情報処理学会論文誌 Vol. 50 No. 9 2103–2117 (Sep. 2009)

放送型高頻度鍵更新方式による超広域モバイル環境向けセキュアリアルタイム通信の実現

辻 宏郷[†1,†2] 米田 健[†2]
水野忠則[†3] 西垣正勝[†3]

モバイル通信端末の高性能化・高機能化や無線通信サービスの帯域拡大にともない，これらの端末を用いたリアルタイム通信が可能となった．しかしながら，通信内容を無線通信区間やバックボーンネットワークにおいて盗聴される可能性や，モバイル通信端末の紛失や盗難を生じる危険性が存在する．したがって，通信内容の端末間 End-to-End 暗号化を行うとともに，モバイル通信端末紛失・盗難時の成りすましによる端末の不正利用，端末内部の暗号鍵の解読による暗号化通信内容の復号や端末内部の機密情報の漏洩を防止する必要がある．本論文では，地球上のいかなる場所においても，厳格にセキュアなリアルタイム通信を実現するための暗号鍵および端末の管理方式を提案する．暗号鍵はシステム管理サーバで一括生成し，ディジタル放送等の 1 方向通信を用いて各々の端末に配布することで，高頻度に更新する．端末の紛失・盗難が発生した場合は，システム管理サーバから遠隔操作命令を送信して，暗号鍵，端末内機密情報の消去や端末の初期化を行う．これらの暗号鍵配布と端末管理を実現するプロトコルを設計・実装し，利用者が特別な操作を必要とせずに暗号鍵の共有や更新を実現できること，端末の紛失・盗難発生時，遠隔管理や他の端末の協調動作によって，該当端末を除外できることを確認した．

Realization of Secure Real-time Communication for Worldwide Mobile Environment by Frequent Key Renewal Method through Broadcast Data Distribution Systems

Hirosato Tsuji,[†1,†2] Takeshi Yoneda,[†2]
Tadanori Mizuno[†3] and Masakatsu Nishigaki[†3]

The evolution of mobile communication terminals and mobile networks enables the real-time communication using these devices. To protect against the unauthorized disclosure of the communication between these terminals, the end-to-end encryption between mobiles is required. In addition, if the terminal is lost or stolen, the unauthorized use of such terminals, the decryption of encrypted communications using the stolen key from such terminals, the leakage of confidential information in such terminals should be also prevented. In this paper, we propose the method of key/device management to realize the secure real-time communication in worldwide mobile environment. In this method, the end-to-end encryption keys are frequently generated on the system management server and distributed to each terminal using one-way communication, such as the digital broadcast data distribution systems. In case of the loss or robbery of terminals, the encryption keys and the secret information will be erased and the terminal will be initialized by the remote control from the system management server. We design the protocol that realizes the management of encryption keys as well as the management of mobile terminals. As a result, we confirmed that the sharing/updating encryption keys are achieved without any operation of the mobile terminal users. We also confirmed that the lost/stolen terminal is excluded by the remote operation command of system management server and the cooperative action of the other terminals.

1. はじめに

ノート PC・UMPC（Ultra-Mobile PC）・携帯情報端末（PDA）・スマートフォン・携帯電話等の携帯可能な情報通信端末（以下，本論文ではモバイル通信端末と呼ぶ）の高性能化・高機能化や無線通信サービスの帯域拡大にともない，端末間で音声・テキスト・静止画・動画等をリアルタイムで通信することが可能となった．しかしながら，これらの通信では，端末間の通信内容を無線通信区間やバックボーンネットワーク（通信サービス提供者のコアネットワークやインターネット）で盗聴される可能性がある．さらに，モバイル通信端末自体は紛失したり，盗難に遭ったりする危険性がある[1)]．したがって，モバイル通信端末を用いて重要機密情報をやりとりする場合は，端末間の通信内容の盗聴防止（通信内容の端末間 End-to-End 暗号化）とともに，端末紛失時の対策（成りすましによる端末の不正利用防止，端末内部の暗号鍵の解読による暗号化通信内容の復号防止や端末内部に格納した機密情報の漏洩防止）が必要である．

本研究では，地球上のいかなる場所においても，厳格にセキュアなリアルタイム通信を提

†1 静岡大学大学院理工学研究科
Graduate School of Science and Engineering, Shizuoka University
†2 三菱電機株式会社情報技術総合研究所
Information Technology R&D Center, Mitsubishi Electric Corporation
†3 静岡大学創造科学技術大学院
Graduate School of Science and Technology, Shizuoka University

供するための方式を提案する．放送型通信によって高頻度に暗号鍵を更新し続けることによって，通信内容の盗聴を最低限に抑えることを実現する．また，更新する暗号鍵配送の仕組みをモバイル通信端末の遠隔管理操作に対しても応用することによって，端末紛失・盗難時の機密情報漏洩対策も実現する．

以下，2 章で，本研究の対象とする超広域モバイル環境向けリアルタイム通信システムの要件を示す．3 章で従来技術の課題を，4 章で提案する暗号鍵・端末の管理方式の詳細を，5 章で提案方式の実装について述べる．6 章において評価について述べ，7 章でまとめる．

2. システム要件

2.1 前 提 条 件

本研究の対象とする超広域モバイル環境向けリアルタイム通信システムの前提条件を示す．

- 地球上のいかなる場所においても利用可能であることを目標とする．たとえば，国内外の情報通信インフラの整備が整っていない場所（定住者の存在しない地域や開発途上国）においても，衛星携帯電話や衛星データ通信サービス等の最終的手段と組み合わせて利用できるようにする．
- 盗聴やモバイル通信端末の盗難といった脅威に対して，厳格な安全性を保証したリアルタイム通信を実現する．
- 端末の利用者は，組織内の一部（たとえば企業内の幹部等）に限定する．このため，1 システムにおける端末数は最大で数百台である．

なお，コストは必ずしも重視しない．低コストで実現できることは考慮しつつ，安全性や可用性を重視し，厳格なセキュリティを提供することを最優先とする．

2.2 基本的要件と具体的要件の定義

2.1 節で述べた前提条件の下で，超広域モバイル環境における機密情報のリアルタイム通信を実現するための 3 つの基本的要件および詳細化，細分化した具体的要件を定義する．

2.2.1 完全なリアルタイム通信

第 1 の基本的要件は，リアルタイム通信内容の端末間 End-to-End 暗号化によって，盗聴を防止すること，このとき，暗号アルゴリズムを用いた通信内容の暗号化に対する以下の攻撃に耐えうる対策を備えることである．

(1) 全数探索法による暗号鍵の解読防止

考えうるすべての鍵を総当たりで試すことによって，暗号鍵を発見しようとする攻撃に耐えうること．

(2) 暗号アルゴリズムに対する攻撃対策

差分解読法[2] や線形解読法[3] 等，暗号アルゴリズムの内部構造を解析することによって，暗号鍵を求めようとする攻撃に耐えうること．サイドチャネル攻撃[4)–6)] 等，暗号アルゴリズムの実装上の脆弱性に対する攻撃に耐えうること．

(3) 暗号鍵生成時の乱数の偏り防止

暗号鍵生成時に利用する乱数生成に偏りが存在した場合，暗号鍵はその鍵長分のエントロピーを持たないため，全数探索法による暗号鍵解読を受ける可能性がある．この攻撃に耐えうること．

これに対し，以下に示す具体的要件を定義する．

要件 1：モバイル通信端末間のリアルタイム通信内容を暗号化すること．

要件 2：安全性が証明された暗号アルゴリズムを採用すること．

要件 3：十分な鍵長[7]（通常は 128 ビット，用途によっては 256 ビットあるいはそれ以上）を選択すること．

要件 4：ハードウェアを用いて実現する場合は，物理乱数（真性乱数）生成装置を用いること．ソフトウェアで実装する場合は，安全な疑似乱数生成アルゴリズム[8] を用いたうえ，適切な seed を与えること．

2.2.2 操作性・可用性の確保

第 2 の基本的要件は，操作性や可用性を確保することである．利用者が暗号化や鍵管理を意識せずにストレスを感じることなく使えること，使いたいときにいつでも使えることが必要である．

これに対し，以下に示す具体的要件を定義する．

要件 5：暗号化通信開始時，暗号鍵の交換や公開鍵証明書の検証等の CPU に負荷のかかる処理をともなわないこと．

要件 6：利用者が，暗号鍵の存在や更新を意識せずに利用可能であること．

要件 7：地球上のいかなる場所に存在する端末に対しても，暗号鍵の配布が可能であること．

要件 8：すべての端末に暗号鍵が届かない場合であっても，いずれか 1 台の端末に暗号鍵が届いていれば，暗号化通信が可能となること．

2.2.3 十分な事故対策

第 3 の基本的要件は，端末の紛失・盗難によって引き起こされる可能性のある，以下に示すリスクを十分に低減させることである．

(1) 暗号鍵の漏洩による盗聴防止

暗号鍵を格納したモバイル端末の紛失・盗難によって，暗号鍵が漏洩した場合，以下に示す盗聴が発生しうるので，そのリスクを低減させること．

- **過去の通信内容の盗聴の試み**
  事前に暗号化通信データを盗聴・録音しておき，端末を盗み出して暗号鍵を抜き出し，保存しておいた暗号化通信内容を復号する．
- **現在・未来の通信内容の盗聴の試み**
  暗号鍵が 3 台以上の端末間の通信（マルチキャスト通信を含む）の暗号化に用いられている場合，端末を盗み出して暗号鍵を抜き出し，他の端末間の暗号化通信データを盗聴して復号する．

