情報処理学会論文誌 Vol.58 No.12 1926–1934 (Dec. 2017)

セキュリティ運用のための経営層向けビジネスリスク評価技術の開発

杉本 暁彦[1,a)] 磯部 義明[1] 仲小路 博史[1]

受付日 2017年2月24日, 採録日 2017年9月5日

概要：近年，特定の企業を狙った標的型攻撃が増加しており，ビジネスを支えるシステムに内在する脅威を発見した場合，ビジネスへの影響を考慮した組織的な判断が求められる．しかし，専門家ではない経営層にとってセキュリティ脅威がもたらすリスクの理解が容易ではないため，対処期間の業務停止による損害の懸念から対処が遅れ，結果的に重大事故を招く場合も少なくない．そこで，本研究では，システム内の脅威がもたらすリスクからセキュリティ投資対効果を算定する技術を開発した．本技術は，経営層の適切な判断を促して経営層と情報部門の迅速な連携を可能にし，対処に経営判断が必要となるような重要インフラシステムなどの迅速な対処に資する．本研究では，プロトタイプを開発することで，提案方式により自動化が可能で，実用に耐えうることを確認した．

キーワード：セキュリティ投資対効果，リスク評価，リスクコミュニケーション，アタックグラフ，ベイジアンネットワーク，BIA

Development of the Business Risk Evaluation Technology for CxO Decision about Cyber Security Operation

Akihiro Sugimoto[1,a)] Yoshiaki Isobe[1] Hirofumi Nakakoji[1]

Received: February 24, 2017, Accepted: September 5, 2017

Abstract: Recently, targeted attacks that aim at a specified company are increasing, so organized decision is essential when threats are found in systems that related business. But there're many cases that concerns about damage due to system downtime delay response and cause serious accidents, because it's not easy for non-expert CxO to understand security risks posed by the threats. Therefore, we develop a technology that converts from risks posed by the threats to return on security investment. This technology enables appropriate CxO Decision and smooth risk communications between CxO and system managers. And it is useful for systems that require CxO Decision to response like critical infrastructure systems. This paper prove that the proposed method can automate the business risk evaluation for CxO and it can evaluate in a practical time.

Keywords: ROSI, risk assessment, risk communication, attack graph, Bayesian network, BIA

1. はじめに

ソフトウェアなどのセキュリティ上の不具合を記した脆弱性情報の報告数は年々増加している．2015 年，NIST（National Institute of Standards and Technology）[*1] や IPA（Information-technology Promotion Agency）[*2] は，約 6,500 件の脆弱性情報を公開した [1]．その中でも特に脅威度が高かった「Joomla」と呼ばれるコンテンツ管理ソフトウェアの脆弱性の場合，脆弱性情報の公開直後から同脆弱性を狙った攻撃が急増したため，企業などの情報システム部門は迅速な対処が求められた [2]．

[1] 株式会社日立製作所研究開発グループ
Research & Development Group, Hitachi, Ltd., Yokohama, Kanagawa 244–0817, Japan
[a)] akihiro.sugimoto.zd@hitachi.com

本論文は第 74 回コンピュータセキュリティ研究会で著者が執筆した「サイバーセキュリティ脅威対策のためのビジネスリスク評価システムの提案」を元としている．

[*1] NIST は，NIST の米国登録商標です．
[*2] IPA は，独立行政法人情報処理推進機構の登録商標です．

このように，システムに内在する脅威を発見した場合，情報部門では迅速な対処が求められるが，インフラシステムのような重要システムでは，テスト環境での動作確認などの対処工数や対処期間の業務停止による損害が大きいため，情報部門だけで意思決定できず，経営層の判断が必要となる場合が多い．しかし，公開される脆弱性情報などのセキュリティ情報は，専門家による技術文書であるため，セキュリティの専門家でない経営者がそれらに基づいて意志決定するのは容易ではない．その結果，対処が遅れ，重大事故を招く場合も少なくない．Apache Struts と呼ばれるソフトウェアの脆弱性のように情報公開の翌日から攻撃が開始される例もあり [3]，対処における経営層の意思決定の遅延は大きな問題である．

本来，経営層とって馴染みがあり，意思決定に資する情報は，技術的な観点から脅威を定量化した評価ではなく，BIA（Business Impact Analysis）[4] のように，事業の継続性への影響などを定量化した評価である．そこで，本研究では，システム内の脅威がもたらすリスクからセキュリティ投資対効果を算定する技術を開発している [5], [6], [7], [8]．本技術では，CVSS（Common Vulnerability Scoring System）[9] のように技術的な側面から脅威をリスク評価した結果とシステムが関連する業務の業務情報を考慮し，対処にかかるセキュリティ投資の効果を算定する．これにより，経営層の適切な判断を促して経営層と情報部門の迅速な連携を可能にし，対処に経営判断が必要となるような重要インフラシステムなどの迅速な対処に資する．本研究では，実際に脆弱性公開情報を利用して実験することで，提案方式が日々のセキュリティ運用の中でも実用に耐えうることを確認した．

本論文では，まず，2 章で関連技術について説明し，3 章で課題を解決するためのセキュリティ投資対効果の算定方式について説明する．4 章では，提案方式の実証環境を説明し，その実用性を評価する．そして，5 章で結果を考察し，6 章にまとめる．

2. 関連技術

2.1 設計段階に適したセキュリティ投資対効果モデル

セキュリティ投資対効果（ROSI: Return of Security Investment）の理論的な枠組みを定義したモデルとして，Gordon らの経済モデル [10] が存在する．彼らのモデルは，脅威による情報資産の潜在的な損失とセキュリティ投資の関係を明らかにし，最適な投資額を決定することを可能にした．また，Matsuura らは，この Gordon らの経済モデルを拡張し，セキュリティ投資による攻撃の抑止効果も考慮したモデルを考案する研究 [11] を行っている．さらに，上野らの研究 [12] では，セキュリティ製品など目に見える資産へのセキュリティ投資対効果だけでなく，人材育成への投資など投資によるインビジブル・アセットの形成効果に着目し，セキュリティ投資とインビジブル・アセットの関係を実証的に検証している．

