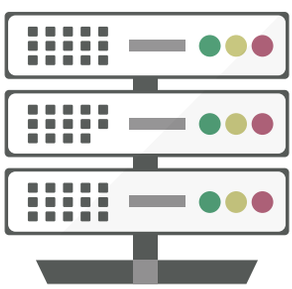
ホームページ閲覧時の暗号化通信 (PC⇔サーバ) の流れ

パソコンで暗号化されたホームページを閲覧するときは
下記のような流れで通信が行われます。
※暗号化されたホームページは URL が https からはじまります。

パソコン

サーバ



1.https のサイトにアクセス！

2. 電子証明書を送信
※認証局により電子署名されている
中には公開鍵が含まれている

3.2 で送られてきた電子証明書の
中の公開鍵を確認

4.Web ブラウザが共通鍵を作成

5.3 で届いたサーバの公開鍵で
4 の共通鍵を暗号化

6. 暗号化された共通鍵を送信

7. サーバの秘密鍵で復号

8.Web ブラウザが作成
した共通鍵を確認

暗号化通信スタート！