7T-3

RFID を用いて過失による個人情報漏洩を防ぐシステム

大谷 孝佑† 井上 亮文† 市村 哲† 松下 温†
†東京工科大学

1. はじめに

２００５年４月,「個人情報保護法」が施行されたが，毎日のように情報漏洩事件が発生しているのが現状である．その主な原因は，①内部者の故意 ②内部者の過失，③外部者の故意，の３つに大きく分けられ，うち①②が全体の８割を占めているといわれている．

現在の個人情報漏洩リスク対策は, 入退出管理, 利用者のアクセス制限，情報利用者のログ管理など悪意(故意)を持ったものに対する対策を中心に進められている．しかし，過失(つい・うっかり)といった「無意識的なミス」に重点を置いたものは少ない.

これまで過失漏洩に対しては，個人情報保護法に関する研修会を開くことで対応してきた．しかし，研修を行った直後は重要情報に対する意識が高まっているが，この高まりは必ずしも持続性のあるものとはいえない.

過失漏洩の根本にある発生要因は個人の意識であると考えられる．[1]常に取り扱う情報に対して組織や個人で「重要な情報を扱う」という意識・注意を払うような工夫があれば，過失による漏洩が防げるのではないかと考えた. そこで本稿では，RFID を用いて複数人で意識・責任を共有しつつ個人情報を取り扱うシステムを提案する.

2. 提案システム

2.1. システムの概要

本システムでは，重要情報・個人情報を扱う者に対して社員証のようにして RFID タグを配布する．利用者は，重要情報・個人情報を利用する際に，RFID リーダを備え付けた PC の前に座る. すると自動的にタグ ID の認証を行い，RFID リーダによって取得されたタグ ID の数(人数)・種類(役職等)，によって，重要情報・個人情報の利用方法が制御される.

本システムの概要を図 １に示す. まず①はユーザ A が単独でシステムを利用する場合である.

Private information protection system for accidental causes using RFID tags
† Kousuke Ohtani , Akifumi Inoue , Satoshi Ichimura , Yutaka Matushita
† Tokyo University of Technology

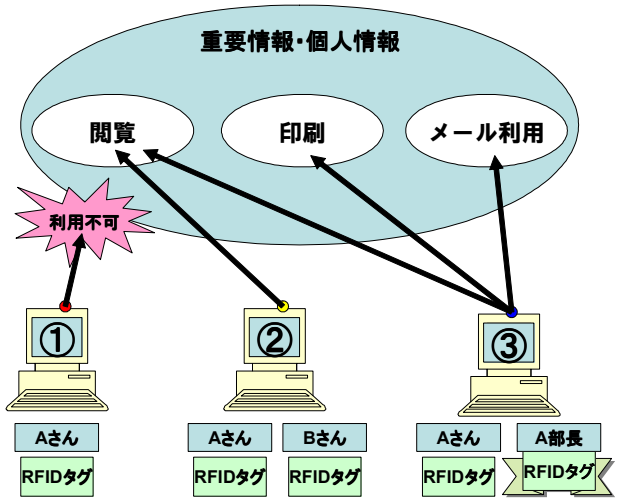

図 1 システムの利用例

この場合，システムが必要数のタグ情報を取得できず, 認証に失敗する. 認証に失敗するので，当然情報の利用はできない. 次に②は A と B が共同でシステムを利用する場合である．この場合，タグ情報の必要数を満たし，認証に成功し閲覧が可能となるが，タグ情報の種類の条件を満たしていないため，一部のサービスができない. 最後の③は A の他に責任者である C が共同でシステムを利用する場合である．この場合，タグ情報の必要数・種類の条件を満たすため，閲覧・印刷・メール利用が可能となる．どの場合においても，利用者の一人が席を離れると，重要情報の取り扱い続行が不可能となる.

RFID を利用して単独での重要情報の取り扱いが制限されることで，単独作業時に無意識に起こしてしまう「うっかりミス」の防止につながると考えられる．また，数人（認証協力者）と利用者を連携させることで，個人の責任保持・責任共有意識が高まり，結果として情報漏洩の抑制につながる.