(2) 紛失端末の不正利用防止

モバイル通信端末の紛失・盗難等が発生した場合，該当端末を入手した者が正規利用者に成りすまし，他の端末利用者と通信を試みる可能性があるので，不正利用を防止すること．

(3) 端末内機密情報の漏洩防止

モバイル通信端末の紛失・盗難発生時，暗号鍵に加えて，端末内部の機密情報の漏洩を防止すること．

これに対し，以下に示す具体的要件を定義する．

要件 9：事前に暗号通信データを盗聴して保存しておき，端末を盗み出して暗号鍵を抜き出し，保存しておいた暗号化通信内容を復号する攻撃（過去の盗聴）を防止すること．

要件 10：紛失・盗難端末から暗号鍵を抜き出し，その後の暗号化通信内容を復号する攻撃（現在・未来の盗聴）を防止すること．

要件 11：紛失・盗難端末を入手した不正利用者による，他の端末との間の成りすまし通信を防止すること．

要件 12：紛失・盗難端末内の機密情報の漏洩を防止すること．

要件 13：他の利用者に，端末の紛失・盗難を通知できること．

要件 14：紛失・盗難時の対策として端末の遠隔管理操作を行う際，紛失・盗難端末が遠隔管理操作から逃れようとする場合の対策を備えること．

要件 15：紛失・盗難時の対策としての端末の遠隔管理操作は，地球上のいかなる場所に存在する端末に対しても可能であること．

3. 従 来 技 術

3.1 暗号鍵の配布・共有方式

モバイル通信端末間で音声・映像・動画等をリアルタイム通信する際の盗聴を防止するためには，端末間 End-to-End 暗号化（送信側端末で通信内容を暗号化し，受信側端末で復号する）が必要である．このためには，暗号化通信を行う端末どうしの間で，暗号鍵を共有しなければならない．暗号鍵の配布・共有方式としては，以下に示す方法が考えられる．

(a) 事前共有[9),10)]

端末間の通信手順を実行する前に，何らかの手段を用いて暗号鍵を事前共有しておく方式．たとえば，あらかじめ端末配布時に必要な鍵をすべて埋め込んでおく方法や，端末配布後に安全な方法で別途鍵だけを配布する方法がある．あらかじめ暗号鍵を共有するため，通信開始直前に鍵共有処理を行う必要がない．その反面，同一の鍵や限定された鍵集合を使い続けることになるため，安全性に問題を生じることがある．

(b) 端末間の鍵共有アルゴリズムを用いた共有[9),10)]

公開鍵暗号アルゴリズムを用いる方式．あらかじめ各々の端末は公開鍵ペア（公開鍵と秘密鍵）を保有しておき，Diffie-Hellman 鍵共有アルゴリズムや RSA 鍵配送アルゴリズム等を用いて，暗号鍵を共有する．各端末ごとに公開鍵ペアを管理し，全体として鍵の総数が少なくて済むので，端末数が増大しても鍵管理コストが上昇しない．その反面，公開鍵の正当性を証明するために，認証局（CA: Certification Authority）の発行する公開鍵証明書を導入する必要がある．また，通信開始前の鍵共有処理に時間を要する場合がある．

(c) 管理サーバを用いた鍵の配布・共有[11)]

鍵配布センタ（KDC: Key Distribution Center）等，鍵管理機能を提供する管理サーバによって集中的に暗号鍵を生成し，各々の端末に配布する方式．各々の端末が暗号鍵の生成や共有を行わないため，システム管理者のセキュリティポリシに従って，適切な間隔で鍵生成や鍵更新を行うことができる．その反面，管理サーバが停止すると鍵の共有や更新ができなくなる可能性がある．

このとき，管理サーバにおいて暗号鍵を一括生成・配布する方法としては，以下に示す方式が考えられる．

－都度生成・配布方式

暗号鍵を必要とする端末は，管理サーバに対して暗号鍵生成要求を行い，端末からの要求に対して管理サーバが暗号鍵を生成・配布する方式．新しい暗号鍵を必要とするたび

に，端末と管理サーバの間で通信を行う必要がある．KDC の代表例である Kerberos[12] における鍵生成・配布は，この方式である．

－事前生成・配布方式

各々の端末において暗号鍵が必要であるか否かにかかわらず，管理サーバにおいて暗号鍵を事前生成，配布しておく方式．暗号鍵を事前生成・配布するコストが必要となる反面，新しい暗号鍵を必要とするたびに端末と管理サーバの間で通信する必要がない．

また，管理サーバで生成した暗号鍵をモバイル通信端末に配布するための通信方法としては，以下に示す方式が考えられる．

－双方向通信方式

管理サーバがモバイル通信端末と同一のネットワーク，またはモバイル通信端末のネットワークと接続されたネットワーク上に存在する方式．管理サーバと端末の間で双方向通信を行うことができる．再送等を用いて確実な通信が可能である反面，管理サーバと端末は双方向通信可能なネットワーク上に存在しなければならない．一般に KDC はこの通信方式を用いている．

－一方向通信方式

管理サーバからモバイル通信端末へ，単一方向の通信のみが可能な放送型の通信路で接続された方式．通信路として，衛星データ配信サービス[13]，衛星放送，ディジタルテレビ放送等の利用が考えられる．モバイル通信端末から管理サーバへの通信ができない代わりに，双方向通信方式と比較して，より広範囲の位置に存在する端末に対して，暗号鍵配布等の通信を行うことができる．

3.2　端末紛失・盗難時の機密漏洩防止対策

(1) 端末の機密漏洩防止対策

2.2 節で示したように，モバイル通信端末の紛失・盗難により，暗号鍵の漏洩による暗号化通信内容の復号や端末内機密情報の漏洩の危険性がある．端末の機密漏洩防止対策としては，以下に示す方法が考えられる．

(a) ユーザ認証による端末保護方式

PIN，パスワード，生体認証等によって，正規利用者以外による端末操作を防止する方法．認証サーバを使用しないユーザ認証であれば，端末単体での認証によって端末保護を実現することができる．その反面，(2) で後述する運用上の問題をかかえており，本方式のみでは端末の機密情報を守ることは困難である．

(b) シンクライアント方式

端末内部に重要な情報を格納せず，サーバに置いた情報をアクセスする方式．これによって，紛失した端末からの機密情報漏洩を防止する．しかしながら，端末間で暗号化通信するための暗号鍵は端末内部に格納する必要があるため，この方式だけでは暗号鍵の漏洩による暗号化通信内容の解読を防ぐことはできない．また，シンクライアント端末を盗み出して，サーバ上の機密情報をアクセスする脅威が存在するため，本方式だけで機密情報を保護することは十分とはいえない．

(c) 管理サーバからの遠隔操作管理方式[14]

管理サーバから遠隔操作命令を送信することによって，端末の紛失・盗難が発生した場合，端末の機能を停止したり，端末内部の機密情報（暗号鍵を含む）をすべて消去したりする方式．システム管理者のセキュリティポリシに従って，厳格なセキュリティ運用，紛失・盗難時の対策を実施できる．その反面，管理サーバが停止した場合，あるいは端末が遠隔操作の範囲外に持ち出された場合には，何ら対策が実施できなくなる可能性がある．

(2) 端末の利用者認証方式とその限界

一般に，モバイル通信端末には，紛失・盗難時の不正利用や端末内部の機密情報漏洩を防止するために，以下に示すような利用者認証機能が設けられている．

(a) PIN 認証

多くの携帯電話端末は，4 桁の数字の暗証番号を入力しないとダイヤル操作を禁止する機能（ダイヤルロック）を持っているが，所有者と関わりが深い数字（生年月日，住所・電話番号等）が設定されていることが多く，その値が容易に類推可能であることが多い[15]．また，暗証番号を設定しないユーザも多い[16]．

(b) パスワード認証

ノート PC や一部の携帯電話端末では，英数字記号を組み合わせた任意の長さの文字列をパスワードとしてユーザ認証することが可能であるが，それによって守ろうとする暗号鍵に対して十分なエントロピーを持たせることは難しい．たとえば，安全なパスワードとして文字数字記号を組み合わせた 14 文字以上が推奨されている[17] が，覚えにくいパスワードをユーザはメモに記録する傾向があり，結果として認証が破られる可能性が増大する[18]．

