2Z-5

クライアント証明書のマルチデバイス認証方式の提案

加藤　大樹 †　　星　徹 †　　手塚　悟 †

東京工科大学　コンピュータサイエンス学部†

1．背景

今日，スマートホンの普及により，SNS を代表とする様々な Web サービスが提供されている．その数は膨大で，情報処理推進機構(IPA)が推奨するような，サービス個々で異なった ID・パスワードをユーザーが管理する事は困難になりつつある．また，ID・パスワードでの認証はビッグデータ解析による予測[1]や入力の際の覗き見，コンピューターの高性能化によるブルートフォースアッタクなど様々な脅威にさらされている．その為，ID・パスワードに依存しない認証方式が必要である．近年，Public Key Infrastructure(PKI)技術をベースとした，クライアント証明書を，ID・パスワードの代わりとしてサービスを利用する研究が，モバイル端末を対象に進められている[2]．具体的には，電子証明書の秘密鍵を，耐タンパ性の高い IC チップ内に格納し，電子署名をすることで，本人である事が保証される．

その一方，サービス提供者側のマルチデバイス化対応が進み，一つのサービスに於いて，OS の種類や PC，モバイルを問わず様々なデバイスの利用が出来るように整備されてきている．こうした中で，一人のユーザーが複数の端末を所有して同一のサービスを利用できる環境構築がクライアント証明書ベースに於いて必要とされている．

2．目的

Universal Subscriber Identity Module Card (USIM)カード搭載端末を中心とし，同一ユーザーが所有している他端末を，この USIM カード搭載端末に紐づけする事を行う．初めに，USIM カードの中にクライアント証明書の秘密鍵を格納する．クライアント証明書ベースでサービスに登録後，同一ユーザーが所有する他端末でそのサービスのアクセスを可能とする事を目的とする．

Client certificates for multi devices

Daiki Kato †　Tohru Hoshi †　Satoru Tezuka †

†School of Computer Science，Tokyo University of Technology

1401-1 Katakuramachi, Hachiouji, Tokyo 192-0982, Japan

つまり，サービス側が既に登録した端末のクライアント証明書を，そのユーザーの身分証として要求することで，同一ユーザーの所有端末であると紐づけ可能とする．このようにする事で，他の端末は別のクライアント証明書が実装されているかにも関わらず，自身の所有する端末であることを認証出来る．

3．研究内容

本研究では，仮想環境上に SQL サーバーを構築し，仮想サービスの会員登録ページを作成する．USIM カードにクライアント証明書の秘密鍵が格納された携帯端末から，この仮想サービスへクライアント証明書を認証の鍵として登録を行う．その後，別の端末から同一ユーザーとしてログイン出来るように，新たに登録する端末を，既に登録されている端末とで紐付け処理を行う．そのシステムの構成図を図 1 に示す．

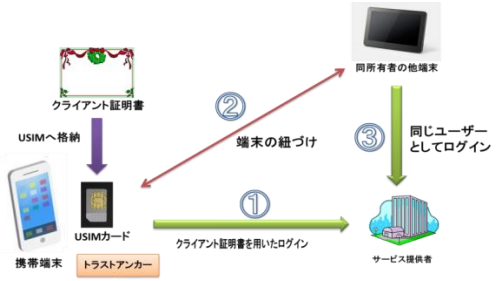

図 1：システム構成図

クライアント証明書を所有している端末は，同一ユーザーが所有する他端末がサービスへ紐付されるときのトラストアンカーとして用いる．図 2 に示す通り，USIM カードを搭載していない端末の機器登録番号をトラストアンカーが集中して管理し，所有端末のリストが記述されたテーブルを作成する．

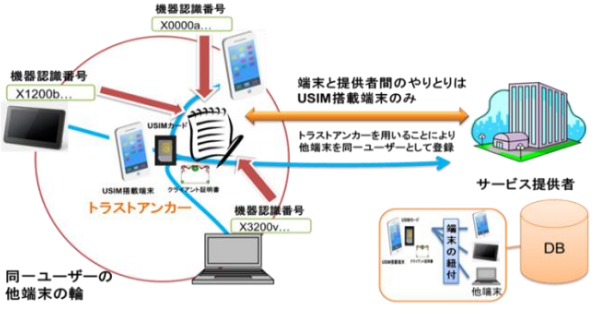

図 2：トラストアンカーを用いた端末追加の概要

そのリストをセキュアな通信経路でサービス提供者へ送信，DB 上での紐付け登録を行う．紐付け登録された端末は，機器認証番号をサービス提供者へ通知することにより，従来の ID，パスワードを手動で入力することなく，ログイン出来るようになる．その概要を図 3 に示す．

