JSSA

情報セキュリティの強化に向けて
—— ISO27001 を利用するヒントとアドバイス ——

Hints and Advices for Effective Information Security Management

2009年6月12日

システム監査学会
情報セキュリティ研究プロジェクト
情報セキュリティ専門監査人部会

本プロジェクト・メンバー

植野 俊雄	ISU
黒川 信弘	パナソニック
小谷野 幸夫	さいたまソリューションズ
齋藤 敏雄	日本大学
内藤 裕之	バルク
永井 好和	山口大学
西川 征一	西川技術士事務所
水谷 穣	水谷情報技術士事務所
安尾 勝彦	ヤフー
山本 孟	優成監査法人
芳仲 宏	東京地方裁判所
米沢 整	――――――

何故、セキュリティ事故は繰り返すか

◆ 他人ごと「自分のところに限って・・・」
・事故事例を自組織に置き換えて考えていますか？
・他社事故事例が活かされず、同様の事故発生

◆ 直視せず「ポリシーも定めたので大丈夫」
・セキュリティ環境変化を見ず、同じ規程で大丈夫？

◆ 横並び意識「認証を取得し、他社以上のレベル」
・目標が不明確なまま、何となくやっていませんか？

◆ 経営意識「セキュリティ推進部門もあるので問題なし」
・必要な経営リソース(人、金、時間)を投入している？

第2次 情報セキュリティ基本計画の「基本目標」

基本目標

「ITを安心して利用可能な環境」の構築

●基本目標に向けて考慮すべき諸点●

■「事故前提社会」への対応力強化

・理解（気付き）の推進、判断力の向上
・事後対応への更なる注力
・主体間の共通理解、信頼関係の構築
・事実把握と被害拡大防止・再発防止への情報共有

■ 合理性に裏付けられたアプローチの実現

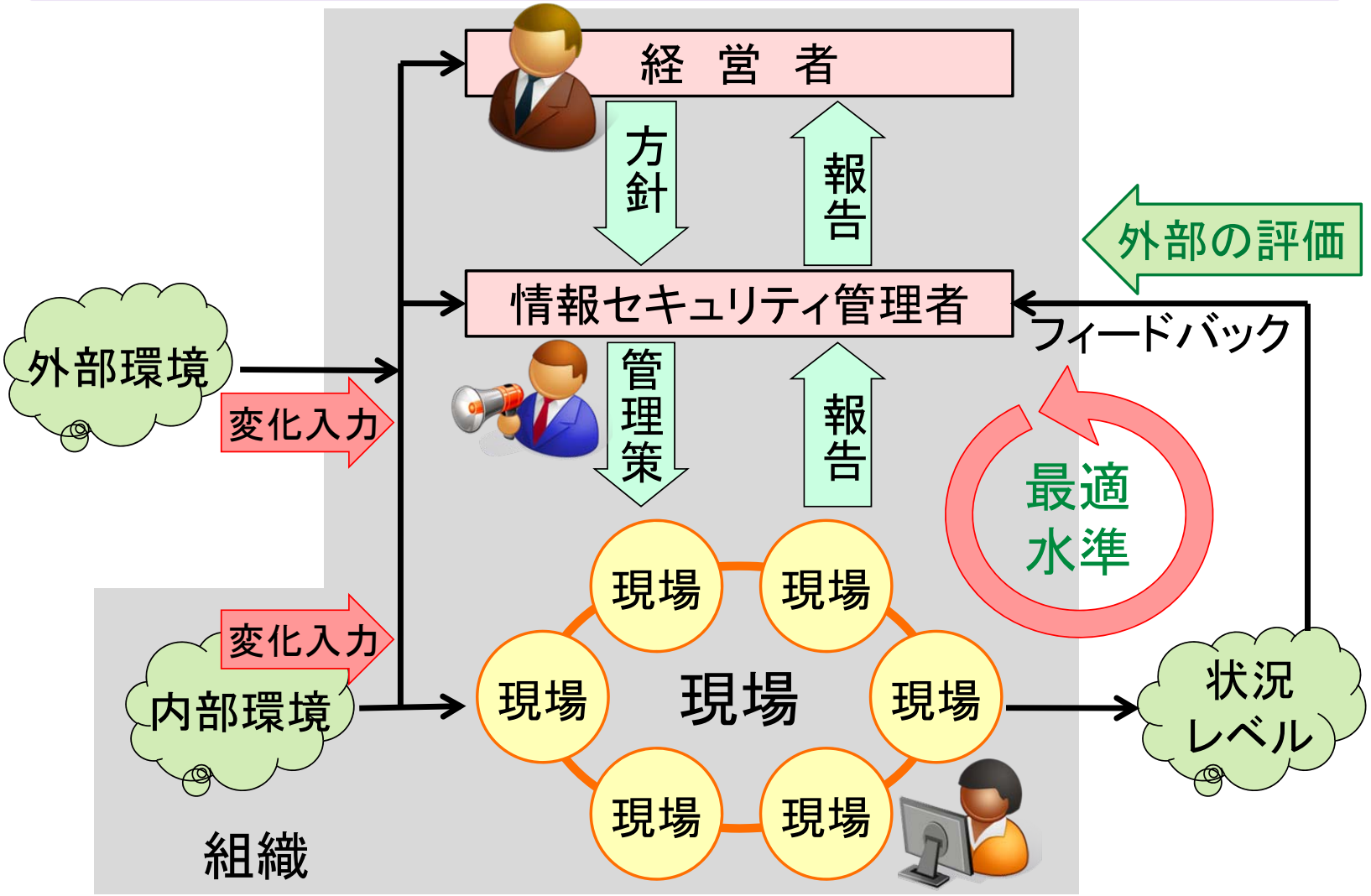
・脅威の把握、リスクへの柔軟な対応
・コスト・利便性とのバランス
・最適な「水準」に関する認識の共有
・人的側面の対策　・説明責任の明確化

