

中小企業の情報セキュリティ対策の 投資に対する費用対効果について

村田真理[†]

情報セキュリティ対策には、ハッキング等の外からの脅威に対する「外部セキュリティ対策」と、情報漏洩等の内からの脅威に対する「内部セキュリティ対策」がある。「内部セキュリティ対策」については、保有する個人情報数と従業員数によって、対策のための投資は変動するであろう。そうであるとすれば、効果的かつ戦略的な「内部セキュリティ対策」によって、企業価値の向上もたらされると考えられる。そこで本稿では、特に日本経済を支えている中小企業を対象とし、個人情報数・従業員数を変数とした「内部セキュリティ対策」の費用対効果について技術的・人的・組織的・物理的側面から検証する。本研究によって、中小企業の「内部セキュリティ対策」における効果的な投資配分が明らかになり、企業価値を高めるための情報セキュリティ対策の実現が可能となる。

The Cost-effectiveness to the Investment of the Information Security Measures of the Small- and Medium-sized Enterprise

Mari Murata[†]

The information security measures are "internal security measures" against the threat of information leak s and "ex ternal security measures" against exte rnal threats such as hacking.

Investment in "inter nal security measures" will change in proportion to the amount of personal information and th e number of employees. Such i nvestment would ac hieve improvement in corporate value th rough the implementation of effective and strategic "internal se curity measures." Finally, this r esearch ver ifies my c ost-effectiveness hypothesis, which concer ns the am ount of personal info rmation and the nu mber of employees, f rom th e technical, human, or ganizational, and ph ysical aspects. T he hypothesis particularly targets the small- and medium-sized enterprises that support th e Japanese economy.

This research could he lp d etermine th e effective a llocation of investment in "internal security measures" within small companies and thereby bring about a clear improvement in the enterprise value.

1. 研究の背景

平成 17 年 4 月に施行された「個人情報の保護に関する法律」の 22 条・委託先の管理により、委託先で起こった個人情報の漏洩事故は委託元の管理責任を問われることになった。このことから委託先での個人情報漏洩事故による損害の回避から、委託元は取引を行う条件として情報セキュリティ対策を委託先へ求める傾向にある。(1) また昨今、内部犯行による個人情報漏洩も多発していることから、情報セキュリティ対策は企業価値を下げないため、また取引において必要な対策といえる。

大多数の委託先は中小企業である。しかし中小企業が情報セキュリティ対策で問題・課題だと感じていることに「投資効果が見えづらい」「どこまで対策すべきか不明」が挙げられている。(2)

そこで本研究では、中小企業の内部的情報セキュリティ対策に的を絞り、考察を試みる。

2. 先行研究の調査

2.1 ROSI

情報セキュリティにおける投資回収率として、研究機関等においてROSI (Return On Security Investment) の算定の研究が進められている。このROSIは「算定方法は各研究機関等によって異なるが、多くはセキュリティ対策コストと年間損失予測 (ALE: Annual Loss Expectancy) に基づいており、セキュリティ対策の効果を算定することは、すなわち、損失を減少させた程度を算定することを意味する」(3)とされている。1977 年に米国連邦標準技術局 (NIST) が推奨した定量リスク分析手法として、

$$ROSI = R - ALE$$

$$ALE = (R - E) + T$$

があり、Rはシステム侵害からの回復コスト、ALEは年間ロス予測値、Eはシステム侵害を阻止することによって節減できる経費、Tはセキュリティ設備及びサービスにかかるコストと定め算定される。(4)しかし前述で示されているR・E・Tの各算定方法また数値の根拠が不明確であるため、取引先など社外または社内の経営幹部などに対し示す数値としては理解されにくい。経済産業省は日本セキュリティ監査協会 (JASA) のセミナーにて、「適切に評価を行わずに情報セキュリティ対策を施し続けていても投資効果 (ROSI) を評価できない」と述べている。(5)現状では、ROSIでは企業の情報セキュリティ対策の投資効果を測る方法として用いるには難しいと考える。

2.2 情報セキュリティ対策ベンチマーク

(独) 情報処理推進機構 セキュリティセンター (IPA) は、情報セキュリティ対策

[†] 大阪市立大学 創造都市研究科
Graduate School for Creative Cities, Osaka City University

で問題・課題だと感じている「投資効果が見えづらい」「どこまで対策すべきか不明」などに対し、情報セキュリティ対策ベンチマークを開発し、2005年8月からIPAのWEB上で無料にて提供されている。設問の内容として、情報セキュリティ対策への取組みに関する項目が25問、企業プロフィールに関する項目が15問で構成されている。多くの企業に利用されることにより回答データが蓄積され、他社との比較・セキュリティの高さなどが、簡易的に自社の情報セキュリティ対策の状況を知ることができる。しかし「取引先（業務委託元）に対する情報セキュリティに係わる対策説明時に有効な方法」の(2)アンケートの結果では、もっとも有効性が高いと回答された「プライバシーマーク」が29.2%、「セキュリティレベルを証明・確認するチェックリスト」が26.3%に対し、「情報セキュリティ対策ベンチマーク」は5.5%と支持は低い。

また設問が簡易的であるため、同業他社でも従業員数・個人情報の保有数が異なっても比較対象になる、また組織的な価値も考慮されていない。これらのことから、その企業にあった情報セキュリティ対策が行われているのか、情報セキュリティ対策ベンチマークでは分かりづらい。

3. 今後の研究予定

情報セキュリティ対策は、ハッキング等の外からの脅威に対する「外部セキュリティ対策」と、情報漏洩等の内からの脅威に対する「内部セキュリティ対策」に分けられる。ハッキングなど、いつ・どのような攻撃されるか分からない状況のなかセキュリティ対策を行わなければならない「外部セキュリティ対策」に対し、「内部セキュリティ対策」は従業員数・保有する個人情報に対するセキュリティ対策はある程度のコントロールができると考えられる。

今後の研究として、個人情報数・従業員数を変数とした「内部セキュリティ対策」の費用対効果について技術的・人的・組織的・物理的側面から、中小企業を対象とし検証する。本研究によって、中小企業の「内部セキュリティ対策」における効果的な投資配分が明らかになり、企業価値を高めるための情報セキュリティ対策の実現が可能となる。

参考文献

- (1) 経済産業省「平成20年度 個人情報の保護に関する取組み実態調査 調査報告」2009年3月 http://www.meti.go.jp/policy/it_policy/privacy/chosakekka.pdf#search='平成20年度 個人情報の保護に関する取組み実態調査 調査報告'
- (2) (独) 情報処理推進機構「中小企業の情報セキュリティ対策 確認手法に関する実態調査」

2008年4月 <http://www.ipa.go.jp/security/fy19/reports/sme/documents/sme-report.pdf>

(3) 日本ネットワークセキュリティ協会「情報セキュリティ会計に関する検討報告書～ガイドライン策定に向けて～」2005年7月 http://www.jnsa.org/houkoku2004/kaikei_report.pdf

(4) 各府省情報化統括責任者（CIO）補佐官等連絡会議「第4ワーキンググループ（情報セキュリティ）報告」2005年12月20日

<http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/dai21/21w4houkoku.pdf#search='R O S I 情報セキュリティ'>

(5) 経済産業省 商務情報政策局 情報セキュリティ政策室 井土和志 「わが国の情報セキュリティ政策について」 <http://www.jasa.jp/seminar/secf2008lh/pdf/s2008osaka01.pdf>