2.2. 関連研究

認証にパスワードを必要とするシステムで，利用者がその場にいるのかという存在を確認するには，席を離れる時，戻ってきた時を利用者本人の入力操作によってシステムに知らせる必要がある. しかし，うっかりその場を離れてしまった場合に

ロックをかけたりするといった対応ができない．さらに，パスワードは基本的にユーザ１人を認証するために用いられている．

本システムでは，RFID タグの通信が可能・不可能かの情報でシステムが自動的に利用者の存在を確認するため，うっかりその場を離れてしまった場合でも，システムが自動的に退席を認識できる．タグの数や種類も自動で取得できるため複数人の組み合わせ認証でも手間がかからない．

3. 実装

3.1. RFID

本研究で使用する RFID タグは，常時携帯する社員証などとの併用を考えているためカード程度の大きさのものが望ましい．また，認証協力者が利用者の利用・作業に注意できるように目の届く範囲のもの，つまり，通信距離が１～２ｍ程度のものが必要となる．よって，通信方式が電波方式であり，通信距離が長く（～8m 程度）障害物に影響されにくい特性を持つ UHF 帯（９５０MHｚ帯）の ALIEN 社製 RFID を使用した．

3.2. システムの流れ

図 2 にシステムの流れを示す．

①ユーザが利用 PC の前に座ることによって，RFID タグの情報が受信可能となる．読み取り可能となった RFID タグの情報をアンテナによって受信する．

②アンテナによって受信した情報を RFID リーダに読み込む．

③取得した RFID タグの情報が利用者 PC に送信される．利用者 PC では，送られてきたタグの情報からタグの個数・種類を読み取り，個人情報・重要情報利用の制限を判断する．

④③の利用者 PC で個人情報・重要情報を利用している最中，常にタグの存在（利用者の存在）を確認する必要があるので，数秒，もしくは数分ごとにタグ情報の取得を繰り返し行う．

図 3 にシステムの利用の様子を示す．システム利用者の 2 名は，首から社員証(ｉ)（RFID タグ）をぶら下げている．また，利用中の PC には RFID リーダライタ(Ⅱ)を取り付けている．壁には RFID リーダライタのアンテナ(Ⅲ)が取り付けてあり，そのアンテナよりタグ情報の読み込みを行う．

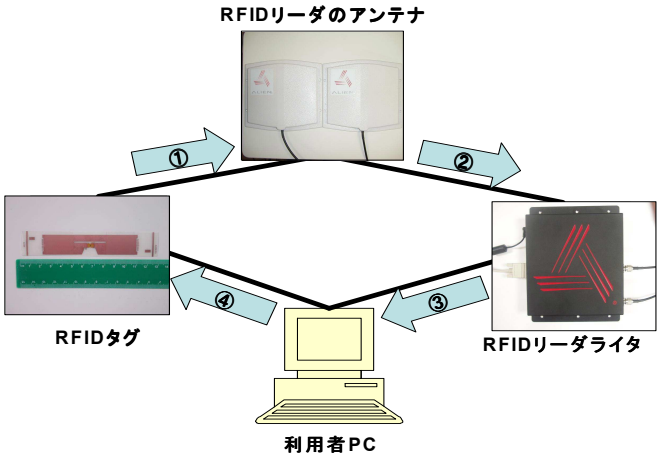

図 2　システムの流れ

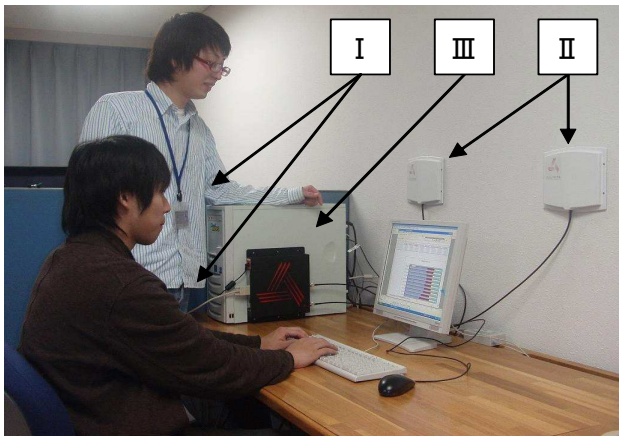

図 3　システム利用の様子

4. まとめ

本システムにより，従来の認証を PC の前にいるだけで簡単に行えるようになった．さらに RFID タグの数・種類，存在の有・無によって，重要情報・個人情報の利用が制限できるため，悪意を持つものによる漏洩だけでなく，特に過失による漏洩の防止に特化したシステムとなった．

今後の課題としては，RFID タグの書き込み領域を利用して更なるセキュリティの強化や，他のセキュリティ対策との連携を取るといった応用などが挙げられる．

参考文献

[1] 江崎，大橋，上野，三菱総合研究所，研究ノート(P66～83)“個人情報防止のためのヒューマンエラー対策”

[2] 日経 BP 社：“無線 IC タグのすべて”　：日経 BP 社／日経 BP 出版センター

[3] RFID について：“RFID テクノロジ”：http://itpro.nikkeibp.co.jp/rfid/