JNSA

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WG活動報告

土屋　茂樹

㈱NTTデータ

2004年5月18日

活動目的

- セキュリティポリシーの必要性は浸透しつつあるが、実際に作成するとなると、具体的なイメージがつかみにくい。
- WG内で仮想企業を想定し、そこで適用されるポリシーを作成することで、雛型として広く利用できることを目指している。

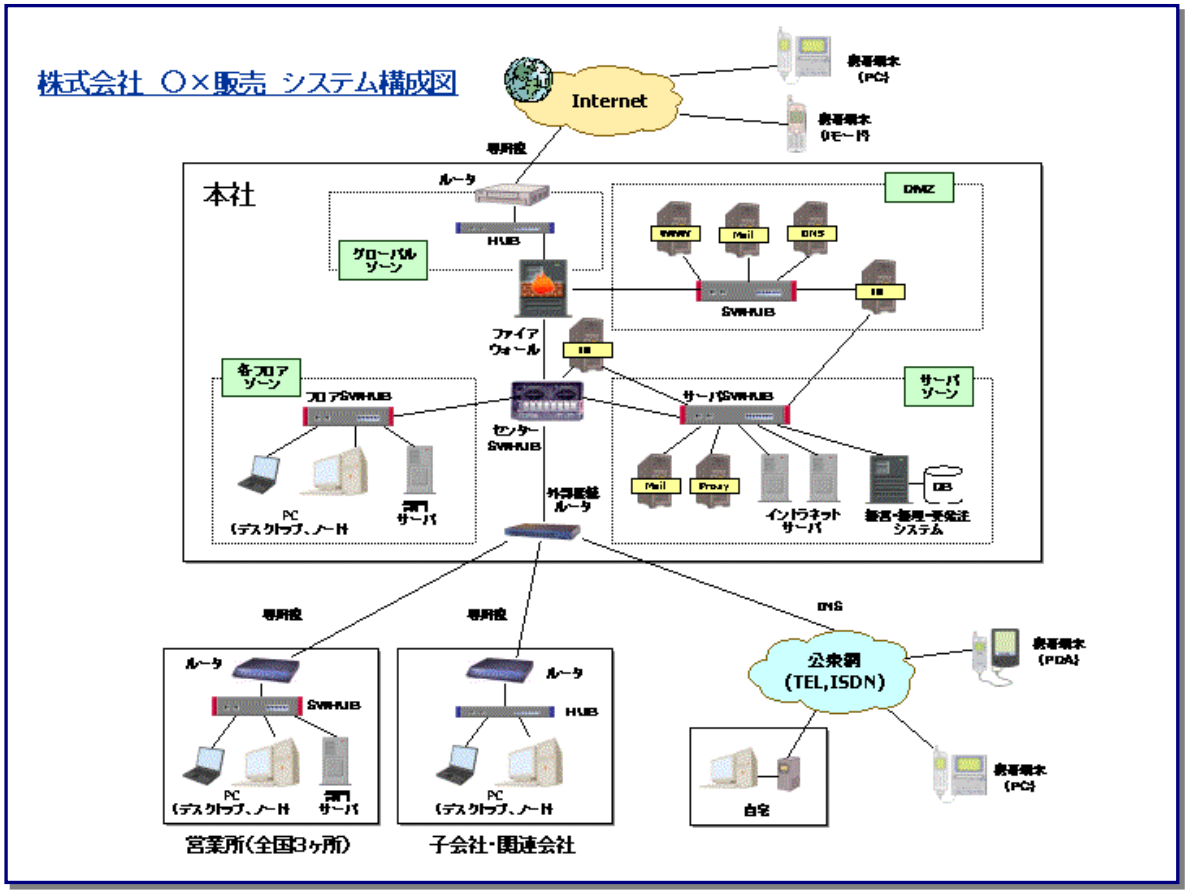
活動内容

- H１２年度は外部ネットワーク接続に限定したポリシーを策定した。
- H１３年度はポリシーの適用範囲を一般的な企業活動全般に広げて策定した。
- H１４年度はポリシーに解説を加えて、読者組織への適用の手助けとなるようにした。
- H１５年度はポリシーから脅威･脆弱性および残存脅威を導いた。

