

なるほど the デジタル

[第9回] 暗号化通信について

【問合せ】 秘書広報課デジタル化推進班 ☎74-8201

今回は、「暗号化通信」についてお話しします。

インターネットでの買い物や手続きを支えているのが「暗号化通信」です。住所・氏名などの個人情報や、 決済に必要なクレジットカード番号などが第三者に盗 み見されないようにする仕組みです。

実際に暗号化通信が適用されているサイトであるかどうかは、URLが「https」から始まっていることや、アドレスの入力欄に鍵マークが表示されていることで確認できます。以前は、個人情報などを扱う場合に限り暗号化通信を行っていました。現在ではサイト全体での暗号化通信が一般的となっており、暗号化されていないサイトの場合には「安全ではありません」のような警告が表示されるようになっています。

また、認証局と呼ばれる第三者機関が組織の実態などを調査の上、サーバー証明書を発行しているので、暗号化通信以外にも「なりすまし」でないということが証明されており、一層の安心にもつながっています。



暗号化通信の仕組み

クライアント(ユーザー端末)



- ①「暗号化通信」をリクエスト
- ②自分の「サーバー証明書」 と「公開鍵」を送信





- ③受け取った「サーバー証明書」 にある組織情報が、リクエス ト先と一致することを確認
- ④以降の通信で暗号化と復号化に 使う「共通鍵」を作成し、これを② の「公開鍵」により暗号化し、送信
- ⑤自分の持つ「公開鍵に対応する秘密鍵」を使って④の「共通鍵」を復号化
- (暗号化されたデータを元に 戻すこと。「公開鍵」で暗号化 されたデータは、それに対応 する「秘密鍵」でのみ復号化で きます。)
- ⑥クライアントとサーバーの両方で上記の「共通鍵」を使用し、データの暗号化・復号化を行いながら通信を行う。

昨年7月からスタートしたこのコーナーの本紙での掲載は、今回までとなります。 次回以降は市ホームページに掲載しますので、引き続きご愛読ください。

