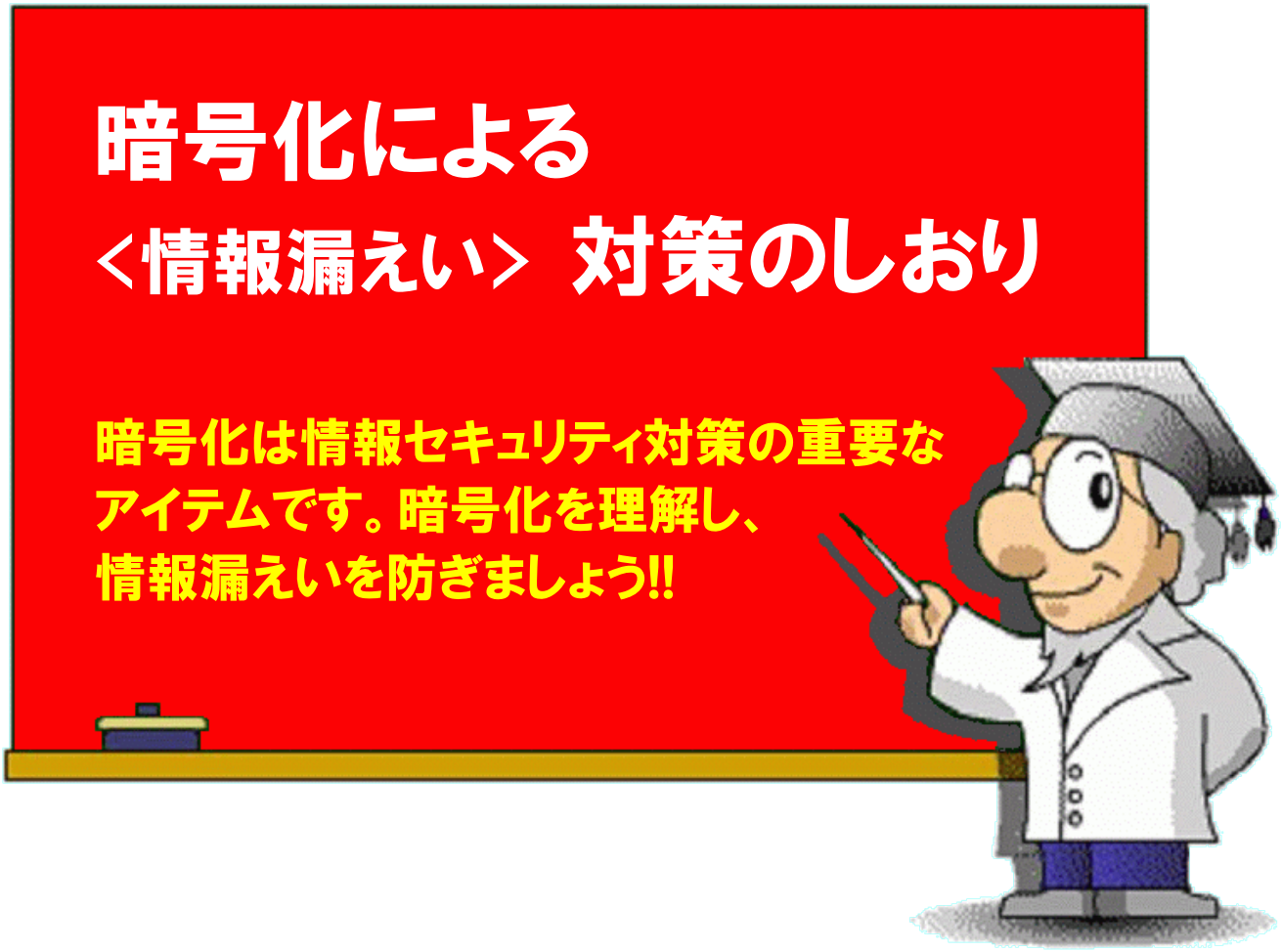
IPA 対策のしおり シリーズ (12)

暗号化による
<情報漏えい> 対策のしおり

暗号化は情報セキュリティ対策の重要なアイテムです。暗号化を理解し、情報漏えいを防ぎましょう!!



