NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

セキュリティポリシー作成のポイント

セキュリティポリシーWG
ＮＥＣソフト株式会社
小杉　聖一

２００２年１１月１４日

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

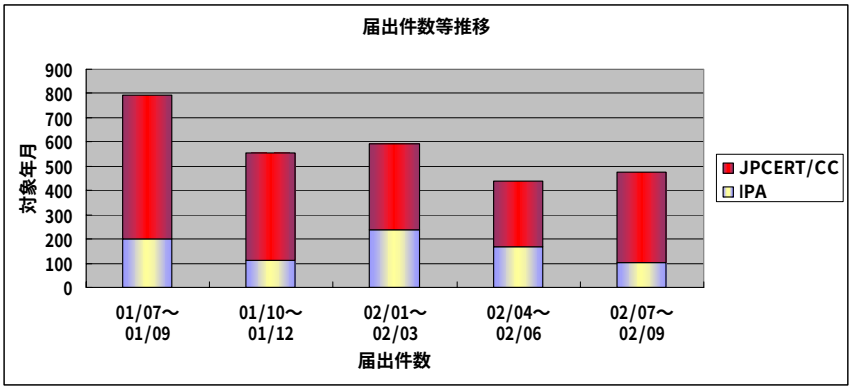
セミナー内容

１．セキュリティ市場状況
２．セキュリティ対策の考え方
３．セキュリティポリシーとは
４．セキュリティポリシーの具体例

1.セキュリティ市場状況

２００２年の３四半期は、昨年の約半分。しかし２００２年に入って被害の届出件数は平行線状態（減少ではない）。

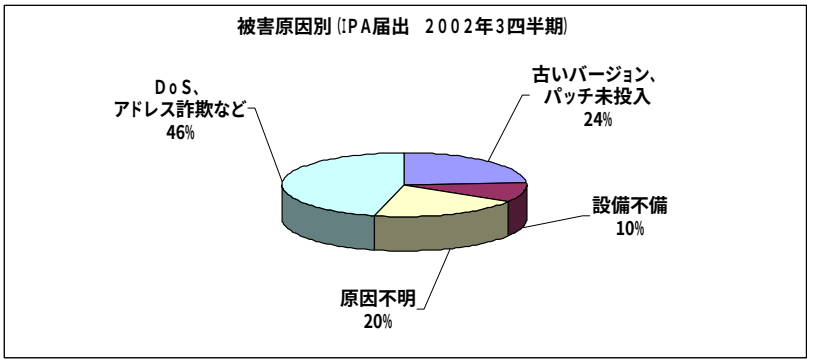
参考：IPA　2002年第３四半期 [7月～9月]不正アクセス届出状況



1.セキュリティ市場状況

実際の被害原因のトップは、古いバージョン・パッチ未投入。設備不備と合わせて３割は事前対策可能。

参考：IPA　2002年第３四半期 [7月～9月]不正アクセス届出状況



1.セキュリティ市場状況

ウィルスの被害は新しいものが続発（常に発生）。
今年になってＷｅｂの情報漏えいが多発し注目。

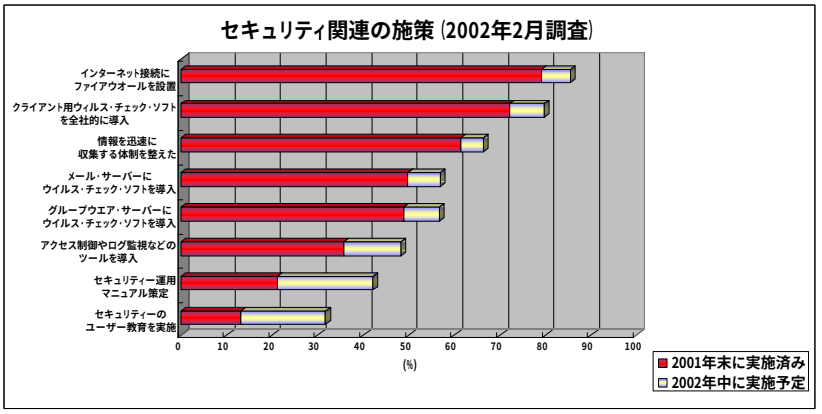
ウィルス多発の記事

個人情報流出の記事

1.セキュリティ市場状況

セキュリティ機器の導入は十分されている。
今後は、利用・管理・運用面のセキュリティ施策が中心。

参考：日経マーケット・アクセス・レポート，2002年6月号



1.セキュリティ市場状況

情報セキュリティ政策ｅ-Japan

ＩＴ基本戦略　２０００年１１月 ＩＴ戦略会議

↓

ｅ－Ｊａｐａｎ戦略　２００１年１月 ＩＴ戦略本部

５年以内に世界最先端のＩＴ国家

↓

ｅ－Ｊａｐａｎ重点計画

・ｅ－Ｊａｐａｎ戦略を具体化
・政府が迅速かつ重点的に実施すべき政策の全容を明示（ＩＴ基本法第３５条）

高度情報通信ネットワークの安全性及び信頼性の確保

制度・基盤の整備
・２００２年度までに暗号技術の標準化
・２００５年度までに刑事基本法制の整備

民間部門の情報セキュリティ対策・普及啓発
・２００３年度までに一般利用者への情報提供体制を強化
・２００４年度までに都道府県等に情報セキュリティアドバイザを配置

政府部内の情報セキュリティ対策
