IC カードによる個人認証

Individual Authentication by Smart Card

佐 藤 良 夫

要 約 e-business の進展とともに，企業に対して企業活動で集めた個人情報の保護の機運が高まっており，これまで以上にセキュアなシステム構築が求められている．

一方，派遣社員の採用や業務のアウトソーシングが一般化するとともに，モバイルやインターネットの活用など，社内ネットワークにアクセスする人や形態が多様化してきており，従来のユーザ ID/パスワードではシステムをセキュアに保つことは不可能である．そこで，PKI（Public Key Infrastructure：公開鍵暗号を用いたセキュリティ基盤）をベースとしたデジタル証明書の適用が一つの解として着目されている．

本稿では，デジタル証明書を納めた IC カードによる個人認証の実現方法を紹介する．

Abstract E-business has driven the necessity for the corporate to protect customers' personal information acquired during the corporate business activities and to implement more secured systems.

On the other hand, it has been getting common that they employ dispatched workers instead of regular full-time staff and outsource some a part of business. In result, various people are accessing to their computer network by means of various methods, and it is no longer possible to keep their computer systems secured by validating accessibility only with user IDs and passwords as before. Therefore, it is now being attracted attention as the solution for to apply Digital Certificates with Public Key Infrastructure（PKI, security base using public key）to their computer systems.

The topic introduced in this paper is the implementation method of individual authentication by smart cards that contain digital certificates.

1. は じ め に

e-business が進展する中，システムをセキュアに保つことの重要性がますます増している．

2001 年 3 月 27 日に閣議決定された『個人情報保護法』では，企業活動を通じて収集された個人情報を適正に取り扱う努力義務を一般企業にも課すと言われており，個人情報流出といった脅威への対応が望まれる．また，個人情報の流出は企業の社会的信用を傷つけるだけでなく，個人情報流出に対する損害賠償へとつながり，企業経営に対する影響も無視できなくなってきている．例えば，百万人の個人情報流出に対して，一人一万円の損害賠償を行えば，百億円の損失が発生することになってしまう．

一方，経営の合理化の観点から派遣社員の採用や外部への業務委託が一般化するとともに，モバイルやインターネット経由での社内ネットワークへのアクセスも増加し，様々な人が様々な場所から社内ネットワークへのアクセスを行うようになってきており，社内ネットワークにおいてもシステムをセキュアに保つことが必要になってきたと言える．

このような状況から，社内ネットワークと言えども，インターネットに潜む『盗聴』

や『改竄』,『なりすまし』,『否認』といった脅威への対応が必要であり，従来のユーザ ID/パスワードではこれらの脅威に対応することができない.

『盗聴』や『改竄』,『なりすまし』,『否認』といった脅威に対しては，PKI をベースとしたデジタル証明書（以降，証明書と略す）が有効であり，証明書を用いた個人認証により社内外からの社内ネットワークへの不正アクセスを防止することが必要である.

本論文では，IC カードに納めた証明書を用いた個人認証の実現方法等について記述する.

2. 個人認証とは

IC カードに格納した証明書を使用した個人認証では，どのようなことを行うのであろうか．ここでは，Web アプリケーションにおける SSL[*1] 相互認証を例に，個人認証について説明する.

SSL 認証には，Web サーバが保持する証明書（サーバ証明書）と Web ブラウザに組み込まれたサーバ認証局証明書（サーバ証明書を発行した認証局自身の証明書）により認証を行う SSL サーバ認証と，SSL サーバ認証に加えて Web ブラウザが保持する証明書（クライアント証明書）と Web サーバに組み込まれたクライアント認証局証明書（クライアント証明書を発行した認証局自身の証明書）により認証を行う SSL クライアント認証も行う SSL 相互認証がある（図 1）.

