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２分冊：モデルの使用法と対策強度レベル判定基準

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

本報告書は、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」についての報告書の第 2 分冊として、この調査研究で開発した「セキュリティ対策評価モデル」の構成要素である、個々の対策要求に対する対策強度レベルの判定基準を示すとともに、セキュリティ対策の計画の策定や、実施しているセキュリティ対策の実態を評価する際の、このモデルの使い方を示すものである。

モデルのコンセプトや対策強度判定の対象となる対策要求については、第 1 分冊を参照されたい。

本モデルは、まだ、十分に成熟したものとは言い難いが、本モデルをたたき台にセキュリティ対策の実践論の検討が広く起されることを期待する。

# 目　　次

## 第 1 部　本モデルの使用法

## 第 2 部　対策強度レベル判定基準

# 第 1 部
# 本モデルの使用法

# 1. 対策強度の概念とその応用について

## 1.1. 対策強度の概念と本モデルの基本コンセプト

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。この利用イメージを、図 1-1 に示す。

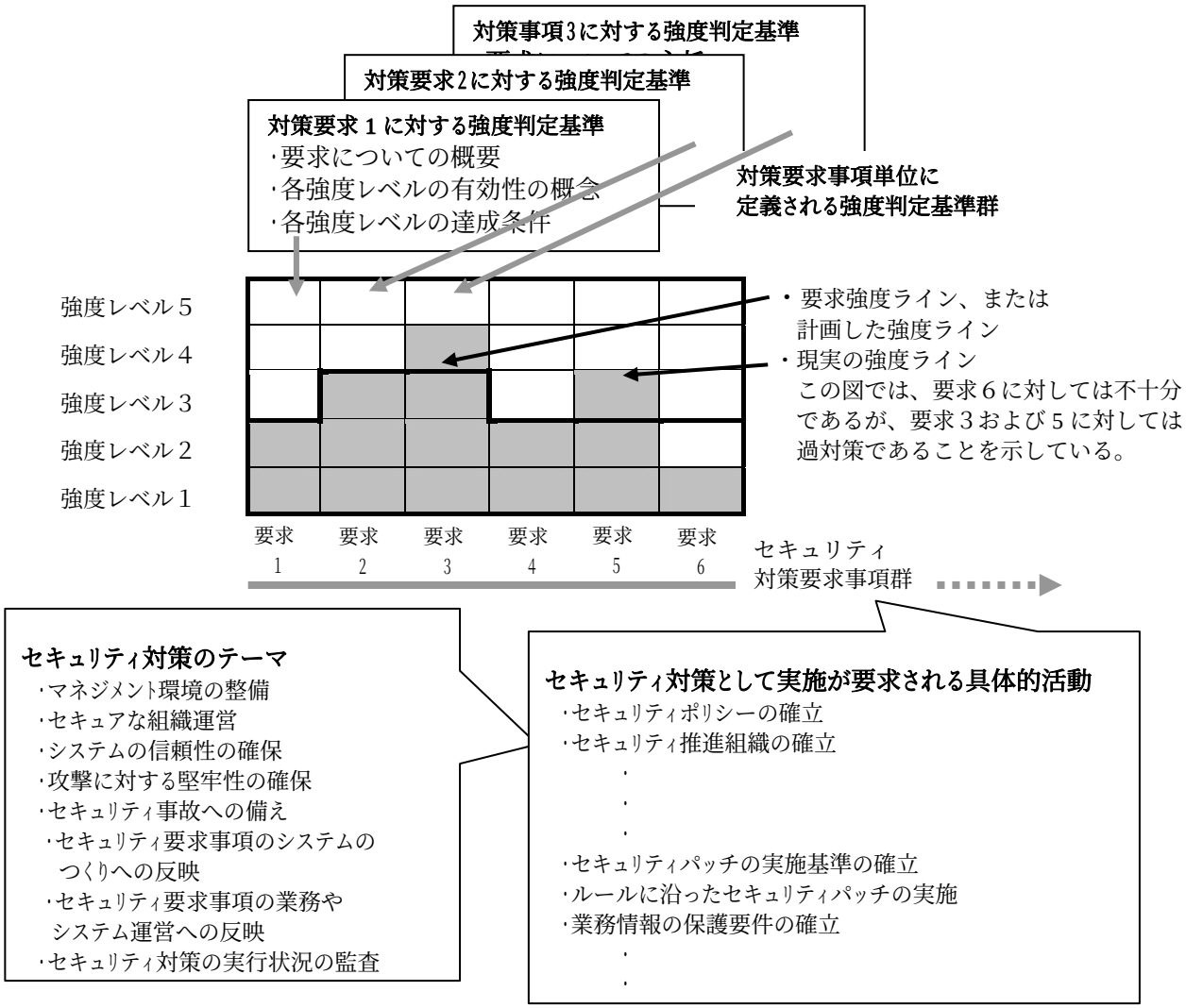


**図 1-1 セキュリティ対策評価モデルのイメージ**

## 1.2. 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、Rdi 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･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

## 1.3. 個々の対策要求における対策強度

### 1.3.1. 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 1-1 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 1-1 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、<br>技術的な要求の場合 | 要求が、<br>業務や管理面についての要求の場合 |
|---|---|---|
| 対策コア<br>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<br>・採用した技術の使用の決め細かさ<br>・適用の網羅性<br>（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<br>・適用の網羅性<br>（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<br>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<br>･実装プロセスの確立のレベル<br>･実装管理の厳格さレベル<br>･見直しの実行レベル<br>･文書化のレベル | ･当該対策の検討のレベル<br>･実行プロセスの確立のレベル<br>･実行管理の厳格さのレベル<br>･見直しの実行レベル<br>･文書化のレベル |

## 1.4. 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 1-2 に示す手順で決める。

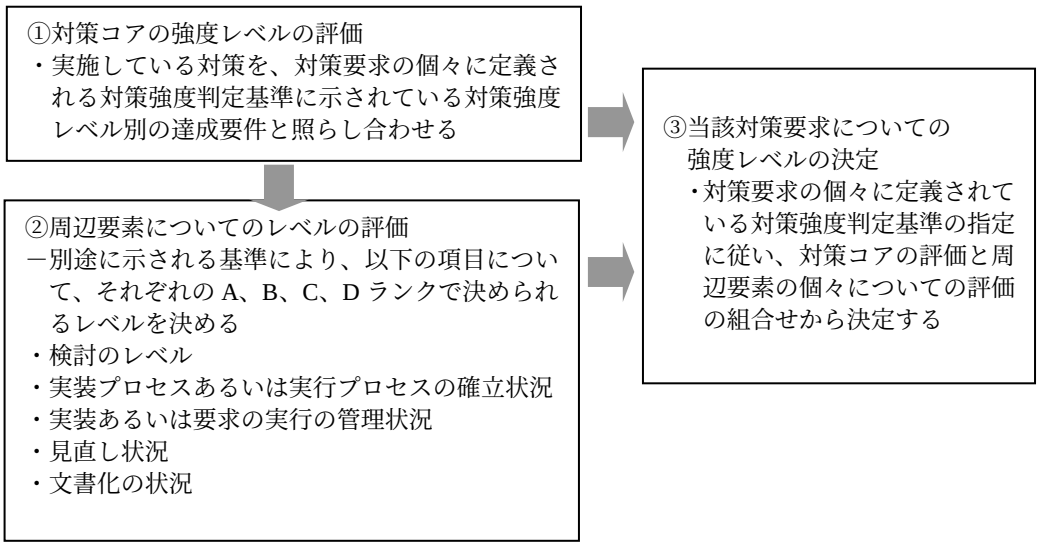


**図 1-2 個々の対策要求に対する対策強度レベルの判定手順**

# 2. 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。

## 2.1. 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 2-1 に示す。

**表 2-1 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<br>・防衛、治安関係、法曹関係機関<br>・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<br>・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<br>・政府機関、地方自治体等の官公庁<br>・金融機関<br>・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<br>・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<br>・一般企業のシステム<br>・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<br>・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 | |

## 2.2. 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 2-2 に示すようなものとした。

**表 2-2 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。<br>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<br>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。<br>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。<br>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 |

## 2.3. 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 2-3 に示す。

**表 2-3 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<br>・防衛、治安関係、法曹関係機関<br>・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<br>・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<br>・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<br>・政府機関、地方自治体等の官公庁<br>・金融機関<br>・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<br>・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<br>・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<br>・一般企業のシステム<br>・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<br>・一般的な対策要求についてはレベル3<br>・リスクが特に低いと見ることができる対策要求についてはレベル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<br>・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。

## 2.4. 個々対策要求の対策強度レベルの決め方

### 2.4.1. 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 2-4 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 2-4 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）<br>・当該要求についての対策の検討レベルは A<br>・実行プロセスの確立状況についてのレベルは A<br>・実行管理の実施状況についてのレベルは A<br>・見直しのレベルは A<br>・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）<br>・当該要求についての対策の検討レベルは B 以上<br>・実行プロセスの確立状況についてのレベルは B 以上<br>・実行管理の実施状況についてのレベルは B 以上<br>・見直しのレベルは B 以上<br>・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<br>・対策コアはレベル3以上（対策要求ごとに示される）<br>・当該要求についての対策の検討レベルは B 以上<br>・実行プロセスの確立状況についてのレベルは B 以上<br>・実行管理の実施状況についてのレベルは B 以上<br>・見直しのレベルは B 以上<br>・文書化のレベルは B 以上 |
| 2 | ベースライン<br>以下であるが<br>場合によっては<br>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）<br>・当該要求についての対策の検討レベルは C 以上<br>・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<br>・実行管理の実施状況についてのレベルは、レベル C 以上<br>・見直しのレベルは、レベル C 以上<br>・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<br>（対策実態の評価結果として使用） |

### 2.4.2. 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 2-5 のようにしている。

**表 2-5 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。<br>(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)<br>・必要な対象部分にすべてに以下が講じられている<br>・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<br>－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<br>・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<br>－信頼度の高い技術の採用<br>－2 重化の実施 |
| レベル 4 | 平均以上であるが、まだ上もある。<br>(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)<br>・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<br>・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<br>・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<br>・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<br>・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<br>・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<br>(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)<br>・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<br>・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。<br>・レベル2の達成要件も満たさない |

### 2.4.3. 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 2-6 のようにする。

**表 2-6 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。<br>(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)<br>・必要な対象部分にすべてに以下が講じられている<br>・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<br>・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<br>・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<br>・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。<br>(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)<br>・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<br>・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<br>・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<br>・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<br>・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<br>(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)<br>・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。<br>・レベル 2 の達成要件も満たさない |

### 2.4.4. 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 2-7 示すようなものとした。

**表 2-7 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 2-8 示すようなものとした。

**表 2-8 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 2-9 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 2-9 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<br>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 2-10 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 2-10 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<br>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 2-11 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 2-11 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

# 3. セキュリティ対策計画時における利用法

## 3.1. 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。

## 3.2. 本モデルを用いたセキュリティ対策の計画手順

図 3-1 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。

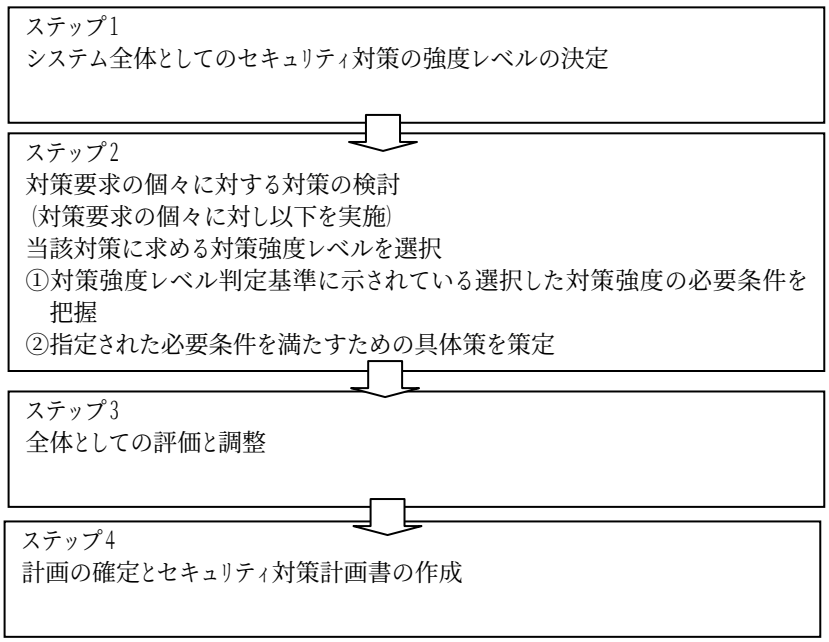


**図 3-1 本モデルをセキュリティ対策の計画手順**

### 3.2.1. 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 3-1に示すようなものがあげられる。

**表 3-1 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<br>－社会的な責任の度合い（広い範囲に影響）<br>－利用者の生命・健康・財産への直結の度合い<br>－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<br>－業務の遂行への影響度合い<br>－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<br>－組織やオフィスの形態（特に分散の形態）<br>－関係者の構成<br>－業務の運営形態（外部委託の有無やそのレベル）<br>－管理面での文化<br>・システムの構成や運用面からの脆弱性<br>－システムの構成うえの特性<br>－システムの運用面での特性 |

### 3.2.2. 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。

### 3.2.3. 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。

### 3.2.4. 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。

### 3.2.5. 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。

# 4. セキュリティ対策の評価への適用

## 4.1. 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。

## 4.2. 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。

## 4.3. 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 4-1に示す手順で決める。

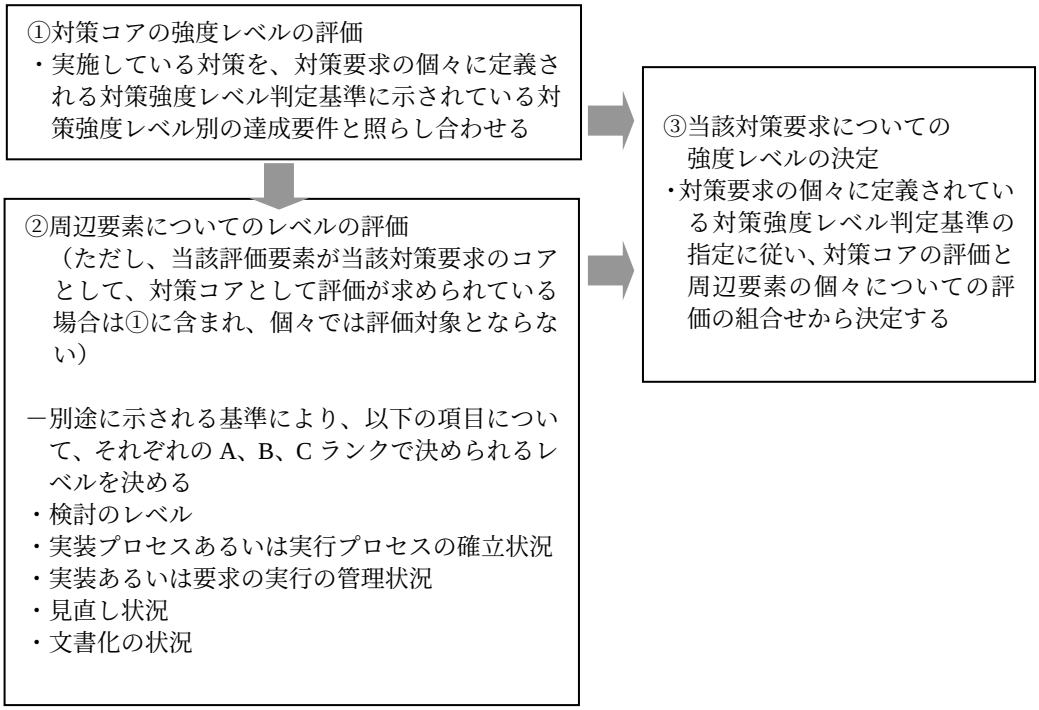


**図 4-1 個々の対策要求に対する対策強度レベルの設定基準**

## 4.4. 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。

### 4.4.1. 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。

### 4.4.2. セキュリティ対策の実態の評価の手順

図 4-2 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。

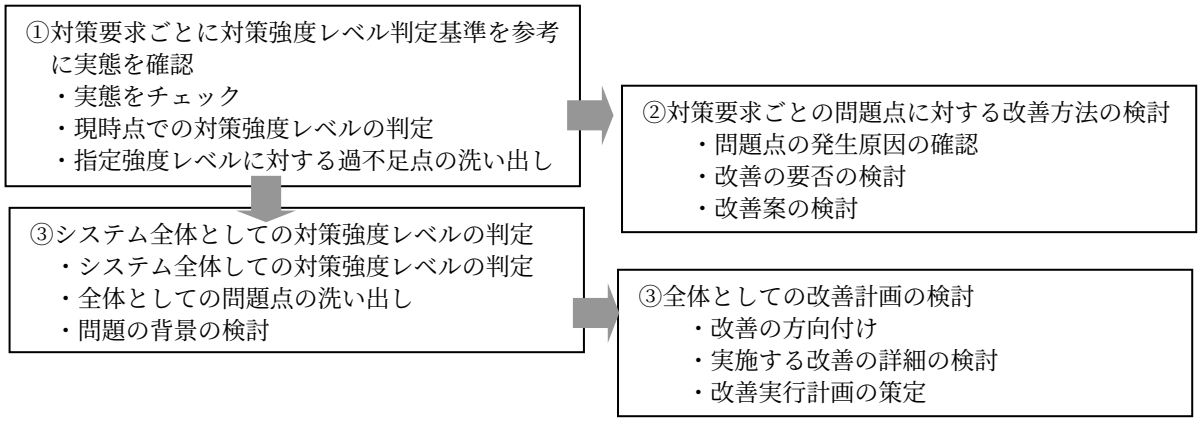


**図 4-2 本モデルを用いたセキュリティ対策の実態評価の手順**

### 4.4.3. 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

⑴ 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。

⑵ 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。

⑶ 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。

### 4.4.4. 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

⑴ 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

⑵ 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。

⑶ 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

### 4.4.5. 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

⑴ 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。

⑵ ステップ2：全体としての問題点の洗い出し

⑴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。

### 4.4.6. 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

# 第2部
# 対策強度レベル判定基準

次ページ以降に示す対策要求別の各強度レベル達成条件の中にある下記事項のついての達成度（クラス A、B、C）については、本文の2．2．4節の周辺要素に対する評価基準を参照のこと。

# 1. マネジメント・ビュー

## 1.1. セキュリティ対策基盤の確立

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 組織的に検討された完成度の高い経営レベルのセキュリティポリシーが確立しており、セキュリティ対策のベースとして十分に機能している。<br>・経営レベルでのセキュリティポリシーとして明示すべき必要な事項はすべて明示されている（注1）<br>・経営陣により承認・発行されている<br>・内容的にもセキュリティ環境や経営の方針を十分に反映している<br>・組織内への周知にはさまざまな手段が用いられ、その周知についての努力は徹底している<br>・関係者におけるセキュリティポリシーの認知も確認されている<br>・作成されたセキュリティポリシーは経営陣も加わり、関係部門も一体となった検討の結果である<br>・1年に一度は見直しが行われるようになっている<br>・経営レベルのセキュリティポリシーについての文書化のレベルはクラスA |
| レベル | 組織的に検討された経営レベルのセキュリティポリシーが確立しており、セキュリティ対策のベースとして十分に機能しているが、まだ、改善の余地もある。<br>・経営レベルでのセキュリティポリシーとして明示すべき必要な事項はすべて明示されている（注1）が、まだ改善すべき点もある<br>・経営陣により承認・発行されている<br>・内容的にもセキュリティ環境や経営の方針を十分に反映しているが、まだ改善の余地もある<br>・組織内への周知にはさまざまな手段が用いられ、その周知についての努力は徹底している<br>・作成されたセキュリティポリシーは経営陣も加わり、関係部門も一体となった検討の結果である<br>・必要に応じ見直しが行われるようになっている<br>・経営レベルのセキュリティポリシーについての文書化のレベルはクラスA |
| レベル3 | 大まかではあるが、組織的に検討された経営レベルのセキュリティポリシーが策定されており、セキュリティ対策のベースとして機能しているが、改善の余地も少なくない。<br>・経営レベルでのセキュリティポリシーとして明示すべき必要な事項は（注1）は概ね示されているが、組織やシステムの運営実態に照らすと見直すべきところも残っている<br>・経営陣により承認・発行されている<br>・セキュリティ環境や経営の方針を、概ね、反映してはいるが、まだ見直すべきところも少なくない<br>・組織内への周知についての手段は講じられているが、関係者に徹底しているとは言い難いが、認識は相当にされている<br>・必要に応じ見直しが行われるようになっている<br>・経営レベルのセキュリティポリシーについての文書化のレベルはクラスB以上 |
| レベル2 | 経営レベルのセキュリティポリシーは存在するものの、形式的で実効性は低い<br>・セキュリティポリシーは作られているが形式的で、組織やシステムの運営実態に照らし、組織的に検討されたものとは言い難い<br>・内容的にも不十分、ただし、情報セキュリティへの取組み姿勢は見せている<br>・組織内への周知についての努力も形式的で、関係者の認識は低い<br>・見直しについては特に意識されていない<br>・経営レベルのセキュリティポリシーについての文書化のレベルはクラスB以上 |
| レベル1 | 実効的な経営レベルのセキュリティポリシーは存在しない<br>・レベル2の達成要件も満たしていない |

(注 1) 経営レベルでのセキュリティポリシーとして明示されるべき主な事項
・情報セキュリティの経営上での位置付け（セキュリティ対策の目的）
・守るべきものの大枠（セキュリティ対策の対象あるいは目指すこと）
・セキュリティ対策として求めるレベルの大枠（セキュリティ対策として実現すべきこと）
・セキュリティ対策の組立て（技術面での組立て、管理面での仕組み）
・セキュリティ対策の推進体制
・セキュリティ対策の予算についての考え方

## Ma1.2 セキュリティ対策の組立ての確立

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 経営陣も承認した完成度の高い戦略的なセキュリティ対策の組立てが確立しており、セキュリティ対策のベースとして機能している。<br>・セキュリティ対策を形作る施策の組立てとして(注1)明示すべきことは、すべて明示されている<br>・セキュリティ対策の推進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こと（注2）は、すべて明示されている<br>・これらはいずれも対象の組織やシステムの運営実態に照らし十分に適切である<br>・セキュリティ対策の組立てについての検討のレベルはクラスA<br>・このセキュリティ対策の組立てについては経営陣の理解と承認を得ている<br>・セキュリティ対策の組立てについての見直し状況はクラスA<br>・セキュリティ対策の組立てについての文書化のレベルはクラスA |
| レベル4 | 経営陣も承認した組織としてよく検討された戦略的なセキュリティ対策の組立てが確立しており、セキュリティ対策のベースとして機能しているが、さらに研究すべきところも残る。<br>・セキュリティ対策を形作る施策の組立てとして(注1)明示すべきことは、概ね明示されている<br>・セキュリティ対策の推進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こと（注2）は、概ね明示されている<br>・これらはいずれも対象の組織やシステムの運営実態に照らし概ね適切であるが、見直すべきところも残る<br>・セキュリティ対策の組立てについての検討のレベルはクラスA<br>・このセキュリティ対策の組立てについては経営陣の承認を得ている<br>・セキュリティ対策の組立てについての見直し状況はクラスB以上<br>・セキュリティ対策の組立てについての文書化のレベルはクラスB以上 |
| レベル3 | ある程度、組織的に検討されたセキュリティ対策の組立てについての考え方が示されており、セキュリティ対策のベースとして機能しているが、さらに見直すべきところも残る。<br>・セキュリティ対策を形作る施策の組立てとし(注1)明示すべきことは、ほとんど概ね明示されている<br>・セキュリティ対策の推進にかかるマネジメントのフレームワーク（注2）もある程度、示されている<br>・これらはいずれも対象の組織やシステムの運営実態をおおむね反映しているが、見直すべきところも残る<br>・セキュリティ対策の組立てについての検討のレベルはクラスC以上<br>・セキュリティ対策の組立てについての見直し状況はクラスC以上<br>・セキュリティ対策の組立てについての文書化のレベルはクラスC以上 |
| レベル2 | 組織的に検討されたものではないが、セキュリティ対策の組立てについてのコンセプトを示すものは存在するが、セキュリティ対策を戦略的なものにするものとは言い難い。<br>・セキュリティ対策を形作る施策の組立てについての考え方はある程度示されている<br>・セキュリティ対策の推進にかかるマネジメントについてはあまり触れられていない<br>・セキュリティ対策の組立てについての文書化のレベルはクラスC以上 |
| レベル1 | セキュリティ対策の組立てについての組織的検討は見らず、セキュリティ対策全体がある方針に沿って組立てられたものになっていない<br>・レベル2の達成要件も満たしていない |

(注 1)　セキュリティ対策を形作る施策の組立てとして明示すべき事項
・対策テーマの体系
・各対策テーマの役割分担と相互の関連
・対策テーマ間の関連

(注2)　セキュリティ対策の推進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
・経営レベルでの監督指導の仕組み
・個々の対策テーマ単位でのＰＤＣＡサイクルのまわし方と、各ステップでのプロセス、チェックのポイント等で示す管理の仕組み
・文書化についての要求
・関係者の責任分担と連携のあり方

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 経営陣も参加した組織全体としての体制が確立しており、情報セキュリティにかかる諸活動が円滑に行われるための組織面での環境が完全に整備されており、これらは完全に機能している。<br>・組織横断的な推進体制が整備されている<br>・経営陣の責任および関与の範囲が明確にされている<br>・情報セキュリティの責任部署およびその責任が明示されている<br>・社内各部門の情報セキュリティについての責任が明示されている<br>・セキュリティ対策を推進するために作られた組織的な仕組みは、すべて期待通りに完全に機能している<br>・セキュリティ対策の推進体制についての検討のレベルはランクＡ<br>・セキュリティ対策の推進体制についての機能状況のチェックや見直しプロセスも確立している<br>・セキュリティ対策の推進体制についての見直し状況はクラスＡ<br>・セキュリティ対策の推進体制や、これらの機能状態についての文書化のレベルはクラスＡ |
| レベル4 | 経営陣も参加した組織全体としての体制が作られており、情報セキュリティにかかる諸活動が円滑に行われるための組織面での環境も作られており、有効に機能しているが、体制の整備や実行面でまだ改善の余地が、少ないが残る。<br>・組織横断的な推進体制が整備されている<br>・経営陣の責任および関与の範囲が明確にされている<br>・情報セキュリティの責任部署およびその責任が明示されている<br>・社内各部門の情報セキュリティについての責任が明示されている<br>・セキュリティ対策を推進するために作られた組織的な仕組みは、実行面で十分に機能していない点も見かける<br>・セキュリティ対策の推進体制についての機能状況のチェックや見直しプロセスも確立している<br>・セキュリティ対策の推進体制についての検討のレベルはランクＢ以上<br>・セキュリティ対策の推進体制についての見直し状況はＢ以上<br>・セキュリティ対策の推進体制や、これらの機能状態についての文書化のレベルはＢ以上 |
| レベル3 | 大まかではあるが、セキュリティ対策の推進体制、経営陣の参加、関係部門間の調整方法等が示されえおり、基本の形はできていて、最低限必要なレベルでは機能しているが、改善する余地は多い。<br>・経営陣の関与もうたわれているが形式的な域に止まっている<br>・情報セキュリティの推進責任部署は示されている<br>・セキュリティ対策を推進するために作られた組織的な仕組みは、形はできているが、実行面で期待通りに機能していない点も少なくない<br>・社内各部門の情報セキュリティにかかる責任も示されているが概念レベルに止まっている<br>・セキュリティ対策の推進体制についての検討のレベルはランクＢ以上<br>・セキュリティ対策の推進体制についての見直し状況はＢ以上<br>・セキュリティ対策の推進体制や、これらの機能状態についての文書化のレベルはＢ以上 |

| | |
|---|---|
| レベル 2 | セキュリティ対策の推進体制は示されている、ある程度機能しているが、全社的な取り組みにはなっているとは言い難い。<br>・セキュリティ対策の推進チームは存在<br>・セキュリティ対策の推進体制についての文書化のレベルはC以上 |
| レベル 1 | 組織的なセキュリティ対策の推進体制はないに等しい<br>・レベル2の達成要件も満たしていない |

## Ma1.4 関係者の責任の明確化と関係者への周知

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | 関係者へのセキュリティ対策にかかるそれぞれ責務に明確化と、その関係者全員への周知も徹底している。<br>・関係者への情報セキュリティにかかる責務の分割や指定は、組織の実態に照らし十分に適切<br>・すべての関係者に対する自己の責務について徹底させる仕組みの確立状況はクラス A<br>・すべての関係者に対する自己の責務について徹底についての実践と管理の徹底状況はクラス A<br>・すべての関係者がそれぞれに自己の責務の承知していることの確認も行われている<br>・すべての関係者に対する責務の割り振りについてについての見直し状況はクラス A<br>・すべての関係者に対する自己の責務やその徹底状況についての文書化のレベルはクラス A |
| レベル 4 | 関係者へのセキュリティ対策にかかるそれぞれ責務に明確化と、その関係者全員への周知も図られているが、関係者への責務の分担や、その周知徹底については、まだ、改善の余地がある。<br>・関係者への情報セキュリティにかかる責務の分割や指定は、組織の実態に照らし、概ね適切であるが、見直す余地は少ないが残る。<br>・すべての関係者に対する自己の責務について徹底させる仕組みの確立状況はクラス B 以上<br>・すべての関係者に対する自己の責務について徹底についての実践と管理の徹底状況はクラス B 以上<br>・すべての関係者がそれぞれに自己の責務の承知していることの確認も、ある程度行われている<br>・すべての関係者に対する責務の割り振りについてについての見直し状況はクラス B 以上<br>・すべての関係者に対する自己の責務やその徹底状況についての文書化のレベルは B 以上 |
| レベル 3 | 大まかではあるが、関係者へのセキュリティ対策にかかるそれぞれ責務は示されており、その関係者全員への周知も図られているが、不徹底で組織全体には十分に行き届いているとは言い難く、改善の余地は少なくない。<br>・関係者への情報セキュリティにかかる責務の分割や指定は、組織の実態に照らし、概ね適切であるが、見直す余地も残る<br>・特に、業務現場やシステムの開発や運用に関わる関係者へのセキュリティ要求の明示が不徹底<br>・関係者に対する自己の責務について徹底させる仕組みの確立状況はクラス B 以上<br>・関係者に対する自己の責務について徹底についての実践と管理の徹底状況はクラス B 以上<br>・すべての関係者に対する責務の割り振りについてについての見直し状況はクラス B 以上<br>・すべての関係者に対する自己の責務やその徹底状況についての文書化のレベルは B 以上 |
| レベル 2 | 関係者へのセキュリティ対策にかかるそれぞれ責務に明確化と、その関係者への周知は、セキュリティ対策を担当する者に限られており、組織全体への展開はほとんど図られていない。<br>・情報セキュリティにかかる責務の分割や指定は、セキュリティ対策の担当者に限定されている<br>・これらについも大まかな範囲でしか示されていない<br>・業務現場やシステムの開発や運用に関わる関係者へのセキュリティ要求の明示が実質的に不在<br>・関係者に対する自己の責務について徹底についての実践と管理は、組織的ではないが、少し行われている<br>・すべての関係者に対する自己の責務やその徹底状況についての文書化のレベルは C 以上 |
| レベル 1 | 関係者への情報セキュリティにかかる自己の責務の周知徹底は、ほとんど行われていない。セキュリティ対策の担当者が、自己の責務を認識している程度。<br>・レベル2の達成要件も満たしていない |

## Ma1.5 関係者のセキュリティ対策推進能力の確保

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | それぞれの関係者に求めるセキュリティ対策推進能力が定義されており、必要な教育訓練が組織的に徹底して行われ、関係者のスキルマップも整備され、関係者のセキュリティ対策推進能力は、常に、適切なレベルに維持されている。<br>・十分に検討された組織運営やセキュリティ対策の実態にあった関係者に求めるスキル等が明示されている<br>・関係者それぞれへに必要なスキルを取得させるための教育計画や教育環境が整備されている<br>・関係者それぞれの情報セキュリティの推進にかかわるスキルマップも整備されている（関係者それぞれに求められる情報セキュリティの推進にかかわるスキルの取得状況は確認されている）<br>・関係者のスキルマップや教育計画にもとづく教育訓練は適宜適切に行われている<br>・関係者それぞれに求めるスキルや、スキル確保についての計画やその実践方法についての検討のレベルはクラスA<br>・関係者それぞれに求めるスキルの確保についての計画やその実践についての管理の仕組みの確立状況はクラスA<br>・関係者それぞれに求めるスキルの確認や教育についての実践と管理の徹底状況はクラスA<br>・関係者それぞれに求めるスキルや、スキル確保についての計画やその実践方法についての見直し状況はクラスA<br>・本対策要求についての計画や実践についての文書化のレベルはクラスA |
| レベル4 | それぞれの関係者に求めるセキュリティ対策推進能力が定義されており、必要な教育訓練が組織的に行われ、関係者のスキルマップも整備されてはいるが、徹底さに欠けるところも見られる。関係者全員が、常に、セキュリティ対策推進に必要なレベルを十分に維持しているとう言い切れない。<br>・関係者に求めるスキル等は、組織運営やセキュリティ対策の実態に照らして検討され明示されている<br>・関係者それぞれへに必要なスキルを取得させるための教育計画や教育環境が作られているが、内容や対象者の網羅性等の点で、十分とは言えないところもある<br>・関係者それぞれの情報セキュリティの推進にかかわるスキルマップも整備されているが、徹底されたものにはなっていない（関係者それぞれに求められる情報セキュリティの推進にかかわるスキルの取得状況は行われているが不十分）<br>・関係者のスキルマップや教育計画にもとづく教育訓練は、適切に行われている<br>・関係者それぞれに求めるスキルや、スキル確保についての計画やその実践方法についての検討のレベルはクラスA<br>・関係者それぞれに求めるスキルの確保についての計画やその実践についての管理の仕組みの確立状況はクラスB以上<br>・関係者それぞれに求めるスキルの確認や教育についての実践と管理の徹底状況はクラスB以上<br>・関係者それぞれに求めるスキルや、スキル確保についての計画やその実践方法についての見直し状況はクラスB以上<br>・本対策要求についての計画や実践についての文書化のレベルはクラスB以上 |
| レベル3 | セキュリティ対策の推進に直接かかわる者についてのみ、大まかではあるが、必要なスキルが定義されており、教育訓練もある程度行われており、必要最小限のスキルは有していると見ることはできるが、これが十分と言える域には、まだ遠い<br>・セキュリティ対策の推進に直接かかわる者に求められる知識やスキルは概ね示されている<br>・セキュリティ対策の推進に直接かかわる者に求められる知識やスキルを取得させるために必要な教育訓練は、担当部門ベースで行なわれている<br>・セキュリティ対策の推進に直接かかわる者に求められる知識やスキルを取得させるための手段は、適宜、実施されており、対象者は最低限必要な知識やスキルを有していると見ることができる<br>・関係者それぞれに求めるスキルや、スキル確保についての計画やその実践方法についての検討のレベルはクラスC以上<br>・担当部門レベルで、必要に応じた外部の研修や、専門家による指導を、適時、受けている<br>・本対策要求についての計画や実践についての文書化のレベルはクラスB以上 |

| | |
|---|---|
| レベル 2 | 組織的に管理されたてはいないが、担当部門で最低限必要な教育は行われており、担当者はセキュリティ対策についての責務に、ある程度対応できるようになっている。<br>・担当部門でセキュリティ対策の担当が必要とする知識やスキルを承知している<br>・担当部門の OJT で、担当者に対する必要な知識やスキルの伝承は行われている<br>・担当部門レベルで、必要に応じた外部の研修や、専門家による指導を、適時、受けている<br>・本対策要求についての計画や実践についての文書化のレベルはクラス C 以上 |
| レベル 1 | セキュリティ対策を直接担当する者についても、必要なスキル取得についての努力は見られない<br>・レベル2の達成要件も満たしていない |

## Ma1.6 セキュリティ対策予算の確保とその適切な執行

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | セキュリティ対策予算の作成は、十分に組織的かつ戦略的に行われており、予算内容もその執行も組織やシステムの運営実態に照らし適切。予算面でセキュリティ対策に制約がかかったり、無駄が生じるようなことはない。<br>・セキュリティ対策予算の組立て方が確立している<br>・セキュリティ対策予算は経営陣の承認事項となっており、その執行状況も経営陣に管理されている<br>・セキュリティ対策予算の審査や執行は、確立したプロセスに沿って適切に行われている<br>・毎年のセキュリティ予算の確保およびその執行は適切に行われている<br>・セキュリティ対策予算の作成についての検討のレベルはクラス A<br>・セキュリティ対策予算の確保とその執行についてのプロセスの確立状況はクラス A<br>・セキュリティ対策予算の確保とその執行についての実行管理の仕組みの確立状況はクラス A<br>・セキュリティ対策予算の組立てについての見直し状況はクラス A<br>・セキュリティ対策予算の確保とその執行状況についての文書化のレベルはクラス A |
| レベル 4 | セキュリティ対策予算の作成は、組織的かつ戦略的に行われており、予算内容もその執行も組織やシステムの運営実態に照らし概ね適切。予算面でセキュリティ対策に制約がでたり、無駄が生じる可能性は低い。ただし、予算の組立てや審査や執行管理について、まだ、改善の余地はのこる。<br>・セキュリティ対策予算の組立て方が確立しているが、大まかな点も残る<br>・セキュリティ対策予算は経営陣の承認事項となっており、その執行状況も経営陣に管理されている<br>・セキュリティ対策予算の審査や執行は、確立したプロセスに沿って適切に行われている<br>・毎年のセキュリティ予算の確保およびその執行は、概ね適切に行われている<br>・セキュリティ対策予算の作成についての検討のレベルはクラス A 以上<br>・セキュリティ対策予算の確保とその執行についてのプロセスの確立状況は B 以上<br>・セキュリティ対策予算の確保とその執行についての実行管理の仕組みの確立状況は B 以上<br>・セキュリティ対策予算の組立てについての見直し状況は B 以上<br>・セキュリティ対策予算の確保とその執行状況についての文書化のレベルは B 以上 |
| レベル 3 | セキュリティ対策の推進体制、経営陣の参加、関係部門間の調整等についての基本の形はできており、最低限必要なレベルでは機能しているが、改善する余地は多い。<br>・経営陣の関与もうたわれているが形式的な域に止まっている<br>・情報セキュリティの推進責任部署は示されている<br>・社内各部門の情報セキュリティにかかる責任も示されているが概念レベルに止まっている<br>・必要に応じた見直しのレベルは B 以上<br>・体制や責任やこれらの仕組みの活動状態についての文書化のレベルは B 以上 |
| レベル 2 | セキュリティ対策の推進体制は示されているが、全社的な取り組みにはなっていない。<br>・セキュリティ対策の推進チームは存在<br>・セキュリティ対策の推進体制についての文書化のレベルはC以上 |
| レベル 1 | 組織的なセキュリティ対策の推進はないに等しい<br>・レベル2の達成要件も満たしていない |

## 1.1.2. 経営レベルでのセキュリティ要求の確立

| 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 組織的に良く検討されたセキュリティ対策の対象となる組織やシステムについてのセキュリティ特性モデルが作成されており、セキュリティ対策検討や評価のベースとして使われている。内容的にも優れている。<br>･セキュリティ特性モデルとして明確にすべき事項(注1)はすべて網羅されている<br>･指定事項はすべてにわたり明確、かつ対象となる組織やシステムを的確に反映している<br>･このセキュリティ特性モデルについての検討のレベルはクラスA<br>･セキュリティ特性モデルの見直し状況はクラスA<br>･セキュリティ特性モデルについての文書化のレベルはクラスA |
| レベル4 | 組織的に検討されたセキュリティ対策の対象となる組織やシステムについてのセキュリティ特性モデルが作成されており、セキュリティ対策検討や評価のベースとして使われているが、内容的にまだ見直すべきところも残る。<br>･セキュリティ特性モデルとして明確にすべき事項は、一応、網羅されている<br>･指定は対象とする組織やシステムの特性を概ね反映しているが、十分に的確とは言い難いところもある。<br>･指定の明確性についてはまだ改善の余地がある<br>･このセキュリティ特性モデルについての検討のレベルはクラスB以上<br>･セキュリティ特性モデルの見直し状況はクラスB以上<br>･セキュリティ特性モデルについての文書化のレベルはクラスB以上 |
| レベル3 | セキュリティ対策の対象となる組織やシステムについてのセキュリティ特性モデルと見ることができるものは作成されており、セキュリティ対策検討や評価のベースとして使われているが、内容的には、本対策要求が求めているものと比べると不十分。<br>･セキュリティ特性モデルと見ることができるセキュリティ対策の前提を示すものが、検討され作成されている<br>･内容的には、本対策要求が求めていることについて、ほぼ網羅はしているが、その明確性や対象組織やシステムの運営実態に照らした的確性については、十分とは言えないところがある<br>･このセキュリティ特性モデルについての検討のレベルはクラスB以上<br>･セキュリティ特性モデルの見直し状況はクラスB以上<br>･セキュリティ特性モデルについての文書化のレベルはクラスB以上 |
| レベル2 | セキュリティ対策の対象となる組織やシステムについてのセキュリティ特性モデルとして検討されたものはないが、セキュリティ対策の対象についての認識を示したものはある。<br>･セキュリティ対策の対象についての認識を示したものはある<br>･内容的には対策要求の要求を満たすものには程遠い<br>･セキュリティ対策の対象についての認識についての文書化のレベルはC以上 |
| レベル1 | セキュリティ対策の対象についての認識を示したものはない |

(注1)　セキュリティ特性モデルとして明確にすべき事項
- ･対象組織の運営形態
- ･適用業務の特性と情報セキュリティについての要求の大枠
- ･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、施設や設備等の保護対象となるものの大枠とその体系
- ･保護対象(群)ごとのライフサイクルを意識した存在場所
- ･保護対象(群)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

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 対象システムが組織内外に提供しているすべてのサービスに対して、組織的によく検討されたセキュリティ要求が確立している。<br>・対象システムが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は、すべてのサービスの個々について必要事項（注1）が明確に示されている、また、その内容もサービスの特性を的確に反映している<br>・この要求はセキュリティ対策の計画や実践の評価のベースとして用いられている<br>・サービスの個々についてのセキュリティ要求についての検討のレベルはクラス A で、それぞれの要求の的確性は関係部門で検証されている<br>・サービスの個々についてのセキュリティ要求についての見直し状況はクラス A<br>・サービスの個々についてのセキュリティ要求についての文書化のレベルはクラス A |
| レベル4 | 対象システムが組織内外に提供しているすべてのサービスに対して、組織的に検討されたセキュリティ要求が明示されているが、一部にきめの細かさに欠けるところもあり、まだ、改善の余地は残る。<br>・対象システムが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は、主要なサービスについてはそのそれぞれに、あまり重要でないサービスについてはグループごとにそれぞれ必要事項（注 1）が明確に示されている<br>・重要とされるサービスについてのセキュリティ要求は的確<br>・重要とされていないサービスについての検討に十分でないものもが見られる<br>・この要求はセキュリティ対策の計画や実践の評価のベースとして用いられている<br>・サービスの個々についてのセキュリティ要求についての検討のレベルはクラス B 以上で、それぞれの要求の的確性は関係部門で検証されている<br>・サービスの個々についてのセキュリティ要求についての見直し状況はクラス B 以上<br>・サービスの個々についてのセキュリティ要求についての文書化のレベルはクラス B 以上 |
| レベル3 | 対象システムが組織内外に提供している重要なサービスに対するセキュリティ要求については、組織的な検討がなされて、大まかではあるが、概ね、適切なものが示されているが、まだ、検討の余地が残されている。また、重要でないサービスに対する要求の検討は十分とは言い難い。<br>・対象システムが組織内外に提供しているサービスにのうち、主要なサービスについてのセキュリティ要求は、それぞれについて必要な検討が関係部門間では行われており、その結果としての要求は大まかではあるが示されている<br>・重要とされていないサービスについての検討は、あまり、十分に行われていない<br>・この要求はセキュリティ対策の計画や実践の評価のベースとして用いられている<br>・サービスの個々についてのセキュリティ要求についての検討のレベルはクラス B 以上で、それぞれの要求の的確性は関係部門で検証されている<br>・サービスに対し定義されているセキュリティ要求についての見直し状況はクラス B 以上<br>・サービスについてのセキュリティ要求についての文書化のレベルはクラス B 以上 |
| レベル2 | 対象システムが組織内外に提供しているサービスに対するセキュリティ要求についての組織的な検討は行われていないが、重要なサービスについては、セキュリティ対策推進チームがセキュリティ対策の前提として示したものは存在。<br>・重要なサービスについては、セキュリティ対策の推進チームレベルが認識しているセキュリティ要求を示すものは存在<br>・サービスについてのセキュリティ要求についての文書化のレベルはクラス C 以上 |
| レベル1 | 提供しているサービスに対するセキュリティ要求の明示は、実務的にも行われていない<br>・レベル2の達成要件も満たしていない |

(注1)システムが組織の内外に提供しているサービスに対するセキュリティ要求として示すべき事項
・可用性についての要求
・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のレベル

・取扱う情報の保護についての具体的な要求（アクセスの制限、アクセス権限者の管理
　－アクセス制限についての要求
　－アクセス権限者の管理についての要求
　－アクセス監視についての要求
・利用者の保護についての要求のレベル
・運用の保全についての要求のレベル

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 完成度の高い情報の保護基準（注 1）が確立していて、対象システムが取り扱っている情報のすべてに対して、この保護基準に沿った、組織的によく検討された的確な保護要件が指定されている。<br>・情報に対する完成度の高い保護基準が確立している<br>・対象組織が取り扱っているすべての情報の個々について、保護要件として示すべきこと（注2）が明確に示されている、また、その内容も対象情報や組織の運営特性を的確に反映している<br>・この要求は、情報の保護についての計画や実践の評価のベースとして用いられている<br>・情報の個々についてのセキュリティ要求についての検討のレベルはクラス A で、それぞれの要求の的確性は、当該情報の責任部門で検証されている<br>・情報の個々についての保護要件の指定に対する見直し状況はクラス A<br>・情報のの個々についての保護要件の指定に対する文書化のレベルはクラス A |
| レベル4 | よく検討された情報の保護基準が示されており、対象システムが取り扱っている情報のすべてに対して、この保護基準に沿った、組織的によく検討された保護要件が概ね的確に指定されているが、きめの細かさに欠けるところも残っている。<br>・よく検討された情報に対する保護基準が支援されているが、まだ、改善の余地がある<br>・対象組織が取り扱っている主要な情報のすべてについて、また、それほど重要でないとしている情報については、グループ単位に保護要件として示すべきことが明確に示されている、また、その内容も対象情報や組織の運営特性を的確に反映している<br>・重要とされていない情報についての検討に十分でないものもが見られる<br>・この要求は、情報の保護の計画や実践の評価のベースとして用いられている<br>・情報の個々についてのセキュリティ要求についての検討のレベルはクラス B 以上で、それぞれの要求の的確性は、当該情報の責任部門で検証されている<br>・情報の個々についての保護要件の指定に対する見直し状況はクラス B 以上<br>・情報の個々についての保護要件の指定に対する文書化のレベルはクラス B 以上 |
| レベル3 | 大まかではあるが、保護基準も示されている。対象システムが取り扱っている情報のうち重要なものについては、この保護基準に沿った保護要件が、組織的に検討され指定されているが、その指定内容のきめの細かさや、指定の対象範囲等については、まだ、改善の余地がある。また、重要でないと見ている情報に対する保護要件の検討については、改善する余地が少なくない。<br>・大まかではあるが情報に対する保護基準は示されている<br>・対象組織が取り扱っている主要な情報のすべてについて、また、一部の情報については、グループ単位に保護要件として示すべきことが明確に示されているが、その指定内容は必要最小限で、厳密に見た場合、十分とは言い難い<br>・重要とされていない情報の保護要件は、組織的な検討の対象外となっている<br>・この要求は、情報の保護の計画や実践の評価のベースとして用いられている<br>・情報の個々についてのセキュリティ要求についての検討のレベルはクラス B 以上で、当該情報の責任部門での指定の的確性についての検証も徹底されていない<br>・情報の個々についての保護要件の指定に対する見直し状況はクラス B 以上<br>・情報の個々についての保護要件の指定に対する文書化のレベルはクラス B 以上 |
| レベル2 | 情報に対する保護要件の指定は、担当チームに任されており、組織的な管理は行われていないが、担当チーム内には情報の保護についての考え方が存在しており、個々の保護対象情報に対する保護要件の指定は、この考えに沿ったものとなっている。重要な情報についてのみ保護要件が大まかに示されているに過ぎない。 |

| | |
|---|---|
| | ・組織的に示された保護基準はないが、担当者間には情報の保護について共有されている考え方が存在している<br>・個々の保護対象情報に対する保護要件の指定は、担当チームに任されているが、この考え方に沿って検討されている<br>・情報に対する保護要件の指定は、重要と見ている情報に限られており、その指定もきめ細かなものではない<br>・情報に対する保護要件の指定に対する組織的な管理はほとんど行われていない<br>・情報の個々についての保護要件の指定に対する文書化のレベルは、クラス C レベル |
| レベル1 | 組織が取り扱っている情報の個々についての実効的な保護要件の明示は行われていない<br>・レベル2の達成要件も満たしていない |

(注1) 情報の保護基準として示すべき事項
- ・保護の厳格性によって分けるクラス構成
- ・各保護クラスに指定すべき事項
  - －対象とする情報の重要性および漏洩等の事故が発生した場合の影響の大きさ
  - －情報の秘匿についての要求のレベル
  - －情報の正確性の確保についての要求のレベル
  - －情報利用の可用性についての要求のレベル(情報の保全についての要求他)
  - －ライフサイクル管理についての要求のレベル
  - －物理媒体への展開の制限についての要求のレベル(印刷の制限や電磁媒体への格納の制限等)

(注2) 情報の個々に対する保護要件として示すべき事項
- ・適用する保護クラス
- ・提供するアクセス制限の詳細(当該情報に対するあらゆるタイプのアクセスの個々についての制限の明示)
- ・必要とするアクセス権限の管理の詳細
- ・適用すべきアクセス
- ・情報のシステムへの格納の制限の詳細
- ・必要な保全についての要求
- ・不正あるいは不審なアクセスに対しとるべき措置

# 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の運営の実現

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 人的要因に帰するセキュリティ事故を予防するために必要な措置（注1）とされることと、その確実な実践を担保するための完成度の高い管理面での仕組みが確立しており、完全に機能している。<br>･人的要因によるセキュリティ事故の予防についての、組織としての取組方針が明確に示されている<br>･このために必要となる措置がきめ細かく示されている<br>･これらの措置の実践を追求するための手段ならびにその実行を管理する仕組みが確立している<br>･これらの措置の実践についての組織的な責任体制も確立している<br>･この仕組みは完全に機能している<br>･人的要因に帰するセキュリティ事故を予防するために必要な措置についての検討のレベルはクラスA<br>･この仕組みについての見直し状況はクラスA<br>･この仕組みについての文書化のレベルはクラスA |
| レベル4 | 人的要因に帰するセキュリティ事故を予防するために必要な措置とされることと、その確実な実践を担保するためのよく検討された管理面での仕組みが確立しており、概ね、十分に機能しているが、まだ改善の余地も残る。<br>･人的要因によるセキュリティ事故の予防についての、組織としての取組方針が明確に示されている<br>･このために必要となる措置がきめ細かく示されているが、まだ改善の余地もある<br>･これらの措置の実践を追求するための、よく検討された手段ならびにその実行を管理する仕組み示されているが、まだ改善の余地もある<br>･これらの措置の実践についての組織的な責任体制も確立している<br>･この仕組みは、概ね、十分に機能している<br>･人的要因に帰するセキュリティ事故を予防するために必要な措置についての検討のレベルはクラスB以上<br>･この仕組みについての見直し状況はクラスB以上<br>･この仕組みについての文書化のレベルはクラスB以上 |
| レベル3 | 大まかではあるが、人的要因に帰するセキュリティ事故を予防するために必要な措置とされることと、その確実な実践を担保するための管理面での仕組みが示されており、ある程度機能しているが、まだ改善の余地は少なくない。<br>･大まかではあるが、人的要因によるセキュリティ事故の予防についての、組織としての取組方針が示されている<br>･大まかではあるが、このために必要となる措置が示されている<br>･これらの措置の実践を追求するための、段ならびにその実行を管理する仕組み示されているが、十分なものには、程遠い。<br>･大まかではあるが、これらの措置の実践についての組織的な責任体制も示されている<br>･人的要因に帰するセキュリティ事故を予防するために必要な措置についての検討のレベルはクラスB以上<br>･この仕組みについての見直し状況はクラスC以上<br>･この仕組みについての文書化のレベルはクラスC以上 |
| レベル2 | 人的要因に帰するセキュリティ事故を予防するために必要な措置とされることとは検討されてはいるが、検討も大まかで、組織としての取組みができているとは言い難い。<br>･担当チームは検討すべき事項については承知しており、非常に大まかではあるが、このために必要となる措置は示されている |

| | |
|---|---|
| | ・十分とは言えないまでも、これらを実践するための手段も示されている。<br>・この仕組みについての見直し状況はクラスＣ以上<br>・この仕組みについての文書化のレベルはクラスＣ以上 |
| レベル1 | 人的要因に帰するセキュリティ事故を予防するための実効的な取組みは見られない。<br>組織的なセキュリティ対策の推進はないに等しい<br>・レベル2の達成要件も満たしていない |

(注1) 職員や使用する外部スタッフに対する牽制措置として実施すべきこと
・採用時におけるセキュリティ要求の明示
・就業規程等によるセキュリティ要求の遵守の義務化
・セキュリティ違反に対する罰則規定の制定
・セキュリティ違反に対する罰則規定のお厳正な適用

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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 関係者に対する情報セキュリティについての取組み意識の醸成と、それぞれの責務の明確化とその各人への周知は徹底して行われており、すべての関係者において、これらは十分であることが確認されている。<br>・関係者に対する情報セキュリティについて認識さすべきことのすべてが明確にされている<br>・各人の情報セキュリティについての責務もきめ細かく示されている<br>・これらの関係者への徹底の仕組みもよく検討されたものが確立している<br>・この仕組みに沿って、関係者へのこれらの徹底が図られており、その周知度もチェックされている<br>・関係者に対する情報セキュリティについての取組み意識の醸成と、それぞれの責務の徹底の手段についての検討のレベルはクラスＡ<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスＡ |
| レベル4 | 関係者に対する情報セキュリティについての取組み意識の醸成と、それぞれの責務の明確化とその各人への周知の追及は行われているが、一部に徹底さを欠くところも見られ、すべての関係者において、これらは十分であることが確認されているところまでには至っていない。<br>・関係者に対する情報セキュリティについて認識さすべきことは、概ね、すべて明確にされているが、まだ見直すべきところも残る<br>・大まかではあるが、各人の情報セキュリティについての責務も、比較的きめ細かく示されている<br>・これらの関係者への徹底の仕組みも確立しているが、まだ、改善する余地もある<br>・この仕組みに沿って、関係者へのこれらの徹底が図られているが、徹底さを欠くところも見られる<br>・関係者に対する情報セキュリティについての取組み意識の醸成と、それぞれの責務の徹底の手段についての検討のレベルはクラスＢ以上<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスＢ以上 |
| レベル3 | 関係者に対する情報セキュリティについての取組み意識の醸成についての組織的な取組みも見られと、大まかではあるがそれぞれの責務も示されている。最低限の組織的な取組みはなされていると言えるが、十分な域には、程遠い。<br>・大まかではあるが、関係者に対する情報セキュリティについて認識さすべきことは示されている<br>・大まかではあるが、各人の情報セキュリティについての責務も示されている<br>・関係者へのこれらの徹底についての組織的な取組みもみられるが、徹底したものではない<br>・関係者に対する情報セキュリティについての取組み意識の醸成と、それぞれの責務の徹底の手段についての検討のレベルはクラスＢ以上<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスＢ以上 |
| レベル2 | 関係者に対する情報セキュリティについての取組み意識の醸成についての組織的な取組みも、十分ではないが、ある程度見らる。形式的なレベルではあるが、最低限の機能は果たしている。<br>・非常に大まかではあるが、関係者に対する情報セキュリティについて認識さすべきことは示されている |

| | |
|---|---|
| | ・非常に大まかではあるが、セキュリティ対策の中心になる者には、各人の情報セキュリティについての責務も示されている<br>・関係者へのこれらの徹底についての取組みもみられるが、形式的な域を出ない<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル 1 | 関係者に対する情報セキュリティについての取組み意識の醸成についての組織的な取組みは、ないに等しい<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | 人的要因に帰するセキュリティ事故を予防するための、関係者に対する信用の確認や、職場での行動に対する管理や指導は、定められえたルールの沿って厳格に運用されており、信用できない者が組織に入りこむ余地や、職場における不正あるいは不適切な行動が見逃されるようなことは、まず、ないとみてよい。<br>・レベル5のセキュリティ対策上の人的要因に対する管理の仕組みが確立している（Ba1.1 参照）<br>・ルールに沿った関係者の信用の確認は徹底している<br>・関係者に対する職場での行動の制限は明示されており、その励行も厳格にチェックされている<br>・これらの措置の実践は、定められた管理の仕組みの上で徹底してチェックされている<br>・本対策要求かかる指定されたの実践状況についての文書化のレベルはクラス A |
| レベル 4 | 関係者に対する信用の確認や、職場での行動に対する管理や指導は、定められえたルールに沿って実施されているが、実践上で厳格さに欠けるところも見られる。信用できない者が組織に入り込んだり、職場における不正あるいは不適切な行動が見逃されることは、ほとんどないと見てよいが、僅かながらの隙は残る。<br>・セキュリティ対策上の人的要因に対する管理の仕組みとして、レベル 4 以上のものが確立している（Ba1.1 参照）<br>・ルールに沿った関係者の信用の確認は、概ね行われている<br>・関係者に対する職場での行動の制限は明示されており、その励行もチェックされているが、厳格さに欠けるところも見られる<br>・不正行為に対する懲罰や不審な行為に対する指導も行われているが、厳格さにかけるところもある<br>・これらの措置の実践は、定められた管理の仕組みの上で徹底してチェックされている<br>・本対策要求かかる指定されたの実践状況についての文書化のレベルはクラス B 以上 |
| レベル 3 | 関係者に対する信用の確認や、職場での行動に対する管理や指導は、ある程度、管理された形で行われているが、十分とは言えず、信用できない者が組織に入り込んだり、職場における不正あるいは不適切な行動が見逃される可能性も残る。<br>・セキュリティ対策上の人的要因に対する管理の仕組みとして、レベル3以上のものが確立している（Ba1.1 参照）<br>・ルールに沿った関係者の信用の確認は、概ね行われている<br>・関係者に対する職場での行動の制限は明示されており、その励行もチェックされているが、十分には程遠い<br>・不正行為に対する懲罰や不審な行為に対する指導も行われているが、十分には程遠い<br>・これらの措置の実践は、定められた管理の仕組みの上で徹底してチェックされている<br>・本対策要求かかる指定されたの実践状況についての文書化のレベルはクラス C 以上 |
| レベル 2 | 関係者に対する信用の確認や、職場での行動に対する管理や指導は、職場の管理者の意識に依存しており、組織的な管理の下には行われていない。信用できない者が組織に入り込んだり、職場における不正あるいは不適切な行動が見逃される可能性も少なくない。 |
| レベル 1 | 関係者に対する信用の確認や、職場での行動に対する管理や指導は、実質的に行われていない |

## 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 |
|---|---|

| 強度<br>レベル | 当該レベル達成要件 |
|---|---|
| レベル<br>5 | 組織の職場ごとに、セキュリティ対策の諸施策が求めていることが、職場の特性に照らした形で的確に示されている。<br>・業務規程あるいは業務マニュアル、あるいはそれに準じるものに、セキュリティ対策の一環として各職場が日常の業務で行うべきこと、あるいは行っていないことが、的確に明示されている<br>・これらには、セキュリティ対策の諸施策の要求はすべて反映されている（ことが確認されている）<br>・各職場へのセキュリティ要求の確認や、日常の業務への反映方法、および関係文書へのこれらについての記述には、関係職場の関係者も加わり、クラス A レベルの検討が行われている<br>・各職場へのセキュリティ要求や職場への業務マニュアル等への反映についての見直し状況はクラス A<br>・本対策要求に関する文書化のレベルはクラス A |
| レベル<br>4 | 組織の職場ごとに、セキュリティ対策の諸施策が求めていることが、職場の特性に照らした形で示されているが、まだ改善の余地も少し残る。<br>・業務規程あるいは業務マニュアル、あるいはそれに準じるものに、セキュリティ対策の一環として各職場が日常の業務で行うべきこと、あるいは行っていないことが、職場単位の、概ね、的確に明示されている<br>・これらには、セキュリティ対策の諸施策の要求はすべて反映されているはずであるが、その確認は完全には行われていない<br>・各職場へのセキュリティ要求の確認や、日常の業務への反映方法、および関係文書へのこれらについての記述には、関係職場の関係者も加わり、クラス B 以上のレベルの検討が行われている<br>・各職場へのセキュリティ要求や職場への業務マニュアル等への反映についての見直し状況はクラス B 以上<br>・本対策要求に関する文書化のレベルはクラス B 以上 |
| レベル<br>3 | セキュリティ対策の諸施策が業務現場に求めていることは、ほぼ、漏れなく、一般的な要求として示されているが、各職場ごとへの要求までにはブレークダウンされていず、各職場におけるセキュリティ要求の展開は、各職場に任されている。セキュリティ対策からの要求の各職場への展開は、概ね出来ていると見ることは出来るが、それが十分に管理されているとは言えない。<br>・業務規程あるいは業務マニュアル、あるいはそれに準じるものに、セキュリティ対策の一環として各職場が日常の業務で行うべきこと、あるいは行っていないことは、すべての場職の共通事項として示されている<br>・これらには、セキュリティ対策の諸施策の要求を、ほぼ、反映したものとなっているが、その確認は十分ではない<br>・これらの要求の整理や業務マニュアル等への反映についての検討のレベルは、クラス C 以上<br>・各職場へのセキュリティ要求の展開は、職場の責任者に任されている<br>・各職場へのセキュリティ要求や職場への業務マニュアル等への反映についての見直し状況はクラス C 以上<br>・本対策要求に関する文書化のレベルはクラス C 以上 |
| レベル<br>2 | 業務現場ごとへのセキュリティ対策の諸施策の反映は組織的には行われていないが、一部の職場では、日常の業務で実施すべき事項や、行ってはならないことについての整理を行い、職場の者に知らしめている。<br>・一部の職場にセキュリティ対策からの要求を纏めた職場で機能している文書がある<br>・該当の職場の関係者は、この文書の内容を承知している |
| レベル<br>1 | 業務現場に対するセキュリティ要求の明確化に対する取り組みは無いに等しい<br>・レベル 2 の達成条件も満たせない |

## Ba2.2 各業務現場におけるセキュリティ要求の実践の追及

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 各業務現場におけるセキュリティ要求の実践を確実にするための完成度の高い仕組みも確立しており、この仕組みの下、要求の確実な厳格な実践が図られており、そのチェックや指導も徹底しており、実践上の漏れや不手際が見逃される余地は、まずない。<br>・職場ごとにセキュリティ要求の実践を管理するための仕組みが確立している<br>・この仕組みにそって、日々の業務活動におけるセキュリティ要求の実践はチェックされ、必要な指導が徹底して行われている<br>・職場ごとにセキュリティ要求の実践を管理するための仕組みについての検討のレベルはクラスA<br>・職場ごとにセキュリティ要求の実践を管理するための仕組みについての見直し状況はクラスA<br>・職場ごとにセキュリティ要求の実践を管理するための仕組み、要求の実践状況についての文書化のレベルはクラスA |
| レベル4 | 各業務現場におけるセキュリティ要求の実践を確実にするための仕組みも確立しており、この仕組みの下、要求の確実な厳格な実践が図られており、そのチェックや指導も行われているが、一部に徹底さにかけるところもあり、実践上の漏れや不手際が見逃されること隙が、僅かではありが残っている。<br>・職場ごとにセキュリティ要求の実践を管理するための仕組みは確立しているが、まだ改善の余地がある<br>・この仕組みにそって、日々の業務活動におけるセキュリティ要求の実践はチェックされ、必要な指導が行われているが、一部に徹底さを欠くところが見られる<br>・職場ごとにセキュリティ要求の実践を管理するための仕組みについての検討のレベルはB以上<br>・職場ごとにセキュリティ要求の実践を管理するための仕組みについての見直し状況はB以上<br>・職場ごとにセキュリティ要求の実践を管理するための仕組み、要求の実践状況についての文書化のレベルはB以上 |
| レベル3 | 各業務現場におけるセキュリティ要求の実践を確実にするための仕組みも作られて、確実な実践を目指して入るが、十分なものではなく、要求の実践については、必ずしも徹底してはいない。そのチェックや指導も、ある程度行われているが、形式的なものになっているところもあり、ある程度は信頼できるものの、実践上の漏れや不手際が見逃されること隙が残されている。<br>・職場ごとにセキュリティ要求の実践を管理するための仕組みは、現場レベルの工夫として機能している者が形成されている<br>・日々の業務活動におけるセキュリティ要求の実践は、一応チェックされ、必要な指導が行われているが、職場任せで十分に機能しているどうかは疑わしい<br>・職場ごとにセキュリティ要求の実践を管理するための仕組みについての見直し状況はC以上<br>・職場ごとにセキュリティ要求の実践を管理するための仕組み、要求の実践状況についての文書化のレベルはC以上 |
| レベル2 | 各業務現場におけるセキュリティ要求の実践は、各職場に任されており、組織的な取組みにはなっていない。<br>・各職場ではセキュリティ要求の実践の追及について意識は存在しており、時々、チェックはされている |
| レベル1 | 各業務現場におけるセキュリティ要求の実践は、ほとんど管理されていない。 |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 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要求の確立し、自社のセキュリティ対策への展開、ならびに業務連携先へのセキュリティ要求の明確化と、連携先におけるその実践の要求、双方での必要なセキュリティ対策の実践状況の交換等も十分に行われていて、問題が発生する余地は、まずないと考えられる。<br>・他社とのリアルタイムの業務コラボレーションについての徹底したリスク分析にもとづく、よく検討されたセキュリティ要求（注1）が確立している<br>・これらは的確にセキュリティ対策の展開されている<br>・連携先におけるこれらの要求の実践についてのお互いの確認や、コミュニケーションの環境も確立している<br>・業務連携にかかる契約書等でのセキュリティの確保にかかる双方の責務と、具体的に実施すべき事項が明確にされている<br>・双方におけるセキュリティ要求の実践状況の交換や、実施にかかわる双方のコミュニケーションは十分行われている<br>・他社とのリアルタイムの業務連携におけるセキュリティの確保の方法についての検討のレベルはクラスA<br>・他社とのリアルタイムの業務連携についてのセキュリティ要求の実践についての確認の徹底状況はクラスA<br>・他社とのリアルタイムの業務連携についてのセキュリティ対策についての見直し状況はクラスA<br>・他社とのリアルタイムの業務連携についてのセキュリティ対策の内容やその実践状況についての文書化のレベルはクラスA |
| レベル4 | 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要求の確立し、自社のセキュリティ対策への展開、ならびに業務連携先へのセキュリティ要求の明確化と、連携先におけるその実践の要求、双方での必要なセキュリティ対策の実践状況の交換等も行われてはいるが、徹底したものと言えないところも残されており、問題が発生する余地は、少ないが残されている考えられる。<br>・他社とのリアルタイムの業務コラボレーションについてのリスク分析にもとづく、よく検討されたセキュリティ要求（検討事項については注1参照）が示されているが、まだ検討が甘いところも残されている<br>・これらは、概ね適切にセキュリティ対策の展開されている<br>・連携先におけるこれらの要求の実践についてのお互いの確認や、コミュニケーションの環境も作られている<br>・業務連携にかかる契約書等でのセキュリティの確保にかかる双方の責務と、具体的に実施すべき事項は示されているが、十分とは言えないところも残されている<br>・双方におけるセキュリティ要求の実践状況の交換や、実施にかかわる双方のコミュニケーションも、行われている<br>・他社とのリアルタイムの業務連携におけるセキュリティの確保の方法についての検討のレベルはクラスB以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ要求の実践についての確認の徹底状況はクラスB以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ対策についての見直し状況はクラスB以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ対策の内容やその実践状況についての文書化のレベルはクラスB以上 |
| レベル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要求の検討、その結果の自社のセキュリティ対策への展開、ならびに業務連携先へのセキュリティ要求の明確化と、連携先におけるその実践の要求も行われてはいるが、いずれも大まかなもので、重要な点は抑えられているが、十分なものにするためには、強化が必要。<br>・他社とのリアルタイムの業務コラボレーションについてのセキュリティ要求は検討され示されているが、重要な点を除いては大まかなものである |

| | |
|---|---|
| | ・これらのセキュリティ対策への展開は行われている<br>・業務連携にかかる契約書等でのセキュリティの確保にかかる双方の責務と、具体的に実施すべき事項は示されているが、十分とは言えない<br>・連携先とのそれぞれのセキュリティ対策の実践状況についての情報交換等の相互コミュニケーションはあまり行われていない<br>・他社とのリアルタイムの業務連携におけるセキュリティの確保の方法についての検討のレベルはクラスB以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ要求の実践についての確認の徹底状況はクラスBC以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ対策についての見直し状況はクラスB以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ対策の内容やその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | 他社とのリアルタイムの業務コラボレーションについてのセキュリティ対策の検討や、連携先への要求も行われて入るが、大まかで、組織的な取組みには程遠い。<br>・担当部門レベルでは、他社とのリアルタイムの業務コラボレーションにおけるセキュリティ要求の検討と、セキュリティ対策への反映は行われている<br>・連携先に、大まかなではあるがセキュリティ対策についのて要求は行われているが、その実施状況の把握にまでには至っていない<br>・他社とのリアルタイムの業務連携におけるセキュリティの確保の方法についての検討のレベルはクラスC以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ要求の実践についての確認の徹底状況はクラスC以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ対策についての見直し状況はクラスC以上<br>・他社とのリアルタイムの業務連携についてのセキュリティ対策の内容やその実践状況についての文書化のレベルはクラスC以上 |
| レベル1 | 外部委託しているシステム運用のセキュリティ対策はすべて委託先任せで、委託先の責任も委託先の方針をそのまま受け入れている。<br>・レベル2の達成要件も満たしていない |

