人物フォーメションを考慮した危険度定量化手法

本間, 博礼 / HONMA, Hironari

(出版者 / Publisher)
法政大学大学院理工学・工学研究科
(雑誌名 / Journal or Publication Title)
法政大学大学院紀要. 理工学・工学研究科編 / 法政大学大学院紀要. 理工学・工学研究科編
(巻 / Volume)
55
(開始ページ / Start Page)
1
(終了ページ / End Page)
7
(発行年 / Year)
2014-03-24
(URL)
https://doi.org/10.15002/00010499

人物フォーメーションを考慮した危険度定量化手法

An approach to quantify the degree of security risk considering formations of persons

本間博礼
Hironari HOMMA
指導教員　金井敦

法政大学大学院工学研究科情報電子工学専攻修士課程

Security control commensurate with the size of the risk is dynamically performed by detecting threats to information to be protected and measuring the risk dynamically from “visualize, quantify”. By doing so, it is possible to protect the information against threats we propose the concept of ensuring availability. In this paper, we propose a method by focusing on the placement of people in the office, this concept, to assess the risk level of your office PC, to be evaluated.

***Key Words** : Dynamic, Security, Threat, Evaluate*

１．はじめに

近年，個人情報保護法の施行に伴い，一般企業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，組織における情報セキュリティを管理するための仕組みである 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によって管理することで，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,それに見合った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り，可用性が悪くなる．そのため，情報の利便性が損なわれる．しかし，実際のリスクはその場の状況によって変化する．例えば，保護するべき情報の周りに部外者が居る場合と居ない場合とでは実際のリスクは異なる．そこで，リスクが小さいときはそれに合わせ，セキュリティレベルを下げて管理することにより，可用性を向上させ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行うことで,安全性を確保した状態を維持しながら,同時に可用性も確保できると考えられる[4]．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る際に、まずセキュリティレベルを決定するための基準が必要となる．本論文では，この基準を時々刻々と変化する脅威の大きさからダイナミックに定量化する手法を提案する．

一般的に，情報システムにおいてセキュリティを確保する場合，考慮すべき脅威は，ネットワークを経由した攻撃や部外者の侵入など，バーチャルからリアルまで様々な脅威が存在する[5]．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，上記のコンセプトをもとに，一例として，一般企業のオフィスへの来客訪問というリアルな環境を想定し，複数人いる来客と社員のオフィスでの立ち位置による危険度の定量化手法を提案する．

具体的には,保護するべき情報は企業のオフィス内に設置された PC からアクセスできるものに限定する．さらに，オフィス内に複数人の来客と社員がランダムな位置に存在することを想定する．その条件下で，PC と来客と社員の位置関係から危険度を定量化する手法を提案し，それを評価する．

２．ダイナミックにセキュリティを制御する手法のコンセプト及び具体例

ここでは，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に関して述べる．一般に脅威の状況は時々刻々と変化しているため，図 1 に示すように，その状況を検知し，可視化し，制御することをダイナミックに行うことが本概念の基本コンセプトである．

以下に図 1 で示した「脅威の検知」，「可視化・数値化」，「セキュリティレベルの制御」の三つの要素について記述する．

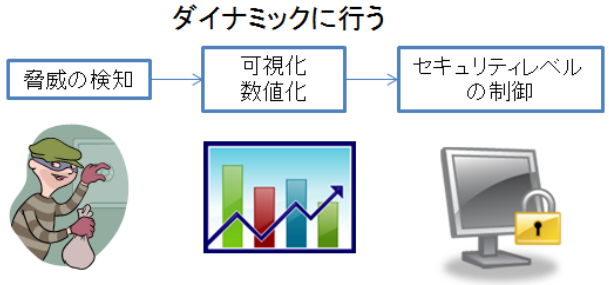

図 1　ダイナミックにセキュリティレベルを制御する手法のコンセプト

1) 脅威の検知

対象となる場において，保護するべき情報に対する脅威をリアルタイムに検知する．例えば，IDS によってネットワークを流れるパケットを観察し，不正アクセスと思われるパケットを検出することや，入退室管理システムによって侵入者の入室を発見することなどが挙げられる．センサの設置やシステムの導入など，事前に検知のための準備が必要とされる．

