

情報セキュリティ管理基準を利用した セルフコントロールチェックのススメ

2002年度 セキュリティ監査WG活動報告

セキュリティ監査WG 河野省二
2003年 5月3日

政策部会 監査ワーキンググループの活動のご紹介

活動目的

8月5日に稼働した住民基本台帳ネットワーク(住基ネット)をはじめとして、今後稼働していく行政の電子化・情報化に関して、大きな役割を担う地方自治体を対象として、セキュリティ監査をする必要性があります。本WGは、地方自治体向けセキュリティ監査基準の策定、セミナーの開催などを当面の成果とします。また、経済産業省主催の「情報セキュリティ監査研究会」へJNSAの意見・成果を反映させる受け皿として、本WGが必要です。

活動内容

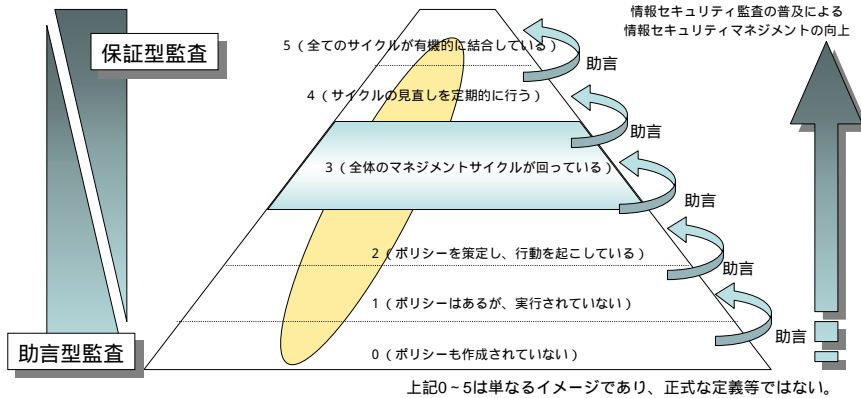
地方自治体向けセキュリティ監査基準の策定
監査手順の検討
啓発セミナーを全国主要都市で開催
情報セキュリティ監査人のスキルマップ作成

予定成果物

地方自治体向けセキュリティ監査基準
情報セキュリティ監査人スキルマップ



まずはセルフコントロールチェックから



- セルフコントロールチェックを行うことによって、「自らのおかれている場所」を知り、「目指すべきセキュリティレベル」とのギャップを図る。目標となるレベルとはどの程度のギャップがあるのか…

情報セキュリティ管理基準の策定について

JIS X 5080

ISO/IEC 17799を邦訳したもので、企業がお手本とするべき情報セキュリティマネジメントのガイドライン

情報セキュリティ管理基準

コントロール

JIS X 5080の127のコントロールを細分化

サブコントロール

「JIS X 5080:2002の管理策(コントロール)のガイダンス」の内容を項目化し、内容に応じて上記のコントロールごとに振り分け

情報セキュリティ監査制度とは

経済産業省では、「情報セキュリティ監査研究会」を開催し、「情報セキュリティ監査制度」についての検討を行った

情報セキュリティ管理基準とは

JIS X 5080をベストプラクティス型の書式から、チェックリストにも利用できる規程書式に変更したもので、管理策が独立した形で並べられ、より使いやすいものとなっている

庁内LANの管理基準とは

電子政府をモデルにした、リセアセスメント、リスクアセスメントを基に策定された管理基準。業態別の管理基準作りのお手本となる

http://www.meti.go.jp/policy/netsecurity/information_audit.html

5. 資産の分類及び管理

5.1 資産に対する責任

目的：組織の資産の適切な保護を維持するため

5.1.1 資産目録 (一部省略) この情報に基づいて、組織は資産の価値及び重要度に対応した保護のレベルを設定することができる。情報システムそれぞれに関連づけて重要な資産について目録を作成し、維持することが望ましい。各資産を、その現在の所在(喪失又は損傷から回復しようとするときに重要)とともに、明確に識別し、その管理責任及びセキュリティの分類(5.2参照)について合意し、文書化することが望ましい。情報システムに関連づけた資産の例を次に示す。