http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0201.pdf

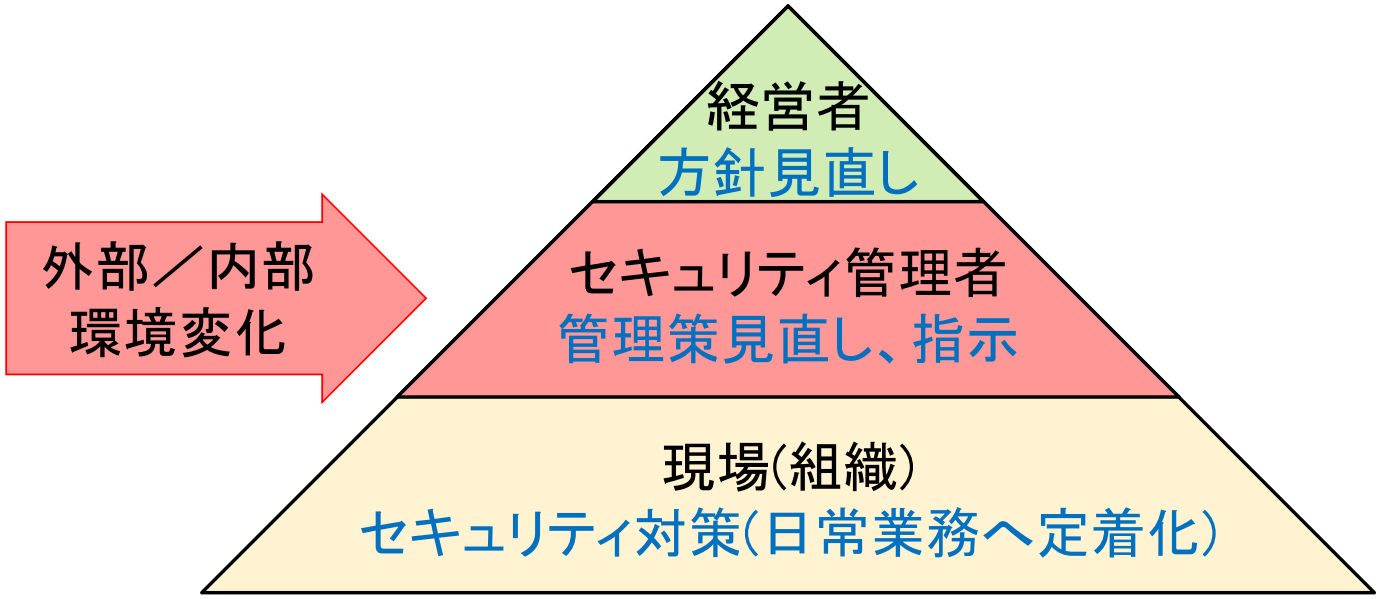
メッセージ

- ◆ 現実と向きあった「情報セキュリティ対策」
- ◆ 過不足ない最適水準への「合理性追求」

情報セキュリティ強化の組織マネジメント･モデル