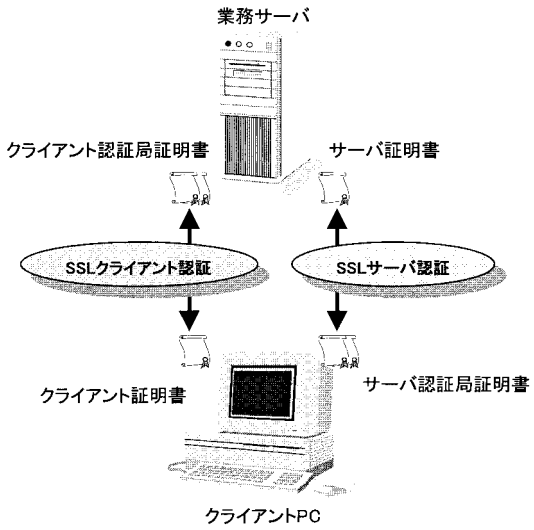

図 1　SSL 相互認証

個人認証では，SSL クライアント認証に用いられたクライアント証明書により，以下の検査を行う.

1） 認証

クライアント証明書より，その証明書を持つユーザを特定し，社内ネットワークや業務サーバなどへのログイン権限を持つユーザであるか否かを検査する.

2) アクセス制御

認証されたユーザが業務へのアクセス（更新や参照など）権限を持つか否かを検査する．

すなわち，ICカードによる個人認証とは，ICカードに格納された証明書より，持ち主が正当なユーザであることを特定するとともに，業務へのアクセス権限を持つか否かを検査することであると言える．

3. 個人認証を支えるソフトウェア

ここでは，ICカードによる個人認証の実現に使用されるソフトウェアと個人認証への適用ポイントを紹介する．

3.1 認 証 局

SSLクライアント認証による個人認証の実現には，個人に対する秘密鍵・公開鍵の生成と証明書の調達が必要なため，証明書を発行する認証局が必要となる．日本における認証局ベンダとしては，日本ボルチモアテクノロジーズ株式会社や日本ベリサイン株式会社，エントラストジャパン株式会社などがある．証明書の調達については，自営にて認証局を構築する方法と，外部の証明書発行サービスを利用する方法がある．

PKIは，秘密鍵・公開鍵のペアと認証局から発行される証明書から成り立っていると言うこともでき，実世界に置き換えれば，秘密鍵が実印，証明書が印鑑証明書に相当する．

証明書の発行に際しては，証明書の有効期限（社員証用であれば，社員証の有効期限と一致させる）や所有者の識別情報（SubjectDNと呼ぶ）への記載項目などを決定しなければならない．SubjectDNには，所属や名前のように証明書の有効期間中に変更される可能性のある情報を指定してはならない．

SubjectDNの設定例

c=jp	国を指定する。日本なのでjpを指定する。
o=nihon unisys ltd.	組織を指定する。会社名などを用いる。
ou=idcard	組織単位を指定する。任意に設定可能である。
cn=123456	共有名を指定する。社員番号やユーザIDを用いる。

社員に対する証明書の発行/失効は，新入社員の入社や定年退職をトリガーとして人事情報と連携して一時期に大量に行うため，アプリケーションと連動した証明書の一括発行/失効機能が必要である．

また，電子署名の確認やS/MIME[*2]などにも使用するため，証明書の発行に際して公開用証明書を容易に取り出せる機能も必要とされる．

ICカードに格納する証明書の一括発行/失効の流れの概略は，図2に示す「証明書発行/失効の流れ」のようになる．ICカード発行支援システムは，人事システムと連携して認証局に対して証明書の発行/失効要求を行う．公開用証明書は，証明書の発行時にディレクトリサーバに書き込まれる．ICカードの券面に印刷する情報や証明書/秘密鍵は，印刷工場に送付されてICカードに書き込まれる．

