**HTTPSについて**

**HTTPSとは**

HTTP over SSL/TLSの略でHTTP通信において暗号化形式であるSSL(Secure Sockets Layer)やTLS(Transport Layer Security)を利用することでWebサイトを安全に使用できるプロトコル

**SSL/TLSの役割**

・Webサイトを閲覧する際に、万が一傍受されても内容を解読させないためにデータを暗号化し、第三者からの盗聴を防ぐ。

A97%dqk5

暗号化されていて盗聴

してもわからない

椅子を1つ注文

椅子を1つ注文

復号化

暗号化



Webサーバ



Webブラウザ

・データの改ざん対策として、メッセージダイジェストが利用される。メッセージダイジェストを使用することで、データ送信時にハッシュ値を比較して改ざんを検知できる。

椅子を5つ注文

データを改ざん



Webブラウザ



Webサーバ

椅子を1つ注文

椅子を5つ注文

xyz

abc

abc

比較

ダイジェスト

・WebサーバにSSLサーバ証明書を設置し接続時に検証することで、Webサイトを運営する会社の身元を確認することができる。また、SSLサーバ証明書は発行が認められた認証局による運営元の認証作業を通過する必要があり、信頼できない発行元のSSLサーバ証明書が利用されている場合はWebブラウザ上に警告画面が出る。



Webブラウザ

HTTPS通信の開始

証明書



Webサーバ

**SSL/TLSハンドシェイク**

1. 暗号化方式の決定やHTTPSで利用されるSSLまたはTLSのバージョンやメッセージダイジェストの方式を決定。
2. Webブラウザが通信しているWebサーバが正しい相手なのかどうかSSLサーバ証明書により確認。正しいWebサーバであることが確認できなかった場合、Webブラウザ上に警告が表示される。
3. データ転送に利用する鍵を交換する鍵はデータを転送する際の暗号化、復号化に利用される。
4. 実際に利用する暗号化方式の最終確認を行う。完了するとWebブラウザとWebサーバ間において暗号化通信が開始される。

○SSL/TLSハンドシェイクの流れ

通信相手の証明

鍵の交換

暗号化方式の確認

暗号化方式の決定

データ暗号化用の鍵を送る

こんな暗号化方式が使える

この暗号化方式を使おう

決めた暗号化方式でデータを転送

SSLサーバ証明書見せる

私の情報全部送った

こんな暗号化方式で暗号化しよう

準備OK

この暗号化で大丈夫

準備OK



Webサーバ



Webブラウザ