これらの研究はいずれも，システムのリプレイスの間隔など，中長期的な期間をかけてシステムのセキュリティをマクロに設計する場合に，有益な示唆を与えている．しかし，個々の脅威に単体ではなく，内在する脅威を総体として扱って評価を行うため，日々のセキュリティ運用の中で刻々と発生する具体的な脅威への対処のセキュリティ投資対効果を継続的に見積もるのには適さない．

2.2 運用段階にも適したセキュリティ投資対効果モデル

米国規格基準局から発行されたリスク分析ガイドライン（FIPS PUB 65）[13] では，年間推定損害額として，ALE（Annualized Loss Expectancy）を定義している．ALE では，損害金額や脅威の発生回数から年間の損害額を推定し，投資による損害額や発生回数の低減効果から投資対効果を明確にする．また，西垣らの研究 [14] では，対処による脅威発生確率の低減効果や対処による資産への影響をモデル化し，資産が最大となるように最適な対策案を計画する手法を提案している．さらに，佐々木らは，脅威ごとに Fault Tree 分析を行い，脅威の発生確率や資産への影響，対処の効果などの因果関係を詳細に分析し，ステークホルダごとに異なる目的を設定することで，適切な合意形成を可能にするリスク・コミュニケーションの研究 [15] を行っている．

これらの手法は，システムのよりミクロな状況を反映してセキュリティ投資対効果を見積もることができ，PDCA（Plan Do Check Action）サイクルで運用するうえで適切なセキュリティ対処計画の策定を可能にする．しかし，近年では脅威を発見してから翌日までに対処が必要な状況 [3] にあり，経営層における迅速な判断が求められている．これらの手法では，脅威の発見からセキュリティ投資対効果の見積りまでを機械的に行う方法までは言及されておらず，上記のような迅速さの観点から評価されていない．

そこで，本研究では，脅威の発見からセキュリティ投資対効果の見積りまでが可能なセキュリティ投資対効果の算定方法を策定し，日々のセキュリティ運用の中でも実用に耐えるか評価を行う．

3. セキュリティ投資対効果算定方式

3.1 セキュリティ投資対効果算定方式の全体像

本研究で提案するセキュリティ投資対効果算定方式の全体像を**図 1** に示す．提案手法では，以下の手続きによりセキュリティ投資対効果を見積もる．

- 運用開始前
  - 本研究では，運用前の事前の取り組みとして，BIA により，システムを構成する機器からビジネスプロセスまでの関係性を記述する．BIA により，関係性を明らかにしておくことで，脅威により機器に機能不全

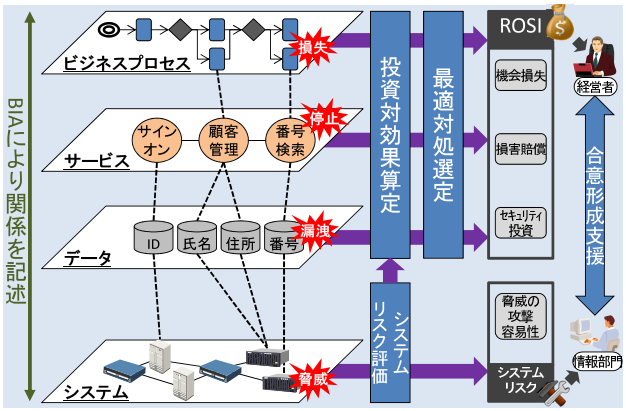

図 1 セキュリティ投資対効果算定方式の全体像
Fig. 1 Overall view of the proposed method.

表 1 CVSSv2 の構成要素 [17]
Table 1 Components of CVSSv2.

基準	概要
基本評価	「攻撃条件の複雑さ」など個々の脆弱性の技術的な特性に基づいた評価
現状評価	「攻撃コードの有無」など脆弱性を取り巻く周辺状況に基づく現状評価
環境評価	「影響を受ける対象システムの範囲」など個々のシステム状況に基づいた評価

が起こった場合に，関係するサービスやビジネス，そのビジネス要件などを逆引きすることが可能になる．

- 運用開始後
  - 日々発生する脅威を検出し，逐次システムリスクを評価する．我々は，これまでの取り組みとして，システムリスクを評価する方式を研究しており，この方式を用いる [7]（3.2 節）．
  - システムリスクおよび，BIA で定義したビジネス情報から，セキュリティ投資対効果算定モデルに基づき，検出された脅威への対処の投資対効果を算定する（3.3 節，3.4 節）．
  - 多数の脅威の中から最適な対処の組合せを選定し，投資対効果を見積もる（3.5 節）．

3.2 システムリスク評価方式

運用段階において，個別の脅威に対して，迅速にセキュリティ投資対効果を見積もるには，まず数多くの脅威の中から対処すべき脅威を特定し，危険度を自動的に評価する必要がある．ソフトウェア脆弱性の場合，評価する標準的な指標として，CVSSv2 が存在する．CVSSv2 は，**表 1** のように基本評価，現状評価，環境評価の 3 つの評価基準から構成されており，基本評価と現状評価については，情報公開機関で一律に評価され，公開情報に付されている．しかし，環境評価は，個々のシステム状況に基づき，脆弱性のある機器へのサイバー攻撃の到達可能性やその容易性，

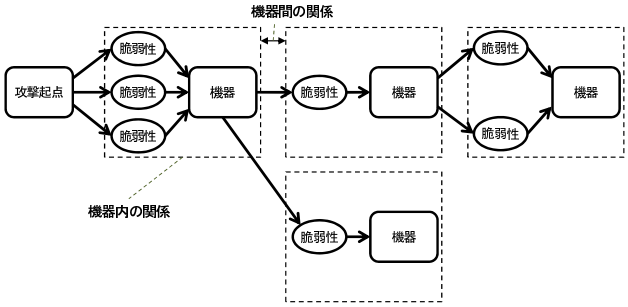

図 2 システムリスク評価におけるグラフモデル
Fig. 2 Graph model for system risk assessment.