2) 可視化・数値化

(1)で検知した脅威を人が理解しやすいように示す．例えば，脅威によってリスクが生じる箇所を特定し，もしくはリスクが生じる可能性のある範囲を特定し，それを示すことや，脅威をリスクの大きさに応じて数値化し，適切な指標とともに表示することなどが挙げられる．

3) セキュリティレベルの制御

脅威を，(2)の内容通り「可視化・数値化」したものを基準にして，システムのセキュリティレベルをダイナミックに制御する．このとき，セキュリティレベルは段階的に分けられていることが前提となり，「可視化・数値化」したものと各段階のセキュリティレベルを対応付ける必要がある．さらに，セキュリティレベルに応じたシステム制御が行われることで，脅威への対策が完了する．システム制御の具体例は，ファイアウォールのポリシー変更や，資産価値の大きな情報の別サーバへの退避，システムのシャットダウンなどが挙げられる．その際，緊急対応時に業務が中断してしまうなどの利便性の低下は許容する．

本論文では，上記の三つの要素のうち，(1)の「脅威の検知」は理想的に行われるものと仮定し，(2)の「可視化・数値化」についての提案を行う．具体的には，検知した脅威の大きさを定量化する手法を提案する．脅威の大きさをこれ以降「危険度」と呼び，危険度の定量化手法について記述する．

３．危険度の定量化手法

ここでは，保護するべき情報に対する脅威をリアルタイムに検知したあと，検知した脅威の大きさを定量化する手法，すなわち危険度の定量化手法について述べる．

3.1　想定する環境

ここでは，危険度の定量化手法を考える環境について述べる．あらゆる状況に対応する危険度の定量化手法を考えるのは現実的ではないため，いくつかの制約を設ける．以下にその制約と想定する環境やシチュエーションを示す．

1) 想定する場所

保護するべき情報は様々な個人、組織のもとにある．本論文では，一般企業のオフィスについて考える．オフィス内には，パーテーションによる仕切りはなく，PC が並べられている状況を想定する．企業のオフィス内における情報漏洩の脅威に対して，危険度の定量化を行う手法について提案する．

2) 保護するべき情報

一般企業のオフィス内には，様々な場所に保護するべき情報が存在する．そして，その情報はデジタルデータから書類やハードディスクといった物理的なものまで考えられる．本論文では，保護するべき情報はオフィス内に設置された PC からアクセスできるものに限定する．それは，社内ネットワーク上の情報や，インターネットを経由してアクセス可能なクラウドサービス内の情報も該当する．

3) 存在する人物

想定する場所である一般企業のオフィス内に存在する人物を，その企業に勤める社員とオフィスを訪れた来客の二種類に限定する．社員には脅威がなく，来客の不審な動きに気づいた場合は警戒するものとする．来客は全員，企業を訪れた際，最初に受付を済ませ，そこで通信可能な来客用のタグを受け取るものとする．社員は全員，通信可能な社員用のタグを持っているものとする．これらのタグから id を取得でき，社員と来客の区別ができるものとする．社員と来客は「自由意志」で行動するものとし，タグは持ち歩いていない場合も考慮する．

4) オフィスに設置された PC

オフィスに設置された PC には，社員と来客の持つタグと通信可能なセンサが取り付けてあるものとする．さらに，PC にタグを持っていない人物が近づいてきた場合にも，人物の接近を検知できるセンサも取り付けてあるものとする．PC から資産価値のある情報や，社外に漏れてはならない情報にアクセスできるものとする．

5) その他の条件

PC，社員，来客の三点におけるそれぞれの距離は適当な通信手段（タグやセンサ）で正確に測れるものとし，それはリアルタイムに測定できるものとする．オフィス内の危険度は来客の脅威によるものに限定し，その危険度は PC，社員，来客の三点におけるそれぞれの距離のみによって求めるものとする．その際，鏡写しの関係など測定した距離が全て等しい複数の位置関係が存在するが，それらの危険度は全て等しくなるものとする．