JIS X 5080

3. 資産の分類及び管理

3.1 資産に対する責任

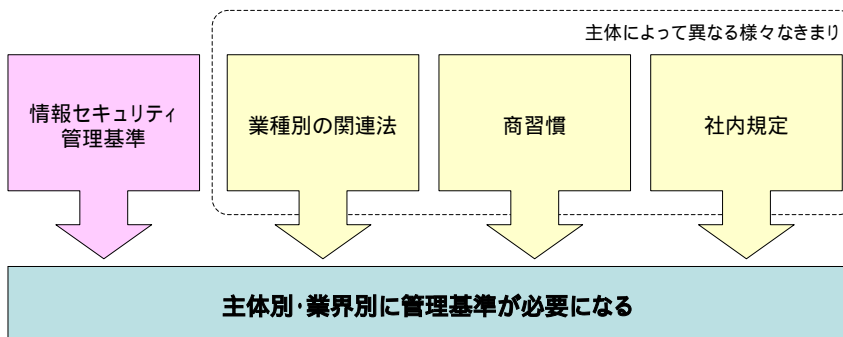
目的：組織の資産の適切な保護を維持するため

3.1.1 情報システムそれぞれに関連づけてすべての重要な資産について目録を作成し、維持すること

- 3.1.1.1 組織は、その資産並びにそれらの相対価値及び重要度を明確に把握できるようにすること
- 3.1.1.2 情報システムそれぞれに関連づけて重要な資産について目録を作成すること

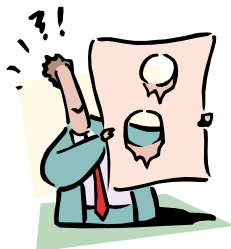
情報セキュリティ管理基準

独自の管理基準が必要

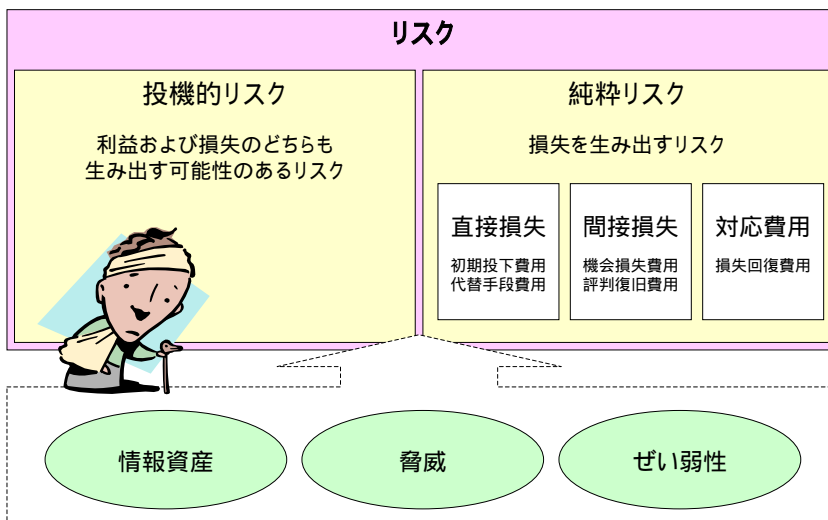


管理基準をそのまま運用しても、どこかにゆがみが生じてしまうのは目に見えている。あらかじめ様々な要素を取り入れておくことで、より堅牢で運用しやすい、主体別の情報セキュリティ管理基準を作成することができる

