New Technology Report

高機能iモード携帯機特集

iモードにおけるセキュリティ
−SSL(Secure Sockets Layer)−

503iではSSLを搭載することでiモード通信におけるセキュリティの強化を図った．SSLは，「成りすまし」「盗聴」「改竄」といったデータ通信に潜む攻撃から，安全性を確保するプロトコルである．

本稿では，iモードにおけるSSLのシステムおよび実装を概説する．

大井 達郎　平松 孝朗　井上 恭子

1. まえがき

近年，インターネット上で注目を集めているECなどのトランザクション系サイトは，そのサービスの実現において，安全な通信路を確保することが前提条件となる．

iモードにおいても，当初より多数のトランザクション系サイトがサービスを展開しており，サービスを拡張するために不可欠であるiモードのセキュリティ強化に対し，強い関心を抱いていた．また，従来のiモードサービスでは，公式サイトの中でセキュリティを重視するプロバイダに対し，コンテンツサーバ〜iモードサーバ間，iモードサーバ〜携帯機間において，それぞれ別のプロトコル／アルゴリズムを提供してきたが，安全な通信路としては不連続であった．

そのため，コンテンツサーバ〜携帯機間（end to end）における連続的，かつ安全な通信路の構築が課題とされていた．

このような背景において，503iではSSL（Secure Sockets Layer）を搭載することにより，end to endのセキュリティを確保した通信プラットフォームを実現した．

本稿では，まず一般的なSSL機能について簡単に述べ，その後，iモードに特化したSSL仕様を中心にシステムおよび実装について述べる．

2. SSL機能概要

SSLは「成りすまし防止」「盗聴防止」「改竄防止」機能を有することを特徴とする[1],[2].

2.1　成りすまし防止

SSLでは，所望の相手との暗号化通信を開始する前に，相手方の証明書を検証し，身元を確認することで，第三者による成りすましを防止する．証明書のデータフォーマットは，ITU-T（International Telecommunication Union-Telecommunication Standardization Sector）勧告X.509[3]で規定されており，図1に示す構造を有する．証明書の検証においては，公開鍵暗号方式が用いられ，秘密鍵で暗号化された署名部を公開鍵で復号化することで，証明書の発行者を確定する．また，一方でハッシュ関数と呼ばれる一方向関数を用いて，証明書データのメッセージダイジェストを算出し，復号された署名部と比較を行い，証明書が改竄されているか否かを検証する．

2.2　盗聴防止

通信相手の身元が確認されると，暗号化／復号化に使用される共通鍵が双方で生成される．それ以降のデータは共通鍵暗号方式により暗号化されるため，悪意を持った第三者が通信路に介在したとしても，共通鍵を所持しない限りは送信データを解読することはできない．共通鍵生成手順の簡略図を図2に示す．

2.3　改竄防止

通信路に介在する第三者は，暗号化データに対し，内容を解読することはできないが，データ自体を改竄することは可能である．改竄に関しては，未然に防ぐことはできないが，SSLでは送信データにMAC（Message Authentication Code）データを付加することで，データが改竄されているか否かを検出することが可能である．MACデータとは双方が秘密に持つMACシークレットと送信データの本文をハッシュ関数により算出した値である．第三者はMACデータよりMACシークレットや送信データの本文を知ることはできない．

3. システム構成

iモードにおけるSSLサービスの実現において必要なシステム構成を以下に概説する．

3.1　プロトコルスタック

図3に示すようにSSLはTL（Transport Layer）の上位レイヤに位置し，AL（Application Layer）レイヤ以上のデータを暗号化する．SSLの利用は，ALからの要求によって行われ，ALはSSLを介さずに直接TLを利用することも可能である．また，SSLプロトコル自体，TLの直上に置かれるRecord Layerプロトコルと Handshake／Alert／Change Cipher Specプロトコルの2層に分かれる．Handshakeプロトコルは暗号化通信を開始する前に，相手の身元確認や暗号化アルゴリズムを決定するなどのネゴシエーションを司る．また，Record Layerプロトコルは，渡されたデータを2^{14}バイト以下のブロックに分割し，これを必要な数のSSLデータユニットにまとめる．送信時の分割および受信時の組み立てはRecord Layerプロトコルによって Handshakeプロトコルには透過的に行われる．