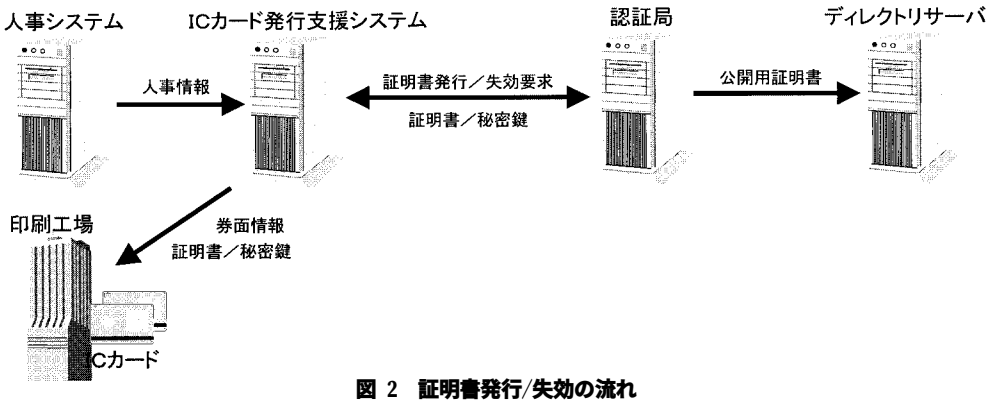

図 2　証明書発行/失効の流れ

3.2　ディレクトリサーバ

ディレクトリサーバは，ディレクトリというデータベースを利用して，指定された名前に対して場所などの情報に変換する仕組み（ディレクトリサービスと呼ぶ）を提供するものであり，代表的なものとして，Active Directory（Microsoft）や eDirectory（Novell），iPlanet Directory Server（iPlanet）などがある．

ディレクトリサーバでは，現実世界の組織構造をツリー構造で表現し，様々なアプリケーションからの情報共有を実現することができる．

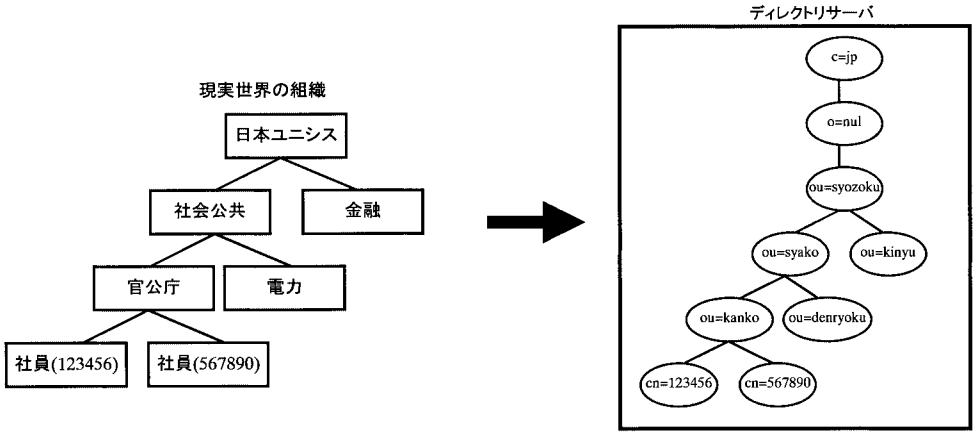

図 3　ディレクトリサーバによる現実世界の組織構造表現例

ディレクトリサーバへのアクセスには，LDAP（Lightweigrht Directory Access Protocol）と呼ぶ標準プロトコルを使用する．ディレクトリサーバ上のオブジェクトへのアクセスは，オブジェクトの識別名（DN : Distinguished Name）を指定することにより行う．図 3 に示す「ディレクトリサーバによる現実世界の組織構造表現例」を例にとると，識別名は cn＝123456,ou＝kanko,ou＝syako,ou＝syozoku,o＝nul, c＝jp のように指定する．

「3.1　認証局」で説明したように，証明書の SubjectDN には組織情報を設定しないため，ディレクトリの社員オブジェクトの検索は，cn に設定した情報のみで行う

ことになる．高速に検索するため，cn に対してはインデックス（索引）を設定すべきである．

「3.1　認証局」の図 2「証明書発行/失効の流れ」で説明した認証局からのディレクトリサーバに対する公開用証明書の書き込みについてであるが，認証局によっては，証明書の SubjectDN の設定に応じた階層構造の cn オブジェクトにしか公開用証明書を書き込むことができないことがある．このような場合は，中間ディレクトリサーバに書き込まれた公開用証明書を，個人認証に使用するディレクトリサーバの組織構造に応じた cn オブジェクトに書き込むプログラムを開発しなければならない．