(注1)　他社とのリアルタイムの業務コラボレーションについてセキュリティ要求として示すべき事項
- ・可用性についての具体的な要求
- ・システムの処理の正確性についての要求レベル
- ・情報の秘匿についての具体的な要求
- ・情報の保全についての具体的な要求
- ・トラブル時における相互が協力する措置
  - －代替手段の準備
  - －原因の究明や対策実施についての連携方法
- ・運用の保全についての要求のレベル

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 外部に委託する業務運用に対するセキュリティ要求の確立し、委託先へのその実践の要求ならびにその監督指導も行える環境も整備され、委託先でのセキュリティ対策も十分に行われていることが担保されている。業務の外部委託を要因とするセキュリティ事故は、まず発生しない。<br>・業務運用の外部委託についてよく検討された審査基準（注1）が確立している<br>・業務運用の外部委託についての徹底したリスク分析にもとづく、よく検討された漏れのない委託先に対するセキュリティ要求（注2）が確立している<br>・委託先におけるこれらの要求の実践についての監督指導の仕組みや、委託先とのコミュニケーションの環境も確立している<br>・委託にかかる契約書等での委託元と委託先双方の責務には、これらはすべて的確に反映されている<br>・委託先におけるセキュリティ要求の実践は十分であることが、常時、確認されている<br>・委託先とのセキュリティ対策に関するコミュニケーションは十分行われている<br>・業務の外部委託におけるセキュリティの確保の方法についんての検討のレベルはクラスA<br>・委託先でのセキュリティ要求の実践についての確認の徹底状況はクラスA<br>・業務の外部委託についてのセキュリティ対策についての見直し状況はクラスA<br>・業務の外部委託についてのセキュリティ対策や委託先も含むその実践状況についての文書化のレベルはクラスA |
| レベル4 | 外部に委託する業務運用に対するセキュリティ要求も明示され、委託先へのその実践の要求ならびにその監督指導も行えるようになっており、委託先でのセキュリティ対策が十分に行われる環境は、一応、形成されているが、セキュリティ要求やその実践の担保については、厳格さを欠くところも残っている。業務の外部委託を要因とするセキュリティ事故が起こる余地もないではない。<br>・組織的に検討された業務運用の外部委託についての審査基準（注1）が示されているが、まだ改善の余地がる<br>・業務の外部委託についてのリスク分析にもとづく、よく検討された委託先に対するセキュリティ要求（注2）が示されているが、リスク分析やセキュリティ対策についての要求には甘いところも残されえている<br>・委託先におけるこれらの要求の実践についての監督指導の仕組みや、委託先とのコミュニケーションの仕組みも、一応、作られている<br>・委託にかかる契約書等での委託元と委託先双方の責務には、これらは概ね反映されているが、まだ、見直すべきところもある<br>・委託先におけるセキュリティ要求の実践は十分であることは、継続的に確認されているが、それほどは徹底したものとは言い難い<br>・委託先とのセキュリティ対策に関するコミュニケーションは行われているが十分に密とは言えない<br>・外部委託におけるセキュリティの確保の方法についての検討のレベルはクラスB以上<br>・委託先でのセキュリティ要求の実践についての確認の徹底状況はクラスB以上<br>・業務の外部委託についてのセキュリティ対策についての見直し状況はクラスB以上<br>・業務の外部委託についてのセキュリティ対策や委託先も含むその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | 外部に委託する業務運用に対するセキュリティ要求の検討、ならびに委託先へのその実践の要求ならびにその監督指導等のシステム運用の委託についてのセキュリティ対策についてお組織的な取組みは行われているが、十分とはいえないところもある。業務の外部委託を要因とするセキュリティ事故も、起こりうる。<br>・委託先に対するセキュリティ要求は示されているが、大まかなもので、重要なところを除いては十分とは言えないところがある<br>・委託にかかる契約書等での委託元と委託先双方の責務は示されているが、大まかなもので、具体性に欠ける<br>・委託先におけるセキュリティ要求の実践は、すべて委託先に任されているが、その状況についての報告は受けている<br>・外部委託におけるセキュリティの確保の方法についての検討のレベルはクラスB以上<br>・委託先でのセキュリティ要求の実践についての確認の徹底状況はクラスB以上 |

| | |
|---|---|
| | ・業務の外部委託についてのセキュリティ対策についての見直し状況はクラスＢ以上<br>・業務の外部委託についてのセキュリティ対策や委託先も含むその実践状況についての文書化のレベルはクラスＢ以上 |
| レベル2 | 外部への業務運用の委託にあたってのセキュリティ要求は行われているが、一般的なものに止まっており、すべては委託策に任されており、実質的な管理は行ってない。<br>・業務運用の委託にあたってのセキュリティ要求は、大まかなものではあるが委託先に示されている<br>・委託先での、セキュリティ要求に対する必要な対応の実践の確認については、大まかなものであるが定期的な報告を受けている<br>・委託先とのセキュリティ対策に関するコミュニケーションは行われているが十分に密とは言えない<br>・外部委託におけるセキュリティの確保の方法についての検討のレベルはクラスＣ以上<br>・委託先でのセキュリティ要求の実践についての確認の徹底状況はクラスＣ以上<br>・業務の外部委託についてのセキュリティ対策についての見直し状況はクラスＣ以上<br>・業務の外部委託についてのセキュリティ対策や委託先も含むその実践状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | 外部委託している業務運用のセキュリティ対策はすべて委託先任せで、委託先の責任も委託先の方針をそのまま受け入れている。<br>・レベル2の達成要件も満たしていない |

(注1) 業務運用の外部委託についてのセキュリティ方針として示されるべき事項
・委託可能な業務の範囲と委託してはならない範囲
・業務の外部委託にあたってセキュリティ面で担保すべき事項への対応方針
・外部に委託している業務に対する管理についての方針
・委託先との責任の分担とその担保についての方針
・委託先の信用のレベルとその確認方法

(注2) 業務運用の外部委託に対するセキュリティ要求として示される事項
・可用性についての具体的な要求
・システムの処理の正確性についての要求レベル
・情報の秘匿についての具体的な要求
・情報の保全についての具体的な要求
・トラブル時における相互が協力する措置
　－代替手段の準備
　－原因の究明や対策実施についての連携方法
・運用の保全についての要求のレベル

## 2.1.3. 業務現場での情報の保護の徹底

| Ba3.1 | 印刷物の作成や安全な取り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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 保護対象となる情報を含む印刷物の作成や取扱いについての完成度の高いきめの細かいルールが確立している。印刷物のルールに沿った取り扱いを実現するための職場環境も十分なものが整備されている。利用者へのこのルールは完全に浸透しており、その遵守も完全に習慣化されている。また、印刷物の作成やルールに沿った取扱いについての管理も徹底しており、印刷物の作成や取り扱いで情報の保全上の不手際が生じる余地は、まずない。<br>・印刷物の全ライフサイクルの管理・取扱いルールが、全社的に定められた保護基準に従って、全ての部門において保護要件が厳密に指定されている<br>・印刷物の作成や安全な取扱いや、その確実な実践を支えるための完成度の完成度の高い取り扱い上のルール（注1）が確立している<br>・保護レベルのものから低いものまで保護対象とすべき印刷物のすべてに対して、網羅的にラベル付けすることが定められている<br>・意図的な不正も含め、不正な印刷や複製を完全に制限することができるルールが確立されている<br>・リスクに応じて十分に安全な配布手段が指定されており、それら配布する際の手続きが明確に定められている<br>・リスクに応じて十分に安全な保管手段が指定されており、アクセス権限者以外の利用を厳格に制限することができるルールが定められている<br>・リスクに応じて十分に安全な廃棄手段が指定されており、廃棄物から情報が漏えいするリスクを最小限に抑えている<br>・全ライフサイクルにおける記録管理が明確に指定され、意図的な不正行為が発生しても、トレースバックすることが可能である<br>・定期的な教育や、日常的な啓蒙活動を通して、印刷物の作成や安全な取扱いついてのルールの徹底と、実践の習慣化が徹底して追及されている<br>・印刷物の安全な管理をするための設備も十分なものが整えられている<br>・印刷物の作成や安全な取扱いについてのルールの遵守を監督、指導する仕組みが確立している<br>・これらの管理上の仕組みに沿った可搬メディアの取扱いについてのルールの遵守についてのチェックは厳格に行われている<br>・印刷物の作成や安全な取扱いに関するルールの見直しのレベルはクラスA<br>・印刷物の作成や安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスA |
| レベル4 | 保護対象となる情報を含む印刷物の作成や取扱いについてのよく検討されたきめの細かいルールが確立している。印刷物のルールに沿った取り扱いを実現するための職場環境も十分なものが整備されている。利用者へのこのルールは完全に浸透しており、その遵守もよく習慣化されている。また、印刷物の作成やルールに沿った取扱いについての管理も行われているが、一部に徹底さを欠くところも見られ、情報の保全という点での、印刷物の作成や取り扱いで、情報の保全上の不手際が生じる隙が僅かながら残っている。<br>・印刷物の作成や安全な取扱いについて、その確実な実践を支えるためのよく検討された取扱い上のルール（注1）が示されているが、まだ改善の余地もある<br>・印刷物の全ライフサイクルの管理・取扱いルールが、全社的に定められた保護基準に従って、主要部署のみならず多くの部署において保護要件が厳密に指定されている<br>・不正な印刷や複製を完全に制限することができるルールが確立されている<br>・配布、保管、廃棄する際の手続き、および、実施手段が定められ、重要な情報については安全な方法といえる<br>・全ライフサイクルにおける記録管理が明確に指定されているが、意図的な不正行為が発生した場合に、トレースバックできるほどではない<br>・保護レベルの高い印刷物から低い印刷物まで網羅的にラベル付けすることが定められている<br>・指定された保護要件を実行に移すためのプロセスが確立している<br>・印刷物の安全な管理をするための設備も十分なものが整えられている |

| | |
|---|---|
| | ・定期的な教育や、日常的な啓蒙活動を通して、印刷物の作成や安全な取扱いについてのルールの徹底と、実践の習慣化を追及しているが、一部に徹底さを欠くところも見られる<br>・印刷物の作成や安全な取扱いについてのルールの遵守を監督、指導する仕組みも確立しているが、まだ改善の余地がある<br>・これらの管理上の仕組みに沿った印刷物の作成や安全な取扱いのルールの遵守に対するチェックは、概ね、厳格に行われているが、徹底さに欠けるところが見られる<br>・印刷物の作成や安全な取扱いに関するルールの見直しのレベルはクラスB以上<br>・印刷物の作成や安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスB以上 |
| レベル3 | 保護対象となる情報を含む印刷物の作成や取扱いについて、ある程度きめの細かいルールが示されている。印刷物のルールに沿った取り扱いを実現するための職場環境も整備されている。利用者へのこのルールの浸透も図られ、概ね、習慣化されている。ルールに沿った印刷物の作成や取扱いについての管理も行われているが徹底したものではなく、印刷物の作成や取り扱いで、情報の保全上の不手際が生じる不安は残る。<br>・大まかではあるが印刷物の作成や安全な取扱いについてのルール（注1）やその実践を管理するための仕組みが示されている<br>・印刷物の全ライフサイクルの管理・取扱いルールが、全社的に定められた保護基準に従って、主要部署に対してのみ保護要件が厳密に指定されている。または、印刷物の全ライフサイクルの管理／取扱いルールが、原則レベルでは全社的に指定されているが、各部門の環境に合わせたルールのブレイクダウンが不十分。または、ライフサイクルの一部分のみの管理／取り扱いルールのみが厳密に指定されている<br>・意図的な不正な印刷／複製を制限することはできないが、ルールを遵守することでそれを制限することが可能なルールが確立されている<br>・配布、保管、廃棄する際の手続き、および、実施手段が定められているが、リスクと比較した場合、十分とは言えない<br>・印刷物の全ライフサイクルの一部分について記録管理するルールが存在する<br>・保護レベルの高い印刷物についてのみラベル付けをすることが定められている<br>・定期的な教育や、日常的な啓蒙活動を通して、印刷物の作成や安全な取扱いに関するルールの徹底と、実践の習慣化を追及しているが、徹底したものではない<br>・印刷物の安全な管理をするために必要な設備も整えられている<br>・大まかではあるが、印刷物の作成や安全な取扱いについてのルールの遵守を監督、指導する仕組みも作られている<br>・これらの管理上の仕組みに沿った印刷物の作成や安全な取扱いについてのルールの遵守に対するチェックも行われるようになっているが、徹底したものではない<br>・印刷物の作成や安全な取扱いに関するルールの見直しのレベルはクラスC以上<br>・印刷物の作成や安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスC以上 |
| レベル2 | 大まかではあるが、印刷物の作成や取扱いについてのルールが決められ、業務現場等に示されているが、その実践は個々人に任されており、組織的な管理は行われていない。印刷物の作成や取り扱いで、情報の保全上の不手際が生じる可能性は低くはない。<br>・大まかではあるが印刷物の作成や取扱いについてのルールや注意事項が示されている<br>・業務現場には、この注意事項の遵守が要求されている<br>・印刷物の作成や安全な取扱いの実践についての組織的なチェックはほとんど行われていない |
| レベル1 | 印刷物の作成や安全な取扱い、全て利用者の注意に任されており、セキュリティ面でのその適切な取扱いの実現についての組織的な取組はないに等しい。<br>・レベル2の達成条件も満たせない |

(注1) 印刷物の作成や安全な取扱いについてルールで規程すべき事項

・印刷物の作成および複製についてのルール（印刷や複写の制限の指定、複製の記録の作成についての指定、印刷出力時の安全の確保についての留意事項）

・配布（輸送・送信）に吐いてのルール（配布手段の指定、配布手続きの指定、配布記録の作成についての指定）

・保管についてのルール（保管場所や保管方法の指定、保管場所への入出庫管理についての指定、アクセス記録の作成についての指定）

・廃棄および資源としての再利用についてのルール（廃棄実施までの保管についての指定、廃棄方法の指定、廃棄手続きの指定、廃棄記録の指定）

| 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 可搬メディアの使用においては、その安全な使用をサポートについて、最も進んだツールや機能を使用するとともに、これらの取扱いについての完成度の高いきめの細かいルールを確立している。利用者へのこのルールは完全に浸透しており、その遵守も完全に習慣化されている。また、可搬メディアのルールに沿った取扱いについての管理も徹底しており、これらの機器の取り扱いで不手際が生じる余地は、まずない。<br>・可搬メディアの安全な利用について、現時点で利用可能な最も進んだ機能やツールが使えるところには、これらの機能を全面的に活用している<br>・可搬メディアのそれぞれについて、その安全な取扱いについての完成度の高いきめの細かい取扱い上のルール(注1)が確立している<br>・可搬メディアの全ライフサイクルの管理・取扱いルールが、全社的に定められた保護基準に従って、全ての部門において厳密に指定されている<br>・意図的な不正も含め、不正な可搬メディアの利用やデータコピーを完全に制限することができるルールが確立されている<br>・リスクに応じて十分に安全な配布手段が指定されており、それら配布する際の手続きが明確に定められている<br>・リスクに応じて十分に安全な保管手段が指定されており、アクセス権限者以外の利用を厳格に制限することができるルールが定められている<br>・リスクに応じて十分に安全な廃棄手段が指定されており、廃棄物から情報が漏えいするリスクを最小限に抑えている<br>・全ライフサイクルにおける記録管理が明確に指定され、意図的な不正行為が発生しても、トレースバックすることが可能である<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の可搬メディアの利用者に定められたルールの徹底と、実践の習慣化が徹底して追及されている<br>・可搬メディアの取扱いについてのルールの遵守を監督、指導する仕組みが確立している<br>・これらの管理上の仕組みに沿った可搬メディアの取扱いについてのルールの遵守についてのチェックは厳格に行われている<br>・可搬メディアの安全な取扱いに関するルールの見直しのレベルはクラスA<br>・可搬メディアの安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスA |
| レベル4 | 可搬メディアの使用においては、その安全な使用をサポートする機能やツールを適切に使用するとともに、その取扱いについてのよく検討されたきめの細かいルールを確立している。業務現場等にこのルールはよく浸透しており、その遵守も、よく習慣化されている。可搬メディアのルールに沿った取扱いについての管理も行われているが、一部に徹底さを欠くところも見られる。可搬メディアの取り扱いで不手際が生じる余地は、少ないが残る。<br>・可搬メディアの安全な利用について、利用可能な機能やツールが使えるところには、これらの機能の使用を追及している<br>・可搬メディアのそれぞれについて、その安全な取扱いについて、よく検討されたきめの細かい取扱い上のルール(注1)が示されているが、まだ改善の余地もある<br>・可搬メディアの全ライフサイクルの管理・取扱いルールが、全社的に定められた保護基準に従って、原則レベルでは全社的に指定され、主要部署のみならず多くの部署において厳密に指定されている<br>・不正な利用やデータコピーを完全に制限することができるルールが確立されている<br>・配布、保管、廃棄する際の手続き、および、実施手段が定められ、重要な情報は漏えいする可能性は少ないといえる<br>・全ライフサイクルにおける記録管理が明確に指定されているが、意図的な不正行為が発生した場合に、トレースバックできるほどではない<br>・保護レベルの高い可搬メディアから低い可搬メディアまで網羅的にラベル付けすることが定められている<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の可搬メディアの利用者に定められたル |

| | |
|---|---|
| | ールの徹底と、実践の習慣化を追及しているが、一部に徹底さを欠くところも見られる<br>・可搬メディアの取扱いについてのルールの遵守を監督、指導する仕組みも確立しているが、まだ改善の余地がある<br>・これらの管理上の仕組みに沿った可搬メディアの取扱いについてのルールの遵守についてのチェックは、概ね、厳格に行われているが、徹底さに欠けるところが見られる<br>・可搬メディアの安全な取扱いに関するルールの見直しのレベルはクラスB以上<br>・可搬メディアの安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスB以上 |
| レベル3 | 可搬メディアの安全な使用のための機能やツールの使用についての工夫も行われており、可搬メディアの取扱いについてのある程度きめの細かいルールが示されている。可搬メディアの利用者へのこのルールの徹底も図られ、その遵守も、概ね、習慣化されている。情報機器のルールに沿った取扱いについての管理も行われているが徹底したものではなく、可搬メディアの取り扱いで不手際が生じる不安は残る。<br>・大まかではあるが可搬メディアの取扱い上のルール（注1）が示されている<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の可搬メディアの利用者に定められたルールの徹底と、実践の習慣化を追及しているが、徹底したものではない<br>・可搬メディアの全ライフサイクルの管理・取扱いルールが、全社的に定められた保護基準に従って、主要部署に対してのみ保護要件が厳密に指定されている。または、可搬メディアの全ライフサイクルの管理／取扱いルールが、原則レベルでは全社的に指定されているが、各部門の環境に合わせたルールのブレイクダウンが不十分。または、ライフサイクルの一部分のみの管理／取り扱いルールのみが厳密に指定されている<br>・意図的な不正利用／データコピーを制限することはできないが、ルールを遵守することでそれを制限することが可能なルールが確立されている<br>・配布、保管、廃棄する際の手続き、および、実施手段が定められているが、リスクと比較した場合、十分とは言えない<br>・可搬メディアの全ライフサイクルの一部分について記録管理するルールが存在する<br>・保護レベルの高い可搬メディアについてのみラベル付けをすることが定められている<br>・大まかではあるが、可搬メディアの取扱いについてのルールの遵守を監督、指導する仕組みも作られている<br>・これらの管理上の仕組みに沿った可搬メディアの取扱いについてのルールの遵守についてのチェックも行われるようになっているが、徹底したものではない<br>・可搬メディアの安全な取扱いに関するルールの見直しのレベルはクラスB以上<br>・可搬メディアの安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守　の状況や管理についての文書化のレベルはクラスB以上 |
| レベル2 | 大まかではあるが、可搬メディアの取扱いについてのルールが決められ、業務現場等に示されているが、その実践は個々人に任されており、組織的な管理は行われていない。可搬メディアの取り扱いで不手際が生じる可能性は低くはない。<br>・大まかではあるが可搬メディアに安全な取り扱いについてのルールや注意事項が示されている<br>・可搬メディアの利用者には、この注意事項の遵守が要求されている<br>・可搬メディアの安全な取扱いの実践についての組織的なチェックはほとんど行われていない<br>・可搬メディアの安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスB以上 |
| レベル1 | 可搬メディアの安全な取り扱いは、全て利用者の注意に任されており、セキュリティ面でのその適切な取扱いの実現についての組織的な取組はないに等しい。<br>・レベル2の達成条件も満たせない |

(注1) 可搬メディアの安全な取扱いについてルールで規程すべき事項
- ・可搬メディアの利用（新規作成・複製の作成）ついてのルール（利用の制限の指定、利用記録の取得についての指定、利用時の情報の保全等の安全確保についての留意事項）
- ・配布（輸送・送信）に吐いてのルール（配布手段の指定、配布手続きの指定、配布記録の作成についての指定）
- ・保管についてのルール（保管場所や保管方法の指定、保管場所への入出庫管理についての指定、アクセス記録の作成についての指定）
- ・廃棄および資源としての再利用についてのルール（廃棄実施までの保管についての指定、廃棄方法の指定、廃棄手続きの指定、廃棄記録の指定）

| 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 情報機器の使用においては、その安全な使用をサポートについて、最も進んだ機能を使用するとともに、これらの機器の取扱いについての完成度の高いきめの細かいルールを確立している。利用者へのこのルールは完全に浸透しており、その遵守も完全に習慣化されている。また、情報機器のルールに沿った取扱いについての管理も徹底しており、これらの機器の取り扱いで不手際が生じる余地は、まずない。<br>・情報機器の安全な利用について、現時点で利用可能な最も進んだ機能が使えるところには、これらの機能を全面的に活用している<br>・情報機器のそれぞれについて、その安全な取扱いについての完成度の高いきめの細かい取扱い上のルール（注1）が確立している<br>・情報機器の全ライフサイクルの管理／取扱いルールが、全ての部門において厳密に指定されている<br>・意図的な不正も含め、不正な情報機器の利用を完全に制限することができるルール（物理的、技術的、人的）が確立されている<br>・リスクに応じて十分に安全な輸送手段が指定されており、それら輸送する際の手続きが明確に定められている<br>・リスクに応じて十分に安全な保管手段が指定されており、利用権限者以外の利用を厳格に制限することができるルールが定められている<br>・リスクに応じて十分に安全な廃棄手段が指定されており、廃棄物から情報が漏えいするリスクを最小限に抑えている<br>・全ライフサイクルにおける記録管理が明確に指定され、意図的な不正行為が発生しても、トレースバックすることが可能である<br>・指定された保護要件を実行に移すためのプロセスが確立している<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の情報機器の利用者に定められたルールの徹底と、実践の習慣化が徹底して追及されている<br>・これらの機器の取扱いについてのルールの遵守を監督、指導する仕組みが確立している<br>・これらの管理上の仕組みに沿ったこれらの機器の取扱いについてのルールの遵守についてのチェックは厳格に行われている<br>・電子機器の安全な取扱いに関するルールの見直しのレベルはクラスA<br>・電子機器の安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスA |
| レベル4 | 情報機器の使用においては、その安全な使用をサポートする機能を持つ機器を使用するとともに、その取扱いについてのよく検討されたきめの細かいルールを確立している。業務現場等にこのルールはよく浸透しており、その遵守も、よく習慣化されている。情報機器のルールに沿った取扱いについての管理も行われているが、一部に徹底さを欠くところも見られる。これらの機器の取り扱いで不手際が生じる余地は、少ないが残る。<br>・情報機器の安全な利用について、利用可能な機能が使えるところには、これらの機能の使用を追及している<br>・情報機器のそれぞれについて、その安全な取扱いについて、よく検討されたきめの細かい取扱い上のルール（注1）が示されているが、まだ改善の余地もある<br>・情報機器の全ライフサイクルの管理／取扱いルールが、原則レベルで全社的に指定され、主要部署のみならず多くの部署において厳密に指定されている<br>・不正な利用を完全に制限することができるルールが確立されている<br>・輸送、保管、廃棄する際の手続き、および、実施手段が定められ、リスクは少ないと言える<br>・全ライフサイクルにおける記録管理が明確に指定されているが、意図的な不正行為が発生した場合に、トレースバックできるほどではない<br>・指定された保護要件を実行に移すためのプロセスが確立している<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の情報機器の利用者に定められたルールの徹底と、実践の習慣化を追及しているが、一部に徹底さを欠くところも見られる<br>・これらの機器の取扱いについてのルールの遵守を監督、指導する仕組みも確立しているが、まだ改 |

| | |
|---|---|
| | 善の余地がある<br>・これらの管理上の仕組みに沿ったこれらの機器の取扱いについてのルールの遵守についてのチェックは、概ね、厳格に行われているが、徹底さに欠けるところが見られる<br>・情報機器の安全な取扱いに関するルールの見直しのレベルはクラスB以上<br>・情報機器の安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスB以上 |
| レベル3 | 情報機器への安全な使用のための機能の使用についての工夫も行われており、情報機器の取扱いについてのある程度きめの細かいルールが示されている。情報機器の利用者へのこのルールの徹底も図られ、その遵守も、概ね、習慣化されている。情報機器のルールに沿った取扱いについての管理も行われているが徹底したものではなく、これらの機器の取り扱いで不手際が生じる不安は残る。<br>・大まかではあるが情報機器の取扱い上のルール（注1）が示されている<br>・情報機器の全ライフサイクルの管理・取扱いルールが、主要部署に対してのみ厳密に指定されている。または、情報機器の全ライフサイクルの管理／取扱いルールが、原則レベルでは全社的に指定されているが、各部門の環境に合わせたルールのブレイクダウンが不十分。または、ライフサイクルの一部分のみの管理／取り扱いルールのみが厳密に指定されている<br>・意図的な不正利用を制限することはできないが、ルールを遵守することでそれを制限することが可能なルールが確立されている<br>・輸送、保管、廃棄する際の手続き、および、実施手段が定められているが、リスクと比較した場合、十分とは言えない<br>・全ライフサイクルの一部分について記録管理するルールが存在する<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の情報機器の利用者に定められたルールの徹底と、実践の習慣化を追及しているが、徹底したものではない<br>・大まかではあるが、これらの機器の取扱いについてのルールの遵守を監督、指導する仕組みも作られている<br>・これらの管理上の仕組みに沿ったこれらの機器の取扱いについてのルールの遵守についてのチェックも行われるようになっているが、徹底したものではない<br>・情報機器の安全な取扱いに関するルールの見直しのレベルはクラスC以上<br>・情報機器の安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスC以上 |
| レベル2 | 大まかではあるが、情報機器の取扱いについてのルールが決められ、業務現場等に示されているが、その実践は個々人に任されており、組織的な管理は行われていない。これらの機器の取り扱いで不手際が生じる可能性は低くはない。<br>・大まかではあるが情報機器に安全な取り扱いについてのルールや注意事項が示されている<br>・情報機器の利用者には、この注意事項の遵守が要求されている<br>・情報機器の安全な取扱いの実践についての組織的なチェックはほとんど行われていない |
| レベル1 | 情報機器の安全な取り扱いは、全て利用者の注意に任されており、セキュリティ面でのその適切な取扱いの実現についての組織的な取組はないに等しい。<br>・レベル2の達成条件も満たせない |

(注1) 電子機器の安全な取扱いについてルールで規程すべき事項
- ・利用上（情報の作成、複製の作成、情報の検索、情報の2次加工）ついてのルール（機器の不正使用の防止策、画面上の情報の安全策、保護の利用の制限の指定、利用記録の取得についての指定、利用時の情報の保全等の安全確保についての留意事項）
- ・配布（輸送・送信）に吐いてのルール（配布手段の指定、配布手続きの指定、配布記録の作成についての指定）
- ・保管についてのルール（保管場所や保管方法の指定、保管場所への入出庫管理についての指定、アクセス記録の作成についての指定）
- ・廃棄および資源としての再利用についてのルール（廃棄実施までの保管についての指定、廃棄方法の指定、廃棄手続きの指定、廃棄記録の指定）

| Ba3.4 | その他の電子機器(注1)の安全な使用についてのルールの確立と、ルールに沿った取扱いの実践 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 保護対象とすべきその他の電子機器については、その安全な使用をサポートについて最も進んだ機能を持つ機器を使用するとともに、これらの機器の取扱いについての完成度の高いきめの細かいルールが確立している。業務現場等へのこのルールは完全に浸透しており、その遵守も完全に習慣化されている。また、情報機器のルールに沿った取扱いについての管理も徹底しており、これらの機器の取り扱いで不手際が生じる余地は、まずない。<br>・利用の安全をサポートする機能を持つ機器については、現時点で利用可能な最も進んだ機能を持つ機器を使用し、これらの機能を全面的に活用している<br>・その他の電子機器で保護対象とすべきものが明確にされており、そのそれぞれに対し完成度の高いきめの細かい取扱い上のルール(注2)が確立している<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の全従業員に対して定められたルールの徹底と、実践の習慣化が徹底して追及されている<br>・これらの機器の取扱いについてのルールの遵守を監督、指導する仕組みが確立している<br>・これらの管理上の仕組みに沿ったこれらの機器の取扱いについてのルールの遵守についてのチェックは厳格に行われている<br>・電子機器の安全な取扱いに関するルールの見直しのレベルはクラスA<br>・電子機器の安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスA |
| レベル4 | 保護対象とすべきその他の電子機器については、その安全な使用をサポートする機能を持つ機器を使用するとともに、その取扱いについてのよく検討されたきめの細かいルールを確立している。業務現場等にこのルールはよく浸透しており、その遵守も、よく習慣化されている。情報機器のルールに沿った取扱いについての管理も行われているが、一部に徹底さを欠くところも見られる。これらの機器の取り扱いで不手際が生じる余地は、少ないが残る。<br>・利用の安全をサポートする機能を持つ機器については、そのような機能を提供する機器を使用し、これらの機能を全面的に活用している<br>・その他の電子機器で保護対象とすべきものが明確にされており、そのそれぞれに対しよく検討されたきめの細かい取扱い上のルール(注1)が示されているが、まだ改善の余地もある<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の全従業員に対して定められたルールの徹底と、実践の習慣化を追及しているが、一部に徹底さを欠くところも見られる<br>・これらの機器の取扱いについてのルールの遵守を監督、指導する仕組みも確立しているが、まだ改善の余地がある<br>・これらの管理上の仕組みに沿ったこれらの機器の取扱いについてのルールの遵守についてのチェックは、概ね、厳格に行われているが、徹底さに欠けるところが見られる<br>・電子機器の安全な取扱いに関するルールの見直しのレベルはクラスB以上<br>・電子機器の安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラスB以上 |
| レベル3 | 組織的に検討された保護対象となるその他の電子機器の取扱いについてのある程度きめの細かいルールが示されており、業務現場等へのこのルールの徹底は図られ、その遵守も、概ね、習慣化されている。これらの電子機器のルールに沿った取扱いについての管理も行われているが徹底したものではなく、これらの機器の取り扱いで不手際が生じる不安は残る。<br>・その他の電子機器で保護対象とすべきものが明確にされており、そのそれぞれに大まかではあるが取扱い上のルール(注1)が示されている<br>・定期的な教育や、日常的な啓蒙活動を通して、全ての部門の全従業員に対して定められたルールの徹底と、実践の習慣化を追及しているが、徹底したものではない<br>・大まかではあるが、これらの機器の取扱いについてのルールの遵守を監督、指導する仕組みも作られている<br>・これらの管理上の仕組みに沿ったこれらの機器の取扱いについてのルールの遵守についてのチェックも行われるようになっているが、徹底したものではない<br>・電子機器の安全な取扱いに関するルールの見直しのレベルはクラスB以上 |

| | |
|---|---|
| | ・電子機器の安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラス B 以上 |
| レベル 2 | 大まかではあるが、保護対象とすべきその他の電子機器の取扱いについてのルールが決められ、業務現場等に示されているが、その実践は個々人に任されており、組織的な管理は行われていない。これらの機器の取り扱いで不手際が生じる可能性は低くはない。<br>・保護対象機器ごとに管理ルールが定められてはいないが、ある程度リスクを有する機器に対してはその利用をある程度、規制する等の措置を行っている<br>・明示的なルールは存在しないが、各部門の責任による安全な利用を義務付けており、対象機器の安全な取扱いは、ある程度習慣化されている<br>・定期的に教育を実施していないが、利用規制や利用上の注意事項は、利用者が常に参照できるところに示している<br>・電子機器の安全な取扱いについてのルールやその遵守を徹底するための管理上の仕組みや、遵守の状況や管理についての文書化のレベルはクラス C 以上 |
| レベル 1 | 保護対象とすべきその他の電子機器の取り扱いは、全て利用者の注意に任されており、セキュリティ面でのその適切な取扱いの実現についての組織的な取組はないに等しい。<br>・レベル 2 の達成条件も満たせない |

(注1) 保護対象としてその安全な利用を検討すべき電子機器
・複写機、FAX、プリンタ、スキャナ等のデジタル複合機
・携帯電話
・デジタルカメラ

(注2) 注 1 に示すような電子機器の取扱いについてのルールで規程すべき事項

| その他の機器の例 | 保護要件（物理的、技術的、人的）として規程すべき事項 |
|---|---|
| デジタル複合機<br>（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<br>・外部からの不正アクセス対策<br>-電話回線を利用する機能の制限<br>-LAN からのアクセス制限<br>・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<br>-パスワードロック<br>-携帯電話内への保存内容の限定<br>・公共の場における機密会話の制限<br>・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<br>-記憶媒体内の情報の完全消去の徹底<br>・社内における不正利用の禁止<br>・情報の消去し忘れ防止対策 |

## 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | ユーザの管理についての完成度の高いルール（注1）が確立しており、このルールに沿ったユーザの管理が徹底して行われており、ユーザの管理で不手際が生じることは、まず考えられない。<br>・登録ユーザに管理についての完成度の高いルール（注1）が確立している<br>・すべての登録ユーザについて、当初の登録時における正当性や必要な属性についての徹底した確認や、その後のユーザの身分の変更等に対するユーザ情報のメンテナンスも、ルールに沿って厳格に行われていて、登録ユーザについての情報に不正なものが入り込む余地は、まずない<br>・すべての登録ユーザについて、権限の付与および付与した権限に対する、ユーザの身分の変更等に対応したメンテナンスも、ルールに沿って厳格に行われていて、ユーザへの権限付与に不手際が入り込む余地は、まずない<br>・すべての登録ユーザについて、ユーザの認証に用いる情報の設定や、そのユーザへの交付も、ルールに沿って厳格に行われていて、ユーザの認証に用いる情報に関して不手際が入り込む余地は、まずない<br>・システムへのユーザの登録ならびに権限の登録、および必要に応じた変更も、ルールに沿って厳格に行われていて、システム上のこれらについての情報に不正なものが入り込む余地は、まずない<br>・ユーザ管理についてのルールに対する見直しのレベルはA<br>・ユーザ管理についてのルールやユーザ管理の実践の記録等についての文書化のレベルはクラスA |
| レベル4 | ユーザの管理についてのよく検討されたルールが確立しており、このルールに沿ったユーザの管理も行われているが、一部に徹底さを欠くところもあるユーザ管理は概ね十分に行われていると見ることができるが、ユーザの管理で不手際が生じる隙が、少ないが残されている。<br>・登録ユーザに管理についてのよく検討されたルール（注1）が確立しているが、まだ改善の余地はある<br>・すべての登録ユーザについて、当初の登録時における正当性や必要な属性についての確認や、その後のユーザの身分の変更等に対するユーザ情報のメンテナンスも、ルールに沿って行われていているが、一部に徹底さを欠くところも見られ、登録ユーザについての情報に不正なものが入り込む隙が僅かではあるが残されている<br>・すべての登録ユーザについて、権限の付与および付与した権限に対する、ユーザの身分の変更等に対応したメンテナンスも、ルールに沿って行われていているが、一部に徹底さを欠くところも見られ、ユーザへの権限付与に不手際が入り込む隙が僅かではあるが残されている<br>・すべての登録ユーザについて、権限の付与および付与した権限に対する、ユーザの身分の変更等に対応したメンテナンスも、ルールに沿って行われているが、一部に徹底さを欠くところもあり、ユーザへの権限付与に不手際が入り込む余地僅かではあるが残されている<br>・すべての登録ユーザについて、ユーザの認証に用いる情報の設定や、そのユーザへの交付も、ルールに沿って行われているが、一部に徹底さを欠くところもあり、ユーザの認証に用いる情報に関して不手際が入り込む余地僅かではあるが残されている<br>・システムへのユーザの登録ならびに権限の登録、および必要に応じた変更も、ルールに沿って行われていているが、一部に徹底さを欠くところも見られ、システム上のこれらについての情報に不正なものが入り込む隙が僅かではあるが残されている<br>・ユーザ管理についてのルールに対する見直しのレベルはB以上<br>・ユーザ管理についてのルールやユーザ管理の実践の記録等についての文書化のレベルはクラス B以上 |
| レベル3 | 大まかではあるが、ユーザの管理についてのルールが示されており、このルールに沿ったユーザの管理も行われているが、徹底したものではない。ユーザ管理は組織的に行われてはいるが、十分なものとは言えず、ユーザの管理で不手際が生じる可能性も残っている。<br>・大まかではあるが、登録ユーザに管理についてのルール（注 1）が示されているが、改善の余地は少なくない<br>・登録ユーザについて、当初の登録時における正当性や必要な属性についての確認や、その後のユーザの身分の変更等に対するユーザ情報のメンテナンスも、ルールに沿って行われていているが、すべてのユーザに徹底したものではない。登録ユーザについての情報に不正なものが入り込む隙が残 |

| | |
|---|---|
| | されている<br>・登録ユーザについて、権限の付与および付与した権限に対する、ユーザの身分の変更等に対応したメンテナンスも、ルールに沿って行われていているが、すべてのユーザに徹底したものではない。ユーザへの権限付与に不手際が入り込む隙が残されている<br>・登録ユーザについて、ユーザの認証に用いる情報の設定や、そのユーザへの交付も、ルールに沿って行われているが、すべてのユーザに徹底したものではない。ユーザの認証に用いる情報に関して不手際が入り込む隙が残されている<br>・システムへのユーザの登録ならびに権限の登録、および必要に応じた変更も、ルールに沿って行われていているが、徹底したものではない。システム上のこれらについての情報に不正なものが入り込む隙が残されている<br>・ユーザ管理についてのルールに対する見直しのレベルはＢ以上<br>・ユーザ管理についてのルールやユーザ管理の実践の記録等についての文書化のレベルはクラス Ｂ以上 |
| レベル2 | ユーザ管理の担当者間で習慣的に形成されてルールは存在し、担当者はこのルールに沿ってユーザの管理を行っている。担当者はそれなりに注意深く行い、ある程度の管理は行われているもの、組織的な管理が行われているとは言い難く、ユーザの管理の信頼性は高くない。<br>・登録ユーザに管理について、大まかではあるが担当者間で習慣的に形成されたルールが存在し、機能している<br>・登録ユーザについて、当初の登録時における正当性や必要な属性についての確認や、その後のユーザの身分の変更等に対するユーザ情報のメンテナンスも、この習慣的なルールに沿って行われていている。登録ユーザについての情報の妥当性の確保は担当チームの注意に依存している<br>・登録ユーザについて、権限の付与および付与した権限に対する、ユーザの身分の変更等に対応したメンテナンスも、この習慣的なルールに沿って行われていている。ユーザへの権限付与の妥当性の確保は担当チームの注意に依存している<br>・システムへのユーザの登録ならびに権限の登録、および必要に応じた変更も、この習慣的なルールに沿って行われていている。システム上のこれらについての情報の妥当性の確保は担当チームの注意に依存している<br>・ユーザ管理についてのルールに対する見直しのレベルはＣ以上<br>・ユーザ管理についてのルールやユーザ管理の実践の記録等についての文書化のレベルはクラス Ｃ以上 |
| レベル1 | ユーザ管理のすべては、担当者に任されており、ユーザ管理を適切なものにするための組織的な取組みはないに等しい。<br>・レベル2の達成要件も満たしていない |

(注1)　ユーザの管理についてのルールとして規程すべき事項
・登録ユーザの正当性についての確認の基準（確認すべきことと確認方法等）と、その確認の手続き
・ユーザの属性の把握とその確認の基準（確認すべきことと確認方法等）と、その確認の手続き
・登録ユーザの身分等の追跡調査についての基準（チェックサイクル、チェックの方法等）と確認の手続き
・登録ユーザへの権限の付与基準と権限不要の手続き
・登録ユーザの身分等の変更に伴うユーザに付与した権限の変更手続き
・登録ユーザに付与した権限の妥当性のチェックの基準（チェックサイクル、チェック事項等）とチェックの手続き
・登録ユーザの認証に用いる情報についての基準とその決定ならびに交付手続き
・登録ユーザについての各種情報（ユーザID、属性情報、付与した権限情報、認証用情報等）のシステムへの登録手続き
・システム上の登録ユーザについての各種情報（ユーザID、属性情報、付与した権限情報、認証用情報等）の妥当性のチェックの基準（チェックサイクル、チェック事項等）とチェックの手続き

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | ユーザの不注意からなりすましによるシステムへのアクセスが発生するのを防ぐためのユーザへの指導が徹底しており、ユーザのこの点についての慎重な対応ができている。<br>・ユーザ側におけるパスワードの適切な管理等のなりすましの防止に向けたユーザ向けのガイドライン（注1）が整備されている<br>・よく検討されたこのガイドラインのユーザへの徹底の仕組み（注2）も確立しており、この仕組みに沿ってこれらのユーザへの伝達も、徹底して図られている<br>・ユーザにおけるガイドラインへの準拠状態の把握と必要に応じた指導も徹底して行われている<br>・当該要求についての対策の検討レベルはA<br>・なりすましの防止に向けたユーザの指導の方法やその管理方法についての見直しのレベルはA<br>・なりすましの防止に向けた施策やその実践についての記録等についての文書化のレベルはA |
| レベル4 | ユーザの不注意からなりすましによるシステムへのアクセスが発生するのを防ぐためのユーザへの指導には相当の努力を行っているが、一部に徹底さを欠くところも見られる。ユーザのこの点についての慎重な対応は、概ね、十分ではあるが、隙がないことはない。<br>・ユーザ側におけるパスワードの適切な管理等のなりすましの防止に向けたユーザ向けのガイドライン（注1）が整備されているが、まだ改善の余地がある<br>・よく検討されたこのガイドラインのユーザへの徹底の仕組み（注2）も確立しているが、まだ改善の余地がある。また、この仕組みに沿ってこれらのユーザへの伝達も努力されているが、徹底さに欠くところもある<br>・ユーザにおけるガイドラインへの準拠状態の把握と必要に応じた指導も行われているが、徹底したものではない<br>・当該要求についての対策の検討レベルはB以上<br>・なりすましの防止に向けたユーザの指導の方法やその管理方法についての見直しのレベルはB以上<br>・なりすましの防止に向けた施策やその実践についての記録等についての文書化のレベルはB以上 |
| レベル3 | ユーザの不注意からなりすましによるシステムへのアクセスが発生するのを防ぐためのユーザへの指導に行われているが、徹底したものではない。僅かではあろうが、不注意なユーザもあるある確率でてると考えなければならない。<br>・簡単なものであるが、ユーザ側におけるパスワードの適切な管理等のなりすましの防止に向けユーザに注意を喚起する文書等は作られている<br>・大まかではあるが、ユーザ側におけるこの注意文書の内容のユーザへの徹底の仕組み（注2）も作られている。また、この仕組みに沿ってこれらのユーザへの伝達も行われているが、徹底したものではない<br>・この注事事項への準拠についてのユーザの指導も、時々、行われているが徹底したものではない<br>・当該要求についての対策の検討レベルはB以上<br>・なりすましの防止に向けたユーザの指導の方法やその管理方法についての見直しのレベルはB以上<br>・なりすましの防止に向けた施策やその実践についての記録等についての文書化のレベルはB以上 |
| レベル2 | ユーザの不注意からなりすましによるシステムへのアクセスが発生するのを防ぐためのユーザへの指導は行われているが、形式的な域をでなく、十分とは言い難い。不注意なユーザも、あるある確率でてると考えなければならない。<br>・簡単なものであるが、ユーザ側におけるパスワードの適切な管理等のなりすましの防止に向けユーザに注意を喚起する文書等は作られている<br>・大まかではあるが、ユーザ側におけるこの注意文書の内容のユーザへの周知は、行われているが形式的な域をでない<br>・当該要求についての対策の検討レベルはC以上<br>・なりすましの防止に向けたユーザの指導の方法やその管理方法についての見直しのレベルはC以上<br>・なりすましの防止に向けた施策やその実践についての記録等についての文書化のレベルはC以上 |
| レベル1 | なりすましの防止についてのユーザへの指導は、行われていないに等しい。<br>・レベル2の達成要件も満たしていない |

(注1)　なりすまし防止策の一環としてユーザ側が注意すべき事項
・パスワード等のユーザ認証に用いる情報の設定うえの制約
・パスワード等のユーザ認証に用いる情報の注意深い取扱い（漏洩の防止）
・電子機器の使用上の注意事項（ログオンしたままの放置、外部の人が覗き見できる環境での使用他）

(注2)　なりすまし防止に向けたユーザへの指導の徹底の仕組みとして規定すべき事項
・ユーザへの注意事項の作成手続き
・これらのユーザでの周知手段（含む通知の確認方法）とその実施手続き
・ユーザにおける注意事項の遵守状況の把握方法

## 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法的要求の遵守 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | ビジネスパートナーとの契約にかかわる法的要求は、すべて正確に把握されており、業務現場他へのそれらへの対応のための具体策（注1）の展開が的確に図られている。また、業務現場におけるこれらの実践も徹底しており、ビジネスパートナーとの契約にかかわる法的要求の遵守に不手際が生じることは、まず考えられない。<br>・契約にかかわる法的要求事項は、すべて正確に把握、理解されている<br>・これらの要求は、要求を遵守するための的確な具体策に展開され、これらはマニュアル化されている<br>・これらの要求とその遵守のための具体策の対策現場への周知は徹底して図られている<br>・これらの要求の遵守をチェックするための仕組みも確立していて、必要な措置の実践は、この仕組みに沿って徹底してチェックされている<br>・契約にかかわる法的要求の遵守についての責任体制が明示され、関係者は自己の責務を十分に理解している<br>・契約にかかわる法的要求への対応についての検討のレベルはクラスA<br>・契約にかかわる法的要求への対応についての見直し状況はクラスA<br>・契約にかかわる法的要求への対応に関し指定された措置や、その実践状況についての文書化のレベルはクラスA |
| レベル4 | ビジネスパートナーとの契約にかかわる法的要求は、すべて正確に把握されており、業務現場他へのそれらへの対応のための具体策の展開が的確に図られている。また、業務現場におけるこれらの実践の徹底も図られているが、一部に徹底さを欠くところも見られ、ビジネスパートナーとの契約にかかわる法的要求の遵守に不手際が生じる隙が、僅かではあるが残されている。<br>・契約にかかわる法的要求事項は、すべて正確に把握、理解されている<br>・これらの要求は、要求を遵守するための的確な具体策に展開され、これらはマニュアル化されているが、これらには、まだ、改善の余地がある<br>・これらの要求とその遵守のための具体策の対策現場への周知の徹底は図られているが、一部に徹底さを欠くところも見られる<br>・これらの要求の遵守をチェックするための仕組みも確立していて、必要な措置の実践は、この仕組みに沿ってチェックされているが、一部に徹底さを欠くところも見られる<br>・契約にかかわる法的要求の遵守についての責任体制が明示され、関係者は自己の責務を、概ね、理解している<br>・契約にかかわる法的要求への対応についての検討のレベルはクラスB以上<br>・契約にかかわる法的要求への対応についての見直し状況はクラスB以上<br>・契約にかかわる法的要求への対応に関し指定された措置や、その実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | ビジネスパートナーとの契約にかかわる法的要求は、概ね、正確に把握されており、業務現場他へのそれらへの対応のための具体策の展開も図られ、業務現場におけるこれらの実践もチェックされているが、十分に徹底したものではない。ビジネスパートナーとの契約にかかわる法的要求の遵守に不手際が生じる余地が残されている。<br>・契約にかかわる法的要求事項は、概ね、正確に把握、理解されているが、すべてについての検証までには至っていない<br>・これらの要求は、大まかではあるが、要求を遵守するための具体策に展開され、マニュアル化されているが、改善の余地がある<br>・これらの要求とその遵守のための具体策の対策現場への周知も図られているが、徹底したものではない<br>・大まかではあるが、これらの要求の遵守をチェックするための仕組みも確立していて、必要な措置の実践は、この仕組みに沿ってチェックされているが、徹底したものではない<br>・契約にかかわる法的要求の遵守についての責任体制が示されているが、必ずしも徹底はしていない<br>・契約にかかわる法的要求への対応についての検討のレベルはクラスB以上<br>・契約にかかわる法的要求への対応についての見直し状況はクラスB以上 |

| | |
|---|---|
| | ・契約にかかわる法的要求への対応に関し指定された措置や、その実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | ビジネスパートナーとの契約にかかわる法的要求は、それぞれの関係者に任されている。担当者レベルでのその遵守について努力は認められるが、要求事項の漏れのない把握や理解、必要な措置への展開、その実践もチェックも組織的に行われているとは言えず、ビジネスパートナーとの契約にかかわる法的要求の遵守に不手際が生じる可能性は、低くはない。<br>・担当者は、契約にかかわる法的要求事項の把握や理解、要求を遵守するための具体策の検討を真剣に行っているが、これらについての組織的なチェックはないに等しい<br>・担当者は、必要な措置を知らされ、その実践について留意はしているが、組織的なチェックや指導は行われていても、形式的なもので実効性は疑問<br>・契約にかかわる法的要求への対応についての検討のレベルはクラスC以上<br>・契約にかかわる法的要求への対応についての見直し状況はクラスC以上<br>・契約にかかわる法的要求への対応に関し指定された措置や、その実践状況についての文書化のレベルはクラスC以上 |
| レベル1 | ビジネスパートナーとの契約からの要求の遵守に対する組織的な取り組みはないに等しい。<br>・レベル2の達成要件も満たしていない |

(注1) 法的要求への対応のための具体策として検討すべき事項
- ・法的要求の業務面での具体的な要求(意味)
- ・業務面での制約事項
- ・業務面での制約事項を遵守するための具体的手段
  - －関係する業務活動とその実行手順とチェックのポイント
- ・組織的なチェックのためのプロセス
- ・使用する文書やその様式等

## Ba5.2 事業に関係する法令やその他のルールの遵守

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 事業に関係する法令やその他のルールからくる要求は、すべて正確に把握されており、業務現場他へのそれらへの対応のための具体策(注1)の展開が的確に図られている。また、業務現場におけるこれらの実践も徹底しており、事業に関係する法令やその他のルールからくる要求の遵守に不手際が生じることは、まず考えられない。<br>・事業に関係する法令やその他のルールからくる要求事項は、すべて正確に把握、理解されている<br>・これらの要求は、要求を遵守するための的確な具体策に展開され、これらはマニュアル化されている<br>・これらの要求とその遵守のための具体策の対策現場への周知は徹底して図られている<br>・これらの要求の遵守をチェックするための仕組みも確立していて、必要な措置の実践は、この仕組みに沿って徹底してチェックされている<br>・事業に関係する法令やその他のルールからくる要求の遵守についての責任体制が明示され、関係者は自己の責務を十分に理解している<br>・事業に関係する法令やその他のルールからくる要求への対応についての検討のレベルはクラスA<br>・事業に関係する法令やその他のルールからくる要求への対応についての見直し状況はクラスA<br>・事業に関係する法令やその他のルールからくる要求への対応に関し指定された措置や、その実践状況についての文書化のレベルはクラスA |
| レベル4 | 事業に関係する法令やその他のルールからくる要求要求は、すべて正確に把握されており、業務現場他へのそれらへの対応のための具体策の展開が的確に図られている。また、業務現場におけるこれらの実践の徹底も図られているが、一部に徹底さを欠くところも見られ、事業に関係する法令やその他のルールからくる要求の遵守に不手際が生じる隙が、僅かではあるが残されている。<br>・事業に関係する法令やその他のルールからくる要求事項は、すべて正確に把握、理解されている<br>・これらの要求は、要求を遵守するための的確な具体策に展開され、これらはマニュアル化されている |

| | |
|---|---|
| | が、これらには、まだ、改善の余地がある<br>・これらの要求とその遵守のための具体策の対策現場への周知の徹底は図られているが、一部に徹底さを欠くところも見られる<br>・これらの要求の遵守をチェックするための仕組みも確立していて、必要な措置の実践は、この仕組みに沿ってチェックされているが、一部に徹底さを欠くところも見られる<br>・事業に関係する法令やその他のルールからくる要求の遵守についての責任体制が明示され、関係者は自己の責務を、概ね、理解している<br>・事業に関係する法令やその他のルールからくる要求への対応についての検討のレベルはクラス B 以上<br>・事業に関係する法令やその他のルールからくる要求への対応についての見直し状況はクラス B 以上<br>・事業に関係する法令やその他のルールからくる要求への対応に関し指定された措置や、その実践状況についての文書化のレベルはクラス B 以上 |
| レベル3 | 事業に関係する法令やその他のルールからくる要求要求は、概ね、正確に把握されており、業務現場他へのそれらへの対応のための具体策の展開も図られ、業務現場におけるこれらの実践もチェックされているが、十分に徹底したものではない。事業に関係する法令やその他のルールからくる要求の遵守に不手際が生じる余地が残されている。<br>・事業に関係する法令やその他のルールからくる要求事項は、概ね、正確に把握､理解されているが、すべてについての検証までには至っていない<br>・これらの要求は、大まかではあるが、要求を遵守するための具体策に展開され､マニュアル化されているが、改善の余地がある<br>・これらの要求とその遵守のための具体策の対策現場への周知も図られているが、徹底したものではない<br>・大まかではあるが、これらの要求の遵守をチェックするための仕組みも確立していて、必要な措置の実践は、この仕組みに沿ってチェックされているが、徹底したものではない<br>・事業に関係する法令やその他のルールからくる要求の遵守についての責任体制が示されているが、必ずしも徹底はしていない<br>・事業に関係する法令やその他のルールからくる要求への対応についての検討のレベルはクラス B 以上<br>・事業に関係する法令やその他のルールからくる要求への対応についての見直し状況はクラス B 以上<br>・事業に関係する法令やその他のルールからくる要求への対応に関し指定された措置や、その実践状況についての文書化のレベルはクラス B 以上 |
| レベル2 | 事業に関係する法令やその他のルールからくる要求は、それぞれの関係者に任されている。担当者レベルでのその遵守について努力は認められるが、要求事項の漏れのない把握や理解、必要な措置への展開、その実践もチェックも組織的に行われているとは言えず、事業に関係する法令やその他のルールからくる要求の遵守に不手際が生じる可能性は、低くはない。<br>・担当者は、事業に関係する法令やその他のルールからくる要求事項の把握や理解、要求を遵守するための具体策の検討を真剣に行っているが、これらについての組織的なチェックはないに等しい<br>・担当者は、必要な措置を知らされ、その実践について留意はしているが、組織的なチェックや指導は行われていても、形式的なもので実効性は疑問<br>・事業に関係する法令やその他のルールからくる要求への対応についての検討のレベルはクラス C 以上<br>・事業に関係する法令やその他のルールからくる要求への対応についての見直し状況はクラス C 以上<br>・事業に関係する法令やその他のルールからくる要求への対応に関し指定された措置や、その実践状況についての文書化のレベルはクラス C 以上 |
| レベル1 | 事業に関係する法令やその他のルールからくる要求の遵守に対する組織的な取り組みは、ないに等しい。<br>・レベル2の達成要件も満たしていない |

(注1)　事業に関係する法令やその他のルールからくる要求への対応のための具体策として検討すべき事項
・事業に関係する法令やその他のルールからくる要求の業務面での具体的な要求（意味）
・業務面での制約事項
・業務面での制約事項を遵守するための具体的手段
　－関係する業務活動とその実行手順とチェックのポイント
・組織的なチェックのためのプロセス
・使用する文書やその様式等

## Ba5.3 紛争の発生への備えの実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 情報セキュリティがかかわる紛争発生に備えての諸活動が円滑に行われるための組織面での環境が十分に整備されており、これらは完全に機能しており、万一、紛争になっても十分な対応はできると見られる。<br>・発生が予想される紛争のすべてが洗いだされ、それぞれの紛争のシナリオも組織的に検討されている<br>・想定される紛争のシナリオごとに対応手順が確立している<br>・検討された対応手順に対応して、必要な証跡の確保等の日常から準備すべき事項が的確に洗い出され、業務運用やシステムの運用への展開が図られている<br>・裁判上の証拠として用いられることが想定される記録確保は、法的効力を持てるような方法で取得、管理されるようになっている<br>・業務現場やシステムの運用現場において、紛争への備えとして、日常から準備すべき事項の確実な実践を図るための仕組みも確立しており、これらの実践は、この仕組みの下で励行されている<br>・また、紛争への備えについての責任体制も明確にされており、関係者は自己の責務を十分に承知している<br>・専門家を含む紛争時の対応体制も確立している<br>・情報セキュリティがかかわる紛争への備えについての検討のレベルはクラスA<br>・情報セキュリティがかかわる紛争への備えについての見直し状況はクラスA<br>・この紛争への備えやその実践状況についての文書化のレベルはクラスA |
| レベル4 | 情報セキュリティがかかわる紛争発生に備えての諸活動が円滑に行われるための組織面での環境整備が進められていて、これらは概ね有効に機能している。万一、紛争になっても、ほぼ十分な対応はできると見られるが、環境の整備や実行面で、まだ改善の余地も残る。<br>・発生が予想される紛争の、概ね、すべてが洗いだされ、それぞれの紛争のシナリオも組織的に検討されているが、検討にきめの細かさが欠けるところがある<br>・完全ではないが、想定される紛争のシナリオごとに対応手順が示されている<br>・検討された対応手順に対応して、必要な証跡の確保等の日常から準備すべき事項が洗い出され、業務運用やシステムの運用への展開が図られているが、一部に徹底さを欠くところがある<br>・裁判上の証拠として用いられることが想定される記録確保は、法的効力を持てるような方法で取得、管理されるようになっている<br>・業務現場やシステムの運用現場において、紛争への備えとして、日常から準備すべき事項の確実な実践を図るための仕組みも作られており、これらの実践は、この仕組みの下で励行されているが、仕組みや実践の管理には改善の余地がある<br>・また、紛争への備えについての責任体制も明確にされており、関係者は自己の責務を、概ね、十分に承知している<br>・専門家を含む紛争時の対応体制も確立している<br>・情報セキュリティがかかわる紛争への備えについての検討のレベルはクラスA<br>・情報セキュリティがかかわる紛争への備えについての見直し状況はクラスB以上<br>・この紛争への備えやその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | 情報セキュリティがかかわる紛争発生に備えての基本の形はできており、最小限なレベルでは機能していると考えられるが、改善する余地は多い。<br>・発生が予想される紛争のうち、典型的なものについては、大まかではあるが紛争のシナリオとポイントが組織的に検討されている<br>・これらの紛争については、必要な証跡の確保等の日常から準備すべき事項が検討され、業務運用やシステムの運用への展開が図られているが、徹底したものではない<br>・裁判上の証拠として用いられることが想定される記録確保は、法的効力を持てるような方法で取得、管理されるようになっている<br>・業務現場やシステムの運用現場において、紛争への備えとして、大まかではあるが、日常から準備すべき事項の確実な実践を図るための仕組みも作られており、これらの実践は、この仕組みの下で励行されることになっているが、徹底したものではない |

| | |
|---|---|
| | ・情報セキュリティがかかわる紛争への備えについての検討のレベルはクラスB以上<br>・情報セキュリティがかかわる紛争への備えについての見直し状況はクラスB以上<br>・この紛争への備えやその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | 情報セキュリティがかかわる紛争発生に備えは、担当者レベルの努力である部分的な取り組みは見られるが、組織的・体系的なものにはなってなく、十分とは言えない。<br>・担当者レベルでは、情報セキュリティがらみの紛争への備えについての意識はあり、必要な証跡の確保等の日常から準備すべき事項の検討は行われているが、部分的なものに止まっている<br>・裁判上の証拠として用いられることが想定される記録確保は、部分的に行われている<br>・情報セキュリティがかかわる紛争への備えについての検討のレベルはクラスC以上<br>・この紛争への備えやその実践状況についての文書化のレベルはクラスC以上 |
| レベル1 | 紛争への備えについての組織的な取り組みは、ないに等しい<br>・レベル2の達成要件も満たしていない |

# 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. システムの処置の正確性の確保

| 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムの処理の正確性を確保するための完成度の高い組織的な仕組みが確立しており、すべてのシステム開発に厳格に適用されている。<br>･精緻に出来た開発プロセスが確立しており、業務仕様の定義からシステムの検収に至るまでのプロジェクトの各フェーズで、システムの処理の正確性確保についてのチェックポイントや、チェックのポイントも確立している<br>･システムの処理の正確性の確保についての、利用者サイドの者も含む責任体制も確立しており、この体制は完全に機能している<br>･業務単位あるいは業務群ごとに、その処理の正確性についての保証要件（注1）が詳細に明示されている<br>･システムの処理の正確性を確保するための仕組みについての検討のレベルはクラスA<br>･システムの処理の正確性を確保するための仕組みについての見直し状況はクラスA<br>･システムの処理の正確性を確保するための仕組みについての文書化のレベルはクラスA |
| レベル4 | システムの処理の正確性を確保するための組織的な仕組みが確立しているが、まだ改善の余地も残っている。また、すべてのシステム開発への厳格な適用も図られているが、一部に徹底に欠けるところも見られる。<br>･精緻に出来た開発プロセスが確立しており、業務仕様の定義からシステムの検収に至るまでのプロジェクトの各フェーズで、システムの処理の正確性確保についてのチェックポイントや、チェックのポイントも、相当にきめ細かく示されているが、まだ改善の余地がある<br>･システムの処理の正確性の確保についての、利用者サイドの者も含む責任体制は明示されている<br>･業務単位あるいは業務群ごとに、その処理の正確性についての保証要件は、大まかではあるが示されている<br>･システムの処理の正確性を確保するための仕組みについての検討のレベルはクラスB以上<br>･システムの処理の正確性を確保するための仕組みについての見直し状況はクラスB以上<br>･システムの処理の正確性を確保するための仕組みについての文書化のレベルはクラスB以上 |
| レベル3 | 準拠すべき開発プロセスの中で、システムの処理の正確性の確保のためのポイントは示されているが、大まかなレベルに止まり、システムの処理の正確性を確保するための組織的な仕組みにまでは至っていない。ただし、開発したシステムのテストや研修については行うべきことや手順等が示され、開発過程でのシステムの処理に正確性の作りこみについての組織的な取組みは評価できる。<br>･システムの処理の正確性の確保についての、利用者サイドの責任はあまり問われていない<br>･業務単位あるいは業務群ごとに、その処理の正確性についての保証要件の提示は行われていなく、個別の開発プロジェクトに任されている<br>･大まかではあるが、開発プロセスが確立しており、業務仕様の定義からシステムの検収に至るまでのプロジェクトの各フェーズで、システムの処理の正確性確保についてのチェックポイントや、チェックのポイントも示されているが、十分の域には達してはいない<br>･システムの処理の正確性を確保するための仕組みについての検討のレベルはクラスB以上<br>･システムの処理の正確性を確保するための仕組みについての見直し状況はクラスB以上<br>･システムの処理の正確性を確保するための仕組みについての文書化のレベルはクラスB以上 |
| レベル2 | 担当者間には、習慣的に形成されたシステムの処理の正確性を確保するための手順が存在し、それぞれのシステムの開発においては、この習慣的な仕組みに沿って、正確性の確保が図られている。組織的な仕組みとしては評価できないが、システムの開発におけるシステムの処理の正確性の確保のた |

| | |
|---|---|
| | めの取組みは、不十分ながらも存在して、ある程度機能している。<br>・習慣的に形成された標準的な開発プロセスが存在し、業務仕様の定義からシステムの検収に至るまでのプロジェクトの各フェーズで、担当者は、システムの処理の正確性確保についてのチェックの方法やチェックのポイントを、概ね、承知している<br>・システムの処理の正確性を確保するための仕組みについての検討のレベルはクラスＣ以上<br>・システムの処理の正確性を確保するための仕組みについての見直し状況はクラスＣ以上<br>・システムの処理の正確性を確保するための仕組みについての文書化のレベルはクラスＣ以上 |
| レベル1 | システムの処理の正確性を確保するための組織的な仕組みは存在しない。すべては開発プロジェクトのスキルに依存している。<br>・レベル２の達成条件も満たせない |

(注1) システムの処理の正確性についての保証要件として指定すべき事項
・正確性についての要求のレベル（問題が生じた場合の影響のレベルと、正確性についての信頼度）
・業務仕様の正確性についてのチェックのレベル
・システムの処理についてテストのレベル（確認のレベル）
－単体テスト他のプログラムの開発過程における各ステップでのテストおよびテスト結果の確認のレベル
－システムの総合テストにおけるテストのレベルおよびテスト結果の確認のレベル
－業務サイドでの検収テストにおけるテストのレベルおよびテスト結果の確認のレベル

## Ta1.2 業務仕様の定義の正確性の確保

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 業務仕様の定義の正確性を確保するための完成度の高い組織的な仕組みが確立しており、すべての業務仕様の定義は、この仕組み沿って検討、検証されており、不備が入り込むことは、まず考えられない。<br>・精緻にできた定義プロセスが確立しており、検討段階や仕様のレビューでの、正確性についてのチェックポイントや、チェックのポイントも確立している<br>・この仕組みに沿って業務仕様の定義の正確性のチェックは徹底して行われている<br>・利用者サイドだけでなく、システム担当者も含む責任体制も確立しており、十分に機能している<br>・業務仕様の定義の正確性を確保のための仕組みについての検討のレベルはクラスＡ<br>・業務仕様の定義の正確性を確保するための仕組みについての見直し状況はクラスＡ<br>・定義した業務仕様に対する見直しの実施状況はクラスＡ<br>・業務仕様の定義の正確性を確保するための仕組みや、各開発プロジェクトにおける業務仕様の定義における正確性の追求についての文書化のレベルはクラスＡ |
| レベル4 | 業務仕様の定義の正確性を確保するためのよく検討された組織的な仕組みも作られてはいるが、まだ、改善の余地がある。また、業務仕様の開発段階へのこの仕組みの厳格な適用も図られているが、一部に徹底さを欠くところも見らる。業務仕様の定義に、不備が入り込む余地が、僅かではあるが残っている。<br>・定義プロセスが確立しており、検討段階や仕様のレビューでの、正確性についてのチェックポイントや、チェックのポイントも相当にきめ細かく示されているが、まだ改善の余地もある<br>・この仕組みに沿って業務仕様の定義の正確性のチェックは厳格に行われることになっているが、一部に徹底さに欠けるところが見られる<br>・利用者サイドだけでなく、システム担当者も含む責任体制も確立しており、概ね、十分に機能している<br>・業務仕様の定義の正確性を確保のための仕組みについての検討のレベルはクラスＢ以上<br>・業務仕様の定義の正確性を確保するための仕組みについての見直し状況はクラスＢ以上<br>・定義した業務仕様に対する見直しの実施状況はクラスＢ以上<br>・業務仕様の定義の正確性を確保するための仕組みや、各開発プロジェクトにおける業務仕様の定義における正確性の追求についての文書化のレベルはクラスＢ以上 |
| レベル3 | 大まかではあるが、業務仕様の定義を正確なものにするための組織的な仕組みが示されており、業務仕様はこの仕組みに沿ってチェックされてはいるが、徹底したものではない。業務仕様の定義に、不備が入り込む余地が残っている。 |

| | |
|---|---|
| | 対象業務ごとに、業務仕様の定義における正確性の確保についての責任の所在と関与すべきものは示されている<br>・業務仕様の定義における組織的なレビューの手順や、大まかではあるがチェックポイントが示されている<br>・業務仕様の定義におけるその正確性についてのレビューも行われているが、レビューの対象範囲もレビューの密度も徹底したものではない<br>・利用者サイドだけでなく、システム担当者も含む責任体制も示されており、概ね、機能している<br>・業務仕様の定義の正確性を確保のための仕組みについての検討のレベルはクラスB以上<br>・業務仕様の定義の正確性を確保するための仕組みについての見直し状況はクラスB以上<br>・定義した業務仕様に対する見直しの実施状況はクラスB以上<br>・業務仕様の定義の正確性を確保するための仕組みや、各開発プロジェクトにおける業務仕様の定義における正確性の追求についての文書化のレベルはクラスB以上 |
| レベル2 | 担当者間には、習慣的に形成された業務仕様の定義の正確性を確保するための手順が存在し、それぞれのシステムの開発においては、この習慣的な仕組みに沿って、利用部門にこれまで蓄積されてきたノウハウにもとづいて、その正確性の確保を図っている。組織的な仕組みとしては評価できないが、システムの開発における業務仕様の正確性の確保のための取組みは、不十分ながらも存在して、ある程度機能している。<br>・習慣的に形成された標準的な業務仕様の定義プロセスが存在し、担当者は、業務仕様の定義の手順やチェックのポイントを、概ね、承知している<br>・これらのノウハウはある程度整理され、継承されている<br>・業務仕様の定義においては、これらの手順に沿って、担当者レベルでのチェックは行われている<br>・業務仕様の定義の正確性を確保のための仕組みについての検討のレベルはクラスC以上<br>・定義した業務仕様に対する見直しの実施状況はクラスC以上<br>・業務仕様の定義の正確性を確保するための仕組みや、各開発プロジェクトにおける業務仕様の定義における正確性の追求についての文書化のレベルはクラスC以上 |
| レベル1 | 業務仕様の定義は、すべて担当者に任されており、その正確性の確保についての組織的な取り組みはないに等しい。<br>・レベル2の達成条件も満たせない |

