「場所の認証」を用いた機密ファイル閲覧システムの提案

川口 信隆* 宮地 玲奈* 重野 寛* 岡田 謙一*

近年，組織関係者による機密情報の漏洩が増加してきている．本稿では，場所の認証を用いた機密ファイル閲覧システムを提案する．本システムでは閲覧者の場所を認証し，場所に応じて閲覧可能な機密ファイルを制限することにより，情報漏洩を防止する．

A Proposal of Confidential File Viewing System Using Location Authentication

Nobutaka KAWAGUCHI* Reina MIYAJI*
Hiroshi SHIGENO* Kenichi OKADA*

Recently, there are many leakages of confidential information by insiders of an organization. In this paper, we propose a confidential file viewing system using location authentication. The system prevents information leakages by regulating files that a user can view according to the location of the user.

1 はじめに

近年，組織の情報管理・運用の電子化に従い，「組織関係者による電子化された機密情報の漏洩」が増加してきている．

既存の機密情報漏洩防止技術の多くは組織部外者を対象としている．これらの技術では予め許可されたユーザに限り情報へのアクセスを認める．しかし，組織関係者は，予め機密情報へのアクセスが許可されていることが多いため，このような対策のみでは不十分である．このため漏洩防止策として，機密情報閲覧者が漏洩が困難となるようなコンテキスト（状況）に存在する場合に限り，閲覧を許可するようにするという方法が考えられる．

本稿ではコンテキストの中でも特に「閲覧場所」を用いた機密ファイル閲覧システムを提案する．機密情報の閲覧場所を規定することにより，漏洩を試みる者には規定された場所に赴かなければならないというリスクが生じ，また情報漏洩が起こりうる場所が限定されるため様々な対策を重点的，効率的に行うことが可能となる．本稿では場所の認証手法として，ウォーキング認証を提案する．ウォーキング認証では，人間が徒歩で移動できる距離は移動時間に比例し，短時間に遠隔地へ移動することは出来ないという性質に注目する。そして，ある規定された場所とユーザが認証を行いたい場所との間を徒歩で移動する際にかかる時間をもとに認証を行う．この手法では既存の場所の認証手法の問題点であった，リダイレクターによって認証情報を送信することによる遠隔地からの不正認証を防ぐことが可能となる。そしてウォーキング認証の有効性を確認し，場所の認証，場所に基づくアクセスコントロールを行うために機密ファイル閲覧システムを設計し評価を行う．

以下，第2章では電子化された機密情報の問題点，場所の認証手法について概観し，その問題点について議論する．第3章ではウォーキング認証を提案する．第4章ではウォーキング認証を用いた機密ファイル閲覧システムを提案し，第5章で実装と評価実験について述べ，第6章を本稿のまとめとする．

2 電子化された機密情報の問題点と場所の認証

2.1 電子化された機密情報の問題点

電子化された機密情報（以下，機密ファイルと呼ぶ）の漏洩防止には，暗号化や認証といった技

* 慶應義塾大学 理工学部 情報工学科
Department of Instrumentation(Information), Faculty of Science and Technology, Keio University

術が用いられてきた．これらは，組織に予め許可されたユーザにのみ機密ファイルを閲覧を許可することにより漏洩を防止する．しかし，組織関係者は元々機密ファイルの閲覧を許可されているので，これらの対策のみでは不十分である．

既存の組織関係者による機密情報漏洩防止策 [1] では，機密ファイルを閲覧する端末に専用ソフトウェアをインストールして，機密ファイル閲覧時のコピー&ペースト，画面のキャプチャー，電子メールへの添付やプリントアウトの禁止等の OS の制御を行う．この手法は，機密ファイルが閲覧の行われる端末の外に漏れないことを保証することにより機密情報の漏洩防止を実現する．しかしノート PC 等のモバイル端末にこの手法を適用した場合，端末自体を組織の監視の目が行き届かない遠隔地に持ち出し，ファイルを閲覧したり部外者に対して公開するなどによる情報漏洩が起きる可能性がある．

組織関係者による情報漏洩の防止策としては，「ユーザが置かれているコンテキスト（状況）の認証を行い，情報漏洩が困難であるようにコンテキストにユーザがいた場合に限り情報の閲覧を許可する」という手法が考えられる．本稿では，このコンテキストとして特に「場所」に注目する．機密ファイルを閲覧する場所を認証するという手法は

