L-034

ダイナミックに制御する情報漏洩対策システムの検討
A study on method to preserve confidential information dynamically

榎本 真也† 金井 敦† 谷本 茂明‡ 佐藤 周行§
Shinya Enomoto Atsushi Kanai Shigeaki Tanimoto Hiroyuki Sato

1. はじめに

近年，個人情報保護法の施行などに伴い，企業などでは情報の守秘管理が重要視されている．そのため，管理している情報の安全の確保については，最も危険な状況を想定し，情報の保護を行っているのが現状である．例えば，情報のセキュリティの管理指針としての ISMS(情報セキュリティマネジメントシステム)は保護するべき情報をレベル分けし，それに見合ったセキュリティレベルで管理することで，情報の安全性を確保している[1][2].

一般的に守秘管理はリスクの最も高い状態を想定し，その高いセキュリティレベルで管理を行っている[3]．一般に，高いセキュリティを確保すると厳重な保管が必要になるなど可用性が悪くなり，情報の利便性が損なわれる．しかし，例えば，守りたい情報の近くに，不審者が居る場合と，居ない場合ではリスクが異なる．すなわち，状況に応じリスクが変化していることがわかる．従って，リスクが小さい時には，セキュリティレベルを下げて管理することにより可用性を良くすることが可能になると考えられる．

このように，脅威の大きさに応じた対策をダイナミックにすること安全性を確保した状態でかつ可用性も確保でききると考えられる．本論文では，セキュリティレベルをダイナミックに制御することで安全性と利便性の両立を考えた手法を新たに提案する．

一般的に，情報システムのセキュリティを確保する場合，考慮すべき脅威は，ネットワークごしの攻撃や不審者の侵入など，バーチャルからリアルまで様々な脅威が存在する．今回提案するダイナミックにセキュリティレベルを制御する手法のコンセプトは，バーチャル，リアルを問わない概念であり，多くの場面や状況に適応できることを想定している．

本論文では，上記コンセプトを提案するとともに，一例として，企業オフィスへの来訪者訪問というリアルな環境を想定し，オフィスの PC に保管されている機密ファイルをダイナミックに守る方式を提案する．

具体的には，特に不審者や情報を知られてはいけない人間によるディスプレイの覗き見や，USB など記録媒体によるデータの持ち出しなどの物理的な情報漏洩から重要な情報を守る方法に焦点をあてる．今回は，最も単純な，来訪者 1 人が保護すべき情報を持つ PC へ接近しているという状況を想定し，その検知および制御方式について検討した結果について述べる．

† 法政大学 Hosei University
‡ 千葉工業大学 Chiba institute of Technology
§ 東京大学 Tokyo University

2. セキュリティダイナミック制御のコンセプト及び具体例

2.1 セキュリティダイナミック制御のコンセプト

ここでは，提案方式のコンセプトに関して述べる．一般に，脅威の状況は，時々刻々変化しているため，図 1 に示すように，その状況を検知し，可視化し，制御することが本概念の基本コンセプトである．以下に，これらの要素について示す.

(1)脅威の検地
現在の脅威の状況をリアルタイムに検知・把握する．例えば，IDS により DOS 攻撃が検知された，ある PC にウィルス感染が検知された，部外者が近付いたなどリスクが増加するような状況をリアルタイムに検知する．リアルな世界では，センサーネットワークなどを駆使した脅威検知が必要である．

(2)可視化・数値化
(1)で検知した脅威の状況を，リススの大きさに応じて数値化して表示したり，危険な部位を示したりするなど具体的に人が理解でき対応できるようにする．

(3)セキュリティレベル制御
検知したリスクレベルに応じて，システムのセキュリティレベルをダイナミックに制御し，変化させる．この場合，リスクは低い通常レベルに比較して，緊急対応時には利便性が落ちたり，業務が中断したりする場合も許容する．また，システムの制御としては，ファイアウォールのポリシー変更，資産価値の大きい情報を別サーバに退避，システムのシャットダウンを行ったりするような対応を行う．

