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

小杉 聖一

ＮＥＣソフト株式会社

2005 年 6 月 13日

WGの活動目的

セキュリティポリシーは、セキュリティマネジメントを実施するために必須のものであり、導入が進められている。
実際に策定する場合、以下の点に注意が必要である。

・規格、標準、法令などの理解
・何を決めればいいのか？の判断
・何に注意しなければならないのか？の知識

ポリシーWGでは、セキュリティポリシー策定のポイントをISMS認証基準などを参考にし、リスク分析や規程書（ドキュメント）作成のポイントや実際の実装方法について情報公開をする。

Copyright (c) 2005 NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会 Page 2

Copyright (C) 2000-2005 NPO日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

今までの活動内容

	活動内容	成果物
2000年度	WGの活動開始	・外部接続に関する セキュリティポリシー公開
2001年度	一般向けポリシーの作成	・情報セキュリティポリシー サンプルドキュメント公開(0.91)
2002年度	一般向けポリシーの改版	・N+I NETWORK Guideの中で サンプルポリシー解説 ・情報セキュリティポリシー サンプルドキュメント公開(0.92)
2003年度	ポリシー作成のポイント を作成	・脅威と脆弱性及び 残存リスク対応表公開

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 3

2004年度の活動にあたって

公開している情報セキュリティサンプルポリシーの改版を実施する。

☆改版のために考えたこと

・作成して3年経過し内容が時代にマッチしていない
・日本で導入されている「ISMS認証基準」を考慮
（他の標準や規格なども考慮）
・ポリシーを実装するための具他的な対策の明確化

実際には2004年度は2つのテーマで活動する。

テーマ1：サンプルポリシーとISMS認証基準の対応確認
テーマ2：ポリシー（管理策）に対応した技術策の調査

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会 Page 4

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

Aチームの活動内容

公開している情報セキュリティサンプルポリシーがISMS認証基準にどれだけ対応しているか？の調査実施

☆調査のための活動内容

・ISMS認証基準(ver2.0)とのチェックシートを作成
→ISMS認証基準だけでは詳細な部分が不明
→JIS X5080と加えたチェックシートを作成
・WGの各メンバで分担しサンプルポリシーの対応状況を確認
・WG（Aチーム）でのレビュー実施

定期的なWGを開催し、各メンバが作成したチェックシートをレビューしほぼ完了。完成したチェックシートを近日公開予定。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Aチームの活動結果[1/4]

以下に示すJIS X5080の項番について、公開している情報セキュリティサンプルポリシーのどこに対応しているか？を確認。無い場合には、記載すべき内容を検討。

☆調査したJIS X5080の項番

4. 組織のセキュリティ
5. 資産の分類及び管理
6. 人的セキュリティ
7. 物理的及び環境的セキュリティ
8. 通信及び運用管理
9. アクセス制限
10. システムの開発及び保守
11. 事業継続管理
12. 適合性

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

Aチームの活動結果[2/4]

ISMS認証基準(Ver2.0)

8.(5) ネットワークの管理
①ネットワーク管理策
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こと。

JIS X5080のサブコントール

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
2)ネットワークの管理者は、ネットワークに接続したサービスを無認可のアクセスから保護することを確実にすること
・
・

※ ISMS認証基準(ver2.0)は、財団法人日本情報処理開発協会(JIPDEC)発行「ISMS認証基準(Ver2.0) JIP-ISMS100-2.0」から引用
JIS X5080は、日本規格協会発行「情報技術－情報セキュリティマネジメントの実践のための規範 JIS X 5080:2002」から引用

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Aチームの活動結果[3/4]

チェック結果

JNSAサンプル項番：8.(5)の①の1) 該当は無し

JNSAサンプル項番：8.(5)の①の2)
ネットワーク構築標準
4.1. 全般規定
(4)インターネット接続環境には、不正アクセスを防止するために仕組みを設置し、不正アクセスを検出した場合には速やかにセキュリティ委員会に報告しなければならない

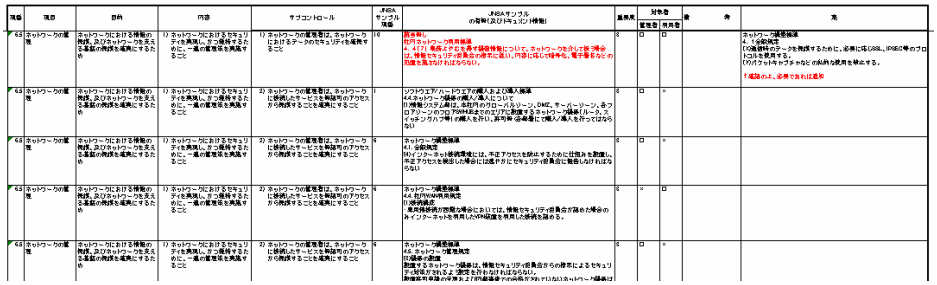
重要度：3 対象者： 管理者：○ 利用者：×

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

Aチームの活動結果[4/4]

☆チェックシート（例）



※ ISMS認証基準(ver2.0)は、財団法人日本情報処置開発協会(JIPDEC)発行「ISMS認証基準(Ver2.0) JIP-ISMS100-2.0」から引用
JIS X5080は、日本規格協会発行「情報技術－情報セキュリティマネジメントの実践のための規範 JIS X 5080:2002」から引用

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Bチームの活動内容

公開している情報セキュリティサンプルポリシーの管理策を実装する時に必要な具体的対策を明確化する。
特に技術的対策について調査する。

☆調査のための活動内容

・脆弱性を列挙しその脆弱性に対応するコントロールを検討
・E-COMは意識しない
・ISMS認証基準(ver2.0)の項目で対応表を作成
・WGの各メンバで分担し検討しレビューを実施

作業を進める中で、当初考えていたことよりも、技術的実装が可能な部分が少ないことや、実装可能なものについても、技術的対策の選択肢が広く最適な選択が困難であることが判った。完成した対応表を中間報告として近日公開予定。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

Bチームの活動結果[1/5]

対応表は、ISMS認証基準（Ver. 2.0）の各管理策について、具体的な実施策、とりわけ技術的な実装策にブレークダウンしたもので、各コントロールについて以下の項目から構成されます。

・項目
・目的
・管理策
・実施策の例
・適用可能な技術、製品など
・解説が必要な用語

実施策は、複数記述可とし技術的な事項のみに限らず、実施可能な方策を記述。多数の実施策が考えられる場合は、最も一般的と考えられるものを、2，3個記述。

適用可能な技術、製品などは、実施にあたって利用意可能なセキュリティ技術、サービス、製品とその利用方法を簡単に記述

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Bチームの活動結果[2/5]

ISMS認証基準(Ver2.0)

9．(4)
ネットワークのアクセス制御
ネットワークを介したサービスの保護のため
①ネットワークサービス利用についての個別方針
利用者には、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること

解釈

サブコントロールを見る限り、どちらかといえばポリシー面での記述だが、技術的には必要最小限のサービスのみを公開し、その他のサービスへのアクセスを行わせないこと、つまりアクセス制御、要塞化などのことと考えるべき

※ ISMS認証基準(ver2.0)は、財団法人日本情報処理開発協会(JIPDEC)発行「ISMS認証基準(Ver2.0) JIP-ISMS100-2.0」から引用
JIS X5080は、日本規格協会発行「情報技術－情報セキュリティマネジメントの実践のための規範 JIS X 5080:2002」から引用

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

Bチームの活動結果[3/5]

実施策の例

サービスを提供するホストにおいては、不要なサービスを可能な限り停止すること。
もし、停止が不可能な場合はサービス（ホスト）が存在するネットワークと他のネットワークとの境界、もしくはサービスを提供するホスト自身において、当該サービスにアクセスする必要がある者が存在しないネットワークから、当該機器またはサービスへの到達を禁止する措置をとる。

