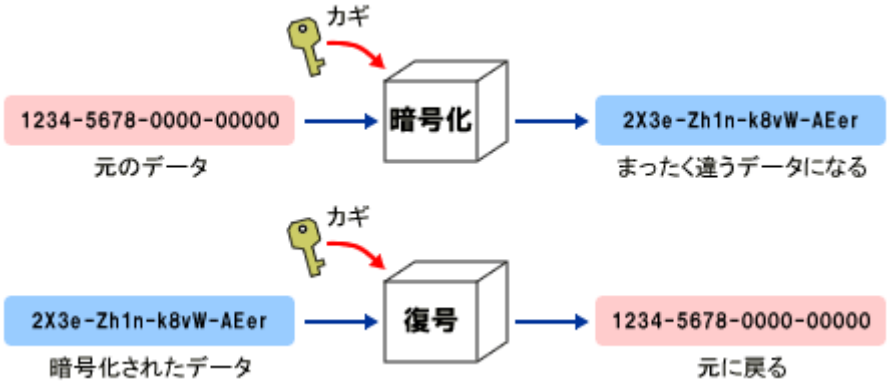
暗号化

暗号は、第三者には知られたくない情報を特別な知識なしでは内容が理解できないように変換する手法、もしくは変換されたもの（暗号文）を言います。
もともとは、情報のやり取り、つまり、封書の配達時や通信の世界で用いられている手法です。暗号の歴史は古く、紀元前 3000 年頃のバビロニア時代から使われ、日本でも戦国武将の上杉謙信が暗号を使っていたと言われています。暗号技術は戦争によって、解読技術とともに進化してきました。初期のコンピュータは戦時中に敵国の暗号を解読するために開発されたとも言われています。

情報のデジタル化が進んでコンピュータやサーバ内に保管されるデータ量が膨大になり、その中には機密のデータや情報も含まれるようになっています。しかも、USB などの媒体やインターネット経由で、それらの情報が簡単に持ち出したり、送受信されたりするようになりました。
ビジネス分野においても、電子メールや Web サイトなどを介して、企業間の情報交換や、契約内容から個人のプライバシー情報に至るまで、機密にしたい重要情報がやりとりされています。

情報化社会の進展とともに、紛失やサイバー攻撃などによる、重要情報の漏えいや盗聴の危険性はますます高まっています。暗号化は、仮に紛失などによる漏えいやサイバー攻撃の被害にあった時でも、情報の機密性を守るための必須の技術であり、また各人が意識して実施すべき重要データの加工処理なのです。

情報システムの世界における「暗号化」とは、デジタル化されているデータや情報をそのままではなく、何らかの規則に従って、意味のわからないデータに変換することをいいます。元の意味のあるデータや情報を「平文」、変換の規則のことを「鍵」（正確にいえば、「鍵」と「暗号アルゴリズム」）、変換された結果を「暗号文」と呼び、暗号文を再変換し、元の判読できる状態（平文）にすることを「復号」（または「復号化」）と呼びます。



暗号化と複合（出典：総務省「暗号化の仕組み」））

【便利知識】
「復号化」と似た言葉に「解読」がありますが、解読は「当事者でない者（鍵を知らない者）が暗号文を平文に戻したり、復号のための鍵を探り出したりする行為」を意味することが多いようです。つまり、スパイ行為か、さもなければ専門家による分析行為ということになります。

暗号化の方式

暗号化の方式には、大別して「共通鍵暗号方式」と「公開鍵暗号方式」とがあります。現在は、両者を組み合わせたハイブリッド暗号方式が良く使われているようです。

【共通鍵暗号方式】
暗号化と復号化に同じ「鍵」を使う方式で、簡便で、暗号化・復号の処理も高速なのですが、この鍵が知られてしまうと暗号化されたデータが読まれてしまうことになりますので、この鍵が関係のない人に渡ったりしないよう厳重に管理しなければなりません。また、メール等で鍵の受渡し時に第三者に傍受されるリスクがあります。暗号化したWord、Excel、PDF などの文書を添付したメールと暗号鍵を受け渡すメールを別にするなどの対策が必要です。

【公開鍵暗号方式】
暗号化と復号化にそれぞれ異なる一対の「鍵」を使う方式です。情報の受信者が、暗号化するための鍵を送信者に公開し（公開鍵）、送信者は「公開鍵」で暗号化した情報を送信します。復号化する鍵は、受信者だけが持つ「秘密鍵」（「プライベート鍵」あるいは「個人鍵」ともいいます）」とすることで、共通鍵暗号方式より手間がかかりますが、鍵の管理が容易で、より安全性を高めた方式です。

