情報処理学会論文誌 Vol.55 No.1 267–279 (Jan. 2014)

# スマートデバイスにおける利用環境に応じた機能制御機構の提案とその考察

佐藤 亮太[1,†1,a)] 知加良 盛[1] 奥田 哲矢[1,†2] 栢口 茂[1]

受付日 2013年4月10日, 採録日 2013年10月9日

**概要**：スマートフォンやタブレットなどスマートデバイスの急速な普及により，個人所有のスマートデバイスを企業における業務でも利用する形態など，スマートデバイスが様々な環境において利用されている．それにともない，スマートデバイスが利用される様々な環境に応じたセキュリティの確保が課題となっている．特に，スマートデバイスの可搬性や多機能性といった特徴から，スマートデバイスの利用される環境に応じた機能の制御が，そのセキュリティ対策として考えられる．さらに，スマートデバイスの利用者のセキュリティ意識が多様であることも指摘されているため，スマートデバイスが利用される環境に応じて，様々な機能が自律的に制御されることが重要である．本稿では，スマートデバイスが利用される場所に応じて，コンテンツの閲覧やアプリケーションの起動といった機能を自律的に制御する機能制御機構を提案する．機能制御機構の実現にむけ，ID ベース暗号と呼ばれる，ID 情報を公開鍵としてデータの暗号化を行う暗号技術を応用する．この ID ベース暗号を用いて，あらかじめ特定の場所を表す ID 情報に基づき暗号化されたコンテンツやアプリケーションの起動制御ファイルが，その特定の ID 情報を取得できるスマートデバイスのみが復号可能とする．これにより，コンテンツの閲覧やアプリケーションの起動といった機能の利用に関する認可情報を事前に配布し，復号の可否をもって機能を制御する新たな手法を提案する．また，本提案方式を，スマートデバイス上で動作するアプリケーションとそれを管理する機能制御サーバ，復号鍵を生成する鍵管理サーバなどで構成されるシステムとして実装する．そして，その実装されたシステムにおいて，構成する各端末の処理性能を評価することで本提案方式の実行性について確認するとともに，特に機能制御機構の管理者側の観点から本提案方式の有用性について述べる．

**キーワード**：スマートデバイス，ID ベース暗号，位置情報，機能制御，セキュリティ

# A Proposal of Situation-sensitive Function Controller for Smart Devices and Its Evaluation.

Ryota Sato[1,†1,a)] Sakae Chikara[1] Tetsuya Okuda[1,†2] Shigeru Kayaguchi[1]

Received: April 10, 2013, Accepted: October 9, 2013

***Abstract:*** According to the rapid spread of smart devices, their usage pattern is becoming diversified. For instance, some companies are allowing employees to use their personal smart devices at work. Such usage style is called BYOD (Bring Your Own Device). The situation in which smart devices are used changes dynamically so that the functions of smart devices should be controlled depending on the situation. In particular, because of the mobility, multi-functionality and the low awareness of security issues among users, the usage of applications and contents should be controlled flexibly and autonomously depending on its situation. In this paper, we propose a platform to control the functions of smart devices according to its situation. We introduce an ID-based encryption mechanism to realize the platform. Functionality can be controlled flexibly according to the usage situation, by decrypting the encrypted configuration file or contents according to decryption key conditions. The policy located in the control server in the company site can be applied automatically, for example, preventing an employee's privately owned smart device application from being launched on company premises, or only allowing corporate applications to be launched on premises. We mention the implementation of the platform and evaluate the performance at smart devices and the servers.

***Keywords:*** smart device, ID-based encryption, location information, function control, security

## 1. はじめに

近年，スマートフォンやタブレットなどのスマートデバイスが急速に普及している [1]．スマートデバイスは，電話やメールなどのコミュニケーションツールや情報収集，スケジュール管理など個人の生活を支える重要な端末の 1 つである．一方で，スマートデバイスの持つ多機能性を活かし，企業における業務端末としてのビジネス利用も進められている．特に，個人所有のスマートデバイスを業務でも利用する形態は，BYOD（Bring Your Own Device）として注目を集めている [2]．このように個人や企業でのスマートデバイスの利用が進む中で，スマートデバイスを対象としたマルウェアの増加や紛失，盗難など，利用時のリスクも数多く指摘されており [3], [4]，そのセキュリティ対策の検討が進められている [5]．特に BYOD においては，個人所有のスマートデバイスが企業において利用されるため，その端末におけるセキュリティ担保は，個人の意識に依存するところが大きい．そのため，業務利用時における企業の機密情報の漏えい防止などに向けて，スマートデバイスの適切な管理や制御が検討されている [6]．

本稿においては，上述した BYOD の例のように，単一のスマートデバイス端末を複数環境で利用する際のセキュリティ確保について検討する．また，本稿が対象とするセキュリティとして，スマートデバイスが取り扱う文書や写真といったコンテンツに対する利用環境に応じた機密性の確保やこれらコンテンツを利用するアプリケーションの適切な利用に着目する．

このセキュリティ確保においては，たとえば，企業のセキュリティポリシに照らし合わせてスマートデバイス上のコンテンツの閲覧やそれらコンテンツを利用するアプリケーションの起動といった機能を，利用環境とは無関係に制御する方法が考えられる．しかし，この方法では自宅など企業の所掌範囲外においてスマートデバイスの利用者（以降，利用者）はスマートデバイスの機能を自由に利用することができないという問題がある．つまり，スマートデバイスの可搬性や多機能性といった特徴を活かしながらセキュリティを確保する必要がある．したがって，スマートデバイスが利用される環境に応じ，その様々な機能が適切に制御される機構が求められる．

一方，スマートデバイスは年齢や性別などによらず広く普及しているため利用者のセキュリティ意識が多様であり，特にセキュリティ意識が低い利用者が多いことも指摘されている [5]．したがって，セキュリティ対策においては利用者のセキュリティ意識に依存しないことも重要な要件と考えられる．そこで，我々はスマートデバイスが利用される環境に応じ，その様々な機能が，利用者の操作などが不要で，自律的かつ適切に制御される機能制御機構を提案する．

本稿では，2 章でスマートデバイスの機能を制御するセキュリティ対策の関連研究と本稿において利用する ID ベース暗号 [7] の関連研究を概観し，3 章で利用環境に応じた機能制御機構に求められる要件を整理するとともに，これら要件を満たす新たな方式を，認証と認可のフレームワークの観点から検討する．この検討で明らかとなった方式実現に向けた課題が，ID ベース暗号を導入した提案方式により解決されることを示す．4 章では，本提案方式をスマートデバイス上のアプリケーションや各種サーバアプリケーションとして実装した結果について述べ，5 章において実装システムの処理性能から本提案方式の実行性について確認する．さらに，6 章では ID ベース暗号を応用した本提案方式が，ID ベース暗号を利用しない方式と比較してサーバの負荷やシステムにおける実装・運用の容易性とスケーラビリティ観点から有用であること述べる．

## 2. 関連研究

Android や iOS，Windows Mobile などのスマートデバイスのプラットフォーム OS は，その端末のセキュリティを担保するための機能を備えている．たとえば，Android OS のバージョン 2.2 以降では，Device Administration API が用意されており，パスワードポリシの強化，強制や端末の遠隔ロックやデータ消去，内部メモリの暗号化などのセキュリティ機能が提供されている [8]．iOS や Windows Mobile でも同様の機能が提供されており [9], [10]，スマートデバイス利用時における各種リスクに対するセキュリティ対策を実現する基本的な機能が OS において提供されている．

これらの機能を利用し，各セキュリティベンダや通信キャリアは MDM（Mobile Device Management）と呼ばれるソリューションを，主に業務利用向けに提供している．MDM では，上述の OS が提供するセキュリティ機能を用いた制御アプリケーションを利用者のスマートデバイスにインストールする．そして，管理者端末からの制御命令や制御設定ファイルを制御アプリケーションが受信し，それに従った機能制御を実行する．これにより，たとえば，盗難された利用者のスマートデバイスを管理者端末から遠隔ロックすることで，その機能を実質的に無効化することができる．したがって，スマートデバイスを業務利用する場合，そのセキュリティを確保するための簡単な手段の 1 つとして，MDM 用の制御アプリケーションをスマートデバイスの利用者に配布し，インストールする方法がある．