・ネットワークアドレス単位のフィルタリング
・サービスポート番号単位のフィルタリングなど

各ネットワークで一律的な禁止が困難な場合は、個々のアドレス単位もしくはネットワークにおけるユーザ認証機能等を併用する

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Bチームの活動結果[4/5]

適用可能な技術・製品など

・サーバ要塞化技術
・ルータ、スイッチ、ファイアウォール等におけるＡＣＬによるフィルタ機能
・当該サービスを行う機器（ＯＳ）等が持つ、もしくは別途導入するフィルタリング機能（ホストベースのファイアウォールソフトウエア等）
・ファイアウォール製品が持つユーザ認証による通過制御機能

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

Bチームの活動結果[5/5]

☆対応表（例）

項目	目的	コントロール	実施策の例	適用可能な技術・製品など	解説が必要な用語
9．(4) ネットワークのアクセス制御	ネットワークを介したサービスの保護のため	a. (4)のネットワークサービス利用についての個別方針 利用者には、使用することが特別に認可されたサービスへの直接のアクセスだけが提供されること (解説) ・サブコントロールを見る限り、どちらかというとポリシー面での記述だが、技術的には必要最小限のサービスのみを公開し、その他のサービスへのアクセスを行わせないこと、つまりアクセス制御、要塞化などのことと考えるべき	サービスを提供するホスト）においては不要なサービスを可能な限り停止すること。もし、停止が不可能な場合はサービス（ホスト）が存在するネットワークと他のネットワークとの境界、もしくはサービスを提供するホスト自身において、当該サービスにアクセスする必要がある者が存在しないネットワークから、当該機器またはサービスへの到達を禁止する措置をとる ・ネットワークアドレス単位のフィルタリング ・サービスポート番号単位のフィルタリングなど 各ネットワークで一律的な禁止が困難な場合は、個々のアドレス単位もしくはネットワークにおけるユーザ認証機能等を併用する	サーバ要塞化技術	要塞化
				ルータ、スイッチ、ファイアウォール等におけるACLによるフィルタ機能	ACL
				当該サービスを行う機器（OS）等が持つ、もしくは別途導入するフィルタリング機能（ホストベースのファイアウォールソフトウエア等）	
				ファイアウォール製品が持つユーザ認証による通信制御機能	
		a. (4)②指定された接続経路 利用者端末からコンピュータサービスまでの経路は管理すること。 (解説)	利用者端末を接続出来るネットワークが複数ある場合は、接続されたネットワークや接続方法をネットワークアドレス等から識別可能な方策を講じる。 （たとえば、以下のようなもの）	内部端末のIPアドレス固定化による識別（登録端末とそうでないものを割り当てるアドレス範囲で識別：不正IP割り当ての検知策を併用）	
				DHCPサーバへのMACアドレス登録による端末固有IPアドレスの割り当て（登録端末でネットワークの接続性を	DHCP

※ ISMS認証基準(ver2.0)は、財団法人日本情報処理開発協会(JIPDEC)発行「ISMS認証基準(Ver2.0) JIP-ISMS100-2.0」から引用
JIS X5080は、日本規格協会発行「情報技術－情報セキュリティマネジメントの実践のための規範 JIS X 5080:2002」から引用

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

2005年度の活動方針

2005年の活動を継続実施。

ISMS認証基準にマッチしたサンプルポリシーを公開し、実際の策定方法を討議。また管理策に対応する適用すべきセキュリティ技術との対応についても調査し報告。

月に1回程度の定例会、年1回（秋頃）の合宿、メーリングリストによるドキュメント作成。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会

WGに参加しませんか？

JNSA

2005年の活動を近日開始！

- 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。

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

JNSA

JNSA

Copyright (c) 2005 NPO日本ネットワークセキュリティ協会

Copyright (C) 2000-2005 NPO日本ネットワークセキュリティ協会