情報処理学会論文誌 Vol.54 No.1 309–317 (Jan. 2013)

プロジェクトの特性を考慮した最適なセキュリティ対策選定手法

呉 洋[1,a)] 小崎 真寛[1] 岡田 謙一[1,2]

受付日 2012年4月20日, 採録日 2012年10月10日

概要：企業がセキュリティインシデントより受ける損害は深刻化しており，セキュリティとコストの間のトレードオフを考慮した適切なセキュリティ対策選定が求められている．本論文は，数あるセキュリティ対策候補の中からどの組合せが最も客観的合理性を持つものかを判断するための手法を提案する．その際，既存手法では扱われることのなかった要員数や開発期間，あるいは仕事の繁閑といった「プロジェクト」の特性を考慮する．そして，プロジェクトの特性に応じてとるべき対策を変化させることで，企業視点での期待支出の総和を減少させることが本論文の目的である．また，本研究ではケーススタディを行い本提案手法の有用性を示すとともに本手法が特に有効な状況を確認する．

キーワード：情報セキュリティ投資，セキュリティ対策選定，リスク分析，プロジェクト管理，脅威

A Selection Method of Security Measure Considering Project Characteristics

Hiroshi Kure[1,a)] Masahiro Kozaki[1] Ken-ichi Okada[1,2]

Received: April 20, 2012, Accepted: October 10, 2012

Abstract: Recently, the increasing damage caused by information leakage has become a growing public concern, and an effective security countermeasures selection technique is necessary for companies. In this paper, we propose a method for security countermeasure optimization considering each project form. A number of personnel, development, or business hours differ depending on project form and security measures selection is also different. On the basis of these characteristics of the project form, the proposed method gives decrease in total expenditure of a company's security countermeasures selection. Finally, we conducted a case study to evaluate the effectiveness of the proposed method and confirm the situation where the proposed method is more valid.

Keywords: information security investment, security measure selection, risk analysis, project management, threat

1. はじめに

セキュリティインシデントによる損害は深刻な社会問題である．情報の電子化は個人が扱うデータ量を爆発的に増加させ，同時に企業のデータ損失リスクを拡大させた．原因を探ると管理ミス・誤操作・紛失・置き忘れによる個人情報漏洩インシデントが全体の漏洩原因の約8割を占めるなど，その要因にはヒューマンエラーが密接に関わっている [1]．このような現状に対し企業側もセキュリティ対策に力を入れているが，一般に情報セキュリティは企業経営にとって重荷であり「セキュリティへの過大投資」や「セキュリティ対策疲れ」が発生している [2], [3]．

この原因の1つはセキュリティ対策の費用対効果が見えにくいことである [4]．セキュリティ担当者や経営者にとってどの程度コスト負担をすればいいのか分からない，あるいはどのような対策を打ち出せばいいのかの判別が難し

[1] 慶應義塾大学大学院理工学研究科
Graduate School of Science and Technology, Keio University, Yokohama, Kanagawa 223–8521, Japan
[2] 独立行政法人科学技術振興機構 CREST
Japan Science and Technology Agency, Chiyoda, Tokyo 102–0076, Japan
[a)] kure@mos.ics.keio.ac.jp

© 2013 Information Processing Society of Japan

いという現状は，必要以上に安全を求める「過剰セキュリティ」の蔓延を引き起こしている．この種の問題を解決するには情報セキュリティ分野に限った技術的議論は必ずしも有効とはいえない．そこで情報技術そのものにフォーカスするのではなく，情報セキュリティに経済学・心理学・社会学・金融工学などを含んだ幅広い行動科学の知見を導入する研究が注目されつつある [5]．セキュリティとは本来，本質的に「経済的問題」である．100%の情報セキュリティを実現する手法は簡単で，それは情報機器を全面的に使用禁止にすれは済む．しかしながら，それは現実的な解決策ではない．問題はリスクをゼロにすることではなく，許容可能なリスクによる損害額と対策にかかるコストの間の「トレードオフ」を考える必要がある．

本論文は，数あるセキュリティ対策候補の中からどの組合せが最も客観的合理性のあるものかを判断するための手法を提案する．その際，既存手法では扱われることのなかった「プロジェクト」単位において動的に対策を変更させることで，より現実的なケースにも対応できるようにする．プロジェクトによって要員数や開発期間，あるいは仕事の繁閑といったものは異なり，当然とるべき対策案の組合せも異なる．このようにプロジェクトの特性に応じてとるべき対策を変化させることで，企業視点での期待支出の総和を減少させることが本論文の目的である．以降，本論文は以下のように構成される．まず 2 章で関連研究を述べ，3 章ではプロジェクトの特性を考慮した最適なセキュリティ対策選定手法を提案する．4 章でその有効性をシミュレーションによる評価で確認し，最後に 5 章を本論文の結びとする．

2. 関連研究

費用対効果の見えにくい情報セキュリティへの投資は，長年セキュリティ担当者や経営者の勘と経験によって決められてきた．しかし最近の研究によれば，金融工学の知見を応用することで情報セキュリティへの投資額に対してある程度理論的な値を提示できるようになった．特に文献 [6] がセキュリティ最適投資理論のランドマークとして発表されて以来，情報セキュリティに金融工学を応用した研究が 1 つの分野として体系的に統一され始めた．同文献の中で，Gordon らは ENBIS と呼ぶ数式モデルを用いることで最適投資額を求める手法を提唱している．さらには，リアルオプションによる金融工学の考え方を導入したセキュリティ投資の最適時期に関する文献 [7] や，金融派生商品の体系的なモデルと価格評価理論（確率微積分学）に関する文献 [8] がある．また，田中らは文献 [9], [10] においてネットワークの脆弱性とセキュリティ投資に関する分析，効果的なセキュリティ投資に関する分析，セキュリティ投資と企業価値に関する分析を詳細な実証データより検証している．

