Vol.2013-DPS-154 No.1
Vol.2013-CSEC-60 No.1
2013/3/14

個人用セキュリティアプライアンスの提案

野田敏達[†1]　海野雪絵[†1]　大久保隆夫[†1]　金谷延幸[†1]

従来、端末のセキュリティは、セキュリティソフトをインストールし、セキュリティ機能を適切に管理することで対策していた。しかし、Android タブレットや iPad、Windows Phone といった多種・多様な端末が使われるようになると、端末毎にセキュリティ機能を管理し、維持することは、困難になってくる。そこで、端末からセキュリティ機能を分離し集約した、個人用のセキュリティアプライアンス、PSER の提案を行う。 PSER は、端末で使用するパスワードや暗号鍵、暗号機能などを安全に管理し、これらの機能の端末への提供や、機能の実行を行う。PSER の管理さえ適切に行っておけば、PSER を利用することで、どんな OS のどんな端末からでも、適切なセキュリティ機能を安全に利用することが可能となる。

1. はじめに

現在のセキュリティの状況として、スマート端末上でのマルウェアの増加、個人端末の乗っ取り、遠隔操作による踏み台攻撃といった、利用者とその端末を狙ったセキュリティ事件やサイバー攻撃による個人情報漏洩が深刻化している。このような脅威に対し、従来は使用する Windows PC にセキュリティソフトをインストールし、セキュリティ機能を正しく使いこなすことで対策をしていた。しかし、Andriod タブレット、iPad、Windows Phone といった多種・多様な端末が使われるようになると、「端末毎にセキュリティ機能・ソフトを用意し、管理し、維持する」ことはますます困難になるため、その対策が求められている。

本稿では、各端末で管理しているセキュリティ機能を利用するかわりに、セキュリティ機能を集約、提供する個人用セキュリティアプライアンス、PSER (Pocketable Security Enforcement Router) を利用する手法を提案する。さらに提案手法により、セキュリティ機能管理、維持のコストが軽減され、また利便性も向上することを確認した。

以下、第 2 章で背景と課題を述べた後、第 3 章で提案する PSER の特徴、技術について述べる。第 4 章で PSER の実装手法と評価結果を述べ、第 5 章で PSER の応用利用について考察する。最後に、第 6 章でまとめと今後の課題を述べる。

2. 背景と課題

スマートフォンやタブレットの急速な普及により、情報システムの使われ方の多様化が進んでいる。それに従い、セキュリティ対策も煩雑化し、安全性の維持が困難となってきており、その対策が求められている。

例えば、サーバにアクセスするためのパスワードに対し、多くの情報セキュリティガイドライン[1][2]は以下のように求めている。

- サーバごとに異なるものにする
- 複雑で推測できない文字列とする
- 紙等に記録しない
- 定期的な変更を行う

ガイドラインに従い、ユーザがそれらのパスワードを記憶し、安全に管理することは困難であるため、パスワードマネージャを利用するのが一般的であった。しかしながら、様々な端末からサーバにアクセスする場合、各端末のパスワードマネージャの管理、維持が困難であった。

また、クラウドサービスの普及に伴い、ファイルをクラウド上で管理することが増えてきている。このとき、情報漏洩の防止のため、暗号化してサーバにアップロードすることが求められている。特に複数の端末からこのファイルにアクセスする場合、暗号化に使用した暗号鍵やパスフレーズを各端末で安全に管理、維持するのは困難であった。

また、Facebook や Twitter、カレンダーサービス等を用い、ユーザ間で情報共有をしたい場合があるが、その中には特定ユーザ以外には秘匿したい情報もある。この対策として、アップロードデータを監視し、データが条件に合致した場合は、暗号化等の処理を行った上でアップロードを行う技術がある。また、自分がそのデータを閲覧する権限がある場合は、ダウンロード後、復号した上で表示する技術がある。しかしながら様々な端末からサーバにアクセスする場合、これらの条件定義や暗号鍵を各端末で安全に管理、維持するのは困難であった。

さらに、メールからの情報漏洩対策[3]や、標的型メール攻撃対策[4]では個人の利用履歴を元に対策を行う。しかしながら様々な端末から利用する場合、各端末で収集された利用履歴の統合や管理は困難であった。

このように、従来は各端末にセキュリティソフトをインストールし、セキュリティ機能を正しく使いこなすことで対策をしていたが、多くの端末が利用されるようになると、従来の方法ではセキュリティ機能の安全な管理、維持が困難となるため、その対策が求められている。

3. PSER の提案

本章では、課題を解決するための提案システムである

†1 (株)富士通研究所
Fujitsu Laboratories limited, 4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki 211-8588, Japan

PSER について述べる.

