2016年度 第1回ITリスク学研究会　2016/8/25

Nish!gaki Laboratory

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 -

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

†1 静岡大学大学院（博士課程） †2 NTT データ
†3 東京電機大学 †4 東芝 †5 NTT †6 静岡大学

概要

Nish!gaki Laboratory

- 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ある.
- 「ISMS＋通常対応」へ事故の学習の詳細手順を加える. これをデルタISMSとよぶ. 手順は次の通り;
  - ①事故データベースの運用
  - ②年間予想損失額の算出
  - ③表を用いた対策改善策の選定
  - ④情報の経営陣への提示.
- 情報セキュリティガバナンスの観点から

情報セキュリティ事故が減らない

Nish!gaki Laboratory

- 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ある.
  - 「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」[1]
- ISMS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（A.16.1.6）

↓

- 「ISMS＋通常対応」へ事故の学習の詳細手順を加える.

[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).

全社的情報セキュリティマネジメントの強化

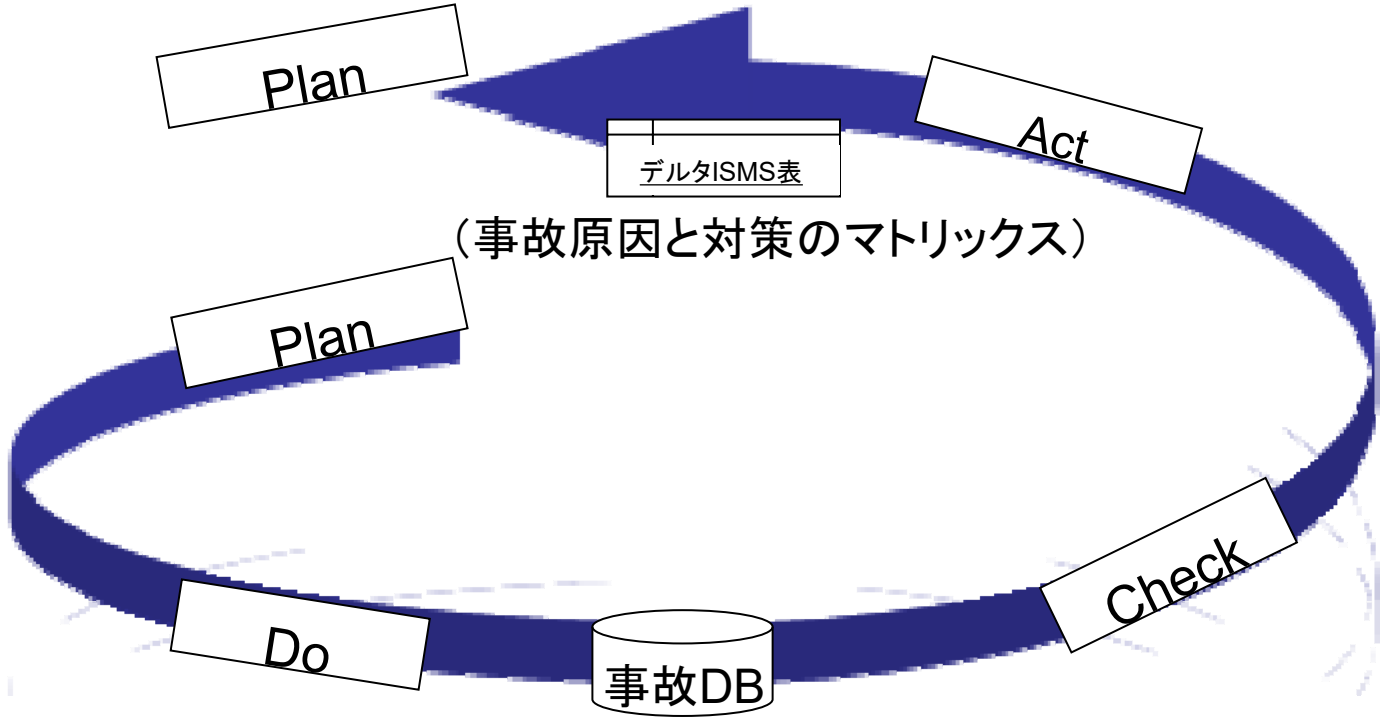
Nish!gaki Laboratory

- 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
- 事故の削減には認証範囲を越えた全社的なセキュリティマネジメントが必要
- CISO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」が担う

デルタISMS モデル

Nish!gaki Laboratory

DOで蓄積された「事故DB」を基にn巡目の結果となる「デルタISMS表」がn+1巡のPlanでの対策選択のためのデータとなる.



