2004－CSEC－25　(4)
2004／5／21

ディスプレイからの視覚的情報漏洩防止システムの開発

竹内 啓 [†1]　　西本 賢城 [†2]　　佐々木 良一 [‡]
東京電機大学工学部 〒101-8457 東京都千代田区神田錦町 2-2
E-mail: †{takeuchi, nisimoto}@isl.im.dendai.ac.jp　‡sasaki@im.dendai.ac.jp

あらまし　複数の人が共有利用する空間で情報端末を利用する場合、そのディスプレイを介して表示される情報は第三者による覗き見などに対して無防備であるのが現状である。現在こういった問題に対する対策技術として PPT 技術があげられる。PPT 技術とは専用ディスプレイとそれに付属する専用メガネとで構成されるシステムで、専用ディスプレイに表示される内容は専用メガネを介さなければ見ることができないという視覚上の情報漏洩防止効果を持つ。しかしこの技術は専用メガネですべての専用ディスプレイを見ることができてしまうという大きな問題がある。本研究ではこの問題に対して RFID 技術を利用したシステムの提案・試作を行った。これは RFID タグを搭載した専用メガネを専用ディスプレイの側で監視し、専用メガネ所持者による覗き見行為等と言った不正行為を利用者に知らせることで、この PPT 技術の持つ問題を未然に防ぐことを目的とするシステムである。

Development of the visual information Leak Prevention system from a Display

Kei Takeuchi [†1], Yosiki Nisimoto [†2], Ryoichi Sasaki [‡]
School of Engineering, Tokyo Denki University 2-2 Kandanishikicho, Chiyoda-ku, Tokyo, 101-8457 Japan
E-mail: †1{takeuchi, nisimoto }@isl.im.dendai.ac.jp　‡sasaki@im.dendai.ac.jp,

Abstract　When an information terminal machine is used in the space in which two or more persons are,the information displayed through a display is defenseless to the peep act by the others.　There is PPT technology as measure technology to this problem now.　PPT technology is the system which consists of an exclusive display and exclusive glasses, and it has The information leak prevention effect on vision that you cannot see the contents on an exclusive display without exclusive glasses.　But, this technology contains the big problem that all exclusive displays will be able to be seen with one exclusive glasses.　In order to solve this problem, we performed the proposal and the trial production using RFID technology of a system.　This system prevents the problem which PPT technology has by supervising the exclusive glasses carrying the RFID tag and telling a user about the dishonest act called peep act by the glasses possessor etc.

1. はじめに

情報端末を利用する以上、その作業内容はディスプレイを介して表示されてしまう。このディスプレイを介して表示される情報は、第三者により容易に覗き見可能であり利用者はその行為が行われていることに対して気づくことすら難しいのが現状である。

特に企業内などにおいて、出願前の特許情報や新製品の情報など社外に漏れることにより重大な損失となりうる情報を取り扱う場合においては無

視することのできない重要な問題であると言える。

本研究ではこの問題解決を目標として PPT 技術と RFID システムを用いた組み合わせについて検討した。PPT 技術とは専用ディスプレイとそれに付属する専用メガネを用いることで視覚的情報の漏洩を防ぐことを目的とする技術であるが、この技術単体では複数の PPT ディスプレイに付属した専用メガネでお互いのディスプレイを区別無く見ることができてしまうという大きな問題を残してしまう。

そこで固体認識技術としての RFID システムを適用させることでそれぞれのディスプレイが自分のペアである専用メガネを識別するようにした。

本稿では、2 章で PPT ディスプレイの概要、3 章で RFID システムの概要、そして 4、5 章で提案システムの説明及びそのシステム利用時に発生する問題点について考察していく。

2　PPT ディスプレイ

PPT ディスプレイと一般ディスプレイにおけるしくみの違いについて、そして PPT ディスプレイ利用時に生じる問題点について記述する。

2.1　PPT ディスプレイのしくみ

一般の液晶ディスプレイは液晶層を挟むように 2 枚の偏光板(ある特定の方向に振動する光のみを透過させる)を設置した構造となっている。(図 2 参照)

