経済産業省委託調査

平成16年度不正アクセス行為等対策業務
（ブロードバンドセキュリティに関する調査研究）

「セキュリティ対策評価モデル」

第１分冊：モデルのコンセプトと対策要求の解説

平成１７年 ２月

電子商取引推進協議会
財団法人日本情報処理開発協会
電子商取引推進センター

この報告書は、平成16年度受託事業として（財）日本情報処理開発協会電子商取引推進センターが経済産業省から委託を受けて、電子商取引推進協議会（ECOM）の協力を得て実施した「不正アクセス行為等対策業務（ブロードバンドセキュリティに関する調査研究）」の成果を取りまとめたものです。

はじめに

平成 16 年度経済産業省受託業務「ブロードバンドセキュリティに関する調査研究」についての成果である「セキュリティ対策評価モデル」の実用試作版の第 1 分冊である本報告書は、セキュリティ対策評価モデルのコンセプトとその有用性についての考察、ならびに評価モデルの中核をなすセキュリティ対策としての対策要求の解説を纏めたものである。

ネット社会の進展とともに社会的な課題となってきた、ネット社会を形作っている数多くのシステムにおけるセキュリティ対策の向上を実現するためには、組織やシステムの規模等にかかわらず適用できる実務的なセキュリティ対策の実践ガイドの提供や、セキュリティ対策の十分性を客観的に評価する手法の確立という要求への応えとして開発したここに紹介する「セキュリティ対策評価モデル」は、実務的なセキュリティ対策ガイドのベースとして、あるいはセキュリティ対策の十分性の評価を行うためのベースとなりうる、セキュリティ対策の評価についての新しい手法として、IT システムベンダーやセキュリティサービスベンダーのセキュリティの専門家で構成される ECOM の研究チームが議論を重ねたものである。

本冊では、対策現場での具体策の展開に合わせて体系化して示されるセキュリティ対策として実施を求めること、その個々に求められる標準的な対策内容を対策の強度レベルに分けて定義したものを中核としたセキュリティ対策の評価についての手法を一つの体系化した「セキュリティ対策評価モデル」の開発の背景、セキュリティ対策評価モデルのコンセプト、その概要、有用性についての考察等、現時点でのこのモデルに対する作業部会の考えを紹介するものである。

本報告書に示す「セキュリティ対策評価モデル」は、まだ、その完成度から見て、実用試作版の域に止まっているかもしれないが、本モデルをたたき台としたセキュリティ対策の実践論についての議論が広く巻き起これば幸いである。できうれば、多くの方がこのモデルの成長に取組み、一つの方法論として広く受け入れられるものにして頂ければと考える。

目 次

第 1 部 セキュリティ対策評価モデルのコンセプト

1. 開発の背景 2

1.1. 情報セキュリティの重要性の拡大 2
1.2. セキュリティ対策の現状 2
1.3. 問題点の背景 6
1.4. 必要な取組み 8

2. セキュリティ対策評価モデルのコンセプト 10

2.1. セキュリティ対策評価モデルのコンセプト 10
2.2. 本モデルの特徴 13
2.3. 本評価モデルの構成 13
2.4. 評価モデルが対象とするセキュリティ対策の領域 14
2.4.1. 物理的な対象領域 14
2.4.2. 論理的な対象領域 15

3. 評価事項の組立て 16

3.1. 対策要求の組立てについての考え方 16
3.2. 対策要求へのブレークダウン 17
3.2.1. 対策要求へのブレークダウンのアプローチ 17
3.2.2. ステップ 1：対策テーマの洗出しと体系化 18
3.2.3. ステップ 2：対策ドメインから対策要求へのブレークダウン 29
3.3. 対策ドメインと対策要求の概要 31
3.3.1. マネジメント・ビューを構成する対策ドメインと対策要求 31
3.3.2. ビジネスオペレーション・ビューを構成する対策ドメインと対策要求 32
3.3.3. テクニカル＆オペレーション・ビューのサブビュー：システムの信頼性の確保を構成する対策ドメインと対策要求 34
3.3.4. テクニカル＆オペレーション・ビューのサブビュー：攻撃に対するシステムの堅牢性の確保を構成する対策ドメインと対策要求 36
3.3.5. テクニカル＆オペレーション・ビューのサブビュー：セキュアなシステムの構築とそのセキュアな運用の実現を構成する対策ドメインと対策要求 40

3.3.6. テクニカル＆オペレーション･ビユーのサブビユー：必要となるその他のセキュリティ対策を構成する対策ドメインと対策要求 42
3.4. アシュアランス･ビユーを構成する対策ドメインと対策要求 45

4. 対策強度レベルの設定基準 58

4.1. 対策強度の概念 58
4.2. システム全体としてのセキュリティ対策強度の考え方 59
4.3. 個々の対策要求における対策強度 59
4.3.1. 個々対策要求の対策強度の決定要素 59
4.4. 対策要求の個々に対する対策強度レベルの決定手順 60
4.5. 本モデルにおける対策強度の設定基準 61
4.5.1. システム全体に対する対策強度レベル基準 61
4.5.2. 対策要求の個々に定義する対策強度レベル基準 62
4.5.3. システム全体が目標とすべき対策強度レベルと個々の対策要求に求められる対策強度レベルの関係 63
4.5.4. 個々対策要求の対策強度レベルの決め方 64

5. 個別システムに対する本評価モデルの利用場面と利用法の概要 70

5.1. 個別システムにおける本評価モデルの利用場面 70
5.2. セキュリティ対策計画時における利用 70
5.2.1. 本モデルを用いたセキュリティ対策の計画手順 70
5.3. セキュリティ対策の評価への適用 73
5.3.1. セキュリティ対策の評価場面 73
5.3.2. セキュリティ対策の評価手順 73
5.3.3. 個々の対策要求に対する対策強度レベルの評価手順 74
5.3.4. セキュリティ対策の実態の評価 75

6. 本モデルのその他の活用場面 79

6.1. 企業等の組織におけるセキュリティ対策の基盤としての利用 79
6.2. 個別システムの情報セキュリティ監査のベースとしての利用 80
6.3. システムモデル別セキュリティ対策基準およびセキュリティ対策プロファイル定義の基盤としての利用 81
6.3.1. システムモデル別セキュリティ対策基準 81
6.3.2. システムモデル別セキュリティ対策プロファイルの作成への応用 81
6.4. セキュリティ対策の評価･格付けサービスにおける評価のベースとしての利用 82

6.5. ネットワーク経由でのサービスの提供におけるセキュリティ面からの公的あるいは自主規制の基盤としての利用 82
6.6. サービスレベルアグリーメントにおけるセキュリティ関連事項の指定のベースとしての活用 83
6.7. 情報セキュリティに関わるトラブル発生時における責任の分界の判断の基盤としての利用 83
6.8. 情報セキュリティにかかわる保険における保険料や保険金の査定の基盤としての利用 83

7. 今後の課題 84

7.1. 評価モデルの完成度の向上 84
7.1.1. コンセプトのブラッシュアップ 84
7.1.2. 評価事項の組立ての完成度の向上 85
7.1.3. 個々の対策要求に指定する対策強度判定基準の完成度の向上 86
7.1.4. 評価モデルの利用ガイドの整備 86
7.2. 実用環境の整備 86
7.2.1. 関係者間でのこのモデルの存在とその有効性についての周知の確立 87
7.3. 本モデルの有効性の維持を確保するためのスキームの確立 87
7.3.1. 本モデルの有効性の維持を確保するためのスキームの創出 89

第 2 部 対策要求の解説

1. マネジメント・ビュー 91

1.1. セキュリティ対策推進基盤の確立 91
1.1.1. セキュリティマネジメント環境の整備 91
1.1.2. 経営レベルでのセキュリティ要求の明確化 98

2. ビジネスオペレーション・ビュー 103

2.1. セキュアな組織運営と業務運営の実現 103
2.1.1. 組織管理上でのセキュリティ対策 103
2.1.2. 業務運営上でのセキュリティ対策 108
2.1.3. 業務現場での情報の保護の徹底 114
2.1.4. ユーザ管理の徹底 128
2.1.5. 法的要求事項の遵守 131

3. テクニカル＆オペレーション･ビユー 138

3.1. システムの信頼性の確保 138
3.1.1. システムの処理の正確性の確保 138
3.1.2. 障害に対するシステムの堅牢性の確保 144
3.1.3. システムの性能の確保 150
3.2. 攻撃に対するシステムの堅牢性の確保 157
3.2.1. 不正アクセス対策 157
3.2.2. セキュリティホール対策 177
3.2.3. ウイルス対策 182
3.2.4. システム情報およびセキュリティ管理情報の保護 190
3.2.5. システム上の業務情報の保護 195
3.2.6. 通信路上の情報の保護 200
3.2.7. インターネットサービスの利用にあたってのセキュリティ対策 205
3.2.8. サービス妨害への備え 207
3.2.9. システムの動きに対する監視の実施 210
3.3. セキュアなシステムの構築とそのセキュアな運用の実現 217
3.3.1. セキュアなシステムの構築とその維持 217
3.3.2. ソフトウェアの管理の徹底 222
3.3.3. 個々の機器における自衛策の実施 229
3.3.4. セキュアなアプリケーションソフトの開発 233
3.3.5. システム運用上のセキュリティ対策 238
3.4. その他のセキュリティ対策 249
3.4.1. 保管電子情報の有効性の確保 249
3.4.2. 特殊な利用環境に対するセキュリティ対策 255
3.4.3. 施設や設備の保護 266
3.4.4. セキュリティ事故への備え 272

4. アシュアランス･ビユー 282

4.1. セキュリティ対策の実施状況の評価 282
4.1.1. 監査手法による対策状況のチェック 282
4.1.2. 技術的な診断によるセキュリティ対策の欠陥のチェック 287

セキュリティ評価モデルの開発プロジェクト委員リスト

第1部
セキュリティ対策評価モデルのコンセプト

1. 開発の背景

1.1. 情報セキュリティの重要性の拡大

インターネットへの接続はさまざまな脅威が存在し、現在でも、情報セキュリティに関する事件・事故の報告は後を立たない。

ブロードバンドネットワーク環境の進展にともない、行政サービス他のさまざまな社会サービスの提供や利用、経済活動、個人の暮らしといった社会のあらゆる分野がインターネットを利用する仕組みを前提とするようになってきた。このような社会にあっては、ネット接続システムの安全性は、新しい社会の仕組みの安全と信頼に直結する。このため、情報セキュリティの重要性は、今後ますます拡大し、社会的なテーマとして扱われるべき課題と言え、ネット社会を形づくる多くのシステムにおける情報セキュリティを確保するためのセキュリティ対策の向上も、社会的な課題の一つにあげなければならない。

なお、本報告書では、“情報セキュリティ”とは、ネットを介したサービスの提供やこれらの利用、あるいはネットを用いる自社または自家用システムの運用および利用の安全、さまざまな場所における情報の取扱いに関するトラブルを防止するための活動の総称と、また、“セキュリティ対策”とは、さまざまな技術的な対応や関係する活動等で組立てられる、求められる情報セキュリティを確保するための備えを総称としている。

1.2. セキュリティ対策の現状

情報セキュリティについての認識に向上にともない、多くの企業・機関等の組織におけるセキュリティ対策に長足の進歩はみられるものの、情報の漏洩や、ホームページの改ざん等の事件・事故の報道は後を絶たない。また、脆弱性情報が公知されているにも関わらず、対策の遅れから自社のシステムがウイルスに感染するだけでなく、ウイルスの感染拡大に手を貸してしまっているシステムも後を絶たない。さらに、報道等で表面化しないまでも、外部に見せてはならない情報が満載された PC の盗難や USB メモリの紛失等への対策で業務に混乱を生じたという話も多く聞こえてくる。

これらの事実は、情報セキュリティの重要性が声高く叫ばれるようになって、多くの組織におけるセキュリティ対策への取組みは、従前にくらべ格段と進んでいると見られるものの、セキュリティ対策の実態は、対策の不備やその運用上の不手際等から隙を残すものが多いことを示している。また、ECOM が平成 13 年度に実施した小規模 EC サイトを対象としたセキュリティ対策の実態調査の結果からも明らかなように、特に、セキュリティ技術的弱者といえる中小企業での対応の遅れは相当と思われる。

組織におけるセキュリティ対策の現状は、一言で言うと不十分と断じなければならない。セキュリティ対策は、技術、組織の運営、要員の管理が一体となって、はじめて期待するようなものになるも

ので、今や、経営課題の一つと見なければならないが、セキュリティ対策が実態として組織的、戦略的なものになっていないところに根本原因があると思われる。

多くの組織で、セキュリティ対策が不十分で期待したレベルに達しないことになっている背景を示したものが図 1-1 である。

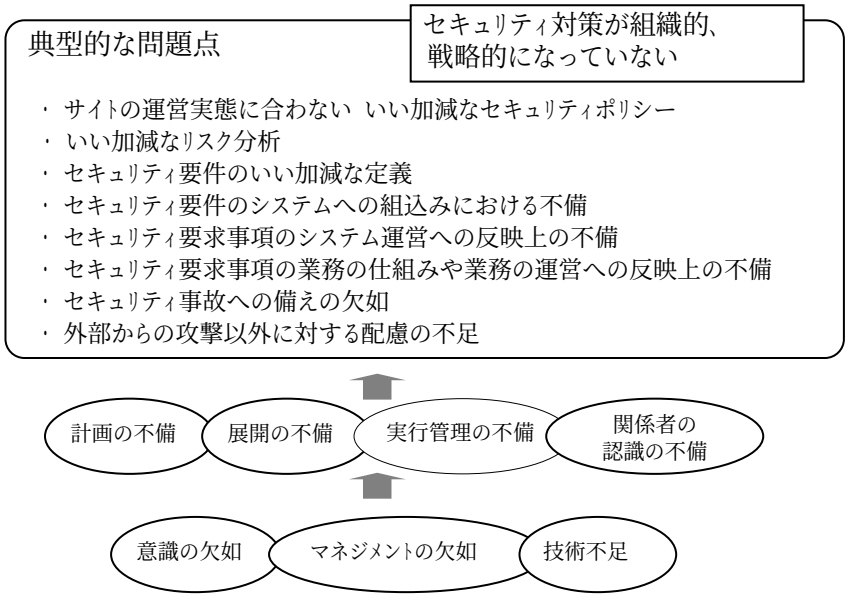

図 1-1 多くに組織に見られるセキュリティ対策における問題点

個々の問題点についての分析を以下に示す。

(1)セキュリティポリシーについての問題点

まず根本問題として、経営レベルの問題として取組まなければならない(トップレベルの)セキュリティポリシーがその本来の役目を果たしていないことがあげられる。セキュリティ対策として“何をどこまで実施するのか”についての枠組みを明確にするこの経営レベルのセキュリティポリシーは、対象とするシステム(注1)のセキュリティ特性(注2)および情報セキュリティに対する経営の方針を反映したもので、かつそれが指示するところはセキュリティ対策として何をどこまで実施するのかについての明確な指針が与えられていなければならない。また、その指示するところが関係者(注3)に徹底しておりセキュリティ対策の実践に的確に反映されていなければならない。

しかし、実態としては、以下の点について、自信をもって十分と言える組織はそう多くないと見られる。

- セキュリティポリシーはリスク分析の結果に照らし適切か？
- セキュリティポリシーは組織や対応システムの運営形態に照らし適切か？
- 経営陣は対象システムに対する情報セキュリティについて明確な指針を有し、かつ、セキュリティポリシーは経営の情報セキュリティについての取組方針を適切に反映しているか？
- セキュリティポリシーは関係者に徹底しているか？
- セキュリティ対策の実践にセキュリティポリシーが反映されていることが確認されているか？

(注1) ここで言う“システム”とは、セキュリティ対策の検討の対象となる情報を取扱うエンティティと

する。情報の取扱いを論ずる時に不可分となる組織運営、業務の運営、および関連情報システムとその運用全体を指す。

(注2) “セキュリティ特性”とは、対象業務、組織および業務の運営形態、対応システムの作りや運用形態からくるリスクの特性を反映した、対象システムに対するセキュリティ対策の要件を決める要素を言う。

(注3) ここで言う“関係者“とは、セキュリティ対策の実践にかかわる者すべてを指す。セキュリティ対策について全責任を持つ経営者や、セキュリティ対策の計画者、システムの構築・運用関係者、業務に携わるもの等を含む。システムの開発や運用、さらには業務の一部をアウトソーシングしている場合、外注先もこの関係者に含まれる。

(2)リスク分析についての問題点

ISMS(注4)の進展等でセキュリティ対策を進めるうえでのリスク分析の重要性についての認識は深まりつつあるものの、リスク分析が適切なセキュリティ対策に結びつくように適切に行われているところはそう多くないように見える。特に、中小の組織にあってはリスク分析がまともに行われているところは少ないと言えるのが現状であろう。この背景としては、セキュリティ対策として、“何をどこまで実施すればいいのか”の判断するための実務的なガイドがないため、専門家がいない中小の組織では、リスク分析で明らかにするところが明確に把握できていため、対象システムの運営形態によって異なったものになるリスク分析のポイントが分からず、過度に細かく掘り下げたり、逆に必要なところに粗かったりとかで、そのポイントをはずしていることにもよると考えられる。

(注4) ISMS：ISO/IEC17799(JISX5080)で、情報セキュリティマネジメントシステム(Information Security Management System)を指す。

(3)セキュリティ要件の定義についての問題点

セキュリティ対策の実施にあたっては、細かい実施上の要件がめられなければならないものがある。情報の保護の基本となる情報へのアクセス制御が適切に行われるためには、保護対象の情報の個々に対し、登録、参照、更新、抹消等の当該情報に対するアクセス権限者やアクセス権限付与者のアクセス権の範囲の指定や、適用すべきアクセス制限の技法の指定等のさまざまなアクセス制御についての条件が適切に指定されていなければならない。セキュリティ要件とは、セキュリティ対策として実施が求められることの個々に対する、実施にあたっての細部を指定するものである。

セキュリティ対策の実施にあたっては、随所にこのような要件の定義が必要となる。その代表的なものとしては、先にあげた情報の保護のほかにも、ユーザ認証、ネットワークの制御、アクセスの監視等々がある。

これらの指定は多岐にわたる上、情報の保護についての要件指定に見られるように対象が相当数になるものもあり、これらの指定に不備がないようにすることも容易ではない。また、組織やシステムの運営環境の変化に合わせ、必要となる指定の変更を迅速かつ適切に行うことも容易ではない。

このため、要件の定義が必要なもののすべてに対し、これらを的確に指定しきれているシステムは少ないと見られている。

(4)セキュリティ要件のシステムへの組込みについての問題点

セキュリティ要件が適切に決められていても、セキュリティ要件のシステムへの組込みが的確でなければ、セキュリティ対策が期待通りに機能しない。通信の制御のためのファイアウォール他に

おけるさまざま設定、ファイルへのアクセス制御を行うための DBMS へのさまざまな設定等、個々のサーバにおける管理者権限の設定やポートの管理等、システムへのセキュリティ対策にかかる実装もシステム上の多くの場所に多くが要求されるため、これらをすべて万全に行うためには相当の努力を必要とする。

これらのセキュリティに関わる実装の点検等に徹底を欠き、これらについての不備が見過ごされ、セキュリティ事故を招いている例も少なくない。

(5)セキュリティ要求事項のシステムの運営への反映についての問題点

アクセスログやバックアップファイルの取得や保管、不正アクセスのチェック等、セキュリティ対策がシステムの運用に求めていることも少なくない。これらが適切に行われるためには、セキュリティ対策がシステムの運用に求めていることが明確にされるとともに、その実行が適切に行われるようにするための管理の仕組みを確立していることも必要となる。

この点についても、多くのシステムでは改善が必要と見られる。

(6)セキュリティ要求事項の業務の仕組みや業務の運営への反映についての問題点

個人情報の取扱いや、電子商取引における関係法の遵守等、業務の運営においても情報の取扱いにかかわる要求が少なくない。これらについて不手際を起こさないようにするためには、業務の仕組みや業務現場における業務の運営に、情報セキュリティにかかる要求が適切に反映されていなければならない。個人情報の漏洩等の事故が相次ぐのも、この点についての対応が不十分であることを示している。

(7)セキュリティ事故への備えについての問題点

セキュリティ対策に万全はありえず、なにがしかのセキュリティ事故は防ぎ得ないとすると、攻撃等を許すことがあっても、事故発生の早期発見、被害拡大の阻止、原因の追求と再発防止ができるようにしておくことが必要となる。

このためには、発生した異常に即応できる仕組みや体制の確立、被害状況の把握と被害からの回復手段の組込み、原因の究明と再発防止策の展開の仕組みの確立等も必要となる。

セキュリティ事故の予防に注力するシステムは多いいが、事故への備えについて十分な検討がなされているシステムは、それほど多くないみられている。これは、これまでセキュリティ対策の焦点がセキュリティ事故の予防に向けられていたことと、セキュリティ事故への備えは、対象業務の特性やシステムの作りによって千差万別となるため適切なガイドが与えられていないことにもよる。ISO/IEC17799 の改定作業では、この点の強化が取り上げられている。

(8)外部からの攻撃以外の内的脅威への対応についての問題点

最近における個人情報漏洩事故の多くは、内部の者の関与と見られている。セキュリティ対策は、つい、技術面についての課題中心に検討されることや、業務運営や組織の管理面の問題については文書管理他で従来からの取組みもあることで、セキュリティ対策の中では比較的比重が軽いように見える。しかし、個人情報保護法の制定や社会の見る目が厳しくなってきた今日では、この点についてのさらなる強化が必要となってきた。

1.3. 問題点の背景

情報セキュリティは、必要な技術の適切な使用、セキュアなシステムの維持管理、関連するシステムや業務の適切な運用、およびシステムや業務の運用に関与する人の管理の総合力で決まるものである。このため、セキュリティ対策は、システムの構築やその維持管理および運用、業務の運営、組織の管理の異なる分野に、お互いに関連する多くの施策が必要になるため、組織的で戦略的な取組みがなければ機能しない。

多くのシステムにおいて、セキュリティ対策の実施において、計画の不備や、計画したセキュリティ対策のシステムや業務運営への展開の不備、実行管理の不徹底、関係者の意識の不足等の 1.2 節に示すような多くの問題点を抱えている原因としては、情報セキュリティについての意識の不足や、対策の展開に欠かせないマネジメントやスキルの不足から、情報セキュリティについて取組みが組織的かつ戦略的になっていないことがあげられる。

情報セキュリティへの取組みを組織的で戦略的なものにするためには、対象システムにおけるリスクについての経営レベルでの評価にもとづく情報セキュリティへの取組みについての経営レベルでの指針にもとづき、必要な情報セキュリティ確保のため“具体的に何をどこまで行うのか”が組織的に決められ、システムの作りやその運用および関係する業務のプロセスやその運用への展開が適切に管理されるようになっていなければならない。また、計画したセキュリティ対策や、その実施状況が対象システムのセキュリティ特性に照らし十分かどうかのチェックも常にできていなければならない。

多くのシステムが、セキュリティ対策をなかなか組織的で戦略的なものにできない背景としては、以下があげられる。

- リスク分析の難しさ
- セキュリティ対策の検討の難しさ
- 計画したセキュリティ対策の展開の難しさ
- セキュリティ対策の十分性についての評価の難しさ

(1)リスク分析の難しさ

リスク分析の難しさは、システムの作りにより脅威の影響が大きく異なってくること、事故の発生確率や被害の大きさについての定量的な把握が困難であること、必要最小限の努力で適切なリスク分析を実現するための実務的な分析評価の技法が確立していないことも、その背景の一つにあげることができる。

(2)セキュリティ対策の検討の難しさ

システムに要求される情報セキュリティが確保されるためには、まず、セキュリティ対策の具体策が、対象とする業務とその運営形態やシステム構成の特性に対し適切なものとして計画され(決められ)なければならない。しかし、セキュリティ対策として、“具体的に何を、どこまで行うのか”を、対象とする業務やシステムの構成やその運用の特性、さらにはリスクの評価にもとづく情報セキュリティについての経営指針であるセキュリティポリシー等に照らし適切なものとして計画することは容易ではない。

セキュリティ対策の計画は、必要なセキュリティ技術の使用を含むシステムの構築と運営、組織および業務の運営といった多岐の分野に要求されるさまざまな施策を、施策相互間のバランスをとりつつ、要求されるセキュリティのレベルや、組織の実行能力を勘案しながら決めなければならないところに、その難しさがある。

セキュリティ対策の実施には、一つの要求に対し多くの選択肢（手段）が存在するため、どのような選択をするかを適切に判断するところにその難しさがあるが、何をもってこれで十分と判断すればいいかの尺度がはっきりしないところも、その難しさを大きくしている考えられる。

(3)計画の展開の難しさ

また、セキュリティが適切に計画されていても、それらがシステムの作りやその運用、さらには業務のプロセスや業務現場での業務の運用や、職場の内外における関係者の諸活動に的確に反映されていなければ、セキュリティ対策は期待通り機能しない。計画したセキュリティ対策の展開は、多岐に渡る技術の実装や、業務やシステムの運用あるいは職場内外における関係者の日々の活動に依存するところも多いいため、実装の確認や対策現場での要求の確実なを追求するための管理が必要となる。しかし、これらは実行上の負担も大きく徹底が難しく不備や不手際が見逃されたままになることが多い。

この計画の展開の難しさも、セキュリティ対策を実施上の大きな困難となっている。

(4)セキュリティ対策の十分性の評価の難しさ

セキュリティ対策は、対象システムのリスクに応じた経営が求めるレベルのものでなければならない。実施しているセキュリティ対策の現状が、この期待に対して応えているものかどうかの評価がある程度客観的にできなければ、実施しているセキュリティ対策の過不足を把握することができない。このような状況では、不備が見逃されたり、部分的に不必要な過対策を実施したりすることになる。

セキュリティ対策の実践には、このような難しさがあるにもかかわらず、リスクの分析と評価、セキュリティ対策として具体的に何をどこまで行うのかを決めるセキュリティ対策の計画作成と、作成した計画の十分性の評価、計画されたセキュリティ対策のシステムや業務への展開、実施中のセキュリティ対策の現状の評価等についてのさまざまなシステムで広く使える適切な実務ガイドが与えられていないのが現状である。

情報セキュリティに関してはセキュリティ評価基準(CC：ISO/IEC15408)や情報セキュリティマネジメントシステム(ISMS：ISOIEC17799)等の国際標準もこれらについてのガイドの一つとしてあげることができる。

しかしながら、セキュリティ評価基準(CC)は運用が含まれていない IT プロダクトを対象としたもので、ITプロダクトへのセキュリティの作りこみや評価のポイントを示しているセキュリティ機能要件や、システムへのセキュリティの作りこみの確認についての手法は、組織の情報セキュリティにおける対策要件の指定や、システムへの対策要求の組込みについては参考にできるものの、日々のシステムや業務の運用が大きくかかわるシステム全体のセキュリティ対策の計画の作成やその展開についての実務的なガイドにはなりえない。

また、情報セキュリティマネジメントシステム(ISMS)は、組織における情報セキュリティの確保のために取組まなければならないことは示しているものの、その要求に応えるための具体策までは示

しておらず、要求に応えるための具体策の検討は、この標準を適用する側に任されており、これらの要求に応えるための具体策の検討とその対策現場に展開を、どうすればいいのかが個々が対策現場の大きな悩みとなっている。

1.4. 必要な取組み

社会全体における情報セキュリティの向上のためには、対象業務の軽重やその規模の大小にかかわらず、ネットにつながるシステムのほとんどすべてが、情報セキュリティマネジメントシステム(ISMS)が求めることを実践することが必要となる。これまでの分析から、このことを実現するためには以下に示すような取組みが必要であると言える。

- 実務的で効果的なリスク分析のガイドの提供
- ISMS の要求を実践に移すための実務的なガイドの提供
- 実施しているセキュリティ対策のレベルを評価するための手段ならびに尺度の提供

(1)実務的で効果的なリスク分析のガイドの提供

リスク分析の手法については、既にさまざまな手法が提供されており、現実に使われてはいるものの、リスク分析は対象とする業務の正確やシステムあるいは組織の運営形態によって千差万別となるため、これらをカバーしようとするためか、これらは非常に重いものになっていて、リスク分析に大きな手間やコストをさくことができない小規模の組織においてはなかなか適用しづらいものとなっている。

手間やコストをそんなにかけずとも、もっと効果的なリスク分析を実施するための手法の開発と適用ガイドの提供が必要であろう。特に、小規模なシステムにおいても、その組織の能力に応じ、必要なリスク分析に挑戦できるようにするための、簡易ガイドの提供も不可欠であろう。

(2)ISMS の要求を実践に移すための実務的なガイドの提供

ISMS の要求を実践に移すための実務的なガイドとは、セキュリティ対策の責任者他の関係者に、対象システムに対するリスク評価や経営からの要求によって決まる情報セキュリティについての要求に応えるための具体的な施策を、対象システムがサポートしている業務や、システムの作りやその運用、関係部門における業務の運営形態に照らし適切なものとして決め、それらがシステムや業務の運営に的確に反映されるようにするために必要な仕組み作りを行うことを、実務に即した形で支援できるものでなければならない。

情報セキュリティマネジメントシステム(ISMS)の要求を実践に移すための実務的なガイドとしては、以下のような要件をそなえているものと考える。

- セキュリティ対策として検討すべきことが、すべて網羅されていること
- セキュリティ対策として、“具体的に何を、どのように行うのか”が具体的に示されていること
- 対象システムの適用業務、システムの作りや規模、運営組織の特性等にかかわらず、すべてのシステムに適用できること
- 適用に特別のスキルを必要とせず、IT システムやセキュリティの専門家でなくても、これらに

ついてのある程度の知識があれば使いこなせ、その適用にあたって多大の手間やコストを必要としないこと

- 実施しているセキュリティ対策が計画されたことを的確に反映しているかどうかのチェックにも使えること

最後の項目は、セキュリティ対策が実施レベルの不手際を見過ごさないようにすることを支援するためのもので、せっかくの計画を活かすためにも欠かせないものである。

(3)実施しているセキュリティ対策のレベルを評価するための手段ならびに尺度の提供

また、経営としては、自社のセキュリティ対策が適切かどうかについての判断を行えるようになることも期待するところであろう。計画したセキュリティ対策が適切かどうかについての判断は、一般には以下のような視点になると考える。

- 対象システムのリスクに見合った強度を維持しているか？
- 他社における類似システムの水準に比べ問題ないか？

最初の問題は、計画したセキュリティ対策が、経営が求めることを実現してくれるものかどうかについての評価であり、個々の対策要求についての実施している対策の強度の総和で決まる全体としてのセキュリティ対策の強度が、想定するリスクに対応し、経営に期待に応えるレベルかどうかの評価である。

また、後者は、自分の判断を他の事例から再評価するだけでなく、何か問題が生じ世間水準の管理が行われたかどうかが問題になったときの備えとしても必要となる。

これらのことから、セキュリティ対策については、その強度について絶対的な評価は無理としても、評価リスクとの対比、および類似システムの対策レベルでの比較はできるようになることも望まれていると考える。

2. セキュリティ対策評価モデルのコンセプト

セキュリティ対策評価モデルとは、対策現場の悩みであるセキュリティ対策の実践をガイドするとともに、セキュリティ対策の現状の十分性についての客観的な評価も支援するものとして、

- セキュリティ対策として“何を、何処まで”行うべきかを適切に決める時の判断材料
- 計画したセキュリティ対策、あるいは実施しているセキュリティ対策の強度をある程度の確度で評価できるような尺度
- 実施しているセキュリティ対策が、同種のシステムにおける平均的な対策と相対的な比較をするための目安

を提供しようするものである。

本節では、この評価モデルのコンセプトを紹介する。

2.1. セキュリティ対策評価モデルのコンセプト

セキュリティ対策は、対象システムにおけるセキュリティに関する要求を実現するための、技術的な対策だけでなく、施設や設備の保護、業務やシステムの運用関係者に対する業務の遂行やオフィス他での行動に対する指導、管理と広い範囲にわたるさまざまな施策の集合体である。

そして、実施が要求される具体策のそれぞれには、実施の手段や厳格さについてさまざまな選択肢がある。セキュリティ対策の実効性についての期待度と言えるセキュリティ対策の強度は、対象システムのセキュリティ環境の特性によって千差万別となるこれらの選択の組み合わせによって決まる。

また、セキュリティ対策の実施については、実施対象の網羅性という概念も存在する。これは、セキュリティ対策においては、OS に対するセキュリティパッチの実施、情報の保護において必要となる保護要件の指定やアクセス制御の実施、アプリケーションソフトの脆弱性検査の実施等の例に見られるように、実施の対象が複数になるものがあるが、これらの対策要求については、すべての対策対象に同じ対策が要求されるわけではない。また、対策の実施に漏れが生じることも少なくない。このような対策要求については、対策が全体のどのような形で行き渡っているかどうかについての網羅性が問題となる。

図 2-1 は、セキュリティ対策を決めるこの 3 つの要素を示している。

横軸の要求対策軸（p）は、セキュリティ対策として実施が要求されることを並べたものである。また、縦軸の対策強度軸（r）は、個々の対策要求に対して存在する実施方法によって決まる当該対策要求に対する対策に対する信頼度または期待度ともいえる強度である。また、奥行きである網羅軸（c）は、先にあげた対策対象が複数にわたるような場合における、対策対象の適用状況（網羅性）示すものである。セキュリティ対策の全体は、これらを軸にした 3 次元の柱の集合と考えることができる。

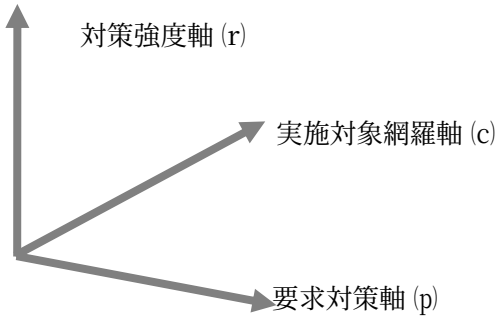

図 2-1 セキュリティ対策 3 要素

このことより、セキュリティ対策の計画とは、セキュリティ対策としてなすべき事項のそれぞれにについて、対策対象としないという適用除外も含めて、実施の方法についての選択肢の選択問題であると考えることができる。そして、その選択にあたっては、当該対策要求について求められる対策強度、すなわち実施する対策について期待する概念的な信頼度が判断基準とされていると見ることができる。また、セキュリティ対策の評価は、絶対的な評価が難しいため、セキュリティ対策が要求されるレベルに達しているかどうかという相対的な評価となろう。

実システムのセキュリティ対策の全体像は、システムによって千差万別となるものの、セキュリティ対策として実施を検討すべきこと（以降、“対策要求”と呼ぶ）のリストと、その個々における実施上の選択肢と、選択肢の組合せによって決まる対策強度の概念は、対象システムのセキュリティ環境の特性に関係ないため、標準的に示すことが可能となる。

このため、セキュリティ対策を対策現場への具体的要求に展開したものと、そのそれぞれについての実施方法についての選択肢を示したものは、それだけで対策現場における具体策の検討を助けるガイドとなる。

さらに、これらの選択肢の選択を助けるものとして、選択肢の選択の組合せを当該対策要求についての対策強度別に示しておけば、当該対策事項についてベースとしたい強度から、当該対策事項についての選択肢の選択基準が与えられることになる。このことは、対策現場に個々の対策事項について“どこまでやるか”を決めるときの判断材料を与えることになる。

また、評価の対象となるシステムに対し、セキュリティ要求事項ごとに要求する強度レベルが示されていれば、個々の要求事項ごとに、指定された強度レベルの達成条件として指定されている対策内容と、計画した対策や対策の現状を比較することも比較的容易である。この方法を用いれば、対策に過不足がある箇所を知ることができるだけでなく、必要な是正措置についても具体的に知ることができる。このため、セキュリティ対策を対策現場への具体的要求に展開したものと、そのそれぞれについての実施方法についての選択肢を示したものは、それだけで対策現場における具体策の検討をガイドするものとなる。

さらに、対策要求事項の個々に指定されている個々の対策強度に指定されている選択肢の選択条件をチェックリストに、現状のチェックを行うことにより計画と現状のギャップを知ることも可能となる。

セキュリティ対策評価モデルは、セキュリティ対策の検討を構成する要素についてのこのような点に着目し、セキュリティ要求事項の個々に対し、強度レベルを判定する基準を与えることで、セキュリティ対策の計画をガイドするだけでなく、計画自体や対策実施の現状を客観的に評価できるようにするもので、

- セキュリティ対策として実施すべき具体策（以降、“対策要求”と呼ぶ）のリスト
- 個々の対策要求における複数の段階に分けた強度レベルの概念と、実施上の選択肢を対策強度とリンクして示す“個々の対策要求に対する強度判定基準”
- これらの利用法

を一つの体系として纏めたものである。

このモデルの概念と利用イメージを示すものである。

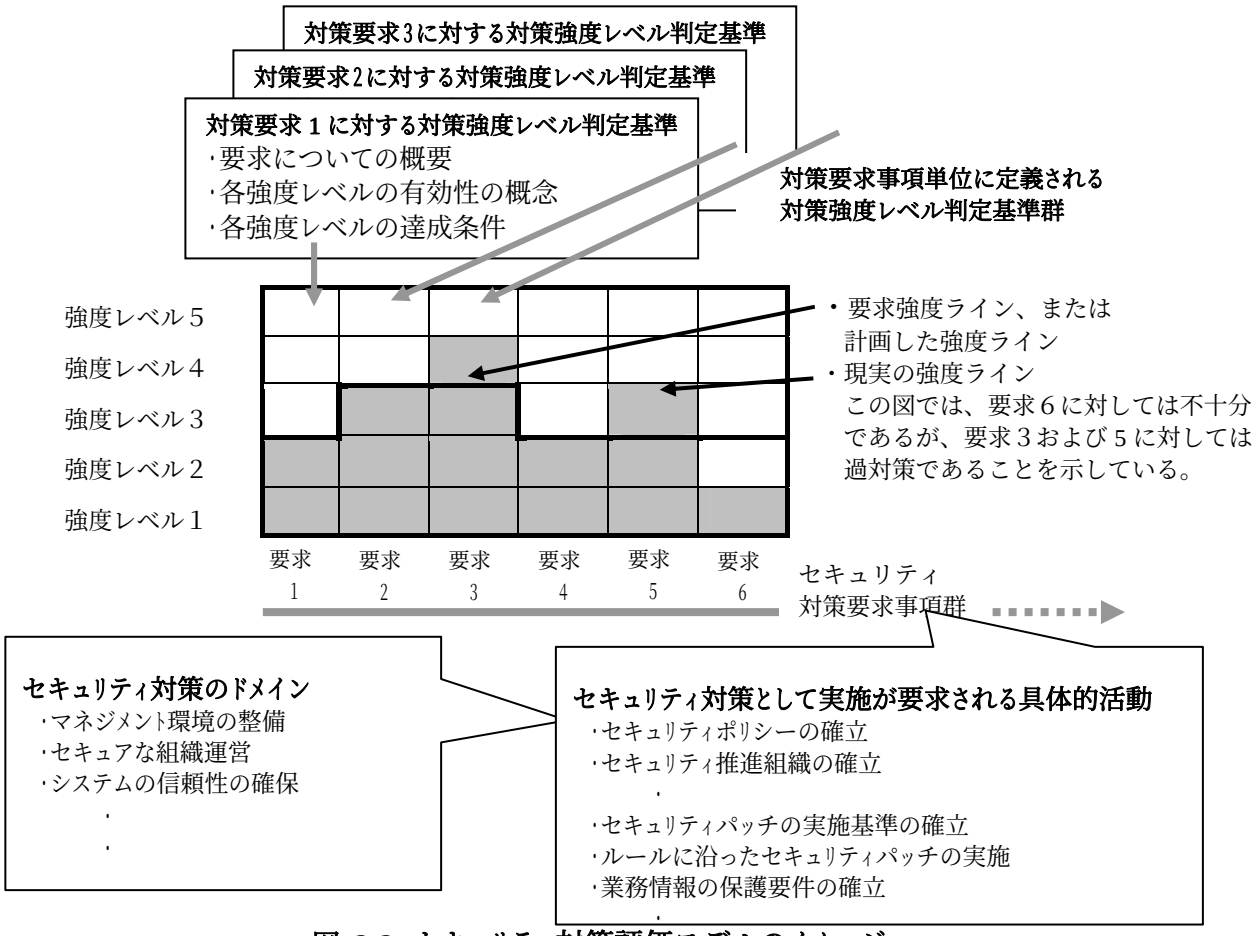

図 2-2 セキュリティ対策評価モデルのイメージ

セキュリティ対策の計画にあたっては、セキュリティ要求事項の個々に定義されている強度判定基準を参照して、当該システムに必要な強度レベルを決めれば、当該レベルの達成条件から、当該要求について実施すべき内容を具体的に知ることができる。また、セキュリティ対策の現状については、強度判定基準に示される該当レベルの達成条件の実現状況を確認することにより、目標レベルに対する十分性や過不足の箇所を把握できることになる。

2.2. 本モデルの特徴

このようなセキュリティ対策の評価モデルは、セキュリティの構築にあたって考慮すべき事項を示したにとどまっている国際基準 ISO/IEC17799（JISX5080）等に比べて、以下のような特長を持つ。

- 対象業務やシステム構成の特徴や規模等のセキュリティ環境の特性や、経営からのセキュリティについての要求に依存せず、すべてのシステムに適用できる
- 対象とするシステムのセキュリティ環境の特性に応じ、セキュリティ対策として実施が求められることについての把握に漏れがでないようにすることができる
- 対象とするシステムにおけるセキュリティ面からの要求に最適な計画を作成することが容易となる
- 計画したセキュリティ対策やセキュリティ対策の現状についての評価を属人的なものからより客観的なものにできる
- セキュリティ対策の現状の要求あるいは計画に対する過不足を具体的に知ることができる
- 要求事項相互間のバランスチェックも可能となる

2.3. 本評価モデルの構成

本評価モデルは、図 2-3 に示すように以下の 4 つの要素で構成される。

評価モデルのコンセプトは、このモデルの概要を理解してもらうことを目的に、その狙い、セキュリティ対策の実務展開と対策の評価のガイドのありよう、全体の組立て、適用範囲、その使い方のイメージを説明するもので、本報告書における本章に相当する。

また、対策要求のリストは、この評価モデルの基盤となっている対策現場に実施を求める具体策を体系的に示すものである。セキュリティ対策として実施すべき活動を具体的に示していること、ならびにこれらが、第 3 章に示すような新しい考えのもとでの体系に纏められているところに特徴がある。

また、個々の対策要求に対する対策強度レベル判定基準は、対策要求の個々に対し、実施上の選択肢を当該対策についての対策強度のレベルにリンクして示したものの集合である。その詳細については、第 4 章を参照されたい。

本モデルの利用法は、この対策評価モデルをセキュリティ対策の計画立案のガイドとして用いる場合や、実施しているセキュリティ対策の十分性についての評価に用いる場合の進め方を示すものである。この利用ガイドの検討は、来年度作業に予定している。

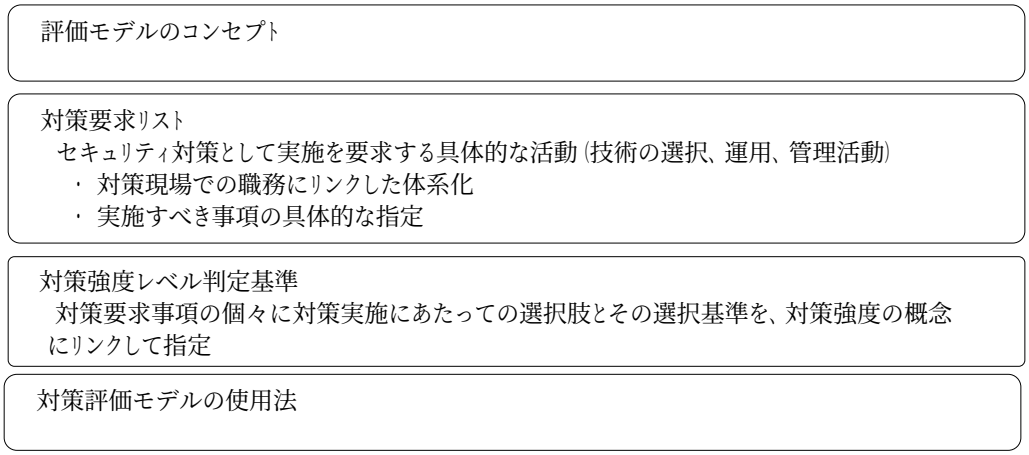

図 2-3 本評価モデルの構成

2.4. 評価モデルが対象とするセキュリティ対策の領域

セキュリティ対策の方法論の一つとしてのこの本評価モデルの適用対象領域については、セキュリティ対策が及ぶ物理的な領域と、セキュリティ対策がカバーしようとしていることの範囲を示す論理的な領域がある。

2.4.1. 物理的な対象領域

本評価モデルの物理的な対象領域は、情報システムの利用を前提とした一つの組織体とする。ここで言う組織体とは、図 2-4 に示すように、情報システムとその運用組織、情報システムを活用している職場等の組織および人等の情報セキュリティに何らかの影響を及ぼすもののすべてとする。したがって、運用を伴わないブラックボックス化した単体としてのシステムや装置の個々についてのセキュリティ問題は、この評価モデルの対象ではない。

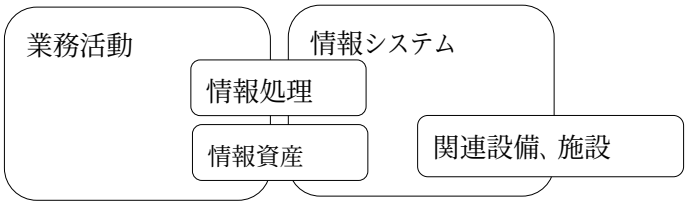

図 2-4 評価モデルの物理的な対象領域

評価モデル適用の対象としてのシステムは、セキュリティ対策の実施を一体として考えることができる範囲であれば、適用する側が自由に特定することができる。全社を一つの対象とすることも、現実の組織やシステムの作りにあわせ、いくつかの領域に分けて個別の適用対象とすることもできる。

セキュリティについての要求レベルが異なるものを一体として考えるのは、問題を複雑にするだけでなく、セキュリティ対策に冗長なところをもたらすことになるため、企業内のシステムのセキュリティ問題を独立に実施することができるいくつかの領域（セキュリティセグメント）に分けて、そのそれぞれについて計画することが望ましい。ただし、セキュリティ対策を別途に考える他の領域との関係において、セキュリティ面での境界が明確で、他のセキュリティセグメントから業務管理的にもシステム的にも切り離して考えることができるようになっていなければならない。他のセキュリティセグメントとのやり取りは、当然あるとしても、これらは当該セキュリティセグメントの外部ファクタとして考えることができるようになっていなければならない。

2.4.2. 論理的な対象領域

本評価モデルが適用の対象として前提としているセキュリティ対策は以下の範囲を言う。

まず、セキュリティ対策が目指す情報セキュリティとは、“企業･機関等の組織において、情報の取扱いにおいてトラブルが生じないようにすること”と定義し、そして、セキュリティ対策とは、“情報システムの利用あるいはその運用、および業務現場他の組織内および関連場所における情報の取扱いにおける安全と信頼を確保すること”と定義する。このため、本モデルにおけるセキュリティ対策して考える範囲は、以下とした。

- 情報および情報処理の正確性の確保
- 情報の秘匿性の確保
- 情報システムに求められる可用性の確保
- 情報システムの不正使用に防止
- 情報の取り扱いにおけるルール違反の防止
- 他サイト攻撃への加担の回避
- セキュリティ事故発生時における被害拡大の阻止

本対策評価モデルにおいては、これらを情報セキュリティのテーマ、すなわち情報セキュリティが目指すところとした。

その個々についての考え方に関しては、3.2.2.1 節参照。

3. 評価事項の組立て

3.1. 対策要求の組立てについての考え方

このような評価モデルが有効に機能するためには、まず、セキュリティ対策として実施を要求すること（対策要求）が適切にあげられていなければならない。本評価モデルにおける対策要求事項のリストアップは、以下の方針に沿って行われた。

- 対策要求は、対策現場に求める活動を具体的に示していること
- 対策として必要なことが漏れていないこと、特に、ISMS の要求は完全にカバーすること
- 要求事項は対策実施現場の実務に即して体系化されていること
- あまりに細かくなりすぎず、現場での適用が可能な数に止めること

セキュリティ対策として実施が要求されることを対策現場へ具体的に示すためには、求める活動を具体的に示さなければならない。このため、本評価モデルにおける対策要求は、対策が実現したい状態を作り出すために必要となる活動を具体的に示すようにした。実現したい状況とは、活動の狙いあるいは結果と言う。また、多くの異なる性格の活動を多く含むような抽象的な要求はしないよう、実施に責任を持つ者あるいは実際に担当する者に、実施すべきことが明確で、かつ、一つの管理の単位となるようにするにした。ただし、個々の活動が単純なものについては、一つの目的（実現したい状態の確保）を達成するための一連の活動を一つの要求に纏めた。

また、要求事項のリストから、必要なことが漏れてはならない。このため、2.4 節にあげた本評価モデルが対象としているセキュリティ対策の範囲をすべて含むようにすることはもちろんのこととして、ISMS の要求は完全にカバーするようにした。

要求事項はできるだけ職務にリンクしたものになるように努めた。これは、職務の異なる者がそれぞれに行うべきことを一体として要求した場合、その責任者が自分の責務があいまいならないようにするためのものである。

要求事項を対策現場の職務の体系に合わせるようにする工夫や、要求を適切な数に押さえる工夫は、この評価モデルの実用性を高めるため、対策現場が要求を受け入れ易くするためのものである。

3.2. 対策要求へのブレークダウン

3.2.1. 対策要求へのブレークダウンのアプローチ

要求事項の組み立ては、前節に示し方針に沿って、以下のような手順で行った。

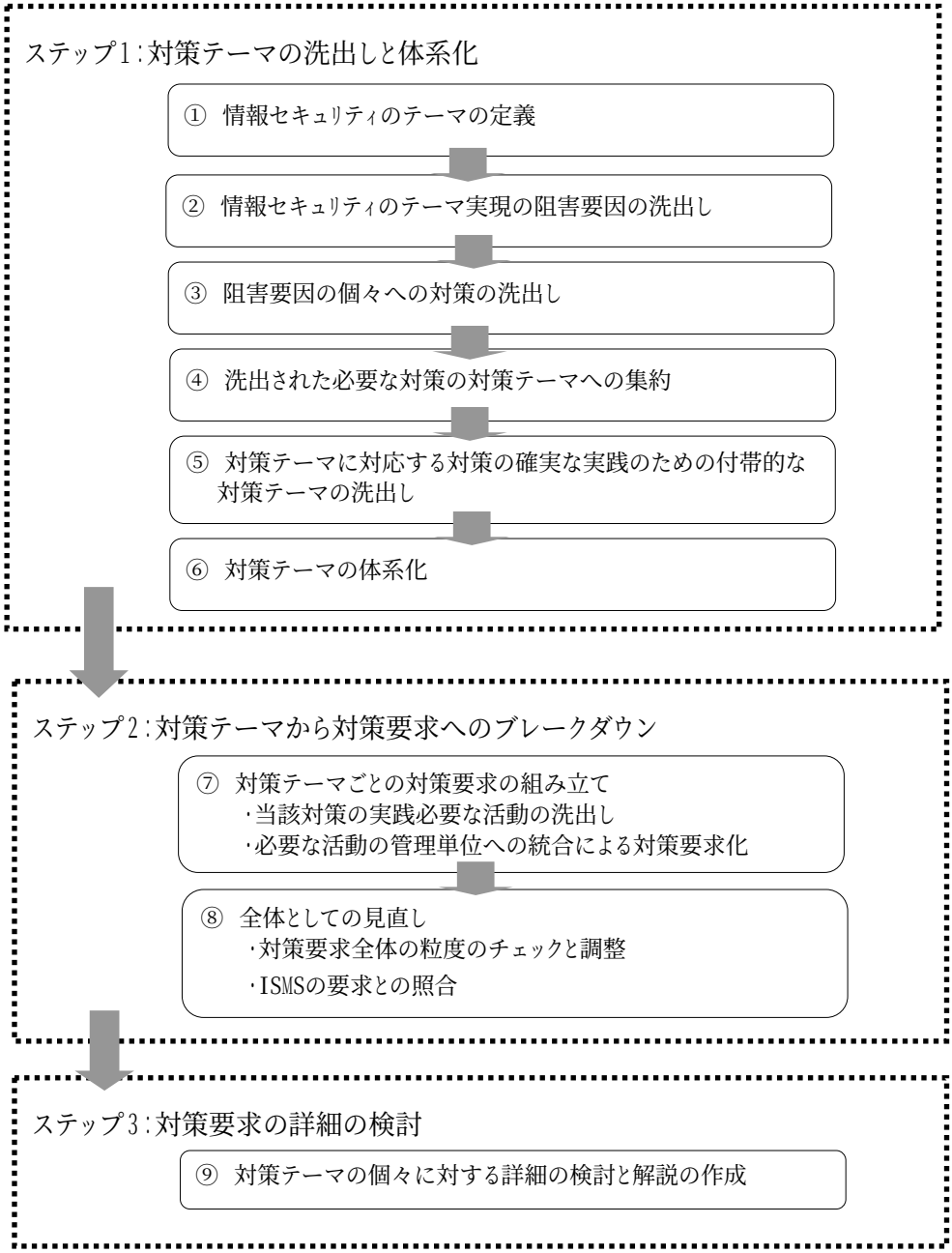

図 3-1 対策要求へのブレークダウンのアプローチ

3.2.2. ステップ 1：対策テーマの洗出しと体系化

3.2.2.1. 情報セキュリティのテーマの定義

セキュリティ対策を論じるためには、まず、情報セキュリティとは何で、何を実現しなければならないのかを定義しなければならない。本モデルの開発においては、情報セキュリティを、“情報システムの利用あるいは運用、および情報の取り扱いにおいてトラブルをこと、すなはち、その安全と信頼を確保すること”と定義とした。

ここで言う、情報システムの利用あるいは運用、および情報の取り扱いにおける安全と信頼とは、以下を実現することを言う。

- 情報の秘匿性の確保
- 情報および情報処理の正確性の確保
- 情報システムに求められる可用性の確保
- 情報システムや情報の不正な使用の防止
- 情報の取り扱いにおけるルール違反の防止
- セキュリティ事故発生時における被害拡大の防止
- 他社サイト攻撃への加担の防止

これらが、情報セキュリティの目指すところ、すなはち情報セキュリティのテーマとなる。

⑴ 情報の秘匿性の確保

組織内が保有している情報について、その情報を見ることが許されていない者に開示することがないようにすることである。組織が取扱う情報は、システム上、外部メモリ等の電磁媒体上、通信路上、印刷物等のさまざまな場所に、さまざまな形態で保有・管理されているため、これらのすべてについて必要な秘匿性を確保することは容易ではない。

また、情報の保護の前提となる情報へのアクセス権限者の管理も容易ではない。

⑵ 情報および情報処理の正確性の確保

情報および情報処理の正確性の確保とは、業務で取扱われる情報やシステムが保有する情報やその処理結果が常に正確なものであるようにすることであり、このことを実現するためには、情報および情報処理の正確性を損ねることにつながる以下のようなことがないようにしなければならない。

- 不正な入力に対する処理の実行
- 業務ソフトの不具合等による、本来あるべき結果と異なる結果を生むようなシステムの誤処理
- 入力ミスや処理すべき情報の紛失等、業務上の後処理やシステムの処理が不正な結果を生むような業務上での情報の取扱い上のミス
- システム運用上のミス等による業務情報が格納されているファイルの破壊や改ざん
- 外部からのシステムへの侵入によるシステムが保有する情報の改ざんや破壊
- 内部関係者によるシステムが保有する情報の改ざんや破壊

⑶ 情報システムに求められる可用性の確保

情報システムは、対象業務の要求に応じ、必要とされる時はいつでも、円滑に使用できなければならない。可用性の要求はシステムにより千差万別となるが、求められる可用性を確保するためには、情報システムに求められる可用性を損ねる原因となる以下のようなことに対する対策ができていなければならない。

- 構成機器等に故障等のトラブルの発生
- 性能面でのオーバーフローの発生
- 外部からの攻撃によるシステムの混乱
- 内部の関係者の犯行あるいは運用の不手際によるシステム運用の混乱

⑷ 情報システムや情報の不正な使用の防止

情報システムが提供するサービスには、当該サービスを受ける資格の者だけに提供されなければならないものもある。資格のない者へのこのようなサービスの提供は、さまざまなトラブルを誘起する。

⑸ 情報の取扱いにおけるルール違反の防止

サービスの提供や組織の業務の遂行にあたっては、システムの個人上の保護や電子商取引に関連する法律等で規制されていることに違反があったり、他社との契約で規制されていることに違反がないようにしなければならない。情報の取得、開示等の情報の取り扱いにおいて、これらへの違反を起こさないようにすることも、情報セキュリティのテーマの一つである。

⑹ セキュリティ事故発生時における被害拡大の防止

ウイルスの侵入等により、知らない間に自社サイトが他社サイトの攻撃に加担しているケースは多い。セキュリティ対策は自社のシステムや業務を守るだけでなく、他社に迷惑を欠けないようすることも、情報セキュリティにテーマの一つである。

⑺ 他社サイト攻撃への加担の防止

新しい攻撃手段の提供やプラットフォームにおける新たな脆弱性の発見等、新たな脅威が次々に発生したり、セキュリティ対策の欠陥を皆無することもそう期待できないことから、セキュリティ対策に万全を期待することはとはできない。このため、トラブルの防止だけでなく、セキュリティ事故に見舞われるような事態の発生に際しては、被害の拡大防止だけでなく、原因の追求や再発防止策の迅速な展開ができるようにするための備えも重要となる。セキュリティ事故に対する備えの重要性を強調する意味でも、本評価モデルでは、このセキュリティ事故への備えも、セキュイティ対策の独立テーマとした。

3.2.2.2. 情報セキュリティ実現の阻害要因の洗出し

3.2.2.1 節に示した情報セキュリティのテーマの実現を阻害する要因の洗出しは、問題の原点（脅威の根源）となる外的な脅威や組織やシステムの脆弱性等をあげ、これらの一つ一つが、どのような形で 3.2.2.1 節に示した情報セキュリティのテーマへの現実的な脅威となるかの分析を行った。セキュリティ対策は、その存在自体を拒否することはできないものの、これらが現実の脅威となることを防ぐことにある。問題の原点となる外的な脅威や組織やシステムの脆弱性として、表 3-1 に示すものをあげた。

表 3-1 情報セキュリティに対する問題の原点（脅威の根源）

問題区分		対策の対象となる問題
悪意の者の存在		関係者による犯行
		外部の者の施設や設備への不正なアクセス
		外部の者によるネットを介したシステムへの工作
組織やシステムの問題	業務面での問題	業務仕様の欠陥
		業務運用面での不手際
		他社との業務連携や他社への業務委託での問題
	IT システム周りの問題	システムの欠陥
		システム運用上の不手際
その他		災害やセ設備やシステム機器の故障

この分析結果を、表 3-2 に示す。

3.2.2.3. 阻害要因の個々への対策の洗出し

セキュリティ対策は、このような問題を封じるために実施すべき活動であり、情報セキュリティへの脅威の分析から、それらの脅威の現実化を防ぐために必要となる施策として浮かび上がってくるセキュリティ対策を、表 3-2 に併せて示す。

3.2.2.4. 洗出された必要な対策の対策テーマへの集約

一つの対策は、複数の脅威の防止にかかわるものが少なくない。表 3-2 は、脅威の根源ごとの情報セキュリティを損なう要因をあげ、それぞれに対応して必要な予防策等の対策を示しているので、一つの対策が複数の場所であげられている。これを再整理し、セキュリティ対策のテーマとして体系化すると、表**のようになる。

この表に示される対策テーマが、実施すべきセキュリティ対策のコアとなる。

表 3-2 情報セキュリティのテーマ実現の阻害要素

問題の原点 (根源的脅威)	情報セキュリティへの具体的な脅威	脅威が影響する情報セキュリティのテーマ								必要な対策(脅威の現実化の防止)
		A 正確性の確保	B 秘匿性の確保	C 可用性の確保	D 不正使用防止	E ルール違反防止	F 有効性の確保	G 他社攻撃回避	H 影響拡大防止	
関係者の犯行	・業務上の権限を悪用した不正行為の実行	●	●	●	●	●	●	●		・信用をおけない者の関係者からの排除 ・関係者の行動の制約と違反行為の牽制 ・保護領域の設置と保護領域に対する立入りの制限と保護領域内における行動の制限の実施 ・システム資産や情報資産がかかわる機器や媒体等についての物理的な保護策の実施 ・アクセス権限者へのなりすましの防止 ・内部ネットワークからのシステムへ不正なアクセスの試みの阻止 ・通信に対する否認への対抗措置の準備 ・ソフトウェアの開発管理の徹底(有害プログラムの組込みの阻止) ・業務現場におけるクリーンデスク、クリーンスクリーンの追求 ・印刷物の適切な取扱いの追及 ・電磁媒体の適切な取扱いの追及 ・PC 等の情報機器の適切な取扱いの追及 ・情報が残る電子機器の使用についての適切な管理の実施
	・職務権限の異なるものへのなりすましによる不正行為の実行 ・内部からのシステムへの不正なアクセスによる不正行為の実行	●	●	●	●	●	●			
	・ソフトウェアへの工作	●	●	●	●	●	●	●		
	・コピー機等の電子機器に残された情報の不正な取得		●							
	・ソーシャルエンジニアリングによるアクセス権限外の情報の不正な取得		●							
	・保護対象情報が記録あるいは格納された印刷物や電磁媒体、電子機器の不正な持ち出し	●	●	●						
	・施設、設備、システム機器に対する破壊や持ち出し他の物理的な工作			●						
	・通信の否認						●			
外部の者の施設等への不正な立ち入り	・施設内にある情報等へのアクセスによる情報の不正な取得や操作 ・施設、設備、システム機器に対する破壊や持ち出し他の物理的な工作	●	●	●	●	●	●	●		・保護領域の設置と保護領域に対する立入りの制限と保護領域内における行動の制限の実施 ・システム資産や情報資産がかかわる機器や媒体等についての物理的な保護策の実施 ・アクセス権限者へのなりすましの防止 ・内部ネットワークからのシステムへ不正なアクセスの試みの阻止 ・業務現場におけるクリーンデスク、クリーンスクリーンの追求 ・印刷物の適切な取扱いの追及 ・電磁媒体の適切な取扱いの追及 ・PC 等の情報機器の適切な取扱いの追及 ・情報が残る電子機器の使用についての適切な管理の実施
	・内部からのシステムへの不正なアクセスによる不正行為の実行	●	●	●	●	●	●	●		
	・保護対象情報が記録あるいは格納された印刷物や電磁媒体、電子機器の不正な持ち出し		●	●						
外部の者のネットを介したシステムや通信への工作	・他の利用者へのなりすましによるサービスの不正な使用	●	●							・ユーザ管理の徹底
	・システムへの不正なアクセス	●	●	●	●	●	●			・内部ネットワークからのシステムへの不正なアクセスの試みの阻止 ・外部ネットワークからのシステムへの不正なアクセスの試みの阻止 ・システムへの不正アクセスの入口となる脆弱性の排除 －セキュリティホール対策の徹底 －通信制御機器から脆弱性の排除 －サーバからの脆弱性の排除 －LAN 上の PC からの脆弱性の排除 ・ウイルス対策の追求 ・システムへの不正アクセスの手がかりを与えるセキュリティ管理情報やシステム情報の保護の追及
	・ウイルスへの感染	●	●	●						・ウイルス対策の追求 －システムのウイルス感染の阻止 －外部へのウイルスの拡散の阻止 ・ウイルスに侵入の入口を与えるセキュリティホールに対する対策の追求
	通信の盗聴		●							・通信路上の情報に対する保護策の実施
	通信データの改ざん	●								
	・DoS 攻撃			●						・DoS 攻撃の影響の極小化

(注) セキュリティ事故の影響の拡大防止は、セキュリティ事故の備えの欠如が原因であり、根源的脅威は直接に関与するものではない。

表 3-2　情報セキュリティのテーマ実現の阻害要素（つづき）

問題の原点 （根源的脅威）	情報セキュリティへの具体的な脅威	脅威が影響する情報セキュリティのテーマ								必要な対策（脅威の現実化の防止）
		A 正確性の確保	B 秘匿性の確保	C 可用性の確保	D 不正使用防止	E ルール違反防止	F 有効性の確保	G 他社攻撃回避	H 影響拡大防止	
業務仕様の欠陥	・業務処理の正確性と言う点での業務仕様、業務処理要領の不備	●								・業務仕様の正確性の確保 ・業務仕様面でのコンプライアンスの確保
	・情報の取扱い面での業務仕様、業務処理要領の不備		●							
	・業務あるいは提供するサービスの利用者の管理面での業務仕様、業務処理要領の不備				●					
	・コンプライアンスという面での業務仕様、業務処理要領の不備					●				
	・長期保管の対象となる電子情報の扱いに関する業務仕様、業務処理要領の不備						●			
業務運用面での不手際	・業務現場における業務処理上の不手際 －業務現場における業務仕様や業務処理要領の理解不足 －業務処理上での業務仕様や業務処理要領の適用上での判断ミス －処理漏れ、入力ミス、記載ミス、計算ミス、処理結果の取扱い上の不注意によるミス	●	●	●	●	●	●			・業務現場での業務処理上の不手際の発生の防止 －業務処理上のミス －業務処理上のコンプライアンスにかかわる違反
	・ユーザの管理の不手際	●	●		●					・ユーザ管理の徹底
	・業務現場における情報あるいは物理的な情報資産のずさんな取扱い	●	●							・業務処理上での情報のずさんな取り扱いの防止 ・印刷物の適切な取扱いの追及 ・電磁媒体の適切な取扱いの追及 ・PC 等の情報機器の適切な取扱いの追及 ・情報が残る電子機器の使用についての適切な管理の実施
	長期保管する電子情報の取扱い上の不手際 －法的効力の維持が必要となる電子情報の取扱い上の不手際 －法的効力の維持が必要となる電子情報の取扱い上の不手際						●			・長期保管する電子情報の対する適切な保管措置の実施 ・長期保管する電子情報の対する適切な保管措置の実施
他社との連携や業務の外部委託での問題	・他社との業務連携における	●	●	●	●	●	●			・他社との業務コラボレーションにおける問題発生の防止 ・外部への業務委託における問題発生の防止
	・業務処理の委託先での業務処理上の不手際	●	●	●	●	●	●			
	・業務処理の委託先での情報の取扱い上の不手際		●	▲	●	●	●			
システムの利用面での不手際	・インターネットサービスの不注意な利用									・インターネットサービスの利用におけるセキュリティ対策
	・モバイルコンピューティングの不注意な利用									・モバイルコンピューティングの利用におけるセキュリティ対策
	・リモートオフィスにおけるセキュリティ対策の不備や不手際									・リモートオフィスにおけるセキュリティ対策の追求

（注）セキュリティ事故の影響の拡大防止は、セキュリティ事故の備えの欠如が原因であり、根源的脅威は直接に関与するものではない。

表 3-2　情報セキュリティのテーマ実現の阻害要素（つづき）

問題の原点 （根源的脅威）	情報セキュリティへの具体的な脅威	脅威が影響する情報セキュリティのテーマ								必要な対策（脅威の現実化の防止）
		A 正確性の確保	B 秘匿性の確保	C 可用性の確保	D 不正使用防止	E ルール違反防止	F 有効性の確保	G 他社攻撃回避	H 影響拡大防止	
システムの欠陥	・業務仕様のシステム化にあたっての不手際 　－システム化の要求の不備、業務システムの仕様上の欠陥、処理方式面での欠陥 　　プログラミング上の欠陥	●	●	●	●	●	●	●		・業務のシステム化仕様の的確性の確保 ・業務仕様の確実なシステム化の実現
	・システムの性能を上回る負荷の発生 （必要な性能の見極めの失敗、性能不足のシステムの構築、付加変動の監視の失敗）			●						・必要な性能の適切な見極め ・必要な性能を確保できるシステムの構築とその維持 ・日常的な性能管理の適切な実施
	・個々の業務システムにおけるアプリケーション上の脆弱性をついた攻撃	●	●	●	●	●	●	●		・業務ソフトへの必要なセキュリティ機能の組込み ・アプリケーションソフトからの脆弱性の排除 ・開発過程での有害プログラムの侵入の阻止
	・システムの構成機器に残された脆弱性をついた攻撃	●	●	●	●	●	●	●		・システムの構成機器からの脆弱性の排除 　－セキュリティホール対策の徹底 　－通信制御機器から脆弱性の排除 　－サーバからの脆弱性の排除 　－LAN 上の PC からの脆弱性の排除
	システム構成の管理上の不手際 　－システム構成の維持管理上の不手際 　－OS 等のプラットフォーム系ソフトの導入や更新における不手際 　－オフィスツール等の汎用業務系ソフトの導入や更新における不手際 　－個別業務ソフトの導入や更新における不手際									・堅牢なシステム構成の構築とその維持 ・ソフトウエアの的確な管理の追求 　－OS 等のプラットフォーム系ソフトの導入や更新における不手際の阻止 　－オフィスツール等の汎用業務系ソフトの導入や更新における不手際の阻止 　－個別業務ソフトの導入や更新における不手際の阻止
システム運用上の不手際	・運用環境の保全上の不手際 　－業務ソフトの誤用 　－業務データの誤用	●	●	●	●	●	●	●		・運用環境の保全の徹底 ・日々のシステム運用の正確な実行 ・セキュリティ対策にかかわシステム運用の確実な実行 ・システム運用委託先での的確なシステム運用の追及 ・法的効力の確保が必要な電子情報に対する必要な処置の的確な実施 ・長期保管電子情報に対する見読性確保に必要な処置の確実な実行 ・システムの可用性の要求に見合ったシステムのシステム機器障害への対応能力の確保
	・ジョブ実行上の不手際	●	●	●	●	●				
	・システム運用へのセキュリティ要求への対応の不手際		●		●					
	・システム運用の委託先でのシステム運用の不手際	●	●	●	●	●				
	・電子情報の法的効力の維持にかかる処理の不手際						●			
	・長期保管電子情報に対する見読性や法的効力の維持に必要な処理の不手際						●			
災害・故障	・システム機器や付帯設備の故障			●						
	・災害等によるシステム機器・関連設備・施設の破損			●						・災害の発生を考慮した配置や設置 ・必要に応じたバックアップ機の準備
	・災害等による情報格納媒体の破損			●						・災害等を考慮した保護対象物の保管 ・必要に応じたバックアップの確保

（注）セキュリティ事故の影響の拡大防止は、セキュリティ事故の備えの欠如が原因であり、根源的脅威は直接に関与するものではない。

表 3-3 脅威の分析から抽出されて脅威の現実化を防ぐための施策の対策ドメインへの集約

脅威の分析から抽出された脅威の現実化の防止に必要な施策	セキュリティ対策のドメイン
・信用のおけない者の関係者からの排除 ・関係者の行動の制約と違反行為の牽制	組織管理上でのセキュリティ対策
・業務仕様の的確性の確保 ・業務現場での業務処理上でのミスの発生の防止 ・他社との業務コラボレーションにおける問題発生の防止 ・外部への業務委託における問題発生の防止	業務運営上でのセキュリティ対策
・業務現場における情報のずさんな取り扱いの防止 ・クリーンデスク・クリーンスクリーンの励行 ・印刷物に対する適切な取扱いの実現 ・電磁媒体に対する適切取扱いの実現 ・PC 等のモバイル機器に対する適切な取り扱いの実施 ・情報が残る電子機器の使用についての適切な管理の実施	業務現場における情報の保護
・アクセス権限者へのなりすましの防止	ユーザ管理の徹底
・業務仕様面でのコンプライアンスの確保 ・業務運営上でのコンプライアンス違反の防止	法的要求事項の遵守
・業務のシステム化仕様の的確性の確保 ・指定した業務仕様の確実なシステム化の実現	システムの処理の正確性の確保
・システムの可用性についての要求の的確な把握 ・システムのシステム機器障害への対応能力の確保	システム機器等の障害に対するシステムの堅牢性の確保
・システムの性能についての要求の正確な把握 ・必要な性能を持つシステムの構築 ・日常からの性能管理の徹底	システムの性能の確保
・内部ネットワークからのシステムへの不正なアクセスの試みの阻止 ・外部からのシステムへの不正なアクセスの試みの阻止	不正アクセス対（システムに対する不正なアクセスの阻止策）
・OS 等のシステムのプラットフォームからのセキュリティホールの除去	セキュリティホール対策
・ウイルス感染の阻止 ・外部へのウイルス拡散の防止	ウイルス対策

表 3-3 脅威の分析から抽出されて脅威の現実化を防ぐための施策の対策ドメインへの集約(つづき)

脅威の分析から抽出された脅威の現実化の防止に必要な施策	セキュリティ対策のドメイン
・システム情報やセキュリティ管理情報に対する不正なアクセスや操作の阻止	システム情報やセキュリティ管理情報の保護
・システム上の業務情報に対する不正なアクセスや操作の阻止	システム上の業務情報の保護
・通信にかかわる問題へ対する攻撃	通信路上の情報の保護
・システムの利用上での不手際の防止 －インターネットの利用にあたっての事故や脆弱性の取込みの防止 －モバイルコンピューティングにおける事故や脆弱性の取込みの防止 －リモートオフィスの利用に伴う脆弱性の取込みの防止	インターネットサービスの使用にあたってのセキュリティ対策 特殊なシステムの利用環境に対するセキュリティ対策の実施 ・モバイルコンピューティングに対するセキュリティ対策 ・リモートオフィスにおけるセキュリティ対策
・DoS 攻撃の影響の極小化	サービス妨害への備え
・攻撃に対する堅牢性が高いシステム構成の確保	セキュアなシステムの構築とその維持
・OS 等のプラットフォームソフトの導入や変更における不手際の防止 ・オフィスツール等の汎用業務ツール系ソフトの導入や変更における不手際の防止 ・個別業務ソフトの導入や変更における不手際の防止	ソフトウェアの管理の徹底
・ネットワーク機器からの脆弱性の排除 ・サーバからの脆弱性の排除 ・LAN 上のクライアント PC からの脆弱性の排除	個々の機器における自衛策の実施
・アプリケーションソフトへの必要なセキュリティ機能の実装 ・アプリケーションソフトからの脆弱性の排除 ・開発過程での有害プログラムの侵入の阻止	セキュアなアプリケーションソフトの開発
・セキュリティ対策にかかわるシステム運用の的確な実践の追求 ・システム運用における不手際の防止 ・システム運用の委託先でのセキュアな運用の追及	システム運用上のセキュリティ対策（セキュアなシステム運用の追求）
・長期保管する電子情報からの見読性の喪失の防止 ・法的な要求にかかわる長期保管する電子情報の法的効力の喪失の防止	保管電子情報の有効性の確保
・保護領域の設置と関係者に対する保護領域への立入りの制限 ・保護領域内における不正行為の防止 ・社内外に設置するシステム機器等の物理資産に対する適切な保護の実施 －災害等を考慮した施設や設備、措置の配置と据付 －災害を考慮した保護対象物の保管 －必要に応じたバックアップの確保	施設や設備の保護

3.2.2.5. 付帯的な対策ドメインの設定

セキュリティ対策の実践を確実なものとするためには、脅威や脆弱性への直接的な対策に加え、多岐に渡るこれらの対策が有効に機能するための組織的な環境整備も必要となる。これらには、セセキュリティ対策の実施にかかわる組織としてのガバナンスやマネジメントの構築に加え、セキュリティ対策の実態のチェックが加えた。

これらは、脅威や脆弱性についての直接的な対策ではないが、セキュリティ対策の計画を適切なものとするとともに、計画した対策を期待通りに機能させるためには不可欠なものである。

また、セキュリティ事故の防止を中心とした 3.2.2.4 節に示した対策には含まれないセキュリティ事故への備えも、これに加えた。

本評価モデルにおいては、これらを表 3-4 のように設定した。

表 3-4 付帯的な対策ドメインの設定

課題	対策ドメイン
セキュリティ対策推進基盤の確立	セキュリティマネジメント環境の整備
	経営レベルからのセキュリティ要求の明確化
セキュリティ対策の実態の評価と必要な是正措置の実施	監査手法によるセキュリティ対策の実施状況のチェックの実施
	技術的な診断によるセキュリティ対策の機能状況のチェックの実施
セキュリティ事故への備え	セキュリティ事故への備え

セキュリティ対策推進基盤の確立とは、組織における情報セキュリティについてのガバナンスの確立であり、セキュリティ対策に対する実効的なマネジメント実施のベースを確立するものである。

また、セキュリティ対策は多岐にわたる対策がさまざまな対策現場で実施されなければならないため、不備や不手際がどうしも残るのも止むをえない。セキュリティ対策の欠陥が大きな事故に結びつかないよう、セキュリティ対策の実施状況については、常に、チェックを怠ってはならない。セキュリティ事故が発生する前に問題点を発見し、必要な是正措置を講じることができるようにを起さないようにするためのセキュリティ対策の実態の評価と必要な是正措置の実施も、セキュリティ対策の重要なテーマとなる。

セキュリティ対策に万全はありえず、如何にセキュリティ対策を尽くしたとしても、セキュリティ事故は起こりうると考えなければならない。このため、セキュリティ事故が発生しても、その影響を極小化する努力も、セキュリティ対策を総合的に強いものにするためには欠かせない。セキュリティ事故の予防策が如何に優れていようと、事故への備えが貧弱ではセキュリティ対策の強度は低いと見なければならない。一方、セキュリティ事故への予防策はそんなに強力でなくとも、セキュリティ対策のレベルから当然に想定される事故への備えが万全で、実務への影響はまずないようになっているシステムは、総合的に見てセキュリティ対策は十分であると言える。

3.2.2.6. 対策ドメインの体系化

洗出された対策テーマは、脅威に対する直接的な施策群を、業務現場における業務遂行に関する要求と、システム周りの要求に大別するとともに、多岐にわたるこれらの諸施策の実践を確実にするためのマネジメント環境の整備と、その実践状況のチェックの実施という付帯テーマの群に分けた。

