情報セキュリティ専門監査人部会活動報告

情報セキュリティ監査に役立つ着眼点と監査ノウハウ

－ Useful Practices for Information Security Audits from Professional Viewpoints －

2008年6月6日

情報セキュリティ専門監査人部会WG

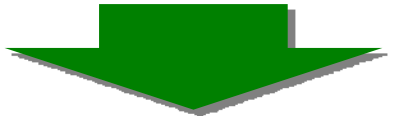
情報セキュリティ専門監査人部会
WGメンバー

氏名（五十音順）	所属
黒川　信弘	松下電器産業株式会社
内藤　裕之	株式会社バルク
水谷　穣	水谷情報技術士事務所
安尾　勝彦	ヤフー株式会社
芳仲　宏	東京地方裁判所
若林　正	株式会社アイ・ティー・ワン

情報セキュリティ専門監査人部会の狙い

情報セキュリティを取り巻く現状

- 企業や団体の情報セキュリティやコンプライアンスニーズの高まり
- 情報セキュリティを担当する真の専門家は質・量ともに不十分



- このような中で、情報セキュリティ、システム監査の双方に精通した専門家の確保・育成への取り組みを通じ、社会に貢献する。

本年度の研究活動

- システム監査人（情報セキュリティ監査人）が監査を行うとき、現場を確認したりアドバイスを行う上で有用なチェックリストを作成
- すべての分野に精通したセキュリティ監査人はおらず、専門分野を相互に補完し合うことが必要と考え、セキュリティ監査時の実践的なヒント集といえるものを目指した。

チェックリストの内容について

- 公表されている各種の基準・ガイドラインはすべての企業や団体に適用できることを基本とするため網羅性を重視しており、その結果、現場に深く根ざしたノウハウになりにくい

※現在の主要な基準・ガイドライン

- JISQ27001／27002
- システム管理基準
- 情報セキュリティ管理基準
- 個人情報保護　経済産業省ガイドライン
- 情報システム・モデル取引・契約書（セキュリティガイドライン）

- 現場で実査時、網羅的でなく部分的でも、情報セキュリティの課題をあぶりだせるような質問をするための着眼点、その課題を解決できる具体的な方策に関する提言のためのノウハウを集めた。

※タイトルは「情報セキュリティ監査人のための監査ヒント集」とした。

情報セキュリティ監査人のための監査ヒント集

分類

1．情報管理	
1−1．コンピュータ（サーバ、パソコンなど）内の情報	入力、送信、加工、消去
1−2．コンピュータ（サーバ、パソコンなど）以外の電子媒体内の情報	取得、移送、保管、廃棄
1−3．紙媒体の情報	取得、移送、利用、保管、廃棄
1−4．その他の情報(人の記憶)	利用
2．組織的対策	
2−1．組織･体制の確立	組織体制の整備、職掌の分離と責任の明確化
2−2．規程の整備	規程の作成
3．人的対策	
3−1．契約	従業者との契約、派遣元との契約、業務委託
3−2．教育･訓練･指導	従業者への規則の周知･徹底、従業者に対する教育･訓練
3−3．従業員の監督･監視	行動監視、業務管理
4．技術的対策	
4−1．アクセス管理	識別と認証、アクセス権限（アカウント）の管理、アクセス制御、情報資産へのアクセス管理と監視
4−2．パソコン管理	クライアント管理、不正ソフトウェア対策
5．物理的対策	
5−1．入退室／入退館管理	オフィスレイアウト、入退館管理、入退室管理
5−2．持ち出し／持ち込み管理	持ち出し／持ち込み管理
5−3．物理的管理、盗難対策	セキュリティ区画、クリアデスク、クリアスクリーン、施錠管理、機密情報の保管場所
5−4．機器類の物理的保護	水害対策、電源対策、通信対策、地震対策

