動的セキュリティ制御方式の研究

嶋津, 将彦 / SHIMAZU, Masahiko

(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)
57
(開始ページ / Start Page)
1
(終了ページ / End Page)
4
(発行年 / Year)
2016-03-24
(URL)
https://doi.org/10.15002/00013276

法政大学大学院理工学研究科　(2016 年 4 月)　　法政大学

動的セキュリティ制御方式の研究

DYNAMIC RISK EVALUATION MODEL AS A SECURITY LEVEL

嶋津将彦

Masahiko SHIMADU

指導教員　金井敦

法政大学大学院　理工学研究科応用情報工学専攻　修士課程

***Abstract*—Generally, high security information management leads to high confidentiality. However, high confidentiality causes low availability. Therefore, we think availability can be increased by choosing the appropriate security level depending on the changing risk. Thus, this paper proposes a risk evaluation model in which risk is quantitatively evaluated using the value of information, protection level, and threat level.**

1. はじめに

近年. 情報化社会が進み IT は我々の生活に必要不可欠な存在となっている. 政府, 企業, 一般家庭を問わず広く普及している一方, 多くの情報は適切に管理できていない場合が多い. 昨今は個人情報の価値が相対的に上昇し, 一度漏洩してしまうと社会的信用や金銭的損失く, 大きい企業の守秘管理も関心が高まっているが毎年被害件数は増加傾向にある.

一般的に企業は情報管理の際常に最高レベルのセキュリティを実装し, 情報の保護を行うがコスト面などから考えると重要度の低いデータや, 元々情報資産に対して悪影響の少ない環境下で管理している場合などは最高レベルのセキュリティを施す必要がないと考えられる. また情報資産の保護という面で見ると情報セキュリティの３要素である「完全性」「機密性」「可用性」のうち機密性が高くなるにつれて強固なセキュリティ対策を実装していると言い換えられる一方, 可用性が減少する傾向にある. 言い換えると高い機密性を維持している状況では可用性が低い状態であり双方の両立が出来ていない環境が多く存在する.

つまり理想的なセキュリティ対策とは情報資産に対して危険が迫っている状況では機密性のセキュリティを, 危険が迫っていない環境では可用性を重視したダイナミックな制御が必要であると考えられる.

本論文では状況に応じたダイナミックなセキュリティ制御を適用するために, 情報資産に迫る危険性を検知し, その危険度を算出, 可視化を行いこれらの工程を用いて最適なセキュリティレベルを算出する手法を提案する. また一例として一般的なオフィス環境内に迫る危険を検知しセキュリティ制御させるが本論文のコンセプトでは物理的環境やサイバー空間を問わない概念であり多くの場面で適応できることを想定としている.

2. 動的セキュリティ制御のコンセプト

本節では動的セキュリティ制御の基本コンセプトを述べる.
一般に,情報資産を取り巻く環境は秒単位で刻々と変化している.また情報資産に対する危険性も同様に変化しているのでまずその危険因子を検知し,影響力を算出,レベルに合わせて制御という一連の流れを繰り返し行うことが動的セキュリティの基本コンセプトである.

また,本論文では ISMS によって定められたリスク対策(リスク=情報資産×脅威×脆弱性)を基に,情報資産に対する危険確率を「リスク」と呼び,危険因子を「脅威」,情報資産そのものを「価値」,脅威から価値を守る因子は「防御力」と定義し,以下の流れをコンセプトフローと呼ぶ.

・1. 各因子の検出

各因子とは対象となる環境においてリスク算出に必要となる価値,脅威,防御力のことであり,この各因子はリアルタイムで正確に観測できるものとする.物理的環境下では IrDA や Bluetooth などの無線センサーの利用や,サーバー上を想定するとパケット監視や IDS を用いて主に価値に対する脅威を検出する.

・2. 数値化・可視化

検知された因子を定量化し, 価値対してどの程度リスクを取っているか算出する. また可視化することで, 価値の管理者が手動でセキュリティレベルを変化させることも可能である.

