（ 続紙 １ ）

京都大学	博士（情報学）	氏名	佐藤直樹
論文題目	情報セキュリティ監査への確率論的リスク評価の適用に関する基礎的研究		

（論文内容の要旨）

情報セキュリティ事故が発生すると企業としての信用が揺らぎ、経済的にも打撃を受けるため、情報セキュリティ対策は、会社の業績と同様に、経営者が真剣に取り組むべきテーマとなっている。そこでPDCA(計画-実施-監査-是正)に基づく情報セキュリティの管理体制が敷かれ、その３ステップ目のプロセスとして情報セキュリティ監査があり、情報資産へのリスクのコントロールが、適切に整備かつ運用されているかどうかを、独立かつ専門的な立場の監査人が検証して評価し、保証や助言を与えている。一方、重要機密情報の漏洩等の重要事故を起こした顧客からは、緊急監査の強い要請がある。監査人はISOなどの監査マニュアルを使うのが通例であるが、セキュリティ事故に関する潜在的で具体的な発生シナリオとの関係が明確でないことのために、効率的で網羅的かつ説得力のある監査ができないという問題がある。本論文は、監査の効率性と完全性と顧客に対する説明性の向上を目的とし、そのために確率論的リスク評価の適用を考え、事故シナリオにもとづく監査を提案したものであり、全体は6つの章から成る。

第１章は序論であり、情報セキュリティ事故予防のための監査の重要性と、現状の監査が克服すべき課題について述べている。

第２章では、どのような種類の監査に対して、その効率化が最も望まれているかを明らかにするために、定期監査と緊急監査に対し、必要とされる工数を明らかにしている。過去の事例データを統計解析した結果、緊急監査のときは事故を起こした企業が監査対象となるために、定期監査に比べて工数がかかり、この緊急監査の効率改善が最優先課題であることを示している。

第３章では、事故シナリオを列挙する前に、確率論的リスク評価の手順に従い、セキュリティ事故の出発点ないしきっかけとなる事象、すなわち起因事象を列挙し分類している。確率論的リスク評価が通常の物理的なシステムに適用された場合を紹介したのち、情報セキュリティリスク定量化の現状について述べ、起因事象という概念の必要性を指摘し、この概念を情報セキュリティの場合へと拡張し、それらを列挙して分類している。従来の起因事象とは異なり、情報セキュリティでは全ての起因事象は、人間の悪意に基づくことを指摘している。

第４章では、起因事象からの事故シナリオを網羅し分類している。起因事象に対する緩和装置の応答の成否を事象木で展開し、事故シナリオの骨格を列挙している。情報セキュリティでは、緩和装置は通常の物理的原因や人的過誤のほか、人間の悪意によっても故障することを指摘している。次に、事象木の展開ノードを分かち書きで詳述して事故シナリオを詳細化している。従来技術としてFMEAやチェックリスト方式の監査を取り上げ、これらは事故シナリオをバックボーンとしていないために、監査項目や監査行為が単体として存在し、シナリオとの関連が明示されていないことを示し、事故シナリオを用いることによりこの弊害が改善できることを示している。また、監査の効率性、完全性、説明性の向上について指摘している。

第5章では、事故リスクの定量化の例として、盗難キーによる不正侵入などを取り

上げ、無防備時間帯の長さとその発生頻度の対の集合としてリスクを評価している。この種の定量化とGMITSとを比較し、事故シナリオが定量的に把握でき、シナリオのスクリーニングや緩和装置の重要度づけも行えるために、監査の効率と顧客への説明性などが向上することを示している。

第６章では、本研究の結論を述べている。

（続紙 ２ ）

（論文審査の結果の要旨）

情報セキュリティ事故が発生すると企業の信用とともに経済的にも打撃を受けるため、セキュリティ対策は、業績と同様に経営者が真剣に取り組むべきテーマである。そこでPDCAサイクルに基づく情報セキュリティの管理体制が敷かれ、その一つのステップとして情報セキュリティ監査があり、情報資産へのリスクのコントロールが、適切に整備かつ運用されているかどうかを、独立かつ専門的な立場の監査人が検証して評価し、保証や助言を与えている。一方、情報漏洩等の重要事故を起こした顧客からは、緊急監査の強い要請がある。監査人はISOなどの監査マニュアルを使うのが通例であるが、セキュリティ事故に関する潜在的で具体的な発生シナリオとの関係が明確でないために、効率的で網羅的かつ説得力のある監査ができないという問題がある。本論文は、監査の効率性と完全性と顧客に対する説明性の向上を目的とし、そのために確率論的リスク評価の適用を考え、事故シナリオにもとづく監査を提案し、下記の成果を得ている。

1. どのような種類の監査に対して、その効率化が最も望まれているかを定量的に明らかにするために、定期監査と緊急監査に対し、過去の事例データを統計解析し、必要とされる工数を明らかにした。緊急監査のときは事故を起こした企業が監査対象となるために、定期監査に比べて工数がかかり、この緊急監査の効率改善が最優先課題であることを示した。

2. 事故シナリオを列挙する前に、確率論的リスク評価の手順に従い、セキュリティ事故の出発点ないしきっかけとなる事象、すなわち起因事象を列挙し分類した。確率論的リスク評価が通常の物理的な工学システムに適用された場合を紹介したのち、情報セキュリティリスク定量化の現状について述べ、起因事象という概念の必要性を指摘し、起因事象を情報セキュリティの場合へと拡張し、それらを列挙して分類した。従来の工学システムの起因事象とは異なり、情報セキュリティでは全ての起因事象は、人間の悪意に基づくことを指摘した。

3. 起因事象からの事故シナリオを網羅し分類した。起因事象に対する緩和装置の応答の成否を事象木で展開し、事故シナリオの骨格を列挙した。情報セキュリティでは、緩和装置は通常の物理的原因や人的過誤のほか、人間の悪意によっても故障することを指摘した。また、事象木の展開ノードを分かち書きで詳述して事故シナリオを詳細化した。従来技術としてFMEAやチェックリスト方式の監査を取り上げ、これらは事故シナリオをバックボーンとしていないために、監査項目や監査行為が単体として存在し、シナリオとの関連付けが明示されていないことを示し、事故シナリオを用いることによりこの弊害が改善できることを示した。また、監査の効率性、完全性、説明性の向上について指摘した。

4. 事故リスクの定量化の例として、盗難キーによる不正侵入などを取り上げ、無防備時間帯の長さとその発生頻度の対の集合としてリスクを評価した。この種の定量化とGMITSとを比較し、事故シナリオが定量的に把握でき、シナリオのスクリーニングや緩和装置の重要度づけも行えるために、監査の効率と顧客への説明性などが向上することを示した。

以上のように本論文は、情報システムにとって重要な情報セキュリティ監査について、その効率性、完全性、顧客への説明性の向上を目的とし、確率論的リスク評価の適用を詳細に論じたものであり、その成果は情報学の展開に寄与するものと認

める。よって本論文は博士（情報学）の学位論文として価値あるものと認める。また、平成２２年３月１日に実施した論文内容とそれに関連した試問の結果合格と認めた。