# FirstPassサービス概要

モバイルインターネット上でのサービス展開を活性化させるため，セキュリティを向上したクライアント認証を可能とする電子認証サービス「FirstPass」のサービスを設計した．

中村 典生　山本 博昭　小野川 雅士

## 1. まえがき

携帯電話にモバイルインターネットアクセス機能が搭載されてから，携帯電話が扱えるコンテンツ種別が多様化し，携帯端末の入出力インタフェースも充実してきた．携帯電話の進化は，利用者の利便性を高めただけではなく，コンテンツ提供者や企業システム構築者（以下，CP（Contents Provider））のサービス展開を促進してきた．一方，第3世代携帯電話サービスFOMA（Freedom Of Mobile multimedia Access）は，2001年10月よりサービスを開始した後，2003年3月末には全国で約91％の人口カバー率を達成し，おおむね主要な市町村がエリア化されている．

また，2003年度には，FOMA端末の基本的な性能の充実や映像表示などの端末機能の拡充に加え，FOMAカード（UIM（User Identity Module））の高機能化による国際ローミング，IMT-2000（International Mobile Telecommunications-2000）/ディジタル携帯電話方式（PDC：Personal Digital Cellular）デュアル端末，電子認証機能などの新サービスを開始した．これらのFOMAの特性を活かす機能拡張により，モバイルインターネットサービスの幅がさらに広がり，その利用促進が期待されている．

本稿では，電子認証の市場動向，携帯電話に必要な電子認証機能，ならびに2003年6月からサービスを開始した電子認証サービス「FirstPass」の内容，運用方法および応用例について述べる．

## 2. 電子認証サービスの市場動向

携帯電話を利用したインターネットショッピング，株取引や企業内イントラネットへのリモートアクセスなど，いわゆるモバイルインターネットの利用形態の拡大に伴い，

個人認証による高いセキュリティの確保がますます重要になってきている．

インターネットを利用する社員向け情報共有や代理店との情報共有などの分野で厳密な個人認証の必要性が認識され，大規模な電子認証システムの導入が進んでいる[1]．また，2002年度からは，主なインターネットサービスプロバイダが会員向けにユーザ証明書発行サービスを開始し，コンシューマ向けのサービスにおける利用が広がってきている．さらに2001年4月に電子署名法，IT書面一括法が施行され，電子的な手段での署名，認証が法的に認められるようになり，行政サービスにおける利用拡大も期待される[2]．

ユーザ証明書は，現在でも数百万IDの規模で利用されており，今後も大きなニーズがあると思われるが，数年前に期待されていたほど普及していない．普及を妨げている主な原因としては，電子認証システムの導入・運用コストや，電子認証の操作性・使い勝手に問題があると報告されている[1]．この状況を打開できれば，電子認証が必要とされている領域は非常に広く，普及は急速に進むと思われる．

電子認証の最も一般的な実施形態は，SSL（Secure Sockets Layer）での利用である．SSLサーバ認証[*1]を行うサイト数は年々増え続けており，その何割かのサイトは携帯電話向けにもサービスを提供している．携帯電話向けサービスの大部分は，企業内あるいは企業間の情報システムを構成するサイトが提供していると思われるが，iモードにおけるコンシューマ向けサイトにも着実に利用数が拡大している．このようなSSLサーバ認証を行っている多数のサイトは，何らかの利用者認証も行っており，SSLクライアント認証を導入する下地は十分に整ってきている．

## 3. 携帯電話での電子認証に要求される機能条件

携帯電話での電子認証とは，携帯電話からインターネット上のさまざまなサービスサイトへアクセスする場合に，認証結果を「個人認証“鍵”」として用いるものである．ここでは，携帯電話で利用する電子認証に対する，サービス面から見た要求条件について述べる．

