関数型暗号を適用したスマートデバイス機能制御システムにおける暗号化条件最適化の検討

青柳 真紀子† 知加良 盛† 伊坂 広明†

†NTT セキュアプラットフォーム研究所
180-8585 東京都武蔵野市緑町 3-9-11
{aoyagi.makiko, chikara.sakae, isaka.hiroaki}@lab.ntt.co.jp

あらまし スマートデバイス機能制御システムは，セキュリティポリシーに基づきアプリケーションやコンテンツの動作・アクセスを制御するシステムである．本システムは関数型暗号を応用し，端末が取得する環境情報およびその論理演算式を関数型暗号の暗号化・復号条件とすることで，端末の利用環境に応じた制御を実現している．一方で，関数型暗号の処理性能は条件として利用する論理演算式の記述内容に応じて変動することも観測されている．本システムにおいて，ユーザビリティへの影響が大きい復号時間について，暗号化ファイルの暗号化条件の属性種別・論理演算式依存性を評価する．

A Study on Optimization method of Encryption Conditions on Application/Content Management System with Functional Encryption Algorithm

Makiko Aoyagi† Sakae Chikara† Hiroaki Isaka†

†NTT Secure Platform Laboratories.
3-9-11, Midori-cho Musashino-shi, Tokyo 180-8585, JAPAN
{aoyagi.makiko, chikara.sakae, isaka.hiroaki}@lab.ntt.co.jp

Abstract The application/content management system for smart devices provides access control for application and content according to pre-defined security policies. The access control achieved by functional encryption algorithm., Application configuration files and contents, encrypted with parameters and their logical connections. are decrypted when the smart device gathers specified parameters such as SSID, , time, and date. Relationship with system performance and encryption conditions are evaluated.

1　はじめに

近年，スマートフォンやタブレットなどの普及により，スマートデバイスが様々な環境下で利用されるケースが増えている[1][2]．一方で，スマートデバイスを対象とした脅威の増加や盗難などのリスクやセキュリティ被害も多く指摘されており，セキュリティ対策の検討がすすめられている[3][4]．

我々はこれまで，スマートデバイスのセキュリティ対策機能としてアプリケーションの起動制御とデータの保護に着目し，スマートデバイスが利用される環境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してきた[5][6][7]．この方式では，許可された環境以外でアプリケーションの制御情報やコンテンツを保護するために暗号技術を用い，これまで ID ベース暗号[8][9]を応用したシステムを提案し，実装・評価を行った．しかしこの方式の場合，特定の属性情報を前提としたシステムに限定されるなど利便性・柔軟性に欠けるという課題があったことから，ID ベース暗号に代わり関数型暗号を応用した方式を提案した[7]．関数型暗号を適用することで，複数の属性情報を用いてそれらの組み合わせ条件を復号条件とすることが可能であり，様々な利用シーンに対応することができるため ID ベース暗号を利用した場合に比べてはるかに柔軟な制御が可能になることを示した．

関数型暗号は近年新しく開発された暗号技術であり，システムとしての運用実績が少ないことから，文献[7]では関数型暗号を応用した提案方式の実装と実現性の検証を中心に行った．本稿では，関数型暗号を適用したスマートデバイス機能制御システムにおいて関数型暗号の処理性能を評価する．特にユーザビリティへの影響が大きい復号処理に着目して処理時間の分析を行うとともに，システム全体としての運用性と安全性のバランスについて検討を行う．

2　システム概要

評価対象のシステム概要について述べる．

2.1　機能制御システム

スマートデバイス機能制御システムは，セキュリティポリシーに基づきアプリケーションやコンテンツの動作・アクセス制御を実現するシステムとして構築した．システムの概要を図 1 に示す．