## 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）

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | アプリケーションソフトの品質確保のための完成度の高い組織的な仕組みが確立しており、すべてのアプリケーションソフトの開発は、この仕組み沿って設計、製造、テストされており、完成したソフトに不良が残されることは、まず考えられない。<br>・アプリケーションソフトの開発における正確性を確保するための管理面での仕組みが確立している<br>・開発するシステムの特性ごとに良く検討された品質確保基準が示されている<br>・開発するシステムの特性ごとに、良く検討された設計レビューの体制、手順、レビューポイント等が明示されている<br>・開発するシステムの特性ごとに、完成度の高いテスト基準が整備されている<br>・レビューやテストの評価、および品質の評価は、開発チームとは別の体制で、厳格な管理の下で徹底して行われている<br>・最終的な検収テストは、利用者サイドが中心となって行われている<br>・アプリケーションソフトの品質確保のための仕組みについての検討のレベルはクラスA<br>・この仕組みについての見直し状況はクラスA<br>・この仕組みや、開発プロジェクトのおける品質の追求状況についての文書化のレベルはクラスA |
| レベル4 | アプリケーションソフトの品質確保のためのよく検討された組織的な仕組みも確立しているが、まだ、改善の余地がある。アプリケーションソフトの開発は、この仕組み沿って設計、製造、テストされてはいるが、一部に厳格さ欠けるところも見られる。完成したソフトの不良が残す余地が、僅かではあるが残され |

| | |
|---|---|
| | ている。<br>・アプリケーションソフトの開発における正確性を確保するための管理面での仕組みが確立しているが、まだ、改善の余地もある<br>・開発するシステムの特性ごとに品質確保基準が示されている<br>・開発するシステムの特性ごとに、設計レビューの体制、手順、レビューポイント等は、示されている<br>・開発するシステムの特性ごとに、テスト基準は示されている<br>・レビューやテストの評価、および品質の評価は、開発チームとは別の体制で、厳格な管理の下で行われているが、一部に徹底さを欠くところも見られる<br>・最終的な検収テストは、利用者サイドが中心となって行われているが、利用者サイドの意識に十分でないところも見られる<br>・アプリケーションソフトの品質確保のための仕組みについての検討のレベルはクラスＢ以上<br>・この仕組みについての見直し状況はクラスＢ以上<br>・この仕組みや、開発プロジェクトのおける品質の追求状況についての文書化のレベルはクラスＢ以上 |
| レベル3 | 大まかではあるが、アプリケーションソフトの品質確保のための組織的な仕組みも形作られているが、まだ、十分なものとは言い難い。アプリケーションソフトの開発は、この仕組み沿って設計、製造、テストされてはいるが、設計のレビューやテストは、担当チーム中心で、組織的に徹底したものとは言い難く、完成したソフトに不良が残さる可能性も残されている。<br>・大まかではあるが、アプリケーションソフトの開発における正確性を確保するための管理面での仕組みが作られている<br>・開発するシステムの特性ごとに、設計レビューの体制、手順、レビューポイント等は、示されている<br>・開発するシステムの特性ごとに、テスト基準は示されている<br>・レビューやテストの評価、および品質の評価は、開発チームでこれらの仕組みに沿って行われているが、厳格な管理は行われていないため、徹底したものではない<br>・開発チームの品質確保に向けた意識は高く、プロジェクトごとの工夫も行われているが、組織的なチェックは行われていないため、その信頼性は不明<br>・アプリケーションソフトの品質確保のための仕組みについての検討のレベルはクラスＢ以上<br>・この仕組みについての見直し状況はクラスＢ以上<br>・この仕組みや、開発プロジェクトのおける品質の追求状況についての文書化のレベルはクラスＢ以上 |
| レベル2 | アプリケーションソフトの開発担当者間には、アプリケーションソフトから不良を排除することについて、習慣的に形成された方法が存在し、それぞれのアプリケーションソフトの開発においては、この習慣的な仕組みに沿って、これまで蓄積されてきたノウハウにもとづいて、不良の排除に努めている。組織的な仕組みとしては評価できないが、開発するアプリケーションソフトから不良を排除するための取組みは、不十分ながらも存在して、ある程度機能している。<br>・担当者間には、習慣的に形成されたアプリケーションソフトから不良を排除する方法が存在し、アプリケーションソフトから不良を排除するための開発上の手順やチェックのポイントを、概ね、承知している<br>・これらのノウハウはある程度整理され、継承されている<br>・アプリケーションソフトの開発においては、これらの手順に沿って、担当者レベルでの不良の排除について努力は行われている<br>・アプリケーションソフトの品質確保のための仕組みについての検討のレベルはクラスＣ以上<br>・この仕組みについての見直し状況はクラスＣ以上<br>・この仕組みや、開発プロジェクトのおける品質の追求状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | アプリケーションソフトの品質確保は、すべて、開発プロジェクトまたは開発担当者に任されており、組織的な検証は行われていない<br>・レベル2の達成条件も満たせない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 重要な点については、ダブルチェックの実行等が業務の流れの中に組み込まれており、業務の現場において、日々の業務処理においてシステムや業務処理の正確性についてのチェックが行き届いており、おいてシステムや業務処理に、万一、齟齬があっても、これが見逃されることは、考えられない。<br>・職場ごとに業務やシステムの処理についてのチェックポイントが、マニュアル化されている<br>・重要なところについては、ダブルチェックの仕組みが導入されている<br>・現場の職員における、この点についての意識は高く、その実践は十分<br>・業務現場への本要求の実践と管理の徹底状況はクラスA<br>・本要求の実践を管理するための仕組みについての見直し状況はクラスA<br>・本要求の実践を管理するための仕組についての文書化のレベルはクラスA |
| レベル4 | 業務の現場において、日々の業務処理においてシステムや業務処理の正確性についてのチェックは十分に指導され行われてはいるが、ほとんどが一人一人の注意に依存しているため、問題を見逃す余地が、僅かではありが残っている。<br>・職場ごとに業務やシステムの処理についてのチェックポイントが、業務マニュアル化されているが、まだ、改善の余地がる<br>・現場の職員に対する、日常の業務におけるこれらについての注意は常に喚起されているが、一部に徹底さを欠くところも見られる<br>・業務現場への本要求の実践と管理の徹底状況はクラスB以上<br>・本要求の実践を管理するための仕組みについての見直し状況はクラスB以上<br>・本要求の実践を管理するための仕組みについての文書化のレベルはクラスB以上 |
| レベル3 | 業務の現場において、日々の業務処理においてシステムや業務処理の正確性についてのチェックポイントや、求められているチェックの励行は指導されているが、その徹底は十分ではなく、問題が見逃される可能性は、低いとは言えない。<br>・職場ごとに業務やシステムの処理についてのチェックポイントが、大まかではあるがマニュアル化されている<br>・日々の業務処理においてシステムや業務処理の正確性についてのチェックの実践についての業務現場への指導も行われているが、必ずしも徹底はしていない<br>・本要求についてのっ組織的な仕組みの検討のレベルはクラスB以上<br>・業務現場への本要求の実践と管理の徹底状況はクラスB以上<br>・本要求の実践を管理するための仕組みについての見直し状況はクラスB以上<br>・本要求の実践を管理するための仕組みについての文書化のレベルはクラスB以上 |
| レベル2 | 業務の現場において、日々の業務処理においてシステムや業務処理の正確性についてのチェックは、一人一人の注意に任されており、組織的な取組みにはなっていない。ただし、処理の正確性についての、常に、注意すべきことは指導されている。<br>・職場ごとに、大まかではあるが業務やシステムの処理についてのチェックポイントは示されているが、すべてにマニュアル化されているわけではない<br>・日々の業務処理においてシステムや業務処理の正確性についてのチェックの実践は、業務現場の各人の注意に任されている<br>・本要求の実践を管理するための仕組みについての見直し状況はクラスB以上<br>・本要求の実践を管理するための仕組みについての文書化のレベルはクラスB以上 |
| レベル1 | 日々の業務処理においてシステムや業務処理の正確性についてのチェックについての、組織的な取組みは見えない。<br>・レベル2の達成条件も満たせない |

## Ta1.5 業務現場における問題発生時の対応能力の確保

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 業務やシステムの処理に問題が生じた場合に必要な措置が確立して、その業務現場への周知も十分で、業務現場はこのような場面に対する対応能力を十分に有していることが確認されている。万一、業務面で問題が発生しても、十分な対応ができる。<br>・問題のタイプごとに必要な措置が確立している<br>・これらは業務マニュアル等で業務現場に示されている<br>・業務現場に対するこの点についての教育や訓練も行き届いている<br>・業務やシステムの処理に問題が発生した場合への備えについての検討のレベルはクラスA<br>・業務やシステムの処理に問題が発生した場合への備えについての見直し状況はクラスA<br>・業務やシステムの処理に問題が発生した場合への備えについての文書化のレベルはクラスA |
| レベル4 | 業務やシステムの処理に問題が生じた場合に必要な措置が確立して、その業務現場への周知も行われているが、十分とは言い切れないところが残る。万一、業務面で問題が発生しても、その対応に不安なほとんどない。<br>・問題のタイプごとに必要な措置が示されて入るが、十分とは言えないところも残っている<br>・これらは業務マニュアル等で業務現場に示されている<br>・業務現場に対するこの点についての教育は行われている<br>・業務やシステムの処理に問題が発生した場合への備えについての検討のレベルはクラスB以上<br>・業務やシステムの処理に問題が発生した場合への備えについての見直し状況はクラスB以上<br>・業務やシステムの処理に問題が発生した場合への備えについての文書化のレベルはクラスB以上 |
| レベル3 | 業務やシステムの処理に問題が生じた場合に必要な措置は、大まかではあるが示されており、業務現場は、このような場面に対しある程度の対応はできると見ることができる。ただし、その内容や業務現場への展開も十分とは言えず、改善の余地は多い。<br>・問題が発生したときに必要な措置が示されて入るが、問題のタイプごとへの展開は不十分<br>・また、示されているその内容も、組織的な対応のレベルにまでは至っていない<br>・これらは、何らかの形で業務現場に示されている<br>・業務やシステムの処理に問題が発生した場合への備えについての検討のレベルはクラスB以上<br>・業務やシステムの処理に問題が発生した場合への備えについての見直し状況はクラスB以上<br>・業務やシステムの処理に問題が発生した場合への備えについての文書化のレベルはクラスB以上 |
| レベル2 | 業務やシステムの処理に問題が生じた場合に必要な措置の原則は示されているが、具体的な対応については示されていない。問題生じたときの処置は、当事者の判断によっており、組織的な取組みにはなっていない。<br>・大まかではあるが、業務やシステムの処理に問題が生じた場合に必要な措置の原則は示されている<br>・各業務現場では、想定される大きな問題についての対処については、ある程度の考え方があり、担当者間で共有されているが、具体的な準備にまでは至っていない<br>・業務やシステムの処理に問題が発生した場合への備えについての検討のレベルはクラスC以上<br>・業務やシステムの処理に問題が発生した場合への備えについての文書化のレベルはクラスC以上 |
| レベル1 | 業務処理上で問題が生じた時の備えはないに等しい。<br>・レベル2の達成条件も満たせない |

### 3.1.2. **障害に対する堅牢性の確保**

| 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 |
|---|---|

| 強度<br>レベル | 当該レベル達成要件 |
|---|---|
| レベル<br>5 | システム構成機器の障害対策が、可用性についての高い要求に対応できるよう、非常にきめ細かく、かつ、全体としてバランスの取れた形で設計されている。周辺機器の障害がシステ、万一、システムダウンが生じても、短時間での回復かできるようになっている。<br>・予備機への自動切換え機能や縮退機能等がきめ細かく設計されており、各機器の障害はシステム停止につながらないようになっている<br>・万一、システム停止になっても、非常な短時間で復旧ができるように設計されている<br>・システムは、障害発生時点に戻ることができるように設計されており、入力情報が失われ再入力が必要となるものは、ほとんどない<br>・予備機の配置他の機器の構成や、これらの障害対策機能の実装方式も的確でまったく無駄がない<br>・これらについての設計レビューも組織的な体制の下で、専門家も参加し、徹底して行われており、この点についての検討のレベルはクラス A<br>・障害対策機能やその方式設計についてについての見直し状況はクラス A<br>・障害対策機能やその方式設計についてについての文書化のレベルはクラス A |
| レベル<br>4 | レベル 5 が対応できるような可用性は達成できるものではないが、システム構成機器の障害対策が、かなりきめ細かく設計されており、システム停止、システム停止発生時における停止時間の長時間化の可能性は、低くなるようになっている。<br>・簡単にシステム停止に陥らないよう、予備機への自動切換え機能や縮退機能等も組み込まれているが、そのきめ細かさは、レベル 5 ほどではなく、システム停止としている場合は少なくない<br>・万一、システム停止になっても、比較的短時間で復旧ができるように設計されている<br>・システムは、障害発生時点に戻ることができるように設計されており、入力情報が失われ再入力が必要となるものは、相当に絞り込まれている<br>・予備機の配置他の機器の構成や、これらの障害対策機能の実装方式も妥当<br>・これらについての設計レビューも組織的な体制の下で、相当に綿密な検討が行われており、この点についての検討のレベルはクラス B 以上<br>・障害対策機能やその方式設計についてについての見直し状況はクラス B 以上<br>・障害対策機能やその方式設計についてについての文書化のレベルはクラス B 以上 |
| レベル<br>3 | システム構成機器の障害対策の設計は、そうきめの細かいものでなく、システム停止の防止よりは、システムの暴走の阻止と、短時間のシステムの復旧に焦点が当てられており、可用性について要求がそれほど厳しくないシステムには、ほぼ、十分な設計になっている。<br>・比較的発生頻度の高い障害に対しては、ある程度の代替措置が組み込まれ、簡単にシステム停止に陥らないようにする設計となっている<br>・システム停止時の情報の回復やシステムの再開始の方式は十分に検討されており、万一、システム停止になっても、ある程度の時間でシステムの復旧ができるようになっている<br>・予備機の配置他の機器の構成や、これらの障害対策機能の実装方式も、概ね、妥当<br>・復旧にあたっての、すでに受け付けた当日の入力の処理の再現の必要性は、相当に絞り込まれており、これらの処理の再現の道は確保されている<br>・これらについての設計レビューも組織的な体制の下で検討が行われており、この点についての検討のレベルはクラス B 以上<br>・障害対策機能やその方式設計についてについての見直し状況はクラス B 以上<br>・障害対策機能やその方式設計についてについての文書化のレベルはクラス B 以上 |
| レベル<br>2 | システム構成機器の障害対策の設計は、異常状態のままでのシステムの暴走の阻止と、当日の開始時点に戻った、復旧に絞っており、システム停止時間の長期化の防止ができるになっている。<br>・システムに自動的な回復やプラットフォームがサポートしている代替措置が機能しない場合は、すぐに停止すことを基本方針としている<br>・システムが停止時しても、当日の開始時点へ戻った復旧はすぐにできるようになっている<br>・重要な処理については、入力が再現できない処理済の入力の措置についての検討も行われており、必要な対応が何らかの形で行われるようになっている |

| | |
|---|---|
| | ・これらについての設計レビューは担当チームに任されているが、担当チームレベルでの検討は行われている。この点についての検討のレベルはクラスＣ以上<br>・障害対策機能やその方式設計についてについての見直し状況はクラスＣ以上<br>・障害対策機能やその方式設計についてについての文書化のレベルはクラスＣ以上 |
| レベル1 | システム構成機器の障害対策への対応は、ほとんど検討されていない。また、現状で十分かどうかのチェックもあまり行われていない。<br>・レベル２の達成条件も満たせない。 |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 設計した障害対策機能のシステムの組込みは、完全にテストされており、期待通り機能することが確認されている。また、障害対策機能の動作に影響が生じるようなシステムの変更が行われた場合は、必要な動作確認と必要な手直しが確実に行われており、これらの実効性の維持も完全に行われている。また、必要なツールやリソースの準備も常に確認されている。<br>・障害対策機能のシステムへの的確な組込みならびにその有効性の維持を確実にするための管理面での仕組みも確立しており、以下の活動はすべて、この仕組に沿って厳格な管理の下で行われている<br>・障害対策機能の個々に対する完全なテスト仕様が作られており、このテスト仕様にもとづくテストが厳格に行われている。<br>・テストは、擬似障害の発生も含み、一部を除き実機テストとして行われている<br>・システム環境の変化に伴う組み込んだ障害対策の有効性の確認や、必要な手直しについては徹底して行われている<br>・必要なツールやリソースの準備についての確認も、頻繁に行われている<br>・テスト仕様のレビューやテストの評価は、開発チームとは別の体制で、厳格に行われている<br>・障害対策機能のテスト仕様やテスト方法についての検討のレベルはクラスＡ<br>・障害対策機能のテストや、システムの変更にともなう再テストの状況についての文書化のレベルはクラスＡ |
| レベル4 | 設計した障害対策機能のシステムの組込みは概ねテストされ、期待通り機能することが確認されているが、テストが難しいところについては、設計チェックに止まっているところが残されている。また、障害対策機能の動作に影響が生じるようなシステムの変更に対する、動作の再確認や必要な手直しに、一部徹底さを欠くところも見られ、これらの実効性の維持は完全と言えないところがある。また、必要なツールやリソースの準備の確認も概ね適切に行われている。<br>・障害対策機能のシステムへの的確な組込みならびにその有効性の維持を確実にするための管理面での仕組みも確立しているがおり、以下の活動はすべて、この仕組みに沿って厳格な管理の下で行われていることになっているが、一部に徹底さを欠くところも見られる<br>・障害対策機能の個々に対する完全なテスト仕様が作られており、このテスト仕様にもとづくテストが厳格に行われている。<br>・テストは、擬似障害の発生も含み、一部を除き実機テストとして行われている<br>・テスト仕様のレビューやテストの評価は、開発チームとは別の体制で、厳格に行われている<br>・必要なツールやリソースの準備についての確認も、頻繁に行われている<br>・システム環境の変化に伴う組み込んだ障害対策の有効性の確認や、必要な手直しについての検討も組織的に行われているが、一部に徹底さに欠けるところも見られる<br>・障害対策機能のテスト仕様やテスト方法についての検討のレベルはクラスＢ以上<br>・障害対策機能のテストや、システムの変更にともなう再テストの状況についての文書化のレベルはクラスＢ以上 |
| レベル | 設計した障害対策機能のシステムの組込みは、設計チェックに止まっているところが多く、実機テストでの確認のレベルは高くない。また、障害対策機能の動作に影響が生じるようなシステムの変更に対す |

| | |
|---|---|
| 3 | る、動作の再確認や必要な手直しは、十分とは言えない。また、必要なリソースの確保についての確認も十分とは言えない<br>・大まかではあるが、障害対策機能のシステムへの的確な組込みならびにその有効性の維持を確実にするための管理面での仕組みも示されている。また、以下の活動はこの仕組みに沿って組織的な管理の下で行われていることになっているが、徹底したものではない。<br>・障害対策機能のについてのテストは開発チーム内では十分に行ったことになっているが、実機テストに十分とは言えないところもある<br>・また、組織的なテスト仕様の作成やそのレビューも行われているが、徹底したものではない<br>・必要なツールやリソースの準備についての確認も、ある程度行われている<br>・システム環境の変化に伴う組み込んだ障害対策の有効性の確認や、必要な手直しについての検討も組織的に行われることになっているが、徹底はしていない<br>・障害対策機能のテスト仕様やテスト方法についての検討のレベルはクラスＣ以上<br>・障害対策機能のテストや、システムの変更にともなう再テストの状況についての文書化のレベルはクラスＣ以上 |
| レベル2 | 設計した障害対策機能のシステムの組込みは、開発担当ベースに任されており、組織的なチェックはほとんど行われていないが、担当ベースでは、一通りのテストは行われている。<br>・障害対策機能についての詳細仕様の作成やそのレビュー、およびそのテストは開発チームに任されており、組織的なチェックに至っていない<br>・実機テストは、代表的なものに止まっている<br>・システム環境の変化に伴う組み込んだ障害対策の有効性の確認は、担当者に任されているが、担当者間には、これらを適切に行うための習慣的に形成された手順があり、概ね、この手順に沿って必要な作業が行われているが、組織的に管理された作業にはなっていない<br>・障害対策機能の動作に影響が生じるようなシステムの変更に対する実装確認の見直しや、必要なリソースの準備状況の確認等は、時々、行われている<br>・障害対策機能のテスト仕様やテスト方法についての検討のレベルはクラスＣ以上<br>・障害対策機能のテストや、システムの変更にともなう再テストの状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | 設計した障害対策機能のシステムの組込みはについての確認や、その有効性の維持についての組織的な取り組みは、ほとんど行われていない。<br>・レベル２の達成条件も満たせない |

## Ta2.3 システム障害の発生時の対応能力の確保

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムに障害が発生した時に必要な措置が確立しており、そのシステム運用現場への周知も十分で、システム運用現場はこのような場面に対する対応能力を十分に有していることが確認されている。障害が発生しても必要な対応に齟齬がでることは考えにくい。<br>・発生障害の状況ごとに必要な措置が確立してマニュアル化されている<br>・これらの障害時の対応に関係する者への周知は徹底している<br>・関係者に対する障害時の対応についての教育や訓練も行き届いており、必要な対応が何時でも迅速に取れる<br>・システム運用サイドでのシステム障害発生時の備えについての検討のレベルはクラスＡ<br>・システム運用サイドでのシステム障害発生時の備えについての見直し状況はクラスＡ<br>・システム運用サイドでのシステム障害発生時の備えについての文書化のレベルはクラスＡ |
| レベル4 | システムに障害が発生した時に必要な措置が確立しており、そのシステム運用現場への周知も行われているが、十分とは言い切れないところが残る。障害が発生したとき、必要な対応に齟齬がでる余地が、僅かではあるが残されている。<br>・発生障害の状況ごとに必要な措置が示されてマニュアル化されているが、まだ改善の余地がある<br>・これらの障害時の対応に関係する者への周知も徹底が図られているが、一部に徹底さを欠くところも |

| | |
|---|---|
| | 見られる<br>・関係者に対する障害時の対応についての教育や訓練も行われており、必要な対応が何時でも、概ね、迅速に取れると見てよい<br>・システム運用サイドでのシステム障害発生時の備えについての検討のレベルはＢ以上<br>・システム運用サイドでのシステム障害発生時の備えについての見直し状況はＢ以上<br>・システム運用サイドでのシステム障害発生時の備えについての文書化のレベルはクラスＢ以上 |
| レベル3 | システムに障害が発生した時に必要な措置は、大まかではあるが示されており、システム運用の現場は、このような場面に対しある程度の対応はできると見ることができる。ただし、指定されている措置の内容や、その対策現場への展開もて、徹底したものとは言い難い。障害の発生に対して、必要な対応に円滑さを欠くこともありうる。<br>・大まかではあるが、システム障害発生時に必要な措置が示されて、マニュアル化もされているが、障害の発生状況ごとの細かい展開は十分出ないところもあり、改善すべきところも少なくない<br>・これらは、何らかの形で障害対策にかかわる者に示されているが、訓練は徹底しているとは言えず、必要な対応が何時でも迅速に取れるかどうかは疑わしいところも残っている<br>・システム運用サイドでのシステム障害発生時の備えについての検討のレベルはＢ以上<br>・システム運用サイドでのシステム障害発生時の備えについての見直し状況はＢ以上<br>・システム運用サイドでのシステム障害発生時の備えについての文書化のレベルはクラスＢ以上 |
| レベル2 | 担当者間では、システムに障害が発生した時に必要な措置についての検討は行われ、必要な対応についての担当者での共通認識はできているが、いざに備えた現場レベルでの準備についての、組織的な管理は、ほとんど行われてなく、万一の場合の対応が適切にできるかどうかは怪しい。<br>・システム障害発生時に必要な措置について、担当者間で検討された対応手順が存在し、その内容は担当者間である程度共有されている<br>・システムの管理者はこの問題についての認識はあり、必要な備えについての努力はしている<br>・システム運用サイドでのシステム障害発生時の備えについての文書化のレベルはクラスＣ以上 |
| レベル1 | システムに発生した障害への対応についての組織的な取り組みはないに等しい。<br>レベル２の達成条件も満たせない |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムの性能を確保するための完成度の高い組織的な仕組みが確立しており、この仕組みの沿った性能･容量管理が的確に行われていれば、システムに性能面でのトラブルが発生することは、考えにくい<br>･システムの性能や容量の確保にかかる責任体制が確立しており、すべての関係者は自己の責務を十分に認識している<br>･負荷の実態や今後の負荷の見通しを図るための仕組み（注1）が確立している<br>･システムへの性能／容量対策の実施基準（注2）が確立している<br>･システムへの性能／容量対策の実施要領（注3）が確立している<br>･システムの性能･容量管理を適切に行うための仕組みについての検討のレベルはクラスA<br>･この仕組みについての見直し状況はクラスA<br>･この仕組みについての文書化のレベルはクラスA |
| レベル4 | システムの性能を確保するためのよく検討された組織的な仕組みが作られているが、まだ改善する余地も残されている。この仕組みの沿った性能･容量管理が的確に行われていれば、システムに性能面でのトラブルが発生することは、あまり考えられない<br>･システムの性能や容量の確保にかかる責任体制が確立しており、すべての関係者は自己の責務を、概ね、十分に認識している<br>･負荷の実態や今後の負荷の見通しを図るための仕組み（注1）が確立しているが、まだ改善の余地もある<br>･システムへの性能／容量対策の実施基準（注2）が確立しているが、まだ改善の余地もある<br>･システムへの性能／容量対策の実施要領（注3）が確立しているが、まだ改善の余地もある<br>･システムの性能･容量管理を適切に行うための仕組みについての検討のレベルはクラスB以上<br>･この仕組みについての見直し状況はクラスB以上<br>･この仕組みについての文書化のレベルはクラスB以上 |
| レベル3 | 大まかではあるが、システムの性能を確保するためのよく検討された組織的な仕組みが作られている。この仕組みの沿った性能･容量管理が的確に行われていれば、通常の状態では、概ね、システムに性能面でのトラブルが発生することは、あまり考えられが、環境の変化等への対応は十分とは言い難い。<br>･システムの性能や容量の確保にかかる責任体制が確立しており、すべての関係者は自己の責務を、概ね、十分に認識している<br>･大まかではあるが、負荷の実態や今後の負荷の見通しを図るための仕組み（注1）が示されているが、きめの細かさには欠け、十分とは言い難い<br>･大まかではあるが、システムへの性能／容量対策の実施基準（注2）が示されている<br>･大まかではなるが、システムへの性能／容量対策の実施要領（注3）が示されている<br>･システムの性能･容量管理を適切に行うための仕組みについての検討のレベルはクラスB以上<br>･この仕組みについての見直し状況はクラスB以上<br>･この仕組みについての文書化のレベルはクラスB以上 |
| レベル2 | 担当者間には、習慣的に形成されたシステムの性能／容量管理についての考え方や手順が存在し、担当チームではこの手順に沿って、自主的に性能／容量管理を行っている。組織的な仕組みとしては評価できないが、システムの性能を確保するため取組みは、不十分ながらも存在して、ある程度機能している。<br>･担当者はシステムの性能／容量管理についての自己の責務をある程度認識している<br>･担当者間には、習慣的に形成されたシステムの性能／容量管理についての考え方や手順が存在し、担当者はこの手順を、概ね、承知している<br>･システムの性能･容量管理を適切に行うための仕組みについての検討のレベルはクラスC以上<br>･この仕組みについての文書化のレベルはクラスC以上 |
| レベル1 | システムのシステムの性能／容量管理を適切に行うための組織的な取り組みは、ないに等しい。<br>･レベル2の達成条件も満たせない |

(注1) 負荷の実態や今後の負荷の見通しを図るための仕組みとして指定すべき事項
・負荷の実態把握要領
－把握すべき負荷の実態（測定対象のトランザクションとそれらについての時間変動等の測定値、各システムにおける記憶領域の使用状況他）
－レスポンスタイムの実態（測定場所、測定項目他）
－それぞれの測定についての測定のサイクルやタイミング
－測定方法
－測定結果やその評価と報告の様式や手順
・今後の負荷の見通し方法
－今後の負荷の予測の方式
－見通しについての報告の様式や手順

(注2) システムへの性能／容量対策の実施基準として指定すべき事項
・性能対策を実施しなければならない状況（不可に対するしきい値等で表現）
・実施時期についての考え方

(注3) システムへの性能／容量対策の実施要領として指定すべき事項
・実施計画の作成要領
－実施計画で検討すべき事項（実施の背景と必要性と実施の範囲、実施の具体的な内容、実施時期、設計から事前テスト、終了後の確認に至るまでの実施の全プロセスにかかる実施上の手順、留意事項）
－実施計画書の作成要領（記載すべき事項、様式）
－実施計画の審査要領（審査体制、審査・承認手続き、審査事項とションさのポイント）

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムの構成や処理方式は、性能や容量についての厳しい要求に対応できるよう、非常にきめ細かい工夫のもとで、無駄なく巧妙に設計されている。<br>・必要最小限のリソースで、負荷変動も考慮に入れても、必要な性能を満足でき、かつ、多少の余裕も持っている<br>・万一のオーバーフローに対しても、システム障害にならないような配慮も行き届いている<br>・対象業務の処理方式に照らした性能設計や容量設計の妥当性のレビューも、専門家も参加し組織的に徹底して行われている<br>・性能対策や容量対策についての方式設計についての見直し状況はクラスA<br>・性能対策や容量対策についての方式設計についての文書化のレベルはクラスA |
| レベル4 | レベル5ほど厳しいものではないが、性能や容量についてのかなり高い要求に対応できている。また、その設計には相当の工夫が行われ、コスト的にも無駄は少ない。<br>・負荷変動も考慮に入れても、必要な性能を満足できるようになっているが、これらはリソースに余裕を持たせることで解決しているところも少なくない<br>・万一のオーバーフローに対しても、システム障害にならないような配慮も、ある程度は行われている<br>・対象業務の処理方式に照らした性能設計や容量設計の妥当性のレビューも、専門的なスキルを持つ者も参加し組織的に行われているが、一部に徹底さを欠くところも見られる<br>・性能対策や容量対策についての方式設計についての見直し状況はクラスB以上<br>・性能対策や容量対策についての方式設計についての文書化のレベルはクラスB以上 |
| レベル3 | 性能や容量についての要求は高くはなく、十分なリソースの確保での対応を中心としているが、処理の高速化や必要容量の削減への工夫は行われている。要求を完全に満たすことは確認されている。<br>・負荷変動も考慮に入れても、必要な性能を満足できるようになっているが、ほとんどはリソースに余裕を持たせることで解決している |

| | |
|---|---|
| | ・対象業務の処理方式に照らした性能設計や容量設計についての検討やレビューは、組織的には行われているが、徹底したものではない<br>・性能対策や容量対策についての方式設計についての見直し状況はクラスB以上<br>・性能対策や容量対策についての方式設計についての文書化のレベルはクラスB以上 |
| レベル2 | 性能や容量に対する負荷が低く、性能設計や容量設計は特に必要とされていないが、開発したシステムが、負荷に十分耐えられることについてのチェックは一応行われている。<br>・機器には、性能的におおよそ十分なものを選んでおり、担当チームレベルではあるが、システムは想定される負荷に、十分耐えられることを確認している<br>・性能対策や容量対策の十分性についての文書化のレベルはクラスC以上 |
| レベル1 | システムが必要な性能や容量を有するものにするための組織的な取り組みは、ないに等しい。<br>・レベル2の達成条件も満たせない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 性能設計や容量設計のシステム構成やシステムへの機能の組込みは、完全にテストされており、期待通り機能することが完全に確認されている。また、性能や容量に影響が生じるようなシステムの変更が行われた場合は、性能や容量に影響が出ていないことの確認や、必要な手直しが確実に行われており、これらの実効性の維持も完全に行われている。また、必要なツールやリソースの準備も常に確認されている。<br>・システムの性能の確保に関し、必要なシステムの構成や機能のシステムへの的確な組込みを実現するための仕組みが確立しており、以下の関連作業はこの仕組みに沿って厳格に管理されている<br>・性能設計に対する完全なテスト仕様が作られており、高負荷テストも含め、このテスト仕様にもとづくテストが厳格に行われている<br>・さまざまな動作環境を想定した実装ベースでの容量確認も行われている<br>・テスト仕様のレビューやテストの評価は、開発チームとは別の体制で、厳格に行われている<br>・性能テストのテスト仕様やテスト方法や事前の確認事項についての検討のレベルはクラスA<br>・性能や容量に影響が生じるようなシステムの変更に対するこれらについての実装確認の見直し状況はクラスA<br>・性能や容量についてのテストや、システムの変更にともなうこれらの再確認の状況についての文書化のレベルはクラスA |
| レベル4 | 性能設計や容量設計のシステム構成やシステムへの機能の組込みは、一通りテストされており、期待通り機能することが概ね確認されている。また、性能や容量に影響が生じるようなシステムの変更が行われた場合の性能や容量に影響が出ていないことの確認や、必要な手直しも、概ね適切に行われており、これらの実効性の維持はできていると考えられる。また、必要なツールやリソースの準備も、適宜確認されているが、これらに徹底を欠くところも残されている。<br>・システムの性能の確保に関し、必要なシステムの構成や機能のシステムへの的確な組込みを実現するための仕組みが確立しているが、まだ改善の余地がある。また、以下の関連作業はこの仕組みに沿って厳格に管理されることになっているが、一部に徹底さを欠くところが見られる<br>・性能設計に対する完全なテスト仕様が作られており、このテスト仕様にもとづくテストが厳格に行われているが、高負荷テスト等テストの実施が困難なテストについて、一部に徹底さを欠くところが見られる<br>・さまざまな動作環境を想定した実装ベースでの容量確認も行われているが、一部に徹底さを欠くところが見られる<br>・テスト仕様のレビューやテストの評価は、開発チームとは別の体制で行われている<br>・性能テストのテスト仕様やテスト方法や事前の確認事項についての検討のレベルはクラスB以上<br>・性能や容量に影響が生じるようなシステムの変更に対するこれらについての実装確認の見直し状況はクラスB以上<br>・性能や容量についてのテストや、システムの変更にともなうこれらの再確認の状況についての文書化のレベルはクラスB以上 |

| | |
|---|---|
| レベル3 | 性能設計や容量設計のシステム構成やシステムへの機能の組込みは、テストされているこになっているが、その十分性については組織的な評価はされていない。また、性能や容量に影響が生じるようなシステムの変更が行われた場合における、性能や容量に影響が出ていないことの確認や、必要な手直しも、十分とは言い難い。また、必要なツールやリソースの準備についての確認も十分とはいい難い。<br>・大まかではあるが、システムの性能の確保に関し、必要なシステムの構成や機能のシステムへの的確な組込みを実現するための仕組みも作られている。また、以下の関連作業はこの仕組みに沿って管理されることになっているが、管理は徹底したものではない<br>・性能や容量についてのテストは開発チーム内では十分に行ったことになっているが、実機テストのレベルは十分とは言えないところがある<br>・また、テスト仕様の作成やそのレビューも組織的に行われているが、徹底したものではない<br>・性能テストのテスト仕様やテスト方法や事前の確認事項についての検討のレベルはクラスＣ以上<br>・性能や容量に影響が生じるようなシステムの変更に対するこれらについての実装確認の見直し状況はクラスＣ以上<br>・性能や容量についてのテストや、システムの変更にともなうこれらの再確認の状況についての文書化のレベルはクラスＣ以上 |
| レベル2 | 担当者間には、習慣的に形成されたシステムの性能／容量計画のシステムへの組込みについての手順が存在し、担当チームではこの手順に沿って、これらについてのシステムの組込みを、慎重に行っているいる。組織的な仕組みとしては評価できないが、システムの性能／容量計画のシステムへの組込みについての取組みは、不十分ながらも存在して、ある程度機能している。<br>・担当者間には、習慣的に形成されたシステムの性能／容量計画のシステムへの組込みについての手順が存在している<br>・担当チームは、この手順に従って、システムの性能／容量計画のシステムへの組込みを慎重に行っているが、そのチェックは担当チーム内でしか行われていない<br>・テスト仕様の作成やそのレビュー、事前の確認事項の検討も、ある程度行われているが、十分なものではない<br>・性能テストのテスト仕様やテスト方法についての検討のレベルはクラスＣ以上<br>・性能や容量に影響が生じるようなシステムの変更に対するこれらについての実装確認の見直し状況はクラスＣ以上<br>・性能や容量についてのテストや、システムの変更にともなうこれらの再確認の状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | 設計した障害対策機能のシステムの組込みはについての確認は、行われていない。<br>・レベル2の達成条件も満足できない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 性能･容量トラブルの発生を防止するために、負荷や性能や容量の使用状況についてのきめ細かい監視の仕組みも確立しており、この仕組みに沿った監視も徹底しており、問題は直ちに性能･容量対策に反映しており、システムが突然に性能･容量トラブルに見舞われることはないようになっている。<br>・負荷状況、性能特性、容量の使用状況についてのきめ細かい監視事項が指定されている<br>・高い頻度で必要な監視が行われ評価されまた報告されている<br>・これらの作業のため必要なツールも十分に整備されている<br>・指摘された問題点についての対応も迅速に行われている<br>・これらの一連の作業を的確に行うための管理面での仕組みも確立している<br>・必要な監視とその方式および監視結果の取扱い要領についての検討のレベルはクラスＡ<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスＡ<br>・本対策要求かかる措置についての見直し状況はクラスＡ |

| | |
|---|---|
| | ・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスA |
| レベル4 | 性能・容量トラブルの発生を防止するために、負荷や性能や容量の使用状況についてのきめ細かい監視の仕組みも作られており、この仕組み沿った監視も行われているが、徹底さに欠けるところも見られる。また、指摘された問題に対する性能・容量対策への反映も迅速とは言えないところもある。システムが突然に性能・容量トラブルに見舞われる可能性が、低いが残されている。<br>・負荷状況、性能特性、容量の使用状況についての相当にきめ細かい監視事項が指定されている<br>・相当な頻度で必要な監視が行われ評価されまた報告されている<br>・これらの作業のため必要なツールもある程度整備されている<br>・指摘された問題点についての対応も、概ね、迅速に行われている<br>・これらの一連の作業を的確に行うための管理面での仕組みも確立しているが、まだ改善の余地がある<br>・必要な監視とその方式および監視結果の取扱い要領についての検討のレベルはクラスB以上<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスB以上<br>・本対策要求かかる措置についての見直し状況はクラスB以上<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | 性能・容量トラブルの発生を防止するために、負荷や性能や容量の使用状況の監視は、定期的に行われることになっている。監視のサイクルやチェック事項も大まかで、性能や容量に余裕のあるシステムでは概ね十分ではあるが、性能や容量に余裕のないシステムでは不十分で、システムが突然に性能・容量トラブルに見舞われる可能性が残されている。<br>・大まかではあるが、負荷状況、性能特性、容量の使用状況についての監視事項が指定されている<br>・監視の頻度は年数解程度、また評価はシステム運用部門中心で、組織的に徹底したものではない<br>・指摘された問題点についての対応も、迅速さに欠くところもある<br>・大まかではあるが、これらの一連の作業を的確に行うための管理面での仕組みも示されている<br>・必要な監視とその方式および監視結果の取扱い要領についての検討のレベルはクラスB以上<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスB以上<br>・本対策要求かかる措置についての見直し状況はクラスB以上<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | 年に一度程度は、負荷状況や性能特性や容量の使用状況の点検は行っており、必要な対応は行うことになっている。これらは、すべて担当チーム任されており、組織的な取り組みができているとは言い難い。<br>・担当チームには、負荷の監視等のシステム運用面での性能・容量事故を防止するために必要なことについての認識はあり、担当者はある程度の注意は払っている<br>・年に一度レベルではあるが、担当チームは総合的なチェックを行っている<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスC以上 |
| レベル1 | システムにおける性能や容量トラブルの事前防止のための運用面での配慮についての組織的な取り組みは行われていないに等しい<br>・レベル2の達成条件も満たせない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムに性能や容量に関するﾄﾗﾌﾞﾙが発生した時に必要な措置が確立しており、そのシステム運用現場への周知も十分で、システム運用現場はこのような場面に対する対応能力を十分に有していることが確認されている。障害が発生しても必要な対応に齟齬がでることは考えにくい。<br>･性能や容量に関するﾄﾗﾌﾞﾙの状況ごとに必要な措置が確立してマニュアル化されている<br>･これらの性能や容量に関するﾄﾗﾌﾞﾙ発生時の対応に関係する者への周知は徹底している<br>･関係者に対する性能や容量に関するﾄﾗﾌﾞﾙ発生時の対応についての教育や訓練も行き届いており、必要な対応が何時でも迅速に取れる<br>･システム運用面での性能や容量に関するﾄﾗﾌﾞﾙ発生時の備えについての検討のレベルはクラス A<br>･システム運用サイドでの性能や容量に関するﾄﾗﾌﾞﾙ発生時の備えについての見直し状況はクラス A<br>･この備えについての文書化のレベルはクラス A |
| レベル4 | システムに性能や容量に関するﾄﾗﾌﾞﾙが発生した時に必要な措置が確立しており、そのシステム運用現場への周知も行われているが、十分とは言い切れないところが残る。障害が発生したとき、必要な対応に齟齬がでる余地が、僅かではあるが残されている。<br>･性能や容量に関するﾄﾗﾌﾞﾙ障害の状況ごとに必要な措置が示されてマニュアル化されているが、まだ改善の余地がある<br>･これらの性能や容量に関するﾄﾗﾌﾞﾙ発生時の対応に関係する者への周知も徹底が図られているが、一部に徹底さを欠くところも見られる<br>･関係者に対する性能や容量に関するﾄﾗﾌﾞﾙ発生時の対応についての教育や訓練も行われており、必要な対応が何時でも、概ね、迅速に取れると見てよい<br>･システム運用面での能や容量に関するﾄﾗﾌﾞﾙ発生時の備えについての検討のレベルは B 以上<br>･この備えについての見直し状況は B 以上<br>･この備えについての文書化のレベルはクラス B 以上 |
| レベル3 | システムに性能や容量に関するﾄﾗﾌﾞﾙが発生した時に必要な措置は、大まかではあるが示されており、システム運用の現場は、このような場面に対しある程度の対応はできると見ることができる。ただし、指定されている措置の内容や、その対策現場への展開もて、徹底したものとは言い難い。障害の発生に対して、必要な対応に円滑さを欠くこともありうる。<br>･大まかではああるが、性能や容量に関するﾄﾗﾌﾞﾙ発生時に必要な措置が示されて、マニュアル化もされているが、性能や容量に関するﾄﾗﾌﾞﾙの発生状況ごとの細かい展開は十分でないところもあり、改善すべきところも少なくない<br>･これらは、何らかの形で障害対策にかかわる者に示されているが、訓練は徹底しているとは言えず、必要な対応が何時でも迅速に取れるかどうかは疑わしいところも残っている<br>･システム運用面での能や容量に関するﾄﾗﾌﾞﾙ発生時の備えについての検討のレベルは B 以上<br>･この備えについての見直し状況は B 以上<br>･この備えについての文書化のレベルはクラス B 以上 |
| レベル2 | 担当者間では、システムに障害が発生した時に必要な措置についての検討は行われ、必要な対応についての担当者での共通認識はできているが、いざに備えた現場レベルでの準備についての、組織的な管理は、ほとんど行われてなく、万一の場合の対応が適切にできるかどうかは怪しい。<br>･性能や容量に関するﾄﾗﾌﾞﾙ発生時に必要な措置について、担当者間で検討された対応手順が存在し、その内容は担当者間である程度共有されている<br>･システムの管理者はこの問題についての認識はあり、必要な備えについての努力はしている<br>･システム運用面での性能や容量に関するﾄﾗﾌﾞﾙへの備えについての文書化のレベルはクラス C 以上 |
| レベル1 | システムに性能や容量に関するﾄﾗﾌﾞﾙへの対応についての組織的な取り組みはないに等しい。<br>レベル 2 の達成条件も満たせない |

## 3.2. 攻撃に対する堅牢性の確保

### 3.2.1. 不正アクセス対策

| Tb1.1 | 接続ルールの確立と適切なネットワークの設計 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 組織的によく検討された、端末からの接続要求に対する接続方針が確立しており、ネットワーク構成はこの方針に沿って、現時点ではこれ以上はない堅牢さを持つ構造となっている。また、これらを前提とした端末間やセグメント間の通信に対する接続ルールも、厳格なものになっている。<br>・接続制御の方針（注1）が明示されている<br>・ネットワークの設計上で検討すべき事項のすべて（注2）について、接続制御の方針に沿ったきめの細かい検討とレビューが組織的に行われている<br>・ネットワーク構成は全体として深い多層構造になっており、それぞれの層の境界での接続制御も厳重なものとなっており、接続制御上の部分的な不備が、システムの重要な部位に影響を与えることはありえないような設計になっている。また、冗長化も十分に行われている<br>・接続ルールとネットワーク構成についての見直しのレベルはA<br>・接続ルールとネットワーク構成についての文書化のレベルはA |
| レベル4 | 組織的によく検討された、端末からの接続要求に対する接続方針が確立しており、ネットワーク構成はこの方針に沿って、現時点では平均以上に堅牢とみなされる構造となっている。また、これらを前提とした端末間やセグメント間の通信に対する接続ルールも、平均以上に厳格なものになっている。<br>・接続制御の方針（注1）が明示されている<br>・ネットワークの設計上で検討すべき事項のすべて（注2）について、接続制御の方針に沿ったきめの細かい検討とレビューが組織的に行われている<br>・ネットワーク構成は、重要な部分については多層化されており、それぞれの層の境界での接続制御も厳重なものとなっており、接続制御上の部分的な不備が、システムの重要な部位に影響を与えることはありえないような設計になっている。また、また、冗長化も相当に行われている。<br>・接続ルールとネットワーク構成についての見直しのレベルはB以上<br>・接続ルールとネットワーク構成についての文書化のレベルはB以上 |
| レベル3 | 端末からの接続要求に対する接続方針が大まかではあるが示され、ネットワーク構成はこの方針に沿った概ね堅牢とみなされる構造となっている。また、これらを前提とした端末間やセグメント間の通信に対する接続ルールが示されているが、一般的なもので特に厳格なものではない。<br>・接続方針として示すべきこと（注1）のうち、端末の管理に関することを除いては、大まかではあるが示されている<br>・ネットワークは、DMZ と内部ネットワークを持つ構造となっており、堅牢性については一般的なレベルであるが、DMZ と内部セグメント間の境界での接続制御については、組織的な検討の下、適切な制御が行われるようになっている。冗長化は部分的あるいは行われていないか<br>・接続ルールとネットワーク構成についての見直しのレベルはB以上<br>・接続ルールとネットワーク構成についての文書化のレベルはB以上 |
| レベル2 | ネットワーク構成は内部システムの保護には必須とされるレベルに止まるものになっている。また、端末からの接続要求の取扱いについての担当者間での共通認識レベルの考え方はできており、端末間やセグメント間の通信に対する接続ルールが、この考え方に沿って、大まかではあるが示されている。<br>・接続要求の取扱いについのて考え方についての担当者間での共通認識は存在している<br>・ファイアウォールにより、DMZと内部セグメントは構成されている<br>・末間の接続ルールやネットワークの構成の検討のレベルはクラスC以上<br>・接続ルールとネットワーク構成についての文書化のレベルはC以上 |
| レベル1 | ファイアウオールの設置等で内部システムの保護のためのシステムの導入は行われているが、ネットワークレベルでの不正アクセス対策について組織的な取組みはないに等しい。<br>・レベル2の達成条件も満たせない |

(注 1) 接続制御方針として指定すべきこと
・端末グループとそれらのシステム面での位置づけとセキュリティ環境
・端末グループ間での接続方針：利用アプリケーション／プロトコル、アクセス制御の方針
・接続経路についての考え方
・接続要求に対する接続条件
・端末管理の方針
・ネットワークの冗長化についての考え方
・ネットワークの構成についての考え方（セグメント分割の方針）

(注2) ネットワークの構成設計で検討すべきこと
・セグメントの分割と各セグメントにおけるネットワーク面でのセキュリティ要求
・ネットワークトポロジー
・物理ネットワークの設計（伝送路、接続形態他）
・ネットワーク機器の論理配置および物理的な配置
・冗長化設計
・使用機器の選択とその使用法

## Tb1.2 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 端末からの接続要求に対する接続制御を行うための接続経路も含む接続条件が、システムがサポートするすべて端末に対し、よく検討された結果が的確に指定されており、またそのチェックも厳格で、その指定に不備が入り込むことは、まず考えられない。<br>・外部セグメントと内部セグメント間に加え、すべての内部セグメントの相互間での接続について、接続条件として検討すべきこと（注1）はすべて組織的に検討され、その結果がセグメント間の接続条件の指定に的確に反映されている（ことが確認されている）<br>・すべての外部端末と内部端末間の接続に加え、セグメント内の通信においてもすべての端末相互間の接続に対し、接続条件として検討すべきこと（注2）(注3)はすべてについてきめ細かく検討され、続条件の指定に的確に反映されていることが組織的に確認されている<br>・接続要求に対する接続条件の指定についてのプロセスならびにそのチェックのプロセスや見直しについてのルールが確立しておりマニュアル化されている<br>・接続要求に対する接続条件の指定は、指定されたプロセスに沿って行われており、そのチェックも徹底している<br>・接続条件の指定に対する見直しはレベル A<br>・接続要求に対する接続条件の指定についての管理の仕組みも確立しており、この仕組みに沿った管理が徹底して行われている<br>・接続条件の指定プロセスや管理の仕組みについての検討のレベルは A<br>・接続条件の指定内容、ならびに指定およびその管理についての文書化のレベルは A |
| レベル4 | 端末からの接続要求に対する接続制御を行うための接続経路も含む接続条件が、システムがサポートするすべて端末に対し、よく検討された結果が指定されているが、検討や指定内容のチェックに徹底さを欠くところも見られ、その指定に不備が入り込む隙が、僅かではあるが残されている。<br>・外部セグメントと内部セグメント間に加え、すべての内部セグメントの相互間での接続について、接続条件として検討すべきこと（注1）はすべて組織的に検討され、その結果がセグメント間の接続条件の指定に的確に反映されていることが確認されているが、一部に徹底さを欠くところも見られる<br>・すべての外部端末と内部端末間の接続に加え、特に重要視する端末についてはセグメント内の端末相互間の接続に対しても、接続条件として検討すべきこと（注2）（注3）はすべてについて、組織的に検討され、その結果がセグメント間の接続条件の指定に的確に反映されるようになっているが、検討や確認に徹底さを欠くところも見られる<br>・接続要求に対する接続条件の指定についてのプロセスならびにそのチェックのプロセスや見直しについてのルールが確立しておりマニュアル化されているが、まだ改善する余地もある<br>・接続要求に対する接続条件の指定は、指定されたプロセスに沿って行われており、そのチェックも概 |

| | |
|---|---|
| | ね徹底している<br>・接続条件の指定に対する見直しはレベルB以上<br>・接続要求に対する接続条件の指定についての管理の仕組みも確立しており、この仕組みに沿った管理が行われているが、徹底さにかけるところも見られる<br>・接続条件の指定プロセスや管理の仕組みについての検討のレベルはB以上<br>・接続条件の指定内容、ならびに指定およびその管理についての文書化のレベルはB以上 |
| レベル3 | 端末からの接続要求に対する接続制御を行うための接続条件が、システムがサポートするすべて端末に対し、組織的な検討の下で行われているが、レベル5、4に比べ、デフォルトの使用が多く、検討にきめ細かさに欠けるところもある。また、接続条件の指定の検討やレビューならびに接続条件の指定の管理についての組織的な管理も行われているが、徹底したものではなく、指定に不備が入り込む余地が残されている。<br>・外部セグメントと内部セグメント間に加え、すべての内部セグメントの相互間での接続について、接続条件として検討すべきこと(注1)はすべて組織的に検討され、その結果がセグメント間の接続条件の指定に的確に反映されるようになっているが、検討やチェックは徹底したものではない<br>・端末間の通信についての接続条件葉の指定の検討は、一部の内部端末についての外部との接続に限られている。その他については、端末間の接続条件はデフォルト指定としている<br>・大まかではあるが、接続要求に対する接続条件の指定についてのプロセスならびにそのチェックのプロセスや見直しについてのルールが確立しておりマニュアル化されているが、まだ改善する余地も多い<br>・接続要求に対する接続条件の指定やそのチェックは、概ね指定されたプロセスに沿って行われているが、検討やチェックは徹底したものとは言い難い<br>・接続条件の指定に対する見直しはレベルB以上<br>・大まかではあるが接続要求に対する接続条件の指定についての管理の仕組みも示されており、この仕組みに沿った管理が行われているが、徹底したものとは言い難い<br>・接続条件の指定プロセスや管理の仕組みについての検討のレベルはB以上<br>・接続条件の指定内容、ならびに指定およびその管理についての文書化のレベルはB以上 |
| レベル2 | 端末からの接続要求に対する接続制御を行うための接続条件の指定や管理は、担当チーム任されており、組織的に管理は行われていないが、担当チーム内で形成された習慣的ルールに沿って行われており、概ね適切であるが、不備が入り込む余地は少なくない。<br>・システムが固有に指定しなければならないところを除き、ほとんどがそれぞれの機器のデフォルトを使用している<br>・接続要求に対する接続条件の指定やそのチェックならびに指定の見直しについては、担当者間で習慣的に形成された手順やルールに沿って行われている<br>・接続条件の指定に対する見直しはレベルC以上<br>・接続条件の指定内容、ならびに指定およびその管理についての文書化のレベルはC以上 |
| レベル1 | 接続要求に対する接続条件の指定を適切に行うための組織的な取組みはないに等しい。<br>・レベル2の達成要件も満たしていない |

(注1) セグメント間の接続条件として検討すべきこと
- ・中継機器の使用方法
  - －利用プロトコルごとの使用経路
  - －利用プロトコルごとのアクセス制御の方法
  - －障害字の代替経路

(注2) 外部端末と内部端末間の接続条件として検討すべきこと
- ・端末間の接続条件(識別および認証の方法、利用プロトコル、接続場所、利用ユーザ、端末種別、接続形態(常時接続・ダイアルアップ)、使用する伝送路、アクセス制御の方式)
- ・中継機器の指定条件(利用プロトコルごとの経路選択、利用プロトコルごとのアクセス制御の方法、障害児の代替経路)

(注3) 同一セグメント内端末相互間での接続条件として検討すべきこと
- ・識別および認証の方法、利用プロトコル、接続場所、利用ユーザ、端末種別、接続形態(常時接続・ダイアルアップ)、使用する伝送路、アクセス制御の方式

## Tb1.3 接続制御機器の的確な実装

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 使用する接続制御機器における機能の設定や諸条件の機器への登録は、環境の変化への対応も含め、徹底してその的確性についての確認がされており、個々の機器に要求されている接続制御に不備が生じることは、まず考えられない。<br>・ルータにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注1)はすべてについて、その設定が厳格にチェックされており、的確であることが確認されている<br>・スイッチにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注2)はすべてについて、その設定が厳格にチェックされており、的確であることが確認されている<br>・ファイアウォールにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注3)はすべてについて、その設定が厳格にチェックされており、的確であることが確認されている<br>・プロキシを使用している場合、このプロキシにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注4)はすべてについて、その設定が厳格にチェックされており、的確であることが確認されている<br>・通信制御機器の実装についての作業プロセスや管理の仕組みが確立しており、これらはマニュアル化されている<br>・これらの機器における実装にかかる作業は所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の管理も徹底している<br>・接続制御機器の実装についての見直しのレベルはA<br>・接続制御機器の実装状況についての文書化のレベルはA |
| レベル4 | 使用する接続制御機器における機能の設定や諸条件の機器への登録は、環境の変化への対応も含め、その的確性についての確認は厳格に行われることになっているが、一部に徹底さを欠くところも見られ、これらの作業におけるミスが見逃される隙が、僅かではあるが残されている。<br>・ルータにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注1)はすべてについて、その設定が組織的にチェックされているが、一部に厳格さを欠くところも見られる<br>・スイッチにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注2)はすべてについて、その設定が組織的にチェックされているが、一部に厳格さをかくところも見られる<br>・ファイアウォールにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注3)はすべてについて、その設定はその設定が組織的にチェックされているが、一部に厳格さをかくところも見られる<br>・プロキシを使用している場合、このプロキシにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注4)はすべてについて、その設定が組織的にチェックされているが、一部に厳格さをかくところも見られる<br>・通信制御機器の実装についての作業プロセスや管理の仕組みが作られ、マニュアル化されているが、まだ改善の余地もある<br>・これらの機器における実装にかかる作業は所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の管理も概ね徹底している<br>・接続制御機器の実装についての見直しのレベルはB以上<br>・接続制御機器の実装状況についての文書化のレベルはB以上 |
| レベル3 | 使用する接続制御機器における機能の設定や諸条件の登録は、環境の変化への対応も含め、その的確性についての確認は決められた手順に沿って組織的に行われているが、徹底さは十分でなく、これらの作業におけるミスが見逃される余地が残されている。<br>・ルータにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注1)はすべてについて、その設定が組織的にチェックされているが、確認は徹底したものではない<br>・スイッチにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注2)はすべてについて、その設定が組織的にチェックされているが、確認は徹底したものではない<br>・ファイアウォールにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注3)はすべてについて、その設定がその設定は組織的にチェックされているが、確認は徹底したものではない<br>・プロキシを使用している場合、このプロキシにおける機能設定ならびにアクセス制御条件の設定において、指定が必要な事項(注4)はすべてについて、その設定が組織的にチェックされているが、確認は徹底したものではない<br>・大まかではあるが、通信制御機器の実装についての作業プロセスや管理の仕組みが作られ、マニュ |

| | |
|---|---|
| | アル化されている<br>・これらの機器における実装にかかる作業は、概ね、所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の管理も行われている<br>・接続制御機器の実装についての見直しのレベルはB以上<br>・接続制御機器の実装状況についての文書化のレベルはB以上 |
| レベル2 | 担当者レベルでは、使用する接続制御機器における機能の設定や諸条件の登録を慎重に行い、その的確性の確認も行ってはいるが、組織的なチェックや管理は行われてなく、これらの作業への信頼性は十分とは言えない。<br>・ルータにおける機能設定ならびにアクセス制御条件の設定において、個別指定が必須なところを除いては、ほとんどがデフォルト指定を使用している<br>・スイッチにおける機能設定ならびにアクセス制御条件の設定において、個別指定が必須なところを除いては、ほとんどがデフォルト指定を使用している<br>・ファイアウォールにおける機能設定ならびにアクセス制御条件の設定において、個別指定が必須なところを除いては、ほとんどがデフォルト指定を使用している<br>・これらの機器における実装にかかる作業やそのチェックは、担当者間での習慣的に形成された手順に、概ね、沿って行われており、これらの作業はある程度信頼できる<br>・接続制御機器の実装についての見直しのレベルはC以上<br>・接続制御機器の実装状況についての文書化のレベルはC以上 |
| レベル1 | 使用している接続制御機器の諸設定は担当者任せで管理されていない。<br>・レベル2の達成条件も満たせない |

(注1) ルータの設定において検討・確認すべきこと
- ・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、通信ログの収集条件（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
- ・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

(注2) スイッチの設定において検討・確認すべきこと
- ・機能設定：MACアドレスの管理、VLANの管理(VLANについては(5)を参照)
- ・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他）、アクセス元の認証、認証プロトコルの選択（CHAP, MS－CHAP, PAP, SPAP他）、帯域制御
- ・アクセス監視設定：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

(注3) ファイアウォールの設定において検討・確認すべきこと
- ・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、内部ネットワークの保護、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、暗号アルゴリズムの選択、ハッシュアルゴリズムの選択
- ・アクセス監視設定：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

(注3) ファイアウォールの設定において検討・確認すべきこと
- ・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：使用するプロキシタイプの選定、プロキシを設置するプロトコルの選定、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

## Tb1.4 VLAN の適切な使用

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | VLANの使用は注意深く行われており、その使用法や関係機能の設定の検討も徹底して検討、レビューされており、その実装の的確性の確認も徹底して行われており、VLANの使用においてセキュリティ面で問題を起こすことは、まず考えられない。<br>・VLANを用いる端末のグルーピングは徹底してチェックされている<br>・選択した方式における設定として検討すべき事項のすべて(注1)についての検討は、組織的に行われ、そのレビューも徹底しており、的確であることが確認されている<br>・VLAN ステーションは最も堅牢な使用法が指定されている(注2)<br>・指定された諸設定の実装も厳格にチェックされており、的確であることが確認されている<br>・VLANの設定や実装についての作業プロセスや管理の仕組みが確立しており、これらはマニュアル化されている<br>・これらの機器における実装にかかる作業は所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の管理も徹底している<br>・接続制御機器の実装についての見直しのレベルはA<br>・接続制御機器の実装状況についての文書化のレベルはA |
| レベル4 | VLANの使用は注意深く行われており、その使用法や関係機能の設定の検討やレビュー、およびその実装の確認も組織的に徹底して行われることになっているが、一部に徹底さを欠くところも見られ、VLANの使用における不備が見逃され、VLANの使用においてセキュリティ面で問題を起こす隙が、僅かではあるが、残されている。<br>・VLANを用いる端末のグルーピングは徹底してチェックされている<br>・選択した方式における設定として検討すべき事項のすべて(注1)についての検討は、組織的に行われ、そのレビューも組織的に行われているが、一部に厳格さを欠くところも見られる<br>・VLAN ステーションは比較的堅牢な使用法が指定されている(注3)<br>・指定された諸設定の実装も厳格にチェックされているが、一部に厳格さを欠くところが見られる<br>・VLANの設定や実装についての作業プロセスや管理の仕組みが確立しており、これらはマニュアル化されているが、まだ改善の余地がある<br>・これらの機器における実装にかかる作業は所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の厳格に管理されているが、一部に厳格さを欠くところが見られる<br>・接続制御機器の実装についての見直しのレベルはB以上<br>・接続制御機器の実装状況についての文書化のレベルはB以上 |
| レベル3 | VLANの使用法や関係機能の設定について、セキュリティ面での検討は行われているが、セキュリティ対策は平均的なレベル。また、その機能や諸設定の実装についてのチェックも組織的に行われているが、徹底したものとは言い難く、VLANの使用における不備が見逃され、VLANの使用においてセキュリティ面で問題を起こす可能性が残されている。<br>・VLANを用いる端末のグルーピングの適切性についてのチェックは、組織的に行われている<br>・選択した方式における設定として検討すべき事項のすべて(注1)についての検討は、組織的に行われ、そのレビューも徹底しており、的確であることが確認されている<br>・VLAN ステーションは平均的な使用法が指定されている<br>・指定された諸設定の実装のチェックは、定められた手順に沿って行われているが、必ずしも厳格なものではない<br>・大まかではあるがVLANの設定や実装についての作業プロセスや管理の仕組みが示されており、これらはマニュアル化されている<br>・これらの機器における実装にかかる作業は所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の管理も行われているが、徹底したものではない<br>・接続制御機器の実装についての見直しのレベルはB以上<br>・接続制御機器の実装状況についての文書化のレベルはB以上 |
| レベル2 | VLANの使用法や関係機能の設定について、セキュリティ面での検討や、実装は担当者に任されている。担当者は、そのリスクを承知しており、最低限の対策をとっているようであるが、組織的なレビューや管理は行われてなく、VLANの使用における不備が入り込む余地は少なくない。<br>・VLAN ステーションの使用は、個別指定を行うところを除いては、ほとんどデフォルトが使用されている |

| | |
|---|---|
| | ・選択した方式における設定として検討すべき事項についての検討は、担当者のスキルレベルに依存している<br>・指定された諸設定の実装のチェックも担当者に任されている<br>・担当者間には、ＶＬＡＮの設定や実装についての作業プロセスや管理の方法について習慣的に形成されたものが存在している<br>・接続制御機器の実装についての見直しのレベルはＣ以上<br>・接続制御機器の実装状況についての文書化のレベルはＣ以上 |
| レベル1 | VLAN の使用に対するセキュリティ対策は、担当者任せで管理されていない。<br>・レベル2の達成条件も満たせない |

(注 1) VLAN ステーションの使用法について検討すべきこと
・使用する VLAN の方式
・アクセス制御の設定
－ポートベースの 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）
－MAC アドレスベースの 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）
－ポリシーベースの 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 等)、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 等)、DHCP サービス、パケットフィルタリング）
・監視機能の設定（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）

(注2) 堅牢な VLAN と見られる要件
・認証 VLAN の使用
・きめの細かい通信ログの収集の指定
・SNMP によるトラフィックの監視の指定

(注3) 比較的堅牢な VLAN と見られる要件
・比較的きめの細かい通信ログの収集の指定
・SNMP によるトラフィックの監視の指定

## Tb1.5 無線 LAN の適切な使用

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 無線ＬＡＮの使用は注意深く行われており、その使用法や関係機能の設定の検討も徹底して検討、レビューされており、その実装の的確性の確認も徹底して行われており、無線ＬＡＮの使用においてセキュリティ面で問題を起こすことは、まず考えられない。<br>・無線ＬＡＮを用いる端末グループは徹底して管理されている<br>・選択した方式における設定として検討すべき事項のすべて（注1）についての検討は、組織的に行われ、そのレビューも徹底しており、的確であることが確認されている<br>・無線ＬＡＮステーションは最も堅牢な使用法が指定されている（注2）<br>・指定された諸設定の実装も厳格にチェックされており、的確であることが確認されている<br>・無線ＬＡＮの設定や実装についての作業プロセスや管理の仕組みが確立しており、これらはマニュアル化されている<br>・これらの機器における実装にかかる作業は所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の管理も徹底している |

| | |
|---|---|
| | ・接続制御機器の実装についての見直しのレベルはＡ<br>・接続制御機器の実装状況についての文書化のレベルはＡ |
| レベル4 | 無線ＬＡＮの使用は注意深く行われており、その使用法や関係機能の設定の検討やレビュー、およびその実装の確認も組織的に徹底して行われることになっているが、一部に徹底さを欠くところも見られ、無線ＬＡＮの使用における不備が見逃され、無線ＬＡＮの使用においてセキュリティ面で問題を起こす隙が、僅かではあるが残されている。<br>・無線ＬＡＮを用いる端末グループは徹底して管理されている<br>・選択した方式における設定として検討すべき事項のすべて（注1）についての検討は、組織的に行われ、そのレビューも組織的に行われているが、一部に厳格さを欠くところも見られる<br>・無線ＬＡＮステーションは比較的堅牢な使用法が指定されている（注3）<br>・指定された諸設定の実装も厳格にチェックされているが、一部に厳格さを欠くところも見られる<br>・無線ＬＡＮの設定や実装についての作業プロセスや管理の仕組みが確立しており、これらはマニュアル化されているが、まだ改善の余地がある<br>・これらの機器における実装にかかる作業は所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の管理も厳格に行われているが、一部に厳格さを欠くところも見られる<br>・接続制御機器の実装についての見直しのレベルはＢ以上<br>・接続制御機器の実装状況についての文書化のレベルはＢ以上 |
| レベル3 | 無線ＬＡＮの使用法や関係機能の設定について、セキュリティ面での検討は行われているが、セキュリティ対策は平均的なレベル。また、その機能や諸設定の実装についてのチェックも組織的に行われているが、徹底したものとは言い難く、無線ＬＡＮの使用における不備が見逃され、無線ＬＡＮの使用においてセキュリティ面で問題を起こす余地も残されている。<br>・無線ＬＡＮを用いる端末のグルーピングの適切性についてのチェックは、組織的に行われている<br>・選択した方式における設定として検討すべき事項のすべて（注1）についての検討は、組織的に行われ、そのレビューも徹底しており、的確であることが確認されている<br>・無線ＬＡＮステーションは平均的な使用法が指定されている<br>・指定された諸設定の実装のチェックは、定められた手順に沿って行われて入るが、必ずしも厳格なものではない<br>・大まかではあるが無線ＬＡＮの設定や実装についての作業プロセスや管理の仕組みが示されており、これらはマニュアル化されている<br>・これらの機器における実装にかかる作業は所定のプロセスに沿って行われており、これらの作業や実装状況についての作業の管理も行われているが、徹底したものではない<br>・接続制御機器の実装についての見直しのレベルはＢ以上<br>・接続制御機器の実装状況についての文書化のレベルはＢ以上 |
| レベル2 | 無線ＬＡＮの使用法や関係機能の設定について、セキュリティ面での検討や、実装は担当者に任されている。担当者は、そのリスクを招致しており、最低限の対応をしているが、組織的なレビューや管理は、行われてなく、ＶＬＡＮの使用における不備が見逃され、無線ＬＡＮの使用においてセキュリティ面で問題を起こすことも考えられる。<br>・無線ＬＡＮステーションの使用は、個別指定を行うところを除いては、ほとんどデフォルトが使用されている<br>・選択した方式における設定として検討すべき事項についての検討は、担当者にレベルに依存している<br>・指定された諸設定の実装のチェックも担当者に任されている<br>・担当者間には、無線ＬＡＮの設定や実装についての作業プロセスや管理の方法について習慣的に形成されたものが存在している<br>・接続制御機器の実装についての見直しのレベルはＣ以上<br>・接続制御機器の実装状況についての文書化のレベルはＣ以上 |
| レベル1 | 無線ＬＡＮの使用についてのセキュリティ対策は担当者任せで、管理されていない。<br>・レベル2の達成条件も満たせない |

