M-001

携帯端末と公共端末の連携による認証システムの提案
Proposal of authentication system by federation of mobile terminal and public terminal

梅澤 克之† 加藤 崇利† 萱島 信† 手塚 悟‡
Katsuyuki Umezawa Takatoshi Kato Makoto Kayashima Satoru Tezuka

1. はじめに

近年，携帯電話の保持率は一人一台以上になっている．また，個人所有だけではなく公共端末なども含めて，様々な端末を使って様々なサービスが受けられるようになってきた．サービスを受ける際にはユーザ認証が重要である．ユーザ認証の際に，個人が所有する携帯端末を「鍵」として利用できれば便利である．例えば，ID/パスワードの保管庫として用いて，携帯端末を PC にかざすだけで Web のフォームへ自動入力がなされると便利である．また，認証用のハードウェアトークンや決済用の IC カード，カーシェアリング向けの乗用車の鍵としての各役割を携帯端末が果すことで，ユーザの利便性が大きく向上することが期待できる．

本報告では，このようなユースケースを実現するための携帯端末を認証情報の保管庫として用いる端末連携認証システムの提案を行う．具体的には，認証情報としての ID/パスワードや Cookie 情報を引き継ぐことによって，旧端末から新端末に切り替えたときに，サーバ側の認証を簡略化する方法を提案する．さらにその際に，認証情報を引き継ぐ先の端末の信頼性を確認し，安全であることが分かった場合のみ認証情報を連携させる方式を提案する．そして，提案に基づいたシステムを開発し性能を評価する．

以下では，まず，2 章で一般的な利用イメージを想定して提案のモチベーションを示す． 3 章で SSO, Cookie による認証，NFC ハンドオーバー技術などの関連技術を示す．4 章で ID/パスワードや Cookie 情報を携帯電話と PC 端末間で転送しあう提案方式について示す．5 章で性能の評価を行い，6 章で提案方式の妥当性の検証を行う．最後に 7 章でまとめと今後の課題を示す．

2. 提案のモチベーション

図 1 に PC 端末を使って Web アクセスを行う際の利用シーンを示す．図 1 に示したように，現状では様々なサービスに対して個別に ID が振られて，それぞれの ID ごとにパスワードの入力を行う必要がある．また，サービスのポリシーによっては短期間で別のパスワードへの変更を強制される場合もある．このように多数の ID とパスワードを覚えておくことはかなり難しい状況にある．これに対して Web ブラウザに覚えさせてしまう方法もあるが，多人数で利用する共用端末（以降，公共端末と呼ぶ）などでは，ユーザが変わるごとにキャッシュをクリアするなどの運用を行わないとキャッシュしたパスワードを勝手に利用されてしまう場合がある．そこで個人が所有する携帯端末に ID/パスワードを覚えさせて，PC にかざすことで，PC の安全性を確認した上で ID/パスワードを渡すことで利便性と安全性の向上が期待できる．

† 日立製作所 横浜研究所 Hitachi, Ltd.
‡ 東京工科大学 Tokyo University of Technology

図 2 に外出先での利用シーンを示す．外出先では利用場所の制限等により携帯端末単体での利用が好ましい場合がある．このときにも外出前に行っていた作業を継続したいという要求や，再認証手続きを簡略化したいという要求が強い．

図 1 携帯端末が認証情報の保管庫に

図 2 PC 端末での業務を引き継ぐ

図 3 に携帯端末を認証トークンとして用いることの利点を示す．例えば PC 端末が置き引きにあったとしても，鍵としての携帯端末が同時に盗まれなければ，PC 端末は利用できない．また，携帯端末を単体で盗まれたとしても，携帯端末の GPS 機能での追跡や，サーバ経由でリモートデータ消去が行えるため，携帯端末は失くしても安心な認証トークンになり得る．

図 3 携帯端末を失くしても安心

3. 関連研究

3.1 シングルサインオン (SSO)

前節の図 1 で ID/パスワードを何回も入力する必要がある旨の課題を示した．このような課題を解決する技術として従来からシングルサインオン(SSO)が実用化されている．この SSO はサーバ間で認証情報をやり取りする技術である．これに対して提案方式は，端末間で認証情報をやり取りして，端末を切り替えた場合にも適用できる方式を目指すものである．

3.2 Cookie 情報を用いた認証

Cookie は HTTP プロトコルを用いた Web ブラウザ間での状態を管理するプロトコルとして使用されている．例えば Web サイトの訪問履歴やログイン情報など Web ブラウザによって保存され，再度同じ Web サイトを訪問した際に保存された Cookie 情報を Web サイトに送信することによって，訪問履歴の更新やログイン処理を省略することが可能となる．Cookie については，RFC2109[1]，RFC2965[2]で規定されている．

3.3 Near Field Communication(NFC) ハンドオーバー

NFC による接続ハンドオーバーは，NFC Forum で規定されている．端末－端末間での接続技術であり，端末と端末の対応関係の確立（ペアリング）だけを NFC(ISO 14443 Type A/Type B 等)で行う．以降のデータ通信は，さらに高速な Bluetooth や WiFi を行う技術である[3].

