Java Cardを用いた 機密ファイル閲覧管理の提案*

川口信隆　宮地玲奈　小宅宏明　重野寛　岡田謙一　†
慶應義塾大学理工学部‡

1　はじめに

近年，電子化された機密情報の組織からの漏洩が大きな社会問題となっている．そして，その大多数は組織内部関係者による犯行である．
内部関係者は，元々組織情報へのアクセスが認められている為，外部の人間に比べて情報を容易に漏洩することができる．このため，機密情報へアクセスする際には，システムとして制約を加えることにより，情報が外部へ漏洩することを防ぐ必要がある．
本研究では，Java Cardを用いた機密ファイル閲覧管理を提案する．耐タンパ性を持つICカードであるJava Card[1]を用いて「場所の認証」を行うことにより，組織外でのファイル閲覧を防止する．又，鍵やファイルのアクセスコントロール情報をカード内に封入することにより安全なアクセスコントロール環境を実現する．

2　既存技術とその問題点

2.1　機密情報漏洩防止のためのシステム

機密情報漏洩防止のためのシステムは多くのベンダーが開発を行っている．このようなシステムでは，ファイルのコピーや印刷を禁止することにより外部への漏洩を防止する．しかし，どのシステムにおいても，閲覧するユーザの「場所の認証」は行われていない．このため，ユーザ自身が認証されれば，本来組織内でのみ閲覧を許されるようなファイルを組織外で閲覧することが出来てしまうという問題がある．

2.2　場所の認証

場所の認証はDebbie Caswell.el[2]が，BlueToothを用いた認証方法を提案している．認証では，システムが，BlueToothを用いて秘密情報を送信して，認証を望む端末はそれを受信し，システムに返信する．BlueToothでは電波の到達範囲が100 m以内と限定されている為，情報を返信できる端末はシステムの近傍に存在すると考え，認証することが出来る．しかし，秘密情報の伝送路が電波であるため，システムの近傍にリダイレクターを設置し，情報を遠隔地へのリダイレクトが可能であるという問題がある．

3　提案

本稿では，Java Cardを用いた機密ファイル閲覧の管理を提案する．JavaCardを用いて，場所の認証と，アクセスコントロールを行うことにより，安全な閲覧環境を実現する．

3.1　構成要素

本システムは, 以下の要素により構成される．

- **閲覧ソフト** ファイルの閲覧，認証サーバ，Java Cardとの通信を行う．カードの共有鍵を持つ．
- **Java Card** 認証サーバ，閲覧ソフトとの通信を行う．又,「場所」と「その場所におけるアクセス権限」をマッピングしたアクセスコントロールリストを持ち，ユーザの場所とファイルのアクセス権限から，閲覧の可否を判定する．ファイルヘッダ復号化のための秘密鍵，閲覧ソフト，認証サーバ, 部屋サーバとの共有鍵を持つ．
- **認証サーバ** Java Card, 部屋サーバと通信し，場所の認証を行う．Java Card, 部屋サーバとの共有鍵を持つ．
- **部屋サーバ** 組織の各部屋に配置され，3節で述べるウォーキング認証を行う．認証サーバ, 部屋サーバとの共有鍵を持つ．

3.2　ファイル閲覧までの手順

3.2.1　機密ファイルの作成

機密ファイル作成者は，共有鍵を作成し，それを用いてファイル本文を暗号化する．次に，ファイルのアクセスレベルを示すタグを作り，タグと共有鍵を合わせてヘッダとする．最後にヘッダをJava Cardの公開鍵を用いて暗号化する．そして，暗号化されたファイル本文とヘッダをまとめて，配布する．

*Browsing Management of Confidencial Files Using Java Card
†Nobutaka Kawaguchi, Reina Miyaji, Hiroaki Ohya, Hiroshi Shigeno, Kenichi Okada
‡Faculty of Science and Technology, Keio University

3.2.2 機密ファイルの閲覧

機密ファイルの閲覧は，以下の手順で行われる．尚，閲覧したいファイルは予め用意してあり，ユーザ端末にJava Card が挿入されていてる．又，通信路は適切に暗号化されている．閲覧までのプロセスを図 1 に示す．

