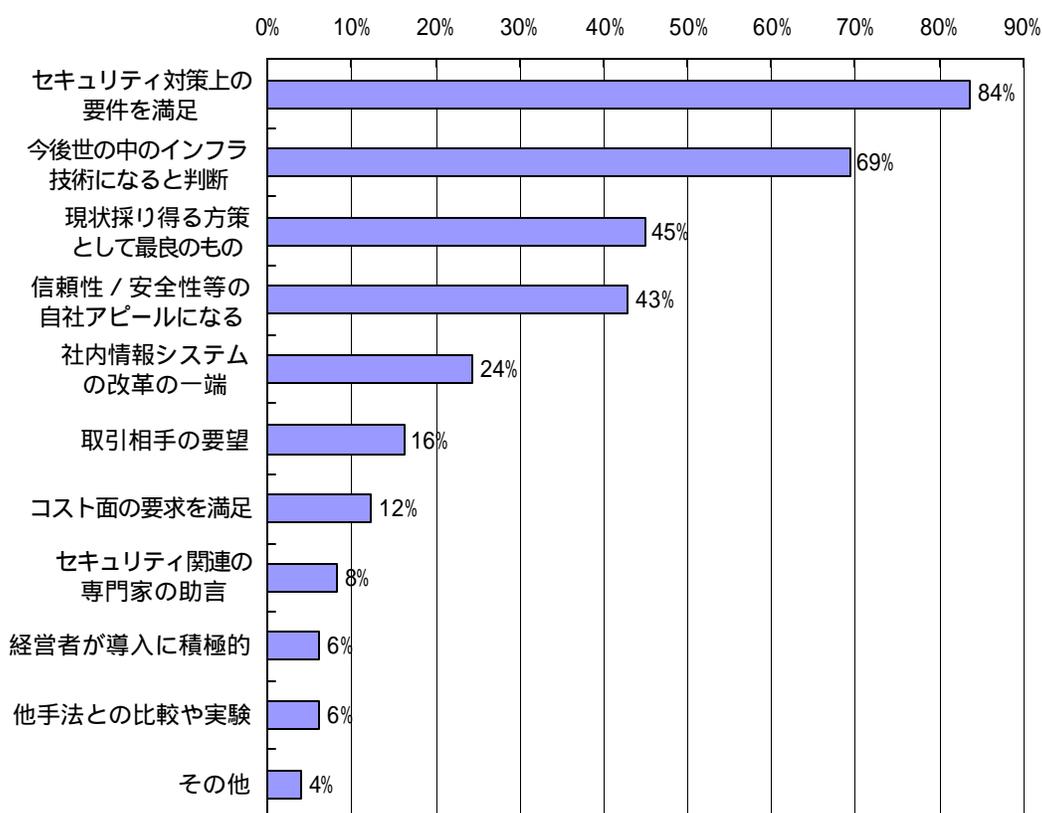


図 2-19 PKI の利用理由 (n=49)

(3) PKI の利用立場

PKI を利用する立場については、「主体としてのみ利用（自らの意思で認証局を持ち証明書を発行している）」28%、「ユーザとしてのみ利用（他社が発行した証明書を取引に利用している）」42%、「主体とユーザの両方の立場で利用」30%となっている。PKI を主体として利用している企業の比率は 58%と半数を超えており、認証局を自社で持っている企業の比率が高いことを表している。

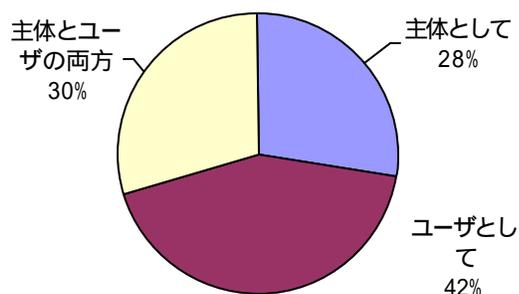


図 2-20 PKI の利用立場 (n=47)

(4) PKI 認証局の運営方式

PKI 認証局の運営方式については、「認証局の全機能を内部化している」が 46%と最も比率が高く、次いで「発行局 (IA) のみ外部化している」が 37%となっている。一方、認証局の全機能を外部化している企業の比率は 7%と低いものとなっている。