- **守るべき領域の限定** 閲覧場所を限定できれば，漏洩防止の労力や費用を集中的に，その場所にかけることができる．
- **漏洩者のリスクの増大** 閲覧の度に規定された場所に赴かなければならないため，漏洩者にとって多くの証拠を残すというリスクが生じる．

という２点の理由で機密情報の漏洩防止に対して有効であるといえる．

2.2 場所の認証

場所の認証手法は，「絶対位置による認証」，「相対位置による認証」の２種類に分類することができる．

絶対位置による認証では，認証の対象者である認証ユーザの絶対的座標上での位置を認証する．「IP アドレスによる認証」では，送信される IP アドレスから送信者の位置を決定するが IP アドレススプーフィングなどの問題点がある．CyberLocator 社は「GPS を用いた認証手法」 [2] を提案している．この手法では，衛星から送られてくる認証ユーザの位置情報を元に認証を行う．しかし認証ユーザが衛星に成りすまし任意の位置情報を作成することが可能であるという問題がある．

相対位置による認証では，認証ユーザと認証サーバとの相対距離を認証する．S. Brands は「伝送遅延を用いた認証手法」 [3] を提案している．しかし実際に物理的な位置と伝送遅延時間を正確にマッピングすることは困難である．Tim Kinderg 等は，「Bluetooth を用いた認証手法」 [4] を提案している．この手法では認証サーバが電波到達範囲が 10 m と限られた Bluetooth を用いてパスフレーズを認証ユーザに送信することでサーバの近傍に存在することを認証する．しかし認証サーバの近傍にリダイレクターを設置し，遠隔地にパスフレーズを転送することで近傍に存在するように振舞うことができるという問題がある．

3 ウォーキング認証

本章ではウォーキング認証を提案する．ウォーキング認証は相対位置による場所の認証である。ウォーキング認証では，「人間がある時間以内に移動できる距離は移動時間に比例し短時間に遠隔地へ移動することはできない」という性質を利用する．前章で述べた通り，既存の認証手法には遠隔地からの不正認証の可能性があった．これは，認証情報をリダイレクトが容易である電波を用いて運んでいたためである．そこでウォーキング認証では，ある規定された場所と，ユーザが認証を行いたい場所との間で認証情報を運ぶ媒体として人間を用いることによりこの問題を解決し，より信頼性の高い認証を行う．

3.1 認証手法

ある規定された場所を認証中心地点とする．認証中心地点には場所サーバが存在する．次に認証中心地点の近傍となる一定範囲を規定し，認証近傍範囲と定義する．このとき認証ユーザと認証ユーザが使用している認証端末が存在する場所（以下，認証対象地点と呼ぶ）が認証近傍範囲に存在することを認証する．図 1 に認証の手順を示す．

1. 認証ユーザはトークンを携帯し場所サーバへ赴く．そして場所サーバから認証情報を取得

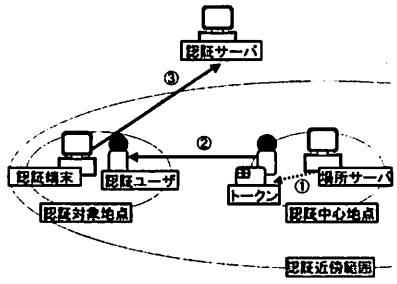

図 1: ウォーキング認証

しトークンに入れる．この認証情報は，場所サーバごとに固有なパラメータと有効期限を持っている．

2. 認証情報の入力後，認証ユーザはトークンを携帯して，認証端末が存在する認証対象地点に徒歩で赴く．
3. 認証ユーザはトークンを認証端末に挿入する．認証端末はトークンから認証情報を読み込み，認証サーバへ送信する．認証サーバは，認証情報が送信された時刻が有効期限以内であるとき，認証対象地点は認証近傍範囲内に存在すると認証する．

認証情報はトークンに保存され，トークンは人間により運ばれる．このとき，トークンから認証情報を引き出すことができるのは認証対象地点に存在する認証端末のみであるようにする．これにより，認証情報が認証中心地点から認証対象地点への移動中に遠隔地へ送信されることを防止する．このため，認証中心地点から認証対象地点への移動時間から，両地点の距離を推測することが可能となる．そして認証中心地点から認証近傍範囲の末端への徒歩での移動時間を推定しこれを認証限界時間とする．認証情報の有効期限は，認証情報の発行時間から認証限界時間だけ経過した時刻となる．