IPA 独立行政法人 情報処理推進機構
技術本部 セキュリティセンター

http://www.ipa.go.jp/security/

2014年3月20日 第1版

目次

はじめに

大まかな暗号の歴史

大昔から、情報を秘匿するために、特定の人たちの間でのみ読める文書を作ることが必要でした。初期の暗号には、文字の置き換えを利用したものが使われていたようです(これを換字と言います)。アルファベットの文字の並びを特定の文字数分ずらして使ったり、文字列の並びを変換する表を利用したりするものでした。これらの場合は、ずらした文字数や変換表が暗号解読の鍵になるわけです。

さらに、変換表を複数組み合わせて機械的に表を換えながら使うなどの暗号方式が先の大戦頃まで多く使われていたようです。このような方式では、ドイツのエニグマなどが有名ですね。興味のある人は調べてみてください。

このような換字で作成された暗号文は、文章中のアルファベット文字の利用頻度などを考慮した解読法などが見出されたり、変換表などが盗み出されたりした結果、重要な情報の暗号化には不向きになっていました。

コンピュータの発達とともに暗号の解読も機械的に実施されるようになり、より複雑な、解読に時間のかかるような鍵が利用されるようになってきています。

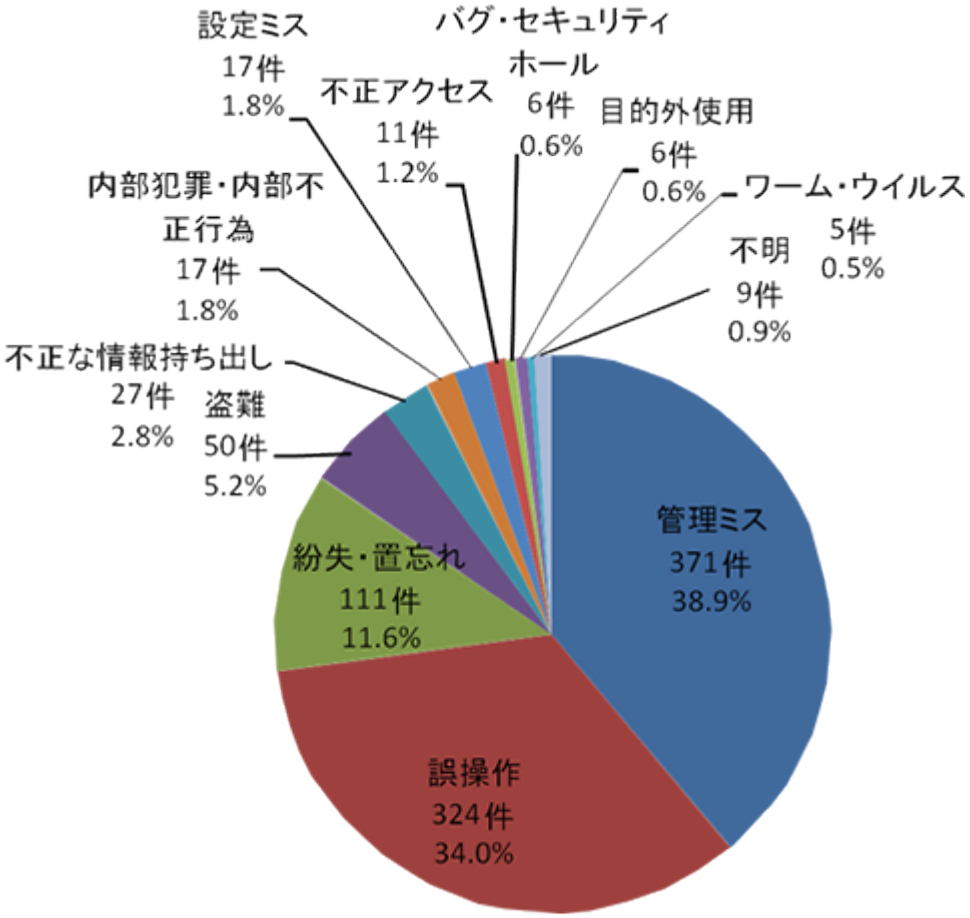
近年の暗号化方式では、暗号化と復号に同一の鍵を利用する共通鍵暗号方式がありますが、この鍵が盗まれると簡単に復号できることから、鍵の受け渡しが危険(受け渡し問題)という理由で、暗号化と復号で別の鍵を利用する方式(公開鍵暗号方式)が使われています。ただし、公開鍵暗号方式は現時点では手続き上の速度が出ないので、鍵の配送に公開鍵暗号方式の暗号化、実際のデータの暗号化には共通鍵暗号方式を使う、いわゆるハイブリッドの方式が多く利用されています。

