Vol.2011-DPS-147 No.20
Vol.2011-MBL-58 No.20
2011/6/3

端末の信頼性を確保した端末連携認証システムの提案

梅澤 克之[†1] 加藤 崇利[†1]
萱島 信[†1] 手塚 悟[†2]

携帯電話やスマートフォンなどの携帯端末を利用者が持ち歩き，自宅や街中などで利用し業務を遂行するモバイルワークが増えてきている．モバイルワークから帰社後の通常業務（あるいはその逆）に業務体系を切り替える際に，モバイルワーク用の携帯端末を「鍵」として用いて，その携帯端末を他の端末にかざすだけで利用者認証が行えると便利である．さらに外出中には，不特定多数のユーザが利用できる端末（公共端末）が使えればより業務効率の向上が期待できる．本報告では，利用者が外出中に，移動先に設置されている不特定多数のユーザが利用する端末でテレワークを実施する場合に，公共端末の安全性をユーザに担保する技術を提案する．具体的には，公共端末上で利用者が遠隔地のサーバからサービスを受ける際に，端末の安全性が確保されていることを利用者に通知後に公共端末を利用可能にする方式を提案する．

Proposal of federated authentication system with technology that confirms reliability of terminal

Katsuyuki Umezawa,[†1] Takatoshi Kato,[†1]
Makoto Kayashima[†1] and Satoru Tezuka[†2]

Recently, the number of those who do mobile work has increased. Mobile work is to do the business in home and the town by using mobile terminals such as cellular phones and smart phones. It is convenient to be able to do the user authentication only by tapping in other terminals by using the mobile terminal as "Key" when switching to a routine work after the user comes back from outside the company. In addition, if the terminal that many and unspecified users use (public terminal) can be used outside the company, it is more convenient. In this report, we propose the technology that guarantees the user the safety of a public terminal. Concretely, we propose the method to enable the use of the public terminal after the user is notified for the safety of a public terminal to be secured when the user receives service from the server in the remote place with a public terminal.

1. はじめに

近年，ホワイトカラーの生産性を向上させるために，あらかじめ定められた勤務場所以外の場所を中心として業務を遂行するテレワークと呼ばれるワークスタイルが普及してきている．特に，営業職などを中心として，自宅や街中，車中などの場所において，モバイルワークと呼ばれる形態でメールの受発信や書類作成を中心とした勤務を行う利用者が増えている．モバイル業務では，一般的に携帯電話やスマートフォンなどの携帯端末を利用者が持ち歩き，自宅や街中などで利用する．

筆者らは，モバイルワークと帰社後の通常業務を切り替える際に，モバイルワーク用の携帯端末を「鍵」として用いて，携帯端末を他の端末にかざすだけで利用者認証が行える方式を提案してきた．具体的には，認証済みの情報としての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した．

本報告では，上記に記載の端末連携技術に加えて，利用者が外出中に，移動先に設置されている不特定多数のユーザが利用する端末（以降，公共端末と呼ぶ）でテレワークを実施する場合に，公共端末の安全性をユーザに担保する技術を提案する．具体的には，公共端末上で利用者が遠隔地のサーバからサービスを受ける際に，端末の安全性が確保されていることを利用者に通知後に公共端末を利用可能にする方式を提案する．

以下では，まず，2章で関連技術を示し，3章で提案方式を示す．4章で安全性に関する考察を行い，5章でまとめと今後の課題を示す．

2. 関連研究

2.1 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[1)2)3)4)]．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

†1 日立製作所 横浜研究所
Hitachi, Ltd. Yokohama Research Laboratory
†2 東京工科大学 コンピュータサイエンス学部
School of Computer Science, Tech. of Tokyo Univ.