そして、そのそれぞれを、マネジメント・ビュー、ビジネスオペレーション・ビュー、テクニカル＆オペレーション・ビュー、およびアシュアランス・ビューと名付けた。また、特に、対策ジャンルが多岐にわたるテクニカル＆オペレーション・ビューについては、これを、システムの信頼性の確保、攻撃に対するシステムの堅牢性の確保、セキュアなシステムの構築とそのセキュアな運用の実現、および、これ乱費ズレにも属さない総合的な施策群からなる必要となるその他のセキュリティ対策の 4 つのサブ・ビューに分けた。

これらの結果としての、本モデルにおける対策ビューの構成を図 3-2 に、本評価モデルにおける対策テーマの構成を表 3-5 に示す。

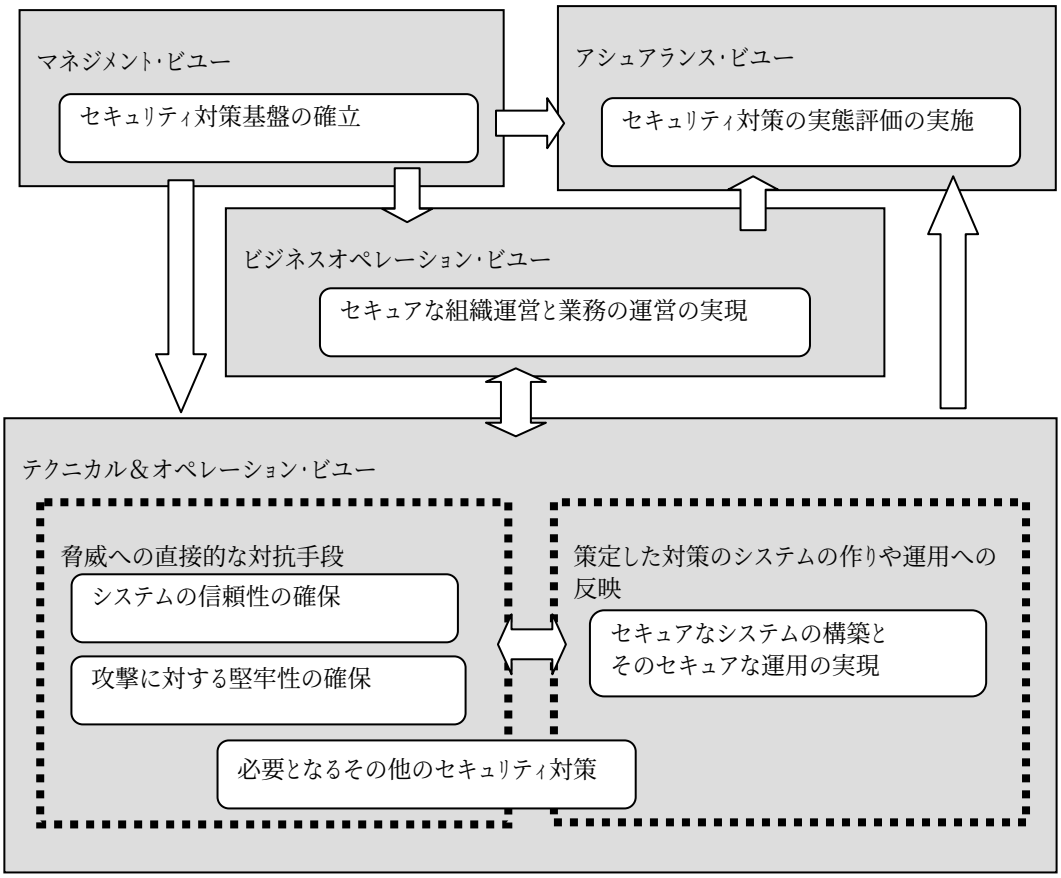

図 3-2 対策要求の体系

表 3-5 本評価モデルにおけるセキュリティ対策として対策要求の体系

ビュー	サブビュー	対策ドメイン	対策要求数
M マネジメント・ビュー	Ma セキュリティ対策推進基盤の確立	Ma1 セキュリティマネジメント環境の整備	6
		Ma2 経営レベルでのセキュリティ要求の明確化	3
B ビジネスオペレーション・ビュー	Ba セキュアな組織運営と業務運営の実現	Ba1 組織管理上でのセキュリティ対策	3
		Ba2 業務運営上でのセキュリティ対策	4
		Ba3 業務現場における情報の保護の徹底	4
		Ba4 ユーザ管理の徹底	2
		Ba5 法的要求事項の遵守	3
T テクニカル＆オペレーション・ビュー	Ta システムの信頼性の確保	Ta1 システムの処理の正確性の確保	5
		Ta2 障害に対するシステムの堅牢性の確保	3
		Ta3 システムの性能の確保	5
	Tb 攻撃に対するシステムの堅牢性の確保	Tb1 不正アクセス対策	12
		Tb2 セキュリティホール対策	4
		Tb3 ウイルス対策	4
		Tb4 システム情報およびセキュリティ管理情報の保護	3
		Tb5 システム上の業務情報の保護	4
		Tb6 通信路上の情報の保護	3
		Tb7 インターネットサービスの利用にあたってのセキュリティ対策	2
		Tb8 サービス妨害への備え	2
		Tb9 システムの動きに対する監視の実施	3
	Tc セキュアなシステムの構築とそのセキュアな運用の実現	Tc1 セキュアなシステムの構築とその維持	2
		Tc2 ソフトウェアの管理の徹底	3
		Tc3 個々の機器における自衛策の実施	3
		Tc4 セキュアなアプリケーションソフトの開発	3
		Tc5 システム運用上のセキュリティ対策	6
	Td その他のセキュリティ対策	Td1 保管電子情報の有効性の確保	4
		Td2 特殊な利用環境に対するセキュリティ対策	8
		Td3 施設や設備の保護	3
		Td4 セキュリティ事故への備え	5
A アシュアランス・ビュー	Aa セキュリティ対策の実施状況の評価の実施	Aa1 監査手法による対策状況のチェック	3
		Aa2 技術的な診断によるセキュリティ対策の欠陥のチェック	2

3.2.3. ステップ2：対策ドメインから対策要求へのブレークダウン

3.2.3.1. セキュリティ対策を構成する活動についての分析

セキュリティ対策は、セキュリティが確保されていることにつながる特定の状態を作り出すためのさまざまな活動の集合である。このセキュリティを確保するために必要となる状態にはさまざまなものがあるが、それを実現するための活動は、コアとなる活動とその活動を支える周辺活動から構成されているのが一般的である。セキュリティ対策の具体策として実施を要求することを洗い出すためには、一つの目的実現のために必要となるこの活動を分析しなければならない。

本モデルの研究チームは、一つのセキュリティ対策の実施を構成する活動を、図 3-3 のようなモデルとして捉え、このモデルを参照して、求める具体活動へのブレークダウンを行った。

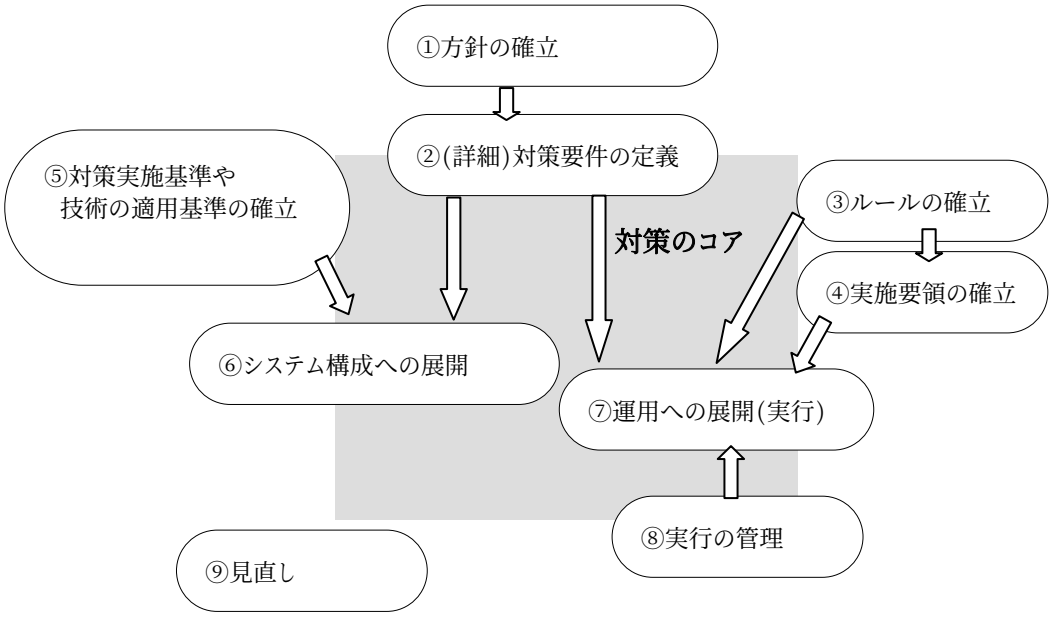

図 3-3 セキュリティ対策にかかる活動の構成

①の方針の確立は、当該対策についての方針であり、情報の保護や人的セキュリティにかかる対策の例に見られるように、対策によっては、この方針により実施内容が大きく左右されるものもある。このような対策テーマについては方針の確立は重要となる。

情報の保護においては、保護の対象となる情報の個々に、アクセス制御や格納や伝送にあたっての暗号化等、そのライフサイクル全体にわたって要求する具体的な保護の内容を指定しなければならないものもある。このように求める対策によっては、保護要件について詳細な定義を必要とするものがある。一方、ウイルス対策等では、あまり重要な位置付けにはならない。②の活動は、このようなものに対する要件の定義と言う活動である。

対策の主体が業務やシステムの運用あるいは組織の運営にかかわるものにあっては、当該活動にかかわるルールに確立が必要なものも存在する。③は、このような対策テーマにおける必要なルールの確立を指す。

また、このような対策テーマについては、実行プロセスや責任体制の明確化等、その活動の実施方法を規程する実施要領を確立しておく必要があるものもある。セキュリティ事故発生に必要となる活動等では必須なものとなる。④は、このような対策テーマにおける実施要領の確立を指す。

一方、技術的な対応を図る場合は、対策テーマによっては適用する技術の水準の選択ルール等を決める必要があるものがある。通信路の選択、認証方式の選択、あるいは暗号方式の選択が関わるような場合は、⑤のこれらの選択についての方針としての技術適用基準の指定も必要となる。

さらに、システムの機能に対策をゆだねる場合、それらの対策のシステムへの組込みが必要となるが、この活動は、設計と設計内容を実装に展開する二つの異なる活動から構成される。

また、業務やシステムの運用あるいは組織の運営にかかわる事項については、業務活動やシステムの運用あるいは組織の管理における、⑦のセキュリティ対策からの要求の実行が必要となる。

また、⑧の実行の管理は、⑦の実行を保証するための管理監督活動である。⑨の見直しは、システムの環境変化が対策内容の劣化につながらないようにするための定期的あるいは必要に応じた①から⑧間での諸活動の計画あるいは実施状況についての見直しであり、すべての対策テーマに不可欠なものである。

①から⑨のうち網目をかけている②、⑥、⑦は対策のコアとなるもので、その他はこのコアの活動を支える周辺活動であると見ることができる。

これらの活動を、ISMS で言う PDCA サイクルで整理したのが、表 3-6 である。

表 3-6 セキュリティ対策を構成する活動の体系

PDA サイクル		活動区分	内容
Plan	計画	①方針確立	関係する組織全体, あるいは対策ドメインごとの(取り組み)方針
		②要件の定義	求められる対策に対する具体的要件
	実施環境の整備	③実施要領の確立	要求事項の実施手順や責任体制等
		④実施基準の確立	要求事項への対応についての選択肢選択の考え方
		⑤施設･設備の準備	必要な設備やツールの確保
Do	実行および実行の管理	⑥システムへの組込み	セキュリティ要求事項のシステムへの反映の
		⑦システム運用･業務運用への反映	セキュリティ要求事項のシステムの運用や業務運用への反映
Check & Action	点検および是正措置	⑧活動に対する監査の実施	業務運用の監査の実施
		⑨技術面での監査の実施	技術面での監査の実施

本評価モデルでの対策要求の洗い出しにおいては、ISMS が求めること等の実現に必要な活動をこのような視点からブレークダウンした。

このとき、個々の活動をすべて一つの対策要求とすると、対策要求は膨大な数となるため、主な活動の一プロセスであり、かつそれが小さな(作業量がその内容や実行が求められる頻度等から見て小さな作業と判断できるものについては、主活動に統合する等で、独立の対策要求とはしなかった。

3.2.3.2. 全体としての見直し

このようにして対策テーマごと対策実践上の管理単位として洗い出した対策要求について、以下の視点で見直しを行った。

- 全体での対策要求の粒度等のバランスのチェック
- ISMS における対策要求との照合

前者は、対策要求が部分的に詳細になりすぎたり、大まかになりすぎることがないよう、実践上の管理単位として適切かどうかを見直したものである。

また、後者は、本モデルにおける対策要求は、ISMS の要求を全て抱合しているかどうかを確認するものである。これにより、、本モデルにおける対策要求は、ISMS の要求をすべて含むことが確認された。これにより、本モデルは、ISMS の要求の実践ガイドとしても位置付けられることになる。

3.3. 対策ドメインと対策要求の概要

3.3.1. マネジメント・ビューを構成する対策ドメインと対策要求

マネジメント・ビューは、セキュリティ対策を推進するためのメネジメント上の基盤としての組織の管理面で実施しなければならないことの集合であり、セキュリティ対策推進のためのマネジメント環境の整備と、経営レベルでのセキュリティ要求の明確化という 2 つのドメインから構成される。

セキュリティ対策の推進にかかるマネジメント環境の整備は、セキュリティ対策を組織的で戦略的なものにするためには不可欠なもので、経営レベルのテーマでもある。また、組織運営にかかわる要求は、情報セキュリティに関する技術面以外での対応が必要となるものを集めたもので、人的な管理を中心とするものである。法的要求事項への準拠は、事業展開や情報の取扱いにおいてルールを違反を起さないようにするものである。

3.3.1.1. セキュリティマネジメント環境の整備 (Ma1)

本体策ドメインは、セキュリティ対策を組織的かつ戦略的なものとし、セキュリティ対策の計画や実践を経営からのガバナンスの下におくためのもので、経営という立場での情報セキュリティへの取組方針や、セキュリティ対策の構築の方向付けや、必要なリソースの確保等を行うものである。

中規模以上の組織においては、特に重要となる。

本対策ドメインは、以下の対策要求で構成される。

(1) 経営レベルでのセキュリティポリシーの確立

(2) セキュリティ対策の組立ての確立

(3) セキュリティ対策を推進するための組織的な仕組みの確立
(4) 関係者の責任の明確化と関係者への周知
(5) 関係者のセキュリティ対策推進能力の確保
(6) セキュリティ対策予算の確保とその適切な執行

3.3.1.2. 経営レベルでのセキュリティ要求の明確化 (Ma2)

セキュリティ対策として、何をどのレベルで実施するかについての枠組みを示すもので、セキュリティ対策の対象領域における対象業務や、その運営形態や使用するシステムの作りや運用形態等の特性等からくるセキュリティ特性の明確化と、想定すべきリスクを踏まえた、セキュリティ対策の強度についての要求ならびに、保護対象資産に対する保護要件の大枠を示すものである。

本ドメインの対策要求が求めているものは、セキュリティ対策の計画の十分性や、実施してセキュリティ対策の十分性の評価のベースを与える。これらの点が、明確にされていないセキュリティ対策は評価以前のものとなる。

本対策ドメインは、以下の対策要求で構成される。

(1) 対象組織・情報システムのセキュリティ特性モデルの作成
(2) 保護対象となる組織内外に提供しているサービスについてのセキュリティ要求の明確化
(3) 保護対象情報資産の洗出しとその個々に対する保護要件の明確化

3.3.2. ビジネスオペレーション・ビューを構成する対策ドメインと対策要求

ビジネスオペラレーション・ビューは、組織の管理や業務現場における日常的な業務の遂行において、実施しなければならないセキュリティ要求をまとめたもので、技術的なものとは別に、日常の組織の運営や業務の運営における管理的な側面と、関係者の日常業務の中に取組まれるもので構成される。

本ビューは、以下の 5 つのドメインで構成される。

- 組織管理上でのセキュリティ対策
- 業務運営上のセキュリティ対策
- 業務現場における情報の保護の徹底
- ユーザ管理の徹底
- 法的要求事項の遵守

3.3.2.1. **組織管理上でのセキュリティ対策** (Ba1)

統計等によると、セキュリティ事故は、悪意や不注意等の人的を要因とするものが圧倒的に多い。本要求は、関係者や外部の者の悪意の行為の阻止や、関係者の業務他での職場における行動が不注意に流されないようにするためのものである。

本対策ドメインは、以下の対策要求で構成される。

(1) セキュリティ対策上の人的要因に対する管理の仕組みの確立

(2) 関係者に対する情報セキュリティについての取組意識の醸成と責務の明確化

(3) 関係者の信用の確認の実施と職場等での行動についての必要な管理の実施

3.3.2.2. **業務運営上でのセキュリティ対策** (Ba2)

セキュリティ対策の多くは、業務現場における業務の遂行や職場での日常的な行動にかかわる。本対策ドメインは、業務現場における業務の遂行や職場での日常的な行動で、セキュリティ対策に関し求められることが、確実に実践されるようにするための施策の集合である。

本対策ドメインは、以下の対策要求で構成される。

(1) 業務現場ごとのセキュリティ要求の明確化

(2) 業務現場におけるセキュリティ要求の実践の追及

(3) 他社とのリアルタイムの業務コラボレーションに対する適切なセキュリティ対策の実施

(4) 業務の外部委託に対する適切なセキュリティ対策の実施

3.3.2.3. **業務現場における情報の保護の徹底** (Ba3)

多くの情報を取扱う業務現場におけるずさんな情報の取り扱いは、情報の正確性の喪失や、情報の漏洩に直結する。本体策ドメインは、特に、情報セキュリティの中心テーマである情報の取り扱いを適切なものにするために必要な施策をまとめたものである。

本対策ドメインは、以下の対策要求で構成される。

(1) 印刷物の作成や安全な取扱いについてのルールの確立と、ルールに沿った印刷物の作成や取扱いの実践

(2) 可搬メディアの安全な取扱いについてのルールの確立と、ルールに沿った可搬メディアの取扱いの実践

(3) 情報機器の安全なと取扱いについてのルールの確立と、ルールに沿った情報機器の取扱いの実践

(4) その他の電子機器の安全な使用についてのルールの確立と、ルールに沿った使用の実践

3.3.2.4. ユーザ管理の徹底 (Ba4)

システムへのアクセスを許すユーザに対しては、以下が適切に行われていないと、容易になりすまし等を許すことになり、システムが提供するサービスの不正な利用や、システムへの不正なアクセスによる情報の不正な取得や、システムに対するさまざまな工作を許すことにつながる。

本対策ドメインは、上記の適切な実施により、アクセス制御機能が本来の役割を果たせるようにするためのものである。

- 個々のユーザの実体性や資格の正確な把握
- 個々のユーザに対するアクセス権の適切な付与
- ユーザに対するアクセス時の識別・認証に必要な情報との適切な付与とユーザにおけるこれらに対する適切な管理の実現

本対策ドメインは、以下の対策要求で構成される。

(1) ユーザ管理についてのルールの確立とルールに沿った管理の実施
(2) なりすまし防止に向けたユーザに対する指導の実施

3.3.2.5. 法的要求事項の遵守 (Ba5)

情報の取り扱いにおいては、法律他からさまざまな制約が存在する。組織の運営や業務の遂行上、これらの制約に違反がないようにしなければならない。本体策ドメインは、他社との契約上の制約や、法律上の制約や、業界のルールや諸ガイドラインや商慣行等からの要求の遵守を実現するために必要となる施策で構成される。

本対策ドメインは、以下の対策要求で構成される。

(1) ビジネスパートナーとの契約からの要求の遵守
(2) 事業に関係する法令やその他のルールの遵守
(3) 紛争の発生への備えの実施

3.3.3. テクニカル＆オペレーション・ビユーのサブビユー：システムの信頼性の確保を構成する対策ドメインと対策要求

システムの信頼性とは、システムの可用性、システムの処理および情報の正確性の主要な阻害要因である、システムの処理の誤りの防止や、システム機器の障害や性能のオーバーフローが求める可用性に影響するのを防止するための施策で構成される。

その実現は、システムの開発から始まるライフサイクル全体に渡り多くの技術的な施策の展開が必要となる、非常に重たいテーマである。

本サブ・ビユーは、以下の対策ドメインで構成される。

- システムの処理の正確性の確保

- 障害等に対するシステムの堅牢性の確保
- システムの性能の確保

3.3.3.1. システムの処理の正確性の確保 (Ta1)

本対策ﾄﾞﾒｲﾝは、システムの処理に誤りがないようにすること、および、万一、誤りが発生しても実害が出ないうちに発見し、必要な処置ができるようにするためのものである。

本対策ﾄﾞﾒｲﾝは、以下の対策要求で構成される。

(1) システムの処理の正確性確保のための仕組みの確立
(2) システムの業務仕様の定義の正確性の確保
(3) ｱﾌﾟﾘｹｰｼｮﾝｿﾌﾄからの不良の排除 (ｱﾌﾟﾘｹｰｼｮﾝｿﾌﾄの品質の確保)
(4) 日々の業務運用での処理結果の妥当性ﾁｪｯｸの実施
(5) 業務現場における問題発生時における対応能力の確保

3.3.3.2. 障害等に対するシステムの堅牢性の確保 (Ta2)

システムの可用性にもっとも影響を与えうるのは、システム機器の障害である。システムの可用性に対する要求が厳しい場合は、システム機器に障害が発生しても、システムの運転が継続できるような仕組みをシステムに組込んでおくことも必要となる。この場合、障害発生時における必要な処置は、日常的なものでないため、計画したことが何時でも円滑に実行できるようにするための備えも必要となる。本体策ﾄﾞﾒｲｲﾝは、システム機器に障害が発生しても、システムが求める可用性を実現できるようにするために必要なことを求めるものである。

本対策ﾄﾞﾒｲﾝは、以下の対策要求で構成される。

(1) 障害に対する堅牢性の確保を実現するための方式の確立
(2) 設計した障害対策機能のシステムへの的確な組込み
(3) システム障害発生時の対応能力の確保

3.3.3.3. システムの性能の確保 (Ta3)

システムの性能や容量のオーバーフローも、システムの可用性に直接的な悪影響を与える。システムが性能ﾄﾗﾌﾞﾙを起さないようにするためには、システムの計画時における性能や容量についんての要求を正確に把握するとともに、システムがこれらの要求に応えられるものとして作り上げることと、負荷の予期せぬ変動が時ならぬ性能ﾄﾗﾌﾞﾙを招かないよう、日頃からの、システムの負荷状態や性能特性の把握と、必要な対策のﾀｲﾑﾘｰな実施も欠かせない。

本体策ﾄﾞﾒｲﾝは、これらを確実に行うためのものである。

本対策ﾄﾞﾒｲﾝは､以下の対策要求で構成される。

⑴ 性能･容量管理の仕組みの確立

⑵ 性能･容量要件を満足するためのシステム面での実現方式の確立

⑶ システムの性能の確保に関し、必要なシステム構成や機能のシステムへの的確な組込み

⑷ 日常からの負荷･性能･容量使用の状況のﾁｪｯｸと問題発生に先立つ対策の実施

⑸ 性能･容量ﾄﾗﾌﾞﾙ発生時における対処能力の確保

3.3.4. テクニカル＆オペレーション･ビユーのサブビユー：攻撃に対するシステムの堅牢性の確保を構成する対策ﾄﾞﾒｲﾝと対策要求

このサブ･ビユーは、システムに対する論理的な攻撃、あるいは内部犯行から、システムの運用が阻害されたり、情報の正確性や秘匿が失われたり、システムの機能の不正使用が行われたり、気がつかないうちに他社ｻｲﾄの攻撃に加担してしまったりしないようにするための施策の集合であり、以下にに示すような対策サブﾄﾞﾒｲﾝで構成される。

- 不正アクセス対策
- セキュﾘﾃｨホール対策
- ウイルス対策
- システム情報およびセキュﾘﾃｨ管理情報の保護
- システム上の情報の保護
- 通信路上の情報の保護
- ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽの使用にあたってのセキュﾘﾃｨ対策
- サービス妨害への備え
- システムの動きに対する監視の実施

3.3.4.1. 不正アクセス対策 (Tb1)

権限のない者によるｻｲﾄｼｽﾃﾑへのアクセスは、システム機能の不正使用による業務やシステム運用の混乱を引き起したり、ｿﾌﾄｳｪｱおよびセキュﾘﾃｨ管理情報やユーザ情報等のシステム資産の破壊、改ざん、不正取得等につながる攻撃を可能にする。

システムへの不正アクセス対策は、システムをこのような被害から守るため、外部ならびに内部からのシステムへの論理的なアクセスを、正規のもの（許可された者がその権限の範囲でのアクセス）に限定し、それ以外のアクセスを排除するために必要となるものである。

本対策ﾄﾞﾒｲﾝは､表 3-7 に示す対策要求で構成される。

表 3-7 不正アクセス対策に関する対策要求

区分	対策要求
ネットワークレベルでの対策	(1) 接続ルールの確立と適切なネットワークの設計
	(2) 個々の端末からの接続要求に対する接続条件の適切な指定
	(3) 接続制御機器の的確な実装
	(4) VLAN の適切な使用
	(5) 無線 LAN の適切な使用
システムレベルでの対策	(6) 一般ユーザアカウントに対する適切な管理の実施
	(7) 一般ユーザに対する適切なアクセス制御の実施
	(8) 特権ユーザアカウントに対する適切な管理の実施
	(9) 特権ユーザに対する適切なアクセス制御の実施
	(10) 必要に応じたセキュアな OS の使用
アプリケーションレベルでの対策 その他	(11) アプリケーションでのアクセス管理の実施基準の確立と、個々のアプリケーションに対するアクセス管理要件の適切な指定
	(12) 個々のアプリケーションへの必要なアクセス管理機能の組込み

3.3.4.2. セキュリティホール対策 (Tb2)

サイトシステムに対するセキュリティホールをついた攻撃は、システム機能の不正使用、ソフトウェアの不正取得、改ざん、破壊、セキュリティ管理情報の破壊、改ざん、不正取得、ユーザ情報の破壊、改ざん、不正取得等の被害につながる。セキュリティホール対策とは、このような被害からシステムを守るため、システムの内在するセキュリティホールの迅速な除去や、システムの都合から危険なセキュリティホールを残したままにする場合に、このことが被害に結びつかないようにするための必要な施策の実行等を求めるものである。

本対策ドメインは、以下の対策要求で構成される。

(1) セキュリティホール対策についての管理のスキームの確立
(2) 脆弱性情報の入手から対策実施への展開の適切な実施
(3) 必要なセキュリティホール対策の迅速かつ安全な実施
(4) セキュリティホール対策の実施状況についての適切な管理の実施

3.3.4.3. ウイルス対策 (Tb3)

システムのウイルスへの感染は、ソフトウェアや情報資産の破壊等の被害を招き、サイト業務やシステムの運用に混乱を招くだけでなく、場合によっては、他サイトへのウイルス攻撃に加担することにもつながる。ウイルス対策とは、サイトのシステムへのウイルス感染による被害を防ぐため、

- システムのウイルス等有害プログラムの侵入の防止
- ウイルス感染時の被害の極小化
- 外部へのウイルス拡散の防止

のための諸施策の総称したものである。

本対策ドメインは、以下の対策要求で構成される。

⑴ ウイルス対策についての管理の仕組みの確立
⑵ 要求レベルに応じたウイルス対策ツールの選択と配置
⑶ ウイルス対策担当チームやシステムの利用者がウイルス対策に関し実行しなければならないことの的確な実施
⑷ ウイルス感染時の即応体制の整備

3.3.4.4. システム情報およびセキュリティ管理情報の保護 (Tb4)

ファイルのディレクトリ等のシステムの構成情報や、暗号鍵やユーザID・パスワード、更にはアクセス制御テーブル情報等のシステムのセキュリティ機能がよりどころにしている情報の漏洩や、改ざんは、なりすましによる不正取引の実行、システム機能の不正利用業務やシステム運用の混乱、システムの破壊、改ざん等につながる。

本体対策ドメインは、セキュリティ対策の鍵を狙うこれらの情報の保護が確実に行われるようにするためのものである。

本対策ドメインは、以下の対策要求で構成される。

⑴ システム情報やセキュリティ管理情報の保護の仕組みの確立
⑵ システム情報やセキュリティ管理情報に対する保護要件の確立
⑶ システム情報やセキュリティ管理情報の保護の実践

3.3.4.5. システム上の業務情報の保護 (Tb5)

システム上には大量の顧客の個人情報、取引先の商業秘密情報、取引情報等の業務情報が置かれている。これらの流出や外部への露呈は、ユーザのプライバシーの侵害や取引先のビジネスに影響を与えることにつながる。また、これらの情報に対する改ざん、破壊行為は、業務の運営を混乱させる。

本体策ドメインは、システム上の業務情報が、流出したり、外部に露呈したり、改ざん破壊等の工作から守るために必要な施策の集合である。

本対策ドメインは、以下の対策要求で構成される。

⑴ システム上の業務情報の保護の仕組みの確立
⑵ システム上の個々の業務データに対する保護要件の適切な指定
⑶ DBMS 管理下にある業務情報に対する適切な保護策の展開
⑷ 業務情報に対する保護を目的とした DBMS との関係におけるアプリケーションソフトの設計への配慮

3.3.4.6. 通信路上の情報の保護 (Tb6)

通信においてもさまざまなリスクが存在する。本宅ドメインは、通信路上のデータに含まれる顧客のID、パスワード等のセキュリティ管理情報、および顧客の個人情報や取引先の商業秘密情報に対する盗聴、改ざん、破壊行為や、通信の否認等を防ぐためのものである。

本対策ドメインは、以下の対策要求で構成される。

(1) 通信に対する保護要件の明確化

(2) 保護要件にあった通信路の選択とその適切な使用

(3) 無線 LAN の使用についてのセキュリティ対策の実施

3.3.4.7. インターネットサービスの利用にあたってのセキュリティ対策 (Tb7)

インターネットサービスのうかつな利用も危険が多い。本対策ドメインは、職場における日常の業務活動において、インターネットの利用におきて、守るべきことあるいは十分に注意すべきことの職場への明確化とその実践を要求するものである。

本対策ドメインは、以下の対策要求で構成される。

(1) 電子メールの使用についてのセキュリティ対策の実施

(2) ファイル転送 (FTP) その他の危険なプロトコルの使用にあたっての保護措置の実施

3.3.4.8. サービス妨害への備え (Tb8)

DoS攻撃等は、不正行がないとされているが、可用性についての要求が厳しいシステムにおいては、万一、そのような攻撃を受けても、その被害を最小限に止める工夫も必要となる。本体策ドメインは、サービス妨害の影響を極小化するために必要となる施策の明確化とその実践を求めるものである。

本対策ドメインは、以下の対策要求で構成される。

(1) アクセス集中を用いたサービス妨害を考慮したシステムの設計

(2) 緊急対応手順の検討と策定

3.3.4.9. システムの動きに対する監視の実施 (Tb9)

攻撃に対するさまざまな対策を講じていても、その不備や不手際をつかれることも考慮しておかなければならない。このような場合、システムに何が起こったかを正確に把握できなければ、被害からの回復や、再発防止策を実施することができない。また、事故には至らないが、警戒すべき事象や、対策の改善が必要な事態を把握するためにも、システムの動きに対する監視は必要となる。

システムの監視には、不審な動きの検出と警報の発出と、事後の調査のためのさまざまなログの取得からなる。

本対策ドメインは、以下の対策要求で構成される。

(1) ネットワークの動きに対する監視の実施

(2) システムへのアクセスに対する監視の実施

(3) アプリケーションへのアクセスに対する監視の実施

3.3.5. テクニカル＆オペレーション・ビューのサブビュー：セキュアなシステムの構築とそのセキュアな運用の実現を構成する対策ドメインと対策要求

セキュリティ対策のうち技術面での対応は、的確にシステムの作りやその運用に反映されていなければならない。本サブ・ビューは、システムの作りや運用が、セキュリティ対策を的確に反映したものであるようにするためのものである。

このドメインは、システムの可用性、性能、処理の正確性を確保するための諸対策、攻撃に対する堅牢性の確保のための諸対策、セキュリティ事故への備えについての諸対策が、システムに作りに求めていることが的確に反映するようにするための施策の集合である。

対策ドメインは、以下の 5 つで構成される。

- セキュアなシステム構成の維持
- ソフトウエア管理の徹底
- 個々の機器における自衛策の実施
- セキュアなアプリケーションソフトの開発
- システム運用上のセキュリティ対策

3.3.5.1. セキュアなシステムの構築と維持 (Tc1)

サイトシステムのセキュリティ対策は、セキュアなシステムの構成の上に置かれた各機器に組込んださまざまなセキュリティサービス機能や、各機器に対するセキュリティ要件に対応した諸設定を基盤としている。このため、システムの構成ならびにセキュリティサービス機能および各機器における諸設定は、個々のセキュリティ対策が求めていることに的確に対応したものでなければならない。

セキュアなシステムの構築とは、サイトの構成の設計やその実装を適切に行い、

- 攻撃を受付けにくい
- 攻撃を受けても被害は限られる

と言えるような、攻撃に対して堅固なシステムを構築することをいう。

サイトシステムの構成や各構成機器におけるセキュリティ対策にかかわる機能を、セキュリティ対

策が求めていることを的確に反映したものにするためには、システムの構成管理面からの適切な対応が必要となる。

個々のセキュリティ対策に対応した機能の実装については、それぞれのセキュリティ対策テーマごとの施策で触れているが、ここでは、実際のシステム構成や各機器における機能の実装が、サイトのセキュリティ確保のために定められた諸施策を的確に反映したものにし、サイトシステムをセキュリティに強いシステムにするよう、システム構成管理面に求めることを纏めている。

本対策ドメインは、以下の対策要求で構成される。

(1) セキュアなシステム構成の設計

(2) システム構成方針の沿ったシステムの構成の構築とその維持

3.3.5.2. ソフトウェアの管理の徹底 (Tc2)

ソフトウエアのずさんな管理も、システムの混乱の元となる。本対策ドメインは、正当なソフトウェアを、適切な状態で用いることができるようにするためのいものである。

本対策ドメインは、以下の対策要求で構成される。

(1) OS 等プラットフォーム系ソフトに対する管理ルールの確立とルールに沿った導入・変更の実施

(2) オフィスツール等の汎用業務ツール系ソフトの管理ルールに対する確立とルールに沿った導入・変更の実施

(3) (個別) 業務ソフトの管理ルールに対する確立とルールに沿った導入・変更の実施

3.3.5.3. 個々の機器における自衛策の実施 (Tc3)

十分な注意を払わなければ、システムを構成する機器それぞれにも脆弱性が残される。これらについも十分な対策がなされいなければ、この脆弱性を足掛かりにシステムのセキュリティ対策全体が崩壊することもありうる。本体対策ドメイインは、システムを構成する機器のうち、脆弱性の除去の処理が必要となる機器に対する脆弱性の除去の実践を求めるものである。

本対策ドメインは、その対象を別にした、以下の対策要求で構成される。

(1) ネットワーク制御機器におけるセキュリティ対策の実施

(2) サーバにおけるセキュリティ対策の実施

(3) LAN 上のクライアント PC におけるセキュリティ対策の実施

3.3.5.4. セキュアなアプリケーションソフトの開発 (Tc4)

個別開発されるアプリケーションソフトに、誤処理を誘起したり、攻撃の足掛かりを与えるような脆

弱性が残されないようにしなければならない。本体策ﾄﾞﾒｲﾝは、開発するｱﾌﾟﾘｹｰｼｮﾝｼｽﾃﾑに、このような脆弱性が残されないようにするための要求からなる。

本対策ﾄﾞﾒｲﾝは、以下の対策要求で構成される。

(1) ｱﾌﾟﾘｹｰｼｮﾝｿﾌﾄへの必要なｾｷｭﾘﾃｨ機能の組込み

(2) ｱﾌﾟﾘｹｰｼｮﾝｿﾌﾄからの脆弱性の排除

(3) 開発ﾌﾟﾛｾｽに対する管理の実施

3.3.5.5. セキュアなシステム運用の追求 (Tc5)

ｾｷｭﾘﾃｨ対策におけるさまざまな施策は、運用に依存しているところが多い。システムの構成や諸機能がｾｷｭﾘﾃｨについて十分に配慮されていたとしても、システムの運用がずさんであれば、システムのｾｷｭﾘﾃｨは危険にさらされ、システムの構築で施したせっかくの苦心も無に帰しかねない。

特に、システムの運用においては、日常の多忙な運用の中にｾｷｭﾘﾃｨにかかる運用処理が埋もれ易いことと、ｾｷｭﾘﾃｨについては専門家でない多くの要員が関係するため、不手際も生じ易い。

個々のｾｷｭﾘﾃｨ対策に対応した運用の的確な実施の実現については、それぞれのｾｷｭﾘﾃｨ対策テーマの施策で述べてきたが、ここでは、システムの運用上におけるｾｷｭﾘﾃｨ対策にかかわる事項が、的確に実施されるように、運用ｻｲﾄﾞに求められることを纏めたものである。

本対策ﾄﾞﾒｲﾝは、以下の対策要求で構成される。

(1) セキュアなシステム運用を実現するための管理の仕組みの確立

(2) 日々のシステム運用におけるｾｷｭﾘﾃｨ要求の実践

(3) 運用環境の保全の確保

(4) システムの切替えの安全の確保

(5) 運用関係者のシステム運用職場での行動に対するｾｷｭﾘﾃｨ要求の実践

(6) システム運用の外部委託についてのｾｷｭﾘﾃｨ対策

3.3.6. テクニカル＆オペレーション･ビューのサブビュー：必要となるその他のセキュリティ対策を構成する対策ﾄﾞﾒｲﾝと対策要求

本ｻﾌﾞ･ﾋﾞｭｰは、これまで述べてきたこと以外に、特に、配慮を要するものを纏めたものであり、以下の 4 つの対策ﾄﾞﾒｲﾝで構成される。

- 保管電子情報の有効性の確保
- 特殊なシステムの利用環境に対するｾｷｭﾘﾃｨ対策
- 施設や設備の保護
- ｾｷｭﾘﾃｨ事故への備え

3.3.6.1. 保管電子情報の有効性の確保 (Td1)

最近、文書他の情報を電子化して保管することが多くなった。電子化しての保管は、保管場所の節約や、検索の容易性から有利な面がある一方、保管が長期になった場合、物理的あるいは論理的は要因による見読性の喪失や、法的な効力の喪失の危険も存在する。このため、情報や文書の長期間にわたる電子的な保管については、十分な配慮が必要となる。

本対策ﾄﾞﾒｲｲﾝは、長期保管が前提の情報の電子化とその保管について、問題を回避するために必要な施策を求めるものである。

本対策ﾄﾞﾒｲﾝは､以下の対策要求で構成される。

(1) 長期保管する電子情報の適切な保管を実現するための管理の仕組みの確立

(2) 長期保管を行う電子情報の作成や保管に必要な技術環境の整備

(3) 長期保管の対象電子情報に対する保管要件の適切な指定

(4) 対象電子情報に対する指定要件に沿った保管措置の実施

3.3.6.2. 特殊なシステム利用環境におけるセキュリティ対策の実施 (Td2)

モバイルＰＣの進化や家庭へのＰＣの浸透等で、職場以外でシステムの利用も一般的なものとなってきた。保護されていない領域でのシステムの利用や、保護対象情報が格納されたＰＣ他の電子機器の外部への持ち出しは、それだけで危険が伴う。また、規模が小さく設備面でも管理面でも必要な施策の実践が困難なﾘﾓｰﾄｵﾌｨｽの運営においては、ｵﾌｨｽ環境に合った対策が必要となる。

本対策ﾄﾞﾒｲﾝは、モバイルコンピューティングや､ﾘﾓｰﾄｵﾌｨｽのずさんな利用や運営が、システム全体のセキュリティを損ねないよう、必要となる対策の実施を求めるものである。

(1) モバイルコンピューティングに対するセキュリティ対策

モバイルコンピューティング環境においては、組織に施設内に比べ脅威は比較にならない程高いため、多くの注意が必要となる。また、注意にも限界があるため、これらの脅威の現実化を前提とすると、重要な情報の持ち出しの制限や、暗号化の徹底等の予防策も必要となる。

モバイルコンピューティングに対するセキュリティ面での管理の甘さから、施設内におけるセキュリティ対策が無意味にならないよう、モバイルコンピューティングの利用についてのセキュリティ要求は明確にされ、利用者に徹底されていなければならない。

(2) ﾘﾓｰﾄｵﾌｨｽの運営に対するセキュリティ対策

ﾘﾓｰﾄｵﾌｨｽとは、本社や情報センターや工場等の本格的な施設に置かれる業務の拠点とは別の、固定のスペースを持った出先の職場のうち、比較的規模も小さく、管理も十分に行き届かないような職場を指す。規模の小さい営業店や出張所等のこのような職場においては、情報セ

キュリティ面で特別な配慮が必要となる。

リモートオフィスに対するセキュリティ対策とは、このような職場に対するセキュリティ面での特別な施策を総称するものである。業務拠点と比べリスクが高いリモートオフィスにおいて必要な情報セキュリティ確保するためには、以下のような施策が必要となる。

本対策ドメインは、以下の対策要求で構成される。

(1) モバイルコンピューティングの利用についてのセキュリティ要求の明確化
(2) モバイルコンピューティングに対するセンターシステム側での必要なセキュリティ対策の実施
(3) 利用者サイドにおけるにモバイルコンピューティングに対するセキュリティ要求の実践の追求
(4) リモートオフィスごとのセキュリティ対策のフレームワークの確立
(5) リモートオフィスサイドのシステムに対するセキュアな構築
(6) リモートオフィスサイドのシステムのセキュアな運営の追求
(7) リモートオフィスの施設や設備に対する必要な保護策の実施
(8) リモートオフィスにおける業務運営や組織管理におけるセキュリティ事故防止の追求

3.3.6.3. 施設や設備の保護 (Td3)

システムへの物理アクセスとは、EC サイトの運営にかかわるソフトウェアや情報がインストールされている機器に直接触れて利用することを言う。サイトのセキュリティ確保に向けてさまざまな施策が実施されていても、システムが物理的な観点から、不正に利用されるような環境に置かれていては、サイトのセキュリティは危いと考えなければならない。 また、機器や記録媒体の盗難にも留意しなければならない。機器や記録媒体の盗難は、それらの中に記録されているソフトウェアやセキュリティ管理情報、ユーザ情報の漏洩につながるため、サイトシステムのセキュリティには大きな脅威となる。

実施しているセキュリティ対策を十分に活かすためにも、システムは正規の運用者のみが利用できるような環境に置き、適切な管理下に置くことが必要である。

このため、サイトシステムを構成する機器や記録媒体等を、可能な限り関係者以外から隔離することを図るとともに、これらへの物理的なアクセスが限定されるような管理の仕組み作ることが必要である。本対策ドメインは、保護対象資産に対する物理的・環境的な保護を求めるものである。

本対策ドメインは、以下の対策要求で構成される。

(1) 閉鎖型の保護領域における必要な保護の実施
(2) 半閉鎖型の保護領域における必要な保護の実施
(3) 社内外に設置する装置や関連設備に対する必要な保護策の実施

3.3.6.4. セキュリティ事故への備え (Td4)

この対策ドメインは、セキュリティ対策を尽くしていたとしても、新しい攻撃手段の登場や、システ

ム運用上の思わぬ不手際により、セキュリティ事故は発生しうる。万一、セキュリティ事故が発生しても、被害が拡大しないようにすることと、情報やシステムの復旧が正確、迅速にできて業務の運営に支障が生じないようにするためには、事故発生の早期検知、原因の確定、被害状況の正確な把握、情報やシステムの回復、業務の再開等の手段が整備されていなければならない。このサブ・ビューは、このようなセキュリティ事故への備えについての要求を纏めたものである。

本対策ドメインは、以下の対策要求で構成される。

(1) 異常検知時における即応能力の確保
(2) システム周りのセキュリティ事故への対応能力の確保
(3) セキュリティ事故が業務面に影響した場合の対処要領の確立と関係者への徹底
(4) セキュリティ事故の処理に必要なシステム環境の整備
(5) システムの長期停止への備え

3.4. アシュアランス・ビューを構成する対策ドメインと対策要求

サイトのセキュリティは、計画されたセキュリティ対策の妥当性と、求められているセキュリティ対策の確実な実行により達成されものである。しかし、十分に検討されたと考えられるセキュリティ対策も、サイトの運営方法やサイトシステムの変更等の運営環境の変化に対応して、その妥当性を維持して行くこと、ならびに、業務の運営やシステムの運用が常に、セキュリティの確保に関し求められていることに対応できているようにすることは、なかなか難しいと考えなければならない。

このため、セキュリティ対策の妥当性とサイトの運営現場でのその実施状況をチェックする、サイト運営全体に対するセキュリティ監査の定期的な実施は、サイト運営におけるセキュリティの確保には欠かせない。

アシュアランス・ビューは、業務の運営やシステムの実態を確認するためのもので、以下の 2 つの対策ドメインで構成される。

- 監査手法による対策状況のチェック
- 技術的な診断によるセキュリティ対策の欠陥のチェック

3.4.1.1. 監査手法による対策状況のチェック (Aa1)

本対策ドメインは、セキュリティ対策の計画の作成や、計画したセキュリティ対策が確実に実践に移されているかどうかを、監査手法により検証することも求めているものである。セキュリティは多くの対策現場における日常的な活動に多くを依存するため、ともすれば、関係者の認識の欠場や管理に甘いところがあれば、すぐにでも抜けが生じる。本要求は、マネジメント上からこのようなことを防ぐためのものである。

本対策ドメインは、以下の対策要求で構成される。

(1) セキュリティ監査実施環境の整備

⑵ 対策ﾄﾞﾒｲﾝごとの対策の実施状況についての監査の実施
⑶ 監査結果の評価･報告とフローアップの実施

3.4.1.2. 技術的な診断によるセキュリティ対策の欠陥のチェック

セキュリティ対策において技術的な対応も実に多くの根気のいる作業の積み上げとなる。このため、どこかにミスが入り込むのも止むを得ない。問題は、このようなミスが見過ごされ、大きな事故につながることである。このため、技術的な診断により、しかるべきタイミングで、セキュリティ対策が機能しているかどうかのチェックを行うことも重要となる。

技術的な診断には、ドキュメントベースで行うものと、診断ツールを用いた実機診断がある。

本対策ﾄﾞﾒｲﾝは､以下の対策要求で構成される。

⑴ 診断ツールによる診断実施要領の確立
⑵ 診断ツールによるセキュリティ対策の欠陥のチェック

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

1 マネジメント・ビュー (M)

サブビュー「(Ma) セキュリティ対策推進基盤の確立」：対策ドメイン「(Ma1) セキュリティメネジメント環境の整備」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ma1.1	経営レベルでのセキュリティポリシーの確立	●									●				
Ma1.2	セキュリティ対策の組立ての確立	●									●		●	●	
Ma1.3	セキュリティ対策を推進するための組織的な仕組みの確立		●				●				●		▲	▲	
Ma1.4	関係者の責任の明確化と関係者への周知						●				●	▲	▲	▲	
Ma1.5	関係者のセキュリティ対策推進能力の確保			●	●	●	●				●	●	●	●	
Ma1.6	セキュリティ対策予算の確保とその適切な執行		●				●				●	▲	▲	▲	

サブビュー「(Ma) セキュリティ対策推進基盤の確立」：対策ドメイン「(Ma2) 経営レベルからのセキュリティ要求の確立」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ma2.1	対象組織・情報システムのセキュリティ特性モデルの作成			●							●	▲	●	▲	
Ma2.2	保護対象となる組織内外に提供しているサービスについてのセキュリティ要求の明確化			●											
Ma2.3	保護対象情報資産の洗出しとその個々に対する保護要件の明確化			●							●	●	●	●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

2 ビジネスオペレーション･ビュー

サブビュー「(Ba) セキュアな組織運営と業務運営の実現」:対策ドメイン「(Ba1) 人的要因によるセキュリティ事故の防止」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ba1.1	セキュリティ対策上の人的要因に対する管理の仕組みの確立		●			●					●				
Ba1.2	関係者に対する情報セキュリティについての取組意識の醸成と責務の明確化		●			●	●				●	▲	▲	▲	
Ba1.3	関係者の信用の確認の実施と職場等での行動についての必要な管理の実施					●	●				●	●	●	●	

サブビュー「(Ba) セキュアな組織運営と業務運営の実現」:対策ドメイン「(Ba2) 業務運営上でのセキュリティ対策」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ba2.1	業務現場ごとのセキュリティ要求の明確化		●					●			●	●			
Ba2.2	各業務現場におけるセキュリティ要求の実践の追求					●	●	●			●	●	●	●	
Ba2.3	他社との業務コラボレーションに対する適切なセキュリティ対策の実施	●	●			●	●	●	▲	▲	●	●	▲	▲	
Ba2.4	業務の外部委託に対する適切なセキュリティ対策の実施	●	●			●	●	●			●	●			

サブビュー「(Ba) セキュアな組織運営と業務運営の実現」:対策ドメイン「(Ba3) 業務現場における情報の保護」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ba3.1	印刷物の作成や安全な取扱いについてのルールの確立と、ルールに沿った印刷物の取扱いの実践	●	●	●		●	●	●			●	●	●	●	
Ba3.2	可搬メディアの安全な利用についてのルールの確立と、ルールに沿った可搬メディアの取扱いの実践	●	●	●		●	●	●			●	●	●	●	
Ba3.3	情報機器の安全な取扱いについてのルールの確立と、ルールに沿った情報機器の取扱いの実践	●	●	●	●	●	●	●			●	●	●	●	
Ba3.4	その他の電子機器の安全な使用についてのルールの確立と、ルールに沿った使用の実践	●	●	●	●	●	●	●			●	●	●	●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

2 ビジネスオペレーション・ビュー

サブビュー「(Ba) セキュアな組織運営と業務運営の実現」：対策ドメイン「(Ba4) 適切なユーザ管理の実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ba4.1	ユーザ管理についてのルールの確立と、ルールに沿ったユーザ管理の実施	●	●	●	●	●					●	●			
Ba4.2	なすまし防止に向けたユーザに対する指導の実施							●							●

サブビュー「(Ba) セキュアな組織運営と業務運営の実現」：対策ドメイン「(Ba5) 法的要求事項の遵守」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ba5.1	ビジネスパートナーとの契約からの法的要求の遵守	●	●	●		●		●			●	●	▲	▲	
Ba5.2	事業に関係する法令やその他のルールの遵守	●	●	●		●		●			●	●	▲	▲	
Ba5.3	紛争の発生への備え	●	●	●		●		●		●	●	●	▲	●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

3 テクニカル＆オペレーション・ビュー

サブビュー「(Ta) システムの信頼性の確保」：対策ドメイン「(Ta1) システムの処理の正確性の確保」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ta1.1	システムの処理の正確性確保のための仕組みの確立		●			●					●	●	●		
Ta1.2	業務仕様の定義の正確性の確保					●		●				●			
Ta1.3	アプリケーションソフトからの不良の排除 (アプリケーションソフトの品質の確保)	●	●			●			●				●		
Ta1.4	日々の業務運用での処理結果の妥当性チェックの実施		●			●		●		●		●		●	
Ta1.5	業務現場における問題発生時の対応の能力の確保					●		●		●		●		●	

サブビュー「(Ta) システムの信頼性の確保」：対策ドメイン「(Ta2) システム機器等の障害に対するシステムの堅牢性の確保」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ta2.1	障害に対する堅牢性の確保を実現するための方式の確立	●		●	●								●		
Ta2.2	設計した障害対策機能のシステムへの的確な組込み								●				●		
Ta2.3	システム障害の発生時の対応能力の確保					●				●				●	

サブビュー「(Ta) システムの信頼性の確保」：対策ドメイン「(Ta3) システムの性能の確保」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Ta3.1	性能・容量管理の仕組みの確立	●		●							●		●		
Ta3.2	性能・容量要件を満足するためのシステム面での実現方式の確立				●				●				●		
Ta3.3	システムの性能の確保に関し、必要なシステム構成や機能のシステムへの的確な組込み								●				●		
Ta3.4	日常からの負荷、性能、容量使用の状況のチェックと問題発生に先立つ対策の実施					●				●				●	
Ta3.5	性能・容量トラブル発生時における対処能力の確保				●	●				●				●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

3 テクニカル＆オペレーション・ビュー

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」：対策ドメイン「(Tb1) システムに対する不正なアクセスの阻止 (不正アクセス対策)」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb1.1	ネットワークレベルでの対策1： 接続ルールの確立と適切なネットワークの設計と実現方針の確立	●											●		
Tb1.2	ネットワークレベルでの対策2： 個々の端末からの接続要求に対する接続条件の適切な指定			●	●	●							●		
Tb1.3	ネットワークレベルでの対策3：接続制御機器の適切な実装				●	▲			●				●		
Tb1.4	ネットワークレベルでの対策4：VLAN の適切な使用					▲			●	●				●	
Tb1.5	ネットワークレベルでの対策5：無線 LAN の適切な使用			●					●	●			●	●	
Tb1.6	システムレベルでの対策1： 一般ユーザアカウントに対する適切な管理の実施	●	●	●			●	●		●	●	●	●	●	
Tb1.7	システムレベルでの対策2： 一般ユーザに対する適切なアクセス制御の実施	●		●	●	●			●				●	●	
Tb1.8	システムレベルでの対策3： 特権ユーザアカウントに対する適切な管理の実施	●	●	●	●	●	●			●			●	●	
Tb1.9	システムレベルでの対策4： 特権ユーザに対する適切なアクセス制御の実施	●		●	●	●			●				●	●	
Tb1.10	システムレベルでの対策4：必要に応じたセキュアな OS の適切な使用	●			●								●		
Tb1.11	アプリケーションレベルでの対策1： アプリケーションにおけるアクセス管理基準の確立と個々のアプリケーションに対するアクセス管理要件の適切な指定	●		●	●				●				●		
Tb1.12	アプリケーションレベルでの対策2： 個々のアプリケーションへの必要なアクセス管理機能の組込み				●				●				●	●	

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」：対策ドメイン「(Tb2) セキュリティホール対策」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb2.1	セキュリティホール対策についての管理のスキームの確立	●	●		●	●			●	●			●	▲	
Tb2.2	脆弱性情報の入手から対策実施への展開の適切な実施					●								●	
Tb2.3	必要なセキュリティホール対策の迅速かつ安全な実施					●				●				●	
Tb2.4	セキュリティホール対策の実施状況についての適切な管理の実施					●				●				●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

3 テクニカル＆オペレーション・ビュー

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」:対策ドメイン「(Tb3) ウイルス対策」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb3.1	ウイルス対策についての管理の仕組みの確立	●	●	●	●	●	●						●	▲	
Tb3.2	要求対策レベルに応じたウイルス対策ツールの選択と配置								●				●		
Tb3.3	ウイルス対策担当チームやシステムの利用者がウイルス対策に関し実行しなければならないことの的確な実施							●		●		●		●	
Tb3.4	ウイルス感染時の即応体制の整備	●				●		●		●		●		●	

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」:対策ドメイン「(Tb4) システム情報やセキュリティ管理情報の保護」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb4.1	システム情報やセキュリティ管理情報の保護の仕組みの確立	●	●		▲	●							●	▲	
Tb4.2	システム情報やセキュリティ管理情報に対する保護要件の確立			●	●								●	▲	
Tb4.3	システム情報やセキュリティ管理情報の保護の実践								●	●				●	

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」:対策ドメイン「(Tb5) システム上の業務情報の保護」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb5.1	システム上の業務情報の保護の仕組みの確立	●	●		▲	●			●				●		
Tb5.2	システム上の個々の業務データに対する保護要件の適切な指定			●	●							▲	●		
Tb5.3	DBMS 管理下にある業務情報に対する適切な保護策の展開	●	●		●				●				●		
Tb5.4	業務情報に対する保護を目的とした DBMS との関係におけるアプリケーションソフトの設計への配慮	●			●				●				●		

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」：対策ドメイン「(Tb6) 通信路上の情報の保護」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb6.1	通信に対する保護要件の明確化	●	●	●	●								●		
Tb6.2	保護要件にあった通信路の選択とその適切な使用				●				●				●		
Tb6.3	無線 LAN の使用についてのセキュリティ対策の実施		●					●	●	●		●	●		

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」：対策ドメイン「(Tb7) インターネットサービスの利用にあたってのセキュリティ対策」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb7.1	電子メールの使用に対するセキュリティ対策の実施	●	●	●	●				●			●	●		
Tb7.2	ファイル転送 (FTP) その他の危険なプロトコルの使用にあたっての保護措置の実施	●	●	●	●					●				●	

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」：対策ドメイン「(Tb8) サービス妨害への備え」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb8.1	アクセス集中を用いたサービス妨害を考慮したシステムの設計	●			●				●				●		
Tb8.2	緊急対応手順の検討と策定	●			●	●				●				●	

サブビュー「(Tb) 攻撃に対するシステムの堅牢性の確保」：対策ドメイン「(Tb9) システムの動きに対する監視の実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tb9.1	システムアクセスに対する監視の実施	●	●		●	●				●			●	●	
Tb9.2	内部ネットワーク内での接続に対する監視の実施	●	●		●	●				●			●	●	
Tb9.3	アプリケーションへのアクセス監視の実施	●	●		●	●				●			●	●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

3 テクニカル＆オペレーション･ビュー

サブビュー「(Tc) セキュアなシステムの構築とセキュアなシステム運用の実現」:対策ドメイン「(Tc1) セキュアなシステム構成の確保」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tc1.1	セキュアなシステム構成の設計	●		●	●								●		
Tc1.2	システム構成方針に沿ったシステムの構成の構築とその維持					●			●				●	●	

サブビュー「(Tc) セキュアなシステムの構築とセキュアなシステム運用の実現」:対策ドメイン「(Tc2) ソフトウエアに対する適切な管理の実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tc2.1	OS 等プラットフォーム系ソフトに対する管理ルールの確立と、ルールに沿った導入･変更の実施	●	●	●	●	●			●	●			●	●	
Tc2.2	オフィスツール等の汎用業務ツール系ソフトの管理ルールに対する確立と、ルールに沿った導入･変更の実施	●	●	●	●	●			●	●			●	●	
Tc2.3	(個別) 業務ソフトの管理ルールに対する確立と、ルールに沿った導入･変更の実施	●	●	●	●	●			●	●			●	●	

サブビュー「(Tc) セキュアなシステムの構築とセキュアなシステム運用の実現」:対策ドメイン「(Tc3) 個々に機器における自衛策の実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tc3.1	ネットワーク制御機器におけるセキュリティ対策			●		●			●				●	●	
Tc3.2	サーバにおけるセキュリティ対策			●		●			●				●	●	
Tc3.3	LAN 上のクライアント PC に対するセキュリティ対策			●		●			●				●	●	

サブビュー「(Tc) セキュアなシステムの構築とセキュアなシステム運用の実現」:対策ドメイン「(Tc4) セキュアなアプリケーションソフトの開発」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tc4.1	アプリケーションソフトへの必要なセキュリティ機能の組込み	●	●			●			●				▲	●	
Tc4.2	アプリケーションソフトからの脆弱性の排除					●			●					●	
Tc4.3	開発プロセスに対する管理の実施	●	●			●			●					●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

3 テクニカル＆オペレーション・ビュー

サブビュー「(Tc) セキュアなシステムの構築とセキュアなシステム運用の実現」:対策ドメイン「(Tc5) セキュアなシステム運用上の追求」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Tc5.1	セキュアなシステム運用を実現するための管理の仕組みの確立	●	●			●				●				●	
Tc5.2	日々のシステム運用におけるセキュリティ要求の実践					●				●				●	
Tc5.3	運用環境の保全の確保		●			●				●				●	
Tc5.4	システムの切替えの安全の確保		●			●				●		▲	●	●	
Tc5.5	運用関係者のシステム運用職場での行動に対するセキュリティ要求の実践		●			●					▲			●	
Tc5.6	システム運用の外部委託についてのセキュリティ対策	●	●	●		●				●	●			●	

サブビュー「(Td) 必要となるその他の対策」:対策ドメイン「(Td1) 長期保管する電子情報に対する必要な措置の実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	システム構成への展開	システム運用への展開	管理部門	業務現場	システム企画開発	システムの運用管理	その他
Td1.1	長期保管する電子情報の適切な保管を実現するための管理の仕組みの確立	●	●		●			●			●	▲	●	▲	
Td1.2	長期保管を行う電子情報の作成や保管に必要な技術環境の整備								●	●			●	●	
Td13.	長期保管の対象情報に対する保管要件の適切な指定			●		●				●	●	●			
Td1.4	対象情報に対する指定要件に沿った保管措置の実施								●	●	●	●		●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

3 テクニカル＆オペレーション･ビュー

サブビュー「(Td) 必要となるその他の対策」:対策ドメイン「(Td2) 特殊なシステムの利用環境に対するセキュリティ対策の実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	ｼｽﾃﾑ構成への展開	ｼｽﾃﾑ運用への展開	管理部門	業務現場	ｼｽﾃﾑ企画開発	ｼｽﾃﾑの運用管理	その他
Td2.1	モバイルコンピューティングの利用についてのセキュリティ要求の明確化	●									●	●	●		
Td2.2	モバイルコンピューティングに対するセンターシステム側での必要なセキュリティ対策の実施			●	●				●				●	●	
Td2.3	利用者サイドにおけるにモバイルコンピューティングに対するセキュリティ要求の実践							●				●		●	
Td2.4	リモートオフィスごとのセキュリティ対策のフレームワークの確立	●	●	●											
Td2.5	リモートオフィスサイドのシステムのセキュな構築				●				●			▲		●	
Td2.6	リモートオフィスサイドのシステムのセキュアな運用の追求					●				●		●			
Td2.7	リモートオフィスにおける業務運営や組織管理におけるセキュリティ事故防止の追求					●		●				●			
Td2.8	リモートオフィスの施設や設備や空間に対する必要な保護策の実施		●					●				●		▲	

サブビュー「(Td) 必要となるその他の対策」:対策ドメイン「(Td3) 施設、設備、保護対象空間に対する適切な保護措置の実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	ｼｽﾃﾑ構成への展開	ｼｽﾃﾑ運用への展開	管理部門	業務現場	ｼｽﾃﾑ企画開発	ｼｽﾃﾑの運用管理	その他
Td3.1	閉鎖型の保護領域における必要な保護の実施	●	●	●	●	●	●				●			●	
Td3.2	半閉鎖型の保護領域における必要な保護の実施	●	●	●	●	●					●	●			
Td3.3	社内外に設置する装置や関連設備に対する必要な保護策の実施	●	●	●	●	●				●				●	

付表　対策要求の一覧
活動区分は当該要求に含まれる活動の種類、また、主たる担当部門は当該要求の実施にかかわる部門を示す

3 テクニカル＆オペレーション･ビュー

サブビュー「(Td) 必要となるその他の対策」:対策ドメイン「(Td4) セキュリティ事故への備え」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	ｼｽﾃﾑ構成への展開	ｼｽﾃﾑ運用への展開	管理部門	業務現場	ｼｽﾃﾑ企画開発	ｼｽﾃﾑの運用管理	その他
Td4.1	異常検知時における即応能力の確保	●				●		●		●		●		●	
Td4.2	システム周りのセキュリティ事故への対応能力の確保	●			●	●			●	●		●	●	●	
Td4.3	セキュリティ事故が業務面に影響した場合の対処要領の確立と、関係者への徹底	●			●	●		●			●	●		▲	
Td4.4	セキュリティ事故の処理に必要なシステムシステム環境の整備	●		●					●				●	●	
Td4.5	システムの長期停止への備え	●	●	●	●	●		●	●	●	▲	●	●	●	

4　アシュアランス･ビュー

サブビュー「(Aa) セキュリティ対策の実態の評価」:対策ドメイン「(Aa1) 監査手法によるセキュリティ対策実践状況のチェックの実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	ｼｽﾃﾑ構成への展開	ｼｽﾃﾑ運用への展開	管理部門	業務現場	ｼｽﾃﾑ企画開発	ｼｽﾃﾑの運用管理	その他
Aa1.1	セキュリティ監査実施環境の整備	●	●	●		●					●	▲	▲	▲	
Aa1.2	対策テーマごとの対策の実施状況についての監査の実施						●				●	▲	▲	▲	
Aa1.3	監査結果の評価･報告とフローアップの実施						●				●	▲	▲	▲	

サブビュー「(Aa) セキュリティ対策の実態の評価」:対策ドメイン「(Aa2) 技術的な診断による技術面でのセキュリティ対策の機能状況のチェックの実施」

対策要求 ID	対策要求名	活動区分									主たる担当部門				
		方針や基準の確立	適用するルールの確立	対策要件の指定	具体的手段の指定	実施要領の確立	組織管理への展開	業務運用への展開	ｼｽﾃﾑ構成への展開	ｼｽﾃﾑ運用への展開	管理部門	業務現場	ｼｽﾃﾑ企画開発	ｼｽﾃﾑの運用管理	その他
Aa2.1	診断ツールによる診断実施要領の確立	●		●	●	●			●				●		
Aa2.2	診断ツールを用いたシステムの脆弱性診断の実施									●				●	

4. 対策強度レベルの設定基準

4.1. 対策強度の概念

本モデルは、セキュリティ対策の計画を妥当なものにするとともに、実施している対策に問題がないかどうかを評価するための尺度を提供するものである。セキュリティ対策の計画や実施しているセキュリティ対策の妥当性とは、多くの施策の集合からなるセキュリティ対策が、対象システムのセキュリティ環境の特性や、経営からのセキュリティについての要求に照らし、必要な範囲で十分なものになっていることを言う。

本モデルは、セキュリティ対策の妥当性の評価に、対策強度という概念を用いる。セキュリティ対策における対策強度とは、セキュリティ対策に対する信頼度についての抽象的な概念であり、本モデルでは、これを 5 段階のレベルに分けて表す。経営レベルが求めるシステム全体に対する対策強度は、セキュリティ対策を構成する対策ドメインの個々における強度により決定される。また、対策ドメイン個々の対策強度は、当該対策ドメインにおける対策要求の個々の対する対策強度によって決まる。このため、対策の計画内容や対策の実施状況から、対策要求の個々についての対策強度レベルを知ることができれば、個々の対策要求についての十分性の評価に加え、システム全体としての対策強度も把握できることになる。

本モデルは、セキュリティ対策の妥当性、すなわち、対策が必要な範囲で十分かどうかを判断するための尺度として、対策に対する信頼度である対策強度を 5 段階のレベルに分け、対策要求の個々について、この 5 段階の各レベルの達成条件を示すことで、個々の対策要求についての対応の妥当性の妥当性を評価できるようにしたものである。

セキュリティ対策の計画にあたっては、まず、対象システムの特性や当該システムのセキュリティに対する経営の要求から、システム全体が達成すべきセキュリティ対策の強度レベルを設定する。そして、この選択したシステム全体としてのセキュリティ対策の強度は、個々の対策要求についての対策強度と、個々の対策要求のセキュリティ対策全体に及ぼす影響によってきまるので、個々の対策要求に求められる対策強度レベルは、一般には、システム全体に求められる対策強度レベルをベースとするが、対象システムのセキュリティ環境によっては、1 レベルあげるべきところや、1 レベル下げても構わないところもでてくる。このため、個々の対策要求に対して、必要な対策強度レベルを、システム全体に求められる対策強度レベルを参照しながら、対象とする対策要求の周辺を勘案し、当該対策要求に求められる対策レベルを設定する。個々の対策要求に対する対策強度レベルが設定できれば、当該対策要求が実施を求めていることと、各対策レベルの達成条件として示されている対策の内容から、実施すべき具体策の枠組みを知ることができる。

また、実施しているセキュリティ対策の妥当性を評価したい場合は、個々の対策要求についての実施状況を、本モデルに示されている当該対策要求についての対策強度レベル判定基準に沿って評価すれば、当該対策要求についての対策強度のレベルを知ることができ、計画を満足しているかどうかと、必要な改善点も知ることができる。この利用イメージは、2.1 節に示している。

4.2. システム全体としてのセキュリティ対策強度の考え方

システム全体のセキュリティ対策の強度とは、対象とする組織領域において実施されているセキュリティ対策に対する信頼度についての抽象的な概念であり、セキュリティ対策を構成する対策ドメイン個々の強度により決定される。対策ドメイン個々の対策強度は、当該対策ドメインにおける対策要求の個々の対する対策強度によって決まる。

システム全体の対策強度は、個々の対策要求の対策強度と、個々の対策のセキュリティ対策への影響度合いによって決まる。この関係を示したのが、式1および式2である。

$$R_S = \sum p_{di} R_{di} \qquad \text{式1}$$

ここで、R_Sは対象システムの全体に対する総合的な対策強度レベル

P_{di} は対策ドメイン i のシステム全体の対策強度評価における比重（$\Sigma di=1$）

R_{di} は対策ドメイン i に対する対策強度レベルの評価値で、下記の式 2 によって決まる。

$$R_{di} = \sum p_{di \cdot cj} R_{di \cdot cj} \qquad \text{式2}$$

ここで、R_{di} は対策ドメイン i の対策強度レベルの評価値

$P_{di \cdot cj}$ は対策ドメイン i を構成する対策要求 j の対策ドメイン i の対策強度評価における比重（$\Sigma di \cdot cj=1$）

$R_{di \cdot cj}$ は対策ドメイン i におけるに対策要求 j に対する対策強度レベルの評価値

4.3. 個々の対策要求における対策強度

4.3.1. 個々対策要求の対策強度の決定要素

本モデルでは、個々の対策要求についての強度レベルを決める要素を表 4-1 のようにしている。これらの評価要素に対する評価を総合的に見たものが、それぞれの対策要求における対策強度レベルとなる。

表 4-1 個々の対策要求についての対策強度の決定要素

区分	要求が、 技術的な要求の場合	要求が、 業務や管理面についての要求の場合
対策コア 当該対策の中核をなし、強度レベル決定の決定的要素となるもの	・採用している技術のレベル ・採用した技術の使用の決め細かさ ・適用の網羅性 （適用の対象が複数ある場合における適用対象の個々に対する適用状態）	・要求のきめ細かさ ・適用の網羅性 （適用の対象が複数ある場合における適用対象の個々に対する適用状態）
周辺要素 対策コアの内容や実施の信頼性の担保に通じる要素	・当該対策の検討のレベル ・実装プロセスの確立のレベル ・実装管理の厳格さレベル ・見直しの実行レベル ・文書化のレベル	・当該対策の検討のレベル ・実行プロセスの確立のレベル ・実行管理の厳格さのレベル ・見直しの実行レベル ・文書化のレベル

4.4. 対策要求の個々に対する対策強度レベルの決定手順

本モデルでは、個々の対策要求についての対策強度レベルは図 4-1 に示す手順で決める。

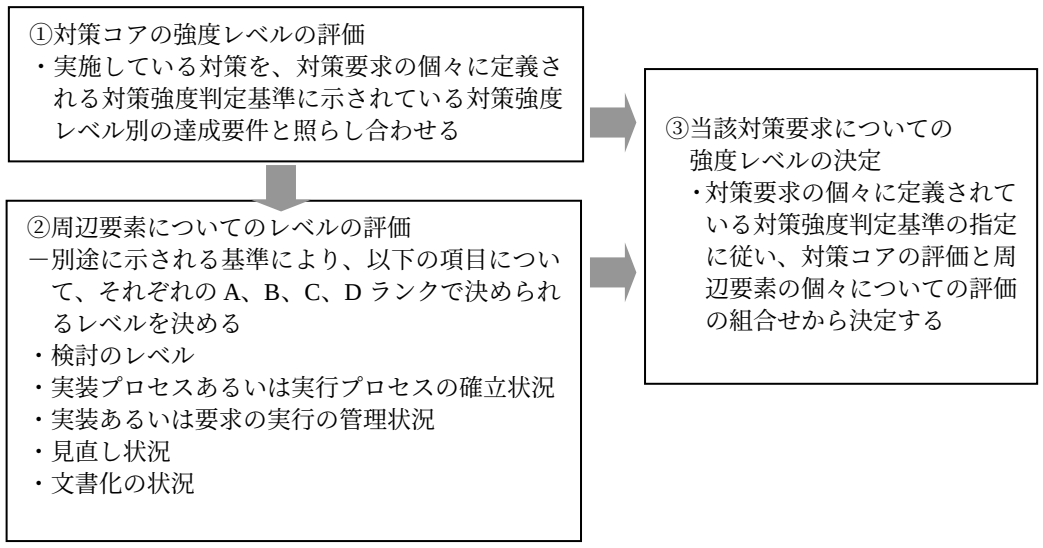

図 4-1 個々の対策要求に対する対策強度レベルの判定手順

4.5. 本モデルにおける対策強度の設定基準

本モデルが示している個々の対策要求に対する対策強度レベルの判定基準は、以下のような考えにもとづき設定されている。

4.5.1. システム全体に対する対策強度レベル基準

本モデルにおける、システム全体についての 5 段階にレベル分けした対策強度の概念を、表 4-2 に示す。

表 4-2 システム全体に対する対策強度の 5 段階のレベル

レベル区分	強度レベルの概念	このレベルのセキュリティ対策が求められるシステムのイメージ
レベル 5	現時点ではこれ以上は望めないレベルで、よほどのことがない限り問題が生じることはないと考えてよいレベル	トラブルは社会不安につながるようなシステム ・防衛、治安関係、法曹関係機関 ・ライフライン関係や通信事業者、交通機関等の社会インフラ関係システム ・医療関係システムの一部
レベル 4	一般に求められるレベルより一段と高いレベルで、通常では問題が生じる可能性はほとんどなく、意図的な攻撃に対してもある程度堅牢と見ることができるレベル	公共的なサービスを提供する等で、ある程度社会的な責任を持つようなシステム ・政府機関、地方自治体等の官公庁 ・金融機関 ・e マーケットプレース他のシステムサービスを提供事業者のシステム ・大企業の一部システム
レベル 3	平均的なシステムに一般に求められる強度で、日常的に問題が生じる可能性は低いが、偶発的なトラブルの可能性は残り、意図的な攻撃に対しては十分とは言えないレベル	問題が生じても外部への影響が少ないシステム ・一般企業のシステム ・教育機関のシステム
レベル 2	必要最低限のレベルで、リスクが低いか、リスクを受入れることを認めたシステムにおいてのみ、セキュリティ対策として有効と認められるレベル	問題が生じても外部への影響も自分の組織にも影響が小さいシステム ・一部の中小企業のシステム
レベル 1	必要最低限に達しないレベルで、セキュリティ対策の有効性について期待できないレベル	

4.5.2. 対策要求の個々に定義する対策強度レベル基準

本モデルにおいては、個々の対策要求についての対策強度レベルの評価が基本となる。システム全体としての対策強度の判定のベースとなる、この個々の対策要求についての対策強度レベルは、システム全体としての対策強度レベル分けに沿ったものでなければならない。このことから、本モデルにおける対策要求の個々についての対策強度レベルの設定基準を、表 4-3 に示すようなものとした。

表 4-3 対策要求の個々に定義する強度のレベルの考え方

レベル区分	強度レベルの概念
レベル5	当該対策要求について、それが技術的な要求の場合は、現時点で考えられる最高水準の技術の採用や対策の2重化等が、また、現場の実務や管理面についての要求の場合には、不手際が発生する余地をほとんどなくすとともに、不手際が発生してもそれをカバーする仕組みや、問題を見逃さないようにする仕組みが完備され、これらが完全に機能していると見なすことができるレベル。 問題が生じる余地は、まず、ないと考えることができるレベル。
レベル4	当該対策要求について、それが技術的な要求の場合は、一般的なシステムが平均的に用いている技術より1ランク信頼性の高いものが使われるか、平均的技術でも平均以上に最適化が図られている。また、現場の実務や管理面についての要求の場合には、不手際が発生する余地をほとんどなくすとともに、平均的なシステムよりきめ細かいルールが策定され、またその運用が厳格に管理されており、これらが機能していることについて高い信頼がおけるレベル 一般に求められるレベルより一段と高いレベルで、通常では問題が生じる可能性はほとんどなく、意図的な攻撃に対してもある程度堅牢と見ることができるレベル
レベル3	当該対策要求について、それが技術的な要求の場合は、平均的なシステムで一般に使用されているツール等が平均的な使われ方をしている。また、現場の実務や管理面についての要求の場合には、平均的な対応がある程度の組織的な管理の下で行われており、対策が機能していることが、相当程度の信頼できる。 日常的に問題が生じる可能性は低いが、偶発的なトラブルの可能性は残り、意図的な攻撃に対しては、必ずしも十分とは言えないレベル
レベル2	レベル3の要求については満足できないが、当該対策要求に対して、ある程度有効と思われる対策が機能していると認められるレベル。 組織的な対応とは言えなくても、相当の実効性が期待できるレベル。
レベル1	必要最低限に達しないレベルで、セキュリティ対策の有効性について期待できないレベル

4.5.3. システム全体が目標とすべき対策強度レベルと個々の対策要求に求められる対策強度レベルの関係

なお、システム全体として目標とすべきレベルと、対策要求の個々が達成しなければならない強度レベルの関係を、表 4-4 に示す。

表 4-4 システム全体が目標とする対策強度レベルと個々の対策要求に求められる対策強度レベルの関係

システム全体の対策レベル	対象システムのイメージ	対策要求の個々に求められる強度レベル
レベル5	トラブルは社会不安につながるシステム ・防衛、治安関係、法曹関係機関 ・ライフライン関係や通信事業者、交通機関等の社会インフラ関係システム ・医療関係システムの一部	・重要な対策要求についてはレベル5 ・その他の対策要求についてはレベル4以上
レベル4	公共的なサービスを提供する等で、ある程度社会的な責任を持つシステム ・政府機関、地方自治体等の官公庁 ・金融機関 ・e マーケットプレース他のシステムサービスを提供事業者のシステム ・大企業の一部システム	・重要な対策要求についてはレベル4以上 ・その他の対策要求についてはレベル3以上
レベル3	問題が生じても外部への影響が少ないシステム ・一般企業のシステム ・教育機関のシステム	・特に重要な対策要求についてはレベル4以上 ・一般的な対策要求についてはレベル3 ・リスクが特に低いと見ることができる対策要求ついてはレベル2でも可
レベル2	問題が生じても外部への影響も自分の組織にも影響が小さいシステム ・一部の中小企業のシステム	・対応が必要な対策要求のすべてに対してレベル2以上

