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

筑波大学審査学位論文（博士）

２０２０

江　口　　彰

筑波大学大学院
ビジネス科学研究科　企業科学専攻

目次

第 1 章　はじめに 1

1.1. 背景と問題意識 2

1.2. 本論文の目的 4

1.3. 本論文の構成 4

第 2 章　関連研究 7

2.1. 関連研究調査の観点 8

2.2. ISO/IEC 27001 規格の概要および特徴 9

2.3. インシデント抑制のためのマネジメントシステムに関する研究 11

2.3.1. ISO/IEC 27001 認証取得の効果 11

2.3.2. ISMS の有効活用に関する研究 17

2.4. インシデント抑制のための管理策に関する研究 19

2.4.1. 管理策を講じるべきリスクの決定手法に関する研究 19

2.4.2. 管理策の決定に関する研究 21

2.5. 不正に情報を持ち出す行為に関する研究 23

2.6. 本論文にて解決すべき課題 25

第 3 章　ISO/IEC 27001 認証有無による インシデント事例の比較分析 30

3.1. 背景と目的 31

3.2. 比較分析用データの作成 32

3.3. 認証有無によるインシデントの比較 34

3.3.1. インシデント発生／未発生組織数の比較 34
3.3.2. インシデント発生／未発生件数の比較 40
3.3.3. 管理策別インシデント発生比率比較 47
3.4. 考察 52
3.5. 結論 54
第 4 章　不正な情報持ち出しの正当化抑制のための施策 56
4.1. 背景と目的 57
4.2. 関連研究 58
4.2.1. ISO/IEC 27001 認証取得の効果に関する研究 58
4.2.2. 不正な情報持ち出し行為の正当化を抑制するための施策に関する研究 59
4.2.3. 本章のアプローチ 60
4.3. 仮説の設定および仮説検証モデルの構築 60
4.3.1. 仮説の設定 60
4.3.2. 仮説検証モデルの構築 62
4.4. 質問紙の設計 62
4.4.1. 観測変数の設定 62
4.4.2. 質問紙調査 64
4.5. 仮説の検証 65
4.5.1. 取得データの特徴 65
4.5.2. 不正な情報持ち出し行為の正当化におよぼす影響の構造分析結果 67
4.6. 結論 73
第 5 章　不正な情報持ち出しの 機会抑制のための施策 75

5.1. 背景と目的 76
5.2. 関連研究 78
5.2.1. 不正に情報を持ち出す行為の要因分析に関する研究 78
5.2.2. 促進活動の効果に関する研究 79
5.2.3. 管理策の策定に関する研究 79
5.2.4. 本章の観点 80
5.2.5. 本章のアプローチ 80
5.3. 仮説の設定および仮説検証モデルの構築 81
5.3.1 促進活動の充実度 81
5.3.2. 仮説の設定 83
5.3.3. 仮説検証モデルの構築 85
5.4. 質問紙の設計 85
5.4.1. 観測変数の設定 85
5.4.2. 質問紙調査 87
5.5. 仮説の検証 88
5.5.1. 仮説検証モデルに対する共分散構造分析結果（職種全体） 88
5.5.2. 職種による特性分析 90
5.5.3. 仮説の検証結果 92
5.6. 結論 94
第６章　結語 96
6.1. 各章の要約 97
6.2. 本論文の実務的貢献 99

6.3. 今後の課題 100

謝辞 102

参考文献 103

付録１：オッズ比の 95%信頼区間の導出 129

付録２：認識を通じた不正行為の正当化抑制に関する質問紙調査項目 132

付録３：管理策の遵守を通じた情報漏えい抑制に関する質問紙調査項目 134

第１章　はじめに

1.1. 背景と問題意識

「ヒト」,「モノ」,「カネ」は経営資源と総称され，組織にとっての成長を支える重要な要素として捉えられてきた．しかし 1990 年代後半のインターネットの普及により，情報は単に保有するものから利活用するものとして捉えられ，経営資源の 1 つとして加えられるようになっている．組織にとっての情報には，広告をおこない，収益拡大につなげるための顧客情報，製品またはサービスを提供する際に他社と差別化をおこなうためノウハウを盛り込んだ技術情報, シェアや収益を拡大させるための経営戦略の情報などが含まれる．すなわち組織にとって価値を持つ情報の有効な活用は，成長を支える重要な要素となっている．これらの情報は知られてはいけない第三者に知られてしまうと，競合他社に模倣した製品またはサービスを提供されてしまうことによる投資回収機会の逸失および顧客の流出，これらを原因とした株価の低下，または信用の失墜などにつながり，事業の継続を脅かす重大な問題となる．

情報の流出抑制を含む，情報を保護するための概念としては,「情報セキュリティ」がある．情報セキュリティとは「情報の機密性，完全性および可用性を維持すること」として定義されている（ISO, 2014a）．組織は，情報を許可されたもの以外の第三者に漏らさないこと（機密性），情報を正確な情報に保つこと（完全性），情報を利用したいときに利用できるようにすること（可用性）を侵害する，情報セキュリティインシデントを抑制するための施策を講じる必要がある．情報セキュリティインシデントとは「望まない単独もしくは一連の情報セキュリティ事象，または予期しない単独もしくは一連の情報セキュリティ事象であって，事業運営を危うくする確率および情報セキュリティを脅かす可能性が高いもの」（ISO, 2014a）をいう．また情報セキュリティ事象とは「情報セキュリティ方針への違反もしくは管理策の不具合の可能性，またはセキュリティに関係し得る未知の状況を示す, システム, サービスまたはネットワークの状態に関連する事象」(ISO, 2014a) をいう．本論文では簡略化のため「情報セキュリティインシデント」を「インシデント」とよぶこととする．

インシデントを抑制するためには，情報セキュリティマネジメントシステム（Information Security Management System，以下「ISMS」という．）を整備し，運用することが有効とされている（Broderick, 2006；Jayawickrama, 2006；Djapic & Lukic, 2007；Dey, 2007；Mellado *et al.*, 2007）．ISMS とは，情報セキュリティに関して Plan（ISMS の

確立），Do（ISMS の導入および運用），Check（ISMS の監視およびレビュー），Act（ISMS の維持および改善）の PDCA サイクルを整備し，運用することで継続的改善につなげるための枠組みである．

ISMS を整備し，運用するには，ISO/IEC 27001 規格（ISO, 2013）が広く用いられている．ISO/IEC 27001 とは，国際標準化機構（ISO：International Organization for Standardization）が定める，ISMS に関する国際規格である．ISO/IEC 27001 規格は，ISMS 適合性評価制度（情報マネジメントシステム認定センター，2018）における第三者認証の基準として用いられている．ISO/IEC 27001 認証は，ISO/IEC 17021-1 規格（ISO, 2015c）や ISO/IEC 27006 規格（ISO, 2015d）といった ISO が定める審査基準に基づいて審査され，適合と判断された場合に付与される．すなわち ISO/IEC 27001 認証が付与されている組織は，ISO/IEC 27001 規格の要求事項に沿った ISMS を整備し，運用しているということができる．このため ISO/IEC 27001 認証は，自組織の情報セキュリティ体制が十分であることの対外的アピールや，委託先の選定要件，官公庁における入札要件として広く使用されている．

筆者はコンサルタントとして数十の組織に対し，ISO/IEC 27001 認証の取得や維持を支援してきている．筆者が支援している組織の多くは，取引要件や官公庁における入札要件など，案件を受注するために必要であることをきっかけとして，ISO/IEC 27001 認証を取得している．しかし筆者の実務経験からは，次のような状態が散見される．ISO/IEC 27001 規格は，業種や規模にかかわらず適用できるように，高い抽象度で記載されている．抽象度の高い規格の解釈は難解であるため，多くの組織はコンサルティング会社が提供する規定・様式類を用いている．認証取得を希望する組織は，コンサルティング会社が提供する規定・様式類をカスタマイズすることなく単純に採用する場合があるため，既存のルールと競合し，混乱を生んでいる．その結果，組織構成員が守るべきルールと，守らなくてよいルールの線引きを勝手におこなっている．認証の取得または維持のみが目的となった組織では，内部監査や審査の直前に証跡の整備をするといった運用がなされている．組織構成員の負荷を強いるルールの存在が「すべてのルール遵守できなくても仕方のない」との意識を生むことがある．

このような整備または運用実態であるとしても，Ⅰ．ISO/IEC 27001 を認証取得しさえすれば，情報セキュリティに関連するインシデントを抑制できるのだろうか．またⅡ．組織は ISO/IEC 27001 規格に準拠する際，どのような点に注意して施策を講じれば効果的

にインシデントを抑制させることができるのだろうか．これが本論文における問題意識である．

1.2. 本論文の目的

本論文では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をおこなう．このため ISO/IEC 27001 規格へ準拠する組織を対象として，インシデント抑制効果のメカニズムをあきらかにする．メカニズムの解明を通じて，インシデントを抑制するために組織が ISO/IEC 27001 規格へ準拠する際，どのような施策を講じるべきかを提案することを目的とする．

1.3. 本論文の構成

第 2 章では，まず本論文で取り上げる ISO/IEC 27001 規格の概要について紹介するとともに，規格の特徴について述べる．続いて ISO/IEC 27001 規格の特徴に基づいて関連研究を紹介する．関連研究は，ISO/IEC 27001 規格における要求事項に該当する ISMS の観点からⅠ．インシデント抑制のためのマネジメントシステムに関する研究を紹介する．また附属書 A に該当する管理策の観点から，Ⅱ．インシデント抑制のための管理策を紹介する．第 4 章および第 5 章では，第 3 章の分析結果に基づき，不正な情報持ち出し行為に焦点をあてて組織が講じるべき施策を検討している．このためⅢ．不正に情報を持ち出す行為の抑制に関する研究を紹介する．Ⅰ～Ⅲの観点における関連研究の紹介を通じて，本論文の目的を達成するにあたって解決すべき課題を特定する．

第 3 章では，インシデントの発生状況について，データを用いて情報セキュリティの ISO マネジメントシステム規格認証である ISO/IEC 27001 認証の認証取得組織と未取得組織を比較する．これを通じて ISO/IEC 27001 認証を取得している組織がインシデントを抑制できているのかを検証する．またインシデントの原因を分析することにより，ISO/IEC 27001 規格に準拠している組織において，インシデントを抑制するうえでの問題点をあきらかにする．さらに本論文では，インシデントの発生に対して業種が影響をおよぼすとの仮定に基づき，業種に応じたインシデントの発生状況を分析する．

第 4 章および第 5 章では，インシデントのうち影響が大きいとされる（情報処理推進機構, 2015；情報処理推進機構, 2016），組織構成員が不正に情報を持ち出す行為に焦点をあてる．組織構成員が不正に情報を持ち出す行為を抑制するための理論として，本論文では不正のトライアングル理論（Cressey, 1971）を用いて講じるべき施策を検討する．不正のトライアングル理論における「動機」,「機会」,「正当化」の 3 つの要素のうち，不正に情報を持ち出す行為に対する「動機」は，たとえば人事制度への不満や，組織風土などがあげられる（情報処理推進機構，2012）．これらの動機を抑制するには，組織や制度に対する改革が必要なため，対応には困難が伴う．このことから本論文では,「機会」および「正当化」の観点から不正な情報持ち出しを抑制するための施策を検討する．

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考察する．さらに組織における ISO/IEC 27001 認証の有無により，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分析する．分析を通じて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する．

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考察する．また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，職種に応じてインシデントの発生状況に違いがあるのかを分析する．分析を通じて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する．

第 6 章では，第 1 章から 5 章の各章を要約する．そのうえで本論文の目的である，ISO/IEC 27001 規格への準拠を通じてインシデント抑制の目的を達成するため，組織が講じるべき施策を提案する．また論文の実務的な貢献および今後の課題について述べる．

本論文の構成を図 1-1 に示す．

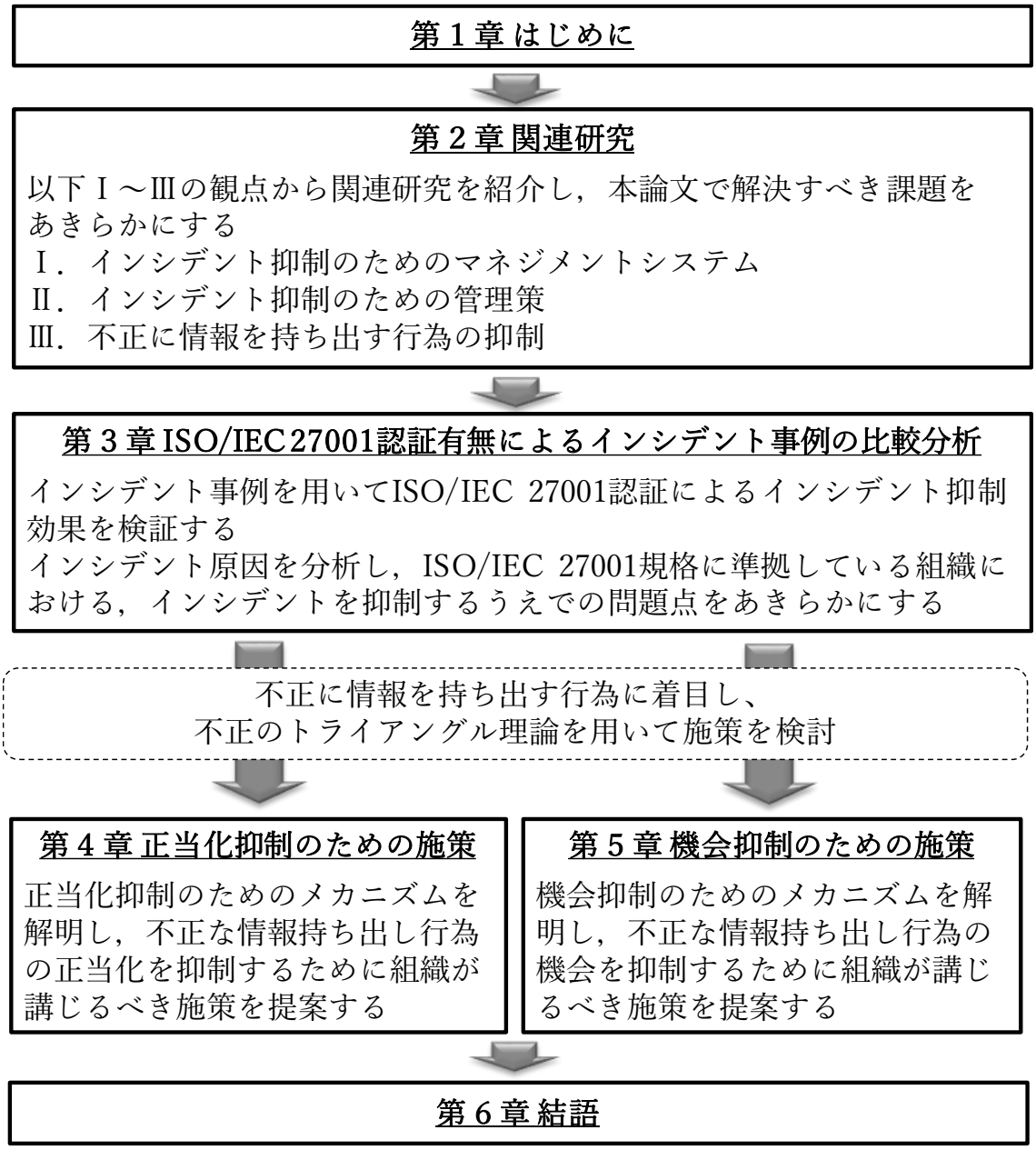
第１章 はじめに
第２章 関連研究
以下Ⅰ～Ⅲの観点から関連研究を紹介し，本論文で解決すべき課題をあきらかにする
Ⅰ．インシデント抑制のためのマネジメントシステム
Ⅱ．インシデント抑制のための管理策
Ⅲ．不正に情報を持ち出す行為の抑制
第３章 ISO/IEC27001認証有無によるインシデント事例の比較分析
インシデント事例を用いてISO/IEC 27001認証によるインシデント抑制効果を検証する
インシデント原因を分析し，ISO/IEC 27001規格に準拠している組織における，インシデントを抑制するうえでの問題点をあきらかにする
不正に情報を持ち出す行為に着目し、
不正のトライアングル理論を用いて施策を検討
第４章 正当化抑制のための施策
正当化抑制のためのメカニズムを解明し，不正な情報持ち出し行為の正当化を抑制するために組織が講じるべき施策を提案する
第５章 機会抑制のための施策
機会抑制のためのメカニズムを解明し，不正な情報持ち出し行為の機会を抑制するために組織が講じるべき施策を提案する
第６章 結語

図 1-1　本論文の構成

第 2 章　関連研究

2.1. 関連研究調査の観点

インシデントの抑制という問題に対しては，組織体制の整備をはじめとして，物理的および論理的アプローチ，さらにはこれらを整備し，運用する者に対する人的なアプローチが考え得る．本章では，インシデントを抑制するための ISO/IEC 27001 規格の活用を切り口として関連研究を調査し，紹介する．関連研究を調査するにあたっての枠組みは図 2-1 に示す．

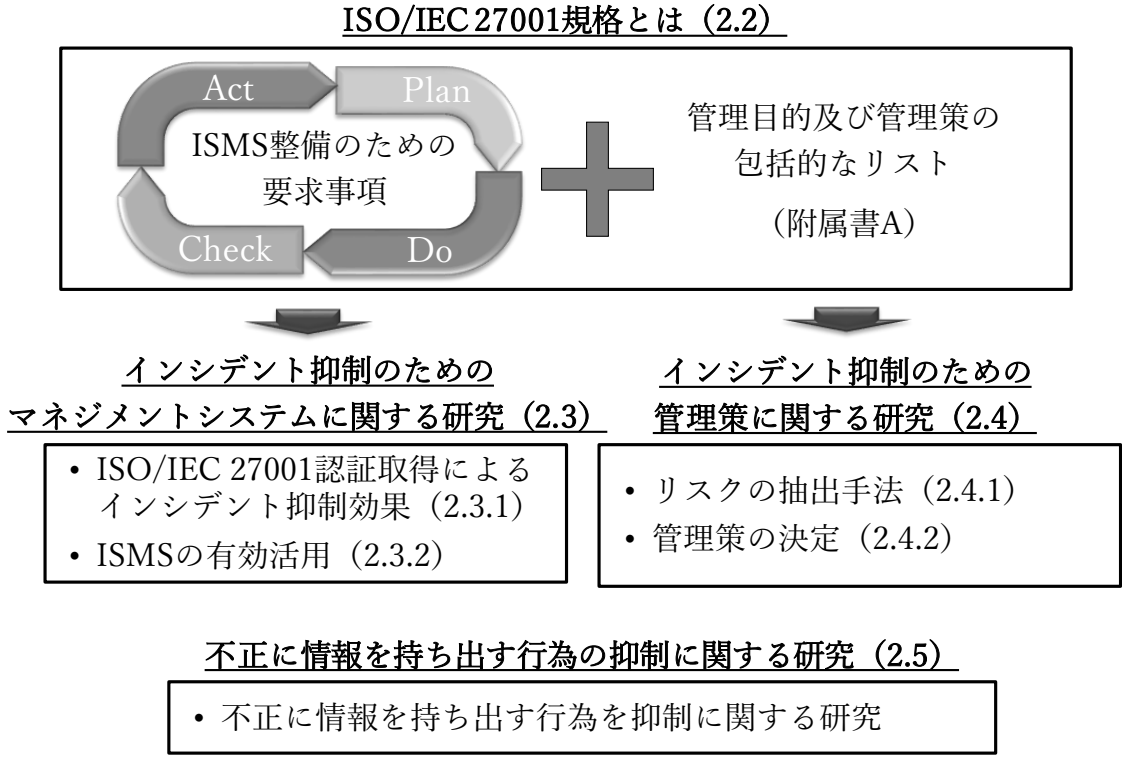

図 2-1　関連研究調査の観点

2.2 節では，本論文で対象としている ISO/IEC 27001 規格の概要および規格の特徴を述べる．その後 ISO/IEC 27001 規格の特徴に沿って情報セキュリティインシデント抑制のための ISO/IEC 27001 規格の活用に関連する研究を紹介する．関連研究の調査にあたっては，2.3 節にて ISO/IEC 27001 規格における要求事項に該当する ISMS に関する研究，2.4 節にて附属書 A に該当する管理策の観点から実施する．第 4 章および第 5 章では，不正に情報を持ち出す行為の観点から，組織が講じるべき施策を検討する．このため

2.5 節にて不正に情報を持ち出す行為に関する関連研究を紹介する．2.6 節では本論文で解決すべき課題を定義する．

2.2. ISO/IEC 27001 規格の概要および特徴

本節では本論文で対象としている ISO/IEC 27001 規格の概要および特徴について，ほかの ISO マネジメントシステムの比較を通じて紹介する．

ISO/IEC 27001 は，国際標準化機構が発行する，ISMS に関する国際規格である．ISO/IEC 27001 規格に準拠した ISMS を整備し，審査員が適合と判断することにより，ISO/IEC 27001 認証が組織に対して付与される．

ISO/IEC 27001 規格は，品質マネジメントシステム（QMS：Quality Management System）の規格である ISO 9001 (ISO, 2015a) や，環境マネジメントシステム（EMS：Environmental Management System）の規格である ISO 14001（ISO, 2015b）などと同様に，ISO マネジメントシステム規格として分類されている．ISO マネジメントシステム規格とは，管理するための仕組み（マネジメントシステム）に対する規格であり，規格を適用することにより，取り扱う対象を保護することを目的としている．ISO/IEC 27001 規格では情報セキュリティの観点から PDCA サイクルを整備し，継続的改善につなげるための要求事項を提供している．ISO マネジメントシステム規格に分類される規格は，いずれもどのような規模または業種にも適用できるよう，高い抽象度で要求事項が記載されている．このため規格に準拠したマネジメントシステムを構築する組織は，自らの解釈に基づき要求事項を実現する必要がある．ISO/IEC 業務指針第 1 部（ISO, 2020）の附属書 SL では，ISO マネジメントシステム規格の要求事項にあたる項目についての指針を示している．2013 年以降に発行される ISO マネジメントシステム規格は，附属書 SL に基づいて作成されている．ISO/IEC 27001 規格のみならず，ほかの ISO マネジメントシステム規格においても，ISO 9001 規格であれば品質の観点から，ISO 14001 規格であれば環境の観点から，ISO/IEC 27001 規格と同様に附属書 SL の構成に基づいて，PDCA サイクルを整備し，継続的改善につなげるための要求事項を提供している．

PDCA サイクルを整備し，継続的改善につなげるという観点においては，すべての ISO マネジメントシステム規格で共通している．一方 ISO/IEC 27001 規格は，PDCA サイクルの整備し，運用することに関する要求事項に加え，附属書 A とよばれる情報を保護する

ための具体的な管理策を集めた管理目的および管理策の包括的なリストを提供しているといった特徴をもつ（Kenning, 2001）．附属書 A とは，情報セキュリティの観点において洗い出されたリスクへの対応をおこなう際，必要な管理策に見落としがないことを検証するために用いられる，管理目的および管理策の一覧である．附属書 A と照らし合わせてリスクへの対応に見落としがないことの検証は，ISO/IEC 27001 規格の 6.1.3 c)における要求事項となっている．また ISO/IEC 27001 規格の要求事項 6.1.3 d)では，適用宣言書と呼ばれる，附属書 A に列挙された管理策の適用状況をまとめた一覧を作成することが求められている．このことから ISO/IEC 27001 規格に準拠した ISMS を構築するには，要求事項のみならず附属書 A に記載された管理策の一覧を適用することが求められる．附属書 A は，ISO 9001 規格や ISO 14001 規格にはみられない, ISO/IEC 27001 規格特有の特徴である．なお管理策とは，「リスクを修正する対策」と定義されており（ISO, 2014a），附属書 A では，情報セキュリティのための方針策定のほか，組織的，人的，物理的，論理的などの観点における対策が含まれている．

ISO マネジメントシステム規格認証は，第三者認証としても位置づけられている．第三者認証は，規格毎に定められた要求事項に対して適合しているかを，当事者である組織とは無関係の第三者が審査し，証明することにより付与される．ISO/IEC 27001 認証の付与を希望する組織は，ISO/IEC 27001 規格に規定される要求事項をすべて満たす ISMS を構築し，それを第三者機関である認証機関による審査を受ける必要がある．審査を受け，すべての要求事項に適合していると判断された組織は，ISO/IEC 27001 認証を取得することができる．ISO/IEC 27001 認証は 3 年間有効である．認証を維持するため，組織は 3 年に 1 度の更新審査を受け，審査機関より適合判断される必要がある．そのほかサーベイランス審査（維持審査とよぶ場合もある．）と呼ばれる年 1 回または半年に 1 回の審査を受ける必要がある．

国際的な第三者認証である ISO/IEC 27001 認証と類似したものに，国内の情報セキュリティに関する第三者認証としての「ISMS 認証」がある．ISMS 認証とは日本産業規格である，JIS Q 27001 規格（日本規格協会，2014）にて規定する要求事項を満たすことで付与される認証である．JIS Q 27001 規格は，ISO/IEC 27001 規格を和訳したものである．ISO/IEC 27001 認証の審査を受ける場合においても ISO/IEC 27001 規格の要求事項への適合性の確認をもって ISO/IEC 27001 認証と ISMS 認証の双方を取得することができる．このことから本論文では，ISO/IEC 27001 規格と JIS Q 27001 規格について特段

の区別をおこなわず，「ISO/IEC 27001 規格」と表現する．同様に ISO/IEC 27001 認証と ISMS 認証においても特段の区別をおこなわず，「ISO/IEC 27001 認証」と表現する．なお JIS Q 27001 規格は，その内容の ISO/IEC 27001 規格に対する同等性が「IDT[1]」とされている．このことからも両者の規格は，実質的に同義のものとみなすことができる．

2.3. インシデント抑制のためのマネジメントシステムに関する研究

本節では PDCA サイクルを整備し，継続的改善につなげるための要求事項の観点から，インシデント抑制のためのマネジメントシステムに関する研究を紹介する．

2.3.1. ISO/IEC 27001 認証取得の効果

本項では ISO/IEC 27001 認証を取得することによるインシデント抑制効果に関する研究を紹介する．

ISO/IEC 27001 認証は，組織が構築する ISMS が，ISO/IEC 27001 規格の要求事項に対して適合していることを第三者機関が審査することで付与されものである．ISO/IEC 27001 認証のみならず，品質マネジメントシステムの ISO マネジメントシステム規格認証である ISO 9001（ISO, 2015a）認証，環境マネジメントシステムの ISO マネジメントシステム規格認証である ISO 14001（ISO, 2015b）認証を取得することによる効果は，「ビジネス上の効果（Business Performance）」と「オペレーション上の効果（Operational Performance）」に二分できる（Beattie & Sohal, 1999；Feng *et al.,* 2008）．ビジネス上の効果とは，財務，市場に関連のある実績に基づくパフォーマンスをいい，収益性，マーケットシェア，販売回転率，資本利益率などを指す．一方，オペレーション上の効果とは，組織内部のオペレーションに関するパフォーマンスをいい，エラー率の抑制，内部コミュニ

---

[1] 同等性に関しては，Identical（IDT），Modified（MOD），Not equivalent（NEQ）の 3 段階に分類されている．このうち以下のいずれかに該当するとき「IDT」に位置づけられる．

- 地域または国家規格が，技術的内容，構成および文言において一致している．
- 地域または国家規格が，ISO/IEC GUIDE 21-1:2005 の 4.2 節に規定した最小限の編集上の変更はあるが，技術的内容において一致している．「逆も同様の原理」があてはまる．

ケーション，業務フローの効率化などを指す．ISO マネジメントシステム規格の第三者認証に対するビジネス上の効果およびオペレーション上の効果について，調査の概要および効果の有無に対する結論について，1994 年から 2011 年までの関連研究をまとめたものを表 2-1 および表 2-2 に示す．

表 2-1 および表 2-2 によるとビジネス上の効果およびオペレーション上の効果いずれにおいても，ISO 9001 認証や ISO 14001 認証を中心に，日本を含め世界各国において様々な組織，団体を対象として分析されている．ISO マネジメントシステム規格認証の取得をもってビジネス上の効果またはオペレーション上の効果の向上に寄与するか否かは，調査実施国や調査方法等により結論が異なっている．

表 2-1　認証取得のビジネス上の効果についての関連研究

文献	対象規格	調査概要			結論
		対象地域	調査対象	調査方法	
Buttle(1996)	ISO 9001	英国	認証取得1220組織	質問紙調査	収益改善につながる
Lee(1998)	ISO 9001	香港	製造業、サービス業、建設業計235組織	質問紙調査	認証そのものからはあまり利益は得られない
Beattie & Sohal(1999)	ISO 9001	オーストラリア	認証取得50組織	事例調査	取引先との関係向上、マーケットシェアの拡大に寄与する
Miles *et al.* (1999)	ISO 14001	－	－	理論研究	コスト削減、市場への参入、などのメリットがもたらされる
Gavin(2000)	ISO 9001	－	－	理論研究	ビジネスパフォーマンスへの影響は実証されていない
Lima *et al.* (2000)	ISO 9001	ブラジル	認証取得129組織	質問紙調査	認証企業と非認証企業との間で違いは見られない
Heras *et al.* (2002)	ISO 9001	スペイン	ARDANデータベースに掲載されている認証取得、未取得各々400組織	既存データベースにある財務情報の二次分析	ISO認証により、パフォーマンスを上げているとはいえない
Tsekouras *et al.* (2002)	ISO 9001	ギリシャ	製造業およびサービス業の認証取得143組織	既存データベースにある財務情報の二次分析	長期的に有効であるが、短期的な財務パフォーマンスには影響を及ぼさない
Chow-Chua *et al*.(2003)	ISO 9001	シンガポール	シンガポール証券取引所上場146組織	質問紙調査	財務パフォーマンスの向上に寄与する
Seddon(2005)	ISO 9001	－	－	理論研究	認証が売り上げ増加などに影響を及ぼす明らかな証拠がない
Sharma(2005)	ISO 9001	シンガポール	SGXまたはSESDAQ上場企業のうち、一定の条件を満たす認証取得企業	既存データベースにある財務情報の二次分析	認証は財務パフォーマンスの向上につながる
島 ほか(2007)	ISO 9001	日本	日本適合性認定協会のウェブサイトに公開されている認定企業のうち、認証取得前後3年間の財務データが取得可能な74組織	既存データベースにある財務情報の二次分析	一時的な売上高の増加はあるものの、長期的には、競争力の獲得には至っていない
Piner & Ozgur(2007)	ISO 9001	トルコ	イスタンブール証券取引所に上場している認証取得103組織、未取得117組織	既存データベースにある財務情報の二次分析	認証取得企業は、非認証企業よりもリターンが高く、ばらつき（リスク）も小さい
Han *et al.* (2007)	ISO 9001	米国	製造業の認証取得441組織	質問紙調査	TQM活動共に組織の競争力を向上させ、結果としてパフォーマンスの向上に繋がる
Dick *et al.* (2008)	ISO 9001	スペイン	ARDANデータベースに掲載されている認証取得、未取得各々400組織	既存データベースにある財務情報の二次分析	認証取得とパフォーマンスに因果関係はない
山田・玉田 (2009)	ISO 9001	日本	認証取得50組織	既存データベースにある財務情報の二次分析	認証取得年度から次年度、次年度からさらによく年度にかけて好影響を与える
Nishitani(2009)	ISO 14001	日本	東証一部上場の製造業433組織	既存データベースにある財務情報の二次分析	財務パフォーマンスにプラスの影響を与える
Park *et al.* (2010)	ISO 27001	韓国	認証取得34組織	質問紙調査	広告効果、企業価値の向上、信頼性の向上につながる
Huang *et al.* (2011)	ISO 9001	米国	電機、化学工業445組織	質問紙調査	将来的な成長につながる

表 2-2　認証取得のオペレーション上の効果についての関連研究（1/2）

文献	対象規格	調査概要			結論
		対象地域	調査対象	調査方法	
Mann & Kehoe(1994)	ISO 9001	英国	製造業142組織	質問紙調査 インタビュー調査	TQMの仕組みを通じて方針の浸透をもたらし，顧客から支持されるようになる
引田ほか（1995）	ISO 9001	日本	認証取得157組織	質問紙調査	標準化の促進，権限／責任の明確化，スムーズな取引欠陥率の改善に寄与する
Rao et al.(1997)	ISO 9001	米国，インド，中国，メキシコ	製造業，加工業，サービス業，その他計649組織 認証取得93組織，取得計画中289組織，	質問紙調査	認証取得組織はリーダシップ，情報分析力，人材開発，品質保証，供給者との関係など8つの視点で高い効果をもたらす
Jones *et al.*(1997)	ISO 9001	オーストラリア	認証取得272組織	質問紙調査	単に認証取得することを目的とした企業は，わずかな効果しか得られない．また，長い期間マネジメントシステムを回している企業と導入して間も無い企業との間では，有意な効果の差はみられない
Mcadam & Mckeown(1999)	ISO 9001	北アイルランド	100名以下の中小企業108組織	質問紙調査	小企業であっても導入により，効果を期待することができる
Douglas *et al.*(1999)	ISO 9001	英国	地方自治体2組織	インタビュー調査	ISO取得を目的としている企業は，利益，不利益を共に得ることがなく，各種改善を目的としている企業は，意図した効果を得ることが出来る
Sun(2000)	ISO 9001	ノルウェー	ノルウェー品質協会所属363組織	質問紙調査	不良品やクレームを減らすことに寄与する
Acharya & Ray(2000)	ISO 9001	インド	BVQI，RWTUV，IRQS，BIS，LRQA，DNVを審査機関とする認証取得組織（件数不明）	質問紙調査	認証取得により，手順や活動，責任と権限，組織全体の連携に効果をもたらす
Calisir *et al.*(2001)	ISO 9001	トルコ	認証取得73組織	質問紙調査	製品やサービスの品質改善や，エラーや欠点率の削減に寄与する
Singels *et al.*(2001)	ISO 9001	オランダ	50～650名規模の192組織	質問紙調査	認証取得によりパフォーマンスの向上に寄与するとは言い切れない（有意な結果が得られない）
Gotzamani &.Tsiotras(2001)	ISO 9001	ギリシャ	ELOT認定により認証取得している84組織	質問紙調査	中小企業では認証取得することに満足する傾向がみられ，パフォーマンスの向上も十分にはみられない
Dissanayaka *et al.*(2001)	ISO 9001	香港	建設業33組織	質問紙調査	文書管理の向上，内部コミュニケーションの改善，競争力の向上が認められる．一方，書類作業，管理に要する時間，プロジェクトコストが増すといった負の側面もみられる
Casadesús *et al.*(2001)	ISO 9001	スペイン	カタルーニャおよびバスク地方の認証取得502組織	質問紙調査	業務への満足度の向上や，管理職と従業者とのコミュニケーションの改善などの効果が得られる
Delmas(2002)	ISO 14001	欧州，米国	欧州での認証取得140組織，米国での認証取得55組織	質問紙調査	パフォーマンスの改善に直接的には結びつかない
Quazi *et al.*(2002)	ISO 9001	シンガポール	認証取得，未取得合わせて93組織	質問紙調査	リーダーシップ，品質保証，サプライヤーとの関係，顧客志向など8つの項目において，認証取得による効果があるとは認められない
Clare, Mark & Tan(2003)	ISO 9001	シンガポール	シンガポール証券取引所上場企業146組織	質問紙調査	効果は有意には認められない
Martinez-Lorente & Martinez-Costa(2004)	ISO 9001	スペイン	大企業442組織	質問紙調査	TQMはオペレーションにプラスの関係があるが，ISO 9001認証取得は関係があるとは言えない
喜屋武(2005)	ISO 14001	日本	中小企業の事例 1 組織	事例調査	環境負荷を低減し効果的である

表 2-2　認証取得のオペレーション上の効果についての関連研究（2/2）

文献	対象規格	調査概要			結論
		対象地域	調査対象	調査方法	
Arimura *et al.*(2007)	ISO 14001	日本	環境省のデータベースに登録された従業員数50名以上の1499組織	質問紙調査	環境保護に効果をもたらす
Lo & Chang(2007)	ISO 9001	台湾	品質管理の専門家に対するインタビュー5名ならびに認証取得企業への質問紙調査171組織	質問紙調査 インタビュー調査	認証を維持している企業は，維持できていない企業よりも効果が得られている
Feng, Terziovski & Samson(2008)	ISO 9001	オーストラリア，ニュージーランド	製造業及びサービス業の認証取得613組織	質問紙調査	コスト削減，生産性，品質改善、顧客満足度の向上，内部手続き，従業員のモラルの面において，高い改善効果をもたらす
Lin & Jang(2008)	ISO 9001	台湾	認証取得441組織	質問紙調査	経営者の関与，品質計画，従業員の巻き込み，継続的改善につながる
Kuo et al.(2009)	ISO 9001	不明	認証取得305組織	質問紙調査	品質管理活動に重大な影響を持ち，小さな部門の方が大きな部門よりも大きな効果がある．また，認証取得は品質のレベル向上にも大きな効果をもたらす
Matuszak-Flejszman(2009)	ISO 14001	ポーランド	認証取得202組織	質問紙調査	水の使用量，騒音，放射線などの削減に効果がある
Nair & Prajogo(2009)	ISO 9001	オーストラリア，ニュージーランド	認証取得328組織	質問紙調査	ISO 9000の浸透は，オペレーションのパフォーマンスと関係がある
Turk(2009)	ISO 14001	トルコ	建設業の認証取得28組織，未取得40組織	質問紙調査	環境に悪影響を及ぼす要素の削減や，環境面における持続可能性の向上などに寄与する
Tang & Lee(2009)	ISO 9001	台湾	従業員数，資産，設立年度の観点から各々均等になるように抽出された30組織	インタビュー調査	従業員数，資本金が多い企業ほど，ISO 9001認証取得による満足度が高く，すべて少ない程，満足度が低い傾向にある
岩田ほか(2010)	ISO 14001	日本	PRTR，JAB，環境マネジメントに関するOECD事業所調査，帝国データバンクからデータを抽出して組み合わせた216組織	トルエン排出量に対するデータ分析	トルエン排出削減に効果を発揮している
Aravind & Christmann(2011)	ISO 14001	米国	認証取得，未取得各々72組織	質問紙調査	EMSが有効に機能している企業では，認証取得企業と未取得企業とでパフォーマンスに優位な差がみられる

オペレーション上の効果の観点における関連研究では，認証取得が目的となった場合に，認証取得組織が意図した効果を発揮することができるのかについても分析されている．そこで，組織はなぜ ISO マネジメントシステム規格認証を取得するのかに関する研究を紹介する．