© 2011 Information Processing Society of Japan

Vol.2011-DPS-147 No.20
Vol.2011-MBL-58 No.20
2011/6/3

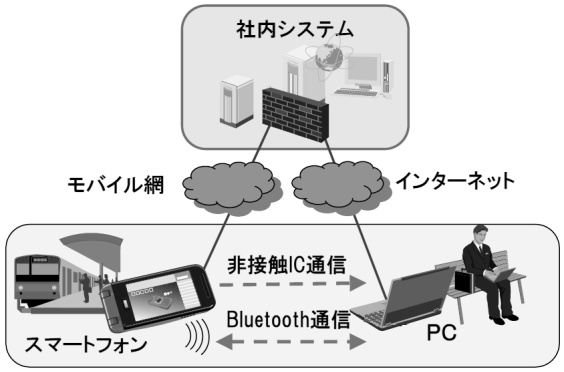

図 1　携帯端末を用いたリモートアクセス技術の概要

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[5)6)7)8)]．

携帯端末を用いたリモートアクセス技術の概要を図 1 に示す．まず，ユーザが，駅のホームなど PC を広げられない時には携帯端末を単体で用いて社内システムにログインし，認証を受けた後に業務を行う．その後，PC を広げられる状況になった場合には，携帯端末を PC にかざすだけで，事前に携帯端末単体で受けている認証済み情報を PC 側に転送することで，再度認証処理を行うことなく業務を再開できるという技術である．

3. 提 案 方 式

本節で提案方式を述べる．

3.1 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 2 に全体概要を示す．

図 2 に示すように，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ことを想定する．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

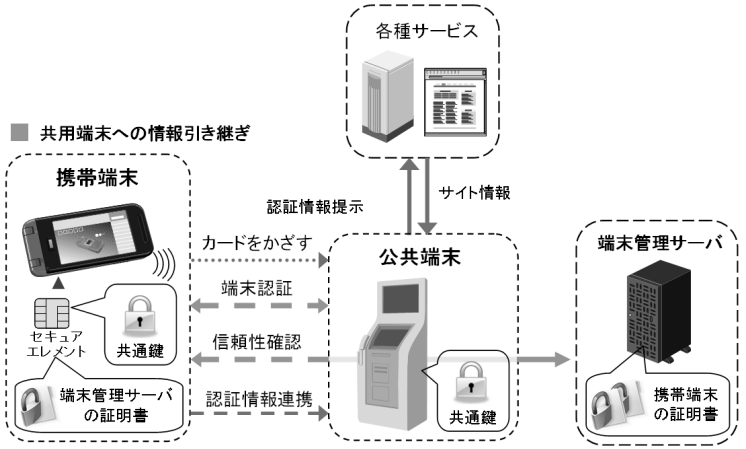

図 2　提案システムの全体概要

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．

ただし，図 2 に示したような公共端末を利用する前に，ユーザは社内の PC 端末と連携してサービスを受けるか，あるいは携帯端末単体でサービスを受けるかのどちらかを行い，サービス提供サーバ側から認証済情報として発行された Cookie 情報が携帯端末内に保管されているものとする．

3.2 提案方式のシーケンス

本節では前節で示した公共端末の利用シーンについて，シーケンスを示す．

3.2.1 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 3 に，その説明を表 1 に示す．

3.2.2 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 4 に，その説明を表 2 に示す．

3.3 公共端末の安全性確保処理の詳細シーケンス

本節で 3.2.1 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 3 のステップ 3〜ステップ 8 までの詳細を図 5 に，その説明を表 3 に示す．また，図 3 のステップ 9〜ステップ 11 までの詳細を図 6 に，その説明を表 4 に示す．

