社団法人　情報処理学会　研究報告
IPSJ SIG Technical Reports

2005－ＤＳＭ－37（10）
2005／5／13

情報資産間の依存性を考慮した情報リスクセスメント法

渥美　清隆†　　浅原　慎哉††

† 鈴鹿工業高等専門学校　〒510-0294 三重県鈴鹿市白子
†† 静岡大学大学院理工学研究科　〒432-8561 静岡県浜松市城北 3-5-1
E-mail: †{kiyotaka,asahara}@ka-lab.ac

あらまし　情報セキュリティマネジメントシステム (ISMS) では，情報リスクアセスメントの実 施が最も重要であるが，これまでのところ，理論的なモデルの形で提案されているものは見あたらない．本論文は，情報資産間の関係をグラフで表現し，情報資産に与える脅威を確率モデルとしてとらえる方法について提案する．本手法は，多数のパラメータを要求するが，情報資産の追加や変更があっても情報リスクアセスメントの再実施コストが低く，また，変更によって影響を受ける情報資産の影響度合いも過不足無く表現できる点で，他の手法よりも優位である．

キーワード　情報セキュリティマネジメントシステム (ISMS)，情報リスクアセスメント，脅威，脆弱性，確率モデル．

A Method of Information Risk Assesment Based on the Dependency between the Information Properties

Kiyotaka ATSUMI† and Shinya ASAHARA††

† Suzuka National College of Technology　Shiroko, Suzuka, 510-0294 Japan
†† Graduate School of Science and Engineering, Shizuoka University　Johoku 3-5-1, Hamamatsu, 432-8561 Japan
E-mail: †{kiyotaka,asahara}@ka-lab.ac

Abstract　In information security management system (ISMS), the execution of the information risk assessment is the most important. However, I have not seen the one proposed in the form of a theoretical model for Information risk assessment up to now. This paper proposes a graph for relation among information property and a probabilistic model for threat on it. As for this model, the cost of re-execution of the information risk assessment is low even if there are an addition and a change in the information property. Moreover, this model can easily change each risk value when the defense method to a certain threat is changed, and a lot of information properties are influenced.

Key words　Information Security Management System (ISMS), Information Risk Assessment, Threat, Vulnerablity, Probabilistic Model.

1. はじめに

情報セキュリティマネジメントシステム (Information Security Management System, ISMS) [1], [2] は，組織内に存在するデータやサービスを維持，管理するための要求仕様書として規定されている．この要求仕様書の通りに組織が構築されているかどうかを第三者機関が認証する制度があり，今日までに多くの組織が認証取得を行っている．

ISMS の要求仕様書を満たす上で最も重要な点は，情報リスクアセスメントの実施である．しかし，ISMS 要求仕様書には情報リスクアセスメント実施のための手順などは記されておらず，各組織に置いて合理的な方法を定めること，と書かれているのみである．そのため，各組織では独自に方法の規定を行っており，また ISMS 認証取得のための参考書 [3] などでも，いくつかの提案を見ることが出来るが，十分な汎用性が無かったり，情報資産変更時の再計算が非常に大変であったりするなど十分な方法とは言えない．

本論文で提案する情報リスクアセスメント手法は，各情報資産と情報資産を結ぶ空間をグラフとして定義し，その上で，脅威の発生を確率モデルとして定義することを提案する．

2. 既存の情報リスクアセスメント

ISMS において、情報リスクアセスメントは非常に重要である。この作業から得られる結果から、どの情報資産に対して、

どのような対策を講じるのかが決定されるためである。ここでは、どのような方法が提案されているのかを簡単に説明する。

ベースライン法　各情報資産の種別に応じて，管理状況を事前に規定し，その規定とのギャップを測定する方法．マニュアルを定めれば評価は単純に行うことが出来る．実際のセキュリティ事情に合わせて規定を随時見直す必要があるほか，ギャップの度合いが必ずしも脅威が具現化した場合の損害額の度合いに合っていない．

詳細法　それぞれの情報資産の個別の状況に応じて，脆弱性を加味した脅威の具現化に至る割合と発生するだろう損害額の度合いを算定する方法．マニュアル化が難しく，通常全ての情報資産の評価のために専門家の知識を必要とする．

混合法　ベースライン法と詳細法を組み合わせた方法．

過去に提案された情報リスクアセスメントの重要な課題として、情報資産間の依存性が考慮されていない、ということを挙げることができる。具体的には、重要なデータが入っているデスクトップパソコンがあったときに、このデスクトップパソコンに接続されているネットワークに係る脅威によって、デスクトップパソコンのリスクは変わる。そして、当初ネットワークがファイアウォールに守られていなかったが、その後ファイアウォールによって守られるようになったという場合には、ネットワークに係る脅威が大きく変わることになる。この様子を先に示した情報リスクアセスメント方法で追随しようとすると、デスクトップパソコンに係る脅威の更新を行ってデータのリスク値を再計算すれば良いのであるが、通常ファイアウォールの配下となるパソコンや重要なデータは非常に多くなり、それら全てが再計算の対象となる。これは非常にコストが高い。また，当該ファイアウォール下にある情報資産を再評価する場合に，それぞれの情報資産などには，同じ程度の情報セキュリティリスクの軽減がなされているにもかかわらず，同じようにリスク評価がされる保証がないという点でも問題である．

3. 提案する手法

ISMS で言うところの情報資産は，情報セキュリティアセスメントにて評価しなければならない全てのデータ，サービス，媒体，筐体などを指す．これらは単独で存在することはなく，必ず，何らかの空間に存在し，空間と空間は，何らかの装置によって隣接していると考えることが出来る．ここでは，そのような関係をグラフとして定義し，その上で，情報資産と脅威の関係を確率モデルとして定義し，その範疇の中で，ファイアウォールなどの防御装置や，電力の 2 重化などに対応した計算方法を議論する．

3.1 情報資産間関係

先に述べたとおり，全ての情報資産は単独で存在することはなく，何らかの空間の中に存在しているか，空間と隣接していると仮定する．互いの情報資産は空間を通じて連接可能であり，情報資産と空間によりネットワークを構成する．これをグラフで表すことを考え，これを情報資産グラフとする．

情報資産グラフ G は $G = (N_i, N_s, E)$ の 3 つ組からなる．N_i は情報資産の集合であり，N_s は空間の集合である．それぞれの要素はグラフ上の節となる．E はグラフの辺であり，$E \subset N_i \times N_s \cup N_s \times N_i$ である．例えば図 1 のように物理的空間やネットワーク上の仮想的空間に情報資産が配置されているとしよう．

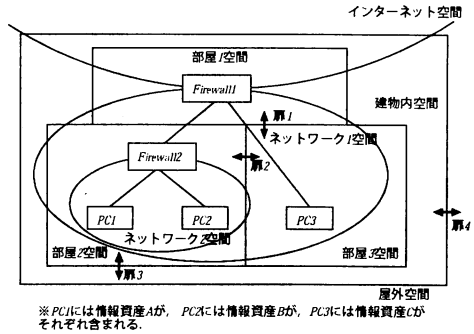

図 1　情報資産の配置例

この場合，グラフ G は $G = (N_i, N_s, E)$，$N_i = \{Firewall1, Firewall2, PC1, PC2, PC3,$ 情報資産 A, 情報資産 B, 情報資産 C, 扉 1, 扉 2, 扉 3, 扉 4$\}$，$N_s = \{$ 屋外空間, 建物内空間, 部屋 1 空間, 部屋 2 空間, 部屋 3 空間, インターネット空間, ネットワーク 1 空間, ネットワーク 2 空間, $PC1$ 空間, $PC2$ 空間, $PC3$ 空間 $\}$, E は図 2 のようになる．もし，Firewall1 の装置がラックマウントされており，電力系統も考慮しなければならないなら，図 3 のようなグラフ G' を考えることもできる．

このグラフの特徴は，原則として情報資産とそれに隣接する空間との連結により構成されていることであり，情報資産の管理者であれば，隣接する空間は容易に特定することが可能である点である．そのため，新しい情報資産が発生しても，容易にこのグラフに追加することが可能である．

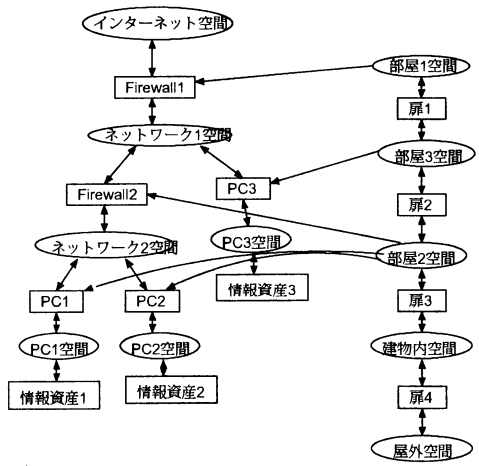

図 2　グラフ G

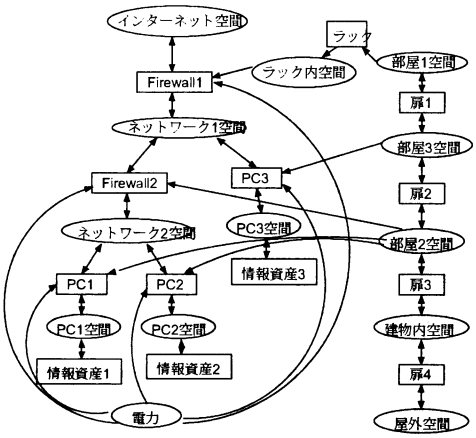

図 3　グラフ G'

3.2　情報資産の重要度

情報資産の重要度が単純に金額によって表現出来る場合は，それを採用するのが最も良いと私は考える．しかし，多くの場合，単純に金額で表現することは難しい．例えば，ある情報資産が盗難にあったとする．盗難された情報はバックアップされていたので，情報そのものは手元に残ったとしても，その情報が同業他社に渡れば，著しい営業損失を受けるかもしれない．また，共同研究の研究情報や個人情報であれば，どのくらいの損害賠償請求を受けるかを事前に計算するのは難しいかもしれない．さらには，そのような状況に陥った場合，信用回復に掛かる費用や，盗難にあった情報と同程度の価値を持つ情報の再構築のために掛かる費用などを考えれば，どのように計算したら良いかすら，想像出来なくなってしまう．

文献 [3] を含め，多くの ISMS 取得のための参考書では，情報資産が機密性，完全性，可用性の観点で毀損した場合の影響の大きさを 1 ～ 4 程度の数値で表すことが多い．例えば資産の重要度が低い場合は 1 を，極めて高い場合は 4 を付ける．この場合の点数付けの判断は，情報資産管理者が過去の経験に基づいて行う場合が多い．

情報資産の価値が 0 の場合，そもそもその資産として扱う価値が無い．本論文では，情報資産の重要度は関数として $V(i,x) = y,\ y \in \Re,\ y > 0$ と定義する．このとき，y は情報資産 i の x(機密性 (C)，完全性 (I)，可用性 (A) の別) について，重要性 y の値を持つという意味である．

3.3　情報セキュリティにおける脅威

情報セキュリティにおける脅威とは，単に情報が盗まれたり，破壊されたりするだけでなく，許可されたアクセスの範囲であるにもかかわらず，アクセスできないとか，人の操作の誤りや，機械の故障など，非常に多岐に渡る．本論文ではこのような脅威を $T = \{(t_p^{L1}, t_s^{L1}, t_C^{L1}, t_I^{L1}, t_A^{L1}), \ldots, (t_p^{Ln}, t_s^{Ln}, t_C^{Ln}, t_I^{Ln}, t_A^{Ln})\}$ と定義する．ここで，Li は脅威のラベル，t_p^{Li} はその脅威が 1 日以内に発生する確率，t_s^{Li} は N_s の部分集合で脅威の発生する場所，$t_C^{Li}, t_I^{Li}, t_A^{Li}$ は機密性，完全性，可用性のどれに影響を与えるかを示すフラグであり，1(真) または 0(偽) の値を持つ．集合 T を定義するために，各脅威の発生する確率を計らなければならないが，実際には適切な方法がなく困難なため，リスクアセスメント担当者が経験に基づいて決定する場合が多いだろう．例えば，インターネット空間から既知の脆弱性を攻撃するという脅威は 1 日に数百回と発生するので，1 日あたりの確率値としては 1 であろう．また，泥棒が建物に侵入しようとする確率は，30 分の 1 程度かもしれない．

3.4　障　　壁

情報資産グラフ G で，情報資産間関係が示されているとき，情報資産を様々な脅威から守るということを計算するため，障壁の概念を定義する．障壁とは情報やサービスがある空間から別の空間へ，情報資産を経由して移動する場合，その情報資産によって予定された移動が機密性，完全性，可用性の観点に置いて，確実に実行できることを保証する仕組みである．具体的には無停電電源装置によるバックアップやポートフィルタリングなどを指す．

本論文では障壁の効果を脅威別の確率値の低減という形で定義する．また障壁の機能を定義可能な対象を情報資産とする．つまり，障壁の集合は $B(i,t) = q, i \in N_i,\ t \in T,\ 0 \leq q \leq 1$ となる．この集合の各要素は情報資産 i が脅威 t に対して，その発生確率を q 倍に低減できると読む．情報資産 i が脅威 t に対して全くの無関係だった場合，q は 0 とする．また，情報資産 i が脅威 t に対して，何ら防御しない場合は q は 1 とする．先の脅威の発生確率が経験的に決められるように，防御による低減の割合も計測困難な事象であり，経験的に決められることが多くなると考えられる．例えばファイアウォールの場合，TCP/IP における全体の重要なポート数に対して，実際に通過可能なポート数を低減の割合と定義するのも一つの考えである．

3.5　代　　替

脅威の発生を押さえる手段は，障壁によるものだけでなく，脅威の発生時に速やかに代替手段に移行するという方法も考えられる．本論文ではそのような手段を代替と呼ぶことにする．例えば，受電系統を 2 箇所にすることが代替である．

情報資産間グラフ上で代替の集合は $S = \{(i,t,s_1,s_2) | i \in N_i,\ t \in T, s_1, s_2 \in N_s,\ (i,s_1) or (s_1,i) \in E,\ (i,s_2) or (s_2,i) \in E\}$ と定義する．この集合の各要素は，情報資産 i にとって空間 s_1 と s_2 は脅威 t に対して代替であると読む．集合の定義における条件の内，$(i,s_1) or (s_1,i) \in E,\ (i,s_2) or (s_2,i) \in E$ は情報資産 i にとって，空間 s_1, s_2 が隣接していなければならないことを示す．

3.6　リスク値の計算

ある脅威の発生する割合が確率事象として定義されている場合，情報セキュリティ上のリスク値は情報資産の重要度を加味した期待値として表現されることが適当である．そのためには，ある脅威が情報資産に実際に影響を及ぼす確率を計算しなければならない．ここでは，その計算方法について議論する．

情報資産 i が機密性，完全性，可用性の別 x について脅威 t の影響をどの程度受けるのかを計算するには，次のような方法を提案する．

$$P_i(i,x,t,N) = \begin{cases} 0 & \text{if } i \in N \text{ or } \{s'|(i,s)' \in E\} = \emptyset \\ \max\limits_{s \in \{s'|(i,s') \in E\}} \{P_t(i,s,x,t,N \cup i)\} & \text{otherwise} \end{cases}$$

$$P_t(i,s,x,t,N) = \begin{cases} 1-(1-B(i,t) \times P_s(s,x,t,N)) & \\ \quad \times(1-B(i,t) \times P_s(s',x,t,N)) & \\ & \text{if } (i,t,s,s') \in S \text{ where } \exists s' \in N_s \\ B(i,t) \times P_s(s,x,t,N) & \\ & \text{otherwise} \end{cases}$$

$$P_s(s,x,t,N) = \begin{cases} t_p \times t_x & \\ & \text{if } s = t_s \\ 0 & \\ & \text{if } \{i'|(s,i') \in E\} = \emptyset \\ \max\limits_{i \in \{i'|(s,i') \in E\}} \{P_i(i,x,t,N \cup i)\} & \\ & \text{otherwise} \end{cases}$$

ここで，t_x は t_C, t_I, t_A のいずれかであり，引数 x と連動する．P_i および P_s は注目する節がそれぞれ情報資産または空間であった場合，そこから遡ることが可能な節の中で最も脅威の発生する確率が高い辺を選択することに相当する．P_t は最初の式が代替がある場合でかつ障壁がある場合，2 番目の式が単に障壁のみがある場合，それぞれ脅威の発生する確率を低減させることを意味する．

情報資産 i に対して，機密性，完全性，可用性の別 x について，脅威 t が具現化して損害を被る大きさをリスク値として定めると，

$$R(i,x,t) = V(i,x) \times P_i(i,x,t,\emptyset)$$

ある脅威に対して，各節でリスク値を計算するために最大値を用いることは議論の余地があるかもしれない．経済学の観点から，あるいはリスクファイナンスの観点から考えれば，ある脅威が様々パスから伝わってくる，その平均値に意味があるかもしれない．しかし，本論文で取り扱いたかった情報リスクアセスメントは，情報システムの弱点を知ることを目的としている．そのためには脅威の発生場所から情報資産までの最も高いリスク値を持つパスを発見することが重要なため，本方式を選択する．これにより，障壁や代替の変更を行った場合に弱点が移り変わる様子も容易に把握可能となる．

4. 考　　察

本論文で提案する情報リスクアセスメント手法は，他の手法と比べて非常に詳細な部分にわたって評価することが特徴である．詳細な評価のためには多くのパラメータが必要となり，評価が煩雑になる欠点がある．本論文ではこの欠点を補うため，表現方法を情報資産と空間の隣接関係というグラフにすることで克服することを試みた．これにより，新たな情報資産を追加する場合，通常何処に追加するかは分かっているはずであり，隣接する空間も把握可能であるはずなので，グラフ上のどこに節を挿入すれば良いかもすぐに分かるはずである．また，障壁や代替の概念を定義し計算可能なモデルを導入したので，それらの性能変化や増設，廃止などが有った場合にも速やかに再計算が可能であり，かつ，関係する情報資産のリスク値への影響を過不足無く計算することができる．

課題としては，設備面以外に教育，規則や人の挙動をこのモデルにどのように盛り込むかが未解決である．特に教育の効果は評価が難しく，影響範囲も広いため，ここで述べるモデルとは異なるものが必要になるかもしれない．今後は，このモデルを用いて様々なリスクアセスメントを実行することでモデルの精度を上げていきたいと考えている．

文　　献

[1] 英国規格協会: "BS 7799 Part 2:2002, defines the specification for an Information Security Management System," 2002.

[2] 日本情報処理開発機構: "ISMS 評価基準 Ver.2.0", http://www.isms.jipdec.jp/v2/index.html, 2003.

[3] 岡田, 川上, 他: "情報セキュリティ認証取得の決定版", 日本工業新聞社, 2003.