**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**

**１. はじめに**

セキュリティは常に進化しており, 新しい攻撃手法が次々に考えられていて, それに対応するように, 防御手法もどんどん考えられている. よって, 新しい認証方法や暗号化に関する論文が既にたくさんあるが, 実際に情報端末をつかう利用者や企業にとってみれば, それに対応する時間やお金が無いというのが現状である. 文献１）では, 企業が実際にセキュリティ対策をする上で, つまり, お金や設備とのすりあわせの中で, どのようにすれば最も効果があるのかという, 実用的な内容であったことに, 魅力を感じ紹介することにした. この論文では, 近頃, 「情報」というものが, 企業にとって大切な資産であることが言われていることを前提に, 効果的な対策手法に関しては, セキュリティ担当者の勘や経験に頼っている事実に問題提起をする. この問題を解決するために著者は資産, 脅威, 対策の三点をリストアップし, それらの関係を抽象化し, それらを組み合わせ問題(離散最適化問題)にパターン化することで, どれが最も効果的なのかということを導き, 実システムの設計者や開発者が勘や経験をもとに選択した対策との比較, 検討によって, 著者の手法が十分実用的であることを示す.

**２. 現状の対策, 課題とモデル化**

現在, 一般的にセキュリティ確保は何のために, 何を, どうやって, の順に対策を決定していき, 実施後PDCA(Plan, Do, Check, Act)を実現している. ここで, 一般的な対策を行った場合に様々な問題が生じるが, 文献１）はその中でも

(a)一部の専門家でないと対策を決定できない.

(b)その対策が効果的であるかを確認できない.

の二点を解決するための実用的手法を検討するものである. そのためにまず, 資産と価値, 脅威とそれが起こる確率, 対策とそれにかかるコストのそれぞれをセットにして, リストアップし, 「資産と脅威の関係」と「脅威と対策の関係」に分けて要素を取り出す. （モデル化を行う）そして資産, 脅威, 対策のモデル化を用いて, パターン化（定式化）を行う. ここでのセキュリティ対策は単に発生確率の高い脅威に対して行うだけでは不十分であり、対策によって, 失う資産の見込み（期待損失）がどれくらい減少するかを決定しなければならないので, （対策によって残った資産の総和）−（対策コスト）の見込み額を最大化するというアプローチをとる.

(Value)：資産の価値（複数の資産を下付きの*k*で区別する. ）

(Effect Flag)：脅威が資産に影響するか否かのフラグ（複数の脅威を下付きの*j*で区別する）

(Probability)：一定期間内に脅威*j*が発生する確率

(Risk Reducing Rate)：脅威*j*に関する攻撃が発生した場合において, 対策*j*によってその攻撃の成功率が減少する割合（何の対策も施されていない場合, 脅威*j*に関する攻撃が発生すると確率１でその攻撃は成功する. 対策の実施によって, 脅威に関する攻撃の成功率は1−に減少する. )

(Select Flag)：対策*j*を選択するか否かのフラグ１により選択, ０により非選択を表す.

(Cost)：対策*j*の実施に必要なコスト

**３. 実システムへの適用**

文献１）では, この組織より, リスク分析自体を公表しないこと, 公表する評価結果からその組織が推定できないことなどを条件に２社からリスク分析表の提供を受けた. その際, 著者の手法で必要となる種々のデータが質を表すものであるため, 数に置き換えるために以下の工夫を行った.

1. 情報資産額 (Vk)

1万円～1億円までを5段階で評価し、それぞれの段階の中間値を資産額とする

1. 脅威の発生確率 (Pj)

3段階で評価し、ぞれぞれの発生確率を0.5, 0.3, 0.1とする

1. 対策 (CMi)

ECOMの「情報セキュリティ対策マネジメント標準の解説」をもとに列挙する

1. 対策コスト (Ci)

実コストまたは一般的なコスト（製品, ランニングコストの合計）とする

1. リスク減少率 (Rij)

対策選定担当者からのヒアリングを通して5段階で評価し, 0.7, 0.5, 0.3, 0.1, 0とする

今回は離散最適化問題であるので, 対策数が増えてくると組み合わせが爆発的に増加し, 総当りで最適解を導くことはできないため, 準最適解を計算している。また,この手法の評価尺度を便宜的に下記のとおり設定する.

適度率＝※１

※１「合致対策数」は選択された対策のうち, 従来の方法でも, この手法でも選択された対策の総数. 「非合致対策数」は選択された対策のうち, 従来の方法, または, この手法のいずれかでしか選択されていない対策の総数とする.

本評価結果では, A社では18/24=75%, B社では16/22=73%となり, この手法の実用性を確認できる結果を導くことができた.

**４. まとめ**

複数の脅威が合わさってはじめて発生するリスクや類似の対策が選択された際の対策効果の実効性, 相補的な対策が選択された際の相乗効果, 資産や対策の時間的変化に関しては論文１）のモデルから外しているが, これまで定性的にしか示されなかったセキュリティ対策の費用対効果を実際の数値として, 示すことが可能になったという点で, 多からずとも得るものがあり, ７０数パーセントという数値に関しても決して低くはないと考えられる. しかし, 文献１）の目的は２. 現状の対策, 課題とモデル化の(a), (b)で示した二点である. (a)に関しては, 著者の手法を用いることにより, 誰もがセキュリティ対策選定を行うことが出来るようになったという点で, 実用的であると言えるであろう. しかし, (b)に関しては, ECOMの「情報セキュリティ対策マネジメント標準の解説」という標準化されたものから選んだとしても, ICカード, 指紋認証, 監視員による入退出管理など, 類似する方法であった場合に, リスク減少率を設計者のヒアリングによって設定しているのでまだ, 専門家の勘や経験に依存している面があり, 著者の手法が本当に実用的であるかは, まだ議論の余地があると, 我々は考える.

今後の課題として, 効果を勘や経験ではなく論理的に評価する手法を導出してもらいたい.

**参考文献**

1. 中村逸一, 兵藤敏之, 曽我正和, 水野忠則, & 西垣正勝. (2004). 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*,  *45*(8), 2022-2033.

コピー＆ペーストで差し替えてください。

<修正案　3.実システムへの適用>---関谷

**３. 実システムへの適用**

文献１）では, この組織より, リスク分析自体を公表しないこと, 公表する評価結果からその組織が推定できないことなどを条件に２社からリスク分析表の提供を受けた. その際, 著者の手法で必要となる種々のデータが質を表すものであるため, 数に置き換えるために以下の工夫を行った.

1. 情報資産額 (Vk)

1万円～1億円までを5段階で評価し、それぞれの段階の中間値を資産額とする

1. 脅威の発生確率 (Pj)

3段階で評価し、ぞれぞれの発生確率を0.5, 0.3, 0.1とする

1. 対策 (CMi)

ECOMの「情報セキュリティ対策マネジメント標準の解説」をもとに列挙する

1. 対策コスト (Ci)

実コストまたは一般的なコスト（製品, ランニングコストの合計）とする

1. リスク減少率 (Rij)

対策選定担当者からのヒアリングを通して5段階で評価し, 0.7, 0.5, 0.3, 0.1, 0とする

今回は離散最適化問題であるので, 対策数が増えてくると組み合わせが爆発的に増加し, 総当りで最適解を導くことはできないため, 準最適解を計算している。また,この手法の評価尺度を便宜的に下記のとおり設定する.

適度率＝※１

※１「合致対策数」は選択された対策のうち, 従来の方法でも, この手法でも選択された対策の総数. 「非合致対策数」は選択された対策のうち, 従来の方法, または, この手法のいずれかでしか選択されていない対策の総数とする.

本評価結果では, A社では18/24=75%, B社では16/22=73%となり, この手法の実用性を確認できる結果を導くことができた.

<修正案おわり>