3.1 コンセプト

セキュリティ機能を 1 つのデバイスに集約し、デバイスによって提供されるセキュリティ機能を各端末から利用することにより、セキュリティ機能の管理、維持が 1 つのデバイスのみですむため、従来の端末毎にセキュリティ機能を用意し、個別に管理する方式よりも、はるかに管理、維持が容易になると考える。そこで、所有者専用のセキュリティアプライアンス、PSER を提案する。PSER はさらに以下の特徴をもつ。

- 所有者向けに特化したセキュリティ機能を端末に提供
- セキュリティ機能の追加、更新、削除が可能
- 端末から独立した耐タンパーデバイス
- 通信機能によるセキュリティ機能の提供
- 携帯可能デバイス

各特徴の詳細について述べる。

3.1.1 セキュリティ機能を端末に提供

PSER 内に所有者のパスワードの管理機能や暗号鍵管理を含めた暗号化、復号機能、秘匿機能等のセキュリティ機能を用意し、各端末に提供する。各端末は PSER が提供するセキュリティ機能を利用することで、各端末におけるセキュリティ機能の用意、管理、維持が不要となる。

3.1.2 セキュリティ機能の追加、更新、削除

PSER 内に必要なセキュリティ機能を追加可能とする。また､不要なセキュリティ機能は削除可能とする｡さらに、セキュリティ機能の更新も可能とする。これにより、常に必要となる最新のセキュリティ技術、機能を各端末で利用することが可能となる。

3.1.3 端末から独立した耐タンパーデバイス

PSER を耐タンパーデバイスとし、端末と PSER の間の情報の入出力を監視、制御する。また､PSER 利用時には、生体認証を行う。それにより、端末内のセキュリティ機能や、パスワード、暗号鍵などの秘密情報を守り、所有者のみが使用できることを保証する。

3.1.4 通信機能によるセキュリティ機能の提供

PSER に通信機能をもたせることで、通信機能搭載の任意の端末から利用可能となる。また、通信の監視を行うことで、セキュリティ機能のシームレスな適用や、ウイルスチェックなどが可能となる。

3.1.5 携帯可能デバイス

PSER を携帯可能な小型デバイスにすることで、いつでもどこでもどんな OS のどんな端末からでもセキュリティ機能の利用が可能となる。

3.2 セキュリティ機能の提供方法

端末にセキュリティ機能を提供するには以下の 2 つの方式が考えられる。

- プロキシによる提供
- Web API による提供

これらの方式は、セキュリティ機能に応じて向き、不向きがあると考えられるため、セキュリティ機能ごとに提供方式を検討する必要がある。

3.2.1 プロキシによる提供

プロキシで通信を監視し、必要時に通信データを加工することでセキュリティ機能を提供する。本方式のメリットは端末や既存アプリケーションに手を加えなくても、端末のブラウザのプロキシの設定を行うだけで、利用することが可能になる点である。サーバへの自動ログインや、ファイルをサーバにアップロードするときの暗号化、ダウンロードするときの復号等に向いていると考えられる。逆にプロトコルや通信のデータフォーマットが分からないような場合には利用できないほか、SSL 通信の場合にも、そのままでは利用できない、という欠点がある。

3.2.2 WebAPI による提供

PSER で Web サービス (WebAPI) を提供する。本方式のメリットは、既存のプロトコルやデータフォーマットに依存せず、多くのセキュリティ機能を柔軟に提供できる点である。しかしながら、端末から PSER が提供する WebAPI を呼び出す必要があるため、利用するアプリケーションの PSER 対応が必要となる。