(c) 生体認証[19]

一部のノート PC および携帯電話端末では，指紋認証等の生体認証技術を用いたユーザ認証機能を備えているものがある．しかしながら，生体認証には本人拒否率と他人受入率のトレードオフ問題があり，結果として，暗証番号やパスワードとの組み合わせる等が必要であり，必ずしも安全とはいえない場合がある．また，人工指を偽造して指紋認証を破る研究

が進んでいる[20]．さらに，指紋認証を破るために，正規ユーザの指が切断される事件[21]が発生しており，生体認証に拒否反応を示すユーザも少なくない．特に，企業や組織の幹部が端末利用者の場合，利用者の安全を考慮して生体認証を導入できない，といったことが考えられる．

上記に示したように，いかなる方法を用いても利用者認証だけでモバイル通信端末の不正利用を防止することは困難であり[22]，他の方法と組み合わせて機密漏洩防止対策を実現する必要がある．

4. 提 案 方 式

4.1 提案方式の概要

2 章で述べたシステム要件を満たすために，我々は，暗号鍵の配布・共有方式として，管理サーバを用いた鍵の配布・共有方式を採用する．管理サーバには，可能な限り，ハードウェアによる物理乱数（真性乱数）生成装置を搭載する．暗号鍵は事前生成・配布することとし，管理サーバからモバイル通信端末への鍵配布は 1 方向通信方式を用いることとする．端末紛失・盗難時の機密漏洩防止対策としては，管理サーバからの遠隔操作管理方式を採用する．モバイル通信端末へ遠隔操作命令を送信する場合は，暗号鍵配布時と同様に 1 方向通信方式を利用する．

以降，本論文においては，暗号鍵管理と端末管理の両方の役割を担うことから，提案方式における管理サーバを「システム管理サーバ」と呼ぶこととする．**図 1** に提案システムの全体アーキテクチャを示す．

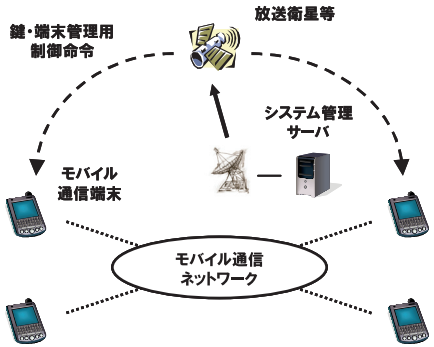


図 1　提案システムのアーキテクチャ
Fig. 1　Proposed system architecture.

4.2 暗号アルゴリズムの選択

2.2 節で述べた**要件 1**〜**要件 4** を満たすために，安全性が証明されている方法を用いて通信内容を暗号化する．すなわち，安全性が証明された共通鍵暗号アルゴリズムを採用する．乱数生成については，暗号鍵の生成に用いる場合は，ハードウェアによる物理乱数（真性乱数）生成を採用する．それ以外の目的で乱数生成を必要とする際，ハードウェアが利用できない場合は，安全性の証明された疑似乱数生成アルゴリズムを用いて，ソフトウェアによる実装を選択する．これによって，暗号アルゴリズムに対する理論的攻撃に完全に対応する．

4.3 暗号鍵の配布・共有方式の選択

2.2 節で述べた要件を満たすため，我々の提案方式は，以下に示す暗号鍵の配布・共有方式を採用する．

(1) 共通鍵暗号アルゴリズムのみによる実現

2.2 節で述べた**要件 4** および**要件 5** を満たすために，鍵配布・共有時の暗号化や改ざん検出を含む暗号処理に共通鍵暗号アルゴリズムのみを使用し，モバイル通信端末において公開鍵暗号アルゴリズムや公開鍵証明書の検証処理の実装を不要とする．共通鍵暗号アルゴリズムには，管理すべき暗号鍵の総数が膨大となるという欠点が存在するが，今回のシステムの前提条件である数百台程度の端末総数であれば，問題ないと考えられる．

(2) 暗号鍵の事前配布

2.2 節で述べた**要件 5** を満たすために，暗号鍵は事前に生成・配布する．暗号鍵の生成・配布は，後述するように，システム管理サーバで行う．これによって，通信開始時の鍵共有処理を不要とし，即時暗号化通信を可能とする．

(3) システム管理サーバにおける暗号鍵の一括生成

2.2 節で述べた**要件 4** を満たすために，システム管理サーバにおいて，ハードウェアを用いた物理乱数（真性乱数）生成装置を搭載し，暗号鍵の生成，更新にあたっては，システム管理サーバにおいて暗号鍵を一括生成・配布する．このことは，2.2 節で述べた**要件 6** をも満たし，端末利用者は特別な操作を必要とせず，かつ適切な時期に暗号鍵の更新を指示することができる．

(4) 一方向性通信路を用いた放送型鍵配布

2.2 節で述べた**要件 7** を満たすために，システム管理サーバからモバイル端末に送信する暗号鍵配布用の制御命令は，1 方向性通信路を用いた放送型鍵配布する方法を採用する．これにより，世界中のあらゆる場所に存在する端末に配布できるようにする．たとえば，国内

外のあらゆる場所でも利用可能とするためには，衛星放送を用いたデータ配信サービスを利用する．

最近のモバイル通信端末は，その主たる通信路とは別に，補助的な情報を受信するための1方向性通信路を備えている．たとえば，最近の携帯電話端末は，携帯電話通信事業者の基地局との双方向通信機能に加えて，ディジタル放送（ワンセグ）やGPS衛星からの電波を受信する機能を備えているものがある．また，無線LAN機能を持った携帯電話等，複数の通信路をサポートし，状況に応じて使い分ける端末も存在している．さらに，ワンセグより高性能でダウンロード型放送に対応する次世代サービス（ISDB-Tmm方式やMediaFLO方式）のフィールド実験も始まっており，近い将来，ディジタル衛星放送や衛星データ通信サービスの受信機能を備えた端末を利用可能になると考えられる．

(5) 暗号鍵の端末間転送による転送

2.2節で述べた**要件8**を満たすために，モバイル通信端末間で暗号鍵を転送することによって，すべての端末に暗号鍵が届いていない場合でも，端末間の暗号化通信を可能とする．

(6) 暗号鍵の定期更新・不定期更新

安全な暗号アルゴリズムや乱数生成アルゴリズム，十分な鍵長を使用していても，モバイル通信端末の紛失・盗難から発生した暗号鍵の漏洩によって，通信内容の漏洩が発生することは避けられないため，暗号鍵の定期更新や端末紛失・盗難発生時の緊急更新を行う仕組みが必要である．2.2節で述べた**要件9**を満たすために，平時からなるべく短い周期で定期的に暗号鍵を更新することによって過去の情報の漏洩をできるだけ少なくする．また，2.2節で述べた**要件10**を満たすために，端末紛失・盗難時に速やかに暗号鍵を更新することによって将来的な情報漏洩についても可能な限り小さく抑える．

4.4　端末紛失・盗難対策の選択

2.2節で述べた要件を満たすため，我々の提案方式は，以下に示す端末紛失・盗難対策を採用する．

(1) 端末紛失・盗難発生時の遠隔管理

モバイル通信端末の紛失・盗難発生時，該当端末を用いた盗聴や成りすまし通信，暗号鍵の抜き出し，機密情報の漏洩等を防止するため，システム管理サーバによる遠隔管理を行い，ユーザ認証による端末保護やシンクライアント方式と併用することによって，機密保護を強化する．2.2節で述べた**要件11**および**要件12**を満たすために，システム管理サーバから該当端末に対して，端末初期化を指示する遠隔操作命令を発行する．端末初期化命令を受信した端末は，端末内部の暗号鍵や暗号化通信用プログラム，機密情報を消去する．また，2.2節で述べた**要件13**を満たすために，遠隔操作命令を他の端末にも送信する．さらに，2.2節で述べた**要件14**を満たすために，遠隔操作命令を他の端末から紛失・盗難端末へ転送する．意図的に遠隔操作命令から逃れていると考えられる端末は，紛失・盗難に遭ったと見なして，自らの初期化を行う．

(2) 1方向性通信路を用いた端末遠隔操作

2.2節で述べた**要件15**を満たすために，遠隔操作命令は，暗号鍵配布用の制御命令と同様に，1方向性通信路を用いた放送型配布を行う．

5. 実　　装

5.1　暗号アルゴリズムの実装

共通鍵暗号アルゴリズムとして，Camellia[23),24)]を実装し，鍵長は128ビットを選択する．また，乱数生成アルゴリズムについては，乱数生成検定を満たすハードウェア（物理乱数生成装置）を採用する．

5.2　鍵配布・共有方式の実装

本節では，モバイル通信端末でEnd-to-End暗号化を行うための暗号鍵の配布・共有方式の実装について説明する．以下に，提案方式における具体的な鍵配布・共有手順を示す．端末紛失・盗難発生時の暗号鍵を含む端末内機密情報の消去については，5.3節で説明する．