・3. 動的な制御

価値に対するリスクを算出したことによってリスクの値に対するセキュリティレベルを動的に制御する. またリスク値によって段階的にセキュリティレベルを区分し, 状況に応じた制御を可能とすることで様々な脅威の対策となる.

3. サンプルモデルの検出,算出

ここでは一例として物理的な環境を想定し,一般的なオフィス内での動的制御モデルを紹介し,本論文内での想定された環境下をセキュリティ場と呼ぶ.

コンセプトフローに基づき各因子の検出を行う前にセキュリティ場に存在する各因子の定義と算出方法を以下に述べる.

・1. 価値

情報資産としての価値は企業において顧客から預かる個人情報を始め,従業員の個人情報,企業運営のための企業情報,ノウハウ等の機密情報など多種多用であり,これらの情報資産が社外に漏洩すると企業の事業運営上甚大な問題,被害を被る.

例えば,守るべきものを金庫とした場合,価値とは金庫に保管されているものはもちろん価値そのものであり,セキュリティ場において価値が存在する箇所は金庫の座標を中心として直接金庫に触れる位置に限られていると考えられる(図 1.参照).一方,情報資産はスピーカーから音源,モニターから視覚的情報などある程度距離が離れていても情報を得られる可能性があるため価値は情報資産を中心とし距離に従い減少するものと考えられる(図 2.参照)

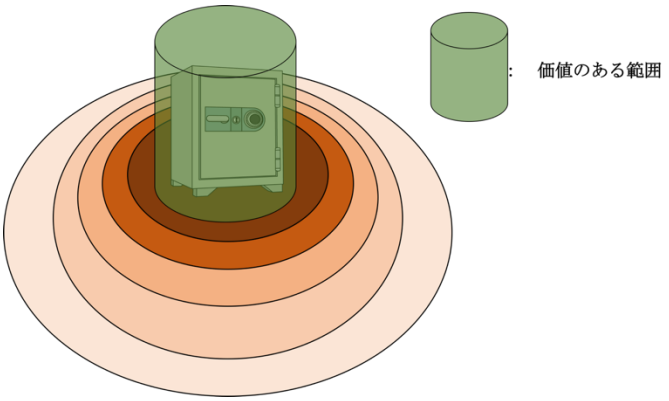

図 1.金庫の価値のある影響範囲イメージ

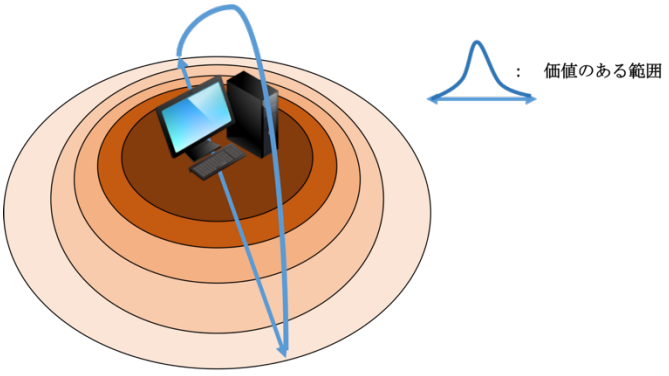

図 2. 情報資産の価値のある影響範囲イメージ

また,モデリングされたセキュリティ場においての価値は図 2 のように中心が最大の影響力を持ち,距離によって影響力が減少するため,中心座標を測定するためにリアルタイムで正確な座標を測定できる無線センサーを利用する.

セキュリティ場に n 個の価値が存在し,価値の中心座標を(X_W, Y_W),算出座標を(x, y)とする場合価値の定量的な値を以下に表す.

$$W(x,y) = \sum_{i=1}^{n} Worth_i\{(x,y)(X_{Wi}, Y_{Wi})\}$$

(式 1)

・2. 脅威

脅威は価値に対してどの程度情報操作する影響力を持つかと定義し,その値を定量的に表す.

価値の考えと同様に脅威が影響を与える範囲は距離によって変化すると考え,また脅威は後述する防御力,リスク値算出との関係のため確率ではなく上限なしの定量的な数値として示す.

上記より,セキュリティ場の 2 次空間において座標(X_T, Y_T)に存在する脅威に対して一定距離離れた座標(x, y)における脅威 T を以下の式(2)で表す.

$$T(x,y) = \sum_{K=1}^{n} Threat_k\{(x,y)(X_{Tk}, Y_{TK})\}$$

(式 2。)

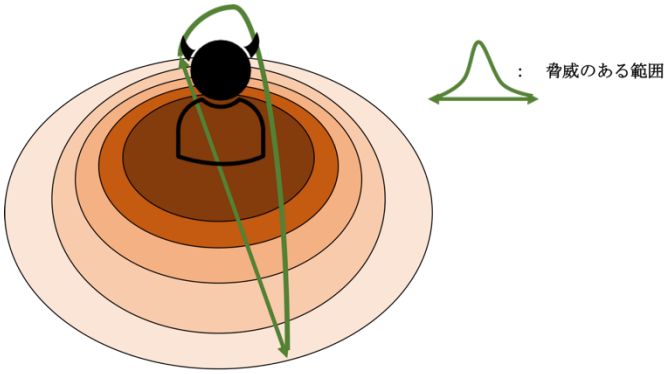

図 3.脅威の与える範囲

・3. 防御力

ここでいう防衛力とは,情報資産(価値)を脅威から防御するために働く力を指す.

脅威に対して価値をどの程度防御できるかの影響量を測るが”脅威から防御できる確率”ではなく脅威と同様,定量的に表す.また,脅威の影響力とその脅威から価値を保護する防御力が同量である場合,互いに影響力を打ち消し合い価値に対して脅威が与える影響力はなくなると考えられる.

また,セキュリティ場に存在する防御力を考えるとき,脅威の算出式と同等の考え方をする.これは脅威が与える範囲と防御力が施される範囲は同等であることを示す.

$$P(x,y) = -\sum_{K=1}^{n} Protection_k\{(x,y)(X_{PK}, Y_{PK})\}$$

(式 3.)

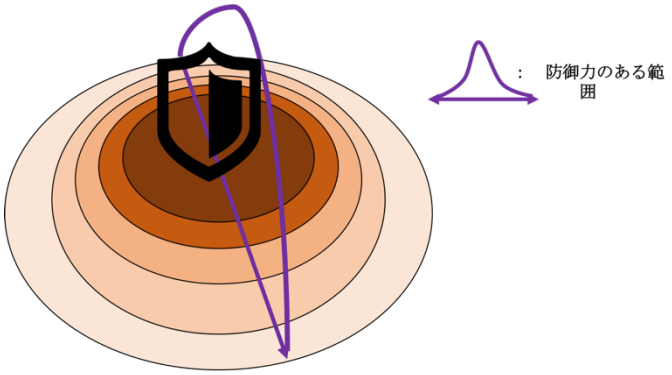

図 4. 防御力のある範囲

・4.　リスク

1. 2. 3. で算出された三要素「価値」・「脅威」・「防御力」を基にセキュリティ場に存在する. リスクの値を求める. セキュリティ場に複数の価値, 脅威, 防御力顔それぞれ存在し, 任意地におけるリスクを以下の式で表す.

$$Risk(x,y) = W(x,y) * \begin{cases} 0 & T(x,y) = 0 \ldots (1) \\ 0 & T(x,y) \leq P(x,y) \ldots (2) \\ \frac{T(x,y)+P(x,y)}{T(x,y)} & T(x,y) \geq P(x,y) \ldots (3) \end{cases}$$

（式 4. ）

式 4 は「リスク=情報資産×脅威×脆弱性」に基づき変化させたものであるがまず根本なリスク算出の考えとして価値に対してどの程度の影響力（脅威・防御力双方）を与え, 漏洩の確立を算出させている. つまり式 4 は「価値×漏洩する確率」を示しており, 漏洩する確率を脅威と防御力の関係で算出する. また脅威の値が算出されない場合は価値に対して脅威としての影響がないと判断されているためリスクはないと考える. 同様に算出された脅威の値より防御力の値が高い場合は脅威の影響を打ち消すと考えリスク値を算出しない.

4.　サンプルモデルの可視化

ここではコンセプトフローに従い,取得したリスク値を可視化する.また今回のセキュリティ場は一般的なオフィス環境であるが各因子の座標を 2 次元空間上にとりリスク値を加えた図で表す.

図 5.リスク値算出要素アイコン

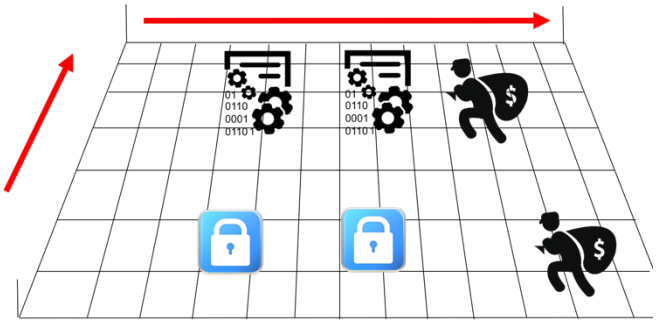

図 6.セキュリティ場

図 6 のような空間に「価値」「脅威」「防御力」が存在するときにリスク値がどのように変化するかを観測する.

また脅威や防御力が移動した際のパラメータ変化を記載する.

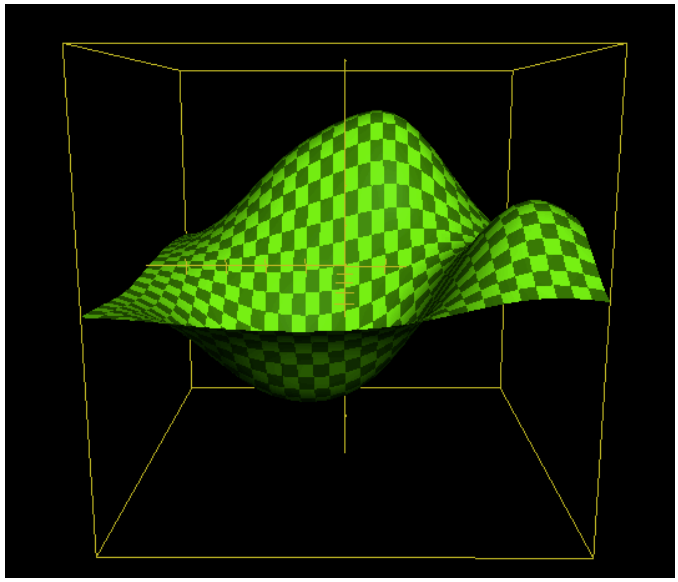

図 7.図 6.に対するリスク値パラメータ可視化

図 7 より,脅威に近い価値はリスク値が高まり,また防御力は脅威の付近に位置していないため,本来の役目を担っていない. 脅威に対して影響力を持たせるために以下に双方の中心座標を近づけた際のリスク値を可視化する.また価値の座標やリスク値は一般的に逐次変化しないため脅威と防御力の関係のみとする.

