Firefox3.0を用いたCamelliaでのSSL通信方法

マルチプラットフォーム型共通鍵ブロック暗号

NTT 情報流通プラットフォーム研究所　2008/06/19 版

この資料は、共通鍵ブロック暗号”Camellia”のユーザーズガイドです。Camellia は、NTT と三菱電機が共同で開発した暗号で、ソフトウェア実装、ハードウェア実装を問わず、さまざまな環境で世界トップクラスの安全性・処理性能を実現します。その Camellia が Firefox3.0 に搭載されたことで、Camellia による SSL 通信が実現できるようになりました。

本ガイドでは、日ごろインターネットをブラウジングされる方を対象とし、ブラウザに Firefox3.0 を使用して、暗号化に Camellia を利用した SSL 通信でのインターネットブラウジングについて紹介します。使用した感想や気になった点等がございましたら、ご一報いただければ幸いです。

なお、詳細な情報については、文中に参照先を記載しましたので、そちらを参考にして下さい。

オープンソース Camellia とは

Camellia は、欧州連合推奨暗号選定プロジェクト NESSIE において、米国政府標準暗号 AES(Advanced Encryption Standard)同等と国際的に認められた純国産暗号です。

2006 年 4 月 13 日より、NTT 製の Camellia のソースコードが、マルチプルライセンス形式のオープンソースとして以下のサイトで公開されました。

■サイト名：NTT の暗号要素技術 > Camellia
http://info.isl.ntt.co.jp/crypt/camellia/index.html

Camellia の Firefox への搭載

国際的なオープンソース・コミュニティである Mozilla Foundation が提供する Firefox のバージョン 3.0 以降に、Camellia が搭載されました。これにより、OpenSSL 0.9.8c 以降を利用するなどして、Camellia をサポートした SSL サーバとの間で Camellia を利用した SSL 通信が可能になります。

Firefox3.0 のインストール方法

はじめに、Camellia が搭載された Firefox3.0 のインストール方法について説明します。

本ガイドでは、Windows 上でのインストール方法を例示しています。

Firefox3.0 のダウンロード

以下の Mozilla Japan サイトから、日本語版 Firefox3.0 をダウンロードして、インストールしてください。詳細は、以下のサイトを参照ください。

■Mozilla Japan：http://mozilla.jp/

Camellia 対応 SSL サーバへの接続

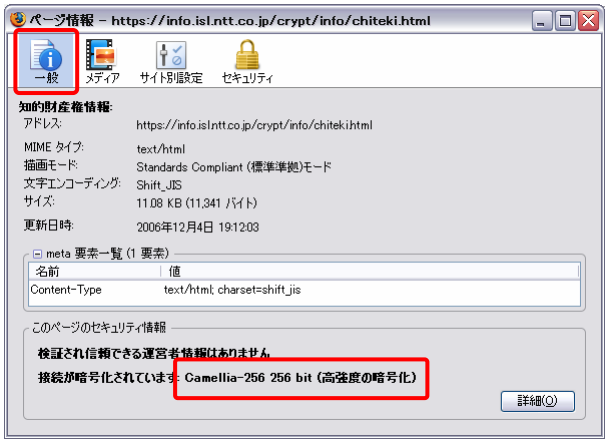
SSL 通信では、サーバ（SSL サーバ）とクライアント（ブラウザ）のネゴシエーションによって利用する暗号を 1 つ決定します。Firefox3.0 を使って Camellia を利用した SSL 通信をするためには、Camellia をサポートした SSL サーバへ接続する必要があります。以下に、Camellia を利用した SSL 通信方法について、NTT のサイトを例に説明します。Firefox3.0 を起動して、以下のアドレスを指定してください。

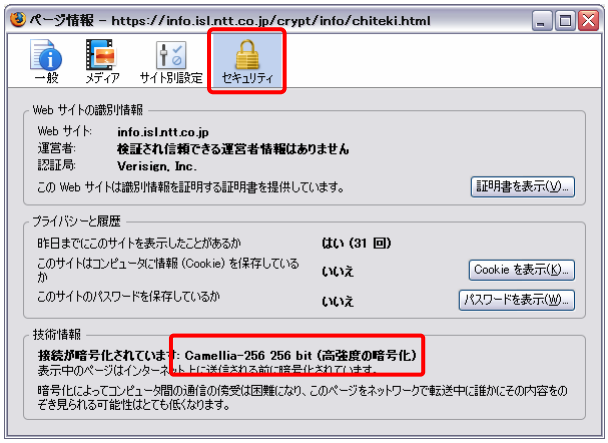
■サイト名：NTT の暗号要素技術 > Camellia

https://info.isl.ntt.co.jp/crypt/camellia/index.html

SSL 通信で使用されている暗号の確認

上記の画面が表示された状態で、メニューバーの“ツール”－“ページの情報”を選択してページ情報を表示してください。ページ情報の一般アイコンかセキュリティアイコンをクリックして、使用している暗号を確認することができます。





Camellia を利用した製品の例

Camellia を利用した製品には、Web でのコンテンツ配信をセキュア化する製品、メールを暗号化する製品、送受信データを暗号化する製品等があります。以下に、その一部を紹介します。

(1) NTT ソフトウェア株式会社

CipherCraft　高速暗号認証ライブラリ

CipherCraft/Mail　セキュリティ暗号メールソフトウェア

CipherCraft/VPN　暗号通信パッケージソフトウェア

CipherCraft/File　ファイル暗号化ソフトウェア

(2) NTT エレクトロニクス株式会社

Camellia-LSI　暗号 LSI

NA5000　IP インタフェース装置

SU1000　IP 超小型 MPEG-2 コーデック

(3) 三菱電機株式会社

MistyGuard(R) < CRYPTOFILE(R) PLUS > Ver.1.30　ファイル暗号ソフトウェア

PowerMISTY(R)　暗号ライブラリ

MCrypto　PKI 暗号ライブラリ

MC　組み込み機器向け暗号ライブラリ

セキュリティ暗号 LSI 開発用暗号アルゴリズム IP　LSI 開発用設計情報

(4) 日本セーフネット株式会社

QuickSec Toolkit　IPsec 組込用ツールキット

(5) nCipher Corporation Ltd

net HSM　ネットワーク型ハードウェアセキュアモジュール　(Network-attached Hardware Security Module)

nShield series　PCI 型ハードウェアセキュアモジュール (Hardware Security Module)

miniHSM　組込型ハードウェアセキュアモジュール (Embedded Hardware Security Module)

(6) 松下電工株式会社

NetCocoon Analyzer　IPsec/SSL 暗号通信プロトコル解析ツール

Camellia に関する情報の入手方法

Camellia に関する最新情報や紹介記事等は、次のサイトから入手することができます。

■サイト名：NTT の暗号要素技術 > Camellia

http://info.isl.ntt.co.jp/crypt/camellia/index.html

■Camellia に関する情報

- ●Camellia に関するニュースリリース・関連記事
- ●Camellia の紹介
- ●標準化情報(Camellia を認定した標準化団体等)
- ●Camellia を採用したセキュリティ製品の紹介
- ●Camellia 仕様書等の技術情報

■本件問い合わせ先：camellia@lab.ntt.co.jp