3.2　危険度の定量化手法

ここでは，一般企業のオフィス内に，PC，社員，来客がそれぞれ複数存在する場合を考える．そして，その三点の間の距離から，来客による脅威の危険度を定量化する手法について述べる．PC，社員，来客とそれぞれの間の距離α（社員と来客間の距離），β（来客と PC 間の距離），γ（社員と PC 間の距離）を図示したものを図 2 に示す．できるだけ単純化し，今後拡張されやすいと思われるものを提案する．

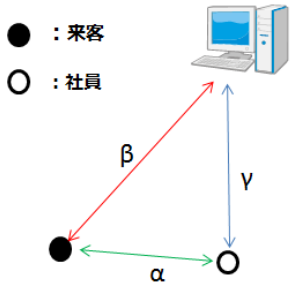

図 2　PC，来客、社員とそれぞれの距離

ここで，オフィスという場に存在する三つの要素（PC，来客，社員）の役割や存在意義について記述する．

1）PC

PC はまず，脅威の検知を行う．タグやセンサによって正確に測定された PC，社員，来客のそれぞれの間の距離をデータとして収集する．収集した距離のデータとあらかじめ組み込まれたアルゴリズムからダイナミックに危険度を定量化する．定量化された危険度をもとに，段階的に分けられたセキュリティレベルから適切なものを選択し，決定する．最後にセキュリティレベルに合わせたシステム制御を行うことで脅威に対して対応する．

2）社員

オフィス内に存在する社員は自由意思で行動する．その社員が悪意のある来客の視界に入ることや，保護するべき情報のそばにいることで，来客に不正行為をさせない状況を作る．また来客に不正行為を思いとどまらせる存在となる．

社員が来客の不正行為や不審な動きを察知できる状態ならば，必ず察知することを前提条件とする．察知した場合，社員は来客の不正行為を阻止し，不審な動きには警戒するものとする．ただし，社員は 2 人以上の来客を同時に監視できないと仮定し，監視できる来客の人数を 1 人とする．

3）来客

オフィス内に存在する来客は全員不正行為を行う可能性を持っているものとする．そして，id を取得可能なタグを持ち歩かない可能性も考える．不正行為は，オフィス内に設置してある PC からアクセス可能な情報に対して行われる行為を対象とする．不正行為は具体的に，情報を漏洩する行為と，情報を使用不可能にする行為を考える．情報を漏洩する行為は，画面を盗み見ることや，PC から流れている音や聞こえる声を盗聴するといった人の記憶によるものと，ネットワークやインターネットを経由して情報を他の場所へ移すこと，それから USB や CD などによる情報の持ち出しを考える．情報を使用不可能にする行為は，情報の削除，暗号化，隠蔽，ハードディスクの物理的な破壊を考える．

次に，本論文で提案する人物フォーメーション考慮した危険度の定量化手法について，全体像を表す大まかな流れを図 3 に示す．

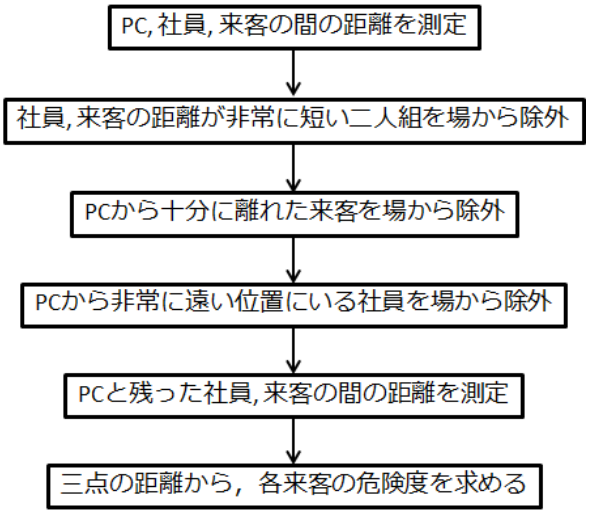

図 3　危険度の定量化手法の全体の流れ

図 3 に示すように，全体の流れとしては，危険度を求める際に，危険度と直接関係性のないと判断される社員，来客を場から除外する．具体的には 3 パターンあり，社員と来客の二人組で行動している場合と，PC から来客が十分離れていると判断できる場合と，PC から社員が十分に離れていると判断できる場合である．

