クラウド情報セキュリティ管理基準

平成 28 年 3 月

特定非営利活動法人　日本セキュリティ監査協会

目　次

詳細目次

Ⅰ．主旨

クラウドコンピューティングは、IT業界のみならず、農業や商業など、様々な業界からその普及、発展が期待されているにもかかわらず、未だ我が国での利用は限定的である。その原因の一つとして、情報セキュリティに対する懸念が挙げられる。情報セキュリティ対策のための実践的な規範はあるが、組織が情報資産を所有することを前提として策定されたものであり、組織が情報資産を所有せずに全面的にクラウドコンピューティングを利用する場合、従来の規範による管理策だけで組織の情報セキュリティを確保するには不足があった。

このような状況を踏まえ、経済産業省は、平成23年4月1日に「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（以下「クラウドセキュリティガイドライン」という。）を公表した。クラウドセキュリティガイドラインは、クラウドサービス利用者の視点からJIS Q 27002:2006の各管理策を再考し、クラウドサービスを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として策定したものである。

クラウドセキュリティガイドラインによってクラウドサービス利用者が実施すべき事項が示されたが、未だクラウドサービス提供者が実施すべき事項は明らかではなく、また、クラウドサービス利用者がクラウドサービスを比較検討できるような標準的な情報セキュリティ尺度が望まれていた。

このような背景から、経済産業省は、既に一般に利用されている情報セキュリティ監査制度を活用して、クラウドサービス提供者のセキュリティレベルに一定の保証を与えることにより、クラウドコンピューティングの普及・発展を促進するため、平成23年度企業・個人の情報セキュリティ対策促進事業（グローバルなクラウドセキュリティ監査の利用促進）において「クラウド情報セキュリティ管理基準」を策定した。「クラウド情報セキュリティ管理基準」は、情報セキュリティ監査制度における主体別・業種別管理基準の一つであり、主体はサービス提供者、業種はクラウドサービス業とする。クラウドサービス提供者が提供するクラウドサービスは多様であり、クラウドサービス提供者がクラウドサービス利用者にコミットする情報セキュリティの水準やそれに関する情報を開示する水準（リスクコミュニケーションの水準）に相違が生じることがある。クラウドサービス提供者はコミットメントやサービス水準の相違を考慮し、本管理基準の趣旨及び体系にのっとって、必要に応じて本管理基準の項目等を取捨選択、追加することにより、クラウドサービス提供者又はクラウドサービス毎の個別管理基準を策定し活用することが望ましい。

「クラウド情報セキュリティ管理基準」は、「情報セキュリティ管理基準（平成28年改正版）」（平成28年経済産業省告示第37号）を基礎として、ISO/IEC27000シリーズの規格体系の変更を考慮し、改正を行った。ISO/IEC 27000シリーズは、セキュリティ全般の要求事項、実践規範をISO/IEC 27001:2013、ISO/IEC 27002:2013で定め、汎用的な管理策は、ISO/IEC 27002を参照し、分野ごとの特徴を踏まえた管理策の補足、追加等を、ISO/IEC 2701Xなどの個別の規格に定めることとしている。

「クラウド情報セキュリティ管理基準(平成28年改正版)」もISO/IEC 27000シリーズの体系に準じ、汎用的な内容については、「 情報セキュリティ管理基準(平成28年改正版) 」を参照する構成とし、ISO/IEC FDIS 27017に示されたクラウドサービスの特性を反映した事項のみを規定することとし、その主な特徴は次のとおりである。

1. 「ガバナンス基準」を追加している。クラウドサービスは、クラウドサービス利用者とクラウドサービス提供者という相互に独立したガバナンスの主体間の関係が問題となるからである。
2. 「マネジメント基準」は、汎用的な内容については、 「情報セキュリティ管理基準(平成28年改正版）」を参照し、クラウドサービスのために追加した「リスクコミュニケーション」のみ規定する。クラウドサービス提供者から利害関係者であるクラウドサービス利用者への情報提供が求められるからである。
3. 「管理策基準」は、汎用的な管理策は「情報セキュリティ管理基準(平成28年改正版）」を参照し、「クラウドサービス提供者の実施が望まれる事項」に対応するため管理策、クラウドサービスにおいて特に考慮すべきリスクに対応するために必要な管理策のみを規定している。また、付録として、「クラウドサービス利用者の実施が望まれる事項」についても補記している。

なお、「クラウド情報セキュリティ管理基準」は、「情報セキュリティ監査基準」（平成15年経済産業省告示第114号）に従って監査を行う場合、原則として、監査人が監査上の判断の尺度として用いるべき基準となる。

クラウドセキュリティ管理基準を用いてクラウドサービスを監査した場合、その報告書に、管理基準との対応状況、順守状況を記載してしまうと、その情報を元にして、クラウドサービスのぜい弱性を検出されてしまうおそれがある。このため、通常の情報セキュリティ監査の報告書の開示は、監査を要求した顧客等の関係者に限定されるべきである。

クラウドサービス利用者は不特定多数であり、このような監査ではクラウドサービスの幅広い利用を促すために資することが出来ない。個々のクラウドサービス利用者の注文に応じるのではなく、あらかじめ標準的な情報セキュリティについても標準的水準を定め、それを監査対象であるクラウド事業経営者が実施している旨の言明を行い、監査をすることでより幅広いクラウドの利用促進を図ることが出来る。

具体的には、以下の言明が想定される。

- 利用者が使用する論理的領域*1は、その利用者以外のアクセスから保護されていること
- 利用者が使用する論理的領域は、その利用者の要求に従って漏れなく正確に処理又は保存されていること
- 利用者が使用する論理的領域は、その利用者が要求した時に使用が可能であること
- 利用者が扱う情報は、その利用者以外のアクセスから保護されていること
- 利用者が扱う情報は、その利用者の要求に従って漏れなく正確に処理又は保存されていること
- 利用者が扱う情報は、その利用者が要求した時に使用が可能であること
- クラウドサービス提供者が扱う利用者に関する情報は、未承認又は不正なアクセスから保護されていること
- クラウドサービス提供者が扱う利用者に関する情報は、業務の必要に応じて漏れなく正確に処理又

*1 「論理的領域」とは、クラウドサービス提供者がコンピュータ等（例えば、サーバ、ストレージ、アプリケーション、ネットワーク等）の物理的なリソースを論理的に分割又は統合して、クラウドサービス利用者に割り当て、使用させる領域のことである。

は保存されていること
・クラウドサービス提供者が扱う利用者に関する情報は、業務の必要に応じて要求した時に使用が可能であること

これらの言明に必要な要件を整理した「クラウド情報セキュリティ基本言明要件」をあわせて記載している。

「クラウド情報セキュリティ基本言明要件」は、標準的な情報セキュリティを実装している旨をクラウドサービス提供者が言明するための要件である。当該要件を満たすことが情報セキュリティ監査を行った結果、保証される場合、クラウドサービス提供者はクラウドサービス利用者に対し、基本的で共通して必要とされる情報セキュリティ管理を行っていることを主張することができる。

Ⅱ．構成と用語の定義

2.1 クラウド情報セキュリティ管理基準の構成

「クラウド情報セキュリティ管理基準」は、「ガバナンス基準」、「マネジメント基準」、及び「管理策基準」から構成される。

「ガバナンス基準」は、情報セキュリティガバナンスのフレームワークの方向付け（Direct）、モニタリング（Monitor）、評価（Evaluate）、監督（Oversee）、報告（Report）に必要な実施事項を定めている。それぞれの事項は「情報セキュリティガバナンス導入ガイダンス」（経済産業省 平成21年6月）を基にして策定した。なお、「ガバナンス基準」は、原則、全て実施すべき事項である。

「マネジメント基準」では、情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項に、リスクコミュニケーションを加えて定めている。それぞれの事項は、JIS Q 27001:2014 情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項及びISO/IEC 27005:2008 情報技術―セキュリティ技術―情報セキュリティリスクマネジメントを基にして策定しているが、抽出に当たっては次の３点を考慮した。

- ISMS認証取得を目指している組織、独自に情報セキュリティマネジメントの確立を検討している組織、情報セキュリティ監査を実施する組織、情報セキュリティ監査を受ける組織など幅広い利用者を想定した記述とする。
- 情報セキュリティマネジメントの計画、実行、点検、処置、及びリスクコミュニケーションの各プロセスで行うべき事項を明確にする。
- 「マネジメント基準」の章構成は、情報セキュリティマネジメントのプロセスを考慮し、JIS Q 27001:2014における構成順序を変更する。その際、JIS Q27001:2014との対応が分かるようにように記載する。

「マネジメント基準」は、原則、全て実施すべき事項である。

「マネジメント基準」の内容は以下のとおりである。なお、汎用的な内容については、「情報セキュリティ管理基準（平成28年改正版）」を参照する。

4.1 マネジメント基準
4.2 記載内容について
4.3 凡例
4.4 情報セキュリティマネジメントの確立
4.5 情報セキュリティマネジメントの運用
4.6 情報セキュリティマネジメントのレビュー
4.7 情報セキュリティマネジメントの維持及び改善
4.8 文書化した情報の管理
4.9 情報セキュリティリスクコミュニケーション
4.9.1 リスクコミュニケーションの計画
4.9.2 リスクコミュニケーションの実施

「管理策基準」は、組織に情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を選択する際の選択肢を与えるものである。「管理策基準」のそれぞれの事項は、JIS Q 27001:2014附属書Ａ「管理目的及び管理策」、JIS Q 27002:2014、「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」及びクラウドサービスにかかわるリスク分析を基に専門家の知

見を加えて作成しており、管理目的と管理策で構成される。なお、汎用的な管理目的・管理策は「 情報セキュリティ管理基準(平成28年改正版）」を参照し、クラウドサービス固有の管理策やクラウドサービス提供者が実装する上での実践規範等のみを規定する。また「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」の「クラウドサービス提供者の実施が望まれる事項」及び既存のISMS認証などとの整合性にも配慮しているが、汎用的な管理策については「情報セキュリティ管理基準（平成28年改正版）」を参照し、クラウドサービスにおいて、クラウドサービス提供者が特に考慮すべき管理策については、「管理策番号.P」と表記している。また、付録に記載するクラウドサービス利用者が特に考慮すべき管理策については、「管理策番号.C」と表記している。

「管理策基準」の内、管理策(X.X.X)は、実施すべき事項であり、詳細管理策(X.X.X.X)は、管理策を実現する方法等に応じて、任意に選択する事項である。ある管理策の下にクラウドサービス提供者が特に考慮すべき詳細管理策(X.X.X.X.P)があるとき、 合理的な理由なくそれらの詳細管理策(X.X.X.X.P)が一つも選択されなければ、クラウドサービス提供者としてその管理策を実装しているとはみなさない。

「管理策基準」の内容は次のとおりである。

5 情報セキュリティのための方針群

5.1 情報セキュリティのための経営陣の方向性

6 情報セキュリティのための組織

6.1 内部組織

6.2 モバイル機器及びテレワーキング

6.3.P クラウドサービス利用者及びクラウドサービス提供者の関係

7 人的資源のセキュリティ

7.1 雇用前

7.2 雇用期間中

7.3 雇用の終了又は変更

8 資産の管理

8.1 資産に対する責任

8.1 資産に対する責任

8.2 情報分類

8.3 媒体の取扱い

9 アクセス制御

9.1 アクセス制御に対する業務上の要求事項

9.2 利用者アクセスの管理

9.3 利用者の責任

9.4 システム及びアプリケーションのアクセス制御

9.5.P 共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御

10 暗号

10.1 暗号による管理策

11 物理及び環境的セキュリティ

11.1 セキュリティを保つべき領域

11.2 装置
12 運用のセキュリティ
12.1 運用の手順及び責任
12.2 マルウェアからの保護
12.3 バックアップ
12.4 ログ取得及び監視
12.5 運用ソフトウェアの管理
12.6 技術的ぜい弱性管理
12.7 情報システムの監査に対する考慮事項
13 通信のセキュリティ
13.1 ネットワークセキュリティ管理
13.2 情報の転送
14 システムの取得、開発及び保守
14.1 情報システムのセキュリティ要求事項
14.2 開発及びサポートプロセスにおけるセキュリティ
14.3 試験データ
15 供給者関係
15.1 供給者関係における情報セキュリティ
15.2 供給者のサービス提供の管理
16 情報セキュリティインシデント管理
16.1 情報セキュリティインシデントの管理及びその改善
17 事業継続マネジメントにおける情報セキュリティの側面
17.1 情報セキュリティ継続
17.2 冗長性
18 順守
18.1 法的及び契約上の要求事項の順守
18.2 情報セキュリティのレビュー