2.2 ダイナミック制御の具現化例

ここでは，2.1 のセキュリティダイナミック制御のコンセプトに基づく具現化例について示す．PC で管理している保護するべき情報を，不審者による覗き見や物理的な持ち出しから防ぐ方法を提案する．具体的に取り上げる場として，企業のオフィスを想定する．他企業からの来客が自社の管理する PC に近づくに従い，その距離に応じて PC がその状況に合った情報漏洩の対策を行う．利用する要素として，PC の状況，来客，距離の要素を利用し，情報漏洩対策の方法を決定する．

さらに今回は，最も単純化するため，来客 1 人，保護すべき情報を持つ PC は 1 台という状況を想定し来客と PC 間に遮蔽物は無いものとする．

Copyright © 2012 by
The Instiute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

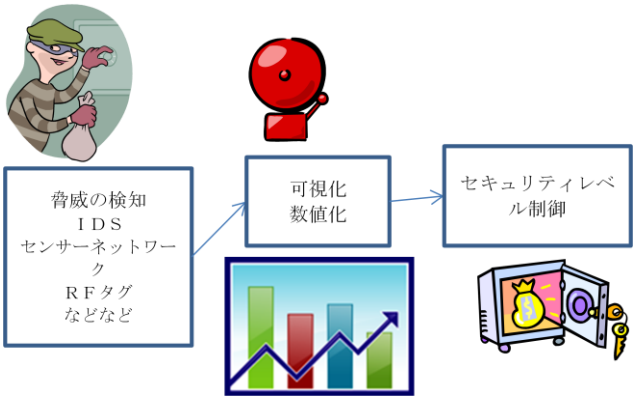

図 1　セキュリティダイナミック制御のコンセプト

前提となる条件として，来客は一番初めに受付を済ませるものとする．来客は来訪の際まず受付で手続きをおこなうのが一般的である．そこで，受付係りの者が来客の種類を判定し，データベースに入力を行う．そして，来客にタグの配布を行う．配布されたタグは来客が常に身に付けておくものとする．

以下に各要素と漏洩対策の方法について詳しく説明する．

・PC の状況

顧客情報や社内資料といった社外秘の情報あり，それらにアクセスできる PC があるとする．その PC に来客が近づいてきた場合，その PC の席に自社の社員が居るときと居ないときでは，情報漏洩の可能性に差ができる．このとき，PC で作業している人が席に居る場合の方が情報漏洩の可能性が低く危険度も低くなり，席に居ない場合は情報漏洩の可能性が高まるため危険度も高くなる．

・来客の種類

今回，来客は社外秘の情報を知られてはいけない人物であると考える．来客は種類を設定し，来客が社外秘の情報を盗みとることにメリットがあるのか，また情報を盗む方法を知っているのかによって，危険度の大きさを変える．表 1 に来客の種類と危険度を認識しやすくしたものを示す．

来客の種類欄の「企業・協力なし」「企業・協力あり」で，企業とは自社と同業界の他社からの来客を示し，協力とはプロジェクトを共同で行っているかいないかを示す．

・来客と PC 間の距離

来客と社外秘の情報にアクセスできる PC との物理的距離とする．この距離が近いほど来客に PC の操作やディスプレイを覗かれる可能性が高くなるため危険度は高くなり，逆に遠くなればそれは難しくなるため危険度は低くなる．

・漏洩対策の方法

今回，PC からの物理的な漏洩の対策を行う．対策方法として，保護したい PC と脅威である来客との物理的距離によって，その距離に必要な漏洩対策を行う．

PC からどの程度離れているかによって漏洩対策の方法が変わってくる．PC から，10 メートル前後離れている範囲では，PC から直接データを持ち出されたり，ディスプレイを覗き見される危険性はほぼ無い．しかし，話し声や音声は聞こえてしまうため，対策として来客が近くに来たことを知らせたり，音を消すなどを行う．また，5 メートル前後の範囲では，ディスプレイの覗き見される危険性があるため，PC の操作の制限や，画面を消すなどの対策を行う．PC が操作できるような近距離では，直接データを持ち出されたりするなどの最も危険な状態なので，電源を切るといった，データの持ち出しや PC の操作ができなくなる対策を行う．表 2 に漏洩対策の方法を示す．