3.3 PSER の安全な利用の実現

PSER 内にはスワード、暗号鍵などの秘密情報が管理されているため、外部から簡単に攻撃できてはならない。特に PSER は端末とは別デバイスとなっているため、ユーザが意図した端末から意図したセキュリティ機能を利用でき、それ以外の場合は利用できないようにすることが必要となる。つまり、ユーザと PSER、ユーザと端末、端末と PSER が正しく認証できることが必要となる。この実現のための「ペアリング」について、3.3.1 で述べる。

また、PSER の紛失、盗難は大きな脅威であるが、PSER を利用するにはユーザの生体認証が必要であり、さらにリモートワイプ機能を導入し、緊急時にはセキュリティ機能や秘密情報を削除することで、対策可能だと考える。

3.3.1 ペアリング

ユーザと PSER、ユーザと端末、端末と PSER が正しく認証するために、以下の手順でペアリングを行う。

1. ユーザが端末から PSER にアクセスする。PSER はユーザに、端末への PIN 入力を要求する。
2. PSER はユーザの生体認証を行った上で､前項で入力するべき PIN を PSER の画面に表示する。
3. ユーザは表示された PIN を端末に入力し、端末は PSER に PIN を送信し、セッションを確立する。

このとき、PIN は毎回異なる値が生成されるため、過去の PIN は利用できない。これにより、ユーザが PSER 上に表示される PIN を見ることが必要となるため、ユーザが PSER のそばにいることを保証できる。このペアリングを

実施することで、ユーザが意図した端末から意図したセキュリティ機能を利用でき、それ以外の場合は利用できないようにすることを実現できる。

3.4 提供セキュリティ機能

PSER に組み込み可能なセキュリティ機能には以下が考えられる。PSER は個人用である特性をいかした所有者に特化したセキュリティ機能や、通信監視をしている特性をいかしたセキュリティ機能が有用であると考えられる。

- パスワード管理機能
- 暗号化/復号機能 /暗号鍵管理機能
- 秘匿機能
- メール送信/受信チェック機能
- 電子署名機能
- ウイルスチェック機能

4. PSER の実装と利便性評価

本章では、実装した PSER の構成およびその評価について述べる.

4.1 実装

利便性の評価を行うために、3.2.1 で述べたプロキシ方式を Android 上に実装した。図 1 にモジュール構成を示す。

実装の上でポイントとなるのは、「バルブプラグイン機能」および「ペアリングバルブ」である。バルブプラグイン機能とは、セキュリティ機能をバルブとして追加、削除、更新するための機能であり、複数のセキュリティ機能の提供を可能とする。また、3.3.1 で述べたペアリングはペアリングバルブとして実装した。

PSER が提供するセキュリティ機能は、WWW 認証バルブおよび暗号化/復号バルブの 2 つのバルブプラグインを用意した。それぞれ、サーバ利用時のベーシック認証代行機能 (パスワード管理機能) およびファイルサーバ利用時の自動暗号化/復号機能 (暗号鍵管理機能および暗号化/復号機能) の提供を行う。

また、実装した Android には生体認証装置がなかったので、PSER によるユーザ認証は Android の画面ロックとパターン入力で代用した。

図 1 モジュール構成

Figure 1

4.1.1 バルブプラグイン機能

バルブプラグイン機能は、PSER の中に複数のバルブを挿入することができ、各々のバルブで HTTP メッセージ、つまり HTTP ヘッダやコンテンツを自由に操作することができるようになっている。そのため、セキュリティ機能をバルブプラグインとして作成することで、複数のセキュリティ機能を同時に提供することを実現している。(図 2)