階層モデルと役割



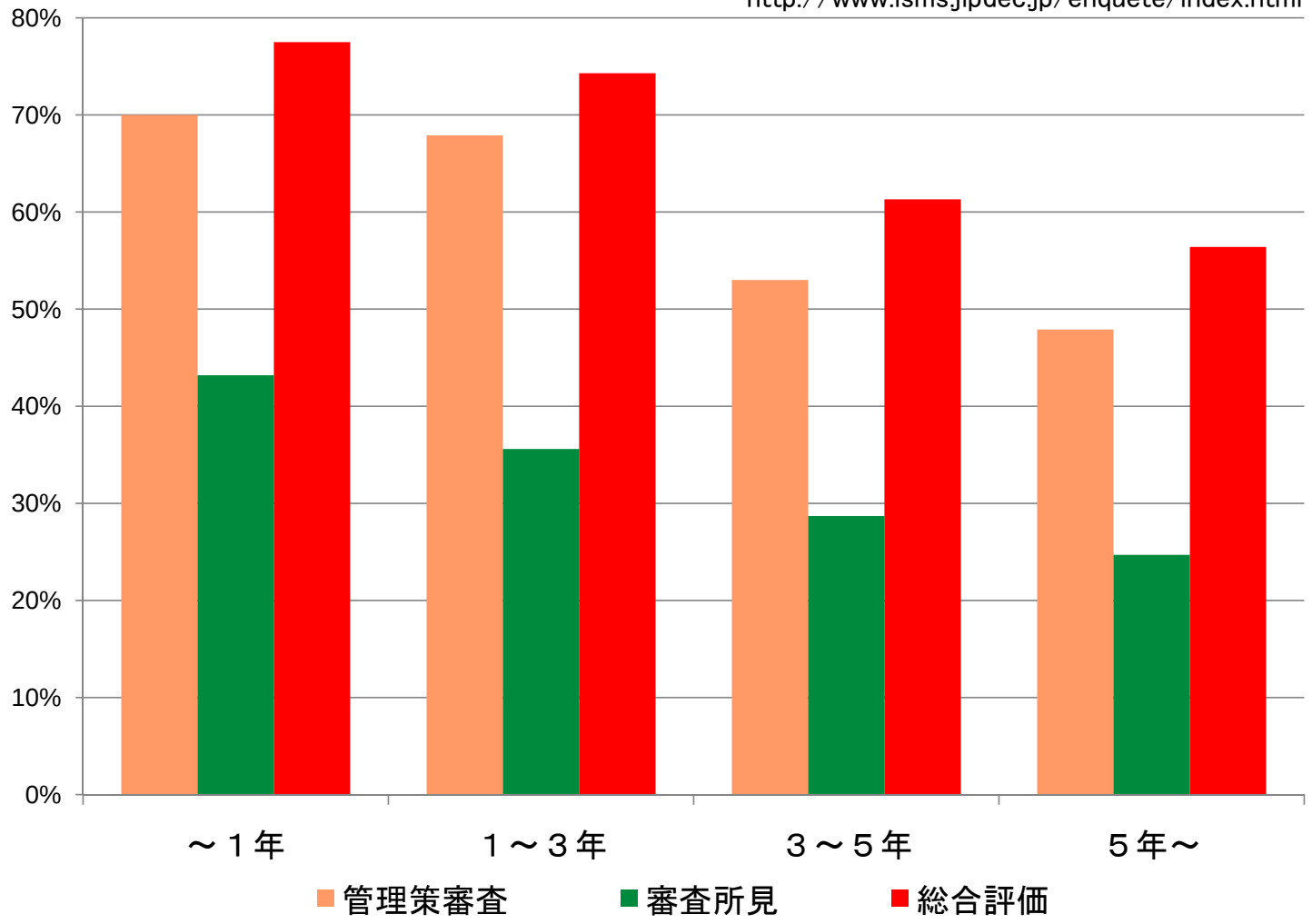
■ 本研究の着眼点

● セキュリティ管理者が、

- セキュリティ環境変化を的確に把握し、管理策に反映
- 自組織として最適の対策へ常時見直し
- 管理策カスタマイズのためのノウハウ提供

ISMS認証審査アンケート(審査の質満足度)