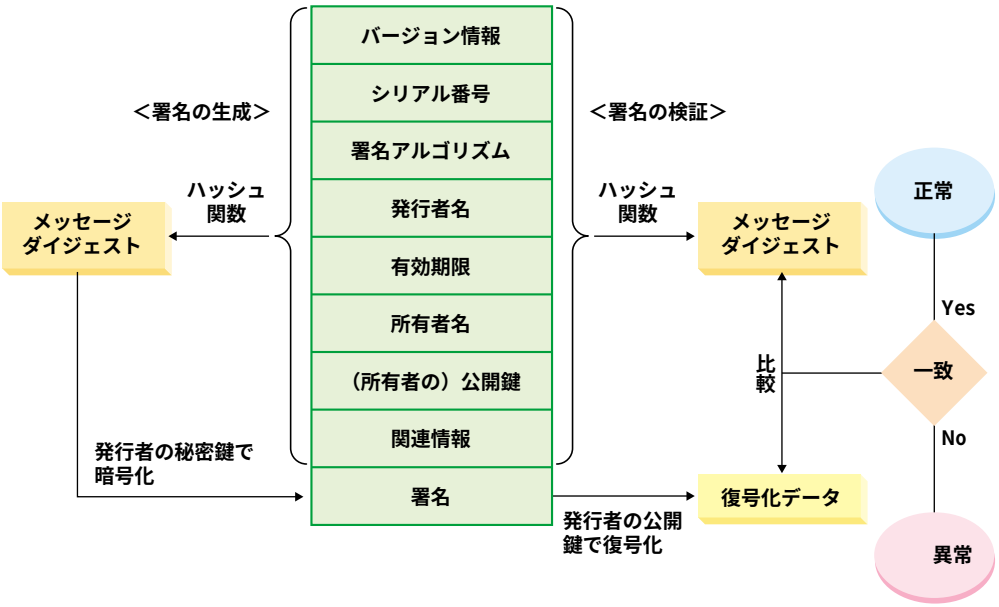

図1　X.509証明書

3.2　トンネリングプロトコル[4]

前述したように，従来においても，コンテンツサーバ～iモードサーバ間におけるSSL通信（以下，s-sSSL）はサービス提供されていた．しかし，503i以降の携帯機においては，コンテンツサーバ～携帯機間におけるSSL通信（以下，e-eSSL）サービスを提供することで，両サービスが利用可能なシステムを構築する必要がある．