しかし，MDM を施したスマートデバイスでは企業の厳

[1] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories, NTT Corporation, Musashino, Tokyo 180–8585, Japan
[†1] 現在，日本電信電話株式会社技術企画部門
Presently with Technology Planning Department, NTT Corporation
[†2] 現在，エヌ・ティ・ティ レゾナント株式会社
Presently with NTT Resonant Inc.
[a)] ryota.sato@hco.ntt.co.jp

しいセキュリティポリシに従った制限がされるために，個人利用の観点から見た利便性が損なわれる場合も多い．結果として，利用者は利用用途や環境に応じて，たとえば，業務用と個人用のスマートデバイスなど，複数台を保持することとなる．そこで，仮想化技術の応用が考えられている．仮想化技術としては，これまでのノートパソコンの社外利用などに適用されてきたVDI（Virtual Desktop Infrastructure）を用いた方法がある．これは，企業内で利用するデスクトップパソコンなどを仮想化してサーバ上に集約する．そして，その仮想化されたパソコンの情報を，利用者が持つシンクライアント端末などへ画面転送する．この利用者端末としてスマートデバイスが利用されている [11]．このVDIを用いた方法により，利用者は1つの端末を保持するだけで，利用用途や環境に応じて機能が制限された複数の仮想化されたパソコン利用することができる．

一般的なVDIでは，Windowsなどのデスクトップ OSのパソコンを仮想化し，その情報を画面転送する．そのため，スマートデバイスに固有の各種アプリケーションやGPSや加速度センサなどの機能は利用できない．そこで，スマートデバイスのプラットフォームOSの仮想化を実現したVirtual Smartphoneが存在する [12]．これは，スマートデバイスの端末環境を仮想化してサーバ上に集約する．そして，その仮想端末から，利用者のスマートデバイスへ画面転送する．利用者のスマートデバイス上の各種デバイスから得られる位置情報や加速度情報などはサーバ上の仮想端末へ送信されるため，スマートデバイスの利用状況を反映した処理が実行可能である．

一方で，サーバ上の仮想端末による演算処理結果を転送する方法ではなく，利用者のスマートデバイスOSを仮想化する技術も存在する [13]．仮想化プラットフォーム上に複数のOSを導入することで，たとえば，業務用と個人用の仮想端末を1台のスマートデバイス上で切り替えて操作することができる．

続いて本稿において利用するIDベース暗号に関連する研究について述べる．IDベース暗号はIDを暗号化の鍵とすることができる公開鍵暗号の一種であり，基本方式 [7] をはじめ各種応用方式 [14] が研究されている．また，電子署名を用いた認証を1つのアプリケーションと想定し，IDベース暗号を電子署名へと応用したIDベース署名が存在する [15], [16], [17], [18], [19]．IDベース署名の典型例では，IDに対応する署名鍵の所有者である署名者が，あるデータに対して，署名鍵で署名し，検証者に提示する．署名検証者は署名者ごとの署名検証鍵を取得する必要はなく，該当するIDを用いて署名を検証することができる．

このようなIDベース署名をネットワークカメラにおける安全なプロファイル設定方式へと応用した研究が存在する [20]．ここでは，複数のネットワークカメラの各種プロファイルをプロファイル管理サーバから安全に設定を行う方式において，各ネットワークカメラへ公開鍵証明書を配布する従来のPKIに基づいた方式ではなく，IDベース署名を利用した方式を提案することによって，証明書の取扱いにかかる利便性の向上やコストの削減が可能になるとしている．

また，ネットワークサービスにおいてユーザが多くのID/PWを管理する必要がある問題に着目し，ユーザの匿名性を確保しながらID/PWを不要とする認証方式においてIDベース署名を応用した研究が存在する [21]．ここでは，ユーザによるWeb閲覧やメールの送受信などネットワークサービス上での行動に対し，その行動が発生するたびにデジタル署名による「ネットワーク行動証明書」を発行する．そして，それら複数の証明書を必要に応じた組合せで第三者へ提示し，検証することで必要最小限のユーザの本人性を認証可能な方式が提案されている．この方式においては，ユーザがネットワークサービス上で行動するたびに証明書が発行されるため，従来のPKIに基づいた署名ではなく，IDベース署名を利用することでその管理や運用の実現性を高めている．

これら研究においては，IDベース暗号やその署名への応用であるIDベース署名を認可の枠組みとしてとらえてはいない．従来のPKIに基づく認証方式における運用の煩雑さや管理のコストを削減する1つの代替手段としてIDベース署名やIDベース暗号の利用手法が議論されている．

## 3. 要件整理と提案方式

1章で述べた機能制御機構の実現に向けて，本章では機能制御機構に求められる要件をスマートデバイスの持つ特徴などから改めて整理する．さらに，その実現方式について，機能の制御が機能を利用する際の認証や認可に相当することに着目し，認証と認可のフレームワークから方式における課題を整理する．そして，課題をIDベース暗号の応用により解決した新たな方式について述べる．

### 3.1 要件整理

1章で述べたように，本稿では，スマートデバイスが取り扱う文書や写真といったコンテンツに対する利用環境に応じた機密性の確保やこれらコンテンツを利用するアプリケーションの適切な利用に着目する．さらに，利用環境を構成する要素としては，位置や時間，気温など様々な要素が考えられるが，分かりやすさのために，本稿における利用環境としては位置を前提として議論を進める．

スマートデバイスの特徴を改めて考察すると，その可搬性の高さがあげられる．スマートデバイスが様々な環境で利用されることで，その通信ネットワークの状況も変化する．したがって，高速な通信環境が確保できない場合も考慮したセキュリティ対策が求められる．

さらに，1章で述べたとおり，スマートデバイスの特徴

として，その利用者のセキュリティ意識が多様であり，特にセキュリティ意識が低い利用者が多いことが指摘されている [5]．特に個人においては，スマートデバイスはいわゆるフィーチャーフォンと呼ばれる携帯電話の延長として取得し，利用される場合が多い．携帯電話においては，各携帯電話キャリアがその端末やアプリケーションの開発，ネットワークの選定などを一元的に管理していた背景から，セキュリティを意識する主体は携帯電話キャリアであり，利用者がセキュリティを意識する機会は比較的少なかった．そのため，携帯電話の延長としてスマートデバイスを利用する者はセキュリティを意識して主体的な対策をすることに慣れていない．このことから，利用者の判断や操作が可能な限り不要なセキュリティ対策が望ましい．

以上で述べたスマートデバイスにおける特徴などから，本稿においては，下記 3 点を機能制御機構に求められる主な要件とした．

- **要件 1**：動的に変化するスマートデバイスの利用環境に応じ，柔軟にその機能制御ができること．
- **要件 2**：高速な通信環境がなくてもスマートデバイスの機能制御ができること．
- **要件 3**：スマートデバイスの機能制御の内容と制御の実施権限は利用者以外が保有すること．

要件 1 に関しては，2 章で述べた仮想化技術を用い，機能が制御された仮想端末を複数用意することで，スマートデバイスが利用される環境に応じ，適切に機能が制御することができる．しかし，サーバを利用した仮想化技術は，サーバからの画面転送に基づく技術であり，高速な通信環境を必要とする．そのため，要件 2 を満たすことが難しい．また，利用者のスマートデバイス OS を仮想化する技術は，通信環境に依存せず要件 2 を満たすが，仮想化できる端末数にはまだ上限があり，また，その仮想化端末の切替えを利用者自身に委ねているため要件 3 を満たさない．

一方，2 章で述べた MDM の場合，管理者端末からの制御命令や制御設定ファイルの送信においては，画面転送と比較して高速な通信環境を必要としない（要件 2 を充足）．また，機能制御は管理者端末を操作する管理者により実行される（要件 3 を充足）．しかし，管理者の操作が必要な MDM は，スマートデバイスの初期設定時や紛失，盗難時における利用が想定されており，利用場所の移動などの頻繁に発生する利用環境の変化に応じた機能制御は想定されていない．したがって，要件 1 から要件 3 を同時に満たす方式を検討する必要がある．

### 3.2 提案方式の検討

要件を満たす方式を検討するうえでの基本的な方針は，スマートデバイスの機能を利用者以外（以降，端末管理者）が管理するために，スマートデバイスの利用環境を把握したうえで，それに応じた制御命令や制御設定ファイルを送信し，スマートデバイスがそれを理解し，実行することである．スマートデバイスの利用環境の把握は，スマートデバイス端末に関する環境という属性を把握することである．また，制御命令や制御設定ファイルの送付はスマートデバイスの機能に対する認可の付与に相当すると考えることができる．つまり，一般的な会員性の Web サービスなどと同様に，あるサービスや機能の要求は，認証と認可のフレームワークにより処理される．そのフレームワークの概念を**図 1** に示す．

