情報セキュリティインシデントデータベースに基づく全社的情報セキュリティマネジメントの強化手法の提案と評価

静岡大学博士論文

情報セキュリティインシデントデータベースに基づく全社的情報セキュリティマネジメントの強化手法の提案と評価

堀川 博史

大学院自然科学系教育部

情報科学専攻

2017 年 6 月

論文要旨

情報セキュリティインシデントや情報セキュリティ事故の対策の一つとして，ISMS（情報セキュリティマネジメントシステム）認証の国際規格および日本規格が制定され，組織の情報セキュリティリスク管理に役立っている．ISMS は，計画段階の活動に重点を置く洗練されたシステムである．しかし，その現状としては，ISMS 認証を取得している組織でも情報セキュリティインシデントや事故が減らない事例が見受けられる．これは，1 巡目の計画段階では運用段階で発生するインシデントを想定しきれないことが原因と考える．そこで本研究では，運用段階において自組織で発生するインシデント情報をインシデントデータベースに蓄え，インシデントデータベースを用いたインシデントの分析から対策を選定し，次巡の PDCA（Plan-Do-Check-Act）サイクルで対策を実施するための一連の方法・手順を「デルタ ISMS」モデルとして提案する．デルタ ISMS のデルタとは，n 巡目の PDCA サイクルと n+1 巡目のサイクルの差分を指す．

情報セキュリティマネジメントの強化は，事業部や事業所を越えた全社的な枠組みの中で達成されるべきものである．ISMS では事業部や事業所といった組織の一部で認証を受けることができるのに対して，本論文ではそのような組織の認証範囲を越えた全社的なセキュリティマネジメントを対象とする．本論文で提案する全社的な情報セキュリティマネジメントの改善は，情報セキュリティマネジメントに責任をもつ経営陣等（例えば CISO，最高情報セキュリティ責任者）の配下に編成される組織横断型の「情報セキュリティ統括組織」によって担われる形となる．

発生したインシデントに対応する対策を実施するため，次の三つの問題を設定する．認証を取得しても情報セキュリティインシデントが減らない，インシデント情報からどのように対策を選定するか，いかに経営陣の認識を向上し，情報セキュリティガバナンスを確立し，対策の実施に繋げるか．

認証を取得しても情報セキュリティインシデントが減らないという問題に対しては，規格における情報セキュリティインシデントに対する手順化不足が原因と考える．ISMS 認証はその附属書の中で，情報セキュリティインシデントの記録や報告を求めている．ある部署でインシデントが起きた際には，当該部署（場合により，情報セキュリティインシデント対応チーム）により 1 次対処（発見された不具合の対処）と 2 次処置（不適合の原因を除去するための処置）までは行われることになっている．しかし規格では，2 次処置の結果を学習することは求めていても，その具体的な手順を与えていない．このため，ISMS 認証取得組織においても，各部署で発生したインシデントのデータを「組織全体のセキュリティ対策の改善」のために活用していくにあたっての方法・手順については整備されていないという状況となっている．これに対してデルタ ISMS では PDCA の Do でインシデント情報をインシデントデータベースに蓄積し，Act でインシデントを分析する．

インシデント情報からどのように対策を選定するかという問題に対しては，インシデント発生部署での 2 次処置が終了した時点で，「当該部署で採択された今回の 2 次処置を，仮に全組織に採用した場合の効果」を算出し，インシデントデータベースに保存する．情報セキュリティ統括組織は，定期的（例えば半年に 1 度）に 3 次対応として，インシデントデータベースを精査し，当該期間に発生したインシデント群に対する対策候補を俯瞰することによって，全組織として新たに採用すべき対策の候補を選択する．投資対効果の高い対策を候補として選択するために，インシデント原因と対策のマトリクスである「デルタ ISMS 表」を用い，対策候補選択タスクを離散最適化問題として定式化することを提案する．

いかに経営陣の認識を向上し，情報セキュリティガバナンスを確立し，対策の実施に繋げるかという問題に対しては，安全係数の考え方を用いて対策候補の案を複数自動導出する．情報セキュリティ統括組織は, CISO 等に, デルタ ISMS 表とともに複数の対策候補案を提示する．CISO は，この情報を説明材料や判断材料として使い，「組織全体のセキュリティ対策の改善」を達成するために採用する対策を決定する．取締役会等で CISO 等が経営陣にこれらの情報を説明することで，経営陣の情報セキュリティリスク管理に対する認識を向上していく．

これらの一連の方法・手順がここで提案する「デルタ ISMS」である．そして，n 巡目の情報セキュリティインシデントの解析から n+1 巡目の対策実施へ繋げる具体的な手順となる．

デルタ ISMS の評価においては，実組織のインシデントデータを用いたケーススタディで，実担当者から良好なコメントを得ることを示す．更に，仮想の組織が標的型攻撃に対してオーストラリア政府が公表した対策集の導入を検討するケーススタディを示し，対策選定のノウハウを持たない者でも，エキスパートと同様の対策を選定できることを示す．加えて，情報セキュリティガバナンス導入ガイダンスのモニタリング項目とデルタ ISMS の提供する情報が同一であることから，デルタ ISMS の情報セキュリティガバナンスの視点での有効性を示す．

本論文では，デルタ ISMS として，情報セキュリティインシデントからの学習の具体的な方法を手順化した．すなわち本論文は，微視的には，JIS Q　27001:2014 の中の「情報セキュリティインシデント管理 (A.16)」に係る一貫性のある効果的な取組みについて手順化するものであり，JIS Q 27001:2014 を補完することを目的としている．一方で，本論文は，巨視的には，全社レベルの情報セキュリティマネジメントの改善に係る一貫性のある効果的な取組みについて手順化するものであり，組織の情報セキュリティガバナンスの補強を目的としている．

目次

第1章　はじめに

あらゆるものが情報化され，システム化される中で企業の IT 投資は情報セキュリティの強化が最重要視されている．情報セキュリティの課題に対抗するには，技術，管理・運営，法制度，倫理の４つが必要とされている [1]．本研究では，情報セキュリティマネジメントシステム（ISMS）の補完として，主に管理・運営についての手法を述べる．ISMS は PDCA（Plan-Do-Check-Act）サイクルの Plan に力点を置いた洗練されたシステムであるが，一巡目の Plan では見えないものがあり，ISMS 認証を取得してもインシデント発生を減らせない組織もあるという問題を持つ．そこで，本研究で提案するデルタ ISMS では，運用フェーズである Do で発生するインシデント情報をインシデントデータベースに蓄え，Act フェーズで全社レベルの分析から対策を選定し，経営陣の認識を向上することで情報セキュリティガバナンスを確立し，次巡の PDCA サイクルでの対策実施に繋げる具体的な手法を提示する．

1．1　　用語と背景

本研究で対象とする「情報セキュリティ」，「情報セキュリティマネジメント」及び「情報セキュリティインシデント」の用語の説明を行い．関連する動向について述べる．

1.1.1　　情報セキュリティ

本項では，用語「情報セキュリティ」の意味すること，及び，情報セキュリティ対策の必要性の認識について述べる．

情報セキュリティを脅かす原因は意図的な場合と偶発的な場合がある．航空業界では安全（safe）とセキュリティ（security）を偶発的か意図的かで区別しているが，情報セキュリティは意図的な場合も偶発的な場合も含み区別していない．

外来語のカタカナはその語源を知ると機微な語感を理解しやすい．まず，safe と security について調べる．

オックスフォード英単語由来大辞典では，『safe は当初，形容詞として用いられた．ラテン語の salvus「無償の」を基にする．名詞としての用法は動詞 save「救う」に由来し，元は「虫か

ら食物を保護するための箱」を表していた』とあり，『security は，ラテン語幹，se「~なしに」と cure「心配」からなる．当初は「不安を感じない」を表していた』とある [2]．safe はモノとしての，security は人としての安全を表しているようだ．航空業界ではフライトレコーダーとボイスレコーダによる（偶発的）事故の解析による改善が安全性を向上させていると共に，セキュリティゲートによるチェックが悪意の有る（意図的）攻撃者に対してセキュリティを向上させている．

情報セキュリティの定義を国際規格から引用する．

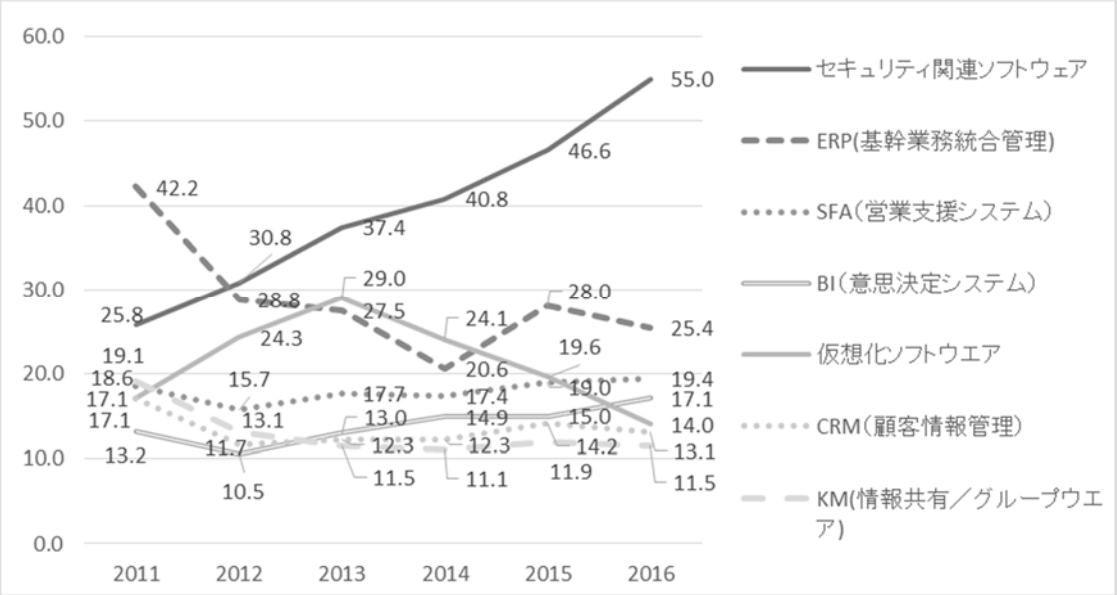
情報セキュリティとは『情報の機密性，完全性及び可用性を維持することであり，機密性とは認許されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性であり，完全性とは正確さ及び完全さの特性であり，可用性とは認許されたエンティティが要求したときに，アクセス及び使用が可能である特性』と定義されている [3].

上述は定義であり，より判り易い説明を次に示す．中尾は，3 要素をそれぞれ，『情報の漏えいや盗難などからの保護，情報の改ざんや欠損などからの保護及び情報が使用できなくなることからの保護』と説明している [4].

羽室は 3 要素を次のように説明している．『機密性は認められたものがアクセスできることを的確に管理しなければならないことを表す．組織内のシステムで，ユーザ認証さえクリアすれば，部署にかかわらず，また，幹部でも平社員やアルバイトでも，同じ機密データにアクセス可能である，ということはないだろうか．完全性は，当該情報が正確であり元のままの状態である，ということで，改ざん等が行われないようにしなければならない．本当に重要であるならば可用性を犠牲にする必要があるかもしれない．いつども，どこでも，気楽にアクセスする必要性はあるのか，出入りが制限された書庫の中で書類を閲覧すれば事足りるのではないか等，利便性をどこまで確保するのかを考える必要がある』 [5].

つまり，情報セキュリティとは情報の機密性，完全性及び可用性を維持することである．次に，企業における投資傾向からセキュリティが最重要視されていることを示す．

矢野経済研究所によれば，2016 年度の IT 投資が増加するソフトウェアは 3 年連続最重要で「情報セキュリティの強化」となっている（図 1） [6].



有効回答数：2011 年 403 件，2012 年 543 件，2013 年 538 件，

2014 年 587 件，2015 年 479 件，2016 年 551 件

図 1　今後 3 年間で IT 投資が増加するソフトウェア [6]

企業において，情報セキュリティ対策の必要性が認識されており，情報セキュリティ技術は重要なテーマの一つとみなすことができる．

1.1.2　情報セキュリティマネジメントシステム（ISMS）

情報セキュリティマネジメントシステム（Information Security Management System: ISMS）とは言葉の通り，情報セキュリティのためのマネジメントシステムである．

最初に用語「マネジメント」の意味することを示し，次に，ISMS 認証取得組織数の増加から ISMS 取得の価値が高く評価されていることを示す．

management の語幹 manage の当初の意味は『「（馬を）menège（=囲まれた場所でのトレーニング）の速度に保つ」であった. ラテン語 maneggiare に由来し, それはラテン語 manus「手」に基づいている』 [2].

Drucker は，マネジメントをその役割によって定義しなければならないとして，3 つの役割を説いている [7].

『①自らの組織に特有の使命を果たす．マネジメントは組織に特有の使命，すなわちそれぞれの目的を果たすために存在する．

②仕事を通じて，働く人たちを生かす．現代社会においては，組織こそ，一人ひとりの人間にとって，生計の資（かて），社会的な地位，コミュニティとの絆を手にし，自己実現を図る手段である．当然，働く人を生かすことが重要な意味を持つ．

③自らが社会に与える影響を処理するとともに，社会の問題について貢献する．マネジメントには，自らの組織が社会に与える影響を処理するとともに，社会の問題の解決に貢献する役割がある．』

このように，マネジメントの語源や定義には，単に「管理する」を超え，マネージャが組織と一緒になって使命を果たすといった意味を含んでいるようだ．

情報セキュリティインシデントや情報セキュリティ事故の対策の 1 つとして，ISMS 認証の国際規格（ISO）および日本規格（JIS）が制定され，組織の情報セキュリティリスク管理に役立っている．

ISO でのマネジメントシステムは,『方針．目的及びその目的を達成するためのプロセスを確立するための相互に関連する又は相互に作用する組織の一連の要素を意味し，システムの要素には，組織の構造，役割及び責任，計画，運用などが含まれる』と注記されている [3].

ISO／IEC 27001 は国際規格であり，ISO／IEC 27000 の 0.3 に，このファミリー規格の目的を 4 項目述べている [3].

『a)ISMS 及び ISMS を認証する機関に対する要求事項の規定.

b)ISMS を確立し，実施し，維持し，改善するためのプロセス全体に関する直接的な支援，詳細な手引き及び／又は解釈の提供.

c)ISMS に関する分野固有の指針.

d)ISMS に関する適合性評価.』

この記述は ISMS の正確な目的である．ISMS はプロセスであり，組織に対して規定したプロセスを実施していることを外部から認証することと理解できる．

次に ISMS の理解を促すために，ISO／IEC　27001 と日本での JIS Q 27001 の制定の歴史を述べる（表 1）.

表 1　ISMS 制定の歴史

ISO／IEC　27001		JIS Q 27001	
2000 年 12 月	ISO/IEC 17799:2000(Information technology-Code of practice for information security management)が英国の規格である BS 7799-1 をベースとして国際規格化された.	2001 年	JIS X 5080:2002(ISO/IEC 17799:2000)制定
2005 年 6 月	ISO/IEC 17799:2005 発行	2006 年 5 月	JIS Q 27001:2006(ISO/IEC 17799:2005)発行
2013 年 9 月	ISO/IEC 27001:2013 発行	2014 年 3 月	JIS Q 27001:2014(ISO/IEC 27001:2013)発行

表より ISMS は 2000 年を初出とする比較的新しい規格であることを見ることができる.

次に ISMS 認証取得の状況を示す.

2015 年の世界の認証事業者数は 27,536 であり，日本の認証事業者数は国別では最も多い. 以下，2 位は英国，3 位はインドである [8]．これらにより，ISMS に関して日本に最も多くの ISMS 認証を取得した組織があり，それゆえ調査データの件数も豊富であると思われる.

図 2 は，日本における ISMS 認証取得事業者数の推移を示す [9]．認証取得事業者数は増加の傾向にある．企業などは ISMS を取得する価値を高く評価し，積極的に認証取得しようとしていることが伺える.

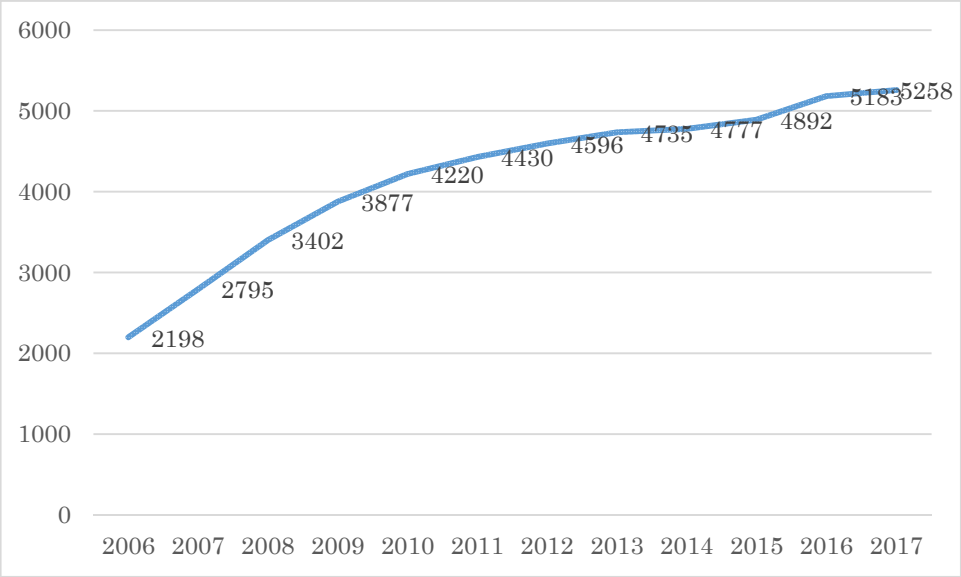


図 2　日本における ISMS 認証取得事業者数の推移 [9]

1.1.3　情報セキュリティインシデント

本項では，用語「インシデント」の意味することを示す.

ISO 情報システムマネジメントの用語では，情報セキュリティインシデント（information security incident）を『望ましくない又は予期しない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及び情報セキュリティを脅かす確率が高いもの』と定義している [3]. ISO リスクマネジメントの用語では,『事象は何かが起こらないことを含むことがある』とあり,『事象は事態(incident）又は事故（accident）と呼ばれることがあり，事態はインシデントと表現される』とある．さらに,『結果(consequence)にまで至らない事象は，ニアミス(near miss), 事態(incident)，ヒヤリハット(hear hit)又は間一髪(close call)と呼ばれることがある』とあり，インシデントと事故とは明確に区別していない場合もある.『場合により結果を持つ事象が事故, 結果の有無によらず事故である事象及び事故でない事象をインシデントとよんで区別する場合もある』ようである [10]．オックスフォード英単語由来大辞典では,『accident は，当初の意味は「出来事」であった. この語はラテン語 accident「起こっている」に由来する. ad-「・・・へ, ・・・の方へ」と cadere-「落ちる」からなるとあり，incident は，ラテン語 incident に由来し，incidere「降りかかる，起こる」（cadere「降る」から派生）の現在分詞語幹である』とある．いずれも語源は偶発的を意味する [2].

英語では意図的か偶発的かの表現は intentionally or accidentally とか whether by accident or by design とかと表現され accident と偶発的の意味は極めて近い．インシデントも語源では

偶発的の意味を持つが，情報セキュリティの分野では意図的原因も含めて情報セキュリティインシデントや情報セキュリティ事故を情報セキュリティインシデントと呼んでいる.

1.1.4 偶発的インシデントと意図的インシデント

佐々木は情報セキュリティインシデントの原因の一つである脅威を偶発的と意図的に分類している（表 2） [11].

表 2 セキュリティへの脅威の分類 [11]

分類		脅威の具体例
偶発的	天災	地震，火災，水害，落雷
	故障	ハードウェア故障ソフトウェア障害，回線故障，過負荷
	誤操作	データ入力ミス，運用ミス，ソフトウェアバグ，誤接続
意図的	第三者の悪意の行為	システムへの不正侵入
	取引相手の悪意の行為	取引内容の事後否認

Reason はヒューマンエラーにおける不安全行為を意図せぬ行為（偶発的）と意図した行為（意図的）に分類している（表 3） [12].

表 3 不安全行為の分類 [12]

意図せぬ行為	スリップ	注意の不全（失敗）
	ラプス	記憶の不全（失敗）
意図した行為	ミステイク	ルールベースのミステイク
		知識ベースのミステイク
	規制違反	日常的規則違反
		例外的規則違反
		破壊行為

JNSA は個人情報漏えいの原因を 13 個に分類している [13]. 表 4 にこれらを偶発的と意図的に分類して示す.

表 4　JNSA の個人情報漏えい原因の分類

偶発的	誤操作，紛失・置忘れ，管理ミス，バグ・セキュリティホール
意図的	不正アクセス，不正な情報持ち出し，盗難，内部不正行為，設定ミス，目的外使用，ワーム・ウイルス
不明	不明，その他

2014 年の JNSA の原因別個人情報漏えいデータ [13]を元に偶発的インシデントと意図的インシデントの件数を図 3 に，人数（被害額に相当）を図 4 に示す.

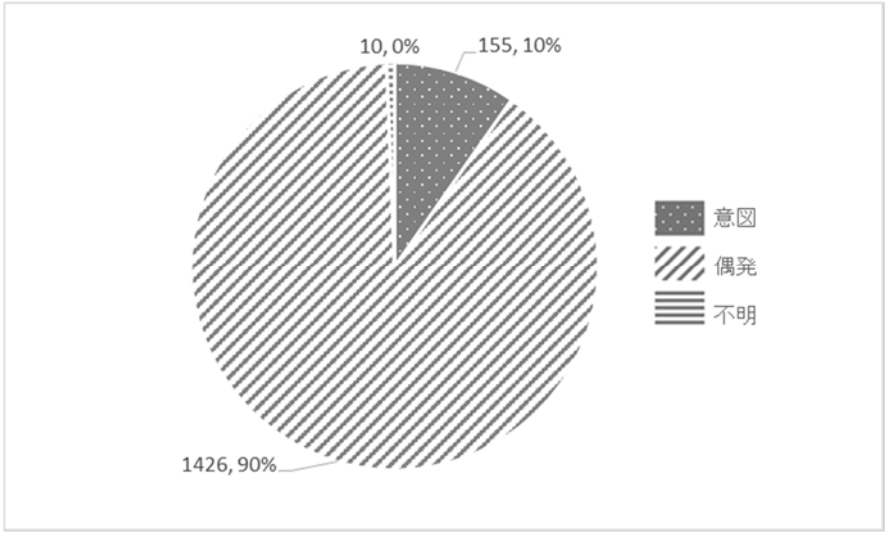


図 3　個人情報漏えい件数（ [13]を元に作成）

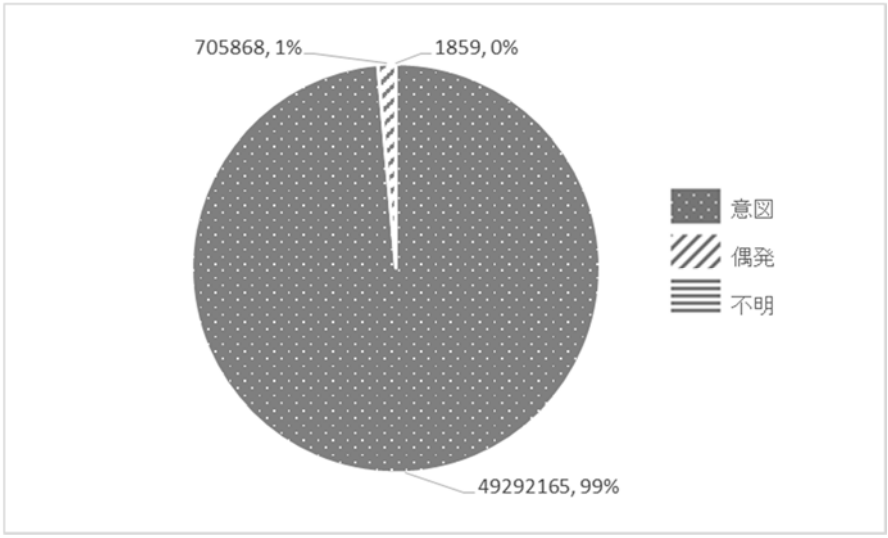


図 4　漏えい人数（ [13]を元に作成）

原因が偶発的である情報セキュリティインシデントの発生頻度は 90%と高く，原因が意図的である情報セキュリティインシデントの被害額は 99%と高い.

1.1.5　情報セキュリティインシデントの推移

次にいくつかの統計データから日本における情報セキュリティインシデントの最近の推移を提示する.

図 5 に不正アクセス禁止法違反の認知件数・検挙事件数の推移を示す．認知件数は 2014 年をピークに減少の傾向になるが，検挙事件数は増加の傾向にある [14].

深刻なインシデントの割合の増加及び／または検挙技能の向上が予想できる.

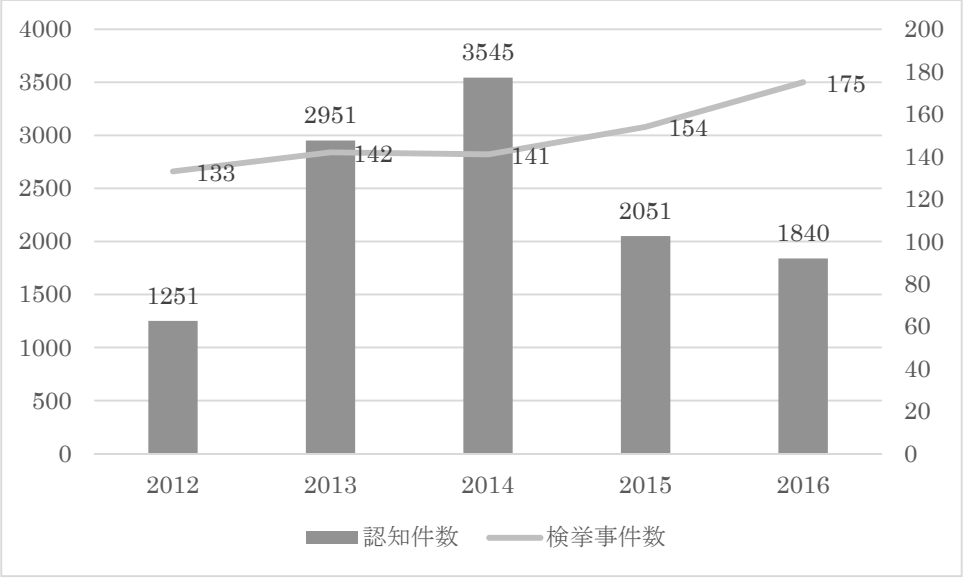
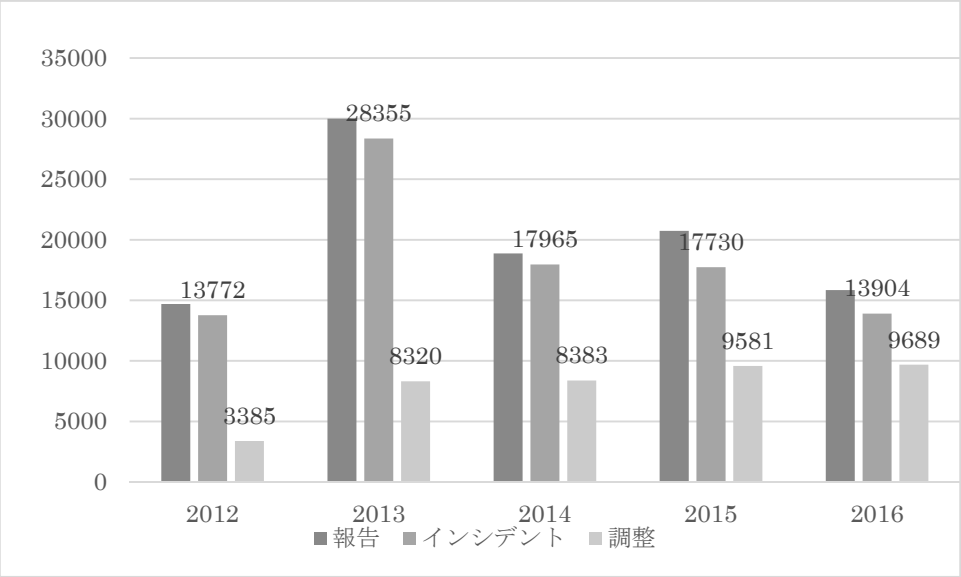


図 5　不正アクセス禁止法違反の認知件数・検挙事件数の推移 [14]

図 6 に JPCERT の 4 半期別のインシデント報告対応レポートを年毎に集計したインシデント件数を示す [15]．インシデント数は 2013 年をピークに減少の傾向にあるが，情報共有が必要な調整は年々増加傾向にある．深刻なインシデントの増加及び／またはインシデント原因の多様化が予想できる.

畠中は統計上の件数は減ってもマルウェアの脅威が巧妙化，凶悪化していると指摘している [16].



報告件数 ： 報告者から寄せられた Web フォーム，メール，FAX による報告の総数を示す.

インシデント件数 ： 各報告に含まれるインシデント件数の合計を示す．1 つのインシデントに関して複数件の報告が寄せられた場合にも，1 件として扱う.

調整件数 ： インシデントの拡大防止のため，サイトの管理者等に対し，現状の調査と問題解決のための対応を依頼した件数

図 6　JPCERT のインシデント報告対応レポート（ [15]を編集）

残念ながら，様々な技術面，管理・運営面，法制度や倫理面の改善努力にも関わらず，情報セキュリティインシデントは巧妙化，凶悪化し，深刻なインシデントが発生し続けている.

1. 2　　一巡目の Plan での問題

ISMS が，PDCA サイクルの中でも Plan に重きを置くシステムであることを示したのち，一巡目の Plan で，必ずしも組織で発生する情報セキュリティインシデントを減らせないことを，業種ごとのインシデント傾向と隠れたインシデントのデータで示す.

1.2.1　　Plan に重きを置く ISMS

本項では，リスクマネジメントの意味と ISMS における PDCA サイクルの要求について説明する.

ISMS は，リスクマネジメントプロセスを適用することによってリスクを適切に管理する仕組みである [17]．リスクとは目的に対する不確かさの影響のことである [3]．risk は，元はイタリア語 risco「危険」，rischiare「危険な目にあう」に由来する [2].

リスクマネジメントとは，ISO では，リスクについて組織を指揮統制するために調整された活動としている [3] [10]．日本セキュリティ・マネジメント学会では『経営の目的達成を阻害する可能性のある不確定要因を対象とし，経常化された最小のコストで総合的な安全対策を講じることによって，その出現を予防・発見・修復して経営の安定化を図る経営手法』としている [18].

次に ISMS における PDCA サイクルの要求を示す.

ISO/IEC27001:2013 においては，明示的な PDCA 要求が無くなっている．これは PDCA 要求がなくなったわけではなく，上位規格で暗に PDCA サイクルが要求されている.

ISO/IEC 27001:2005 では規格要求事項自体が PDCA サイクルを要求していた．対応部分を次に示す [19].

序文

この規格は“Plan-Do-Check-Act(計画-実行-点検-処置)”（PDCA）モデルを採用し，これを ISMS プロセスすべての構築に適用する．図 7 は，ISMS が，利害関係者からの情報セキュリティ要求事項及び期待をインプットとしどう取り入れ，必要となる活動及びプロセスを経て，その要求事項及び期待を満たした情報セキュリティの成果をどう生み出すかを表している．また，図 7 は，箇条４，５，６，７及び８に規定するプロセス間のつながりも表している．

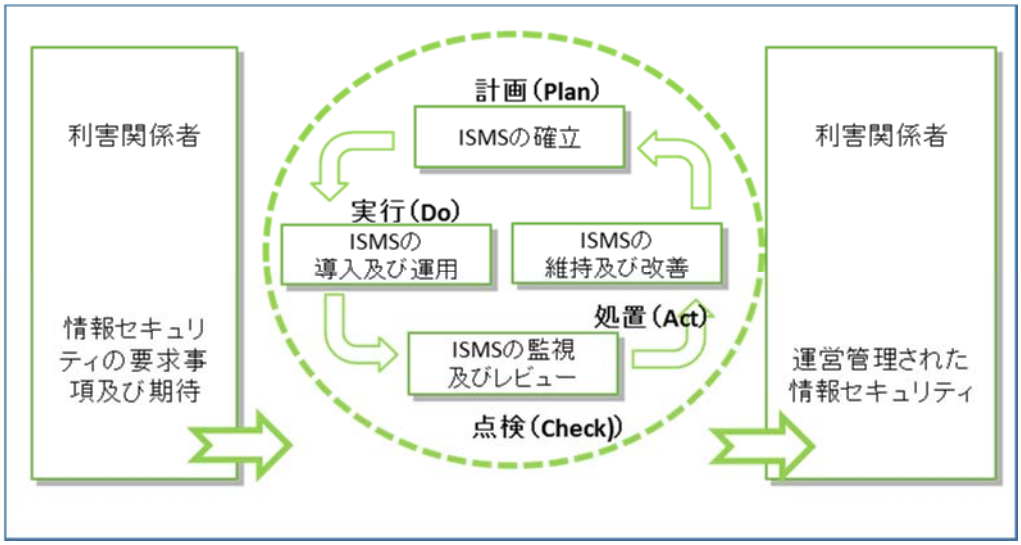


図 7　ISO/IEC27001:2005 の PDCA モデル [19]

『最新の ISO/IEC27001:2013 はマネジメント規格として共通化された要求事項には, PDCA

サイクルの記述も PDCA モデルの記述もない．ただし，マネジメントシステムの基盤である Annex　SL を通して PDCA モデルを踏襲していることに変わりはない．なお，Annex　SL にも明示的な PDCA モデルの記載はなく，図 8 に示す箇条 6 の計画(Plan)に続いて，箇条 8 の「運用」で実行(Do)，箇条 9 の「パフォーマンス評価」で評価(Check)へと展開し，また，箇条 9.3 の 「マネジメントレビュー」では，箇条 4.1 の「外部内部の課題の変化」と箇条 4.2 の「利害関係者の課題」を見直す要求があるため，箇条 4 からスタートしてぐるりと一周する仕組となっている』 [20].

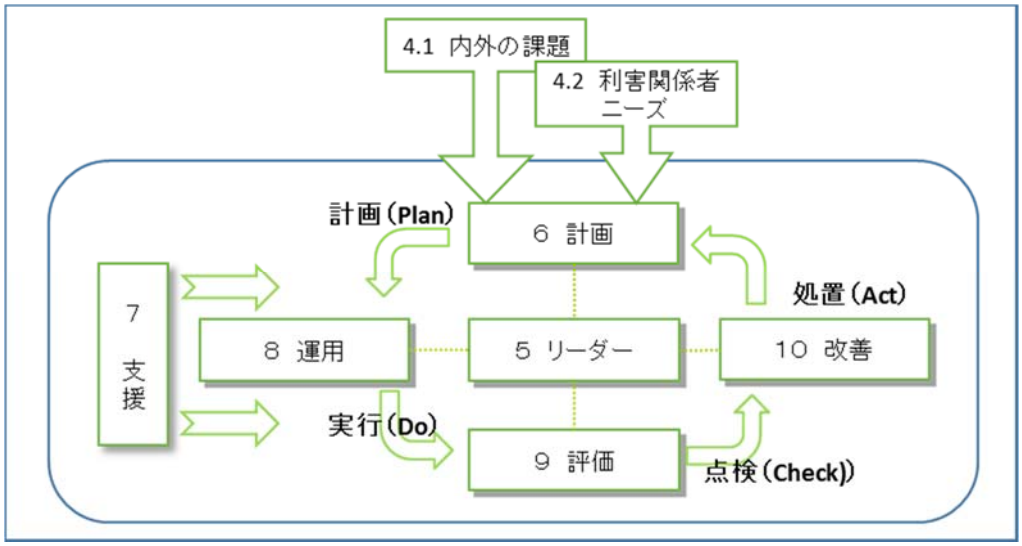


図 8　Annex　SL の PDCA モデル

PDCA モデルは実行の結果をフィードバックすることで実行の改善を図ることができる．

図 8 に基づき，ISMS の規格の PDCA について記載した文章量を比較し，表 5 に示す．ISMS の規格では Plan（計画）に重きを置いた規格となっていることを見て取ることができる．対策を予め実施することは，対策をインシデント発生後に実施するのに比べて，被害を抑止することができるため，洗練されたマネジメントシステムと見なすことができる．

表 5　PDCA の文章量

フェーズ	文書量の割合
Plan（6 計画）	48.4%
Do（8 運用）	12.3%
Check（9 評価）	27.0%
Act（10 改善）	12.3%

1.2.2　一巡目の Plan の問題

本項では，ISMS とは何かを判り易く図説した後，ISMS の課題として，一巡目の Plan の問題について述べる．

ISMS は，リスクマネジメントプロセスを適用することによってリスクを適切に管理する仕組みであることを特徴とする [17].

リスクマネジメントとは，ISO では，リスクについて組織を指揮統制するために調整された活動としている [3] [10]. 日本セキュリティ・マネジメント学会では『経営の目的達成を阻害する可能性のある不確定要因を対象とし，経常化された最小のコストで総合的な安全対策を講じることによって，その出現を予防・発見・修復して経営の安定化を図る経営手法』としている [18].

中尾は ISMS の必要性をより判り易く次のように述べている [21].

- 情報処理，情報通信（ICT）が重要なビジネス手段となっており，いかなるビジネス戦略を迅速に的確に決定・選択するために企業・組織が保有する情報資産は重要になっている．
- サイバー攻撃，内部犯罪やコンピュータシステムの誤操作，システムの内在するプログラムバグなど様々な要因による情報資産の喪失，漏えいは，ビジネスやサービスの停止／延期，企業イメージ／ブランド力の失墜，経営状況の悪化，収入の大幅低下，従業員・職員のインセンティブの低下などが発生し，その影響は計り知れない．
- したがって，企業・組織が安定したビジネスを展開するためには，情報資産の安全性を確保することが鍵となり，この実現のために，経営層も参画した ISMS の実施が必要となってきている．

ISMS は，情報資産の安全性を確保するために実施する．

ISMS におけるリスクマネジメントは，PDCA サイクルの Plan で実施され，図 9 に示すように次の手順を取る．

① 情報資産の調査
② 脅威の調査
③ 重要性の分類

④　脅威の発生頻度／被害額の大きさ分析

⑤　セキュリティ要求水準の設定

⑥　対策の選定

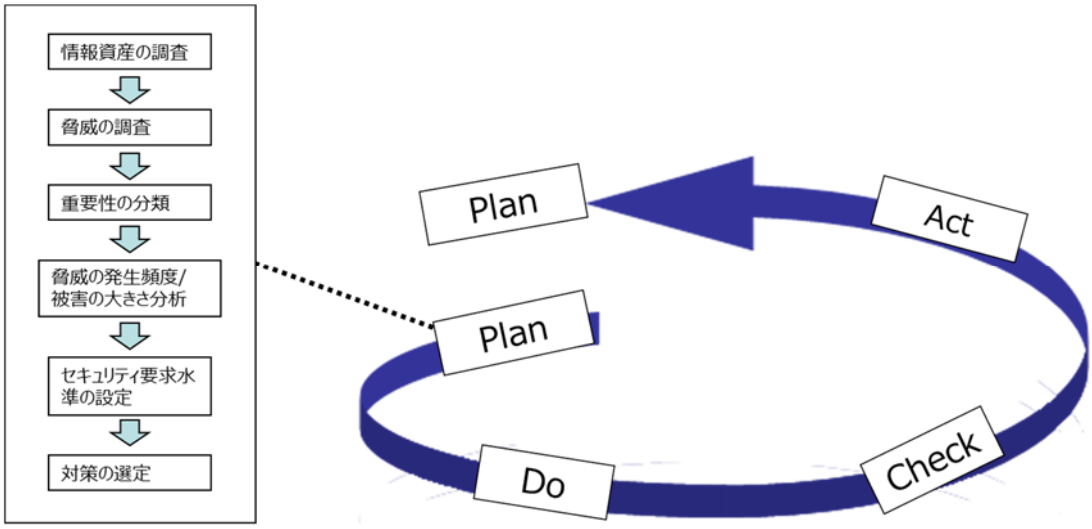


図 9　ISMS とは

JIPDEC（日本情報経済社会推進協会）による情報セキュリティマネジメントシステム適合性評価制度の概要の ISMS 認証取得の必要性は正確ではないかもしれないが，判り易い.『組織が取組むべきリスクマネジメントを維持し，適切な管理策を実施することによって，情報セキュリティインシデントの発生可能性やインシデントが顕在化したときの損害を減らすことができ，企業価値の向上につなげることができる』としている [22].

日本における ISMS 適合性評価制度を運用している JIPDEC が ISMS は明確にインシデントの発生頻度や被害額を減じることができると述べている．組織の情報資産は確固とした存在であり，情報資産を数え上げ，その資産価値を評価した後，重要な資産価値が保たれるように対策を実施すれば，重要な資産のセキュリティは確保され，その資産に情報セキュリティインシデントが発生した場合でも被害額を低減できるはずである．リスクマネジメントを Plan で実施することはプロアクティブ（事前対策）な活動となっており，良くできた仕組みと見なすことができる．しかし，ISMS の課題として，認証取得後のインシデント発生が減らない組織もあることを複数の文献が示している [23] [24]．詳細は，後述する（2．1 節参照）.

一巡目の Plan でプロアクティブ（事前対策）な活動がうまくいかないことは，Do フェーズで起きることが予測できないことに拠る（図 10）.

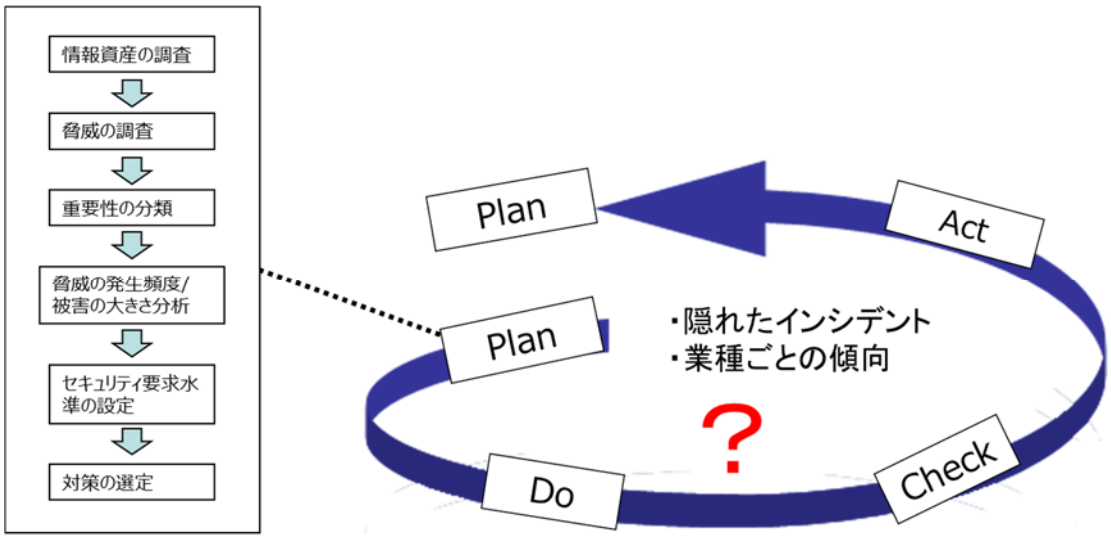


図 10　一巡目の Plan の問題

一巡目の Plan でそれに続く Do フェーズで起きることの予測の難しさを示す二つの事象を次項からの「隠れたインシデント」と「業種ごとのインシデント傾向」で示す.

1.2.3　隠れたインシデント

JNSA は，個人情報漏洩に関わる情報セキュリティインシデントデータベースを一般公開する活動を実施している．公開データベースに蓄積される情報は，公表された情報セキュリティインシデントとなっている.

公表されたインシデントの分布から隠れた情報セキュリティインシデントがあることが報告されている．大谷は 1 件 1000 人以上のインシデントの分布からシンシデント全体の件数を推定している（図 11） [25].

28,504 + 5,343 + 1,002 + 186 + 29 + 10 + 1 = 35,075

公表率は 4.5%となる（1,609 ÷ 35,075）．公表率は決して高くない.

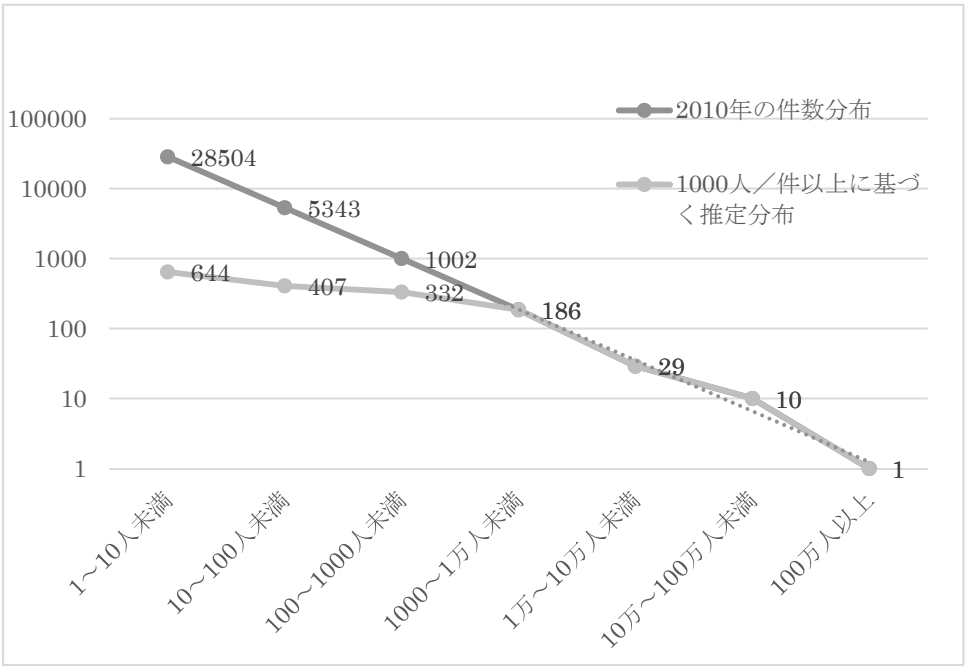


図 11　インシデント全体の件数の推定 [25]

また，インシデントを公開するより，インシデントを公開しない人の方が多いことがアンケートにより示されている.

島は『内部不正に関して発生したインシデント情報等が内部（社内及び関係者間）で解決できた場合に, 公的または中立的な機関に対して,「個人や企業などが特定できない状態での公開」を条件に，有益な対策を検討する事例として情報を公開する可能性があるかをアンケートしたところ，公開する 9%に対して公開しない 31%であった』（図 12） [26].

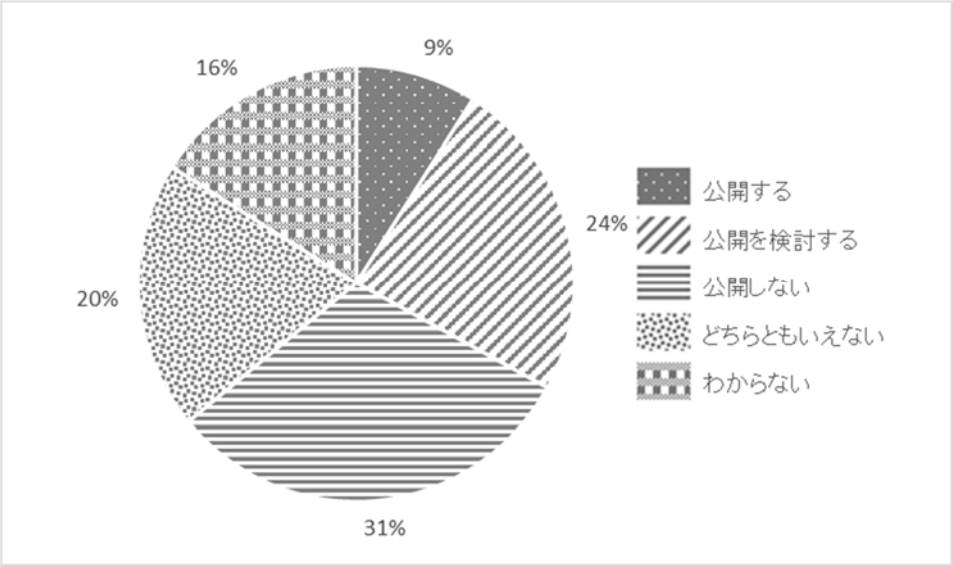


図 12　公的・中立的機関への情報提供について（n=3,000）[26]

上述したインシデントの隠匿は意図した行為であるが，インシデントそのものの存在が認識されない場合もある．

Glenn らは米国防総省のコンピュータシステムへの不正アクセスに関して防衛システムがどの程度まで攻撃されているのか，情報やシステムへのさらなる被害の可能性，機密情報を確保する上で防衛が直面する課題について報告するよう求められたため，DISA（Defense Information Systems Agency）は侵入テストを実施した．『DISA は防衛コンピュータシステムに対する防御の程度をテストするために，防御コンピュータシステムに対する 38,000 件の攻撃を実施した．65%の成功率を達成したが，成功した攻撃のうち，標的組織が検出した攻撃は 4%のみであり，96%は検出できなかった』（図 13）[27].

隠れたインシデントは，発生するまでどのようなインシデントであるかを予想することが困難なため，一巡目の Plan での発生インシデントの予想を難しくする．

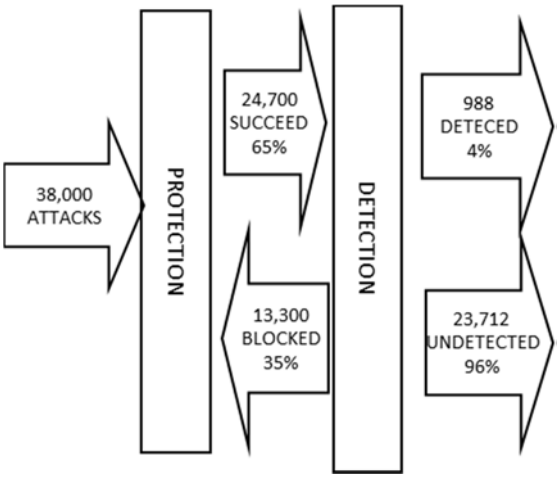


図 13　DISA 脆弱性アセスメント [27]

1.2.4　　業種ごとのインシデント傾向

佐藤は，業種により発生インシデントに傾向があり，同じ業種では同様のインシデントが発生していることを指摘した [28]．図 14 に 2012 年から 2014 年の金融業・保険業の原因別件数を示し，図 15 に公務の原因別件数を示す．

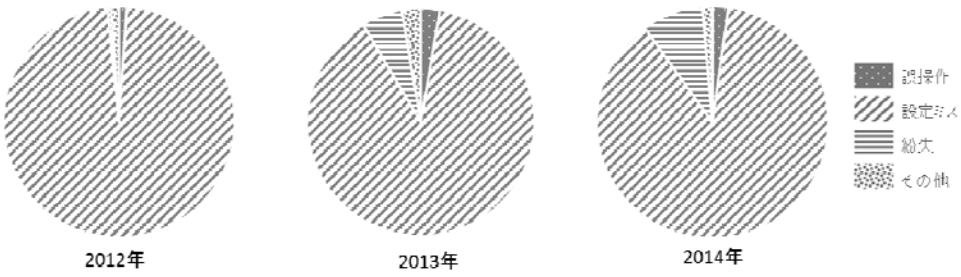


図 14　金融業・保険業の原因別件数 [28]

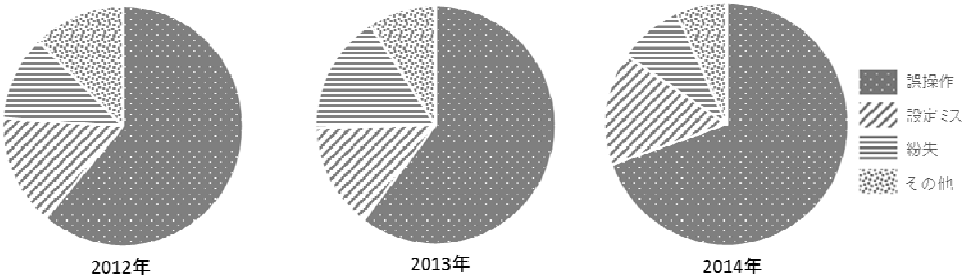


図 15　公務の原因別件数 [28]

業務内容に依存するためか，金融業・保険業と公務では原因が異なると同時に同一原因のインシデントが発生し続けている．ISMS の附属書 A（あるいは ISO/IEC　27002）に記載のある対策集は，業種に依存しない一式の対策集である．この対策集は成功した対策を集めたベストプラクティスであるが，業種にインシデント原因の偏りがあるため，必ずしも一式の対策集がすべての業種への効果を保証するものではないと見ることができる．業種にインシデント原因の偏りがある理由は，業種ごとに業務のパターンが似ていることに拠ると推定できる．だからこそ，同じ業種でも細かく見ると，組織が変われば業務も変わっていくため，本来は組織ごとに情報セキュリティ対策を検討する必要がある．

インシデント発生が改善できない組織では，改善の PDCA が循環していないこととなる．中でも次巡の計画（Plan）が適切でないなら，前巡の Act から次巡の Plan へ渡される情報に問題があると考える．この現状の ISMS の課題を図 16 に示す．

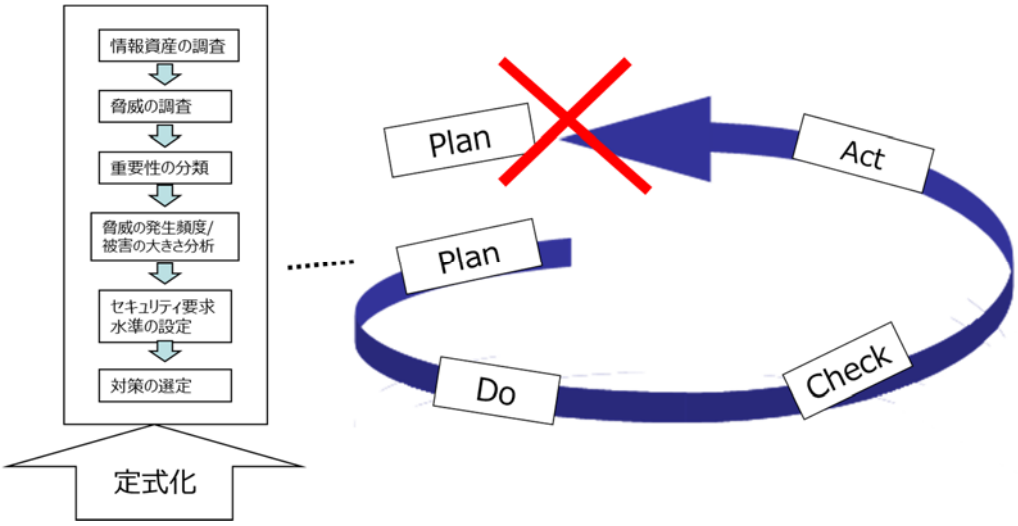


図 16　現状の ISMS の課題

本研究では，ISMS の PDCA サイクルにおける Act から次巡の Plan にいかに情報を渡すかを考察する．

1．3　　デルタ ISMS モデルの概要

ISMS は，計画段階の活動に重点を置く洗練されたシステムである．しかし，その現状としては，ISMS 認証を取得している組織でも情報セキュリティインシデントが減らない事例が見受けられる．1 巡目の計画段階では運用段階で発生するインシデントを想定しきれないことが

原因と考える．そこで本研究では，インシデントの発生に対応できる手順を示すことを研究テーマとする．ISMS は，事業部や事業所といった部分認証を許しているが，情報セキュリティインシデントの対応は，部分認証の範囲を越えた全社的な枠組みの中で実施されるべきものである．そして，全社的な組織の情報セキュリティマネジメントシステムにおいては経営陣の理解を求める必要がある．本研究で提案するデルタ ISMS は，運用段階において自組織で発生するインシデント情報をインシデントデータベースに蓄え，インシデントデータベースを用いたインシデントの分析から対策を選定し，経営陣の理解を得て，次巡の PDCA サイクルで対策を実施するための一連の方法・手順からなる．

1.3.1　全社的情報セキュリティマネジメント

ISMS は組織の部分認証を許している．部分認証により，認証が取得しやすいというメリットを持つものの，インシデントの二重管理に管理上の手間が発生する．

ISMS では組織，事業，所在地，資産，技術を適用範囲の観点とすることができ，○○部署，○○事業所，○○工場のような場所や○○ネットワークや○○システムというような限定した組織の一部の対象範囲を，合理的に説明ができる範囲の場合，「適用範囲」として認証取得範囲に選定することができる．これに対して，例えば，個人情報保護法に対応するプライバシーマーク認定制度では，企業または組織の全体が認証取得範囲としてあらかじめ指定されている．このため，ISMS の場合は，プライバシーマーク認定制度と異なり，認証範囲を限定し，段階的にその範囲を拡大することもできる．ISMS の適用範囲の規定を次に示す [17].

> 4.3　情報セキュリティマネジメントシステムの適用範囲の決定
> 組織は，ISMS の適用範囲を定めるために，その境界及び適用可能性を決定しなければならない.
> この適用範囲を決定するとき，組織は，次の事項を考慮しなければならない.
> a)4.1 に規定する要求事項
> b)4.2 に規定する要求事項
> c)組織が実施する活動と他の組織が実施する活動との間のインタフェース及び依存関係
> ISMS の適用範囲は，文書化した情報として利用可能な状態にしておかなければならない.

全体認証と部分認証はどちらが多いのであろうか.

JIPDEC のアンケート調査報告書の中の「認証範囲の従業員数について, 全社からみた割合」

において，半数（50%）の組織が部分認証として ISMS を取得している（図 17） [29].

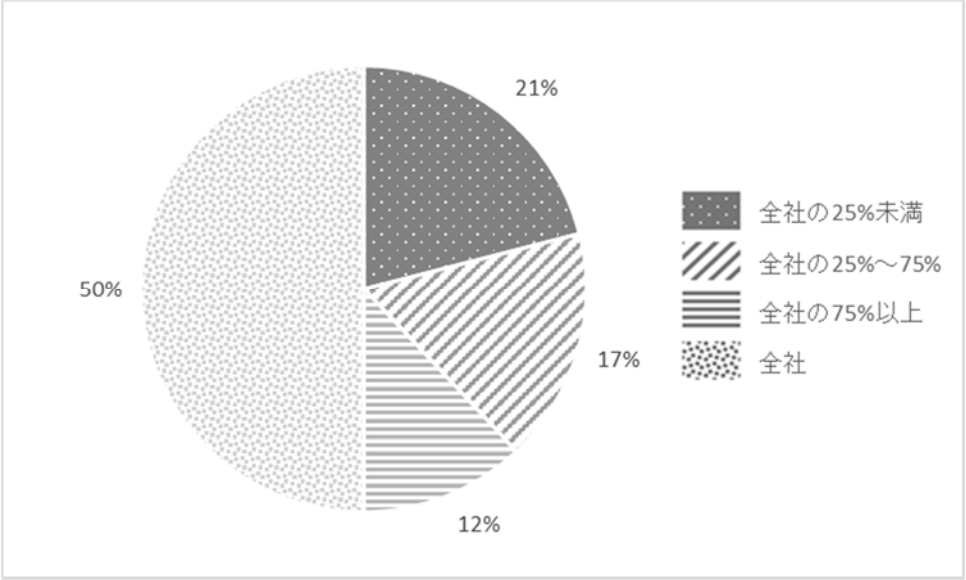


図 17　認証範囲（従業員数の割合による，n=1072） [29]

ISMS を組織の一部で認証を受けた場合，認証を受けた組織の一部だけで発生した情報セキュリティインシデントに対する情報セキュリティマネジメントの強化を実施することが非効率なため，ISMS 活動と情報セキュリティマネジメントの強化が乖離しがちとなる

情報セキュリティマネジメントの強化は，事業部や事業所を越えた全社的な枠組みの中で達成されるべきものである．ISMS では事業部や事業所といった組織の一部で認証を受けることができるのに対して，そのような組織の認証範囲を越えた全社的なセキュリティマネジメントを実施していかなければならない．

1.3.2　情報セキュリティガバナンス

全社的な組織の情報セキュリティマネジメントシステムには，経営陣の理解が必要となる．経営陣側の視点では，情報セキュリティガバナンスという研究分野が関連する．

最初に用語「ガバナンス」の意味することを示し，次に，情報セキュリティガバナンスの規格を紹介する．

govern 及び government は，『ラテン語 gubernnare「舵を取る，統制する」に由来する．元の動詞は，ギリシャ語 kubernan-「舵を取る」である』 [2].

マネジメントもガバナンスも馬や船での移動を意味するが，マネジメントは組織全体の在り方に係るものであり，ガバナンスは組織の最上位層，例えば，企業における取締役会の活動と解釈すると違いを理解しやすい.

経済産業省は「情報セキュリティガバナンス」の確立を,『企業の事業基盤の安定的な確立を図り，ひいては企業価値の向上を図るために，自社が保有する情報の価値を正しく認識し，リスク管理の一環として，経営者がリーダーシップを持って戦略的に情報セキュリティ対策を推進すること』としている [30].

経済産業省の「情報セキュリティガバナンス導入ガイダンス」は，次のように述べている.『必要な時に経営層の方針が見えない，企業の現場において講じられている事故を未然に防ぐための情報セキュリティ対策の効果が見え難いといった問題に対して，経営層と現場の管理者層との間のギャップを埋め，適正な情報セキュリティガバナンスを確立するために，経営陣が行うべき役割と，情報セキュリティガバナンスの効果について提示している．なお，このガイダンスは ISMS を補完する意味で策定されている』 [31].

そして，このガイダンスを元に，日本が規格を主導する形態で，ISO/IEC　27014:2013 及び JIS　Q　27014:2015 が発行されている [32].

1.3.3　　デルタ ISMS

本研究で提案する全社的な情報セキュリティマネジメントの改善は，情報セキュリティマネジメントに責任を持つ経営陣または CISO（Chief Information Security Officer，最高情報セキュリティ責任者）等の配下に編成される組織横断型の「情報セキュリティ統括組織」によって担われる形となる.

認証を取得した組織でも情報セキュリティインシデントが減らないという問題に対し，情報セキュリティインシデントデータを「組織全体のセキュリティ対策の改善」のために活用していくための具体的な方法・手順を,「デルタ ISMS」モデルとして提案する．デルタ ISMS のデルタとは，n 巡目の PDCA サイクルと n+1 巡目のサイクルの差分を指す.

デルタ ISMS は，Do でインシデント情報をインシデントデータベース（DB）に蓄積し，Act でインシデントデータベースを用いてインシデントを分析し，必要な対策を選定し，経営陣の認識を向上し，情報セキュリティガバナンスを確立する．次巡の Plan で対策を実施するため

の具体的な一連の手順から成る（図 18）.

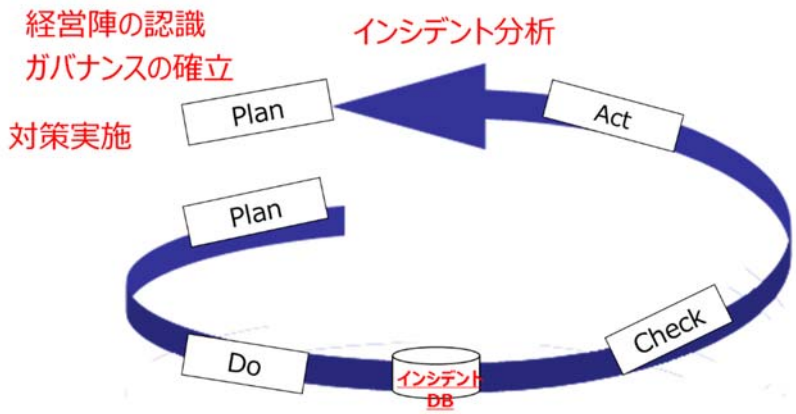


図 18　デルタ ISMS

1．4　　本章のまとめと本論文の構成

以上，本章のまとめと本論文の構成を述べる.

ISMS 認証を取得した組織でも情報セキュリティインシデントが減らないという課題を受けて，業種による情報セキュリティインシデント原因の違いと隠れたインシデントの存在から一巡目の Plan に重点を置く ISMS の対策選定の困難さを示し，Do から始める情報セキュリティインシデントの対応を手順化する．本研究で提案する「デルタ ISMS」モデルは，インシデントデータベースへのインシデント情報の蓄積，Act でのインシデント分析と対策選定，経営陣の認識向上による情報セキュリティガバナンスの確立により，次巡の PDCA サイクルでの対策実施を行うための一連の具体的な手順からなり，ISMS を補完することを目的とする.

以下，第２章では，ISMS 認証を取得した組織でもインシデントが減らないことを示した調査をあげ，インシデントが減らない原因は規格における情報セキュリティインシデントに対する手順化不足が原因であることから，インシデントデータベースへの蓄積と分析を提案する．そして，インシデントの分析からの対策の選定については，リスクマネジメントに対する定式化の先行研究を示し，定式化による投資対効果の明示を提案する．更に，ISMS 規格におけるマネジメントレビューが第 3 者検証に留まり，ガバナンスの観点を欠いていること，及び，現状では経営陣の認識向上活動ができておらず，経営陣と管理者層の橋渡し人材が不足しているという関連研究を述べる．デルタ ISMS では，経営陣の認識向上により情報セキュリティガバナンスを確立するため，複数対策の提示を提案する.

第3章では，デルタ ISMS モデルをその特徴的構成要素であるインシデントデータベース，3 次対応，デルタ ISMS 表，定式化，安全係数及び経営陣への 3 パターンの対策案の提示を詳説し，運営段階で発生したインシデントの情報からその対策を次巡の PDCA で実施するための一連の具体的手順を詳説する.

第4章では，実組織の過去データを用いたケーススタディ，仮想の組織を想定した標的型攻撃対策のケーススタディよりデルタ ISMS の手順で対策選定のノウハウを持たない人でもエキスパートと同じ対策が選定できることを示し，更に，情報セキュリティガバナンス導入ガイダンスのモニタリング項目とデルタ ISMS の処理対象の比較を行い，デルタ ISMS が経営陣の認識向上に有効であることを示す.

第2章　関連研究と研究アプローチ

本章で扱う問題は，「認証取得後もインシデントが減らない」，「インシデントデータからどのように対策を選定するか」，「どのように経営陣の認識を向上させ，情報セキュリティガバナンスを確立するか」の三点である．

まず，「認証取得後もインシデントが減らない」という問題については，発生したインシデントから学習する必要がある．関連研究で詳細に述べ，問題の原因が，規格の情報セキュリティインシデントに対する手順化不足であることを示し，インシデントからの学習の準備として「インシデントデータベースへの蓄積と分析」を提案する．そして，「インシデントデータからどのように対策を選定するか」という問題については，インシデントからの対策の自動選定が望ましい．「リスクマネジメントの定式化」に関する先行研究を踏襲し，「定式化による投資対効果」の明示による自動選定を提案する．更に，「どのように経営陣の認識を向上させ，情報セキュリティガバナンスを確立するか」という問題は，経営陣と管理者層の間の階層の壁を越える必要がある．課題の原因が規格の「マネジメントレビュー」であることを示した後，関連研究として「橋渡し人材不足」を述べ，「複数対策案の提示」を提案する．

2. 1 認証取得後のインシデントの発生

ISMS 認証を取得してもインシデントが減らない組織がある. 江口らは ISO27001 認証取得企業が未取得企業に比べて必ずしもインシデントが低減できていないことを示した [24]. 中尾らが実施した ISMS 認証取得事業所へのアンケートには，最後に自由回答欄があり，2013 年度は 103 事業者の回答，2010 年度は 130 事業者の回答が公開されている [23] [33]. 自由回答から「事故」と「インシデント」を検索すると 19 件のコメントを得ることができる．その記載内容から，その組織でインシデントが起きているか否かを判読したところ， インシデントが起きている組織が 19 件中 11 件という結果であった.

ISMS 規格は附属書の中で，インシデントから得られた知識はインシデントが将来起こる可能性や影響を低減するために用いなければならないことを要求している（A.16.1.6） [17]. 要求通りに対応すればインシデントを減らせることになるが，実態はインシデントが減らない組織があり，それは，インシデントから得られた知識を改善のために用いることができない組織があることを暗示している．インシデントを減らせない組織にインシデントデータを活用して

いくための方法・手順を明示することが情報セキュリティインシデントを減らす方法と考える.

2.1.1 ISMS 認証取得事業所へのアンケート

中尾らのアンケートによる情報セキュリティインシデントを細かく見る.

ISMS 認証取得事業所へのアンケートの最後に自由コメントがあり，2013 年度は 103 事業者の回答，2010 年度は 130 事業者の回答が公開されている [23] [33]. 自由コメントから「事故」と「インシデント」を検索すると 19 件のコメントを得ることができる. 記載されている内容からその組織でインシデントが起きているのか起きていないのかを判定した結果， 19 件中 11 件でインシデントは発生し，8 件ではインシデントは発生していない（表 6）.

表 6 自由コメントのインシデント [23] [33]

No	コメント	インシデントは
1	事故は起こさないのが常識であり，ウイルスによる被害も極々軽微なものでしかない.	起きない
2	事故の発生はこれまでもなく，人的要因が絡んだ情報セキュリティインシデントはほとんど発生していない.	起きない
3	事故を未然に防止することも大事だが，機密性と可用性をバランスよくカバーし，「当社にあった仕組みを効率よく」作りあげたいと感じている	起きない
4	何か事件・事故が起きたら大変と思う立場とそんなに出来ないという現場との立場をどの様に近づけるか	起きない
5	元々，セキュリティ事故を起こした事のない社風や仕事への取組方だと思う	起きない
6	これからも維持運用のレベルを上げて，事件・事故を防ぐつもり	起きない
7	情報セキュリティインシデント 0 件に向けて，取組み，更なる理解レベルの向上を図ることとする.	起きない
8	現状は，大きなインシデントは発生していない	起きない
9	認証企業が他社からみて，本当にセキュリティ事故が低いのか判断できない.	起きる
10	ISMS は事故が発生して当たり前で運用のモチベーションを維持するのが難しい	起きる

11	セキュリティ事故は仕組みだけでは防げない．起きる時は起きてしまう．99%は出来ても，100%は出来ない．100%防げないなら意味がないと感じる	起きる
12	この調査で，情報セキュリティの実態を改めて見直す良い機会となり，進化するウイルス感染や事故・事件に現状対策では不十分ではないか？との検証視点を変えてみる事にした．	起きる
13	セキュリティ事故の要因が組織内の人間にあるケースが最も多いことから考えれば，個々人の倫理観を高めることが最も重要なのか？	起きる
14	当所では以下のように切り分けている．・ISMS 教育・・・リスク分析等の手法等．・情報セキュリティ教育・・・事故事例や規則，運用の解説	起きる
15	審査員の質問は本質的には毎年同じで，新鮮味が薄れているが，事故・トラブルがなくなることはない	起きる
16	軽微なセキュリティ事故（入館証の紛失，携帯電話の紛失）がなくならない	起きる
17	何がセキュリティ事故で，何がそうでないか（例えば，パスワード失念等）判断が難しい（特に，一般社員にとって）	起きる
18	入館証や携帯電話の紛失事故が無くならない．	起きる
19	インシデントや指摘事項の推移状況を考慮した審査方法があっても良いのではないかと思われる	起きる

「軽微なセキュリティ事故（入館証の紛失，携帯電話の紛失）がなくならない」というコメント（No16 及び No.18）は複数の組織からよく耳にする事象である．

現状としては，ISMS 認証を取得している組織でも情報セキュリティインシデントが減らない事例が見受けられる．

2.1.2　一部上場企業での認証取得後のインシデントの発生

江口らは ISO27001 の観点から，情報セキュリティインシデント事例を用いて，認証取得企業と未取得企業を比較して分析を行うことで，認証取得がインシデント低減に寄与するかどうかを調査している．JNSA の個人情報漏えいデータ，一部上場企業情報と ISO27001 認証取得事業者一覧を突き合わせて，認証取得企業は，未収得企業よりもインシデント発生割合が高い

ことを示している（表 7） [24]．JNSA の個人情報漏えいデータは新聞やインターネットニュースなどで報道された，あるいは，組織が自組織のウェブなどで公開した個人情報漏えいインシデントの情報を集計したものであり，中尾らの調査の自由コメントで述べられたインシデントより，より深刻なインシデントと捉えることができる．

表 7　認証取得企業・未取得企業におけるインシデント件数 [24]

	一部上場企業数		インシデント件数		1 社あたり	
	認証	未取得	認証	未取得	認証	未取得
2008 年	170	1545	32	84	0.188	0.054
2009 年	177	1507	18	84	0.102	0.056
2010 年	181	1489	30	55	0.166	0.037

認証取得企業は，未収得企業よりもインシデント発生割合が高いが，これは，次が原因として考えられ，発生割合の高さは好意的に捉えることができる．

・認証取得企業の方が，インシデントを検出できる体制が整っているため，インシデント割合や件数が多くなりやすい．

・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，もともと未取得企業よりもリスクの高い企業が認証を取得している．

いずれにしても，認証を得ても情報セキュリティインシデントは発生している．

2.1.3 情報セキュリティインシデントが減らない原因

本項では，ISMS 規格では，情報セキュリティインシデント対応の結果を学習することは求めていても，その具体的な手引きを与えていないことを規定文に立ち返り示す．

ISMS では，情報セキュリティインシデントからの学習が規定されている．対応部分を次に示す [17] [34]．

A.16.1.6　情報セキュリティインシデントからの学習
管理策
情報セキュリティインシデントの分析及び解析から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いなければならない．

16.1.6　情報セキュリティインシデントからの学習

実施の手引

　情報セキュリティインシデントの形態，規模及び費用を定量化及び監視できるようにする仕組みを備えることが望ましい．情報セキュリティインシデントの評価から得た情報は，再発する又は影響の大きいインシデントを特定することが望ましい．

関連情報

　情報セキュリティインシデントの評価は，将来の発生頻度，損傷及び費用を抑制するための，又は情報セキュリティのための方針群のレビュー手続きの中で考慮するための，強化した管理策又は追加の管理策の必要性を提起する場合がある．

　機密性の側面に十分に留意すれば，実際に発生した情報セキュリテティインシデントを，発生し得るインシデントの事例，こうしたインシデントへの対応方法の事例，及び以後これらを回避するための方法の事例として，利用者の意識向上訓練において用いることができる．

　ある部署でインシデントが発生した際には，当該部署（場合により，情報セキュリティインシデント対応チーム）により 1 次対処（発見された不具合の対処）と 2 次処置（不適合の原因を除去するための処置）までは行われることになっている．対応部分を次に示す [17].

10.　改善

10.1　不適合及び是正処置

　不具合が発生した場合，組織は，次の事項を行わなければならない．

a)その不具合に対処し（react），該当する場合には，必ず，その事項を行う．

　1）その不具合を管理し，修正するための処置をとる．

　2）その不具合によって起こった結果に対処する．

b)その不具合が再発又は他のところで発生しないようにするため，次の事項によって，その不適合の原因を除去するための処置をとる必要性を評価する．

　1)その不具合をレビューする．

　2)その不具合の原因を明確にする．

　3)類似の不具合の有無，又はそれが発生する可能性を明確にする．

c)必要な処置（action）を実施する．

d)とった全ての是正処置の有効性をレビューする．

e)必要な場合には，ISMS の変更を行う．

　しかし，規格では，2 次処置の結果の学習を求めていても，その具体的な手引きを与えていない．このため，インシデント対応の学習がうまく実施できない組織の存在が予想される．

2.1.4　インシデントデータベースの蓄積と分析

前節で示した問題に対する解決策として，情報セキュリティ統括組織が組織内のインシデントデータベースを運用し，インシデントデータから組織に潜在するリスクを探索し，組織全体のセキュリティ対策の改善案を導出する方法を採用する．潜在しているリスクの探査は，闇雲に進めても難しい．インシデント（顕在化したリスク）を起点にすることで，潜在的なリスク源に対して「あたり」をつけることができるという効果がある．また，当該組織で実際に発生したインシデントデータを用いて組織のセキュリティ対策を改善していくことによって，それぞれの組織にフィットした対策にチューンアップされていくことが期待できる．もちろん，公開しないインシデント情報を活用することができる．

情報セキュリティ統括組織は，インシデントの発生からインシデントの記録をインシデントデータベースに保存する．そして，情報セキュリティ統括組織は，インシデント発生部署での 1 次対処および 2 次処置が終了した時点で,「当該部署において採択された今回の 2 次処置を，仮に全組織に採用した場合の効果」を算出する．具体的には，潜在化しているリスクについても洗い出した上で，今回のインシデントの原因に対して SLE（1 回の損害発生における予想損失額）と ARO（損害の年間予想発生回数）を見積り，そのリスクを低減させるための対策の候補を列挙するとともに，それらの対策候補の導入コストと残存リスクを計算し，インシデントデータベースに保存する．

情報セキュリティ統括組織は，定期的（例えば半年に 1 度）に，つまり，n+1 巡目の PDCA サイクルの Plan のフェーズで，本研究で提案する 3 次対応として，インシデントデータベースを精査し，n 巡目の PDCA サイクルの Do のフェーズで発生したインシデント群に対する対策候補を俯瞰することによって，全組織として新たに採用すべき対策の候補を選択する（図 19）．

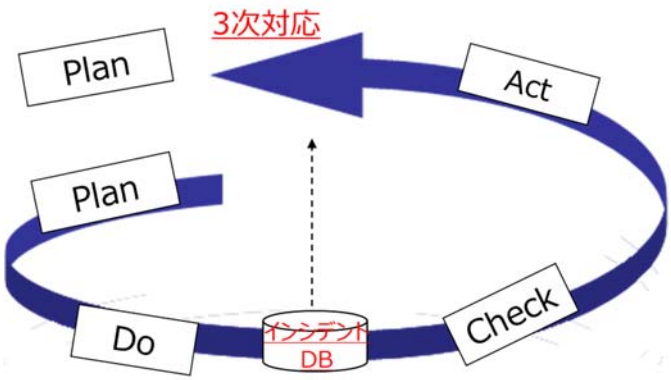


図 19　インシデントデータベースと 3 次対応

2. 2　ISMS のリスクマネジメントにおける定式化

ISMS のリスクマネジメントにおける定式化について述べる．この定式化は，本研究で提案するデルタ ISMS のインシデントに対する対策コストの定式化と類似である．

2.2.1　リスクマネジメントの手順

本項では，ISMS が規定するリスクマネジメントの手順について説明する．

リスクアセスメントとリスク対応は次の作業手順を取る（図 20） [35].

作業１：リスクアセスメントの取り組み方法を定義する．

作業２：リスクを特定する．

作業 3：リスクを分析する．

作業 4：リスクを評価する．

作業 5：リスク対応を行う．

作業 6：リスク対応の選択肢に対する管理策を決定する．及び附属書 A との比較．

作業 7：適用宣言書を作成する．

作業 8：情報セキュリティリスク対応計画を作成する．

作業 9：残留リスクを承認する．

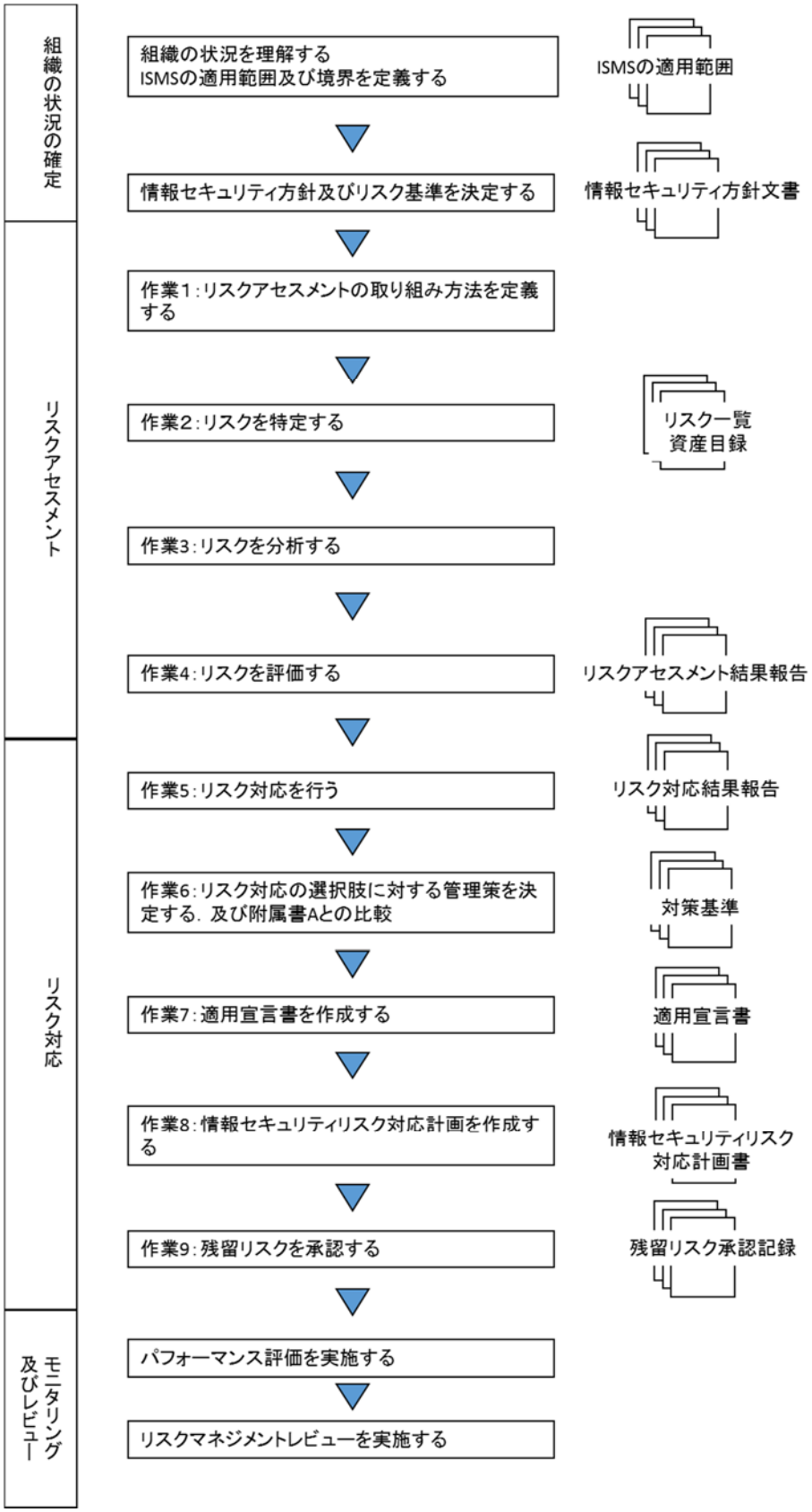


図 20　リスクアセスメント及びリスク対応に関する作業 [35]

(1) 資産目録

「作業２：リスクを特定する」で作成される資産目録の例を表 8 に示す [36].

表 8　資産目録の例（一部） [36]

項目	情報資産名	管理責任者	情報資産管理手順			廃棄		
			保管場所	保管方法	保管期限	廃棄方法	廃棄担当者	廃棄の記録
1	見積依頼書	営業担当者	営業部ファイルキャビネット	担当者別	3 年	シュレッダー	営業担当者	ー
2	見積データ	営業担当者	販売管理システム	自動登録	2 年	削除	IT 担当者	必須
3	見積書	営業担当者	営業部ファイルキャビネット	担当者別	3 年	シュレッダー	営業担当者	ー

(2) リスクアセスメント結果報告

リスクレベルは, 例えば,「資産の価値」×「脅威のレベル」×「脆弱性」で計算される [35].

「作業 4：リスクを評価する」で作成されるリスクアセスメント結果報告の例を表 9 に示す [37].

表 9　リスクアセスメント結果報告の例（一部） [37]

資産	場所	脅威	脆弱性	資産価値	脅威のレベル	リスク値
ソフトウェア	コンピュータ	悪意または過失によるコピー	教育の不足	5	高	7
			新入社員のモラル不足		高	7
		ウイルス感染	管理策の不備		高	7
	可搬型媒体	悪意または過失によるコピー	管理策の不備		高	7
		媒体の盗難	管理策の不備		中	6
		媒体の廃棄	管理の不備		中	6

2.2.2　リスクマネジメントにおける定式化

情報資産のモデル化に対して，リスク分析の分野では古くから ALE（Annual Loss Expectancy）により年間予想損失額を定式化する方法が採られている [38]. Soo Hoo は情報セキュリティの分野にリスク分析を持ち込んだのは現在の NIST（アメリカ国立標準技術研究所）の前身である国立標準局（National Bureau of Standards， NBS）が 1979 年に発行した Guideline for Automatic Data Processing Risk Analysis, FIPS PUB 65 を初出としている [39].

ALE は

ALE = SLE× ARO

SLE = AV ×EF

として定式化される．ここで，SLE は 1 回の損害発生における予想損失額，ARO は損害の年間予想発生回数，AV(Asset Value)は資産価値，EF(Exposure Factor)は起こりうる損害の可能性である．なお，ここでの用語「対策」は ISMS の用語における「管理策」を指す.

中村らは，資産，脅威，対策の対応を図 21 にて示す関係として捉えた [40].

ここで,

V_k ： 資産の価値.

E_{jk} ： 脅威が資産に影響するか否かのフラグ.

P_j ： 一定期間内に脅威が発生する確率.

C_i ： 実施に必要なコスト.

R_{ji} ： 脅威に対する攻撃が発生した場合において，対策によってその攻撃の成功率が減少する.

S_i ： 対策 i を選択するか否かのフラグ.

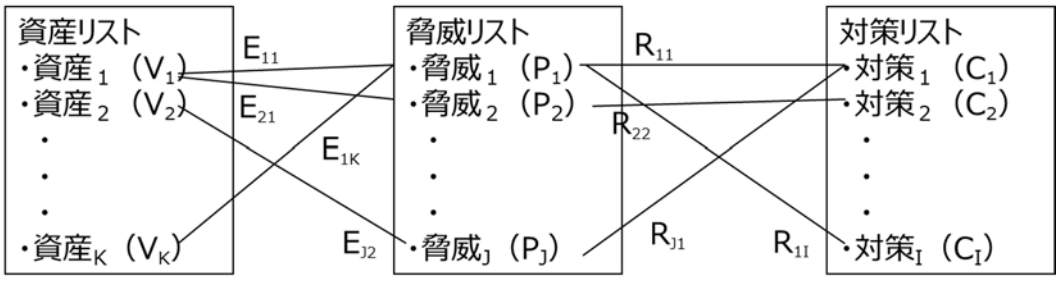


図 21　資産，脅威及び対策の対応 [40]

そして，次式の値が最大になる i の組合せを最適な対策の組合せとして求めることができる

ことを示した.

式 1：

残存する資産 k の価値 V_k の期待値の総和

$$\sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i \right) \right] \right\} - \sum_i C_i S_i$$

脅威 j が有効な資産 k が一定期間内に失われる確率　　対策コスト

表 10 に脅威と対策案の表を例示する.

表 10　脅威と対策案の表 [37]

				1	2	3	4	･･
脅威Tj			脅威の発生確率Pj	情報提供サービスの利用	インシデントレスポンスチーム設置	外部による研修の実施	WBTや関係書籍の配付と自己研修	･･
対策コストCi（万円）				36	2400	100	50	･･
ソフトウェア資産	1	内部者の悪意または過失によるコピー	0.5	0	0.1	0.5	0.3	･･
	2	ウイルスの感染	0.5	0.5	0.3	0.3	0.1	･･
	:	:	:	:	:	:	:	:

中村らの提案する方法により，対策選定のノウハウのない人でも定式化された手順に従い選定が行えるようになる，同時に対策選定における結果の再現性を保証できる．しかし，一巡目の Plan 時のリスクマネジメントに対する定式化であるため，今回課題とする Act から次巡の Plan への結合に関しては解決策とならない（図 22）.

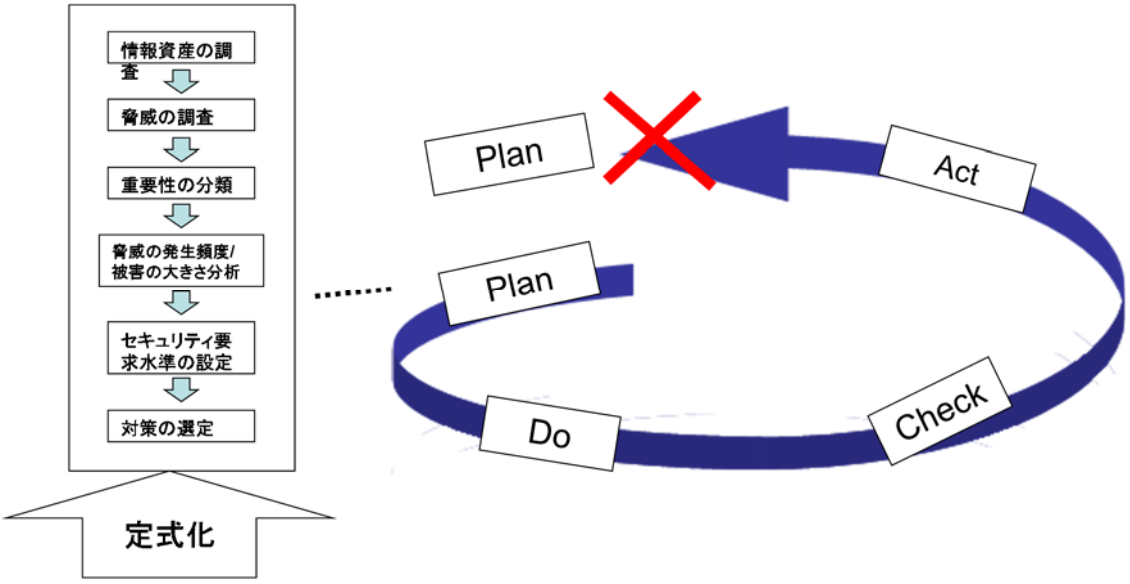


図 22　リスクマネジメントの定式化

なお，西垣らは中村らの手法で情報セキュリティ対策とデジタルフォレンジック対策の両者を，費用対効果の観点からセキュリティ対策の選定を最適化する方式を提案している [41].

2.2.3　インシデント分析での定式化

投資対効果の高い対策を候補として選択するために，インシデント原因と対策のマトリクスである「デルタ ISMS 表」を用い，対策候補選択タスクを離散最適化問題として定式化する（図 23）. 対策選定の手法については，中村らの方法以外にも FTA（Fault Tree Analysis）や Medical SAFER など（付録 1 参照）が情報セキュリティインシデントと対策を関連付ける手法として著名である．これらの，対策やインシデントの関係に論理素子や時系列を持ち込む方法は記述力を増すものの，多くのインシデントや対策を扱う場面では，インシデントと対策の関係性を必要以上に複雑化することとなる．加えて，ISMS の手順で作成される各種の表データとの親和性より，デルタ ISMS は中村らの手法をベースとする．デルタ ISMS 表と定式化については次章で詳述する．

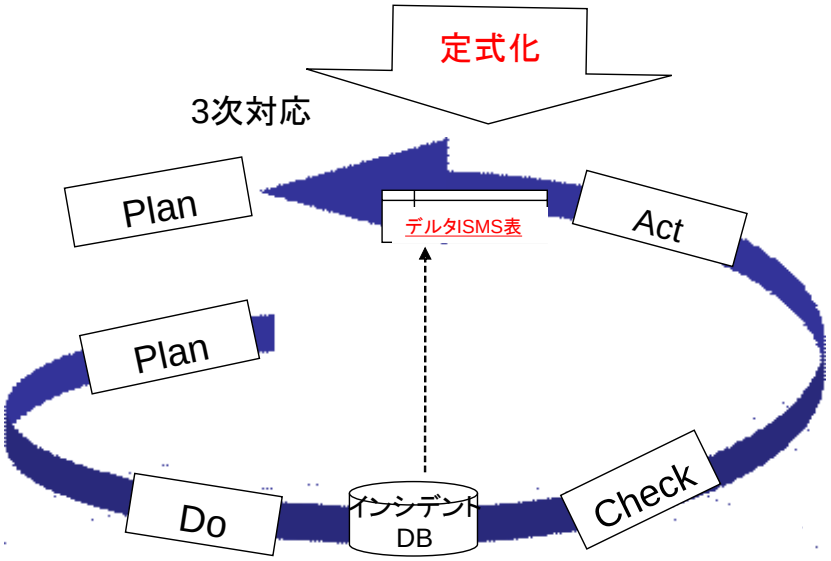


図 23　デルタ ISMS 表と定式化

2. 3　経営陣と管理者層の橋渡し

対策を実施するためには経営陣の認許を得る必要がある．経営陣と管理者層の間には階層の壁が存在する．経営陣の認許を得るためには，階層の壁を越えて経営陣の認識向上を図る必要がある．これを経営陣と管理者層の橋渡しとよぶ．しかし，ISMS が規定するマネジメントレビューは情報セキュリティガバナンスの観点が欠けており，このことは，ISMS 認証組織へのアンケートでも経営陣の認識向上があまり取り組まれていないという現状から見ることができる．経営陣の認識不足という問題に対しては，経営陣と管理者層の橋渡し人材不足という先行研究もある．こうした背景の下，デルタ ISMS では複数対策案を提示することで，経営陣の方向性と合致できる対策を選択できるようにし，経営陣と管理者層の橋渡しを実現する．

2.3.1　マネジメントレビュー

ISMS の規格が求めるマネジメントレビューは，トップマネジメントの認識向上のためではなく，ISMS の PDCA サイクルの第 3 者 Check の一つとして位置づけられている．

ISMS をうまく進めていくためには，管理者層からトップマネジメントへの効率的な情報提供が必要となる．ISO/IEC27001 の「マネジメントレビュー」では，組織の ISMS が引き続き適切，妥当，かつ，有効であることを確実にするためのレビューの活動であり，適切なインプットに基づいて，組織の ISMS がこのままで良いのか，どこに欠陥があり，その欠陥をどのように修復すべきかを判断する．マネジメントレビューは図 24 に示すようなトップマネジメン

トの活動と解釈されており，ISMS の PDCA（plan-do-check-act）サイクルを Check する位置付けとなる．

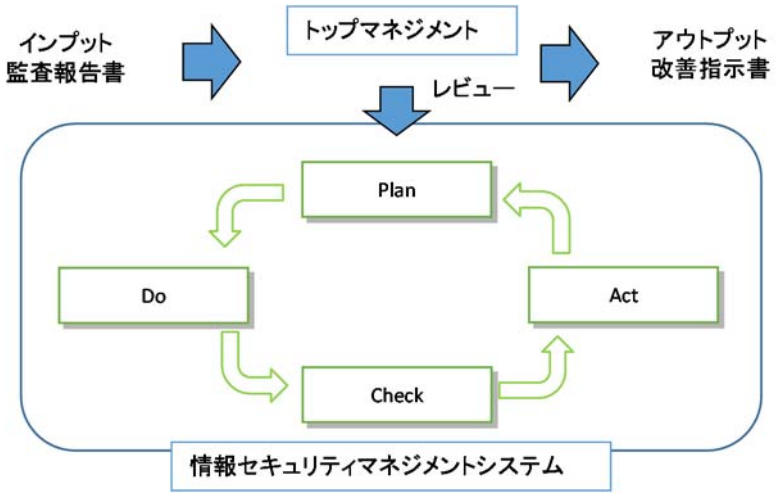


図 24　ISMS のマネジメントレビュー

マネジメントレビューでの考慮事項として，①前回までのマネジメントレビューの結果によりとった処置の状況，②ISMS に関連する外部及び内部の課題の変化，③情報セキュリティパフォーマンスに関するフィードバック，④利害関係者からのフィードバック，⑤リスクアセスメントの結果及びリスク対応計画の状況，及び⑥継続的改善の機会が求められている [4]．マネジメントレビューは考慮事項が規格で規定されており，文書で考慮結果を残すことにもなっているため，全事項の考慮が必要となる．

次に，マネジメントレビューの現状として，ある実際のマネジメントレビューで考慮項目がどのように扱われたかを見てみる．

最初の 6 項目は ISMS が規定するマネジメントレビューでのチェック項目である．

① 前回までのマネジメントレビューの結果によりとった処置の状況:
指摘事項を ISMS マニュアルへどのように反映したかが報告された．

② ISMS に関連する外部及び内部の課題の変化:
組織変更やロケーションがどのように適用範囲に影響を与え，それらをどのように ISMS マニュアルへ反映したかが報告された．

③ 情報セキュリティパフォーマンスに関するフィードバック:
外部審査報告書（パフォーマンス評価，不適合，改善の余地）及び内部監査報告書（不適合や改善の余地）に関する件数と対処の状況が報告された．加えて，「目標とその結果」について報告された．

④ 利害関係者からのフィードバック:

客先指摘・改善件数とその対応状況が報告された.

⑤ リスクアセスメントの結果:

リスク対応計画の状況，及び資産管理台帳，リスク管理表，リスク対応計画の状況が報告された.

⑥継続的改善の機会:

ISMS 会議の概要が報告された.

この報告と平行して，次の事項が報告された.

⑦セキュリティインシデント

⑧外部審査の予定

⑨内部監査の予定

⑩年間計画

⑪ISMS 導入効果

⑫残存リスク

⑬次年度の適用範囲の変更予定

この議事録におけるセキュリティインシデントの占める記述量の割合は 7.6%であった.

特に，ISMS の認証範囲が組織の一部である場合や目標にインシデントに関する項目が含まれなかった場合は審査や監査での不適合の扱いに重きが置かれ，セキュリティインシデントの扱いは軽くなる．マネジメントレビューが認証継続のためのレビュー会となると，インシデント報告は形骸化し， トップマネジメントが「組織全体のセキュリティ対策の改善」を行うにあたって必要となる判断材料（対策を追加したり改定を採用したりするかどうかを判断するための情報）を提供することが達成されていない．マネジメントレビューの考慮事項は ISMS の状況チェックであり，アウトプットは改善指示である．組織の中でインシデントが減らない状況があっても，それが報告されることは必須ではなく，インシデント軽減に対する対策実施を方向付けることも ISMS の枠組みの中では求められておらず，前述した Act から次巡の Plan への連絡が途切れることなる（図 25）.

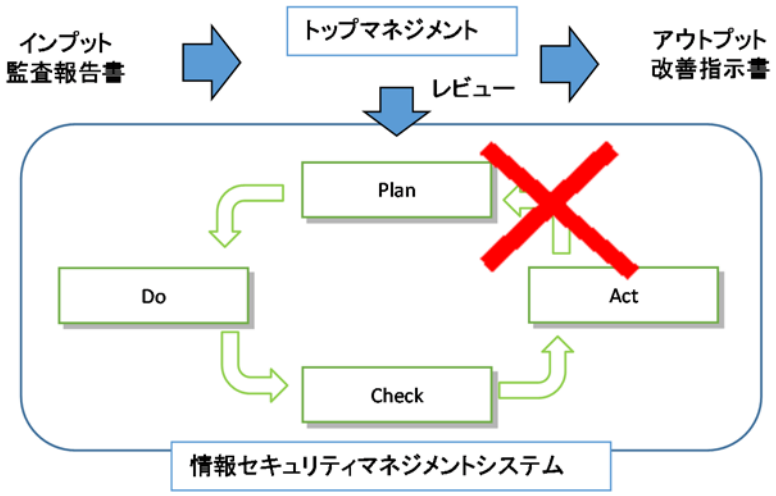


図 25　PDCA が途切れるマネジメントレビュー

インシデント報告において，経営陣が「組織全体のセキュリティ対策の改善」を行うにあたって必要となる判断材料（対策を追加したり改定を採用したりするかどうかを判断するための情報）はどのような内容であるべきであろうか.

2.3.2　経営陣の認識

ISMS 認証取得事業所へのアンケート [23]には，重点的な取り組みについてのデータがある.「ISMS の効果を高めるため重点的に取り組んでいるもの」についての調査では，「認識」について調べると「一般社員の認識」と「管理者層の認識」については重点的に取り組む組織が多いが，「経営陣の認識」について重点的に取り組んでいる組織は多くない（表 11）.

これは，ISMS の規格が経営陣の認識向上を求めていないことによる.

表 11　ISMS の効果を高めるため重点的に取り組んでいるもの [23]

%	**一般社員の認識**	教育研修の改善	内部監査人スキル強化	**管理者層の認識**	マニュアルの整備	有効性評価手法	文書・記録管理	リスク分析手法	インシデント対応	**経営陣の認識**	費用対効果	その他	有効回答数
2012 年	66.4	29.7	27.6	26.7	22.1	21.9	20.3	19.2	15.5	11.0	4.1	1.1	438
2010 年	67.5	30.5	31.5	29.6	24.8	31.5	22.6	24.3	20.9	15.6	5.8	1.0	416
2008 年	62.5	29.0	25.9	21.6	22.4	31.8	20.7	20.7	17.3	9.9	4.8	2.6	352
2006 年	69.3	36.0	23.1	28.8	31.4	40.9	23.5	23.5	20.5	10.2	4.5	1.5	264

2.3.3　橋渡し人材不足

管理者・従業員層は，経営陣が「組織全体のセキュリティ対策の改善」を行うにあたって必要となる判断材料を提供する術を持っていないがために，マネジメントレビューとして経営陣に報告できる内容は「処置が完了しているか否か」というインシデントの状態のみとなってしまう．したがって，経営陣は「対策を追加したり改定を採用したりする必要があるか否か」の判断を下すことができず，情報セキュリティリスク管理に対する経営陣の認識も向上しないまま留まってしまう．この結果，組織の情報セキュリティマネジメントが情報セキュリティガバナンスと乖離するという深刻な問題へと至っているものと考えられる．

ISMS 認証取得事業所へのアンケートによれば，トップマネジメントが経営陣である割合は約 6 割であり，約 4 割は経営陣でない（図 26） [23]．ISMS のトップマネジメントから経営陣への認識向上活動が別途必要となる．

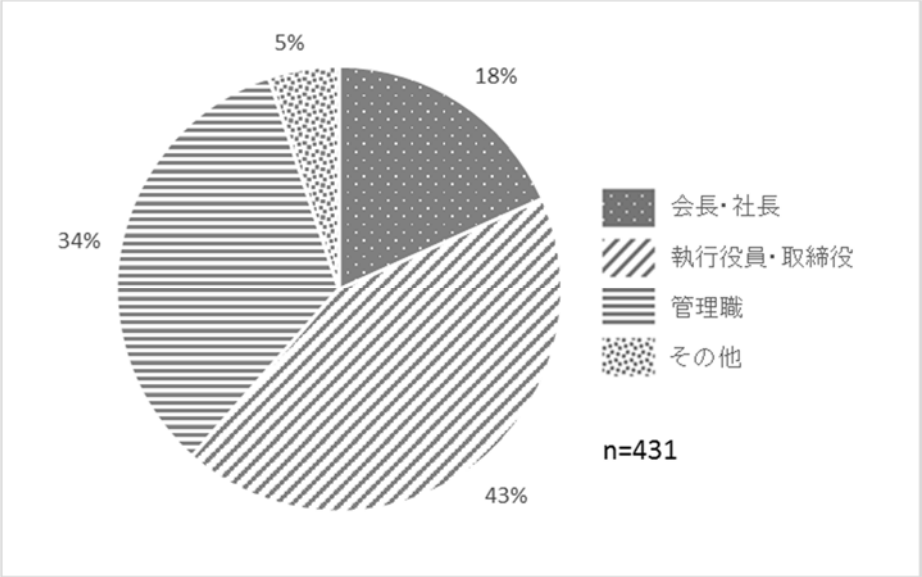


図 26　ISMS の運用責任者 [23]

CISO は経営陣（ガバナンス）と実務者グループの間に位置し，情報セキュリティ管理を担当する．CISO がリスク管理方針から情報セキュリティ目的・目標を展開し，経営陣の意思を反映した対応策の実装を可能にする．CISO は経営陣の一員，若しくは経営トップからその役を任命された管理者である．

2015 年に IPA が実施した「企業におけるサイバーリスク管理の実態調査 2015」では CISO（情報セキュリティ管理の担当役員）の設置率は 23%であった（図 27） [42].

一方，Westby は米国， 欧州及びアジア地域における CISO の設置割合はそれぞれ 58%，72%，52%であったという調査報告を行っている [43]．アジア地域の CISO の設置割合は欧州と比較して低い水準となっている．これらと比べても日本の CISO の設置率は低い.

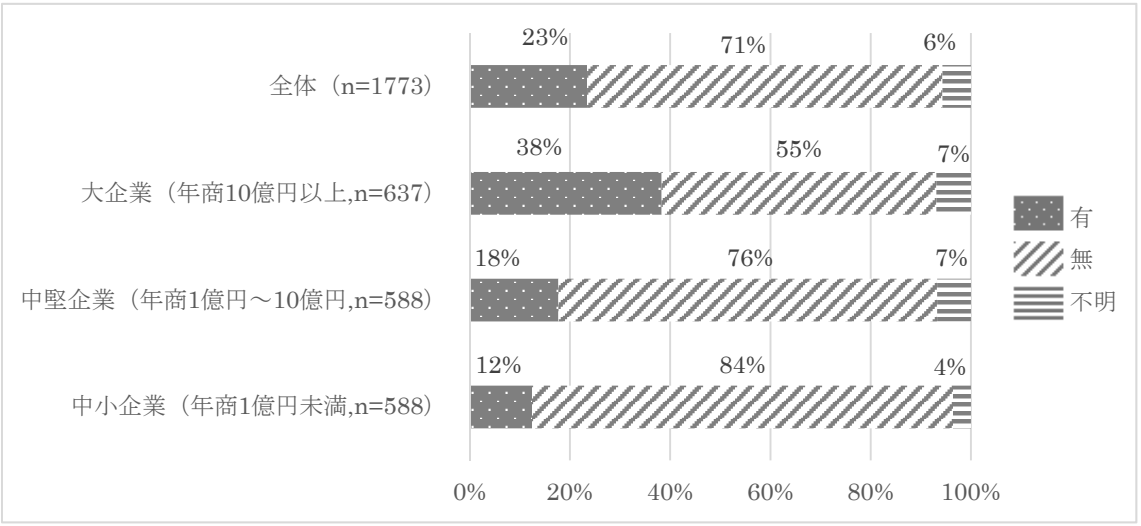


図 27　CISO の有無 [42]

IPA の調査による情報セキュリティ管理の担当部署・部門の設置率は兼務も含めて 42%であった（図 28）. Westby の調査では,『 2008 年に全世界で 17%であった情報セキュリティ管理の組織横断のチームが 2012 年には 72%に改善されている』となっている [43]. これらの値と比較すると日本の情報セキュリティ管理の担当部署・部門の設置率には改善が推奨される.

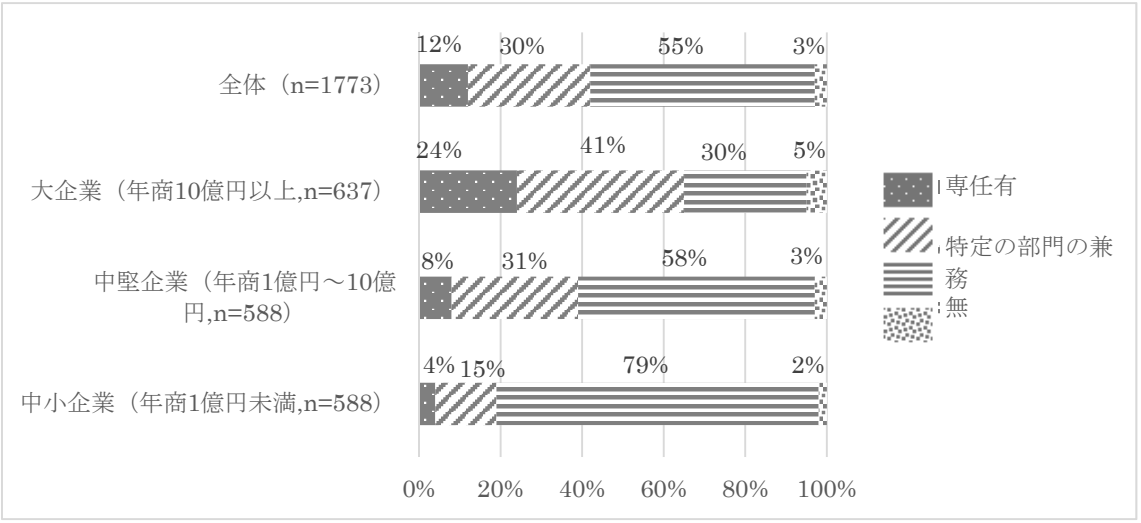


図 28　情報セキュリティ管理の担当部署・部門の有無 [42]

更に佐々木は CISO の組織における位置づけから単に組織に CISO が設置されれば良いという問題ではないことを示している（図 29） [44]. ここでの望ましい形はまさしく実質的な経営層・実務者層間の橋渡し人材である.

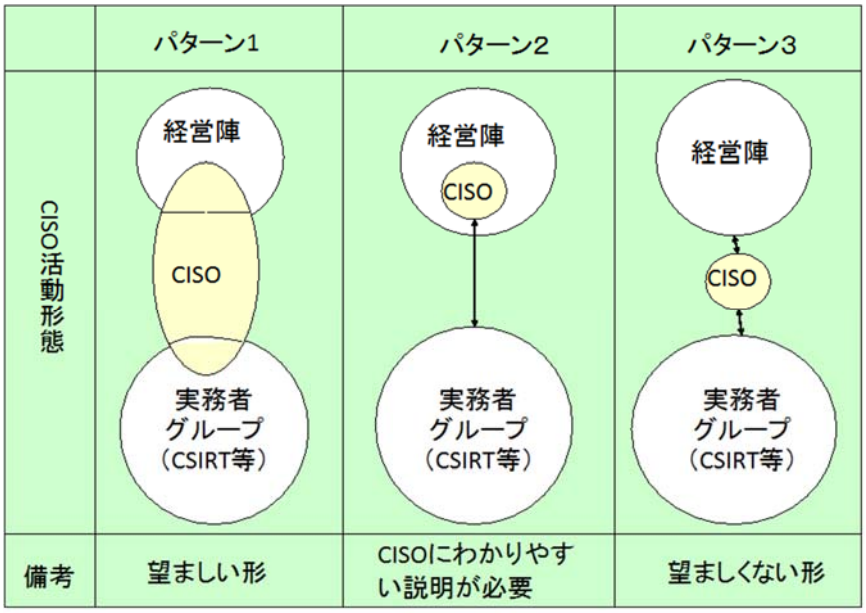


図 29　CISO の関与パターン [44]

内閣サイバーセキュリティセンター（NISC）は,『サイバーセキュリティを推進する経営層・実務者層間の橋渡し人材（旗振り役）が不足しているとしている』 [45]. 図 30 において，橋渡し人材が不足と回答した企業が 72.9%である.

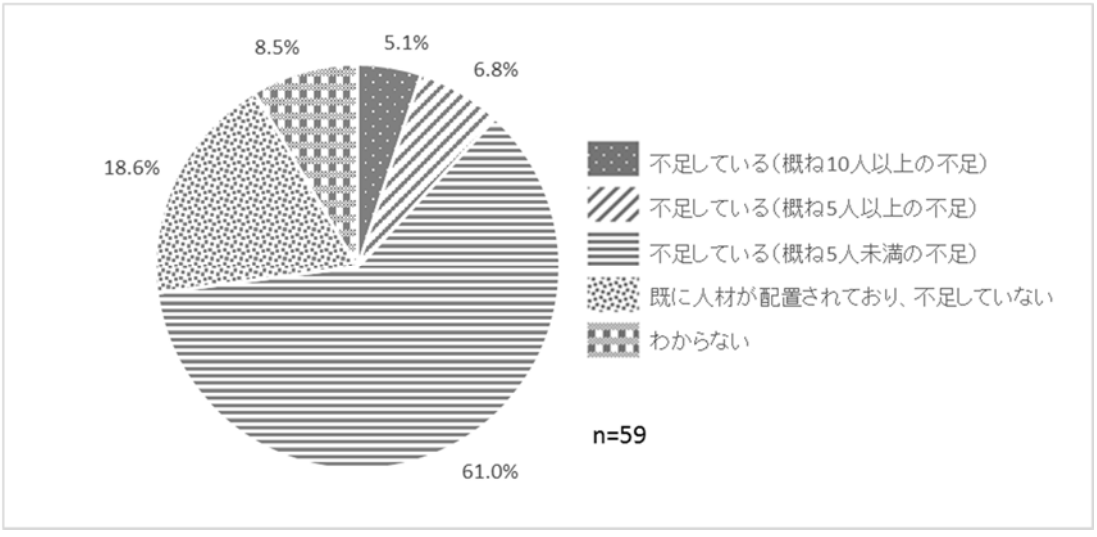


図 30　サイバーセキュリティ人材（橋渡し人材）の不足状況（n=59） [45]

情報セキュリティの経営陣と ISMS の橋渡しは重要な研究テーマの一つであり，橋渡し人材が提供すべき情報が整理されているべきであり，それらの情報をどのように得るかを手順化しておれば，経営陣と ISMS の橋渡し人材不足を解消することができると考える.

2.3.4　情報セキュリティガバナンス

2009 年，経営陣の認識向上などを経営陣の視点からの役割を明示し，ISMS を補完するために経済産業省から情報セキュリティガバナンスガイドラインが公表された [31]．情報セキュリティガバナンス導入ガイダンスは情報セキュリティ対策において経営陣が取り組むべき行動指針として，情報セキュリティガバナンスの導入を提唱している．

情報セキュリティガバナンスとは，企業の経営陣（代表取締役，取締役，役員等）において，情報資産に係るリスクの管理を狙いとして，情報セキュリティに係る意識，取組み及びそれらに基づく業務活動を組織内に徹底させるための仕組みを構築，運用する取組みを指す．従来は，経営陣と管理者・従業員層との間で情報セキュリティに関するリスクや対策についての共通認識が乏しく，全体最適化された構築・運用がなされないという問題があった．このガイドは，この問題への対処指針となっている．

図 31 に情報セキュリティガバナンスのフレームワークを示す．情報セキュリティガバナンスのフレームワークは，「モニタリング」「評価」「方向付け」の基本サイクルを持つ．情報セキュリティガバナンスの確立とは図 31 の活動を企業内に実装していくこととなる．

ISMS では，部署，事業所，工場といった場所というように対象範囲を合理的に説明ができる範囲に限定して「適用範囲」として認証取得範囲に選定することができることもあり，PDCA サイクルが管理者・従業員層に留まりやすい．このため，情報セキュリティガバナンスでは，ISMS 認証取得部署の PDCA サイクルのモニタリング・評価・方向付けを行う監視サイクルが設けられ，情報セキュリティガバナンスの監視サイクルが ISMS の PDCA サイクルを駆動する形態となっている．

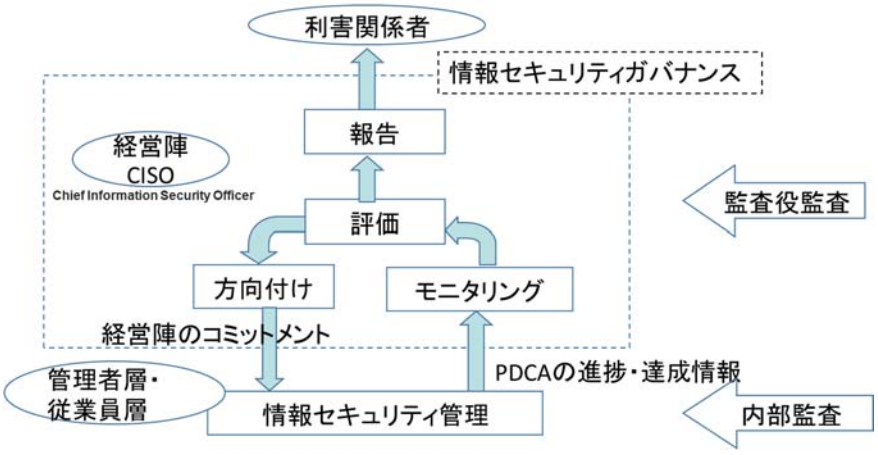


図 31　情報セキュリティガバナンスのフレームワーク [31]

マネジメントレビューがISMSのチェックのための仕組みであるのに対して，情報セキュリティガバナンスシステムは，経営陣のあるべき役割を示した仕組みと捉えられる．（付録 2 にISMSとコンプライアンスを対象とする内部統制システムとの比較を行う）．

2.3.5　複数対策案の提示

本論文で提案するデルタISMS モデル（次章で詳述する）において，情報セキュリティ統括組織は，n+1 巡目のPDCAサイクルのPlan のフェーズにて，インシデント原因と対策のマトリクスである「デルタISMS 表」を用いる時に，安全係数を用いて対策の安全率を変動させることで，金銀銅の3 パターンの対策候補の案を自動導出できる．

定式化により得られた対策群は，投資対効果を加味した最適解ではあるが，あくまでも情報セキュリティ対策における最適解であり，全組織から見た場合は，部分最適化となっていることもある．全体最適化の観点からは，対策選択には，経営陣による方向付けが必要となる．そこで，金銀銅などの複数パターンを導出し，経営陣に仰ぐことで経営状況に則した対策選定を可能とする．例えば，銀を合理的な対策群案とするなら，よりコストを掛けた対策群案を金とし，ステイクホルダーには，しっかりとしたセキュリティ対策を実施する組織としてアピールすることができる．また，コストを抑止した銅の対策群案は重点を絞った対策選択と表明することができる．

情報セキュリティ統括組織は，マネジメントレビューの際に，デルタISMS 表とともに3パターンの対策候補案を提示する．CISOは，この情報を説明材料や判断材料として使い，「組織全体のセキュリティ対策の改善」を達成するために採用する対策を決定する．取締役会等でCISO 等が経営陣にこれらの情報を説明することで，経営陣の情報セキュリティリスク管理に対する認識を向上していく（図 32）．

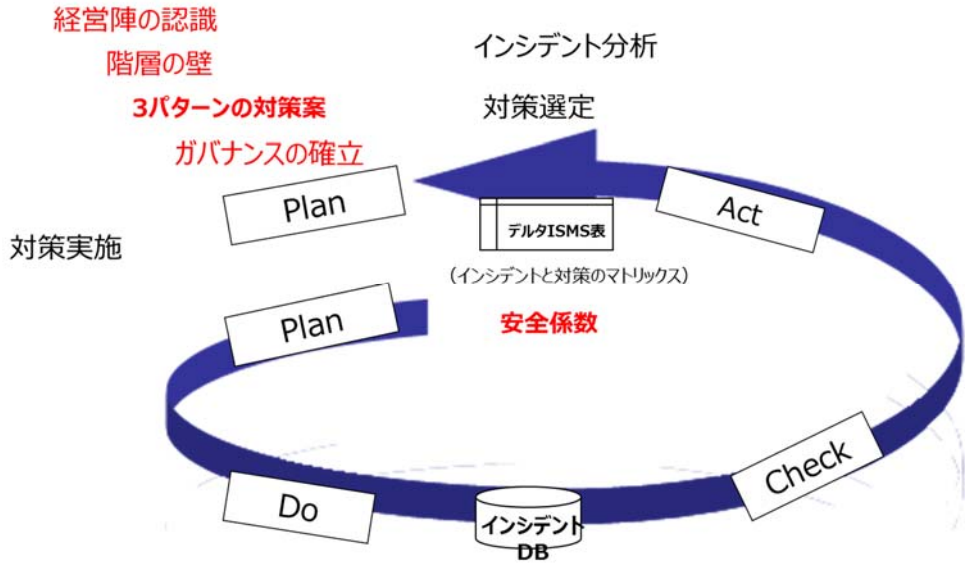


図 32　安全係数と 3 パターンの対策案

ISMS の課題である Act から次巡の Plan への連結を目指すものであり，これらの一連の方法・手順が「デルタ ISMS」である（図 33）.

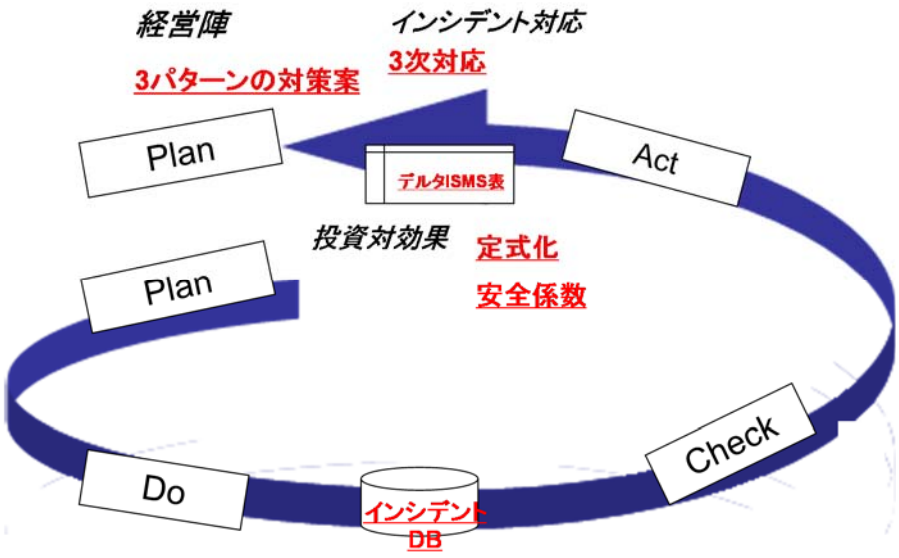


図 33　デルタ ISMS

2. 4 まとめ

2 章では，ISMS 認証を取得した組織でもインシデントが減らないことを示した関連研究を

述べ，本研究で提案するデルタ ISMS としてインシデントデータベースへのインシデント情報の登録・蓄積を提案した．次に，リスクマネジメントに対する定式化の関連研究を示したのち，インシデントに対する全社レベルの 3 次対応，インシデントと対策のマトリックスであるデルタ ISMS 表とその定式化を提案した．最後に，経営陣の認識向上を課題とする橋渡し人材不足の問題という関連研究を示し，安全係数による複数対策の自動選定と経営陣への 3 パターンの対策案の提示を提案した．

経営陣への 3 パターンの対策案の提示により，情報セキュリティ統括組織は，マネジメントレビューの際に，デルタ ISMS 表とともに複数の対策候補案を CISO に提示することができる．CISO は，この情報を説明材料や判断材料として使い，セキュリティの対策を決定する．取締役会等で CISO 等が経営陣にこれらの情報を説明することで，経営陣の情報セキュリティリスク管理に対する認識も向上していく．この結果，組織の ISMS に対する監視サイクルが実質的に機能するようになり，デルタ ISMS による良好なスパイラルアップを得ることができ，情報セキュリティガバナンスが確立する（図 34）．

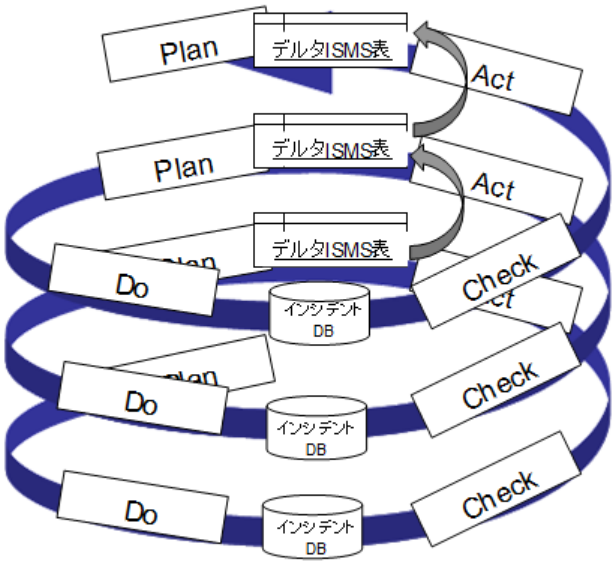


図 34　デルタ ISMS によるスパイラルアップ

第3章　デルタ ISMS モデル

本章では本論文で提案するデルタ ISMS モデルについて詳しく説明する．デルタ ISMS モデルは，組織内で実際に発生した情報セキュリティのインシデントデータを使って， ISMS の PDCA サイクルの 2 巡目以降で組織の情報セキュリティリスク管理を改善していくための方法・手順を具現化したものである（図 35）．

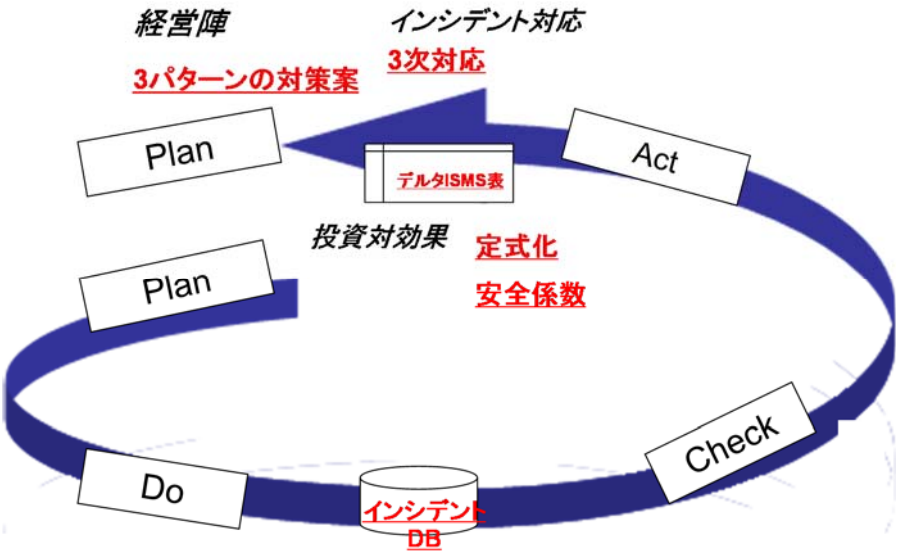


図 35　デルタ ISMS モデル

3. 1 インシデントデータベースの運用

Do フェーズで発生する情報セキュリティインシデントに対処するため，インシデント情報を登録・蓄積する．デルタ ISMS では，インシデント情報の蓄積にインシデントデータベースを用いる．本節では，インシデントデータベースの緒元を詳説する．登録する内容をより明確にするため，インシデントの原因区分を定め，被害額の考え方を整理する．

3.1.1　インシデントデータベース

情報セキュリティ統括組織は，インシデント対応の結果を，インシデントデータベースに登録・蓄積していく．登録はインシデント対応の直後に行う．インシデントデータベースは，日時，インシデント内容，インシデント原因，インシデント経路，影響範囲，1 次対処の内容および被害額，2 次処置の内容および対策コスト，3 次対応の内容からなる．表 12 にインシデ

ントデータベースの諸元を示す．ここで示す項目は，後工程（3．4 節参照）の対策導出のために必要な最低限の項目である．

表 12　インシデントデータベースの諸元

列名	意味
日時	インシデントの発生した日時.
インシデント内容	インシデントの内容（自由書式）.
インシデント原因	インシデント原因を次の 13 種の区分から選択する. 誤操作 / 紛失・置忘れ / 不正アクセス / 不正な情報持ち出し / 管理ミス / バグ・セキュリティホール / 盗難 / 内部不正行為 / 設定ミス / 目的外使用 / ワーム・ウイルス /　不明 / その他
インシデント経路	インシデントの経路を次の 7 種類から選択する. USB 等 / 紙媒体 / パソコン / インターネット / 携帯電話・スマートフォン / 電子メール / その他
影響範囲	影響範囲を選択する．ヒヤリハットから深刻なインシデントまで.
1 次対処	1 次対処の内容.
1 次対処の被害額	インシデントが収束するまでの間に掛かった費用を社内人工費を含めて積み上げる．なお，再発防止対策に掛けた費用は含めない.
2 次処置	2 次処置の内容.
2 次処置の対策コスト	再発防止のための対策コストを社内人工費を含めて積み上げる.
3 次対応	3 次対応の内容. 想定される潜在リスク，SLE，ARO，ALE，リスクの扱いを記録.

インシデントはリスクが顕在化した事象である．インシデントデータベースは単なる「インシデントの事実」のみを羅列したものに留まらず，そのインシデントから顕在化したリスクと潜在的なリスクの両方を洗い出すためのものとなる．

インシデントデータベースにはヒヤリハットに関する情報も含め，組織内で起こったすべてのインシデントを記録・蓄積する．また，リスクの洗い出しのためには，インシデントだけに限らず外部審査と内部監査で指摘された是正項目や改善提案も有効である．外部審査と内部監

査の是正項目や改善提言は，次の 3 個に区分できる．

・組織の規則や記録などの文書に係る項目．

・リスクアセスメントやパフォーマンス評価など ISMS のやり方に係る項目．

・実地検査により発見された不具合項目

このうちの実地検査により発見された不具合は，リスクの直接的な顕在化であり，有効にインシデントデータベースに取り込める．

3.1.2 インシデントの原因

インシデントデータベースに登録する項目を明確にするために, あいまいとなり易い「原因」の分類を定義しておく．

インシデントは，原因のプロパティをもつ．原因について，JNSA は情報漏えい原因区分の 13 種を定義している [46]．次に示す．

1) 誤操作：あて先を書き間違えたり，操作ボタンを押間違えたりするなどの人間のオペレーションによって情報が漏えいした場合．
2) 紛失・置忘れ：持ち出し許可を得た情報を，持ち出し先や移動中に置忘れたり，紛失したりした場合．個人の管理ミスによって発生した場合．
3) 不正アクセス：外部の第三者が，主にネットワークを経由して不正にアクセスを行って情報が漏えいした場合．
4) 不正な情報持ち出し：業務上の必要性などから，ルールを逸脱して情報を持ち出した場合．
5) 管理ミス：社内や主要な流通経由によって紛失・行方不明となった場合．作業手順の誤りや，情報の公開，管理ツールが明確化されていなかったために業務上において漏えいした場合．紛失の責任が組織にある場合．
6) バグ・セキュリティホール：OS やアプリケーション等の既存ソフトウェア上のバグ・セキュリティホールが原因で情報が漏えいした場合．
7) 盗難：第三者によって情報記録媒体と共に情報が盗まれた場合．
8) 内部不正行為：社員，管理下にある他社社員（派遣社員など）が，不正アクセス，その他不正な行為によって情報を持ち出して悪用した場合．
9) 設定ミス：ユーザが Web サーバやファイルのアクセス権などの設定を誤ったことによって情報が漏えいした場合．
10) 目的外使用：個人情報を当初の目的以外の用途に使用した場合．
11) ワーム・ウイルス：ワームやウイルスによって，情報が漏えいした場合．

12) 不明：原因が不明なもの.
13) その他：上述したいずれにも該当しないもの.

本研究では，上述した原因区分をそのまま使用する．これにより，組織内のインシデント原因と市場で発生しているインシデント原因の比較が可能であるメリットを持つ.

3.1.3 被害額

インシデントは，被害額のプロパティをもつ．被害額については，大谷は，被害額が直接被害額と間接被害額に加え，復旧コスト，対応コスト，事業継続コストから構成されることを示した [47]．田中は，被害額に加えて，投資コストを影響額としている（図 36） [48].

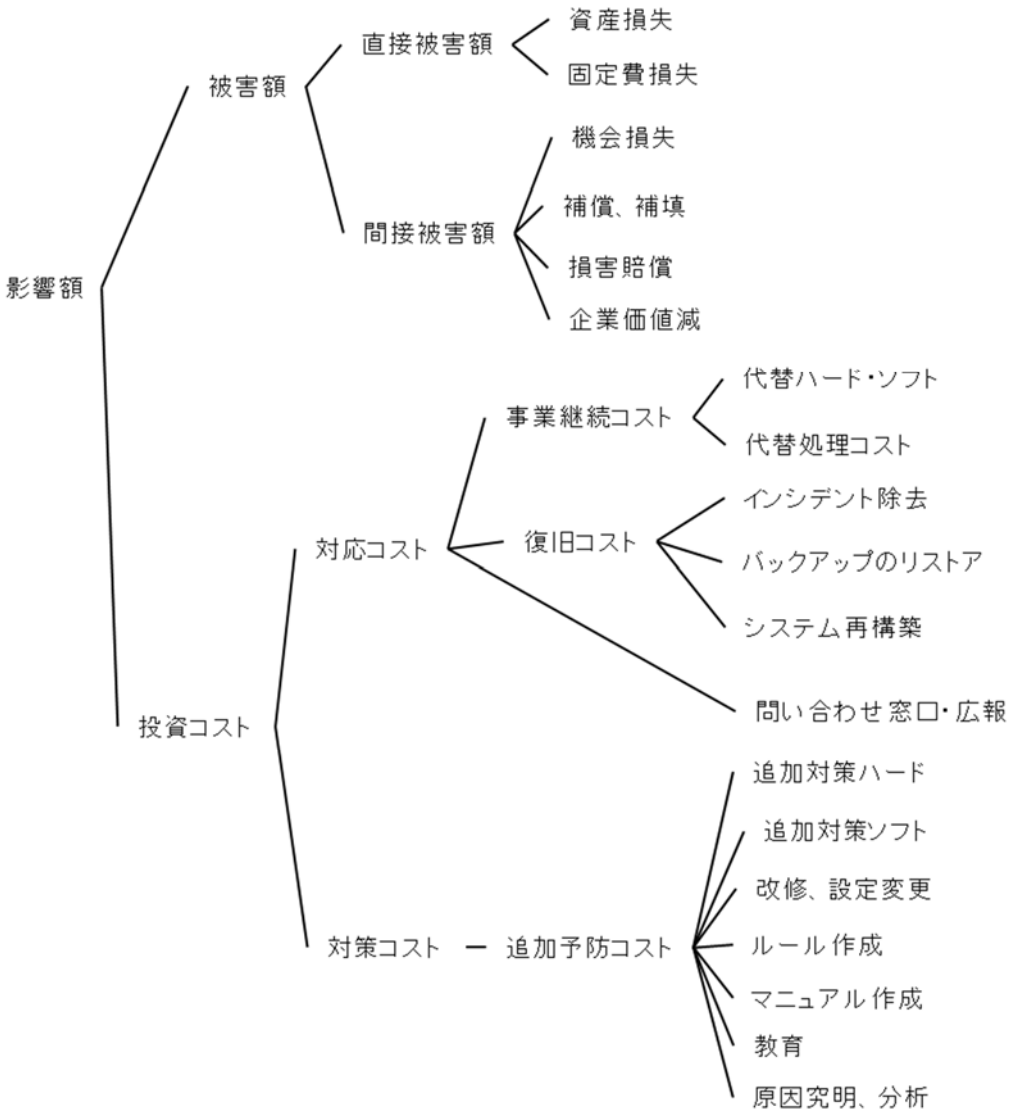


図 36 影響額の構成図 [48]

被害額，影響額をどのレベルに取るかについて，まず，本研究では被害額の減少を対策の効果とし，各種コストは効果を達成するための負担と見なす．次に被害額については機会損失と企業価値減の正確な算出は困難である場合もあることから，被害額と対応コストとを加算したものから機会損失と企業価値減を外した値とする．とはいえ，機会損失や企業価値減が正確に算出できる場合は，それらを被害額として組み込むことに問題はない．そして対策コストをコストとする．

なお, 被害額については, 他に, 石川らは個人情報賠償金額の算出モデルを比較している [49]. Cichonski らは情報セキュリティインシデントを機能のインパクト，情報のインパクト及び復帰容易性から優先順位付けており重みから被害額を得るようにすることもできる [50]. 永井らはシステムの停止時間から被害額を導く式を提案しており [51]，大学における情報セキュリティインシデントの被害額を定量化している [52].

3. 2 全社レベルの 3 次対応

組織内でインシデントが発生した場合, デルタ ISMS では, 従来の ISMS 規定 [17]の「10.1 不適合及び是正処置」に規定されている 1 次対処と 2 次処置を実施した後, 本研究で提案する 3 次対応までを行う．なお，1 次対処と 2 次処置がインシデント発生部門にて実施されるのに対し，3 次対応は情報セキュリティ統括組織で定期的におよび重大な変化が発生した時に行われる．

- 1 次対処（発見された不具合の対処）
  - 不具合を管理（記録，報告，評価）する．
  - 不具合を修正するための処置をとる．
  - その不適合によって起こった結果に対処する．
- 2 次処置（不適合の原因を除去するための処置）
  - レビューする．
  - 原因を明確化する（分析，解析する）．
  - 類似の不適合の有無，又はそれが発生する可能性を明確にする．
  - 是正処置する（将来起こる可能性又はその影響を低減する）．
  - 有効性をレビューする．
- 3 次対応（組織全体としての対応）
  - インシデント発生部門にて発生した不具合から，その不具合に関する組織全体の潜在リスクを想定し，SLE（単一損失予想額）と ARO（年間損失発生確率）を算出する．
  - SLE，ARO，ALE よりリスクの扱いを決める．

SLE と ARO を正確に評価することは困難である．そこで，一般に，おおよその SLE と ARO を組織に合った段階で評価することが多い．

NIST 推奨の方法は，各脅威の ALE を以下のように近似計算してリスク値を算出して評価する [53].

$$\mathrm{ALE} = \frac{10^{(P+V-3)}}{3}$$

『ここで,

予想発生頻度；P

300 年に 1 回なら　　P=1

30 年に 1 回なら　　P=2

3 年に 1 回なら　　P=3

100 日に 1 回なら　　P=4

10 日に 1 回なら　　P=5

1 回当たりの予想損失額；V

10 円なら　　V=1

100 円なら　　V=2

1000 円なら　　V=3

1 万円なら　　V=4

10 万円なら　　V=5

100 万円なら　　V=6

1000 万円なら　　V=7

1 億円なら　　V=8

例えば，3 年に 1 回の発生頻度で予想損失額が 10 万円の脅威であれば,

ALE＝ $\frac{10^{(3+5-3)}}{3}$ = 33,333（円/年）．』

なお，3 年で 10 万円なら 10 万円÷3 でも同様に 33,333（円/年）となる．乗数を 3 引き，全体を 3 で割っているのは 1 年＝300 日と近似している為である．

他に，GMITS 方式は，資産価値×脅威×脆弱性によりリスクを計算評価する [54].

中村らは，SLE を「1～10 万円，11～100 万円，101～1000 万円，1001 万～1 億円，1 億

円以上」と区分し，ARO を「数十年に一度，数年に一度，年間 1 件程度，年間数件，年間数十件」と区分している [37] [40]．3 次対応においても中村らの方法を採ることができる．本稿では，ALE は SLE×ARO であり，計算をする時は，それぞれの値の中間値を用いる．

3. 3 デルタ ISMS 表

情報セキュリティ統括組織は，n+1 巡目の PDCA サイクルの Plan のフェーズでインシデントデータベースを精査し，n 巡目の PDCA サイクルの Do のフェーズ中で発生したインシデント群に対する対策候補を俯瞰することによって，全組織として新たに採用すべき対策の候補を選択する．

インシデント原因と対策は多対多の関係にある．対策の選択は脆弱性を下げることにより予想損失額を低減できる．最適な対策の選択のためには，対策コストの積み上げとその効果である損失低減額の積み上げを比較する必要がある．このため，デルタ ISMS では「デルタ ISMS 表」というインシデント原因と対策のマトリクスを作成する．

表 13 がデルタ ISMS 表である．ここで，

・L_jP_j：そのインシデント原因の年間予想損失額.

・R_{ji}：その対策により低下する ALE 軽減率（0%～100%）.

・F：安全係数（安全を重視するか，コストを重視するかの係数．詳細は 3．5 節参照）.

・S_i：各対策の有無（0 or 1）.

・C_i：対策のコスト.

である.

表 13　デルタ ISMS 表

インシデント原因	ALE	対策 1 の投資コスト(S_1C_1)	対策 2 の投資コスト(S_2C_2)	・・・	対策 i の投資コスト(S_IC_I)
1	L_1P_1	R_{11}	R_{12}	・・・	R_{1I}
2	L_2P_2	R_{21}	R_{22}	・・・	R_{2I}
・	・	・	・	・	・
・	・	・	・	・	・
・	・	・	・	・	・
J	L_JP_J	R_{J1}	R_{J2}	・・・	R_{JI}

Act の段階で，インシデントデータベースの「インシデント内容」＋「インシデント原因」，「1 次対処の被害額」，「2 次処置」及び「2 次対処の対策コスト」をデルタ ISMS 表の「インシデント原因 $_j$」，「ALE$_j$」，「対策 $_i$」及び「投資コスト $_i$」へそれぞれ転記する（図 37）．

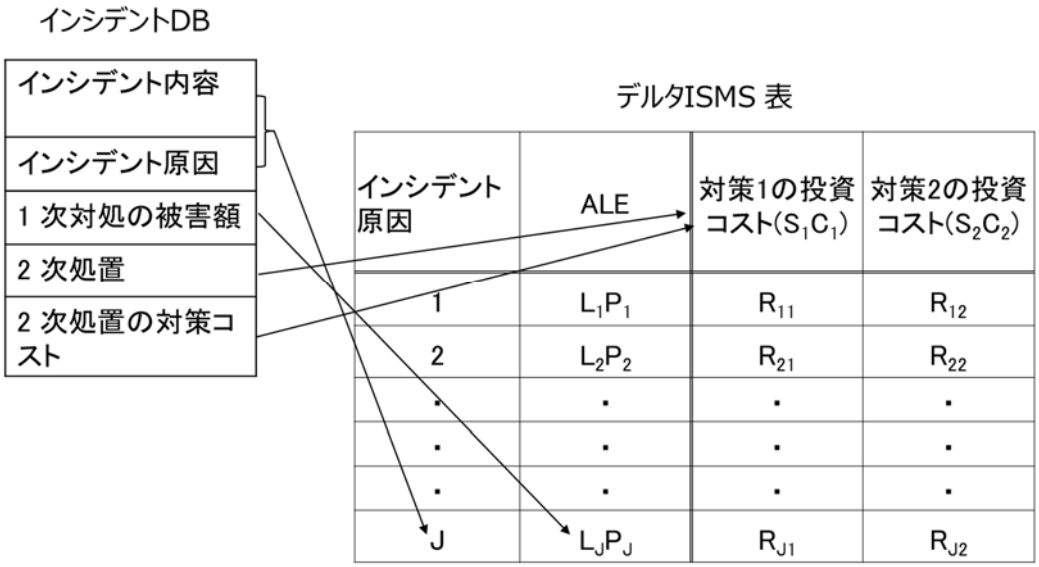


図 37　インシデント DB からデルタ ISMS 表へ

3．4　定式化

デルタ ISMS で使用するインシデントベースのリスクアセスメントにおいてもっとも投資効果の高い対策の選択は，式 2 の値 $E_{◿}$が最も大きくなる対策の選択として表される．式 2 の定式化は，中村らの手法 [37] [40]を参考としている．

式 2：

被害低減額

$$E_{◿} = F \times \sum_j \left\{ L_j P_j \left(1 - \prod_i (1 - R_{ji} S_i) \right) \right\} - (1 - F) \times \sum_i C_i S_i$$

対策後低減率　　対策コスト

表 13 より、対策を行った場合の組織全体として被害低減額を算出する．対策 i の実施によって，インシデント原因 j に関する被害低減率は R_{ji} であり，実施後の被害額は（1-R_{ji}）倍にな

る．すなわち、対策 i を選択するか否かのフラグ S_i を用意し，S_i=1 により，対策 i の選択、S_i=0 により対策 i の非選択を表すと，被害額は次となる．

$$L_j P_j(1 - R_{ji} S_i)$$

インシデント原因に関する被害額を低減できる対策は i だけでなく，すべての対策（1≦i≦I）それぞれが R_{ji} の割合でインシデント原因に関して被害額を低減させる．対策の相関関係は考慮の対象から外すことにし，各対策による効果が単純に相乗されると仮定するならば，すべての対策案の選択／非選択により，全対策による被害額は次式のように減少する．

$$L_j P_j \left(\prod_i (1 - R_{ji} S_i) \right)$$

これにより，インシデント j の全対策による被害低減額は元の被害額から全対策後の被害額を減じた次の値となる．

$$L_j P_j \left(1 - \prod_i (1 - R_{ji} S_i) \right)$$

対策は次の 3 種に区別できる．

・組織全体に対して既に適用している対策
・2 次処置で適用した組織に部分的に適用した対策
・組織に未適用の対策

情報セキュリティ統括組織は，デルタ ISMS 表と式 2 を用い，インシデント発生部署に対して 2 次処置で適用した対策の中から，組織全体に適用したほうが良いと考えられる対策を選定する．その際，JIS Q27002:2014 [34]，米国国立標準技術研究所の NIST SP800-53 [55]または JNSA の対策マップ [56]といった情報セキュリティ対策集を参考にしながら，対策の導入コストと効果に応じて対策候補の案を複数導出する．FTA 等付録 1 にて紹介した手法で対策を案出することもできる．なお，ここでの対策案はリスクの保有，リスクの回避およびリスクの共有 [10]を含めて検討する．

デルタ ISMS 表を用いた投資効果の計算の例を図 38 に示す．図 38 において対策 2（ストラップの導入：導入コスト 30 万円）を選択した場合，携帯電話紛失と USB メモリ紛失のリ

スクに対して各 30%の改善により, 損失低減額は各 750 万円, 75 万円となる. 実際の計算は, I 個の対策の有無を全て列挙すると 2^I 個のケース（組合せ）が得られ，2^I 個の式 2 の値の中から値が最大である組合せが最適解となる．なお，図 38 のコストと ALE は，企業規模，業態，物価などにより変化し得る．

	対策	対策1	対策2	・・・	対策i
		設定変更	ストラップ	・・・	暗号化ソフト
インシデント原因	コスト / ALE	300万円	30万円	・・・	400万円
メール誤送信	2500万円	30%	0%	・・・	15%
携帯電話紛失	2500万円	0%	30%	・・・	0%
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・・・	・ ・ ・
USBメモリ紛失	500万円	0%	30%	・・・	40%

図 38　対策選択による ALE の低減の例

3. 5 安全係数

安全係数 F とは，被害低減額と対策コストの重みを変動させる係数であり，値を変動させることで複数の最適解を得ることができる．安全係数 F を大きくすると対策コストよりも安全を重視する対策群を導出することができ，安全係数 F を小さくすると対策コストを重視して最低限の安全を得る対策群を導出することができる．安全係数 F を 0.9～0.1 まで 0.1 刻みで変動させて 9 個の対策案を導出し，パターン別に 3 個導出する．導出された 3 案をコストの高い順に並べ，それぞれ金銀銅と呼ぶ.

対策による被害額の低減率は，選択された対策が複数ある場合，対策間での相関が発生することもあり，高い精度で設定することは難しい．そこで，安全係数の考え方を用いて，精度不足をカバーすることができる.

本研究では, 選択案を求めるに当たって, 次のアルゴリズムを採用することとする. ただし, このアルゴリズムは単に経験的に得たものであり，このアルゴリズムの根拠の明示や更なる洗練化の検討が今後，必要である.

パターンは 1～9 パターン現れる.

パターン数が 4 個以上の場合は，F=0.5 を銀として，上下に最初に現れる別パターンをそれぞれ金と銅とする．ただし，F=0.5 より上（下）に別パターンが現れないときは， F=0.5 を金（銅）として，下（上）に 2 パターン，銀と銅（金）を割り当てる.

パターン数が 3 個の場合はそれらをコストの高い順に金銀銅とし，パターン数が 2 個の場合はそれらを金銀とし，パターン数が 1 個の場合はそれを金とする．パターン数が 2 個以下の場合は，適切な対策を追加し再計算することによって，パターン数を増やすこともできる．

3. 6 経営陣への 3 パターンの対策案の提示

情報セキュリティ統括組織は，次巡目の Plan の際に，前節によって選定された組織全体のセキュリティ対策の改善案を CISO 等に提示する．CISO 等は，デルタ ISMS 表と式の計算結果を「対策を追加したり改定を採用したりするかどうかを判断するための情報」や説明材料として利用し対策を経営戦略に合致した形で決定し，CISO 対策を取締役会等で経営陣に説明する．この結果，組織全体の情報セキュリティマネジメントが改善され，経営陣の情報セキュリティリスク管理に対する認識も向上し，組織の ISMS に対する監視サイクルが実質的に機能するようになる．その組織がセキュリティインシデントの発生を公表した後などは，セキュリティ対策を重視していることをアピールする目的でコストより安全を重視する場合もあるし，経営上のコスト低減が必須な場合は，安全よりコストが重視される場合もある．選択が複数あると，経営陣や CISO は決定を下しやすく，また，選択活動を通して理解を深めることが期待できる．

3. 7 まとめ

本章では，本研究で提案するデルタ ISMS モデルをその特徴的構成要素であるインシデントデータベース，3 次対応，デルタ ISMS 表，定式化，安全係数及び経営陣への 3 パターンの対策案の提示を詳説した．

図 39 に，デルタ ISMS の繰り返しによる獲得できる組織のセキュリティ強度のスパイラルアップを示す．インシデントデータ（デルタ ISMS 表）の前巡比較（差分）に注目することにより，ISMS の継続的改善のために重要となる「複数巡回におけるインシデントデータのトレンドの観察」も容易となり，隠れたインシデントの洗い出しから，組織特有のインシデント原因の把握が可能となり，根本的なセキュリティ対策の実施が可能となる．

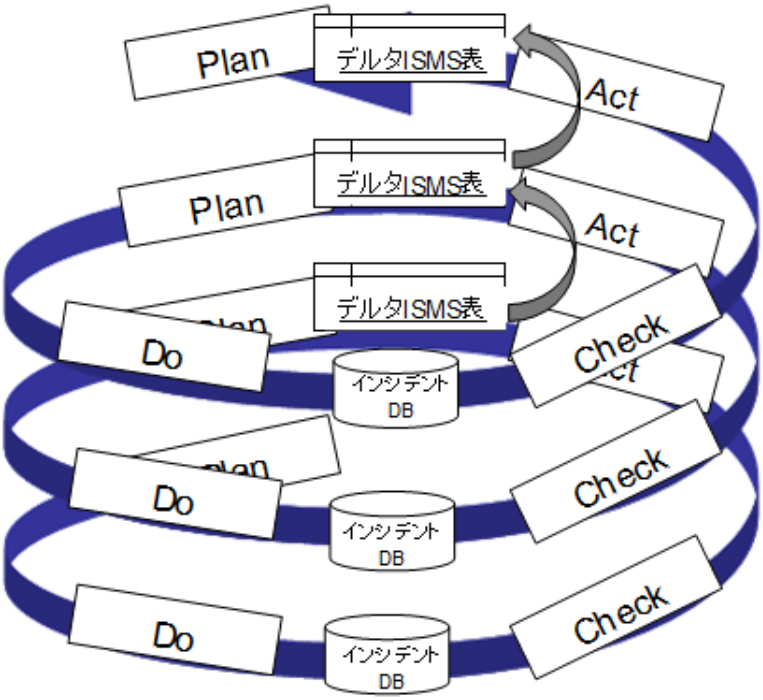


図 39　デルタ ISMS モデルの繰り返し

第4章　評価

本論文のような研究の場合，実組織での比較実験が行えない．このため，本章では，以下の3種の評価でもって本研究に対する評価とする．まず，デルタISMS手法が，対策選定のノウハウのない人でも定式化された手順に従い対策選定が行え，エキスパートと同様の対策選定ができることを，二つのケーススタディを通じて示す．一つ目のケーススタディは，偶発的なインシデントが発生した場合のISMSの改善である．軽微な偶発的インシデントは多数発生しているので，実組織の過去データを用いたケーススタディを行う．二つ目のケーススタディは，意図的インシデントが発生した場合のISMSの改善である．意図的インシデントに対する対策を公表することは，当該組織やシステムの弱点を公表することになるため，対策が公表されることはない．このため，標的型攻撃対策を実施する仮想の組織を想定してケーススタディを行う．次に，デルタISMS手法が橋渡し人材に求められる役割を手順化していることを，情報セキュリティガバナンス導入ガイダンスのモニタリング項目とデルタISMSの処理対象を比較することによって示す．

ここで再度，偶発的インシデントと意図的インシデントの比較を示す（図 40，図 41）．

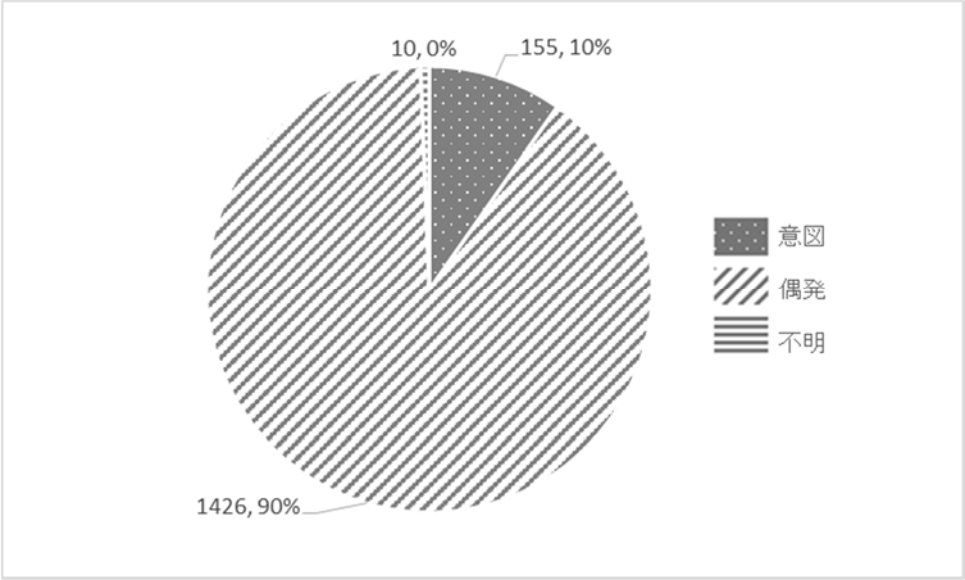


図 40　原因別個人情報漏えい件数（ [13]を元に作成）

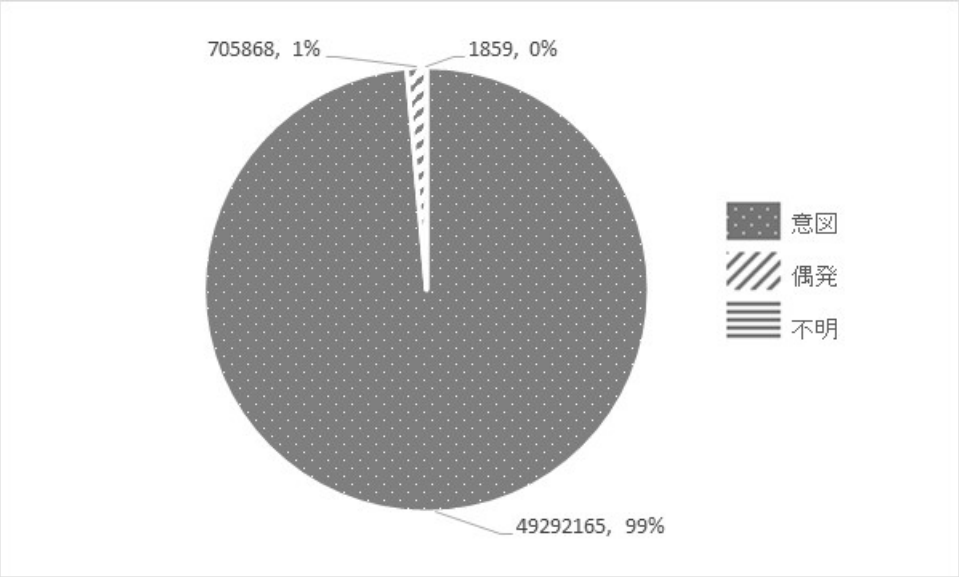


図 41　原因別漏えい人数（ [13]を元に作成）

偶発的インシデントの発生頻度は高く，実データは比較的入手しやすい．そこで，実組織の過去データを用いてケーススタディを行う．一方，意図的インシデントの発生頻度は低く，実データは入手しがたいため，仮想の組織を想定してケーススタディを行う．

4．1　　実組織の過去データを用いたケーススタディ

ISMS 認証を取得している従業員数約 800 名のある組織（資産数 : 6,600，脅威数×脆弱性 : 250）において，実際のインシデントデータ（2013 年度のインシデント数 : 30）から提案方式を用いて対策の改善を導出する手順を後追いで適用した．

4.1.1　　インシデントデータベース

インシデントデータベースのサンプルを表 14 に示す．

表 14　インシデントデータベースのサンプル（部分）

日時	インシデント内容	インシデント原因	インシデント経路	1次対処の被害額	影響範囲	2次処置の対策コスト
4月3日	帰宅時に電車の網棚においたカバンから紛失	紛失	携帯電話	25万円	事故	6万円（MDM）
5月4日	洗面所で胸ポケットに入れたカードが滑り出た模様	紛失	自社セキュリティカード	1万円	ヒアリハット	3万円（蓋つきケース）
6月5日	社外秘扱いの紙をプリンターの裏紙に使用していた	誤操作	紙資料	1万円	（実地検査による）ヒアリハット	1万円（規則変更）

2.1.1ISMS 認証取得事業所へのアンケートで述べた「入館証や携帯電話の紛失」というインシデントが減らないという状況は，この組織でも発生しており，ここでは，入館証や携帯電話の紛失を中心にサンプルを示す.

4.1.2 デルタ ISMS 表

デルタ ISMS 表のサンプルを表 15 に示す.

表 15 デルタ ISMS 表のサンプル

		対策済									
	対策	1 使用前ロックを設定する	2 履歴を残さない設定にする	3 毎持ち出し時には許可制とする	4 連絡先を貼りつける	5 蓋つきフォルダーに入れる	6 ストラップを付ける		7 移動する度にチェックリストでチェックする	8 遠隔データ初期化サービスを利用する	9 毎月定期確認する
	コスト(万円)	100	50	80	20	20	30		600	240	45
インシデント	ALE										
携帯電話紛失	2500万円	0.3	0.3	0.2	0.1	0	0.3		0.3	0.4	0.06
セキュリティカード紛失	2500万円	0	0	0	0.1	0.3	0.3		0.3	0	0.06
紙資料紛失	500万円	0	0	0.2	0	0	0		0.3	0	0

表 15 のデルタ ISMS 表の最左列の「インシデント」は，表 14 のインシデントデータベースにおいてインシデント経路とインシデント原因が同一のものをまとめている. 上部の「対策」には，インシデントに対する対策案の候補が列挙されている．この内，対策 1～6 は，当該組織で既に実施中の対策である．対策 7～9 は，インシデントデータベースにあるインシデント発生部門で実施した対策やインシデント原因などを参考に案出した追加対策である.「コスト」には，各対策に必要な年間予算を記入している.「ALE」は，インシデントデータベースの 1 次対処の実績被害額を加算することで算出できる.

インシデントが発生する前（Plan フェーズ）のリスク分析においては，当該組織内にて実際にインシデントがどれくらいの頻度で発生し，その結果どれくらいの額の実被害かを正確に予測することは難しい．これに対し，デルタ ISMS 表においては，組織内で実際に発生したインシデントが並べられるので，現実の数値を用いての評価が可能である．同様に，インシデントが発生する前のリスク分析においては，インシデントの原因としては一般的な事例を想定することしかできないため，類型的な対策を挙げることしかできない．これに対し，デルタ ISMS 表においては，組織内で実際に発生したインシデントが並べられるので，具体的なインシデント原因を究明することが可能であり，そこから導出される対策はその組織に真に必要な対策となる．このように，デルタ ISMS では情報セキュリティ対策を組織の実態にあわせてチューニングしていくことができる．

4.1.3 3 パターンの対策案

表 15 のデルタ ISMS 表 に対してデルタ ISMS 式を用いて離散最適解を求めると，安全係数を 0.9 から 0.1 まで 0.1 刻みで振ることで，9 個の追加対策を得ることができる．

表 16 過去データに対する 9 個の対策案

F 値	追加対策	追加コスト（万円）	パターン
0.9	7,8,9	885	
0.8	7,8,9	885	
0.7	7,8,9	885	
0.6	7,8,9	885	金
0.5	7,9	645	銀
0.4	9	45	銅
0.3	-	0	
0.2	-	0	
0.1	-	0	

追加対策には，（7，8，9），（7，9），（9），（-）の 4 パターンが表れている．3．5 節で提案したアルゴリズムにより，F=0.5 の（7，9）が銀，F=0.6 の（7，8，9）が金，F=0.4 の（9）が銅となる．選定の結果を表 16 に示す．CISO（場合により経営陣）へ提示する 3 パターンの対策候補案は表 17 となる．このようにデルタ ISMS では自動的に再現性をもって 3 組の対策案を得ることができる．CISO や経営陣は経営方針や経営状況を考慮しながら，金銀銅の 3 パターンから追加対策を選択することができる．

表 17　3 パターンの対策案

パターン	追加コスト	対策	F 値	低減率（%）
金	885 万円	7,8,9	0.6	77.3
銀	645 万円	7,9	0.5	74.3
銅	45 万円	9	0.4	63.3

銅パターンの対策 9 は，安価ではありながらコスト対効果が高く，予算の余裕がない場合などに，重点対策として選択しえる．銀パターンは，対策 9 に対策 7 を追加することであり，確認の頻度を高めることで更なる効果が期待できる．金パターンは更に対策 8 を加えることで紛失防止に加えて，紛失時の被害額削減の効果を加えられる．金パターンは，対策実施時に従業員を含めた全てのステイクホルダーに「現時点で採り得る全ての対策を実施する」というメッセージを付加することで企業の取り組み姿勢を表明することもできる．

今回のケーススタディの対象とした実組織では，CISO は，対策 9 のみを選択し，経営陣は経営方針や経営状況を背景に，CISO の対策選択を承認し，対策 9 が追加実施されることとなった．これは，表 17 の銅パターンと同一である．

このように，デルタ ISMS の対策選定が実組織のエキスパートによる対策選定と合致し，デルタ ISMS 手法では対策選択のノウハウのない人でも定式化された手順に従いスムーズに選定が行え，実組織のエキスパートと同様の対策選定ができることを示すことができた．

なお，入館証や携帯電話の紛失の発生を減じる対策の追加調査を付録 3 に示す．

提案方式が実際の組織でどの程度効果がありそうかを，従業員数約 3 万人のある組織の情報セキュリティ統括組織の長にインタビューした．情報セキュリティ統括組織の長より「第 3 章に記載のある手順の流れは実務上妥当である．業務を手続きとして定めておくことは検討抜け防止や作業結果の再現性の観点から有効である．実際，記載されている手順群は部分的には実施している．実施できていない部分についても実施する意義を認めるので，実施に向けて検討していきたい」とのコメントを得られた．

また，本内容を 2016 年 8 月 25 日，日本セキュリティ・マネジメント学会，IT リスク学研究会に発表することでセキュリティ専門家の方々に紹介した．終了後，多くの意見を得たが，参加者の約半数から，「得心の行く手法である」と評価いただけた．

4. 2　標的型攻撃対策のケーススタディ

本節では，ある A 社を想定し，オーストラリアの国防総省（DSD）の選択した標的型攻撃対策の公表を受けて，自社は大丈夫かと自社の実施済対策と比較して確認するケーススタディを示す．オーストラリアの国防総省（DSD）は実インシデントを統計解析して対策集を公表しているが，実インシデント情報そのものは公開していないため，想定実験となる．A 社は，実施中のセキュリティ対策に追加すべき対策はないかをデルタ ISMS の手法を用いて確認するというシナリオを示す. 実際には本シナリオを基にした細かな調整項目が存在する. 調整項目とは，例えば運用状況，実製品の機能やコスト，対策の関連付け等であり，これらは，個々の組織によって変動する．ここではベースシナリオの提供を目的とする．

4.2.1　想定する会社

FireEye はアジアにおける標的型攻撃が政治的，経済的，軍事的なサイバースパイ活動であり，ハイテクや金融サービスへの攻撃が多いことを示した [57]．標的攻撃の手口はたとえば，Hatta ら [58]や Caselden ら [59]に見ることができる．

ある A 社を想定し，今，2015 年 2 月 1 日とする．A 社は IT 系のハイテク企業であり，社員数 1000 名である． A 社はネットワーク事業部，データセンター事業部及びシステムインテグレート事業部の 3 個の事業部から成る．ネットワーク事業部では公共系のネットワーク（社会インフラの）の設計・敷設も行っている．なお，A 社は ISO27001 の認証を取得しており，ISO27002 の対策をすべて実施している．A 社ではリモートアクセスできる社員をできるだけ制限している．主にマネージャと外勤の多い社員である 250 名がリモートアクセスできる．

A 社の端末数は 1250 台，サーバ数は 100 台である．A 社の通信施設は共通部門である情報システム部が一括管理しているが，事業部内のサーバ，端末は各事業部で管理している．ネットワーク事業部の社員数は 250 名であり，ネットワーク事業部は 320 台の端末と，5 台のサーバを持つ.

2014 年にオーストラリアの国防総省（DSD）が標的型サイバー攻撃に有効な対策集を公表したのを受けて，A 社では標的型サイバー攻撃の被害をシミュレートし，DSD の対策集から追加すべき対策を検討することとした.

4.2.2　1 次対処

2015 年 2 月 1 日にセキュリティ監視会社からの警告により，不審通信が観察され，その発信源を特定し，遮断，1 次対処を実施したこととする.

1 次対処までの報告をインシデントデータベースの形式で表 18 に示す.

表 18　インシデントデータベース

項目	内容
日時	2015 年 2 月 1 日
インシデント内容	情報漏えい
インシデント原因	ワーム・ウイルス
インシデント経路	インターネット
1 次対処	2 月 1 日にセキュリティ監視会社からの警告により，不審通信が観察され，その発信源を特定し，遮断した

4.2.3　2 次処置

フォレンジック調査の結果，標的型攻撃により，社会インフラに係る機密情報が漏えいしたことが判明した.

機密情報の被害額は 10 億円（$10M）と見積られた．同様の情報漏えいインシデントでそれを超える事例も報告されている．例えば，2008 年のシカゴのハイテク企業での情報漏えいの被害額は，内部犯行であるが，600 億円($600M)の損失が試算されている [60] [61]．このため，この見積額は決して過大ではない.

今回の攻撃が標的型攻撃であることが判明したため，その対策を調査したところ，オーストラリアの国防総省（DSD）による標的型攻撃対策集に行き当たった [62] [63]．サイバーセキュリティを担当する諜報機関である DSD は，最も効果的で最も頻繁に行われた標的型攻撃を調査し，最も頻繁な標的型攻撃が成功した理由を分析した． 他の調査の報告と同様に，彼らは大部分の成功した標的型攻撃が基本的な脆弱性を悪用していることを発見した． これにより，頻度と成功率によって脆弱性をランク付けした． DSD は，これらの脆弱性を緩和することで，攻撃者の成功率が大幅に低下することを発見した．そして，DSD はその分析の情報を使用して

35 の対策のリストを作成した． 対策は効果のランキング順に並べている．DSD は，オーストラリア政府の 2012 年の標的型攻撃に関するインシデントの分析に基づいて，どの対策が標的型攻撃を防止できるかを調べた. その結果, 最初の 4 つで, 85%以上を防止できることが判り，この 4 個の効果を Essential と置いた [64].

35 個の対策を効果，初期コスト，運用コストと共に表 19 に示す．なお，コストは High, Medium，Low で区分されているが，定量的な数値は提供されていない.

表 19　DSD の 35 個の対策 [62]

番号	対策	効果	初期コスト	運用コスト
1	アプリケーションのホワイトリスト	Essential	High	Medium
2	アプリケーションのパッチ	Essential	High	High
3	オペレーティングシステムの脆弱性のパッチ	Essential	Medium	Medium
4	管理者権限の制限	Essential	Medium	Low
5	ユーザーアプリケーション構成の強化	Excellent	Medium	Medium
6	（サンドボックスを用いた）自動ダイナミック解析	Excellent	Medium	Low
7	オペレーティングシステムの一般的なエクスプロイトの軽減	Excellent	Medium	Low
8	ホストベースの侵入検知/防御システム	Excellent	Medium	Medium
9	ローカル管理者アカウントの無効化	Excellent	Medium	Low
10	ネットワークのセグメンテーションと分離	Excellent	High	Medium
11	マルチファクタ認証	Excellent	High	Medium
12	ソフトウェアベースのアプリケーションファイアウォール（着信のブロック）	Excellent	Medium	Medium
13	ソフトウェアベースのアプリケーションファイアウォール（発信のブロック）	Excellent	Medium	Medium
14	非永続仮想化サンドボックス・トラステッド・オペレーティング環境	Excellent	High	Medium
15	成功したおよび失敗したコンピュータイベントの集中型および時間同期型のロギング	Excellent	High	High
16	許可されたネットワークアクティビティとブロックされたネットワークアクティビティの集中管理と時間同期ロギング	Excellent	High	High
17	メールコンテンツのフィルタリング	Excellent	High	Medium

18	Web コンテンツのフィルタリング	Excellent	Medium	Medium
19	すべてのドメインの Web ドメインホワイトリスト	Excellent	High	Medium
20	偽の電子メールのブロック	Excellent	Low	Low
21	ワークステーションとサーバの構成管理	Good	Medium	Low
22	次世代型アンチウイルスソフトウェア	Good	Low	Low
23	ワークステーションからの直接インターネットアクセスの拒否	Good	Low	Low
24	サーバプリケーション構成の強化	Good	High	Medium
25	強力なパスフレーズポリシーの適用	Good	Medium	Low
26	取り外し可能でポータブルなメディアコントロール	Good	Medium	Medium
27	サーバメッセージブロック（SMB）と NetBIOS へのアクセス制限	Good	Medium	Low
28	ユーザ教育	Good	High	Medium
29	Microsoft Office ファイルのワークステーション検査	Good	Low	Low
30	シグネチャベースのウイルス対策ソフトウェア	Good	Low	Low
31	電子メールサーバ間の TLS 暗号化	Good	Low	Low
32	IP アドレスでウェブサイトへのアクセスのブロック	Average	Low	Low
33	ネットワークベースの侵入検知/防御システム	Average	High	High
34	ゲートウェイブラックリスト	Average	Low	High
35	ネットワークトラフィックのキャプチャ	Average	High	Low

A 社は ISO27001 を取得しており，ISO　27002 の対策をすべて実装していたので，いくつかの対策は本検討前から実施済であった．表 20 に DSD の 35 個の対策と実施済である ISO 27002 の対策の対応を示す. 列 27002 に記載のないものは, 未実施であり, 追加の対策となる.

なお，ここでは DSD の対策と ISO27002 の対応表の作成を人手で実施したが，高橋らのシステムを利用すれば機械的に対応付けを行うことができる [65] [66] [67] [68].

表 20　DSD の対策と 27002 の対策との対応

番号	DSD の対策	27002	27002 の対策
1	Application whitelisting	12.2.1b	Implementing controls that prevent or detect the use of unauthorized software - e.g. application whitelisting

2	Patch applications	12.6.1f	If a patch is available from a legitimate source the risks associated with installing the patch should be assessed.
3	Patch operating system vulnerabilities	12.6.1f	If a patch is available from a legitimate source the risks associated with installing the patch should be assessed.
4	Restrict administrative privileges	9.2.3	Management of privileged access rights
5	User application configuration hardening	12.6.2	Restrictions on software installation
6	Automated dynamic analysis(sandbox)	-	-
7	Operating system generic exploit mitigation	-	-
8	Host‐based Intrusion Detection/Prevention System	13.1.2	Security of network services
9	Disable local administrator accounts	9.2.3	Management of privileged access rights
10	Network segmentation and segregation	13.1.3	Segregation in Networks
11	Multi‐factor authentication	-	-
12	Software‐based application firewall, blocking incoming network traffic	13.1.2	Security of network services
13	Software‐based application firewall, blocking outgoing network traffic	13.1.2	Security of network services
14	Non‐persistent virtualised sandboxed trusted operating environment	-	-
15	Centralised and time‐synchronised logging of successful and failed computer events	12.4.1	Event logging
16	Centralised and time‐synchronised logging of allowed and blocked network activity	12.4.1	Event logging
17	Email content filtering	-	-
18	Web content filtering	12.2.1c	Implementing controls that prevent or detect the use of known or suspected malicious websites - e.g. blacklisting
19	Web domain whitelisting for all domains	9.1.2	Access to networks and network services
20	Block spoofed emails	-	-

21	Workstation and server configuration management	12.6.2	Restrictions on software installation
22	Antivirus software using heuristics and automated Internet‐based reputation ratings	-	-
23	Deny direct Internet access from workstations	-	-
24	Server application configuration hardening	12.6.2	Restrictions on software installation
25	Enforce a strong passphrase policy	9.3.1	Use of secret authentication information
26	Removable and portable media control	8.3.1	Management of removable media
27	Restrict access to Server Message Block (SMB) and NetBIOS	-	-
28	User education	7.2.2	Information security, awareness, education and training
29	Workstation inspection of Microsoft Office files	-	-
30	Signature‐based antivirus software	12.2.1g	Installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis
31	TLS encryption between email servers	13.2.1f	Use of cryptographic techniques to protect the confidentiality, integrity and authenticity of information
32	Block attempts to access websites by their IP address	-	-
33	Network‐based Intrusion Detection/Prevention System	13.1.2	Security of network services
34	Gateway blacklisting	13.1.1g	Systems connection to the network should be restricted
35	Capture network traffic	13.1.1d	Appropriate logging and monitoring should be applied to enable recording and detection of actions that may affect, or are relevant to, information security

追加の対策は，6，7，11，14，17，20，22，23，27，29，32 の 11 個である．このうちの

7，11，22，27，29 の 5 個は部門コンピュータ（サーバ，ワークステーション）での対策であり，インシデント発生事業部門で全ての対処をすませた．6，14，17，20，23，32 の 6 個は全社的な通信系の対策であったため，対応を情報システム部門に申し送りした．

対策コストは商用の製品・サービスの価格や作業人工の見積もりにより得ることができる．表 21 にネットワーク部門における対策コストを示す．人工は 1 人月を 50 万円と置いた．

表 21　部門における対策コスト

番号	対策	初期コスト	初期コスト（万円）
7	オペレーティングシステムの一般的なエクスプロイトの軽減	Medium	310
11	マルチファクタ認証	High	320
22	次世代型アンチウイルスソフトウェア	Low	300
27	サーバメッセージブロック（SMB）と NetBIOS へのアクセス制限	Medium	300
29	Microsoft Office ファイルのワークステーション検査	Low	150

A 社の対応部門からのインシデント報告を表 22 に示す．なお，インシデント報告は単に再発防止が十分であることだけを示すだけでなく，デルタ ISMS の考え方に基づき，部門で実施した対策を全社的に展開することを示唆する項目も記載しなければならない．ここでは申し送り事項に記載した内容がそれに相当する．

表 22　インシデントデータベース（2 次処置）

項目	内容
影響範囲	深刻なインシデント
被害額	漏えいした機密情報の価値を 10 億円（$10M）と評価
2 次処置	感染端末のフォレンジック調査の結果，機密情報の漏えいが発覚した. DSD の 35 個の標的型攻撃対策の内，24 個の対策は実施済であったので，再度，実施の抜けがないかを確認すると共に，未実施の次の 5 項目を再発防止として導入し実施した. ＜実施した対策＞ 7　オペレーティングシステムの一般的なエクスプロイトの軽減. 11　マルチファクタ認証. 22　次世代型アンチウイルスソフトウェア. 27　サーバメッセージブロック（SMB）と NetBIOS へのアクセス制限. 29　Microsoft Office ファイルのワークステーション検査. 3 月 10 日より通常業務を再開した.
申し送り事項	次の 6 項目は全社的な通信系の対策であり，情報システム部門へ実施を依頼した. 6　（サンドボックスを用いた）自動ダイナミック解析. 14　非永続仮想化サンドボックス・トラステッド・オペレーティング環境. 17　メールコンテンツのフィルタリング. 20　偽の電子メールのブロック. 23　ワークステーションからの直接インターネットアクセスの拒否. 32　IP アドレスでウェブサイトへのアクセスのブロック.
2 次処置の対策コスト	5 項目の実施に対して 1380 万円（$1,380,000）.

4.2.4　3 次対応

3 次対応が通常は定期的に実施されるが，深刻なインシデントが発生した場合は必要により臨時に実施することとなる．今回は深刻なインシデントに相当するという判断がなされ，2 次処置終了の時点で引き続き 3 次対応が実施されることになった. 情報セキュリティ統括組織は，デルタ ISMS 表を参考にしながら，対策の導入コストと効果に応じて対策候補の案を複数選出する．

インシデントデータベースを元にデルタ ISMS 表を構成する方法は以下のとおりである．まず，インシデントデーベースのインシデント内容欄に情報漏えい，被害額欄に 10 億円と記載されていることから，デルタ ISMS 表のインシデント名と ALE にそれらを転記する．次に，今回選択した追加の 11 個の対策の番号，対策名を表 19「DSD の対策」より転記する．既存対策は規格上外さないため，今回は追加対策が選択の解析対象となる．

次に各対策のコストを求める．対策コストは 2 次と同様に，対応製品・サービスの価格や作業人工の見積もりによる．表 23 に 3 次対応の対策コストを示す．人工においては 1 人月を 50 万円と置いた．対策コストは初期コストと運用コストの和とする．なお，この表は「表 21　部門における対策コスト」と異なり全社での対応コストとなる．表 23「3 次対応のコスト」の合計コストの値をデルタ ISMS の対策コストに転記する．

表 23　3 次対応の対策コスト

番号	対策	初期コスト	運用コスト	初期コスト（万円）	運用コスト（万円）	合計コスト（万円）
6	（サンドボックスを用いた）自動ダイナミック解析	Medium	Low	1800	200	2000
7	オペレーティングシステムの一般的なエクスプロイトの軽減	Medium	Low	1000	500	1500
11	マルチファクタ認証	High	Medium	900	500	1400
14	非永続仮想化サンドボックス・トラステッド・オペレーティング環境	High	Medium	2500	1300	3800
17	メールコンテンツのフィルタリング	High	Medium	200	100	300
20	偽の電子メールのブロック	Low	Low	200	100	300
22	次世代型アンチウイルスソフトウェア	Low	Low	500	600	1100

23	ワークステーションからの直接インターネットアクセスの拒否	Low	Low	500	500	1000
27	サーバメッセージブロック（SMB）と NetBIOS へのアクセス制限	Medium	Low	1000	500	1500
29	Microsoft Office ファイルのワークステーション検査	Low	Low	400	500	900
32	IP アドレスでウェブサイトへのアクセスのブロック	Low	Low	500	500	1000

最後に，マトリックの本体に ALE の低減率を記載する．ALE 軽減率は，Essential を 0.38 とし， Excellent，Good，Average はそれぞれ半減させた 0.19，0.09，0.05 とする．この値は，Essential4 個の対策が 85%の被害が防げること拠り，次式より α=0.38 であることによる．

$$1-\left(1-\alpha\right)^{4}=0.85$$

構成したデルタ ISMS 表を表 24 に示す．表は横に伸びた表となるが，紙面の都合により途中で折り返して 2 段で示す．上段のすべてと下段の左から 6 個の対策 35 までは，既存の対策であり，今回の追加検討対策は，下段の対策 6 から対策 32 までの 11 個である．

表 24　デルタ ISMS 表

	No.	1	2	3	4	5	8	9	10	12	13	15	16	18	19	21	24	25	26
	対策	Application whitelisting	Patch applications	Patch operating system vulnerabilities	Restrict administrative privileges	User application configuration hardening	Host - based Intrusion Detection/Prevention System	Disable local administrator accounts	Network segmentation and segregation	Software - based application firewall, blocking incoming network traffic	Software - based application firewall, blocking outgoing network traffic	Centralised and time synchronised logging of successful and fail computer events	Centralised and time synchronised logging of allowed and block network activity	Web content filtering	Web domain whitelisting for all domains	Workstation and server configuration management	Server application configuration hardening	Enforce a strong passphrase policy	Removable and portable media control
インシデント	コスト(K$) / ALE	230	270	190	140	190	190	140	230	190	190	270	270	190	230	140	230	140	190
情報漏えい	$10M	0.38	0.38	0.38	0.38	0.19	0.19	0.19	0.19	0.19	0.19	0.19	0.19	0.19	0.19	0.09	0.09	0.09	0.09

	No.	28	30	31	33	34	35		6	7	11	14	17	20	22	23	27	29	32
	対策	User education	Signature - based antivirus software	TLS encryption between email servers	Network - based Intrusion Detection/Prevention System	Gateway blacklisting	Capture network traffic		Automated dynamic analysis(sandbox)	Operating system generic exploit mitigation	Multi - factor authentication	Non - persistent virtualised sandboxed trusted ...	Email content filtering	Block spoofed emails	Antivirus software using heuristics and automated Internet - based reputation ratings	Deny direct Internet access from workstations	Restrict access to Server Message Block (SMB) and NetBIOS	Worksiation inspection of Microsoft Office files	Block attempts to access websites by their IP address
インシデント	コスト(K$) / ALE	230	90	90	270	180	180		200	150	140	380	30	30	110	100	150	90	100
情報漏えい	$10M	0.09	0.09	0.09	0.05	0.05	0.05		0.19	0.19	0.19	0.19	0.19	0.19	0.09	0.09	0.09	0.09	0.05

表 24 のデルタ ISMS 表 に対してデルタ ISMS 式を用いて離散最適解を求めると，安全係数を 0.9 から 0.1 まで 0.1 刻みで振ることで，9 個の追加対策を得ることができる.

表 25　標的型攻撃に対する 9 個の対策案

F 値	追加対策	追加コスト（万円）	パターン
0.9	17,20	600	
0.8	17,20	600	金
0.7	20	300	銀
0.6	-	0	銅
0.5	-	0	
0.4	-	0	
0.3	-	0	
0.2	-	0	
0.1	-	0	

追加対策には，（17，20），（20），（-）の 3 パターンが表れている．3．5 節のアルゴリズムにより，F=0.8 の（17，20）が金，F=0.7 の（20）が銀，F=0.6 の（-）が銅となる．結果を表 25 に示す． CISO（場合により経営陣）へ提示する 3 パターンの対策候補案は表 26 となる．このようにデルタ ISMS では自動的に再現性をもって 3 組の対策案を得ることができる．CISO や経営陣は経営方針や経営状況を考慮しながら，金銀銅の 3 パターンから追加対策（追加の見送りを含む）を選択することができる．

表 26　3 パターンの対策候補案

パターン	追加コスト	対策	F 値	低減率（%）
金	600 万円	17,20	0.8	99.5
銀	300 万円	20	0.7	99.4
銅	0 万円	-	0.6	99.2

ISMS の附属書 A で規定された対策集は上位 4 対策を含み，加えて 20 個の対策が実施済である. 追加対策を行わない銅パターンでは, この計算による被害の防止率は 99.2%と高い. DSD は，過去のオーストラリア政府への標的型攻撃を分析し，上位 4 対策で 85%の被害が防げるとしている．そして，DSD がすべての組織へ上位 4 対策の実施を標的型攻撃に対する最低限の対策として推奨している．この観点から銅パターンが選択されることもあるであろう．

3 次対応では，追加予防を検討することになる．追加予防について，CISO は，効果やコストを経営陣に説明し，承認を得る必要がある．金パターン，銀パターンの追加対策は比較的安価であり，安価な対策は経営に与える影響は小さいため選択しやすい．また，全社的な対策を加

える続けることは，一般社員の情報セキュリティに対する意識や自覚を高める効果も期待できるため，銀パターンや金パターンが選択されることは十分考えられる．銀パターンである対策20の追加の結果，防止率は99.4%となり，金パターンである対策17,20の追加の結果，防止率99.5%となる．

これらの事象を紐解くと，対策選択のノウハウのない人でも定式化された手順に従いエキスパートと同様の対策選定がスムーズに行えることになる．

4．3　情報セキュリティガバナンス導入ガイダンスのモニタリング項目との比較

経済産業省の「情報セキュリティガバナンス導入ガイダンス [31]」のモニタリング項目とデルタISMSを比較する．

デルタ ISMS において，CISO 等はリスクアセスメントに使用したデルタ ISMS 表の情報（インシデント原因と対策の投資対効果）を経営陣に報告する．本節ではデルタISMS を従来の情報セキュリティガバナンスと比較し，違いを考察する．この比較は，デルタISMSの有効性を情報セキュリティガバナンスから見た効果を示すことを目的としている．

経営陣が検討しなければならない分野は情報セキュリティ分野にとどまらず広範なため，要点を絞った情報伝達が求められる．CISOはデルタISMS表を経営陣に報告するときに，対策効果の大きい対策や実施コストの高い対策に絞って報告することになる．ここでは，あるべき経営陣とCISOの共通語という観点からデルタISMS表と情報セキュリティガバナンスのモニタリング項目とを比較する．

経済産業省から公表された「情報セキュリティガバナンス導入ガイダンス」には，経営陣，CISO および管理者が行うモニタリング項目の例がモニタリング内容と指標例として 80 項目（重複を含む）記載されている．これらをグループ化すると15個のグループに分けることができた．

そしてグループ15 項目の関連を図 42 に示す．このうち経営陣と CISO が共にモニタすべき項目は円が重なる部分の 4 項目である．これらの中でデルタ ISMS 表がカバーする 2 項目を下線で示す．これにより，デルタ ISMS 表が提供する情報が CISO と経営陣の間での共通語であることを見ることができる．つまり，デルタISMS 表はCISOと経営陣に対して状況や課題が的確に理解でき，評価が容易な内容と見なせる．

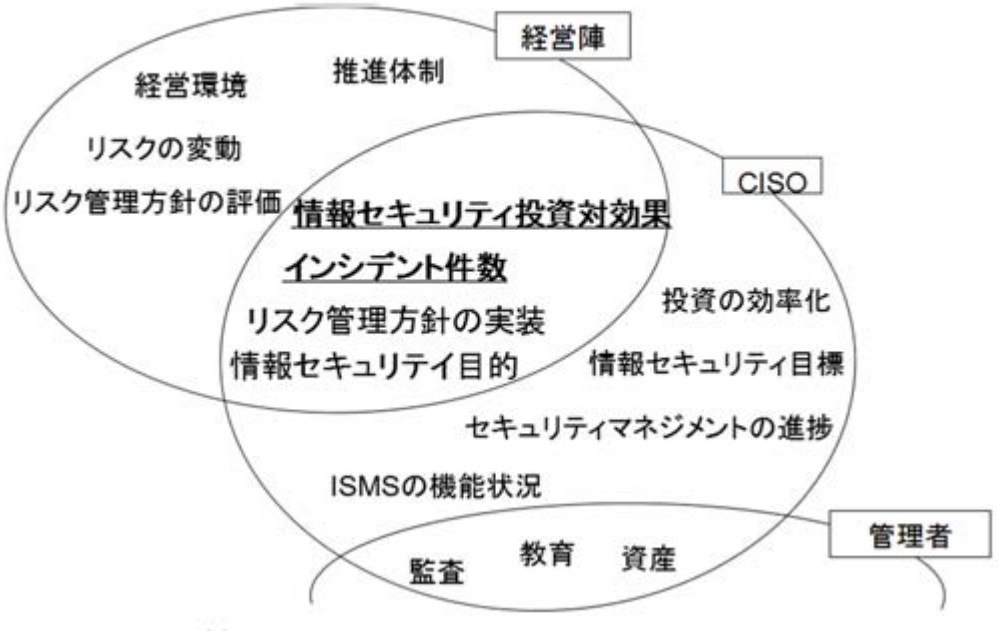


図 42　情報セキュリティガバナンスにおけるモニタリング項目

そして，デルタ ISMS 表の提供する情報は，正しくインシデント件数と情報セキュリティ投資対効果である（図 43）.

デルタISMS 表　　情報セキュリティ投資対効果

インシデント原因	被害額	頻度	対策1の投資コスト	対策2の投資コスト	…	対策Kの投資コスト
			(S_1C_1)	(S_2C_2)		(S_KC_K)
1	L_1	P_1	R_{11}	R_{12}	・・・	R_{1K}
2	L_2	P_2	R_{21}	R_{22}	・・・	R_{2K}
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・
J	L_J	P_J	R_{J1}	R_{J2}	・・・	R_{JK}

インシデント件数

図 43　デルタ ISMS 表の中のインシデント件数と投資対効果

なお，ここで対象としない「リスク管理方針」とは，経営陣が情報セキュリティに限らずあらゆる経営リスクに対して，どのレベルまで許容するかを示したものであり，ISMS においては，リスクアセスメント結果報告（表 9）のリスク値に対して対応の有無を判断するレベルに

相当する．デルタ ISMS においては，対策をどのインシデント原因（脅威）に対処するかを決める，つまり，3 パターンの選択に相当する．

また，「情報セキュリティ目的」は， ISMS 規格の箇条 6.2 に規定された内容であり，組織の情報セキュリティ方針に基づいて CISO が決める目的であるが，ここでは，細かな説明を省略する．

図 43 に示したデルタ ISMS 表に盛りこまれている「インシデントの対応」と「費用対効果」は殆どの組織で注力していない項目であることを，前出した ISMS 認証取得事業所へのアンケート（2.3.2 項参照）にて確認されたい（表 27）．デルタ ISMS は多くの組織で取り組まれていない項目を補強する役目を担っている．

表 27　ISMS の効果を高めるため重点的に取り組んでいるもの [23]

%	一般社員の認識	教育研修の改善	内部監査人スキル強化	管理者層の認識	マニュアルの整備	有効性評価手法	文書・記録管理	リスク分析手法	インシデント対応	経営陣の認識	費用対効果	その他	有効回答数
2012 年	66.4	29.7	27.6	26.7	22.1	21.9	20.3	19.2	15.5	11.0	4.1	1.1	438
2010 年	67.5	30.5	31.5	29.6	24.8	31.5	22.6	24.3	20.9	15.6	5.8	1.0	416
2008 年	62.5	29.0	25.9	21.6	22.4	31.8	20.7	20.7	17.3	9.9	4.8	2.6	352
2006 年	69.3	36.0	23.1	28.8	31.4	40.9	23.5	23.5	20.5	10.2	4.5	1.5	264

4．4　まとめ

本節では，3 種の評価でもって本研究に対する評価とした．最初が実組織の過去データを用いたケーススタディであり，2 番目が，仮想の組織を想定した標的型攻撃対策のケーススタディである．この二つのケーススタディでデルタ ISMS 手法は，対策選定のノウハウのない人でも定式化された手順に従いスムーズに対策選定が行え，エキスパートと同様の対策選定ができることを示した．最後に，情報セキュリティガバナンス導入ガイダンスのモニタリング項目とデルタ ISMS の処理対象の比較により，デルタ ISMS 手法が橋渡し人材に求められる役割を手順化しており，経営陣の認識向上に有効であることを示した．

情報セキュリティインシデントデータベースの運用，全社レベルの 3 次対応，インシデントと対策のデルタ ISMS 表，定式化による対策案の自動選定，安全係数を用いた複数対策案の自動選定，経営陣への複数対策案の提示から成る一連の方法を「デルタ ISMS」手法として提案した．すなわち本論文は，微視的には，企業の ISMS 手法の日本工業規格 JIS Q 27001:2014 [17]の中の「情報セキュリティインシデント管理（A.16 information security incident management）」に係る一貫性のある効果的な取組みについて手順化するものであり，JIS Q 27001:2014 を補完することを目的としている．

一方で，情報セキュリティマネジメントの強化は，事業部や事業所を越えた全社的な枠組みの中で達成されるべきものである．ISMS では事業部や事業所といった組織の一部で認証を受けることができるのに対して，本論文ではそのような組織の認証範囲を越えた全社的なセキュリティマネジメントを対象とする．すなわち本論文は，巨視的には，全社レベルの情報セキュリティマネジメントの改善に係る一貫性のある効果的な取組みについて手順化するものであり，組織の情報セキュリティガバナンスを補強することを目的としている．

第5章　おわりに

終章として，研究テーマと設定課題の解決を振り返る．本研究では ISMS（情報セキュリティマネジメントシステム）の補完としてのデルタ ISMS モデルを提案している．

第 1 章では，本研究の背景とテーマについて述べた．本研究は「情報セキュリティ」，「情報セキュリティマネジメントシステム」及び「情報セキュリティインシデント」を対象とし，それらの語源や定義から背景を紐解いた．情報セキュリティを脅かす原因は意図的な場合と偶発的な場合があるが，情報セキュリティは，安全（safe）とセキュリティ（security）を偶発的か意図的かで区別している航空業界とは異なり，意図的な場合も偶発的な場合も区別していない．企業における IT 投資が増加するソフトウェアは 3 年連続最重要が「情報セキュリティの強化」となっており，あらゆるものが情報化され，システム化される中で企業の IT 投資は情報セキュリティの強化が最重要視されている．情報セキュリティに対するマネジメント規格として ISMS が生まれ，企業の情報セキュリティ強化が最重要視されている背景の下，日本における ISMS 認証取得事業者数の推移は増加の傾向にあり，企業などは ISMS を取得する価値を高く評価し，積極的に認証取得しようとし続けている．情報セキュリティに対する様々な技術面，管理・運営面，法制度や倫理面の改善努力にも関わらず，情報セキュリティインシデントは巧妙化，凶悪化し，深刻なインシデントが発生し続けており，情報セキュリティインシデントが社会現象と捉えられるようになって久しい．

ISMS は “Plan-Do-Check-Act(計画-実行-点検-処置)”（PDCA）モデルの Plan に重きを置いており，対策を予め実施することは，対策をインシデント発生後に実施するのに比べて，被害を抑止することができるため，洗練されたマネジメントシステムと見なすことができる．ISMS の認証取得はインシデントの発生頻度や被害額を減じることができるはずであるが，実際にはインシデントの発生を減じることができていない組織もあり，これを解消することを本研究のテーマとした．ISMS 認証を取得してもインシデントが減らせない利用は，一巡目の Plan でそれに続く Do フェーズで起きることの予測の難しさにある．この難しさを，先行研究による情報セキュリティインシデントを隠そうとする傾向や表出されていない情報セキュリティインシデントが多いといった調査より示した．

ISMS は組織の部分認証を許している．情報セキュリティマネジメントの強化は，事業部や事業所を越えた全社的な枠組みの中で達成されるべきものである．ISMS では事業部や事業所

といった組織の一部で認証を受けることができるのに対して，そのような組織の認証範囲を越えた全社的なセキュリティマネジメントを実施していかなければならない．本研究で提案する全社的な情報セキュリティマネジメントの改善は，情報セキュリティマネジメントに責任を持つ経営陣または CISO（Chief Information Security Officer，最高情報セキュリティ責任者）等の配下に編成される組織横断型の「情報セキュリティ統括組織」によって担われる形となる．認証を取得した組織でも情報セキュリティインシデントが減らないという問題に対し，情報セキュリティインシデントデータを「組織全体のセキュリティ対策の改善」のために活用していくための具体的な方法・手順を，「デルタ ISMS」モデルとして提案した．

第２章では，関連研究と研究アプローチについて述べた．本研究が扱う問題を「認証取得後もインシデントが減らない」，「インシデントデータからどのように対策を選定するか」，対策を実施するために「どのように経営陣の認識を向上させ，情報セキュリティガバナンスを確立するか」の三点とした．

「認証取得後もインシデントが減らない」という問題については「ISMS 認証取得事業所へのアンケート」と「一部上場企業での認証取得後のインシデントの発生」という関連研究で詳細に述べ，問題の原因が，規格の情報セキュリティインシデントに対する手順化不足であることを規定文に立ち返り示し，「インシデントデータベースへの蓄積と分析」を提案した．

「インシデントデータからどのように対策を選定するか」という問題に対しては，「ISMS のリスクアセスメント手順を資産，脅威及び対策の対応として捉えなおしたリスクマネジメントの定式化」に関する先行研究を参考に，「インシデントと対策の対応を用いた定式化による投資対効果」の明示による自動選定を提案した．

「どのように経営陣の認識を向上させ，情報セキュリティガバナンスを確立するか」という問題は，ISMS が規定するマネジメントレビューにおいて情報セキュリティインシデントに対処することが求められていない現状をあげ，ISMS 認証組織へのアンケートから経営陣の認識向上があまり取り組まれていないことを示し，経営陣と管理者層の橋渡し人材不足という先行研究を述べた．デルタ ISMS では「複数対策案の提示」により，経営陣の方向性と合致できる対策を選択できるようにし，経営陣と管理者層の橋渡しを実現することで経営陣の認識を向上させることができる．この結果，組織の ISMS に対する監視サイクルが実質的に機能するようになり，デルタ ISMS による良好なスパイラルアップを得ることができ，情報セキュリティガバナンスが確立する．

第３章では，本論文で提案するデルタ ISMS モデルについて詳しく説明した．デルタ ISMS

モデルは，組織内で実際に発生したインシデントデータを使って， ISMS の PDCA サイクルの 2 巡目以降で組織の情報セキュリティリスク管理を改善していくための方法・手順を具現化したものである．Do フェーズで発生する情報セキュリティインシデントに対処するため，インシデント情報をインシデントデータベースへ登録・蓄積する．インシデントデータベースは，発生日時，インシデント内容，インシデント原因，インシデント経路，影響範囲，1 次対処の内容および被害額，2 次処置の内容および対策コスト，3 次対応の内容からなる．これらは，対策導出のために必要な最低限の項目である．インシデントデータベースに登録する項目を明確にするために，あいまいとなり易いインシデントの原因区分を定め，被害額の考え方を整理した．

組織内でインシデントが発生した場合，デルタ ISMS では，ISMS で規定されている 1 次対処と 2 次処置を実施した後，本研究で提案する 3 次対応までを行うこととした． 1 次対処と 2 次処置がインシデント発生部門にて実施されるのに対し，3 次対応は情報セキュリティ統括組織で定期的におよび重大な変化が発生した時に行う．インシデント原因と対策は多対多の関係にあり，対策の選択は脆弱性を下げることにより予想損失額を低減できる．最適な対策の選択のためには，対策コストの積み上げとその効果である損失低減額の積み上げを比較する必要があるため，デルタ ISMS では「デルタ ISMS 表」というインシデント原因と対策のマトリクスを作成することとした．定式化にはデルタ ISMS 表を構成する年間予想損失額，ALE 軽減率，対策のコスト及び安全係数を用いる計算を提示した．

安全係数は，被害低減額と対策コストの重みを変動させる係数であり，値を変動させることで複数の最適解を得ることができる．安全係数を大きくすると対策コストよりも安全を重視する対策群を導出することができ，安全係数を小さくすると対策コストを重視して最低限の安全を得る対策群を導出することができる．これにより，安全係数を変動させて複数の対策候補パターンを自動導出できる．導出された 3 個の対策案を金銀銅と呼ぶこととし，情報セキュリティ統括組織は，n+1 巡目の Plan の際に，n 巡目に選定された組織全体のセキュリティ対策の改善案を CISO 等に提示する．CISO 等は，デルタ ISMS 表と式の計算結果を「対策を追加したり改定を採用したりするかどうかを判断するための情報」や説明材料として利用し対策を経営戦略に合致した形で決定し，取締役会等で経営陣に説明することとした．この結果，組織全体の情報セキュリティマネジメントが改善され，経営陣の情報セキュリティリスク管理に対する認識も向上し，組織の ISMS に対する監視サイクルが実質的に機能するようになり，情報セキュリティガバナンスが確立できる．以上、デルタ ISMS はインシデントデータベース，3 次対応，デルタ ISMS 表，定式化，安全係数及び金銀銅の 3 パターンの対策案という特徴的な構成要素からなっている．

第４章では，3 種の評価でもって本研究に対する評価とした．軽微な偶発的インシデントは多数発生しているので，最初に実組織の過去データを用いた偶発的インシデントに対するケーススタディを行った．意図的インシデントに対する対策を公表することは，当該組織やシステムの弱点を公表することになるため，対策が公表されることはない．このため，2 番目に，意図的インシデントである標的型攻撃対策を仮想の組織を想定してケーススタディを行った．この二つのケーススタディでデルタ ISMS 手法は，対策選定のノウハウのない人でも定式化された手順に従い対策選定が行え，エキスパートと同様の対策選定ができることを示せた．最後に，情報セキュリティガバナンス導入ガイダンスのモニタリング項目とデルタ ISMS の処理対象の比較により，デルタ ISMS 手法が橋渡し人材に求められる役割を手順化していることを示した．

インシデントが発生する前（Plan フェース）のリスク分析においては，当該組織内にて実際にインシデントがどれくらいの頻度で発生し，その結果どれくらいの額の実被害となるかを正確に予測することは難しい．これに対し，デルタ ISMS 表においては，組織内で実際に発生したインシデントを並べるので，現実の数値を用いての評価が可能である．同様に，インシデントが発生する前のリスク分析においては，インシデントの原因としては一般的な事例を想定することしかできないため，類型的な対策を挙げることしかできない．これに対し，デルタ ISMS 表においては，組織内で実際に発生したインシデントを並べるので，具体的なインシデント原因を究明することが可能であり，そこから導出される対策はその組織に真に必要な対策となる．このように，デルタ ISMS では情報セキュリティ対策を組織の実態にあわせてチューニングしていくことができる．

実組織の過去データを用いたケーススタディでは，実組織で選択された対策が選定でき,エキスパートと同様の対策制定ができることを示すことができ，加えて，実務者の意見から本手法の有効性を示せた．

仮想の組織を想定した標的型攻撃対策のケーススタディでは，ISMS の対策を全て実施している組織を想定し,オーストラリアの国防総省が公表した 35 個の対策から，対策選定のノウハウの無い人でも定式化された手順に従いエキスパートと同様の対策選定がスムーズに行えることを示すことができた．

加えて，本研究ではあるべき経営陣と CISO の共通語という観点からデルタ ISMS 表と情報セキュリティガバナンスのモニタリング項目とを比較した．デルタ ISMS では，CISO 等はリスクアセスメントに使用したデルタ ISMS 表の情報（インシデント原因と対策の投資対効果）を経営陣に報告する．経営陣が検討しなければならない分野は情報セキュリティ分野にとどまらず広範なため，要点を絞った情報伝達が求められる．経済産業省から公表された「情報セキ

ュリティガバナンス導入ガイダンス」には，経営陣，CISO および管理者が行うモニタリング項目の例がモニタリング内容と指標例として 80 項目記載されている．これらをグループ化し 15 個のグループに分け，経営陣と CISO が共にモニタすべき項目は 4 項目であることを明らかにした．これらの 4 項目にはデルタ ISMS 表がカバーする 2 項目（インシデント件数，投資対効果）があり，デルタ ISMS 表が提供する情報が CISO と経営陣の間での共通語であり，デルタ ISMS 表は CISO と経営陣に対して状況や課題が的確に理解できるための共通語となることを示した．

本研究では，ISMS 認証を取得した組織でもインシデントが発生していることより，インシデントの発生件数を減らすことを課題とし，組織で発生したインシデントに着目して改善につなげていくための，インシデント対応の手順化を提案した．本研究は，微視的には，企業の ISMS 手法の日本工業規格 JIS Q 27001:2014 の中の「情報セキュリティインシデント管理（A.16 information security incident management）」に係る一貫性のある効果的な取組みについて手順化するものであり，JIS Q 27001:2014 を補完することを目的とする．同時に，本研究は，巨視的には，全社レベルの情報セキュリティマネジメントの改善に係る一貫性のある効果的な取組みについて手順化するものであり，組織の情報セキュリティガバナンスを補強することを目的とする．

本研究結果は，今後，規格の改善に役立てたい．本研究の発端は ISMS 規格がインシデントからの学習を求めていてもその手順が示されていないことであった．ISO27001 の規格は何をするかを規定されているが，いかに行うかを規定していない．「いかに」に関しては ISO27002 がガイドラインとして示されているが，「インシデントからの学習」は十分でなく，ISO27002（あるいはそれに準じるガイダンス）の追加改善が必要と考える．

本文から参照のない付録 4 と付録 5 は研究の過程で気づいたトピックであり，今後の研究課題となる．付録 4 は情報セキュリティマネジメント学における会計的アプローチ研究で「情報セキュリティインシデントと情報セキュリティの取り組みの関係性についての検討」及び「情報セキュリティの取り組みの有無が会計情報に対する評価にどのようにインパクトを与えるかについての検証」の研究が皆無であることを指摘している．これから，情報セキュリティインシデント対策の効果の場合分けから始めて，会計的にインシデントと対策の関係性の分類を行っていきたい．付録 5 では「保険という対策をセキュリティ対策選定法でどのように扱っていくか」という従来の課題に保険の損害低減率を求めることができた．一方，金融工学の中には，金融商品のリスクを数学やコンピュータを使って数値化しリスクマネジメントに役立たせる分野がある．これらの研究成果を情報セキュリティインシデントや対策へ適用できるか検討を進めて行きたい．

付録 1　FTA と Medical SAFER

(1) FTA

ISMS のリスク分析の定式化による一連の研究に対して，FTA （Fault Tree Analysis）を用いる一連の研究がある．

FTA の情報セキュリティ解析への使用は，1988 年に宝木らから始まったようだ [69]．永井らは，各脅威の因果関係を表現した FTA を行い，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脅威を抑止する必要最小限の基本事象の組合せを特定する方法を提案している [70]．加藤らは FTA を利用して管理者とユーザが交渉を行うことでセキュリティと利便性を維持した特別な利用が可能な対策の組合せを決定できることを示している [71]．永井らは，複数のフォルト・ツリーの相対正規化重要度計算とファジイ関数を用いた適合度計算に基づいて，対策目標に対して機能的に適合する実現方式を決定できるようにした [72]．呉らは FTA を利用して要員数や開発期間の特性を入れ，繁忙期には生産性を優先し，閑散期にセキュリティを強化できることを提案し [73]，芝口らはフォルト・ツリー解析を利用して在宅勤務モデルを分析し，仕事量が変動する企業で，期待支出を削減できることを示した [74]．相原らは標的型攻撃の攻撃パターンを FTA で記述し最適な対策を選定している（図 44） [75]．

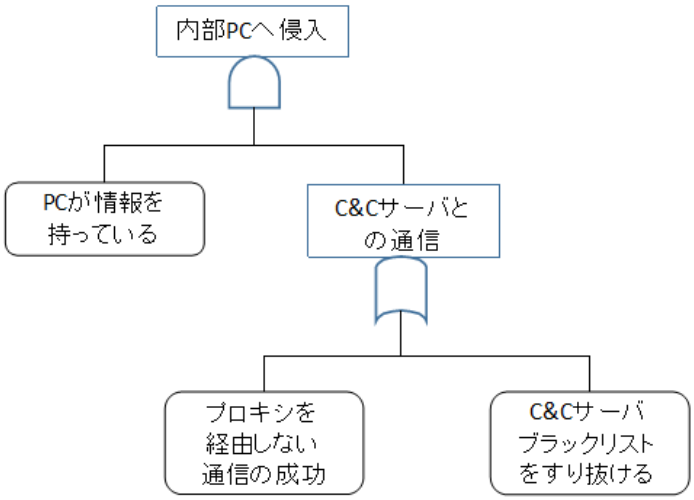


図 44　フォルト・ツリー例 [75]

FTA は AND と OR の演算子を用いて，複雑な条件も正しく記述できるメリットがあるものの実運用でノードの数が増えた場合，計算が多段となり複雑さが増すというデメリットを持つ．脅威を特定できる場合は，効果的であるが，ISMS では想定される脅威全てを対象とするため

妥当ではない．加えて，ISMS でのリスク分析との親和性から，デルタ ISMS では， FTA 記法ではなく，表形式による表記を用いる．

(2) その他の対策導出手法

FTA 以外にも，各種の対策導出手法が報告されている．

2006 年に，佐々木が疫学からのアプローチを提案した [76]．佐藤らは，機械工学で発展した失敗学を情報セキュリティに取り組んでいる．ISO／IEC27002 が運用者向けの対策であることに対して，失敗学の対策は設計者向けの対策となる．頻発しているマルウェアの脅威に対して，ISO／IEC27002 に記載のない次の対策群を提案している．

『・ウイルス感染の発生後，外部への情報送信が行われる前に送信パケットを自動的に遮断し，機密性を維持するソフトウェアや，ウイルス感染後にシステムが停止しても冗長系に切り替わり，可用性を維持する冗長設計．

・改ざん検知ができる仕組を用意し，バックアップデータを取得するだけでなく，さらにバックアップデータを丸ごと格納したディスクと容易に交換・換装できるようにハードウェアを設計する』 [77].

新原らは，情報セキュリティ対策分析手法として，IRAS（Information Systems Audit and Control Association），VTA(Variation Tree Analysis)，4M-4E 分析，Medical-SAFER を比較し, Medical-SAFER が高度な予備知識が不要で, 未知対策の発想に適していると評価した [78]. 村上らは，Medical-SAFER をマルウェア感染に適用している [79]．Medical SAFER は，7 手順から成る. 本研究は, 手順化をテーマとしているので, 参考のために, ここで Medical SAFER の手順を詳しく説明する．Medical SAFER は次の手順で進める．①ヒューマンファクター―の考え方を理解する．②時系列図を作成する（図 45）.

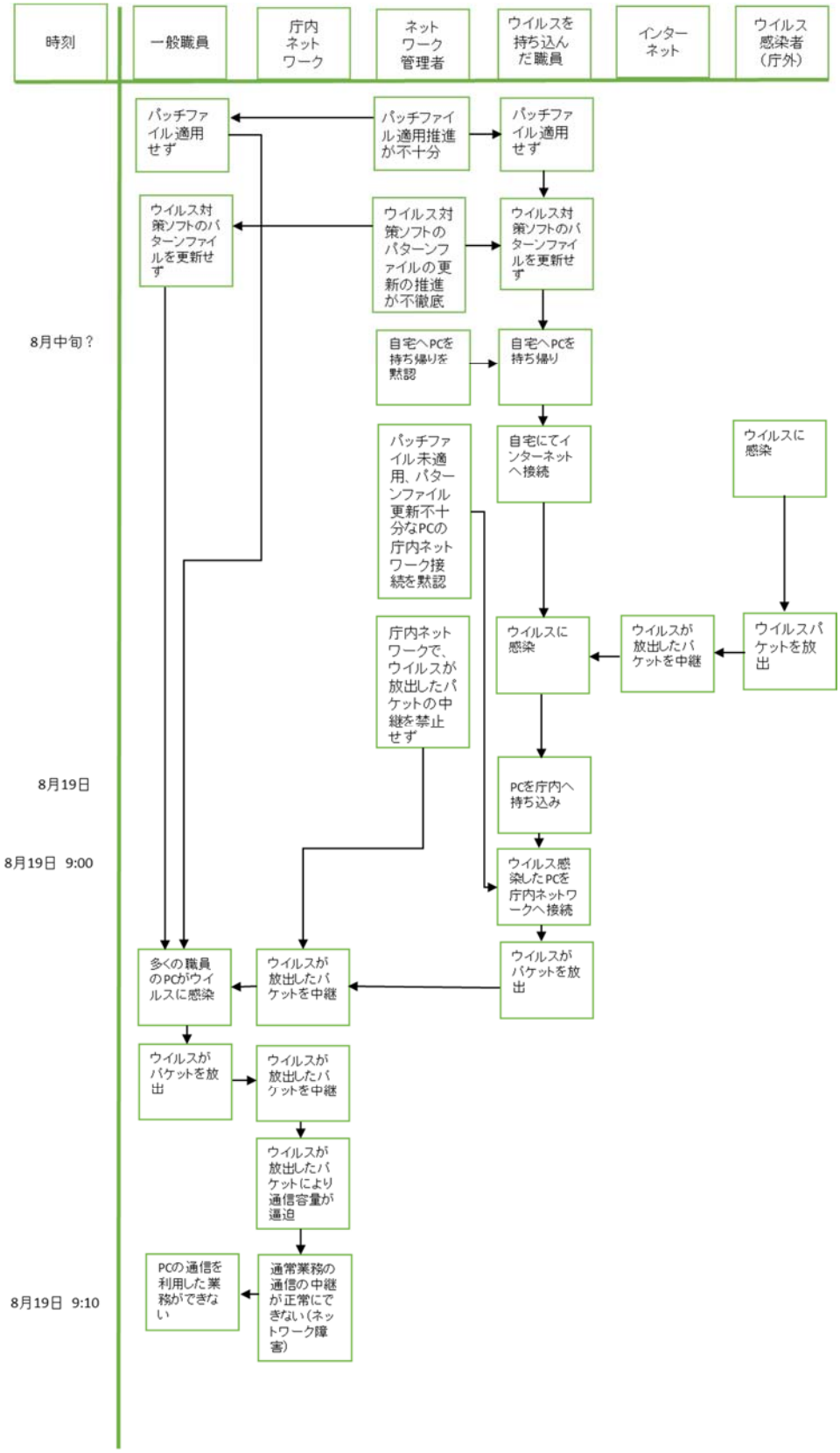

時刻
一般職員
庁内ネットワーク
ネットワーク管理者
ウイルスを持ち込んだ職員
インターネット
ウイルス感染者（庁外）
パッチファイル適用せず
パッチファイル適用推進が不十分
パッチファイル適用せず
ウイルス対策ソフトのパターンファイルを更新せず
ウイルス対策ソフトのパターンファイルの更新の推進が不徹底
ウイルス対策ソフトのパターンファイルを更新せず
8月中旬？
自宅へPCを持ち帰りを黙認
自宅へPCを持ち帰り
パッチファイル未適用、パターンファイル更新不十分なPCの庁内ネットワーク接続を黙認
自宅にてインターネットへ接続
ウイルスに感染
庁内ネットワークで、ウイルスが放出したパケットの中継を禁止せず
ウイルスに感染
ウイルスが放出したパケットを中継
ウイルスパケットを放出
8月19日
PCを庁内へ持ち込み
8月19日 9:00
ウイルス感染したPCを庁内ネットワークへ接続
多くの職員のPCがウイルスに感染
ウイルスが放出したパケットを中継
ウイルスがパケットを放出
ウイルスがパケットを放出
ウイルスが放出したパケットを中継
ウイルスが放出したパケットにより通信容量が逼迫
PCの通信を利用した業務ができない
通常業務の通信の中継が正常にできない（ネットワーク障害）
8月19日 9:10

図 45　時系列図 [79]

③ 背後要因関連図を作成する（図 46）.

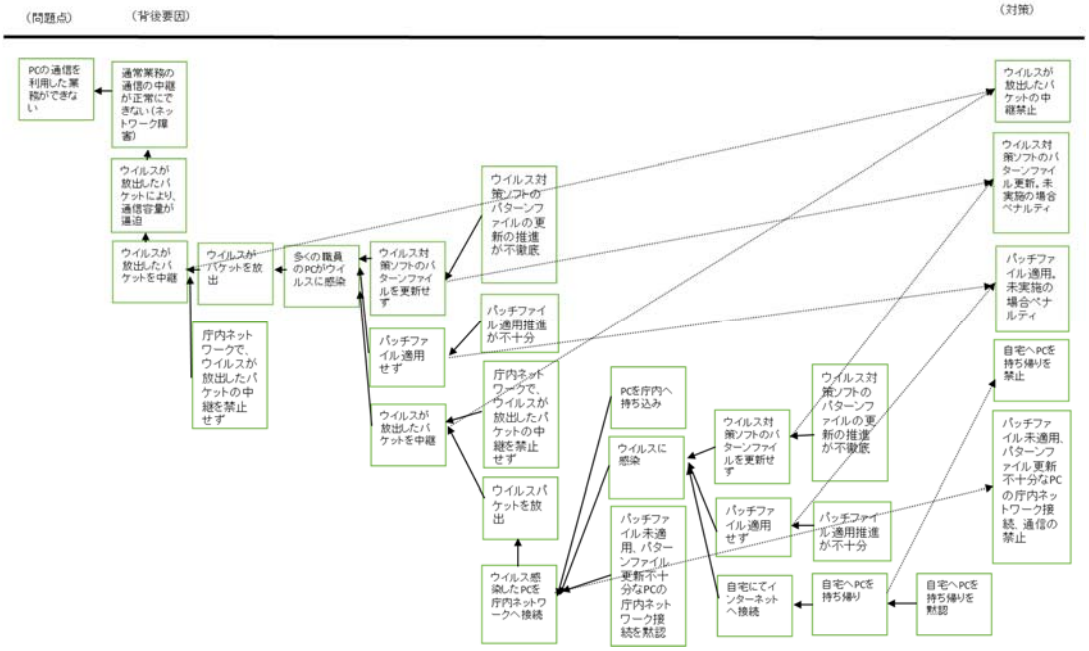


図 46　背後要因関連図 [79]

④ 考えられる対策案の列挙で発想手順マトリックスを作成する．⑤対策の優先順位付け，⑥対策の実施，⑦実施した対策の評価と続く（表 28）.

表 28　対策決定・効果評価 [79]

No	背後要因	対策案	効果点 GUIDE	点数	残留リスク	その他懸念事項	採用	いつまでに	誰が
1	ウイルスが放出したパケットを中継	ウイルスが放出したパケットの中継禁止	②できないようにする	8	中継を禁止するネットワーク機器（システム）の設定更新もれ	システム導入・運用費用	△	次年度	ネットワーク管理者
2	ウイルス対策ソフトのパターンファイル更新せず	ウイルス対策ソフトのパターンファイル更新．未実施の場合ペナルティ	⑨安全を優先させる	1	個人の意識に依存 自動更新設定を行っても解除される可能性あり	ペナルティ内容の検討	○	即時	各職員（PC利用者）
3	パッチファイル適用せず	パッチファイル適用．未実施の場合ペナルティ	⑨安全を優先させる	1	個人の意識に依存 自動更新設定を行っても解除される可能性あり	ペナルティ内容の検討	○	即時	各職員（PC利用者）
4	自宅へPCを持ち帰り	自宅へPCを持ち帰りを禁止	⑨安全を優先させる	1	個人の意識に依存	ペナルティ内容の検討 持ち物検査の実施可否検討	○	即時	各職員（PC利用者）
5	ウイルス感染したPCを庁内ネットワークへ接続	パッチファイル未適用，パターンファイル更新不十分なPCの庁内ネットワーク接続，通信の禁止	②できないようにする	8	パッチファイル，パターンファイル情報の更新漏れ 適用時にシステムに影響の出るパッチファイルの検討	システム導入・運用費用	○	次年度	ネットワーク管理者

導出された対策を次に示す.

『・ウイルスが放出したパケットの中継禁止.

・ウイルス対策ソフトのパターンファイル更新．未実施の場合ペナルティ.

・パッチファイル提供．未実施の場合ペナルティ.

・自宅への PC の持ち帰り禁止.

・パッチファイル未適用，パターンファイル更新不十分な PC のネットワーク接続，通信の禁止.』

Medical SAFER は複雑な一連の作業の中から，改善のための気づきを抜けなく対策に導くことには向いている．しかし，特に，対策の投資対効果が重要視される様々な脅威を並列で捉う ISMS が対象とするような分野には向かないように思われる．なお，安藤らは，Medical SAFER，FTA 及びシステム解析プロセス解析で使われる FMEA（Failure Mode and Effects Analysis）を用いて情報セキュリティにおけるヒューマンエラーの対策を導出比較している [80]．菅野らは対策のモチベーション要因を抽出した [81]．畑らは費用対効果の観点から段階的な対策の導入を提案した [82].

以上，様々な対策選定手法について示してきたが，これらの手法は，規格の求める附属書 A の対策以外の対策の案出に用いることができる．本研究が課題とする対策選定手法とは互いに補完する関係となる．

付録２　ISMS と内部統制システムの比較

IPA（独立行政法人情報処理推進機構）より 2015 年に公開された「組織における内部不正防止ガイドライン [83]」においても情報セキュリティガバナンス導入ガイダンスと同様に経営層におけるリーダーシップの強化が重要な項目の一つとなっており，会社法 [84]の内部統制の体制を参照している．

ここでは，内部統制の意味を示した後，会社法の内部統制システムを概観する．

『内部統制は，英語の internal control の訳語である．直訳すれば内部のコントロールである．Control という語は Contrast(照合)と roll（巻物）の合成語で，中世の英国の荘園で所有する羊の数が巻物に記録された数とあっているかどうかを突き合わせるところから生まれたといわれている．本来，internal control とは，組織内において正確な記録が維持されているかどうかをチェックすることという用語である』 [85].

内部統制システムとは,『すべての会社において取締役が会社を事業目的に沿って適切に運営するために本来必要なもの』を指す [86].

内部統制システムの目的は，法令違反・定款違反・不正・不祥事・事故といった問題の発生を未然防止することである．内部統制システムは，会社法により，大会社（資本金として計上した額が 5 億円以上，または，負債として計上した額の合計額が 200 億円以上）が設備義務を負う．会社不祥事をきっかけに監査役制度の強化がされ，近年では委員会設置会社や内部統制システムの導入など，会社に対する規制が強化される方向に進んでいた．会社法は 2005 年に成立した．21 世紀の比較的新しい法律である．全ての会社を対象とするが，大会社と委員会設置会では取締役（会）に整備義務がある．取締役（会）が業務の適正を確保するための体制の整備を構築しなければならない.（内部統制システムの構築の基本方針を決定しなければならない）これは事業報告書にて書面化と開示が必要であり，監査役が監査報告書で監査結果を報告しなければならない [87] [88].

会社法の法文上では内部統制システムという言葉は全く使われていない．会社法 362 条 4 項六号の体制が会社法にいう内部統制システムを意味している．

法 362 条（取締役会の権限等）抜粋

4　取締役会は，次に掲げる事項その他の重要な業務執行の決定を取締役に委任することができない.

＜中略＞

六　取締役の職務の執行が法令及び定款に適合することを確保するための体制その他株式会社の業務の適正を確保するために必要なものとして法務省令で定める体制の整備

『内部統制システムにおいて，取締役は，事業運営上のリスクを洗出し，評価をした上で体制を構築し（Plan），実際にこれを運用し（Do），構築された体制が期待通り有効に機能しているか，あるいは問題が無いかを確認し（Check），問題の有無に係らず法令や社会の要請に適合しているか見直していく（Act）という PDCA サイクルを確立する・させることが必要である.

ただし，取締役が内部統制システムを PDCA サイクルにより構築・運営する際に，自らが会社の隅々まで目を光らせて，会社の規模，業容，業態に則したリスクを洗出し，そのリスクを評価した上で，体制を Plan・Do すること，あるいは Check することは実質的に困難である. また一方で，何がしかのリスク・懸念がありながら，その状態を放置し問題が発生したならば，やはり取締役は善管注意義務違反に問われることになる.

そこで，経営層は，法務，財務，リスク対策，環境部門といったコーポレート・ガバナンスに係る個々の専門部門を設置し，これら個々の領域における PDCA サイクルを委ねることになる．これら内部統制の専門部門を設置し，適切に運用していくことも，内部統制システムの一貫となる．さらに，各部門・業務の中で内部統制のシステムを運用することが，問題発生の未然防止のために必要不可欠なこととなる.』 [89].

図 47 は内部統制システムと情報セキュリティガバナンスにおける PDCA サイクルの違いを組織の階層の観点から示したものである．内部統制システムでは，会社内でいくつかの大小様々な PDCA サイクルが回るが最初に求められている PDCA サイクルは経営陣，管理者・従業員層に跨ったサイクルである．一方，ISMS では，部署，事業所，工場といった場所というように対象範囲を合理的に説明ができる範囲に限定して「適用範囲」として認証取得範囲に選定することができることもあり，PDCA サイクルが管理者・従業員層に留まりやすい.「適用範囲」が全社の場合，PDCA サイクルは経営陣，管理者・従業員層に跨ることもあるが，場合によっては，PDCA サイクルが従業員層に留まる事もある.

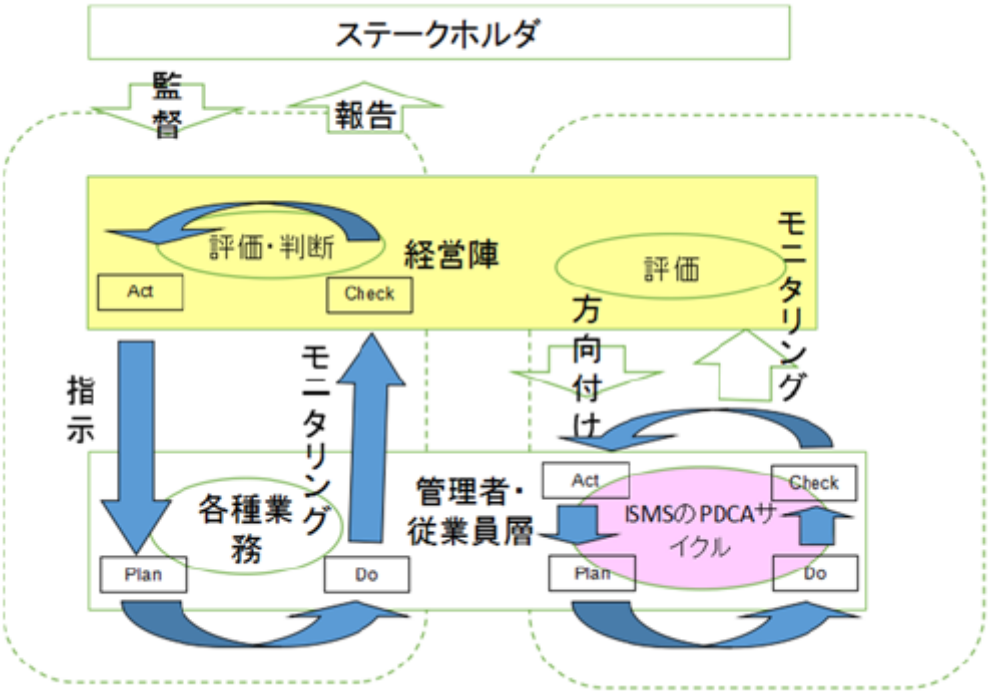


図 47　内部統制システムと ISMS

付録３　入館証や携帯電話紛失に関する追加調査

遠隔データ初期化サービスはインシデント発生後の被害額軽減策である．インシデント発生そのものを軽減するための方策は無いのだろうか．この疑問に対して，ヒューマンエラーの Reason は Norman の The Psychology of Everyday Things(邦訳『誰のためのデザイン？』)を推奨している [12].

『長年にわたって私はドアに正面から突っ込んだり，水道の蛇口の使い方に首をひねったりといったふうに, 日常生活のごく簡単なことを扱いかねてヘマばかりしてきた. 自分のせいだ，なんて機械音痴なのだと，声にもならないつぶやきをもぐもぐ唱えていたものだった．しかし私が心理学を学んで他の人々の行動を観察していくにつれ，私だけの問題ではなさそうだと気づくようになった．私がヘマをしたり，難しくて首をひねったりした問題は，他の人も鏡に映したように同じことを抱えていた．しかし誰もが自分のせいにしているようなのだ．いったい全体，世界中の人々全員が機械音痴なんてことがありうるのだろうか．だんだん真相が見えてきた．私の研究領域がヒューマンエラーや産業事故まで広がると，ヒューマンエラーはデザインが悪いからおこるのだと気づき始めた』 [90].

上述した示唆に基づくと，携帯電話やセキュリティカードのデザインを変えれば，もっとインシデント発生を軽減できると思われる．例えば，携帯電話を腕時計にしたり，セキュリティカードを腕輪にしたりすれば，紛失はより少なくできると思われる．

付録４　情報セキュリティマネジメント学における会計的アプローチ研究

加賀谷は，情報セキュリティマネジメント学における会計的アプローチ研究を次の 4 タイプに分類している（図 48） [91].

① 情報セキュリティインシデントが企業価値をどれほど棄損させるか.
② 情報セキュリティインシデントと情報セキュリティの取り組みの関係性についての検討.
③ 情報セキュリティに係る取り組みや開示が株式市場でそのような評価を受けるかを検討するアプローチ.
④ 情報セキュリティの取り組みの有無が会計情報に対する評価にどのようなインパクトを与えるかについての検証.

これまでに蓄積されている先行技術は①と③の研究のみで，②と④の研究は皆無である．②と④については，各社の情報セキュリティに関わる取り組み実態を示したデータベースがこれまで全く蓄積されてこなかったため，検証の対象外となってきた．データベースの構築とそれに基づく検証を通じて，情報セキュリティに関する取り組みが外部ステイクホルダーに開示する一連のプロセスを通じて企業価値を創造する経路を可視化し，それを定量的な指標に基づき評価分析できる「情報セキュリティ会計」の構築が可能になるかもしれない.

なお，①と③の研究は例えば石黒らが比較している [92].

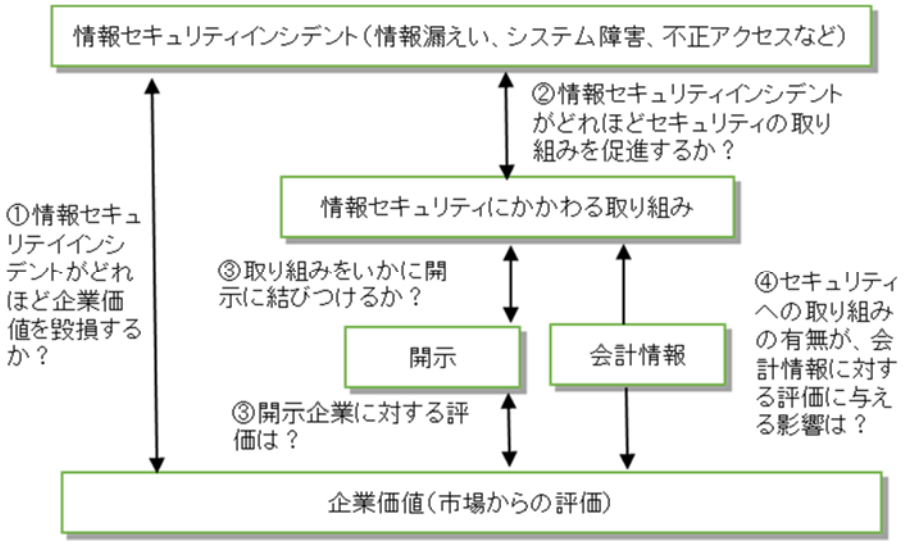


図 48　情報セキュリティと企業会計の関係性 [91]

本研究は，会計情報と関連するものではないが，情報セキュリティインシデントの企業会計に与える影響の研究はこれから注目される分野となっている.

付録５　サイバーリスク保険

従来，保険を対策の一つとしたときの低減率が不明であったが，ここでは，低減率を導出することができたので，それを示す.

『保険契約とは不慮のインシデントによって低い確率ながら多大な損害を被る可能性を回避するために行うものである．今，平均的に年間 222 社に 1 社の割合でのセキュリティインシデントの発生（0.45%）とインシデントにあうと 1 億円の顧客への賠償責任の発生を想定する．保険会社が保険料を加入社から集めるとして，加入社の支払う保険料は年間 45 万円に保険会社の利益をのせて，例えば 50 万円となる．保険契約とは，保険会社と加入社の間での確実性と不確実性の交換，つまりリスクの売買が行われている．加入社は金銭を支払って，不確かさを保険業者に引き取って貰っている 1 社あたりの保険料 50 万円から，セキュリティインシデント被害者に保険金として平均的に還付される金額を加入社 1 社あたりで換算した 45 万円を引き算して残る 5 万円が「リスクプレミアム」と呼ばれる．「リスクプレミアム」にはインシデント発生が想定した確率を超えて発生した場合の保険会社の負担も含まれる』 [93].

保険は，ISMS におけるリスク対応の選択肢の一つである.

ISMS のリスクマネジメントにおける作業 5「リスク対応」において，保険は選択肢の一つとなっている.『一つ以上の他者とリスクを共有すること（契約及びリスクファイナンシングを含む） [10]』.

そして，JIPDEC は，『リスク管理上は，JIS　Q　27001 附属書 A の管理策に相当する管理策を適用できない場合や，適用してもリスクレベルが受容水準以上の場合，保険を検討することとなる.』リスクファイナンスとして保険を採用する例として『地震などの不可避な脅威については，事業に与える影響は大きいが，比較的発生する可能性が低いので保険の利用を検討する等ということになります.』と説明している [31].

従来，保険採用時に低下する ALE 軽減率が不明であったため，保険を対策として定式化の中に組み込むことができなかった.

臼井らは，脅威の発生確率を下げることを目的とした「事前対策」と脅威の発生による損失を回復することを目的とした「事後対策」の併用を提案したが，その『おわりに』に『既存のセキュリティ対策選定法においては，保険という対策をどのように取り扱っていくかが問題となっている.』と述べ，保険の対策として ALE 低減率を不明としていた [94].

松浦が早い段階で，保険の経済モデルを示したが [95]，その式から，保険を対策として扱うための ALE 軽減率を得ることはできない.

松浦は Gordon-Loeb モデルを拡張してサイバーリスク保険の最適解を検討している．Gordon-Loeb モデルは次式の値が最大にある値を最適解としている [96].

『式 3:

$$\mathrm{ENBIS} = \{v - S(z,v)\}t\lambda - z$$

ここで,

- ENBIS は the Expected Net Benefits from an Investment in information Security の略語.
- v ： 脆弱性. 攻撃等の脅威が生起した際に，生起したという条件の下で，脅威が成功する条件付き確率（0≦v≦1）.
- $S(z,v)$ ： セキュリティ侵害確率関数.（投資 Z により改善されるvの値）
- t ： 攻撃等の脅威が生起する確率（0≦t≦1）.
- λ ： 攻撃等の脅威が成功したときの経済的損失.
- z ： 情報セキュリティ投資（対策のコスト）.』

松浦は次式の値が最大にする最適解を求めると結論付けている [95].

『式 4:

$$\{v - S(z,v)\}t(\lambda - \lambda_k) - z - z_k$$

ここで,

λ_k ：保険によって見込まれる被害額の減少.

z_k ： 保険の料金.』

λはデルタ ISMS 式における LP_j に相当するので，松浦の式４は次のデルタ ISMS 式に取り込むことができる.

$$E_{\triangle} = \sum_j \left\{ (LP_j - \lambda_k)\left(1 - \prod_i (1 - R_{ji}S_i)\right)\right\} - \sum_i C_i S_i - Z_k$$

この式では，保険の効果が，対策選定の式Πの外側にあるため，他の対策と同等に扱うことができない.

石川らは費用便益分析手法を用いてサイバーリスク保険の有効性を示している（表 29）[97].

表 29　サイバーリスク保険の有効性結果一覧 [97]

	CASE1	CASE2	CASE3	CASE4
SQLI	16.40%	5.00%	16.40%	5.00%
サイバー保険	なし	なし	あり	あり
攻撃成功件数	163,909	50,282	165,068	50,157
コスト（最小値）	0.000	4.200	0.500	4.700
コスト（最大値）	302.244	305.796	172.643	176.822
コスト（平均値）	24.831	11.808	8.856	7.232
コスト（中央値）	0.000	4.200	0.500	4.700
平均相対コスト	1	0.476	0.357	0.291
ROSI	-	3.101	31.95	3.744

この計算経緯を利用してサイバーリスク保険の ALE 軽減率を求めてみる.

CASE1～4 は，セキュリティ診断とサイバーリスク保険という二つ対策を採った場合と採らなかった場合で，ある会社を想定して，SLQ インジェクションに対するコスト（被害額と対策コストの合計）を比較している．表 30 に被害改善額を示す.

表 30　診断と保険の被害改善額

	CASE1	CASE2	CASE3	CASE4	備考
診断	なし	あり	なし	あり	
保険	なし	なし	あり	あり	
対策コスト	0.000	4.200	0.500	4.700	
被害額	24.831	7.608	8.356	2.532	平均値　－　対策コスト
改善額	0.000	17.223	16.475	22.299	被害額　－　24.831

診断の低減率を α_1，保険の低減率を α_2 とおくと，次式より α_1=0.694，α_2=0.663 が求まる.

$24.831\times(1-(1-\alpha_1))=24.831\times\alpha_1=17.223$

$24.831\times(1-(1-\alpha_2))=24.831\times\alpha_2=16.475$

α_2の値の根拠を追うと次のようになる.

α_2=16.475／24.831＝（24.831－8.356）／24.831＝

151.2×0.164－（151.2－100）×0.164／（151.2×0.164） ＝ 100／151.2

ここで 100 は保険による顧客への賠償責任　1 億円．151.2 は表 31 の値の合計による SLE である.

表 31　SLE の内訳

項目	金額	根拠
インシデント対策コスト	62.8 百万円	調査費用 4.0 改竄検知ツール　1.1 FW 監視サービス　4.2 IPS 監視サービス　15.0 診断サービス　4.2 諸工事　0.3 サーバ交換　34.0
顧客へのお詫び	82.875 百万円	750 円×110,500 件
顧客 QA 対応	5.525 百万円	1000 円×0.05×110,500 件
合計	151.2 百万円	

以上より，保険の低減率は次式となる.

$$保険の低減率 = \frac{保険の賠償金}{SLE}$$

以上，臼井らが不明とした保険の低減率を求めることができた.

なお，脆弱性の存在確率や対策による脆弱性の存在確率の変化は各種ベンチマーク資料に見ることができる [98] [99].

謝辞

本研究を行うにあたり指導教員としてテーマ設定から発表スライドのレビュー，論文の書き方まで親身なご指導を賜りました静岡大学情報学部西垣正勝教授に深く感謝を申し上げます.

また，副指導教員である静岡大学機械工学科近藤淳教授，静岡大学情報科学科峰野博史准教授を始め，論文審査委員の立場から適切な助言をくださいました静岡大学情報科学科酒井三四郎教授，静岡大学情報基盤センター副センター長長谷川孝博准教授に感謝いたします.

2 か月に 1 回，東京電気大学にて開催される T-SAP のメンバーの方々に深く感謝いたします．毎回の議論・ご教授に加えて，研究のテーマ設定や情報セキュリティ実務に関しては，株式会社 NTT データの CSIRT であり，JNSA セキュリティ被害調査 WG のリーダーである大谷尚通氏に多くの示唆をいただきました．東京電機大の勅使河原可海先生，髙橋雄司氏，株式会社東芝の加藤岳久氏には，毎回 T-SAP 前に個別ゼミをご開催いただき，加えて，情報処理論文の回答文作成のレビュー会にご参加いただきました．NTT の間形文彦氏には特に ISMS 制度に関して各種ご教授いただきました. T-SAP 主査の東京電機大の佐々木良一教授には, T-SAP 発表時に毎回欠かさずご好評を頂き，加えて，日本セキュリティ・マネジメント学会 IT リスク学研究会での報告をご調整いただました．深く感謝を申し上げます.

更に, 静岡大学の博士課程をご紹介頂きました愛知工業大学水野忠則教授に感謝いたします.

静岡大学の安藤敦子様には，国際学会の旅費処置や博士論文提出時の書類準備にご助力いただき感謝いたします.

三菱電機インフォメーションネットワーク株式会社の馬場慎也氏には，静岡大学入学時・通学時にご支援をいただき，お礼申し上げます.

参考文献

[1] 日本セキュリティ・マネジメント学会： セキュリティマネジメント学ー理論と事例ー， 共立出版（ 2011）.

[2] G.Chantrell (Ed.) ： The Oxford Dictionary of Word History, （オックスフォード英単語由来大辞典)，柊風舎（2015）.

[3] ISO/IEC 27000：Information technology - Security techniques - Information security management systems -Overview and vocabulary（JIS Q 27000：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-概要及び用語），日本規格協会（2014).

[4] 中尾康二： ISO/IEC27001:2013 情報セキュリティマネジメントシステム要求事項の解説, 日本規格協会（ 2013）.

[5] 羽室英太郎： 情報セキュリティ入門[第2 版]， 慶應義塾大学出版会（ 2013）.

[6] 矢野経済研究所： 国内企業のIT 投資実態と予想2016， 矢野経済研究所（ 2016）.

[7] P.F.Drucker： Management: Tasks, Responsibilities, Practices（マネジメント――課題・責任・実践)，ダイヤモンド社（1974).

[8] ISO： The ISO Survey of Management System Standard Certifications(2006-2015)， ISO（ 2016）.

[9] 一般財団法人 日本情報経済社会推進協会（JIPDEC）： 認証機関別・県別認証取得組織数.(オンライン)， https://isms.jp/lst/ind/suii.html，(引用日: 2017―7―14)（2017 ）.

[10] ISO Guide 73： Risk management – Vocabulary（JIS Q 0073 リスクマネジメント用語）（2010).

[11] 佐々木良一： インターネットセキュリティ入門，岩波書店（1999）.

[12] J.Reason： Human Error（ヒューマンエラー)，海文堂（2014）.

[13] NPO 日本ネットワークセキュリティ協会(JNSA) : 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～, NPO 日本ネットワークセキュリティ協会（2016）.

[14] 国家公安委員会，総務大臣，経済産業大臣：不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況，国家公安委員会，総務大臣，経済産業大臣（2016）.

[15] 一般社団法人JPCERT コーディネーションセンター： JPCERT/CC インシデント報告対応レポート[2012 年1 月1 日 ～ 2016 年12 月31 日]，一般社団法人JPCERT コーディネーションセンター（2012-2017）.

[16] 畠中伸敏： 機密上の保護と情報セキュリティ，日科技連（2016）.

[17] ISO/IEC 27001:2013： Information technology - Security techniques - Information security management systems -Requirements (JIS Q 27001, 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), 日本規格協会（2014).

[18] 日本セキュリティ・マネジメント学会：セキュリティハンドブックⅠ 情報化とリスクマネジメント, 日科技連（1998）.

[19] ISO/IEC 27001:2005：Information technology - Security techniques - Information security management systems -Requirements (JIS Q 27001, 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), 日本規格協会（2006）.

[20] Annex AL of ISO/IEC Directives part1： Proposals for management system standards（Annex SL 和文テンプレート），日本規格協会（2015）.

[21] 中尾康二，中野初美，平野芳行，吉田健一郎： ISO/IEC17799:2005 詳解 情報セキュリティマネジメントの実践のための規範, 日本規格協会（2007）.

[22] 一般財団法人 日本情報経済社会推進協会 (JIPDEC)： 情報セキュリティマネジメントシステム適合性評価制度の概要, 一般財団法人 日本情報経済社会推進協会（2014）.

[23] 中尾宏，内田勝也：情報セキュリティマネジメントシステム(ISMS)認証事業者実態調査,

東京情報大学研究論集, Vol. 17 , No. 2,PP. 125-182（2014 ）.

[24] 江口彰,山田秀：ISO27001 認証の有無による情報セキュリティインシデント事例の比較分析,日本セキュリティ・マネジメント学会誌, Vol. 27, No.1, pp. 3-16（2013）.

[25] 大谷尚通： 発生確率調査と2010 年個人情報漏えい調査の報告，NPO 日本ネットワークセキュリティ協会（2011）.

[26] 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， 情報処理学会，コンピュータセキュリティシンポジウム2012 論文集，pp. 539-546（2012）.

[27] J.Glenn， S.Nunn，W.H.Zeliff. Jr： Computer Attacks at Department of Defense Pose Increasing Risks，U.S. Government Printing Office（1996）.

[28] 佐藤智裕，田中英彦 :インシデント情報を使用した最適なセキュリティ対策の選定，情報処理学会,研究報告コンピュータセキュリティ, Vol. (CSEC) 2015, No. 5, pp. 1-8（2015）.

[29] 一般財団法人 日本情報経済社会推進協会（JIPDEC）情報マネジメント推進センター：ISMS 適合性評価精度に関するアンケート調査報告書， 一般財団法人 日本情報経済社会推進協会（2014）.

[30] 経済産業省：企業における情報セキュリティガバナンスのあり方に関する研究会報告書，経済産業省（2005）.

[31] 経済産業省： 情報セキュリティガバナンス導入ガイダンス， 経済産業省（2009）.

[32] ISO/IEC 27014:2013： Information technology - Security techniques - Governance of information security (JIS Q 27014, 情報セキュリティガバナンス), 日本規格協会(2015).

[33] 財団法人 ニューメディア開発協会： ISMS 認証事業所調査 調査報告書，財団法人ニューメディア開発協会（2010）.

[34] ISO/IEC 27002:2013： Information technology - Security techniques - Code of practice for information security controls（JIS Q27002:2014 情報技術-セキュリティ技術-情報セキ

ュリティ管理策の実践のための規範），日本規格協会（2014).

[35] 一般財団法人 日本情報経済社会推進協会 (JIPDEC)： ISMS ユーザーガイド -リスクマネジメント編-， 一般財団法人 日本情報処理協会, JIP-ISMS113-3.0（2015）.

[36] 打川和男： 最新ISO27001 2013 の仕組みがよくわかる本， 秀和システム（2013）.

[37] 中村逸一： 計算機援用情報セキュリティマネジメントの提案とその評価ー情報セキュリティマネジメントにおける課題を解決する実用的なアプローチー, 静岡大学博士論文 (2004).

[38] R.Bojanc，B.Jerman-Blazic： An economic modelling approach to information security risk management， International Journal of Information Management, No.28, pp. 413-422（2008）.

[39] K.J. Soo Hoo： How Much Is Enough? A Risk-Management Approach to Computer Security， Stanford University（2000）.

[40] 中村逸一，兵藤敏之，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, 2004 年, 情報処理学会論文誌, Vol.45， No.8， pp. 2022-2033（2004）.

[41] 西垣正勝，臼井佑真，山本匠，間形文彦，勅使河原可海，佐々木良一：賠償リスクを考慮した情報セキュリティ対策選定方式の提案と評価, 情報処理学会，情報処理学会論文誌, Vol. 52, No.3, pp. 1173-1184（2011）.

[42] IPA(独立行政法人情報処理推進機構)：企業におけるサイバーリスク管理の実態調査2015, IPA（2015）.

[43] J.R.Westby： How Boards & Senior Executives are manageing cyber risks.，CyLab Carnegie Mellon University（2012）.

[44] 佐々木良一：経営者とサイバーセキュリティ， マカフィ第4 回CIOSummit，講演資料（2016）.

[45] 内閣サイバーセキュリティセンター（NISC）： 企業のサイバーセキュリティに関する

NISCの調査結果（速報）について， 内閣サイバーセキュリティセンター（2016）.

[46] NPO 日本ネットワークセキュリティ協会(JNSA)： 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～， NPO 日本ネットワークセキュリティ協会（2014）.

[47] 大谷尚通:情報セキュリティ投資の費用対効果，高圧ガス, Vol. 49 , No.7, pp.28-33（2012）.

[48] 田中秀幸：情報セキュリティ被害と対策に関する委員会 報告～企業における脅威と被害の新たなモデル構築～， IPA, 情報セキュリティエコノミクス シンポジウム（2013）.

[49] 石川朝久，櫻井幸一：個人情報漏洩補償に関する一検討， 情報処理学会, 情報処理学会コンピュータセキュリティシンポジウム2014, pp. 1185-1191（2014）.

[50] P.Cichonski，T.Millar，T.Grance，K.Scarfone： Computer Security Incident Handling Guide, SP 800-61 Rev2. , National Institute of Standards and Technology (2012).

[51] 永井好和，市川哲彦，長谷川孝博，伊藤賢，三池秀敏，多田村克己：国立大学における情報セキュリティ事故コスト定量化方式， 一般社団法人 経営情報学会, 経営情報学会 全国研究発表大会要旨集 2008 年秋季全国研究発表大会, pp. 1-4（2008）.

[52] 永井好和，市川哲彦，長谷川孝博，小河原加久治，多田村克己： ISMS 導入のための情報セキュリティインシデントコスト定量化について， 国立大学法人情報系センター協議会(NIPC)， 学術情報処理研究編集委員会, No.16， pp. 86-99（2012）.

[53] 土居範久： 情報セキュリティ事典， 共立出版（2003）.

[54] 経済産業省商務情報政策局情報セキュリティ政策室：サイバーセキュリティ経営ガイドライン ～情報化社会を勝ち抜く企業の経営戦略～， 経済産業調査会（2009）

[55] NIST(National Institute of Standards and Technology)： Security and Privacy Controls for Federal Information Systems and Organizations, NIST, SP 800-53 Revision 4（2013）.

[56] NPO 日本ネットワークセキュリティ協会(JNSA)： 2013 年度 情報セキュリティ対策マップ検討WG 活動報告書， NPO 日本ネットワークセキュリティ協会（2014）.

[57] FireEye： Regional advanced threat report: Asia Pacific 1H 2015. Milpitas ， FireEye , Inc.（2015）.

[58] J.Hatta，Y.Ishikawa，H.Kaneko：Research Report on Advanced Persistent Threats in Japan.，LAC Corporation， Cyber GRID View, Vol. 1 （2014）.

[59] D.Caselden, X.Chen, M.Scott, J.Weedon, N.Moran： Operation GreedyWonk: Multiple Economic and Foreign Policy Sites Compromised, Serving Up Flash Zero-Day Exploit.Milpitas，FireEye , Inc.（2014）.

[60] R.H.Girgenti，T.P.Hedley： Managing the Risk of Fraud and Misconduct. New York City（不正・不祥事のリスクマネジメント），日本経済新聞出版社（2012）.

[61] V.Ortiz： Woman Indicted in the Theft of business Secrets， Chicago Tribune. 2008 -4-3（2008）.

[62] Australia’s Defence Signals Directorate： Strategies to Mitigate Targeted Cyber Intrusions, Australian Goverment Department of Defence Intelligence and Security Cyber Security Operation Center（2014).

[63] Australia’s Defence Signals Directorate： Strategies to Mitigate Targeted Cyber Intrusions － Mitigation Details, Australian Goverment Department of Defence Intelligence and Security Cyber Security Operation Center（2014）.

[64] J.A.Lewis： Raising the bar for cybersecurity, the Center for Strategic and International Studies(CSIS)（2013）.

[65] 髙橋雄志，勅使河原可海：国際標準の参照関係に基づくセキュリティ評価方式におけるデータ移行機能の検討， 情報処理学会， 情報処理学会コンピュータセキュリティシンポジウム 2011 論文集, Vol. 2011 , No.3，pp. 666-671（2011）.

[66] 髙橋雄志，勅使河原可海：国際標準の参照関係に基づくセキュリティ評価方式における非専門家への対応策提示機能の検討， 情報処理学会，情報処理学会マルチメディア，分散協調とモバイルシンポジウム2011 論文集, Vol. 2011, pp. 127-134（2011）.

[67] 髙橋雄志，篠宮紀彦，勅使河原可海：セキュリティ標準間の関連情報作成手法の検討とその適応， 情報処理学会， 情報処理学会論文誌コンシューマ・デバイス＆システム（CDS）, Vol. 3, No.4, pp. 22-32（2013）.

[68] 髙橋雄志，篠宮紀彦，勅使河原可海：国際標準に基づいたセキュリティ評価プラットフォームの改善とその適用， 情報処理学会， 情報処理学会マルチメディア，分散協調とモバイルシンポジウム2013 論文集, Vol. 2013, pp. 846-853（2013）.

[69] 宝木和夫，佐々木良一，永井康彦：情報システムにおけるリスク分析の一方法（エキスパートシステム開発技術< 特集>)， 電気学会， 電気学会論文誌 C 電子・情報・システム部門誌, Vol. 108 ， No.4， pp. 260-267（1988）.

[70] 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,情報処理学会論文誌, Vol. 41，No. 8，pp.2264-2271（2000）.

[71] 加藤弘一，勅使河原可海：ネットワーク特別利用時におけるセキュリティと利便性を考慮した最適対策決定手法の提案，情報処理学会，情報処理学会論文誌, Vol. 49, No.9, pp. 3209-3222（2008）.

[72] 永井康彦，藤山達也，荒井正人，柚原直弘：機能的適合性を考慮した情報システムのセキュリティ基本設計法の提案，情報処理学会, 2004 年, 情報処理学会論文誌, Vol. 45, No.4, pp. 1163-1175（2004）.

[73] 呉洋，小崎真寛，岡田謙一：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，情報処理学会論文誌, Vol. 54, No. 1, pp. 309-317（2013）.

[74] 芝口誠仁, 稲場太郎, 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， 情報処理学会論文誌, Vol. 51, No.2, pp. 648-657（2010）.

[75] 相原遼，佐々木良一：イベントツリーとディフェンスツリーを併用したリスク分析における共通事象を考慮したリスク計算法の提案， 情報処理学会，マルチメディア，分散協調とモバイルシンポジウム 2016 論文集, pp. 1062-1067（2016）.

[76] 佐々木良一：コンピュータウイルスに対する疫学的アプローチの提案と評価， 情報処理

学会， 情報処理学会研究報告コンピュータセキュリティ（CSEC）, No.2006-CSEC-034, pp. 291-297（2006）.

[77] 佐藤亮太，間形文彦，高橋克巳，桑名栄二：情報セキュリティの失敗事例における原因の類型化とその対策に関する考察， 情報処理学会，情報処理学会論文誌, Vol. 54, No. 9, pp. 2208-2219（2013）.

[78] 新原功一，原田要之助：情報セキュリティインシデントに対するヒューマンエラー対策の提案，情報処理学会， 情報処理学会論文誌, Vol. 55, No.10, pp. 2318-2326（2014）.

[79] 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，情報処理学会研究報告コンピュータセキュリティ（CSEC）, Vol. 2010-CSEC-48, No.45, pp. 1-8（2010）.

[80] 安藤玲未，芦野佑樹，島成佳： IT システム運用時におけるインシデント分類に関する一考察， 情報処理学会，研究報告セキュリティ心理学とトラスト（SPT）, Vol. 33, No. 2014-SPT-8，pp. 1-5（2014）.

[81] 菅野泰子，寺田真敏，山田安秀，鎌倉稔成，土居範久：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， 情報処理学会論文誌,Vol. 50, No. 9, pp. 2193-2206（2009）.

[82] 畑健一郎，佐藤彰，米田翔一，谷本茂明，佐藤周行，金井敦：情報セキュリティマネジメントシステムにおけるスローポリシー導入に関する検討，電子情報通信学会，電子情報通信学会技術研究報告, Vol. 114, No.389 (ICM2014 32-53), pp. 91-96（2015）.

[83] IPA(独立行政法人情報処理推進機構)： 組織における内部不正防止ガイドライン，IPA（2015）.

[84] 法務省： 会社法， 法務省（2014）.

[85] 町田祥弘： 内部統制の知識（3 版）， 日本経済新聞社出版（2015）.

[86] 日本監査役協会： 監査役実施要領， 日本監査役協会（2011）.

[87] 岡村久道： 会社の内部統制， 日本経済新聞出版社（2007）.

[88] 岡村久道：情報セキュリティの法律[改訂版]， 商事法務（2011）.

[89] 日本監査役協会： 会社法内部統制システムに係る監査役監査活動の概要， 日本監査役協会（2012）.

[90] D.A.Norman： The Psychology of Everday Things（誰のためのデザイン？ー認知科学者のデザイン原論），新曜社（1990）.

[91] 加賀谷哲之： 会計学的アプローチ. (監修) 松浦幹太： セキュリティマネジメント学，共立出版（2011）.

[92] 石黒正揮，村瀬一郎，松浦幹太，田中秀：情報セキュリティ対策による企業価値向上の影響分析， SCI2009 Organizating Commitee， 2009 年暗号と情報セキュリティシンポジウム（SCI2009）, pp.: 2D1-3（2009）.

[93] 小島寛之： サイバー経済学， 集英社（2001）.

[94] 臼井佑真，間形文彦，勅使河原可海，佐々木良一，西垣正勝：事前・事後対策の併用を考慮した2 フェーズ型セキュリティ対策選定方式の提案. 情報処理学会， コンピュータセキュリティシンポジウム2008 論文集, pp. 737-742（2008）.

[95] 松浦幹太：情報セキュリティと経済学， SCIS2003 Organizing Committee, The 2003 Symposium on Cryptography and Information Security(SCIS), pp.475-480（2003）.

[96] L.A.Gordon， M.P.Loeb：The economics of information security investment， ACM Transactions on information and system security， ACM Transactions on information and system security, Vol. 5, No.4, pp. 438-457（2002）.

[97] 石川朝久，櫻井幸一：セキュリティ管理におけるサイバーリスク保険の有効性評価， 情報処理学会，情報処理学会論文誌, Vol. 57 ， No.9， pp. 2088-2098（2016）.

[98] NRI セキュアテクノロジー株式会社： サーバーセキュリティ：傾向分析レポート2014, NRI セキュアテクノロジー株式会社（2014）.

[99] 粕淵卓，西本真弓，富居姿寿子，大森章充：10 の疑問を試して解明 セキュリティ大実験室， 日経BP,，日経NETWORK, 2016 年1 月，pp. 20-21（2016）.

[100] 一般財団法人 日本情報経済社会推進協会（JIPDEC）： ISMS ユーザーガイド， 一般財団法人 日本情報経済社会推進協会， JIP-ISMS111-3.0（2014）.

[101] ISO/IEC 27005:2011：Information technology - Security techniques - Information security risk management，ISO/IEC（2011）.

筆者発表論文

A 学位論文申請資格に関わる論文

堀川博史，大谷尚通， 髙橋雄志，加藤岳久，間形文彦，勅使河原可海，佐々木良一，西垣正勝：デルタ ISMS モデルの提案–事故データベースに基づく ISMS の強化，情報処理学会論文誌,Vol.57, No.9,pp. 2099-2109 (2016).

B 学位論文内容に関わる論文

Hiroshi Horikawa, Hisamichi Ohtani, Yuji Takahashi, Takehisa Kato, Fumihiko Magata, Yoshimi Teshigawara, Ryoichi Sasaki, and Masakatsu Nishigaki : ” Delta ISMS Model to Enhance Company-Wide Information Security Management Using incident Database: The Concept”, IWIN (International Workshop on INformatics), pp.235-241(2016).

C その他の論文

なし

D 口頭発表など

堀川博史，大谷尚通， 髙橋雄志，加藤岳久，間形文彦，勅使河原可海，佐々木良一，西垣正勝：デルタ ISMS モデルの提案–事故データベースに基づく ISMS の強化，情報処理学会研究報告，Vol.2015-CSEC-70, No.24, pp.1-7 (2015).

堀川博史，大谷尚通， 髙橋雄志，加藤岳久，間形文彦，勅使河原可海，佐々木良一，西垣正勝：デルタ ISMS モデル - 事故データベースに基づく全社的情報セキュリティマネジメントの強化 -，日本セキュリティ・マネジメント学会，IT リスク学研究会，2016 年度 第 1 回 IT リスク学研究会（2016）.