Vol.2015-CSEC-70 No.24
Vol.2015-SPT-14 No.24
2015/7/3

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 －

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[†6]

本稿では事故データベースに基づき ISMS を強化する「デルタ ISMS モデル」を提案する．組織の情報セキュリティマネジメントを進めるうえで経営陣の関与は重要であるが，従来，「費用対効果の説明手法」や「経営者の認識・理解の向上のための手法」の改善は十分でなかったという課題に対して，組織で実際に発生した事故データベースに基づき，経営陣と管理者・従業員層が共有できる KPI を提供することで，経営陣の情報セキュリティマネジメントの関与を促し，組織全体の PDCA サイクルの実現を目指す．事故データベースに基づくリスクアセスメント情報セキュリティガバナンスの経営陣と CISO 間のモニタリング項目に対して余分な情報がないことを示す．デルタ ISMS が提供する情報は経営陣に対して状況や課題を的確に示すことで理解を促進させることができ，リスク管理方針の評価に有用な情報となる．

Proposal of a Delta ISMS model
- Enhancement to ISMS 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[†6]

1. はじめに

組織の情報セキュリティマネジメントを進めるうえで経営陣の関与は重要であるが,従来,「費用対効果の説明手法」や「経営者の認識・理解の向上のための手法」の改善は十分でなかった．本稿で提案するデルタ ISMS（情報セキュリティマネジメントシステム）モデルは，事故データベースに基づくリスクアセスメントであり，経営陣と管理者・従業員層が共有できる KPI（Key Performance Indicator）を提供でき，組織での情報セキュリティガバナンスの構築・運用の実現に効果が期待できる．本稿では，デルタ ISMS が提供する情報が，経営陣に対して状況や課題を的確に示すことで理解を促進させ，リスク管理方針の評価が容易になることを示す．

2. 経営陣の情報セキュリティマネジメントへの関与

本章では,組織の情報セキュリティマネジメントを進めるうえで経営陣の関与は重要であるが，従来,「費用対効果の説明手法」や「経営者の認識・理解の向上のための手法」の改善は十分でないという課題を述べる．

2.1 情報セキュリティガバナンス

経済産業省の「情報セキュリティガバナンス導入ガイド[1]」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（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．本ガイドは，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フレームワークは，「方向付け」「モニタリング」「評価」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 1 の活動を企業内に実装していくこととなる．

経営陣と管理者・従業員層の ISMS の調整という課題は

†1 静岡大学大学院　（博士課程）
Shizuoka University
†2 NTT データ
NTT DATA CORPORATION
†3 東京電機大学
Tokyo　Denki　University
†4 東芝
TOSHIBA CORPORATION
†5 NTT
NTT
†6 静岡大学大学院
Shizuoka University

Vol.2015-CSEC-70 No.24
Vol.2015-SPT-14 No.24
2015/7/3

経営陣と管理者層との間をつなぐための役割を CISO（Chief Information Security Officer）が担う．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．

情報セキュリティガバナンス導入ガイドは，企業の情報セキュリティ管理手法の国際標準 ISO/IEC27001[2]の中の「リーダシップ及びコミットメント」と「マネジメントレビュー」について明確化したもので，ISO/IEC27001 を補完する位置付けとしている．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．一般に図 2 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）サイクルに対して傍観的な位置づけとなっている．

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[3]」においても情報セキュリティガバナンス導入ガイドと同様に経営層におけるリーダシップの強化が重要な項目の一つとなっており，会社法[4]の内部統制の体制を参照している．