第1に，携帯電話におけるメモリ容量の制限から，複数のユーザ証明書を保持することは得策ではなく，1つのユーザ証明書を複数の用途に使いたいという要求がある．既存のユーザ証明書は，ほとんどが用途を限定したものである．例えば，暗号メールのためのメールアドレスの証明書や，特定のサービスを受けるためのIDの証明書がある．しかし，ユーザ証明書の記載内容が個人の属性（個人情報）や特定のサービスにかかわるものであると，CPにとっては都合が良いが，これは利用者にとって不利益となる．これでは，利用者が1つのユーザ証明書をさまざまな目的で使うことに適さない．すなわち，ユーザ証明書の記載内容は最少限にすべきであり，個々の利用者を識別するための識別情報にとどめるのが適当であるといえる．

第2に，携帯電話の利用者が誰でも使える簡便性と安全性が求められる．すなわち，電子認証技術やITの専門家でなくても理解できる簡単な操作でユーザ証明書が扱えることが重要である．着メロやiアプリなどを探したり，ダウンロードしたりする場合と同様にメニュー操作だけで，ユーザ証明書に関するすべての操作を完結できれば，利便性が高い．

通信時のクライアント認証は，利用者が慣れ親しんだID/パスワードによる認証を置き換えるものであり，需要も多く，何より利用者に受け入れられやすい．電子認証を応用したアプリケーションには，暗号化メールや電子署名，VPN（Virtual Private Network）など，さまざまなものがあるが，利用者が最も受け入れやすい認証方法としてSSLクライアント認証が有望といえる．

また，電子認証を基本的な機能としてすべての利用者が気軽に使えるようにするためには，認証によるコスト負担を小さくすること，プライバシーが保護されることや認証手段としての信頼性が保たれていることも重要な要件となる．

## 4. FirstPassにおける電子認証サービスの内容

ドコモでは，次のような電子認証サービス「FirstPass」を2003年6月28日より開始した．

### 4.1 概要

本サービスは，インターネット上で広く普及している公開鍵暗号基盤（PKI：Public Key Infrastructure）[3][*2]を使用し，ドコモがFOMA契約ごとに割り当てたユーザ証明書を発行し，高いセキュリティで保護されたFOMAカードにユーザ証明書を格納するものである．

FOMA利用者はFirstPass対応CPにユーザ証明書を送信することにより，サービスごとに複数のID/パスワードを管理する従来のID/パスワード認証よりもシンプルな操作で安全性の向上したインターネットアクセス（SSLクライアント認証）を行うことが可能となる．この場合，CPは，受信したユーザ証明書の有効性を確認するだけでよく，従来のパスワード認証などの認証方法に比べて第三者による“なりすまし”などのリスクを軽減することができる（図1）．