「ISMS適合性評価制度に関するアンケート調査報告書」(JIPDEC情報マネジメント推進センター、2009/3)
http://www.isms.jipdec.jp/enquete/index.html



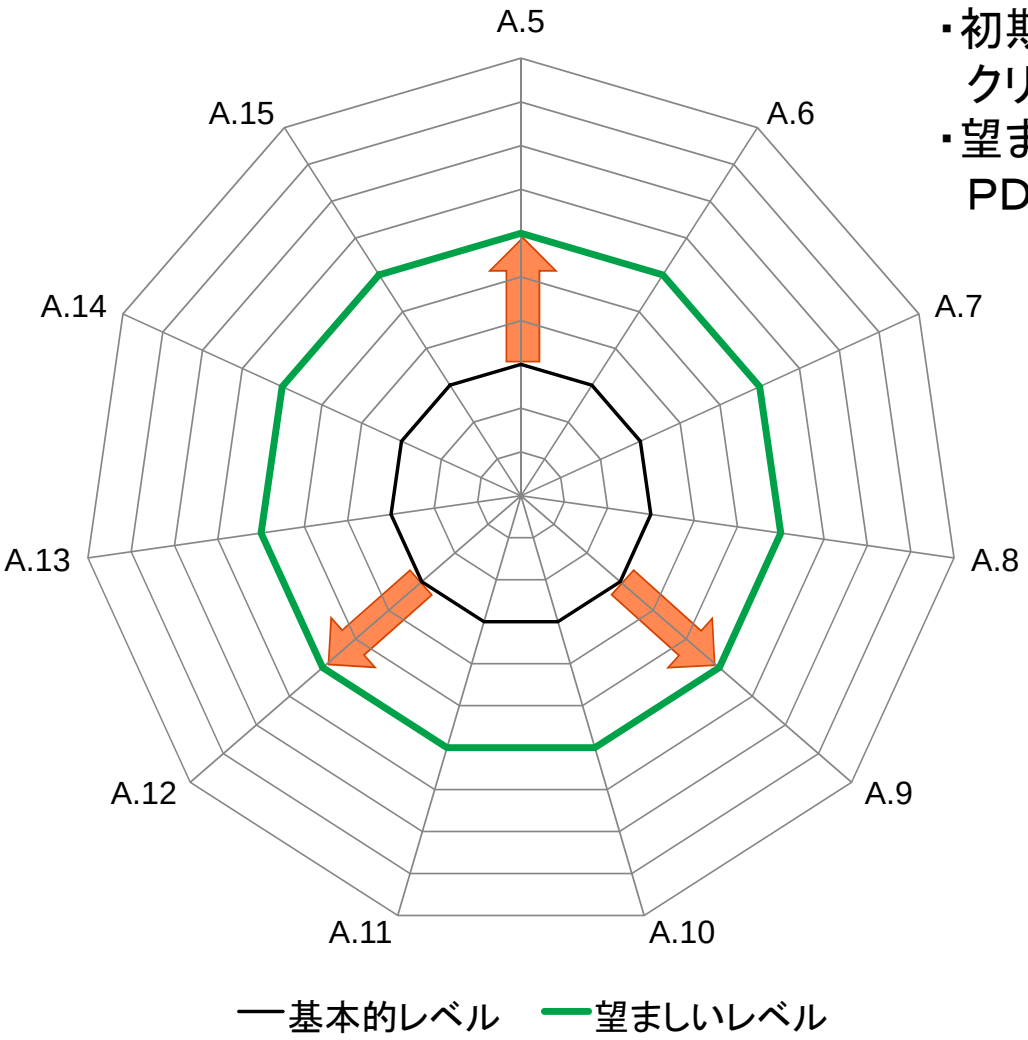
「審査員の力量」や「審査の質」が課題だろうか

■ アンケート結果(ISMS運用の実績を積むとともに)
- 審査に対する要求度、期待度が高くなる
- 審査側の対応が
  受審側の要求、期待に応えきれていない

■ 本質的な課題だろうか？？？
- 基本的なセキュリティ対策ができ、
  今後どうすれば良いか明確にできていない
- セキュリティ対策の重点分野を絞り込みたいが、
  実行していいのわからない
- 経営者から「合理的なコスト」を指示されるが、
  対策が甘くなってしまうのではないか

