偽装環境によるPC保護と不正操作者情報収集技術の提案

上村 宗嗣† 金井 敦† 谷本茂明†† 佐藤周行†††

† 法政大学大学院 †† 千葉工業大学 ††† 東京大学

あらまし PC を攻撃者から防御する一般的な方法は，侵入を防ぐことにより攻撃者の攻撃を遮断する戦略がとられている．しかし，この方法では，防御はできるが攻撃者の意図や情報を得ることができない．そこで，あえて通常の環境に見せかけた偽装環境に侵入させることにより，侵入目的や攻撃者の情報を得ること可能とする防御方式を提案する．本研究では PC が攻撃を受ける可能性が高いと判断した場合や正規利用者の指示により，攻撃者に偽装環境を提供し操作させ，攻撃者の情報を収集可能なセキュリティモデルを考案し，実装した．

A Methodology to preserve PC security and obtain malicious user information using disguised OS

Munetsugu Kamimura† Atsushi Kanai†

Shigeaki Tanimoto†† Hiroyuki Sato†††

†Hosei University Graduate School
††Chiba institute of Technology †††Tokyo University

Abstract The usual way to protect PC information is that PC requires password not to be operated by a suspicious user. However, we cannot obtain the malicious user's information by the above technique. This paper presents the methodology to obtain the malicious user's behaves as well as to preserve PC security by using disguised OS. A prototype is developed and the methodology is evaluated.

1. はじめに

ある情報を外敵から防御する事を考えた時，セキュリティレベルが高いほど安全性は高くなるが，その分情報の利便性は低下してしまう．もし対象物の回りに外敵の存在が無い場合，セキュリティレベルを高く設定する事は無駄であり，単に利便性を損ねる結果となる．ゆえに，防御対象が置かれた環境によってセキュリティレベルを変化させることで，セキュリティの可用性を高める事が可能である．安全性を保持したまま可用性を上げる方法として，攻撃者の接近を検知して動的にセキュリティレベルを変更する方法が提案されている[1]．この方法は，ユーザが PC の前にいない状況で攻撃者が最も接近した際に電源を切ることで防御を行なっている．しかし，攻撃者が PC に接近し操作する事は，攻撃者の容姿や攻撃意図を収集する最大の機会であり，単にコンピュータの電源を切るだけでは攻撃者の情報を得ることは出来ない．そこで本研究で

は，攻撃者からの PC 保護と同時に攻撃者特定のための情報収集を行うセキュリティモデルと方式を提案する．

2. 基本コンセプト

提案するセキュリティモデルは攻撃者の情報収集という点で，情報収集モデルであるハニーポットと共通する部分がある．本章ではまずハニーポットの概要及びハニーポットと今回の環境との違いについて述べる．次に今回の環境で想定する攻撃者を定義し，最後にモデルが満たすべき要件，基本コンセプトについて述べる．

2．1 ハニーポットと提案モデルの関係性

2．1．1 ハニーポット

ハニーポットは有用な情報が入っていると思わせる端末をネットワーク上に設置し，セキュリティ的に脆弱で侵入が容易であるように振る舞い，侵入者の侵入手法や攻撃手法，侵入後の内部動向を記録し解析するものである．ハニーポットの中には以下のような種類が存在する[2].

(1) 高対話型：攻撃者が OS の機能を直接操作可能である．攻撃者が可能である操作が多いため得られる情報が多いがリスクは大きい．

(2) 中対話型：高対話型の機能を一部利用不可にし，攻撃者の行動を制限してリスクを抑える．行動を制限する分得られる情報は少なくなる．偽装を施す事で行動制限の露呈を防ぐ手法[2]も存在する．

また，ハニーポットの中に仮想ハニーポットと呼ばれる種類がある． 仮想ハニーポットは仮想マシン上で OS を動作させ攻撃者に操作させることで攻撃者の情報を比較的安全に収集する事が可能であるが，仮想マシンである事が攻撃者に看破されてしまう可能性がある．

2．1．2 ハニーポットと本研究の環境の違い

ハニーポットはネットワークで用いられるモデルであるが，本研究は現実空間でのセキュリティを目的としている．従来のハニーポットが設置される環境と今回の環境では，以下の点で異なる．