5.2.1　3種類の暗号鍵

提案方式では，以下に示す3種類の鍵を用いる．

(1) デバイス鍵 Kd

モバイル通信端末ごとに異なる鍵．システム管理サーバとモバイル通信端末の間で事前共有することによって，システム管理サーバとモバイル通信端末の間の通信（マスタ鍵の配布等）の暗号化や改ざん防止を実現する．以下，端末Xのデバイス鍵をKd<X>と表す．

(2) マスタ鍵 Km

モバイル通信端末間の暗号化通信に用いるベースとなる鍵．システム管理サーバによって一括生成されて，各々のモバイル通信端末に配布される．システム管理サーバによって採番され，鍵ごとに異なる鍵IDを含む．以下，端末Aと端末Bの間の暗号化通信用マスタ鍵をKm<A,B>と表す．

(3) セッション鍵 Ks

モバイル通信端末間のリアルタイム暗号化通信において，実際に通信内容の暗号化に用いられる鍵．モバイル通信端末どうしで共有したマスタ鍵をもとに，それぞれの端末において

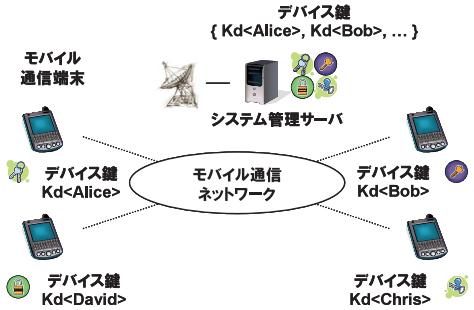


図 2　デバイス鍵の事前共有
Fig. 2　Pre-sharing device key.

導出する．セッション鍵は，導出関数を繰り返し適用することによって，1 つのマスタ鍵から複数生成可能である．以下，マスタ鍵 Km<A, B> から導出される最初のセッション鍵を Ks^1(Km<A, B>) と，第 N 世代目のセッション鍵を Ks^N(Km<A, B>) と表す．

これらの暗号鍵を用いて，暗号化・復号・改ざん検出用認証値の計算を行う．以下，鍵 K を用いた平文 X の暗号化を Enc(K, X) と，鍵 K を用いた改ざん検出対象 X の認証値の計算を MAC(K, X) と，鍵 K を用いた平文 X の改ざん検出対象認証値付き暗号化を EncM(K, X) と表す．

5.2.2　デバイス鍵の事前共有

システム運用開始にあたり，あらかじめ，システム管理サーバにおいて，モバイル通信端末ごとに異なるデバイス鍵 Kd を生成し，各々の端末に事前配布する．この結果，システム管理サーバと各々の端末は，それぞれのデバイス鍵 Kd< · · · > を共有する．**図 2** の例では，システム管理サーバは，Alice，Bob，Chris，David のモバイル通信端末に対して，それぞれ Kd<Alice>，Kd<Bob>，Kd<Chris>，Kd<David> を生成し，事前配布する．デバイス鍵 Kd を用いた暗号化や改ざん検出用認証値の演算を行うことで，システム管理サーバ・端末間の通信をセキュアに行うことができる．すなわち，システム管理サーバと各端末の間で，安全な通信路が確保されたことになる．

5.2.3　マスタ鍵の生成と配布

運用期間中，システム管理サーバは各々のモバイル通信端末間で暗号化通信に必要となるすべての暗号鍵（マスタ鍵）Km を生成し，その鍵を利用する端末のみが復号可能となるように暗号化する．

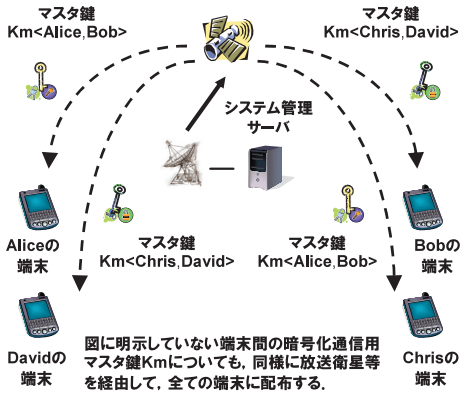


図 3　マスタ鍵の生成と配布
Fig. 3　Generation and distribution of master keys.

たとえば，Alice と Bob が暗号化通信するためのマスタ鍵 Km<Alice, Bob> を生成し，Alice と Bob の端末のデバイス鍵 Kd<Alice>，Kd<Bob> でのみ復号可能となるように暗号化する．鍵暗号化用の一時鍵 Ktmp を生成してマスタ鍵 Km<Alice, Bob> を暗号化し，一時鍵を Alice と Bob の端末のデバイス鍵 Kd<Alice>，Kd<Bob> でそれぞれ改ざん検出用認証値付き暗号化したものを添付する．すなわち，

$$M_{Km<Alice,Bob>} = Enc(Ktmp, Km<Alice, Bob>) \| EncM(Kd<Alice>, Ktmp) \| EncM(Kd<Bob>, Ktmp)$$

という暗号鍵配布命令 $M_{Km<Alice,Bob>}$ を生成する．

また，Chris と David が暗号化通信するためのマスタ鍵 Km<Chris, David> を生成し，Chris と David のデバイス鍵 Kd<Chris>，Kd<David> でのみ復号可能となるように暗号化し，暗号鍵配布命令 $M_{Km<Chris,David>}$ として配布する．同様に，Alice，Bob，Chris，David がそれぞれの間で暗号化通信するためのすべての組合せのマスタ鍵を生成，配布する．

暗号化したマスタ鍵は，システム管理サーバから各端末への制御コマンドを送信するための 1 方向性通信路を通して，各々の端末に配布する（**図 3**）．マスタ鍵は，定期的に（たとえば 24 時間ごとに），あるいは一定の条件を満たす（たとえば一定回数の暗号化通信に使用する）ごとに更新する．システム管理サーバからの鍵配布時，圏外に存在した端末や電源が入っていない端末には，暗号鍵が届かない可能性がある．したがって，同じ鍵を繰り返し（たとえば 1 時間ごとに）再送配布する．

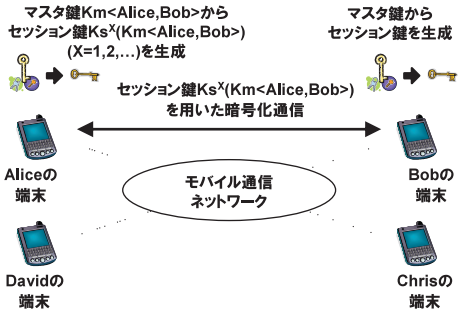


図 4　セッション鍵の生成
Fig. 4　Derivation of session key.

5.2.4　セッション鍵の生成

システム管理サーバによるマスタ鍵 Km の配布によって，暗号化通信開始時，各々のモバイル通信端末は，マスタ鍵 Km を事前共有している．各々の端末は，マスタ鍵 Km を直接暗号化に利用する代わりに，マスタ鍵 Km から計算して求められるセッション鍵 Ks を生成し，通信内容を暗号化する．セッション鍵は，一定回数の暗号化に使用するごとに，再生成する[25]．**図 4** の例では，Alice と Bob の端末は，事前共有したマスタ鍵 Km<Alice, Bob> から生成するセッション鍵 Ks^1(Km<Alice, Bob>), Ks^2(Km<Alice, Bob>), ⋯ を用いて，通信内容 $\{C_1, C_2, \cdots, C_N\}$ を暗号化する．たとえば，1000 回暗号化するごとにセッション鍵を更新する場合は，

$$\mathrm{Enc}(Ks^1(\mathrm{Km<Alice, Bob>}), \mathrm{Cn}) | 1 \leqq n \leqq 1000$$
$$\mathrm{Enc}(Ks^2(\mathrm{Km<Alice, Bob>}), \mathrm{Cn}) | 1001 \leqq n \leqq 2000$$
$$\cdots$$

のように，通信内容を暗号化してやりとりする．

5.2.5　マスタ鍵の転送

マスタ鍵 Km は，システム管理サーバにおいて一括生成・配布し，各々のモバイル通信端末で生成することは許可しない．通信相手の端末にシステム管理サーバから配布されるマスタ鍵 Km が届かなかった場合に備えて，各端末はシステム管理サーバから受信した，利用端末向け暗号化および改ざん検出用認証値付きの暗号鍵配布命令形式のマスタ鍵 $M_{Km<X,Y>}$ を，そのまま端末内部に保管しておく．通信開始時，暗号化に使用予定のマスタ鍵 Km の鍵 ID（鍵ごとに異なる値）を交換して，共通のマスタ鍵 Km を事前共有していることを確認する．相手端末との間でマスタ鍵 Km の共有状態でない場合，たとえば，いずれか一方がマスタ鍵 Km をまったく保有していない場合は，保有する端末から他方の端末へ，配布命令形式のマスタ鍵 $M_{Km<X,Y>}$ を転送する．あるいは，保有しているマスタ鍵 Km の世代（鍵 ID）が一致しない場合，より新しい世代のマスタ鍵 Km を保有する端末から他方の端末へ，配布命令形式のマスタ鍵 $M_{Km<X,Y>}$ を転送する．転送された配布命令 $M_{Km<X,Y>}$ を受け取った端末は，システム管理サーバと自端末のみが保有するデバイス鍵 Kd で復号することによって，その正当性を確認したうえで利用する．

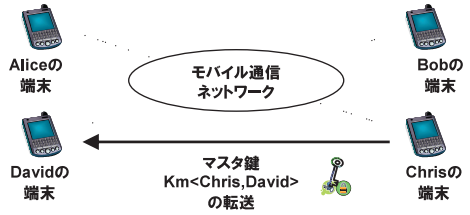


図 5　マスタ鍵の転送
Fig. 5　Transfer of master key.