ユーザ証明書発行申請，ダウンロードはFirstPass対応

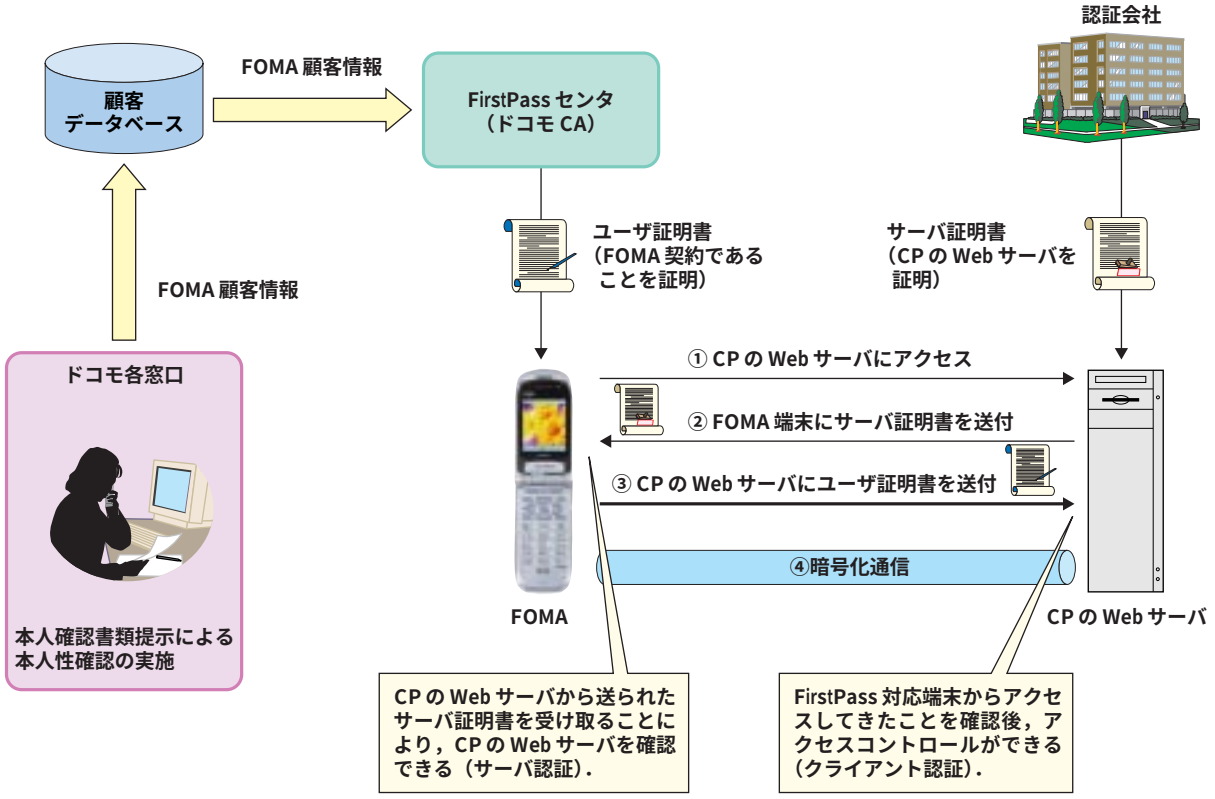


**図1　サービスイメージ**

FOMA端末に設けられたメニューから行う仕組みとした．これにより，FirstPassでは，パソコン用の証明書を一般のPKIベンダやサービスプロバイダに申し込む場合発生する本人性確認のための書類送付やメール送信などの煩雑な手続きが不必要となる．なぜならば，ドコモではFOMA新規契約時に本人性確認を実施しており，ユーザ証明書の発行は顧客データベースと連携しているため，FOMA端末の操作だけでユーザ証明書発行申請からユーザ証明書ダウンロードまでを実現できる．

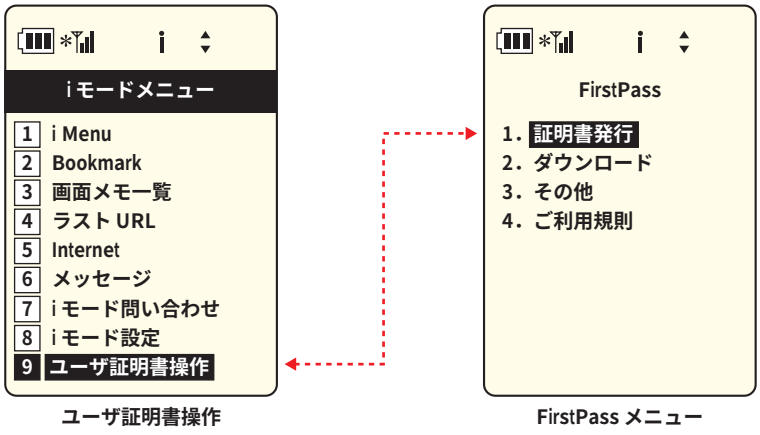


**図2　ユーザ証明書の取得操作**

ユーザ証明書発行申請からユーザ証明書ダウンロード，FOMAカードへの保管，ユーザ証明書利用までの機能がFOMA端末の操作に集約されているため，安全性・利便性を高め，トータルコストを低く抑えられている．これらの具体的手法については本特集中，後稿[4]で述べる．