ISO マネジメントシステム規格認証の普及の要因として舛本・角南（2004）は，ISO 14001 認証の観点から，認証取得が取引先からの要求や他社に対する競争優位となっていることに加え，認証取得が入札要件とされる業界が存在することを指摘している．Shannon *et al.*（1999）は，ISO 9001 認証の観点から，政府，顧客からの要求に従って認証取得する傾向があることを指摘している．また Lee & Palmer（1999）は，ISO 9001 認証の観点から，小規模の組織は内的よりも外的要因により認証取得をする傾向があることを指摘している．Delmas & Toffel（2008）は，市場を構成するものから圧力を受けた場合，ISO 14001 認証を取得しやすい傾向にあるとしている．以上より ISO マネジメントシステム規格の認証の普及は，取引先や競合等の圧力が発生している．

取引先や競合等の圧力による普及については，Meyer & Rowan（1977）が提唱する新制度派組織論により説明することができる．佐藤（2005）によると新制度派組織論は，「なぜ，組織は互いによく似ているのか」，「なぜ特定の組織構造や慣行，あるいは戦略が普及しているのか」の問いに対して，「組織が組み込まれている環境において働いている制度的プレッシャーの影響を強く受けているから」との答えを提供するものとされている．新制度派組織論の理論的枠組みでは，「なぜ組織は驚くほど似ているのか」を問題意識とし，同型のメカニズムを競争的同型化と制度的同型化に分類したうえで，制度的同型化が，強制的同型化，模倣的同型化，規範的同型化の 3 種類に分類できるとしている（DiMaggio & Powel, 1983；安田・高橋，2007）．佐藤・山田（2004）や佐藤（2005）によると ISO マネジメントシステム規格認証の普及は，新制度派組織論を用いて説明できるとしている．新制度派組織論を用いた ISO マネジメントシステム規格認証の普及のメカニズムについて，三木（2008a）は，制度的圧力と自律的な組織実践が相互に影響し合い，自律的な組織実践によって生成された制度的圧力は，時とともに変容し規格普及に影響を与えるとしている．また三木（2008b）は，ISO 14001 認証の普及のメカニズムとして，取得したタテマエの理由とホンネの理由の乖離が発生する「取得目的の乖離」，および制度的圧力が組織による認証取得行動を促す一方で，組織による取得行動が新たな制度的圧力の源泉となり，新しい制度的な圧力のもとでさらに取得が進むことをあらわす「制度的圧力の動態的相互作用」が

働くことに言及している．このほか，新制度派組織論の理論的枠組みにおいては，政治的圧力や社会的圧力，機能的圧力が要因となって自堕落または拒否感を生み出し，非制度化（deinstitutionalization）が生み出される（Oliver, 1992）とした研究もある．

認証取得が目的となった場合の組織の行動については, Yoshida(1989)や Yoshida(1995)により説明することができる．Yoshida（1989）や Yoshida（1995）は，目標を達成しようとする際，合格点志向（Acceptability）と究極点志向（Desirability）の 2 つの志向があることを定義した上で，一度目標が設定されると，努力をして究極点に向かおうとする傾向よりも，単に達成すること目的とするようになるとしている．Seddon（2000）は，Yoshida の理論を ISO 9001 認証に応用し，認証制度が抱える問題として，認証取得が目的となった組織は，要求事項に記載された項目のみを満たそうとする動きがあることを指摘している．

単に認証取得が目的となった組織が，認証取得により目的とした効果を発揮できるのかに着目すると，単に認証取得することを目的とした組織は，わずかな効果しか得られない（Jones *et al.,* 1997），ISO 取得を目的としている組織は，利益，不利益を共に得ることがなく，各種改善を目的としている組織は，意図した効果を得ることができる（Douglas *et al.,* 1999），中小企業では ISO 9001 を認証取得することに満足する傾向がみられ，パフォーマンスの向上に寄与しない（Gotzamani & Tsiotras, 2001），顧客からの要求などによって認証取得した場合，認証後に売上や利益が向上するといった決定的な証拠がない（Dick *et al.,* 2008），ISO 9001 を認証取得してもうまくいかない原因と一つとして大企業からの圧力により，単に認証取得すればよいとする動きがあることが挙げられる（Kumar & Balakrishnan, 2011）など，いずれも効果を発揮できないとした結論が出されている．

2.3.2. ISMS の有効活用に関する研究

本項では ISMS における PDCA サイクルをどのように整備または運用すればよいかについての研究を紹介する．PDCA サイクルの Plan（計画）は，情報セキュリティにおけるリスクおよび機会を決定し，管理策の決定を含むリスクへの対応をおこなうフェーズである. また情報セキュリティ目的およびそれを達成するための計画策定についてもおこなう. Plan フェーズは，リスクおよび機会を決定し，情報セキュリティリスクに対するアセスメントを実施したうえで，具体的な管理策を講じることに関する項目が要求されている．情報セキュリティリスクアセスメントおよび管理策の決定については 2.4 節で述べる．この

ため本節では PDCA サイクルのうち Do（実行），Check（評価）および Act（改善）に関する関連研究を紹介する．

組織は情報セキュリティリスクを抑制するための管理策を決定した後，組織構成員に遵守させるなどにより組織に適用する必要がある．この活動が Do（実行）に該当する．組織構成員に遵守させるための施策としては，策定した管理策を周知および徹底するための教育・動機付けなどがある．教育・動機付けについては，情報セキュリティについて先進的な自治体を取り上げ，民間企業との比較考察をおこなった上で，内発的な倫理綱領の作成に始まり，具体性をもって浸透させる仕組みの構築と制度改革を実行・維持できる人材の確保が必要と結論づけている研究（吉田・島田，2009）や e ラーニングに実践的な擬似攻撃システムを導入することで，従来に比べて脆弱性の理解などが高まることを確認した研究（竹下ほか，2010）が，セキュリティ・コミュニケーションの観点からは，セキュリティ・コミュニケーションを活性化させる推進策として，対面によるコミュニケーションに加え，ICT を活用することを考慮している研究（井戸田，2005）がある．

適用する管理策に対しては, その内容が, 組織が設定する基準に対して適合しているか, または有効かを評価する必要がある．この活動が Check（評価）に該当する．評価の手法は，組織による自己点検や内部監査，組織外の審査機関からの審査などがある．監査または審査に対する関連研究として川中・六川（2012）は，クラウド事業者とクラウド利用者の間の情報の非対称性に着目し，両者の関係をゲーム理論により考察を行い，クラウドサービス市場が健全に発展していくための情報セキュリティ監査が果たすべき役割について言及している．Satoh & Kumamoto（2009）は，インシデントのシナリオ発生を量的にリスク評価し, 情報セキュリティ監査におけるリスクの確率を評価している, Delmas(2001) は ISO 14001 規格の観点から，監査は環境パフォーマンスに対して量的情報は提供しないと結論づけている．有賀（2008）は，故意的ミスやモラル違反の不適合・不適切な業務は通常の内部監査や外部監査は無力であることについて言及している. 美濃ほか (2010) は, ISO 14001 規格に関する研究は多くあるが，審査機関に関する研究はほとんど見ることがなく，審査機関の抱える現状や課題などについて論じた研究論文はないとした上で，主流になりつつある有効性審査の定義と手法を紹介している．

組織は，評価をおこなった結果，内容に不備がある場合，または改善が望ましいと考えられる事項が発生した場合に対する是正をおこなう必要がある．この活動が Act（改善）に該当する．不備の内容や改善が望ましいと考えられる事項は，検出された個々の事象に

より異なるが，どのような是正処置を実施すべきかについては，他社の対応状況や類似のインシデント事例を参考にすることができる．他社の対応状況に関する関連研究は，個人情報保護法への対応状況に関する調査（経済産業省，2012），日本企業における情報セキュリティに対する取り組み状況に関する調査（NRI セキュアテクノロジーズ，2011），人的脅威のうち特に問題である内部犯行について，類型化などにより事案発生過程およびその原因を把握し，対策を検討している調査（社会安全研究財団，2010b），インターネット利用者を対象に，個人の PC ユーザが情報セキュリティ関連の脅威に対する意識をどの程度深めているのか，またどの程度対策を進めているのかに関する調査（情報処理推進機構，2012）などがある．インシデント事例に関する関連研究は，日本におけるネットワークに関するコンピュータセキュリティインシデントの届出状況，その対応の状況，および関連する対策に関する調査（情報処理振興事業協会，2000），インシデントの発生状況およびその傾向の調査（日本ネットワークセキュリティ協会，2006；2007；2008；2009；2010；2011a；2011b；2014a；2014b；2015；2016a；2016b；2017；2018；2019），各組織に対する情報セキュリティ対策の現状，コンピュータウィルスによる被害状況，サイバー攻撃の有無，被害により生じた直接的損失，内部者の不正による被害状況の調査（情報処理推進機構，2012）などがある．そのほか事例を分析した関連研究としては，インシデントの原因であるヒューマンエラーを左右するのは末端ユーザであるとして，調査を実施し，本人認証技術と性格特性に関係があると結論づけている研究（加藤ほか，2011）や，個人情報インシデントの地域特性に関する分析をおこなっている研究（文倉ほか，2011），インシデントと管理策の実施に関する因果関係を分析した研究（川中・六川，2011）などがある．

2.4. インシデント抑制のための管理策に関する研究

本節ではインシデントを抑制するための管理策に関する研究を紹介する．管理策を決定するには，情報セキュリティに関して，どのようなリスクがあるかを特定し，分析し，評価する．これらを通じて対応を要するリスクを決定する必要がある．また決定されたリスクに対しては，どのような管理策を講じるかを決定する必要がある．

2.4.1. 管理策を講じるべきリスクの決定手法に関する研究

本項では管理策を講じるための基礎となる，リスクの決定手法に関する研究を紹介する．

講じるべき管理策を検討するためには，インシデント発生によるリスクを特定し，リスク分析し, リスク評価するプロセスを通じて, 対応を要するリスクを特定する必要がある．情報セキュリティに関するリスクの特定，リスク分析およびリスク評価のプロセス全体を情報セキュリティリスクアセスメントという（ISO, 2014a）．

情報セキュリティリスクアセスメントは，ISO/IEC 27005（ISO, 2018）によりリスクの特定，リスク分析およびリスク評価の手法についての国際標準化がなされている．そのほか情報セキュリティリスクアセスメントの手法についての関連研究は，プロセスの段階ごとに，起こり得る事故の原因をリストアップしてリスクを発見していくプロセスチェックによるリスク検出法（経済産業省，2004）や，近々に何をすべきかを，その行動の結果起こることを推定し, それらを考慮しながら決定する, シナリオアプローチ（松岡ほか, 2001）がある．

プロセスチェックによるリスク検出法の関連研究は，二次元の資産分類とビジネスプロセスに基づき量的評価をおこなう手法（Eom *et al.,* 2005）や，自己統制評価により，業務プロセス上にどのようなリスクがあるかを把握する手法（土井・内田，2008）が提案されている．

シナリオアプローチによる関連研究は，各情報と情報を結ぶ空間グラフとして定義し，その上で脅威の発生に関する確率モデルの提案（渥美・浅原，2005），UML グラフィカルモデリングを使用した分析手法（Li *et al.,* 2006；Bahtit & Regragui, 2013），Analytic Hierarchy Process とファジィ理論の組み合わせた分析手法（Zhao *et al.,* 2007），Fault Tree Analysis および Event Tree Analysis を使用した分析手法（Satoh & Kumamoto, 2009），ベイジアンネットワークを使用した分析手法（Rahmad *et al.,* 2007），ファジィ理論を使用した分析手法（Shameli-Sendi *et al.,* 2012）などが提案されている．

プロセスチェックによるリスク検出法やシナリオアプローチのほか，リスク分析ツールを使用した分析手法（Chung *et al.,* 2006；村上・内田，2010），ISO/IEC 17799 の管理項目に記載された記述をもとに管理策を構造化し，リスクの発生前，中，後に分類した上で，管理策の選択基準を提示する手法（高橋ほか，2007），管理策ごとに管理策が効いていない場合の脅威と脆弱性を定義し，影響の大きさと発生の可能性からリスク値を算出する手法（Atyam, 2010）など，様々な切り口から情報セキュリティリスクアセスメントの手法が提案されている．

2.4.2. 管理策の決定に関する研究

本項では 2.4.1 項にて紹介する情報セキュリティリスクアセスメント手法を用いて検出されたリスクに対し，どのような管理策を講じるべきかの決定に関する研究について紹介する．

情報セキュリティリスクアセスメントを通じて対応を要すると判断されたリスクに対しては，管理策を決定し，組織に導入する必要がある．リスク対応の要否，ならびに組織にとって最適な管理策の選定については，管理策実施に要する投資の妥当性の評価に基づく研究が中心に行われている．Gordon & Loeb（2002）は，情報セキュリティ管理策への投資額に対する純利益を最大化するため，投資に対し得られる利益と投資額を用いて定式化をおこなっている．Gordon *et al.*（2003）は，Gordon & Loeb（2002） の式を拡張し，組織の情報セキュリティ投資とセキュリティ情報の共有がコストに与える影響を評価している．また田村ほか（2009）は，Gordon *et al.*（2003）のモデルが 2 企業系であることを指摘し，企業数を一般化したn 企業系への適用可能性を分析している．Gordon & Loeb（2002），Gordon *et al.* （2003），田村ほか（2009）の研究は，管理策実施に要する投資の妥当性を評価する観点では有用であるが，複数ある管理策の候補から最適な管理策および管理策の組み合わせを選定することはできない．数ある管理策の候補から合理的に管理策を選定する手法として，必要最小限の管理策選定（永井ほか，2000）や，採用すべき管理策案の組み合わせを明確化した研究（佐々木ほか，2004）がある．永田ほか（2000）は，Fault Tree を作成したうえで，ミニマルパスセット探索アルゴリズムを適用することで，必要最小となる対策目的補集合群を特定し，特定された対策目的補集合群に対する必要コストを最小化する最適な管理策を決定する手法を提案している．また佐々木ほか（2004）は，不正コピー対策の観点から Fault Tree を作成し，ミニマルパスセット探索アルゴリズムを適用することで，必要最小となる対策目的補集合群を特定し，管理策を実施した際の不正攻撃の発生確率低減を考慮することで，リスクに対抗する適用効率が最も高い対策を選定する手法を提案している．これに対して中村ほか（2004）は，永田ほか（2000）や佐々木ほか（2004）の提案について『組織のセキュリティマネジメントおよび複数のサービスを提供する統合システムにおける一般的な設計手順の中で Fault Tree を作ることは通常おこなっておらず（または，複雑になりすぎて Fault Tree を作成することができない），実用性に問題があるといえる』と指摘する．中村ほか（2004）は，資産と脅威の関係ならびに管理策と脅威の関係をモデル化した上で，情報の残存資産という概念を導入し，選択さ

れた対策の組み合わせごとに管理策実施コスト”C”と平均残存資産”RA”を算出し，”$RA-C$”の期待値を最小化する管理策選定問題を定式化する手法を提案している．このほか，中村ほか（2004）の主張を拡張した関連研究としては，利便性低下コストと仕事量に注目した管理策選定手法（芝口ほか，2010）や要員数や開発期間，仕事の繁閑を考慮に入れた管理策選定手法（呉ほか，2013）が提案されている．以上のように，情報セキュリティ管理策の選定は，脅威発生時の損害額とコストと管理策実行にかかるバランスにより，最適な管理策または管理策の組み合わせを選定する研究が中心となっている．これらの関連研究で提案されている手法は，損害額が特定できることを前提とした手法であるため，損害賠償額のほか，発生原因，経路，被害範囲などの原因究明にかかる工数，対策検討コスト（担当弁護士などとの関係者との調整含む），ブランド価値が低下することにコスト，クレーム対応にかかる工数，各種対応により発生する機会損失が発生するなど，損害額の予測が難しい事例に対して適用することは困難である．

損害額が予測しづらい事例の場合は，発生した場合の影響が大きく，かつ発生しやすいインシデントを特定し，その発生原因を解明したうえで，発生原因の除去につながる管理策を検討することが実務上有用である．情報セキュリティ実現のための管理策は，ウェブサイトの構築の観点（情報処理推進機構，2012），内部不正を防止する観点（情報処理推進機構，2013），ヒューマンエラーを防ぐ観点（システム監査学会，2007），情報全般に対する管理策の観点（ISO, 2013）などにおいて具体例が示されている．

管理策の決定にあたっては，より効果的な管理策を導入するための具体的な施策についても研究がおこなわれている．物理的なアクセス制御の観点からは，制服を着用した悪意を持った者を迅速に検出するためのシステムを提案している研究（藤川ほか，2007）がある．本人認証の観点からはタッチスクリーンによる認証技術を提案，検証している研究（野口ほか，2013）などがある．またネットワークを介した不正アクセスの観点からは，踏み台攻撃を検出する手法を提案している研究（竹尾ほか，2007），ソフトウェアや装置のぜい弱性を対象としたデータベース JVN（JP Vendor status Notes）を提案している研究（寺田ほか，2005），ワームの流布対策を提案している研究（寺田ほか，2004），不正アクセスやデータの盗聴，改ざんを防止するため，自律分散制御される路側網システムのセキュリティ要件と実現要件を評価している研究（福澤ほか，2003），膨大な IDS ログからの不正アクセス抽出作業を支援する通報・検索システムを構築している研究（沢田ほか，2003），各部署の不正アクセス対策活動の支援ならびに，部署間にまたがった情報交換の場を提供す

るために構築した不正アクセス対策情報サービスシステムの有効性について検証している研究（寺田ほか，2000）などがある．

2.5. 不正に情報を持ち出す行為に関する研究

本節では不正な情報持ち出し行為を抑制するためのメカニズムに関する研究を紹介する．本論文における「不正に情報を持ち出す行為」とは，組織構成員が，必要な許可を得ないまま，業務で利用する情報を，私物の PC や外付記憶媒体，自宅の引き出しなど，組織が管理できる範囲外に持ち出す行為をいう．

情報処理推進機構（2012）は，内部不正の分析に関係すると考えられる犯罪心理学や環境犯罪学の理論として，不正のトライアングル理論，ルーティンアクティビティ理論，状況的犯罪予防論の 3 つがあるとしている．

不正のトライアングル理論（Fraud Triangle Theory）（Cressey, 1971）は，不正が行われる際,「動機」,「正当化」,「機会」の 3 つの要素がそろったときに発生するとした理論である．不正のトライアングル理論を用いた研究として北野（2015）は，動機を脅威，機会をぜい弱性と読みかえ，正当化の代わりに価値を用いた「古くて新しい不正のトライアングル」を提唱し，内部不正行為の抑制策を検討している．岡野・奥山（2017）は，不正のトライアングル理論における 3 要素それぞれに対して情報持ち出しに関する仮説を設定し，持ち出し経験の有無による組織構成員の意識を比較し，有意な差がみられるかについて分析している．

ルーティンアクティビティ理論[2]（Routine Activity Theory）（Cohen & Felson, 1979）は,「犯罪企図者」,「犯罪のターゲット」,「監視者の不在」の 3 つの要素がそろったときに犯罪が発生するとした理論である. これらを防ぐため, 犯罪企図者に対しては「行動規制者」, 犯罪のターゲットに対しては「管理」, 監視者の不在に対しては「監視者」が必要とされる. 情報処理推進機構（2012）は，ルーティンアクティビティ理論に於ける 3 つの要素をもとに，組織構成員による情報セキュリティ上の内部犯行を防ぐための施策を提案している．

ルーティンアクティビティ理論では，犯罪企図者の意図や目的に対して外部からのコントロールが困難な場合があるとの指摘がある（情報処理推進機構，2012）. 外部からのコン

[2]文献により「日常活動理論」とよぶこともある．

トロールを可能な「環境」を適切に定めることを主眼として犯罪機会の低減，予防する理論としては，状況的犯罪予防論（Situational Crime Prevention）（Cornish & Clarke, 2003）の考え方がある．状況的犯罪予防論とは「状況が弱い人間を犯罪企図者にしてしまう」側面を重視した理論である（甘利，2015）． 社会安全研究財団（2010a）は，犯罪を予防するための施策を 5 つのカテゴリに分け，さらに各カテゴリを 5 項目ずつに分類した計 25 の技法と IT セキュリティ対策の例を提案している．甘利ほか（2012）は社会安全研究財団（2010a）が提案する対策の例を応用し，職業ライフサイクルや組織論的観点からの内部不正やミス抑制の手法を提案している．

内部不正を含む不正な情報持ち出しのメカニズムに関する理論としては，上記のほかに計画的行動理論（Theory of Planned Behavior）が知られている．計画的行動理論は，合理的行動理論（Theory of Reasoned Action）を再構築した理論である．合理的行動理論（Fishbein & Ajzen, 1975；Ajzen & Fishbein, 1980）とは，相関関係にある態度と主観的規範が行動意図に影響し，行動意図が行動に影響することを体系化した理論である．これに対し計画的行動理論（Ajzen, 1985；Ajzen & Madden, 1986；Ajzen, 1991）は，合理的行動理論に統制可能性の因子を追加し，再構築した理論である．計画的行動理論の応用研究として小池ほか（2003）は，環境問題の観点から計画的行動理論に知識の因子を追加したモデルを構築し，因果関係の構造をあきらかにしている．また諏訪ほか（2012）は小池ほか（2003）のモデルを情報セキュリティ分野に応用し，因果関係の構造を分析している．Khan *et al.*（2011） は情報セキュリティに対する理解から行動に至るまでの 5 段階に分類した測定モデルを構築したうえで，情報セキュリティ意識を向上させるための手段を提案している．AL-Omari *et al.*（2012）は，計画的行動理論に情報セキュリティの理解と技術的セキュリティの理解の因子を追加したモデルを構築し，情報セキュリティポリシーへの準拠意図に対する因果関係の構造をあきらかにしている．また Cohen *et al.*（2010）は，不正行為を抑制するための理論として FT/TPB（Fraud Triangle/Theory of Planned Behavior applied to fraud）を提唱している．FT/TPB とは計画的行動理論を用いて不正のトライアングルの 1 つである正当化を説明する考え方をいい，複数の理論を組み合わせた試みがなされている．

行動意図におよぼす影響については防護動機理論（Protection Motivation Theory）（Rogers, 1975）による分析もおこなわれている．防護動機理論は，リスクを回避または軽減する行動を分析するための心理モデルである．防護動機理論を応用した研究としては，

情報システム利用にあたっての情報セキュリティ維持（Yoon *et al.*, 2012），クラウド提供者によるクラウド連携採用（Haile & Altmann, 2015），公的機関における情報セキュリティの維持（Kolosenia *et al.*, 2018），BYOD（Bring-Your-Own-Device）プログラムの参加（Weeger *et al.*, 2018）などの観点から行動意図におよぼす影響が分析されている．

そのほか行動意図におよぼす影響に関する理論としては，技術受容モデル（Technology Acceptance Model）（Davis,1986；Davis *et al.*, 1989）がある．技術受容モデルは，システム利用に至る要因の因果関係をモデル化したものである．技術受容モデルを応用した研究としては，PC 利用者における IT の脅威を回避する行動（Liang & Xue, 2010），オンラインバンキングの採用意図（Yaghoubi & Bahmani, 2010），電子税務申告システムの利用意図（Chu & Wu, 2005）などにおいて，因果関係の構造をモデル化し，共分散構造分析の手法を用いて影響が分析されている．そのほか関連研究では，計画的行動理論，技術受容モデル, 防護動機理論などの各種理論を融合したモデルを構築し，その影響を分析している（例えば Ifinedo, 2012；Sun *et al.*, 2013；Chen *et al.*, 2017）．

行動意図におよぼす影響のほか不正に情報を持ち出す行為に対しては，行動を引き起こす要因の抽出（菅野・島田，2010；竹村ほか，2015），教育を含む対策の適用時期の提案（甘利ほか，2012）がおこなわれている．ほかにも組織風土（濱田・廣松，2012）の観点における影響が分析されている．また不正な情報持ち出し行為については職種による意識の違いについても確認されている．島（2012）は，不正に情報を持ち出す行為に関するシナリオを用意し，シナリオに対する共感度について技術，営業，そのほかの各職種で比較をおこなっている．分析の結果，島（2012）は，与えられたシナリオの逸脱行動を許容するか否かの共感度は職種により異なることを確認している．

2.6. 本論文にて解決すべき課題

本節では 2.3 節から 2.5 節にて紹介する関連研究に基づき，本論文の土台となる解決すべき課題を設定する．

2.3.1 項では ISO 9001 認証や ISO 14001 認証を中心とした認証取得の効果について紹介している（Mann & Kehoe, 1994；引田ほか，1995；Rao *et al.*,1997；Jones *et al.*, 1997；Mcadam & Mckeown, 1999；Douglas *et al.*, 1999；Sun, 2000；Acharya & Ray, 2000；Calisir *et al.*, 2001；Singels *et al.*, 2001；Gotzamani &.Tsiotras, 2001；Dissanayaka *et al.*, 2001；

Casadesús *et al.*, 2001；Delmas, 2002；Quazi *et al.*, 2002；Clare *et al.*, 2003；Martinez-Lorente & Martinez-Costa, 2004；喜屋武，2005；Arimura *et al.*, 2007；Lo & Chang, 2007；Feng *et al.*, 2008；Lin & Jang, 2008；Kuo *et al.*,2009；Matuszak-Flejszman, 2009；Nair & Prajogo, 2009；Turk, 2009；Tang & Lee, 2009；岩田ほか，2010；Aravind & Christmann, 2011）．本論文が対象としているオペレーション上の効果に着目すると，認証取得の効果の関連研究は，質問紙調査やインタビューなど，整備または運用者の認識に基づく調査結果を分析したものが中心となっている．客観的な事実に基づく分析結果は岩田ほか（2010）によるトルエン排出量に対するデータ分析などに限定されている．本論文の問題意識である「Ⅰ．ISO/IEC 27001 を認証取得しさえすれば，情報セキュリティに関連するインシデントを抑制できるのだろうか.」を解決するには，インシデント事例を用いて認証取得組織と未取得組織の発生状況を比較し，分析する必要がある．比較分析にあたっては，客観的に入手可能なインシデント事例を用いる必要があるため，本論文では日本ネットワークセキュリティ協会が発表する個人情報の漏えいや紛失に関するインシデント事例（日本ネットワークセキュリティ協会，2009；2010；2011）を用いる．本論文では以下を解決すべき課題①として設定する．これにより認証取得組織という ISO/IEC 27001 規格に準拠している組織におけるインシデント抑制に対しての問題点を明らかにすることができ，実務面における有用な示唆を得ることができると考える．課題①は第 3 章にて取り扱う．

解決すべき課題①：個人情報の漏えいや紛失に関するインシデント事例を用いて ISO/IEC 27001 認証によるインシデント抑制効果を検証する．また ISO/IEC 27001 規格に準拠している組織における，インシデントを抑制するうえでの問題点をあきらかにする．

第 3 章では課題①の解決を試み，ISO/IEC 27001 規格に準拠した ISMS を適切に整備し，運用できていれば，個人情報の漏えいや紛失に関するインシデントを抑制が抑制し得たことを確認している．これを受け，本論文におけるもう 1 つの問題意識である「Ⅱ．組織は ISO/IEC 27001 規格に準拠する際，どのような点に注意して施策を講じれば効果的にインシデントを抑制させることができるのだろうか.」については，組織構成員に対して規定した管理策を遵守させるための施策が必要と考える．第 4 章および第 5 章では組織構成員が管理策を遵守しない行為をあらわす「不正な情報持ち出し行為」に着目し，組織が

講じるべき施策を提案する．施策の提案にあたっては不正のトライアングル理論を採用する．不正のトライアングル理論における 3 つの要素のうち，「動機」の原因にはさまざまなものがあると考えられ，ISO/IEC 27001 規格への準拠のみによって抑制することは困難であり，本論文の範疇を超える．不正のトライアングル理論は 3 要素が揃わないことが重要である．このため第 4 章および第 5 章では「正当化」および「機会」の抑制のために講じるべき施策を提案する．本論文では組織構成員が必要な許可を得ないまま，業務で利用する情報を組織が管理できる範囲外に持ち出す行為を「不正な情報持ち出し行為」とよぶ．

2.3.2 項では ISO/IEC 27001 規格の要求事項に着目し，ISMS を有効に機能させるために PDCA サイクルそれぞれのフェーズにおける効果的な適用手法を紹介している（井戸田，2005；吉田・島田，2009；Satoh & Kumamoto, 2009；竹下ほか，2010；Delmas, 2001；美濃ほか，2010；加藤ほか，2011；文倉ほか，2011；川中・六川，2011）．しかし本論文の目的である ISO/IEC 27001 規格に準拠する際，どのような施策を講じるべきかを提案するためには，ISO/IEC 27001 規格における要求事項の観点から，不正な情報持ち出し行為を抑制する効果を実証する必要があると考える．不正な情報持ち出し行為の正当化を抑制する観点においては，FT/TPB が提唱されている（Cohen *et al.*, 2010）．計画的行動理論（Ajzen, 1985；Ajzen & Madden, 1986；Ajzen, 1991）に基づくと，不正をおこなおうとする意図が，不正な情報持ち出し行為を引き起こす要因とされている（Khan *et al.*, 2011；AL-Omari *et al.*, 2012，諏訪ほか，2012）．また不正をおこなおうとする意図に対しては，情報セキュリティ知識や，組織内外からの情報セキュリティに対する要請が影響するとされている（井川ほか，2009；濱田・廣松，2012；竹村ほか，2015）．しかし ISO/IEC 27001 規格を採用することの有用性をあきらかにするには，規格の要求事項の項目に着目した因子を定義し，不正な情報持ち出し意図におよぼす影響を実証する必要がある．このため以下を本論文で解決すべき課題②として設定する．課題②を解決することにより，不正な情報持ち出し行為の正当化を抑制するために ISO/IEC 27001 規格を採用する際，要求事項のどの項目に経営資源を重点的に投入すべきかがあきらかになる．これにより実務面において有用な示唆を得ることができると考える．課題②は第 4 章にて取り扱う．

解決すべき課題②：ISO/IEC 27001 規格の要求事項の観点から，不正な情報持ち出し意図の正当化を抑制する効果を実証し，組織が講じるべき施策を提案する．

不正のトライアングル理論における「機会」の抑制にあたっては，管理策をいかに有効に機能させるかが重要となる．2.4.1 項では，情報セキュリティリスクアセスメントの手法について様々な観点からのアプローチを紹介している（松岡ほか，2001；Eom *et al.*, 2005；渥美・浅原，2005；Chung *et al.*, 2006；Li *et al.*, 2006；Zhao *et al.*, 2007；高橋ほか，2007；Rahmad *et al.*, 2007；土井・内田，2008；Satoh & Kumamoto, 2009；Atyam, 2010；村上・内田，2010；Shameli-Sendi *et al.*, 2012；Bahtit & Regragui, 2013；ISO, 2014a；ISO, 2018）．情報セキュリティリスクアセスメント手法を用いて検出されたリスクに対しては，講じるべき管理策を決定し，組織に導入する必要がある．2.4.2 項では，リスク対応の要否や組織にとって最適な管理策の選定方法などについての関連研究を紹介している（永井ほか，2000；寺田ほか，2000；Gordon & Loeb, 2002；Gordon *et al.*, 2003；福澤ほか，2003；沢田ほか，2003；寺田ほか，2004；佐々木ほか，2004；中村ほか，2004；寺田ほか，2005；藤川ほか，2007；竹尾ほか，2007；田村ほか，2009；芝口ほか，2010；呉ほか，2013；野口ほか，2013）．

管理策は単に導入するのみでなく，組織構成員に対して遵守させる必要がある．組織構成員に対して管理策を自動的かつ強制的に遵守させるための活動としては，IT を用いた「自動化の整備」がある．しかし管理策を遵守させるためには自動化の整備のみでは限界があり，人的対策を含むマネジメントの面での活動も求められる（岡野・奥山，2017）．マネジメント面での活動には，管理策を文書化するための「マニュアルの整備」が必要である（竹村ほか，2015）．また組織構成員に対して管理策を遵守させるためには，必要な知識や教養を得させるため，または管理策の遵守を意識させるための活動である「教育・動機付けの実施」も必要となる．上述の関連研究に基づき，本論文では組織構成員に対して管理策の遵守を促すために組織が講じる活動として「教育・動機付けの実施」，「マニュアルの整備」，「自動化の整備」があるものとし，これらを総称して「促進活動」とよぶ．組織は促進活動を選択もしくは組み合わせることにより，組織構成員に適用している．組織にとって有限である経営資源を効果的かつ効率的に配分するには，促進活動が管理策の遵守に対してどの程度寄与しているかを把握することが有用である．本論文は以下を解決すべき課題③として設定する．課題③を解決することにより，組織は，効果的かつ効率的な経営資源の配分をおこなうことができるなど，実務面において有用な示唆を得ることができると考える．課題③は第 5 章にて取り扱う．

解決すべき課題③：促進活動の観点から不正な情報持ち出し行為の機会を抑制する効果をあきらかにし，組織が講じるべき施策を提案する．

本論文で設定する 3 つの解決すべき課題に対して，第 3 章では，インシデント事例を用いて ISO/IEC 27001 認証によるインシデント抑制効果を検証する．また認証取得を通じて規格に準拠している組織における，インシデントを抑制するうえでの問題点をあきらかにする．第 4 章では，不正のトライアングル理論における「正当化」の観点から，ISO/IEC 27001 規格の要求事項のうち「認識」という個別的観点において，どの認識を持たせれば不正な情報持ち出し行為を抑制できるのかを考察する．第 5 章では，不正のトライアングル理論における「機会」の観点から，教育・動機付けの実施，マニュアルの整備，自動化の整備のうち，どの促進活動に注力すれば不正な情報持ち出し行為を抑制することができるのかを考察する．

以上をまとめたものを図 2-2 に示す．

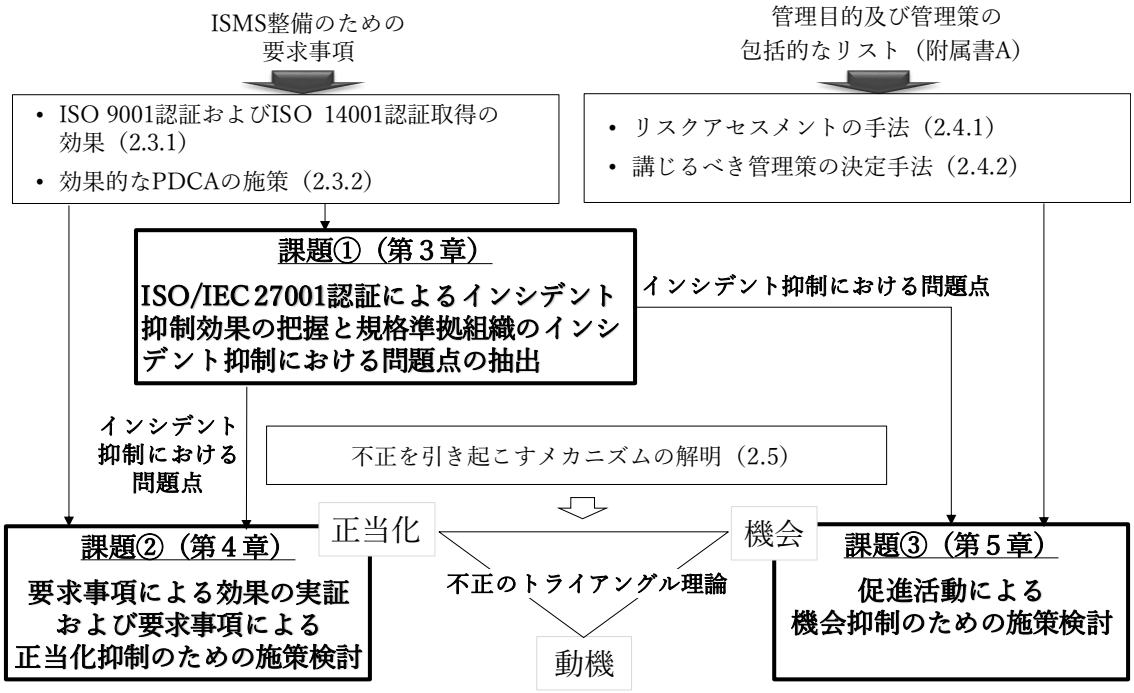

図 2-2　本論文で解決すべき課題

第 3 章　ISO/IEC 27001 認証有無による インシデント事例の比較分析

3.1. 背景と目的

ISO/IEC 27001 規格（ISO, 2005b[3]；ISO, 2013）は，情報資産を対象とした情報セキュリティに対する ISO マネジメントシステム規格認証に用いられる規格である. この ISO マネジメントシステム規格認証の制度では, 取り組み内容についてなどは開示されておらず, 取引先を選定するものにとっては，認証の有無しか判断する材料がない（岩田，2007）. 多くの官公庁や組織では，情報資産を取り扱う業務を委託する際，認証の有無がインシデントを抑制できている組織であるか否かの判断基準とされ，認証を有しないと入札資格すら与えられない場合がある.

認証取得によりインシデントの抑制を期待できるのかに着目すると, 経済産業省（2008）によれば，ISO 認証取得組織がインシデントを多発させていることを問題視している．すなわち認証が情報セキュリティに関するインシデントを抑制することを目的としているにもかかわらずインシデントの発生抑制に必ずしも寄与できていないことが示唆されている. 一方で, ISO/IEC 27001 規格の認定機関でもある日本情報処理開発協会（以下「JIPDEC」[4]という.）（2006）では,「委託先の候補者が ISMS 認証を取得しているか否かを委託先の選定における評価に利用することは, 極めて効果的かつ信頼性が高いといえる.」としており，認証取得をもってインシデントを抑制することができることを示唆している.

ISO/IEC 27001 認証を含む ISO マネジメントシステム規格認証の取得効果は，オペレーション上の効果とビジネス上の効果に二分できる（Beattie & Sohal, 1999；Feng *et al.,* 2008）. オペレーション上の効果とは，組織内部のオペレーションに関するパフォーマンスをいい，エラー率の低減，内部コミュニケーション，業務フローの効率化などを指す. ビジネス上の効果とは，財務，市場に関連のある実績に基づくパフォーマンスをいい，収益性，マーケットシェア，販売回転率，資本利益率などを指す．このうちオペレーション

[3] ISO/IEC 27001 は 2020 年現在，2013 年版が最新となっている．第 3 章で取り扱うデータは 2008 年～2010 年としており，この時点における最新版は 2005 年版である．このため第 3 章に限り，2005 年版を参照規格として取り扱うものとする.

[4] 財団法人日本情報処理開発協会は，2011 年 4 月に一般財団法人日本情報経済社会推進協会へと組織名が変更された．組織名の変更かかわらず，略称である「JIPDEC」（Japan Institute for Promotion of Digital Economy and Community）は変更されていないことから，本論文では変更前後の組織名称にかかわらず「JIPDEC」の略称を使用する.