(注 1) 無線 LAN ステーションの使用法について検討すべきこと

・機能設定（無線規格の選択： IEEE802.11(b,a,g,i)、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 等)、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）

(注2) 堅牢な無線 LAN と見られる要件
・最強の暗号化アルゴリズム（AES）の使用
・識別 ID の隠蔽
・認証機能の使用
・認証機能の使用

(注3) 比較的堅牢な無線 LAN と見られる要件
・比較的きめの細かい通信ログの収集の指定
・SNMP によるトラフィックの監視の指定

## Tb1.6 一般ユーザアカウントに対する適切な管理の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 一般ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）についての基準に沿ったユーザアカウントの管理が厳格に行われており、一般ユーザアカウントの管理で不手際が生じることは、まず考えられない。<br>・一般ユーザに対するシステムレベルでのアクセス管理についてきめの細かい基準（注1）が確立している<br>・一般ユーザアカウントの管理についてのきめの細かい仕組みも確立している<br>・ユーザの管理（注2）も、この仕組みに沿って厳格に管理されている<br>・ユーザグループの設定ならびに各ユーザグループへのユーザの登録も、この仕組みに沿った厳格な管理の下で行われている<br>・管理しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、この仕組みに沿って厳格に管理されている<br>・ユーザアカウントに関する情報への、ユーザの資格変更等への対応のタイムラグは１日以内<br>・不要なデフォルトアカウントの削除や無効化は徹底して行われていて、管理されていない稼動アカウントはシステムに存在しないことが確認されている<br>・システムで使用されるすべての一般ユーザアカウントは、何時でも正確に把握できるようになっている<br>・一般ユーザアカウントの使用やその管理についての見直し状況はクラス A<br>・一般ユーザアカウントの使用やその管理についての文書化のレベルはクラス A |
| レベル4 | 一般ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）についての基準に沿ったユーザアカウントの管理が組織的に行われているが、一部に厳格さに欠けるところが見られる。一般ユーザアカウントの管理で不手際が生じる隙が、僅かではあるが残されている。<br>・一般ユーザに対するシステムレベルでのアクセス管理について、相当にきめの細かい基準（注1）が確立している<br>・一般ユーザアカウントの管理についての相当にきめの細かい仕組みも確立している<br>・ユーザの管理（注2）も、この仕組みに沿って厳格に管理されているが、一部に厳格さに欠けるところが見られる<br>・ユーザグループの設定ならびに各ユーザグループへのユーザの登録も、この仕組みに沿って組織的な管理の下で行われているが、一部に厳格さに欠けるところが見られる<br>・管理しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、この仕組みに沿った組織的な管理の下で行われているが、一部に厳格さに欠けるところが見られる<br>・ユーザアカウントに関する情報への、ユーザの資格変更等への対応のタイムラグは3日以内<br>・不要なデフォルトアカウントの削除や無効化は徹底して行われていて、管理されていない稼動アカウントはシステムに存在しないことが確認されている<br>・システムで使用されるすべての一般ユーザアカウントは、何時でも正確に把握できるようになっている<br>・一般ユーザアカウントの使用やその管理についての見直し状況はクラス B 以上<br>・一般ユーザアカウントの使用やその管理についての文書化のレベルはクラス B 以上 |

| | |
|---|---|
| レベル 3 | 大まかではあるが、システムレベルでのアクセス管理（アクセスの制御や監視）についての基準が示され、一般ユーザアカウントはこの方針に沿って、組織的な管理の下で行われているが、管理は徹底したものとは言い難い。一般ユーザアカウントの管理で不手際が生じる可能性も残されている。<br>・大まかではあるが、一般ユーザに対するシステムレベルでのアクセス管理について基準は示されている<br>・大まかではあるが、一般ユーザアカウントの管理についての仕組みも作られている<br>・ユーザの管理（注2）はこの仕組みに沿って、組織的な管理の下で行われているが、管理は徹底したものではない<br>・ユーザグループの設定ならびに各ユーザグループへのユーザの登録も、この仕組みに沿って組織的な管理の下で行われているが、管理は徹底したものではない<br>・管理しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、この仕組みに沿った組織的な管理の下で行われているが、管理は徹底したものではない<br>・ユーザアカウントに関する情報への、ユーザの資格変更等への対応のタイムラグは 1 週間以内<br>・不要なデフォルトアカウントの削除や無効化も追及されており、管理されていない稼動アカウントはシステムに存在しないことになっている<br>・システムで使用されるすべての一般ユーザアカウントは、把握できるようになっている<br>・一般ユーザアカウントの使用やその管理についての見直し状況はクラス B 以上<br>・一般ユーザアカウントの使用やその管理についての文書化のレベルはクラス B 以上 |
| レベル 2 | 一般ユーザアカウントの管理については、担当者間に習慣的に形成された方法が存在していて、一般ユーザアカウントの管理は、担当チームでのチェックの下で、この方法によって行われている。担当者は相応の注意を払って行っているが、組織的なチェックや管理が行われているとは言い難く、このユーザ管理に不手際が生じることも考えられる。<br>・一般ユーザに対するシステムレベルでのアクセス管理について、担当者間での共通認識的な基準は存在している<br>・担当者間には、一般ユーザアカウントの管理の方法について習慣的に形勢された手順等が存在し、ユーザ管理は概ねこの手順に沿って行われている<br>・ユーザグループの設定にも注意が払われている<br>・管理しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、担当チームに任されている。担当者は不手際を起こさないようにする努力は行われている<br>・一般ユーザアカウントの使用やその管理についての文書化のレベルはクラス C 以上 |
| レベル 1 | 一般ユーザアカウントの管理は、ほとんど行われていない<br>・レベル 2 の達成条件も満たせない |

(注 1) 一般ユーザに対するシステムレベルでのアクセス管理（アクセス制御とアクセスの監視）についての基準として検討すべき事項
- ・システム（OS）レベルでアクセスを許可するサービス
- ・認証方式の選択
- ・アクセスを許可するユーザとその権限
- ・ユーザの識別・認証に用いる情報
- ・ユーザグループの編成方針
- ・必要に応じ、端末アドレスや時間帯によるアクセス制限やセッション管理の方針

(注2) ユーザ管理として行うべきこと
- ・ユーザとしての資格の確認の方法
- ・ユーザグループとの関係
- ・システムへのアクセスに関し付与される権限
- ・見直しを行わなければならないタイミングやイベント

## Tb1.7 一般ユーザに対する適切なアクセス制御の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 一般ユーザに対するシステムレベルのアクセスに対して、最も厳格とみられるアクセス制御やアクセスの監視(注1)が適用されている。また、一般ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）機能のシステムへの組込みは、組織的な管理の下で、徹底してチェックされており、常に、その的確性は維持されている。一般ユーザに対するシステムレベルのアクセス管理で不手際が生じることは、まず考えられない。<br>・システムレベルのアクセス制御やアクセスの監視としては、現時点では最も厳格なレベル（注1）のものが適用されている<br>・システムへのこれらにかかわる機能の組込みや、登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックについての作業プロセスや管理の仕組みが確立している<br>・システムへのこれらにかかわる機能の組込みは徹底してチェックされおり、その的確性は組織的に確認されている<br>・システムへのこれらの機能が使用する情報の登録は徹底してチェックされおり、その的確性は組織的に確認されている<br>・システムに登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、これらにかかわる仕組みに沿って厳格に管理されており、システムの登録されている一般ユーザアカウントは、すべて何時でも正確に把握できるようになっている<br>・ユーザアカウントにかかわる変更のシステムへの反映のタイムラグは１日以内<br>・システム上での一般ユーザアカウントやシステムレベルのアクセス管理についての見直し状況はクラスA<br>・システム上での一般ユーザアカウントやシステムレベルのアクセス管理についての文書化のレベルはクラスA |
| レベル4 | 一般ユーザに対するシステムレベルのアクセスに対して、相当に厳格とみられるアクセス制御やアクセスの監視（注2）が適用されている。また、一般ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）機能のシステムへの組込みは、組織的な管理の下でチェックされ、常に、その的確性を維持する努力は行われているが、一部に徹底さを欠くところも見られる。まず十分といえるが、一般ユーザに対するシステムレベルのアクセス管理で不手際が生じる隙が、僅かではあるが残されている。<br>・システムレベルのアクセス制御やアクセスの監視としては、現時点では相当に厳格なレベル（注2）のものが適用されている<br>・システムへのこれらにかかわる機能の組込みや、登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックについての作業プロセスや管理の仕組みが確立しているが、まだ改善の余地もある<br>・システムへのこれらにかかわる機能の組込みは徹底してチェックされおり、その的確性は組織的に確認されているが、一部に徹底さに欠けるところがある<br>・システムへのこれらの機能が使用する情報の登録は徹底してチェックされおり、その的確性は組織的に確認されている、一部に徹底さに欠けるところがある<br>・システムに登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、これらにかかわる仕組みに沿って厳格に管理されており、システムの登録されている一般ユーザアカウントは、すべて何時でも正確に把握できるようになっている、一部に徹底さに欠けるところがある<br>・ユーザアカウントにかかわる変更のシステムへの反映のタイムラグは3日以内<br>・システム上での一般ユーザアカウントやシステムレベルのアクセス管理についての見直し状況はクラスB以上<br>・システム上での一般ユーザアカウントやシステムレベルのアクセス管理についての文書化のレベルはクラスB以上 |
| レベル3 | 一般ユーザに対するシステムレベルのアクセスに対して、一般に用いるべきと見られるアクセス制御やアクセスの監視（3）は、ほとんど適用されている。また、一般ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）機能のシステムへの組込みは、組織的な管理の下でチェックされているが、徹底したものではない。概ね、十分といえるが、一般ユーザに対するシステムレベルのアクセス管理で不手際が生じる余地が残されている。<br>・システムレベルのアクセス制御やアクセスの監視としては、一般的なレベル（注3）が適用されている |

| | |
|---|---|
| | ・システムへのこれらにかかわる機能の組込みや、登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックについて、大まかではあるが作業プロセスや管理の仕組みは作られている<br>・システムへのこれらにかかわる機能の組込みは、組織的な管理の下でチェックされているが、徹底したものではない<br>・システムへのこれらの機能が使用する情報の登録は、組織的な管理の下でチェックされているが、徹底したものではない<br>・システムに登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、これらにかかわる仕組みに沿って組織的な管理の下でチェックされているが、徹底したものではない。また、システムの登録されている一般ユーザアカウントは、何時でも把握できるようになっているが、この点では十分とは言えないところもある<br>・ユーザアカウントにかかわる変更のシステムへの反映のタイムラグは1週間以内<br>・システム上での一般ユーザアカウントやシステムレベルのアクセス管理についての見直し状況はクラスB以上<br>・システム上での一般ユーザアカウントやシステムレベルのアクセス管理についての文書化のレベルはクラスB以上 |
| レベル2 | 一般ユーザに対するシステムレベルのアクセスに対して、最低限必要とされるアクセス制御やアクセスの監視（注3）は適用されている。一般ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）機能のシステムへの組込みは、担当チームに任されており、組織的なチェックや管理は行われていない。最小限の管理は行われてはいるが、一般ユーザに対するシステムレベルのアクセス管理で不手際が生じることも考えられる。<br>・システムレベルのアクセス制御やアクセスの監視としては、一般的なレベル（注3）が適用されている<br>・担当者間には、システムへのこれらにかかわる機能の組込みや、登録しているアカウントおよび対応する権限リストの登録・変更・削除についての作業やそのチェックについて、習慣的に形成された手順が存在している<br>・システムへのこれらにかかわる機能の組込みや、これらの機能が使用する情報の登録は、およびそのチェックは担当者に任されている<br>・システムに登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、担当者に任されている。<br>・担当者は、これらの作業の重要性を認識しており、それなりの注意を払ってこれらを行っている<br>・システム上での一般ユーザアカウントやシステムレベルのアクセス管理についての見直し状況はクラスC以上<br>・システム上での一般ユーザアカウントやシステムレベルのアクセス管理についての文書化のレベルはクラスC以上 |
| レベル1 | 一般ユーザに対するシステムレベルでのアクセス管理は、組織的に管理されていない<br>・レベル2の達成条件も満たせない |

(注1) 一般ユーザに対するシステムレベルでのアクセス管理を、最も厳格なものとしたい場合に実施を検討すべき事項
（注2）に示した“相当に厳格なものとしたい場合に実施を検討すべき事項”に以下を加える
・必要に応じた現時点ではもっとも強力と見られる認証方式の適用
－ローカルアクセスに対しては、生体認証と他の認証方式による二要素認証の使用
－ネットワークアクセスについては、十分な鍵長さを持った電子証明書による認証の適用、等

(注2) 一般ユーザに対するシステムレベルでのアクセス管理を、相当に厳格なものとしたい場合に実施を検討すべき事項
・デバイス認証におけるパスワードとの二要素認証の使用
・平均以上の強度を持ったパスワードの使用
－容易に推測できる文字列の使用の禁止
－一定の長さと複雑性のある文字列の使用
－定期的な更新
－同一パスワードの繰返し使用や循環使用の禁止
・ネットワークアクセスのためにクライアントに置く認証鍵の暗号化と、十分な強度をもったパスワードの使用

・認証試行回数の制限および一定回数失敗時のアカウントロックアウトの適用
・パスワードを平文で流すプロトコル/サービス、および弱いチャレンジ・レスポンス認証を行うプロトコル/サービスの使用の禁止
・アカウント登録とアクセス制御の設定についての要件
　－認可され、記録されたユーザアカウントのみがシステムに登録されている
　－すべてのアカウントは個人に対して発行され、アクセスを識別できる
　－アカウントはルールに基づく適切なグループ/ロールが設定されている
　－接続元アドレスによる制限等、OS レベルでのサービス接続制限が行われている
　－OS への対話的ログインは不必要なユーザに与えられていない
　－デフォルトのパーミッションが適切に設定されている
・システムユーティリティが識別され、使用できるユーザが制限されている
・グループアカウントを用いる場合の補強策
・システムのアクセスログの取得
　－ログインの成功と失敗およびログアウトについてのログの取得
　－保護対象ファイルへのアクセス（成功・失敗を問わず）についてのログの取得

(注3) 一般ユーザに対するシステムレベルでのアクセス管理として一般に実施を検討すべき事項
・適切に運用されたパスワード認証または IC カード等によるデバイス認証の実施
・平均以上の強度を持ったパスワードの使用
　－容易に推測できる文字列の使用の禁止
　－一定の長さと複雑性のある文字列の使用
　－定期的な更新
　－同一パスワードの繰返し使用や循環使用の禁止
・認証試行回数の制限および一定回数失敗時のアカウントロックアウトの適用
・パスワードを平文で流すプロトコル/サービスの使用の禁止
・アカウント登録とアクセス制御の設定についての要件
　－認可され、記録されたユーザアカウントのみがシステムに登録されている
　－すべてのアカウントは個人に対して発行され、アクセスを識別できる
　－アカウントはルールに基づく適切なグループ/ロールが設定されている
　－接続元アドレスによる制限等、OS レベルでのサービス接続制限が行われている
　－OS への対話的ログインは不必要なユーザに与えられていない
　－デフォルトのパーミッションが適切に設定されている
・グループアカウントを用いる場合の補強策
・システムのアクセスログの取得
　－ログインの成功と失敗およびログアウトについてのログの取得
　－保護対象ファイルへのアクセス（成功・失敗を問わず）についてのログの取得

## Tb1.8 特権ユーザアカウントに対する適切な管理の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 特権ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）についての基準に沿ったユーザアカウントの管理が厳格に行われており、特権ユーザアカウントの管理で不手際が生じることは、まず考えられない。<br>・特権ユーザに対するシステムレベルでのアクセス管理について、きめの細かい基準が（注1）確立している<br>・特権の使用についての制限は、特に厳しいもの（注 2）になっている<br>・特権ユーザアカウントの管理についてのきめの細かい仕組みも確立している<br>・特権ユーザの管理（注 3）も、この仕組みに沿って厳格に管理されている<br>・特権ユーザグループの設定ならびに各ユーザグループへのユーザの登録も、この仕組みに沿った厳格な管理の下で行われている |

| | |
|---|---|
| | ・管理しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、この仕組みに沿って厳格に管理されている<br>・特権の取扱いや特権ユーザに変更の必要が生じた場合の、必要な措置が終わるまでのタイムラグは1日以内<br>・システムで使用されるすべての特権ユーザアカウントは、何時でも正確に把握できるようになっている<br>・特権ユーザアカウントの使用やその管理についての見直し状況はクラスA<br>・特権ユーザアカウントの使用やその管理についての文書化のレベルはクラスA |
| レベル4 | 特権ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）についての基準に沿った特権ユーザアカウントの管理が組織的に行われているが、一部に厳格さに欠けるところが見られる。特権ユーザアカウントの管理で不手際が生じる隙が、僅かではあるが残されている。<br>・特権ユーザに対するシステムレベルでのアクセス管理について、相当にきめの細かい基準が（注1）確立しているが、まだ改善する余地もある<br>・特権の使用についての制限は、一般に比べ厳しいもの（注2）になっている<br>・特権ユーザアカウントの管理についての相当にきめの細かい仕組みも確立している<br>・ユーザの管理（注5）も、この仕組みに沿って厳格に管理されているが、一部に厳格さに欠けるところが見られる<br>・特権ユーザグループの設定ならびに各ユーザグループへのユーザの登録も、この仕組みに沿って組織的な管理の下で行われているが、一部に厳格さに欠けるところが見られる<br>・管理している特権アカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、この仕組みに沿った組織的な管理の下で行われているが、一部に厳格さに欠けるところが見られる<br>・特権の取扱いや特権ユーザに変更の必要が生じた場合の、必要な措置が終わるまでのタイムラグは3日以内<br>・システムで使用されるすべての特権ユーザアカウントは、何時でも正確に把握できるようになっている<br>・特権ユーザアカウントの使用やその管理についての見直し状況はクラスB以上<br>・特権ユーザアカウントの使用やその管理についての文書化のレベルはクラスB以上 |
| レベル3 | 大まかではあるが、システムレベルでのアクセス管理（アクセスの制御や監視）についての基準が示され、特権ユーザアカウントはこの方針に沿って、組織的な管理の下で行われているが、管理は徹底したものとは言い難い。特権ユーザアカウントの管理で不手際が生じる可能性も残されている。<br>・大まかではあるが、特権ユーザに対するシステムレベルでのアクセス管理についての基準(注 1)は示されている<br>・特権の使用についての制限は、一般的なレベルが指定されている<br>・大まかではあるが、特権ユーザアカウントの管理についての仕組みも作られている<br>・ユーザの管理はこの仕組みに沿って、組織的な管理の下で行われているが、管理は徹底したものではない<br>・特権ユーザグループの設定ならびに各ユーザグループへのユーザの登録も、この仕組みに沿って組織的な管理の下で行われているが、管理は徹底したものではない<br>・管理しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、この仕組みに沿った組織的な管理の下で行われているが、管理は徹底したものではない<br>・特権の取扱いや特権ユーザに変更の必要が生じた場合の、必要な措置が終わるまでのタイムラグは1週間以内<br>・システムで使用されるすべての特権ユーザアカウントは、把握できるようになっている<br>・特権ユーザアカウントの使用やその管理についての見直し状況はクラスB以上<br>・特権ユーザアカウントの使用やその管理についての文書化のレベルはクラスB以上 |
| レベル2 | 特権ユーザアカウントの管理については、担当者間に習慣的に形成された方法が存在していて、特権ユーザの管理は、この方法によって行われている。担当者は相応の注意を払って行って、一般ユーザに不用意に特権を与えるようなことはないが、組織的なチェックや管理が行われているとは言い難く、この特権ユーザ管理に不手際が生じる可能性がある。<br>・特権の使用および特権ユーザの管理について、担当者間での共通認識的な基準は存在している<br>・担当者間には、特権の使用および特権ユーザの管理の方法について習慣的に形成された手順等が存在し、これらの管理は概ねこの手順に沿って行われている<br>・ユーザグループの設定にも注意が払われている<br>・特権ユーザや権限リストの登録・変更・削除とそのチェックは、担当チームに任されている。担当者は不手際を起こさないようにする努力は行われている<br>・特権ユーザアカウントの使用やその管理についての文書化のレベルはクラスC以上 |

| | |
|---|---|
| レベル 1 | 特権の使用および特権ユーザの組織的な管理は、行われていないに等しい。<br>・レベル 2 の達成条件も満たせない |

(注1) 特権ユーザに対するシステムレベルでのアクセス管理（アクセス制御とアクセスの監視）についての基準として検討すべき事項
- ・管理対象の特権
- ・特権付与の基本方針（権限の制限化、分散）
- ・特権グループ／ロール
- ・特権アカウントへのアクセス制御の方針
- ・特権アカウントでのログインの制限についての方針
- ・特権アクセスおよび特権使用のログの取得方針
- ・特権の変更の制限

(注 2) 厳格と見ることができる特権の使用についての制限
- ・特権ユーザまたは特権ユーザに su できるログインの認証への最強と思われる認証方式の適用（認証デバイスを使用した二要素認証あるいは生体認証の使用）
- ・特権グループの設定とロールの付与
- ・特権アカウントでのネットワークログインの禁止
- ・UNIX の場合、root アカウントでの直接ログインの禁止（su コマンドの使用）
- ・sudo コマンドの利用等の制限（su root の使用の制限）
- ・特権アカウントでのログインの成功と失敗およびログアウトのログの取得
- ・UNIX の場合、su コマンド実行の成功と失敗のログの取得

(注 3) 特権ユーザ管理として行うべきこと
- ・特権ユーザとしての資格の確認の方法
- ・特権グループの設定とロールの付与
- ・見直しを行わなければならないタイミングやイベント

## Tb1.9 特権ユーザに対する適切なアクセス制御の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | 特権ユーザに対するシステムレベルのアクセスに対して、最も厳格とみられるアクセス制御やアクセスの監視(注1)が適用されている。また、特権ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）機能のシステムへの組込みは、組織的な管理の下で、徹底してチェックされており、常に、その的確性は維持されている。特権ユーザに対するシステムレベルのアクセス管理で不手際が生じることは、まず考えられない。<br>・システムレベルのアクセス制御やアクセスの監視としては、現時点では最も厳格なレベル（注1）のものが適用されている<br>・システムへのこれらにかかわる機能の組込みや、登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックについての作業プロセスや管理の仕組みが確立している<br>・システムへのこれらにかかわる機能の組込みは徹底してチェックされおり、その的確性は組織的に確認されている<br>・システムへのこれらの機能が使用する情報の登録は徹底してチェックされおり、その的確性は組織的に確認されている<br>・システムに登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、これらにかかわる仕組みに沿って厳格に管理されており、システムの登録されている一般ユーザアカウントは、すべて何時でも正確に把握できるようになっている<br>・ユーザアカウントにかかわる変更のシステムへの反映のタイムラグは 1 日以内 |

| | |
|---|---|
| | ・システム上での特権ユーザアカウントやシステムレベルのアクセス管理についての見直し状況はクラスA<br>・システム上での特権ユーザアカウントやシステムレベルのアクセス管理についての文書化のレベルはクラスA |
| レベル4 | 特権ユーザに対するシステムレベルのアクセスに対して、相当に厳格とみられるアクセス制御やアクセスの監視（注1）が適用されている。また、特権ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）機能のシステムへの組込みは、組織的な管理の下でチェックされ、常に、その的確性を維持する努力は行われているが、一部に徹底さを欠くところも見られる。まず十分といえるが、特権ユーザに対するシステムレベルのアクセス管理で不手際が生じる隙が、僅かではあるが残されている。<br>・システムレベルのアクセス制御やアクセスの監視としては、現時点では相当に厳格なレベル（注1）のものが適用されている<br>・システムへのこれらにかかわる機能の組込みや、登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックについての作業プロセスや管理の仕組みが確立しているが、まだ改善の余地もある<br>・システムへのこれらにかかわる機能の組込みは徹底してチェックされおり、その的確性は組織的に確認されているが、一部に徹底さに欠けるところがある<br>・システムへのこれらの機能が使用する情報の登録は徹底してチェックされおり、その的確性は組織的に確認されている、一部に徹底さに欠けるところがある<br>・システムに登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、これらにかかわる仕組みに沿って厳格に管理されており、システムの登録されている特権ユーザアカウントは、すべて何時でも正確に把握できるようになっている、一部に徹底さに欠けるところがある<br>・ユーザアカウントにかかわる変更のシステムへの反映のタイムラグは3日以内<br>・システム上での特権ユーザアカウントやシステムレベルのアクセス管理についての見直し状況はクラスB以上<br>・システム上での特権ユーザアカウントやシステムレベルのアクセス管理についての文書化のレベルはクラスB以上 |
| レベル3 | 特権ユーザに対するシステムレベルのアクセスに対して、特権に用いるべきと見られるアクセス制御やアクセスの監視（注1）は、ほとんど適用されている。また、特権ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）機能のシステムへの組込みは、組織的な管理の下でチェックされているが、徹底したものではない。概ね、十分といえるが、特権ユーザに対するシステムレベルのアクセス管理で不手際が生じる隙が残されている。<br>・システムレベルのアクセス制御やアクセスの監視としては、一般的なレベルが適用されている<br>・システムへのこれらにかかわる機能の組込みや、登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックについて、大まかではあるが作業プロセスや管理の仕組みは作られている<br>・システムへのこれらにかかわる機能の組込みは、組織的な管理の下でチェックされているが、徹底したものではない<br>・システムへのこれらの機能が使用する情報の登録は、組織的な管理の下でチェックされているが、徹底したものではない<br>・システムに登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、これらにかかわる仕組みに沿って組織的な管理の下でチェックされているが、徹底したものではない。また、システムの登録されている特権ユーザアカウントは、何時でも把握できるようになっているが、この点では十分とは言えないところもある<br>・ユーザアカウントにかかわる変更のシステムへの反映のタイムラグは1週間以内<br>・システム上での特権ユーザアカウントやシステムレベルのアクセス管理についての見直し状況はクラスB以上<br>・システム上での特権ユーザアカウントやシステムレベルのアクセス管理についての文書化のレベルはクラスB以上 |
| レベル2 | 特権ユーザに対するシステムレベルのアクセスに対して、最低限必要とされるアクセス制御やアクセスの監視（注1）は適用されている。特権ユーザに対するシステムレベルでのアクセス管理（アクセスの制御や監視）機能のシステムへの組込みは、担当チームに任されており、組織的なチェックや管理は行なわれていない。特権ユーザに対するシステムレベルのアクセス管理で不手際が生じることも考えられる。<br>・システムレベルのアクセス制御やアクセスの監視としては、一般的なレベル（注3）が適用されている<br>・担当者間には、システムへのこれらにかかわる機能の組込みや、登録しているアカウントおよび対応 |

| | |
|---|---|
| | する権限リストの登録・変更・削除についての作業やそのチェックについて、習慣的に形成されてた手順が存在している<br>・システムへのこれらにかかわる機能の組込みや、これらの機能が使用する情報の登録は、およびそのチェックは担当者に任されている<br>・システムに登録しているアカウントおよび対応する権限リストの登録・変更・削除とそのチェックは、担当者に任されている。<br>・担当者は、これらの作業の重要性を認識しており、それなりの注意を払ってこれらを行っている<br>・システム上での特権ユーザアカウントやシステムレベルのアクセス管理についての見直し状況はクラス C 以上<br>・システム上での特権ユーザアカウントやシステムレベルのアクセス管理についての文書化のレベルはクラス C 以上 |
| レベル 1 | 特権ユーザに対するシステムレベルでのアクセス管理は、組織的に管理されていない<br>・レベル 2 の達成条件も満たせない |

(注1) 特権ユーザに対するシステムレベルでのアクセス管理（アクセス制御とアクセスの監視）についての基準として検討すべき事項
- ・管理対象の特権
- ・特権付与の基本方針（権限の制限化、分散）
- ・特権グループ／ロール
- ・特権アカウントへのアクセス制御の方針
- ・特権アカウントでのログインの制限についての方針
- ・特権アクセスおよび特権使用のログの取得方針
- ・特権の変更の制限

## Tb1.10 必要に応じたセキュアな OS の適切な使用

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | 組織的に徹底して行われたセキュアな OS の使用法の研究にもとづいた最適化された使用法（注1）が確立しており、その実装も的確であることが徹底してチェックされている。諸設定等の維持管理も厳格な管理下で行われており、セキュア OS は、常に、期待通りの機能している<br>・専門家の支援も受けた組織的な検討により、使用法はそれぞれの使用場所に対応した最適化が図られている<br>・管理者権限の管理も決定された使用法に沿って厳格に行われている<br>・プロセスのパーティションやコンパートメントの設定も、的確であることが確認されている<br>・ファイルやリソースへの機密ラベルの設定も、的確であることが確認されている<br>・諸設定の維持変更を管理するための仕組みも確立している<br>・これらのシステムへの実装の的確性は、この仕組みに沿って組織的な管理の下で徹底してチェックされている<br>・セキュア OS の使用法や使用状況についての見直し状況はクラス A<br>・セキュア OS の使用法や使用状況についての文書化のレベルはクラス A |
| レベル 4 | 組織的に行われたセキュアな OS の使用法の研究にもとづいた使用法が確立しており、その実装も的確であることの追及も行われている。諸設定等の維持管理も組織的な管理下で行われているが、一部に徹底さを欠くところもあり、セキュア OS が期待通りの機能していないところもでることがありうる<br>・専門家の支援も受けた組織的な検討により、使用法はそれぞれの使用場所に対応した最適化が図られているが、まだ改善の余地もある<br>・管理者権限の管理も決定された使用法に沿って、概ね、厳格に行われているが、一部に徹底さを欠くところも見られる<br>・プロセスのパーティションやコンパートメントの設定も、的確であることが確認されているが、一部に徹 |

| | |
|---|---|
| | 底さを欠くところも見られる<br>・ファイルやリソースへの機密ラベルの設定の、的確であることの確認は行われているが、一部に徹底さを欠くところも見られる<br>・諸設定の維持変更を管理するための仕組みも確立しているが、まだ改善する余地もある<br>・これらのシステムへの実装の的確性は、この仕組みに沿って組織的な管理の下でチェックされている、一部に徹底さを欠くところも見られる<br>・セキュア OS の使用法や使用状況についての見直し状況はクラス B 以上<br>・セキュア OS の使用法や使用状況についての文書化のレベルはクラス B 以上 |
| レベル 3 | セキュアな OS は使用されているが、その使用法は担当者に任されている。担当者はセキュアな OS の使用法の研究を行っているが、最適化されているとはいえない。また、その実装もおよびその維持管理も担当チームに任されており、その使用に不手際が入り込む余地がある。<br>・それぞれの使用場所に対応した使用の最適化が図られているが、徹底したものではない<br>・管理者権限の管理も決定された使用法に沿って行われているが、徹底したものではない<br>・プロセスのパーティションやコンパートメントの設定も、概ね、的確である<br>・ファイルやリソースへの機密ラベルの設定の的確性についての組織的なチェックは行われているが、徹底したものではない<br>・大まかではあるが、諸設定の維持変更を管理するための仕組みも示されている<br>・これらのシステムへの実装の的確性は、この仕組みに沿って組織的な管理の下でチェックされているが徹底したものではない<br>・セキュア OS の使用法や使用状況についての見直し状況はクラス C 以上<br>・セキュア OS の使用法や使用状況についての文書化のレベルはクラス C 以上 |
| レベル 2 | (本要求についてはレベル 2 の該当はない) |
| レベル 1 | セキュアな OS の使用についての組織的な管理は行われていない<br>・レベル3の達成条件も満たせない |

(注 1) セキュアな OS の使用法として基準とすべき事項
- ・パーティションあるいはコンパートメントの適切な区分
- ・プロセスに対する適切なパーティション/コンパートメントの指定
- ・ファイルやリソースへの適切な機密ラベルの設定
- ・管理者権限の適切な分割

## Tb1.11 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | アプリケーションに適用するアクセス管理について、完成度の高い基準 (注1) が確立しており、すべてのアプリケーションに対して、この基準に沿ったアクセス管理要件(注2)が的確に指定されている。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に不備が入り込むことは、まず考えられない。<br>・アクセス管理の立場からの完成度の高いアプリケーションのクラス分けが確立している<br>・アプリケーションのクラス別のアクセス管理についての要求レベルを示したアクセス管理基準として完成度の高いものが確立している<br>・個々のアプリケーションにおけるアクセス管理要件の指定についての管理の仕組みが確立している<br>・個々のアプリケーションに対するアクセス要件の指定やそのチェックならびに指定状況についての管理は、定められた仕組みに沿って、徹底して行われ管理されている<br>・アプリケーションにおけるアクセス管理実施基準についての検討のレベルはクラス A<br>・アプリケーションにおけるアクセス管理実施基準の見直しのレベルはクラス A<br>・個々のアプリケーションに対するアクセス管理要件についての見直し状況はクラス A<br>・アプリケーションにおけるアクセス管理実施基準や、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、およびこの管理の仕組み等についての文書化のレベルはクラス A |

| | |
|---|---|
| レベル4 | アプリケーションに適用するアクセス管理について、よく検討された基準（注1）が確立しており、アプリケーションレベルでのアクセス管理が必要となるすべてのアプリケーションに対して、この基準に沿ったアクセス管理要件(注2)が指定されているが、それらの検討に徹底さを欠くところも見られ、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に不備が入り込む余地が、僅かではあるが残されている。<br>・アクセス管理の立場からのアプリケーションのクラス分けがよく検討されている<br>・アプリケーションのクラス別のアクセス管理についての要求レベルを示したアクセス管理基準が確立しているが、まだ改善の余地がある<br>・個々のアプリケーションにおけるアクセス管理要件の指定についての管理の仕組みも確立しているが、まだ改善の余地もある<br>・個々のアプリケーションに対するアクセス要件の指定やそのチェックならびに指定状況についての管理は、定められた仕組みに沿って実施、管理されているが、一部に徹底さを欠くところも見られる<br>・アプリケーションにおけるアクセス管理実施基準についての検討のレベルはクラスB以上<br>・アプリケーションにおけるアクセス管理実施基準の見直しのレベルはクラスB以上<br>・個々のアプリケーションに対するアクセス管理要件についての見直し状況はクラスB以上<br>・アプリケーションにおけるアクセス管理実施基準や、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、およびこの管理の仕組み等についての文書化のレベルはクラスB以上 |
| レベル3 | 大まかではあるが、アプリケーションに適用するアクセス管理についての基準（注1）が示され、アプリケーションレベルでのアクセス管理が必要となるすべてのアプリケーションに対して、この基準に沿ったアクセス管理要件(注2)が概ね適切に指定されている。ただし、レビュー等は徹底したものでなく、妥当性を欠く指定が、見逃されている余地が残されている。<br>・アクセス管理の立場からのアプリケーションのクラス分けが行われている<br>・大まかではあるが、アプリケーションのクラス別のアクセス管理についての要求レベルを示したアクセス管理基準が示されている<br>・大まかではあるが、個々のアプリケーションにおけるアクセス管理要件の指定についての管理の仕組みも作られている<br>・個々のアプリケーションに対するアクセス要件の指定やそのチェックならびに指定状況についての管理は、定められた仕組みに沿って実施、管理されているが、徹底した管理は行われていない<br>・アプリケーションにおけるアクセス管理実施基準についての検討のレベルはクラスB以上<br>・アプリケーションにおけるアクセス管理実施基準の見直しのレベルはクラスB以上<br>・個々のアプリケーションに対するアクセス管理要件についての見直し状況はクラスB以上<br>・アプリケーションにおけるアクセス管理実施基準や、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、およびこの管理の仕組み等についての文書化のレベルはクラスB以上 |
| レベル2 | 組織的に定義されたアクセス管理基準は存在しないが、アプリケーションの設計チーム内に習慣的に形成されている考え方があり、個々のアプリケーションへのアクセス管理要件の指定は、概ね、この考えに沿っているが、特に、管理されていないためばらつきもあり、不備が入り込む余地は少なくない。<br>・アプリケーションの設計関係者間では、アプリケーションレベルで実施すべきアクセス管理についての共通的な考え方は存在<br>・重要なアプリケーションに対するアクセス管理要件の指定は、この考えに沿って行われているが、担当者任せで、特に重要なアプリケーション以外は、特に、指定内容についての組織的なチェックは行われていない。また、検討の対象漏れについてのチェックも行われていない<br>・アプリケーションにおけるアクセス管理実施基準や、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、およびこの管理の仕組み等についての文書化のレベルはクラスC以上 |
| レベル1 | アプリケーションレベルでのアクセス管理についての要求の指定は、すべて担当者任せでほとんど行われていない<br>・レベル2の達成要件も満たしていない |

(注1) アプリケーションにおけるアクセス管理基準として、アプリケーションのクラスごとに指定すべきこと
- ・アクセス管理面から見た当該アプリケーションクラスの特性
- ・アクセス制御の適用レベル（全機能、一部機能）
- ・アクセス要求者の本人性の確認レベル
- ・アクセス要求者の認証のレベル
- ・アクセス権限の管理のレベル
- ・不正なアクセスまたは不審なアクセスへの対処についての原則

・アクセスログの取得範囲の大枠
・アクセスログの分析についての要求

(注2) 個々のアプリケーションに指定すべきアクセス管理におけるアクセス管理基準として、アプリケーションのクラスごとに指定すべきこと
・アクセス制御の適用場面
・アクセス要求者の識別方式
・アクセス要求者の認証方式
・アクセス制御の場面ごとに付与する権限
・不正なアクセスまたは不審なアクセスへの対処
・アクセスログの取得方法（取得の対象とすべきイベント、取得する情報、取得形式等）
・アクセスログの取扱い（保全他）についての具体的な指示
・アクセスログの分析についての具体的な指示（解析のタイミング、解析のポイント、報告要領等）

## Tb1.12 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 個々のアプリケーションソフトへの指定されたアクセス要件の実装、およびアクセス管理に必要な諸情報の確実なシステムへの登録が行われ、その維持管理も徹底していて、アプリケーションレベルでの指定されたアクセス管理に不備が入り込むことは、まず考えられない。<br>・個々のアプリケーションへの指定されたアクセス制御機能やアクセス監視についての要求の組込みは、設計に対するレビューや実装に対するテストは徹底しており、正しい実装が確認されている<br>・各アプリケーションのアクセス制御機能が使用する認証情報やアクセス権限情報のライフサイクルの全過程についての作業やそのチェックおよびそれらの管理の仕組みが確立している<br>・各アプリケーションのアクセス制御機能が使用する認証情報やアクセス権限情報等は、定められた仕組み沿って作成、更新、管理されており、これらについてのチェックも徹底している<br>・これらの情報のシステムへの登録も登録も定められたプロセスに沿って厳格に実施、チェック、管理されている<br>・個々のアプリケーションに組込んでいるアクセス管理機能や、システムの登録されているこれらの機能が用いる情報についての見直し状況はクラスA<br>・個々のアプリケーションへのアクセス管理機能の組込みに関する諸情報についての文書化のレベルはクラスA |
| レベル4 | 個々のアプリケーションソフトへの指定されたアクセス要件の実装、およびアクセス管理に必要な諸情報の確実なシステムへの登録が行われ、その維持管理もよく行われているが、一部に徹底さを欠くところも見られ、アプリケーションレベルでの指定されたアクセス管理に不備が入り込む余地が、僅かではあるが残されている。<br>・個々のアプリケーションへの指定されたアクセス制御機能やアクセス監視についての要求の組込みは、設計に対するレビューや実装に対するテストは比較的厳格で、正しい実装がされていると見てよい<br>・各アプリケーションのアクセス制御機能が使用する認証情報やアクセス権限情報のライフサイクルの全過程についての作業やそのチェックおよびそれらの管理の仕組みも確立しているが、まだ改善の余地もある<br>・各アプリケーションのアクセス制御機能が使用する認証情報やアクセス権限情報等は、定められた仕組み沿って作成、更新、管理されており、これらについてのチェックも比較的厳格に行われているが、一部に徹底さに欠けるところも見られる<br>・これらの情報のシステムへの登録も登録も定められたプロセスに沿って概ね厳格に、実施、チェック、管理されている<br>・個々のアプリケーションに組込んでいるアクセス管理機能や、システムの登録されているこれらの機能が用いる情報についての見直し状況はクラスB以上<br>・個々のアプリケーションへのアクセス管理機能の組込みに関する諸情報についての文書化のレベル |

| | |
|---|---|
| | はクラスＢ以上 |
| レベル3 | 個々のアプリケーションソフトへの指定されたアクセス要件の実装、およびアクセス管理に必要な諸情報の確実なシステムへの登録が行われ、その維持管理も大まかなものではあるが定められたルールに沿って行われているが、徹底したものではない。アプリケーションレベルでの指定されたアクセス管理に不備が入り込む可能性は残されている。<br>・個々のアプリケーションへの指定されたアクセス制御機能やアクセス監視についての要求の組込みは、設計に対するレビューや実装に対するテストは行われているが、そう厳格なものではない。また、それらについての管理も行われているが、徹底したものではない<br>・各アプリケーションのアクセス制御機能が使用する認証情報やアクセス権限情報のライフサイクルの全過程についての作業やそのチェックおよびそれらの管理に方法も、大まかではあるが示されている<br>・各アプリケーションのアクセス制御機能が使用する認証情報やアクセス権限情報等は、定められた仕組み沿って作成、更新、管理されており、これらについてのチェックも行われているが、厳格なものではない<br>・これらの情報のシステムへの登録も登録も、概ね、定められたプロセスに沿って、実施、チェック、管理されている<br>・個々のアプリケーションに組込んでいるアクセス管理機能や、システムの登録されているこれらの機能が用いる情報についての見直し状況はクラスＢ以上<br>・個々のアプリケーションへのアクセス管理機能の組込みに関する諸情報についての文書化のレベルはクラスＢ以上 |
| レベル2 | 個々のアプリケーションソフトへの指定されたアクセス要件の実装、およびアクセス管理に必要な諸情報の確実なシステムへの登録は、担当者レベルで行われているが、担当者は習慣的に形成された手順や管理の方法に沿って、その信頼性の確保にある程度努力している。組織的な管理が十分でないため、アプリケーションレベルでの指定されたアクセス管理に不備が入り込むことも考えられる。<br>・担当者レベルでは、個々のアプリケーションに指定されたアクセス制御機能やアクセス監視についての設計に対するレビューや実装に対するテストは行われている<br>・担当チームには習慣的に形成されたものであるが、各アプリケーションのアクセス制御機能が使用する認証情報やアクセス権限情報のライフサイクルの全過程についての作業やそのチェックおよびそれらの管理に方法が存在している<br>・各アプリケーションのアクセス制御機能が使用する認証情報やアクセス権限情報等は、この習慣的な手順に沿って作成、更新、管理されており、これらについてのチェックも行われているが、組織的に管理されたものとは言い難い<br>・これらの情報のシステムへの登録も登録も、概ね、この習慣的な手順に沿って、実施、チェック、管理されているが、組織的に管理されているとは言い難い<br>・個々のアプリケーションに組込んでいるアクセス管理機能や、システムの登録されているこれらの機能が用いる情報についての見直し状況はクラスＣ以上<br>・個々のアプリケーションへのアクセス管理機能の組込みに関する諸情報についての文書化のレベルはクラスＣ以上 |
| レベル1 | 個々のアプリケーションソフトへの指定されたアクセス要件の実装、およびアクセス管理に必要な諸情報の確実なシステムへの登録は、すべて担当者に任されている。<br>・レベル2の達成要件も満たしていない |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 必要なセキュリティホール対策が迅速かつ安全に行えるようにするための完成度の高い管理スキームが確立しており、セキュリティホール対策がこの仕組み沿っ厳格に行われれば、必要なセキュリティホール対策の実施に不手際が生じることは、まず考えられない。<br>・セキュリティホール対策についての責任体制が確立されている(注 1)<br>・セキュリティホール対策について専門的なスキルを持つメンバーが存在し、外部の専門家の支援も、何時でも受けられるようになっている<br>・現時点で最新のツールを駆使し、セキュリティホール対策を実施している<br>・セキュリティホールの発見や対策管理を行う上で自動化できるところはほとんど自動化している<br>・セキュリティホール対策の実施の管理単位が確立している<br>・脆弱性情報の取得ならびに取得脆弱性情報に対する対策の要否や対策方法の決定に至るまでのプロセスが確立している<br>・完成度の高い脆弱性情報の評価基準（注2）が確立している<br>・対策を実施すべきと判断された脆弱性に対する対策の計画作成要領（注 3）が確立している<br>・セキュリティパッチの入手要領が確立しておりマニュアル化されている<br>・セキュリティパッチの準備から実施後の検証までのプロセスについて完成度の高い実施要領(注4)が確立しており、マニュアル化されている<br>・入手した脆弱性情報やセキュリティパッチや対策にかかわる活動に関する記録の保管管理要領の確立している<br>・これらのセキュリティホール対策にかかわる管理スキームについての検討のレベルはクラス A<br>・このセキュリティホール対策についての管理スキームは関係者に徹底されている<br>・このセキュリティホール対策についての管理スキームについての見直しのレベルはクラス A<br>・このセキュリティホール対策についての管理スキームについての文書化のレベルはクラス A |
| レベル4 | 組織的な検討の下、必要なセキュリティホール対策が迅速かつ安全に行えるようにするための管理スキームが策定されている。検討すべき事項は概ね網羅されてはいるが、細部については、まだ、改善の余地も残されている。<br>・セキュリティホール対策についての責任体制が確立されている<br>・セキュリティホール対策について専門的なスキルを持つメンバーが存在し、外部の専門家の支援も、受けられるようになっている<br>・最先端のツールの採用を図り、概ね採用してセキュリティホール対策を実施している<br>・セキュリティホールの発見や対策管理を行う上で、可能な範囲については自動化に努めている<br>・セキュリティホール対策の実施の管理単位が確立している<br>・脆弱性情報の取得ならびに取得脆弱性情報に対する対策の要否や対策方法の決定に至るまでのプロセスが確立しているが、まだ改善する余地もある<br>・脆弱性情報に対する相当にレベルの高い評価基準（注 2）が確立しているが、まだ改善の余地もある<br>・対策を実施すべきと判断された脆弱性に対する対策の計画作成要領（注 3）は示されている<br>・セキュリティパッチの入手要領が確立しておりマニュアル化されている<br>・セキュリティパッチの準備から実施後の検証までのプロセスについて実施要領(注4)が纏められ、マニュアル化されているが、まだ改善の余地もある<br>・入手した脆弱性情報やセキュリティパッチや対策にかかわる活動に関する記録の保管管理要領の確立<br>・これらのセキュリティホール対策にかかわる管理スキームについての検討のレベルはクラス B 以上<br>・このセキュリティホール対策についての管理スキームは関係者に、概ね徹底されている<br>・このセキュリティホール対策についての管理スキームについての見直しのレベルはクラス B 以上<br>・このセキュリティホール対策についての管理スキームについての文書化のレベルはクラス B 以上 |
| レベル3 | 組織的な検討の下、必要なセキュリティホール対策が迅速かつ安全に行えるようにするための管理スキームが、大まかではあるが示されている。検討すべき事項は概ね網羅されてはいるが、基本的なことが中心で、細部についての多くは、対策現場に任されている。 |

| | |
|---|---|
| | ･セキュリティホール対策の計画、実施、管理を担当するチームの編成、責任者の指名、緊急時の対応も決められているが、十分とは言えないところもある<br>･セキュリティホール対策の実施で最低限自動化すべきところには、自動化が行われている<br>･セキュリティホール対策の実施の管理単位は分けられている<br>･大まかではあるが脆弱性情報の取得ならびに取得した脆弱性情報に対する対策の要否の判断や対策方法の検討のプロセスや各ステップにおけるチェックポイントは示されている<br>･大まかではあるが入手した脆弱性情報に対する評価基準が示されている<br>･対策を実施すべきと判断された脆弱性に対する対策の実施計画の作成方法が示されている<br>･おおまかではあるが、セキュリティパッチの入手要領は示されている<br>･セキュリティパッチの準備から実施後の検証までの基本的なプロセスと、各ステップにおけるチェックポイントは示されている<br>･おおまかではあるが、入手した脆弱性情報やセキュリティパッチや対策にかかわる活動についての記録の保管管理の方法が示されている<br>･これらのセキュリティホール本対の管理スキームについての検討のレベルはクラス B 以上<br>･このセキュリティホール対策の管理スキームについての見直し状況はクラス B 以上<br>･このセキュリティホール対策の管理スキームについての文書化のレベルはクラス B 以上 |
| レベル 2 | 必要なセキュリティホール対策が迅速かつ安全に行えるようにするための組織的に検討された管理スキームは作られてはいないが、セキュリティホール対策の担者間で習慣的に機能している管理の仕組みは存在している。<br>･担当者間で決めたものではあるが、セキュリティホール対策の実施の管理単位は存在<br>･脆弱性情報の取得についての担当チーム内での習慣的な手法は存在<br>･収集した脆弱性情報の分析･評価についての担当チーム内での考え方は存在<br>･対策を実施すべきと判断された脆弱性に対する対策の実施内容や実施計画への展開についての対策現場レベルでの考え方は形成されている<br>･対策を実施すべきと判断された脆弱性に対する対策の実施内容や実施計画への展開についての対策現場レベルでの考え方は形成されている<br>･セキュリティパッチの準備から実施後の検証までのプロセスについて、対策現場レベルで習慣的に形成された手順が存在し、また、関係者はそれぞれのステップでのチェックポイントもある程度承知している<br>･セキュリティパッチの入手についての担当チーム内での習慣的な手法は存在<br>･このセキュリティホール対策の管理スキームについての文書化のレベルはクラス C 以上 |
| レベル 1 | 必要なセキュリティホール対策が迅速かつ安全に行えるようにするための管理スキームは存在しない。セキュリティホール対策は、担当チームにすべて任されている。<br>･レベル 2 の達成条件も満たしていない |

(注 1)セキュリティホール対策の推進体制の確立に必要とされること
- ･セキュリティホール対策実施の責任者の指名とそのタスクの明確化
- ･セキュリティホール対策の計画、実施、管理を担当するチームの設置と、そのタスクの明確化
- ･システムの管理者やクライアント PC 利用者のタスクの明確化
- ･責任者からクライアント PC の利用者に至るまでの、セキュリティホール対策にかかわる者における自己の責務の周知

(注 2) 脆弱性情報に対する評価基準として示されるべきこと
- ･対策の要否についての判断基準
- ･対策対象システムの範囲についての判断基準
- ･対策の緊急性についての判断基準
- ･セキュリティパッチ実施までの暫定対策の要否とその緊急性についての判断基準

(注 3) セキュリティホール対策の実施計画作成要領として示されるべきこと
- ･セキュリティホール対策実施計画書の記載事項、様式
- ･作成及び承認プロセス
- ･計画のチェックポイント

(注 4) セキュリティホール対策の実施要領として示されるべきこと
- ･対象となる脆弱性とシステムへの影響

・対策対象システムと対象システムごとに実施する対策内容
・対策時期
・準備から実施、事後処理までの作業の流れ（関係者との連絡や調整を含む）
・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方法
・システムの復旧方法

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 脆弱性情報の入手、および入手脆弱性情報に対する評価、対策実施の要否の検討から対策計画の作成までの展開は、確立されたセキュリティホール対策の管理スキームに沿って、適切に行われており、必要なセキュリティホール対策の見逃しや、実施計画上の不備が入り込むことは、まず考えられない。<br>・脆弱性情報の入手から対策実施への展開までの諸作業は、レベル4以上の管理スキームの示すところに沿って行われている<br>・脆弱性情報は、複数の情報源から毎日入手している。緊急情報については365日24時間何時でも関係者に遅滞なく伝わることになっている<br>・脆弱性情報は、専門メンバーで分析評価されている、また、外部の専門家の支援がいつでも得られるようになっている<br>・脆弱性情報に対する対策の要否や対策方法および対策実施計画は、組織的なレビューの上で決定されている<br>・脆弱性情報の入手から対策の要否の判断ならびに対策計画の確定までのタイムラグは、緊急を要するものは1日以内、その他のものでも3日以内<br>・重要な機器に対しては、最低1ヶ月に一度、その他の機器に対しても、2 ヶ月以下のサイクルで定期的な対策を実施している<br>・入手した脆弱性情報、その評価分析結果、対策の要否および対策実施計画の検討状況、および対策実施計画についての文書化のレベルはクラスA |
| レベル4 | 脆弱性情報の入手、および入手脆弱性情報に対する評価、対策実施の要否の検討から対策計画の作成までの展開は、確立されたセキュリティホール対策の管理スキームに沿って行われているが、徹底さを欠くところも見られる。必要なセキュリティホール対策の見逃しや、実施計画上の不備が入り込む隙が、僅かではあるが残されている。<br>・脆弱性情報の入手から対策実施への展開までの諸作業は、レベル4以上の管理スキームの示すところに沿って行われているが、厳格さに欠けるところも見られる<br>・脆弱性情報は、複数の情報源から毎日入手している。緊急情報については365日24時間何時でも関係者に迅速に伝わることになっている<br>・脆弱性情報は、専門メンバーで分析評価されている、また、外部の専門家の支援がいつでも得られるようになっている<br>・脆弱性情報に対する対策の要否や対策方法および対策実施計画は、組織的なレビューの上で決定されているが、レビューに徹底さを欠くことも見られる<br>・脆弱性情報の入手から対策の要否の判断ならびに対策計画の確定までのタイムラグは、緊急を要するものは1日以内、その他のものでも大体1週間以内<br>・重要な機器に対しては、最低1ヶ月に一度、その他の機器に対しても、2 ヶ月以下のサイクルで定期的な対策を実施している<br>・入手した脆弱性情報、その評価分析結果、対策の要否および対策実施計画の検討状況、および対策実施計画についての文書化のレベルはクラスB以上 |
| レベル3 | 脆弱性情報の入手、および入手脆弱性情報に対する評価、対策実施の要否の検討から対策計画の作成までの展開は、大まかに示されたセキュリティホール対策の管理スキームに沿って行われており、組織的な取組みはできている。しかし、十分に組織的な管理の下で行われているとは言い難く、また、専門メンバーの支援も少ないことから、必要なセキュリティホール対策の見逃しや、実施計画上の不備 |

| | |
|---|---|
| | が入り込む余地が残されている。<br>・脆弱性情報の入手から対策実施への展開までの諸作業は、概ねレベル3クラスの管理スキームの示すところに沿って行われているが、細部は担当者の知見や見識やスキルに依存している<br>・脆弱性情報は、ほぼ、毎日入手している。緊急情報については、遅くとも翌営業日までには関係者に伝わることになっている<br>・脆弱性情報の分析評価は担当チームに任されている、また、外部の専門家の助言も受けることもできるようにはなっている<br>・脆弱性情報に対する対策の要否や対策方法および対策実施計画のレビューは、担当チーム内に止まっており、あまり厳格なものでなく、標準的なチェックポイントをチェックしている程度<br>・脆弱性情報の入手から対策の要否の判断ならびに対策計画の確定までのタイムラグは、問題が生じた場合や特に緊急と判断された場合を除き、ほぼ１ヶ月以内<br>・重要な機器に対しては、最低2ヶ月に一度、その他の機器に対しても、3 ヶ月以下のサイクルで定期的な対策を実施している<br>・入手した脆弱性情報、その評価分析結果、対策の要否および対策実施計画の検討状況、および対策実施計画についての文書化のレベルはクラスＣ以上 |
| レベル2 | 脆弱性情報の入手、および入手脆弱性情報に対する評価、対策実施の要否の検討から対策計画の作成までの展開は、担当チームの知見やスキルに全面的に依存している。担当者は習慣的な手順に沿って、最低限必要な対応ができるように努力してはいるが、専門的なスキルの不足や、組織的な管理がなされていないことから、必要なセキュリティホール対策の見逃しや、実施計画上の不備が入り込む可能性が、少なからずある。<br>・脆弱性情報の入手から対策実施への展開までの諸作業は、概ね、担当チーム内に形成された習慣に沿って行われている、入手した脆弱性情報の評価や対策の実施計画の作成等は担当者の知見や見識やスキルに依存している<br>・脆弱性情報は、概ね、毎日入手してはいるが、緊急情報を除いては、その評価や必要な対策の検討は、優先扱いにはなってなく遅れがち<br>・脆弱性情報の入手から必要な対策の実施計画の作成までのタイムラグは、問題が生じた場合や特に緊急と判断された場合を除き、１ヶ月以上になることもある<br>・重要な機器に対しては、最低3ヶ月に一度は定期的な対策を実施している<br>・入手した脆弱性情報、その評価分析結果、対策の要否および対策実施計画の検討状況、および対策実施計画についての文書化のレベルはクラスＣ以上 |
| レベル1 | 脆弱性情報の入手から必要な対策の実施計画の作成は、すべて担当者任せで、組織的な取組みは見られない<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 対策実施計画にもとづく対策が、確立した対策実施要領に沿って徹底した管理の下で、慎重に確実に行われており、対策の実施に不手際が生じることは、まず考えられない。<br>・対策実施に際しては、十分にレビューされた対策実施計画が作成されている<br>・事前準備から対策後の確認までのすべてのプロセスは、対策計画と個々のステップについての実施要領に沿って行われている<br>・対策の個々について、必要な環境の確認やテストは徹底して行われており、この事前準備は厳格に管理されている<br>・実施結果は診断ツールにより完了が確認されている<br>・指示されたセキュリティホール対策の実施にかかわる文書化のレベルはクラスＡ |
| | 対策実施計画にもとづく対策が、確立した対策実施要領に沿って徹底した管理の下で、慎重に行われ |

| | |
|---|---|
| レベル4 | ているが、一部に徹底さを欠くところも見られ、対策の実施に不手際が生じる隙が、僅かではあるが残されている。<br>・対策実施に際しては、十分にレビューされた対策実施計画が作成されている<br>・事前準備から対策後の確認までのすべての工程は、対策実施要領に沿って行われることになっているが、一部に徹底さを欠くところもある。<br>・対策の個々について、必要な環境の確認やテストは、相当に丁寧に行われており、この事前準備の管理も相当に厳格であるが、一部に徹底さを欠くところもある<br>・実施結果は診断ツールにより完了が確認されている<br>・指示されたセキュリティホール対策の実施にかかわる文書化のレベルはクラスB以上 |
| レベル3 | 対策実施計画にもとづく対策が、対策実施要領に沿って、担当部門内ではるが組織的な管理の下でおおむね適切に行われているが、事前の準備や実施にあたって注意すべき点についての対応等に、十分とは言えないところもある。対策の実施に不手際が生じる余地が残されている。<br>・対策実施に際しては、担当部門内でレビューされた対策実施計画が作成されている<br>・事前準備から対策後の確認までのすべての工程は、対策実施要領に沿って行われることになっているが、細部は対策チームに任されているため、不適切なところも入り込む余地が少なくない<br>・対策の個々について、必要な環境の確認やテストも行われており、この事前準備の管理も管理部門内では行われているが、十分なものとは言い難い<br>・指示されたセキュリティホール対策の実施にかかわる文書化のレベルはクラスC以上 |
| レベル2 | 対策の実施は、担当レベルで作成された計画に沿って行われているが、担当チームは、事前の準備や実施にあたって注意すべき点については承知しており、安全な実施を心がけており、ある程度は信頼できる。しかし、組織的な管理は行われているとは言えない。対策の実施に不手際が生じる可能性が、少なからずある。<br>・対策実施に際しては、担当チームで対策実施計画を作成している<br>・事前準備から対策後の確認までのすべての工程は、経験にもとづいて形成された習慣的な手法に沿って行われている。これらは、すべて対策チームに任されているため、不適切なところも入り込む余地が少なくない<br>・対策の個々について、最低限の環境の確認やテスト他の事前準備は、十分とは言えないものの行われている<br>・指示されたセキュリティホール対策の実施にかかわる文書化のレベルはクラC以上 |
| レベル1 | セキュリティホール対策の実施は、すべて担当者任せで、組織的な取組みは行われていないに等しい<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | セキュリティホール対策の管理スキームに沿った、対策の実施状況についての管理が厳格に行われており、その状況については何時でも正確に把握できるようになっている。<br>・セキュリティホール対策の実施状況(注 1)についての把握やその記録の保管管理の仕組みが確立している<br>・入手した脆弱性情報、それらに対する評価の実施経過や評価結果は、すべて組織的に保管管理されており、何時でも検索が可能<br>・入手したパッチデータは、すべて組織的に保管管理されている<br>・暫定措置も含む対策の実施計画や実施の経緯等についての記録も、すべて組織的に保管管理されており、何時でも検索が可能<br>・ツールの使用等を適切に行い、すべての対象機器について、対策済み、暫定措置実施中、あるいは対策待ちの脆弱性の把握が完全にできている<br>・セキュリティホール対策の実施状況の把握状況や関係する記録の保管管理の情況についてのチェッ |

| | |
|---|---|
| | クが頻繁に行われ、必要な是正阻止がとられている |
| レベル4 | セキュリティホール対策の管理スキームに沿った、対策の実施状況についての管理が行われており、その状況については何時でも正確に把握できるようになっているが、一部に徹底さを欠くところも見られ、保管すべき記録の保管管理は万全とは言えないところがある。<br>・セキュリティホール対策の実施状況（注 1）についての把握や記録の保管管理の仕組みは確立しているが、まだ、改善する余地もある<br>・入手した脆弱性情報、それらに対する評価の実施経緯および評価結果は、組織的に保管管理されており、何時でも検索が可能となっているが、徹底を欠くところもある<br>・入手したパッチデータは、ほとんど組織的に管理保管されている<br>・暫定措置も含む対策の実施計画や実施の経緯等についての記録も、組織的に保管管理されており、何時でも検索が可能であるが、一部に徹底さを欠くところもある<br>・ツールの使用等を適切に行い、すべての対象機器について、対策済み、暫定措置実施中、あるいは対策待ちの脆弱性の把握は、概ね十分にできている<br>・定期的にセキュリティホール対策の実施状況の把握状況や関係する記録の保管管理の状況についてのチェックが行われ、必要な是正阻止がとられているが、徹底したものではない |
| レベル3 | 担当部門内では、セキュリティホール対策の管理スキームに沿った、対策の実施状況についての管理が行われており、過去の対策の実施状況については、概ね把握できるようになっているが、十分とは言えないところもある。<br>・セキュリティホール対策の実施状況についての記録の保管管理の仕組みは示されているが、大まかなもので、細部は担当チームの判断に任されている<br>・入手した脆弱性情報、それらに対する評価の実施経緯や評価結果は、担当部門の判断により保管管理されている<br>・入手したパッチデータの保管管理は行われているが、その実施は担当チームに任されている<br>・暫定措置も含む対策の実施計画や実施の経緯等についての記録も作られており、おおよそのことは把握できているが、組織的に管理はされてなく、その正確性は十分なものとは言えない<br>・各機器における対策済み、暫定措置実施中、あるいは対策待ちの脆弱性の把握には努めてはいるが、その正確性や把握が出来ている対象機器の範囲等から、十分とは言えないところがある |
| レベル2 | セキュリティホール対策の実施状況についての管理は、担当チームが自主的に行ってはいるが、組織的に管理されているとは言い難い。ある程度の記録は残されているが、問題が生じた場合、必要な情報が得られるかどうかは疑問。<br>・セキュリティホール対策の実施状況についての記録の保管管理は、担当チームの習慣的なルールに沿って行われている<br>・入手脆弱性情報およびそれらに対する評価の実施状況および評価結果についての記録の保管や、入手したパッチデータの管理保管は、担当チームの意識に依存<br>・パッチ未適用の脆弱性のリストは、パッチに変わり適用している暫定措置の詳細についての信頼すべき記録は、作られていない |
| レベル1 | セキュリティホール対策の実施状況の管理についての組織的な取組みはないに等しい<br>・レベル2の達成要件も満たしていない |

(注 1) セキュリティホール対策の実施状況として把握すべきこと
- ・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
- ・未実施の場合の理由、および実施予定
- ・セキュリティパッチにか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記録

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | ウイルス対策が適切に計画され機能するようにするための完成度の高い管理の仕組みが確立しており、ウイルス対策がこの仕組みに沿って厳格に行われれば、計画したウイルス対策の実施に不手際が生じることは、まず考えられない。<br>・ウイルス対策についての責任体制が確立されている(注 1)<br>・ウイルス対策について専門的なスキルを持つメンバーが存在し、外部の専門家の支援を何時でも受けられるようになっている<br>・現時点で最新のツールを駆使し、ウイルス対策の実施で自動化できるところは自動化している<br>・システム全体の中で、ウイルス対策実施の管理単位が分けられている<br>・ウイルス情報の取得ならびに取得したウイルスに関する情報に対する対策の要否や対策方法の決定に至るまでのプロセスが確立している<br>・配置したウイルス対策ツールのすべてについてウイルス定義ファイルの更新状況等の使用状況が完全に把握できる仕組みが作られている<br>・緊急時におけるシステムの利用者も含む関係者との迅速で適切な連携がいつでもできる<br>・ウイルス感染が検知されたり、感染の恐れが発生した場合に必要となる措置が迅速に行えるようにするための仕組み(注2)が確立している<br>・入手したウイルスに関する情報やウイルス対策にかかわる活動に関する記録の保管管理要領も確立している<br>・この管理スキームについての検討のレベルはクラス A<br>・この管理スキームは関係者に徹底されている<br>・この管理スキームについての見直しのレベルはクラス A<br>・この管理スキームについての文書化のレベルはクラス A |
| レベル4 | 組織的な検討の下、ウイルス対策が適切に計画され機能するようにするための管理スキームが策定されている。検討すべき事項は概ね網羅されてはいるが、細部については、まだ、改善の余地も残されている。<br>・ウイルス対策についての責任体制が確立されている<br>・ウイルス対策について専門的なスキルを持つメンバーが存在し、外部の専門家の支援も、受けられるようになっている<br>・現時点で最新のツールを駆使し、ウイルス対策の実施で自動化できるところは自動化している<br>・システム全体の中で、ウイルス対策実施の管理単位が確立している<br>・ウイルス情報の取得ならびに取得したウイルスに関する情報に対する対策の要否や対策方法の決定に至るまでのプロセスが確立しているが、まだ改善する余地もある<br>・配置したウイルス対策ツールのすべてについてウイルス定義ファイルの更新状況等の使用状況が完全に把握できる仕組みが作られているが、まだ改善の余地もある<br>・緊急時におけるシステムの利用者も含む関係者との迅速で適切な連携がいつでもできる<br>・ウイルス感染が検知されたり、感染の恐れが発生した場合に必要となる措置が迅速に行えるようにするための仕組み(注2)が確立しているが、まだ改善の余地もある<br>・入手したウイルスに関する情報やウイルス対策にかかわる活動に関する記録の保管管理要領の確立しているが、まだ改善の余地もある<br>・この管理スキームについての検討のレベルはクラス B 以上<br>・この管理スキームは関係者に、概ね徹底されている<br>・この管理スキームについての見直しのレベルはクラス B 以上<br>・この管理スキームについての文書化のレベルはクラス B 以上 |
| レベル3 | 大まかではあるが、計画したウイルス対策が適切に機能するようにするための管理スキームが示されている。検討すべき事項は概ね網羅されてはいるが、基本的なことが中心できめ個細かさに欠け、細部についての多くは、対策現場に任されている。<br>・ウイルス対策の計画、実施、管理を担当するチームが編成され、責任者も指名され、緊急時の対応も決められているが、十分とは言えないところもある |

| | |
|---|---|
| | ・ウイルス対策の実施でツールの使用等で自動化できるところは、概ね、自動化が行われている<br>・ウイルス対策実施の管理単位は分けられている<br>・大まかではあるがウイルスに関する情報の収集ならびに取得したウイルス情報に対する対策の要否の判断についてのチェックポイントは示されている<br>・大まかではあるが、配置したウイルス対策ツールのウイルス定義ファイルの更新状況等を把握するための仕組みは存在している<br>・大まかではあるが、ウイルス感染が検知されたり、感染の恐れが発生した場合に必要となる措置が迅速に行えるようにするための仕組みは示されている<br>・大まかではあるが、入手した脆弱性情報やウイルス対策にかかわる活動についての記録の保管管理の方法が示されている<br>・この管理スキームについての検討のレベルはクラス B 以上<br>・この管理スキームについての見直し状況はクラス B 以上<br>・この管理スキームについての文書化のレベルはクラス B 以上 |
| レベル 2 | 組織的に検討されたウイルス対策が適切に機能するようにするための管理スキームは作られてはいないが、ウイルス対策の担当者間で習慣的に形成された管理の方法が存在している。<br>・ウイルス対策ツールの配置状況や、配置した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状況等の把握について、チーム内に習慣的に形成された方法が存在する<br>・担当チームには、ウイルス感染が検知されたり、感染の恐れが発生した場合に必要となる措置の実施についての考え方および実行についての方法が形成されている<br>・このセキュリティホール対策の管理スキームについての文書化のレベルはクラス C 以上 |
| レベル 1 | ウイルス対策が適切に行えるようにするための管理スキームは存在しない。ウイルス対策は、担当チームにすべて任されている。<br>・レベル 2 の達成条件も満たしていない |

