セキュリティポリシーWG活動報告「ポリシー・サンプルの解釈と応用」

2003年 6月 4日

ポリシーWG　リーダ
(株) NTTデータ　土屋茂樹

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。

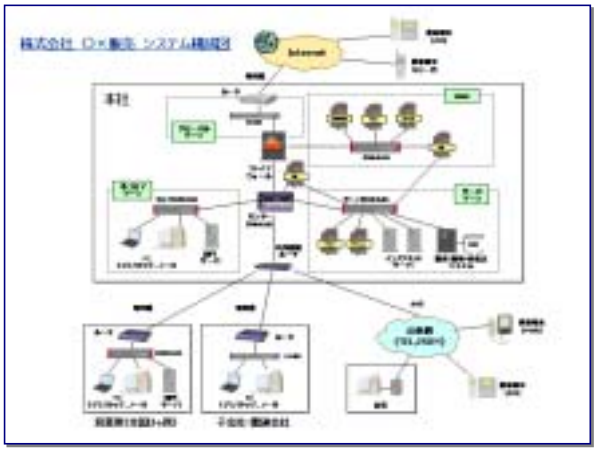
活動内容

- 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。

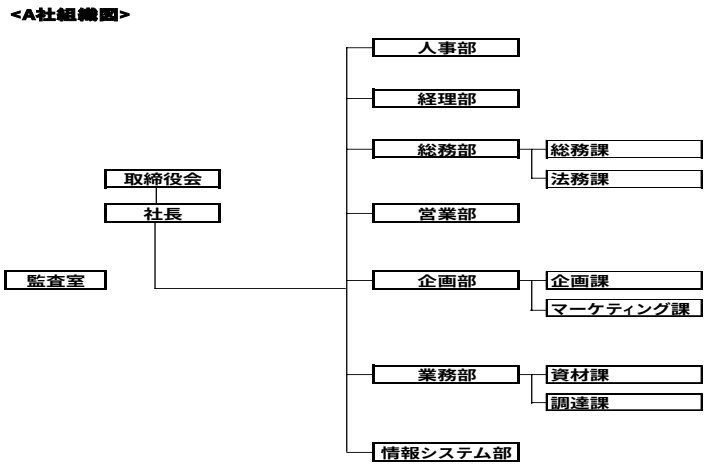
想定企業

- 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

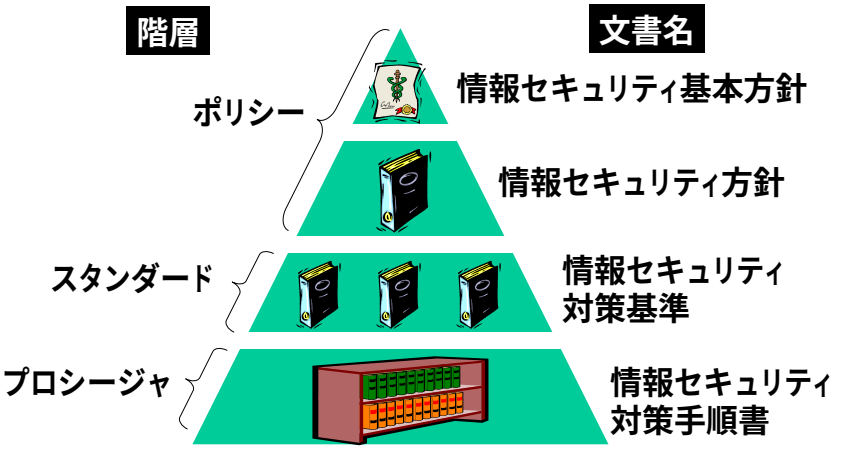
ポリシーの適用範囲



組織体制



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

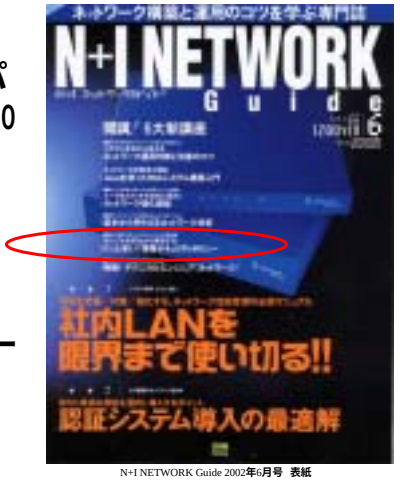
スタンダード項目一覧

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

N+I Network Guideへの連載

「N+I Network Guide」（ソフトバンクパブリッシング）にて、２００２年６月～２００３年１月まで計８回の連載を実施。

＜連載タイトル＞
セキュリティ対策講座
サンプルを見ながら策定する
ドンと来い！情報セキュリティポリシー



N+I NETWORK Guide 2002年6月号 表紙

ポリシー・サンプル解説書目次

連載		タイトル	解説対象のポリシー・サンプル
第1回	解説編	情報セキュリティ対策とポリシーの関係	情報セキュリティ基本方針 情報セキュリティ方針
第2回	準備編	スタンダードの策定内容と構成	情報セキュリティ対策標準
第3回	作成編	サーバ対策なんてドンと来い	ユーザ認証標準 アカウント管理標準 外部公開サーバに関する標準
第4回		クライアント対策なんてドンと来い	クライアント等におけるセキュリティ対策標準 ウイルス対策標準 電子メール利用標準 Webサービス利用標準
第5回		ネットワーク対策なんてドンと来い	ネットワーク接続標準 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 リモートアクセスサービス利用標準
第6回		物理的な対策なんてドンと来い	物理的対策標準 サーバールームに関する標準 環境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
第7回		セキュリティ運用なんてドンと来い	システム維持に関する標準 システム監視に関する標準 セキュリティインシデント報告、対応標準
第8回		その他いろいろなんでもござれ集	監査標準 セキュリティ教育に関する標準 委託時の契約に関する標準

解説内容例（1）

サンプル名	ユーザ認証標準
記述	＜パスワードを忘れた場合の処置＞ （1）利用者がパスワードを忘れた場合には、システム管理者に新規パスワード発行の申請を行わなければならない。 （2）システム管理者は、申請してきた利用者が本当に本人自身であることを何らかの方法で確認しなければならない。 （3）新規パスワード発行の申請を受けたシステム管理者は、速やかに新規のパスワードを発行して、利用者に通知しなければならない。
解説のポイント	・システム管理者は、現状のパスワードを教えるべきか、否か –複数のシステムに同じパスワードを設定している ・申請方法は何がよいか –電子メール、電話、書類、出頭 ・本人確認方法は何がよいか –メールヘッダ情報（電子メール）、電話？ ・その他盛り込むべき内容 –規定回数以上間違えた場合、アカウントを自動的にロック –発行した新規パスワードの通知方法

解説内容例（2）

サンプル名	アカウント管理標準
記述	＜新規アカウントの発行＞ （1）新規のアカウントが必要になった場合には、必要な権限と共に人事権を持った管理者に申請する。 （2）申請を受けた人事権を持った管理者は、必要な権限と必要性を検討し、妥当と判断した場合には、システム管理者に新規アカウントの発行を申請する。
解説のポイント	・アカウントの申請には、誰の承認が必要か –人事権を持った管理者が承認／特になし –当該アカウントで実行できるレベルに応じた運用 ・申請は誰が行うか –申請者本人、人事権を持った管理者 ・その他盛り込むべき内容 –申請内容について記録の保存 –アカウントの共有について許容するか

解説内容例（3）

サンプル名	クライアント等におけるセキュリティ対策標準
記述	＜私物ＰＣの使用禁止＞ （1）当社の業務において、従業員が使用できるＰＣは、当者が支給・貸与したＰＣのみとする。 （2）いかなる場合でも、当者システム環境に私物ＰＣを接続・利用してはならない。
解説のポイント	・私物ＰＣの使用を禁止できるか –私用でウィルスに感染し、社内接続時に蔓延させる可能性 –契約社員が、所属元で支給されたＰＣを使う –ＰＤＡの取扱いをどうするか ・その他盛り込むべき内容 –もし私物ＰＣの接続・利用を許可する場合には、その条件を示す

解説内容例（4）

サンプル名	ネットワーク構築標準
記述	＜無線ＬＡＮについて＞ （1）ネットワーク接続構成 ●スイッチングハブ（レイヤ3、レイヤ2）とハブを使用し、ビル内のネットワークとする
解説のポイント	・無線ＬＡＮの導入を許可するか –メリットは大きいが脅威も大きい –導入する場合、どのレイヤでどの対策を実施するか。（物理層、データリング層、ネットワーク層・・） ・その他盛り込むべき内容 –導入を許可する場合の承認体制の確立 –有線ＬＡＮセグメントと無線ＬＡＮセグメントの分離

