CISO STRATEGY

企業のリスクをマネージする戦略考

セキュリティー管理において常に主要な技術だと言われつつも、一部の分野でしか利用されていない暗号技術。電子メールの暗号化はもとより、ファイルの暗号化など、さまざまなアプリケーションは生まれたものの、その普及は一般的になっているとは言いがたい。この問題はどこに原因があるのか。あるいは、暗号化はユーザーが意識すべきものではないのか。

第八回 暗号化は何のためにあるか

text : 山口英 奈良先端科学技術大学院大学情報科学研究科教授

暗号の技術開発は長い歴史がある。もともと軍事技術として生まれたために、その技術そのものを国家が独占する状態が続いてきた。またコンピュータ登場後の暗号技術は、コンピュータによる解読に対抗するために高度に数学に立脚した技術として成長し、第二次世界大戦中まで使われてきた暗号とはまったくレベルの異なる技術を生み出した。とはいえ、国家が暗号技術を独占してきた現状は長い間変わることはなかった。しかし1990年代初頭になると、民間側での暗号技術開発も盛んになり、その結果暗号技術利用についての規制緩和が行われた。民間における暗号利用が比較的自由になり、今や暗号技術を使った数多くのアプリケーションが提供されるようになっている。

暗号は、平文(clear text)を解読困難な暗号文(encrypted text)に変換する処理である。暗号文は変換処理アルゴリズムと変換処理を特徴付ける鍵(key)を知らなければ、元の平文に戻すために膨大な時間が必要となる。

暗号は通信保護に使われるのが一般的である。通信をする二者が暗号に使用する鍵を事前に共有し、通信内容を暗号化する。結果として、第三者による傍受があったとしても内容が漏洩することはない。鍵の共有と秘匿は大きな問題であるが、基本的に別チャンネルでの交換を前提としていれば鍵漏洩の危険性を小さくできる。つまり、実際の通信に使われる通信路とは別に鍵を事前に交換しておく方法を用いる。また、同一の鍵を長期間使うのは暗号解読の可能性を高めるので、定期的に鍵を変更するために、俗にコードブックと呼ばれる鍵表を事前に交換しておいて、その鍵表の中から適当な取り決めによって鍵を決める方法が伝統的に使われている(しかしこの方法には多くの欠陥がある)。

公開鍵暗号という大発明

1970年代になると暗号技術として画期的な方式が開発された。公開鍵暗号である。それまでの暗号は、暗号処理と復号処理で同じ鍵を使うものばかりであり、現在は対称鍵暗号と呼ばれている。これに対して公開鍵暗号は、暗号処理と復号処理で異なる鍵を使えるものである。この方式は、従来の対称鍵暗号と比較すると画期的な環境を提供する。たとえば、私が暗号処理に使用する鍵を公開しておくとしよう。この公開した鍵を入手した誰もが、私だけが復号可能な暗号文を作成できる。公開鍵の安全な公開方式を作り上げてしまえば、鍵交換のオーバーヘッドを激減させられ、かつ、事前に鍵を交換することなく安全に第三者と通信できるのだ。これは対称鍵暗号の持つ性質と大きく異なり、新たな暗号利用の世界を生み出すことになる。

しかし、公開鍵暗号方式は高度に数学的に設計された巧みな方式を使っていることから、換字や転置を何段も組み合わせた対称鍵暗号方式と比較して処理量が大きく、処理速度が遅い。このため、公開鍵暗号と対称鍵暗号を組み合わせたアプリケーションが一般的になっている。すなわち、公開鍵暗号を使って対称鍵暗号で使う鍵を交換し、実際の通信処理には対称鍵暗号を使うというものである。これにより、実時間通信でも暗号処理が可能なシステムを構築できている。

暗号の技術が認証の技術に

公開鍵暗号が開発されて、すぐさま考案されたのが、ユーザー認証に公開鍵暗号を使う方式である。

ユーザー認証とは、ユーザーの素性を検証できる方法で、確実性を持って誰かを示す方法である。実生活の中では、私たちの身元を示す方法として、パスポートのような写真付き身分証明書が使われ、私たち自身の顔つきをチェックする。また、本人しか知らないと思われる情報(たとえば母親の結婚前の苗字)を口頭で確認することも併せて行い、より本人確認を確実にするのである。ところがこのような方法は、ネットワーク環境ではうまく機能しない。ネットワーク環境で使える認証技術は、ネットワーク環境が拡大するにつれて1980年代後半からその必要性が叫ばれてきた。