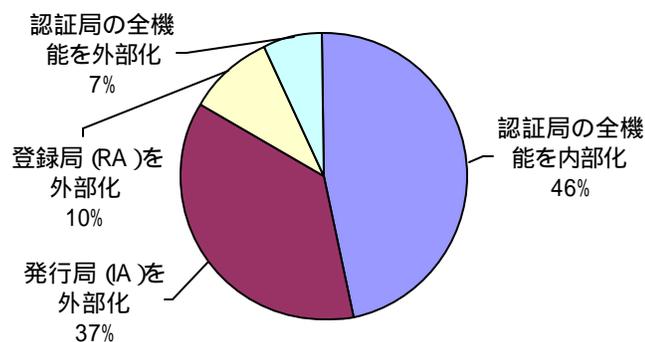


図 2-21 PKI 認証局の運営方式 (n=27)

(5) 認証機関の PKI サービスの利用状況

認証機関の PKI サービスの利用状況については、「利用している」40%、「計画はある」22%、「利用しない」38%となっており、将来的には 60%以上の企業が認証機関のサービスを利用する可能性を示唆している。

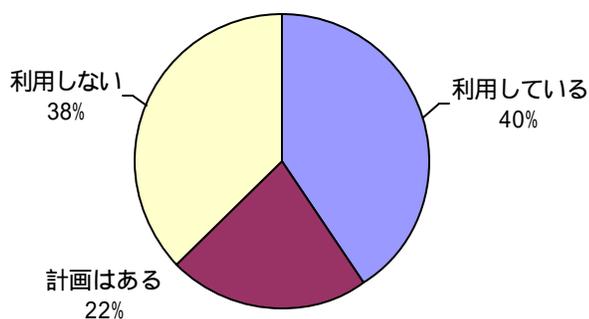


図 2-22 認証機関の PKI サービスの利用状況 (n=32)

(6) PKI の利用規模

PKI の利用規模については、十分な回答数が得られなかったため、参考値として PKI 利用者数 (RA 登録者数) および電子証明書累積発行枚数の平均値の対前年伸び率 (%) を示すにとどめる。

表 2-7 RA 登録者数の推移予測

	2002 年 (予測)	2003 年 (予測)
PKI 利用者数	277%	528%
電子証明書累積発行枚数	276%	515%
クライアント認証用	111%	217%
サーバ認証用	303%	298%
その他機器認証用	138%	138%

(7) PKI の認証局における運用規定

PKI の認証局における運用規定の設定状況について調査したところ、図 2-23に示す結果を得た。証明書申請の手続き～鍵の管理 / 保護までが全体の指摘率が 50%を超える項目となっている。認証局の運用形態別に見ても、運用規定の設定状況はほぼ同じ傾向を示しており、大きな違いは見られない。