(1) 攻撃者が操作から得られる情報の差

一般的に，ハニーポットへのクラッキングはツールを用いて行われる．しかし，今回の環境は現実空間であり，攻撃者は PC を直接操作する．そのため，視覚要素や操作感から PC が保護された状態であることを看破されないようにする必要がある．

(2) 利用形態の違い

ハニーポットは攻撃者の攻撃手法の解析などを主とした目的で用いられ，情報収集に特化した動作のみを行う．しかし，今回は PC 保護の付加価値として情報の収集を行うため，PC は正規ユーザによる通常利用も可能でなくてはならない．

2．2 攻撃者の定義

今回想定する攻撃者の種類は以下の 3 種類である．

(1) 操作対象の PC に保存されている情報の窃盗を目的とする者

(2) 操作対象の PC の内部的破壊を目的とする者

(3) 操作対象の PC が属するネットワーク上のアクセス可能な PC への侵入を目的とする者

2．3 モデルの満たすべき条件とコンセプト

ここで，今回の提案モデルが満たすべき条件を考える．まず，本研究の目的は防御と情報収集の両立であるため，以下の2つが要求される．

(1) 攻撃を受ける PC と，その同一ネットワーク上の PC が保護される

(2) 攻撃者の情報が収集可能である

また，2．1．2より以下の二点が要求される．

(3) 攻撃者に操作させる過程で PC 保護，情報収集が動作した状態である事を看破されにくい

(4) PC が正規利用と攻撃者の情報収集利用の両方を行うことが出来る

最後に，運用する上でユーザが使いやすい事は重要であるため，これも満たすべき条件に含む．

(5) ユーザが運用しやすい

これらの条件を満たすために，本研究では，PC が攻撃を受ける危険性が高い際に，仮想マシンアプリケーションを用いて情報収集機能を持つ偽装環境を起動し，攻撃者に操作させる方式を提案する．提案する方法のコンセプトを図1に示す．図1(b)で攻撃者が操作するのは，高対話型仮想ハニーポットという分類になる．

3．偽装・防御・情報収集方式

本章では攻撃者に提示する偽装環境について記す．3．1では，2．3の条件(3)を満たすため，情報収集完了までに看破されにくい偽装環境の構築方式について述べる．3．2では，2．2で想定した攻撃者に偽装環境を操作させる際に，2．3の条件(1)，(2)を満足するよう，攻撃者ごとに PC 保護，情報収集の方法を考える．

3．1 偽装環境の構築

攻撃者が偽装環境である事を看破する可能性は，攻撃者の「攻撃対象 PC でどのような作業が行われているか」という知識に依存する．看破を防止するためには，攻撃者に操作させる偽装環境を実環境と似せた環境にすべきである．今回の方式では実環境の情報の一部を偽装環境で利用することで偽装性を向上させる．今回偽装環境で利用する情報は以下の通りである．