公開鍵暗号方式では、暗号化する際の鍵は一般に公開されたもの(公開鍵)とし、この公開鍵で暗号化したものは、復号専用の鍵(プライベート鍵)でのみ復号できるようにしたものです。公開鍵とプライベート鍵が常にペアの状態で運用されるものです。電子メールの電子署名などには、公開鍵で復号できるもの(RSA 方式等)を利用し、電子メールの本文をハッシュ化したものをプライベート鍵で暗号化する(受信者は公開鍵で復号する)ことで電子メールの本文が改ざんされていないことを証明するなどの電子認証に使われたりしています。

最近ではさらに進んだ暗号方式が研究・開発されていますが、暗号の危殆化(きたいか:暗号の安全性が下落すること)に飲み込まれないための進化が続くと言うことになります。

1. なぜ暗号化が必要なのか

暗号の歴史はともかくとして、最近、個人情報の漏えい問題が取り沙汰されています。個人情報あるいは企業の機密情報は、いろいろなルートで漏えいしています。世間では、コンピュータシステムへの不正アクセスによって漏えいするケースが大きく報道されていますが、実はこんな統計情報があります。



これは、特定非営利活動法人　日本ネットワークセキュリティ協会(JNSA)が調査・公表した「2012　年度の個人情報漏えいの原因比率（インシデント件数）」を示したものです。

不正アクセスやコンピュータウイルスによるものに比べて、「管理ミス」「誤操作」「紛失・置き忘れ」「盗難」で大方９割しめていることになります。ここでいう「管理ミス」とは、本来個人情報を管理する方法やルールがあるのに、それが守られなかったようなケースなどのことで、「誤操作」には電子メールの送信ミスなどが含まれるようです。

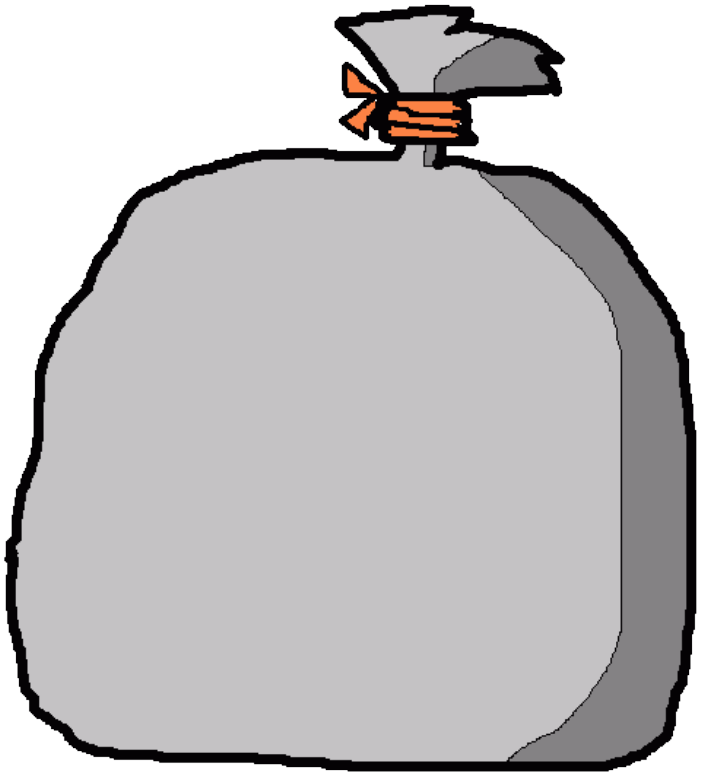
このような状況では、大切な情報はそのままの形では漏えいの危険があるということになります。

