認証の基礎

田中美里，牧野浩之
Misato TANAKA，Hiroyuki MAKINO

1　はじめに

認証（Authentication）とは，対象となる何かが真正であることを証明する行為のことを言う．

近年インターネットの発達により，ネット上における情報交換，商取引は日常的なものとなった．しかしネット上では相手の顔が見えず，他人への偽装が容易に行える．従って，通信している相手が本人であるかどうか，または送られてきたデータが真に本人のものであるのか確認しなければならない．

本報告では基礎的な認証の知識から，公開鍵暗号方式，ディジタル署名，そして現代の認証システムを支える公開鍵インフラ（Public Key Infrastructure：PKI）の構成について述べる．また，発展的な認証技術としてシングルサインオン（SingleSign-On：SSO）についても簡単に触れる．

2　認証の基礎

2.1　電子認証

コンピュータシステムにおける認証は，ユーザ，サービス，およびパケットが正規のものであるかどうかの真正性の確認を意味する．その中でもユーザやサービスなど，データの送受信相手を確認するものを本人認証（相手認証）．パケットなどデータの改竄の有無を問うものをメッセージ認証と呼ぶ．

従来の本人認証では，パスワードが利用されていた．パスワード認証には，以下のような手法がある．

- 固定式パスワード認証
  最も古典的な認証方式．ユーザ ID とそれに対応するパスワードを入力させ，本人であるか否か認証する．
- チャレンジレスポンス認証
  使い捨ての乱数であるチャレンジコードを生成し，それとパスワードを元に求めたハッシュ値を比較して認証する．
- ワンタイムパスワード認証
  使い捨てのパスワードを専用装置などで自動生成し，毎回異なるパスワードで認証を行う．

メッセージ認証においては，共通鍵暗号方式が利用されてきた．共通鍵暗号方式とは，暗号化，復号化に必要な記号列である鍵が，受信者，送信者ともに同じものを使う暗号方式である．

一方，暗号化と復号化で異なる鍵を用いる方式を公開鍵暗号方式といい，現在ではこの方式による認証が主流となっている．しかし，全ての状況において公開鍵暗号方式が利用されているわけではない．上記のパスワード認証や共通鍵暗号方式を使用する方が，適切なケースもある．

2.2　公開鍵暗号方式

公開鍵暗号方式では公開鍵と秘密鍵という 2 つの異なる鍵をセットとして用いる．

公開鍵は多数の通信相手に配布され，もう一方は秘密鍵として漏洩することの無いよう厳重に管理される．公開鍵によって暗号化されたデータは，対となる秘密鍵でしか復号できず，また秘密鍵によって暗号化されたデータは対応する公開鍵でしか復号できないという特性を持つ．

2.3　ディジタル署名

電子データに付加され，サインや印の役割を果たすものを電子署名という．その中でも特に公開鍵暗号方式を利用したものをディジタル署名と呼ぶ．1995 年に施行された「電子署名及び認証業務に関する法律」[1)] では，公開鍵暗号方式のアルゴリズムである RSA などを用いたディジタル署名に法的効力があることが認められている．

以下にディジタル署名の流れを示す．

1. 送信者は平文メッセージをハッシュ化して作成したメッセージダイジェストを，自身の秘密鍵で暗号化する．
2. 送信者は，暗号化したメッセージダイジェストをディジタル署名として，メッセージと共に送る．
3. 受信者は送信者からのメッセージを基に，メッセージダイジェストを作成する．
4. 受信者は送信者の公開鍵を取得し，ディジタル署名を復号して受信メッセージから作成したメッセージダイジェストと比較する．

以上の流れでメッセージダイジェストが一致していれば，データが改竄されていないこと，また，メッセージが送信者本人のものであると認証される．

3　公開鍵インフラ（PKI）

3.1　公開鍵の問題

暗号化技術は通信の安全性と秘匿性を保ち，認証にも不可欠な技術である．公開鍵暗号方式はその中でも特に安全性が高いとされているが，このアルゴリズムだけでは運用上，問題がある．

公開鍵暗号方式において秘密鍵は厳重に管理される．しかし万が一流出した場合，第三者がその秘密鍵を悪用して正当な送信者になりすまし，悪質なソフトウェアなどをインストールさせて個人情報などを盗み出してしまう危険性がある．また，電子メールに付加するディジタ

ル署名に，別のユーザのものと見なされる署名を利用するなど，公開鍵を悪意を以って利用することも可能である．そのため，受け取った公開鍵が正当な送信者からの有効な公開鍵であるかを検証する必要がある．この公開鍵の安全な配布と真正性の確保をするために作られた仕組みが**公開鍵インフラ（PKI）**である．