上の効果に焦点をあてると，日本を含め世界各国において実証研究が行われている．ISO 9001 認証の観点からは，標準化の促進，権限／責任の明確化，スムーズな取引欠陥率の改善に寄与している（引田 ほか，1995），コスト削減効果をもたらす（Miles, 1999），オペレーション上の改善をすることができる（Calisir *et al.,* 2001），文書管理の向上，内部コミュニケーションの改善，競争力の向上が認められる（Dissanayaka *et al.,* 2001）などがある．また ISO 14001 認証の観点からは，環境保護効果をもたらす（Arimura *et al.,* 2007），トルエン排出削減に効果を発揮している（岩田ほか，2010）などがある．このように認証取得によりオペレーション上の効果の向上に寄与するとしている研究が多数ある．一方で，認証取得組織と未取得組織では有意な差がない（Jones *et al.,* 1997；Quazi *et al.,* 2002；Dick *et al.,* 2008）とする研究もあり，認証取得をもってオペレーション上の効果の向上に寄与するか否かは，調査実施国や研究手法などにより結論が異なっている．

オペレーション上の効果に関する研究は多くが質問紙調査やインタビューなどの組織内の整備または運用者の認識を調査した実証分析である．発生した事故など客観的なデータに基づく認証取得組織に対する研究は，ISO 14001 認証取得組織に対するトルエン排出量の削減効果の分析（岩田ほか，2010）に限定されている．また ISO/IEC 27001 規格は，ISO 9001 規格や ISO 14001 規格など，ほかの ISO マネジメントシステム規格で求められる PDCA サイクルを回すためのフレームワークに加え，附属書 A を提供しているといった特徴をもっている．このことからほかの ISO マネジメントシステム規格認証の分析結果をもって ISO/IEC 27001 認証の効果を結論づけることはできない．

本章では，ISO/IEC 27001 認証の観点から，個人情報の漏えいまたは紛失にかかるインシデントという実例を用いたうえで，認証取得組織と未取得組織を比較して分析をおこなうことにより，認証取得組織がインシデントを抑制できているのかを調査する．また ISO/IEC 27001 認証を取得している組織において，インシデントを抑制するうえでの問題点をあきらかにすることを目的とする．

3.2. 比較分析用データの作成

認証取得組織と未取得組織におけるインシデント発生状況の比較をおこなうためには，各々の総組織数が必要となる．認証取得組織の総数は，JIPDEC の Web サイトで公開されているため取得可能であるが，未取得組織の総数を特定することが困難である．未取得組

織の総数を特定し，定量的な比較分析をおこなうため，本論文では東京証券取引所市場第一部上場企業（以下「一部上場企業」という.）を対象とする．一部を含む上場企業は，一定の基準を満たす内部統制の仕組みを整備し，整備内容に従って運用することが求められている（東京証券取引所，2015）．一部上場企業を対象とすることで，分析対象となる組織が上場基準を満たす程度の内部統制が整備されているとの前提を置くことができる．これにより非上場または中小の組織を分析対象とした場合と比較して，情報管理に関する体制や規程類の有無など，組織ごとの内部統制の充実度の違いがインシデントの発生に交絡する影響を抑制することができる．

本章では，2008 年～2010 年における日本ネットワークセキュリティ協会の『インシデントに関する調査報告書』（日本ネットワークセキュリティ協会，2009；2010；2011a）におけるインシデント一覧[5]を利用する．インシデント一覧に対して，一部上場企業一覧[6]，JIPDEC の Web サイトに掲載された ISO/IEC 27001 認証取得事業者一覧を突合せし，2008 年～2010 年における一部上場企業インシデント一覧を作成する．一部上場企業一覧の作成手法は図 3-1 に示す.

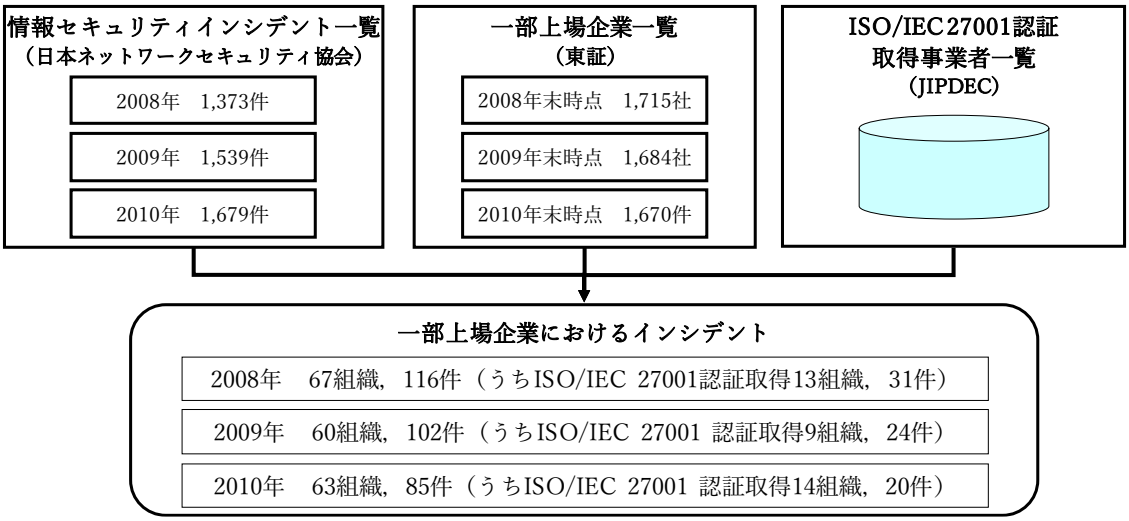

図 3-1 インシデント一覧作成手法

[5] 日本ネットワークセキュリティ協会のインシデント一覧は，インシデント発生組織名が非公開となっている．本一覧は，利用目的を研究に限定することを条件に組織名の開示を受けたものである.

[6] 各年末時点の一部上場企業一覧は，東京証券取引所より利用目的を研究に限定することを条件に提供を受けたものである.

本一覧作成にあたっては, 一部上場企業が持ち株会社の場合, 資本比率が 100%であり, 大企業相当の規模を持つ主要子会社は一部上場企業と同等とみなし，調査対象に含めている．同一インシデントで支社ごとに報告するなど，同一日かつ同一内容で報告されたインシデントはまとめて「1 件」として取り扱う．なお日本ネットワークセキュリティ協会より受領したインシデント一覧は，全件，個人情報の漏えいまたは紛失事例となっている．このため本章では，個人情報漏えいまたは紛失にかかるインシデント事例をもとにした分析および考察をおこなうものとする．

3.3. 認証有無によるインシデントの比較

3.3.1. インシデント発生／未発生組織数の比較

（1）業種全体にみるインシデント発生割合

認証有無によるインシデントの発生状況は，インシデントの発生割合または 1 組織あたりのインシデント発生比率で比較することができる．インシデント発生割合は，インシデント総発生組織数÷総組織数と定義する． 1 組織あたりのインシデント発生比率は，インシデント総発生件数÷総組織数と定義する．

インシデントの発生割合または 1 組織あたりのインシデント発生比率を用いて分析する際は，それぞれの分析手法および，確率変数 X がどの確率分布に従うのかを決定する必要がある．永田（1992）によると「n 個の製品をランダムに選んだとき，そのうち何個が不良品だったか」を取り扱うときは，二項分布を考えるとしている．また「1 単位あたり何個の欠点（キズ等）があったか」を取り扱うときは，ポアソン分布を考えるとしている．本章では永田（1992）を参考に,「認証有無によるインシデント発生割合」についてはオッズ比を用いて比較をおこなう．オッズ比の 95%信頼区間を算出する際は，確率変数 X は二項分布に従うものとする．一方,「認証有無による 1 件あたりのインシデント発生比率」に対する p 値を算出するとき，確率変数 X はポアソン分布に従うものとする．ところで事象が起こる確率をPr，標本の大きさを n とする二項分布において，$nPr \geq 5$ かつ $n(1-Pr) \geq 5$ ならば，これを正規分布に近似しても実用上問題ないとされている．また，ポアソン分布についても同様である（たとえば，久米（1989））．これに基づき本章では，認証の有無にかかわらず「インシデント発生件数が 5 件（または 5 組

織）以上」の条件を満たす時に信頼区間または p 値を算出することによる有意水準との比較を用いた推測をする．これより信頼区間または p 値の算出は，表 3-1，表 3-2，表 3-5-1，表 3-5-2 にておこなう．

一部上場企業における認証取得組織と未取得組織を比較分析するため，2008 年～2010 年の各年において認証取得組織と未取得組織それぞれに対し，インシデントを発生させた組織とインシデントを発生させなかった組織に分割した 2 × 2 のクロス集計表，オッズ比およびオッズ比の 95%信頼区間を表 3-1 に示す．インシデント発生割合の比較にあたっては，認証有無それぞれにおいてインシデントを発生させた組織数を用いて分析をおこなう．

表 3-1 認証有無によるインシデント発生割合

2008年

認証区分	インシデント有組織数	インシデント無組織数	合計	オッズ	オッズ比		95%信頼区間
認証取得	**13**	157	**170**	0.083	2.29	上限	4.282
未取得	54	1491	1545	0.036		下限	1.221
合計	**67**	1648	**1715**	0.039			

2009年

認証区分	インシデント有組織数	インシデント無組織数	合計	オッズ	オッズ比		95%信頼区間
認証取得	**9**	168	**177**	0.054	1.53	上限	3.162
未取得	51	1456	1507	0.035		下限	0.740
合計	**60**	1624	**1684**	0.036			

2010年

認証区分	インシデント有組織数	インシデント無組織数	合計	オッズ	オッズ比		95%信頼区間
認証取得	**14**	167	**181**	0.084	2.46	上限	4.558
未取得	49	1440	1489	0.034		下限	1.332
合計	**63**	1607	**1670**	0.038			

表 3-1 に示すクロス集計表は，認証取得組織と未取得組織それぞれの属性に対し，インシデント発生有組織数とインシデント発生無組織数のようにグループ別に集計したものである．認証取得組織と未取得組織各々に対して，インシデント発生有組織数÷インシデント発生無組織数で計算したものをオッズという．認証取得組織と未取得組織それぞれの属性のオッズの比をオッズ比という．オッズ比とは，２×２のクロス集計表において，２つの変数の関係の強さをあらわす指標である．オッズ比は，１より大きいとき２つの変数の間に正の相関がある，１に等しいとき２つの変数は独立である，０以上１未満のとき２つ

の変数は負の相関があるという．オッズ比の詳細については，例えば廣瀬・寺島（2010）など統計の書籍を参照されたい．なお，95%信頼区間は，オッズ比の漸近標準誤差をもとに正規分布近似をおこなった以下の式①を用いている．式①の導出は「付録 1 ：オッズ比の 95%信頼区間の導出」に示す.

$$exp\left[ln(or) \pm 1.96\sqrt{\frac{1}{CA}+\frac{1}{CN}+\frac{1}{NA}+\frac{1}{NN}}\right] \quad \cdots ①$$

式①における各記号は以下をあらわす.

- or：標本オッズ比
- CA：認証取得組織のうち，インシデントを発生させている組織数
- CN：認証取得組織のうち，インシデントを発生させていない組織数
- NA：未取得組織のうち，インシデントを発生させている組織数
- NN：未取得組織のうち，インシデントを発生させていない組織数

表 3-1 についてオッズ比を各年に対してみると，いずれの年も 1 を超えている．さらに 2008 年および 2010 年においては 95%信頼区間が 1 を含んでいないため，5 %有意である．このことからインシデント発生割合において，認証取得組織は未取得組織と比較してインシデントを抑制できているとは言い切れない.

一部上場企業数における 1 組織あたりのインシデント発生比率をまとめたものを表 3-2 に示す．1 組織あたりのインシデント発生比率の比較にあたっては，認証有無それぞれのインシデントの発生件数を用いて分析をおこなう.

表 3-2 認証有無による 1 組織あたりのインシデント発生比率比較

	一部上場企業数		インシデント発生件数		1 組織あたりのインシデント発生比率		1 組織あたりのインシデント発生比率（認証－未取得）	p値
			認証	未取得	認証	未取得		
2008年	170	1545	31	85	0.182	0.055	0.127	0.000
2009年	177	1507	24	78	0.136	0.052	0.084	0.000
2010年	181	1489	20	65	0.110	0.044	0.067	0.000

1 組織あたりのインシデント発生比率および p 値は，小数点以下第 4 位を四捨五入している.「認証取得組織と未取得組織の 1 組織あたりのインシデント発生比率が等しい」とす

る帰無仮説の下で得られた検定統計量である p 値は，ポアソン分布の正規近似法を使用して算出する．ポアソン分布とは，二項分布 $B(n,Pr)$ において $nPr \equiv \lambda$ を一定に保って，$n \to \infty$ ，$Pr \to 0$ とした極限の確率分布をいう．ポアソン分布の正規近似法とは，確率変数 X がポアソン分布 $Po(\lambda)$ に従うとき，$X + 0.5$ が近似的に $N(\lambda,\lambda)$ に従うことをいう．ここで λ は 1 組織あたりのインシデント発生比率をあらわすものとする．ポアソン分布の正規近似法の詳細については，例えば永田（1992）など統計の書籍を参照されたい．

表 3-2 によれば認証有無による 1 組織あたりのインシデント発生比率の差は，いずれも正の値を示しており，認証取得組織のほうが未取得組織よりもインシデント発生件数が多い．p 値は，2008 年から 2010 年の 3 年にわたりいずれも 0.05 未満となっているため有意水準 5 %で有意である．このことから 1 件あたりのインシデント発生比率においても，認証取得組織は未取得組織と比較してインシデントを抑制できているとは言い切れない．

（2）業種別にみるインシデント発生割合

インシデントの発生状況は，取り扱う情報の性質により異なる可能性がある．本章では，業種がインシデント発生状況に交絡していることを確認するため，業種別に分析し，分析結果について考察する．一部上場企業における業種別の ISO/IEC 27001 認証取得件数は表 3-3 に示す．

表 3-3 業種別一部上場企業 ISO/IEC 27001 認証取得件数

業種	2008年		2009年		2010年	
	認証件数	上場企業数	認証件数	上場企業数	認証件数	上場企業数
建設業	21	102	23	100	20	96
製造業	46	811	48	797	51	788
情報通信業	41	95	42	98	41	97
運輸業	11	68	12	67	13	66
卸売・小売業	22	286	21	282	22	286
金融・保険業	15	141	15	136	14	132
不動産業	2	54	2	47	2	44
サービス業	12	97	14	95	18	97

表 3-3 によれば製造業，情報通信業，建設業，卸売・小売業において認証取得件数が多

い傾向がある．業種により認証取得件数の傾向が異なることから，インシデントの発生有無は，業種の影響を受けている可能性がある．表 3-1 に対して，総務省『日本標準産業分類（平成 19 年 11 月改定）－分類項目名』における大分類別に分類し，オッズ比を算出したものを表 3-4 に示す．なお認証取得組織がない業種は表より割愛している．また表における「サービス業」には，「他に分類されないもの」を含めている．表 3-4 によれば，インシデントを発生させた組織数が認証取得組織，未取得組織ともに 5 組織以上の年および業種はない．先述の基準（「インシデント発生件数が 5 件（または 5 組織）以上」の条件を満たす時に信頼区間または p 値を算出することによる有意水準との比較を用いた推測をする．）に基づき，p 値による有意推定はおこなわず，各業種のオッズ比をもとにインシデントの発生傾向を探る．

2008 年～2010 年の 3 年間を通じて建設業，製造業，情報通信業は，オッズ比が 1 以上，不動産業，サービス業は，オッズ比が 0 である．これより建設業，製造業，情報通信業は，認証取得組織の方が未取得組織よりも発生割合は高く，不動産業，サービス業は，認証取得組織の方が未取得組織よりもインシデント発生割合は低い傾向がある．2.3.1 項より関連研究では，取引先や競合からの圧力が ISO マネジメントシステム規格の普及の要因であることが指摘されている．また圧力などにより単に認証取得が目的となった組織は，期待した効果を発揮できていないことも関連研究で指摘されている．インシデント発生割合が多い建設業，製造業，情報通信業は，表 3-3 より，いずれも認証取得件数が多い業種である．これらの業種では他の業種よりも認証取得に対する取引先や競合からの圧力が強いものと推察する．このため圧力が認証取得およびインシデントの発生に対する交絡因子となり，業種によるインシデント発生割合に影響しているものと推察する．

表 3-4 業種別インシデント発生割合のオッズ比

業種	年	認証区分	インシデント			オッズ	オッズ比
			有	無	合計		
建設業	2008	認証取得	2	19	21	0.105	1.600
		未取得	5	76	81	0.066	
	2009	認証取得	2	21	23	0.095	1.738
		未取得	4	73	77	0.055	
	2010	認証取得	4	16	20	0.250	6.083
		未取得	3	73	76	0.041	
製造業	2008	認証取得	5	41	46	0.122	23.201
		未取得	4	761	765	0.005	
	2009	認証取得	1	47	48	0.021	2.255
		未取得	7	742	749	0.009	
	2010	認証取得	2	49	51	0.041	4.257
		未取得	7	730	737	0.010	
情報通信業	2008	認証取得	3	38	41	0.079	4.184
		未取得	1	53	54	0.019	
	2009	認証取得	4	38	42	0.105	1.860
		未取得	3	53	56	0.057	
	2010	認証取得	4	37	41	0.108	1.910
		未取得	3	53	56	0.057	
運輸業	2008	認証取得	1	10	11	0.100	2.750
		未取得	2	55	57	0.036	
	2009	認証取得	0	12	12	0.000	0.000
		未取得	3	52	55	0.058	
	2010	認証取得	1	12	13	0.083	1.021
		未取得	4	49	53	0.082	
卸売・小売業	2008	認証取得	2	20	22	0.100	1.931
		未取得	13	251	264	0.052	
	2009	認証取得	0	21	21	0.000	0.000
		未取得	11	250	261	0.044	
	2010	認証取得	1	21	22	0.048	1.349
		未取得	9	255	264	0.035	
金融・保険業	2008	認証取得	0	15	15	0.000	0.000
		未取得	17	109	126	0.156	
	2009	認証取得	2	13	15	0.154	1.087
		未取得	15	106	121	0.142	
	2010	認証取得	2	12	14	0.167	1.346
		未取得	13	105	118	0.124	
不動産業	2008	認証取得	0	2	2	0.000	0.000
		未取得	6	46	52	0.130	
	2009	認証取得	0	2	2	0.000	0.000
		未取得	2	43	45	0.047	
	2010	認証取得	0	2	2	0.000	0.000
		未取得	4	38	42	0.105	
サービス業	2008	認証取得	0	12	12	0.000	0.000
		未取得	1	84	85	0.012	
	2009	認証取得	0	14	14	0.000	0.000
		未取得	3	78	81	0.038	
	2010	認証取得	0	18	18	0.000	0.000
		未取得	2	77	79	0.026	

3.3.2. インシデント発生／未発生件数の比較

インシデント事例は，１組織あたり複数件のインシデントを発生している組織がある．よって本節では，１組織あたりのインシデント発生比率を用いて比較分析をおこなうこととする．

（1）影響度別インシデント発生件数比較

a. 影響度別区分の定義

たとえば１件メールの誤送信などの場合，影響が軽微であることから組織構成員や部門などで解決してしまい，組織として把握できないことがあると推察する．認証取得組織では，このような軽微なインシデントを検出でき，かつ積極的に公表する傾向があると考えうる．一方，未取得組織では，組織構成員や部門などで解決してしまうことにより組織として把握できないため，公表されるインシデント件数が少なくなることが考え得る．このことから 3.3.1 節において認証取得組織がインシデントを抑制できていない原因の一つとして，インシデントの検出力や，公表への積極性が影響している可能性がある．

日本ネットワークセキュリティ協会が公表した『2010 年インシデントに関する調査報告書』によれば，「漏えい人数が 1000～1 万人/件以上のインシデントは，ほぼ隠さず公表されていると思われる」としている．これより１件あたりのインシデント対象人数が 1,000 人以上か否かを指標としてインシデントの影響度区分を以下のように定義する．

- 大規模インシデントとは，1,000 人/件以上のインシデントとする．
- 小規模インシデントとは，999 人/件以下のインシデントとする．

小規模インシデントは，組織の報告方針体制に依存する可能性がある．一方，大規模インシデントは，検出力や公表への積極性にかかわらず，公表されているものとする．大規模インシデントの発生状況を対象とすることにより，検出力や，公表への積極性による影響を除外したインシデントの発生傾向を分析することができる．

b. 業種全体にみるインシデント発生件数比較

2008 年～2010 年の各年において，１組織あたりのインシデント発生比率を計算し，認証取得組織，未取得組織それぞれに対して大規模インシデントについてまとめたものを表

3-5-1 に，小規模インシデントについてまとめたものを表 3-5-2 に示す.

表 3-5-1 大規模インシデント 1 組織あたりのインシデント発生比率

	一部上場企業数		大規模インシデント発生件数		1 組織あたりのインシデント発生比率		差（認証－未取得）	p値
	認証	未取得	認証	未取得	認証	未取得		
2008年	170	1545	6	21	0.035	0.014	0.021	0.024
2009年	177	1507	4	20	0.023	0.013	0.010	0.186
2010年	181	1489	5	15	0.028	0.010	0.018	0.029

表 3-5-2 小規模インシデント 1 組織あたりのインシデント発生比率

	一部上場企業数		小規模インシデント発生件数		1 組織あたりのインシデント発生比率		差（認証－未取得）	p値
	認証	未取得	認証	未取得	認証	未取得		
2008年	170	1545	25	64	0.147	0.041	0.106	0.000
2009年	177	1507	14	64	0.079	0.042	0.037	0.030
2010年	181	1489	22	43	0.122	0.029	0.093	0.000

1 組織あたりのインシデント発生比率について，認証取得組織の比率より未取得組織の比率を引いた差は, 2008 年～2010 年の各年において, 大規模インシデントで 0.021, 0.010, 0.018 と，正となっている. p 値も 2008 年および 2010 年は，有意水準 5 %で有意である. これより認証取得組織は，インシデントを抑制できているとは言い切れない．小規模インシデントでは，インシデント発生比率の差は，0.106，0.037，0.093 と，すべての年において正となっている．p 値もすべて年で 5 %有意となっている．よって小規模インシデントでも認証取得組織は，インシデントを抑制できているとは言い切れない.

認証取得組織と未取得組織における 1 組織あたりのインシデント発生比率の差は，2008 年～2010 年のすべての年において，表 3-5-1 に示す大規模インシデントよりも表 3-5-2 に示す小規模インシデントのほうが多い．このことから認証取得組織の方が軽微なインシデントであっても検出することができ，積極的に公表する傾向にあると推察する．一方，大規模インシデントは，検出力や，公表への積極性にかかわらず報告されているインシデントである．表 3-5-1 より大規模インシデントにおいて認証取得組織の方が，1 組織あたりのインシデント発生比率が多いことから，組織における報告体制などの要因にかかわらず認証取得組織は，インシデントを抑制できているとは言い切れない.

c. 業種別にみるインシデント発生比率比較

1 組織あたりの認証取得組織のインシデント発生比率と未取得組織のインシデント発生比率の差を業種別にあらわしたものについて大規模インシデントを表 3-6-1 に，小規模インシデントを表 3-6-2 に示す．不動産業およびサービス業は，認証取得組織によるインシデント事例がないため，表から割愛している．

大規模インシデントでは，1 組織あたりのインシデント発生比率に対する認証取得組織と未取得組織の差が，製造業において 2008 年に 0.065，2010 年に 0.014 となっている．また情報通信業では 2008 年に 0.049，2009 年に 0.030 と複数年でインシデント発生比率の差が正となっている．一方，卸売･小売業において 2009 年に－0.011，2010 年に－0.011，金融・保険業において 2008 年に－0.103，2010 年に－0.022 と，複数年でインシデント発生比率の差が負となっている．これより製造業，情報通信業では，認証取得組織の方がインシデント発生比率は多く，卸売・小売業，金融・保険業では，認証取得組織の方が，インシデント発生比率が少ない傾向があると推察する．

小規模インシデントでは，製造業および情報通信業において 3 年間を通じて認証組織と未取得組織の 1 組織あたりのインシデント発生比率の差が正の値を示している．また，運輸業で 2008 年に 0.056，2010 年に 0.020 と複数年でインシデント発生比率の差が正となっている．一方，建設業，卸売・小売業，金融・保険業では，複数年でインシデント発生比率の差が負となっている．これより，製造業，情報通信業，運輸業では，認証取得組織の方がインシデント発生比率は多く，建設業，卸売・小売業，金融・保険業では認証取得組織の方がインシデントは少ない傾向にある．

業種によるインシデント発生比率の差は，認証取得に対する圧力や，取り扱う情報の種類または形態，情報の取り扱い手順などが，業種により異なることが原因であると推察する．

表 3-6-1 大規模インシデント：１組織あたりのインシデント発生比率（業種別）

		一部上場企業数		大規模インシデント発生件数		１組織あたりのインシデント発生比率		差（認証－未取得）
		認証	未取得	認証	未取得	認証	未取得	
建設業	2008年	21	81	0	2	0.000	0.025	-0.025
	2009年	23	77	0	0	0.000	0.000	0.000
	2010年	20	76	0	0	0.000	0.000	0.000
製造業	2008年	46	765	3	0	0.065	0.000	0.065
	2009年	48	749	0	0	0.000	0.000	0.000
	2010年	51	737	1	4	0.020	0.005	0.014
情報通信業	2008年	41	54	2	0	0.049	0.000	0.049
	2009年	42	56	2	1	0.048	0.018	0.030
	2010年	41	56	1	3	0.024	0.054	-0.029
運輸業	2008年	11	57	0	3	0.000	0.053	-0.053
	2009年	12	55	0	0	0.000	0.000	0.000
	2010年	13	53	2	0	0.154	0.000	0.154
卸売・小売業	2008年	22	264	1	0	0.045	0.000	0.045
	2009年	21	261	0	3	0.000	0.011	-0.011
	2010年	22	264	0	3	0.000	0.011	-0.011
金融・保険業	2008年	15	126	0	13	0.000	0.103	-0.103
	2009年	15	121	2	8	0.133	0.066	0.067
	2010年	14	118	1	11	0.071	0.093	-0.022

表 3-6-2 小規模インシデント：１組織あたりのインシデント発生比率（業種別）

		一部上場企業数		小規模インシデント発生件数		１組織あたりのインシデント発生比率		差（認証－未取得）
		認証	未取得	認証	未取得	認証	未取得	
建設業	2008年	21	81	3	14	0.143	0.173	-0.030
	2009年	23	77	2	12	0.087	0.156	-0.069
	2010年	20	76	6	5	0.300	0.066	0.234
製造業	2008年	46	765	4	3	0.087	0.004	0.083
	2009年	48	749	1	5	0.021	0.007	0.014
	2010年	51	737	2	3	0.039	0.004	0.035
情報通信業	2008年	41	54	14	1	0.341	0.019	0.323
	2009年	42	56	16	4	0.381	0.071	0.310
	2010年	41	56	5	4	0.122	0.071	0.051
運輸業	2008年	11	57	1	2	0.091	0.035	0.056
	2009年	12	55	0	4	0.000	0.073	-0.073
	2010年	13	53	1	3	0.077	0.057	0.020
卸売・小売業	2008年	22	264	3	20	0.136	0.076	0.061
	2009年	21	261	0	15	0.000	0.057	-0.057
	2010年	22	264	0	11	0.000	0.042	-0.042
金融・保険業	2008年	15	126	0	8	0.000	0.063	-0.063
	2009年	15	121	1	13	0.067	0.107	-0.041
	2010年	14	118	1	8	0.071	0.068	0.004

（2）発生原因別インシデント発生件数比較

a. 発生原因区分の定義

インシデントを抑制するうえでの問題点をあきらかにするため，インシデント事例をもとに発生原因を分析する．インシデントの発生原因区分は以下にて定義する．

- 「管理策の整備／運用不備」とは，インシデント抑制のために講じるべき管理策が整備されていなかった，または管理策が整備されていたが適切な運用がなされていなかったインシデントと定義する．「管理策の整備／運用不備」には，日本ネットワークセキュリティ協会のインシデント報告書において，認可されていない情報の不正な持ち出し，社内規定の意図的な違反，２重チェック漏れによる情報の誤送付，誤配信またはシステム上の設定ミスなど，詳細内容を確認し，管理策を適切に整備し，かつ運用していれば，防ぎ得たと推察するインシデントが含まれる．
- 「抑制困難」とは，管理策を適切に整備・運用しても抑制することが困難なインシデントと定義する．「抑制困難」には，施錠した保管庫の破壊による盗難など，十分な管理策を講じられたにもかかわらず発生したインシデントが含まれる．
- 「不明」とは，管理策を適切に整備・運用しても抑制できたか否かを判断することができないインシデントと定義する．「不明」には，報告書の内容からは上記区分への分類が判断できないインシデントが含まれる．

b. 業種全体にみるインシデント発生件数比較

発生原因別のインシデント発生件数およびインシデントに対する「管理策の整備／運用不備」の割合は，表 3-7 に示す．

表 3-7 発生原因別インシデント発生件数（業種全体）

	一部上場企業数		インシデント発生件数						管理策の整備／運用不備割合	
			管理策の整備／運用不備		抑制困難		不明			
	認証	未取得	認証	未取得	認証	未取得	認証	未取得	認証	未取得
2008年	156	1347	28	54	2	3	1	9	90.3%	81.8%
2009年	161	1319	22	58	1	1	1	6	91.7%	89.2%
2010年	161	1304	18	44	1	1	1	10	90.0%	80.0%

業種全体では，2008 年～2010 年にわたり認証取得組織では 9 割以上，未取得組織では 8 割以上が「管理策の整備／運用不備」を原因としてインシデントが発生している．すなわち多くのインシデントについては，講じるべき管理策を整備し，かつ適切な運用がなされていれば抑制し得たインシデントであったと考える．認証取得組織では，認証取得の要件でもあるため，附属書 A に記載されている管理策を原則としてすべて整備している．これに対して未取得組織では ISO/IEC 27001 の要求事項を満たす義務がないため，附属書 A に記載される管理策のうち，整備されていない項目があるものと推察する．附属書 A に基づく管理策の整備状況が認証有無により異なるため，「管理策の整備／運用不備」を原因とするインシデント発生割合が認証有無により異なっているものと推察する．

c. 業種別にみるインシデント発生比率比較

業種別に 1 組織あたりの認証取得組織のインシデント発生比率と未取得組織のインシデント発生比率の差をあらわしたものを表 3-8 に示す．

「管理策の整備／運用不備」では，製造業および情報通信業において，2009 年および 2010 年，運輸業において 2008 年および 2009 年と，複数年でインシデント発生比率の差が正となっている．一方，建設業において，2008 年および 2009 年，卸売・小売業において 2009 年および 2010 年，金融・保険業において 2008 年および 2010 年と，複数年でインシデント発生比率の差が負となっている．これより，製造業，情報通信業，運輸業では，認証取得組織の方がインシデント発生比率は多く，建設業，卸売・小売業，金融・保険業では，認証取得組織の方がインシデント発生比率は少ない傾向があると推察する．

「抑制困難」では，情報通信業において 2008 年および 2009 年の複数年でインシデント発生比率の差が正となっており，卸売・小売業において，2008 年および 2010 年の複数年でインシデント発生比率の差が負となっている．これより情報通信業では，認証取得組織の方がインシデント発生比率は多く，卸売・小売業では，認証取得組織の方がインシデント発生比率は少ない傾向があると推察する．なお，そのほかの業種については，特筆すべき傾向はみられない．

表 3-8 発生原因別 1 組織あたりのインシデント発生比率（業種別）

		一部上場企業数		インシデント発生件数						1 組織あたりのインシデント発生比率						1 組織あたりのインシデント発生比率（認証取得－未取得）		
				管理策の整備／運用不備		抑制困難		不明		管理策の整備／運用不備		抑制困難		不明		管理策の整備／運用不備	抑制困難	不明
		認証	未取得	認証	未取得	認証	未取得	認証	未取得	認証	未取得	認証	未取得	認証	未取得			
建設業	2008年	21	81	2	9	0	0	1	7	0.095	0.111	0.000	0.000	0.048	0.086	0.111	0.000	-0.039
	2009年	23	77	1	11	0	0	1	1	0.043	0.143	0.000	0.000	0.043	0.013	0.143	0.000	0.030
	2010年	20	76	6	4	0	0	0	1	0.300	0.053	0.000	0.000	0.000	0.013	0.053	0.000	-0.013
製造業	2008年	46	765	6	3	1	0	0	0	0.130	0.004	0.022	0.000	0.000	0.000	-0.018	0.022	0.000
	2009年	48	749	1	5	0	0	0	0	0.021	0.007	0.000	0.000	0.000	0.000	0.007	0.000	0.000
	2010年	51	737	2	6	0	0	1	1	0.039	0.008	0.000	0.000	0.020	0.001	0.008	0.000	0.018
情報通信業	2008年	41	54	15	1	1	0	0	0	0.366	0.019	0.024	0.000	0.000	0.000	-0.006	0.024	0.000
	2009年	42	56	17	5	1	0	0	0	0.405	0.089	0.024	0.000	0.000	0.000	0.065	0.024	0.000
	2010年	41	56	6	4	0	0	0	3	0.146	0.071	0.000	0.000	0.000	0.054	0.071	0.000	-0.054
運輸業	2008年	11	57	1	5	0	0	0	0	0.091	0.088	0.000	0.000	0.000	0.000	0.088	0.000	0.000
	2009年	12	55	0	3	0	1	0	0	0.000	0.055	0.000	0.018	0.000	0.000	0.055	-0.018	0.000
	2010年	13	53	2	3	1	0	0	0	0.154	0.057	0.077	0.000	0.000	0.000	-0.020	0.077	0.000
卸売・小売業	2008年	22	264	4	15	0	3	0	2	0.182	0.057	0.000	0.011	0.000	0.008	0.057	-0.011	-0.008
	2009年	21	261	0	14	0	0	0	4	0.000	0.054	0.000	0.000	0.000	0.015	0.054	0.000	-0.015
	2010年	22	264	0	10	0	1	0	3	0.000	0.038	0.000	0.004	0.000	0.011	0.038	-0.004	-0.011
金融・保険業	2008年	15	126	0	21	0	0	0	0	0.000	0.167	0.000	0.000	0.000	0.000	0.167	0.000	0.000
	2009年	15	121	3	20	0	0	0	1	0.200	0.165	0.000	0.000	0.000	0.008	0.165	0.000	-0.008
	2010年	14	118	2	17	0	0	0	2	0.143	0.144	0.000	0.000	0.000	0.017	0.144	0.000	-0.017

3.3.3. 管理策別インシデント発生比率比較

（1）ISO/IEC 27001 規格における附属書 A

ISO/IEC 27001 規格の附属書 A に列挙される管理策は，要求事項上，適用の要否およびその実現方法は組織に委ねられている．しかし，適用宣言書に除外理由を明文化する必要があることから，認証取得組織の場合,「該当する業務を実施していないため適用除外」などの明確な理由を有するものを除き，すべての管理策を適用しているものと考える．

3.3.2.（2）a. で定義したインシデント発生原因区分のうち,「管理策の整備／運用不備」の対象となる管理策は，すべて附属書 A で網羅されている．すなわち ISO/IEC 27001 規格の附属書 A に列挙される管理策を整備し，適切に運用していれば，認証取得組織では 9 割以上，未取得組織では 8 割以上のインシデントが抑制し得たと推察する．認証取得組織では，特段の事情がない限り全ての管理策が整備され組織に組み込まれている．すなわち認証取得組織では，管理策を整備しているにもかかわらず，運用が伴っていないことによりインシデントが発生しているといえる．

「管理策の整備／運用不備」に分類するインシデントに対し，有効に機能することでインシデントを抑制できたと推察する管理策を業種毎にまとめる．表 3-9 は，認証取得組織の管理策を業種毎にまとめたものである．表 3-10 は，未取得組織の管理策を業種毎にまとめたものである．表 3-11 は，認証取得組織，未取得組織各々のインシデント件数に対して，認証取得組織の管理策の件数から未取得組織の管理策の件数を引いた結果をまとめたものである．なお各表における附属書 A 欄は，該当する管理策の番号およびその項目名をあらわしている．

表 3-9　管理策別 1 組織あたりのインシデント発生比率（認証取得組織）

附属書A	建設業	製造業	情報通信業	運輸業	卸売・小売業	金融・保険業	合計
A.7.2.1　分類の指針	4	3	7	1	3	4	22
	0.364	0.273	0.175	0.250	0.750	0.800	0.293
A.7.2.2　情報のラベル付け及び取り扱い	4	3	7	1	3	4	22
	0.364	0.273	0.175	0.250	0.750	0.800	0.293
A.9.1.2　物理的入退管理策	0	1	0	0	0	0	1
	−	0.091	−	−	−	−	0.013
A.9.2.6　装置の安全な処分又は再利用	0	1	0	0	0	0	1
	−	0.091	−	−	−	−	0.013
A.10.4.2　モバイルコードに対する管理策	0	1	2	0	0	0	3
	−	0.091	0.050	−	−	−	0.040
A.10.7.1　取り外し可能な媒体の管理	2	1	0	1	0	1	5
	0.182	0.091	−	0.250	−	0.200	0.067
A.10.7.2　媒体の処分	0	1	1	0	0	3	5
	−	0.091	0.025	−	−	0.600	0.067
A.10.7.3　情報の取扱手順	5	7	17	2	4	4	39
	0.455	0.636	0.425	0.500	1.000	0.800	0.520
A.10.8.1　情報交換の方針及び手順	1	4	10	0	1	0	16
	0.091	0.364	0.250	−	0.250	−	0.213
A.10.8.3　配送中の物理的媒体	4	1	3	0	0	0	8
	0.364	0.091	0.075	−	−	−	0.107
A.10.8.4　電子的メッセージ通信	1	2	3	0	1	0	7
	0.091	0.182	0.075	−	0.250	−	0.093
A.10.9.3　公開されている情報	0	0	4	0	0	0	4
	−	−	0.100	−	−	−	0.053
A.11.4.1　ネットワークサービスの利用についての方針	0	0	2	1	0	0	3
	−	−	0.050	0.250	−	−	0.040
A.11.4.2　外部から接続する利用者の認証	0	0	2	1	0	0	3
	−	−	0.050	0.250	−	−	0.040
A.11.5.2　利用者の識別及び認証	0	0	2	1	0	0	3
	−	−	0.050	0.250	−	−	0.040
A.12.2.2　内部処理の管理	0	0	3	0	0	0	3
	−	−	0.075	−	−	−	0.040
A.15.1.4　個人データ及び個人情報の保護	0	0	6	0	0	0	6
	−	−	0.150	−	−	−	0.080
インシデント件数	11	11	40	4	4	5	75
管理策件数	21	25	69	8	12	16	151