3.4 携帯端末を用いたリモートアクセス技術

筆者らは，携帯端末をセキュリティデバイスと見なして PC 端末と連携させてリモートアクセスを行うシステムの提案を行ってきた[4][5][6][7]．しかし，これらの提案では携帯端末と PC 端末は個人の持ち物という前提でそれらの端末の組み合わせは固定的であった．例えば共有 PC 端末を利用する場合などは動的な端末の組み合わせが必要とされていた．

このような動的な端末の組み合わせを可能とし，いくつかの通信プロトコルに対応させる提案も行ってきた[8][9][10][11]．しかしこれらの提案では，認証情報を引き継ぐ先の端末の安全性について考慮していなかった．

4. 提案方式

本節では，認証情報を引き継ぐ先の端末の信頼性を確認し，安全であることが分かった場合のみ認証情報を連携させる方式を提案する．

4.1 提案方式の概要

本節では提案方式の全体概要について記述する．図 4 に全体概要を示す.提案方式では図 4 に示すように，3 つの利用シーンを想定する．

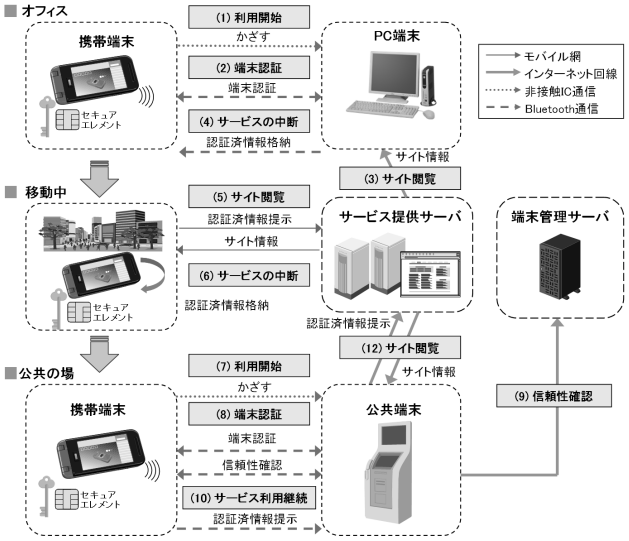

図 4　提案システムの全体概要

- 携帯端末を PC 端末にかざすことによって ID/パスワードを転送し，Web のフォームへ自動入力しサービス提供サーバに自動的に接続する．一度 Web 認証がなされると，サービス提供サーバ側から認証済情報としての Cookie が発行されるので，その Cookie 情報を携帯電話に保管する（図 4 の「オフィス」）．
- 携帯端末自身でサービスを受ける場合には，前記 Cookie 情報を自身のブラウザにセットし，サービス提供サーバに接続しサービスを受ける（図 4 の「移動中」）．
- 最後に，公共の場で，不特定多数のユーザが利用する端末（公共端末）でサービスを受ける（図 4 の「公共の場」）．不特定多数のユーザが利用する公共端末では，端末の安全性が確保されていない状態でパスワードや Cookie 情報を転送してしまうことはセキュリティ上問題がある．よって，携帯端末と公共端末で端末認証を行ったうえで，さらに，ウィルスやマルウェアが存在していないことを端末管理サーバで確認することで端末の安全性を確認する．その後，携帯端末内に保管されている Cookie 情報を公共端末に転送し，公共端末のブラウザにセットし，サービス提供サーバに接続しサービスを受ける．

なお，図 4 の(2)(8)の端末認証は，これらの端末同士が提案方式のスキームに従っているかを確認するためであり，(9)の信頼性確認は，提案方式のスキームに従っている端末だとしても利用時に安全な状態になっているとは限らないため，その確認のために必要な処理である．

4.2 提案方式のシーケンス

本節では前節で示した 3 つの利用シーンについて，それぞれ下記に列挙するシーケンスについて詳細を示す.

- オフィスで，携帯端末を PC 端末にかざしてサービスを受ける.
- 移動中に，携帯端末でサービスを受ける.