危険度と直接関係性のないと判断される社員と来客を除外した状態から改めて，PC1 台，社員 1 人，来客 1 人の組み合わせを決定する．この組み合わせ方は複数通り考えられる．そこで，本研究では，PC1 台，社員 1 人，来客 1 人の組み合わせ方を 3 通り提案する．組み合わせが決定したあと、組み合わせられた 3 点の距離から危険度を求めていく．

さらにここから，本論文で提案する手法について詳細を記述していく．

① オフィスに存在するすべての PC，社員，来客から，PC1 台ずつに対して，図 4 のようにα（社員と PC 間の距離），β（来客と PC 間の距離），γ（社員と PC 間の距離）を測定する．その際，αは（A_1~A_5），βは（B_1~B_4），γは（Γ_1~Γ_3）というように段階的に分ける．段階的に分けるときの基準とその詳細を，α, β, γ について，それぞれ順番に表 1，表 2，表 3 に示す．

本論文で提案する手法では，まず始めに PC1 台に対してオフィス内に存在する全ての社員，来客とのそれぞれの距離から危険度の定量化を行う．各々の PC にダイナミックなセキュリティ対策を行わせることで，オフィス全体としても提案するコンセプトが充足される．そして，今回の環境において保護するべき情報はオフィス内に設置された PC からアクセスできるものとしているので，安全性に問題はない．さらに，オフィス内の PC の配置は企業ごとに異なる．PC1 台ずつに対して危険度の定量化を行うモデルを提案することで，あらゆるオフィス内における PC の配置に対応できると考えられる．

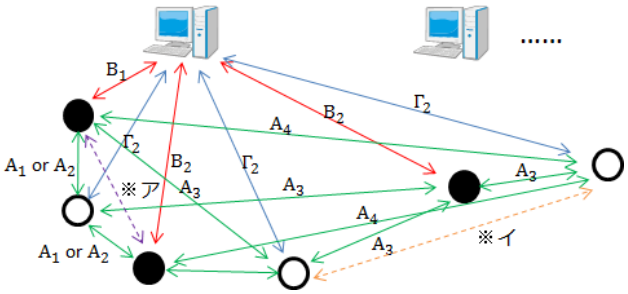

図 4　PC，社員，来客の間の距離の測定

※ア：来客間の距離は測定しない．

※イ：社員間の距離は測定しない．

来客同士の距離と危険度は，相関関係にないと考える．しかし，前提条件が与えられていない場合，相関関係が認められる場合がある．例えば，来客同士が手を組んでいて，複数犯で連携しながら社外秘の情報を得ようとしている場合は相関関係が認められる．これは来客間の距離が近い場合，お互いに話し合う機会ができるので，より社員に疑われないように不正行為を行える可能性が上がる．そこで，より汎用性の高い提案をするために，来客間の連携は考慮せず，個々の来客についての危険度を定量化する．そのため，オフィス内に存在する PC，社員，来客のそれぞれの間の距離を測定する際，来客間の距離は測定しない．

さらに，社員同士の距離と危険度の間にも相関関係はないと考える．今回の提案における危険度は，来客による脅威としている．社員の存在意義は，来客の不正行為または不審な動きを察知し，阻止や警戒を行うことと，来客に不正行為を思いとどまらせることである．一人の社員が来客の不正行為や不審な行動に対して断定する自信がなく，社員同士で相談することにより阻止や警戒の可能性が上がることも考えられるが，本論文では社員個人が来客の不正行為や不審な動きを断定する決断力を有するものとする．このことから，オフィス内に存在する PC，社員，来客のそれぞれの間の距離を測定する際，社員間の距離は測定しない．