なお、同様に、クラウドサービス利用者が特に考慮するべき管理策については、参考に「付録　クラウドサービス利用者向け管理策基準」として示す。

2.2 クラウド情報セキュリティ基本言明要件の構成

「クラウド情報セキュリティ基本言明要件」は、「ガバナンス基準」、「マネジメント基準」、及び「管理策基準」から構成される。「ガバナンス基準」及び「マネジメント基準」は、「クラウド情報セキュリティ管理基準」のものと同じである。

管理策[X.X.X]は、クラウドサービスを利用する際のリスクとして専門家が抽出した21種類のリスクのうち、「高」と「中」に分類される11種類のリスク*2に加えて、「低」のうちクラウドサービス提供者

*2 経済産業省委託事業 平成２３年度企業・個人の情報セキュリティ対策促進事業 （グローバルなクラウドセキュリティ監査の利用促進）による。

が顧客からよく問われるもの３つ*3を加えた基本リスクへの対策として実施すべき事項である。

21種類のリスク*4および基本リスクは、下記の表の通りある。

番号	リスクの識別名	基本リスク
H01	リソース・インフラの高集約によるインシデントの影響の拡大	○
H02	仮想／物理の設計・運用の不整合	○
H03	他の共同利用者の行為による信頼の喪失	○
H04	リソースの枯渇（リソース割当の過不足）	○
H05	隔離の失敗	○
H06	サービスエンジンの侵害	○
M07	クラウドプロバイダでの内部不正－特権の悪用	○
M08	管理用インタフェースの悪用（操作、インフラストラクチャアクセス）	○
M09	データ転送途上における攻撃、データ漏えい（アップロード時、ダウンロード時、クラウド間転送）	○
M10	セキュリティが確保されていない、または不完全なデータ削除	○
M11	クラウド内DDoS/DoS攻撃	○
L12	ロックインによるユーザの忌避	
L13	ガバナンスの喪失	
L14	サプライチェーンにおける障害	○
L15	EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）	
L16	事業者が管理すべき暗号鍵の喪失	
L17	不正な探査・スキャンの実施	
L18	証拠提出命令と電子的証拠開示	○
L19	司法権の違い	○
L20	個人データ保護	
L21	ライセンス	

さらに、クラウドサービス利用における重要なリスクに対応するため、専門家により特に必要性があると認められた詳細管理策が基本言明要件に含まれる。また、ISO/IEC 27002:2013に記載のないISO/IEC FDIS 27017の新規の管理策、及び既存の管理策のうち新たな「実施の手引」が加筆された管理策を基本言明要件とした。クラウドのリスク対応のために他に選択の余地のない詳細管理策は、それ自体が基本言明要件である。

「クラウド情報セキュリティ基本言明要件」の内容は次のとおりである。なお、項番は「クラウド情報セキュリティ管理基準」と同じ項番を使用しているため、抜けている項番は「クラウド情報セキュリ

*3 日本セキュリティ監査協会（JASA－クラウドセキュリティ推進協議会）加入メンバーによる検討に基づく。

*4 リスクの説明は付録2に記載。

ティ管理基準」と「クラウド情報セキュリティ基本言明要件」との差分を示す。

「ガバナンス基準」のすべて

「マネジメント基準」のすべて

「管理策基準」の以下の節のうちの一部（詳細は「VI. クラウド情報セキュリティ基本言明要件」参照）

5 情報セキュリティのための方針群

5.1 情報セキュリティのための経営陣の方向性

6 情報セキュリティのための組織

6.1 内部組織

6.2 モバイル機器及びテレワーキング

6.3.P クラウドサービス利用者及びクラウドサービス提供者の関係

7 人的資源のセキュリティ

7.1 雇用前

7.2 雇用期間中

8 資産の管理

8.1 資産に対する責任

8.2 情報分類

8.3 媒体の取扱い

9 アクセス制御

9.1 アクセス制御に対する業務上の要求事項

9.2 利用者アクセスの管理

9.3 利用者の責任

9.4 システム及びアプリケーションのアクセス制御

9.5.P 共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御

10 暗号

10.1 暗号による管理策

11 物理及び環境的セキュリティ

11.1 セキュリティを保つべき領域

11.2 装置

12 運用のセキュリティ

12.1 運用の手順及び責任

12.2 マルウェアからの保護

12.3 バックアップ

12.4 ログ取得及び監視

12.5 運用ソフトウェアの管理

12.6 技術的ぜい弱性管理

13 通信のセキュリティ

13.1 ネットワークセキュリティ管理

13.2 情報の転送

14 システムの取得、開発及び保守
14.1 情報システムのセキュリティ要求事項
14.2 開発及びサポートプロセスにおけるセキュリティ
15 供給者関係
15.1 供給者関係における情報セキュリティ
15.2 供給者のサービス提供の管理
16 情報セキュリティインシデント管理
16.1 情報セキュリティインシデントの管理及びその改善
17 事業継続マネジメントにおける情報セキュリティの側面
17.1 情報セキュリティ継続
18 順守
18.1 法的及び契約上の要求事項の順守
18.2 情報セキュリティのレビュー

2.3 用語及び定義

「情報セキュリティ管理基準（平成20年改正版）」（平成20年経済産業省告示第246号）になく、本管理基準で用いる新たな用語及び定義は、次による。

2.3.1 情報セキュリティガバナンス

社会的責任にも配慮したコーポレート・ガバナンスと、それを支えるメカニズムである内部統制の仕組みを、情報セキュリティの観点から企業内に構築・運用すること。

2.3.2 クラウドコンピューティング

共有化されたコンピュータリソース（サーバ、ストレージ、アプリケーション等）について、利用者の要求に応じて適宜・適切に配分し、ネットワークを通じて提供することを可能とする情報処理形態。注記これよりも広い定義が使われることもある。

2.3.3 クラウドサービス

クラウドコンピューティングを提供するサービス。

2.3.4 クラウドサービス利用者

クラウドサービスを利用する組織。

2.3.5 クラウドサービスのユーザ

クラウドサービス利用者（クラウドサービスを利用する組織）において、クラウドサービスを利用する者。

Ⅲ. ガバナンス基準

既に記載している通り、ガバナンス基準は、原則としてすべて実施しなければならない。

3.1 情報セキュリティガバナンス

情報資産にかかわるリスクの管理をねらいとして、経営陣が方針を決定し、組織内の状況をモニタリングする仕組み及び利害関係者に対する開示と利害関係者による評価の仕組みを構築・運用することにより、情報セキュリティガバナンスを確立する。情報セキュリティガバナンスは、経営陣が情報セキュリティマネジメントの確立における「コミット」を行うための基礎となる活動である。

3.1.1 情報セキュリティガバナンスのフレームワーク

情報セキュリティガバナンスは、経営戦略やリスク管理の観点から行う「方向付け（Direct）」、ガバナンス活動の状況を指標に基づき可視化する「モニタリング（Monitor）」、結果を判断する「評価（Evaluate）」、これらのプロセスが機能していることを確認する「監督（Oversee）」、結果を利害関係者などに提示する「報告（Report）」の5つの活動から構成される。

3.1.2 方向付け（Direct）

3.1.2.1　経営陣は、経営戦略に基づくリスク管理方針を提示する

経営陣は、企業価値の向上と社会的責任の遂行のために、適法性・適正性に配慮した上で、経営戦略やそれに基づくリスク管理の方針を提示する。

3.1.3 モニタリング（Monitor）

3.1.3.1　経営陣は、リスク管理の評価を行うために有効かつ適切な評価指標を設定し、必要な情報を収集する

経営陣が示した方向付けに従って、適切にリスク管理がなされていることを経営陣が理解できる形で示し、経営陣が評価を行えるようにするために必要な情報を収集する。モニタリングを行うために有効かつ適切な評価指標が設定されることが必要である。

3.1.4 評価（Evaluate）

3.1.4.1　経営陣は、リスク管理方針の達成状況とリスクの変化を評価する

方向付け（Direct）した方針や情報セキュリティ目的・目標が実現できたかどうかを評価する。リスク管理方針が達成できたか、リスクが変化していないかを評価する。

3.1.5 監督（Oversee）

3.1.5.1　リスク管理方針の提示、評価指標の設定と情報の収集、リスク管理方針の達成状況とリスクの変化の評価のそれぞれについて確認し、必要に応じて問題の改善を促す

方向付け（Direct）、モニタリング（Monitor）、評価（Evaluate）が適切に遂行していることを確認し、必要に応じて問題の改善を促す。監督（Oversee）の実装に際しては、業務執行者を監督する制度が国によって異なることに配慮する。

3.1.6 報告（Report）

3.1.6.1　経営陣は、利害関係者に対しリスク管理の状況について報告する

経営陣は、株主、取引先や顧客、従業員、社会全体を含めた利害関係者に対し、リスク管理の責任者として、情報セキュリティにかかわるリスク管理の状況について報告する。報告は、利害関係者が当該企業の価値について評価し、取引先や投資先の選別・選定を行うためであることに留意する。

Ⅳ. マネジメント基準

既に記載している通り、マネジメント基準は、原則としてすべて実施しなければならない。

4.1 マネジメント基準

「情報セキュリティ管理基準」の「マネジメント基準」に同じ。

4.2 記載内容について

「情報セキュリティ管理基準」の「マネジメント基準」に同じ。

クラウドサービスにおいては、クラウドサービス利用者の環境等を考慮して、クラウドサービス提供者の管理策等を検討し、実施する必要がある。そのため、クラウドサービス利用者及びクラウドサービス提供者間において、クラウドサービスにおける情報セキュリティリスクとその対応について、情報交換することが非常で重要である。

当該情報セキュリティリスクコミュニケ―ションについては、クラウドサービスにおいて特に考慮するべき事項として、4.9章に規定する。

4.3 凡例

「情報セキュリティ管理基準」の「マネジメント基準」に同じ。

4.4 情報セキュリティマネジメントの確立

「情報セキュリティ管理基準」の「マネジメント基準」に同じ。

4.5 情報セキュリティマネジメントの運用

「情報セキュリティ管理基準」の「マネジメント基準」に同じ。

4.6 情報セキュリティマネジメントのレビュー

「情報セキュリティ管理基準」の「マネジメント基準」に同じ。

4.7 情報セキュリティマネジメントの維持及び改善

「情報セキュリティ管理基準」の「マネジメント基準」に同じ。

4.8 文書化した情報の管理

「情報セキュリティ管理基準」の「マネジメント基準」に同じ。

4.9 情報セキュリティリスクコミュニケーション

利害関係者間の有効なコミュニケーションは、意思決定に大きな影響を与えることがある。情報セキュリティリスクコミュニケーションは、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間で情報セキュリティリスクに関する情報を交換、共有し、リスクを管理する方法に関する合意を得る。

4.9.1 リスクコミュニケーションの計画

4.9.1.1　リスクコミュニケ―ション計画を策定する。

リスクコミュニケーション計画は、以下の２つに分けて策定し、文書化する。

・通常運用のためのリスクコミュニケーション計画

・緊急事態のためのリスクコミュニケーション計画

リスクコミュニケーション計画は、意思決定者とその他の利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）との間でどのようにコミュニケーションを図るかに留意し、以下の内容について含める。

・適切な利害関係者の参画による、効果的な情報交換／共有

・法律、規制及びガバナンスの要求事項の順守

・コミュニケーション及び協議に関するフィードバック及び報告の提供

・組織に対する信頼を醸成するためのコミュニケーションの活用

・危機又は不測の事態発生時の利害関係者とのコミュニケーションの実施

4.9.2 リスクコミュニケーションの実施

4.9.2.1　リスクコミュニケ―ションを実施する仕組みを確定する。

リスクに関する論議、その優先順位の決定及び適切なリスク対応、並びにリスク受容を行い、主要な意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の協調を得る仕組みを確定する。この仕組みでは次の事項を確実にする。

・リスクマネジメントの枠組みの主要な構成要素、及びその後に行うあらゆる修正の適切な伝達

・枠組み、その有効性及び成果に関する適切な内部報告

・適切な階層及び時期に利用可能な、リスクマネジメントの適応から導出される関連情報

・内部の利害関係者との協議のためのプロセス

仕組みには、適切な場合には、多様な情報源からのリスク情報について、まとめ上げるプロセスが含まれ、また、リスク情報の影響の受けやすさを考慮する必要がある場合もある。なお、この仕組みを設ける場として、委員会がある。

