教育効果を考慮した セキュリティ対策選定手法の検討

加藤 岳久† 山本 匠† 西垣 正勝†

中村らは，情報セキュリティ対策を効率よく選択する具体的な方法論として，資産・脅威・対策の関係をモデル化することによってセキュリティ対策選択問題として定式化する方法を提案した．本稿では，企業等の組織で導入されているセキュリティ対策の効果が従業員の教育レベルによって左右されることに鑑み，中村らが提案したモデルにセキュリティ教育による対策効果およびそれに要するコストの項を追加することによって，セキュリティ対策選定に関する定式化を拡張する．

A Proposal of Security Measure Selection Considering the Effect of Education

Takehisa KATO† Takumi YAMAMOTO†
Masakatsu NISHIGAKI†

Nakamura et al. proposed a method to formulate an optimization problem to select security countermeasures that maximize cost-effectiveness, which is established by modeling the relationship between assets and threats and countermeasures. The effectiveness of countermeasures are, however, also depending on the user's security consciousness which is expected to be nurtured through security education. Therefore, this paper studies a strategy to modify the formulation proposed by Nakamura et al. to achieve more accurate security countermeasure selection by considering effect of education.

1. 背景

情報システムの導入なくしては，情報資産や業務の様々な運用管理を行うことが困難な時代になっている．このため情報マネジメントは各組織にとっての最重要課題の一つと認識されている．2005 年 10 月に ISMS 認証基準の国際規格が ISO/IEC 27001:2005 として発行されたことを受け，国内でも 2006 年 5 月に JIS Q 27001 が発行され，ISMS (Information Security Management System ： 情報セキュリティマネジメントシステム) 適合認証制度として運用が始まっている．認証を受ける組織の数は堅調に増加しており（図 1），また企業等では認証を取得しないまでも，情報セキュリティポリシを策定し，ポリシに従い構築したネットワークやシステムの運用管理を行う組織が少なくない．

これにともない，組織のリスク分析を行うための方法論やツールが整備される[12]とともに，経済学的なアプローチによって組織にとって最適なセキュリティ対策を選択する方法論の研究が進められてきている[13]-[17]．この中で，2004 年に中村らによって提案された方法[10]は，資産・脅威・対策の関係を適切かつ簡便にモデル化することによってセキュリティ対策選択問題を離散最適化問題として定式化しており，具体的な情報セキュリティ対策を効率よく選択することが可能となっている．

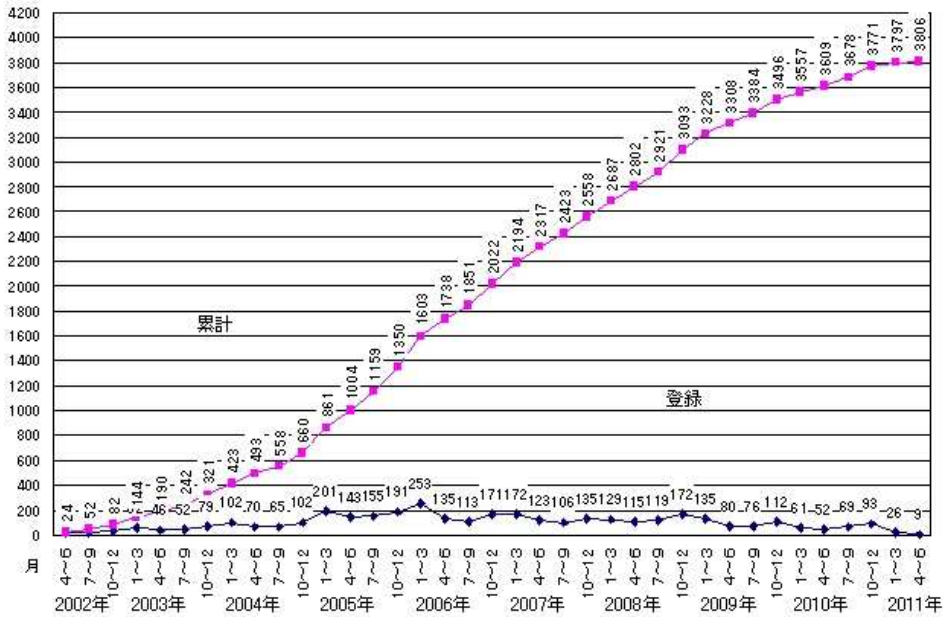

図 1. ISMS 認証取得組織数推移[1]

(財)ニューメディア開発協会の調査によれば，企業が ISMS を取得する目的として，情報資産の明確化と整理（約 80%），事故発生時の体制・計画の整備（約 62%），情報流出や漏え

† 静岡大学創造科学技術大学院，Graduate School of Science and Technology, Shizuoka University

いの防止・軽減(約 61%)を挙げている. しかし, その一方で, 実業務と ISMS との乖離を約 26.5%の企業が感じており, 前回調査から 2 倍以上増加したと報告している[2]. 実際, Verizon Business 社による企業の情報流出事件に関する実態調査報告書では, 情報が流出した企業のうち, 59%はセキュリティポリシと手順を定めておきながら実行していなかったと報告している. また, 情報漏えいの 87%は適切な対策を講じれば防止できたとも指摘している[3]. この様に, ISMS を導入する企業は多いが, 実業務との乖離があり, 決められた手順による運用がなされておらず, 情報漏えい等のセキュリティ事故の発生につながっていることがわかる.

決められた手順が守られない理由として, 従業員のリスク認知意識の欠如による規則違反がその主な原因となっていると, 松本は分析している[4]. リスク認知意識の低い従業員の「うっかり」や「慢心」等のヒューマンエラーが, 常識的には認められない操作ミスにつながり, セキュリティ事故が引き起こされる. 個人情報漏洩インシデントに焦点をあてた報告[6]においても, やはり, 同様の知見が得られており, 管理ミス, 誤操作, 紛失・置忘れなどのヒューマンエラーが情報漏えいの原因の上位 85%以上を占めていると報告されている.

この様な「うっかり」や「慢心」によるヒューマンエラーに対し, 大和田らは教育によるリスク認知向上施策等, 3 つの柱からなる情報セキュリティ対策を提案している[7]. 竹村も, 従業員への Web 調査結果から, 問題行動をとる従業員のセキュリティ意識が低いことを示し, 情報セキュリティ教育への意識が高ければ, 従業員は問題行動を起こしにくくなり, 対策を遵守する可能性がある, としている[8]. 初期段階でのミスほど被害の拡大を招くため, 事前の教育によって, 情報摂取の段階で危険を予知し回避する能力を養成することは確かに重要である[5].

ISMS の運用に教育が効果的であることは, 現場レベルでも認知されており, 例えば, 情報セキュリティに関するインターネット利用者意識調査 2008 によれば, 企業等では, 社員への情報セキュリティ教育をきちんと行うべきであり, 研修の機会を増やすべきであると考えている(図 2)[9]. また, 企業内の情報管理に対しては, 技術的対策を求めると共に, 情報管理のルールを明確にし, 教育により周知徹底を図るべきと考えている(図 3)[9].

以上から, 企業での情報セキュリティ事故の多くはヒューマンエラーが原因で起きており, これを防ぐためには従業員のセキュリティ意識(リスク認知意識)を高めることが重要で, そのためには情報セキュリティ教育の質と量を確保すべき, ということがわかる. すなわち, 組織において導入されている情報セキュリティ対策の対策効果は, その組織において従業員にどのような情報セキュリティ教育が実施されたかによって左右されることになる. そこで本稿では, 中村らが資産・脅威・対策の三者を用いて定式化したセキュリティ対策選択問題[10]に, 情報セキュリティ教育の効果を導入し, 中村モデルの拡張を行う.

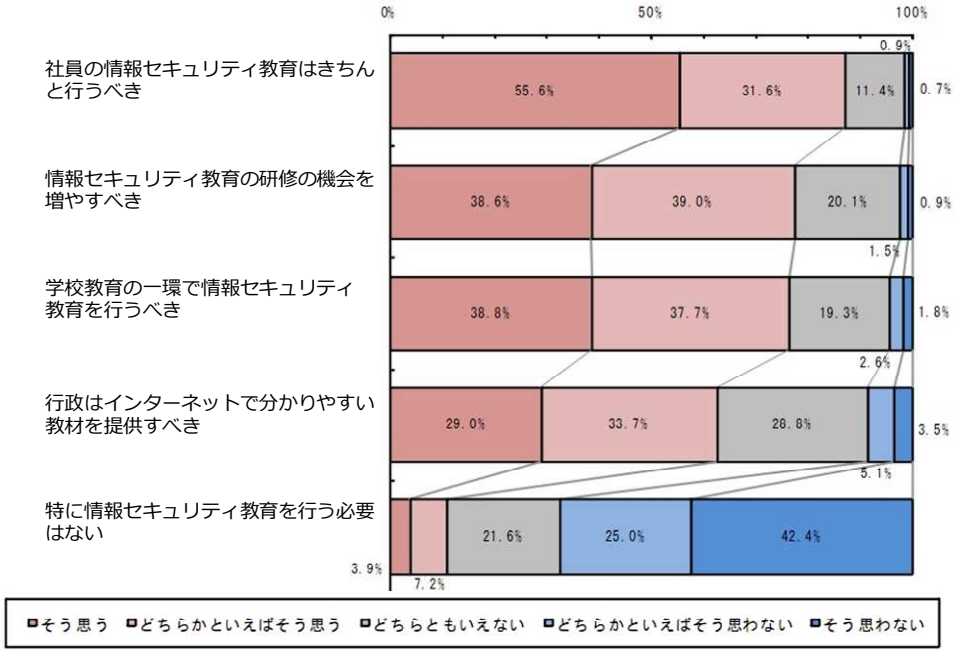

図 2. 情報セキュリティ教育に対する考え方[9]

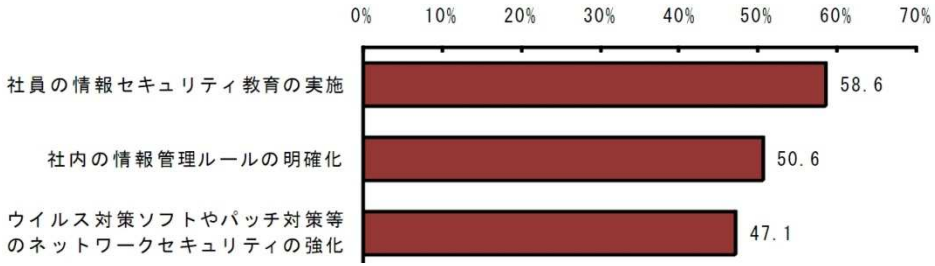

図 3. 企業内の情報管理を徹底させるために望ましいと考える方策[9]

2. 中村らのセキュリティ対策の選定方式

中村らは，情報資産，脅威，セキュリティ対策の関係をモデル化し，セキュリティ対策選択問題を定式化した[10]．中村モデルでは，一定期間後に脅威により失われなかった情報資産の価値（残存資産）を最大化するセキュリティ対策を見つけるというアプローチによって，セキュリティ対策選定問題を定式化する．中村モデルにおけるパラメータを表 1 に示す．

表 1. 中村モデルにおけるパラメータ[10]

A_k (*Asset*)	組織内の資産．総資産数を K とし，複数の資産を k $(1 \leqq k \leqq K)$ で区別する．
V_k (*Value*)	資産 A_k の価値
T_j (*Threat*)	資産 A_k に対する脅威．脅威の総数を J とし，複数の脅威を j $(1 \leqq j \leqq J)$ で区別する．
P_j (*Probability*)	一定期間内に脅威 T_j が発生する確率
E_{jk} (*Effect Flag*)	脅威 T_j が資産 A_k に影響するか否かのフラグ
CM_i (*Countermeasure*)	脅威 T_j に対する情報セキュリティ対策．情報セキュリティ対策の総数を I とし，複数の対策を i $(1 \leqq i \leqq I)$ で区別する．
C_i (*Cost*)	情報セキュリティ対策 CM_i にかかるコスト$(1 \leqq i \leqq I)$
S_i	情報セキュリティ対策 CM_i を実施するか否かのフラグ $(\in \{0, 1\})$
R_{ji} (*Risk Reducing Rate*)	脅威 T_j となる攻撃が発生した場合，情報セキュリティ対策 CM_i によりその攻撃の成功率が減少する割合．脅威 T_j となる攻撃に対する対策を行わなければ，攻撃が発生すると確率 1 で成功する．対策を行なっていれば，攻撃の成功率は $(1- R_{ji})$ に減少する．

まず，何のセキュリティ対策も施されていない場合の残存資産 *RA* を考える．情報資産 A_k は，$E_{jk} = 1$ の脅威 T_j の影響を受けると資産が失われる．無対策の状態では，脅威の発生によって資産は必ず失われる（脅威の攻撃成功確率は 1 である）ため，一定期間内に情報資産 A_k が失われる確率は，その期間内に脅威 T_j が発生する確率 P_j に等しい．よって，情報資産 A_k が残る確率は，情報資産 A_k に対して $E_{jk} = 1$ である全ての脅威 T_j が発生しない確率

$$\prod_j \left(1 - E_{jk} P_j\right)$$

と等しくなる．よって，一定期間後に残存している情報資産 A_k の価値 V_k の期待値は

$$V_k \prod_j \left(1 - E_{jk} P_j\right)$$

となり，残存する全資産の総和である残存資産の期待値 RA は，

$$\sum_k \left\{ V_k \prod_j \left(1 - E_{jk} P_j\right) \right\} \qquad \cdots (2\text{-}1)$$

となる．

次に，セキュリティ対策を行った際の残存資産ついて考える．情報セキュリティ対策 CM_i により脅威 T_j の攻撃成功確率は $(1- R_{ji})$ に低減されるため，脅威 T_j の攻撃により資産 A_k が失われる確率は，脅威 T_j の発生確率 P_j とその攻撃成功確率 $(1- R_{ji})$ の積 $P_j(1- R_{ji})$ となる．実際には採用される情報セキュリティ対策は一つではなく，複数の対策 CM_i $(1 \leqq i \leqq I)$ それぞれが確率 R_{ji} で脅威 T_j の攻撃成功率を下げる．採用されている全ての情報セキュリティ対策の効果が単純に相乗されると仮定した場合，各対策の選択/非選択のフラグ S_i を用い，脅威 T_j の攻撃成功確率は

$$\prod_i \left(1 - R_{ji} S_i\right)$$

と表される．よって，脅威 T_j により一定期間内に情報資産 A_k が失われる確率は，

$$P_j \prod_i \left(1 - R_{ji} S_i\right) \qquad \cdots (2\text{-}2)$$

となる．これは，式(2-1)において $P_j \times 1$（無対策時においては脅威 T_j が確率 P_j で発生した場合に確率 1 で攻撃が成功する）で示されていた資産 A_k の損失確率が，対策の採用によって式(2-2)に変化することを意味する．従って，式(2-1)の P_j を式(2-2)に変更することで，$S_i = 1$ である情報セキュリティ対策 CM_i が選択された場合の残存資産の期待値 *RA* は

$$RA = V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i\right) \right] \qquad \cdots (2-3)$$

と定式化される．

情報資産を脅威から守ることは，情報セキュリティ対策により多くの情報資産を残すことである．つまり，式(2-3)の残存資産の期待値 *RA* を最大化することと同意である．しかし，セキュリティ対策の採用にはコストが発生する．対策のコスト Cost は

$$Cost = \sum_i C_i S_i \qquad \cdots (2-4)$$

で表されるため，残存資産 *RA* からコスト *Cost* を差し引けば，講じた情報セキュリティ対策の純粋な効果となる．以上より，セキュリティ対策問題は，

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i\right) \right] \right\} - \sum_i C_i S_i \qquad \cdots (2-5)$$

が最大となるフラグ S_i の組合せを見つける問題に帰着する．これは，

$$S_i \in \{0,1\} \quad (1 \le i \le I)$$

となる制約条件の下で，式(2-6)の目的関数を最大化するという離散最適化問題を解くことと等価となる．

3. セキュリティ教育を考慮したセキュリティ対策選定

中村らのモデルを拡張し，セキュリティ教育を考慮した形でセキュリティ対策選択問題を定式化する方式を考える．情報セキュリティ対策を，図 4 の様に

- A 郡：従業員のセキュリティ意識によって対策効果が変わらない対策
  ゲートウエイに設置されるファイアウォール，データ暗号化，等
- B 郡：従業員のセキュリティ意識によって対策効果が変わる対策
  ユーザ認証，等

に分類する．この時，A 郡の対策の効果は，表 1 の R_{ji} のみによって表せられる．一方，B 郡の対策の効果は，従業員のセキュリティ意識により効果が変わるため，R_{ji} に従業員のセキュリティ意識のレベルが乗じられた値となると考えられる．

本稿では，従業員のセキュリティ意識は，組織において実施される種々の情報セキュリティ教育 SE_m によって養われると想定する．セキュリティ教育 SE_m の効果 W_{ijm} は，その教育を受けた従業員が，その内容をどれくらい理解できると期待されるか（$0 \leqq W_{ijm} \leqq 1$）によって表す．従業員がセキュリティ教育 SE_m を通じて脅威 T_j に対するセキュリティ対策 CM_i に関する知識を 100%理解した場合（W_{ijm}=1）に，対策効果の実効値 $R_{ji} \times W_{ijm}$ は最大となる．理解度の期待値は従業員一人一人で異なるが，ここでは全従業員の理解度の平均期待値を考えることとする．パスワード認証という対策に対するセキュリティ教育は，P2P ファイル共有ソフトの使用法に対するセキュリティ教育とは異なり，同様に，パスワードの総当り攻撃という脅威に対するセキュリティ教育はウイルスメールに対するセキュリティ教育とは異なる．このため，ある一つのセキュリティ教育 SE_m の理解度 W_{ijm} は，各脅威 T_j または各対策 CM_i 毎に値が定義されることになる．セキュリティ教育に関係するパラメータを表 2 に示す．