想定企業

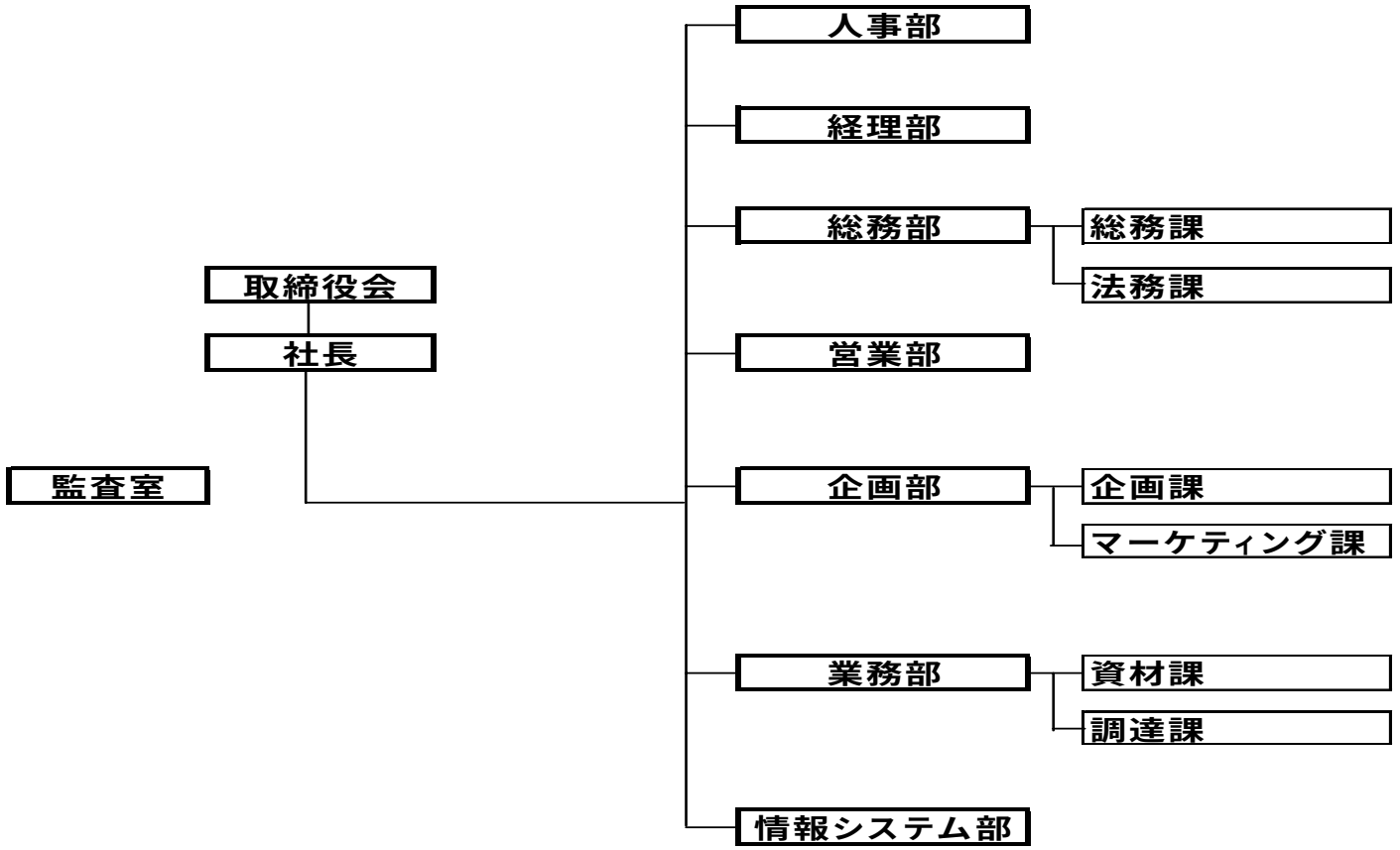
- 流通系の会社（社内開発は行わない）
- 本社以外に、営業所や子会社等があり、専用線で接続されている
- 本社はインターネット接続されている
- 社外からのリモートアクセスが可能である