4.9.2.2　リスクコミュニケ―ションを実施する。

リスクコミュニケーションは、次の点を達成するために、リスクマネジメントプロセスのすべての段階で継続的に実施する。

・組織のリスクマネジメント結果の保証を提供する

・リスク情報を収集する

・リスクアセスメントの結果を共有しリスク対応計画を提示する

・意思決定者と利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）の相互理解の欠如による情報セキュリティ違反の発生及び結果を回避又は低減する

・意思決定を支援する

・新しい情報セキュリティ知識を入手する

・他の組織と協調しすべてのインシデントの結果を低減するための対応計画を立案する
・意思決定者及び利害関係者（クラウドサービス利用者及びクラウドサービスの提供にかかわる委託先を含む。）にリスクについての責任を意識させる
・セキュリティ意識を改善する

リスクコミュニケーションの実施においては、組織内の適切な広報又はコミュニケーション部門と協力し、リスクコミュニケーション関連の全タスクを調整して行う。

Ⅴ．管理策基準

管理策基準に記載される管理策[X.X.X]は、情報セキュリティリスクアセスメントの結果に基づき、適切に選択すべき事項である。詳細管理策[X.X.X.X]については、管理策を実装するために組織・環境・技術等に応じて必要とする事項を選択する。

「P」は、クラウドサービスにおける、クラウドサービス提供者向け管理策であることを示す。

5　情報セキュリティのための方針群

5.1　情報セキュリティのための経営陣の方向性

目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。

5.1.1　情報セキュリティのための方針群は、これを定義し、管理層[*5]が承認し、発行し、従業員及び関連する外部関係者に通知する。

5.1.1.1 / 5.1.1.2 / 5.1.1.3 / 5.1.1.4 / 5.1.1.5 / 5.1.1.6 / 5.1.1.7 / 5.1.1.8 / 5.1.1.9 / 5.1.1.10 / 5.1.1.11 / 5.1.1.12 / 5.1.1.13 / 5.1.1.14 / 5.1.1.15 / 5.1.1.16 / 5.1.1.17 / 5.1.1.18 / 5.1.1.19 / 5.1.1.20 / 5.1.1.21は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

5.1.1.22.P　クラウドサービス提供者は、クラウドサービスの設計及び実装に適用可能な基本的な情報セキュリティ要求事項を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.23.P　クラウドサービス提供者は、認可された内部関係者からのリスクを考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.24.P　クラウドサービス提供者は、マルチテナント及びクラウドサービス利用者の隔離（仮想化を含む）を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.25.P　クラウドサービス提供者は、クラウドサービス提供者の職員によるクラウドサービス利用者の資産へのアクセスを考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.26.P　クラウドサービス提供者は、例えばクラウドサービスへの管理上のアクセスのための強固な認証などのアクセス制御手順を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.27.P　クラウドサービス提供者は、変更管理中のクラウドサービス利用者への通知を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.28.P　クラウドサービス提供者は、仮想化セキュリティを考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.29.P　クラウドサービス提供者は、クラウドサービス利用者のデータへのアクセス及び保護を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方

---

*5 管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。

針を拡大する。

5.1.1.30.P　クラウドサービス提供者は、クラウドサービス利用者のアカウントのライフサイクル管理を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.31.P　クラウドサービス提供者は、調査及びフォレンジックを支援するための、違反の通知及び情報共有の指針を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.2　情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。

5.1.2.1 / 5.1.2.2 / 5.1.2.3 / 5.1.2.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6　情報セキュリティのための組織

6.1　内部組織

目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

6.1.1　全ての情報セキュリティの責任を定め、割り当てる。

6.1.1.1 / 6.1.1.2 / 6.1.1.3 / 6.1.1.4 / 6.1.1.5 / 6.1.1.6 / 6.1.1.7 / 6.1.1.8 / 6.1.1.9 / 6.1.1.10 / 6.1.1.11 / 6.1.1.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.1.13.P　クラウドサービス提供者は、クラウドサービス利用者、クラウドサービス提供者及び供給者と情報セキュリティの役割及び責任の適切な割当てについて合意し、文書化する。

6.1.2　相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。

6.1.2.1 / 6.1.2.2 / 6.1.2.3 / 6.1.2.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.3　関係当局との適切な連絡体制を維持する。

6.1.3.1 / 6.1.3.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.3.3.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス提供者の組織の地理的所在地、及びクラウドサービス提供者がクラウドサービス利用者のデータを保管する可能性のある国々を通知する。

6.1.4　情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。

6.1.4.1 / 6.1.4.2 / 6.1.4.3 / 6.1.4.4 / 6.1.4.5 / 6.1.4.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.5　プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。

6.1.5.1 / 6.1.5.2 / 6.1.5.3 / 6.1.5.4 / 6.1.5.5 / 6.1.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.2　モバイル機器及びテレワーキング

目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

6.2.1　モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。

6.2.1.1 / 6.2.1.2 / 6.2.1.3 / 6.2.1.4 / 6.2.1.5 / 6.2.1.6 / 6.2.1.7 / 6.2.1.8 / 6.2.1.9 / 6.2.1.10 / 6.2.1.11 / 6.2.1.12 / 6.2.1.13 / 6.2.1.14 / 6.2.1.15 / 6.2.1.16 / 6.2.1.17 / 6.2.1.18 / 6.2.1.19 / 6.2.1.20 / 6.2.1.21 / 6.2.1.22は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.2.2　テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。

6.2.2.1 / 6.2.2.2 / 6.2.2.3 / 6.2.2.4 / 6.2.2.5 / 6.2.2.6 / 6.2.2.7 / 6.2.2.8 / 6.2.2.9 / 6.2.2.10 / 6.2.2.11 / 6.2.2.12 / 6.2.2.13 / 6.2.2.14 / 6.2.2.15 / 6.2.2.16 / 6.2.2.17 / 6.2.2.18 / 6.2.2.19 / 6.2.2.20 / 6.2.2.21は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.3.P　クラウドサービス利用者及びクラウドサービス提供者の関係

目的：情報セキュリティマネジメントのための、クラウドサービス利用者及びクラウドサービス提供者間の共同責任の関係を説明するため。

6.3.1.P　クラウドサービス利用者及びクラウドサービス提供者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装する。

6.3.1.1.P　クラウドサービス提供者は、クラウドサービス利用の一環としてクラウドサービス利用者が実施及び管理を必要とする情報セキュリティの役割と責任に加え、クラウドサービスの利用に対する、クラウドサービス提供者の情報セキュリティ管理策及び責任を文書化し、通知する。

7　人的資源のセキュリティ

7.1　雇用前

目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。

7.1.1　全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。

7.1.1.1 / 7.1.1.2 / 7.1.1.3 / 7.1.1.4 / 7.1.1.5 / 7.1.1.6 / 7.1.1.7 / 7.1.1.8 / 7.1.1.9 / 7.1.1.10 / 7.1.1.11 / 7.1.1.12 / 7.1.1.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.1.2　従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。

7.1.2.1 / 7.1.2.2 / 7.1.2.3 / 7.1.2.4 / 7.1.2.5 / 7.1.2.6 / 7.1.2.7 / 7.1.2.8 / 7.1.2.9 / 7.1.2.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.2　雇用期間中

目的：従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを

確実にするため。

7.2.1　経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。

7.2.1.1 / 7.2.1.2 / 7.2.1.3 / 7.2.1.4 / 7.2.1.5 / 7.2.1.6 / 7.2.1.7 / 7.2.1.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.2.2　組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。

7.2.2.1 / 7.2.2.2 / 7.2.2.3 / 7.2.2.4 / 7.2.2.5 / 7.2.2.6 / 7.2.2.7 / 7.2.2.8 / 7.2.2.9 / 7.2.2.10 / 7.2.2.11 / 7.2.2.12 / 7.2.2.13 / 7.2.2.14 / 7.2.2.15 / 7.2.2.16 / 7.2.2.17 / 7.2.2.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.2.2.19.P　クラウドサービス提供者は、クラウドサービス利用者のデータ及びクラウドサービスの派生データ[6]の適切な取扱いに関して、従業員に意識向上のための教育及び訓練を提供し、かつ同じことをするよう契約相手に要請する。

7.2.3　情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備える。

7.2.3.1 / 7.2.3.2 / 7.2.3.3 / 7.2.3.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.3　雇用の終了及び変更

目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。

7.3.1　雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。

7.3.1.1 / 7.3.1.2 / 7.3.1.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8　資産の管理

8.1　資産に対する責任

目的：組織の資産を特定し、適切な保護の責任を定めるため。

8.1.1　情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。

8.1.1.1 / 8.1.1.2 / 8.1.1.3 / 8.1.1.4 / 8.1.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.1.6.P　クラウドサービス提供者の資産目録は、クラウドサービス利用者のデータ及びクラウドサービスの派生データを明確に特定する。

8.1.2　目録の中で維持される資産は、管理する。

8.1.2.1 / 8.1.2.2 / 8.1.2.3 / 8.1.2.4 / 8.1.2.5 / 8.1.2.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.3　情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関

---

[6] このデータは、クラウドサービス利用者に秘密の情報を含む可能性がある、又はクラウドサービス提供者によるアクセス及び利用において、規制による制限を含む特別な制限が科される可能性がある。

する規則は、明確にし、文書化し、実施する。

8.1.3.1 / 8.1.3.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.4　全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。

8.1.4.1 / 8.1.4.2 / 8.1.4.3 / 8.1.4.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.5.P　クラウドサービス提供者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時期を失せずに返却または除去する。

8.1.5.1.P　クラウドサービス提供者は、クラウドサービス利用の合意の終了時における、クラウドサービス利用者の全ての資産の返却及び除去の取決めについて、情報を提供する。

8.1.5.2.P　クラウドサービス提供者は、資産の返却及び除去についての取決めにおいては、合意して文書化し、時期を失せずに実施する。

8.1.5.3.P　クラウドサービス提供者は、取決めにおいて返却及び除去する資産を特定する。

8.2　情報分類

目的：組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

8.2.1　情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。

8.2.1.1 / 8.2.1.2 / 8.2.1.3 / 8.2.1.4 / 8.2.1.5 / 8.2.1.6 / 8.2.1.7 / 8.2.1.8 / 8.2.1.9 / 8.2.1.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.2.2　情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。

8.2.2.1 / 8.2.2.2 / 8.2.2.3 / 8.2.2.4 / 8.2.2.5 / 8.2.2.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.2.2.7.P　クラウドサービス提供者は、クラウドサービス利用者が情報及び関連資産を分類し、ラベル付けするためのサービス機能を文書化し、開示する。

8.2.3　資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。

8.2.3.1 / 8.2.3.2 / 8.2.3.3 / 8.2.3.4 / 8.2.3.5 / 8.2.3.6 / 8.2.3.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.3　媒体の取扱い

目的：媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。

8.3.1　組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。

8.3.1.1 / 8.3.1.2 / 8.3.1.3 / 8.3.1.4 / 8.3.1.5 / 8.3.1.6 / 8.3.1.7 / 8.3.1.8 / 8.3.1.9 / 8.3.1.10 / 8.3.1.11は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.3.2　媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。

8.3.2.1 / 8.3.2.2 / 8.3.2.3 / 8.3.2.4 / 8.3.2.5 / 8.3.2.6 / 8.3.2.7 / 8.3.2.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.3.3　情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。

8.3.3.1 / 8.3.3.2 / 8.3.3.3 / 8.3.3.4 / 8.3.3.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9　アクセス制御

9.1　アクセス制御に対する業務上の要求事項

目的：情報及び情報処理施設へのアクセスを制限するため。

9.1.1　アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。

9.1.1.1 / 9.1.1.2 / 9.1.1.3 / 9.1.1.4 / 9.1.1.5 / 9.1.1.6 / 9.1.1.7 / 9.1.1.8 / 9.1.1.9 / 9.1.1.10 / 9.1.1.11 / 9.1.1.12 / 9.1.1.13 / 9.1.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.1.2　利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。

9.1.2.1 / 9.1.2.2 / 9.1.2.3 / 9.1.2.4 / 9.1.2.5 / 9.1.2.6 / 9.1.2.7 / 9.1.2.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2　利用者アクセスの管理

目的：システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。

9.2.1　アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施する。

9.2.1.1 / 9.2.1.2 / 9.2.1.3 / 9.2.1.4 / 9.2.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.1.6.P　クラウドサービスのユーザによるクラウドサービスへのアクセスをクラウドサービス利用者が管理するため、クラウドサービス提供者は、クラウドサービス利用者に、ユーザの登録及び登録削除の機能及び仕様を提供する。