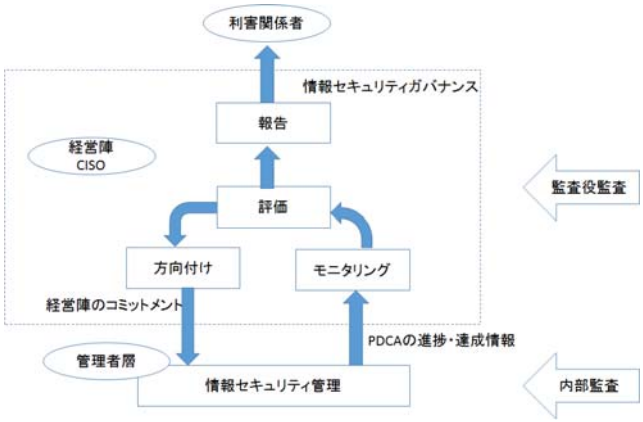

図 1　情報セキュリティガバナンスのフレームワーク[1]

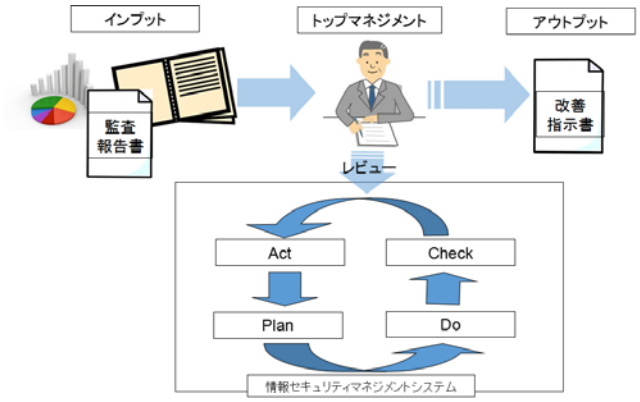

図 2　ISMS のマネジメントレビュー

2.2　会社法の内部統制システム

本節では会社法の内部統制システムを概観する．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[5]．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．内部統制システム[6]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．

2.3　２つのシステムの比較と ISMS の課題

図 3 は２つのシステムにおける 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．

Vol.2015-CSEC-70 No.24
Vol.2015-SPT-14 No.24
2015/7/3

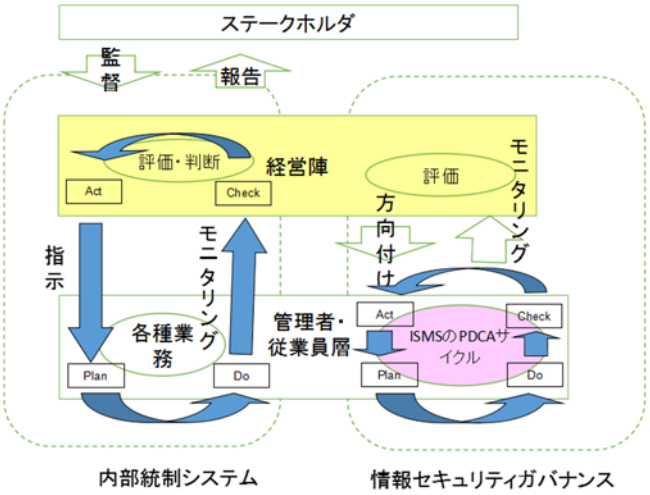

図 3　内部統制システムと ISMS

2.4 ISMS の現状

ニューメディア協会の「ISMS 認証事業所調査　調査報告書[7]」に「ISMS の継続的な運用のための経営陣のマネジメントレビュー以外での ISMS への係り」が 81%と高く，ISMS においても経営陣に跨る PDCA サイクルが好循環していることを示すデータがある．このデータは「ISMS 認証の運用責任者が経営陣の一員である割合」が 67%と高いことが要因と考えられる．「ISMS の効果を高めるため重点的に取り組んでいるもの」の調査では，ISMS の運用を成功に導くには経営陣の理解が欠かせないにもかかわらず，「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 11 項目中 11 位と 10 位となっており，ほとんど取り組まれていない結果となっている．つまり，ISMS における良好な PDCA サイクルを形成するための手法などの検討は十分でなく，CISO の個人能力に依存する形で ISMS の好循環 PDCA サイクルが進んでいることが伺える．

