日本オペレーションズ・リサーチ学会
2004年秋季研究発表会

一般化したセキュリティの数理モデリング

セコム株式会社IS研究所　*高橋 和久　TAKAHASHI Kazuhisa
セコム株式会社IS研究所　甘利 康文　AMARI Yasufumi

1　はじめに

近年，幅広い意味で用いられている「セキュリティ」の評価に関して，チェックリスト等による定性的な手法 [1] は多数存在するにも関わらず，統一的に扱って数値で示す定量的な手法は未だ試みられていない．本稿では，一般化したセキュリティの定義に基づき，確率的アプローチによる数理モデルを提案する．

2　一般化したセキュリティ

甘利 [2] は一般化したセキュリティを「正当な目的を持たないエージェントを管理区画の中に入れないこと」と定義している．ここで，エージェントとは人や動物であったり，プログラムや病原体であったり，さまざまな様態を持つ．また，セキュリティの実現要件として，以下の 4 点を挙げている．

ボーダー明確化 ... 管理区画とそれ以外の区画 (非管理区画) を明確に区別すること

エージェント区別 ... 正当な目的を持つエージェントとそれ以外とを区別すること

選択的侵入許可 ... 正当な目的を持つエージェントのみ管理区画への侵入を許可すること

緊急対応準備 ... 正当目的外のエージェントが管理区画内に存在した場合に，被害拡大を抑制すること

以下に，物理セキュリティ，サイバーセキュリティ，ヘルスケアといった様々な分野における「セキュリティ」の事例を示す．

事例	守るべき対象	エージェント	ボーダー	緊急対応体制
侵入盗	財産	泥棒	門，玄関，窓	隣人，機械警備
データ改竄	データ	クラッカー，プログラム	ファイアウォール	監視ツール
インフルエンザ	健康，生命	病原性ウィルス	粘膜 (口鼻部)，皮膚	体内免疫，投薬

3　セキュリティレベルの定義

上記で述べた一般化したセキュリティの度合いを「正当目的外のエージェントが管理区画内に存在する確率」と「正当目的外の行為に対する被害抑制の度合い」の積で表すこととする．一方，セキュリティに関係深いリスクの大きさの定義は「損失の発生確率」と「損失の期待値」の積で表されることから，セキュリティとリスクの度合いは同一のものと見なすことができる．

セキュリティ対策を講じる者にとって，「損失の期待値」は絶対的な大きさよりも，最大値のうち期待値がどれだけ占めるか，すなわち，相対的な大きさである「損失の期待割合」の方が意味を持つであろう．また，セキュリティは「万が一」の事象であるため，非常に小さな発生確率の数値を直感的に理解することは難しい．そこで，セキュリティの度合いを表すセキュリティレベルを式 1 の如く定義する．式 1 では，対数をとることによってセキュリティレベルの構成要素の和の形式で表現しており，また，マイナスを掛けることによって正数に変換している．

(1) セキュリティレベル $[S] = -\log$(損失発生確率 $[P]$ × 損失期待割合 $[R]$)

P = エージェント存在確率 $[P_1]$ × エージェント侵入確率 $[P_2]$ × 不測事態発生確率 $[P_3]$

P_2 = 遭遇頻度 $[p_{21}]$ × 試行確率 $[p_{22}]$ × 成功確率 $[p_{23}]$

P_3 = 遭遇頻度 $[p_{31}]$ × 試行確率 $[p_{32}]$ × 成功確率 $[p_{33}]$

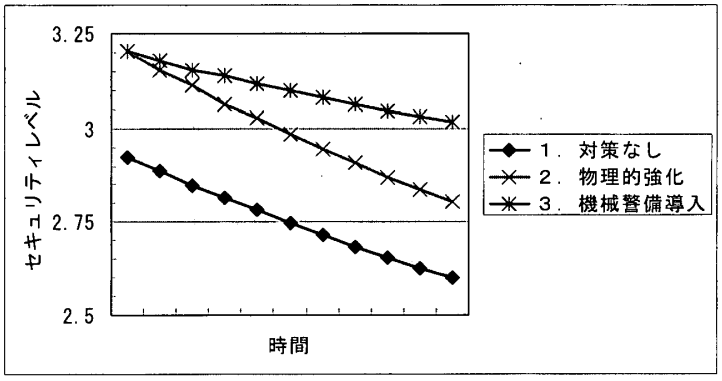
R = 緊急対応が存在しない場合の損失最大割合 $[R_1]$ × 緊急対応による軽減後の損失割合 $[R_2]$

4 「侵入盗」のシミュレーション

シミュレーションは「侵入盗」を想定して，以下の如く数理モデルの簡略化を行う．

- 遭遇頻度 (p_{21}, p_{31}) はポアソン分布，その他の確率過程 (P_1, p_{22}, p_{23}, p_{32}, p_{33}) は二項分布に従う．
- 以下のパラメータは正規分布に従い，それぞれセキュリティレベルの構成要素に影響を与える．
  - エージェント攻撃力，ボーダー防御力，予防対策強度，緊急対応強度，緊急対応所要時間
- エージェント攻撃力は時間の経過に伴い増加するという仮定のもと，次の 3 つのシナリオを用意する．
  1. セキュリティ対策を一切講じない
  2. 防犯ガラスや金庫による物理的な強化 ... ボーダー防御力，予防対策強度の増加
  3. 機械警備の導入 ... ボーダー防御力，緊急対応強度の増加，緊急対応所要時間の短縮

各シナリオに対してモンテカルロ・シミュレーションを行った結果を，以下に示す．物理的な強化と機械警備は，初めは同等の効果を示すものの，時間を経るに従ってセキュリティレベルの減少度に差が生じることが分かる．



5 おわりに

本稿で提案した数理モデルは，一般的な「セキュリティ」を統一的に扱う評価手法である．確率モデルやパラメータを適切に選択して，理論と現実の乖離を減少することによって，セキュリティ対策の効果の検証，費用対効果に基づくセキュリティ対策の立案など，様々な場面で有効活用できる可能性を秘めていると考えられる．

参考文献

[1] 「建物・設備のセキュリティシステム技術調査研究」，電気学会技術報告第 950 号

[2] 甘利 康文,「セキュリティの一般化した定義とその実現要件について」，第 36 回安全工学研究発表会