情報セキュリティ対策推進における中小企業経営者の心理的要因の研究

A Study on the Psychological Factors of Small and Medium-sized Enterprise Managers in Promoting Information Security Measures

堺祐一・法制倫理分科会・情報セキュリティ大学院大学

Small and medium-sized enterprises (SMEs) may be vulnerable to cyber-attacks and computer virus infections if they fail to implement appropriate information security measures. However, especially for companies forming part of the supply chain, addressing these threats is crucial. This study focuses on the psychological factors influencing executives' promotion of information security measures, utilizing protection motivation theory. The research adds factors related to the mutual relationship between one's own company and others, creating a hypothesis model. Subsequent steps involve validating these hypotheses through a survey, and based on the results, exploring effective approaches for information security measures targeted at SME executives.

1.研究背景

中小企業は、情報セキュリティに対する理解や知識、必要性の実感の欠如、リソース不足などにより、対策が不十分となり、サイバー攻撃に対して脆弱なことが多い。しかし、攻撃者は中小企業をターゲットとする割合を増やしている。特にサプライチェーンを構成する企業では、他社の感染が自社に影響を及ぼす可能性があるため、リスク対応が求められており、自社だけでなく取引先など他社の対策も考慮する必要がある。

2.研究目的

中小企業における情報セキュリティインシデントを減らすため、その耐性強化を目的とした対策導入・行動を推進するには、どのような心理的要因からのアプローチが有効であるかを明らかにすることを目的とする。特に本研究では、情報セキュリティ対策導入・推進の意思決定を行う経営者の心理的要因に焦点を絞る。

3.関連研究

■3-1.サプライチェーン等企業の関係性

脅威に対して脆弱さが残る構成企業から、取引ネットワークに侵入されインシデント発生につながるため、情報セキュリティ対策状況や脆弱性についての正確な把握が必要となる。企業間での「相互依存関係」や「対策未実施に対しての責任・影響」などの認識が求められる。

■3-2.中小企業経営者の意思決定と心理的要因

対策推進の決定を行う経営者について、脅威から自社が受ける影響についての認識は研究されているが、自社の脆弱性による他社への影響や、他社の脆弱性による自社が受ける影響の認識については調査されていない

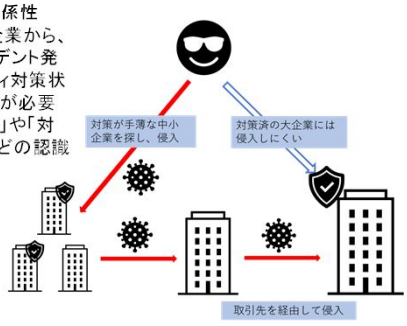

図1　取引先を利用した侵入例

■3-3.防護動機理論（Protection Motivation Theory ）

人々がある脅威から身を守る行動を説明するための枠組みをRogersらがモデル化した。本研究では、中小企業経営者の対策行動に対する促進および阻害する心理的要因を明確にすることを目的として、当理論を利用する。各心理的要因が、対策を実施しようとする「行動意図」や「実際の行動」への影響を調査し、分析する。

●各要因の説明
「重大性認知」･･･脅威に関する深刻さについての認知
「脆弱性認知」･･･脅威が発生する可能性について認知
「自己効力感」･･･脅威への対処行動を実行する能力があるかどうかについての認知
「反応効力感」･･･勧告された脅威への対処行動の効果についての認知
「反応コスト」･･･対処行動の実行に伴うコストについての認知
「行動意図」･･･対処行動を行おうとする考え