※1 各管理策の上段はインシデントに対応する管理策の件数、下段は該当業種全体に占める管理策の割合を表している。

※2 1つのインシデントに対して複数の管理策が機能する場合があるため、合計の管理策の割合は1を超えている。

※3 不動産業及びサービス業は、認証取得企業によるインシデント事例がないため、表から割愛している。

表 3-10 管理策別 1 組織あたりのインシデント発生比率（未取得組織）

附属書A	建設業	製造業	情報通信業	運輸業	卸売・小売業	金融・保険業	合計
A.7.2.1　分類の指針	6	3	0	8	24	42	88
	0.182	0.200	−	0.667	0.462	0.689	0.413
A.7.2.2　情報のラベル付け及び取り扱い	6	3	0	8	24	42	88
	0.182	0.200	−	0.667	0.462	0.689	0.413
A.9.1.2　物理的入退管理策	0	0	0	0	0	0	0
	−	−	−	−	−	−	−
A.9.2.6　装置の安全な処分又は再利用	0	0	0	0	0	0	0
	−	−	−	−	−	−	−
A.10.4.2　モバイルコードに対する管理策	0	0	3	0	1	0	4
	−	−	0.231	−	0.019	−	0.019
A.10.7.1　取り外し可能な媒体の管理	1	1	0	1	1	7	12
	0.030	0.067	−	0.083	0.019	0.115	0.056
A.10.7.2　媒体の処分	0	0	0	3	4	33	41
	−	−	−	0.250	0.077	0.541	0.192
A.10.7.3　情報の取扱手順	11	6	3	10	25	45	107
	0.333	0.400	0.231	0.833	0.481	0.738	0.502
A.10.8.1　情報交換の方針及び手順	6	3	3	2	1	3	21
	0.182	0.200	0.231	0.167	0.019	0.049	0.099
A.10.8.3　配送中の物理的媒体	9	4	2	1	11	8	46
	0.273	0.267	0.154	0.083	0.212	0.131	0.216
A.10.8.4　電子的メッセージ通信	3	3	3	2	1	2	16
	0.091	0.200	0.231	0.167	0.019	0.033	0.075
A.10.9.3　公開されている情報	0	0	0	0	1	0	2
	−	−	−	−	0.019	−	0.009
A.11.4.1　ネットワークサービスの利用についての方針	0	2	0	0	0	0	4
	−	0.133	−	−	−	−	0.019
A.11.4.2　外部から接続する利用者の認証	0	2	0	0	0	0	4
	−	0.133	−	−	−	−	0.019
A.11.5.2　利用者の識別及び認証	0	2	0	0	0	0	4
	−	0.133	−	−	−	−	0.019
A.12.2.2　内部処理の管理	0	3	1	0	0	0	5
	−	0.200	0.077	−	−	−	0.023
A.15.1.4　個人データ及び個人情報の保護	2	0	0	0	0	1	3
	0.061	−	−	−	−	0.016	0.014
インシデント件数	33	15	13	12	52	61	213
管理策件数	44	32	15	35	93	183	445

※1 各管理策の上段はインシデントに対応する管理策の件数、下段は該当業種全体に占める管理策の割合を表している。
※2 1つのインシデントに対して複数の管理策が機能する場合があるため、合計の管理策の割合は1を超えている。

表 3-11 管理策別 1 組織あたりのインシデント発生比率比較

（認証取得組織－未取得組織）

附属書A	建設業	製造業	情報通信業	運輸業	卸売・小売業	金融・保険業	不動産業	サービス業	合計
A.7.2.1　分類の指針	0.182	0.073	0.175	-0.417	0.288	0.111	-0.294	0.000	-0.120
A.7.2.2　情報のラベル付け及び取り扱い	0.182	0.073	0.175	-0.417	0.288	0.111	-0.294	0.000	-0.120
A.9.1.2　物理的入退管理策	0.000	0.091	0.000	0.000	0.000	0.000	0.000	0.000	0.013
A.9.2.6　装置の安全な処分又は再利用	0.000	0.091	0.000	0.000	0.000	0.000	0.000	0.000	0.013
A.10.4.2　モバイルコードに対する管理策	0.000	0.091	-0.181	0.000	-0.019	0.000	0.000	0.000	0.021
A.10.7.1　取り外し可能な媒体の管理	0.152	0.024	0.000	0.167	-0.019	0.085	-0.059	0.000	0.010
A.10.7.2　媒体の処分	0.000	0.091	0.025	-0.250	-0.077	0.059	-0.059	0.000	-0.126
A.10.7.3　情報の取扱手順	0.121	0.236	0.194	-0.333	0.519	0.062	-0.412	0.000	0.018
A.10.8.1　情報交換の方針及び手順	-0.091	0.164	0.019	-0.167	0.231	-0.049	-0.118	-0.100	0.115
A.10.8.3　配送中の物理的媒体	0.091	-0.176	-0.079	-0.083	-0.212	-0.131	-0.412	-0.400	-0.109
A.10.8.4　電子的メッセージ通信	0.000	-0.018	-0.156	-0.167	0.231	-0.033	-0.118	0.000	0.018
A.10.9.3　公開されている情報	0.000	0.000	0.100	0.000	-0.019	0.000	0.000	-0.100	0.044
A.11.4.1　ネットワークサービスの利用についての方針	0.000	-0.133	0.050	0.250	0.000	0.000	0.000	-0.200	0.021
A.11.4.2　外部から接続する利用者の認証	0.000	-0.133	0.050	0.250	0.000	0.000	0.000	-0.200	0.021
A.11.5.2　利用者の識別及び認証	0.000	-0.133	0.050	0.250	0.000	0.000	0.000	-0.200	0.021
A.12.2.2　内部処理の管理	0.000	-0.200	-0.002	0.000	0.000	0.000	0.000	-0.100	0.017
A.15.1.4　個人データ及び個人情報の保護	-0.061	0.000	0.150	0.000	0.000	-0.016	0.000	0.000	0.066

（2）業種全体にみるインシデント発生比率比較

インシデント発生に直接的に影響する管理策は，附属書 A の 133 項目のうち 17 項目である．すなわち特定の管理策の不備がインシデントの発生に大きく影響している．認証取得組織，未取得組織各々の管理策別 1 組織あたりのインシデント発生比率をみると，表 3-9 より認証取得組織では，A.10.7.3（情報の取扱手順），A.7.2.1（分類の指針），A.7.2.2（情報のラベル付けおよび取扱い），A.10.8.1（情報交換の方針および手順），A.10.8.3（配送中の物理的媒体）と，順に多くなっている．表 3-10 より未取得組織では，A.10.7.3，A.7.2.1，A.7.2.2，A.10.8.3，A.10.7.2（媒体の処分）と，順に多くなっている．これより認証取得組織，未取得組織ともに，多くは同じ管理策の不備を起因としてインシデントが発生していることがわかる．

インシデント発生比率の高い管理策を認証取得組織と未取得組織とで比較すると，表 3-9 より，全体の半数を占める A.10.7.3（情報の取扱手順）は，ともに大差がない．A.10.7.3 に次いでともに多い件数を占めている管理策のうち，A.7.2.1（分類の指針），A.7.2.2（情報のラベル付けおよび取扱い），A.10.7.2（媒体の処分），A.10.8.3（配送中の物理的媒体）については，いずれも認証取得組織の方が未取得組織に比べて 1 組織あたり 0.1 件以上少ない．これより認証取得組織では，未取得組織に比べて情報資産をその価値に沿って適切に分類し，分類に従ったラベル付けを行なっている．また，ほかの情報資産に紛れて紛失または廃棄してしまうといったインシデントや，車上荒らしなどに対する管理策は，比較的有効に機能している傾向にあると推察する．

一方で，A.7.2.1，A.7.2.2，A.10.7.2，A.10.8.3 以外の管理策はすべて認証取得組織の方が高い傾向にある．とりわけ，A.10.8.1（情報交換の方針および手順）は，認証取得組織の方が未取得組織よりも 1 組織あたり 0.115 件多くなっていることから，電子メールの送信時や FAX 送信時，郵送物の配送・梱包時における手順や運用などに不備があり，管理策が有効に機能していない傾向にあると推察する．

（3）業種別にみるインシデント発生比率比較

製造業では，A.11.4.1，A.11.4.2，A.11.5.2，A.12.2.2 のネットワーク通信時における管理策やシステム処理の管理策に関連するインシデントが未取得組織で複数件発生しているのに対し，認証取得組織では，一切発生していない．この現象の理由に対する 1 つの可能性としては，ISO/IEC 27001 規格の附属書 A が提供している網羅的な観点からの管理策を

適用することにより，リスクがあるものの対応が漏れがちな管理策に目が届くようになったと考える．

情報通信業では，A.7.2.1，A.7.2.2，A.10.9.3，A.11.4.1，A.11.4.2，A.11.5.2 の資産の管理や，ネットーワーク通信時，個人情報の取り扱いに関する管理策が，認証取得組織で複数件発生しているのに対し，未取得組織では一切発生していない．情報通信業は，業界の中でも，より高度な通信技術や個人情報などの重要情報を取り扱う組織が ISO/IEC 27001 規格を認証取得する傾向にあると推察する．このため認証取得組織において取り扱う情報の種類や量，また情報を取り扱う際の通信技術などが複雑化している結果，該当する管理策に関連するインシデントが発生しているものと考える．

金融・保険業では，認証取得組織，未取得組織ともに A.10.7.2 が突出して件数が多い傾向がみられる．金融・保険業で取り扱う情報は，証憑など一定期間保管を求められる情報が多い．書類を中心に膨大な情報の取り扱いが求められる業種であることから，人手による処理ミスが要因となる誤廃棄が，ほかの業種よりも発生しやすくなっていると考える．

これらの傾向は，業種により発生しやすいインシデントの傾向が異なっている．また，インシデント抑制の目的達成のための管理策も業種により注力すべき項目が異なっていることを示唆している．

3.4. 考察

本章では，日本ネットワークセキュリティ協会の調査報告書において掲載されている個人情報の漏えいまたは紛失に関するインシデントを対象としている．当該報告書は，インシデントを発生させた組織によるプレスリリース，もしくは新聞などのメディアへ公表されたインシデントをもとに集計されているものである．また本章で分析の対象としている組織は，一部上場企業に限定している．考察にあたっては上記データの特性を考慮しておこなっている．

表 3-1 および表 3-2 より，認証有無によるインシデント発生数も，１組織あたりのインシデント発生比率も認証取得組織の方が多い．また表 3-5-1 より組織における検出力や公表への積極性などの要因にかかわらず，認証取得組織は未取得組織と比較してインシデントを抑制できているとは言い切れない．この理由として認証取得組織では，単に認証取得することが目的となっているため，多くが管理策を整備したのみで遵守されず，管理策の

形骸化を招いていることが仮説の一つとして考えられる．

1 件あたりのインシデントが 1000 人以上の個人情報を含むか否かを基準として，影響度別にインシデント発生件数をみると，表 3-5-1 および表 3-5-2 より，大規模インシデント，小規模インシデント双方において，認証取得組織は未取得組織と比較してインシデントを抑制できているとは言い切れない．この理由として小規模インシデントについては，認証取得により組織内のインシデント報告体制が整備されたため，インシデント検出力が上がり，より多く報告するようになったという前述の理由が挙げられる．一方，大規模インシデントについては，業種全体における考察に加え，1000 人以上の膨大な個人情報を保有している，情報の管理に高度な情報技術が必要となるなど，もともと未取得組織よりもリスクの高い組織が認証を取得していることが要因の 1 つであると推察する．

各業種の傾向に目を向けると，製造業，情報通信業では，表 3-4 におけるインシデント発生割合，表 3-6-1 および表 3-6-2 における大規模インシデントおよび小規模インシデントの影響度区分で認証取得組織の方がインシデントは発生しやすい傾向がみられる．一方で認証取得件数の少ない不動産業，サービス業では，インシデントは発生しておらず，また卸売・小売業，金融・保険業においても 1 組織あたりのインシデント発生比率が少ない傾向にある．これより ISO/IEC 27001 規格に基づいて ISMS を整備した組織であっても，整備した管理策に沿って適切に運用されているかについては，業種によって異なる傾向がある．インシデント発生割合および 1 組織あたりのインシデント発生比率の多い製造業および情報通信業は，表 3-3 より，いずれも認証取得件数の多い業種である．製造業は，1990 年代より，ほかの業種に先んじて ISO 9001 認証の取得に取り組んでいる．ISO/IEC 27001 規格は ISO 9001 規格と同様，マネジメントシステムを構築することを要求している規格であり，ISO 9001 認証を取得している組織にとっては，マネジメントシステムの構築・運用経験があるため ISO/IEC 27001 規格は導入しやすい．製造業でのインシデントが高まっている要因として，ほかの業種に比べてマネジメントシステムが成熟し，現場レベルで運用が浸透しているため，インシデントが検出しやすくなっていると考える．情報通信業は，大量のデータを高速に処理することが多く，情報セキュリティが当然視されている業界といえる．このため，認証の有無にかかわらず，ISO/IEC 27001 規格の附属書 A に記載されている管理策は多くの組織が実行していると考えられ，ほかの業界に比べて情報セキュリティに対する意識が高いと推察する．情報セキュリティに敏感となり，インシデントが検出しやすくなっているため，インシデントが未取得組織よりも多くなっていると考え

る．

表 3-7 よりインシデントのうち，認証取得組織では 9 割以上，未取得組織では 8 割以上が管理策の不備，または整備した管理策が運用されていないことにより発生している．ここでインシデント抑制のために講じるべきであった管理策は，すべて ISO/IEC 27001 規格の附属書 A にて網羅されている．このことから ISO/IEC 27001 規格に準拠した ISMS が適切に整備し，運用されていれば，多くのインシデントは抑制し得るものと推察する．ISO/IEC 27001 規格では附属書 A に示す管理策の適用が要求されている．すなわち認証取得組織では，特段の事情がない限りすべての管理策が整備されているものと推察する．つまり ISO/IEC 27001 規格を適用することで，インシデントの抑制を実現するためには，組織構成員に対して，規定した管理策を遵守させるような施策が組織に求められると考える．

3.5. 結論

本章では，ISO/IEC 27001 認証の観点から，個人情報の漏えいまたは紛失にかかるインシデントという実例を用いたうえで，認証取得組織と未取得組織を比較して分析をおこなうことにより，認証取得組織がインシデントを抑制できているのかを調査している．また ISO/IEC 27001 認証取得組織におけるインシデント抑制に対する問題点をあきらかにすることを目的としている．

業種全体としてインシデント発生割合，インシデント発生比率ともに，認証取得組織は，未取得組織と比較してインシデントを抑制できているとは言い切れない．このことから第 1 章において問題意識として掲げている，「認証取得または維持のみが目的となった組織であっても，情報セキュリティに関連するインシデントの抑制ができるのだろうか」に対しては，「認証取得をすることのみをもってインシデントを抑制できるとは言い切れない」ことを実証している．

情報処理推進機構（2015）によるとインシデントにおける 1 件あたりの被害は，外部からの攻撃よりも組織構成員によるもののほうが大きい場合がある．また情報処理推進機構（2016）によると近年では，組織構成員が不正に情報を持ち出す行為を原因としたインシデント事例が多く報告されている．第 4 および第 5 章では，組織構成員による不正に情報を持ち出す行為に着目し，どのような施策を講じて組織構成員に管理策を遵守させるかについて考察する．

個人情報の保護に関するマネジメントシステムの構築には，プライバシーマーク認定の要求事項である JIS Q 15001 規格（日本規格協会，2017）や ISO マネジメントシステム規格である ISO/IEC 27701 規格（ISO, 2019）がある．これらの規格はいずれも個人情報を取得する際における利用目的の特定など，法令に基づく個人情報の取り扱いに特化した項目を除き，ISO/IEC 27001 の要求事項や附属書 A，もしくは ISO/IEC 27001 規格における附属書 A に示す管理策の具体的な実現方法を例示した ISO/IEC 27002（ISO, 2014b）を準用している．個人情報の保護に関する規格では，個人情報に特化した項目を除き ISO/IEC 27001 または ISO/IEC 27002 を準用していることから，管理策を遵守させるための施策は，個人情報のみならず技術情報や経営情報などの情報にも適用できると考える．このため第 4 章および第 5 章では個人情報に限定せず，技術情報や経営情報などの情報資産全般に対象を広げて施策を検討する．

第４章　不正な情報持ち出しの正当化抑制のための施策

4.1. 背景と目的

第 3 章では ISO/IEC 27001 規格を適用することでインシデントの抑制という目的を達成するにあたり，組織構成員に対して管理策を遵守させるための施策が必要であるとの示唆が得られている．

本章および次章では管理策を遵守させるための施策のうち，不正に情報を持ち出す行為を抑制するための施策に焦点をあてる．どのような施策を講じれば不正に情報を持ち出す行為を抑制できるのかという問題について本章では，不正のトライアングル理論（Cressey, 1971），ならびに ISO/IEC 27001 規格（ISO，2013）を用いて解決を図る．

本章では不正のトライアングル理論のうち「正当化」を抑制するためにどのような施策を講じるべきかを考察する．具体的には，組織は ISO/IEC 27001 規格における「認識」の要求事項のうち，どの項目に注力すれば不正な情報持ち出し行為の正当化が抑制できるのかについての知見を得ることを目的とする．本章の対象についての概念図は図 4-1 に示す．分析にあたっては仮説の設定および仮説検証モデルを構築し，上場企業かつ ISO/IEC 27001 認証の取得件数が多い業種の組織構成員を対象とした質問紙調査により取得するデータに対し，認証有無全体に対する共分散構造分析，さらに認証取得／未取得の組織についての多母集団分析により，仮説検証をおこなう．仮説の検証を通じて正当化を抑制するためのメカニズムを解明し，組織が講じるべき施策を提案する．

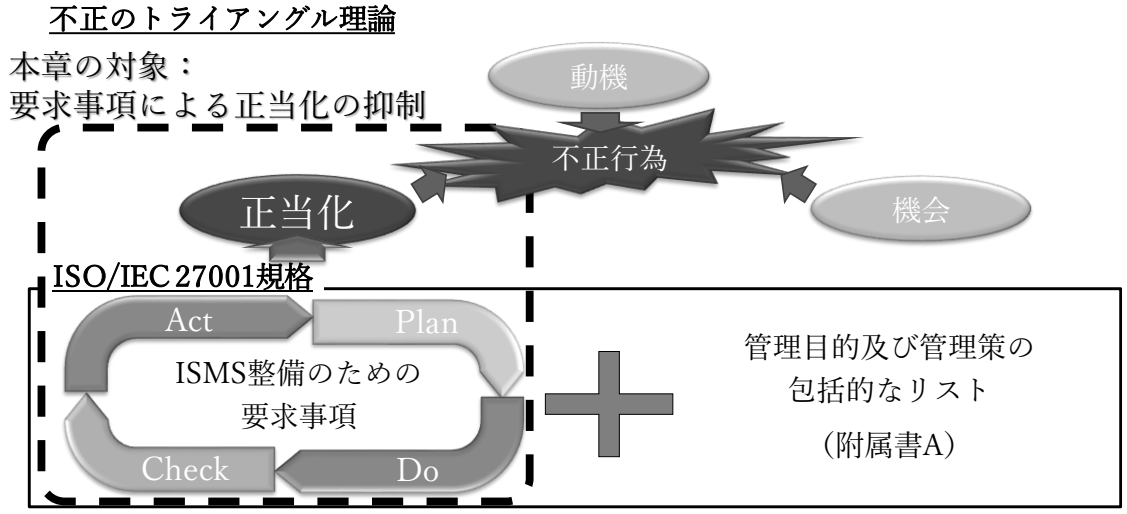

図 4-1　本章の対象

本章の構成は次のとおりである．4.2 節にて関連する研究を紹介し本章のアプローチを導出する．4.3 節にて関連研究から得られた知見と ISO/IEC 27001 規格の要求事項をもとにいくつかの仮説を設定し，仮説検証モデルを構築する．4.4 節で組織構成員の認識および正当化に関するデータ収集のための調査票設計と調査について述べる．4.5 節にて分析結果の記述と考察をおこない，最後に 4.6 節にてまとめと今後の課題について述べる．

4.2. 関連研究

本節では不正な情報持ち出し行為の正当化を抑制するにあたり，ISO/IEC 27001 規格を採用することの効果および不正に情報を持ち出す行為に関する研究を紹介する．関連研究の紹介を通じて，本章のアプローチを述べる．

4.2.1. ISO/IEC 27001 認証取得の効果に関する研究

ISO/IEC 27001 認証を取得している組織は，ISO/IEC 27001 規格が定める要求事項をすべて満たし，第三者機関である審査機関により適合と判断されている．ISO/IEC 27001 認証のみならず ISO 認証取得の効果は ISO 9001 認証（品質）や ISO 14001 認証（環境）の観点において確認されている．ISO 9001 認証では，認証および TQM（Total Quality Management）導入有無の比較による品質改善効果（Martínez‐Lorente & Martínez‐Costa, 2004），認証取得組織における品質改善効果（Feng *et al.*, 2008）や，製品のパフォーマンス（Nair & Prajogo, 2009）などが確認されている．ISO 14001 認証では，認証取得組織における環境負荷の低減効果（Matuszak-Flejszman, 2009），認証有無の比較による環境に対する意識や環境マネジメントに対する改善効果（Turk, 2009），認証取得組織におけるトルエン排出量の削減効果（岩田ほか，2010）などが確認されている．ISO/IEC 27001 認証によるインシデント抑制効果については，第 3 章にて認証を取得している組織がインシデントを抑制できているか否か，および附属書 A とインシデントの内容を突き合わせ，附属書 A 記載の管理策が遵守されていれば防ぎ得たかを確認している．

ISO を認証取得することによる効果の関連研究では，認証の有無など要求事項に対して包括的観点から分析がおこなわれている．しかし正の影響をおよぼす要求事項と負の影響をおよぼす要求事項が混在する場合，包括的観点からの分析のみでは規格が有用か否かを結論づけることは困難である．このため ISO/IEC 27001 規格を採用することの有用性を

あきらかにするには，個別の要求項目に着目した個別的観点から効果を分析する必要がある．また第 3 章にてインシデント事例と突き合わせをおこなっている附属書 A の多くは不正のトライアングルにおける「機会」を抑制するための策である．このため「正当化」を抑制するための施策については改めて検討する必要がある．

4.2.2. 不正な情報持ち出し行為の正当化を抑制するための施策に関する研究

Cohen *et al.*（2010）は，不正な情報持ち出し行為を抑制するための理論として FT/TPB（fraud triangle/theory of planned behavior applied to fraud）を提唱している．FT/TPB とは計画的行動理論を用いて不正のトライアングルの 1 つである正当化を説明する考え方をいう．

計画的行動理論（Theory of Planned Behavior）（Ajzen, 1985；Ajzen & Madden, 1986；Ajzen, 1991）とは，互いに相関関係にある態度，主観的規範，統制可能性が，行動意図に影響し，行動意図が行動に影響することを体系化した理論である．小池ほか（2003）は環境保護の観点において計画的行動理論を適用し，態度から行動意図を通じて行動に至る段階の進行を仮定している．そのうえで知識，関心，動機が行動意図を通じて行動に至るモデルを構築し，因果関係の構造をあきらかにしている．諏訪ほか（2012）は，小池ほか（2003）のモデルを情報セキュリティ分野に応用し，知識が関心を通じて行動に至るモデルを構築したうえで，共分散構造分析の手法を用いて因果関係の構造をあきらかにしている．Khan *et al.*（2011）は情報セキュリティに対する知識から態度，規範的概念，行動意図を通じて行動に至るまでのモデルを構築し，情報セキュリティ意識を向上させるための手段を提案している．AL-Omari *et al.*（2012）は，計画的行動理論に情報セキュリティ知識と技術的セキュリティ知識を追加したモデルを構築し，情報セキュリティポリシーへの準拠意図に対する因果関係の構造をあきらかにしている．

不正に情報を持ち出す行為についての研究では，計画的行動理論を用いた研究のほか，行動を引き起こす要因の抽出（竹村ほか，2015），組織風土（濱田・廣松，2012）の観点における影響が分析されている．また井川ほか（2009）はセキュリティ知識がセキュリティ行動に影響することについて実証している．

計画的行動理論を用いた関連研究によれば，不正をおこなおうとする意図が不正な情報持ち出し行為を引き起こす要因となっている．筆者は FT/TPB を用いて，不正な情報持ち出し行為の正当化を抑制することが，不正に情報を持ち出す行為の抑制につながるものと

考える．そのほか関連研究では，行動または行動意図に影響する因子が抽出され，共分散構造分析などの手法により因果関係があきらかにされている．しかし ISO/IEC 27001 規格を採用することの有用性をあきらかにするには，要求事項の項目に着目した因子を定義する必要がある．さらに要求事項に影響する因子についても定義したうえで行動意図に至るまでの因果関係のモデルを構築し，その影響を分析する必要がある．

4.2.3. 本章のアプローチ

本章では ISO/IEC 27001 が要求する認識が不正な情報持ち出し行為の正当化の抑制に寄与することを実証する．実証にあたり ISO/IEC 27001 の要求事項より「認識」の因子を定義する．加えて関連研究を参考に，認識に影響する因子を定義する．そのうえで認識に影響する因子が認識を通じて不正な情報持ち出し行為の正当化に至るまでの因果関係について仮説を設定し，仮説検証モデルを構築する．仮説の検証は，質問紙調査で得られるデータをもとに共分散構造分析の手法を用いておこなう．さらに ISO/IEC 27001 認証の有無について，多母集団分析により認証の有無に応じて組織構成員に持たせるべき認識が異なるかについて検証する．

4.3. 仮説の設定および仮説検証モデルの構築

本節では不正な情報持ち出し行為の正当化に影響する因子を定義する．そのうえで仮説を設定し，仮説検証モデルを構築する．

4.3.1. 仮説の設定

（1）不正な情報持ち出し意図におよぼす影響についての仮説

ISO/IEC 27001 規格（ISO, 2013）の 7.3 節に記載される認識の要求事項では，a）情報セキュリティ方針, b）情報セキュリティパフォーマンスの向上によって得られる便益を含む，ISMS の有効性に対する自らの貢献，c）ISMS 要求事項に適合しない意味，の 3 つを組織構成員に対して持たせなければならない認識として定めている．不正な情報持ち出し意図におよぼす影響は，ISO/IEC 27001 規格 7.3 節に記載される認識の要求事項 a)～c）より抽出する．これより本章では「方針の認識」,「自らの貢献の認識」,「不正な情報持ち出し行為による影響の認識」を不正な情報持ち出し行為の正当化を抑制するために組織構

成員が持つべき認識の因子として採用し，仮説Ｈ１～Ｈ３を設定する．

Ｈ１：方針に対する認識度の向上が，不正行為の正当化を抑制する．

Ｈ２：自らの貢献に対する認識度の向上が，不正行為の正当化を抑制する．

Ｈ３：不正行為による影響に対する認識度の向上が，不正行為の正当化を抑制する．

（２）認識におよぼす影響についての仮説

関連研究では知識が意図に対して間接的に影響することが確認されている（たとえば小池ほか，2003；井川ほか，2009；Khan *et al.*, 2011；諏訪ほか，2012；AL-Omari *et al.*, 2012；竹村ほか，2015）．本章では情報を保護するために何をすべきかを知っている状態をあらわす「セキュリティ知識」を認識に影響する因子として採用し，仮説Ｈ４－１～Ｈ４－３を設定する．

Ｈ４－１：セキュリティ知識が向上すると，方針に対する認識度が向上する．

Ｈ４－２：セキュリティ知識が向上すると，自らの貢献に対する認識度が向上する．

Ｈ４－３：セキュリティ知識が向上すると，不正行為による影響に対する認識度が向上する．

Nair & Prajogo（2009）は ISO 9001 認証を取得するにあたり組織内外からの認証取得に対する圧力があることを指摘している．そのうえで組織内外からの圧力が，品質に対するパフォーマンスへ影響することについて確認している．情報セキュリティ分野においても認証取得のなど，組織内外から圧力が発生しており，圧力と不正に情報を持ち出す行為についての因果関係が確認されている（諏訪ほか，2012；濱田・廣松，2012）すなわち認識の因子には周囲からの圧力による影響も考慮する必要がある．圧力とは情報セキュリティを維持することに対する要請をさす．本章では「セキュリティ要請」を認識に影響する因子として採用し，仮説Ｈ５－１～Ｈ５－３を設定する．

Ｈ５－１：セキュリティ要請が強まると方針に対する認識度が向上する．

Ｈ５－２：セキュリティ要請が強まると自らの貢献に対する認識度が向上する．

Ｈ５－３：セキュリティ要請が強まると不正行為による影響に対する認識度が向上する．

セキュリティ要請を受けている組織では，情報セキュリティ確保のため，教育など知識向上のための施策が講じられているものと推察する．またセキュリティ知識の高い組織構成員が所属する組織では，情報セキュリティを確保することを前提とした商品またはサービスを提供しているものと推察する．このため社内外からのセキュリティ要請が高まるも

のと推察する．以上より仮説H６を設定する．

Ｈ６：セキュリティ知識とセキュリティ要請との間には相関関係がある．

4.3.2. 仮説検証モデルの構築

Ｈ１～Ｈ５の仮説に基づく仮説検証モデルを図 4-2 にて構築する．なお図 4-2 中の符号は，正負のいずれに影響する仮説であるかをあらわしている．図 4-2 に示す仮説検証モデルに対して，4.5 節以降，認証の有無を考慮しない場合，および認証の有無それぞれの場合において仮説を検証するものとする．

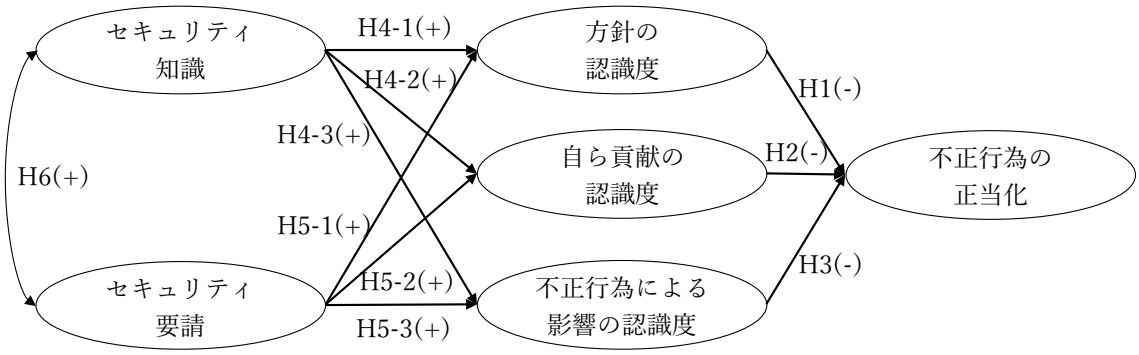

図 4-2　不正な情報持ち出し行為の正当化を抑制するための仮説検証モデル

4.4. 質問紙の設計

本節では 4.3 節で設定する因子に対して観測変数を定義し，質問紙調査の実施対象，回答者を設定する．なお観測変数はいずれも 7 段階リッカート尺度で評価するものとする．

4.4.1. 観測変数の設定

（１） 不正な情報持ち出し行為の正当化の観測変数

不正な情報持ち出し行為の正当化は，不正に情報を持ち出す行為を正当化しようとする考えに対する賛成の度合いをあらわす指標として定義する．関連研究では組織構成員がなぜ不正に情報持ち出す行為に至るのかについて分析し，その因子が抽出されている（濱田・廣松，2012；諏訪ほか，2012；竹村ほか，2015）．本章では，関連研究において抽出され

る因子に該当する事象が発生した場合，不正に情報持ち出す行為をやむを得ないと思うかを調査する．本章では関連研究を参考に，「ルールの妥当感のなさ」，「手間・ 効率」，「自己帰属意識」，「職場環境」，「例外業務の発生」，「多忙」，「ルールの有効性のなさ」の７項目に対する賛成の度合いを，不正な情報持ち出し行為の正当化を構成する観測変数として設定する．

（２）方針の認識度の観測変数

情報処理推進機構の Web サイトよれば，情報セキュリティ方針は，「なぜセキュリティが必要か」について規定するものとしている．これより方針の認識度は，なぜ情報を保護する必要があるのかについて認識している程度をあらわす指標として定義する．方針の認識度に対する観測変数は，ISMS ユーザーズガイド（日本情報経済社会推進協会，2014）における情報セキュリティ基本方針の策定事例を参考に抽出する．本章では「セキュリティの重要性」，「トップの意思」，「フレームワーク」，「実施すべき対策」，「組織の責任」の５項目に対する認識度合いを，方針の認識度を構成する観測変数として設定する．

（３）自らの貢献の認識度の観測変数

自らの貢献の認識度は，組織が持つ情報を保護することで組織や顧客にどのような貢献をもたらすことができるか，また情報を保護するために自身が何を実施すべきかを認識している程度をあらわす指標として定義する．自らの貢献の認識度に対する観測変数は，ISO/IEC 27001 規格（ISO, 2013）を参考に抽出する．本章では「関連文書」，「利害関係者からの期待」，「役割，責任および力量」，「機会」，「セキュリティ目的」の５項目に対する認識度合いを，自らの貢献の認識度を構成する観測変数として設定する．

（４）不正な情報持ち出し行為による影響の認識度の観測変数

不正な情報持ち出し行為による影響の認識度は，不正な情報の持ち出しがおこなわれることにより，組織に対してどのような影響が発生するかを認識している程度をあらわす指標として定義する．不正な情報持ち出し行為による影響の認識度に対する観測変数は，中小企業の情報セキュリティ対策ガイドライン第３版（情報処理推進機構，2019）における情報セキュリティ対策を怠ることで組織が被る不利益を参考に抽出する．本章では「業務の停止」，「取引の停止」，「対策コストの増大」，「損害賠償請求」，「社会的信用の低下」，「売

上の減少」の 6 項目に対して不正な情報持ち出し行為が発生した際の影響の認識度合いを，不正な情報持ち出し行為による影響の認識度を構成する観測変数として設定する．

（5）セキュリティ知識の観測変数

セキュリティ知識は，情報セキュリティの実現にあたって必要な対策が何かを理解している程度をあらわす指標として定義する．個人情報保護委員会（2017）は，講ずべき措置として，組織的，人的，物理的，技術的の 4 分類からなる安全管理措置を定めている．当該ガイドラインは個人情報保護法を準拠する観点からまとめた資料であるが，個人情報のみならず，一般的な情報資産でも適用可能である．本章では「組織的安全管理措置」，「人的安全管理措置」，「物理的安全管理措置」，「技術的安全管理措置」の 4 項目に対する理解度合いを，セキュリティ知識を構成する観測変数として設定する．

（6）セキュリティ要請の観測変数

セキュリティ要請は，情報セキュリティの実現に対して組織内外から要請を受けている程度をあらわす指標として定義する．セキュリティ要請の因子は，ISMS 適合性評価制度に関する調査報告書（情報マネジメントシステム認定センター，2018）における ISMS の導入の目的または動機，およびセキュリティ要請と不正に情報を持ち出す行為について関連研究（諏訪ほか，2012；濱田・廣松，2012）を参考に抽出する．本章では，「取引要件」，「顧客からの信頼」，「企業イメージ」，「優位性確保」の 4 項目に対する賛成の度合いを，セキュリティ要請を構成する観測変数として設定する．

4.4.2. 質問紙調査

上場企業では一定の基準を満たす内部統制の仕組みを適切に整備し，整備内容に従って運用されていることが求められている（東京証券取引所，2015）．上場企業およびその関連会社では，情報を管理するための体制が整備され，運用されているものと推察する．また第 3 章によれば製造業，情報通信業，建設業，卸売・小売業において，ISO/IEC 27001 が多く認証取得されている．

本章における質問紙調査の調査対象，対象となる回答者，調査実施期間を表 4-1 に示す．質問紙調査で使用した設問については付録 2 に示す．

表 4-1　質問紙調査概要

調査対象	Web調査会社に登録している者のうち、以下双方に該当する者 ・ 上場企業またはその関連会社に勤務する ・ 製造業、情報通信業、建設業、卸売・小売業のいずれかに勤務する
回答者	・ ISO/IEC 27001認証取得組織 ：143名 ・ ISO/IEC 27001未取得組織：166名 合計：309名
調査実施期間	2019年3月28～29日

4.5. 仮説の検証

4.5.1. 取得データの特徴

本章で設定する観測変数に対する，認証取得組織と未取得組織それぞれの平均値，標準偏差，認証取得組織の平均値と未取得組織の平均値の差，および平均値の差に対し有意水準を 5 %として Welch の t 検定をおこなった結果を表 4-2 に示す.

不正な情報持ち出し行為の正当化の各観測変数に対する平均値は，認証有無ともにおおむね 3 未満となっている．本調査の評価は 7 段階リッカート尺度で評価している．すなわち各観測変数において得られた平均値は評価尺度の中央値である 4 より少ない．認証有無にかかわらず組織構成員は，許可がないまま不正に情報持ち出してはならないと考えている傾向がある．不正な情報持ち出し行為の正当化の各観測変数に対する認証有無のそれぞれの平均値の差をみると，いずれの設問項目も有意な差がみられない．このことから不正な情報持ち出し行為の正当化しようとする考えに対する賛成の度合いには，認証取得組織と未取得組織との間で平均値に差があるとは言い切れない.

