ドコモ電子認証サービス
FirstPass特集

電子認証局システム構築技術

公開鍵暗号技術に基づいて，コンテンツプロバイダが携帯電話利用者を認証するために必要な電子認証局システムを開発した．

関野 公彦　古屋 浩　木原 文典
小栗 伸幸　河本 賢一朗

1. まえがき

情報化社会における電子商取引（EC：Electoronic Commerce）や電子申請の実現には，通信相手の確実な認証が不可欠である．認証の方法としては，公開鍵暗号技術に基づく方式が主流になると考えられる．実際，PCやWebサーバでは，公開鍵暗号アルゴリズムや証明書格納機能がすでに出荷段階で実装されている．また，電子署名法の施行や住基カードの配布，特定認証業務の開始などの社会基盤の建設も国策として着々と進んでおり，次第に民間にも浸透していくであろう．これらの公開鍵暗号方式を使うための基盤を総称して，公開鍵暗号基盤（PKI：Public Key Infrastructure）と呼ぶ．

ドコモでは，ディジタル携帯電話方式（PDC：Personal Digital Cellular）の503i以降のiモード移動機に，公開鍵暗号方式に基づく暗号化とサーバ認証を行うSSL（Secure Sockets Layer）通信機能を搭載した．そして，FOMA（Freedom Of Mobile multimedia Access）用移動機であるF2102V，N2102Vからは，これにCP（Contents Provider）が利用者側を認証するクライアント認証機能が追加された．これに伴い，ドコモではSSLクライアント認証用の証明書（ユーザ証明書）を発行する電子認証局，ドコモCA（Certification Authority）を開発した．

本稿では，電子認証局の構築技術に関して，2章でドコモCA構築における背景とドコモCAの概要，3章ではドコモCA構築技術，4章ではドコモCAが発行するユーザ証明書記載事項について述べる．

2. 背景とドコモCAの概要

2.1 証明書を使った認証とCAの役割

(1) 証明書を使った認証

公開鍵暗号方式の応用である電子署名を利用した認証は，次のように行われる．文書の送信者は，送信する文書からメッセージダイジェストを生成する．このメッセージダイジェストを，送信者だけが持っている秘密鍵を用いて演算することで電子署名を生成する．この電子署名を文書に添付して送信する．受信者は，文書に添付されている電子署名の正当性を送信者の公開鍵を用いて検証する．

電子署名から送信者が本人であることを確認するためには，公開鍵が送信者のものであることが証明されている必要がある．このために，本人と公開鍵の関連を証明する証明書を発行する機関がCAである．送信者が，文書と電子署名に加えて，証明書を提示することによって，受信者は送信者が本人であることを確認できる．

(2) CAの役割

CAが本人と公開鍵の関連を証明するためには，アイデンティティの保証とアイデンティティと公開鍵の関連の証明が必要となる．多くの場合，CAはRA（Registration Authority）とIA（Issuing Authority）から構成されており，RAによって本人確認が行われ，アイデンティティが保証される．そして，RAが保証するアイデンティティに基づき，IAはアイデンティティと公開鍵の関連を証明する．このために，IAの秘密鍵を用いて生成した電子署名を付与した証明書を発行する．

信頼できる電子署名を生成するために，利用者は安全に秘密鍵を管理する必要がある．また，信頼できる証明書を発行するために，CAは高いセキュリティレベルを確保する必要がある．これらを可能にすることで，安全な認証手段を提供するPKIが構築される．

2.2 ドコモのPKI設計思想

PKIとは，利用者のアイデンティティの認証や，名前や住所など属性の認証，電子署名，タイムスタンプ局による時刻保証など，さまざまな機能を含む概念である[1],[2]．しかし，本開発ではPKIの普及を図ることを最優先に考え，イントラネットアクセスやECポータルなどに利用が見込めるSSLクライアント認証のみを基本機能として提供することとした．

また，ドコモCAは安全な通信を提供するための網サービスの位置付けであるため，ドコモCAが発行する証明書は回線契約に基づくIDを保証するものとした．これにより，通信経路の安全性が保証されないインターネット上のSP（Service Provider）に対しても，網内におけるID通知と同様の安全性を提供することを目的とした．