- 移動先の公共の場で，携帯端末を公共端末にかざして，公共端末の安全性を確認する．
- その後，携帯端末内の認証情報を使って公共端末でサービスを受ける．

4.2.1 PC 端末利用のシーケンス

PC 端末に携帯端末をかざして PC 端末上でサービスを享受し，携帯端末に認証情報を連携するまでの処理フローを図 5 に，その説明を表 1 に示す．

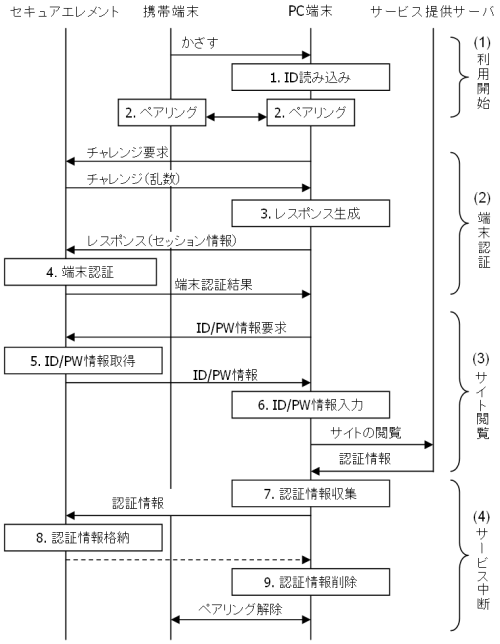

図 5　PC 端末利用のシーケンス

表 1　図 5 の説明

No.	説明
1	PC 端末に携帯端末をかざすと，PC 端末はかざされた FeliCa の ID を読み込む
2	PC 端末と携帯端末間で Felica の ID をパスフレーズとして Bluetooth のペアリングを行う
3	PC 端末は携帯端末のセキュアエレメントからチャレンジを取得し，PC 端末があらかじめ共有している共通鍵でチャレンジを暗号化したレスポンスを生成し，セキュアエレメントに送付する
4	セキュアエレメントは，チャレンジを共通鍵で暗号化した出力値と PC 端末から送付されたレスポンスを比較し，値が一致した場合は，端末認証成功と見なす．以降，本レスポンス値をセッション情報として保持する
5	セキュアエレメントは，PC 端末からの要求に従い，ウェブサイトへログインするための ID/パスワード情報を PC 端末に送付する
6	PC 端末は実行中のブラウザを検索し，ID/パスワード情報を入力し，PC 端末からサービス提供サイトにアクセスする．サイトから認証情報(Cookie) が発行され，サービスを受ける
7	PC 端末は，自端末のブラウザが管理している認証情報を収集し，携帯端末に接続されているセキュアエレメントに送付する
8	セキュアエレメントは受信した認証情報をセキュア領域に書き込む
9	PC 端末は，自端末のブラウザが管理している認証情報を削除する

4.2.2 携帯端末利用のシーケンス

セキュアエレメントに格納されている認証情報を利用して，携帯端末上で引き続きサービスを享受する処理のフローを図 6 に，その説明を表 2 に示す．なお，携帯端末は個人利用を想定しているため信頼性確認は省略している．

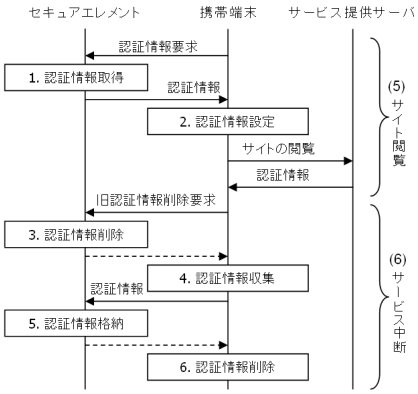

図 6　携帯端末利用のシーケンス

表 2　図 6 の説明

No.	説明
1	セキュアエレメントは，セキュア領域内に格納している認証情報を取得し，携帯端末に渡す
2	携帯端末は受信した認証情報をブラウザに格納し，サービス提供サイトにアクセスする．サイトから認証情報が発行され，サービスを受ける
3	セキュアエレメントは携帯端末からの要求に従い，格納している旧認証情報を削除する
4	携帯端末はブラウザが管理している認証情報を収集し，セキュアエレメントに渡す
5	セキュアエレメントは認証情報をセキュア領域に書き込む
6	携帯端末はブラウザが管理している認証情報を削除する

