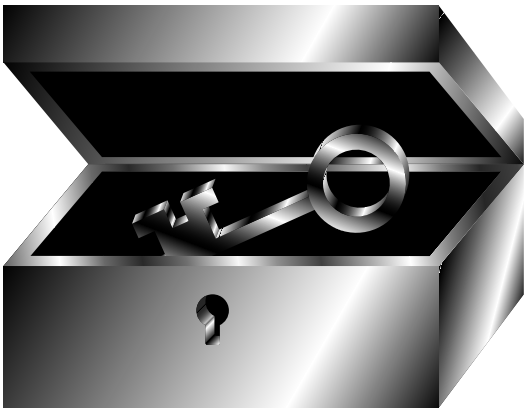
インターネット最新テクノロジー：第39回

安全性を確保する「鍵」のインフラ

PKI（Public Key Infrastructure）

IT技術の利用が拡大するにつれて、それを脅かす不正行為の増加も著しく、社内システムのセキュリティー強化が情報システム部門の大きな課題となっている。また、電子商取引の発展が期待される中で、安全なビジネストランザクションの実現が今後の利用拡大の鍵だと考えられている。PKIは、こうしたセキュリティーに対する要求を、効率良く安価に、拡張性と相互接続性を保ちながら実現できる唯一の手段である。

前田 司　RSAセキュリティ株式会社



公開鍵暗号の仕組み

PKIの基本的な役目とは、公開鍵暗号において利用される公開鍵の配布と管理である。PKIを通して他者の公開鍵を入手して利用することにより、その相手との間で公開鍵暗号の基本的機能である守秘や認証などのセキュリティーを伴う通信を実現することが可能となる。ここではまず、公開鍵暗号について簡単に紹介する。

現在、広く利用されている暗号の方法は、大きく共通鍵暗号と公開鍵暗号の2種類に分けられる。共通鍵暗号は古くから利用されてきた暗号方式で、メッセージを送る側と受け取る側で共通の「鍵」を持ち、この鍵によって暗号化および復号（解読）を行う方法である。この方式では、事前の秘密裏の暗号鍵合意を必要とするため、暗号通信を行う相手を事前に確認し、その相手ごとに鍵の決定と管理が必要となること、事前の鍵合意のためメッセージ交換とは別の秘密の通信路が要求されることなど考慮すべき点が多い。

一方、公開鍵暗号は20世紀後半に考案された新たな概念の暗号方法で、暗号鍵と復号鍵が異なるという特徴を持つ。この2つの鍵は数学的に関係付けられているが、暗号鍵から復号鍵を計算によって導き出すのは大変困難である。公開鍵暗号では、暗号鍵は「公開鍵」、復号鍵は「秘密鍵」と呼ばれる。自分の暗号鍵を広く公開し他者が入手可能なようにしておくことにより、自分に対するメッセージを暗号化できるため、不特定多数の相手からの通信を容易に実現できる。

ただし、公開鍵暗号の暗号・復号処理は複雑な数学演算を必要とし、秘密鍵暗号にくらべて単位メッセージあたりの処理時間が長くなるため、大量のメッセージを暗号化するようなアプリケーションには不向きである。実際のアプリケーションでは、両暗号方法の欠点を相互に補うため、まず公開鍵暗号によって事前に共通鍵暗号の鍵を交換し、その鍵を用いてデータの通信を行うことが一般的に行われている。

公開鍵暗号による署名

公開鍵暗号には守秘機能とは別に、もう1つ有効な働きがある。公開鍵暗号の公開鍵と秘密鍵は数学的に関係付けられており、あるメッセージを自分の秘密鍵で変換した文は、それに対応する公開鍵でのみ、元のメッセージに復元することが可能である。秘密鍵で変換した文は、公開鍵を知っている者は誰でも容易に元の文を復元できるため、これは秘密通信にはなり得ないが、ある公開鍵で、ある文を意味あるメッセージに復元できるということは、その文を作成した者がその公開鍵に対応する（秘密の）秘密鍵を知っているということを意味している。公開鍵暗号は、自分の秘密鍵を用いることにより、自身を認証してもらうためのデータの作成に利用できる。

この公開鍵暗号の認証機能を利用し、文書に署名を付けることが可能である。文書作成者は（あらかじめ合意された手順により）その文書全体あるいは一部分、あるいはハッシュと呼ばれる関数を用いて生成した文書の（一種の）要約を自分の秘密鍵で認証用データに変換し、これを署名として文書に添付する。文書を受け取った者は、その署名部分を署名者が公開している公開鍵で逆変換し、そ