(1) 漏洩が生じても正規ユーザに害が無いファイルの内容全て

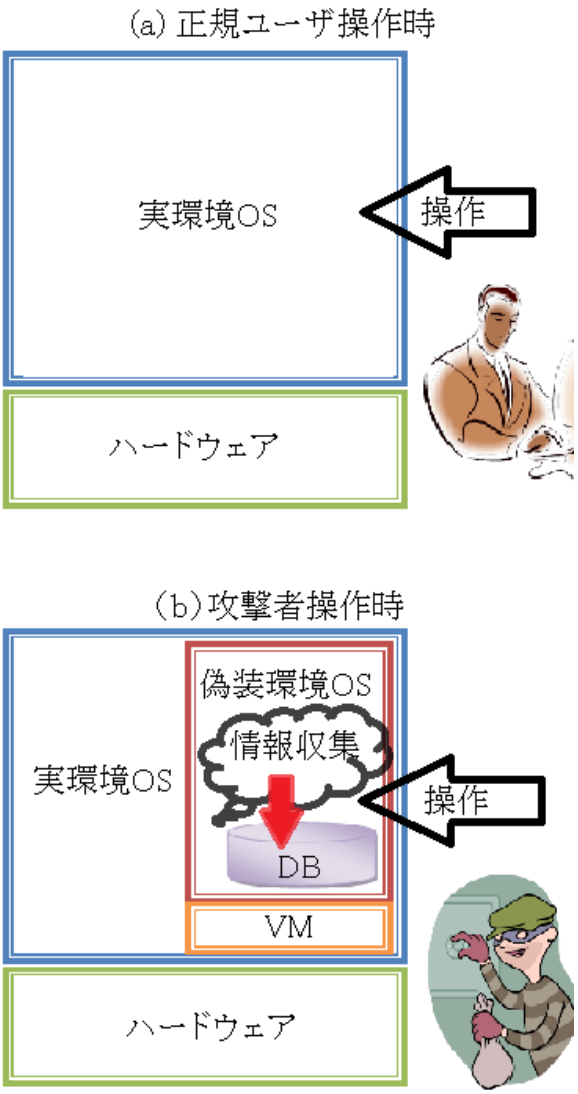

図1 提案手法のコンセプト

(2) 内容を漏洩させる事が出来ない重要なファイルのファイル名

(3) (1)，(2)が格納されるディレクトリの構成

(2)は重要ファイルと同名の，内容が偽装されたファイルを作成することで実現する．

3．2 攻撃者に対する防御，情報収集

以下では，3．1で構築した偽装環境を用いて，想定する攻撃からの防御，攻撃者の情報収集を行う手法について記す．

3．2．1 共通の情報収集

想定した全ての攻撃者について収集可能な情報として，攻撃者の画像が収集可能である．

PC を不正操作する場合，攻撃者は PC に近い位置に一定時間留まるため，攻撃者の画像の収集は容易である．

3．2．2 操作対象 PC に保存されている情報の窃盗

PC 内部の情報窃盗を目的とする攻撃は，情報が盗まれた場合正規ユーザに不利益が生じるファイルへアクセスさせない事で PC が保護されると言える．情報漏洩について，3．1で構築した偽装環境には，防御対象となるファイルのファイル名のみしか存在しないので，攻撃対象 PC は保護された状態である．

攻撃者が窃盗の目標とするファイルが判明すれば，攻撃者の攻撃目的が分かる．3．1で構築したファイル・ディレクトリの構成は，重要なファイルの内容以外実環境と同じものであるため，攻撃者が偽装環境でアクセスしたファイルを記録することで攻撃目的の収集が可能となる．

3．2．3 操作対象 PC の内部的破壊

マルウェアを仕掛ける，情報を改ざんするなどの内部破壊への防御は，偽装環境内部の破壊が実環境に影響を及ぼさないため，偽装環境を利用させる事で PC の保護が成されている．

攻撃者情報の収集は，操作履歴を保存する事による破壊が行われた箇所の特定，仕掛けられたマルウェアの解析を行う事で攻撃目的の特定が可能である．

3．2．4 操作対象 PC と同一ネットワーク上の他 PC への攻撃

ネットワーク上の PC への攻撃の防御は，攻撃者が操作する PC をネットワークから切り離す事で実現する．今回のモデルは PC 保護と攻撃者情報の収集を両立するものであるが，前提として攻撃対象の PC 及び同一ネットワーク上の PC が保護されていなければならない．そのため，収集可能な情報が減少する事を許容し，攻撃者に操作させる偽装環境をネットワーク的に独立させる事で PC 保護を実現する．

ネットワークを独立させた場合，攻撃者が可能な動作は少なく，情報収集が完了する前に偽装環境であることを看破される可能性が高い．しかし，攻撃者が攻撃に利用するツールを USB メモリ等の外部記憶媒体を経由して導入するなど，有用なものが取得出来る可能性がある．

3．2．5 収集した情報の格納

偽装環境を用いて収集した情報を保存するために，偽装環境内部に攻撃者情報の格納データベースを用意する．データベースは攻撃者にアクセスされにくいよう，操作者が通常意図的にアクセスしない場所に配置する．よって，攻撃者がデータベースにアクセスする時，攻撃者は偽装環境であることを看破しているとみなす．

4．動作方式

4．1 PC の状態による動作の切り替え

2．3の(4)を満たすためには，実環境と偽装環境を切り替えるための条件を設定する必要がある．今回は，PC の置かれる状態を3つに分類し，状態の遷移によって PC の稼働形態を切り替える．以下に分類した状態の内容と，その時の稼働形態について記す．

(1) セーフティ状態
正規ユーザが PC の前にいる状態である．この時 PC で操作可能なのは実環境である．

(2) スタンバイ状態
正規ユーザが席を離れ，攻撃者が PC の操作を行なっていない状態である．この時 PC では偽装環境が動作するが，情報収集動作は開始しない．