4.2.3 公共端末の安全性確認のシーケンス

公共端末に携帯端末をかざして，公共端末の安全性を確認する処理のフローを図 7 に，その説明を表 3 に示す．

なお，本節で説明する端末認証および信頼性確認の処理の詳細について付録に図示する．

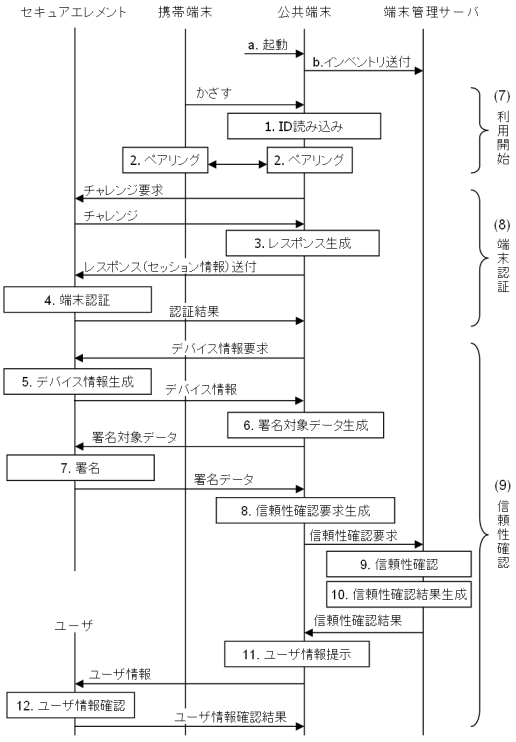

図 7　公共端末の安全性確認のシーケンス

表 3　図 7 の説明

No.	説明
a	信頼性確保のアプリケーションを起動する
b	信頼性確保は自端末のインベントリ情報を収集し，定期的に端末管理サーバに送付する
1	公共端末に携帯端末をかざすと，公共端末はかざされた FeliCa の ID を読み込む
2	公共端末と携帯端末間で Felica の ID をパスフレーズとして Bluetooth のペアリングを行う
3	公共端末は携帯端末のセキュアエレメントからチャレンジを取得し，公共端末があらかじめ共有している共通鍵でチャレンジを暗号化したレスポンスを生成し，セキュアエレメントに送付する．（今回の提案では共通鍵を使っているが公開鍵方式を用いても良い）
4	セキュアエレメントは，チャレンジを共通鍵で暗号化した出力値と公共端末から送付されたレスポンスを比較し，値が一致した場合は，端末認証成功と見なす．以降，本レスポンス値をセッション情報として保持する
5	セキュアエレメントは，公共端末からの要求に従い，ステップ 4 の端末認証結果を確認し認証済みの場合には，デバイス情報を構成し，事前に保持している端末管理サーバの公開鍵でデバイス情報を暗号化し，公共端末に送付する（デバイス情報とは，携帯端末のデバイス ID，ユーザテキスト（ユーザが事前に設定した任意の文字列），セッション情報，およびデバイス情報生成時刻から構成される情報である）
6	公共端末は，署名対象元データ（自端末の端末 ID と，携帯端末から受信した暗号化されたデバイス情報を連結したデータ）のハッシュ値（＝署名対象データ）を生成し，セキュアエレメントに送付する．（署名対象データの生成はセキュアエレメント内でも行えるが，転送データ量，処理速度の観点から公共端末内で行うこととした）
7	セキュアエレメントは，ステップ 4 の端末認証結果を確認し認証済みの場合には，署名対象データを自身の秘密鍵で暗号化した署名データを生成し，公共端末に送付する
8	公共端末は端末管理サーバに対し，信頼性確認要求（ステップ 6 で生成した署名対象元データとステップ 7 で受信した署名データ）を生成し，端末管理サーバに送付する
9	端末管理サーバは受信した署名データを，その署名を生成したセキュアエレメントの秘密鍵に対応した公開鍵で検証し，署名検証が成功した場合は続いて信頼性確保のインベントリ情報を確認する
10	署名とインベントリ情報がともに問題ないことが確認できると，信頼性確認結果（署名対象元データ内の暗号化されたデバイス情報を復号し，復号されたデバイス情報中のセッション情報と信頼性確認を行った時刻情報を連結し，端末管理サーバの秘密鍵で暗号化したデータ）を生成し，信頼性確認結果とユーザ情報（ユーザが事前に設定した画像データとユーザテキスト）を公共端末に送付する
11	公共端末は，端末管理サーバから受け取ったユーザ情報をユーザに提示する
12	ユーザは公共端末に表示された内容を視認し，事前に設定・登録したユーザ情報と相違ないことを確認し，続行／中止のいずれかのボタンを押下する．公共端末は，以降の処理におけるセキュアエレメントへのコマンドには，ステップ 18 で端末管理サーバがら受信した信頼性確認結果をコマンドに付加してセキュアエレメント内でその信頼性確認結果を検証することでセキュアエレメントへの不正なコマンド実行を防ぐことができる

4.2.4 公共端末利用のシーケンス

公共端末の安全性を確認したうえで，PC 端末から引き継いだ認証情報を引渡し，公共端末上で引き続きサービスを享受する処理のフローを図 8 に，その説明を表 4 に示す．

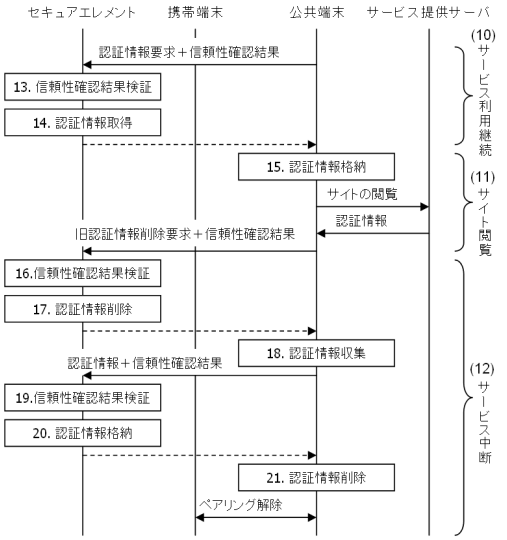

図 8　公共端末利用のシーケンス

表 4　図 8 の説明

No.	説明
13	セキュアエレメントは，公共端末からの認証情報要求に対して，信頼性確認結果を検証する．具体的には，端末管理サーバの秘密鍵を使って生成された信頼性確認結果をセキュアエレメント内にあらかじめ設定された端末管理サーバの公開鍵で検証する）
14	信頼性確認結果の検証に成功すれば，セキュア領域に格納している認証情報を，携帯端末を経由して公共端末に送付する
15	公共端末は受信した認証情報を，自端末のブラウザに格納し，サービス提供サイトにアクセスする．サイトから認証情報が発行され，サービスを受ける
16	ステップ 13 と同様に信頼性確認結果を検証する
17	信頼性確認結果の検証に成功すれば，セキュア領域に格納している旧認証情報を削除する
18	公共端末は，自端末のブラウザが管理している認証情報を収集し，携帯端末に接続されているセキュアエレメントに送付する
19	ステップ 13 と同様に信頼性確認結果を検証する
20	信頼性確認結果の検証に成功すれば，セキュアエレメントは受信した認証情報をセキュア領域に書き込む
21	公共端末は，自端末のブラウザが管理している認証情報を削除する