たとえば，Chris と David が暗号化通信を行う際，David の端末に Chris との暗号化通信用マスタ鍵 Km<Chris, David> が届いていない，と仮定する．通信開始時，Chris の端末は保有しているマスタ鍵 Km<Chris, David> の鍵 ID を送信し，David の端末が同じマスタ鍵を保有していないことを確認した場合，システム管理サーバから受信した状態で保管しておいた配布命令形式のマスタ鍵

$$M_{Km<Chris,David>} = \mathrm{Enc}(\mathrm{Ktmp}, \mathrm{Km<Chris, David>}) \| \mathrm{EncM}(\mathrm{Kd<Chris>}, \mathrm{Ktmp}) \| \mathrm{EncM}(\mathrm{Kd<David>}, \mathrm{Ktmp})$$

を転送する．David の端末は，転送された配布命令 $M_{Km<Chris,David>}$ に対して，David のデバイス鍵 Kd<David> を用いて EncM(Kd<David>, Ktmp) の復号および改ざん検出用認証値の演算を行い，システム管理サーバによって生成された配布命令であることを確認した後，Enc(Ktmp, Km<Chris, David>) を復号してマスタ鍵 Km<Chris, David> を取り出す．これによって，Chris と David の端末はマスタ鍵 Km<Chris, David> を共有し，暗号化通信を行うことができる（**図 5**）．

なお，Chris と David の両方にマスタ鍵が届かなかった場合は，両端末は暗号化通信を行うことができない．しかしながら，たとえば，0.1%の確率でマスタ鍵の不達が発生すると仮定すると，マスタ鍵の転送を行わない場合は 0.2%の確率で暗号化通信に失敗するが，転

表 1　各暗号鍵の更新周期の運用例
Table 1　Example of key renewal cycles.

暗号鍵の種類	更新周期	
	ケース A	ケース B
デバイス鍵	一日	一週間
マスタ鍵	4 時間	24 時間
セッション鍵	約 30 秒毎	約 3 分毎

送を行うことによって，その確率は 0.0001%まで減少させることができる．

5.2.6　デバイス鍵の更新

これまで示したように，提案方式では，デバイス鍵 Kd を用いてマスタ鍵 Km を配布し，マスタ鍵 Km から生成したセッション鍵 Ks で通信内容を暗号化する．このとき，デバイス鍵 Kd が漏洩すると，それによって配布されたすべてのマスタ鍵 Km やそこから生成したすべてのセッション鍵 Ks，Ks を用いて暗号化されたすべての通信内容が盗聴されてしまう．したがって，デバイス鍵 Kd の更新が不可欠である．

たとえば，毎日，あるいは 1 週間に 1 回，モバイル通信端末が安全な保管場所に持ち帰られる運用を考える．保管場所にシステム管理サーバが設置されている場合は，更新するデバイス鍵 Kd' を生成し，システム管理サーバおよびモバイル通信端末上のデバイス鍵 Kd を更新する．保管場所にシステム管理サーバが設置されていない場合は，システム管理サーバにおいて，あらかじめ複数世代分のデバイス鍵 Kd, Kd', Kd", $\cdots$ を生成し，メモリカード等に格納して，保管場所で安全に保管しておく．モバイル通信端末が保管場所に持ち帰られた際，デバイス鍵の更新周期に応じて，メモリカードからデバイス鍵をコピーすることで更新を行う．

あるいは，モバイル通信端末を定期的に安全な保管場所に持ち帰ることが運用上困難なことも考えられる．この場合は，1 方向性関数に基づく鍵更新メカニズムをシステム管理サーバとモバイル通信端末に実装しておき，システム管理サーバからデバイス鍵更新命令を送信することによって，事前共有した鍵を更新する方法[26] を用いて，デバイス鍵 Kd の定期的な更新を行う．各暗号鍵の更新周期として考えられる運用例を**表 1** に示す．

5.3　端末紛失・盗難対策の実装

本節では，モバイル通信端末の紛失・盗難による，暗号鍵の漏洩，端末の不正利用，端末内機密情報の漏洩を防止するための対策の実装について説明する．以下に，提案方式における具体的な遠隔管理手順を示す．

5.3.1　端末初期化命令の生成と配布

端末紛失・盗難に気付いた利用者は，何らかの方法でシステム管理者に連絡する．端末紛失・盗難の連絡を受けた管理者は，システム管理サーバで端末初期化命令を生成する．端末初期化命令 M_{Init} には，該当端末を特定する端末 ID を示す TermID，命令日時 Date，初期化する理由 Reason，システム管理サーバが作成した正規の情報であることを検証するための改ざん検出用認証値 MACs を含む．すなわち，

$$M_{InitTBA} = \mathrm{TermID}\|\mathrm{Date}\|\mathrm{Reason}$$
$$\mathrm{MACs} = \mathrm{MAC}(\mathrm{Kd}<\mathrm{Target}>, M_{InitTBA})\| \mathrm{MAC}(\mathrm{Kd}<\mathrm{Others}_1>, M_{InitTBA})\|\mathrm{MAC}(\mathrm{Kd}<\mathrm{Others}_2>, M_{InitTBA})\|\cdots$$
$$M_{Init} = M_{InitTBA}\|\mathrm{MACs}$$

である．システム管理サーバは，1 方向性通信路を通して，端末初期化命令 M_{Init} を各端末に緊急配布する．自端末宛の端末初期化命令 M_{Init} を受信した端末は，改ざん検出用認証値 $\mathrm{MAC}(\mathrm{Kd}<\mathrm{Target}>, M_{InitTBA})$ を検証して命令の正当性を確認した後に端末の初期化を行い，これによって，該当端末内の機密情報は消去される．他の端末宛の端末初期化命令を受信した端末は，改ざん検出用認証値 $\mathrm{MAC}(\mathrm{Kd}<\mathrm{Others_X}>, M_{InitTBA})$ を検証して命令の正当性を確認した後，自らが保持する初期化端末のリスト（通信禁止端末リスト）に TermID を追加するとともに，該当端末との間のマスタ鍵 $\mathrm{Km}<\mathrm{Mine}, \mathrm{Target}>$ を端末から消去する．さらに，端末初期化命令 M_{Init} を端末内部に保管しておく（**図 6**）．

端末初期化命令 M_{Init} の不達に備えて，システム管理サーバは，命令を繰り返し再送する．たとえば，最初の 1 時間以内は 1 分ごとに送信し，その後 24 時間以内は 10 分ごとに送信する．

5.3.2　端末初期化命令の交換と転送

各々のモバイル通信端末は，受信した端末初期化命令 M_{Init} を，端末内に格納しておき，端末間で通信が発生した際に命令を転送しあうことによって，通信禁止端末リストを更新する（**図 7**）．たとえば，命令受信後 24 時間以内に端末間で通信が行われた場合，互いが保有している端末初期化命令 M_{Init} を確認しあい，必要に応じて命令の転送を行う．

紛失・被盗難端末を入手した不正利用者は，圏外への移動・一時的な端末電源断等によって，端末初期化命令 M_{Init} の受信を逃れた後，他の端末への成りすまし通信を試みる可能性がある．該当端末からの通信要求を受けた端末は，通信に応じる代わりに，システム管理サーバから受信しておいた端末初期化命令 M_{Init} を転送する．他の端末から端末初期化命令 M_{Init} を転送された該当端末は，M_{Init} に含まれる改ざん検出用認証値 $\mathrm{MAC}(\mathrm{Kd}<\mathrm{Target}>, M_{InitTBA})$

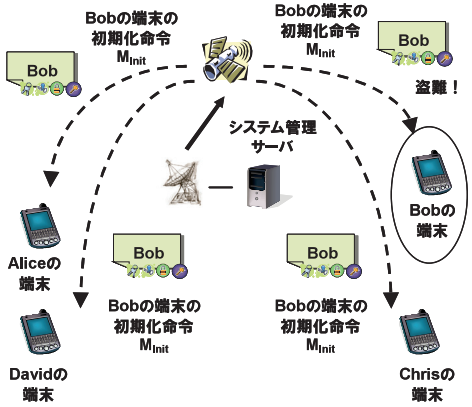


図 6　端末初期化命令の生成と配布
Fig. 6　Generation and distribution of terminal initialization command.