© 2011 Information Processing Society of Japan

Vol.2011-DPS-147 No.20
Vol.2011-MBL-58 No.20
2011/6/3

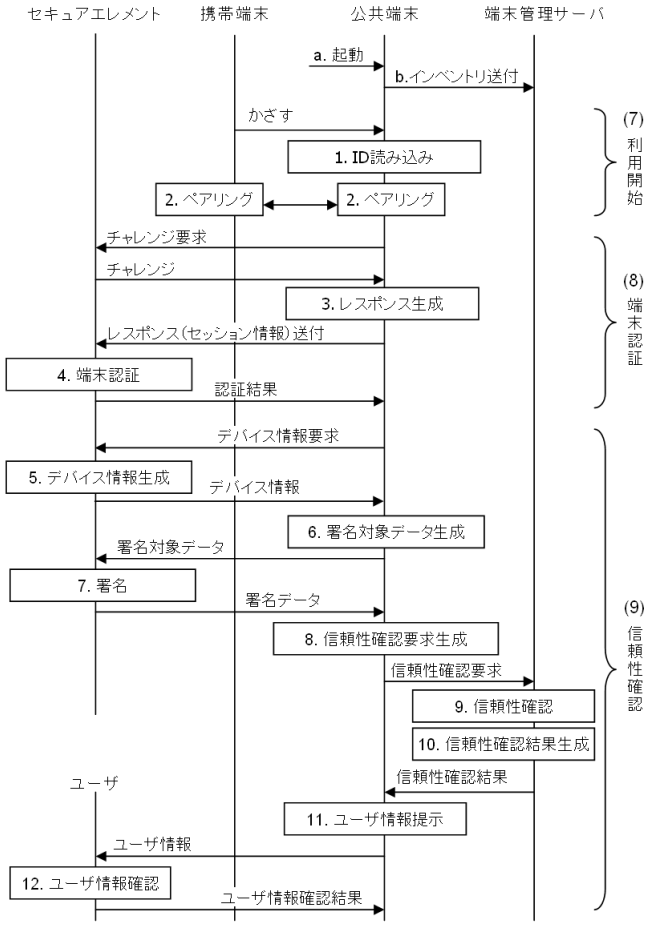

図 3 公共端末の安全性確認のシーケンス

表 1 図 3 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 Bluetooth のペアリングを行う
3〜4	端末認証を行う（詳細は，3.3 節を参照）
5〜11	端末の信頼性確認を行う（詳細は，3.3 節を参照）
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

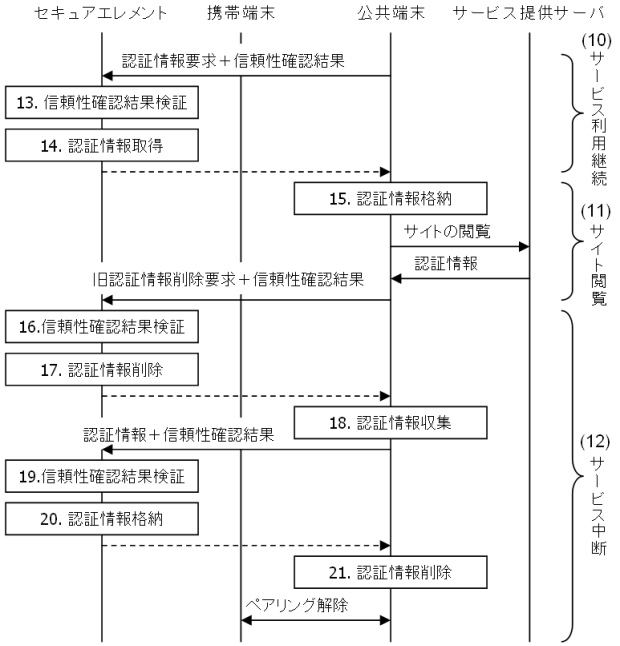

図 4 公共端末利用のシーケンス

© 2011 Information Processing Society of Japan

Vol.2011-DPS-147 No.20
Vol.2011-MBL-58 No.20
2011/6/3

表 **2**　図 4 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
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	セキュアエレメントは，公共端末からの旧認証情報削除要に対して，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	セキュアエレメントは，公共端末からの認証情報格納要求に対して，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

表 **3**　図 5 の説明

No.	説明
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
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
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