(注 1) ウイルス対策の推進体制の確立に必要とされること
- ・ウイルス対策実施の責任者の指名とそのタスクの明確化
- ・ウイルス対策の計画、実施、管理を担当するチームの設置と、そのタスクの明確化
- ・システムの管理者やクライアント PC 利用者のタスクの明確化
- ・責任者からクライアント PC の利用者に至るまでの、ウイルス対策にかかわる者における自己の責務の周知

(注2) ウイルス感染発見時や感染の恐れが発生した場合に必要となる措置を迅速に行えるようにするための仕組み
- ・対応体制と関係者のタスク
- ・想定される即応処置とその実施方法その実施の確認方法
- ・関係者への連絡方法
- ・本格的な対策検討への展開方法

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | 使用するウイルス対策ソフトの選択やその配置、ウイルス定義ファイルのメンテナンスの方法、検疫システムの導入等の技術面で、現時点では最も強力と見られる組み立てが採用されている。また、その使用法も最適化が徹底していて、その実装確認も徹底しており、これらに不備が見逃されることは、まず考えられない。<br>・ウイルス対策ツールが、すべての侵入経路に配置されている<br>・外部ネットワークとの境界には、2 社のウイルス対策ソフトを配置しダブルチェックを行っている<br>・ウイルス対策ソフトだけでなく、IDC/IPS やファイアウオール等ネットワーク制御機器においてもウイルス対策を実施している<br>・ゲートウェイ型に加え、サーバやクライアントのすべてにウイルス対策ソフトを配置している<br>・検疫システムも導入している |

| | |
|---|---|
| | ・ウイルス定義ファイルのメンテナンスは、完全に自動化されており、随時最新のウイルス定義ファイルに更新されるシステムになっている<br>・各ウイルス対策ソフトの導入時や変更時における機能テストは徹底しており、期待通り機能することが確認されている<br>・使用するウイルス対策ソフトはそれぞれに最適化のためのカスタマイズが追及されている<br>・ウイルス対策ツールの選択や配置についての検討のレベルはクラス A<br>・ウイルス対策ツールの選択や配置についての見直し状況はクラス A<br>・ウイルス対策ツールの選択や配置についての文書化のレベルはクラス A |
| レベル 4 | 使用するウイルス対策ソフトの選択やその配置、パターンファイルのメンテナンスの方法、検疫システムの導入等の技術および運用の両面で、レベル 5 に示すように最強とは言えないが、現時点では平均以上と見られるウイルス対策が講じられている。また、その使用法の最適化やその実装確認の追及も行われて、一部に徹底さを欠くところも見られる。<br>・ウイルス対策ツールが、すべての侵入経路に配置されている<br>・ウイルス対策ソフトだけでなく、IDC/IPS やファイアウォール等ネットワーク制御機器においてもウイルス対策を実施している<br>・ゲートウェイ型に加え、サーバやクライアントのすべてにウイルス対策ソフトを配置している<br>・検疫システムも導入している<br>・ウイルス定義ファイルのメンテナンスは、完全に自動化されており、随時最新のウイルス定義ファイルに更新されるシステムになっている<br>・使用するウイルス対策ソフトはそれぞれに最適化のためのカスタマイズが追求されている<br>・各ウイルス対策ソフトの導入時や変更時における機能テストは徹底しており、期待通り機能することが確認されている<br>・ウイルス対策ツールの選択や配置やその使用法についての検討のレベルはクラス B 以上<br>・ウイルス対策ツールの選択や配置やその使用法についての見直し状況はクラス B 以上<br>・ウイルス対策ツールの選択や配置やその使用法についての文書化のレベルはクラス B 以上 |
| レベル 3 | 使用するウイルス対策ソフトの選択やその配置、パターンファイルのメンテナンスの方法、検疫システムの導入等の技術および運用の両面において、平均的な手段が、使われている。また、その使用法の最適化やその実装確認の検討も行われているが徹底したものではない。<br>概ね、適切に行われている。<br>・ウイルス対策ツールが、すべての侵入経路に配置されている<br>・ウイルス対策ソフトだけでなく、ファイアウォール等ネットワーク制御機器においてもウイルス対策を実施している<br>・ゲートウェイ型に加え、サーバやクライアントのすべてにウイルス対策ソフトを配置している<br>・ウイルス定義ファイルのメンテナンスや対策状況の管理ツールの導入も行われている。ウイルス定義ファイルのメンテナンスは、スケジュールによって最新のウイルス定義ファイルに更新されるシステムになっている<br>・使用するウイルス対策ソフトに対し、最低限のカスタマイズは行われている<br>・ウイルス対策ツールの導入時や変更時の機能テストは行われているが、十分手は言えない<br>・ウイルス対策ツールの選択や配置やその使用法についての検討のレベルはクラス B 以上<br>・ウイルス対策ツールの選択や配置やその使用法についての見直し状況はクラス B 以上<br>・ウイルス対策ツールの選択や配置やその使用法についての文書化のレベルはクラス B 以上 |
| レベル 2 | 使用するウイルス対策ソフトの選択やその配置、パターンファイルのメンテナンスの方法、検疫システムの導入等は、担当チームに任されている。これらの選択はもっとも簡単にできる最低限のレベルに止まっている。また、その使用法は、ほとんどデフォルトレベルで、最適化等は余り検討されていない。<br>・ウイルス対策ソフトは、ゲートウェイ型またはクライアント型のウイルス対策ソフトのどちらかに依存<br>・ウイルス定義ファイルのメンテナンスは、スケジュールによって最新のウイルス定義ファイルに更新されるシステムになっている<br>・ウイルス対策ツールの選択や配置やそれらの使用法についての検討のレベルはクラス C 以上<br>・ウイルス対策ツールの選択や配置やそれらの使用法についての見直し状況はクラス C 以上<br>・ウイルス対策ツールの選択や配置やそれらの使用法についての文書化のレベルはクラ C 以上 |
| レベル 1 | 使用するウイルス対策ソフトの選択やその配置、パターンファイルのメンテナンスの方法、検疫システムの導入等は、ベンダーの提案をそのまま採用しており、自組織での検討はほとんど行われていない。<br>・ウイルス対策ソフトは、ゲートウェイ型のウイルス対策ソフトまたは、サーバやクライアント PC に組込みのパーソナルファイアウォールに依存 |

| 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | ウイルス対策担当部署に求められていることが細部に渡り示されており、関係者へのそれらの周知や、それらの実践を管理するための仕組みも確立しており、ウイルス対策がウイルス担当部署の作業に依存していることの実践も厳格に管理されており、この点で不手際が生じることは、まず考えられない。<br>・ウイルス対策チームが行わなくてはならないこと（注1）と、その実施方法がきめられ、マニュアル化されている<br>・ベンダーから緊急対策が必要なウイルス定義ファイルがリリースされた場合、ゲートウェイ型の装置で15分以内、ファイルサーバやアプリケーションサーバで60分以内、クライアントで12時間以内にすべての更新が完了しており、その確認も徹底している<br>・配置しているすべてのウイルス対策ツールにおけるパターンファイルの更新状況は、週に1回以上はチェックされており、問題点は遅滞なく是正されている<br>・ウイルス対策ソフトのメンテナンスやトラブルシュートが、適切に行われている<br>・緊急点検が必要となった場合、ウイルス対策ツールを配置したすべての機器におけるウイルスチェックが遅滞なく行われるようになっている<br>・システムの利用者がウイルス対策に関し行わねばならないこと（注2）が示され、システムの利用者に徹底されている<br>・システムの利用者は、ウイルス対策に関し実施すべきことが生じた場合、何時でも適切な対応ができるようになっている<br>・ウイルス対策を担当する者のすべてに、ウイルス対策に関して日常的に行わなければならないことは徹底されている<br>・ウイルス対策の運用についての要求事項の実践状況は組織的に管理されている<br>・ウイルス対策の運用に関する文書化のレベルはクラスA |
| レベル4 | ウイルス対策に関してシステムの運用に求められていることが細部に渡り示されており、これらの実践を確実にするための仕組みも確立しており、この仕組みの下、要求の確実な厳格な実践が図られており、そのチェックや指導も行われているが、一部に徹底さにかけるところもあり、この点で不手際を生じさせる隙が、僅かではあるが残されている。<br>・ウイルス対策チームが行わなくてはならないこと（注1）と、その実施方法がきめられ、マニュアル化されている<br>・配置している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状況は、週に1回以上はチェックされており、問題点は遅滞なく是正されている<br>・ベンダーから緊急対策が必要なウイルス定義ファイルがリリースされた場合、ゲートウェイ対策装置で15分以内、ファイルサーバやアプリケーションサーバで60分以内、クライアントで24時間以内にすべての更新が完了しているが、徹底さに欠けるところも見られる<br>・ウイルス対策ソフトのメンテナンスやトラブルシュートが、適切に行われている<br>・緊急点検が必要となった場合、ウイルス対策ツールを配置したすべての機器におけるウイルスチェックが遅滞なく行われるようになっている<br>・システムの利用者がウイルス対策に関し行わねばならないこと（注2）が示されており、システムの利用者に、概ね徹底されている<br>・システムの利用者は、ウイルス対策に関し実施すべきことが生じた場合、概ね、適切な対応ができるようになっている<br>・ウイルス対策を担当する者のすべてに、ウイルス対策に関して日常的に行わなければならないことが概ね、徹底されている<br>・ウイルス対策の運用についての要求事項の実践状況は組織的に管理されているが、徹底しているとは言い難い<br>・ウイルス対策の運用に関する文書化のレベルはクラスB以上 |
| レベル3 | ウイルス対策に関してシステムの運用に求められていることが細部に渡り示されており、これらの実践を確実にするための仕組みも確立しており、この仕組みの下、要求の確実な厳格な実践が図られており、そのチェックや指導も行われているが、一部に徹底さにかけるところもあり、この点で不手際が生じる余地が残されている。 |

| | |
|---|---|
| | ・大まかではあるが、ウイルス対策チームが行わなくてはならないこと（注1）は示されている<br>・配置している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状況は、1ヶ月に1回以上はチェックされており、問題点は概ね対策されているが、厳格な管理は行われていない<br>・ベンダーから緊急対策が必要なウイルス定義ファイルがリリースされた場合、ゲートウェイ型で1時間以内、ファイルサーバやアプリケーションサーバで6時間以内、クライアントで48時間以内にすべての更新が完了しているが、徹底さに欠けるところも見られる<br>・ウイルス対策ソフトのメンテナンスやトラブルシュートも、適宜、行われている<br>・緊急点検が必要となった場合、遅滞なく、ウイルス対策ツールを配置したすべての機器におけるウイルスチェックが行われるようになっているが、徹底はしていない<br>・大まかではあるが、システムの利用者がウイルス対策に関し行わねばならないことは示されている<br>・ウイルス対策の運用に関する文書化のレベルはクラスB以上 |
| レベル2 | 関係者においては、ウイルス対策に関してシステムの運用に求められていることは、概ね承知しており、必要なことは日常的に行われはいるが、特に管理はされてなく、担当者の意識や注意に依存している。この点で、何時、不手際が生じても不思議ではない。<br>・ウイルス対策担当チーム内には、ウイルス対策に関して行うべきことと、それらへ対処方法についての習慣的に形成されてものを有している<br>・ベンダーから緊急対策が必要なウイルス定義ファイルがリリースされた場合、ウイルス対策担当者は必要な対応を心がけてはいるが、何時も、十分なものとは言い難い<br>・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状況の把握の努力は見られるが、十分とは言えない<br>・必要に応じた臨時のにウイルスチェックや、点検を行っていないクライアントに対する管理側から強制的な点検の実施等は、あまり行われていない<br>・ウイルス対策の運用に関する文書化のレベルはクラスC以上 |
| レベル1 | ウイルス対策担当者がウイルス対策に関して、日常的に行わなくてはならないこと、ならびにその実践の管理についての認識も希薄で、必要なことの適切な実践やその実行管理は行われていない。<br>・レベル2の達成要件も満たしていない |

(注1) ウイルス対策チームが行わなくてはならないこととして示すべき事項
- ・ウイルス対策ツールの使用状況の把握
- ・ウイルス定義ファイルの配布
- ・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の推進
- ・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の実施

(注2) システムの利用者がウイルス対策に関し行わねばならないこととして示すべき事項
- ・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
- ・ウイルス対策ファイルの更新の徹底
- ・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り離し等の緊急措置の実施と、ウイルス対策担当チームへの報告

## Tb3.4 ウイルス感染時の即応体制の整備

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | ウイルスへの感染が検知された場合における必要となる緊急措置（注 1）や本体策（注2）が確立しており、その関係者への周知も十分で、ウイルス侵入への対応に関わる関係者のこのような場面に対する対応能力も十分であることが確認されており、ウイルス感染事故への備えは万全である。<br>・ウイルス感染事故に対する対応体制が整備され、対応者へのタスクの明示もおこなわれ、それぞれは自己の責務を十分に承知している<br>・ウイルス感染事故の状況ごとに必要な措置および対応要領が確立しマニュアル化されている<br>・これらはウイルス感染事故への対応にかかわる者に周知されている<br>・関係者に対するウイルス感染事故への対応についての教育や訓練も行き届いており、必要な対応が何時でも迅速に取れるようになっている<br>・実際のウイルス感染事故の発生に際して、必要な対応は、期待通り円滑に機能している<br>・必要な場合、外部の専門家の支援も受けられるようになっている<br>・ウイルス感染事故への備えについての検討のレベルはクラス A<br>・ウイルス感染事故への備えについての見直し状況はクラス A<br>・ウイルス感染事故への備えについての文書化のレベルはクラス A |
| レベル4 | ウイルスへの感染が検知された場合における必要となる緊急措置（注 1）や本体策（注2）が確立しており、その関係者への周知も行われ、ウイルス侵入への対応に関わる関係者のこのような場面に対する対応能力もほぼ十分と見られており、ウイルス感染事故への備えは、概ね十分ではあるが、まだ強化の余地もある。<br>・ウイルス感染事故に対する対応体制が整備され、対応者へのタスクの明示もおこなわれ、それぞれは自己の責務を承知している<br>・ウイルス感染事故の状況ごとに必要な措置および対応要領が確立しマニュアル化されているが、まだ改善の余地もある<br>・これらはシステム運用マニュアル等で、感染事故への対応にかかわる者に周知されている<br>・関係者に対する障害時の対応についての教育や訓練も、概ね、行き届いており、必要な対応が何時でも迅速に取れるようにする努力が行われている<br>・実際のウイルス感染事故の発生に際して、必要な対応は、概ね期待通り機能している<br>・必要な場合、外部の専門家の支援も受けられるようになっている<br>・ウイルス感染事故への備えについての検討のレベルはクラス B 以上<br>・ウイルス感染事故への備えについての見直し状況はクラス B 以上<br>・ウイルス感染事故への備えについての文書化のレベルはクラス B 以上 |
| レベル3 | ウイルスへの感染が検知された場合において必要となる措置が大まかではあるが決められ、関係者へ示されており、このような場面に対し、基本的な対応はできると見ることができる。ただし、指定されている措置の内容や、その関係者への展開も十分とは言えず、改善の余地は多い。<br>・ウイルス感染事故発生時に必要となる措置および対応要領が示されているが大まかで、発生事故の状況ごとの細かい展開は不十分<br>・これらは、何らかの形でウイルス感染事故への対応にかかわる者に示されており、訓練も試みられているが、十分とは言い難い<br>・実際のウイルス感染事故の発生に際しては、ある程度適切な対応はできているが、何らかの問題点は出ている<br>・ウイルス感染事故への備えについての検討のレベルはクラス B 以上<br>・ウイルス感染事故への備えについての見直し状況はクラス B 以上<br>・ウイルス感染事故への備えについての文書化のレベルはクラス B 以上 |
| レベル2 | ウイルス対策チーム内で検討されたウイルスへの感染が検知された場合において必要となる措置はあるが、内容も基本的なところに止まっており、対応にかかわる者への周知も不十分で、万一の場合の対応が適切にできるかどうかは怪しい。<br>・ウイルス対策担当チームは、ウイルス感染事故発生時に必要となる措置を検討しており、基本的なことは決められ、担当チーム内の共通認識はできている |

| | |
|---|---|
| | ・ウイルス感染事故への備えについての文書化のレベルはクラス C 以上 |
| レベル 1 | ウイルスへの感染が検知された場合において必要となる措置は、示されていない。 |

(注 1) ウイルス感染時の緊急措置として行うべきこととして示されるべきこと
・関係者への連絡と対策体制の立ち上げ
・ネットワークの切断等の緊急措置とその適用方法（適用範囲、実施方法他）
・感染状況の確認および分析要領（現象および感染ウイルスの特定他）
・被害状況の確認（被害の内容や範囲他）
・復旧への手続き

(注 2) ウイルス感染に対する本体策として行うべきこと
・感染ウイルス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

### 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

| 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システム情報やセキュリティ管理情報の保護において、不手際が生じることはまず考えられないレベルの完成度の高い管理上の仕組みが確立しいる。<br>・システム情報やセキュリティ管理情報の保護管理についての責任体制が確立している<br>・保護管理の対象となるシステム情報やセキュリティ管理情報は、完全に洗いだされている<br>・システム情報やセキュリティ管理情報(群)に対して指定すべき保護要件の指定要領、ならびにその指定をレビュー承認するプロセスが確立している<br>・現実の保護管理の対象となるこれらの情報が含まれた印刷物や電子ファイル等に対す対して指定すべき保護要件の指定要領、ならびにその指定をレビュー承認するプロセスが確立している<br>・これらの情報および現実の保護対象となる印刷物や電子ファイル等のすべてについて、そのライフサイクルの全過程において、指定された保護要件に沿った取扱いの実践を管理するための仕組みが確立している<br>・これらの仕組みは、指定の不備や指定された保護の実践上の不手際が、見逃される余地はない程、きめ細かく厳格に作られている<br>・保護管理の対象となるシステム情報やセキュリティ管理情報が含まれた印刷物や電子ファイル等の内容や、ライフサイクルににについての記録、保護管理状況は何時でも、正確に把握できるようにするための仕組みが確立している<br>・システム情報やセキュリティ管理情報の保護の仕組みについての見直しのレベルはクラスA<br>・システム情報やセキュリティ管理情報の保護の仕組みついての文書化のレベルはクラスA |
| レベル4 | システム情報やセキュリティ管理情報の保護を確実にするためのよく検討された管理上の仕組みが確立しいるが、まだ改善の余地もある。<br>・システム情報やセキュリティ管理情報の保護管理についての責任体制が確立している<br>・保護管理の対象となるシステム情報やセキュリティ管理情報は、ほぼ、完全に洗いだされている<br>・システム情報やセキュリティ管理情報(群)に対して指定すべき保護要件の指定要領、ならびにその指定をレビュー承認するプロセスが確立しているが、まだ改善する余地もある<br>・現実の保護管理の対象となるこれらの情報が含まれた印刷物や電子ファイル等に対す対して指定すべき保護要件の指定要領、ならびにその指定をレビュー承認するプロセスが確立している、まだ改善する余地もある<br>・これらの情報および現実の保護対象となる印刷物や電子ファイル等のすべてについて、そのライフサイクルの全過程において、指定された保護要件に沿った取扱いの実践を管理するための仕組みが確立している、まだ改善する余地もある<br>・これらの仕組みは、指定の不備や指定された保護の実践上の不手際が、見逃されないようにする工夫が、相当になされているが、まだ改善の余地もある<br>・保護管理の対象となるシステム情報やセキュリティ管理情報が含まれた印刷物や電子ファイル等の内容や、ライフサイクルににについての記録、保護管理状況は何時でも、正確に把握できるようにするための仕組みが確立している、まだ改善する余地もある<br>・システム情報やセキュリティ管理情報の保護の仕組みについての見直しのレベルはクラスB以上<br>・システム情報やセキュリティ管理情報の保護の仕組みついての文書化のレベルはクラスB以上 |
| レベル3 | 大まかではあるが、システム情報やセキュリティ管理情報の保護を確実にするための管理上の仕組みが示されている。この仕組みには、これらの情報の保護において、不手際が生じないようにするための工夫がなされているが、不手際が見逃さないようにするレベルには至っていない。<br>・システム情報やセキュリティ管理情報の保護管理についての責任体制は示されている<br>・保護管理の対象となるシステム情報やセキュリティ管理情報は、概ね、洗いだされている<br>・大まかではあるが、システム情報やセキュリティ管理情報(群)に対して指定すべき保護要件の指定要領、ならびに指定プロセスが示されている<br>・大まかではあるが、これらの情報および現実の保護対象となる印刷物や電子ファイル等について、そのライフサイクルの全過程において、指定された保護要件に沿った取扱いの実践を管理するための仕組みも示されているが、対象の網羅性や、指定のきめ細かさは、十分な域には達していない |

| | |
|---|---|
| | ・大まかではあるが、保護管理の対象となるシステム情報やセキュリティ管理情報が含まれた印刷物や電子ファイル等の内容や、ライフサイクルについての記録、保護管理状況を、把握するための仕組みも示されている<br>・システム情報やセキュリティ管理情報の保護の仕組みについての見直しのレベルはクラスＢ以上<br>・システム情報やセキュリティ管理情報の保護の仕組みついての文書化のレベルはクラスＢ以上 |
| レベル2 | 組織的に検討された、システム情報やセキュリティ管理情報の保護を確実にするための管理上の仕組みはないが、関係者間に習慣的に形成された管理の仕組みが存在し機能している。<br>・関係者は、システム情報やセキュリティ管理情報の保護管理について、自己の責務を承知している<br>・保護管理の対象となるシステム情報やセキュリティ管理情報の把握は、概ね、洗いだされている<br>・システム情報やセキュリティ管理情報（群）に対して指定すべき保護要件の指定や指定のプロセスについて、関係者間に習慣的に形成された方法があり使われている<br>・これらの情報および現実の保護対象となる印刷物や電子ファイル等について、、指定された保護要件に沿った取扱いの実践の管理について、関係者間に習慣的に形成された方法があり使われているが、十分なものとは言い難い<br>・担当者間には、保護管理の対象となるシステム情報やセキュリティ管理情報が含まれた印刷物や電子ファイル等の内容や、ライフサイクルににについての記録、保護管理状況を把握することについて、習慣的に形成された方法があり、実際に機能している<br>・システム情報やセキュリティ管理情報の保護の仕組みについての見直しのレベルはクラスＣ以上<br>・システム情報やセキュリティ管理情報の保護の仕組みついての文書化のレベルはクラスＣ以上 |
| レベル1 | システム情報やセキュリティ管理情報の保護を確実にするための仕組み作りについての組織的な取り組みは、行われて存在しないに等しい。<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 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は、組織的で徹底した検討、レビューの下で決められており、これらの情報に対する保護要件の指定に不備が入り込むことは、まず考えられない。<br>・保護管理の対象とすべきシステム情報やセキュリティ管理情報は、完全に洗いだされている<br>・すべてのシステム情報やセキュリティ管理情報（群）について、組織的で徹底した検討ならびにレビューの下で、保護要件（注1）の指定が行われている<br>・これらの情報を含む印刷物や電子ファイル等の業務現場やシステム上での現実の管理対象が、その存在場所とともに、完全に洗いだされている<br>・これらの情報を含む現実の管理対象のそれぞれについて、関係する情報に対して指定された保護要件（注2）を反映した保護要件が、組織的で徹底した検討ならびにレビューの下で指定されている<br>・特に重要としたセキュリティ管理情報（群）に対しては、まず、技術面からも管理面からも問題の発生が考えられないような最高水準の保護を要求している<br>・比較的重要としたシステム情報やセキュリティ管理情報に対しては、比較的進んだ技法を用いた攻撃にも耐えられ、また、保護管理の不備や不手際を見逃されない仕組みの下におかれることが要求されている<br>・その他の情報についても、比較的容易に利用できる手法を用いた攻撃に耐えられることが要求されている<br>・システム情報やセキュリティ管理情報、およびこれらの情報にかかわる現実の保護管理対象に指定している保護要件についての見直し状況はクラスＡ<br>・システム情報やセキュリティ管理情報、およびこれらの情報にかかわる現実の保護管理対象に指定についての文書化のレベルはクラスＡ |
| | 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は、組織的な検討、レビューの下で決 |

| | |
|---|---|
| レベル4 | められているが、一部に徹底さを欠くところも見られ、これらの情報に対する保護要件の指定に不備が入り込む隙が、僅かではあるが残されている。<br>・保護管理の対象とすべきシステム情報やセキュリティ管理情報は、ほぼ、完全に洗いだされている<br>・すべてのシステム情報やセキュリティ管理情報（群）について、組織的な検討ならびにレビューの下で、保護要件（注1）の指定が行われているが、検討やレビューに徹底さに欠けるところも見られる<br>・これらの情報を含む印刷物や電子ファイル等の業務現場やシステム上での現実の管理対象が、その存在場所とともに、ほぼ、完全に洗いだされている<br>・これらの情報を含む現実の管理対象のそれぞれについて、関係する情報に対して指定された保護要件（注2）を反映した保護要件が、組織的な検討ならびにレビューの下で指定されている検討やレビューに徹底さに欠けるところも見られる<br>・重要としたシステム情報やセキュリティ管理情報に対しては、比較的進んだ技法を用いた攻撃にも耐えられ、また、保護管理の不備や不手際を見逃されない仕組みの下におかれることが要求されている<br>・その他の情報についても、比較的容易に利用できる手法を用いた攻撃に耐えられることが要求されている<br>・システム情報やセキュリティ管理情報、およびこれらの情報にかかわる現実の保護管理対象に指定している保護要件についての見直し状況はクラスB以上<br>・システム情報やセキュリティ管理情報、およびこれらの情報にかかわる現実の保護管理対象に指定についての文書化のレベルはクラスB以上 |
| レベル3 | 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は、組織的な検討、レビューの下で決められているが、検討やレビューは徹底したものでなく、また、指定の対象の網羅性にも欠けるところがあり、これらの情報に対する保護要件の指定に、不備が入り込む余地が残されている。<br>・保護管理の対象とすべきシステム情報やセキュリティ管理情報は、概ね洗いだされていが、すべて把握されているとは言えない<br>・システム情報やセキュリティ管理情報（群）について、組織的な検討ならびにレビューの下で、保護要件（注1）の指定が行われているが、対象情報の網羅性や、検討やレビューは徹底したものではない<br>・これらの情報を含む印刷物や電子ファイル等の業務現場やシステム上での現実の管理対象の把握も、行われているが徹底したものではなく、主なものを見逃していることはないにしても、網羅されているとは言えない<br>・これらの情報を含む現実の管理対象のそれぞれについて、関係する情報に対して指定された保護要件（注2）を反映した保護要件が、組織的な検討ならびにレビューの下で指定されているが、検討やレビューは徹底したものではない<br>・重要としたシステム情報やセキュリティ管理情報に対しては、比較的進んだ技法を用いた攻撃にも耐えられ、また、保護管理の不備や不手際を見逃されない仕組みの下におかれることが、概ね、要求されている<br>・その他の情報についても、概ね、比較的容易に利用できる手法を用いた攻撃に耐えられることが要求されている<br>・システム情報やセキュリティ管理情報、およびこれらの情報にかかわる現実の保護管理対象に指定している保護要件についての見直し状況はクラスB以上<br>・システム情報やセキュリティ管理情報、およびこれらの情報にかかわる現実の保護管理対象に指定についての文書化のレベルはクラスB以上 |
| レベル2 | システム情報やセキュリティ管理情報、および現実の保護管理対象としての担当者間に共有されているこれらが含まれた印刷物や電子ファイル等に対する保護についての考え方が存在し、これらに対する保護要件は、担当チームで決められている。担当チーム内でのレビューは行われているが、組織的な管理は行われてない。<br>・担当チーム内では、これらの保護についての共有されている考え方が存在し使われている<br>・これらに対する保護要件の指定については、チーム内でのレビューは行われているが、その他のものについては担当者任せとなっている<br>・重要な情報にかかわるものの一部に対しては、意図的な攻撃に対する保護も意識されているが、その他については、実務上の必須条件の指定に止まっている<br>・システム情報やセキュリティ管理情報、およびこれらの情報にかかわる現実の保護管理対象に指定についての文書化のレベルはクラスC以上 |
| レベル1 | 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は、特に管理されていない。<br>・レベルの達成条件も満たせない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システム情報やセキュリティ管理情報の保護管理は、そのすべてについて、それぞれに指定された保護要件に沿って、そのライフサイクル全般にわたって、厳格な組織管理の下で取り扱われている。システム情報やセキュリティ管理情報に的確性の喪失や漏洩等の事故が発生することは、まず、考えられない。<br>・すべてのシステム情報やセキュリティ管理情報は、そのライフサイクルの全過程において、それぞれに指定された手順に沿って指定された保護要件通りに適切に取り扱われている<br>・システム情報やセキュリティ管理情報のシステムへの登録は、所定の手順に沿って行われ、その操作や登録内容の的確性について厳格なチェックが行われている<br>・システム上のこれらの情報に対するアクセスに対しては、保護要件に沿ったアクセス制御とアクセスについての監視の仕組みが的確に組み込まれている<br>・システム上のこれらの情報のうち、特に重要なものに対しては、最も進んだ技術を用いた攻撃にも耐えられるレベルの保護手段が、比較的重要とした情報に対しては、専門的な技術を用いた攻撃にも耐えられるレベルの保護手段が、そのたのものに対しても、容易に使用できる攻撃手段には耐えられるレベルの保護手段が適用されている<br>・システム上のこれらの情報の保全も、指定どおりに確実に行われている<br>・これらの情報に対するアクセス権やアクセス権限者の管理も、指定された仕組み沿って徹底して行われている<br>・システム上のこれらの情報の操作の履歴はすべて記録保管されている<br>・システム情報やセキュリティ管理情報の保護管理の実践と管理の徹底状況はクラスA<br>・システム情報やセキュリティ管理情報の保護管理の実践についての見直し状況はクラスA<br>・システム情報やセキュリティ管理情報の保護管理の実践やその管理の状況についての文書化のレベルはクラスA |
| レベル4 | システム情報やセキュリティ管理情報の保護管理は、そのすべてについて、それぞれに指定された保護要件に沿って、そのライフサイクル全般にわたって、組織管理の下で厳格に取扱われているが、一部に徹底さを欠くところも見られる。システム情報やセキュリティ管理情報に的確性の喪失や漏洩等の事故が発生する隙が、僅かではあるが残されている。<br>・すべてのシステム情報やセキュリティ管理情報は、そのライフサイクルの全過程において、それぞれに指定された手順に沿って指定された保護要件通りに適切に取り扱われているが、一部に徹底さを欠くところも見られる<br>・これらの情報のシステムへの登録は、所定の手順に沿って行われ、その操作や登録内容の的確性についてチェックが厳格に行われているが、一部に徹底さを欠くところも見られる<br>・システム上のこれらの情報に対するアクセスに対しては、保護要件に沿ったアクセス制御とアクセスについての監視の仕組みが的確に組み込まれている<br>・システム上のこれらの情報のうち、特に重要なものに対しては、最も進んだ技術を用いた攻撃にも耐えられるレベルの保護手段が、比較的重要とした情報に対しては、専門的な技術を用いた攻撃にも耐えられるレベルの保護手段が、そのたのものに対しても、容易に使用できる攻撃手段には耐えられるレベルの保護手段が適用されている<br>・システム上のこれらの情報の保全も、指定どおりに確実に行われている<br>・これらの情報に対するアクセス権やアクセス権限者の管理も、指定された仕組み沿って厳格に行われているが、一部に徹底さを欠くところも見られる<br>・システム上のこれらの情報の操作の履歴はすべて記録保管されているが、一部に徹底さを欠くところも見られる<br>・システム情報やセキュリティ管理情報の保護管理の実践と管理の徹底状況はクラスB以上<br>・システム情報やセキュリティ管理情報の保護管理の実践についての見直し状況はクラスB以上<br>・システム情報やセキュリティ管理情報の保護管理の実践やその管理の状況についての文書化のレベルはクラスB以上 |
| レベル3 | システム情報やセキュリティ管理情報の保護管理は、そのほとんどについて、それぞれに大まかであるが指定された保護要件に沿って、そのライフサイクル全般にわたって、組織的な管理の下で取扱われているが、管理は徹底したものではない。システム情報やセキュリティ管理情報に的確性の喪失や漏洩等の事故が発生する隙が残されている。 |

| | |
|---|---|
| | ・重要なシステム情報やセキュリティ管理情報については、そのライフサイクルの全過程において、それぞれに指定された手順に沿って指定された保護要件通りに取り扱われているが、徹底さを欠くところもある。また、この管理の適用も重要でないと見ている情報に対しては、大まかなものである<br>・これらの情報のシステムへの登録は、概ね、所定の手順に沿って行われ、その操作や登録内容の的確性についてチェックも組織的に行われているが、徹底したものとは言えない<br>・システム上のこれらの情報に対するアクセスに対しては、保護要件に沿ったアクセス制御とアクセスについての監視の仕組みが、概ね、適切に組み込まれている<br>・システム上のこれらの情報のうち、比較的重要とした情報に対しては、専門的な技術を用いた攻撃にも耐えられるレベルの保護手段が、そのたのものに対しても、容易に使用できる攻撃手段には耐えられるレベルの保護手段が適用されている<br>・システム上のこれらの情報の保全も、指定どおりに確実に行われている<br>・これらの情報に対するアクセス権やアクセス権限者の管理も、指定された仕組み沿って行われているが、徹底したものではない<br>・システム上のこれらの情報の操作の履歴の記録保管は、重要なものについては、概ね､取得されている<br>・システム情報やセキュリティ管理情報の保護管理の実践と管理の徹底状況はクラスＣ以上<br>・システム情報やセキュリティ管理情報の保護管理の実践についての見直し状況はクラスＣ以上<br>・システム情報やセキュリティ管理情報の保護管理の実践やその管理の状況についての文書化のレベルはクラスＣ以上 |
| レベル2 | 関係者間には、システム情報やセキュリティ管理情報の保護管理について、習慣的に形成された方法が存在していて、これらの取扱いや管理は、概ね、この方法に沿って行われている。組織的に管理されているとは言い難く、システム情報やセキュリティ管理情報の保護管理は、十分とは言えない。<br>・関係者は、重要なシステム情報やセキュリティ管理情報については、そのライフサイクルの主要なステップについては、担当者レベルとしては十分な注意を払って取り扱っているが、重要でないと見ている情報に対する取扱いは、注意を払っている程度である<br>・これらの情報のシステムへの登録は、担当者間では習慣となっている手順に沿って行われ、担当者レベルでの、その操作や登録内容の的確性についてチェックも行われている<br>・システム上のこれらの情報に対するアクセスに対しては、保護要件に沿ったアクセス制御とアクセスについての監視の仕組みも組み込まれているが、すべてに対し十分とは言えない<br>・攻撃手段からの保護は、比較的容易に使用できる攻撃手段には耐えられるレベルの保護手段が適用されている<br>・システム上のこれらの情報の保全は、一部の者に限られている<br>・これらの情報に対するアクセス権やアクセス権限者の管理も、あまり厳格には行われていない<br>・システム情報やセキュリティ管理情報の保護管理の実践についての見直しは、あまり行われていない<br>・システム情報やセキュリティ管理情報の保護管理の実践やその管理の状況についての文書化のレベルはクラスＤ以上 |
| レベル1 | システム情報やセキュリティ管理情報の保護管理の保護の実践についての組織的な取組みはないに等しい<br>・レベル2の達成要件も満たしていない |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システム上の業務情報の保護において、不手際が生じることはまず考えられないレベルの完成度の高い管理上の仕組みが確立しいる。<br>･システム上の業務情報の保護管理についての責任体制が確立している<br>･保護管理の対象となるシステム上の業務情報は、完全に洗いだされている<br>･システム上の業務情報（群）に対して指定すべき保護要件（注1）の指定要領（注2）、ならびにその指定をレビュー承認するプロセスが確立している<br>･現実の保護管理の対象となるこれらの情報が含まれた電子ファイル等に対す対して指定すべき保護要件の指定要領、ならびにその指定をレビュー承認するプロセスが確立している<br>･現実に保護の対象となる電子ファイル等のすべてについて、そのライフサイクルの全過程において、指定された保護要件に沿った取扱いの実践を管理するための仕組みが確立している<br>･これらの仕組みは、指定の不備や指定された保護の実践上の不手際が、見逃される余地はない程、きめ細かく厳格に作られている<br>･保護管理の対象となる電子ファイル等の内容や、ライフサイクルににについての記録、保護管理状況は何時でも、正確に把握できるようにするための仕組みが確立している<br>･システム上の業務情報の仕組みについての見直しのレベルはクラスA<br>･システム上の業務情報の保護の仕組みついての文書化のレベルはクラスA |
| レベル4 | システム上の業務情報の保護を確実にするためのよく検討された管理上の仕組みが確立しいるが、まだ改善の余地がある。<br>･システム上の業務情報の保護管理についての責任体制が確立している<br>･保護管理の対象となるシステム上の業務情報は、ほぼ、完全に洗いだされている<br>･システム上の業務情報（群）に対して指定すべき保護要件の指定要領、ならびにその指定をレビュー承認するプロセスが確立しているが、まだ改善する余地もある<br>･現実の保護管理の対象となるこれらの情報が含まれた電子ファイル等に対す対して指定すべき保護要件の指定要領、ならびにその指定をレビュー承認するプロセスが確立している、まだ改善する余地もある<br>･現実の保護対象となる電子ファイル等のすべてについて、そのライフサイクルの全過程において、指定された保護要件に沿った取扱いの実践を管理するための仕組みが確立している、まだ改善する余地もある<br>･これらの仕組みは、指定の不備や指定された保護の実践上の不手際が、見逃される余地が、まず、ないと考えられる程、きめ細かく厳格に作られている<br>･保護管理の対象となるシステム上の業務情報が含まれた電子ファイル等の内容や、ライフサイクルにについての記録、保護管理状況は何時でも、正確に把握できるようにするための仕組みが確立している、まだ改善する余地もある<br>･システム上の業務情報の保護の仕組みについての見直しのレベルはクラスB以上<br>･システム上の業務情報の保護の仕組みついての文書化のレベルはクラスB以上 |
| レベル3 | 大まかではあるが、システム上の業務情報の保護を確実にするための管理上の仕組みが示されている。この仕組みには、これらの情報の保護において、不手際が生じないようにするための工夫がなされているが、不手際が見逃さないようにするレベルには至っていない。<br>･システム上の業務情報の保護管理についての責任体制は示されている<br>･現実の保護の対象となる電子ファイル等はその存在場所も含め、概ね、洗いだされている<br>･大まかではあるが、システム上の業務情報（群）に対して指定すべき保護要件の指定要領、ならびに指定プロセスが示されている<br>･大まかではあるが、現実の保護対象となる電子ファイル等について、そのライフサイクルの全過程において、指定された保護要件に沿った取扱いの実践を管理するための仕組みも示されているが、対象の網羅性や、指定のきめ細かさは、十分な域には達していない<br>･大まかではあるが、保護管理の対象となるシステム上の業務情報が含まれた印刷物や電子ファイル等の内容や、ライフサイクルにについての記録、保護管理状況を、把握するための仕組みも示されて |

| | |
|---|---|
| | いる<br>・システム上の業務情報の保護の仕組みについての見直しのレベルはクラスＢ以上<br>・システム上の業務情報の保護の仕組みついての文書化のレベルはクラスＢ以上 |
| レベル2 | 組織的に検討された、システム上の業務情報の保護を確実にするための管理上の仕組みはないが、関係者間に習慣的に形成された管理の仕組みが存在し機能している。<br>・関係者は、システム上の業務情報の保護管理について、自己の責務を承知している<br>・保護管理の対象となるシステム上の業務情報がの把握は、概ね、洗いだされている<br>・システム上の業務情報（群）に対して指定すべき保護要件の指定や指定のプロセスについて、関係者間に習慣的に形成された方法があり使われている<br>・現実の保護対象となる電子ファイル等について、、指定された保護要件に沿った取扱いの実践の管理について、関係者間に習慣的に形成された方法があり使われているが、十分なものとは言い難い<br>・担当者間には、保護管理の対象の電子ファイル等の内容や、ライフサイクルににについての記録、保護管理状況を把握することについて、習慣的に形成された方法があり使われている<br>・システム上の業務情報の保護の仕組みについての見直しのレベルはクラスＣ以上<br>・システム上の業務情報の保護の仕組みついての文書化のレベルはクラスＣ以上 |
| レベル1 | システム上の業務情報の保護を確実にするための仕組み作りは存在しないに等しい。<br>・レベル2の達成要件も満たしていない |

(注1) システム上の業務情報（群）データベースに対して指定すべき保護要件として指定すべき事項
・システム上の業務情報データベースのバックアップの取得等の保全についての指定
・データベース上の個々の情報対象情報に対するライフサイクルのすべてのプロセス（新規作成、参照、更新、削除他）についての権限の指定
・データベース上の個々の情報対象情報の参照や操作の権限を与えるものについての管理の方法の指定
・データベース上の個々の情報対象情報の参照や操作についての履歴の取得についての指定

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システム上の業務データの個々に対する保護要件は、組織的で徹底した検討、レビューの下で決められており、これらの情報に対する保護要件の指定に不備が入り込むことは、まず考えられない。<br>・保護管理の対象とすべきシステム上の業務データは、完全に洗いだされている<br>・すべてのシステム上の業務データ（群）について、組織的で徹底した検討ならびにレビューの下で、保護要件（注1）の指定が行われている<br>・保護対象となるシステム上の業務データ、その存在場所とともに、完全に洗いだされている<br>・これらの情報を含む現実の管理対象のそれぞれについて、関係する情報に対して指定された保護要件（注2）を反映した保護要件が、組織的で徹底した検討ならびにレビューの下で指定されている<br>・特に重要なシステム上の業務データ（群）に対しては、まず、技術面からも管理面からも問題の発生が考えられないような最高水準の保護を要求している<br>・比較的重要としたシステム上の業務データに対しては、比較的進んだ技法を用いた攻撃にも耐えられ、また、保護管理の不備や不手際を見逃されない仕組みの下におかれることが要求されている<br>・その他のシステム上の業務データについても、比較的容易に利用できる手法を用いた攻撃に耐えられることが要求されている<br>・システム上の業務データに指定している保護要件についての見直し状況はクラスＡ<br>・システム上の業務データに指定についての文書化のレベルはクラスＡ |
| レベル4 | システム上の業務データの個々に対する保護要件は、組織的な検討、レビューの下で決められているが、一部に徹底さを欠くところも見られ、これらの情報に対する保護要件の指定に不備が入り隙が、僅かではあるが残されている。<br>・保護管理の対象とすべきシステム上の業務データは、ほぼ、完全に洗いだされている |

| | |
|---|---|
| | ・すべてのシステム上の業務データ（群）について、組織的な検討ならびにレビューの下で、保護要件（注 1）の指定が行われているが、検討やレビューに徹底さに欠けるところも見られる<br>・システム上の業務データが、その存在場所とともに、ほぼ、完全に洗いだされている<br>・これらの情報を含む現実の管理対象のそれぞれについて、関係する情報に対して指定された保護要件（注 2）を反映した保護要件が、組織的な検討ならびにレビューの下で指定されている検討やレビューに徹底さに欠けるところも見られる<br>・重要としたシステム上の業務データ報に対しては、比較的進んだ技法を用いた攻撃にも耐えられ、また、保護管理の不備や不手際を見逃されない仕組みの下におかれることが要求されている<br>・その他の情報についても、比較的容易に利用できる手法を用いた攻撃に耐えられることが要求されている<br>・システム上の業務データに指定している保護要件についての見直し状況はクラス B 以上<br>・システム上の業務データに指定についての文書化のレベルはクラス B 以上 |
| レベル 3 | システム上の業務データの個々に対する保護要件は、組織的な検討、レビューの下で決められているが、検討やレビューは徹底したものでなく、また、指定の対象の網羅性にも欠けるところがあり、これらの情報に対する保護要件の指定に、不備が入り込む余地が残されている。<br>・システム上の業務データは、概ね洗いだされていが、すべて把握されているとは言えない<br>・システム上の業務データ（群）について、組織的な検討ならびにレビューの下で、保護要件（注 1）の指定が行われているが、対象情報の網羅性や、検討やレビューは徹底したものではない<br>・システム上の業務データの把握も、行われているが徹底したものではなく、主なものを見逃していることはないにしても、網羅されているとは言えない<br>・これらの情報を含む現実の管理対象のそれぞれについて、関係する情報に対して指定された保護要件（注 2）を反映した保護要件が、組織的な検討ならびにレビューの下で指定されているが、検討やレビューは徹底したものではない<br>・重要としたシステム上の業務データに対しては、比較的進んだ技法を用いた攻撃にも耐えられ、また、保護管理の不備や不手際を見逃されない仕組みの下におかれることが、概ね、要求されている<br>・その他の情報についても、概ね、比較的容易に利用できる手法を用いた攻撃に耐えられることが要求されている<br>・システム上の業務データに指定している保護要件についての見直し状況はクラス BC 以上<br>・システム上の業務データに指定についての文書化のレベルはクラス B 以上 |
| レベル 2 | システム上の業務データの保護について、担当者間に共有されている考え方が存在し、これらに対する保護要件は、担当チームで決められている。担当チーム内でのレビューは行われているが、組織的な管理は行われてない。<br>・担当チーム内では、これらの保護についての共有されている考え方が存在し使われている<br>・これらに対する保護要件の指定については、チーム内でのレビューは行われているが、その他のものについては担当者任せとなっている<br>・重要な情報にかかわるものの一部に対しては、意図的な攻撃に対する保護も意識されているが、その他については、実務上の必須条件の指定に止まっている<br>・システム上の業務データに指定についての文書化のレベルはクラス C 以上 |
| レベル 1 | システム上の業務データに対する保護要件の指定は、特に管理されていない。<br>・レベルの達成条件も満たせない |

(注 1) システム上の業務情報（群）データベースに対して指定すべき保護要件として指定すべき事項
・システム上の業務情報データベースのバックアップの取得等の保全についての指定
・データベース上の個々の情報対象情報に対するライフサイクルのすべてのプロセス（新規作成、参照、更新、削除他）についての権限の指定
・データベース上の個々の情報対象情報の参照や操作の権限を与えるものについての管理の方法の指定
・データベース上の個々の情報対象情報の参照や操作についての履歴の取得についての指定

(注 2) システム上の業務情報（群）への保護要件の指定要領として指定すべき事項
・保護要件の指定についての責任体制
・保護要件の定義様式
・保護要件の検討・審査・承認の手順
・保護用嫌悪指定におけるレビューのポイント

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 想定される脅威に対して最高レベルの対策を実装しており、検討段階や運用といった設計・構築の前後のプロセスについても高いレベルを維持している。<br>・パスワード認証では不十分と思われるシステム・アカウントについては IC カード、バイオメトリクス、電子証明書など他の認証技術を使用して現段階で最も高い認証強度を保持している。<br>・アクセスマトリックスに基づいて情報をレベル4からより更に細かく分類し行・列単位でのアクセスコントロールを行っている。<br>・3層構造アプリケーションのユーザも全て識別してアクセスコントロールを行っている。<br>・不正なルートからの接続に対しては権限の無効化や閲覧禁止などの防御措置が実装されている<br>・3層構造アプリケーションのユーザも含めて全ユーザの操作に関するログを保管し、暗号化、タイムスタンプ等の技術を用いて不正な改ざんを防止・検知できるよう保全措置がとられている。<br>・ログの定期的な分析を実施して不審な操作を早期に発見できるプロセスを確立している。または不審な操作を検知して管理者への警告を行うような仕組みを導入している。<br>・ルール（アクセスポリシーなど）の検討レベルは A<br>・必要に応じた見直しのレベルは A<br>・運用体制や責任、これらの仕組みの活動状態についての文書化のレベルは A |
| レベル4 | より厳密なセキュリティ対策を実装しており、通常考えられる脅威に対しては概ね対応できる。アプリケーションとの連携も行いながら対策を行っている。<br>・RDBMS ユーザのパスワードはレベル 3 に加えて有効期限・定期的な変更・簡単な文字列の使用、同じ文字列の再利用禁止がシステムで強制されている。<br>・あらかじめ組織構成や役職などユーザの属性と格納情報の Classification を行いアクセスマトリックスが作成されている。<br>・アクセスマトリックスに基づいて表・ビューに対するアクセス権が最小化され厳密に付与されている。（特定の行・列単位での制御は行われていない）<br>・管理者権限の利用についてもある一部ログを収集しているが完全な客観性は保持されていない。<br>・3層構造アプリケーションのユーザも特定したログを収集・保管している。保管しているログの内容に SQL テキストを含んでいる<br>・ルール（アクセスポリシーなど）の検討レベルは B 以上<br>・実装管理や実行管理の徹底状況（アクセス権限管理の実行プロセス）についてはレベルB以上<br>・必要に応じた見直しのレベルは B 以上<br>・仕組みについての文書化のレベルは B 以上 |
| レベル3 | ある程度設定・設計はセキュリティを意識して行われており最低限必要なレベルでは機能しているが、いくつかの脅威に対しては脆弱な点を残しており改善する余地は多い。<br>・RDBMS ユーザのパスワードはデフォルトから確実に変更されている。<br>・ユーザアカウントは共有されていない。<br>・ユーザごとに表・ビューに対してある程度限定的な権限が付与されているが厳密な最少化ではない。<br>・管理者を限定して管理者権限を使用させている。<br>・RDBMS の標準的な機能を使ったログ収集を行っている。3層構造アプリケーションのユーザについては必ずしも個人の特定ができないが、操作の内容や日時は概ね追跡できる。<br>・これらの仕組みについての文書化のレベルは C 以上<br>・対策の検討レベルについてはB以上 |
| レベル2 | セキュリティ対策としては十分ではないがシステムによってはある程度許容できるレベル。<br>・ユーザアカウントは共有されていない。<br>・管理者以外のユーザ・アプリケーションには管理者権限を付与していない。<br>・最も重要な情報についてのみアクセス権の制限が行われている。<br>・セキュリティ対策の実装についての文書化のレベルは D 以上 |
| レベル1 | RDBMS でのセキュリティは考慮されていない。<br>・レベル2の達成要件も満たしていない |

| 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ソフトの設計への配慮 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 想定される脅威に対して最高レベルの対策を実装しており、検討段階や運用といった設計・構築の前後のプロセスについても高いレベルを維持している。<br>・パスワードについては暗号化し、またその鍵管理方法などについても現状では最高レベルの強度を持つ手法をとっている<br>・アクセスマトリックスに基づいて情報をレベル4から更に細かく分類し、ユーザの分割、行・列単位までのアクセスコントロールを考慮した表・ビュー・ロールの実装を行っている<br>・3層構造アプリケーションのユーザを DBMS 側で識別してアクセスコントロールや監査を行うために必要なユーザ情報等をDBMS側に引き渡すことができる仕組みを備えている。(DBMS側にこのような機能が搭載されている場合)<br>・ルール(アクセスポリシーなど)の検討レベルはA<br>・必要に応じた見直しのレベルはA<br>・運用体制や責任、これらの仕組みの活動状態についての文書化のレベルはA |
| レベル4 | より厳密なセキュリティ対策を実装しており、通常考えられる脅威に対しては概ね対応できる。アプリケーションとDBMSの連携が比較的緊密に行われている。<br>・RDBMS ユーザのパスワードはレベル 3 と異なり暗号化されている、または平文で読むことができないような形でのハードコーディング・隠蔽対策等がとられている<br>・あらかじめ組織構成や役職などユーザの属性と格納情報の Classification を行いアクセスマトリックスが作成されている<br>・アクセスマトリックスに基づいて表・ビューに対するアクセス権を最小化するためにアプリケーションの接続用ユーザ・権限・ロールが厳密に定義され、付与されている。(特定の行・列単位での制御までは行われていない)<br>・ルール(アクセスポリシーなど)の検討レベルはB以上<br>・実装管理や実行管理の徹底状況(アクセス権限管理の実行プロセス)についてはレベルB以上<br>・必要に応じた見直しのレベルはB以上<br>・仕組みについての文書化のレベルはB以上 |
| レベル3 | ある程度設定・設計は DBMS 側のセキュリティ実装を意識して行われており最低限必要なレベルでは機能しているが、いくつかの脅威に対しては脆弱な点を残しており改善する余地は多い。<br>・RDBMS ユーザのパスワードは暗号化されていないが代替手段としてOSの保護を強化している<br>・接続用ユーザアカウントは管理者用権限を付与されていない<br>・ユーザごとに表・ビューに対する権限の制御を行うために複数のユーザと権限・ロールを定義し、アプリケーション側で使い分けているが厳密な最少化ではない<br>・これらの仕組みについての文書化のレベルはB以上<br>・対策の検討レベルについてはB以上 |
| レベル2 | セキュリティ対策としては十分ではないがシステムによってはある程度許容できるレベル。<br>・最低限必要なOSのセキュリティ対策ができている<br>・接続用ユーザアカウントは管理者用権限を付与されていない<br>・セキュリティ対策の実装についての文書化のレベルはC以上 |
| レベル1 | RDBMSでのセキュリティは考慮されていない。<br>・レベル2の達成要件も満たしていない |

### 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 |
|---|---|

| 強度<br>レベル | 当該レベル達成要件 |
|---|---|
| レベル<br>5 | 通信に対する保護基準が確立しており、個々の通信に対する保護要件は、この基準に沿って組織的な検討の下で決められており、通信に対する保護要件の指定に不備が入り込むことは、まず考えられない。<br>・完成度の高い通信の保護基準（注 1）が確立している<br>・すべての通信（群）について、組織的で徹底した検討ならびにレビューの下で、保護基準にのっとった保護要件の指定が行われている<br>・すべての通信路、装置に対する物理的保護は、それぞれがサポートするすべての通信の保護要件を満たしていることが確認されている。特に、重要な通信路や装置に対しては、通常手段では通信の横取りができないような物理的な保護策が講じられている<br>・特に重要とした通信に対しては、最高水準の技術を駆使した盗聴、暗号解読、改ざん、なりすましには対抗できる手段（注2）の提供が要求されている<br>・比較的重要とした通信に対しては、一般的に知られている技術を使った盗聴、暗号解読、改ざん、なりすましには対抗できる手段（注3）の提供が要求されている<br>・その他の保護対象通信のすべてに対しても、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、なりすましに対する対抗策として一般的に適用を検討すべき手段（注4）の提供が要求されている<br>・通信に対する保護要件の指定プロセスおよびその管理の仕組みが確立しており、保護要件の指定はこの仕組みに沿って行われ十分に管理されている<br>・通信の保護基準についての検討のレベルはクラス A<br>・通信の保護基準や個々の通信（群）に対して指定している保護要件についての見直し状況はクラス A<br>・通信に対する保護要件の指定についての文書化のレベルはクラス A |
| レベル<br>4 | 通信に対する保護基準が確立しており、個々の通信に対する保護要件は、この基準に沿って組織的な検討の下で決められているが、徹底さを欠くところもあり、通信に対する保護要件の指定に不備が入り込む隙が、僅かではあるが残されている。<br>・よく検討された通信の保護基準（注 1）が確立している<br>・すべての通信（群）について、組織的な検討ならびにレビューの下で、保護基準にのっとった保護要件の指定が行われているが、検討の対象や検討のレベルあるいはレビューに、徹底さを欠くところも見られる<br>・特に重要とした通信に対しては、最高水準の技術を駆使した盗聴、暗号解読、改ざん、なりすましには対抗できる手段（注2）の提供が要求されている<br>・比較的重要とした通信に対しては、一般的に知られている技術を使った盗聴、暗号解読、改ざん、なりすましには対抗できる手段（注3）の提供が要求されている<br>・その他の保護対象通信のすべてに対しても、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、なりすましに対する対抗策として一般的に適用を検討すべき手段（注4）の提供が要求されている<br>・通信に対する保護要件の指定プロセスおよびその管理の仕組みが確立しており、保護要件の指定はこの仕組みに沿って行われ管理されているが、管理に徹底さを欠くところも見られる<br>・通信の保護基準についての検討のレベルはクラス A<br>・通信の保護基準や個々の通信（群）に対して指定している保護要件についての見直し状況はクラス A<br>・通信に対する保護要件の指定についての文書化のレベルはクラス B 以上 |
| レベル<br>3 | 大まかではあるが通信に対する保護基準が示されており、個々の通信に対する保護要件は、この基準に沿って組織的な検討の下で決められているが、検討やそのレビューは徹底したものではなく、これらについての管理もそう厳格でない。通信に対する保護要件の指定に不備が入り込む余地が残されている。<br>・おおまかではあるが通信の保護基準（注 1）が示されている<br>・すべての通信（群）について、組織的な検討ならびにレビューの下で、保護基準にのっとった保護要件の指定が行われているが、検討の対象や検討のレベルあるいはレビューに、徹底さを欠くところも |

| | |
|---|---|
| | 見られる<br>・重要としている通信に対しては、一般的に知られている技術を使った盗聴、暗号解読、改ざん、なりすましには対抗できる手段（注3）の提供が要求されている<br>・その他の保護対象の通信に対しても、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、なりすましに対する対抗策として一般的に適用を検討すべき手段（注4）の提供が要求されている<br>・大まかではあるが、通信に対する保護要件の指定プロセスおよびその管理の仕組みも示されており、保護要件の指定はこの仕組みに沿って行われ管理されているが、厳格な管理は行われていない<br>・通信の保護基準についての検討のレベルはクラスＢ以上<br>・通信の保護基準や個々の通信（群）に対して指定している保護要件についての見直し状況はクラスＢ以上<br>・通信に対する保護要件の指定についての文書化のレベルはクラスＢ以上 |
| レベル2 | 担当者間に共有されている通信に対する保護についての考え方が存在し、個々の通信に対する保護要件は、担当チームで決められ、概ね、適切に行われてはいるが、検討やレビューは担当チーム内に止まっており、組織的な管理は行われてないため、通信に対する保護要件の指定に不備が入り込む可能性は、少なくない。<br>・担当チーム内では、通信の保護についての考え方は共有されている<br>・重要な通信（群）については、チーム内でのレビューは行われているが、その他のものについては担当者任せとなっている<br>・重要な通信に対しては比較的高い水準が指定されているが、その他のものについては特に指定は行われていない<br>・指定されている通信の保護は、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、なりすましに対する対抗できるレベルに止まっている<br>・個々の通信（群）に対して指定している保護要件についての見直し状況はクラスＣ以上<br>・通信に対する保護要件の指定についての文書化のレベルはクラスＣ以上 |
| レベル1 | 通信に対する保護要件の指定はすべて担当者任せで、組織的な管理は行われていない。<br>・レベルの達成条件も満たせない |

(注1) 通信の保護基準として指定すべき事項
- ・保護レベル（通信の重要性にかかわりきまる保護の厳格性のレベル）
- ・保護レベルの適用基準（各保護レベルが適用される通信の特性等）
  - －通信に含まれる情報の重要度
  - －盗聴、改ざん、否認等の通信上でのトラブルが生じた場合の影響度
  - －提供する通信の代表例
- ・実施すべき保護策のレベル（指定すべき事項例）
  - －必要とする物理的な保護策のレベル
  - －適用可能な通信路と通信方式
  - －識別・認証のレベル
  - －暗号化のレベル
  - －電子証明、タイムスタンプの適用
  - －不正機器接続防止策の要否

(注2) 最高水準の技術を駆使した盗聴、暗号解読、改ざん、なりすましには対抗できる手段としての検討対象
- ・通信路、装置全般に対する通常手段では通信の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）、自動復旧技術、認証技術の使用
- ・最高水準の暗号技術の使用
- ・通信路に対する不正行為の検出手段

(注3) 一般的に知られている技術を使った盗聴、暗号解読、改ざん、なりすましには対抗できる手段としての検討対象
- ・通信路、装置全般に対する専用線レベルでの物理的な保護
- ・比較的強度が高い改ざん防止（検知）、自動復旧技術、認証技術の使用
- ・強度の高い暗号技術の使用

・通信路に対する不正行為の検出手段

(注4) 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、なりすましに対する対抗策として一般的に適用を検討すべき手段としての検討対象
・専用通信回線あるいは閉域網サービスの利用
・SSL 等の比較的簡単に用いることができる暗号化
・電子署名の利用

## Tb6.2 保護要件にあった通信路の選択とその適切な使用

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 個々の通信に使用されている通信路や通信方式や適用している暗号化他の保護策は、すべての保護対象の通信について、指定された保護要件を満たすものであり、これらのシステムへの実装も的確であることが確認されている。通信に求められている保護に問題が生じることは、まず考えられない。<br>・すべての保護対象の通信について、適用する保護策(注1)が組織的な検討、レビューの下で決められ、これらは当該通信に指定されている保護要件をすべて満足するものであることが確認されている<br>・保護対象のすべての通信についてのこれらの実装も、すべての対策場所(注2)について、組織的な徹底したチェックにより的確であり、期待通り機能していることが確認されている<br>・重要な通信路や装置に対しては、通常手段では通信の横取りができないような物理的な保護策が講じられている<br>・最高水準の技術を駆使した盗聴、暗号解読、改ざん、なりすましには対抗できる手段が、それらが必要な通信に実装されている<br>・一般的に知られている技術を使った盗聴、暗号解読、改ざん、なりすましには対抗できる手段が、それらが必要な通信に実装されている<br>・一般の通信のすべてに対しても、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、なりすましに対する対抗策として、一般的に適用を検討すべき手段が実装されている<br>・通信の保護策の実装についての定期的な点検、見直しも徹底して行われている<br>・通信の保護策にかかる実装の状況についての文書化のレベルはクラス A |
| レベル4 | 個々の通信に使用されている通信路や通信方式や適用している暗号化他の保護策は、すべての保護対象の通信について、指定された保護要件を満たすようにしているが、これらのシステムへの実装の確認に一部徹底さを欠くところも見られ、通信に求められている保護に問題が生じる隙が、僅かではあるが残されている。<br>・すべての保護対象の通信について、適用する保護策(注1)が組織的な検討、レビューの下で決められているが、一部に通信については、その的確性の確認に徹底さを欠くところも見られる<br>・保護対象のすべての通信についてのこれらの実装も、すべての対策場所(注2)について、組織的なチェックが行われているが、そのチェックに、一部、徹底さを欠くところも見られる<br>・重要な通信路や装置に対しては、通常手段では通信の横取りができないような物理的な保護策が講じられている<br>・最高水準の技術を駆使した盗聴、暗号解読、改ざん、なりすましには対抗できる手段が、それらが必要な通信に実装されている<br>・一般的に知られている技術を使った盗聴、暗号解読、改ざん、なりすましには対抗できる手段が、それらが必要な通信に実装されている<br>・一般の通信のすべてに対しても、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、なりすましに対する対抗策として、一般的に適用を検討すべき手段が実装されている<br>・通信の保護策の実装についての定期的な点検、見直しも徹底して行われている<br>・通信の保護策にかかる実装の状況についての文書化のレベルはクラス B 以上 |
| レベル3 | 特に保護が必要な通信に対しては、一般に知られている技術を使った盗聴、暗号の解読、かいざん、なりすましに対する対抗策が、その他の保護対象の通信に対しては一般的に適用を検討すべき手段(注3)が実装されるようになっているが、その確認は徹底したものではなく、不備が見逃される可能性も残されている。<br>・重要でない通信の一部を除く保護対象の通信について、適用する保護策(注1)が組織的な検討、レ |

| | |
|---|---|
| | ビューの下で決められているが、対象とする通信の網羅性やその的確性の確認は徹底したものではない<br>・重要でない通信の一部を除く保護対象のすべての通信についてのこれらの実装も、すべての対策場所（注2）について、組織的なチェックが行われているが、対象とする通信や実施しているチェックは徹底したものではない<br>・一般的に知られている技術を使った盗聴、暗号解読、改ざん、なりすましには対抗できる手段が、それらが必要な通信に実装されている<br>・一般の通信のすべてに対しても、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、なりすましに対する対抗策として、一般的に適用を検討すべき手段が実装されている<br>装されているかどうかの確認は徹底していない<br>・通信の保護策の実装についての定期的な点検、見直しも、年に１回以上行われている<br>・通信の保護策にかかる実装の状況についての文書化のレベルはクラスＢ以上 |
| レベル2 | 通信への保護策のシステムへの展開は担当者に任されており、組織的な管理は行われているないが、担当者レベルでは、習慣的に形成されたチェックの仕組みが機能しており、担当者レベルで以下のような施策は、概ね、適切に実施している。重要な通信に対する基本的な保護は、概ね、適切に行われていると見ることができるが、全体としての信頼性は十分とは言えない。<br>・担当者チームは、保護策の検討や実装についての確認を、習慣的に形成されたプロセスの中で行っている<br>・特に重要と見た通信に対しては、一般的に知られている技術を使った盗聴、暗号解読、改ざん、なりすましには対抗できる手段が、実装している<br>・保護の対象と見た通信に対しては、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、なりすましに対する対抗策として、一般的に適用を検討すべき手段が実装している<br>・通信の保護策にかかる実装の状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | 通信への保護策のシステムへの展開は、すべて担当者に任されており、その実態はほとんど管理されていない。<br>・レベル2の達成条件も満たせない |

(注１) 保護対象となる通信に対する保護策として検討すべき事項
- ・通信路およ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）
- ・通信路の選択
- ・通信方式
- ・暗号化
- ・識別／認証の方式
- ・電子署名やタイムスタンプの適用法
- ・不正ソフトウェア対策（スパイウェア、スニファ対策他）
- ・アプリケーションに組み込むべき対策

(注2) 通信の保護策が組込まれる場所
- ・通信路
- ・通信装置
- ・通信ソフト
- ・アプリケーション

## Tb6.3 無線 LAN の使用についてのセキュリティ対策の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 無線 LAN の使用による通信の保護やシステムへの不正なアクセスを防ぐため、現時点で、とりうるすべての手段が的確に講じられていて、無線 LAN の使用で問題が生じることは、まず考えられない。<br>・特に重要な情報を扱う通信については、無線 LAN の使用は原則として禁止され、その使用については厳しい条件（注1）が付けられている<br>・利用者の不正な無線 LAN 利用を防止するため、常時監視や、コンピュータ上で無線 LAN が利用できなくするような措置を講じている<br>・無線 LAN の使用が許されない領域に対し、物理的に、無線ＬＡＮ機器を接続できないような機構（認証 VLAN など）を導入するか、無線ＬＡＮアクセスポイント不正設置を常時監視し、必要に応じて強制的に排除できるような対策を導入している<br>・無線 LAN の安全を充分に確保するために、最新の技術水準にてらして最も高いレベルの保護策（注2）を導入している<br>・屋外や域外の不正アクセスポイントへの誘導を防止するため、電波の遮蔽措置、もしくはなんらかの監視、接続防止手段を導入している<br>・必要に応じ、屋外への電波漏洩、もしくは屋外からの電波混入の影響の防止策を講じている<br>・無線ＬＡＮ接続機器への利用ポリシーを強制するツールの導入<br>・定期的に無線 LAN の利用状況および不正利用の有無についての調査を実施している<br>・無線 LAN の利用者に対する無線 LAN の安全な利用について教育を定期的に実施している<br>・無線 LAN の使用の認可と使用環境の管理についての厳格な仕組みが確立している<br>・無線 LAN の使用の認可は、この仕組みに沿って厳格に審査されている<br>・無線 LAN の使用実態が認可条件に準拠しているかどうかについてのチェックも、この仕組みの下で厳格に行われている<br>・無線 LAN の使用に関するセキュリティ対策についての見直し状況はクラス A<br>・無線 LAN の使用に関するセキュリティ対策やその実践状況についての文書化のレベルはクラス A |
| レベル4 | 無線 LAN の使用による通信の保護やシステムへの不正なアクセスを防ぐため、現時点で、とりうるすべての手段を講じているが、これらのシステムへの実装の確認に一部徹底さを欠くところも見られ、無線 LAN の使用で問題が生じる隙が、僅かではあるが残されている。<br>・無線ＬＡＮの使用は必要最小限に制限されており、、その使用については厳しい条件（注1）が付けられている<br>・最新の技術水準に照らした盗聴、攻撃手段に対しても、相当に対抗できる対抗手段（注2）を講じている<br>・屋外や域外の不正アクセスポイントへの誘導を防止するため、電波の遮蔽措置、もしくはなんらかの監視、接続防止手段を導入している<br>・必要に応じ、屋外への電波漏洩、もしくは屋外からの電波混入の影響の防止策を講じている<br>・無許可の無線ＬＡＮ機器を監視するツールの導入による不正利用の監視を行っている<br>・無線ＬＡＮ接続機器への利用ポリシーを強制するツールの導入している<br>・定期的に無線 LAN の利用状況および不正利用の有無についての調査を実施している<br>・無線 LAN の利用者に対する無線 LAN の安全な利用について教育を定期的に実施している<br>・無線 LAN の使用の認可と使用環境の管理についての厳格な仕組みが確立している<br>・無線 LAN の使用の認可は、この仕組みに沿って、概ね、厳格に審査されている<br>・無線 LAN の使用実態が認可条件に準拠しているかどうかについてのチェックも、この仕組みの下で行われているが、一部に徹底さに欠けるところも見られる<br>・無線 LAN の使用に関するセキュリティ対策についての見直し状況はクラス A<br>・無線 LAN の使用に関するセキュリティ対策やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル3 | 無線 LAN の危険性を十分に承知し、組織的な検討の下、無線 LAN の使用による通信の保護やシステムへの不正なアクセスを防ぐため手段が講じられているが、これらの手段は、容易に入手可能な盗聴や、一般的によく知られている攻撃手段に対抗できるレベルに止まっている。また、その実装の確認も徹底したものではない。無線 LAN の使用で問題が生じる可能性も、残されている。<br>・最新の技術水準に照らし、比較的容易に利用が可能な盗聴、攻撃手段に対して、最低限必要な対抗 |

| | |
|---|---|
| | 手段(注3)を講じている<br>・無線 LAN の利用者に対する無線 LAN の安全な利用について教育を定期的に実施している<br>・実施策の検討レベルは B 以上<br>・必要に応じた実施策の見直しのレベルは B 以上<br>・規程類の文書化のレベルは B 以上 |
| レベル 2 | 無線LANの安全な使用に対して必要となる措置は、担当チームに任されており、組織的な管理は行われていないが、担当チームにおける無線LANの使用の安全について努力は見られる、十分には程遠いが、最低限実施すべきことは展開されている。<br>・少なくとも WEP による暗号化は実施している<br>・無線 LAN の利用者に対する一般的な利用上の注意事項の周知努力は実施している。<br>・無線LANの使用のかかるセキュリティ対策についての文書化のレベルは C 以上 |
| レベル 1 | 無線 LAN について有効な対策は取られていない |

(注1) 無線LANの使用制限として検討すべき事項
- ・利用目的(利用業務)と利用者
- ・利用者における無線LAN利用上の制約
  - －公衆無線アクセスポイントの利用の禁止
  - －その他の無線LAN使用上の一般的なセキュリティ面での注意事項

(注2) 最新の技術水準に照らした盗聴、攻撃手段に対しても、相当に対抗できる対抗手段の例
- ・SSIDの推測が困難な値への設定と、SSID放送の抑止
- ・少なくともWPA／TKIPを利用、AES256ビット以上の暗号鍵での暗号化と、比較的高いサイクルでの暗号鍵の変更
- ・EAP 認証の適用

(注3) 比較的容易に利用が可能な盗聴、攻撃手段に対して、最低限必要な対抗手段の例
- ・デフォルト値でのSSIDの変更と、SSID放送の抑止
- ・少なくとも 128 ビット以上の鍵長のWEPの使用と、暗号鍵の定期的な変更
- ・MAC アドレスによる接続制限
- ・必要に応じた EAP 認証の使用

### 3.2.7. 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

| 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 電子メールの使用において情報の漏洩事故を起こさないようにするために、現時点で、とりうるすべての手段が的確に講じられていて、その運用も徹底しており電子メールの使用で問題が生じることは、まず考えられない。<br>・特に秘密性の高い情報に対してはインターネットを経由する電子メールの利用およびインターネットを経由したメールの閲覧を禁止している。<br>・組織内の電子メールについても、本文を含め最新の技術水準にてらして最高レベルの強度を持つ暗号を使用して暗号化を行うと同時に、発信者の身元を明らかにし、改ざん、否認を防止するための電子署名やタイムスタンプを併用している。電子署名等に使用するアルゴリズムについても最新の技術水準に照らして最高レベルの強度を持つものを使用している。<br>・本対策要求についての検討のレベルはクラスA<br>・本対策要求かかる指定された措置の実践に対する管理の仕組みの確立状況はクラスA<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスA<br>・電子メールの安全な使用についての対策についての見直し状況はクラスA<br>・電子メールの使用に関する規程等についてのについての文書化のレベルはクラスA |
| レベル4 | 電子メールの使用において情報の漏洩事故を起こさないようにするために、現時点で、とりうるすべての手段を講じているが、これらのシステムへの実装の確認に一部徹底さを欠くところも見られ、電子メールの使用で問題が生じる隙が、僅かではあるが残されている。<br>・インターネット、組織内を問わず、電子メールは本文を含め、最新の技術水準に照らして最高レベルの強度を持つ暗号を使用して暗号化を行っている<br>・重要な情報を含むメールについては、通信相手の身元確認や改ざんや否認を防止するための電子署名や、必要に応じてタイムスタンプを使用している。また、電子署名に使用するアルゴリズムについても最新の技術水準にてらして最高レベルの強度を持つものとする<br>・安全が確保できないネットワークを経由したメールの閲覧においては、適切な強度のVPNもしくはSSL等の暗号通信（電子メールの暗号強度に相当するレベルのもの）を使用している<br>・フリーメール、自組織以外が運営する Web メール等、一般のインターネットプロバイダなどのメールアカウントの利用を禁止している<br>・本対策要求についての検討のレベルはクラスB<br>・本対策要求かかる指定された措置の実践に対する管理の仕組みの確立状況はクラスB以上<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスB以上<br>・電子メールの安全な使用についての対策についての見直し状況はクラスB以上<br>・電子メールの使用に関する規程等についてのについての文書化のレベルはクラスB以上 |
| レベル3 | 電子メールの危険性を十分に承知し、組織的な検討の下、電子メールの使用において情報の漏洩事故を起こさないようにするため手段が講じられているが、採用している手段は平均的なもので、その運用も徹底しているとは言えず、電子メールの使用にかかわり問題が生じる可能性も、残されている。<br>・電子メールの利用者に、電子メールの使用にあたって注意すべき事項（注 1）を示し、その遵守を求めている。管理や指導も行われているが、徹底したものではない<br>・本対策要求についての検討のレベルはクラスB<br>・本対策要求かかる指定された措置の実践に対する管理の仕組みの確立状況はクラスB以上<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスB以上<br>・電子メールの安全な使用についての対策についての見直し状況はクラスB以上<br>・電子メールの使用に関する規程等についてのについての文書化のレベルはクラスB以上 |
| レベル2 | 一般的な電子メール利用上の注意点についての、ユーザへの教育は行われているが、具体的な情報保護の方法などについては、特に明示しておらず、個々の判断に委ねられている。<br>・電子メールの使用に関する注意事項についての文書化のレベルはC以上 |
| レベル1 | 電子メール使用に関する保護措置はほとんど実施されていない |

(注1) 電子メールの使用にあたって利用者が注意すべきこと

・インターネットを経由するメールについて漏洩の影響が大きい情報を含むものについては本文を含め暗号化すること
・止むを得ず平文メールに重要情報を含むファイルを添付するような場合は、ファイル自体を暗号化したり、アプリケーションの機能によるパスワード保護や暗号化の機能を使用して、安全性を高めること
・平文の本文には機微な内容は書かないように注意する。必要な場合は添付ファイル文書として、別途保護手段を講じること
・フリーメール、自組織以外が運営するWebメール等については、前項の条件を満たすと満たさざるとにかかわらず、利用してはならないこと、一般のインターネットプロバイダのメールアカウント利用の際は、メールサーバ上でメールを保存しないように留意すること

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | インターネット経由でのファイル転送についての安全確保は徹底しており、ファイル転送により情報漏洩等の事故が起きることは、まず考えられない。<br>・保護対象の情報が含まれるファイルについては、安全が確保されていないネットワーク（注1）経由でのファイル転送は、原則禁止とし、使用は厳しく制限されている<br>・ファイル転送の利用は、認可された相手との指定された伝送路のみで行っている<br>・利用が許されたファイル転送は、ファイルを現時点では最も強度が高いとされている暗号化や電子署名、およびタイムスタンプを適用している<br>・ファイル転送の利用についての管理の仕組みが確立している<br>・安全が確保されていないネットワーク（注1）経由でのファイル転送は、この仕組みに沿って認可され、その実行は厳しく管理されている<br>・ファイル転送の利用の安全の確保についての検討のレベルはクラスA<br>・ファイル転送の利用についての安全対策についての見直し状況はクラスA<br>・ファイル転送の利用についての安全対策やその実践状況についての文書化のレベルはクラスA |
| レベル4 | インターネット経由でのファイル転送についての安全確保の徹底は図られているが、一部に徹底さを欠くところも見られる。ファイル転送により情報漏洩等の事故が起きる隙が、僅かではあるが残されている。<br>・保護対象の情報が含まれるファイルについては、安全が確保されていないネットワーク（注1）経由でのファイル転送は、原則禁止とし、使用は厳しく制限されている<br>・ファイル転送の利用は、認可された相手との指定された伝送路のみで行っている<br>・利用が許されたファイル転送は、ファイルを現時点では相当に強度が高いとされている暗号化や電子署名を適用している<br>・ファイル転送の利用についての管理の仕組みが確立している<br>・安全が確保されていないネットワーク（注1）経由でのファイル転送は、この仕組みに沿って認可され、その実行は管理されているが、徹底さに欠けるところも見られる<br>・ファイル転送の利用の安全の確保についての検討のレベルはクラスB以上<br>・ファイル転送の利用についての安全対策についての見直し状況はクラスB以上<br>・ファイル転送の利用についての安全対策やその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | インターネット経由でのファイル転送についての安全確保についての追求は行われているが、徹底したものではなく、ファイル転送により情報漏洩等の事故が起きる余地も残されている。<br>・安全が確保されていないネットワーク（注1）経由でのファイル転送の使用は、原則禁止され、許可制となっている<br>・ファイル転送の利用は、認可された相手とのみ許されている<br>・利用が許されたファイル転送は、重要なファイルを場合は、適度の強度の暗号化や電子署名を適用することを原則としているが、一部については、アプリケーションによるパスワードの保護、簡易暗号化、パスワード付き圧縮等が用いられているが、いずれにせよ情報の保護は実施されている |

| | |
|---|---|
| | ・大まかではあるが、ファイル転送の利用についての管理の仕組みは示されている<br>・安全が確保されていないネットワーク（注1）経由でのファイル転送は、この仕組みに沿って認可され、その実行は管理されているが、徹底したものではない<br>・ファイル転送の利用の安全の確保についての検討のレベルはクラスB以上<br>・ファイル転送の利用についての安全対策についての見直し状況はクラスB以上<br>・ファイル転送の利用についての安全対策やその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | インターネット経由でのファイル転送の安全な使用に対して必要となる措置は、担当チームに任されており、組織的な管理は行われていないが、担当チームにおけるインターネット経由でのファイル転送の使用の安全について努力は見られる、十分には程遠いが、最低限実施すべきことは展開されている。<br>・保護すべきファイル転送は関係者に承知されている<br>・転送するファイルの暗号化等は習慣的に行われている<br>・インターネット経由でのファイル転送の安全な使用について注意事項は、その利用者に示されている<br>・インターネット経由でのファイル転送の安全な使用についての文書化のレベルはＣ以上 |
| レベル1 | ファイル転送による情報交換における保護措置は、全て担当者任せで管理されていない。<br>・レベル2の達成条件も満たせない |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | アクセス集中を考慮したシステム設計が行き届いており、計画した対策のシステムへの組込みも的確であることが常に維持されている。また、アクセス集中による意図的なサービス妨害にさらされても、対処能力も十分で、最悪の事態でも必要最小限の業務の継続はできるようになっており、アクセス集中を用いたサービス妨害に対する備えは、万全に近いと言える。<br>・使用機器（サーバ、ネットワーク機器、セキュリティ機器）の性能面での余裕確保では、複数の代替機器の準備や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）が行われている。<br>・ネットワークについての余裕の確保では、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なっている。また、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している。<br>・アクセス集中検知、緩和手段については、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っている。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、自動的に接続制限したり、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が導入されている。<br>・アクセス状況は適宜調査されていて、定期的に最新の調査をもとに、設計の見直しが行われている。<br>・アクセス集中発生時における対象要領が確立しており、マニュアル化されている<br>・アクセス集中への対処にかかわる者にこの要領は徹底されており、また、訓練も適宜行われており、関係者は何時でも必要な措置が迅速に取れる<br>・アクセス集中への備えについての検討のレベルはクラス A<br>・アクセス集中への備えとして指定された措置の実践に対する管理の仕組みの確立状況と、それらの実践と管理の徹底状況はクラス A<br>・アクセス集中への備えについての見直し状況はクラス A<br>・アクセス集中への備えとして指定された措置やその実践状況についての文書化のレベルはクラス A |
| レベル4 | アクセス集中を考慮したシステム設計がよく検討されており、計画した対策のシステムへの組込みも的確であることが常に維持されているようにする努力も行われている。また、サービス妨害が発生した場合の対処能力の確保も、概ね十分で、最悪の事態でも制限は多いが、業務の継続はできるようになっ |

| | |
|---|---|
| | ている。アクセス集中を用いた意図的なサービス妨害に対しても、相当の対応ができると見られるが、まだ改善する余地も残る。<br>・使用機器（サーバ、ネットワーク機器、セキュリティ機器）の性能面での余裕確保では、少なくとも1台の代替機器の確保や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が行われている。<br>・ネットワークについての余裕の確保では、WAN 回線について、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なっている。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している。<br>・アクセス集中検知、緩和手段については、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っている。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接続制限などにより、負荷を軽減できる手段を用意している。<br>・アクセス集中発生時における対象要領が確立しており、マニュアル化されているが、まだ、改善の余地がある<br>・アクセス集中への対処にかかわる者にこの要領は徹底されており、また、訓練も適宜行われており、関係者は何時でも必要な措置が迅速に取れるようにする努力は行われているが、一部に徹底さに欠けるところもある<br>・アクセス状況は常時掌握されていて、定期的に最新の統計をもとに、設計の見直しが行われている。<br>・アクセス集中への備えについての検討のレベルはクラス B 以上<br>・アクセス集中への備えとして指定された措置の実践に対する管理の仕組みの確立状況と、それらの実践と管理の徹底状況はクラス B 以上<br>・アクセス集中への備えについての見直し状況はクラス B 以上<br>・アクセス集中への備えとして指定された措置やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル 3 | 重要な業務を守るための、システムの設計にはアクセス集中も考慮され、運用面では緊急時の対応等も検討されているが、いずれも徹底したものではなく、被害を限定的にできるある程度の備えである。<br>・使用機器（サーバ、ネットワーク機器、セキュリティ機器）の性能面での余裕確保では、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が行われている。<br>・ネットワークについての余裕の確保では、LAN 及び WAN の回線について、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している。<br>・アクセス集中検知、緩和手段については、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重要なネットワークについて用意している。重要なネットワークについては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接続制限などにより、負荷を軽減できる手段について検討または導入している。<br>・大まかではあるが、アクセス集中発生時における対処要領が示されている、基本的なところを示しているに止まっている<br>・アクセス集中への対処にかかわる者にこの要領は渡されているが、訓練等は特に行われていない<br>・アクセス状況は適宜調査されていて、定期的に最新の調査をもとに、設計の見直しが行われている。<br>・アクセス集中への備えについての検討のレベルはクラス B 以上<br>・アクセス集中への備えとして指定された措置の実践に対する管理の仕組みの確立状況と、それらの実践と管理の徹底状況はクラス B 以上<br>・アクセス集中への備えについての見直し状況はクラス B 以上<br>・アクセス集中への備えとして指定された措置やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル 2 | 使用機器の性能に多少の余裕を持たせてはいるが、それ以上の対策は考慮されていない。ただし、システムの運用チームは、サービス妨害と思われるアクセス集中が発生した場合における、最低限行うべき措置については承知している。<br>・攻撃に直接さらされる機器に、ある程度の性能的余裕は持たせている<br>・システムの運用関係者はサービス妨害と思われるアクセス集中が発生した時の現象、およびこのとき行うべき措置をある程度、承知している<br>・アクセス集中時への備えについての文書化のレベルは C 以上 |
| レベル 1 | アクセス集中に対する備えは、ほとんど意識されていない。 |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 現時点では最も強力と考えられる監視を実施しており、監視結果の取扱いは的確に行われており、ネットワークの動きに関し、対処が必要な事象を見逃す可能性は、まずない。<br>・監視の対象を、外部との通信および内部セグメント間の通信のすべてだけでなく、すべてのノードも対象にノードレベルでの通信も監視の対象としている<br>・監視は常時（365 日 24 時間）リアルタイムベースで実施<br>・攻撃の疑いのある通信（注 1）および情報の漏洩につながる可能性のある通信（注2）他の監視すべき通信や事象のすべてを監視の対象としている。特に脆弱性をついた攻撃の監視については、新たに報告された脆弱性に対して、3 日以内に対応ができるようになっている。<br>・未知の攻撃についてもある程度の検出もできる仕組みも使われている<br>・各種の監視情報を総合的に分析するための支援ツールも効果的に用いられている<br>・重要な事象については、検知から 15 分以内に警告が出されるようになっている<br>・監視結果の分析や統計的な報告は、翌朝には管理者に届けられるようになっている<br>・詳細な分析のための、監視データの詳細は 1 時間以内に向こう 1 ヶ月以内の閲覧可能にされている<br>・監視のための諸機能の実装やその維持管理は、定められた手順に沿って行われており、確認も徹底している<br>・監視は、自社内での専門チームによる監視に加え、専門会社のリアルタイムの監視支援サービスを受けており、外部の専門家と一体となった監視を行っている<br>・監視データの保管はルールに沿って厳格に行われている<br>・問題の検出時の措置や、監視結果の定例報告の取り扱いや、監視ツールの維持管理についてのプロセス確立しており、これらはチェックポイントとともマニュアル化されている<br>・ネットワークの動きに対する監視に関し実施すべきことの実践に対する管理は、定められた仕組みの沿って厳格に行われている<br>・ネットワークの動きに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラス A<br>・ネットワークの動きに対する監視の実践に対する管理の仕組みの確立状況はクラス A<br>・ネットワークの動きに対する監視についての見直し状況はクラス A<br>・ネットワークの動きに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラス A |
| レベル4 | 平均以上に徹底した監視を実施しており、監視結果の取扱いも適切に行われているが、監視結果への対応等に、レベル 5 に比べ劣るところがあるが、現時点では相当に強力な監視と見てよい。ネットワークの動きに関し、対処が必要な事象を見逃す可能性は、あまりない。<br>・監視の対象を、外部との通信および内部セグメント間の通信のすべてに加え、重要なノード間の通信も監視の対象としている<br>・監視は常時（365 日 24 時間）リアルタイムベースで実施<br>・攻撃の疑いのある通信（注 1）および情報の漏洩につながる可能性のある通信（注2）他の監視すべき通信や事象のすべてを監視の対象としている。特に脆弱性をついた攻撃の監視については、新たに報告された脆弱性に対して、3 日以内に対応ができるようになっている。<br>・未知の攻撃についてもある程度の検出もできる仕組みも使われている<br>・各種の監視情報を総合的に分析するための支援ツールも効果的に用いられている<br>・重要な事象については、検知から 15 分以内に警告が出されるようになっている<br>・監視結果の分析や統計的な報告は、翌朝には管理者に届けられるようになっている<br>・詳細な分析のための、監視データの詳細は 1 時間以内に向こう1ヶ月以内の閲覧可能にされている<br>・監視のための諸機能の実装やその維持管理は、定められた手順に沿って行われており、確認も徹底して行われているが、一部に徹底さを欠くところも見られる<br>・監視は、自社内でのレベルの高い専門チームによる監視、または専門会社のリアルタイムの監視支援サービスによって行われている。また、必要に応じ、何時でも外部の専門家の支援が受けられるよう |

| | |
|---|---|
| | になっている<br>・監視データの保管はルールに沿って、概ね厳格に行われている<br>・問題の検出時の措置や、監視結果の定例報告の取り扱いや、監視ツールの維持管理についてのプロセス確立しており、これらはチェックポイントとともマニュアル化されている<br>・ネットワークの動きに対する監視に関し実施すべきことの実践に対する管理は、定められた仕組みに沿って行われているが、一部に徹底さを欠くところも見られる<br>・ネットワークの動きに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラスB以上<br>・ネットワークの動きに対する監視の実践に対する管理の仕組みの確立状況はクラスB以上<br>・ネットワークの動きに対する監視についての見直し状況はクラスB以上<br>・ネットワークの動きに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | 平均的なシステムでは一般には必須とされる必要とされる監視を実施しており、監視結果の取扱いも概ね適切に行われている。それほど厳格なものではないが、レベル3のセキュリティを要求システムには必要な監視は行われているが、徹底したものではない。ネットワークの動きに関し、対処が必要な重要な事象を見逃す可能性も残されている。<br>・監視の対象を、外部との通信および内部セグメント間の通信のうち重要なセグメント間での通信としている<br>・監視は常時（365日24時間）リアルタイムベースで実施<br>・攻撃の疑いのある通信（注1）および情報の漏洩につながる可能性のある通信（注2）他の監視すべき通信や事象のすべてを監視の対象としている。特に脆弱性をついた攻撃の監視については、新たに報告された脆弱性に対して、3日以内に対応ができるようになっている。<br>・重要な事象については、検知から1時間以内に警告が出されるようになっている<br>・月ベースで、監視結果の分析や統計的な報告がなされている<br>・詳細な分析のための、監視データの詳細は1日以内に向こう1ヶ月以内の閲覧可能にされている<br>・監視のための諸機能の実装やその維持管理は、定められた手順に沿って行われており、その機能確認も行われているが、そう徹底したものではない<br>・監視は、自社内での専門チームにより行われており、担当者はある程度のスキルを有している<br>・監視データの保管はルールに沿って行われている<br>・大まかではあるが、問題の検出時の措置や、監視結果の定例報告の取扱いや、監視ツールの維持管理についてのプロセス確立しており、これらはチェックポイントとともマニュアル化されている<br>・ネットワークの動きに対する監視に関し実施すべきことの実践に対する管理は、定められた仕組みに沿って行われているが、そう厳格には管理されていない<br>・ネットワークの動きに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラスB以上<br>・ネットワークの動きに対する監視の実践に対する管理の仕組みの確立状況はクラスB以上<br>・ネットワークの動きに対する監視についての見直し状況はクラスB以上<br>・ネットワークの動きに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | リアルタイムの監視は使用するツールが一般に提供している機能レベルで、監視は、生じた問題の分析のためのログの取得に重点が置かれており、最低限必要なログは取得され、保管されているが、組織的な管理はされていない。<br>・監視の対象は、外部との通信および内部セグメント間の通信のうち重要なセグメント間での通信としている<br>・通信制御機器が提供するログ取得機能を活用したログの取得は実施<br>・通信ログの保管は担当チーム内で形成された習慣に沿って行われている<br>・問題が生じた場合は、専門家の支援をうるようにしている<br>・ネットワークの動きに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラスC以上<br>・ネットワークの動きに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラスC以上 |
| レベル1 | 通信制御機器の提供する監視機能は使われてはいても、収集したログの分析や管理はほとんど行われてなく、ネットワークの動きに対する監視についての組織的な取組みはないに等しい<br>・レベル2の達成要件も満たしていない |

(注 1) 一般に監視の対象とすべき攻撃の疑いのある事象や通信
・スキャン行為
・認証の失敗
・DoS 攻撃とみなされる通信
・システムの脆弱性をついた攻撃とみなされる通信
・バックドアを用いた攻撃とみなされる通信

(注2) 監視の対象とすべき情報の漏洩につながる可能性がある通信
・チャットや Web メール、SQL 接続
・その他の当該組織が禁止しているネットワークサービス

## Tb9.2 システムへのアクセスについての監視の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムへのアクセスについて、現時点では最も強力と考えられる監視を実施しており、監視結果の取扱いは的確に行われており、システムへのアクセスに関し、対処が必要な事象を見逃す可能性は、まずない。<br>・すべてのサーバおよび特に監視が必要とするクライアントサーバのすべてを監視の対象としている<br>・監視は常時（365 日 24 時間）リアルタイムベースで実施で、不審な<br>・攻撃の疑いのあるアクセス（注 1）他の監視すべき通信や事象のすべてを監視の対象としている。特に脆弱性をついた攻撃の監視については、新たに報告された脆弱性に対して、3 日以内に対応ができるようになっている。<br>・未知の攻撃についてもある程度の検出もできる仕組みも使われている<br>・監視結果の分析や報告を支援するツールも効果的に用いられている<br>・重要な事象については、検知から 15 分以内に警告が出されるようになっている<br>・監視結果の分析や統計的な報告は、翌朝には管理者に届けられるようになっている<br>・詳細な分析のための、監視データの詳細は 1 時間以内に向こう 1 ヶ月以内の閲覧可能にされている<br>・監視のための諸機能の実装やその維持管理は、定められた手順に沿って行われており、確認も徹底している<br>・監視は、自社内での専門チームによる監視に加え、専門会社のリアルタイムの監視支援サービスを受けており、外部の専門家と一体となった監視を行っている<br>・アクセスログの保管やバックアップの取得はルールに沿って厳格に行われている<br>・問題の検出時の措置や、監視結果の定例報告の取り扱いや、監視ツールの維持管理についてのプロセス確立しており、これらはチェックポイントとともマニュアル化されている<br>・システムへのアクセスに対する監視に関し実施すべきことの実践に対する管理は、定められた仕組みの沿って厳格に行われている<br>・システムへのアクセスに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラス A<br>・システムへのアクセスに対する監視の実践に対する管理の仕組みの確立状況はクラス A<br>・システムへのアクセスに対する監視についての見直し状況はクラス A<br>・システムへのアクセスに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラス A |
| レベル4 | システムへのアクセスについて、平均以上に徹底した監視を実施しており、監視結果の取扱いも適切に行われているが、監視結果への対応等に、レベル 5 に比べ劣るところがいる。現時点では相当に強力な監視と見てよい。システムへのアクセスについてに関し、対処が必要な事象を見逃す可能性は、あまりない。<br>・監視の対象を、外部との通信および内部セグメント間の通信のすべてに加え、重要なノード間の通信も監視の対象としている |

| | |
|---|---|
| | ・監視は常時（365 日 24 時間）リアルタイムベースで実施<br>・攻撃の疑いのある通信（注 1）および情報の漏洩につながる可能性のある通信（注2）他の監視すべき通信や事象のすべてを監視の対象としている。特に脆弱性をついた攻撃の監視については、新たに報告された脆弱性に対して、3 日以内に対応ができるようになっている。<br>・未知の攻撃についてもある程度の検出もできる仕組みも使われている<br>・各種の監視情報を総合的に分析するための支援ツールも効果的に用いられている<br>・重要な事象については、検知から 15 分以内に警告が出されるようになっている<br>・監視結果の分析や統計的な報告は、翌朝には管理者に届けられるようになっている<br>・詳細な分析のための、監視データの詳細は 1 時間以内に向こう1ヶ月以内の閲覧可能にされている<br>・監視のための諸機能の実装やその維持管理は、定められた手順に沿って行われており、確認も徹底して行われているが、一部に徹底さを欠くところも見られる<br>・監視は、自社内でのレベルの高い専門チームによる監視、または専門会社のリアルタイムの監視支援サービスによって行われている。また、必要に応じ、何時でも外部の専門家の支援が受けられるようになっている<br>・監視データの保管はルールに沿って、概ね厳格に行われている<br>・問題の検出時の措置や、監視結果の定例報告の取り扱いや、監視ツールの維持管理についてのプロセス確立しており、これらはチェックポイントとともマニュアル化されている<br>・ネットワークの動きに対する監視に関し実施すべきことの実践に対する管理は、定められた仕組みの沿って行われているが、一部に徹底さを欠くところも見られる<br>・ネットワークの動きに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラス B 以上<br>・ネットワークの動きに対する監視の実践に対する管理の仕組みの確立状況はクラス B 以上<br>・ネットワークの動きに対する監視についての見直し状況はクラス B 以上<br>・ネットワークの動きに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル 3 | システムへのアクセスについて、平均的なシステムでは一般には必要とされる監視を実施しており、監視結果の取扱いも概ね適切に行われている。それほど厳格なものではないが、レベル3のセキュリティを要求システムには要求される監視は行われており、システムへのアクセスについて、対処が必要な重要な事象を見逃す可能性は、あまりない。<br>・監視の対象を、外部との通信および内部セグメント間の通信のうち重要なセグメント間での通信としている<br>・監視は常時（365 日 24 時間）リアルタイムベースで実施<br>・攻撃の疑いのある通信（注 1）および情報の漏洩につながる可能性のある通信（注2）他の監視すべき通信や事象のすべてを監視の対象としている。特に脆弱性をついた攻撃の監視については、新たに報告された脆弱性に対して、3 日以内に対応ができるようになっている。<br>・重要な事象については、検知から 1 時間以内に警告が出されるようになっている<br>・月ベースで、監視結果の分析や統計的な報告がなされている<br>・詳細な分析のための、監視データの詳細は 1 日以内に向こう1ヶ月以内の閲覧可能にされている<br>・監視のための諸機能の実装やその維持管理は、定められた手順に沿って行われており、その機能確認も行われているが、そう徹底したものではない<br>・監視は、自社内での専門チームにより行われており、担当者はある程度のスキルを有している<br>・監視データの保管はルールに沿って行われている<br>・大まかではあるが、問題の検出時の措置や、監視結果の定例報告の取扱いや、監視ツールの維持管理についてのプロセス確立しており、これらはチェックポイントとともマニュアル化されている<br>・ネットワークの動きに対する監視に関し実施すべきことの実践に対する管理は、定められた仕組みの沿って行われているが、そう厳格には管理されていない<br>・ネットワークの動きに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラス B 以上<br>・ネットワークの動きに対する監視の実践に対する管理の仕組みの確立状況はクラス B 以上<br>・ネットワークの動きに対する監視についての見直し状況はクラス B 以上<br>・ネットワークの動きに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル 2 | システムへのアクセスについては、システムが一般に提供している機能レベルで、監視は、生じた問題の分析のためのログの取得に重点が置かれている。取得したログの分析や保管は、システム運用チームに任されており、組織的な管理はされていない。 |

| | |
|---|---|
| | ･重要なサーバに対するログは、担当チーム内での習慣で管理されている<br>･問題が生じた場合、専門家の支援を受けることができるようになっている<br>･担当チームはログの分析についてある程度の知識を有している<br>･システムへのアクセスの監視についての検討のレベルはＣ以上<br>･システムへのアクセスの監視にかかる指定された措置やその実践状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | システムが提供しているログの取得機能は使われてはいても、収集したログの分析や管理はほとんど行われてなく、ネットワークの動きに対する監視についての組織的な取組みはないに等しい<br>･レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | アプリケーションへのアクセスについて、現時点では最も強力と考えられる監視を実施しており、監視結果の取扱いは的確に行われており、アプリケーションへのアクセスに関し、対処が必要な事象を見逃すことは、まず考えられない。<br>･重要なアプリケーションおよび重要な情報を扱うアプリケーションのすべてを監視の対象とし、そのそれぞれに組織的な検討の下で、アクセスに対する監視についての適切な要求が示されている<br>･これらのアプリケーションには必要なアクセス監視機能や必要に応じた改ざん防止措置が的確に実装されている<br>･アプリケーションへの不審なアクセスに対してはリアルタイムで警告が出されている<br>･これらのアプリケーションへのアクセスについては、後日の監査に必要なログがきめ細かく取得されている。<br>･取得した監査ログの保管、監査結果の分析等の監査ログの取扱いについて完成度の高い要領が確立していて、マニュアル化されている<br>･改ざん防止策を始め、収集したログの保全は、ルールの沿って行われ、その管理も徹底しており、万全と見てよい<br>･監査ログの分析はルールに沿って高い密度（頻度とチェックのレベル）で行われ、その管理も徹底している<br>･アクセスログの保管やバックアップの取得はルールに沿って厳格に行われている<br>･アプリケーションへのアクセスに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラスＡ<br>･アプリケーションへのアクセスに対する監視についての見直し状況はクラスＡ<br>･アプリケーションへのアクセスに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラスＡ |
| レベル4 | アプリケーションへのアクセスについて、平均以上に徹底した監視を実施しており、監視結果の取扱いも適切に行われているが、監視結果への対応等に、レベル 5 に比べ劣るところがいる。現時点では相当に強力な監視と見てよい。アプリケーションへのアクセスについてに関し、対処が必要な事象を見逃す隙が、僅かではあるが残されている。<br>･重要なアプリケーションおよび重要な情報を扱うアプリケーションのすべてを監視の対象とし、そのそれぞれに組織的な検討の下で、アクセスに対する監視についての適切な要求が示されている<br>･これらのアプリケーションには必要なアクセス監視機能や必要に応じた改ざん防止措置が的確に実装されている<br>･アプリケーションへの不審なアクセスに対してはリアルタイムで警告が出されている<br>･これらのアプリケーションへのアクセスについては、後日の監査に必要なログがきめ細かく取得されている。<br>･取得した監査ログの保管、監査結果の分析等の監査ログの取扱いについて完成度の高い要領が確立していて、マニュアル化されているが、これらにはまだ改善の余地がある |

| | |
|---|---|
| | ・改ざん防止策を始め、収集したログの保全は、ルールの沿って行われ、その管理も、ほぼ万全と見なされるが、徹底さにかけるところも見られる<br>・監査ログの分析はルールに沿って比較的高い密度（頻度とチェックのレベル）で行われ、その管理も行われているが、一部に徹底さに欠けるところも見られる<br>・アクセスログの保管やバックアップの取得はルールに沿って、概ね、厳格に行われている<br>・アプリケーションへのアクセスに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラスＢ以上<br>・アプリケーションへのアクセスに対する監視についての見直し状況はクラスＢ以上<br>・アプリケーションへのアクセスに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラスＢ以上 |
| レベル3 | アプリケーションへのアクセスについて、平均的なシステムでは一般には必要とされる監視を実施しており、監視結果の取扱いも概ね適切に行われている。それほど厳格なものではないが、レベル3のセキュリティを要求システムには要求される監視は行われており、システムへのアクセスについて、対処が必要な重要な事象を見逃す可能性も残されている。<br>・監視の対象は、重要なアプリケーションおよび重要な情報を扱うアプリケーションのうちの一部に限られている。監視の対象としたアプリケーションに対しては、組織的な検討された監視要件が示されているが、それほど厳格な要求ではない<br>・これらのアプリケーションには必要なアクセス監視機能は実装されている<br>・アプリケーションへの不審なアクセスに対してはリアルタイムで警告が出されている<br>・これらのアプリケーションへのアクセスログは、一般的な内容になっており、特にきめ細かいものではない<br>・大まかではあるが、取得した監査ログの保管、監査結果の分析等の監査ログの取扱いについてのやり方が決められている<br>・収集したログの保全は、概ね、ルールの沿って行われ、その管理も行われているが徹底したものではない<br>・監査ログの分析はルールに沿って定期的に行われており、その管理も行われているが、徹底したものではない<br>・アクセスログの保管やバックアップの取得はルールに沿って行われている<br>・アプリケーションへのアクセスに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラスＢ以上<br>・アプリケーションへのアクセスに対する監視についての見直し状況はクラスＢ以上<br>・アプリケーションへのアクセスに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラスＢ以上 |
| レベル2 | アプリケーションへのアクセスについては、特に重要としたものに限られている。また、取得ログの保管や、その分析はシステム運用チームに任されており、組織的な管理はされていないが、担当者ベースで最低限のことは行われている。<br>・重要なアプリケーションに対しては、監査ログの取得を行っている<br>・取得したログは、担当チーム内で形成された習慣に沿って管理されている<br>・取得したログの分析はも、担当者レベルで行われるているが、管理はされていない<br>・アプリケーションへのアクセスに対する監視の要求、ならびに実行手段やそれらの運用方法についての検討のレベルはクラスＣ以上<br>・アプリケーションへのアクセスに対する監視についての見直し状況はクラスＣ以上<br>・アプリケーションへのアクセスに対する監視にかかる指定された措置やその実践状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | 問題が生じた時に追跡調査のためのアクセスログの取得が、一部のアプリケーションについて行われているが日常的な監視は行われていない<br>・レベル2の達成要件も満たしていない |

## 3.3. セキュアなシステムの構築とその維持

### 3.3.1. セキュアなシステム構成の維持

| Tc1.1 | セキュアなシステム構成の設計 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムが想定すべきさまざまな技術面での脅威に対し、それが現実になっても、実害に結びつかないようにするための手段が2重、3重に講じられており、現時点ではこれ以上期待できないほどの堅牢な構成となっている。<br>・システム構成に組立て方針として明示すべきこと（注1）は、すべて明示されている<br>・想定されるセキュリティインシデントが実害に結びつかないようにするための手段が2重、3重に組込まれ、ほとんどの検討対象について現時点での最強手段が組込まれている<br>・示されているシステム構成の組立て方針は、経営レベルのセキュリティポリシーを実現でき、セキュリティ対策の詳細と完全にあったものであることが確認されている<br>・セキュリティ対策面からのシステム構成の組立て方針についての検討のレベルはクラスA<br>・セキュリティ対策面からのシステム構成の詳細設計についての検討のレベルはクラスA<br>・システム構成設計の妥当性を確保するため管理の仕組みの確立状況はクラスA<br>・システム構成の組立ての方針や、構成設計についての見直し状況はクラスA<br>・システム構成の組立ての方針や、構成設計や、その検討状況についての文書化のレベルはクラスA |
| レベル4 | システムが想定すべきさまざまな技術面での脅威に対し、それが現実になっても、実害に結びつかないようにするための手段が随所に講じられているが、すべての設計事項にわたり、現時点で最も強力と見られるものが採用されいるわけではない。<br>・システム構成に組立て方針として明示すべきこと（注1）は、概ね適切に示されているが、一部に検討が十分でないところがある<br>・想定されるセキュリティインシデントが実害に結びつかないようにするための手段が随所に講じられているが、すべてにわたり最強手段が講じられているわけではない<br>・示されているシステム構成の組立て方針は、経営レベルのセキュリティポリシーを実現でき、セキュリティ対策の詳細とマッチしているとしているが、一部に確認が不十分なところもある<br>・セキュリティ対策面からのシステム構成の組立て方針についての検討のレベルはクラスB以上<br>・セキュリティ対策面からのシステム構成の詳細設計についての検討のレベルはクラスB以上<br>・システム構成設計の妥当性を確保するため管理の仕組みの確立状況はクラスB以上<br>・システム構成の組立ての方針や、構成設計についての見直し状況はクラスB以上<br>・システム構成の組立ての方針や、構成設計や、その検討状況についての文書化のレベルはクラスB以上 |
| レベル3 | 大まかではあるが、セキュリティ面からのシステムの構成方針は示されている。システムの構成は、十分に堅牢なものとは言い難いが、経営レベルのセキュリティポリシーを実現できるものになっている。また、セキュリティ対策とのマッチングもチェックされている。<br>・システム構成に組立て方針として明示すべきこと（注1）は、概ね適切に示されているが、一部に検討が十分でなりところがある<br>・システム構成に一般的に採用すべき手段は、当該システムに不要なものを除き、ほとんど組み込まれている<br>・被害の拡大防止やシステムの障害対策他の可用性の確保のための手段も、ある程度組込まれている<br>・示されているシステム構成の組立て方針は、経営レベルのセキュリティポリシーを実現でき、セキュリティ対策の詳細とマッチしているとしているが、一部に確認が不十分なところもある<br>・セキュリティ対策面からのシステム構成の組立て方針についての検討のレベルはクラスB以上<br>・セキュリティ対策面からのシステム構成の詳細設計についての検討のレベルはクラスB以上<br>・システム構成設計の妥当性を確保するため管理の仕組みの確立状況はクラスB以上<br>・システム構成の組立ての方針や、構成設計についての見直し状況はクラスB以上 |

| | |
|---|---|
| | ・システム構成の組立ての方針や、構成設計や、その検討状況についての文書化のレベルはクラス B 以上 |
| レベル 2 | ファイアウオールやウイルス対策ソフト等の基本的なセキュリティ対策ツールの配置に加え、DMZの確保等、システム構成面での堅牢性の確保のための最低限の手段は講じられているが、その使用法にしても十分検討されたものとは言い難い。<br>・ファイアウオールやウイルス対策ソフト等の基本的なセキュリティ対策ツールは配置<br>・内部システムを外部ネットワークから隔離する手段は採用<br>・被害の拡大防止やシステムの障害対策他の可用性の確保のための特別な手段は組込まれていない<br>・セキュリティ対策面からのシステム構成の組立て方針についての検討のレベルはクラス C 以上<br>・セキュリティ対策面からのシステム構成の詳細設計についての検討のレベルはクラス C 以上<br>・システム構成設計の妥当性を確保するため管理の仕組みの確立状況はクラス C 以上<br>・システム構成の組立ての方針や、構成設計についての見直し状況はクラス C 以上<br>・システム構成の組立ての方針や、構成設計や、その検討状況についての文書化のレベルはクラスC 以上 |
| レベル 1 | ファイアウオールやウイルス対策ソフト等の基本的なセキュリティ対策ツールは配置されているものの、システム構成面からの堅牢性の確保は考慮されていない<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | システム構成は、きめの細かいシステム構成方針に沿って設計され、その実装も設計どおりで、システム環境やセキュリティ環境の変化やセキュリティ対策の変更に応じた変更も迅速的確に行われており、システムの構成にセキュリティ面での不備が入りことは、まず考えられない。<br>・セキュリティ面からシステム構成の設計や実装の的確性を確保するための完成度の高い管理の仕組みが確立している<br>・システムの導入に際して、この仕組みに沿った組織的なレビューチェックが、セキュリティ対策面からのシステム構成の妥当性にかかわる事項（注1）のすべてに対して徹底して行われている<br>・セキュリティ対策面からシステム構成の見直しが必要となるような、システム環境の変更やセキュリティ環境の変更を見逃さないようにする仕組みが完全に機能している<br>・システム環境の変更やセキュリティ環境の変更に際して、システム構成についての導入時と同じレベルの徹底さで設計面での見直しが行われている<br>・システム構成に変更の必要が生じた場合の必要な対応のタイムラグは平均１週間以内<br>・システム構成の変更に際しても、システム導入時と同じような厳格なシステム構成の実装についてのチェックが行われている<br>・年に数回以上、システム構成の的確性についての定期的なチェックも実施している<br>・システム構成の妥当性を維持するための管理面での仕組みについのて検討状況はレベルA<br>・システム構成の妥当性の確認のレベルや方法についての検討レベルはクラス A<br>・システム構成のセキュアなシステム運用を実現するためのスキームについての見直し状況はクラス A<br>・システム構成の実装状況や実装の維持管理活動についての文書化のレベルはクラス A |
| レベル 4 | システム構成は、きめの細かいシステム構成方針に沿って設計され、その実装も設計どおりで、システム環境やセキュリティ環境の変化やセキュリティ対策の変更に応じた変更も迅速に行われているが、一部に徹底さを欠くところもみられる。可能性は低いが、システムの構成にセキュリティ面での不備が入り込む水が、僅かではあるが残されている。<br>・セキュリティ面からシステム構成の設計や実装の的確性を確保するための良く検討されたスキームが確立している<br>・システムの導入に際して、この仕組みに沿った組織的なレビューチェックが、セキュリティ対策面から |

| | |
|---|---|
| | のシステム構成の妥当性にかかわる事項（注1）のほとんどに対して行われている<br>・システム環境の変更やセキュリティ環境の変更に際して、システム構成について設計面での見直しが組織的に行われているが、徹底さを欠くところもある<br>・システム構成に変更の必要が生じた場合の必要な対応のタイムラグは、平均２週間以内<br>・システム構成の変更に際しても、システム構成の実装について相当厳格なチェックが行われている<br>・年に2回以上、システム構成の的確性についての定期的なチェックも実施している<br>・システム構成の妥当性を維持するための管理面での仕組みについのて検討状況はレベルＢ以上<br>・システム構成の妥当性の確認のレベルや方法についての検討レベルはクラスＢ以上<br>・システム構成の実装状況や実装の維持管理活動についての文書化のレベルはクラスＢ以上 |
| レベル3 | システム構成は、概ねシステム構成方針に沿ったものになっているが、その設計や実装が本来あるべきものになっているかどうかのレビューやチェックや、システム環境やセキュリティ環境の変化やセキュリティ対策の変更に応じた変更も、組織的に行われてはいるが、徹底したものとは言い難く、システムの構成にセキュリティ面での不備が入り込む余地が残されている。<br>・システム導入時点における、セキュリティ対策面からのシステム構成の設計の妥当性や実装の的確性について組織的なレビューやチェックが行わるれてはいるが、レビューやチェックの対象の網羅性や厳格性にかけるところがある（レビューやチェックは注2のすべてを対象にしていない）<br>・システム環境の変更やセキュリティ環境の変更に際して、システム構成について設計面での見直しが組織的に行われているが、十分とは言えない<br>・システム構成に変更の必要が生じた場合の必要な対応のタイムラグは、平均1ヶ月以内<br>・システム構成の変更に際しても、システム構成の実装について、ある程度のチェックが組織的に行われている<br>・年に1回以上、システム構成の的確性についての定期的なチェックも実施している<br>・システム構成の妥当性を維持するための管理面での仕組みについのて検討状況はレベルＣ以上<br>・システム構成の妥当性の確認のレベルや方法についての検討レベルはクラスＣ以上<br>・システム構成の実装状況や実装の維持管理活動についての文書化のレベルはクラスＢ以上 |
| レベル2 | セキュリティ対策面からのシステム構成の的確性の確保についての組織的な取組みは見られないが、担当者レベルでの努力は見られ、システム構成にセキュリティ面から大きな欠陥が残されたままになっているようなことはないが、あちこちに不備が残されている可能性は低くない。<br>・システム導入時点における、セキュリティ対策面からのシステム構成の妥当性を確保するための組織的な仕組みはないに等しい<br>・システム導入時点における、セキュリティ対策面からのシステム構成の設計の妥当性や実装の的確性について担当者レベルでのレビューやチェックが行わるれてはいるが、レビューやチェックの対象の粗く不十分<br>・システム環境の変更やセキュリティ環境の変更に際して、システム構成について設計面での見直しは、担当者の注意に任されており、組織的な管理は行われていない<br>・システム構成に変更の必要が生じた場合の必要な対応のタイムラグは、平均2ヶ月以上<br>・システム構成の変更に際しても、システム構成の実装についてのチェックは、担当者まかせ<br>・システム構成の実装状況や実装の維持管理活動についての文書化のレベルはクラスＣ以上 |
| レベル1 | セキュリティ対策面からのシステム構成の的確性の確保についての取組みは見られない<br>・レベル2の達成要件も満たしていない |

(注 1)　システム構成について検討すべき事項
- ・ゾーン分割の方針と各ゾーンの使い方の詳細
  - －それぞれのゾーンの位置付け
  - －各ゾーンに配置するサービスや DB の配置
  - －各ゾーンに対するセキュリティ要求
  - －ゾーン間での通信についてのルール
- ・ネットワーク上のサーバや通信制御機器やセキュリティツールの配置
- ・各サーバへのサービスの配置
- ・各サーバへの DB の配置
- ・プラットフォームの使用法

### 3.3.2. ソフトウエアの管理の徹底

| 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | OS 等のプラットフォーム系ソフトの導入や変更に対する完成度の高い管理スキームが確立しており、これらのソフトに対しては、この管理スキームに沿った徹底した管理が行われており、OS 等のプラットフォーム系ソフトの導入や変更に関して不手際が入り込むことは、まず考えられない。<br>･OS 等のプラットフォーム系ソフトに対し、網羅された対象システムの運用形態にマッチしたよく検討された管理のスキームが確立している<br>･これらのソフトの導入や変更は、このスキームに完全に沿って徹底した組織的な管理の下で行われている<br>･すべてのサーバやクライアント PC における、これらのソフトの使用状況は常に正確に把握されている<br>･これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラス A<br>･これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラス A<br>･これらのソフトの導入や変更に対する管理スキームや、その実践についての文書化レベルはクラス A |
| レベル4 | OS 等のプラットフォーム系ソフトの導入や変更に対する管理スキームが確立しており、これらのソフトに対しては、この管理スキームに沿った管理が行われているが、一部に徹底さを欠いたところも見られ、OS 等のプラットフォーム系ソフトの導入や変更に関して不手際が入り込む余地が、僅かではあるが残されている。<br>･OS 等のプラットフォーム系ソフトに対し、(注1) に示すようなことがほぼ網羅された対象システムの運用形態にマッチしたよく検討された管理のスキームが策定されている<br>･これらのソフトの導入や変更は、このスキームに完全に沿って、組織的な管理の下で行われているが、一部に徹底さを欠くところも見られる<br>･すべてのサーバやクライアント PC における、これらのソフトの使用状況は、常に正確に把握されている<br>･これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラス B 以上<br>･これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラス B 以上<br>･これらのソフトの導入や変更に対する管理スキームや、その実践についての文書化のレベルはクラス B 以上 |
| レベル3 | OS 等のプラットフォーム系ソフトの導入や変更は、ある程度組織的に管理されており、概ね適切に行われているが、これらに対する管理スキームは十分なものとは言えず、OS 等のプラットフォーム系ソフトの導入や変更に関して不手際を起こす可能性は少ないとは言えない。<br>･OS 等のプラットフォーム系ソフトの導入や変更の実施に対して基本的なルール (注2) は示されている<br>･これらのソフトの導入や変更は、このルールに沿って担当部門の組織的な管理下で行われているが、徹底した管理の下で行われているとは言い難い<br>･重要なサーバや一部のクライアント PC における、これらのソフトの使用状況は、ほぼ正確に把握されているが、その他についてはあまり把握されていない<br>･これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラス B 以上<br>･これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラス B 以上<br>･これらの系ソフトの導入や変更に対する管理スキームや、その実践についての文書化のレベルはクラス B 以上 |
| レベル2 | OS 等のプラットフォーム系ソフトの導入や変更の管理は、担当チームの注意に任されているが、担当者は経験もあり、これらについての作業は相応の注意の下で、概ね適切に行われているが、組織的な管理の下で行われているとは言い難く、不手際が入り込んでもおかしくはない。<br>･OS 等のプラットフォーム系ソフトの導入や変更の実施に対する注意事項 (注2相当) についての、担当者チーム内での共通認識は存在<br>･これらのソフトの導入や変更は、チームとしての管理下で、この共通認識である注意事項を留意して行われている<br>･これらのソフトの使用状況は、ある程度把握されているが、十分とは言えない<br>･これらのソフトの導入や変更に対する管理スキームや実行についての文書化のレベルはクラス C 以上 |

| | |
|---|---|
| レベル1 | OS 等のプラットフォーム系ソフトの導入や変更の妥当性は、すべて担当者の注意に依存している<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 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対する完成度の高い管理スキームが確立しており、これらのソフトに対しては、この管理スキームに沿った徹底した管理が行われており、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関して不手際が入り込むことは、まず考えられない。<br>・オフィスツール等の汎用業務ツール系ソフトに対し、(注1) に示すようなことが網羅された対象システムの運用形態にマッチしたよく検討された管理のスキームが確立している<br>・これらのソフトの導入や変更は、このスキームに完全に沿って徹底した組織的な管理の下で行われている<br>・すべてのサーバやクライアント PC における、これらのソフトの使用状況は常に正確に把握されている<br>・これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラス A<br>・これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラス A<br>・これらのソフトの導入や変更に対する管理スキームや、その実践についての文書化レベルはクラス A |
| レベル4 | 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対する管理スキームが確立しており、これらのソフトに対しては、この管理スキームに沿った管理が行われているが、一部に徹底さを欠いたところも見られ、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関して不手際が入り込む余地が、僅かではあるが残されている。<br>・オフィスツール等の汎用業務ツール系ソフトに対し、(注1) に示すようなことがほぼ網羅された対象システムの運用形態にマッチしたよく検討された管理のスキームが策定されている<br>・これらのソフトの導入や変更は、このスキームに完全に沿って、組織的な管理の下で行われているが、一部に徹底さを欠くところも見られる<br>・すべてのサーバやクライアント PC における、これらのソフトの使用状況は、常に正確に把握されている<br>・これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラス B 以上<br>・これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラス B 以上<br>・これらのソフトの導入や変更に対する管理スキームや、その実践についての文書化のレベルはクラス B 以上 |
| レベル3 | 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は、ある程度組織的に管理されており、概ね適切に行われているが、これらに対する管理スキームは十分なものとは言えず、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関して不手際を起こす可能性は少ないとは言えない。<br>・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の実施に対して基本的なルール (注2) は示されている<br>・これらのソフトの導入や変更は、このルールに沿って担当部門の組織的な管理下で行われているが、徹底した管理の下で行われているとは言い難い<br>・重要なサーバや一部のクライアント PC における、これらのソフトの使用状況は、ほぼ正確に把握されているが、その他についてはあまり把握されていない<br>・これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラス B 以上<br>・これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラス B 以上<br>・これらの系ソフトの導入や変更に対する管理スキームや、その実践についての文書化のレベルはクラス B 以上 |
| レベル2 | 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の管理は、担当チームの注意に任されているが、担当者は経験もあり、これらについての作業は相応の注意の下で、概ね適切に行われているが、組織的な管理の下で行われているとは言い難く、不手際が入り込んでもおかしくはない。 |

| | |
|---|---|
| | ・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の実施に対する注意事項（注2相当）についての、担当者チーム内での共通認識は存在<br>・これらのソフトの導入や変更は、チームとしての管理下で、この共通認識である注意事項を留意して行われている<br>・これらのソフトの使用状況は、ある程度把握されているが、十分とは言えない<br>・これらのソフトの導入や変更に対する管理スキームや実行についての文書化のレベルはクラスＣ以上 |
| レベル1 | 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の妥当性は、すべて担当者の注意に依存している<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 個別業務ソフトの導入や変更に対する完成度の高い管理の仕組みが確立しており、これらのソフトに対しては、この管理スキームに沿った徹底した管理が行われており、個別業務ソフトの導入や変更に関して不手際が入り込むことは、まず考えられない。<br>・個別業務ソフトに対し、対象システムの運用形態にマッチしたよく検討された管理の仕組みが確立している<br>・これらのソフトの導入や変更は、この管理の仕組みに完全に沿って徹底した組織的な管理の下で行われている<br>・すべてのサーバやクライアントPCにおける、これらのソフトの使用状況は常に正確に把握されている<br>・これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラスＡ<br>・これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラスＡ<br>・これらのソフトの導入や変更に対する管理スキームや、その実践についての文書化レベルはクラスＡ |
| レベル4 | 個別業務ソフトの導入や変更に対する管理の仕組みが確立しており、これらのソフトに対しては、この管理スキームに沿った管理が行われているが、一部に徹底さを欠いたところも見られ、個別業務ソフトの導入や変更に関して不手際が入り込む余地は、」僅かではあるが残されている。<br>・個別業務ソフトに対し、対象システムの運用形態にマッチしたよく検討された管理の仕組みが作られているが、まだ改善する余地がある<br>・これらのソフトの導入や変更は、このスキームに完全に沿って、組織的な管理の下で行われているが、一部に徹底さを欠くところも見られる<br>・これらのソフトの使用状況は、常に正確に把握されている<br>・これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラスＢ以上<br>・これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラスＢ以上<br>・これらのソフトの導入や変更に対する管理スキームや、その実践についての文書化のレベルはクラスＢ以上 |
| レベル3 | 大まかではあるが個別業務ソフトの導入や変更に対する管理の仕組みが示されており、個別業務ソフトソフトの導入や変更は、この仕組みに沿って行われ管理されているが、徹底したものではない、個別業務ソフトソフトの導入や変更は、概ね、適切に行われてはいるが、個別業務ソフトの導入や変更に関して不手際を起こす可能性は、残されている。<br>・個別業務ソフトの導入や変更の実施に対して基本的なルールは示されている<br>・これらのソフトの導入や変更は、このルールに沿って担当部門の組織的な管理下で行われているが、徹底した管理の下で行われているとは言い難い<br>・これらのソフトの使用状況は、概ね正確に把握されている<br>・これらのソフトの導入や変更に対する管理のスキームについての検討のレベルはクラスＢ以上<br>・これらのソフトの導入や変更に対する管理スキームについての見直し状況はクラスＢ以上<br>・これらの系ソフトの導入や変更に対する管理スキームや、その実践についての文書化のレベルはクラスＢ以上 |

| | |
|---|---|
| レベル2 | 個別業務ソフトの導入や変更の管理は、担当チームの注意に任されているが、担当者は経験もあり、これらについての作業は相応の注意の下で、概ね適切に行われているが、組織的な管理の下で行われているとは言い難く、不手際が入り込んでもおかしくはない。<br>・個別業務ソフトの導入や変更の実施に対する注意事項についての、担当者チーム内での共通認識は存在<br>・これらのソフトの導入や変更は、チームとしての管理下で、この共通認識である注意事項を留意して行われている<br>・これらのソフトの使用状況は、ある程度把握されているが、十分とは言えない<br>・これらのソフトの導入や変更に対する管理スキームや実行についての文書化のレベルはクラスＣ以上 |
| レベル1 | 個別業務ソフトの導入や変更の妥当性は、すべて担当者の注意に依存している<br>・レベル2の達成要件も満たしていない |

### 3.3.3. 個々の機器の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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムの構成要素としてネットワーク制御機器自体に求められるセキュリティ対策が、すべての機器に対して徹底しており、ネットワーク機器自体にセキュリティ面での脆弱性が残されている可能性は、まず考えられない。<br>・ネットワーク制御機器の種類ごとに機器自体に求められる（注1）に示すようなセキュリティ対策（注1）が明確にされている<br>・各ネットワーク制御機器におけるこれらの要求への対応を確実にするための完成度の高い管理の仕組みが確立している<br>・各ネットワーク制御機器に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームに沿って徹底して行われている<br>・すべてのネットワーク制御機器について、各機器自体に対するセキュリティ対策の実施状況は完全に把握されている<br>・問題が生じた場合における関連機器におけるセキュリティ対策の見直しと、必要な対応は数日以内に行われている<br>・各ネットワーク制御機器に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラスA<br>・本対策要求かかる管理スキームや各通信制御機器に実施しているセキュリティ対策についての文書化のレベルはクラスA |
| レベル4 | システムの構成要素としてネットワーク制御機器自体に求められるセキュリティ対策が、すべての機器に対して、組織的な管理の下で実施されて、概ね十分と言えるが、その実施や管理に徹底さを欠くところも見られ、ネットワーク機器自体にセキュリティ面での脆弱性が残されている隙が、僅かではあるが残されている。<br>・ネットワーク制御機器の種類ごとに機器自体に求められるセキュリティ対策（注1）が明確にされている<br>・各ネットワーク制御機器におけるこれらの要求への対応を確実にするためのよく検討された管理の仕組みが確立している<br>・各ネットワーク制御機器に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームに沿って行われているが、一部に徹底さを欠くところが見られる<br>・すべてのネットワーク制御機器について、各機器自体に対するセキュリティ対策の実施状況は、ほぼ完全に把握されている<br>・問題が生じた場合における関連機器におけるセキュリティ対策の見直しと、必要な対応は 2 週間以内に行われている<br>・各ネットワーク制御機器に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラスB以上<br>・本対策要求かかる管理スキームや各通信制御機器に実施しているセキュリティ対策についての文書化のレベルはクラスB以上 |
| レベル3 | システムの構成要素としてネットワーク制御機器自体に求められるセキュリティ対策は、ある程度、組織的な管理の下で実施されているが、管理のスキームやその実行管理は十分なものとは言えず、ネットワーク機器自体にセキュリティ面での脆弱性が見逃される可能性も残されている。<br>・ネットワーク制御機器の種類ごとに機器自体に求められるセキュリティ対策についての検討レベルはクラスCレベル以上で、内容的には概ね十分ではあるが、細部についてはさらなる研究が必要<br>・大まかではあるが、各ネットワーク制御機器におけるこれらの要求への対応を確実にするための管理の仕組みも作られている<br>・各ネットワーク制御機器に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、担当部門レベルでこの管理の仕組みに沿って行われているが、徹底したものではない<br>・ネットワーク制御機器について、各機器自体に対するセキュリティ対策の実施状況の把握は、行われることになっているが、全機器について常に正確な把握は出来ていない |

| | |
|---|---|
| | ・問題が生じた場合における関連機器におけるセキュリティ対策の見直しと、必要な対応は１ヶ月ぐらいを要している<br>・各ネットワーク制御機器に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラスＣ以上<br>・本対策要求かかる管理スキームや各通信制御機器に実施しているセキュリティ対策についての文書化のレベルはクラスＣ以上 |
| レベル2 | システムの構成要素としてネットワーク制御機器自体に求められるセキュリティ対策は、担当チームの注意に任されているが、担当者はある程度の知識や経験を有し、担当者レベルでは相応の注意の下で、これらの機器に対するセキュリティ対策を実施しているものの、組織的な管理の下にあるとは言い難く、ネットワーク機器自体がセキュリティ面での脆弱性が残されたまま使用されている可能性は低くはない。<br>・ネットワーク制御機器の種類ごとに機器自体に求められるセキュリティ対策は、担当チームの知識や経験任せ、ただしチーム内でのチェックは行われている<br>・担当チームのこの点に関しての知識と経験はある程度評価できる<br>・ネットワーク制御機器について、各機器自体に対するセキュリティ対策の実施状況の把握は、あまり行われてなく、管理はされてはいない<br>・問題が生じた場合における関連機器におけるセキュリティ対策の見直しと、必要な対応は １ ヶ月以上かかることもある<br>・本対策要求かかる管理スキームや各通信制御機器に実施しているセキュリティ対策についての文書化のレベルはクラスＣ以上 |
| レベル1 | ネットワーク制御機器の個々に対し必要なセキュリティ対策の実施は、組織的な管理下におかれてなく、担当者の注意に依存しているだけで、ネットワーク制御機器自体がセキュリティ上の脆弱性を抱えたまま使われていても不思議ではない。<br>・レベル2の達成要件も満たしていない |

## Ｔｃ3.2　サーバにおけるセキュリティ対策

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムの構成要素としてのサーバ自体に求められるセキュリティ対策が、すべての機器に対して徹底しており、サーバ自体にセキュリティ面での脆弱性が残されていることは、まず考えられない。<br>・サーバごとに機器自体に求められるに示すようなセキュリティ対策（注1）が明確にされている<br>・各サーバにおけるこれらの要求への対応を確実にするためのよく検討された管理の仕組みも確立している<br>・各サーバに対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理の仕組みに沿って徹底して行われている<br>・すべてのサーバについて、各機器自体に対するセキュリティ対策の実施状況は完全に把握されている<br>・問題が生じた場合における各サーバにおけるセキュリティ対策の見直しと、必要な対応は数日以内に行われている<br>・各サーバに対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラスＡ<br>・本対策要求かかる管理スキームや各サーバに実施しているセキュリティ対策についての文書化のレベルはクラスＡ |
| レベル4 | システムの構成要素としてのサーバ自体に求められるセキュリティ対策が、すべての機器に対して、組織的な管理の下で実施されて、概ね十分と言えるが、その実施や管理に徹底さを欠くところも見られ、サーバ自体にセキュリティ面での脆弱性が残されている隙が、僅かではあるが残されている。<br>・サーバごとに機器自体に求められるに示すようなセキュリティ対策（注1）が明確にされている |

| | |
|---|---|
| | ・各サーバにおけるこれらの要求への対応を確実にするための管理の仕組みも作られているが、まだ改善の余地がある<br>・各サーバに対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームに沿って行われているが、一部に徹底さを欠くところが見られる<br>・すべてのサーバについて、各機器自体に対するセキュリティ対策の実施状況は、ほぼ完全に把握されている<br>・問題が生じた場合における各サーバにおけるセキュリティ対策の見直しと、必要な対応は 2 週間以内に行われている<br>・各サーバに対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラス B 以上<br>・本対策要求かかる管理スキームや各サーバに実施しているセキュリティ対策についての文書化のレベルはクラス B 以上 |
| レベル 3 | システムの構成要素としてのサーバ自体に求められるセキュリティ対策は、ある程度、組織的な管理の下で実施されているが、管理のスキームやその実行管理は十分なものとは言えず、サーバ自体にセキュリティ面での脆弱性が見逃される可能性も残されている。<br>・サーバごとに機器自体に求められるセキュリティ対策についての検討レベルはクラス C レベル以上で、内容的には概ね十分ではあるが、細部についてはさらなる研究が必要<br>・大まかではあるが、各サーバにおけるこれらの要求への対応を確実にするための管理の仕組みも作られている<br>・各サーバに対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、担当部門レベルで管理スキームに沿って行われているが、徹底したものではない<br>・サーバについて、各機器自体に対するセキュリティ対策の実施状況の把握は、行われることになっているが、全機器について常に正確な把握は出来ていない<br>・問題が生じた場合における各サーバにおけるセキュリティ対策の見直しと、必要な対応は 1 ヶ月ぐらいを要している<br>・各サーバに対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラス C 以上<br>・本対策要求かかる管理スキームや各サーバに実施しているセキュリティ対策についての文書化のレベルはクラス C 以上 |
| レベル 2 | システムの構成要素としてサーバ自体に求められるセキュリティ対策は、担当チームの注意に任されているが、担当者はある程度の知識や経験を有し、担当者レベルでは相応の注意の下で、サーバに対するセキュリティ対策を実施しているものの、組織的な管理の下にあるとは言い難く、サーバ自体がセキュリティ面での脆弱性が残されたまま使用されている可能性は低くはない。<br>・サーバごとに機器自体に求められるセキュリティ対策は、担当チームの知識や経験任せ、ただしチーム内でのチェックは行われている<br>・担当チームのこの点に関しての知識と経験はある程度評価できる<br>・システムで使われいる各サーバについて、サーバ自体に対するセキュリティ対策の実施状況の把握は、あまり行われてなく、管理はされてはいない<br>・問題が生じた場合における各サーバにおけるセキュリティ対策の見直しと、必要な対応は 1 ヶ月以上かかることもある<br>・本対策要求かかる管理スキームやシステム内の各サーバに実施しているセキュリティ対策についての文書化のレベルはクラス C 以上 |
| レベル 1 | システムで使われているサーバの個々に対し必要なセキュリティ対策の実施は、組織的な管理下におかれてなく、担当者の注意に依存しているだけで、システム内のサーバ自体がセキュリティ上の脆弱性を抱えたまま使われていても不思議ではない。<br>・レベル2の達成要件も満たしていない |

