ISSN 2186-5647

セキュリティリスク管理モデルにおけるコスト制約を考慮した最適化に関する一検討

日大生産工(学部)　○黒澤 洸樹　　日大生産工　新井雅之

1. はじめに

インタネットでのビジネス・アプリケーションの開発の際に，企業に損害を与えるなどといった問題が生じるため，インターネットセキュリティが重要視されている．先行研究として，セキュリティレベルを客観的・定量的に判定するためのリスク管理モデルが提案されている[1]．しかし，数式に曖昧な点があり，実用的な計算が困難であった．本稿では，与えられた入力パラメータを元に，資産価値，リスク値を算出するセキュリティレベルのモデル化について提案し，算出方法を示す．また，コスト制約を考慮した最適な解決策の比較・評価について検討する．

2. コスト制約を考慮したセキュリティレベルのモデル化概要

いくつかの入力パラメータを用いて，資産価値，リスク値を計算し，セキュリティレベルの評価を行う．

資産価値，リスク値を計算する際に必要となる入力パラメータは以下の通りである．

・V_i　(i = 1, 2, 3, …, n_V):脆弱性．

・T_i　(i = 1, 2, 3, …, n_T):脅威．

・S_i　(i = 1, 2, 3, …, n_S):解決策への期待値．

また，資産価値，リスク値を計算する手順を図1に示す．

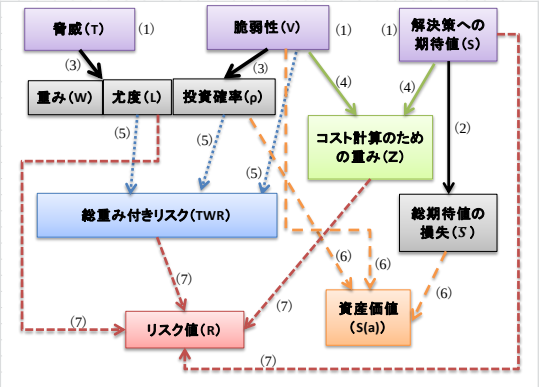

図1．計算フローチャート

計算手順の概要は以下の通りである．

(1)脆弱性，脅威，解決策への期待値を入力．

(2)解決策への期待値の入力値から総期待値の損失を出力．

(3)脆弱性，脅威の入力値から投資確率，重み，尤度を出力．

(4)脆弱性，解決策への期待値の入力値からコスト計算のための重みを出力．

(5)重み，尤度，投資確率の出力結果から総重み付きリスクを出力．

(6)投資確率，脆弱性，総期待値の損失の出力結果から資産価値を出力．

(7)総重み付きリスク，尤度，コスト計算のための重み，解決策への期待値の出力値からリスク値を出力．

詳しい値の入力・出力方法は，次節で説明していく．

Note on Optimization of Security Risk Management Model Considering Cost Constraints

Kouki KUROSAWA and Masayuki ARAI

3. 解析手順

3-1. 入力パラメータの設定

資産価値，リスク値を出力する際に，脆弱性，脅威，解決策への期待値の各リスト項目の入力値が必要になる．今回は，資産価値，リスク値を計算しやすくするために以下の条件を加える．

・脆弱性，脅威，解決策への期待値のリスト項目は 10 個までとする（$n_V = 10$, $n_T = 10$）．

・各リスト項目からの選択個数は 5 個とする（$n_S = 5$）．

脆弱性の入力パラメータとして，表 1 に示す通り，10 個の脆弱性の項目を仮定する．式(1)に脆弱性の入力パラメータの設定方法を示す．

$$V_i = \{1,\ 0\} \quad (i = 1, 2, 3, \cdots, n_V). \quad (1)$$

ここで，$V_i = 1$ なら，i 番目の項目に対して脆弱性が高く，$V_i = 0$ なら，脆弱性が低いことを意味している．

表 1. 脆弱性のリスト

パラメータ	脆弱性の種類	*CIA* への影響
V_1	パスワードを設定していない	機密性
V_2	ウィルスアップグレードをしていない	保全性
V_3	デバイスが脆弱している	可用性
V_4	管理者パスワードの開示	保全性
V_5	オープンポート端末（*SSH*）の弱点	機密性
V_6	不正な形式の*UDP*パケットの脆弱性	機密性
V_7	ルート権限を使用しているデータベース	可用性
V_8	制限付きのネットワークアプリケーション	保全性
V_9	アクセス制御が弱い、ローカルアクセスの許可	機密性
V_{10}	コントロール管理が弱い	保全性

例えば，表 1 におけるV_1は，パスワードの設定に関する入力パラメータである．設定をしていない場合は，$V_1 = 1$ と入力を行い，設定している場合は、$V_1 = 0$ と入力を行う．