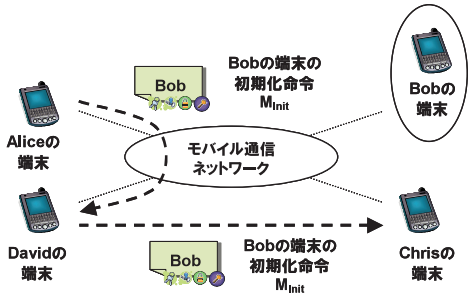


図 7　端末初期化命令の交換
Fig. 7　Exchange of terminal initialization command.

を検証して命令の正当性を確認した後，システム管理サーバから直接送信された場合と同様に，初期化処理を行う．これよって，システム管理サーバからの直接制御に加えて，他の端末の協調動作によって，不正端末を除外することができる（**図 8**）．

5.3.3　制御信号の圏外逃亡対策

システム管理サーバからの制御信号，あるいは他の端末から転送される制御信号から逃れるために，圏外に持ち去ったまま二度と圏内に戻らない端末への対策を考える必要がある．

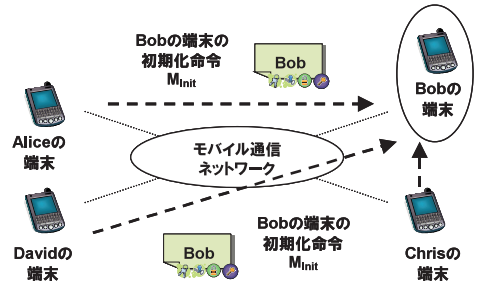


図 8　端末初期化命令の転送
Fig. 8　Transfer of terminal initialization command.

たとえば，システム管理サーバから端末へ定期的にアクティベーション信号を送信することとし，一定期間信号を受信しない端末は，「盗難に遭い圏外に持ち出された可能性がある」として自律的に初期化する方法がある．ただし，今回は正規利用者が所有中に誤って紛失・盗難と判断してしまうリスクを回避するために，この対策は実装していない．

5.4　プロトコル設計と実装例

5.4.1　プロトコル設計

我々は，5.2 節で述べた暗号鍵管理を実現する鍵配布・共有プロトコル，5.3 節で述べたモバイル通信端末の管理を実現する端末管理プロトコルを設計した．システム管理サーバと端末の間の通信（1 方向性通信を用いた鍵・端末管理用制御命令）については，新たにプロトコルを開発した．端末間の暗号化リアルタイム通信は，業界標準プロトコルである SIP [27]（Session Initiation Protocol），RTP（Real-Time Transport Protocol），SRTP（Secure Real-time Transport Protocol）を採用し，SRTP で暗号化に用いる鍵を共有する手段の候補の 1 つとして規定されている MIKEY（Multimedia Internet KEYing）の代わりに，先に述べた鍵管理と端末管理を両立させた独自プロトコルを採用した．また，端末間で共有済みの鍵が存在しない場合のネゴシエーションや鍵の転送については，SDP [28]（Session Description Protocol）を独自拡張して，これらの情報を SIP メッセージとともに交換することとした．

以下に，マスタ鍵 Km の転送処理（図 5）の実装において設計した具体的なプロトコルの例を示す．**図 9** は，モバイル通信端末間の暗号化通信開始時における，マスタ鍵 Km を転送するシーケンスの一例である．端末の保有するマスタ鍵 Km の世代にずれが生じて同じ鍵を持っていないため，通信要求側の端末から受信側の端末にマスタ鍵 Km を転送してい

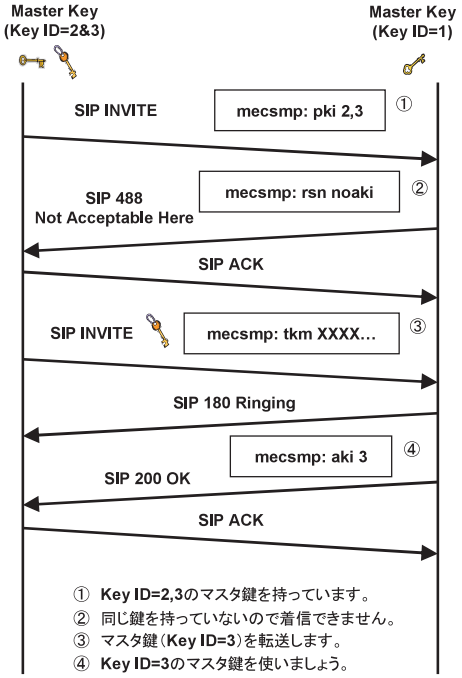


図 9　マスタ鍵の転送シーケンス例 1
Fig. 9　Sequence example 1 of transferring master key.

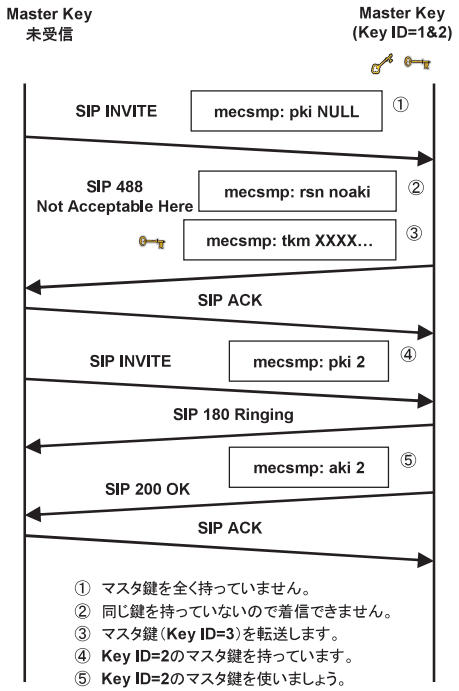


図 10　マスタ鍵の転送シーケンス例 2
Fig. 10　Sequence example 2 of transferring master key.

る．シーケンス図において，四角で囲んだテキストは，拡張した SDP を用いたネゴシエーション情報や転送する配布命令形式のマスタ鍵 $M_{Km<X,Y>}$ である．

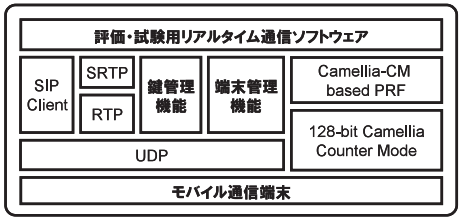
図 10 は，マスタ鍵 Km を転送するシーケンスのもう 1 つの例である．通信要求側の端末はマスタ鍵 Km をいっさい保有していないにもかかわらず，暗号化通信の開始を要求する．受信側の端末から通信要求側の端末に配布命令形式のマスタ鍵 $M_{Km<X,Y>}$ を転送することによって，暗号化通信を可能としている．その他のプロトコル例については，紙面の都合で割愛する．

5.4.2　プロトタイプ実装

設計したプロトコルを実装したモバイル通信端末のアーキテクチャを，**図 11** に示す．プロトタイプ実装では，CPU にクロック周波数 400 MHz または 528 MHz のマイクロプロセッサ，OS に Microsoft Windows Mobile を用いたスマートフォンをモバイル通信端末として採用し，暗号化リアルタイム通信，鍵管理，端末管理に必要な各プロトコルを実装した．また，SRTP における共通鍵暗号アルゴリズムとして，標準で規定されたアルゴリズムの代わりに，Camellia を実装した．なお，今回のプロトタイプ実装においては，システム管理サーバ上のハードウェア乱数生成装置を，疑似乱数生成ソフトウェアの実装で代用している．

6.　評　　価

5.4 節で述べたプロトタイプ実装を行ったモバイル通信端末を 16 台用意し，無線 LAN（IEEE 802.11 b/g）および移動体データ通信サービス（W-CDMA，HSDPA）を介して，



SIP : Session Initiation Protocol
SRTP : Secure Real-time Transport Protocol
RTP : Real-time Transport Protocol
UDP : User Datagram Protocol
CM : Counter Mode
PRF : Pseudo-Random Function

図 11　モバイル端末上の実装例
Fig. 11　Implementation example on mobile device.