本稿では，CISO が経営陣に ISMS の，プロセスの中で作成される成果物が経営陣と管理者・従業員層が共有できる KPI となることで，経営陣が情報セキュリティマネジメントの状況や課題を的確に示すことで理解を促進しやすくするモデルを提案する．

3. デルタ ISMS モデル

本章では，組織の情報セキュリティマネジメントを進めるうえで経営陣の関与は重要であるが，従来，「費用対効果の説明手法」や「経営者の認識・理解の向上のための手法」の改善は十分でなかったという課題に対して，組織で実際に発生した事故データベースに基づき，経営陣と管理者・従業員層が共有できる KPI を提供することで，CISO の個人能力に依存せず，経営陣の情報セキュリティマネジメントの関与を促すデルタ ISMS モデルを提案する．

3.1 事故データベースに基づくリスクマネジメント

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， PDCA サイクルの 2 巡目以降で ISMS を改善していく．デルタ ISMS のデルタとは，初期サイクルと 2 巡目以降のサイクルの差分を指す．

次にデルタ ISMS の特徴を示す．

（1）計測された値による信頼度の向上

1 巡目のリスクアセスメントで，想定される脅威または攻撃とその発生確率及び想定される被害額に基づいて評価する．これらの値は組織内で計測されたものではないので，いわゆる世間一般に知られている知識に基づくため，計測された値に比べると信頼度が低い．事故データを用いたデルタ ISMS は，実際に自組織で発生した被害を入力として評価するため，2 巡目以降で，経営陣への説明が容易で，理解し易いものとなる．

（2）検知の対策による効果

対策の中には脅威を検知するための物もある．検知の対策を施すと従来表面化しなかった脅威，攻撃または事故が表出することがある．これらの脅威，攻撃または事故に対する対策は 1 巡目では対応できず，2 巡目以降に対策が可能となる．

（3）組織ごとのチューンアップ

自組織内で実際に起きた事故や被害のデータを使って対策を改善していくので,それぞれの組織に応じた形で ISMS をチューンアップすることができる．

（4）定量的な改善効果

組織で実際に起きている事故に対処するデルタ ISMS では投資の効果が明確になる．

表 1 に事故データベースの列名と意味を示す．このデータベースに各事故が各行として登録・蓄積してゆく．

2 巡目で，セキュリティ対策検討時に，図 4 に示す事故原因と対策のマトリックス（以下，デルタ ISMS 表とよぶ）を使用する．デルタ ISMS 表の項目は次の意味を持つ．

事故原因：事故データベースの事故原因×事故経路．

被害額：同一事故原因の被害額平均を事故データベースより記載する（単位は円）．

頻度：事故の発生頻度（年間発生件数）．

対策：考えられる事故対策．

コスト：その対策を選択した場合のコスト（単位は円）．

対策による被害額（頻度）軽減率：その対策による被害額（または発生頻度）軽減率（0%～100%）．

デルタ ISMS 表では事故データベースの各事故を同一事故原因で束ねるため，事故データベースの事故内容を転記しない．これは，なるべく攻撃者への有用情報としないための配慮にもなる．

デルタ ISMS 表の上辺に並べる対策は，JIS Q27002:2014

[8]や米国国立標準技術研究所の NIST SP800-53[9]といった情報セキュリティ対策集より転記して列挙することとなる．

表 1　事故データベース

列名	意味
日時	事故の発生した日時。発生した日時が不明な場合は期間を判明した日時と合わせて記載する.
事故内容	事故の内容を自由書式で記載する.
事故原因	事故原因。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
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、再発防止策に掛かった費用は含めない.