事故の対応

Nish!gaki Laboratory

- 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）
- 今回，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.

事故データベース

Nish!gaki Laboratory

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
影響範囲	影響範囲を選択する. ヒヤリ・ハットから大事

事故データベース(続き)

Nish!gaki Laboratory

列名	意味
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.

事故原因と対策のマトリックス

Nish!gaki Laboratory

デルタISMS 表

事故原因	被害額	頻度	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_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}

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

L_j:その事故原因が発生した時の被害額。
P_j:事故原因の発生確率。
R_{ji}:その対策により低下する事故原因の割合。
S_i:各対策の有無（0or1）。
C_i:対策のコスト。

デルタISMS表

Nish!gaki Laboratory

n巡目のActからn+1巡目のPlaningで渡されるデルタISMS表のイメージ

	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	80万円	・・・	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%

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（JIS Q27002やNIST SP800-53より転記）.
コスト：その対策を選択した場合のコスト.
対策による被害額（頻度）軽減率：その対策による発生頻度軽減率（0%～100%）.

デルタISMS表

Nish!gaki Laboratory

デルタISMS表から最も効果が高い対策の組み合わせを選択する。

n巡目

	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	80万円	・・・	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%

対策2を選択した場合、各30%の改善が、損失低減額として750万円，75万円が想定される。

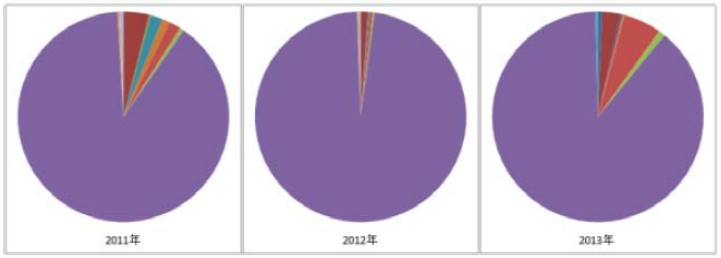
n＋1巡目の被害額、頻度の実測値と比較できる。

巡を重ねるとトレンドとして見ることができる。

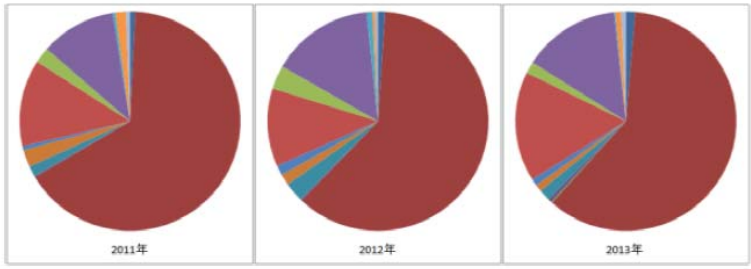
組織ごとのチューンアップ

Nish!gaki Laboratory

- 自組織内で実際に起こった事故や被害の情報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がチューンアップされていくことになる.