こういった状況の対策はないのでしょうか？

ここで考えられるのが、こういったインシデント（事故あるいは事件）が起きることが前提ならどうだろうかと言うことになります。人の行為が原因であることを考えれば、うっかりミスをなくすなどの対策も重要ですが、情報が漏れる可能性があるならば、漏れても簡単には読めなければ良いことになります。

そこで情報の暗号化がこういった状況の大きな対策になるわけです。「電子メールの送信ミスでメールに書かれた重要な情報が漏れるのなら、重要な情報は暗号化しておきましょう」と言うことになります。

前述の「管理ミス」については、暗号化のルールが守れないことが原因にもなりますので、対策にはならないかも知れませんが、「誤操作」や「紛失・置き忘れ」「盗難」については、十分な対策になるだろうと考えていいでしょう。



2. 例えば電子メールの暗号化

電子メールの暗号化というとハードルが高いと思われるかも知れません。確かに、電子メールそのものを暗号化する場合は専用の仕組みが必要となります。また、公開鍵暗号方式を使うことが前提であれば、相手が提供する公開鍵で暗号化（復号するにはメール受け取り側のプライベート鍵が必要）するために、暗号化メールのやり取りは一般的には公開鍵とプライベート鍵を持っている受け手を中心にした 1 対 n になってしまいます。つまり、暗号化メールのやり取りをする場合は、それぞれが公開鍵とプライベート鍵のペアを持っていなければならないことになります。