(注) 特に重要な対策要求や重要な対策要求は、システムのセキュリティ特性や経営からのセキュリティについての要求によって異なったものとなる。このため、本モデルを使用するユーザが個々に判断するものとして、本評価モデルでは特に示していない。

4.5.4. 個々対策要求の対策強度レベルの決め方

4.5.4.1. 対策要求の個々に対する対策強度レベルの設定基準

本モデルでは、個々の対策要求についての対策強度レベルの設定については、表 4-5 をベースとしている。ただし、対策要求によっては、このベースと異なったものが指定されていることもある。

表 4-5 対策要求個々に対する対策強度レベルの設定基準

対策強度レベル	評価	対策強度レベルの定義
5	さらに強	・対策コアはレベル5（対策要求ごとに示される） ・当該要求についての対策の検討レベルは A ・実行プロセスの確立状況についてのレベルは A ・実行管理の実施状況についてのレベルは A ・見直しのレベルは A ・文書化のレベルは A
4	相当に強	・対策コアはレベル 4 以上（対策要求ごとに示される） ・当該要求についての対策の検討レベルは B 以上 ・実行プロセスの確立状況についてのレベルは B 以上 ・実行管理の実施状況についてのレベルは B 以上 ・見直しのレベルは B 以上 ・文書化のレベルは B 以上
3	ベースライン	・対策コアはレベル3以上 ・対策コアはレベル3以上（対策要求ごとに示される） ・当該要求についての対策の検討レベルは B 以上 ・実行プロセスの確立状況についてのレベルは B 以上 ・実行管理の実施状況についてのレベルは B 以上 ・見直しのレベルは B 以上 ・文書化のレベルは B 以上
2	ベースライン 以下であるが 場合によっては 可とできる	・対策コアはレベル2以上（対策要求ごとに示される） ・当該要求についての対策の検討レベルは C 以上 ・実行プロセスの確立状況についてのレベルは、レベル C 以上 ・実行管理の実施状況についてのレベルは、レベル C 以上 ・見直しのレベルは、レベル C 以上 ・文書化のレベルは C 以上
1	不十分	対策はされていてもレベル2の達成要件も満足せず，対策に有効とはみなされない （対策実態の評価結果として使用）

4.5.4.2. 技術的な要求についての対策コアに対する評価基準

本モデルでは、技術的な要求についての対策コアに対する評価の基準を、表 4-6 のようにしている。

表 4-6 技術的な要求についての対策コアについての評価基準

レベル	当該レベルの達成条件
レベル 5	現時点では、これ以上のものは望めない。 (特に重要なシステムにおける重点テーマについてのみ要求されるレベル) ・必要な対象部分にすべてに以下が講じられている ・当該要求で本来的に考慮しなければならないことの全てに対し、十分な考慮がなされている －細部に渡る綿密な前提条件の確認にもとづくきめ細かい設計 ・レベル4が採用している技術(方式)に比べ、信頼度は１ランク上のものが採用されている －信頼度の高い技術の採用 －2 重化の実施
レベル 4	平均以上であるが、まだ上もある。 (特に重要なシステムにおいては、全体的に、平均以上のセキュリティレベルが求められるシステムにおいては、重要テーマについて要求されるレベル) ・重要な対象部分については、以下が講じられており、その他の部分についてはレベル3以上が講じられている ・当該要求で本来的に考慮しなければならないことのほとんどが十分に考慮されている ・レベル3の基準となっているような平均的に用いられている技術(方式)に比べ、信頼度は 1 ランク上のものが採用されている
レベル 3	一般のシステムにおいて平均的に求められるレベル ・重要な部分に対しては以下が講じられており、その他の部分に対してはレベル2以上の対策が講じられている ・当該要求で本来的に考慮しなければならないもののうち、重要なところについては十分に考慮されている ・採用技術(方式)は、平均的に用いられているものである
レベル 2	信頼度は、ベースラインであるレベル3より１ランク低いが、システムによってはおおむね十分と見ることができるレベル (リスクが低いシステムや、他の対策によってカバーされているような場合に採用できるレベル) ・当該要求で本来的に考慮しなければならないもののうち、重要なところについては考慮されている ・採用技術(方式)は、平均的に用いられているものより１ランク低いがある程度信頼できる
レベル 1	実務的に無体策に近い。問題が生じる可能性は高い。 ・レベル2の達成要件も満たさない

4.5.4.3. 業務面や管理面についての要求における対策コアに対する評価基準

本モデルでは、業務面や管理面についての要求についての対策コアに対する評価の基準を、表 4-7 のようにする。

表 4-7 業務面や管理面についての要求に対する対策コアについての評価基準

レベル	当該レベルの達成条件
レベル 5	現時点では、これ以上のものは望めない。 (特に重要なシステムにおける重点テーマについてのみ要求されるレベル) ・必要な対象部分にすべてに以下が講じられている ・当該要求で本来的に考慮しなければならないことの全てに対し、十分な考慮がなされている ・良く検討された、発生した不手際をカバーする仕組みや、不手際を見逃さない仕組みが組み込まれている ・実行のプロセスや実行管理についての厳格な仕組みが確立している ・実行は厳しく管理されており、不手際が見逃される可能性はほとんどない
レベル 4	平均以上であるが、まだ上もある。 (特に重要なシステムにおいては、全体的に、平均以上のセキュリティレベルが求められるシステムにおいては、重要テーマについて要求されるレベル) ・重要な対象部分については、以下が講じられており、その他の部分についてはレベル 3 以上が講じられている ・当該要求で本来的に考慮しなければならないことのほとんどに対し、十分な考慮がなされている ・発生した不手際をカバーする仕組みや、不手際を見逃さない仕組みがある程度組み込まれている
レベル 3	一般のシステムにおいて平均的に求められるレベル ・重要な部分に対しては以下が講じられており、その他の部分に対してはレベル 2 以上の対策が講じられている ・最低限の必要なことは明確にされているが、発生した不手際をカバーする仕組みや、不手際を見逃さない仕組みまでは配慮が及んでいない
レベル 2	信頼度は、ベースラインであるレベル 3 より 1 ランク低いが、システムによってはおおむね十分と見ることができるレベル (リスクが低いシステムや、他の対策によってカバーされているような場合に採用できるレベル) ・必要最小限のレベルであるが、対策現場で習慣的なものが成立している
レベル 1	実務的に無体策に近い。問題が生じる可能性は高い。 ・レベル 2 の達成要件も満たさない

4.5.4.4. 周辺要素に対する評価基準

本モデルでは、周辺要素についてはクラスA（十分）、クラスB（概ね十分）、クラスC（十分とはいえないがある程度評価できる）の3ランクで評価する。それぞれの評価要素に対する評価基準は、以下の通り。なお、クラスCに満たないものは、不合格としてみるものとする。

（1）対策の検討レベルについての評価基準

対策内容の的確性の判断材料の一つとして、対策内容がどのような経緯で決められたものかを問うもので、検討やレビューの体制、検討からレビューや承認に至るまでのプロセスの確立、検討の密度、組織としての承認の有無、専門家の参画等が、評価のポイントとなる。

この評価要素についての評価基準は、表 4-8 に示すようなものとした。

表 4-8 検討のレベルについての評価基準

評価	検討体制（注2）	プロセスの確立	検討の密度	組織としての承認	専門家の参画
クラスA	○	○	○	○	○
クラスB	○	○	○	○	△
クラスC	△	―	△	△	―

（注1）個々の評価ポイントの ○は十分、△は概ね十分、×は不十分、―は特に問わない

（注2）○：検討体制が組織的なものとして構築されている

△：担当チーム内での検討であっても、チームとしての検討として行われている

（2）実装プロセスや実行プロセスの確立状況についての評価基準

計画通りに対策が実践されているかどうかも対策強度を大きく左右する。対策が計画通りに実践されるようになっているか、あるいはされているかどうかの判断材料の一つとしてその実践を担保するための基盤となる実装や実行のプロセスの確立状況を問うもので、対応プロセスの検討体制、検討の密度と内容きめの細かさ、組織としての承認の有無、対象現場での実効性等が、評価のポイントとなる。

この評価要素についての評価基準は、表 4-9 示すようなものとした。

表 4-9 関係プロセスの確立状況についての評価基準

評価	プロセスについての検討の体制	検討の密度と	内容の決めの細かさ	組織としての承認	対策現場での実効性（注 2）
クラスA	○	○	○	○	○
クラスB	○	△	△	○	△
クラスC	△	△	△	△	△

（注1） 個々の評価ポイントの ○は十分、△は概ね十分、×は不十分

（注2） 対策現場での実効性とは、対策現場の実態に照らした実行可能性および実際の適用状況を言う

（3）実装の管理や実行管理の徹底状況についての評価基準

計画通りに対策が実践されているかどうかも対策強度を大きく左右する。対策が計画通りに実践されているかどうかの判断材料の一つとして、実行状況が管理されているかどうかを問うもので、管理の仕組みの確立、管理の仕組みに沿った管理の実行状況の検討の密度と内容きめの細かさ、組織としての承認の有無、対象現場での実効性等が、評価のポイントとなる。

この評価要素についての評価基準は、表 4-10 示すようなものとした。この表に見られるように、組織的に確立した仕組みがなくても、実際に何がしかの管理が行われていれば、クラス C として“よし”としている。

表 4-10 関係プロセスの確立状況についての評価基準

評価	実行管理の仕組みの確立（注2）	実行管理の 実施状況（注3）
クラス A	○	○
クラス B	○	△
	△	○
クラス C	△または×	△

（注 1）個々の評価ポイントの ○は十分、△は概ね十分、×は不十分
（注 2）管理の当該対策要求の実行を徹底するための仕組みの確立状況を問うもので、内容の決めの細かさ、組織としての承認、関係者への徹底状況をポイントに評価する。
（注 3）実行管理の徹底度問うもので、管理としてのチェックの実施密度やチェックの内容の密度から評価する。

(4) 対策の見直しの実行状況についての評価基準

定期的あるいは必要に応じた対策内容の見直しが行われ、技術面あるいは組織の運営面でのセキュリティ環境の変化に対応した対策の変更も、当該対策要求に対する対策の有効性の維持も、その対策強度に直結する。この対策の見直しの実行状況は、対策内容の妥当性の判断材料の一つとして、当該対策についての見直しが実際にどの程度に行われているかを問うもので、見直しの実行およびその管理についての仕組みの確立状況、定期的な見直しの状況、必要に応じた見直しの状況、対策に変更が必要となった場合の対応の実態等が、評価のポイントとなる。

この評価要素についての評価基準は、表 4-11 示すようなものとした。この表に示すように、見直しについてのルールは確立されていなくても、見直しが実際に行われてよれば、クラス C として、よしとしている。

表 4-11 対策の見直しの実施状況についての評価基準

評価	見直しについてのルールの確立（注1）	定期的な見直しの実施状況（注 2）	必要に応じた見直しの実施状況（注3）	対策の変更が必要となった場合の 対応の実態（注 4）
クラス A	○	○	○	○
クラス B	○	△	△	○または△
	△	○	○	○または△
クラス C	△または×	△	△	△

（注１）当該対策の見直しについてルールの確立状況を問うもので、見直しの体制、内容

の決めの細かさ、組織としての承認、関係者への徹底状況等で判断する
（注２）定期的な見直しのが実際にどのようなレベルで行われているかどうかを問うもので、評価のサイクル、見直しのきめ細かさ、見直し結果の対策への反映状況等で判断する
（注３）必要に応じた見直しのが実際にどのようなレベルで行われているかどうかを問うもので、見直しの必要性の見落としがないかどうか、必要が生じた場合の見直しの迅速さ等で判断する
（注４）対策への見直し結果の反映がどの程度的確かつ迅速に行われているかどうかを問うもので、対策実施までのタイムラグ、対策の検証のレベル等で判断する

⑸ 文書化のレベルについての評価基準

対策内容や対策の実施について記録等についての文書化のレベルも、対策内容や対策の実践が適切かどうかの判断材料となる。そのため、これらについての文書化のレベルを問うもので、文書化について管理の仕組みや、実際の文書化の状況が、評価のポイントとなる。

この評価要素についての評価基準は、表 4-12 示すようなものとした。この表に示すように、文書化についての管理の仕組みは確立していなくても、実務に用いられ機能している文書が作成され使われていれば、クラス C として、“よし”としている。

表 4-12 関係プロセスの確立状況についての評価基準

評価	文書化の管理の仕組みの確立（注1）	文書化の実態（注2）	備考
クラス A	○	○	確立したルールのもと文書化は徹底している
クラス B	○	△	文書化のルールは確立されており、文書化はある程度行われているが、ルールは十分に守られていない
	△	○	文書化のルールは確定していないが、実務的に必要な文書化は行われている
クラス C	△または×	△	文書化ができているとは言えないまでも、現場で必要な文書として機能しているものがある

（注１）当該対策要求の実行を徹底するための仕組みの確立状況を問うもので、文書化についてのるルールの決めの細かさ（様式、承認や保管のついてのルール他）、組織としての承認、関係者への徹底状況等で判断する
（注２）対策現場で当該対策についての文書化がどの程度行われているかを問うもので、ルールに沿った作成、承認、保管の状況や、必要に応じた検索性等で判断する

5. 個別システムに対する本評価モデルの利用場面と利用法の概要

5.1. 個別システムにおける本評価モデルの利用場面

個別の組織あるいはシステムを対象にした場合、このセキュリティ対策評価モデルは、次の 2 通りの利用が考えられる。

- セキュリティ対策の計画策定への利用
- 実施しているセキュリティ対策の妥当性の評価とセキュリティ対策の見直しへの利用

それぞれの利用場面における、本評価モデルの利用の概念を、以下に概説する。

5.2. セキュリティ対策計画時における利用

セキュリティ対策の計画とは、セキュリティ対策としての具体策の検討を行い、実施する対策を決めるプロセスをさす。このような場合、本評価モデルは、対象システムのセキュリティ特性や経営からの当該システムのセキュリティ対策について要求される強度レベルから、セキュリティ対策として検討すべき事項と、そのそれぞれについて対策としてどこまで実施するかについての検討のフレームワークを与えてくれる。

本評価モデルを用いることにより、検討すべき事項を漏れなく知ることができるとともに、検討事項のそれぞれにおいて、対象システムのセキュリティ特性や、経営からのセキュリティについての取り組み方針に照らし標準的な対策を知ることができる。

セキュリティ対策の詳細を決めるにあたっては、本モデルが示すところを基準に、対象システムの特性を入れ、対策への取組みのレベルについて必要な修正を施すことにより、適切な対策を計画を立案することができる。

本モデルを用いたセキュリティ対策の計画プロセスを以下に示す。

5.2.1. 本モデルを用いたセキュリティ対策の計画手順

図 5-1 に、本モデルを用いたセキュリティ対策の計画手順を示す。

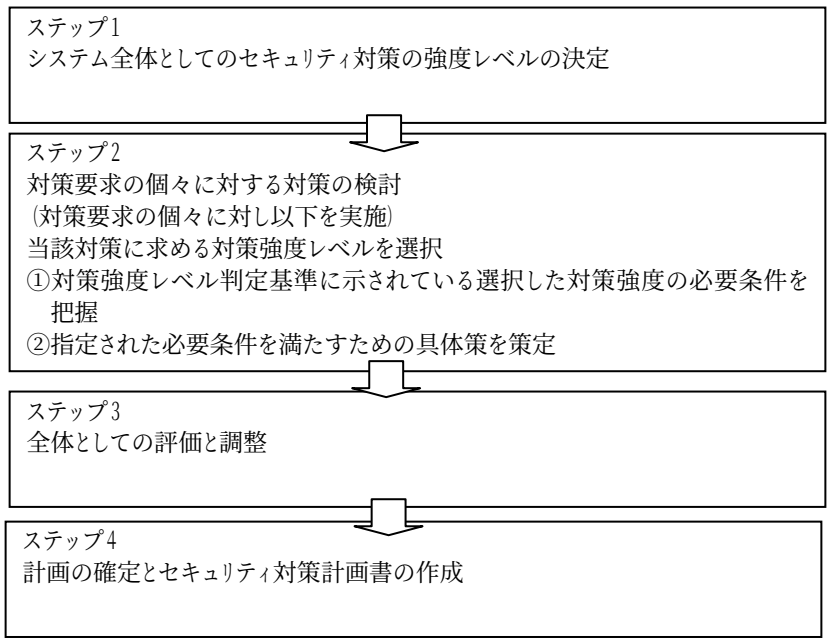

図 5-1 本モデルをセキュリティ対策の計画手順

5.2.1.1. ステップ1：システム全体としての目標とするセキュリティ対策の強度レベルの選択

セキュリティ対策として何をどこまで行うのかの判断は、システム全体に要求されるセキュリティ対策の強度レベルが基準となる。このため、まず、当該システムが目標とすべきセキュリティ対策の強度レベルを選択しなければならない。

目標とすべき対策強度レベルの判定要素としては、表 5-1に示すようなものがあげられる。

表 5-1 システム全体として目標とすべきセキュリティ対策の強度レベルの検討要素

項目	検討すべき事項
1 対象業務の特性	・問題が生じた場合の影響の大きさ －社会的な責任の度合い(広い範囲に影響) －利用者の生命・健康・財産への直結の度合い －取り扱う情報の性格
2 組織における重要性	・事業継続性への影響さ －業務の遂行への影響度合い －組織の信用への直結の度合い
3 システムの運営環境の脆弱性	・組織の運営形態面からの脆弱性 －組織やオフィスの形態(特に分散の形態) －関係者の構成 －業務の運営形態(外部委託の有無やそのレベル) －管理面での文化 ・システムの構成や運用面からの脆弱性 －システムの構成うえの特性 －システムの運用面での特性

5.2.1.2. ステップ2：対策要求の個々に対する対策強度レベルの選択

ステップ1で選択した対象システム全体としてのセキュリティ対策の強度レベルを基準に、個々の対策要求について、選択すべき対策強度レベルを決める。一般には、システム全体に対する対策強度レベルがそのまま適用されるが、システムの特性によって、対策要求によっては強度レベルを上げるべきところや、強度レベルを下げても差し支えないところがあれば、該当する対策要求については、システム全体にに選択した対策要求レベルから、1 ランクは上下にずらすことができる。

5.2.1.3. ステップ3：対策要求の個々に対する具体策の検討

個々の対策要求に対する対策強度レベルの選択ができれば、当該対策強度レベルに定義された達成条件から、個々の対策要求の選択した対策強度レベルを確保するために実施すべきことを、実施すべきことを知ることができる。本モデルでは、この達成条件は、当該対策要求について必要な活動の信頼性で表現しているため、その具体策としては、そのような事項を満足するに足るだけの具体策として、技術的要求については、要求レベルを満足する手段を選び、管理的要求の場合は、要求される精度での実施が担保できるための仕組みの確立等を行わなければならない。

5.2.1.4. ステップ4：ステップ4：全体としての評価と調整

個々の対策要求に対する具体策が策定できたら、これらの対策の集合体が、システム全体としてのセキュリティを目標とする対策強度レベルを満足するかどうか、個々の対策要求への対応に全体から見てバランスを欠くところはないか等についての評価を行う。

全体としての評価のチェックポイントとしては、以下があげられる。

- 個々の対策要求についての具体策は、当該対策要求に指定された対策強度レベルを達成きるか
- 対策要求間で、対策強度に不自然なばらつきはないか
- 結果として、システム全体として要求されている対策強度レベルを実現できるか

セキュリティ対策は、必要以上の要求や計画も実践が伴わず破綻のもととなるので、適切なレベルに設定しなければならない。

5.2.1.5. ステップ5：計画の確定とセキュリティ対策計画書の作成

ステップ3での評価が終了し、全体が目的を達成し、バランスが取れたものになっている確認できた時点で、これらの経緯や結果を、セキュリティ対策計画書にまとめ、経営レベルでの承認を得てセキュリティ対策の計画は完了する。

5.3. セキュリティ対策の評価への適用

5.3.1. セキュリティ対策の評価場面

本評価モデルは、実施しているセキュリティ対策の十分性や問題点の発見にも使用することができる。本モデルを用いたセキュリティ対策の評価場面としては、以下のような場面が考えられる。

- 計画自体の十分性の評価や問題点の把握
- 対策実態と計画とのずれのチェックによるセキュリティ対策の現状についての問題点の把握

前者の、計画自体の十分性の評価と問題点の把握は、計画したセキュリティ対策が対象システムのセキュリティ環境や、経営からのセキュリティについての要求レベルとに照らして過不足な点がないかどうかを見極めるものである。この評価は、計画策定時も行われるが、セキュリティ環境は常に変化するため、その妥当性を維持するためには、定期的あるいは、必要に応じた再評価が必要となる。この評価においては、業界基準等対象システムに対するセキュリティ対策について外部の基準等があれば、これもチェックの指標としなければならない。

この点についての評価は、計画策定時と同じとなる。対策の前提条件が大きく変わり、その結果として、計画自体の見直しが必要とされる場合は、迅速な対応が必要となる。

後者の、対策の実態と計画のズレのチェックは、計画は問題がないとしても、実施上の不備や不手際が見過ごされないようにし、計画したセキュリティ対策が、常に、期待通り機能するようにするためのものである。

5.3.2. セキュリティ対策の評価手順

対策実態の評価は、個々の対策要求について計画で指定した対策強度を維持できているかどうか、また、結果として指定の1ランクあるいは2ランク上の対策がとられ過対策になっていないかどうかを見極めるものである。

この評価は、対策要求別に指定されている対策強度レベル判定基準にそって、実態を評価することにより、当該対策が実態として、どの対策強度レベルに相当するかどうかをチェックすることにより判断することができる。

この評価においては、計画で要求した対策強度レベルの達成条件と示されていることの一つ一つについて実現しているかどうかをチェックすることにより行うことができる。多くの項目において、実現されていないと判断される場合は、1 ランク下のレベルの達成条件をチェックリストに、1 ランク下のレベルは実現されているかどうかのチェックを行う。

また、計画した強度レベルを満足していう場合は、1 ランク上のレベルの達成条件についてチェックを行う。この 1 ランク上の達成条件の実現度合いを見ることにより、実態は 1 ランク上にクリアあるいは近づいているかどうかを知ることもできる。

計画が要求した強度レベルを満足していない場合は、改善措置が必要となる。また、上位の強

度レベルに完全に達している場合は、過対策の場合もあるため、その必要性について再確認することも必要となる。

5.3.3. 個々の対策要求に対する対策強度レベルの評価手順

本モデルでは、個々の対策要求についての強度レベルは図 5-2 に示す手順で決める。

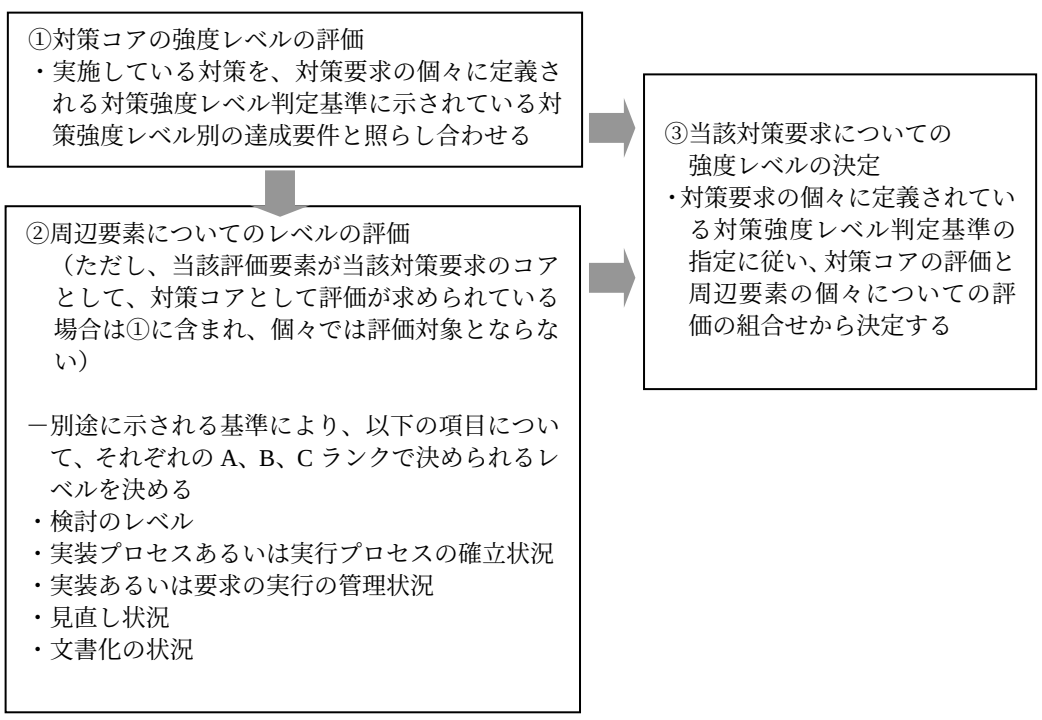

図 5-2 個々の対策要求に対する対策強度レベルの設定基準

5.3.4. セキュリティ対策の実態の評価

セキュリティ対策は多岐にわたることと、日々の業務やシステムの運用･管理に依存していることが多いいため、不手際が入り込んだり、馴れによるずさんな対応等により、そのレベルは低下しやすい。また、セキュリティ対策の強度は、セキュリティ環境の変化とともに変動する。このため、一度評価したとしても、その評価時点での強度レベルが維持できているとは言い難い。このため、定期的に対策の実態を再評価することは欠かせない。

ここでは、定期的あるいは随時に実施すべきセキュリティ対策の実態の評価に、このモデルを用いる場合の手順を示す。

5.3.4.1. セキュリティ対策の実態の評価の意味

セキュリティ対策の実態の評価の狙いは、次の二つある。

- 対策要求単位での、計画に対する実態の十分性の評価と問題点の確認
- 計画したセキュリティ対策そのものの妥当性の十分性

前者の対策要求単位での問題点の確認は、対策要求ごとに対策の実態から、計画した施策が的確に実施されているかどうか、過不足はないかどうかを見るものである。このことにより、指定された問題点を改善することにより、セキュリティ対策を当初計画した強度を維持することができる。

後者の実態としてのセキュリティ対策の十分性の評価は、個別の対策要求に対する現在の強度レベルが、全体として計画時に期待したレベルにあるかどうかをも見るものである。大幅な乖離がある場合は、セキュリティ対策の計画が実態に合わないか、セキュリティ対策の組立てや管理に大きな欠陥があることを示す。

5.3.4.2. セキュリティ対策の実態の評価の手順

図 5-3 に、セキュリティ対策の実態の評価に、本モデルを用いる場合の手順を示す。

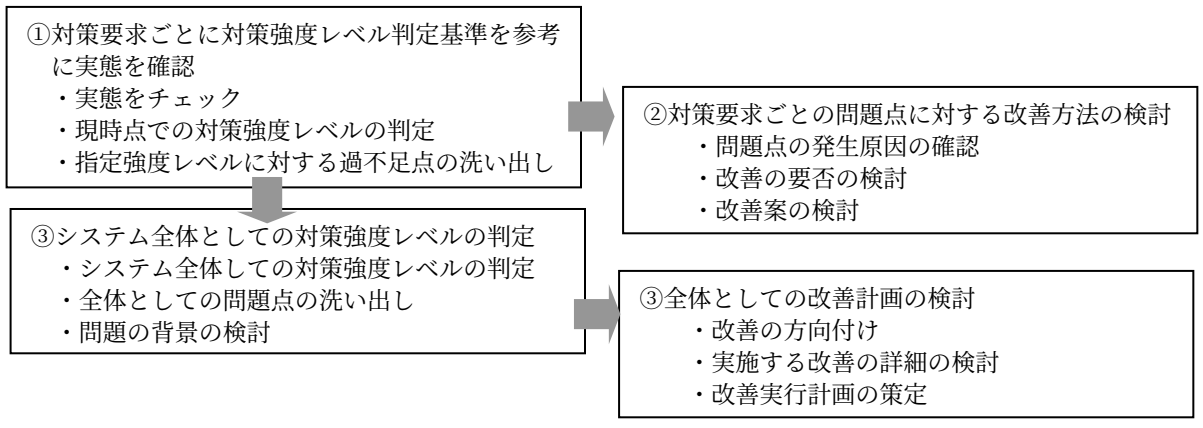

図 5-3 本モデルを用いたセキュリティ対策の実態評価の手順

5.3.4.3. 対策要求の個々についての対策強度レベルの判定

対策要求の個々についての対策強度レベルの判定についての作業は、次の 3 つのステップで行う。

- 対策強度レベル判定基準を用いた実態のチェック
- 現時点での対策強度レベルの判定
- 指定強度レベルに対する過不足点の整理

(1) ステップ1：対策強度レベル判定基準を用いた実態のチェック

当該対策要求に対する対策強度レベルに示されている各強度レベルの判定条件と実態を比較し、実態と合うものをチェックする。この結果に沿って、実態の対策強度レベルを判定する。このとき、その要求の詳細については、対策要求の解説に示されている要求の詳細についての確認を必要とする。

(2) ステップ2：現時点での対策強度レベルの判定

この結果に沿って、実態の対策強度レベルを判定する。

(3) 指定強度レベルに対する過不足点の整理

当該対策要求に対して指定された強度レベルの達成条件と比べ、実態で欠けているところ、および結果として過対策となっている事項について、何がどのように計画よりずれているかを明らかにする。

5.3.4.4. 対策要求ごとの問題点に対する改善方法の検討

個々の対策要求に対する対策強度の判定により、実態の対策強度レベルが計画した対策強度レベルとズレがある場合、および、評価としては対策強度レベルを実現していても、この評価におけるチェックで、十分でない点が明らかになった場合は、計画段階での期待に添うよう、この点について必要な改善を行わなければならない。

対策要求ごとの問題点に対する改善方法の検討は、次の3つのステップで行われる。

- 問題点の発生原因の分析
- 改善の要否の検討
- 改善案の検討

(1) ステップ1：問題点の発生要因の分析

改善を効果的なものにするためには、指摘された問題が発生した背景を把握しなければならない。背景としてあげられるものには、以下のようなものがる。

- 計画の無理
- 現場への展開の不手際
- 管理の不徹底
- 現場の対応能力の欠如

(2) ステップ1：改善の要否の検討

計画との対比で指摘された問題点は、場合によっては、目標とする強度レベルの再設定も、その解として考えられる。したがって、指摘された問題点すべてについて、現場レベルの対策が必要とは限らない。このため、指摘された問題についてどのような方向で望むかについての検討が必要となる。

(3) ステップ3：改善案の検討

問題の背景分析等から、問題点に対してどのような改善を行うかについての詳細を検討する。この検討の対象となることは、以下があげられるが、対策要求によってその対象範囲は異なったものとなる。

- 技術面での見直し
- ルールや実践の管理の仕組み等の見直し
- 対策現場への要求の展開の方法についての見直し
- 要求の実践の監督指導、関係者に意識

5.3.4.5. システム全体しての対策強度レベルの判定

システム全体としての対策強度レベルの判定は、全体としての十分性を俯瞰するためのものである。このシステム全体としてみた場合のセキュリティ対策の強度レベルの判定は、計画に本質的な問題がないかどうか、また、実施に大きな問題がないかどうかの判断をするもので、改善の方向付けをするのに用いる。

システム全体としての対策強度レベルの判定は、次の4つのステップで行われる。

- システム全体としての対策強度レベルの判定
- 全体としての問題点の洗い出し
- 問題の背景の検討
- 改善実施についての方向付け

(1) ステップ1：システム全体としての対策強度レベルの判定

システム全体としての対策強度レベルの判定は、まず、個々の対策要求についての対策強度の判定結果をもとに、対策ドメイン単位での対策強度の算定を行う。対策ドメイン単位の対策強度レベルは、当該ドメインを構成する個々の対策要求の当該対策ドメイン内での重みと、個々の対策要求についての対策強度の判定結果により算定できる。

次に、この結果を用い、個々の対策ドメインの対策全体の中での重みを設定すれば、この重みを用いて、システム全体としての対策強度レベルを算定できる。

(2) ステップ2：全体としての問題点の洗い出し

(1) の作業から、どのドメインがどの程度問題なのかも判定できる。この結果から、セキュリティ対策全体として、どこにどのレベルの改善が必要かが判断できる。

計画した対策強度レベルが、概ね、達成できている場合は、個別の要求ごとの問題点に対する対策だけで済むが、目標とする強度レベルが達成できていないような場合は、この検討は重要となる。

(3) ステップ3：問題点の背景の検討

目標とする強度レベルが達成できていないような場合は、問題点の指摘だけでなく、計画に対し、なぜそのようなギャップができたかについての背景の検討が必要となる。

考えられる問題としては、以下があげられる。

- 計画自体の欠陥

  リスク分析の不備や、当初の計画時点からセキュリティ環境や経営の方針が変わって、計画自体の妥当性が失われたことも計画自体の欠陥の大きな要因としてあげることができるが、組織やシステムの実態に合わない計画は、一般に実践が伴わなく、これも、計画と実態の大きなギャップの元となるため、計画自体の欠陥の一つにあげることができる。

- 計画の実施への展開あるいは管理の不徹底

  計画の対策現場への展開や、技術面での不備や不手際、あるいは、日常の業務運営やシステム運用上でのセキュリティ要求に対する実践の監督指導の欠如によっても、セキュリティ対策の実態は計画から大きくずれる。

5.3.4.6. 全体としての改善計画の検討

最後にセキュリティ対策の全体を見た、改善計画を纏める。この計画策定は、次の3つのステップで行われる。

- システム全体としての改善の方向付け
- 実施する改善の詳細の検討
- 改善実行計画の策定

(1) ステップ1：システム全体としての改善の方向付け

セキュリティ対策の見直しとそれに伴う改善は、多岐にわたるため簡単ではない。このため、必要な改善をタイムリーに効果的に行うためには、改善についての方向付けについての検討が必要となる。

(2) ステップ2：実施する改善の詳細の検討

(1) で定めた全体としての改善の方向付けをベースに、改善の対象となる事項の個々について詳細な改善案の検討を行う。

このとき、従来の対策との継続性や現場での要求の消化能力についての検討を疎かにしないことが肝要となる。

(3) ステップ3：改善実施計画の策定

(2) を踏まえて、どのようなタイミングでどのように改善案を現場に展開するかについての計画を定める。この計画では、以下のようなことを明確にしなければならない。

- 改善の狙い (改善で実現すること)
- 具体的改善内容 (システム、ルール、管理方法、他)
- 対策現場への展開手順
- 実施時期
- 実施責任者

6. 本モデルのその他の活用場面

本評価モデルの利用場面としては、以下をあげることができる。

- 企業等の組織におけるセキュリティ対策の基盤としての利用
- 情報セキュリティ監査のベース
- システムモデル別セキュリティ対策基準の確立およびセキュリティ対策プロファイル作成のベース
- セキュリティ対策の評価･格付けサービスにおける評価の基準のベース
- ネットワーク経由でのサービスの提供におけるセキュリティ面からの公的あるいは自主規制のベース
- サービスレベルアグリーメントにおけるセキュリティ関連事項の指定のベース
- 情報セキュリティに関わるトラブル発生時における責任の分界の判断の尺度
- 情報セキュリティにかかわる保険における保険料や保険金の査定のベース

このような場面にこの評価モデルが用いられることは、この評価モデルがセキュリティ対策の実践における基盤として位置付けられることを示している。

以下に、本評価モデルの適用場面のそれぞれについての考察を示す。

6.1. 企業等の組織におけるセキュリティ対策の基盤としての利用

企業や各種機関等の組織において、必要なレベルの情報セキュリティを確保するためには、対象システムの特性に応じた適切なセキュリティ対策を計画し、計画したセキュリティ対策を的確に実行することが必要である。

本モデルは、以下の点で、企業等の情報セキュリティのレベルの向上に寄与できると考えられる。

- セキュリティ対策の計画検討時のガイド
- セキュリティ対策の実施状況の評価時のガイド

(1)セキュリティ対策の計画検討時のガイド

本評価モデルは、セキュリティ対策として実施すべきことに加え、実施内容を対策強度にリンクして示している。このため、セキュリティ対策の計画立案にあたっては、この評価モデルの対策要求のすべてに対し、適用する強度レベルを検討することにより、対策の詳細についての検討ベースを得ることができる。

このことから、検討すべきことに漏れが生じる可能性が小さくなるとともに、検討はゼロからのスタートでなく、目標とする対策強度を中心とした細かい点の選択により、対策の概要を決めることができるため、検討のスピードアップと検討内容の水準を平均以上のものにすることが期待できる。後は、ここのシステムの特性にあわせ、細部を決めるだけとなる。

本評価モデルを用いたセキュリティ対策の計画作成プロセスのイメージを、図 6-1 に示す。

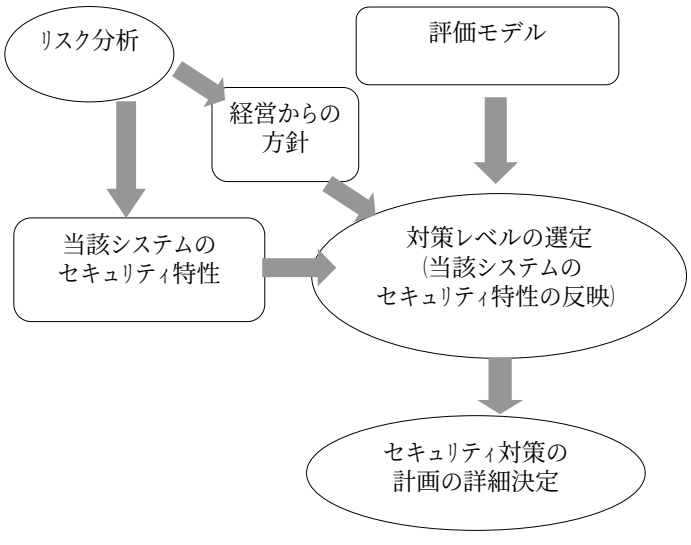

図 6-1 評価モデルを用いたセキュリティ対策の計画立案プロセス

(2)セキュリティ対策の実施状況の評価時のガイド

実施しているセキュリティ対策については、定期的にその十分性についてのチェックが必要となる。この評価モデルでは、対策要求ごとに強度判定条件が示されているため、これをチェックリストに、現状を評価すれば、計画に対する過不足や、システムに求められるセキュリティについての要求の現状と対比しての過不足を具体的に知ることができる。

このことを活用すれば、システムのセキュリティを常に適切なものとして維持することが期待できる。

6.2. 個別システムの情報セキュリティ監査のベースとしての利用

ネット社会の進展につれて、ネット経由でのサービスの提供や、企業間でのネットを介したリアルタイムコラボレーションは、益々拡大する。このため、情報セキュリティにかかるトラブルは、自社だけに止まらなくなる。そして、これらは訴訟等に発展する可能性も拡大している。

このため、企業等の組織にあっては、自社の情報セキュリティが必要とされるレベルにあることを確認するための、自社あるいは第三者の監査を求める傾向は、今後さらに拡大するものと思われる。

このような場合、この監査が監査人のスキルに依存せず客観的に行われ、その結果を信頼できるものにするためには、監査基準の確立が必要となる。本モデルは、監査目的で構築されたものではないものの、セキュリティ対策の実態やその十分性の評価ができるだけでなく、後述のように同種のシステムに対する平均的な水準を示すものにもなっているため、この監査における評価尺度の一部として使用することも可能であると考える。

6.3. システムモデル別セキュリティ対策基準およびセキュリティ対策プロファイル定義の基盤としての利用

6.3.1. システムモデル別セキュリティ対策基準

対象業務と規模が同じようなものであれば、個々のセキュリティ要求事項に要求される強度レベルは、ほぼ同一となる。そこで、対象業種ごとに代表的な業務と、例えば、大、中、小に分けたシステム規模を組合せた標準的なシステムモデルに対しては、セキュリティ要求事項の個々について標準的に指定すべき強度レベルを示すことは可能となる。そして、その集合は、対象となるシステムに求められるセキュリティ対策の強度基準と見ることができる。

システムモデル別に、要求する強度レベルがセキュリティ要求事項単位に示されたセキュリティ対策基準が確立されれば、個別システムにおけるセキュリティ対策の計画の作成や現状の評価にあたってのチェックのベースが与えられることになる。

6.3.2. システムモデル別セキュリティ対策プロファイルの作成への応用

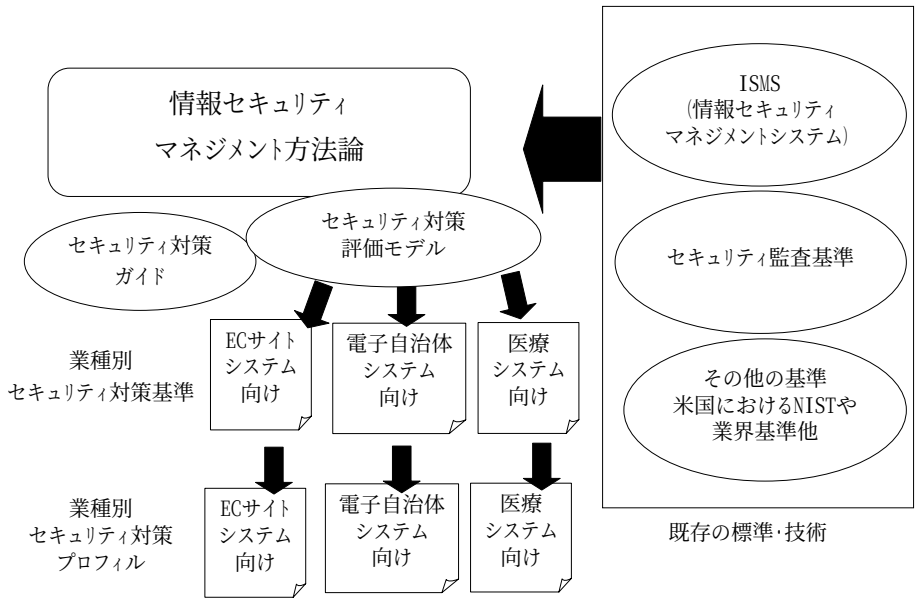

図 6-2 評価モデルとシステムモデル別のセキュリティ対策基準、セキュリティ対策プロファイルの関係

前節であげたシステムモデル別のセキュリティ対策基準が定義されていれば、その要求を実現するための標準的な施策を具体的に示せば、システムモデルごとの標準セキュリティ対策のプロファイルができる。このようなセキュリティ対策プロファイルが出揃えば、個々のシステムは、該当する

システムモデルのプロファイルに、対象システムの特性を加味する修正を加えるだけで、適切なセキュリティ対策を計画できる。前節に示すセキュリティ対策基準が、セキュリティ対策の目標の設定とその十分性の評価を支援するのに対し、標準セキュリティ対策プロファイルは、セキュリティ対策の計画作成を支援するものとなる。

6.4. セキュリティ対策の評価・格付けサービスにおける評価のベースとしての利用

今後、ネットワーク経由でサービスを提供するシステムや、自社あるいは自家用のネット利用システムのセキュリティレベルについての評価や格付けサービス、さらには認証制度も本格化してくるものと想定される。利用するシステムのセキュリティのレベルについて、第三者の評価を得ることができるこのようなサービスが普及し、活用されるようになるためには、情報セキュリティの専門家だけでなく、システムの構築や運用にかかわる多くの人やネットの利用者にも、広く受け入れられるセキュリティレベルについての評価尺度が確立していることが必要となる。ここに紹介したセキュリティ対策の評価モデルは、このようなサービスにおけるセキュリティレベルの評価基準の検討におけるベースにもなると考える。

このため、自社のセキュリティ対策がどのレベルであるかを、一般公開しないまでも、ビジネスの関係者に示す必要も増えてこよう。

6.5. ネットワーク経由でのサービスの提供におけるセキュリティ面からの公的あるいは自主規制の基盤としての利用

政府機関のシステム、社会のインフラと言えるシステム、利用者の生命、健康、財産に直結するようなシステムにおけるシステムのトラブルは、ネット社会に不安をもたらすため、十分な対策と、トラブルが発生しても被害に結びつかないような措置が講じられていなければならない。このようなシステムに対しては、そのセキュリティ対策は、社会が納得できるレベルのものでなければならない。このことを実現するためには、このようなシステムがそのサービスを提供するに当たっては、そのセキュリティのレベルについて第三者の評価認証を必要とするような公的あるいは業界単位での自主規制の導入も必要と思われる。このような制度は、もちろん、今後の検討課題ではあるが、もしこのような制度の検討が俎上にあがるような場合は、その合否ラインの設定や評価のポイントが、社会的な認知を受けたものでなければならない。

本モデルが成熟したものになれば、合否ラインを決めたり、客観的な評価を実現するための尺度となりうるはずである。

6.6. サービスレベルアグリーメントにおけるセキュリティ関連事項の指定のベースとしての活用

ネット経由でのサービスの提供や、ネットを介した企業間のコラボレーションの拡大は、サービスの提供やコラボレーションに生じた紛争解決の準備として、サービスの提供やコラボレーションにかかわる契約に、情報セキュリティについての双方の義務の明示の必要性を拡大する。これらは、契約におけるサービスレベルアグリーメントに含まれるべき事項であるが、現時点では、情報セキュリティについてのそれぞれの義務をどのようなレベルで記述すべきかについて、標準的なガイドは確立していない。このため、抽象的な記述に止まっており、実際に問題が生じた時の、その有効性については相当に疑わしい。

本モデルは、セキュリティ対策として、“具体的に何をどこまで行うのか”を判断する尺度を与えているため、このモデルを活用することにより、サービスレベルアグリーメントについての記述をより有効なものにするための基盤となりうると考える。

6.7. 情報セキュリティに関わるトラブル発生時における責任の分界の判断の基盤としての利用

ネットを介したサービスや、企業間のネットを介したリアルタイムコラボレーションにおける情報セキュリティに関わる事故により被害が生じ、関係者間で紛争が生じた場合、その責任の分界（＝損害賠償）等についての紛争解決が円滑に行われるためには、それぞれがセキュリティ対策についてどの程度適切に取組んでいたかが分岐点になることが考えられる。

この場合、それぞれがセキュリティ対策として“何を、どこまで行っていた”が、客観的に把握できることも、またそれが、世間一般の水準に達していたものかどうかの判断の基準も必要となる。このモデルは、そのコンセプトから、このような要求に対しても、評価尺度として用いることができると考えられる。

6.8. 情報セキュリティにかかわる保険における保険料や保険金の査定の基盤としての利用

今後、情報セキュリティにカラムトラブルについての保険が普及も必要となろう。ただし、情報セキュリティに関する保険が普及するためには、保険料の考え方や、事故時の保険金の査定の方法についてのコンセンサスの確立も必要となる。これらを解決するためには、

- 保険料の査定の元となる想定されるトラブルに対する被害の想定方法
- 保険料の設定の元となる被保険企業におけるセキュリティ対策の査定方法
- 被害発生時の保険金の査定もベースとなる過失範囲の査定方法

等の確立が必要となる。

これらについては、現在、それぞれの保険会社がさまざまな工夫を凝らしているが、標準となるような基盤は与えられていない。

本モデルは、個々の評価事項に対して対策強度が定義されているため、これを情報セキュリティ保険における被保険企業のセキュリティ対策についての査定の基準に適用することも期待できる。

7. 今後の課題

以上、情報セキュリティ対策評価モデルのコンセプトと、その応用について述べてきた。本評価モデルが期待に応える形で実用化され、多くのシステムのセキュリティレベルの向上に寄与するようになるためには、以下のような課題の克服が必要となる。

- 評価モデルとしての完成度の向上
- 実用環境の整備

7.1. 評価モデルの完成度の向上

この評価モデルが、広く用いられるような成熟したものになるためには、まだ、以下の点について相当の努力が必要となる。

- コンセプトのブラッシュアップ
- 対策要求事項の組み立ての完成度の向上
- 個々の対策要求に定義する対策強度判定基準の定義の完成度の向上
- 利用ガイドの整備

7.1.1. コンセプトのブラッシュアップ

現時点では、まだ外観的なコンセプトを示しているに過ぎない。この評価モデルが広く受け入れられるためには、コンセプトレベルでもまだシステムとしての総合的な対策強度の評価への拡大他のブラッシュアップが必要となる。

現時点では、対策要求単位に対策強度の判定基準を示しているに過ぎないが、いずれは、システム全体として、あるいは不正アクセス対策、ウイルス対策、情報の保護、アプリケーションの脆弱性排除等の対策ドメインや対策テーマ単位にも、包括的な対策強度を評価できるようにすること要求されることになろう。

このため、このようなモデルは、個々の対策要求に対する対策強度の評価が、システム全体としてのおおよその対策強度や、対策テーマや対策ドメインごとの対策強度の評価に結びつけられるようにすることも考えておくべきである。このことを実現するためには、対策要求の個々に対する対

策強度を対策テーマや対策ドメイン単位の対策強度に結びつけるとともに、対策ドメインや対策テーマ単位の対策強度がシステム全体としての対策強度にどのように結びつくのかという点についての分析と、評価の展開の方法論の研究が必要となる。

7.1.2. 評価事項の組立ての完成度の向上

評価モデルの要である対策要求の体系化についての考え方や、個々の対策要求の設定基準は、まだまだ議論するところが多い。本報告書に示す対策要求の組み立ては、まだまだ未熟なものであり、新たな議論のたたき台を示しているにすぎない。

まず、対策要求の組み立てについての考え方にコンセンサスが得られるようになれならない。特に議論を要するポイントしては、以下があげられる。

- 分離と統合
- 網羅性の取扱い
- 技術的な要素の取扱い
- 職務区分との整合性
- 脅威対応の対策と、多くの施策を統合するシステム構成論的なものとの 2 重構造になっているところの扱い

分離と統合とは、一つの対策要求は一般にコアとなる活動とその周辺活動で構成されるが、そのそれぞれ独立の要求としてあげるか、または周辺活動をコアの活動に含めて要求するか、周辺活動をいくつかにまとめたものとして要求するかといった問題である。対策が目指すことの性格により考えなければならない問題であるが、原則の確立は必要となる。今回提示されている対策要求の組み立ては、この点について明確な指針に沿ったものとは言い難い。

また、網羅性の取扱いは、対策対象の個々のあるいは対象グループごとに対策の考え方を変えるべきケースにおいては、実際は別個な対策要求としてならないが、すべてに同じ対策方針が適用されるようなケースでは、一つの対策要求の対策強度の問題と扱うこともできる。このような性格を持つ網羅性についての取扱いについても明確にしなければならない。

技術的な要素については、対策要求へのブレークダウンをどのレベルまで考えるべきかについての議論が必要となる。関係する技術によって異なってくるものではあるが、原則の確立も必要となる。さまざまなケースから一般原則を探し、その結果から対策要求を見直すアプローチになろう。

職務区分との整合性とは、対策要求が対策現場の実務に即したものになるようにするためには、異なる部門または職務が担当すべき活動が一つの要求に纏められていないようにしなければならない。したがって対策要求はの組み立ては、この点からも精査されなければならない。

ネットワークアクセスの制御についての要求は、システム構成についての要求を含んでいる。しかし、システム構成は信頼性の確保やウイルス対策や情報の保護他の要求をすべて満たすものでなければならないため、ネットワークアクセスの制御についての要求とシステム構成についての要求は独立のものとして扱わなければならない。このように対策要求がお互いに関連するものは少なくない。最後の課題は、このような対策要求間の関連をどのように扱えばいいかという問題であり、

これからの検討課題としてそのまま残されている。

7.1.3. 個々の対策要求に指定する対策強度判定基準の完成度の向上

個々の対策要求に指定する対策強度の判定基準の指定が広く受け入れられるためには、対策強度についてのコンセプトと強度判定の論理の確立、第 4 章に示した評価要素の個々に対する強度評価の考え方、特に技術的な要求事項に対する強度評価の有り方等、まだ議論すべきことは多い。

また、対策強度判定基準の定義が成熟したものになるためには、個々の要求に対する強度の分離論だけでなく、評価事項相互間での強度のバランスが取れていなければならない。

個々の対策要求に指定する対策強度の判定基準の完成度の向上には、これらについての議論を踏まえ、試案の作成、専門メンバーでの審議、パブリックコメントの収集とその反映、適用実験によるフィードバック等が必要となる。これは膨大な作業であり、一気にレベルの高いものになることは期待できないが、一歩一歩進めなければならない。この評価モデルの完成度の向上に取組む関係者の皆様の継続的な努力を期待するものである。

7.1.4. 評価モデルの利用ガイドの整備

本評価モデルは、使用されながら成長するものと考える。このため、本評価モデルは使い易いものにならなければならない。このためには、前節までに示したモデル本体の完成度の向上と平行して、本モデルの利用者が容易にこのモデルを使いこなせるようにするための利用ガイドの整備が必要になる。

このガイドに含まれるものとしては、以下があげられる。

- 適用要領
- 利用にあたって使用するドキュメントの様式

7.2. 実用環境の整備

評価モデルが実用性の高い成熟したものになったとしても、その実用環境が整備されなければ、広く使われるものになりえない。そして、実際に広く使われなければ、継続的なセキュリティ環境の変化に対するモデルの有効性の維持のための努力の継続も困難になり、このモデルは消滅しなければならなろう。

このモデルが成熟したものであるという前提で、広く実用に供されるようにするためには、以下のような施策の展開が必要となる。

- 関係者間でのこのモデルの存在とその有効性についての周知の確立

- 本モデルの有効性の維持を確保するためのスキームの確立
- ニーズとマッチした形での多くの場面での本モデルの利用が必須な場面の創出

7.2.1. 関係者間でのこのモデルの存在とその有効性についての周知の確立

このモデルがその使用が期待されるところで実際に使用されるためには、多くの関係者に、その有効性、実用性が周知されてなければならない。このモデルの存在とその有用性について周知が求められる対象としては、以下があげられる。

- 企業、機関等のシステム運営組織および業界団体
- システムベンダーおよびシステムコンサルタント
- セキュリティサービス関連機関（ISMS 認証機関他）
- セキュリティサービスベンダーおよびセキュリティコンサルタント
- システム監査機関
- 保険業界
- 法曹界
- 大学等の研究機関における情報セキュリティ担当部門

さまざまな周知拡大の手段が考えられるが、最も効果的な手段は、以下のようなものになろう。

- 開発段階からの参画
- 有効性の維持活動への参画
- システムベンダーおよびセキュリティサービスベンダーにおけるサービス提供過程での活用
- 本モデルの参照が必須な場面の創出
- セキュリティ実践教育のなかでの紹介

7.3. 本モデルの有効性の維持を確保するためのスキームの確立

継続的に発生する新しいプラットフォームやセキュリティ技術の登場等によるシステム構築環境の変化や、新しい脅威の発生にともなう情報セキュリティ環境は、セキュリティ対策への要求や、要求や実現手段を常に変へゆくものと考えなければならない。

このため、評価モデルのベースとなっている“対策要求“および“個々の対策要求に指定する対策強度判定基準“は、最低でも年１回、必要に応じては、随時、環境の変化の応じた改訂を加えなければ、その時点で、このモデルの有効性は失われることになる。

このため、このモデルの有効性の維持のための体制を中心とした恒久的な運用スキームの確立が必要となる。考えられるスキームのイメージを、図 7-1 に示す。このスキームにおいては、評価モデルの維持管理母体を“セキュリティ対策評価モデル管理機関”と呼んでいる。セキュリティ対策評

価モデルの実効性の維持の作業は、高度に専門的なものであるため、専門家集団からなる‘セキュリティ対策評価モデル検討委員会“を付属させおく必要がある。管理機関はこの検討委員会の検討結果にもとづきセキュリティ対策評価モデルを発行することと、ユーザでのその利用を支援することが主なタスクとなろう。

また、このスキームにおけるセキュリティ評価モデル管理機関とセキュリティ対策評価モデル検討委員会のタスクを、表 7-1 に示す。

管理機関や検討委員会をどのように形成するかは、この評価モデルの有用性が認知された後のこれからの議論になろう。

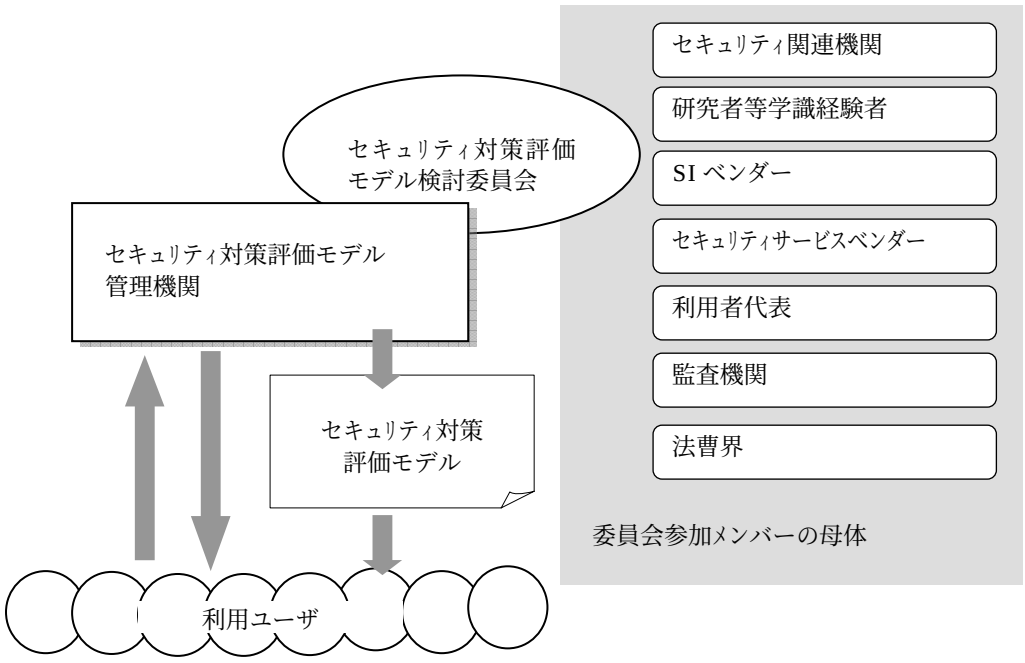

図 7-1 セキュリティ対策評価モデルの運営スキームのイメージ

表 7-1 セキュリティ対策評価モデルの主要運営機関のタスク

主要機関	基本タスク
セキュリティ対策評価モデル管理機関	･セキュリティ対策評価モデルの発行 ･関連機関との連携 ･実証実験や実用からのセキュリティ評価モデルの評価まとめ ･セキュリティ対策評価モデルについての周知、利用促進 ･セキュリティ対策評価モデルの利用指導 ･利用者とのコミュニケーション
セキュリティ対策評価モデル検討委員会	･セキュリティ対策評価モデルの実効性他の評価作業 ･セキュリティ対策評価モデルの年次更新の検討 ･セキュリティ対策評価モデルの問題点の分析と改善の提案

7.3.1. 本モデルの有効性の維持を確保するためのスキームの創出

本モデルがその有効性を維持するため必要とする多大な努力を継続させる力は、本モデルがネットワーク化する社会の中で、不可欠のベースとしての地位を確保しなければならない。この評価モデルが、このような位置付けにする演出としては、以下のような場面での使用が広がることと考える。この評価モデルの有用性についてのコンセンサスが得られた段階で、このような使用についての推進を行うことも必要となろう。

- 業界・業務別セキュリティ対策基準およびセキュリティ対策プロファイルのベースとしての使用の拡大
- ネットワーク経由でのサービスの提供におけるセキュリティ面からの公的あるいは自主規制が登場した場合における審査基準のベースとしての使用
- 情報セキュリティ監査の普及とこの監査におけるチェック・評価項目作成のベースとしての活用
- ネットワーク経由でのオンラインサービスの提供や、企業間でのネットワークコラボレーションについての契約に際してのサービスレベルアグリーメントにおけるセキュリティ関連事項の指定の普及と、このような場合におけるサービスレベルを規定するベースとしての使用
- 法曹界における情報セキュリティに関わるトラブル発生時における責任の分界の判断の尺度としての使用の拡大
- 情報セキュリティにかかわる保険における保険料や保険金の査定のベースとしての使用の拡大

第2部
対策要求事項の解説

1. マネジメント･ビユー

1.1. セキュリティ対策推進基盤の確立

1.1.1. セキュリティマネジメント環境の整備

Ma1.1	経営レベルのセキュリティポリシーの確立

【主旨】

情報セキュリティは、組織や関係する情報システムの運営にかかわる多くの関係者が一体となったセキュリティ対策にかかる諸施策ついての継続的な努力があって始めて達成されるものである。

情報セキュリティを目標とするレベルで実現するための第一歩は、組織におけるセキュリティ対策をどのような考えで、また、どのような方法で実施するかについて、関係者に共通の基盤を与えるための、組織の運営にかかわる経営レベルでのセキュリティポリシーが確立し、関係者に周知されていなければならない。

【対策のポイント】

(1) 適切なトップレベルのセキュリティポリシーの確立

情報セキュリティの確保についての経営レベルでの取組方針を示すものとしてのトップレベルのセキュリティポリシーとしては、以下が満たされていなければならない。

- 以下に示すような必要事項の明示
  - ･情報セキュリティの経営上の位置付け（目的）
  - ･守るべきものの大枠（セキュリティ対策が目指すもの）
    - －保護の対象とすべき組織内外に提供しているサービス、情報資産、システム資産、施設･施設等のと、それぞれに対す必要となる保護（セキュリティ対策の意味）の大枠
  - ･セキュリティ対策として求めるレベルの大枠（実現すべきこと）
    - －保護の対象の組織内外に提供しているサービス、情報資産、システム資産、施設･施設等のと、それぞれに対す必要となる保護（セキュリティ対策の意味）のレベル（強度）の大枠
  - ･セキュリティ対策の組立ての大枠
    - －保護を実現するための対策の集合であるセキュリティ対策の対策ドメインと相互の関係
  - ･セキュリティ対策の予算の考え方
  - ･推進体制の大枠
    - －組織的な対策推進の仕組み
    - －外部パワーとの利用についての方針
- 内容の妥当性

トップレベルのセキュリティポリシーで宣言されていることは、以下を満足するものでなければならない。

・対象組織および関連システムとの整合性（対策レベルの要求の妥当性）

－想定されるリスクに対する経営レベルでの経営レベルでの対応方針との整合性

－組織の運営形態との整合性

－対象業務ならびに業務の運営形態との整合性

－対応情報システムとの整合性

(2) トップレベルのセキュリティポリシーの位置付けの確立

トップレベルのセキュリティポリシーは、情報セキュリティの確保が経営課題であることを組織内外に示すとともに、セキュリティ対策の方向付けをするという役割を果たせるよう、その位置付けが明確でなければならない。このためには、以下が必要となる。

- 経営陣による承認・発行
- 社内への告知
- 必要と認めた場合における社外への告知

(3) 関係者への周知

トップレベルのセキュリティポリシーは、組織内に徹底していなければならない。周知を徹底させるためには、以下のようなことも必要となる。

- 関係者の周知徹底のための文書やポスター等の作成と配布あるいは掲示
- さまざまな機会における関係者間での、トップレベルのセキュリティポリシーの再確認や意見の交換
- 関係者の周知のレベルについての確認

(4) 必要に応じた見直し

問題が生じた場合はその都度、できれば定期的に以下のついての見直しも必要となる。

- トップレベルのセキュリティポリシーにおける指定事項
  ・指定事項の過不足
  ・指定内容の現状との整合性
  ・関係者への周知の方法

【対応 ISMS コントロール】

3.1.1 情報セキュリティ基本方針文書

Ma1.2	セキュリティ対策の組立ての確立

【主旨】

セキュリティ対策とは、情報セキュリティを確保するためのさまざまな活動を総称するものである。これらは、相互に関連するだけでなく、その実践を要求される部署も複数にわたる。このため、これ

らが有機的な連携を果たし、所期の目的を果たすためには、要求される個々の施策の役割や位置付けが明示されなければならない。

本要求は、セキュリティ対策の全体像を明確にするため、要求のポイントに示すような事項を明確にすることを要求するものである。

【対策のポイント】

- セキュリティ対策を形作る施策の組立ての明確化

セュリティ対策の組立てとして明示すべき事項としては、表 1-1 に示すようなものがあげられる。

表 1-1 セキュリティ対策の組立てとして明示すべき事項

区分	セキュリティ対策の組立てとして明示すべき事項
1 全体像	・本モデルの対策要求の組み立てに示すようなセキュリティ対策の体系（各ビューの関係や、各ビューを構成する対策ドメインの体系的な明示が必要）
2 セキュリティ対策の構成要素とその個々の関連	・各対策ドメイン間の役割分担と連携の大枠 ・管理の対象となる対策テーマ（モデルの対策要求の相当）とそのそれぞれが目標とする対策強度レベル

なお、これらは以下を満足するようなものでなければならない。

・経営レベルのセキュリティポリシーとの整合性の確保

・リスク評価との整合性

・対象組織の運営形態との整合性の確保

・対象システムの構造や運用形態との整合性の確保

- セキュリティ対策にかかるマネジメントのフレームワークの確立

セキュリティ対策の計画やその確実な実行を実現するためには、多岐にわたる対策それぞれに適切な管理が欠かせない。セキュリティ対策にかかるマネジメントのフレームワークとは、この管理をどのように実現するかの大枠を示すものである。セュリティ対策にかかるマネジメントのフレームワークてとして明示すべき事項としては、表 1-2 に示すようなものがあげられる。

表 1-2 セキュリティ対策にかかるマネジメントのフレームワークとして示すべき事項

区分	セキュリティ対策にかかるマネジメントのフレームワークとして示すべき事項
1 セキュリティ対策にかかるマネジメントの対象	・セキュリティ対策の計画や計画した対策の確実な実行を実現するためにマネジメントすべき事項の洗出しと体系化
2 必要なマネジメントの仕組みの大枠	・マネジメント対象事項に対する責任体制（責任を持つべき立場や部門等）の大枠 ・対象区分ごとの管理の仕組み（管理の実施要領他）の大枠

【対応 ISMS コントロール】

ISMS には、明示的に本要求に対応するものはない。

Ma1.3 セキュリティ対策を推進するための組織的な仕組みの確立

【主旨】

セキュリティ対策は、さまざまな活動の集合体であり、多くの関係者の総合力に依存している。このため、計画したセキュリティ対策が期待通りに機能するようにするためには、セキュリティ対策の実践を可能にする組織的な枠組みの確立も必要となる。

本要求は、セキュリティ対策の計画や実践を統括するための組織的な枠組みの確立のため、対策のポイントに示すような事項の実践を求めるものである。

【対策のポイント】

(1) 経営陣の責任および関与の範囲の明確化

経営陣の情報セキュリティについての責任ならびに関与の範囲に関し、検討すべき事項としていは、以下があげられる。

- 経営陣の情報セキュリティについての責任の明確化
- 経営陣がどのような形でセキュリティ対策の推進に関わるかを示す経営陣の関与の仕組みの確立
- 経営陣への情報セキュリティの確保にかかる責務の周知

(2) セキュリティ対策を推進するための組織横断的な連携の仕組みの確立

セキュリティ対策の実践には多くの部門がかかわるため、セキュリティ対策の計画作成にも、計画したセキュリティ対策が有機的に機能するようにするためにも、組織内の各部門の連携は欠かせない。これらの連携を効果的にするためには、以下のような、セキュリティ対策を推進するための組織横断的な連携を行うための組織的な仕組みの確立が必要となる。

- 情報セキュリティ委員会等の組織横断的な推進母体の確立
- 関係部門間の会議の開催等の意識合わせや活動の整合性確保のための仕組みの確立
- 報告や情報の管理等の情報共有の仕組みの確立

(3) セキュリティ対策推進部署の責任の明確化

セキュリティ対策としての諸施策の推進担当者の、担当する対策についての責務は明示されていなければならない。その責務を明確にすべき推進担当者は、組織の形態ややセキュリティ対策の組立てや進め方によって組織ごとに異なるものの、一般には以下のようなものがあげられる。

- 組織全体としての情報セキュリティ推進責任者
- セキュリティ対策テーマ(注)ごとの実施責任者

(注) ここで言うセキュリティ対策テーマとは、セキュリティ対策の組立てで宣言された、別個に管理される対策群を指す。不正アクセス対策、ウイルス対策、行情報の保護等々となる。

【対応 ISMS コントロール】

4.1.1 情報セキュリティ委員会

4.1.2 情報セキュリティの調整
4.1.3 情報セキュリティ責任の割当て
4.1.6 阻止機関の協力

Ma1.4	関係者の責任の明確化と関係者への周知

【主旨】

セキュリティ対策は、さまざまな活動の集合体であり、多くの関係者の総合力に依存している。このため、計画したセキュリティ対策が期待通りに機能するようにするためには、要求されたセキュリティ対策の実践を受け持つ者が、それぞれの責務が明確に認識していることが不可欠となる。

【対策のポイント】

(1) 社内各部門の情報セキュリティについての責任の明確化

これは、業務現場やシステムの運用現場等の職場において、セキュリティ対策の一環としてなすべきことや、本来の職務の遂行上あるいは職場での日常的な行動において、情報セキュリティに関し守らなければならないことが確実に行われるようにするための各職場の責任を明らかにすることを求めるものである。

明確にすべきこととしては、以下があげられる。

- 管理部門の責任
- 各業務現場における責任
- システム企画･開発部門の責任
- システム運用部門の責任
- 設備の管理部門の責任

(2) 関係者へのそれぞれのセキュリティ対策にかかわる責務についての教育の実施

(3) 関係者へのそれぞれのセキュリティ対策にかかわる責務についての認識の確認の実施

【対応 ISMS コントロール】

4.1.1 情報セキュリティ委員会
4.1.2 情報セキュリティの調整
4.1.3 情報セキュリティ責任の割当て

Ma1.5 関係者のセキュリティ対策推進能力の確保

【主旨】

セキュリティ対策の実践は、組織のさまざまな部署における多くの者がかかわる。日常の業務の流れの中に含まれるものもあれば、専門的なスキルを必要とするものもある。いずれにせよ、関係する者のすべてにおいて、それぞれが実践しなければならないことについて、十分な理解と実行に必要なスキルを有していなければならない。

このことを実現するためには、それぞれがセキュリティ対策の実践で必要とする知識やスキルを明確にし、これらについての教育を行うとともに、それぞれの習得状況の確認も必要となる。

【対策のポイント】

(1) セキュリティ対策の実践に関し、関係者のそれぞれに必要とされる知識やスキルの把握

(2) 関係者のそれぞれに対するセキュリティ対策の実践に必要な知識やスキルの提示

(3) 必要な教育の実施

必要な教育を効果的に行うためには、以下も必要となる。

- 教育計画およびカリキュラムの確立
- 教材の整備や指導員の確保
- 計画に沿った教育の実施
  - ・定期的な教育の実施
  - ・人事異動やセキュリティ対策の変更に伴う臨時教育の実施

(4) 関係者のセキュリティ対策推進能力のチェックの実施

必要な知識の提示や教育を行っていても、関係者が必要な知識やスキルを習得しているとは限らない。このため、定期的に関係者のセキュリティ対策推進能力のチェックを行うことも必要となる。

【対応 ISMS コントロール】

6.2.1 情報セキュリティ教育および訓練

Ma1.6 セキュリティ対策予算の確保とその適切な執行

【主旨】

セキュリティ対策の実施にはコストがかかる。計画したセキュリティ対策にかかる諸施策が機能するようにするためには、対策の実践に必要な予算は確保されなければならない。

このためには、情報セキュリティの確保に必要となる諸費用が、経営コストの中で意識され、適切に審議、確保され、適切に執行されるようになっていなければならない。

本要求は、セキュリティ対策予算の確保とその執行を適切に行うために必要となる、対策のポイ

ントに示すような事項の実践を求めるものである。

【対策のポイント】

(1) セキュリティ予算の管理の仕組みの確立

セキュリティ対策予算の確保や、確保した予算の執行を適切なものとするためには、以下が確立していなければならない。

- セキュリティ予算の枠組みの明確化

  セキュリティ対策予算を適切なものとするためには、セキュリティ対策の実践に、どこにどのような費用が発生するかが明確にされていなければならない。このため、以下を明確にするセキュリティ予算の枠組みが確立していることが必要となる。

  ・予算として管理すべき費用項目
  ・それぞれの費用項目の算定基準
  ・それぞれの費用の使用についての基本的な考え方や予算額の大枠

- セキュリティ予算審議および予算の執行を管理する仕組みの確立

  セキュリティ対策予算の計上、審議、決定、さらには執行の管理を組織的に行うためには、これらについてのプロセスや、責任体制が確立していなければならない。検討事項としては、以下のようなものがある。

  ・予算の提案手順
  ・予算の審議および決定手順
  ・予算の執行管理の仕組み

- セキュリティ予算の評価方法の確立

  セキュリティ対策予算が継続的に適切に確保され、その執行が適切であるようにするためには、予算の使用についての評価も適切に行われなければならない。このためには、以下の確立も必要となる。

  ・予算の評価基準
  ・予算評価の実施手順

(2) 適切なセキュリティ対策予算の確保とその適切な執行の実践

- セキュリティ対策予算の確保

  セキュリティ対策予算は、以下のような形で確保されることが望ましい。

  ・予算は必要なレベルで細分化されていること
  ・計画したセキュリティ対策の実践に必要な予算が計上されていること

- セキュリティ予算の執行についての管理の実践
- セキュリティ予算の評価の実施

【対応 ISMS コントロール】

ISMS には、明示的に本要求に対応するものはない。

【参考】

- セキュリティ対策予算として計上すべき費用項目

表 1-3 セキュリティ対策予算として計上すべき費用項目

区分	費用項目	費用項目例
セキュリティ対策のマネジメントコスト	社内関係者の工数コスト	・セキュリティ計画作成や実行管理の人員や工数のコストへの換算値
	外部委託費	・セキュリティ対策にかかるコンサルタント費他
セキュリティ対策の展開コスト	設備費	・保護領域の構築のための隔壁や入退室管理のための設備費 ・装置の安全保護のための設備費
	セキュリティツールの導入費用	・ファイオアウォールやウイルス対策ソフト、ネットワーク監視システム等の導入費
	セキュリティ運用コスト	・セキュリティ対策の計画や実行および実行の管理の人員や工数のコストへの換算値
	業務面でのオーバヘッド	・主に業務現場におけるセキュリティ対策に関連して必要となる手間のコストへの換算値
	外部委託費	・セキュリティ監視の外部委託費 ・事故処理への応援依頼費他

- 現時点では、セキュリティ対策予算は、システムの導入日やシステムの運用費の中に含まれ一括管理されているのが一般で、セキュリティ対策にかかる経費を、一つの管理対象の費用項目にしている組織は少ないと見られる

1.1.2. 経営レベルでのセキュリティ要求の明確化

Ma2.1	対象組織･情報システムのセキュリティ特性モデルの作成

【主旨】

セキュリティ対策を適切に計画し、計画したセキュリティ対策を適切に実践するためには、対策の対象となる組織の運営形態や対象業務、さらには対応する情報システムの形態等から、守るべきものがどのような形で存在し、これらにどのような脅威が存在するかが適切に把握されていなければならない。

このためには、要求のポイントに示すような事項を示すセキュリティ対策の対象領域のセキュリティ特性を示す組織･情報システムの情報セキュリティ面からのモデルの確立が必要となる。

【対策のポイント】

(1) セキュリティ対策の特性モデルの作成

セキュリティ対策を検討するための対象組織･情報システムモデルでは、以下が明示されなければならない。

- 組織の運営形態
- 適用業務の特性と情報セキュリティについての要求とそのレベル
- 対象システムの構成形態、運用形態

- 組織の内外に提供するサービス、情報資産、システム資産、施設･設備等の保護対象となるものの体系
- 保護対象グループ（同じような保護が要求あるいは適用される保護対象の集合）ごとのライフサイクルの特性
- 保護対象グループごとのライフサイクルを意識した存在場所
- 保護対象グループごとのライフサイクルや存在場所を前提とした想定する脅威とその程度

（2）セキュリティ対策の対象モデルの見直しの実施

セキュリティ対策の計画の前提となる対象システムのセキュリティ特性モデルは、組織や業務の運営実態や対象となる情報システムの実態に合ったものでなければならない。これらの変化は日常的なものと考えなければならないので、一旦、完成された対象システムのセキュリティ特性モデルの妥当性を維持するためには、必要に応じた見直しが常に行われ、その妥当性が常に維持されなければならない。

- 必要に応じた見直しの実施

  以下のような状況が発生し他場合における遅滞のない見直しの実施

  ートップレベルのセキュリティポリシーの変更
  ー新しい脅威の登場
  ーセキュリティ対策の不備が顕在化
  ー組織の運営体系の変更
  ー適用業務の変更やその運営形態の変更
  ーシステムの構成や運用形態の変更
  ーセキュリティ対策として求めるレベルの大枠
- 定期的な見直しの実施

  見直しのさぼりや、見直し時の漏れ等をカバーするため、セキュリティ対策対象モデルは、定期的に見直しを実施することも必要である。

【対応 ISMS コントロール】

ISMS には、明示的に本要求に対応するものはない。

Ma2.2	保護対象となる組織内外に提供しているサービスについてのセキュリティ要求の明確化

【主旨】

組織は、一般に、情報システムを介して、外部に対する事業サービスの提供や、内部業務処理やオフィス処理をサポートしている。組織が内外に提供しているこれらの情報システムを用いたサービスの提供における情報セキュリティを確保するためには、それぞれのサービスについての情報セキュリティついての要求が明確に示されていなければならない。

【対策のポイント】

(1) 保護対象サービスの提供において求められる情報セキュリティのレベルの明示

要求されるセキュリティレベルを同じくするサービスのグループごとに、以下が明示されなければならない。

- 当該グループに該当するサービス
- 各サービスに求められる情報セキュリティのレベル(注1)
  - ・可用性についての要求レベル
  - ・システムの処理の正確性についての要求レベル
  - ・不正使用の防止についての要求レベル
  - ・情報の保護についての要求レベル
  - ・利用者の保護についての要求レベル
  - ・運用管理者の立場からの要求のレベル

(注1) 要求のレベルとしては、絶対を 100 としたときの%表示が分かりやすいが、その指定そのものの信憑性や実現レベルとの比較は困難であるため、定性的な表現でもかまわない。以下のような区分が一例として考えられる。
(指定区分の例) 絶対、非常に大、中、小

(2) 保護対象サービスへの情報セキュリティのレベルの指定の見直しの実施

保護対象サービスへの情報セキュリティのレベルの指定の妥当性の維持のためには、必要に応じた見直しが行われなければならない。

- 必要に応じた見直しの実施
- 定期的な見直しの実施
  見直しのさぼりや、見直し時の漏れ等をカバーするため、セキュリティ対策対象モデルは、定期的に見直しを実施することも必要である。

【対応 ISMS コントロール】

ISMS には、明示的に本要求に対応するものはない。

Ma2.3	保護対象の情報資産の洗出しとその個々に対する保護要件の明確化

【主旨】

情報資産の保護が適切に行われるためには、まず、保護の対象となる情報資産の個々について、組織内においてどのような使われ方をしているかについての正確な把握をベースとした、求められる保護はどのようなものであり、具体的などのような保護策を適用すべきかが明確に示されていなければならない。

なお、ここで言う情報資産とは、個人情報、経営情報、技術情報等の情報のコンテンツを指す。情報の保護の実践は、これらの情報が格納されたシステム上の業務ファイルや電磁媒体や関係す

る印刷物が対象になる。これらの扱いについては、別途に要求がなされており、ここでは、これらについての保護策を定める前提としての、これらに含まれる情報そのものに求められている保護を明確にすることを求めている。

【対策のポイント】

(1) 情報資産に対する保護基準の確立

- 保護対象情報資産の重要度に応じた保護の厳格さで示す保護クラスの分類
- 保護クラス別に実施すべき具体的な保護の基準の指定

　　－情報のライフサイクルの全過程(取得・作成から～抹消)における標準的な保護の指定

(2) 保護対象情報資産の漏れのない把握

保護対象の情報資産のそれぞれに対する保護要件の指定が、適切に行われるためには、まず、保護対象の情報資産の漏れない把握と、組織内において当該情報がどのような形態で存在し、どのように用いられているかの正確な把握にもとづく、個々の情報に求められる保護の大枠が示されなければならない。

保護対象情報の個々について、その保護という観点で、把握すべき事項としては、表 1-4 に示すようなものがあげられる。

表 1-4 保護要件を検討するにあたって把握すべき保護対象情報の特性

区分	指定事項
情報内容とその基本属性	・情報名情報内容と組織における情報の役割 ・管理責任者
組織内での情報の位置付け形態、利用形態	・組織内での情報の存在形態(利用メディアとその存在場所他) ・組織内での情報の利用形態(利用部署、利用業務等) ・取扱い上の制約 　－法的な要求他 ・取扱い上の不手際がもたらす影響 　－情報内容の誤り、漏洩、改ざん他
取扱い上の制約	・取得あるいは作成についての制約 ・開示についての制約 　－閲覧権限者と閲覧権限の範囲 ・組織内で使用についての制約 　－使用できる部署や者の制限 　－利用目的の制限 　－利用方法の制限 第三者提供についての制約
管理についての要求	・保管についての要求 　－日常的な保管についての要求 　－長期保管についての要求

(3) 保護対象情報資産の個々に指定すべき保護要件の指定を管理する仕組みの確立

保護対象情報資産に指定した保護要件の的確性を確保するためには、保護要件の指定を管理する仕組みの確立も必要となる。

システム上の業務情報に対する保護要件の指定要領に示すべき事項としては、以下があげられる。

- 情報資産に対する保護要件の指定についての責任体制

- 保護要件の指定（検討から、レビュー、承認までの）手続き
- 保護要件として指定すべき事項
- 保護対象情報資産に対する保護要件の指定の見直し要領
  - ・定期的な見直しサイクルおよび臨時の見直しが必要な場合
  - ・見直しの進め方
  - ・見直しのポイント

（4）保護対象情報資産の個々に対する保護要件の指定

保護対象の情報の個々に対し、指定保護クラスと該当する保護基準に準じた求める保護策を具体的に指定する。保護対象情報資産の個々に対する保護要件として指定すべき事項としては、表 1-5 に示すようなものがあげられる。

なお、この指定にあたっては、同一の管理（保護）が適用されるものについては、一つの情報グループに纏め、この単位に指定してもよい。

表 1-5　保護対象情報資産に対する保護要件として指定すべき事項

区分	指定事項
情報内容とその基本属性	・情報名情報内容と組織における情報の役割 ・管理責任者
組織内での情報の位置付け形態、利用形態	・組織内での情報の存在形態（利用メディアとその存在場所他） ・組織内での情報の利用形態（利用部署、利用業務等） ・取扱い上の制約 　－法的な要求他 ・取扱い上の不手際がもたらす影響 　－情報内容の誤り、漏洩、改ざん他
取得あるいは作成要件	・取得あるいは作成についての制約 ・取得あるいは作成の手続き
閲覧および使用についての要件	・閲覧および使用の権限付与についての要件 　－権限付与者の範囲と権限の付与対象者についての管理の方法 　－利用権限を持つ者に与える利用できる範囲と利用に当たっての制限の指定 　　＊情報のライフサイクルの全過程を通じてのさまざまな使い方(注1)ごとのきめ細かい指定が必要 ・アクセス制御にあって適用すべき認証手段 ・閲覧および使用の記録に記録についての要求
保管についての要求	・保管形態、保管場所、保管にかかわる管理についての要求 　－有効性の確保の留めに実施すべき措置 ・バックアップの取得とその保管についての要求
その他	・ライフサイクルにかかる履歴の確保についての要求 ・情報に事故（正確性の喪失、破壊、紛失、漏洩、有効性の喪失等）がへの備えについての要求

(注1) 情報のライフサイクルの全過程を通じてのさまざまな使い方には、以下のようなものがる。
－情報の検索・閲覧、情報の業務での使用、情報の更新・削除、情報の 2 次加工、複写の作成
情報の移動、情報の第三者への開示や提供

（4）保護対象情報資産の保護基準、保護対象資産の指定およびその個々に対する保護要件の指定の見直しの実施

- 見直しの仕組みの確立
- ルールに沿った見直しの実施

- ルールの沿った指定変更の実施

【対応 ISMS コントロール】

5.1.1 資産目録
5.1.2 分類の方針
5.1.3 情報の分類

2. ビジネスオペレーション･ビュー

2.1. セキュアな組織運営と業務運営の実現

2.1.1. 組織管理上でのセキュリティ対策

Ba1.1	セキュリティ対策上の人的要因に対する管理の仕組みの確立

【主旨】

人的要因による情報セキュリティ違反やセキュリティ対策上の不手際がないようにするためには、関係者への情報セキュリティにかかる責務の徹底や、違反行為に対する牽制等の必要な管理上の仕組みが確立していることが必要となる。

【対策のポイント】

(1) 人的要因によるセキュリティ事故の防止についての取組方針の明確化

人的な要因によるセキュリティ事故を防ぐためには、まず、どのような管理をどのレベルで行うかについての方針を確立しておくことが必要となる。この方針で示すべきこととしては、表 2-1 に示すようなものがある。

表 2-1 人的要因によるセキュリティ事故の防止についての取組方針で示すべき事項

検討事項	内容
信用が不十分な者の職場からの排除についての考え方	･職員の信用の確認についての考え方 　－職員の採用にあたっての信用にチェック 　－常日頃における職員の信用のチェック ･信用できなくなった職員への対処の方針 ･常駐させる外部スタッフの信用の確保についての考え方 　－外部スタッフの使用にあたっての信用のチェック 　－常日頃における使用している外部スタッフ信用のチェック ･信用ができなくなった外部スタッフに対する対処の方針
関係者の情報セキュリティに対する意識や責務についての認識の醸成の進め方	･職員に意識醸成の方針 ･常駐させる外部スタッフへの意識醸成の方針 ･保護領域に一時的に立入る者に対する対応方針
関係者のセキュリティ違反防止手段	･セキュリティ要求事項の明確化の方針

の組み立て	･セキュリティ要求事項の実践の監督指導についての方針 ･セキュリティ違反についての対処の方針

⑵ 職員の採用や常駐させる外部スタッフの採用についての管理の仕組み確立

職員の採用や常駐させる外部スタッフの採用についての管理の仕組みとして検討すべき事項としては、以下のようなものがある。

- 関係者の信用の担保の仕組み
- 関係者の行動に対する監視の仕組み
- 関係者の監督、指導の仕組み

⑶ 職員の信用を確保するための仕組みの確立

職員の信用を確保するための仕組みとして検討すべき事項としては、以下のようなものがある。

- 採用にあたっての信用のチェックの実施
- 採用にあたっての情報セキュリティにかかる責務の遵守の確認と関係する懲戒規程についての明確化についての手続き
- 定期的な信用の再チェックについての規程

⑷ 常駐させる外部スタッフの信用を確保するための仕組みの確立

常駐させる外部スタッフの信用を確保するための仕組みとして検討すべき事項としては、以下のようなものがある。

- 採用にあたっての信用のチェックの実施
- 採用にあたっての情報セキュリティにかかる責務の遵守の確認と関係する懲戒規程についての明確化についての手続き
- 定期的な信用の再チェックについての規程
- 所属会社における責任の認知手続き

⑸ 職場における関係者のセキュリティ要求の遵守を管理する仕組みの確立

職場における関係者のセキュリティ要求の遵守を管理する仕組みとして検討すべき事項としては、以下のようなものがある。

- 関係者へのセキュリティ要求事項の徹底方法の明確化
- 管理者による職場におけるセキュリティ要求の実践状況についての管理要領の確立
  - ーチェックリストの作成
  - ー実施サイクル確認手段等のチェックの実施要領
- 職場における相互牽の実現

⑹ セキュリティ違反に対る懲戒規程の確立

検討すべき規程としては、以下のようなものがある。

- 職員に対する懲戒規程
- 外部スタッフならびに所属会社に対する処罰等の規程

【対応 ISMS コントロール】

4.2.1 第三者のアクセスから生じるリスクの識別

4.2.2 第三者との契約書に記載するセキュリティ要求事項

6.1.1 セキュリティを職責に含めること
6.1.2 要員審査およびその方針
6.1.3 秘密保持契約
6.1.4 雇用条件

Ba1.2	関係者に対する情報セキュリティについての取組意識の醸成と責務の明確化

【主旨】

情報セキュリティは、組織や業務の運営や使用する情報システムの構築や運用関係者のすべての積極的な取り組みが欠かせない。このため、セキュリティ対策の推進のためには、関係者に対する意識付け等の活動が必須となる。

【対策のポイント】

(1) 関係者における情報セキュリティについての認識の醸成

関係者における情報セキュリティについての認識を醸成するには、以下のようことが必要となる。

- 情報セキュリティに関する教育、啓蒙の実施
- 関係者の情報セキュリティについての認識レベルの確認

(2) 業務現場やシステムの運用現場に対する業務遂行上のセキュリティ要求の徹底

業務現場やシステムの運用現場に対する業務遂行上のセキュリティ要求を徹底するには、以下のようことが必要となる。

- セキュリティ要求事項の明確化
- 就業規程等への反映
- 関係者へのセキュリティ要求の周知
- その認識レベルの確認

【対応 ISMS コントロール】

6.2.1 情報セキュリティ教育および訓練

Ba1.3	関係者の信用の確認の実施と職場等での行動についての必要な管理の実施

【主旨】

関係者にセキュリティ違反が起きないようにするためには、信用できない者を就業させないとか、職場等における従業者の行動のチェックを行うことも必要となる。職場等における関係者の行動に対する適切なチェックの実施は、セキュリティ違反の牽制だけでなく、違反行為の発見にも有効である。また、セキュリティ違反に対しては、適切な対処も必要となる。

【対策のポイント】

⑴ 関係者の信用の確保

関係者の信用を確保するためには、以下のようことが必要となる。

- 職員採用にあたっての信用についてのある程度の審査の実施
- 派遣スタッフの受入れ時における対象者の信用についてのある程度の審査の実施
- 職場内外における不審な行動についてのチェックの実施
  - ・不審な行動への関心
  - ・必要に応じたチェックと指導の実施
- 職員の不正行為に対する懲戒規程の確立
  - ・不正行為に対する適切な懲戒規程の確立
  - ・就業規程への反映
  - ・職員への周知
- 外部スタッフの不正行為に対する対処の確立
  - ・不正行為者に対する対処の確立
  - ・派遣元会社の責任の明確化と派遣先との合意の形成
  - ・派遣契約等での処分の明示
  - ・外部スタッフへの周知
- 発生した不正行為に対する規程に沿った厳正な処置の実行
  - ・職員に対する懲戒等の処置の実施
  - ・契約に沿った外部スタッフの処置の実施
  - ・必要に応じた派遣元会社の責任の追及

⑵ 職場等における行動の制限の明確化

職場の関係者の行動がセキュリティ事故に結びつかないようにするためには、職場における関係者に要求する行動の制限を明確にしておく必要がある。

- 外部からのシステムの構築・運用支援スタッフの施設への立入りについてのセキュリティ要求事項の明確化
  - ・立入りの認可とIDの表示と立入りの記録の作成
  - ・行動の制限の明確化
  - ・違反に対する処置の明確化
  - ・立入り者への要求の明示
  - ・所属会社への要求の明確化と、その責任の明確化
- 外部からのシステムの保守要員の施設への立入りについてのセキュリティ要求事項の明確化
  - ・立入りの認可とIDの表示と立入りの記録の作成
  - ・行動の制限の明確化
  - ・違反に対する処置の明確化
  - ・立入り者への要求の明示
  - ・所属会社への要求の明確化と、その責任の明確化

- 清掃等の施設の管理要員の施設への立入りについてのセキュリティ要求事項の明確化
  ・立入りの認可とIDの表示と立入りの記録の作成
  ・行動の制限の明確化
  ・違反に対する処置の明確化
  ・立入り者への要求の明示
  ・所属会社への要求の明確化と、その責任の明確化④ビジネスパートナーのスタッフや出入りの営業マン等のその他の外部スタッフの施設への立入りについてのセキュリティ要求事項の明確化
  ・必要な行動制限の実施
  ・違反に対する処置の明確化

(3)職場等における行動の制限や監視の実施

職場の関係者の行動がセキュリティ事故に結びつかないようにするためには、職場の関係者が関係するルールを遵守するよう、職場における関係者の行動の制限や監視を行うことが必要となる。

- 外部からのシステムの構築・運用支援スタッフの施設への立入りについての管理の実施と、職場内での行動の監視と必要な場合における指導の実施
- 外部からのシステムの保守要員の施設への立入りについての管理の実施と、職場内での行動の監視と必要な場合における指導の実施
- 清掃等の施設の管理要員の施設への立入りについての管理の実施と、職場内での行動の監視と必要な場合における指導の実施

(4)関係者におけるセキュリティ違反に対する懲戒等の必要な措置の実施

セキュリティ違反に対しては、厳正で公平な処置を実施しなければ、関係者に対するセキュリティ要求は有名無実のものとなる。このためには、セキュリティ違反に対しては、以下のようことが必要となる。

- 適切な指導の実施(セキュリティ違反に対する見逃しの排除)
- 規程に沿った懲戒の実施

【対応 ISMS コントロール】

4.2.1 第三者のアクセスから生じるリスクの識別
4.2.2 第三者との契約書に記載するセキュリティ要求事項
6.1.1 セキュリティを職責に含めること
6.1.2 要員審査およびその方針
6.1.3 秘密保持契約
6.1.4 雇用条件

2.1.2. 業務運営上でのセキュリティ対策

Ba2.1	業務現場ごとのセキュリティ要求の明確化

【主旨】

業務現場における業務の遂行上や職場で諸活動においても、情報セキュリティにかかわることが少なくない。業務現場における情報のずさんな取扱い他で、セキュリティ対策に穴をあけることがないようにするためには、まず、業務現場に対するセキュリティ対策にかかる要求が明確にされていなければならない。この要求の詳細は、部門ごとの異なったものとはなるが、その大枠はどの部門にも共通となる。

これらの要求は、セキュリティ対策として計画したものすべてを反映したものでなければならない。

【対策のポイント】

(1) 業務現場に対するセキュリティ要求の洗い出し

セキュリティ対策の実践は、担当業務や要員構成、オフィスの物理的環境、情報システムの利用あるいは運営形態等の職場の特性により多少、異なったものとなる。また、セキュリティ対策は多岐にわたるため、業務現場がなさなければならないことの認識に漏れが出るようなことがあってはならない。このため、業務現場にセキュリティ要求の実践を期待するためには、まず、多岐にわたるセキュリティ対策が業務現場に求めていることを漏れなく洗い出す必要がある。

セキュリティ対策の実施に関し、業務現場に求めることの主なものとしては以下があげられる。細かい要求については、関係するセキュリティ対策の個々を参照しなければならない。

- 業務処理の確実な実行
- 情報の適切な取扱いと情報の保護
- 適切なユーザ管理の実施
- 情報やサービスへのアクセス権限の的確な管理
- システムや業務処理の異常発見時における適切な対応
- 職場等の保護領域における不審な者の立入りや不審な行為の監視および抑止
- 職場におけるセキュリティ違反への適切な対処
- 発生したセキュリティ事故への適切な対応

(2) 各職場におけるセキュリティ要求の明確化

セキュリティ対策の実践は、担当業務や要員構成、オフィスの物理的環境、情報システムの利用あるいは運営形態等の職場の特性により多少、異なったものとなる。このため、セキュリティ対策が業務現場に求めていることを、それぞれの職場にどのような形で展開するかの検討を、職場単位に行い、その結果を、当該職場に対するセキュリティ要求として再整理する必要がある。

このことが、きちんと行われなければ、業務現場におけるセキュリティ要求の実践は、そのベースが与えられないため期待できるものにはなりえない。

また、この結果は、業務要領や業務手順書等へ的確に反映されていなければならない。また、これらを分かり易く纏めた情報セキュリティ・ハンドブック等の編集と配布も有効である。

また、これらの内容はセキュリティ対策に変更が加えられた場合、その変更が確実に反映されるようになっていなければならない。

(3) 各職場に対するセキュリティ要求についての見直しの実施

各職場に対するセキュリティ要求は、職場環境の変更やセキュリティ対策の変更にともなって変わってくるものである。各職場に対するセキュリティ要求が妥当性を欠くようになったり、職場の実態と会わなくなってしまっていることを見逃さないためには、各職場に対するセキュリティ要求についての見直しを、定期的あるいは問題の発生等を契機とした臨時に実施すべきである。

【対応 ISMS コントロール】

4.2.1 第三者のアクセスから生じるリスクの識別
4.2.2 第三者との契約書に記載するセキュリティ要求事項
6.1.1 セキュリティを職責に含めること
6.1.2 要員審査およびその方針
6.1.3 秘密保持契約
6.1.4 雇用条件
6.3.5 懲戒手続き

Ba2.2	業務現場におけるセキュリティ要求の実践の追求

【主旨】

各職場は職務の遂行にあたって、セキュリティ対策にかかわる要求を確実に実践しなければならない。このことを実現するためには、職場の関係者へのセキュリティ要求の徹底、業務現場におけるセキュリティ要求の実践を管理する仕組みの確立、必要な監督、指導の実施、問題点に対する是正措置の迅速な実施が必要となる。

【対策のポイント】

(1) 職場の関係者へのセキュリティ要求の徹底

職場の関係者が、セキュリティ対策に関連して実践しなければならないことをよく理解できてなければ、その実践はありえない。職場の関係者にセキュリティ対策に関連して実践しなければならないことを徹底するためには、以下のような施策も必要となる。

- 必要に応じたセキュリティ要求と職場での実践上のポイントについての教育の実施
- 情報セキュリティへの取組みについての意識や、具体的な要求の理解状況についての定期的なチェックの実施

(2) セキュリティ要求の実践を管理する仕組みの確立

職場での業務の遂行やその他の活動のなかでのセキュリティ要求についての対応は、つい、疎かになりがちなものである。このため、その実践については十分な監督、指導が必要となる。日常の業務の中で、この点についての監督、指導が行き渡るようにするためには、以下も必要となる。

- 要求事項の実践状況についてのチェックリストの作成
- 定期的なチェックの実施

(3) セキュリティ要求の実践についての日常的な監督指導の実施

職場の管理者は、職場におけるセキュリティ要求の実践が適切になされているかどうかについて、日常的に監督指導しなければならない。このとき、要求に対するずさんな対応を大目に見るようなことがないように注意しなければならない。

(4) 問題点に対する是正措置の実施

職場におけるセキュリティ要求の実践に問題が生じた場合は、その原因を分析し、再発防止のために必要な措置を取らなければならない。想定される問題としては、以下があげられる。

- 対応すべきセキュリティ要求についての認識漏れ
- 職場へのセキュリティ要求の展開の不手際
- 職場の関係者の認識や努力の不足
- 監督、指導の不足

【対応 ISMS コントロール】

4.2.1 第三者のアクセスから生じるリスクの識別
4.2.2 第三者との契約書に記載するセキュリティ要求事項
6.1.1 セキュリティを職責に含めること
6.1.2 要員審査およびその方針
6.1.3 秘密保持契約
6.1.4 雇用条件
6.3.5 懲戒手続き

Ba2.3 他社とのリアルタイムの業務コラボレーションに対するセキュリティ対策の実施

【主旨】

企業間電子商取引やサプライチェーンマネジメントシステム (SCM) 等に見られるように、他社とのオンラインコラボレーションも日常的な業務の中に組み込まれるようになってきた。業務の中で重要な位置付けとなる、この他社とのオンライコラボレーションにおいて、セキュリティ面での問題を生じさせないためには、以下のような特別の配慮も必要となる。

- 自社の問題による相手側の業務遂行への大きな影響の排除
- 相手側の問題による相手側の業務遂行への大きな影響の排除
- それぞれの機密情報および共有情報の保護

- システムの連携に問題が生じた場合における責任の分界の明確化

【対策のポイント】

⑴ 他社とのオンラインコラボレーションにおけるセキュリティを確保するための仕組みの確立

他社とのオンラインコラボレーションにおいてセキュリティ問題を起さないようにするためには、他社とのオンラインコラボレーションにおけるセキュリティを確保するための組織的な仕組みを確立していることが必要となる。この点について、検討すべきこととしては、表2-2に示すようなものがある。

表 2-2 他社とのオンラインコラボレーションにおけるセキュリティを確保するための仕組みとして検討すべき事項

検討事項	内容
他社とのオンラインコラボレーションにおけるセキュリティ確保についての基本方針	・オンラインコラボレーションに求められるセキュリティ要求に大枠 　－正確性、可用性、情報の保護等についての要求の大枠 ・その実現の仕組み 　－システム面での対処すべき範囲 　－運用で対処すべき範囲 　－双方の管理についての要求レベル ・責任体制 ・問題が生じた時の双方の責任についての考え方
計画要領	・他社とのオンラインコラボレーションをセキュアなものにするための計画の作成やその評価の方針等 　－セキュリティ要求の計画、レビューの実施についての方針 　－システムの設計ならびに実装のチェックの実施についての方針 　－運用規程の設計ならびにチェックの実施についての方針 　－運用開始後のセキュリティ監査に実施についての方針 ・認可手続き
運用管理要領	・運用に対するセキュリティ要求の実践状況についてのチェック要領 　－チェックすべき事項の大枠 　－チェックの実施方法の大枠
契約等	・契約等への反映についての方針

⑵ 対応システム単位のセキュリティ方針の明確化

他社とのオンラインコラボレーションでのセキュリティ対策を適切なものにするためには、まず、対応するシステムごとに、セキュリティ対策として、何をどのように行うかを検討、決定するためのベースを確立さひておく必要がある。オンラインコラボレーションに対するセキュリティ方針として、システムごとに明確にすべきこととしては、以下のようなものがある。

- 適用する業務や交換する情報の制約についての方針
- 相手側のシステムの問題による自社業務への影響の極小化についての方針
- 自社システムの問題の連携先への影響の極小化の方針
- 問題が生じた時の責任分担についての考え方

⑶ 連携先ごとの責任の分担の明確化

他社とのオンラインコラボレーションでは、さまざまなトラブルを想定しなければならない。問題が生じた場合、お互いにどのような対応を取るべきか、また、どちらかに損失が生じた場合、どちらがどのような責任を負うべきかについて、予め明確にしておくことが必要となる。

問題が生じた場合の処置を円滑に行うためには、以下のような備えが必要となる。

- システム連携におけるシステム面での相互の責任分担
- 問題が生じた場合における原因の追求と改善についての相互の協力方法の明確化
- 被害が生じた場合の責任の分担のルール
- 上記の取決めについての契約やサービスレベルアグリーメント上での明確化

(4) システムへの必要な機能の組込み

他社とのオンラインコラボレーションにおいては、自社側の問題が連携先に大きく波及したり、連携先のシステムの問題が自社の業務に大きく影響したりすることがないようにするためにも、また、問題が生じた時の責任の分界ができるようにするためには、必要な機能をシステムに組込んでおかなければならない。

この点について検討すべきこととしては、以下のようなものがある。

- 自社の機密情報の保護
- 交換する情報および共有情報の保護
- 自社システムのトラブルの相手への影響を小さくするための機能や運用
- 相手側システムのトラブルの自社業務への影響を小さくするための機能や運用
- 問題が生じた場合における責任の所在を明確にするための機能

(5) 問題が生じた場合における適切な対処の実施

問題が生じた場合における適切な対処が迅速に行えるようにするためには、以下のような備えも必要となる。

- 関係者に対する連携先との取決めの徹底
- 問題発生時における対処要領の確立

【対応 ISMS コントロール】

4.3.1 外部委託契約によるセキュリティ要求事項

Ba2.4	業務の外部委託に対する適切なセキュリティ対策の実施

【主旨】

今日では、業務の一部を外部に委託している組織が多い。業務の外部への委託は、また、さまざまなセキュリティ面でのリスクが多い。このため、業務の外部委託については、セキュリティ面から以下のような特別な配慮が必要となる。

- 業務委託先の選択
- 業務委託を行うにあたっての委託先へのセキュリティ面での要求の明確化
- 業務委託先に対するセキュリティ対策面での監督、指導の実施
- 問題が生じた場合における双方の責任の明確化

【対策のポイント】

(1) 業務委託におけるセキュリティを確保するための仕組みの確立

業務の外部への委託でセキュリティ問題を起さないようにするためには、業務委託におけるセキュリティを確保するための仕組みが組織的に確立していることが必要となる。確立すべき業務委託におけるセキュリティを確保するための仕組みとして検討すべき事項としては、票 2-3 に示すようなものがある。

表 2-3 業務委託におけるセキュリティを確保するための仕組みとして検討すべき事項

検討事項	内容
業務委託におけるセキュリティ確保についての基本方針	・セキュリティ面から外部に業務委託ができる範囲 ・業務委託先の選定についての考え方 ・業務委託先において必要なセキュリティの実現を図る仕組みの大枠 　－委託先へのセキュリティにかかわる要求の明確化の手段 　－委託先におけるセキュリティ要求の実践の監督指導の方法 ・問題が生じた場合の責任の分界についての考えかた
業務委託先の選定についての基本方針	・業務委託先としての資格 ・業務委託先の情報セキュリティについての取組みについての評価基準
セキュリティ面からの業務委託の手続き	・業務委託先の認可手続き 　－業務の外部委託計画要領 　－業務委託先の審査選定要領 　－業務委託先へのセキュリティ要求の明確化要領 　－契約手続き

(2) 信頼できる業務委託先の選定

業務委託先の選定を適切に行うためには、以下が必要となる。

- 定められた審査の実施
  - －資格審査
  - －セキュリティ面での要求に対する対応能力
- 定められた手続きに沿った決定

(3) 業務委託先ごとのセキュリティ面での双方の責任の明確化

業務委託先ごとのセキュリティ面での双方の責任の明確化にあたっては、以下が必要となる。

- 双方の責任の明確化と合意の形成
- セキュリティ要求事項の実践方法についての合意の形成
- 契約等でのそれぞれの責任の明文化

(4) 業務委託先ごとのセキュリティ要求への対応状況のチェックと必要な指導の実施

業務委託先ごとのセキュリティ要求への対応状況のチェックと必要な指導を円滑かつ効果的に行うためには、以下が必要となる。

- チェックの方法の確立と双方の合意の形成
- チェックと評価の実施
- 問題点の是正処置への展開

(5) 業務委託との継続的なコミュニケーションの確保

業務委託先でセキュリティ問題を起こさないようにするためには、(4) に示した監督指導だけでなく、常日頃からの、セキュリティ要求やその実践についての意見の交換等についての継続的なコミ

ュニケーションも欠かせない。

(6) 問題が生じた場合における適切な対処の実施

また、問題が生じた場合における適切な対処が迅速に行えるようにするためには、以下のような備えも必要となる。

- 関係者に対する連携先との取決めの徹底
- 問題発生時における対処要領の確立

【対応 ISMS コントロール】

4.3.1 外部委託契約によるセキュリティ要求事項

2.1.3. 業務現場での情報の保護の徹底

Ba3.1	印刷物の作成や取扱いについてのルールの確立と、ルールに沿った印刷物の作成や取扱いの実践

【主旨】

印刷物は日常業務に密着し、取り扱う量が多いため、管理がおろそかになりやすい。しかし、印刷物による情報漏えい事故の事例が多いといった事実を認識し、システム上の情報以上に取扱いに十分気をつけなければならない。そのため、組織は取扱いルールを決定し、紙媒体の利用を適切に管理していく必要がある。取扱いルールの策定にあたっては作成／配布／保管／廃棄といった印刷物のライフサイクルごとに策定することが必要となる。

また、業務現場における情報の保護を徹底するには、単に管理･取扱いルールを定めるだけではなく、業務現場の全従業員にルールを遵守させなければならない。そのためには、まずはルールを周知徹底させることが必要である。さらに、ルール違反時の対応方法といった仕組みを作るとともに、ルールの遵守状況を定期的に確認してゆくことも必要となる。

印刷物は日常業務に密着し、業務現場での取り扱う量が非常に多いため、管理の徹底をするのが難しい媒体といえる。また、印刷物は紛失したのか廃棄したのか管理しにくい性質があり、万が一漏洩したとしても気づかないリスクが高い。それだけに高いレベルで実行管理してゆくことが求められる。

【対策のポイント】

(1) 保護要件の指定およびラベリングについての管理の仕組みの確立

保護対象の印刷物に対する保護要件の指定が適切に行われるためには、その指定および指定状況がマネジメントされていることが必要となる。このためには、保護要件の指定およびラベリングについての管理の仕組みを確立しておくことも要となる。

印刷物に対する保護要件の指定およびラベリングについての管理の仕組みとして検討すべき事項としては、以下のようなものがあげられる。

- 保護要件の指定者、ラベリング実施者
- 保護要件の指定手順
- ラベリング方法、ラベリングの手順
- 保護要件を実行に移すためのプロセス

(2) 保護対象の印刷物に対する保護要件の指定

保護対象の印刷物が外部の委託先も含む業務現場で適切に取扱われるためには、保護対象の印刷物の個々に対してその取り扱い条件を示した保護要件が定義されていなければならない。

印刷物に対する保護要件として検討すべき事項としては、表 2-4 に示すようなものがある。

表 2-4 印刷物に対する保護要件として検討すべき事項

ライフサイクル	保護要件	保護要件指定の具体例
作成 (印刷／複製) 時	不正な印刷／複製の制限	・無許可の複製禁止を義務化 ・電子ファイルに対して、印刷不可の設定を施す ・認証機能 (パスワード、IC カード) が装備された印刷装置の利用 ・アプリケーション、OS、NW 的なアクセス制限等による印刷制限 ・印刷、複製状況の監視 -オープンスペースへの印刷装置の設置 (衆人による監視) -監視カメラの設置 等 ・業務時間外利用の禁止 (印刷装置の電源 OFF 等)
	複製記録の取得	・複製した印刷物に管理番号を振り、台帳の管理
	印刷出力時の留意事項	・印刷装置の出力トレイに印刷物を放置禁止の義務化 ・置き忘れアラーム機能のついた印刷装置の導入 ・機密情報の印刷出力時の印刷装置前待機の義務化
配布 (輸送・送信) 時	配布手段の指定	・安全な配布手段の検討 -改ざん防止シール、耐タンパー性のある包装の利用 -施錠コンテナの利用 -社員の携行義務化 ・外部配達業者の利用時の検討 -信頼できる運送業者の選定 -書留、速達、内容証明郵便、受取人指定郵便等の利用
	配布手続きの明確化	・承認者、承認手続きの明確化 -審査部門の承認 -上司の承認 ・ (FAX、e-mail 等の) 誤送信防止手続きの明確化 -送信作業のペアオペレーション -送信先の再確認の義務化
	配布記録の取得	・輸送／送信記録の取得 (日時、情報名、配布先等) ・受け取り確認書を同封し、受け取りの確認の実施
保管時	保管方法の指定	・机上等への放置禁止の義務化 ・施錠キャビネット、耐熱金庫の利用 ・別地保管 (二重保管、遠隔地保管) の実施 ・アクセス権限者の明確化
	印刷物の入出庫管理 (アクセスの管理) の実施	・鍵の貸し出し管理等による入出庫管理の実施 ・複数人による入出庫実施 (ペアオペレーション)
	アクセス記録の取得	・入出庫記録の取得 (入出庫した情報、利用者、日時等の記録等) -台帳による記録 -電子的な自動アクセス記録
廃棄・再利用時	廃棄実施までの安全な保護手段 (廃棄処理前の管理)	・廃棄物保管場所への立ち入り制限 ・施錠可能な廃棄 BOX の利用

	廃棄方法の検討	･機密情報の裏紙利用の禁止 ･廃棄手段の検討 　-シュレッダー等による破砕処理 　-焼却･溶解処理 ･廃棄作業時のペアオペレーションの実施 ･外部業者に委託する際の検討 　-信頼できる廃棄業者の選定 　-機密保持契約の締結 　-廃棄時の立会いの実施、または、廃棄処理証明の提出依頼
	廃棄記録の取得	･作業実施報告書の提出 ･廃棄時の許認可手続きの記録

(3) 保護対象の印刷物に対するラベル付け

保護対象の印刷物が外部の委託先も含む業務現場で適切に取扱われるためには、当該印刷物に指定された保護要件が認識できるようなラベルが明示されるようにしなければならない。

このラベルとして表示されるべき項目としては、以下があげられる。

- 管理者、管理番号、機密レベル (例えば「極秘」「社外秘」等)
- 開示対象者、開示範囲、開示手段
- 指定された保護要件
  ･作成 (印刷･複製) 時の保護要件
  ･配布 (輸送･送信) 時の保護要件
  ･保管時の保護要件
  ･廃棄･再利用時の保護要件

なお、「極秘」「秘」「社外秘」といったように、あらかじめ管理クラスを分けた上でそれぞれの管理クラスにおける作成／配布／保管／廃棄時の保護要件を定めておき、その管理クラスのみを印刷物にラベリングすることによって、個別の印刷物に対して詳細に保護要件を記述する手間を省略することができる。

(4) 業務現場における管理ルールの周知徹底

保護対象情報が記載された印刷物が、業務現場で適切に取扱われるためには、まずはその管理ルールが周知徹底されなければならない。周知徹底の主な手段としては、定期的な教育のほか、日常的な啓蒙活動も重要である。

(5) 業務現場における印刷物に対する取扱いルールの遵守の徹底

保護対象情報が記載された印刷物が、業務現場で適切に取扱われるためには、印刷物のライフサイクルに沿って定義された保護要件を、各従業員が遵守しなければならない。その中でも、業務現場等における印刷物の取扱いにおいて、特に留意すべき事項を、表 2-5 に示す。

表 2-5 業務現場における印刷物に対する取扱いでとくに留意すべき事項

ライフサイクル	保護要件の指定事項
作成 (印刷･複製) 時	不正な印刷／複製の制限
	印刷／複製の記録の取得
	印刷出力時の放置等の抑止
配布 (輸送･送信) 時	安全な配布手段の指定
	配布手続きの明確化
	配布記録の取得

保管時	保管方法（施錠キャビネットなど）の指定
	印刷物の入出庫管理（アクセスの管理）の実施
	アクセス記録の取得
廃棄・再利用時	廃棄実施までの安全な保護手段（廃棄処理前の管理）
	廃棄方法の検討
	廃棄記録の取得

（6）業務現場における印刷物の適切な取扱いを実現するための環境の整備

業務現場における印刷物の適切な取扱いを実現するための環境の整備として、検討すべき事項としては、以下があげられる。

- 必要な装置や設備の準備

  印刷物の作成や取扱いに対する管理ルールを遵守させるには、ルール遵守を従業員に一方的に押付けるだけではなく、ルールが自動的に遵守されるような機器・システムやツールを使うなど、環境面の整備が必要である。例えば、認証機能が装備された印刷装置を使うことで、自動的に印刷制限が施されることが該当する。管理ルール遵守を担保する環境は、印刷物のライフサイクルに沿って網羅的に整備されることが望ましい。

- 管理ルール違反時の仕組みの確立

  業務現場において管理ルールの実効性を担保するためには、管理ルールが遵守されなかった場合に対応する仕組みを整えておくことが必要である。ルール違反発見時の報告体制や、懲罰等の対応方法が明確化されていることが求められる。

- 管理ルール遵守を定期的に確認する仕組みの確立

  業務現場において管理ルールの実効性を担保するためには、管理ルールの遵守状況を全部門・全従業員に渡って定期的にチェックし、問題があれば改善の指導をすることが必要である。また、結果を分析し、管理・取扱いルールを見直す際の材料としておくことも重要である。

【対応 ISMS コントロール】

5.1.1 資産目録
5.2.1 分類の指針
5.2.2 情報のラベル付けおよび取扱い
8.6.2 媒体の処分
8.7.2 配送中の媒体のセキュリティ

Ba3.2	可搬メディアの安全な利用についてのルールの確立と、ルールに沿った可搬メディアの取扱いの実践

【主旨】

可搬メディアは、電子情報を容易に持ち運びができるといった使い勝手の良さから、広く利用されているが、その反面、不正な情報の持ち出しを規制することが困難な情報記憶媒体といえる。特に、保存容量の大容量化に伴い、大規模な情報漏えいにつながるリスクが大きい。そのため、組織は可搬メディアの取扱いルールを決定し、可搬メディアの利用を適切に管理していく必要がある。取扱いルールの策定にあたっては利用／配布／保管／廃棄といった可搬メディアのライフサイクルごとに策定しなければならない。

また、業務現場における情報の保護を徹底するには、単に管理･取扱いルールを定めるだけではなく、業務現場の全従業員にルールを遵守させなければならない。そのためには、まずはルールを周知徹底させることが必要である。更に、ルール違反時の対応方法といった仕組みを作るとともに、ルールの遵守状況を定期的に確認してゆくことも必要となる。

業務現場における情報の保護を徹底するには、単に管理･取扱いルールを定めるだけではなく、業務現場の全従業員にルールを遵守させなければならない。そのためには、まずはルールを周知徹底させることが必要である。更に、ルール違反時の対応方法といった仕組みを作るとともに、ルールの遵守状況を定期的に確認してゆくことも必要となる。

可搬メディアはその利便性から業務現場での利用は増える傾向にあり、また保存容量が大容量化しているため、大規模な情報漏えいにつながるリスクが高い。管理ルール遵守の徹底が求められる。

【対策のポイント】

(1) 可搬メディア対する保護要件の指定およびラベリングについての管理の仕組みの確立

保護対象のに可搬メディア対する保護要件の指定が適切に行われるためには、その指定および指定状況がマネジメントされていることが必要となる。このためには、保護要件の指定ならびにラベリングについての管理の仕組みを確立しておことも必要となる。

可搬メディアに対する保護要件の指定およびラベリングについての管理の仕組みとして検討すべき事項としては、以下があげられる。

- 保護要件の指定者、ラベリング実施者
- 保護要件の指定手順
- ラベリング方法、ラベリングの手順
- 保護要件を実行に移すためのプロセス

(2) 組織的に管理する可搬メディアに対する保護要件の指定

組織にはサーバ等のバックアップのための可搬メディアや、各種情報をアーカイブするための可搬メディアといった、組織的管理を実施する可搬メディアが存在する。これらの可搬メディアが外部の委託先も含む業務現場で適切に取扱われるためには、保護対象の可搬メディアの個々に対

してその取り扱い条件を示した保護要件が定義されていなければならない。

組織が管理する可搬メディア対する保護要件の指定で検討すべき事項としては、表 2-6 に示すようなものがある。

表 2-6 組織が管理する可搬メディア対する保護要件の指定で検討すべき事項

ライフサイクル	保護要件	保護要件指定の具体例
利用（新規保存／複製等）時	不正な利用の制限	・利用に際する許可申請の義務化 ・システム的な利用の制限措置 -OS の設定 -専用ソフトウェアの導入 ・外部接続ポートの物理的な封鎖
	利用記録／ログの取得	・複製した可搬メディアに管理番号を振り、台帳管理 ・システム的な利用ログの取得
	利用時の留意事項	・機器内への可搬メディアの取り残し禁止の義務化
配布（輸送）時	配布手段の指定	・安全な配布手段の検討 -改ざん防止シール、耐タンパー性のある包装の利用 -施錠コンテナの利用 -社員の携行義務化 ・外部配達業者の利用時の検討 -信頼できる運送業者の選定 -書留、速達、内容証明郵便、受取人指定郵便等の利用
	配布手続きの明確化	・承認者、承認手続きの明確化 -審査部門の承認 -上司の承認
	配布記録の取得	・輸送／送信記録の取得（日時、情報名、配布先等） ・受け取り確認書を同封し、受け取りの確認の実施
保管時	保管方法の指定	・机上等への放置禁止の義務化 ・施錠キャビネット、耐熱金庫の利用 ・別地保管（二重保管、遠隔地保管）の実施 ・アクセス権限者の明確化
	可搬メディアの入出庫管理（アクセスの管理）の実施	・鍵の貸し出し管理等による入出庫管理の実施 ・複数人による入出庫実施（ペアオペレーション）
	アクセス記録の取得	・入出庫記録の取得（入出庫した情報、利用者、日時等の記録等） -台帳による記録 -電子的な自動アクセス記録
廃棄／再利用時	廃棄実施までの安全な保護手段（廃棄処理前の管理）	・廃棄物保管場所への立ち入り制限 ・施錠可能な廃棄 BOX の利用
	廃棄／再利用方法の検討	・再利用手段の検討 -情報の完全削除 ソフトウェアイレーサ、磁気的な消去装置の利用 等 ・廃棄手段の検討 -情報の完全削除 ソフトウェアイレーサ、磁気的な消去装置の利用 等 -物理的な破砕処理 ・廃棄作業時のペアオペレーションの実施 ・完全消去済みの確認作業の義務化 ・外部業者に委託する際の検討 -信頼できる廃棄業者の選定 -機密保持契約の締結 -廃棄時の立会いの実施、または、廃棄処理証明の提出依頼

	廃棄記録の取得	･作業実施報告書の提出 ･廃棄時の許認可手続きの記録

なお、上記ライフサイクルのすべてにおいて共通する保護要件として、可搬メディア内のデータ暗号化が挙げられる。この場合、暗号鍵の管理ルールを明確にしておく必要がある。

(3) ユーザが個別管理する可搬メディアに対する保護要件の指定

組織的に管理する可搬メディア以外にも、組織にはユーザがデータ受け渡し等の用途で利用する可搬メディアが存在する。これらの個々の可搬メディアに対してもその取り扱い条件を示した保護要件が定義されていなければならない。

ユーザが個別管理する可搬メディア対する保護要件の指定で検討すべき事項としては、表 2-7 に示すようなものがある。

表 2-7 ユーザが個別管理する可搬メディア対する保護要件の指定で検討すべき事項

ライフサイクル	保護要件	保護要件指定の具体例
利用 (新規保存･複製等) 時	不正な利用の制限	･可搬メディアの全面的な利用禁止の義務化 ･個人所有の可搬メディア等の持ち込み禁止の義務化 ･利用に際する許可申請の義務化 ･システム的な利用制限措置 (OS、アプリケーション) ･外部接続ポートの物理的な封鎖
	利用記録／ログの取得	･システム的な利用ログの取得
	利用時の留意事項	･機器内への可搬メディアの取り残し禁止の義務化
配布 (社外持ち出し) 時	持ち出し手段の指定	･安全な配布手段の検討 -社員の携行義務化
	持ち出し手続きの明確化	･社外持ち出し時の承認者、承認手続きの明確化 -上司の承認
	持ち出し記録の取得	･社外持ち出し記録の取得 (日時、情報名、配布先等)
保管時	保管方法の指定	･机上等への放置禁止の義務化 ･施錠キャビネット、施錠可能なデスクへの保管
廃棄／再利用時	廃棄実施までの安全な保護手段 (廃棄処理前の管理)	･廃棄物保管場所への立ち入り制限 ･施錠可能な廃棄 BOX の利用
	廃棄／再利用方法の検討	･再利用手段の検討 -情報の完全削除 ソフトウェアイレーサ、磁気的な消去装置の利用 等 ･廃棄手段の検討 -情報の完全削除 ソフトウェアイレーサ、磁気的な消去装置の利用 等 -物理的な破砕処理 ･廃棄作業時のペアオペレーションの実施 ･完全消去済みの確認作業の義務化 ･外部業者に委託する際の検討 -信頼できる廃棄業者の選定 -機密保持契約の締結 -廃棄時の立会いの実施、または、廃棄処理証明の提出依頼
	廃棄記録の取得	･作業実施報告書の提出 ･廃棄時の許認可手続きの記録

なお、上記ライフサイクルのすべてにおいて共通する保護要件として、可搬メディア内のデータ暗号化が挙げられる。この場合、暗号鍵の管理ルールを明確にしておく必要がある。また、可搬メディアの種類によっては、パスワードやバイオメトリクス等による論理的なアクセス制限機能 (ロック

機能）を有するものも存在する。これらのロック機能の強度は可搬メディアの種類によって多種多様であるため、当該機能を利用する際は、ロック機能の強度を事前に評価すべきである。

（4）保護対象の可搬メディアに対するラベル付け

保護対象の可搬メディアが外部の委託先も含む業務現場で適切に取扱われるためには、当該可搬メディアに指定された保護要件が認識できるようなラベルが明示されるようにしなければならない。

このラベルとして表示されるべき項目としては、以下があげられる。

- 管理者、管理番号、機密レベル（例えば「極秘」「社外秘」等）
- 開示対象者、開示範囲、開示手段
- 指定された保護要件
  - ・利用（新規保存／複製等）時の保護要件
  - ・配布（輸送／社外持ち出し）時の保護要件
  - ・保管時の保護要件
  - ・廃棄／再利用時の保護要件

なお、「極秘」「秘」「社外秘」といったように、あらかじめ管理クラスを分けた上でそれぞれの管理クラスにおける利用／配布／保管／廃棄時の保護要件を定めておき、その管理クラスのみを印刷物にラベリングすることによって、個別の可搬メディアに対して詳細に保護要件を記述する手間を省略することができる。

（5）管理ルールの周知徹底

保護対象情報が記録された可搬メディアが、業務現場で適切に取扱われるためには、まずはその管理ルールが周知徹底されなければならない。周知徹底の主な手段としては、定期的な教育のほか、日常的な啓蒙活動も重要である。

（6）業務現場における管理ルールの遵守

業務現場には、サーバ等のデータバックアップに用いて組織的に管理する可搬メディア(DVD,DAT 等)の他に、個々の従業員がデータ受け渡し等に用いて個人的に管理している可搬メディア（USB フラッシュメモリ、フロッピーディスク等）が存在する。

いずれのタイプの可搬メディアであっても、保護対象情報が記録されたものについては、可搬メディアのライフサイクルに沿って定義された保護要件を、各従業員が適切に遵守しなければならない。可搬メディアの取扱いについて、得に留意すべき事項を表 2-8 および表 2-9 に示す。

表 2-8　組織的に管理する可搬メディアの取扱いで特に留意すべき事項

ライフサイクル	保護要件の指定事項
利用（新規保存･複製等）時	不正な利用の制限
	利用記録／ログの取得
	利用時の留意事項の指定
配布（輸送）時	配布手段の指定（情報の暗号化、本人限定受取郵便など）
	配布手続き（承認手続きなど）の明確化
	配布記録（受取確認書等）の取得
保管時	保管方法（施錠キャビネットなど）の指定
	可搬メディアの入出庫管理（アクセスの管理）の実施
	アクセス記録（台帳管理など）の取得
廃棄／再利用時	廃棄実施までの安全な保護手段（廃棄処理前の管理）

	廃棄／再利用方法（情報の完全削除など）の検討
	廃棄記録の取得

表 2-9　ユーザ個人的に管理している可搬メディアの取扱いで特に留意すべき事項

ライフサイクル	保護要件の指定事項
利用（新規保存･複製等）時	不正な利用の制限
	利用記録／ログの取得
	利用時の留意事項の検討
配布（社外持ち出し）時	持ち出し手段の指定
	持ち出し手続きの明確化
	持ち出し記録の取得
保管時	保管方法の指定
廃棄／再利用時	廃棄実施までの安全な保護手段（廃棄処理前の管理）
	廃棄／再利用方法の検討
	廃棄記録の取得

（7）業務現場等における可搬メディアの適切な取扱いを実現するための環境の整備

業務現場等における可搬メディアの適切な取扱いを実現するための環境の整備として、検討すべき事項としては、以下があげられる。

- 必要な装置や設備の準備

  可搬メディアの取扱いに対する管理ルールを遵守させるには、ルール遵守を従業員に一方的に押付けるだけではなく、ルールが自動的に遵守されるような機器･システムやツールを使うなど、環境面の整備が必要である。例えば、可搬メディアを接続する計算機の外部接続ポートを物理的に封鎖することで、不正な利用ができないようにすることが該当する。管理ルール遵守を担保する環境は、可搬メディアのライフサイクルに沿って網羅的に整備されることが望ましい。

- 管理ルール違反時の仕組みの確立

  業務現場において管理ルールの実効性を担保するためには、管理ルールが遵守されなかった場合に対応する仕組みを整えておくことが必要である。ルール違反発見時の報告体制や、懲罰等の対応方法が明確化されていることが求められる。

- 管理ルール遵守を定期的に確認する仕組みの確立

  業務現場において管理ルールの実効性を担保するためには、管理ルールの遵守状況を全部門･全従業員に渡って定期的にチェックし、問題があれば改善の指導をすることが必要である。また、結果を分析し、管理･取扱いルールを見直す際の材料としておくことも重要である。

【対応 ISMS コントロール】

5.1.1　資産目録
5.2.1　分類の指針
5.2.2　情報のラベル付けおよび取扱い
8.6.1　コンピュータの取外し可能な付属媒体の管理
8.6.2　媒体の処分

Ba3.3	情報機器の安全な取扱いについてのルールの確立と、ルールに沿った情報機器の取扱いの実践

【主旨】

外部への持ち出しを前提としたモバイル PC 等の情報機器は、内部利用の機器と比較して物理的なアクセス制限等の各種セキュリティ対策による保護が少なく、盗難／紛失の可能性が高いといえる。すなわち、社内にある情報機器と比較して、情報漏えいリスクが大きい。そのため、組織はこれらの情報機器の取扱いルールを決定し、情報機器の利用を適切に管理していく必要がある。取扱いルールの策定にあたっては利用／保管／輸送／廃棄といった情報機器のライフサイクルごとに策定することも必要となる。

業務現場における情報の保護を徹底するには、単に管理･取扱いルールを定めるだけではなく、業務現場の全従業員にルールを遵守させなければならない。そのためには、まずはルールを周知徹底させることが必要である。更に、ルール違反時の対応方法といった仕組みを作るとともに、ルールの遵守状況を定期的に確認してゆくことも必要となる。

モバイル PC 等の情報機器は外部に持ち出す機会が多く、盗難／紛失の可能性が高くなるゆえ情報漏えいリスクは高いといえる。このため組織は、モバイル PC 等の情報機器の管理･取扱いルールを定め、遵守を徹底してゆくことが求められる。

【対策のポイント】

(1) 保護要件の指定およびラベリングについての管理の仕組みの確立

情報機器に対する保護要件の指定が適切に行われるためには、その指定および指定状況がマネジメントされていることが必要となる。このためには、保護要件の指定およびラベリングについての管理の仕組みの確立することも必要となる。

情報機器の取扱いについての保護要件の指定およびラベリングについての管理の仕組みの確立に関し検討すべき事項としては、以下があげられる。

- 保護要件の指定者の明確化
- 保護要件の指定手順の明確化
- 保護要件を実行に移すためのプロセスの明確化

(2) 保護要件の指定

保護対象の情報機器が外部の委託先も含む業務現場で適切に取扱われるためには、保護対象の情報機器の個々に対してその取り扱い条件を示した保護要件が定義されていなければならない。保護対象の情報機器の個々に対してその取扱い条件として検討すべき事項としては、表 2-10 に示すようなものがある。

表 2-10 保護対象の情報機器の個々に対してその取扱い条件として検討すべき事項

ライフサイクル	保護要件	保護要件指定の具体例
利用時	不正な利用の制限（物理的保護）	･画面上に表示されている情報の保護 -プライバシーフィルタ（盗み見防止フィルタ）の利用
	不正な利用の制限（技術的、システム的保護）	･機器の不正使用防止機能の実装 -BIOS パスワード、HDD パスワード、ログオンパスワード ･利用者の離席時のキーボードロック機能の実装 -スクリーンセーバロック、ログオフ -トークンを利用したログオフ 等 ･システムの利用時間の制限（ログインタイムアウト） ･情報機器の機能限定化（シンクライアント化等）
	不正な利用の制限（その他）	･個人所有のモバイル PC 等の持ち込み禁止の義務化 ･社外で利用する際の遵守事項の明確化 -周囲に気を配る（覗き込み防止） -公共の場においたままにしない 等
	利用記録の取得	･システム的な利用ログの取得を実施
	利用時の留意事項	･離席時のキーボードロックの実行を義務化 ･帰宅時の電源断の義務化 ･パスワードの適正管理の義務化 -他人に教えない -付箋等にメモしない
移送（持ち出し）時	持ち出し手続きの明確化	･承認者、承認手続きの明確化 -審査部門の承認、上司の承認
	持ち出し記録の取得	･台帳管理（日時、場所、持ち出し先、理由等の記録）
	持ち出し時の留意事項	･社内外における機器の取扱いルールの明確化 -社員の携行義務化 電車の網棚に置かない、車中に放置しない 等
保管時	物理的保護	･機器を保管する場所への入室制限 ･機器の盗難防止対策の実施 -盗難防止ワイヤー -保管庫内での施錠保管の実施 -IC タグによる物品管理 等
	技術的、システム的保護	･機器の盗難防止対策の実施 -IC タグによる物品管理 等
廃棄時（再利用／保守時も含む）	廃棄実施までの安全な保護手段（廃棄処理前の管理）	･廃棄物保管場所への立ち入り制限
	廃棄方法の検討	･再利用手段の検討 -情報の完全削除 ソフトウェアイレーサ、磁気的な消去装置の利用 等 ･廃棄手段の検討 -情報の完全削除 ソフトウェアイレーサ、磁気的な消去装置の利用 等 -物理的な破砕処理 ･廃棄作業時のペアオペレーションの実施 ･完全消去済みの確認作業の義務化 ･外部業者に委託する際の検討 -信頼できる廃棄業者の選定 -機密保持契約の締結 -廃棄時の立会いの実施、または、廃棄処理証明の提出依頼 ･修理／保守作業時の管理 -外部の保守業者が操作する際も、データの削除を徹底する -保守契約に機密保持条項を盛り込む

	廃棄記録の取得	･作業実施報告書の提出 ･廃棄時の許認可手続きの記録

なお、上記ライフサイクルのすべてにおいて共通する保護要件として、情報機器内のデータ暗号化（HDD 暗号化等）が挙げられる。この場合、暗号鍵の管理ルールを明確にしておく必要がある。

(3) 管理ルールの周知徹底

モバイル PC 等の情報機器が、業務現場で適切に取扱われるためには、まずはその管理ルールが周知徹底されなければならない。周知徹底の主な手段としては、定期的な教育のほか、日常的な啓蒙活動も重要である。

(4) 業務現場における管理ルールの遵守

モバイル PC 等の情報機器が、業務現場で適切に取扱われるためには、情報機器のライフサイクルに沿って定義された保護要件を、各従業員が遵守しなければならない。その中でも、電子機器の取り扱いにおいて、特に留意すべき事項を、表 2-11 に示す。

表 2-11 電子機器の取り扱いにおいて特に留意すべき事項

ライフサイクル	保護要件の指定事項
利用時	不正な利用の制限（PC 起動制御、キーボードロックなど）
	利用記録／ログの取得
	利用時の留意事項の検討（離席時のキーボードロック等）
輸送（持ち出し）時	持ち出し手続き（承認手続きなど）の明確化
	持ち出し記録の取得
	持ち出し時の留意事項（常時携行など）の検討
保管時	保管方法の指定
廃棄時（再利用／保守時も含む）	廃棄実施までの安全な保護手段（廃棄処理前の管理）
	廃棄方法の検討
	廃棄記録の取得

(5) 管理ルールの遵守を担保する環境の整備

業務現場等における可搬メディアの適切な取扱いを実現するための環境の整備として、検討すべき事項としては、以下があげられる。

- 必要な装置や設備の準備

  情報機器の取扱いに対する管理ルールを遵守させるには、ルール遵守を従業員に一方的に押付けるだけではなく、ルールが自動的に遵守されるような機器･システムやツールを使うなど、環境面の整備が必要である。例えば、ハードディスクを暗号化する専用ソフトウェアを全てのモバイルＰＣに実装し、万が一盗難にあっても情報漏えいのリスクを最小限に抑えることが該当する。管理ルール遵守を担保する環境は、情報機器のライフサイクルに沿って網羅的に整備されることが望ましい。

- 管理ルール違反時の仕組みの確立

  業務現場において管理ルールの実効性を担保するためには、管理ルールが遵守されなかった場合に対応する仕組みを整えておくことが必要である。ルール違反発見時の報告体制や、懲罰等の対応方法が明確化されていることが求められる。

- 管理ルールの遵守を定期的に確認する仕組みの確立

業務業務現場において管理ルールの実効性を担保するためには、管理ルールの遵守状況を全部門･全従業員に渡って定期的にチェックし、問題があれば改善の指導をすることが必要である。また、結果を分析し、管理･取扱いルールを見直す際の材料としておくことも重要である。

【対応 ISMS コントロール】

9.8.1 移動型計算処理

Ba3.4	その他の電子機器の安全な取扱いについてのルールの確立と、ルールに沿った使用の実践

【主旨】

プリンタ、デジタル複合機、携帯電話、デジタルカメラ、IC レコーダーなど、PC や可搬メディア以外にも、日常的に情報を取り扱う各種情報機器があり、それぞれに情報漏えいのリスクが存在する。そのためこれらの機器についても管理ルールを定め、適切にルールを遵守する仕組みを作る必要がある。

【対策のポイント】

(1) 管理対象機器の特定、および管理対象機器の保護要件の検討

保護対象の情報機器が業務現場で適切に取扱われるためには、まず、保護対象の機器を特定し、保護対象の情報機器の個々に対してその取り扱い条件を示した保護要件が定義されていなければならない。

これらの情報機器の保護要件は、基本的には PC や可搬メディアと同様であるが、各情報機器の特性によって別途検討しなければならない保護要件も存在する。そのため、上述した保護要件（印刷物、可搬メディア、モバイル PC）に準ずる保護要件を定めることの他に、例えば表 2-12 に示すようなことも別途検討する必要がある。

表 2-12 電子機器の取扱いに関し特別に検討を要する事項

その他の機器の例	保護要件（物理的、技術的、人的）の指定を検討すべき事項
デジタル複合機 （コピー、FAX、プリンタ、スキャナ）	･記憶装置内の情報を暗号化する機能の利用 ･外部からの不正アクセス対策 -電話回線を利用する機能の制限 -LAN からのアクセス制限 ･IC カード、パスワード等による利用制限
携帯電話	･紛失時の情報漏えい防止対策 -パスワードロック -携帯電話内への保存内容の限定 ･公共の場における機密会話の制限 ･のぞき見防止の対策
デジタルカメラ	･紛失時の情報漏えい防止対策 -記憶媒体内の情報の完全消去の徹底

	･社内における不正利用の禁止 ･情報の消去のし忘れ防止対策
IC レコーダー	･紛失時の情報漏えい防止対策 　-記憶媒体内の情報の完全消去の徹底 ･社内における不正利用の禁止 ･情報の消去し忘れ防止対策

⑵ 管理ルールの周知徹底

その他の情報機器が業務現場で適切に取扱われるためには、まずはその管理ルールが周知徹底されなければならない。周知徹底の主な手段としては、定期的な教育のほか、日常的な啓蒙活動も重要である。

⑶ 業務現場における管理ルールの遵守

⑴の保護要件に対応して定められたルールを業務現場の従業員一人一人が適切に遵守していることが求められる。

⑷ 管理ルールの遵守を担保する環境の整備

業務現場等におけるオフィス用の電子機器の適切な取扱いを実現するための環境の整備として、検討すべき事項としては、以下があげられる。

- 情報の保護機能のある危機の採用と保護機能の適切な使用法の確立
- 管理ルール違反時の仕組みの確立

  管理ルールの実効性を担保するためには、ルールが遵守されなかった場合に対応する仕組みを整えておくことが必要である。ルール違反発見時の報告体制や、懲罰等の対応方法が明確化されていることが求められる。
- 管理ルール遵守を定期的に確認する仕組みの確立

  管理ルールの実効性を担保するためには、ルールの遵守状況を全部門･全従業員に渡って定期的にチェックし、問題があれば改善の指導をすることが必要である。確認すべき事項としては、以下があげられる。

  ･施設･設備等の物理的な管理ルールの遵守確認

  ･人的な管理ルールの遵守確認

  ･システム的･技術的な管理ルールの遵守確認

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

2.1.4. **ユーザ管理の徹底**

Ba4.1	ユーザ管理についてのルールの確立とルールに沿ったユーザ管理の実施

【主旨】

ユーザによる情報システム資源への不正なアクセスの防止は、情報システム資源へアクセス管理にかかっている。このアクセス管理が適切に行われるためには、まず、システムのユーザ、すなはちアクセス要求をする者の資格の確認とか、これらの者に対するアクセス権の付与が適切に行われていなければならない。本要求は、システム資源へのアクセスを管理するための基本となる、ユーザの資格の管理ならびにユーザに与えるシステムへ資源へのアクセスにかかる権限の付与を的確なものにすることを求めるものである。

【対策のポイント】

(1) ユーザ管理の仕組みの確立

ユーザエンティティの管理やユーザへのアクセス権の不要の的確性を確保するためには、ユーザ管理にかかわるさまざまなルールと、これらの確実な運用を実現するための組織的な仕組みの確立が欠かせない。

ユーザ管理の仕組みとして検討すべき事項としては、表 2-13 に示すようなものがあげられる。

表 2-13　ユーザ管理の仕組みの確立で検討すべき事項

区分	検討すべき事項
管理単位	ユーザエンティティの管理やアクセス件の管理についての要求は、使用場面によって異なったものとなる。このため、ユーザの管理やアクセス権の付与についての管理の仕組みは、管理単位ごとの策定されなければならない。 ・ユーザ管理の必要場面（アクセス管理が必要な場面と必要なアクセス管理の大枠） ・管理責任者
管理単位ごとの管理ルール	・ユーザエンティティの管理 －ユーザの個々に対する管理情報（ユーザの属性情報等）の取得ならびにその確認手続き －ユーザおよびユーザ管理情報の登録、変更、抹消の手続き －登録ユーザおよびユーザ管理情報の点検ルール ・アクセス権の付与の管理 －ユーザに付与するアクセス権限の範囲とアクセス権限付与のルール －ユーザへのアクセス権限付与、変更、抹消の手続き －ユーザに付与したアクセス権の点検ルール ・認証方式の承認手続き ・認証に用いる情報の管理 －ID/パスワード等のユーザに認証に用いる情報の取扱いルール ・ID/パスワード等の設定ルールと設定手続き ・ID/パスワードのユーザへの引渡しに手続き －ID/パスワード等のユーザに認証に用いる情報の管理方法 ・ユーザ管理情報や付与したアクセス権のシステムへの登録の管理 －ユーザおよびユーザ管理情報のシステムへの登録、変更、抹消手続き －システムに登録しているユーザならびにユーザ管理情報の点検ルール －システムへのユーザに付与したアクセス権限の登録、変更、抹消の手続き －システムに登録されたユーザに付与したアクセス権限の点検ルール

(1) ルールに沿ったユーザエンティティの管理の徹底

ユーザエンティティに関する管理のポイントとしては、以下があげられる。

- 登録するユーザの正当性（本人性ならびに実在性）の確認

  利用権限が付与されるユーザに正当でないものが含まれないようにしなければならない（他をかたっての登録等を避けるため)。登録するユーザ自体の信頼性を確保するためには、ユーザ管理の重要度に応じた厳格さで、登録ユーザの本人性や実在性の確認を行わなければならない。

  一般的に用いられる確認手法としては、以下がある。必要に応じ、これらを組合せることも検討すべきである。

  ・公的な証明書による確認
  ・電子証明書による確認
  ・電話やメールの着信による確認
  ・面談や訪問による確認
  ・第三者を用いた確認

- 登録ユーザの管理に用いる情報（属性情報）の正確な把握

  登録ユーザの管理に用いられるユーザの属性情報の把握は正確でなければならない。このことを実現するためには、取得する情報の個々について定められたルールに沿った確認が行われなければならない。

  公的な資格等の場合のように、情報によっては、本人の申請だけでなく傍証のよる確認も必要となる。

- 登録ユーザに関し管理している情報の正確性の維持

  ユーザの登録は定められたルールに沿って行われなければならない。ユーザの登録抹消やユーザ管理情報（ユーザに関する諸情報）が変更になった場合における登録情報への迅速な反映も欠かせない。

  ユーザ情報の管理に不手際が生じているのを見逃さないようにするためには、ルールに沿った定期的な点検も欠かせない。

(2) ユーザへのアクセス権の付与の管理の徹底

ユーザへのアクセス権の付与の管理のポイントとしては、以下があげられる。

- 利用者権限の適切なグルーピング
- それぞれのグループに与える利用権限の範囲

  利用権限が付与は、可能な範囲できめ細かくすべきである。

- 利用権限の付与におけルールの遵守との所定の手続きを踏んだ付与
- ユーザの資格の変更他の付与したアクセス権の見直しや変更の必要が生じた場合における、必要な変更の迅速な実施
- ルールに沿ったアクセス権の付与状況の点検の実施

(3) 認証に用いる情報の管理の徹底

ユーザの認証に用いる情報の管理のポイントとしては、以下があげられる。

- ルールに沿った認証情報の作成

- ルールに沿った認証用情報のユーザへの引渡し
- ユーザの認証に用いる情報に対する適切な保護の実施(この要求については、Ba3.1、Ba3.2、Ba3.3、Ba3.4 参照)

⑷ ユーザ管理情報や付与したアクセス権に関する情報のシステムへの正確な登録

システムに登録されたユーザ管理情報や付与したアクセス権に関する情報を、常に、正確なものとして維持するためには、以下が求められる。

- システムへの登録や変更の要が発生した場合の遅滞のない必要なシステム処理の実施
- 定められた手順に沿ったこれらの情報のシステムへの登録と、登録時の確認の徹底
- 定められたルールにもとづくシステムへの登録情報の点検の実施

【対応 ISMS コントロール】

9.2.1 利用者の登録
9.2.3 利用者のパスワードの管理
9.2.4 利用者のアクセス権の見直し

Ba4.2 なりすまし防止に向けたユーザに対する指導の実施

【主旨】

ユーザサイドにおける認証用の情報のずさんな取扱いは、その不正な使用を招き、なりすましによるシステム資源へのアクセスを許すことにつながる。ユーザのそれぞれが自らに割当てられた認証情報を適切に取扱うようにするためには、ユーザに対するこれらの情報の適切な取扱いについての指導が必要となる。

【対策のポイント】

⑴ ユーザに対するユーザ管理にかかわる情報の取扱いについての指導の実施

ユーザサイドにおけるユーザ管理にかかわる情報の取扱いを適切なものにするために実施すべきこととしては、以下があげられる。

- ユーザサイドにおけるこれらの情報の取扱いについての留意事項の明示

  まず、ユーザが守らなければならないことを周知させなければならない。このためには、以下のうようなことが必要となる。

  ・ユーザサイドにおけるこれらの情報の取扱いガイドの作成と交付
  ・ユーザ登録時におけるユーザへのこれらの周知の実施
- ユーザサイドにおけるこれらの要求への対応状況の点検と注意の喚起の定期的な実施

【対応 ISMS コントロール】

9.3.1 パスワードの使用

2.1.5. 法的要求事項の遵守

Ba5.1	ビジネスパートナーとの契約からの要求の遵守

【主旨】

法的要求事項のうち、いわゆる強行法規や法的規制に属するものと、当事者間の合意により取り決められるものとがあるが、ここでは後者が取り扱われる。情報セキュリティに関連して、ビジネスパートナーとの契約上、さまざま要求事項が想定されうる。ここで言う契約には、法律的には一般的な基本契約から、情報セキュリティに固有の運用マニュアルと呼ばれる種類の取り決めに至るまで、多様なレベルの合意が含まれる。

情報セキュリティの側面から、ビジネスパートナーとの契約からの要求の遵守を実現するためには、法的に表現されている制約を洗出し、担当者レベルまでその遵守に必要なことを具体化し、その履行がチェックされなければならない。

【対策のポイント】

(1) 対象となる契約からの制約の洗出し

契約上、法的に表現されている制約を情報セキュリティの面から洗出す必要がある。一般に対象として考えられるものとしては、以下のようなものがある。

- 契約上の守秘義務に関する事項
- 情報セキュリティに関して、一定のサービスレベルに関する事項
  - ・可用性や通信の速度や安定性に関する事項
  - ・データの保存期間、方法等に関する事項
- データ交換協定書や運用マニュアルに関する事項
  - ・基本契約との関係
  - ・データ交換の安全および信頼性確保のための手順確認
  - ・事故発生時の対応手順の確認
- 商法、有限会社法及び株式会社の監査等に関する商法の特例に関する法律の関係規定に基づく電磁的方法による情報の提供等に関する承諾の手続等を定める政令
  - ・電磁的方法によることへの株式申込人などの承諾など

(2) 該当する制約への組織としての対応策の確立と対策現場への展開

契約等からの制約の遵守のためには、まず、組織としてのこれらの制約への具体的な対応策を確立し、これらを関係部署に展開するとともに、必要な場合には、関係する規程や手順の変更を行う必要がある。

- 関係業務現場への要求の展開
  - ・要求事項の明確化と関係者への周知

・業務規程や業務要領への反映

- システムへの要求の展開

・要求事項の明確化と関係者への周知

・システムへの必要機能の組込み

- システム運用への要求の展開

・要求事項の明確化と関係者への周知

・システム運用規程やシステム操作マニュアルへの反映

(3) その実施を確実にするための仕組みの確立

展開された具体策を各業務において確実に遵守するためには、以下が必要となる。

- 管理責任者の明確化
- 実施担当者および実施手順の明確化

(4) 関係職場における要求事項の徹底

契約上の要求事項への対応が要求される職場においては、指定された要求の実践に努めなければならない。これらの実践を徹底するためには、関係する管理の仕組みに沿った実行のチェックを厳格に行うことも必要となる。

(5) 定期的あるいは必要に応じた見直し

要求事項の見落としや、対応策の不備や、実施上の不手際や徹底の欠如等が見逃されないようにするためには、要求事項の把握とその理解、対応策の妥当性、実施の徹底度と的確性について、定期的な見直しを行い、問題点については必要な改善措置を実施しなければならない。

また、契約の変更等の業務環境の変更や、問題が生じた場合は、適宜、関連事項についての見直しを行わなければならない。

【対応 ISMS コントロール】

12.1.1 適用法令の識別

【参考】

ビジネスパートナーといってもその関係により、契約内容にも様々なものがありうるが、例えば次のようなものが想定される。

- 取引(契約)
- 業務委託(または受託)
- 業務コラボレーション(例えばSCMなど)
- 株主や債権者との契約

Ba5.2	事業に関係する法令やその他のルールの遵守

【主旨】

法的要求事項のうち、いわゆる強行法規や法的規制に属するものと、当事者間の合意により取り決められるものとがあるが、ここでは前者が取り扱われる。法令その他のルールといっても直接に情報セキュリティ一般をまとめて規定するものではなく、各業法等で個別に規定されるものが多い。また、必ずしも罰則を伴わない規定もあるが、その場合にも取引上の不利益を被るものがある。

法令その他のルールの遵守は、直接に自社の情報セキュリティの強化につながるものではないことも多いが、共同体全体の情報セキュリティの強化の視点ばかりでなく、法令その他のルール遵守が、不法行為その他の法的責任を免れさせる場合も多い。また、法令ではないが、公的または私的な組織から公表されている各種のガイドラインがあり、情報セキュリティの一定の基準として留意することが必要である。

【対策のポイント】

(1) 対象となる法令その他ルールの制約の洗出し

一般法としての不法行為 (民法709条) のほか、情報セキュリティに関わる法令その他のルールとして主なものには、次のようなものがある。

- 業法関連
  - ・特定商取引に関する法律
    - ー インターネット通販に関しては、特商法11条および特商規則8条の広告記載事項あり
  - ・電子契約法(電子消費者契約及び電子承諾通知に関する民法の特例に関する法律)
    - ー電子消費者契約に関しては、事業者が操作ミスを防止するための措置を講じること
  - ・景品表示法 (消費者向け電子商取引における表示についての景品表示法上の問題点と留意事項 (平成14年6月5日公正取引委員会)
    - ー取引条件の具体的内容を正確かつ明瞭な表示
    - ー重要事項に関してはリンク先内容の明示
    - ー最終更新日の明示
  - ・電子署名法 (電子署名及び認証業務に関する法律)
    - ー特定認証業務の指定要件
  - ・改正古物営業法
    - ー インターネット・オークションのサイト運営者は「古物競りあっせん業者として営業届出その他の義務を負う
  - ・プロバイダ責任制限法(特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律)
    - ー プロバイダ責任制限要件の充足
  - ・特定商取引に関する法律の改正、特定電子メールの送信の適正化等に関する法律

－「未承諾広告※」表示義務

- 個人情報保護関連
  ・個人情報保護法（2005年4月施行）（個人情報取り扱い事業者の義務）
    －利用目的の特定（15条）
    －利用目的による制限（16条）
    －適正な取得（17条）
    －利用目的の通知または公表（18条）
    －安全管理措置（20条）
    －従業員・委託先の監督（21・22条）
    －第三者提供の制限（23条）（オプトアウト）
    －利用目的を本人の知り得る状況に置く（24条）
    －本人の求めによる開示・訂正・利用停止（25－27条）
    －苦情の適切かつ迅速な処理（31条）
  ・電気通信事業における個人情報保護に関するガイドライン
    －収集
    －利用及び提供
    －適正管理
    －開示及び訂正
    －その他
- 文書管理関連
  ・電子計算機を使用して作成する国税関係帳簿書類の保存方法の特例に関する法律
    －所得税及び法人税に係る保存義務者は、電子取引を行った場合には電磁的記録の保存義務（10条）
  ・IT 書面一括整備法
    －対象であれば電磁的記録が許容
  ・e 文書法（2005年4月施行）
    －対象であれば電子化が許容
- ソフトウエアの著作権関連
  ・管理対象のソフトウエアとライセンス契約内容の把握
    －インストール数とライセンス数の把握
    －従業員その他による不正コピーの排除
    －ライセンス契約終了時のユーザの義務
    －パッケージの転売とライセンス
  ・ソフトウエアの使用に定められたセキュリティ要求事項の洗出し
    －バグに関する担保責任
    －ソフトウエアの加工制限
    －契約終了の担保措置の効力
- ソフトウエア以外の知的財産権関連

・不正競争防止法違反
　－営業秘密
　－技術的制限手段により制限されているコンテンツ
　－ドメイン名
・著作権違反
　－他人の著作物を利用するホームページ
　－フレーム

⑵ 法令その他のルールによる制約の組織としての対応策の確立と対策現場への展開

法令等にからむ制約の遵守のためには、まず、組織としてのこれらの制約への具体的な対応策を確立し、これらを関係部署に展開するとともに、必要な場合には、関係する規程や手順の変更を行う必要がある。

- 関係業務現場への要求の展開
　－要求事項の明確化と関係者への周知
　－業務規程や業務要領への反映
- システムへの要求の展開
　－要求事項の明確化と関係者への周知
　－システムへの必要機能の組込み
- システム運用への要求の展開
　－要求事項の明確化と関係者への周知
　－システム運用規程やシステム操作マニュアルへの反映

⑶ その実施を確実にするための仕組みの確立

展開された具体策を各業務において確実に遵守するためには、以下が必要となる。

- 管理責任者の明確化
- 実施担当者および実施手順の明確化

⑷ 関係職場における要求事項の徹底

契約上の要求事項への対応が要求される職場においては、指定された要求の実践に努めなければならない。これらの実践を徹底するためには、関係する管理の仕組みに沿った実行のチェックを厳格に行うことも必要となる。

⑸ 定期的あるいは必要に応じた見直し

要求事項の見落としや、対応策の不備や、実施上の不手際や徹底の欠如等が見逃されないようにするためには、要求事項の把握とその理解、対応策の妥当性、実施の徹底度と的確性について、定期的な見直しを行い、問題点については必要な改善措置を実施しなければならない。

法令その他のルールは、改正や更新されることが予想されるため、常時、現行の法令その他のルールを監視する必要がある。関係する法令が変更されたり、新たな法令が作られた場合や、関係する業務環境の変更や、問題が生じた場合は、適宜、関連事項についての見直しを行わなければならない。

【対応 ISMS コントロール】

12.1.1 適用法令の識別
12.1.2 知的所有権(IPR)
12.1.4 データの保護および個人情報の保護

Ba5.3	紛争の発生への備えの実施

【主旨】

情報セキュリティの確保に努力していても、情報セキュリティには万全はありえないため、情報セキュリティ関連の法的紛争に巻き込まれることもありうると考えておかなければならない。このため、そのような場合に対して予め備えることが賢明である。被告側として防御のための備えが中心的課題であるが、場合によっては、相手側に請求することも想定する必要があり、また、業態によっては、関係者として証拠の提出を求められることもありうる。

紛争の発生への備えとしては、どのような手順で紛争に対応するかという問題と、どのようにして証拠記録を確保するかという二つの課題がある。

【対策のポイント】

(1) 予想される紛争の洗出し

予想される紛争の種類と状況により、後の対応と備えるべき記録とが想定されることになる。契約の形態にはさまざまなものがあるが、一応、契約がある場合には、契約内容遵守の立証のための記録は容易に想定される。

- 被告としての場合
  ・契約の相手方が原告(契約違反)
  ・契約関係にない相手方が原告(不法行為)
  －知的財産権侵害等
- 原告としての場合
  ・契約の相手方が被告(契約違反)
  ・契約関係にない相手方が被告(不法行為)
  －無権限アクセス等
- 関係者としての場合
  ・プロバイダー事業者等データ保管者の場合

(2) 紛争発生時の対応

紛争発生時の対応は、情報セキュリティ関連以外の紛争と大きく異なるところはない。ただし、合意管轄による裁判のためには、書面による合意が必要である(民事訴訟法11条)ことには注意を要する。

(3) 記録確保

裁判上の証拠としての記録確保は、証拠力の確保の観点から改竄の可能性を排除する方法で行われることが必要であり、また、どの記録をどのような手順で保管するかを一定のルールで処理することが便宜である。

- 必要な証跡の明確化
- 保管すべき証跡の取得と保管要領の確立
  ･取得すべき記録の内容
  ･保管の方法と手続き
  ･実行状況のチェック要領
- 必要なリソース等の準備
  ･格納媒体や保管庫等の必要な設備の準備
  ･必要な書式等の整備
- 証跡の取得と保管の業務運用やシステム運用への反映
  ･業務運用規程や業務要領への反映
  ･システム運用規程やシステム運用要領への反映
  ･関係部署、関係者への周知
- 規程に沿った証跡の取得と保管
  ･規程に沿った取得
  ･規程に沿った保管と管理

なお、関係する文書や記録等を電子情報の形態で保管する場合は、保管期間を通じてのその有効性の確保に努めなければならない。電子情報の保管については、Td1.1、Td1.2、Td1.3Td1.4 を参照。

⑷ 紛争への備えとして定められたことの確実な実施

各職場に要求される紛争への備えを確実に実施するためには、以下のようなことが必要となる。

- 管理責任者の明確化
- 実施担当者および実施手順の明確化
- 実施記録

【対応 ISMS コントロール】

12.1.7 証拠の収集

3. テクニカル＆オペレーション･ビュー

3.1. システムの信頼性の確保

3.1.1. システムの処理の正確性の確保

Ta1.1	システムの処理の正確性の確保のための仕組みの確立

【主旨】

IT システムの処理の正確性を確保するためには、システムの開発段階から運用を通じての多岐の作業にわたり、その正確性の確保のための活動が必要となる。これらが適切に行われるようにするためには、システムの正確性の確保のための組織的な仕組みの確立も必要となる。

このような仕組みが確立していない組織においては、システムの処理の正確性の確保は、開発チーム他の関係者の個々の認識やスキルに依存することになるため、正確性についての組織的な保障は期待できない。

【対策のポイント】

(1) 開発プロセスの標準の確立

開発されたシステムの処理の正確性の確保を図るためには、開発過程がマネジメントされていなければならない。開発過程のマネジメントのためには、開発プロセスが確立されていなければならない。開発プロセスは組織の実態に合ったものであるとともに、対象システムの特性から来る正確性の保障レベルに応じ、開発プロジェクトに合わせ、柔軟に適用できるものであることが要求される。

開発プロジェクトごとの開発プロセスを適切なものとして決めるためには、典型的なタイプの開発形態に対するを開発プロセスの標準を確立しておかなければならない。

(2) 責任体制明確化

システムの処理の正確性の確保を図るためには、IT システムの処理の正確性の確保にかかわる組織や関係者の責務や相互の連携方法が明確にされていなければならない。検討すべき事項としては、以下のがある。

- 業務グループ単位の総括責任者とその責務
- 個々の業務システムに対する業務サイドでの責任者とその責務
- 個々の業務システムの開発にかかる責任者とその責務

(3) 業務(群)ごとの正確性の保証要件の明確化

業務処理の正確性は対応システムの品質に依存する。システムの品質をどのレベルで担保するかについては、以下を明確にする必要がある。

- 業務(群)ごとの誤処理の防止･検出機能についての要求の明確化

・処理要求の妥当性チェックについての要求
・入力のチェックについての要求
・ファイルの整合性チェックについての要求
・処理結果の整合性チェックについての要求

- 業務(群)ごとの処理結果のチェックについての要件の明確化
  ・チェック対象の出力とチェックポイント
  ・チェックのタイミング
- 正確性の要求レベルごとの開発システムに対する検証のレベルの明確化
  ・業務仕様の妥当性・的確性のレビューのレベル
    ー検証の方法、チェックの精度、合格基準他
  ・処理方式のレビューのレベル
  ・プログラムの機能レビューのレベル
  ・プログラムテストのレベル
  ・検収テストのレベル
- テストデータ、テスト結果の保管についての要件の明確化

(4) システム稼働後における不良の顕在化に対する正確性の見直し基準の確立

システム稼働後に不良が他出したような場合においては、対象システムの正確性についての見直しが必要となる。正確性の見直しが、適宜、行われるようにするためには、見直しの実施についての基準を定めておくことも有効である。

この基準として検討すべき事項としては、以下のようなものがある。

- 見直しを必要とする状況
- 業務仕様の妥当性・的確性のレビューのレベル(検証の方法、チェックの精度、合格基準他)
- 処理方式のレビューのレベル
- 業務仕様の不備に対する見直しのレベル
- プログラム不良に対する見直しのレベル
- 業務サイドにおける処理のチェックの不手際に対する見直しの基準

【対応 ISMS コントロール】

10.2.1 入力データの妥当性の確認
10.2.2 内部処理の管理

Ta1.2 システムの業務仕様の定義の正確性の確保

【主旨】

業務仕様が的確でなかったり、業務現場や対応システムへの開発要求への業務仕様の展開が不適切であれば、サポートする IT システムや業務現場における業務処理は正確なものとなりえない。このため、業務仕様の正確性の保障と、業務現場や対応 IT システムの開発要求への展開を適切に行うためには、以下のようなことが要求される。

【対策のポイント】

(1) 業務タイプごとの業務仕様の検討プロセスの確立

業務仕様が的確なものとして設計されるためには、その検討プロセスがマネジメントされていることが必要となる。検討プロセスが適切にマネジメントされるためには、業務仕様の検討についても、その検討プロセスが確立していることが望ましい。

確立すべき検討プロセスで明確にすべきこととしては、下表に示すようなものがある。

- 検討手順
- 検討体制
- 仕様書等関係文書の様式の確立

検討の対象の範囲や検討の進め方等は、業務仕様の特性により大きく異なるため、標準とする検討プロセスも、業務の特性に合わせ、いくつか準備するのが望ましい。

(2) 規程に沿った業務仕様の検討の実施

(3) 保証要件に沿った業務仕様の妥当性･的確性についてのレビューの実施

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない

Ta1.3 アプリケーションソフトからの不良の排除（アプリケーションソフトの品質の確保）

【主旨】

IT システムにおける業務の処理に問題があれば、正確な業務処理は期待できない。IT システムが業務仕様を正確に反映したものであるようにするためには、業務ソフトの開発において、業務仕様の誤解、処理条件の見落としやロジック不良等の開発過程にはつきもののミスが見落とされたまま、開発されたシステムが運用に供されないようにしなければならない。

【対策のポイント】

(1) 開発プロジェクトごとの適切な開発計画の確立

不良の少ない品質の高いアプリケーションソフトを開発するためには、まず、当該開発に適切な開発計画を確立しなければならない。開発計画に不備があると、開発に無理や管理の不良を招き、これらは確実に開発するアプリケーションの品質に影響する。

開発計画の検討においては、体制の問題や生産性の確保等も検討要素となるが、品質の確保について特に検討すべき事項としては、以下があげられる。

- 品質目標の設定
- 品質目標を実現するための方針の明確化
- 開発の各フェーズで行う品質管理の明確化
  - ・各フェーズに要求するレビューあるいはテストのレベル
    - ―処理方式のレビューのレベル
    - ―プログラムの業務機能レビューのレベル
    - ―誤処理防止や誤処理検出機能のレビュー
      - ・入力チェック
      - ・ファイルの整合性チェック
      - ・出力の整合性チェック
      - ・関連処理の出力結果の整合性のチェック
    - ―プログラムテストのレベル
    - ―検収テストのレベル
  - ・各フェーズで実施するレビューやテストの方法、必要とする情報
  - ・各フェーズで実施する品質管理における管理指標や評価の方法
- 品質管理の実施体制

(2) システムへの誤処理検出機能の組込み

システムの誤処理は、データベースうえの情報間での矛盾のチェックを行うことにより、検出することもできる。このようなチェックが可能なところについては、必ずこのようなチェックを行う機能をシステムに組込むようにしなければならない。

(3) 定められた開発プロセスに沿った開発作業の展開

(4) 開発の各フェーズにおける定められた品質管理の徹底

開発のフェーズごとに、当該アプリケーションソフトの正確性についての保障要件を満たすためのレビューやテスト、ならびに品質管理を徹底しなければならない。

品質管理で問題が指摘された場合は、必要な改善がその都度、図られなければならない。

(5) 必要に応じた品質管理にかかわる情報やテストデータ、テスト結果の確保

後日の品質に見直しには、開発時点での品質管理に関する記録や、テストで使用したデータやテストの結果を参照しなければならないこともある。

このため、必要となる品質管理にかかわる情報やテストデータ、テスト結果は、一定の期間か保管されるようにすべきである。保管の対象とすべきものは、開発計画で示されるべきである。

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない

Ta1.4	日々の業務運用での処理結果の妥当性チェックの実施

【主旨】

業務仕様の設計や業務システムの開発において、その的確性の確保に努力を尽くしたとしても、万全はありえず、業務処理上での誤処理を犯してしまうこともありうる。このような事態が発生しても、システムの誤処理が実害に結びつかないよう、また、その被害が小さいうちに、誤りの是正ができるようにするための工夫が必要となる。

このため、システムに誤処理検出機能の使用によるｼｽﾃﾑの誤処理の早期の発見や、業務現場での日常の業務処理においてシステムの出力の妥当性の確認が習慣付けられるようにすることも必要となる。

【対策のポイント】

(1) システムの誤処理検出機能の使用によるシステムの誤処理の早期発見の実施

データベース上の情報の矛盾のチェックにより、システムの誤処理を検出できるところもある。システムこのために準備された機能がある場合は、システムのジョブスケジュールの中にこれらの使用を組込み、定期的なチェックを行わなければならない。

(2) 業務現場における日常の業務運用における処理結果の妥当性チェックの習慣化

業務現場における日常の業務に中で、システムの出力について、業務面からチェックをすることを習慣化しておき、システムの誤処理を見逃さないようにすることも、システムの誤処理あるいは印刷ずれ等の処理の乱れが業務に影響を与えないようにするために有効である。

業務現場における日常の業務運用における処理結果の妥当性チェックの習慣化するためには、以下が必要となる。

- チェック事項の明確化
- 業務処理手順への組込み
- 異常発見時の対象要領の確立
- 業務現場への指導

【対応 ISMS コントロール】

10.2.4　出力データの妥当性の確認

Ta1.5	業務現場における問題発生時における対応能力の確保

【主旨】

業務処理現場での業務の処理や、IT システムに誤処理等の問題が発見された場合、発見された問題への対処は当然であるが、万全を尽くしたはずの業務処理や IT システムに、これらに問題が残されていたことは、未発見の問題がまだ残されている可能性も示唆している。

このため、発見された問題が、なぜ見過ごされていたかを分析し、その結果にもとづき必要に応じ業務仕様や IT システムの品質の再点検を行うことも必要となる。

【対策のポイント】

(1) 適切な問題分析（トラブルに結びついた背景の分析）の実施

- 構造的要因の抽出
- 必要な是正処置の明確化

(2) 障害対策全体に対する指摘された是正処置の反映

(3) 障害対策についてのノウハウの抽出と蓄積

(4) 業務（群）ごとの問題発生に伴う過去の処理やシステムの見直し要領の確立

業務処理（群）ごとに指定すべきこの見直し要領で検討すべき事項としては、以下のようなものがある。

- 見直しの体制の確立
- 過去の処理結果の見直しポイントとその実施要領
- 見直し結果の評価と必要な処置への展開

(5) 業務（群）ごとの問題発生に伴うシステムの見直し要領の確立

業務処理（群）ごとに指定すべきこの見直し要領で検討すべき事項としては、以下のようなものがある。

- 見直しの体制の確立
- 過去の処理結果の見直しポイントとその実施要領
- 見直し結果の評価と必要な処置への展開

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない。

3.1.2. 障害に対するシステムの堅牢性の確保

Ta2.1	障害に対する堅牢性の確保を実現するための方式の確立

【主旨】

システムを構成するさまざまな機器に発生しうるさまざまな障害が、システムが求められる可用性を損ねないようにするためには、必要に応じた障害の影響の回避策を講じる必要がある。障害機器の切離しやバックアップ機への切替え、縮退運転等による障害の影響の排除や、システム停止が生じても短時間で復旧するための情報の回復やシステムの復旧機能等のさまざまな障害対策機能をシステムに組込む必要がある。

これらの機能のシステムへの組込みや必要な設備等の準備は、費用がかかるだけでなくシステムの作りを複雑にするため、効率的にかつ期待通り機能するようにするためには、システムの全体を見渡した設計が必要となる。

【対策のポイント】

(1) 可用性についての要件の確立

障害対策の検討には、その前提となるシステムの可用性についての要件の正確な把握が必要となる。障害対策の検討の前提となる可用性の要件は、経営レベルのセキュリティ要求で示される業務(群)ごとの可用性の要件から、システムの処理方式やネットワークやシステムの構成から、表 3-1 に示すような単位で明らかにしておくことが必要となる。

表 3-1 可用性要件として明確にすべき事項

区分	明確にすべき事項
業務(群)ごとの可用性要件	・必要な許容発生頻度(MTTB) ・必要な許容ダウン時間(MTTR)
ネットワークについての可用性要件	・外部ネットワークに対する可用性要件(MTTB、MTTR) 　－通信路についての可用性要件 　－使用ネットワーク機器についての可用性要件 ・内部ネットワークに対する可用性要件(MTTB、MTTR) 　－通信路についての可用性要件 　－使用ネットワーク機器についての可用性要件
システムの構成機器のそれぞれについての可用性要件	・各サーバに対する可用性要件(MTTB、MTTR) ・その他の機器に対する可用性要件(MTTB、MTTR) 　－専用装置(ATM、認証装置他) 　－クライアント PC

ただし、これらについての要求は、可用性についての要求が厳しい場合にのみ、厳格に行う必要があるものの、可用性についての要求が総厳しくない場合や、負荷がそれほどでもなく、性能面で十分な余裕があると見込まれる場合は、大枠を検討する程度でいい。

(2) 可用性に影響を与える障害と要求される可用性への影響の明確化

必要となる障害対策のレベルは、対策の対象とする障害の要求される業務等への影響の大きさによって決まる。このため、想定される障害の個々について、業務の処理方式やシステムの構成の

大枠によって決まる業務への影響の度合いを把握しなければならない。

検討すべき事項としては、表 3-2 に示すようなものがあげられる。

表 3-2 各機器のシステムの可用性に与える影響についての検討事項

区分	明確にすべき事項
外部ネットワーク（群）ごとの障害タイプごとの業務（群）ごとへの影響	・評価対象の洗出し －障害の種類の網羅性 －障害の発生頻度の評価 －障害の種類と影響する業務（群）の組合せの網羅性 ・影響についての適切な評価
内部ネットワーク（群）ごとの障害タイプごとの業務（群）ごとへの影響	・評価対象の洗出し －障害の種類の網羅性 －障害の発生頻度の評価 －障害の種類と影響する業務（群）の組合せの網羅性 ・影響についての適切な評価
サーバ（群）ごとの障害タイプごとの業務（群）ごとへの影響の明確化	・評価対象の洗出し －障害の種類の網羅性 －障害の発生頻度の評価 －障害の種類と影響する業務（群）の組合せの網羅性 ・影響についての適切な評価
その他の機器（群）ごとの障害タイプごとの業務（群）ごとへの影響	・対象機器の洗出し（含む敷地外設置機器） ・各機器における評価対象の洗出し －障害の種類の網羅性 －障害の発生頻度の評価 －障害の種類と影響する業務（群）の組合せの網羅性 ・各機器における影響についての適切な評価
電源・空調等・建屋他の施設の障害の発生頻度と影響	・電源障害 ・空調障害 ・建屋自体他、システム全体にかかわる災害の影響

（3）それぞれの業務（群）ごとに設定した可用性目標の実現方式の明確化

それぞれの業務（群）ごとに、障害が発生したとしても設定した可用性を実現するための方式の大枠を明確にする。この検討で、検討すべきこととしては、以下があげられる。

- 機器の2重化
- 予備機の準備
- 各アプリケーションに組込む障害対策機能の大枠の明確化
- システムに組み込むべき障害対策機能

  ・障害対策機能を組込むべきアプリケーションのタイプ明確化

  ・対象となるアプリケーションに組込むべきあるいは使用する障害対策機能の大枠の明確化

  －障害検知機能、障害報告機能、影響の回避あるいは局所化機能、情報回復機能、サービス復旧機能他

  －待機系への切換え機能
- データのバックアップの取得要件

  ・バックアップ取得対象 DB あるいは情報

  ・バックアップの取得タイミング

  ・バックアップの取得方式

  ・取得バックアップの保管方法

- 運用による対応

⑷ 設定した可用性の目標についての見直しの実施

システムの環境の変化により可用性要件は変化する可能性がある。求められる可用性が変わっていることが見逃されたままになっていると、必要な可用性を確保ができなくなる場面も発生する。このようなことがないようにするためには、システムの周辺環境に変化が生じた場合は、設定した可用性の目標の見直しを行わなければならない。

⑸ システムが障害の発生に対し必要な堅牢性を実現するための方式についてお見直しの実施

システムの可用性についての目標値が変更されたり、システムの構成に変更が加えられた場合は、必要な障害対策は変化する可能性がある。このような事態が見逃されたままになっていると、必要な可用性を確保ができなくなる場面も発生する。このようなことがないようにするためには、可用性についての目標値が変更されたり、システムの構成に大きな変更が行われた場合は、障害対策の方式の見直しを行わなければならない。

【対応 ISMS コントロール】

11.1.1 事業継続管理手続き
11.1.2 事業継続および影響分析
11.1.3 事業継続計画の作成のための枠組み

Ta2.2	設計した障害対策機能のシステムへの的確な組込み

【主旨】

方式設計にそって、システムを構成する各機器に発生しうるさまざまな障害を意識して、必要な検知や対策機能の設計をひなければならない。この障害対策設計を適切なものとするためには、以下のようなことが必要となる。

【対策のポイント】

⑴ 目標とする可用性を実現するためのシステム構成の設計

要求 Ta2.1 で策定した方式を適切にシステム構成の設計に反映しなければならない。主な検討時効としては、以下があげられる。

- 構成や機器の 2 重化
- 予備機の配置
- 内部ネットワーク構成
- 内部ネットワーク上のサーバの配置
- システム構成上でのサービスや DB の配置

⑵ アプリケーションに組み込む障害対策機能の適切な設計

障害対策機能の組込みが必要なアプリケーションについては、その個々について必要な障害

対策機能を適切に設計しなければならない。検討すべき事項としては、当該アプリケーションが使用する機器のすべてについて、想定される障害ごとに、以下のような検討を行うのが本来である。ただし、この検討は相当に負荷がかかるため、可用性についての要求が厳しくないシステムや、余裕のあるシステムにおいては、重障害のみを対象にすることができる。

- 障害検知機能
- 検した障害の告機能
- 影響の回避あるいは局所化機能（待機系への切替や縮退機能等）
- 情報回復機能
- サービス復旧機能他

(3) アプリケーションに組み込む障害対策機能の的確な実装

障害対策機能の実装は、業務仕様のシステム化に比べ、テストのために障害現象を起こすことが容易ではないこと等から、その的確な実装は容易ではない。しかし、この障害対策機能に欠陥が残された状態では、傷害の発生の仕方によっては思わぬ事態を起こすことがあるので、難しいからといってその完全性の追求を怠ってはならない。

- 議事障害の発生方法
- 機能の確認方法
- テストの記録の確保

(4) 障害対策を機能させるために必要なシステムリソースの確保

設計した障害対策機能を期待通りに機能させるためには、障害対策機能が機能するために前提とするシステムのリソースの準備は欠かせない。検討の対象としては、以下があげられる。

- 予備機の準備
  －予備機の配備と即時使用可能状態の確保
  ・ネットワーク系機器に対する予備機の準備
  ・サーバに対する予備機の準備
  ・クライアント PC に対する予備機の準備
  ・その他機器に対する予備機の準備
- バックアップ情報の取得および保管用リソースの確保
- 情報の回復用ツールの整備
  ・適切なツールの選択と機能の確認
  ・即時使用可能状態の確保

(5) 施設や設備系の障害への備え

施設や設備系の障害への備えとして、準備すべき事項には以下があげられる。

- 電源障害に対する備え
  ・バックアップ電源の確保
    －必要な設備の設置
    －即時使用可能状態の確保
- 空調機の障害に対する備え
  ・バックアップ機の確保

－必要な設備の設置
－即時使用可能状態の確保

- 必要に応じたバックアップセンターへの切替え
  ･バックアップセンターの設置
  ･切替え方式の確立
  ･即時切替え可能状態の確保

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

Ta2.3	システム障害発生時の対応能力の確保

【主旨】

システム運用面での障害対策についての対応能力が欠けていれば、計画した障害対策は機能しない。システムの運用サイドが、システムに発生した障害に適切に対応できるようにするためには、以下が欠かせない。

- 障害発生時の対応要領の確立
- 関係者の対応能力の確保

【対策のポイント】

(1) 障害発生時の対処要領の確立

障害発生時には、システムの運用や業務の運用に何がしかの対処が必要となる。障害発生時におけるシステム運用面や業務運用面での処置が適切に行われるためには、障害発生時におけるシステム運用面や業務運用面での対処要領が適切に示されていなければならない。

障害発生に対する対処要領の中で明確にしておくべきこととしては、以下があげられる。

- 障害対策についての責任体制の明確化
- 障害発生時の即応体制の整備（－体制、連絡、報告他）
- 障害発生時の緊急処置の確立
  ･施設系の障害への緊急処置
  ･外部ネットワーク系障害への緊急処置
  ･内部ネットワーク障害への緊急処置
  ･主要サーバの障害への緊急処置
- システム障害の発生に対する対策手順の明確化
  －問題点の確認、対策方法の確定、実施の準備、対策の実施、対策実施後の確認
  ･外部ネットワークの障害に対する対策手順
  ･内部ネットワークの障害に対する対策手順

・主要サーバの障害に対する対策手順
・その他サーバの障害に対する対策手順
・クライアント PC の障害に対する対策手順
・その他機器の障害に対する対策手順

- 施設の外に設置した機器の障害に対する対策手順の確立
  －問題点の確認、対策方法の確定、実施の準備、対策の実施、対策実施後の確認
- オンラインコラボレーションをしている他社システムの障害に対する対策手順の確立

⑵ 関係者の対応能力の確保

障害字の対応は、日常的でないため不慣れなことと、技術的にもスキルが求められることから、システム運用関係者で障害発生時における対応にかかわる者は、必要なスキルを確保しているようにしなければならない。

このためには、日頃からの準備として、以下が求められる。

- 関係者への対処要領の徹底
  －マニュアル等必要文書の配布
  －実施要領についての教育
  －習熟度のチェック
- 関係者への異常の発見方法についての教育の実施
- 関係者への問題分析や対策の実施に必要なスキルの確保
  ・必要な知識・スキルの明確化
  ・関係者への必要な知識・スキルの取得方法の提示
  ・必要に応じた教育の実施
  ・必要な知識やスキルの取得状況の把握と取得推進のための必要な指導の実施
- 緊急処置についての訓練の実施
  ・実施計画の確立
  ・実施要領の確立
  ・実施サイクル
  ・訓練結果の評価と問題点の是正に向けた処置の実施

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

3.1.3. システムの性能の確保

Ta3.1	性能･容量管理の仕組みの確立

【主旨】

システムの性能･容量の確保は、前提とする負荷の設定、必要となる性能･容量を確保するためのシステム面での仕組み（方式）の設計とシステムへのその的確な実装に加え、計画した性能や容量の確保のために日常のシステム運用に求められていることの適切な実行、および、想定外の負荷の発生によるオーバーフローの予防のための、常日頃からの負荷の状況やシステムの性能特性や容量の使用状況についての監視と、問題が生じる前の性能強化対策等が適切の実施があっては始めて達成されるものである。

このため、このことが適切に行われるためには、責任体制の確立も含め、システムの性能や容量の計画やシステムへの実装と、性能や容量の維持を適切に行うための仕組みの確立が必要となる。

【対策のポイント】

(1) 性能や容量の管理についての責任体制の明確化

性能や容量の管理の責任体制として検討すべき事項には、以下がある。

- 負荷の分析ならびに性能や容量の要求の指定についての責任体制
- システムの負荷の監視と問題の指摘についての責任体制
- システムが要求された性能を確保することについての責任体制
- 関係者間の連携の仕組み

(2) 負荷の分析と性能･容量についての要求を管理する仕組みの確立

システムに要求される性能や容量の指定が、的確な負荷の分析の上に立って適切に行われるようにするためには、以下が必要となる。

- 負荷の分析要領の確立

  負荷の分析要領として示すべきこととしては、以下のようなものがある。

  ･分析事項およびチックポイントの明確化

  －分析事項

  －分析事項ごとのチェックポイントと測定法

  －分析事項ごとのチェックサイクル

  ･負荷分析のプロセス

  －日常業務に組み込む事項とその実施要領

  －分析事項群ごとの評価手順

- 負荷分析にもとづく要求性能や容量の指定要領

  負荷分析にもとづく要求性能や容量の指定要領として示すべきこととしては、以下のようなものがある。

・要求性能や容量の指定プロセス
・指定されたプロセスにもとづく要求性能や容量の検討と承認プロセス
・指定した要求性能や容量の見直し要領
　－見直しを行うべき場合
　－見直しのポイントと実施方法

(3) 実システムに対する性能・容量の管理の仕組みの確立

- 性能・容量の監視要領の確立

日常的に実施すべき負荷状況、性能特性、容量使用状況のチェック要領の確立

・負荷や性能特性や容量の使用状況に対するチェック事項
　－チェック事項ごとのチェックポイントと測定法の明確化
　－チェック事項ごとのチェックサイクルの明確化
・性能や容量の余裕についての評価プロセスの確立

- 性能強化策や付加の制限等の必要性が確認された場合の対処手順

【対応 ISMS コントロール】

8.2.1 容量・能力の計画作成

Ta3.2	性能・容量要件を満足するためのシステム面での実現方式の確立

【主旨】

システムが性能や容量についての要求を満足するようにするためには、対象業務の特性を前提としたシステムの構成ならびに処理の方式を適切に決めなければならない。性能や容量についての要求は業務ごとに指定されるものであるが、システムの構成要素の多くは、多くの業務で共用されるため、システム全体としては、個々の業務からの要求をすべて満足するように設計されなければならない。

このためには、多くの検討要素に対する十分な検討を踏まえた、適切なシステムの方式設計が必要となる。コスト面から、性能容量面でぎりぎりの設計を余儀なくされる場合は、本要求への適切な対応は、特に重要となる。

【対策のポイント】

(1) 個々の業務ごとの性能・容量設計の適切な実施

個々の業務ごとに性能・容量設計として、以下について十分な検討が行われなければならない。

- 使用するネットワークやサーバ等に期待できる性能や容量とその負荷変動に対する特性
- 業務処理の方式の性能特性の把握と、性能面からの処理方式の最適化
- 性能面からの DB 設計の最適化
- 必要に応じたサーバや DB の負荷分散

- 前提とするシステム構成や DB の構成や配置、業務処理の方式等からくる対象システムの処理方式における性能や容量についてのボトルネックの確認

また、これらについては、十分なレビューが行われていなければならない。

(2) システム全体としての性能･容量の十分性の評価の実施

個々の業務ごとの性能･容量設計が適切に行われたとしても、システムリソースを共用する多くのシステムが、同時に稼働した場合、システム全体に大きな負荷がかかり、個々のシステムが期待した性能や容量の確保ができなくなることも考えられる。このようなことがないようにするためには、新しいシステムが追加されるたびに、システム全体としての性能･容量の見直しを行い、システムリソースの強化や、個々のシステムにおける必要な改善を適切に行わなければならない。

(3) 使用するシステムリソース個々の性能や容量特性の正確な把握

システムが必要な性能や容量を確保できるようにするための方式設計には、使用するシステムリソース個々の性能や容量特性が正確に把握できていなければならない。

性能や容量面でぎりぎりの設計が必要な場合は、このことは、特に重要となる。性能や容量設計の前提として、把握すべき事項としては、以下のようなものがある。

- 使用するネットワークの性能特性（容量や使用方法、使用状況に性能変動）
- 使用するサーバやクライアントのハードウェアの性能特性（容量や使用環境、使用方法、使用状況に性能変動）
- 使用する OS 等のシステムのプラットフォームソフト性能特性（容量や使用環境、使用方法、使用状況に性能変動）
- 使用する DBMS の性能特性（容量や使用環境、使用方法、使用状況に性能変動）
- 使用する言語等の開発環境の性能特性（容量や使用環境、使用方法、使用状況に性能変動）

【対応 ISMS コントロール】

8.2.1 容量･能力の計画作成

Ta3.3	システムの性能の確保に関し、必要なシステム構成や機能のシステムへの的確な組込み

【主旨】

システムが求める性能を発揮するためには、システムの作りは性能設計や容量設計に定めるところに沿って的確に実装されていなければならない。

また、性能や容量の管理に必要となるツールやリソースの確保も必要となる。

【対策のポイント】

(1) システム全体としての性能要件を満足するネットワーク構成の構築

ネットワークの性能の確保に関する構成上のチェックポイントとしては、以下があげられる。

- 性能要件を満足するネットワーク構成の構築
- 性能要件を満足する通信路の確保
  - ・専用線
  - ・ISP 接続
  - ・LAN
- 性能設計に沿ったネットワーク上への使用機器の適切な配置

(2) 各機器における必要な性能の確保

システムが要求される性能や容量を確保できているようにするためには、システムを構成する各機器が、それぞれに要求される性能や容量を確保できていなければならない。

このことを実現するためには、以下のようなことが必要となる。

- 必要な性能を提供できる仕様の機器の選択と所要のリソースの確保(メモリ容量等)
- 性能を確保するための使用法の選択
- 必要に応じた性能チューンアップの実施
- インストールにあたっての個々の機器の性能・容量特性の確認

(3) 必要な場合における要求を満足する負荷分散機能の的確な組込み

システムの性能の確保に負荷分散の手法を用いる場合、システムに組み込む負荷分散を実現する機能は、期待通りに機能するよう出なければならない。

このためには、方式の設計とその実装に問題がないかどうかについての徹底した確認が必要となる。

(4) システム全体としての性能テストの実施

システムが所期の性能を発揮できるように構築されているかどうかについての確認を欠かしてはならない。特に、高負荷状態に対する性能テストは簡単でないため、性能テストについては、十分な検討が必要となる。性能テストを適切に行うためには、以下のようなことについての検討が必要となる。

- 性能テストの範囲と確認事項
- 性能テストの実施方法と実施手順
- 必要な負荷の現出方法
- 4性能の測定方法
- 測定結果の評価方法

(5) 性能・容量管理に必要なツールやリソースの確保

性能や容量のオーバーフローが突然に発生しないようにするためには、常日頃からの負荷の変動状況や性能特性、容量の使用状況を正確に把握して、性能や容量がオーバーフローする前に必要な対策が打てるようにしなければならない。負荷状況や性能特性や容量の使用状況の把握のためにはツールの活用も必要となる。可用性が重視されるシステムにおいては、このことは特に重要な問題となる。

性能や容量の管理に使用するツールやリソースとして、検討の対象となるものとしては、以下のようなものがある。

- 外部ネットワークとの接続についての負荷分析・性能特性の把握・分析ツールの整備

- 外部ネットワークについての負荷分析･性能特性の把握･分析ツールの整備
- サーバの負荷分析･性能特性の把握･分析、および容量使用状況の把握ツールの整備
- 関係情報の格納に必要な装置の準備

【対応 ISMS コントロール】

8.2.1 容量･能力の計画作成

Ta3.4	日常からの負荷･性能･容量使用の状況のチェックと問題発生に先立つ対策の実施

【主旨】

性能や容量のオーバーフローが突然に発生しないようにするためには、常日頃からの負荷の変動状況や性能特性、容量の使用状況に注意を払い、問題が発生する前に必要な処置を講じなければならない。これらは、Ta3.1 に示された性能･容量管理の仕組みに沿って行われなければならない。

【対策のポイント】

(1) 関係する業務量の実態把握

- トラフック特性に影響する業務量の変動の把握
- 容量の確保に影響する業務量の変動の把握

(2) 性能特性データの収集と分析の実施

システムの性能や容量に関し、日常からチェックすべき事項としては、以下があげられる。

- 業務(群)ごとの性能特性データの取得と保管
- ネットワーク管理単位(外部とをつなぐネットワーク、LAN の各層等)負荷特性および性能特性
- サーバごとの負荷特性と性能特性データ
- サーバごとの容量使用状況についてのデータの取得と保管

(3) 負荷や性能の特性や容量の使用状況に異常が見られた場合の適切な処置の迅速な実施

負荷や性能の特性や容量の使用状況に異常が見られた場合は、定められた要領に沿って、適切な措置を迅速に行わなければならない。一般的に考えられる措置としては、以下に示すようなものがある。

- 負荷の制限
- リソースの強化等による緊急の性能強化
- 負荷予測の見直し
- 要求性能の見直し

  設定されている性能や容量の要求値は、システム環境や業務の環境に変化があれば、変更しなければならないこともある。目標とすべき要求性能や容量に変化が生じていることを見逃さないようにするためには、周辺環境に大きな変更が生じた場合だけでなく、定期的な見直

しも行わなければならない。

【対応 ISMS コントロール】

8.2.1 容量･能力の計画作成

Ta3.5	性能･容量ﾄﾗﾌﾞﾙ発生時における対処能力の確保

【主旨】

性能･容量管理に努力していても、管理上の不手際や思わぬ負荷変動で、性能や容量にオーバーフローが生じることもある。このような事態の発生時に、問題の解決が迅速にでき、システムが正常に稼働するようにするためには、性能･容量ﾄﾗﾌﾞﾙ発生時に必要となる処置が的確迅速に行えるような備えが、技術面でも管理面でも必要となる。

【対策のポイント】

(1) 性能･容量ﾄﾗﾌﾞﾙの処理についての責任体制の明確化

(2) 性能･容量ﾄﾗﾌﾞﾙ発生時の即応体制の整備

－体制、連絡、報告

(3) 性能･容量ﾄﾗﾌﾞﾙ発生時の緊急処置実施要領の確立

性能･容量ﾄﾗﾌﾞﾙ発生時における緊急的に行う暫定措置についての実施要領として、検討すべき事項としては以下のようなものがある。

- 外部ﾈｯﾄﾜｰｸおよび関係機器のﾄﾗﾌﾞﾙへの緊急処置の実施要領
- 内部ﾈｯﾄﾜｰｸおよび関係機器のﾄﾗﾌﾞﾙへの緊急処置の実施要領
- 主要サーバの性能や容量のオーバーフロー等のﾄﾗﾌﾞﾙへの緊急処置の実施要領

(4) 性能･容量ﾄﾗﾌﾞﾙの本対策の実施要領の確立

発生した性能･容量ﾄﾗﾌﾞﾙに対する本対策は、原因に応じ行われることになるが、これらが円滑に進められるようにするためには、以下に示すような備えも必要となる。

- 外部ﾈｯﾄﾜｰｸの性能ﾄﾗﾌﾞﾙに対する本対策要領の確立
- 内部ﾈｯﾄﾜｰｸの性能ﾄﾗﾌﾞﾙに対する本体策要領の確立
- サーバサーバ(群)ごとの性能ﾄﾗﾌﾞﾙに対する要領の確立
- システム構成やシステムの処理方式に大きな問題が発見された場合の要領の確立

それぞれの場面ごとに、問題点の確認、対策方法の確定、実施の準備、対策の実施、対策実施後の確認の各作業ステップにおいて行うべき作業やその手順等が示されなければならない。

(5) 性能･容量ﾄﾗﾌﾞﾙへの対処にかかわる関係者における対処能力の確保

システム面や管理面でさまざまな準備がなされていても、性能･容量ﾄﾗﾌﾞﾙへの対処にかかわる関係者が対処に必要な能力を確保していなければ、必要な対応の実施は円滑に行われないことが考えられる。このような事態を避けるためには、日頃から以下のような備えが必要となる。

- 関係者への対処要領の徹底
  ･マニュアル等必要文書の配布
  ･実施要領についての教育
  ･習熟度のチェック
- 関係者に対する異常の発見方法についての教育の実施
- 関係者に対する問題分析や対策の実施に必要なスキルの確保
  ･必要な知識･スキルの明確化
  ･関係者への必要な知識･スキルの取得方法の提示
  ･必要に応じた教育の実施
  ･必要な知識やスキルの取得状況の把握と取得推進のための必要な指導の実施
- 緊急処置についての訓練の実施
  この訓練が計画的かつ効率的に行われるようにするには、以下のついての検討が必要となる。
  ･実施計画の確立
  ･実施要領の確立
  ･実施サイクルの確立
  ･訓練結果の評価と問題点の是正に向けた処置の実施

【対応 ISMS コントロール】

8.2.1 容量･能力の計画作成

3.2. 攻撃に対するシステムの堅牢性の確保

3.2.1. 不正アクセス対策

Tb1.1	ネットワークレベルでの不正アクセス対策1： 接続ルールの確立と適切なネットワークの設計

【主旨】

システムへの不正なアクセスの防止の第一歩は、システムの目的に照らしシステムが必要と認めている通信以外の通信を行わないことである。このためには、個々の接続要求に対する諾否がシステム上で適切に行われなければならない。このことが的確に行われるためには、まず、通信の接続要求に対する接続ルールが確立し、このルールに沿った接続制御を実現するネットワークの構成を設計しなければならない。

ここでいう接続ルールとは、エンドーエンド間の接続の可否を決めるためのルールであり、以下のようなもので構成される。

- 端末のグループ化
- 端末グループ間での接続方針
- 接続経路の指定
- 接続条件
- 使用端末の管理についての要求

これらは、対象システムのセキュリティポリシーやネットワーク構成や使用端末のシステム上での役割の組み合わせによって決まる。また、接続ルールとネットワークトポロジーとセグメント分けは表裏一体なものであるため、この接続ルールとネットワークトポロジーの設計とセグメント分けは接続ルールと一体として決めなければならない。

【対策のポイント】

(1) 端末のグループ化

接続ルールは接続する端末(含むサーバ)相互間に指定されるものであるため、接続ルールの検討にあたっては、まず、使用する端末を機器のタイプや使用目的や使用環境に沿ってグルーピングすることが必要となる。端末のグループ化の検討要素としては、表 3-3 に示すようなものがあげられる。

表 3-3 端末のグループ化の検討要素

検討事項	備考
利用目的	・適用業務
グループユーザ	・設置職場 ・ユーザが担当する職務
端末種別	・PC、モバイル機器、専用端末他
端末の OS	・Windows、Linux、MacOS 他
ネットワークの利用環境	・インターネットの閲覧、メールの送受信
使用プロトコル	・HTTP、POP3、IMAP、SMTP、FTP 他

(2) 端末グループ間での接続方針の明確化

端末グループ間での接続方針として明確にすべき事項を、表 3-4 に示す。

表 3-4 端末グループ間の接続方針として指定すべき事項

指定事項	概要
利用アプリケーション／サービス	・HTTP、SMTP、FTP 等
接続場所	・組織内 ・組織外
アクセス制御の方針	・利用プロトコルの制限 ・接続経路の制限

(3) 接続経路の指定の方針

接続経路の指定方針として明確にすべき事項を、表 3-5 に示す

表 3-5 接続経路の指定方針として指定すべき事項

指定事項	備考
物理ネットワークの形態	・通信路の選択（有線・無線） ・接続形態（常時接続・ダイヤルアップ）
使用すべき中継機器	・ファイアウォール、プロキシ、ルータ、スイッチ等
中継機器の使用方針	・利用アプリケーション・サービス毎に、経路によって適切な中継機器を選択 ・接続場所によって、適切な中継機器を選択 ・端末種別によって、適切な中継機器を選択

(4) 接続条件の方針の明確化

接続条件の方針として示すべき事項としては、表 3-6 にあげるようなものがある。

表 3-6 接続条件の方針として指定すべき事項

指定事項	備考
識別と認証	・ネットワーク利用時の認証と認証方式 ・MAC アドレス、IP アドレス等
接続端末の接続条件	・端末種別毎の接続端末セキュリティ設定（パッチ適用、ウイルスパターンなど）

(5) 端末の管理に関する要求

また、不用意に、本来、接続すべきでない端末の接続を許してしまうようなことを防止するためにも、接続する端末に対する適切な管理も必要である。

端末に対する管理事項としては、表 3-7 に示すようなものがあげられる。

表 3-7 端末に対する管理の対象項目

指定事項	備考
固体としての端末種別等	・メーカ、製造番号、機器名称、導入アプリケーションなど
MAC アドレス	・接続端末の MAC アドレス
IP アドレス	・接続端末の IP アドレス（動的な付与の場合は付与ルール）
利用ユーザ	・利用ユーザの定期的な見直し（人事データとの連携） ・パスワード変更、付与ルール ・特権ユーザ

(5) 適切なネットワーク構成の設計

接続ルールに沿った接続制御を実現するためには、接続ルールにマッチしたネットワークを構築しなければならない。ネットワークの設計にあたっての検討事項としては、以下があげられる。

- ネットワーク構成についてお基本方針の確立

ネットワークの設計を的確なものにするためには、まず、ネットワーク構成についての基本方針の確立が必要となる。ネットワーク構成についての基本方針として検討すべき事項を、表 3-8 に示す。

表 3-8 ネットワーク構成の設計方針として検討すべき事項

指定事項	備考
ネットワークトポロジーの選択	･各接続端末や中継機器がどのような形態で接続されるかを、効率性や耐障害性を合わせて十分に検討し、適切なトポロジーを選択する（スター型、バス型、リング型など）
セグメント化	･端末グループ単位を基本とし、利用アプリケーション･サービス別、業務別、利用場所を十分に検討し、適切にセグメントを分割する
中継機器の役割分担	･ルータの役割分担 ･スイッチの役割分担 ･プロキシを使用する場合におけるその役割分担 ･ファイアウォールの役割分担
ネットワークサービス利用	･ネームサービスの利用(DNS, LDAP) ･時刻サービスの利用(NTP)

- ネットワークの構成の設計

ネットワークの設計において検討すべき事項を、表 3-9 に示す。

表 3-9 ネットワーク設計で検討すべき事項

検討項目	備考
ネットワークトポロジーと セグメンテーションの設計	･トポロジーの設計（バス型、スター型、リング型など） ･セグメント化の方針に基づく設計(LAN, WAN)
物理ネットワークの設計	･伝送路の設計（有線、無線） ･接続形態の設計（常時、ダイヤルアップ）
ネットワーク機器の論理配置	･下記機器のネットワーク上での配置場所 －スイッチ、ルータ、ファイアウォール、プロキシ、無線ＬＡＮステーション
冗長化設計	･障害対策 ･負荷分散 ･冗長化制御方式
物理設計	･配線設計 ･機器設置場所

- 使用機器の選択

ネットワークの設計において検討すべき事項を、表 3-10 に示す。

表 3-10　ネットワーク設計で検討すべき事項

検討項目	備考（検討内容等）
ルータ	・経路選択方法（ルーティングテーブル等） ・接続制御方法(IP アドレス等)
スイッチ	・レイヤー層（ネットワーク層、データリンク層等） ・接続制御方法（MAC アドレス等）
ファイアウォール	・接続制御方式（IP アドレス等） ・対応プロトコル（TCP、UDP、ICMP 等） ・制御機能（パケットの破棄、接続遮断等）
プロキシ	・タイプ（フォワードプロキシ、リーバスプロキシ、SOCKS） ・対応プロトコル（HTTP、SMTP 等） ・接続制御方式（URI、メールアドレス等）

（6）接続制御ルールやネットワーク構成についての見直しの実施

接続制御ルールやネットワーク構成も、システムの導入当初は適切なものであっても、システム環境の変化に伴い、その妥当性が失われることもある。このような事態が見逃されたままにならないよう、接続ルールやネットワーク構成については、適宜、見直しを行い、問題があれば変更を行わなければならない。

【対応 ISMS コントロール】

9.4.1　ネットワークサービスの使用についての個別方針
9.4.2 指定された接続経路
9.4.4　ノードの認証
9.4.6 ネットワークの領域分割
9.4.7 ネットワークの接続制御
9.4.8　ネットワーク経路を指定した制御
9.4.9 ネットワークサービスのセキュリティ

Tb1.2　ネットワークレベルでの不正アクセス対策2：個々の端末からの接続要求に対する接続条件の適切な指定

【主旨】

端末からの接続要求に対する接続制御が適切に行われるためには、接続制御を行うネットワーク制御機器のそれぞれが、ネットワーク構成設計が期待した役割を果たすようになっていなければならない。

このためには、ネットワーク制御を行う各機器が、その役割分担に応じ、Tb1.1 で示した接続ルールを的確に反映したものになるように、それぞれの機器に対する細かい接続条件の指定が正確になされていなければならない。重要な指定事項としては、以下のようなものがある。

- セグメントーセグメント間の接続条件
- 外部端末ー内部端末間の接続条件

- セグメント内での端末間（内部端末－内部端末間）の接続条件

【対策のポイント】

（1）セグメント－セグメント間の接続条件

セグメント－セグメント間の接続条件として指定すべき事項を、表 3-11 に示す。

表 3-11　セグメント－セグメント間の接続条件として指定すべき事項

区分	指定事項	備考
中継機器の指定条件	利用プロトコル毎の経路選択	・ルーティングテーブル
	利用プロトコル毎のアクセス制御	・プロトコルごとの制御ルール －プロトコル（HTTP、SMTP,POP3等） －制御する対象（IPアドレス、MACアドレス等
	障害時の代替経路	・選択方法 ・障害対策手順

（2）外部端末－内部端末間の接続条件

外部端末－内部端末間の接続条件として指定すべき事項を、表 3-12 に示す。

表 3-12　外部端末－内部端末間の接続条件として指定すべき事項

区分	指定事項	備考
接続条件	接続の可否	適切な識別、・適用すべき認証方法
	利用プロトコル	HTTP、SMTP、POP、IMAP 等
	接続場所	組織内、組織外
	利用ユーザ	職場とユーザの職務
	端末種別	PC、モバイル機器、専用端末等
	接続形態	常時接続、ダイアルアップ
	伝送路の選択	有線、無線
	アクセス制御	判断基準（IP アドレス、MAC アドレス、メールアドレス、ユーザ ID 等）
中継機器の指定条件	利用プロトコル毎の経路選択	ルーティングテーブル
	利用プロトコル毎のアクセス制御	プロトコルごとの制御ルール －プロトコル（HTTP、SMTP,POP3等） －制御する対象（IP アドレス、MAC アドレス等
	障害時の代替経路	選択方法、障害対策手順

（3）セグメント内にある端末間の接続条件

セグメント内にある端末間の接続条件として指定すべき事項を、表 3-13 に示す。

表 3-13　セグメント内にある端末間の接続条件として指定すべき事項

区分	指定事項	備考
接続条件	接続の可否	適切な識別、・適用すべき認証方法
	利用プロトコル	HTTP、SMTP、POP、IMAP 等
	接続場所	組織内、組織外
	利用ユーザ	職場とユーザの職務
	端末種別	PC、モバイル機器、専用端末等

	接続形態	常時接続、ダイアルアップ
	伝送路の選択	有線、無線
	アクセス制御	判断基準（IP アドレス、MAC アドレス、メールアドレス、ユーザ ID 等）
中継機器の指定条件	利用プロトコル毎の経路選択	ルーティングテーブル
	利用プロトコル毎のアクセス制御	プロトコルごとの制御ルール －プロトコル（HTTP、SMTP,POP3等） －制御する対象（IP アドレス、MAC アドレス等
	障害時の代替経路	選択方法、障害対策手順

（4）接続条件の指定についての見直しの実施

接続条件の指定も設定当初は適切なものであっても、システム環境の変化に伴い、その妥当性が失われることもある。このような事態が見逃されたままにならないよう、接続条件の指定については、適宜、見直しを行い、問題があれば変更を行わなければならない。

【対応 ISMS コントロール】

9.4.1 ネットワークサービスの使用についての個別方針
9.4.2 指定された接続経路
9.4.6 ネットワークの領域分割
9.4.8 ネットワーク経路を指定した制御

Tb1.3 ネットワークレベルでの不正アクセス対策3：接続制御機器の的確な実装

【主旨】

ネットワークレベルでの不正アクセス対策が、期待通りに機能するためには、ネットワーク上に配置する個々の制御機器に対する実装が的確に行われていなければならない。このためには、各接続制御機器に求められている接続制御の行うための実装設計を的確なものとするとともに、その実装についての確認を徹底しなければならない。

また、接続制御機器の実装上の不備が見逃されないようにするためには、実装の妥当性についての定期的な点検も必要となる。

【対策のポイント】

（1）接続制御機器の的確な設計

接続制御機器の設計項目としては、表 3-14、表 3-15、表 3-16、表 3-17 に示すようなものがる。すべての機器においてこれらについての指定が、要求を確実に反映したもにするためには、組織的な検討および徹底したレビューが必要となる。

表 3-14 ルータにおける設計項目

区分	十分な検討が必要な設計項目
機能設定	･ルーティング経路の設定 ･静的／動的ルーティング経路の設定 ･動的ルーティングプロトコルの選択
アクセス制御設定	･ルーティング経路の適切な維持 ･MAC アドレスによる制御 ･送信元／送信先アドレスによるパケットフィルタリング ･内部ネットワークの保護（NAT、 NAPT、ポートフォワーディング等） ･アクセス元の認証 ･認証プロトコルの選択（CHAP、 MS-CHAP、 PAP、 SPAP 等） ･帯域制御
監視設定	･通信ログの収集条件設定（保存方法、保存期間、解析手段） ･SNMP によるトラフィックの監視

表 3-15 ファイアウォールにおける設計項目

区分	十分な検討が必要な設計項目
機能設定	･各ネットワークの IP アドレス範囲設定 ･DMZ の設定
アクセス制御設定	･MAC アドレスによる制御 ･送信元／送信先アドレスによるパケットフィルタリング ･プロトコル別フィルタリング（HTTP：コンテンツフィルタリング等） ･内部ネットワークの保護（NAT、 NAPT、 ポートフォワーディング等） ･ステートフルインスペクションによる不正アクセス防止 ･アクセス元の認証 ･認証プロトコルの選択（CHAP、 MS-CHAP、 PAP、 SPAP 等） ･暗号アルゴリズムの選択（DES、 3DES、 RSA 等） ・ハッシュアルゴリズムの選択（MD4、 MD5、 SHA-1 等）
監視設定	･通信ログの収集条件設定（保存方法、保存期間、解析手段） ･SNMP によるトラフィックの監視

表 3-16 プロキシにおける設計項目

区分	十分な検討が必要な設計項目
機能設定	･使用するプロキシタイプの選定 （フォワードプロキシ･リバースプロキシ･SOCKS） ･プロキシを設置するプロトコルの選定 （http、ftp、telnet、smtp、pop、Gopher etc） ･認証方式の選択（使用するプロトコルに則した認証） ･通信の暗号化（SSL） ･ICP(internet cache protocol)機能（キャッシュ機能）
アクセス制御設定	･アクセス制御（inbound、outbound 双方向、送信元及び送信先） ･フィルタリング （ネットワーク層、IP, Domain, MAC アドレス,アプリケーション層,コンテンツ）
監視設定	･通信ログの収集条件設定（保存方法、保存期間、解析手段） ･SNMP によるトラフィックの監視

表 3-17 スイッチにおける設計項目

区分	十分な検討が必要な設計項目
機能設定	･MAC アドレスの管理 ･VLAN の管理(VLAN については、Tb1.4 を参照)
アクセス制御設定	･MAC アドレスによる制御 ･送信元／送信先アドレスによるパケットフィルタリング
監視設定	･通信ログの収集条件設定（保存方法、保存期間、解析手段） ･SNMP によるトラフィックの監視

⑵ 接続制御機器の実装についての確認の徹底

接続制御機器のすべてについて、すべての実装項目について完全な確認が行われていなければならない。このことを実現するためには、これらの実装の確認についての管理の仕組みの確立も必要となる。

⑶ 接続制御機器の実装についての見直しの実施

各接続制御機器における各種機能の設定等の実装は、機器導入時は適切なものであっても、システム環境の変化に伴い、その妥当性が失われることもある。このような事態が見逃されたままにならないよう、接続制御機器の実装については、適宜、見直しを行い、問題があれば変更を行わなければならない。

【対応 ISMS コントロール】

9.1.1 アクセス制御方針
9.4.2 指定された接続経路
9.4.4 ノードの認証
9.4.7 ネットワークの接続制御
9.4.8 ネットワーク経路を指定した制御

Tb1.4 ネットワークレベルでの不正アクセス対策4：VLAN の適切な使用

【主旨】

VLAN はアクセス制御技術と暗号技術を用いて、公衆回線上に擬似的な専用回線を提供する技術である。したがって、これらの基盤となっている技術の使用に脆弱性がある場合、VLAN を使っていても、セキュリティ上の危険性は公衆回線上の一般通信と同等となる。このため、VLAN の使用においては、VLAN に期待することの実現が損なわれないようにする注意が必要となる。

【対策のポイント】

⑴ VLANの適切な使用法の設定

VLAN を本来の目的に沿った形で適切に使用するためには、その使用法についての十分な検

討が必要となる。VLAN の使用にあたって、十分な検討が必要な事項を、表 3-18 に示す。

表 3-18　VLAN の使用にあたって十分な検討が求められる事項

検討項目	検討内容等
VLAN 方式の選択	・選択対象の VLAN －ポートベース VLAN、MAC アドレスベース VLAN、・ポリシーベース VLAN サブネットベース VLAN、プロトコルベース VLAN、 認証 VLAN（RADIUSLDAP）
アクセス制御についての設定	・ポートベース VLAN の場合 －接続ポートによる物理的なアクセス制御 －タグ VLAN －未使用ポートの保全(enable／disable ポート機能) －フィルタリングルール等ポリシーの設定 ・MAC アドレスベース VLAN の場合 －MAC アドレスによる制御 －DHCP サービスとの併用 －ポート制御 ・ポリシーベース VLAN の場合 －サブネットによるアクセス制御 －IP マルチホーミング －プロトコルによるアクセス制御(IP、IPv6、IPX、AppleTalk etc) －DHCP サービス －パケットフィルタリング ・認証 VLAN の場合 －サブネットによるアクセス制御 －IP マルチホーミング －プロトコルによるアクセス制御(IP、IPv6、IPX、AppleTalk etc) －DHCP サービス －パケットフィルタリング
暗号化についての設定	・暗号強度の選択
監視についての設定	・通信ログの収集条件設定（保存方法、保存期間、解析手段） ・SNMP によるトラフィックの監視

(2) VLAN の実装についての確認の徹底

すべての実装項目について完全な確認が行われていなければならない。このことを実現するためには、これらの実装の確認についての管理の仕組みの確立も必要となる。

(3) VLAN の実装についての見直しの実施

VLAN における各種機能の設定等の実装は、VLAN 導入時は適切なものであっても、システム環境の変化に伴い、その妥当性が失われることもある。このような事態が見逃されたままにならないよう、VLAN　の実装についても、適宜、見直しを行い、問題があれば変更を行わなければならない。

【対応 ISMS コントロール】

9.1.1　アクセス制御方針
9.4.2　指定された接続経路
9.4.4　ノードの認証
9.4.7　ネットワークの接続制御

Tb1.5	ネットワークレベルでの不正アクセス対策5： 無線 LAN の適切な使用

【主旨】

無線 LAN は、通信路に有線を用いるのに比べ、配線敷設のコストや手間の削減や、メンテナンスの容易性から、使用上の便が高く、最近、急激に普及してきたが、セキュリティ面からは相当に危うい技術と見なければならない。設計、実装、運用のいずれかにでも脆弱な点があれば危険性の排除は困難となる。このため、無線 LAN の使用にあたっては、十分な注意が必要となる。

【対策のポイント】

(1) 無線 LAN の使用制限の検討

無線 LAN は、有線を用いる通信に対し脆弱性が高いため、特に必要がない限り、使用の制限がなされるべきである。無線 LAN の使用制限として検討すべき事項としては、以下があげられる。

- 無線 LAN が使用できる端末の制限（職場あるいは職務等による制限他）
- 無線 LAN が使用できる業務（無線 LAN が使用できない通信等の指定を含む）

(2) 無線 LAN ステーションの適切な設計

無線 LAN を本来の目的に沿った形で適切に使用するためには、無線 LAN ステーションの設計についての十分な検討が必要となる。無線 LAN ステーションの設計にあたって、十分な検討が必要な事項を、表 3-19 に示す。

表 3-19 無線 LAN ステーションの設計にあたって十分な検討が求められる事項

検討項目	検討内容等
機能設定	・無線規格の選択（ IEEE802.11(b,a,g,i) ） （通信速度、電波到達距離、汎用性／互換性、セキュリティ機能の検討） ・暗号化の確保（鍵の取り扱い方法、暗号化方式の選択） ・識別IDの隠蔽（ANYプローブ応答禁止、SSIDの隠蔽） ・認証機能の利用（EAP－TLS，EAP－TTLS） ・DHCP サービス利用時の範囲指定
アクセス制御設定	・フィルタリング（MACアドレスフィルタリング、ANY接続禁止） ・IP マルチホーミング ・プロトコル制御（IP、IPv6、IPX、AppleTalk etc） ・パケットフィルタリング
監視設定	・通信ログの収集条件設定（保存方法、保存期間、解析手段） ・SNMP によるトラフィックの監視

(3) 無線 LAN ステーションの実装についての確認の徹底

すべての実装項目について完全な確認が行われていなければならない。このことを実現するためには、これらの実装の確認についての管理の仕組みの確立も必要となる。

(4) 無線 LAN の実装や使用状況についての見直しの実施

無線 LAN における各種機能の設定等の実装は、無線 LAN 導入時は適切なものであっても、システム環境の変化に伴い、その妥当性が失われることもある。このような事態が見逃されたままにならないよう、無線 LAN の実装についても、適宜、見直しを行い、問題があれば変更を行わなければならない。

また、無線LANがルール通り使われているかどうかのチェックを定期的に行うことも必要である。

【対応 ISMS コントロール】

9.1.1 アクセス制御方針
9.4.2 指定された接続経路
9.4.4 ノードの認証
9.4.7 ネットワークの接続制御
9.4.8 ネットワーク経路を指定した制御

Tb1.6	システムレベルでの不正アクセス対策1： 一般ユーザアカウントに対する適切な管理の実施

【主旨】

システムレベルでの不正アクセスの一つである一般ユーザに対するシステムのアクセス制御が適切に行われるためには、まず、一般ユーザに対するアクセス制御ルールを確立するとともに、このルールにもとづく一般ユーザに対するアカウントの管理が適切に行われなければならない。

本要求の一部は、ユーザ管理についての要求 Ba4.1、Ba4.2 と重なりところがあるが、ここでは、組織の関係者で、システムに一般ユーザアカウントが登録される者を対象としている。

【対策のポイント】

(1) アクセス制御ルールの確立

一般ユーザからのシステムへのアクセス要求に対するアクセス制御ルールとして検討すべき事項としては、以下があげられる。

- アクセスを許可するサービス
- 必要な場合サービスへの接続制限
- 認証方式の選択と認証にあたっての要求
- 必要に応じたセッション管理に関する要求
- アクセスを許可するユーザおよび付与する権限
  －対話的ログインの可否、使用可能サービス、リソースへのアクセス権等
- ユーザグループ編成方針
- アカウント付与方針

(2) 一般ユーザアカウントの管理の仕組みの確立

さまざまな活動で構成される一般ユーザアカウントの管理が適切に行なわれるようにするために

は、一般ユーザアカウントの管理の仕組みの確立も必要となる。一般ユーザアカウントの管理の仕組みとして検討すべき事項としては、下記があげられる。

- 一般ユーザに対するアカウントの付与要領
  ・アカウントを付与するユーザの資格の確認手順
  ・アカウント付与および抹消の手続き
  ・付与する権限の指定、変更、抹消の手続き
- 一般ユーザアカウントの管理要領
  ・一般ユーザアカウントおよび権限リストの作成と維持管理方法
  ・一般ユーザアカウントの定期的なチェック要領
    －チェックのポイント
    －チェックを行うべきタイミング
- パスワードの運用管理要領
  ・パスワードの設定ルール
  ・パスワードの管理要領
    －管理すべき事項
    －管理の方法
  ・パスワードの付与、変更、抹消の手続き
- 認証デバイスの管理要領

(3) ルールに沿った一般ユーザアカウントの管理実施

- ルールに沿ったユーザの資格確認の実施
- ルールに沿った一般ユーザアカウントと権限の付与
- 必要が生じた場合の変更、抹消の適切な実施
- ルールに沿った一般ユーザアカウントリストおよび権限リストの作成とその妥当性の維持
- ルールに沿った使用するパスワードの管理の実施
- アカウント付与ユーザにおける ID/パスワードの適切な取扱いの指導と管理の実施

【対応 ISMS コントロール】

9.1.1 アクセス制御方針
9.2.1 利用者の登録
9.2.3 利用者のパスワードの管理
9.2.4 利用者のアクセス権の見直し
9.5.4 パスワード管理システム

Tb1.7	システムレベルでの不正アクセス対策2： 一般ユーザに対する適切なアクセス制御の実施

【主旨】

一般ユーザからのアクセス要求に対し、システムレベルでのアクセス制御が、それぞれのアカウントに指定された通りに機能するようにするためには、システムへのアカウントの登録や、必要なアクセス制御機能の的確な組込みが必要となる。

【対策のポイント】

(1) 一般ユーザアカウントのシステムへの的確な登録

一般ユーザアカウントのシステムへの登録に不備がないようにするためには、この登録の実施要領を定め、定められた手順に沿って組織的な管理の下で、一般ユーザアカウントのシステムへの登録が行われるようにしなければならない。登録されたアカウントの検証は十分に行われなければならない。

(2) 不要なアカウントのシステムからの除去

システムに管理されていないアカウントが存在しないようしなければならない。このためには、以下の励行が必要となる。

- 不要なデフォルトアカウントの削除または無効化
- 不要となったアカウントの速やかな削除

(3) 適切な識別と認証の適用

適切な識別と認証を行うためには、以下が必要となる。

- セキュリティ要求レベルに応じた認証方式の採用
- 認証方式に応じた適切な認証強度の保証
  - パスワード認証の場合、強度の高いパスワードの強制
- 認証破りの試みに対する防護措置
  - 認証試行回数の制限
  - 一定回数の認証失敗によるアカウントロックアウトの設定
- パスワード盗聴への対策
  - 平文でパスワードを流すプロトコル/サービスの使用禁止
  - 弱いチャレンジ・レスポンス認証を行うプロトコル/サービス（チャレンジとレズポンスを盗聴することによりオフラインの辞書攻撃・総当たり攻撃が可能なもの）の使用禁止
- 認証ログの取得

(4) 必要なアクセス制御機能のシステムへの組込み

システムレベルでのアクセス制御として、必要に応じ以下のような機能をシステムに組込む。これらが期待通り機能するようになっていることの確認を怠ってはならない。

- OS レベルでのサービス接続制限
  - 接続元アドレス等によるサービスへの接続の制御（TCP Wrapper、PFW 等）
- 端末（クライアント）接続の管理

- 一定時間アクセスの無い場合のセッション切断
- 必要に応じ接続時間の制限

- ユーザ権限の適切な設定
  - 特定サービスのみを利用するユーザの対話的ログインの禁止
  - 適切なユーザグループまたはロールの設定
  - デフォルトのパーミッション（UNIX の場合 umask）の適切な設定
- システムユーティリティの識別と利用制限
  - 起動ユーザの権限を超えて動作するプログラム（UNIX の suid/sgid プログラム等）の把握
  - 不要なシステムユーティリティの削除
  - システムユーティリティを使用できるユーザの制限

【対応 ISMS コントロール】

9.1.1 アクセス制御方針
9.5.1 自動の端末識別
9.5.2 端末のログオン手順
9.5.3 利用者の識別および認証
9.5.5 システムのユティリティの利用
9.5.7 端末のタイムアウト機能
9.5.8 接続時間の制限

Tb1.8	システムレベルでの不正アクセス対策3： 特権ユーザアカウントに対する適切な管理の実施

【主旨】

システム特権の不適切な使用は、不正アクセスの原因となる。システムに必要な特権を識別し、最小権限の原則に従って特権を付与するとともに、特権アカウントの管理を厳格に行うことが必要である。また、特権アカウントを奪取しての侵入を防ぐために、特権アカウントによるアクセスに適切な制限を加えることも必要となる。これらが適切に行われるためには、まず、特権の使用法についての方針を確立するとともに、特権ユーザに対するアクセス制御ルールを確立し、このルールにもとづく特権ユーザアカウントの管理が適切に行われなければならない。

【対策のポイント】

(1) 特権の使用方針の確立

特権の使用方針についての主な検討事項としては、以下のようなものあがる。

- システム管理上必要とされる特権の識別と最小限の特権付与
- 適切な権限分割方針の決定とグループ/ロールの編成
  ・OS 機能が許すなら、必要に応じ権限の分割を実施

・UNIX の場合、su root 可能なグループを制限

(2) アクセス制御ルールの確立

特権ユーザからのシステムへのアクセス要求に対するアクセス制御ルールとして検討すべき事項としては、以下があげられる。

- 特権アカウントの使用の制限
  ・特権アカウントdのリモートログインの禁止等
- 認証方式の選択と認証にあたっての要求
- 必要に応じたセッション管理に関する要求
- 特権アカウントの付与方針
- 特権使用ログの取得についての要求

(2) 特権ユーザアカウントの管理の仕組みの確立

さまざまな活動で構成される特権ユーザアカウントの管理が適切に行なわれるようにするためには、特権ユーザアカウントの管理の仕組みの確立も必要となる。特権ユーザアカウントの管理の仕組みとして検討すべき事項としては、下記があげられる。

- 特権ユーザアカウントの付与要領
  ・アカウントを付与するユーザの資格の確認手順
  ・アカウント付与および抹消の手続き
  ・付与する権限の指定、変更、抹消の手続き
- 特権ユーザアカウントの管理要領
  ・特権ユーザアカウントおよび権限リストの作成と維持管理方法
  ・特権ユーザアカウントの定期的なチェック要領
    ―チェックのポイント
    ―チェックを行うべきタイミング
- パスワードの運用管理要領
  ・パスワードの設定ルール
  ・パスワードの管理要領
    ―管理すべき事項
    ―管理の方法
  ・パスワードの付与、変更、抹消の手続き
- 認証デバイスの管理要領

(3) ルールに沿った一般ユーザアカウントの管理実施

- ルールに沿ったユーザの資格確認の実施
- ルールに沿った特権ユーザアカウントと権限の付与
- 必要が生じた場合の変更、抹消の適切な実施
- ルールに沿った特権ユーザアカウントリストおよび権限リストの作成とその妥当性の維持
- ルールに沿った使用するパスワードの管理の実施
- 特権アカウントを保有する者における ID/パスワードの適切な取扱いの指導と管理の実施

【対応 ISMS コントロール】

9.1.1 アクセス制御方針

9.2.2 特権管理

Tb1.9	システムレベルでの不正アクセス対策4： 特権ユーザに対する適切なアクセス制御の実施

【主旨】

特権ユーザからのアクセス要求に対するアクセス制御が、それぞれのアカウントに指定された通りに機能するようにするためには、システムへの特権アカウントの登録や、必要なアクセス制御機能の的確な組込みが必要となる。

多くの場合、システムへの攻撃者の最終的な標的となるのは特権アカウントである。特権アカウントに対して一般ユーザより強力な認証を適用して保護するとともに、万一、特権アカウントを奪取されても他の管理策による防衛が可能なよう、特権アカウントによる直接のログインを禁止する設定とするなど、特権アカウント固有のアクセス制限を適用する必要がある。

【対策のポイント】

(1) 特権ユーザアカウントのシステムへの的確な登録

特権ユーザアカウントのシステムへの登録に不備がないようにするためには、この登録の実施要領を定め、定められた手順に沿って組織的な管理の下で、特権ユーザアカウントのシステムへの登録が行われるようにしなければならない。登録された特権ユーザアカウントについての情報の的確性についての確認は十分に行われなければならない。

(2) 適切な識別と認証の採用

一般ユーザアカウントより厳格な認証方式の使用または認証強度の保証が必要となる。このため、特権ユーザに対しては、以下が求められる。

- パスワード認証の場合、より強度の高いパスワードの使用（ツールによる生成等）
- 一般ユーザより短期間でのパスワード変更

(3) 特権アカウントに対するアクセス制御の実施

特権アカウントでのログインについては、以下のようなを制限も必要となる。

- 特権アカウントで直接ログインせず、su、runas 等を使用
- ネットワークログインの禁止、ログインする端末の制限等
- 使用するサービス/プロトコルの制限

(4) システムへの特権の使用を適切なものにするための機能の適切な実装

特権の使用を適切なものにするために、システムに組込むべき機能としては、以下のようなものがある。

- 特権管理方針に基づく権限分割の実装

- 特権使用制限の確実な実装
  - ･UNIX の場合、一般ユーザに対話的ログインを許可しているシステムであれば、su コマンドを実行できるユーザの制限
  - ･UNIX の場合、sudo コマンドの利用等により、必要以上の運用担当者に root 権限を渡さない。
- 特権アカウントのログインログの取得
- 特権使用ログ（su ログ等）の取得

【対応 ISMS コントロール】

9.1.1 アクセス制御方針
9.5.2 端末のログオン手順
9.5.3 利用者の識別および認証
9.5.5 システムのユティリティの利用

Tb1.10	システムレベルでの不正アクセス対策5： 必要に応じたセキュアな OS の使用

【主旨】

高度のセキュリティが要求されるシステムでは、従来の OS のアクセス制御機能ではその要件を満たせず、トラステッド OS あるいはセキュア OS が必要となることがある。これらの OS を利用する場合には、その特徴であるシステムによるアクセス制御の強制や特権の分割の機能を最大限に発揮させる設定をおこなうことが重要である。

【対策のポイント】

（1）トラステッド/セキュア OS の使用要件および使用方針の明確化

セキュアな OS を使いこなし導入の目的を達成するためには、これらセキュアな OS の使用方針や使用方法についての十分な件等が必要となる。

（2）設定の確実な実装

セキュアな OS は、一般の OS に比べ、設定事項が多い。せっかく導入したセ急な OS が本来の機能を発揮するためには、これらの設定を的確に行わなければならない。以下については、特に、十分な検討が必要とされる。

- ファイル･リソースへの適切な機密ラベルの設定
- アプリケーションごとの適切なコンパートメントの設定
- 管理者権限の適切な分割

  とりわけ、セキュリティ管理者の権限とシステム運用管理者の確実な分離が重要となる。

また、これらの実装については、十分な確認が行われていなければならない。

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない。

Tb1.11	アプリケーションレベルレベルでの不正アクセス対策1： アプリケーションでのアクセス管理の実施基準の確立と、個々のアプリケーケーションに対するアクセス管理要件の適切な指定

【主旨】

サービスの不正な使用やアプリケーションソフトの管理下にある業務情報への不正なアクセスを防止するための最後の砦である、アプリケーションレベルでのアクセス管理が適切に行われるためには、まず、個々のアプリケーションが実装すべきアクセス制御やアクセス監視についての要求を示すアクセス管理要件が、当該アプリケーションの機能や、アクセスする情報の保護要件等に照らして適切に指定されなければならない。

このことを実現するためには、アプリケーションに対するアクセス管理要件の指定を管理する仕組みの確立も必要となる。また、多くのアプリケーションに定義するアクセス管理要件がシステム全体としてバランスのとれた適切なものとなるため、システムに対してアプリケーションレベルのアクセス管理の実施基準が定められている必要がある。そして、個々のアプリケーションに対するアクセス管理要件の指定は、この管理実施基準に沿って行われることが望ましい。

【対策のポイント】

(1) アプリケーションにおけるアクセス管理実施基準の確立

アプリケーションレベルでのアクセス管理にも、その厳格さによっていくつかのレベルがある。このレベルごとに、アクセス管理についての以下のような諸要件の適用基準の標準を決めておくことにより、システム全体として必要なアプリケーションレベルでのアクセス管理要件の指定を適切に行うことが容易となる。

アプリケーションに定義する管理要件がシステム全体としてバランスよくするためには、アプリケーションレベルでのアクセス管理実施基準として検討にすべき事項としては、表 3-20 に示すようなものがあげられる。

表 3-20 アプリケーションにおけるアクセス管理基準として検討すべき事項

項番	基準事項	説明
1	アクセス管理レベル適用基準	当該レベルを適用すべきアプリケーションの特性 （このレベルのアクセス管理は、どのようなアプリケーションに適用されるのかを意識して作られたかを示す）
2	アクセス制御のきめの細かさ	適用すべきアクセス制御のきめの細かさを示すもので、大きくは、 ・アプリケーション単位 ・要求機能単位 がある。管理レベルについての要求が高い大きなアプリケーションでは、一般に、要求機能単位でのアクセス制御が望ましい
3	アクセス要求者の認証方式	当該レベルが採用すべきアクセス要求者の識別と認証に用いる手段 管理レベルに着いての要求が高いほど、信頼度の高い技術の採用を要求する

4	アクセス権限の管理方法	当該レベルに要求されるアクセス制御のベースとなるアクセス権に管理についての要求を示す。 ･アクセス権付与者の確認の方式 ･アクセス権付与者に付与するアクセス権の管理の方式
5	不審なアクセスに対する処置	アクセス制御プロセスで不審なアクセス要求が検知された場合の報告ならびに対処の基準
6	アクセスログの取得範囲	アクセスログを取得するイベント アクセスログとして取得する情報 アクセスログの保管ルール
7	アクセスログの解析方法	アクセスログの解析ポイント アクセスログの解析タイミング 不審なアクセスの報告ならびに対処の基準

(2) 個々のアプリケーションに対するアクセス管理要件の指定を管理する仕組みの確立

個々のアプリケーションに対するアクセス管理要件の指定が、組織的に管理されたものにするためには、以下のようなことが必要となる。

- アプリケーション開発プロセスの中へのアクセス管理要件の検討の組込み
- 個々のアプリケーションに対するアクセス管理要件の指定のレビュー要領
- 個々のアプリケーションに指定しているアクセス管理要件の管理要領
- 個々のアプリケーションに指定しているアクセス管理要件の見直し要領

(2) 個々のアプリケーションに対するアクセス管理要件の指定

個々のアプリケーションに対してアクセス管理基準に沿ってアクセス管理要件を指定する。個々のアプリケーションに対してアクセス管理要件として指定すべき事項としては、表 3-21 に示すようなものがあげられる。

表 3-21 個々のアプリケーションに対するアクセス管理要件として指定すべき事項

NO	指定項目	説明
1	必要とするアクセス制御の詳細	アクセス制御の実施の有無をはじめ、アクセス制御を行う対象範囲を指定 ･機能単位 ･サービス単位
2	アクセス要求者の認証方式	当該レベルが採用すべきアクセス要求者の識別と認証に用いる手段
3	アクセス権限の管理方法	･アクセス権の付与対象者の範囲 ･アクセス権付与者に付与するアクセス権の範囲 ･アクセス権限付与対象者の管理の方法
4	不審なアクセスに対する処置	アクセス制御プロセスで不審なアクセス要求が検知された場合の報告ならびに対処の基準
5	アクセスログの取得範囲	･アクセスログを取得するイベント ･アクセスログとして取得する情報 ･アクセスログの保管ルール
6	アクセスログの解析方法	･アクセスログの解析ポイント ･アクセスログの解析タイミング ･不審なアクセスの報告ならびに対処の基準

(3) 必要に応じた個々のアプリケーションに指定しているアクセス管理要件の見直し

アプリケーションに対するアクセス管理要件の指定の不備や、セキュリティ環境の変化からその適切性が減じられているのを見過ごさないためには、適宜、これらの指定についての見直しと、必要な修正を行わなければならない。

【対応 ISMS コントロール】

9.1.1 アクセス制御方針

9.5.3 利用者の識別及び認証

Tb1.12	システムレベルでの不正アクセス対策2： 個々のアプリケーションへの必要なアクセス管理機能の組込み

【主旨】

アプリケーションが定められたアクセス制御要件を満たすため、アプリケーションに必要な機能を的確に実装しなければならない。実装の対象としては以下がある。

- アクセス制御機能
- アクセス監視機能
- アクセス管理テーブル

【対策のポイント】

(1) 各アプリケーションへのアクセス管理に必要な機能の的確な実装

それぞれのアプリケーションには、指定されたアクセス管理要件に応えるために必要な機能が的確に組込まれていなければならない。このためには、アプリケーションの開発において、この点について設計上の漏れがあったり、テストに徹底を欠くようなことがあってはならない。

このためには、アプリケーションの開発プロセスでの、アクセス管理の実装を確実にするためのレビューの実施やテストの徹底等を管理する仕組みも必要となる。

各アプリケーションに組込みを検討すべき機能としては、以下のようなものがある。

- アクセス制御機能
  - ・ユーザの識別および認証のための機能
    - ―この機能は認証のレベルに応じて必要な技術を選択しなければならない
  - ・不正あるいは不審なアクセスを検知したときの処理
  - ・アクセス制御機能が動作しなくなったときの処理
- アクセス監視機能
  - ・アプリケーションの動作状況の監視機能
  - ・アプリケーションへのアクセス状況の監視機能
  - ・ログ収集・蓄積・外部メディアへの退避の機能
  - ・ログが取得できなくなっとき（蓄積したログが一杯、ログ取得機能の停止、高負荷によるログ取得失敗、マシン障害など）の処理の組み込み
- パスワードやアクセス管理テーブル等のアクセス制御が用いる情報の管理機能
  - ・アクセス管理情報へアクセス制御機能
  - ・アクセス管理情報の登録、削除、編集、閲覧機能
  - ・アクセス管理情報へのアクセスログの取得機能

・アクセス管理情報へのアクセスログへのアクセス制御機能

⑵ 使用ツールの整備

ユーザの識別に生態認証を用いるような場合のように、特別なツールを使用する場合は、以下のような配慮が不可欠となる。

- ツールの的確な実装と使用環境の整備
- 故障等でツールの使用が出来なくなったときの対処方法の確立

⑶ アクセス管理情報の正確な登録

ユーザ ID やパスワード等のアクセス者の認証に用いる情報や、権限に関する情報のシステムへの登録に不備があれば、アクセス制御機能は信頼のおけないものになる。システムへのアクセス管理情報の登録を常に正確なものとして維持するためには、以下が必要となる。

- システムへのこれらの情報の登録を管理する仕組みの確立
- この仕組みの沿った登録時の厳格なチェックの実施
- この仕組みに沿った定期的な妥当性チェックの実施

【対応 ISMS コントロール】

9.5.3 利用者の識別及び認証

3.2.2. セキュリティホール対策

Tb2.1	セキュリティホール対策についての管理スキームの確立

【主旨】

セキュリティホールにつながる脆弱性の情報は、毎日、複数のものが発表されている。対策実施の間隔が長いとその間、セキュルティホールは累積し、システムの堅牢性を保つ上で好ましくないので、関係するセキュリティホールについては迅速な対策が必要となる。しかし、OS 等のシステムのプラットフォームへのセキュリティパッチの実施は、システムによっては、安易に実施できないものもあるため、祖温容なシステムにおいては、実施のタイミングを適切に図らなければならない。このため、セキュリティホール対策においては、対策の必要性の把握、実施についての判断、実施にあたってのシステムの安全の確保、対策を保留している案件等組織的な管理が必要なことが多い。

このため、セキュリティホール対策を適切に行うためには、まず、セキュリティホール対策についてお管理のスキームの確立が必要となる。

セキュリティホール対策を適切に行うための管理のスキームとして検討すべき事項としては、以下があげられる。

- セキュリティホール対策実施基準の確立
- セキュリティホール対策についての責任体制の確立

- 脆弱性情報の入手･分析要領の確立
- セキュリティホール対策の実施要領の確立
- セキュリティホール対策の実施状況についての管理要領の確立
- 可能な範囲でのセキュリティホール対策の自動化の推進

【対策のポイント】

(1) セキュリティホール対策実施基準の確立

セキュリティパッチはその重要性や対策の対象システムの特性によって、対策の要否や緊急度が異なる。このため、セキュリティホール対策の実施においては、脆弱性情報に対しどのように対応するかを適切に判断することが重要となる。この判断が適切に行われるようにするためには、どのような脆弱性については、どのシステムに対し、どのタイミングで対策を実施するかについての判断基準と、対策の実施にあたっての留意事項等を示したセキュリティホール対策実施基準を確立しておくことが必要となる。

セキュリティホール対策実施基準として、示すべき事項としては以下があげられる。

- セキュリティホール対策の実施管理単位の指定
- 脆弱性情報に対する下記についての判断基準

･対策の要否

･対策対象システムの範囲

･対策の緊急性

･セキュリティパッチの実施までの暫定措置の実施の要否とその緊急性

(2) セキュリティホール対策についての責任体制の確立

セキュリティホール対策についての責任体制として検討すべき事項としては、以下があげられる。

- セキュリティホール対策についての責任者の明確化とそのタスク
- 脆弱性情報の入手･分析からセキュリティホール対策の計画と実施、対策の実施状況の管理の担当チーム(者)とそのタスク
- システム管理者やクライアント PC の利用者のタスク
- 外部の専門家の活用

また、責任者からクライアント PC の利用者に至るまでの関係者のすべてに、セキュリティホール対策にかかる自己の責任を周知させることも欠かせない。

(3) 脆弱性情報の入手･分析要領の確立

セキュリティホール対策の適切な実施には、必要な脆弱性情報の漏れのない入手と、入手した脆弱性情報に対する適切な分析･評価が欠かせない。これらが適切に行われるためには、脆弱性情報の入手･分析要領の確立も必要となる。脆弱性情報の入手･分析要領で示すべきこととしては、以下があげられる。

- 脆弱性情報の入手方法

･脆弱性情報の入手先

･入手手段

・入手脆弱性情報の取扱い（情報のファイリング、台帳の作成、関係者への配布等）

- 脆弱性情報の分析・評価・報告手順
- 必要な対策の検討手順

（4）セキュリティホール対策の実施要領の確立

必要と判断されたセキュリティパッチや暫定措置の実施を、必要なタイミングで確実かつ安全に行うためには、計画から実施後の確認に至るまでの手順を定めたセキュリティホール対策の実施要領の確立も必要となる。セキュリティホール対策の実施要領で示すべき事項としては、以下があげられる。

- セキュリティホール対策実施計画書の記載事項、記載様式

セキュリティホール対策の実施計画書に記載すべき事項としては、以下のようなものがある。

・対策対象システムと対策対象システムごとの実施する対策内容
・実施時期
・準備から実施、事後処理までの作業の流れ（間易者への連絡や調整他）
・必要な事前準備（安全性他についての事前チェック、業務運用との調整、バックアップの取得等の安全措置他）の詳細
・実施後に行うべき確認事項と確認の方法
・システムの普及方法

- セキュリティホール対策実施計画の審査承認手順（含む実施計画のチェックポイント）
- 準備から実施、事後処理までの対策実施にかかる一連の作業の流れに対する管理の方法

（5）セキュリティホール対策の実施状況についての管理要領の確立

セキュリティホール対策は実施を保留にするものがあったり、対策の対象システムが多かったりするため、必要な対策が漏れなく行われているかどうかの確認や、実施保留としてシステムの脆弱性として残されているものは何かを正確に把握しておくことも必要となる。これらの脆弱性情報に対する対応状況の把握が確実に行われるようにするためには、脆弱性情報に対する対応状況についての管理要領の確立も必要となる。

（6）可能な範囲でのセキュリティホール対策の自動化の推進

セキュリティホール対策で自動化できるところは、できるだけ自動化することが望ましいが、自動化してはならないところもある。このため、セキュリティホール対策の自動化については、十分な検討と、自動化の対象とした領域においては、この機能が実装され、確実に使用できる状況にある ことについての確認が必要となる。k

（6）セキュリティホール対策についての管理のスキームについての見直しの実施

セキュリティホール対策についての管理のスキームの妥当性を維持するためには、その妥当性についての見直しを、定期的な実施も含め、適宜、行わなければならない。

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない。

Tb2.2	脆弱性情報の入手から対策実施への展開の適切な実施

【主旨】

セキュリティホール対策の適切な実施には、まず、脆弱性情報の入手、その分析･評価、実施が必要な対策について適切な実施計画の作成が適切に行われなければならない。これらは、Tb2.1 に示したセキュリティホール対策の管理のスキームに沿って、組織的な管理の下で行われなければならない。

また、脆弱性情報の入手は、信頼できるソースからの情報の入手が不可欠である。情報の入手はベンダーのみの情報に頼らず、他の情報源からも入手することが望まれる。

【対策のポイント】

(1) ルールに沿った脆弱性情報の入手

日々、報告されている脆弱性情報の入手と分析･評価の速やかな実施に漏れがないようにしなければならない。これらを確実なものにするためには、脆弱性情報の入手が適切に行われているかどうかについてのチェックを行うことも必要となる。チェックのポイントとしては以下のようなものがある。

- 脆弱性情報の漏れのない入手方法 (定められた入手先からの情報の確実な入手)
- 入手情報に対し定められてい処置の確実な実施
  －情報のファイリング、台帳の作成、関係者への配布等

(2) 入手した脆弱性情報に対する分析と評価の実施

日々、報告されている脆弱性情報の入手と分析･評価の速やかな実施に漏れがないようにしなければならない。これらを確実なものにするためには、脆弱性情報の入手やその分析評価の実体についてのチェックを行うことも必要となる。チェックのポイントとしては以下のようなものがある。

- 入手した脆弱性のすべてに対する分析･評価の実施 (分析･評価が放置されているものはないか)
- 危険性の評価や対策要否や必要な実施時期の判断の妥当性

(3) 対策が必要とされたものに対する対策実施計画の作成

対策の実施が必要と判断された脆弱性に対する対策実施計画を作成する。今計画は定められて容量によって審査商人を受けなければならない。計画で明確にすべき事項については Tb1.1 参照。

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない。

Tb2.3	セキュリティホール対策の迅速かつ安全な実施

【主旨】

セキュリティホール対策は、自動化されている場合を除き、作成された実施計画に沿って手順を踏んで、実施されなければならない。実施に遅れがでないようにすること、事前の準備を入念に行い、実施が事故に結びつかないようにすること、ならびに事後処理を適切に行うことが求められる。

【対策のポイント】

(1) 実施計画にもとづく事前準備の実施

セキュリティホールパッチの実施に先立ち、実施計画に示された事前準備を確実に行う。この事前準備での留意事項としては、以下があげられる。

- セキュリティパッチの信頼性の確保
  パッチが信頼できるソースから入手できており、必要に応じてパッチ適用後にシステムに対する影響がないことを事前に確認されていること。
- 必要に応じた事前テストの実施
- 実施上の事故に備えたシステムのバックアップの確保
- 実施を担当する者への実施の手順書やパッチの配布

(2) 実施計画にもとづくセキュリティパッチの実施

事前準備で実施に環境が整ったのを確認したら、実施計画に沿ってセキュリティパッチの実施を行う。セキュリティパッチの実施での留意事項としては、以下があげられる。

- 指定された手順に沿った実施
- パッチ終了後のシステムの動作確認

(3) 実施計画にもとづく事後処理の実施

セキュリティホールパッチが完了したら、実施記録の作成等の実施計画に示された事後処理を確実に行わなければならない。

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない。

Tb2.4	セキュリティホール対策の実施状況についての適切な管理の実施

【主旨】

セキュリティホール対策は実施を保留にするものがあったり、対策の対象システムが多かったりするため、必要な対策が漏れなく行われているかどうかの確認や、実施保留としてシステムの脆弱性として残されているものにはどのようなものがあり、システムはどのような脆弱点を抱えているかを

を正確に把握しておくことも必要となる。

【対策のポイント】

(1) セキュリティホール対策の実施状況の把握

セキュリティホール対策の実施状況について把握しておくべき事項としては以下があげられる。これらは、Tb2.1 に示したセキュリティホール対策の実施状況についての管理要領に沿って組織的に管理されなければならない。

- すべてのシステムにおける実施すべきセキュリティパッチの実施・未実施の状況
- 未実施の場合の理由および実施予定時期
- セキュリティパッチに代わる緊急措置を実施している場合、その理由と実施している措置の内容
- それぞれのシステムにおけるセキュリティパッチの実施の履歴

(2) 定期的なセキュリティホール検査の実施

セキュリティホールパッチの実施漏れが見逃されていることがないようにするためには、定期的あるいは緊急の確認が必要になった時点で、システムに残されている未対策のセキュリティホールを発見するための検査を実施することも必要である。

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない。

3.2.3. ウイルス対策

Tb3.1	ウイルス対策についての管理の仕組みの確立

【主旨】

ウイルス対策の基本は、ウイルスの侵入経路を検討し、その経路を遮断することにある。ウイルスの侵入は、メールやメールへの添付ファイルあるいはインターネット(ftp/http)からダウンロードするデータやファイルに付着したウイルスであることが多い。また、最近の傾向では脆弱性を狙ったネットワーク型感染もある。このため外部ネットワークとの接点や内部ネットワークを流れるデータを監視し、浸入を防ぐことがウイルス対策の基本となる。

また、不要なソフトウェアのインストールはウイルス感染の可能性が高いため、それらのソフトウェアのインストールはなるべく避け、必要な場合にはインストール前にウイルス検査を実施し、ウイルスに感染していないことを確認しなければならない。さらに外部から持ち込まれるファイル(FD、CD、DVD 等)も使用する前にウイルス検査を実施することも必要となる。さらに、ウイルス感染ファイルの持出しを防止するために、持出すファイルのウイルス検査も必要となる。

また、チェックをすり抜けたウイルスは早期にシステムから排除しなければならない。このため、定

期的にシステムに対しウイルス検査を行うことも必要となる。

これらのウイルス対策に用いるウイルス定義ファイルは常に最新にされていなければ、ウイルス対策ツールを用いたウイルス対策はあまり意味のないものになる。このため、ウイルス定義ファイルの確実なメンテナンスもウイルス対策の要の一つとなる。

また、ウイルス対策を尽くしたとしても、新たなウイルスの登場を考えると、万全はありえないため、ウイルス感染事故の発生への備えも欠かせない。

このようにさまざまな活動で構成されるウイルス対策が的確に行われ、実施に不手際がないようにするためには、ウイルス対策の実施を管理する仕組みを確立しておくことが必要となる。

ウイルス対策が適切に行なわれるようにするための管理の仕組みとして検討すべき事項としては、以下があげられる。

- ウイルス対策の組立ての確立
- ウイルス対策についての責任体制の確立
- ウイルスについての情報の収集とその分析･評価の仕組みの確立
- ウイルス対策の実施状況についての管理の要領の確立
- ウイルス感染事故発生時の対応のフレームワーク

【対策のポイント】

(1) ウイルス対策の組立ての確立

効果的なウイルス対策を効率的に行うためには、ウイルス対策の組立て、即ちウイルス対策ツールをどのように使いこなし、運用面では何をどのように行うのかと言ったようなこと決めておかなければならない。このウイルス対策の組立てとして検討すべき事項としては、以下のようなものがあげられる。

- システム区分ごとの要求されるウイルス対策の厳格さ

  システムの領域ごとに要求されるウイルス対策の厳格さは、システムの特性によって異なってくる。すべての領域に対し、最も厳格な対策を実施することも現実的でないので、システムの領域ごとにウイルス対策に関し必要となる厳格さを決めておくことが対策の詳細の検討のベースとなる。

- ウイルス対策の組立て

  ウイルス対策の組立てとして検討すべき事項としては、以下があげられる。

  ･ネットワークからの浸入を防止するためのウイルス対策ツールの選択と配置
  ･サーバやクライアント PC で用いるウイルス対策ツールの選択
  ･検疫システムの導入の要否
  ･ウイルス定義ファイルの更新方法
  ･ウイルス定義ファイルの更新の管理方法
  ･インストールするソフトウェアからの浸入の防止策
  ･ウイルス情報の利用法

(2) ウイルス対策の推進体制の確立

ウイルス対策についての責任体制として検討すべき事項としては、以下があげられる。

- ウイルス対策についての責任者の明確化とそのタスク
- ウイルス対策担当チーム（者）とそのタスク
- システム管理者やクライアントPCの利用者のタスク
- 外部の専門家の活用

また、責任者からクライアントPCの利用者に至るまでの関係者のすべてに、ウイルス対策にかかる自己の責任を周知させることも欠かせない。

(3) ウイルスに関する情報の収集とその分析・評価の仕組みの確立

日々、報告されているウイルスに関する情報に加え、システムの脆弱性にはウイルスの浸入の足掛かりを与えるものもあるため、システムの脆弱性情報も適切に入手し、入手した情報に対する分析・評価の速やかな実施と、必要な対応の検討も欠かせない。このことを適切に行うためには、ウイルスに関する情報の収集とその分析・評価の仕組みの確立も必要となる。

この仕組みとして検討すべき事項としては、以下があげられる。

- 情報の入手ルートと入手方法
- 入手した情報の取扱い方法（関係者への引渡し、必要な対応の検討、入手情報のファイリング、検討の記録の管理他）

(4) ウイルス対策の実施状況についての管理の要領の確立

ウイルス定義ファイルの更新、検疫システムの利用、インストールするソフトウェアに対するウイルス検査の実施、システムに対する定期的なウイルス検査の実施等がルールに沿って、適切に行われるようにするためには、これらの実施を管理する仕組みも必要となる。この仕組みについて検討すべき事項には、以下がある。

- チェックサイクル
- チェック事項
- チェックの実施方法

(5) ウイルス感染事故発生時の対応のフレームワーク

ウイルス感染事故発生時の対応のフレームワークとして検討すべき事項としては、以下があげられる。

- ウイルス感染事故発生時の即応体制
- ウイルス感染事故発生時の対応についての基本方針

【対応 ISMS コントロール】

8.3.1 悪意のあるソフトウェアに対する管理策

【参考】

(1) ウイルス対策の組立てについて

ウイルス対策の組立ての検討にあたっての検討事項としては、表 3-22 に示すものがあげられる。

表 3-22　ウイルス対策の組立ての検討にあたっての検討事項

区分	検討すべき事項
ネットワークからの侵入に対する阻止策	･サイトシステムと外部との間のデータフローに対するウイルスの監視 ･サイトシステム内のデータフローに対するウイルスの監視
サービス(アプリケーション)単位で行う入力データに対するウイルスの監視	･ゲートウェイ型ウイルス対策ソフトによる動的なウイルス検査の実施 ･特定のアプリケーションサーバに対応するウイルス対策ソフトでの動的なウイルス検査 ･クライアント、サーバでのウイルス対策ソフトでの検査の実施 ･IDS/IPS 装置によるネットワークの動的な監視 ･ウイルス検査の多重化
持ち込みファイルからの侵入に対する阻止策　（インストール、FD、CD、DVD、メール添付、ftp/http からのダウンロードのよる感染の阻止）	･ウイルス対策の視点からのソフトウェアのインストールに関するルールの確立 ･インストールするソフトウェアに対する素性確認の実施 ･インストールするソフトウェアに対するウイルス検査の実施と記録 ･外部から持ち込まれる形態･ファイルの形態の明確化 ･外部から持ち込まれるファイルの素性審査 ･圧縮データ、暗号化データの扱いの明確化 ･ゲートウェイ型ウイルス対策ソフトによる動的なウイルス検査の実施 ･特定のアプリケーションサーバに対応するウイルス対策ソフトでの動的なウイルス検査 ･クライアント、サーバでのウイルス対策ソフトでの検査の実施 ･ウイルス検査の多重化
感染の早期発見策（システムに対する徹底したウイルス検査）	･ウイルス検査要件の設定の明確化 ･臨時ウイルス検査の実施が必要なケースの明確化 ･新しい危険度の高いウイルスが報告され、このウイルスに対する定義ファイルが提供されたときに検査 ･定期ウイルス検査に不備が見つかった場合
ウイルスの外部への持出し防止策	･外部に持出す可能性のあるファイル形態や持ち出してもよい形態の明確化 ･外部に持出すファイルに対する素性確認の実施 ･ゲートウェイ型ウイルス対策ソフトによる動的なウイルス検査の実施 ･特定のアプリケーションサーバに対応するウイルス対策ソフトでの動的なウイルス検査 ･クライアント、サーバでのウイルス対策ソフトでの検査の実施 ･ウイルス検査の多重化
チェックをする抜けた場合の対策	･定義ファイルを最新のものに更新した後の点検の実施 　－感染可能性のある領域の点検 　－すべての領域の点検 ･ベンダーから提供される駆除ツールで点検する ･感染源の追跡調査をし、2 次感染、3 次感染の対策の作成 ･感染源の PC、ネットワークの遮断 ･感染ポートの遮断
検疫システムの導入	･検疫システムの適用方法 ･検疫システムでのチェック事項 ･使用するウイルス定義ファイルについての条件他の検疫システムの運用条件

Tb3.2	要求レベルに応じたウイルス対策ツールの選択と配置

【主旨】

ウイルス対策のほとんどはウイルス対策ツールに依存している。このため、ウイルス対策ツールの選択とシステム上への配置は、ウイルス定義ファイルのきめの細かい更新と並んで、ウイルス対策の成否を決定する要素となる。このため、ウイルス対策ソフトの選択とシステム構成の中での配置は、適切に行われ、かつ、計画通りの的確な実装が必要となる。

対象となるウイルス対策ツールとしては、以下がある。

- ウイルス検査ツール
- 検疫ツール
- ウイルス対策管理ツール

【対策のポイント】

(1) 適切なウイルス検査ツールと使用法の適切な選択

これらのツールの実装上での検討事項としては、表 3-23 に示すようなものがある。

表 3-23 ウイルス対策ツールの実装上の留意点

作業区分	検討事項
検査ツール	・ツールの選択と配置場所 選択の対象としては、以下が考えられる。これらは多重に使われることが多い 　－ゲートウェイ型ウイルス対策ソフト 　－クライアント、サーバにおくウイルス検査ツール 　－ネットワーク型ウイルス対策（IDS/IPS） ・機能の選択 　－未知のウイルスに対するチェックの実施 　－スパイウェア等の不審なプログラムのチェックの実施 ・危険を察知した場合におけるポートの遮断等の実施すべき措置の使用 ・ウイルス定義ファイルの更新機能の使用法 　－ウイルス定義ファイルの配布方法の指定 　－自動更新の指定等 ・システムに対する定期検査の実施に関する指定
検疫ツール	・ツールの選択 ・検査内容の指定 ・運用条件の指定
ウイルス定義ファイルの管理ツール	・ウイルス定義ファイルのメンテナンス方法の選択 　－定義ファイルの配布方法 　－定義ファイルの自動更新の適用とその適用法 　　・自動更新のサイクル 　　・強制更新の方法 ・ウイルス定義ファイルのバージョン管理の適用法 ・ウイルス検査ツールのバージョン管理の適用法 ・定期検査のスケジューリング機能の使用

(2) ウイルス検査ツールの適切な実装

ウイルス検査ツールの的確な実装の実現には、組込んだツールに対し、以下の時点時点での

確実な確認が必要となる。

- ウイルス対策ツールの新規導入時
- ウイルス対策ツールの変更時
- ウイルス対策ツールの使用機能の変更時
- ウイルス感染事故が発生し、ウイルス対策ツールやその使い方に問題があった場合
- システム構成の変更時

(3) ウイルス検査ツールの実装の的確性についての定期的なチェックの実施

ウイルス検査ツールの実装上の不備や、その使用法にシステムの現状との整合性が失われているようなことを見逃さないためには、ウイルス検査ツールが期待通り実装され、指定された運用で、期待通りに機能しているかどうかについて、定期的にチェックすることも必要となる。

【対応 ISMS コントロール】

8.3.1 悪意のあるソフトウェアに対する管理策

Tb3.3	ウイルス対策担当チームやシステムの利用者がウイルス対策に関し実行しなければならないことの的確な実施

【主旨】

ウイルス対策が定められていても、ウイルス対策チームがウイルス対策に関し運用上で実施しなければことを確実に実行するとともに、システム利用者がウイルス対策について行うべきことが、日常的に行われるようにしていなければ、期待したウイルス対策は実現しない。そのため、管理側・利用側ともにウイルス対策として定められていることが確実に実施されているかどうかについて、定期的にチェックを行い、習慣化を図るとともに、問題点を発見し、その問題点を改善していくことが必要である。

【対策のポイント】

(1) ウイルス対策チームがウイルス対策に関して行わねばならないことの明確化

ウイルス対策チームがウイルス対策に関して行わねばならないこととしては、以下があげられる。

- ウイルス対策ツールの使用状況の把握
- ウイルス対策定義ファイル
- ウイルス定義ファイルの更新状況の確認と実施漏れに対する対策の指示または強制実行
- 定期的なウイルス検査の実施
- システムの利用者に対する利用者サイドでのウイルス対策の支援
- 利用者に対するウイルス対策についての啓蒙

(2) システムの利用者がウイルス対策に関して行わねばならないことの明確化

システムの利用者がウイルス対策に関して行わねばならないこととしては、以下があげられる。

- 定義ファイルの更新を利用者の責任で行うようにしている場合における、ウイルス定義ファイルのきめ細かい更新、および緊急を要するウイルス定義ファイルの更新の遅滞のない実施

- システムに対するウイルス検査を利用者の責任で行うようにしている場合における、指定されたサイクルでウイルス検査の実施や、緊急を要するウイルス検査の遅滞のない実施
- 定期的なバックアップの確保
- ウイルス感染の兆候が見られた場合のネットワークからの切離し等の緊急措置の実施と、ウイルス担当チームへの報告

(3) ウイルス対策担当チームやシステムの利用者がウイルス対策に関し実行しなければならないことの実施を管理する仕組みの確立

ウイルス対策担当チームやシステムの利用者がウイルス対策に関し実行しなければならないことの実施に漏れや不手際が生じないようにするためには、これらの励行をチェックする組織的な仕組みの確立も必要となる。

(4) 使用中のすべてのウイルス対策ツールにおけるウイルス定義ファイルの更新の徹底

ウイルス対策担当チームやシステムの利用者がウイルス対策に関し実行しなければならないことの実施に漏れや不手際が生じないようにするためには、これらの励行をチェックする組織的な仕組みの確立も必要となる。

ウイルス定義ファイルの更新については、以下が確実に行われなければならない。

- 緊急を要するウイルス定義ファイルの更新やウイルス検査の迅速な実施
- 指定されたサイクルでの定期更新の実施
- 定期的あるいは必要に応じた更新状況のチェックの実施と、実施漏れシステムに対する更新実施の指導あるいは強制

(5) 定期的なウイルス検査および必要に応じた緊急のウイルス検査の実施

ウイルスチェックをすり抜けてシステムに侵入したウイルスの早期発見と駆除のためには、システムの全領域に対して、定期的あるいは緊急を要する場合の臨時のウイルス検査の実施が必要となる。定期検査の実施サイクルは、対象領域の重要性によって異なる。また、検査の実施状況もチェックし、検査漏れが出ないようにしなければならない。

(6) システムの利用者におけるウイルス対策にかかわる責務の励行

- 定義ファイルの更新を利用者の責任で行うようにしている場合における、ウイルス定義ファイルのきめ細かい更新、および緊急を要するウイルス定義ファイルの更新の遅滞のない実施
- システムに対するウイルス検査を利用者の責任で行うようにしている場合における、指定されたサイクルでウイルス検査の実施や、緊急を要するウイルス検査の遅滞のない実施
- 定期的なバックアップの取得と保管
- ウイルス感染の兆候が見られた場合のネットワークからの切離し等の緊急措置の実施と、ウイルス担当チームへの報告

【対応 ISMS コントロール】

8.3.1 悪意のあるソフトウェアに対する管理策

Tb3.4	ウイルス感染時の即応体制の整備

【主旨】

ウイルス対策を実施していても、対策上の盲点や不備、新しいウイルスの発生等で、ウイルスに感染してしまう可能性があり、ウイルス対策に完全はなく、感染してしまう可能性を考慮しておかなければならない。実際にウイルスに感染してしまった場合、直ちに対処する体制を整備しておき、具体的な処理や作業手順を明確化する必要がある。

【対策のポイント】

(1) ウイルス感染時の処理に必要な備えについての要求の明確化

ウイルス感染への備えとして準備すべき事項を、表 3-24 に示す。

表 3-24 ウイルス感染への備えとして準備すべき事項

区分	検討事項
ウイルス対策担当チームとして準備すべき事項	･当該タイプ事故の定義 ･事故の検知方法 ･必要な処置と処理手順 ･事故処理に必要なシステム環境 ･被害状況や原因の調査に必要な情報の指定 ･システム復旧に必要なバックアップの指定 ･連絡体制･手順の確立
利用側の備えとして準備すべき事項	･ウイルス対策についての教育の実施 ･ウイルス対策の実施に必要なスキルの確保 ･必要な処置と処理手順 ･連絡手順の把握

(2) ウイルス感染事故発生時における必要な緊急措置の遅滞のない実施

ウイルス感染事故への対応は、一般に、緊急の措置と本対策の 2 段階で行われる。

まず、緊急措置としては、以下の実施が必要となる。

- 感染状況の把握と分析
- 関係者への連絡と対策体制の立上げ
- ネットワークの切断等やシステムの利用の停止等の緊急措置
- 本体策の立上げ

また、緊急措置が行われ、被害の拡大防止が図られたら、本体策として以下を実行しなければならない。

- 感染ウイルスの特定と感染経緯の調査
- 感染ウイルスのシステムからの完全な駆除とその確認
- 被害範囲の再確認
- 情報等の回復
- システムの復旧

- 2 次被害の調査と、被害に対する必要な措置の実施
- 関係機関への報告

【対応 ISMS コントロール】

8.3.1 悪意のあるソフトウェアに対する管理策

3.2.4. システム情報およびセキュリティ管理情報の保護

システム構成情報とは、ネットワークの構成や使用しているソフトウェアのバージョンや設定やファイルのディレクトリ等のシステムの内部構成を示す情報を言う。また、セキュリティ管理情報とは、ファイアウォールに設定している接続制御に用いる情報や、ID/パスワードやアクセスコントロールテーブル等アクセス制御のベースとなっている情報や、暗号鍵等のセキュリティ対策を支えているツールが用いている情報を言う。これらの情報の漏洩や正確性の欠如は、実施しているセキュリティ対策の無効化につながる。このため、これらの情報の的確性の確保と秘匿性の確保には、徹底を期さなければならない。

本体策ドメインは、これらの情報の保護の徹底を求めるものである。

(注) ここでいうシステム情報やセキュリティ管理情報の例:
一般アカウント情報、特権アカウント情報、アクセス管理テーブル、電子証明書、暗号鍵、ID/パスワード
システム設定情報、ネットワーク設定情報、ファイアウォールの設定情報他

Tb4.1	システム情報やセキュリティ管理情報の保護の仕組みの確立

【主旨】

システム情報やセキュリティ管理情報は、多岐に渡るとともに、情報によっては大量なものもある。また、情報によっては変更も少なくないことから、これらの情報のすべてに対し、的確な保護を実現することは簡単ではない。このため、これらの情報の保護に不手際を起こさないようにするためには、これらの情報の保護についての組織的な仕組みの確立が欠かせない。

【対策のポイント】

(1) 厳重な保護を必要とするシステム情報やセキュリティ管理情報の漏れのない把握

システム情報やセキュリティ管理情報の保護を確実なものにするためには、まず、保護の対象となるこれらの情報のすべてがリストアップされ、そのそれぞれについてのライフサイクルがどのようなものであるかが正確に把握しておかなければならない。

これらの情報の個々について、把握すべき事項としては、以下があげられる。

- 情報名と情報の役割
- 情報の内容
- 管理責任者
- 情報の発生または作成および変更（含む抹消）の契機
- 情報の作成やシステムへの登録および変更に必要な手続き
- 情報の漏洩や正確性の欠如がセキュリティに与える影響
- 情報の漏洩が発生した場合に必要となる処置
- 情報やシステムへの登録に誤りが発見された場合に必要な措置
- 定期的な点検等の管理についての要求

(2) システム情報やセキュリティ管理情報の個々に指定すべき保護要件の指定要領の確立

これらの情報の保護が適切に行われるためには、まず、これらの情報のそのそれぞれにどのような管理や保護を行わねばならないかを明確にする保護要件の指定が適切に行われなければならい。このことが組織的な管理の下で適切に行われるようにするためには、これらの情報に対する保護要件の指定要領が確立していなければならない。

システム情報やセキュリティ管理情報に対する保護要件の指定要領に示すべき事項としては、以下があげられる。

- システム情報やセキュリティ管理情報に対する保護要件の指定（検討から、レビュー、承認までの）手続き
- システム情報やセキュリティ管理情報に対する保護要件として指定すべき事項（Tb4.2 参照）
- システム情報やセキュリティ管理情報に対する保護要件の指定の見直し要領
  - ・定期的な見直しサイクルおよび臨時の見直しが必要な場合
  - ・見直しの進め方
  - ・見直しのポイント

(3) システム情報やセキュリティ管理情報の保護についての要求の実践をチェックする仕組みの確立

これらの情報の保護が適切に行われるためには、これらの情報の保護に関し要求されていることの実践に正確で漏れがないようにするためには、要求の実践をチェックするための組織的な仕組み作り必要となる。この仕組み作りで検討すべきこととしては、以下があげられる。

- システム情報やセキュリティ管理情報の操作についての手続きの確立とチェックリストの作成
- 定期的な点検の手続きとチェックリストの作成

(4) システム情報やセキュリティ管理情報の保護についての責任体制の明確化

これらの情報の的確性の維持や保護には、管理する者も含め多くの者がかかわる。関係する者それぞれにおける責務と、関係者間の連携方法も明確にされていなければならない。

【対応 ISMS コントロール】

5.1.1 資産目録
5.2.1 分類の指針
5.2.2 情報のラベル付けおよび取扱い

Tb4.2	システム情報やセキュリティ管理情報に対する保護要件の確立

【主旨】

これらの情報の保護が適切に行われるためには、まず、これらの情報のそのそれぞれにどのような管理や保護を行わねばならないかを明確にする保護要件の指定が適切に行われなければならい。これらの情報の保護は、指定された保護要件の範囲でしか保護されないため、この指定の的確性は十分にチェックされていなければならない。

【対策のポイント】

(1) システム情報やセキュリティ管理情報の個々に対する保護要件の的確な指定

システム情報やセキュリティ管理情報の保護要件として、指定する事項としては表 3-25 に示すようなものがあげられる。

表 3-25 システム情報やセキュリティ管理情報の保護要件として指定すべき事項

区分	保護要件としての指定事項
サイトのセキュリティとの関係	・当該情報がサイトのセキュリティに果たす役割 ・当該情報が不正であったり、当該情報に漏洩、改ざん、破壊が発生した場合に考えられる影響とその範囲
当該情報の存在場所	・システム上での存在場所（格納サーバやサーバ内での格納場所や格納方法） ・PC 等の電子機器での取扱い状況（これらの情報が取扱われる PC や PC 上での使用状況） ・関係する印刷物の作成使用状況
情報内容についてのライフサイクル管理	・情報オーナー ・情報の発生あるいは作成についての手続き ・情報の変更の手続き ・情報の抹消の手続き
アクセス権限の管理	・アクセス権限者の範囲 ・アクセス権限者の指定の手続き ・アクセス権限者に付与する権限の範囲 ・アクセス権限者へのアクセス権の付与の手続き ・アクセス権限およびアクセス権限者に関する情報のシステムへの登録の手続き
システム上に置かれた対象情報の保護	・システム上の対象情報に対し必要とするアクセス制御 －アクセス要求の内容（情報の新規登録、更新、削除、参照、印刷や電磁媒体へのダウンロードを含む複写の作成、参照、バックアップの作成、再編成他）ごとに適用すべきアクセス制限 －アクセス者の識別と認証の方法 －アクセス制御の実現方法 －不審なアクセスに対する処置 ・システム上の情報についての要求 －暗号化の要否と暗号化を行う場合の暗号アルゴリズムや暗号の適用方法 －システム構成上での配置についての要求 ・アクセスの監視についての要件 －監視の対象と監視の方法
対象情報が記録された印刷物や電磁媒体の保護	・関係する印刷物の取扱い（作成から使用、保管、廃棄の全ライフサイクルを対象）についての制限と要求 ・関係する電磁媒体の取扱い（作成から使用、保管、廃棄の全ライフサイクルを対象）についての制限と要求

	・これらの情報が取扱われる電子機器の取扱いについての制限と要求 ・これらの情報を取扱う複写機等のその他の電子機器の取扱いについての要求
保全についての要件	・バックアップの取得範囲 ・バックアップの取得サイクル ・バックアップの保管についての要求

この保護要件の指定は、本要求に求められる対策強度レベルに対応できるだけのきめの細かさをもたなければならない。

これらの指定の的確性を確保するためには、これらの指定は定められた手順に沿って行われ、組織的な管理下で行われなければならない。

⑶ システム情報やセキュリティ管理情報の個々に対して指定した保護要件に対する見直しの実施

システム情報やセキュリティ管理情報も時間の経過とともに、管理の隙により、その的確性が失われたままになっていることも考えられる。このようなことがないようにするためには、これらの情報の内容や、そのシステムへの登録が正確かどうかについての定期的な点検を行わなければならない。

この点検がきちんと行われるようにするためには、定期点検や臨時に行う点検についての実施要領や、チェックリストの整備も必要となる。

【対応 ISMS コントロール】

5.1.1 資産目録
5.2.1 分類の指針
5.2.2 情報のラベル付けおよび取扱い

Tb4.3 システム情報やセキュリティ管理情報の保護の実践

【主旨】

多岐に渡るだけでなく変更も少なくないシステム情報やセキュリティ管理情報のすべてについて、保護要件に指定された保護に不手際が発生しないようにするためには、個々のシステム情報やセキュリティ管理情報に指定されている保護要件を、業務現場やシステムの運用現場での実際の保護対象であるシステム上のファイルや印刷物やこれらの情報が格納された PC 等の電子機器や電磁媒体に対する具体的な保護策への展開と、それぞれの保護対象物に指定された保護策の確実な実践が必要となる。

これらを適切に行うためには、業務現場やシステムの運用現場における以下の活動は、組織的な管理の下で行われなければならない。

【対策のポイント】

⑴ 情報内容の的確性の確保の追及

システム構成情報やセキュリティ管理情報そのものが的確なものであるようにするためには、これ

らの情報のすべてに対し、そのライフサイクルの全過程について、所定の手続きに従った作成、変更、抹消が、組織的な管理の下で行われなければならい。

また、定期的な点検も欠かせない。

(2) これらの情報のシステムへの登録の正確性の追及

システム構成情報やセキュリティ管理情報は、システムに登録されてはじめてその本来の役目を果たすものである。これらの情報のシステムへの登録過程での不手際があってはならない。システム上のこれらの情報が的確なものであるためには、これらの情報のすべてに対し、そのシステム上でのライフサイクルの全過程について、所定の手続きに従った新規登録、変更、抹消が、組織的な管理の下で行われなければならい。

また、定期的な点検も欠かせない。

(3) システム上のこれらの情報の保護の追及

システム上におかれたシステム構成情報やセキュリティ管理情報に対する、その秘匿性の確保や、不正な操作や、必要が生じた時の回復のためのバックアップの確保等、保護対象のこれらの情報の保護についての要求に応えるためには、以下が必要となる。

- 現実的な保護策の対象となるこれらの情報が含まれたファイルの把握
- 保護対象のファイルに対する保護要件の適切な指定
- 指定された保護要件に沿ったライフサイクル管理の実施
- 指定された保護要件に沿ったシステムへの格納
- 指定された保護要件に沿ったアクセス制御機能の組込み
- 当該ファイルに対するアクセス権限者とアクセス権限者に付与するアクセス権の妥当性の確保
- 必要に応じたバックアップの取得
- 必要に応じたアクセス監視や操作についての記録の確保

(4) システム構成情報やセキュリティ管理情報が記録された印刷物や PC 等の電子機器や電磁媒体に対する適切な取扱いの追求

システム構成情報やセキュリティ管理情報は、印刷物や PC 等の電子機器や電磁媒体上にもおかれる。このため、これらの情報の保護のためには、これらについての安全な取扱いも欠かせない。

- 保護対象となる印刷物や PC 等の電子機器や電磁媒体とそれらの使用環境の把握
- これらについての保護要件の適切な指定
- 関係者における保護対象となるこれらの一つ一つに対する、それぞれに指定された保護要件に沿った安全な取扱いの追及 (関係者への保護要件の明確化と保護の実践の指導の徹底)

なお、業務現場やシステムの運用職場における保護対象の印刷物や電子機器や電磁媒体の安全な取扱いについては、2.1.3 節を参照。

(5) 業務現場やシステムの運用職場におけるシステム構成情報やセキュリティ管理情報の取扱いについての管理の徹底

管理のポイントとしては、以下があげられる。

- 現実の保護対象に対する保護要件の指定の妥当性 (指定内容および指定のプロセス)

- 指定された保護要件のシステムへの反映の妥当性（反映内容およびシステムへの組込みのプロセス）
- アクセス権限者の管理およびアクセス権限者に付与する（した）アクセス権限の妥当性（アクセス権限者の指名、付与したアクセス権限の内容およびこれらの管理についてのプロセス）
- 必要な見直しの実施状況

【対応 ISMS コントロール】

5.1.1 資産目録
5.2.1 分類の指針
5.2.2 情報のラベル付けおよび取扱い

3.2.5. システム上の業務情報の保護

Tb5.1	システム上の業務情報の保護の仕組みの確立

【主旨】

システム上の業務情報は多岐に渡るとともに、情報によっては大量なものもある。また、情報によっては変更も少なくないことから、これらの情報のすべてに対し、的確な保護を実現することは簡単ではない。このため、これらの情報の保護に不手際を起こさないようにするためには、これらの情報の保護についての組織的な仕組みの確立が欠かせない。

【対策のポイント】

（1）厳重な保護を必要とするシステム情報やセキュリティ管理情報の漏れのない把握

システム上の業務情報の保護を確実なものにするためには、まず、保護の対象となるこれらの情報のすべてがリストアップされ、そのそれぞれについてのライフサイクルがどのようなものであるかが正確に把握しておかなければならない。

これらの情報の個々について、把握すべき事項としては、以下があげられる。

- 情報名と情報の役割
- 情報の内容
- 管理責任者
- 情報の発生または作成および変更（含む抹消）の契機
- 情報の作成やシステムへの登録および変更に必要な手続き
- 情報の漏洩や正確性の欠如がセキュリティに与える影響
- 情報の漏洩が発生した場合に必要となる処置
- 情報やシステムへの登録に誤りが発見された場合に必要な措置
- 定期的な点検等の管理についての要求

(2) システム上の業務情報の個々に指定すべき保護要件の指定要領の確立

これらの情報の保護が適切に行われるためには、まず、これらの情報のそのそれぞれにどのような管理や保護を行わねばならないかを明確にする保護要件の指定が適切に行われなければならない。このことが組織的な管理の下で適切に行われるようにするためには、これらの情報に対する保護要件の指定要領が確立していなければならない。

システム上の業務情報に対する保護要件の指定要領に示すべき事項としては、以下があげられる。

- システム上の業務情報に対する保護要件の指定（検討から、レビュー、承認までの）手続き
- システム上の業務情報に対する保護要件として指定すべき事項（Tb4.2 参照）
- システム上の業務情報に対する保護要件の指定の見直し要領
  - ・定期的な見直しサイクルおよび臨時の見直しが必要な場合
  - ・見直しの進め方
  - ・見直しのポイント

(3) システム上の業務情報の保護についての要求の実践をチェックする仕組みの確立

これらの情報の保護が適切に行われるためには、これらの情報の保護に関し要求されていることの実践に正確で漏れがないようにするためには、要求の実践をチェックするための組織的な仕組み作り必要となる。この仕組み作りで検討すべきこととしては、以下があげられる。

- システム上の業務情報の操作についての手続きの確立とチェックリストの作成
- 定期的な点検の手続きとチェックリストの作成

(4) システム上の業務情報の保護についての責任体制の明確化

これらの情報の的確性の維持や保護には、管理する者も含め多くの者がかかわる。関係する者それぞれにおける責務と、関係者間の連携方法も明確にされていなければならない。

【対応 ISMS コントロール】

5.1.1 資産目録
5.2.1 分類の指針
5.2.2 情報のラベル付けおよび取扱い

Tb5.2	システム上の個々の業務データに対する保護要件の適切な指定

【主旨】

システム上の業務データの保護管理を適切に行うためには、どのような保護をどのように行うかを定めた保護管理要件が、個々のファイルに対し適切に定められていなければならない。その際、前記保護管理要件は、当該業務データファイルに含まれる業務情報の保護要件を満たさねばならない。これらの情報の保護は、指定された保護要件の範囲でしか保護されないため、この指定の的確性は十分にチェックされていなければならない。

【対策のポイント】

(1) システム上の業務情報の個々に対する保護要件の的確な指定

システム上の業務情報の保護要件として、指定する事項としては表 3-26 に示すようなものがあげられる。

表 3-26 システム上の業務情報の保護要件として指定すべき事項

区分	保護要件としての指定事項
サイトのセキュリティとの関係	・当該情報がサイトのセキュリティに果たす役割 ・当該情報が不正であったり、当該情報に漏洩、改ざん、破壊が発生した場合に考えられる影響とその範囲
当該情報の存在場所	・システム上での存在場所（格納サーバやサーバ内での格納場所や格納方法） ・PC 等の電子機器での取扱い状況（これらの情報が取扱われる PC や PC 上での使用状況） ・関係する印刷物の作成使用状況
情報内容についてのライフサイクル管理	・情報オーナー ・情報の発生あるいは作成についての手続き ・情報の変更の手続き ・情報の抹消の手続き
アクセス権限の管理	・アクセス権限者の範囲 ・アクセス権限者の指定の手続き ・アクセス権限者に付与する権限の範囲 ・アクセス権限者へのアクセス権の付与の手続き ・アクセス権限およびアクセス権限者に関する情報のシステムへの登録の手続き
システム上に置かれた対象情報の保護	・システム上の対象情報に対し必要とするアクセス制御 －アクセス要求の内容（情報の新規登録、更新、削除、参照、印刷や電磁媒体へのダウンロードを含む複写の作成、参照、バックアップの作成、再編成他）ごとに適用すべきアクセス制限 －アクセス者の識別と認証の方法 －アクセス制御の実現方法 －不審なアクセスに対する処置 ・システム上の情報についての要求 －暗号化の要否と暗号化を行う場合の暗号アルゴリズムや暗号の適用方法 －システム構成上での配置についての要求 ・アクセスの監視についての要件 －監視の対象と監視の方法
対象情報が記録された印刷物や電磁媒体の保護	・関係する印刷物の取扱い（作成から使用、保管、廃棄の全ライフサイクルを対象）についての制限と要求 ・関係する電磁媒体の取扱い（作成から使用、保管、廃棄の全ライフサイクルを対象）についての制限と要求 ・これらの情報が取扱われる電子機器の取扱いについての制限と要求 ・これらの情報を取扱う複写機等のその他の電子機器の取扱いについての要求
保全についての要件	・バックアップの取得範囲 ・バックアップの取得サイクル ・バックアップの保管についての要求

この保護要件の指定は、本要求に求められる対策強度レベルに対応できるだけのきめの細かさをもたなければならない。また、この保護要件の定義にあたっては、対象ファイル等のライフサイクルやシステム上の配置、利用形態を軸に、考えられる脅威を考慮に入れたものとする必要がある。

これらの指定の的確性を確保するためには、これらの指定は定められた手順に沿って行われ、

組織的な管理下で行われなければならない。

(3) システム上の業務情報の個々に対して指定した保護要件に対する見直しの実施

システム上の業務情報も時間の経過とともに、管理の隙により、その的確性が失われたままになっていることも考えられる。このようなことがないようにするためには、これらの情報の内容や、そのシステムへの登録が正確かどうかについての定期的な点検を行わなければならない。

この点検がきちんと行われるようにするためには、定期点検や臨時に行う点検についての実施要領や、チェックリストの整備も必要となる。

【対応 ISMS コントロール】

5.1.1 資産目録
5.2.1 分類の指針
5.2.2 情報のラベル付けおよび取扱い

Tb5.3 DBMS 管理下にある業務情報に対する必要な保護策の展開

【主旨】

機密性の高い情報が格納されているリレーショナル・データベース(RDBMS:以下同じ)はその情報の「金庫」そのものである。たとえ他の対策によってシステムの可用性や OS 上のファイル保護が実現されていたとしても、特に内部犯行者による情報そのものへの不正行為に対しては必ずしも十分ではない。従って(近年多発している個人情報漏洩事件に象徴される)機密情報の漏洩や、不正な改ざん、消去といった格納情報に関わる脅威に対してはセキュリティを十分意識した RDBMS の設計・実装・運用管理といった対策が不可欠である。

【対策のポイント】

(1) RDBMS ユーザに対する適切な認証

管理者として RDBMS にアクセスするユーザ、クライアント・サーバ型のシステムを利用するユーザ等 RDBMS 上に登録されて直接接続を行うユーザについては、なりすまし等のリスクを低減するため適切な認証を行う必要がある。

- パスワードポリシーの明確な定義と実施(有効期限・使用履歴・定期変更・難易度)
- 必要に応じた他の認証技術(電子証明書、IC カード、バイオメトリクス等)の利用

(2) 情報に対する厳密なアクセスコントロールと最小権限の実装

格納情報に対する読み取り、追加、更新、削除について、業務上必要な最小限の権限を各ユーザ付与しなければならない。通常これらの権限は表・ビューといった単位で付与されるが、それが十分な厳密さでない場合はさらに行・列といったレベルまでの権限付与を検討する必要がある。

- アクセスポリシーの明確化(ユーザの分類と権限付与方針)

- 情報の Classification（機密性など情報の属性整理）
- 表･ビューに対する SELECT、INSERT、UPDATE、DELETE の各権限をユーザごとに必要最小限にする。
- 不正なルート、不正なアプリケーションを使ったアクセスに対しては権限を無効にする、閲覧を不可能にする、などの機能を実装する。
- アプリケーションと連携して行や列といった更に細かい単位でのアクセスコントロールを行う。

（3）RDBMS 全体に関わる権限の管理

RDBMS 全体に影響を及ぼすようなシステム上の特権については管理業務を行う、限られた管理者ユーザにのみ付与するようにする。管理者は単一のユーザ･権限である必要はなく複数の管理者で管理業務が分割されているような場合は当該業務で必要な特権だけを付与するようにする。

- 起動･停止の権限
- ユーザ作成･削除･権限付与
- 表･ビューの作成･削除･変更
- 監査機能の利用

（4）RDBMS におけるログの取得

セキュリティ侵害発生後の追跡･不正な行為の特定（日時、方法、犯人等）をより効率的かつ確実なものとするためには RDBMS 内部で行われた操作についてのログを収集し、保管しておくことが必要となる。

- 起動･停止･ログインに関わるログ
- ネットワークからの接続に関するログ
- 管理者権限の利用に関するログ
- 表･ビュー等格納された情報自体に対する操作ログ（トランザクションログを含む）
- アプリケーションユーザとの対応
- ログ自体の保管と保全
- プライバシー･機密情報への配慮

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

Tb5.4	業務情報に対する保護を目的とした DBMS との関係におけるアプリケーション構築への配慮

【主旨】

機密性の高い情報が格納されているリレーショナル･データベース（RDBMS：以下同じ）ではその情報保護のための対策が不可欠であるが、その一方 DBMS を利用して動作するアプリケーションとの関連を抜きにして完結できるものでもない。この項目では DBMS の利用部分についてアプリケーション側で対策を実装するべき部分について言及している。

【対策のポイント】

(1) アプリケーションに対する適切な権限付与

従来管理者権限で RDBMS にアクセスするアプリケーション等が見受けられたが、これは非常に危険な状態と考えるべきである。開発の段階から必要な権限を割り出し不要な権限がアプリケーション(アプリケーションが DBMS 接続に使うユーザ)に付与されることがないようにしなければならない。

(2) 情報に対する厳密なアクセスコントロールと最小権限の実装

格納情報に対する読み取り、追加、更新、削除について、業務上必要な最小限の権限を各ユーザ付与しなければならない。通常これらの権限は表・ビューといった単位で付与されるが、それが十分な厳密さでない場合はさらに行・列といったレベルまでの権限付与を検討する必要がある。

この実装を行うためにはアプリケーション側で必要なユーザが単一ではなく付与されるべき権限によって複数のデータベースユーザを用い、DBMS 側で適切な権限(またはロール)を付与できるような構造にしておく必要がある。

(3) 接続用の ID・パスワードのコーディング

アプリケーションが RDBMS に接続するためのユーザ ID・パスワードが接続用のプログラムや、バックアップ等のバッチ処理用スクリプトファイルに平文(暗号化されないテキスト)で書き込まれていることがしばしばあるが、これは OS 上の権限を奪取された場合等にそのまま DBMS への不正な接続を許すことにつながるため、可能な限り避けなければならない。

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

3.2.6. 通信路上の情報の保護

Tb6.1	通信に対する保護要件の確立

【主旨】

通信によって交換される情報の盗聴や改ざん、通信の妨害等の通信路上での脅威から守るためには、個々の通信に対して適切な保護措置が講じられなければならない。多岐にわたる通信に漏れなく必要な保護措置が講じられるようにするためには、通信の個々に対して必要な保護が明確にされていなければならない。

【対策のポイント】

(1) 通信に対する保護基準の明確化

多岐にわたる通信の個々に対する保護要件を適切に指定するためには、通信に対する保護

要件の指定のベースとなる保護基準を決めておくことが望ましい。

通信に対する保護基準として明確にすべき事項としては、以下があげられる。

- 通信情報の重要度と脅威の度合いの組み合わせから決まる通信の保護レベル
- 通信における盗聴対策、改ざんやなりすましに対する対策、通信妨害への対策についての保護レベルごとの手段の選択肢の範囲

それぞれの詳細については、参考を参照。

(2) 個々の通信に対する保護要件の指定

個々の通信に対する保護要件として指定すべき事項としては、以下のようなものがる。

- 通信対象となる情報
  - ・通信に含まれる情報
  - ・当該情報に対し指定されている保護要件
- 当該通信に適用する通信の保護基準で指定している保護レベル
- 盗聴対策についての要求
- 改ざん対策についての要求
- なりすまし対策についての要求
- 通信妨害対策についての要求
- 使用する通信路についての要求
- 使用する通信プロトコルについての要求
- 認証についての要求

(3) 個々の通信に対する保護要件の指定についての管理の仕組みの確立

通信に対する保護要件の指定に漏れが生じたり、指定に適切性を欠くようなことがないよう、その指定についても適切な管理が必要となる。このため、以下のような管理の仕組みの確立も必要となる。

- 通信に対する保護要件の指定についての責任体制
- 通信に対する保護要件の作成承認プロセス
- 通信に対する保護要件の指定状況の把握および定期的なチェックの実施要領
- 必要に応じた通信に対する保護要件の見直し要領

【対応 ISMS コントロール】

8.5.1 ネットワーク管理策

【参考】

通信の保護レベルのイメージを、表 3-27、表 3-28、表 3-29 に示す。ここでは、5 段階に分けた保護レベルを、それぞれのレベルに求められる保護で示している。

表 3-27 通信に対する保護レベル：盗聴に対する要求

レベル	保護要件
5	情報の絶対的な価値にみあう現在の最高水準の盗聴技術、暗号解読技術に対して対抗可能な保護を講じる必要がある ・通信路、装置全般について、通常手段では通信横取りが不可能なレベルの物理的な保護 ・高水準の暗号技術の併用

	･通信路に対する不正行為の検出手段の準備 など
4	一般的に知られている技術を使った盗聴、暗号解読に対して、ほぼ完全に対抗可能な保護を講じる必要がある。 ･通信路、装置全般について、専用線レベルの物理的な保護 ･民生用途で使用される最高水準の暗号技術の併用
3	意図的な盗聴以外の漏洩がなく、一般に流通していて容易に入手可能なツール、機器などの盗聴手段に対して対抗可能な保護を講じる必要がある。 ･一般の専用通信回線、閉域網サービス程度の保護、もしくは民生用途で使用される一般的なレベルの暗号技術の使用
2	意図的な盗聴以外の漏洩をほぼ防止できる程度の対策を講じればよい。 ･一般的な公衆通信回線の利用
1	特に対策は講じなくてもよい

表 3-28 通信に対する保護レベル：改ざんに対する要求

レベル	保護要件
5	情報の絶対的な価値にみあう現在の最高水準の技術を使った改ざん、なりすましに対して対抗可能な保護を講じる必要がある ･通信路、装置全般について、通常手段では通信横取りが不可能なレベルの物理的な保護 ･最高水準の改ざん防止（検知）及び自動復旧技術、認証技術の併用 ･通信路に対する不正行為の検出手段の準備 など
4	一般的に知られている技術を使った改ざん、なりすましに対して、ほぼ完全に対抗可能な保護を講じる必要がある。 ･通信路、装置全般について、専用線レベルの物理的な保護と通信相手先の正当性についての保証 ･民生用途で使用される最高水準の改ざん防止、認証技術の併用
3	一般に流通していて容易に入手できるツール、機器などの手段を使った改ざん、なりすましに対して対抗可能な保護を講じる必要がある。 ･一般の専用通信回線、閉域網サービス程度の保護、もしくは民生用途で使用される一般的なレベルの改ざん防止技術の使用
2	偶然による通信内容の破壊、相手先の誤認などをほぼ防止できる程度の対策を講じればよい。 ･一般的な公衆通信回線と信頼性の高い通信手順の利用
1	特に対策は講じなくてもよい

表 3-29 通信に対する保護レベル：通信妨害に対する要求

レベル	保護要件
5	意図的な妨害に対して、複数の異なる方式による代替通信･サービス手段を準備し、通信やサービスが停止する可能性をほぼゼロとするようなレベルでの対策が必要。
4	意図的な妨害に対して、少なくとも一つの代替通信･サービス手段を準備し、一方が完全にサービス不能になった場合も通信やサービスが停止することがないレベルでの対策が必要。
3	意図的でない通信集中による負荷には充分に耐えられる設計であって意図的な妨害に対して、影響を緩和することができ、完全な通信･サービス停止を可能な限り防止するようなレベルでの対策が必要。
2	意図的でない通信集中による負荷をある程度考慮した設計であること。
1	特に対策は講じなくてもよい

Tb6.2	保護要件にあった通信路の選択とその適切な使用

【主旨】

通信を保護する場合、適切な通信路や通信方式の選択は不可欠である。通信に用いる通信路や通信方式は、当該通信路を用いる通信の個々に指定されている保護要件を満たすようなものでなければならない。個々の通信に対して、保護要件を満たす通信路や通信方式を個別に採用すれば、それに越したことはないであろうが、現実的には、一つの通信路を多くの通信で共用することが多い。一つの通信路を複数の異なる保護要件を持つ通信で共有する場合は、通信路の保護要件を、通過する通信の保護要件を総合的に考慮したものを選ばなければならない。

このとき、保護要件が最も厳しい通信に合わせるか、通信路に適用する保護手段よりも厳しい要件を持つ通信に対しては、個別に適切な通信方式を選ぶことを前提に、保護要件が最も厳しい通信にあわすことをせず、コスト面でも機能面でも最も適切なものを選んでもいい。

【対策のポイント】

(1) 当該通信路を用いる通信の保護要件と性能、コストを考慮した通信路の選択

通信路の選択で考慮すべき事項としては、以下があげられる。

- 専用線、閉域サービス、公衆網、インターネット等の適切な使い分け
- LAN 媒体方式の適切な使い分け
- 暗号化された仮想通信路（VPN）の併用による安全性確保

(2) 通信路上で個別保護が必要な通信に対する保護策の指定

複数の通信と通信路を共有する場合で、その中に通信路がサポートする保護以上の保護が必要な通信が含まれている場合は、この通信に対しては、必要に応じ、以下のような個別の保護策を講じなければならない。

- 通信路及び使用する装置の物理的な安全策（通信の横取りの防止策他）
- 暗号化
- 必要な識別／認証
- 電子署名やタイムスタンプの適用
- 不正ソフトウェア対策（スパイウェア、スニファ対策他）
- アプリケーションレベルでの対策

(3) 指定された通信路の的確な実装

使用する通信路の確保と、それぞれに通信路に指定された保護要件の的確な実装を行うためには、以下が必要となる。

- 使用する通信路に対する保護要件の指定
- 必要な保護対策の実装の確認

(4) 通信に個々に対する必要な保護策の組込み

通信単位に保護策の実装が必要な通信については、その実装に漏れや不備が出ないようにし

なければならない。このためには、保護策の組込みについての確認の徹底が必要となる。

(5) ネットワークへの不正機器等接続防止策の実施

ネットワークに機器が不正に接続され、通信の盗聴等が行われないようにするためには、以下の対策も必要となる。

- LAN,ネットワーク機器に対する適切な保護策の実施
- コンピュータ等への盗聴用ソフトウェア導入防止策の実施

・無線ネットワーク (LAN) に固有の対策は 3.2.6(3)で取り扱うため除外する。

【対応 ISMS コントロール】

7.2.1 装置のセキュリティ

7.2.2 ケーブル配線のセキュリティ

8.5.1 ネットワーク管理策

Tb6.3	無線 LAN の使用についてのセキュリティ対策の実施

【主旨】

無線 LAN の使用にあたっては、電波による情報の拡散、外部からのアクセス可能性など、考慮が必要な事項が多いため、その仕様にあたっては、特別の配慮が必要となる。

【対策のポイント】

(1) 無線 LAN の使用についての基本方針の確立

危険の多い無線 LAN の不用意な使用をを避けるためには、無線 LAN の使用についての基本方針の確立が必要となる。無線 LAN の使用についての基本方針で明確にすべき事項としては、表 3-30 に示すようなものがあげられる。

表 3-30 無線 LAN の使用についての基本方針で検討すべき事項

項目	内容
利用基準	・使用が許される場合 (場所や適用業務等) ・使用を制限する業務または通信
通信の保護の方針	・講習無線アクセスポイントの利用制限 ・暗号化の適用方針 ・電波漏洩対策の方針 ・接続認証についての方針
利用者の啓蒙	・利用者への要求の範囲 ・利用者への利用上の留意事項の徹底方法の大枠
利用状況の監視	・監視についての方針

(1) 盗聴、アクセスポイントへの不正接続への対策の実施

具体策としての検討事項としては、表 3-31 に示すようなものがる。

表 3-31　盗聴、アクセスポイントへの不正接続への対策として検討すべき事項

項目	選択肢例
採用する暗号化機構	･128bit 以上の WEP や WPA/TKIP の利用
採用する電波漏洩対策	･固定暗号鍵を使用する場合の適切な管理 ･電子証明書による認証 ･MAC アドレスによる認証の併用
公衆無線アクセスポイントの利用制限	

(2) 無線 LAN 利用ポリシーの策定と不正なアクセスポイント設置防止対策の実施

- 無線 LAN 利用基準の明確化
- 不正アクセスポイント設置禁止の規定と周知
- 外部者による不正アクセスポイント設置の危険性の周知
- 適切な監視、監査の実施

　－定期的もしくは常時のモニタリング実施など

(3) 無線 LAN 適正利用の推進、利用状況の監視、定期的な監査の実施

【対応 ISMS コントロール】

8.5.1　ネットワーク管理策

3.2.7. インターネットサービスの利用にあたってのセキュリティ対策

Tb7.1	電子メールの使用についてのセキュリティ対策の実施

【主旨】

電子メールはその利用頻度、使われ方から見て、最も情報保護の検討が必要なアプリケーションである。現在の電子メールの機構は、インターネット上を平文で通過したり、発信元や宛先の正当性についての保証がないなど、それ自体は情報の安全を保証しない。厳しい保護要件が科された情報の送信にはメールの利用を避けるか、もしくは、暗号化、電子署名、タイムスタンプの付加など別段の対策を講じる必要がある。

【対策のポイント】

(1) 通信の機密性が保護されない通信路上での情報の漏洩対策の実施

通信の機密性が保護されない通信路上での情報の漏洩対策としては、下記に示すような方法での通信の暗号化を行うことにより、情報漏洩の防止を図ることができる。

- 個別メールの暗号化による保護
- サーバ間通信への暗号通信の導入
- サーバ、クライアント間通信への暗号通信の導入

(2) システム上での情報の漏洩防止策の実施

システム上での情報の漏洩対策としては、下記に示すような方法でのシステム上のメール情報の暗号化を行うことにより、情報漏洩の防止を図ることができる。

- 暗号利用による情報漏洩の防止
- 個別メールの暗号化による保護
- メール保存領域全体の暗号化による保護

(3) 改ざん、なりすまし、否認防止策の実施

通信の改ざん、なりすまし、否認への対抗手段としては、下記に示すような方法がある。必要に応じ、これらを使用する。

- 電子署名の使用
- 電子証明書の使用
- タイムスタンプの使用

(4) 公衆サービス利用ガイドラインの整備

以下に示すような公衆のメールサービスの利用は危険が多い。

- フリーメール等の業務利用
- 自組織以外のメールアカウントの業務利用
  - ―プロバイダ提供のメールアカウント
  - ―個人のメールアカウント
  - ―Web メールサービス

このため、その使用は制限されなければならない。原則として、使用しないことを原則とすべきであるが、使用が止むを得ない場合は、不用意な使用をさけるため、利用の制約や利用上の注意事項を示した利用のガイドラインを作成し、関係者にこれを徹底しておかなければならない。

【対応 ISMS コントロール】

8.7.4 電子メールのセキュリティ

Tb7.2	ファイル転送(FTP)他の危険なプロトコルの使用にあたっての保護措置の実施

【主旨】

ファイル転送で一般に使用される FTP や HTTP は、通信の経路上、転送されるデータの安全性（特に、完全性及び機密性）に関して、なんら保証のないプロトコルである。情報の保護要件を満たすためには、SSL の併用、情報（ファイル）の暗号化、VPN の併用などの措置が必要になることがある。また、ファイル転送に関して、各種の公衆サービスが存在するが、これらの利用についても、その安全性と情報の保護要件を考慮して利用する必要がある。

【対策のポイント】

(1) 通信の機密性が保護されない通信路上での情報の漏洩対策の実施

通信の機密性が保護されない通信路上での情報の漏洩対策としては、下記に示すような方法での通信の暗号化を行うことにより、情報漏洩の防止を図ることができる。

- 個別メールの暗号化による保護
- サーバ、クライアント間通信への暗号通信の導入

(2) 改ざん防止策の実施

通信の改ざんへの対抗手段としては、下記に示すような方法がある。必要に応じ、これらを使用する。

- 電子署名またはハッシュ値の使用
- タイムスタンプの使用

(3) 公衆サービス利用ガイドラインの整備

以下に示すような公衆サービスの利用には危険が多い。

- ファイル転送サービスの業務利用
- 匿名 FTP サーバの業務利用など自組織外のファイル転送
- サーバの利用

このため、その使用は制限されなければならない。原則として、使用しないことを原則とすべきであるが、使用が止むを得ない場合は、不用意な使用をさけるため、利用の制約や利用上の注意事項を示した利用のガイドラインを作成し、関係者にこれを徹底しておかなければならない。

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

3.2.8. サービス妨害への備え

Tb8.1	アクセス集中を用いたサービス妨害を考慮したシステムの設計

【主旨】

サービス妨害攻撃のなかでも、大量の通信を強要し、負荷を増大させるようなもの、とりわけ分散した攻撃元から一斉に開始されるような攻撃への対策は困難かつ限定的である。しかし、サービス停止の影響が非常に多いような場合、もしくは、攻撃によって他への影響が懸念されるような場合は、あらかじめ性能面で余裕を大きく確保したり、代替手段を準備するなどの対応が必要になる場合もある。サービス妨害の対象は、サーバなど直接的なサービスを提供するもののみでなく、セキュリティ機器など安全面での監視、制御なその機能を提供する機器にも及ぶ点に留意する必要がある。

【対策のポイント】

(1) サービス能力における余裕の確保

- 使用機器の性能面での余裕確保
  -ルータ、スイッチ等のネットワーク機器
  -サーバ（CPU速度、メモリ）
  -負荷分散装置
- ネットワーク設計における余裕の確保
  -アクセス回線の帯域についての余裕確保
  -LAN 回線、ポート単位の帯域についての余裕確保

(2) セキュリティシステムの能力における余裕の確保

- 使用機器の性能面での余裕確保
  -ファイアウォールその他、インラインに導入されるセキュリティ装置等
  -IDS などモニタリングを行うセキュリティ機器
- ログの安全性の確保
  -アクセス集中によるログあふれの防止

表 3-32、表 3-33 に、機器やネットワークの性能に余裕を持たせる k とにより、アクセス集中によるサービス妨害への備とする方法についのてイメージを、要求のレベルに応じて示す。

表 3-32 使用機器（サーバ、ネットワーク機器、セキュリティツール）の性能面での余裕の確保によるアクセス集中によるサービス妨害への備とする方法についてのイメージ

レベル	実施策
5	複数の代替機器の準備 ネットワークトラフィックが飽和した状態でも、1台の機器が過負荷で停止しない程度の性能的な余裕の確保（全体としてサービスが充分継続できる程度の余裕確保）
4	少なくとも1台の代替機器の確保 ネットワークトラフィックが飽和した状態において、全体として過負荷による停止を引き起こさない程度の性能的余裕の確保
3	設計上想定される通常のアクセス量のピーク時程度の負荷が長時間継続しても、処理が大きく滞留しない程度の性能的余裕の確保
2	設計上想定される通常のアクセス量のピーク時においても、過負荷による停止を引き起こさない程度の性能的余裕の確保
1	余裕については、特に考慮しない

表 3-33 ネットワークの性能面での余裕を持たせることでアクセス集中による サービス妨害への備える方法についてのイメージ

レベル	実施策
5	LAN/WAN ともに、複数の代替回線を用意し、必要に応じて、これらの回線を単独もしくは同時に利用できる構成とする。 個々の回線の帯域は、想定される通常トラフィックのピーク時の倍程度高い負荷においても、あふれない程度の余裕を確保する。
4	WAN 回線については、少なくとも一つの代替回線が用意されていて、必要に応じてこれらの回線を単独もしくは同時に利用できる構成とする。 WAN/LAN の個々の回線の帯域は、想定される通常トラフィックのピーク時の倍程度を確保する。
3	LAN 及び WAN の回線は、想定される通常トラフィックのピーク時より50%程度以上高い帯域を確保する。
2	LAN/WAN 回線は想定される通常トラフィックのピーク時においても、あふれない程度の帯域を確保する。
1	余裕については、特に考慮しない

(3) アクセス集中検知手段の検討

- アクセス集中(異常)検出手段の導入
  ・サーバ負荷の監視と異常検出
  ・トラフィック状況の監視と異常の検出
  ・アクセスログの監視と異常の検出

(4) アクセス集中緩和策の検討

- ネットワークトラフィック集中緩和策の導入
  ・帯域制限機能の導入
  ・代替回線の導入
- サービス配置の検討
  ・重要なサービスの分散配置(同じサーバに同居させない)など

表 3-34 に、アクセス集中を感知したとき、負荷を緩和する手段を用い、アクセス集中によるサービス妨害への備とする方法についのてイメージを、要求のレベルに応じて示す。

表 3-34 アクセス集中検知時における負荷の緩和を行うことで
アクセス集中によるサービス妨害への備とする方法についてのイメージ

レベル	実施策
5	日常的なアクセス、トラフィック監視に基づいて、異常な傾向(アノマリー)を発見するような機構を使用して常時監視を行う。 異常な傾向を検出した場合に、警告を発生させるほか、明らかに負荷が異常に高くなった際に、自動的にネットワークの帯域を制御したり、代替回線や機器に振り分けたりして、負荷を軽減させるような自動対応が可能なシステムを用意する。
4	日常的なアクセス、トラフィック監視に基づいて、異常な傾向(アノマリー)を発見するような機構を使用して常時監視を行う。異常な傾向についての警告を受けた場合、管理者がネットワークの帯域制限などにより、負荷を軽減できる手段を用意する。
3	ネットワークの帯域、サーバ負荷などが一定レベルを超えた場合に警告を発生するような監視機構を用意する。異常な傾向についての警告を受けた場合、管理者がネットワークの帯域制限などにより、負荷を軽減できる手段を用意することが望ましい。
2	監視機構は用意せず、管理者が適宜、状態を調べて異常があれば対応する。
1	特に考慮しない

(5) 定期的なアクセス状況の掌握

- ネットワークトラフィックの定期的な計測
- サービスアクセスログの定期的な解析

(6) 状況の変化に応じた設計の変更

- 使用機器等の性能・容量見直し
- サービス配置の見直し
- ネットワーク帯域の見直し
- 異常検出手段等の見直し

保護要件レベル3以上においては、定期的に⑤及び⑥を実施する。

【対応 ISMS コントロール】

8.2.1 容量、能力の計画作成

Tb8.2	緊急対応手順の検討と策定

【主旨】

アクセス集中によるサービス妨害攻撃への有効な対抗策はほとんどないが、サービスの停止を防ぐことで、少なくともサービスを継続させたり、あらかじめ予見可能なワーム等による分散サービス妨害の場合は、サーバのアドレスをあらかじめ変更して、DNS への登録先を変更するといった回避策をとれる可能性がある。攻撃によるサービス停止が、広範囲の影響を及ぼすような場合は、このような措置も検討されるべきである。また、このような措置を実際に素早く行うために、あらかじめ手順を検討し、文書化しておくことが重要である。

【対策のポイント】

(1) アクセス集中が発生した場合の対応手順、体制の策定と文書化

- 異常検出時の連絡、対応の体制
- サービスの優先順位付けと重要サービスの保護手順
- 負荷回避もしくは緩和策と実施手順
- サービスダウン等の障害発生時の復旧手順

(2) ワーム等による攻撃が予想される際の回避手順の策定と文書化

- DNS 操作による回避
- IP アドレス変更による回避
- その他回避、緩和策

(3) 緊急対応訓練の実施

【対応 ISMS コントロール】

8.1.3 事件･事故管理手順

3.2.9. システムの動きに対する監視の実施

Tb9.1	ネットワークの動きに対する監視の実施

【主旨】

攻撃に対する堅牢性を確保するためには、ここまでに述べた対策を実施することに加えて、ネットワークの動きを監視する必要もある。ネットワークの動きを監視することにより、攻撃を受けたことや、その兆候を早期に発見することも可能となり、原因の究明および対策の立案を行うことができる。

【対策のポイント】

(1) ネットワークの動きに対する監視のスキームの確立

ネットワークの動きに対する監視が適切に行われるようにするためには、監視が戦略的かつ効果的に行われるようにするためのスキームの確立が必要となる。ネットワークの動きに対する監視のスキームの確立として、検討すべき事項としては表 3-35 に示すようなものがある。

表 3-35 ネットワークの動きに対する監視のスキームとして検すべき事項

検討事項	検討内容等
監視の目的	・監視に期待することの大枠 －発見したい問題点(検知したい動き他) －問題が生じた場合の処理の追跡
監視のポイントと監視の対象	・監視のポイント －外部ネットワークと内部ネットワークの接点 －企業グループ内のセグメント間 －内部ネットワークにおけるセグメント間　等 ・各監視ポイントにおける監視の内容 －監視すべき動き －監査ログの取得対象 必要に応じたアクセプトログの取得等の指定
監視の運用	・リアルタイムで行うべきこと －リアルタイムで行うべき警告等 ・日次ベースで行うべきこと(報告事項と報告への対応) ・週次ベースで行うべきこと(報告事項と報告への対応) ・月次ベースで行うべきこと(報告事項と報告への対応) ・監視項目に対するチェックのタイミング
監視の仕組み	・使用する監査ツールと監査機能の選択 －必要に応じた IDC の利用 ・使用する監査ログの分析ツール
監査ログの保全	・監査ログに求める改ざん防止策 ・監査ログのオーバーフローへの備え ・監査ログの保管方法 －保管形態(使用媒体等) －保管場所と保管期間 －管理方法 －バックアップの取得
監査の運営体制	・監査の責任体制 －監査責任者と監査担当者およびそれぞれの責務 －システム運用チームとの連携方法 ・監査の外部への委託 ・外部の専門家の助言の利用

(2) 必要なツールの的確な実装

計画した監視が期待した機能を発揮するするためには、使用するツールが的確にシステムに組み込まれていなければならない。このことを確実なものとするためには、以下が必要となる。

- 使用するツールの適切な選択

  ツールの選択は、監視をどのレベルまで行うかに依存する。使用する監視ツールの選択に当たってのチェックポイントとしては、以下のようなものがある。

  ・可能な範囲での未知の攻撃に対する監視の要否

  ・警告のリアルタイム性の要否

・監視内容と監査ログの取得についてのサポート範囲
・監査ログの保全についてのサポート範囲
・監査ログの分析についてのサポート範囲

- 使用するツールのそれぞれについての使用法の検討と、それぞれのツールについての機能要件の確立
- 使用するツールのシステムへの的確な実装

この点についてのチェックポイントとしては、以下があげられる。

・各ツールへの要求の確認
・諸設定の確実な設定と機器への正確な登録
・さまざまな視点からの機能テストの徹底

これらが適切に行われるようにするためには、ツールの選択や使用法の決定やシステムへの実装についての管理の仕組みの確立も必要となる。

また、監視ツールの実装については、問題が生じた場合はもちろん、定期的な見直しを行うことも必要となる。

(3) 監視実施要領の確立

監視の実施には、日常的な処理が含まれることもあって、監視活動が所期の期待通りに行われるようにするためには、監視の実施要領の確立が必要となる。監視の実施要領として検討すべき事項としては、以下のようなものがある。

- 日次、週次、月次等の定例的に行うべきこととその実施手順

検討すべき事項としては、以下があげられる。

・監視報告書の作成要領
・監査報告書の取扱い要領(チェックのポイントと評価の進め方)
・取得した監査ログの取扱い要領
・ツールのメンテナンスの実施要領

- 監査ログの分析要領

膨大な監査ログの分析が適切に行われるようにするためには、以下のようなことを明確にした監査ログの分析要領を確立しておくことも必要となる

・ログ分析の観点、チェックするログ項目
・不正なアクセスとみなすログ項目の値、基準
・ログ分析実施者、実施日時、実施手順
・不正アクセスが検知した場合の対応フロー・手順

- 緊急時に必要な対処とその実施手順

(4) ルールに沿った監視の実施

指定された監視に手抜きが見逃されないようにするためには、監視の実行を管理する仕組みの作成と、この仕組みにもとづく実施についての管理と、必要な指導も必要となる。

(5) ルールに沿った監査ログの保管

【対応 ISMS コントロール】

9.7.1 事象の記録

9.7.2 システムの使用状況の監視

Tb9.2	システムへのアクセスに対する監視の実施

【主旨】

攻撃に対する堅牢性を確保するためには、ここまでに述べた対策を実施することに加えて、システムレベルの監視を実施することにより、攻撃やその兆候を早期に発見するとともに、原因の究明および対策の立案を行うことができる。

特に、情報の流出や改ざんなどが発生した場合、システムアクセスに対する監視が適切に行われていないと、事件を追跡することはできない。

【対策のポイント】

(1) システムへのアクセスに対する監視のスキームの確立

システムへのアクセスに対する監視が適切に行われるようにするためには、監視が戦略的かつ効果的に行われるようにするためのスキームの確立が必要となる。システムへのアクセスに対する監視のスキームの確立として、検討すべき事項としては表 3-36 に示すようなものがある。

表 3-36 ネットワークの動きに対する監視のスキームとして検すべき事項

検討事項	検討内容等
監視の目的	・監視に期待することの大枠 －発見したい問題点(検知したい動き他) －問題が生じた場合の処理の追跡
監視のポイントと監視の対象	・サーバごとの監視の内容 －監視すべき動き －監査ログの取得対象
監視の運用	・リアルタイムで行うべきこと －リアルタイムで行うべき警告等 ・日次ベースで行うべきこと(報告事項と報告への対応) ・週次ベースで行うべきこと(報告事項と報告への対応) ・月次ベースで行うべきこと(報告事項と報告への対応) ・監視項目に対するチェックのタイミング
監視の仕組み	・システムの監査機能の使用法 ・使用する監査ログの分析ツール
監査ログの保全	・監査ログに求める改ざん防止策 ・監査ログのオーバーフローへの備え ・監査ログの保管方法 －保管形態(使用媒体等) －保管場所と保管期間 －管理方法 －バックアップの取得
監査の運営体制	・監査の責任体制 －監査責任者と監査担当者およびそれぞれの責務

	―システム運用チームとの連携方法 ･外部の専門家の助言の利用

⑵ 必要なツールの的確な実装

計画した監視が期待した機能を発揮するするためには、使用するツールが的確にシステムに組み込まれていなければならない。このことを確実なものとするためには、以下が必要となる。

- 使用するツールの適切な選択
- 使用するツールのそれぞれについての使用法の検討と、それぞれのツールについての機能要件の確立
- 使用するツールの的確な実装

  この点についてのチェックポイントとしては、以下があげられる。

  ･各ツールへの要求の確認

  ･監視機能についての設定

⑶ 監視実施要領の確立

監視の実施には、日常的な処理が含まれることもあって、監視活動が所期の期待通りに行われるようにするためには、監視の実施要領の確立が必要となる。監視の実施要領として検討すべき事項としては、以下のようなものがある。

- 日次、週次、月次等の定例的に行うべきこととその実施手順

  検討すべき事項としては、以下があげられる。

  ･監視報告書の作成要領

  ･監査報告書の取扱い要領（手続きや体制等）

  ･取得した監査ログの取扱い要領

  ･ツールのメンテナンスの実施要領
- アクセスログの分析要領

  膨大なアクセスログの分析が適切に行われるようにするためには、以下のようなことを明確にしたアクセスログの分析要領を確立しておくことも必要となる

  ･アクセスログ分析の観点、チェックするログ項目

  ･不正なアクセスとみなすログ項目の値、基準

  ･アクセスログ分析実施者、実施日時、実施手順

  ･不正アクセスが検知した場合の対応フロー･手順
- 緊急時に必要な対処とその実施手順

⑷ ルールに沿った監視の実施

指定された監視に手抜きが見逃されないようにするためには、監視の実行を管理する仕組みの作成と、この仕組みにもとづく実施についての管理と、必要な指導も必要となる。

⑸ ルールに沿った監査ログの保管

【対応 ISMS コントロール】

9.7.1 事象の記録

9.7.2 システムの使用状況の監視

Tb9.3	アプリケーションへのアクセスに対する監視の実施

【主旨】

アプリケーションへのログインやアクセスは、システムログには記録されないものが多い。このため、システムに対するアクセスログを監視するだけでは不十分であり、アプリケーションのログについても監視を行う必要がある。

WEB サーバ、メールサーバなどの汎用的なアプリケーションについては、ログが用意されていることが多いが、開発された業務アプリケーションには、十分なログ機能が用意されていない場合があるので、機能を補うための対策が必要となる。

【対策のポイント】

(1) アプリケーションへのアクセスに対する監視のスキームの確立

アプリケーションへのアクセスに対する監視が適切に行われるようにするためには、監視が戦略的かつ効果的に行われるようにするためのスキームの確立が必要となる。アプリケーションへのアクセスに対する監視のスキームの確立として、検討すべき事項としては表 3-37 に示すようなものがある。

表 3-37 ネットワークの動きに対する監視のスキームとして検すべき事項

検討事項	検討内容等
監視の目的	・監視に期待することの大枠 －発見したい問題点（検知したい動き他） －問題が生じた場合の処理の追跡
監視が必要なアプリケーションと監視の内容	・アクセス監視が必要なアプリケーション ・対象アプリケーション（群）ごとの必要とする監視の内容 －監視すべき動き －監査ログの取得対象
監視の運用	・リアルタイムで行うべきこと －リアルタイムで行うべき警告等 ・日次ベースで行うべきこと（報告事項と報告への対応） ・週次ベースで行うべきこと（報告事項と報告への対応） ・月次ベースで行うべきこと（報告事項と報告への対応） ・監視項目に対するチェックのタイミング
監視の仕組み	・監査機能の実装方法 ・使用する監査ログの分析ツール
監査ログの保全	・監査ログに求める改ざん防止策 ・監査ログのオーバーフローへの備え ・監査ログの保管方法 －保管形態（使用媒体等） －保管場所と保管期間 －管理方法 －バックアップの取得
	・監査の責任体制

監査の運営体制	－監査責任者と監査担当者およびそれぞれの責務 －システム運用チームとの連携方法

(2) アプリケーションへの必要な監視機能の実装

アプリケーションへのアクセスの監視は、システムごとに個々のアプリケーションへの必要な機能を組込むことが必要となる。必要な監視機能の実装を的確なものにするためには、以下が必要となる。

- アプリケーションごとのアクセス監視についての要求の確認
- アプリケーションに組込むアクセス監視機能の設計
- 設計したアクセス監視機能のアプリケーションへの確実な組込み

(3) 監視実施要領の確立

監視の実施には、日常的な処理が含まれることもあって、監視活動が所期の期待通りに行われるようにするためには、監視の実施要領の確立が必要となる。監視の実施要領として検討すべき事項としては、以下のようなものがある。

- 日次、週次、月次等の定例的に行うべきこととその実施手順

  検討すべき事項としては、以下があげられる。

  ・監視報告書の作成要領
  ・監査報告書の取扱い要領(手続きや体制等)
  ・取得した監査ログの取扱い要領
  ・ツールのメンテナンスの実施要領

- アクセスログの分析要領

  アクセスログの分析が適切に行われるようにするためには、以下のようなことを明確にしたアクセスログの分析要領を確立しておくことも必要となる

  ・アクセスログ分析の観点、チェックするログ項目
  ・不正なアクセスとみなすログ項目の値、基準
  ・アクセスログ分析実施者、実施日時、実施手順
  ・不正アクセスが検知した場合の対応フロー・手順

- 緊急時に必要な対処とその実施手順

(4) ルールに沿った監視の実施

指定された監視に手抜きが見逃されないようにするためには、監視の実行を管理する仕組みの作成と、この仕組みにもとづく実施についての管理と、必要な指導も必要となる。

(5) ルールに沿った監査ログの保管

【対応 ISMS コントロール】

9.7.1 事象の記録

9.7.2 システムの使用状況の監視

3.3. セキュアなシステムの構築とそのセキュアな運用の実現

3.3.1. セキュアなシステムの構築とその維持

Tc1.1	セキュアなシステム構成の設計

【主旨】

セキュリティ対策はシステムの構成に大きくかかわる一方、システムの構成もセキュリティ対策の組立てを左右する。このように、システムの構成とセキュリティ対策は表裏一体のものであるため、システムの構成の設計にあたっては、セキュリティ対策面からの配慮が欠かせない。システムの構成をセキュアなものとして設計するためには、セキュリティ面からのシステムの構成の組立てについての考え方を確立するとともに、この考え方に沿った構成方針を決め、その細部の設計は多岐にわたるセキュリティ対策からの要求を適切に反映したものにしなければならない。

システムの構成をセキュアなものとして設計するためには、以下を適切に行うことが必要となる。

- 構成の組立てについての基本的な考え方の確立
- これらを反映したネットワーク構成のフレームワークの確立

【対策のポイント】

(1) システム構成の組立てについての基本的な考え方の確立

サイトのネットワーク構成と、各機器の機能の分担、およびサイトのセキュリティ確保のための機能の分担を決めるための考え方を示すもので、システムのネットワーク構成や各機器への機能の配置等は、この考え方にもとづいて行われなければならない。

このシステム構成についての基本的な考え方として明確にすべきこととしては、以下があげられる。

- システム構成方針の明示

  ゾーン構成、情報の保護、障害対策、性能対策、事故対応等からのシステムのトポロジーについての考え方の明示
- ゾーン分割方針の明確化

  ゾーンの分割方針を決めるにあたって検討すべき事項としては、以下がある。

  ・それぞれのゾーンの意味

  ・各ゾーンに配置するサービスや DB の配置原則

  ・各ゾーンに対するセキュリティ要件

  ・ゾーン間の通信ルール(経路制御、接続方式、アクセス制御、通信の秘匿化等)
- ネットワーク上の各機器の配置に対する考え方

  ファイアウォールや各種サーバ等の機器を、どのゾーンにどのように配置するかについての考え方を定義する。
- サーバへのサービスの配置についての方針の明確化

- サーバへの DB の配置についての方針の明確化
- クライアントへのセキュリティ要求の明確化
- セキュアなプラットフォームの使用についての方針の明示

  セキュアなプラットフォームの使用についての検討事項としては、以下がある。

  ・セキュアな OS の使用についての方針の明確化

  ・セキュアな DBMS の使用についての方針の明確化
- セキュリティツールの使用方針

  セキュリティツールの使用についての検討事項としては、以下がある。

  ・通信制御ツールの使用方針とシステム構成上の配置とタスクの明示

  ・アクセス制御ツールの使用方針とシステム構成上の配置とタスクの明示

  ・ウイルス対策ツールの使用方針とシステム構成上の配置とそれぞれのタスクの明示
- セキュリティサービス機能の配置についての考え方

  アクセス制限や、アクセス監視、ウイルス検査等、サイトのセキュリティ確保のための機能をネットワーク上にどのように配置するかについての考え方を明確にする。

  このシステム構成にの組立てについての考え方は、サイトのセキュリティ確保のための諸施策を反映したものでなければならない。

(2) セキュリティ対策面でのシステム構成のフレームワークの確立

実際にシステムを構築するためのシステム構成のフレームワーク設計を、システム構成の基本的な考え方に沿って適切に行う。

この設計においては、以下の点が明確にされていなければならない。

- サイトのネットワーク構成
- サイトのネットワーク構成上における各機器の配置（接続図）
- 各接続機器への機能配置

  ・当該機器に配置する本来機能

  ・当該機器に格納する DB 等で示す収容するファイル

  ・当該機器がサポートするサイトのセキュリティ確保のための機能
- 各構成機器に求められるセキュリティ要件

  ・アクセス制限等の当該機器に求められるセキュリティ対策

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない。

【参考】

(1) セキュアなシステム構成検討の視点

サイトシステムをセキュアなものにするために、その構成の検討にあたって考慮すべき事項としては、以下をあげることができる。

- システムに組込むセキュリティサービス機能が、効率的に所期の役割を果たすようにする
- システムに組込むセキュリティサービス機能の実装に漏れを生じにくくする

- セキュリティに関する事故が生じても、その影響は出来るだけ局所化されるようにする
- 性能等、システムの本来機能の提供とのバランスをとる
- システムの構築やその維持管理が複雑になり過ぎないようにする

(2) サービスの分散についての考え方

Web サーバ、ショッピングや決済をサービスするアプリケーションサーバ、さらに消費者情報等を格納する DB サーバ等を、その負荷分散や事故時における影響範囲の局所化といった観点から、複数の機器に分散して配置することも検討の対象である。

サービスの分散についての検討ポイントをあげると、以下のようになる。

- 分散を検討すべきサービス
  - ・分散の目的と期待効果
  - ・目的に添った分散のあり方とその有効性
- 分散方式
  - ・分散のメッシュ
  - ・分散処理の方式と、分散されたものの間での連携の方式
- システムの維持管理等システム運用上の負担
- コスト負担
- ネットワークの負担等のシステムの性能問題

(3) 同一機器への異なるサービスの配置についての考え方

コストや運用上の問題から一つの機器にいろいろなサービスを同居させることも多い。一つのサーバへの異なるサービスの配置は、一つのサービスにおけるセキュリティに関係する問題が、そのサービスの特性や問題の内容によっては、同居している他のサービスにもセキュリティ問題を波及させる可能性もある。

できれば異なるサービスは同一機器に配置しないことが望ましいが、システムの構築およびその維持管理の手間、コスト等とのバランスから、どうしても一つの機器に複数のサービスを同居させなければならない場合は、運用面でのカバーも含め、他への影響をなくすためのシステム運用上の配慮について十分に検討を行うことが必要である。

以下のサービスについては、できれば同一機器に配置しないことが望ましい。

- DNS サーバ
- Web サーバ
- メールサーバ
- ftp サーバ

(4) ネットワーク上へのサービスの配置についてのポイント

システムに組込む各種のサービスをどのゾーンへどう配置（接続）するかを決めるものであり、その検討にあたって配慮すべきこととしては、以下をあげることができる。

- 当該サービスに求められるアクセス制限
- 異なるサービスとの同一機器上での共存の可否と、共存が必要な場合の条件
- 被害の発生等に備えた分散配置の要否と、分散が必要な場合の分散の方法

(5) アクセス制限の配置と機能分担についてのポイント

サイトにおける各サーバへのアクセス制御は、ファイアウォールのアクセス制御機能や各機器におけるアクセス制御機能を用いて行われる。個々の機能の使用上の不備や、機能間の連携の不備により、アクセス制御に漏れがないよう、その配置と機能分担については十分な検討と点検が必要となる。

アクセス制御機能の配置と機能の分担に関し、特に検討すべき点としては、以下をあげることができる。

- ファイアウォールを複数用いる場合の役割分担
- ファイアウォールと各サーバのアクセス制御機能間の役割分担と連携

(6) アクセス監視機能の配置と機能分担について

アクセス監視機能についても、アクセス監視機能の配置と、アクセス監視をサポートしている機器間での機能の分担が、適切に行われていなければならない。

この点に関し、検討すべき事項としては、以下をあげることができる。

- アクセス監視の対象範囲
  ―全てのアクセスを監視にするのか、特定対象だけの監視にするのか
- 監視装置等監視サービスの機能と各サーバ、各サービスが独自に行う監視機能との役割分担

(7) ウイルス対策範囲の明確化と監視機能の配置と機能分担について

ウイルス対策を行うシステム構成上の範囲を明確にする。ウイルス監視機能は、ウイルス対策の対象とする範囲に対して、最適な位置に配置する。また、ウイルス監視機能についても、そのサポートしている機能間での機能の分担が適切に行われていなければならない。

ウイルス監視機能の配置と機能の分担に関し、特に検討すべき点としては、以下をあげることができる。

- 全体監視にするか特定対象だけの部分監視にするか
- 監視装置等監視サービスの機能と各サーバ、各サービスが独自に行う監視機能との役割分担

(8) 保護対象の情報資産の配置についての考え方

セキュリティ管理情報やユーザデータ等の保護対象とすべき情報資産のシステム構成上の配置については、特に慎重な検討を必要とする。

保護対象の情報資産については、情報ごとに個別にアクセス制限が行われているはずであるが、収容されているサーバ自体が攻撃を受けるとその影響を受けることも考えられるため、ネットワーク的に見てアクセスが制限されている位置に配置すべきである。

また、その保護が特に重要なものについては、他とは隔離されたサーバへの配置も検討すべきである。

保護対象情報資産のシステム構成上での配置は、その情報の保護の重要度により決められるものであるが、その配置に関し、検討すべき点とは以下のようになる。

- 配置ゾーン
- 外部から直接的なアクセスを排除する多重配置
- 当該サーバへの外部からのアクセスと、当該サーバから内部サーバへのアクセスのタイプを

別々に分離することにより、外部から内部サーバへの直接アクセスを防止する。

- 他のサービス、情報資産との分離
- サイトのネットワーク上で配置する位置の限定

特に、外部から直接アクセスが可能なサーバへの保護対象情報の配置は危険である。

(9) 保全データの配置

セキュリティにかかる事故に備えたシステムの保全は、脅威に対応して検討されるが、システム構成の検討にあたっては、これらの保全処置がサイト全体として適切に行われるように配慮しなければならない。

検討すべき事項としては、以下があげられる。

- サイト全体としての保全ファイルの構成
- 保全ファイルの配置

Tc1.2 システム構成方針に沿ったシステム構成の構築とその維持

【主旨】

システム構成は、常に、セキュリティ面からの要求に沿ったものでなければならない。システムの構成をセキュアなものとして構築し、その的確性を維持するためには、システムの構成や各機器の実装を設計通りのもとして構築するとともに、セキュリティ環境の変化に伴う必要な変更を適宜行い、その的確性を維持しなければならない。

【対策のポイント】

(1) 設計通りのシステム構成の構築

システムの構成をセキュリティ対策とマッチしたものとするためには、システムの構成をセキュリティ対策面からの要求を入れたシステム構成の設計どおりにしなければならない。このことを実現するためには、構築したシステムについて、以下の点からの確認を徹底しなければならない。

- ゾーン構成およびゾーン間の通信制御における要求の確実な反映
- 各ゾーンへのサービスの配置の妥当性
- サーバへのサービスの配置の妥当性
- 各ゾーンへの DB の配置の妥当性
- サーバへの DB の配置の妥当性
- 通信制御ツールの配置と設定機能の妥当性
- ウイルス対策ソフトの配置と配置場所の妥当性
- 監視ツールの配置と設定機能の妥当性
- 性能対策への対応状況
- －各機器の性能･容量の妥当性、負荷分散や過負荷発生時への対策
- システム障害発生時の影響の局所化や情報の回復やシステムの復旧に必要な機器等の配

置

(2) 環境の変化への的確な対応の迅速な実施

システム構成面での変更やセキュリティ対策の変更等のセキュリティ面での環境変化は、頻繁に発生する。システムの構成は、これらの変化に適切に対応し、システムの構成に求められているセキュリティ対策面からの要求を常に満たすようにしておかねばならない。このことを実現するためには、異化が必要となる。

- システムの構成をセキュリティ面からも的確なものとして維持するための仕組みの確立
  - ・メンテナンスが必要な事態の明確化
  - ・システム構成の的確性の維持に必要な活動の明確化
    - ―日常オペレーションへの要求の明確化
    - ―メンテナンス実施の必要性の把握方法の確立
    - ―メンテナンスの実施要領の確立
- 必要事項の日常のオペレーションへの反映
- 日常のオペレーションに要求されることの的確な実施
- メンテナンスが必要な事態の発生についてのチェックの実施
- 必要な時点でのメンテナンスの適切な実施
  - ・遅滞のないメンテナンスの実施
  - ・的確なメンテナンスの実施(実施前のレビュー、事後の確認の徹底他)
- システム構成についての定期的な妥当性チェックの実施

  システム構成の維持管理に努めていても、万全は期待できない。システム構成の維持管理の不手際が見逃されたままにしないためには、システムの構成についてセキュリティ面からの妥当性チェックを定期的に行うことも必要である。

【対応 ISMS コントロール】

ISMS に、本要求に明示的に対応する要求はない。

3.3.2. ソフトウェアの管理の徹底

Tc2.1	OS 等のプラットフォーム系ソフトに対する管理ルールとルールの沿った導入・変更・管理の実施

【主旨】

OS 等のプラットフォーム系のソフトはシステムの円滑の稼働の要であるため、これらの使用の適切性の確保は重要である。OS 等のプラットフォーム系のソフトの使用にあたっては、

- 適切な製品の適切な使用
- 使用にあたってのライセンス違反等のルール違反の防止
- 問題が生じた場合の対処の容易性の確保

の実現が求められる。

適切な製品の適切な使用とは、使用目的に合った製品やバージョンの選択と、使用機能の適切な選択と、それらの的確なインストールに加え、有害コードを含む恐れのあるプログラムの導入の排除を実現するものである。

【対策のポイント】

(1) プラットフォーム系ソフトの管理の仕組みの確立

適切な管理の実現のためには、まず、プラットフォーム系ソフトを対象とした管理の仕組みを確立しておくことが必要となる。この管理の仕組みとして検討すべきこととしては、表 3-38 に示すようなものがある。

表 3-38　プラットフォーム系ソフトの管理の仕組みとして検討すべき事項

指定項目	指定内容
基本方針	・管理の狙い 　－もっともふさわしい製品の利用場面に最適な使用 　－契約に沿った使用 ・管理のポイント 　－使用するソフトの選択や調達先 　－保有状況ならびに使用状況の的確な把握 　－ルールに沿った使用
責任体制	・管理についての責任者 ・利用者の責任
導入ソフトウエアの決定プロセス	・提案・審査・決定の流れ ・提案要領（様式、必要事項の記入要領等） ・審査要領（審査事項、審査のポイント） ・承認手続き（承認責任者や審査の流れ）
インストールの実施手順 （インストールの計画・レビュー・テスト・インストールの流れと進め方）	・計画要領 ・レビュー要領（レビュー事項、レビューのポイント） ・テスト要領（要確認事項、テスト方法、テストの体制、） ・インストールと切り替え要領 　－運用環境へのインストール手順 　－切り替えの手順 　－切り替え後の内容と確認方法 　－異常時の対処要領 ・事後の確認要領
保有ソフトのチェック要領	・把握項目（保有製品ごとの調達先、調達日、調達手段、使用状況他） ・チェック項目（保有ソフトの棚卸と管理台帳との照合、保有の妥当性） ・チェックのタイミング（定期チェックのサイクル、臨時チェックを必要とする事態） ・チェック結果の報告 ・問題点に対する対処要領
使用中のソフトのチェック要領	・チェック項目 　－実装ソフトと実装管理台帳との照合 　－インストール仕様の妥当性 　－ライセンスへの準拠 ・チェックのタイミング（定期チェックのサイクル、臨時チェックを必要とする事態） ・チェック結果の報告 ・問題点に対する対処要領

(2) ルールに沿ったプラットフォーム系ソフトの導入

- ルールに沿った導入ソフトウェアの決定

適切なソフトウェアの選択を行うとともに、有害なコードが含まれている可能性のあるソフトウェアの導入を避けるためには、ソフトウェアの導入は定められた手順に沿って以下が適切に行われなければならない。導入決定プロセスで重要なポイントとしては、以下があげられる。

・導入計画の明確化とその審査
(導入製品、必要性、適用範囲、使用開始時期、切り替え方法他)
・対象ソフトとその使用法についての審査
(提供元、仕様、使用法等の妥当性、安全性の確認、切り替えの方法)
・指定された手続きを経た承認

- ルールに沿ったインストール

導入ソフトのインストールにあたっても、定められた手順に沿って、以下が適切に行われなければならない。

・諸設定等使用法の事前レビューの実施
・実施可否の判断の実施
・インストール後の異常がないかどうかの確認の実施
・インストールに関する記録の確保

(3) ルールに沿った切替えの実施

使用ソフトのバージョンアップや他の製品への切替えの不手際で事故を起さないためには、プラットフォーム系ソフトの変更に際しては、以下がルールに沿って適切に行われなければならない。

- 変更内容についての事前レビューの実施
- 変更実施可否の判断の実施
- 変更後の異常がないかどうかの確認の実施
- 変更に関する記録の確保

(4) ルールに沿った保有状況のチェックの実施

(5) ルールに沿った使用状況のチェックの実施

【対応 ISMS コントロール】

10.4.1 運用ソフトウェアの管理
10.4.3 プログラムソースライブラリへのアクセス制御
10.5.1 変更管理手順
10.5.2 オペレーティングシステムの変更の技術的レビュー

Tc2.2	オフィスツール等の汎用業務ツール系のソフトに対する管理ルールとルールの沿った導入･変更･管理の実施

【主旨】

文書作成ソフトや表計算ソフトやメール等の業務現場が日常的に用いる汎用ツール系のソフトの使用にあたっては、

- 適切な製品の適切な使用
- 使用にあたってのライセンス違反等のルール違反の防止
- 問題が生じた場合の対処の容易性の確保

の実現が求められる。これらを実現し、これらのソフトの使用上で問題を起さないためには、その使用についての適切な管理も欠かせない。

ここでいう適切な製品の適切な使用とは、使用目的に合った製品やバージョンの選択と、使用する機能の選択と、それらの適切なインストールに加え、有害コードを含む恐れのあるプログラムの導入がないようにすることを言う。

【対策のポイント】

(1) 汎用業務ツール系ソフトの管理の仕組みの確立

適切な管理の実現のためには、まず、汎用業務ツール系ソフトを対象とした管理の仕組みを確立しておくことが必要となる。この管理の仕組みとして検討すべきこととしては、表 3-39 に示すようなものがある。

表 3-39 汎用業務系ソフトの管理の仕組みとして検討すべき事項

指定項目	指定内容
基本方針	･管理の狙い －もっともふさわしい製品の利用場面に最適な使用 －契約に沿った使用 ･管理のポイント －使用するソフトの選択や調達先 －保有状況ならびに使用状況の的確な把握 －ルールに沿った使用
責任体制	･管理についての責任者 ･利用者の責任
導入ソフトウエアの決定プロセス	･提案･審査･決定の流れ ･提案要領（様式、必要事項の記入要領等） ･審査要領（審査事項、審査のポイント） ･承認手続き（承認責任者や審査の流れ）
インストールの実施手順 （インストールの計画･レビュー･テスト･インストールの流れと進め方）	･計画要領 ･レビュー要領（レビュー事項、レビューのポイント） ･テスト要領（要確認事項、テスト方法、テストの体制、） ･インストールと切り替え要領 －運用環境へのインストール手順 －切り替えの手順 －切り替え後の内容と確認方法 －異常時の対処要領 ･事後の確認要領

保有ソフトのチェック要領	・把握項目（保有製品ごとの調達先、調達日、調達手段、使用状況他） ・チェック項目（保有ソフトの棚卸と管理台帳との照合、保有の妥当性） ・チェックのタイミング（定期チェックのサイクル、臨時チェックを必要とする事態） ・チェック結果の報告 ・問題点に対する対処要領
使用中のソフトのチェック要領	・チェック項目 　－実装ソフトと実装管理台帳との照合 　－インストール仕様の妥当性 　－ライセンスへの準拠 ・チェックのタイミング（定期チェックのサイクル、臨時チェックを必要とする事態） ・チェック結果の報告 ・問題点に対する対処要領

（2）ルールに沿った汎用業務ツール系ソフトの導入

● ルールに沿った導入ソフトウェアの決定

適切なソフトウェアの選択を行うとともに、有害なコードが含まれている可能性のあるソフトウェアの導入を避けるためには、ソフトウェアの導入は定められた手順に沿って以下が適切に行われなければならない。導入決定プロセスで重要なポイントとしては、以下があげられる。

・導入計画の明確化とその審査

（導入製品、必要性、適用範囲、使用開始時期、切り替え方法他）

・対象ソフトとその使用法についての審査

（提供元、仕様、使用法等の妥当性、安全性の確認、切り替えの方法）

・指定された手続きを経た承認

● ルールに沿ったインストール

導入ソフトのインストールにあたっても、定められた手順に沿って、以下が適切に行われなければならない。

・諸設定等使用法の事前レビューの実施

・実施可否の判断の実施

・インストール後の異常がないかどうかの確認の実施

・インストールに関する記録の確保

（3）ルールに沿った切替えの実施

使用ソフトのバージョンアップや他の製品への切替えの不手際で事故を起さないためには、業務系汎用ソフトのソフトの変更に際しては、以下がルールに沿って適切に行われなければならない。

● 変更内容についての事前レビューの実施
● 変更実施可否の判断の実施
● 変更後の異常がないかどうかの確認の実施
● 変更に関する記録の確保

（4）ルールに沿った保有状況のチェックの実施

（5）ルールに沿った使用状況のチェックの実施

【対応 ISMS コントロール】

10.4.1 運用ソフトウェアの管理
10.4.3 プログラムソースライブラリへのアクセス制御
10.5.1 変更管理手順
10.5.3 パッケージソフトウェアの変更に対する制限

Tc2.3	(個別) 業務ソフトに対する管理ルールとルールの沿った導入・変更・管理の実施

【主旨】

ここで言う(個別)業務ソフトとは、各組織が独自に開発した業務ソフトに加え、導入した業務システムのパッケージソフト、またはカスタマイズして使用する業務システムのパッケージソフトを言う。事業を支える業務処理を行うシステムに固有の業務ソフトは、事業活動の要であるため、これらの使用の適切性の確保は重要である。汎用業務ツール系のソフトの使用にあたっては、

- 適切な製品の適切な使用
- 不適切なカスタマイズの防止
- 使用に当たってのライセンス違反等のルール違反の防止
- 問題が生じた場合の対処の容易性の確保

の実現が求められる。適切な製品の適切な使用とは、使用目的に合った製品やバージョンの選択と、その適切なインストールに加え、有害コードを含む恐れのあるプログラムの導入の排除を実現するものである。

【対策のポイント】

(1) 業務ソフトの管理の仕組みの確立

適切な管理の実現のためには、まず、業務ソフトを対象とした管理の仕組みを確立しておくことが必要となる。この管理の仕組みとして指定すべきこととしては、表 3-40 に示すようなものがある。

表 3-40 個別業務ソフトの管理の仕組みとして指定すべき事項

指定項目	指定内容
基本方針	・管理の狙い 　－もっともふさわしい製品の利用場面に最適な使用 　－契約に沿った使用 ・管理のポイント 　－使用するソフトの選択や調達先 　－保有状況ならびに使用状況の的確な把握 　－ルールに沿った使用
責任体制	・管理についての責任者 ・利用者の責任
導入ソフトウエアの決定プロセス	・提案・審査・決定の流れ ・提案要領(様式、必要事項の記入要領等) ・審査要領(審査事項、審査のポイント)

	･承認手続き（承認責任者や審査の流れ）
パッケージソフトに対する カスタマイズの実施要領	･カスタマイズの内容とその必要性の明確化とその審査要領 ･カスタマイズについての提供元との連携要領 ･カスタマイズ仕様のレビュー要領 ･カスタマイズにかかわるシステムテストの実施要領 ･カスタマイズにかかわる記録の作成と保管要領
変更要領	･仕様変更他の変更内容とその必要性の明確化とその審査要領 ･変更仕様や他への影響についてのレビュー要領 ･変更部分ならびに変更にかかわるシステムテストの実施要領 ･変更にかかわる記録の作成と保管要領

(2) ルールに沿った業務ソフトの導入

- ルールに沿った導入ソフトウェアの決定

適切なソフトウェアの選択を行うとともに、有害なコードが含まれている可能性のあるソフトウェアの導入を避けるためには、ソフトウェアの導入は定められた手順に沿って以下が適切に行われなければならない。導入決定プロセスで重要なポイントとしては、以下があげられる。

･導入計画の明確化とその審査
（導入製品、必要性、適用範囲、使用開始時期、切り替え方法他）
･対象ソフトとその使用法についての審査
（提供元、仕様、使用法等の妥当性、安全性の確認、切り替えの方法）
･指定された手続きを経た承認

- ルールに沿ったインストール

導入ソフトのインストールにあたっても、定められた手順に沿って、以下が適切に行われなければならない。

･諸設定等使用法の事前レビューの実施
･実施可否の判断の実施
･インストール後の異常がないかどうかの確認の実施
･インストールに関する記録の確保

(3) パッケージソフトに対するカスタマイズの慎重な実施

業務にパッケージソフトを用いる場合、なにがしかのカスタマイズが行われるのが一般である。パッケージソフトのカスタマイズは、自社開発ソフトの変更に比べ不手際を起こし易い。また、ソフトウェアの著作権上の問題もかかわる場合がある。このため、汎用パッケージのカスタマイズにあたっては、提供元との密接な連携の下、慎重に行われなければならない。

汎用パッケージのカスタマイズが必要な場合は、以下が適切に行われなければならない。

- カスタマイズの内容とその必要性の明確化とその審査
- カスタマイズについての提供元との連携
- カスタマイズ仕様のレビュー要領･カスタマイズにかかわるシステムテストの実施
- カスタマイズにかかわる記録の作成と保管

(4) ルールに沿った変更の実施

部分的な仕様変更やバージョンアップ等によるソフトの変更の不手際で事故を起さないためには、業務ソフトのソフトの変更に際しては、以下がルールに沿って適切に行われなければならな

い。

- 変更内容についての事前レビューの実施
- 変更実施可否の判断の実施
- 変更後の異常がないかどうかの確認の実施
- 変更に関する記録の確保

【対応 ISMS コントロール】

10.4.1 運用ソフトウェアの管理
10.4.3 プログラムソースライブラリへのアクセス制御
10.5.1 変更管理手順

3.3.3. 個々の機器における自衛策の実施

Tc3.1	ネットワーク制御機器におけるセキュリティ対策

【主旨】

ネットワーク制御機器自体に脆弱性が残されていると、この脆弱性をつかれた攻撃により、システム全体のセキュリティ対策に穴があきかねない。このため、システム構成機器としてのネットワーク制御機器としてのルータ、ファイアウォール、プロキシ等に、脆弱性が残されないようにしなければならない。特に、ネットワーク制御機器は、不正アクセスの最前線に置かれるため、この点は重要となる。

このことを実現するためには、ネットワーク制御機器に対する脆弱性の除去という観点での管理の仕組みの確立と、個々のネットワーク制御機器に対する脆弱性の排除の努力が必要となる。

【対策のポイント】

(1) ネットワーク制御機器に対し対策が必要となる脆弱性の明確化

ネットワーク制御機器から脆弱性を完全に排除するためには、そのベースとして以下のようなことが明確にされていなければならない。

- ネットワーク機器それぞれの構造面から排除しなければならない脆弱性の認識
- 排除の対象となる脆弱性の摘出方法
- 排除の方法

ネットワーク機器における排除すべき代表的な脆弱性を、表 3-41 に示す。

表 3-41 ネットワーク機器における排除すべき代表的な脆弱性

対象機器	排除すべき脆弱性の代表例
ルータ	・危険なポート(Telnet、SSH、FTP 他)の開放 ・アクセス制御の不備(本来許可しないネットワークへのアクセスの許可) ・ファームウエアに存在する脆弱性 (OSPF の処理に起因するサービス妨害に対する脆弱性、SNMP の処理に起因する

	サービス妨害に対する脆弱性他)
ファイアウォール	・危険なポート(Telnet、SSH、FTP 他)の開放 ・アクセス制御の不備(本来許可しないネットワークへのアクセスの許可) ・ファームウエアに存在する脆弱性 (FiareWall-1 におけるsyslog の処理に起因するサービス妨害に対する脆弱性、他)
プロキシ	・危険なポート(Telnet、SSH、FTP 他)の開放 ・アクセス制御の不備(本来許可しないネットワークへのアクセスの許可) ・アプリケーション部分に存在する脆弱性 (squid LDAP 認証ルーチンの不具合に起因する認証バイパスの可能性、suid NTLM 認証ルーチンの不具合に起因するバッファーオーバーフロー脆弱性他)

(2)ネットワーク制御機器に対する脆弱性対策実施要領の確立

ネットワーク制御機器に対する脆弱性対策は適切に行われるためには、対策実施要領の確立も必要となる。ネットワーク制御機器に対する脆弱性対策実施要領の中で指定すべき事項としては、以下のようなものがある。

- 対象機器
- 対象機器ごとの脆弱性検査・除去の実施サイクル
- 対象機器ごとの脆弱性検査・除去として実施すべきチェックと実施手順
- 結果の記録と報告の方法

(3)ルールに沿ったネットワーク制御機器に対する脆弱性対策の実施

ネットワーク制御機器に対する脆弱性対策は、指定された実施サイクルごとに、定められた検査を行わなければならない。このような脆弱性は、インストールや日々のシステムの管理面でのセキュリティ要求が確実に実践されていれば、入り込まないはずのものである。このため、この検査で脆弱性が発見された場合は、脆弱性が入り込んだ原因の調査を行い、必要な是正措置をとらなければならない。

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

Tc3.2 サーバにおけるセキュリティ対策

【主旨】

システムの処理の中核を担うサーバ自体に脆弱性が残されていると、この脆弱性をつかれた攻撃により、システム全体のセキュリティ対策に穴があきかねない。このため、システムの主要構成機器としてのサーバには脆弱性が残されないようにしなければならない。

すべてのサーバに脆弱性が残されないようにするためには、サーバに対する脆弱性の除去という観点での管理の仕組みの確立と、すべてのサーバにネットワーク制御機器に対する脆弱性の排除の努力が必要となる。

【対策のポイント】

(1) サーバに対し対策が必要となる脆弱性の明確化

サーバから脆弱性を完全に排除するためには、そのベースとして以下のようなことが明確にされていなければならない。

- サーバの構造面から排除しなければならない脆弱性の認識
- 排除の対象となる脆弱性の摘出方法
- 排除の方法

サーバから排除すべき脆弱性の代表的なものを、表 3-42 に示す。

表 3-42　サーバから排除すべき代表的な脆弱性

指定項目	指定内容
OS 部分	・デフォルト設定による不要プロセスの稼動 ・不要なアカウントの存在 　－長期間ログインしていないアカウント 　－テスト用のアカウント 　－退職者等資格喪失者に付与していたアカウント ・脆弱なパスワードの使用 ・セキュリティパッチの未適用セキュリティホールの存在 ・デフォルト設定のままでの運用 　(r 系サービスや RPC プログラム等の脆弱性が多く確認されているサービスを放置する運用) ・不要なポートの開放
Web サーバ	・セキュリティパッチの未適用セキュリティホールの存在 ・不要なメソッド(機能)の有効化 ・独自開発の CGI による OS/SQL インジェクションやクロスサイトスクリプト脆弱性
DNS サーバ	・セキュリティパッチの未適用セキュリティホールの存在 ・ゾーン転送のアクセス制御の不備 ・再帰的問合わせの許可範囲の不備

(2) サーバに対する脆弱性対策実施要領の確立

サーバに対する脆弱性対策は適切に行われるためには、対策実施要領の確立も必要となる。サーバに対する脆弱性対策実施要領の中で指定すべき事項としては、以下のようなものがある。

- 対象サーバの脆弱性管理単位へグルーピング

  サーバのネットワーク上の位置によってリスクはことなる。このため、脆弱性対策のレベルは、ネットワーク上の位置によって差をつけることもできる。このグルーピングは、実効的な対策の効率用行うための工夫の一つであり、
- 管理単位サーバ群ごとの脆弱性検査･除去の実施サイクル
- 対象機器ごとの脆弱性検査･除去として実施すべきチェックと実施手順
- 結果の記録と報告の方法

(3) ルールに沿ったサーバに対する脆弱性対策の実施

サーバに対する脆弱性対策は、指定された実施サイクルごとに、定められた検査を行わなければならない。このような脆弱性は、インストールや日々のシステムの管理面でのセキュリティ要求が確実に実践されていれば、入り込まないはずのものである。このため、この検査で脆弱性が発見された場合は、脆弱性が入り込んだ原因の調査を行い、必要な是正措置をとらなければならない。

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

Tc3.3 LAN 上のクライアント PC に対するセキュリティ対策

【主旨】

LAN 上のクライアント PC 自体に脆弱性が残されていると、この脆弱性をつかれた攻撃により、システム全体のセキュリティ対策に穴があきかねない。このため、LAN 上のクライアント PC に対してもサーバと同様に、脆弱性が残されないようにしなければならない。

LAN 上のクライアント PC のすべてに脆弱性が残されないようにするためには、LAN 上のクライアント PC に対する脆弱性の除去という観点での管理の仕組みの確立と、すべての LAN 上のクライアント PC にネットワーク制御機器に対する脆弱性の排除の努力が必要となる。

【対策のポイント】

(1) LAN 上のクライアント PC に対し対策が必要となる脆弱性の明確化

LAN 上のクライアント PC から脆弱性を完全に排除するためには、そのベースとして以下のようなことが明確にされていなければならない。

- LAN 上のクライアント PC の構造面から排除しなければならない脆弱性の認識
- 排除の対象となる脆弱性の摘出方法
- 排除の方法

LAN 上のクライアント PC から排除すべき脆弱性の代表的なものを、表 3-43 に示す。

表 3-43 LAN 上のクライアント PC から排除すべき代表的な脆弱性

指定項目	指定内容
Windows クライアント	・不要なポートの開放 (ftp、http、https 等) ・セキュリティパッチの未適用セキュリティホールの存在 ・不要なアカウントの存在 　－長期間ログインしていないアカウント 　－プログラムが自動的に設定したアカウント ・不要な共有フォルダの存在 　－以前に使用されたものが放置されているフォルダ 　－アクセス制限がかけられていないフォルダ ・ローカルセキュリティ (グループ) ポリシーの不備 　(パスワードの強度やロックアウトにかかわる設定等)

(2) LAN 上のクライアント PC に対する脆弱性対策実施要領の確立

LAN 上のクライアント PC に対する脆弱性対策は適切に行われるためには、対策実施要領の確立も必要となる。LAN 上のクライアント PC に対する脆弱性対策実施要領の中で指定すべき事項としては、以下のようなものがある。

- 対象クライアントPCの脆弱性管理単位へグルーピング
  クライアントPCのネットワーク上の位置によってリスクはことなる。このため、脆弱性対策のレベルは、ネットワーク上の位置によって差をつけることもできる。このグルーピングは、実効的な対策の効率用行うための工夫の一つであり、必須ではない。すべてのクライアントに同じ対策を講じてもよういが、規模の大きなシステムは困難が伴う。
- 管理単位クライアントPC群ごとの脆弱性検査･除去の実施サイクル
- 対象機器ごとの脆弱性検査･除去として実施すべきチェックと実施手順
- 結果の記録と報告の方法

(3)ルールに沿ったサーバに対する脆弱性対策の実施

LAN上のクライアントPCに対する脆弱性対策は、指定された実施サイクルごとに、定められた検査を行わなければならない。このような脆弱性は、インストールや日々のシステムの管理面でのセキュリティ要求が確実に実践されていれば、入り込まないはずのものである。このため、この検査で脆弱性が発見された場合は、脆弱性が入り込んだ原因の調査を行い、必要な是正措置をとらなければならない。

【対応ISMSコントロール】

ISMSには、本要求に明示的に対応する要求はない。

3.3.4. セキュアなアプリケーションソフトの開発

Tc4.1	アプリケーションソフトへの必要なセキュリティ機能の組込み

【主旨】

アプリケーションソフトには、対象業務や処理方式の特性から必要となる情報セキュリティにかかわる機能が的確に組み込まれていなければならない。検討の対象となるものとしては、一般に以下のようなものがある。

- 入力チェック機能
- 出力の検証機能
- ユーザ識別･認証機能
- 機能や情報へのアクセス制御機能
- アクセスや処理のログ取得機能
- 障害対策機能
- 性能対策機能

個々のアプリケーションソフトに、これらが必要に応じて適切に組み込まれるようにするためには、設計や実装でこれらに不備が出ないようにするための工夫も必要となる。

【対策のポイント】

(1) セキュリティ設計ルールの確立

アプリケーションの開発において、セキュリティ面での設計が抜けないようにするためには、これらに対する設計基準を示したり、設計レビューのチェック項目に入れておく等の、セキュリティ設計上のルールを確立しておくことも必要となる。

アプリケーション開発におけるセキュリティ設計についてのルールとして検討すべき事項としては、以下のようなものがある。、

- 設計の対象となるシステムの概要、他システムとの関係等の明確化
- 開発アプリケーションのセキュリティ環境の定義方法
  - ・セキュリティ面での考慮すべき前提
  - ・想定されるセキュリティ上の脅威
  - ・対象アプリケーションを利用する組織のセキュリティポリシー
- 対象システムで達成すべきセキュリティ目標の設定方法
- 対象アプリケーションが具備すべきセキュリティ要件の定義方法
- アプリケーションにおけるセキュリティ仕様の作成ルール
- セキュリティ仕様の評価ルール
  - ・チェックポイント
  - ・チェックの進め方

(2) 設計レビューにおけるセキュリティ面からのチェックの実施

セキュリティ機能については、以下の観点について、要求されるセキュリティレベルに応じた十分性のチェックが必要である。

- セキュリティに対する監査
- 受信側、発信側の否認防止
- 利用者データの保護
- 識別と認証
- プライバシー保護
- セキュリティ機能の保護
- 資源の利用の管理
- 対象システムへのアクセスの管理
- セキュアな通信
- 暗号の管理
- セキュリティ機能の管理

(3) 開発ソフトに対するセキュリティ検査の実施

セキュリティ検査においては、要求されるセキュリティレベルに応じたテスト計画を作成し、テスト計画に基づき実施しなければならない。その際、以下を考慮することが必要である。

- セキュリティ要求事項を網羅してテストケースを設定して実施
- テストデータの作成はテスト計画に基づき実施
- セキュリティテストは本番環境と隔離した環境で実施

- セキュリティテストは開発当事者以外の者が参画
- 適切なテスト手法、可能であれば標準手法を使用
- テストの経過及び結果を記録及び保管

【対応 ISMS コントロール】

10.1.1 セキュリティ要求事項の分析および明示

Tc4.2	アプリケーションソフトからの脆弱性の排除

【主旨】

アプリケーションソフトは、その構造上の問題から、セキュリティ事故を招く脆弱点を持ち易いところが少なくない。アプリケーションソフトにおけるこのような欠陥をついた攻撃による事故も多く報告されている。

このため、アプリケーションソフトにこのような脆弱性が見逃されないようにすることも、外部からの攻撃を防ぐためには大きな要素となる。

【対策のポイント】

(1) 開発環境ごとの脆弱性チェックリストの作成

開発ソフトに脆弱性が残されないようにするためには、開発環境ごとに、留意すべきところを示したチェックリストの確立が欠かせない。対象とすべき開発環境と、おもな留意点を、表 3-44 に示す。

表 3-44 アプリケーションの開発におけるセキュリティ面での留意点

対象領域		留意点
Web アプリケーション	データベース	データベースアクセス環境において陥りやすい脆弱性
	Java	Java 使用時の陥りやすい脆弱性
	Perl	Perl 使用時の陥りやすい脆弱性
	VBScript/ASP	VBScript/ASP 使用時の陥りやすい脆弱性
	画面設計	Web ページ設計での陥りやすい脆弱性
	セッション実装	セッション管理実装において陥りやすい脆弱性
	SSL の使用	SSL の使用において陥りやすい脆弱性
	万一への備え	さらに安全性を高めるために要求されること
	その他	一般的に Web アプリで脆弱性
その他のアプリケーション	C／C＋＋	C／C＋＋使用時の陥りやすい脆弱性
	Unix／Linux	Unix／Linux上で動作するプログラムに対する脆弱性
	Windows	Windows上で動作するプログラムに対する脆弱性
	セキュアな実装方法	一般的にプログラミングで脆弱性

(2) 開発者への脆弱性対策の徹底

開発者に脆弱性対策を徹底するためには以下が必要である。

- 開発者への脆弱性対策教育実施による、脆弱性に対する理解と必要な対応の実践の徹底

- 開発者が随時チェックリストを参照できる環境の整備

(3) 脆弱性対策実施の確認

チェックリストで示された対策が確実に行われていることの確認が確実に行われるようにするためには、以下も必要となる。

- 設計上での対策の明示
- テストでの確認とテスト結果の記録と保管

(4) 新しい脅威が報告された場合におけるアプリケーションソフトの見直しの実施

開発時点でのアプリケーションソフトにおける脆弱性対策は、貴地の脆弱点に対してのみしか行われないため、新たに報告された脆弱点については対策されてないと考えるのが妥当である。このため、新しい脅威が報告された場合は、当該脆弱点がかかわる既存のアプリケーションについて、問題がないかどうかを見直すことが必要となる。

この処置が適切に行われるためには、以下のようなことが求められる。

- 新しい脆弱性情報の入手方法
- 新しい脆弱性情報の入手時点における対処手順の確立
- 新しい脆弱性情報の入手時点における必要な対処の実施

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

Tc4.3	開発プロセスに対する管理の実施

【主旨】

開発過程で、不正なプログラムが組み込まれたりするようなことを排除するためには、快活過程に対するセキュリティ面からの管理も必要となる。開発過程に対するセキュリティ面からの管理のポイントとしては、以下があげられる。

- 不正コードの混入防止
- セキュリティ要求の実装の確認
- 一般品質の確保

このためには、開発プロセスの確立と、開発現場でのルールに沿った開発の実施が必要となる。

【対策のポイント】

(1) 開発プロセスの確立

開発プロセスの確立においては以下の点の考慮が必要である。

- 開発方法に基づいた開発ルールの確立
- 開発の規模、対象となるシステムのセキュリティ上の特性を考慮した開発プロセスの確立
- 開発時のリスクを評価し必要な対策を講じた開発プロセスの確立

- 開発する対象のセキュリティレベルに応じた開発環境の構築

(2) 開発現場でのルールに沿った開発の徹底

開発現場での開発ルールに則った開発の実施の徹底ためには以下が必要である。

- 開発ルールについての開発者への教育を通じた実践の徹底
- 開発プロセス遵守状況のチェックの実施

(3) ソフトウェア開発の外部委託に対するセキュリティ対策

ソフトウェアの開発を外部に委託する場合は、開発したソフトにセキュリティ面での問題がないようにするとともに、開発過程における情報の漏洩の防止等の開発を外部への委託することにともなう以下に示すようなセキュリティ対策が必要となる。

- セキュリティ面からのシステム開発委託の手続きの確立
- 委託する開発のタイプごとのセキュリティに関する要求の明確化
- 規程に沿った開発委託先の審査と決定
  - ・定められた審査の実施
    - ―資格審査
    - ―セキュリティ面での要求に対する対応能力
  - ・定められた手続きに沿った決定
- 開発委託先ごとのセキュリティ面での双方の責任の明確化
  - ・双方の責任の明確化と合意の形成
  - ・セキュリティ要求事項の実践方法についての合意の形成
  - ・契約等でのそれぞれの責任の明文化
- 開発委託先ごとのセキュリティ要求への対応状況のチェックと必要な指導の実施
  - ・チェックの方法の確立と双方の合意の形成
  - ・チェックと評価の実施
  - ・問題点の是正処置への展開
  - ・委託先との継続的なコミュニケーションの確保
- 外部に開発を委託したソフトに対するセキュリティ検査の実施

【対応 ISMS コントロール】

10.1.1 セキュリティ要求事項の分析および明示
10.5.4 隠れチャネルおよびトロイに木馬
10.5.5 外部委託によるソフトウェアの開発

3.3.5. システム運用上のセキュリティ対策

Tc5.1	セキュアなシステム運用を実現するための管理の仕組みの確立

【主旨】

セキュリティ対策の実践は、システム運用に依存しているところも少なくない。セキュリティ対策がシステムの運用に要求していることを確実に実施するだけでなく、日常的なシステム運用でセキュリティ事故につながるような不手際を起さないようにするためには、セキュアなシステム運用を追求するための仕組みも必要となる。

セキュアなシステム運用を実現するための管理の仕組み確立して、実施すべき事項としては、以下があげられる。

- システム運用に対するセキュリティ要求の明確化
- システムテム運用職場での職務遂行にかかるセキュリティ要求の明確化
- システム運用規程、システム運用･操作マニュアルへのセキュリティ要求の反映
- システム運用上でのセキュリティ要求の実践を管理できる仕組みの確立

【対策のポイント】

(1) システム運用に対するセキュリティ要求の明確化

システム運用に対するセキュリティ要求として明確にすべき事項としては、以下のようなものがある。

- ジョブの実行にかかる要求の明確化
- セキュリティ対策にかかるシステム運用についての要求
- デジタル情報の保管についての要求
- 情報の取扱いについての要求
- 運用上のトラブルへの対応についての要求
- システム運用の記録の取得についての要求

(2) システムテム運用職場での職務遂行にかかるセキュリティ要求の明確化

システムテム運用職場での職務遂行にかかるセキュリティ要求として明確にすべき事項としては、以下のようなものがある。

- 保護資産と保護要件の明確化
- セキュリティ要求事項の実践についての基本方針の明確化

  ―職務の分離、職場の物理的な分離、情報の取扱いおよび保護等についての基本方針
- 関係者のの資格

  ･関係者に対する職務の遂行ならびに職場での行動に対する管理についての基本方針

(3) システム運用規程、システム運用･操作マニュアルへのセキュリティ要求の反映

- システム運用･操作マニュアルへのセキュリティ要求事項の反映

- システム運用規程、システム運用･操作マニュアルの妥当性の維持
  ･システム運用環境やセキュリティ対策に変更が生じた場合のこれらの見直しと必要な修正の実施
  ･定期的な妥当性チェックの実施

(4) システム運用上でのセキュリティ要求の実践を管理できる仕組みの確立

システム運用上でのセキュリティ要求の実践を管理できる仕組みに関し検討すべき事項としては、以下のようなものがある。

- 責任体制の確立
- 関係者への情報セキュリティにかかる責務の明確化
- 必要に応じた職務の分離
  ･職務の分離
  ･必要に応じた職場の物理的な分離
    －職場単位の
- セキュリティ要求事項の遵守をチェックする仕組みの確立
  ･対象職場ごとのチェック要領の確立
    －実施サイクル、チェック事項、チェックの方法、評価と報告
  ･対象職場ごとのチェックリストの作成

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

Tc5.2	日々のシステム運用におけるセキュリティ要求の実践

【主旨】

日々のシステム運用におけるセキュリティ要求は、以下の要素から構成される。

- 当日に予定された業務処理の実行
- セキュリティ対策にかかわるシステム運用の実行
- 行処理ならびにセキュリティにかかわるシステム運用の記録の作成

これらを的確に行うためには、システム運用関係者における常日頃の情報セキュリティについての意識の確立と、要求事項の実践についてのチェックと指導が必要となる。

【対策のポイント】

(1) システム運用関係者へのセキュリティ要求の実践についての意識の醸成

(2) 的確なシステム運用計画の作成

的確なシステム運用を実現するためには、まず、日々のシステム運用で実行すべきジョブの計画が的確なものとして作成されなければならない。日々のシステム運用計画の作成を的確なものにするためには、以下が必要となる。

● システム運用計画作成要領の確立

システム運用計画作成要領で明確にすべき事項としては、表 3-45 に示すようなものがあげられる。

表 3-45　システム運用計画策要領で明示すべき事項

区分	明確にすべき事項
当日の運用スケジュール	･実行すべき業務処理とその実行条件 ･実行すべきセキュリティ対策関連処理とその実行条件 ･システムの立上げから終了までのジョブスケジューリング ･その他の留意事項
運用計画の作成承認手続き	･作成手続き ･承認手続き
その他	･使用ツール ･使用文書の様式

● 規定に沿った運用計画の作成とチェック

日々のシステム運用計画は作成要領の指定にもとづき作成、承認されなければならない。この作成や承認の過程で、不手際が発見できるようにならなければならない。

(3) 運用計画に沿った確実なシステム運用の実践

システムの運用を確実なものにするためには、以下のような工夫も必要となる。

● ジョブ管理ツール等のツールの有効な活用による実行上のミスの排除
● 処理結果についての指定された確認の確実な実施
● 運用要領に沿ったシステム運用についての報告の実施
● 日々のシステム運用に対するチェックの実施

このチェックを有効なものにするためには、計画時に作成したチェックリストを用いるようなシステムを確立しておくことも必要な工夫である。

(4) セキュリティ対策にかかわる運用の記録の作成と保管

事後に何か問題が生じた場合における必要な対応を、迅速かつ適切に行うためには、システムの運用についての記録の作成とその適切な保管も欠かせない。これらを適切に行うためには、以下が必要となる。

● システムの運用にかかわる記録の作成･保管要領の確立

システム運用にかかわる記録の作成･保管要領として明確にすべき事項を表 3-46 に示す。

表 3-46　システムの運用にかかわる記録の作成･保管要領で明示すべき事項

区分	明確にすべき事項
作成すべき記録の内容	･業務処理についての記録すべき事項とその様式 ･セキュリティ対策に関わる処理について記録すべき事項とその様式 ･運用上のトラブルとその対処について記録すべき事項とその様式 ･運用上で遭遇したセキュリティインシデンツについて記録すべき事項とその様式
記録の作成･承認要領	･作成者 ･承認者と承認の手続き
保管要領	･保管期間 ･保管形態､保管場所、保管責任者 ･保管の手続き

(2)　ルールに沿ったシステムの運用にかかわる記録の作成と保管の実施

【対応 ISMS コントロール】

ISMS には、本要求に明示的に対応する要求はない。

Tc5.3	運用環境の保全の確保

【主旨】

システム運用における事故の要因の一つに運用環境の保全の不手際にある。運用環境の保全の不手際による事故は、その影響が小さくないため、その阻止には徹底を期さなければならない。運用環境に対する脅威としては、運用上の不手際による運用環境の破壊、運用環境保全上の処理の不手際による運用環境の破壊、開発作業での運用環境の使用による運用システムや業務データの破壊、内部の者や侵入者による運用ソフトや業務データに対する工作等があげられる。

運用環境の保全とは、これらの脅威の発生を防ぐとともに、万一、運用環境が破壊されても、迅速な回復が行えるようにしておくための施策を総称するものである。これらを適切に行うためには、

- 運用環境保全スキームの確立
- 運用環境保全スキームの沿った開発環境の分離、運用環境を開発に使う場合の開発環境の保全策の実施、運用環境へのアクセスの制限、運用環境のバックアップの確保等の的確な実施

等が必要となる。

【対策のポイント】

(1) 運用環境の保全スキームの確立

運用環境の保全は、運用環境を他の環境から確立ことが原則ではあるが、その実現方法は、システムの特性によってさまざまなものとなる。そのやり方によっては、日々の運用に多くを委ねることにもなる。このため、運用環境をどのような形で行うかを示す運用環境の保全スキームを、システムの運営形態に合った形で適切なものとして確立することが、運用環境の保全の第一歩となる。

運用環境の保全のスキームとして検討すべき事項をあげると、表 3-47 に示すようなものになる。

表 3-47 運用環境の保全スキームとして検討べき事項

区分	検討すべき事項
他の環境との物理的な隔離	･物理的な隔離の方法 ･他の環境と物理的な隔離が行われている場合における、他の環境との連携の制限
他の環境との論理的な隔離および連携	･他の環境と物理的な環境の隔離が行われていない場合における、論理的な隔離の方式
物理的なアクセスの制限	･運用環境に物理的にアクセスできる者の制限とアクセス制限の実現方法
論理的なアクセスの制限	･運用環境への論理的にアクセスができる者の制限とアクセス制限

	の実現方法
運用環境のソフト資産および情報資産の保護の方針	・他の環境との間でのソフト資産や情報資産の移動に対する管理の仕組み －ルールの確立 －ルール遵守の管理の仕組みの確立

⑵ システムの運用管理の中への運用環境の保全プロセスの組込み

運用ソフトや業務データ等の運用のベースになるものが、本来のものからずれたままでシステムの運用が続けられると、システムの処理や情報の正確性が損なわれるだけでなく、その回復は容易ならざるものとなる。運用環境が、常に、正しいものであることを保証するためには、システムの運用管理の中に、運用環境の保全プロセスが組み込まれそれが確実に実行されるようにしておかなければならない。

運用環境の保全プロセスとして特にその実行について十分な管理が必要なこととしては、表 3-48 に示すようなものがある。

表 3-48 運用環境の保全に関し特に重点的な管理が必要なシステム運用プロセス

重点管理プロセス	備考
運用環境の操作	・運用ソフトの入替え ・業務データの入替え
日々の運用開始に当たっての環境の正当性の確認	
運用環境のバックアップの取得と保管	

⑶ 運用環境の保全スキームに沿った運用環境と開発環境の分離

運用環境と開発環境の分離は、運用環境の保全の原則である。システム構成についての制約から、運用環境と開発環境の十分な分離ができない場合は、そのことからくる運用環境の保全上の脆弱性を補うだけの管理が、システムの運用や開発環境の使用に徹底されなければならない。

⑷ 運用環境へのアクセスの制限

システムの利用を除く運用環境へのアクセスは、厳重に制限されるとともに、アクセスは組織的な管理下におかれなければならない。このためには、以下のような施策が必要となる。

- 運用環境へのアクセス制限についてのルールの確立
- 運用環境へのアクセス権限者の管理の徹底
- 運用環境へのアクセス権限付与者に対する付与権限の管理の徹底
- ルールに沿った運用環境へのアクセスの制限の実施
- 運用環境に対する物理的な保護策の実施

⑸ 運用環境の操作についての管理の実施

運用環境の操作を適切に行うためには、運用環境の操作についての管理の仕組みの確立と、確立された管理の仕組みに沿った操作の実施が必要となる。

- 運用環境の保全に関わる管理の仕組みの確立

  運用環境の保全にかかわる管理の仕組みとして検討すべき事項としては、表 3-49 に示すようなものがある。

表 3-49 運用環境の保全にかかわる管理の仕組みとして検討すべき事項

区分	検討すべき事項

運用ライブラリの管理要領	・運用ライブラリの妥当性の確認要領 ・運用ライブラリの変更手続き ・運用ライブラリの変更の記録要領 ・現用運用ライブラリの内容把握要領 ・運用ライブラリの世代管理要領 ・テスト等運用以外の目的での運用ライブラリの使用の制限と必要な場合における使用要領
運用データの管理要領	・運用データの妥当性の確認要領 ・運用データの変更または運用的な操作実行の手続き ・運用データの変更の記録要領 ・現用運用データの内容把握要領 ・運用データのバックアップの管理要領 ・テスト等運用以外の目的での運用データの使用の制限と必要な場合における使用要領

● ルールに沿った運用環境の操作についての管理の実施

ルールに沿った運用環境の操作についての管理のポイントとしては、表 3-50 に示すようなものがある。

表 3-50 運用環境の操作についての管理のポイント

区分	管理のポイント
規程に沿った運用ライブラリの操作や管理の実施	・規程に沿った運用ライブラリの妥当性の確認の実施 ・規程に沿った運用ライブラリの変更の実施 ・規程に沿った運用ライブラリの変更の記録の作成と保管 ・規程に沿った運用ライブラリの世代管理の実施 ・テスト等運用以外の目的での運用ライブラリの使用の制限と必要な場合における使用の管理
規程に沿った運用データの操作や管理の実施	・規程に沿った運用データの妥当性の確認の実施 ・規程に沿った運用データの変更の実施 ・規程に沿った運用データの変更の記録の作成と保管 ・運用データのバックアップの取得と保管 ・テスト等運用以外の目的での運用データの使用の制限と使用が必要な場合における使用要領規程に沿った使用の管理

(6) サーバごとの保全策の策定とその実践

基幹業務系の運用環境の保全は前項までの施策でカバーされるが、支援業務やオフィス系システムをサポートしている各職場等に分散配置されているサーバ等における運用環境の保全については、別立ての保全策が必要となる。これらの運用環境の保全策としては以下が必要となる。

● サーバ(群)ごとの運用環境の管理要領の確立

サーバごとの運用環境の管理要領として検討すべき事項としては、表 3-51 に示すようなものがあげられる。

表 3-51 サーバ(群)ごとに指定する運用環境の管理要領で指定すべき事項

区分	指定すべき事項
サーバ(群)ごとの運用システムの保全要領の確立	・搭載ソフトの変更要領 ・搭載ソフトの使用状況についての実態把握要領 (設定機能や使用の制限等) ・バックアップの管理要領 ・搭載ソフトの変更や操作やバックアップの取得についての記録の作成と保管要領
	・搭載運用データの変更・操作要領要領

サーバ(群)ごとの運用データの管理要領	・搭載運用データの実態把握要領 ・バックアップの管理要領 ・搭載運用データの変更や操作やバックアップの取得についての記録の作成と保管要領

● サーバ単位での規程に沿った運用環境の保全の実施

サーバ単位での運用環境の保全についてのチェックポイントとしては、表 3-52 に示すようなものがあげられる。

表 3-52　サーバ単位での運用環境の保全についてのチェックポイント

区分	管理のポイント
規定に沿ったサーバ(群)ごとの運用システムの保全の実施	・規程に沿った搭載ソフトの変更の実施 ・規程に沿った搭載ソフトの使用状況の把握 ・規定に沿ったバックアップの取得と保管 ・規程に沿った搭載ソフトの変更や操作やバックアップの取得についての記録の作成と保管
規程に沿ったサーバ(群)ごとの運用データの管理の実施	・規定に沿った搭載運用データの変更と操作の実施 ・規定に沿った搭載運用データの実態の把握 ・規定に沿ったバックアップの管理の実施 ・規程に沿った搭載運用データの変更や操作やバックアップの取得についての記録の作成と保管

【対応 ISMS コントロール】

10.4.1　運用ソフトウェアの管理
10.4.2　システム試験データの保護
10.5.1　変更手順管理

Tc5.4　システムの切替えの安全の確保

【主旨】

システムの全面的な切替え時だけでなく、日常的に行われるシステム環境の変更や、アプリケーションソフトの変更における事故は、影響が小さくない。システムの変更に起因した事故の発生を防ぐとともに、万一、事故が発生しても、影響が広がる前に旧システムに戻すことができるようにしておくことも欠かせない。

本要求は、

● システムの切替えや変更における事故の防止
● システムの切替えや変更による事故発生時における、切替えあるいは変更前の状態への速やかな戻り

を実現するためのものである。

【対策のポイント】

(1) システムの切替えについての管理の仕組みの確立

システムの切替えの安全を図るためには、システムの切替えの実施についての管理の仕組みの確立が必要となる。システムの切替えについての管理の仕組みとして検討すべき事項としては、表 3-53 に示すようなものがあげられる。

表 3-53　システムの切替えについての管理の仕組みとして検討すべき事項

区分	指定すべき事項
さまざまなタイプのシステム構成の変更ごとの変更実施要領	･変更の要否の検討要領と決定の手続き ･変更計画の作成要領 　－変更の内容および実現方式の検討レビュー、承認手順 　－切替えについての課題のレビュー手順 　－切替えの実施方法についてのレビュー、承認手順 ･変更内容の的確性の確認要領 　－変更内容の的確性の確認のレベルとその方法 ･切替えの準備要領 　－必要な準備事項とその実施手順 ･切替えの実施要領
さまざまなタイプのアプリケーションの変更ごとの変更実施要領	･変更の要否の検討要領と決定の手続き ･変更計画の作成要領 　－変更の内容および実現方式の検討レビュー、承認手順 　－切替えについての課題のレビュー手順 　－切替えの実施方法についてのレビュー、承認手順 ･変更内容の的確性の確認要領 　－変更内容の的確性の確認のレベルとその方法 ･切替えの準備要領 　－必要な準備事項とその実施手順 ･切替えの実施要領

(2) 定められた手順に沿った切替えの実施

運用環境の切替えの安全を確保するためには、切替えは定められた手順に沿って行われなければならない。特に、以下のプロセスは慎重に行われなければならない。

- ルールに沿った変更システムの受入れの実施

  この点について特に留意すべき事項としては、以下があげられる。

  ･検収に必要なものの明確化

  ･必要なものの受領と内容の確認

  ･システムの検収テストの実施

- システムの運用部門としてのシステムの切替えに関する準備の実施

  この点について特に留意すべき事項としては、以下があげられる。

  ･システム環境の準備

  ･関係者の訓練

  ･移行データの検証

  ･切替えテスト

- 規定された手順に沿ったシステムの切替えならびに運用の開始の実施

【対応 ISMS コントロール】

10.4.1　運用ソフトウェアの管理

10.4.2 システム試験データの保護
10.5.1 変更手順管理

Tc5.5	運用関係者のシステム運用職場での行動に対するセキュリティ要求の実践

【主旨】

運用関係者はシステムへのアクセスが容易であるため、意図的な工作や不注意によるシステム運用環境の破壊等を起こし易い。このため、関係者に対するシステム運用職場における行動に関するセキュリティ要求の実践は追及されなければならない。この点については、特に厳重な管理指導が要求される。

【対策のポイント】

(1) システム運用関係者へのセキュリティにかかる要求、責務の徹底
- 必要な教育の実施と認識レベルのチェック
- 必要に応じた関係者の行動のチェック

(2) システム運用職場でのセキュリティ要求事項の実践
(3) システム運用職場でのセキュリティ要求の遵守状況のチェックの実施と必要な指導の実施
- 管理対象職場の網羅性
- 必要なサイクルでのチェックの実施

(4) 業務遂行上での不正行為のチェックの実施

【対応 ISMS コントロール】

4.2.1 第三者のアクセスから生じるリスクの識別
4.2.2 第三者との契約書に記載するセキュリティ要求事項
6.1.1 セキュリティを職責に含めること
6.1.2 要員審査およびその方針
6.1.3 秘密保持契約
6.1.4 雇用条件
6.3.5 懲戒手続き

Tc5.6	システム運用の外部委託についてのセキュリティ対策

【主旨】

システム運用のすべてあるいは一部を外部に委託する場合、システム運用の委託先においても、自社のセキュリティポリシーに沿った情報セキュリティが確保されなければならない。直接的な管理ができないシステム運用の委託先において、必要なセキュリティ対策が適切に講じられるようにするためには、以下のような施策の実施が必要となる。

- システム運用の外部委託におけるセキュリティを確保するため管理の仕組みの確立
- 委託先の適切な選択
- 委託システム運用のタイプごとのセキュリティに関する要求の明確化
- システム運用の委託先ごとのセキュリティ面での双方の責任の明確化
- システム運用の委託先ごとのセキュリティ要求への対応状況のチェックと必要な指導の実施

【対策のポイント】

(1) システム運用の外部委託におけるセキュリティを確保するため管理の仕組みの確立

システム運用の外部委託におけるセキュリティの確保のためには、セキュリティ面からシステム運用の外部委託を管理するための仕組みの確立は欠かせない。この管理の仕組みとして検討すべき事項としては、以下があげられる。

- システム運用の外部委託についてのセキュリティ方針

  システム運用の外部委託についてのセキュリティ方針として検討すべき事項としては、以下のようなものがある。

  ・委託先の選定方針

  ・委託先に対するセキュリティ要求の明確化とその実践の追及の方針

  ・セキュリティ事故発生時における委託先との責任の分界についての考え方
- システム運用の外部への委託についてのルール

  システム運用の外部への委託についてのルールとして検討すべき事項としては、以下のようなものがある。

  ・委託先の選定手続きと選定基準

  ・委託範囲と委託先に要求する委託付帯事項

  ・委託先に対するセキュリティ要求の基準

  ・委託先に対する要求の実践状況についての管理事項と管理の方法

  ・委託契約におけるセキュリティ条項の規定基準
- 外部に委託したシステム運用に求められるセキュリティ対策の実践の管理要領
- 問題発生時の対処要領

(2) ルールに沿った運用委託先の審査と決定

システム運用の外部委託の安全の確保は、まず、適切な委託先に選定にある。適切な委託先の

選定には、以下が必要となる。

- 規程に沿った審査の実施
  - －資格審査
  - －セキュリティ面での要求に対する対応能力
- 定められた手続きに沿った決定

(3) 委託するシステム運用のタイプごとのセキュリティに関する要求の明確化

(4) 運用委託先ごとのセキュリティ面での双方の責任の明確化

システム運用の外部委託で、事故が発生した場合、その責任の所在について、委託先と紛争が生じないようにするためには、委託契約の中等で、運用の委託にかかわる双方の責任を明確にしておかなければならない。このためには、以下のようなことが必要となる。

- 双方の責任の明確化と合意の形成
- セキュリティ要求事項の実践方法についての合意の形成
- 契約等でのそれぞれの責任の明文化

(5) 運用委託先ごとのセキュリティ要求への対応状況のチェックと必要な指導の実施

システム運用の委託先におけるセキュリティ要求の実践を確保するためには、委託先に対する指導や管理を継続的に行うことも必要となる。このことを適切に行うためには、以下のようことも必要となる。

- チェックの方法の確立と双方の合意の形成
- チェックと評価の実施
- 問題点の是正処置への展開
- 委託先との継続的なコミュニケーションの確保

【対応 ISMS コントロール】

4.3.1 外部委託契約におけるセキュリティ要求事項

3.4. その他のセキュリティ対策

3.4.1. 保管電子情報の有効性の確保

Td1.1	長期保管する電子情報の適切な保管を実現するための管理の仕組みの確立

【主旨】

2005年4月から施行されるe文書法の適用に伴い、紙媒体による保管義務から電磁的記録による保管方法が許容されたことで、企業等においては、今後、長期保管が義務付けられている文書等を、さまざまな利点がある電子情報という形態で保管することが、拡大することになると思われる。しかし、これらの情報を、電子情報という形態で長期に保管する場合は、その完全性の確保ができることが前提となる。

電子情報の長期保管にあたっては、保管の全期間を通じて、見読性の確保、機密性の確保、保存性の確保に加え、法的に保管が義務付けられているものについてはその法的有効性の確保も必要となる。これらの実現には、必要な技術的な環境の準備に加え、これらの情報に対する保管にかかわる適切な取扱いが欠かせない。これらの電子情報の長期保管を適切に行うためための諸施策が適切に機能するためには、組織的な取組みが欠かせず、これらの情報の取扱いについての管理の仕組みの確立が必要となる。

【対策のポイント】

⑴ 電子保管に該当する法令･規則･ガイドラインの把握

電子保存情報の保存対象となる国税関係帳簿類や製造物責任法関連書類、医療関係書類等々、その他、保管電子情報の保存が義務化されている保管電子情報については、それぞれ法制度に規定されている保管年数に応じた適切な保管が必要となる。これらの文書にかかわる電子情報の適切な保管を実現するためには、まず、これら電子情報の保管についての法律他の外的な要求を漏れなく正確に把握する必要がある。

⑵ 長期保管の対象となる電子情報に対する保管基準の確立

電子情報の長期保管を目的にあったものにするためには、個々の対象電子情報に対する保管要件の指定が、適切に行われ無ければならない。多岐にわたる対象電子情報に対する保管要件の指定を適切なものにするためには、保管要件の指定についての基準が確立していることが必要となる。

長期保管の対象となる電子情報に対する保管基準として指定すべき事項としては、以下のようなものがあげられる。

- 法的要求
- 保管期間
- 保管方法の大枠

保管方法はさまざまであるが、必要な保管期間によって、一般的にとるべき手段が異なる。一

般的に検討すべき保管方法は以下のようになる。

・保管期間が比較的短期なもの　：各種アプリケーションに依存したデータ形式の状態で保管（変化作業不要）
・保管期間が中期なもの　　：標準仕様のデータ形式に変換して保管（変換作業要）
・補完期間が長期にわたるもの　：標準仕様のデータ形式に変換して保管するのに加え、他のCOM 形式（マイクロフイルム化）やその他長期間の見読性が保障された記録システムの使用

- 保管に使用する媒体
- 検索性の確保
- 法的要求への対応方式
- 見読性の維持の方法
- 可視性の確保
- バージョン管理
- 電子署名およびタイムスタンプの付与
- 作成要件（入力プロセス）
- システム要件（解像度、階調、ファイル形式）
- 保管についての物理的な条件

これらの基準の検討にあたっては、必要な保管期間の長短によって保管についての方針を定めておくことも有効である。

（注）保管期間による保管についての一般的な原則
短期：各種アプリケーションに依存したデータ形式の状態で保管（変換作業なし）
中期：標準仕様のデータ形式に変換し、保管する（変換作業あり）
長期：電子データの他に COM 形式（マイクロフィルム化）やその他、長期間の見読性が保証された記録システムとの併用

（3）長期保管の対象となる電子情報の保管にかかる措置の実施要領の確立

長期保管する電子情報の目的に沿った保管を実現するためには、これらの電子情報の作成から廃棄に至るまでのライフサイクルの全過程における取扱い方法を示したものも必要となる。

長期保管の対象となる電子情報の保管にかかる措置の方法を示した実施要領に示すべき事項としては、以下があげられる。

- 保管要件の指定手続きと保管要件の管理方法
- 保管電子情報の作成手続き
- 保管情報の物理的保管手続き（入庫や棚卸し）
- 保管情報の使用手続きと使用の管理
- 保管情報の完全性の維持手順とその実施手続き
- 保管情報の廃棄手続き
- 保管に関わる措置の記録の作成とその保管

（4）長期保管する電子情報の適切な保管の実践を管理する仕組みの確立

長期保管する電子情報の目的に沿った保管を実現するためには、これらの電子情報の保管に

かかわる措置が的確に実践されなければならない。このためには、必要な措置の実施を管理する組織的な仕組み作りも必要となる。

(5) 保管電子情報に係わる管理責任体制の確立

電子保管情報の保護要件としては、長期期間の安全性を確保しなければならない。そのための組織的な取り組みが必要であり、管理責任者の任命および責務の明確化や管理責任組織および体制の明確化が必要となる。また、個々の具体的な保護要件に対応するため、電子保管情報の棄損、滅失、改ざん、漏洩等々が生じないようにするための管理規定の策定や責任者の任命および業務内容を明確に規定する必要がある。

- 保管電子情報に関する管理規定の策定
- 保管電子情報責任者および担当者の任命
- 保管電子情報の業務内容の明確化
- 保管電子情報の情報区分およびレベル付け
- 保管電子情報の法的準拠性対応の明確化
- 法的･技術的な専門家による助言体制の明確化
- タイムスタンプ付与に関する利用規程

【対応 ISMS コントロール】

ISMS に、本対策要求に明示的に対応する要求はない。

【参考】

- 電子情報の保管についての法的な要求の例
  ･国税関係帳簿類　8.5 年 (タイムスタンプの検証が必要)
  ･製造物責任法関連書類　10 年 (タイムスタンプの検証が必要)

Td1.2　長期保管を行う電子情報の作成や保管に必要な技術環境の整備

【主旨】

長期に保管する電子情報を、それぞれに指定された保管要件を満たすように保管するためには、法的有効性の確保や、機密性の確保や、見読性確保の確保や、完全性の確保のための、媒体の保管設備やタイムスタンプの適用等のための技術的な環境が必要となる。

これらの適切な選択と的確な実装も、電子情報の目的に沿った長期保管には欠かせない。

【対策のポイント】

(1) 保管電子情報の取り扱いに関する技術環境の整備

電子情報の目的に応じた長期保管の実現のためには、技術的なツールも必要となる。必要な技術の選択と、その適切な使用法の選択も、電子情報の目的に応じた長期保管の実現に欠かせな

い。

検討の対象としては、以下があげられる。

- 保管の物理的環境の整備（温度、湿度、要員の訓練）
- 保管ツールの整備（保存媒体、保存装置）
  - ・適切な保存装置の確保および管理
  - ・適切な媒体の確保
  - ・各種保管ツールのマイグレーション管理
- 適切なソフトウェアの確保および管理
  - ・文書情報の出力に必要なソフトウェアの適切な保管
  - ・ソフトウェアのバージョン管理
- 電子署名やタイムスタンプサービス利用の整備
  - ・認定取得事業者の選定および管理
- 電子媒体の劣化、喪失、損壊防止の適切な管理および必要に応じたバックアップ体制

(2) 使用技術の的確な実装

電子情報の長期保管にかかわる技術環境に対しては、実装が的確に行われ、期待通りに機能していることを、導入時の徹底したテストによる確認に加え、定期的なチェックも行わなければならない。

(3) 対応する技術環境の見直しの実施

電子情報の長期保管に用いている技術環境の的確性を維持するためには、定期的あるいは保管要件の変更等にともなう必要に応じた、その的確性についての見直しも欠かせない。

【対応 ISMS コントロール】

ISMS に、本対策要求に明示的に対応する要求はない。

Td1.3 長期保管の対象情報に対する保管要件の適切な指定

【主旨】

電子情報の長期保管の目的や保管にあたっての条件や要件は、電子情報によって異なりさまざまである。電子情報に長期保管する電子情報の目的沿った保管を実現するためには、対象情報の個々に対して保管要件の適切な指定が必要となる。保管の有効性に直結する、この長期保管する電子情報に対する保管要件の指定を的確なものにするためには、その指定は十分に管理されなければならない。

【要求のポイント】

(1) 対象電子情報（群）に対する保存要件の適切な指定

長期保管を行う電子情報（群）の個々に対し、保管についての具体的な要求を指定する。長期

保管の対象となる個々の電子情報（群）に対し、その保管要件として指定すべき事項としては以下のようなものがある。

- 法的要求事項
- 目標とする保管期間
- 保管方法
- 保管に使用する媒体
- 必要とする検索性
- 法的要求への対応方式
- 見読性の維持の方法
- 可視性の確保の方法
- バージョン管理が必要な場合におけるバージョン管理についての要求
- 電子署名およびタイムスタンプの付与
  ・電子署名：認定認証事業者より発行された証明書の利用指定
  ・タイムスタンプ：認定時刻認証事業者より発行されたタイムスタンプの利用指定
- 保管電子情報の検証および完全性確保の手段
  対象とする保管電子情報の完全性の確保が可能なデジタル署名およびタイムスタンプの検証手段の実装や検証内容の保証、検証手順の指定を行う。
  ・対象情報の完全性の確保手段および物理的な保存方式の方針
  －第三者委託、保存媒体の2重化、媒体の劣化対策の方針
  ・長期保管に適応した暗号化アルゴリズムの方針
  ・長期タイムスタンプ付与や再スタンプ処理、ES フォーマット等々の指定。
  ・対象となる電子保管情報の完全性を確保する技術要件として、タイムスタンプ付与や再スタンプ処理、ES フォーマット等々の指定を行う必要がある。
- アナログ情報の電子化を伴う場合における作成要件（入力プロセス）
- 保管についての物理的な条件
- 廃棄の手順

これらの項目は、Td1.1 に示した保管基準に沿って決められなければならない。

また、この指定は、定められたルールにより審査、決定されなければならない。

（2）指定した保管要件に対する見直しの実施

長期保管する電子情報に対して指定した保管要件の不備が見逃されたままにならないようにするためには、定期的にその妥当性の見直しを行うことも必要となる。

【対応 ISMS コントロール】

ISMS に本対策要求に明示的に対応する要求はない。

【参考】

国税関係帳簿類、製造物責任法関連書類、医療関係書類等については、法的な保存義務が科せられていることから、適切な保存期間や目的に合わせた保存要件を満たすとともに保管電子

情報の存在日時と非改ざん性を証明するための電子署名およびタイムスタンプ付与が必要となる。

Td1.4	対象情報に対する指定要件に沿った保管措置の実施

【主旨】

長期に保管する電子情報が適切に保管され、長期の保管の全期間を通じて、保管の目的が損なわれないようにするためには、保管電子情報のすべてについて、電子情報ごとに指定されている保管要件に沿った保管上の取扱いが確実に行われなければならない。

このことを実現するためには、これらの情報に対して必要となる完全性、見読性、秘匿性、法的効力の確保に必要な措置が的確に実践されなければならない。

【対策のポイント】

⑴ 保管電子情報の完全性の維持の実施

保管電子情報の完全性を長期間維持するには、物理的な媒体の安定確保や保管電子情報の改ざん検知、削除防止等々の機能確認を実施しなければならない。

- 保存装置および物理媒体の確認
- 保存性、機密性、完全性、見読性の確認
- タイムスタンプの付与、更新、有効期間の確認

⑵ 遵守状況のチェックと必要に応じた指導の実施

保管電子情報の法制度に遵守した運用チェックと必要に応じた教育指導を実施する。

- 業務現場における遵守状況の確認
- 保管要件の機能保全の確認
- 保管運用現場における遵守状況の確認および指導の実施

⑶ 情報ライフサイクル(「作成」、「利用」、「保管」、「廃棄」)管理の徹底および実施

- 情報の価値に合わせた情報ラフサイクル管理の方針決定
- 個々の情報ライフサイクルにおける適切な実施。

⑷ 対策現場への展開

運用規定通りの適切な運用が実施されているか、対策現場の展開状況についての確認を行う。

- 関係業務現場への要求展開
- システム運用への要求展開

【対応 ISMS コントロール】

ISMS に、本対策要求に明示的に対応する要求はない。

3.4.2. 特殊な利用環境に対するセキュリティ対策

Td2.1	モバイルコンピューティングの利用についてのセキュリティ要求の明確化

【主旨】

モバイルコンピューティングをセキュアなものにするためには、まず、モバイルコンピューティングの利用における脅威を踏まえた、利用上の条件等が明確にされていなければならない。

【対策のポイント】

(1) モバイルコンピューティングの管理単位の明確化

モバイルコンピューティングの利用は、出先からの基幹業務へのアクセス、出先からのセンターにある情報へのアクセス、各種の連絡の他、出先でのオフラインでの文書の作成他の情報処理その用途は幅が広い。取り扱う情報や接続するセンターシステムによってセキュリティについての要求レベルは異なるため、モバイルコンピューティングをセキュアなものにするためには、利用できる業務の範囲等から、モバイルコンピューティングの利用機器グループを決め、この管理単位に使用の制限等のセキュリティについての要求を決めることが必要となる。

(2) 利用の制限

危険の大きいモバイル環境でのシステムの利用が安易に行われないようにするとともに、万一、事故があっても大事に至らないよう、その使用には相当の制約がかけられるべきである。モバイルコンピューティングの利用制限として検討すべき事項としては、表 3-54 に示すようなものがある。これらは、(1)項で示したモバイルコンピューティングの利用機器グループ単位に指定されなければならない。

表 3-54 モバイルコンピューティングの利用制限として検討すべき事項

項番	検討が必要な事項	備考
1	適用業務の制限	･アクセスできる業務の制限 ･アクセスできる外部サービス モバイルコンピューティングは、出先でのシステムの利用が必須となる業務に限定すべきである。また、重大な結果を伴う業務は本来、モバイルコンピューティングの対象にしてはならない。
2	利用者の制限	･利用者の職務や資格の制限が必要。 重要な業務については厳しい制限が必要 ･利用者の認可手続き
3	モバイル機器への情報の格納についての制限	格納を禁止される情報(群)
3	利用場所	適用業務ごとに、利用していい場所、もしくは利用してはならない場所を指定

(3) 情報の格納条件の制限

モバイル機器の盗難や紛失や外部の者による不正な使用に備え、モバイル機器に格納する情報の制限も必要となる。また、格納が許される情報でも、特に秘匿性の要求が高い情報については暗号化等の万一の場合における秘匿性の確保についての要求も明確にしておく必要がある。

情報の格納条件として指定すべき事項としては、表 3-55 に示すものがあげられる。これらは、モバイルコンピューティングの利用機器グループ単位に指定しなければならない。

表 3-55　モバイル機器への情報の格納条件として検討すべき事項

項番	検討が必要な事項	備考
1	格納可能情報	モバイルコンピューティングは、出先でのシステムの利用が必須となる業務に限定すべきである。また、重大な結果を伴う業務は本来、モバイルコンピューティングの対象にしてはならない。
2	秘匿性確保についての要求	･暗号化他の秘匿性確保策が必要な情報（群） ･暗号化他の秘匿性確保のための手段 ･暗号鍵の管理方式等の関連する運用

(4) アクセス制限等のモバイル機器に対するセキュリティ対策の要求

モバイル機器の盗難や紛失や外部の者による不正な使用に備え、本来の使用者以外の者は容易に使用できないようにするための工夫も必要となる。この点についての検討事項としては、以下のようなものがある。

- ログイン認証のレベル
- ロック機能の実装

【対応 ISMS コントロール】

9.8.1　移動型計算処理

Td2.2	モバイルコンピューティングに対するセンターシステム側での必要なセキュリティ対策の実施

【主旨】

モバイルコンピューティングにおいては、本来の利用者でない者による不正な利用の危険も考えられるため、センターに置かれたき業務システムにおいては、モバイル機器からのアクセスに対しては、社内の端末からのアクセスに対するよりは厳重な認証や、利用機能の制限等を行わなければならい。

【対策のポイント】

(1) モバイルアクセスが行われる業務システムごとに必要なセキュリティ機能の明確化

業務や取扱う情報の重要性から、モバイル機器からのアクセスに対し、特別な認証が求められる業務においては、信頼度の高い認証方式の適用が必要となる。また、アクセスできる機能の制限も必要となる場合がある。このため、モバイルアクセスが行われる業務システムについては、それぞれにモバイルコンピューティングに関し実装すべきセキュリティ機能を指定する必要がある。

検討すべき機能としては、表 3-56 に示すようななものがある。

表 3-56　モバイルアクセスに対するセキュリティ機能として検討すべき事項

項番	検討が必要な事項	備考
1	利用者の認証	･適用する認証手段 ･認証のタイミング（場合によっては、要求ごとに認証も必要） ･不審なアクセスに対する警告他の必要な処置
2	利用機能の制限	･当該業務の中でモバイルアクセスが利用できる機能（情報へのアクセス、要求に対する業務処理、情報の転送等）の制限 （利用者のグループ別に検討が必要）
3	通信の保護	・ 通信路の制限（無線の使用の禁止他） ・ 通信の暗号化の要否と暗号化の方式 ･通信データの改ざん検知の要否と検知方式
4	使用時間帯の制限機能	･モバイル機器からのアクセスが許される時間帯
5	タイムアウト機能	･1 回の接続に許される時間
6	アクセスログの取得機能	･モバイルアクセスについて特に必要となるものがある場合

(2) モバイルアクセスを許す業務システムにおけるモバイルコンピューティングに対し必要なセキュリティ機能の実装

モバイルアクセスを許す業務システムは、モバイルアクセスに対し要求される認証や利用機能制限や通信の保護を実現するために指定された機能が的確に実装されていなければならない。これらを適切に行うためには、以下が必要となる。

- 設計レビューの徹底
- 実装に対する確認テストの徹底
- 利用者の登録等の関連情報の的確性の維持

(3) 利用者や利用機器の管理の徹底

モバイルアクセスに対するセンター側でのセキュリティ対策が的確に機能するためには、その利用者や利用機器について、表 3-57 に示すような管理が徹底していなければならない。

表 3-57　モバイル機器のりようについて必要な管理

項番	検討が必要な事項	備考
1	利用者の管理	･利用者の資格の管理(注1) ･利用者へのアクセス権限の付与(注1) ･利用状況の把握
2	利用モバイル機器の管理	･使用機器とその ID ･実装しているセキュリティ機能

(注1)人事異動他での資格の変更やそれに伴う付与権限の管理は、厳格に行われなければならない。

【対応 ISMS コントロール】

9.8.1　移動型計算処理

Td2.3	利用者サイドにおけるモバイルコンピューティングに対するセキュリティ要求の実践の追及

【主旨】

モバイルコンピューティングの安全の確保は、

- モバイル機器への必要なセキュリティ機能の実装
- モバイルコンピューティングの利用にあたっての注意事項の厳守
- モバイル機器の盗難・紛失の防止

といった利用者サイドにおける必要な対応の実践にも大きく依存する。

このため、モバイルコンピューティングを利用する者は、モバイルコンピューティングの利用にあたって、これらについての要求の実践を追及しなければならない。

【対策のポイント】

(1) モバイル機器への必要なセキュリティ機能の実装

モバイル機器側にもセンター側の機能に対応した機能の実装が必要となる。実装の検討が必要となる機能としては、表 3-58 に示すようなものがあげられる。

表 3-58　モバイル機器に実装すべきセキュリティ機能

項番	検討が必要な事項	備考
1	モバイル機器としての利用者認証関連機能	・指定された認証方式に対応した機能 ・認証情報の管理機能 ・警告機能や端末のロック機能とうの不審な利用に対する安全処置機能
2	センターアクセスのための認証関連機能	・指定された認証方式に対応した機能 ・認証情報の管理機能
3	格納情報の秘匿化機能	・格納情報に対する暗号化等の秘匿化機能
4	通信の保護機能	・暗号化機能 ・通信データの改ざん検知機能

(2) 利用上の注意事項の遵守

モバイルコンピューティングを利用する者には、その利用にあたって、以下のような注意が要求される。

- 使用するモバイル機器への必要はセキュリティ機能の的確な実装の確認
- アクセス制御に用いるパスワード等の認証情報の確実な保護
- 稼動状態でのモバイル機器の放置の禁止
- 外部の者が画面を覗ける環境での利用の禁止
- 盗難や紛失の阻止

これらが徹底するためには、以下が必要となる。

- 利用マニュアルの作成
- 利用者への利用上の注意事項の周知の徹底

- 利用者に対する使用条件の遵守の監督と指導
- 注意事項遵守状況のチェックの仕組みの確立

【対応 ISMS コントロール】

9.8.1 移動型計算処理

Td2.4	リモートオフィスごとのセキュリティ対策のフレームワークの確立

【主旨】

リモートオフィスにおいても、本社、営業拠点、工場やシステムセンター等の事業の拠点を中心とした組織全体に対するセキュリティ対策の実践が必要となるが、不十分な管理環境の下で、その要求に応えることは容易ではない。このため、それぞれのオフィスの運営形態を反映した個別の対策の確立が必要となる。

リモートオフィスごとのセキュリティ対策のフレームワークとは、それぞれのリモートオフィスにおいて、組織全体として情報セキュリティについての要求に、どのような形で応えるかを示すものである。検討すべき事項としては、以下があげられる。これらは、リモートオフィスのタイプごとに検討されなければならない。

- セキュリティ対策という観点からのリモートオフィスの運営環境の評価
- リモートオフィスが保有する保護対象情報資産やシステム資産の明確化
- リモートオフィスにおいてセキュリティ対策上の特に配慮すべき事項
- リモートオフィスにおけるセキュリティ対策の組み立て
- リモートオフィスにおけるシステムの構成とそのセキュアな運用方法
- リモートオフィスの施設や設備の物理的･環境的保護の方針

【対策のポイント】

(1) セキュリティ対策という観点からのリモートオフィスの運営環境の評価

リモートオフィスのタイプごとに、リモートオフィスにおけるセキュリティ対策上の特に配慮すべき事項を洗い出すための、その運営環境にかかわる表 3-59 に示すような点についての評価を行う。

表 3-59 リモートオフィスに対するセキュリティ面からの運営環境についての評価事項

項番	検討が必要な事項	備考
1	立地条件	･環境的な環境 ･社会的な環境
2	施設の状況	･施設の堅牢性 ･立ち入り制限の実効性他

3	適用業務と情報の取扱い状況	･本来業務 ･付帯業務 ･取扱っている重要な情報 ･独自に保有する保護対象情報
4	組織の運営形態	･組織形態（従業者の規模、従業者種別他） ･管理体制
5	システムの形態	･リモートオフィス内でのシステムの構成 ･機能の範囲 ･運用体制

(2) リモートオフィスが保有する保護対象情報資産やシステム資産の明確化

リモートオフィスのタイプごとに、取扱われている情報でリモートオフィスが保護管理しなければならない情報と、そのそれぞれに対する保護要件の明確化が必要となる。

(3) リモートオフィスにおいてセキュリティ対策上の特に配慮すべき事項

リモートオフィスが要求される情報セキュリティを確保するためには、リモートオフィスのタイプごとに、先にあげたセキュリティ対策面からの環境の評価を踏まえ、事業拠点での対策に比べ特に配慮や工夫が必要となる事項と、それらへの対応をどのように行うかについての方針を明確にしていかなければならない。

この点について検討が必要な事項としては、以下があげられる。

- 組織的な脆弱性に対する対策
- 業務運営やその管理についての特別な配慮
- システム面でのリモートオフィスゆえの脆弱性への配慮
- 施設や設備の物理的･環境的な脆弱性への対策

(4) リモートオフィスにおけるセキュリティ対策の組み立て

組織全体からの要求に、前項であげたリモートオフィスにおけるセキュリティ対策で必要な特別な配慮を加え、表 3-60 に示すような事項についての基本方針をリモートオフィスのタイプごとに定める。

表 3-60 リモートオフィスにおけるセキュリティ対策の組立てにおいて検討すべき事項

項番	検討が必要な事項	備考
1	情報セキュリティについての責任体制	･責任者とタスク ･セキュリティ対策実施の責任分担
2	組織管理面でのセキュリティ対策	･従業者の監督指導のポイントと実施方法
3	業務運営面でのセキュリティ対策	･業務現場でのセキュリティ対策対応活動 ･業務現場での必要な対応に対する実践のチェックと指導
4	業務現場での情報の保護の実践	･リモートオフィスで取扱うあるいは管理している保護対象情報に対する保護要件 ･必要な保護策の展開方法 ･指定された保護策の実施についてのチェックと指導
5	オフィス内システムに実装するセキュリティ対策	･不正アクセス対策 ･セキュリティホール対策 ･ウイルス対策 ･セキュリティ管理情報やシステム構成情報の保護 ･通信の保護 ･適用するシステムの監査 ･セキュリティ事故への備え

6	オフィス内システムのセキュアな構築とそのセキュアな運用	･オフィス内システムの構成のフレームワーク ･オフィス内システムの妥当性の維持の確保についての方針 ･オフィス内システムの適切な運用を実現についての方針
7	施設や設備に対する物理的･環境的保護の方針	･保護領域の確保やその管理についての方針 ･施設や設備の保護についての方針
8	セキュリティ監査の実施	･リモートオフィスの運営に対するセキュリティ面からの要求を全体的に監査する仕組み

この場合、リモートオフィスの環境的な脆弱性や、運用体制面での脆弱性への配慮を欠かさないようにすることが肝要である。

【対応 ISMS コントロール】

9.8.2 遠隔作業

Td2.5 リモートオフィスサイドのシステムのセキュアな構築

【主旨】

リモートオフィス内のシステムの構成に対するセキュリティ面からの要求を満たしたものとして構築維持し、そのセキュな運用を実現するためには、リモートオフィスにおいても、以下が必要となる。

- システム構成の的確性の確認
- システム構成機器のそれぞれにおける機能や諸設定の的確な実装の確認
- 日々のシステム運用における計画作成やその実行管理の徹底

【対策のポイント】

(1) システム構成の的確性の確保

リモートオフィス内のシステムの構成に対するセキュリティ面からの要求を満たしたものとして構築維持し、そのセキュな運用を実現するためには、リモートオフィスにおいても、以下が必要となる。

- システム構成の設計が、セキュリティについての要求他のさまざまな要求を満たしていることについてのレビューの実施。セキュリティ面からの主なチェックポイントしては以下のようなものがある。
  - ･システム機器の障害に対する求める可用性の確保
  - ･要求される性能や容量の確保
  - ･セグメント構成とセグメント間での通信ルール
  - ･ネットワーク制御機器の配置と機能の割り当て
  - ･ウイルス対策ソフトの配置
  - ･サーバや重要な情報の配置
  - ･監視ツールの配置

● 設計どおりの構成の構築

導入当初だけでなく、定期的な点検も必要である。このため、リモートオフィス内のシステム構成に対する定期的なチェックの実施要領の確立も必要となる。

(2) システム構成機器のそれぞれにおける機能や諸設定の的確な実装

リモートオフィス内のシステムを構成する機器の実装を的確なものにするためには、以下の施策の実施が必要となる。

● 各機器における機能の使用方法の明確化
● 諸設定の設定条件の明確化とそのレビューの徹底
● 機能の設定やパラメータ等の設定の的確性の確認の徹底
● 各機器からの脆弱性の除去(注1)

これについてもシステムの構成と同様、導入当初時点だけでなく、定期的な点検も必要である。このため、リモートオフィス内のシステム構成機器それぞれに対する定期的なチェックの実施要領の確立も必要となる。

(3) 日々のシステム運用における計画作成やその実行管理

リモートオフィス内のシステムのセキュアな運用を実現するためには、日々のシステム運用について、以下のような施策の実施が必要となる。

● システム運用上のセキュリティ要求事項の明示
  ・正確なオペレーションの実施
  ・セキュリティ管理情報の更新
  ・要求されているセキュリティ面での監視の実施
  ・指定されたバックアップの確保
● 運用規程、運用マニュアルへのセキュリティ要求事項の反映
● 日常の運用スケジュールへの反映
● 要求事項の実行を管理する仕組みの確立と、ルールに沿った日常のシステムオペレーションにおけるセキュリティ要求事項の実行状況のチェックと必要な指導の実施

【対応 ISMS コントロール】

9.8.2 遠隔作業

Td2.6	リモートオフィスサイドのシステムのセキュアな運用の追求

【主旨】

リモートオフィス内のシステムの構成に対するセキュリティ面からの要求を満たしたものとして構築維持し、そのセキュな運用を実現するためには、リモートオフィスにおいても、以下が必要となる。

● システム構成の的確性の確認

- システム構成機器のそれぞれにおける機能や諸設定の的確な実装の確認
- 日々のシステム運用における計画作成やその実行管理の徹底

【対策のポイント】

(1) システム構成の的確性の確保

リモートオフィス内のシステムの構成に対するセキュリティ面からの要求を満たしたものとして構築維持し、そのセキュな運用を実現するためには、リモートオフィスにおいても、以下が必要となる。

- システム構成の設計が、セキュリティについての要求他のさまざまな要求を満たしていることについてのレビューの実施。セキュリティ面からの主なチェックポイントしては以下のようなものがある。
  - ・システム機器の障害に対する求める可用性の確保
  - ・要求される性能や容量の確保
  - ・セグメント構成とセグメント間での通信ルール
  - ・ネットワーク制御機器の配置と機能の割り当て
  - ・ウイルス対策ソフトの配置
  - ・サーバや重要な情報の配置
  - ・監視ツールの配置
- 設計どおりの構成の構築

導入当初だけでなく、定期的な点検も必要である。このため、リモートオフィス内のシステム構成に対する定期的なチェックの実施要領の確立も必要となる。

(2) システム構成機器のそれぞれにおける機能や諸設定の的確な実装

リモートオフィス内のシステムを構成する機器の実装を的確なものにするためには、以下の施策の実施が必要となる。

- 各機器における機能の使用方法の明確化
- 諸設定の設定条件の明確化とそのレビューの徹底
- 機能の設定やパラメータ等の設定の的確性の確認の徹底
- 各機器からの脆弱性の除去(注1)

これについてもシステムの構成と同様、導入当初時点だけでなく、定期的な点検も必要である。このため、リモートオフィス内のシステム構成機器それぞれに対する定期的なチェックの実施要領の確立も必要となる。

(3) 日々のシステム運用における計画作成やその実行管理

リモートオフィス内のシステムのセキュアな運用を実現するためには、日々のシステム運用について、以下のような施策の実施が必要となる。

- システム運用上のセキュリティ要求事項の明示
  - ・正確なオペレーションの実施
  - ・セキュリティ管理情報の更新
  - ・要求されているセキュリティ面での監視の実施

･指定されたバックアップの確保

- 運用規程、運用マニュアルへのセキュリティ要求事項の反映
- 日常の運用スケジュールへの反映
- 要求事項の実行を管理する仕組みの確立と、ルールに沿った日常のシステムオペレーションにおけるセキュリティ要求事項の実行状況のチェックと必要な指導の実施

【対応 ISMS コントロール】

9.8.2 遠隔作業

Td2.7	リモートオフィスの施設や設備に対する必要な保護策の実施

【主旨】

リモートオフィスの施設や設備についても、適切な物理的･環境的な保護策の実施が必要となる。検討事項としては、保護領域の確立と立入りや物品の搬入･搬出の制限と管理、設備の対する破壊や持ち出し等の工作や、災害等への配慮となる。

これらの検討にあたっては、以下のような配慮が必要となる。

- 立地条件からくる制約下での適用可能性
- 絶対的な要求についての対応
- 予算や運用上の負担とのバランス

【対策のポイント】

(1) 必要な保護領域の確保

当該リモートオフィスにおけるセキュリティ対策のフレームワークで示された保護領域を実現するための設備やシステムの導入。導入の検討が必要となることとしては、表 3-61 に示すようなものがあげられる。

表 3-61 リモートオフィスの施設や設備に対する保護策として検討すべき事項

項番	検討が必要な事項	備考
1	保護領域の空間を確保するための設備	･隔壁等 ･物品の搬入･搬出口
2	保護空間を管理するための設備	･立ち入りの制限や管理のための設備 ･出入りを監視するための設備
3	保護空間を管理するための管理の仕組み	･保護領域に出入りを許可する者についての管理の仕組み ･保護領域の出入りや物品の移動を管理の仕組み

(2) 設備に対する安全措置の実施

設備の安全の確保についての検討事項としては、以下があげられる。

- 設置場所

- 設置方法
- 外部からの工作に対する強度の補強策
- 保守等の定期的な点検の実施

【対応 ISMS コントロール】

4.1.1

Td2.8	リモートオフィスにおける業務運営や組織管理におけるセキュリティ事故防止の追及

【主旨】

リモートオフィス業務の遂行にあたってセキュリティ事故を起さないためには、日々の業務遂行上で実践しなければならない情報セキュリティにかかわる要求への対応を確実に実践しなければならない。このことを実現するためには、セキュティ要求を実践を管理するための仕組みの確立と、組織の管理や業務の運営やシステムの維持管理やその運営に対する、その仕組みの上に立った監督と指導が欠かせない。

【対策のポイント】

(1) 業務遂行面でのセキュティ要求の実践を管理するための仕組みの確立

リモートオフィスにおける業務の遂行にあたってのセキュリティ面からの要求の実践を確実にするためには、その実践を管理するための仕組みも必要となる。このためには、以下のようなことも必要となる。

- 業務遂行上でのセキュリティ要求の明確化
- セキュアなリモートオフィス業務の遂行についての責任体制の確立
- チェックリストの確立
- チェックの実施サイクルやチェック方法等を示したチェック実施要領の確立

(2) 必要な監督と指導の実施

リモートオフィスの運営をセキュアなものとするためには、日々の組織の管理や業務の運営、システムの維持管理や運営に対するセキュリティ面からの要求の実践についてチェックと指導が欠かせない。これらは、確立した管理の仕組みに立脚したものであることが望ましい。

(3) リモートオフィスの運営に対するセキュリティ監査の実施

出先であるため厳格な管理が行き届かない恐れがあるリモートオフィスに対しては、特別な監査も有効である。リモートオフィスに対するセキュリティ面での監査として検討すべき事項としては、以下があげられる。

- それぞれのリモートオフィスにおけるセキュリティ監査要領の確立
  ・監査の実施要領
  ・システムのセキュリティ対策の監査ポイントの明確化

・リモートオフィスの運営についてのセキュリティ監査ポイントの明確化
・施設、設備の保護についてのセキュリティ監査ポイントの明示
・システムに対する技術診断による対策の効果の確認

- それぞれのリモートオフィスにおけるセキュリティ監査要領の実施
  ・システムのセキュリティ対策状況の監査の実施
  ・リモートオフィス運営についてのセキュリティ対策状況の監査の実施
  ・施設、設備の保護についてのセキュリティ対策状況の監査の実施
- 監査結果の有効活用
  ・監査結果の評価（問題点の分析状況）
  ・監査指摘事項に対する是正処置の実施

【対応 ISMS コントロール】

9.8.2 遠隔作業

3.4.3. 施設や設備の保護

Td3.1	閉鎖型の保護領域における必要な保護の実施

【主旨】

重要な施設全体や、重要な設備や情報が置かれている場所については、人の出入りや物品の搬入・搬出が、所定の管理下でなければ行えないような閉鎖型の保護領域を設定し、人物等の立ち入りだけでなく、物品の搬入・搬出についても厳格な管理下に置くことが必要となる。この閉鎖型の保護領域の設定には、設備面でも運用面でも負担が少なくないため、その必要性と実施する保護のレベルについては十分な検討が必要となる。

【対策のポイント】

(1) 必要に応じた閉鎖型の保護領域の設定

必要かつ十分な閉鎖型の保護領域の設定には、まず、その必要性と実施する保護のレベルについては十分な検討が必要となる。閉鎖型の保護領域の設定について検討すべき事項としては、以下があげられる。

- 閉鎖型の保護領域設置の必要性
- 求められる保護のレベル
- 前提とする設備と運用形態

閉鎖型の保護領域の設置には、相当のコストと運用体制が必要となるため、経営レベルの判断が必要となる。

(2) 対象保護領域ごとの領域保護要件の確立

保護領域を適切に保護するためには、まず、個々の保護領域に対し表 3-62 に示すような保護要件を明確にしなければならない。

表 3-62 閉鎖型の保護領域に対する保護要件として指定すべき事項

No	項目	内容等
1	対象領域の物理的な隔離の方法	･隔壁のレベル -隔壁の強度、隔壁の間隙（床下、天井裏）への配慮 ･出入り口の物理的な構造 ･入退室の物理的な制限方法 -サークルゲート、フラッパーゲート等の利用 ･入退室の監視設備
2	領域内における行動の制限	･立ち入り者の資格に沿った領域内で許される行動および禁止される行動 ･違反行為に対する罰則等
3	領域内における立ち入り者の行動の管理･牽制	･行動の監視の方法 -監視カメラ、各種センサーの利用 -警備員の配置 ･違反行為や不審な行動の対する対処
4	入退室の権限	･入室が許される者の範囲
5	入退室の管理方法の大枠	･入室許可を持つ者のチェックの手段 -IC カード、虹彩認証、指紋認証等の認証システム -警備員によるチェック 入退室の記録の作成と保管
6	物品の搬入･搬出の制限	･搬入出物品および搬入出者のチェックの手段 -金属探知機、X 線走査機、タグゲート等 -警備員によるチェック ･搬入･搬出物および関与者の記録の作成と保管

（2）保護領域ごとの管理要領の作成

保護領域の保護が実務上で機能するためには、当該領域の使用や管理の方法が確立していなければならない。管理要領で明確にすべき事項としては、表 3-63 に示すようなものがあげられる。

表 3-63 閉鎖型の保護領域に対する管理要領として指定すべき事項

No	項目	内容等
1	立ち入りが許可される者の管理要領	･立ち入りが許可される者の認可の手続き ･立ち入りが許可された者の登録手続き ･立ち入りが許可された者の妥当性についての定期チェックの方法 ･ID 等の付与の手続き ･ID 等の更新手続き ･不正行為や不審な行動を見つけた場合の手続き
2	入退室の管理要領	･入室の手続き ･退室の手続き ･入退室の記録の作成
3	物品の搬入･搬出の制限	･物品の搬入の手続き ･物品の搬出の手続き ･物品の搬入･搬出の記録の管理
4	管理実態のチェック要領	･チェックサイクル ･チェックすべき事項 ･チェック結果の取扱い

(3) 管理要領に沿った管理の実施

管理の対象としては、以下があげられる。

- 立ち入りを許可する者についての管理の実施
- ルールに沿った厳格な入退室管理の実施
- ルールの沿った物品の搬入･搬出の管理の実施
- ルール違反に対する処罰や指導の実施

(4) 半閉鎖型の保護領域における管理の実施状況についてのチェックと必要な見直しの実施

半閉鎖型の保護領域における必要な保護における不手際が見逃されないようにするためには、保護策の妥当性やルールに沿った保護の実施が適切に行われているかどうかについてのチェックと、発見された問題点に対する適切な措置の遅滞のない実施も欠かせない。このことを適切に実行するためには、半閉鎖型の保護領域における保護策の妥当性やその実施状況についてのチェックと必要な見直しの実施要領の確立も必要となる。

特にチェックすべき事項としては、以下があげられる。

- 設備面での閉鎖性の有効性
- 人の出入りに対するルールの励行状態
- 立入りが許される者についての管理の徹底状況
- 立入りが許可された者に交付した認証に用いる情報の管理状況
- 物品の搬入･搬出に対するルールの励行状態
- 閉鎖領域内での立入り者に対する行動監視の実施状況

【対応 ISMS コントロール】

7.1.1 物理的セキュリティ境界
7.1.2 物理的入退管理策
7.1.3 オフィス、部屋及び施設のセキュリティ
7.1.4 セキュリティが保たれた領域での作業
7.1.5 受渡し場所の隔離

Td3.2 半閉鎖型の保護領域における必要な保護の実施

【主旨】

関係者以外の者が立ち入ることは原則として禁止されるものの、Td3.1 で示した閉鎖型の保護領域ほど、関係者外の者の侵入の阻止について厳重な措置がとられていない領域を、半閉鎖型の保護領域と呼ぶ。また、店舗内でも顧客が立ち入ることができる場所等、外部の者が比較的自由に立ち入ることができる領域を開放型の保護領域と呼ぶ。これらの領域においても、情報セキュ

リティの観点から保護すべきものが存在することもある。

このような領域の保護については、閉鎖型の保護とは異なった施策が必要となる（検討すべき事項は、閉鎖型と変わらないが、内容が異なったものとなる）。

【対策のポイント】

（1）対象保護領域ごとの領域保護要件の確立

保護領域を適切に保護するためには、まず、個々の保護領域に対して保護要件を明確にしなければならない。この際の保護要件は、 Td3.1 閉鎖型の保護領域における必要な保護の実施の(1)の表を参考にするとよい。ただし、半隔離型･開放型の領域は、閉鎖型の領域と比較して入退室の制限を緩くすることを前提とした領域であるため、それ以外の保護要件を重点的に考慮すべきである。特に、行動を監視する等により、不正行為や不審な行動の事前の検知･牽制、および、事後の対処に重点を置くのが有効である。

（2）保護領域ごとの管理要領の作成

保護領域の保護が実務上で機能するためには、当該領域の使用や管理の方法が確立していなければならない。管理要領で明確にすべき事項としては、Td3.1 閉鎖型の保護領域における必要な保護の実施の(2)の表を参考にするとよい。ただしこの場合も、半隔離型･開放型の領域の特性を考慮した管理要領にすべきである。

（3）管理要領に沿った管理の実施

管理の対象としては、以下があげられる。

- 立ち入りを許可する者についての管理の実施
- ルールに沿った厳格な入退室管理の実施
- ルールの沿った物品の搬入･搬出の管理の実施
- ルール違反に対する処罰や指導の実施

（4）半閉鎖型の保護領域における管理の実施状況についてのチェックと必要な見直しの実施

半閉鎖型の保護領域における必要な保護における不手際が見逃されないようにするためには、保護策の妥当性やルールに沿った保護の実施が適切に行われているかどうかについてのチェックと、発見された問題点に対する適切な措置の遅滞のない実施も欠かせない。このことを適切に実行するためには、半閉鎖型の保護領域における保護策の妥当性やその実施状況についてのチェックと必要な見直しの実施要領の確立も必要となる。

特にチェックすべき事項としては、以下があげられる。

- 人の出入りに対するルールの励行状態
- 物品の搬入･搬出に対するルールの励行状態
- 保護領域内での立入り者に対する行動監視の実施状況

【対応 ISMS コントロール】

7.1.1 物理的セキュリティ境界
7.1.2 物理的入退管理策
7.1.3 オフィス、部屋及び施設のセキュリティ

7.1.4 セキュリティが保たれた領域での作業
7.1.5 受渡し場所の隔離

Td3.3	社内外に設置する装置や設備に対する必要な保護策の実施

【主旨】

社内に設置されたシステム機器等の装置、及び電源、空調、ケーブル等の関連設備が、いつでも支障なく稼働できる状態を維持するためには、破壊工作や偶発的なことにより容易に破壊されないよう、また災害に対してもある程度の配慮が必要となる。さらに、適切な点検・保守も欠かせない。

一方、店舗外の場所に置かれた銀行の ATM のように、システムの一部としての装置を、誰でもアクセスできるオープンな場所に設置しなければならないこともある。このように、外部の者が自由にアクセスできる場所に設置する装置については、社内に設置する装置以上に、災害や不慮の事故に加え、破壊工作、盗難及び不正な使用に対する配慮が必要となる。

また装置の保護については、設置時・稼動時だけでなく、その移動においても十分な配慮が必要となる。装置の移動における事故を防ぐためには、移動が想定される重要な装置についての移動要領の確立と、規程に沿った移動の実施が必要となる。

【対策のポイント】

⑴ 設置環境面での配慮

装置や関連設備の設置に際しては、災害や不慮の事故に対する配慮が必要である。検討対象としては、表 3-64 に示すようなものがあげられる。

表 3-64 装置や関連設備の設置環境についての検討事項

No	項目	内容等
1	火災対策	・防火区画の設置 ・煙感知器、火災検知器、消化設備の設置と保守
2	地震対策	・耐震構造または免震構造の建物への設置 ・移動、転倒及び振動防止の措置
3	水災対策	・水災の可能性のある場合における防水対策 - 漏水検知器 - 防水カバーの常備 - 漏水・浸水の可能性ある場所への機器設置制限

⑵ 配置や据付上の工夫実施

電源、空調装置、電源ケーブル等の付帯設備の据付にあたっては、地震、火災、水害等の災害や、人的な要因による思わぬ事故に見舞われないよう、表 3-65 に示すような点についての配慮が必要となる。

表 3-65　装置や関連設備の配置や据付上での必要な配慮

No	項目	内容等
1	設置場所	･水害や火災の類焼被害の可能性の極小化 ･外部からの工作がしにくい場所 ･保守が困難にならない場所
2	設置方法	･地震や不慮の出来事による倒壊や破損の防止 ･保守を困難にしない設置

(3) 必要に応じた堅牢性の補強策の適用

特に重要な設備や機器、あるいは保護が行き届かない外部設置の機器等については、必要に応じ、外装の強化等の物理的な補強策の適用も必要となる。機器等の堅牢性の確保について検討すべき事項としては、以下があげられる。

- 破壊工作を意識した物理的補強策の適用 (保護カバーの設置等)
- 盗難防止策の適用
- 物理的な工作や盗難行為に対する警報機能の組込み
- 不正使用の検出機能の組込み
- 監視機能の組込み

(4) 定期的な予防保守の実施

社内の設備や機器の安定稼働を期待するためには、それぞれの設備や機器に指定された予防保守を怠ってはならない。また、必要に応じたリニューアルも適切に行わなければならない。一方、社外に置かれた設備の安全を確保し、安定稼動を保証するためには、その設置状況についての定期的な点検が欠かせない。これらを適切に行うためには、以下の実施が必要である。

- 社外設置機器の設置状況のチェック要領の確立
- 規程に沿った設置状況のチェックの実施と必要な改善措置の遅滞のない実施

(5) 装置の移動要領の確立

装置の移動についての要領で規定すべき事項としては、表 3-66 に示すようなものがあげられる。

表 3-66　装置の移動について規制すべき事項

No	項目	内容等
1	管理対象	･移動が管理の対象となる装置と移動区間
2	移動の手続き	･承認手続き ･実施手順 (含む報告) ･移動記録の取得
3	移動にあたって実施すべき保護策	･事故による破損の防止策 (梱包等についての要求) ･盗難防止 (輸送手段についての要求) 　－輸送ルート 　－使用業者 　－紛失や盗難事故への備え (情報の暗号化他)
4	事故発生への備え	･バックアップの準備 ･事故処理の手続き

(6) 規程に沿った装置の移動の実施

管理の対象となる装置の移動は、指定された規程に沿って行われなければならない。装置の移

動にあたって遵守すべき事項としては、以下があげられる。

- 定められた手続きに沿った装置の移動の実施
- 装置の移動における保護策の実施
  ・移動途中での破損の防止策の実施
  ・移動途中での紛失及び盗難の防止策の実施

⑺ 施設や設備に対する保護策の実施状況についてのチェックと必要な見直しの実施

施設や設備の保護における不手際が見逃されないようにするためには、保護策の妥当性やルールに沿った保護の実施が適切に行われているかどうかについてのチェックと、発見された問題点に対する適切な措置の遅滞のない実施も欠かせない。このことを適切に実行するためには、施設や設備に対する保護策の実施状況についてのチェックと必要な見直しの実施要領の確立も必要となる。

【対応 ISMS コントロール】

7.2.1 装置の設置及び保護
7.2.2 電源
7.2.3 ケーブル配線のセキュリティ
7.2.4 装置の保守
7.2.5 事業敷地外における装置のセキュリティ
7.3.2 資産の移動

3.4.4. セキュリティ事故への備え

Td4.1	異常検知時における即応能力の確保

【主旨】

システムへの侵入やウイルス感染の兆候が見られたり、システムに異常な動きが見られたりと言ったような、システムの利用や運用において何らかの異常が見られた場合、適切な措置が迅速に行われれば、事故への発展を防いだり、被害の拡大を防ぐこともできる。このため、システムの運用を担当するものだけでなく、システムの利用者や業務現場にも、このような事態において、適切な対応を迅速に行えるようしておくことも、セキュリティ事故への備えの一つとして重要となる。

【対策のポイント】

⑴ システムの異常発見時の対応要領の確立

システムの動きや取り扱う情報等に異常を検知した者が適切な対応を迅速に行えるようにするためには、このような事態に対処するための対応要領が確立していることが必要となる。

システム等の異常発見時の対応要領として示しておくべき事項としては、以下があげられる。

- システムの利用者が注意すべき事象
- 状況に応じた、異常を感知した場合のネットワークの遮断等の必要となるとっさの処置とその実施方法
- 状況に応じた、状況の把握や記録の方法
- システム管理者等への報告方法

(2) これらの関係者への周知

異常発見時の対応要領が確立していても、これらが関係者に周知されていなければ、必要な対応は期待できない。これらを関係者に周知させるためには、以下のような施策も必要となる。

- 実施要領の配布
- 実施要領が求めていることについての教育の実施

【対応 ISMS コントロール】

11.1.1 事業継続管理手続き
11.1.2 事業継続および影響分析
11.1.3 継続計画の作成および実施
11.1.4 事業継続計画作成のための枠組み
11.1.5 事業継続計画の試験、維持、および再評価

Td4.2	システム周りのセキュリティ事故への対応能力の確保

【主旨】

システム周りにセキュリティにかかわる事故が発生した場合は、その影響が拡大することを阻止するとともに、情報の回復やシステムの復旧の迅速な実現に加え、業務面に及んだ影響に対する措置等を適切に行うための影響範囲の迅速な特定も必要となる。

また、システム周りに発生したトラブルがセキュリティ事故に結びついた原因の追求と、再発防止も迅速に行われなければならない。

これらのことが適切かつ円滑の行われるためには、以下に示すような多方面からの準備が必要となる。

- セキュリティ事故の処理についての全体的なフレームワークの確立
- 事故種別ごとの事故処理要領の確立
- セキュリティ事故の処理に必要なシステム環境の整備
- 関係者における事故処理対応能力の確保

【対策のポイント】

(1) セキュリティ事故の処理についてのフレームワークの確立

セキュリティ事故への対応を円滑に進めるためには、セキュリティ事故が発生した場合、どのよ

うな体制で、どのような手順で対策を進めるかといった、事故処理についての全体的なフレームワークが確立していることが必要となる。セキュリティ事故の処理を円滑に進めるためのフレームワークとして明確にしていくべき事項としては、以下があげられる。

- 事故処理の体制
- 事故処理の基本手順
- 実施すべき事後処理

事故発生時の処理の手順を示すセキュリティ事故の処理についてのフレームワークにおいて示すべき事項を、表 3-67 に示す。

表 3-67 セキュリティ事故の処理についてのフレームワークとして示すべき事項

項番	定義項目	内容
1	事故処理体制	・ 事故処理の責任者 ・ 事故の状況に応じた事故処理チームの動員手順編
2	事故処理手順	・ 事故発生の認知から関係する事故処理単位に計画された事故処理の実行開始に至るまでの活動とその手順(注)
3	事故の後処理	・ 再発防止策の評価 ・ 事故処理経緯の整理要領 ・ 事故処理の報告要領 ・ 関係機関への報告要領

(2) 事故原因別の事故処理要領の確立

被害状況の確認や、情報の回復や、業務の再開等の事故処理は、事故の種別によって異なる。事故処理を適切にかつ円滑に行うためには、以下に示すような事故の種別ごとに対象要領を確立しておかなければならない。

- システムの不正使用発生時の対処要領
- システムの処理に誤処理が発生した場合の対象要領
- システムに障害事故が発生した場合の対処要領
- システム性能事故が発生した場合の対処要領
- 不正アクセスが検知された場合の対処要領
- ウイルス感染が検知された場合の対処要領
- システム情報やセキュリティ制御情報に関する事故が発生した場合の対処要領
- 業務情報の保護に関する事故が発生した場合の対象要領
- 通信にかかる事故が発生した場合における対象要領
- 保管電子情報の保護にかかる事故が発生した場合における対象要領
- システムの運用環境に保全に関わる事故が発生した場合における対処要領

それぞれの事故種別ごとに作成すべき事故処理要領で明確にすべきことを、表 3-68 に示す。

表 3-68　事故種別ごとに確立すべき事故処理要領で定義すべき事項

項番	定義項目	内容
1	事故処理単位の名称	・ 当該事故処理に単位につける名称
2	当該事故に対する基本方針	・ 被害の重要度について 　－業務や事業への影響の度合い 　－二次被害の可能性 ・ システム（含むデータ）の回復についての要件 　－データ等の必要な回復のレベル 　（完全な修復、完全な修復を求めない場合における情報の喪失が許される範囲）（注1） ・ 業務（サービス）の復旧についての要件 　－業務（サービス）中断時間の許容値 　－制限付での業務の再開を行う場合その条件
3	対象となる事故	・ 想定される攻撃の種類とそれぞれの特性（被害の形態やその範囲）
4	事故処理体制	・ 当該事故の処置についての責任者 ・ 事故処理の対応に参加すべきメンバーまたは組織
5	事故処理の手順	・ 事故発生を確認した時からすべての処理が終わるまでの手順
6	サービスの停止に関する処置	・ ファイルの公開停止やサービスの一時停止等の暫定処置の要否についての考え方 ・ サービス停止の手順
7	関係者への事故発生の連絡	・ 連絡が必要な先 ・ 連絡すべき事項 ・ 連絡方法
8	事故の内容と被害範囲の特定	・ 事故原因の特定 ・ 発生した事故の特性（被害の形態や想定される被害の範囲の確認 ・ ファイル等のチェックによる被害範囲や被害の状況の確認
9	システムの回復	・ 回復対象の個々に対する回復方法 ・ 回復手順 ・ 回復結果の確認
10	業務（サービス）の復旧	・ 業務（サービス）の復旧手順 ・ 復旧の確認 ・ 関係者（利用者も含む）への連絡
11	二次被害の調査と必要な対策	・ 想定される二次被害 ・ 想定される二次被害に対する調査方法 ・ 二次被害の調査の実施と被害状況の確認 ・ 二次被害に対する対処要領
12	原因の分析と再発防止策の検討と実施	・ 事故発生を許した原因の特定 ・ 再発防止策の検討とセキュリティ対策への反映
13	事故処理の経緯の記録	・ 記録すべき事項
14	事故処理の報告	・ 報告者と報告先および報告内容 ・ 関係機関への報告要領

(3) 被害範囲の調査や情報の回復およびシステムの復旧のためのツールの整備

発生したセキュリティ事故への対応を円滑に行うためには、一般に、以下が必要となる。

- 被害範囲の調査や情報の回復およびシステムの復旧のためのツール
- 情報の回復を行うためのバックアップ
- 被害範囲の特定や事故に結びついた原因の調査等のための運用の記録
- 予備のサーバや記録媒体等の事故処理を進めるために必要となるリソース

これらの備えが十分でなければ、事故処理は混乱し被害を拡大することになる。これらが適切に準備されるためには、セキュリティ事故への対応で必要となるものが明示され、日常の業務の運用やシステムの運用のなかでこれらが適切に準備されるようになっていなければならない。

事故処理に使用するツールは、期待通りに機能することが確認されていなければならない。開発当初は問題がなくても、システム環境の変化により、いざという時に動作できないこともよくあるので注意が必要となる。このため、本要求については、以下が必要となる。

- 事故処理の方針に沿った設計レビューの徹底
- 開発時点における実装の的確性の確認の徹底
- 定期的な動作確認の実施

(4) 情報の回復を行うためのバックアップの取得と管理

確保すべきバックアップの個々に指定する取得とその保管についての要件の定義おいて定義すべき事項を、に示す。

表 3-69　バックアップの取得･保管要件における定義事項

項番	定義項目	内容
1	取得サイクル	・ バックアップを取得すべき時点 ・ 取得の範囲
2	取得方法	・ 取得媒体 ・ 取得に用いる技術･機能 ・ 取得バックアップの妥当性に確認についての要求
3	保管についての要件	・ 二重化についての要求 ・ 保管場所についての要求 ・ 保管世代
4	取得および保管についての記録	・ 記録事項 ・ 記録の管理方法

(5) 被害範囲の特定や事故に結びついた原因の調査等のための運用の記録の取得と保管

事故によっては、被害範囲の特定や事故原因の調査に、システムや業務の運用の記録も必要となる。想定される事故の処理に必要となるシステムや業務の運用の記録は、日々のシステムや業務の運用の中で確実に確保されるようになっていなければならない。このためには、以下が必要となる。

- 実用な記録の作成要領や保管要領等の運用の記録作成･保管についてのルールの確立
- ルールに沿った記録の作成と保管の実践を管理する仕組みの確立
- システム運用現場や業務運用現場におけるルールに沿った記録の作成と保管の実践の徹

底

(6) 予備のサーバや記録媒体等の事故処理を進めるために必要となるリソースの確保

事故処理では、バックアップデータからの情報の回復他で、日常の運用では必要のないリソースも必要となる。準備した事故処理のプロセスにあわせたリソースの確保に手違いがないようにしなければならない。

(7) 関係者におけるセキュリティ事故への対応能力の確保

事故処理要領が定められ、事故処理のためのシステム的な環境が整備されていても、事故処理に当たる者に、必要な行動を適切かつ迅速に実行できる能力が備わっていなければ、事故処理計画は機能しない。

このためには、事故処理に当たる者は、何時どのような事故が発生したとしても、必要な対応が取れるよう訓練されていなければならない。

これらの達成のためには、以下が必要となる。

- 事故処理に関係する者に必要となるスキルの明確化
- 事故処理を担当する者に対する事故処理手順についての教育の実施
- 定期的な事故処理訓練の実施

事故処理は日常的なものでないため、不慣れから事故処理に不手際がでないよう、定期的に事故処理訓練を行い、事故処理に関わるの者に事故処理に慣れさせるとともに、必要なスキルの確実な取得を図ることも必要となる。

事故処理訓練は、多くの項目からなるなるだけでなく、実施は運用に大きな影響も与えるため、十分な計画と準備が必要となる。事故処理訓練を適切に行うためには、以下が必要となる。

・年間を通じた事故処理訓練計画の確立

・訓練テーマごとの実施要領の確立

なお、事故処理訓練の実施要領としては、以下を明確にしていくことが必要となる。

－事故処理訓練のシナリオ

－事故処理訓練のための環境の整備

－訓練終了後の運用環境の回復

【対応 ISMS コントロール】

11.1.1 事業継続管理手続き

11.1.2 事業継続および影響分析

11.1.3 継続計画の作成および実施

11.1.4 事業継続計画作成のための枠組み

11.1.5 事業継続計画の試験、維持、および再評価

Td4.3	セキュリティ事故が業務面に影響した場合の対処要領の確立と関係者への徹底

【主旨】

システム周りあるいは業務現場等で発生したセキュリティにかかわる問題が、セキュリティ事故に発展した場合、情報の漏洩とか取引うえの誤処理等の業務面に影響が出ることも少なくない。このような場合、システム的な対応等の社内的な対応だけでなく、外部に対する後処理も必要となる。

これらを、迅速かつ適切に行われるようにするためには、想定される事故についての対外的な処置も確立し、必要な場合、それが機能するようにしておくための準備も必要となる。

【対策のポイント】

⑴ 影響を及ぼした他社への対応

システムの誤処理や個人情報の漏洩等で、情報のセキュリティ事故が外部に影響を及ぼした場合は、自社側の対策だけでなく、影響を与えた外部への対応も必要となる。この対応が不手際であれば、問題を大きくしかねない。セキュリティ事故に際して、影響を与えた外部への対応を適切に行うためには、事故のタイプごとに、他社との対応要領を予め検討しておくことも重要となる。

この場合、明確にすべき事項としては、以下があげられる。

- 処理の方針
- 責任体制
- 処理手順
- 実施にあたっての留意事項

⑵ 社外への発表

事故によっては、社会に広くその実態を発表せざるをえないことも考えられる。このような事態を想定した、社外への発表の要否や、必要なな場合における実施要領を定めておくことも必要となる。

【対応 ISMS コントロール】

11.1.1 事業継続管理手続き
11.1.2 事業継続および影響分析
11.1.3 継続計画の作成および実施
11.1.4 事業継続計画作成のための枠組み
11.1.5 事業継続計画の試験、維持、および再評価

Td4.4	セキュリティ事故への対応に必要なシステム環境の整備

【主旨】

セキュリティ事故発生時における必要な対応の適切な実行には、これらの対応に必要なシステム環境が、必要な時点にいつでも使える状態が確保さえていなければならない。このためには、必要な設備やツールの整備、バックアップ情報の確保等に不手際がないようにしなければならない。

【対策のポイント】

(1) セキュリティ事故の対応に必要な技術環境の整備とその維持

セキュリティ事故への対処に必要な機器やツールについては、常に、何時でも使用できる状態におかなければならない。このためには、必要な機器や機能のシステムへの的確な組込みと、それらについての定期的な動作確認も欠かせない。対象となる設備やツールとしては、以下があげられる。

- バックアップ用の機器
- 情報の回復用のツール
- システムに組込んでいるシステム復旧用の機能
- 被害範囲調査用のツール
- 処理のトレースツール等原因の分析用のツール
- セキュリティ事故の処理に必要なバックアップ情報や運用の記録の確保
- セキュリティ事故の処理に必要な技術環境の整備についての仕組みの整備

セキュリティ事故の処理に必要な技術環境の整備に手落ちがないようにするためには、これらにかかわる活動を管理する仕組みの確立も必要となる。

この管理の仕組みとして検討すべき事項としては、以下があげられる。

- セキュリティ事故の処理に必要な技術環境の整備要領の策定
  - ･対象事項とその妥当性の確認要領
  - ･日常の運用で実行すべき事項の実行要領とそのチェック要領

(1)　準備事項の妥当性やその機能の保全状況についての定期的なチェック要領

【対応 ISMS コントロール】

11.1.1 事業継続管理手続き
11.1.2 事業継続および影響分析
11.1.3 継続計画の作成および実施
11.1.4 事業継続計画作成のための枠組み
11.1.5 事業継続計画の試験、維持、および再評価

Td4.5	システムの長期停止への備え

【主旨】

システムには、災害による施設やシステム機器や業務ソフトや業務データの損壊や、システムにおける思わぬ重大事故等で、短期間でのシステムの復旧の目処がたたなくなるような事態の発生の可能性も考慮に入れなければならない。このような事態においても、事業の継続ができるようにするためには、バックアップセンターの準備や、ソフト資産や業務データの安全な保管、あるいは手作業により業務の遂行ができるようにしておく準備も必要となる。事業運営の多くを情報システムに依存している組織においては、この問題は特に重要である。

【対策のポイント】

(1) 業務毎の重要度や、情報システムのトラブルが業務に及ぼす影響の把握

(2) 情報システムも長期の停止に対する事業継続計画の確立

情報システムの停止が長期に及ぶような場合を想定したにおける事業継続計画は、業務毎の重要度や、情報システムのトラブルが業務に及ぼす影響に着いての判断にのっとったものでなければなりません。また、この計画は、非常時における貴社の事業活動を大きく左右するもののので、経営陣も承認したものでなければならない。

情報システムも長期の停止に対する事業継続計画に関し、重要な検討事項としては以下があげられる。

- 必要とする業務の継続のレベル
- 必要とする業務の継続を実現するための仕組み
- バックアップセンターの要否と必要とする場合のその機能範囲と運営形態
- 必要とする業務の継続を実現するために必要となる設備やシステムの大枠
- 必要とする業務の継続を実現するために必要となる日頃からの準備すべき事項の大枠

(3) バックアップセンターを利用する場合、バックアップセンターへの切替えの準備

バックアップセンターを利用する場合、バックアップセンターへの業務の切替えが円滑に行われるようにするためには、日頃から、以下のような備えが必要となる。

- バックアップセンターシステムの確保
- バックアップセンターへの切替え要領の確立
- バックアップセンターに業務を切替るために必要となる機能やツールの準備
- バックアップセンターへの切替えに関わる要員に対する教育や訓練による対応能力の確保

(4) バックアップセンターへの切替時や修復後のセンターでの業務の再開始に用いる業務データやソフトの安全な場所での保管

また、このような事態においては、現用の業務データも失われていることも多いいため、日常のシステム運用の中で、バックアップセンターへの切替時や修復後のセンターでの業務の再開始に用いる業務データやソフトを他の安全な場所で保管するようにしておくことも必要となります。

(5) 非常時における手作業での業務の遂行の準備

バックアップセンターへの切替を準備しない場合や、バックアップセンターへの切替えが旨く行かない場合は、業務を手作業に切り替えなければなりません。手作業に切替えて情報システムに頼っていた業務処理を行えるようにするためには、日頃から、以下のような備えが必要となります。

- 手作業での業務処理要領
- 手作業での業務の遂行時の体制やオフィスの使用方法等の検討
- 手作業での業務に用いる台帳等の必要な情報の日頃からの準備

【対応 ISMS コントロール】

11.1.1 事業継続管理手続き
11.1.2 事業継続および影響分析
11.1.3 継続計画の作成および実施
11.1.4 事業継続計画作成のための枠組み
11.1.5 事業継続計画の試験、維持、および再評価

【参考】

社会の仕組みの中で重要な位置づけを占めているシステム等、システムによってはシステムの復旧に長時間かけられないものもある。また、災害等で情報の回復やシステムの復旧が困難になった場合、社会的な責任のまっとうだけでなく、事業の継続が困難になることも考えられる。

このように、どのような事態になっても、社会的な責任を持つサービスの提供や事業の継続に致命的な影響が出ないようにするためには、バックアップセンターの準備も検討の対象となる。

本要求は、このバックアップセンターの要否の判断も含め、必要な場合の、その適切な準備を問うものである。

4. アシュアランス･ビュー

4.1. セキュリティ対策の実施状況の評価

4.1.1. 監査手法による対策状況のチェック

Aa1.1	セキュリティ監査実施環境の整備

【主旨】

セキュリティ監査を実効性のあるものにするためには、監査についての基本的な方針、実施の方法、評価基準等の確立等の監査活動が円滑に機能するための環境整備が必要となる。

【対策のポイント】

(1) 監査基本方針の確立

組織的、戦略的な監査の実現には、セキュリティ監査についての基本方針が明確にされていることが望ましい。セキュリティ監査の方針で明確にすべきこととしては、以下のようなものがある。

- 監査の狙いや範囲
- 監査の権限と責任
- セキュリティ監査の組み立て

規模が比較的大きいシステムにおいては、監査はシステム全体に対して総合的に行うとは限らない、テーマごとに必要に応じ、対象テーマに沿って実施することが実務的かつ効果的であろう。このため、まず、以下のようなことを検討し、セキュリティ監査の組立てを確立することも必要となる。

･セキュリティ監査の実施単位の組み立て

･個々の実施単位における監査のテーマと対象となる組織やシステムの範囲

- 監査の実施形態（それぞれの監査単位における実施サイクルや実施方法や監査の体制の大枠等）

(2) セキュリティ監査の実施単位ごとの監査実施基準の確立

セキュリティ監査が計画的かつ効果的に行われるようにするためには、監査を計画するにあたってのベースを示す監査の実施基準を、監査の実施単位ごとに確立しておくことも欠かせない。監査実施基準で示すべきこととしては、表 4-1 に示すようなものがある。

表 4-1 セキュリティ監査の実施単位ごとに作成する監査実施要領で示すべき事項

区分	監査実施要領としての指定事項
監査対象領域	･対象の職場 ･対象とするシステムの範囲
監査テーマ	･監査の狙い ･評価のポイント
実施サイクル	･定期監査の実施サイクル

	･臨時監査の実施が必要となる状況
監査実施についての基本方針	･監査の形態 －外部監査、内部監査（自社の監査部門による監査、関係部門内での監査） ･監査の実施方法の大枠 ･監査体制の大枠
適用する評価基準	･当該監査において評価事項の設定基準と判定基準等
監査のために必要となるもの	･監査における評価のために提示すべき記録等で、日常の業務やシステムの運営の取得保管すべき記録とその取扱い
報告要領	･報告書の様式 ･承認ならびに報告先

(3) 監査体制の整備

組織的な監査の実施には実施体制の整備も欠かせない。実施体制の整備において検討すべき事項には、以下のようなものがある。

- 監査チームの編成
- 監査関係者に対する必要なスキルの確保
- 監査の外部への委託や外部スタッフとの連携の確立

【対応 ISMS コントロール】

4.1.7　情報セキュリティの他者によるレビュー
12.2.1 セキュリティ基本方針との適合性
12.2.2 技術適合の検査
12.3.1 システム監査管理策
12.3.2 システム監査ツールの保護

【参考】

監査の実施単位はセキュリティ対策の組立ての沿うのが分かり易い。本評価モデルでは、対策ドメインを一つの監査実施単位とすることを推奨する。

Aa1.2　対策ドメインごとの対策の実施状況についての監査の実施

【主旨】

必要なセキュリティ監査は、セキュリティ監査についての基本方針や実施要領に沿って実施されなければならない。個々のセキュリティ監査が適切に実施されるためには、監査の実施単位ごとに、実施計画の策定し、十分な準備の下で行わなければならない。また、監査の実施にあたっては、関係部門の協力が欠かせない。

【対策のポイント】

⑴ 監査実施計画の策定

監査目的を有効かつ効率的に達成するためには、個々の監査ごとに監査実施計画を策定する必要がある。実施すべき監査手続の内容や実施時期, 範囲および担当者などを監査実施計画書で明確にすることによって、限られた期間と監査人で効率的に監査を実施することができる。

監査実施計画の策定にあたって検討すべき事項としては、表 4-2 に示すようなものがある。

表 4-2　監査実施計画の策定にあたって検討すべき事項

項目	内容
監査対象領域	･対象の職場 ･対象とするシステムの範囲
監査テーマ	･監査の狙い ･評価のポイント
実施スケジュール	実施期間他
監査実施要領	･監査体制 ･受査側の体制および必要な準備 ･聞き取り場所や立入りチェックを行う場所 ･監査手続き -必要情報の収集方法 -監査調書の作成
監査項目	監査項目 ･見届けるべきこと ･確認すべき情報や記録 個々の監査項目における評価基準
監査のために必要となるもの	監査における評価のために提示すべき記録等で、日常の業務やシステムの運営の取得保管すべき記録とその取扱い
報告要領	･報告書の様式 ･承認ならびに報告先

(注 1)

監査手続は, 監査計画書に記載された各監査項目について, 具体的にどのような方法で実施するかを明確にしたものである。監査手続書には, 監査項目をブレイクダウンした監査チェックポイント, 適用すべき監査手法(レビュー, インタビュー, 視察など), 収集すべき証拠資料などを記載する。収集すべき証拠資料を事前に想定することによって, 監査の実施において具体的に何をレビューしたり, ヒアリングしたりすればよいかが明確になる。さらに, 設定する監査チェックポイントの漏れや重複をチェックすることにも役立つ。

監査手続書を作成することによって, 監査手続の重複や漏れ, 証拠資料の過不足を防ぐことができ, 監査の品質を確保するうえで重要なマニュアルとなる。また, 監査手続書にもとづいて監査を実施することにより, 効率よく監査を実施することができる。

(注2)

監査調書とは, 監査の計画, 実施および報告の各過程で監査人が作成した記録, 被監査部門から入手した証拠資料をとりまとめたものなどである。監査調書は, 監査報告書を作成する際の基礎資料となるものである。監査調書は, 監査人が専門家としての相当な注意を払って監査を実施し, 監査目的に適合した監査意見を表明するために不可欠な資料である。したがって, 監査人が実施したプロセスや監査結果などを正確に記録するとともに, 適切な方法によって整理し, 保存する必要がある。

⑶ 監査の実施

策定した監査計画に沿って監査単位ごとの監査を、定期的に実施する。

⑷ 監査結果の評価と報告

- 監査結果の評価と監査報告書の取り纏め

  あらかじめ策定した評価基準を参考に、実態に対する適切な評価を行い、問題点の指摘と改善についての提言を、監査報告書に纏める。

  監査報告書は，監査人が実施した監査の結果をとりまとめたもので，監査人の意見を表明したものである。したがって，監査報告書は，監査業務のなかでも最も重要な成果物であり，最終成果物である。また，経営者や被監査部門などに監査結果を報告する際の文書でもある。そこで，実施した監査の内容および結果が正確に伝わるよう，監査報告書の作成には細心の注意を払う必要がある。

- 監査結果のの経営陣への報告と承認

  監査結果は経営陣に報告され、セキュリティ対策の実施状況について正確な理解をもらうとともに、その評価や必要な指示を受けなければならない。

(5) 指摘事項に対する改善対応の指示

監査で提起された事項は、そのすべてについて、適切な改善が迅速に実施されなければならない。このためには、以下のステップを踏まなければならない。

- 指摘事項に対する対応策の検討
- セキュリティ対策への反映計画の作成（実施のタイミングや実施の手順等）
- 計画にもとづきた改善策の実施
- 改善措置の実施についての報告

(4) 改善対応状況の管理（フォローアップ）

監査で指摘されたことが放置されたままになってしまうようなことを避けるためには、以下も必要となる。

- 指摘事項に対する対策消化状況
- 実施済みの対策の実効状況の確認

【対応 ISMS コントロール】

4.1.7　情報セキュリティの他者によるレビュー
12.2.1 セキュリティ基本方針との適合性
12.2.2 技術適合の検査
12.3.1 システム監査管理策
12.3.2 システム監査ツールの保護

Aa1.3	監査結果の評価報告とフォローアップの実施

【主旨】

セキュリティ監査が実施されても、監査結果の報告が適切になされ、監査指摘事項の改善が適

切に実施されなければ、監査の意味はない。監査を意味あるものにするためには、実施したセキュリティ監査についての適切な報告、ならびに監査指摘事項に対する必要な改善措置の実施のフォローは欠かせない。。

【対策のポイント】

(1) 監査結果の評価と報告

- 監査結果の評価と監査報告書の取り纏め

  あらかじめ策定した評価基準を参考に、実態に対する適切な評価を行い、問題点の指摘と改善についての提言を、監査報告書に纏める。

  監査報告書は，監査人が実施した監査の結果をとりまとめたもので，監査人の意見を表明したものである。したがって，監査報告書は，監査業務のなかでも最も重要な成果物であり，最終成果物である。また，経営者や被監査部門などに監査結果を報告する際の文書でもある。そこで，実施した監査の内容および結果が正確に伝わるよう，監査報告書の作成には細心の注意を払う必要がある。

- 監査結果のの経営陣への報告と承認

  監査結果は経営陣に報告され、セキュリティ対策の実施状況について正確な理解をもらうとともに、その評価や必要な指示を受けなければならない。

(2) 指摘事項に対する改善対応の指示

監査で提起された事項は、そのすべてについて、適切な改善が迅速に実施されなければならない。このためには、以下のステップを踏まなければならない。

- 指摘事項に対する対応策の検討
- セキュリティ対策への反映計画の作成(実施のタイミングや実施の手順等)
- 計画にもとづきた改善策の実施
- 改善措置の実施についての報告

(3) 改善対応状況の管理(フォローアップ)

監査で指摘されたことが放置されたままになってしまうようなことを避けるためには、以下も必要となる。

- 指摘事項に対する対策消化状況
- 実施済みの対策の実効状況の確認

【対応 ISMS コントロール】

4.1.7　情報セキュリティの他者によるレビュー
12.2.1　セキュリティ基本方針との適合性
12.2.2　技術適合の検査
12.3.1　システム監査管理策
12.3.2　システム監査ツールの保護

4.1.2. 技術的な診断によるセキュリティ対策の欠陥のチェック

Aa2.1	診断ツールによるシステムの脆弱性診断要領の確立

【主旨】

診断ツールを用いたシステムの脆弱性診断は、手間やコストがかかるため、実効性を高い診断を効率的に行うためには、その狙いや対象とするシステムの範囲や、診断する事項の選定に加え、診断の実施にあたって必要となる準備や、実施後の評価の手順等についての十分な検討が必要である。

効果的なシステムの脆弱性診断を効率的に行うためには、これらについての検討結果を纏めた実施要領の確立が欠かせない。

【対策のポイント】

(1) 基本方針の確立

技術的な診断によるシステムの脆弱性診断を実効性のあるものにするためには、脆弱性診断についての基本方針が明確にされていることが望ましい。この基本方針で明確にすべきこととしては、以下のようなものがある。

- 対象システムの範囲 (対象セグメントやサーバ等)
- 診断テーマ (診断の対象とする脆弱性群)
- 診断の実施サイクル
- 診断の手段、使用するツールや必要なシステム環境
- 実施体制 (責任体制た外部への委託を行う場合は委託の範囲の大枠等)

(2) 診断テーマごとの診断実施要領の確立

脆弱性診断が効果的に行われるようにするためには、表 4-3 に示すようなことを明確にした脆弱性診断の実施要領を確立しておかなければならない。この実施要領は、診断テーマごと作成されなければならない。

表 4-3 脆弱性診断の実施要領として検討すべき事項

項目	内容
監査対象領域	・対象とするネットワークセグメント ・対象となるサーバやクライアント等のシステム構成機器
診断事項	・診断で摘出を狙う脆弱性 (診断テーマによって異なる) 注1:【参考】参照
実施サイクル	・定期的な診断のサイクル ・臨時の実施を必要とする場合
監査のために必要となるもの	・使用するツールと使用する機能 ・システムへの実装方法
監査実施要領	・事前に準備すべきことと準備の手順 ・診断の開始、終了方法 ・診断データの収集と評価 (評価基準等) 方法 ・収集情報の保管方法 ・診断結果の集約と報告書の取り纏め方法

報告要領	･報告書の様式 ･承認ならびに報告先

(3) 実施体制の整備

技術的な診断によるシステムの脆弱性の診断には、専門的な知識やスキルを必要とする。このため、実施体制の整備も欠かせない。実施体制の整備において検討すべき事項には、以下のようなものがある。

- 監査チームの編成
- 監査関係者に対する必要なスキルの確保
- 監査の外部への委託や外部スタッフとの連携の確立

【対応 ISMS コントロール】

12.2.1 セキュリティ基本方針との適合性
12.2.2 技術適合の検査
12.3.1 システム監査管理策
12.3.2 システム監査ツールの保護

【参考】

システムの脆弱性診断についての代表的なテーマを、表 4-4 に示す。

表 4-4 システムの脆弱性診断における代表的な診断テーマ

検査対象機器		代表的な検査項目
ネットワーク制御機器	ルータ	･不要なポートの開放 ･アクセス制御の不備（本来許可すべきではないネットワークへアクセス） ･ファームウエアに存在する脆弱性（OSPF や SNMP の処理に起因するサービス妨害攻撃に対する脆弱性他）
	ファイアウォール	･不要なポートの開放 ･アクセス制御の不備（本来許可すべきではないネットワークへアクセス） ･アプリケーション部分に存在する脆弱性（サービス妨害攻撃に対する脆弱性他）
	プロキシ	･不要なポートの開放 ･アクセス制御の不備（本来許可すべきではないネットワークへアクセス） ･アプリケーション部分に存在する脆弱性（認証機能の不具合による認証バイパスの可能性やバファオーバーフローの可能性）
サーバ	OS 等のプラットフォーム部分	･デフォルト設定による不要プロセスの稼動 ･不要なアカウントの存在（長期間ログインしていないアカウントや、テスト用のアカウント、退職者のアカウントの存在等） ･脆弱なパスワード ･セキュリティパッチの未適用 ･デフォルト設定による運用（r 系サービスや PPC プログラム等の多くの脆弱性の存在が確認されているサービスを放置する運用等）

	Web サーバ	・不要なポートの開放 ・セキュリティパッチの未適用 ・不要なメソッド（機能）の有効化 ・独自開発ソフトにおける CGI による OS・SQL コマンドインジェクションやクロスサトスクリプティングに関する脆弱性の存在
	DNS サーバ	・セキュリティパッチの未適用 ・ゾーン転送のアクセス制御の不備 ・再帰的問合せの許可範囲
クライアント	Windows クライアント	・不要なポートの開放 ・セキュリティパッチの未適用 ・不要なアカウントの存在（長期間ログインしていないアカウントや、プログラムが自動的にインストールしたアカウント等） ・不要な共有フォルダーの存在（以前に使用したものが放置されているフォルダーやアクセス制限が掛けられていないフォルダー等） ・ローカルセキュリティ（グループ）ポリシーの不備（パスワードの強度やロックアウトにかかわる設定値等）

Aa2.2 診断ツールを用いたシステムの脆弱性診断の実施

【主旨】

診断ツールを用いたシステムの脆弱性診断は、脆弱性診断についての基本方針や実施要領に沿って実施されなければならない。脆弱性診断が適切に実施されるためには、診断の実施単位ごとに、実施計画の策定し、十分な準備の下で行わなければならない。また、診断の実施にあたっては、関係部門の協力が欠かせない。

また、結果の纏めや、指摘事項に対するフローアップも適切に行わなければ、診断の実効性は失われる。

【対策のポイント】

脆弱性診断の目的を有効かつ効率的に達成するためには、個々の診断テーマごとに診断の実施計画を策定する必要がある。脆弱性診断の実施計画の策定にあたって検討すべき事項としては、表 4-5 に示すようなものがある。

表 4-5 脆弱性診断の実施計画の作成上で検討すべき事項

項目	内容
診断対象領域	・対象とするネットワークセグメント ・対象となるサーバやクライアント等のシステム構成機器
診断事項	・診断で摘出をねらう脆弱性（診断テーマによって異なる）
実施時期	・実施日と実施時間帯
診断のために必要となるもの	・使用するツールと使用する機能 ・システムへの実装方法
監査実施要領	・事前に準備事項 ・診断の開始と終了要領 ・診断データの収集と評価方法 ・収集情報の保管 ・診断結果の集約と報告書の取り纏め

報告要領	･報告書の様式 ･承認ならびに報告先

(3) 監査の実施

策定した診断の実施計画に沿って、診断単位ごとの診断を実施する。

(4) 診断結果の評価と報告

- 診断結果の評価と監査報告書の取り纏め
- 監査結果のの経営陣への報告と承認

(5) 指摘事項に対する改善対応の指示

脆弱性診断で摘出された脆弱性は、そのすべてについて、適切な改善が迅速に実施されなければならない。このためには、以下のステップを踏まなければならない。

- 指摘事項に対する対応策の検討
- セキュリティ対策への反映計画の作成(実施のタイミングや実施の手順等)
- 計画にもとづきた改善策の実施
- 改善措置の実施についての報告

(4) 改善対応状況の管理(フォローアップ)

脆弱性診断で指摘されたことが放置されたままになってしまうようなことを避けるためには、以下も必要となる。

- 指摘事項に対する対策消化状況
- 実施済みの対策の実効状況の確認

【対応 ISMS コントロール】

12.2.3　セキュリティ基本方針との適合性

12.2.4　技術適合の検査

セキュリティ対策評価モデルの開発プロジェクト委員リスト

主査	重松孝明	ECOM
委員	井上陽一	(株)ﾋｭｰｺﾑ
	上畑正和	ｾｲｺｰｲﾝｽﾙﾒﾝﾄ(株)
	遠藤孝行	セコム(株)
	織茂昌之	(株)日立製作所
	河村太郎	(株)サイバーデフェンス
	岸田　明	富士通(株)
	北野晴人	日本オラクル(株)
	五井　　孝	(株)大和総研
	高橋正和	ｲﾝﾀｰﾈｯﾄｾｷｭﾘﾃｨｼｽﾃﾑｽﾞ(株)
	鶴　田正文	ｸﾞﾛｰﾊﾞﾙｾｷｭﾘﾃｨｴｷｽﾊﾟｰﾄ(株)
	寺島　崇幸	(株)ﾋｭｰｺﾑ
	渡並　　智	セコム(株)
	中山　亮	(株)ｴﾇ･ﾃｨ･ﾃｨ･ﾃﾞｰﾀ
	二木真明	住商ｴﾚｸﾄﾛﾆｸｽ(株)
	平井正行	(株)日立製作所
	平野　勝	(株)ﾋｭｰｺﾑ
	堀内多桂雄	(株)ﾋｭｰｺﾑ
	松田　彰	ﾏｶﾌｨｰ(株)
	宮川晃一	ｸﾞﾛｰﾊﾞﾙｾｷｭﾘﾃｨｴｷｽﾊﾟｰﾄ(株)
	山崎文明	ｸﾞﾛｰﾊﾞﾙｾｷｭﾘﾃｨｴｷｽﾊﾟｰﾄ(株)
	横山竜太郎	(株)サイバーデフェンス
	吉田　一雄	清和大学
	吉松孝文	(株)日立製作所

平成16年度 経済産業省 受託事業
(ブロードバンドセキュリティに関する調査研究)
「セキュリティ対策評価モデル」
第1分冊:モデルのコンセプトと対策要求の解説
平成 17年 2月 発行

発行所 財団法人 日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園三丁目5番8号
機械振興会館 3階
TEL : 03(3436)7500

印刷所 株式会社 美行企画
東京都千代田区神田錦町2丁目5番地
鈴木第2ビル
TEL:03(3219)2971

この資料は再生紙を使用しています。