表 1　来客の種類と危険度

危険度	来客の種類
高	企業・協力なし
↕	企業・協力あり
↕	搬入業者
↕	郵便配達
↕	一般人
低	同社・他部署

表 2　漏洩対策の方法と危険度

危険度	対策方法
高	電源を切る
↕	USB ポートの使用を禁止する
↕	ディスプレイを消す
↕	通信を切断する
↕	ファイル(フォルダ)をロック・隠す
↕	ファイル(フォルダ)を閉じる
↕	音を消す
低	来客を通知する

2.3 制御内容の決定

2.3.1 漏洩対策の決定

PC の状況，来客の種類，来客と PC 間の距離の 3 つの要素を組み合わせて危険性を決定する．そして，それぞれの状況にあった漏洩対策の方法を行う．

図 2 に示す様に，洩対策の方法の決定までの流れは，まず，PC の状況の判定を行い，PC から情報が盗まれる危険性の判断を行う．次に，来客の種類を判定しどの程度の危険な来客が居るのかを判断する．その後，来客の種類と PC の状況を考慮し，来客と PC の間にどの程度の距離があるのかを測定する．そして，その距離に合わせ，必要と考えられる漏洩対策の方法を決定する．表 3 に 3 つの要素の状況と，その時の漏洩対策の方法を示す．

Copyright © 2012 by
The Instiute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

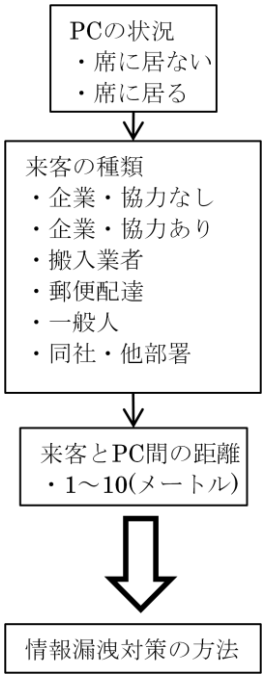

図 2　情報漏洩対策の方法の決定までの流れ

表 3　3 つの要素の状況と漏洩対策の方法

(1)PC の状況(席に居ない場合)

距離	企業･協力なし	企業･協力あり	搬入業者/郵便宅配業者/一般客	同社･他部署
10	来客を通知，音を消す	来客を通知，音を消す	来客を通知，音を消す	来客を通知，音を消す
9				
8	ファイルを閉じる	ファイルを閉じる	ファイルを閉じる	
7	ファイル(フォルダ)をロック･隠す	ファイル(フォルダ)をロック･隠す		ファイルを閉じる
6	通信を切断する	通信を切断する	ファイル(フォルダ)をロック･隠す，通信を切断する	
5				ファイル(フォルダ)をロック･隠す
4	ディスプレイを消す，USB ポートの使用禁止	ディスプレイを消す	ディスプレイを消す	
3				通信を切断する
2	電源を切る	電源を切る	USB ポートの使用禁止	ディスプレイを消す
1			電源を切る	USB ポートの使用禁止

(2) PC の状況(席に居る場合)

距離	企業･協力なし	企業･協力あり	搬入業者/郵便宅配業者/一般客	同社･他部署
10	来客を通知	来客を通知	来客を通知	来客を通知
9				
8	音を消す	音を消す	音を消す	音を消す
7				
6				
5	ファイルを閉じる	ファイルを閉じる	ファイルを閉じる	
4	ファイル(フォルダ)をロック･隠す	ファイル(フォルダ)をロック･隠す		ファイルを閉じる
3				
2	通信を切断する	通信を切断する	ファイル(フォルダ)をロック･隠す	
1	ディスプレイを消す	ディスプレイを消す		ファイル(フォルダ)をロック･隠す