公開鍵暗号方式の短所は、概して処理が複雑で、暗号化・復号に要する時間がかかるという点です。このため，大量のデータを暗号化するのには向いていません。

【ハイブリッド暗号方式】
公開鍵暗号方式の「鍵の管理・配布が容易」という長所と、共通鍵暗号方式の「処理が高速」という長所の両方を生かすように、両方式を組み合わせたハイブリッド暗号方式が考えられ、現在ではこの方法が多く利用されています。
ハイブリッド暗号方式では、鍵の受け渡しには公開鍵暗号方式を用いて、実際のデータの暗号化は処理の早い共通鍵暗号方式を用います。つまり、データの暗号化に使う共通鍵を予め受信者側から知らされた公開鍵を使って暗号化して受信者に連絡するとともに、共通鍵で暗号化されたデータを受信者に送るのです。暗号化された共通鍵は受信者の秘密鍵でしか復号できませんので、共通鍵の管理が楽になります。
通常、共通鍵は送信者側が任意に作成します。ただし送信のたびに変え、一度使った共通鍵を繰り返し使わないようにします。この方法により，悪意のある第三者に共通鍵が盗聴され解読されたとしても、これを使用して復号されることを極力防ぎます。1 回の通信（セッション）に限って有効なことから、この共通鍵のことを「セッション鍵」とも呼びます。

文書ファイルの暗号化

文書を保存したパソコンや USB などを紛失したり盗難にあったりした時のために、また、メールに添付した文書やクラウド上に保存した文書が配信ミスや盗聴された時のために、文書ファイルが暗号化されていれば、情報漏えいの被害をかなり抑えることができます。

Word や Excel などの Office 文書には、2 つの方法で文書を暗号化して保存できます。

1. 「ファイルタブ」の「情報」画面中の「文書の保護」（注）アイコンをクリックして、「パスワードを使用して暗号化」を選ぶ
2. 「名前を付けて保存」ダイアログボックス画面下部の「ツール」をクリックして、「全般オプション」を指定する。この方法の場合は、読み取り用と書き込み用でパスワードを変えることができる。

（注）Excel では「ブックの保護、Powerpoint では「プレゼンテーションの保護」

PDF 文書の暗号化もできますが、通常は、Adobe Acrobat という割と高価な PDF 作成・編集用のソフトか、フリーソフトの CubePDF などを使う必要があります。

但し、元が Word 文書の場合だけは、パスワード保護付きの PDF 文書をエクスポートできます。残念ながら、Excel や Powerpoint の場合はパスワード付き PDF 文書をエクスポートできません。

（注）Word 文書を「PDF で保存」する方法の時はパスワード設定できません。

具体的な手順は次の通りです。

「ファイルタブ」⇒「エクスポート」⇒「PDF/XPS ドキュメントの作成」⇒「オプション」
⇒「PDF/A 準拠」のチェックマークを外し、「ドキュメントをパスワードで暗号化する」にチェックマークを付けた上で、「OK」ボタンを押す⇒パスワードを設定する
（以下、略）

【便利知識】

暗号化にはパスワードがつきもので、パスワードは暗号データを復号するための鍵（キー）と思いがちですが、実は違います。鍵自体は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るのです。これにより、パスワードが漏れても、暗号化された媒体から直接的には暗号データを復号できないようになっています。

内蔵ディスク全体の暗号化

情報漏えいの原因の多くが「紛失・置き忘れ」と「盗難」によるものです。

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、USB メモリなどの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。ログイン認証をセットしているから大丈夫、と思っても、内臓ディスクや SSD ストレージが抜かれて別のパソコンなどに繋いで読まれてしまう可能性があります。

内蔵ディスク全体を暗号化しておけば、紛失・置き忘れ・盗難時の情報漏えいの被害がかなり救えます。

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ます。

個人情報や機密情報を保存しているノートパソコン等は、ぜひ内蔵ディスクを暗号化するよう設定しましょう。

- Windows　「BitLocker」という機能が用意されています
- MAC　「FileVault」という機能が用意されています
- Android　「スマートフォンの暗号化」という機能が用意されています
- iOS（iPhone/iPAD）　内蔵ディスクは自動的に暗号化されます

ポータブルハードディスクや USB メモリには、暗号化機能が実装されているものが市販されています。できるだけそのようなものを使いましょう。暗号化機能のない USB メモリなどを用いざるを得ない時は、暗号化した圧縮データに変換して持ち出すことをおすすめします。

SSL/TSL

インターネット上では、住所・氏名といった個人情報はもちろん、クレジットカード番号、各種パスワードといった重要な情報が、頻繁に送受信されています。一方で、それら重要情報を狙う通信データの盗聴などのサイバー犯罪は絶えません。
SSL/TLS は、盗聴などを防ぐためのインターネット通信における世界標準のセキュリティ技術です。