PPT(Picture Protect Technology)ディスプレイではこの偏光板 2 枚のうち片方を取り外すことで必要以上の光の透過が発生し、肉眼でモニタ上に表示されている内容を見ることができないしくみとなっている。これを見るには、その取り外した偏光板、また偏光板を取り付けたメガネ等を介してのみ画面上の内容を読み取ることができる。

この技術の主な用途例としては、ATM や入退出管理システム、電子投票などでの利用が現在検討されている。

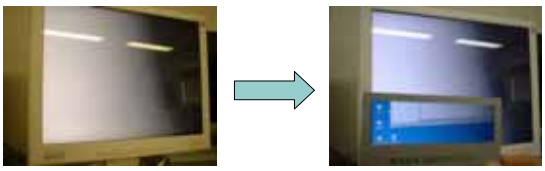

図 1　実際の PPT ディスプレイ利用画面

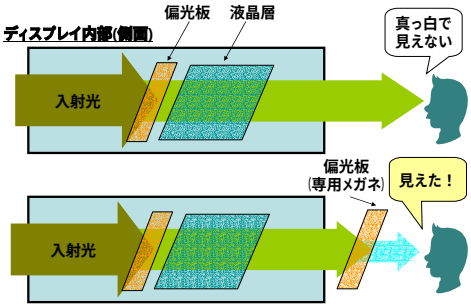

図 2　PPT ディスプレイのしくみ

2.2　PPT ディスプレイの持つ問題点

2.1 の PPT ディスプレイのしくみで記述したように、専用メガネには偏光板が取り付けられている。しかしそれら専用メガネに取り付けられた偏光板には物理的な違いはなく、専用メガネを 1 つ持ってさえいればすべての PPT ディスプレイを読み取ることが可能になってしまうのである。

結果として、図 3 のように共有空間における PPT ディスプレイ利用者 A と利用者 B は、専用メガネをかけることで自分のディスプレイだけでなく A は B のディスプレイを、B は A のディスプレイをお互いに見ることができてしまうのである。

このように、複数の人が専用メガネを所持していた状況で PPT ディスプレイを利用した場合、そのメガネ所持者間でのディスプレイ上の情報は保護されていない状態となってしまうといえる。

図 3　複数利用時における問題

3　RFID システム

3.1　既存 RFID システム

RFID とは IC タグを用いた無線通信による識別技術である。主に、RFID タグ、RFID リーダから構成され、それら情報管理システムを総称して RFID システムと呼ぶ。

RFID タグは超小型 IC チップとアンテナを内蔵した媒体であり、RFID リーダに対して情報を非接触で送出する。そして、RFID リーダはタグから情報を読み取るための装置である。RFID タグには表１のように複数の組み合わせがある。

また、RFID タグと RFID リーダとの通信距離は、利用周波数や内蔵電池の有無により異なる。利用周波数が 13.56MHz では数センチから数十センチ程度、900MHz や 2.45GHz 帯のタグは、数メートルと通信距離の選択幅は広い。

3.2 RFID タグ・リーダ間のプロトコル

一般的 RFID タグとリーダ間のプロトコルを示す

ⅰ) リーダが ID 取得要求をブロードキャスト
ⅱ) 電波到達範囲内に存在するタグが ID を返送
ⅲ) リーダから ID を指定してユーザ領域のデータ読み取り要求をブロードキャスト
ⅳ) 指定された ID のタグがユーザ領域のデータを返送

表 1. RFID タグの種類

内蔵電池の有無	パッシブ型 (電池無し)	アクティブ型 (電池有り)	
メモリタイプ	ROM 型	RAM 型	
記憶領域	64 ビット　から　数 K バイト		
特殊回路	暗号処理プロセッサ等の セキュリティ回路の有無		
利用周波数	13.56MHz	900MHz	2.45GHz