・２００３年度ま情報セキュリティポリシーの評価・見直しの実施等により十分なセキュリティ水準を確保

重要インフラのサイバーテロ対策
・２００１年中に官民の連絡・連携体制の整備
・２００３年度までに関係省庁の緊急対処体制を整備

研究開発・人材育成・国際連携
・２００１年中に情報セキュリティ関連資格制度を整備
・２００５年度までに不正アクセスやサーバーテロの予防・検知等に関する技術等を実用化

参考：http://www.kantei.go.jp/jp/singi/it2/dai12/12siryou1.html

1.セキュリティ市場状況

インターネットが情報社会の中心となっている現在、セキュリティ対策について政府も色々な取り組みをしており、セキュリティに関する標準化が進化。

設計・評価

ISO/IEC 15408
情報処理関連製品および情報処理装置のセキュリティレベルを評価するための国際標準。ソフトウェア・ハードウェア・ファームウェアなど、セキュリティ機能をもったすべての情報処理製品や情報処理システムを対象とし、それらに必要なセキュリティ対策がされているかの確認をするための基準。

運用・管理

BS7799(ISO/IEC 17799
情報セキュリティマネジメントに関する基準と仕様を規定したドキュメント。二部構成となっており、第一部には、あらゆる業種や規模の組織において共通して適用可能な情報セキュリティの管理方法、第二部には、情報セキュリティ管理システムとして実装するための必要事項を仕様書形式で記載。ISO/IEC 17799は、この第１部である

ISO/IEC TR 13335(GMITS)
GMITSは、情報技術のセキュリティに関連した運用管理、計画を対象とした 国際標準。５部構成となっており、機密性・完全性・可用性・責任追跡性・真正性・信頼性を実現するために必要なプロセス等について広い範囲をカバー。

2.セキュリティ対策の考え方

インターネットを利用したシステムは各企業が導入し、セキュリティ機器の導入もほぼできてきたが、ウィルス含めシステムは常に脅威にさらされている。また内部犯行による情報漏えいも多い。

各企業は、情報システム（情報資産）を守ることが重要であるとの認識が高まり、その情報システムを守るために、さらなるセキュリティを確保しようとしている。

しかし、ただやみくもにセキュリティ確保しても、結局方針を持っていないため、意味のないものになっているのが現実である。そこで情報セキュリティポリシーといったセキュリティを確保するための利用・運用・管理ルールが注目され、国際標準等も出てきている。