金融業・保険業

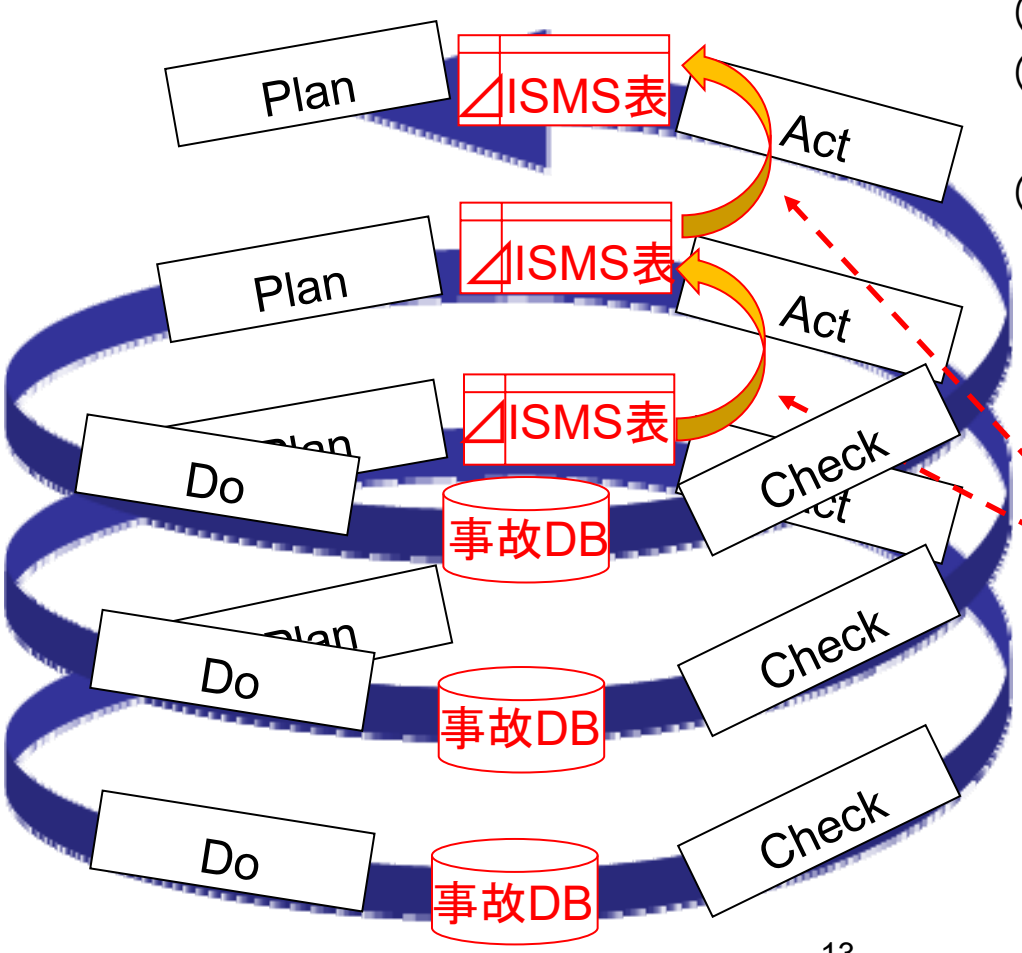


公務

業種ごとに違いがあり,同じ業種では同様のインシデントが発生している.
[2]佐藤他：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

デルタISMS モデル

Nish!gaki Laboratory



(1)対策による脅威の表出
(2)組織ごとのチューンアップ
(3)定量的データによる
　共通認識の形成
(4)投資対効果の明確化

経営者の認識・理解の向上

PDCAサイクルは1年で回すものも数週間で回すものもある。

デルタISMS表の中の事故データの前巡比較(差分)、更に複数巡回における事故データのトレンドを観察することが重要

事故データベースのサンプル

Nish!gaki Laboratory

ISMS 認証を取得している従業員数約800 名のある組織において，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

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2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15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）