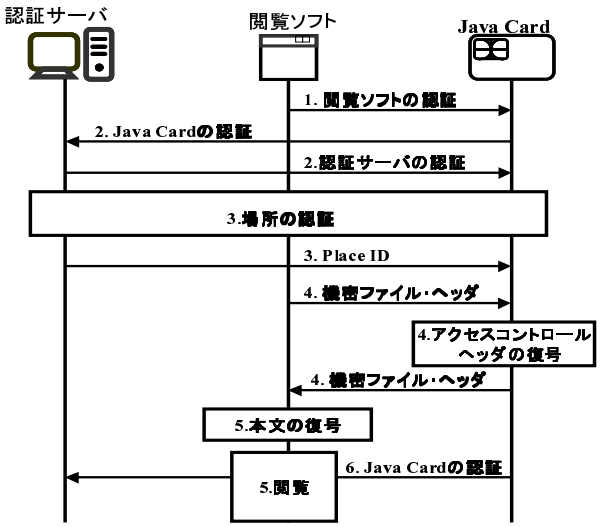

図 1: 閲覧までのプロセス

1. 閲覧ソフトは，JavaCard に対して認証を行う．
2. JavaCard は閲覧ソフトを介して認証サーバと相互認証を行う．
3. 認証サーバは，「場所の認証」を行う．認証後に，ユーザ端末の場所を示す PlaceID を JavaCard に対して発行する．
4. 閲覧ソフトは，閲覧したい機密ファイルのヘッダを Java Card に渡す．Java Card はアクセスコントロールを行い，閲覧が許可される場合，カードの秘密鍵でヘッダを復号化し，閲覧ソフトに送る．
5. 閲覧ソフトは，ヘッダに含まれる鍵を用いてファイル本文を復号化し，閲覧する．
6. 閲覧中，認証サーバに対してカードは定期的に認証を行う．これは，閲覧中に端末がネットワークから切断され，遠隔地へ移動されることを防ぐためである．

場所の認証については次節以降で述べる．

3.3 CPU ID 認証

CPU ID 認証は PSN(Processor Serial Number)[3] を用いて，場所の認証を行う．PSN は CPU ごとに固有のシリアルナンバーである．認証サーバは，各 CPU の PSN と，CPU が入っている端末の場所とのテーブルを保持している．このため，閲覧ソフトが，自身が動作している端末の PSN を申告することにより，ユーザの場所を認証することが出来る．しかし，ノート PC 等のモバイル環境では使用できないという問題点がある．

3.4 ウォーキング認証

ウォーキング認証では，端末が自身の位置を認証サーバに申告する．認証サーバは申告された場所を管轄する部屋サーバに対してパスフレーズを送信する．ユーザは Java Card を携帯して部屋サーバに徒歩で赴き，パスフレーズをカードに入力した後，端末へ戻る．端末に戻ったユーザはカードを挿し，パスフレーズを認証サーバに送信する．認証サーバではパスフレーズを照合すると同時に，部屋サーバでカードを抜いてからパスフレーズを送信するまでの時間を調べ，これが閾値以内ならば認証を行う．この方法では，伝送路として「人間」を用いるため，遠隔地へのリダイレクトを防ぐことが出来る．CPU ID 認証では不可能だったモバイル環境を認証することが可能である反面，人間に負担がかかる，位置を CPU ID 認証ほど正確に判定することが出来ないという問題がある．このため，本提案では，端末がデスクトップのときは CPU ID 認証を用い，モバイル環境のときはウォーキング認証を用いることとする．

4 まとめ

本研究では，Java Card を用いた機密ファイル閲覧管理を提案した．Java Card を用いることにより，「場所の認証」を行い，安全なアクセスコントロール環境を実現することが出来た．

5 謝辞

本研究は ASF(応用セキュリティフォーラム) に支援された．

参考文献

[1] Sun Microsystems,"Java Card Technology" http://java.sun.com/products/javacard/index.html

[2] Debbie Caswell & Philippe Debaty(2000) "Creating web representations for places" Proceedings Handheld and Ubiquitous Computing 2000, Springer, pp. 114-126.

[3] intel,"Processor Serial Number Overview" http://www.intel.com/support/processors/pentiumiii/psu.htm