iモードのシステムは，プロキシサーバ経由によるインタ

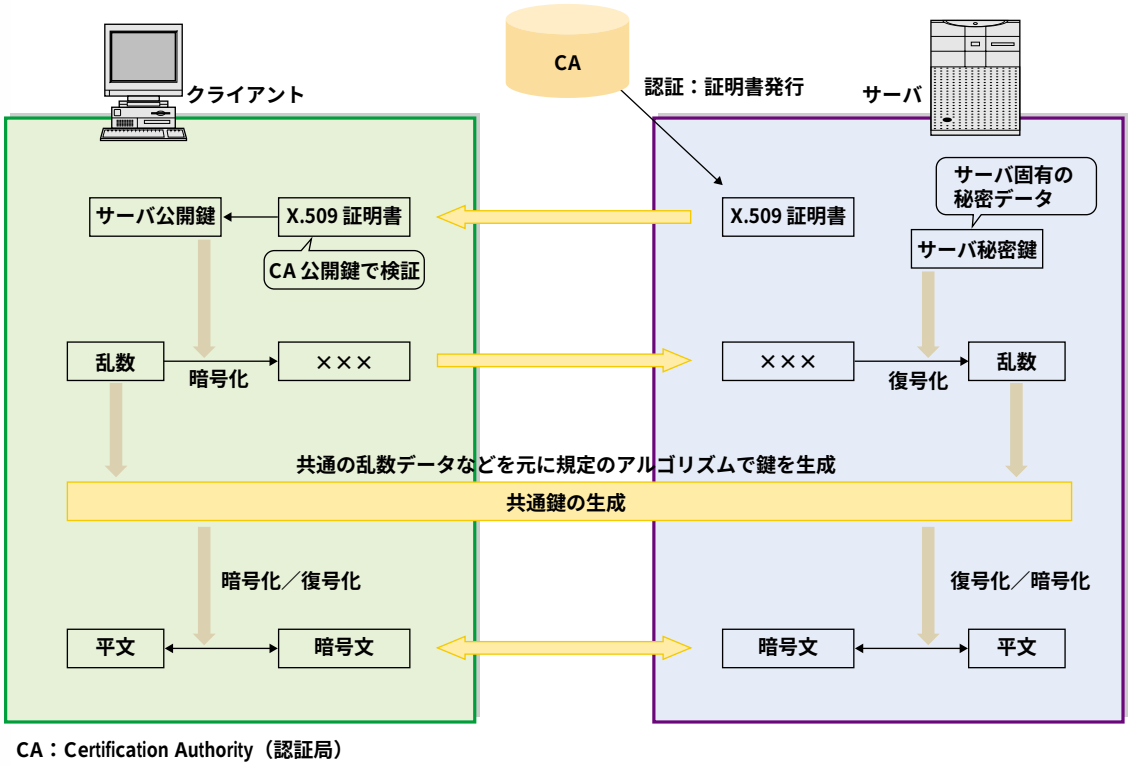

図2　共通鍵生成手順

ーネット接続である．それゆえ，e-eSSLの実現にあたり，プロキシに対し透過的に通信を行う必要があるため，トンネリングプロトコルを採用している．503i携帯機は接続先のURLのスキームが「https」であると，接続先に対しHTTPリクエストを送信する前に，iモードサーバに対し接続先のURL情報を付加したトンネリング要求を送信する．iモードサーバはURL情報に従い，トンネリングを許容するか否かを判断し，結果を携帯機に返信する．

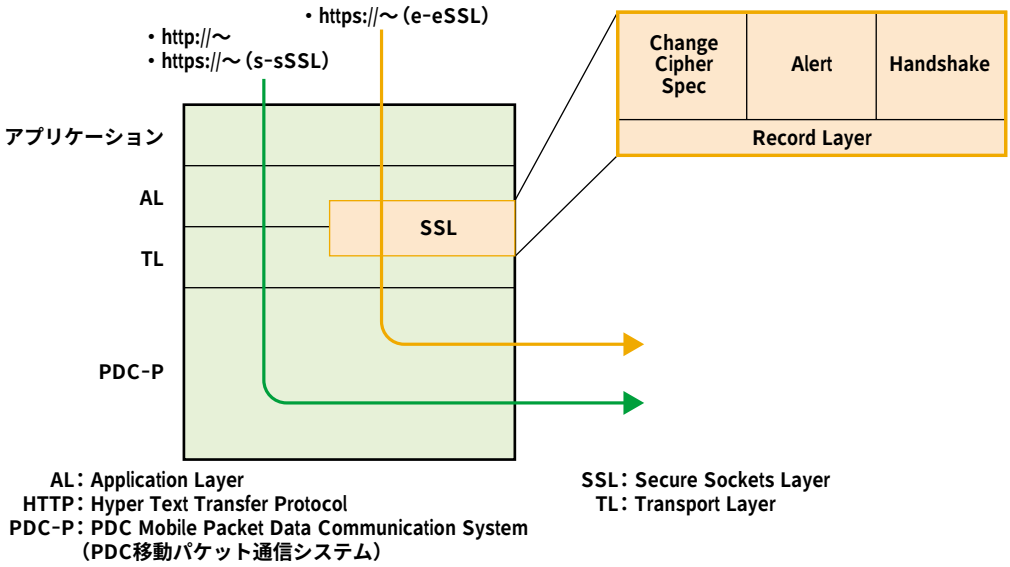

図3　プロトコルスタック

（1）　s-sSSL

iモードサーバは，事前にs-sSSLサービスを希望するコンテンツプロバイダのURLをデータベースで管理しているため，トンネリング要求の接続先URLがs-sSSLサービス該当のサーバであると，携帯機に対しトンネリング要求を拒否する．トンネリング要求が拒否されると，携帯機は接続方式をs-sSSLと認識し，502i携帯機などと同様にSSLを介さずに，HTTPリクエストをiモードサーバに送信する．

HTTPリクエストを受信したiモードサーバは，URLのスキーム（https）からSSL通信であることを判断し，SSLセッションを確立後，コンテンツサーバに対しHTTPリクエストを送信する．