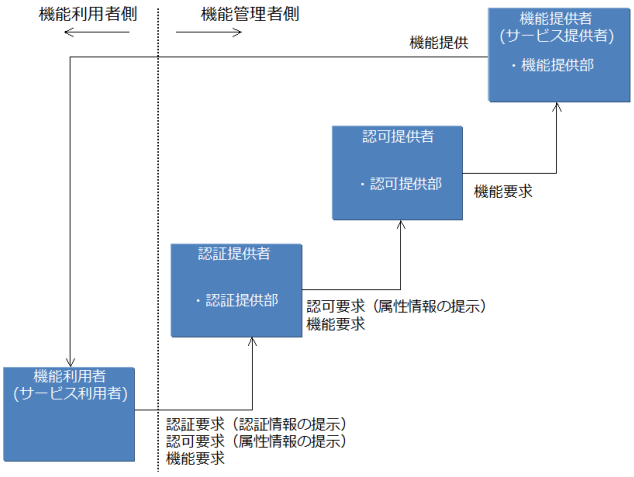


**図 1** 認証認可の概念図
**Fig. 1** Conceptual diagram of authentication and authorization.

機能利用者は，その機能の要求とともに認証と認可に必要となる認証情報と属性情報を提示する．認証提供者は，その認証情報を用いて認証を実施し，続く認可提供者は，その属性情報を用いて認可情報をサービス提供者へと渡す．この認可情報に基づき，たとえば，Web サービスの提供者はサービス利用者へ提供するサービスや機能を制御する．

図 1 に示した一般的な認証と認可のフレームワークを機能制御機構へと応用することを想定した場合，下記 3 点の課題が存在する．

1 点目は，属性の管理に関する課題である．図 1 において，認証提供者は機能利用者の属性値を管理している．具体的には，ある機能利用者の「役職」属性の値として「課長」，「性別」属性の値として「男性」などをあらかじめ登録し，管理する．したがって，属性値がスマートデバイスの「位置」など動的に変化するものである場合，そのつど認証提供者がその値を更新する作業する必要があるため，認証提供者に多くの負荷がかかる．

2 点目は，認証と認可の連携に関する課題である．前述のとおり，図 1 において，認証提供者は機能利用者の属性値を管理している．一方，認可提供者は属性に応じた認可情報を管理している．具体的には，スマートデバイスが「会社内」といった位置の属性値を持っていた場合，認証提供者からこの属性値を受け取った認可提供者は，この属

性値に対応した「社外秘コンテンツを閲覧可」などの制御命令を認可情報として取り出すことになる．つまり，認証提供者と認可提供者は属性に関して連携している必要がある．たとえば，会社や店舗，自宅，電車など多様な位置に応じた制御を想定した場合，各位置に応じた認可情報を管理する認可提供者は複数になると考えられ，認可提供者ごとに認証提供者と連携する必要がある．したがって，認証提供者は認可提供者が増えるたびに，その認可提供者に対応する属性との対応の管理する必要があり，機能制御機構のスケーラビリティの観点から課題がある．

3 点目は機密性の課題である．スマートデバイス上のコンテンツやアプリケーションのように機能提供部を機能利用者が持つ場合，認可提供者から渡される認可情報は機能管理者側から外部へと送信されることになる．送信の際に利用されるネットワークにも依存するが，インターネットなどの利用も想定した場合，認可情報の機密性を担保する必要がある．

### 3.3 提案方式

上述した 3 つの課題を解決した方式を実現するため，本稿では ID ベース暗号と呼ばれる公開鍵暗号系の暗号方式を導入する [7]．ID ベース暗号は下記 2 つの特徴を持つ．

1 つ目は，たとえば受信者の email アドレスや電話番号，社員番号などの既知の ID とあらかじめシステムで設定された公開パラメータだけを用いて受信者に向けた暗号文を作成できる点である．暗号文を取得した受信者は，暗号化に利用された ID を保持していることを鍵管理者へ示し，その復号のための秘密鍵を取得する．これにより，ID ベース暗号によって暗号化された暗号文は，その暗号化に用いた ID を持つものだけが復号できる [14]．

2 つ目は，秘密鍵の生成のタイミングに関する特徴である．RSA などに代表される一般的な公開鍵暗号では，公開鍵と秘密鍵の組は，暗号化を実施する前に生成する必要がある．一方で，ID ベース暗号では，公開鍵に相当する ID に対応する秘密鍵は，暗号化を実施した後，つまり復号を実施するタイミングで生成することができる [14]．

この ID ベース暗号を，上述した認証と認可の枠組みでとらえなおす．認可提供者に相当する端末管理者が機能利用者の属性値を ID と見なして，制御命令や制御設定ファイルをその ID で暗号化すると，その結果として生成された暗号文は，暗号化された認可情報である．そして，復号のための秘密鍵を認証提供者に相当する鍵管理者から取得することを認証の取得と考えることができる．この新たな方式について**図 2** に示す．

このとき，ID ベース暗号の 1 つ目の特徴から，暗号化に用いた属性値である ID を持つものだけが復号できるため，属性値と認可情報との対応管理は暗号化の条件として，暗号文に付与されている．つまり，前述した 1 点目の課題に

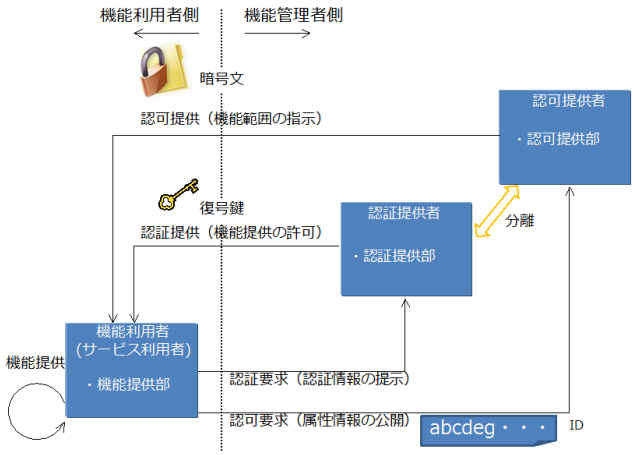


**図 2** 認証認可の枠組みから見た ID ベース暗号の概念図
**Fig. 2** Conceptual diagram of Identity-based encryption from the point of view of authentication and authorization.

関して本提案方式においては，認証提供者は認証のみを行えばよく，動的に変化する属性値を管理する必要はない．

また，ID ベース暗号の 2 つ目の特徴から，秘密鍵の生成と暗号化の実施のタイミングを独立にすることができる．秘密鍵の生成と取得を認証ととらえ，属性値である ID による制御指示が記載された情報の暗号化を認可と考えると，図 2 に示したような認証と認可を分離したフレームワークと考えることができる．つまり，前述した 2 点目の課題に関し本提案方式においては，認証提供者は認可提供者と連携する必要はない．

さらに，機能管理者側から外へ出る認可情報は暗号化により秘匿されており，3 点目の課題についても対応できる．

この ID ベース暗号を用いた提案方式においては，会社などのある環境でスマートデバイスを制御したい企業の端末管理者などが，その利用環境を表す ID を用いてデータを暗号化し，スマートデバイスへ任意のタイミングで配布する．このとき，上記暗号化対象のデータは，閲覧を制御したいコンテンツそのものやアプリケーションの起動可否を記した制御設定ファイルなどである．

端末管理者は，本機構に共通の公開パラメータのみを知っていれば，データの暗号化が可能となる．そのため，事前に公開鍵と秘密鍵のペアの生成と共有の作業が鍵管理者との間で必要となる一般的な公開鍵暗号を用いた仕組みと比較してシステムの運用性が向上する．さらに，新たな端末管理者のシステム参入コストが低下するため，システムのスケーラビリティが向上すると期待される．

スマートデバイスは，自動的に自らの利用環境を表す ID に対応した秘密鍵を鍵管理者から取得し，上記暗号文を復号することで端末管理者が利用環境ごとに指定した制御が実施される（要件 1，3 を充足）．復号のタイミングで必要な通信は復号鍵の配布のみであり，画面転送型の技術と比較して，高速な通信環境を必要としない（要件 2 を充足）．