その中で開発された考え方が、信頼できる第三者によって保証される認証方式である。英語ではTrusted Third-Party Authenticationと言う。いわば電子的に裏書された身分証明書を使う。この方式を標準化したものがX.509 PKI(public key infrastructure)である。

この仕掛けは公開鍵暗号の構造をうまく使ったものだ。まず、公開鍵暗号では、各ユーザーが1組の鍵を使用する。1つを公開鍵として広く公開し、もう1つを秘密鍵として本人以外に漏洩しないように厳重に管理して利用しているとしよう。公開鍵暗号の性質から、公開鍵によって暗号化された情報は秘密鍵によって復号できるが、同様に秘密鍵によって暗号化されたものは、公開鍵によって復号できる。この性質をうまく使って、次のような処理をしたとしよう。

①身分を証明したい人は、事前に決めたバイト列を自分自身の秘密鍵を使って暗号化する。
②作成した暗号文を他の人に送る。
③受信者は送信者の公開鍵を入手し、復号処理を行う。
④復号した結果、事前に決めたバイト列が正しく得られれば、送信者が本人だとわかる。

問題は、入手する公開鍵が本当に本人のものかどうかを確認する手段が提供されていないことである。そこでX.509 PKIでは、各公開鍵について本人確認を厳重に行い、信頼できる第三者が電子署名をすることで、この問題を解決している。X.509 PKIでは、この信頼できる第三者を証明書発行者と呼ぶ。また、第三者によって電子署名のされた公開鍵は、X.509証明書として決められた書式で表現される。

認証できれば電子署名も可能に

公開鍵暗号を使うと、さらに電子署名が可能になる。

電子データとしてLというデータがあるとしよう。入力したデータをあるルールに従って決められた長さのデータに変換する関数(これをセキュアーハッシュ関数という)に、Lを入力してH(L)という値を得る。このH(L)を公開鍵Kpで暗号化したものをE(H(L), Kp)と表現する。

E(H(L), Kp)とLを同時に送信すると、受信者は、秘密鍵KsでE(H(L), Kp)を復号してH(L)を得られ、またLをセキュアーハッシュ関数を使ってH(L)を得られる。この2つのH(L)の値を比べ、同じ値であれば、通信内容が改ざんされていないことがわかる。これが電子署名である。このような電子署名技術もX.509 PKIの中ではうまく使われている。

暗号は使われない!?

ここまで述べてきたように、暗号技術で生み出したものは、(1)データ暗号化、(2)認証、(3)電子署名という3つの重要な機能である。そして、X.509 PKIという標準が生まれたことにより、これらの取り扱いが一本化できている。

また、1990年代に開発された暗号アプリケーションのPGPはオープンソースとして普及し、暗号化・認証・電子署名の機能を提供し、世界中で広く使われている。つまり、現在のところ、X.509 PKIとPGPを利用できる基盤を用意すれば、ユーザーにとって必要なことの大部分は実現できるのだ。

ところが、ユーザーが暗号技術をうまく使ってくれるかというと、中々利用が広がっているとは言いにくい。大部分のユーザーは暗号化機能を積極的に使ったことはなく、どちらかといえばほかのユーザーから「今度送るメールは暗号化してくれ」とか、「電子メールによる書類の提出では、電子署名を必ず添付してくれ」と言われたので仕方なく使っているというのがよくある状況だろう。なぜこのような状況になってしまっているのだろうか。

第一の理由は、現在の暗号利用がadd-onシステムとして作られているからだろう。つまり、暗号を利用するためには、現在使っているシステムに暗号処理用パッケージを後から追加して利用することになる場合が多いのだ。したがって、暗号を使わなければならないと強い意志を持っているユーザー以外は、暗号処理パッケージを追加することに強いインセンティブがない。結果として、暗号処理パッケージすら入れられていないことが多いのだ。とりあえず、自分の周りにいる人たちに「PGPの設定をしている人はどれだけいますか?」「X.509 PKIの有効な証明書を持っている人はいますか?」と聞いてみるのがいいだろう。恐らくほとんどのユーザーは、そんなものを持っていない。

第二の理由は、仮に暗号処理システムが入っていても、それを使わなければならない理由が思いつかないことだろう。なぜ電子メールを暗号化しなければなら

ないのか。なぜWWWアクセスを暗号化しなければならないのか。本当に通信内容を覗き見るようなことが技術的に可能なのか。また、ISPが運営しているインターネットの中で、そんなことがありうるのか。こんな素朴な疑問に対して、正しい理解を与えてないために、インターネットにおける通信の脆弱さに気が付いてないのだ。