4.3 提案方式のモジュール構成

本節では，提案方式のモジュール構成を示す．PC 端末，携帯端末，端末管理サーバのそれぞれのモジュール構成を図 9 に示す．

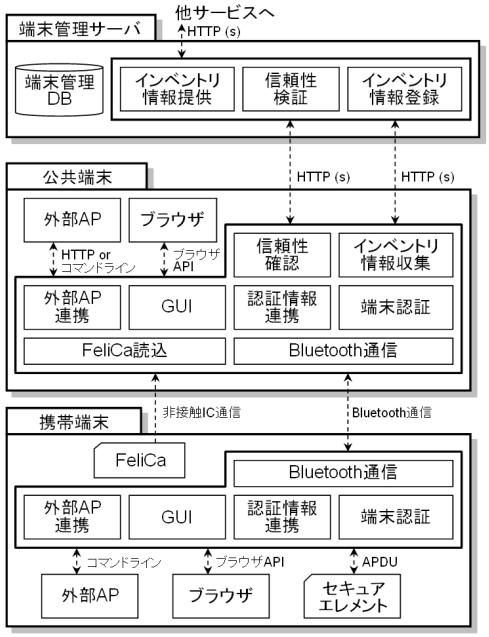

図 9　提案方式のモジュール構成

図 9 に示したように公共端末側は下記の機能モジュールで構成される．

- **GUI:** 通信パラメータの設定やログの表示などを行う
- **認証情報連携:** Bluetooth 通信を使って，携帯電話と ID/パスワードや Cookie などの認証情報の送受信を行う
- **外部 AP 連携:** PC 上の外部アプリケーションからの認証情報の転送や削除などの命令を受け認証情報連携モジュールに伝える
- **端末認証:** 携帯端末からの要求に応じて端末認証処理を実行する
- **信頼性確認:** 端末管理サーバに，端末情報（自端末と ID デバイスの情報)，および端末情報に対してセキュアエレメントが署名した署名値を送信し，信頼性確認処理を実行する
- **インベントリ情報収集:** 定期的に端末内のインストール済みソフトウェア情報等のインベントリ情報を収集し，端末管理に送付する
- **Bluetooth 通信:** Felica 読み込みモジュールで読み込んだ Felica の ID を使って携帯電話と Bluetooth のペアリングを行い携帯電話とデータの送受信を行う
- **FeliCa 読込:** Felica がかざされるのを待ち受けて，Felica の ID を読み込
- **外部 AP:** サービスに関連した細部アプリケーション
- **ブラウザ:** Web 閲覧用のブラウザ

また，図 9 に示した携帯端末側は下記の機能モジュールで構成される．

- **GUI:** 通信パラメータの設定やログの表示などを行う．
- **認証情報連携:** Bluetooth 通信を使って，PC 端末と ID/パスワードや Cookie などの認証情報の送受信を行う．
- **外部 AP 連携:** 携帯電話上の外部アプリケーションからの認証情報の転送や削除などの命令を受け認証情報連携モジュールに伝える．
- **端末認証:** セキュアエレメントに接続し，認証および暗号処理を中継する
- **Bluetooth 通信:** Felica の ID を使って PC と Bluetooth のペアリングを行い PC 端末とデータの送受信を行う．
- **外部 AP:** サービスに関連した細部アプリケーション
- **ブラウザ:** Web 閲覧用のブラウザ
- **FeliCa:** 非接触 IC 通信を行う IC チップ
- **セキュアエレメント:** 認証情報などを保管する IC チップ

さらに，図 9 に示した端末管理サーバ側は下記の機能モジュールで構成される．

- **信頼性検証:** 携帯端末の署名と公共端末のインベントリ情報を検証し，検証結果とユーザ情報を公共端末に返す
- **インベントリ情報登録:** 公共端末から送付されたインベントリ情報を登録，検証する
- **インベントリ情報提供:** 登録されているインベントリ情報を提供する
- **端末管理 DB:** インベントリ情報とデバイス情報を管理する

5. 評価

本節では，ID／パスワード連携によるサービスへのログイン処理と Cookie 連携によるサービスへのログイン処理，端末の安全性確認処理，インベントリ情報登録関連処理の性能評価結果について記述する．

5.1 測定条件

性能測定対象の端末のスペックは，表 5，表 6，表 7 に示した通りである．端末間の非接触 IC 通信には FeliCa を用い，ハンドオーバー後の Bluetooth に関しては Bluetooth Ver.2.1 対応のアダプタを用いた．また，PC とサーバ間のネットワークには表 8 に示した有線 LAN と ADSL 通信網，および CDMA 1X WIN 対応の 3G データ通信を用いた．また，計測に用いたインベントリ情報のサイズは 45kB であった．

表 5　測定に用いた PC 端末，公共端末のスペック

OS	Windows XP SP3
CPU	Intel Core2 Duo T8100 (2.10 GHz)
Memory Size	3 GB
Browser	Internet Explorer 8

表 6　測定に用いた端末管理サーバのスペック

OS	CentOS 5.5
CPU	Intel Core2 Duo T8100 (2.10 GHz)
Memory Size	3 GB

表 7　測定に用いた携帯端末のスペック

OS	Windows Mobile 6.5 Professional Edition
CPU	Qualcomm QSD8650 1 GHz
Memory Size	512 MB (ROM)/384 MB (RAM)
Browser	Internet Explorer Mobile

表 8　測定に用いた回線スペック

Cable LAN	Gigabit Ethernet
ADSL	8 Mbps (downstream)\/1 Mbps (upstream)
3G	2.4 Mbps (downstream)\/114 Kbps (upstream)

5.2 測定項目

以下のシーケンスを測定した.