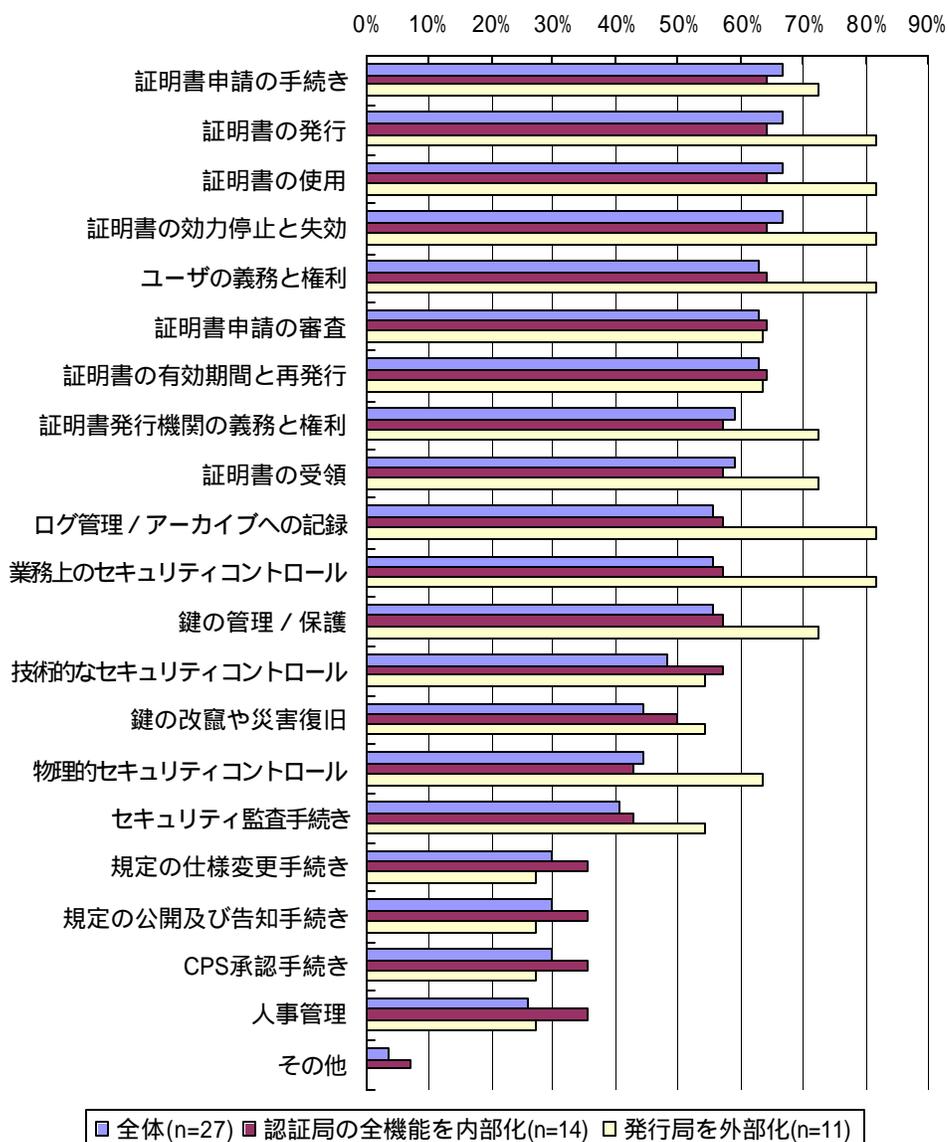


図 2-23 PKI の認証局における運用規定の設定状況 (n=27)

前述した運用規定のうち、特に重要と考えられる項目について尋ねたところ、「鍵の管理 / 保護」、「証明書発行機関の義務と権利」、「ユーザの義務と権利」、「業務上のセキュリティコントロール」といった項目の指摘率が高いことが分かる。認証局の運用形態別では、認証局の全機能を内部化している場合は、「鍵の管理 / 保護」に次いで「証明書の効力停止と失効」の指摘率が高いのに対し、発行局を外部化している場合は、「証明書発行機関の義務と権利」、「ユーザの義務と権利」、「業務上のセキュリティコントロール」に関する指摘率が高いことが分かる。

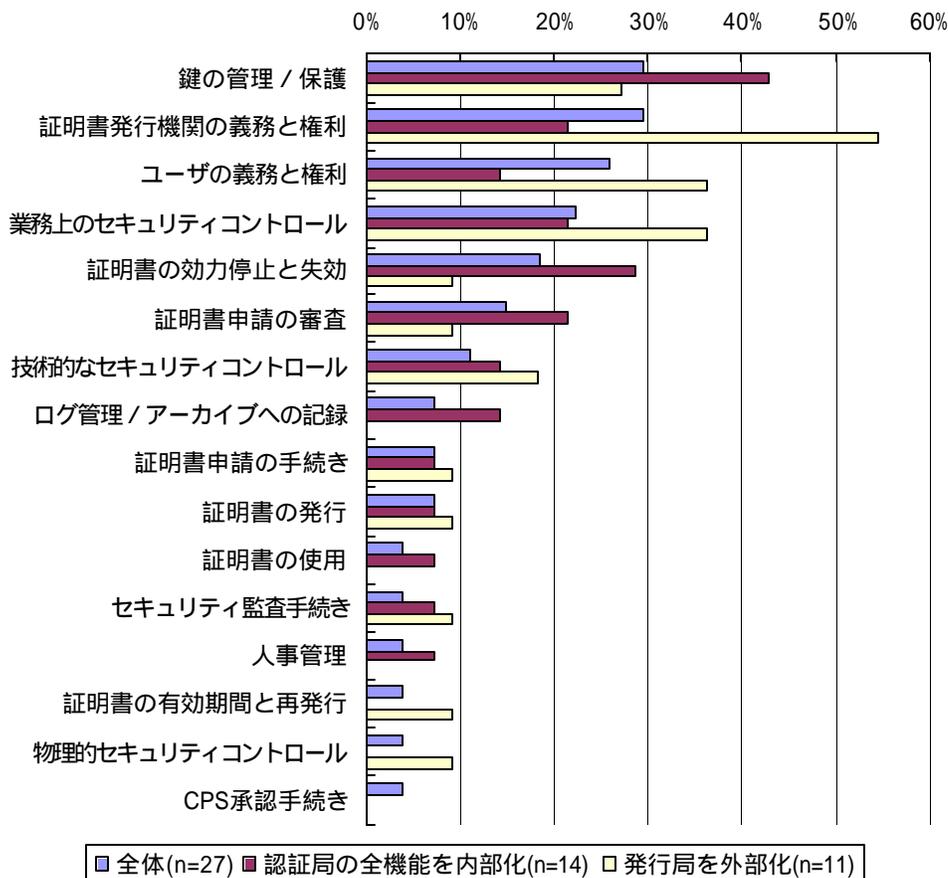


図 2-24 PKI 認証局における運用規定の重要項目 (n=27)