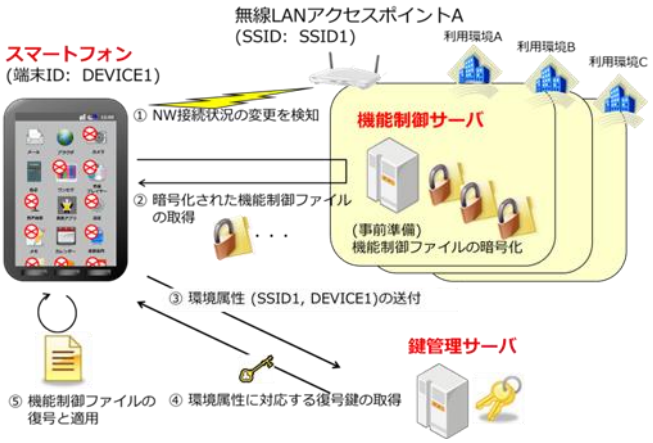


図 1 スマートデバイス機能制御システム概要

アプリケーション制御とコンテンツ制御を実現するために，サーバ側の機能として機能制御ファイル管理機能，コンテンツ管理機能，復号鍵生成機能，をそれぞれ機能制御サーバ，コンテンツ管理サーバ，鍵管理サーバ，として実装する．クライアントアプリとしては，上記 3 サーバと通信するアプリをそれぞれ機能制御アプリ，コンテンツビューワアプリ，復号制御アプリ，として実装した．サーバ/クライアントアプリの機能構成を図 2 に示す．暗号化ファイルは機能制御アプリやコンテンツビューワアプリに配信されるが，ファイルの復号は復号制御アプリが行う．本システムではスマートデバイスの利用環境に応じた制御を行うため，復号制御アプリには当該端末の環境属性情報を収集する環境情報エンジンを内包する．

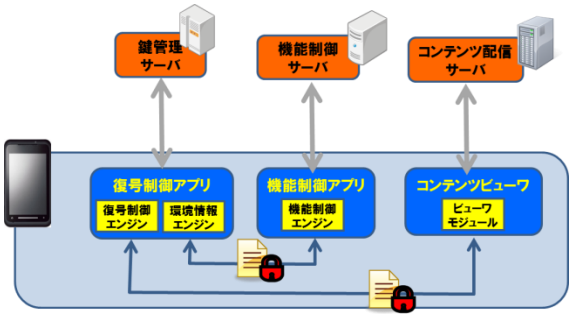


図 2　機能制御システムの機能構成

本システムにおいて環境属性として定義した属性一覧を表 1 に示す.

属性ID	属性パラメータ
osi_ssid	無線アクセスポイントのID. SSIDとしてOSから取得する文字列.
osi_bssidssid	無線アクセスポイントの個体識別子. OSから取得するBSSIDとSSIDを連結した文字列を条件とすることでSSIDのなりすまし対策としても有効.
osi_date	OSから取得する日付情報．YYYYMMDD形式
osi_time	OSから取得する時間情報．24時間表記の2桁文字。
usr_id	ユーザID．本システムでは機能制御アプリの設定情報としてに保管された情報を参照
usr_device	デバイスID。スマートデバイス機能制御エンジンv2では、機能制御アプリの設定ファイルに保管された情報を参照
opt_env	拡張用の属性IDとして定義．他のアプリからインテント形式で取得する情報などを想定.

表 1　環境属性一覧

端末の OS から取得できる環境属性として，無線アクセスポイントの SSID(osi_ssid)，そのアクセスポイントの個体番号を示す BSSID と SSID を連結させた情報(osi_bssidssid)，日時(osi_date)，時間(osi_time)，の 4 属性を定義した.

また，アプリケーション側に設定可能な情報としてユーザ ID，デバイス ID の 2 属性，さらに拡張可能な属性として外部属性を定義している. 本稿では，アプリケーションに依存しない情報として OS から取得可能な 4 属性を評価対象とする.

なお，本システムでは無線アクセスポイントの情報をその電波を受信可能な位置情報とみなして利用することとした. そのため，ある時点での環境情報として，日時(osi_date)，時間(osi_time)は一意に決まるが，SSID (osi_ssid)，BSSID(osi_bssidssid)は，検知している情報すべてを復号を実行する時点での環境情報として扱う.