図4にs-sSSL接続におけるSSLv3利用時のシーケンスを示す．

（2）　e-eSSL

一方で，iモードサーバは，トンネリング要求の接続先

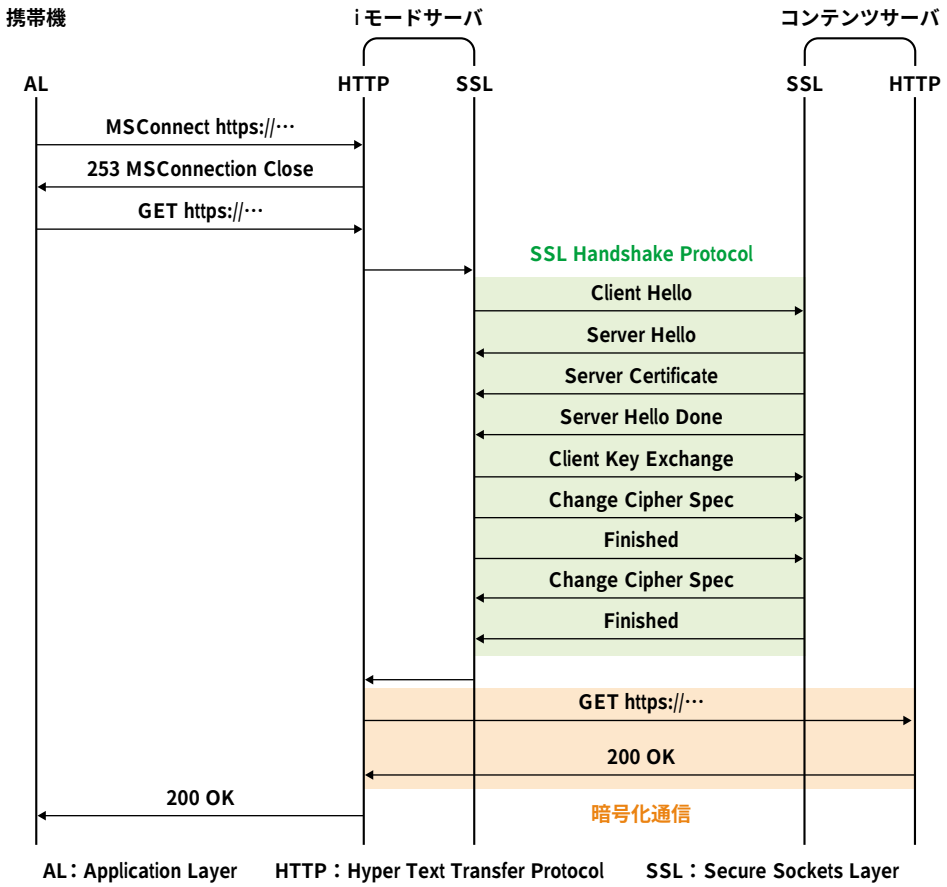

図4　s-sSSLシーケンス

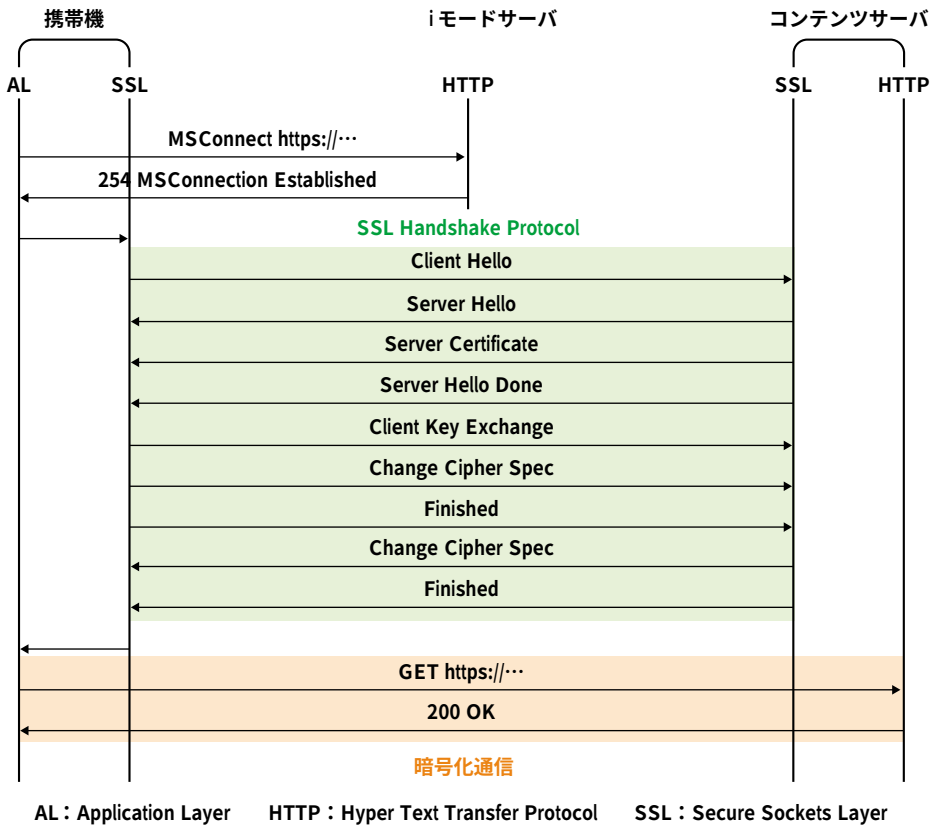

図5　e-eSSLシーケンス

URLがデータベース上にない場合，トンネリング要求を許容する．トンネリング要求が許容されると，携帯機は接続方式をe-eSSLと認識し，SSLセッションを確立後，HTTPリクエストをコンテンツサーバに送信する．トンネリング要求が許容された以降の通信はiモードサーバには，透過的に行われるため，end to endにおいて，連続的かつ安全な通信路が提供される．

図5にe-eSSL接続におけるSSLv3利用時のシーケンスを示す．

4. 携帯機の実装仕様

本章では，503i携帯機におけるSSLの実装仕様について概説する．

4.1　スペック

503i携帯機の対応する主要スペックを表1に示す．

4.2　ユーザインタフェース機能

SSL通信は，比較的セキュリティが必要とされる通信に利用される．そのため，ユーザに対し，その接続がSSLを利用しているか否かを認識できるよう配慮する必要がある．そこで503iにおいては，以下のような各種表示機能を規定している．

(1)　通信中／閲覧中メッセージ

SSL通信中においては，それが暗号化通信であることを示すワーディングを表示する．また取得したコンテンツがブラウザ上に表示されている際には，SSLピクトを点灯させる（図6）．

(2)　警告メッセージ

ユーザがSSL対応コンテンツの閲覧を終了する際には，以後の接続先もしくは閲覧先がSSLに対応していないことを警告することで，SSLの終了を認識させる．

(3)　エラーメッセージ

図6　SSLピクト

SSLにおいて，その安全性が確保できないような致命的なエラーが発生した場合，通信を切断しユーザに通知する．また，今回503i携帯機に実装する認証局（CA：Certification Authority）証明書は表1に示すもののみであり，他のCAに認証されたサイトに関しては，「このサイトは安全でない可能性があります．接続しますか？」というメッセージを表示し，ユーザに接続の判断を促す．

(4)　証明書参照機能

閲覧中のコンテンツに対しては，取得先サーバの証明書を参照できる機能を有することで，パスワードなどの秘密情報を送信する際，ユーザが送信先を明確に認識することを可能にしている．

