情報セキュリティのお話 ～ HTTPS(HTTP over SSL)～

今年4月に当センターのWebページのURLを [https://www.kptc.jp]に変更しました。このURLの冒頭部「https」は「HTTP over SSL」を表し、Webページデータの通信(HTTP)を暗号化し、情報セキュリティ対策をする仕組み(SSL)を使って通信することを意味します。昨今、情報流出の防止や通信の信用性確保のため、ひろく採用されているこのHTTPSについて紹介します。

1. HTTP と情報セキュリティ

多くのWebページのURLは「http」(最近では「https」)で始まります。この「http」はHyperText Transfer Protocol(HTTP)のことで「ハイパーテキストを通信するための規約」という意味です。平たく言えば、「単なる文章だけでなく、その文章の体裁、ページや画像へのリンクなどを織り込んだデータを通信するための方法」を指し、ブラウザ上に画像やリンクの表示、検索エンジンでの検索ワードやサイトへのログインのパスワードなどの入力、やりとりができる仕組みとなっています。

このHTTPを用いた通信は現在、非常によく使われているのですが、そのままでは情報セキュリティ的に問題があります。その大きな問題が「通信内容が丸見え」というところです。例えば、通販サイトでクレジット番号を入力した場合、HTTPのままだとネット上をクレジット番号がそのまま流れます。これを第三者が傍受すれば、番号が分かってしまいます。また、通信時には上記の①「盗聴傍受」の他、②通信内容を書き換える「改ざん」、③正当な通信相手への「なりすまし」などの危険があります(図1)。

このような危険を排除するため、現在HTTPによる通信にSSL(Secure Sockets Layer)もしくはその上位のTSLという技術を用いた通信が使われています。これがHTTPS(「HTTP over SSL」もしくは「HTTP Secure」とも。)と言われる通信です。

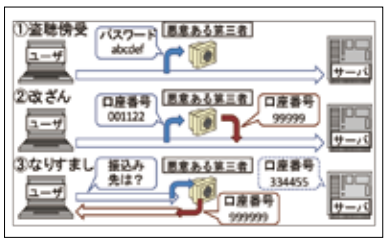

図1　通信時の危険

2. HTTP over SSL –暗号化について-

SSLは通信において暗号化技術などを提供する仕組みです。例えば「盗聴傍受」に対しては暗号化通信を行います。暗号には「共通鍵暗号」と「公開鍵暗号」という2つの種類があります。前者は暗号化に必要な情報(鍵)が1つで、暗号化と復号(暗号化の解除)のどちらもこの鍵を使います。このため通信の送受信の両者とも同じ鍵を使う必要があるため、この鍵自体を暗号化して通信する必要が出てきます。(一般に、「鍵配送問題」と言われます。)

一方、公開鍵暗号は暗号化と復号で別の鍵を使います。このため復号の鍵を秘匿(秘密鍵)にしておけば、一方の暗号化の鍵を公に(公開鍵)しても問題がありません。ですので、何も気にせず相手に公開鍵を教え、情報を暗号化してもらい(この復号は世界で自分しかできません。)相手と暗号で通信ができます。ただ、共通鍵暗号にくらべて暗号化と復号に手間がかかるため、SSLでは公開鍵暗号を使って共通鍵暗号の鍵を共有し、処理が軽い共通鍵暗号で通信を行います。

また、この他にも改ざんの有無や通信相手の正当性を保障するために「ダイジェスト認証」や「デジタル署名」等の技術が使われています。

3. HTTPSの確認

「https」で始まるサイトにアクセスした時にはアドレスバーに鍵マークが出てきます(図2)。このマークはSSLを利用した通信が行われていることを示すもので、通信が暗号化されているかを確認できます。ただ、「URLがhttpsで始まっている」・「鍵マークが表示されている」からといって、確実に安全というわけではありません。SSLにも種類があり保障するレベルが異なります。また、HTTPSで通信したとしても、そのデータ保管方法がずさんであったり、通信画面の盗撮・覗き見があれば意味がありません。

情報は一度流出すると、取り返しがつきません。より安全な通信を確立するために、このような暗号化通信などの対策を活用いただくとともに、日ごろの通信の中でも情報セキュリティについて、常に意識いただくことをお薦めします。

図2　ブラウザの表示(Internet Explorerの場合)

お問い合わせ先
京都府中小企業技術センター 企画連携課 企画・情報担当　TEL：075-315-8635　FAX：075-315-9497　E-mail：kikaku@kptc.jp