デルタISMS表のサンプル

Nish!gaki Laboratory

		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

情報セキュリティガバナンス

Nish!gaki Laboratory

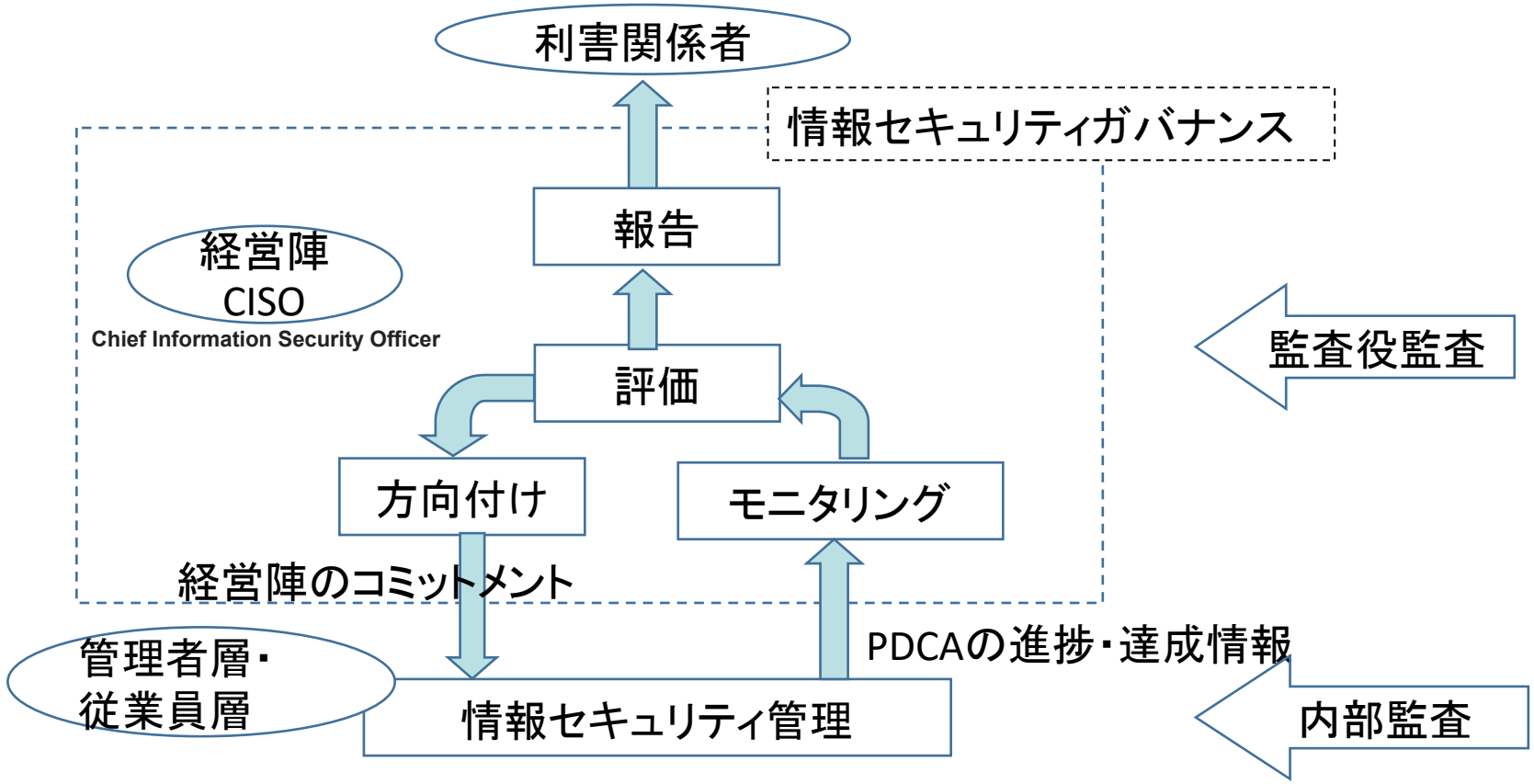
•情報セキュリティガバナンス

企業の経営陣において，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

[3]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