IC カードによる個人認証では，ディレクトリサーバを個人に対して発行された証明書の失効管理や，業務に対するアクセス権限情報（アクセス制御ルールと呼ぶ）の管理などに使用することが考えられる．

例えば，図 4 の「ディレクトリサーバによる情報管理例」では，ディレクトリサーバの組織ツリーが組織構造を表し，業務ツリーが人事，経理といったコンピュータで処理する業務の構造を表している．組織ツリーの社員オブジェクトで有効な証明書を管理し，業務ツリーのルール・オブジェクトでアクセス制御ルールを管理すれば，以下のように Web アプリケーションでディレクトリサーバを利用することが可能である．

① SSL 相互認証によりクライアント PC から差し出されたクライアント証明書を Web サーバより得る．

② クライアント証明書より cn を抽出する．

③ cn の値を指定してディレクトリサーバの社員オブジェクトより有効な証明書を得て，クライアント証明書と突き合わせを行う．一致するものが無ければ，クライアント証明書は失効されたものであるため，エラー画面を表示するとともに，不正アクセスログを採取して処理を終了する．

④ 業務名とアクセス制御ルール名称を指定してディレクトリサーバのルールオブジェクトよりアクセス制御ルール（例．役職コードがマネージャのみアクセス可）を得る．

⑤ cn の値を指定してディレクトリサーバの社員オブジェクトより役職コードの値（例．一般社員）を得，アクセス制御ルールに適合するか検査する．

⑥ アクセス制御ルールに適合しない社員からのアクセスであれば，エラー画面を表示するとともに，不正アクセスログを採取して処理を終了する．

⑦ アクセス制御ルールに適合する社員からのアクセスであれば，認証ログを採取した後，業務処理を行う．

3.3　PKI 対応個人認証システム Hubware

SSL 相互認証による個人認証を実現するためには，証明書を PC の Web ブラウザに組み込むのではなく，“ 鍵 ” のように持ち運びできる IC カードのような外部トークンに格納して運用することが求められる．証明書を PC の Web ブラウザに直接組み込む運用では，個人認証ではなく，PC 認証になってしまう．

SSL 相互認証に IC カードを使用するためには，クライアントとなる PC に IC カードリーダライタドライバや PC/SC[*3] ベースコンポーネント，PKCS[*4]#11 モジュール，CSP[*5] モジュールなどのインストールが必要である．また，IC カーでは，PIN（Per-

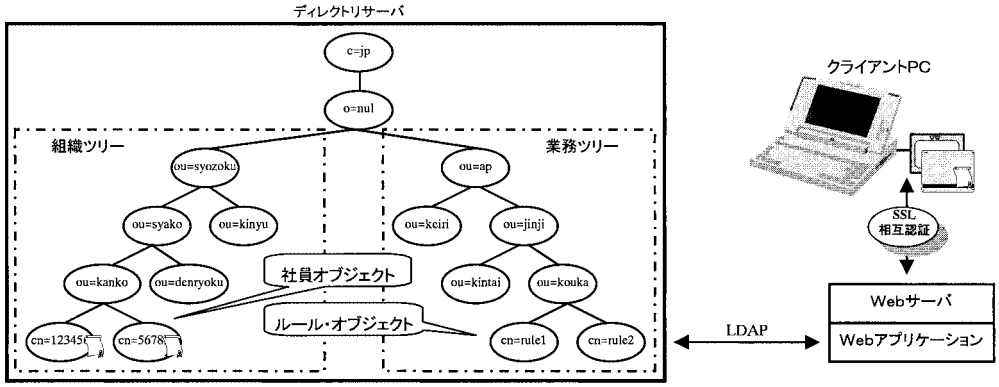

図 4　ディレクトリサーバによる情報の管理例

sonal Identification Number）と呼ぶ暗証番号を規定回数以上連続して誤った場合，IC カードがロック（PIN ロックと呼ぶ）されて使用不能となるため，PIN ロック解除機能なども必要である．

