SSLプロトコル

2001/10/25

兼子　譲

SSL(Secure Socket Layer)

- Netscape Communications Corporationが提唱
- アプリケーション層とTCP/IPとの間にデータセキュリティ層を提供
  - Webブラウザとサーバ間の暗号通信技術
  - 電子メール
  - LDAPディレクトリサービス

SSLプロトコルの概要

- 機密性
  - 共有鍵暗号を用いて通信データの暗号化
- 相手認証
  - 公開鍵暗号を用いたサーバ認証とクライアント認証
- 完全性
  - ハッシュ関数を用いてMAC(Massage Authentication Code)を計算して改ざんを検出

SSLプロトコル

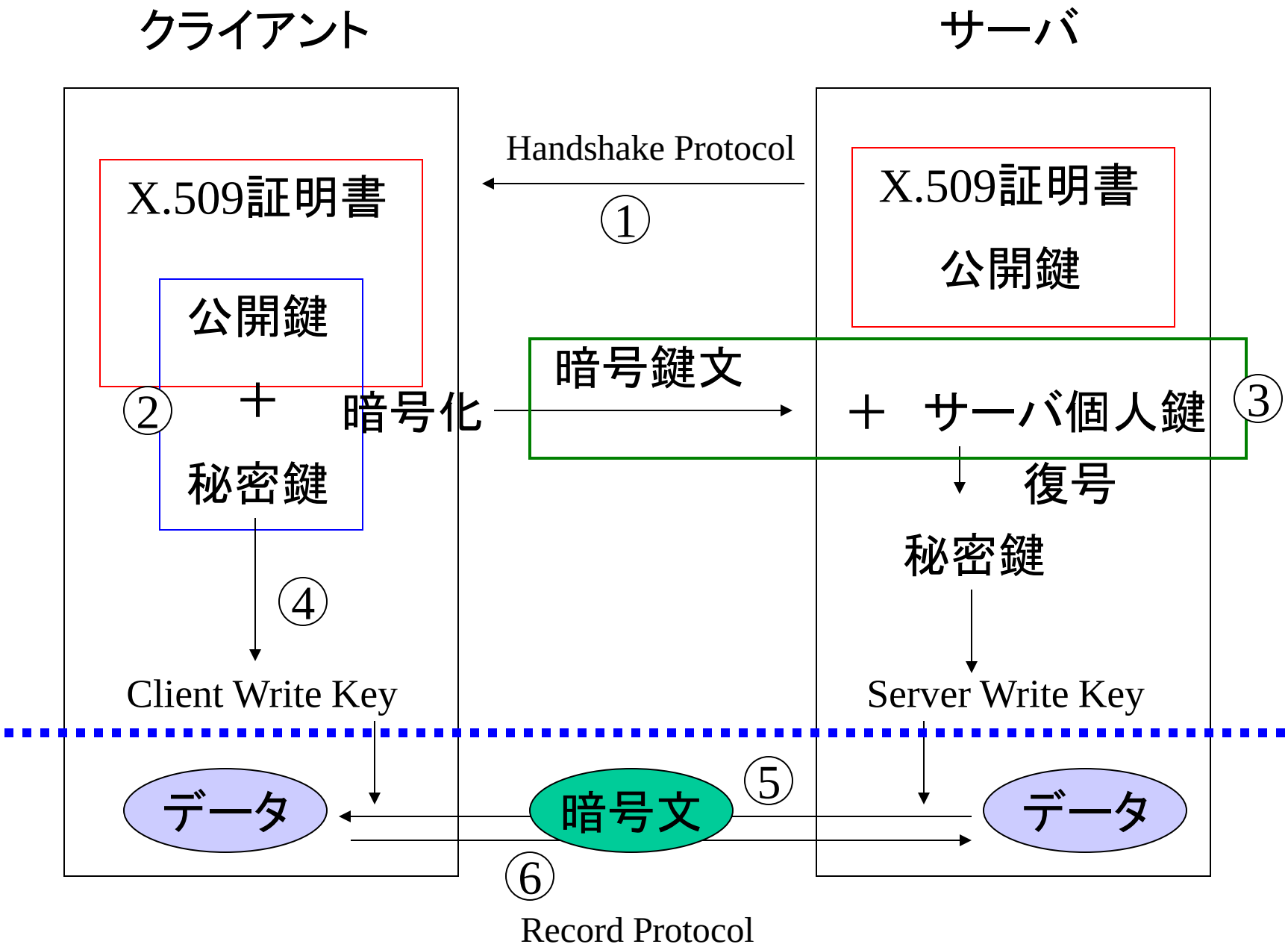
- SSL Recordプロトコル
  - データの暗号化
  - データの完全性
- SSL Handshakeプロトコル
  - プロトコルのバージョン
  - 暗号化アルゴリズムのネゴシエーション
  - サーバ認証・クライアント認証
    - X.509証明書を用いて認証

SSL Handshake Protocol

1. クライアントがサーバにアクセスすると、クライアントに対してサーバの証明書を送付
2. クライアントは受信したX.509サーバ証明書を確認し、格納されている公開鍵で秘密鍵を暗号化して返送
3. サーバはクライアントから受信した秘密鍵をサーバ個人鍵で復号
4. サーバとクライアントは秘密鍵からサーバ用、クライアント用の秘密鍵(Server Write Key , Client Write Key)を生成

SSL Record Protocol

5. サーバはServer Write Keyで暗号化してデータを送信し、クライアントのServer Write Keyを用いて復号
6. クライアントの送信するデータについてはClient Write Keyを使用


クライアント
サーバ
Handshake Protocol
①
X.509証明書
公開鍵
X.509証明書
公開鍵
暗号鍵文
②
＋
暗号化
＋ サーバ個人鍵
③
復号
秘密鍵
秘密鍵
④
Client Write Key
Server Write Key
データ
暗号文
⑤
データ
⑥
Record Protocol