(3) アラート状態
攻撃者が PC の操作を行う状態である．アラート状態で操作可能であるのは偽装環境であり，アラート状態となった PC は偽装環境による情報収集動作を行う．攻撃者が攻撃者情報データベースにアクセスした時，収集した情報が改ざんされる事を防ぐため，PC の電源を切る．

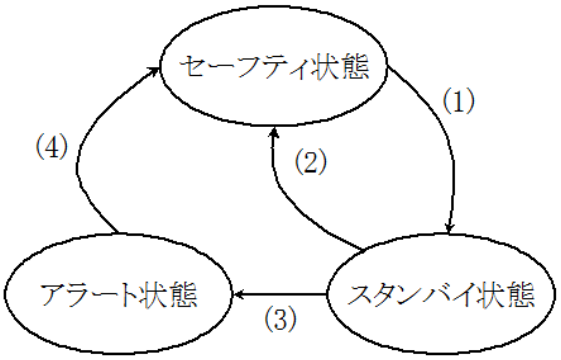

図2 PC の状態遷移図

3つの状態は図2の状態遷移図に従って，その状態が移行する．状態遷移が発生する時の動作について以下に記す．

(1) 正規ユーザが PC の前から離れる．この時 PC 上では偽装環境が起動する．

(2) 正規ユーザが席を離れている間に攻撃者が現れず，正規ユーザが再びPCの前に戻るとき，PC 上の偽装環境が終了する．

(3) 正規ユーザが席を離れている間に攻撃者が PC の操作を行うとする．この時攻撃者が操作可能であるのは偽装環境である．PC は偽装環境を用いた情報収集を開始する．

(4) 攻撃者が攻撃を完了し，席を離れている時，正規ユーザは偽装環境の状態を保存し，PC をセーフティ状態に戻す．

4．2 実環境情報と偽装環境情報の同期

偽装環境で用いる実環境の情報は，アラート状態で攻撃者が偽装環境を操作する時点で最新のものであることが望ましい．そのためにはセーフティ状態で偽装環境を更新する必要がある．2．3の条件(5)は，ユーザがファイルの同期について意識しない事で満足する．今回は，正規ユーザが偽装環境で利用する実環境情報をディレクトリ単位で指定し，指定されたディレクトリ内部のファイルの追加，更新，削除を記録し一定時間毎に偽装環境と同期する手法を用いた．選択したディレクトリ内に存在する重要ファイルは，内容の偽装を行うためディレクトリ選択とは別に重要ファイルであることを指定する必要がある．

5．実装

本章ではここまでの内容を用いてセキュリティシステムを実装する．セキュリティシステムは実環境と偽装環境に Microsoft .NET Framework 及び Python 2.7 が導入されている環境上で動作するよう実装した．また，偽装環境として仮想マシンアプリケーションである VMware Player を用い，攻撃者にフルスクリーン状態の VMware Player を操作させることで提案動作を実現した．PC の状態遷移を実現するため，システムの利

表1 各状態における常駐アプリケーションの主要な動作

	実環境常駐アプリケーション	偽装環境常駐アプリケーション
セーフティ	偽装環境への環境更新指示 正規ユーザの検出 スタンバイへの状態遷移	実環境の指示による偽装環境の更新
スタンバイ	正規ユーザ及び攻撃者の検出 セーフティ及びアラートへの状態遷移	状態遷移発生まで待機
アラート	攻撃者の撮影 PC の終了	操作ログの収集

用者はコントローラとして Android 端末を持つとする.

今回の実装では，実環境と偽装環境でそれぞれ常駐アプリケーションを動作させることでモデルの動作を実現した．表1に各常駐アプリケーションの主要な動作について記す．以下に，各状態の実装について記す.

5．1 セーフティ状態の実装

セーフティ状態で偽装環境に存在するユーザが指定したファイルを実環境の最新状態の内容に更新する動作について，本実装では更新を行う際に偽装環境である仮想マシンアプリケーションを一時的に立ち上げ，実環境常駐アプリケーションと偽装環境常駐アプリケーション間で通信を行い，偽装環境のディレクトリ構成とファイル内容を実環境常駐アプリケーションが指示する内容に更新する．更新する内容は，ユーザが指定したディレクトリの内容を前回更新時の内容と比較することで指示情報を作成し，偽装環境へ指示情報とファイルデータを送信する.