2.2　関数型暗号の概要とその利用形態

ここで，関数型暗号の概要とその利用形態について簡単に触れる. 関数型暗号とは，公開鍵暗号をより高度にした暗号方式であり，暗号文と復号鍵に様々なパラメータ（属性情報と条件式）を導入することで「暗号—復号」のロジックを規定することができる. 具体的な利用形態として 2 通りあり，「復号鍵に属性情報，暗号文に条件式」あるいは「暗号文に属性情報，復号鍵に条件式」を組み込むことができる. 前者を Ciphertext Policy 方式，後者を Key Policy 方式という. 本システムでは Ciphertext Policy 方式を利用し，保護対象のファイルを環境情報と祖の組み合わせによる条件で暗号化しておき，ファイル利用時にスマートデバイスが取得する環境情報を復号鍵として利用する.

3　性能評価

3.1　評価対象

本システムの利用形態としては，保護対象とするファイルは予め想定する利用環境を条件として暗号化しておき，利用者による選択もしくは利用者のリアルタイムな環境変化に応じて，当該ファイルの復号を行う. つまり復号処理の性能が最もユーザビリティへの影響が大きいことから，暗号化ファイルの復号処理に着目して評価を行う. 復号処理における基本の流れを図 3 に示す.

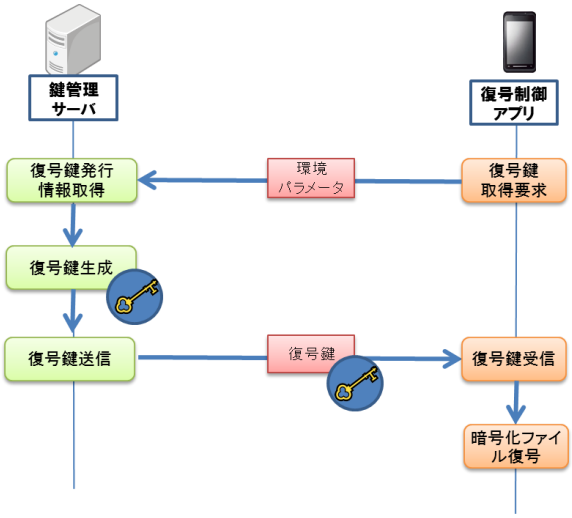


図 3 ファイル復号時の基本シークエンス

上記のとおり，復号鍵は鍵管理サーバで生成され端末に送信されるため，サーバ-クライアント間の通信路上で復号鍵の安全性を保護する必要がある．その方法には SSL で通信自体を暗号化するなどいくつかの方式があるが，本システムでは，生成した復号鍵を共通鍵で暗号化する方式とした．共通鍵方式を利用するためには，予めサーバ-クライアント間で鍵共有をしておく必要がある．その処理を加えた，本システムにおけるファイル復号の流れを図 4 に示す．端末側で共通鍵を生成，暗号化したうえで復号鍵の取得要求をする際に，復号鍵を生成するための環境パラメータとともにサーバに送信する．このとき共通鍵はセッション情報を用いて関数型暗号で暗号化したうえで送付する．リクエストを受けた鍵管理サーバは，取得した環境パラメータをもとに復号鍵を生成する．その一方で取得した暗号化共通鍵を復号しておき，当該共通鍵で生成した復号鍵を暗号化して端末に送信する．端末側では取得した暗号化復号鍵を共通鍵で復号して復号鍵を取得し，暗号化ファイルを復号する．