日本ユニシス（以下，当社）では，IC カードによる個人認証を実現するためのクライアント用ソフトウェアと各種支援機能を『PKI 対応個人認証システム Hubware』として提供している（図 5）．

Hubware は，クライアント PC に対しては，離席時に IC カードを抜くことによりキーボードの操作や画面の盗み見などを防止するスクリーンロック機能や，IC カードを挿入しないとログオンできなくするログオン制御機能，PC のシャットダウン時に IC カードの抜き忘れを警告する機能なども提供する．また，IC カードの自営発行機能（Hubware カード発行システム）も提供しており，中小企業などでの IC カードの少量発行にも対応可能である．

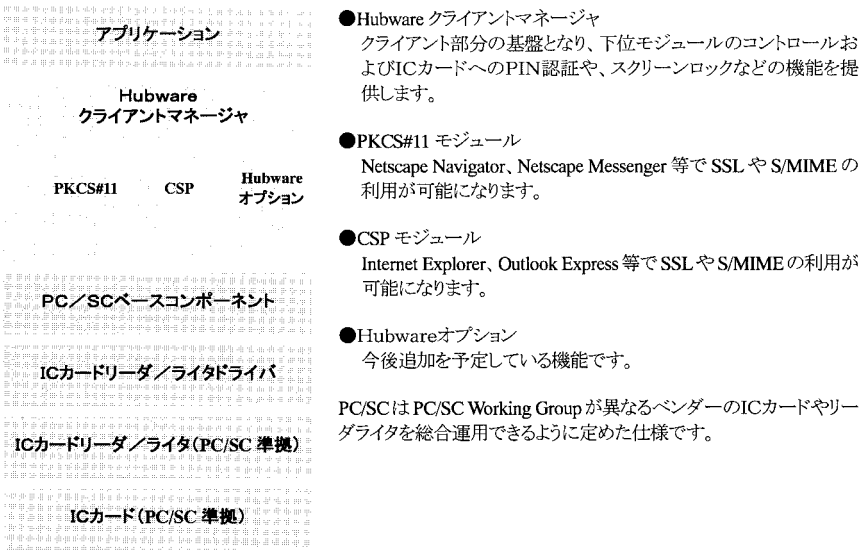

図 5　Hubware クライアントシステムアーキテクチャ

4. 個人認証実現への検討課題

前章では，IC カードによる個人認証を支えるソフトウェアを簡単に紹介したが，これらのソフトウェアを採用するだけでセキュリティを保てると考えるのは早計である．ソフトウェア，あるいは，技術のみでセキュリティを確保することは不可能であり，エンドユーザに対するセキュリティの啓蒙も含めて，会社としてのセキュリティポリシの策定と運用が最も重要である．

本章では，個人認証を実現する上での検討課題について，運用の観点から幾つかを紹介する．

1）　不正発行の防止

最初に検討すべきは，IC カードの不正発行を如何に防止すべきかである．

IC カードの不正発行の防止は，極論すれば，IC カードに格納される証明書の不正発行防止と言い換えることができる．

このため，IC カードの不正発行の防止は，IC カードに格納される証明書の不正発行防止に準拠するものとし，CPS（認証局運用規定）にて定められた証明書発行手順を遵守することになる．

認証局など証明書の発行に必要な機器は，鍵の掛かる専用の部屋に設置するとともに，ファイアウォールに守られたバリアセグメントに設置し，ネットワーク面でも社内 LAN からの不正アクセスを防止する配慮が必要である．

認証局の操作においても，専用の IC カードによる認証を行うとともに，複数人による操作を義務づけるなどの対策も必要となる．

2）　不正使用の防止

次に検討すべきは，IC カードの不正使用を如何に防止すべきかである．

IC カードの不正使用防止は，「他人に IC カードを使用されないようにする」ことと，「他人が IC カードを使用できないようにする」という観点などから検討を行う．

①　他人に IC カードを使用されないようにする

他人に IC カードを使用されないようにするとは，IC カードの机の上などへの放置等を防止することである．

机の上などに放置されることは，IC カードを常時携帯する社員証にすることにより防止できるであろう．PC の終了時に IC カードリーダから IC カードの抜き忘れを警告する機能も有効である．