情報セキュリティガバナンスのフレームワーク

Nish!gaki Laboratory



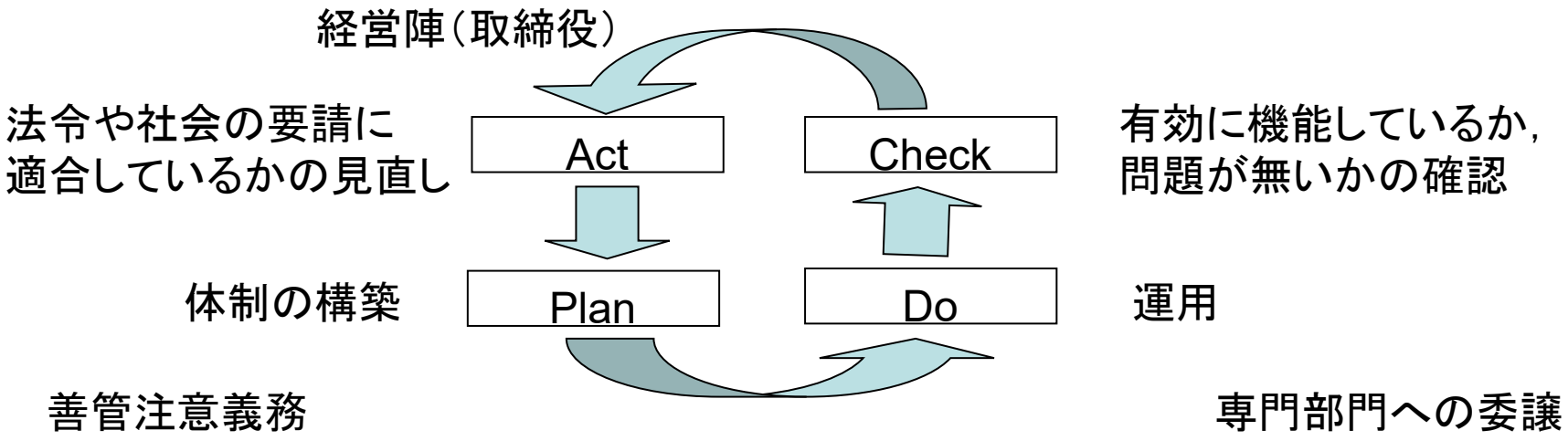
[3]経済産業省：情報セキュリティガバナンス導入ガイダンス

会社法の内部統制システム

Nish!gaki Laboratory

•内部統制システム

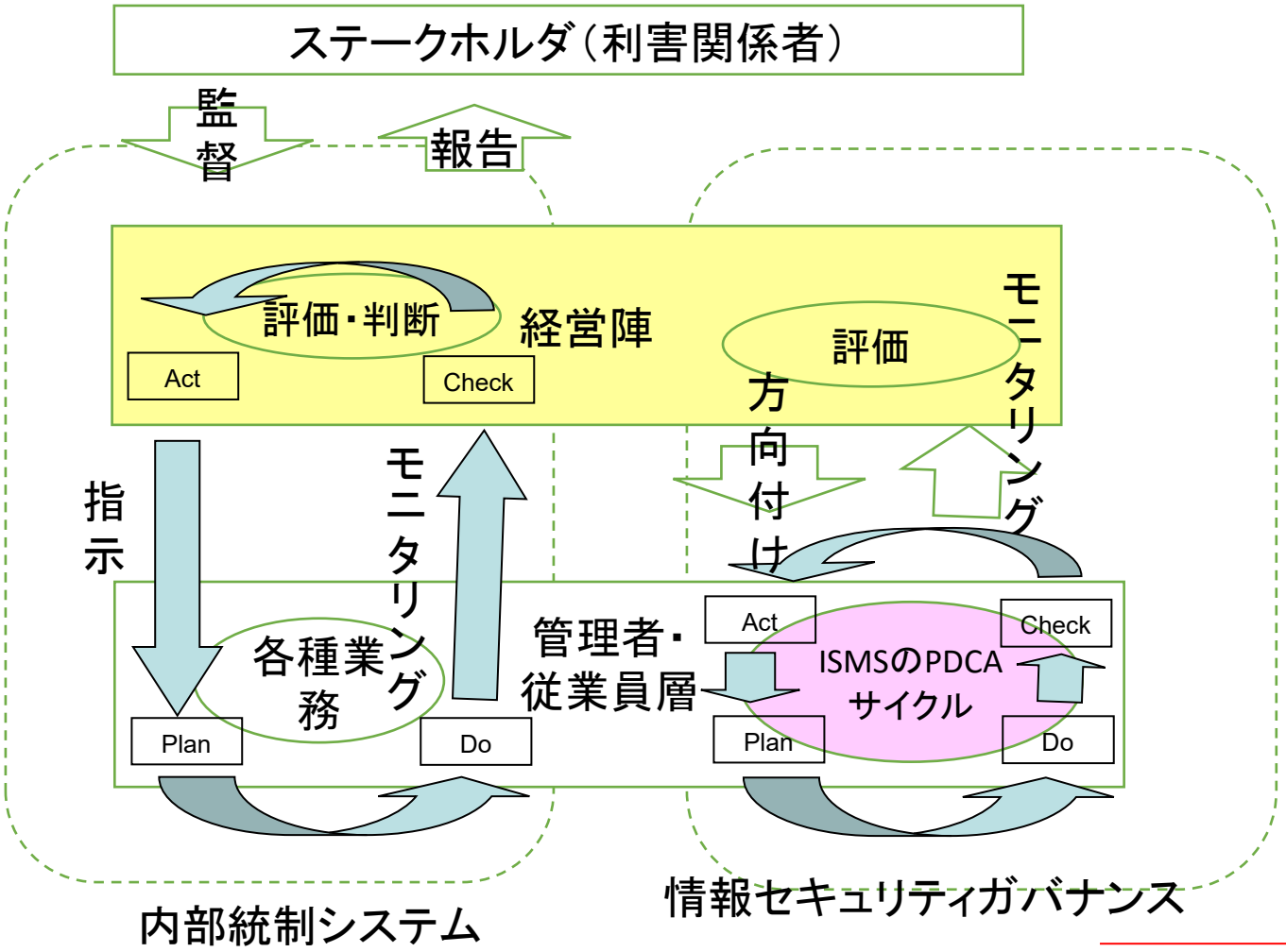
すべての会社において，法令違反・定款違反・不正・不祥事・事故といった問題の発生を未然防止するため，取締役が会社を事業目的に沿って適切に運営するために本来必要なもの．