2.3 電子署名・認証の普及課題

ここでは PKI の普及課題として、「PKI ユーザが感じている PKI の課題」および「PKI 非ユーザが PKI を導入していない理由」について調査分析を実施し、PKI の課題の位置付けを整理した。

2.3.1 PKI 利用企業の課題評価

PKI 利用企業に対して、PKI の課題について尋ねたところ 図 2-25 に示す結果を得た。PKI の課題として指摘率が特に高いのは、「PKI システムの運用コスト」89%、「PKI の操作性 / 使い勝手」74% の 2 つであり、そのほか「PKI システムの導入コスト 56%」、「既存の業務システムとの親和性」52%、「PKI システムの導入効果」48%と続いている。基本的に経済性および導入効果に関する課題を指摘する企業が多いことが分かる。

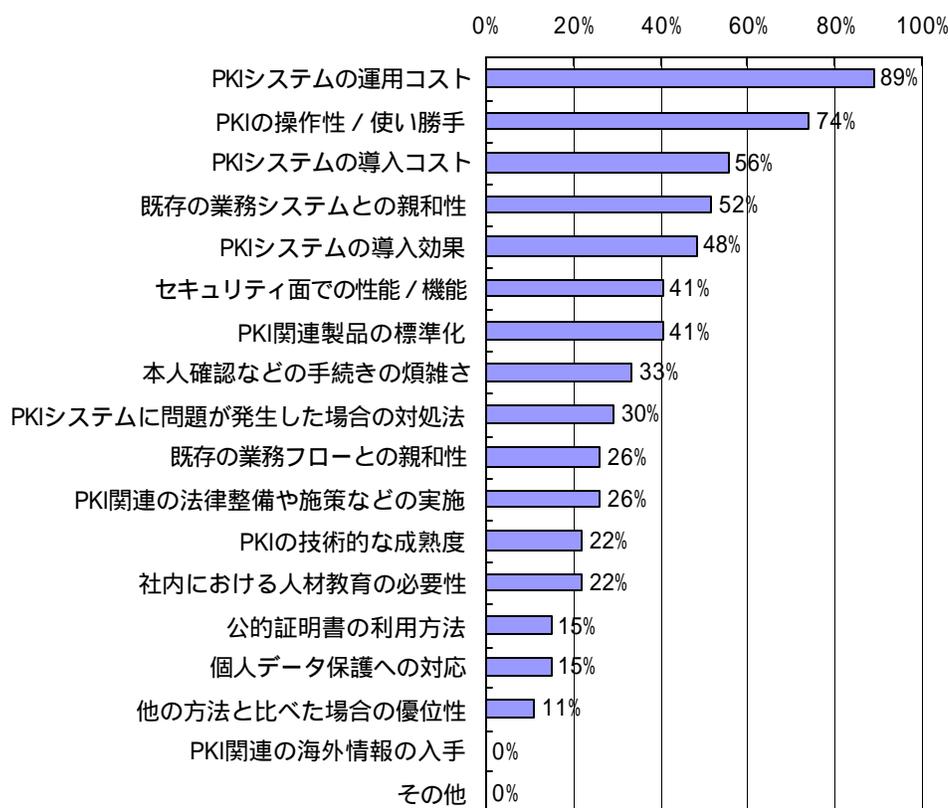


図 2-25 PKI の課題 (n=27)

2.3.2 PKI 非導入企業の非導入理由

PKI 非導入企業（ユーザとしてのみ PKI を利用している場合を含む）に対して、PKI を導入していない理由を尋ねたところ、図 2-26 に示す結果を得た。PKI を導入していない理由として指摘率が高いのは、「PKI システムの導入コストが高い」30%、「PKI システムの運用コストが高い」30%、「PKI 導入の費用対効果が捉えにくい」30%などであり、PKI 利用企業の場合と同様に経済性と導入効果に関する指摘が高いことが分かる。

