




計装豆知識

セキュア通信について

インターネット通信の様々なリスクを回避することができるセキュア通信についてご説明します。

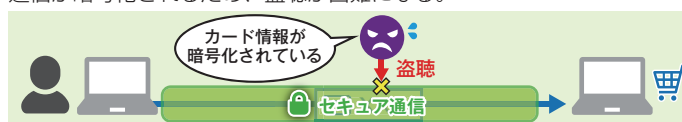

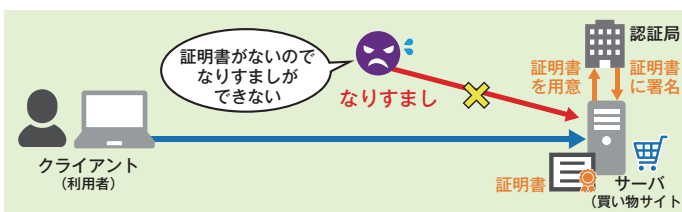
通信のリスク

我々は日々インターネット通信を利用していますが、これには様々なリスクが伴います。代表的な例として、以下のリスクが挙げられます。

想定されるリスク	内容
盗聴	攻撃者が通信を傍受し、情報を盗み見すること。 (例) 買い物サイトとの通信データ内にあるキャッシュカード情報が盗み取られる。 
改ざん	攻撃者が通信データを改ざんすること。 (例) 送信したメールの内容が書き換えられて先方に届く。 
なりすまし	攻撃者がサイト運営者になりますこと。 (例) 買い物サイトと似た画面の偽サイトに誘導され、ログイン名・パスワード等の個人情報が盗まれる。 

TLS

セキュア通信の実現手段としては、TLS (Transport Layer Security) があります。TLSを導入することで、上記リスクに対応することができます。

想定されるリスク	TLS 導入後
盗聴	通信が暗号化されるため、盗聴が困難になる。 
改ざん	改ざんを検知する仕組みが入っているため、改ざんがあればわかります。 
なりすまし	サーバ(買い物サイト)は自身の身元を記した証明書(*1)を用意し、第三者の認証局に署名(*2)を依頼する。認証局は依頼者の存在やURL(*3)等の身元確認を行った後、証明書を署名する。サーバはクライアント(利用者)からの接続毎にこの署名付き証明書を渡し、これを受け取ったクライアントは接続したサーバが目的のものであることを確認できる。 

HTTP、FTPにTLSを適用したものが、それぞれHTTPS、FTPSとなります。TLSを用いたセキュア通信プロトコルは上記の例以外にも多数あり、広く利用されています。

注意事項

ブラウザでHTTPSサーバに接続すると、URLの横に鍵マーク(🔒)が表示されます(図1)。鍵マークの表示によって、ユーザはセキュリティが確保されていることを認識できます。しかし、鍵マークが付いているからと言って絶対に安全という訳ではありません。TLS環境下においても、以下の注意が必要です。

- ① ブラウザに入力したURLが悪意のあるサイトのものであっても、鍵マークが表示される場合がある。URLに間違いがないことの確認が常に必要。
- ② ログイン名やパスワードが流出した場合、不正アクセスされるリスクは残る。引き続き、定期的なパスワード変更が必要。



図1 ブラウザで表示されるURLの鍵マーク

エム・システム技研のセキュア通信対応製品

•IoT用端末 データマル® タイプE (写真1)

データマルは、Web画面による遠隔監視機能、データロギング機能、イベント通報機能などを備えたIoT用端末です。**データマル タイプE** (形式: DL8-E) は、セキュア通信機能(HTTPS、FTPS)を搭載しています(*4)。

•現場設置形データロガー Webロガー2 高機能仕様タイプ(写真2)

Webロガー2は、Web画面による遠隔監視機能、データロギング機能、イベント通報機能に加え帳票の作成機能などを備えた現場設置形のデータロガーです。**Webロガー2 高機能仕様タイプ** (形式: DL30-G) は、セキュア通信機能(HTTPS、FTPS)を搭載しています(*4)。



< 参考文献 >

- IPA (情報処理推進機構) PKI関連技術情報
<https://www.ipa.go.jp/security/pki/index.html>
 グローバルサイン 電子証明書とは?
<https://jp.globalsign.com/ssl-pki-info/pki/digitalcertificate.html>

- (*1) 証明書: 名前やURL等が記された、インターネット上の身分証明書に該当する電子データ(電子証明書)。有効期限がある。
 (*2) 署名: 認証局が証明書に署名データを付加すること。これにより、証明書の改ざんを検出できる。また、署名がその認証局のものであることは誰でも確認できる(認証局の証明書が必要)が、署名はその認証局にしかできない。
 (*3) URL (Uniform Resource Locator):
 [https://www.m-system.co.jp]のように、インターネット上の住所に該当するもの。
 (*4) セキュア通信機能を利用するには、ローカル認証局作成支援ソフトウェアを使用します。ソフトウェアは、エム・システム技研のホームページから無料でダウンロードできます。

【(株)エム・システム技研 開発部】