解説内容例（5）

サンプル名	物理的対策標準
記述	＜サーバルームの設置＞ （1）サーバルームは独立した部屋として設置し、一般オフィスとの共用や他社オフィスとの隣接は避けなければならない。 （3）サーバルームの外観は目立ちにくいものとし、室名表示等も最小限にとどめなければならない。 （4）サーバルームの出入り口は原則1ヶ所に限定し、施錠設備を設けなければならない。
解説のポイント	・独立した部屋を確保できるか –扱う資産の重要性、脅威、コスト等に基づく ・区画の区切り方をどうするか –部屋、鍵付きラック、パーティション ・目立ちにくさをどのように考えるか –表示しないことで、第三者が気づきにくいことによって外部脅威を低減する –窓等を設けて、第三者が監視できる状態を作って内部脅威を低減する ・その他盛り込むべき内容 –電磁波漏洩についての考慮 –情報種別に応じた区画の定義

解説内容例（6）

サンプル名	システム監視に関する標準
記述	＜対象システムのログによる監視について＞ （1）情報システム部は、対象システムに関して次にあげるログを取得すること。なお取得されたログは２４時間以内に書き換え不能なメディアに転送し、3年間、安全に保存すること。 取得対象：①ログオン、ログオフの記録　②‥　③‥　④‥　⑤‥ 取得内容：①アクセス時刻　②‥　③‥　④‥　（※　‥は記述省略） （2）情報システム部は、許可された処理だけが実行されていることを確認するために、ログを月1回確認すること。
解説のポイント	・ログは保管するだけか、解析するか –定期的なログ解析は人件費を増大させるが、侵害の検知が迅速になる ・ログをとる目的は何か –不正アクセス時に犯人を特定する、システム障害の原因を切り分ける ・ログの保管期間はどの程度か –究明したい原因が発生してから、ログ解析が終了するまでの見積 ・その他盛り込むべき内容 –システムの重要度に応じた監視体制の記述 –システム以外の監視の記述（入退室管理など）

解説内容例（7）

サンプル名	監査標準
記述	＜監査人の選定について＞ （1）監査組織は、被監査組織、対象に対して独立していなければならない。もし独立した監査組織を構成できない場合には、相互監査体制をとることで、できる限り独立性を維持しなければならない。
解説のポイント	・すべての部門から独立した組織によって実行可能か –外部に監査を依頼する –社内の独立した監査人が行う –相互監査を行う –自己検査を行う ・その他盛り込むべき内容 –監査基準を誰が策定するか –他のマネジメントシステム（ISO9000等）との整合性

ポリシー･サンプルの入手

ポリシー･サンプルは、ＪＮＳＡホームページよりダウンロードできます。
http://www.jnsa.org/policy/guidance

ポリシー･サンプル解説書は、ＪＮＳＡ事務局までお問い合わせください。

Ｈ１５年度の活動

- Ｈ１４年度の成果物について、定義された対策から脅威と脆弱性を洗い出し、対策の妥当性についての分析を行っていきます。

対象標準	アカウント管理標準			
該当項番	遵守事項	脅威	脆弱性	残存リスク
4.1(1)	新規のアカウントが必要になった場合には、必要な権限と共に人事権を持った管理者に申請する。	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。	本来、必要な範囲を超えてシステム権限を付与してしまうこと。	
4.1(2)	申請を受けた人事権を持った管理者は、必要な権限と必要性を検討し、妥当と判断した場合には、システム管理者に新規アカウントの発行を申請する。	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。	システム管理者だけでは、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可能性があること。 申請者が本来、必要とされる範囲以上の権限を申請すること。	・適切な承認ルートを介さずにシステム権限が設定されてしまうこと。 ・人事権を持った管理者からシステム管理者への指示ミス ・システム管理者の設定ミス
4.1(3)	申請を受けたシステム管理者は、申請を受けたアカウントに必要最小限のアクセス権限を設定する。	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。	本来、必要な範囲を超えてシステム権限を付与してしまうこと。	

成果について

- WGで作成したポリシーは公開します。
- ポリシーは、組織の存在意義、文化、活動内容などによって大きく変わります。よって、WGの成果物をそのまま流用するのではなく、組織に合った内容に修正してください。

引用時の注意

- ポリシーサンプルの版権は日本ネットワーク・セキュリティ協会（JNSA）に属します。
- ポリシーサンプルへのリンクは、JNSA事務局（sec@jnsa.org）への一報をもってフリーです。ただしリンクには必ずJNSAサイトのトップページ（http://www.jnsa.org）を指定してください。
- ポリシーサンプルの全文もしくは一部を引用する場合には、必ず引用元として「JNSA セキュリティポリシーWG作成サンプルポリシー」を明記して下さい。営利目的でも非営利目的の区別はありません。
- ポリシーサンプルを利用したことによって生ずるいかなる損害に関してもJNSAは一切責任を負わないものとします。
- 本ポリシーサンプルを報道などマスコミで用いられる場合には、JNSA事務局にご一報ください。

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。