セキュリティ対策選定のための関与者に応じた評価指標の検討

佐々木　剛史[†]　西村　啓渡[‡]　加藤　弘一[‡]　勅使河原　可海[‡]

[†]創価大学工学部　[‡]創価大学大学院工学研究科

1. 研究の背景と目的

情報システムの発展と脅威の多様化に伴い，企業や大学などの組織における情報セキュリティ対策は重要な課題となっている．組織のネットワークにおける対策選定では，費用対効果，業務手順の増加など，様々な評価の観点がある．そのため，経営者，管理者，社内ユーザ，顧客といった各関与者が満足することが重要である．このとき，各関与者に対して，リスク顕在化時の損失額といったコスト，リスク低減度，利便性など，適切な評価指標を提示することが必要である．

これに対し，いくつかの評価指標を考慮したセキュリティ対策選定手法が研究されている[1][2][3]．文献[1]では，リスクと利便性を定量化し対策選定を行っているが，対策導入・運用コストは考慮されていない．文献[2]では，各関与者の要望を反映させるために，合意形成により対策選定を行っている．文献[3]では，対策変更に影響するリスク値，利便性低下度，対策コストを算出し，運用時における対策見直しを可能にしている．しかし，文献[2]，[3]は，対策ごとに利便性を算出しているため，業務における影響を認識できない．

これらの研究とは異なり，文献[4]では，探索的因子分析を用い，セキュリティ技術に対する利用者の安心感の要因の構造化を図っており，心理的側面が強い概念であることから，定量的な評価が困難であることを指摘している．

このように，従来の手法では，対策選定に必要な評価項目および提示方法が体系化されていない．そこで，本研究では，各関与者の要望を反映したセキュリティ対策選定を目的とし，本稿では，各関与者を満足させるため，セキュリティ選定のための関与者に応じた評価指標を検討する．

2. 研究課題

一般的な対策選定において，リスク分析と，対策の選定が，重要なフェーズとなる．そこで，そのフェーズに対する課題を述べる．

2.1 対策選定の評価指標の特定と正確な評価

適切なセキュリティ対策選定を行うためには，まず，基準となる評価指標を決定することが重要である．しかし，関与者ごとに対策を評価する観点は異なるため，まず対策選定に必要な評価指標を分析して体系化をする必要がある．しかし，従来の対策選定では必要な要素が体系化されていないため，過不足のない評価指標の特定は非常に困難であると考えられる．

また，評価した結果から対策案を導出する際に，妥当性を持たせるために，決定した各評価指標の正確な評価を行う必要がある．しかし，同じ評価指標でも，関与者によって評価の観点が異なるため，妥当性のある評価は困難が予想される．

2.2 評価結果に基づく対策案の導出

関与者に応じた要望を正確に反映させた対策を選定するためには，対策導入・変更によって影響を受けるリスク，コスト，利便性などの，各評価指標すべてを，関与者が認識して対策を選択できなければならない．しかし，対策の種類が増加すると，対策組合せ数が膨大になり，対策導入・変更による全影響を認識することは容易ではない．そのため，評価項目の結果に基づいた対策案の導出法の確立が必要になる．

2.3 対策案に基づく合意形成

導出した対策案に基づいて，関与者が意見交換し，合意を形成する際，関与者に満足してもらうため，評価した項目を関与者に提示する必要がある．その際，管理者は，各対策における影響を表す多くの情報が必要となると考えられるが，経営者は詳細な情報は必要ではないと考えられる．つまり関与者によって必要となる情報は異なる．しかし，多種多様な関与者が考えられるため，関与者に応じて適切に評価結果を提示することは困難になる．

3. 対象とする関与者

経営者，社内ユーザ，攻撃者など，関与者の分類の仕方や対象の選定は多様である．そこで本稿では，対象とする関与者を経営者，管理者，ユーザに限定する．経営者とは，組織全体の営利を目的とし，事業活動の統括をする人物である．管理者とは，セキュリティに関する専門家で，情報システムに関する運用・管理を行う人物である．ユーザとは，原則的に同一の権限を有し，情報システムを利用し，事業活動を行う人物である．

4. 関与者の要望を考慮した評価指標

4.1 対策選定における評価指標の分析・体系化

2.1 節の課題に対するアプローチとして，各関与者の対策選定における目標や要望を基に，評価指標を体系化する．

各関与者の目標・要望を想定し，体系化したものを表 1 に示す．本稿では，評価指標を，コスト，セキュリティ，関与者への技術的・心理的影響の 4 項目とした．コストは，リスク顕在化時の損失額や，対策導入・運用費，対策導入に要する労力といった要素を包括する．セキュリティはリスク値やリスク低減効果といった要素を包括する．関与者への技術的影響は，業務への影響を意味する．心理的影響は，組織への社会的信用やコンプライアンス，安心感やプライバシーといった要素を包括する．

4.2 各評価指標の評価手法の検討

前節で決定した各評価指標はいくつかの要素を持つため，これらの要素を考慮した評価手法が必要となる．まず，コストに関しては，コストの概

A Study on Stakeholder-based Metrics for Selecting Security Countermeasures

Takeshi Sasaki[†], Keito Nishimura[‡], Koichi Kato[‡] and Yoshimi Teshigawara[†]

[†]Faculty of Engineering, Soka University

[‡]Graduate School of Engineering, Soka University

表 1　各関与者が考慮する評価指標と構成要素

	コスト（運用費、損害額、労力）	セキュリティ（リスクの期待値×リスク低減効果）	関与者への影響(制限)	
			技術的	心理的
経営者	対策導入費 対策運用費 リスク顕在化時の損失額	リスク低減効果	—	組織の社会的信用 コンプライアンス
管理者	対策導入に要する労力 保守運用に要する労力	リスク値 リスク低減効果	業務への影響	関与者の要望の反映 安全・安心の提供
ユーザ	—	—	業務への影響	安全・安心感 プライバシー

念が持つ 3 つの要素ごとに評価値を算出し，それらの和をコスト指標の評価値とする．リスク顕在化時の損失額は，リスクが顕在化した場合の組織の被害額と，リスクが顕在化しなければ得られていた利益である逸失利益，リスク顕在化から業務が正常に戻るまでに要するコストであるシステム復旧コストの和により金額として算出する．対策導入・運用費は，過去の事例などを参考に推計をする．対策導入に要する労力は，人月を単位として評価する[5].