## 4. 実装

前章で述べた ID ベース暗号を用いた提案方式は，端末管理者や鍵管理者におけるシステム運用性の向上などが期待され有用であると考えられるが，スマートデバイス上での ID ベース暗号の復号処理などが必要となる．ID ベース暗号を利用したシステムに関しては，米 Voltage Security 社が電子メールにおける暗号化ソリューションを提供しているが [22]，それ以外ではまだ研究段階での利用にとどまっている．特にスマートデバイス上での利用に関しては，米 Voltage Security 社の同ソリューションが存在するが，その詳細は不明である．また，基礎的な実装報告はされているものの [23], [24]，限られたリソース上における復号処理などの負荷によって，利用者や管理者の観点から見たシステムの実行性が低下するおそれがある．そこで，本章では提案方式を実装した機能制御機構について述べる．

実装したシステムの構成を**図 3** に示す．機能制御クライアントと機能制御サーバ，鍵管理サーバの 3 者構成からなり，スマートデバイスの利用環境に応じてアプリケーションの起動可否を制御する．また，コンテンツの閲覧制御を実行する場合は，機能制御サーバの代わりにコンテンツ管理サーバが用いられる．アプリケーション起動とコンテンツ閲覧の機能を同時に制御する場合は，機能制御サーバとコンテンツ管理サーバが同時に存在してもよい．さらに，機能制御クライアントは他のアプリケーションと連携することで，利用環境に応じた様々な制御を実現できる．本実装においては，スマートデバイスの利用環境として，その位置に着目し，位置を表す ID（以降，環境 ID）として，無線 LAN アクセスポイントの Service Set Identifier（以降，SSID）と MAC アドレスを採用する．

なお，以降は簡単のため SSID を例に述べるが，SSID は無線 LAN アクセスポイントの管理者であれば任意の値を設定可能であり，場所を表す ID としての信頼性が低いため注意が必要である．ただし，本提案方式は，ID ベース暗号の公開鍵となる ID として利用可能な ID を SSID に限定したものではなく，また，利用する ID の信頼性を保証するものではない．本提案方式においては，環境 ID として今回実装した無線 LAN アクセスポイントの SSID や MAC アドレスだけでなく，GPS も利用可能である．また，位置を表す ID 以外でも，加速度の値や NFC 経由で取得したチップ情報など，スマートデバイスで取得できる各種情報が利用可能であり，適用されるサービスの内容やサービスが求める ID の信頼性の度合いなどにより適切な ID が選択される必要がある．

本実装においては，無線 LAN アクセスポイントの SSID の値である「SSID1」が届く範囲内において起動を禁止，もしくは起動を許可するアプリケーションを記載した制御設定ファイル（以降，機能制御ファイル）を，「SSID1」と

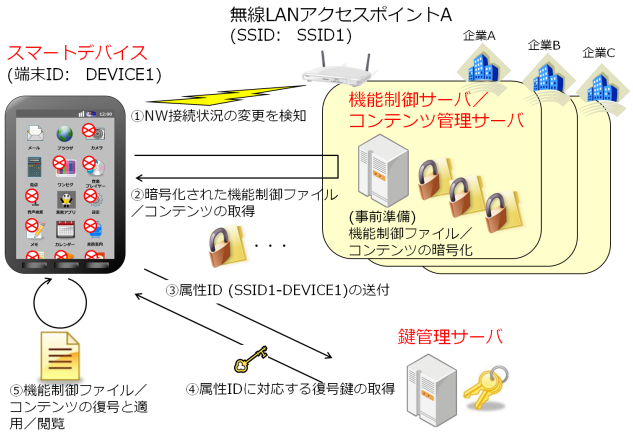


**図 3** システム構成図
**Fig. 3** System configuration diagram.

スマートデバイスの端末に固有の ID（以降，端末 ID）である「DEVICE1」を結合したものを ID に用いて ID ベース暗号化を行っている．「SSID1」の配下に入ったスマートデバイスは，この暗号化された機能制御ファイルを取得するとともに，自らの端末の ID と取得した SSID を結合し，それに対応した復号鍵を鍵管理サーバから取得する．この復号鍵を用いて，暗号化されていた機能制御ファイルを復号し，スマートデバイスに適用する．これにより，機能制御ファイルに記載されたアプリケーションの起動可否に応じた制御が実現される．

また，図 2 に記載した機能管理者や機能利用者と図 3 における各エンティティとの対応については，機能利用者がスマートデバイス端末，認可提供者が機能制御サーバもしくはコンテンツ管理サーバ，認証提供者が鍵管理サーバに相当する．機能利用者としてのスマートデバイス端末が，アプリケーションの利用やコンテンツの閲覧といった機能の利用を要求する．認可提供者としての機能制御サーバもしくはコンテンツ管理サーバは，機能制御ファイルもしくはコンテンツに対して ID ベース暗号による暗号化をし，特定の環境のみで復号可能という認可情報を暗号文に付与する．認証提供者としての鍵管理サーバは，暗号文に対する復号鍵について，その配布の可否を確認する．

### 4.1 機能制御サーバ

スマートデバイスの機能を制御する管理者が本サーバを利用する．機能制御サーバにおいては，OS として RedHat Enterprise Linux（RHEL）6.3 とその上に Apache 2.2 系，Tomcat 6 系，PostgreSQL 8 系などを利用した．

機能制御サーバを利用する管理者は，スマートデバイスが，ある場所で，どのような制御を実行するかを決定する．そのためのユーザ I/F として**図 4** に示す Web ブラウザから利用する管理画面を実装した．

この管理画面を利用し，管理者はスマートデバイス上の制御対象アプリケーションの名とそれらに対する起動可


図 4 機能制御サーバにおける管理画面
**Fig. 4** Image of interface for the system administrator.

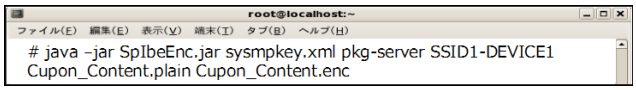


図 5 ID ベース暗号の暗号化実行コマンド
**Fig. 5** Command for encrypting files with Identity-based encryption.

否を，たとえば社内のアプリケーション利用ポリシなどに従って決定する．ここで指定されたアプリケーション名とそれらに対する起動可否の情報は，機能制御ファイルへと記載される．

続いて，「DEVICE1」などの端末 ID と「SSID1」などの環境 ID を選択したうえで，機能制御ファイルを指定すると，上記 2 つの ID の結合した ID を用いた ID ベース暗号化が機能制御ファイルに対して実行される．この暗号化された機能制御ファイルは，スマートデバイスが取得できるよう機能制御サーバ上で公開する．

### 4.2 コンテンツ管理サーバ

機能制御サーバにおいては，アプリケーションの起動可否を記載した機能制御ファイルを暗号化することによって，アプリケーションを制御した．一方，コンテンツ管理サーバにおいては，コンテンツの管理者が，閲覧制御をしたいコンテンツに対して直接に ID ベース暗号化を実施する．コンテンツ管理サーバは，OS として RHEL 6.3 とその上に Apache 2.2 系などを利用した．コンテンツ管理サーバを中心とした機能制御機構は，図 3 において，機能制御サーバをコンテンツ管理サーバに，機能制御ファイルをコンテンツに置き換えたものとなる．この場合，アプリケーションに対する制御とは異なり，コンテンツの暗号化された状態がそのままコンテンツの閲覧が制御された状態となる．

コンテンツ管理サーバにおいては，**図 5** に示す ID ベース暗号化を実行するためのコマンドのみを用意した．ここで，第 1 引数は ID ベース暗号に必要な公開パラメータ情報であり，第 2 引数は後述する鍵管理サーバのサーバ ID，第 3 引数は ID ベース暗号化に用いる ID，第 4 引数は入力となるコンテンツ（平文），第 5 引数は出力となる暗号化されたコンテンツである．なお，このコマンドは機能制御サーバにおいても用意されており，ID ベース暗号化の際，管理画面経由で実行されている．

### 4.3 鍵管理サーバ

スマートデバイスからの鍵生成の要求に対し，ID ベース暗号の復号鍵の生成を行う．鍵管理サーバにおいては，OS として RHEL 6.3 とその上に Apache 2.2 系，Tomcat 6 系，OpenSSL 1.0.0 系を利用し，ID ベース暗号の鍵生成モジュールを配置した．