表 1　社員と来客の距離

文字(α)	社員と来客の距離	詳細
A_1	手を伸ばせば相手に届く	お互いに話をしている二人組で行動している
A_2	声を張らずに聞こえる	相手を意識していない
A_3	大声を出さないと聞こえない	すぐに相手の動きを封じることができない
A_4	相手の存在を目で確認できる	遠くの方に見える
A_5	相手が見えない	相手が見えない

表 2　来客と PC との距離

文字(β)	来客と PC との距離	詳細
B_1	PC を操作できる	コピー，通信，改ざん席についている
B_2	画面を見ることができる	携帯のカメラやデジカメによる盗撮
B_3	音を盗聴できる	音を聞くことができる
B_4	何もできない	PC との距離が遠すぎて，何もできない

表 3　社員と PC との距離

文字(γ)	社員と PC との距離	詳細
Γ_1	PC を操作できる	席についている
Γ_2	席周辺の状況を確認できる	担当のＰＣの席の人の有無を確認可能 担当のＰＣの席周辺の状況を確認可能
Γ_3	席周辺の状況を確認できない	席から離れているため、席の状況を監視できない

② A_1, A_2 の距離だった社員と来客は優先的にペアを組み，その社員と来客のペアはその場から除外する．

A_1, A_2 の距離だった社員と来客は二人で話をしていたり，一緒に行動していたりする可能性が高い．もし，そうでなかったとしても，来客の不審な動きや，不正行為に社員が気づく可能性が極めて高い．そうした理由から，来客の不正行為を社員が防ぐことができると考えられる．

このとき前提条件として，社員が来客を監視できる人数を n 人とし，n=1 の場合を考えることとする．そうした場合，来客は監視されている社員に不正行為を防がれ，その社員は他の来客を監視する余裕はないため，二人とも危険度に直接関係しなくなると考えた．よって二人を場から除外する．②の操作を視覚化したものを図 5 に示す．

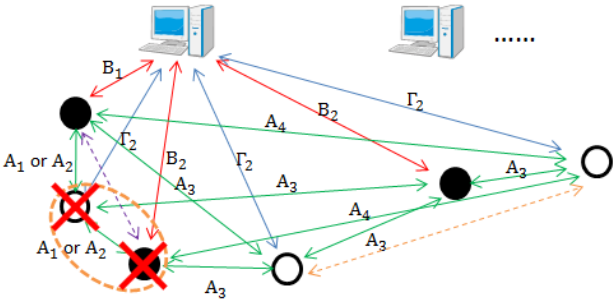

図 5　A_1，A_2 の距離である社員と来客のペアは除外

この過程でA_1, A_2 の距離である社員と来客のペアが複数作れる場合がある．その複数のペアの中でも，危険度が最小になるよう，合理的に社員と来客のペアを作る場合と，危険度が最大になるよう，不合理に社員と来客のペアを作る場合がある．これは，社員が複数いる来客のうちどの来客を気にかけているかに依存する．このような場合，最悪のケースを考慮して，危険度が最大になるよう不合理に社員と来客のペアを作る．

図 5 では不合理にペアを作ったものを示したが，参考に合理的にペアを作った場合のものを図 6 に示す．

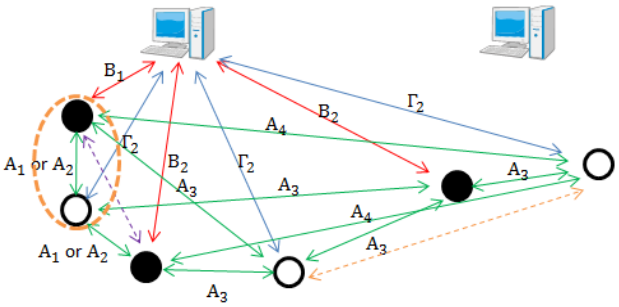

図 6　合理的に社員と来客のペアを作った場合

③　B_4の距離だった来客はその場から除外する．

上記の表 2 より，測定の結果B_4の距離だった来客は PC からの距離が十分遠いため，PC を操作することはおろか, PC のディスプレイに表示された文字や写真などを盗み見ることや，盗撮することができない．さらに，PC から流れる音や聞こえる声を盗聴することもできない距離である．なので，B_4の距離だった来客は脅威を持っていないと考える．そのため，該当する来客はその場にいないものとし，提案する危険度の定量化手法の要素としては考えない．

④　　Γ_3の距離だった社員をその場から除外する．

上記の表 3 より，測定の結果Γ_3の距離だった社員はトイレや，喫煙所，食事などのためオフィスを一時的に離れていると考えられる. PC のある席の状況が確認できないほど遠い位置にいるので，来客がオフィス内で何をしているのか把握できない．なので，脅威から情報を保護する能力はないと考える．そのため，該当する社員はその場にいないものとし，提案する危険度の定量化手法の要素として考えない．

⑤　PC1 台，来客 1 人，社員 1 人の位置関係から，来客全員の危険度を一人ずつ求める．

まず，PC1 台，来客 1 人，社員 1 人の位置関係から，来客の危険度を求める方法を記述する. 図 1 と表 1, 表 2, 表 3, でα（社員と来客間の距離），β（来客と PC 間の距離），γ（社員と PC 間の距離）を測定する際，αは$(A_1 \sim A_5)$，βは$(B_1 \sim B_4)$，γは$(\Gamma_1 \sim \Gamma_3)$というように段階的に分けた．$(A_1 \sim A_5)$，$(B_1 \sim B_4)$，$(\Gamma_1 \sim \Gamma_3)$の組み合わせをすべてシミュレートし，そのときの危険度を決定した．危険度 r は，R_1, R_2, R_3に分類した．それを表 4 に示す．

表 4　危険度の表現

危険度(r)	説明
R_1	極めて危険 （情報漏洩を防げない）
R_2	危険性あり （情報漏洩の可能性もあり，情報漏洩を防げる可能性もある。）
R_3	安全

$(A_1 \sim A_5)$，$(B_1 \sim B_4)$，$(\Gamma_1 \sim \Gamma_3)$のすべての組み合わせと危険度の関係を表したものを表 5~表 7 に示す．

表 5　Γ_1のときの網羅表

Γ_1のとき	B_1	B_2	B_3	B_4
A_1	R_3	R_3	R_3	×
A_2	×	R_3	R_3	×
A_3	×	×	R_3	×
A_4	×	×	×	×
A_5	×	×	×	R_3

表 6　Γ_2のときの網羅表

Γ_2のとき	B_1	B_2	B_3	B_4
A_1	R_3	R_3	R_3	R_3
A_2	R_3	R_3	R_3	R_3
A_3	R_2	R_2	R_2	R_3
A_4	R_1	R_1	R_1	R_3
A_5	×	×	×	R_3

表 7　Γ_3のときの網羅表

Γ_3のとき	B_1	B_2	B_3	B_4
A_1	×	×	×	R_3
A_2	×	×	×	R_3
A_3	×	×	×	R_3
A_4	×	×	×	R_3
A_5	R_1	R_1	R_1	R_3

表 5~7 中の”×”印はα, β, γ の組み合わせのうち，その位置関係が存在し得ないことを示している．

ここでは，オフィス内に社員と来客の二種類の人物が存在するときを考えているが，どちらか一方だけが存在する可能性も考えられる．本論文では社員の危険性については考えないので，オフィス内に社員しかいない場合は危険度を考える必要はない．オフィス内に来客しかいない場合は危険度が常に高く，βとの関連性は以下の表 8 のようになる．

表 8　来客 1 人の場合の距離βと危険度の関係

Bの値	危険度(r)
B_1	R_1
B_2	R_1
B_3	R_1
B_4	R_2

以上のことを踏まえ，PC1 台，来客 1 人，社員 1 人の位置関係から，来客全員の危険度を一人ずつ求める．全ての来客の危険度が求まったとき，その中で一番危険度の高かった来客がもっとも脅威を持っていることになる．よって，その来客の危険度を場の危険度とし，その危険度に対応したセキュリティレベルを決定する．

ここで各来客の危険度を決定する方法を三通り提案する．ただし，来客の人数と社員の人数は等しいものとする．

(ア)　各来客に対し，最も距離の近い社員との組み合わせで危険度を求めていく方法

始めに，PC からの距離が最も近い来客から順に，その来客との距離が最も近い社員との組み合わせで危険度を求める．危険度を求めた組み合わせの来客と社員を除き，同様の手順で全ての来客の危険度を求めていく．