9.2.2　全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。

9.2.2.1 / 9.2.2.2 / 9.2.2.3 / 9.2.2.4 / 9.2.2.5 / 9.2.2.6 / 9.2.2.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.2.8.P　クラウドサービス提供者は、クラウドサービスのユーザのアクセス権を管理する機能及び仕様を提供する。

9.2.3　特権的アクセス権の割当て及び利用は、制限し、管理する。

9.2.3.1 / 9.2.3.2 / 9.2.3.3 / 9.2.3.4 / 9.2.3.5 / 9.2.3.6 / 9.2.3.7 / 9.2.3.8 / 9.2.3.9 / 9.2.3.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.3.11.P　クラウドサービス提供者は、特定したリスクに応じて、クラウドサービスの管理能力にあわせたクラウドサービス利用者の管理者認証に、十分に強固な認証技術[7]を提供する。

9.2.4　秘密認証情報の割当ては、正式な管理プロセスによって管理する。

9.2.4.1 / 9.2.4.2 / 9.2.4.3 / 9.2.4.4 / 9.2.4.5 / 9.2.4.6 / 9.2.4.7 / 9.2.4.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.4.9.P　クラウドサービス提供者は、秘密認証情報を割り当てる手順、及びユーザ認証手順を含む、クラウドサービス利用者の秘密認証情報の管理手順について、情報を提供する。

9.2.5　資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。

9.2.5.1 / 9.2.5.2 / 9.2.5.3 / 9.2.5.4 / 9.2.5.5 / 9.2.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.6　全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。

9.2.6.1 / 9.2.6.2 / 9.2.6.3 / 9.2.6.4 / 9.2.6.5 / 9.2.6.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.3　利用者の責任

目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。

9.3.1　秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。

9.3.1.1 / 9.3.1.2 / 9.3.1.3 / 9.3.1.4 / 9.3.1.5 / 9.3.1.6 / 9.3.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4　システム及びアプリケーションのアクセス制御

目的：システム及びアプリケーションへの、認可されていないアクセスを防止するため

9.4.1　情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。

9.4.1.1 / 9.4.1.2 / 9.4.1.3 / 9.4.1.4 / 9.4.1.5 / 9.4.1.6 / 9.4.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.1.8.P　クラウドサービス提供者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスにて保持されるクラウドサービス利用者のデータへのアクセスを、クラウドサービス利用者が制限できるよう、アクセス制御を提供する。

9.4.2　アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。

9.4.2.1 / 9.4.2.2 / 9.4.2.3 / 9.4.2.4 / 9.4.2.5 / 9.4.2.6 / 9.4.2.7 / 9.4.2.8 / 9.4.2.9 / 9.4.2.10 / 9.4.2.11 / 9.4.2.12 / 9.4.2.13 / 9.4.2.14 / 9.4.2.15 / 9.4.2.16は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

---

[7] 例えば、クラウドサービス提供者は多要素認証機能を提供し、又はサードパーティの多要素認証の仕組みを利用可能にすることができる。

9.4.3　パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。

9.4.3.1 / 9.4.3.2 / 9.4.3.3 / 9.4.3.4 / 9.4.3.5 / 9.4.3.6 / 9.4.3.7 / 9.4.3.8 / 9.4.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.4　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。

9.4.4.1 / 9.4.4.2 / 9.4.4.3 / 9.4.4.4 / 9.4.4.5 / 9.4.4.6 / 9.4.4.7 / 9.4.4.8 / 9.4.4.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.4.10.P　クラウドサービス提供者は、クラウドサービス内で利用する全てのユーティリティプログラムのための要求事項を特定する。

9.4.4.11.P　クラウドサービス提供者は、通常の操作手順又はセキュリティ手順を回避することのできる全てのプログラムは、認可された要員に厳重に制限し、そのようなプログラムの利用は、定期的にレビューし、監査する。

9.4.5　プログラムソースコードへのアクセスは、制限する。

9.4.5.1 / 9.4.5.2 / 9.4.5.3 / 9.4.5.4 / 9.4.5.5 / 9.4.5.6 / 9.4.5.7 / 9.4.5.8 / 9.4.5.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.5.P　共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御

目的：共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。

9.5.1.P　クラウドサービス利用者のクラウドサービス上の仮想環境は、他のクラウドサービス利用者及び認可されていない者から保護する。

9.5.1.1.P　クラウドサービス提供者は、マルチテナント環境におけるクラウドサービス利用者の使用する資源を分離するため、仮想化されたアプリケーション、オペレーティングシステム、ストレージ及びネットワークの適切な論理的分離を実施する。

9.5.1.2.P　クラウドサービス提供者は、クラウドサービス利用者の使用する資源からのクラウドサービス提供者の内部管理を分離するため、仮想化されたアプリケーション、オペレーティングシステム、ストレージ及びネットワークの適切な論理的分離を実施する。

9.5.1.3.P　クラウドサービスがマルチテナントである場合には、クラウドサービス提供者は、異なるテナントが使用する資源を適切に分離するための情報セキュリティ管理策を実施する。

9.5.1.4.P　クラウドサービス提供者は、クラウドサービス提供者が提供するクラウドサービスの内部において、クラウドサービス利用者の所有するソフトウェアの実行が関係するリスク対応を検討する。

9.5.2.P　クラウドコンピューティング環境における仮想マシンは、事業上のニーズを満たすため、要塞化する。

9.5.2.1.P　クラウドサービス提供者は、仮想マシンを設定する際には、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする）、利用する各仮想マシンに適切な技術的管理策(例えば、マルウェア対策、ログ取得）を実施する。

10　暗号

10.1　暗号による管理策

目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため

10.1.1　情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。

10.1.1.1 / 10.1.1.2 / 10.1.1.3 / 10.1.1.4 / 10.1.1.5 / 10.1.1.6 / 10.1.1.7 / 10.1.1.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

10.1.1.9.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス利用者が処理する情報を保護するために暗号技術を利用する環境について、情報を提供する。

10.1.1.10.P　クラウドサービス提供者は、クラウドサービス利用者が独自の暗号による保護を適用することを支援するための機能について、クラウドサービス利用者に情報を提供する。

10.1.2　暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施する。

10.1.2.1 / 10.1.2.2 / 10.1.2.3 / 10.1.2.4 / 10.1.2.5 / 10.1.2.6 / 10.1.2.7 / 10.1.2.8 / 10.1.2.9 / 10.1.2.10 / 10.1.2.11 / 10.1.2.12 / 10.1.2.13 / 10.1.2.14 / 10.1.2.15 / 10.1.2.16 / 10.1.2.17 / 10.1.2.18 / 10.1.2.19は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11　物理的及び環境的セキュリティ

11.1　セキュリティを保つべき領域

目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。

11.1.1　取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。

11.1.1.1 / 11.1.1.2 / 11.1.1.3 / 11.1.1.4 / 11.1.1.5 / 11.1.1.6 / 11.1.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.2　セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。

11.1.2.1 / 11.1.2.2 / 11.1.2.3 / 11.1.2.4 / 11.1.2.5 / 11.1.2.6 / 11.1.2.7 / 11.1.2.8 / 11.1.2.9 / 11.1.2.10 / 11.1.2.11 / 11.1.2.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.3　オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。

11.1.3.1 / 11.1.3.2 / 11.1.3.3 / 11.1.3.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.4　自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。

11.1.4.1は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.5　セキュリティを保つべき領域での作業に関する手順を設計し、適用する。

11.1.5.1 / 11.1.5.2 / 11.1.5.3 / 11.1.5.4 / 11.1.5.5 / 11.1.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.6　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。

11.1.6.1 / 11.1.6.2 / 11.1.6.3 / 11.1.6.4 / 11.1.6.5 / 11.1.6.6 / 11.1.6.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2　装置

目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。

11.2.1　装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。

11.2.1.1 / 11.2.1.2 / 11.2.1.3 / 11.2.1.4 / 11.2.1.5 / 11.2.1.6 / 11.2.1.7 / 11.2.1.8 / 11.2.1.9 / 11.2.1.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.2　装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。

11.2.2.1 / 11.2.2.2 / 11.2.2.3 / 11.2.2.4 / 11.2.2.5 / 11.2.2.6 / 11.2.2.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.3　データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。

11.2.3.1 / 11.2.3.2 / 11.2.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.4　装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。

11.2.4.1 / 11.2.4.2 / 11.2.4.3 / 11.2.4.4 / 11.2.4.5 / 11.2.4.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.5　装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。

11.2.5.1 / 11.2.5.2 / 11.2.5.3 / 11.2.5.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.6　構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。

11.2.6.1 / 11.2.6.2 / 11.2.6.3 / 11.2.6.4 / 11.2.6.5 / 11.2.6.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.7　記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。

11.2.7.1 / 11.2.7.2 / 11.2.7.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.7.4.P　クラウドサービス提供者は、資源（例えば、装置、データストレージ、ファイル、メモリ）のセキュリティを保った処分又は再利用の取り決めを、時期を失せずに行うことを確実にする仕組みを整備する。

11.2.8　利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。

11.2.8.1 / 11.2.8.2 / 11.2.8.3 / 11.2.8.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.9　書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。*8

11.2.9.1 / 11.2.9.2 / 11.2.9.3 / 11.2.9.4 / 11.2.9.5 / 11.2.9.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12　運用のセキュリティ

12.1　運用の手順及び責任

目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため

12.1.1　操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。

12.1.1.1 / 12.1.1.2 / 12.1.1.3 / 12.1.1.4 / 12.1.1.5 / 12.1.1.6 / 12.1.1.7 / 12.1.1.8 / 12.1.1.9 / 12.1.1.10 / 12.1.1.11 / 12.1.1.12 / 12.1.1.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.2　情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。

12.1.2.1 / 12.1.2.2 / 12.1.2.3 / 12.1.2.4 / 12.1.2.5 / 12.1.2.6 / 12.1.2.7 / 12.1.2.8 / 12.1.2.9 / 12.1.2.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.2.11.P　クラウドサービス提供者は、クラウドサービス利用者の情報セキュリティに悪影響を及ぼす可能性のあるクラウドサービスの変更に関する情報[9]を、クラウド

---

*8　クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。

9　次の事項は、クラウドサービス利用者がその変更がもたらす情報セキュリティにおける影響を特定するのに役立つ。
- 変更の種別
- 変更の予定日時
- クラウドサービス及び基盤システムへの変更の技術的説明
- 変更の開始及び終了の通知

また、クラウドサービス提供者は、ピアクラウドサービス提供者（注）に依存するクラウドサービスを提供しているとき、ピアクラウドサービス提供者に起因する変更をクラウドサービス利用者に通知する必要性が生じる可能性がある。
（注）ピアクラウドサービス提供者：一又は複数の他のクラウドサービス提供者が利用するために、その事業者のクラウドサービスの一環として、一又は複数のクラウドサービスを提供するクラウドサービス提供者（ISO/IEC 17789:2014 3.2.5 peer cloud service provider）

サービス利用者に提供する。

12.1.3　要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。

12.1.3.1 / 12.1.3.2 / 12.1.3.3 / 12.1.3.4 / 12.1.3.5 / 12.1.3.6 / 12.1.3.7 / 12.1.3.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.3.9.P　クラウドサービス提供者は、資源不足による情報セキュリティインシデントを防ぐため、全資源の容量を監視する。

12.1.4　開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離する。

12.1.4.1 / 12.1.4.2 / 12.1.4.3 / 12.1.4.4 / 12.1.4.5 / 12.1.4.6 / 12.1.4.7 / 12.1.4.8 / 12.1.4.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.5.P　クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視する。

12.1.5.1.P　クラウドサービス提供者は、重要な操作及び手順に関する文書を、それを求めるクラウドサービス利用者に提供する。

12.2　マルウェアからの保護

目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。

12.2.1　マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。

12.2.1.1 / 12.2.1.2 / 12.2.1.3 / 12.2.1.4 / 12.2.1.5 / 12.2.1.6 / 12.2.1.7 / 12.2.1.8 / 12.2.1.9 / 12.2.1.10 / 12.2.1.11 / 12.2.1.12 / 12.2.1.13 / 12.2.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.3　バックアップ

目的：データの消失から保護するため

12.3.1　情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。

12.3.1.1 / 12.3.1.2 / 12.3.1.3 / 12.3.1.4 / 12.3.1.5 / 12.3.1.6 / 12.3.1.7 / 12.3.1.8 / 12.3.1.9 / 12.3.1.10 / 12.3.1.11 / 12.3.1.12 / 12.3.1.13 / 12.3.1.14 / 12.3.1.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.3.1.16.P　クラウドサービス提供者は、クラウドサービス利用者にバックアップ機能の仕様を提供する。