また，セーフティ状態からスタンバイ状態への状態遷移は，席を立つ際に正規ユーザが Android 端末を操作し，通信によって指示を PC に送ることで遷移する．状態遷移した時 PC 上ではスクリーンセーバーが作動し，PC の状態は視認できなくなる.

5．2 スタンバイ状態の実装

システムがスタンバイ状態に移行した時，実環境上では偽装環境である VMware Player が稼働する．スタンバイ状態では正規ユーザの帰参及び攻撃者出現の検出を行い，それによってシステムの状態が遷移する．正規ユーザの検出はセーフティ状態と同じく正規ユーザの持つ Android 端末からの指示によって検出する．正規ユーザが席に戻る事を検出する時，システムは VMware Player を終了し，PC はセーフティ状態に戻る.

攻撃者の検出はスタンバイ状態で PC が操作された際に検出と判断される．この状態では攻撃者が操作可能であるのは実環境上で動作する偽装環境である．攻撃者を検知した後システムはアラート状態へ遷移する.

5．3 アラート状態の実装

アラート状態での攻撃者情報の収集動作について，今回の実装では攻撃者の画像情報，攻撃者の操作履歴の収集を行った．まず実環境常駐アプリケーションでは攻撃者の顔画像を取得するため，PC に接続されたカメラを用いて攻撃者の撮影を行う．情報の正確性を得るため，画像の撮影は一定時間毎に実行する．次に，偽装環境では攻撃者の操作履歴を収集するためキーロガーとプロセス履歴記録アプリケーションを稼働させ，収集した情報を攻撃者情報のデータベースに保存する.

攻撃者情報データベースへのアクセスを検知した時，情報の改ざんを防ぐため，偽装環境常駐アプリケーションは VM 上の OS をシャットダウンする．実環境は VM のシャットダウンを検知し，PC をシャットダウンする.

6．評価

本章では，実装したシステムを表2の環境で動作させ，偽装環境の動作速度による偽装性能，システムのユーザビリティの2点から評価する.

6．1 偽装環境動作速度による偽装性能評価

実行する操作の速度が実環境と偽装環境で差がある場合，実環境と偽装環境で操作性に差が出るため，システムの偽装性能に大きく関わる．今回は実環境と偽装環境でアプリケーション

表2 システム動作環境

CPU	Intel Core i7-2600k
OS	Windows7 Professional 64bit
メモリ	8.00GB
VM 側 OS	Windosw7 Professional 32bit
VM 側メモリ	4.00GB

表3 実環境と偽装環境における各動作時間の比較

	実環境での動作時間	偽装環境での動作時間
アプリケーション起動時間	3.4 秒	3.6 秒
ファイルの転送時間 (236KB)	USB→PC 1 秒未満 PC→USB 1 秒未満	USB→PC 1 秒未満 PC→USB 2.1 秒
ファイルの転送時間 (48.1MB)	USB→PC 2.1 秒 PC→USB 4.7 秒	USB→PC 23.1 秒 PC→USB 37.4 秒
ファイルの転送時間 (1.27GB)	USB→PC 2 分 5 秒 PC→USB 1 分 37 秒	USB→PC 15 分 59 秒 PC→USB 15 分 56 秒

の起動時間，USB メモリ利用時のデータの転送速度を測定した，動作させるアプリケーションは Microsoft Office Word 2010 を用いた．USB メモリを用いて転送するデータは 236KB，48.1MB，1.27GB とサイズに差のある3つのデータについて USB メモリから環境への転送，環境から USB メモリへの転送速度をそれぞれ計測した．表3に実環境と偽装環境での操作実行時間を示す．

アプリケーションの起動時間は実環境と偽装環境で特に差はなく，偽装環境看破の要素になる事は無い．一方で USB と各環境とのファイル転送時間はファイルサイズによって大きく差が開いた．この結果から，今回の実装では，攻撃者が転送を行うファイルが大きくなるにつれて，偽装環境であることを看破する可能性が高くなる．