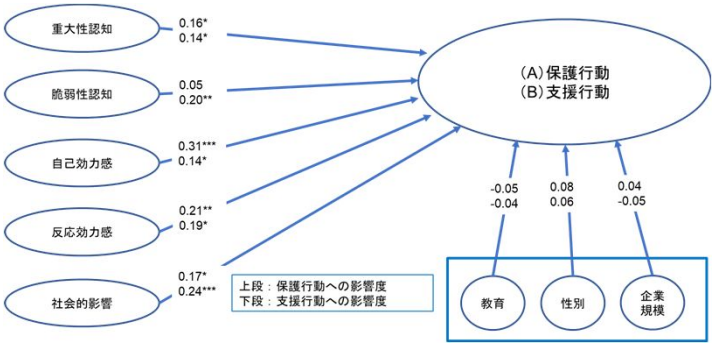

図2　Barletteらのモデル図と影響度の数値（論文を参考し著者が再作成）

※「社会的影響（同業他社や取引先が、自社が情報セキュリティ対策を行うべきであるという認識）」要因を追加し、「実際の行動」について調査している

4.提案モデル・調査

■4-1.調査を踏まえて追加した要因

防護動機理論をベースに、関連研究にて未調査となっていた脅威への対処に対する企業間の関係性、自社の対策導入有無による影響などについての要因を新たに追加する。

●追加した要因の説明
「相互関係認知」･･･自社と他社間での対策導入有無による影響の認識
「社会的影響」･･･社外からの対策実施要求等の認識
「責任認知」･･･自社の対策実施に対する責任の認識
「必要性認知」･･･自らの対策導入に対する必要性の認識

■4-2.要因間のモデル

各要因が、「行動意図」「実際の保護行動」へ与える影響（矢印）についてのモデル図（仮説）を示す。

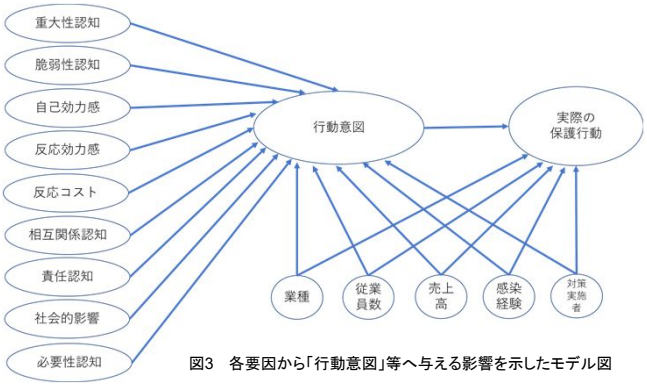

図3　各要因から「行動意図」等へ与える影響を示したモデル図

■4-3.アンケート調査

図3の仮説モデルを検証するため、アンケート調査を行った。より研究範囲を明確にするため、①中小企業の中でも企業数の多い「従業員50人以下」 ②個人データの扱いが比較的少ない「主たる取引を事業者間で行っている」中小企業経営者を対象とした。

表1　アンケート調査で使用した質問文例（一部抜粋）

番号	要因名	設定した質問文
1	重大性認知	自社の業務用PC・システムがウイルスに感染すると、自社の独自技術やノウハウの漏えいなどが発生すると思う
2	脆弱性認知	今後1年間に、自社の業務用PC・システムが、ウイルスに感染するかもしれないと思う
3	自己効力感	自社だけで、および、外部企業の協力を得て、自社の業務用PC・システムをウイルス感染から守ることができると思う
4	反応効力感	ウイルス対策は、自社の業務用PC・システムのウイルス感染を防ぐことに有効であると思う
5	反応コスト	ウイルス対策を初期導入する時に、時間・人件費・手間等の負担が大きいと思う
6	相互関係認知	自社の業務用PC・システムがウイルスに感染すると、そのウイルスはさらに発注元を狙う可能性がある
7	責任認知	発注元から自社に求められるウイルス対策やその実施レベルは、それぞれの企業ごとの人材や予算等の制約が考慮されるべきであると思う
8	社会的影響	自社は、発注元から、ウイルス対策の実施を期待されていると思う
9	必要性認知	自社の業務用PC・システムがウイルスに感染しないよう、その対策を実施する必要性があると思う

6.今後の予定

中小企業経営者向けのアンケート調査をWeb調査会社に委託し実施した。現在、回答データを受け取り、分析を始め、仮説モデルを検証している。この結果に基づき、情報セキュリティ対策導入・推進についての効果的なアプローチ案を考察した後、この案について、実際に中小企業経営者にインタビューを行う。