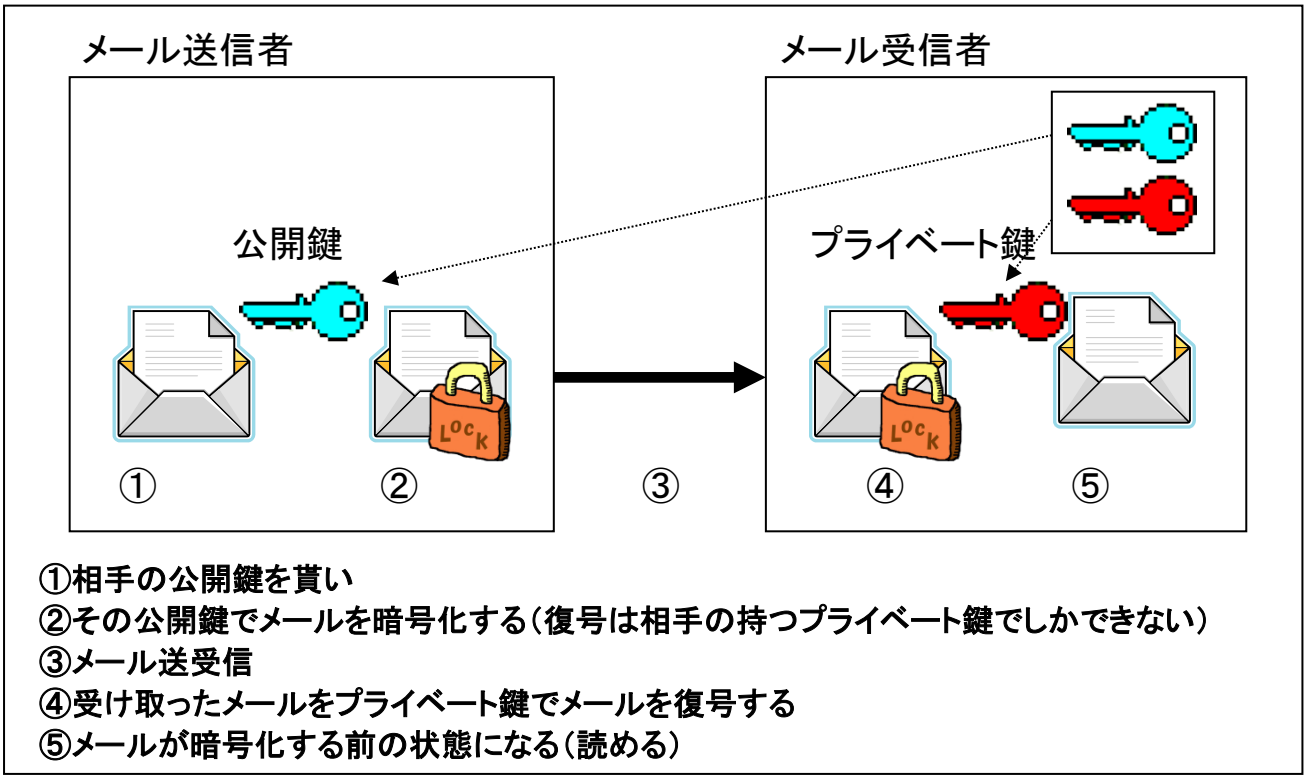


図　公開鍵方式でのメール暗号化のイメージ

こういった運用上の煩わしさもメールの暗号化を行うことのハードルになってしまう場合があるようです。しかしながら、手軽な方法がないわけではありません。それは、添付ファイルの暗号化です。

電子メールの本文には重要な情報を記載せず、重要な情報はドキュメント化して添付ファイルで送受信する方法です。この際、ドキュメント化された電子データを暗号化しておけば、電子メールを暗号化するのと近い安全性が保たれるわけです。

では、ドキュメントを暗号化するのはどうすればよいでしょうか？

専用の暗号化アプリケーションを使うことでも OK ですが、例えば、皆さんが Microsoft 社の Office アプリケーションをお使いであれば、以下に示すような方法でドキュメントを暗号化することもできます。

Microsoft Office 2010 を例に暗号化の方法を説明しますが、Microsoft Office 2013 でも同じ手順で暗号化できます。

Microsoft Office 2010 Word の場合、
①「ファイル」タブから②「情報」を選択し、
③「文書の保護」から④「パスワードを利用して暗号化」を選択する
あとは⑤パスワードを設定すればよいわけです

注意書きにもありますが、パスワードを忘れてしまうとドキュメントを回復（復号）できないので注意してください。

また、このパスワードを、暗号化したドキュメントを添付した電子メールの本文に書いてはいけないことはお分かりですよね…それはジョーク以外の何物でもありませんから…

さらに、容易に推測可能なパスワードの設定はせっかくの暗号化が役立たずになる可能性もあるので注意してください。

3. 例えば、「紛失・置き忘れ」「盗難」対策の暗号化

「紛失・置き忘れ」「盗難」が原因の情報漏えいインシデントも数多く報告されていますが、これらの事故の漏えい媒体が電子データであれば、紛失・置き忘れおよび盗難対策には暗号化は大きな効果を発揮します。

漏れては困る重要な情報をノートパソコンやタブレット、スマートフォン、ポータブルハードディスク、電子メモリ等に保存して持ち出す場合、それらの電子媒体には「紛失・置き忘れ」「盗難」のリスクが存在します。

ノートパソコンやタブレット、スマートフォン等の場合、それらを利用するための認証（ログイン操作や暗証番号によるセキュリティロック等）があるから大丈夫とおっしゃる方もあるかも知れません。確かに、こういったデバイスを第三者に利用されないようにするためには効果的です。でも、ノートパソコンやタブレット、スマートフォンの内蔵ディスクやメモリがそっくりそのまま抜かれた場合はどうでしょうか？別のパソコンなどに直接つなげば、そのまま内容が読めてしまう可能性があります。

では、どうすれば読めない状態にできるかとなりますが、それが暗号化です。

最新のOSを搭載したノートパソコンやタブレット、スマートフォンでは、内蔵するディスクを自動的に暗号化して利用する機能が搭載されていたりします。これらの機能を利用することで、ディスク（メモリ）の抜き取りによる情報漏えいは防ぐことができます。

さらに、ポータブルハードディスクや電子メモリ（USB メモリ）についても、初めから暗号化機能が実装されたものもありますし、電子メールの話の中で説明したような、電子ファイルを暗号化する方法を利用すれば、電子媒体に暗号化機能が付いていなくても暗号化で電子データを守ることができるわけです。