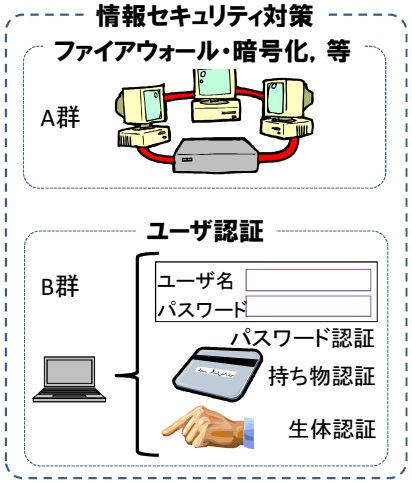

図 4. セキュリティ対策の分類

まず，残存資産の期待値 RA の式(2-3)に対して，対策 CM_i を A 群と B 群に分離すると次式となる．

$$RA = V_k \prod_j \left[1 - E_{jk} P_j \prod_{i \in A} \left(1 - R_{ji}^A S_i^A\right) \prod_{i \in B} \left(1 - R_{ji}^B S_i^B\right) \right] \quad \cdots (3-1)$$

上述のように，A 群の対策においてはその対策効果は攻撃成功減少率 R^A_{ji} のみによって表せられるが，B 郡の対策の効果は攻撃成功減少率 R^B_{ji} とセキュリティ教育の理解度 W_{ijm} との積 $R^B_{ji} \times W_{ijm}$ で表されることになる．ここで，脅威 T_j に対するセキュリティ対策 CM_i に関する知識を教える情報セキュリティ教育は一つだけではない．このため，採用されている全ての教育 SE_m $(1 \leqq m \leqq M)$のそれぞれの W_{ijm} を相乗し，

$$R_{ji}^B \prod_m \left(W_{ijm} S_m\right)$$

によって，B 群の対策の対策効果を定式化する．以上より，式(3-1)は

$$RA = V_k \prod_j \left[1 - E_{jk} P_j \prod_{i \in A} \left(1 - R_{ji}^A S_i^A\right) \prod_{i \in B} \{1 - R_{ji}^B \prod_m \left(W_{ijm}\right) S_i^B\} \right] \quad \cdots (3-2)$$

となる．

表 2. セキュリティ教育を考慮した定式化に用いるパラメータ

SE_m (*Security Education*)	情報セキュリティ教育. 情報セキュリティ教育の総数を M とし, 複数の教育を m ($1 \leqq m \leqq M$) で区別する.
C_m (*Cost*)	情報セキュリティ教育 SE_m にかかるコスト($1 \leqq m \leqq M$)
W_{ijm} (*Comprehension Level*)	情報セキュリティ教育 SE_m の実施によって期待される脅威 T_j および対策 CM_i に関する従業員の理解度
S_m	セキュリティ教育 SE_m を実施するか否かのフラグ ({0, 1})

情報資産を脅威から守ることは, 情報セキュリティ対策により多くの情報資産を残すことである. つまり, 式(3-2)の残存資産の期待値 RA を最大化することと同意である. しかし, ここに情報セキュリティ教育のコスト $Cost$

$$Cost = \sum_m C_m S_m \qquad \cdots (3-3)$$

を加えることによって, 情報セキュリティ教育を考慮したセキュリティ対策問題は

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_{i \in A} \left(1 - R_{ji}^A S_i^A\right) \prod_{i \in B} \{1 - R_{ji}^B \prod_m \left(W_{ijm}\right) S_i^B\} \right] \right\}$$

$$- \left\{ \sum_i C_i S_i + \sum_m C_m S_m \right\} \qquad \cdots (3-4)$$

が最大となるフラグ(S_i, S_m)の組合せを見つける問題に帰着する. これは,

$$S_i = (S_i^A, S_i^B) \in \{0,1\} \quad (1 \leq i \leq I)$$

$$S_m \in \{0,1\} \quad (1 \leq m \leq M)$$

となる制約条件の下で, 式(3-4)の目的関数を最大化するという離散最適化問題を解くことと等価となる.