3.2　PKI の仕組み

PKI の基本的な仕組みは，公開鍵が正当な送信者のものであることを保証する公開鍵証明書（ディジタル証明書）を，第三者機関である認証局 (Certificate Authority : CA) が発行するというものである．Fig. 1 に PKI の利用の流れを示す．

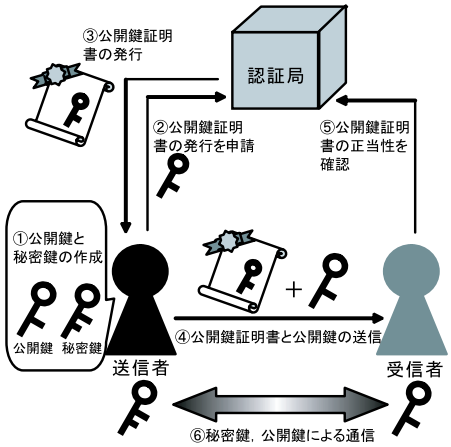

Fig.1　PKI の利用の流れ（出典：自作）

公開鍵証明書は，送られて来た公開鍵の正当性を保証するものである．公開鍵証明書そのものの正当性については，認証局の電子署名を使って確認する．公開鍵証明書では，署名前証明書にディジタル署名が付加されており，署名前証明書のメッセージダイジェストとディジタル署名を比較することによって証明書の正当性を判断している．

この公開鍵証明書を利用したプロトコルには SSL（Secure Sockets Layer）や，S/MIME (Secure/Multipurpose Internet Mail Extensions）などが挙げられる．SSL は公開鍵によってサーバの認証を行い，その後公開鍵によって配布した共通鍵を利用して，通信回路を暗号化するというセキュリティプロトコルである．S/MIME は電子メールへのディジタル署名と暗号化を行う．

3.3　ルート認証局

認証局は公開鍵証明書の送付にも，やはり公開鍵暗号方式を用いている．そのために認証局の公開鍵の正当性をさらに証明する必要がある．認証局の証明を行うための手法には，以下の 2 つがある．

1. 公開鍵を配布した認証局自身が証明書を発行する
2. さらに上位の認証局が存在し，その認証局が公開鍵証明書を発行する

2 の場合でもその発行先を辿ると，1 の方式で証明書を発行した認証局が存在する．このような認証局を**ルート認証局**[2] という．個々のユーザが互いに異なる認証局に属していても，その認証局が同一のルート認証局を持つならば，ユーザ間にも信頼関係が成立するとされる．Fig. 2 に示すような PKI の階層構造によって，多数のユーザ間における公開鍵暗号方式による通信が可能となる．

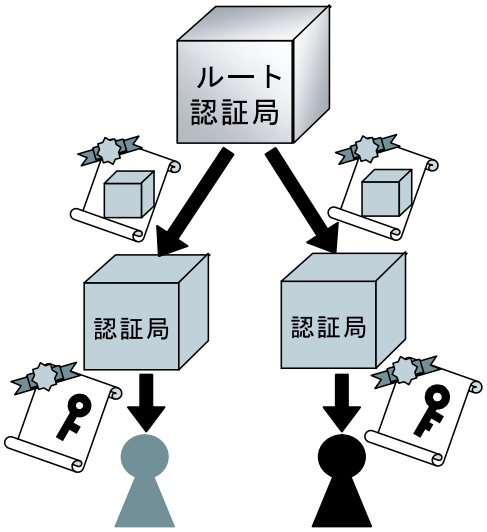

Fig.2　PKI の階層構造（出典：自作）

3.4　PKI の導入

PKI を利用したサービスを提供するには，自身でルート認証局を立てるか，もしくは上位の認証局からの認証が必要となる．前者の場合，信用ある機関からの認証，即ちディジタル署名がないため，主にプライベートなネットワークで利用される．特に企業が社内文書などを対象として，社内でのみ有効な認証局を構築するというパターンが多い．

PKI の導入には，認証局，証明書リポジトリ，公開鍵証明書などの幾つかの構成要素が必要となる．公開鍵証明書を発行する認証局は，PKI システムに 1 つ存在する．しかし，大規模な PKI システムを運営する場合，証明書の発行や再発行，ハードウェアトークンの配布などの作業のために登録局（Registration Authority : RA）が複数用意される．また，証明書データベースや失効した公開鍵証明書のリスト（Certificate Revocation List : CRL）を格納するリポジトリも用意される．CRL には秘密鍵の流出や証明書の期限切れなどで，失効した公開鍵証明書のシリアル番号が記載されている．公開鍵証明書の受信者は，リポジトリにアクセスして証明書と CRL の情報をつき合わせ，その正当性を検証する．

