情報処理学会論文誌 Vol.57 No.9 2099–2109 (Sep. 2016)

デルタISMSモデルの提案——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

堀川 博史[1] 大谷 尚通[2] 髙橋 雄志[3] 加藤 岳久[4] 間形 文彦[5]
勅使河原 可海[3] 佐々木 良一[3] 西垣 正勝[1]

受付日 2015年12月4日, 採録日 2016年6月2日

概要：本論文は，事故データベースに基づき全社的情報セキュリティマネジメントを強化する「デルタISMSモデル」を提案する．ISMSでは，情報セキュリティインシデントからの学習を求めているが，ISMS認証を取得している組織でも情報セキュリティ事故が減らず，改善が効果的に働かない組織もある．筆者らは改善が効果的に働かない理由は学習の具体的な方法が手順化されていないことにあると考える．そこで本論文では，事故データベースの運用，事故データからの年間予想損失額の算出，事故原因と対策のマトリクスを用いた定期的な対策改善案の選定，対策選定の判断材料となる情報の経営陣への提示からなる一連の方法・手順を解決策として提示する．実担当者の評価，情報セキュリティガバナンスのモニタリング項目との比較，デジタルフォレンジックとの関係の検討を通じ，提案方式の有効性を評価する．

キーワード：情報セキュリティマネジメントシステム（ISMS），事故データベース，情報セキュリティインシデント，リスクアセスメント，情報セキュリティガバナンス

Proposal of Delta ISMS Model – Enhancement to Company-wide Information Security Management Using Accident Database

Hiroshi Horikawa[1] Hisamichi Ohtani[2] Yuji Takahashi[3] Takehisa Kato[4]
Fumihiko Magata[5] Yoshimi Teshigawara[3] Ryoichi Sasaki[3]
Masakatsu Nishigaki[1]

Received: December 4, 2015, Accepted: June 2, 2016

Abstract: In this paper, we propose “Delta ISMS model” which strengthens company-wide information security management using accident database. ISMS requires learning from information security incidents, however, ISMS certified organizations where information securities accidents do not always diminish in number because of ineffective improvements from learning. We recognize insufficiency of the detailing of learning procedures does not make an appropriate improvement. Therefore, we consider detailing of learning procedures is the solution to make appropriate improvements. Regarding detailing of learning procedures, we show a series of such procedures as operation of an accident database, calculation of the annual loss expectation, periodical selection of the countermeasure using a matrix of accidents and countermeasures and offering information to executive for making a decision of countermeasure selection. We evaluate the validity of the proposed system through evaluation by the person in charge, comparison of monitoring by information security governance with those items by the processed Delta ISMS method, and consideration of the relation with digital forensics.

Keywords: information security management system (ISMS), accident database, information security incident, risk assessment, information security governance

[1] 静岡大学
Shizuoka University, Hamamatsu, Shizuoka 432–8011, Japan
[2] 株式会社エヌ・ティ・ティ・データ
NTT DATA Corporation, Koto, Tokyo 135–8671, Japan
[3] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[4] 株式会社東芝
TOSHIBA CORPORATION, Fuchu, Tokyo 183–8512, Japan
[5] 日本電信電話株式会社
NIPPON TELEGRAPH AND TELEPHONE CORPORATION, Musashino, Tokyo 180–8585, Japan

1. はじめに

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，情報セキュリティマネジメントシステム（Information Security Management System: ISMS）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．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事故が減らない事例が見受けられる [1], [2], [3]．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が，改善が効果的に働いていない組織もある．筆者らは，この課題は，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が手順化されていないことが原因だと考える．そこで本論文では，事故データベースの運用，事故データからの年間予想損失額の算出，事故と対策のマトリクスを用いた定期的な対策改善案の選定，対策選定の判断材料となる情報の経営陣への提示からなる一連の方法・手順を「デルタ ISMS」モデルとして具現化する．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 [4] 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．

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 [5], [6] を補強することを目的とする．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持つ経営陣または CISO（Chief Information Security Officer）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．