5. あとがき

iモードにおけるSSLのシステムおよび実装を概説した．今後は，より高度な認証技術を取り入れ，よりセキュリティの高い通信プラットフォームを提供することが課題である．

用語一覧

AL：Application Layer
CA：Certification Authority（認証局）
HTTP：Hyper Text Transfer Protocol
ITU-T：International Telecommunication Union-Telecommunication Standardization Sector（国際電気通信連合・電気通信標準化部門）
MAC：Message Authentication Code
MS：Mobile Station（携帯機）
PDC-P：PDC Mobile Packet Data Communication System（PDC移動パケット通信システム）
SSL：Secure Sockets Layer
TL：Transport Layer

表1　503i携帯機主要スペック

バージョン	SSLv2，SSLv3
必須最大鍵長（共通鍵）	128bit
必須最大鍵長（公開鍵）	1024bit
認証機能	サーバ認証
実装CA証明書	VeriSign Class3 Primary CA
	VeriSign Class3 Primary CA G2
	RSA Secure Server CA
	GTE Cyber Trust Root
	GTE Global Root

CA：Certification Authority（認証局）
SSL：Secure Sockets Layer

文　献

[1] A.O.Freier, P.Karlton, P.C.Kocher, “The SSL Protocol Version 3.0”, draft-freier-ssl-version3-02.txt, Nov.1996.
[2] http://www.netscape.com/eng/security/ssl_2.html
[3] R.Housley, W.Ford, W.Polk, D.Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile”, RFC2459, Jan.1999.
[4] A.Luotonen, “Tunneling SSL Through a WWW Proxy”,draft-luotonen-ssl-tunneling-02.txt,Dec.1995.