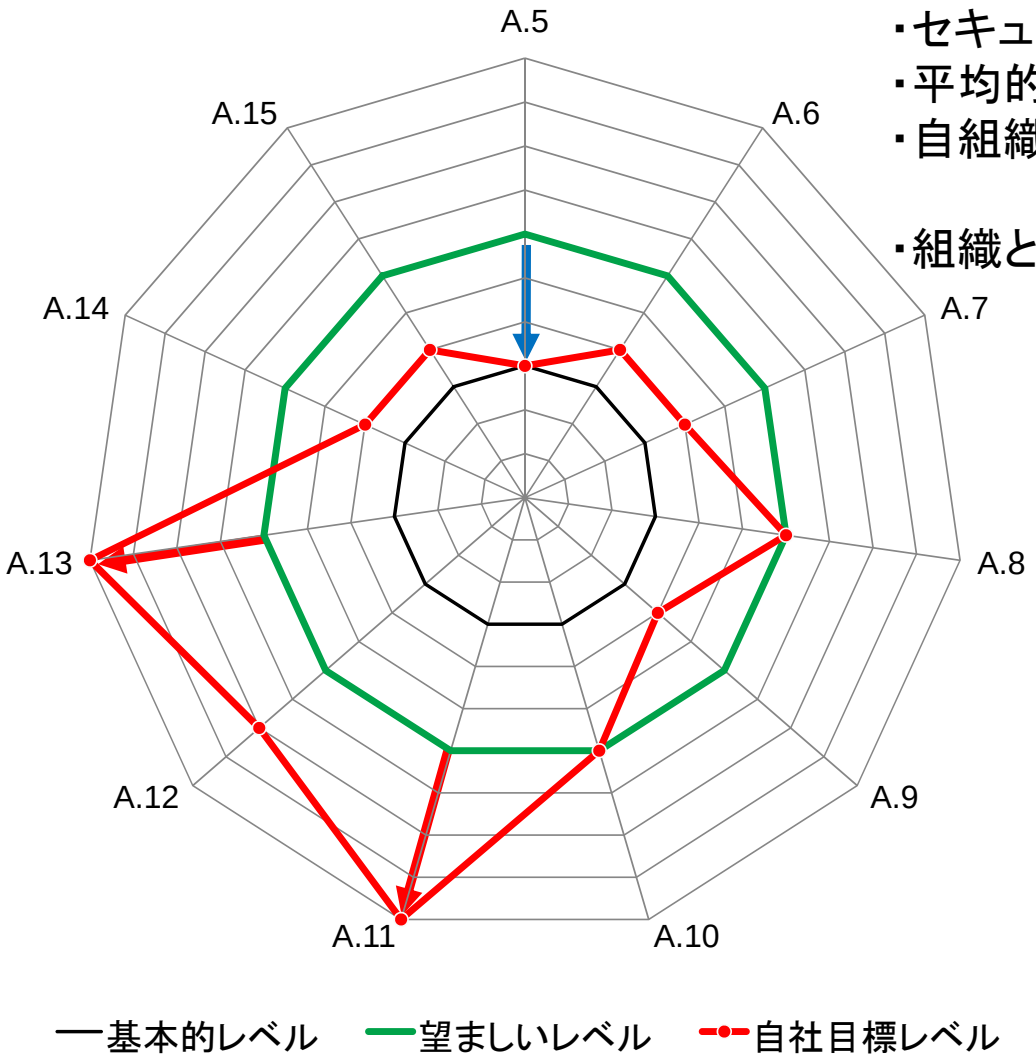
● 自組織のセキュリティ推進に自信がもてない！

PDCAで管理レベル向上(初期段階)



- 初期は基本的レベルのクリアから
- 望ましいレベルに向けPDCAで管理向上

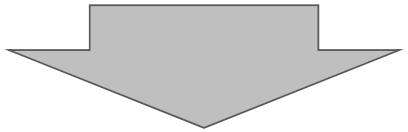
組織として過不足ない対策レベルの設定



・セキュリティの成熟度アップ
・平均的レベルの対策に不安
・自組織に必要性低い部分が顕在化
・組織として重点対策が明確化

勇気とノウハウ

一定レベルに 抑える対策	◆ 積極的に対策しない「勇気」 ◆ 代替の管理策との連動
組織として力点を置く 重点分野の対策	◆ 基準やチェックリストにない ◆ 対策のレベルが見えない ◆ 尖った対策の事例、ノウハウがない