前述のとおり，機能制御機構においては認可情報に相当する暗号化ファイルは事前にスマートデバイス側で取得されており，それを復号するための復号鍵を発行する際に認証を実施する．しかし，認証方式は，単純な ID/PW の認証や OpenID や SAML といった認証連携を考慮した認証など，サービスの提供形態により様々な形態が考えられる．したがって，本実装においては特定の認証方式を採用せず，認証機能を組み込みやすいモジュール構成のみを考慮した．

また，鍵管理サーバから発行される復号鍵は安全にスマートデバイスへ渡す必要がある．以前の我々の研究 [25] においては，スマートデバイスと鍵管理サーバ間における安全な鍵共有を実現するため，KEM（Key Encapsulation Mechanism）による復号鍵の保護策を実施した [26]．しかし，この保護策を実行する際にも ID ベース暗号を応用しており，復号の処理時間が増大していた．そこで，本実装においては，KEM に代わり SSL/TLS を用いた通信路暗号化を行うことによって，5.1 節に後述のとおり処理時間の削減と管理サーバからスマートデバイスへの安全な鍵共有を実現した．

### 4.4 機能制御クライアント

スマートデバイスに対する制御をするため，端末に機能制御クライアントをインストールする．本実装においては，Android OS 2.2 と 4.0 を対象に，サービスと呼ばれる画面を持たない常駐型アプリケーションとして実装した．機能制御クライアントが持つ機能は主に，環境 ID の取得，機能制御ファイルの取得，復号鍵の取得，ID ベース暗号の復号処理の 4 機能である．機能制御クライアントの機能構成を**図 6** に示す．

機能制御クライアントは常駐型のアプリケーションではあるが，定期的なスマートデバイスの位置の監視などはせず，下記 2 つの動作開始契機で動作させることで，電池の消費を抑えている．

1 つ目は，スマートデバイスの位置の変化に関する情報を OS が発信したタイミングである．具体的には，無線 LAN のアクセスポイントの発見や消失の情報を，OS から受け取る．これを契機にして，機能制御サーバから暗号化され

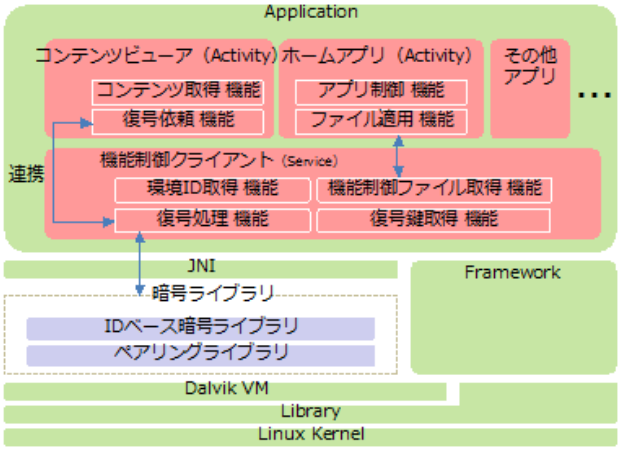


図 6 機能制御クライアントと連携アプリ

**Fig. 6** Relationship among client application, cooperative application and Android OS structure.


図 7 機能制御ホームアプリの表示例

**Fig. 7** An example of the image of home application for Situation-Sensitive function control system.

た機能制御ファイルを取得し，鍵管理サーバから復号鍵を得て，復号を実行する．

2 つ目は，後述する機能制御連携アプリケーション（以降，連携アプリ）からの復号処理の依頼を受けたタイミングである．機能制御クライアントは連携アプリから復号対象の暗号化ファイルと復号に必要な各種情報を受け取る I/F を有しており，その I/F 経由での復号依頼を受けて復号処理を実行する．

なお，ID ベース暗号の復号処理のため，機能制御クライアントのインストール時には，ID ベース暗号ライブラリとその演算過程で利用するペアリング演算 [23], [24], [27] のためのライブラリとを含む暗号ライブラリが同時にインストールされる．この暗号ライブラリは C 言語で記述されており，Java ベースの Android アプリケーションである機能制御クライアントからは JNI（Java Native Interface）を経由して実行される．

### 4.5 機能制御連携アプリケーション

前節でも述べた機能制御クライアントと連携した Android アプリケーションである．本実装においては，2 つの連携アプリを，画面を有するアクティビティと呼ばれるアプリケーションとして実装した．

1 つ目は，機能制御ホームアプリである．図 6 に記載のとおり，機能制御クライアントが復号した機能制御ファイル内の記載に応じ，起動が許可されないアプリケーションのアイコン付近にその旨を表す印をつけ，起動を制御する．その画面の表示例を**図 7** に示す．

この連携アプリは Android 上のホームアプリケーションとして実装されており，スマートデバイスが，ある無線 LAN アクセスポイントの配下へ移動すると，動的にホーム画面が変化し，その環境下で利用できるアプリケーションのみが起動可能となるよう動作する．

2 つ目は，4.2 節で述べたコンテンツ管理サーバと連携するコンテンツビューアアプリである．これは，図 6 に記載のとおり，コンテンツ管理サーバより暗号化されたコンテンツを取得し，機能制御クライアントにその復号を依頼する．これにより，その暗号化に用いられた ID を持つ端末だけがコンテンツを復号でき，閲覧可能となる．たとえば，割引クーポンをコンテンツとした場合，特定の端末や店舗においてのみ閲覧可能なコンテンツの配布が実現できる．

## 5. 評価

前章で述べた機能制御機構の処理性能を測定し，スマートデバイス利用者と各種サーバ運用者の観点からシステムの実行性について評価する．評価環境は，スマートデバイスとして Android OS 2.2 である GALAXY Tab SC-01C（CPU: Samsung S5PC110 1.0 GHz，Mem: 512 MB）と GALAXY S SC-02B（CPU: Samsung S5PC110 1.0 GHz，Mem: 512 MB）に加えて，Android OS 4.0 である GALAXY S III SC-06D（CPU: MSM8960 1.5 GHz (Dual Core)，Mem: 2.0 GB）を用意した．また，機能制御サーバおよび鍵管理サーバには CPU: Intel(R) Core(TM) i5-3470 CPU 3.20 GHz（4 CPUs），Mem: 4.0 GB のハードウェアスペックを持つサーバを用意し，それら機器が，無線 LAN アクセスポイントを介したローカルネットワークに接続された環境を用意した．

### 5.1 機能制御クライアントの処理性能

1,724 byte の機能制御ファイルを用意し，機能制御サーバ上で暗号化した．機能制御クライアントが無線 LAN アクセスポイントを検知してから，そのファイルを取得，復号し，そこに記載された制御内容を機能制御ホームアプリにおいて図 7 のように表示反映するまでの時間を，上述した 3 機種についてそれぞれ 3 回測定した．その結果を**表 1** に示す．

表 1 3 機種における処理の測定結果
**Table 1** Measurements of processing time on three devices.

| | GALAXY Tab SC-01C | GALAXY S SC-02B | GALAXY S III SC-06D | 3機種の平均値 |
|---|---|---|---|---|
| 1回目 | 2.61 (1.94) | 2.56 (1.94) | 3.29 (2.10) | 2.82 (1.99) |
| 2回目 | 3.31 (2.83) | 2.70 (1.98) | 3.59 (2.32) | 3.20 (2.38) |
| 3回目 | 2.41 (1.88) | 2.58 (1.89) | 3.24 (2.20) | 2.74 (1.99) |
| 3回の平均値 | 2.77 (2.22) | 2.61 (1.94) | 3.38 (2.21) | 2.92 (2.12) |

表 2 復号処理の計測結果と分析
**Table 2** Measurements of processing time of decrypting files with Identity-based encryption and its analysis.

| | 全体の処理時間（秒） | IDベース暗号の処理時間（秒） | 全体に対するIDベース暗号処理の割合（%） |
|---|---|---|---|
| 1回目 | 2.61 | 1.94 | 74.5 |
| 2回目 | 3.31 | 2.83 | 85.6 |
| 3回目 | 2.41 | 1.88 | 78.3 |
| 平均値 | 2.77 | 2.22 | 79.4 |
| (参考) | 10.44 | 10.01 | 95.9 |