動作確認を行った．実験環境上の制約から，システム管理サーバからモバイル通信端末への各制御命令の配布は，端末どうしのモバイルネットワーク経由とし，通信方向を 1 方向に限定することで，放送型配布をエミュレートした．

6.1　端末数=16 台での評価

16 個のデバイス鍵 Kd を事前作成し，システム管理サーバとモバイル通信端末 16 台の間で各々デバイス鍵 Kd を事前共有するようにインストールした．16 台のモバイル通信端末に対して，システム管理サーバから暗号鍵（マスタ鍵）Km を配布・更新することで，暗号化通信を実施した．システム管理サーバにおいて，10 分ごとにマスタ鍵 Km を更新し，同じ鍵を 2 分間隔で再送するように設定した．それぞれのマスタ鍵 Km の有効期限は，発行後 1 時間として発行した．鍵長 128 ビットのマスタ鍵 Km を配布するための暗号鍵配布メッセージ M_{Km} は 1 つあたり 1,056 ビットであった．端末数=16 台の場合，マスタ鍵 Km の総数は 120 個であり，通信速度 64 kbps の帯域保証型 1 方向性通信路を用いて，マスタ鍵 Km 一式の送信は約 2 秒で完了した．各々のモバイル通信端末において，マスタ鍵 Km を受信して復号するための処理時間は，1.0×10^{-5} 秒以下と，無視できる範囲内であった．すなわち，前述の条件での鍵配布は，システム管理サーバ，モバイル通信端末，ネットワークのそれぞれに対して負荷とはならなかった．

マスタ鍵 Km の配布終了後，任意の端末間で暗号化通信を試みたところ，システム管理サーバから事前に受信したマスタ鍵 Km から各々の端末で生成するセッション鍵 Ks を用いて，即時暗号化通信ができることを確認した．いずれか一方の端末にマスタ鍵 Km が届かない状況を作り出したところ，5.4 節で示した転送シーケンスに従って，端末間で自動的に配布命令形式のマスタ鍵 M_{Km} を転送した．転送されたマスタ鍵 Km の正当性は，鍵付きハッシュアルゴリズムにより確認のうえ，複雑な検証をすることなく，即時通信に使用することができた．また，共通鍵暗号アルゴリズムとして Camellia を用いた SRTP によるリアルタイム通信内容の暗号化処理は，40 ミリ秒分のリアルタイム通信データの暗号化時間が 1.29×10^{-2} ミリ秒（実効暗号化速度 38.4 Mbps）と十分高速であり，そのオーバヘッドは無視できる範囲内であった．この間，利用者は，端末内部で行われる通信内容の暗号化やセッション鍵 Ks の更新処理等を意識することなく，セキュアなリアルタイム通信を行うことができた．この結果，利用者が特別な操作を必要とせず，暗号鍵の共有や定期的更新，暗号化通信を実現できることを確認した．

また，モバイル通信端末の紛失・盗難が発生したことを想定して，端末初期化の実験を実施した．システム管理サーバから，事故発生から 1 時間の間，1 分間隔で端末初期化命令 M_{Init} を送信した．端末初期化命令 M_{Init} は，端末数=16 台の場合，1 命令あたり 3,139 ビットであった．これによって，該当不正端末の初期化を行うとともに，他の端末に事故発生を通知した．不正端末に端末初期化命令 M_{Init} が届いた場合は，不正端末はただちに初期化された．また，不正端末が端末初期化命令 M_{Init} を回避した状況を作り出し，その場合は，他の端末と通信を試みた瞬間に命令が転送されて，ただちに端末初期化の遠隔操作が行われた．このように，モバイル通信端末の紛失・盗難が発生した場合，システム管理サーバからの遠隔管理や他の端末の協調による動作によって，該当不正端末を除外できることを確認した．

以上のことから，端末数=16 台の場合，機能面および性能面で問題なく実運用可能であることを確認した．

6.2　端末数=100〜1,000 台での評価

2.1 節で述べたように，提案方式は最大数百台のモバイル通信端末で運用することを想定している．端末数が増加した場合，事前準備する端末台数分のデバイス鍵 Kd の数は増加するが，運用自体が複雑化することはない．しかしながら，運用中にシステム管理サーバによって生成・配布されるマスタ鍵 Km の総数が増加するため，システム管理サーバの処理性能，システム管理サーバから各モバイル通信端末への 1 方向性通信路の通信性能が十分でなければならない．また端末初期化命令 M_{Init} の長さが増加するので，考慮する必要がある．本節では，端末数=100〜1,000 台の場合の実現可能性を評価する．なお，実際に 1,000 台の端末を用意することはできないので，実効値を用いて理論的に計算した値によって性能

表 2　モバイル通信端末数と暗号鍵の総数の関係
Table 2　Number of mobile terminal and encryption key.

モバイル通信端末数	暗号鍵の総数
16	120
100	4,950
1,000	499,500

表 3　端末数，乱数生成速度と鍵生成時間の関係
Table 3　Number of terminals, random number generation speed and key generation time.

端末数	乱数生成速度と鍵生成に要する時間	
	1Mbyte/s	24Mbyte/s
16	1.8×10^{-3} 秒	7.6×10^{-5} 秒
100	7.6×10^{-2} 秒	3.1×10^{-3} 秒
1,000	7.6 秒	0.32 秒

評価を行う．

最初に，暗号鍵（マスタ鍵）Km の配布・更新を行う際の性能を評価する．モバイル通信端末数の二乗のオーダでマスタ鍵 Km の総数は増大する（**表 2**）ので，マスタ鍵 Km の生成時間，配布形式 M_{Km} に変換するためのマスタ鍵 Km の暗号化時間，システム管理サーバから各モバイル通信端末へのマスタ鍵配布命令 M_{Km} の通信時間を検証する．

実効乱数生成速度 1 Mbyte/s および 24 Mbyte/s の物理乱数生成装置を利用した場合のマスタ鍵 Km の鍵生成時間を**表 3** に示す．端末数に応じて適切な物理乱数生成装置を選択することによって，十分実現可能である．

マスタ鍵 Km を配布形式 M_{Km} に変換する際に行う暗号化時間に関して，実効暗号化速度 300 Mbps（800 MHz クラスのマイクロプロセッサ使用）および 1.2 Gbps（3 GHz クラスのマイクロプロセッサ使用）とした場合の値を**表 4** に示す．システム管理サーバとして，市販の PC 程度の処理能力を持った計算機を利用することで，十分実現可能である．

システム管理サーバから各々のモバイル通信端末へのマスタ鍵配布命令 M_{Km} の通信時間を検証する．**表 5** に示したように，端末数に応じて通信速度 384 Mbps や 54 Gbps の高速回線を 1 方向性通信路として用いることによって，実現可能である．ただし，通信路は理論値と実際のスループットとの間で差を生じやすいので，余裕を持った回線を準備することが重要である．

次に，端末の紛失・盗難発生時の遠隔管理を行う際の性能を評価する．端末初期化命令

表 4　端末数，暗号化速度と鍵暗号化時間の関係
Table 4　Number of terminals, encryption speed and key encryption time.

端末数	暗号化速度と鍵暗号化に要する時間	
	300Mbps	1.2Gbps
16	9.8×10^{-5} 秒	2.4×10^{-5} 秒
100	4.0×10^{-3} 秒	9.8×10^{-4} 秒
1,000	0.41 秒	9.9×10^{-2} 秒

表 5　端末数，通信速度と鍵配布時間の関係
Table 5　Number of terminals, communication speed and key distribution time.

端末数	通信速度と鍵配布に要する時間		
	64kbps	384Mbps	54Gbps
16	1.9 秒	3.1×10^{-4} 秒	2.1×10^{-6} 秒
100	77 秒	1.3×10^{-2} 秒	8.7×10^{-5} 秒
1,000	130 分	1.3 秒	8.8×10^{-3} 秒

表 6　モバイル通信端末数と端末管理遠隔操作命令の長さの関係
Table 6　Number of terminals and length of remote terminal management command.