2.セキュリティ対策の考え方

今までのセキュリティ対策

セキュリティ関連の機器の導入が主体
・ファイアウォールやＩＤＳ（侵入検知）
・ウィルス対策（サーバ、クライアントでの実施）
・ＶＰＮや認証サーバ

導入しただけでは十分機能せず、日々の運用・管理が重要

システム運用部門だけでなく、利用者も含めて取り組まないとセキュリティを維持することができない

2.セキュリティ対策の考え方

これからのセキュリティ対策

利用者・運用者が主体になり企業全体で取り組む
・人的対策（情報システムの利用方法等）
・技術対策（各セキュリティ機器の導入）
・運用対策（情報システムの運用方法等）
・物理的対策（設備（マシンルーム）等）

利用者全員に教育（なぜ必要か？何をいつどのようにするか？）し同意確認（違反時の罰則有）

新技術取込みや企業のシステムのリスクを定期的に評価・分析をし、問題などは見直しを実施し常にベストな状態に！

3.セキュリティポリシーとは

セキュリティポリシーは、企業の情報システムの利用・運用の方針を、情報システムの利用者や管理者に徹底・遵守させることを目的としたもので、「何を」「誰が」「どのようにして」「どこまで」行うのかを明確に表明したものである。

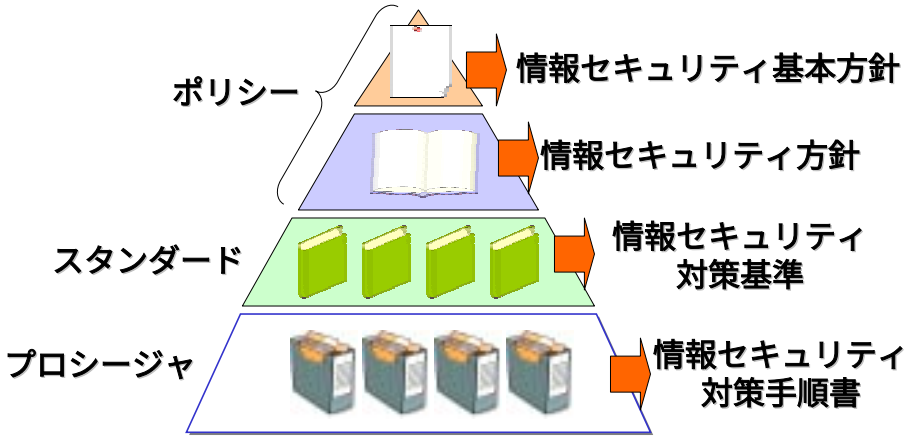
企業の情報システム（ネットワーク・コンピュータ）を、外部や内部からの不正アクセスなどの脅威から守る

情報システムの利用者や管理者のセキュリティ意識を向上させる

企業の情報システムを法的（法律・規定）に守る

3.セキュリティポリシーとは

セキュリティポリシーは、３つの階層で管理。



3.セキュリティポリシーとは

●ポリシー

「セキュリティ基本方針」：

　企業の情報資産を適切に保護・管理することを経営者が意思表明したもの。

「セキュリティ方針」：

　全社に向けて、情報セキュリティの方針を記述したもの。

●スタンダード：「xx標準」

　セキュリティ方針に従い、必要な対策を分野別に規定したもの。

● プロシージャ：

　定められた対策を現場で運用するために、より詳細・具体的に規定したもの。

3.セキュリティポリシーとは

ISO/IEC 17799

1 適用範囲

BS7799のこの第1部では、組織においてセキュリティを開始、実行又は維持することに責任を有する人々が用いるために、情報セキュリティ管理についての勧告を記述する。 その目的は、・・・・・・