情報セキュリティ監査人のための監査ヒント集

記載内容の例

項目は、「項目」「確認内容」「アドバイス内容」の順で、詳細な説明を記載

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
1. 情報管理		
1-1. コンピュータ(サーバ、パソコンなど)内の情報		
入力	取得した情報を機密性レベルなどで分類しているか	他者から取得した情報は、社内で的確かつ効率的な管理を行うため、当該情報の保管管理者が、管理対策を明確にした機密性レベルなどによる分類をして管理策を講じなければならない。 情報の管理責任者や保管管理者を明確に定めていないケースが散見される。 機密保持契約がある場合は、契約担当者が情報保管管理者に対し、契約内容による順守事項を契約部門以外でも容易にわかる内容で周知しておくべきである。
	取扱者の権限・責任を明確にしているか	Web から直接入力し、受け取る情報は、その処理を可能な限り自動化し、従業員がアクセス(確認、訂正など)しなくて良いようなシステムにする努力が重要である。 情報を入力した人からの問い合わせに限り、厳密な本人確認を行うとともに、参照／更新できる人は、お客様対応部門などに限定していないと、情報流出のリスクが大きくなる。 システム担当者のアクセスを認めているケースもあるが、リスクが高い。
	預った個人情報や重要情報などの保管は、特定のサーバに限定しているか	個人情報や経営情報、開発情報など重要な情報は、サーバ管理者もアクセスすべきでないため、アクセス権限を大幅に絞り込むが、そのサーバに一般情報と同居させると、一般情報へのアクセスも制限することになり、現実的ではなく、そのために、サーバを分離させるのが良い。