端末数	命令長
16	3.2k ビット
100	18.9k ビット
1,000	188k ビット

M_{Init} の大きさは，モバイル通信端末の総数に比例する（5.4 節で述べたプロトタイプ実装における実測値を**表 6** に示す）が，端末数に応じた通信回線を用いていれば，1 秒未満で配布することが可能である．遠隔管理が必要となる端末の紛失・盗難は，定期的な鍵配布・更新のように頻繁に発生するわけではないので，これらの処理に関するシステム管理サーバおよび端末の処理のオーバヘッドは，無視できる範囲内であり，十分実現可能である．

6.3　暗号アルゴリズムの選択に関する評価

共通鍵暗号アルゴリズムは，高速処理が可能な反面，端末数の増加にともない鍵総数が膨大となる欠点がある．一方，公開鍵暗号アルゴリズムは鍵総数を抑えることができる反面，処理が遅い（モバイル通信端末における RSA と Camellia の暗号化速度を測定したところ，公開鍵は共通鍵の 60 倍，秘密鍵は共通鍵の 1,200 倍の処理時間を要した）という欠点がある．6.2 節に示したように，本システムの前提条件である数百台程度のモバイル通信端末で

運用するならば，端末の総数に応じて適切な装置，計算機，通信回線を選択することによって，共通鍵の運用コストは許容範囲内に収まる．したがって，本論文の提案方式である共通鍵暗号アルゴリズムのみを用いて暗号鍵および端末の管理を実現する選択は正しいといえる．

7. おわりに

地球上のいかなる場所においても，厳格にセキュアなリアルタイム通信を提供するための方式として，放送型通信を用いて端末間通信用の暗号鍵を高頻度に更新し続けることによって，盗聴の脅威を最小限に抑える方式を提案した．暗号鍵配送の仕組みを端末の遠隔操作に対しても応用することによって，端末紛失・盗難時の機密情報漏洩対策も実現した．システム管理サーバとモバイル通信端末の間および端末どうしの間の通信プロトコルを設計し，プロトタイプ実装を行って，暗号化通信が可能であること，端末遠隔管理が機能することを確認した．システム規模に応じて適切な機器，計算機，通信回線を選択することによって，提案方式に基づく運用が可能であることを示した．

現在の提案方式では，システム管理サーバにおいてすべての暗号鍵（マスタ鍵）そのものを生成・配布している．モバイル通信端末の台数が n の場合，システム管理サーバにおいて生成・配布すべき鍵の総数は，${}_nC_2 = n(n-1)/2$ となる．すべての端末どうしの組合せにおいて暗号化通信を行わないことが自明であれば，あらかじめ生成・配布する暗号鍵を通信する可能性のある関係に限定することも可能であるが，端末数の増加にともない鍵の総数は膨大となるため，端末数が数百台という現在の前提条件が成り立たない場合の適用は難しい．今後は，Blom の事前鍵配送方式[29] 等の方法と組み合わせることによって，生成・配布すべき情報量を削減することを検討する．

5.2.6 項で述べた放送型通信を用いたデバイス鍵の更新については，プロトタイプ実装を行っていない．今後，実装して有効性を評価する必要がある．また，5.3.3 項で述べたシステム管理サーバからのアクティベイト信号による端末遠隔管理に関しては，正規ユーザが端末を正しく保有し続けていても，アクティベイト信号が受信できない状況にあった場合，盗難と判断して初期化されてしまうという弊害があり，現時点ではこの機能を実装していない．今後，この点を考慮し，適切な改良策を検討する余地がある．

謝辞　本研究の内容に関してご議論・ご教授いただいた，三菱電機情報技術総合研究所情報セキュリティ技術部の松井充部長，酒井康行チームリーダ，反町亨主席研究員をはじめとする同部の方々に，謹んで感謝の意を表する．

参考文献

1) ITmedia：携帯,「10 台に 1 台以上が紛失経験あり」～ガードナー.
http://plusd.itmedia.co.jp/mobile/0206/20/n_funsitu.html （参照 2008-05-19）
2) Biham, E. and Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystem, Lecture Notes in Computer Science, 537, Springer Verlag (1990).
3) Matsui, M.: Liner Cryptanalysis Method for DES, *Proc. Eurocrypt '94 – Advances in Cryptology*, Lecture Notes in Computer Science, 765, Springer Verlag (1993).
4) Kocher, P.: Timing Attacks on Implementation of Diffie-Hellman, RSA, DSS and Other Systems, *CRYPTO'96* (1996).
5) Kocher, P., Jaffe, J. and Jun, B.: Differential Power Analysis, *CRYPTO'99* (1999).
6) Tsunoo, Y., Tsujihara, E., Minematsu, K. and Miyauchi, H.: Cryptoanalysis of Block Ciphers Implemented on Computers with Cache, *ISITA2002* (2002).
7) NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General (Revised) (2007).
8) NIST Special Publication 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) (2007).
9) RFC 3830, MIKEY: Multimedia Internet KEYing (2004).
10) Zimmermann, P., Johnston, A. and Callas, J.: ZRTP: Media Path Key Agreement for Secure RTP (2008).
11) RFC 4949, Internet Security Glossary, Version 2 (2007).
12) Neuman, B.C. and Ts'o, T.: Kerberos: An Authentication Service for Computer Networks, *IEEE Communications Magazine*, Vol.32, No.9 (1994).
13) JSAT 株式会社：新衛星マルチキャスト配信サービス「Sky-Access IPcast」本格営業開始．http://www.sptvjsat.com/newsJSAT/news_pdf/070419_JS_Sky-Access.pdf（参照 2008-12-01）
14) Open Mobile Alliance: OMA Device Management Protocol, Approved Version 1.2.1 – 17 Jun 2008 (2008).
15) 金融庁：偽造キャッシュカード問題に関する実態調査結果（資料）.
http://www.fsa.go.jp/news/newsj/16/ginkou/f-20050222-1/01a.pdf（参照 2008-05-20）
16) 楽天リサーチ：携帯電話紛失時の通信事業者によるデータ消去サービス，利用意向は 7 割．http://research.rakuten.co.jp/report/20051110/（参照 2008-05-19）
17) マイクロソフト：強力なパスワード：その作り方と使い方.
https://www.microsoft.com/japan/protect/yourself/password/create.mspx （参照 2008-05-20）
18) ITmedia：パスワードをメモる社員は 3 分の 1—米調査報告書.
http://www.itmedia.co.jp/news/articles/0610/18/news037.html（参照 2008-05-19）

19) 宇根正志，松本　勉：生体認証システムにおける脆弱性について：身体的特徴の偽造に関する脆弱性を中心に，金融研究，日本銀行金融研究所 (2005.7).
20) Matsumoto, T., Matsumoto, H, Yamada, K. and Hoshino, S.: Impact of artificial "gummy" fingers on fingerprint systems, *Proc. SPIE*, Vol.4677 (2002).
21) BBC NEWS: Malaysia car thieves steal finger. http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm（参照 2008-05-19）
22) 國米　仁：奇怪論理と優良誤認に脅かされる情報セキュリティ，日本セキュリティ・マネジメント学会第 19 回全国大会 (2005).
23) 青木和麻呂，市川哲也，神田雅透，松井　充，盛合志帆，中嶋純子，時田俊雄：128 ビットブロック暗号 Camellia，電子情報通信学会技術報告 ISEC2000-6 (2000).
24) Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J. and Tokita, T.: The 128-Bit Block Cipher Camellia, *IEICE Trans. Fundamentals*, Vol.E85-A, No.1 (2001).
25) RFC 3711, The Secure Real-time Transport Protocol (SRTP) (2004).
26) 辻　宏郷，米田　健：複数モバイル端末間における事前共有鍵の更新方式，2009 年暗号と情報セキュリティシンポジウム (SCIS2009) (2009).
27) RFC 3261, SIP: Session Initiation Protocol (2002).
28) RFC 4566, SDP: Session Description Protocol (2006).
29) Blom, R.: An optional class of symmetric key generation schemes, Lecture Notes in Computer Science, 209 (1985).

(平成 20 年 12 月 1 日受付)
(平成 21 年 6 月 4 日採録)

辻　宏郷（正会員）

1988 年東北大学工学部情報工学科卒業．1989 年三菱電機（株）入社．現在，同情報技術総合研究所情報セキュリティ技術部主席研究員．静岡大学大学院理工学研究科博士後期課程在学．コンピュータネットワーク，分散処理システム，情報セキュリティの研究に従事．情報処理学会情報規格調査会委員として，OSI アーキテクチャとセキュリティ，ディレクトリ，PKI/PMI の国際標準化活動に従事．

米田　健（正会員）

1965 年生．1989 年慶應義塾大学理工学部計測工学科卒業．1991 年同大学大学院理工学研究科修士課程修了．1994 年同大学院博士課程修了．博士（工学）．同年三菱電機（株）入社．現在，同社にて情報セキュリティアーキテクチャ，組み込み機器セキュリティ，暗号認証通信プロトコルの研究・開発に従事．著書『コラボレーションとコミュニケーション』（共著，共立出版),『IT Text 情報セキュリティ』（共著，オーム社）．ACM 会員．

水野　忠則（フェロー）

1945 年生．1969 年名古屋工業大学経営工学科卒業．同年三菱電機（株）入社．1993 年静岡大学工学部情報知識工学科教授．1996 年情報学部情報科学科教授．2006 年より創造科学技術大学院教授．工学博士．情報ネットワーク，モバイルコンピューティング，ユビキタスコンピューティングに関する研究に従事．著訳書としては,『コンピュータネットワーク』（日経 BP),『モダンオペレーティングシステム』（ピアソン・エデュケーション）等がある．電子情報通信学会，IEEE，ACM，Informatics Society 各会員．情報処理学会フェロー．

西垣　正勝（正会員）

1990 年静岡大学工学部光電機械工学科卒業．1992 年同大学大学院修士課程修了．1995 年同博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報学部助手．1999 年同講師，2001 年同助教授．2006 年より同創造科学技術大学院助教授．2007 年より准教授．博士（工学）．情報セキュリティ，ニューラルネットワーク，回路シミュレーション等に関する研究に従事．