9.3.1 パスワードの使用

ユーザは、パスワードの選択及び使用に際しては、正しいセキュリティ慣行に従うことが望ましい。

パスワードは、ユーザIDを確認する手段、ひいては、情報処置施設／設備又はサービスへのアクス権を確立するための手段となる。すべてのユーザは、次の事柄を実行するように助言されることが望ましい。

a) パスワードを秘密にしておく。
b) パスワードのメモは作らない。ただし、メモが安全に保管される場合はその限りでない。
c) システム又はパスワードに対する危険の恐れがある場合は、パスワードを変更する。
d) 最低6文字長の有効なパスワードを選択する。・・・
e) パスワードは定期的に、もしくはアクセス回数に基づいて変え、古いパスワードを再使用したり、循環させて使用したりしない

スタンダード

9. パスワードについての規定

・パスワードは本人が確実に管理でき他人には判りにくいものにすること

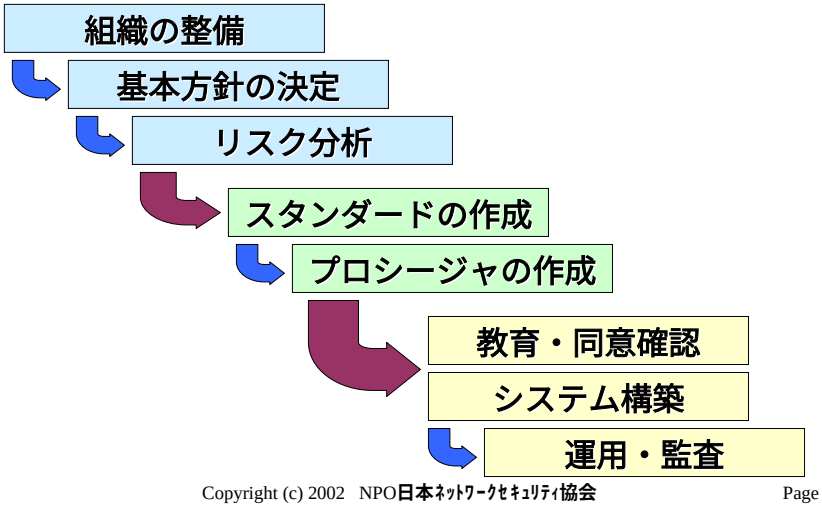
プロシージャ

9. パスワードについての利用手順

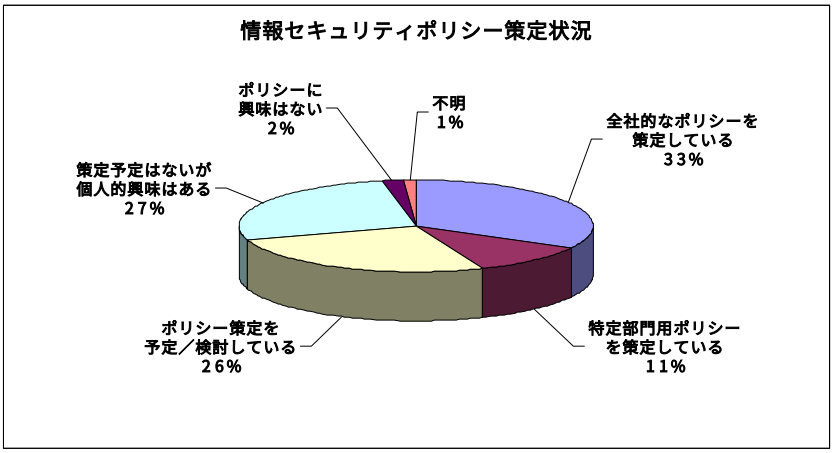
・パスワードは6文字以上でなければならない
・パスワードに氏名、生年月日・電話番号などの個人情報を使用してはならない