開発に当たっては，IMT-2000（International Mobile Telecom-munications-2000）網の特長（UIM（User Identity Module）の耐タンパ性（Tamper Resistant）*1，ネットワークダウンロード，通信設備の安全性など）を有効活用することで，従来のPKI普及の阻害要因であったICカード管理，利用者管理，証明書配布のコスト，CAファシリティの安全性確保などの諸課題を解決し，ドコモとしての強みを活かすことに留意した（図1）．

*1 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．

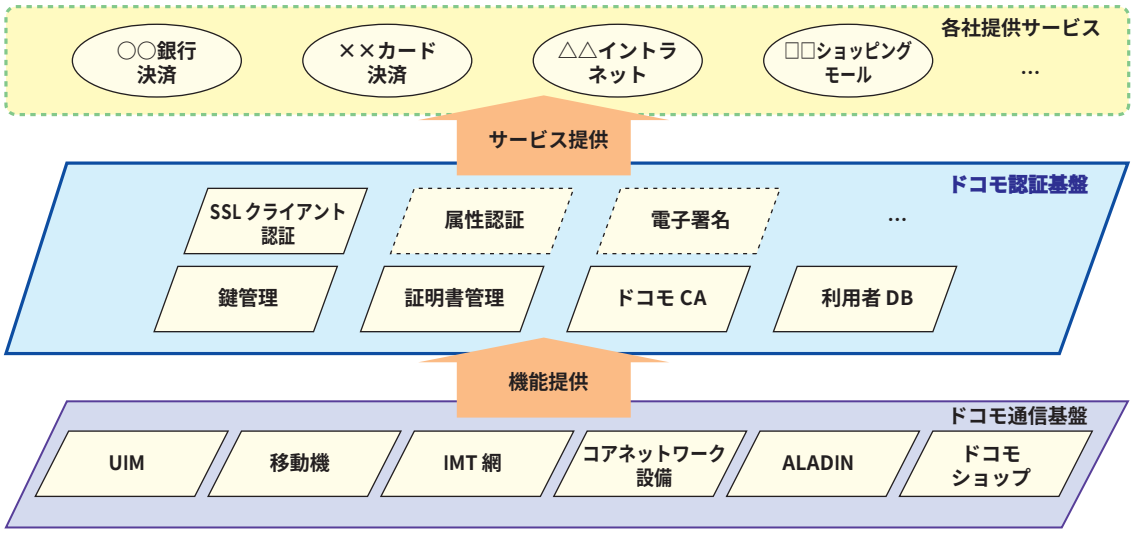

図1 ドコモ認証基盤の位置付け概念図

2.3 ドコモCAの課題と概要

2.2節で述べた設計思想に基づいて，ドコモがPKIを構築する際の技術上の課題と概要を述べる．

(1) 利用者登録および利用者認証

一般のCAでは，窓口などにおいて利用者の本人性を確認した後，利用者データベースに登録し，証明書を発行する．利用者登録において，利用者は本人を証明するための公的書類準備などの煩雑な作業が必要となる．また，CAにおいても登録窓口や利用者DBの構築・運用が必要となり多大なコストがかかる．ドコモCAでは，本人確認手続きが回線契約時に完了している事実に着目し，証明書発行時にドコモの顧客管理システム（ALADIN：ALl Around DoCoMo INformation systems）の情報を活用することでこれらの問題を解決した．詳細は，3.2節で述べる．

(2) 鍵および証明書の状態管理

従来のPKIではCAが発行する証明書は利用者のファイルとして管理される．また，証明書発行処理（申請，ダウンロードなど）は固定網経由で行われることが多い．したがって，発行処理の中断はまれであり，中断時も利用者による再試行などの解決が可能である．一方，ドコモCAの発行する証明書は，安全なモバイル通信を提供するための手段として提供するものであり，ドコモの責任においてUIM内で管理されるものである．また，申請やダウンロードはIMT網を利用して行われるため，処理中の通信切断の可能性も高い．したがって，処理中断時に網機能としてリカバリ処理を行うことが重要な課題となる．ドコモCAでは，UIM内の鍵および証明書の状態を定義することによって，通信切断により中断した処理を再接続後に継続する方式を実現した．詳細は，3.3節で述べる．