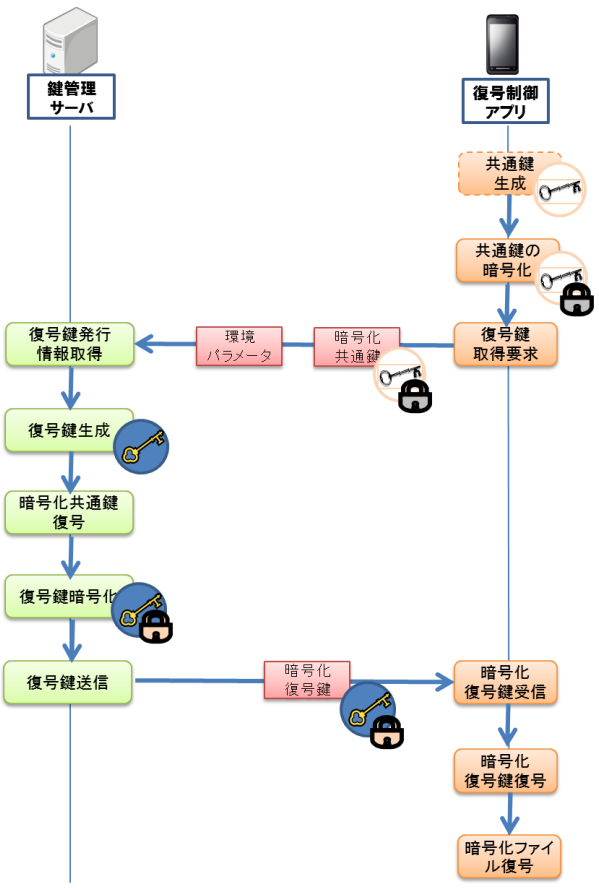


図 4
本システムにおけるファイル復号シークエンス

一つの暗号化ファイルを復号する場合，図 4 の通り端末側での共通鍵生成から暗号化ファイル復号までの工程を要する．ファイル復号時間の性能評価を行うにあたり，端末側で実行時間を測定すると，図 4 の「共通鍵の暗号化」から「暗号化ファイル復号」までを含む（「共通鍵生成」はアプリ起動時のみ実施するため各復号処理工程には含まない）．つまりファイル復号処理にかかる処理時間の内訳を分解すると，復号鍵要求処理とデータ復号処理に大別され，さらに復号鍵要求処理は復号鍵生成処理と復号鍵配送処理に分割できる．復号鍵配送処理は，復号鍵要求処理のうち復号鍵生成処理を除く，共通鍵送信に係る処理や復号鍵の暗号・復号処理，そしてサーバ-クライアント間の通信時間を含むものとする．図 5 に処理時間の内訳を示す．

暗号化ファイルを復号する際，その処理時間

が変動する要因としては，ファイルサイズや当該ファイルの暗号化条件，復号鍵生成のために与えられる環境パラメータ，などが考えられる．上記の各種要因を変更することで，復号鍵生成処理，データ復号処理は変動する可能性があるが，復号鍵配送処理に関してはシステム設計時点で決定される要件のためほぼ固定時間とみなしてよいと考える．

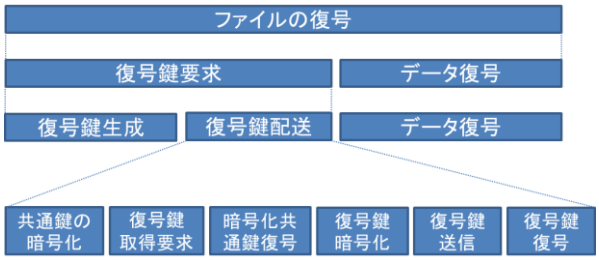


図 5 ファイル復号時間の内訳

3.2 評価環境

ここで，性能評価のために構築したシステムの環境について述べる．サーバ側の実装環境としては CPU：Intel(R) Core(TM) i7-3520MCPU 2.90GHz，Mem：8.0GB のハードウェアスペックを持つ PC 上に，OS として RedHat Enterprise Linux（RHEL）6.3 とその上に Apache2.2 系，Tomcat6 系，OpenSSL1.0.0 系などを利用して構築した．処理速度測定環境でもある端末は SONY Xperia Tablet Z(SGP312)，OS は Android4.1.2 を利用した．

復号対象のファイルは 1MB サイズの画像ファイルとし，予め暗号化して端末にダウンロードしておく．当該ファイルの復号はコンテンツビューワアプリを利用して暗号化ファイルを選択することにより開始し，そのファイルが復号，表示されるまでの処理時間を計測した．

3.3 環境情報種別による性能比較

2.1 節に示した環境属性情報のうち，アプリケーションに依存しない属性情報として OS から取得可能な 4 属性について復号処理性能を比較した．それぞれの環境属性で暗号化したファイルの復号に要した時間を図 6 に示す．下図はファイル復号のトータル時間を示したものであり，単位は(秒)である．測定はそれぞれ 5 回行い，その平均値を示している．