セキュリティに関しては，セキュリティ指標が持つリスク値とリスク低減効果の 2 つの要素の積により，評価値を算出する．なお，評価値はリスクごとに算出するため，対象とするリスクの数だけ評価値が存在する．リスク値は，情報の資産価値と脅威の発生確率の積から求める．ここで，情報の資産価値は，リスク顕在化時における，資産の機密性，完全性，可用性の損失の度合いを，ISMS ユーザーズガイドを参考に求める[6]．また，脅威の発生確率は，フォルトツリー解析を活用し，リスク顕在化に至る流れを考慮して算出する[1]．一般的には，リスク値を算定する際に，資産価値に加え，脅威，脆弱性を考慮するが，今回は脆弱性を突く脅威が本当の脅威であるという考えから，資産価値と脅威の発生確率からリスク算定を行う．一方,リスク低減効果は，対策と低減・抑止効果のあるリスクを関連付け，ISMS ユーザーズガイドを参考に算出する[6].

関与者への技術的影響に関しては，対策と関与者の業務を関連付けて，その影響を評価する．今回は，業務を ICT 技術に関連する業務，またはサービス利用に限定する．具体的には，ビデオ会議や，メールの送受信などが考えられる．

関与者への心理的影響に関しては，対策による関与者の不満を，危険・不安・煩雑といった要素で表現し，それぞれ大中小の 3 段階で定性的に評価を行う．

例として，FW（ファイアウォール）とログ監視の対策を組み合わせた場合による，各評価指標の評価結果の例を表 2 に示す．想定するリスクは，情報漏えい，データ改ざん，システム停止とした．想定する業務は，管理者はログ監視とネットワーク帯域制御とし，ユーザはビデオ会議，メール送受信，Web 閲覧とした．

表 2 の例から，コスト，関与者への技術的影響，心理的な影響などの評価指標の各要素は，関与者ごとに評価結果が異なることがわかる．たとえば，技術的な影響に関しては，FW によるポート制限が考えられるため，ユーザのビデオ会議の利用への影響は大となる．このように，各関与者への対策による影響を明確に示すことで，関与者の要望を反映した対策選定が可能になると期待できる．

表 2　FW とログ監視の組み合わせの場合の各評価指標の評価結果例

	コスト（運用費、損害額、労力）		リスク（資産のCIAの損失×脅威の発生確率）		制限(影響) 技術的		心理的	
	項目	評価値[万円]	項目	評価値	項目	評価値	項目	評価値
経営者	導入費	100	情報漏えいの発生確率×低減効果	0.01×0.05	—	—	危険	小
	運用費	20	データ改竄の発生確率×低減効果	0.25×0.4	—	—	不安	中
	情報漏えい時の年間損害額	200	システム停止時の発生確率×低減効果	0.10×0.15	—	—	煩雑	小
	データ改竄時の年間損害額	100	—	—	—	—	—	—
	システム停止時の年間損害額	50	—	—	—	—	—	—
管理者	対策導入労力	30	情報漏えいの発生確率×低減効果	0.01×0.05	ログ監視	小	危険	大
	保守運用	100	データ改竄の発生確率×低減効果	0.25×0.4	ネットワーク帯域制御	小	不安	大
	—	—	システム停止時の発生確率×低減効果	0.10×0.15	—	—	煩雑	中
	—	—	—	—	—	—	—	—
ユーザ	—	—	—	—	ビデオ会議	大	危険	小
	—	—	—	—	メール送受信	中	不安	小
	—	—	—	—	Web閲覧	小	煩雑	大

5. まとめと今後の課題

本稿では，従来の手法は，対策選定に必要な評価項目および提示方法が体系化されていないという問題を解決するために，対策選定時に必要な要素を分析し，その各要素の評価手法の検討を行った．関与者に応じた評価指標を考慮することで，各関与者の対立する要望のバランスを考慮した対策選定が可能になると期待できる．

今後は，評価結果に基づいた理論上の最適対策組合せの導出，および全関与者が満足する対策組合せの決定手法を検討する．さらに，提案手法を実現するシステムの実装・評価を行う．

参考文献

[1] 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.3209-3222，2008.9

[2] 佐々木良一ら：多重リスクコミュニケータの開発と適用，情報処理学会論文誌，Vol.49，No.9，pp.3180-3190，2008.9

[3] 榊啓ら：多目的最適化によるセキュリティ対策立案方式の提案，コンピュータセキュリティシンポジウム 2007（CSS2007）論文集，Vol.2007，No.10，pp.193-198，2004

[4] 日景奈津子ら：情報セキュリティ技術に対する安心感の構造に関する統計的検討，情報処理学会論文誌，Vol.48，No.9，pp.3193-3203，2007.9

[5] IPA：「被害額算出モデル」報告書 http://www.ipa.go.jp/security/fy14/reports/current/2002-calc-model.pdf

[6] JIPDEC：ISMS ユーザーズガイド—JIS Q 27001:2006（ISO/IEC 27001:2005）対応—リスクマネジメント編