		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	被害額	頻度	200万円	80万円	・・・	400万円
メール誤送信	2百万円	13件	30%	0%	・・・	15%
携帯電話紛失	4百万円	9件	0%	10%	・・・	0%
⋮	⋮	⋮	⋮	⋮	・・・	⋮
USBメモリ紛失	9百万円	3件	0%	10%	・・・	40%

図 4　事故原因と対策のマトリックス（デルタ ISMS 表）

3.1.1 公表されている事故データベース

事故データベースには組織内のローカルなデータベースと一般に公開されているデータベース[10][11]の 2 種類がある．

ローカルの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が記録・蓄積されるのに対して，公開データベースに蓄積される情報はその一部（公表や報告が求められるレベル以上の事故のみ）となる．

1 巡目の PDCA サイクルの時は, 特に組織が新たにできたばかりの時は，組織内のデータベースには事故情報は溜まっていないため，資産に基づくリスクアセスメントに変えて（あるいは加えて）公開データベースを使ってデルタ ISMS のセキュリティアセスメントの手法を用いて対策を立てることもできる．

3.2 従来の ISMS 手法との比較

ここでは 3.1 事故データベースに基づくリスクマネジメントを従来の ISMS 手法と比較し，違いを明らかにする．

3.2.1 資産ベースのリスクアセスメント

表 2 と表 3 は従来の資産ベースのリスクアセスメントを説明する表である[12]. 情報セキュリティリスクは, 資産, 脅威, ぜい弱性に基づいて特定することが要求されていた．事故ベースのリスクアセスメントを行う場合でも 1 巡目の PDCA サイクルでは，事故データが無いため，資産ベースのリスクアセスメントを行う必要がある．

表 2 は脅威と資産の表であり，表 3 は脅威と対策の表である．ここで,

Vk:資産価値.

Ejk:その脅威が発生した時のそれぞれの資産への影響（0or1）.

Pj:脅威の発生確率.

Rji:その対策により低下する脅威の発生確率.

Si:各対策の有無（0or1）.

Ci:対策のコスト.

である．

もっとも投資効果の高い対策の選択は, 式 1 の値 E_0 が最も大きくなる対策の選択として表される．

式 1：

$$E_0 = \sum_k \left\{ V_k \prod_j \left[1 - E_{jk} P_j \prod_i \left(1 - R_{ji} S_i \right) \right] \right\} - \sum_i C_i S_i$$

表 2　脅威と資産の表[12]

	資産$_1$ V_1	資産$_2$ V_2	…	資産$_K$ V_K
脅威$_1$ P_1	E_{11}	E_{12}	…	E_{1K}
脅威$_2$ P_2	E_{21}	E_{22}	…	E_{2K}
⋮	⋮	⋮	⋱	⋮
脅威$_J$ P_J	E_{J1}	E_{J2}	…	E_{JK}

表 3　脅威と対策の表[12]

	対策$_1$ C_1	対策$_2$ C_2	…	対策$_I$ C_I
脅威$_1$ P_1	R_{11}	R_{12}	…	R_{1K}
脅威$_2$ P_2	R_{21}	R_{22}	…	R_{2K}
⋮	⋮	⋮	⋱	⋮
脅威$_J$ P_J	R_{J1}	R_{J2}	…	R_{JK}

3.2.2　事故ベースのリスクアセスメント

表 4 はデルタ ISMS 表である．事故ベースのリスクアセスメントは 2 巡目以降の PDCA サイクルで行われるものである．ここで

Vol.2015-CSEC-70 No.24
Vol.2015-SPT-14 No.24
2015/7/3

Lj:その事故原因が発生した時の被害額.
Pj:事故原因の発生確率.
Rji:その対策により低下する事故原因の割合.
Si:各対策の有無（0or1）.
Ci: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もっとも投資効果の高い対策の選択は，式 2 の値 $E_{\triangle}$が最も大きくなる対策の選択として表される.