事例、ノウハウを蓄積する核が必要

「ヒントとアドバイス」の作成と利用

- ISO27001の管理策をベースに検討
- ISO27001に記述されていない役立ち情報の抽出
- 抽出項目に関するノウハウの形成
- すべての管理策を網羅せず
- 管理レベルを下げる内容は各組織の判断で

詳細は「セキュリティ管理策作成のヒントとアドバイス」を参照

A.6 情報セキュリティのための組織「例外措置」

管理項目	A.6 情報セキュリティのための組織「例外措置」
管理策の課題	・基準や手順書はすべてのケースを網羅せず ・例外事項への対処手順は、明確でない場合が多い ・例外措置発生時、対策基準から外れていると見られる行為も生じる
ヒントとアドバイス	・例外措置が発生することを前提とする ・セキュリティ以外の社内規程で、例外対処手順があるか確認する ・即断即決できる態勢にしておくべき ・情報セキュリティ管理者に、例外措置判断と許可の権限を付与

A.8 人的資源のセキュリティ「雇用の終了／変更」

管理項目	A.8 人的資源のセキュリティ「雇用の終了／変更」
管理策の課題	・雇用の終了／変更手続で、当事者に守秘義務を負わせていない場合がある
ヒントとアドバイス	・終了／変更後も、守秘義務を負わせる ・守秘義務を負わせるため、退職願と同時手続が合理的 ・突発的な退職も考慮すると、退職願で担保できず ・採用時の誓約書は、在職中の守秘義務だけでなく退職／契約終了後の守秘義務も記載しておく

A.9 物理的及び環境的セキュリティ「媒体持込」

管理項目	A.9 物理的および環境的セキュリティ「媒体持込」
管理策の課題	・個人的な記録装置持ち込みのリスク対応を定めていない場合がある ・社内情報の録画、録音、複写など
ヒントとアドバイス	・撮影・録音機能つき機器、記録媒体持ち込みのルールを定める（禁止／申請／許可） ・来訪者や業務委託者も被写体となるリスクを考慮

A.10 通信及び運用管理「情報のバックアップと保存」

管理項目	A.10 通信及び運用管理「情報のバックアップと保存」
管理策の課題	・バックアップが情報保存も目的にする場合、 法的要求を考慮する必要あり ・バックアップ方針に「情報保存期間」を盛り込むべき
ヒントとアドバイス	・法的要求を考慮した管理手順を定める ・保存期間を保証できる 媒体の世代管理、保管管理の方法を採用 ・バックアップを改ざんされるリスクへの考慮も必要

A.11 アクセス制御「持込情報機器の接続制限」

管理項目	A.11 アクセス制御「持込情報機器の接続制限」
管理策の課題	・パソコンなど個人用機器を持ち込み、社内ネットワーク接続への対応が不明確 ・会社が認めた持込への対応はガイドされているが、無断接続を排除する対策でない
ヒントとアドバイス	・持ち込んだ機器を社内ネットワークへの接続を制限する管理方法を定める ・ネットワーク認証で、登録済みのMACアドレスのみ接続を許可する制御方式が現実的である

A.13 情報セキュリティ･インシデントの管理「ヒヤリハットの報告」

管理項目	A.13 情報セキュリティ･インシデントの管理 「ヒヤリハットの報告」
管理策の課題	･情報セキュリティ･インシデント報告を規定 ･「ヒヤリハット体験」は報告されず、インシデント対策の対象とならず
ヒントとアドバイス	･「ヒヤリハット体験」の報告を義務づけ ･ヒューマン･エラー再発予防のノウハウ蓄積 ･紛失や誤配送の原因はヒューマンエラーが多い

A.14 事業継続管理「リスクアセスメント」

管理項目	A.14 事業継続管理「リスクアセスメント」
管理策の課題	・「ISMS確立」の「情報資産のリスクアセスメント」と「事業継続のリスクアセスメント」を混同している場合あり
ヒントとアドバイス	・事業継続管理を正しく理解し、適切なリスクアセスメントを実施する ・業務ごとに、復旧の優先度や目標時間を設定 ・ディザスタリカバリ対策を準備する

果たすべき役割

- われわれが取りあげた「ヒントとアドバイス」は
  氷山の一角にすぎない

- これを核として、内容が充実できれば、
  大きなノウハウとなる

- 組織の枠を超えたノウハウ共有の仕組を持つべき
  国レベルでなく、業界単位ぐらいが現実的でしょうか