（1） PKI について

前回まで、暗号技術について紹介をしてきました。そもそも、暗号技術が注目されてきた背景には、インターネットの爆発的な普及がありました。当初は商用の利用は制限されていたインターネットですが、そこは利用者のニーズには勝てず、インターネット上での商取引の要求は強く、多くの人たちがその利便性に期待を寄せました。しかし、その利便性を悪用する人たちがいるのが世の常です。そのような悪用から商取引の安全を確保するために注目されたのが暗号技術というわけです。その中でもとりわけ、公開鍵暗号技術は、共通鍵暗号の鍵交換の安全性確保、成りすまし・不正アクセスの防止、改ざん防止などインターネット上での商取引のセキュリティを確保するために必要な機能をもっていることは前回までに説明をしてきました。ただ、技術だけがあればいいというものではなく、成りすまし・不正アクセスの防止に必要な、「その人であることの証明」ということに関しては、信頼のおける第三者による証明が必要になるということもご理解いただけたと思います。

つまり、暗号技術とそれを活かすためのインフラ（社会的な基盤）が必要というわけです。この公開鍵暗号機能を活用するためのインフラのことを PKI（パブリック・キー・インフラストラクチャー）と呼びます。この PKI、具体的には「認証局　英語では CA（Certification Authority）」という信頼できる第三者機関が必要になりますが、端的に言えば、公開鍵証明書を発行するサービスを行う機関ということになります。このようにサービスそのものは比較的単純と言えますが、「信頼できる」ということが非常に重要になってきます。そのためには、まず認証局自身が信頼のできる第三者から証明されていることや、自身が強固なセキュリティを確保していることも重要です。認証局はその親（上位の）の認証局から認証を受けているという具合に階層的になっており、その一番の元の認証局をルート認証局と呼びます。このルート認証局は厳重なセキュリティが確保された運営がなされ、それ自体で自身の信頼度を示すことが必要となります。そのため、証明書発行のサーバーコンピュータは何重にも入室管理のされたサーバールームに設置されているだけでなく、その場所は関係者以外には明かされていません。またその運用管理規定は厳しく監査され認定を受ける必要があります。このルート認証局を認証する元をたどると、政府機関による認証が必要ということになり、我々が日常利用する役所が発行する証明書類と同じように政府機関が大元の証明をしてくれているということがわかると思います。

さて、話が一気に技術的な内容から、社会のしくみのような内容になってしまいましたが、インターネットの利用を安全にするためには、このように技術と社会基盤が重要であるということをご理解いただきたいと思います。

（2） 暗号技術の標準化

さて、社会的なしくみに話が移ってきましたが、暗号技術を円滑に利用するために暗号の標準化という課題があります。なぜ標準化なんでしょうか？そもそも標準化などして、安全性が保てるのでしょうか？という疑問がわいてくる方はセキュリティについてご理解いただいている方だと思います。そもそも解読するためには、どんなアルゴリズムが使われているかわからなければ、鍵が盗まれても大丈夫ではないか？と思われると思います。そのとおりです。しかし、もう一度、暗号技術が使われる背景を思い浮かべて下さい。インターネット上で使われるということです。そして暗号技術は利用者双方が同じアルゴリズムを使わなければ情報の伝達ができません。つまり、不特定の利用者の双方が同じアルゴリズムを使うためには、アルゴリズムそのものは公開されたものでなければ運用できないということになってしまいます。そのため、暗号はアルゴリズムそのものは公開されていても、鍵が盗まれない限りその解読は不可能に近い（数百億年かければ解読できる可能性もあるので不可能とは言いませんが、ビッグバンが今から 137 億年前と言われていますので、解読まで地球そのものが存在しているかも怪しいですが）アルゴリズムを利用するということが必要になります。そのため、専門家がその技術を評価し、その安全性が認定された暗号アルゴリズムを標準暗号とするということが必要です。これは、ISO にて国際的にも標準化されました。日本の暗号技術もいくつか国際標準となっています。

（3） 日本の暗号技術標準化

国際標準は ISO によって策定されましたが、日本においては、日本としての技術政策が実施されています。日本の暗号技術の技術政策を所管しているのは、経済産業省と総務省で、CRYPTREC（Cryptography Research and Evaluation Committees）と呼ばれるプロジェクトが実務を運営しています。この CRYPTREC というプロジェクトは暗号技術の専門家（研究者、関係機関、企業など）が参加し、多方面からかつ深く技術の評価を行っています。

日本における暗号技術は、経済産業省と総務省が上記 CRYPTREC プロジェクトの評価活動の結果を受け、推奨技術のリストという形で発表されました。そのリストが「電子政府推奨暗号リスト」と呼ばれる一覧表です。このリストの中には、公開鍵暗号、共通鍵暗号、

ハッシュ関数、疑似乱数生成技術などが含まれており、前回までの技術説明の中で紹介したものが含まれています。

（4） 暗号の解読について

情報セキュリティの概要の話のなかで、情報セキュリティの「脅威」という言葉が出てきましたが、暗号においてもこの「脅威」に相当するものとして、暗号の解読という問題があります。「解読」というと暗号文を元の日本語の文章にして内容を盗み読むということですが、暗号の研究者や技術者などは、その暗号の鍵を特定あるいは推定するという方法が判明したことを持って、解読とみなします。この場合、暗号文だけでなくそれに対応する平文とのペアを用いて鍵を推定するというような方法が研究されています。解読技術が研究されているということは、悪事を働くためではなく、暗号技術に対する脅威の最先端技術、スキルを知るということにより、より強固な暗号技術を発明する。あるいは、解読の危険が高まった場合、その暗号技術は標準暗号から外し、より強固な暗号技術によって置き換えるという処置がなされる必要があるということを意味しています。先ほど紹介したCRYPTRECプロジェクトでは、このような暗号技術の解読の危険性が高まること（「暗号の危殆化」と表現されます）に対し、安全性評価、解読技術等の監視業務を行っています。

（5） 暗号製品の試験・認証制度

正式には「暗号モジュール試験及び認証制度」と呼び、JCMVP（Japan Cryptographic Validation Program）という略称で呼ばれています。情報処理推進機構（略称IPA）に認証機関が置かれて、運用されている制度です。この認証制度の意義を説明する場合、よく参考として引き合いになるのが、「航空機」です。情報セキュリティの認証制度のなかにも、ISMS（情報セキュリティマネジメントシステム）の認証は情報セキュリティが組織として運用管理されているかを監査するための認証制度ですし、CC（ISO/IEC 15408）と呼ばれる情報セキュリティ製品の評価制度も運用されています。これらとの対比で説明すると、航空システム運営管理がISMS、航空機そのものがCC、航空機のエンジンの安全性がJCMVPに対応すると紹介します。つまり暗号は表面上、その安全性についてユーザから直接は見えませんが、情報セキュリティの観点からはキーとなる重要な部分であることは間違いないので特にそこを取り出して試験・認証を行い、その安全性を確保しようという意図で作られた制度なのです。

このように暗号技術は、その安全性の確保のためにいろいろな施策、制度が実施されており、日々新たに発生する脅威から情報資産を守っています。

さて、情報セキュリティについて、その概要の説明から始まり、暗号技術に関してその技術解説、その技術政策、制度等についてご紹介してきました。次回以降は、情報セキュリティから離れまして、コンピュータのハードウェアについてご紹介してみたいと思います。