## 4.2 ユーザ証明書の取得

FirstPass対応FOMA端末のiモードメニュー内「ユーザ証明書操作」を選択することにより，FirstPassセンタに接続し，ユーザ証明書発行申請およびダウンロードを行うことができる（図2）．

## 4.3 ユーザ証明書の失効

ユーザ証明書を第三者に悪用されることを防ぐために，FirstPassではユーザ証明書の失効を行うことができる．失効はユーザ証明書取得と同様，FOMA端末操作で行えるようにした．また，FOMAカード紛失時でも失効ができるように利用者からの失効依頼を受け付ける体制も構築している．

## 4.4 ユーザ証明書失効リストの発行

FirstPass対応CPにユーザ証明書の失効リスト（CRL：Certificate Revocation List）を提供する．失効申請されたユーザ証明書の情報はFirstPassセンタで一括管理し，1日1

回CRLとして発行される．CPはユーザからのアクセスの際にユーザ証明書が利用可能か否かを検証する目的で，このCRLを利用することが可能となる．CRLはPKIの仕組みの中で定義されているために，既存のWebサーバなどですぐに利用できる．

### 4.5 SSLクライアント認証

ユーザ証明書が格納されているFOMAカードを挿入したFirstPass対応FOMA端末でCPにアクセスした後，利用者はPIN（Personal Identity Number）2コードを入力することによりSSLクライアント認証が利用可能となる（図3）．CPはSSLクライアント認証時に受け取ったユーザ証明書を基にサイトへのアクセス制御ができる．SSLクライアント認証は，インターネット標準のセキュリティ技術を使用しているため，さまざまなWebサーバ，各種アプリケーション，認証製品で対応することができる．

FirstPassで提供するユーザ証明書には，FOMA契約ごとに重複しない識別情報が記載されている．識別情報はFOMA契約が継続される限り，一定かつ安全にCPに伝えられるため，高い信頼性と継続性を求められるサービス・コンテンツに有効である．

これらの携帯電話での具体的手法については，本特集中，後稿[5]で述べる．

## 5. 運用方法

### 5.1 FirstPass運用規程

本サービスを提供するうえで重要となるのは，「ユーザ証明書が不正に発行されず利用されない」ということである．本サービスの電子認証局は，インターネット標準のセキュリティ技術であるPKIを基盤として構築しており，この技術を前提としてファシリティおよび運用の基準・指針を定めたRFC（Request For Comments）-2527などに則った運用を実施している[6]．この基準・指針に従って，CPS（Certification Practice Statement）とCertificate Policyをまとめ，FirstPass運用規程として公開している．広く公開することにより，利用者やCPは公開されたFirstPass運用規程から信頼性，安全性を判断することができる．官民問わず運用されるほとんどの認証局がCPSを公開している．

具体的には下記を策定・公開することで，利用者向けにサービスの信頼性・安全性が評価可能となっている．

① サービスモデル…発行する証明書の種類，発行する証明書の対象
② サービスレベル…発行する証明書の信頼性確保レベル
③ 運用手順と体制…信頼性を確保するための体制やルール

### 5.2 セキュリティ管理の仕組み

FirstPassのセンタ施設は，ドコモの重要な通信設備のセキュリティポリシーを基本とし，さらに高度なセキュリティレベルをいくつか設け，各セキュリティレベルはそれぞれに定めた規約や機器にて一定の保護を行っている．具体的には，セキュリティレベルの重要度に応じた入退室管理を行い，入退室の際の識別・認証をICカード，生体認証装置，2名以上の同時入出などの細かいルールに従って管理されている．