2.3.2 数値化による漏洩対策の決定

情報漏洩対策の方法を数値化して算出を行うため，PC の状況，来客，距離の各要素に数値を設定する．

表 4 に PC の状況に設定する数値，表 5 に来客の種類に設定する数値を示す．このとき，距離の数値[d]は，測定した距離(メートル)の値が，そのまま数値となる．

それぞれの値を式(1)にあてはめ計算を行う．その計算結果によって情報漏洩対策の方法を決定する．表 6 に計算結果と対策方法を示す．

$$R = P \times G \times \frac{(10-d)}{10} \quad (1)$$

表 4　PC の状況に設定する数値

数値[P]	PC の状況
1	席に居ない
0.6	席に居る

表 5　来客の種類に設定する数値

数値[G]	来客の種類
5	企業・協力なし
4.5	企業・協力あり
4	搬入業者
4	郵便配達
4	一般人
3.5	同社・他部署

Copyright © 2012 by
The Instiute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

表 6　計算結果と対策方法

計算結果[R]	対策方法
4 以上	電源を切る
3.15 以上	USB ポートの使用を禁止する
2.7 以上	ディスプレイを消す
2 以上	通信を切断する
1.8 以上	ファイル(フォルダ)をロック・隠す
1.2 以上	ファイル(フォルダ)を閉じる
0.35 以上	音を消す
0 より大きい	来客を通知する

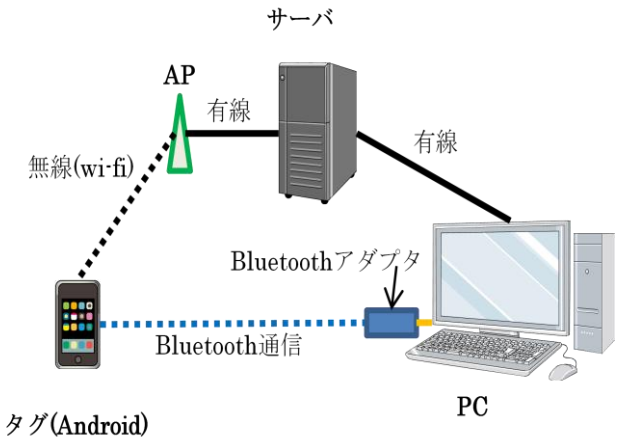

図 3　システムの全体像

3. 実現方式

3.1 システムの全体像

システムの全体像を図 3 に示す.

現状，Bluetooth が搭載されている PC は，ノート PC などの一部のものに限られている．しかし近年，Bluetooth を搭載したマザーボードが出はじめ，今後 Bluetooth は PC に標準的に搭載されると考えることができる．さらに，機能拡張とともに発展していくと考えられる[4].

また，Android 端末や携帯端末の多くは Bluetooth を搭載し，現在ほとんどの人がそれらを所持しており必需品となっている．そのため，今後 Android 端末や携帯端末などは，社員証の様な個人を特定する機能を持つことも考えられる.

このように，今後 Bluetooth が PC に標準化し，PC と携帯端末の通信が普及すると考えられる．そこで距離の測定には，位置推定にも利用されている Bluetooth の電波強度を利用する[5].

今回，来客が所持するタグとして，Android 端末を利用した．PC に Bluetooth アダプタを取り付け，Android 端末と PC 側の Bluetooth アダプタが Bluetooth 通信を行い距離の測定を行う．Bluetooth 通信で取得できる電波受信強度(RSSI：Received Signal Strength Indication)を取得し，その値から距離を判定する.

電波受信強度とは，無線通信時の電波の強度であり，最大が 0[dBm]で最小が-200[dBm]となり，その範囲内の値をとる.