次に，脅威の入力パラメータとして，表 2 に示す通り，10 個の脅威の項目を仮定する．式(2)に脅威の入力パラメータの設定方法を示す．

$$T_i = \{1,\ 0\} \quad (i = 1, 2, 3, \cdots, n_T). \quad (2)$$

ここで，$T_i = 1$ なら，ある入力パラメータ i に対して脅威が大きく，$T_i = 0$ なら，脅威が小さいことを意味している．

表 2. 脅威のリスト

脅威の対象	脅威の手段	パラメータ	*T* と *V* の関係性
一般のユーザー	アクセスされやすい	T_1	$V_1, V_2, V_5, V_6, V_9, V_{10}$
	物理的な取り付け	T_2	V_1, V_4, V_5, V_6, V_9
ハッカー	ソーシャルエンジニアリング	T_3	V_4, V_9, V_{10}
	保護関連の仕組み	T_4	V_2, V_8, V_9
特殊な攻撃	管理者の制御を失う	T_5	$V_2, V_4, V_5, V_7, V_9, V_{10}$
	ウイルス、トロイの木馬、ワーム	T_6	V_2, V_3, V_8
サービスの管理者	パスワードの侵害（盗まれる）	T_7	V_1, V_4, V_7, V_8
	強制攻撃	T_8	V_1, V_3, V_4, V_9
業界	*DOS* 攻撃	T_9	V_2, V_3, V_8
	監査されない	T_{10}	V_1, V_2, V_3, V_{10}

例えば，表 2 におけるT_1は一般ユーザーに対するアクセスのしやすさに関するパラメータである．アクセスがされやすい状態なら，$T_1 = 1$ と入力を行い，アクセスされにくい状態なら，$T_1 = 0$ と入力を行う．

T と *V* の関係性の列は，脅威の入力パラメータの設定によって，脆弱性が高くなってしまう可能性があるか，または，投資確率の出力結果に影響するような組み合わせを示している．

最後に，解決策の期待値の入力パラメータの設定を行うために，10 個の入力パラメータ項目を仮定する．表 3 に仮定した解決策への期待値のリストを示す．表 3 を参照にして，解決策の期待値の入力パラメータを設定する．式(3)に解決策への期待値の入力パラメータの設定方法を示す．

$$S_i = \{1, 0, -1\} \quad (i = 1, 2, 3, \cdots, n_S). \quad (3)$$

ここで，$S_i = 1$ なら，ある入力パラメータ i に対して解決策が実施されたことを意味する，$S_i = 0$ なら，解決策が実施されていないことを意味する，$S_i = -1$ なら，解決策が実施したが，別の問題が生じることを意味している．

表 3. 解決策のリスト

パラメータ	種類	解決手段	主流の解決策
S_1	技術面	識別管理	メンテナンスシステムのユーザー
S_2	技術面	システムの保護	システムの保護（OS）
S_3	技術面	検出システム	ファイヤーウォールの作成
S_4	技術面	ウィルスの検出	ウィルス対策システムの導入
S_5	操作面	ウィルスソフト	パッチの適用
S_6	操作面	制御端末	セキュリティのロック
S_7	操作面	物理的なセキュリティの提供	CCTV（監視カメラ）の設置
S_8	管理面	セキュリティの認識度&技術研修	研修の実施
S_9	管理面	定期的なシステム監査	侵入監査の実施
S_{10}	管理面	テストとメンテナンス	定期的な監査報告書の作成

例えば，表 3 の入力パラメータS_1はメンテナンスシステムユーザーの導入についてである．導入を行ったなら，$S_1 = 1$ と入力を行い，導入を行っていないなら，$S_1 = 0$ と入力を行う．また，導入を行ったが，別の問題が発生した場合は，$S_1 = -1$ と入力を行う．

3−2. 資産価値とリスク値

前節で決めた入力値を用いて，以下の出力値を得ることができる．今回は，計算仮定を省略する．

・ρ_{ji} （$i = 1, 2, 3, \cdots, n_V, j = 1, 2, 3, \cdots, n_T$）：脆弱性．

・$\bar{S}_i$ （$i = 1, 2, 3, \cdots, n_{\bar{S}}$）：総期待値の損失．

・TWR： 総重み付きリスク．

・L_{ji} （$i = 1, 2, 3, \cdots, n_V, j = 1, 2, 3, \cdots, n_T$）：尤度．

・Z_{ji} （$i = 1, 2, 3, \cdots, n_V$, $j = 1, 2, 3, \cdots, \mathrm{n_T}$）：コスト計算のための重み

上記の出力値と脆弱性の入力値を用いて，資産価値 $S(a)$を出力する．式(4)に資産価値の導出式を示す．

$$S(a) = \sum_{j=1}^{m} \sum_{i=1}^{n} \rho_{ji} * V_i * \bar{S}_i . \qquad (4)$$

