情報セキュリティポリシーサンプル
改版（1.0版）　概要

2016年3月

NPO日本ネットワークセキュリティ協会（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

目　次

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ました。

0.92a 版の改版は、当初、1 年で行う予定でしたが、2 年を費やすこととなりました。

JNSA 西日本支部はこれまで、情報セキュリティ対策の必要性への気付きや、対策状況のチェックのためのツールの作成を行ってきましたが、その活動の中で、いかにリスクを認識するか、また対策の導入後のその効果や運用状況のチェックの重要性を痛感しておりました。

今回、このリスク認識と、対策の効果や運用状況のチェックを行うための体制やチェックポイントを、どう改版に盛り込むべきか、ということの悩みが、いつの間にか、2 年もの期間を費やした要因です。

情報セキュリティポリシーサンプルの改版を、1.0 版として公開いたします。

本書は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ます。

1　0.92a 版との違い

0.92a 版と 1.0 版の違いを表 1-1 に示します。

表 1-1　0.92a 版と 1.0 版の相違

	0.92a 版	1.0 版
作成年	2000 年～2001 年	2014 年～2015 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 ・JNSA 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[1]	ISO/IEC27001:2013[2] ISO/IEC27002:2013[3] ISO/IEC27005:2008[4] ISO 31000:2009[5]
サンプル文書数	31	15
PDCA	PDCA のうち D が中心	PDCA 全て

[1] ISO/IEC17799　情報セキュリティ対策管理策の国際標準、ISO/IEC27002 の元になったもの

[2] ISO/IEC27001:2013　情報セキュリティマネジメントの国際標準、管理策の運用が適切に行っていることを認証するための規格、2013 年に改訂

[3] ISO/IEC27002:2013　情報セキュリティ対策管理策の国際標準、2013 年に改訂

[4] ISO/IEC27005:2008　情報セキュリティ管理とリスク管理プロセスの国際標準

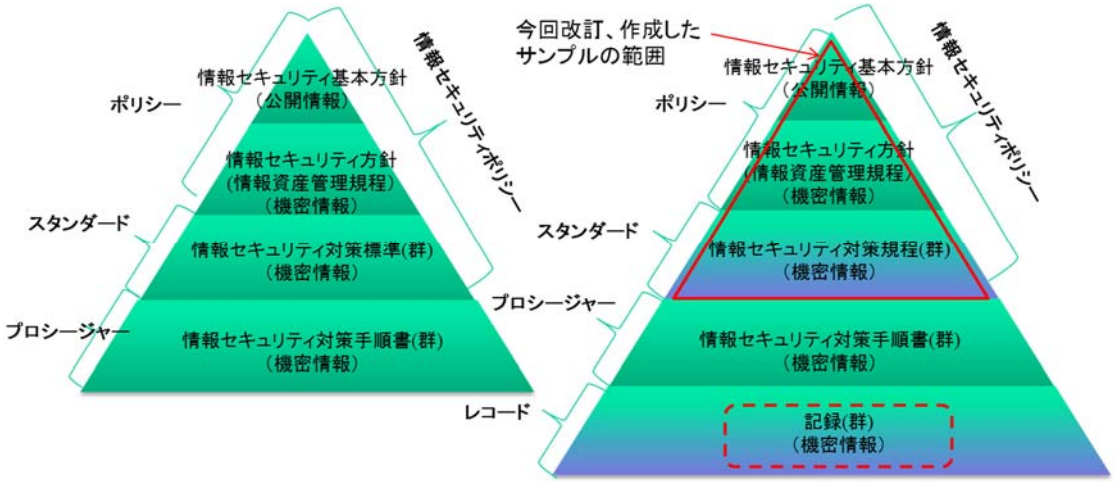
[5] ISO 31000:2009　組織経営のためのリスクマネジメントに関する国際標準

２　1.0 版の文書構成

1.0 版の情報セキュリティポリシーサンプルの文書構成を 0.92a 版と合わせて図 2-1 に示します。

0.92a 版との大きな違いは、記録（群）の追加です。

なお、1.0 版は 0.92a 版と同様、情報セキュリティ基本方針」、「情報セキュリティ方針」、「情報セキュリティ対策規程（群）」の３つからの構成です。



0.92a 版　　1.0 版

図 2-1 情報セキュリティポリシーサンプルの文書構成

1.0 版の文書の内容を表 2-1 に示します。

表 2-1 情報セキュリティ文書の内容(1/2)

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

表 2-1 情報セキュリティ文書の内容(2/2)

文書	内容
情報セキュリティ対策手順書	情報セキュリティ対策を実現する製品などを利用し日々、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、運用プロセスに伴い作成する記録。 例) JNSA 社のｳ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

２．１　1.0 版の情報セキュリティポリシーの構成

0.92a 版では、図 2-2 のどのパターンも作成可能なようにポリシーサンプルを用意しています。

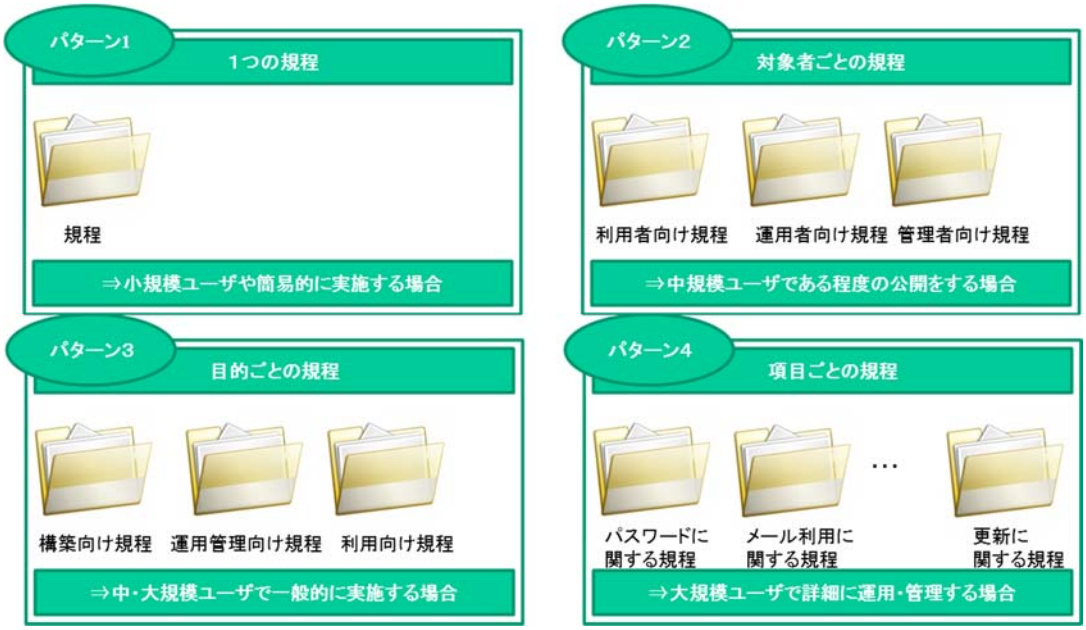


図 2-2 情報セキュリティポリシーの構成パターン

1.0 版の改版においては、規程の数が多いと、遵守事項の羅列と受け取られ、中小企業が自ら組み合わせを考えることが面倒であり、細かすぎると各規程の関連性の確保、矛盾なく運用することが困難と考え、以下の構成に改訂版では組み換えを行い１５項目に集約しました。

・読み手の対象者と対象システム単位に目的を集約し、パターン 2 と 3 をまとめまし

た。

・パターン 4 の項目毎に分かれている規程を、対象者、システム単位に対応する項目として配置しました。

・ 運用を確実とするため、各規程に運用確認事項を記載しています。

・ 西日本支部の成果物である「情報セキュリティチェックシート」、「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」と 0.92a 版の関連性についても考慮しました。（西日本支部の成果物との関係は、後述）

表 2-2 に 1.0 版の情報セキュリティポリシーサンプルの読み手の対象者と文書一覧を示します。

表 2-2　読み手と情報セキュリティポリシーサンプル一覧

対象者	情報セキュリティポリシーサンプル　1.0 版
全員	①情報セキュリティ基本方針 情報セキュリティ方針
	③外部委託先管理規程
	⑧セキュリティインシデント報告・対応規程
管理者	②人的管理規程
	④文書管理規程
	⑤監査規程
	⑥物理的管理規程
	⑦リスク管理規程
	⑨システム変更管理規程
	⑩システム開発規程
	⑪システム管理規程
	⑫ネットワーク管理規程
利用者	⑬システム利用規程
	⑭スマートデバイス利用規程
	⑮ＳＮＳ利用規程

利用者向けの「⑭スマートデバイス利用規程」、「⑮SNS 利用規程」は「⑬システム利用規程」にまとめることを、当初考えましたが、 スマートデバイス、SNS については改版作成に取り込む背景もあり、 あえて独立した項目としています。

なお、クラウドサービスについては、⑪システム管理規程に含めています。

クラウドサービスの利用は、システムの実現方法をオンプレミスではなくサービスの利用という差異はあるものの、 自組織のシステムに求める情報セキュリティ要件に違いはない、という考えに基づき、 ⑪システム管理規程に含めました。

表 2-3 に 0.92a と改版文書との関係を示します。なお、0.92a 版の各文書の通番（Cx）は、今回の改版にあたり付与したものです。

表 2-3　1.0 版と 0.92a 版の情報セキュリティポリシーサンプルの対応(1/2)

1.0 版	0.92a 版
①情報セキュリティ基本方針 情報セキュリティ方針	C0. 情報セキュリティ基本方針 C0. 情報セキュリティ方針
②人的管理規程	C20. プライバシーに関する標準 C24. セキュリティ教育に関する標準 C25. 罰則に関する標準
③外部委託先管理規程	C2. 委託時の契約に関する標準
④文書管理規程	C26. スタンダード更新手順に関する標準 C29. プロシージャ配布の標準
⑤監査規程	C23. 監査標準
⑥物理的管理規程	C3. サーバルームに関する標準 C4. 物理的対策標準 C5. 職場環境におけるセキュリティ標準
⑦リスク管理規程	―
⑧セキュリティインシデント報告・対応規程	C22. セキュリティインシデント報告・対応標準
⑨システム変更管理規程	―
⑩システム開発規程	―
⑪システム管理規程	C3. サーバルームに関する標準 C8. サーバなどに関する標準 C11. ユーザー認証標準 C12. ウィルス対策標準 C16. 媒体の取扱に関する標準 C17. アカウント管理標準 C18. システム維持に関する標準 C19. システム監視に関する標準 C21. セキュリティ情報収集及び配信標準
⑫ネットワーク管理規程	C6. ネットワーク構築標準 C7. 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 C27. 専用線及び VPN に関する標準 C28. 外部公開サーバに関する標準

表 2-3　1.0 版と 0.92a 版の情報セキュリティポリシーサンプルの対応(2/2)

1.0 版	0.92a 版
⑬システム利規程	C1. ソフトウェア／ハードウェアの購入及び導入標準 C9. クライアントなどにおけるセキュリティ対策標準 C10. 社内ネットワーク利用標準 C12. ウィルス対策標準 C13. 電子メールサービス利用標準 C14. Web サービス利用標準 C15. リモートアクセスサービス利用標準
⑭スマートデバイス利用規程	―
⑮SNS 利用規程	―

２．２　1.0 版の情報セキュリティポリシー構成とサンプル文書

表 2-2 に示す各文書と図 2-1 に示す情報セキュリティポリシーの文書構成との対応は図 2-3 となります。

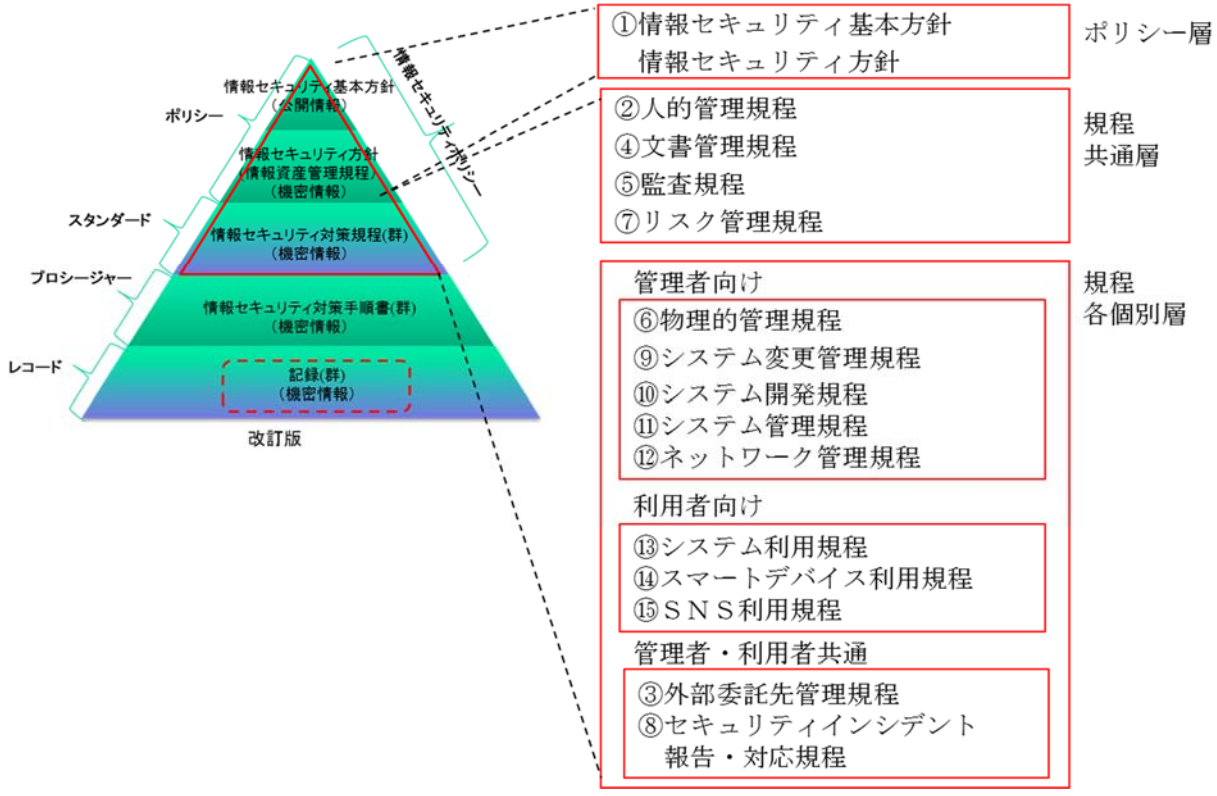


図 2-3 各文書と情報セキュリティポリシーサンプルの文書構成との対応

２．３　情報セキュリティポリシー文書間、他文書との関連性

図 2-3 に示すポリシー文書、スタンダード文書には経営方針、就業規則などの既存の企業文書と関連性があります。また、スタンダード文書は、その文書の目的、対象によりスタンダード文書間においても関連性を持っています。それらの関連性を図 2-4 に示します。

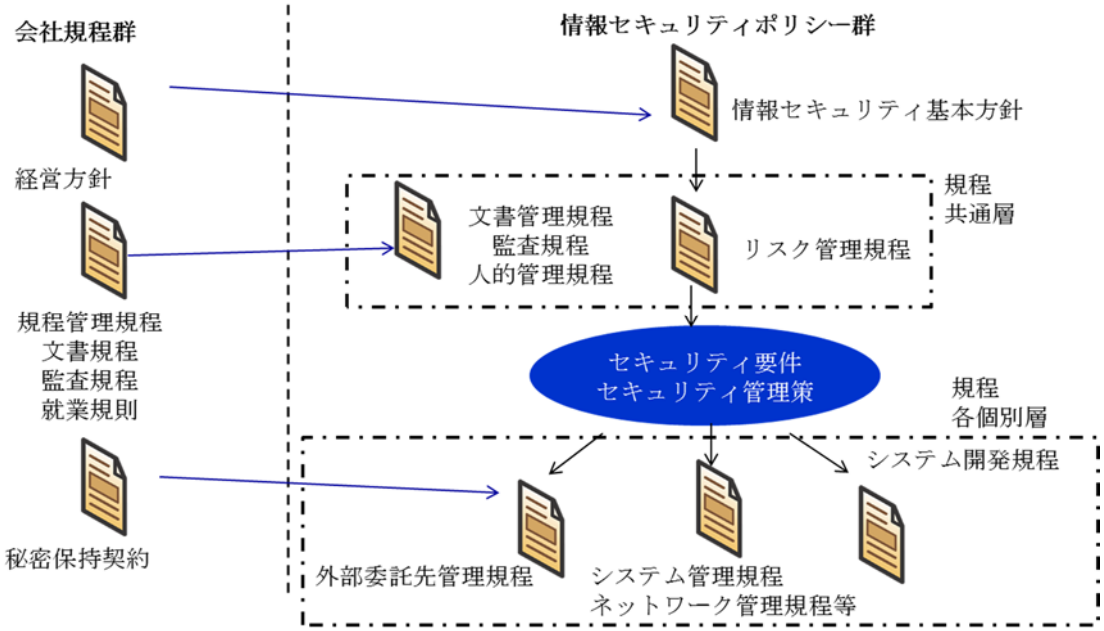


図 2-4 企業の既存文書とポリシー文書、スタンダード文書の関連性

企業文書と情報セキュリティポリシー群の関連性を表 2-4 に、情報セキュリティポリシー群の中の関連性を表 2-5 に示します。

表 2-4 企業文書と情報セキュリティポリシー群の関連性

企業文書	情報セキュリティポリシー群	関連性
経営方針	情報セキュリティ基本方針	情報セキュリティは、企業活動を支えるものであり、そのため情報セキュリティ基本方針は経営方針を反映させたものとなります。
規程管理規程 文書規程 監査規程 就業規則	文書管理規程 監査規程 人的管理規程	情報セキュリティ文書の発行、承認など、情報セキュリティ監査の実施者などは、企業の文書管理、監査活動の一環として行うべきで、また情報セキュリティポリシー違反時の処分も、就業規程を超えるものであってはなりません。
秘密保持契約	外部委託先管理規程	委託先に情報の秘密保持を求めるために、本契約を締結します。

表 2-5 情報セキュリティポリシー群の中での関連性

情報セキュリティポリシー群		関連性
関連元	関連先	
情報セキュリティ基本方針	リスク管理規程	リスクを洗い出し、分析、特定を行い、対策の決定は、闇雲に行うのではなく、自組織の経営方針､経営環境を反映したものであるべきです。そのため、自組織の経営方針、経営環境を反映した情報セキュリティ基本方針に示す情報セキュリティの範囲、目的に沿ったリスク管理を行います。
リスク管理規程	規程 各個別層	各個別層の規程は、リスクの対応の結果に基づく対策について、記載、整備します。そのため、リスク管理の結果に基づくもの、という位置づけとなります。

３　改版のポイント

1.0 版への改版で心がけたこと、改版の方針としたことを以下に示します。

３．１　改版のネットワーク構成

1.0 版の情報セキュリティポリシーサンプルは、図 3-1 のネットワーク、システム構成を想定したものです。

多くの方に参考にして頂く情報セキュリティポリシーサンプルとすることから、保有する情報、ビジネスモデルなどの固有なものを想定せず、昨今の外部、内部の脅威への対策を ISO/IEC27001：2013、ISO/IEC27002：2013 を参考に情報セキュリティポリシーサンプルを改版しています。

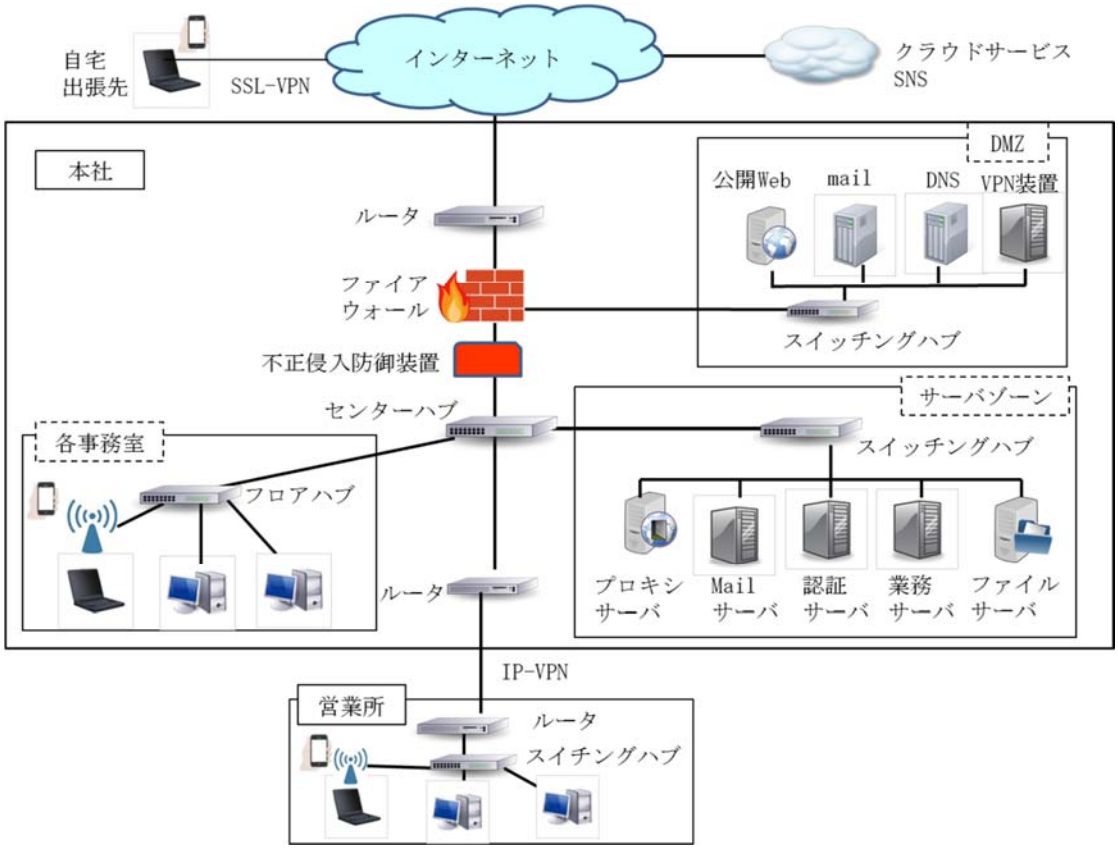


図 3-1　情報セキュリティポリシーサンプルのネットワーク、システム構成

３．２　情報セキュリティの推進体制

1.0 版の情報セキュリティポリシーサンプルは、図 3-2 に示す情報セキュリティを推進する体制が可能な組織を想定したものです。

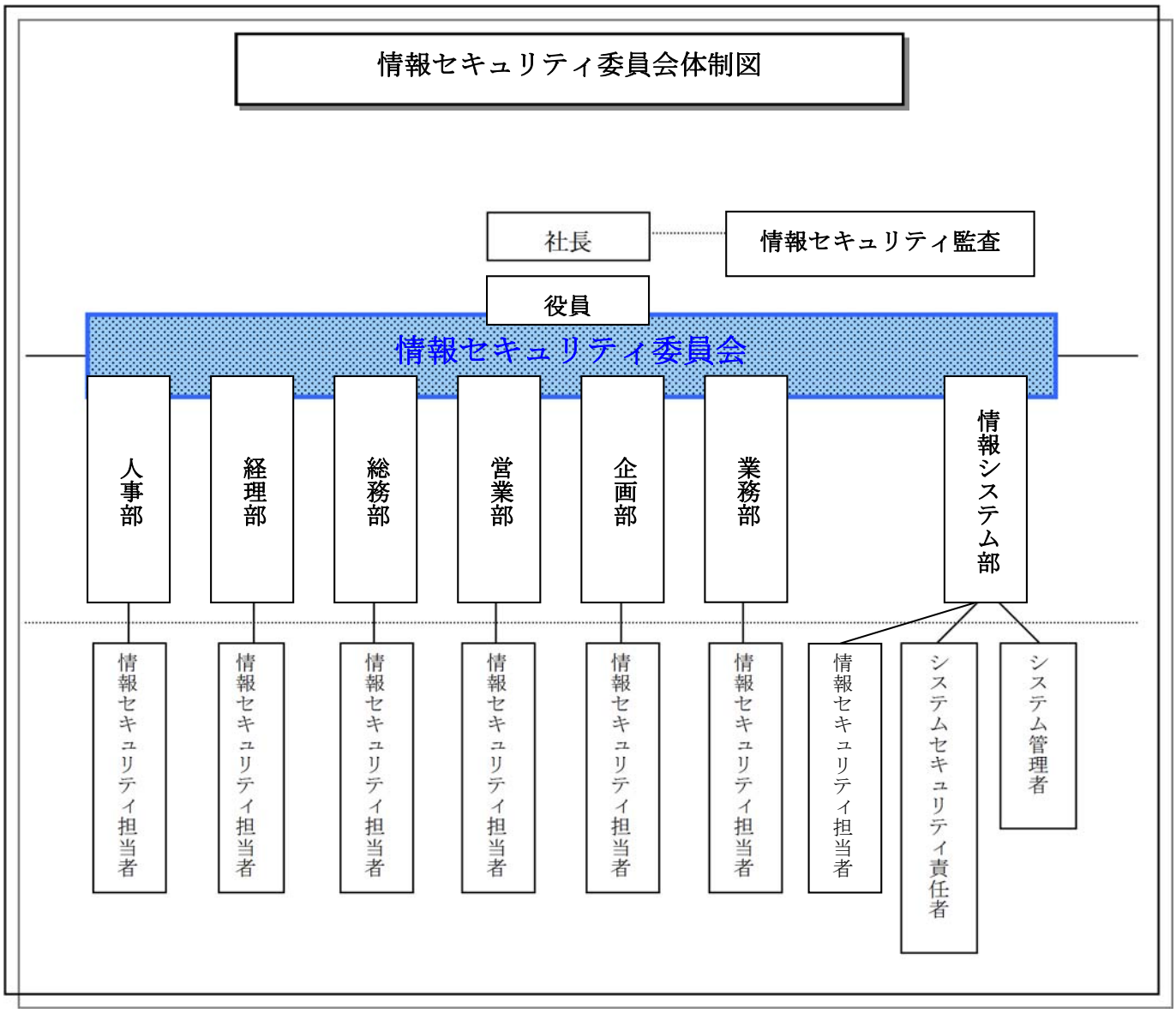


図 3-2 情報セキュリティ推進体制

３．３　0.92a 版の踏襲

1.0 版の作成にあたり、0.92a 版の文書を踏襲することを基本としています。ただし、以下の 3 点を考慮しています。

①ISO/IEC27001：2013 付属書 A の対応を考慮

改版では ISO/IEC27001：2013 の付属書 A との対応付けを行いました。

情報セキュリティポリシーサンプルの各文書の各項目のうち、付属書 A の各管理策に対応付けが可能なものについては、対応する管理策を記載しました。

なお、対応付けを強引に行っている箇所もあること、ご容赦ください。

②ISO/IEC27002：2013 の実施の手引きレベルを考慮

情報セキュリティポリシーサンプルに記載する対策は、ISO/IEC27002：2013 の実施の手引きの記載レベルで追加、 削除、修正を実施しています。

③管理者、利用者を分離

2.1 項に前述したとおり、対策項目別ではなく、対象のシステム毎に読み手を意識し、0.92a 版よりさらに管理者、利用者を分離した情報セキュリティポリシーサンプルの文書としています。

図 3-3 にネットワーク管理規程を記載例として示します。

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*

・

図 3-3　記載例

３．４　情報セキュリティ対策の日々の運用を重視

日々の情報セキュリティ対策の運用が適切に実施されていることを確認するプロセスを確立するための項目を規程に盛り込みました。

「図 2-1 情報セキュリティポリシーサンプルの文書構成」の 1.0 版には「記録（群）」を追加しています。

日々の情報セキュリティ対策の運用確認とは、この「記録（群）」を確認する項目です。

ここで言う「記録（群）」には、PC や情報の持ち出し申請書や、定期的な情報セキュリティ対策状況のチェックシート、報告書など以外に、システムで取得するログやコンフィグファイルの日時、システムの管理画面などの電子データも含みます。

0.92a 版と 1.0 版の文書の目次構成の違いを表 3-1 に示します。

表 3-1 0.92 a 版と 1.0 版の目次構成の相違

0.92a 版	1.0 版
趣旨	趣旨/目的
対象者	対象者
対象システム	対象システム/対象範囲
遵守事項	遵守事項
―	運用確認事項 -運用点検(第三者、自主点検として) -記録・エビデンスベースで確認できること
例外事項	例外事項
罰則事項	罰則事項
公開事項	公開事項
改訂	改訂

表 3-1 に示す運用確認事項は管理部門である情報システム部門以外に、利用部門でも行う必要があります。

情報システム部門での確認は、導入した情報セキュリティ対策の定着、維持、効果などの確認であり、利用部門である業務部門でしかできない情報の持ち出し手続きの実施などについては、利用部門の確認が必要です。

表 3-2 に情報システム部門、業務部門が確認すべき事項の例を示します。

表 3-2 情報システム部門、業務部門で確認すべき事項（例）

	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 （例：情報/PC 持出し申請） (2)対策による業務への効果 ・安全な業務遂行 （例:支給デバイスのみの利用） (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 ・PC、サーバ、ネットワーク （ｱｸｾｽﾛｸﾞ、ｲﾍﾞﾝﾄﾛｸﾞなど） (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（ｷｬﾝﾍﾟｰﾝ） ・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（ｷｬﾝﾍﾟｰﾝ） ・インシデント

図 3-4 にネットワーク管理規程を記載例として示します。

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。

図 3-4　記載例

３．５　情報セキュリティ対策の日々の運用確認プロセス確立のための記載

日々の情報セキュリティ対策の運用が適切に実施されていることを確認するプロセスを確立するために、規程の記載にはホワイトリスト型の記載とすることとしました。

ホワイトリスト型とブラックリスト型の表現の違いを表 3-3 に示します。

表 3-3 ホワイトリスト型とブラックリスト型の表現の違い

	二者択一時	複数選択時
ホワイトリスト型	白であること	白であること
ブラックリスト型	黒でないこと 二者択一なので「白であること」読みかえる必要あり	黒でないこと 「白」か「灰色」判らない

ホワイトリスト型とブラックリスト型の書き方による違いの具体的な事例を下記に示します。

ホワイトリスト型とブラックリスト型事例

セキュリティの規程には、“～の利用を禁止する”という書き方が多いですが、以下の記載の場合、どうすれば明確となるでしょうか？

例えば、“業務には私物携帯電話の利用を禁止する。”

携帯電話にスマートフォンは含まれるのか、データ通信に利用するのであれば私物のスマートフォンは良いのでしょうか？

そこで、この改版では極力、“業務には会社が貸与した携帯電話またはスマートフォンのみを利用すること。”というホワイトリスト型の記述を心がけるようにしました。

また、禁止事項はチェックすること（利用していないこと、禁止行為を行っていないことの証明）が難しいため、ホワイトリスト型の記述は監査や日常のチェックにも有効

です。

３．６　主語、対象、役割を明記

改版では、なるだけ主語、対象、役割を明記することとしました。

誰が（責任者、管理者、利用者）、何を行うのか、どういう責任（行為、記録、確認・承認）を果たすのか、を明確にすることとしました。

また、運用確認で検証可能な記録に何を残すのかを明確にすることとしました。

図 3-5 にネットワーク管理規程を記載例として示します。

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）

・

・

（２）構成管理　*←何の目的に、何を行うのかを明確化*

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

・

・

図 3-5　記載例

４　リスクの認識

リスクの認識は、経営方針、情報セキュリティ基本方針、企業を取り巻く内外の状況を把握し、自組織に適したセキュリティ要件・セキュリティ管理策を決定する上で重要です。

このため、リスク管理規程は、リスクを認識し自組織に適したセキュリティ要件・セキュリティ管理策を決定するためのプロセスを定めた情報セキュリティ規程群の中心となる規程となります。

リスクアセスメントの結果、決定したセキュリティ要件を基に図 2-4、表 2-5 に示す関係により、各規程個別層（外部委託管理規程、システム開発規程や、システム管理規程、ネットワーク管理規程など）を整備します。

４．１　リスクアセスメントの概要

リスク管理規程のプロセスは各規程を整備するために行う重要なものですが、各プロセスが分かりにくいため、リスク管理プロセスのポイントについてまとめました。

リスク管理は、図 4-1 に示すプロセスにより行います。

自組織内、または組織外の利害関係者との意思疎通によりリスクについて認識合せを行いながら、リスクアセスメント、リスクへの対応を経て管理策を決定するプロセスです。

情報セキュリティ対策を行う目的、範囲、強度などを決定するため、組織を取り巻く環境や経営課題並びに顧客など利害関係者からの要求事項などから、組織の状況を確定します。

次に、組織が保有する情報資産の重要度とその管理状況、脅威、脆弱性を洗い出し、洗い出した結果からリスクの大きさを算定します。

リスクの大きさの算定までが、リスクアセスメントであり、算定したリスクの大きさに応じた対策が、情報セキュリティ対策となります。

これらのプロセスを経ることにより、小さなリスクに多額の対策費用を投資する、または逆に、大きなリスクを見逃し対策費用を投資しない、という矛盾を防ぐことが可能となります。

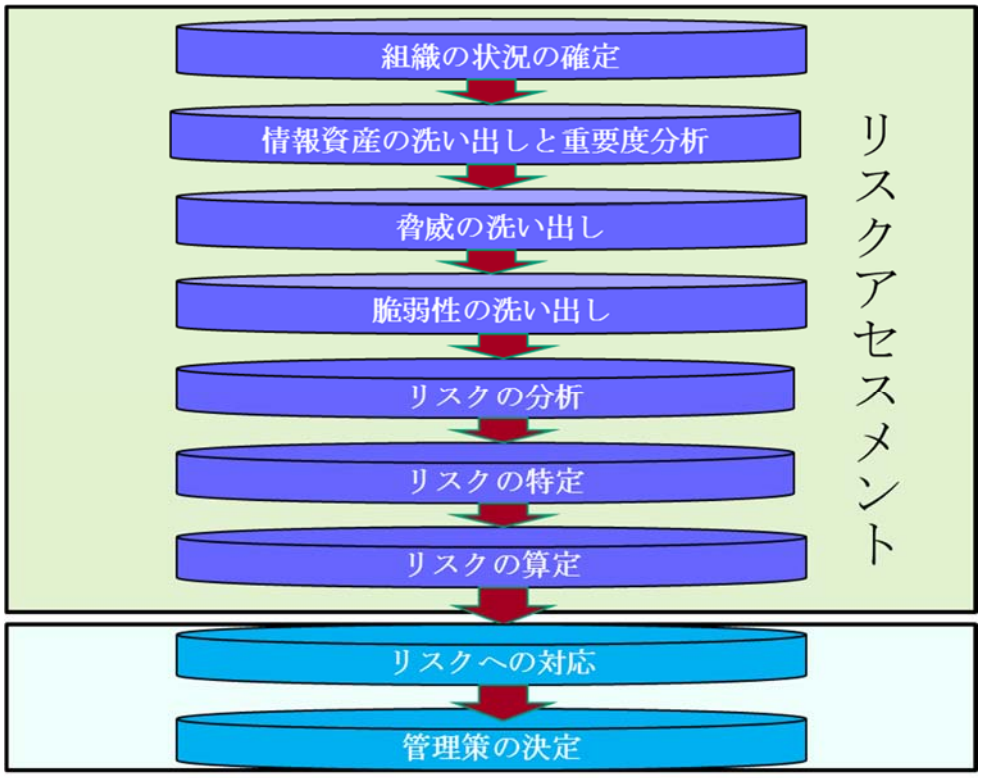


図 4-1 リスク管理の流れ

４．２　組織の状況の確定

「組織の状況の確定」とは、自組織を取り巻く外部、内部の状況を洗い出し、リスク管理をする目的は何か、範囲は何処までか、どの程度のリスクであればリスク対策を行うのか、どの程度リスクを低減するのかなど組織を取り巻く諸条件を確認し、組織が進む方向を確定することです。

表 4-1 に、ISO 31000:2009 に記載される「組織の状況の確定」で考慮すべき、自組織を取り巻く外部、内部の状況の例を示します。

表 4-1　「組織の状況の確定」で考慮すべき自組織を取り巻く外部/内部の状況(例)

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、内容及び範囲

４．３　情報資産の洗い出し

自組織の保有する情報資産を洗い出し、情報資産台帳[6]として整理します。

以下に情報資産の洗い出しのポイントを示します。

４．３．１　情報資産の洗い出し

表 4-2 に情報資産の分類例を示します。

情報資産には、「情報」そのもの以外にＩＴ基盤を支えるサーバ、ネットワーク機器や利用するサービスも含みます。

[6]情報資産台帳の例　JNSA 西日本支部「中小企業の情報セキュリティ対策支援 WG 活動報告書」にフォーマット例と金型製造業、鞄製造業における事例を掲載
http://www.jnsa.org/result/2008/west/0812report.pdf

表 4-2 情報資産の分類（例）

情報資産分類	対象の情報資産（例）
情報	電子ファイル、紙他
ソフトウェア	業務用ソフトウェア、事務用ソフトウェア、開発ソフトウェア、システムツール他
物理的資産	サーバ、ネットワーク機器、媒体、収容設備他
サービス	クラウドサービス、通信サービス、電気・空調サービス他

４．３．２　情報資産の洗い出し粒度

最終的に洗い出した情報資産に対し、情報セキュリティ対策を行います。

一つ一つの情報資産(例えば、各ファイル単位)を洗い出してもかまいませんが、表 4-3 に示すグループ(例えば、顧客情報など)ごとに洗い出し、グループごとにセキュリティ対策を検討することで、作業の効率化、効果的な情報セキュリティ対策が可能となります。

表 4-3 情報資産グループ化（例）

グループ単位	対象の情報資産（例）
利用場所	社内、社外、DMZ など
保管形態	サーバ、PC、クラウド、USB など
保管場所	サーバルーム、キャビネット、事務机上など
重要度	秘密、社外秘など

４．３．３　情報資産の重要度

リスクアセスメントにおいて、対象となる情報資産の価値を把握することは重要です。使えることを求めるサーバやネットワーク機器、自組織外や、関係者外には秘密であることを求める営業秘密、改ざんされないことを求める公開情報など、情報資産の価値により必要な情報セキュリティ対策が異なります。

情報資産の重要度は、表 4-4 に示す情報セキュリティの特性を考慮して決定します。表 4-5 に機密性による情報資産の分類例を示します。

表 4-4 情報セキュリティの特性

特性	説明
機密性	情報が漏えいした場合の影響度
完全性	情報が改ざんされた場合、または装置が正確に動作しなかった場合の影響度
可用性	情報、装置が利用できない場合の影響度

表 4-5 機密性による情報資産の分類（例）

重要度	分類	説明
1	公開	第三者に開示・提供可能 情報漏えいした場合、損失は無い
2	社外秘	社内のみ開示・提供可能 情報漏えいした場合、損失または売り上げ減
3	秘密	特定の関係者または部署のみに開示・提供可能 情報漏えいした場合、大きな損失または大幅な売り上げ減

４．４　脅威と脆弱性の洗い出し

洗い出した情報資産への脅威と情報資産の脆弱性を洗い出します。

脅威とは、自然災害や外部からの攻撃と同様に、コントロールできないものです。

脆弱性とは、その資産が持っている弱点のことです。

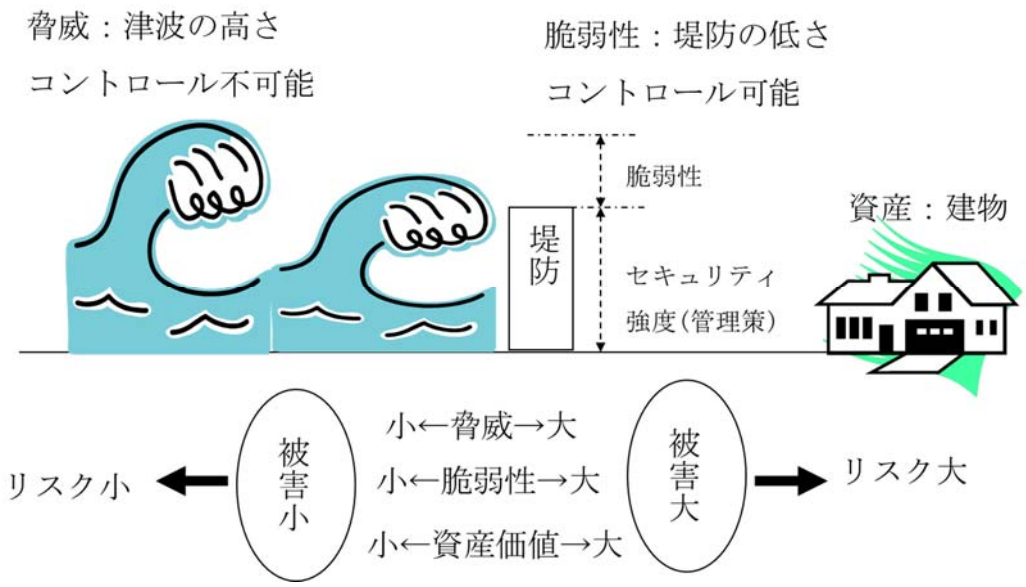
脅威と脆弱性と資産価値が大きくなるとリスクは増加し、脅威と脆弱性と資産価値が減るとリスクは減少します。

リスクコントロールでは、脅威はコントロールできませんので、コントロール可能な脆弱性と資産価値の大きさを変化させます。

一般的には、資産価値を小さくする(不要な資産は持たないなど)か、脆弱性を小さくするかで検討します。

脅威に対する脆弱性のコントロールと、それに伴うリスクの変化についてのイメージを図 4-2 に示します。

津波という大きな脅威に対し、守るべき建物という資産があるにも係らず堤防が低いという脆弱性がある場合は、リスクは大きなものとなります。その一方、堤防で守るべき価値のある資産がない場合、堤防が低くてもリスクは小さいとなります。また、堤防で守る必要性もないため、堤防を作ることが過剰な投資と判断できます。



JNSA「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」より

図 4-2 脅威に対する脆弱性のコントロールとリスクの変化

脅威の洗い出しには、ISO/IEC27005:2008 Annex.C(付属書 C)が参考になりますので、脅威を洗い出すさいの参考となる脅威の分類とその例を表 4-6 に示します。

表 4-6 脅威の分類とその例

分類		脅威の例
人為的	意図的	不正アクセス、マルウェア、改ざん、盗聴、なりすまし攻撃
	偶発的	人為的ミスを誘因するもの、障害を誘因するもの
環境的		災害

４．５　リスクの分析と特定

洗い出した脅威と脆弱性から、実際にどのようなリスクが発生するのかを考えます。

リスクが発生した場合に、機密性、完全性、可用性の観点からどのような影響があるのかを分析します。

また、リスクが発生する場合の発生源、頻度、状況についても分析します。

頻度は外部公開、組織内部の情報資産で、脅威の発生源（例えば、悪意のある組織外の第 3 者）からの直接的な不正行為が容易か否という環境の差異により、頻度に差をつけてリスク分析する方法があります。

表 4-7 にリスク分析の例を示します。

インターネット上の情報公開用 Web サーバは、誰でもアクセス可能な環境にあることか

ら､｢外部の悪意のある人｣はなんら制約もなく不正アクセスを試みることが可能なため、発生頻度は“高“と判断します。

そこに脆弱性が存在すると、表 4-7 に示す「攻撃が成立したときの影響」のような被害が生じます。

表 4-7 リスク分析の例

対象の情報資産	発生源	発生頻度	脆弱性	攻撃が成立したときの影響
情報公開用 Web サーバ	外部の悪意のある人からの不正アクセス	公開サーバのため、不正アクセスの頻度は高	CMS[7]パッチ未適用	･改ざんにより完全性の毀損 ･サービス継続が不可能となり可用性の毀損

４．６　リスクの算定

特定されたリスクに対し、定量的にリスクを算定します。 算定例を以下に示します。

〈算定例 1〉

リスクの大きさ=リスクの発生頻度×リスク発生時の損害額

〈算定例 2〉

リスクの大きさ=脅威の大きさ×脆弱性の大きさ×資産価値の大きさ

上記算定例を元に 算定例毎の算出例を表 4-8 に示します。また、リスクの発生頻度の数値化を表 4-9 に、機密性、完全性、可用性の影響度（クラス）による資産価値評価基準例を表 4-10 に示します。

[7] CMS　コンテンツ管理システム　Web サイトに掲載する文章や画像などのデジタルコンテンツを管理、処理を行うシステム

表 4-8 リスク算定の例

	対象の情報資産	発生源	発生頻度	脆弱性	攻撃が成立したときの影響
分析結果	情報公開用 Web サーバ	外部の悪意のある人からの不正アクセス	公開サーバのため、不正アクセスの確率は高	CMS パッチ未適用	・改ざんにより完全性の毀損 ・サービス継続が不可能となり可用性の毀損
数値化（例）	資産価値 CIA で評価（表 4-10 参照） C:1 I:2 A:1 評価 2	-	発生頻度は発生確率と対策状況の組合せ（表 4-9 参照） 発生確率：3	対策状況で評価(表 4-9 参照) 脆弱性：3	・損害額 公開情報だが改ざんに気が付かないと売り上げに影響がでる 500 万/日の損害見込み
算定	算定例 1	リスクの発生頻度×リスク発生時の損害額=1×500=500 発生確率、損害額は変化しないが、対策することで脆弱性は 3->1 に小さくなり、発生頻度が小さくなる。その結果リスクの大きさは 0.2×500=100 に減少。			
	算定例 2	脅威の大きさ×脆弱性の大きさ×資産価値=3×3×2=18 （脅威の大きさは発生確率で評価） 脅威の大きさ、資産価値は変化しないが、対策することで脆弱性評価は 3->1 に小さくなる。その結果リスクの大きさは 3×1×2=6 に減少。			

表 4-9 発生頻度の数値化（例）

()内は各状況を数値化したもの		発生確率（注）		
		大(3)	中(2)	小(1)
対策状況	充分できている(1)	低 (0.2)	低 (0.2)	低 (0.2)
	代替策のみ(2)	中 (0.5)	中 (0.5)	低 (0.2)
	対策していない(3)	確実 (1.0)	確実 (1.0)	中 (0.5)

赤枠内が発生頻度を数値化した例、数値化は比較しやすいように設定

（注）発生確率は情報資産の環境で判断

例えば、公開サーバへの不正アクセスは、不特定多数の者がなんら制限もなく試みることが可能なため、確率を“高“とする

表 4-10　資産価値評価基準（例）

	影響度	クラス	説明
機密性（C）	1	公開	第三者に開示・提供可能
	2	社外秘	特定の関係者または部署のみ利用可能
	3	関係者外秘	特定の関係者または部署のみに開示・提供可能
完全性（I）	1	低	情報の内容を変更された場合、ビジネスへの影響は少ない
	2	中	情報の内容を変更された場合、ビジネスへの影響は大きい
	3	高	情報の内容を変更された場合、ビジネスへの影響は深刻かつ重大
可用性（A）	1	低	利用不可能な場合、ビジネスへの影響は少ない
	2	中	利用不可能の場合、ビジネスへの影響は大きい
	3	高	利用不可能の場合、ビジネスへの影響は深刻かつ重大

（注）情報資産を CIA それぞれの特性、影響度で数値化。数値が大きいほどその情報資産が毀損されたときの影響が大きい。CIA の中で最も大きな数値をその情報資産の価値とする。

４．７　リスクへの対応

リスクアセスメントの結果をもとに、それぞれのリスクのうち、受容レベルを超えるリスクに対し、どのように対応するかを決定します。

決定したリスク対応から、具体的なセキュリティ管理策を決定します。

リスクへの対応例を図 4-2 の場合を例に表 4-11 に示します。

リスクへの対応方法には、現実には実行不可能なもの、実行は可能だが費用のかかるものがあります。

表 4-11 に示す「リスク源の除去」、「起こりやすさの変更」は実行不可能であり、「結果の変更」には費用がかかります。

そのためリスクの対応は、自組織が目指す経営方針、ビジネスの重要度とリスクの大きさを元に決定し、場合によってはリスク回避のため、ビジネスを止めるという対応も選択肢として考えます。

なお、情報セキュリティではなじみのない「リスクテイク」を表 4-11 には含めています。ビジネスには、なんらかのリスクはつきものであり、そのビジネスへのチャンレジのために、あえてリスクを取るという考え方です。

表 4-11 リスク対応例

対応事項	内容
リスクの回避	津波の発生する可能性のある場所の建物を所有しない。
リスクテイク	津波の発生する可能性は有るが、景観などを目的に、海辺の建物を所有する。
リスク源の除去	津波の原因である地震が発生する原因を取り除く。
起りやすさの変更	津波の原因である地震の発生頻度を変更させる。
結果の変更	堤防を高くする。
リスクの共有	災害保険に加入する。
リスクの保有	リスクがあることを認識し、状況を受け入れる。

次に持ち出し PC の紛失盗難による情報漏えいリスク対応例を表 4-12 に示します。

表 4-12 持ち出し PC の紛失盗難による情報漏えいリスク対応例と管理策例

対応事項	内容	具体的な管理策
リスクの回避	PC の持ち出しを禁止する。	PC は机に固定する。
リスクテイク	業務効率を追求し積極的に PC の持ち出しを行う。	通信機能を有するノート PC を利用する。
リスク源の除去	仮想化技術により PC に情報を保存できなくする。	シンクライアント PC を利用する。
起りやすさの変更	PC の持ち出しを必要最低限に制限する。	持ち出し専用 PC を利用する。
結果の変更	保存データの暗号化及び認証強度を向上する。	PC のハードディスクを暗号化する。
リスクの共有	情報漏えい保険に加入する。	同左。
リスクの保有	PC の持ち出しにリスクが有ることを認識し、その状況を受け入れる。	PC の持ち出し記録を作成する。

４．８　リスクの見直し

リスクは定期的に見直し、リスクアセスメントを行う必要があります。

現在のリスクアセスメントやリスク対応はあくまでも想定できた範囲であり、想定外のリスクが存在する可能性があります。

そのため、想定外を減らし想定内を増やすためには、見直しが必要です。

リスクの見直しは、リスク管理の「各プロセスから出た結果」と「決定した管理策の運用結果」をモニタリングし、評価し、改善して行くプロセスです。

想定外のリスクの例を以下に示します。

想定外のリスク

(1)リスクは把握していたが、リスクを引き起こすことが想定されなかった事象の存在

(2)議題にならなかった未知領域のリスクの存在

(3)人に起因するリスク

①行動や判断の誤差やばらつき

②私生活や経済的な背景に起因する予測不能な行動

③不測の故意や過失

(4)環境の変化や技術の進歩による新たな脅威の発生

(5)対応、対策に漏れや不備（事象が発生しないとわからないもの）

４．９　リスク管理プロセスのまとめ

4.2 項から 4.8 項に記載したリスクを認識する一連のプロセスは、自組織の内外の利害関係者とコミュニケーションと協議を通じ、図 4-3 に示す PDCA サイクルのリスク管理プロセスの確立が必要です。

図 4-3 に示す「D:リスク管理の実践」は 4.2 項から 4.7 項であり、「C:モニタリングと評価」は 4.8 項が対応します。

「P:リスク管理の仕組みの設計」、「A:リスク管理の仕組みの改善」は、リスク管理そのものを自組織で推進するための体系、プロセスを明確化し、リスク管理プロセス自体をモニタリングし、評価し、改善して行くプロセスです。

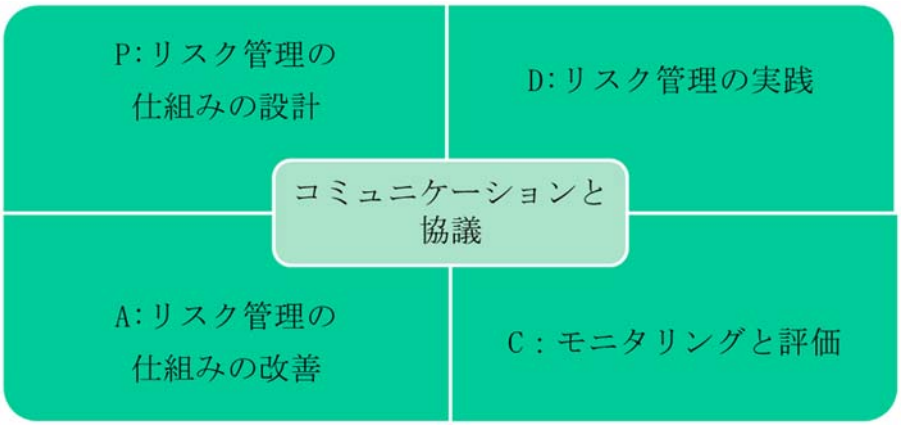


図 4-3 リスク管理における PDCA サイクル

５　JNSA 西日本支部成果物との関係

JNSA 西日本支部では、これまで「中小企業向け情報セキュリティチェックシート[8]」、「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[9]」を作成してきました。

今回、改版した情報セキュリティポリシーサンプルとこれまでの成果物には以下の関係があります。

組織は、JNSA 西日本支部の成果物を活用することで情報セキュリティを自律的に推進が可能になり、具体的な情報セキュリティ対策の実現の検討では「JNSA ソリューションガイド[10]」が活用できると考えています。

なお、「中小企業向け情報セキュリティチェックシート」、「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」は、ともに ISO/IEC 27001:2005 を参考としています。

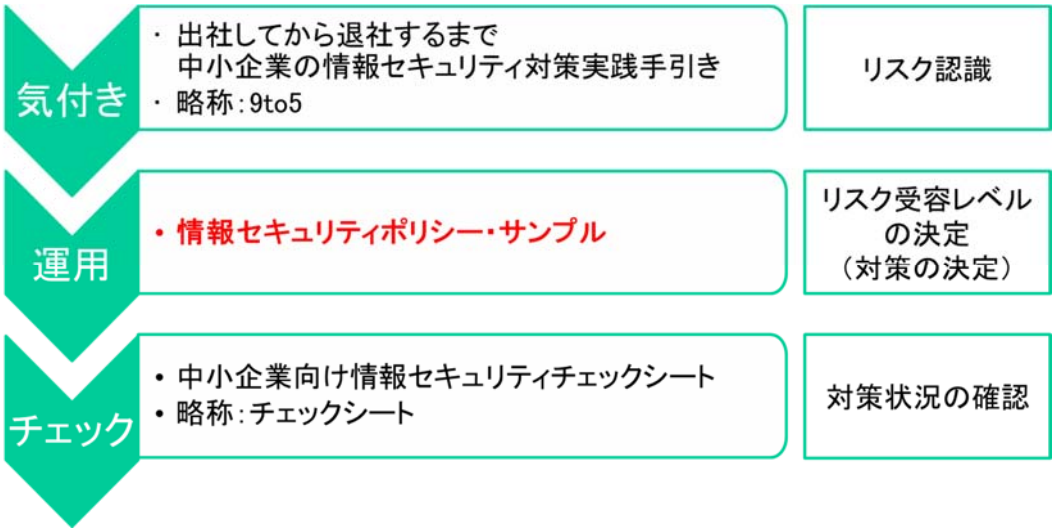


図 5-1　JNSA 西日本支部の成果物の関係

改版した情報セキュリティポリシーサンプルの各文書と「中小企業向け情報セキュリティチェックシート」、「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」、0.92a 版との関係を、表 5-1 に示します。表 5-1 の参照方法は下記のとおりです。

---

[8]中小企業向け情報セキュリティチェックシート　公開サイト
http://www.jnsa.org/seminar/nsf/2014kansai/data/3_shimakura_2.xlsx

[9] 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　公開サイト
http://www.jnsa.org/result/2013/chusho_sec/index.html

[10] JNSA ソリューションガイド
http://www.jnsa.org/JNSASolutionGuide/IndexAction.do;jsessionid=9D3183A453F6E1F8512CEF473ECDC621

表 5-1 の見方

- ①～⑮の規程　：改版後の情報セキュリティポリシーサンプルの各文書
- チェックシート　：「中小企業向け情報セキュリティチェックシート」を指す
- 9to5　：「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」を指す
- Ax（x は数字）　：チェックシートの「上位」と位置付けたもの、x はその項番
- Bx（x は数字）　：9to5 に記載した情報セキュリティ管理策、x はその項番
- Cx（x は数字）　：0.92a 版に記載され、今回付与したもの、x はその項番
- □　：0.92a 版にないもの

表 5-1 情報セキュリティポリシーサンプルと西日本支部成果物、0.92a 版の関係（1/3）

0.92a 版	チェックシート/9to5
① 報セキュリティ基本方針 情報セキュリティ方針	
C0. 情報セキュリティ基本方針 C0. 情報セキュリティ方針	A1. 情報セキュリティ基本方針
② 人的管理規程	
C20. プライバシーに関する標準 C24. セキュリティ教育に関する標準 C25. 罰則に関する標準	A2. 責任の明確化 A3. 職務の分離 A7. 法令順守 A8. 秘密保持
③ 外部委託先管理規程	
C2. 委託時の契約に関する標準	A4. 委託先の管理 B2. クラウドサービスの利用
④ 文書管理規程	
C26. スタンダード更新手順に関する標準 C29. プロシージャ配布の標準	A6. 規程の文書化とレビュー
⑤ 監査規程	
C23. 監査標準	A9. 情報セキュリティの確認
⑥ 物理的管理規程	
C3. サーバルームに関する標準 C4. 物理的対策標準 C5. 職場環境におけるセキュリティ標準	B1. セキュリティ境界と入退出管理
⑦ リスク管理規程	
	A5. 情報資産管理台帳

表 5-1 情報セキュリティポリシーサンプルと西日本支部成果物、0.92a 版の関係（2/3）

0.92a 版	チェックシート/9to5
⑧ セキュリティインシデント報告・対応規程	
C22. セキュリティインシデント報告・対応標準	B3. 障害・事故管理
⑨ システム変更管理規程	
	B16. 変更管理
⑩ システム開発規程	
	B12. Web の開発管理
⑪ システム管理規程	
C3. サーバルームに関する標準 C8. サーバ等に関する標準 C11. ユーザー認証標準 C12. ウィルス対策標準 C16. 媒体の取扱に関する標準 C17. アカウント管理標準 C18. システム維持に関する標準 C19. システム監視に関する標準 C21. セキュリティ情報収集及び配信標準	B2. クラウドサービスの利用 B4. IT 継続性 B5. 認証と権限 B7. パッチの適用 B8. ウイルス及び悪意のあるプログラムに対する対策 B9. 記憶媒体の管理 B10. スマートデバイス B13. ログの取得 B14. バックアップ B15. 容量・能力の管理 B17. 構成管理 B19. 暗号化
⑫ ネットワーク管理規程	
C6. ネットワーク構築標準 C7. 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 C27. 専用線及び VPN に関する標準 C28. 外部公開サーバに関する標準	B4. IT 継続性 B6. ネットワークのアクセス制限 B5. 認証と権限 B7. パッチの適用 B8. ウイルス及び悪意のあるプログラムに対する対策 B13. ログの取得 B15. 容量・能力の管理 B17. 構成管理 B19. 暗号化

表 5-1 情報セキュリティポリシーサンプルと西日本支部成果物、0.92a 版の関係（3/3）

0.92a 版	チェックシート/9to5
⑬システム利用規程	
C1. ソフトウェア／ハードウェアの購入及び導入標準 C9. クライアント等におけるセキュリティ対策標準 C10. 社内ネットワーク利用標準 C12. ウィルス対策標準 C13. 電子メールサービス利用標準 C14. Web サービス利用標準 C15. リモートアクセスサービス利用標準	B2. クラウドサービスの利用 B3. 障害・事故管理 B5. 認証と権限 B6. ネットワークのアクセス制限 B7. パッチの適用 B8. ウイルス及び悪意のあるプログラムに対する対策 B9. 記憶媒体の管理 B11. 電子メールの利用 B14. バックアップ B19. 暗号化 B20. アプリケーションの利用 B21. クリアデスク・クリアスクリーン
⑭スマートデバイス利用規程	
	B10. スマートデバイス
⑮SNS 利用規程	
	B18. SNS の利用

５．１　９to５の活用

図 5-1 に示すとおり「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)」はリスクの認識に活用します。

「9to5」では、「日常業務に潜むリスク」を認識できます。

５．１．１　９to５の構成

「9to5」は、「導入部」、「第 1 部　情報セキュリティ管理策」、「第 2 部　業務に基づく情報セキュリティ対策」、「付録」、「参考資料」という構成です。

表 5-1 に各章の概要を示します。

表 5-1 9to5 概要

<table>
<tr><th>部</th><th>記載概要</th></tr>
<tr><td>導入部</td><td>以下について記載
1.概要
2.本ガイドライの対象企業
3.本ガイドラインの対象読者
4.本ガイドラインの使用方法</td></tr>
<tr><td>第 1 部</td><td>以下の 21 の情報セキュリティ管理項目を記載
<table>
<tr><td>1.セキュリティ境界と入退出管理</td><td>12.Web の開発管理</td></tr>
<tr><td>2.クラウドサービスの利用</td><td>13.ログの取得</td></tr>
<tr><td>3.障害・事故管理</td><td>14.バックアップ</td></tr>
<tr><td>4.IT 継続性</td><td>15.容量・能力の管理</td></tr>
<tr><td>5.認証と権限</td><td>16.変更管理</td></tr>
<tr><td>6.ネットワークのアクセス制限</td><td>17.構成管理</td></tr>
<tr><td>7.パッチの適用</td><td>18.SNS の利用</td></tr>
<tr><td>8.ウイルス及び悪意のあるプログラムに対する対策</td><td>19.暗号化</td></tr>
<tr><td>9.記憶媒体の管理</td><td>20.アプリケーションの利用</td></tr>
<tr><td>10.スマートデバイス</td><td>21.クリアデスク・クリアスクリーン</td></tr>
<tr><td>11.電子メールの利用</td><td></td></tr>
</table></td></tr>
<tr><td>第 2 部</td><td>以下の 6 つのシーンで 69 業務に基づく情報セキュリティ対策例を記載
<table>
<tr><th>シーン</th><th>業務数</th></tr>
<tr><td>出社</td><td>1</td></tr>
<tr><td>社内業務</td><td>33</td></tr>
<tr><td>社外業務</td><td>15</td></tr>
<tr><td>退社</td><td>1</td></tr>
<tr><td>帰宅</td><td>4</td></tr>
<tr><td>システム管理業務</td><td>15</td></tr>
</table></td></tr>
<tr><td>付録</td><td>以下について記載
用語、情報資産の洗い出しについて、本手引き管理項目と ISMS 詳細管理策との対応、システム概念図</td></tr>
<tr><td>参考情報</td><td>9to5 が参考、参照する情報</td></tr>
</table>

５．１．２　９to５の活用方法

「9to5」の「第 1 部　情報セキュリティ管理策」、「第 2 部　業務に基づく情報セキュリティ対策」、「参考情報」との関係を、図 5-2 に示します。

第 2 部で業務に潜むリスクを把握し、第 1 部の管理策を参考にその対策を検討します。

対策の具体的な実現方法、設定などについては参考情報に記載する参照先を活用します。

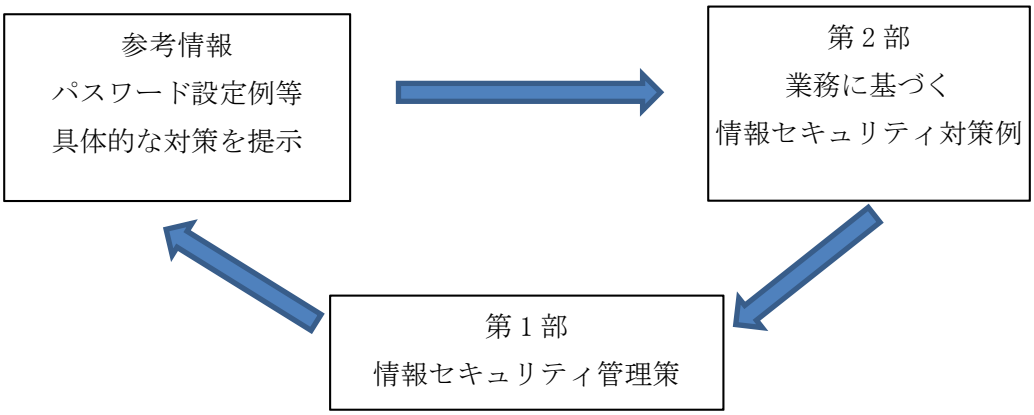


図 5-2 9to5 の活用方法

５．１．３　９to５　第 2 部からの活用事例

第 2 部では、業務を大きく、「出社」、「社内業務」、「社外業務」、「退社」、「帰宅」、「システム管理業務」に分け、各業務に潜むセキュリティ上の主な脆弱性の例を列挙し、それにより発生する可能性のあるリスク例を記載しています。

これにより、読者の方には一般的な業務に潜む情報セキュリティ上のリスクをご理解して頂くと伴に、自組織にあてはめることで、自組織に潜むリスクを把握して頂けるものと、考えています。

「9to5」の「第 2 部　業務に基づく情報セキュリティ対策」を参考に、業務に潜むリスクを把握する事例を図 5-3 に示します。

図 5-3 の例では、「PC を起動しログインするさいのパスワード入力」、という業務シーンにおいて、「現状のセキュリティレベル」に記載する弱いパスワードを利用することが、「脅威の要因」と「リスクシナリオ」から、誰から、どのような攻撃があり、そのリスクがなにか、把握できます。

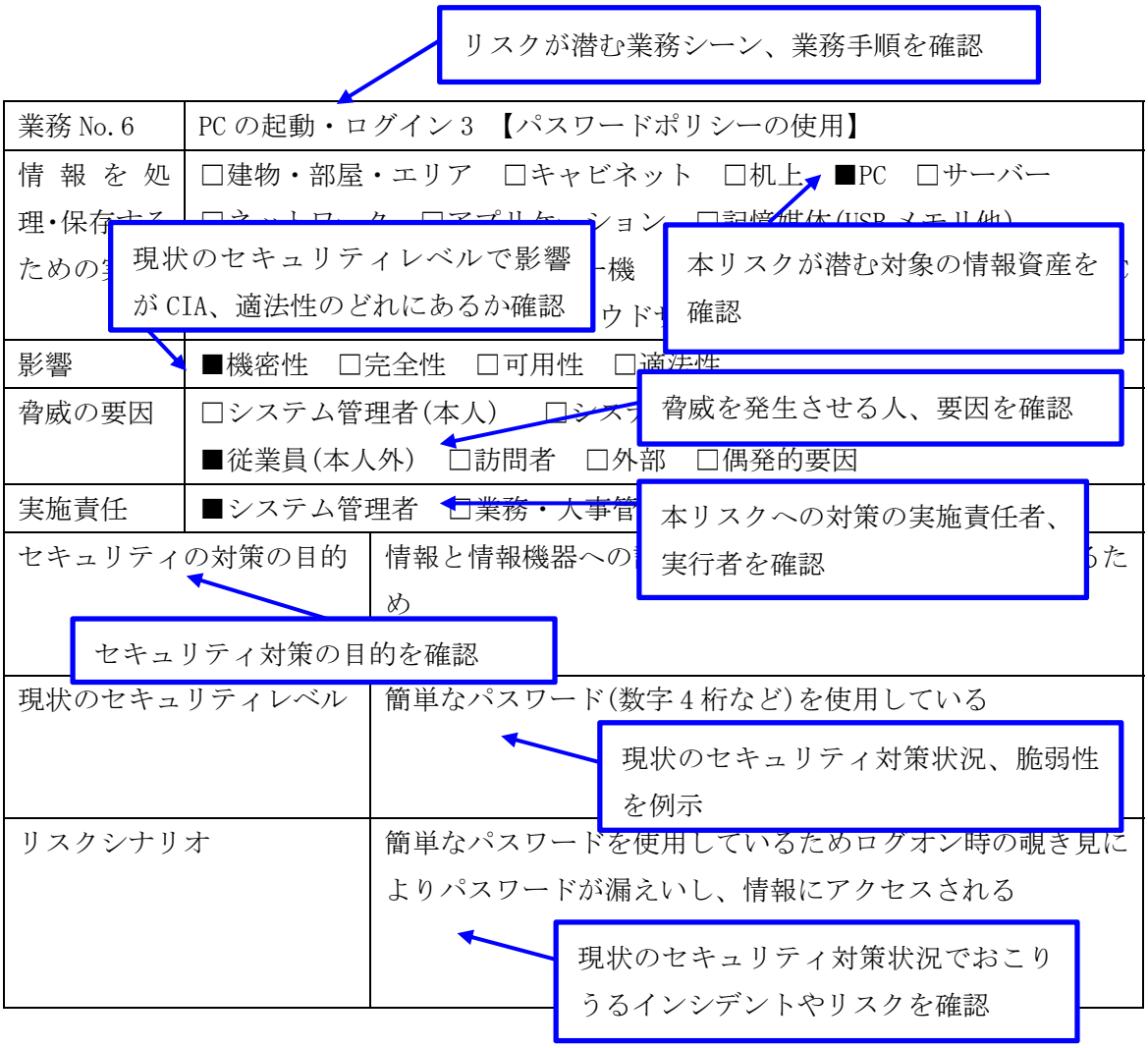


図 5-3　リスク認識への活用事例

認識したリスクへの対応は、「セキュリティ対策の目的」で強固なパスワードを使う理由を再確認し、「実施責任」を確認することで強固なパスワードを設定するためのコントロールや実行を誰が行うか、明らかとなります。

図 5-4 には、図 5-3 に続く対策を記載した後半を示します。

対策には IT を活用した「技術的対策」と、人の行動による「人的対策」があり、それぞれに示す例から、どのような対策があるか、確認します。

また、対策の導入後に、適切に対策が実行されているか、無効化されていないか、などの運用の確認が重要であり、確認すべき事項を「運用で心がけるポイント」に記載しています。これは、当、情報セキュリティサンプルポリシーの改版におけるポイントとなっています。(「３．４　情報セキュリティ対策の日々の運用を重視ポリシー」参照)

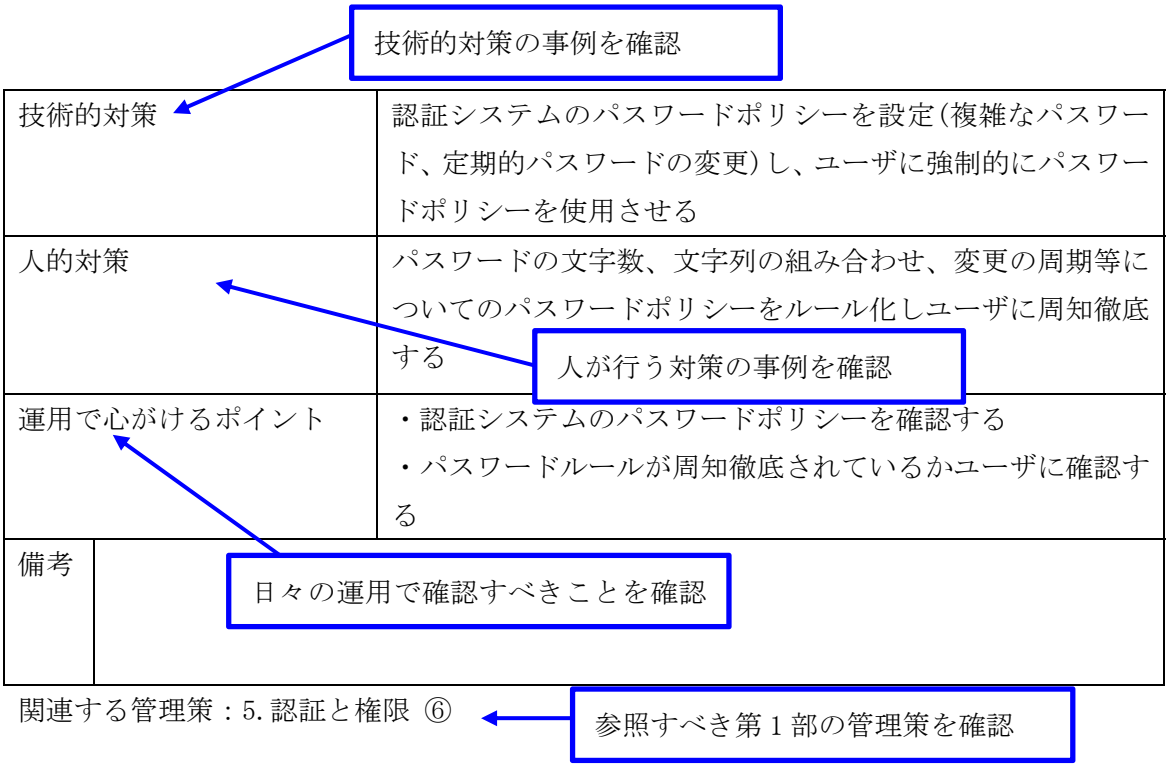


図 5-4　対策の例示

また、「関連する管理策」から、本対策の具体的な内容を第 1 部の管理策で確認します。図 5-4 の例では、パスワード対策の具体的な内容は、第 1 部の「5. 認証と権限」の管理策の⑥を参照先として示しています。図 5-5 に第 1 部の記載例を示します。

5. 認証と権限

(1)管理目的

情報と情報機器への許可されていないアクセスを防止するため

(2)管理策

①入館・入室設備、・・・・

・

・

・

()数字は 9to5 の「参考資料」の項番

⑥パスワード[13]は例えば「12 文字以上に設定し、
大文字、小文字、数字、特殊文字の 4 つを組み合わせ、
3 カ月に 1 度変更する」

図 5-5　第 1 部の記載例

「9to5」の「参考情報」には、管理策の具体化に役立つ参考となる資料を示しています。図 5-5 の例では、パスワードの強度の推奨について以下の参照先を示しています。

9to5「参考情報」 (13)

(13)Japan Vulnerability Notes
「共通セキュリティ設定一覧 CCE 概説 (パスワード編)」
http://jvndb.jvn.jp/apis/myjvn/cccheck/cce_password.html

５．２　情報セキュリティポリシーサンプルの活用

守る対象の情報資産の価値と「５．１　９to５の活用」で把握したリスクから、リスクの受容レベルを判断し、「５．１　９to５の活用」で抽出した対策例を参考に、受容レベルを超えるリスクへの対応を決定します。

導入を決定した対策は、情報セキュリティポリシーに明記します。

情報セキュリティポリシーの作成には、情報セキュリティポリシーサンプルを活用しますが、改版した情報セキュリティポリシーサンプルは、組織によっては、過剰な対策の記載となっています。

そのような組織では、自組織に適した情報セキュリティポリシー策定には、以下の手順をふむことで、効率的に情報セキュリティポリシーサンプルの活用が可能です。

(1) 組織に合わせた体制を考える

情報セキュリティポリシーサンプルの「情報セキュリティ方針」には、情報セキュリティを維持するための組織、役割について記載しています。組織のどの部門が、誰が「情報セキュリティ方針」の記載例に相当するのか、また、組織内に設置が困難な役割はないか、などを検討します。

その結果を元に、情報セキュリティポリシーサンプルの「情報セキュリティ方針」の体制を組織に合わせて記載を変更します。

(2) 組織で実施する対策の記載を確認

組織で実施済や導入を決めた対策が、情報セキュリティポリシーサンプルに記載があるか、確認します。

記載があるものについては、情報セキュリティポリシーサンプルの記載内容、記載レベルを確認します。

実施済や導入を決めた対策でも実現方法や運用方法など詳細な部分では、組織の実態と異なる部分があるため、細かに確認が必要です。

(3) 過剰な対策、不要な対策の記載を削除

組織で導入しない対策や、実施済や導入を決めた対策でも詳細な部分、運用方法などで異なる部分を確認し、情報セキュリティポリシーサンプルからその記載を削除します。

(4) 全体の整合を確認

全体を確認し、体制と役割と各規程の実施者との間に矛盾がないか、表現が異なる役割がないか、どこにも定義されていない役割、担当がないか、などを確認します。

また、記載する対策に矛盾がないか、削除した対策があることを前提にした記載が他の規程に残っていないか、などを確認し、該当するものがあれば修正します。

５．３　中小企業向け情報セキュリティチェックシートの活用

図 5-1 に示すとおり「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)」は対策状況の確認に活用します。

チェックシートは、「9to5」で把握した業務において起こりうるリスクを念頭に、現状の対策状況を確認し、リスクに応じた適切な対策を導くことに活用します。

５．３．１　チェックシートの構成

「チェックシート」は、「上位層」、「下位層」の 2 階層の構成です。

「上位層」は「9to5」では前提条件となった、対策を持続的に行うためのマネージメント項目であり、「下位層」は具体的な情報セキュリティ対策項目です。

「下位層」は、「9to5」の第 1 部と対応していますが、「9to5」の第 1 部の「19.暗号化」、「20.アプリケーションの利用」、「21.クリアデスク・クリアスクリーン」は「チェックシート」では確認内容の各項目に分散されるため、対応付けはありません。

表 5-2 に各層の概要を示します。

表 5-2　チェックシート概要

<table>
<tr><th>部</th><th>記載概要</th></tr>
<tr><td>上位層</td><td>以下の 9 のマネージメント項目をチェック対象
<table>
<tr><td>1. 情報セキュリティ基本方針</td></tr>
<tr><td>2. 責任の明確化</td></tr>
<tr><td>3. 職務の分離</td></tr>
<tr><td>4. 委託先の管理</td></tr>
<tr><td>5. 情報資産管理台帳</td></tr>
<tr><td>6. 規程の文書化とレビュー</td></tr>
<tr><td>7. 法令順守</td></tr>
<tr><td>8. 秘密保持</td></tr>
<tr><td>9. 情報セキュリティの確認</td></tr>
</table></td></tr>
<tr><td>下位層</td><td>以下の 18 項目の情報セキュリティ対策がチェック対象
<table>
<tr><td>1. セキュリティ境界と入退出管理</td><td>10. スマートデバイス</td></tr>
<tr><td>2. クラウドサービスの利用</td><td>11. 電子メールの利用</td></tr>
<tr><td>3. 障害・事故管理</td><td>12. Web の開発管理</td></tr>
<tr><td>4. IT 継続性</td><td>13. ログの取得</td></tr>
<tr><td>5. 認証と権限</td><td>14. バックアップ</td></tr>
<tr><td>6. ネットワークのアクセス制限</td><td>15. 容量・能力の管理</td></tr>
<tr><td>7. パッチの適用</td><td>16. 変更管理</td></tr>
<tr><td>8. ウイルス及び悪意のあるプログラムに対する対策</td><td>17. 構成管理</td></tr>
<tr><td>9. 記憶媒体の管理</td><td>18. SNS の利用</td></tr>
</table></td></tr>
</table>

５．３．２　チェックシートの活用方法

前述のとおり、下位層は、「9to5」の第 1 部と紐づいており、「9to5」の第 1 部でリスクを認識したあと、自組織の状況確認をチェックシートで行います。

図 5-6 に上位層を、図 5-7 に下位層のチェックシートを示します。

なお、チェックシートの項目毎に、具体的な対策を検討するさいに参考となる「JNSA ソリューションガイド」の項目を記載しています。

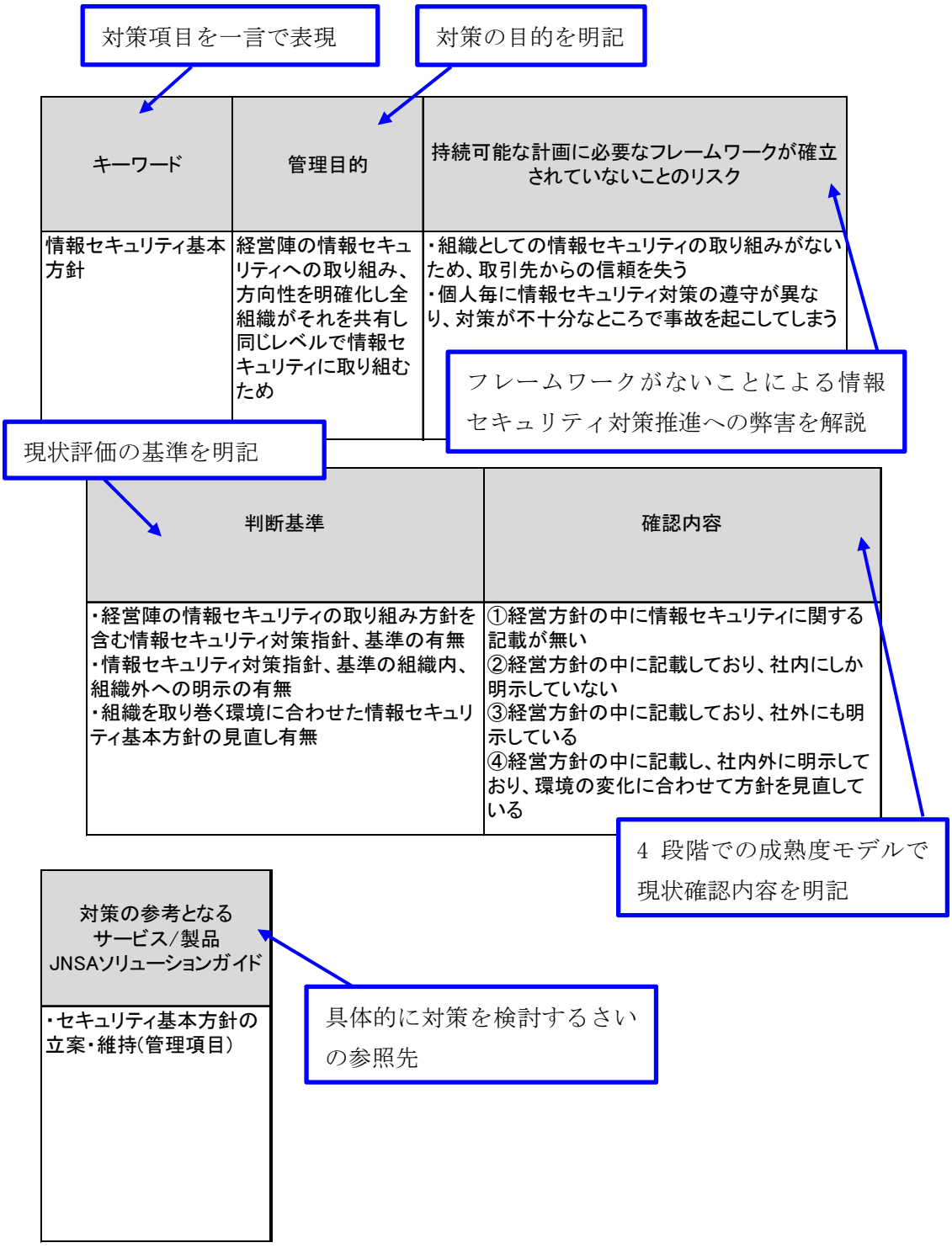


図 5-6 チェックシート（上位層）

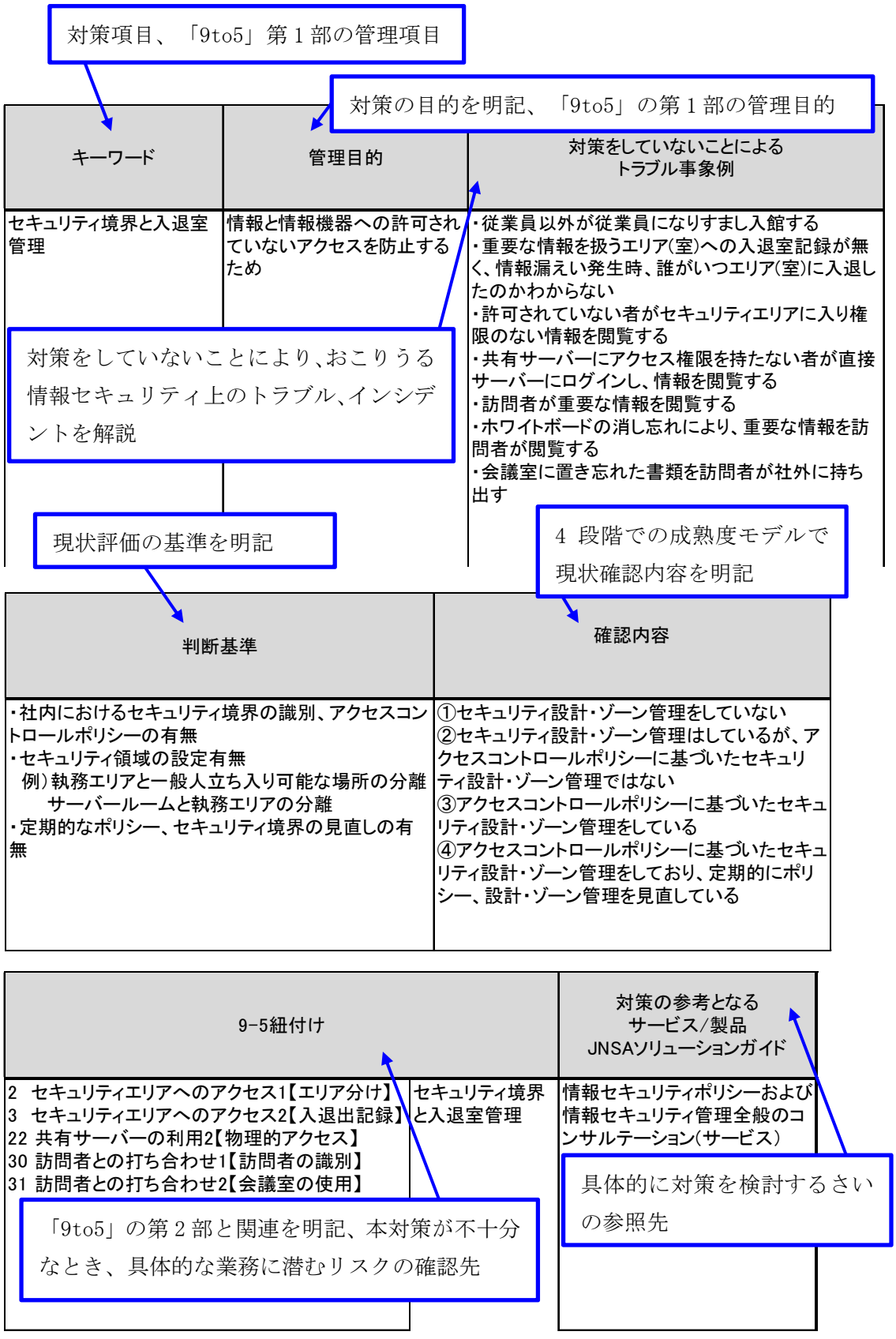


図 5-7 チェックシート（下位層）

チェックシートの上位層、下位層とも、「判断基準」と「確認内容」を記載しています。

「判断基準」は、対策状況を評価するさいの重要ポイントを記載しており、自組織の現状の確認は、「確認内容」の設問で行います。

「判断基準」、「確認内容」とも図 5-8 に示す成熟度の段階となっています。

レベル１は、何ら対策をしていない状況です。最高レベルは４であり、情報セキュリティポリシーサンプルに盛り込んだ、日々の情報セキュリティ対策の運用が適切に実施されていることを確認するプロセス、その延長で実施すべきリスクの見直しの運用が行われている状態です。

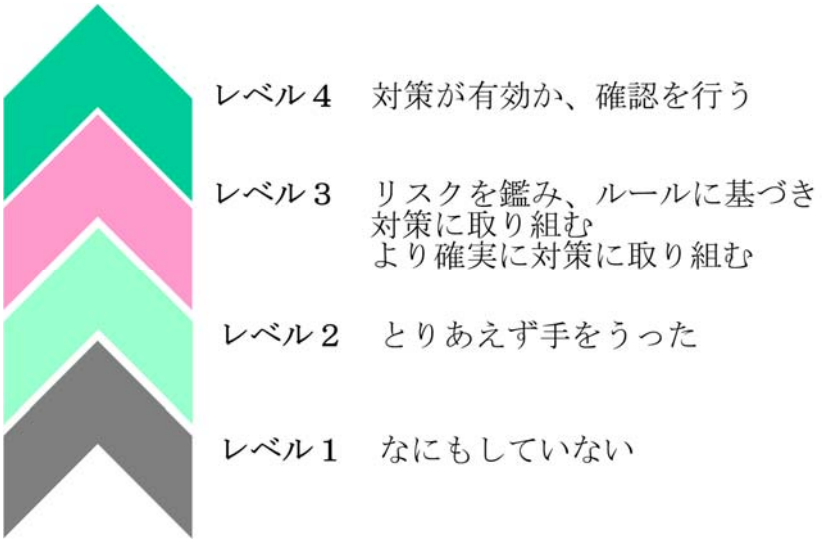


図 5-8 判断基準、確認内容の成熟度の段階

(1) 上位層でマネージメント状況をチェック

上位層のチェック項目は、「9to5」では前提条件となったため、「9to5」で上位層の各項目に関するリスクは認識できません。

そこで上位層ではこの前提条件の対策が行われなかった場合の弊害について「持続可能な計画に必要なフレームワークが確立されていないことのリスク」という項目に記載しています。

図 5-6 の例では、「情報セキュリティ基本方針」を確立する目的を「管理目的」で確認し、「情報セキュリティ基本方針」が確立されていないとどのような弊害があるのかを「持続可能な計画に必要なフレームワークが確立されていないことのリスク」で確認することができます。

「判断基準」には図 5-8 に示す成熟度での段階で評価する重要ポイントを記載しており、「確認内容」の設問で自組織の状況を確認し、自組織の対策状況の把握と評価を行います。

(2) 下位層で対策状況をチェック

下位層のチェック項目は、「9to5」の第 1 部と紐づいており、「9to5」の第 1 部でリスクを認識したあと、自組織の状況確認をチェックシートで行います。

「キーワード」は「9to5」の第 1 部の各項目名となっており、「管理目的」は「9to5」の第 1 部の各項目の「(1)管理目的」と同じ内容です。

「判断基準」には図 5-8 に示す成熟度での段階で評価する重要ポイントを記載しており、「確認内容」の設問で自組織の状況を確認し、自組織の対策状況の把握と評価を行います。

「対策をしていないことによるトラブル事象例」は、「9to5」の第 2 部に記載する対策をしていないことにより、おこりうる情報セキュリティ上のトラブル、インシデントである「リスクシナリオ」の再確認に利用できます。

「9-5 紐付け」では、対応する「9to5」の第 2 部の業務シーンを記載しており、具体的な業務に潜むリスクの確認を行うさいに、参照します。

(3) チェックシートから入るリスク認識

「チェックシート」、「9to5」は、ともに ISO/IEC 27001:2005 を参考としていますが、ISO/IEC 27001:2005 の管理策を元に体系的に現状を把握しリスクの把握を行いたい方は、「チェックシート」を初めから利用し現状を把握、リスクの評価を行います。

そのさい、「チェックシート」の「9-5 紐付け」で対応する「9to5」の第 2 部の業務シーンを参照し、業務のリスクを参考にすることができます。

(4) ＪＮＳＡソリューションガイドの活用

「チェックシート」で自組織の状況を把握し、改善に向け具体的な対策を検討するさい、「JNSA ソリューションガイド」が参考になります。

「チェックシート」の各項目の対策を実現する製品やサービス、ソリューションを「JNSA ソリューションガイド」では紹介しています。

5.1 項から 5.3 項に記載した JNSA 西日本支部成果物と JNSA ソリューションガイドの活用の関係を図 5-9 に示します。

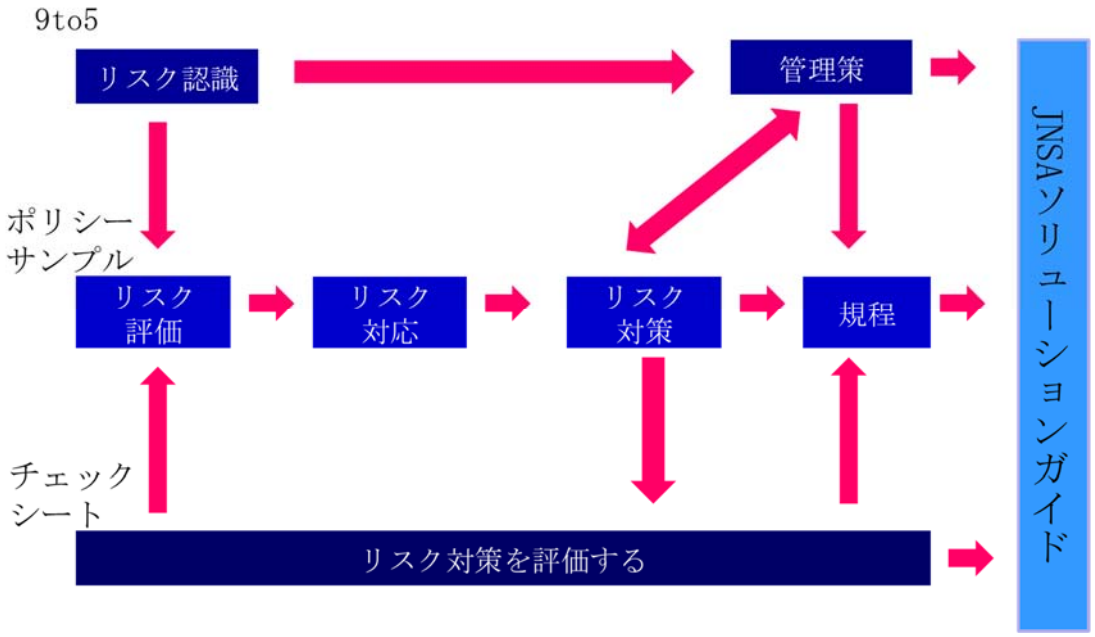


図 5-9 JNSA 西日本成果物と JNSA ソリューションガイドの活用における関係

補足

セキュリティと情報セキュリティ

情報セキュリティポリシーサンプル　改版（1.0版）では、「セキュリティ」と「情報セキュリティ」はそれぞれ下記を対象として使い分けをしています。

・セキュリティ

環境、物理的なものや過失なども含まれるもの

・情報セキュリティ

マネージメントを含めた情報システムに関わるもの

システム開発規程について

システム開発を行うさい、その企画段階から情報セキュリティ委員会との連携は不可欠です。

情報セキュリティ委員会は、システム開発及び運用開始後に必要となる各種規程類を提示し、この範囲の中で適切なシステムが開発されることを求め、開発プロジェクト遂行においても遵守されるべき規定を提示する必要があります。

システム開発において、一般的に情報セキュリティ委員会が提示すべき規程類は以下の通りです。

・外部委託先管理規程
・文書管理規程
・リスク管理規程
・セキュリティインシデント報告・対応規程
・システム管理規程
・ネットワーク管理規程
・システム利用規程
・スマートデバイス利用規程

(1)要件定義

セキュリティ要件を担当する者は、システム要件定義においてセキュリティ要件を、情報セキュリティ委員会から提示された各種規程を元に作成しなければなりません。

セキュリティ要件の中には、開発するシステムが運用段階に入った時点のリスクアセスメントを、設計フェーズ完了時点で実施するための要項を明記します。

また、要件定義が完了した時点では開発プロジェクト遂行に関するリスクアセスメントを情報システム主管部門とともに実施します。

(2) 開発環境

開発環境は、本番環境と別に構築されるのが理想ですが、本番環境を開発環境に用

いる場合も少なくありません。

本番環境を開発環境に用いる場合は、開発用として本番環境に追加・変更された要件については明確にしておき、本番開始時点ではそれらを適切に対処しておく必要があります。一般的に想定される追加・変更内容には以下のものがあります。

・開発者用アカウントの追加
・管理者権限を持つアカウントのパスワードの変更
・テストデータの追加
・開発環境用のログデータ取得設定およびログデータ

(3) 導入

設計段階で実施されたリスクアセスメントで抽出された対応すべきリスクをもとに、導入するシステム上で対策についての検査を実施しますが、この段階で新たに抽出されるリスクが判明することもあります。リスクアセスメントについては、導入開始直前に再度実施することが必要です。また、以降も定期的に実施するべきです。

スマートデバイスについて

情報セキュリティポリシーサンプルでは、スマートデバイスとしてスマートフォンやタブレット端末を想定し、次のように規定しています。

・持ち運びができる
・通信事業者が設置運用するネットワークに接続できる
・Wi-Fi 通信ができる

また次のような特徴を持つことが多い前提で、遵守事項を定めています。

・位置情報機能（GPS）を備える
・SNS との連携やクラウドサービスとの親和性が高い

(1) 利用できるスマートデバイス

情報セキュリティポリシーサンプルでは、組織から支給・貸与されたスマートデバイスを使用することを前提としていますが、組織によっては個人の所有物を業務に用いるいわゆる BYOD を認める場合もあるかと思います。その場合は以下の点に注意が必要です。

・組織が支給、貸与するスマートデバイスと組織が求める同等のセキュリティレベルを担保できること。
・社内ネットワークへの接続や紛失時の対応で必要となる端末の識別情報を提出させ、万が一の場合はリモートワイプ機能などを使って所有者個人のデータも消去される可能性があるなど、所有者にとって損失となる事項について事前に合意を得ておく必要がある。

・アプリケーションの利用においては、個人用途にのみ使っているつもりが、電話帳やクラウドサービスとの連携機能によって、業務上の機密情報にアクセスされる場合がある。アプリケーションの権限設定については、安易に権限を ON にしないなど充分注意しなければならない。

(2) 社外ネットワークの利用

街中や施設での無料 Wi-Fi 通信サービスは、パスワード設定があっても通信が暗号化されていない場合や、暗号化されていても共通の暗号・復号鍵を用いるため、当該サービスを利用する者同士では通信のモニタリングが可能など、通信の秘匿が確立されていないことを前提に、機密情報の取扱いは行わない、また、行う必要のある場合は https といった暗号化通信を行う環境を利用するなどの注意が必要です。

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 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