暗号化と認証の技術

1.セキュリティに関する問題点

インターネットのようなオープンなネットワークに住みついている人々とって、セキュリティーは治安が良く住み心地の良い社会を作るための社会資本といえる。セキュリティーは水のようなもので、普段からそれの恩恵を受けている人達にとってその存在は当たり前であり、忘れがちであるが、たまに使用できなくなったりすると大変な不安や不自由を感じる。簡単に手に入れたり使用することができない場合は、それを補うために直接的、間接的に多くのコストがかかる。

インターネットの中で、セキュリティについてどのような問題があるのか整理してみよう。インターネットのセキュリティの問題点はおおよそ以下の5つに大別できる。

・インターネットを情報伝達路だと考えると
　(1)「盗み見」と(2)「改ざん」
・インターネットを他人とのコミュニケーションの道具だと考えると
　(3)「なりすまし」、(4)「しらばくれ」
・インターネットとつながっているコンピュータをわが家、インターネットを野外と考えると、
　(5)「侵入」

という問題である。

「盗み見」はインターネットを利用している特定の二者間の情報のやりとりを、第三者が知る問題である。インターネットは世界中に網のように張り巡らされているので、データが届くまで途中の回線やルーター上で簡単に特定の通信内容を盗み見ることができる。誰が見ているか分からない状況下では契約書や請求書など、機密性が高い情報は流せない。

「改ざん」はインターネットを利用してやりとりされている特定の二者間の情報が、発信者から受信者に送られる途中で第三者によって変更を加えられる問題である。「盗み見」と同じように、データが届くまでの途中で比較的簡単にデータを書き換えられる。契約書や請求書のやりとり、株式の売買などには「改ざん」を防止する必要がある。「なりすまし」は、AさんはBさんと情報のやりとりしていると思っているが、実のBさんのふりをしたCさんだった、という問題である。

「なりすまし」は、実際に会って話しをしたり電話を利用する場合には難しいが、インターネットの場合は相手の姿や声などを確認できないので簡単に他人を装うことができる。

オンラインショッピングやインターネット上の各種サービスを利用する場合、今通信しているのが正しい相手であることを確認できなくてはならない。

「しらばくれ」は、AさんがBさんに対して何か約束事をしたが、後になってAさんがそんなことはしていないと言い張り、自分の過去の行為を認めないという

問題である。インターネットショッピングなどで人に物を販売する時には、相手が購入することに同意したという事実を証明できる必要がある。

「侵入」は、インターネットを通じて他人に自分のオフィスやコンピュータを不正にアクセスされるという問題である。大切な情報を見られたり、悪意をもってコンピュータに破壊行為を加えることが考えられる。

2.技術面での対応策

セキュリティに関する問題点には、技術的な解決方法が存在する。

「盗み見」には送り手と受け手の二者のみが知る暗号鍵を使用し、インターネット上を通過する情報を暗号化することで防ぐことができる（図1）。暗号鍵を持っている者だけが情報を復号化できるので、第三者は「盗み見」できない。

「改ざん」には電子印鑑という技術を用いる。電子印鑑は暗号化時に使用する鍵と、復号化時に使用する鍵がペアになった公開鍵暗号方式*の技術である。送り手はまず一方向ハッシュ関数*を使用して、ダイジェストと呼ばれる元データの中の特徴データを計算する。そのダイジェストを自分の秘密鍵で暗号化し、元データとともに受け手に送る。受け手は同じ一方向ハッシュ関数を使用して受けとった元データのダイジェストを算出し、それが元データとともに受けとったダ

公開鍵暗号方式
秘密鍵と公開鍵の2つのデータ暗号鍵を利用する暗号化の1手法。公開鍵の所有者に対して誰でもがメッセージを暗号化して送信できるが、その所有者だけが自分の秘密鍵を使ってメッセージを解読できる。RSAなどがこの方式にあたる。