(3) IAのシステム監視

これまで述べたように，証明書に署名するための秘密鍵を管理しているIAは高いセキュリティが求められる．そのため，一般のIAはRA以外からの通信を遮断している．したがって，通常のシステム監視方法である，双方向通信による遠隔監視が適用できない．しかし，保守者の利便性を考慮すると，IAも他のシステムと同様に遠隔監視できる必要があった．このため，SNMP（Simple Network Management Protocol）トラップの非同期性を利用し，片方向通信による遠隔監視を実現した．詳細は，3.4節で述べる．

(4) ユーザ証明書の形式と記載事項

ドコモCAが発行するユーザ証明書には，インターネット上でのECポータルなどで利用されることを想定しているため，インターネットとの接続性を考慮する必要がある．また，モバイルオペレータが運用するCAには，利用者のプライバシー保護などを考慮する必要がある．そこで，ドコモCAにはこれらの要件を満たすユーザ証明書の記載事項を規定した．詳細は，4章で述べる．

3. ドコモCA構築技術

3.1 システム全体構成

ドコモCAのシステム全体構成を図2に示す．ドコモ

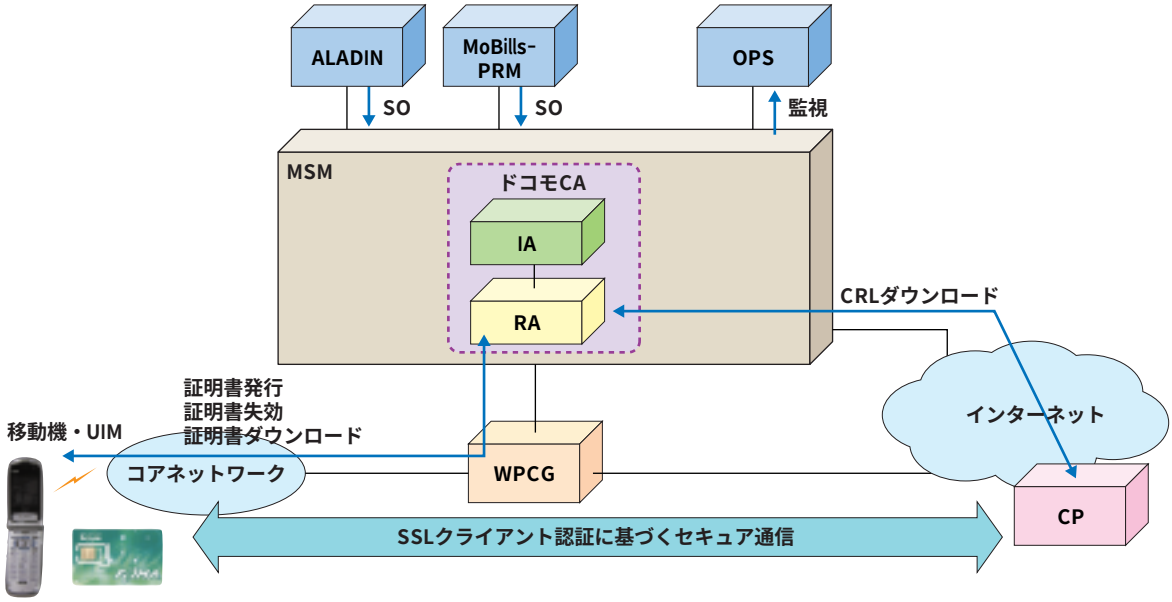

図2　システム全体構成

CAはM³In（Mobile MultiMedia Services Deployment Infrastructure）のサービス管理層であるMSM（Multimedia Service Management）の内部に位置し，WPCG（Wireless Protocol Conversion Gateway）を介してコアネットワークと接続する．利用者は移動機を操作することによりドコモCAへアクセスし，証明書発行申請，ダウンロード，失効を行うことが可能である．CPに対してはインターネットを介して失効者リストのCRL（Certificate Revocation List）を提供する．またALADIN，MoBills-PRM（Mobile communication Billing systems card rating system-Partner Relationship Management system）と接続し，それぞれから利用者情報，CP情報を取得する．システムの遠隔監視を実現するためにOPS（OPeration Systems）とも接続している．

ドコモCAは，RAとIAで構成される．利用者が証明書発行申請を行うと，RAが受け付けた後，審査・登録が行われる．登録された発行申請はIAに送られ，証明書の発行処理が行われる．発行されたユーザ証明書はRAで管理され，利用者がダウンロード操作を行うことによってUIMに格納される．