- 携帯端末と PC 端末の連携による処理

(1-1) ID/パスワード連携によるログイン処理（図 5 の(1)利用開始処理と(3)サイト閲覧処理）
(1-2) PC 端末から認証済み情報のセキュアエレメントへの移行処理（図 5 の(4)サービス中断処理）

- 携帯端末単体での処理

(2-1) 携帯端末単体によるログイン処理（図 6 の(5)サイト閲覧処理）
(2-2) 携帯端末内でのセキュアエレメント内の認証済み情報の削除処理（図 6 の(6)サービス中断処理の前半）
(2-3)携帯端末内での認証済み情報のセキュアエレメントへの移行処理（図 6 の(6)サービス中断処理の後半）

- 携帯端末と公共端末の連携による処理

(3-1) 端末の安全性確認（端末認証と信頼性確認）処理（図 7 の(8)端末認証処理と(9)信頼性確認処理）
(3-2) 認証情報連携によるログイン処理（図 8 の(10)サービス利用継続処理と(11)サイト閲覧処理）
(3-3) PC 端末からセキュアエレメント内の認証済み情報の削除処理（図 8 の(12)サービス中断処理の前半）
(3-4) PC 端末から認証済み情報のセキュアエレメントへの移行処理（図 8 の(12)サービス中断処理の後半.ただし(1-2)と同様の処理のため計測なし）

- インベントリ関連処理

(4-1) インベントリ情報の新規登録（図 7 のステップ a～b）
(4-2) インベントリ情報の更新（図 7 のステップ a～b（2 度目以降の場合））
(4-3) インベントリ情報の提供（図 9 の他サービスがインベントリ情報提供モジュールへ情報提供要求を送りインベントリ情報を受けるまでの処理）

5.3 測定結果

本節では，各測定項目の処理の詳細と測定結果を記載する．各測定項目において 12 回測定し，全体の時間が最小と最大のデータを除外した 10 回分の測定値から平均値を算出した.

表 9 の(1-1)より，ID パスワード連携方式で携帯端末をかざしてから 2 秒以内でログインできることが確認できた．また，(2-1)より，移動中に 3G 網を用いる携帯端末単体利用で約 10 秒で業務が継続できることが確認できた．さらに，(3-1)(3-2)より，端末の安全性確認が必要な公共端末利用においても 10 秒以内で業務を開始できることが確認できた[1].

表 9　測定結果

No.	Process	Time (Sec)
(1-1)	ID/パスワード連携によるログイン処理	1.71(LAN), 1.74(ADSL)
(1-2)	PC 端末から認証済み情報のセキュアエレメントへの移行処理	4.60(Bluetooth)
(2-1)	携帯端末単体によるログイン処理	10.48(3G)
(2-2)	携帯端末内でのセキュアエレメント内の認証済み情報の削除処理	2.03(内部処理)
(2-3)	携帯端末内での認証済み情報のセキュアエレメントへの移行処理	3.03(内部処理)
(3-1)	端末の安全性確認（端末認証と信頼性確認）処理	4.35(ADSL)
(3-2)	認証情報連携によるログイン処理	5.04(LAN), 5.34(ADSL)
(3-3)	PC 端末からセキュアエレメント内の認証済み情報の削除処理	3.87(Bluetooth)
(4-1)	インベントリ情報の新規登録	0.75(ADSL)
(4-2)	インベントリ情報の更新	0.73(ADSL)
(4-3)	インベントリ情報の提供	0.95(ADSL)

6. 提案方式の妥当性検証

図 4 で説明したシステムでは，公共の場において作業を継続する場合に，多数のユーザが公共端末に対してユーザの個人情報等を提示する必要がある．これらの情報の機密性を保証するには，公共端末の信頼性が確保されていることが重要である．以下では，公共端末で想定すべき攻撃手法と，それらの攻撃に対して，本提案手法が有効に機能することを説明する.

6.1 攻撃手法

公共端末に対する攻撃手法は，以下の 2 種類に大別される.

6.1.1 公共端末のすり替え

公共端末のハードウェア全体を偽の端末にすり替える手法や，汎用のオペレーティングシステムを用いた公共端末であれば，HDD を差し替えたり，CD-ROM，USB メモリを用いてブートさせたりすることにより，公共端末をすり替えることが可能になる．すり替えた端末に処理させることにより，攻撃者は機密情報の入手，改ざんといった行為を実行することが可能となる.

6.1.2 マルウェアの混入

公共端末にキーロガー等のマルウェアを混入させることにより，公共端末上で処理される機密情報の入手，改ざんといった行為を実行することが可能となる.

6.2 対策手法

本課題においては，以下の方式により上記の攻撃手法に対する対策を実施した.

6.2.1 公共端末のすり替えの検知

セキュアエレメントを備えた携帯端末が公共端末内の信頼性検証モジュールに対し，認証シーケンスを実行することにより，公共端末のすり替えを検知する．セキュアエレメントと信頼性確保モジュール間の通信を盗聴されるとリプレイアタックが可能になるため，認証シーケンスはチャレンジ＆レスポンス方式を採用する.

[1] (1-2),(2-2),(2-3),(3-3),(4-1),(4-2),(4-3)はバックエンドで処理ができるステップなので，ユーザの使い勝手には影響しないようにできる.