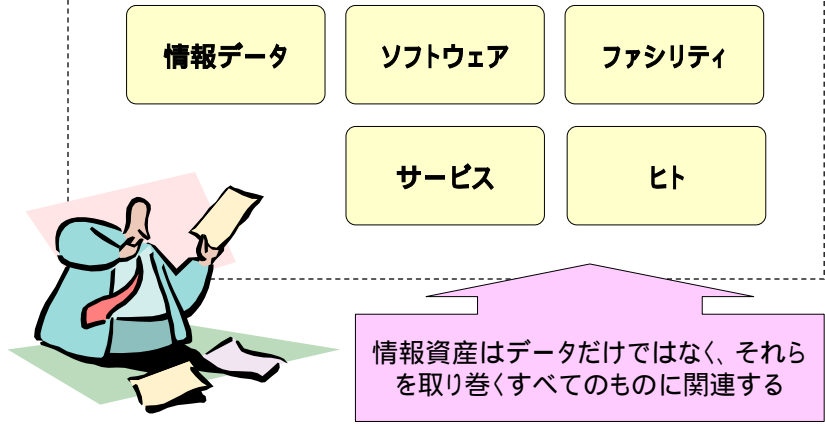
まずは正しいリスク分析から



リスクを正しくとらえるために - リスクの概念



情報資産の分類

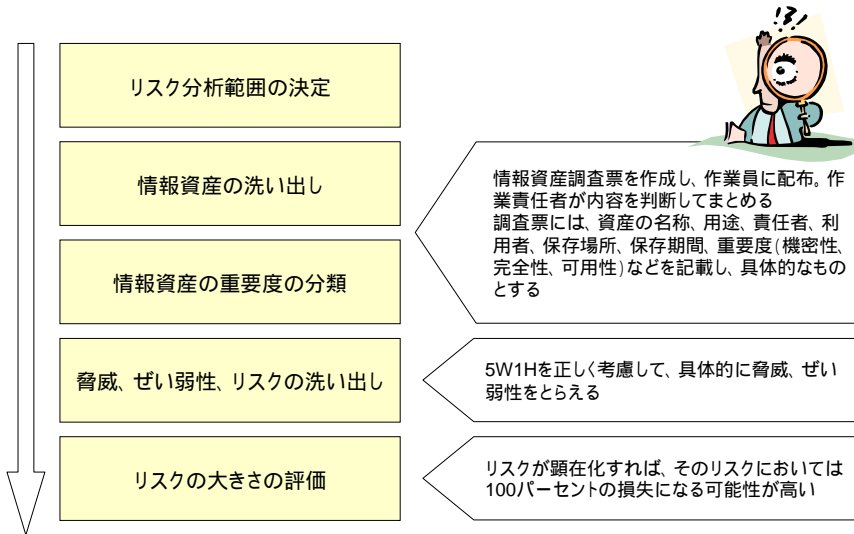


組織内のすべての人員が同じ価値観を持つためには、情報の分類方法の策定が必要

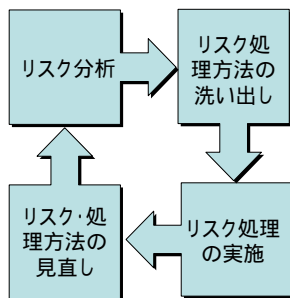
機密性 情報の漏洩防止	<ul style="list-style-type: none">✓ 極秘✓ 機密✓ 社外秘✓ 公開
完全性 破壊、改ざんからの保護	<ul style="list-style-type: none">✓ 高✓ 低
可用性 サービスの維持	<ul style="list-style-type: none">✓ 早急✓ 優先✓ 標準

情報分類は書類作成者が行うことが肝心

リスク分析の手順と手法



リスクマネジメントのプロセスとリスク処理



リスクコントロール

潜在的なリスクに対して物理的対策、技術的対策、運用管理的対策を行うこと。リスク回避、損失予防、損失軽減、リスク分離、リスク結合、リスク移転に分類できる



リスクファイナンス

リスクが顕在化して損失が発生した場合に備えて、損失の補填や対応費用の確保をしておくこと。リスク保有、リスク移転に分類できる



リスクの容認

リスクコントロールとリスクファイナンスを行っても、まだ対処できないリスク(残余リスク)について、あえて対処を行わないという判断

独自の管理基準を策定する



独自管理基準策定のステップ

情報セキュリティ管理基準

- ・コントロール
- ・サブコントロール

適用範囲の決定

- ・情報資産の洗い出し
- ・リスクアセスメント

それぞれの企業に見合った内容にするためには、適用範囲の決定は必須

1. コントロールの検討
2. サブコントロールの抽出
3. 社内規定、関連法律によるサブコントロールの追加
4. 全体的な文章の見直し

検討の際には、それぞれに対して理由付けが必要。後からトレスできるように記録を残す

独自の管理基準

それぞれのコントロールについて、技術面、マネジメント面でそれらが正しく実施されていることを確認できるようにしておくこと



管理策(コントロール)の選択

コントロール	チェック	理由
1.1.1 基本方針文書は、経営者によって承認され、適当な手段で、全従業員に公表し、通知すること		
1.1.2 基本方針には、定められた見直し手続に従って基本方針の維持及び見直しに責任をもつ者が存在すること		
2.1.1 セキュリティを主導するための明りょうな方向付け及び経営者による目に見える形での支持を確実にするために、運営委員会を設置すること	×	-- -- -- -- --

リスクアセスメントによって管理基準作成の適用範囲を決定したら、それに伴って、コントロールを全体的に見直す

適用範囲において必要なコントロールを抽出する

この際に必要でないと判断したコントロールについてはその理由を別記することを忘れないように...