脆弱性攻撃を受けた際に他機器に与えうる影響などを考慮して評価する必要があるため，各情報部門に委ねられており，自動化の課題となっている．

そこで，本研究では，以下 3 つの手続きにより，環境評価も考慮した脆弱性の危険度の自動的な評価を可能にしている．これにより，情報部門では，危険度に応じて対処すべき脅威の優先度付けが可能になる．

(1) インターネット上から収集した脆弱性公開情報とシステムから自動収集したシステム情報を突き合わせて，システムに内在する脆弱性を特定する．
(2) 図 **2** のように，機器と脆弱性の関係をグラフ構造化し，侵入経路を網羅的に抽出する．
(3) ベイジアンネットワーク技術 [16] により，効率的に解析することで，危険度として各脆弱性の攻撃容易性を算定する．

3.3 単体脅威のセキュリティ投資対効果算定モデル

システムレイヤでのリスク評価結果は，技術的な観点からシステムの現状を把握するのに有用であるが，経営層の経営判断に資する情報ではない．対処の重要度を適切に把握するため，機会損失や対処しなかった場合の損害額，対処にかかる費用などを考慮して，セキュリティ投資対効果を見積もる必要がある．

そこで，本研究では，脅威 v に対してインシデントが発生する前に対処を行った場合（pre）とインシデントが発生した後に事後処理を行った場合（$post$）の 2 つのケース（$case$）で発生するコストを算出し，投資対効果 $ROSI$ を算定する．具体的には，下式のように，事前（pre）の対処に必要な投資額 SI と事後（$post$）の想定被害額 BR を定義する．各変数の意味は，**表 2** に示す．

なお，情報セキュリティでは，情報の機密性，完全性，可用性を維持することを目的としており，一般的に脅威 v は，機密性，完全性，可用性のいずれかの毀損を目的としている．しかし，本研究では，脅威を分類せず，機密性，完全性，可用性のすべてが毀損されるものとする．そのため，機密性毀損の影響は情報の価値から情報毀損被害額 $LD(v)$ を算定することで見積もり，可用性毀損の影響は発

表 2 セキュリティ投資対効果算定モデルの変数
Table 2 Variable of the ROSI calculation model.

変数	概要
$LD(v)$	脅威 v による情報毀損被害額
$A(v)$	脅威 v により侵害されうるデータ
$GA(a)$	データ a の 1 件あたりの価値
$N(a)$	データ a の件数
$case$	インシデント発生前に対処する場合と発生後に対処する場合の 2 値のケース
$OL(v, case)$	脅威 v による機会損失
$T_d(v, case)$	脅威 v の対処により発生するダウンタイム
$B(v)$	脅威 v の影響を受けるビジネス
$OI(b)$	ビジネス b の営業利益
$BR(v)$	脅威 v による想定被害額
P	対処人員 1 人あたりの費用
$T_r(v, case)$	脅威 v の対処にかかる時間
$IC(v, case)$	脅威 v の対処にソフトウェアなどを導入した場合にかかるセキュリティ設備投資額
$SI(v)$	脅威 v の事前対処にかかる投資額
$ROSI(v)$	脅威 v の対処のセキュリティ投資対効果
$\alpha(v, t)$	脅威 v の危険度に基づいた係数

生するダウンタイムから機会損失 $OL(v, case)$ を算定することで見積もる．完全性毀損の影響は，毀損される情報の種類によって，情報の価値が毀損される場合やサービス継続に障害を与える場合など異なるが，提案手法では，情報を区別せずに，情報の毀損とサービスの両方が発生すると考え，情報毀損被害額 $LD(v)$ と機会損失 $OL(v, case)$ に完全性毀損の影響を見込む．

(1) 式 (1) により，脅威 v により侵害されうるデータ $A(v)$ の価値と総数から情報毀損被害額 $LD(v)$ を算定する．脅威 v により侵害されうるデータ $A(v)$ は，BIA により機器とデータの関係と，3.2 節のシステムリスク評価により機器と脅威の関係から，特定される．

(2) 式 (2) により，対処により発生するダウンタイムとビジネスによる営業利益から機会損失 $OL(v, case)$ を求める．脅威 v に関係するビジネスは，BIA とシステムリスク評価結果から特定する．

(3) 式 (3) により，人件費，セキュリティ設備投資額，情報毀損被害額 $LD(v)$，機会損失 $OL(v, case)$ を加算して，想定被害額 BR を求める．

(4) 式 (4) により，人件費，セキュリティ設備投資額，機会損失 $OL(v, case)$ を加算して，投資額 SI を求める．

(5) 式 (5) により，想定被害額 BR と投資額 SI から投資対効果 $ROSI$ を求める．被害は必ずしも発生するわけではないため，想定被害額 BR には，脅威 v の危険度に基づいた係数 $\alpha(v, t)$ をかける．一般的に危険度は時間経過により高まるため，係数 $\alpha(v, t)$ は時間 t の関数とし，3.2 節のシステムリスク評価の結果とベライゾンの調査 [18] による統計データに基づいた値とする．投資対効果 $ROSI$ は，大きいほど投資効果が高いことを意味する．

