

| | |
|--------------|---|
| Title | インターネット時代の情報セキュリティ管理 |
| Author(s) | 井戸田, 博樹 |
| Citation | 大阪大学, 2003, 博士論文 |
| Version Type | |
| URL | https://hdl.handle.net/11094/44191 |
| rights | |
| Note | 著者からインターネット公開の許諾が得られていないため、論文の要旨のみを公開しています。全文のご利用をご希望の場合は、 〈a href="https://www.library.osaka-u.ac.jp/thesis/#closed"〉 大阪大学の博士論文について 〈/a〉 をご参照ください。 |

Osaka University Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

Osaka University

| | |
|------------|---|
| 氏名 | 井戸田 博樹 |
| 博士の専攻分野の名称 | 博士(経済学) |
| 学位記番号 | 第 17448 号 |
| 学位授与年月日 | 平成15年2月20日 |
| 学位授与の要件 | 学位規則第4条第1項該当 経済学研究科経営学専攻 |
| 学位論文名 | インターネット時代の情報セキュリティ管理 |
| 論文審査委員 | (主査) 教授 辻 正次 (副査) 教授 田畑 吉雄 助教授 小郷 直言 助教授 今川 拓郎 |

論文内容の要旨

本稿において、インターネット時代における情報セキュリティ管理の理論的基礎の研究と、その実施フレームワークの確立を試みた。組織体は従来、情報セキュリティの諸課題に対応するためにさまざまな対策を講じてきた。しかし、継続的に組織体全体として有効な対策を実施するには、情報セキュリティ管理の実施が必要となる。そのフレームワークを確立のために、経営管理論、工学的意思決定手法、監査論などを援用した。またそれを受けて実践的課題である情報システムのアウトソーシングの管理と新技術導入に関する管理について考察した。

序章では、インターネット時代に適応した情報セキュリティ管理の研究が急務であることを述べ、管理面からの研究があまりなされていないことを明らかにした。そして、本論分のねらいとして情報セキュリティ管理のフレームワークを確立し、実践上の諸課題について考察することを述べた。第1章では、インターネット時代の情報セキュリティ管理についての特徴を分析するために、情報セキュリティについて歴史的考察を行った。そして経営管理論を援用し、管理サイクルのスパイラルアップの考え方を取り込んだ情報セキュリティ管理のフレームワークを提案した。また、このスパイラルアップは、予想を超える自然災害の発生などにより不連続的になされることを論じた。第2章では、計画過程として、情報セキュリティの方針であるセキュリティ・ポリシーの策定について論じた。英国企業に比べ、日本企業のセキュリティ・ポリシーの項目が技術偏重であるという調査結果を受け、情報セキュリティ管理における人の問題として、情報倫理の項目をセキュリティ・ポリシーに記載することを述べた。また限られた経営資源を有効に活用するために、対策の実施に先駆けてリスク分析をしなければならない。その際、できるだけ多くの構成員が分析に参加すれば情報セキュリティ意識の向上につながる。そこで情報資産の評価方法として、AHP (Analytic Hierarchy Process) を用いた方法について提案した。アンケート調査を通じて、その有用性を明らかにした。第3章では、事例を参考に情報セキュリティ対策について述べた。また継続的に有効な管理を行うために、情報セキュリティ管理を計画、推進、実施、評価の組織体制の整備が不可欠であることを論じた。併せて、不測事態における組織体制についても述べた。そして、構成員のモチベーションを向上させるには、全構成員に情報セキュリティの重要性を理解させて、情報セキュリティに対する当事者意識を持たせるように働きかけねばならない。そのために不可欠となるセキュリティ・コミュニケーションについて考察した。最後に情報セキュリティ対策にナレッジ・マネジメントの手法を活用することを考察した。第4章では、統制過程として、情報セキュリティ管理の内部統制について述べた。また、情報セキュリティ管理のシステム監査を実施するには、従来型の情報セキュリティ監査では不十分なことを指

摘し、その解決策について検討した。そして、監査結果について組織体を超えて共有することが、インターネット時代の情報セキュリティ管理にとって重要であることを論じた。情報セキュリティ管理における内部統制は、情報セキュリティ管理者によるチェック機能や内部牽制機能だけでなく、むしろ現場の管理者や従業員が主体的にセルフチェックできる仕組みを整備することが望ましいので、情報セキュリティ管理の内部統制を現場の管理者や従業員が主体的に評価するために、CSA (Control Self-Assessment) を用いた情報セキュリティ管理のシステム監査について考察した。第5章では、情報システムのアウトソーシングの情報セキュリティ管理について、自治体情報システムを取り上げて論じた。まず電子自治体の実現に自治体情報システムのアウトソーシングが不可欠であることを述べた。そして宇治市の個人情報漏えいの事例を参考にして、情報システムのアウトソーシングの脆弱性とアウトソーシングの情報セキュリティ管理について考察した。また電子自治体を早期に実現するには、自治体間でいかに共同化して情報システムを立ち上げるかが課題となり、その解決策として、ASP (Application Service Provider) の利用があることを述べた。自治体によるその活用事例を紹介し、その情報セキュリティ管理のための管理項目について具体的に考察した。最後に小規模の自治体でアウトソーシングを行う場合に、自治体がアウトソーサーにイニシアティブを持つ手段として、新に共同利用組織や都道府県による自治体情報システムのアウトソーシング管理監督制度を提言した。第6章では、新技術の導入に伴う情報セキュリティ管理について考察するために、次世代インターネット技術として Peer-to-Peer を取り上げた。次にその脆弱性と対策について、機密性、完全性、可用性、否加害性の観点から考察した。新技術の導入に伴う情報セキュリティ管理について、新技術の調査、導入前のテストの強化、テスト内容などの確認と承認制度、試験的導入と導入計画の再検討、導入段階でのシステム監査などの必要性を説いた。

論文審査の結果の要旨

学位申請者に対して論文内容及びこれに関連する事項について試問を実施した。セキュリティ技術の革新による今後の情報セキュリティ管理の必要性や地方自治体における情報資産評価への AHP 適応の可能性などの質疑に対し、適切に回答しており、審査委員全員の協議の結果、学位申請者 井戸田 博樹 は、博士 (経済学) の学位を授与される資格があるものと認めた。