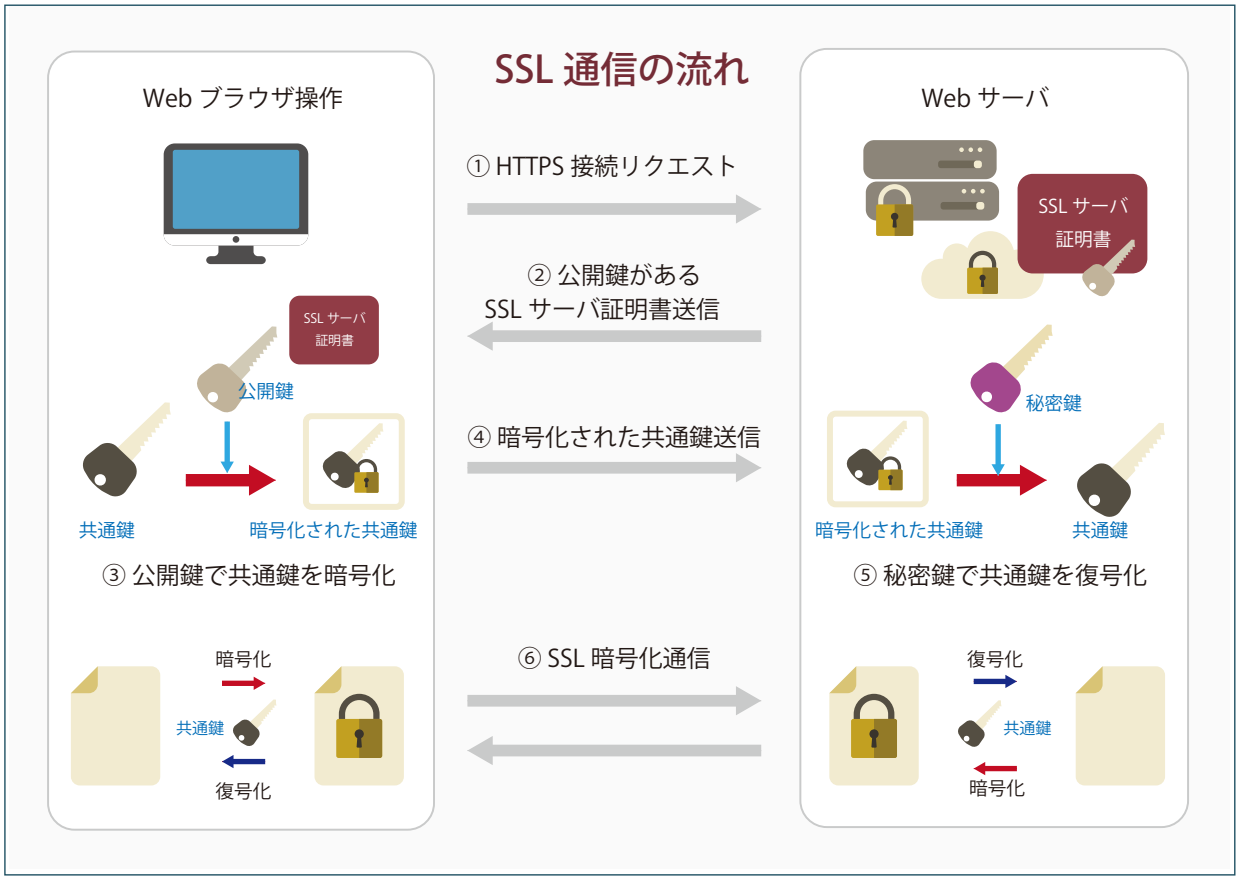
常識となった常時 SSL



URL が”http:// ～”ではなく、”https:// ～”で始まる Web ページは、インターネット上で暗号化されて通信されます。HTTPS（HyperText Transfer Protocol Secure）は、HTTP (HyperText Transfer Protocol) 通信が、SSL（Secure Sockets Layer）によって暗号化されたプロトコルのことです。但し、厳密には、当初使用されていた SSL では、バージョンアップを重ねた SSL3.0 でも脆弱性が見つかったため、現在はまったく別の設計である TLS（Transport Layer Security）というプロトコルが使用されています。ただ、目的も同じで馴染みがあるため SSL という言葉は、ウェブブラウザとウェブサーバ間でのデータの通信を暗号化し、送受信させる仕組みとして今でも使われており、SSL/TLS と表記することもあります。
数年前までは、個人情報等のやり取りを Web 上で暗号化して通信させるために、金融系でない一般企業は、問合せなどのデータ入力フォームがあるようなページのみ SSL 化しておりました。これは、暗号・復号によってパフォーマンスにも影響があるため、特定の Web ページのみに適用していました。
しかしながら、2015 年 12 月に Google が、SSL 化された Web ページを検索結果で優遇すると発表してから、Web サイトすべてを常時 SSL 化する動きがでてきました。また、SSL 化には認証局から SSL サーバ証明書を発行してもらう必要がありますが、それが低額で取得できるサービスもでてきたことも、SSL 化が進んだ要因です。2018 年 7 月からは、Google は、Chrome のウェブブラウザを使用する際に、SSL 化されていないページは、「保護されていません」というセキュリティ警告を出すようになり、今では、サイトにある Web ページすべてを常時 SSL 化することが常識となりました。
SSL 化されていないページでは、暗号化されていない平文のまま通信されているわけですから、すりガラスでない窓のお風呂を利用するようなもので、いつ第三者に通信内容を盗み見されてもおかしくありません。そのために SSL 化すれば、「共通鍵暗号方式」と「公開鍵暗号方式」の両方を用いて、インターネット上のデータ通信を暗号化することができるので、第三者からの盗聴を防ぐことができます。
また、SSL の通信では、ウェブサイト所有者の情報や、暗号化に必要な鍵、証明書発行者の署名データを持つ SSL サーバ証明書を利用して、サービスの運営元が誰なのかを確認をすることができ、利用者にとっても、信頼できるサイトかどうかの安心度が高まります。
今や企業の顔でもある Web サイトは、セキュリティ強化のために常時 SSL 化することは必須となりました。