氏名（本籍）	江口　彰
学位の種類	博士（経営学）
学位記番号	博乙第　2979　号
学位授与年月日	令和　3　年　2　月　28　日
学位授与の要件	学位規則第４条第２項該当
審査研究科	ビジネス科学研究科
学位論文題目	情報セキュリティインシデント抑制のためのISO/IEC 27001 規格の活用に関する研究

主	査	筑波大学准教授	博士（工学）	領家　美奈
副	査	筑波大学教授	博士（システムズ・マネジメント）	倉橋　節也
副	査	筑波大学教授	博士（学術）	佐藤　忠彦
副	査	筑波大学准教授	博士（文学）	尾碕　幸謙
副	査	岐阜聖徳学園大学准教授	博士（経営学）	山田　浩喜

論文の内容の要旨

情報技術が企業活動に深く浸透することに伴い，情報セキュリティは欠くことのできない経営基盤と位置付けられる．情報セキュリティマネジメントに関わる重要な国際規格として ISO/IEC 27001 が策定され，多くの企業が認証を取得してきた．しかしながら，現在でも情報セキュリティインシデントが皆無というわけではない．このような状況を踏まえ，本論文では，我が国の ISO/IEC 27001 規格の認証取得組織における情報漏えいに係る実態を把握し，情報セキュリティインシデントのより効果的な抑制を狙いとしてインシデント抑制効果のメカニズムを解明し，講じるべき施策の導出を目的とする．本論文は全６章から構成される．

第１章では，研究の背景と目的を述べたうえで，本論文の問題意識を明らかにしている．

第２章では，ISO/IEC 27001 規格の概要および特徴を紹介したのち，ISO マネジメントシステム規格認証取得による効果分析，インシデント抑制のためのリスク分析と対策のための管理策の同定に関する先行研究を概観し，本研究の位置付けを述べている．さらに，不正に関連する行動理論を概観し，不正のトライアングル理論に基づいた本研究目的を達成するための接近方法を述べている．

第３章では，我が国の情報セキュリティインシデント報告書データを基づき，ISO/IEC 27001 認証の認証取得組織と未取得組織のインシデント発生に係る比較，業種による比較，インシデント発生の原因分析を行い，実態把握を行う．インシデント発生のオッズ比等に基づく比較検討と状況報告に基づく原因分析の結果等から，諸外国における認証取得を目的にしている組織では認証取得の効果が薄れるという先行研究に準ずる実態であること，インシデント発生の多くについては ISO/IEC 27001 の要求事項・管理策を遵守していれば防ぎ得たものであることを確認している．

第４章および第５章では，情報セキュリティマネジメントシステムのユーザーである組織構成員を対象に，組織が講じている ISO/IEC 27001 規格の要求事項あるいは管理策を核とした施策から情報漏えい抑制に至るメカニズムを解明し，より効果的な施策の導出を行う．その接近方法として不

正のトライアングル理論の「動機」，「機会」，「正当化」の３つの要素のうち，組織がルール策定することで効果を見込むことができる「機会」と「正当化」に焦点をあてて，不正な情報持ち出しを抑制するための施策を検討している．

第４章では，不正のトライアングル理論における「正当化」を抑制する観点から，不正に情報を持ち出す行為の正当化を抑制するために組織がどのような施策を講じるべきかを，ISO/IEC27001 の要求事項を核とした項目について調査収集したデータならびに仮説に基づいて共分散構造分析を行っている．さらに組織における ISO/IEC 27001 認証の有無による多母集団分析を行い，組織構成員による不正に情報を持ち出す行為の正当化におよぼす影響が異なるかを検討している．これらに基づき正当化を抑制するためのメカニズムを解明し，認証の有無により講じるべき施策を提案している．

第５章では，不正のトライアングル理論における「機会」を抑制する観点から，組織がどのような施策を講じるべきかを，ISO/IEC 27001 規格の管理策を核とした項目について調査収集したデータならびに仮説に基づいて共分散構造分析を行っている．職種に応じて取り扱う情報の種類が異なると推察することから，職種による多母集団分析を行い，インシデントの発生状況に違いがあるのかを検討している．これらに基づき機会の観点からインシデントを抑制するためのメカニズムを解明し，職種に応じて講じるべき施策を提案している．

最後の第６章では，本論文の研究成果を総括している．

審査の結果の要旨

【批評】情報セキュリティの確保は組織体が健全な事業活動を継続するための基盤要件であり，情報技術の急速な高度化に従い，その重要性が増している．迅速な業務，例外処理が生ずる顧客対応等が組織構成員に要求される中，ISO/IEC 27001 規格を核とした施策から情報セキュリティインシデント発生に至るメカニズム解明，それに基づくリスク低減のための施策導出に実務的な関心は高い．ISO/IEC 27001 規格の認証取得を目的とせず，認証取得後の PDCA サイクルを効果的に繰り返すための提案，継続可能なルール遵守や組織構成員の認識と業種に則った施策提案を提示した意義は大きい．

本論文が提案する施策を実組織に適用し，その有効性の評価を実施できていない点に，論文審査委員会は課題が残ると考えているものの，本研究は，ISO/IEC 27001 規格のより効果的な活用のための多くの示唆を提示しており，博士（経営学）を授与するに十分な内容と判断する．

【学力の確認】ビジネス科学研究科学位論文審査(博士後期課程)に関する内規第 11 条を適用し，学力の確認の全部に代え，十分に学力があるものと認定した．

【結論】よって，著者は，博士（経営学）の学位を受けるのに十分な資格を有するものと認める．