式 2：

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

表 4　デルタ ISMS 表

事故原因	事故発生時の被害額	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Kの投資コスト（S_KC_K）
1	L_1P_1	R_{11}	R_{12}	・・・	R_{1K}
2	L_2P_2	R_{21}	R_{22}	・・・	R_{2K}
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・
J	L_JP_J	R_{J1}	R_{J2}	・・・	R_{JK}

図 5 に従来の資産ベースのリスクアセスメントにおける項目間の関係と事故ベースのリスクアセスメントにおける項目間の比較を示す.

資産ベースの「資産価値」と「対策の影響」の 2 項目を，事故ベースでは「被害額」の 1 項目に置き換えることができるため，項目間関係を説明する 2 枚の表から 1 枚の表に縮退できる.

n 巡目のリスクアセスメントで選択した対策を実施すると n+1 巡目には対応する事故原因の発生確率 Pj は低下するはずである．その予想低下率は Rji から計算できる．事故原因が発生した時の被害額 Lj に変動がないこと，対策のコスト Ci が低率で下がること及び予想低下率 Rji を用いて n 巡目で選択した対策のみ事故原因の発生確率 Pj を下げることで，n 巡目に n+1 巡目以降のリスクアセスメントをシミュレートできる.

対策コストには設備導入などの初期導入コストと定常的な運用コストに分かれることもあるが，高額な設備は資産品として耐用年数に応じて年度別に資産償却するため，特に初期導入コストを別勘定する必要はない.

n+1 巡目のリスクアセスメントでは，実測された発生確率 Pj が判っているので n 巡目での予想発生確率 Pj との差異から予想低下率 Rji をより正確な値に再計算できる．事故ベースのリスクアセスメントはサイクルを繰り返すごとにより正確になる.

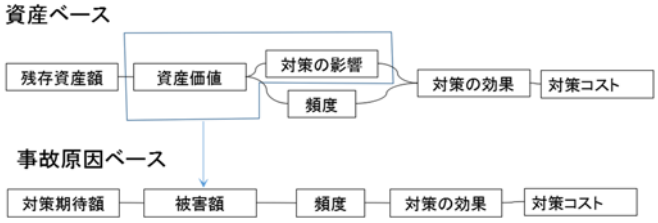

図 5　二方式の比較

3.3 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 はリスクアセスメントに使用したデルタ ISMS 表より選択した対策列のみ残して経営陣に報告し，更に，管理者・従業員層に方向づけしてゆく．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 及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 6 に示す．このうち経営陣と CISO が共にモニタすべき項目は下線の 4 項目である．これらの中でデルタ ISMS 表がカバーする 2 項目を赤字で示す．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.

- 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
- 管理策の有効性は確認できたか

図 6　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

Vol.2015-CSEC-70 No.24
Vol.2015-SPT-14 No.24
2015/7/3

3.4 ドキュメントからデータベースへ

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）及び 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」というプロシージャを追加することになる．内部犯の抑止力として，または，訴訟対策として日常業務のログを取っている組織も少なくないが，ログを取ることは，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．そういう意味では，各部署の PDCA の横でデジタルフォレンジックが併設されることになる．

また，ISO/IEC27001 は規格の各所で文書化を求めているが，将来的には，データベース化のような IT 処理可能なデジタル化が求められると考えられる．

以上を総合すると，図 7 のようになる．

4. まとめ

4.1 研究の成果

本稿における研究の成果を次に示す．

(1)事故データベースに基づくリスクマネジメント

組織で実際に発生した事故データベースに基づき，経営陣と管理者･従業員層が共有できる KPI を提供することで，経営陣の情報セキュリティマネジメントの関与を促し，組織全体の PDCA サイクルが実現できる．

(2)情報セキュリティガバナンスとしてのデルタ ISMS

事故データベースに基づくリスクマネジメントは，従来の資産ベースのリスクマネジメントと比較して簡便であるとともに，情報セキュリティガバナンスの経営陣と CISO 間のモニタリング項目に対して余分情報がなく，デルタ ISMS が提供するデルタ 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みなせる．