一方，端末（FOMAカード）のセキュリティについては，電子認証に必要となる公開鍵，秘密鍵の鍵ペアを専用の装置にて生成後，耐タンパ性（Tamper Resistant）[*3]に優れたFOMAカードに格納し，格納と同時にFOMAカード外の秘密鍵を消去しており，この秘密鍵をFOMAカード外へ取り出すことはできない仕組みとしている．利用者にとっては，ユーザ証明書の申請時および利用時にFOMAカード内の秘密鍵を活性化するためのPIN2コード入力が必要となり，秘密鍵の利用を終えると自動的に非活性状態に移行する仕組みとしたので，不正利用のできない管理が行われている．

## 6. FirstPass認証の応用例

### 6.1 アクセス制御への応用と課題

「FirstPass」サービスにより，利用者はユーザ証明書を

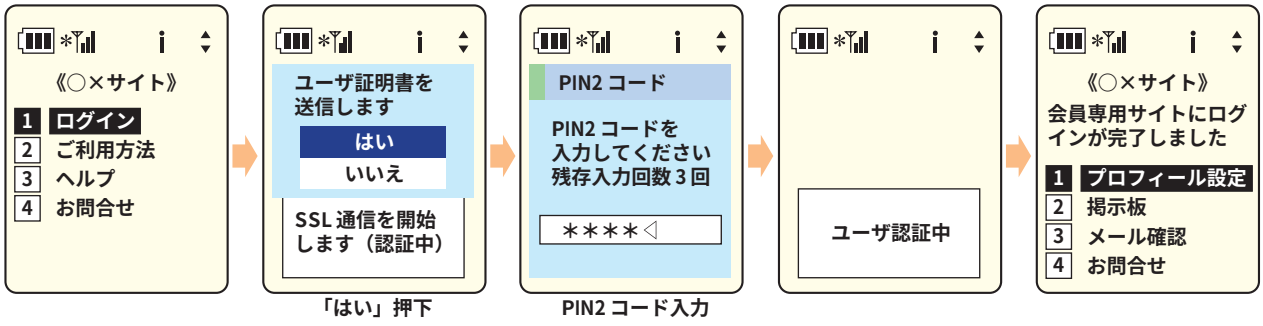


図3　SSLクライアント認証のイメージ

容易に取得できるため，CPは利用者がFirstPassを持っていることを前提としてサービスを行うことができる．

FirstPassのユーザ証明書は，一般的に利用されているID/パスワードに比べて強固なセキュリティを持っており，CPにとって利用価値が高い．

しかしながら，FirstPassサービスが発行するユーザ証明書には，識別情報としてユニークなIDが記載されるのみであるため，利用モデルとしてログイン認証を想定した場合，CPが付与したものでないFirstPassのIDだけではCP自身のアクセス制御には利用することができない．CPでの利用のためには，ユーザ証明書に利用者情報（権限）を付加することが必要となる．情報を付加する方法としては，図4に示すように，CP自身が利用者情報（権限）をユーザ証明書に付加する方法と，第三者が持つ個人情報をCPがユーザ証明書とともに利用する方法などがある．

このような方法により，ユーザ証明書に利用者属性情報を付加すれば，アクセス制御としての利用が可能であるため，CPにとっては有用な電子認証手段となる．さらに，CPのトータルな運用コストを考慮すると，CPの発行する自社証明書よりもFirstPassで提供されるユーザ証明書を利用するケースが多くなると考えられる．このとき，重要となるのは，ユーザ証明書が次の要件を満たすことである．

① FOMA端末における利用者の操作性，利便性（アクセスパフォーマンスを含む）の向上

② FirstPassを利用することにより発生するCPの運用コストの低減

## 6.2 具体的利用例

### (1) 企業内イントラネットでの利用

iアプリを利用すれば，必要なデータを必要に応じてサーバと送受信することができ，パケット通信料を減少できる利点がある．そのため，企業内でのイントラネットアクセスにiアプリが使用されることが多くなっているが，FirstPassはiモードブラウザからの利用はもとより，サーバとの通信を行うiアプリからの利用も可能であるため，業務用アプリケーションをモバイルアクセス利用する際に，イントラネットへのアクセスをより安全に実行できる．

