HTTPS/SSL の仕組み

——忍者とSSLの意外な関係——

日本電信電話株式会社 NTT セキュアプラットフォーム研究所

奥田哲矢 Tetsuya Okuda

1. まえがき

スマートフォンでのインターネット利用が一般化し、ネットショッピングを今まで以上に利用している方が多いと思います。アプリを含むWebサービスの多くは、クレジットカード番号等の個人情報を安全に扱うためにHTTPSの仕組みで動作しています。「HTTPS」と初めて聞いた方は、ChromeやSafariで普段使うWebページを開いて、画面上部の文字列(URL)を確認してみてください(図1)。文字列先頭にHTTPまたはHTTPSと付いていると思います。

2. HTTP「S」の意味

インターネット上の通信は、階層的に役割を分担して行われています(図2)。HTTP(Hypertext Transfer Protocol)は、Webサービスを実現するための最も上位に位置する通信手順です。HTTPS(HTTP Secure)は、更に、これから通信する相手が信頼できるWebサービスであることを確認し、通信内容を暗号化して、安全に通信を行うための手順です。HTTPSで通信している場合は、URL左側に緑色の鍵マークが表示されます(図1)。

HTTPSが安全であるのは、SSL(Secure Socket Layer)という下位の通信手順のおかげです(図2)。SSLに関して、日常生活で直接目にすることは少ないですが、縁の下での力持ちとして、インターネット上の通信を安全に守っています。SSLの役割からすれば、イメージは「縁の下の忍者」に近いかもしれません(図2)。以降、SSLの役割を忍者になぞらえて紹介します。

3. 忍者の通信手段

伊賀忍者は、歴史上有名な「家康の伊賀越え」の際、徳川家康の命に関わる情報を安全に伝える重要な任務を負っていたと言われています。忍者の通信手段には、現代のSSL通信に通じるエッセンスがあるため、簡単に紹介します(図3)。

(1) [暗号化]: 通信内容を、敵が盗み見ても分からないようにランダムに変換する技術です。忍者が同様の目的に使ったと言われる「忍びいろは」は、各7個のへん／つくりを組み合わせて作られる架空の漢字49文字に対して、ひらがな48文字及び句読点を対応させて、元の文章をランダムに変換します。(図3、参考ページ: <https://ja.wikipedia.org/wiki/忍びいろは>)

wiki/ 忍びいろは)

(2) [認証]: 通信内容を、味方になりすました敵に誤って伝えないように通信相手を確認する技術です。忍者は夜間に行動することが多かったため、現代のように周囲に街灯のない状況では、出会った相手の顔も見えません。そのような状況でも敵/味方を判断するために、合言葉(有名な例では「山」「川」)を用いたと言われています。インターネットという通信相手の顔が見えない状況におけるユーザ認証と、利用される状況は似ています(図3)。

4. SSL通信の説明

本章では、現代の通信における暗号化/認証について、忍者(SSL)と

図1 「HTTPS」の確認方法(例)

図2 SSL/TLSの動作する階層

道具屋（ショッピングサイト）の会話の流れを通じて、技術的内容を紹介します（図4）。SSLの通信手順は、事前手続きと通信本体に分かれています。実際の通信手順とは前後しますが、技術的ポイントを①～④に抜粋して説明します。

①ユーザ認証（パスワード）

ショッピングサイトが、ユーザの本人確認に利用します。3.「合言葉」同様に、ユーザのみ知るパスワードを使う方法がよく利用されます。しかし、パスワードを使っている通信を敵に盗み見られると、敵が同じパスワードを使って不正になりすましをする恐れがあります。このため、ユーザ認証は、SSL通信で暗号化された後にHTTP通信中（図4の巻き物内）で行われることが多いです。（実際のショッピングサイトが、ユーザにパスワードを求めるタイミングも、来店早々ではなく、注文時や支払時が多いと思います。）

②サーバ認証（証明書）

ユーザが、ショッピングサイトの信頼性確認に利用します。これからクレジットカード等の情報を渡す相手が、偽のショッピングサイトでないことを確認するため、事前手続きで行われます（図4）。日常生活で例えると、飲食店は、各自治体が認めた食品衛生責任者を置いて、各自治体から営業許可証を受けています。営業許可証は、「各自治体が飲食店の食品衛生を確認している」証拠になります。一方、SSL通信では、ショッピングサイトは営業許可証の代わりにサーバ証明書をユーザに送信します。サーバ証明書は「証明書発行会社がショッピングサイトの存在を確認している」証拠になります。信頼できる証明書発行会社一覧は、ChromeやSafariに元々登録されており、この仕組みで「GoogleやAppleが間接的にショッピングサイトを信頼している」と確認できます。

③メッセージ暗号化+メッセージ認証

ユーザ/ショッピングサイト間の通信内容を、ここではメッセージと呼びます。メッセージ内のクレジットカード情報が盗まれて高額の買い物をされる等のトラブルを回避するために、メッセージ暗号化を行います。

図3 忍者の通信手段における暗号化/認証のイメージ

図4 SSL通信の流れ（イメージ：忍者と道具屋の会話）

具体的には、文字単位の3.「忍びいろは」に似たビット単位の変換表を使って、ランダムなビット列（暗号文）に変換します（図2）。変換過程で、秘密のビット列（共通鍵と呼ぶ）を計算に使うため、秘密の共通鍵を知るユーザ/ショッピングサイトのみが、元のメッセージを復元できます。

また、認証（①、②）した相手と通信を行う場合でも、通信途中でメッセージ内の注文情報が不正に書換えられると、誤って高額を請求される等の恐れがあります。こうした事態を回避するために、メッセージの正しさを保証するメッセージ認証を行います。具体的には、メッセージを（一方通行的に）圧縮して生成される認証用ビット列を、メッセージに添付します。圧縮時に、秘密のビット列を計算に使うことで、秘密を知るユーザ/ショッピングサイトのみが、添付の認証用ビット列を検算し、メッセージが不正に変更されていないと確認できます。

④鍵交換

ユーザ/ショッピングサイト間の通信で、暗号化/認証（①～③）を実現するためには、パスワード/共通鍵等の秘密を事前に共有する必要があります。インターネット上では初めて通信する相手が多く、新しいショッピングサイトを使うたびに、口頭で共通鍵等を伝えることは現実的ではありません。このため、インターネット上で安全に共通鍵等を配送する、鍵交換の技術が利用されます。

以上、技術的ポイント①～④を組み合わせて、HTTPS/SSL通信は実現されています（図4は組合せ方法の一例です）。

5. むすび

アプリ/Webサービスの裏側で、縁の下の忍者として通信を守るSSLを紹介しました。あなたのスマートフォンの中でも、忍者SSLが今も頑張っているかもしれません。