また，CRLの提供はあらかじめ登録されたCPのみを対象とするため，MoBills-PRMから取得した企業情報を基にアクセス制御を行っている．

3.2 利用者登録および利用者認証

RAでは，ALADINの情報を活用して利用者のUIMの正当性を審査し，登録を行っている[3]．以下では，その詳細を説明する．

利用者がFOMAの新規回線契約を行う際，ALADINに登録されたMSISDN（Mobile Station Integrated Services Digital Network number）およびUIMの製造番号は，同時にドコモCAに転送され，利用者情報として格納される．次に，証明書発行申請を行う利用者がドコモCAにアクセスすると，RAのコマンドによってUIMから製造番号が自動的に送信される．このとき，WPCGによってHTTP（HyperText Transfer Protocol）ヘッダに付加されるMSISDNを併せて取得する．RAは，このMSISDNをキーにUIMから取得した製造番号と，あらかじめドコモCAに格納されている製造番号とを照合する．これによって，ドコモCAにアクセスした利用者のUIMが，FOMA契約された正しいドコモのUIMである事が認証できる．すなわち，証明書発行申請を行う利用者は，改めて窓口などで利用登録を行う必要や移動機から利用者情報を入力する必要はなく，FOMAの回線契約さえ行われていれば証明書発行申請を行うことが可能となる（図3）．

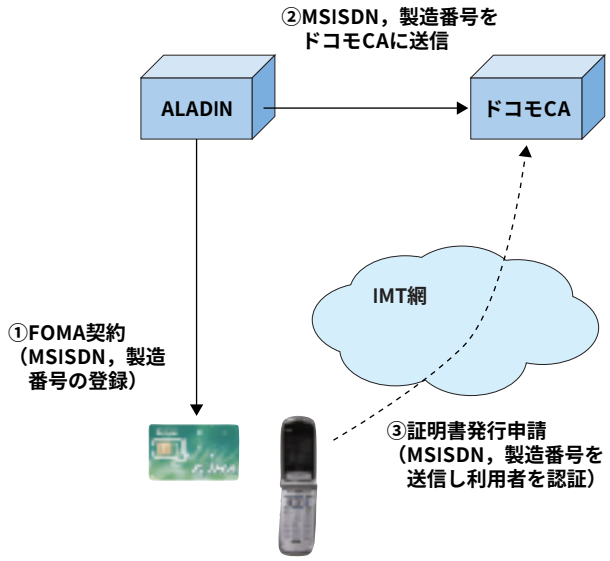

図3　利用者登録と利用者認証

3.3 鍵および証明書の状態管理

UIM内の鍵状態，証明書状態を管理することにより，再接続時に処理再開を可能とする方式についての詳細を以下に説明する[3]．鍵状態は運用中，鍵生成済，証明書申請済，証明書書込済の4種の状態を，証明書状態は未発行，発行申請中，発行済ダウンロード未了，ダウンロード完了，失効申請中，失効済の計6種の状態をそれぞれ定義し，証明書発行申請，ダウンロード，失効の各処理シーケンスに従って遷移する．この状態を参照すれば，処理シーケンスの中断箇所を判別できる．

例えば，図4に示すように証明書発行申請のシーケンスにおいて，UIMが生成した鍵をRAに送信する途中で通信が切断されたとする．再接続時には鍵状態は鍵生成済み，証明書状態は未発行となっているため，生成済みの鍵をRAに送信する事によって処理を続行できる．

このように，鍵と証明書の状態を管理することにより，利用者の通信待ち時間の短縮やUIM内に格納されている鍵の有効活用が可能となる．

3.4 IAのシステム監視

SNMPトラップ[*2]を用いた片方向通信によるIA遠隔監視の方式について以下に詳細を説明する．図5に示すようにIAに設けた部門管理サーバがポーリングを行うことにより，各サーバのハード，OS，アプリケーションなどの障害情報を集約する．部門管理サーバは，この集約した障害情報をSNMPトラップの形式に変換し，OPSへ通知する．