の内容が（あらかじめ合意された）受け取った文書全体、あるいは受け取った文書の要約と一致する場合には、署名者を認証し、受け取った文書の内容が署名時の内容と相違ない（改ざんされていない）ことを確認できる。またこれは、事後における文書作成事実の否認の防止にも役立つ。

このように、公開鍵暗号を利用することで、守秘、認証、改ざん防止、否認防止といった、メッセージ交換・処理において要求されるセキュリティー機能を実現することが可能となる。しかも公開鍵の公開方法を工夫することにより、不特定多数の通信相手との間で利用できるため、近年利用が拡大しているインターネット上での電子商取引におけるセキュリティー確保の手段として大変有効である。

なお、公開鍵暗号を安全に利用するためには、いずれの用途の場合でも自分の秘密鍵を安全に保管することがもっとも重要な点である。署名用の鍵の場合には、署名後にその秘密鍵を廃棄することにより、秘密鍵漏洩の危険性を低下させられる。守秘用の秘密鍵は、後日の復号のために保存されることが一般的である。

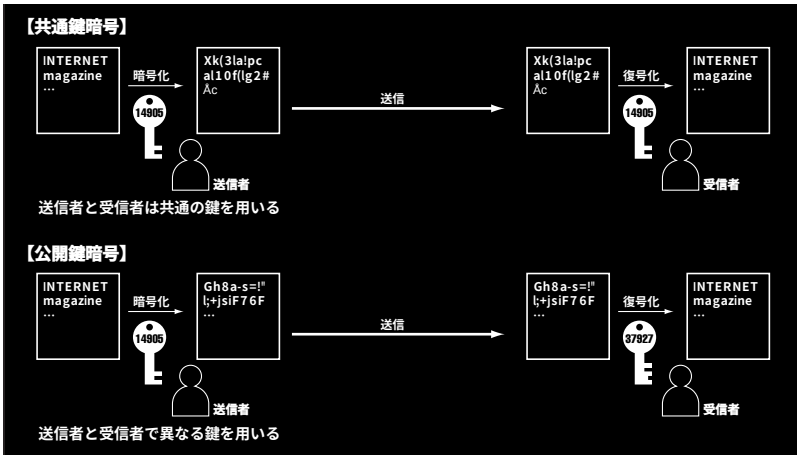
公開鍵の所有者を保証する電子証明書

他者の公開鍵を利用してその相手に暗号通信を行ったり、その相手の署名の検証を行う際に、その公開鍵が相手が所有する鍵であることを確認することは、安全性確保の必須要件となる。それを怠れば上述の公開鍵暗号がもたらすセキュリティーは意味をなさない。信頼できる（正しく公開鍵と所有者の身分が対応する）公開鍵の入手が保証されなくてはならない。

電子証明書はその目的のために考案されたデータ構造の一種である。一口に電子証明書と言っても多様な形態が考えられるが、一般にはITU-Tが定めた標準であるX.509公開鍵証明書を指すと考えてよい。本稿でもX.509に基づいた説明を行う（他の証明書の例については後述する）。

電子証明書とは、公開鍵と、その所有者（エンティティー）の身分（名前、所属など）を表すデータが記載された文書、さらにその文書全体を証明書を発行する機関（認証機関、CA：Certification Authority）が署名した署名データ、その他証明書自身のデータ（番号、利用目的、有効期限）を合わせたものである。電子証明書の利用者は、CAが正しくエンティティーの情報と公開鍵を結び付けていることを信頼することにより、電子証明書を信頼する。

証明書利用者は、CAの署名をチェックすることにより、エンティティーと公開鍵の組み合わせを検証するが、CAの署名をチェックするためにはCAの公開鍵が必要となる。CAの公開鍵もやはりCA自身の証明書の形で配布されて証明書利用者に利用される。



❶ 共通鍵暗号と公開鍵暗号

❷ 公開鍵暗号による署名

ITU-T（アイ・ティー・ユー・ティー／International Telecommunication Union, Telecommunication Standardization Sector）：国連の専門機関、国際電気通信連合（ITU）の電気通信標準化部門。電気通信に関する各種の調整や勧告を行う。