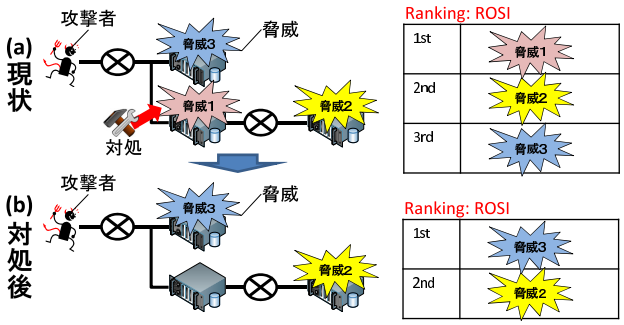

図 3 単体脅威の投資対効果算定の問題
Fig. 3 Problem of the individual ROSI calculation.

$$LD(v) = \sum_{a \in A(v)} \{GA(a) * N(a)\}, \quad (1)$$

$$OL(v, case) = T_d(v, case) * \sum_{b \in B(v)} OI(b), \quad (2)$$

$$BR(v) = P * T_r(v, post) + IC(v, post) + LD(v) + OL(v, post), \quad (3)$$

$$SI(v) = P * T_r(v, pre) + IC(v, pre) + OL(v, pre), \quad (4)$$

$$ROSI(v) = \frac{\alpha(v, t) * BR(v) - SI(v)}{SI(v)}. \quad (5)$$

3.4 複数脅威のセキュリティ投資対効果算定モデル

実際の情報システムでは，同時に脆弱性情報が公開された場合や，それまでの運用で対策不要と判断して残存させた脅威がある場合など，複数の脅威を同時にかかえることが多い．この場合，現状のシステムに対して ROSI を評価した結果のみに従い，ROSI が高い脅威から順に対処を行った場合，対処計画を見誤る可能性がある．たとえば，図 3 の例のように，(a) 現状システムの評価では，脅威 1，脅威 2，脅威 3 の対処の順に ROSI が高かったとしても，脅威 1，脅威 3，脅威 2 の順に対処すべき場合がある．なぜなら，脅威 1 に対処することで，脅威 2 の危険度が著しく下がり，(b) 脅威 1 に対処した状況下では，ROSI の値が逆転する可能性があるからである．そのため，セキュリティ投資対効果算定モデルにより，個々の脅威に対して ROSI を見積もることが可能であるが，それだけでは，適切な経営判断を下すことはできない．すなわち，複数の脅威に対する ROSI を見積もるには，以下のように ROSI の計算式 (5) を式 (8) のように拡張する必要がある．

(1) 式 (6) により，想定被害額の期待値の総和 $sumBR(V_{res})$ を求める．なお，システムに内在する脅威すべての集合を V_a とし，その中で対処を実施する脅威の集合を V_{res} とする．3.2 節のシステムリスク評価結果は，脅威の対処状況により異なる結果となるため，係数 $\alpha(v, t, V_{res})$ は，V_{res} にも依存する係数となる．なお，

対処予定の脅威（$v \in V_{res}$）に対する係数 $\alpha(v,t,V_{res})$ は，対処により危険度がなくなるため 0 となる．

(2) 式 (7) により，セキュリティ投資額の総額 $sumSI$ を求める．

(3) 式 (8) により，想定被害額と投資額の総額から投資対効果 $ROSI$ を求める．対処前の想定被害総額 $sumBR(\emptyset)$ と対処後の想定被害総額 $sumBR(V_{res})$ の差から想定被害の削減効果を評価し，さらに投資総額 $sumSI$ を減算し，投資額の総額 $sumSI$ に対する比率を計算することで，費用対効果 $ROSI(V_{res})$ を見積もる．なお，対処後にも想定被害が発生するのは，対処せずに残存させた脅威が存在するためである．

$$sumBR(V_{res}) = \sum_{v \in V_a} \{\alpha(v,t,V_{res}) * BR(v)\}, \quad (6)$$

$$sumSI(V_{res}) = \sum_{v \in V_{res}} SI(v), \quad (7)$$

$$ROSI(V_{res}) = \frac{sumBR(\emptyset) - sumBR(V_{res}) - sumSI(V_{res})}{sumSI(V_{res})}. \quad (8)$$

3.5 脅威に対する対処の最適な選定方式

前記モデルにより，セキュリティ投資対効果を算定する場合，対処予定の脅威 V_{res} の組合せ 1 つ 1 つに対して，3.2 節のシステムリスク評価と 3.4 節の ROSI 算定を行う必要があるため，計算コストが増大することが予想される．図 3 の例程度の規模のシステムであれば，すべての脅威の組合せを総当たりで評価し，最適な組合せを評価することは難しくない．しかし，機器数が増えるにつれて，その組合せの数が爆発してしまい，より効率の良い最適化問題 [19] を解くアルゴリズムが必要となる．

最適化問題を解く手法には，時間をかけて大域的最適解を求める方法と短時間に局所最適解を求める方法が考えられるが，本研究では，日々の運用の中でリスク評価する点を考慮し，以下の点に着目した．

- 日々のセキュリティ運用で利用可能な時間で評価する．
- 新たな脅威が発生しうるため，大域的最適解は時々刻々と変化する．そのため，時間をかけて大域的最適解を求める手法は適さない．
- セキュリティ運用では，脅威の発見・評価・対処のサイクルを回す．局所最適解であってもシステムの安全性を高める方向に働き，改悪はしないため，素早くサイクルを回すことがより安全性を高めることにつながる．

以上より，本研究では，局所最適解を求める最適化方法を検討した．また，セキュリティポリシにより，最適化したい目的関数や制約条件は異なると考えられるが，一般的なセキュリティ運用では投資対効果を最大化したいと考え，一例として目的関数をセキュリティ投資対効果 $ROSI(V_{res})$ とした．また，概してセキュリティ投資にかけられる投資額には，制限があるため，一例として制約条件を $SI(V_{res}) < Cost_{req}$ とした．