[4]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）.

2つのシステムの比較

Nish!gaki Laboratory



ISMS の現状

Nish!gaki Laboratory

- 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」についてはほとんど取り組まれていない．

ISMS の効果を高めるため重点的に取り組んでいるものは？

	有効回答数	3. 一般社員の認識	6. 有効性評価手法	5. 内部監査人スキル強化	9. 教育研修の改善	2. 管理者層の認識	4. マニュアルの整備
今回	416	281	131	131	127	123	103
(2010年)	(%)	67.5	31.5	31.5	30.5	29.6	24.8
前回	352	220	112	91	102	76	79
(2008年)	(%)	62.5	31.8	25.9	29.0	21.6	22.4
前々回	264	183	108	61	95	76	83
(2006年)	(%)	69.3	40.9	23.1	36.0	28.8	31.4

8. リスク分析手法	10. 文書・記録管理	11. インシデント対応	1. 経営陣の認識	7. 費用対効果	12. その他
101	94	87	65	24	4
24.3	22.6	20.9	15.6	5.8	1.0
73	73	61	35	17	9
20.7	20.7	17.3	9.9	4.8	2.6
62	62	54	27	12	4
23.5	23.5	20.5	10.2	4.5	1.5

[5]ニューメディア協会:ISMS 認証事業所調査 調査報告書(2010).