＊2　SNMPトラップ：エージェントからマネージャに送ることができる非同期メッセージ．設備の異常や回復を伝えるのに主に使用される．

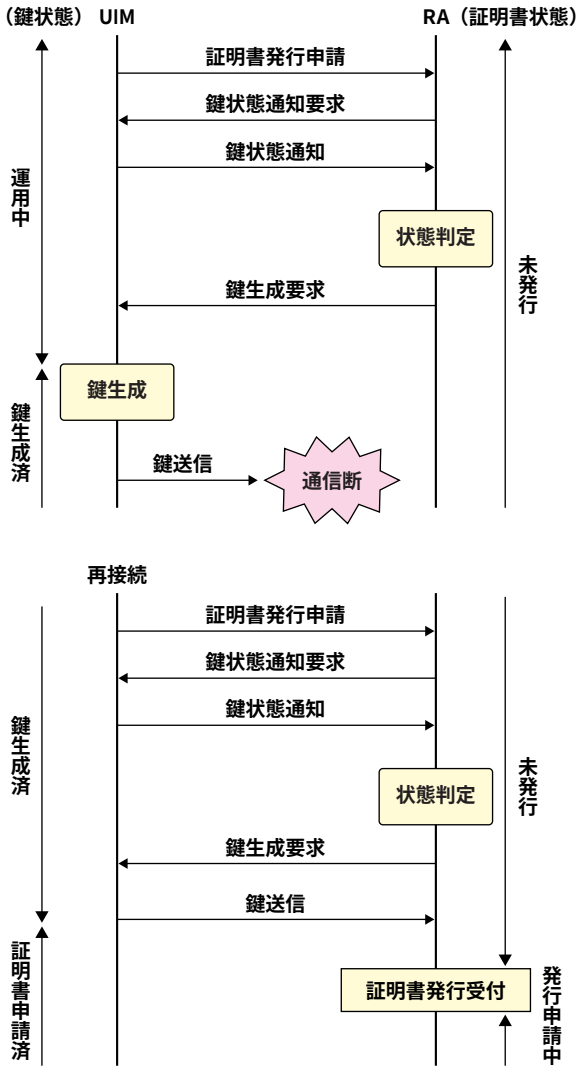

図4　発行申請シーケンスにおける状態管理

SNMPトラップは片方向の通信で障害を通知する機能を持ち，既存OPSでサポートされているインタフェースである．

このように，既存OPSのインタフェースに変更を加えることなくセキュリティレベルを維持した遠隔監視を実現し，従来のシステムと同様にオペレーションセンタの大画面で監視することを可能にした．

4. ユーザ証明書記載事項

インターネットで標準的に用いられる証明書の規格として，国際電気通信連合・電気通信標準化部門（ITU-T：International Telecommunication Union-Telecommunication standardization sector）で規格化されているX.509がある[4]．ドコモCAにより発行される証明書は，インターネットとの接続性を考慮し，X.509に準拠することとした．X.509の証明書プロファイルには，所有者（subject），有効期間（validity），シリアル番号（serial number），署名（signature）などがある．本章では，ドコモCAが発行するユーザ証明書における所有者と有効期間の規定方針について述べる．

4.1 所有者

証明書では，IDを証明するため，所有者フィールドにIDが記載される．一般にIDとして，氏名，電話番号，製造番号などが考えられるが，モバイルオペレータがIDを証明するにあたって，利用者のプライバシー保護，IDの継続性を考慮する必要があった．