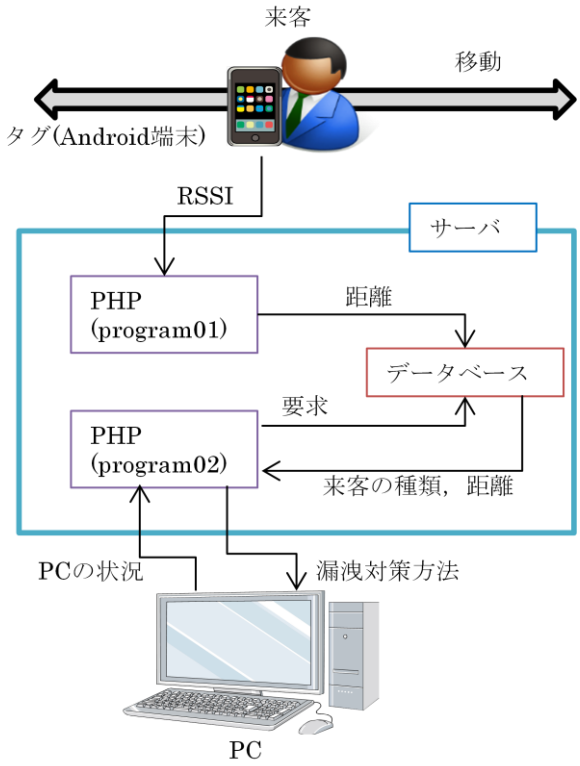

図 4　システム構成

3.2 システム構成

システム構成を図 4 に示す．さらに，以下にシステムの説明を記す.

・タグ(Android 端末)

来客は一箇所に留まらず，移動があるものとし，そのとき常にタグを持っているものとする．そのときの来客と PC 間の距離を測定するために電波受信強度を利用する．来客と PC 間で Bluetooth 通信を行い，電波受診強度の取得する．そして，取得した値とあらかじめ設定した ID を http 通信によってサーバに送信する．リアルタイムの距離を測定するため，これらの動作を一定秒毎に繰り返す.

・サーバ

[PHP－program01]

タグから電波受信強度と ID を受け取り，電波受信強度を距離に変換する．ID を元にデータベース内の距離と電波受信強度のデータを更新する.

[PHP－program02]

PC から PC の状況を受け取る．その後，データベースから距離，来客の種類のデータを取得する．受け取った PC の状況，距離，来客の種類を数値化し，計算結果に従い漏

Copyright © 2012 by
The Instiute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

洩対策の方法を決定する．そして，PC に漏洩対策の方法を送る．

[データベース]

ID，電波受信強度，距離，来客の種類，備考の管理を行う．

・PC

席の状況を http 通信によってサーバに送信する．その後，返ってくる漏洩対策の方法に従い，それを実行する．そして，これらの動作を一定秒毎に繰り返す．

3.3 システムの動作の流れ

以下にシステムの動作の流れを示す．

① 受付でデータベースとタグに，「来客の種類」と ID を登録し，タグを来客に渡す．
② PC とタグ間で通信(Bluetooth)を行う．
③ タグ側で電波受信強度を取得する．
④ タグは取得した電波受信強度の値と ID をサーバに送る．
⑤ サーバは受け取った電波受信強度の値を「距離」に変換し，受け取った ID を元にデータベース内の「距離」の項目を更新する
⑥ PC は「PC の状況」の判定を行い，その結果をサーバに送る．
⑦ サーバは受け取った「PC の状況」，さらにデータベースから「来客の種類」と現在の「距離」を取得し，それぞれの数値を元に計算を行う．
⑧ 計算結果に対応する PC の「漏洩対策の方法」を決定し，PC に送る．
⑨ PC はサーバから「漏洩対策の方法」を受け取り実行する．
⑩ ②～⑤，⑥～⑨をそれぞれ繰り返す

4. 環境と考察

4.1 環境

今回，Bluetooth 通信を利用した距離の測定と Bluetooth による距離測定を利用したシステムの動作の考察を行う．

4.1.1 Bluetooth 通信による距離の測定

方法として，Bluetooth 通信を行い 1～10 メートルまで 1 メートル毎に電波受信強度の測定を行った．1 回の測定で電波受信強度を 10 回取得し，その取りうる値を求めることで，距離と電波受信強度の関係性を調べる． 表 7 に使用した機材を示す．