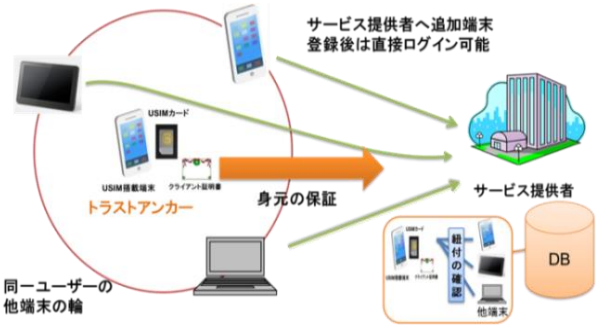

図 3：端末の紐付け後のログイン概要

4. 提案手法

研究内容で記述した機器認証番号は，ID,パスワードを用いたログインに於ける,ID に相当するものである.ID とは自身が世界の誰であるのかを申告するものであり，申告が確かなものであると証明するパスワードに相当するものが必要である．そこで，本研究では，トラストアンカーが電子署名を行い，身分を証明出来る点に着目する．

図 4 にトラストアンカーを用いたセキュアなログイン方法を示す．尚，ここでは Kp を公開鍵，Ks を秘密鍵とする．更に，USIM 搭載端末の鍵は Kp1，Ks1 とし，サービス提供者の鍵は Kp2，Ks2 とする．

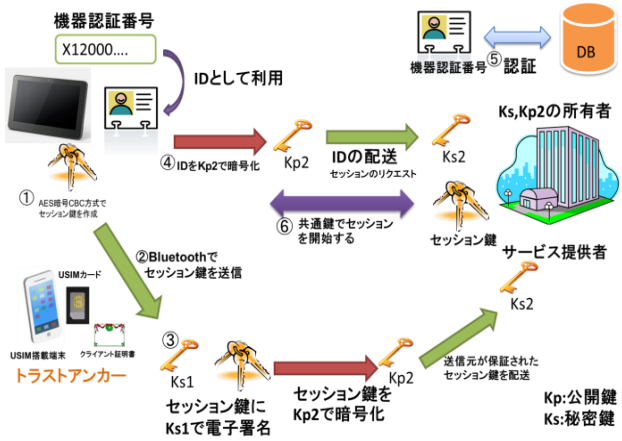

図 4：トラストアンカーを用いたセキュアなログイン

① ログインの実施を行う端末にて Advanced Encryption Standard (AES)暗号方式でセッション鍵を生成.

② セッション鍵を Bluetooth 経由で USIM 搭載端末へ送信.

③ USIM 搭載端末でセッション鍵を復号した後，Ks1 で電子署名を行って，Kp2 で暗号化を実施しサービス提供者へ送信.

④ 機器認証番号を ID として Kp2 で暗号化しサービス提供者へ送信.

⑤ サービス提供者は機器認識番号を DB 上で照会し紐付している USIM 端末からセッション鍵が送信されているかを確認.

⑥ それぞれの有効性が確認された場合，送信された共通鍵でセッションを開始.

トラストアンカーがセッション開始時に，電子署名を行える状況下でなければならないが，これらの手順を踏むことにより，セキュアにログインを行うことが可能となる.

5. まとめ

今後，益々スマートホンのようなモバイル端末が個人の所有する通信端末の中心となってくることが予想される．昨今の Bring Your Own Device (BYOD)問題のように，今まで以上に個人情報や業務内容などを携帯端末で取り扱うようになれば，攻撃の対象もモバイル端末に集中的に集まるようになる．個人の端末は，各々が自覚を持ってセキュリティ対策を行っていく必要があるが，一般ユーザーに於けるコンピュータリテラシーの問題により，セキュリティに対する高度な対策が困難な場合も多い．そうした中で，モバイル PKI を利用したセキュリティ対策が今後普及し，コストや端末の制約の問題が発生した際に，本研究が活かされることを望む．今後は，実際に環境を構築したうえで，トラストアンカーが圏外になってしまったときの対処方なども，課題として解決していきたい.

参考文献

[1]萩原 栄幸(2013)「内部犯罪防止策とサイバー攻撃防御における共通点」pp17-20 第 27 回全国大会研究報告書

[2]梅沢 克之,手塚 悟(2011)「スマートホ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」pp530-538 電子情報通信学会論文誌 B Vol.J94-B