ポリシーの適用範囲

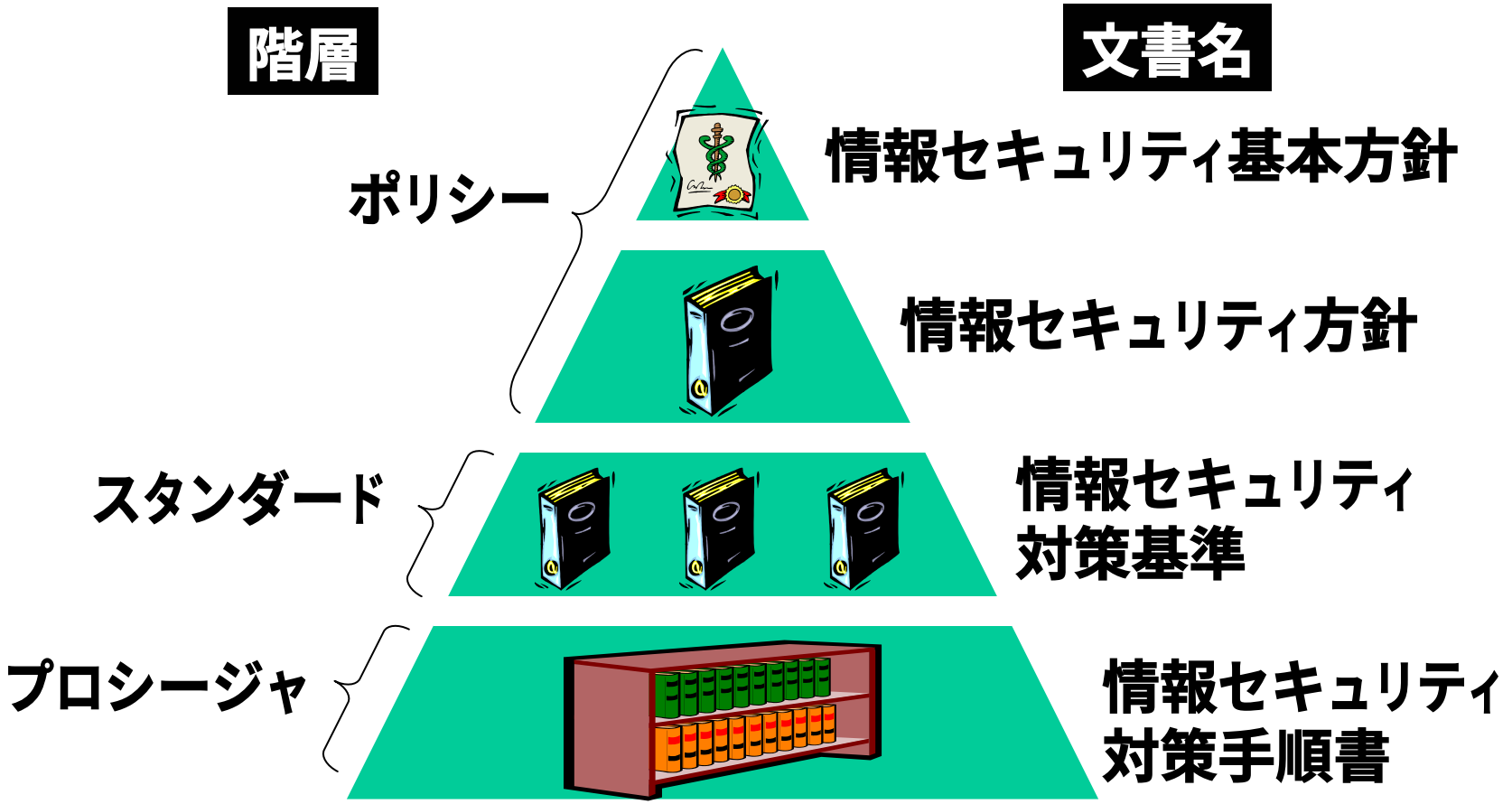


組織体制

<A社組織図>



ポリシー関連文書群の構成



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

スタンダード項目一覧

項番	スタンダード項目
1	ソフトウェア／ハードウェアの購入及び導入標準
2	委託時の契約に関する標準
3	サーバルームに関する標準
4	物理的対策基準
5	職場環境におけるセキュリティ標準
6	ネットワーク構築標準
7	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
8	サーバー等に関する標準
9	クライアント等におけるセキュリティ対策標準
10	社内ネットワーク利用標準
11	ユーザー認証標準
12	ウィルス対策標準
13	電子メールサービス利用標準
14	Ｗｅｂサービス利用標準
15	リモートアクセスサービス利用標準
16	媒体の取扱いに関する標準
17	アカウント管理標準
18	システム維持に関する標準
19	監視に関する標準
20	プライバシーに関する標準
21	セキュリティ情報収集及び配信標準
22	セキュリティインシデント報告、対応標準
23	監査標準
24	セキュリティ教育に関する標準
25	罰則に関する標準
26	スタンダード更新手順
27	専用線及びVPNに関する標準
28	外部公開サーバに関する標準
29	プロシージャ配布の標準