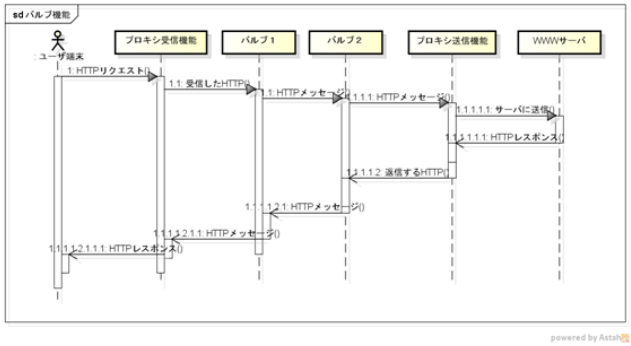

図 2 バルブプラグイン機能

Figure 2

4.1.2 ペアリングバルブ

3.3.1 で述べたペアリングはペアリングバルブとして実装した。その処理手順を図 3 に示す。これにより、ユーザと端末、PSER の相互認証を実現している。

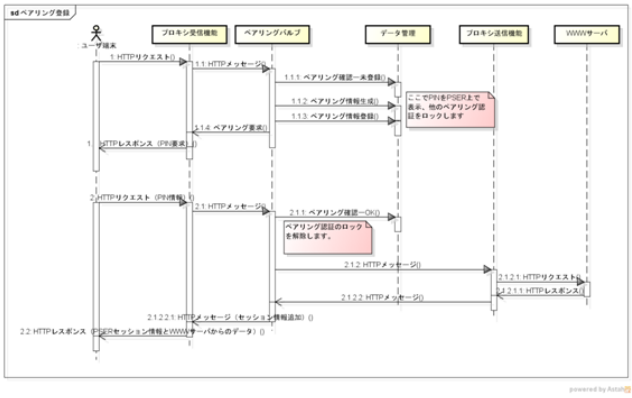

図 3 ペアリング機能 (成功の場合)

Figure 3

4.1.3 WWW 認証バルブ

サーバ利用時のベーシック認証代行機能 (パスワード管理機能) を WWW 認証バルブとして実装した。その処理手順を図 4 に示す。これにより、端末からサーバにアクセスするときの自動ログインを実現している。