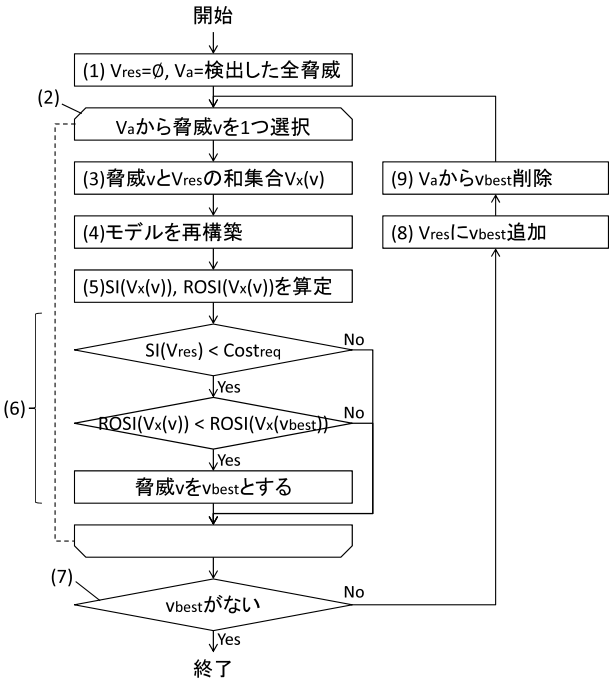

図 4 対処の最適な選定方式の概要
Fig. 4 Overview of the optimal selection method.

最適化は，以下アルゴリズムで実施される（図 4）．

(1) 未対処の脅威の集合 V_a を検出した脅威すべてとし，対処予定の脅威の集合 V_{res} を $\emptyset$ とする．

(2) 未対処の脅威の集合 V_a 内の脅威 v すべてに対して，工程 (3)〜(5) を繰り返す．

(3) 脅威 v と V_{res} との和集合を $V_x(v)$ する．

(4) V_{res} の脅威を対処済と仮定して，システムリスク評価モデルとセキュリティ投資対効果モデルを再構築する．

(5) $SI(V_x(v))$ と $ROSI(V_x(v))$ を算定する．

(6) 脅威 v が制約条件である $SI(V_x(v)) < Cost_{req}$ を満たし，かつ $ROSI(V_x(v)) < ROSI(V_x(v_{best}))$ となる場合，脅威 v を目的関数 $ROSI$ が最良となる v_{best} とする．

(7) 脅威 v_{best} が存在しない場合は，処理を終了する．存在する場合は，工程 (8)，(9) を経て，工程 (2) に戻る．

(8) 対処予定の脅威の集合 V_{res} に脅威 v_{best} を追加する．

(9) 未対処の脅威の集合 V_a から脅威 v_{best} を削除する．

4. 実装と評価

本研究では，図 1 に示すような脅威の検知から，システムリスク評価，投資対効果算定，最適対処選定，Web 画面による合意形成支援までを実装したプロトタイプを開発した．そして，実際に脆弱性公開情報を利用して実験することで，前記提案方式が日々のセキュリティ運用の中でも実用に耐えうるか，評価を行った．

4.1 プロトタイプの仕様

本実験で利用する機器およびソフトウェアの仕様を**表 3** に示す．

4.2 評価対象システムの概要

評価対象としては，典型的な電子商取引を行う EC サイトシステムを構築し，評価を行っている．**図 5** のようなネットワークトポロジを持つシステムであり，外部から直接つながるフロントエンドには，フロント WEB サーバや認証サーバなどを持ち，バックエンドには顧客 DB や決済サーバなどを持つシステムである．

このシステムに対し，我々が開発してきたシステムリスク評価方式 [7] で評価した場合，**表 4** のような評価結果が得られた．このシステムは計 36 個の脅威を内包しており，そこから想定される侵入経路が 2,952 通り存在し，うち 608 通りが危険度の高い経路であった．なお，今回検出対象とした脅威は，NVD（National Vulnerability Database）[1] で情報が公開されている脆弱性 79,959 件である．

表 3 プロトタイプ仕様
Table 3 Specification of the prototype system.

項目	値
OS	CentOS 6.4 64 bit（仮想マシン）
CPU	Intel(R) Xeon(R) CPU X7560 @2.27 GHz [*3]
メモリ	4 GB
ベイジアンネットワーク	Weka 3 [20] [*4]
描画ライブラリ関係	vis.js [*5]，Font Awesome [*6]

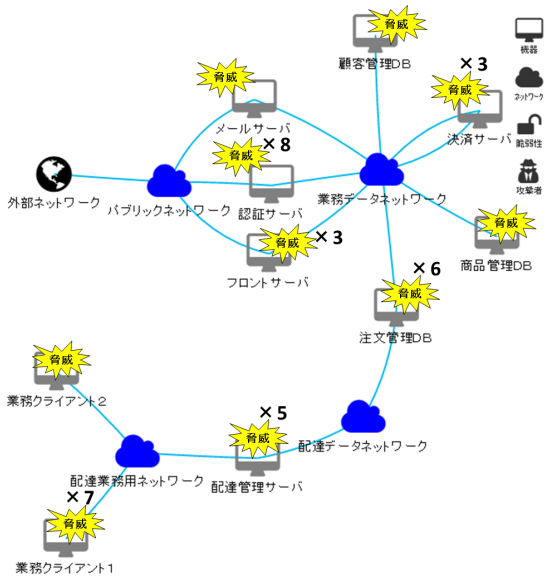

図 5 脅威の検知結果
Fig. 5 Result of threats detection.