表 1 の結果の単位は秒である．また，括弧内の値は全体の処理時間のうち，ID ベース暗号の処理にかかった時間を記載している．この ID ベース暗号の処理時間は，機能制御クライアントにおいて，ID ベース暗号の復号が始まってから終了するまでの時間であり，鍵管理サーバからの復号鍵取得にかかる時間を含んでいる．

表 1 の結果から，GALAXY Tab と GALAXY S ではほぼ同じ値となっており，GALAXY S III では他の 2 機種と比較して大きな値となった．ただし，ID ベース暗号の処理時間に着目すると，3 機種の平均値からの乖離は 3 機種ともに大きな違いはない．そのため，機能制御サーバや鍵管理サーバとの通信処理や図 7 のような画面の描画処理など ID ベース暗号の処理以外にかかる時間の違いによるものと考えられる．

続いて，GALAXY Tab の結果をもとに，全体の処理時間に対する ID ベース暗号の処理時間の割合と以前の我々の研究における処理時間 [25] との比較について**表 2** に示す．

表 2 の結果から，全体の処理時間としては平均 2.77 秒である．そのうち ID ベース暗号の処理時間は平均 2.22 秒であり，全体に対し，平均で 79.4%が復号処理に要している．また，表 2 において参考と記載された値が以前の我々の研究において実装した際の各処理時間の平均値である．測定環境が厳密には異なるため，単純な比較をすることはできないが，ID ベース暗号の処理時間は平均値で 1/4 以上短縮されていることが分かる．

この処理時間の短縮の要因としては 2 点考えられる．

1 点目は，4.3 節でも述べたとおり，以前の我々の研究において採用していた KEM を用いた復号鍵に対する保護策（以降，従来方式）をやめ，SSL/TLS を用いた通信路暗号化へ変更した点である．従来方式は，PSEC-KEM [28] と呼ばれる楕円曲線暗号に基づく方式を採用し，楕円曲線上のペアリングを用いた ID ベースの鍵共有方式 [7], [14] を利用した．一方で，SSL/TLS においては一般的に楕円曲線暗号ではなく RSA 暗号を利用して鍵の共有が行われる．したがって，従来方式と SSL/TLS の処理時間の比較においては，楕円曲線暗号のペアリング演算処理と RSA 暗号の演算処理の違いが重要となる．この違いについては，参考文献 [24] において，Android OS2.2 上での RSA 暗号の演算処理がペアリングの処理に比べて 22 倍以上高速となるという結果が示されている．また，その原因については，Android 上の BigInteger の利用においてネイティブ関数への呼び出しなどのオーバヘッド処理が発生し，その BigInteger メソッドを RSA 暗号よりもペアリング暗号の方が多く使用していることが述べられている．

SSL/TLS を用いた通信路暗号化においては，鍵管理サーバ側で SSL 証明書を準備する必要があるなど，サーバ側の構築・運用コストが増加するものの，上述した理由により全体の処理時間が短縮され，利用者側の利便性は向上する．

2 点目は，暗号ライブラリの変更である．以前の実装においては，Java 言語で書かれた暗号ライブラリを使用した．一方，本実装においては，4.4 節でも述べたとおり，C 言語で書かれた暗号ライブラリを JNI 経由で利用することで高速化を図っている．

なお，表 2 において ID ベース暗号の処理以外の時間に着目すると，今回の実装における平均値は 0.55 秒，従来方式の参考値は 0.43 秒であり，0.1 秒程度今回の実装の方が大きな値である．測定した全体の処理は 3 つに大別できる．

- **処理 1**：（無線 LAN アクセスポイントを検知後）端末が機能制御サーバから機能制御ファイルを取得
- **処理 2**：ID ベース暗号の処理（KEM もしくは SSL/TLS の処理含む）
- **処理 3**：復号された機能制御ファイルのパースとホーム画面の描画

このうち，ID ベース暗号の処理以外の処理は，処理 1 と 3 を合わせたものである．処理 1，3 においては，KEM もしくは SSL/TLS に関わる処理は含まれておらず，KEM を SSL/TLS に置き換えたことによる影響はない．

処理 1，3 における従来方式から今回の実装の変化としては，機能制御ファイルのフォーマットにおいて，制御指示などについての拡張性を考慮した形式に変更した点があげられる．それにともない，測定時に用いる機能制御ファイルのサイズが，従来方式の 558 byte から [25]，1,724 byte と大きくなっている．このことから，処理 1 における機能制御ファイルの取得に関する処理時間は，少なくとも今回の実装の方が大きくなると考えられる．また，処理 3 における機能制御ファイルのパース処理に関する処理時間についても，拡張性を考慮したフォーマットとしたことにより情報量は増えたため，少なくとも今回の実装の方が大きくなると考えられる．

さらに，表 1 に記載の評価から得られた 3 機種の平均 2.92 秒という処理速度について，一般的な Web サイトの

表示速度に対する米 Akamai 社が実施した調査結果を参考に評価する [29]．この調査はネットショップの利用者を対象としており，その結果から Web サイトの読み込み時間が 3 秒を超えると 40%以上の利用者は待つことができないことが示されている．つまり，3 秒以内での Web サイトの読み込みが，Web 利用者の観点からの 1 つの指標となっている．機能制御クライアントにおいてもこの指標を参考とすると，その処理速度はこの指標を満たしており，機能制御機構の利用者の観点からのシステム実行性はあるといえる．

### 5.2 機能制御サーバ，鍵管理サーバの処理性能

機能制御サーバと鍵管理サーバに対し，1 分間に 120 人分のスマートデバイスがアクセスする状況を想定した負荷をかけ，その処理性能を測定した．スマートデバイス側の機能制御クライアントとしてはエミュレータを用いて，上記アクセスを疑似的に再現した．このアクセスを 1 時間継続した際に，機能制御サーバと鍵管理サーバにおいて vmstat コマンドによる CPU の id 値（CPU のアイドル時間のパーセンテージ）を測定した結果を**図 8** に示す．

機能制御サーバ，鍵管理サーバともに値が 100%に近い値で推移しており，CPU の負荷は高くないことが分かる．機能制御サーバにおいては，このサーバ上に置かれた機能制御ファイルに対するアクセスが，機能制御クライアントからあるのみであり，高い負荷の処理が発生しない．

なお，本節では機能制御サーバの処理性能を計測したが，4.2 節でも述べたとおり，構成としては ID ベース暗号の暗号化対象が機能制御ファイルとコンテンツで異なるだけと考えられるコンテンツ管理サーバにおいても，ファイルサイズが同じであれば，機能制御サーバと同様の処理性能になると考えられる．

一方，鍵管理サーバにおいては，機能制御クライアントから要求された ID に対応する復号鍵を生成する処理が発生する．しかし，図 8 の結果から，1 分間に 120 人分の復号鍵の生成処理に対しても十分な性能が確保できることが分かる．なお，私物端末を企業の業務でも利用する BYOD において機能制御機構を適用したと想定すると，1 分間に 120 人という測定条件は，たとえば 8 時から 9 時までの出勤ピーク時間に合計 7,200 人の社員が出社した場合に相当する．経済産業省の統計によれば [30]，平成 24 年度の 1 企業あたり常時従業者数は最も多い業種でも 3,500 人程度であることから，大きな規模の企業への適用を想定した場合であっても，機能制御機構の管理者側の観点からのシステム実行性はあるといえる．

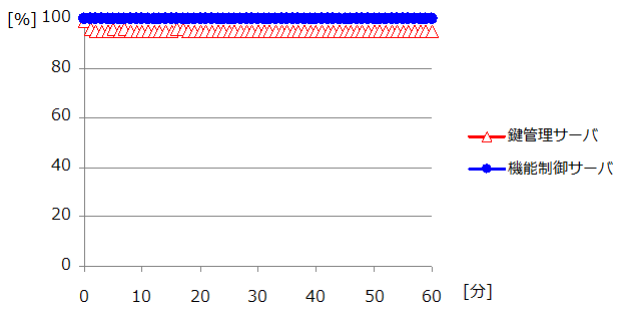


**図 8** CPU の id 値の推移
**Fig. 8** Measurements of 'id' value of the CPU.

## 6. 考察

5.1 節と 5.2 節においては，機能制御機構の端末やサーバにおける性能測定からシステムの実行性について評価した．本章においては，アプリケーションの利用やコンテンツの閲覧といった機能を制御する本機構のメリットやデメリットについて，システムにおける処理性能や実装・運用の容易性，スケーラビリティの観点から考察をする．なお，簡単のためコンテンツの閲覧制御の場合を想定して考察する．また，利用者に対するコンテンツの閲覧制御を行う方法としては，ID ベース暗号を利用した本提案方式と，単純に端末から送信される SSID の情報に基づき，コンテンツ管理サーバが暗号化されていないコンテンツを返送する方式（以降，平文コンテンツ方式）が考えられる．そこで，本章では本提案方式と平文コンテンツ方式を対比しながら考察を進める．