12.3.1.17.P　バックアップ機能の仕様には、バックアップ範囲及びスケジュールを含める。

12.3.1.18.P　バックアップ機能の仕様には、関係するならば暗号を含む、バックアップ手法及びデータ書式を含める。

12.3.1.19.P　バックアップ機能の仕様には、バックアップデータ保持期間を含める。

12.3.1.20.P　バックアップ機能の仕様には、バックアップデータの完全性の検証手順を含める。

12.3.1.21.P　バックアップ機能の仕様には、バックアップからのデータの復旧に要する手順

及び時間的尺度を含める。

12.3.1.22.P　バックアップ機能の仕様には、バックアップ機能の試験手順を含める。

12.3.1.23.P　バックアップ機能の仕様には、バックアップの保管場所を含める。

12.3.1.24.P　クラウドサービス提供者は、仮想スナップショットなどのサービスをクラウドサービス利用者に提供する場合には、バックアップへのアクセスは、セキュリティを保ち分離して提供する。

12.4　ログ取得及び監視

目的：イベントを記録し、証拠を作成するため

12.4.1　利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。

12.4.1.1 / 12.4.1.2 / 12.4.1.3 / 12.4.1.4 / 12.4.1.5 / 12.4.1.6 / 12.4.1.7 / 12.4.1.8 / 12.4.1.9 / 12.4.1.10 / 12.4.1.11 / 12.4.1.12 / 12.4.1.13 / 12.4.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.1.15.P　クラウドサービス提供者は、クラウドサービス利用者に、ログ取得機能を提供する。

12.4.2　ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。

12.4.2.1 / 12.4.2.2 / 12.4.2.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.3　システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。

12.4.3.1 / 12.4.3.2 / 12.4.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.4　組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。

12.4.4.1 / 12.4.4.2 / 12.4.4.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.4.4.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス提供者のシステムで利用するクロックに関する情報及びクラウドサービス利用者がクラウドサービスのクロックにローカルクロックを同期させる方法についての情報を提供する。

12.4.5.P　クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有する。

12.4.5.1.P　クラウドサービス提供者は、クラウドサービス利用者に関連するクラウドサービスの操作の特定の側面[10]をクラウドサービス利用者が監視できる機能を提供する。

12.4.5.2.P　監視機能の利用は、適切なアクセス制御によりセキュリティを保つ。

12.4.5.3.P　監視機能は、クラウドサービス利用者自身のクラウドサービスインスタンスについての情報へのアクセスのみを提供する。

12.4.5.4.P　クラウドサービス提供者は、クラウドサービス利用者に、サービス監視機能の文書を提供する。

12.4.5.5.P　監視は、箇条12.4.1に記載したイベントログと整合したデータを提供し、かつ、SLAの条件の実行を補助する。

12.5　運用ソフトウェアの管理

目的：運用システムの完全性を確実にするため。

12.5.1　運用システムに関わるソフトウェアの導入を管理するための手順を実施する。

12.5.1.1 / 12.5.1.2 / 12.5.1.3 / 12.5.1.4 / 12.5.1.5 / 12.5.1.6 / 12.5.1.7 / 12.5.1.8 / 12.5.1.9 / 12.5.1.10 / 12.5.1.11 / 12.5.1.12 / 12.5.1.13 / 12.5.1.14 / 12.5.1.15 / 12.5.1.16 / 12.5.1.17 / 12.5.1.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.6　技術的ぜい弱性管理

目的：技術的ぜい弱性の悪用を防止するため。

12.6.1　利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。

12.6.1.1 / 12.6.1.2 / 12.6.1.3 / 12.6.1.4 / 12.6.1.5 / 12.6.1.6 / 12.6.1.7 / 12.6.1.8 / 12.6.1.9 / 12.6.1.10 / 12.6.1.11 / 12.6.1.12 / 12.6.1.13 / 12.6.1.14 / 12.6.1.15 / 12.6.1.16 / 12.6.1.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.6.1.18.P　クラウドサービス提供者は、提供するクラウドサービスに影響を及ぼす可能性のある技術的ぜい弱性の管理についての情報を、クラウドサービス利用者が利用可能となるようにする。

12.6.2　利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。

12.6.2.1 / 12.6.2.2 / 12.6.2.3 / 12.6.2.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

---

[10] 例えば、クラウドサービスが他者を攻撃する基盤として使われていないか、クラウドサービスから機微なデータが漏洩していないかを監視し、検知する。

12.7　情報システムの監査に対する考慮事項

目的：運用システムに対する監査活動の影響を最小限にするため。

12.7.1　運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。

12.7.1.1 / 12.7.1.2 / 12.7.1.3 / 12.7.1.4 / 12.7.1.5 / 12.7.1.6 / 12.7.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13　通信のセキュリティ

13.1　ネットワークセキュリティ管理

目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。

13.1.1　システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。

13.1.1.1 / 13.1.1.2 / 13.1.1.3 / 13.1.1.4 / 13.1.1.5 / 13.1.1.6 / 13.1.1.7 / 13.1.1.8 / 13.1.1.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.2　組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。

13.1.2.1 / 13.1.2.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.3　情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。

13.1.3.1 / 13.1.3.2 / 13.1.3.3 / 13.1.3.4 / 13.1.3.5 / 13.1.3.6 / 13.1.3.7 / 13.1.3.8 / 13.1.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.3.10.P　クラウドサービス提供者は、マルチテナント環境において、各テナントを分離するため、ネットワークアクセスを分離する。

13.1.3.11.P　クラウドサービス提供者は、クラウドサービス提供者の内部管理環境を、クラウドサービス利用者のクラウドコンピューティング環境から分離するため、ネットワークアクセスを分離する。

13.1.3.12.P　クラウドサービス提供者は、クラウドサービス提供者が実施する分離について、適切な場合にクラウドサービス利用者による検証が行える仕組みを整備する。

13.1.4.P　仮想ネットワークを設定する際には、クラウドサービス提供者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証する。

13.1.4.1.P　クラウドサービス提供者は、物理ネットワークの情報セキュリティ方針と整合の取れた、仮想ネットワークの設定のための情報セキュリティ方針を定め、文書化する。

13.1.4.2.P　クラウドサービス提供者は、設定手段が何であれ、仮想ネットワークの設定が、情報セキュリティ方針に整合することを確実にする仕組みを整備する。

13.2　情報の転送

目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。

13.2.1　あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。

13.2.1.1 / 13.2.1.2 / 13.2.1.3 / 13.2.1.4 / 13.2.1.5 / 13.2.1.6 / 13.2.1.7 / 13.2.1.8 / 13.2.1.9 / 13.2.1.10 / 13.2.1.11 / 13.2.1.12 / 13.2.1.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.2.2　合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。

13.2.2.1 / 13.2.2.2 / 13.2.2.3 / 13.2.2.4 / 13.2.2.5 / 13.2.2.6 / 13.2.2.7 / 13.2.2.8 / 13.2.2.9 / 13.2.2.10 / 13.2.2.11 / 13.2.2.12 / 13.2.2.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.2.3　電子的メッセージ通信に含まれた情報は、適切に保護する。

13.2.3.1 / 13.2.3.2 / 13.2.3.3 / 13.2.3.4 / 13.2.3.5 / 13.2.3.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.2.4　情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化する。

13.2.4.1 / 13.2.4.2 / 13.2.4.3 / 13.2.4.4 / 13.2.4.5 / 13.2.4.6 / 13.2.4.7 / 13.2.4.8 / 13.2.4.9 / 13.2.4.10 / 13.2.4.11 / 13.2.4.12 / 13.2.4.13 / 13.2.4.14 / 13.2.4.15 / 13.2.4.16は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14　システムの取得、開発及び保守

14.1　情報システムのセキュリティ要求事項

目的：ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。

14.1.1　情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。

14.1.1.1 / 14.1.1.2 / 14.1.1.3 / 14.1.1.4 / 14.1.1.5 / 14.1.1.6 / 14.1.1.7 / 14.1.1.8 / 14.1.1.9 / 14.1.1.10 / 14.1.1.11 / 14.1.1.12 / 14.1.1.13 / 14.1.1.14 / 14.1.1.15 / 14.1.1.16 / 14.1.1.17 / 14.1.1.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.1.1.19.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス利用者が利用する情報セキュリティ機能について、情報を提供する。

14.1.1.20.P　クラウドサービス提供者は、クラウドサービス利用者が利用する情報セキュリティ機能についてクラウドサービス利用者に提供する有益な情報が、悪意ある者にとって役立つ情報の開示にならないようにする。

14.1.2　公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。

14.1.2.1 / 14.1.2.2 / 14.1.2.3 / 14.1.2.4 / 14.1.2.5 / 14.1.2.6 / 14.1.2.7 / 14.1.2.8 / 14.1.2.9 / 14.1.2.10 / 14.1.2.11 / 14.1.2.12 / 14.1.2.13 / 14.1.2.14 / 14.1.2.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.1.3　アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。

・不完全な通信

・誤った通信経路設定

・認可されていないメッセージの変更

・認可されていない開示

・認可されていないメッセージの複製又は再生

14.1.3.1 / 14.1.3.2 / 14.1.3.3 / 14.1.3.4 / 14.1.3.5 / 14.1.3.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2　開発及びサポートプロセスにおけるセキュリティ

目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため

14.2.1　ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。

14.2.1.1 / 14.2.1.2 / 14.2.1.3 / 14.2.1.4 / 14.2.1.5 / 14.2.1.6 / 14.2.1.7 / 14.2.1.8 / 14.2.1.9 / 14.2.1.10 / 14.2.1.11 / 14.2.1.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.1.13.P　クラウドサービス提供者は、開示方針に反しない範囲で、セキュリティを保つための開発手順及び慣行についての情報を提供する。

14.2.2　開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。

14.2.2.1 / 14.2.2.2 / 14.2.2.3 / 14.2.2.4 / 14.2.2.5 / 14.2.2.6 / 14.2.2.7 / 14.2.2.8 / 14.2.2.9 / 14.2.2.10 / 14.2.2.11 / 14.2.2.12 / 14.2.2.13 / 14.2.2.14 / 14.2.2.15 / 14.2.2.16 / 14.2.2.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.3　オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。

14.2.3.1 / 14.2.3.2 / 14.2.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.4　パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。

14.2.4.1 / 14.2.4.2 / 14.2.4.3 / 14.2.4.4 / 14.2.4.5 / 14.2.4.6 / 14.2.4.7 / 14.2.4.8 / 14.2.4.9 / 14.2.4.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.5　セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。

14.2.5.1 / 14.2.5.2 / 14.2.5.3 / 14.2.5.4 / 14.2.5.5 / 14.2.5.6 / 14.2.5.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.6　組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。

14.2.6.1 / 14.2.6.2 / 14.2.6.3 / 14.2.6.4 / 14.2.6.5 / 14.2.6.6 / 14.2.6.7 / 14.2.6.8 / 14.2.6.9 / 14.2.6.10 / 14.2.6.11 / 14.2.6.12は、「情報セキュリティ管理基準」の

「管理策基準」に同じ。

14.2.7　組織は、外部委託したシステム開発活動を監督し、監視する。

14.2.7.1 / 14.2.7.2 / 14.2.7.3 / 14.2.7.4 / 14.2.7.5 / 14.2.7.6 / 14.2.7.7 / 14.2.7.8 / 14.2.7.9 / 14.2.7.10 / 14.2.7.11は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.8　セキュリティ機能（functionality）の試験は、開発期間中に実施する。

14.2.8.1 / 14.2.8.2 / 14.2.8.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.9　新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。

14.2.9.1 / 14.2.9.2 / 14.2.9.3 / 14.2.9.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.3　試験データ

目的：試験に用いるデータの保護を確実にするため。

14.3.1　試験データは、注意深く選定し、保護し、管理する。

14.3.1.1 / 14.3.1.2 / 14.3.1.3 / 14.3.1.4 / 14.3.1.5 / 14.3.1.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15　供給者関係

15.1　供給者関係における情報セキュリティ

目的：供給者がアクセスできる組織の資産の保護を確実にするため。

15.1.1　組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。

15.1.1.1 / 15.1.1.2 / 15.1.1.3 / 15.1.1.4 / 15.1.1.5 / 15.1.1.6 / 15.1.1.7 / 15.1.1.8 / 15.1.1.9 / 15.1.1.10 / 15.1.1.11 / 15.1.1.12 / 15.1.1.13 / 15.1.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.1.2　関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのIT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。