[*3] Intel および Xeon は，Intel Corporation の登録商標です．
[*4] Weka は，Waikato 大学の著作物です．
[*5] vis.js は，Almende B.V. の著作物です．
[*6] Font Awesome は Dave Gandy の著作物です．

4.3 ビジネスリスク評価機能の評価

4.2 節の評価対象システムに対してシステムでビジネスリスクを評価した結果，**表 5** と**表 6** の結果を得た．表 5 のように，提案手法では，5 つの脅威の対処候補を選定している．この対処候補は，フロントの機器から優先するなどの経験則に基づいた人手で評価結果と一致したが，必ず一致するわけではなく，妥当性を高める取り組みが必要となる．また，同対処を実施することで，表 6 のように各機器のリスク値を削減することができる．

また，上記における想定被害額 $\sum_v BR(v)$ の算定結果を**図 6** に示す．3.3 節で述べたように，想定被害額の値は時間関数となっており，対処のタイミングで，想定被害額が削減できていることが確認できる．

さらに，本プロトタイプでは，**図 7** のように BIA で分析したビジネスプロセスと残存脅威との対応付けを可視化する．今回の対処で残存する脅威が，どの業務に影響を及

表 4 システムリスク評価結果
Table 4 Result of system risk assessment.

項目		値	[単位]
機器数		10	[台]
脅威検出数		36	[個]
内	脅威大	15	[個]
	脅威中	7	[個]
	脅威小	12	[個]
侵入経路検出数		2.952	[通り]
内	脅威大	608	[通り]
	脅威小	2,344	[通り]

表 5 対策候補の脅威
Table 5 Threat of countermeasure candidate.

脅威	対象機器
CVE-2016-3699	フロントサーバ
CVE-2016-5195	フロントサーバ
CVE-2016-3699	決済サーバ
CVE-2016-7212	認証サーバ
CVE-2016-1522	注文管理 DB

表 6 各機器のシステムリスク値
Table 6 System risk of devices.

機器	対策前	対策後
フロントサーバ	7.5	3.2
メールサーバ	3.1	3.1
商品管理 DB	3.0	0.8
業務クライアント 1	4.9	1.2
業務クライアント 2	0.9	0.3
決済サーバ	7.3	2.0
注文管理 DB	7.7	0.3
認証サーバ	8.0	2.7
配達管理サーバ	6.2	1.7
顧客管理 DB	3.0	0.8

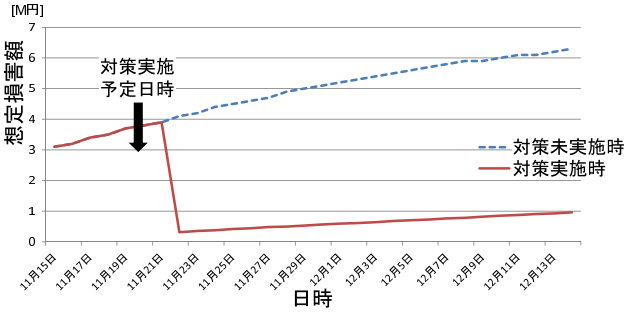

図 6 想定被害額

Fig. 6 Estimated loss amount.

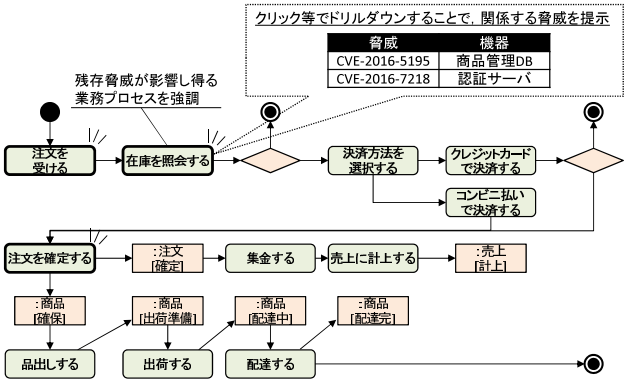

図 7 ビジネスプロセスと残存脅威の関係

Fig. 7 Relationship between business processes and remaining threats.

ぼすか知ることで，対処の見直しや次回の追加投資などの意思決定の判断材料とする．

本プロトタイプでは，以上の結果をレポートとしてまとめ，経営者に提出する．従来は，このレポート作成作業を人手で行うため，我々が社内で評価した事例では調査からレポート提出までに 70 時間ほどがかかっていた．この時間が許容できない脅威の場合，現場だけで意思決定することも多かった．しかし，今回の提案システムでは，1.5 時間ほどで経営者までのレポートが提出可能となり，経営者が意思決定に参画できる機会が増え，経営者が現状をつねに把握しておくことが可能になった．

4.4 性能評価

本技術を日々のセキュリティ運用で活用するには，日々の運用で利用可能な時間内で評価できる必要がある．近年の調査報告では，脅威の情報が公開された翌日から攻撃が開始される事例 [3] が見つかっており，これらに対処するためには，翌日までに対処までを完了させなければならない．実際の対処にかかる時間を考慮すると，遅くとも時間オーダで評価が完了する必要があり，1 時間で評価できることが 1 つの性能要件となる．そこで，提案方式により，この性能要件が達成可能か，典型的なシステム例を用いて評価を行った．この評価では，4.2 節で記載した脅威および侵入経路 1 つ 1 つに対処を行った場合を想定して再計算を繰り返し，最適な対処の組合せを検討していくこととなる．

表 7 総当たり法との比較

Table 7 Comparison with the brute force method.

手法	時間 [s]	試行回数 [回]
総当たり法	206,000	376,992
提案手法	93.0	170
要件	< 3,600	

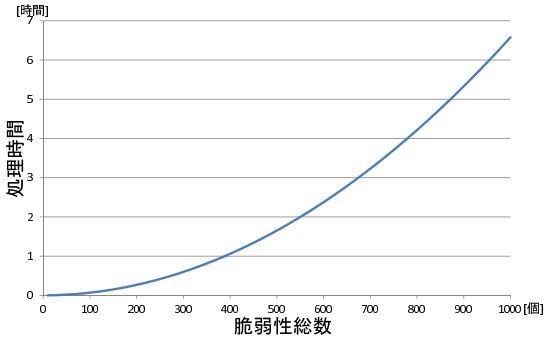

図 8 脅威の数に応じた処理時間

Fig. 8 Processing time for each threat number.