たとえば，ある企業の創業を想定する．その企業が営業上の理由（たとえば，顧客からの要請や，入札上の要件等）から ISMS 認証取得が必要となった場合，創業の時点で完璧なリスク分析を実施することは不可能といってよいであろう．また，創業後，時間の経過とともに，企業を取り巻く環境や状況は変化していく．これらが，PDCA（plan-do-check-act）サイクルの 2 巡目以降でセキュリティ対策を改善し続けることが重要とされている理由である．ISMS 認証の規格も，ISMS 認証取得組織へ PDCA のアプローチを用いたプロセス管理を基盤とした継続的なセキュリティ対策の改善を求めている．

しかし，現実には ISMS 認証を取得しても情報セキュリティ事故が減らず，ISMS の PDCA サイクルの 2 巡目以降の改善が効果的に働いていない組織が存在する [1], [2], [3]．その理由は，ISMS 認証における情報セキュリティ事故（ISMS 認証の用語ではインシデント）の扱いにあると考える．ISMS 認証はその付属書の中で，情報セキュリティ事故の報告や記録を求めている．ある部署で事故が起きた際には，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，その具体的な手引きを与えていない．このため，ISMS 認証取得組織においても，各部署で発生した事故のデータを「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．

各部署の事故から組織全体の対策改善に資する情報を抽出するための仕組みが不在であるという現状が，マネジメントレビューにおける事故報告の形骸化に直結している．すなわち，事故データがマネジメントレビューとしてトップマネジメントに報告される場合，処置が完了しているか否かの状態が提示されるだけで，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．この結果，情報セキュリティリスク管理に対するトップマネジメントの認識が向上せず，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が生じている．

この問題に対し，本論文では，情報セキュリティ事故データを「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」モデルとして具現化する．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．

情報セキュリティ統括組織は，事故の発生から事故の記録を事故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事故発生部署での 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」を算出する．具体的には，潜在化しているリスクも含め，今回の事故の原因に対して SLE（Single Loss Expectancy：1 回の損害発生における予想損失額）と ARO（Annual Rate of Occurrence：損害の年間予想発生回数）を見積もり，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，事

故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（たとえば半年に1度）に事故データベースを精査し，当該期間に発生した事故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，事故原因と対策のマトリクスである「デルタISMS表」を用い，対策の導入コストと効果に応じて対策候補の案を複数（たとえば，上中下の3パターン）導出し，トップマネジメントが経営戦略に応じて最適な対策を選択できるようにする．また，推奨案として，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もできる．

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表とともに複数の対策候補案を提示する．トップマネジメントは，この情報を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，組織のISMSと情報セキュリティガバナンスを結合し，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させていく．

これらの一連の方法・手順が「デルタISMS」である．以下，2章では従来のリスク分析，ISMSおよび情報セキュリティガバナンスの関連研究をまとめる．3章では，デルタISMSの背景とアプローチをより詳しく説明する．4章ではデルタISMSの内容を手順に従って詳述する．5章で実担当者の評価，情報セキュリティガバナンスのモニタリング項目との比較，デジタルフォレンジックとの関係の検討を通じ，デルタISMSの有効性を評価する．6章でまとめる．

2. 関連研究

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[4]．リスクとは目的に対する不確かさの影響のことである[7]．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とられている[8]．ALEは

$$ALE = SLE \times ARO$$
$$SLE = AV \times EF$$

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．

情報セキュリティ事故はISMS認証の規格の中では情報セキュリティインシデントとよばれる．情報セキュリティインシデントとは，事業運営を危うくする確率および情報セキュリティを脅かす確率の高い事象を指す[7]．リスクは，情報セキュリティインシデントとして表出し，その度合いによっては事故として扱われる．Robertoは優れたリーダは問題を脅威と見なしておらず，すべての問題は改善と学習の機会だと考えており，インシデント報告制度を進展すべきことを述べている[9]．情報セキュリティインシデントに対しては他分野での各種インシデント対策手法が取り組まれている[10], [11], [12], [13]．

事故は，原因と損害額のプロパティを持つ．原因について，JNSAは情報漏えい原因区分の10種を定義している[14]．JNSAは，事故データベースを一般公開する活動も実施している．公開データベースに蓄積される情報は，公表や報告が求められるレベル以上の事故のみとなっている．損害額については，大谷は，損害額が直接損害額と間接損害額に加え，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ている[15]．

多くの組織がリスク分析時に詳細リスク分析手法を利用している[16]．加えて，組織固有の情報セキュリティ事故からリスク分析を実施することもできる[17], [18]．本論文では，筆者らが文献[18]で示した事故データベースに基づくセキュリティ対策選定方法を利用している．なお，対策選定の定式化は中村らの手法[19]を参考とした．

中尾らはISMS認証取得事業所からのアンケートをまとめており，本論文におけるISMSの現状の問題は中尾らの報告[1], [2]および江口らの評価[3]を参考にしている．また，ISMSをより実効的なものにするために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が経済産業省によりガイダンスとして提唱された[5]．このガイダンスは国際規格化の後にJIS規格となった[6]．IPAも経営陣におけるリーダーシップの強化をISMSの重要な項目の1つとしている[20]．

3. 既存のISMSの問題の原因と解決方法

ISMS認証を取得している組織でも情報セキュリティ事故が減らない場合があるという問題から，その温床となっている原因を考察するとともに，その問題を解決するための方法を検討する．

3.1 情報セキュリティ事故が減らない原因

ISMS認証を取得しても事故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[3]．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[1], [2]．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，その組織で事故が起きているか否かを判読したところ，事故が起きている組織が19件中11件という結果であった．

ISMS 規格の付属書の中で，事故から得られた知識は事故が将来起こる可能性や影響を低減させ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）．要求どおりに対応すれば事故を減らせることになるが，実態は事故が減らない組織があり，それは，事故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．事故を減らせない組織に事故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事故を減らす方法と考える．

3.2 組織内の事故データベースの活用

3.1 節に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事故データベースを運用し，事故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．事故（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事故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．

情報セキュリティ統括組織は，事故発生部署での 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うえで，今回の事故の原因に対して 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）を見積もり，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，事故データベースに保存する．

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 のフェーズで事故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事故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，事故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ができる．デルタ ISMS 表については次章で詳述する．

3.3 情報セキュリティガバナンスの必要性

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 [5]」では，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，企業の経営陣において情報資産に係るリスクの管理を狙いとし，情報セキュリティに係る意識，取組みおよ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．

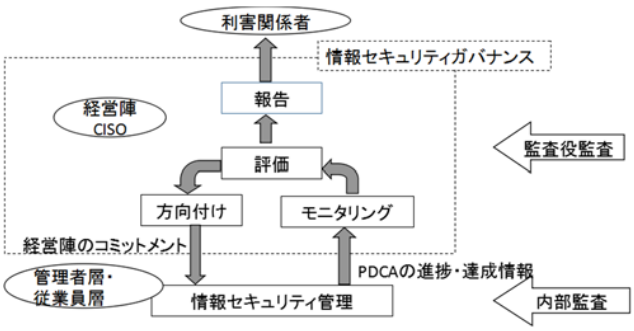

図 1 情報セキュリティガバナンスのフレームワーク [5]
Fig. 1 Framework of information security governance [5].

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，組織として全体最適化された情報セキュリティリスク管理の構築・運用がなされないという問題があった．このガイダンスは，この問題への対処指針となっている．**図 1** 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確立とは，図 1 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・従業員層にとどまりやすい．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．

3.4 ISMS と情報セキュリティガバナンスの乖離

情報セキュリティガバナンスを成功に導くには，ISMS の PDCA サイクルに対する経営陣の理解と関与が欠かせない．ISMS 認証取得事業所へのアンケート [1] によると，「ISMS 認証の運用責任者が経営陣の一員である」の割合が 78.9%，「経営陣のマネジメントレビュー以外での ISMS への関与」が 82.4%といずれも高い結果となっており，これらは，経営陣の関与によって ISMS の PDCA サイクルが好循環していることを示すデータととらえることができる．しかし，その一方で，「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，「費用対効果の説明手法」と「経営者の認識・理解の向上」についてはそれぞれ 3 年連続で 11 項目中 11 位と 10 位となっている．つまり，管理者・従業員層から経営陣に向けての情報提供が十分に達成できていないことがうかがえる．

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」という事故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とどまってしまう．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．

3.5 ISMS と情報セキュリティガバナンスの結合

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 のフェーズにおいて，全組織として新たに採用すべき対策の候補を複数（たとえば，上中下の 3 パターン）導出することが可能となっている．このため，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トップマネジメントに提示することができる．トップマネジメントは，この情報を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，組織の ISMS と情報セキュリティガバナンスの結合が達成される．

4. デルタ ISMS モデルと PDCA サイクル

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事故データを使って，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 2**）．

4.1 事故の対応

組織内で事故が発生した場合，デルタ ISMS では，従来の ISMS 規定 [4] 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，3 次対応までを行う．なお，1 次対処と 2 次処置が事故発生部門で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ときに行われる．

- 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）

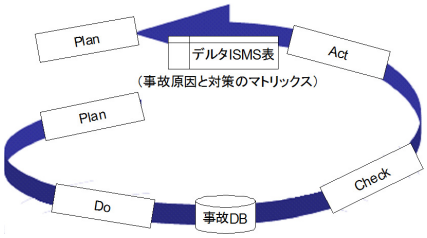

図 2 デルタ ISMS モデル
Fig. 2 Delta ISMS model.

  - 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，またはそれが発生する可能性を明確にする．
  - 是正処置する（将来起こる可能性またはその影響を低減させる）．
  - 有効性をレビューする．
- 3 次対応（組織全体としての対応）
  - 事故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 [19]．たとえば，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」と区分する．3 次対応においてもこの方法をとることができる．ALE は SLE × ARO であり，計算をするときは，それぞれの値の中間値を用いる．

4.2 事故データベースの運用

情報セキュリティ統括組織は，4.1 節で説明した事故対応の結果を，事故データベースに登録・蓄積してゆく．登録は事故対応の直後に行う．事故データベースは，日時，事故内容，事故原因，事故経路，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 1** に事故データベースの諸元を示す．

事故はリスクが顕在化した事象である．事故データベースは単なる「事故の事実」のみを羅列したものにとどまらず，その事故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．

事故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事故を記録・蓄積する．また，リスクの洗い出しのためには，事故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 つに区分できる．

表 1 事故データベース
Table 1 ccident database.

列名	意味
日時	事故の発生した日時.
事故内容	事故の内容（自由書式）.
事故原因	事故原因を次の 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
事故経路	事故の経路を次の 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・ハットから大事故まで.
1 次対処	1 次対処の内容.
1 次対処の被害額	事故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.

- 組織の規則や記録等の文書に係る項目
- リスクアセスメントやパフォーマンス評価等 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，有効に事故データベースに取り込める．

4.3 組織のセキュリティ対策の改善案の選定

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 のフェーズで事故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事故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．

事故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させることができる．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」という事故原因と対策のマトリクスを作成する．

表 2 がデルタ ISMS 表である．ここで，

- LP_j：その事故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%）.
- S_i：各対策の有無（0 or 1）.
- C_i：対策のコスト.

である．

デルタ ISMS で使用する事故ベースのリスクアセスメントにおいて最も投資効果の高い対策の選択は，式 (1) の値 E_Δ が最も大きくなる対策の選択として表される．式 (1) の定式化は，中村らの手法 [19] を参考としている．詳細については，文献 [19] を参照されたい．

表 2 事故原因と対策のマトリクス（デルタ ISMS 表）
Table 2 Matrix of accidents and countermeasures (Delta ISMS table).

事故原因	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	LP_1	R_{11}	R_{12}	・・・	R_{1i}
2	LP_2	R_{21}	R_{22}	・・・	R_{2i}
・	・	・	・	・	・
・	・	・	・	・	・
・	・	・	・	・	・
j	LP_j	Rj_1	Rj_2	・・・	R_{ji}

表 3 対策選択による ALE の低減の例
Table 3 Example of reduction in ALE by choosing control.

	対策	対策1	対策2	・・・	対策n
		設定変更	ストラップ	・・・	暗号化ソフト
事故原因	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	250万円	0%	30%	・・・	40%

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

対策は次の 3 種に区別できる．

- 組織全体に対してすで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 (1) を用い，事故発生部署に対して 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 [21] や米国国立標準技術研究所の NIST SP800-53 [22] 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．たとえば，上中下の 3 パターンを用意する場合は，高コストで効果の高い対策案（たとえば，新たな情報セキュリティシステムの導入による対策）が「上」，低コストで効果の低い対策案（たとえば，教育等での注意喚起による対策）が「下」，その中間の対策が「中」となる．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 [7] 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**表 3** に示す．表 3 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．なお，表3のコストとALEは，企業規模，業態，物価等により変化しうる．

4.4 経営陣による改善対策案の決定

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，4.3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トップマネジメントに提示する．トップマネジメントは，デルタISMS表と式(1)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」として利用し，情報セキュリティ統括組織から提示された複数の対策候補案の中から対策を選択する．この結果，経営戦略に合致した形で組織全体のセキュリティ対策の改善が達成される．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，組織のISMSと情報セキュリティガバナンスの結合が実現する．

4.5 デルタISMSによるスパイラルアップ

図3に，デルタISMSの繰返しによる組織のセキュリティ強度のスパイラルアップを示す．デルタISMSによって事故データの前巡比較（差分）に注目することによって，ISMSの継続的改善のために重要となる「複数巡回における事故データのトレンドの観察」も容易となる．

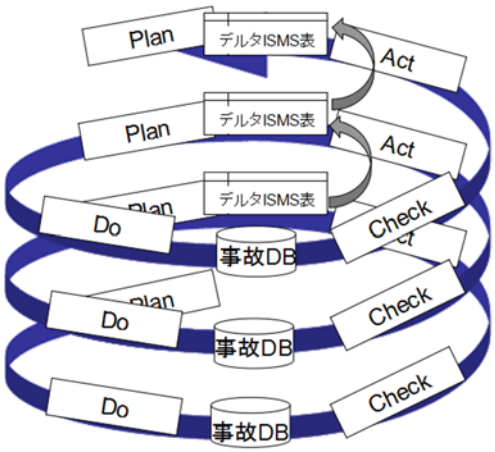

図3 デルタISMSモデルの繰返し
Fig. 3 Repeat of Delta ISMS model.

5. デルタISMSモデルの評価

本章では，実担当者へのインタビュー，情報セキュリティガバナンスのモニタリング項目とデルタISMSの情報との比較，および，事故データベースとデジタルフォレンジックの親和性の検討を行う．

5.1 事故データから対策を導出する手法

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，実際の事故データ（2013年度の事故数：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．事故データベースのサンプルを**表4**に，デルタISMS表のサンプルを**表5**に示す．

表5のデルタISMS表の最左列の「事故」は，表4の事故データベースにおいて事故経路と事故原因が同一のものをまとめている．上部の「対策」には，事故に対する対策案の候補を列挙している．このうち，対策1〜6は，当該組織ですでに実施中の対策である．対策7〜9は，事故データベースにある事故発生部門で実施した対策や事故原因等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が記入されている．「ALE」は，事故データベースの1次対処の実績被害額と2次処置の対策コストを加算することで算出できる．ただし，実績額を使うと結果が敏感すぎるため，4.1節で示した「段階の数値」で丸めている．

事故が発生する前のリスク分析においては，当該組織内にて実際に事故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事故が並べられるので，現実の数値を用いての評価が可能である．同様に，事故が発生する前のリスク分析においては，事故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，類型的な対策をあ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事故が並べられるので，具体的な事故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

表4 事故データベースのサンプル（部分）
Table 4 Sample of an accident database (part).

日時	事故内容	事故原因	事故経路	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）

表 5 デルタ ISMS 表のサンプル（部分）
Table 5 Sample of delta ISMS table (part).

		対策済						上	中	下
	対策	1 使用前ロックを設定する	2 履歴を残さない設置にする	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 移動時チェックシステムを導入する	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
事故	コスト（万円） / ALE	100	50	80	20	20	30	1200	300	110
携帯電話紛失	2500万円	0.3	0.3	0.2	0.1	0	0.3	0.6	0.6	0.05
セキュリティカード紛失	2500万円	0	0	0	0.1	0.3	0.3	0.6	0	0.05
紙資料紛失	250万円	0	0	0.2	0	0	0	0.6	0	0

チューニングしていくことができる．

なお，表 5 に対して式 (1) を用いて離散最適解を求めると，対策 1〜6 と 8 の組合せで投資対効果が最大となった．対策 1〜6 と 8 の組合せは数値に裏付けられた推奨案となる．

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『本論文 4 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，手法の妥当性が確認された．

5.2 デルタ ISMS と情報セキュリティガバナンスとの比較

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（事故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．

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した 15 項目の関連を図 4 に示す．このうち経営陣と CISO がとも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 と経営陣の間で共有すべき情報として余分がないことを見ることができる．つまり，デルタ ISMS 表は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．デルタ ISMS 表は情報セキュリティガバナンスのモニタリング項目のうち，次をカバーしている．

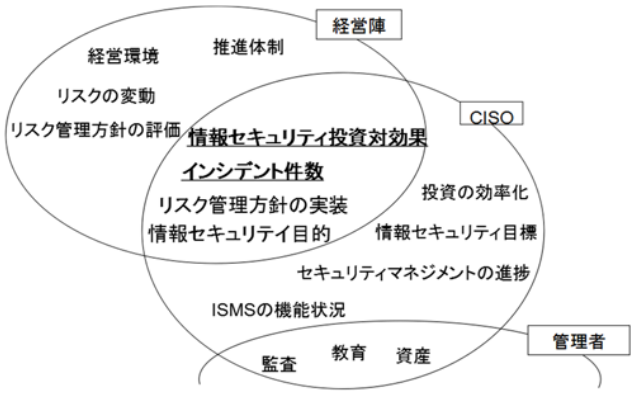

図 4 情報セキュリティガバナンスにおけるモニタリング項目
Fig. 4 monitoring items in the information security governance.

- 新規の管理策：投資対効果が検討されたか
- 情報セキュリティ投資効果
- リスク分析の結果に照らして情報セキュリティ投資は効率的かつ効果的か
- リスク分析の結果に照らして期待されるリスク低減の効果が発揮できているか
- インシデント報告件数は低減できているか
- インシデントの被害額は低減できているか

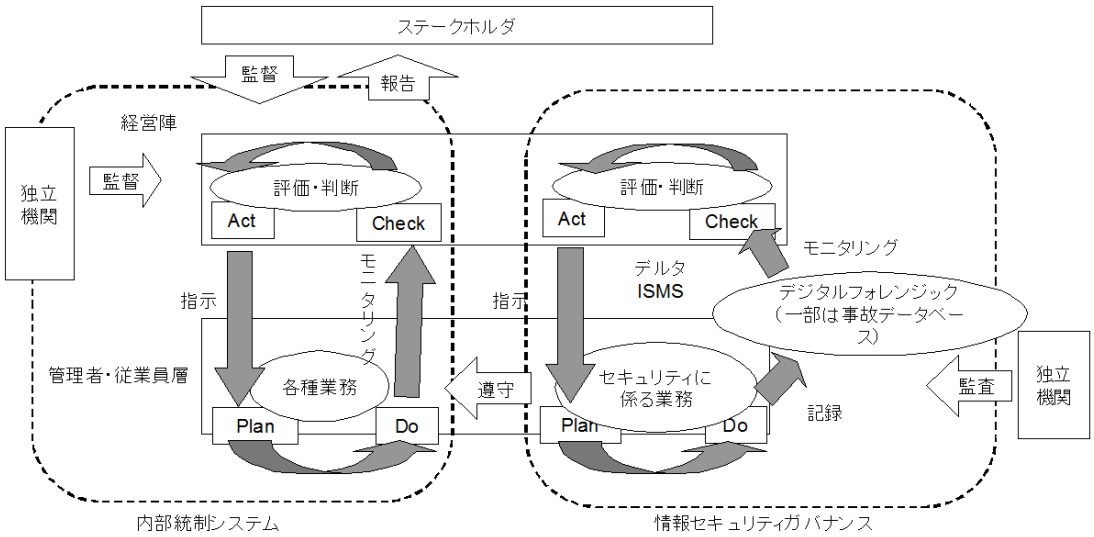

図 5 デジタルフォレンジックを用いたデルタ ISMS
Fig. 5 Delta ISMS using digital forensics.

5.3 事故データベースとデジタルフォレンジック

デルタ ISMS を実施するためには，組織内で事故データベースを運用することが必要となる．その情報を活用して経営陣が現在のセキュリティ対策の Check（評価）および Act（改善）を実施する．各部署のセキュリティに係る業務に事故が発生したら，その情報をデータベースに遅漏なく登録することになる．ここで，内部犯行の抑止力として，または，訴訟対策として日常業務のログをとっている組織も少なくない．デジタルフォレンジック [23] の定常的なログの記録が，実際に発生した事故をデータベース化することにもなっていると効率が良い．このように，デジタルフォレンジックの仕組みの一部を，デルタ ISMS の事故データベースとして用いることができる．

以上を総合すると**図 5** のようになる．

6. まとめ

本論文において，情報セキュリティ事故を減らすため，事故データから対策を導出する手法として，組織で実際に発生した事故データベースに基づき，デルタ ISMS 表を用いて全社的な情報セキュリティ改善策を導出する手法を提示した．提案方式に対し，実担当者の評価も得られた．デルタ ISMS 表と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比較することで，デルタ ISMS 表が提供する情報が CISO 等と経営陣の間で共有すべき情報として余分がないことを確認した．

今後，提案方法の普及活動とともに，提案方式の適用によって実際に事故が減るかの追跡調査が必要である．また，デルタ ISMS 表を実施に使用する CISO 等，情報セキュリティ統括組織，さらには経営陣に対して，デルタ ISMS 表の分かりやすさをインタビューで検証していく．事故データベースとデジタルフォレンジックの融合では，情報システムのログから事故を発見する技術も進展しており（たとえば，SIEM（Security Information and Event Management）は，ファイアウォール，プロキシーサーバ，IDS/IPS 等のセキュリティ機器のログを取得し，それらの相関分析から多角的に攻撃検知を行う），事故とログ解析技術のマッピングを作成することから始めていきたい．

参考文献

[1] 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).
[2] ニューメディア協会：ISMS 認証事業所調査 調査報告書 (2010).
[3] 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).
[4] JIS Q 27001:2014：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).
[5] 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 (2009).
[6] JIS Q 27014:2015：情報セキュリティガバナンス，日本規格協会 (2015).
[7] JIS Q 27000:2014：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).
[8] Bojanc, R. and Jerman-Blazic, B.: An economic modelling approach to information security risk management, *International Journal of Information Management*, No.28, pp.413–422 (2008).
[9] Roberto, M.A.: *Know what you don't know*（なぜ危機に気づけなかったのか），英治出版 (2010).
[10] 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，情報処理学会論文誌，Vol.54, No.9, pp.2208–2219 (2013).
[11] 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：電子情報通信学会技術研究報告，Vol.113, No.502 (ICSS2013 62-94),

pp.191–195 (2014).
[12] 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，情報処理学会論文誌，Vol.55, No.10, pp.2318–2326 (2014).
[13] 村上　靖，内田勝也：情報セキュリティ事件・事故の分析と対策に関する考察，情報処理学会研究報告，Vol.2010-CSEC-48, No.45, pp.1–8 (2010).
[14] 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).
[15] 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).
[16] 財団法人日本情報処理協会（JIPDEC）：ISMS ユーザガイド—リスクマネジメント編，財団法人日本情報処理協会 (2008).
[17] 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，Vol.2015-CSEC-68, No.5, pp.1–8 (2015).
[18] 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).
[19] 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，情報処理学会論文誌，Vol.45, No.8, pp.2022–2033 (2004).
[20] 独立行政法人情報処理推進機構（IPA）：組織における内部不正防止ガイドライン (2015).
[21] 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).
[22] Ross, R. et al. (NIST): Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 800-53 Revision 4 20JIS Q 0073，リスクマネジメント—用語，日本規格協会 (2010).
[23] 佐々木良一，舟橋　信，安冨　潔：デジタル・フォレンジック事典，日科技連 (2014).

堀川 博史　（正会員）

1978 年名古屋工業大学情報工学科卒業．1980 年北海道大学大学院工学研究科情報工学専攻修了．同年三菱電機株式会社入社．現在，静岡大学創造科学技術大学院博士課程にて情報セキュリティを研究中．三菱電機インフォメーションネットワーク株式会社所属．情報セキュリティスペシャリスト，情報セキュリティアドミニストレーター．

大谷 尚通　（正会員）

1998 年山梨大学大学院電子情報工学科修士課程修了．同年 NTT データ入社．現在，NTTDATA-CERT 所属．ネットワークセキュリティ，セキュリティ被害の定量化，マルウェア解析，フォレンジック等の研究開発に従事．

髙橋 雄志　（正会員）

2001 年創価大学工学部情報システム学科卒業．2003 年同大学大学院工学研究科情報システム工学専攻博士前期課程修了．2014 年同大学院博士後期課程修了，博士（工学）．現在，東京電機大学総合研究所複合領域サイバー・セキュリティプロジェクトサイバーセキュリティ研究所研究員．情報セキュリティマネジメントの研究に従事．日本セキュリティ・マネジメント学会会員．

加藤 岳久　（正会員）

1989 年信州大学工学部卒業．1991 年同大学大学院修了．同年株式会社東芝総合研究所入社．符号理論，情報セキュリティの研究に従事．2013 年静岡大学創造科学技術大学院博士課程修了．博士（情報学）．現在，株式会社東芝インダストリアル ICT ソリューション社にて情報セキュリティ研究に従事．電子情報通信学会会員．

間形 文彦　（正会員）

1992 年中央大学法学部法律学科卒業．同年日本電信電話株式会社入社．現在，NTT セキュアプラットフォーム研究所に所属．社会科学と情報工学の境界領域から情報セキュリティの研究に従事．日本セキュリティ・マネジメント学会，情報ネットワーク法学会各会員．技術士（情報工学）．

勅使河原 可海 （正会員）

1970 年東京工業大学大学院理工学研究科博士課程制御工学専攻修了．工学博士．同年日本電気入社．コンピュータネットワーク，ネットワークアーキテクチャ，衛星データネットワーク等の開発に従事．1994～1996 年ハワイ大学アロハシステム客員研究員．1995 年創価大学工学部教授，工学部長，工学研究科長を歴任．2013 年東京電機大学未来科学部およびサイバーセキュリティ研究所研究員，現在に至る．ユビキタスコンピューティング，グループウェア，e-learning，ネットワークセキュリティ等の研究に従事．情報処理学会，オペレーションズリサーチ学会各フェロー，電子情報通信学会，日本セキュリティ・マネジメント学会，経営情報学会，IEEE，ACM 各会員．本会フェロー．

佐々木 良一 （正会員）

1971 年東京大学卒業．同年日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001 年より東京電機大学工学部教授，2007 年より未来科学部教授．工学博士（東京大学）．1998 年電気学会著作賞受賞．2002 年情報処理学会論文賞受賞．2007 年総務大臣表彰等．著書に，『IT リスクの考え方』（岩波新書，2008 年）等．日本セキュリティ・マネジメント学会会長，内閣官房サイバーセキュリティ補佐官．本会フェロー．

西垣 正勝 （正会員）

1990 年静岡大学工学部光電機械学科卒業．1995 年同大学大学院博士課程修了．日本学術振興会特別研究員（PD）を経て，1996 年静岡大学情報工学科助手．同講師，助教授の後，2010 年より同大学創造科学技術大学院教授．博士（工学）．情報セキュリティ全般，特にヒューマニクスセキュリティ，メディアセキュリティ，ネットワークセキュリティ等に関する研究に従事．2013～2014 年情報処理学会コンピュータセキュリティ研究会主査．2015 年より電子情報通信学会バイオメトリクス研究専門委員会委員長．