15.1.2.1 / 15.1.2.2 / 15.1.2.3 / 15.1.2.4 / 15.1.2.5 / 15.1.2.6 / 15.1.2.7 / 15.1.2.8 / 15.1.2.9 / 15.1.2.10 / 15.1.2.11 / 15.1.2.12 / 15.1.2.13 / 15.1.2.14 / 15.1.2.15 / 15.1.2.16 / 15.1.2.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.1.2.18.P　クラウドサービス提供者は、クラウドサービス提供者とクラウドサービス利用者の間に誤解が生じないように、クラウドサービス提供者が実行する適切な情報セキュリティ対策を、合意の一環として定める。

15.1.3　供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。

15.1.3.1 / 15.1.3.2 / 15.1.3.3 / 15.1.3.4 / 15.1.3.5 / 15.1.3.6 / 15.1.3.7 / 15.1.3.8 / 15.1.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.1.3.10.P　クラウドサービス提供者は、ピアクラウドサービス提供者[11]のクラウドサービスを利用する場合には、自身のクラウドサービス利用者に対する情報セキュリティの水準が維持されるか又は上回ることを確実にする仕組みを整備する。

15.1.3.11.P　クラウドサービス提供者は、サプライチェーンに基づきクラウドサービスを提供する際には、供給者に情報セキュリティの目的を与え、各供給者にその目的を達成するためのリスク管理活動を実施することを要求する。

15.2　供給者のサービス提供の管理

目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。

15.2.1　組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。

15.2.1.1 / 15.2.1.2 / 15.2.1.3 / 15.2.1.4 / 15.2.1.5 / 15.2.1.6 / 15.2.1.7 / 15.2.1.8 / 15.2.1.9 / 15.2.1.10 / 15.2.1.11 / 15.2.1.12 / 15.2.1.13 / 15.2.1.14 / 15.2.1.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.2.2　関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理する。

15.2.2.1 / 15.2.2.2 / 15.2.2.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16　情報セキュリティインシデント管理

16.1　情報セキュリティインシデントの管理及びその改善

目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

16.1.1　情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。

16.1.1.1 / 16.1.1.2 / 16.1.1.3 / 16.1.1.4 / 16.1.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

[11] ピアクラウドサービス提供者：一又は複数の他のクラウドサービス提供者が利用するために、その事業者のクラウドサービスの一環として、一又は複数のクラウドサービスを提供するクラウドサービス提供者（ISO/IEC 17789:2014 3.2.5 peer cloud service provider）

16.1.1.6.P　クラウドサービス提供者は、サービス仕様の一部として、クラウドサービス利用者とクラウドサービス提供者の間の、情報セキュリティインシデント管理の責任の割当て及び手順を定める。

16.1.1.7.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス提供者がクラウドサービス利用者に報告する情報セキュリティインシデントの範囲を含む文書を提供する。

16.1.1.8.P　クラウドサービス提供者は、クラウドサービス利用者に、情報セキュリティインシデントの検知及び関連する対応策の開示レベルを含む文書を提供する。

16.1.1.9.P　クラウドサービス提供者は、クラウドサービス利用者に、情報セキュリティインシデントの発生を通知する目標時間枠を含む文書を提供する。

16.1.1.10.P　クラウドサービス提供者は、クラウドサービス利用者に、情報セキュリティインシデントの通知手順を含む文書を提供する。

16.1.1.11.P　クラウドサービス提供者は、クラウドサービス利用者に、情報セキュリティインシデント関連の問題に対処するための連絡先情報を含む文書を提供する。

16.1.1.12.P　クラウドサービス提供者は、クラウドサービス利用者に、特定の情報セキュリティインシデントが発生した場合に適用可能なあらゆる回復策を含む文書を提供する。

16.1.2　情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。

16.1.2.1 / 16.1.2.2 / 16.1.2.3 / 16.1.2.4 / 16.1.2.5 / 16.1.2.6 / 16.1.2.7 / 16.1.2.8 / 16.1.2.9 / 16.1.2.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.2.11.P　クラウドサービス提供者は、クラウドサービス利用者が、情報セキュリティ事象をクラウドサービス提供者に報告するための仕組みを提供する。

16.1.2.12.P　クラウドサービス提供者は、クラウドサービス提供者が、情報セキュリティ事象をクラウドサービス利用者に報告するための仕組みを提供する。

16.1.2.13.P　クラウドサービス提供者は、クラウドサービス利用者が、報告された情報セキュリティ事象の状況を追跡するための仕組みを提供する。

16.1.3　組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。

16.1.3.1 / 16.1.3.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.4　情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。

16.1.4.1 / 16.1.4.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.5　情報セキュリティインシデントは、文書化した手順に従って対応する。

16.1.5.1 / 16.1.5.2 / 16.1.5.3 / 16.1.5.4 / 16.1.5.5 / 16.1.5.6 / 16.1.5.7 / 16.1.5.8 / 16.1.5.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.6　情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起

こる可能性又はその影響を低減するために用いる。

16.1.6.1 / 16.1.6.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.7　組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。

16.1.7.1 / 16.1.7.2 / 16.1.7.3 / 16.1.7.4 / 16.1.7.5 / 16.1.7.6 / 16.1.7.7 / 16.1.7.8 / 16.1.7.9 / 16.1.7.10 / 16.1.7.11 / 16.1.7.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.7.13.P　クラウドサービス提供者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。

17　事業継続マネジメントにおける情報セキュリティの側面

17.1　情報セキュリティ継続

目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。

17.1.1　組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。

17.1.1.1 / 17.1.1.2 / 17.1.1.3 / 17.1.1.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

17.1.2　組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。

17.1.2.1 / 17.1.2.2 / 17.1.2.3 / 17.1.2.4 / 17.1.2.5 / 17.1.2.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。。

17.1.3　確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。

17.1.3.1 / 17.1.3.2 / 17.1.3.3 / 17.1.3.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

17.2　冗長性

目的：情報処理施設の可用性を確実にするため。

17.2.1　情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。

17.2.1.1 / 17.2.1.2 / 17.2.1.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18　順守

18.1　法的及び契約上の要求事項の順守

目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため

18.1.1　各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。

18.1.1.1 / 18.1.1.2 / 18.1.1.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.1.4.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービスを管

轄する法域を通知する。

18.1.1.5.P　クラウドサービス提供者は、自身の関連する法的要求事項（例えば、個人を特定できる情報（PII)を保護するための暗号に関するもの）を特定する。

18.1.1.6.P　クラウドサービス提供者は、自身の関連する法的要求事項を特定した情報を、要求するクラウドサービス利用者に提供する。

18.1.1.7.P　クラウドサービス提供者は、クラウドサービス利用者に、適用法令及び契約上の要求事項を現時点で順守していることの証拠を提供する。

18.1.2　知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。

18.1.2.1 / 18.1.2.2 / 18.1.2.3 / 18.1.2.4 / 18.1.2.5 / 18.1.2.6 / 18.1.2.7 / 18.1.2.8 / 18.1.2.9 / 18.1.2.10 / 18.1.2.11 / 18.1.2.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.2.13.P　クラウドサービス提供者は、知的財産権の順守に対応するためのプロセスを確立する。

18.1.3　記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。

18.1.3.1 / 18.1.3.2 / 18.1.3.3 / 18.1.3.4 / 18.1.3.5 / 18.1.3.6 / 18.1.3.7 / 18.1.3.8 / 18.1.3.9 / 18.1.3.10 / 18.1.3.11 / 18.1.3.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.3.13.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービスの利用に関して、クラウドサービス提供者が収集し、蓄積する記録の保護について、情報を提供する。

18.1.4　プライバシー及びPIIの保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。

18.1.4.1 / 18.1.4.2 / 18.1.4.3 / 18.1.4.4 / 18.1.4.5 / 18.1.4.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.5　暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。

18.1.5.1 / 18.1.5.2 / 18.1.5.3 / 18.1.5.4 / 18.1.5.5 / 18.1.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.5.7.P　クラウドサービス提供者は、クラウドサービス利用者に、適用する協定、法令及び規則を順守していることをレビューするため、クラウドサービス提供者が実装した暗号化機能の記載を、提供する。

18.2　情報セキュリティのレビュー

目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

18.2.1　情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。

18.2.1.1 / 18.2.1.2 / 18.2.1.3 / 18.2.1.4 / 18.2.1.5 / 18.2.1.6 / 18.2.1.7 / 18.2.1.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.2.1.9.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス提供者が主張する情報セキュリティ管理策の実施を立証するための、文書化した証拠を提供する。

18.2.1.10.P　個別のクラウドサービス利用者の監査が実用的でない又は情報セキュリティのリスクを増加させる可能性のある場合には、クラウドサービス提供者は、情報セキュリティがクラウドサービス提供者の方針及び手続に従って実装及び運用されているという、独立した証拠を提供する。

18.2.1.11.P　クラウドサービス提供者は、情報セキュリティがクラウドサービス提供者の方針及び手続に従って実装及び運用されているという、独立した証拠を、クラウドサービス利用者となる見込みのある者が、契約に先立って入手できるようにする。

18.2.1.12.P　クラウドサービス提供者が選択する適切な独立した監査は、十分な透明性が提供されることを条件に、クラウドサービス提供者の運用に対するレビューへのクラウドサービス利用者の関心を満たすための、通常受入れ可能な手段とする。

18.2.1.13.P　独立した監査が実用的でない場合は、クラウドサービス提供者は、自己評価を実施し、クラウドサービス利用者に、そのプロセス及び結果を開示する。

18.2.2　管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。

18.2.2.1 / 18.2.2.2 / 18.2.2.3 / 18.2.2.4 / 18.2.2.5 / 18.2.2.6 / 18.2.2.7 / 18.2.2.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.2.3　情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューする。

18.2.3.1 / 18.2.3.2 / 18.2.3.3 / 18.2.3.4 / 18.2.3.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

クラウド情報セキュリティ基本言明要件

VI. クラウド情報セキュリティ基本言明要件

ガバナンス基準

「クラウド情報セキュリティ管理基準」の「ガバナンス基準」に同じ。

既に記載している通り、原則としてすべて実施しなければならない。

マネジメント基準

「クラウド情報セキュリティ管理基準」の「マネジメント基準」に同じ。

既に記載している通り、原則としてすべて実施しなければならない。

管理策基準

既に記載している通り、「管理策基準」は、「クラウド情報セキュリティ管理基準」の「管理策基準」から基本リスクに対応する項目を抽出している。項番は「クラウド情報セキュリティ管理基準」と同じ項番を使用しているため、抜けている項番は「クラウド情報セキュリティ管理基準」と「クラウド情報セキュリティ基本言明要件」との差分を示す。

詳細管理策[X.X.X.X]については、管理策を実装するために組織・環境・技術等に応じて必要とする事項を選択する。詳細管理策番号の末尾にBが付されたものについては、管理策を実装するための単なる選択肢ではなく、それ自体が基本言明要件であることを示す。

詳細管理策番号の末尾の「P」及び「PB」は、クラウドサービスにおける、クラウドサービス提供者向け管理策であることを示す。

5 情報セキュリティのための方針群

5.1 情報セキュリティのための経営陣の方向性

目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。

5.1.1 情報セキュリティのための方針群は、これを定義し、管理層[*12]が承認し、発行し、従業員及び関連する外部関係者に通知する。

5.1.1.1 / 5.1.1.2 / 5.1.1.3 / 5.1.1.4 / 5.1.1.5 / 5.1.1.6 / 5.1.1.7 / 5.1.1.8 / 5.1.1.9 / 5.1.1.10 / 5.1.1.11 / 5.1.1.12 / 5.1.1.13 / 5.1.1.14 / 5.1.1.15 / 5.1.1.16 / 5.1.1.17 / 5.1.1.18 / 5.1.1.19 / 5.1.1.20 / 5.1.1.21は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

5.1.1.22.P クラウドサービス提供者は、クラウドサービスの設計及び実装に適用可能な基本的な情報セキュリティ要求事項を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.23.P クラウドサービス提供者は、認可された内部関係者からのリスクを考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.24.P クラウドサービス提供者は、マルチテナント及びクラウドサービス利用者の隔離（仮想化を含む）を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.25.P クラウドサービス提供者は、クラウドサービス提供者の職員によるクラウドサービス利用者の資産へのアクセスを考慮し、クラウドサービスの提供及び利用に言