## Tc3.3 LAN 上のクライアント PC に対するセキュリティ対策

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムの構成要素としての LAN 上のクライアント PC 自体に求められるセキュリティ対策が、すべての機器に対して徹底しており、サーバ自体にセキュリティ面での脆弱性が残されている可能性は、まず考えられない。<br>・LAN 上のクライアント PC ごとに機器自体に求められるに示すようなセキュリティ対策（注 1）が明確にされている<br>・各 LAN 上のクライアント PC に対するこれらの要求への対応を確実にするためのよく検討された管理仕組みが確立している<br>・各 LAN 上のクライアント PC に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理のい仕組みに沿って徹底して行われている<br>・すべての LAN 上のクライアント PC について、脆弱性の排除措置の実施状況は完全に把握されている<br>・問題が生じた場合における LAN 上のクライアント PC におけるセキュリティ対策の見直しと、必要な対応は数日以内に行われている<br>・各 LAN 上のクライアント PC に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラス A<br>・本対策要求かかる管理スキームや各 LAN 上のクライアント PC に実施しているセキュリティ対策についての文書化のレベルはクラス A |
| レベル4 | システムの構成要素としての LAN 上のクライアント PC 自体に求められるセキュリティ対策が、すべての機器に対して、組織的な管理の下で実施されて、概ね十分と言えるが、その実施や管理に徹底さを欠くところも見られ、LAN 上のクライアント PC 自体にセキュリティ面での脆弱性が残されている隙が、僅かではあるが残されている。<br>・LAN 上のクライアント PC ごとに機器自体に求められるに示すようなセキュリティ対策（注 1）が明確にされている<br>・各 LAN 上のクライアント PC におけるこれらの要求への対応を確実にするための管理の仕組みが作られているが、まだ改善する余地もある<br>・各 LAN 上のクライアント PC に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームに沿って行われているが、一部に徹底さを欠くところが見られる<br>・すべての LAN 上のクライアント PC について、各機器自体に対するセキュリティ対策の実施状況は、ほぼ完全に把握されている<br>・問題が生じた場合における各 LAN 上のクライアント PC におけるセキュリティ対策の見直しと、必要な対応は 2 週間以内に行われている<br>・各 LAN 上のクライアント PC に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラス B 以上<br>・本対策要求かかる管理スキームや各 LAN 上のクライアント PC に実施しているセキュリティ対策についての文書化のレベルはクラス B 以上 |
| レベル3 | システムの構成要素としての LAN 上のクライアント PC 自体に求められるセキュリティ対策は、ある程度、組織的な管理の下で実施されているが、管理のスキームやその実行管理は十分なものとは言えず、LAN 上のクライアント PC 自体にセキュリティ面での脆弱性が見逃される可能性も残されていると考えなければならない。<br>・LAN 上のクライアント PC ごとに機器自体に求められるセキュリティ対策についての検討レベルはクラス C レベル以上で、内容的には概ね十分ではあるが、細部についてはさらなる研究が必要<br>・大まかではあるが、各 LAN 上のクライアント PC におけるこれらの要求への対応を確実にするための管理の仕組みが作られている<br>・各 LAN 上のクライアント PC に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、担当部門レベルで管理スキームに沿って行われているが、徹底したものではない<br>・LAN 上のクライアント PC について、各機器自体に対するセキュリティ対策の実施状況の把握は、行われることになっているが、全機器について常に正確な把握は出来ていない |

| | |
|---|---|
| | ・問題が生じた場合における各 LAN 上のクライアント PC におけるセキュリティ対策の見直しと、必要な対応は 1 ヶ月ぐらいを要している<br>・各 LAN 上のクライアント PC に対しては、必要なセキュリティ対策の実施と、その的確性についての確認は、この管理スキームについての見直し情況はクラス B 以上<br>・本対策要求かかる管理スキームや各 LAN 上のクライアント PC に実施しているセキュリティ対策についての文書化のレベルはクラス B 以上 |
| レベル 2 | システムの構成要素として LAN 上のクライアント PC 自体に求められるセキュリティ対策は、担当チームの注意に任されているが、担当者はある程度の知識や経験を有し、担当者レベルでは相応の注意の下で、LAN 上のクライアント PC に対するセキュリティ対策を実施しているものの、組織的な管理の下にあるとは言い難く、LAN 上のクライアント PC 自体がセキュリティ面での脆弱性が残されたまま使用されている可能性は低くはない。<br>・LAN 上のクライアント PC ごとに機器自体に求められるセキュリティ対策は、担当チームの知識や経験任せ、ただしチーム内でのチェックは行われている<br>・担当チームのこの点に関しての知識と経験はある程度評価できる<br>・システムで使われいる各サーバについて、LAN 上のクライアント PC 自体に対するセキュリティ対策の実施状況の把握は、あまり行われてなく、管理はされてはいない<br>・問題が生じた場合における各 LAN 上のクライアント PC におけるセキュリティ対策の見直しと、必要な対応は 1 ヶ月以上かかることもある<br>・本対策要求かかる管理スキームやシステム内の各 LAN 上のクライアント PC に実施しているセキュリティ対策についての文書化のレベルはクラス C 以上 |
| レベル 1 | システムで使われている LAN 上のクライアント PC の個々に対し必要なセキュリティ対策の実施は、組織的な管理下におかれてなく、担当者の注意に依存しているだけで、システム内の LAN 上のクライアント PC 自体がセキュリティ上の脆弱性を抱えたまま使われていても不思議ではない。<br>・レベル 2 の達成要件も満たしていない |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 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が的確に行われるようにするための完成度の高い管理の仕組みも確立しており、この仕組みに沿って、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は徹底して管理されている。また、必要なセキュリティ機能の組込みについてのよく検討されたセキュリティ設計ガイドも確立し、開発関係者への徹底も図られており、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に不手際が起こることは、まず考えられない。<br>・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が的確に行われるようにするための完成度の高い管理の仕組みも確立している<br>・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についてのよく検討されたセキュリティ設計ガイドも確立している<br>・アプリケーションソフトの開発におけるこのセキュリティ設計ガイドに沿って設計、設計レビュー、テストは、管理の仕組みに沿って、組織的な管理の下で厳格に行われている<br>・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に関する管理の仕組みについての見直しのレベルはクラスA<br>・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に関するセキュリティ設計ガイドについての見直しのレベルはクラスA<br>・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に関する管理の仕組みについての文書化レベルはクラスA<br>・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に関するセキュリティ設計ガイドについての文書化レベルはクラスA |
| レベル4 | 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が的確に行われるようにするためのよく検討された管理の仕組みも確立しており、この仕組みに沿って、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は厳格に管理されている。また、必要なセキュリティ機能の組込みについてのセキュリティ設計ガイドも確立し、開発関係者への周知も図られているが、管理の仕組みやこの点についての技術ガイドには、まだ改善の余地がある。また、その管理に、一部徹底さを欠くところも見られ、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に不手際が入り込む隙が、僅かではあるが残されている。<br>・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が的確に行われるようにするための管理の仕組みも確立しているが、まだ改善の余地がある<br>・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についてのよく検討されたセキュリティ設計ガイドも作られているが、まだ改善の余地がある<br>・アプリケーションソフトの開発におけるこのセキュリティ設計ガイドに沿って、設計と設計レビュー、テストは、この管理の仕組みに沿って、組織的な管理の下で行われているが、一部に徹底さを欠くところも見られる<br>・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に関する管理の仕組みについての見直しのレベルはクラスA<br>・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に関するセキュリティ設計ガイドについての見直しのレベルはクラスB以上<br>・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に関する管理の仕組みについての文書化レベルはクラスB以上<br>・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に関するセキュリティ設計ガイドについての文書化レベルはクラスB以上 |
| レベル3 | 大まかではあるが、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が的確に行われるようにするための管理の仕組みも示されており、この仕組みに沿って、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は管理されている。また、大まかなものであるが、必要なセキュリティ機能の組込みについての技術ガイドも確立し、開発関係者への周知も図られているが、管理の仕組みやこの点についての技術ガイドには、まだ改善の余地が多い。また、その管理は徹底したものではなく、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に不手際が入り込む可能性は、残されている。 |

| | |
|---|---|
| | ・大まかではあるが、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が的確に行われるようにするための管理の仕組みも示されている<br>・大まかではあるが、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に関するセキュリティ設計ガイドも作られている<br>・アプリケーションソフトの開発におけるこのセキュリティ設計ガイドに沿って、設計と設計レビュー、テストは、管理の仕組みに沿って、組織的な管理の下で行われているが、徹底したものではない<br>・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に関する管理の仕組みについての見直しのレベルはクラス A<br>・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に関するセキュリティ設計ガイドについての見直しのレベルはクラス B 以上<br>・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に関する管理の仕組みについての文書化レベルはクラス B 以上<br>・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に関するセキュリティ設計ガイドについての文書化レベルはクラス B 以上 |
| レベル 2 | 設計者間には、アプリケーションソフトへの必要なセキュリティ機能に組込みについてのノウハウが蓄積されており、開発担当者に指導がなされて、開発レビューも開発チーム内で行われている。組織的な管理はできていないが、この点についての取り組みはある程度評価できる。<br>・開発チーム内のノウハウは大まかではあるが整理されており、開発者に示されている<br>・開発者はこのノウハウを用い、開発ソフトへの必要なセキュリティ機能の組込みに漏れがないように注意している<br>・徹底したものではないが、開発チーム内でのレビューやチェックが行われている<br>・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に関する組織的な対応についての検討はクラス C 以上<br>・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に関する文書化のレベルはクラス C 以上 |
| レベル 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は、すべてアプリケーションソフトの開発者に任され、開発担当者の認識とスキルに依存している<br>・レベル 2 の達成要件も満たしていない |

## Tc4.2 アプリケーションソフトからの脆弱性の排除

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | アプリケーションソフトからの脆弱性の排除が的確に行われるようにするための完成度の高い管理の仕組みも確立しており、この仕組みに沿って、すべてのアプリケーションソフトに対する脆弱性排除の排除が組織的な管理の下で、徹底して行われている。アプリケーションソフトから脆弱性の排除についてのよく検討された技術ガイドも確立し、開発関係者への徹底も図られており、アプリケーションソフトに脆弱性が見逃されることは、まず考えられない。<br>・開発環境ごとの脆弱性チェックリスト等のアプリケーションソフトの脆弱性の排除に関する技術ガイドが確立している<br>・アプリケーションソフトに脆弱性を残さないようにするための完成度の高い管理の仕組みも確立している<br>・このセキュリティ設計ガイドに沿ってアプリケーションソフトからの脆弱性の排除は、策定された管理の仕組みに沿って、組織的な管理の下で厳格に行われている<br>・新しい脅威が報告された場合における関係するアプリケーションソフトのすべてに対する、見直しも徹底した管理の下で行われている<br>・アプリケーションソフトからの脆弱性の排除についての技術についての検討はクラスA<br>・アプリケーションソフトからの脆弱性の排除に関する組織的な対応についての検討はクラス A<br>・アプリケーションソフト開発における脆弱性の排除ティ機能の組込みに関する文書化のレベルはクラス A |

| | |
|---|---|
| レベル4 | アプリケーションソフトからの脆弱性の排除が的確に行われるようにするための管理の仕組みも確立しており、この仕組みに沿って、すべてのアプリケーションソフトに対する脆弱性排除の排除が組織的な管理の下で行われている。また、アプリケーションソフトから脆弱性の排除についての技術ガイドも示されている、開発関係者への徹底も図られているが、この管理の仕組みや技術ガイドには、まだ改善の余地も残され、その実践と管理に、一部徹底さを欠くところも見られる。アプリケーションソフトに脆弱性が見逃される隙が、僅かではあるが残されている。<br>・開発環境ごとの脆弱性チェックリスト等のアプリケーションソフトの脆弱性の排除に関する技術ガイドが確立しているが、まだ改善の余地がある<br>・アプリケーションソフトに脆弱性を残さないようにするための管理の仕組みも確立しているが、まだ改善の余地がある<br>・このセキュリティ設計ガイドに沿ってアプリケーションソフトからの脆弱性の排除は、策定された管理の仕組みに沿って、組織的な管理の下で行われているが、一部に徹底さにかけるところも見られる<br>・新しい脅威が報告された場合における関係するアプリケーションソフトのすべてに対する、見直しも組織的な管理の下で行われているが、一部に徹底さにかけるところも見られる<br>・アプリケーションソフトからの脆弱性の排除についての技術についての検討はクラスＢ以上<br>・アプリケーションソフトからの脆弱性の排除に関する組織的な対応についての検討はクラスＢ以上<br>・アプリケーションソフト開発における脆弱性の排除ティ機能の組込みに関する文書化のレベルはクラスＢ以上 |
| レベル3 | 大まかではあるが、アプリケーションソフトからの脆弱性の排除が的確に行われるようにするための管理の仕組みも示され、アプリケーションソフトから脆弱性の排除についての大まかな技術ガイドも示されている。この仕組みに沿って、すべてのアプリケーションソフトに対する脆弱性排除の排除が組織的な管理の下で行われているが、徹底したものではない。アプリケーションソフトに脆弱性が見逃される隙が残されている。<br>・大まかではあるが、開発環境ごとの脆弱性チェックリスト等のアプリケーションソフトの脆弱性の排除に関する技術ガイドが確立しているが、まだ改善の余地がある<br>・大まかではあるが、アプリケーションソフトに脆弱性を残さないようにするための管理の仕組みも示されている<br>・このセキュリティ設計ガイドに沿ってアプリケーションソフトからの脆弱性の排除は、策定された管理の仕組みに沿って、組織的な管理の下で行われているが、徹底したものではない<br>・新しい脅威が報告された場合における関係するアプリケーションソフトのすべてに対する、見直しも組織的な管理の下で行われているが、対象のアプリケーションの網羅性や見直しの密度は十分とは言えない。<br>・当該要求についての対策の検討レベルはＢ以上<br>・アプリケーションソフトからの脆弱性の排除についての技術についての検討はクラスＢ以上<br>・アプリケーションソフトからの脆弱性の排除に関する組織的な対応についての検討はクラスＢ以上<br>・アプリケーションソフト開発における脆弱性の排除ティ機能の組込みに関する文書化のレベルはクラスＢ以上 |
| レベル2 | 設計者間には、アプリケーションソフトの脆弱性の排除についてのノウハウが蓄積されており、開発担当者に指導がなされて、開発レビューも開発チーム内で行われている。組織的な管理はできていないが、この点についての取り組みはある程度評価できる。<br>・開発チーム内のノウハウは大まかではあるが整理されており、開発者に示されている<br>・開発者はこのノウハウを用い、開発ソフトからの脆弱性の排除に漏れがないように注意している<br>・徹底したものではないが、開発チーム内でのレビューやチェックが行われている<br>・アプリケーションソフトからの脆弱性の排除についての技術についての検討はクラスＣ以上<br>・アプリケーションソフトからの脆弱性の排除に関する組織的な対応についての検討はクラスＣ以上<br>・アプリケーションソフト開発における脆弱性の排除ティ機能の組込みに関する文書化のレベルはクラスＣ以上 |
| レベル1 | アプリケーションレベルのアクセス管理についての基準は考えられていない<br>・レベル2の達成要件も満たしていない |

## Tc4.3 開発プロセスに対する管理の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 完成度の高い開発プロセスが確立しており、すべての開発は、このプロセスに示された管理の仕組みに沿って、開発の全工程が厳格に管理されており、開発過程で開発システムにセキュリティ問題が入り込むことは、まず考えられない。<br>・管理の仕組みも含む開発プロセスが厳密に作成されている。<br>・開発ルールに沿った開発がすべての開発部門において厳密に実施されている<br>・開発過程でのセキュリティ問題が入り込まないようにする注意は、概ね、徹底している<br>・外部委託開発したソフトに対するセキュリティ検査のためのルールも厳格なルールが規程されており、管理の仕組みに沿って、このルールが厳格に運用されている<br>・本対策要求についての検討のレベルはクラスA<br>・本対策要求かかる措置についての見直し状況はクラスA<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスA |
| レベル4 | 開発プロセスが確立しており、すべての開発は、このプロセスに示された管理の仕組みに沿って、開発の全工程が管理されているが、開発プロセスにはまだ改善の余地もある。また、規程された仕組みに沿った開発プロセスの管理に、徹底さを欠くところも見られる。開発過程で開発システムにセキュリティ問題が入り込むこ隙が、僅かではあるが残されている。<br>・管理の仕組みも含む開発プロセスが厳密に作成されているが、まだ改善の余地がある<br>・開発ルールに沿った開発がすべての開発部門において厳密に実施されているが、一部に徹底さを欠くところが見られる<br>・開発過程でのセキュリティ問題が入り込まないようにする注意は、概ね、徹底している<br>・外部委託開発したソフトに対するセキュリティ検査のためのルールも厳格なルールが規程されており、管理の仕組みに沿って、このルールが厳格に運用されているが、一部に徹底さを欠くところが見られる<br>・本対策要求についての検討のレベルはクラスB以上<br>・本対策要求かかる措置についての見直し状況はクラスB以上<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | 開発プロセスが確立しており、すべての開発は、このプロセスに示された管理の仕組みに沿って、開発の全工程が管理されているが、規程された開発プロセスは大まかなもので、改善すべきと少なくない。また、規程された仕組みに沿った開発プロセスに対する組織的な管理も行われているが、徹底したものではない。開発過程で開発システムにセキュリティ問題が入り込むこ余地が残されている。<br>・管理の仕組みも含む開発プロセスが作成されているが、大まかで、改善の余地が少なくない<br>・開発ルールに沿った開発がすべての開発部門において実施されているが、徹底したものではない<br>・開発過程でのセキュリティ問題が入り込まないようにする注意は、相当に払われている<br>・外部委託開発したソフトに対するセキュリティ検査のためのルールも厳格なルールが規程されており、管理の仕組みに沿って、このルールが運用されているが、徹底したものではない<br>・本対策要求についての検討のレベルはクラスB以上<br>・本対策要求かかる措置についての見直し状況はクラスB以上<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | ルール化されている開発プロセスは大まかで、十分な管理ができるレベルのものではないが、開発チームごとにこの開発プロセスを、開発プロジェクトの実状に合わせて工夫して用いている。組織的な取り組みは十分とは言えないが、基本的な管理は行われていると見ることができる。<br>・大まかなではるが、開発プロセスをルール化したものはある<br>・開発プロジェクトは、このルールをプロジェクトの実態に合わせ適用を工夫している<br>・開発過程でのセキュリティ問題が入り込まないようにする注意は、ある程度払われている<br>・外部委託開発したソフトに対するセキュリティ検査も行われているが、形式的な域を出ない<br>・本対策要求についての検討のレベルはクラスC以上<br>・本対策要求かかる措置についての見直し状況はクラスC以上<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスC以上 |
| レベル1 | アプリケーションレベルのアクセス管理についての基準は考えられていない<br>・レベル2の達成要件も満たしていない |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システム運用をセキュアなものにするための環境整備が行き届いており、システム運用周りで、不手際が生じることも、まず考えられない上、問題が生じても、それが実害に結びつかないようにする仕組みも整っている。<br>・システムの運用に対するセキュリティ要求は、検討すべき事項のすべてについて、セキュリティ対策として検討された諸施策のすべてを漏れなく反映したものとして整理されている<br>・システム運用職場における運用関係者の職務遂行にかかるセキュリティ面での要求も必要事項のすべてについて明確にされている<br>・システム運用に対するセキュリティ要求は、システム運用マニュアルやシステム操作マニュアルに的確に反映されている<br>・システム運用上の不手際は、実害に結びつかないうちに発見できるようにする工夫も行き届いている<br>・システム運用に対するセキュリティ要求の実践をチェックする仕組みも、システムの運用形態にあうものが整備されている<br>・セキュアなシステム運用を実現するためのスキームについての検討のレベルはクラス A<br>・セキュアなシステム運用を実現するためのスキームについての見直し状況はクラス A<br>・セキュアなシステム運用を実現するためのスキームについての文書化のレベルはクラス A |
| レベル4 | システム運用をセキュアなものにするための環境整備が進められていて、システム運用周りで、不手際が生じる可能性は低い。また、問題が生じても、それが見逃されないようにする工夫も行われているが、まだ改善の余地は残る。<br>・システムの運用に対するセキュリティ要求は、検討すべき事項のすべてについて、セキュリティ対策として検討された諸施策を反映したものとして整理されているが、すべてについて徹底した確認が行われてはいない<br>・システム運用職場における運用関係者の職務遂行にかかるセキュリティ面での要求も明示されている<br>・システム運用に対するセキュリティ要求は、システム運用マニュアルやシステム操作マニュアルに、概ね、適切に反映されているが、まだ改善の余地がある<br>・システム運用上の不手際は、実害に結びつかないうちに発見できるようにする工夫も行われているが、まだ改善の余地がある<br>・システム運用に対するセキュリティ要求の実践をチェックする仕組みも整備されているが、まだ改善の余地がある<br>・セキュアなシステム運用を実現するためのスキームについての検討のレベルはクラス B 以上<br>・セキュアなシステム運用を実現するためのスキームについての見直し状況はクラス B 以上<br>・セキュアなシステム運用を実現するためのスキームについての文書化のレベルはクラス B 以上 |
| レベル3 | システム運用をセキュアなものにするための工夫は相当に見られるが、十分とは言えない。システム運用周りで、不手際が生じる可能性は残る。また、問題が見逃される芳が残されている。<br>・システムの運用に対するすべてのセキュリティ対策を反映したセキュリティ要求の洗い出しに取り組んではいるが、十分とは言えない<br>・システム運用職場における運用関係者の職務遂行にかかるセキュリティ面での要求は、大まかではあるが、概ね適切に洗い出されている<br>・システム運用に対するセキュリティ要求のシステム運用マニュアルやシステム操作マニュアルへの反映は行われているが、確認は十分ではなく、その十分性は不透明<br>・大まかではあるが、システム運用に対するセキュリティ要求の実践をチェックする仕組みも作られている<br>・セキュアなシステム運用を実現するためのスキームについての検討のレベルはクラス B 以上<br>・セキュアなシステム運用を実現するためのスキームについての見直し状況はクラス B 以上<br>・セキュアなシステム運用を実現するためのスキームについての文書化のレベルはクラス B 以上 |
| レベル2 | システム運用チーム内には、習慣的に形成されたセキュアなシステム運用を実現するための仕組みがあり、現実に用いられおり、十分には程遠いが、システム運用チームのセキュアなシステム運用の実現への取り組みは評価できる。 |

| | |
|---|---|
| | ・システム運用チーム内には、セキュなシステム運用を実現するための仕組みとして、習慣的に形成されたものがあり、実際に機能している<br>・重要な事項については、システム運用の関係者に伝えられている<br>・システム運用関係者は、これらについて承知している<br>・セキュアなシステム運用を実現するためのスキームについての文書化のレベルはクラスＣ以上 |
| レベル1 | システム運用をセキュアなものにするための組織的な取組みについては、ほとんど検討されていない。<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システム運用職場における、日々のシステム運用に求められているセキュリティ要求の実践は、徹底しているともに、そのチェックも徹底しており、システム運用におけるセキュリティ要求の実践に、漏れやミス等の不手際が生じることは、まず考えられない。<br>・実施すべきセキュリティ対策にかかわるシステム運用は、日々的確に指定されている<br>・その計画や実行は、チェックリスト他の管理上の仕組みに沿って、十分にチェックされている<br>・セキュリティ対策にかかわるシステム運用の記録も、指定にそって的確に行われている<br>・日々のシステム運用におけるセキュリティ要求の実行についての管理の徹底状況はクラスＡ<br>・日々のシステム運用におけるセキュリティ要求のの実践状況についての文書化のレベルはクラスＡ |
| レベル4 | システム運用職場における、日々のシステム運用に求められているセキュリティ要求の確実な実践の追及は行われているが、一部に徹底さを欠くところが見られる。システム運用におけるセキュリティ要求の実践に、漏れやミス等の不手際が生じる隙が、僅かではあるが残されている。<br>・実施すべきセキュリティ対策にかかわるシステム運用は、日々的確に指定されている<br>・その計画や実行は、チェックリスト他の管理上の仕組みに沿って、チェックはされているが、徹底さに欠けるところも見られる<br>・セキュリティ対策にかかわるシステム運用の記録も、指定にそって概ね適切に行われている<br>・日々のシステム運用におけるセキュリティ要求の実行についての管理の徹底状況はクラスＢ以上<br>・日々のシステム運用におけるセキュリティ要求の実践状況についての文書化のレベルはクラスＢ以上 |
| レベル3 | システム運用職場における、日々のシステム運用に求められているセキュリティ要求の実行は、管理されてはいるが、十分とは言えない。日々のシステム運用におけるセキュリティ要求の実践に、漏れやミス等の不手際が生じる余地が残されている。<br>・実施すべきセキュリティ対策にかかわるシステム運用は、日々、指定されている<br>・その計画や実行は、なんらかの管理上の仕組みに沿って、チェックされることになっているが、十分なものとは言えない<br>・セキュリティ対策にかかわるシステム運用の記録も、一部行われている<br>・日々のシステム運用におけるセキュリティ要求の実行についての管理の徹底状況はクラスＢ以上<br>・日々のシステム運用におけるセキュリティ要求の実践状況についての文書化のレベルはクラスＢ以上 |
| レベル2 | システム運用におけるセキュリティ要求の実行は、システム運用関係者に任されているが、システム運用関係者は、セキュリティ要求の実行についての意識はあり、それなりの注意を払っている。組織的な管理にはなっていない。日々のシステム運用におけるセキュリティ要求の実践に、漏れやミス等の不手際が生じる可能性がある。<br>・システム運用関係者は、システム運用におけるセキュリティ対策関係の作業について、その確実な実行に心がけている<br>・組織的な管理はほとんど行われていない |

| | |
|---|---|
| | ・日々のシステム運用におけるセキュリティ要求の実践状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | システム運用におけるセキュリティ要求の実行についての明確な取組みは見られないに等しい<br>・レベル2の達成要件も満たしていない |

## Ｔｃ5.3　運用環境の保全の確保

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 運用環境の保全についての仕組みも完備し、この仕組み沿った運用環境の保全措置が確実に行われており、運用環境の保全についての事故の発生は、まず考えられない。<br>・他の環境との物理的な隔離や論理的な隔離は十分に行われている<br>・運用環境のソフト資産や情報資産の保護について、よく検討されたルールやその実践を管理する仕組みも確立している<br>・運用環境への物理的アクセスならびに論理的なアクセスについて、十分に厳格な制限が設けられている<br>・運用環境への要求される物理的なアクセス制限や、論理的なアクセス制限を実現するための設備やシステムへの必要な機能の組込みは完全で、これらは期待通り機能している<br>・運用環境の操作に対するよく検討された管理の仕組みが確立している<br>・運用環境の操作は、ルールに沿って丁寧に行われており、その確実な運用についてのチェックも徹底している<br>・万一に備えたバックアップの取得と保管も確実に行われている<br>・運用環境の保全手段ならびにその実行管理の仕組みについての検討状況はクラスＡ<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスＡ<br>・運用環境の保全にかかる措置についての見直し状況はクラスＡ<br>・運用環境の保全にかかる指定された措置やその実践状況についての文書化のレベルはクラスＡ |
| レベル4 | 運用環境の保全についての仕組みもよく整備され、この仕組み沿った運用環境の保全措置が行われているが、一部に見直すべきところも残る。運用環境の保全についての事故が発生する隙が、僅かではあるが残されている。<br>・他の環境との物理的な隔離や論理的な隔離は、ほぼ十分<br>・運用環境のソフト資産や情報資産の保護についてのルールやその実践を管理する仕組みも作られているが、まだ強化すべきところもある<br>・運用環境への物理的アクセスならびに論理的なアクセスについて、相当に厳格な制限が設けられている<br>・運用環境への要求される物理的なアクセス制限や、論理的なアクセス制限を実現するための設備やシステムへの必要な機能の組込みは、ほぼ完全<br>・運用環境の操作に対する管理の仕組みも作られている<br>・運用環境の操作は、ルールに沿って行われており、その確実な運用についてのチェックも行われている<br>・万一に備えたバックアップの取得と保管も行われているが、徹底さに欠けるところもある<br>・運用環境の保全手段ならびにその実行管理の仕組みについての検討状況はクラスＢ以上<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスＢ以上<br>・運用環境の保全にかかる措置についての見直し状況はクラスＢ以上<br>・運用環境の保全にかかる指定された措置やその実践状況についての文書化のレベルはクラス Ｂ 以上 |
| レベル3 | 運用環境の保全についての仕組みも作られ、運用環境の保全措置についての組織的な取組みは行われているが、環境の隔離や、運用上での必要な措置等は、一通り行われているが、十分なものとは言い難い。運用環境の保全についての事故が発生する余地が残されている。<br>・他の環境との物理的な隔離や論理的な隔離は、一応行われているが、十分とは言えない |

| | |
|---|---|
| | ・運用環境のソフト資産や情報資産の保護についてのルールやその実践を管理する仕組みも示されているが、大まかなものである<br>・運用環境への物理的ならびに論理的なアクセスに対する制限も行われているが、厳格なものではない<br>・運用環境への要求される物理的なアクセス制限や、論理的なアクセス制限を実現するための設備やシステムへの必要な機能の組込みも行われているが、その検証は徹底されたものではない<br>・運用環境の操作に対する管理の仕組みも作られているが、大まかなものである<br>・運用環境の操作についてのチェックも行われているが、徹底したものではない<br>・万一に備えたバックアップの取得と保管も行われているが、十分とは言い難い<br>・運用環境の保全手段ならびにその実行管理の仕組みについての検討状況はクラスB以上<br>・本対策要求かかる指定された措置の実践と管理の徹底状況はクラスB以上<br>・運用環境の保全にかかる措置についての見直し状況はクラスB以上<br>・運用環境の保全にかかる指定された措置やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル2 | たの環境との分離も十分とは言えず、運用環境の保全は運用部門に任されている。運用部門では相応の注意を払っているが、組織的な取組みにはほど遠い。運用環境の保全にかかる事故が発生する可能性がある。<br>・他の環境との物理的な隔離や論理的な隔離は、あまり行われていない<br>・運用環境への物理的ならびに論理的なアクセスに対する制限も存在するが、あまり実効的なものとは言えない<br>・運用環境の操作は、システム運用の管理者や担当者の注意に任されている<br>・万一に備えたバックアップの取得と保管は、あまり行われていない<br>・運用環境の保全にかかる指定された措置やその実践状況についての文書化のレベルはクラス C 以上 |
| レベル1 | 運用環境の保全についての取組みは、ないに等しい<br>・レベル2の達成要件も満たしていない |

## Tc5.4 システムの切替えの安全の確保

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムの切替えにおける安全の確保についての仕組みも完備し、この仕組み沿ったシステムの切替えが確実に行われており、システムの切替えにおいて事故は、まず考えられない。<br>・必要な事項のすべてを網羅した厳格な切替えシステムの受入れ要領ならびにシステムの切替え要領が確立している<br>・システムの受入れならびに切替えは、定められたルールに沿って厳格な管理の下で行われている<br>・切替えは、ルールに沿った十分な準備の下で行われている<br>・システムの切替えの安全の確保のための手段ならびにその実行管理の仕組みについての検討状況はクラスA<br>・システムの切替えの安全の確保のために要求されている措置の実践と管理の徹底状況はクラスA<br>・システムの切替えの安全の確保にかかる措置についての見直し状況はクラスA<br>・システムの切替えの安全の確保のために要求されている措置やその実践状況についての文書化のレベルはクラスA |
| レベル4 | システムの切替えの安全を図るための仕組みもよく整備され、システムの切替えはこの仕組みに沿って行われているが、一部に見直すべきところも残る。システムの切替えにおいて事故が発生する可能性が、僅かではあるが残されている。 |

| | |
|---|---|
| | ･必要な事項のすべてを網羅した厳格な切替えシステムの受入れ要領ならびにシステムの切替え要領が確立しているが、内容的に厳格さに欠けるところも残る<br>･システムの受入れならびに切替えは、定められたルールに沿って、概ね、組織的な管理の下で厳格に行われているが、一部に徹底さを欠くところが見られる<br>･切替えは、ルールに沿った準備の下で行われることになっているが、一部に厳格さに欠けるところが見られる<br>･システムの切替えの安全の確保のための手段ならびにその実行管理の仕組みについての検討状況はクラスＢ以上<br>･システムの切替えの安全の確保のために要求されている措置の実践と管理の徹底状況はクラス Ｂ 以上<br>･システムの切替えの安全の確保にかかる措置についての見直し状況はクラスＢ以上<br>･システムの切替えの安全の確保のために要求されている措置やその実践状況についての文書化のレベルはクラスＢ以上 |
| レベル3 | 大まかではあるが、システムの切替えを安全に行うため仕組みも作られ、システムの切替えの安全確保についての組織的な取組みは行われているが、必要な措置の実践や管理は徹底したものではない。システムの切替えにおいて事故が発生する余地が残されている。<br>･必要な事項のすべてを網羅した厳格な切替えシステムの受入れ要領ならびにシステムの切替え要領が確立しているが、内容的には大まかなものである<br>･システムの受入れならびに切替えは、定められた手順に沿って行われているが、その管理は運用部門に任され、あまり厳格なものではない<br>･切替えの実行にあたってのは、諸準備は丁寧に行われているが、徹底した管理の下で行われているわけではない<br>･システムの切替えの安全の確保のための手段ならびにその実行管理の仕組みについての検討状況はクラスＣ以上<br>･システムの切替えの安全の確保のために要求されている措置の実践と管理の徹底状況はクラス Ｃ 以上<br>･システムの切替えの安全の確保にかかる措置についての見直し状況はクラスＣ以上<br>･システムの切替えの安全の確保のために要求されている措置やその実践状況についての文書化のレベルはクラスＣ以上 |
| レベル2 | システムの切替えの安全はシステムの運用部門に任されている。運用部門では相応の注意を払っているが、組織的な取組みにはほど遠い。システムの切替えにおいて事故が、発生してもおかしくはない。<br>･システムの切替えについての手順等は確立しいないが、システムの運用現場で習慣的なものは形成されている |
| レベル1 | システムの切替えの安全の確保についての取組みは、ないに等しい<br>･レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システム運用関係者におけシステム運用職場での行動に対する厳格なセキュリティが決められ、その実践も徹底しており、システム運用職場で人的要因による事故の防止は十分に図られている。<br>･運用関係者に対するシステム運用職場での行動についての厳しい要求が明示されている<br>･これらは教育等を通じシステム運用の職場に出入りする者に徹底されている<br>･システム運用職場では、これらを遵守するとともに、全員による人的事故防止への取組みがなされている<br>･不審な行動やセキュリティ違反については、厳しい追及が行われている |

| | |
|---|---|
| | ・システム運用職場における人的要因による事故防止策についての検討のレベルはクラスA<br>・システム運用職場における人的要因による事故防止策に関連する要求の実践とその管理の徹底状況はクラスA<br>・システム運用職場における人的要因による事故防止策についての見直し状況はクラスA<br>・システム運用職場における人的要因による事故防止策やその実践状況についての文書化のレベルはクラスA |
| レベル4 | システム運用関係者におけシステム運用職場での行動に対する厳格なセキュリティが決められ、その実践も追及されている。その徹底さを欠くところも見られるが、システム運用職場で人的要因による事故の防止は概ね十分に図られているが、まだ改善の余地がある。<br>・運用関係者に対するシステム運用職場での行動についての要求は明示されているが、厳格さに欠くところもある<br>・システム運用の職場に出入りする者に対するこれらの周知努力は行われている<br>・システム運用職場ではこれらはほぼ十分に遵守されているが、全員による人的事故防止への取組みにまでは至っていない<br>・不審な行動やセキュリティ違反については、追及は行われているが、厳格さに欠くと言える<br>・システム運用職場における人的要因による事故防止策についての検討のレベルはクラスB以上<br>・システム運用職場における人的要因による事故防止策に関連する要求の実践とその管理の徹底状況はクラスB以上<br>・システム運用職場における人的要因による事故防止策についての見直し状況はクラスB以上<br>・システム運用職場における人的要因による事故防止策やその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | 大まかで一般的なものではあるが、システム運用関係者におけシステム運用職場での行動に対するセキュリティ要求は示されており、システムの運用職場では、これらは概ね遵守されていると見ることができるが、その実践とその管理は徹底したものではない。システム運用職場で人的要因による事故の防止は、一応、図られているレベル。<br>・運用関係者に対するシステム運用職場での行動についての要求は示されているが、一般的なもので、対象システムの特性を反映したものでもない<br>・システム運用の職場に出入りする者に対するこれらの周知努力は、一応、行われている<br>・システム運用職場ではこれらは概ね遵守されていると見られるが、全員による人的事故防止への取組みには程遠い<br>・不審な行動やセキュリティ違反に対する追及は十分いは行われていない<br>・システム運用職場における人的要因による事故防止策についての検討のレベルはクラスB以上<br>・システム運用職場における人的要因による事故防止策に関連する要求の実践とその管理の徹底状況はクラスB以上<br>・システム運用職場における人的要因による事故防止策についての見直し状況はクラスB以上<br>・システム運用職場における人的要因による事故防止策やその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | システム運用職場においては、システム運用職場に出入りする者に対する行動の制約や不審な行動に対するチェック等についての認識は存在し、それなりの注意が行われているが、組織的な取組みには至っていない。<br>・システム運用職場の管理者は、システム運用職場における人的要因による事故防止に関心を持っている<br>・システム運用職場での一般的な注意事項はある程度守られている<br>・システム運用職場における人的要因による事故防止策についての文書化のレベルはクラスC以上 |
| レベル1 | システム運用職場における人的要因による事故防止に対する、組織的な取組みはないに等しい<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 外部に委託するシステム運用に対するセキュリティ要求の確立し、委託先へのその実践の要求ならびにその監督指導も行える環境も整備され、委託先でのセキュリティ対策も十分に行われていることが担保されている。システム運用の外部委託を要因とするセキュリティ事故は、まず考えられない。<br>・システム運用の外部委託についての徹底したリスク分析にもとづく、よく検討された漏れのない委託先に対するセキュリティ要求が確立している<br>・委託先におけるこれらの要求の実践についての監督指導の仕組みや、委託先とのコミュニケーションの環境も確立している<br>・委託にかかる契約書等での委託元と委託先双方の責務には、これらはすべて的確に反映されている<br>・委託先におけるセキュリティ要求の実践は十分であることが、常時、確認されている<br>・委託先とのセキュリティ対策に関するコミュニケーションは十分行われている<br>・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方法についんての検討のレベルはクラスA<br>・委託先でのセキュリティ要求の実践についての確認の徹底状況はクラスA<br>・システム運用の外部委託についてのセキュリティ対策についての見直し状況はクラスA<br>・システム運用の外部委託についてのセキュリティ対策や委託先も含むその実践状況についての文書化のレベルはクラスA |
| レベル4 | 外部に委託するシステム運用に対するセキュリティ要求も明示され、委託先へのその実践の要求ならびにその監督指導も行えるようになっており、委託先でのセキュリティ対策が十分に行われる環境は、一応、形成されているが、セキュリティ要求やその実践の担保については、厳格さを欠くところも残っている。システム運用の外部委託を要因とするセキュリティ事故が起こる隙が、僅かではあるが残されている。<br>・システム運用の外部委託についてのリスク分析にもとづく、よく検討された委託先に対するセキュリティ要求が示されているが、リスク分析やセキュリティ対策についての要求には甘いところも残されえている<br>・委託先におけるこれらの要求の実践についての監督指導の仕組みや、委託先とのコミュニケーションの仕組みも、一応、作られている<br>・委託にかかる契約書等での委託元と委託先双方の責務には、これらは概ね反映されているが、まだ、見直すべきところもある<br>・委託先におけるセキュリティ要求の実践は十分であることは、継続的に確認されているが、それほどは徹底したものとは言い難い<br>・委託先とのセキュリティ対策に関するコミュニケーションは行われているが十分に密とは言えない<br>・外部委託におけるセキュリティの確保の方法についての検討のレベルはクラスB以上<br>・委託先でのセキュリティ要求の実践についての確認の徹底状況はクラスB以上<br>・システム運用の外部委託についてのセキュリティ対策についての見直し状況はクラスB以上<br>・システム運用の外部委託についてのセキュリティ対策や委託先も含むその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | 外部に委託するシステム運用に対するセキュリティ要求の検討、ならびに委託先へのその実践の要求ならびにその監督指導等のシステム運用の委託についてのセキュリティ対策についてお組織的な取組みは行われているが、十分とはいえないところもある。システム運用の外部委託を要因とするセキュリティ事故が発生する余地が残されている。<br>・委託先に対するセキュリティ要求は示されているが、大まかなもので、重要なところを除いては十分とは言えないところがある<br>・委託にかかる契約書等での委託元と委託先双方の責務は示されているが、大まかなもので、具体性に欠ける<br>・委託先におけるセキュリティ要求の実践は、すべて委託先に任されているが、その状況についての報告は受けている<br>・外部委託におけるセキュリティの確保の方法についての検討のレベルはクラスB以上<br>・委託先でのセキュリティ要求の実践についての確認の徹底状況はクラスB以上 |

| | |
|---|---|
| | ・システム運用の外部委託についてのセキュリティ対策についての見直し状況はクラスB以上<br>・システム運用の外部委託についてのセキュリティ対策や委託先も含むその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | 外部へのシステム運用の委託にあたってのセキュリティ要求は行われているが、一般的なものに止まっており、すべては委託策に任されており、実質的な管理は行ってない。<br>・システム運用の委託にあたってのセキュリティ要求は、大まかなものではあるが委託先に示されている<br>・委託先では、セキュリティ要求に対する必要な対応は行われることになっている<br>・システム運用の外部委託についてのセキュリティ対策や委託先も含むその実践状況についての文書化のレベルはクラスC以上 |
| レベル1 | 外部委託しているシステム運用のセキュリティ対策はすべて委託先任せで、委託先の責任も委託先の方針をそのまま受け入れている。<br>・レベル2の達成要件も満たしていない |

## 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 長期間にわたる保管が必要となる電子情報に対し、長期保管のための必要な措置が適切にとられ、何時でも使用できるようにするとともに、保管期間を通じて、その有効性が維持されるようにするための完成度の高い組織的な管理の仕組みが確立している。<br>・電子情報の長期保管についての責任体制が確立している<br>・長期保管する電子情報（群）とその保管形態（注 1）、およびそのそれぞれに対するきめの細かい保管基準（注2）が決められている<br>・保管に法的な要求がかかわる電子情報に対しては、この保管基準の作成において、その法的準拠性についての確認が、技術ならびに法律の両面から専門家の助言も得て行われている<br>・タイムスタンプに用いる公開鍵の有効期間切れ対策として必要な措置が明示されマニュアル化されている<br>・電子情報の保管にかかわる措置等についての記録の作成やその保管についても、厳格なルールが決められている<br>・長期保管の対象となる電子情報のルールに沿った物理的な保管や有効性維持のために必要となる措置の実施を管理する仕組みも確立している<br>・特に、電子化して長期保管する情報に対する電子化プロセスについての、関係法令に準拠した厳格な管理の下で行うようにされている<br>・この電子情報の長期保管にかかわる管理スキームについての検討のレベルはクラス A<br>・この管理スキームについての見直し状況はクラス A<br>・この管理スキームについての文書化のレベルはクラス A |
| レベル4 | 長期間にわたる保管が必要となる電子情報に対し、長期保管のための必要な措置が適切にとられ、何時でも使用できるようにするとともに、保管期間を通じて、その有効性が維持されるようにするためのよく検討された組織的な仕組みが作られているが、まだ改善の余地も残る。<br>・電子情報の長期保管についての責任体制が確立している<br>・長期保管する電子情報（群）とその保管形態（注 1）、およびそのそれぞれに対するきめの細かい保管基準（注2）が決められているが、まだ、手を入れるべきところも一部残されている<br>・保管に法的な要求がかかわる電子情報に対しては、この保管基準の作成において、その法的準拠性についての確認が、技術ならびに法律の両面から専門家の助言も得て行われている<br>・タイムスタンプに用いる公開鍵の有効期間切れ対策として必要な措置が明示されマニュアル化されているが、まだ、手を入れるべきところも一部残されている<br>・電子情報の保管にかかわる措置等についての記録の作成やその保管についても、厳格なルールが決められている<br>・長期保管の対象となる電子情報のルールに沿った物理的な保管や有効性維持のために必要となる措置の実施を管理する仕組みも確立している<br>・特に、電子化して長期保管する情報に対する電子化プロセスについての、関係法令に準拠した管理の下で行うようにされている<br>・この電子情報の長期保管にかかわる管理スキームについての検討のレベルはクラス B 以上<br>・この管理スキームについての見直し状況はクラス B 以上<br>・この管理スキームについての文書化のレベルはクラス B 以上 |
| レベル3 | 長期間にわたる保管が必要となる電子情報に対し、長期保管のための必要な措置が適切にとられ、何時でも使用できるようにするとともに、保管期間を通じて有効性が維持されるようにするための仕組みが、組織的な検討の下で作られている。必要なことは概ね適切に示されているが、細部について十分とは言い難い。<br>・電子情報の長期保管についての責任体制が確立している<br>・おおまかではあるが、長期保管する電子情報（群）とその保管形態（注 1）、およびそのそれぞれに対 |

| | |
|---|---|
| | するきめの細かい保管基準（注2）が決められている<br>・保管に法的な要求がかかわる電子情報に対しては、この保管基準の作成において、その法的準拠性についての確認が、技術ならびに法律の両面から専門家の助言も得て行われている<br>・タイムスタンプに用いる公開鍵の有効期間切れ対策として必要な措置が明示されマニュアル化されているが、まだ、手を入れるべきところも一部残されている<br>・電子情報の保管にかかわる措置等についての記録の作成やその保管についても、厳格なルールがおおまかではあるが決められている<br>・長期保管の対象となる電子情報のルールに沿った物理的な保管や有効性維持のために必要となる措置の実施を管理する仕組みも、大まかなものが作られている<br>・特に、電子化して長期保管する情報に対する電子化プロセスについての、関係法令に準拠した管理の下で行うようにされている<br>・この電子情報の長期保管にかかわる管理スキームについての検討のレベルはクラスB以上<br>・この管理スキームについての見直し状況はクラスB以上<br>・この管理スキームについての文書化のレベルはクラスB以上 |
| レベル2 | 法的要求への対応は考えていないが、長期間にわたる保管が必要となる電子情報に対する保管についての方針が示されており、長期保管のために必要となる措置については、電子情報の保管を担当するチーム内で決めたものである。基本的なものは概ね適切に示されているが十分なもの言えない。<br>・電子情報の長期保管についての担当者は決められている<br>・長期保管する電子情報（群）とその保管形態（注1）、およびそのそれぞれに対する保管基準（注2）については、基本的なことは示されているが、実施上の細部は担当チームに任されている<br>・この電子情報の長期保管にかかわるスキームについての検討のレベルはクラスC以上<br>・このスキームについての見直し状況はクラスC以上<br>・このスキームについての文書化のレベルはクラスC以上 |
| レベル1 | 電子情報の長期的な保管を適切に行うための組織的な管理スキームは作られていないに等しい。<br>・レベル2の達成要件も満たしていない |

(注1) 保管形態として指定すべきこととしては、以下があげられる。
- ・使用媒体（マイクロフィルム、電子データ、紙）
- ・保管場所と保管方法
- ・保管装置

(注2) 長期保管の対象となる電子情報の保管基準として指定すべき事項
- ・法的要求
- ・保管期間
- ・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
- ・入力要件（入力プロセス）
- ・システム要件（解像度、階調、ファイル形式）

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 長期保管を行う電子情報の有効な長期保管を実現するために用いるツールや設備は、現時点では最も強力なものが採用され、また、その実装および必要な維持管理も徹底しており、期待通りに機能していることが、常に、確認されている。<br>・文書等のデジタル化は認定を受けている組織・システムを用いている<br>・タイムスタンプの取得には、認定を受けた業者を使用している<br>・タイムスタンプに用いる暗号強度は、現時点で最強レベルのものを使用している<br>・タイムスタンプに用いる公開鍵の有効期間切れ対策は完全に行われている<br>・これらのシステムの有効性の維持管理のための仕組みも確立しており、これらの導入時のテストならびに維持管理は徹底しており、すべての関係しいステムは期待通り機能していることが確認されている<br>・保管対象の物理媒体の保管場所として、電子媒体の長期保管を前提とした特別な設備が準備されている<br>・電子情報の長期保管に用いるシステムや施設や設備についての検討のレベルはクラスA<br>・これらのシステムの維持管理を適切に行うための管理の仕組みの確立状況はクラスA<br>・これらのシステムについての見直し状況はクラスA<br>・これらのシステムの文書化ならびにその維持管理についての記録の作成のレベルはクラスA |
| レベル4 | 長期保管を行う電子情報の有効な長期保管を実現するために用いるツールや設備は、最強とは言えないまでも平均以上のものが採用され、その実装および必要な維持管理も徹底しており、期待通りに機能していることが確認されている。<br>・文書等のデジタル化は認定を受けている組織・システムを用いている<br>・タイムスタンプの取得には、認定を受けた業者を使用している<br>・タイムスタンプに用いる暗号強度は、現時点で最強レベルのものを使用している<br>・タイムスタンプに用いる公開鍵の有効期間切れ対策は完全に行われている<br>・これらのシステムの有効性の維持管理のための仕組みも確立しており、これらの導入時のテストならびに維持管理は徹底しており、すべての関係しいステムは期待通り機能していることが確認されているが、一部に徹底さを欠くところも見られる<br>・保管対象の物理媒体の保管場所として、電子媒体の長期保管を前提とした特別な設備が準備されている<br>・電子情報の長期保管に用いるシステムや施設や設備についての検討のレベルはクラスB以上<br>・これらのシステムの維持管理を適切に行うための管理の仕組みの確立状況はクラスB以上<br>・これらのシステムについての見直し状況はクラスB以上<br>・これらのシステムの文書化ならびにその維持管理についての記録の作成のレベルはクラスB以上 |
| レベル3 | 長期保管を行う電子情報の有効な長期保管を実現するために用いるツールや設備としては、平均的なものが使われている。その実装および必要な維持管理も、組織的にチェックされており、ツール面での不備が、長期保管する電子情報の有効性を損ねることは、あまり考えられない。<br>・文書等のデジタル化は認定を受けている組織・システムを用いている<br>・タイムスタンプの取得には、認定を受けた業者を使用している<br>・タイムスタンプに用いる暗号強度は、現時点で最強レベルのものを使用している<br>・タイムスタンプに用いる公開鍵の有効期間切れ対策は完全に行われている<br>・これらのシステムの有効性の維持管理のための仕組みも確立しており、これらの導入時のテストならびに維持管理は徹底しており、すべての関係しいステムは期待通り機能していることが確認されているが、一部に徹底さを欠くところも見られる<br>・保管対象の物理媒体の保管場所は、マシン室レベルの場所を使用<br>・電子情報の長期保管に用いるシステムや施設や設備についての検討のレベルはクラスB以上<br>・これらのシステムの維持管理を適切に行うための管理の仕組みの確立状況はクラスB以上<br>・これらのシステムについての見直し状況はクラスB以上 |

| | |
|---|---|
| | ･これらのシステムの文書化ならびにその維持管理についての記録の作成のレベルはクラス B 以上 |
| レベル 2 | 長期保管を行う電子情報の有効な長期保管を実現するために、特別にツールや設備は準備せず、通常のマシン室まわりの通常の設備を用いている。法的な効力の確保･維持についての要求には応えられないが、内部情報としての長期保管については、最低限の対応はできる。<br>･保管対象の物理媒体の保管場所は、マシン室レベルの場所を使用<br>･電子情報の長期保管に用いるシステムやその維持管理の方法についての検討はレベル C<br>･これらのシステムについての見直し状況はクラス C 以上<br>･これらのシステムの文書化ならびにその維持管理についての記録の作成のレベルはクラス C 以上 |
| レベル 1 | (該当なし) |

(注 1) 本要求に対しては、タイムスタンプに用いる暗号強度や、媒体の保管場所の設備のレベル以対策強度 3～5は共通 (差がない)

## Td1.3 長期保管の対象情報に対する保管要件の指定

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | 長期保管する情報のそれぞれに対し、その有効性を維持するために要求されること、ならびにその要求に応えるためにその保管の全期間を対して必要な措置が、確立した管理の仕組みに沿って、徹底した検討とレビューの下で指定されており、その指定に不備が入り込むことは、まず考えられない。<br>･長期保を行う電子情報に対する保管要件の指定要領ならびに適切な指定を管理するための組織的な仕組みとしては、レベル 5 相当として確立している (注1)<br>･電子情報として長期保管の対象となるものはすべて洗い出されている<br>･長期保管する電子情報の個々に対する保管要件として指定されなければならないこと (注2) のすべてに適切な指定がされている<br>･これらの指定のレビューもルールどおり徹底して行われている<br>･長期保管をおこなう電子情報に対する保管要件の指定についての検討ならびにそのレビューのレベルはクラス A<br>･長期保管をおこなう電子情報に対する保管要件の指定ついての見直し状況はクラス A<br>･長期保管をおこなう電子情報に対する保管要件の指定についての文書化のレベルはクラス A |
| レベル 4 | 長期保管する情報のすべてに対し、保管の全期間において、その有効性を維持するために要求されること、ならびにその要求に応えるために必要な措置が、確立した仕組みの上で個々によく指定されているが、対象情報の網羅性や指定のきめ細かさに、まだ改善の余地がある。その指定に不備が入り込む隙が、僅かではあるが残されている。<br>･長期保を行う電子情報に対する保管要件の指定要領ならびに適切な指定を管理するための組織的な仕組みとしては、レベル4相当以上のものが確立している (注1)<br>･電子情報として長期保管の対象となるものは、すべて洗い出されている<br>･長期保管する電子情報の個々に対する保管要件として指定されなければならないこと (注2) のすべてに適切な指定がされているが、一部に徹底さを欠くところも見られる<br>･これらの指定のレビューもルールどおり行われているが、一部に徹底さを欠くところも見られる<br>･長期保管をおこなう電子情報に対する保管要件の指定についての検討ならびにそのレビューのレベルはクラス B 以上<br>･長期保管をおこなう電子情報に対する保管要件の指定ついての見直し状況はクラス B 以上<br>･長期保管をおこなう電子情報に対する保管要件の指定についての文書化のレベルはクラス B 以上 |
| レベル 3 | 長期保管する情報に対する、保管の全期間において、その有効性を維持するために要求されること、ならびにその要求に応えるために必要な措置の指定が、策定された管理の仕組みに沿って、検討･レビューされ指定されているが、徹底したものではなく、対象情報の網羅性や指定のきめ細かさに、まだ改善の余地があり、この指定に不備が入り込む可能性も残されている。 |

| | |
|---|---|
| | ・長期保を行う電子情報に対する保管要件の指定要領ならびに適切な指定を管理するための組織的な仕組みとしてはは、レベル3相当以上のものが確立している（注1）<br>・電子情報として長期保管の対象となるものは、概ね、洗い出されている<br>・長期保管する電子情報の個々に対する保管要件として指定されなければならないこと（注2）の指定は、概ね指定がされているが、きめの細かさに足りないところも少なくない<br>・これらの指定のレビューは、担当社レベルに止まっている<br>・長期保管をおこなう電子情報に対する保管要件の指定についての検討ならびにそのレビューのレベルはクラスＣ以上<br>・長期保管をおこなう電子情報に対する保管要件の指定ついての見直し状況はクラスＢ以上<br>・長期保管をおこなう電子情報に対する保管要件の指定についての文書化のレベルはクラスＢ以上 |
| レベル2 | 長期保管する情報に対する、保管の全期間において、その有効性を維持するために要求されること、ならびにその要求に応えるために必要な措置の指定が、担当チーム内に習慣的に形成された考えにもとづいて指定されているが、対象情報の網羅性や指定は大まかなもので、すべては担当チームに任されている。<br>・電子情報として長期保管の対象となるものは、重要なものについては洗い出されている<br>・長期保管する電子情報の個々に対する保管要件として指定されなければならないこと（注2）の指定は、基本的なことに止まっている<br>・これらの指定は担当チームに任されている<br>・長期保管をおこなう電子情報に対する保管要件の指定についての検討ならびにそのレビューのレベルはクラスＤ以上<br>・長期保管をおこなう電子情報に対する保管要件の指定ついての見直し状況はクラスＣ以上<br>・長期保管をおこなう電子情報に対する保管要件の指定についての文書化のレベルはクラスＣ以上 |
| レベル1 | （該当せず） |

(注 1) このことについては、対策要求 Tb1.1でも求められている。本要求について該当レベルの強度を持つためには、対策要求 Tb1.1についても対応の強度レベルが達成されていなければならない。

(注2) 長期保管の対象となる電子情報の保管要件として指定すべき事項

・保管の目的
・保管期間
・保管に使用する媒体
・保管場所と保管場所での保管方法
・求められる検索性と前提とする検索方法
・法的な要求に対する必要な措置
・ライフサイクルの各ステップにおける保管上の要件
　－作成にかかわる要件
　－電子化が必要な場合に必要となる電子化のプロセス
　－保管の手続き
　－保管場所と保管場所での保管方法
　－見読性の維持に必要な措置
　－廃棄の手続き
・長期電子署名の署名再検証を可能とする手段
　- 署名存在（検証）時刻を明確にすること（タイムスタンプの付与）
　- 署名検証時に署名再検証に必要な情報を明確にしておくこと
　- 署名再検証に必要な情報を改ざん検出可能な状態にすること（タイムスタンプの付与）
　- 署名再検証に必要な情報を保存すること（長期署名フォーマット）

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 長期保管を行う電子情報の作成から廃棄に至るまでの全ライフサイクルの個々のステップについて、指定されて管理要件に沿った保管上の措置の実施は厳格な管理の下で行われている。長期保管の対象となる電子情報に対する、指定要件に沿った保管に不手際が生じることは、まず考えられない。<br>・法的な有効性が問われる保管電子情報に対する法的有効性維持のための措置(注1)は、すべて的確に行われている<br>・保管電子情報に対する見読性の維持のために必要な措置(注2)も、すべての対象情報に対し、的確に行われている<br>・対象電子情報はすべて、指定された保管場所において指定方法で保管されている<br>・これらの措置を的確に行うための管理の仕組みは期待通り機能していて、実践上の不手際を見逃す可能性はまずない<br>・定期的にその実施状況や保管の適切さの確認検査も徹底して行われている<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスA |
| レベル4 | 長期保管を行う電子情報の作成から廃棄に至るまでの全ライフサイクルの個々のステップについて、指定されて管理要件に沿った保管上の措置の完全な実施を追及してはいるが、一部に徹底さをかくところも見られる。長期保管の対象となる電子情報に対する、指定要件に沿った保管は、まず、十分に行われている見ることができるが、不手際が生じる隙が、僅かではあるが残されている。<br>・法的な有効性が問われる保管電子情報に対する法的有効性維持のための措置(注1)は、ほとんどすべての情報に対して的確に行われている<br>・保管電子情報に対する見読性の維持のために必要な措置(注2)も、すべての対象情報に対し、ほとんどすべての情報に対し的確に行われている<br>・対象電子情報はすべて、指定された保管場所において指定方法で保管されている<br>・これらの措置を的確に行うための管理の仕組みは、概ね期待通り機能しているが、一部に徹底さを欠くところもあり、実践上の不手際を見逃す可能性が、少ないが残っている<br>・定期的にその実施状況や保管の適切さの確認検査も行われている<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | 法的有効性が問われる電子情報のすべてに対しては、レベル4と同等の措置がとられているが、法定期有効性が問われない電子情報については、重要なステップについて、指定されて管理要件に沿った保管上の措置の完全な実施を追及してはいるが、それほど厳格な保管管理は行われていない。長期保管の対象となる電子情報に対する、指定要件に沿った保管は、概ね、適切に行われている見ることができるが、不手際が生じる隙が残されている。<br>・法的な有効性が問われる保管電子情報に対する法的有効性維持のための措置(注1)は、ほとんどすべての情報に対して的確に行われている<br>・保管電子情報に対する見読性の維持のために必要な措置(注2)も、すべての対象情報に対し、ほとんどすべての情報に対し的確に行われている<br>・対象電子情報はすべて、指定された保管場所において指定方法で保管されているが、法的有効性が問われない情報に対する保管にずさんなところも見られる<br>・これらの措置を的確に行うための管理の仕組みは、概ね期待通り機能しているが、一部に徹底さを欠くところもあり、実践上の不手際を見逃す可能性が、少ないが残っている<br>・定期的にその実施状況や保管の適切さの確認検査も行われている<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラスB以上 |
| レベル2 | 担当チームは、担当チーム内で習慣的に形成されている方法に沿って、長期保管を行う電子情報に対して、保管上必要としている措置を講じており、基本的なことは行われていると見ることができるが、組織的な管理の下で行われているとは言い難く、長期保管の対象となる電子情報に対する、指定要件に沿った保管に、不手際が生じることも考えられる。<br>・保管電子情報に対する見読性の維持のために必要な措置は、一応、行われてはいるが、徹底には |

| | |
|---|---|
| | 程遠い<br>・対象電子情報は、概ね、指定された保管場所において指定方法で保管されている<br>・これらの措置の管理は担当者に任されている<br>・本対策要求かかる指定された措置やその実践状況についての文書化のレベルはクラス C 以上 |
| レベル 1 | 長期保管する電子情報はあるが、組織的な取組みは行われていない。<br>・レベル 2 の達成条件にも満たない |

(注 1) 保管電子情報の法的な有効性維持のために必要な措置とは、以下のようなものを指す。
・法令に準拠した保存期間の確保
・認定取得事業者のサービスを利用した電子署名およびタイムスタンプの付与
・各種ガイドラインに準拠した保存手段の実装

(注2) 長期保管する電子情報の見読性の維持のために必要な措置としては、以下のようなものがある。
・別媒体への定期的な書き換え
・表示・印刷環境の確保（ハードウェア、OS、ソフトウェア）
・エミュレータの使用（他のハードウェアや他の OS による代替システムの確保）
・電子文書を紙やマイクロフィルムに出力して保管
・文書形式の変換（例＞Word 形式->PDF、HTML、TIFF）
・アプリケーションの継続確保
・アプリケーションに依存しない文書形式の使用

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | モバイルコンピューティングの利用業務ごとに、リスク分析にもとづくきめの細かいセキュリティ要求が示されており、これらはモバイル機器、モバイルコンピューティングをサポートするセンターシステム、およびモバイルコンピューティングの利用者のそれぞれについてのセキュリティ対策のテーマに的確に展開されている。<br>・モバイルコンピューティングの利用業務ごとのリスク分析にもとづく、適用業務の制限、利用者の制限、モバイル機器への情報の格納の制限、利用場所の制限等のそれぞれについてセキュリティ要求がきめ細かく定義されている<br>・このセキュリティ要求は、モバイル機器、モバイルコンピューティングをサポートするセンターシステム、およびモバイルコンピューティングの利用者のそれぞれに対するセキュリティ要求に展開されている<br>・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検討のレベルはクラスA<br>・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についての見直し状況はクラスA<br>・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についての文書化のレベルはクラスA |
| レベル4 | モバイルコンピューティングの利用業務ごとに、リスク分析にもとづくセキュリティ要求が、適用業務の制限、利用者の制限、モバイル機器への情報の格納の制限、利用場所の制限等のそれぞれについて示され、これらのモバイル機器、モバイルコンピューティングをサポートするセンターシステム、およびモバイルコンピューティングの利用者のそれぞれについてのセキュリティ対策のテーマへの展開も行われているが、リスク分析やセキュリティ要求への展開にきめの細かさに欠けるところもあり、まだ見直す余地も残る。<br>・リスク分析やセキュリティ要求の洗い出しは、モバイルコンピューティングの利用業務ごとに行われて入るが、きめ細かさに欠くところもある<br>・モバイル機器、モバイルコンピューティングをサポートするセンターシステム、およびモバイルコンピューティングの利用者に対するセキュリティ要求への展開も行われているが、十分とは言えないところがある<br>・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検討のレベルはクラスB以上<br>・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についての見直し状況はクラスB以上<br>・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についての文書化のレベルはクラスB以上 |
| レベル3 | 大まかではあるが、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は示され、モバイル機器、モバイルコンピューティングをサポートするセンターシステム、およびモバイルコンピューティングの利用者のそれぞれについてのセキュリティ対策のテーマへの展開も行われている。必要なことは、概ね、適切に指摘されているが、適用業務ごとの細かいリスク分析にもとづいたものではなく、十分な検討を基盤としたものとは言い難いところもある。<br>・モバイル機器、モバイルコンピューティングをサポートするセンターシステム、およびモバイルコンピューティングの利用者に対するセキュリティ要求は示されている適用業務やその利用環境の特性を細かく分析した結果とは言い難い<br>・適用業務やその利用環境の特性を細かい分析は行われていない<br>・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検討のレベルはクラスB以上<br>・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についての見直し状況はクラスB以上<br>・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についての文書化のレベルはクラスB以上 |
| レベル2 | 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は、個々の適用業務ごとのセキュリティ対策の検討に任されている。ただし、モバイルコンピューティングに対するセキュリティについて、一般的に言われている検討事項は意識されている。<br>・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注意事項は、システムの設計者やセキュリティ対策の担当者には意識されている<br>・適用業務ごとにシステムモバイル機器、モバイルコンピューティングをサポートするセンターシステム、およびモバイルコンピューティングの利用者に対するセキュリティ要求は、ある程度検討されている<br>・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検討のレベルはクラスC以上<br>・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についての見直し状況はクラスC以上 |

| | |
|---|---|
| | ・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についての文書化のレベルはクラスC以上 |
| レベル1 | モバイルコンピューティングについてのセキュリティ要求についての組織的な検討は、ほとんどおこなわれていない。<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | モバイルコンピューティングをサポートするセンターサイドのシステムには、モバイルコンピューティングにおけるセキュリティの確保のために、必要なセキュリティ機能が組み込まれ、これらは完全に機能していることが確認されている。<br>・モバイルコンピューティングの適用業務ごとに、モバイルコンピューティングにかかるセキュリティ要求を満足するための必要な機能が明確にされている<br>・これらの機能のシステムの組込みは完全であることが十分なテストで確認されている<br>・センターシステムサイドで必要な機能とその実装方式についての検討のレベルはクラスA<br>・必要な機能の見直しのレベルはクラスA<br>・モバイルコンピューティングに対するセンサーシステムサイドでの必要なセキュリティ対策にについての文書化のレベルはクラスA |
| レベル4 | モバイルコンピューティングをサポートするセンターサイドのシステムには、モバイルコンピューティングにおけるセキュリティの確保のために、利用者の認証、利用系脳の制限、通信の保護、使用時間対の制限、タイムアウト機能、アクセスログの取得等のすべてについて、必要なセキュリティ機能が組み込まれているが、これらのシステムへの組込みの的確性についての確認に、一部徹底さを欠くところも見られる。<br>・モバイルコンピューティングの適用業務ごとに、モバイルコンピューティングにかかるセキュリティ要求を満足するための必要な機能が示されているが、検討に十分とはいい難いところが残されている<br>・これらの機能のシステムの組込みについてはのテストは相当に厳格に行われているが、一部徹底さを欠くところも見られる<br>・センターシステムサイドで必要な機能とその実装方式についての検討のレベルはクラスB以上<br>・必要な機能の見直しのレベルはクラスB以上<br>・モバイルコンピューティングに対するセンサーシステムサイドでの必要なセキュリティ対策にについての文書化のレベルはクラスB以上 |
| レベル3 | モバイルコンピューティングをサポートするセンターサイドのシステムには、モバイルコンピューティングにおけるセキュリティの確保のための機能もある程度組み込まれているが、その的確性についての確認は徹底したものではない。<br>・モバイルコンピューティングの適用業務ごとに、モバイルコンピューティングにかかるセキュリティ要求に応えるための機能が示されいるが、利用者の認証、利用系脳の制限、通信の保護、使用時間対の制限、タイムアウト機能、アクセスログの取得等のすべてを十分にカバーしてはいない<br>・センターシステムサイドで必要な機能とその実装方式についての検討のレベルはクラスC以上<br>・必要な機能の見直しのレベルはクラスB以上<br>・モバイルコンピューティングに対するセンサーシステムサイドでの必要なセキュリティ対策にについての文書化のレベルはクラスB以上 |
| レベル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サイドのセキュリティ対策として、利用者の認証や利用機能の制限について、特別な配慮がされている程度。<br>・必要な機能の検討や実装およびその確認は、担当者に任されいる<br>・本要求についての文書化のレベルはC以上 |
| レベル1 | モバイルコンピューティングを意識したセキュリティ対策は、センターシステムサイドではほとんど考慮されていないに等しい。<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | モバイル端末へのセキュリティ要求の実現のための機能の実装や、利用者のモバイルコンピューティングの利用上でのセキュリティ要求についての実践は十分。<br>・モバイル端末に実装すべきセキュリティ対策機能は、すべてのモバイル端末に確実に実装されていることが、徹底して確認されている<br>・モバイルコンピューティングの利用者に対する利用上の注意事項は明確にされ、徹底されている<br>・利用者におけるこれらの注意事項の遵守は徹底してチェックされている<br>・モバイル端末に必要な機能とその実装方式についての検討、およびその見直しのレベルはクラスA<br>・モバイル端末へのセキュリティ対策機能とその実装状況についての文書化のレベルはクラスA<br>・モバイルコンピューティング利用者に対する利用上のセキュリティ要求の実践の管理や指導も徹底して行われている |
| レベル4 | モバイル端末へのセキュリティ要求の実現のための機能の実装や、利用者のモバイルコンピューティングの利用上でのセキュリティ要求についての実践の追求はされているが、徹底さに欠けるところも残る。<br>・モバイル端末に実装すべきセキュリティ対策機能は、すべてのモバイル端末に確実に実装されていることは確認されているが、徹底さに欠くところも残る<br>・モバイルコンピューティングの利用者に対する利用上の注意事項は明確にされているが、一部に徹底さに欠けるところが見られる<br>・利用者におけるこれらの注意事項の遵守はチェックされているがいるが、一部に徹底さに欠けるところが見られる<br>・モバイル端末への必要な機能とその実装方式についての検討、およびその見直しのレベルはクラスB以上<br>・モバイル端末へのセキュリティ対策機能とその実装状況についての文書化のレベルはクラスB以上<br>・モバイルコンピューティング利用者に対する利用上のセキュリティ要求の実践の管理や指導もよく行われているが、徹底さにかけるところも見られる |
| レベル3 | モバイル端末へのセキュリティ要求の実現のために必要となる機能の実装や、利用者のモバイルコンピューティングの利用上でのセキュリティ要求についての実践の要求はされているが、十分とは言えない。<br>・すべてのモバイル端末に対する、実装すべきセキュリティ対策機能の指定や、その実装の確認、および定期的な必要なセキュリティ機能の稼働状況の確認は十分とは言えない<br>・モバイルコンピューティングの利用者に対する利用上の注意事項は示されているが、利用者におけるこれらの注意事項の遵守は、ほとんどチェックされていない<br>・モバイル端末への必要な機能とその実装方式についての検討、およびその見直しのレベルはクラスB以上<br>・必要な機能の組込みの確認および定期的な機能の稼働確認のレベルはクラスB以上<br>・モバイル端末へのセキュリティ対策機能とその実装状況についての文書化のレベルはクラスB以上<br>・モバイルコンピューティング利用者に対する利用上のセキュリティ要求の実践についてのチェックや指導も行われることになっているが、徹底したものではない |
| レベル2 | 利用者の認証についてある程度の検討がなされ、利用上の一般的な注意がなされている程度で、モバイルコンピューティングの利用についての利用者サイドでの安全確保は、利用者の意識に依存している。 |
| レベル1 | 利用者サイドにおけるモバイルコンピューティングを意識したセキュリティ対策は、ほとんど考慮されていないに等しい。<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | すべてのリモートオフィスについてのリスク分析にもとづくきめの細かいセキュリティ対策が検討され、それぞれのオフィスごとに的確なセキュリティ対策の組み立てが示されている。<br>・すべてのリモートオフィスごとに、保護資産の洗い出しやリスク分析が行われている<br>・すべてのリモートオフィスごとに、そのセキュリティ環境の特性を反映したセキュリティ要求と、セキュリティ対策の組み立ては検討が、十分きめ細かく検討されている<br>・リモートオフィスごとのセキュリティ要求のフレームワークに検討のレベルはクラスA<br>・リモートオフィスごとのセキュリティ要求のフレームワークについての見直し状況はクラスA<br>・リモートオフィスごとのセキュリティ要求のフレームワークについての文書化のレベルはクラスA |
| レベル4 | すべてのリモートオフィスについてのリスク分析にもとづくセキュリティ対策が検討され、それぞれのオフィスごとに的確なセキュリティ対策の組み立てが示されているが、きめの細かさにかけるところがある。<br>・保護資産の洗い出しやリスク分析は、すべてのリモートオフィスごとに行われている<br>・すべてのリモートオフィスごとに、そのセキュリティ環境の特性を反映したセキュリティ要求と、セキュリティ対策の組み立ては検討されているが、十分きめ細かく検討されているわけではない<br>・リモートオフィスごとのセキュリティ要求のフレームワークに検討のレベルはクラスB以上<br>・リモートオフィスごとのセキュリティ要求のフレームワークについての見直し状況はクラスB以上<br>・リモートオフィスごとのセキュリティ要求のフレームワークについての文書化のレベルはクラスB以上 |
| レベル3 | リモートオフィスに対するセキュリティ対策の組み立ての検討は、拠点におけるセキュリティ対策を、リモートオフィスの環境に適用させるような検討が中心で、リモートオフィスごとのリスク分析にもとづく、きめ細かい検討は行われていない。<br>・拠点を対象に検討されたセキュリティ対策の組み立ての、リモートオフィスへの適用法についての研究は行われ、リモートオフィスに対するセキュリティ対策の組み立ては、拠点とは別に示されている。<br>・検討は、すべてのリモートオフィスのセキュリティ環境の特性を十分に反映したものとは言い難い<br>・リモートオフィスごとのセキュリティ要求のフレームワークに検討のレベルはクラスB以上<br>・リモートオフィスごとのセキュリティ要求のフレームワークについての見直し状況はクラスB以上<br>・リモートオフィスごとのセキュリティ要求のフレームワークについての文書化のレベルはクラスB以上 |
| レベル2 | リモートオフィスに対するセキュリティ対策の検討は、特に組織的に行われてはいないが、結果として、拠点のセキュリティ対策を、リモートオフィスの環境に適合するような修正が行われている。<br>・リモートオフィスごとのセキュリティ要求のフレームワークに検討のレベルはクラスC以上<br>・リモートオフィスごとのセキュリティ要求のフレームワークについての文書化のレベルはクラスC以上 |
| レベル1 | リモートオフィスを意識したセキュリティ対策の検討は行われていないに等しい。<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | リモートオフィス内のシステムは隙のないセキュアなものとして構築されており、セキュリティ面での構成の的確性の維持管理も徹底している。システムの作りに関してセキュリティ面での不備や不手際が入り込む余地は、まずない。<br>・リモートオフィスにおけるシステムの構成についてセキュリティ面から組織的によく検討された方針が確立している<br>・各リモートオフィスにおけるシステム構成の設計の妥当性や実装の的確性、セキュリティ対策ツールの適切な使用、ならびに各構成機器における脆弱性対策の実施についてのレビューやチェックについての完成度の高い管理の仕組みが確立している<br>・各リモートオフィスにおけるシステム構成の設計の妥当性や実装の的確性、セキュリティ対策ツールの適切な使用、ならびに各構成機器における脆弱性対策の実施について、この管理の仕組みに沿ってレビューやチェックが徹底して行われている<br>・リモートオフィスのシステム環境やセキュリティ環境の変化に対応した、システムのセキュリティ対策についての見直しや、問題が生じた場合の見直しは、適宜、適切に行われ、これらのシステムへの反映のタイムラグは1週間以内<br>・各リモートオフィスに対するこれらについて、専門チームによる指導やチェックが行われている<br>・各リモートオフィスにおけるシステム構成面でのセキュリティ対策は、すべてのリモートオフィスについて詳細についてまで、完全に把握されている<br>・年に数回以上、システム構成の妥当性についての定期的なチェックを実施している<br>・リモートオフィスにおけるシステムにおけるセキュリティ対策と管理状況についての文書化のレベルはクラスA |
| レベル4 | リモートオフィス内のシステムは隙のないセキュアなものとして構築されており、セキュリティ面での構成の的確性の維持管理も組織的な管理下で行われているが、一部に徹底さを欠くところが見られる。システムの作りに関してセキュリティ面での不備が入り込む隙が、僅かではあるが残されている。<br>・リモートオフィスにおけるシステムの構成についてセキュリティ面から組織的によく検討された方針が示されている<br>・各リモートオフィスにおけるシステム構成の設計の妥当性や実装の的確性、セキュリティ対策ツールの適切な使用、ならびに各構成機器における脆弱性対策の実施についてのレビューやチェックについての管理の仕組みが確立しているが、まだ改善の余地もある<br>・各リモートオフィスにおけるシステム構成の設計の妥当性や実装の的確性、セキュリティ対策ツールの適切な使用、ならびに各構成機器における脆弱性対策の実施について、この管理の仕組みに沿って組織的なレビューやチェックが、徹底さにかけるところも見られる<br>・リモートオフィスのシステム環境やセキュリティ環境の変化に対応した、システムのセキュリティ対策についての見直しや、問題が生じた場合の見直しは、適宜、適切に行われているが、これらのシステムへの反映のタイムラグは平均2週間近くを要している<br>・各リモートオフィスに対するこれらについて、専門チームによる指導やチェックが行われている<br>・各リモートオフィスにおけるシステム構成面でのセキュリティ対策は、すべてのリモートオフィスについてほぼ正確に把握されている<br>・年に2回以上、システム構成の妥当性についての定期的なチェックを実施している<br>・リモートオフィスにおけるシステムにおけるセキュリティ対策と管理状況についての文書化のレベルはクラスB以上 |
| レベル3 | リモートオフィス内のシステムに対するセキュリティ対策は、組織的な検討の下で設計されているが、各リモートオフィスにおけるシステムのセキュリティ面での構成の的確性の維持管理については、各リモートオフィスに任されており、専門メンバーによる指導やチェックが行き届くようにはなっていず、システムの作りに関してセキュリティ面での不備が入り込む可能性が、残されている。<br>・大まかではあるが、リモートオフィスにおけるシステムの構成についてセキュリティ面から組織的に検討された方針が示されている<br>・大まかではあるが、各リモートオフィスにおけるシステム構成の設計の妥当性や実装の的確性、セキュリティ対策ツールの適切な使用、ならびに各構成機器における脆弱性対策の実施についてのレビュ |