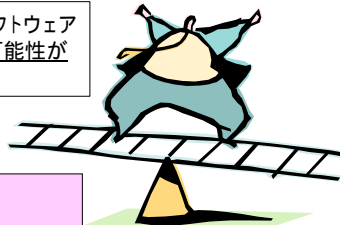


たとえばこんな管理策では...

10.1.2 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は、法的制限事項に適合するように、適切な手続を実行すること

現在は知的所有権がある物件や所有権があるソフトウェアを利用していないとしても、将来的には利用する可能性があると判断したほうがよい

このコントロールは必要だと判断



サブコントロール	チェック	技術	理由
10.1.2.1 ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること		×	
10.1.2.2 ソフトウェア製品の取得手続に関する標準類を発行すること		×	
10.1.2.3 ソフトウェア著作権及び取得方針に対する意識をもたせ、それらの方針に違反した職員に対して懲戒措置を取る意志を通知すること		×	

コントロールの選択において、必要だと判断したコントロールに含まれるサブコントロールを検討

サブコントロールは具体性が高いため、主体によっては適さないものがある

サブコントロールは万能ではないので、必要に応じて追加する技術的検証の必要性を検討



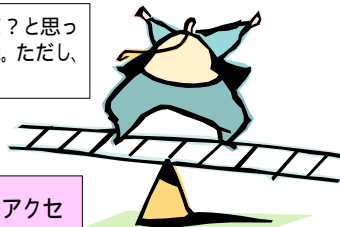
第三者契約書を例にとると・・・

2.2.2.2 第三者アクセスに関する契約書は、組織と第三者との間に誤解が全くないことを確実にするものであること

「誤解が全くないことを確実にするもの」ってなんだ？と思ったら、これを独自の言い回しに変更することも可能。ただし、項目としては必要だと考える

2.2.2.2 第三者アクセスに関する契約書にはアクセス方法の手順書を添付すること

・・・などに変更



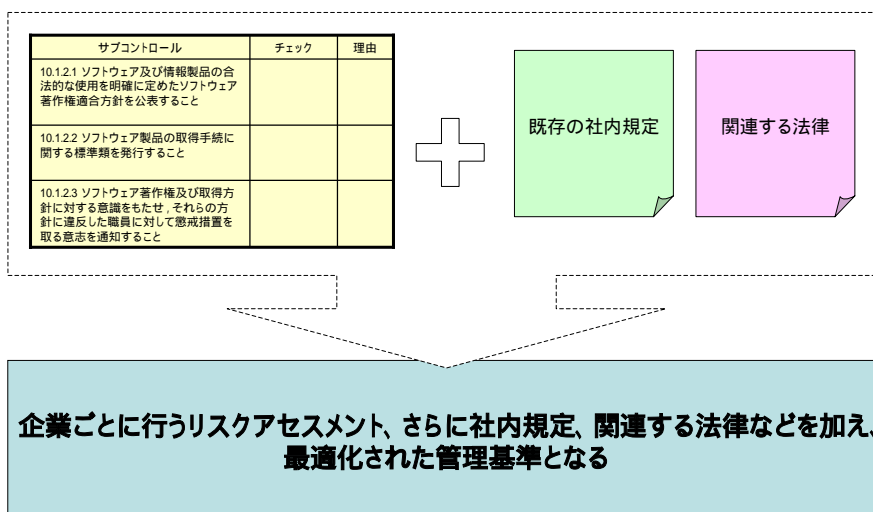
技術的検証が必要なサブコントロールでは

6 通信及び運用管理	6.5 ネットワークの管理	
目的	ネットワークにおける情報の保護、及びネットワークを支える基盤の保護を確実にするため	
コントロール	1)	ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施する
サブコントロール	1)	ネットワークの管理者は、ネットワークにおけるデータのセキュリティを確保すること
技術的検証項目	1)	アカウント認証に使用するパスワードは、OTP (One-Time Password) などを利用し、通信路上暗号化して送信する
	2)	重要なセッション (管理者のセッション等) は、SSH (Secure Shell) などを利用し、通信路上暗号化する
	3)	必要なサーバとクライアントの接続以外は、スイッチハブなどで隔離する