### 6.1 コンテンツ管理サーバにおける処理負荷

本提案方式と平文コンテンツ方式をコンテンツ管理サーバにおける処理負荷の観点から比較した結果を**表 3** に示す．なお，表 3 においては，認証がすべて成功した場合を想定している．

端末から送信される SSID に応じた平文のコンテンツを返送する処理と ID ベース暗号により暗号化されたコンテンツを返送する処理に関しては，コンテンツ管理サーバにおける処理の複雑さやその処理負荷について差分はない．しかし，平文コンテンツ方式の場合，端末はコンテンツの取得後すぐに閲覧が可能となるため，会員サービスにおける利用などを想定すると，「1．コンテンツを提供可能な端末であるか」や「2．その端末の属性（たとえば，有料会員であるか，無料会員であるか）に応じ，どのコンテンツを提供可能か」を事前に確認する必要がある．つまり，コンテンツを返送する前にコンテンツ管理サーバ側において「1．認証」，「2．認可」を実施する必要がある．そのため，

**表 3** コンテンツ管理サーバにおける処理負荷の比較
**Table 3** Processes on contents management server.

| | 本提案方式 | 平文コンテンツ方式 |
|---|---|---|
| 認証の処理負荷 | 端末からのコンテンツ要求の数に比例 | 端末からのコンテンツ要求の数に比例 |
| 認可の処理負荷 | 一定<br>(コンテンツ暗号化時に一度だけ) | 端末からのコンテンツ要求の数に比例 |
| コンテンツ返送の処理負荷 | 端末からのコンテンツ要求の数に比例 | 端末からのコンテンツ要求の数に比例 |

認証や認可の機能やそれに必要な端末の識別情報や属性情報，属性に対する認可情報などをコンテンツ管理サーバが保有する必要がある．さらに，端末からコンテンツ取得の要求があるたびに認証や認可の処理がコンテンツ管理サーバ上で実施される．

一方で，本提案方式の場合は，3.3 節で述べた ID ベース暗号の特徴を利用することにより「2．認可」を，復号の条件として暗号化コンテンツに付与できる．具体的には，ある SSID を ID ベース暗号の ID として用いることで，ある SSID が取得できる環境下にいるという属性を持つ端末のみが復号し，閲覧できるコンテンツとなる．したがって，本提案方式においては，認可のために，ID ベース暗号を用いた暗号化の機能やそれに必要な ID や公開パラメータなどの情報をコンテンツ管理サーバにおいて保有する必要がある．ただし，認可の処理はコンテンツを暗号化する際に 1 度だけすればよく，端末からコンテンツ取得の要求があるたびに処理を実施する必要はない．

つまり，認可の処理に着目すると，コンテンツ管理サーバを利用する端末数の増加や端末の移動などによる属性変化にともなうコンテンツ取得要求数の増加に対して，平文コンテンツ方式はコンテンツ管理サーバの処理負荷が増加するが，本提案方式は処理負荷が一定となる．このことは，3.1 節の要件 1 において記載したとおり，動的に変化するスマートデバイス端末の利用環境に応じた機能制御を目的とした場合においては大きなメリットとなる．なお，本提案方式における認証機能については，コンテンツ管理サーバにおいて保有する必要はない．本稿においては別途用意した鍵管理サーバが，端末からコンテンツ取得の要求に応じ，復号鍵の配布にする際に認証を実施することとなる．

本提案方式のデメリットは，コンテンツ管理サーバにおける認可の処理負荷が不変となる一方で，端末においてコンテンツ取得のたびに ID ベース暗号の復号処理が発生することである．4 章で述べたとおり，ID ベース暗号は実システムでの利用報告は少なく，特にスマートデバイスの限られたリソース上における復号処理の実行性が不明である点が課題であった．この点については，5.1 節においてその実行性を確認している．

### 6.2 システムの実装・運用の容易性とスケーラビリティ

3.3 節で述べたとおり，RSA などの一般的な公開鍵暗号とは異なり，ID ベース暗号においては公開鍵と秘密鍵のペアを事前に生成し，共有する必要がないという特徴を持つ．この特徴により，公開鍵となる SSID などの ID を利用して暗号化を実施するコンテンツ管理サーバと秘密鍵を提供する鍵管理サーバとの間においては，最初に 1 度公開パラメータなどの情報を共有するのみで，通常運用時はいっさいやりとりが発生しない．

そのため，ID ベース暗号を利用した本提案方式は，認可機能を持つコンテンツ管理サーバから認証機能を持つ鍵管理サーバを分離したシステムの実装と運用が可能となる．一方で，平文コンテンツ方式においても，認証と認可の機能を独立のサーバに実装可能と考えられるが，運用時には両サーバ間において認証結果や認可情報などのやりとりが発生する．

したがって，たとえば新規のコンテンツ管理サーバがシステムに参入する際は，本提案方式の場合，コンテンツ管理サーバにおいて認可機能だけを実装すればよく，また，運用時に鍵管理サーバとのやりとりが発生しないため，システムのスケーラビリティの点からもメリットがある．

なお，この場合のデメリットは，導入実績も多い一般的な認証や認可の機能を実装するのではなく，ID ベース暗号を用いた暗号化機能をコンテンツ管理サーバ上で実装し，鍵管理サーバを含め，ID ベース暗号を利用したシステムの運用設計をする必要がある点である．この点については，4 章において ID ベース暗号を用いたシステムの実装報告をし，システムが運用可能であることを確認している．

## 7. まとめ

本稿では，単一のスマートデバイス端末を複数環境で利用する際のセキュリティ確保について，スマートデバイスの可搬性や多機能性などの特徴に着目し，スマートデバイスが利用される環境に応じ，その様々な機能が，利用者の操作などが不要で，自律的かつ適切に制御される機能制御機構を提案した．

上記のスマートデバイスの特徴から，機能制御機構に求められる要件を整理したうえで，これら要件を満たす新たな方式を，認証と認可のフレームワークの観点から検討した．この検討で明らかとなった方式実現に向けた課題は，ID ベース暗号の特徴により解決されることを示し，ID ベース暗号を導入した新たな方式は，従来の公開鍵暗号を用いた場合と比較して，システムの運用性やスケーラビリティの向上が期待できることを述べた．

ただし，ID ベース暗号は実システムとしての利用報告が少なく，特にスマートデバイス上での利用に関しては基礎的な研究報告が主であるため，提案方式が有用であっても，その実行性は明らかではなかった．そこで，提案方式を Android 端末や各種サーバによってシステムとして実装した．具体的には，位置を表す ID を用いた ID ベース暗号により暗号化されたコンテンツやアプリケーションの起動制御ファイルを，スマートデバイス上で復号することで，コンテンツの閲覧やアプリケーションの起動を，スマートデバイスの位置に応じて制御するシステムを実装した．

さらに，その実装したシステムの処理性能について，利用者側と管理者側の双方観点から評価し，その実行性を検証した．利用者側の観点からは，ID ベース暗号の復号処理を含む画面の表示処理時間において，評価に用いた 3 機種

の平均が 2.92 秒であり，一般的な Web ページの表示処理に関する指標である 3 秒以内と比較して，その実行性が確認された．また，管理者側の観点からは，1 分間に 120 人分の復号鍵生成などを実行させた際のサーバの CPU 負荷が十分に低いことを示し，大きな規模の企業などの利用を想定した場合でも十分な実行性があることを明らかにした．

そして，ID ベース暗号を応用した本提案方式について，ID ベース暗号を利用しない方式との比較から，サーバの負荷が軽減され，システムにおける実装・運用の容易性とスケーラビリティが向上することを示し，管理者側の観点からも有用であることを確認した．

## 参考文献


[1] Gartner: Gartner Says Sales of Mobile Devices Grew 5.6 Percent in Third Quarter of 2011; Smartphone Sales Increased 42 Percent, Gartner (Online), available from ⟨http://www.gartner.com/it/page.jsp?id=1848514⟩ (accessed 2013-04-03).