6.2.2 マルウェアの混入の検知

インベントリ情報収集モジュールが，公共端末のインベントリ情報を定期的に端末管理サーバに報告する[1]．また，信頼性確認モジュールは，ユーザが公共端末を使用する際に，携帯端末より入手したデバイス情報と，自身の端末情報を"信頼性確認要求"として端末管理サーバに送付する．端末管理サーバは，インベントリ情報の確認結果を携帯端末に返送することにより，マルウェアの混入を検知する．マルウェアが混入した公共端末に携帯端末と端末管理サーバ間の通信を中継されると，情報の漏えいや改ざん，およびリプレイアタックが可能になるため，以下の対策を採用する．

- デバイス情報がマルウェアが混入した公共端末に漏えいしないように，セキュアエレメント内で端末管理サーバの公開鍵を用いてデバイス情報を暗号化する．毎回暗号結果が異なるように，デバイス情報にはデバイス情報生成時刻を付加する．
- 公共端末の端末 ID の改ざんにより，端末 ID を別端末のものに変更されないように，公共端末から端末管理サーバに送信する信頼性確認要求は，セキュアエレメントによって署名されたデータとする[2]．
- マルウェアがアプリケーション起動後の偽画面の提示によるフィッシングができないように，公共端末がリプレイすることのできない画面情報（携帯端末側で生成する毎回異なるテキスト情報を含んだ）を公共端末に表示させる．

7. おわりに

本論文では，ユーザ認証の際に，携帯端末を「鍵」として利用する利便性と安全性を兼ね備えた認証システムを提案した．具体的には，ID/パスワードや Cookie 情報のような認証情報を携帯端末内に保管し，非接触 IC 通信と近距離無線通信を利用して，携帯端末を PC 端末にかざすだけで Web 認証が行える認証システムを提案した．また，携帯端末をかざす先の端末として，共用の公共端末を想定した場合に，その公共端末の安全性をユーザに示したうえで認証情報を連携させる方式を提案した．さらに，プロトタイプシステムを開発し，性能の評価を行った．これにより，ユーザはサービスを受ける別端末に携帯端末をかざすだけで安全に認証が行われサービスを受けることが可能となった．

今回の研究開発では，携帯端末として Windows Mobile 端末を用いてプロトタイプ実装を行った．今後は，多種多様な携帯端末の登場が予想されるために，それらの端末に対応させていく必要がある．また，携帯端末と対になる認証情報を連携させサービスを受ける側の端末としては，Windows PC 端末を用いた．今後は Windows PC 以外の Linux 端末や，タブレット型の端末の利用も想定されるために，それらの端末に対応させていく必要がある．また，携帯端末と PC 端末間の近距離無線通信として，Bluetooth 通信を用いたが，今後は，Wi-Fi や ZigBee などのような Bluetooth 以外の近距離無線通信に対応させる必要がある．さらに，今回は，ID/PW および Cookie 方式における認証情報連携機能の実装を行ったが，例えば VPN や SSL など他のプロトコルに対応させていく必要がある．また，インベントリ情報として管理しているソフトウェアの構成を意図的に途中で変更しなくてはならない事象に対応させるために，ソフトウェアのホワイトリスト等による運用を行う必要がある．

[1] 公共端末内のインベントリ情報収集モジュールは正しく動作することを仮定する．また，インベントリ情報そのものには，インベントリ情報収集モジュールが署名付きの情報として端末管理サーバへ送信するものとする．

[2] 公共端末の端末 ID と公共端末の公開鍵，事前に端末管理サーバに登録されているものとする．端末 ID は，公共端末の識別子とその識別子の署名値（識別子を公共端末の秘密鍵で署名を付したもの）とする．これにより端末 ID が偽造されても端末管理サーバ側で不正をチェックできる．

謝辞

本研究は，独立行政法人情報通信研究機構(NICT)の委託研究「端末プラットフォーム技術に関する研究開発」の成果の一部である．

参考文献

[1]D. Kristol and L. Montulli, RFC2109: HTTP State Management Mechanism, IETF, Feb. 1997.
[2]D. Kristol and L. Montulli, RFC2965: HTTP State Management Mechanism, IETF, Oct. 2000.
[3]Connection Handover Technical Specification, NFC Forum, Nov. 2008
[4]梅澤克之, 洲崎誠一, “スマートフォンを用いたリモート接続システムの開発,”第 31 回情報理論とその応用シンポジウム予稿集, pp.971--974, Oct. 2008.
[5]梅澤克之, 加藤崇利, 手塚悟, “携帯端末を用いた FMC 認証方式の開発,” 電子情報通信学会 技術研究報告(ISEC2009-36, SITE2009-28, ICSS2009-50), pp.203--208, Jul. 2009.
[6]梅澤 克之, 加藤 崇利, 手塚 悟,“スマートフォンを用いたリモート接続システムの開発と評価,”第 8 回情報科学技術フォーラム(FIT2009)予稿集 第 4 分冊, pp.67-73, Sep. 2009.
[7]梅澤克之, 手塚悟, “スマートフォンをセキュアデバイスとして用いるリモート接続システムの開発と評価,”電子情報通信学会論文誌 B Vol. J94-B No.4 pp. 530-538, April 2011.
[8]梅澤克之, 田代卓, 手塚悟, “GBA プロトコルに基づいた認証情報連携技術の開発と評価,”電子情報通信学会情報通信システムセキュリティ(ICSS) 技術研究報告 Vol. 110, No.115, pp.47-53, Jul. 2010.
[9]梅澤克之, 加藤崇利, 田代卓, “認証済み Cookie 情報の端末間での連携技術の開発と評価,”コンピュータセキュリティシンポジウム(CSS2009)予稿集, pp.81-86, Oct. 2009.
[10] Katsuyuki Umezawa, Takashi Tashiro and Satoru Tezuka, “A Proposal for Federation Technology for authenticated information Between Terminals, ” International Conference on Mobile,

Ubiquitous and Pervasive Computing (ICMUPC 2010), World Academy of Science, Engineering and Technology, Vol. 63, pp.277-284, March. 2010.