4　シングルサインオン（SSO）

SSO とは一回のユーザ認証によって，許可された複数のシステムへのアクセスについても認証する技術のことである．

4.1　Cookie

SSO の利便性が特に発揮される場が，Web システムにおける認証である．Web はステートレスな通信形態を持ち，その簡便さによってインターネットにおいて爆発的に普及した．しかし，以前の状態が保存されないため，同じサーバ内のデータにアクセスするにもその都度，認証が必要であった．

これを解決したのが，Cookie（HTTP Cookie）である．これは Web サーバが発行し，ユーザのマシンに保存される認証データである．ブラウザは Cookie のデータを他のページや他の Web サーバーへ送ることで，異なるページ間でも情報を共有することができる．しかし，Cookie には異なるドメインとの互換性はなく，またセキュリティ上の脆弱性も抱えている．

4.2　OpenID

4.2.1　概要

Cookie によって同一ドメイン間での認証を繰り返す必要性はなくなった．現在では，各サイトの認証を統一し，1 つの ID，パスワードでより多くのサイトへのアクセスができる ID 統合化への流れが加速している．

その代表的な技術が OpenID[3] である．OpenID とは個々のユーザに与えられた認証用の URL 値のことを指す．コンシューマ（Consumer）と呼ばれる OpenID 対応サイトで一度ログインしたユーザの情報は，OpenID 認証サーバに保持され，ユーザが他のコンシューマにアクセスした際も，認証を行うことなくそのサービスにログインすることができる．

4.2.2　実装

OpenID を利用するには，OpenID として用いる URL とコンシューマ，そして認証サーバに対し，それぞれ OpenID の規格に対応した実装を行う必要がある．

OpenID として用いる URL に対しては，この URL に置いた HTML ファイルのヘッダに認証サーバへのリンクを張る．

```
% <link rel="openid.server"
href="認証サーバ URL">
```

また，ユーザが OpenID として利用している URL とは異なる ID で認証サーバにアクセスする場合は，以下のタグを link タグの後ろに追加する．

```
% <link rel="openid.delegate"
href="サーバにアクセスする OpenID の URL">
```

delegate 指定によって，認証サーバにアクセスする OpenID とは異なる OpenID を，コンシューマに入力することができる．次に認証サーバとコンシューマであるが，これらの実装には OpenID 公式サイト上で提供されている API，プラグインなどが無償で利用できる．

4.2.3　日本における今後の展望

OpenID の規格は既に，Windows Vista の ID 管理機構 CardSpace と統合されている．従って CardSpace に対応したサービスが増加すれば，その影響によって，一般ユーザにおける OpenID の認知度も向上するものと考えられる．しかし，そこで OpenID 自体が多数の一般ユーザを獲得できるかは，OpenID を利用するサービスの成熟具合に依存すると考えられる．現在，OpenID に対応した日本語のサービスは非常に少ない．従って，OpenID を取得したものの，利用する機会がないといった事態が起きている．ユーザの獲得にはまず，日本語対応のコンシューマを増やさなければならない．

しかし，OpenID によって多数のアカウントを管理するユーザ側の利便性が明らかに向上するの比べ，サービス側が受ける恩恵はアカウント管理の負担が減る程度と少ない．既に多数のユーザを獲得している既存のサービスにとって，OpenID の魅力は弱いだろう．

また，このシステムにおいては，ユーザがパスワードを入力して認証を行うのは認証サーバに対してであり，コンシューマは認証サーバから認証の成否を受け取る，または個人情報をやりとりすることになる．よって，認証サーバの運用は信頼性を以って行われなければならないが，OpenID の仕様においてコンシューマと認証サーバの間には，事前に定義された信頼関係はなく，OpenID 認証サーバの信頼性の評価基準も存在しない．これらの事実は OpenID のセキュリティ上の問題として指摘されている．実際，現在コンシューマとして存在するのはニュースサイトやブログなどのライトなサービスが多く，強固なセキュリティを必要とする場面では OpenID は利用されていない．

日本のサービスにおいて OpenID が普及するかは，OpenID の抱えるセキュリティ問題がどこまで改善されるかに依ると考えられる．Microsoft や AOL（America Online），Verisign などが OpenID へのサポートを表明しており，今後の開発と大規模なプロモーション活動が期待される．

参考文献

1）日本情報処理開発協会: 電子署名及び認証業務に関する法律の施行状況等について
http://www.jipdec.jp/esac/promotion/pdf/18_01.pdf

2）電子証明書と認証局
http://www.atmarkit.co.jp/fnetwork/rensai/pki02/pki01.html

3）OpenID.ne.jp
http://www.openid.ne.jp/

4）OpenID
http://openid.net/