社員以外に発行するセキュリティカードについては，IC カードに氏名を印刷することにより，IC カードの持ち主であることを意識させることが，持ち主の退社後にその IC カードを他の社員に使用させるような持ち回りの防止に有効であろう．

②　他人が IC カードを使用できないようにする

紛失した IC カードを他人に拾われた場合などに，IC カードを他人に使用できないようにすることが必要である．対策は，PIN の管理と証明書の失効管理になる．

PIN の管理とは，PIN の値が簡単に他人に判別できないようにすることであ

る．社員番号や電話番号，生年月日など簡単に判別されるような PIN を使わないように啓蒙することや，PIN の最小桁数をあまり短くしないこと，PIN ロックに至る PIN 施行回数を適切に設定すること，定期的に PIN の値を変更することなどが対策としてあげられる．また，大量の IC カード発行時に初期 PIN を機械的に設定するような場合は，他人の初期 PIN を推測することが容易にできるため，IC カードを最初に使用する時に強制的に PIN を変更させる機能が有効である．

紛失した IC カードは，格納されている証明書を失効させることにより使用不可とすることができる．証明書の失効管理とは，失効させた証明書を管理することにより，紛失した IC カード等の不正使用を防止することである．証明書の失効管理方法には，認証局に対して失効要求を行って作成した CRL[*6]．を用いて行う方法や，検証局（VA：Validation　Authority）を構築する方法，ディレクトリサーバに有効な証明書のみを管理する方法などがある．

③　秘密鍵を盗まれないようにする

秘密鍵は，PKI の根幹をなすものであり，これを盗まれることはセキュリティが保てないことを意味する．

このため，秘密鍵については，鍵預託方式（鍵ペアのバックアップを保管する方式）を採用しないことが望ましい．鍵預託方式を採用しなければ，秘密鍵は IC カードの中にのみ存在することになり，セキュリティが低下する懸念が無くなる．

IC カードの破損・紛失時には，新たな鍵ペア（秘密鍵・公開鍵）を生成して再発行された証明書を格納した IC カードを発行することになる．

3）　不正使用の早期発見

不幸にして，PIN の値が盗まれ，IC カードを他人に不正使用された場合，どのような手段で早期に発見すべきかについても検討が必要である．

例えば，不用意なユーザが机の上に放置した IC カードを不正使用されても，IC カードが戻されていれば，不正使用されたことに気が付かないであろう．

不正使用の発見には，Web アプリケーションによる最終ログイン日時の表示が有効である．SSL 相互認証を行う業務毎に，ユーザの最終ログイン日時を記録し，ログイン時に前回のログイン日時を表示するのである．利用者が，表示されたログイン日時を見て，身に覚えがなければ不正使用されたことになる．

4）　不正使用発覚時の対応

不正使用されたことが発見された場合，どのような対応を実施するかについても事前に検討しておくことが重要である．不正使用が発見されてから対応策を検討するのでは，泥縄となり，有効な対策が施せない場合も考えられる．

その IC カードが何時不正使用されたかを把握するためには，Web アプリケーションでの認証時に認証ログを採取することが有効であり，過去の認証ログを調査することにより不正使用された日時を把握することが可能となる．

5）　使用不可時の対応

最後に IC カードが使用できない事態への対応方法についても検討が必要であ

る．

IC カードが使用できない事態とは，IC カードの紛失・破損や不携帯，PIN ロック，証明書の有効期限満了などである．証明書の有効期限満了については，当然，新たな証明書が格納された IC カードが配布されるので，ここでは対象外とする．

IC カードの紛失・破損に対しては，業務的な困窮度合いと新たな IC カードがユーザの手元に届くまでの期間から検討することになる．例えば，IC カードを紛失した場合に即日再発行されれば問題がないが，一ヶ月毎にまとめて再発行ならば，再発行されるまでの間のことを検討する必要がある．