管理策の分類は、大項目、中項目とカテゴリ分けして整理

アドバイス内容は、できるだけ具体的、かつ複数の切り口でわかりやすく記載

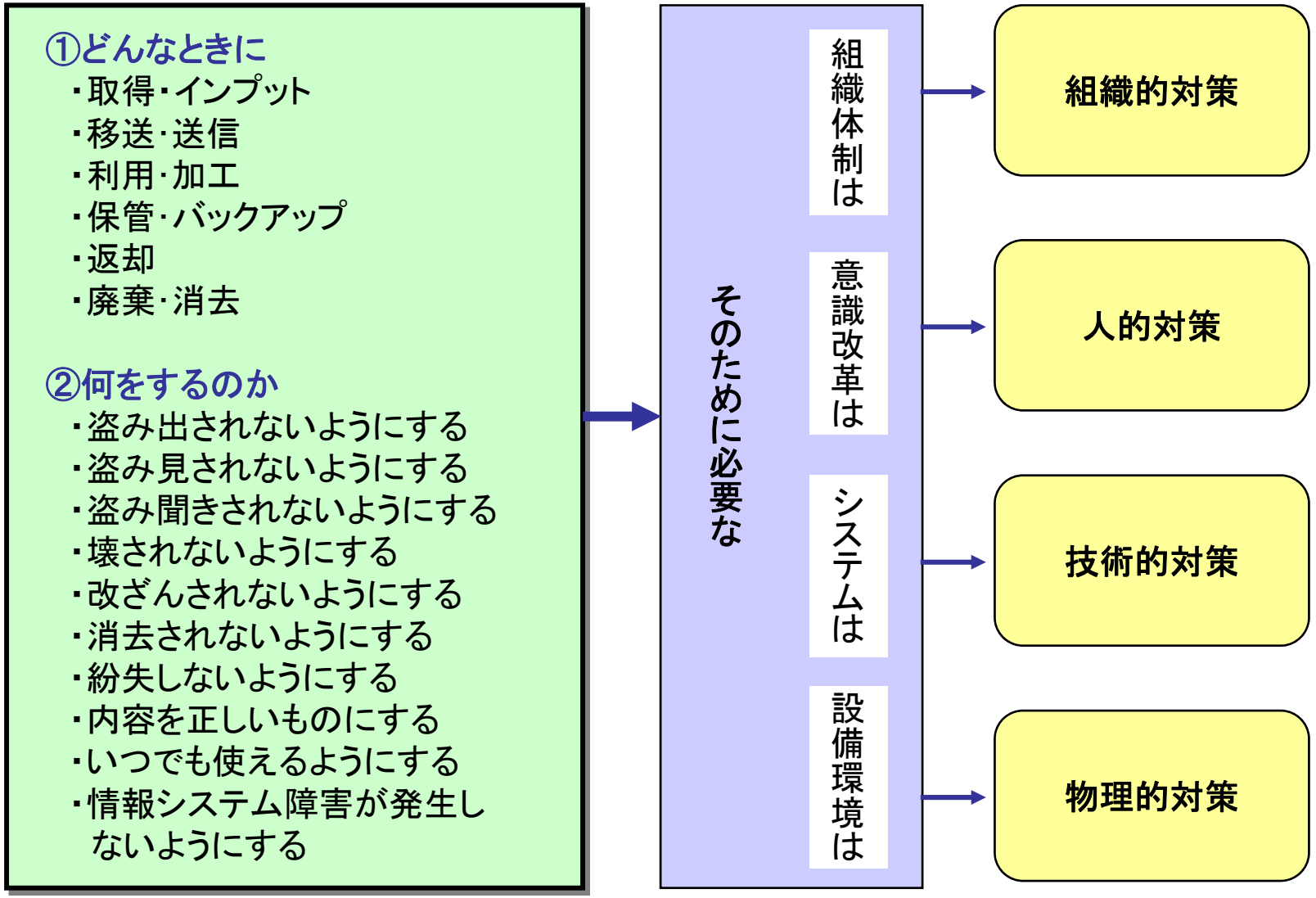
情報セキュリティ監査人のための監査ヒント集
アドバイス記載のポイント

- メンバーは、セキュリティ要求度の高い職種に従事、或いは管理責任を持つなど、情報セキュリティ現場への関与が高い。
- よって、メンバーの知識、知見をもとに、実務的かつ見落とされがちな観点からのアドバイスを深掘りしている。
- 管理策を考慮するための起点として、「情報管理」の視点を取り入れた。

情報管理の視点

- 情報管理とは、情報を守ることである。
- 情報を守ることとは、漏れないようにすること(機密性）、正しい内容を維持すること(完全性)、いつでも使える状態にしておくこと(可用性）である。
- 　そのために、先ずは「どんなときに」、「何を」するかを明確にし、実施するにあたって必要なことを整備することが求められる。

情報管理の視点からみた対策



実施する対策を有効なものにするためには

- 守るべき情報が何であるかを特定すること
- その情報に対する脅威はどんなものが想定されるかを知ること
- その脅威による影響を知ること
- 影響の大きさにより重要度を決めること

情報の分類[格付け]

情報と脅威を結びつけ、情報の重要度に応じた対策を考えることが必要である。(リスク分析・評価)

情報セキュリティ監査人のための監査ヒント集抜粋

- 情報管理
  - 紙媒体の情報

項目	確認内容	アドバイス内容
利用	情報の閲覧／持出を制限しているか	重要な情報を閲覧する場合、認められた人が、許可された場所でのみ閲覧し、その閲覧記録を残さなければならない。閲覧スペースは、一般オフィスとは情報を授受できないよう分離されており、作業していることが一般オフィス側からも見えるようにガラスなどで仕切られていることが望ましい。

情報セキュリティ監査人のための監査ヒント集抜粋

- 情報管理
  - その他の情報（人の記憶）

項目	確認内容	アドバイス内容
利用	記憶内容の流出制限	毎日少しずつ自分の頭脳に記憶し、帰宅後に記録をすれば、日数をかけることにより、大量の情報持ち出しにもつながるので、職業倫理意識の低い人は、個人情報や経営情報など機密性レベルの高い業務から外すなどの措置を講じた方が良い。また、機密性レベルの比較的低い業務を担当する中で、職業倫理観の確立した人のみ、重要な業務へ配置転換する方法もある。

情報セキュリティ監査人のための監査ヒント集抜粋

- 技術的対策
  - アクセス管理

項目	確認内容	アドバイス内容
識別と認証	正当なアクセス権限を保有しているものの識別と認証をできているか	ITリテラシーが低い利用者でも記憶できるレベルの複雑さで、類推しづらい範囲に設定できているか。難しい文字列を要求し過ぎると、パスワードをメモする結果にもつながるので注意が必要である。 ・・・ パスワードは、システムが自動発行するのではなく、利用者が記憶しやすい文字列を指定できる方式が望ましい。

情報セキュリティ監査人のための監査ヒント集抜粋

- 物理的対策
  - 入退室／入退館管理

項目	確認内容	アドバイス内容
入退室管理	執務室への入室／退室制限ができるようになっているか	・・・ 来訪者が立ち入る許可エリア毎に、名札やストラップの色分けなど、瞬時に判断できる区分をしておく。

情報セキュリティ監査人のための監査ヒント集抜粋

- 物理的対策
  - 入退室／入退館管理

項目	確認内容	アドバイス内容
入退館管理	窓から侵入される危険はないか	機密性レベルの高い情報を扱うオフィスでは、窓から、書類や外部記憶媒体などを落下させ、外部に持ち出せる方法がリスクとして存在するので、窓を開けなくする対策も必要である。
	共連れ防止ができているか	ICカードだけの認証でドアから入れる場合は、１枚のICカードで複数人が同時に入室できる共連れ現象になるので、フラッパーゲートなどで防止しているか。

今後の課題

- 情報セキュリティの裾野の広がり
  - すべての領域の対策に精通することは困難
  - カテゴリー毎の専門家を養成する必要性
  - 模擬監査等による実践経験の場を提供
- 様々な分野で専門特化した経験者にも参画いただき、研究活動を発展させていきたい。
- 情報セキュリティ研究プロジェクトとの合同研究も予定

皆様の積極的な参加をお待ちしています。