方針，自らの貢献，不正な情報持ち出し行為による影響に対する認識度の平均値は，認証取得組織において，すべての項目で 5 を超えており，未取得組織でも下限がセキュリティ目的の 4.651 である．認証有無にかかわらず，方針，自らの貢献，不正な情報持ち出し行為による影響に対する認識度は高い傾向がある．平均値の差をみるとすべての設問で認証取得組織のほうが大きく，またすべての因子で複数の設問項目に有意な差がみられる．方針，自らの貢献，不正な情報持ち出し行為による影響に対して認識を持たせることは，ISO/IEC 27001 の要求事項となっている．認証取得組織では，教育実施時,「なぜ ISO/IEC

表 4-2　認証有無による平均値の差の検定

潜在変数	設問項目	認証		未取得		平均の差
		平均	標準偏差	平均	標準偏差	
不正行為の正当化	ルールの妥当感	2.916	1.563	2.843	1.414	0.073
	手間・効率	2.804	1.521	2.819	1.345	-0.015
	自己帰属	2.804	1.576	2.801	1.436	0.003
	職場環境	2.706	1.605	2.681	1.397	0.026
	例外業務	3.035	1.576	2.970	1.386	0.065
	多忙	2.874	1.695	2.837	1.407	0.037
	ルールの有効性	2.916	1.647	2.759	1.419	0.157
方針の認識度	セキュリティの重要性	5.343	1.311	5.199	1.276	0.144
	トップの意思	5.217	1.262	4.813	1.395	0.404 **
	フレームワーク	5.196	1.223	4.819	1.403	0.377 *
	実施すべき対策	5.252	1.195	4.928	1.351	0.324 *
	組織の責任	5.301	1.222	5.066	1.232	0.234
自らの貢献の認識度	関連文書	5.203	1.172	4.825	1.353	0.377 **
	利害関係者からの期待	5.007	1.248	4.771	1.287	0.236
	役割、責任及び力量	5.273	1.170	4.916	1.337	0.357 *
	機会	5.105	1.315	4.735	1.317	0.370 *
	セキュリティ目的	5.070	1.191	4.651	1.357	0.419 **
不正行為による影響の認識度	業務の停止	5.350	1.296	5.036	1.409	0.314 *
	取引の停止	5.406	1.158	5.102	1.395	0.303 *
	対策コスト	5.462	1.243	5.211	1.329	0.251
	損害賠償	5.462	1.255	5.157	1.375	0.305 *
	社会的信用の低下	5.531	1.209	5.337	1.346	0.194
	売上の減少	5.434	1.196	5.127	1.317	0.307 *
セキュリティ知識	組織的安全管理	5.147	1.394	4.880	1.464	0.267
	人的安全管理	5.217	1.430	4.988	1.410	0.229
	物理的安全管理	5.049	1.450	4.771	1.459	0.278
	技術的安全管理	5.119	1.441	4.717	1.560	0.402 *
セキュリティ要請	取引要件	4.524	1.310	4.078	1.284	0.446 **
	顧客からの信頼	5.119	1.292	4.952	1.343	0.167
	企業イメージ	5.175	1.318	4.873	1.380	0.301
	優位性確保	5.028	1.278	4.765	1.321	0.263

** 有意水準１％で有意

* 有意水準５％で有意

27001 の認証取得が必要なのか」を周知すると同時に，方針，自らの貢献，不正な情報持ち出し行為による影響を認識させるような施策が講じられているものと推察する．セキュリティ知識に対し各観測変数において得られた平均値は 4 より大きい．認証有無にかかわらず組織構成員は，一定水準以上のセキュリティ知識を有している傾向がある．平均値の差をみると技術的安全管理のみ認証取得組織の方が有意に高い．ISO/IEC 27001 認証取得組織では，情報セキュリティ実現のため未取得よりも情報システムの導入が進んでいることが一因と推察する．セキュリティ要請に対し各観測変数において得られた平均値は 4 より大きい．認証有無にかかわらず，何らかのセキュリティ要請を利害関係者より受けている傾向がある．平均値の差をみると取引要件のみ認証取得組織の方が有意に高い．ISO/IEC 27001 認証は取引先からの要請を受けて取得されていることが一因と推察する．

4.5.2. 不正な情報持ち出し行為の正当化におよぼす影響の構造分析結果

本節では質問紙調査から得られたデータをもとに，設定する仮説に対する検証をおこなう．仮説の検証にあたっては，認証有無全体，認証の有無それぞれの場合に対しておこなう．また検証から得られた結果のうち特筆すべき事項に対して考察をおこなう．本章で収集しているデータは，一定の基準を満たす内部統制の仕組みを整備し，運用している組織に勤務しており，かつ ISO/IEC 27001 認証の取得件数が多い業界に所属する組織構成員から取得したものである．考察にあたっては上記データの特性を前提としておこなっている．仮説検証のための分析ツールは，AmosVer.25 を使用する．適合度指標は，CFI（Comparative Fit Index），RMSEA（Root Mean Square Error of Approximation）を使用する．本論文では小塩（2014）を参考に，CFI を 0.9 以上，RMSEA を 0.1 未満とする基準を設定する．

（1）認証有無全体に対する分析結果

図 4-2 の仮説検証モデルに対して，共分散構造分析をおこなった結果を図 4-3 に，各潜在変数におけるクロンバックの α 係数を表 4-3 に，各潜在変数に対する各観測変数の因子負荷量を表 4-4 に示す．

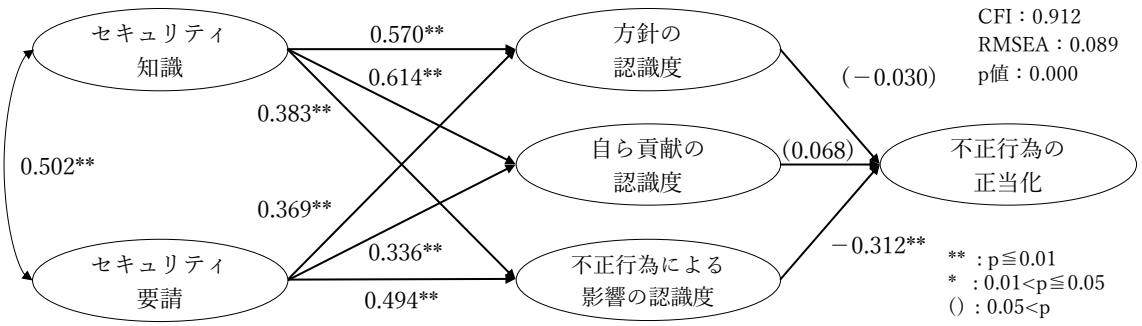

図 4-3　仮説検証モデルに対する分析結果（認証有無全体）（標準化済）

表 4-3　クロンバックの α 係数

潜在変数	設問数	クロンバックのα係数
不正行為の正当化	7	0.935
方針の認識度	5	0.936
自らの貢献の認識度	5	0.951
不正行為による影響の認識度	6	0.968
セキュリティ知識	4	0.951
セキュリティ要請	4	0.896

図 4-3 によると CFI は 0.9 を超えており，かつ RMSEA も 0.1 未満であることから，あてはまりが悪いモデルとは言い切れない．このため本モデルを採用する．表 4-3 ではクロンバックの α 係数が最も小さいもので 0.896 である．信頼性係数の値の大きさに関する判断は，尺度の目的によって異なるが，一般的に性格検査などでは 0.7 以上を満たすことが一つの基準とされている（豊田，2014）．表 4-4 ではすべての因子負荷量が正であり，かつ因子負荷量が最も小さいものでも 0.577 となっている．これより潜在変数を構成する各観測変数は妥当性を有しているとみなす．

表 4-4　潜在変数に対する因子負荷量

		潜在変数											
		不正行為の正当化		方針の認識度		自らの貢献の認識度		不正行為による影響の認識度		セキュリティ知識		セキュリティ要請	
観測変数	ルールの妥当感	0.858	**										
	手間効率	0.911	**										
	自己帰属	0.910	**										
	職場環境	0.927	**										
	例外業務	0.879	**										
	多忙	0.927	**										
	ルールの有効性	0.868	**										
	セキュリティの重要性			0.805	**								
	トップの意思			0.814	**								
	フレームワーク			0.939	**								
	実施すべき対策			0.933	**								
	組織の責任			0.837	**								
	関連文書					0.881	**						
	利害関係者からの期待					0.896	**						
	役割、責任および力量					0.928	**						
	機会					0.889	**						
	セキュリティ目的					0.863	**						
	業務の停止							0.909	**				
	取引の停止							0.915	**				
	対策コスト							0.933	**				
	損害賠償							0.931	**				
	社会的信用の低下							0.907	**				
	売上の減少							0.890	**				
	組織的安全管理									0.891	**		
	人的安全管理									0.921	**		
	物理的安全管理									0.930	**		
	技術的安全管理									0.892	**		
	取引要件											0.577	**
	顧客からの信頼											0.912	**
	企業イメージ											0.921	**
	優位性確保											0.918	**

** 有意水準 1 %で有意

* 有意水準 5 %で有意

（2）認証の有無による分析結果

仮説検証モデルに対して認証の有無による等値制約を置かずに多母集団分析をおこなった結果を図 4-4 に示す．図 4-4 では CFI が 0.9 に満たないものの RMSEA は 0.1 未満であり，あてはまりが悪いモデルとは言い切れない．このため本モデルを採用し，配置不変

性が確認されたものとする．配置不変性とは等値制約を置かないことで，集団間でパス図は同じであっても推定値はそれぞれ異なってもよいとの仮説をいう（豊田，2013）．

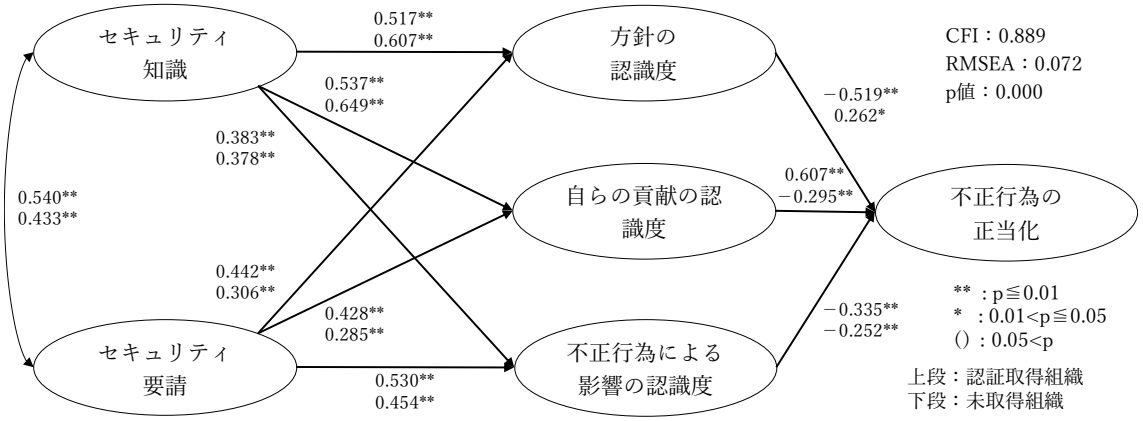

図 4-4　仮説検証モデルに対する分析結果（認証有無別）（配置不変モデル）（標準化済）

（3）母集団間の等質性の分析

図 4-4 より 1）方針の認識度から不正行為の正当化へのパス，および 2）自らの貢献の認識度から不正行為の正当化へのパスは符号が異なることから，これらのパスを除き，母集団間で等質性があると推察する．認証有無による母集団間の等質性を検討するため，制約条件を設定したモデルを構築し，モデルごとに適合度をまとめたものを表 4-5 に示す．モデルの比較にあたっては，赤池情報量規準（AIC：Akaike's Information Criterion）を採用する．表 4-5 のすべてのモデルにおいて各構成概念から任意の 1 つの観測変数へのパス係数，および観測誤差から観測変数へのパス係数は 1 に固定している．またパス係数に対する等値制約は，標準化をおこなっていない状態において設定している．

表 4-5 によれば，等値制約モデルが RMSEA および AIC が最も低い値を示している．これより 1）および 2）を除くパスにおいて，認証の有無による母集団間の等質性があるものと判断する．本章では等値制約モデルを採用し，認証有無による母集団間の特性を分析する．等値制約モデルに基づいて多母集団分析をおこなった結果を図 4-5 に示す．

表 4-5　認証有無による母集団間の等質性に対するモデル比較

モデル名	モデル説明	CFI	RMSEA	P値	AIC
配置不変モデル	等値制約を置かないモデル	0.889	0.072	0.000	2612.945
等値制約モデル	潜在変数間および潜在変数から観測変数へのパス係数に等値制約をおいたモデル．ただし以下に等値制約を置かないものとする． 1)方針の認識度から不正行為の正当化へのパス係数 2）自らの貢献の認識度から不正行為の正当化へのパス係数	0.888	0.071	0.000	2594.723

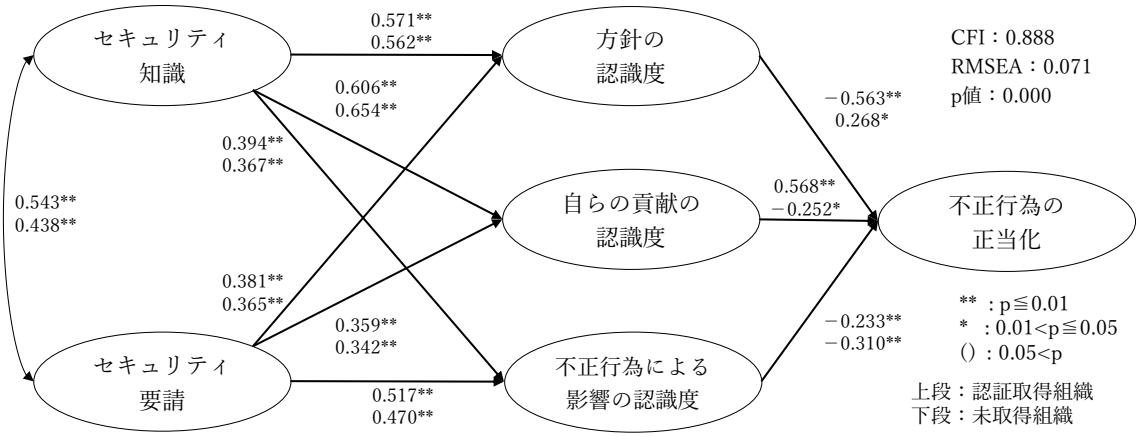

図 4-5　仮説検証モデルに対する分析結果（認証の有無別）
（等値制約モデル）（標準化済）

（4）仮説検証結果および考察

4.3.1. にて設定する仮説に対して図 4-2 および図 4-3 より，有意水準を 5 %として検定量が有意かどうか，および符号が設定した仮説と合致するかを検証した結果を表 4-6 にまとめる．表 4-6 における「○」は仮説が検証されている，「×」は有意であるものの仮説と異なる結論が得られている，「－」は有意でないため結論が得られていないことをあらわしている．

認証有無全体では，Ｈ１およびＨ２のみが検証されない．認証有無による分類をおこなわない状態においてセキュリティ方針を認識させること，および自らの貢献について認識させることは，不正な情報持ち出し行為の正当化を抑制するとは言い切れない．後述するが，方針および自らの貢献に対する認識は，認証有無により不正な情報持ち出し行為の正当化を抑制する効果と，抑制できない効果の双方が存在している．正と負の影響が相殺し合っているため，有意な結果が得られなくなっているものと推察する．

表 4-6　仮説検証結果

仮説		仮説検証結果		
		全体	認証取得	未取得
H1	方針に対する認識度の向上が，不正行為の正当化を抑制する．	－	○	×
H2	自らの貢献に対する認識度の向上が，不正行為の正当化を抑制する．	－	×	○
H3	不正行為による影響に対する認識度の向上が，不正行為の正当化を抑制する．	○	○	○
H4－1	セキュリティ知識が向上すると，方針に対する認識度が向上する．	○	○	○
H4－2	セキュリティ知識が向上すると，自らの貢献に対する認識度が向上する．	○	○	○
H4－3	セキュリティ知識が向上すると，不正行為による影響に対する認識度が向上する．	○	○	○
H5－1	セキュリティ要請が強まると方針に対する認識度が向上する．	○	○	○
H5－2	セキュリティ要請が強まると自らの貢献に対する認識度が向上する．	○	○	○
H5－3	セキュリティ要請が強まると不正行為による影響に対する認識度が向上する．	○	○	○
H6	セキュリティ知識とセキュリティ要請との間には相関関係がある．	○	○	○

認証有無に分けてみると，認証取得組織においてH2は仮説と異なる結論が得られている．すなわち自らの貢献に対する認識度が向上すると，不正な情報持ち出し行為を正当化してしまう．このことから認証取得組織では，方針および不正行為による影響についての認識を向上させることが有効な施策であると考える．表 4-2 より自らの貢献に対する認識度は，すべての観測変数で認証取得組織の方が未取得組織よりも平均が高く，複数の項目で有意である．このことから認証取得組織の構成員のほうが未取得組織と比べて，自社の規定や情報セキュリティ上達成すべき目的をはじめとした自らの貢献に対する認識度が高い．このとき組織構成員は，どの程度の対策を講じていれば顧客満足度の低下や，インシデントが起きないのかについて，講じるべき対策の基準を自ら設定してしまうものと推察する．自らの貢献に対する認識度が高まることにより，自ら設定する基準と照らし合わせて「この程度であれば，組織の許可がなくとも情報を持ち出して構わない」とする意識が高まるため，不正な情報持ち出し行為を正当化してしまうものと推察する．

未取得組織におけるH 1 は仮説と異なる結果が得られている．方針に対する認識度が向上すると、不正な情報持ち出し行為を正当化してしまう．このことから未取得組織では，自らの貢献および不正行為による影響についての認識を向上させることが有効な施策であると考える.情報マネジメントシステム認定センター(2018)によると認証取得組織の 80%以上が，ISMS 導入の目的または動機の設問のうち「入札，受注の条件，取引先からの要請による」に対して「該当する」または「やや該当する」と回答している．これより多くの組織では，情報セキュリティ体制の整備が取引要件となっていることをきっかけの一つとしてISMS の導入を含む情報セキュリティに取り組んでいると考える．これに対し表 5-2 より，未取得組織では情報セキュリティに対する取引先からの要請が弱い．このため，「なぜセキュリティが必要か」を認識させても，不正に情報を持ち出す行為が取引停止を引き起こし，組織に損害を与えることについて実感がわいていないことが原因であると推察する．

4.6. 結論

本章の目的は，ISO/IEC 27001 規格における「認識」の要求事項のうち，どの項目に注力すれば不正な情報持ち出し行為の正当化が抑制できるのかについての知見を得ることである．このため関連研究で得られる知見を用いて仮説の設定，仮説検証モデルの構築をおこない，質問紙調査で得られるデータをもとに，認証有無全体に対する共分散構造分析，さらに認証取得組織および未取得組織それぞれの集団に対する多母集団分析により，仮説の検証をおこなっている．仮説の検証を通じて正当化を抑制するためのメカニズムを解明し，組織が講じるべき施策を提案している．

認識の要求事項における，方針，自らの貢献，不正な情報持ち出し行為による影響の 3 項目それぞれが不正な情報持ち出し行為の正当化を抑制する効果について分析をおこなった結果，次の事項を確認している．セキュリティ知識が向上する，もしくはセキュリティ要請や強まると，方針，自らの貢献，不正行為による影響の認識度がいずれも向上する．不正行為による認識度の向上は，認証有無いずれにおいても不正行為の正当化を抑制する効果がある．これに対し方針の認識度および自らの貢献の認識度は，認証の有無により効果を有する項目と，有さない項目が異なることを確認している．以上より，不正な情報持ち出し行為の正当化を抑制するため，認証取得組織では方針および不正行為による影響に

ついての認識を向上させることが有効な施策である．未取得組織では自らの貢献および不正行為による影響についての認識を向上させることが有効な施策である．

本章での検証結果は，ISO/IEC 27001 規格を適用する場合に，他社事例などに合わせて画一的に適用すると，インシデントの抑制など期待する効果が得られない可能性があることを示唆している．ISO/IEC 27001 規格を適用する際，組織は，情報セキュリティに対する成熟度や，組織を取り巻く状況に応じて，どの要求事項に注力すべきかを検討する必要がある．

認証取得組織では，自らの貢献の認識度の向上による不正な情報持ち出し行為の正当化への効果が正の値（抑制効果を有さない）となっている．また未取得組織では，方針の認識度の向上による不正な情報持ち出し行為の正当化の効果が正の値となっている．本章では不正な情報持ち出し行為の正当化について部分的に考察している．しかし認証取得組織では自らの貢献に対する認識を，未取得組織では方針の認識を持たせるべきでないと結論づけるには，それぞれの認識を持たせた組織構成員についての分析が必要となる．このことについては今後の研究課題である．

第５章　不正な情報持ち出しの機会抑制のための施策

5.1. 背景と目的

本章では，不正のトライアングル理論のうち「機会」を抑制するためにどのような施策を講じるべきかを考察する．具体的には，組織が講じる活動（促進活動）に着目し，情報セキュリティを推進する者の観点から，どのような手段で管理策を提供すれば，不正な情報持ち出し行為における機会の抑制（管理策の遵守）につなげることができるのかをあきらかにする．また職種による不正に情報を持ち出す行為への影響の比較を通じて，職種に応じた施策を探る．これにより附属書 A の観点における ISO/IEC 27001 規格採用の際の問題点をあきらかにする．本章の対象についての概念図は図 5-1 に示す．分析にあたっては仮説の設定および仮説検証モデルを構築し，上場企業かつ ISO/IEC 27001 認証の取得件数が多い業種の組織構成員を対象とした質問紙調査により取得するデータに対し，職種全体に対する共分散構造分析，さらに職種別の多母集団分析により，仮説検証をおこなう．仮説の検証を通じて機会を抑制するためのメカニズムを解明し，組織が講じるべき施策を提案する．

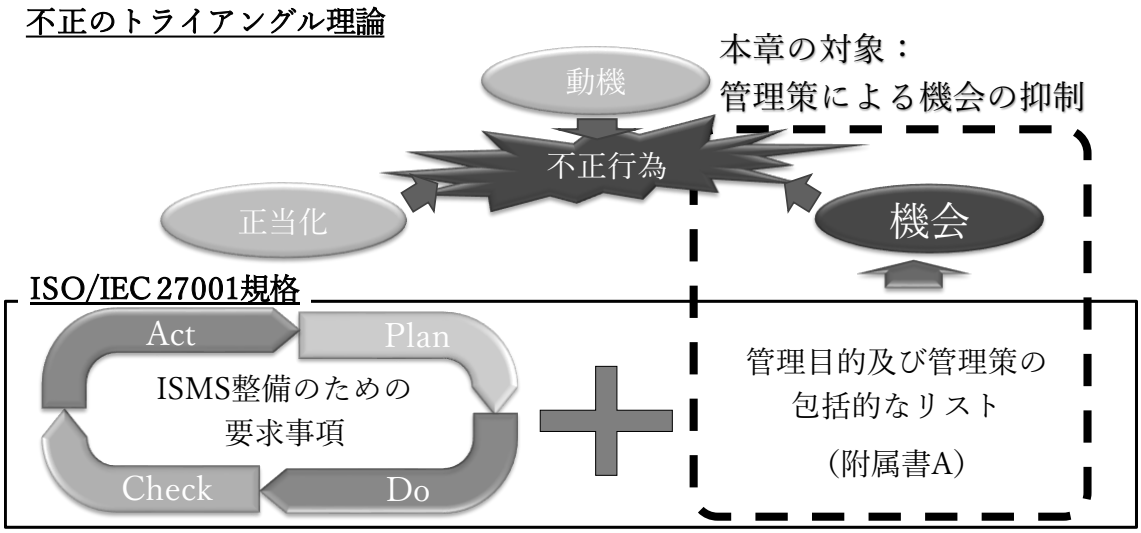

図 5-1 本章の対象

組織にとって，保護すべき情報が漏えいすることは，ノウハウの流出や社会的な信用の失墜などにつながり，事業の継続を脅かす重大な問題となる場合がある．情報漏えいを抑制するため多くの組織では，許可のない情報の持ち出しを禁ずる取り決め（管理策）を設

定し，管理策を遵守させるための施策を講じている．

不正に情報を持ち出す行為を抑制するには，管理策を定め，組織構成員に遵守させなければならない．組織構成員に対し，管理策を自動的かつ強制的に遵守させるための活動としては，IT を用いた「自動化の整備」がある．しかし管理策を遵守させるためには，自動化の整備のみでは限界があり，人的対策を含むマネジメントの面での活動も求められる（岡野・奥山，2017）．マネジメント面での活動には，管理策を文書化するための「マニュアルの整備」が必要である（竹村ほか，2015）．組織構成員に対して管理策を遵守させるためには，必要な知識や教養を得させるため，または管理策の遵守を意識させるための活動である「教育・動機付けの実施」も必要となる．

本論文では，組織構成員に対して管理策の遵守を促すため，組織が講じる活動として，「教育・動機付けの実施」，「マニュアルの整備」，「自動化の整備」があるものとし，これらを総称して「促進活動」とよぶ．組織は，促進活動を選択もしくは組み合わせることにより，組織構成員に適用している．組織にとって有限である経営資源を，効果的かつ効率的に配分するには，「教育・動機付けの実施」，「マニュアルの整備」，「自動化の整備」のそれぞれが，管理策遵守に対してどの程度寄与しているかを把握することが有用である．これにより組織は，管理策を遵守させるために注力すべき促進活動をあきらかにすることができる．さらに不正に情報を持ち出す行為に対する意識が職種により異なる（島，2012）ことを考慮すると，職種に応じた促進活動の効果を把握することで，組織は，より適切な施策を講じることができる．

本章では，不正のトライアングル理論のうち「機会」を抑制するための施策について検討する．具体的には，組織構成員に管理策を遵守させることを通じて，促進活動の観点から組織が講じるべき施策についての知見を得ることを目的とする．目的達成のため，「教育・動機付けの実施」，「マニュアルの整備」，「自動化の整備」が，管理策の遵守におよぼす影響を比較する．また情報漏えいを抑制するにあたり，組織が講じる施策に効果をもたせるため，管理策の策定状況から情報漏えいの抑制へ至るまでの因果関係の構造の解明を試みる．解明のための手法として本章では，仮説を設定し，検証モデルを構築する．また上場企業かつ ISO/IEC 27001 認証取得件数の多い業種の組織構成員を対象とした質問紙調査により取得するデータを，共分散構造分析の手法を用いて仮説を検証する．さらに職種について多母集団分析をおこない，職種に応じた施策について考察する．

5.2. 関連研究

甘利ほか（2012）は，不正に情報を持ち出す行為の成立要件を崩す手法として，２つの考え方に基づく防犯の方法論があるとしている．１つは，犯罪者が犯罪者たるに至った社会原因を究明し，それを除去することより，犯罪を抑制する「犯罪原因論」である．もう１つは，犯罪者に犯罪の機会を与えないことによって，犯罪を未然に抑制する「犯罪機会論」である. 本章では, 仮説設定の骨子となる仮説検証モデル構築するため,「犯罪原因論」および「犯罪機会論」の観点から，管理策の遵守と情報漏えいの関係についての関連研究を紹介する．関連研究の紹介を通じて，本章であきらかにすべき観点および本章のアプローチを述べる.

5.2.1. 不正に情報を持ち出す行為の要因分析に関する研究

不正に情報を持ち出す行為の要因は，犯罪原因論の観点から,「なぜ組織構成員は管理策を守らないのか」をテーマとして分析されている．不正に情報を持ち出す行為を引き起こす要因分析には，計画的行動理論（Ajzen, 1985；Ajzen, 1991）が広く用いられている．計画的行動理論によれば，不正に情報を持ち出す行為は，不正に情報を持ち出す行為を起こそうとする意図の発生により引き起こされる．不正に情報を持ち出す行為を起こそうとする意図の関連研究として浜屋（2009）は，組織感情と情報セキュリティ対策の関係を分析し，情報セキュリティ対策への否定的な意識が，職場の組織感情に影響を受けることを確認している．菅野・島田（2010）は，情報セキュリティ対策の実施が困難である要因（阻害要因）として，管理策の遵守に対して，職場・組織への感情や，コスト，手間・効率などの感情があることを確認している．濱田・廣松 (2012) は，職場や組織に対する感情や，管理策の妥当感が不正に情報を持ち出す行為におよぼす影響を分析している．諏訪ほか（2012）は，セキュリティ知識が管理策に対する感情を通じて不正に情報を持ち出す行為に至る構造について，仮説検証モデルを構築している．仮説の検証を通じて諏訪ほかは，セキュリティ行動を，予防的行動，習慣的行動，意識的行動に分類し，行動に応じた施策を提案している．竹村ほか（2015）は，抵抗感のなさやポリシ違反意図などの要因が，情報漏えいにつながる行動に影響をおよぼすことを確認している．岡野・奥山（2017）は，持ち出し経験を有するものと有しないものとの比較を通じて,「早急に対応する必要がある」や「仕事が終わらない」といったプレッシャーにさらされることが，不正に情報を持

ち出す行為の根本的な原因であることを確認している．

5.2.2. 促進活動の効果に関する研究

犯罪機会論を用いた不正に情報を持ち出す行為は，「策定した管理策をどのように遵守させるか」および「どのような管理策を策定するか」をテーマとして，その要因が分析されている．「策定した管理策をどのように遵守させるか」の関連研究は，教育・動機付けの実施，マニュアルの整備，自動化の実施が存在する．以下にて各々についての関連研究を示す．

教育・動機付けの実施について菅野ほか（2009）は，組織構成員が情報セキュリティ対策を講じるにあたっての動機要因と阻害要因を分析したうえで，情報セキュリティに対する意識向上と対策の手順を普及させるための教育が必要であると提言している．諏訪ほか（2012）は，セキュリティ知識が向上するとコスト感が上昇し，情報セキュリティ行動に対して負の影響をおよぼすとしている．岡野・奥山（2017）は，研修などで知識を高めることは，不正に情報を持ち出す行為に限定して述べると，抑止効果があるとは言いがたいとしている．しかし，不正に情報を持ち出す行為が原因で引き起こされた情報漏えい事故によって，どんな影響があるかを認知させることは有効であるとしている．

マニュアルの整備について鈴木・真田（2008）は，情報セキュリティポリシー関連文書に各担当者の役割分担や責任権限を明確にすることが必要であるとしている．濱田・廣松（2012）は，管理策の記載内容の妥当感の強さ（または弱さ）の度合いが，管理策の遵守に影響を与えないことを確認している．吉野（2014）は，マニュアルに基づく業務遂行の組織化を可能とした，マニュアルのデザインの手段とその機能を分析し，その特徴を整理している．

自動化の整備について荒井ほか（2004）は，ファイルの暗号化が，取り扱い資格（復号鍵）をもつ不正に情報を持ち出す行為に対抗できないことを指摘している．そのうえで荒井ほかは，復号化された機密情報をユーザの悪意や過失から保護する強制アクセス制御方式と，暗号機能を組み合わせた方式を採用した情報漏えいを抑制するための情報システムを提案している．

5.2.3. 管理策の策定に関する研究

「どのような管理策を策定するか」について，中村ほか（2004）は，資産・脅威・対策

の関係をモデル化し，適用する管理策の最適な組み合わせを論理的に求める手法を導出した結果，セキュリティ対策選択問題が離散最適化問題として定式化されることを示している．芝口ほか（2010）は，対策に徹底度を付与したうえで，一定期間ごとに仕事量を評価し，徹底度と仕事量をもとに取るべき対策を決定する手法を提案している．鈴木ほか（2011）は，情報セキュリティ対策が相互に依存する関係に注目し，内部犯行に対する情報セキュリティ体制の有効性を評価し，不足する対策を指摘する手法を提案している．品川・橋本（2015）は，管理策を軽視している場合や，管理策が必要以上に厳格な場合に管理策違反が発生するとしたうえで，情報の保護と利用の調和をはかり，妥当な管理策の範囲を探ることが必要であると指摘している．

5.2.4. 本章の観点

犯罪原因論の観点による関連研究では，5.2.1 項より，組織風土，セキュリティ知識，管理策に対する感情，外部要請を含む例外業務の発生などが，不正に情報を持ち出す行為の抑制を阻害する要因とされている．犯罪機会論における「策定した管理策をどのように遵守させるか」の観点では，5.2.2 項より，教育・動機付けの実施，マニュアルの整備，自動化の整備それぞれが，どのように充実させるべきかが提案されている．「どのような管理策を策定するか」の観点では，5.2.3 項より，策定する管理策の決定手法が提案されている．

本章では，犯罪機会論の観点から，組織構成員に管理策を遵守させることで，情報漏えいを抑制するための施策を検討する．このため本章では，教育・動機付けの実施，マニュアルの整備，自動化の整備からなる促進活動に着目し，それぞれが管理策の遵守におよぼす影響を比較分析する．併せて，管理策の策定状況が，促進活動の充実度の向上におよぼす影響を探る．これらの観点は，関連研究で得られる知見に加え，どのような管理策を策定すべきかの検討や，どの促進活動に注力すべきかの検討の一助となり，限られた経営資源を適切に配分するうえで有用であると考える．

5.2.5. 本章のアプローチ

本章では，管理策の策定状況から促進活動の充実，管理策の遵守を介して情報漏えいの抑制へ至るまでの因果関係について仮説検証モデルを構築し，実証分析をおこなう．実証分析を通じて，本章では，促進活動の観点から，情報漏えい抑制に寄与する施策についての知見を得ることを目的とする．実証分析は，情報漏えい抑制に関する質問紙調査により

得られるデータを，分析することにより実施する．

5.3 節では，以下①～③を分析するために，促進活動の充実度を定義したうえで仮説を設定し，仮説検証のモデルを構築する．

① 組織構成員が管理策を遵守することによる情報漏えい抑制効果

② 各促進活動がおよぼす管理策遵守効果の比較

③ 管理策の策定状況が促進活動の充実度におよぼす影響

5.4 節では，実証分析にあたっての具体的な質問項目の設計について述べる．さらに情報漏えい抑制に影響をおよぼす要因として，必要となる観測変数についても 5.4 節にて述べ，質問紙を設計する．5.5 節では，仮説の検証結果を記載する．不正に情報を持ち出す行為に対する共感度が職種により異なる（島，2012）ことを考慮すると，職種に応じた施策の効果を探ることで，組織は有効な施策を検討できると推察する．職種に応じた施策を提案するために，多母集団分析を用いて職種による特性の有無を探る．5.6 節では，分析結果をもとに，情報漏えい抑制に寄与する施策について考察する．5.7 節では，本章による貢献および課題を述べる．図 5-2 にて，本章で前提とする基本モデルを示す．図 1 中の符号は，基本モデルにおける各段階が，正または負のいずれに影響を与えているかをあらわしている．

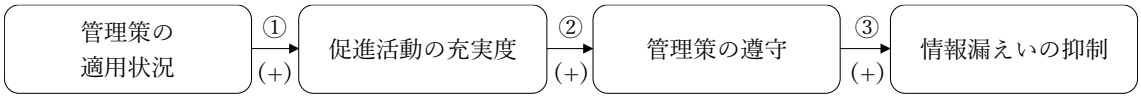

図 5-2　情報漏えい抑制のための基本モデル

5.3. 仮説の設定および仮説検証モデルの構築

5.3.1 促進活動の充実度

本項では，図 5-2 の基本モデルの基礎となる促進活動の充実度について，関連研究を紹介する．また関連研究をもとに，本章にて使用する，教育・動機付け，マニュアル，自動化それぞれの充実度を定義する．

（1）教育・動機付けの充実度

菊地・中條（2000）は，a）標準を知らなかったミスは，教育の計画度，教育の完全度，教育の評価度が影響をおよぼす．b）標準どおりできなかったミスは，訓練の完全度，訓練の評価度が影響をおよぼす．c）標準どおり従う気がなかったミスは，必要性の指導度，観察の徹底度が影響をおよぼすことを確認している．標準とは，プロセスに関する性能，能力，配置，状態，動作，手順，方法，手続き，責任，義務，権限，考え方，概念などが時間とともに変わらないように定めた取り決めをいう（中條，2010）．本章において標準は，管理策と同義のものとする．

本章では，菊地・中條（2000）における「a）標準を知らなかったミス」および「c）標準どおり従う気がなかったミス」を参考に，「計画的実施」，「遵守事項の網羅」，「理解度評価」，「必要性の周知」，「遵守状況の観察」より構成される概念を，「教育・動機付けの充実度」として取り扱う．なお「b）標準どおりできなかったミス」は，管理策に従い作業をおこなうための，必要な技能を習得していなかったことにより発生するミスである管理策を遵守させる目的においては，実施にあたり高度な技能は要求されない．このため「b）標準どおりできなかったミス」は除外する．

（２）マニュアルの充実度

吉野（2014）は，航空整備現場のメンテナンスマニュアルが a）通過点を設置する，b）更新情報を流さない，c）ほかのルーティン（メンテナンスマニュアル）を見せない，d）証拠を残す，e）免罪符として活用する，f）曖昧さを解消する，を満たすようデザインされていることを確認している．このうち管理策遵守の観点からマニュアルの整備に要求される事項は，c)，f)である．c）は，若手の場合，メンテナンスマニュアル以外にあるいろいろなマニュアルを参照して作業することが困難なことから，提案されているデザイン手段である．このことから c)は，１つのマニュアルに遵守すべき事項が「集約」されている状態とする．また f）は，個人の判断の必要がないほど管理策が「具体化」されている状態，および記載されたもののみを遵守すればよいほど管理策が「詳細化」されている状態とする．

マニュアルの整備にあたっては，作業を標準化したうえで文書化する必要がある．中條ほか（1999）は，作業を標準化する方法を，マニュアルを作るかどうかの判断基準，標準書の作成者，標準書の内容確認，標準書の管理，標準書の見直しの５つの観点に分類している．これら５つの観点について中條ほかは，数量化Ⅲ類により分析し，作業を標準化する方法を特徴づける軸として，標準の網羅度と現場との密着度を抽出している．標準の網

羅度は，本章において「管理策の数」とよぶ．中條ほかは，密着度が低い職場の場合，標準の内容の不適切さが目立つと指摘している．これは作成者が現場を理解できないままマニュアルを作成した場合，マニュアルの内容が誤ったものとなるため，管理策に従って業務を遂行できなくなることを示唆している．このため現場との密着度は，「業務との整合」，「定期的見直し」と読み替える．

本章では，「集約」，「具体化」，「詳細化」ならびに「管理策の数」，「定期的見直し」，「業務との整合」より構成される概念を，「マニュアルの充実度」として取り扱う．

（３）自動化の充実度

IT 管理のためのベストプラクティス集である COBIT では，ビジネス目標を達成するために従うべき統制基準として，有効性，効率性，機密性，完全性，可用性，コンプライアンス，信頼性の７つを定めている（ISACA, 2012）．このうち「完全性」は，情報の誤りや漏れがないことを確保するための指標であるため，組織構成員による不正に情報を持ち出す行為に影響をおよぼさない．また「コンプライアンス」においても情報が仕様に準拠していることを確保する指標であるため，組織構成員による不正に情報を持ち出す行為に影響をおよぼさない．そこで本章では，完全性，コンプライアンスを除外した「有効性」，「効率性」，「機密性」，「可用性」，「信頼性」より構成される概念を，「自動化の充実度」として取り扱う．

5.3.2. 仮説の設定

情報漏えい抑制の効果を示すには，管理策の遵守と情報漏えい抑制との因果関係を実証する必要がある．図１における①に基づき，仮説としてＨ１を設定する．

Ｈ１：　　管理策が遵守されると情報漏えいが抑制される．

教育・動機付けの実施と管理策遵守の因果関係は，諏訪ほか（2012）や岡野・奥山（2017）により実証されている．マニュアルの整備と管理策遵守の因果関係は，濱田・廣松（2012）によりマニュアルの記載内容の妥当感が，管理策遵守におよぼす影響について実証されている．しかし自動化の整備と管理策遵守の因果関係は，関連研究において実証されていない．管理策の遵守に対して，どの促進活動が効果的かを示すには，管理策遵守に対する教育・動機付けの実施，マニュアルの整備，自動化の整備それぞれの効果について，条件を同一にして比較する必要がある．図１における②に基づき，仮説としてＨ２－１～Ｈ２－

３を設定する．

Ｈ２－１：教育・動機付けの充実度が増すと管理策の遵守につながる．

Ｈ２－２：マニュアルの充実度が増すと管理策の遵守につながる．

Ｈ２－３：自動化の充実度が増すと管理策の遵守につながる．

関連研究では，組織風土，セキュリティ知識，管理策に対する感情，例外業務の発生などが，不正に情報を持ち出す行為の抑制を阻害する要因として抽出されている．このうち例外業務は，社外からの要請や緊急時の対応など，やむを得ない場合に発生する業務であり，組織構成員が管理策を遵守する意図を持っていたとしても，その意図を曲げ，不正に情報を持ち出す行為に向かわせる要因となりうる．このため例外業務は，促進活動の充実度が管理策の遵守におよぼす効果にも影響するものと推察する．これより本章では，Ｈ３を仮説として設定し，図２における仮説検証モデルに組み込むものとする．

Ｈ３：　　例外業務が増えると管理策の逸脱度が増す．

教育・動機付けは，整備する管理策を周知する目的が含まれる．マニュアルが充実すると周知すべき管理策が増加する．マニュアルが教育・動機付けの充実に影響をおよぼすものとし，Ｈ４を仮説として設定する．

Ｈ４：　　マニュアルの充実度が増すと，教育・動機付けの充実度が増す．

管理策の策定状況が促進活動におよぼす影響を実証するためには，管理策の策定状況と促進活動の因果関係を示す必要がある．図１における③に基づき，仮説としてＨ５－１～Ｈ５－６を設定する．

Ｈ５－１：　管理策の厳しさが増すと教育・動機付けの充実度が増す．

Ｈ５－２：　管理策の数が増えると教育・動機付けの充実度が増す．

Ｈ５－３：　管理策の厳しさが増すとマニュアルの充実度が増す．

Ｈ５－４：　管理策の数が増えるとマニュアルの充実度が増す．

Ｈ５－５：　管理策の厳しさが増すと自動化の充実度が増す．

Ｈ５－６：　管理策の数が増えると自動化の充実度が増す．

情報セキュリティ意識が高い組織では，厳しさ，管理策の数の双方を充実させているものと考える．このためＨ６を仮説として設定する．

Ｈ６：　　管理策の厳しさと管理策の数には正の相関がある．

5.3.3. 仮説検証モデルの構築

Ｈ１～Ｈ６で設定する仮説を検証するためのモデルを図 5-3 に構築する．図 5-3 中の符号は，正負のいずれに影響する仮説かをあらわしている．

島（2012）は，職種により，不正に情報を持ち出す行為に対する意識が異なることを確認している．そこで本章では，図 5-3 で構築する仮説検証モデルに対し，多母集団分析の手法を用いて，職種による特性の有無を探る．

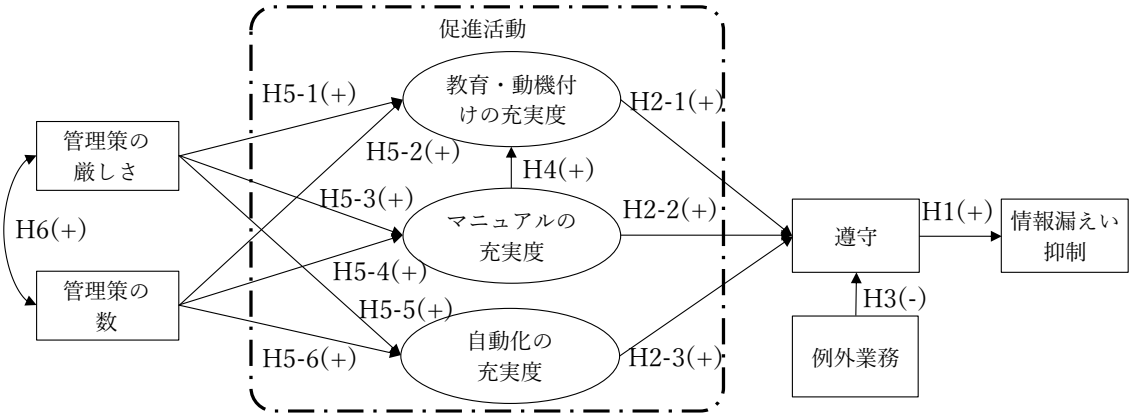

図 5-3　情報漏えい抑制のための仮説検証モデル

5.4. 質問紙の設計

本節では，質問紙の設計にあたり，仮説検証モデルに含める観測変数と，潜在変数を構成する観測変数について記述する．

5.4.1. 観測変数の設定

（１）管理策の遵守および漏えいの観測変数

管理策の遵守に対しては，管理策が遵守されている状態について，「非常にあてはまる」から「全くあてはまらない」の７段階リッカート尺度で回答を得る．情報漏えいに対しては，情報漏えいが発生していない状態を３，情報漏えいが発生している状態を１とし，「わからない」は欠損値として回答を得る．

（２）促進活動の潜在変数および観測変数

教育・動機付けの充実度は,「計画的実施」,「遵守事項の網羅」,「理解度評価」,「必要性の周知」,「遵守状況の観察」を観測変数とする構成概念である．マニュアルの充実度は,「具体化」,「詳細化」,「管理策の網羅」,「定期的見直し」,「業務との整合」を観測変数とする構成概念である．自動化の充実度は,「有効性」,「効率性」,「機密性」,「可用性」,「信頼性」を観測変数とする構成概念である．各観測変数は,「非常にそう思う」から「全くそう思わない」の7段階リッカート尺度で測定する．

（3）例外業務の観測変数

関連研究では，犯罪原因論の観点から，業務を遂行するにあたっては，取引先からの要請や緊急時など，管理策に反して，例外的な処理が必要な業務（以下「例外業務」という．）が発生する場合がある．例外業務は，不正に情報を持ち出す行為を引き起こすことが指摘されている（諏訪ほか，2012；竹村ほか，2015；岡野・奥山，2017）．本章では，管理策の遵守に影響をおよぼす要素として，例外業務による影響を考慮する．例外業務は，頻度が「頻繁にある」から「全くない」の7段階リッカート尺度で測定する．

（4）管理策の策定状況の観測変数

管理策の策定状況は，数多くの管理策を採用する，もしくは，厳しい管理策を採用するといったものが考えられる．これより本章では,「管理策の数」および「管理策の厳しさ」を管理策の策定状況の観測変数として採用する．

本章は，不正に情報を持ち出す行為を抑制するための管理策を対象としている．このため質問紙調査では，被験者が所属する組織における管理策の採用状況を確認している．表5-1 は，組織の管理下にある情報が，管理外に移動する際に講じるべき管理策を抽出したものである．

表5-1 における「附属書A」欄は，管理策抽出にあたり，参考としたISO/IEC 27001規格（ISO, 2013）の附属書Aの項番をあらわしている．また管理策の具体的な実現方法は，ISO/IEC 27002（ISO, 2014b）を参考にしている．回答者からは，表5-1のうち，所属する組織で採用されている管理策について回答を得るものとする．「管理策の厳しさ」は,「非常に厳しい」から「全く厳しくない」の7段階リッカート尺度で測定する．

表 5-1　不正に情報を持ち出す行為を抑制するための管理策

項目	管理策	附属書A
論理的 アクセス制御	業務上必要な範囲を超えた情報に対する、サーバやデータベース、ネットワーク経由のアクセスが制限されている（例：他部署のファイルサーバへのアクセス制限など）	A.9.1.2 A.9.2.1 A.9.4.1
物理的 アクセス制御	業務で利用する情報を取り扱う執務室への入退室管理や、重要な情報を保存するキャビネットの施錠など、物理的なアクセス制御が行われている	A.11.1.1 A.11.1.2 A.11.1.3
物理的な 情報持ち出し制限	業務で利用する情報が記録されている紙、外部記憶媒体（USBメモリなど）、PCを執務室外に持ち出すことが制限または禁止されている	A.11.2.5
会社貸与PCからの 情報持ち出し制限	シンクライアント（ハードディスクを持たないPC）化、暗号化など会社貸与PCに対する書き込みまたは書き出しが制限されている	A.6.2.1
私物媒体の 利用制限	私物の外部記憶媒体（USBメモリなど）や私物PCの業務利用が制限または禁止されている	A.8.3.1
会社貸与の 外部記憶媒体 利用制限	会社貸与の外部記憶媒体（USBメモリなど）の利用が制限または禁止されている（外部記憶媒体が強制的に暗号化されている場合を含む）	A.8.3.1
外部通信制限	外部サイトへのファイルのアップロード、電子メールの送信制限など、業務上重要な情報を社外とやり取りする場合の通信が制限または禁止されている	A.13.2.3
プリントアウト制限	業務で利用する情報のプリントアウトが制限または禁止されている	A.11.2.9
情報のラベル付け	業務で利用する情報に対して必要に応じたラベル付け（『社外秘』、『厳秘』などの表記）がされている	A.8.2.1 A.8.2.2 A.8.2.3
持ち出し状況 の監視	業務で利用する情報の持ち出し状況が監視されている	A.9.1.2 A.12.4.1

5.4.2. 質問紙調査

菅野・島田（2010）によれば，組織の規模に応じて，阻害因子による影響度合いが異なる．このため管理策を遵守させるための施策は，組織の規模や業態により異なるものと推察する．東京証券取引所（2015）では，上場のため，一定の基準を満たす内部統制の仕組みを適切に整備し，整備内容に従って運用されていることを求めている．内部統制とは，財務報告の信頼性や資産の保全などの 4 つの目的を達成するために，事業に組み込まれ，組織内のすべての者によって遂行されているプロセスである（八田，2006）．このため上場企業またはその関連会社では情報を管理するための体制が整備され，運用されているものと推察する．また第 3 章では，製造業，情報通信業，建設業，卸売・小売業において，ISO/IEC 27001 規格が多く認証取得されていることを確認している．ISO/IEC 27001 認証は，情報セキュリティの管理体制（マネジメントシステム）が整備され，要求事項に照らして適合していることを，審査機関が審査することで付与される．保護すべき情報多く保有してい

る組織は，情報漏えいを抑制するための体制を整備する必要があるため，ISO/IEC 27001 認証においても，取得組織が増加するものと推察する．

島（2012）によれば，不正に情報を持ち出す行為に対する共感度は，職種により異なっている．営業・販売・サービス系は，顧客情報や，製品またはサービスの価格などの営業情報を主に扱っている．技術・専門職系は，技術情報を主に扱っている．これに対し，事務・企画・管理系は，経営管理に関する情報を主に扱っている．このように職種に応じて取り扱う情報が異なるため，講じるべき施策は，職種に応じて異なるものと推察する．

以上を踏まえ，質問紙調査の概要を表 5-2 に示す．

表 5-2　質問紙調査の概要

調査対象	Web調査会社に登録している者のうち、以下双方に該当する者 ・ 上場企業またはその関連会社に勤務する ・ 製造業、情報通信業、建設業、卸売・小売業のいずれかに勤務する
回答者	・ 営業・販売・サービス系 ：100名 ・ 事務・企画・管理系 ：100名 ・ 技術・専門職系 ：100名 合計：300名
調査実施期間	2016年3月5～7日

5.5. 仮説の検証

本節では図 5-3 で示すモデルに対し，質問紙調査を通じて取得したデータを用いて仮説検証をおこなう．仮説検証のための分析ツールは，AmosVer.25 を使用する．分析データには欠損値が含まれるため，完全情報最尤推定法でパラメータ推定をおこなっている．適合度指標は，4 章と同様に CFI および RMSEA を使用する．適合か否かの判断基準についても 4 章と同様に，CFI を 0.9 以上，RMSEA を 0.1 未満とする．

5.5.1. 仮説検証モデルに対する共分散構造分析結果（職種全体）

図 5-3 の仮説検証モデルに対し，共分散構造分析をおこなった結果を図 5-4 に，各潜在変数におけるクロンバックの α 係数を表 5-3 に，各潜在変数に対する各観測変数の因子負荷量を表 4-4 に示す．

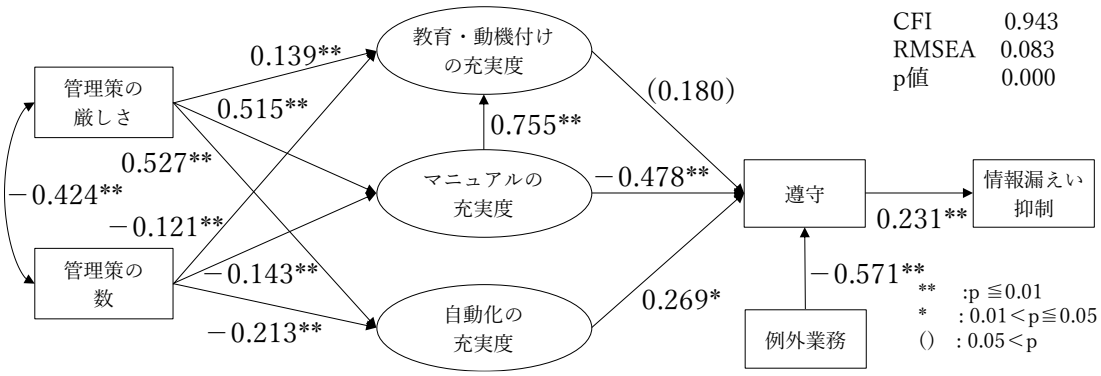

図 5-4　仮説検証モデルに対する分析結果（職種全体）（標準化済）

表 5-3　クロンバックの α 係数

潜在変数	設問数	クロンバックのα係数
教育・動機付けの充実度	5	0.955
マニュアルの充実度	6	0.932
自動化の充実度	5	0.961

表 5-4　潜在変数に対する因子負荷量

		潜在変数					
		教育・動機付けの充実度		マニュアルの充実度		自動化の充実度	
観測変数	計画的実施	0.925	**				
	必要性周知	0.911	**				
	遵守事項の網羅	0.912	**				
	理解度評価	0.888	**				
	遵守状況の観察	0.864	**				
	業務との整合			0.898	**		
	管理策の網羅			0.934	**		
	具体化			0.917	**		
	詳細化			0.588	**		
	集約			0.829	**		
	定期的見直し			0.866	**		
	有効性の確保					0.920	**
	効率性の確保					0.857	**
	機密性の確保					0.942	**
	可能性の確保					0.914	**
	信頼性の確保					0.939	**

** 有意水準１％で有意

* 有意水準５％で有意

図 5-4 では，CFI は 0.9 を超えており，かつ RMSEA も 0.1 未満であることから，あてはまりが悪いモデルとは言い切れない．このため本モデルを採用する．表 5-3 ではクロンバックの α 係数がいずれも 0.9 を超えている．また表 5-4 ではすべての因子負荷量が正であり，かつ因子負荷量が最も小さいものでも 0.588 となっている．これより潜在変数を構成する各観測変数は妥当性を有しているとみなす．

5.5.2. 職種による特性分析

仮説検証モデルに対して，職種別に等値制約を置かずに多母集団分析をおこなった結果を図 5-5 に示す．図 5-5 では，CFI が 0.9 を超えており，また RMSEA が 0.1 未満であるため，職種別においてもあてはまりが悪いモデルとは言い切れない．このため本モデルを採用し，配置不変性が確認されたものとする．

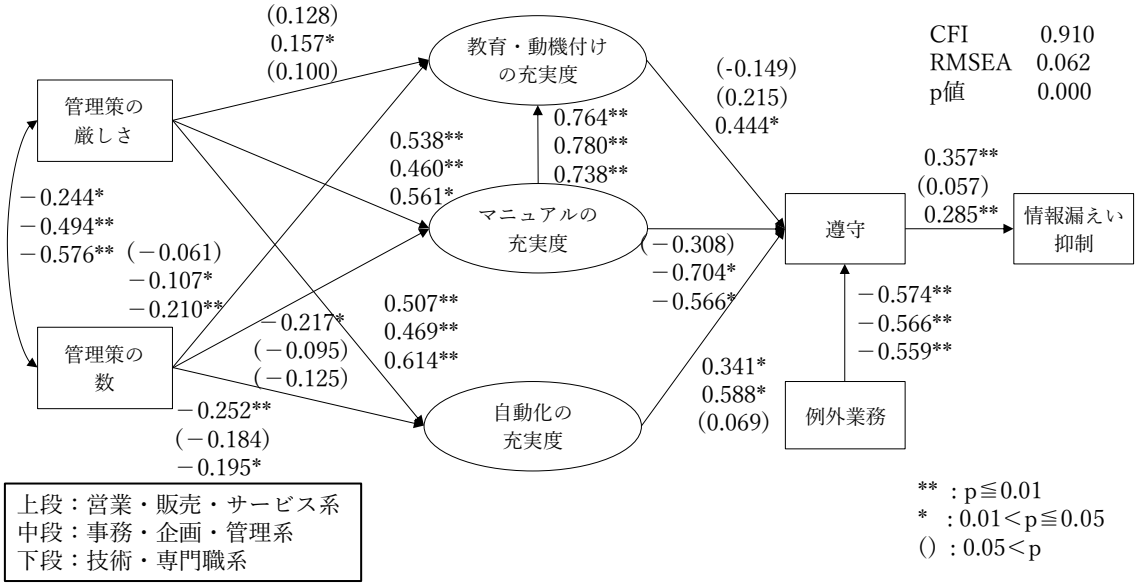

図 5-5　仮説モデルに対する多母集団分析結果（配置不変モデル）（標準化済）

図 5-5 より 1）事務・企画・管理系における遵守から情報漏えいへのパス，2）各職種における教育・動機付けの充実度から遵守へのパス，3） 技術・専門職系における自動化の充実度から遵守へのパスには，パス係数が大きく異なり，かつ有意性の有無が異なることから 1）から 3）を除き，等質性があると推察する．職種による母集団間の等質性を検討するため，制約条件を設定したモデルを構築し，モデルごとに適合度をまとめたものを

表 5-5 に示す．モデルの比較にあたっては，第 4 章と同様に AIC を採用する．表 5-5 のすべてのモデルにおいて各構成概念から任意の 1 つの観測変数へのパス係数，および観測誤差から観測変数へのパス係数は 1 に固定している．またパス係数に対する等値制約は，標準化をおこなっていない状態において設定している．

表 5-5 によれば，等値制約モデルが本論文で設定する適合基準をすべて満たし，かつ RMSEA および AIC が最も低い値を示している．これより 1）～3）を除くパスにおいて職種による母集団間の等質性があるものと判断する．本章では等値制約モデルを採用し，職種の特性を分析する．等値制約モデルに基づいて多母集団分析をおこなった結果を図 5-6 に示す．

表 5-5　職種による母集団間の等質性に対するモデル比較

モデル名	モデル説明	CFI	RMSEA	P値	AIC
配置不変モデル	等値制約を置かないモデル	0.910	0.062	0.000	1583.328
等値制約モデル	潜在変数間および潜在変数から観測変数へのパス係数に等値制約をおいたモデル．ただし以下に等値制約を置かないものとする． 1)事務・企画・管理系における遵守から情報漏えい抑制へのパス係数 2)技術・専門職系における教育・動機付けから遵守へのパス係数 3)技術・専門職系における自動化統制から遵守へのパス係数	0.911	0.059	0.000	1527.485

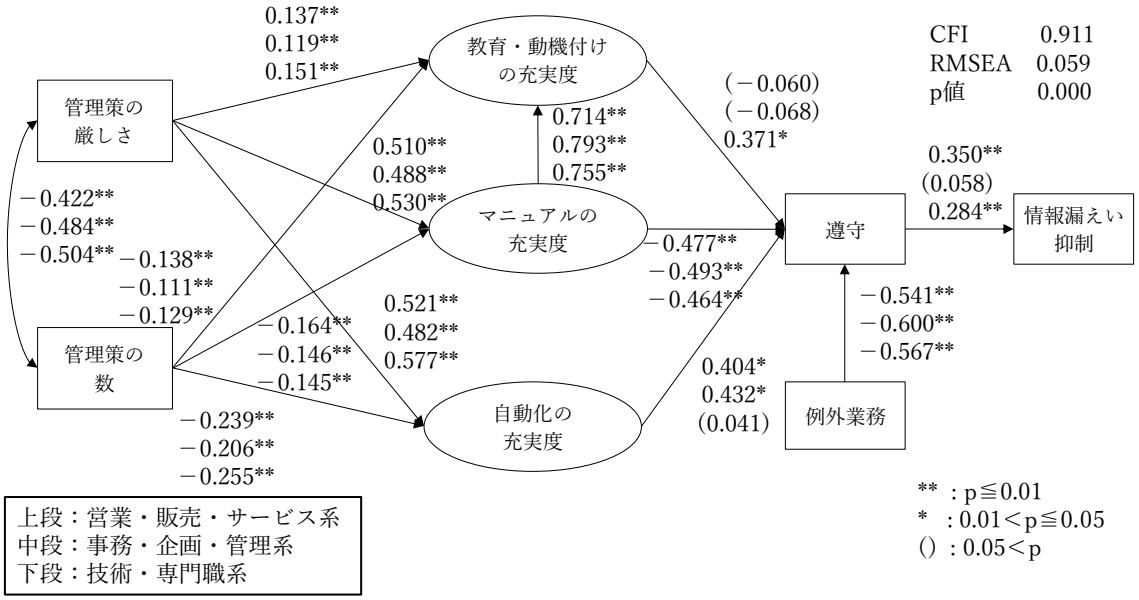

図 5-6　仮説検証モデルに対する多母集団分析結果（等値制約モデル）（標準化済）

5.5.3. 仮説の検証結果

本章では，設定した仮説群について，因果関係に符号を持つ形式で示している．表 5-6 では，有意水準を５％として検定統計量が有意かどうか，符号が設定した仮説と合致するかをまとめている．表 5-6 における「○」は，仮説が検証できていることをあらわしている.「×」は, 有意であるものの, 仮説と異なる結論が得られていることをあらわしている.「－」は，有意でないため，結論が得られないことをあらわしている.

表 5-6　仮説の検証結果

仮説		仮説検証結果			
		職種全体	営業・販売・サービス	事務・企画・管理	技術・専門職
Ｈ１	ルールが遵守されると情報漏えいが抑制される。	○	○	－	○
Ｈ２－１	教育・動機付けの充実度が増すとルールの遵守につながる。	－	－	－	○
Ｈ２－２	マニュアルの充実度が増すとルールの遵守につながる。	×	－	×	×
Ｈ２－３	自動化の充実度が増すとルールの遵守につながる。	○	○	○	－
Ｈ３	例外業務が増えるとルールの逸脱度が増す。	○	○	○	○
Ｈ４	マニュアルの充実度が増すと、教育・動機付けの充実度が増す。	○	○	○	○
Ｈ５－１	ルールの厳しさが増すと教育・動機付けの充実度が増す。	○	○	○	○
Ｈ５－２	ルールの数が増えると教育・動機付けの充実度が増す。	×	×	×	×
Ｈ５－３	ルールの厳しさが増すとマニュアルの充実度が増す。	○	○	○	○
Ｈ５－４	ルールの数が増えるマニュアルの充実度が増す。	×	×	×	×
Ｈ５－５	ルールの厳しさが増すと自動化の充実度が増す。	○	○	○	○
Ｈ５－６	ルールの数が増える自動化の充実度が増す。	×	×	×	×
Ｈ６	ルールの厳しさとルールの数には正の相関がある。	×	×	×	×

5.2.5 の①～③で述べた観点に対する分析結果を，以下に整理する．

① 組織構成員が管理策を遵守することによる情報漏えい抑制効果

事務・企画・管理系を除き，管理策遵守による情報漏えいを抑制する効果がみられる（Ｈ１）.

② 各促進活動がおよぼす管理策遵守効果の比較

教育・動機付けの充実は，技術・専門職系においてのみ，管理策の遵守効果がみられる（Ｈ２－１）. マニュアルの充実は, 事務・企画・管理系および技術・専門職系では, 仮説と異なる結論が得られており，管理策の遵守効果がみられない（Ｈ２－２）. 自動化の充実は，営業・販売・サービス系および事務・企画・管理系において，管理策の遵守効果がみられる（Ｈ２－３）.

③　管理策の策定状況が促進活動におよぼす影響

管理策の厳しさが増すことは，営業・販売・管理系および技術・専門職系における，教育・動機付けの場合を除き，促進活動の充実につながる（Ｈ５－１，Ｈ５－３，Ｈ５－５）．しかし，管理策の数が増すことは，促進活動の充実につながらない，もしくは有意でない（Ｈ５－２，Ｈ５－４，Ｈ５－６）

5.5.4. 仮説検証結果に対する考察

本項では 5.5.3 項の仮説検証結果に対する考察をおこなう．第 4 章と同様に本章で収集しているデータは，一定の基準を満たす内部統制の仕組みを整備し，運用している組織に勤務しており，かつ ISO/IEC 27001 認証の取得件数が多い業界に所属する組織構成員から取得したものである．考察にあたっては上記データの特性を前提としておこなっている．

（1）職種全体の分析結果に対する考察

本項では，図 5-4 に基づき，職種全体の傾向について考察する．

Ｈ１より，管理策が遵守されることで，情報漏えいを抑制する効果がみられる．不正に情報を持ち出す行為は，転職などにより他社に持ち出すことが目的の一つとなっている（情報処理推進機構，2016）．管理策を遵守させることにより，他社への流出が抑制され，情報漏えい抑制につながっているものと推察する．

自動化の充実は，Ｈ２－３の検証結果より，管理策遵守につながっている．組織構成員に対して強制的に管理策が適用されるため，自動化による管理策の遵守効果が得られているものと推察する．例外業務は，Ｈ３の検証結果より，管理策の遵守が低下を招いている．例外業務が発生する場合は，管理策を遵守しないことが，やむを得ないとされる傾向あると推察する．これに対し，Ｈ２－２の検証結果より，マニュアルの充実は，管理策遵守の低下を招いている．マニュアルの充実は，組織の定める規定類が具体化かつ詳細化されることにつながる．これによりわずかな逸脱をも認めない厳しい規定が策定されることとなる．実務担当者の負荷を考慮していない，厳しく，かつ膨大なマニュアルが整備されることにより「遵守できなくても仕方のない」との意識が組織構成員の中で発生するため，管理策の遵守につながっていないものと推察する．

管理策の厳しさから各促進活動へのパスは，Ｈ５－１，Ｈ５－３，Ｈ５－５のいずれも検証されている．管理策の厳しさが増すことで組織構成員は，不正に情報を持ち出す行為

を起こしづらくなっている．管理策の厳しさが増すことは，不正に情報を持ち出す行為が困難となるため，組織としての情報セキュリティへの取組みが認識され，各促進活動が充実していると捉えられる傾向があると推察する．一方，管理策の数から各促進活動へは，Ｈ５－２，Ｈ５－４，Ｈ５－６より，いずれも有意であるが，負の値を示している．このことから，管理策の数が増えても，促進活動の充実度は向上しない．管理策の数が増えると，マニュアルに対する条文の追加，教育による周知，新たなシステムの導入などの負荷やコストが発生する.負荷やコストを,組織が十分に捻出できないことが一因と推察する．

Ｈ６より，管理策の数と，管理策の厳しさの間には，負の相関関係がある（－0.424）．組織が投入できる経営資源は限りがある．このため管理策は，数を増やすか厳しさを増すかのいずれかに偏って採用されていることが要因と推察する．

（２）職種別の分析結果に対する考察

本項では，図 5-4 と図 5-6 を比較し，職種による傾向がみられる点について考察する．

教育・動機付けから管理策の遵守へのパス（Ｈ２－１）は，図 5-4 における職種全体の分析結果が有意でない．一方，図 5-6 における技術・専門職系では有意な結果が得られている（0.371）ため，教育・動機付けの充実が，管理策の遵守につながっている．教育・動機付けの充実度は，マニュアルの充実度の影響を強く受けている（0.755）．技術・専門職系は，技術情報など，ノウハウを作り出す職種であるため，情報に対する価値や，管理策遵守の必要性に対する理解がほかの職種に比べて得られている．このため，マニュアルの内容を理解させるような教育･動機付けが,管理策の遵守に寄与しているものと推察する．

5.6. 結論

本章は，不正のトライアングル理論における「機会」の抑制の観点から，組織構成員に管理策を遵守させることを通じて，情報漏えいを抑制するため，促進活動の観点から組織が講じるべき施策について，知見を得ることを目的としている．目的を達成するため本章では，管理策の策定状況から促進活動，管理策の遵守を介して情報漏えい抑制へ至るまでのそれぞれの因果関係について仮説の設定，仮説検証モデルの構築をおこなっている．本章では，上場企業という一定水準の内部統制が整備されており，かつ ISO/IEC 27001 認証の取得件数が多いとされる業種に属する構成員を対象とした質問紙調査で得られるデータ

に基づいて，職種全体に対する共分散構造分析，さらに各職種の集団に対する多母集団分析により，仮説の検証をおこなっている．仮説の検証を通じて機会を抑制するためのメカニズムを解明し，組織が講じるべき施策を提案している．

教育・動機付けの実施，マニュアルの整備，自動化の整備の 3 つの促進活動が管理策の遵守におよぼす影響について分析をおこなった結果，次の事項を確認している．事務・企画・管理系を除き，管理策遵守による情報漏えいを抑制する効果がある．教育・動機付けの充実は，技術・専門職系においてのみ，管理策の遵守効果がある．マニュアルの充実は，事務・企画・管理系および技術・専門職系では，仮説と異なる結論が得られており，管理策の遵守効果がみられない．自動化の充実は，営業・販売・サービス系および事務・企画・管理系において，管理策の遵守効果がある．管理策の厳しさが増すことは，営業・販売・管理系および技術・専門職系における，教育・動機付けの場合を除き，促進活動の充実につながる．しかし管理策の数が増すことは，促進活動の充実につながらない，もしくはつながるとは言い切れない．以上より営業・販売・サービス系および事務・企画・管理系では，自動かつ強制的に管理策を遵守させること提案する．一方，技術・専門職系では，自動かつ強制的に管理策を遵守させる施策は有効な手段とは言い切れない．技術・専門職系に対しては，管理策に理解を求め，自ら手動で遵守するよう促すことを提案する．

以上の施策により，営業・販売・サービス系および技術・専門職系は，管理策の遵守が向上し，管理策の遵守を通じて，情報漏えい抑制につながることが期待できる．一方，事務・企画・管理系では，管理策を遵守させることによる情報漏えい抑制の効果が，本章の結果からは検証できていない．職種に応じて，取り扱う情報の特性が異なることが，職種による効果の違いに起因する可能性がある．このことに対する検討は今後の課題である．

第 6 章　結語

6.1. 各章の要約

本論文では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をおこなっている．

第 1 章では，本論文における問題意識を述べたうえで，本論文の目的を設定している．

第 2 章では，インシデントを抑制するための ISO/IEC 27001 規格の活用を切り口とした関連研究の調査をおこなっている．また ISO/IEC 27001 規格における要求事項に該当する ISMS，および附属書 A に該当する管理策の観点，ならびに不正に情報を持ち出す行為の観点から関連研究を紹介している．その結果，本論文の目的を達成するにあたり，以下の 3 点を解決すべき課題として設定している．

① 個人情報の漏えいや紛失に関するインシデント事例を用いて ISO/IEC 27001 認証によるインシデント抑制効果を検証する．また ISO/IEC 27001 規格に準拠している組織における，インシデントを抑制するうえでの問題点をあきらかにする

② ISO/IEC 27001 規格の要求事項の観点から，不正な情報持ち出し意図の正当化を抑制する効果を実証し，組織が講じるべき施策を提案する．

③ 促進活動の観点から不正な情報持ち出し行為の機会を抑制する効果をあきらかにし，組織が講じるべき施策を提案する．

第 3 章では，解決すべき課題①に基づき，個人情報の漏えいまたは紛失にかかるインシデントの観点から ISO/IEC 27001 認証による抑制効果を検証している．またインシデントの原因を分析することにより，ISO/IEC 27001 規格に準拠している組織において，インシデントを抑制するうえでの問題点をあきらかにしている．日本ネットワークセキュリティ協会が公表する 2008 年～2010 年の事例をもとに ISO/IEC 27001 認証を取得している組織がインシデントを抑制できるかを実証した結果，一部上場企業という一定水準の内部統制が整備されており，かつ 1000 人以上の大規模な個人情報を保有している組織では ISO/IEC 27001 認証を取得してもインシデントを抑制できているとは言い切れない．すなわち ISO/IEC 27001 を認証取得しても，組織が整備する ISMS に対して運用が伴っていない場合は，インシデント抑制という目的を達成できないことが示唆される．このことから本論文の問題意識として掲げている，「認証取得または維持のみが目的となった組織であっても，情報セキュリティに関連するインシデントの抑制ができるのだろうか」に対しては，「認証取得をすることのみをもってインシデントを抑制できるとは言い切れない」と結

論づけている．一方，多くのインシデントは，管理策の不備，または整備した管理策が運用されていないことにより発生している．インシデント抑制のために講じるべきであった管理策は，すべて ISO/IEC 27001 規格の附属書 A にて網羅されていることから，ISO/IEC 27001 規格に準拠した ISMS が適切に整備し，運用されていれば，多くのインシデントは抑制し得る．ISO/IEC 27001 規格を適用することで，インシデントの抑制を実現するためには，組織構成員に対して，規定した管理策を遵守させるような施策が組織に求められることが示唆される．業種別にみると業種による認証取得による効果は業種により異なっている．また効果を有し得た管理策は，業種により異なっていることを確認している．これより，どの管理策に対して重点的に経営資源を投入すべきかを検討するにあたっては，業種の特性を加味する必要があることが示唆される．

第 4 章では解決すべき課題②に基づいて，組織は ISO/IEC 27001 規格における「認識」の要求事項のうち，どの項目に注力すれば不正な情報持ち出し行為の正当化が抑制できるのかについての知見を得ることを目的としている．目的達成のため ISO/IEC 27001 規格における，方針，自らの貢献，不適合からなる 3 つの「認識」の要求事項に焦点をあて，どのような認識を持たせれば，不正に情報を持ち出す行為を正当化することを抑制できるかについて仮説を設定し，仮説検証モデルを構築している．仮説の検証を通じて，不正な情報持ち出し行為の正当化を抑制するためのメカニズムを解明し，組織が講じるべき施策を提案している．上場企業という一定水準の内部統制が整備されており，かつ ISO/IEC 27001 認証の取得件数が多いとされる業種を対象に，認証有無全体に対する共分散構造分析および認証有無による多母集団分析をおこなった結果，ISO/IEC 27001 認証の有無により，効果を有する項目と有さない項目が異なること確認している．すなわち ISO/IEC 27001 規格に準拠した ISMS を導入するなど，情報セキュリティに対する組織の成熟度により，組織構成員に持たせるべき認識が異なることを確認している．認証取得組織の構成員に対しては，方針および不正な情報持ち出し行為による影響を認識させることが，不正な情報持ち出し行為の正当化を抑制するために有効な施策である．未取得組織の構成員に対しては，自らの貢献不正な情報持ち出し行為による影響を認識させることが有効な施策であることを提案している．

第 5 章では解決すべき課題③に基づいて，促進活動の観点から組織が講じるべき施策についての知見を得ることを目的としている．目的達成のため，組織構成員に管理策を遵守させるための活動を「促進活動」と定義し，「教育・動機付け」，「マニュアル」，「自動化」

の 3 つの観点から不正に情報を持ち出す行為のうち，機会の抑制におよぼす影響について仮説を設定し，仮説検証モデルを構築している．仮説の検証を通じて，不正な情報持ち出し行為の機会を抑制するためのメカニズムを解明し，組織が講じるべき施策を提案している．第 4 章と同様に上場企業という一定水準の内部統制が整備されており，かつ ISO/IEC 27001 認証の取得件数が多いとされる業種を対象に，職種全体に対する共分散構造分析および職種別に対する多母集団分析をおこなった結果，職種により不正に情報を持ち出す行為を抑制する効果をもつ促進活動が異なることを確認している．営業・販売・サービス系および事務・企画・管理系では，自動かつ強制的に管理策を遵守させること提案している．一方，技術・専門職系では，自動かつ強制的に管理策を遵守させる施策は有効な手段とは言い切れない．技術・専門職系に対しては，管理策に理解を求め，自ら手動で遵守するよう促すことを提案している．

6.2. 本論文の実務的貢献

本論文では管理策の選定や，正当化抑制のために組織構成員に持たせるべき認識，管理策を遵守させるための促進活動が業種や職種，認証の有無に応じて異なることを確認している．すなわち ISO/IEC 27001 規格を組織に適用する場合，規格への準拠によるインシデント抑制効果を発揮するため，組織は，取り扱う情報の特性や，ISMS 導入有無などの情報セキュリティに対する組織の成熟度を加味した施策を講じる必要があることが示唆される．

ISO/IEC 27001 規格は業種や規模によらず適用可能なものとされている．ISO/IEC 27001 規格は，情報セキュリティリスクアセスメントや管理策の決定，監査などをはじめとする PDCA サイクルを通じた継続的改善のための要求事項に加えて，管理目的および管理策のリストである附属書 A を提供している．ISO/IEC 27001 認証を取得するなど，規格に準拠することにより，PDCA サイクルおよび包括的な管理策を導入することができる．このことからインシデントを抑制する目的において，ISO/IEC 27001 規格を適用することは有用であると考える．また自組織にて ISO/IEC 27001 規格に準拠する際，コンサルティング会社の活用や，他組織の事例を参考にすることも，効果的かつ効率的な ISMS の導入につながるため有用であると考える．一方で ISO/IEC 27001 規格は，業種や規模によらず適用可能なものとされているため，その解釈は規格に準拠する組織がそれぞれでおこなう

必要がある. すなわち, どの程度の水準の情報セキュリティを組織構成員に要求するかは, 組織において決定する必要がある．ISO/IEC 27001 認証取得のための文書や様式類を，自組織に向けてカスタマイズすることなく導入することや，自組織の特性を加味せず，他組織における導入事例に沿って画一的に整備する場合，組織構成員に対して過大または過少な対応を求めることになり得る．この場合，ISO/IEC 27001 規格へ準拠しても，インシデントの抑制は期待できない．ISO/IEC 27001 規格への準拠により，インシデントの抑制につなげるためには，単に ISO/IEC 27001 を認証取得し，維持することや，他組織おける画一的な導入事例の模倣のみでは不十分である．期待した効果を発揮するには，組織を取り巻く状況や，取り扱う情報の特性に応じた施策を講じる必要がある．このことが本論文から得られる実務上の示唆である.

本論文では，情報セキュリティインシデントのうち，組織構成員が不正に情報を持ち出す行為に焦点をあてている．不正に情報を持ち出す行為を抑制するため，ISO/IEC 27001 規格の要求事項，附属書 A それぞれの観点から，規格に準拠している組織が講じるべき施策について分析をおこなっている．業種や職種，ISO/IEC 27001 認証の有無に応じて，選定すべき管理策の項目や，正当化抑制のために組織構成員に持たせるべき認識の項目，管理策を遵守させるための促進活動の手段が異なることを，本論文ではデータを用いて実証している.「上場企業かつ ISO/IEC 27001 認証の取得件数が多いとされる業種に属する組織」を対象として，不正のトライアングル理論における正当化および機会を抑制する観点から，不正に情報を持ち出す行為を抑制するために ISO/IEC 27001 規格に準拠する際，講じるべき施策を提案していることが，本論文の実務的な貢献である.

6.3. 今後の課題

インシデント抑制のための施策検討にあたり，本論文では第 3 章において日本ネットワークセキュリティ協会が公表する個人情報の漏えいまたは紛失事例をもとに分析をおこなっている．第 4 章および第 5 章では，第 3 章で得られる「インシデントを抑制するには組織構成員に管理策を遵守させる必要がある」との示唆から，技術情報や経営情報などを含む情報全般を対象として講じるべき施策を検討している．個人情報は取得した組織の保有物ではなく，情報主体である本人のものである．このことから知り得るはずのない第三者から本人に連絡が届く場合や，参照できるはずのない者が個人情報を参照できるなどの場

合，インシデントとして検出しやすい．一方，技術情報や経営情報は，「社外秘」などのラベル付けがおこなわれていない限り，第三者が，参照できる情報が漏えいや紛失の対象であることを認識することは困難である．このため第 3 章については，個人情報に限定したインシデント事例をもとに分析をおこなっている．第 3 章にて個人情報に関するインシデント事例を用いて分析し，「インシデント抑制のためには，管理策を遵守させる必要がある」として得られる示唆は，技術情報や経営情報に対して分析した場合，本論文の分析結果と異なる可能性がある．また一定の基準を満たす内部統制が要求される上場企業を分析の対象としていることから，内部統制の整備要請を受けていない組織や，上場基準に満たない規模の組織において本論文の結論を適用できない可能性がある．

第 3 章におけるインシデント事例は個人情報の漏えいまたは紛失を対象としており，第 4 章および第 5 章は不正な情報持ち出しに焦点をあてている．すなわち本論文では，機密性の中でも不正な情報持ち出し行為を抑制するための施策を提案しており，完全性や可用性を対象外としている．しかし情報セキュリティの定義は「情報の機密性，完全性および可用性を維持すること」（ISO, 2014a）である．情報の利活用の場は急速に広まってきており，たとえば金融分野における情報の取り扱いや，IoT（Internet of Things）の活用，車の自動運転のための情報の利活用，クラウドの利活用にあたっては，完全性および可用性の侵害によるインシデントが事業継続に影響をおよぼす可能性がある．

以上のとおり，インシデントを抑制するうえでの問題点をあきらかにする際，個人情報に限定したインシデント事例をもとに分析している点，施策検討の際，ISO/IEC 27001 認証取得件数の多い業種および上場企業を分析の対象としている点，完全性や可用性を対象外としている点が本論文における限界である．技術情報や経営情報など，個人情報以外の情報を対象にした施策の検討や，非上場組織に対する分析，完全性または可用性の維持のための施策の検討については今後の研究課題である．

謝辞

本論文は筆者が筑波大学大学院ビジネス科学研究科企業科学専攻在籍中の研究成果をまとめたものです．本論文の執筆にあたり，2019 年から主指導教官を引き受けていただき，博士論文の完成に向けたご指導・ご鞭撻をいただいた領家美奈先生および 2011 年から 2019 年までの 8 年間にわたり主指導教官としてご指導・ご鞭撻をいただきました山田秀先生（現慶應義塾大学大学院理工学研究科教授）には，心より感謝申し上げます．

副指導教官の佐藤忠彦先生，倉橋節也先生をはじめ，筑波大学大学院ビジネス科学研究科の諸先生方には，統計分析結果の解釈の仕方など，研究推進にあたって多くの有用なご助言や叱咤激励をいただきました．厚く御礼申し上げます．

また博士号取得したいと考えるきっかけを与えていただいた吉田耕作先生（元青山学院大学専門職大学院教授），博士を見据えた論文を執筆したいとの筆者の希望を受け入れ，修士課程において論文の書き方を基礎からご教授いただいた常田稔先生（元早稲田大学大学院社会科学研究科教授），研究内容に対して各種専門分野の観点から貴重なご意見をいただいた筑波大学大学院山田秀ゼミの皆様，くじけそうになった際，叱咤激励により本論文の完成に向けて奮い立たせていただいた筑波大学大学院ビジネス科学研究科 2011 年入学の同期の皆様にも厚く御礼申し上げます．

最後に 2005 年の青山学院大学専門職大学院への進学から，早稲田大学大学院，筑波大学大学院と，社会人でありながら 3 つもの大学院への通学を受け入れ，プライベートの時間の多くを研究に割くことを許容し，見守りながら支え続けてくれた家族に感謝の意を伝えたいと思います．

参考文献

[1] Acharya, U.H. & Ray, S., "ISO 9000 certification in Indian industries: a survey", *Total Quality Management*, Vol.11, No.3, pp.261-266, 2000.

[2] Ajzen, I., and Fishbein, M., *Understanding attitudes and predicting social behavior. Englewood-Cliffs*, NJ: Prentice-Hall, 1980.

[3] Ajzen, I., From intention to actions: A theory of planned behavior. In J. Kuhl and J. Beckman(Eds.), *Action-control: From cognition to behavior*(pp.11-39), Heidelberg: Springer, 1985.

[4] Ajzen, I. and Madden, T.J., "Prediction of Goal-Directed Behavior: Attitudes, Intentions, and Perceived Behavioral Control", *Journal of Experimental Social Psychology*, Vol.22, pp.453-474, 1986.

[5] Ajzen, I., "The theory of planned behavior", *Organizational Behavior and Human Decision Processes*, Vol.50, No.2, 179-211, 1991.

[6] Al-Najjar, S.M. & Jawad, M.K., "ISO 9001 Implementation Barriers and Misconceptions: An Empirical Study", *International Journal of Business Administration*, Vol.2, No.3, pp.118-131, 2011.

[7] AL-Omari, A., El-Gayar, O., and Deokar, A., "Information Security Policy Compliance: The Role of Information Security Awareness", *Proceedings of the Eighteenth Americas Conference on Information Systems, Seattle, Washington, August 9-12*, 2012.

[8] Aravind, D. & Christmann, P., "Decoupling of standard implementation from certification: Does quality of ISO 14001 implementation affect facilities' environmental performance?", *Business Ethics Quarterly*, Vol.21, No.1, pp.73-102, 2011.

[9] Arimura, T.H., Hibiki, A. & Katayama, H., "Is a voluntary approach an effective environmental policy instrument? A case for environmental Management system.", *Resources for The Future, Discussion Paper*, pp.07-31, 2007.

[10] Atyam, S.B., "Effective of Security Control Risk Assessments for Enterprises: Assess on the Business Perspective of Security Risks", *Information Security Journal: A*

Global Perspective, Vol.19, pp.343-350, 2010.

[11] Babakri, K.A., Bennett, R.A & Franchetti, M., "Critical factors for implementing ISO 14001 standard in United States industrial companies", *Journal of Cleaner Production*, Vol.11, pp.749-752, 2003.

[12] Bahtit, H. & Regragui, B., "Risk Management for ISO 27005 Decision support", *International Journal of Innovative Research in Science, Engineering and Technology*, Vol.2, Issue 3, pp.530-538, 2013.

[13] Beattie, K.R. & Sohal, A.S., "Implementing ISO 9000: A study of its benefits among Australian organizations", *Total Quality Management*, Vol.10, No.1, pp.95-106, 1999.

[14] Boiral, O & Roy, M.J., "ISO 9000: Integration rationales and organizational Impacts", *International Journal of Operations & Production Management*, Vol.27, No.2, pp.226-247, 2007.

[15] Boiral,O., "ISO 9000: Outside the Iron Cage", *Organization Science*, Vol.14, No.6, November-December 2003, pp. 720-737, 2003.

[16] Boiral,O., "Corporate Greening Through ISO 14001: A Rational Myth?", *Organization Science*, Vol.18, No.1, pp.127-146, 2007.

[17] Broderick, J.S., "ISMS, security standards and security regulations", *Information Security Technical Report*, pp.26-31, 2006.

[18] Brouwer, M.A.C. & C.S.A van Koppen., "The soul of the machine: continual improvement in ISO 14001", *Journal of Cleaner Production*, Vol.16, pp.450-457, 2008.

[19] Buttle,F., "ISO 9000: marketing motivations and benefits", *International Journal of Quality & Reliability Management*, Vol.14, No.9, pp.936-947, 1996.

[20] Calisir, F., Bayraktar, C.A. & Beskese, B., "Implementing the ISO 9000 standards in Turkey: A study of large companies' satisfaction with ISO 9000", *Total Quality Management*, Vol.12, No.4, pp.429-438, 2001.

[21] Cantero, M., "Processes of Institutionalization", *The International Journal of Knowledge, Culture & Change Management in Organization*, Vol.5, 2005/2006.

[22] Casadesús, M., Giménez, G. & Heras, I., "Benefits of ISO 9000 implementation in Spanish industry", *European Business Review*, Vol.13, No.6, pp.327-335, 2001.

[23] Casadesus, M., Marimon,F & Heras, I., "ISO 14001 diffusion after the success of the

ISO 9001 model", *Journal of Cleaner Production*, Vol.16, pp.1741-1754, 2008.

[24] Chen, A., Chen, H., and Chang, S. C., "Understanding the Antecedents of Individuals Intention of Using Cloud Services", *Journal of Economics and Management*, Vol. 13, No.2, pp.139-166, 2017.

[25] Chow-Chua, C., Goh, M. & Wan, T.B., "Does ISO9000 certification improve business performance?", *The International Journal of Quality & Reliability Management*, Vol.20, No.8, pp.936-953, 2003.

[26] Chu, P., and Wu, T., "In-Depth Citizen Interaction with E-Government from Taxpayers' Behavioral Perspectives", *International Journal of the Information Systems for Logistics and Management*, Vol. 1, No.1, pp. 27-37, 2005.

[27] Chung, Y., Kim, I. & Lee, D., "A Practical Security Risk Analysis Process and Tool for Information System" *International Journal of Information Processing Systems*, Vol.2, No.2, pp.95-100, 2006.

[28] Cohen, L, E., & Felson, M., "Social Change and Crime Rate Trends: A Routine Activity Approach", *American Sociological Review*, Vol. 44, No. 4, pp. 588-608, 1979.

[29] Cohen, Jeffrey., Yuan Ding, Cedric Lesage and Herve Stolowy., "Corporate Fraud and Managers' Behavior: Evidence from the Press.", *Journal of Business Ethics*. 95: pp.271-315, 2010.

[30] Coles-Kemp, L. & Overill, R.E., "On the role of the Facilitator in information security risk assessment", *The Journal in Computer Virology*, Vol.3, pp.143-147, 2007.

[31] Cornish, D, B. and Clarke, R, V., "Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention", *Crime Prevention Studies*, Vol. 16, pp.41-96, 2003.

[32] Cressey, D.R., *Other People's Money: A Study in the Social Psychology of Embezzlement*, Wadsworth Publishing Company, Inc., 1971.

[33] Davis, F., *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results*, Massachusetts Institute of Technology, Sloan School of Management, 1986.

[34] Davis, F., "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", *MIS Quarterly*, Vol. 13, No.3, pp. 319-340, 1989.

[35] Delmas, M.A., "Stakeholders and Competitive Advantage: The Case of ISO 14001", *Production and Operations Management*, Vol.10, No.3, pp.343-358, 2001.

[36] Delmas, M.A. "The diffusion of environmental management standards in Europe and in the United States: An institutional perspective", *Policy Sciences*, Vol.35, pp.91-119, 2002.

[37] Delmas, M.A. & Toffel, M.W., "Organizational responses to environmental demands: Opening the black box", *Strategic Management Journal*, Vol.29, Issue, 10, pp.1027-1055, 2008.

[38] Deming, W.E., *Out of the crisis*, MIT Center for Advanced Engineering Study, Cambridge, Mass, 1986.

[39] Dey, M., "Information Security Management –A Practical Approach", *AFRICON 2007*, pp. 1-6, 2007.

[40] Dick, G.P.M., Heras, I. & Casadéus, M., "Shedding light on causation between ISO 9001 and improved business performance", *International Journal of Operations & Production Management*, Vol.28, No.7, pp.687-708, 2008.

[41] DiMaggio, P.J. & Powell, W.W., "The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields", *American Sociological Review*, Vol.48, Issue2 (Apr.1983), pp.147 – 160, 1983.

[42] Dissanayaka, S.M., Kumaraswamy, M.M & Marosszeky, M., "Evaluating outcomes from ISO 9000-certified quality systems of Hong Kong contractors", *Total Quality Management*, Vol.12, No.1, pp.29-40, 2001.

[43] Djapic, M. & Lukic, L., "Information assets security management system standardization on railways", *Mechanics Transport Communications Academic journal*, Vol.3, article.0178, pp.85-90, 2007.

[44] Douglas, A., Kirk, D., Brennan,C. & Ingram, A., "Maximizing the benefits of ISO 9000 implementation", *Total Quality Management*, Vol.10, No.4&5, pp.507-513, 1999.

[45] Eom, J.H., Park, S.H., Kim, T.K. & Chung, T.M., "Two-Dimensional Qualitative Asset Analysis Method based on business Process-Oriented Asset Evaluation", *International Journal of Information Processing Systems*, Vol.1, No.1, pp.79-85, 2005.

[46] Feng,M. Terziovski,M. & Samson,D., "Relationship of ISO 9001:2000 quality system

certification with operational and business performance -A survey in Australia and New Zealand-based manufacturing and service companies", *Journal of Manufacturing Technology Management*, Vol.19, No.1, pp.22-37, 2008.

[47] Fishbein, M., and Ajzen, I., *belief, attitude, and behavior: An introduction to theory and research*, Reading, MA: Addison-Wesley, 1975.

[48] Gavin P.M. Dick., "ISO9000 certification benefits, reality or myth?", *The TQM Magazine*, Vol12, No.6, pp.365-371, 2000.

[49] Gordon, L.A. & Loeb, M.P., "The Economics of Information Security Investment", *ACM Transactions on Information and Systems Security*, Vol.5, No.4, pp.438-457, 2002.

[50] Gotzamani, K & Tsiotras, G., "An empirical study of the ISO 9000 standards' contribution towards total quality management", *International Journal of Operations & Production Research*, Vol.21, No.10, pp.1326-1342, 2001.

[51] Greenwood, R. & Hinings, C.R., "Understanding radical organizational change: Bringing together the old and the new institutionalism", *Academy of Management Review*, Vol.21, No.4, pp.1022-1054, 1996.

[52] Guler, I. Guillen,M.F and Macpherson, J. M., "Global competition, institutions, and the diffusion of organizational practices: The international spread of ISO 9000 quality certificates", *Administrative Science Quarterly*, Vol. 47, pp.207-232, 2002.

[53] Haile, N., & Altmann, J., "Risk - Benefit - Mediated Impact of Determinants on the Adoption of Cloud Federation", *The Technology Management, Economics, and Policy Program Discussion Paper*, No. 2015:122, 2015.

[54] Han, S.B., Chen, S.K & Ebrahimpour, M., "The impact of ISO 9000 on TQM and business performance", *Journal of Business and Economic Studies*, Vol.13, No.2, pp.1-23, 2007.

[55] Henriksen, E., Burkow, T.M., Johnsen, E. & Vognild, L.K., "Privacy and information security risks in a technology platform for home-based chronic disease rehabilitation and education", *BMC Informatics and Decision Making*, http://www.biomedcentral.com/content/pdf/1472-6947-13-85.pdf (11/Feb/2014)

[56] Heras, I., Casadéus, M. & Dick., G.P.M., "ISO 9000certification and the bottom line:

a comparative study of the profitability of Basque region companies", *Managerial Auditing Journal*, Vol.17, No.1/2, pp.72-78, 2002.

[57] Heras, I., Casadéus, M., Ochoa, C., "Effects of ISO9000 certification on companies' profitability: an empirical study", *Integrated Management Proceedings of the 6th International Conference on ISO 9000 and TQM*, pp.66-72, 2001.

[58] Heras, I., Dick., G.P.M & Casadéus, M., "ISO 9000 registration's impact on sales and profitability. A longitudinal analysis of performance before and after accreditation", *International Journal of Quality & Reliability Management*, Vol.19, No.6, pp.774-791, 2002.

[59] Huang, L., Chen, S.K. & Han, S.B., "The effect of business reorganization and technical innovation on firm performance", *Journal of Business and Economic Studies*, Vol.17 No.1, pp.29-36, 2011.

[60] Ifinedo, P., "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory", *Computers & Security*, vol.31, 2012, pp.83-95.

[61] Internal Organization for Standardization., *ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management second edition*, Internal Organization for Standardization, Geneva, 2005a.

[62] Internal Organization for Standardization., *ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements*, Internal Organization for Standardization, Geneva, 2005b.

[63] Internal Organization for Standardization., *The ISO Survey 2008*, ISO Central Secretariat, 2009a.

[64] Internal Organization for Standardization., *ISO 31000 Risk Management – Principles and guideline*, Internal Organization for Standardization, Geneva, 2009b.

[65] Internal Organization for Standardization., *The ISO Survey 2009*, ISO Central Secretariat, 2010

[66] Internal Organization for Standardization., *ISO/IEC 27001 Information technology - Security techniques - Information security management systems – Requirements*,

Internal Organization for Standardization, Geneva, 2013.

[67] Internal Organization for Standardization., *ISO/IEC 27000:2014 Information technology - Security techniques - Information security management systems – Overview and Vocabulary*, Internal Organization for Standardization, Geneva, 2014a.

[68] Internal Organization for Standardization., *ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management*, Internal Organization for Standardization, Geneva, 2014b.

[69] Internal Organization for Standardization., *ISO 9001:2015 Quality management systems – Requirements*, Internal Organization for Standardization, Geneva, 2015a.

[70] Internal Organization for Standardization., *ISO 14001:2015 Environmental management systems - Requirements with guidance for use*, Internal Organization for Standardization, Geneva, 2015b.

[71] Internal Organization for Standardization., *ISO/IEC 17021-1:2015 Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements*, Internal Organization for Standardization, Geneva, 2015c.

[72] Internal Organization for Standardization., *ISO/IEC 27006 Information technology - - Security techniques -- Requirements for bodies providing audit and certification of information security management systems*, Internal Organization for Standardization, Geneva, 2015d.

[73] Internal Organization for Standardization., *ISO/IEC 27005 Information technology - Security techniques - Information security risk management*, Internal Organization for Standardization, Geneva, 2018.

[74] Internal Organization for Standardization., *ISO/IEC 27701 Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines*, Internal Organization for Standardization, Geneva, 2019.

[75] Internal Organization for Standardization., *ISO/IEC Directives Part 1 Consolidated ISO Supplement, Eleventh edition, 2020*, Internal Organization for Standardization, Geneva, 2020.

[76] ISACA, *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*, ISACA, 2012.（日本 IT ガバナンス協会訳　2012 年）

[77] Jayawickrama, W., "Managing Critical Information Infrastructure Security Compliance: A Standard Based Approach Using ISO/IEC 17799 and 27001", *OTM Workshops 2006*, pp.565-574, 2006.

[78] Jones, R., Arndt, G & Kustin, R., "ISO 9000 among Australian companies: impact of time and reasons for seeking certification on perceptions of benefits received", *The International Journal of Quality & Reliability Management*, Vol.14, No.7, pp.650-660, 1997.

[79] Kenning, M.J., "Security management standard -ISO 17799/BS 7799", *BT Technology Journal*, Vol.19, No.3, pp.132-136, 2001.

[80] Khan, B., Alghathbar, K, S., Nabi, S, I., and Khan, M, K., "Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management*, Vol. 5(26), pp. 10862-10868, 28 October 2011.

[81] Kolosenia, D., Lee, C, Y., and Lee, G, W., "Security Policy Compliance in Public Institution: An Integrative Approach", *Journal of Applied Structural Equation Modeling*, Vol. 2, No.1, pp.13-28, January 2018.

[82] Koo, H., Koo, L.C. & Tao, F.K.C., "Analyzing employee attitudes towards ISO certification", Managing Service Quality, Vol.8, No.5, pp.312- 319, 1998.

[83] Koo, L.C., Tao, F.K.C. & Koo, H., "Charting staff attitude along the journey towards getting ISO certification", *Managing Audit Journal*, Vol.14, No.1/2, pp.44- 50, 1999.

[84] Ku, C., Chang, Y. & Yen, D.C., "National information security policy and its implementation: A case study in Taiwan", *Telecommunications Policy*, Vol.33, pp.371-384, 2009.

[85] Kumar, D.A. & Balakrishnan, V., "A study on ISO 9001 quality management system (QMS) certifications -reasons behind the failure of ISO certified organizations", *Journal of Research in International Business and Management*, Vol. 1, No.6, pp.147-154, 2011.

[86] Kuo, T., Chang, T., Hung, K. & Lin, M., "Employees' perspective on the effectiveness of ISO 9000 certification: A Total Quality Management framework", *Total Quality*

Management, Vol.20, No.12, pp.1321-1335, 2009.

[87] Kwon, S., Jang, S., Lee, J. & Kim, S., "Common defects in information security management system of Korean companies", *The Journal of Systems and Software*, Vol.80, pp.1631-1638, 2007.

[88] Lee, K.S. & Palmer, E., "An empirical examination of ISO 9000-registered companies in New Zealand", *Total Quality Management*, Vol.10, No.6, pp.887-899, 1999.

[89] Lee, T.Y., "The development of ISO 9000 certification and the future of quality management: A survey of certified firms in Hong Kong", *The International Journal of Quality & Reliability Management*, Vol.15, No.2, pp.162-177, 1998.

[90] Li, Hetian., Liu, Y., He, D., "A Fuzzy Set-Based Approach for Mode-Based Internet-Banking System Security Risk Assessment", *Wuhan University Journal of Natural Sciences*, Vol. 11, No.6, pp.1869-1872, 2006.

[91] Liang, H., & Xue, Y., "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective", *Journal of the Association for Information Systems*, Vol. 11(7), pp.394-413, 2010.

[92] Lima,M.A.M., Resende,M & Hasenclever,L., "Quality certification and performance of Brazilian firms: An empirical study", *International Journal of Production Economics*, Vol.66, pp.143-147, 2000.

[93] Lin, C.I & Jang, W.Y., "Successful ISO 9000 implementation in Taiwan. How can we achieve it, and what does it mean?", *International Journal of Productivity and Performance Management*, Vol.57, No.8, pp.600-622, 2008.

[94] Lo, L.K. & Chang, D.S., "The difference in the perceived benefits between firms that maintain ISO certification and those that do not", *International Journal of Production Research*, Vol.48, No.5, pp.1881-1897, 2007.

[95] Mann, R. & Kehoe, D., "An evaluation of the effects of quality improvement on business performance", *The International Journal of Quality & Reliability Management*, Vol.11, No.4, pp.29-44, 1994.

[96] Martínez - Lorente, A.R., Martínez - Costa, M., "ISO 9000 and TQM: substitutes or complementaries? An empirical study in industrial companies", *The International Journal of Quality & Reliability Management*, Vol.21, No.3, pp.260-

276, 2004.

[97] Matuszak-Flejszman, K., "Benefits of Environmental Management System in Polish Companies Compliant with ISO 14001", *Polish Journal of Environmental Studies*, Vol.18, No.3, pp.411-419, 2009.

[98] Mcadam, R. & Mckeown, M., "Life after ISO 9000: An analysis of the impact of ISO 9000 and total quality management on small businesses in Northern Ireland", *Total Quality Management*, Vol.10, No.2, pp.229-241, 1999.

[99] Mellado, D., Fernandez-Medina, E. & Piattini, M., "A common criteria based security requirements engineering process for the development of secure information systems", *Computer Standards & Interfaces*, Vol.29, pp.244-253, 2007.

[100] Meyer,J. W. & Rowan, B., "Institutionalized Organizations: Formal Structure as Myth and Ceremony", *American Journal of Sociology*, Vol.83, Issue2(Sep.,1977), pp.340-363, 1977.

[101] Miles, M.P., Munilla, L.S. & McClurg, T., "The impact of ISO 14000 environmental management standards on small and medium sized enterprises", *Journal of Quality Management*, Vol.4, No.1, pp.111-122, 1999.

[102] Nair, A and Prajogo, D., "Internalization of ISO 9000 standards: the antecedent role of functionalist and institutionalist drivers and performance implications", *International Journal of Production Research*, Vol 47, No.16, pp.4545-4568, 2009.

[103] Nakamura, M., Takahashi, T. & Vertinsky, I., "Why Japanese firms choose to certify: A study of managerial responses to environmental issues", *Journal of Environmental Economics and Management*, Vol.42, pp.23-52, 2001.

[104] Nishitani, K., "An empirical study of the initial adoption of ISO 14001 in Japanese manufacturing firms", *Ecological Economics*, Vol.68, pp.669-679, 2009.

[105] Oliver, C., "Strategic responses to institutional processes", *Academy of Management Review*, Vol.16, No.1, pp.145-179, 1991.

[106] Oliver, C., "The Antecedents of deinstitutionalization", *Organization Studies*, Vol.13, No.4, pp.563-588, 1992.

[107] Park, C., Jang,S & Park,Y., "A study of effect of information security management system[ISMS] certification on organization performance", *International Journal of*

Computer Science and Network Security, Vol.10, No.3, pp.10-21, 2010.

[108] Piner, M. & Ozgur, C., "The Long-Term impact of ISO 9000 certification on business performance: A longitudinal study using Turkish stock market returns", *The Quality Management Journal*, Vol.14, No.4, pp.21-40, 2007.

[109] Quazi, H.A., Hong, C.W. & Meng, C.T., "Impact of ISO 9000 certification on quality management practices: A comparative study", *Total Quality Management*, Vol.13, No.1, pp.53-67, 2002.

[110] Rao, S.S., Ragu-Nathan, T.S. & Solis, L.S., "Does ISO 9000 have an effect on quality management practices? An international empirical study", *Total Quality Management & Business Excellence*, Vol.8, No.6, pp.335-346, 1997.

[111] Rarmad, B., Supangkat, S.H., Sembiring, J. & Surrendo, K., "Threat Scenario Dependency-Based Model of Information Security Risk Analysis International", *Journal of Computer Science and Network Security*, Vol.10, No.8, pp.93-102, 2010.

[112] Rogers, R. W., "A protection motivation theory of fear appeals and attitude change", *The Journal of Psychology*, Vol.91, No.5, pp.93- 114, 1975.

[113] Saleh, Z.I., Refai, H. & Mashhour, A., "Proposed Framework for Security Risk Assessment", *Journal of Information Security*, Vol.2, pp.85-90, 2011.

[114] Sampaio,P. Saraiva,P. & Rodrigues, A.G., "ISO 9001 certification research: questions, answers and approaches", *International Journal of Quality & Reliability Management*, Vol.26, No.1, pp.38-58, 2009.

[115] Satoh, N., Kumamoto, H., "Analysis of Information Security Problem by Probabilistic Risk Assessment", *International Journal of Computers*, Issue.3, Vol.3, pp.337-347, 2009.

[116] Satoh, N., Kumamoto, H., "Viewpoint of Probabilistic Risk Assessment in Information Security Audit", *International Journal of Computers*, Issue.4, Vol.3, pp.368-376, 2009.

[117] Seddon, J., *The Case Against ISO 9000*, Oak Tree Press (Ireland), 2000.

[118] Seddon, J., "ISO 9000: an economic disease?" *European Quality*, Vol.11, No.2, pp.42-47, 2005.

[119] Shameli-Sendi, A., Shajari, M., Hassanabadi, M., Jabbarifar, M. & Dagenais, M.," Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment",

The Open Cybernetics & Systemic Journal, Vol.6, pp.26-37, 2012.

[120] Shannon,W. Anderson,J. Daniel,Daly. & Marilyn,F.Johnson., "Why firms seek ISO 9000 certification: Regulatory compliance or competitive advantage?", *Production and Operations Management*, Vol.8 No.1, pp.28-43, 1999.

[121] Sharma, D.H., "The association between ISO9000 certification and financial performance", *The International Journal of Accounting*, Vol.40, pp.151-172, 2005.

[122] Shimada,T. & Okamoto,N., "Effectiveness of ISO9001 System Implementation in Japanese Companies", *Kobe University discussion paper series*, 2010.

[123] Singels, J., Ruel, G & Henny, W., "ISO 9000 series - Certification and performance", *The International Journal of Quality and Reliability Management*, Vol.18, No.1, pp.62-75, 2001.

[124] Sun, Hongyi., "Total quality management, ISO 9000 certification and performance improvement", *The International Journal of Quality and Reliability Management*, Vol.17, No.2, pp.168-179, 2000.

[125] Sun, Y., Wang, N., Guo, X., and Peng, Z., "Understanding the Acceptance of Mobile Health Service: A Comparison and Integration of Alternative Models", *Journal of Electronic Commerce Research*, Vol. 14(2), 2013, pp.183-200.

[126] Takahashi, T. & Nakamura, M., "The impact of operational characteristics on firm's EMS decisions: Strategic adoption of ISO14001 certification", *Corporate Social Responsibility and Environmental Management*, Vol.17, pp.215-229, 2010.

[127] Tang, J & Lee, S.C., "The effect of organizational factors on managerial satisfaction with ISO9001 quality standard certification: An empirical study", *International Journal of Management*, Vol.26, No.1, pp.107-114, 2009.

[128] Texeira-Quiros, J., Almaca, J.A. & Fernandes-Justino, M.R., "How quality affects the bottom line?: A literature review", *Intangible Capital*, Vol.6, No.2, pp.258-271, 2010.

[129] Tolbert, P.S. & Zucker, L.G., "The institutionalization of institutional theory", *Handbook of Organization Studies*, Vol.44, Issue.020, pp.175-190, 1996

[130] Tsekouras, K., Dimara, E. & Skuras, D., "Adoption of a quality assurance scheme and its effect on firm performance: A study of Greek firms implementing ISO 9000", *Total Quality Management*, Vol.13, No.6, pp.827-841, 2002.

[131] Turk, A.M., “The benefits associated with ISO 14001 certification for construction firms: Turkish case”, *Journal of Cleaner Production*, Vol.19, pp.559-569, 2009.

[132] Weeger, A., Wang, X., Gewald, H., Raisinghani, M., Sanchez, O., Grant, G., and Pittayachawan, S., ”Determinants of Intention to Participate in Corporate BYOD-Programs: The Case of Digital Natives”, *Information Systems Frontiers*, pp.1-17, 2018.

[133] Wright, S., “Measuring Security Effectiveness with ISO 27001”, *ISSA Journal*, pp.34-37, 2006.

[134] Yaghoubi, N., and Bahmani, E., “Factors Affecting the Adoption of Online Banking An Integration of Technology Acceptance Model and Theory of Planned Behavior”, *International Journal of Business and Management*, Vol. 5, No.9, pp.159-165, 2010.

[135] Yin,H & Schmedler,P.J., “Why do standardized ISO14001 environmental management system lead to heterogeneous environmental outcome?”, *Business strategy and the Environment*, Vol.18, pp.469-486, 2009.

[136] Yoon, C., Hwang, J., and Kim, R., ”Exploring Factors That Influence Students’ Behaviors in Information Security”, *Journal of Information Systems Education*, Vol. 23(4), pp.407-415, Winter 2012.

[137] Yoshida,K., “Deming Management Philosophy : Does It Work in the US as Well as in Japan?”, *The Columbia Journal of World Business*, pp.10-17, 1989.

[138] Yoshida,K., “Revisiting Deming's 14 Points in light of Japanese Business Practice” *Quality Management Journal ASQC*, Vol.3, Issue1, pp.14-30, 1996.

[139] Zhao, D., Wang, C., Ma, J., “A Risk Assessment Method of The Wireless Network Security”, *Journal of Electronics (China)*, Vol.24, No.3, pp.425-432, 2007.

[140] 天野裕子・大木榮二郎「外部委託における個人情報漏洩に関わる課題の研究」『日本セキュリティ・マネジメント学会誌』第 25 巻，第 1 号，3-24 ページ，2011 年.

[141] 甘利康文「状況的犯罪予防論による内部不正・事故抑制手法」『内部不正対策 14 の論点』175-198 ページ，2015 年.

[142] 甘利康文・新井真司・内田純一「セキュリティ実現の原点から見た内部要因事故抑制手法」『JNSA Press』第 33 号，3-29 ページ，2012 年 3 月.

[143] 荒井正人・甲斐賢・永井康彦・冨田理「情報漏洩システムの提案」『情報処理学会研究報告』 2004 - CSEC - 24, 61–67 ページ, 2004 年 3 月.

[144] 有賀正彦『仕組みが無くてダメな会社 仕組みがあってもダメな会社　ISO 思考で考察する組織不祥事』, 日刊工業新聞社, 2008 年.

[145] 芦野佑樹,・佐々木良一「セキュリティデバイスとヒステリシス署名を用いたデジタルフォレンジックシステムの提案と評価」『情報処理学会論文誌』Vol.49, No.2, 999-1009 ページ, 2008 年.

[146] 渥美清隆・浅原慎哉「情報資産間の依存性を考慮した情報リスクアセスメント法」『情報処理学会研究報告』2005-DSM-37, 53-56 ページ, 2005 年.

[147] 飯塚悦功「マネジメントシステム規格の現状・課題・展望～社会・適用組織にとっての意義, そして有効活用～」『予防時報』第 227 号, 30-35 ページ, 2006 年.

[148] 井川将・黒田浩司・鈴木栄幸・森本康彦・横山節雄・宮寺庸造「情報セキュリティ行動と情報関連知識の関係分析」『日本情報科教育学会誌』第 2 巻, 第 1 号, 2009 年, 18–26 ページ.

[149] 井戸田博樹「情報セキュリティ・マネジメントにおけるセキュリティ・コミュニケーションの意義と推進策」『日本セキュリティ・マネジメント学会誌』第 19 巻, 第 1 号, 15-25 ページ, 2005 年.

[150] 岩橋建治「組織環境の脱制度化プロセスと組織間コンフリクト：タクシー運賃規制緩和を事例として」『日本経営学会誌』第 11 巻, 39-50 ページ, 2004 年.

[151] 岩田裕樹『環境情報管理と企業戦略・組織』, 京都大学博士学位論文, 2007 年.

[152] 岩田和之・有村俊秀・日引聡「ISO14001 認証取得の決定要因とトルエン排出量削減効果に関する実証研究」『日本経済研究』第 62 巻, 16-38 ページ, 2010 年.

[153] MS 信頼性ガイドライン対応委員会『MS 信頼性ガイドライン対応委員会　報告書』, MS 信頼性ガイドライン対応委員会, 2009 年.

[154] NRI セキュアテクノロジーズ『企業における情報セキュリティ実態調査 2010～アンケートから見えた企業における情報セキュリティの現状～』, NRI セキュアテクノロジーズ, 2010 年.

[155] NRI セキュアテクノロジーズ『企業における情報セキュリティの実態と課題「企業における情報セキュリティ実態調査 2011」の結果と, それを踏まえた提言』, NRI セキュアテクノロジーズ, 2011 年.

[156] NRI セキュアテクノロジーズ『企業における情報セキュリティ実態調査 2012』, NRI セキュアテクノロジーズ, 2013 年.

[157] 大木栄二郎「委託契約に伴う保証型セキュリティ監査の具体的意味－保証型情報セキュリティ監査の促進に向けて－」『日本セキュリティ・マネジメント学会誌』第 20 巻, 第 3 号, 40-49 ページ, 2006 年.

[158] 岡本卓馬「情報セキュリティにおけるリスクの定量化手法」『UNISYS TECHNOLOGY REVIEW』第 86 号, 86-96 ページ, 2005 年.

[159] 岡野裕樹・奥山浩伸「セキュリティルール違反行動の抑止に関する一考察」『情報処理学会論文誌』第 58 巻, 第 1 号, 258–268 ページ, 2017 年.

[160] 小塩真司『第 2 版はじめての共分散構造分析 - Amos によるパス解析』, 東京図書, 2014 年.

[161] 亀山嘉和「総論：マネジメントシステム認証制度の課題と解決法」『品質』第 41 巻, 第 2 号, 150-158 ページ, 2011 年.

[162] 加藤慧,・小宮山功一朗・瀬古敏智・一瀬友祐・河野耕平・中山心太・吉浦裕「コンテンツベースフィッシング検知手法大規模実例評価と改良」『日本セキュリティ・マネジメント学会誌』第 25 巻, 第 2 号, 42-56 ページ, 2011 年.

[163] 加藤岳久・中澤優美子・漁田武雄・山田文康・山本匠・西垣正勝「本人認証技術におけるユーザの性格とセキュリティ意識との相関に関する考察」『情報処理学会論文誌』第 52 巻, 第 9 号, 2537-2548 ページ, 2011 年.

[164] 川中孝章・六川修一「クラウドサービス市場における情報セキュリティ監査のゲーム理論的考察」『日本セキュリティ・マネジメント学会誌』第 26 巻, 第 2 号, 3-23 ページ, 2012 年.

[165] 川中孝章・六川修一「情報セキュリティの脅威・脆弱性・対策に関する構造分析－決定論的事象と確率論的事象の二重構造－」『日本経営システム学会誌』第 28 巻, 第 2 号, 149-157 ページ, 2011 年.

[166] 菊地貴志・中條武志「作業者を教育・訓練・動機付けする方法と標準に従って作業していなかったミスとの関係」『品質』第 30 巻, 第 2 号, 63–71 ページ, 2000 年 4 月.

[167] 北野晴人『日本的経営における内部不正行為抑止の研究』,情報セキュリティ大学院大学博士学位論文, 2015 年.

[168] 喜屋武昌健「企業における環境管理システム（ISO14001）と改善活動の有効性」『産業総合研究』第 13 巻, 71-88 ページ, 2005 年.

[169] 久米均『統計解析への出発シリーズ入門統計的手法 1』, 岩波書店, 54-61 ページ,

1989 年.

[170] 呉洋・小崎真寛・岡田健一「プロジェクトの特性を考慮した最適なセキュリティ対策選定手法」『情報処理学会論文誌』第 54 巻，第 1 号, 309-317 ページ, 2013 年.

[171] 経済産業省『事業リスクマネジメント ： テキスト』，経済産業省，2004 年.

[172] 経済産業省『「マネジメントシステム規格認証制度の信頼性確保のためのガイドライン」の公表について』，経済産業省, 2008 年.

[173] 経済産業省『平成 23 年度個人情報の保護に関する取組実態調査報告書』，経済産業省, 2012 年.

[174] 小池俊雄・吉谷崇・白川直樹・澤田忠信・宮代信夫・井上雅也・三阪和弘・町田　勝・藤田浩一郎・河野真巳・増田満・鈴木孝衣・深田伊佐夫・相ノ谷修通「環境問題に対する心理プロセスと行動に関する基礎的考察」『水工学論文集』第 47 巻，2003 年, 361-366 ページ.

[175] 個人情報保護委員会『個人情報の保護に関する法律についてのガイドライン（通則編)』，個人情報保護委員会，2017 年.

[176] 櫻田貴道「組織論における制度学派の理論構造」『経済論羨（京都大学)』第 172 巻，第 3 号，54-69 ページ，2003 年.

[177] 佐々木明穂・和田武「「KES・環境マネジメントシステム・スタンダード」とその認証取得企業の研究」『立命館産業社会論集』第 40 巻，第 2 号, 93-112 ページ，2004 年.

[178] 佐々木良一・吉浦裕,・伊藤信次「不正コピー対策の最適組合せに関する考察」『情報処理学会論文誌』第 43 巻，第 8 号, 2435-2446 ページ, 2002 年.

[179] 佐藤秀典「正当性獲得のジレンマ－損害保険業における近視眼的問題対応－」『組織科学』第 44 巻，第 1 号，74-84 ページ，2010 年.

[180] 佐藤郁哉「大学の歩き方：新制度派組織理論のレンズで見る高等教育」，一橋論叢，第 133 巻，第 4 号，341-358 ページ，2005 年.

[181] 佐藤郁哉,・山田真茂留『制度と文化 －組織を動かす見えない力』，日本経済新聞出版社，2004 年.

[182] 沢田篤史・高倉弘喜・岡部寿男「開放型大規模ネットワークのための IDS ログ監視支援システム」『情報処理学会論文誌』第 44 巻，第 8 号，1861-1871 ページ，2003 年.

[183] 芝口誠仁・稲葉太郎・中山佑輝・岡田謙一「仕事量を考慮したセキュリティ対策選定手法」『情報処理学会論文誌』第 51 巻，第 2 号，648-657 ページ，2010 年.

[184] 柴田陽一・三村昌弘・高橋健太・中村逸一・曽我正和・西垣正勝「メカニズム PKI－指紋からの秘密鍵動的生成」『情報処理学会論文誌』第 45 巻，第 8 号，1833-1844 ページ，2004 年.

[185] 島吉伸・安酸建二・梶原武久「ISO9000 が財務業績に及ぼす影響に関する実証分析」『商経学叢』第 53 巻，第 3 号，365-390 ページ，2007 年.

[186] 島成佳「内部不正による情報セキュリティインシデントにおける内部者の意識と対策に関する分析と考察」『コンピュータセキュリティシンポジウム 2012 論文集』第 2012 巻，第 3 号，539–546 ページ，2012 年 10 月.

[187] 品川佳満・橋本勇人「患者の個人情報取扱い事故のパターンと違反したルールに関する分析」『川崎医療福祉学会誌』第 24 巻，第 2 号，221–227 ページ，2015 年.

[188] システム監査学会情報キュリティ研究プロジェクト『ヒューマンエラーの事例と影響』，システム監査学会，2007 年.

[189] 社会安全研究財団『環境犯罪学と犯罪分析』，社会安全研究財団，2010 年.

[190] 社会安全研究財団情報セキュリティにおける人的脅威対策に関する調査研究会『情報セキュリティにおける人的脅威対策に関する調査研究報告書』，社会安全研究財団情報セキュリティにおける人的脅威対策に関する調査研究会，2010 年.

[191] 情報マネジメントシステム認定センター『ISMS 適合性評価制度』，情報マネジメントシステム認定センター，2018 年.

[192] 情報セキュリティ大学院大学『情報セキュリティ事故対応ガイドブック』，情報セキュリティ大学院大学，2011 年.

[193] 情報処理振興事業協会『コンピュータセキュリティインシデントとその対応に関する調査　調査報告書』，情報処理振興事業協会，2000 年.

[194] 情報処理推進機構『2011 年度情報セキュリティ事象被害状況調査－報告書－』，情報処理推進機構，2012 年.

[195] 情報処理推進機構『2012 年度情報セキュリティの脅威に対する意識調査　報告書』，情報処理推進機構，2012 年.

[196] 情報処理推進機構『組織内部者の不正行為によるインシデント調査－調査報告書－』，情報処理推進機構，2012 年.

[197] 情報処理推進機構『2013 年版 10 大脅威～身近に忍び寄る脅威～』，情報処理推進機構セキュリティセンター, 2013 年.

[198] 情報処理推進機構『安全なウェブサイトの作り方　改訂第 6 版』，情報処理推進機構セキュリティセンター，2012 年.

[199] 情報処理推進機構『組織における内部不正防止ガイドライン』，情報処理推進機構, 2013 年.

[200] 情報処理推進機構『組込みソフトウェア開発における品質向上の勧め[バグ管理手法編]』，情報処理推進機構　技術本部ソフトウェア・エンジニアリング・センター, 2013 年.

[201] 情報処理推進機構『内部不正による情報セキュリティインシデント実態調査 - 調査報告書 - 』，情報処理推進機構，2006 年.

[202] 情報処理推進機構『情報セキュリティ対策ベンチマーク活用集』, 情報処理推進機構, 2008 年.

[203] 情報処理推進機構『組織における内部不正防止ガイドライン　第 3 版』，情報処理推進機構，2015 年.

[204] 情報処理推進機構『内部不正による 情報セキュリティインシデント実態調査　－調査報告書－』，情報処理推進機構，2016 年.

[205] 情報処理推進機構，情報セキュリティマネジメントと PDCA サイクル, https://www.ipa.go.jp/security/manager/protect/pdca/policy.html（2019.07）.

[206] 情報処理推進機構『中小企業の情報セキュリティ対策ガイドライン　第 3 版』，情報処理推進機構，2019 年.

[207] 情報マネジメントシステム認定センター『ISMS 適合性評価制度に関する調査報告書』，情報マネジメントシステム認定センター，2018 年.

[208] 菅野泰子・島田裕次「情報セキュリティ対策における阻害要因の構造に関する企業規模別比較研究」,『日本情報経営学会誌』第 30 巻，第 3 号，109-121 ページ，2010 年.

[209] 菅野泰子「連載（インターネットセキュリティ）8　情報セキュリティマネジメントシステム」『経営情報学会誌』第 13 巻，第 1 号，137-144 ページ，2004 年.

[210] 菅野泰子・寺田真敏・山田安秀・鎌倉稔成・土井範久「企業の情報セキュリティ対策におけるモチベーションの構造に関する考察」『情報処理学会論文誌』第 50 巻，第

9 号，2193–2206 ページ，2009 年.

[211] 鈴木宏幸・内田勝也「情報セキュリティ施策における有効性評価についての一考察」『情報処理学会研究報告』第 2010-DPS-142 巻，第 51 号，1-7 ページ，2010 年.

[212] 鈴木武俊・真田大志「情報セキュリティポリシー運用における課題と対策」『UNISYS TECHNOLOGY REVIEW』第 98 号，337-350 ページ，2008 年 11 月.

[213] 鈴木智也・田沼均・今井秀樹「情報セキュリティ対策間の相互依存関係を用いた内部犯行防止対策のための有効性評価手法」『情報処理学会論文誌』第 52 巻，第 9 号，2575-2585 ページ，2011 年.

[214] 諏訪博彦・原賢・関良明「情報セキュリティ行動モデルの構築　－人はなぜセキュリティ行動をしないのか－」『情報処理学会論文誌』第 53 巻，第 9 号，2204–2212 ページ，2012 年.

[215] 総務省統計局『業種コード表（日本標準産業分類)』，総務省統計局，2007 年.

[216] 総務省統計局，日本標準産業分類（平成 19 年 11 月改定）－分類項目名，http://www.stat.go.jp/index/seido/sangyo/19-3-1.htm（2012 年.2 月）.

[217] 高橋達明・ラミレス・カセレス・ギジェルモ・オラシオ・勅使河原可海「ISO/IEC 17799 の管理項目の関連性を考慮したセキュリティ対策の選択基準の検討」『情報処理学会研究報告』2007-DPS-130，2007-CSEC-36，447-452 ページ，2007 年.

[218] 高取敏夫「ISMS 制度推進の現状について（前編)」『経営情報学会誌』第 14 巻，第 3 号，107-111 ページ，2005 年.

[219] 高取敏夫「ISMS 制度推進の現状について（中編)」『経営情報学会誌』第 14 巻，第 4 号，107-115 ページ，2006 年.

[220] 高取敏夫「ISMS 制度推進の現状について（後編)」『経営情報学会誌』第 15 巻，第 1 号，88-94 ページ，2006 年.

[221] 竹村敏彦・三好祐輔・花村憲一「情報漏えいにつながる行動に関する実証分析」『情報処理学会論文誌』第 56 巻，第 12 号，2191–2199 ページ，2015 年.

[222] 竹尾大輔・伊藤将志・鈴木秀和・岡崎直宣・渡邊晃「コネクションベース方式による踏み台攻撃検出手法の提案」『情報処理学会論文誌』第 48 巻，第 2 号，644-655 ページ，2007 年.

[223] 竹下数明，小林偉昭，佐々木良一「脆弱性対策教育のための e ラーニングシステムの開発と評価」『日本セキュリティ・マネジメント学会誌』第 24 巻，第 1 号，17-26

ページ，2010 年.

[224] 田沼均・大塚玲・松浦幹太・今井秀樹「Gordon-Loeb-Lucyshyn モデルを拡張した情報セキュリティ情報共有のインセンティブ分析」『日本セキュリティ・マネジメント学会誌』第 23 巻，第 2 号，3-16 ページ，2009 年.

[225] 寺田真敏・萱島信・倉田盛彦・佐々木良一「企業内不正アクセス対策情報サービスシステムの構築」『情報処理学会論文誌』第 41 巻，第 8 号，2246-2254 ページ，2000 年.

[226] 寺田真敏・磯川弘実・永井康彦・倉田盛彦・土居範久「Web サービスを攻略するワーム流布対策方式の提案」『情報処理学会論文誌』第 45 巻，第 12 号，2815-2823 ページ，2004 年.

[227] 寺田真敏・高田眞吾・土居範久「脆弱性対策情報データベース JVN の提案」『情報処理学会論文誌』第 46 巻，第 5 号，1256-1265 ページ，2005 年.

[228] 土井智朗・内田勝也「情報セキュリティ意識向上に向けた効果的なリスクアセスメント手法の提案」『情報処理学会研究報告』2008-CSEC-43，43-48 ページ，2008 年.

[229] 東京証券取引所『上場会社数の推移』，東京証券取引所，2011 年.
http://www.tse.or.jp/listing/companies/b7gje6000000pj9r-att/b7gje6000000pjqx.pdf(2014 年 2 月)

[230] 東京証券取引所『新規上場ガイドブック 2015（市場第一部・第二部編)』，東京証券取引所，2015 年.

[231] 豊田秀樹『共分散構造分析[疑問編]』，朝倉書店，2003 年.

[232] 豊田秀樹『共分散構造分析 - Amos 編』，東京図書，2013 年.

[233] 豊田秀樹『共分散構造分析 - R 編』，東京図書，2014 年.

[234] 内閣官房情報セキュリティセンター『外部委託における情報セキュリティ対策に関する評価手法の利用の手引』，内閣官房情報セキュリティセンター，2011 年.

[235] 永田靖『入門統計解析法』，日科技連出版社，213-217 ページ，1992 年.

[236] 永井康彦・藤山達也・佐々木良一「セキュリティ対策目標の最適決定技法の提案」『情報処理学会論文誌』第 41 巻，第 8 号，2264-2271 ページ，2000 年.

[237] 内閣官房情報セキュリティセンター『外部委託における情報セキュリティ対策実施規程策定手順書』，内閣官房情報セキュリティセンター，2011 年.

[238] 中條武志・吉井克宜・菊地貴志「作業管理システムが作業ミスの発生に与える影響」

『品質』第 29 巻，第 2 号，111–119 ページ，1999 年 4 月.

[239] 中條武志『人に起因するトラブル・事故の未然防止と RCA～未然防止の観点からマネジメントを見直す』，日本規格協会，2010 年.

[240] 中村修・後藤大太郎・山口龍虎・清水耕平・遠藤はる奈「ISO14001 のシステムに関わる問題と運用上の問題」『長崎大学総合環境研究』第 8 巻, 第 1 号, 47-56 ページ, 2006 年.

[241] 中村逸一・兵頭敏之・曽我正和・水野忠則・西垣正勝「セキュリティ対策選定の実用的な一手法の提案とその評価」『情報処理学会論文誌』第 45 巻，第 8 号，2022-2033 ページ，2004 年.

[242] 日本規格協会『対訳 ISO9001 品質マネジメントの国際規格』，日本規格協会，2001 年.

[243] 日本規格協会『適合性評価－適合性評価機関の認定を行う機関に対する一般要求事項 JIS Q 17011:2005（ISO/IEC 17011:2004）』，日本規格協会, 2007 年 a.

[244] 日本規格協会『適合性評価－マネジメントシステムの審査及び認証を行う機関に対する要求事項 JIS Q 17021:2007（ISO/IEC 17021:2006）』，日本規格協会，2007 年 b.

[245] 日本規格協会『ISMS ガイド（Ver.1.0）』，日本規格協会，2002 年.

[246] 日本規格協会『ISMS ユーザーズガイド－JIS Q 27001:2006（ISO/IEC 27001:2005）対応－』，日本規格協会，2008 年.

[247] 日本規格協会『情報技術－セキュリティ技術－情報セキュリティマネジメントシステムの審査及び認証を行う機関に対する要求事項 JIS Q 27006:2008（ISO/IEC 27006:2007）』，日本規格協会，2008 年.

[248] 日本規格協会『IMS 認証機関認定の手順 (JIP-IMAC110-2.2)』，日本規格協会，2010 年.

[249] 日本規格協会『情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項 JIS Q 27001:2014（ISO/IEC 27001:2013）』, 日本規格協会, 2014 年.

[250] 日本規格協会『個人情報保護マネジメントシステム－要求事項　JIS Q 15001：2017』, 日本規格協会，2017 年.

[251] 日本情報経済社会推進協会，ISMS 認証取得組織検索, http://www.isms.jipdec.or.jp/lst/ind/index.html （2012 年 2 月）.

[252] 日本情報経済社会推進協会『ISMS ユーザーズガイド - JIS Q 27001:2014（ISO/IEC 27001:2013）対応』，日本情報経済社会推進協会，2014 年.

[253] 日本情報処理開発協会『ISMS 構築事例集　～情報セキュリティへの取組み事例～』，日本情報処理開発協会，2005 年.

[254] 日本情報処理開発協会『外部委託における ISMS 適合性制度の活用方法－JIS Q 27001:2006 対応－』，日本情報処理開発協会，2006 年.

[255] 日本情報処理開発協会『ISMS ユーザーズガイド－JIS Q 27001:2006（ISO/IEC 27001:2005）対応－リスクマネジメント編』，日本情報処理開発協会，2008 年.

[256] 日本情報処理開発協会『IMS 認証機関の認定に関わる料金（JIP-IMAC-2.2)』，日本情報処理開発協会，2010 年.

[257] 日本能率協会審査登録センター『2006 年 ISMS の JIS 化対応　審査員が教える ISO27001 実践導入マニュアル』，日本能率協会マネジメントセンター，2006 年.

[258] 日本ネットワークセキュリティ協会『2005 年情報セキュリティインシデントに関する調査報告書 Ver.1.0』，日本ネットワークセキュリティ協会，2006 年.

[259] 日本ネットワークセキュリティ協会『2006 年情報セキュリティインシデントに関する調査報告書 Ver.2.1』，日本ネットワークセキュリティ協会，2007 年.

[260] 日本ネットワークセキュリティ協会『2007 年情報セキュリティインシデントに関する調査報告書 Ver.1.6』，日本ネットワークセキュリティ協会，2008 年.

[261] 日本ネットワークセキュリティ協会『2008 年 情報セキュリティインシデントに関する調査報告書 Ver.1.3』，日本ネットワークセキュリティ協会，2009 年.

[262] 日本ネットワークセキュリティ協会『2009 年 情報セキュリティインシデントに関する調査報告書 Ver.1.1』，日本ネットワークセキュリティ協会，2010 年.

[263] 日本ネットワークセキュリティ協会『2010 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　Ver.1.4』, 日本ネットワークセキュリティ協会，2011 年 a.

[264] 日本ネットワークセキュリティ協会『2010 年 情報セキュリティインシデントに関する調査報告書　～発生確率編～　Ver.1.4』，日本ネットワークセキュリティ協会, 2011 年 b.

[265] 日本ネットワークセキュリティ協会『2011 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　Ver.1.3』, 日本ネットワークセキュリティ

協会，2014 年 a.

[266] 日本ネットワークセキュリティ協会『2012 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　Ver.1.2』, 日本ネットワークセキュリティ協会，2014 年 b.

[267] 日本ネットワークセキュリティ協会『2013 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　Ver.1.2』, 日本ネットワークセキュリティ協会，2015 年.

[268] 日本ネットワークセキュリティ協会『2014 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　Ver.1.1』, 日本ネットワークセキュリティ協会，2016 年 a.

[269] 日本ネットワークセキュリティ協会『2015 年 情報セキュリティインシデントに関する調査報告書【速報版】 Ver.1.0』，日本ネットワークセキュリティ協会，2016 年 b.

[270] 日本ネットワークセキュリティ協会『2016 年 情報セキュリティインシデントに関する調査報告書　～個人情報漏えい編～　Ver.1.2』, 日本ネットワークセキュリティ協会，2017 年.

[271] 日本ネットワークセキュリティ協会『2017 年 情報セキュリティインシデントに関する調査報告書【速報版】 第 1.0 版』，日本ネットワークセキュリティ協会，2018 年.

[272] 日本ネットワークセキュリティ協会『2018 年 情報セキュリティインシデントに関する調査報告書【速報版】』，日本ネットワークセキュリティ協会，2019 年.

[273] 西沢隆二『ISO マネジメントシステムの崩壊は何故起きたか』, 近代文藝社, 2009 年.

[274] 沼田晋作・柴田賢介・岡崎聖人・高橋克巳「企業における情報セキュリティ基準と対策の関係に関する一考察」『情報処理学会研究報告』第 2009-CSEC-46 巻, 第 39 号, 1-8 ページ，2009 年.

[275] 野口敦弘・納富一宏・斎藤恵一「自己組織化マップを用いたタッチスクリーンによるリズム認証手法」『バイオメディカル・ファジィ・システム学会誌』第 15 巻，第 1 号，31-39 ページ，2013 年.

[276] ニューメディア開発協会『ISMS 第三者認証制度をより有効なものにするための ISMS 認証事業所調査概要報告書』，ニューメディア開発協会，2011 年.

[277] 馬場俊幸・武政剛弘・江頭和彦「大学における ISO14001 認証取得の現状と特徴」『九大農学芸誌』第 61 巻，第 1 号，7-23 ページ，2006 年.

[278] 濱田良隆・廣松毅「情報セキュリティにおける逸脱行動の助長及び抑止要因に関する考察 - 組織構成員による情報持ち出し逸脱行動についてのアンケート調査結果分析 - 」『経営情報学会誌』第 21 巻，第 3 号，205–226 ページ，2012 年 12 月.

[279] 浜屋敏「情報セキュリティと組織感情, Enterprise 2.0」『富士通総研経済研究レポート』第 345 巻，2009 年 6 月.

[280] 原田要之助「大規模な情報漏えい事件の特性と対策の考え方」『情報セキュリティ総合科学』第 4 号，183-195 ページ，2012 年.

[281] 八田信二『これだけは知っておきたい内部統制の考え方と実務』，日本経済新聞社，2006 年.

[282] 引田邦夫・眞田史行・八木裕子・中條武史「ISO9000 シリーズの有効性に関する調査研究」『品質』第 25 巻，第 4 号，95-105 ページ，1995 年.

[283] 平野晃治「オブジェクト指向評価基準設計法による情報セキュリティマネジメント規準の要求内容解釈及び調査項目設計」『日本セキュリティ・マネジメント学会誌』第 19 巻，第 1 号，44-57 ページ，2005 年.

[284] 廣瀬毅士・寺島拓幸『社会調査のための統計データ分析』，オーム社，197-202 ページ，2010 年.

[285] 藤川真樹・青木洋之・西垣正勝・吉澤昌純・辻井重男「制服を着た部外者を検知できるオフィス・セキュリティ・システムの提案－ずる賢い悪人から事業所を守るために－」『日本セキュリティ・マネジメント学会誌』第 21 巻，第 2 号，43-54 ページ，2007 年.

[286] 福永弘之「グローバル・スタンダードとオフィス(3)－個人情報保護法・情報セキュリティマネジメントから個人情報セキュリティマネジメントを考える－」『兵庫県立大学環境人間学部研究報告』第 8 号，19-30 ページ，2006 年.

[287] 福澤寧子・石田修一・平岩賢志・瀬戸洋一「自律分散制御路側網システムのセキュリティ機能の開発」『情報処理学会論文誌』第 44 巻，第 12 号，3090-3097 ページ，2003 年.

[288] 文倉斉・小林哲郎・佐々木良一「個人情報漏洩の地域特性に関する統計分析と考察」『日本セキュリティ・マネジメント学会誌』第 25 巻，第 3 号，15-23 ページ，2011

年.

[289] 堀康則「情報セキュリティ対策の実装に際して納得性を確保するための一考察」『日本セキュリティ・マネジメント学会誌』第 20 巻，第 2 号，19-27 ページ，2006 年.

[290] 牧田正裕「高等教育機関のアカウンタビリティとコントロール－経営・会計系大学院，学部における国際認証の動向を中心に－」『国際会計学会年報 2009 年度』，111-125 ページ，2009 年.

[291] 舛本 匡宏・角南靖夫「広島県内の ISO14001 認証取得（審査登録）企業の現状と対策」『社会科学研究』，第 10 巻，45-56 ページ，2004 年.

[292] 松岡譲・原沢英夫・高橋潔「地球環境問題へのシナリオアプローチ」『土木学会論文誌』第 678/Ⅶ-19 巻，1-11 ページ，2001 年.

[293] 三木朋乃「制度的圧力の生成・変容のメカニズム－日本における ISO14001 の普及事例分析－」『組織科学』第 41 巻，第 3 号，43-54 ページ，2008 年 a.

[294] 三木朋乃『日本における ISO14001 の普及メカニズム－組織の同型化プロセスの視点から－』，一橋大学博士学位論文，2008 年 b.

[295] 美濃英雄・丸谷一耕・中村修「ISO14001 における審査機関と有効性審査」,『長崎大学総合環境研究』第 13 巻，第 1 号，15-20 ページ，2010 年.

[296] 水沼彩子・澤近俊輔・新原功一・鈴木宏幸・宮本智・村上靖・大和田竜児・小野康史・星智恵・内田勝也「ISMS 認証取得及びその継続における課題と解決策について」『情報処理学会研究報告』第 2009-CSEC-46 巻，第 12 号，1-8 ページ，2009 年.

[297] 村上靖・内田勝也「情報セキュリティ事件・事故の分析と対策に関する考察」『情報処理学会研究報告』2010-DPS-142 No.45，2007-CSEC-48 No.45，2010 年.

[298] リスクマネジメント規格活用検討会『ISO 31000:2009 リスクマネジメント解説と適用ガイド』，日本規格協会，2010 年.

[299] 山田真茂留「構築主義的組織観の彼方に－社会学的組織研究の革新－」『組織科学』第 36 巻，第 3 号，46-58 ページ，2003 年.

[300] 山田吉輝・玉田俊平太「日本の製造業における ISO9000 認証取得と財務業績との関係」『研究 技術 計画』第 24 巻，第 1 号，101-111 ページ，2009 年.

[301] 山口高康・青野博・本郷節之・松浦幹太「分類された情報セキュリティ対策に依存する脅威発生率を導入したリスクアセスメントモデル」『情報処理学会研究報告』，2006-CSEC-33，7-12 ページ，2006 年.

[302] 山倉健嗣「組織間関係と組織間関係論」『横浜経営研究』第 16 巻，第 2 号，166-178 ページ，1995 年.

[303] 山倉健嗣『組織間関係－企業間ネットワークの変革に向けて－』，有斐閣，1993 年.

[304] 安田雪・高橋伸夫「同型化メカニズムと正当性－経営学輪講 DiMaggio and Powell」『赤門マネジメント・レビュー』第 6 巻，第 9 号，2007 年.

[305] 吉田健一郎・島田達巳「地方自治体における情報セキュリティ・レベルの向上～倫理的接近の必要性とその展開～」『日本セキュリティ・マネジメント学会誌』第 23 巻，第 2 号，17-33 ページ，2009 年.

[306] 吉野直人「組織ルーティン研究のアイデンティティ：仕事実践を組織化するデザイン原理の探求」『日本情報経営学会誌』第 34 巻，第 2 号，84–96 ページ，2014 年 2 月.

[307] 吉澤正『対訳 ISO14001:2004 環境マネジメントシステム』, 財団法人日本規格協会, 2005 年.

付録１：オッズ比の 95%信頼区間の導出

表 3-1 を以下にて一般化する.

	インシデント発生あり	インシデント発生なし	合計
認証あり	CA	CN	C_1
認証なし	NA	NN	C_2

母オッズ比を OR ，標本オッズ比を or，$ln(OR)$の標準誤差をSE_{OR}とする.

このとき$Z = \frac{ln(or)-ln(OR)}{SE_{OR}}$である.

95%信頼区間は以下であらわせる.

$$ln(or) - 1.96SE_{OR} \leq ln(OR) \leq ln(or) + 1.96SE_{OR}$$

すなわちオッズ比の信頼区間は以下②式により求めることができる.

$$exp[ln(or) \pm 1.96SE_{OR}] \quad \cdots②$$

ここで永田（1992）によれば確率変数xが$B(n,P)$に従うとき,

$\widehat{P^*} = \frac{x+0.5}{n+1}$　は近似的に　$N\left(P, \frac{P(1-P)}{n}\right)$　に従う.

※$\widehat{P^*}$は離散変量をもとに連続変量の分布に近似した確率

これより

$$B(C_1, P_1) \rightarrow N\left(P_1, \frac{P_1(1-P_1)}{C_1}\right) \quad \cdots③$$

$$B(C_2, P_2) \rightarrow N\left(P_2, \frac{P_2(1-P_2)}{C_2}\right)$$

と近似することができる.

$\widehat{\omega_1} = \frac{\widehat{p_1}}{1-\widehat{p_1}}$, $\widehat{\omega_2} = \frac{\widehat{p_2}}{1-\widehat{p_2}}$とすると

$$\begin{aligned}\frac{\partial}{\partial p} ln(\widehat{\omega_1}) &= \frac{\partial}{\partial \omega} ln(\widehat{\omega_1}) \cdot \frac{\partial \omega}{\partial p} \\ &= \frac{1}{\widehat{\omega_1}} \cdot \frac{\partial}{\partial p} \frac{\widehat{p_1}}{1-\widehat{p_1}} \\ &= \frac{1-\widehat{p_1}}{\widehat{p_1}} \cdot \frac{\widehat{p_1}}{(1-\widehat{p_1})^2} \\ &= \frac{1}{\widehat{p_1}(1-\widehat{p_1})} \quad \cdots④\end{aligned}$$

デルタ法によれば確率変数xが正規分布$N(\mu,\sigma^2)$に従うとき，$y=f(x)$は正規分布$N(f(\mu),\{f'(\mu)\}^2\sigma^2)$に近似的に従う．

デルタ法より

$$V(ln(\widehat{\omega_1})) \approx \{f'(ln(\widehat{\omega_1}))\}^2 \cdot V(\widehat{p_1})$$

③および④より

$$= \left(\frac{1}{\widehat{p_1}(1-\widehat{p_1})}\right)^2 \cdot \frac{\widehat{p_1}(1-\widehat{p_1})}{C_1} = \frac{1}{C_1\widehat{p_1}(1-\widehat{p_1})} \quad \cdots⑤$$

同様に

$$V(ln(\widehat{\omega_2})) \approx \frac{1}{C_2\widehat{p_2}(1-\widehat{p_2})} \quad \cdots⑥$$

とすることができる．

ここで

$$\widehat{OR} = \frac{\widehat{\omega_1}}{\widehat{\omega_2}}$$

であることから

$$V(ln(\widehat{OR})) = V\left(ln\left(\frac{\widehat{\omega_1}}{\widehat{\omega_2}}\right)\right)$$
$$= V(ln(\widehat{\omega_1})) + V(ln(\widehat{\omega_2}))$$

⑤および⑥より

$$= \frac{1}{C_1\widehat{p_1}(1-\widehat{p_1})} + \frac{1}{C_2\widehat{p_2}(1-\widehat{p_2})}$$
$$= \frac{1}{\widehat{p_1}C_1} + \frac{1}{(1-\widehat{p_1})C_1} + \frac{1}{\widehat{p_2}C_2} + \frac{1}{(1-\widehat{p_2})C_2}$$

C_1に$CA+CN$を，C_2に$NA+NN$を代入する

$$= \frac{1}{\widehat{p_1}(CA+CN)} + \frac{1}{(1-\widehat{p_1})(CA+CN)} + \frac{1}{\widehat{p_2}(NA+NN)} + \frac{1}{(1-\widehat{p_2})(NA+NN)}$$
$$= \frac{1}{CA} + \frac{1}{CN} + \frac{1}{NA} + \frac{1}{NN}$$

以上より

$$SE_{OR} = \sqrt{V(ln(or))}$$

$$= \sqrt{\frac{1}{CA} + \frac{1}{CN} + \frac{1}{NA} + \frac{1}{NN}} \quad \cdots⑦$$

となる．

②に⑦を代入すると

$$exp\left[ln(or) \pm 1.96\sqrt{\frac{1}{CA}+\frac{1}{CN}+\frac{1}{NA}+\frac{1}{NN}}\right]$$

となり，式①が導出される．

付録２：認識を通じた不正行為の正当化抑制に関する質問紙調査項目

No	因子	観測変数	設問	評価尺度
1	不正行為の正当化	ルールの妥当感のなさ	定められているルールに妥当感がなければ、会社の許可がなくとも、情報を社外に持ち出してもかまわない	「７：非常にそう思う」から「１：まったくそう思わない」の７段階リッカート尺度で評価
2		手間・効率	手間や業務効率の改善につながるのであれば、会社の許可がなくとも、情報を社外に持ち出してもかまわない	
3		自己帰属意識	自分が作り出した情報であれば、会社の許可がなくとも、情報を社外に持ち出してもかまわない	
4		職場環境	周りの従業員が持ち出していれば、自身も会社の許可なく、情報を社外に持ち出してかまわない	
5		例外業務の発生	顧客要求により、規定のルール以外の対応が求められる場合や、緊急で対応すべき業務が発生した場合、会社の許可がなくとも、情報を社外に持ち出してもかまわない	
6		多忙	多忙により業務時間内に作業を終わらせることができない場合、会社の許可がなくとも、情報を社外に持ち出してもかまわない	
7		ルールの有効性のなさ	ルールが有効に機能していなければ、会社の許可がなくとも、情報を社外に持ち出してもかまわない	
8	方針の認識度	セキュリティの重要性	情報セキュリティを実現することがなぜ重要性かを認識している	「７：よく認識している」から「１：まったく認識していない」の７段階リッカート尺度で評価
9		トップの意思	情報セキュリティに対する経営者の意思を認識している	
10		フレームワーク	情報セキュリティを維持するために必要な枠組み（リスクアセスメントなど）を認識している	
11		実施すべき対策	情報セキュリティ対策として何を実施すべきかを認識している	
12		組織の責任	情報セキュリティ上、組織に課されている責任（遵守べき事項など）を認識している	
13	自らの貢献の認識度	関連文書	自社の情報セキュリティ関連文書（規程類や手順など）を認識している	「７：よく認識している」から「１：まったく認識していない」の７段階リッカート尺度で評価
14		利害関係者からの期待	情報セキュリティにおける利害関係者（取引先、従業員など）からの期待を認識している	
15		役割、責任および力量	情報セキュリティにおいて組織から課されている自身の役割および責任について認識している	
16		機会	情報セキュリティを実現することにより、好影響を与える事項を認識している	
17		セキュリティ目的	情報セキュリティ上、達成すべき目的を認識している	
18	不正行為による影響の認識度	業務の停止	不正な情報の持ち出しがおこなわれると、自社の情報漏えいにつながり、業務の停止に追い込まれる恐れがある	「７：非常にそう思う」から「１：まったくそう思わない」の７段階リッカート尺度で評価
19		取引の停止	不正な情報の持ち出しがおこなわれると、自社の情報漏えいにつながり、取引先との取引停止に追い込まれる恐れがある	
20		対策コスト	不正な情報の持ち出しがおこなわれると、自社の情報漏えいにつながり、多大な対策コストが発生する恐れがある	
21		損害賠償	不正な情報の持ち出しがおこなわれると、自社の情報漏えいにつながり、多大な損害賠償が請求される恐れがある	
22		社会的信用の低下	不正な情報の持ち出しがおこなわれると、自社の情報漏えいにつながり、社会的な信用が低下する恐れがある	
23		売上の減少	不正な情報の持ち出しがおこなわれると、自社の情報漏えいにつながり、売上の減少につながる恐れがある	

（続き）

No	因子	観測変数	設問	評価尺度
25	セキュリティ知識	組織的安全管理	業務で使用する情報が漏えいしないために、組織がどのようなルールを定めるべきかを知っている。	「7：よく知っている」から「1：まったく知らない」の7段階リッカート尺度で評価
26		人的安全管理	業務で使用する情報が漏えいしないために、従業員に対して講じるべき対策を知っている。 例：情報セキュリティ教育や、機密保持誓約書の取得など	
27		物理的安全管理	業務で使用する情報が漏えいしないために講じるべき、物理的なアクセス制御の方法について知っている 例：重要な情報を管理する執務室への入退室管理、キャビネット施錠管理など	
28		技術的安全管理	業務で使用する情報が漏えいしないために講じるべき、技術的セキュリティ対策の方法について知っている 例：ファイルサーバへのアクセス権限の設定、暗号化技術の実装、パスワード管理など	
29	セキュリティ要請	取引要件	情報セキュリティ対策が入札、受注の条件となっている、または取引先から要請されている	「7：非常にそう思う」から「1：まったくそう思わない」の7段階リッカート尺度で評価
30		顧客からの信頼	情報セキュリティ対策は、顧客からの信頼を確保するために必要である	
31		企業イメージ	情報セキュリティ対策は、企業イメージ向上のために必要である	
32		優位性確保	情報セキュリティ対策は、同業他社との差別化、営業上の優位性確保のために必要である	

付録３：管理策の遵守を通じた情報漏えい抑制に関する質問紙調査項目

No	観測変数	設問	評価尺度
①情報の持ち出しを防ぐための管理策の適用状況について			
1	管理策の数	あなたの所属する会社で適用されている情報持ち出しを防ぐためのルールすべてにチェックを入れてく	
		業務上必要な範囲を超えた情報に対する、サーバやデータベース、ネットワーク経由のアクセスが制限されている（例：他部署のファイルサーバへのアクセス制限など）	
		業務で利用する情報を取り扱う執務室への入退室管理や、重要な情報を保存するキャビネットの施錠など、物理的なアクセス制御が行われている	
		業務で利用する情報が記録されている紙、外部記憶媒体（USBメモリなど）、PCを執務室外に持ち出すことが制限または禁止されている	
		私物の外部記憶媒体（USBメモリなど）や私物PCの業務利用が制限または禁止されている	左記選択肢の数
		会社貸与の外部記憶媒体（USBメモリなど）の利用が制限または禁止されている（外部記憶媒体が強制的に暗号化されている場合を含む）	※すべてが実施されていない場合、「いずれも実施されていない」の回答を得る
		シンクライアント（ハードディスクを持たないPC）化、暗号化など会社貸与PCに対する書き込みまたは書き出しが制限されている	
		外部サイトへのファイルのアップロード、電子メールの送信制限など、業務上重要な情報を社外とやり取りする場合の通信が制限または禁止されている	
		業務で利用する情報のプリントアウトが制限または禁止されている	
		業務で利用する情報に対して必要に応じたラベル付け（『社外秘』、『厳秘』などの表記）がされている	
		会社が定めるルールに違反した場合における罰則が整備されている	
		業務で利用する情報の持ち出し状況が監視されている	
		いずれも実施されていない	
2	管理策の厳しさ	情報の持ち出しを防ぐためのルールについて回答してください	「７：非常に厳しい」～「１：全く厳しくない」の７段階リッカート尺度で評価
②情報の持ち出しを防ぐために作成された規程やガイドブックなどのルール集の整備状況について			
3	業務との整合	規程やガイドブックなどのルール集は、日常業務への支障ないよう、矛盾なく作成されている	「７：非常にそう思う」～「１：全くそう思わない」の７段階リッカート尺度で評価
4	管理策の網羅	規程やガイドブックなどのルール集は、情報の持ち出しを防ぐために守るべき事項が抜け漏れなく全て記載されている	
5	具体化	規程やガイドブックなどのルール集は、個人で判断する必要なく作業できるよう、具体的に記述されている	
6	詳細化	規程やガイドブックなどのルール集に記載されている事項のみを守ればよく、記載されていない事項は実施する必要がない	
7	集約	ルールを守るにあたって、複数の文書を参照する必要がないよう、規程やガイドブックなどのルール集は1冊に集約されている	
8	定期的見直し	規程やガイドブックなどのルール集は定期的に見直しがされている	

（続き）

No	観測変数	設問	評価尺度
③情報の持ち出しを防ぐためのルールに対する教育・訓練などの実施状況について			
9	計画的実施	情報の持ち出しを防ぐために必要な教育が計画的に実施されている	「7：非常にそう思う」～「1：全くそう思わない」の7段階リッカート尺度で評価
10	必要性の周知	教育では、ルールを守ることの必要性について説明されている	
11	遵守事項の網羅	教育では、情報の持ち出しを防ぐために守るべき事項が抜け漏れなく全て説明されている	
12	理解度評価	教育後、理解度を確認するための評価が行われている（テストの実施など）	
13	遵守状況の観察	ルールを守っていることの自己点検または監査が行われている	
④情報の持ち出しを防ぐために導入されているシステム（ITなどの自動化による制御）の整備・導入状況について			
14	有効性	導入されているシステムは、不正な情報の持ち出しを防ぐために有効に機能している	「7：非常にそう思う」～「1：全くそう思わない」の7段階リッカート尺度で評価
15	効率性	導入されている自動化されたシステムは、手作業で行う場合と比較して、ルールを守るために必要な負荷を減らしている	
16	機密性	導入されているシステムにより、社外または関係者以外に漏れてはならない情報が漏えいしないよう保護されている	
17	可用性	導入されているシステムは、必要なときに利用することができる	
18	信頼性	導入されているシステムは、不正な情報持ち出しを防ぐために十分な強度の管理レベルにある	
⑤例外対応について（例外業務）			
19	例外業務	日常業務では、定められたルールを守ることができず*、例外的な処理が必要な場合がある *顧客要求により、規定のルール以外の対応が求められる場合や、緊急で対応すべき業務のため、必要な承認が得られない場合などを指します。	「7：頻繁にある」～「1：全くない」の7段階リッカート尺度で評価
⑥職場における会社管理外環境への情報の持ち出し状況について			
20	持ち出し状況（遵守）	あなたの職場では、会社の許可がないまま、業務で利用する情報（紙または電子）を、私物のPCや外付記憶媒体（USBなど）、自宅の引き出しなど、会社管理外の場所に保管している人（同僚、上司、部下など）がいる。	「7：非常にあてはまる」～「1：全くあてはまらない」の7段階リッカート尺度で評価
21	情報漏えいの状況（情報の保護）	あなたの職場における従業者（退職者を含みます）の情報持ち出しに起因する情報漏えいの発生状況について選択してください	「3：情報漏えいが発生した事例がある」、「2：情報漏えいが疑われる事例ある」、「1：情報漏えいは発生していない」、「わからない」の3段階リッカート尺度で評価 ※わからないは欠損値として処理