(3)事故データベースとデジタルフォレンジックの融合

ISMS の IT 支援による強化を図るためにも，事故データベースとデジタルフォレンジックの融合により，現状 ISMS の文書化が軽減できる．

4.2 今後の課題

最後に，本研究における今後の課題を示す．

(1) デルタ ISMS 表の十分性

情報セキュリティガバナンスの実現に向けて，経営陣でも状況や課題が理解でき，評価が容易であることを示したが，デルタ ISMS 表に不足する情報の検討が必要である．

(2)管理者・従業員層にとってのデルタ ISMS

ISMS の PDCA サイクルを経営陣に伸ばすためのモデルを提示したが，本モデルの管理者・従業員層にとってのメリットの検討も必要である．

(3)事故データベースとデジタルフォレンジックの融合

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具体的な機能・仕様検討が必要である．

(4)効果の測定

デルタ ISMS モデルの実組織への適用試行などを通してモデルの有効性を検証する必要がある．組織内のローカルな事故データベースは組織外には非公開情報となるため，検証方法の工夫が必要となる．

参考文献

1) 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).
2) 日本規格協会:ISO/IEC 27001:2013 情報セキュリティマネジメントシステムの国際規格（2014）.
3) IPA:組織における内部不正防止ガイドライン(2015).
4) 法務省：会社法(2014).
5) 日本監査役協会: 監査役実施要領（2011）.
6) 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（2012）.
7) ニューメディア協会:ISMS 認証事業所調査 調査報告書（2010）.

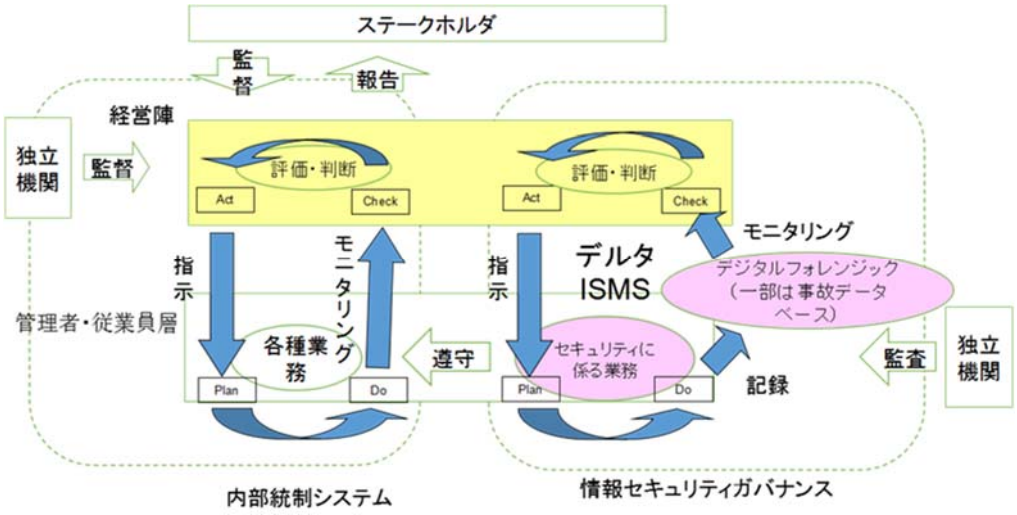

図 7 デジタルフォレンジックを用いたデルタ ISMS

8) 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（2014）.
9) NIST: Security and Privacy Controls for Federal Information Systems and Organizations，NIST SP 800-53 Revision 4 (2013) .
10) 日本ネットワークセキュリティ協会：2013 年度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～，日本ネットワークセキュリティ協会（2014）.
11) 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，Vol2015-CSEC-68 No5(2015).
12) 中村逸一，兵頭敏之，曽我正和，水野忠則，西垣正勝：セキュリティ対策選定の実用的な一手法の提案とその評価，情報処理論文誌，Vol．45，No．8，pp2022-2033(2004).