成果物イメージ

脅威

脆弱性

ポリシー

残存リスク

NO	脅威	脆弱性		遵守事項（JNSAポリシーサ…ルv0．92a版）			残存リスク
				項番	項タイトル	内容	
1	・社外の第三者からウイルス付メールを送信されたことによるウィルス感染 ・メールが利用できないことによる業務停止	・クライアントが勝手にメールソフトを選択すること ・セキュリティ上脆弱なメールソフトを利用すること ・ヘルプデスクが対応できないこと	⇨	4.1(1)	電子メールサービス利用端末機器のセキュリティ	電子メールの送受信にあたっては、情報セキュリティ委員会が指定した電子メールソフトウェアを用いなければならない。また、情報セキュリティ委員会の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。	・クライアントＰＣ設定もれ。 ・パターンファイルの更新もれ ・システム管理者設定ミス ・セキュリティパッチの適用漏れ
2	・社外の第三者からウイルス付メールを送信されたことによるウィルス感染	・クライアントが勝手にメールソフトの設定をしていること ・OSのパッチがあたっていない ・指定された機種を使用していない	⇨	4.1(2)	電子メールサービス利用端末機器のセキュリティ	上記ソフトウェアを使用するコンピュータは、『ソフトウェア/ハードウェアの購入および導入標準』に基づいて導入され、『クライアント等におけるセキュリティ対策標準』に基づいたセキュリティ対策を施したものでなければならない。	・指定されていないOSを例外的に使用した場合のサポート不可
3	・管理者による不正アクセス ・ソーシャルエンジニアリング	・初期パスワードをそのまま使っていること ・初期パスワードが漏えいすること	⇨	4.1(3)	電子メールサービス利用端末機器のセキュリティ	電子メールアドレスは初期パスワードとともに発行される。初期パスワードは直ちに変更しなければならない。	・遵守規定が徹底されず、初期パスワードのまま利用されてしまうこと ・システム管理者の不正によるパスワード漏洩

アカウント管理標準

ポリシー

アカウントに与えられている権限を変更する場合には、新規アカウントの発行と同様に人事権を持つ管理職を通してシステム管理者に申請する。

脅威

- 本来、必要でないシステム権限を用いた不正アクセスの試み。

脆弱性

- システム管理者が人事面を考慮した権限の妥当性チェックを適切に行なえないこと。

残存脅威

- 適切な承認ルートを介さずにシステム権限が変更されてしまうこと。

電子メールサービス利用標準

JNSA

ポリシー

電子メールの送受信にあたっては、情報セキュリティ委員会が指定した電子メールソフトウェアを用いなければならない。また、情報セキュリティ委員会の指示に従い、当該ソフトウェアのバージョンアップを行わなければならない。

脅威

- 社外の第三者からウイルス付メールを送信されたことによるウィルス感染
- メールが利用できないことによる業務停止

脆弱性

- クライアントが勝手にメールソフトを選択すること
- セキュリティ上脆弱なメールソフトを利用すること
- ヘルプデスクが対応できないこと

残存脅威

- クライアントＰＣ設定もれ。
- パターンファイルの更新もれ
- システム管理者設定ミス
- セキュリティパッチの適用漏れ

リモートアクセスサービス利用標準

ポリシー

利用者は、ダイヤルアップルータおよびサーバ･モデムなどによる社内ネットワークへの接続手段を、情報システム部の許可を得ることなく設置してはならない。

脅威

- 第三者によるシステムへの不正アクセス

脆弱性

- 情報システム部がネットワーク機器を管理しきれない

残存脅威

- 利用者の設置ミスにより予期しない接続ポイントができている可能性。

職場環境におけるセキュリティ標準

ポリシー

従業員は重要度の高い書類や媒体を施錠保管し、特に必要な場合は耐火金庫･耐熱金庫に保管しなければならない。

脅威

- 重要度の高い書類や媒体等の盗難や火災による焼失

脆弱性

･盗難や火災を考慮して、情報資産(書類や媒体)を重要度に応じた適切な場所（施錠されたキャビネットや耐火金庫など）に保管していないこと

残存脅威

- キャビネットや金庫等の保管場所の鍵の管理が杜撰な場合、盗難のリスクがある。
- 金庫の盗難･紛失の恐れ。
- 金庫の耐火性能･耐熱時間を超える火災による、焼失の恐れ。

セキュリティインシデント報告・対応標準

ポリシー

情報セキュリティ委員会は、各システムの復旧優先度を決定しなければならない。復旧優先度の決定は、対象システムにおいて運用される業務の停止許容時間を観点において行う。

脅威

- 各種インシデントの発生によるサービスの停止。

脆弱性

- インシデント発生時にどのサービスを優先的に復旧させればいいかがわからず、復旧の遅れ等により損失が発生すること。

残存脅威

- 優先度の低いシステムの復旧が遅れることによる損失。
- 復旧優先度の設定ミスによる損失。
- 許容時間内に発生する損失。

Ｈ１６年度活動方針

今まで作成し公開しているサンプルを全面改訂

- ＩＳＭＳ及びＸ５０８０との適合性を確認
- サンプルの見直しを行い改版作業
  （特にポリシー（基本方針など）を改訂）
- 適用者（利用者、管理者）などを明確にする
- セキュリティ技術の実装（構築）との関係検討

月に１回程度のＷＧ開催を検討結果のレビュー
秋の合宿でサンプル等の改訂開始予定

WGに参加しませんか？

- さまざまな企業の方々と一緒に議論をしながら、楽しく活動をしています。
- 検討に参加することで、ポリシー策定のプロセスを理解できます。
- ご興味のある方は事務局までご連絡ください。