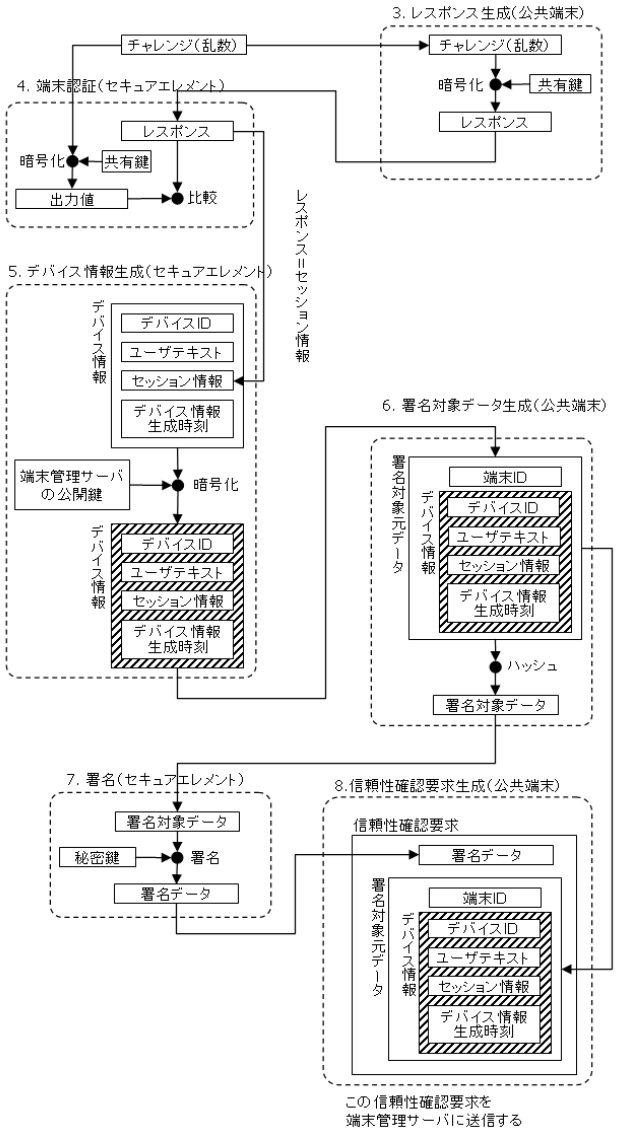

図 **5**　図 3 のステップ 3 からステップ 8 の詳細

© 2011 Information Processing Society of Japan

Vol.2011-DPS-147 No.20
Vol.2011-MBL-58 No.20
2011/6/3

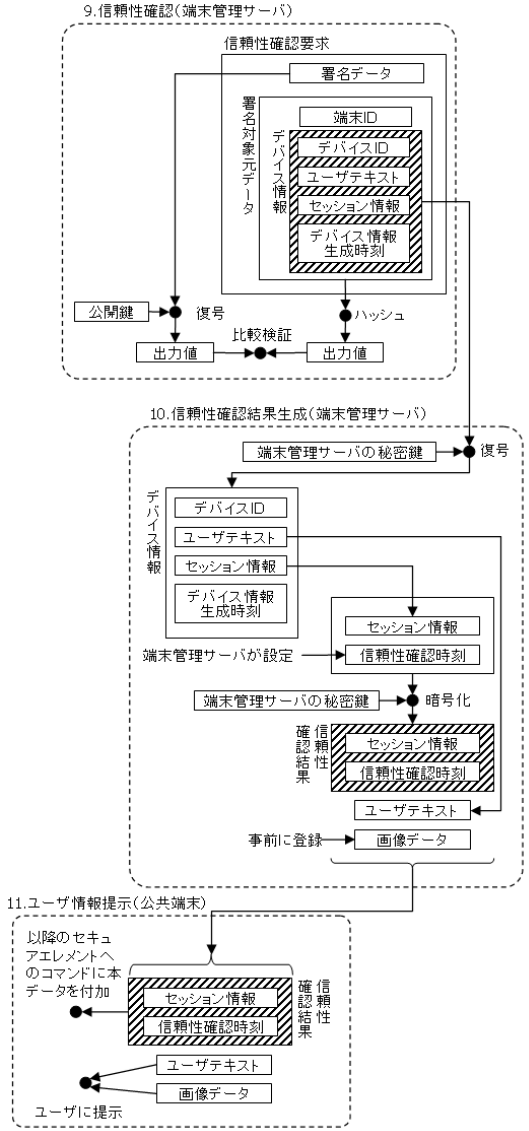

図 6 図 3 のステップ 9 からステップ 11 の詳細

表 4 図 6 の説明

No.	説明
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

3.4 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 7 に示す．

図 7 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
- **Felic** 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 7 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