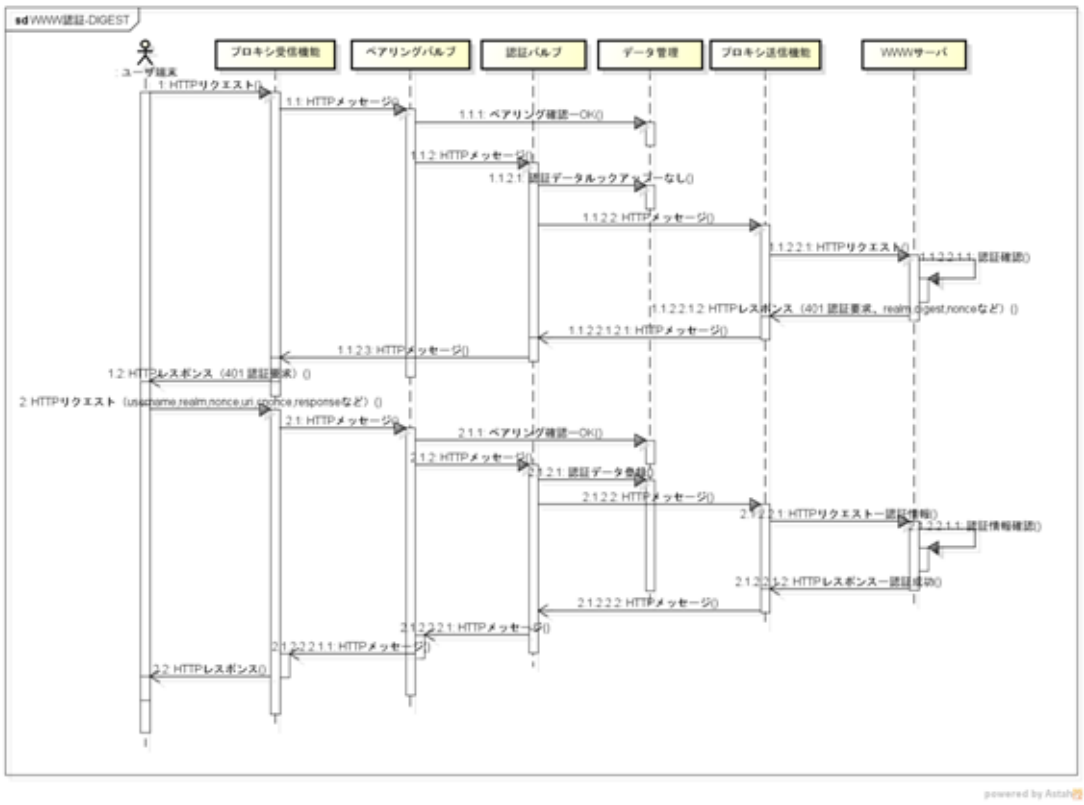

図 4 ベーシック認証代行機能

Figure 4

4.1.4 暗号化/復号バルブ

ファイルサーバ利用時の自動暗号化/復号機能 (暗号鍵管理機能) を暗号化/復号バルブとして、認証バルブと同様に実装した。これにより、端末からサーバにファイルをアップロードするときに自動的に暗号化を行い、ダウンロードするときに自動的に復号を行う。

4.2 利便性の評価

利便性が低下すると、セキュリティ機能が使われなくなる危険性が高まる。そこで、実装した PSER を用いて、実際に以下の操作を行い、利便性の評価を行った。

1. ファイルサーバ (WebDAV)、Windows PC、Android タブレット、iPad を用意
2. Windows PC から PSER を用いてファイルサーバにアクセスし、ファイルをアップロード
3. Android タブレットおよび iPad から PSER を用いてファイルサーバにアクセスし、ファイルを閲覧

ファイルのアップロードと、閲覧に関する詳細について述べる。

4.2.1 ファイルのアップロード

ファイルアップロード時の詳細手順は以下のとおりとなる。

1. Windows PC のプロキシを PSER に設定する。
2. Windows PC から WebDAV サーバにアクセスする。すると、PIN 入力が要求される。
3. PSER の認証を行い、画面に表示された PIN を端末に入力する。
4. ファイルをアップロードする。

PSER を利用しないときと比較して、プロキシの設定が増え、ID/パスワード入力のかわりに PIN 入力となっている。プロキシの設定については、一度行ってしまえば 2 回目からは行う必要はないので大きな負担増ではない。また、複数のサーバにアクセスする場合も PIN 入力は一度の入力ですむので負担減となる。またファイルアップロード時の暗号化も自動で行われるのでこれも負担減となる。

実際に iPad を使い、アクセスするサーバ数に必要となるタップ数をカウントし、サーバ数が多くなると負担減になることを確認した (図 5)。

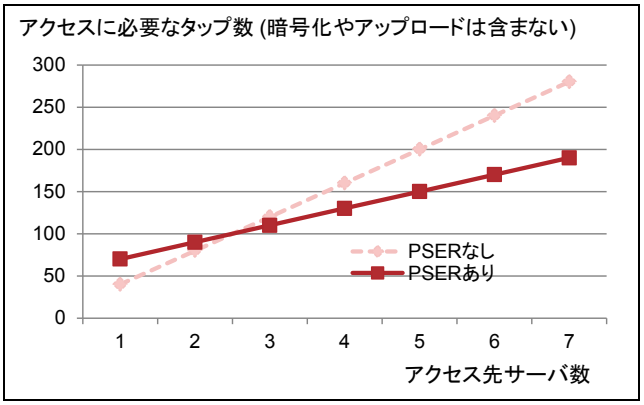

図 5 アクセス先サーバ数に対し必要なタップ数

Figure 5

4.2.2 ファイルの閲覧

ファイル閲覧時の詳細手順は以下のとおりとなる。

1. タブレットのプロキシを PSER に設定する。
2. タブレットのブラウザから WebDAV サーバにアクセスする。すると、PIN 入力が要求される。
3. PSER の認証を行い、画面に表示された PIN を端末に入力する。
4. ファイルを閲覧ロードする。

PSER を利用しないときと比較して、プロキシの設定が増え、ID/パスワード入力のかわりに PIN 入力となっている。プロキシの設定については、一度行ってしまえば 2 回目からは行う必要はないので大きな負担増ではない。また、複数のサーバにアクセスする場合も PIN 入力は一度の入力ですむので負担減となる。またファイル閲覧時の復号も自動で行われるのでこれも負担減となる。