上記状況下で，ビジネスリスク評価を評価した結果，投資対効果の算定と最適な対処の選定に**表 7** のような処理時間を要した．なお，本結果はすべてサーバサイドの処理でかかった時間であり，画面上への描画時間などは含まれていない．表 7 から分かるように，提案手法は総当たり法と比べて，2 千分の 1 程度まで計算コストを削減し，性能要件として定めた 1 時間（3,600 秒）の目標を達成できている．また，同様の方法で，脆弱性総数を変えて評価実験を行い，脆弱性総数と処理時間の関係を表す近似曲線を**図 8** に示す．図 8 の結果から，提案手法では，1 時間で 200 個程度の脅威を持つシステムを評価することができることが分かる．1 機器が 0 個～数個の脅威を持つ可能性があることを考えると，要件とする 1 時間で 100 台程度の機器で構成されるシステムの評価が可能と考えられる．

5. 考察

上記評価実験により，提案方式が脅威の特定から，システムレベルでのリスク評価，経営層の経営判断に資するセキュリティ投資対効果の算定までの自動化を可能することを確認した．また，上記評価の中で以下 4 点の知見を得た．

(1) 提案方式を利用すれば，公共システムや金融システムなど，システムを安易に止めることができず，対処を実施するうえで経営判断が必要となるような重要システムの迅速な対処が可能になる．システムに内在する脅威の情報から分析して，経営層の判断に資する情報を導くような評価を人手で行えるようなセキュリティ人材は限られ，そういった人材を有さない機関では，経営層がリーダシップを発揮できない．この問題は，経産省が公開したガイドライン [21] でも指摘されてお

り，今後企業がIT活用を進めていくうえで，避けては通れない．本技術は，システムに内在する脅威の情報から経営観点のセキュリティ投資対効果を算定する評価を機械化しており，上記のような機関の経営層がセキュリティ運用へ参画する一助となると考える．

(2) 本技術は，最適化問題を解くアルゴリズムにより，セキュリティ投資効果の高速な算定を可能にしている．1時間以内で評価を行うという性能要件に対して，提案方式により，100台程度の機器で構成されるシステムであれば，評価が可能になるとの見込みを得た．本評価は，表3に示すようなサーバ1台で評価を行っているため，より大規模なシステムであっても，スケールアップやスケールアウトで対応できると考える．ただし，今回は局所最適解を求めているため，必ずしも最良の解を求められるわけではない．今後は，より最適化のアルゴリズムを改良し，現実的な時間内でより大域的最適解，あるいはそれにより近い解を求める方法を検討していくつもりである．

(3) 本技術では，投資対効果 $ROSI$ を策定するうえで，いくつかのパラメータを要する．データの価値 GA のように，ベライゾンの1レコードあたりの平均損害額の調査結果 [18] や過去の個人情報漏洩の損害賠償事例など，統計情報を参考にできるものもあるが，大半のパラメータは各組織に依存するものであり，ステークホルダなども含めた協議によって繰り返し調整していく必要がある．この調整は，リスク評価のモデルの妥当性を高めるために必要な工程であり，妥当性確認のプロセスとして一般的なリスク評価でも実施され，調整によるモデルの妥当性の高さはリスク評価の頻度や一律性によって決まる．本技術では，機械的な評価を実現することで，人手での評価のような評価のバラつきがなく，迅速に評価できるため，日々の運用の中でモデルの妥当性を高めやすいと考えている．

(4) 提案手法では，3.3節で記載したように脅威を分類せず，モデルを策定しているが，脅威の種別や脅威にさらされる情報の種別に基づき，より精緻なモデルへの拡張が必要と考える．たとえば，公開されるソフトウェア脆弱性情報では，各脆弱性による機密性・完全性・可用性への影響が定量的に評価されており，これらに基づいて脅威 v ごとに情報毀損被害額 $LD(v)$ や機会損失 $OL(v, case)$ の有無や大きさを評価してもよいと考えられる．また，今回の提案手法は，ITシステムを対象としており，情報セキュリティの範囲で評価を行っているが，IoT化が進む昨今では，実世界に作用するモノがITシステムにつながるため，機器への物理的な影響や，反対に人の身体への物理的な影響などが重要になってきており，今後は，安全性や環境への影響も考慮したモデルへの拡張が必要と考えている．

6. まとめ

近年，特定の企業を狙った標的型攻撃が増加しており，ビジネスを支えるシステムに内在する脅威を発見した場合，ビジネスへの影響を考慮した組織的な判断が求められる．しかし，専門家ではない経営層にとってセキュリティ脅威がもたらすリスクの理解が容易ではないため，対処期間の業務停止による損害の懸念から対処が遅れ，結果的に重大事故を招く場合も少なくない．そこで，本研究では，システム内の脅威がもたらすリスクからセキュリティ投資対効果を算定する技術を開発した．

本技術では，事前にBIAによりシステムを構成する機器からビジネスプロセスまでの関係を記述することで，日々の運用の中で検知される脅威への対処のセキュリティ投資対効果を算定することができる．また，最適化アルゴリズムにより複数の脅威に対して投資対効果が最適になるような投資計画を策定できる．

そして，上記提案方式を実装したプロトタイプを開発し，評価することで，経営層と情報部門の迅速な合意形成を支援する機能を有していることを確認し，提案方式が日々のセキュリティ運用の中でも実用に耐えうることを確認した．

以上により，本技術は，経営層の適切な判断を促して経営層と情報部門の迅速な連携を可能にし，対処に経営判断が必要となるような重要インフラシステムなどの迅速な対処に資すると考える．

ただし，提案手法で用いるパラメータは評価を行う各組織に依存するものであるため，今後は，ステークホルダと協議し，より適正なパラメータの検証を進めていく予定である．

謝辞 本研究の評価にご協力いただいた皆様方に，謹んで感謝いたします．

参考文献

[1] NIST: National Vulnerability Database (NVD) CVE Statistics, NIST (online), available from ⟨https://web.nvd.nist.gov/view/vuln/statistics-results⟩ (accessed 2017-01-30).