3.セキュリティポリシーとは

セキュリティポリシーは、以下の手順で実施。

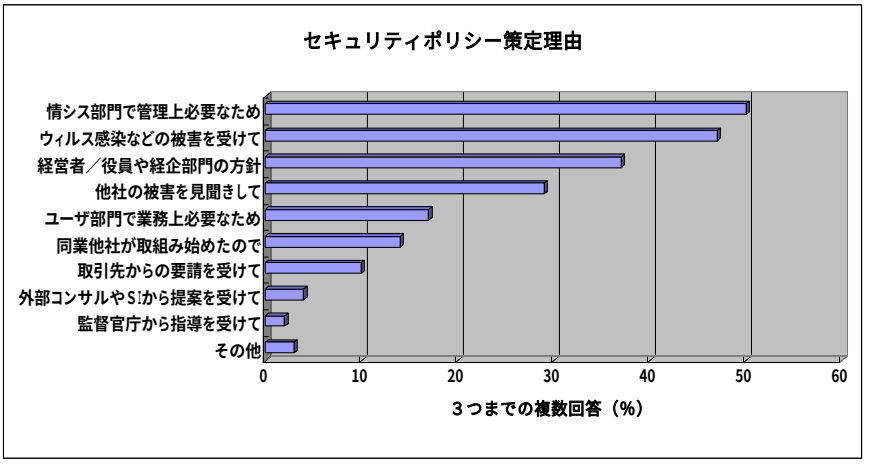


3.セキュリティポリシーとは



参考：Security&Trust読者調査　情報セキュリティポリシーの策定状況は？
http://www.atmarkit.co.jp/fsecurity/survey/survey04/survey01.html

3.セキュリティポリシーとは



参考：Security&Trust読者調査　情報セキュリティポリシーの策定状況は？
http://www.atmarkit.co.jp/fsecurity/survey/survey04/survey01.html

4.セキュリティポリシーの具体例

業界の動向や標準に着目

情報セキュリティポリシーを作成するのに、業界の動向や標準を調査し参考にすることが重要。

金融業界においては、ＦＩＳＣ（The Center for Financial Industry Information Systems）がある。ＦＩＳＣは旧大蔵省の許可を得て、昭和59年11月、金融機関・保険会社・証券会社・コンピュータメーカー・情報処理会社等によって設立された財団であり、金融機関等における金融情報システムの活用や安全性確保等に関する諸問題について調査・研究を行い、指針の提示や提言を行っている機関である。

現在、約8000社の金融機関・保険会社・証券会社・コンピュータメーカー等が会員であり、調査研究の成果の出版、ホームページ公開、講演会、セミナー等様々な活動をしている。

4.セキュリティポリシーの具体例

ＦＩＳＣの出版物の中に『金融機関等のセキュリティポリシーの策定・運用に関する研究会報告書』があり、セキュリティポリシー策定に参考になる。本報告書は、より効果的なセキュリティポリシーの策定や効果的な運用に役立つ情報を提供している。

★研究会報告　　参考ＵＲＬ：http://www.fisc.or.jp/ippan_2.htm

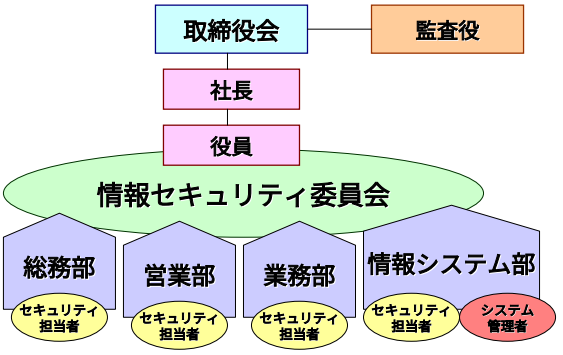
- Ⅰ 調査・研究の概要
- Ⅱ モデル金融機関を事例とした策定・運用プロセスについての討議
  - 1 モデル金融機関の概要
  - 2 セキュリティポリシー策定の立ち上げ
  - 3 セキュリティポリシー（基本方針）の策定
  - 4 セキュリティスタンダード（自社の安全対策基準）の策定
  - 5 セキュリティポリシーの運用
- Ⅲ セキュリティスタンダードのサンプルについて
  - 1 サンプル案について討議した事項
  - 2 サンプル案に反映しなかった項目