4　提案システム

第 3 章でも記述したように、PPT モニタ単独での利用は利用者が複数居る場合において大きな不安を残してしまう。

そこでこの問題の原因が PPT モニタと付属の専用メガネがそれぞれ厳密なペアでないことで生じてしまう問題であると考え、それぞれの専用メガネに識別 ID を持たせ、それを PPT モニタ側で識別する方法について検討した。

4.1 RFID 利用法

メガネに取り付けた RFID タグの ID 情報を元に PPT モニタとの間で認証を行わせる。これにより、正規ユーザがモニタの前に座るだけで、ユーザの手間をかけることなく認証が行える。また、許可のないタグが探知された場合、PPT モニタ側でそれに応じた対応を行うことが可能となる。

4.2 DEF システム

本研究では、この PPT モニタと RFID システムを組み合わせた方式のシステムを、『識別化された専用メガネの探知･監視を目的とするシステム』という意味を込めて **DEF**(Discrimination Eyes sight Finder)システムと呼ぶことにする。

4.3 システムの要点と構成図

(ⅰ)専用メガネを所持していないとモニタを見ることはできない。
(ⅱ)すべての専用メガネ(タグ付)を DEF システムで監視することにより作業中に発生する覗き見等といった行為に対して警戒することが可能となる。

今回開発した DEF システムは以下のような構成となる。

図 4　DEF システムの構成図

4.4 開発環境

OS：Windows　XP　Pro
言語：C++（Visual C++ 6.0）
装置：ＰＰＴモニタ（SKR テクノロジー）
RFID システム(FEIG　ELECTRONIC)

今回のシステムは、利用した RFID のメーカーである FEIG ELECTRONIC 社から提供されるクラスライブラリを利用して開発を行った。
開発したソフトウェアのステップ数は 686 行。

今回プロトタイプシステムを開発するにあたり使用した RFID システムの仕様を以下に示す。

- 利用周波数　　：13.56[MHz]
- 内蔵電池　　：パッシブ型
- 通信距離　　：最大約 30[cm]
- タグの内部メモリ容量　：2048[Byte]
  (うち 2024Byte がユーザ領域)

本研究で利用した RFID タグは、内部メモリにおいてシリアル ID と呼ばれる「タグを一意に識別するための読み取り専用 ID」と、「利用者が書き換え可能なユーザ領域」とを持っている。

プロトタイプシステムでは、シリアル ID(読み取り専用 ID)をタグ識別 ID とし、これを DEF 用アプリケーションにて監視する。

4.5　システム全体の流れ

DEF システムの全体的な流れを以下の図に示す。

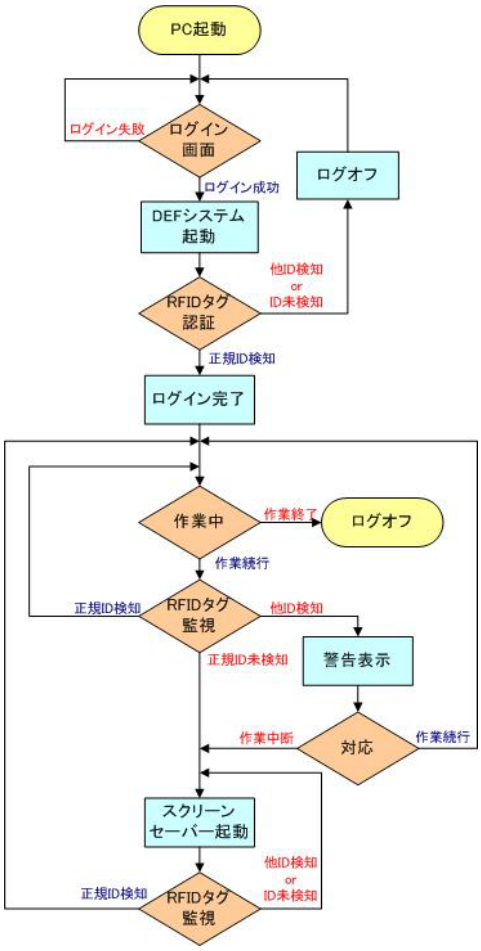

図 5　フローチャート

4.6　システムの動作

RFID リーダによりタグが検知された状況によって、DEF システムがどのような動作処理をするかを動作順序と併せて以下に示す。

①パソコンを起動させ、OS によるログイン認証の後、DEF システムが起動し同時に RFID による認証を行う

- ■ 正規 ID が検知された場合は認証完了となる
- ■ 登録された正規 ID が検知されなかった場合は強制的にログオフし、最初のログイン画面に戻る

②正規ユーザ作業中は定期的に RFID リーダから ID 取得要求を送出し、電波到達範囲内にあるタグを DEF システムにより監視する。

- ■ 正規 ID のみが検知されている場合そのまま作業中の状態を継続
  (図 6 参照)
- ■ 正規ユーザが席を離れ、正規タグが検知されないときは DEF 側でスクリーンセーバーを起動させ画面上の内容を覆い隠し、この時キーボード等の操作はすべて無効
  (図 7 参照)
- ■ 正規ユーザ作業中に、正規タグと不正タグ[1]が同時に検知された場合、DEF 側で覗き見行為をされていると判断し画面上に警告ウィンドウを表示してユーザ側に知らせる
  (図 8 参照)

③警告表示後の対応について
ここでは覗き見されている可能性のある状況でどういった対応をするかをユーザ側で選択させる

- ■ 問題はないとして作業を継続する
  (図 6 参照)
- ■ スクリーンセーバーを起動させ作業を一時中断
  (図 9 参照)

③ログオフし作業を終える

[1] ここでの不正タグとは未許可(正規以外の)ID タグを付けた専用メガネ所持者のこと

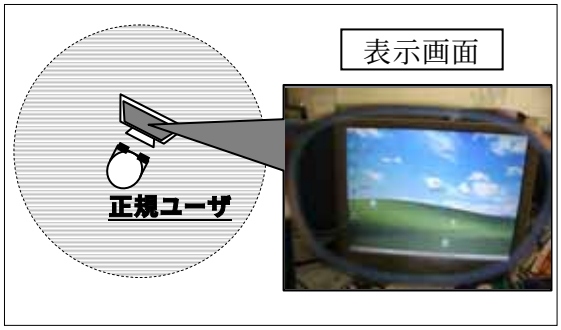

図 6　通常時

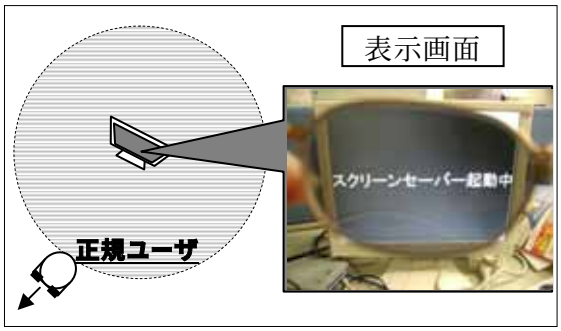

図 7 ユーザ離席時

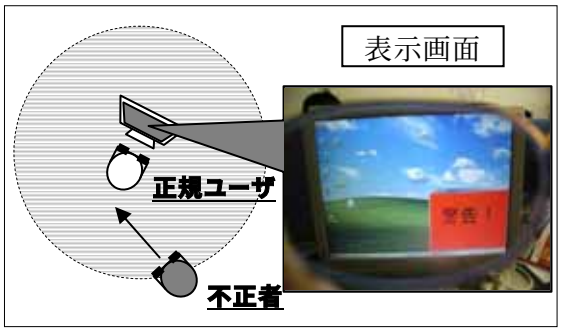

図 8　不正者の検知

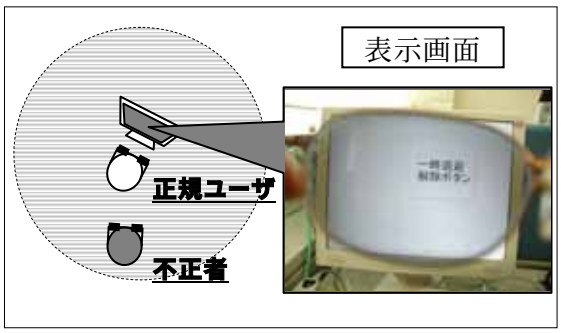

図 9　検知後の一時的退避

5　考察

今回開発した DEF システムは、利用した RFID システムの通信距離が短いなどの制約があったものの基本動作においては 4 章の 4.6 で記述した通りの動作をすることが確認できた。しかし、現在のシステムでは実用性の面においていくつかの問題を含んでいることがわかった。