[2] Sybase: Enterprise Mobility Guide 2011, Sybase (Online), available from ⟨http://www.sybase.com/mobilityguide⟩ (accessed 2013-04-03).

[3] 独立行政法人 情報処理推進機構：スマートフォンへの脅威と対策に関するレポート，IPA Technical Watch（オンライン），入手先 ⟨http://www.ipa.go.jp/about/technicalwatch/pdf/110622report.pdf⟩（参照 2013-04-03）．

[4] 独立行政法人 情報処理推進機構：スマートフォンのセキュリティ＜危険回避＞対策のしおり，IPA 対策のしおりシリーズ（オンライン），入手先 ⟨http://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf⟩（参照 2013-04-03）．

[5] スマートフォン・クラウドセキュリティ研究会：スマートフォンを安心して利用するために実施されるべき方策，総務省（オンライン），入手先 ⟨http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000020.html⟩（参照 2013-04-03）．

[6] JSSEC：スマートフォン&タブレットの業務利用に関するセキュリティガイドライン，JSSEC（オンライン），入手先 ⟨http://www.jssec.org/dl/guidelines2011_v1.1.pdf⟩（参照 2013-04-03）．

[7] Boneh, D. and Franklin, M.: Identity-based Encryption from the Weil Pairing, *CRYPTO 2001*, LNCS 2139, pp.213–229, Springer Verlag (2001).

[8] Google: Device Administration, Android developers (Online), available from ⟨http://developer.android.com/guide/topics/admin/device-admin.html⟩ (accessed 2013-04-03).

[9] Apple：iPhone と iPad の配備，Apple（オンライン），入手先 ⟨http://images.apple.com/jp/iphone/business/docs/iOS_MDM_JP.pdf⟩（参照 2013-04-03）．

[10] Microsoft: Security Policies in MDM, TechNet (Online), available from ⟨http://technet.microsoft.com/en-us/library/dd261828.aspx⟩ (accessed 2013-04-03).

[11] Citrix: XenDesktop, Citrix (Online), available from ⟨http://www.citrix.co.jp/products/xendesktop/overview.html⟩ (accessed 2013-04-03).

[12] Chen, E.Y. and Itoh, M.: Virtual Smartphone over IP, *Proc. IEEE Symposium on a World of Wireless, Mobile and Multimedia Networks* (*WoWMoM 2010*), IEEE Computer Society, pp.1–6 (2010).

[13] VMware: VMware Mobile Virtualization Platform, VMware (Online), available from ⟨http://www.vmware.com/jp/products/desktop_virtualization/mobile.html⟩ (accessed 2013-04-03).

[14] ID ベース暗号調査 WG：ID ベース暗号に関する調査報告書，CRYPTREC（オンライン），入手先 ⟨http://www.cryptrec.go.jp/report/c08_idb2008.pdf⟩（参照 2013-04-03）．

[15] Shamir, A.: Identity-based Cryptosystems and Signature Schemes, *CRYPTO 1984*, LNCS 196, pp.47–53, Springer Verlag (1984).

[16] Cui, Y., Fujisaki, E., Hanaoka, G., Imai, H. and Zhang, R.: Formal Security Treatments for IBE-to-signature Transformation: Relations among Security Notions, *IEICE Trans.*, Vol.92-A, No.1, pp.53–66 (2009).

[17] Boneh, D., Lynn, B. and Shacham, H.: Short Signatures from the Weil Pairing, *Journal of Cryptology*, Vol.17, No.4, pp.297–319 (2004).

[18] Boneh, D. and Boyen, X.: Short Signatures without Random Oracles, *EUROCRYPT 2004*, LNCS 3027, pp.41–55, Springer Verlag (2004).

[19] Waters, B.: Efficient Identity Based Encryption without Random Oracles, *EUROCRYPT 2005*, LNCS 3494, pp.114–127, Springer Verlag (2005).

[20] 阿倍博信，若土剛之，中島宏一，小林信博：ID ベース暗号を用いたネットワークカメラ向けセキュアプロファイル設定方式，マルチメディア通信と分散処理ワークショップ論文集，Vol.2009, No.9, pp.55–60（オンライン），入手先 ⟨https://ipsj.ixsq.nii.ac.jp/ej/⟩ (2009).

[21] 斉藤典明, 山崎哲朗, 知加良盛, 小林　透, 金井　敦：FACE 技術と認証サービスの提案, グループウェアとネットワークサービス，Vol.2007, No.56 (2007-GN–064), pp.43–48（オンライン），available from ⟨https://ipsj.ixsq.nii.ac.jp/ej/⟩ (2007).

[22] Voltage Security: Voltage SecureMail, Voltage Security (Online), available from ⟨http://www.voltage.com/products/securemail/⟩ (accessed 2013-04-03).

[23] 井山政志：携帯電話を利用したペアリング暗号の実装実験，Pairing-Forum（オンライン），入手先 ⟨http://www.pairing-forum.jp/index.php?plugin=attach&refer=%E7%AC%AC13%E5%9B%9E%E3%83%9F%E3%83%BC%E3%83%86%E3%82%A3%E3%83%B3%E3%82%B0&openfile=NTT_pairing_iyama.pdf⟩（参照 2013-04-03）．

[24] 井山政志，清本晋作，福島和英，田中俊昭，高木　剛：携帯電話におけるペアリング暗号の実装，電子情報通信学会論文誌，Vol.J95-A, No.7, pp.579–587（オンライン），入手先 ⟨http://search.ieice.org/⟩ (2012).

[25] 佐藤亮太，武藤健一郎，知加良盛，栢口　茂：スマートフォンにおける利用環境に応じた機能制御機構の提案，電子情報通信学会技術研究報告，Vol.111, No.470, pp.61–66（オンライン）(2012)，入手先 ⟨http://ci.nii.ac.jp/⟩.

[26] NTT：情報通信用語集 ハイブリッド暗号，NTT（オンライン），入手先 ⟨http://www.ntt-review.jp/yougo/word.php?word_id=4212⟩（参照 2013-04-03）．

[27] 川原祐人，吉田麗生，星野文学，小林鉄太郎：NEON を利用した Android 上でのペアリング暗号の高速実装，暗号と情報セキュリティシンポジウム 2013（SCIS2013），3E1-2 (2012).

[28] NTT：PSEC-KEM 紹介，NTT（オンライン），入手先 ⟨http://info.isl.ntt.co.jp/crypt/psec/intro.html⟩（参照 2013-07-13）．

[29] Akamai: Akamai Reveals 2 Seconds as the New Threshold of Acceptability for eCommerce Web Page Response Times, Akamai (Online), available from ⟨http://www.akamai.com/html/about/press/releases/2009/press_0914

09.html⟩ (accessed 2013-04-03).
[30] 経済産業省：平成 24 年企業活動基本調査速報—平成 23 年度実績—，経済産業省（オンライン），入手先 ⟨http://www.meti.go.jp/statistics/tyo/kikatu/result-2/h24sokuho.html⟩（参照 2013-04-03）．

**佐藤 亮太**

2002 年大阪大学工学部応用自然科学科卒業．2004 年同大学大学院応用物理学専攻修士課程修了．同年日本電信電話株式会社入社．以来，情報セキュリティ，暗号システムの研究開発に従事．現在，日本電信電話株式会社技術企画部門所属．2011 年 FIT 論文賞受賞．電子情報通信学会会員．

**知加良 盛**　（正会員）

1988 年東京工業大学工学部電気電子工学科卒業．1990 年同大学大学院総合理工学研究科修士課程修了．同年日本電信電話株式会社入社．以来，ネットワーク管理，情報セキュリティの研究開発に従事．現在，NTT セキュアプラットフォーム研究所所属．2011 年 FIT 論文賞受賞．

**奥田 哲矢**　（正会員）

2009 年東京大学工学部航空宇宙工学科卒業．2011 年同大学大学院航空宇宙工学専攻修士課程修了．同年日本電信電話株式会社入社．以来，情報セキュリティ，暗号システムの研究開発に従事．現在，エヌ・ティ・ティ レゾナント株式会社所属．

**栢口 茂**

日本電信電話株式会社およびグループ企業にて，情報システム関連企画，新規事業開発，インターネットメディアベンチャー経営，情報セキュリティ研究開発等に従事．現在，NTT セキュアプラットフォーム研究所所属．2011 年 FIT 論文賞受賞．