6．2 ユーザビリティによる評価

実装したシステムのユーザビリティについて，以下の項目から評価する．

1. 実環境から偽装環境への移行時間
2. 偽装環境から実環境への移行時間
3. 偽装環境作成のためにユーザが行う操作の煩雑さ

表4に環境の遷移にかかる時間を記す．ユーザが席を立つ時に実環境から偽装環境に切り替わる事で PC の保護がなされるが，環境の切り替えが完了するまではシステムが完全な状態で動作しない．今回の実装ではユーザが席を立つ動作をしてから約 40 秒間は VMware Player の起動を行う． OS をブートしている段階であっても攻撃者が操作可能なのは偽装環境のみなので PC の保護はなされるが，スクリーンセーバーが解除された時点で偽装環境だと看破される可能性が高い．今回の実装では，システムを完全な状態で動作させるためには，ユーザが席を立つ指示を送ってから約 40 秒間 PC から離れられないという運用上の制約が発生した．偽装環境から実環境への切り替えは約 15 秒であるため，ユーザが PC にある程度近い位置で状態遷移指示を行なっても PC の前に戻るまでにセーフティ状態への移行を完了できるので，この状態移行のユーザビリティは問題ないと言える．

表4 状態遷移時間

実環境から偽装環境への遷移	40.1 秒
偽装環境から実環境への遷移	14.8 秒

操作の煩雑さについて，今回の実装では，偽装環境で用いる実環境ファイルの情報はユーザが指定する．指定したディレクトリ下に新たな重要ファイルを作成する，または指定したディレクトリ下でない場所で別途同期したいディレクトリを作成する場合，ユーザが改めて同期する情報を設定しなければならないので，このような状況が頻繁に発生する環境での利用はユーザビリティが損なわれる．

7. 関連研究と今後の課題

(1) 攻撃者心理について

今回のモデルは攻撃者が PC に直接操作を行うため，攻撃者の置かれる環境によって，攻撃者の心理や動向が変化すると推測できる．特に今回は攻撃者が PC を直接操作するため，泥棒の犯罪心理[3]を適用し，攻撃者に与えられた時間や犯人の動向の詳細な設定が期待できる．また，情報セキュリティ心理学[4]の分野は本モデルの発展に大きく関わるものであるだろう．

(2) 収集した操作履歴の利用について

本研究では攻撃者の操作情報の収集を行ったが，収集した情報を用いた攻撃者の分析については行わなかった．今後，攻撃者の操作履歴を効果的に利用する分析方法について検討する．

(3) 提案手法について

今回提案したモデルは実環境の情報の利用を，ユーザにとって価値の無い情報を持つファイル，重要ファイルのファイル名，ディレクトリ構成といった漏洩しても被害が少ない物のみ認め，偽装環境のネットワークは孤立するものとした．これらから収集可能な情報は攻撃者の攻撃意図の大まかな部分に限られてしまい，詳細まで確認することは難しい．攻撃者の攻撃意図の詳細まで安全に解析可能とするには，重要ファイルの内容を意味のある偽装物にする，攻めこませても安全な仮想ネットワークを実装する事が求められる．

(4) 実装について

今回の実装で用いた仮想マシンアプリケーションは PC に高い性能を要求する．よって，性能が低い PC のための別な実装手法として，偽装環境にリモートデスクトップを用いてネットワーク上の別マシンで処理を行う手法が考えられる．

8. おわりに

本研究では偽装環境によって PC の保護と不正操作者の情報収集を両立するセキュリティモデルを提案し実装した．偽装環境に実環境の情報の一部を用いることで，偽装性能の向上，攻撃者の攻撃意図の収集を行った．本研究では仮想マシンアプリケーションを用いて提案手法を実装した．

謝辞

本稿の作成にあたりご協力頂いた皆様に深く感謝いたします．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]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”，情報科学技術フォーラム FIT 2012 講演論文集

[2]小泉芳，小池英樹，安村通晃，“行動制限型ハニーポットの改良方法の提案・実装・運用”，情報処理学会研究報告，2004 vol.129，pp.57-pp.62

[3]泥棒の心理と行動（安全暮らしマニュアル）http://anzen.fn69.com/home/archives/060/（アクセス日時 2012 年 8 月 22 日）

[4] 内田勝也，矢竹清一郎，森貴男，山口健太郎，東華枝，“情報セキュリティ心理学の提案”，情報処理学会研究報告，2007 vol.16,pp327-331