[2] 日本IBM：2015年下半期Tokyo SOC情報分析レポート，技術報告，日本IBM (2016).

[3] LAC Co., Ltd.: Apache Struts2の脆弱性（S2-016）を悪用した攻撃の急増について，LAC Co., Ltd.（オンライン），入手先 ⟨http://www.lac.co.jp/security/alert/2013/07/18_alert_01.html⟩（参照 2015-11-05）.

[4] Swanson, M., Bowen, P., Phillips, A.W., Gallup, D. and Lynes, D.: Contingency Planning Guide for Federal Information System, Technical report (2010).

[5] 杉本暁彦，磯部義明：動的モデリングに基づいたリスク評価システム，コンピュータセキュリティシンポジウム2014論文集，Vol.2014, No.2, pp.100–107 (2014).

[6] 磯部義明，杉本暁彦：ベイジアンネットワークを利用した動的モデリングによるセキュリティリスク評価システムの開発，情報処理学会研究報告コンピュータセキュリティ（CSEC），Vol.2015, No.6, pp.1–6 (2015).

[7] 杉本暁彦，磯部義明，仲小路博史：サイバー攻撃の侵入経路を考慮したセキュリティリスク評価技術，情報処理学会論文誌，Vol.57, No.9, pp.2077–2087 (2016).
[8] 磯部義明，杉本暁彦，仲小路博史：サイバーセキュリティ脅威対策のためのビジネスリスク評価システムの提案，電子情報通信学会技術研究報告，Vol.116, No.131, pp.83–90 (2016).
[9] CVSS-SIG: A Complete Guide to the Common Vulnerability Scoring System Version 2.0, Technical report, FIRST (2007).
[10] Gordon, L.A. and Loeb, M.P.: The Economics of Information Security Investment, *ACM Trans. Inf. Syst. Secur.*, Vol.5, No.4, pp.438–457 (2002).
[11] Matsuura, K.: Productivity Space of Information Security in an Extension of the Gordon-Loeb's Investment Model, *Managing Information Risk and the Economics of Security*, pp.99–119 (2009).
[12] 上野景真，田中秀幸：企業の情報セキュリティ投資に対する市場評価の実証研究（大会報告論文：市場主義と社会システムの再設計），社会・経済システム学会大会報告論文，pp.33–39 (2007).
[13] Institute for Computer Sciences and Technology National Bureau of Standards: Guidelines for Automatic Data Processing Risk Analysis, *FIPS PUB 65* (1975).
[14] 西垣正勝，臼井佑真，山本 匠，間形文彦，勅使河原可海，佐々木良一：賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価，情報処理学会論文誌，Vol.52, pp.1173–1184 (2011).
[15] 佐々木良一，石井真之，日高 悠，矢島敬士，吉浦 裕，村山優子：多重リスクコミュニケータの開発構想と試適用，情報処理学会論文誌，Vol.46, pp.2120–2128 (2005).
[16] Pearl, J.: Bayesian Networks: A Model of Self-Activated Memory for Evidential Reasoning, *Cognitive Science Society*, pp.329–334 (1985).
[17] IPA：共通脆弱性評価システム CVSS 概説，IPA（オンライン），入手先 ⟨https://www.ipa.go.jp/security/vuln/CVSS.html⟩（参照 2016-03-28）.
[18] Verizon: 2015 Data Breach Investigations Report (DBIR), Technical report, Verizon (2016).
[19] ALBERT Inc.：最適化問題とは，ALBERT Inc.（オンライン），入手先 ⟨http://www.albert2005.co.jp/technology/machine_learning/OPTproblem.html⟩（参照 2017-02-03）.
[20] Machine Learning Group at the University of Waikato: Weka 3 – Data Mining with Open Source Machine Learning Software in Java, the University of Waikato (online), available from ⟨http://www.cs.waikato.ac.nz/ml/weka/⟩ (accessed 2015-11-11).
[21] 経済産業省，IPA：サイバーセキュリティ経営ガイドライン Ver 1.0，技術報告 (2015).

杉本 暁彦

2011 年東京大学大学院知能機械学専攻修士課程修了．同年（株）日立製作所入社．横浜研究所配属．以来，公共システム，情報セキュリティの研究開発に従事．現在，同社研究開発グループシステムイノベーションセンタセキュリティ研究部研究員．電子情報通信学会員．

磯部 義明

1993 年豊橋技術科学大学大学院知識情報工学専攻修士課程修了．同年（株）日立製作所入社．システム開発研究所配属．以来，医用画像処理，医用情報システム，指紋画像処理，生体認証システム，情報セキュリティの研究開発に従事．現在，同社研究開発グループシステムイノベーションセンタセキュリティ研究部主任研究員．電子情報通信学会会員．

仲小路 博史 （正会員）

2001 年東京理科大学大学院理工学研究科情報科学専攻修士課程修了．同年（株）日立製作所入社．システム開発研究所配属．以来，サイバー攻撃対策技術の研究開発に従事．現在，同社研究開発グループシステムイノベーションセンタセキュリティ研究部主任研究員．明治大学大学院先端数理科学研究科現象数理学専攻博士後期課程在籍．