(イ)　各来客に対し，全社員との危険度を求め，その中から最も低い危険度を選択していく方法

始めに，PC からの距離が最も近い来客を選択する．その来客について，全社員それぞれとの組み合わせで危険度を求める．

(ウ)　全ての組み合わせを考慮し，場の危険度を決定する方法

場に存在する全ての来客と社員との組み合わせで危険度を求める．あらかじめ作っておいた危険度の組み合わせパターンから場の危険度を決定する．

４．評価と考察

4.1　評価

3.2 で危険度の定量化手法について記述した．この手法の⑤の最後で社員 n 人，来客 n 人のときの危険度の導出方法を三通り提案した．これらの計算量から，実現性と有効性を評価する．

(ア) 各来客に対し，最も距離の近い社員との組み合わせで危険度を求めていく方法

まず，来客 n 人の中から PC との距離が最も近い来客を選択するのに 2(n-1)回の計算量が必要であり，選択された来客との距離が最も近い社員を n 人の中から選択するのに 2(n-1)回の計算量が必要となる．次に，来客の人数と社員の人数が 1 人になるまで繰り返したあと，n 組のペアの危険度をそれぞれ求めるのに n 回，そして最後に n 組の組み合わせのうち最も危険度の高いものを選択するのに 2(n-1)回の計算量が必要となる．

すべて合計すると，$2n^2 + n - 2$回となる．

(イ) 各来客に対し，全社員との危険度を求め，その中から最も低い危険度を選択していく方法

まず，来客 n 人の中から PC との距離が最も近い来客を選択するのに 2(n-1)回の計算量が必要であり，選択された来客と全ての社員との危険度を求めるのに n 回の計算量が必要となる．次に，n 組の組み合わせから最も危険度の低い組み合わせを選択するのに 2(n-1)回必要で，これを来客の人数と社員の人数が 1 人になるまで繰り返す．最後に n 組の組み合わせの中から最も危険度の高いものを選択するのに 2(n-1)回の計算量が必要となる．

すべて合計すると，$2.5n^2 + 0.5n - 2$回となる．

(ウ) 全ての組み合わせを考慮し，場の危険度を決定する方法

来客 n 人，社員 n 人の全ての組み合わせの危険度を求めるのにn^n回必要となる．そして，あらかじめ作っておく危険度の組み合わせパターンは$n^{n\times n}$個あり，その中から一つ選ぶのに最低$n^{n\times n}$回必要となる．

すべて合計すると，　$n^n + n^{n\times n}$回となる．

4.2　考察

4.1 において評価した三通りの定量化方法を比較した．以下に表 9 として示す．

表 9　定量化方法の比較

定量化方法	計算量	実現性	有効性
(ア)	$2n^2 + n - 2$回	○	△
(イ)	$2.5n^2 + 0.5n - 2$回	○	△
(ウ)	$n^n + n^{n\times n}$回	×	○

定量化方法の(ア)については計算量が$o(n^2)$ であるので，実現性はあると考えた．保護するべき情報にとって最も危険な存在である PC との距離が近い来客から順に危険度を求めているので，本研究の設定においては PC との距離が近い来客ほど正確な危険度を求めることができる．しかし，全体を考えたとき，来客と社員の最適な組み合わせを選択できている可能性は極めて低くなる．本来なら，来客の不正行為に気付けるはずの社員がどの来客も監視できない状態だと判断されてしまう可能性が出てくる．このことより，有効性に関しては評価を下げた．

定量化方法の(イ)については計算量が(ア)とほぼ等し

く$o(n^2)$なので，実現性はあると考えた．この方法においても，保護するべき情報にとって最も危険な存在である PC との距離が最も近い来客から順に危険度を求めている．(ア)とは異なり，各来客に対して，全社員との組み合わせで危険度を求めてから組み合わせる社員を選択するので, より正確に危険度を求めることが可能である．しかし，この方法も全体を最適化することを考えていないので，無駄な組み合わせ方を選択してしまう場合がある．このことより，有効性の評価を下げた．