3.2 トークンに求められる要件

認証情報を格納するトークンには「情報を場所サーバから入力し，許可された認証端末以外に格納した情報を公開しない」ことが求められる．このためトークンは耐タンパ性を備え，さらに認証端末を認証するための機能（暗号化など）を実装する必要がある．このためトークンとしては，暗号化機能を持ったICカード等の使用が考えられる．

4 「場所の認証」を用いた機密ファイル閲覧システムの設計

本章では，第3章で提案したウォーキング認証を利用した機密ファイル閲覧システムの設計について述べる．

4.1 システムデザイン

本章で設計する機密ファイル閲覧システムでは，機密ファイル閲覧者が使用している閲覧端末の存在する場所をウォーキング認証を用いて認証し，場所に応じた，閲覧可能な機密ファイルのアクセスコントロールを実現する．

4.1.1 閲覧システムの構成

閲覧システムの構成要素を図2に示し以下に説明する．

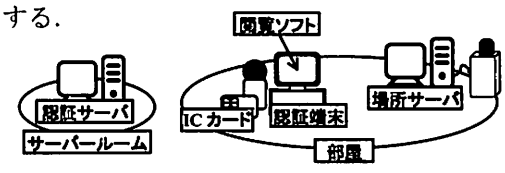

図 2: システム構成

- **閲覧ソフト** 認証端末にインストールされ機密ファイルの閲覧，認証サーバ，ICカードとの通信を行う．
- **ICカード** ファイル閲覧者のユーザ情報を格納する．認証サーバ，閲覧ソフトとの通信を行う．又，閲覧場所に応じて機密ファイルの閲覧のアクセスコントロールを行う．暗号化された機密ファイルを復号するための秘密鍵を保持する．
- **認証サーバ** サーバルームに設置され，ICカード，部屋サーバと通信し，ウォーキング認証を行う．
- **場所サーバ** 組織の各部屋に設置され，ウォーキング認証の際に用いられる．

以上の構成の下で，システムは動作する．

4.1.2 想定条件

閲覧システムは，以下に挙げる想定条件の下で設計される．

- 機密ファイルを閲覧する端末は組織により管理されるデスクトップPC，モバイルPCである．一般の組織関係者が不正に端末を改変したり，許可されていないソフトウェア等を端末上で利用することはできないものとする．

- 閲覧ソフトは改ざんなどを受けず，安全に正しく動作するものとする．

- ICカードが挿入されるカードリーダは認証端末に物理的に密着しておりカードと端末間の情報を通信路上で取得してリダイレクトすることは不可能であるとする．

4.1.3 機密ファイル閲覧までの流れ

機密ファイル閲覧までの流れを以下に示す．

1. 機密ファイル作成フェーズ
2. 機密ファイル閲覧フェーズ

機密ファイル作成フェーズではファイル本文を元に，機密ファイルを作成する．作成された機密ファイルは任意の手段で配布される．機密ファイル閲覧フェーズでは，ユーザは場所の認証，場所に基づく閲覧のアクセスコントロールを経てファイルを閲覧する．

4.2 機密ファイル作成フェーズ

機密ファイルは，ファイル本文とファイルヘッダから構成される．ファイルヘッダは乱数部とアクセス権限部から構成される．乱数部は数百ビットの乱数であり，アクセス権限部は機密ファイルのファイルアクセス権限レベルを示す．ファイルアクセス権限レベルは機密ファイルの重要度を示し，このレベルが高いほど重要なファイルとなる．機密ファイルの作成手順を以下に示す．

1. ヘッダを暗号鍵として，ファイル本文全体を暗号化する．
2. ICカードが保持する秘密鍵に対応する公開鍵でヘッダ全体を暗号化する．

機密ファイルを復号化するには，ICカード内の秘密鍵を用いる必要がある．ICカードはアクセスコントロールの結果，閲覧が許可された場合に限りファイルヘッダの復号化を行う．