インターネット環境を考えると、実際には電子メールの内容は漏れる可能性があり、WWWアクセスは盗聴される可能性がある。また通信路においても漏洩する可能性は0ではない。近年の無線LAN利用の広がりは、その危険性を高めている。さらに実際の情報処理を行うエンドノードでは、その管理がしっかりしてなければ情報が漏洩する可能性は高い。インターネットは、通信システムと情報処理システムの両者から成立しており、特にセキュリティーはエンドノードのセキュリティーに依存しているところがある。このため、インターネットの利用では、情報漏洩の可能性がいたるところにあると思うことが重要だ。

第三として、暗号処理システムの「ボロさ」も大きな理由となっている。確かに暗号処理システムは存在しているが、既存のアプリケーションとのインテグレーションがうまくいっているとは言い難いケースが多い。たとえば、PGPを1つとっても、普段使う電子メールプログラムとうまく統合されて、快適に使えるような環境が提供されている例はほとんどどない。システムとしてのボロさは、利用者が継続的に利用していくうえで大きな障害になっている。だれも使いにくいものを使い続けることはしたくないのだ。

第四に、暗号利用の経験が少ないことから、結果として暗号化以外の認証や電子署名といった便利な機能を使うことまでユーザーは気が付かないことが多いのだ。

このようないくつもの理由が絡み合って、暗号技術の利用は促進されていない。これまで暗号技術を使わなくても何とかなっていたからと言って、これからもそれでいいと考えるのは、セキュリティー管理者としては問題である。そこで今回はいくつかの状況での暗号化処理の効果的な利用を紹介する。

ファイルシステムの暗号化

データ暗号化は、システム内に蓄積されたファイルなどのデータの暗号化で利用するのが一般的である。

データの暗号化を真剣に考えるべきなのは、社員に使わせているノートPCだろう。特に重要なデータを取り扱っていると思われるユーザーのノートPCでは、データ暗号化を真剣に検討すべきだ。ノートPCはユーザーが持ち歩くシステムである。当然、置き忘れや盗難の危険性がある。また、ノートPCは換金性がいいものでもあり、盗難の危険性は高いのだ。

現在では、ファイルシステムに暗号化機能が用意されているものがある。たとえば、ウィンドウズ環境であれば、PGPdiskのような暗号化したファイルシステムを構成するアプリケーションが開発されている。ファイルシステム全体を暗号化し、取り扱うファイルすべてを一括して暗号化して保護するような簡単に使えるシステムを導入するのが、ノートPCの盗難や紛失によるデータ漏洩の防御策だと考える。

もう1つの危険性は、リースあるいはレンタルなどで導入したシステムのディスクにデータが残っているケースである。レンタル期間が終了して、システムを返却するときに、ディスクの内容を完全に消去して返却することがルール化されているのであれば問題はない。しかし、大量導入や大量入れ替えが行われている環境で、データの完全消去の処理は手間がかかることから実際に十分に行われているのだろうか。もしも行われていない環境があるとしたら、データが漏洩する危険性を避けるためにも、ユーザーのデータを蓄積するファイルシステムを暗号化するのは悪くないアイデアだろう。

戦略1 暗号化ファイルシステムの導入は、まずはノートPCのような盗難の可能性があるシステムでの利用を考えるべきだ。さらに、デスクトップシステムでもレンタルやリースで使用しているシステムでは検討するのが望ましい。

電子メールは電子署名から

電子メールでの暗号技術の利用というと、電子メール本文の暗号化を考える人が多いだろう。一対一でメールを交換する場合には暗号化することは簡単である。しかし、複数の受信者がいるような場合やメーリングリストでの暗号化は、技術的にも面倒な処理が必要であったり、機構的に実装が難しかったりする場合が多い。このため、ユーザーに対して暗号化を強要しても実行してくれないことも多いだろう。

現時点で電子メールでの暗号技術利用で最も有効性があると思われるのは、電子署名である。電子メールは、ヘッダーが保護されているわけではないので、発信者を偽ったメールを作ることは簡単である。実際、2003年夏に流行したSoBig.Fウイルスでは、発信者を偽造した電子メールをばら撒くという機能が、ウイルスの伝搬に一役買ったという面が指摘されている。また、電子メールが実際の業務でも広く使われるようになっていることから、発信者を確実に特定することが必要になる場面も多い。このようなことから、まずは電子メールの電子署名から始めるのが暗号技術利用の第一歩として有効だろう。電子署名の利用が一般化すれば、次に電子メールの暗号化のステップに進むのはいつでもできる。