また，企業が直面する情報リスクとその対策の組合せに関するセキュリティ対策選定手法最適化の研究としては，以下のようなものがある．中村らは，文献 [11] において資産・脅威・対策の組合せを「資産と脅威の関係」と「脅威と対策の関係」に分けて数式モデル化し考察している．西垣らは，文献 [12] において直接的なセキュリティ損害だけでなく，事後の訴訟リスクも勘案した対策選定手法を提案している．加藤らは，文献 [13] において管理者の求めるセキュリティレベルとユーザの求める利便性を考慮し，管理者とユーザの両者が満足する選定案を交渉によって見出す手法を提唱している．しかしながら，これらの関連研究ではセキュリティ対策を施行する対象があくまで就業者 1 人に限定されている，対策の施工期間が考慮されていないなど，より実際的なプロジェクト単位での要員数，繁閑期，開発期間を考慮したセキュリティ対策の選定手法に関する研究はほとんど行われていないのが現状である．

3. プロジェクトの特性を考慮した最適なセキュリティ対策選定手法

通常，企業では，内部統制の仕組みとして SOX 法（金融商品取引法）などをもとに，情報システムの活用に対して単一の情報セキュリティポリシを設けていることが多い [14]．しかしながら，単一の情報セキュリティポリシによって選定されたセキュリティ対策リスト（USB メモリの使用禁止，機密ファイルのメールでのやりとり禁止など）を企業全体にあてはめることは，セキュリティとコストの間にあるトレードオフの問題を適切に解決できない可能性がある．本提案手法は，企業などにおける各々のプロジェクトの要員数，繁閑期，開発期間といった特性を考慮し，数式モデルを用いてコストと効果のバランスを定量的に測りながら企業がとるべきセキュリティ対策選定の最適化を行うことを目的としている．

これにより，たとえば仕事の繁閑に応じて就業者の仕事時間が多い繁忙期には想定しうる必要最小限のセキュリティ対策で生産性を重視し，多少仕事速度が遅くなってもかまわない閑散期にはセキュリティを強化し損失防止に努めるといった柔軟な対策の選定が可能となる．このようなプロジェクトの特性に応じてセキュリティを変化させる動的対策の考え方は，それによって理論上の計算で対策をつねに固定する静的対策を用いた場合よりも企業の期待支出の総和を減少させることを目指している．

静的対策とは，一般の企業で行われているつねに固定されたセキュリティ対策選定リストに基づいて行うセキュリティ対策のことである．動的対策とは，本研究においては，要員数や開発期間，仕事の繁閑といった企業の個々のプロジェクトの特性に合わせて動的にセキュリティ対策選定リストを変更し，それに基づいて行うセキュリティ対策のことである．そして，企業では自らの持つ情報を管理し機密を守るためのセキュリティが重要であり，そのために セキュリティを脅かすリスク（脅威）に対して，包括的な

© 2013 Information Processing Society of Japan

枠組みとしてのリスク対策（セキュリティ対策）が必要となる．したがって，本提案手法は次のような流れになる．

1. リスク分析
2. リスク対策分析
3. リスク対策最適化

ここで，リスク分析は発生しうるリスクの発生確率と損害額を後述する FTA 法によって分析するフェーズである．リスク対策分析はリスクに対して想定される対策手法や付随するコストを本提案で構築する数式モデルより洗い出すフェーズである．最後に，リスク対策最適化は得られたリスクと対策より期待損害額が最小となるような組合せをこちらも本提案で構築する数式モデルより算出するフェーズである．

3.1 リスク分析

本提案手法において実行されるリスク分析の対象は，企業における就業者とし，フォールトツリー法（Fault-Tree Analysis，FTA 法）によるリスク分析を行う [15]．本提案におけるリスク分析でフォールトツリー法を用いる理由は，リスクを引き起こす潜在的な根本原因を全体として漏れや抜けなく論理的に抽出するためである．そうすることで，就業者に対して起こりうるセキュリティインシデントを列挙し，それによる推定被害額を設定する．具体的な分析手順は以下であり，それぞれ詳説する．

3.1.1 脅威の列挙と被害額の推定

ここでは，就業者へ起こりうる脅威（セキュリティインシデント）をあげ，それによる推定被害額を決定する．脅威は，想定しうるものを被りなくあげる必要がある．また，漏れをなくすために「情報漏洩」「盗聴被害」などの大きな分類が望ましいが，分類の範囲を大きくしすぎると逆に発生確率や損害額の推定が難しくなる．たとえば，ある就業者 1 名が 1 年間で「情報漏洩」を起こす確率と損害額を想定することはもとの情報漏洩が何を指すのか曖昧であるため，その設定値にはなかなか説得力を持たせることができない．そこで原因別や経路別にもう一段深く分類し，そこから FTA 法を用いることでさらに詳細なリスク分析を行う．

3.1.2 フォールトツリー法（FTA 法）による分析

FTA 法による分析では，まず初めに望ましくない事象を定義する．これを頂上事象としてフォールトツリーの頂上に配置し，その発生のもととなる事象を AND もしくは OR のゲートを用いて分解していく．分解はそれ以上分解が困難である本質的に発生確率が同等と推定される基本事象まで行う．その結果，頂上事象の発生はすべて基本事象の和と積で表すことができ，基本事象に発生確率を与えることで頂上事象の発生確率の計算ができるようになる．

3.1.3 各基本事象に対する発生確率の設定

図 1 は「情報漏洩」を頂上事象とした場合の FTA 法による分析結果の例である．脅威自体に発生確率をあてはめることは困難であるが，基本事象ならば発生確率を推定することが可能となる．なお，基本事象の発生確率は類似事象の統計や過去に実施されたリスク分析などより値を推定して議論を行う．これは，推定値であっても各脅威に対するオーダ的なリスクの評価が可能なためである [16]．

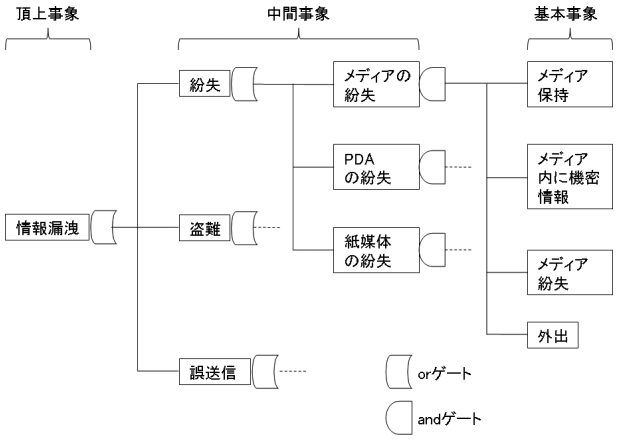

図 1 情報漏洩の分析例
Fig. 1 An example of an analysis on information leakage.

3.1.4 ミニマルカットセット計算による脅威の発生確率の算出

ここでは，設定した各基本事象の発生確率より，頂上事象である脅威の発生確率算出を行う．リスクが発生する基本事象の組合せをカット，すべてのカットの集まりをカットセットと呼ぶ [15]．さらに，カットセットに含まれる冗長な基本事象を除き，どの基本事象がカットセット内からなくなっても頂上事象が発生しなくなるような組合せをミニマルカットセットと呼ぶ．つまり，リスクが発生にいたるまでの最小なイベントの組合せである．カットセットからミニマルカットセットを求める際には次の 2 つの法則を導入する．

- 吸収則：$(\{ab\}, \{a\}) \rightarrow \{a\}$
- べき乗則：$\{aa\} \rightarrow \{a\}$

今，あるリスクのミニマルカットセットが (a)，(a, b)，(c, d, e) であり，それぞれの基本事象の発生確率を P_a，P_b，P_c，P_d，P_e とすると，ある就業者が直面しているリスク全体の発生確率 P_t（就業者 1 人・1 日あたり）は以下のようになる．

$$P_t = 1 - (1 - Pa)(1 - P_a P_b)(1 - P_c P_d P_e) \qquad (1)$$

3.2 リスク対策分析

FTA 法によるリスク分析終了後，今度はそれぞれのリスクに対し脅威を抑えるためのリスク対策を考える必要がある．ここでは以下にあげる数式モデルより各対策候補のコストと効果を設定し，リスクの低減，受容，回避のどの対策をとるかを決定する．

3.2.1 リスク対策による効果とコストの設定

リスク対策は対策を採用すればするほど良いというもの

© 2013 Information Processing Society of Japan

ではなく，そこには対策を採用することによるプラス面とマイナス面が存在するため，そのトレードオフを考えて選定を行わなければならない．つまり，プラス面がマイナス面より大きければ対策採用となり，逆にマイナス面の方が大きければ対策不採用となる．

対策採用によるプラス面は，当然リスクの低減効果である．低減効果とは，洗い出した各々のリスクに対して各対策がどれだけ発生確率を低減させるかの値であり，ここでその設定を行う．たとえば，ある基本事象に対策を施した際のリスク低減効果 E は，対策前の発生確率 P_1，対策後の発生確率 P_2 とすると以下のように算出される．

$$E = 1 - \frac{P_2}{P_1} \tag{2}$$

たとえばあるリスク（損害額 b 円，発生確率 α）があり，ある対策を行ったとする．対策のリスク低減効果を E とすると，対策採用によるリスク金額 A は次式となる．

$$A = b \times \alpha \times E \tag{3}$$

また，対策採用によるマイナス面は，生産性低下によるコストである．生産性低下とは就業者 1 人あたりの仕事速度が低下し，仕事時間が増えることを指す値であり，ここでその設定を行う．たとえば電子メール経由での漏洩が大きなリスクを持つ場合，全社的に電子メールの使用を禁止するリスク対策が考えられる．それにより電子メールによる情報漏洩は確実に防ぐことが可能であるが，メール以外の代替手段を使わなければならなくなったことで普段以上の仕事時間がかかってしまう可能性がある．したがって，就業者 1 人 1 日あたり通常 T_1 時間で終わる仕事がある対策を実施した際に T_2 時間かかるとすると，その際の生産性低下度 D は以下のとおりとなる．

$$D = \frac{T_2}{T_1} - 1 \tag{4}$$

たとえばあるプロジェクト（就業者 1 名 1 時間あたりの残業コスト c 円，要員数 M 人）があり，ある対策を行ったとする．仕事時間を W，対策による生産性低下度を D とすると，対策採用による生産性低下コスト（総残業コスト）C は次式となる．

$$C = W \times D \times c \times M \tag{5}$$

3.2.2 3 つのリスク対策

本提案では，リスク対策としてリスクの低減，受容，回避の 3 つを考える．一般的には，これら 3 つのリスク対策とは別に転嫁（対価を払ってリスクを第三者に移す，保険など）が用いられる場合もあるが，本研究では転嫁を，対価（金銭的コスト）によりリスクを外部へ移すことで，そのリスクを回避（本研究において本来は金銭的コストはない）するものとして，考慮に含めなかった．

リスク低減対策とは管理対策を適用し，情報資産に対する脅威や脆弱性に対してリスク値を一定幅だけ下げる方策である．たとえばメールの使用を全面的に禁止するのではなく，「機密情報を添付ファイルとしたメール送信を禁止」すればメール経由での情報漏洩をある程度抑えることが可能となる．一定幅のリスクを低減させるため，前述の低減効果は $0 < E < 1$ の幅をとる．

リスク受容対策とは，対象のリスクの発生確率および損害額が小さくリスク対策を行うことが合理的でない場合，そのリスクを受け入れ対策を行わないことをいう．前述の対策採用によるマイナス面がプラス面より大きい場合の対策不採用がリスク受容にあたる．リスクは低減されないため，その低減効果は $E = 0$ である．

リスク回避対策とはコスト上対応が難しい場合や低減，受容が適用できない場合，リスクを回避するためにリスクの発生がともなう業務手段自体をやめることをいう．これによってリスクは回避され，そのリスク低減効果 $E = 1$ であるが，回避対策は多くの場合生産性低下の度合いが大きい．つまり対策採用によるプラス面が非常に大きな場合，いい換えれば非常に大きなリスクに対してのみ有効である．

3.3 リスク対策最適化

本節では，最適化フェーズにおけるリスクとリスク対策の組合せの最適化について考える．一般に，企業におけるプロジェクトは複数の工程に分かれており，各々で仕事時間も異なる．そして脅威による損害額，対策採用による生産性の低下，対策にかかるコストなどを最小化するような組合せを数式モデルとして表す．つまり，次式を満足するような組合せを算出することが目的である．

$$\begin{aligned}\text{期待支出額} \ = \ &\min(\text{損失額} \\ &+ \text{生産性低下コスト} + \text{対策コスト})\end{aligned} \tag{6}$$

損害額

対策選定を考える場合，まず回避対策が有効かどうかを検討する．回避対策が採用された場合，そのリスクはゼロとなるので低減対策を考える必要はない．回避対策が不採用と判断された場合，今度は低減対策が有効かどうかを検討する．低減対策が採用となった場合，そのリスクは採用された低減対策の低減効果の分だけ低減される．低減対策が不採用となった場合，リスク対策は行われずリスクの許容となる．ここで，就業者 1 名が直面しているリスク k の 1 日あたりの発生確率を P_k は以下のように表される．

$$\begin{aligned}P_k \ = \ B_n \times \Bigg(&\prod_l (E_{l,n} \times PF_l) \\ &+ \prod_l \prod_m (E_{m,n} \times CF_m \times (1 - PF_l)) \Bigg)\end{aligned} \tag{7}$$

B_n はリスク k の発生条件を満たすミニマルカットセッ

© 2013 Information Processing Society of Japan

トに含まれる基本事象の発生確率，$E_{l,n}$ は回避対策 l が基本事象 B_n の発生確率に及ぼす低減効果，PF_l はそのフラグである（$PF = 1$ で採用，$PF = 0$ で不採用）．同様に，$E_{m,n}$ は低減対策 m が基本事象 B_n の発生確率に及ぼす低減効果，CF_m はそのフラグである．次に，あるプロジェクトの 1 工程中でのリスク k の発生確率 $J_{i,k}$ は次式で表される．

$$J_{i,k} = 1 - (1 - P_k)^{(M_i \times T_i)} \tag{8}$$

M_i はプロジェクトの要員数，T_i はプロジェクト内の 1 工程の日数である．プロジェクトは全部で 6 つの工程からなると仮定し，それぞれの工程日数は簡単のため同じであるとした．したがってプロジェクトの総開発期間を $Ttotal_i$ とすると，1 工程の期間 T_i は $T_i = Ttotal_i/6$ である．以上をまとめると，プロジェクト全体としての損害額 D_i は，発生しうるリスク k による損害額を $d_{i,k}$ として，以下のように表される．

$$D_i = \sum_k J_{i,k} \times d_{i,k} \tag{9}$$

生産性低下コスト

あるプロジェクトの j 番目の工程を考える．工程 j 中の総残業時間 $Wtotal_{i,j}$ は，その工程の日数を T_i，その工程 1 日あたりの仕事時間 W_i，対策 r による生産性低下度を D_r，対策 r を採用するか否かのフラグを F_r とすると，次式のように表される．

$$Wtotal_{i,j} = T_i \times W_j \times \sum_r D_r \times F_r \tag{10}$$

よって，あるプロジェクトの工程 j における生産性低下コスト $C_{i,j}$ は，就業者 1 名 1 時間あたりの残業コスト（円）を c，要員数を M とすると次のように表される．

$$C_{i,j} = Wtotal_{i,j} \times c \times M \tag{11}$$

対策コスト

対策にかかるコスト Q は，対策 r にかかるコスト C_r とその対策を採用するか否かのフラグ F_r を用いて以下のように表せる．

$$Q = \sum_r C_r \times F_r \tag{12}$$

4. 企業のソフトウェア開発プロジェクトを想定した適用例

セキュリティ対策を選定する際，動的に対策を変更することの有効性を確認するため，企業のソフトウェア開発プロジェクト（以下，プロジェクトとする）を想定した適用例を示し，それに対する評価を行った．なお，本評価ではプロジェクトの特性を考慮した最適なセキュリティ対策選定手法を理論上の計算で評価するため，評価条件やリスク分析における基本事象，発生確率，被害額，対策コストなどは推定値より議論を進めている．

図 2 プロジェクトの各工程
Fig. 2 The process flow of a project.

4.1 評価条件

今回は要員数：5 名，10 名，20 名，30 名，50 名の 5 つ，総開発期間：90 日，120 日，180 日，270 日，360 日，450 日，540 日の 7 つ，の組合せからなる動的対策を行う計 35 のプロジェクトを想定した．比較対象のための静的対策は，ソフトウェア産業の調査報告書 [17] および労働基準法 [18] より，一般の企業が行う標準的なプロジェクト（要員数：20 名，総開発期間：270 日，1 日の仕事時間：8 h）に準拠した対策組合せとした．また，現在様々な企業で用いられている v 字モデル [19] を参考に，1 つのプロジェクトは全 6 工程からなるとした．それぞれの工程は，工程 1 から 6 まで「要件定義」「基本設計」「詳細設計」「実装」「テスト」「保守・運用」に相当するとし，**図 2** のように各工程で就業者 1 名が行う 1 日の仕事時間が異なるとした．

4.2 評価手順

4.2.1 リスク分析

情報セキュリティリスクとして 6 つの一般的な脅威を，文献 [20] を参考に想定した．また，それぞれの脅威をフォールトツリーによって分析し，各基本事象によるミニマルカットセットの和の形で表した．**表 1** には想定した情報セキュリティリスクの一例を示し，**表 2** にはリスクを構成する基本事象の一例を情報の紛失・盗難リスクに関する就業者 1 名・1 日あたりの発生確率と共に示す．最後に，**表 3** には分析したリスクの損害額とそのミニマルカットセットの一例を示す．ここで，基本事象の発生確率は文献 [12] と文献 [20] を参考に，リスクの損害額は文献 [11] と文献 [16] を参考に推定されている（たとえば，文献 [20] より PC 内にデータ保存という基本事象の発生確率を 0.9 としている場合に，表 2 の PC 内に機密情報の発生確率を 0.9 と推定する，文献 [11] より可搬型媒体の電子情報の資産価値を 500 万円としている場合に，表 3 の中間事象である小型デバイスの盗難（USB メモリ）の損害額を 500 万円と推定する，など）．

4.2.2 リスク対策分析

リスク分析終了後，前述した脅威（を構成する基本事象）の発生確率を低下させるための対策候補をあげ，対策の種類，生産性低下度，コスト，各基本事象への低減効果を与えた．**表 4** は実際にリスク対策分析をした一例の抜粋である．結果として総回避対策数が 11，総低減対策数が 24 となった．ここで，各項目の推定値は文献 [11] と文献 [16] を参考にしている（たとえば，文献 [11] より IC カードに

© 2013 Information Processing Society of Japan

表 1 リスク分析の例
Table 1 An example of risk analysis.

頂上事象	中間事象
情報の紛失	小型デバイスの紛失（USB メモリ）
	小型デバイスの紛失（携帯端末）
	紙媒体の紛失
	セキュリティカード・キーの紛失
	PC の紛失
情報の盗難	小型デバイスの盗難（USB メモリ）
	小型デバイスの盗難（携帯端末）
	紙媒体の盗難
	セキュリティカード・キーの盗難
	PC の盗難
誤送信	電子メールの誤送信
	FAX の誤送信
盗み見・盗み聞き	外出時に紙媒体の盗み見
	外出時に PC の盗み見
	外出時に仕事会話の盗み聞き
ワーム・ウイルスへの感染	ワームへの感染
	ウイルスへの感染
その他	データの不適切な破棄による情報漏洩

表 2 リスクを構成する基本事象の例
Table 2 Basic events of the risk.

ID	基本事象	発生確率
B_1	外出	0.2
B_2	USB メモリ保持	0.9
B_3	USB メモリ内に機密情報	0.6
B_4	USB メモリ紛失	0.01
B_5	携帯端末保持	0.9
B_6	携帯端末内に機密情報	0.8
B_7	携帯端末紛失	0.01
B_8	紙媒体への印刷	0.8
B_9	紙媒体への筆記	0.8
B_{10}	紙媒体に機密情報	0.2
…	…	…
B_{15}	PC 内に機密情報	0.9
B_{16}	PC 紛失	0.01
…	…	…

よる入退出管理装置導入による対策コスト 200 万円，生体情報による入退出管理装置の導入による対策コスト 500 万円，文献 [16] よりユーザの識別および認証の実施による対策コスト 100 万円としている場合に，表 4 の指紋認証システムの導入による対策コストの推定値をそれらの間の 200 万円と推定する，など）．

4.2.3 リスク対策分析最適化

先述したリスク対策分析の結果をもとに，計 35 のプロジェクト形態において対策を動的に変化させていき，企業の期待支出額を算出した．期待支出額は式 (6) に示されるように，損失額と生産性低下コストと対策コストの和で表されるものである．また，比較対象のために静的対策の場合（要員数：20 名，総開発期間：270 日，1 日の仕事時間：8 h とした標準的なプロジェクトにおける最適な対策組合せに準拠）についても期待支出額を算出した．

表 3 リスクの損害額とそのミニマルカットセットの例
Table 3 An example of loss and minimal cutset of the risk.

中間事象	損害額（円）	ミニマルカットセット
小型デバイスの紛失（USB メモリ）	300 万	(B_1, B_2, B_3, B_4)
小型デバイスの紛失（携帯端末）	500 万	(B_1, B_5, B_6, B_7)
紙媒体の紛失	300 万	(B_8, B_9, B_{10}, B_{11}, B_{12})
セキュリティカード・キーの紛失	300 万	(B_1, B_{13}, B_{14})
PC の紛失	1000 万	(B_1, B_5, B_6)
小型デバイスの盗難（USB メモリ）	500 万	(B_1, B_2, B_3)
紙媒体の盗難	300 万	(B_1, B_8, B_{10}, B_{12}), (B_1, B_9, B_{10}, B_{12})
セキュリティカード・キーの盗難	500 万	(B_1, B_{13})
PC の盗難	1000 万	(B_1, B_{15})
…	…	…

表 4 リスク対策分析の例
Table 4 An example of counter-risk analysis.

対策内容	対策の種類	生産性低下度	対策コスト	対象事象	低減効果
全ての USB メモリ使用禁止	回避	0.1	0	B_2, B_3, B_4	1.0
全ての携帯端末使用禁止	回避	0.1	0	B_1, B_5, B_6	1.0
全ての紙媒体の使用禁止	回避	0.1	0	B_8, B_9, B_{10}, B_{11}, B_{12}	1.0
指紋認証システムの導入	回避	0	200 万	B_{13}, B_{14}	1.0
PC 持ち出し禁止	回避	0.2	0	B_{14}, B_{16}, B_{17}	1.0
USB メモリ機密情報保存禁止	低減	0	0	B_3	0.05
携帯端末の USB メモリ使用禁止	低減	0.01	0	B_6	0.05
機密情報を含む印刷・筆記禁止	低減	0.01	0	B_8, B_9, B_{10}	0.05
…	…	…	…	…	…

4.3 評価項目

評価項目は，$D_{dynamic}$ を動的対策による期待支出，D_{static} を静的対策による期待支出として，以下の式で表される支出削減率 R を用いた．ここで，R は静的対策に対して動的対策をとった場合にどれだけ支出が削減できたかを表す値であり，これより本提案手法の有用性を評価し，また本提案手法が効果的な条件を明らかにした．

$$R = \frac{D_{static} - D_{dynamic}}{D_{static}} \tag{13}$$

4.4 結果と考察

図 3 は工程 1，**図 4** は工程 6，**図 5** は工程 4 における各々のプロジェクトの削減率（%）を表している．各図において横軸は要員数，縦軸は総開発期間を表しており，図中

© 2013 Information Processing Society of Japan

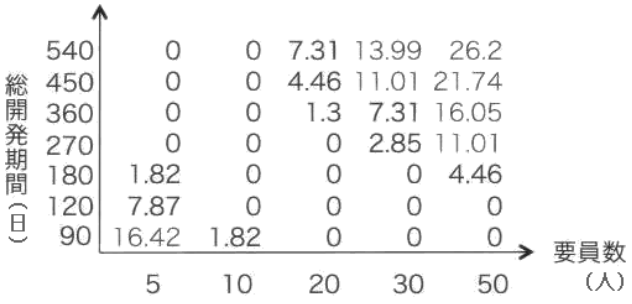

図 3 工程 1 の各プロジェクトの削減率（仕事時間：8 h）
Fig. 3 Rate of expenditure decrease in process flow 1.

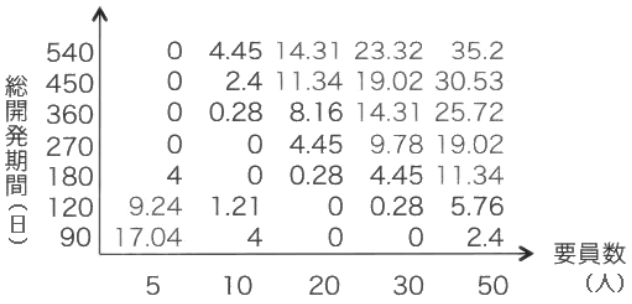

図 4 工程 6 の各プロジェクトの削減率（仕事時間：11 h）
Fig. 4 Rate of expenditure decrease in process flow 6.

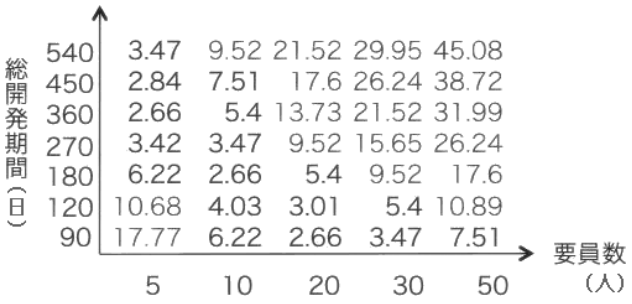

図 5 工程 4 の各プロジェクトの削減率（仕事時間：14 h）
Fig. 5 Rate of expenditure decrease in process flow 4.

の数値は対応するパラメータを持つプロジェクトに静的対策と動的対策を適用した場合の削減率を表している．図において，削減率が大きいということは，対応するパラメータを持つプロジェクトに対して，動的にセキュリティ対策を変更することが有効であることを示している．また，工程 2，3，5 については，静的対策と動的対策の期待支出の差があまりなく，そのため本提案手法の有効なケースを示すにあたっては，図を載せることを割愛した．

まず，図 3，図 4，図 5 と仕事時間が大きくなるにつれ動的対策が有効な領域が増大しており，仕事時間の大きな繁忙期には特に動的対策が有効なケースが多いことを示している．また，図 3，図 4，図 5 を見れば左下の領域（＝小規模プロジェクト）と右上の領域（＝大規模プロジェクト）の削減率が高いことが分かる．今回は一般にプロジェクト単位でセキュリティ対策を動的に変更している例が見られないため，一般の企業が先述した標準プロジェクトを想定してセキュリティ対策を選定していると仮定した．ゆえに標準プロジェクトから離れるほど動的対策の効果が高いと考えられる．つまり，企業の仕事時間が大きくなる繁忙期の場合，あるいは要員数が多くかつ総開発期間が長いプロジェクトや要員数が少なくかつ総開発期間が短いプロジェクトを企業がかかえる場合，対策をつねに固定する静的対策を用いた場合よりも理論上の計算で企業の期待支出の総和が大きく減少することが数式モデルより算出され，本提案手法の有用性が示された．

また，これは標準プロジェクトで最適だと判定された対策選定が，実際のプロジェクトの特性に合わせると必ずしも最適だとは限らないためだと考えられる．例として，ある標準プロジェクトにおいて対策リストが対策 1〜5 まで 5 つあり，判断された対策選定が対策 1〜3 は採用，対策 4〜5 が不採用だったとする．大規模プロジェクトで動的対策を行った場合，標準プロジェクトより要員数も開発期間も大きいため，対策採用による生産性低下（＝残業コスト）の増大は大きくなる．したがってこの大規模プロジェクトにおける最適な対策選定リストは，たとえば対策 1 は採用，対策 2〜5 は不採用といったように，標準プロジェクトを想定して選定した対策選定リストよりも不採用になった対策の数が大きくなる．

同様に，小規模プロジェクトで対策選定を行った場合，標準プロジェクトよりも要員数も開発期間も小さいため，対策選定による生産性低下（＝残業コスト）の増大は小さくなる．したがってこの小規模プロジェクトにおける最適な対策選定リストは，たとえば対策 1〜4 は採用，対策 5 は不採用といったように，標準プロジェクトよりも採用する対策数が大きくなる．結果，標準プロジェクトから離れ対策が多く変更される分，削減率に貢献すると推測できる．

そして本提案手法は，各数値に対してアセスメント誤差を考慮しても実務上受けいれられる頑強さで同様の効果が得られる．たとえば，仕事時間の大きな繁忙期において，要員数および総開発期間のアセスメント誤差を 20%とした場合の感度分析による削減率の振れ幅は，最も大規模なプロジェクトである要員数 50 名，総開発期間 540 日のプロジェクトで −4.51%〜+5.19%，最も小規模なプロジェクトである要員数 5 名，総開発期間 90 日のプロジェクトで −2.79%〜+3.55%，と両方で十分に小さい．したがって，各数値をある程度のアセスメント誤差のある値に変えても，仕事時間が大きくなる繁忙期，そして企業の大規模プロジェクトおよび小規模プロジェクトにおいて本提案手法は大きな削減率を維持すると考えられる．

5. おわりに

セキュリティインシデントによる損害は多くの企業にとって深刻な問題である．近年では企業側のセキュリティ対策も強化されているが，「セキュリティへの過大投資」や「セキュリティ対策疲れ」が企業経営にとっての重荷となっ

© 2013 Information Processing Society of Japan

ている．この種の問題を解決するために，最近では情報セキュリティに経済学・心理学・社会学・金融工学などを含んだ幅広い行動科学の知見を導入する研究が注目されつつある．本論文では，数あるセキュリティ対策候補の中からどの対策の組合せが最も客観的合理性のあるものなのかを判断する手法を提案した．従来研究では対策選定の対象を就業者 1 名に絞り，また現実においてもプロジェクト単位で動的に対策を変更するケースは見受けられない．そこで要員数や開発期間，仕事の繁閑といったプロジェクトの特性に合わせて動的に対策選定を行うことで企業視点での期待支出の総和を減少させることが本論文の目的である．

また，本研究では企業のソフトウェア開発プロジェクトを想定した適用例を示し，静的な対策選定を行った場合と，本提案手法による動的な対策選定を行った場合とでその期待支出の差を削減率として算出した．その結果，提案手法が向いている環境とそうでない環境があることが分かり，仕事時間の大きな繁忙期，そして大規模プロジェクトおよび小規模プロジェクトにおいて大きな削減率が示され，本提案手法の有用性が示された．これからの情報セキュリティは技術的な完成度の高さのみを追求すればよいというものではなく，セキュリティ対策選定手法最適化に関する研究はまだまだ発展の余地や課題も多い．リスクというものは往々にして人の合理的な判断を誤らせるものであり，またセキュリティ対策選定の現状を考えればそれだけこの分野へのニーズは大きいと考えられる．場合によっては経済学や心理学など他の分野との連携を探り，客観的かつ合理的な判断によって「過剰セキュリティ」という幻想から脱却する必要性が求められている．

参考文献

[1] NPO 日本ネットワークセキュリティ協会：2010 年情報セキュリティインシデントに関する調査報告書（個人情報漏えい編），入手先 ⟨http://www.jnsa.org/result/incident/2010.html⟩.

[2] 内閣官房情報セキュリティセンター情報セキュリティ政策会議：セキュアジャパン 2008，入手先 ⟨http://www.nisc.go.jp/active/kihon/pdf/sjf_2008.pdf⟩.

[3] 警察庁生活安全局情報技術犯罪対策課：不正アクセス行為対策等の実態調査平成 20 年，入手先 ⟨http://www.npa.go.jp/cyber/research/h19/H19countermeasures.pdf⟩.

[4] NRI セキュアテクノロジーズ株式会社：企業における情報セキュリティ実態調査 2008，入手先 ⟨http://www.nri-secure.co.jp/news/2008/1127.html⟩.

[5] 独立行政法人情報処理推進機構：セキュリティエコノミクスの挑戦，入手先 ⟨http://www.ipa.go.jp/security/economics/index.html⟩.

[6] Gordon, L.A. and Loeb, M.P.: The Economics of Information Security Investment, *ACM Trans. Information and Security*, Vol.5, No.4, pp.438–457 (2002).

[7] Tatsumi, K. and Goto, M.: Optimal Timing of Information Security Investment: A Real Options Approach, *Economics of Information Security and Privacy*, pp.211–228, Springer (2010).

[8] Matsuura, K.: Security tokens and their derivatives, Technical Report 29, Centre for Communications Systems Research, University of Cambridge (2001).

[9] 田中秀幸，松浦幹太：情報セキュリティ投資の経済的動機付けに関する企業レベルの実証研究，電気通信普及財団研究調査報告書，No.21, pp.17–24 (2006).

[10] 田中秀幸，松浦幹太：情報ネットワーク・システムの脆弱性とセキュリティ投資に関する実証分析，日本経済政策学会第 63 回全国大会，日本経済政策学会 (2006).

[11] 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).

[12] 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, No.3, pp.1173–1184 (2011).

[13] 加藤弘一，勅使河原可海：ネットワーク特別利用時におけるセキュリティと利便性を考慮した最適対策決定手法の提案，情報処理学会論文誌，Vol.49, No.9, pp.3209–3222 (2008).

[14] 鈴木武俊，真田大志：情報セキュリティポリシー運用における課題と対策，*UNISYS TECHNOLOGY REVIEW*, No.98, pp.91–104 (2008).

[15] McCormic, N.J.: *Reliability and Risk Analysis*, Academic Press Inc. (1981).

[16] 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, No.8, pp.2264–2271 (2000).

[17] 経済産業省商務情報政策局：組込みソフトウェア産業実態調査報告書 2008，入手先 ⟨http://www.meti.go.jp/policy/mono_info_service/joho/downloadfiles/2008software_resarch/project_houkokusho.pdf⟩.

[18] 労働基準法第 32 条第 2 項，入手先 ⟨http://law.e-gov.go.jp/htmldata/S22/S22HO049.html⟩.

[19] Coley Consulting: Types of Testing in the V-Model, 入手先 ⟨http://www.coleyconsulting.co.uk/testtype.htm⟩.

[20] 芝口誠仁，稲場太郎，中山佑輝，岡田謙一：仕事量を考慮したセキュリティ対策選定手法，情報処理学会論文誌，Vol.51, No.2, pp.648–657 (2010).

呉 洋 （学生会員）

2012 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科修士課程在学中．ネットワークセキュリティ，デジタルフォレンジックスの研究に従事．

小崎 真寛 （学生会員）

2010 年慶應義塾大学理工学部情報工学科卒業．2012 年同大学大学院理工学研究科修士課程修了．在学中，ネットワークセキュリティ，デジタルフォレンジックスの研究に従事．2012 年ソニー株式会社入社．

© 2013 Information Processing Society of Japan

岡田 謙一 （フェロー）

慶應義塾大学理工学部情報工学科主任教授，工学博士．専門は，CSCW，グループウェア，ヒューマン・コンピュータ・インタラクション．『ヒューマンコンピュータインタラクション』（オーム社），『コラボレーションとコミュニケーション』（共立出版）をはじめ著書多数．情報処理学会誌編集主査，論文誌編集主査，GN 研究会主査，日本 VR 学会理事等を歴任．現在，情報処理学会理事，電子情報通信学会 HB/KB 幹事長．情報処理学会論文賞（1996，2001，2008 年），情報処理学会 40 周年記念論文賞，日本 VR 学会サイバースペース研究賞，IEEE SAINT'04，ICAT'07 最優秀論文賞等を受賞．IEEE，ACM，電子情報通信学会，人工知能学会各会員．

© 2013 Information Processing Society of Japan