4.3 機密ファイル閲覧フェーズ

機密ファイルの閲覧は，図3に示される手順で行われる．尚，各通信路は適切に暗号化されているものとする．

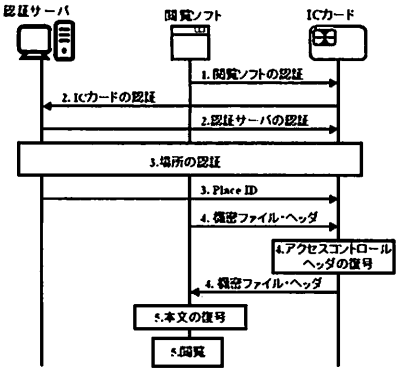

図 3: 閲覧までのプロセス

1. ICカードは閲覧ソフトの認証を行う．
2. ICカード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，認証端末の場所を示すPlaceIDをICカードに対して送信する．
4. 閲覧ソフトは，閲覧したい機密ファイルのヘッダをICカードに渡す．ICカードは，ヘッダとPlaceIDを用いて閲覧のアクセスコントロールを行う．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，閲覧ソフトに送信する．
5. 閲覧ソフトは，ICカードから送られてきたヘッダに含まれる鍵を用いてファイル本文を復号化し，ユーザはファイルを閲覧をする．ファイル閲覧中，ICカードと認証サーバは定期的に相互認証を行う．これは，閲覧中に端末をネットワークから切り離し組織外へ持ち出すことを防ぐためである．

場所の認証，アクセスコントロールについては次節以降で述べる．

4.4 場所の認証

本システムでは，ウォーキング認証での認証近傍範囲を「部屋内」とする．これは，通常機密情報の閲覧の可否は部屋単位で決められることが多いからである．このときの限界認証時間の適切な値については評価の章で議論する．

4.5 場所に基づくアクセスコントロール

IC カードは，カード内に保管されているアクセスコントロールリストと認証サーバから受信した PlaceID と閲覧ソフトから受信した機密ファイルヘッダを用いて，図 4 の例に示されるような機密ファイル閲覧のアクセスコントロールを行う．

まず最初に，PlaceID とアクセスコントロールリストから，PlaceID が示す場所（図 4 では社長室) におけるユーザアクセス権限レベル（図 4 では 3) が決定される．次に，このユーザアクセス権限レベルと機密ファイルヘッダのアクセス権限部が示しているファイルアクセス権限レベル（図 4 では 2) を比較し，ユーザアクセス権限レベルがファイルアクセス権限レベル以上である場合，機密ファイルの閲覧は許可される．

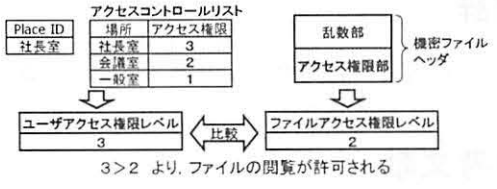

図 4: アクセスコントロールの例

5 実装と評価

5.1 システムの実装

第 4 章で設計した機密ファイル閲覧システムの実装を行った．開発環境として JDK1.4.1，暗号化アルゴリズムとして RSA，3DES，一方向性ハッシュ関数として MD5 を用いた．また IC カードとして，SunMicrosystems の提供する Java Card を利用した．Java Card は Java 実行システムを持ち，アプリケーションを自由に追加・削除することが可能な IC カードである．閲覧ソフトの実装画面を図 5 に示す．この画面は，場所の認証，アクセスコントロール後の機密ファイル閲覧時のものである．

図 5: 閲覧ソフトの実装画面

5.2 適切な認証限界時間の設定

ウォーキング認証では認証限界時間が認証近傍範囲を決定するパラメータになる．この値が大きすぎると，意図した範囲外での認証が可能になり (false positive)，この値が小さすぎると範囲内であっても認証が成功しなくなる (false negative)．そこで，実装したシステムを用いて認証近傍範囲に応じた適切な認証限界時間を求めるための評価実験を行った．

5.2.1 実験方法

実験環境として，図 6 に示される部屋を認証近傍範囲として用いた．場所サーバ（認証サーバを兼任) を部屋の出入り口から最も遠いデスク (S) に設置した．そして，認証端末を（1）～（4）の 4 箇所の認証対象地点に設置した．(S) からの最短距離は（1）が 9.44m,（2）が 6.6m,（3）が 6.64m,（4）が 1.74m となる．