### (2) 会員制サイトでの利用

FirstPassの利用により，モバイルコマースや会員制サイトなどの複数のサイトへのアクセスも1つのIDでアクセスが可能となる（図5）．サイトごとに異なる複数のID/パスワードを記憶する必要がなくなれば，IDやパスワードを忘れてアクセスできなくなりサービスの利用を諦めることもなくなる．

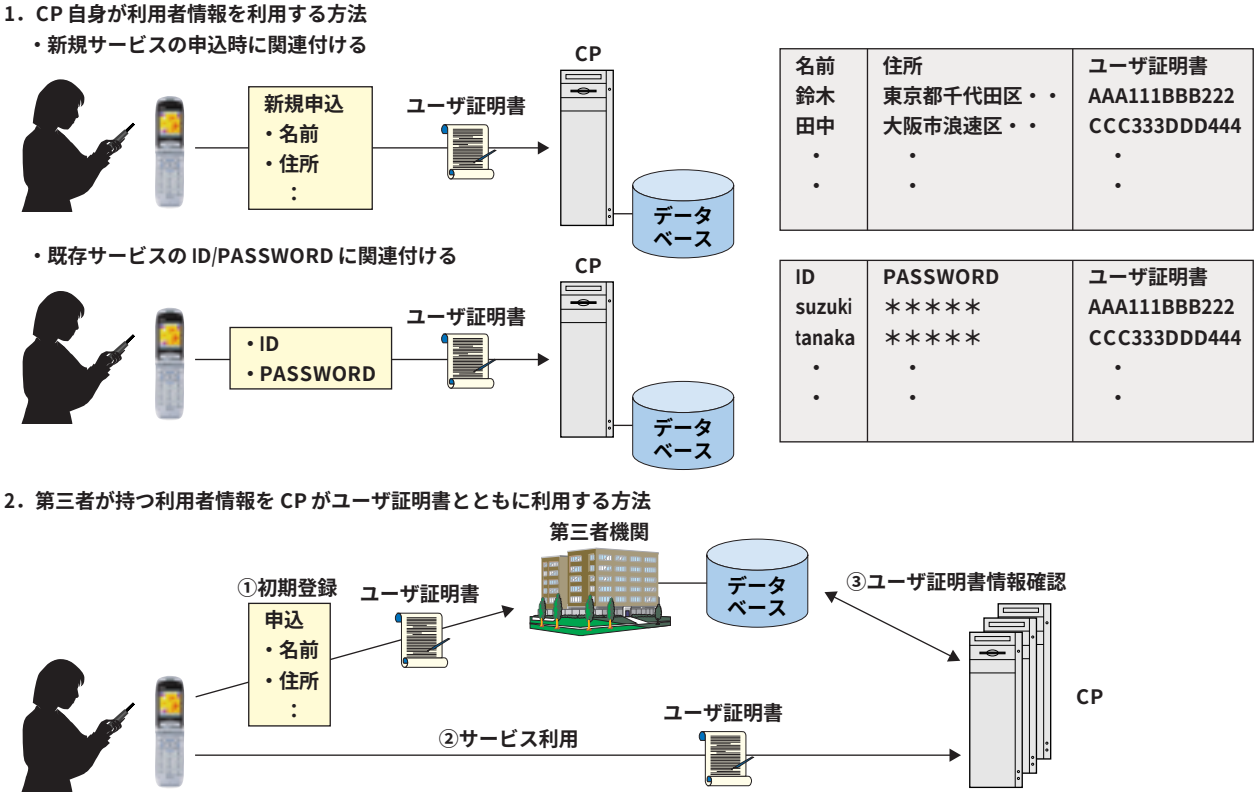


図4　利用者とユーザ証明書の関連付け

## 7. あとがき

FOMAの電子認証サービス「FirstPass」の背景とサービス内容を解説し，モバイルインターネットのサービスが，より便利で安心して使えるようになることを利用方法を交えて示した．