内部目的監査であっても、技術的項目については第三者の指導を仰ぐのが望ましい。最近ではセキュリティベンダーがチェックツールを販売しており、それらを利用するのも良い



足りない項目を補足する チェックリストの完成



サブコントロール	チェック	理由
10.1.2.1 ソフトウェア及び情報製品の合法的な使用を明確に定めたソフトウェア著作権適合方針を公表すること		
10.1.2.2 ソフトウェア製品の取得手続に関する標準類を発行すること		

チェックリストをさらに、

- ✓ インタビューでの確認
- ✓ 実施現場での確認
- ✓ 文書による確認

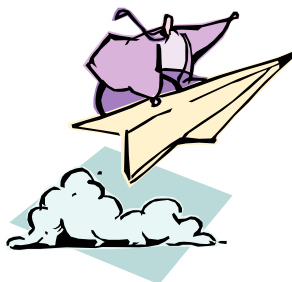
という場面で使いやすく分類する
(PD DISC 3005などを参考に)



「誰に確認をするのか」が重要な要素

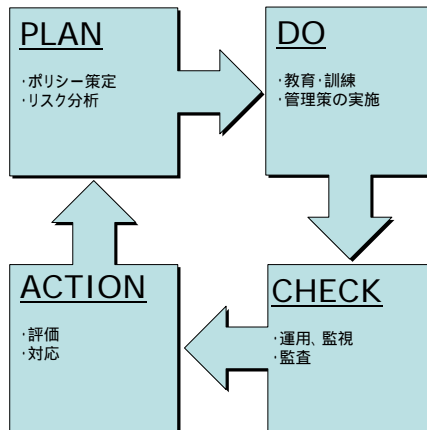
誰に聞いたらよいのかわからないという項目があるとすれば、それは管理策の選択が正しくないか、管理策が正しく運用できていないかのどちらかであると判断できる。よりよい管理基準策定のためにも、「誰に確認するのか」は重要な要素となる。個別のインタビューシートなども作成するとよい。

情報セキュリティ成熟度向上のために





- ✓ どこから始めても良いので、サイクルを回すことが重要
- ✓ サイクルを回せば回すほどよりよいセキュリティが構築できる
- ✓ 中長期的に運用できる管理基準を作成し、ポリシーの見直しを行うことも重要



セキュリティマネジメントのPDCAサイクル

内部監査の問題点

- リスクアセスメント、項目の洗い出しの妥当性に欠ける
- 監査の実施において、客観性・独立性に欠ける
- 対外的に公表できる形を作るのが難しい

外部監査を行うことをお勧めします



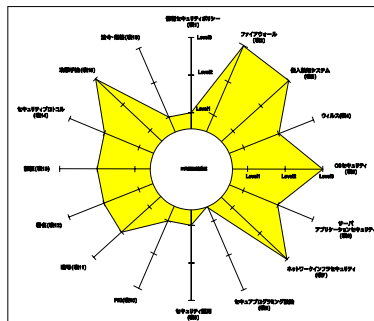
セキュリティポリシー策定の補助資料として利用

- 外部監査で作成されたチェックリストは社内ポリシー策定、見直しに重要な資料として活かすことができる

目標としてISMS適合性評価制度を設定するのも良い

- 適用範囲によってはプライバシーマーク制度なども検討すると良い

- JNSAは、外部監査もさることながら、内部監査においても、適切な技術および知識を持った情報セキュリティ監査人が必要だと考えています。
 - 現在JNSAが作成中の「セキュリティ技術者スキルマップ」を参考に、監査に必要なスキルをマッピング
 - この結果はパブリックコメントとして経済産業省に提出したいと考えています
- 監査ワーキンググループでは今後、セキュリティ監査人に必要な知識項目についての教育などについても考察したいと考えています



セキュリティ技術者スキルマップ
レーダーチャート

- このワーキンググループは現在、地方自治体向けの管理基準策定を研究項目として、活動を継続しています
 - 地方自治体を実際に監査したり、より実践的な研究を継続的に行っていきます
- 皆様のご参加をお待ちしております
 - 参加されたい会員の方はJNSA事務局までお問い合わせください