つまり、積極的に暗号化を利用すれば、「紛失・置き忘れ」「盗難」対策になるということです。

ただし、暗号化する際に利用したパスワード等を忘れてはいけないということです。これらを忘れると、データは再利用できなくなります。また、前述の内蔵ディスクを自動的に暗号化する場合は、それらを内蔵する機器の利用者認証のためのパスワードを忘れてしまうとデータの再利用ができなくなることもお忘れなく…

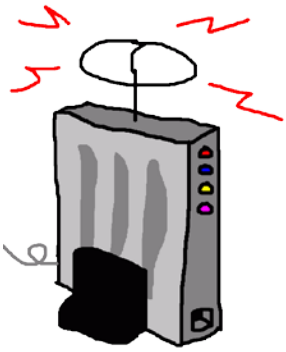
さらにつけ加えておきますが、内蔵ディスクを自動的に暗号化する機能を利用しているからと言って、それらを内蔵する機器の利用者認証が脆弱だと、デバイスそのものを紛失したり盗まれたりした場合は、利用者認証が破られ内蔵ディスクの内容が筒抜けと言うことになりますので、利用者認証も強固なものにしておかなければ意味がありません。

ここで、うんちくを一つ…パスワードと暗号化の関係は…

暗号化にはパスワードがつきものですが、パスワードと暗号化には微妙な関係があります。パスワードがなければ暗号が解けないと言われますが、最近の暗号方式では、実際にパスワードが暗号を復号するための鍵になっているわけではありません。何故ならば、鍵が漏れれば暗号そのものが破られるからです。そこで、最近では鍵自体を暗号化機能が自動生成し、パスワードはその暗号化機能を使うための認証に使われているわけです。その結果、パスワードが漏れても暗号化された媒体からは、直接暗号データを復号することができないようになっています。パスワード＝暗号を復号するためのキーワードと考えても間違いではありませんが、物理的にはパスワードと鍵は別物ということになります。こんなことは意識せずに暗号化機能を使ってくれればOKですがね…

4. 例えば、無線LANを安全に利用するための暗号化

最近、無線LANが会社でも自宅でも普及しています。LAN用ケーブルを引き回さなくても良いし、10BASE(最高 10Mbps で通信が可能な LAN の規格)とか100BASE(最高 100Mbps で通信が可能な LAN の規格)あたりの LAN ケーブル環境であるならば、無線の方がLANケーブルを利用するより通信速度が速かったりします。こういった通信機器を安全に利用するために、暗号化は一役かっています。



LANケーブルを利用するのであれば、そのケーブルが繋げない機器は通信できません。しかし、無線LANの場合は通信を暗号化していなければ誰でも繋げることができてしまいます。これを防ぐためには無線LANで暗号化通信方式を利用します。これにより暗号化のためのパスワード(パスフレーズ)を知らない人は繋げないようにすることができます。当然、通信内容が第三者に傍受されても、暗号化通信を行っていれば安全ということになります。

ただし、忘れてはならないことがあります。自分たちが管理する無線LANの環境であれば前述の話は有効ですが、自分たちが管理していない無線LANの環境(例えば街中のWi－Fi環境)では話が違ってきます。こういった環境では、不特定多数の人が無線LANに接続するわけで、ある意味では誰でも繋げる環境であると考えてください。言ってみれば公の場と言うことになり、公衆無線LANと言われるわけです。少し極論になるかもしれませんが、このような環境では暗号化通信が行われていることが安全であるという方程式は成り立たないと考えてください。何故ならば、無線LAN環境での暗号化通信は、あなたのデバイスと無線LANのアクセスポイント(AP)間でのみ有効であり、AP より内側では通信が復号されているということです。つまり、会社の業務でこういった環境で利用する場合は、無線 LAN の暗号化に頼らず、自前の暗号化通信ができる方法を利用されることをお勧めします。これについては次の項目で説明します。