PIN ロックや不携帯についても同様である．

基本は，セキュリティポリシーに則って基本原則を決定することである．しかし，原理原則にとらわれすぎると利用者の利便性を損ない，強い抵抗に出会うこともあるため，ケースバイケースで緊急対応が必要なものに対しては，セキュリティ重視の基本運用であっても利便性重視の緊急対応を実施するなど，弾力的な運用についても検討しておくことが必要であろう．

5. おわりに

本稿では，SSL 相互認証を使用した IC カードによる個人認証の実現方法について簡単に紹介したが，証明書の用途は PDF 文書や XML 文書，電子申請への電子署名，インターネット経由や RAS 接続，ドメイン等での各種ログイン認証，VPN などへと拡大されつつあり，e-business 時代における『盗聴』，『改竄』，『なりすまし』，『否認』への最適解と言え，セキュアなシステムの構築に必須の技術である．

なお，既に述べたことではあるが，技術のみでセキュリティを確保することは不可能である．セキュリティポリシーをベースとした運用とエンドユーザへのセキュリティの啓蒙が非常に重要である．あくまでも，人が中心となることを忘れてはならない．

本稿で，より具体的な事例を紹介したいところであるが，内容がセキュリティに関することであるため，割愛せざるを得なかったことを理解して頂きたい．

最後に，本稿がセキュアなシステム作りの一助になれば幸である．

＊ 1　SSL（Secure Sockets Layer）：Web サーバと Web ブラウザ間の通信を暗号化するプロトコル．

＊ 2　S/MIME（Secure/Multipurpose Internet Mail Extensions）：電子メールを暗号化する技術．

＊ 3　PC/SC（Personal Computer/Smart Card）：PC/SC は PC/SC Working Group が異なるベンダーの IC カードやリーダライタを総合運用できるように定めた仕様．

＊ 4　PKCS（Public Key Cryptography Standard）：PKCS は，RSA Laboratories が中心となって定義した規格であり，PKCS#1 から PKCS#15 の 15 種類が定義されている．PKCS#11 は，暗号化機能を実行する IC カードなどのデバイスに対する API を定義したものである．

＊ 5　CSP（Cryptography Service Provider）：CSP は，Windows においてすべての暗号化操作を実行し，秘密鍵を管理することにより，Internet Explorer，Outlook Express 等で SSL や S/MIME の利用を可能とする．

＊ 6　CRL（Certification Revokation List）：有効期限内にも関わらず，「無効」とされた証明書の一覧リスト．

参考文献［1］「LDAP インターネットディレクトリアプリケーションプログラミング」（著：ティム・ハウズ＋マーク・スミス訳：松島　栄樹＋岡　薫　株式会社ピアソン・エデュケーション）
［2］「all about PKI vol.2」（著：浅野　昌和　日本ボルチモアテクノロジーズ株式会社）
［3］「連載：電子メールに潜むリスク」（http : //www.atmarkit.co.jp/fitbiz/feature/em-risk/02/01.html）
［4］「連載：PKI 基礎講座」（http : //www.atmark.co.jp/fsecurity/rensai/pki 01/pki 01.html）
［5］「「敵は身内にあり」, 社内ネットへの不正行為の大半がアクセス権を持つ従業員」（日経 IT Pro：米 Eweek の調査結果
http : //itpro.nikkeibp.co.jp/free/ITPro/USENEWS/20010620/10/print.shtml）
［6］「技術だけでは守れない，認識すべき「セキュリティポリシー」の必要性」（日経 IT Pro : http : //itpro.nikkeibp.co.jp/free/ITPro/SEC_CHECK/2000110/1/print.shtml）
［7］「What's IC CARD？」http : //www.jicsap.com/what/intro.html

執筆者紹介　佐　藤　良　夫（Yoshio Sato）
1975 年日本大学文理学部卒業．同年日本ユニシス（株）入社．生命保険，損害保険の客先担当 SE を経て，1980 年より FAST 1100 の開発・保守，1983 年より AIS 1100 の開発・保守，1990 年より UA/ASDF の日本化，1993 年より客先担当 SE としてミドルソフトウェアの開発等に従事．現在，社公システム二部ソリューション＆開発技術室に所属．