[11] 梅澤克之, 手塚悟, “携帯電話を認証情報の保管庫として用いる端末連携認証システムの提案,” 電子情報通信学会 モバイルマルチメディア通信(MoMuC) 技術研究報告 Vol. 110, No.290, pp.73-78, Nov. 2010.

付録

本節で 4.2.3 節で示した公共端末の安全性確認シーケンスの詳細を図示する.

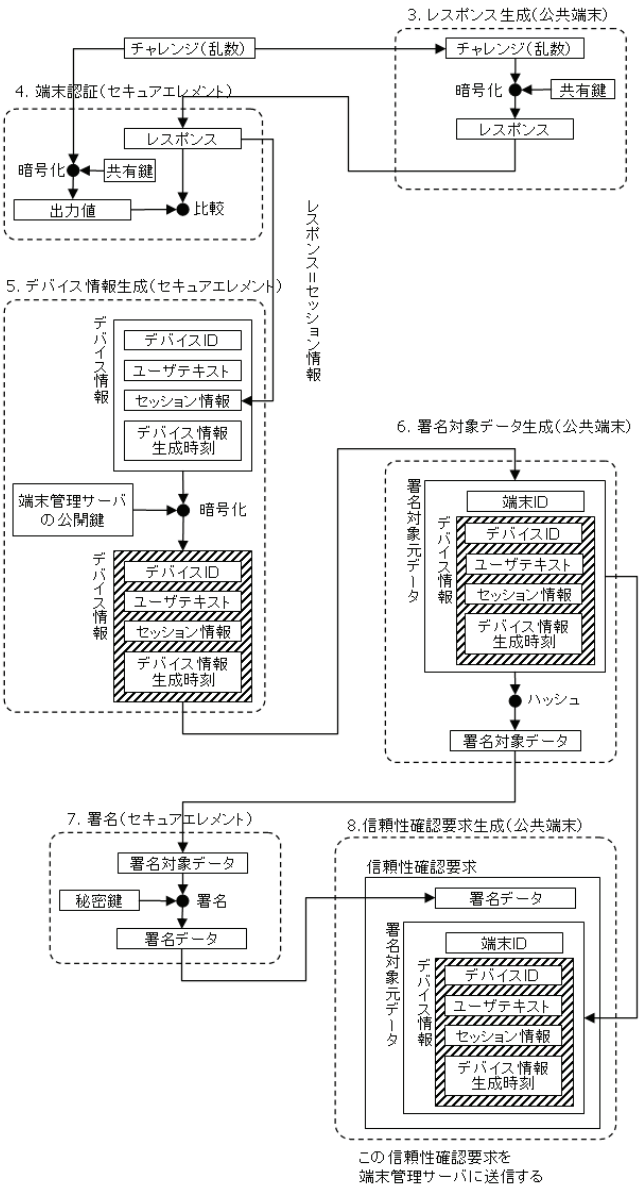

図 10 図 6 のステップ 3 からステップ 8 の詳細

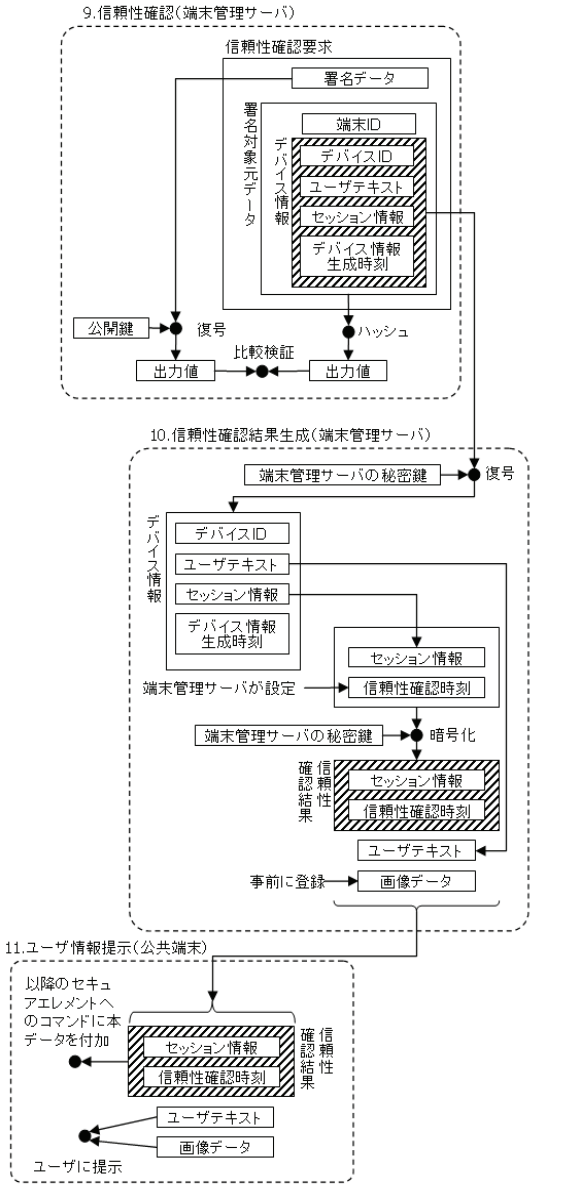

図 11 図 6 のステップ 9 からステップ 11 の詳細