4. まとめ

本稿では, 中村らが提案した資産・脅威・対策の三者モデルに基づく情報セキュリティ対策選択問題に対して, 情報セキュリティ教育を考慮したモデルの拡張を提案した. 今後は, 本方式の実用性を検証するためのシミュレーションを行い, 有用性を実証する. 本稿においては, 教育によって期待される従業員の理解度 W_{ijm} によって教育効果を定式化したが, 実際の教育現場では期待通りの教育効果が必ず得られるとは限らない. 従業員に対するテスト等を通じて実際の教育効果を測り, その結果によってセキュリティ対策選択問題のパラメータを適応的に修正していく必要があると考えている. また, 情報セキュリティ事故が発生してしまった後, もしくは事故につながるリスクが新たに発見された場合に実施される事後教育(ケーススタディ, e-Learning, 等)も考慮した情報セキュリティ対策選択問題の定式化の方針を具体化し妥当性の評価をしていく.

参考文献

[1] (財)日本情報経済社会推進協議会, 認証取得組織数推移, 認証機関別・県別認証取得組織数, http://www.isms.jipdec.jp/itsms/lst/ind/suii.html (2011.5.4 アクセス)

[2] (財)ニューメディア開発協会, ISMS 第三者認証制度をより有効なものにするための ISMS 認証事業所調査, http://www.uchidak.com/isms/2010/2010_ISMS_Report.pdf (2011.4.20 アクセス)

[3] Verizon Business, 2008 Data Breach Investigations Report, http://www.verizonbusiness.com/resources/security/databreachreport.pdf (2011.4.18 アクセス)

[4] 松本匡史, IPS と NAC によりシステム的に構築する社内セキュリティポリシー, http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1199, McAfee blog (2011.4.18 アクセス)

[5] 大山正, 丸山康則, ヒューマンエラーの科学, 麗澤大学出版会(2004)

[6] セキュリティ被害調査ワーキンググループ, 2009 年情報セキュリティインシデントに関する調査報告書 第 1.1 版, NPO 日本ネットワークセキュリティ協会(2010.9)

[7] 大和田竜児 , 内田勝也, 従業員のリスク行動に対する企業の取り組みモデルの提案, 情報処理学会研究報告, 2010-DPS-142(52), pp.1-81(2010.2)

[8] 竹村俊彦, Web アンケート調査データを用いた情報セキュリティ教育に対する意識と行動に関する分析, 情報通信政策レビュー (2010.7) http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/01/takemura2010.pdf (2011.3.10 アクセス)

[9] NRI セキュアテクノロジーズ, 情報セキュリティに関するインターネット利用者意識調査 2008, 情報セキュリティレポート Vol.4 No.1 (2008.5), http://www.nri-secure.co.jp/news/2008/pdf/20080522_net.pdf (2011.4.23 アクセス)

[10] 中村逸一, 兵藤敏之, 曽我正和, 水野忠則, 西垣正勝, セキュリティ対策選定の実用的な一手法の提案とその評価, 情報処理学会論文誌 Vol.45 No.8, pp.2022-2033(2004.8)

[11] (社)情報処理推進機構, 情報セキュリティマネジメントと PDCA サイクル, http://www.ipa.go.jp/security/manager/protect/pdca/index.html (2011.5.17 アクセス)
[12] Rok Bojanc, and Borka Jerman-Blazic.: An economic modeling approach to information security risk management, International Journal of Information Management, Volume 28, Issue 5, pp.413-422(2008.10)
[13] Gordon, L.A., Loeb, M.P., The Economics of Information Security Investment, ACM Trans. Information and System Security, Vol.5, No.4, pp.438-457(2002).
[14] 松浦幹太, 情報セキュリティと経済学, 2003 年暗号と情報セキュリティシンポジウム予稿集, Vol.1, pp.475-480(2003.1)
[15] 永井康彦, 藤山達也, 佐々木良一, セキュリティ対策目標の最適決定技法の提案, 情報処理学会論文誌, Vol.41, No8, pp.2264-2271(2000.8)
[16] 榊啓, 矢野尾一男, 小川隆一, 多目的最適化によるセキュリティ対策立案方式の提案, 2007 年コンピュータセキュリティシンポジウム論文集 pp.193-198(2007.10)
[17] 大谷尚通, 不正アクセス行為の状態遷移モデルに基づくセキュリティ脅威と対策作成方法, 2007 年コンピュータセキュリティシンポジウム論文集, pp.283-288(2007.10)