4.3 安全性の議論

実装した PSER を用いてセキュリティ機能を利用した場合の安全性について考察する。

4.3.1 PSER 提供のセキュリティ機能

パスワードや暗号鍵などの情報は PSER で管理されており、所有者自身もわからないため、安全性は高いと言える。

4.3.2 セキュリティ機能の利用によって得られた情報

端末でセキュリティ機能を利用し、ファイルを復号した場合、復号した後のファイルの管理は端末側に求められる。このように、PSER では暗号鍵の管理等のセキュリティ機能の安全な利用までは保証するが、セキュリティ機能の利用によって得られた情報についての、その後の管理は保証されない。

4.3.3 SSL 通信

実装した PSER はプロキシ方式でセキュリティ機能を提供している。セキュリティを求められる通信は SSL で通信することが求められるが、SSL は端末上のアプリケーションとサーバの間で暗号化して行われるものであり、PSER のような通信路上で盗聴から保護されている。今回は PSER がサーバを偽装し、端末と PSER の間で SSL 通信を行い、PSER とサーバの間で SSL 通信を行うように実装したが、SSL 通信の趣旨を考えた場合、健全な実装方式ではないため、今後の検討が必要である。

5. PSER の応用

PSER ではプライバシー情報や重要情報を安全に格納、利用することができるので、電子マネーの管理等にも利用できる。本章では、電子クーポン利用システムへの応用およびヒューマンセントリックコンピューティングへの応用について述べる。

5.1 電子クーポン利用システム

5.1.1 背景と課題

店が客の囲い込みを目的としたサービス利用クーポンを発行する際、店側と客側でそれぞれ以下の要望を持つ場合があると考えられる。

- 店側の要望
  - クーポンを他人に譲渡してほしくない (個人を特定できなくても良いが、クーポン発行対象本人かどうかを確認したい)
- 客側の要望
  - どのようなクーポンを利用したか、という利用履歴を店側に把握されたくない。

課題を整理すると、以下の 2 つの条件を同時にみたすクーポンシステムが求められている。(図 6)

1. クーポン発行装置およびサービス提供者は、個人を特定する情報を得ることはできない (クーポンにユーザ名やユーザ ID を記入できない)
2. サービス提供者はクーポン発行対象本人かどうかを検証できる

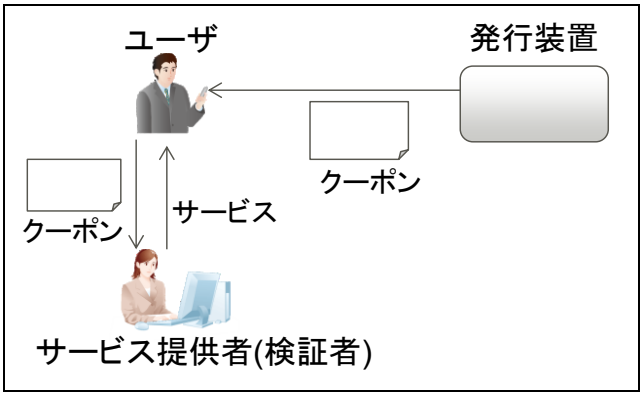

図 6 クーポンの利用

Figure 6

5.1.2 PSER を用いた実現方式

PSER を 1 つの信頼点とすることで、以下の方式で課題を解決できる。(図 7)

- 発行装置はクーポンを PSER に紐づけて発行する。また、サービス利用時は、クーポンと PSER をセットでクーポンの検証を行う。
- クーポンには以下の 2 つの特徴を持つ PSER 識別子を付与する。
  1. PSER 識別子だけでは、どの PSER と紐づいているのか判別不能。(クーポンごとに PSER 識別子は異なるものにする)
  2. PSER 識別子と PSER の両方があれば、PSER 識別子がその PSER と紐づいているかを判定可能。
- PSER 認証局を用意し、サービス提供者は PSER が偽造されたものではないことを確認できるようにする。