ここで、うんちくを一つ…WEP とWPAの違い

無線LANの暗号化通信方式には一般的に WEP、WPA/WPA2 がありますが、この違いはパスワード(パスフレーズ)の桁数だけではありません。実は、前述のうんちくの内容に関係しています。WEP の場合はパスフレーズが鍵となり、WPA/WPA2 の場合はパスフレーズが暗号化機能の認証のためのもので、鍵は自動生成されます。鍵が固定されていると、通信内容から鍵が推測されやすく、結果、暗号そのものを直接解読する意味ではWPA/WPA2 の方が鍵を推測されにくいので安全となります。

まぁ暗号アルゴリズムの違いがあるのは当然として、こういった違いがあるわけです。

無線 LAN については「無線 LAN〈危険回避〉 対策のしおり」も参照いただけると幸いです。

5. 例えば、会社の外と中との通信を安全に利用するための暗号化

一般的に会社の外と中との通信を行う場合は、2 つの方法が利用されます。一つ目は、会社の情報システム側に用意された Web アプリケーションを介する方法です。二つ目は、リモート接続機能を利用して、会社内のサーバと直接通信する方法です。(ある意味では Web アプリケーションですがクライアント側に用意されたアプリケーションを使うか否かの違いがあります)

こういった機能を利用する場合、あなたと会社の間に存在するネットワーク(インターネット)上で通信の盗聴行為(あるいは悪意のない通信の記録)が行われる可能性があります。つまり、第三者に通信内容が見られてしまう(情報漏えいの)可能性があるわけです。

こういった問題に対処するためには、Web アプリケーションとの通信を暗号化したり、リモートデスクトップ接続機能*1で暗号化通信を行ったりする必要があります。

会社の情報システム側に用意された Web アプリケーションを介する方法では、情報システム側に SSL(Secure Socket Layer)/TLS(Transport Layer Security)*2が使える環境(例えばサーバ証明書*3を用意する)にしておく必要があります。この環境下では、利用者側のブラウザで通信相手の URL が **https://...**となります。この URL を介しての通信は暗号化され、通信経路上では盗聴されても内容を復号して読まれることはありません。

会社にこういった環境を用意する場合は、俗にオレオレ証明書と言われる自前のサーバ証明書を使えば構築することができますが、正式なサーバ証明書を利用する場合は認証機関に依頼して作成してもらうことになります(有償)。

社内環境でのみ利用する場合は、オレオレ証明書でもあまり問題は起きませんが、会社の顧客や会社が提供する Web サービスのお客様に使ってもらう場合には、接続先が正しいことを証明(確認)できる正式なサーバ証明書を利用することをお勧めします。これにより、お客様の個人情報を暗号化で守ることができるわけです。

また、リモートデスクトップ接続機能を使う場合も原理は同じで、通信には VPN(Virtual Private Network)*4と SSH(Secure Shell) *5が利用されます。一般的には会社内に用意されたファイアウォール装置などに実装された機能を利用すれば構築できます。

***1)リモートデスクトップ接続機能**

リモート接続とは、LAN などで構成されたネットワークやコンピュータ（サーバ）に対して、それらから離れたところから電話回線やインターネット経由でアクセスすることをいいます。それを実現する機能がリモート接続で、サーバ側のデスクトップ環境をリモートで使う機能がリモートデスクトップ接続機能です。

***2) SSL (Secure Socket Layer)/TLS (Transport Layer Security)**

SSL/TLS は Web アクセスのための通信データを暗号化するものです。クライアント側は、ブラウザが処理を行ってくれるので、利用者はこの仕組みについて特別な操作は不要です。サーバ側が提供する暗号化機能ということです。

***3) サーバ証明書**

サーバ証明書とは、内蔵された暗号化通信に利用される公開鍵が誰のものであるか証明するものです。一般的には、認証局（CA：Certificate Authority)と呼ばれる機関が証明するものです。実際に、証明されたい者が用意した公開鍵を認証局に証明してもらう必要があります。その証明の方法は、認証局が持つプライベート鍵で証明書を暗号化してもらうことで、その証明書は認証局で認証されたものとなります。つまりこれを使えば、通信相手が正しいことを確認できるわけです。

***4) VPN (Virtual Private Network)**

VPN とは仮想的な専用ネットワークのことです。かつて、企業などが拠点間を結ぶ通信経路（バックボーン）として専用回線を利用していましたが、一般の公衆回線をあたかも専用線として利用する方法として考案されました。公衆回線を使うということでセキュリティ上の問題がでてきますが、認証技術や暗号化技術により安全性を保つ工夫がなされています。