情報セキュリティガバナンスとの比較

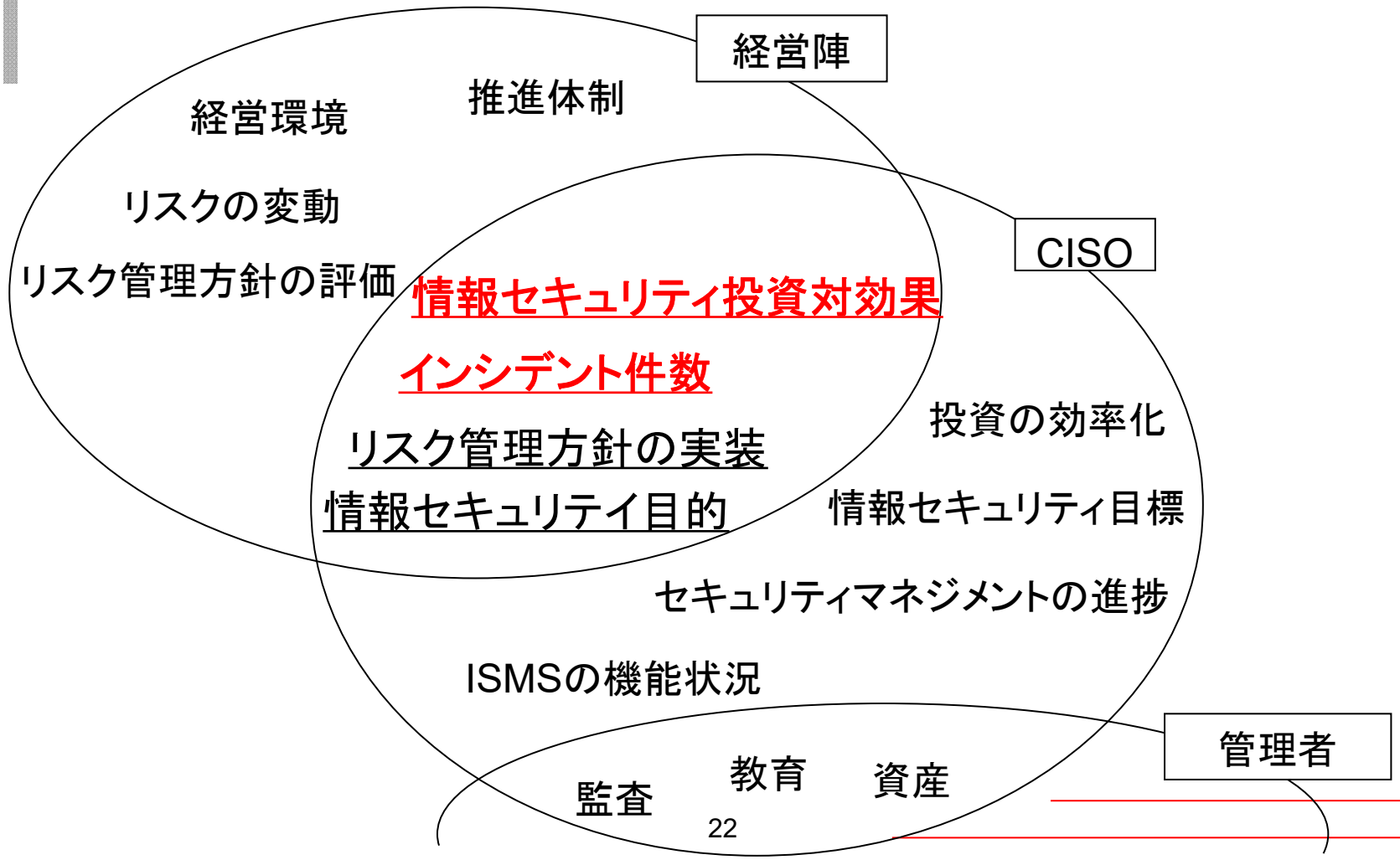
Nish!gaki Laboratory

- 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，集約された項目であることが求められる.
- CISOはデルタISMS表を経営陣に報告するときに，実施コストの高いものや対策効果の大きい項目に絞って報告することになる.
- ここでは、デルタISMSモデルの項目と情報セキュリティガバナンス[3]でのモニタリング項目とを比較し，集約という観点から、項目に余分なものがないことを示す.
- 80項目を15個にグループ化する.

[3]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

情報セキュリティガバナンスのモニタリング項目

Nish!gaki Laboratory



モニタリング項目

Nish!gaki Laboratory

- 情報セキュリティ投資対効果
  - 新規の管理策（対策）：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
  - 管理策（対策）の有効性は確認できたか

- インシデント件数
  - 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

事故ベースのリスクアセスメント

Nish!gaki Laboratory

デルタISMS 表

情報セキュリティ投資対効果

事故原因	被害額	頻度	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_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

L_j:その事故原因が発生した時の被害額。
P_j:事故原因の発生確率。
R_{ji}:その対策により低下する事故原因の割合。
S_i:各対策の有無（0or1）。
C_i:対策のコスト。

ドキュメントから データベースへ

Nish!gaki Laboratory

- 組織内で事故データベースを運用
- 「事故が発生したら，その情報をDBに遅漏なく登録する」というプロシージャを追加
- 各部署のPDCA の横でデジタルフォレンジックが併設
- ISO/IEC27001 は各所で文書化を要求
- 文書のIT 処理可能なデジタル（DB）化
- 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.
- フォレンジックから事故DBを導けるとヒアリハットも含めた高いカバー率を得ることができる.

デルタISMSの一構成要素としてのデジタルフォレンジック

Nish!gaki Laboratory