電子メールの電子署名については、PGPでもX.509 PKIを使ったS/MIME

でも可能である。どちらも管理と運用は比較的簡単にできる。もしも企業などで組織的に利用を広げるのであればS/MIMEの利用を促進するほうがトップダウンアプローチを取れるので、導入が比較的簡単だ。一方、小規模な組織や個人で対応しようとするのであれば、PGPの導入が適切だ。

戦略2 電子メールでの暗号技術の利用は、電子署名から進めるのが得策。大規模な組織では、X.509 PKIを使ったS/MIMEの利用から始めるのがいいだろう。PGPは個人や小規模組織での運用に適している。

電子メールのサーバーとの通信にも

電子メールに関係した暗号技術の利用は、メール送信時のSMTPサーバーへの通信の暗号化と認証、POP/IMAPサーバーとの通信における暗号化と認証での利用である。これには、SMTPやPOP/IMAPサーバーでSSLを使って、通信の安全性を高めるのがいい。最近の電子メール関連のサーバーでは、SSLを使った通信路保護の機能が大抵用意されている。また、ユーザーが使用する電子メールリーダーでも、SSLを使った通信保護機能がデフォルトで用意されている。この機能をフルに使うことで、高度に保護された認証も利用可能だ。業務での電子メール利用の広がりの中で、サーバーとの通信を保護することは重要だ。

戦略3 電子メール関連のサーバーとの通信を暗号化する機能を付加しよう。少なくともサーバー側でSSL/TLSを使うだけでも、通信路での情報漏洩を防ぐ強力な対策となる。

WWWでは個人認証に使える

WWWにおける暗号化機能の利用は、サーバー側で提供するサービスでSSL/TLSを用いて通信路暗号化を進めることが第一歩になる。重要な情報をサーバーに対して提供するような部分ではSSL/TLSを使うのが一般的である。しかも、サーバー側だけが対応すればよいので、その意味で、管理者だけがその恩恵を被る。また導入の手間も少ない。

もしも電子メールの電子署名のためにX.509 PKI証明書を各ユーザーに分けているとしたら、その証明書を利用して、クライアント認証を行うこともできる。これにより、単純なパスワードでのページの保護だけではなく、ユーザー本人かどうかを確認することもできる。最近のブラウザーには証明書の利用機能が大抵用意されており、導入の手間は少ない。さらに、証明書の保全にはICカードやUSBメモリーキーなどのデバイスも使えるようになっているものが多く、より強力なシステムを作り上げられる。WWWを用いて重要な情報を社員が共有している環境であれば、導入を検討するのは悪いアイデアではない。

戦略4 WWWを用いて重要な情報を共有する環境を社内的に作っているのであれば、X.509 PKI証明書とSSL/TLSを使ったクライアント認証機能の導入を検討するのが望ましい。

はたして暗号化は福音なのか？

暗号技術を情報システムのセキュリティー管理で効果的に使うと、取り扱いが厄介な種々の問題が数多く解決するのは事実だ。だからと言って暗号技術だけで問題が解決するわけではない。

暗号技術利用の要は、暗号鍵の管理をどのように行うかに尽きる。最近の暗号システムでは、暗号鍵は人間が扱えない巨大数であることが多い。このため、暗号鍵を保管するセキュリティーデバイスを用いて管理する。このセキュリティーデバイスに対するアクセスはパスワードで行われているものも多い。また、USBキーやICカードの場合には、媒体そのものの管理を適正に行わなければ意味がない。このためには、新たに注意深くセキュリティーポリシーの改訂とルール作りが必要である。

また、なぜ暗号化をしなければならないかについてのユーザーの教育も必要である。暗号化が必要な情報を取り扱っていることに対する認識を持たせ、インターネット環境における情報漏洩の危険性に対する正しい理解を持たせる。さらに、ユーザーに暗号機能を使え使えと強要するばかりではなく、なぜ使わなければならないのかという点について、十分な理解を与えることが必要である。正しく理解しているユーザーは、セキュリティー管理の面でも力になる存在である。ユーザーが能動的に管理に協力することになれば、それは大きな力になるはずだ。暗号化については、まだまだ一般ユーザーの認知度は低い。その底上げを進めると共に、どのように暗号技術を使えばいいのかを追究することが必要だろう。

［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