リスク値も同様に中間出力値と解決策への期待値の入力値を用いて，リスク値を出力する．式(5)にリスク値の導出式を示す．

$$R = TWR - \sum_{j=1}^{m} \sum_{i=1}^{n} L_{ji} * Z_{ji} * S_i . \quad (5)$$

3−3. 資産価値とリスク値の評価方法

前節で，出力された資産価値とリスク値を用いて，CIA (Confidentiality, Integrity, Availability)に対する評価，解決策の見直しの必要性を決定する．

資産価値から CIA を評価する方法は，以下の通りとした．

・値 0～3 なら，CIA に対するレベルは 1.
・値 3.1～7 なら，CIA に対するレベルは 2.
・値 7.1～11 なら，CIA に対するレベルは 3.
・値 11.1 以上なら，CIA に対するレベルは 4.

このレベルが高い場合はリスクの危険性が大きく，低い場合はリスクの危険性が小さいことを意味している．

リスク値から解決策に対する見直しの必要性を決定する．その決定方法は，以下の通りとした．

・値 0～3 なら，優先的に見直す必要がない．
・値 3.1～7 なら，すぐに見直す必要性が低い．
・値 7.1～10 なら，見直す必要性が高い．
・値が 10.1 以上なら，優先的に見直す必要がある．

この評価で，優先的に見直す必要がないとな

る, すなわち, リスク値が0～3であることを目標とする. それ以外の場合は解決策の実施, 解決策に掛けるコストの見直しが必要であることを意味する.

4. 評価

4-1. 評価環境

本稿では, リスク値を求める際に, 3 通りの解決策の実行パターンで, 評価を行う. 今回使用する3パターンは以下の通りである.

・パターン1:表3に示した10個の解決策から5個選択し, 実行した場合
・パターン2:パターン1で選択しなかった5個の解決策を実行した場合
・パターン3:パターン1で選択した解決策から2個選択し, パターン2で選択した解決策から3個選択した場合

4-2. 結果

最初に, 3 パターンの解決策を実行した場合の資産価値を求め, 評価を行った. 3 パターンの資産価値の結果を図 2 に示す. パターン 1 は 6.6, パターン 2 は 4.5 と低い値を出力し, リスクの危険性が低いことを示した. しかし, パターン 3 では 12.1 と高い値を出力してしまい, リスクの危険性が極めて高い結果を示した. パターン1とパターン2で実施している解決策の組み合わせが重要になることが考慮されることを示すことができた.

次に, 3 パターンの解決策を実行した場合のリスク値を求め, 評価を行った. 3 パターンのリスク値の結果を図3に示す. パターン1は6.86と低い値を出力し, 解決策の見直しをする必要性が低いことを示した. しかし, パターン2は8.56, パターン3は8.46と高い値を出力し, 解決策の見直しをする必要性が高いという結果を示した. 資産価値の出力結果で, パターン 2 がリスクの危険性が一番低いことを示している. しかし, リスク値の出力では, 一番で高い結果を示した. このことから, パターン2の解決策の組み合わせは, 脅威を大きくし, 脆弱性を高くする結果を示した.

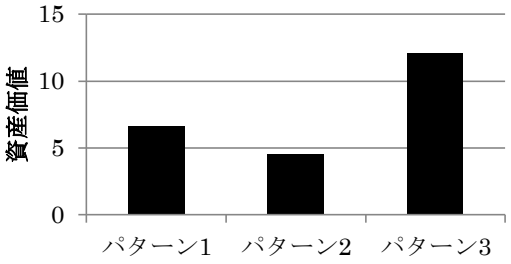

図 2. 条件に対する資産価値

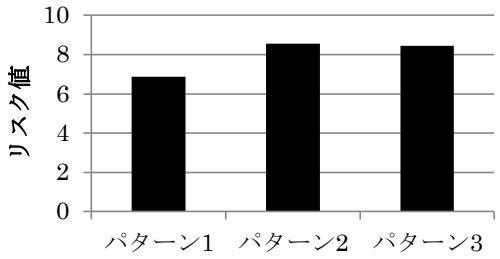

図 3. 条件に対するリスク値

5. まとめ

本研究では, 入力パラメータを設定する. 設定した入力値を用いて, 資産価値とリスク値を 3 パターン出力し, 評価・比較を行った. パターン 1 の解決策を用いることでリスク値を低くすることができる. しかし, 解決策の組み合わせ次第ではリスク値が高く出力されてしまうという結果が得られた.

今後の課題として, コストに関しての考慮を含めた最適な解決策の組み合わせを算出することが挙げられる.

参考文献

[1] Martin Suhartana, Bens Pardamean and Benfano Soewito, "Modeling of Risk Factors in Determing Network Security Level," International Journal of Security and Its Applications, Vol. 8, No. 3, pp. 193-208, 2014.