***5) SSH （Secure Shell）**

主に UNIX コンピュータで利用されるネットワークを介して別のコンピュータに接続(ログイン)したり、遠隔地の端末からコマンドを実行したり、他の端末へファイルを移動したりするためのプログラム。ネットワーク上を流れるデータは暗号化されるため、インターネット経由でも一連の操作を安全に行うことができます。

ここで、うんちくを一つ…**https://…**で接続された Web メールは安全か？

メールの暗号化で記述したように大事な情報を電子メールで送受信する場合は、メールの暗号化や添付ファイルの暗号化が効果的としていましたが、メールサーバとクライアント間で暗号化通信ができる Web メールは同じ意味合いで安全かどうかお話しします。

メールサーバに蓄積されたメールを読んだり、メールサーバに対してメールの送信を依頼したりする際には、通信内容が暗号化されるため安全といえます。

ところで、漏えいしては困るような重要な情報をメール送信する際に Web メールを使うと、メールサーバとの通信が暗号化されているので安全と思いがちですが、メールサーバから先つまり送信先のメールサーバへの通信は暗号化の対象ではないので、実際にはすべての経路で暗号化が行われていないことになり、安全とは言えない場合があります。

暗号化していれば安全というのは、通信経路すべてが暗号化により安全な場合だけなので注意してください。これはちょうど、無線 LAN の暗号化通信の場合と同じ問題となります。一つのメールサーバしか介さない同一ネットワーク内の社内メールならともかく、社外との通信を行う場合は、重要情報は暗号化して添付ファイルにするなどの対策を実施することをお勧めします。

6. 参考情報（もっと詳しく知りたい人のために）

＜総務省＞

- 国民のための情報セキュリティサイト 暗号化の仕組み
  http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/02.html

＜IPA＞

- 無線 LAN 利用環境のための運用上のセキュリティ対策
  http://www.ipa.go.jp/security/fy18/reports/contents/enterprise/html/411.html
- Web サイトの SSL 暗号化通信の設定
  http://www.ipa.go.jp/security/fy14/contents/soho/html/chap4/httpd/IIS-SSL.html
- 暗号化技術 講義ノート
  http:// www.ipa.go.jp/files/000018633.docl
- 暗号技術 Q&A
  http://www.ipa.go.jp/security/enc/qa.html
- 情報漏えいを防ぐためのモバイルデバイス等設定マニュアル
  https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html
- 一般家庭における無線 LAN のセキュリティに関する注意
  https://www.ipa.go.jp/security/ciadr/wirelesslan.html
- IPA テクニカルウォッチ 『暗号をめぐる最近の話題』に関するレポート
  https://www.ipa.go.jp/about/technicalwatch/20110511.html

IPA 対策のしおり シリーズ

http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA 対策のしおり シリーズ(1) ウイルス対策のしおり
- IPA 対策のしおり シリーズ(2) スパイウェア対策のしおり
- IPA 対策のしおり シリーズ(3) ボット対策のしおり
- IPA 対策のしおり シリーズ(4) 不正アクセス対策のしおり
- IPA 対策のしおり シリーズ(5) 情報漏えい対策のしおり
- IPA 対策のしおり シリーズ(6) インターネット利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり
- IPA 対策のしおり シリーズ(8) スマートフォンのセキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(9) 初めての情報セキュリティ 対策のしおり
- IPA 対策のしおり シリーズ(10) 標的型攻撃メール 対策のしおり
- IPA 対策のしおり シリーズ(11) 無線 LAN 対策のしおり
- IPA 対策のしおり シリーズ(12) 暗号化による 情報漏えい対策のしおり

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

〒113-6591 東京都文京区本駒込2丁目28番8号
（文京グリーンコートセンターオフィス16階）
URL http://www.ipa.go.jp/security/

【情報セキュリティ安心相談窓口】
URL http://www.ipa.go.jp/security/anshin/
E-mail anshin@ipa.go.jp