★セキュリティスタンダードのサンプル集

★研究会の運営の概要

4.セキュリティポリシーの具体例

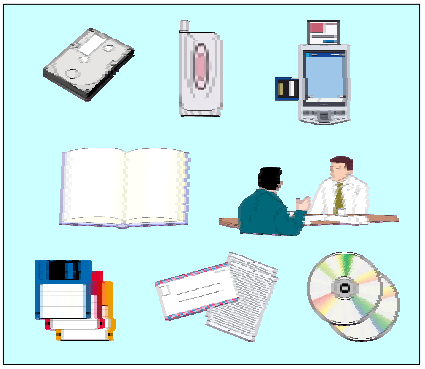
まずはセキュリティ対策の組織作り



情報システムのセキュリティは企業全体で取り組むもの。そのためには、企業のトップ（経営者）を含めた全社的な組織を作り取り組むべき。

4.セキュリティポリシーの具体例

対象範囲はシステム構成機器だけで無い！



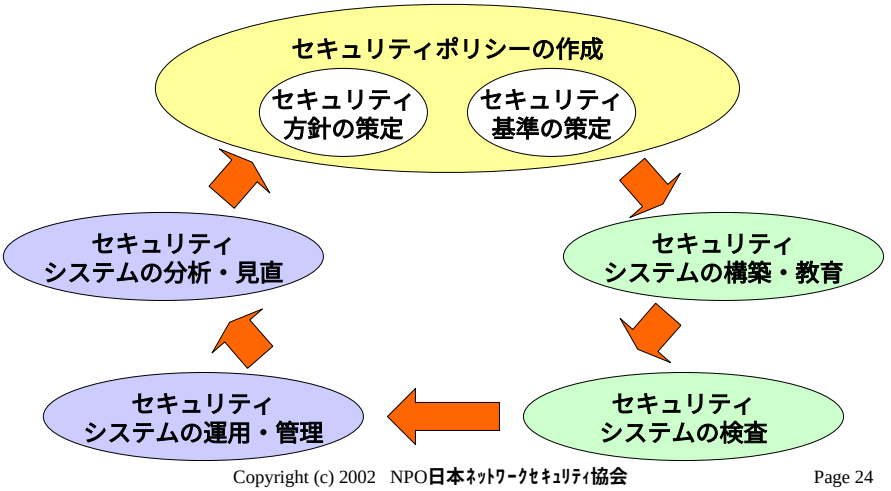
企業が守るべき「情報資産」は必ず しもコンピュータを中心としたシステムに関するものだけでなく、印刷した紙や人間の会話などにも対応すべきである。

4.セキュリティポリシーの具体例

スタンダードは目的に合わせて作成

4.セキュリティポリシーの具体例

セキュリティポリシーのサイクル



4.セキュリティポリシーの具体例

効率的に作成するならサンプルの利用

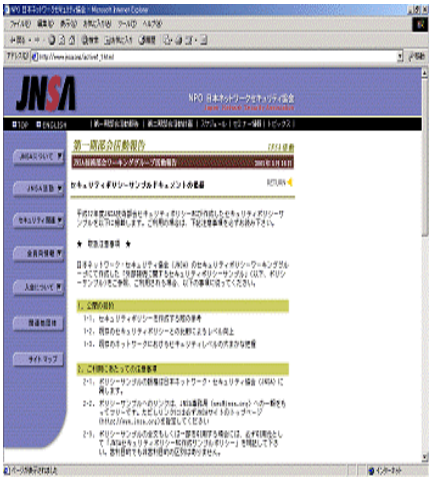
情報セキュリティポリシーを作成するのには、コンサルティングに任せて作成することが多い。これは経験豊かでレベルの高い専門化に任せ質の高いものを作るための手段である。短期間で作成できるがコストがかかる。