4.1.2 システムの環境

今回提案するシステムを実装し，その動作の評価を行う．表 8 にタグの環境，表 9 にサーバの環境，表 10 に PC の環境を示す．

動作は 3.3 で説明した流れで動作する．ただし，今回は Bluetooth によるリアルタイムの距離の測定と，その距離に応じて，動的に情報漏洩対策の方法が変化することの確認

表 7　使用機材

使用機材	名称
Android 端末	ドコモ スマートフォン Xperia SO-01B
PC	FMV-BIBLIO LOOX C/E70

表 8　タグの環境

タグ(Android 端末)	開発環境
端末機種	ドコモ スマートフォン Xperia SO-01B
OS	Android OS 2.1

表 9　サーバの環境

サーバ PC	開発環境
OS	windows 7
サーバ OS	apache
データベース	MySQL

表 10　PC の環境

PC	開発環境
開発環境	eclipse
使用言語	Java

を行う．

そのため 3.3 の動作で，⑥の部分にあたる「PC に状況」の判定は手動で入力する．また，⑨の部分では，PC はサーバから「漏洩対策の方法」を受け取るが，実行はしないものとする．

方法として，システムの動作させた後，タグを持ったままの状態で 10～1 メートルまで 1 メートルずつ 60 秒毎にと PC に近づいて行く．測定は 3 回行う．

Android アプリ開発の Bluetooth を制御する API の関係上，電波受信強度はデバイススキャンを行い，他のデバイスを検知した時のみ取得できる．そのため，今回リアルタイムの距離を測定するため，デバイススキャンを 2.5 秒毎に繰り返す．

PC はサーバに，PC の状況を送信し，漏洩対策の方法を受信する．

状況として，来客は「企業・協力なし」，PC の状況としては，「席に居ない」状況を設定した．

4.2 測定と考察

4.2.1 Bluetooth 通信による距離の測定の考察

Bluetooth を利用した距離測定結果を図 5 に示す．

図 5 のグラフで，電波受信強度である縦軸を y，距離である横軸を x とした時，それらの関係性は，おおよそ $y = -2x - 54$ で表せることが確認できた．

さらに，各距離での取りうる値は近距離の場合，平均値から約±3[dBm]の範囲となり，遠距離の場合は平均値から

Copyright © 2012 by
The Instiute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

約±5[dBm]の範囲となった．このことから，ある値を取得した場合，近距離では，実際の距離とは約 1 メートル，遠距離では約 2 メートルの誤差が出ると考えられる．

このことから，Bluetooth を使用した距離の測定は多少の誤差はあるが，望んだ値に近いものが取れるため利用可能であることがわかった．

4.2.2 システムの考察

今回，リアルタイムの距離を測定するため，電波受信強度の取得のためのデバイススキャンを 2.5 秒おきに繰り返し行った．測定を行った結果，1 回目は 3 か所，2 回目は 4 か所，3 回目は 6 か所での取得となった．

このことから，デバイススキャンを繰り返し行っても，電波受信強度が毎回取得できるわけではなく，スキャンのタイミングによってデバイスの検知ができず，電波受信強度の取得ができないことがあるとわかった．

よって，デバイススキャンを繰り返し行うことで，移動する来客のリアルタイムの距離を測定する方法は，今回難しいことがいえる．現状の，Android アプリ開発の API では，デバイススキャンを行い，他のデバイスを検知した時のみ，電波受信強度が取得できるものとなっている．そのため今後は，距離測定専用の API の開発が必要である．

システム全体の動作では，上記のようにリアルタイムの距離の測定ができなかった．しかし，電波受信強度の取得が成功した時，2 章の表 3 で示した，その時の距離にあった漏洩対策の方法を得ることができたため，サーバの動作は現状問題なく動作することが確認できた．