日時や時間を用いた場合に比べ，SSID や BSSID を鍵として用いた場合に処理時間が長くなる結果となった．これは，2.1 節で述べたとおり，本システムでは無線アクセスポイントの情報を，その電波を受信可能な位置情報とみなして利用するため，検知した情報すべてを環境パラメータとして復号鍵生成に利用していることが原因と考えられる．また，SSID（osi_ssid）より BSSID（osi_bssidssid）を用いた場合のほうが処理時間を要することから，環境パラメータの文字列の長さが処理の負荷に影響を及ぼすと考えられる．

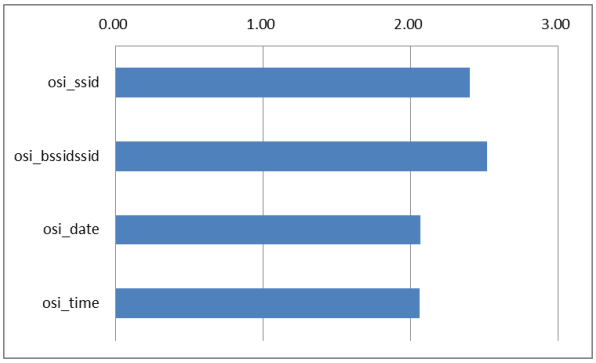


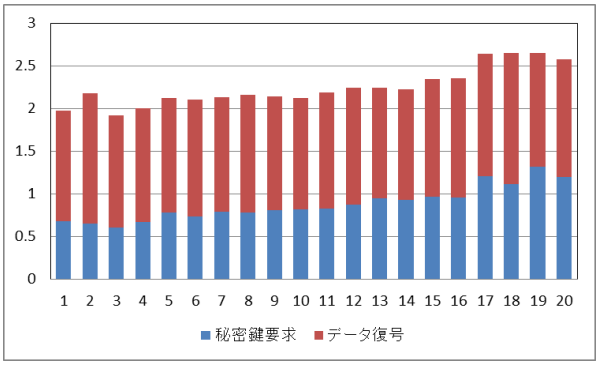
図 6 4 属性の測定結果

3.4 環境パラメータ数による性能比較

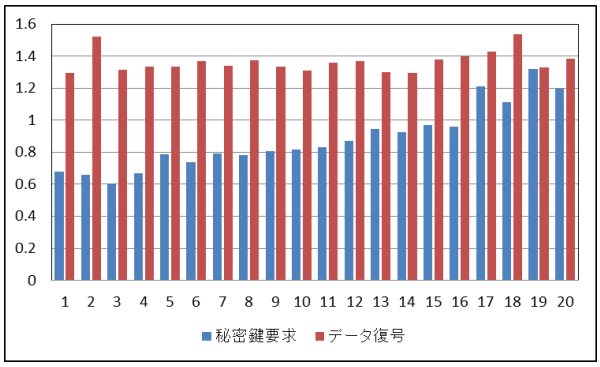
3.3 節の結果から，取得する環境情報の数に流動性のある環境属性の場合に性能劣化が生じる可能性があることから，特定の環境属性において与える環境パラメータの数を変えて性能特性を測定した．ここでは，SSID（osi_ssid）の 1 属性値を条件（例：osi_ssid=SSID001）として暗号化した暗号化ファイルに対して，復号鍵を生成するために与える環境パラメータの数

を変化させた場合に，暗号化ファイル復号処理時間に見られる特性を測定した．

測定結果を図 7 に示す．横軸は復号鍵要求時に鍵管理サーバに送信する環境パラメータの数，縦軸は処理時間(秒)を表したものである．また，処理時間は図 5 に示したようにファイル復号処理にかかる処理を復号鍵要求処理部分(青色)とデータ復号処理部分(赤色)に分けて計測し，図 7(a)はトータル処理時間を積み上げて比較したグラフ，図 7(b)はそれぞれの工程を分割して並べて比較したグラフである．図 7(a)から，鍵管理サーバに送るパラメータ数の増加に伴い，全体の処理時間が増加していることがわかるが，図 7(b)に示すように復号鍵要求とデータ復号のそれぞれの処理にかかる時間を分割して比較すると，復号鍵要求にかかる処理時間がパラメータ数に比例して増加している一方で，データ復号にかかる時間はパラメータ数にかかわらずほぼ一定の時間(約 1.3 秒)であることがわかる．ただし，3.1 節にて述べたとおり，本システムでは復号鍵配送時の安全性を確保するために復号鍵を暗号化する共通鍵を用いており，この処理を省くかもしくは SSL 通信などのほかの手段に置き換えることで復号鍵要求時間に含まれる復号鍵配送時間を短縮することが可能である．