今回、研究・開発を通してわかった DEF システムに対して想定される脅威を、それぞれハード面、システム面、ユーザビリティ面に分けて以下に示す。

5.1　ハード面での課題

通信距離の問題

今回用いた RFID システムのリーダとタグ間の通信距離は約 30 センチとなっているが、この通信距離で覗き見を検知するにはあまりに距離が短すぎる。しかし、通信距離が長すぎることで覗き見不可能な距離にあるタグに対しても過度に反応してしまう問題も考えられるので、新しい RFID システム導入後、最適な距離の検証が必要であると考える。

タグの付いていないメガネ

今回のシステムは、あくまですべての PPT 専用メガネに RFID タグが取り付けられていることを想定してのシステムであるため、タグの取り外された専用メガネに対しては DEF システムで監視することができず無防備な状態になってしまう。

この問題の解決案としては、専用メガネ製造時、RFID タグ取り付けにおいて、取り外し不可能にするなどの工夫を講じる必要がある。

5.2　システム面での課題

スクリーンセーバー起動時のキーボード無効化

正規ユーザが退席中はスクリーンセーバーを表示させることでユーザ不在時の盗み見行為を防止しているが、現段階の DEF システムでは、*Del + Ctrl + Alt* などシステムキーを利用した DEF システム解除が可能となっている。

現在は、DEF システムの利用を Windows OS と限定して、優先度の高いシステムキーを無効化するため、仮想デバイスドライバを利用して

の実現に向け検討中である。

RFID のトレーサビリティ問題

RFID タグはその性質上、RFID リーダに対して常に同一のユニークな ID を受動的に送信してしまう。そのためタグ付専用メガネを所持して出歩くことにより、所持者による ID 追跡による行動範囲の特定などが行われる危険性がある。現システムは識別している ID に読み取り専用(書き換え不可)のシリアル ID を利用しているためこの危険性を含んでいる。

5.3 ユーザビリティ面での問題

ユーザによる専用メガネの扱い方

この問題は利用者が離席する際に専用メガネをディスプレイの前などリーダの読み取れる範囲内に置き忘れることで生じる。本来であれば、利用者が離席することによりスクリーンセーバーが起動されるが、本研究では専用メガネを持たずにディスプレイの前から離席するといった状況を想定していないため、正規の専用メガネが検知されているだけで DEF システムは正規ユーザがそばに居ると錯覚してしまう。

この課題に対しては、めがねを机の上などに置かないよう注意することが必要になっていく。また，机の上などにおいて動かないと分かる仕組みの検討をする必要がある。

5.4 その他の問題

上記の問題以外にタグ内部のデータ漏洩やそれによるタグ偽造・なりすましといった問題も挙げられるが、この問題は RFID に共通する問題であるのでここでは詳しく言及しない。

6 おわりに

現システムの段階ではまだまだ課題点は多く実用性レベルには至っていない。また実際に複数の人にシステムを利用してもらうことで、利便性の面での評価も検証する必要がある。

また、今回用いた RFID システムでは実現できなかったが、タグの位置や距離を測れる機能を持たせた RFID システムで、専用メガネに付いているタグとモニタの距離を計測し、使用者の顔の位置や向きなど身体的特徴を利用した認証方法の可能性も検討していく。

参考文献

[1] 荒川弘照(編)NTT データ・ユビキタス研究会(著)「IC タグって何だ？」カットシステム

[2] 社団法人日本自動認識システム協会(編)「これでわかった RFID」オーム社

[3] 木下真吾 他 「RFID プライバシー保護を実現する可変秘匿 ID 方式」CSS2003