またコンサルティングのアドバイスを受けながら情報セキュリティポリシーを作成する手段もある。これは情報システム部門が知識の習得をしながら行うため期間がかかってしまう。

情報セキュリティポリシーを作成する費用を削減したり期間を短縮するためには、サンプルを利用することで実現できる。

しかしサンプルをそのまま利用するのではなく、企業のリスク分析を行い対象範囲や組織構成を含めた十分な検討をし合意をして作成する。できれば専門化（コンサルティング）の支援を得て作成する方がよい。

4.セキュリティポリシーの具体例



NPO日本ネットワークセキュリティ協会（JNSA）
http://www.jnsa.org/policy/guidance

日本ネットワークセキュリティ協会はネットワークセキュリティに関するさまざまな活動を行っている。

「セキュリティポリシー策定WG」では、さまざまなシステムに汎用的に適用できる情報セキュリティポリシーのテンプレート（ひな型）が必要と考え、仮想企業における情報セキュリティシステムの構築・運用のための情報セキュリティポリシーのサンプルを作成し公開している。

★雑誌「N+I NETWORK Guide」の６月～１月まで連載で解説中！

ポリシーサンプルの構成

- ポリシー
  情報セキュリティ基本方針
  情報セキュリティ方針
- スタンダード
  情報セキュリティ対策標準（概要）
  情報セキュリティ対策標準集：全２９項目
- プロシージャ
  （現在は公開無（未作成））

対策基準の項目（1）

- サーバ対策
  - ユーザ認証に関する標準
  - アカウント管理標準
  - ソフトウェア／ハードウェアの購入及び導入標準
  - サーバ等に関するセキュリティ標準
  - 外部公開サーバに関する標準

4.セキュリティポリシーの具体例

対策基準の項目（２）

- クライアント対策
  - クライアント等におけるセキュリティ対策標準
  - ウィルス対策標準
  - 電子メール利用標準
  - Webサービス使用標準

4.セキュリティポリシーの具体例

対策基準の項目（３）

- ネットワーク対策
  - ネットワーク構築標準
  - LANにおけるPC（サーバ、クライアント等）設置／変更／撤去の標準
  - 社内ネットワーク利用標準
  - 専用線及びVPNに関する標準
  - リモートアクセスサービス利用標準

4.セキュリティポリシーの具体例

対策基準の項目（4）

- 物理的対策
  - サーバルームに関する標準
  - 物理的対策標準
  - 職場環境におけるセキュリティ標準
  - 媒体の取扱に関する標準

4.セキュリティポリシーの具体例

対策基準の項目（5）

- セキュリティ運用対策
  - システム維持に関する標準
  - システム監視に関する標準
  - セキュリティ情報収集および配信標準
  - セキュリティインシデント報告・対応標準
  - 監査標準

4.セキュリティポリシーの具体例

対策基準の項目（6）

- その他
  - 第三者契約に関する標準
  - プライバシーに関する標準
  - セキュリティ教育に関する標準
  - 罰則に関する標準
  - スタンダード更新手順
  - プロシージャ配布の標準

4.セキュリティポリシーの具体例

ユーザ認証標準

1　目的

2　対象者

3　対象システム

4　遵守事項

まとめ

まず情報セキュリティポリシーの作成！！
・脅威に対する具体的な対策をしているのか？
・各システムに対するリスクはどうなっているのか？
・国内及び国際的なセキュリティ標準に準拠
を考え、企業の取り組みを外部アピール

技術（システム）的対策＋人的対策＋管理対策
への対応を確認（定期的な監査・評価・改版）

情報セキュリティポリシーの教育と同意
最新の技術でのシステム構築
そして一人一人のセキュリティ対策実施

NPO日本ネットワークセキュリティ協会（JNSA）
http://www.jnsa.org/