インターネットことはじめ

協力:株式会社日本レジストリサービス(JPRS)

1 インターネットと暗号

暗号というとなにやら難しそうですが、実はたいていの人が意識すること無く、インターネットにおいて暗号を使っています。安全な通信を行うSSL/TLSはショッピングサイトや金融サイトの利用には欠かせませんし、近年では、Webの通信をすべてTLSで暗号化することが、世界的な流れになっています。

また、DNSにも暗号が使われています。DNSSECではDNS応答を検証する電子署名に暗号の技術が使われており、DNSの通信を暗号化するDoT(DNS over TLS)やDoH(DNS over HTTPS)も、普及してきています。

2 SSL/TLSの普及

一般的な暗号は、紀元前からの歴史があります。ただ、インターネットにおいては当初学術ネットワークであって用途が限られていたこともあり、暗号通信による情報の秘匿についてはさほど考慮されませんでした。しかし、インターネットが商用化され、ショッピングサイトなどが登場すると、クレジットカード番号など第三者に知られては困る情報をやりとりする必要が出てきました。

こうした、第三者に知られては困る情報を安全にやりとりするため、1994年にNetscape社がSSL(Secure Socket Layer)を開発し、同社のWebブラウザであるNetscape Navigator 1.1に採用しました。これによって、それと意識されないまま、暗号はインターネットに普及することになりました。なお、SSLはプロトコルの改良と脆弱性の修正を経て、2021年現在ではTLS1.3となっています。

3 ファイルの暗号化

SSL/TLSは通信を暗号化するものですが、記録するデータそのものを暗号化するアプローチも存在します。古典的にはUnixのcryptコマンドがあり、これは1979年にリリースされたSeventh Edition Unixに含まれていたほど古い物です。現在ではパスワード付きzipファイルという形でお馴染みかもしれません。また、個々のファイルでは無く、記録装置全体を暗号化することもあります。

前述したcryptコマンドや暗号化zipでは共通鍵暗号という、情報の暗号化と復号に共通の鍵を用いる暗号方式が使われます。共通鍵暗号に使われる手順(アルゴリズム)の例として、DES(Data Encryption Standard)やAES(Advanced Encryption Standard)が挙げられます。

共通鍵暗号では、暗号化と復号に同じ鍵を使います。そのため、情報交換をする相手と事前に安全な方法で鍵を共有し、管理する必要があります。共通鍵が第三者に漏れると、データの秘匿性が保てなくなります。そのため、せっかく暗号化しても、鍵を平文のまま、暗号化されていないメールで送ったのでは、簡単に解読されてしまうことになります。

4 公開鍵暗号

この問題を解決したのが、公開鍵暗号です。これは暗号化と復号で、異なる鍵を使う方法です。データの作成者は暗号化のための公開鍵を外部に公開し、復号のための秘密鍵を外部に漏れないよう、厳重に管理します。秘密鍵を持たない第三者は公開鍵で暗号化したデータを入手しても復号できないため、データの秘匿性が保たれます。

有名な公開鍵暗号として、Ronald Rivest、Adi Shamir、Leonard Adlemanの3人が開発した、RSA暗号が挙げられます。RSA暗号は3人の頭文字にちなんで名付けられ、1977年に初版が公開されました。

公開鍵暗号の技術は、データの作成者を証明する電子署名にも使われます。電子署名では、データの送信者が自身の秘密鍵でデータを署名し、受信者が対応する公開鍵で署名を検証します。公開鍵で署名を検証できた場合、そのデータは秘密鍵を保有する送信者が作成したものであると証明できます。

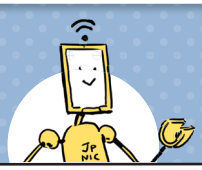
SSL/TLSでは証明書の検証と以降の通信に使う共通鍵の伝達に公開鍵暗号を用い、実際の通信には共通鍵を用いることで、通信相手の認証とデータの暗号化を実現しています。利用者が直接使える公開鍵暗号を用いたソフトウェアとして、1991年にPhilip Zimmermann氏が初版を公開したPGP、GNUプロジェクトにより開発されたPGPの実装であるGnuPG、SSL/TLSのプロトコルを実装したOpenSSLなどが挙げられます。

5 暗号の危殆(きたい)化

多くの暗号の安全性は、「計算量的安全性」に基づいています。計算量的安全性とは、暗号解読に必要な計算量に着目した、暗号の安全性に関する考え方です。具体的には、暗号を解読するために必要な計算量が安全性を保ちたい期間内では解読可能にならない場合、その暗号は計算量的に安全であるとするものです。

計算量的安全性は、新しい解読方法が発見されて必要な計算量が減少したり、新型の計算機が登場して解読に利用可能な計算能力が増大したりすることで低下します。もし、安全性を保ちたい期間内に暗号が解読可能になってしまうと、その暗号は安全ではなくなります。これを、「暗号の危殆化」と言います。

危殆化を回避する方法として、使用する鍵の長さを十分に長くする、暗号のアルゴリズムをより安全なものに変更するといった項目が挙げられます。このように、暗号による安全の確保にも他の技術と同様、常にアップデートが必要になります。



次回は「画像フォーマット」を取り上げる予定です。

「インターネット歴史年表」も見てね!!
https://www.nic.ad.jp/timeline/