- PKI利用者（エンドエンティティー）の登録
- 認証機関（CA）による証明書発行：決められたポリシーに基づく証明書の発行
- 証明書失効（廃棄）：証明書失効管理
- 発行証明書の情報提供：発行された証明書の公開のためのリポジトリー（保管庫）
- 失効証明書の情報提供：失効証明書リストの公開（CRL：Certificate Revocation List）、失効情報検索手段（たとえばOCSP：Online Certificate Status Protocol）
- 鍵バックアップ：守秘機能に用いられる秘密鍵のバックアップ、秘密鍵を保護するパスワードなどのバックアップ
- 鍵更新・鍵履歴管理：有効期限切れの証明書の更新、履歴の管理
- 信頼関係の維持管理：信頼チェーンに連なるCAのセキュリティーポリシーと手順の定期的検査。CAの相互認証、特に異なるPKI同士の相互認証（信頼）
- 否認防止のサポート、タイムスタンプ生成
- クライアントソフト：PKIサービスを利用できる（要求する）利用者環境の提供

PKIサービスの例

CA自身の証明書には他のCAによる署名か、そのCA自身による署名がされる。他のCAによる証明書はさらにそのCAの証明書を必要とする。このようにエンティティーの証明書は複数のCAの証明書をたどるチェーン構造を持つ。そのチェーンの最終がエンド・エンティティー（CAではないPKIエンティティー）の証明書であり、始まりは自分自身の署名をもつCAの証明書となる。このCAをルートCAと呼ぶ。チェーンの途中にあるCAへの信頼はその先（上位）のCAによって確認されるから信頼関係もこのチェーンをルートからたどる構造となる。ルートCAが信頼関係の出発点であり、証明書利用者はルートCAを信頼（公開鍵とエンティティー情報の正しい対応付けを行っている）することにより、その下に連なるすべてのCAを信頼し、それらが発行する証明書を信頼（公開鍵とエンティティー情報の正しい対応付けが行われている）する。

電子証明書にはその用途、あるいは使われている公開鍵暗号の強さなど安全性確保を勘案した有効期限が設定される。この有効期限を超えた証明書は信頼できない（公開鍵とエンティティー情報の対応付けが正しくない）とみなされる。

有効期限内の証明書であっても、その証明書（の公開鍵）に対応する秘密鍵の内容が露見したり、証明書の所有者の身分が変更となったりした場合には、その証明書は発行したCAによって廃棄されなければならない。原則として廃棄は所有者の要求に基づいてCAの責任で行われる。証明書の廃棄情報はCAから利用者に通知される。

PKIの機能

PKIとは、公開鍵暗号に基づくセキュリティー技術を広範囲に利用するために必要とされるサービスを提供するインフラである。その基本機能は、電子証明書の形態で、PKIに参加するエンドエンティティーの公開鍵を配布して利用可能とすることである。その証明書（の公開鍵）によりエンドエンティティー同士は公開鍵暗号によりもたらされるセキュリティー機能を実現することが可能となる。その環境を実現して維持するための各種サービス・管理機能、たとえば証明書の信頼を維持し、有効期限や廃棄処理を行うこともPKIの一部である。具体的なPKIサービスには左表のようなものがある。これらは必須項目ではなく、これに限られることもない。実装形態もさまざまである。

CAという言葉は、単にPKIサービスの1つを表す場合と、証明書管理、鍵管理といったPKIサービスを実施する実体を表す場合がある。PKI運用コスト削減のため、CA機能のうちエンティティーの登録や証明書管理の一部機能を実体としてのCAから分離して利用者の近くで代行する機関をRA（Registration Authority）と呼ぶ。RAはPKI構成要素の一部である。ほかに証明書リポジトリー（保管庫）なども具体的構成要素の1つである。

PKIの用途とアプリケーション

PKIはインフラとして、上で述べたサービスを提供するもので、実際にセキュリティー機能を実現するアプリケーションはPKIサービスの一部ではない。エンドユーザーが直接的にPKIサービスを利用する以外にも、たとえばSSLや、VPN機能の標準であるIPsecといったアプリケーションを利用する際に、ユーザーが意識することなくPKIサービスが提供されることもある。また、利用者自身がより安全性の高いアプリケーションを開発することや、PKIへの参加を前提に複数のアプリケーションの個別の認証を省略するシングルサインオンの機能もPKI利用の有効な例として期待される。ダウンロードプログラムやファイルへの署名添付技術も利用が始まっているが、このアプローチを大規模ユーザーに展開するためにはPKIの利用が最適である。

▼

SSL（エス・エス・エル／Secure Sockets Layer）：ブラウザーやサーバー間で安全にデータをやり取りするためのプロトコル。米ネットスケープ社が開発し、マイクロソフトなどが採用している。認証と暗号の機能を持ち、ブラウザーとサーバーの間でお互いを確認したり、やり取りするデータを暗号化したりする機能を持つ。

PKIのセキュリティー

PKIはセキュリティー実装に必要なサービスを提供するインフラであって、直接的に安全な環境をエンドユーザーに提供するものではなく、PKIへの参加が即セキュリティーの向上をもたらすわけではない。不完全なPKIサービスの利用や誤ったPKIサービスの利用は、かえってセキュリティー上の脅威を増大させかねない。

また、PKIがインフラとして、セキュリティー環境構築の基礎となる以上、不十分なPKIポリシーの設計やPKI運用の不備は深刻なセキュリティーホールとなりえる。注意深い設計と運用、不断の状況監視と内容の改善がセキュリティー維持の必須要件である。

公開鍵のセキュリティー機能の源は秘密鍵の秘密性にある。PKIを整備して確固としたセキュリティーアプリケーションを構築した場合でも、秘密鍵の管理がおろそかで、たとえば固定パスワードで守るなどの方策にとどまれば、システム全体としてのセキュリティーは固定パスワードのレベルまで低下する。

PKIの標準化と法整備の状況

PKIの標準化は相互運用確保の点からも大変重要であり、国際標準化組織や各種業界において積極的に進められている。PKI関連標準は大きく2つに分類することができる。PKIの内容そのものを定義するものと、PKIを前提に、ユーザーレベルでの利用方法を定めるものである（右表）。

2000年5月には「電子署名及び認証業務に関する法律」が公布され、2001年4月の施行が予定されている。この法律により、電子証明に対する法律上の取り扱いが明確となる。法的に根拠を持って流通する電子署名（証明書など）を認証する機関の認定制度が規定されることにより、電子商取引などが依るべき根拠が整備され、いっそうの進展が期待できると考えられている。

また、1999年11月の総理大臣決定で、「ミレニアム・プロジェクト」の情報化関連プロジェクトの1つとして「電子政府の実現」が挙げられ、2003年の実現を目指して各省庁によるCAの構築、またそれらCA間の相互認証を仲介するブリッジCAの構築が開始されようとしている。

こうした、公的機関から連なる認証のチェーンが法的根拠を持って整備されることにより、各企業やその他の組織においても、PKIの整備が推進されると考えられる。

【標準化が終了、あるいは採用が可能なもの】
- ITU-T X.509（ISO/IEC9594-8）
  証明書、証明書廃棄リスト（CRL）のデータ構造。
- ITU-T X.500（ISO/IEC9594）
  ディレクトリーアクセスサービスの規約。X.509V1とV2では必須。V3からは他の選択可。
- IETF PKIX
  一連のPKI関連技術仕様RFC。主なものとして、X.509PKIXロードマップ、X.509PKI証明書とCRLプロファイル（RFC2459）、X.509PKI証明書ポリシーと認証プラクティスフレームワーク（RFC2527）、X.509PKIオンライン証明書状態プロトコルOCSP（RFC2560）などがある。
- IETF LDAP
  ディレクトリーアクセスプロコトル。
- ANSI X9.X
  ANSIでの金融関連標準。PKIに関連して、暗号アルゴリズム（X9.30、9.31）、証明書とCRL（X9.55）、証明書管理（X9.57）などがある。
- その他の業界標準（よく参照されるもの）
  RSA社PKCS。暗号メッセージシンタックス（PKCS#7）、証明書要求シンタックス（PKCS#10）などが良く参照される。ベリサイン社CPS。

【PKIの利用標準】
- SSL/TLS（IETF）
  ウェブアクセス、クライアント・サーバー通信。
- IETF IPsec
  一連のIP暗号化RFC（RFC2401、2402、2406、2409など）。VPNの基本プロトコル。
- IETF S/MIME
  一連のセキュアメッセージングRFC（RFC2311、2312、2633、2632など）。

【その他PKIに関連する規約、標準】
- IETF SPKI：X509にかわる小型証明書を規定。
- WAP・WTLS：ワイヤレスアプリケーションの標準。セキュリティー通信としてSSLをベースにしたWTLSを策定。証明書としてX509の他にWTLS証明書を採用。
- SET：セキュアなクレジットカードトランザクションの規約。一部はPKI標準を採用。証明書チェーンの圧縮。
- XML：W3Cコンソーシアムが規定するテキスト記述言語。署名などのセキュリティー機能も盛込んでいる。証明書としてX509をラップしたものやSPKIの形式を採用。
- PGP：PKIとは違う信頼モデル、証明書形式。

PKIの標準化状況

ミレニアム・プロジェクト：1999年12月19日に内閣総理大臣決定として発表された、今後日本政府として取り組むべきプロジェクトの総称。事業内容としては、教育の情報化、電子政府の実現、超高速インターネットの推進などが挙げられている。 www.kantei.go.jp/jp/mille/

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp