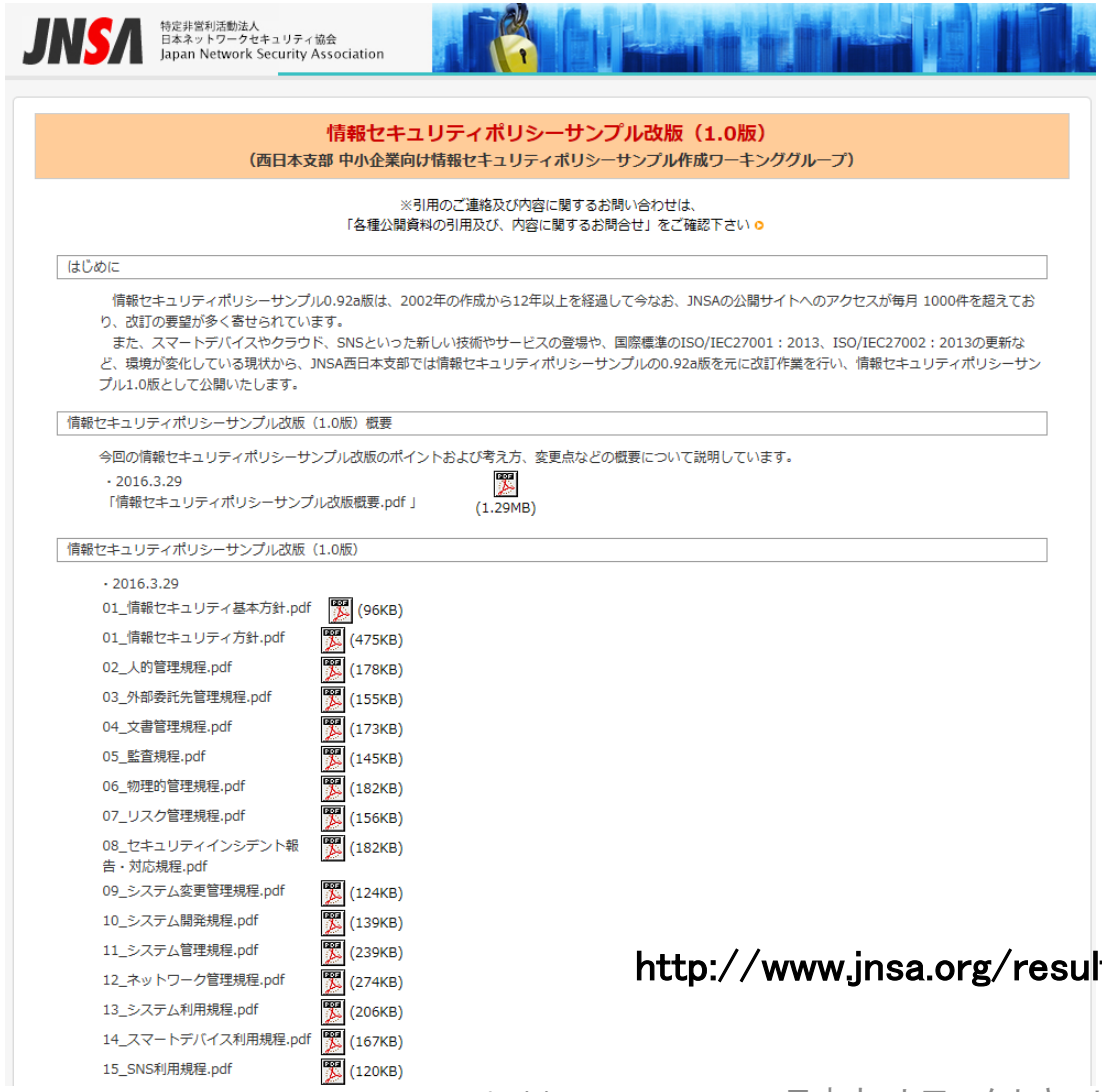
NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

情報セキュリティポリシーサンプルの改訂

JNSA西日本支部
中小企業向け
情報セキュリティポリシーサンプル作成WG
富士通関西中部ネットテック㈱
嶋倉　文裕

2002年以来　3/29に公開！



特定非営利活動法人
日本ネットワークセキュリティ協会
Japan Network Security Association

情報セキュリティポリシーサンプル改版（1.0版）
（西日本支部 中小企業向け情報セキュリティポリシーサンプル作成ワーキンググループ）

※引用のご連絡及び内容に関するお問い合わせは、
「各種公開資料の引用及び、内容に関するお問合せ」をご確認下さい

はじめに

情報セキュリティポリシーサンプル0.92a版は、2002年の作成から12年以上を経過して今なお、JNSAの公開サイトへのアクセスが毎月 1000件を超えており、改訂の要望が多く寄せられています。
また、スマートデバイスやクラウド、SNSといった新しい技術やサービスの登場や、国際標準のISO/IEC27001：2013、ISO/IEC27002：2013の更新など、環境が変化している現状から、JNSA西日本支部では情報セキュリティポリシーサンプルの0.92a版を元に改訂作業を行い、情報セキュリティポリシーサンプル1.0版として公開いたします。

情報セキュリティポリシーサンプル改版（1.0版）概要

今回の情報セキュリティポリシーサンプル改版のポイントおよび考え方、変更点などの概要について説明しています。
・2016.3.29
「情報セキュリティポリシーサンプル改版概要.pdf」 (1.29MB)

情報セキュリティポリシーサンプル改版（1.0版）

・2016.3.29
01_情報セキュリティ基本方針.pdf (96KB)
01_情報セキュリティ方針.pdf (475KB)
02_人的管理規程.pdf (178KB)
03_外部委託先管理規程.pdf (155KB)
04_文書管理規程.pdf (173KB)
05_監査規程.pdf (145KB)
06_物理的管理規程.pdf (182KB)
07_リスク管理規程.pdf (156KB)
08_セキュリティインシデント報告・対応規程.pdf (182KB)
09_システム変更管理規程.pdf (124KB)
10_システム開発規程.pdf (139KB)
11_システム管理規程.pdf (239KB)
12_ネットワーク管理規程.pdf (274KB)
13_システム利用規程.pdf (206KB)
14_スマートデバイス利用規程.pdf (167KB)
15_SNS利用規程.pdf (120KB)

http://www.jnsa.org/result/2016/policy/index.html

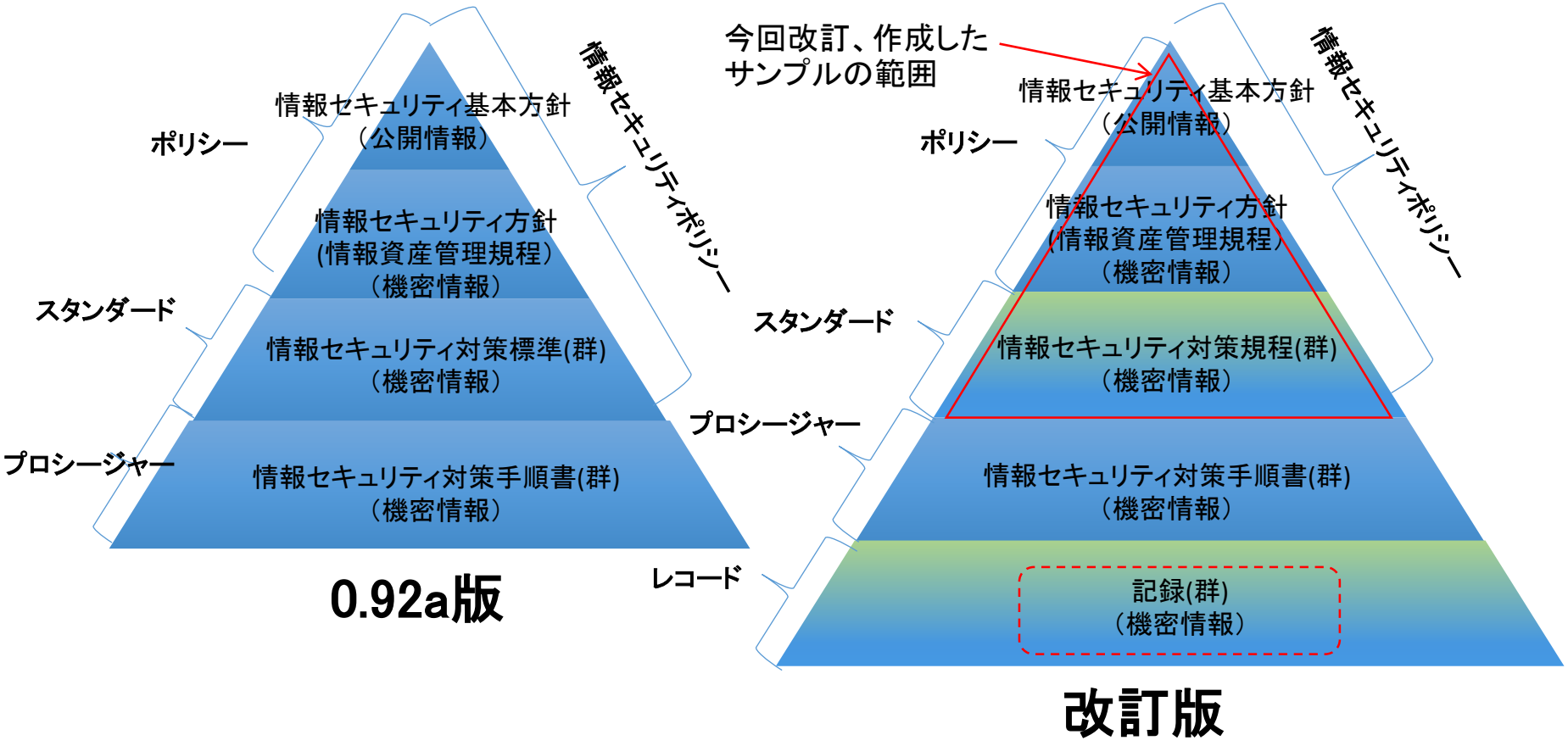
0.92a版と改訂版の違い

0.92a版と改訂版の相違点は以下のとおりです。

	0.92a版	改訂版
作成年	2000年～2001年	2014年～
作成目的	ポリシー作成の概念に留まらず、実際の文書を提示することで、ポリシーの考え方と作り方を提示する	・ISO/IEC27002:2013への対応 ・スマートデバイス、クラウド、SNSなど新技術への対応 ・西日本支部の成果物との連携
対象企業	小 ⇔ 中 ⇔ 大	小 ⇔ 中 ⇔ 大
関連規格	ISO/IEC17799	ISO/IEC27001:2013 ISO/IEC27002:2013 ISO/IEC27005:2008 ISO 31000:2009
サンプル文書数	31	15予定
PDCA	PDCAのうちDが中心	PDCA全て

サンプルの文書階層

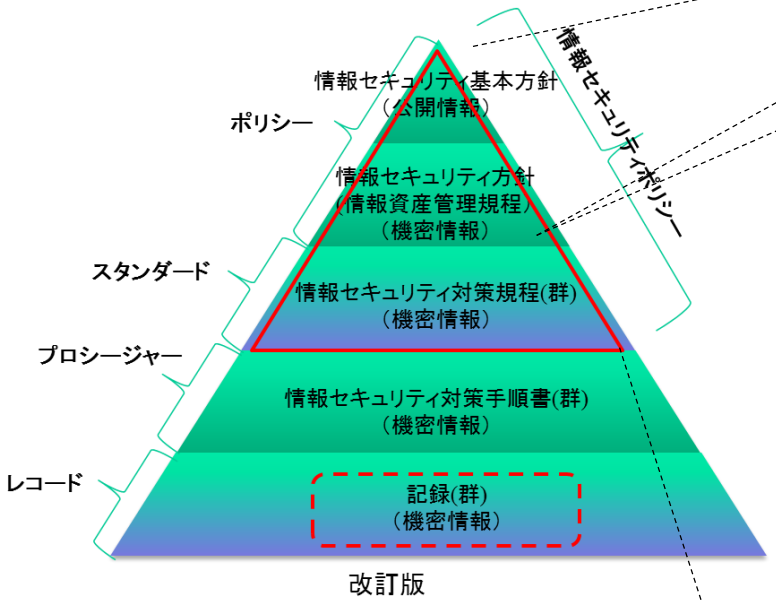
・改訂版では情報セキュリティの運用における記録（群）を定義



改訂版情報セキュリティ文書の定義

文書	内容
情報セキュリティ基本方針	情報セキュリティに取り組む姿勢を広く、世の中に宣言する文書。
情報セキュリティ方針	情報セキュリティマネジメントにおける方針を記載する文書。情報セキュリティに取り組む体制、役割、責任を明確にする。
情報セキュリティ対策規程	導入、遵守すべき情報セキュリティ対策を日常の運用を含め明確にする。 例）ウィルス対策ソフトの導入、パターンファイルの自動更新
情報セキュリティ対策手順書	導入、遵守すべき情報セキュリティ対策を実現する製品やその製品で日々、実施すべき具体的な行動を明確にする。 例)JNSA社のウィルス対策ソフトの管理システムからパターンファイルを自動的にPCに配布
記録	情報セキュリティ対策の遵守、運用プロセス確認に伴い作成する記録。 例）JNSA社のウィルス対策ソフトの管理システムでパターンファイル更新が全PCに行われたことを確認する記録

改訂版　ポリシーサンプル構成



- 情報セキュリティ基本方針
- 情報セキュリティ方針

ポリシー層

- 人的管理規程
- 文書管理規程
- 監査規程
- リスク管理規程

規程
共通層

規程
各個別層

管理者向け

- 物理的管理規程
- システム変更管理規程
- システム開発規程
- システム管理規程
- ネットワーク管理規程

利用者向け

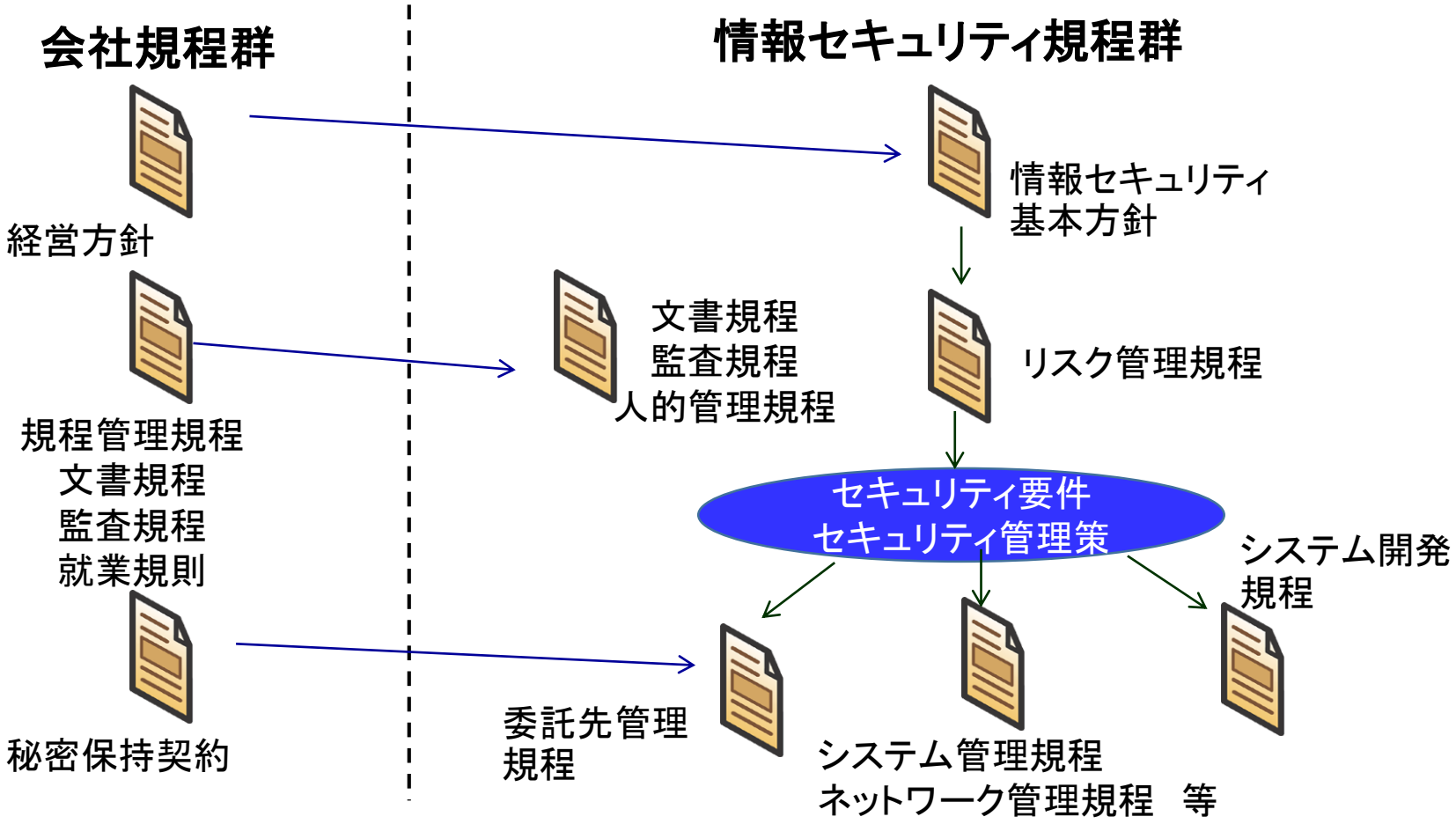
- システム利用規程
- スマートデバイス利用規程
- SNS利用規程

管理者・利用者共通

- 外部委託先管理規程
- セキュリティインシデント報告・対応規程

文書間の関係

・情報セキュリティ規程の各文書間で関係と会社規程との関係



改訂の概要 ①

① 0.92a版を踏襲しつつ、以下を考慮

- ISO27001付属書Aの各管理策と対応付
- ISO27002実施の手引きのレベル感での記載
- システム管理者、システム利用者の分離

２．対象者

ネットワークの構築、運用、管理する全ての従業員。*← 管理者と利用者を分離*

・

・

４．２．２　インターネット接続環境における導入時遵守事項

（A.9.1.2、A.12.6.1、A.13.2.1、A.13.2.3）　*← 対応する 27001 付属書 A の管理策を記載*

（１）ネットワーク接続構成

インターネット接続環境に設置するネットワーク機器は、以下のセキュリティ対策を考慮した構成を行わなければならない。

・　*← 27002 実施の手引きレベルでの記載*

・

改訂の概要 ②

② 情報セキュリティ対策の日々の運用を意識

- 日々の運用が実施されていることを確認するプロセスの確立

５．１　共通の運用確認事項

（１）構成管理

ネットワーク機器の追加、撤去や設定の変更に伴う構成管理が、変更履歴やコンフィグファイルの日時から適切に行われていることを確認すること。

←確認目的と確認する記録を記載

（２）変更管理

パッチ適用、ソフトウェアの版数アップは、実施しなかった時の影響や変更による影響の確認、または検証したうえで実施していることを、確認/検証日時、パッチ適用日時、実施者、承認者などの記録により確認すること。

改訂の概要 ③

② 情報セキュリティ対策の日々の運用を意識

	情報システム部門（管理部門）	業務部門（利用部門）
確認したいこと（目的）	(1)対策の定着 ・対策の全社展開 (2)対策の効果 ・脅威の検知、抑止、防御 (3)対策の維持 ・対策の回避、無効化の有無	(1)対策に伴う手続きの定着 ・部門での申請、確認 (2)対策による業務への効果 ・安全な業務遂行 (3)対策に伴う手続きの維持 ・申請/確認行為の有無
確認の対象（記録）	(1)システムログ ・サーバログ、PCログ、ネットワークログ （アクセスログ、イベントログetc） (2)管理画面 ・統計、適用、検知/防御状況 (3)人（対象：部門管理者） ・定着、課題などのヒアリング	(1)人（対象：部門） ・手順書&チェックシート ・ワークフロー ・申請書 (2)管理画面 ・適用状況
確認契機	(1)定期的 ・毎週、毎月etc. (2)不定期 ・イベント（キャンペーン） ・インシデント	(1)日常業務 ・情報持出し時 (2)定期的 ・毎週、毎月 (3)不定期 ・イベント

改訂の概要 ④

② 情報セキュリティ対策の日々の運用を意識

- **対策の定着**
  - ー対策の実施、実行といった定着の確認
  - ー従業員への周知の確認
- **対策の効果**
  - ー脅威を検知し防御していることの確認
  - ー異常を検知していることの確認
  - ー対策の結果に基づく見直しを行っていることの確認
- **対策の維持**
  - ー対策の回避、無効化がないことの確認
  - ー定期、不定期での見直しを行っていることの確認

改訂の概要 ⑤

③ ホワイトリスト型の記述

- **運用のプロセス確立のための表現**

ー白と黒の世界（二者択一）での表現

ホワイトリスト型表現　　：白であること
ブラックリスト型表現　　：黒でないこと
　　->「白であること」

ー白と黒と灰色の世界（複数選択肢）での表現

ホワイトリスト型表現　　：白であること
ブラックリスト型表現　　：黒でないこと
　　-> 「白」か「灰色」かは不明

改訂の概要 ⑥

④ 主語、対象、役割（行為、記録、確認・承認）を明記

- 運用のプロセス確立のための表現
  - ー責任の明確化
  - ー後で検証可能な記録の明確化

４．３　運用時の遵守事項

インターネット接続環境、社内ＬＡＮ環境、社内ＷＡＮ環境、リモート接続環境にネットワーク機器の運用時におけるネットワーク管理者の遵守事項を以下に示す。

←ネットワーク管理者、と主語を明確化

４．３．１　共通の遵守事項

（A.6.2.2、A.9.1.2、A.9.2.2、A.9.2.3、A.9.2.5、A.9.2.6、A.12.6.1、A.13.1.1）

・

←何の目的に、何を行うのかを明確化

（２）構成管理

ネットワーク機器の以下の現状の構成管理の維持と最新情報の把握を行う。

①ネットワーク構成図（物理構成及び論理構成）

②ネットワーク機器のＩＰアドレスの管理

サンプル利用の注意事項 ①

（1） 組織に合わせた体制

「情報セキュリティ方針」の情報セキュリティを維持するための組織、役割の利用

- 自組織の部門、誰が記載例に相当するのか
- 組織内に設置が困難な役割はないか

サンプル利用の注意事項 ②

（2）組織で実施する対策の記載を確認

各サンプル文書の管理策の利用

- 自組織の実施済や導入する対策がサンプルに記載有無の確認
- 記載があるものはサンプルの記載内容、記載レベルを確認
- 実現方法や運用方法など詳細な部分の確認
- 組織で導入しない対策、過剰な対策の記載の削除
- 実施済や導入する対策でも詳細な部分、運用方法などで異なる部分の削除と修正

サンプル利用の注意事項 ③

（3）全体の整合を確認

文書間での矛盾の解消

- 全体の体制、役割と各規程の実施者間で矛盾
- 表現が異なる役割
- どこにも定義されていない役割、担当
- 対策間での矛盾
- 削除した対策を前提にした記載の有無

西日本支部成果物との関係

西日本支部のこれまでの成果物と今回のポリシーサンプルの関係

気付き	・出社してから退社するまで 中小企業の情報セキュリティ対策実践手引き ・略称：9to5	リスク認識
運用	• **情報セキュリティポリシー・サンプル**	リスク受容レベルの決定（対策の決定）
チェック	• 中小企業向け情報セキュリティチェックシート • 略称：チェックシート	対策状況の確認

http://www.jnsa.org/result/2013/chusho_sec/index.html

http://www.jnsa.org/seminar/nsf/2014kansai/data/3_shimakura_2.xlsx

2016年度　関連する活動

新WGでは経営者へのリスク見える化をテーマに活動

ISO31000　組織の状況の確定　具体的には？

外部状況例	国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制、金融、技術、経済、自然並びに競争の環境
	組織の目的に影響を与える主要な原動力及び傾向
	外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観
内部状況例	統治、組織体制、役割及びアカウンタビリティ
	方針、目的及びこれらを達成するために策定された戦略
	資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）
	内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
	組織の文化
	情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
	組織が採択した規格、指針及びモデル
	契約関係の形態及び範囲

最後に　WGメンバー

井上　陽一	JNSA顧問
大財　健治	株式会社ケーケーシー情報システム
河野　愛	株式会社インターネットイニシアティブ
久保　智夫	株式会社サーバーワークス
久保　寧	富士通関西中部ネットテック株式会社
嶋倉　文裕	富士通関西中部ネットテック株式会社
西川　和予	株式会社GENUSION
元持　哲郎	アイネット・システムズ株式会社
吉崎　大輔	日本電気株式会社　（現、NECソリューションイノベータ株式会社）

改訂にご協力を頂いた皆様

青木　茂

今村　武司

宇佐川　道信

塩田　廣美