*12 管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。

及して情報セキュリティ方針を拡大する。

5.1.1.26.P　クラウドサービス提供者は、例えばクラウドサービスへの管理上のアクセスのための強固な認証などのアクセス制御手順を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.27.P　クラウドサービス提供者は、変更管理中のクラウドサービス利用者への通知を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.28.P　クラウドサービス提供者は、仮想化セキュリティを考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.29.P　クラウドサービス提供者は、クラウドサービス利用者のデータへのアクセス及び保護を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.30.P　クラウドサービス提供者は、クラウドサービス利用者のアカウントのライフサイクル管理を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

5.1.1.31.P　クラウドサービス提供者は、調査及びフォレンジックを支援するための、違反の通知及び情報共有の指針を考慮し、クラウドサービスの提供及び利用に言及して情報セキュリティ方針を拡大する。

6　情報セキュリティのための組織

6.1　内部組織

目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

6.1.1　全ての情報セキュリティの責任を定め、割り当てる。

6.1.1.1 / 6.1.1.2 / 6.1.1.3 / 6.1.1.4 / 6.1.1.5 / 6.1.1.6 / 6.1.1.7 / 6.1.1.8 / 6.1.1.9 / 6.1.1.10 / 6.1.1.11 / 6.1.1.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.1.13.PB　クラウドサービス提供者は、クラウドサービス利用者、クラウドサービス提供者及び供給者と情報セキュリティの役割及び責任の適切な割当てについて合意し、文書化する。

6.1.2　相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。

6.1.2.1 / 6.1.2.2 / 6.1.2.3 / 6.1.2.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.3　関係当局との適切な連絡体制を維持する。

6.1.3.1 / 6.1.3.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.3.3.PB　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス提供者の組織の地理的所在地、及びクラウドサービス提供者がクラウドサービス利用者のデータを保管する可能性のある国々を通知する。

6.2　モバイル機器及びテレワーキング

目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

6.2.1　モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。

6.2.1.1 / 6.2.1.2 / 6.2.1.3 / 6.2.1.4 / 6.2.1.5 / 6.2.1.6 / 6.2.1.7 / 6.2.1.8 / 6.2.1.9 / 6.2.1.10 / 6.2.1.11 / 6.2.1.12 / 6.2.1.13 / 6.2.1.14 / 6.2.1.15 / 6.2.1.16 / 6.2.1.17 / 6.2.1.18 / 6.2.1.19 / 6.2.1.20 / 6.2.1.21 / 6.2.1.22は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.3.P　クラウドサービス利用者及びクラウドサービス提供者の関係

目的：情報セキュリティマネジメントのための、クラウドサービス利用者及びクラウドサービス提供者間の共同責任の関係を説明するため。

6.3.1.P　クラウドサービス利用者及びクラウドサービス提供者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装する。

6.3.1.1.PB　クラウドサービス提供者は、クラウドサービス利用の一環としてクラウドサービス利用者が実施及び管理を必要とする情報セキュリティの役割と責任に加え、クラウドサービスの利用に対する、クラウドサービス提供者の情報セキュリティ管理策及び責任を文書化し、通知する。

7　人的資源のセキュリティ

7.1　雇用前

目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。

7.1.1　全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。

7.1.1.1 / 7.1.1.2 / 7.1.1.3 / 7.1.1.4 / 7.1.1.5 / 7.1.1.6 / 7.1.1.7 / 7.1.1.8 / 7.1.1.9 / 7.1.1.10 / 7.1.1.11 / 7.1.1.12 / 7.1.1.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.2　雇用期間中

目的：従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。

7.2.2　組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。

7.2.2.1 / 7.2.2.2 / 7.2.2.3 / 7.2.2.4 / 7.2.2.5 / 7.2.2.6 / 7.2.2.7 / 7.2.2.8 / 7.2.2.9 / 7.2.2.10 / 7.2.2.11 / 7.2.2.12 / 7.2.2.13 / 7.2.2.14 / 7.2.2.15 / 7.2.2.16 / 7.2.2.17 / 7.2.2.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.2.2.19.PB　クラウドサービス提供者は、クラウドサービス利用者のデータ及びクラウドサービスの派生データ[13]の適切な取扱いに関して、従業員に意識向上のための教育及び訓練を提供し、かつ同じことをするよう契約相手に要請する。

8　資産の管理

8.1　資産に対する責任

目的：組織の資産を特定し、適切な保護の責任を定めるため。

8.1.1　情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。

8.1.1.1 / 8.1.1.2 / 8.1.1.3 / 8.1.1.4 / 8.1.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.1.6.PB　クラウドサービス提供者の資産目録は、クラウドサービス利用者のデータ及びクラウドサービスの派生データを明確に特定する。

8.1.4　全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。

8.1.4.1 / 8.1.4.2 / 8.1.4.3 / 8.1.4.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.5.P　クラウドサービス提供者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時期を失せずに返却または除去する。

8.1.5.1.P　クラウドサービス提供者は、クラウドサービス利用の合意の終了時における、クラウドサービス利用者の全ての資産の返却及び除去の取決めについて、情報を提供する。

8.1.5.2.P　クラウドサービス提供者は、資産の返却及び除去についての取決めにおいては、合意して文書化し、時期を失せずに実施する。

8.1.5.3.P　クラウドサービス提供者は、取決めにおいて返却及び除去する資産を特定する。

8.2　情報分類

目的：組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

8.2.2　情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施する。

8.2.2.1 / 8.2.2.2 / 8.2.2.3 / 8.2.2.4 / 8.2.2.5 / 8.2.2.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.2.2.7.PB　クラウドサービス提供者は、クラウドサービス利用者が情報及び関連資産を分類し、ラベル付けするためのサービス機能を文書化し、開示する。

8.3　媒体の取扱い

目的：媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。

8.3.2　媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。

8.3.2.1 / 8.3.2.2 / 8.3.2.3 / 8.3.2.4 / 8.3.2.5 / 8.3.2.6 / 8.3.2.7 / 8.3.2.8は、

---

[13] このデータは、クラウドサービス利用者に秘密の情報を含む可能性がある、又はクラウドサービス提供者によるアクセス及び利用において、規制による制限を含む特別な制限が科される可能性がある。

「情報セキュリティ管理基準」の「管理策基準」に同じ。

9　アクセス制御

9.1　アクセス制御に対する業務上の要求事項

目的：情報及び情報処理施設へのアクセスを制限するため。

9.1.1　アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。

9.1.1.1 / 9.1.1.2 / 9.1.1.3 / 9.1.1.4 / 9.1.1.5 / 9.1.1.6 / 9.1.1.7 / 9.1.1.8 / 9.1.1.9 / 9.1.1.10 / 9.1.1.11 / 9.1.1.12 / 9.1.1.13 / 9.1.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.1.2　利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。

9.1.2.1 / 9.1.2.2 / 9.1.2.3 / 9.1.2.4 / 9.1.2.5 / 9.1.2.6 / 9.1.2.7 / 9.1.2.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2　利用者アクセスの管理

目的：システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。

9.2.1　アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施する。

9.2.1.1 / 9.2.1.2 / 9.2.1.3 / 9.2.1.4 / 9.2.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.1.6.PB　クラウドサービスのユーザによるクラウドサービスへのアクセスをクラウドサービス利用者が管理するため、クラウドサービス提供者は、クラウドサービス利用者に、ユーザの登録及び登録削除の機能及び仕様を提供する。

9.2.2　全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。

9.2.2.1 / 9.2.2.2 / 9.2.2.3 / 9.2.2.4 / 9.2.2.5 / 9.2.2.6 / 9.2.2.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.2.8.PB　クラウドサービス提供者は、クラウドサービスのユーザのアクセス権を管理する機能及び仕様を提供する。

9.2.3　特権的アクセス権の割当て及び利用は、制限し、管理する。

9.2.3.1 / 9.2.3.2 / 9.2.3.3 / 9.2.3.4 / 9.2.3.5 / 9.2.3.6 / 9.2.3.7 / 9.2.3.8 / 9.2.3.9 / 9.2.3.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.3.11.PB　クラウドサービス提供者は、特定したリスクに応じて、クラウドサービスの管理能力にあわせたクラウドサービス利用者の管理者認証に、十分に強固な認証技術[14]を提供する。

9.2.4　秘密認証情報の割当ては、正式な管理プロセスによって管理する。

9.2.4.1 / 9.2.4.2 / 9.2.4.3 / 9.2.4.4 / 9.2.4.5 / 9.2.4.6 / 9.2.4.7 / 9.2.4.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.4.9.PB　クラウドサービス提供者は、秘密認証情報を割り当てる手順、及びユーザ認証手順を含む、クラウドサービス利用者の秘密認証情報の管理手順について、情報を提供する。

9.2.5　資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。

9.2.5.1 / 9.2.5.2 / 9.2.5.3 / 9.2.5.4 / 9.2.5.5 / 9.2.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.6　全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。

9.2.6.1 / 9.2.6.2 / 9.2.6.3 / 9.2.6.4 / 9.2.6.5 / 9.2.6.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.3　利用者の責任

目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。

9.3.1　秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。

9.3.1.1 / 9.3.1.2 / 9.3.1.3 / 9.3.1.4 / 9.3.1.5 / 9.3.1.6 / 9.3.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4　システム及びアプリケーションのアクセス制御

目的：システム及びアプリケーションへの、認可されていないアクセスを防止するため

9.4.1　情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。

9.4.1.1 / 9.4.1.2 / 9.4.1.3 / 9.4.1.4 / 9.4.1.5 / 9.4.1.6 / 9.4.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.1.8.PB　クラウドサービス提供者は、クラウドサービスへのアクセス、クラウドサービス機能へのアクセス、及びサービスにて保持されるクラウドサービス利用者のデータへのアクセスを、クラウドサービス利用者が制限できるよう、アクセス制御を提供する。

9.4.2　アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。

9.4.2.1 / 9.4.2.2 / 9.4.2.3 / 9.4.2.4 / 9.4.2.5 / 9.4.2.6 / 9.4.2.7 / 9.4.2.8 / 9.4.2.9 / 9.4.2.10 / 9.4.2.11 / 9.4.2.12 / 9.4.2.13 / 9.4.2.14 / 9.4.2.15 / 9.4.2.16は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

---

[14] 例えば、クラウドサービス提供者は多要素認証機能を提供し、又はサードパーティの多要素認証の仕組みを利用可能にすることができる。

9.4.2.2B　強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いる。

9.4.3　パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。

9.4.3.1 / 9.4.3.2 / 9.4.3.3 / 9.4.3.4 / 9.4.3.5 / 9.4.3.6 / 9.4.3.7 / 9.4.3.8 / 9.4.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.4　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。

9.4.4.1 / 9.4.4.2 / 9.4.4.3 / 9.4.4.4 / 9.4.4.5 / 9.4.4.6 / 9.4.4.7 / 9.4.4.8 / 9.4.4.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.4.10.P　クラウドサービス提供者は、クラウドサービス内で利用する全てのユーティリティプログラムのための要求事項を特定する。

9.4.4.11.P　クラウドサービス提供者は、通常の操作手順又はセキュリティ手順を回避することのできる全てのプログラムは、認可された要員に厳重に制限し、そのようなプログラムの利用は、定期的にレビューし、監査する。

9.4.5　プログラムソースコードへのアクセスは、制限する。

9.4.5.1 / 9.4.5.2 / 9.4.5.3 / 9.4.5.4 / 9.4.5.5 / 9.4.5.6 / 9.4.5.7 / 9.4.5.8 / 9.4.5.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.5.P　共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御

目的：共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。

9.5.1.P　クラウドサービス利用者のクラウドサービス上の仮想環境は、他のクラウドサービス利用者及び認可されていない者から保護する。

9.5.1.1.P　クラウドサービス提供者は、マルチテナント環境におけるクラウドサービス利用者の使用する資源を分離するため、仮想化されたアプリケーション、オペレーティングシステム、ストレージ及びネットワークの適切な論理的分離を実施する。

9.5.1.2.P　クラウドサービス提供者は、クラウドサービス利用者の使用する資源からのクラウドサービス提供者の内部管理を分離するため、仮想化されたアプリケーション、オペレーティングシステム、ストレージ及びネットワークの適切な論理的分離を実施する。

9.5.1.3.P　クラウドサービスがマルチテナントである場合には、クラウドサービス提供者は、異なるテナントが使用する資源を適切に分離するための情報セキュリティ管理策を実施する。

9.5.1.4.P　クラウドサービス提供者は、クラウドサービス提供者が提供するクラウドサービスの内部において、クラウドサービス利用者の所有するソフトウェアの実行が関係するリスク対応を検討する。