| | |
|---|---|
| | ーやチェックについての管理の仕組みが示されているが、その実施は各リモートオフィスに中心で行われている<br>・各リモートオフィスにおけるシステム構成の設計の妥当性や実装の的確性、セキュリティ対策ツールの適切な使用、ならびに各構成機器における脆弱性対策の実施について、この管理の仕組みに沿ってレビューやチェックが行われているが、徹底したものではない<br>・リモートオフィスのシステム環境やセキュリティ環境の変化に対応した、システムのセキュリティ対策についての見直しや、問題が生じた場合の見直しは、適宜、適切に行われているが、これらのシステムへの反映のタイムラグは平均 2 週間近くを要している<br>・これらについて専門チームによる指導やチェックは、十分に行われるようにはなっていない<br>・各リモートオフィスにおけるシステム構成面でのセキュリティ対策に把握は、リモートオフィスサイドに任されており、十分に把握されているとは言えない<br>・各リモートオフィスにおけるシステム構成や各機器の実装の妥当性についての定期的なチェックは、年 1 度程度<br>・リモートオフィスにおけるシステムにおけるセキュリティ対策と管理状況についての文書化のレベルはクラス B 以上 |
| レベル 2 | リモートオフィス内のシステムに対するセキュリティ対策は、組織的には基本方針が存在し、セキュリティ対策のモデルは示されているが、その実装や構成の妥当性の維持管理は、各リモートオフィス任せとなっている。専門メンバーによる指導やチェックが組織的に行われるようにはなってなく、それぞれのリモートオフィスのシステムの作りにセキュリティ面での不備が入り込むことも考えられる。<br>・リモートオフィスにおけるシステムの構成についてセキュリティ面から対応方針や構成モデルは示されている<br>・各リモートオフィスにおけるシステム構成の設計の妥当性や実装の的確性、セキュリティ対策ツールの適切な使用、ならびに各構成機器における脆弱性対策の実施についてのレビューやチェックのポイントは示されているが、その実施は各リモートオフィスに任されている<br>・リモートオフィスのシステム環境やセキュリティ環境の変化に対応した、システムのセキュリティ対策についての見直しや、問題が生じた場合の見直しについての指示は、組織的になされているが、その実施は、各リモートオフィスに任されており、特別な場合を除き、管理はほとんど行われていない<br>・各リモートオフィスにおけるシステム構成面でのセキュリティ対策に把握は、リモートオフィスサイドに任されており、あまり把握されていない<br>・各リモートオフィスにおけるシステム構成や各機器の実装の妥当性についての定期的なチェックは、ほとんど行われていない<br>・リモートオフィスにおけるシステムにおけるセキュリティ対策と管理状況についての文書化のレベルはクラス C 以上 |
| レベル 1 | リモートオフィス内のシステムに対するセキュリティ対策についての管理はほとんど行われていない。<br>・レベル 2 の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | リモートオフィス内のシステムのセキュアな運用の実現するための完成度の高いスキームが確立しており、すべてのリモートオフィスにおいて、このスキームに沿ったシステムの運用が確実に行われており、リモートオフィスにおけるシステム運用においてセキュリティ面での不手際が入り込むことは、まず考えられない。<br>・組織的に検討されたリモートオフィスにおけるシステム運用についてのセキュリティ要求が明示されている<br>・各リモートオフィスにおいて、リモートオフィス内のシステム運用についてのセキュリティ要求の実行を確実にするための完成度の高い管理の仕組みが確立している<br>・各リモートオフィスにおけるリモートオフィス内システムの運用についてのセキュリティ要求の実行は、この管理の仕組みに沿って、リモートオフィス内でもまたセンターサイドからも徹底した管理下で行われている<br>・各リモートオフィスにおける、リモートオフィスのシステム環境やセキュリティ環境の変化に伴う、リモートオフィス内システムの運用におけるセキュリティ要求の見直しや、問題が生じた場合の見直しは、適宜、適切に行われ、これらのシステム運用への反映のタイムラグは1週間以内<br>・各リモートオフィスに対するこれらについて、専門チームによる指導やチェックが行われている<br>・各リモートオフィスにおいては、年に数回以上、リモートオフィス内システムの運用についてのセキュリティ面からの妥当性についての定期的なチェックを実施している<br>・各リモートオフィスにおけるリモートオフィス内システムの運用におけるセキュリティ要求やその実践状況についての文書化のレベルはクラスA |
| レベル4 | リモートオフィス内のシステムのセキュアな運用の実現するためのスキームが確立しており、すべてのリモートオフィスにおいて、このスキームに沿ったシステムの運用が行われているが、一部に徹底差を欠くところも見られ、リモートオフィスにおけるシステム運用においてセキュリティ面での不手際が入り込む隙が、僅かではあるが残されている。<br>・組織的に検討されたリモートオフィスにおけるシステム運用についてのセキュリティ要求が明示されている<br>・各リモートオフィスにおいて、リモートオフィス内のシステム運用についてのセキュリティ要求の実行を確実にするための管理の仕組みが確立している<br>・各リモートオフィスにおけるリモートオフィス内システムの運用についてのセキュリティ要求の実行は、この管理の仕組みに沿って、リモートオフィス内でもまたセンターサイドからも管理が行われているが、一部に徹底さをかくところも見られる<br>・各リモートオフィスにおける、リモートオフィスのシステム環境やセキュリティ環境の変化に伴う、リモートオフィス内システムの運用におけるセキュリティ要求の見直しや、問題が生じた場合の見直しは、適宜、行われているが、これらのシステム運用への反映のタイムラグは平均2週間程度<br>・各リモートオフィスに対するこれらについての、専門チームによる指導やチェックも行われることもある<br>・各リモートオフィスにおいては、年に2回以上、リモートオフィス内システムの運用についてのセキュリティ面からの妥当性についての定期的なチェックを実施している<br>・各リモートオフィスにおけるリモートオフィス内システムの運用におけるセキュリティ要求やその実践状況についての文書化のレベルはクラスB以上 |
| レベル3 | リモートオフィス内のシステムのセキュアな運用の実現するため要求事項や管理上のチェックポイントは示されているが、その実施は各リモートオフィスに任されており、すべてのリモートオフィスにおいて、セキュなシステム運用が実現できているかどうかは全体として十分な管理は行われていない。概ね、適切に行われていると見ることができるが、リモートオフィスにおけるシステム運用においてセキュリティ面での不手際が入り込む隙が残されている。<br>・組織的に検討されたリモートオフィスにおけるシステム運用についてのセキュリティ要求は示されている<br>・各リモートオフィスにおいて、リモートオフィス内のシステム運用についてのセキュリティ要求の実行を確実にするためのチェックポイントは示されている |

| | |
|---|---|
| | ・各リモートオフィスにおける、これらの要求についての理解やその実践に必要なスキルは必ずしも十分とは言えない<br>・各リモートオフィスにおけるリモートオフィス内システムの運用についてのセキュリティ要求の実行についのて管理は、一応は行われてはいるが、徹底したものではない<br>・各リモートオフィスにおける、リモートオフィスのシステム環境やセキュリティ環境の変化に伴う、リモートオフィス内システムの運用におけるセキュリティ要求の見直しや、問題が生じた場合の見直しは、適宜、行われているが、これらのシステム運用への反映のタイムラグは平均１ヶ月近い<br>・各リモートオフィスにおいては、年に１回は、リモートオフィス内システムの運用についてのセキュリティ面からの妥当性についての定期的なチェックを実施している<br>・各リモートオフィスにおけるリモートオフィス内システムの運用におけるセキュリティ要求やその実践状況についての文書化のレベルはクラスＢ以上 |
| レベル2 | リモートオフィス内のシステムのセキュアな運用の実現するため要求事項や管理上のチェックポイントは大まかなものが示されている程度で、その実施はすべて各リモートオフィスに任されており、すべてのリモートオフィスにおいて、セキュなシステム運用が実現できているかどうかは全体としての管理はほとんど行われていない。リモートオフィスにおけるシステム運用においてセキュリティ面での不手際が入り込む可能性は低くはない。<br>・担当チームレベル検討されたリモートオフィスにおけるシステム運用についてのセキュリティ要求は示されている<br>・各リモートオフィスにおいて、リモートオフィス内のシステム運用についてのセキュリティ要求の実行を確実にするためのチェックポイントは大まかではあるが示されている<br>・各リモートオフィスにおけるリモートオフィス内システムの運用についてのセキュリティ要求の実行についのて管理は、あまり行われてはいない<br>・各リモートオフィスにおける、リモートオフィスのシステム環境やセキュリティ環境の変化に伴う、リモートオフィス内システムの運用におけるセキュリティ要求の見直しや、問題が生じた場合の見直しは、適宜、行われているが、遅れがちで、これらのシステム運用への反映のタイムラグは平均１ヶ月以上<br>・各リモートオフィスにおけるリモートオフィス内システムの運用におけるセキュリティ要求やその実践状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | リモートオフィス内システムのセキュアな運用の実現に対する取組みは、ないに等しい。<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | リモートオフィスでの業務の運営や組織の管理におけるセキュリティ事故を防止するための完成度の高いスキームが確立しており、すべてのリモートオフィスにおいて、このスキームに沿った業務の運営が確実に行われており、リモートオフィスでの業務運営においてセキュリティ事故が起こることは、まず考えられない。<br>・組織的によく検討されたリモートオフィスにおける業務運営や組織の管理についんのセキュリティ要求が明示されている<br>・各リモートオフィスにおいて、業務の運営においてセキュリティ事故を防止するための完成度の高い管理の仕組みが確立している<br>・各リモートオフィスにおける業務の運営や組織の管理に関するセキュリティ要求の実行は、この管理の仕組みに沿って、徹底した管理下で行われている<br>・各リモートオフィスにおける、リモートオフィスの運営環境やセキュリティ環境の変化に伴う、リモートオフィスでの業務の運営や組織の管理についてのセキュリティ要求の見直しや、問題が生じた場合の見直しは、適宜、適切に行われ、これらの業務の運営や組織の管理への反映のタイムラグは1週間以内 |

| | |
|---|---|
| | ・各リモートオフィスに対するこれらについて、専門チームによる指導やチェックが行われている<br>・各リモートオフィスにおいては、年に数回以上、業務の運営や組織の管理についてのセキュリティ面からの妥当性についての定期的なチェックを実施している<br>・各リモートオフィスにおける業務の運営や組織の管理に対するセキュリティ要求やその実践状況についての文書化のレベルはクラス A |
| レベル 4 | リモートオフィスでの業務の運営や組織の管理におけるセキュリティ事故を防止するためのスキームが確立しており、すべてのリモートオフィスにおいて、このスキームに沿った業務の運営が追求されているが、一部に徹底さを欠くところも見られる。概ね、十分な対策が行われていると見ることができるが、リモートオフィスでの業務運営においてセキュリティ事故が起こる隙が、僅かではあるが残されている。<br>・組織的に検討されたリモートオフィスの業務運営や組織の管理についてのセキュリティ要求が明示されている<br>・各リモートオフィスにおいて、業務の運営や組織の管理においてセキュリティ事故を防止するための管理の仕組みが確立しているが、まだ改善の余地もある<br>・各リモートオフィスにおける業務の運営や組織の管理に関するセキュリティ要求の実行は、この仕組みに沿って実行、管理が行われているが、一部に徹底さを欠くところも見られる<br>・各リモートオフィスにおける、リモートオフィスの運営環境やセキュリティ環境の変化に伴う、リモートオフィスでの業務の運営や組織の管理についてのセキュリティ要求の見直しや、問題が生じた場合の見直しは、適宜、適切に行われ、これらの業務の運営や組織の管理への反映のタイムラグは平均 2 週間程度<br>・各リモートオフィスに対するこれらについての、専門チームによる指導やチェックも行われることもある<br>・各リモートオフィスにおいては、年に 2 回は、業務の運営や組織の管理についてのセキュリティ面からの妥当性についての定期的なチェックを実施している<br>・各リモートオフィスにおける業務の運営や組織の管理に対するセキュリティ要求やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル 3 | リモートオフィスでの業務の運営や組織の管理においてセキュリティ事故を防止するために必要な施策は示されているが、その実践は各リモートオフィスに任されている。各リモートオフィスにおいては、必要な施策の実践に努めてはいるが、管理は徹底したものとは言い難く、リモートオフィスにおける業務の運用や組織の管理においてセキュリティ事故が発生する余地が残されている。<br>・組織的に検討されたリモートオフィスにおける業務の運営や組織に管理についてのセキュリティ面からの要求は示されている<br>・各リモートオフィスにおいて、リモートオフィスにおける業務の運営や組織に管理についてのセキュリティ事故事故を防止するために実施すべき事項、ならびにその管理上のチェックポイントは示されている<br>・各リモートオフィスにおいては、これらの要求についての理解は概ね十分である<br>・各リモートオフィスにおいて、業務の運営や組織の管理についての必要な施策の実行についのて管理は、一応は行われてはいるが、徹底したものではない<br>・各リモートオフィスにおける、実施している業務の運営や組織の管理についてのセキュリティ事故防止策に対する、業務の運営環境やセキュリティ環境の変化に伴う見直しや、問題が生じた場合の見直しは、適宜、行われているが、これらのシステム運用への反映のタイムラグは平均 1 ヶ月近い<br>・各リモートオフィスにおいては、年に 1 回は、業務の運営や組織の管理についてのセキュリティ事故防止策の妥当性についての定期的なチェックを実施している<br>・各リモートオフィスにおける業務の運営や組織の管理についてのセキュリティ事故防止策やその実践状況についての文書化のレベルはクラス B 以上 |
| レベル 2 | リモートオフィスでの業務の運営や組織の管理におけるセキュリティ事故の防止のための要求事項や管理上のチェックポイントは大まかなものが示されている程度で、実施すべき施策の検討やその実践は、すべて各リモートオフィスに任されており、すべてのリモートオフィスにおいて、業務の運営や組織の管理についてのセキュリティ対策が適切に行われているかどうかは全体としての管理はほとんど行われていない。リモートオフィスでの業務の運営や組織の管理で、セキュリティ事故が発生する可能性は、低くはない。<br>・リモートオフィスでの業務の運営や組織の管理におけるセキュリティ事故防止のために必要となる施策は、大まかではあるが示されている<br>・各リモートオフィスにおいて、リモートオフィス内のシステム運用についてのセキュリティ要求の実行を確実にするためのチェックポイントは大まかではあるが示されている<br>・各リモートオフィスにおいて、業務の運営や組織の管理についての必要な施策の実行は、業務現場に要求されてはいるが、その実施についんての管理はあまり行われてはいない<br>・各リモートオフィスにおける、実施している業務の運営や組織の管理についてのセキュリティ事故防止 |

| | |
|---|---|
| | 策に対する、業務の運営環境やセキュリティ環境の変化に伴う見直しや、問題が生じた場合の見直しは、行われてはいるが、十分には程遠い<br>・各リモートオフィスにおける業務の運営や組織の管理についてのセキュリティ事故防止策やその実践状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | リモートオフィスにおける業務の運営や組織の管理におけるセキュリティ事故の防止についての取組みは、ないに等しい。<br>・レベル2の達成要件も満たしていない |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 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は、ほぼ完全に実施されており、リモートオフィスのシステムや設備は、環境的、物理的な要因に対する堅牢性は、十分に高い。<br>・リモートオフィスの施設や設備や空間に対するきめの細かいリスク分析にもとづく、リモートオフィスごとのこれらについてのきめの細かい保護策が決められている<br>・各リモートオフィスにおいて、その施設や設備や空間について必要とされる保護策の確実な実施を実現するための完成度の高い管理の仕組みが確立している<br>・各リモートオフィスにおけるシステムや設備や空間に対する必要な保護策の実施は、この管理の仕組みに沿って、徹底した管理下で行われている<br>・各リモートオフィスにおける、施設や設備あるいは空間に対するセキュリティ要求のオフィスの運営環境の変化に伴う見直しや、問題が生じた場合の見直しは、適宜、適切に行われ、これらの施設や設備および空間に対する保護策への反映のタイムラグは１ヶ月以内<br>・各リモートオフィスに対するこれらについて、専門チームによる指導やチェックが行われている<br>・各リモートオフィスにおいては、年に数回以上、施設や設備や空間に対する必要な保護策の妥当性についての定期的なチェックを実施している<br>・各リモートオフィスにおける施設や設備や空間に対する必要な保護策やその実践状況についての文書化のレベルはクラスＡ |
| レベル4 | 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は、概ね十分に実施されており、リモートオフィスのシステムや設備は、環境的、物理的な要因に対する堅牢性は、相当に高いが、すべてに十分と言うわけではなく、問題が発生する余地はある。<br>・リモートオフィスの施設や設備や空間に対するリスク分析にもとづく、リモートオフィスごとのこれらについて相当にきめの細かい保護策が決められている<br>・各リモートオフィスにおいて、その施設や設備や空間について必要とされる保護策の確実な実施を実現するための管理の仕組みも作られているが、まだ改善の余地もある<br>・各リモートオフィスにおけるシステムや設備や空間に対する必要な保護策の実施は、この管理の仕組みに沿って実行、管理されているが、一部に徹底さを欠くところも見られる<br>・各リモートオフィスにおける、施設や設備あるいは空間に対するセキュリティ要求のオフィスの運営環境の変化に伴う見直しや、問題が生じた場合の見直しは、適宜、適切に行われているが、これらの施設や設備および空間に対する保護策への反映のタイムラグは２ヶ月近い<br>・各リモートオフィスに対し、これらの点について、専門チームによる指導やチェックがある程度行われている<br>・各リモートオフィスにおいては、年に2回以上、施設や設備や空間に対する必要な保護策の妥当性についての定期的なチェックを実施している<br>・各リモートオフィスにおける施設や設備や空間に対する必要な保護策やその実践状況についての文書化のレベルはクラスＢ以上 |

| | |
|---|---|
| レベル3 | 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についてのポイントと、対策のモデルは示されているが、各ﾘモートオフィスのシステムや設備や施設や空間に対する保護策の策定と実施は、各ﾘモートオフィスに任されている。各ﾘモートオフィスでは、必要最低限の対策は実施されていると見ることができる。<br>・ﾘモートオフィスの施設や設備や空間に対する必要最小限の要求は示されている<br>・大まかではあるが、各ﾘモートオフィスにおいて、その施設や設備や空間について必要とされる保護策の確実な実施についてのチェックポイントは示されている<br>・各ﾘモートオフィスは、それぞれにこの要求の実現に取組んでおり、設備や施設に対する必要最小限の対策はとっているが、空間の保護については徹底さに欠くところが少なくない<br>・各ﾘモートオフィスにおける、それぞれに施設や設備あるいは空間に対するセキュﾘﾃｨ要求のオフィスの運営環境の変化に伴う見直しや、問題が生じた場合の見直しも、行われているが、これらの施設や設備および空間に対する保護策への反映の迅速とは言い難い<br>・各ﾘモートオフィスに対し、これらの点について、専門チームによる指導やチェックもある程度行われている<br>・各ﾘモートオフィスにおいては、年に1回以上、施設や設備や空間に対する必要な保護策の妥当性についての定期的なチェックを実施している<br>・各ﾘモートオフィスにおける施設や設備や空間に対する必要な保護策やその実践状況についての文書化のレベルはクラスＢ以上 |
| レベル2 | 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はある程度、実施されているが十分なものとは、程遠く、その堅牢性は、そう高くない。<br>・各ﾘモートオフィスにおいては、施設や設備や空間の保護についての大まかな認識は存在<br>・これらの要求は、平均的なものよりは低いが、システムの可用性や攻撃に対する堅牢性の要求に関連して、施設や特に重要視する設備や空間についての最低限の要求は示されている<br>・各ﾘモートオフィスにおいては、これらの要求への対策は実施しているが、空間の管理については、徹底しているとは言えない<br>・各ﾘモートオフィスにおけるシステムや設備や空間に対する保護策についての、セキュﾘﾃｨ環境の変化に伴う見直しや、問題が生じた場合の見直しも、十分ではないが行われている<br>・各ﾘモートオフィスにおける施設や設備や空間に対する必要な保護策やその実践状況についての文書化のレベルはクラスＣ以上 |
| レベル1 | ﾘモートオフィスの施設や設備や空間の保護についての取組みは、ないに等しい。<br>・レベル2の達成要件も満たしていない |

### 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 |
|---|---|

| 強度<br>レベル | 当該レベル達成要件 |
|---|---|
| レベル<br>5 | 閉鎖型の保護領域に対する保護は、現時点では最も堅牢と考えられる設備が整えられ、厳格な保護ルールの運用も徹底していて、この領域の保護に問題が生じることは、まず考えられない<br>･保護領域に対する物理的な保護は、現時点では最も堅牢と考えられるレベル<br>･すべての閉鎖型の保護領域について、保護要件、および、保護要領が明確に定められている<br>･すべての閉鎖型の保護領域について厳格な保護要件と保護要領が確立している<br>･保護領域内へ入室（または搬入出）できる権限を有する者の管理は徹底して行われている<br>･保護領域への立ち入りや物品の半有や搬出は、厳格な保護要領に沿って、組織的な管理の下で厳格に管理されている<br>･権限を有しない者が、保護領域内に立ち入ることが事実上不可能<br>･権限を有しない者が、保護領域内に物品等を搬入･搬出することが事実上不可能<br>･すべての人の入退室、物品等の搬入出について記録が取得されている<br>･すべての入退室記録、搬入出記録について、不整合がないことを定期的にチェックしている<br>･保護領域内外における不正行為の実施を、事前に牽制するに足る十分な措置が講じられている<br>･保護領域内外における不正行為が発覚した場合の対処について明確に定められている<br>･閉鎖型の保護領域に対する保護の方式や保護のルールについての検討のレベルはクラス A<br>･これらについての見直しのレベルは A<br>･閉鎖型の保護領域の保護策やその実践についての記録の文書化のレベルはクラス A |
| レベル<br>4 | 閉鎖型の保護領域に対する保護は、現時点では相当に堅牢と考えられる設備が整えられ、厳格な保護ルールの運用も設けられているが、運用の一部に徹底さ欠くところも見られ、この領域の保護に問題が生じる隙が、僅かではあるが残されている。<br>･保護領域に対する物理的な保護は、現時点では平均以上で相当に堅牢と考えられるレベル<br>･すべての閉鎖型の保護領域について、保護要件、および、保護要領が明確に定められている<br>･すべての閉鎖型の保護領域について、相当に厳格な保護要件と保護要領が確立しているが、レベル 5 ほどの厳格さはない<br>･保護領域内へ入室（または搬入出）できる権限を有する者の管理は相当に厳格に行われているが、一部に徹底さを欠くところも見られる<br>･保護領域への立ち入りや物品の半有や搬出は、厳格な保護要領に沿って、組織的な管理の下で相当に厳格に行われているが、一部に徹底さを欠くところも見られる<br>･権限を有しない者が、保護領域内に立ち入ることは、まず不可能<br>･権限を有しない者が、保護領域内に物品等を搬入･搬出することは、まず不可能<br>･すべての人の入退室、物品等の搬入出について記録が取得されているが、一部に徹底さを欠くところも見られる<br>･すべての入退室記録、搬入出記録について、不整合がないことを定期的にチェックしているが、一部に徹底さを欠くところも見られる<br>･保護領域内外における不正行為の実施を、事前に牽制するに足る措置が講じられているが、まだ改善の余地はある<br>･保護領域内外における不正行為が発覚した場合の対処が示されているが、、まだ改善の余地はある<br>･閉鎖型の保護領域に対する保護の方式や保護のルールについての検討のレベルはクラス B 以上<br>･これらについての見直しのレベルは B 以上<br>･閉鎖型の保護領域の保護策やその実践についての記録の文書化のレベルはクラス B 以上 |
| レベル<br>3 | 閉鎖型の保護領域に対する保護は、比較的堅牢と考えられる設備が整えられいる。保護ルールも比較的厳格で、その運用も組織的に管理されているが、徹底さ欠くところも見られ、この領域の保護に問題が生じる隙が残されている。<br>･保護領域に対する物理的な保護は、現時点では比較的堅牢と考えられるレベル<br>･すべての閉鎖型の保護領域について、大まかではあるが、保護要件、および、保護要領が明確に定められている<br>･すべての閉鎖型の保護領域について、保護要件と保護要領が示されているが、大まかなものであり、 |

| | |
|---|---|
| | その厳格さも平均レベル<br>・保護領域内へ入室（または搬入出）できる権限を有する者の管理は、組織的に行われているが、徹底したものではない<br>・保護領域への立ち入りや物品の半有や搬出は、保護要領に沿って、組織的な管理の下で行われているが、徹底したものでははない<br>・権限を有しない者が、保護領域内に立ち入ることは、比較的困難<br>・権限を有しない者が、保護領域内に物品等を搬入・搬出することは、比較的困難<br>・保護領域内外における不正行為の実施を、事前に牽制するに足る措置が講じられているが、形式的な域を出ない<br>・大まかではあるが、保護領域内外における不正行為が発覚した場合の対処が示されている<br>・閉鎖型の保護領域に対する保護の方式や保護のルールについての検討のレベルはクラスＢ以上<br>・これらについての見直しのレベルはＢ以上<br>・閉鎖型の保護領域の保護策やその実践についての記録の文書化のレベルはクラスＢ以上 |
| レベル2 | 閉鎖型の保護領域に対する保護は、平均的な設備によっている。保護ルールも作られているが厳格とは言い難い。またその運用も厳格とは厳格には程遠い。<br>・保護領域に対する物理的な保護は、通常の設備を利用するか、平均的なものを用いており、特に堅牢は言えない<br>・すべての閉鎖型の保護領域について、大まかな保護要件が示されているが、保護要領は明確にされていない<br>・保護領域内へ入室（または搬入出）できる権限を有する者の管理も形式的であるが行われている<br>・保護領域内に立ち入りはチェックされることになっているが、実行は形式的なレベル<br>・閉鎖型の保護領域に対する保護の方式や保護のルールについての検討のレベルはクラスＣ以上<br>・これらについての見直しのレベルはＣ以上<br>・閉鎖型の保護領域の保護策やその実践についての記録の文書化のレベルはクラスＣ以上 |
| レベル1 | 保護領域の境界も不明確であり、対策も実施していない。 |

## Td3.2 半閉鎖型の保護領域における必要な保護の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 半閉鎖型の保護領域に対しても、できうる限りの保護策がとられており、有効に機能している。<br>・対象の半閉鎖型の閉鎖系の保護領域について、相当に厳格な保護要件、および保護要領が示されている<br>・この領域についての入退室や物品の搬入や搬出は、このルールに沿って、相当に厳格にチェックされている<br>・半閉鎖型の保護領域内へ入室（または搬入出）できる権限を有する者が、明確にされている<br>・権限を有しない者が、半閉鎖型の保護領域内に立ち入ることが事実上不可能<br>・権限を有しない者が、半閉鎖型の保護領域内に物品等を搬入・搬出することが事実上不可能<br>・すべての人の半閉鎖型の保護領域内への入退室、物品等の搬入出について記録が取得されている<br>・すべての半閉鎖型の保護領域内への入退室記録、搬入出記録について、不整合がないことを定期的にチェックしている<br>・半閉鎖型・開放型の保護領域内における不正行為の実施を、事前に牽制するに足る十分な措置が講じられている<br>・半閉鎖型・開放型の保護領域内外における不正行為が発覚した場合の対処について明確に定められている<br>・この領域の保護策についての検討レベルはクラスＡ<br>・この領域の保護策についての見直しのレベルはＡ |

| | |
|---|---|
| | ･この領域の保護策や保護策の実践の記録についての文書化のレベルは A |
| レベル 4 | 半閉鎖型の保護領域に対しても、相当に厳格な保護策がとられており有効に機能しているが、レベル 5 ほど厳格なものではない。<br>･対象の半閉鎖型の閉鎖系の保護領域について、平均以上に厳格な保護要件、および保護要領が示されている<br>･この領域についての入退室は、このルールに沿って、相当に厳格にチェックされているが、一部に徹底さを欠くところも見られる<br>･半閉鎖型の保護領域内へ入室（または搬入出）できる権限を有する者が、明確にされている<br>･権限を有しない者が、半閉鎖型の保護領域内に立ち入ることは、まず不可能。<br>･権限を有しない者が、半閉鎖型の保護領域内に物品等を搬入･搬出することは、まず不可能<br>･すべての人の入退室、物品等の搬入出について記録が取得されている<br>･半閉鎖型･開放型の閉鎖系の保護領域内における不正行為の実施を、事前に牽制する何らかの措置が講じられている<br>･この領域の保護策についての検討レベルはクラス B 以上<br>･この領域の保護策についての見直しのレベルは B 以上<br>･この領域の保護策や保護策の実践の記録についての文書化のレベルは B 以上 |
| レベル 3 | 半閉鎖型の保護領域に対しても、工夫した保護策がとられており、ある程度有効に機能しているが、厳格なものではない。<br>･対象の半閉鎖系の保護領域について、大まかではあるが保護ルールが示されれいる<br>･半閉鎖型の保護領域内へ入室できる権限を有する者が、明確にされている<br>･権限を有しない者が、半閉鎖型の保護領域内に立ち入ることが比較的困難である<br>･権限を有しない者が、半閉鎖型の保護領域内に物品等を搬入･搬出することが比較的困難である<br>･この領域の保護策についての検討レベルはクラス B 以上<br>･この領域の保護策についての見直しのレベルは B 以上<br>･この領域の保護策や保護策の実践の記録についての文書化のレベルは B 以上 |
| レベル 2 | 実効性は低いが、半閉鎖型の保護領域に対する保護策が示されており、形式的なレベルにせよ、一定の管理は行われている。<br>･保護領域を保護するための物理的な対策は脆弱であるが、保護領域の境界が明確にされている<br>･大まかで厳格でなものではないが、保護ルールが示されている<br>･形式的に近いが入退室のチェックは行われることになっているが実行は形式的なレベル<br>･この領域の保護策についての検討レベルはクラス B 以上<br>･この領域の保護策についての見直しのレベルは B 以上<br>･この領域の保護策や保護策の実践の記録についての文書化のレベルは B 以上 |
| レベル 1 | 保護領域の境界も不明確であり、対策も実施していない。 |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | 社内外に設置する装置や設備に対して、できうる限りの保護策がとられており、有効に機能している。<br>･社内外に設置する全ての装置や関連設備に対して、保護要件及び保護要領が明確に定められている<br>･装置や関連設備の設置に際して、火災･地震･水害等のあらゆるリスクを想定し、設置環境面での配慮が完全になされている<br>･装置や関連設備の配置･据付にあたって、あらゆるリスクを想定し、これ以上ないレベルの配慮がなされている。特に重要な装置や関連設備については、堅牢性を確保するための補強策が網羅的に施されている |

| | |
|---|---|
| | ･保護対象とする全ての装置や関連設備に対して点検･保守が定期的にされており、記録が取得されている。<br>･移動対象となる装置を明確にしており、それら全てに対して移動要領を定め、要領に沿った移動を確実に実施している<br>･社内外に設置する装置や設備に対する保護策についての検討レベルはクラスA<br>･社内外に設置する装置や設備に対する保護策についての見直しのレベルはクラスA<br>･社内外に設置する装置や設備に対する保護策や保護策の実施の記録についての文書化のレベルはA |
| レベル4 | 社内外に設置する装置や設備に対して、相当に工夫された保護策がとられており有効に機能しているが、レベル5ほど徹底したものではない。<br>･社内外に設置する全ての装置や関連設備に対して、保護要件及び保護要領が明確に定められている<br>･装置や関連設備の設置に際して、火災･地震･水害等のあらゆるリスクを想定し、設置環境面での配慮が、完全とはいわないまでもほぼ網羅的になされている<br>･装置や関連設備の配置･据付にあたって、リスクに応じた十分な配慮がなされている。特に重要な装置や関連設備については、堅牢性を確保するための補強策が実施されている<br>･保護対象とする全ての装置や関連設備に対して、点検･保守が定期的にされている<br>･移動対象となる装置を明確にしており、それら全てに対して移動要領を定め、要領に沿った移動を実施している<br>･社内外に設置する装置や設備に対する保護策についての検討レベルはクラスB以上<br>･社内外に設置する装置や設備に対する保護策についての見直しのレベルはクラスB以上<br>･社内外に設置する装置や設備に対する保護策や保護策の実施の記録についての文書化のレベルはB以上 |
| レベル3 | 社内外に設置する装置や設備に対して、平均的な保護策がとられており、機能している。<br>･社内外に設置する装置や関連設備のうち特に重要なものに対しては、保護要件及び保護要領が定められている<br>･災害等のリスクのうち特に重要なものに対しては、設置環境面での対策が配慮されている<br>･特に重要な装置や関連設備の配置･据付にあたっては、リスクに応じた配慮がなされている（堅牢性を確保するための補強策を含む）<br>･重要な装置や関連設備に対してのみ、点検･保守が定期的にされている<br>･重要な装置に対してのみ、移動要領が定められており、要領に沿った移動を実施している<br>･重要な装置や関連設備については、リスクに応じた保護策が実質的には機能している<br>･社内外に設置する装置や設備に対する保護策についての検討レベルはクラスB以上<br>･社内外に設置する装置や設備に対する保護策についての見直しのレベルはクラスB以上<br>･社内外に設置する装置や設備に対する保護策や保護策の実施の記録についての文書化のレベルはB以上 |
| レベル2 | 社内外に設置する装置や設備に対する保護策は必要最小限のレベル<br>･保護対象とする装置や関連設備が不明確であるが、重要な装置･設備については、不十分ながらも保護策が講じられている<br>･社内外に設置する装置や設備に対する保護策についての検討レベルはクラスB以上<br>･社内外に設置する装置や設備に対する保護策についての見直しのレベルはクラスB以上<br>･社内外に設置する装置や設備に対する保護策や保護策の実施の記録についての文書化のレベルはB以上 |
| レベル1 | 保護対象とする装置や関連設備が不明確であり、保護策も講じていない。 |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 業務遂行中に、システムの動きや業務の処理結果に異常を見つけた場合、発見者が取るべき措置が確立しており、その関係者への周知も十分で、すべての関わる関係者が、このような場面に対する対応能力を十分に有していることが確認されている。<br>・発生セキュリティ事故の状況ごとに必要な措置および対応要領が確立している<br>・これらは業務マニュアルへの記載や、教育等で、関係者セキュリティ事故の対応にかかわる者に周知されている<br>・関係者に対する障害時の対応についての教育や訓練も行き届いており、必要な対応が何時でも迅速に取れる<br>・異常を発見した時に発見者が取るべき措置とその展開についての検討のレベルはクラスA<br>・異常を発見した時に発見者が取るべき措置とその展開についての見直し状況はクラスA<br>・異常を発見した時に発見者が取るべき措置とその展開についての文書化のレベルはクラスA |
| レベル4 | 業務遂行中に、システムの動きや業務の処理結果に異常を見つけた場合、発見者が取るべき措置が示されており、その関係者への周知も行われており、すべての関係者が、このような場面に対する対応能力は、ほぼ十分と見てよいが、まだ改善の余地がある。<br>・発生セキュリティ事故の状況ごとに必要な措置および対応要領が示されているが、まだ改善の余地がある<br>・これらは業務マニュアルへの記載や、教育等で、セキュリティ事故の対応にかかわる者への周知が図られているが、一部に徹底鎖を欠くところが見られる<br>・関係者に対する障害時の対応についての教育や訓練も、概ね行き届いており、必要な対応が何時でも迅速に取れると見られているが、一部に徹底鎖を欠くところが見られる<br>・異常を発見した時に発見者が取るべき措置とその展開についての検討のレベルはクラスB以上<br>・異常を発見した時に発見者が取るべき措置とその展開についての見直し状況はクラスB以上<br>・異常を発見した時に発見者が取るべき措置とその展開についての文書化のレベルはクラスB以上 |
| レベル3 | 業務遂行中に、システムの動きや業務の処理結果に異常を見つけた場合、発見者が取るべき措置が示されており、ほとんどの関係者は、このような場面に対する基本的な対応はできると見ることができる。ただし、指定されている措置の内容や、その関係者への展開も十分とは言えず、改善の余地は多い。<br>・セキュリティ事故発生時に必要となる措置および対応要領が示されているが大まかで、発生事故の状況ごとの細かい展開は不十分<br>・これらは、何らかの形でセキュリティ事故への対応にかかわる者に示されているが、訓練は十分とは言えず、必要な対応が何時でも迅速に取れるかどうかは疑わしいところがある<br>・異常を発見した時に発見者が取るべき措置とその展開についての検討のレベルはクラスB以上<br>・異常を発見した時に発見者が取るべき措置とその展開についての見直し状況はクラスB以上<br>・異常を発見した時に発見者が取るべき措置とその展開についての文書化のレベルはクラスB以上 |
| レベル2 | 業務遂行中に、システムの動きや業務の処理結果に異常を見つけた場合、発見者が取るべき措置は示されてはいるが、内容も基本的なところに止まっており、対応にかかわる者への周知も不十分で、万一の場合の対応が適切にできるかどうかは怪しい。<br>・関係者は大まかなものであるが、異常を発見した時に発見者が取るべき基本的な対応を承知している<br>・異常を発見した時に発見者が取るべき措置とその展開についての検討のレベルはクラスC以上<br>・異常を発見した時に発見者が取るべき措置とその展開についての文書化のレベルはクラスC以上 |
| レベル1 | 業務遂行中に、システムの動きや業務の処理結果に異常を見つけた場合、発見者が取るべき措置についての検討は、実質的に行われていない。 |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | セキュリティ事故発生時においてシステム周りで必要となる措置が確立しており、その関係者への周知も十分で、この事故に対するシステム周りでの対応に関わる関係者が、このような場面に対する対応能力を十分に有していることが確認されている。<br>・発生セキュリティ事故の状況ごとに必要な措置および対応要領が確立している<br>・これらはシステム運用マニュアル等で、セキュリティ事故の対応にかかわる者に周知されている<br>・関係者に対する障害時の対応についての教育や訓練も行き届いており、必要な対応が何時でも迅速に取れる<br>・システム周りでのセキュリティ事故発生時の備えについての検討のレベルはクラスA<br>・システム周りでのセキュリティ事故発生時の備えについての見直し状況はクラスA<br>・システム周りでのセキュリティ事故発生時の備えについての文書化のレベルはクラスA |
| レベル4 | セキュリティ事故発生時においてシステム周りで必要となる措置が確立しており、その関係者への周知も行われており、セキュリティ事故に対するシステム周りでの対応に関わる関係者の対応能力は、ほぼ十分と思われるが、改善の余地がある。<br>・発生セキュリティ事故の状況ごとに必要な措置および対応要領が確立している<br>・これらはシステム運用マニュアル等で、セキュリティ事故の対応にかかわる者に周知されている<br>・関係者に対する障害時の対応についての教育や訓練も行き届いており、必要な対応が何時でも迅速に取れる<br>・システム周りでのセキュリティ事故発生時の備えについての検討のレベルはクラスB以上<br>・システム周りでのセキュリティ事故発生時の備えについての見直し状況はクラスB以上<br>・システム周りでのセキュリティ事故発生時の備えについての文書化のレベルはクラスB以上 |
| レベル3 | セキュリティ事故発生時においてシステム周りで必要となる措置は、大まかではあるが関係者へ示されこのような場面に対し、基本的な対応はできると見ることができる。ただし、指定されている措置の内容や、その関係者への展開も十分とは言えず、改善の余地は多い。<br>・セキュリティ事故発生時に必要となる措置および対応要領が示されているがおおまかで、発生事故の状況ごとの細かい展開は不十分<br>・これらは、何らかの形でセキュリティ事故への対応にかかわる者に示されているが、訓練は不十分で、必要な対応が何時でも迅速に取れるかどうかは疑わしいところがある<br>・システム周りでのセキュリティ事故発生時の備えについての検討のレベルはクラスB以上<br>・システム周りでのセキュリティ事故発生時の備えについての見直し状況はクラスB以上<br>・システム周りでのセキュリティ事故発生時の備えについての文書化のレベルはクラスB以上 |
| レベル2 | セキュリティ事故発生した時にシステム周りで必要な措置は示されてはいるが、内容も基本的なところに止まっており、対応にかかわる者への周知も不十分で、万一の場合の対応が適切にできるかどうかは怪しい。<br>・関係者は大まかなものであるが、システム周りでのセキュリティ事故発生時に取るべき基本的な対応を承知している<br>・システム周りでのセキュリティ事故発生時の備えについての検討のレベルはクラスC以上<br>・システム周りでのセキュリティ事故発生時の備えについての文書化のレベルはクラスC以上 |
| レベル1 | 問題が生じた時の備えはないに等しい。 |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | セキュリティ事故発生時において業務サイドで必要となる措置が確立しており、その関係者への周知も十分で、この事故に対す業務サイドでの対応に関わる関係者が、このような場面に対する対応能力を十分に有していることが確認されている。<br>・発生セキュリティ事故の状況ごとに必要な措置および対応要領が確立している<br>・これらは業務マニュアル等で、業務面での後処理等のセキュリティ事故への対応にかかわる者に周知されている<br>・関係者に対するセキュリティ事故発生時の対応についての教育や訓練も行き届いており、必要な対応が何時でも迅速に取れる<br>・業務サイドでのセキュリティ事故発生時の備えについての検討のレベルはクラスA<br>・業務サイドでのセキュリティ事故発生時の備えについての見直し状況はクラスA<br>・業務サイドでのセキュリティ事故発生時の備えについての文書化のレベルはクラスA |
| レベル4 | セキュリティ事故発生時において業務サイドで必要となる措置が確立しており、その関係者への周知も行われており、セキュリティ事故に対する業務サイドでの対応に関わる関係者の対応能力は、ほぼ十分と思われるが、強化の必要性もある。<br>・発生セキュリティ事故の状況ごとに必要な措置および対応要領が確立している<br>・これらは業務マニュアル等で、業務面での後処理等セキュリティ事故の対応にかかわる者に周知されている<br>・関係者に対するセキュリティ事故発生時の対応についての教育や訓練も行き届いており、必要な対応が何時でも迅速に取れる<br>・業務サイドでのセキュリティ事故発生時の備えについての検討のレベルはクラスB以上<br>・業務サイドでのセキュリティ事故発生時の備えについての見直し状況はクラスB以上<br>・業務サイドでのセキュリティ事故発生時の備えについての文書化のレベルはクラスB以上 |
| レベル3 | セキュリティ事故発生時において業務サイドで必要となる措置は、大まかではあるが関係者へ示されこのような場面に対し、基本的な対応はできると見ることができる。ただし、指定されている措置の内容や、その関係者への展開も十分とは言えず、改善の余地は多い。<br>・セキュリティ事故の発生時に必要となる措置および対応要領が示されているがおおまかで、発生セキュリティ事故の状況ごとの細かい展開は不十分<br>・これらは、何らかの形により業務面でセキュリティ事故への対応にかかわる者に示されているが、訓練は不十分で、必要な対応が何時でも迅速に取れるかどうかは疑わしいところがある<br>・業務サイドでのセキュリティ事故発生時の備えについての検討のレベルはクラスB以上<br>・業務サイドでのセキュリティ事故発生時の備えについての見直し状況はクラスB以上<br>・業務サイドでのセキュリティ事故発生時の備えについての文書化のレベルはクラスB以上 |
| レベル2 | セキュリティ事故発生した時に業務サイドで必要となる措置は示されてはいるが、内容も基本的なところに止まっており、対応にかかわる者への周知も不十分で、万一の場合の対応が適切にできるかどうかは怪しい。<br>・関係者は大まかなものであるが、業務サイドでのセキュリティ事故発生時に取るべき基本的な対応を承知している<br>・業務サイドでのセキュリティ事故発生時の備えについての検討のレベルはクラスC以上<br>・業務サイドでのセキュリティ事故発生時の備えについての文書化のレベルはクラスC以上 |
| レベル1 | 業務サイドにおける問題が生じた時の備えはないに等しい。 |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | セキュリティ事故への対応に必要なシステム環境の洗い出しも十分で、これらは何時でも使える状態で整備されている。セキュリティ事故への対応で、システム環境面での準備の不備が、事故処理の障害になることは、まず考えられない。<br>・被害範囲の調査や、情報の回復、システムの復旧に必要なツールやリソースは、ほとんど準備されている<br>・これらは、何時でも使用できるようになっていることが定期的にチェックされている<br>・セキュリティ事故への対応で必要となるシステム環境の整備についての検討のレベルはクラスA<br>・セキュリティ事故への対応で必要となるシステム環境の整備についての見直し状況はクラスA<br>・この点に関するシステム環境の整備についての文書化のレベルはクラスA |
| レベル4 | セキュリティ事故への対応に必要なシステム環境が定義され、これらは何時でも使える状態で整備されていることになっている。ただし、必要なリソースやツールは十分とは言えず、また、その定期的な動作確認も徹底さを欠くところが見られ、セキュリティ事故への対応で、システム環境面での準備の不備が、事故処理の障害をもたらす可能性が、僅かではあるが残されている。<br>・被害範囲の調査や、情報の回復、システムの復旧に必要なツールやリソースは、概ねすべて準備されているが、費用他の関係で常備からは外されているものがある<br>・これらは、何時でも使用できるようになっていることが、定期的にチェックされていることになっているが、その確認に徹底さに欠くところもある<br>・セキュリティ事故への対応で必要となるシステム環境の整備についての検討のレベルはクラスB以上<br>・セキュリティ事故への対応で必要となるシステム環境の整備についての見直し状況はクラスB以上<br>・この点に関するシステム環境の整備についての文書化のレベルはクラスB以上 |
| レベル3 | セキュリティ事故への対応に必要なリソースやツールの検討はされているが、設備としての準備は、重要なもの中心となっている。また、その定期的な動作確認もあまり行われていない。システム環境面での準備の不徹底が、事故処理の障害になる余地が残されている。<br>・被害範囲の調査や、情報の回復、システムの復旧に必要なツールやリソースは、絶対不可欠なものは準備されているが、費用他の関係で常備からは外されているものもかなりある<br>・これらは、何時でも使用できるようになっていることが、定期的にチェックされていることになっているが、その確認は不十分で、必要な対応が何時でも迅速に取れるかどうかは疑わしいところがある<br>・セキュリティ事故への対応で必要となるシステム環境の整備についての検討のレベルはクラスB以上<br>・セキュリティ事故への対応で必要となるシステム環境の整備についての見直し状況はクラスB以上<br>・この点に関するシステム環境の整備についての文書化のレベルはクラスB以上 |
| レベル2 | セキュリティ事故への対応に必要なリソースやツールの検討はあまりされてなく、ツールやリソースの準備は一部に限られており、十分には程遠い。<br>・セキュリティ事故への対応のために最低限必要となるリソースやツールの整備への努力は見られる<br>・セキュリティ事故への対応で必要となるシステム環境の整備についての検討のレベルはクラスC以上<br>・この点に関するシステム環境の整備についての文書化のレベルはクラスC以上 |
| レベル1 | セキュリティ事故への対応に必要なリソースやツールの検討はあまりされてなく、準備はされていないに等しい。 |

## Td4.5 システムの長期停止への備え

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | システムの長期停止に対する備えが整備されており、システムの長期停止に対しても、普段とほぼ同じレベルで事業の継続ができるようなっている。<br>・システムの長期停止への対応策についての基本方針は経営レベルの承認されている<br>・リアルタイムで切り替えることができるバックアップセンターが準備され、大規模な災害にも、業務にほとんど影響を与えないようようになっている<br>・万一に備えた手作業での対応も十分に準備されている<br>・システムの長期停止への対応策は、実効的で、かつ、対象事業の経営での位置付けや、対象業務の特性等に照らし適切<br>・このような事態に対する対処要領は綿密に作成されている<br>・非常時に必要となる外部との連携も含め、これらの計画がいつでも迅速に機能するための確認も、随時行われている<br>・システムの長期停止への備えについての検討のレベルはクラスA<br>・システムの長期停止への備えについての見直し状況はクラスA<br>・システムの長期停止へのの備えについての文書化のレベルはクラスA |
| レベル4 | システムの長期停止に対する備えは整備されており、正常状態に比べある程度の制約はあるものの、事業の継続はできるようなっている。<br>・システムの長期停止への対応策についての基本方針は経営レベルの承認されている<br>・非常時の外部システムの使用等についての準備が完全になされていて、必要となったときは迅速な対応ができる準備はできている。ただし、業務の再開始までには、ある程度の時間が必要で、最開始後もある程度の制約はあるが、事業の継続への大きな影響はないようにされている<br>・万一に備えた手作業での対応も、十分に準備されている<br>・システムの長期停止への対応策は、実効的で、かつ、対象事業の経営での位置付けや、対象業務の特性等に照らし適切<br>・このような事態に対する対処要領は、かなり綿密に作成されているが、改善の余地もある<br>・非常時に必要となる外部との連携も含め、これらの計画がいつでも迅速に機能するための確認も、随時行われているが、十分とは言えない<br>・システムの長期停止への備えについての検討のレベルはクラスB以上<br>・システムの長期停止への備えについての見直し状況はクラスB以上<br>・システムの長期停止へのの備えについての文書化のレベルはクラスB以上 |
| レベル3 | システムの長期停止に対する備えについての計画は作られており、何時でも実施に移せる準備は行われている。実際の対応は必要時に行われるようになっている。計画している対策が機能するまでの間は、相当な制約がでる、最開始後も等分の間、相当の制約はでるものの、事業の継続に致命的な問題が生じることはないと考えられる。<br>・システムの長期停止への対応策についての基本方針は経営レベルの承認されている<br>・システムの長期停止への対応策は、実効的で、かつ、対象事業の経営での位置付けや、対象業務の特性等に照らし概ね適切<br>・このような事態に対する対処要領は纏められてはいるが、まだ十分とは言い切れない<br>・非常時に必要となる外部との連携も含め、これらの計画がいつでも迅速に機能するための確認は不十分<br>・システムの長期停止への備えについての検討のレベルはクラスB以上<br>・システムの長期停止への備えについての見直し状況はクラスB以上<br>・システムの長期停止へのの備えについての文書化のレベルはクラスB以上 |
| レベル2 | システムの長期停止に対する対応策は、検討されているが、具体的な準備に間では至っていない。万一、このような事態が生じても、別途の方法等もあり、事業の継続に大きな支障はないと見切っている。<br>・システムの長期停止に対する考え方は、経営陣は承知 |

| | |
|---|---|
| | ･システムの長期停止への備えについての検討のレベルはクラスＣ以上<br>･システムの長期停止へのの備えについての文書化のレベルはクラスＣ以上 |
| レベル1 | システムの長期停止に対する対応策は、検討されていない。万一、このような事態が生じても、別途の方法等もあり、事業継続は懸念される。 |

# 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 経営レベルでのセキュリティ監査を行うために完成度の高い仕組みが確立しており、組織的なセキュリティ監査実施の基盤が整備されている。<br>･経営陣が承認した監査方針、および監査計画のたて方や監査の実施手順を示した監査実施要領が確立している<br>･監査結果の評価および監査指摘事項のフォロー等の監査の後処理についての要領も確立している<br>･専門的な監査体制が整備されている<br>･何を、どのようにチェックし、どのような視点で評価するかを示す監査基準が確立している<br>･監査環境の整備についての検討のレベルはクラスA<br>･監査環境の整備についての見直し状況はクラスA<br>･監査環境の整備についての文書化のレベルはクラスA |
| レベル4 | 経営レベルでのセキュリティ監査を行うため仕組みが確立しており、組織的なセキュリティ監査実施の基盤が整備されているが、まだ改善の余地がある。<br>･経営陣が承認した監査方針、および監査計画のたて方や監査の実施手順を示した監査実施要領が確立している<br>･監査結果の評価および監査指摘事項のフォロー等の監査の後処理についての要領も確立している<br>･監査の専門部署は作られていないとしても、監査の実施に際して、被監査部門外の者を中心とする監査実施体制が作られるようにしている<br>･何を、どのようにチェックし、どのような視点で評価するかを示す監査基準が作られているが、十分に綿密とは言いがたい<br>･監査環境の整備についての検討のレベルはクラスB以上<br>･監査環境の整備についての見直し状況はクラスB以上<br>･監査環境の整備についての文書化のレベルはクラスB以上 |
| レベル3 | 監査の実施についての方針や大まかな監査ガイドは示され、監査の実施についての基盤は与えられているが、経営レベルでの監査環境の整備にまでは至っていない。組織的な取組みとしては評価できる。<br>･セキュリティ対策の責任者レベルでの監査方針や大まかな監査要領は作成されている<br>･監査は、セキュリティ対策の責任者が指名する者で行うようにされている<br>･何をチェックすべきかは相当なレベルで示されてはいるが、どのようなチェックを行い、どのような視点で評価するかまでは示されてなく、監査基準と言えるものには至っていない<br>･監査環境の整備についての検討のレベルはクラスB以上<br>･監査環境の整備についての見直し状況はクラスB以上<br>･監査環境の整備についての文書化のレベルはクラスB以上 |
| レベル2 | 監査については大まかな指針が与えられているだけで、実施要領や監査基準等は、関係者のメモレベルに止まっている。セキュリティ監査への取組姿勢は見える。<br>･セキュリティ対策の責任者レベルでの監査方針や大まかな監査要領は示されている<br>･監査は、セキュリティ対策の責任者が指名する者で行うようにされている<br>･何をチェックすべきかは大まかに示されてはいるが、どのようなチェックを行い、どのような視点で評価するかまでは示されてなく、監査基準と言えるものには至っていない<br>･監査環境の整備についての検討のレベルはクラスC以上<br>･監査環境の整備についての見直し状況はクラスC以上<br>･監査環境の整備についての文書化のレベルはクラスC以上 |

| | |
|---|---|
| レベル 1 | (本対策要求への対応に、レベル 1 は存在しない) |

## 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

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル 5 | 定められた監査実施基準や実施要領にもとづいて作成された監査計画に沿った経営レベルでの監査が、所定の体制の下で厳格に行われ、セキュリティ対策の実施状況が管理的側面から完全にチェックされている。<br>・年に 1 回以上、経営レベルの監査が実施されている<br>・監査は経営レベルの承認をえた監査計画に沿って、監査の専門体制の下で行われている<br>・監査は、はセキュリティ対策として要求のすべてに対して漏れなく実施されている<br>・監査は監査基準に沿って実施されており、監査についての信頼性は高い<br>・各監査項目についての証拠資料のチェックや被監査対象者に対するインタビューも徹底している<br>・技術的な監査事項については、専門家が参画している<br>・必要に応じ外部の専門家の支援も得ている<br>・監査計画や監査報告書および実施した監査についての文書化のレベルはクラス A |
| レベル 4 | 定められた監査実施基準や実施要領にもとづいて作成された監査計画に沿った経営レベルでの監査が、所定の体制の下で行われているが、監査事項の設定やその検証に厳格さに欠けるところがあり、細かい点についての問題点を見逃す可能性は残る。<br>・年に 1 回以上、経営レベルの監査が実施されている<br>・監査は経営レベルの承認をえた監査計画に沿って、監査の専門体制の下で行われている<br>・監査は、セキュリティ対策として要求のほぼすべてに対して実施されている<br>・監査は監査基準に沿って実施されており、監査についての信頼性は高い<br>・各監査項目についての証拠資料のチェックや被監査対象者に対するインタビューも行われているが厳格とは言いがたいところがある<br>・技術的な監査事項については、社内の専門家も参画している<br>・監査計画や監査報告書および実施した監査についての文書化のレベルはクラス B 以上 |
| レベル 3 | 監査は担当部門ベースで行われて経営陣に報告することになっている。監査事項やその検証のレベルは、セキュリティ対策の構造的な欠陥や実践面での要求への対応のレベルを大まかに見るレベル。経営レベルでの監査とは言い難いが、最低限の組織的な監査として評価できる。<br>・年に 1 回以上、部門レベルあるいはセキュリティ対策責任者による監査が実施されている<br>・結果は経営レベルに報告されている<br>・監査事項やチェックのレベルは、監査の実施責任者に任されているが、セキュリティ対策として要求のほぼすべてを対象にすることになっている<br>・監査の内容やチェックのレベルはは監査人個人のスキルに依存しておりバラツキがありうる<br>・各監査項目についての証拠資料のチェックや被監査対象者に対するインタビューも行われているがサンプリングベースで厳格さは低い<br>・監査計画や監査報告書および実施した監査についての文書化のレベルはクラス B 以上 |
| レベル 2 | 組織的な監査にはほど遠いが、対策現場単位での責任者によるチェックは年に一度は行われている。<br>・実施頻度は 2 年に 1 回以上<br>・監査実施単位で監査事項はある程度定められている<br>・監査計画や実施した監査についての文書化のレベルはクラス C 以上 |
| レベル 1 | 対策現場単位でも、監査と言う意味でのチェックは行われていない。 |

## Aa1.3 監査結果の評価･報告とフォローアップの実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | セキュリティ対策実施状況に対する監査結果は経営レベルで評価され、必要な指示がされている。また、指摘された改善の実施も、組織的な管理下、迅速かつ適切に行われている。<br>･監査報告書が作成され、監査責任者による承認が行われ、経営陣をはじめ関係者に報告されている<br>･監査結果に基づく的確な改善計画書が作成されている<br>･経営者から指摘事項に対する改善対応の指示を行っている<br>･改善計画書の沿った改善は、1ヶ月以内に適切に行われている<br>･指摘事項に対する改善対応状況のフォローアップ監査を必ず行っている<br>･監査報告書の評価や問題点の指摘、および改善計画についての検討のレベルはA<br>･監査報告書に対する経営陣の指示や改善事項に対するフォローアップについての文書化のレベルはA |
| レベル4 | セキュリティ対策実施状況に対する監査結果は経営レベルで評価され、必要な指示がされている。また、指摘された改善の実施も、組織的な管理下におかれているが、迅速さやそのフォローアップに不十分なところが見られる。<br>･監査報告書が作成され、監査責任者による承認が行われ、経営陣をはじめ関係者に報告されている<br>･経営者から指摘事項に対する改善対応の指示を行っている<br>･改善計画書の沿った改善は、遅くとも2ヶ月以内には行われている<br>･指摘事項に対する改善対応状況のフォローアップ監査を行っている<br>･監査報告書の評価や問題点の指摘、および改善計画についての検討のレベルはB以上<br>･監査報告書に対する経営陣の指示や改善事項に対するフォローアップについての文書化のレベルはB以上 |
| レベル3 | セキュリティ対策実施状況に対する監査結果の評価はセキュリティ対策の責任者に委ねられている。監査結果の報告やその評価および改善提案は経営レベルに報告されている。改善についてのフォローは、担当部門に任されているが、経営陣への報告事項にはなっている。<br>･監査報告書が作成され、セキュリティ対策の責任者の評価と、改善提案は、経営陣をはじめ関係者に報告されている<br>･経営者から指摘事項に対する改善対応の指示を行っている<br>･改善計画書の沿った改善は、3ヶ月以上かかっているものもある<br>･監査報告書の評価や問題点の指摘、および改善計画についての検討のレベルはB以上<br>･監査報告書に対する経営陣の指示や改善事項に対するフォローアップについての文書化のレベルはB以上 |
| レベル2 | 監査的なチェックによる指摘事項にたういての改善は、対象対策の責任者に任されているが、概ね、対応はされている。<br>･監査的なチェックは行われているが改善について組織的なフローは、あまり行われていない<br>･監査結果の報告や改善提案についての文書化のレベルはC以上<br>･指摘事項に吐いてのフォローについての文書化のレベルはC以上 |
| レベル1 | (本対策要求への対応に、レベル1は存在しない) |

### 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 |
|---|---|

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 綿密に検討された診断ツールを用いたシステムの脆弱性診断の実施要領が確立している。<br>・完成度の高い診断ツールを用いたシステムの脆弱性診断の実施要領が作成、承認されている<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての検討のレベルはクラスA<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての見直し状況はクラスA<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての文書化のレベルはクラスA |
| レベル4 | よく検討された診断ツールを用いたシステムの脆弱性診断の実施要領が確立しているが、まだ改善の余地がある。<br>・完成度の高い診断ツールを用いたシステムの脆弱性診断の実施要領が作成、承認されているが、きめの細かさにかけるところもあり、まだ改善の余地がある<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての検討のレベルはクラスB以上<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての見直し状況はクラスB以上<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての文書化のレベルはクラスB以上 |
| レベル3 | 診断ツールを用いたシステムの脆弱性診断の実施要領として大まかなものが示されているが、きめの細かさに欠けるところもあり、改善すべきところは少なくない。<br>・診断ツールを用いたシステムの脆弱性診断の実施要領が作成、承認されているが、大まかなもので、改善すべきところは少なくない<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての検討のレベルはクラスB以上<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての見直し状況はクラスB以上<br>・診断ツールを用いたシステムの脆弱性診断の実施要領についての文書化のレベルはクラスB以上 |
| レベル2 | 組織的に検討したものではないが、。担当チーム内には、習慣的に使用されている診断ツールを用いたシステムの脆弱性診断の手順が存在する。<br>・担当チーム内は、組織的に検討されたものではないが、診断ツールを用いたシステムの脆弱性診断の手順を持っており、実際に使われている<br>・診断ツールを用いたシステムの脆弱性診断の実施についての文書化のレベルはC以上 |
| レベル1 | （本対策要求への対応に、レベル1は存在しない） |

## Aa2.2 診断ツールを用いたシステムの脆弱性診断の実施

| 強度レベル | 当該レベル達成要件 |
|---|---|
| レベル5 | 定められた実施要領に沿ったシステムの脆弱性診断が高い密度で行われ、その結果についての評価も厳格に行われ、問題点に対するセキュリティ対策への反映も迅速に行われており、技術面での計画したセキュリティ対策は、完全に機能していることが常に確認されている。<br>・監視は 365 日 24 時間ベースでリアルタイム監視を実施<br>・現時点で可能な監視はほとんど適用<br>・監視結果の分析等も自動化されており、問題点はほぼリアルタイムの対応を行っている<br>・問題点の分析能力は十分に高い<br>・診断の実施や結果の評価や指摘された問題点への対処の実践と管理の徹底状況はクラス A<br>・診断の実施や結果の評価や指摘された問題点への対処についての文書化のレベルはクラス A |
| レベル4 | 定められた実施要領に沿ったシステムの脆弱性診断が、かなり高い密度で行われ、その結果についての評価も行われているが、実施頻度や分析事項、および結果の分析や問題点の判断、問題点のセキュリティ対策への反映等に十分とは言えないところも残る。技術面での計画したセキュリティ対策は、ほぼ十分に機能していることは確認されていると見てよいが、問題点が見逃されている可能性も残る。<br>・一部の監視については、365 日 24 時間ベースでリアルタイム監視を実施<br>・一般的に必要とされている監視はほとんど適用<br>・監視結果の分析等も自動化されており、問題点はほぼリアルタイムの対応を行っている<br>・問題点の分析能力は相当に高い<br>・診断の実施や結果の評価や指摘された問題点への対処の実践と管理の徹底状況はクラス B 以上<br>・診断の実施や結果の評価や問題点への対処についての文書化のレベルはクラス B 以上 |
| レベル3 | システムの脆弱性診断はあるレベルで行われているが、実施頻度や分析事項、および結果の分析や問題点の判断、問題点のセキュリティ対策への反映等は、十分とは言えない。技術面での計画したセキュリティ対策に欠陥があることが見逃されている可能性は低くない。<br>・一部の監視については、365 日 24 時間ベースでリアルタイム監視を実施<br>・一般的に重要とされている監視はほとんど適用<br>・監視結果の分析等も自動化されており、問題点はほぼリアルタイムの対応を行っている<br>・診断結果に対する最小限の分析能力は持っている、また、必要に応じ専門家の支援を得ている<br>・診断の実施や結果の評価や指摘された問題点への対処の実践と管理の徹底状況はクラス B 以上<br>・診断の実施や結果の評価や問題点への対処についての文書化のレベルはクラス B 以上 |
| レベル2 | 診断ツールによるシステムの脆弱性診断は、担当者レベルで行われているが、組織的な管理は行われてなく、実効性は疑問。<br>・レベル 3 の達成条件も満足できない |
| レベル1 | （本対策要求への対応に、レベル 1 は存在しない） |

## 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

| | | |
|---|---|---|
| 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ズ(株) |
| | 鶴 田正文 | グローバルセキュリティエキスパート(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･データ |
| | 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 | グローバルセキュリティエキスパート(株) |
| | 山崎文明 | グローバルセキュリティエキスパート(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2分冊:モデルの使用法と対策強度レベル判定基準
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。