(a)



(b)

図 7 パラメータ数の変化に対する
ファイル復号処理速度の変化

パラメータ数をより広範囲に広げた場合の処理性能の変化を図 8 に示す．データ復号にかかる時間はパラメータ数に依存せず一定のため，復号鍵要求時間にのみ着目した．パラメータ数の増加に比例して，復号鍵要求にかかる処理時間が線形に増加することがわかる．このことから，無線アクセスポイントの基地局が多数存在するような場所では処理性能の劣化が起きやすいといえる．

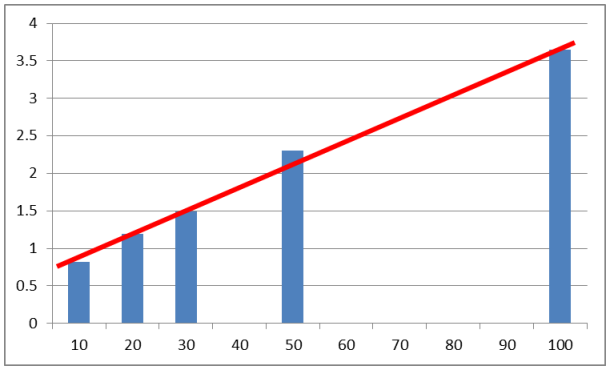


図 8 復号鍵要求時間の変化

3.5 暗号化条件による性能比較

次に，暗号化条件を複数情報の組み合わせに拡張した場合の処理性能について述べる．暗号化条件に用いる環境属性種別はSSID(osi_ssid)とし，属性数を1～5まで変化させた．さらに複数属性の場合にはそれらのOR条件とAND条件の

組み合わせを用いた．例として，属性数3の場合のAND条件では，(osi_ssid=SSID001)and(osi_ssid=SSID002)and(osi_ssid=SSID003)という条件式で暗号化しておき，SSID001, SSID002, SSID003という3つの環境パラメータを与えた場合にファイル復号にかかる処理時間を測定した．測定結果を図9に示す．

OR条件に比べるとAND条件で暗号化したファイルの復号処理により時間を要することがわかる．また，OR条件で条件式を追加しても復号処理の時間はほとんど変化がないが，AND条件で条件式を追加した場合には，条件式の数に比例して処理時間が長くなる結果となった．つまり，暗号条件に組み込むAND条件の数が暗号化ファイルの復号処理に負荷を与えると言える．

ただし，これは属性種別を1種類に限定した場合の測定結果であり，属性種別のバリエーションを増やした場合や，AND条件，OR条件が複雑に混在する場合などの性能評価は今後の課題である．

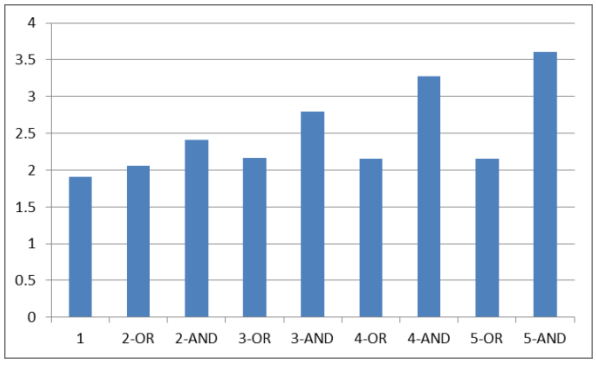


図9 暗号化条件による処理性能の変化

4 まとめ

我々はスマートデバイス機能制御機構を提案し，関数型暗号を適用したシステムを実装してきた．本稿では，当該システムにおける関数型暗号の復号処理性能に関する評価を行った．