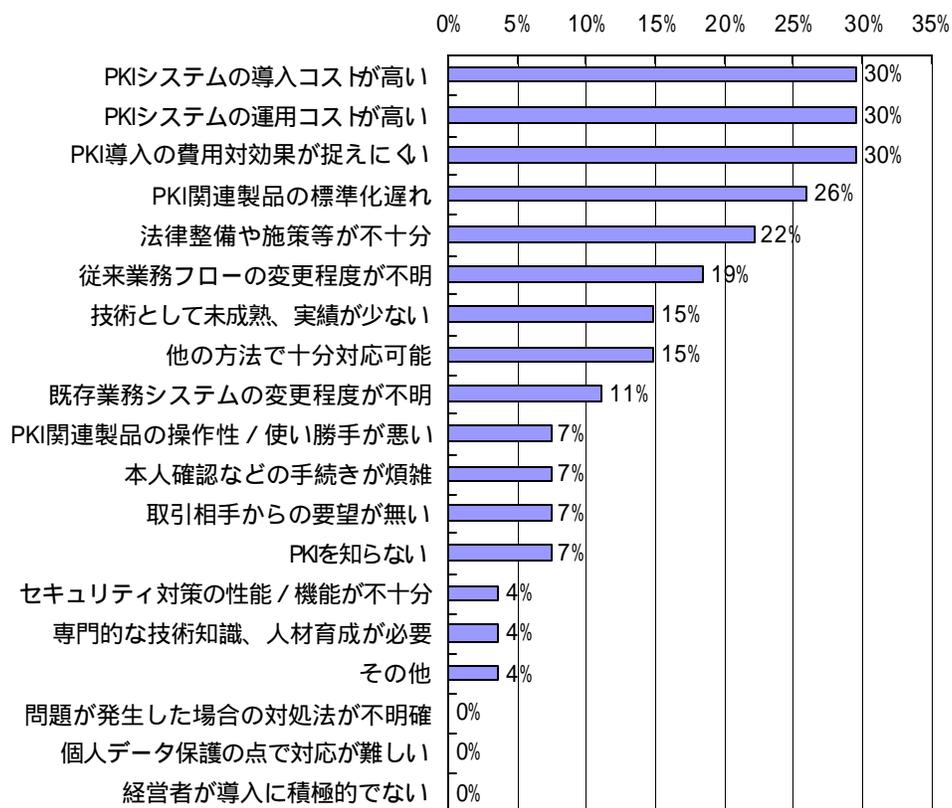


図 2-26 PKI の非導入理由 (n=27)

2.3.3 PKIの課題分析

PKI利用企業の課題（不満）とPKI非導入企業の理由（不安・想像）を分析することで、PKIの課題を「1. イメージ先行課題」、「2. 顕在課題」、「3. 潜在課題」、「4. 二次的課題」の4つに分類した。

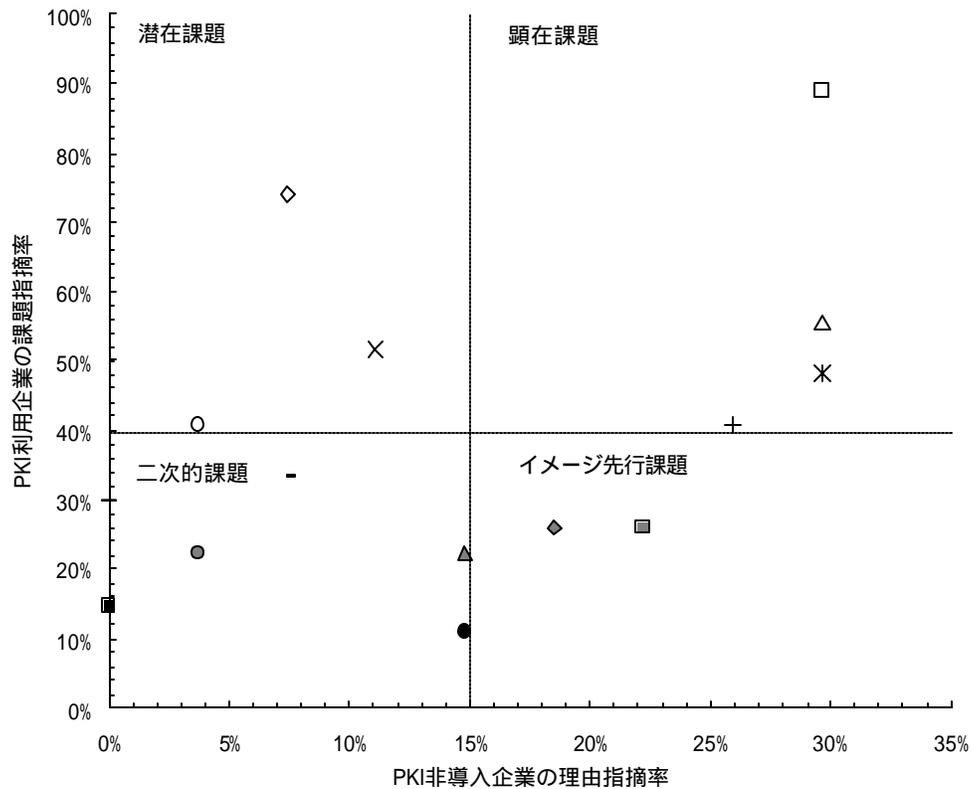
ここで「イメージ先行課題」とは、PKI利用企業の指摘率が低く、PKI非導入企業の指摘率が高い項目であり、PKI導入のためにはユーザの啓発が重要となる。「顕在課題」とは、両方の企業の指摘率が高い項目であり、イメージと実際が一致している課題である。