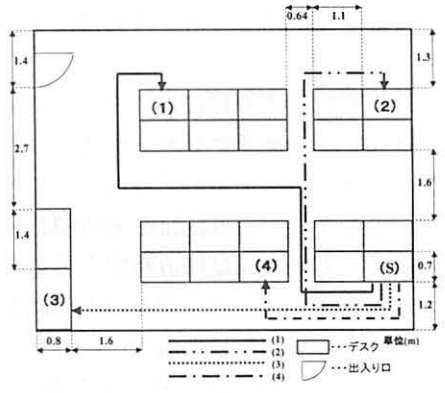

図 6: 認証近傍範囲となる部屋

実験では，10 人の学生が 3 回づつ（1）～（4）の 4 箇所でウォーキング認証を行い，その際に (S)

からカードを抜き各地点の端末に徒歩で移動し，カードを挿入するのにかかる到達時間を測定した．測定された到達時間はそのときの認証セッションにおいて最も最適な認証限界時間とみなすことができる．

5.2.2 実験結果

各地点における到達時間の平均時間，最長時間，最短時間，分布の比較を表1に，頻度を図7に示す．　本実験では，部屋の中で最も出入り口に近く場所サーバから最も遠い地点に存在する（1）までの最長時間が18.96秒であることから，この程度の値を認証限界時間に設定すれば部屋のどこにいても認証が成功すると言える．

表 1: 認証中心地点ごとの到達時間の比較

認証中心地点	(1)	(2)	(3)	(4)
平均時間 (Sec)	15.57	12.50	10.03	6.81
最長時間 (Sec)	18.96	14.60	12.27	8.57
最短時間 (Sec)	13.53	10.34	8.80	5.56
分散	1.91	0.99	0.64	0.69

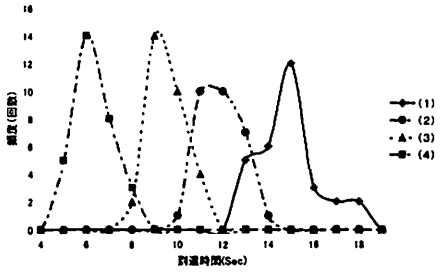

図 7: 到達時間の分布

しかし（1）は出入り口に近いため，最短時間13.53秒で（1）に到達するユーザはその後数秒間，部屋外に出て遠くに移動することができることになる．これを防ぐには認証限界時間を短くする必要がある．しかし認証限界時間を短くすればするほど認証近傍範囲は狭くなり（1）に端末があるにもかかわらず認証に失敗するユーザが増えることになる．例えば認証限界時間を16秒とした場合，本実験では23.3 %のfalse negativeが発生する．

また（1）は出入り口に近すぎ情報が外部漏洩する可能性が高いという理由から（1）での閲覧を禁止するために認証限界時間を13.53秒未満に設定して認証近傍範囲を狭めた場合，（2）では16.7 %のfalse negativeが発生する．逆に，（2）でのfalse positveを完全に無くすために認証限界時間を14.60秒に設定した場合には（1）では16.7 %のfalset positiveが発生する．

このように認証限界時間の設定ではfalse positiveとfalse negativeのトレードオフが発生する．このため，使用用途や求められる条件に合った認証限界時間を設定することが重要であると言える．

6 おわりに

組織関係者による機密情報漏洩の防止には，情報を閲覧することが可能な場所を規定することが効果的であると言える．そこで本稿では「人間が一定時間内に移動できる距離は移動時間に比例し短時間で遠隔地に移動することはできない」という性質を利用して場所の認証を行うウォーキング認証を提案した．そしてウォーキング認証を組み込み，機密ファイルの閲覧場所を認証し，閲覧場所に応じたアクセスコントロールを行う機密ファイル閲覧システムを設計した．これにより，従来に比べてより信頼性の高い，組織関係者を対象とした機密情報漏洩防止策が可能となった．

謝辞

この研究は，応用セキュリティフォーラムの支援を受けて行われた．

参考文献

[1] 青柳慶光, 鮫島善信: 機密ファイル持ち出し防止システムの検討, コンピュータセキュリティシンポジウム, pp. 59-64 (2002).

[2] Location-Based Authentication Grounding Cyberspace for Better Security, http://www.cosc.georgetown.edu/denning/infosec/Grounding.txt

[3] S.Brands,D.chaum:Distance-Bounding Protocols,Proc.EUROCRYPT'93 Lecture Notes in Computer Science,pp. 344-359 (1993).

[4] Tim kindberg, Kan Zhang:Context authentication using constrained chaneels, IEEE workshop on Mobile Computing Systems and Applications, pp. 14-21 (2002).