我々が開発したシステムではスマートデバイスの OS から取得する環境情報として，4 つの環境属性を定義しているが，それら 4 つの属性種別を暗号条件に用いた場合の復号処理性能を評価した結果，SSID と BSSID を条件とした場合に性能劣化が生じることを確認した．これは，我々のシステムでは無線アクセスポイントの情報を，その電波を受信可能な位置情報とみなしていることにより，検知した情報すべてを復号鍵の生成に利用していることが原因であることが分かった．

次に，復号鍵生成のために与える環境パラメータの数を変化させた場合にファイルの復号にかかる処理性能を測定した．暗号化ファイルを復号する際の処理工程を復号鍵の生成時間とファイル復号処理時間に分割して計測結果を分析した結果，データ復号処理時間は環境パラメータの数に依存せず一定時間を計測したが，鍵生成に要する時間は与える環境パラメータの数に比例して線形に増加することが分かった．本システムの実装のように環境情報として取得する情報が一意にならず，情報数が流動的になる環境属性の場合には復号処理の性能劣化が生じることに注意する必要がある．処理性能の劣化を防ぐには，位置情報として一意に決定できる環境属性を利用するなどの方法や，取得する情報をフィルタリングする対策，復号鍵取得依頼の時点で送信する環境パラメータを精査する対策などが効果的である．また，システム全体の効率運用という観点では，復号鍵配送時の安全性とのトレードオフにはなるが，復号鍵の暗号化処理を省く，もしくは SSL 通信などの手段とすることで復号鍵配送にかかる時間を短縮することが可能である．

最後に，暗号化条件による性能比較を行った結果，OR 条件に比べ AND 条件で暗号化した場合に復号処理に時間を要することが分かった．本稿では，1 種類の属性種別で条件式を組み立て，AND 条件の場合と OR 条件の場合で処理性能を比較した結果，OR 条件を追加しても処理性能にさほど変化はないものの，AND 条件を追加すると AND 条件の数に比例して処理時間が長くなることが分かった．この特性に

ついては本質的な改善策を示すことが難しいが，暗号処理に係るロジックの外部で工夫することにより暗号化の条件式をシンプルにするなどで改善の余地はあると考える．

複数の属性種別を含む場合や，OR 条件と AND 条件の復号的な組み合わせなど複雑な条件式とすることで処理性能にどのような影響が生じるかは今後の検討課題である．

参考文献

[1] 総務省，平成 25 年版情報通信白書，http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h25/index.html 第 2 部 第 3 節 1-（1） 主な情報通信機器の普及状況（参照 2014-08-22）

[2] ARUBA networks, “BYOD in Europe, Middle East and Africa: An overview of adoption, challenges and trends”, http://www.arubanetworks.com/wp-content/uploads/Aruba-Networks-Infographic-v6.jpg, (accessed 2014-08-22)

[3] 独立行政法人情報処理推進機構セキュリティセンター，“IPA Technical Watch スマートフォンへの脅威と対策に関するレポート”，https://www.ipa.go.jp/files/000024773.pdf，（参照 2014-08-22）

[4] 独立行政法人情報処理推進機構セキュリティセンター，“スマートフォンのセキュリティ<危機回避>対策のしおり”2012 年 6 月 8 日 第 2 版，https://www.ipa.go.jp/files/000011456.pdf，（参照 2014-08-22）

[5] 佐藤亮太，知加良盛，奥田哲矢，栢口茂，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，情報処理学会論文誌 第 55 巻 第 1 号，2014 年 1 月発行

[6] 佐藤亮太，知加良盛，奥田哲矢，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実装と評価，電子情報通信学会技術研究報告，Vol.112, No.466, pp.203-208, Mar. 2013.

[7] 青柳真紀子，知加良盛，伊坂広明，栢口茂：関数型暗号を適用したスマートデバイス機能制御機構の実装，情報処理学会シンポジウムシリーズ Vol.2014, No.1, pp.758-764.

[8] D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing, ” CRYPTO 2001, LNCS 2139, Springer Verlag, pp. 213-229, 2001.

[9] 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, http://www.cryptrec.go.jp/report/c08_idb2008.pdf,（参照 2014-04-30）

[10] T. Okamoto, K. Takashima, “Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption”, CRYPTO 2010, LNCS6223, pp.191-208, 2010.