© 2011 Information Processing Society of Japan

Vol.2011-DPS-147 No.20
Vol.2011-MBL-58 No.20
2011/6/3

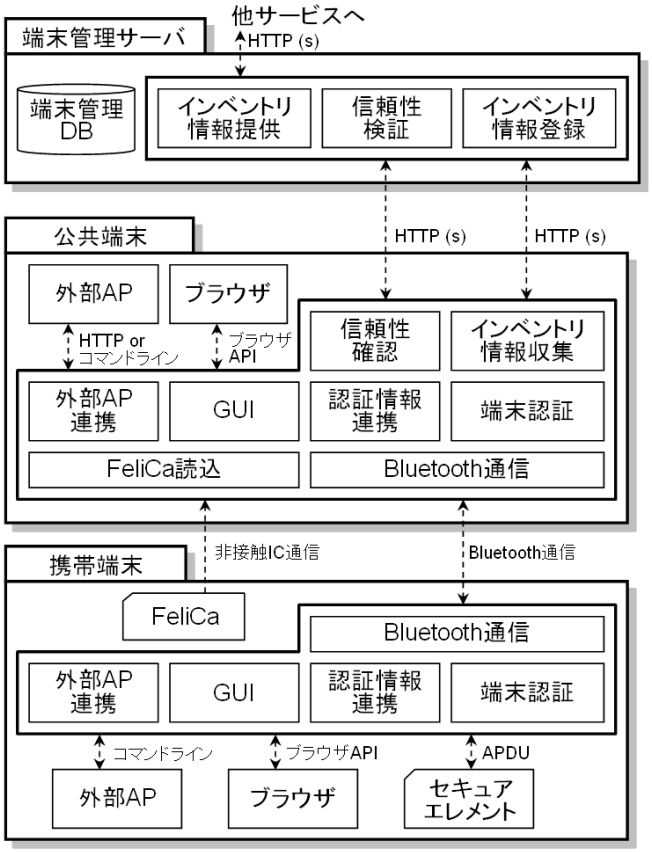

図 7　提案方式のモジュール構成

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

また，図 7 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

4. 提案方式の妥当性検証

図 2 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．

4.1 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．

4.1.1 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．

© 2011 Information Processing Society of Japan

Vol.2011-DPS-147 No.20
Vol.2011-MBL-58 No.20
2011/6/3

4.1.2 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．

4.2 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．

4.2.1 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確保モジュールに対し，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．

4.2.2 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．また，信頼性確保モジュールは，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．
- 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．

5. お わ り に

本報告では，利用者が外出中に，移動先に設置されている不特定多数のユーザが利用する公共端末でテレワークを実施する場合に，公共端末の安全性をユーザに担保する技術の提案を行った．具体的には，公共端末上で利用者が遠隔地のサーバからサービスを受ける際に，端末の安全性が確保されていることを利用者に通知後に公共端末を利用可能にする方式を提案した．今後は，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．

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．

商標等に関する表示

- Bluetooth は，Bluetooth-SIG Inc. の登録商標です．
- FeliCa は，ソニー株式会社の登録商標です．

参 考 文 献

1) 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.
2) 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.
3) 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.
4) 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.
5) 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 技術研究報告　Vol. 110, No.113, pp.47-53, Jul. 2010.
6) 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.
7) 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.
8) 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 技術研究報告　Vol. 110, No.290, pp.73-78, Nov. 2010.

© 2011 Information Processing Society of Japan