定量化方法の(ウ)については計算量が$n^n + n^{n\times n}$回となってしまい，n の値によっては計算量が多すぎてしまうため，実現性がないと考えた．さらに，この方法においては全体の最適化を考えるため，あらかじめ$n^{n\times n}$個の危険度の組み合わせパターンを考えておかなければならない．これも n の値によって膨大な数となってしまい，危険度の組み合わせパターンを作成できないので実現性がないと判断する要因となった．

(ア)，(イ)，(ウ)の定量化方法の考察から，これら三つの方法を比較した結果，(イ)の方法が最適な方法だと判断した．これは，まず実現性がないと判断した(ウ)の方法を除外して考え，(ア)と(イ)を比べたとき，(イ)の方法の方がより全体最適化できていると考えたためである．

他にも n の値によって定量化方法を変えるという選択肢も考えた．これは(ウ)の方法が n の値によっては実現可能であると考えたためである．n の値が小さいとき，定量化方法(ウ)を適用する．そして，計算量が増え，(ウ)の方法が使えないような n の値のときは定量化方法(イ)に切り替えるのがよいと考えた．

５．おわりに

本論文では，ダイナミックにセキュリティレベルを制御するというコンセプトをもとに，一例として，一般企業のオフィスへの来客訪問というリアルな環境を想定し，複数人いる来客と社員のオフィスでの立ち位置による危険度の定量化手法を提案した．

具体的には，保護するべき情報を一般企業のオフィス内に設置された PC からアクセスできるものに限定した．さらに，オフィス内に複数人の来客と社員がランダムな位置に存在することを想定した．その条件下で，PC と来客と社員という三点の位置関係から危険度を定量化する手法を提案した．

提案した危険度の定量化手法は，実現性と有効性の異なる 3 種類の方法があり，それらを比較し，評価した．

評価し，考察した結果，提案した三つの方法の中では定量化方法(イ)が最適であると判断した．これは，全体最適化がもっとも正確に行われていると判断した(ウ)の方法の実現性が低いため度外視し，(ア)と(イ)の方法を比べたときに(イ)のほうがより全体最適化が行われると判断したためである．ただし，これらの 3 通りの方法を単体で用いずに，組み合わせることを考えた場合，n の値が小さい場合は定量化方法(ウ)を適用し, n の値が大きいときは定量化方法(イ)に切り替えるという案が現時点で最良の方法だと判断した．

提案した定量化手法の①において，来客間や社員間の距離は測定しなかった．これは来客間や社員間の連携を考慮していないことになるので，今後来客間や社員間の距離も危険度を定量化するための要素として考える必要がある．

危険度を定量化するために，PC，社員，来客の距離に注目し，重視して定量化手法を提案した．しかし，距離を測定したとき，実際の位置関係は一通りに定まらず，鏡写しの関係や，PC からの角度が異なる配置が考えられる．他にも，PC と来客の間に社員が位置するような配置も考えられ，このとき来客が PC を覗きこもうとした場合に遮蔽物の役割を果たし，また，来客が PC に近づこうとしたときにも近づきにくくなる．これらのような場合には，危険度が変わる可能性があるので考慮する必要がある．

本論文では，社員が来客を監視する際，監視できる人数を一人とした．監視できる人数が二人，三人と変わる場合も考える必要がある．

危険度$\mathbf{R_2}$の定義を、「情報漏洩の危険性もあり，情報漏洩を防げる可能性もある」とした．この定義はまだ意味が広すぎる．$\mathbf{R_2}$という危険度をより細かく分類することで，危険度を定量化したあとのセキュリティ制御やシステム制御がより適切に行えるようになる．そのため，危険度$\mathbf{R_2}$をさらに細分化する必要がある．

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) 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) 榎本真也, “ダイナミックに制御する情報漏洩対策システムの検討”, 第 11 回情報科学技術フォーラム（FIT2012）論文集, 発行年(2012/09)
5) 社内セキュリティ事情, http://www.cgm-japan.com/