CookieのSecure属性とHttpOnly属性

2013/08/24
第7回カスタムWeb勉強会発表資料

松尾 篤（株式会社エミック）

株式会社エミック

HTTP Cookie

- RFC 6265などで定義されたHTTPにおけるウェブサーバとウェブブラウザ間で状態を管理するプロトコル、またそこで用いられるウェブブラウザに保存された情報のことを指す。（Wikipediaより引用）

Set-Cookieヘッダー

- HTTPではSet-Cookieヘッダーを使用してWebサーバーがWebブラウザーにCookieを発行

Cookieヘッダー

- HTTPではCookieヘッダーを使用して
  WebブラウザーがWebサーバーにCookie
  を送信

セキュリティ関連の属性

- Secure属性
- HttpOnly属性

Secure属性

- Cookieにこの属性が設定されている場合、WebブラウザーはHTTPSによる通信時のみCookieをWebサーバーに送信する

HttpOnly属性

- Cookieにこの属性が設定されている場合、Webブラウザーでクライアント側のスクリプト（JavaScript等）経由でCookieに保存されているデータを読み出すことができなくなる

まとめ

- Secure属性とHttpOnly属性を使用すると、Cookieの盗難につながるクロスサイトスクリプティングによる脅威を軽減できる

関連URL

- http://ja.wikipedia.org/wiki/HTTP_cookie
- http://tools.ietf.org/html/rfc6265