一方向ハッシュ関数
メッセージからそのダイジェストを作成するために用いられる関数で、1文字だけしか違わないメッセージでもハッシュ値が大きく異なるような特徴のあるものが使われる。

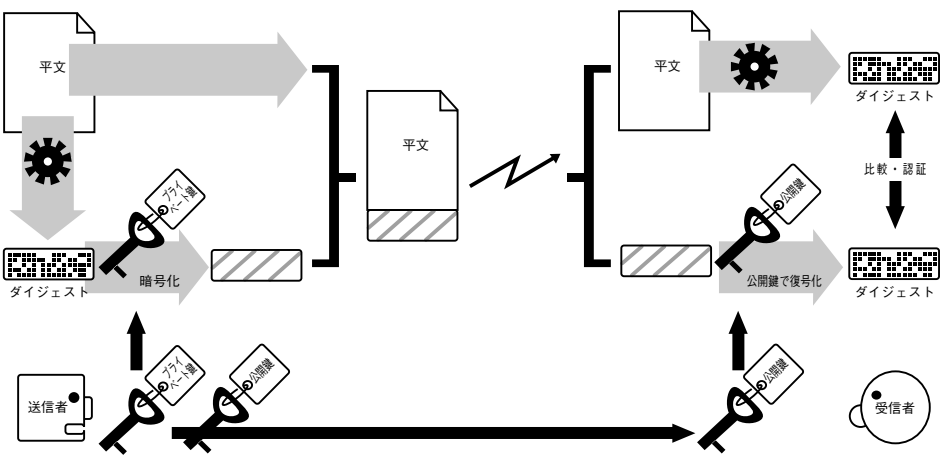

図1 デジタル認証の仕組み

(1) 送信者はメッセージの特徴を表すような短いデータ（ダイジェスト）を作成し、そのデータだけ暗号化してメッセージ本体と一緒に送る。
(2) このとき送信者の公開鍵も一緒に送信する。
(3) ダイジェストの暗号文とメッセージ本体を受け取った受信者は、送信者の公開鍵を使用してダイジェストを復号化する。
(4) そのダイジェストと自分で求めたダイジェストを比較し、同じなら暗号化されてきたダイジェストが正しい、つまり、確かに送信者が作成したものであることがわかる。また、そのメッセージが途中で改竄されていないことも証明できる。

イジェストを送り手の公開鍵で復号化したものと同じになるかどうか調べる。もし同じになれば改ざんされていないことが証明される。送り手の公開鍵で復号化できるデータは送り手の秘密鍵で暗号化されたものだけなので、そのデータ全体が作成されたままの姿であり、誰も手を加えていないことを証明できる。

「なりすまし」と「しらばくれ」は一緒に解決できる。両方とも、データの送り手がどこの誰であるかを確認できれば防ぐことができる。送り手を確認するには、送られたデータの中に送り手にしか作成できない部分が含まれていればよい。そのために、前述の電子印鑑の技術とともに電子印鑑証明書を使用する。電子印鑑証明書とは公開鍵とその持ち主の関係を証明するものである。この公開鍵の持ち主はどこの誰かということが記述されており、信頼のおける機関が電子印鑑を捺印して発行する。受け手はデータ中の電子印鑑部分を確認し、使用された鍵から持ち主を特定することで「なりすまし」を防止するわけである。同様に相手を確認することによって「しらばくれ」も防止できる。

「侵入」は、基本的には相手を確認することと「盗み見」を防止することで解決できる。自分のコンピュータへアクセスしてくる人に対し、電子印鑑などの技術で誰であるかを確認し、正しい相手の場合だけ「盗み見」を防止しながらアクセスを許せばよい。

インターネットを低コストで利用するにはリスクを軽減する必要があり、そのための基盤技術の1つが情報セキュリティー技術である。特に意識することなく誰もがこのような技術を利用するようになるのが理想である。

（浅田一憲）

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

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、データ、URL、名称など）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・図の作成者、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掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したり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される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期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。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp