Vol.2013-DPS-154 No.25
Vol.2013-CSEC-60 No.25
2013/3/14

侵入者の距離によりダイナミックにセキュリティレベルを制御するシステムの検討

末次 正人†1　榎本 真也†1　金井 敦†1　谷本 茂明†2　佐藤 周行†3

近年、情報の守秘管理が重要視されている。一般的に安全の確保についてはリスクが最も高い状況を想定し、安全性を保っている。一方で、時間や場所によりセキュリティレベルは変化するため、リスクが小さい場合はセキュリティレベルを下げて管理することで可用性が良くなる。そこで本論文では、距離から脅威の状況を検知し、変化するセキュリティレベルに対応した端末の制御機能を検討し、実装し、機能を確認した。

A study on method to control security level dynamically from distance of intruder

MASATO SUETSUGU[†1]　SHINYA ENOMOTO[†1]　ATSUSHI KANAI[†1]
SHIGEAKI TANIMOTO[†2]　HIROYUKI SATO[†3]

In recent years, importance is attached to confidentiality management of information. About reservation of safety, safety is kept general supposing the highest-risk situation. On the other hand, since a security level changes with time or places, when a risk is small, availability becomes good by lowering and managing a security level. So, in this paper, a threatening situation is detected from distance and the control system which protects the security level of a system dynamically is examined according to a risk level.

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].

利用者の状況を考慮した対策を行うことで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，利用者の状況を考慮し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端末方式を提案する．

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，制御端末方式について検討した結果について述べる．

一般的にセキュリティレベルに応じた対策を行うことで情報の安全性を確保できる．しかしながら，この対策を行うことで不利益を被る状況も存在する．例えば，ファイルを使用している時，安全性を確保するためファイルの保存をせず，強制的にファイルを閉じてしまうと作業を進めることが出来なくなる．すなわち，セキュリティレベルだけでなく利用者の状況に応じた制御が必要である．従って，利用者の状況に応じた制御を行うことで利便性を良くすることが可能になると考えられる．

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及び具体例

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．

†1 法政大学
Hosei University
†2 千葉工業大学
Chiba institute of Technology
†3 東京大学
Tokyo University

ⓒ 2013 Information Processing Society of Japan

(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．

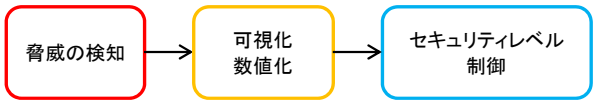

図 1：セキュリティダイナミック制御のコンセプト

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．

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たりす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，音を消したりする．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：エンドユーザ端末のセキュリティ制御

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
	フォルダをロックする
	ファイルを閉じる
	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．

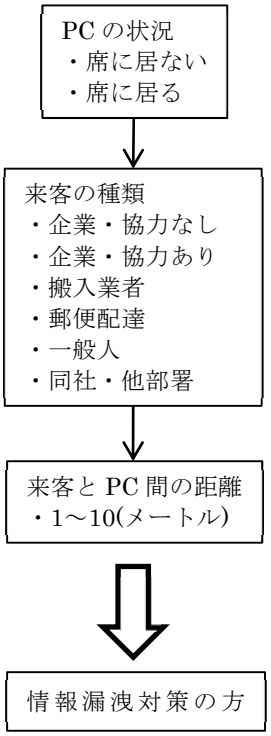

図 2　情報漏洩対策の方法の決定までの流れ

3. 実現方式

3.1 制御システムの全体像

システムの全体像を図 2 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．

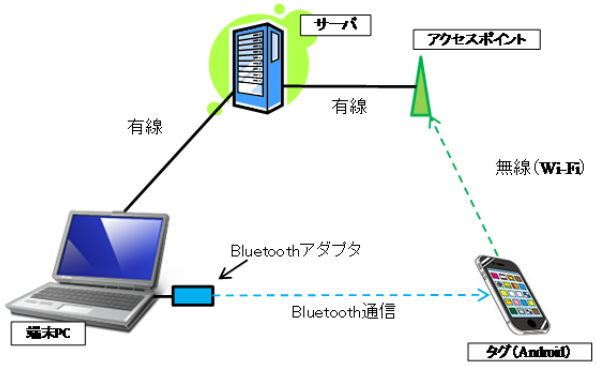

図 2：システムの全体図

3.2 PC のシステム構成

PC のシステム構成を図 3 に示す．さらに，以下にシステムの説明を記す．

・クライアント

一般的な企業のオフィスで使用されることを想定し，常に PC を使っていないものと想定する．

・PC

[App－test01]

クライアントが PC を使用しているかを判断するため，マウスやキーボードの入力を利用する. PC がクライアントの入力信号を監視し，席の状況をサーバに送信する．送信した情報とサーバに保管されている情報から計算処理を行った後，漏洩対策，来客の種類，来客者と PC 間の距離の情報を受け取る．受け取った情報を元に状況に応じた制御を実行する. なおリアルタイムに席の状況を判断するため, これらの動作を一定秒毎に繰り返す.

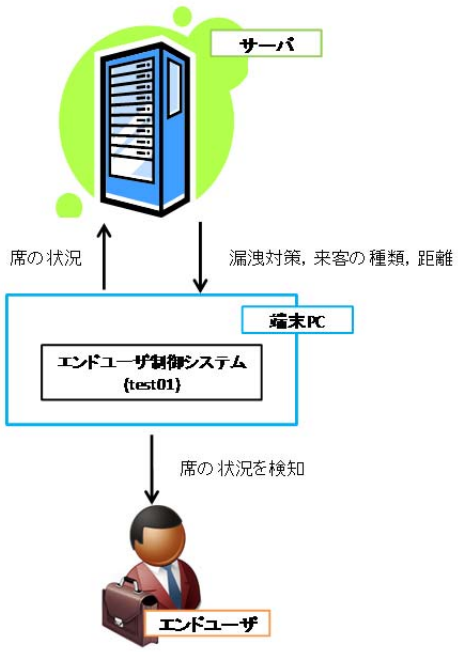

図 3：エンドユーザ制御システムの構成図

ⓒ 2013 Information Processing Society of Japan

3.3 エンドユーザ制御システム

ここでは，2.2 の表 2 エンドユーザ端末のセキュリティ制御について，ユーザの状況に応じた制御アクションについて示す．

3.3.1 エンドユーザ制御システムの制御の視点

ここでは、エンドユーザ制御システムの制御要件について述べる．表 2 のセキュリティ制御をダイレクトに行うとユーザにとって不都合な状況がある．そこで，制御を行うにあたり，制御アクションを行うと問題がある状況，制御アクションを行わないと問題がある状況について考える．また，利用者がいる状況といない状況によっても状況が変化すると考えられる．そこで，表 3 に制御アクションと利用者の状況の特徴を示す．

表 3　制御アクションと利用者の状況の特徴

	利用者がいる	利用者がいない
制御する	・操作できる ・来客を監視できる ・情報漏洩の危険性低下 ・利便性低下	・操作できない ・来客を監視できない ・情報漏洩の危険性低下 ・利便性低下
制御しない	・操作できる ・来客を監視できる ・情報漏洩の危険性上昇	・操作できない ・来客を監視できない ・情報漏洩の危険性上昇

3.3.2 エンドユーザ制御システムの問題点

表 3 制御と利用者の状況の特徴から各制御内容の問題点を表 4 から表 7 に示す．表 4 には制御アクションを行い，かつ利用者がいる状況の問題点，表 5 には制御アクションを行い，かつ利用者がいない状況の問題点，表 6 には制御アクションを行わず，かつ利用者がいる状況の問題点，表 7 には制御アクションを行わず，かつ利用者がいない状況の問題点について示す．

表 4　制御アクションを行う状況(利用者がいる)

		PC の状況
		利用者がいる
制御内容	電源を切る	・ファイルが保存できない ・ダウンロード中のファイルが中断される ・アップロード中のファイルが中断される
	USB ポートの使用禁止	・USB のデータを転送中できない ・自身のデバイスを接続できない
	ディスプレイを消す	・画面を操作できない ・動画を見られない
	通信を切断	・インターネットを使用できない ・ダウンロード中のファイルが中断される ・アップロード中のファイルが中断される ・サーバから制御命令を受信できない
	フォルダをロック	・ファイルを保存できない ・ダウンロード中のファイルが中断される ・アップロード中のファイルが中断される ・ファイルを閲覧できない
	ファイルを閉じる	・ファイルを保存できない ・ファイルを閲覧できない
	音を消す	・警告音を出せない ・通知音を出せない ・音楽を聞けない
	来客を通知	なし

表 5　制御アクションを行う状況(利用者がいない)

		PC の状況
		利用者がいない
制御内容	電源を切る	・ファイルを保存されない ・ダウンロード中のファイルが中断される ・アップロード中のファイルが中断される
	USB ポートの使用禁止	・USB のデータを転送中できない
	ディスプレイを消す	なし
	通信を切断	・ダウンロード中のファイルが中断される ・アップロード中のファイルが中断される ・サーバから制御命令を受信できない
	フォルダをロック	・ファイルを保存できない ・ダウンロード中のファイルが中断される ・アップロード中のファイルが中断される
	ファイルを閉じる	・ファイルを保存できない
	音を消す	なし
	来客を通知	なし

表 6　制御アクションを行わない状況(利用者がいる)

		PC の状況
		利用者がいる
制御内容	電源を切る	なし
	USB ポートの使用禁止	なし
	ディスプレイを消す	・来客が機密情報を閲覧できる
	通信を切断	なし
	フォルダをロック	なし
	ファイルを閉じる	・来客が機密情報を閲覧できる
	音を消す	・来客が機密情報を聞くことができる
	来客を通知	・危険が迫っていることに気が付かない

表 7　制御アクションを行わない状況(利用者がいない)

		PC の状況
		利用者がいない
制御内容	電源を切る	・来客がパスワードロック解除して，不正アクセスできる
	USB ポートの使用禁止	・来客がデバイスを接続できるため，機密情報を持ち出せる
	ディスプレイを消す	・来客が機密情報を閲覧できる
	通信を切断	・来客が外部に機密情報を送信できる ・来客が社内サーバへアクセスできる
	フォルダをロックする	・来客が機密ファイルを開くことができる
	ファイルを閉じる	・来客が機密情報を閲覧できる
	音を消す	・来客が機密情報を聞くことができる
	来客を通知	・危険が迫っていることに気が付かない

ⓒ 2013 Information Processing Society of Japan

3.3.3 エンドユーザ制御システムの解決策

3.3.2 エンドユーザ制御システムの問題点の解決策とその理由を表 8，表 9 に示す．表 8 に利用者がいる状況の解決策とその理由，表 9 に利用者がいない状況の解決策とその理由を示す．ただし，太字で表示した部分は既存のシステムで制御を行う．

表 8　利用者がいる状況の解決策とその理由

		解決策	理由
制御内容	電源を切る	・ダミー画面（スクリーンセーバーなど）を表示する **・ファイルを保存するか選択させる** **・ファイルのダウンロードを続行するか選択させる** **・ファイルのアップロードを続行するか選択させる**	・ダミー画面を表示することで覗き見を防止 ・ファイルの終了や保存，転送を利用者が状況に応じて選択してから電源を切ることができる
	USB ポートの使用禁止	**・データの転送を継続するか選択させる** ・デバイス（USB，スマホ等）を接続するか選択させる	・データ転送を継続できる ・接続するデバイスを選択できる
	ディスプレイを消す	・ダミー画面（スクリーンセーバーなど）を表示する ・ディスプレイを消すか選択させる	・ダミー画面を表示することで覗き見を防止 ・状況に応じて作業を継続できる
	通信を切断	・サーバとの通信は継続する ・Port を制御し，データの通信を続行するか選択させる	・漏洩対策を継続しながら，通信を制限できる
	フォルダをロック	・ダミー画面（スクリーンセーバーなど）を表示する ・フォルダのアクセス権を制御し，ロックするか選択させる **・ファイルの転送を続行するか選択させる**	・ダミー画面を表示することで覗き見を防止 ・フォルダへのアクセスを 利用者が状況に応じて選択できる
	ファイルを閉じる	・ダミー画面（スクリーンセーバーなど）を表示する ・ファイルを閉じるか選択させる **・ファイルを保存するか選択させる**	・ダミー画面を表示することで覗き見を防止 ・ファイルの終了や保存を 利用者が状況に応じて選択できる
	音を消す	・マスタ音量をミュートにするか選択させる	・音量を利用者が状況に応じて選択できる
	来客を通知	・通知画面を表示する	・利用者に危険を知らせる

表 9　利用者がいない状況の解決策とその理由

		解決策	理由
席を離れた時		・パスワード付きのダミー画面を表示する	・覗き見，不正アクセスを防止
制御内容	電源を切る	・危険な状態が一定時間継続した場合，電源を切る	・不正アクセスを防止
	USB ポートの使用禁止	・デバイスの変更を検知し，新しく検知したデバイスの使用を禁止する	・マウスやキーボードは使える状態を保ち，デバイスを用いた情報漏洩を防ぐ
	ディスプレイを消す	なし	・席を離れた時にダミー画面を表示しているため，操作は行わない
	通信を切断	・サーバとの通信は継続する ・一定時間待機した後，サーバ以外の通信 Port を閉じる	・漏洩対策を継続しながら，通信を制限できる
	フォルダをロック	・特定のフォルダのアクセス権を制御し，ロックする	・システムフォルダなど重要なフォルダをロックしないように
	ファイルを閉じる	・開いているファイルを閉じる	・覗き見を防止
	音を消す	・マスタ音量をミュートにする	・音による情報漏洩を防止
	来客を通知	・警告音を出す	・周囲に危険を知らせる

4. 実装と考察

今回，ダイナミックに制御する端末システムの動作の考察を行う．表 8，表 9 を元にシステムを構築する．

4.1 システムの実装

今回提案するシステムを実装し，その動作の確認を行う．表 10 にサーバの環境，表 11 に PC の環境を示す．

動作は 3.3.1 で説明した流れで動作する．今回は PC の状況をサーバに送信し，サーバからの情報漏洩対策に動的に対応できているか確認を行う．

そのための条件として，来客は「企業・協力なし」，距離は 1~10 の値を手動で入力する．「PC の状況」の検知は 10 秒毎に行い，1 分間入力が検知されなければスクリーンセーバーを起動する．

表 10　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 11　端末 PC の環境

端末 PC	開発環境
OS	windows 7
開発環境	.NET Framework
使用言語	Visual Basic

ⓒ 2013 Information Processing Society of Japan

4.2 システムの考察

利用者がいる状況では，状況に応じて制御を選択させることで利便性を向上させた．しかし，利用者がいない状況では制御内容を選択できないため，利用者の状況による選択肢が少なく，強制的に制御を行う状況が多かった．そのため今後は，より詳細な状況を検知することが必要である．例えば画像認識を用いることで，自動で覗き見を防止やスクリーンセーバーの解除を行ったりできる．

今回，システムの機能毎に動作の確認を行った．状況に応じた漏洩対策の方法を得ることができたため，エンドユーザ制御システムの動作は現在問題なく動作することが確認できた．図 4 に実行画面を示す．

図 4：エンドユーザ制御システムの実行画面

5. おわりに

5.1 まとめと今後の課題

ダイナミックに端末を制御するシステムを構築した．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，その端末システム方式について検討を行った．

今回利用者がいる状況では，状況に応じて制御を選択させることで利便性を向上させることが確認できた．しかし，実際の環境で制御するには不十分であるため，機能の拡張が必要である．システムの動作では，エンドユーザ制御システムは今回の構成では問題なく動作することが確認できた．

今後の課題として，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．

また，今回は距離測定に Bluetooth を用いたが，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，リアルタイムの測定は困難であることがわかった．そのため，将来的には RF タグなどを用いた来客の検知方法を検討する．

謝辞

本研究は JSPS 科研費 24300029 の助成を受けたものです．

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
6) 榎本真也,金井敦,谷本茂明,佐藤周行，“ダイナミックに制御する情報漏洩対策システムの検討”

ⓒ 2013 Information Processing Society of Japan