SSL（Secure Socket Layer）/TLS（Transport Layer Security）はウェブ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です。

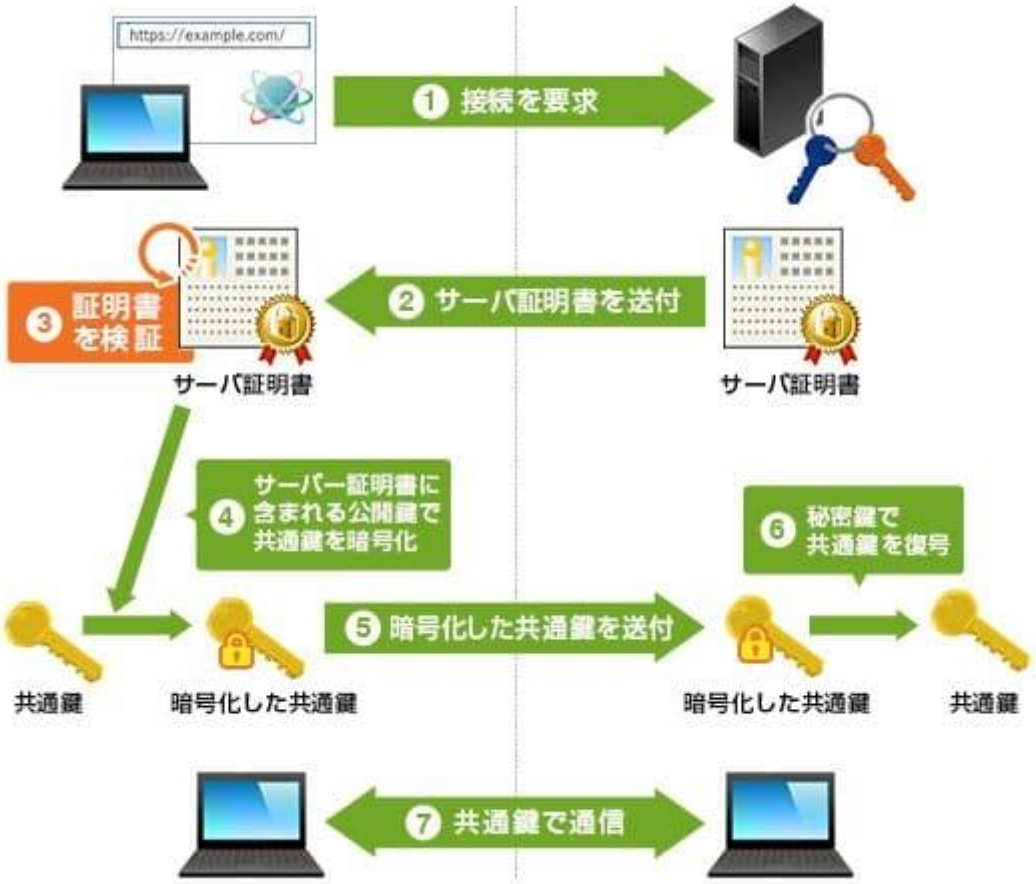
実は、SSL は TLS の前の規格で、現在一般的に SSL と呼んでいるものは TLS を指しています。SSL の名称がまだ一般に広く認知されているため、SSL/TLS と併記されることが多いのです。

SSL/TLS が導入されているウェブページでは、ブラウザのアドレスバーに表示される URL の「http://」部分に、セキュア（Secure）を表す「s」が付き、「https://」になります。

SSL/TLS を利用するには、サーバに SSL サーバ証明書を導入します。SSL サーバ証明書は信頼のおける認証局が発行する電子的な証明書で、ウェブサイトを安全に利用するための 3 つの機能が備わっています。

1. ウェブサイト所有者の確認
2. 通信データの暗号化 （ハイブリッド暗号方式）
3. 改ざんの検出

SSL/TLS の技術的な仕組みについては、下図を参照ください。



SSL/TLS の仕組み （出典：シオトラスト（デジサート・ジャパン・セキュリティ合同会社））

仕事では社内や組織内の独自のメールシステムを利用している方でも、自宅ではパソコン内のメールソフトを経由して、Gmail などのクラウド型のメールサービスを利用している場合が多いと思います。
この場合、Gmail などのメールサーバとパソコン内のメールソフト（Outlook など）の間は、インターネット上の通信が行われ、メールデータが SSL/TSL で暗号化されています。メールソフトで暗号化通信を行う旨の設定が必要です。