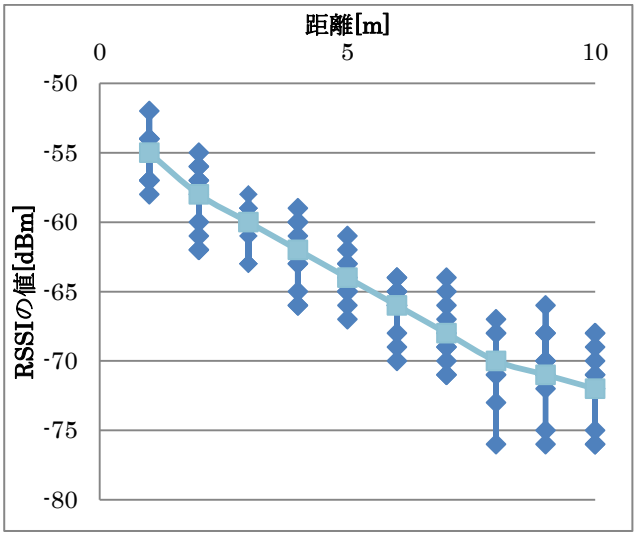

図 5　Bluetooth 通信時の RSSI と距離の関係

5. おわりに

5.1 まとめ

ダイナミックにセキュリティレベルを制御する提案を行い．その 1 つの例として，企業オフィス環境での物理的な情報漏洩対策として，来客から重要な情報を守る方法に焦点をあてた．そして，来客 1 人が PC へ接近しているという状況を想定し，その検知および制御方式について検討を行った．

来客と PC の距離に応じて漏洩対策を行い，距離の測定方法として Bluetooth の電波受信強度を利用した．

Bluetooth による距離の測定では，得られた結果から，利用が可能であることが確認できた．しかし，電波受信強度の取得がタイミングによってできない場合があり，今回行った方式では距離のリアルタイムの測定は難しいといえる．

システム全体では距離のリアルタイムの測定を除き，サーバの動作は今回の構成で問題なく動作をすることが確認できた．

5.2 今後の課題

今回実装したシステムの課題点として，距離のリアルタイムの測定は今回の方式では難しいため，今後は，距離測定専用の API の開発が必要である

また今回実装したシステムは，PC がサーバと通信し，漏洩対策の方法を受け取るところまでの動作を行った．今後 PC がサーバから受け取った漏洩対策を実際に実行するように，PC の実装とサーバとの連携を行う．

さらに，今回は来客が 1 人，PC が 1 台の環境で検証を行ったが，実際のオフィス環境を考えた場合，来客は複数人の場合や種類の異なる来客が同時にくる可能性がある．さらに，PC は複数台ある場合が一般的である．今後，そういった場合を想定した漏洩対策の方法の検討や，来客の検知方式の検討を行う．

さらには，オフィスだけでなく，さまざまな環境を想定したダイナミックなセキュリティ制御方法を検討する．

謝辞

本稿の作成にあたりご協力頂いた皆様に感謝申し上げます．ご尽力いただきありがとうございました．

参考文献

[1] 鳩原恵二, 浅川浩, “図解 よくわかる ISMS とプライバシーマーク”, 日本実業出版社, 初版発行(2004.10.10)
[2] 情報マネジメントシステム推進センター, http://www.officegate.jp/security/
[3] ジョゼフ・コバラ, 夏井高人, 細谷僚一, 青木裕, 武藤弘和, 小山覚, 西山敏雄, 森慎一, 大沢彰, “NTT コミュニケーションズ新・情報セキュリティ対策ガイドブック　.com Security Master”, NTT 出版, 第 1 版第 1 刷発行(2004)
[4] 技術委員会監修, “近距離無線①　（総論・Bluetooth）”, http://www.qiaj.jp/pages/frame20/docs/handbook-shortradio-01.pdf
[5] 佐藤智美, 小宮山哲, 下田雅彦, 劉渤江, 横田一正, “Bluetooth の電波強度を用いた位置推定方式の検討”, DEIM Forum 2011 B9-4, http://db-event.jpn.org/deim2011/proceedings/pdf/b9-4.pdf

Copyright © 2012 by
The Instiute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan　All rights reserved.