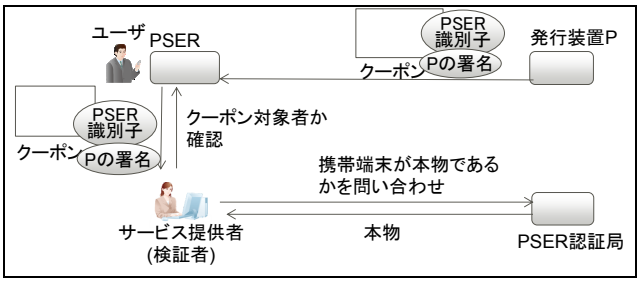

図 7 電子クーポン利用システム

Figure 7

PSER 識別子は、乱数値と PSER がもつ秘密鍵で乱数値を加工したものの組とし、サービス提供者は PSER が乱数値を同じように加工できるかを判定することで、クーポン発行対象本人を確認できる。

また、PSER 認証局でも、問い合わせ側 (サービス提供者) が生成した乱数と、PSER がもつ秘密鍵で乱数値を加工したものの組から、PSER が偽造されたものではないことを確認できる。(図 8)

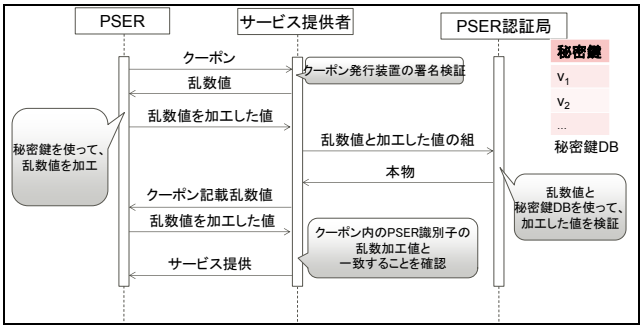

図 8 電子クーポン利用に対するサービス提供手順

Figure 8

本システムでは、発行装置が発行したクーポンをサービス提供者が信頼する必要があるが、システム全体として発行装置やサービス提供者を信頼できる必要はない。そのため、発行装置およびサービス提供には認可等は不要であり、すぐにサービスを開始できる。

5.2 ヒューマンセントリックコンピューティング

ユーザの興味・関心や行動状況といったコンテキスト情報から、ユーザの状況にあわせたサービスを実現するための研究が行われている[5]。このとき使用されるコンテキスト情報には、ユーザの秘密情報やプライバシー情報を含むことになるため、それらの情報を安全に管理することが求められている。PSER はそれらの情報を安全に管理するデバイスとしても応用できると考えている。

6. おわりに

本稿では、従来、各端末で管理していたセキュリティ機能を、耐タンパーなデバイスである PSER に集約し、PSER から各端末にセキュリティ機能を提供する方式を提案した。また、プロキシ方式で実現できるセキュリティ機能について、Android 上に実装し利便性の評価を行い、有効であることを示した。さらに、PSER の応用例についても考察を行った。今後の課題は、PSER 内のセキュリティ機能や秘密情報を安全に管理、維持するための方式の検討、および、セキュリティ機能や秘密情報ごとに安全に提供するための方式の検討、を行うことである。

参考文献

[1] 総務省, “一般利用者のための情報セキュリティ対策−実践編 パスワードの検討と管理, “ http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/j_enduser/ippan07.htm

[2] IPA, “情報セキュリティ対策のしおり”, http://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf

[3] 株式会社富士通研究所, “メールからの情報漏洩対策技術を開発”, http://pr.fujitsu.com/jp/news/2009/03/13.html

[4] 株式会社富士通研究所, “業界初！標的型メール攻撃を端末側でリアルタイムに検知・警告する技術を開発”, http://pr.fujitsu.com/jp/news/2012/05/15-3.html

[5] 株式会社富士通研究所, “スマートフォンを安全に業務で利用可能とするアプリケーション実行基盤技術を開発”, http://pr.fujitsu.com/jp/news/2012/08/31-1.html

[6] 海野雪絵，野田敏達，大久保隆夫，金谷延幸：Web アプリから利用者端末内情報へのコンテキストアウェアなアクセス制御手法の提案，情報処理学会第 60 回コンピュータセキュリティ研究会研究報告(2013).

[7] 大久保隆夫，海野雪絵，野田敏達，金谷延幸：近傍デバイスを利用したコンテキスト依存セキュリティシステムの提案，情報処理学会第 60 回コンピュータセキュリティ研究会研究報告(2013).