「潜在課題」とは、PKI利用企業の指摘率が高く、PKI非導入企業の指摘率が低い項目であり、企業が実際に利用することではじめて分かる項目である。二次的課題は、両方の企業の指摘率が低い項目であり、対応の優先度は最も低い課題となる。ここで指摘率の高低は、各項目の指摘率の平均値を基準として判断している。

表 2-8および図 2-27に分析結果を示す。PKIの顕在課題となるのは経済性（運用コスト、導入コスト）、導入効果、標準化に関する問題である。また、潜在課題となるのは、PKI製品の操作性/使い勝手、既存業務システムとの親和性、セキュリティ面での性能/機能など運用面での問題となっている。一方、既存業務フローとの親和性や法整備/施策などの実施は、イメージ先行課題に分類されることが分かる。

表 2-8 PKIの課題および非導入理由に関する分析

PKI 利用 企業 の 指 摘 率 (%)	3. 潜在課題 PKIの操作性/使い勝手 既存の業務システムとの親和性 セキュリティ面での性能/機能	2. 顕在課題 ・PKIシステムの運用コスト ・PKIシステムの導入コスト ・PKIシステムの導入効果 ・PKI関連製品の標準化
	4. 二次的課題 本人確認などの手続きの煩雑さ PKIに問題が発生した場合の対処法 社内における人材教育の必要性 PKIの技術的な成熟度 社内における人材教育の必要性 個人データ保護への対応 他の方法と比べた場合の優位性	1. イメージ先行課題 ・既存の業務フローとの親和性 ・PKI関連の法整備や施策などの実施
PKI非導入企業の指摘率 (%)		



- | | |
|-------------------------|--------------------|
| □ PKIシステムの運用コスト | ◇ PKIの操作性 / 使い勝手 |
| △ PKIシステムの導入コスト | × 既存の業務システムとの親和性 |
| × PKIシステムの導入効果 | ○ セキュリティ面での性能 / 機能 |
| + PKI関連製品の標準化 | - 本人確認などの手続きの煩雑さ |
| - PKIシステムに問題が発生した場合の対処法 | ◆ 既存の業務フローとの親和性 |
| ■ PKI関連の法律整備や施策などの実施 | ▲ PKIの技術的な成熟度 |
| ● 社内における人材教育の必要性 | ■ 個人データ保護への対応 |
| ● 他の方法と比べた場合の優位性 | |

図 2-27 PKI の課題および非導入理由に関する分析結果

参考文献

- 1) 情報化月間特別シンポジウム「電子署名・認証でどう変わる電子商取引 - 電子認証基盤・サービスの現状と展望」(平成13年10月1日)
URL : <http://www.ecom.or.jp/pkiforum/program.html>
- 2) 「電子署名・認証利用パートナーシップ(仮称)」設立準備会
URL : <http://www.ecom.jp/jpkip/action.htm>
- 3) 「電子署名及び電子認証の現状及び将来像に関する調査(仮題)」
2002.5 公開予定

・作成者

前田 陽二	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
紙田 政典	電子商取引推進協議会 (ECOM)	主席研究員

禁無断転載

平成 14 年 3 月発行
発行 :電子商取引推進協議会
東京都港区芝公園 3-5-8
機械振興会館 3F
Tel 03-3436-7500
e-mail info@ecom.jp

この資料は再生紙を使用しています。