FirstPassを用いたシステム構築が容易となるよう，SSL関連製品やシングルサインオン製品などのサービスをWebサーバと組み合わせて利用できるように環境を整備している．今後は，FOMA利用者の利便性をさらに高められるよう，インターネットのさまざまなサービスの認証手段としてFirstPassの適用領域を広げていく．

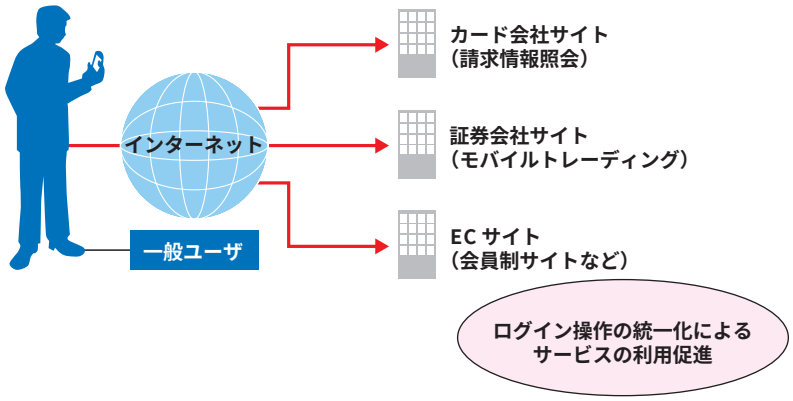


図5　会員制サイトへのログオン

### 文　献

[1] “電子署名および電子認証の現状および将来像に関する調査”，財団法人日本情報処理開発協会，Mar. 2002.
[2] “電子認証ビジネス市場規模調査の結果”，http://www.soumu.go.jp/s-news/2002/020412_2.html，総務省，Apr. 2002.
[3] A. Arsenault and S. Turner:“Internet X.509 Public Key Infrastructure Roadmap”, IETF draft-ietf-pkix-roadmap-09, IETF PKIX Working Group, Jul. 2002.
[4] 関野，ほか：“本特集 電子認証局システム構築技術”，本誌，Vol.11，No.3，pp.12-17，Oct. 2003.
[5] 高橋，ほか：“本特集 移動機へのPKI実装技術”，本誌，Vol.11，No.3，pp.18-23，Oct. 2003.
[6] S. Chokhani and W. Ford:“Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, RFC2527, IETF Network Working Group, Mar. 1999.

### 用語解説

＊1　SSLサーバ認証：第三者機関によって，インターネット上のサーバ（ドメイン）が実在している組織であることを認証することであり，その際，利用者とサーバ間の通信データが暗号化される．
＊2　公開鍵暗号基盤（PKI：Public Key Infrastructure）：公開鍵暗号技術を使用した基盤技術で，インターネットのセキュリティ標準技術となっている．特に，電子証明書を用いた認証や電子署名で多く利用されている．IETF PKIXにて定義．
＊3　耐タンパ性：装置の内部に格納されている秘密情報が正当な権利者以外に漏洩・改ざんされないことを意味する．

### 用 語 一 覧

CA：Certification Authority（認証局）
CP：Contents Provider
CPS：Certification Practice Statement
CRL：Certificate Revocation List
FOMA：Freedom Of Mobile multimedia Access
IMT-2000：International Mobile Telecommunications-2000（第3世代移動通信）
PDC：Personal Digital Cellular（ディジタル携帯電話方式）
PIN：Personal Identity Number
PKI：Public Key Infrastructure（公開鍵暗号基盤）
RFC：Request For Comments
SSL：Secure Sockets Layer
UIM：User Identity Module
VPN：Virtual Private Network