ドコモCAでは，利用者のプライバシー保護のため，回線契約時に登録する情報を非公開にすること，またIDの継

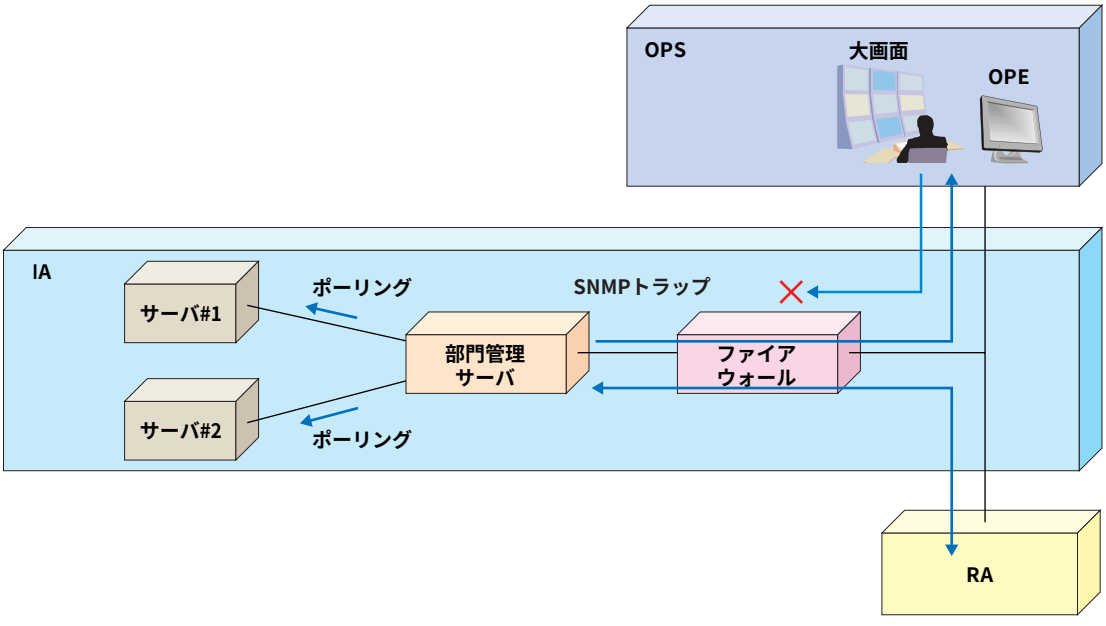

図5　IAシステム監視

続性のために電話番号や機種を変更してもIDを変更しないことを考慮した．その結果，ドコモCAが証明するIDは，FOMA契約ごとに割り当てられた電話番号と異なるIDとした．

4.2 有効期間

多くのCAは，ユーザ証明書の有効期間を1年間としている．これは，ユーザ証明書に記載する利用者情報の変化などを考慮すると，1年ごとに更新する必要があったからと考えられる．

ドコモCAでは，1つのUIMでの証明書発行回数が5回に限られることから，ユーザ証明書の有効期間を長くする必要があった．また，ユーザ証明書に記載するIDが利用者情報を含まないため，有効期間を長くすることが可能であった．一方，有効期間を長くすることにより，CRLサイズの肥大化が懸念された．これらを総合的に考慮した結果，ユーザ証明書の有効期間を2年間とした．

5. あとがき

FirstPassは，移動通信においてPKIを利用した認証を行う，国内初の商用サービスである．現在は，ドコモCAを活かしたサービス導入に取り組むとともに，さまざまな利用シーンにおいて同じIDを使って認証するといった「利用環境の拡大」に向けて技術的な検討を行っている．

将来的には，今回の開発で実現した安全な設備と運用ノウハウを活かした基盤機能の充実やインターネット上のWebサービスと統合された2nd Generation PKIへの発展などが考えられるだろう．

文　献

[1] A.Arsenault and S.Turner:“ Internet X.509 Public Key Infrastructure: Roadmap ”, IETF draft-ietf-pkix-roadmap-09, IETF PKIX Working Group, Jul. 2002.
[2] R.Shirey:“ Internet Security Glossary ”, RFC2828, IETF Neteork Working Group, May. 2000.
[3] K.Kawamoto and N.Nakamura:“ Study of Management on the Mobile Public Key Infrastructure ”, NOMS 2002, Apr. 2002.
[4] ITU-T Recommendation X.509:“ Information Technology-Open Systems Interconnection-The Directory Authentication Framework ”, Jun. 1997.

用 語 一 覧

ALADIN：ALl Around DoCoMo INformation systems（顧客管理システム）
CA：Certification Authority
CP：Contents Provider
CRL：Certificate Revocation List
EC：Electoronic Commerce（電子商取引）
FOMA：Freedom Of Mobile multimedia Access
HTTP：HyperText Transfer Protocol
IA：Issuing Authority
IMT-2000：International Mobile Telecommunications-2000（第3世代移動通信）
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）
M^{3}In：Mobile MultiMedia services deployment Infrastructure
MoBills-PRM：Moble communication Billing systems card rating system-Partner Relationship Management system
MSISDN：Mobile Station Integrated Services Digital Network number
MSM：Multimedia Service Management
OPS：OPeration Systems
PDC：Personal Digital Cellular（ディジタル携帯電話方式）
PKI：Public Key Infrastructure（公開鍵暗号基盤）
RA：Registration Authority
SNMP：Simple Network Management Protocol
SO：Service Order
SP：Service Provider
SSL：Secure Sockets Layer
WPCG：Wireless Protocol Conversion Gateway