

第二回：マインドマップで学ぶ、技術者のための システムセキュリティ対策入門

梅原 伸行¹

前回は、セキュリティ対策の全体像を示すと共に、「システムセキュリティ対策」の位置づけについて述べました。今回は、「情報資産」²を蝕む「脅威」³のうち、「盗聴」に対するシステムセキュリティ対策のポイントを取り上げたいと思います。

一般に「盗聴」というと、「盗聴器を設置する」あるいは「通信を傍受する」といったプロフェッショナルなスパイ活動を連想するかもしれませんが、主にインターネットで情報交換を行っている今日、「盗聴」⁴の敷居はむしろ素人レベルまで低くなっているといえます。

その理由の一つとして、通常のインターネット(IPv4)⁵では、データを秘匿する機能が標準装備されていないということがあります。

インターネット上を流れるメッセージは、例えていうなら「はがき」に書いた文章のようなもので、内容を覗こうと思えば覗ける仕組みとなっています。普段、メールソフトやWebブラウザを使用しているとあまり気にすることはないかもしれませんが、メールでやり取りする機密情報も、Webで入

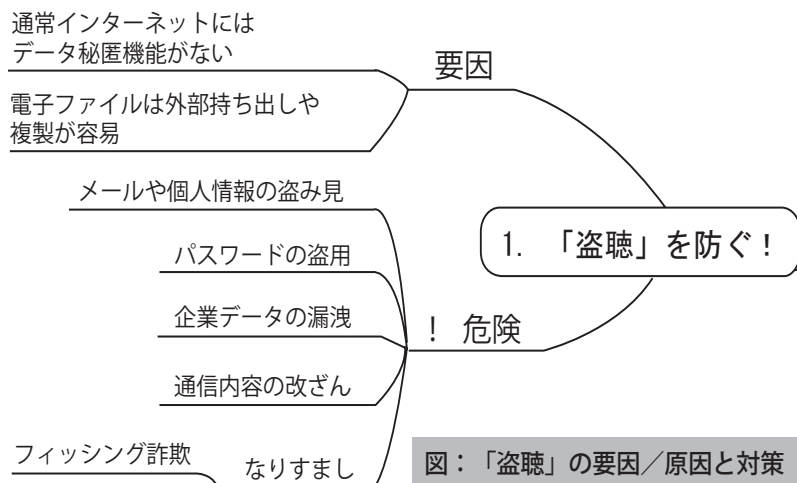
力するパスワードや個人情報も、そのままでは第三者が「覗こうと思えば覗ける」ものとなっています。(通信内容の改ざんも可。)現実世界では、他人に見られたくない手紙の場合は「封書」、より機密性の高い書類の場合は「書留」のような郵送手段がありますが、インターネットを利用する場合も同じような考え方が必要になってきます。

また、「盗聴」の敷居を低くしている別の理由として、「電子ファイルは外部持ち出しや複製が容易」という点があります。

コンピュータがインターネットで結ばれる以前、機密情報が「紙

で鍵のかかる場所に管理されていた時代であれば、外部持ち出しは難しく、侵入にも物理的な障壁がありました。一方、ほとんどの重要書類が「電子ファイル」の形で保存されている今日、ファイルは簡単にUSBメモリにコピーして持ち出すことができますし、場合によっては自宅に居ながらネットワーク越しに入手することも可能になっています。

例えば、ある企業がアンケートを採るWebサイトを立ち上げることにしたとしましょう。期間限定サイトのため、手早く・低コストで開発するよという指示のもと、サーバー台で運営することにします。さて、サイトを公開す



図：「盗聴」の要因/原因と対策

1. JIPDEC ISMS 審査員補、SAAJ システム監査人補
 2. 情報資産：組織が所有し、ビジネスで活用するすべての情報。ハードウェアやソフトウェア、ネットワークのようなシステムだけでなく、「会話」や「記憶」、「信頼」など人的な要素も含まれる。
 3. 脅威：情報資産に影響を与え、損失を発生させる直接の原因。事故の潜在的原因。
 4. インターネットの場合、音声の「盗聴」というよりも、メッセージやデータの盗み見、盗用になります。
 5. IPv4：Internet Protocol version 4。ちなみに、次世代のインターネットプロトコル「IPv6」では、IPセキュリティプロトコル (IPSec) が標準装備されている。
 6. ディレクトリ・リスティング：ディレクトリ名で終わる URL を指定すると、ディレクトリ配下にあるファイルの一覧が表示されるという、Web の伝統的な約束事。

ると、アンケートに答えた見返りにプレゼントが当たるということで、顧客は自分の氏名や住所、電話番号、生年月日といった個人情報をこぞって入力します。しかし、数日後、アンケートに答えた顧客のデータが大量に漏洩していることが発覚します。原因を調べてみると、Webサーバ設定の単純なミスのため、「ディレクトリ・リスティング」⁶が可能になっており、Webサーバ上に保存した個人情報ファイルが容易にダウンロードできる状態になっていることが判明しました。つまり、「素人」であったとしてもちょっとしたWebの知識があれば、自宅に居ながらにして「盗聴」できてしまったわけです。

「Webサーバ上に個人情報を置かない」というのがWebアプリケーション開発の鉄則ですが、予算や納期などの都合でこれをショートカットしてしまうと、このケースのように「脅威」がWeb

サイトのセキュリティホール（「脆弱性」⁷という）を突いて、思いがけない事件・事故に発展する可能性があります。

では、こうした「盗聴」の背景を踏まえて、どのようにシステムセキュリティ対策を採ることができのでしょうか？

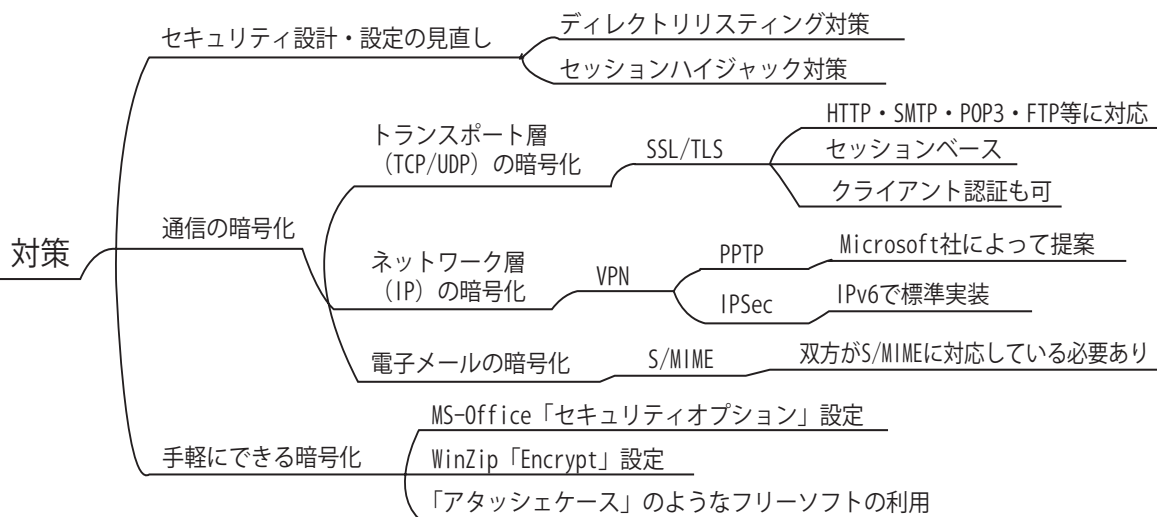
結論を言えば、「敷居を高くする」ということになりますが、まず「メールやデータの盗み見」対策としては「通信の暗号化」があります。「通信の暗号化」も、目的に応じて様々ですが、いずれもインターネット上に送り出す「はがき」のようなデータを「封筒」で包んで第三者が覗けないように機能します。

代表的なものとして、Webサーバとブラウザ間の通信（HTTP⁸）等を暗号化する「SSL/TLS⁹」、拠点間の通信を暗号化する「VPN¹⁰」、メールを暗号化する「S/MIME¹¹」があります。

しかし、「アンケートサイト」の事例にあるように、暗号化すれば「盗聴」対策は万全というわけではなく、定期的なセキュリティ設定や設計の見直しをルール化することも大切です¹²。

では、個人（または家庭）レベルでは、どのようにインターネット「盗聴」対策ができるのでしょうか？例えば、クレジット情報など、第三者に知られたくない内容を記したメールをそのまま流すのではなく、MS Wordの「セキュリティオプション」¹³でパスワードを設定したものを添付で送ったり、WinZipの「Encrypt」でパスワードを設定するといった手軽な暗号化機能を利用することができるかもしれません。

さて、今回は、近年、アメリカ国内を中心に日本でも被害を及ぼしている「フィッシング詐欺」を含めた「なりすまし」対策について、システムセキュリティ対策のポイントを取り上げたいと思います。



7. 脆弱性：脅威を受けた場合、情報資産の損失を起しやすく、かつ拡大させる要因。
 8. HTTP：Hyper Text Transport Protocol
 9. SSL/TLS：Secure Socket Layer/Transport Layer Security
 10. VPN：Virtual Private Network。仮想閉域網。
 11. S/MIME：Secure/Multipurpose Internet Mail Extensions。電子メールの

標準プロトコルの MIME の枠組みの中で暗号化機能を実現。
 12. 例えば、Webサイトを運営している場合、「Nimda」や「Code Red」のようなウイルスが、Webサーバのセキュリティホールを突いて感染する危険が常にあるので、最新パッチを迅速に適用するルールが求められます。
 13. 「名前を付けて保存」→「ツール」→「セキュリティオプション」で「読み取りパスワード」を設定します。