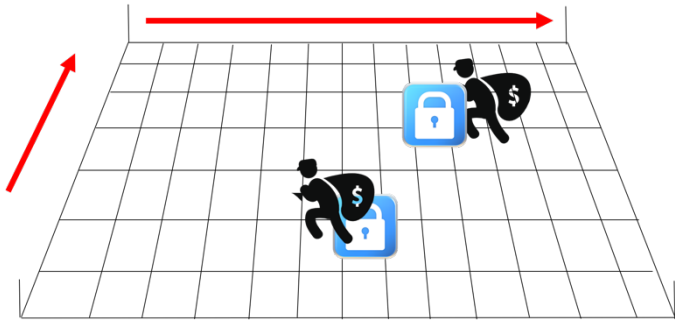

図 8.脅威,防御力の座標移動後

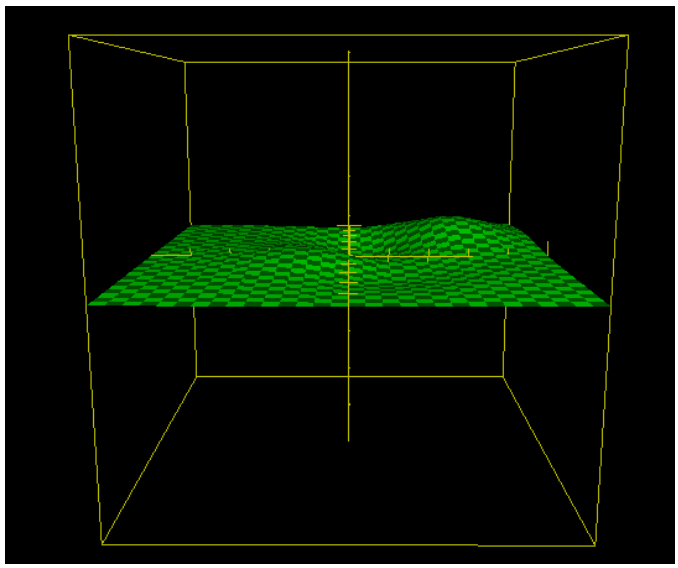

図 9.脅威,防御力座標移動後のパラメータイメージ

図 8.9.より脅威の中心座標と防御力の中心座標が非常に近い場合,脅威の値を軽減する事ができる.任意の座標に対応するリスク値によって式 4 の計算式に当てはリスク値を算出する.

5. 動的制御

セキュリティ場から任意の座標に対してリスク値を算出,可視化をしたためその値に対して制御を行う.
また,脅威の種類によっても脅威そのものの影響力が変化するため,属性判断をして算出する.

表 1.今日の属性判断

数値[R]	来客の種類
5.0	企業･協力無し
4.5	企業･協力有り
4.0	搬入業者
4.0	宅配業者
4.0	一般人
3.5	同社･他部署

表 2.リスク値に応じた制御内容

数値[R]	制御内容
4.0 以上	電源を切る
3.15 以上	USB ポートの使用禁止
2.7 以上	ディスプレイを消す
2.0 以上	通信を切断する
1.8 以上	ファイルをロック･隠す
1.2 以上	ファイルを閉じる
0.35 以上	音を消す
0 より大きいとき	来客の通知

表 1.2 より脅威の属性,リスク値により制御内容を動的に決定し制御する.

6. 考察・課題

今回提案したセキュリティ場の動的制御モデリングを検証するために一般的なオフィス空間を仮想しリスク値を算出した.脅威の数と防御量の数を同数として算出したが,脅威が圧倒的に多い場合であっても脅威の属性によってリスク値が変化するため,微弱な脅威が多数いる状況下でも防御側の値が高ければ保護できると考えられる.また,センサーがリアルタイムに正しく計測する事を仮定したが現状の IrDA や Bluetooth での無線通信では誤差が大きく,リスク値算出の際に正しい値か判断しにくい.

物理的空間には机やパーテーションなどの障害物が多くあり,それらの考慮が必要であると考えられる

また,サイバー場でのセキュリティ場の検証も行う必要がある

7. 謝辞

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

8. 参考文献

1)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)

2)総務省, 平成 25 年度版情報通信白書, 2013/07, http://www.soumu.go.jp/johotsusintokei/whitepaper/h25.ht ml

3)情報マネジメントシステム推進センター, http://www.isms.jipdec.or.jp/isms.html

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)講演論文集, 2012/09

5)末次正人, “侵入者の距離によるダイナミックにセキュ リティレベルを制御する端末方式”, 法政大学大学院工 学研究科情報電子工学専攻 2012 年度修士論文

6)本間博礼, “人物フォーメーションを考慮した危険度定 量化手法”, 2014 年暗号と情報セキュリティシンポジウ ム, 2014/01

7)米田 翔一,牧野 駿,谷本 茂明,佐藤 周行,金井 敦,” 動的リスク評価に基づくセキュリティ場の提案”,プロ ジェクトマネジメント学会 2013 年度春季研究発表大会, pp.303-307,2013.