9.5.2.P　クラウドコンピューティング環境における仮想マシンは、事業上のニーズを満たすため、要塞化する。

9.5.2.1.PB　クラウドサービス提供者は、仮想マシンを設定する際には、適切に要塞化し(例

えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする）、利用する各仮想マシンに適切な技術的管理策（例えば、マルウェア対策、ログ取得）を実施する。

10　暗号

10.1　暗号による管理策

目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。

10.1.1　情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。

10.1.1.1 / 10.1.1.2 / 10.1.1.3 / 10.1.1.4 / 10.1.1.5 / 10.1.1.6 / 10.1.1.7 / 10.1.1.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

10.1.1.9.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス利用者が処理する情報を保護するために暗号技術を利用する環境について、情報を提供する。

10.1.1.10.P　クラウドサービス提供者は、クラウドサービス利用者が独自の暗号による保護を適用することを支援するための機能について、クラウドサービス利用者に情報を提供する。

11　物理的及び環境的セキュリティ

11.1　セキュリティを保つべき領域

目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。

11.1.1　取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。

11.1.1.1 / 11.1.1.2 / 11.1.1.3 / 11.1.1.4 / 11.1.1.5 / 11.1.1.6 / 11.1.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.2　セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。

11.1.2.1 / 11.1.2.2 / 11.1.2.3 / 11.1.2.4 / 11.1.2.5 / 11.1.2.6 / 11.1.2.7 / 11.1.2.8 / 11.1.2.9 / 11.1.2.10 / 11.1.2.11 / 11.1.2.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.3　オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。

11.1.3.1 / 11.1.3.2 / 11.1.3.3 / 11.1.3.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.4　自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。

11.1.4.1は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.5　セキュリティを保つべき領域での作業に関する手順を設計し、適用する。

11.1.5.1 / 11.1.5.2 / 11.1.5.3 / 11.1.5.4 / 11.1.5.5 / 11.1.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.6　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所

を情報処理施設から離す。

11.1.6.1 / 11.1.6.2 / 11.1.6.3 / 11.1.6.4 / 11.1.6.5 / 11.1.6.6 / 11.1.6.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2 装置

目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。

11.2.1 装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。

11.2.1.1 / 11.2.1.2 / 11.2.1.3 / 11.2.1.4 / 11.2.1.5 / 11.2.1.6 / 11.2.1.7 / 11.2.1.8 / 11.2.1.9 / 11.2.1.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.2 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。

11.2.2.1 / 11.2.2.2 / 11.2.2.3 / 11.2.2.4 / 11.2.2.5 / 11.2.2.6 / 11.2.2.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.3 データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。

11.2.3.1 / 11.2.3.2 / 11.2.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.4 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。

11.2.4.1 / 11.2.4.2 / 11.2.4.3 / 11.2.4.4 / 11.2.4.5 / 11.2.4.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.5 装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。

11.2.5.1 / 11.2.5.2 / 11.2.5.3 / 11.2.5.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.6 構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。

11.2.6.1 / 11.2.6.2 / 11.2.6.3 / 11.2.6.4 / 11.2.6.5 / 11.2.6.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.7 記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。

11.2.7.1 / 11.2.7.2 / 11.2.7.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.7.4.PB クラウドサービス提供者は、資源（例えば、装置、データストレージ、ファイル、メモリ）のセキュリティを保った処分又は再利用の取り決めを、時期を失せずに行うことを確実にする仕組みを整備する。

11.2.8 利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。

11.2.8.1 / 11.2.8.2 / 11.2.8.3 / 11.2.8.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.9 書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するク

リアスクリーン方針を適用する。*15

11.2.9.1 / 11.2.9.2 / 11.2.9.3 / 11.2.9.4 / 11.2.9.5 / 11.2.9.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12 運用のセキュリティ

12.1 運用の手順及び責任

目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため。

12.1.1 操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。

12.1.1.1 / 12.1.1.2 / 12.1.1.3 / 12.1.1.4 / 12.1.1.5 / 12.1.1.6 / 12.1.1.7 / 12.1.1.8 / 12.1.1.9 / 12.1.1.10 / 12.1.1.11 / 12.1.1.12 / 12.1.1.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.2 情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。

12.1.2.1 / 12.1.2.2 / 12.1.2.3 / 12.1.2.4 / 12.1.2.5 / 12.1.2.6 / 12.1.2.7 / 12.1.2.8 / 12.1.2.9 / 12.1.2.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.2.11.PB クラウドサービス提供者は、クラウドサービス利用者の情報セキュリティに悪影響を及ぼす可能性のあるクラウドサービスの変更に関する情報[16]を、クラウドサービス利用者に提供する。

12.1.3 要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。

12.1.3.1 / 12.1.3.2 / 12.1.3.3 / 12.1.3.4 / 12.1.3.5 / 12.1.3.6 / 12.1.3.7 / 12.1.3.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.3.9.PB クラウドサービス提供者は、資源不足による情報セキュリティインシデントを防ぐため、全資源の容量を監視する。

12.1.5.P クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視する。

12.1.5.1.PB クラウドサービス提供者は、重要な操作及び手順に関する文書を、それを求めるクラウドサービス利用者に提供する。

12.2 マルウェアからの保護

目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。

---

*15 クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。

16 次の事項は、クラウドサービス利用者がその変更がもたらす情報セキュリティにおける影響を特定するのに役立つ。
- 変更の種別
- 変更の予定日時
- クラウドサービス及び基盤システムへの変更の技術的説明
- 変更の開始及び終了の通知

また、クラウドサービス提供者は、ピアクラウドサービス提供者（注）に依存するクラウドサービスを提供しているとき、ピアクラウドサービス提供者に起因する変更をクラウドサービス利用者に通知する必要性が生じる可能性がある。
（注）ピアクラウドサービス提供者：一又は複数の他のクラウドサービス提供者が利用するために、その事業者のクラウドサービスの一環として、一又は複数のクラウドサービスを提供するクラウドサービス提供者（ISO/IEC 17789:2014 3.2.5 peer cloud service provider）

12.2.1　マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。

12.2.1.1 / 12.2.1.2 / 12.2.1.3 / 12.2.1.4 / 12.2.1.5 / 12.2.1.6 / 12.2.1.7 / 12.2.1.8 / 12.2.1.9 / 12.2.1.10 / 12.2.1.11 / 12.2.1.12 / 12.2.1.13 / 12.2.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.3　バックアップ

目的：データの消失から保護するため。

12.3.1　情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。

12.3.1.1 / 12.3.1.2 / 12.3.1.3 / 12.3.1.4 / 12.3.1.5 / 12.3.1.6 / 12.3.1.7 / 12.3.1.8 / 12.3.1.9 / 12.3.1.10 / 12.3.1.11 / 12.3.1.12 / 12.3.1.13 / 12.3.1.14 / 12.3.1.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.3.1.16.P　クラウドサービス提供者は、クラウドサービス利用者にバックアップ機能の仕様を提供する。

12.3.1.17.P　バックアップ機能の仕様には、バックアップ範囲及びスケジュールを含める。

12.3.1.18.P　バックアップ機能の仕様には、関係するならば暗号を含む、バックアップ手法及びデータ書式を含める。

12.3.1.19.P　バックアップ機能の仕様には、バックアップデータ保持期間を含める。

12.3.1.20.P　バックアップ機能の仕様には、バックアップデータの完全性の検証手順を含める。

12.3.1.21.P　バックアップ機能の仕様には、バックアップからのデータの復旧に要する手順及び時間的尺度を含める。

12.3.1.22.P　バックアップ機能の仕様には、バックアップ機能の試験手順を含める。

12.3.1.23.P　バックアップ機能の仕様には、バックアップの保管場所を含める。

12.3.1.24.P　クラウドサービス提供者は、仮想スナップショットなどのサービスをクラウドサービス利用者に提供する場合には、バックアップへのアクセスは、セキュリティを保ち分離して提供する。

12.4　ログ取得及び監視

目的：イベントを記録し、証拠を作成するため。

12.4.1　利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。

12.4.1.1 / 12.4.1.2 / 12.4.1.3 / 12.4.1.4 / 12.4.1.5 / 12.4.1.6 / 12.4.1.7 / 12.4.1.8 / 12.4.1.9 / 12.4.1.10 / 12.4.1.11 / 12.4.1.12 / 12.4.1.13 / 12.4.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.1.15.PB　クラウドサービス提供者は、クラウドサービス利用者に、ログ取得機能を提供する。

12.4.2　ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。

12.4.2.1 / 12.4.2.2 / 12.4.2.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.3　システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。

12.4.3.1 / 12.4.3.2 / 12.4.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.4　組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。

12.4.4.1 / 12.4.4.2 / 12.4.4.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.4.4.PB　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス提供者のシステムで利用するクロックに関する情報及びクラウドサービス利用者がクラウドサービスのクロックにローカルクロックを同期させる方法についての情報を提供する。

12.4.5.P　クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有する。

12.4.5.1.P　クラウドサービス提供者は、クラウドサービス利用者に関連するクラウドサービスの操作の特定の側面[17]をクラウドサービス利用者が監視できる機能を提供する。

12.4.5.2.P　監視機能の利用は、適切なアクセス制御によりセキュリティを保つ。

12.4.5.3.P　監視機能は、クラウドサービス利用者自身のクラウドサービスインスタンスについての情報へのアクセスのみを提供する。

12.4.5.4.P　クラウドサービス提供者は、クラウドサービス利用者に、サービス監視機能の文書を提供する。

12.4.5.5.P　監視は、箇条12.4.1に記載したイベントログと整合したデータを提供し、かつ、SLAの条件の実行を補助する。

12.5　運用ソフトウェアの管理

目的：運用システムの完全性を確実にするため。

12.5.1　運用システムに関わるソフトウェアの導入を管理するための手順を実施する。

12.5.1.1 / 12.5.1.2 / 12.5.1.3 / 12.5.1.4 / 12.5.1.5 / 12.5.1.6 / 12.5.1.7 / 12.5.1.8 / 12.5.1.9 / 12.5.1.10 / 12.5.1.11 / 12.5.1.12 / 12.5.1.13 / 12.5.1.14 / 12.5.1.15 / 12.5.1.16 / 12.5.1.17 / 12.5.1.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.6　技術的ぜい弱性管理

目的：技術的ぜい弱性の悪用を防止するため。

12.6.1　利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。

12.6.1.1 / 12.6.1.2 / 12.6.1.3 / 12.6.1.4 / 12.6.1.5 / 12.6.1.6 / 12.6.1.7 / 12.6.1.8 / 12.6.1.9 / 12.6.1.10 / 12.6.1.11 / 12.6.1.12 / 12.6.1.13 / 12.6.1.14 / 12.6.1.15

[17] 例えば、クラウドサービスが他者を攻撃する基盤として使われていないか、クラウドサービスから機微なデータが漏洩していないかを監視し、検知する。

/ 12.6.1.16 / 12.6.1.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.6.1.18.PB　クラウドサービス提供者は、提供するクラウドサービスに影響を及ぼす可能性のある技術的ぜい弱性の管理についての情報を、クラウドサービス利用者が利用可能となるようにする。

13　通信のセキュリティ

13.1　ネットワークセキュリティ管理

目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。

13.1.1　システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御する。

13.1.1.1 / 13.1.1.2 / 13.1.1.3 / 13.1.1.4 / 13.1.1.5 / 13.1.1.6 / 13.1.1.7 / 13.1.1.8 / 13.1.1.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.2　組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。

13.1.2.1 / 13.1.2.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.3　情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。

13.1.3.1 / 13.1.3.2 / 13.1.3.3 / 13.1.3.4 / 13.1.3.5 / 13.1.3.6 / 13.1.3.7 / 13.1.3.8 / 13.1.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.3.10.P　クラウドサービス提供者は、マルチテナント環境において、各テナントを分離するため、ネットワークアクセスを分離する。

13.1.3.11.P　クラウドサービス提供者は、クラウドサービス提供者の内部管理環境を、クラウドサービス利用者のクラウドコンピューティング環境から分離するため、ネットワークアクセスを分離する。

13.1.3.12.P　クラウドサービス提供者は、クラウドサービス提供者が実施する分離について、適切な場合にクラウドサービス利用者による検証が行える仕組みを整備する。

13.1.4.P　仮想ネットワークを設定する際には、クラウドサービス提供者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証する。

13.1.4.1.P　クラウドサービス提供者は、物理ネットワークの情報セキュリティ方針と整合の取れた、仮想ネットワークの設定のための情報セキュリティ方針を定め、文書化する。

13.1.4.2.P　クラウドサービス提供者は、設定手段が何であれ、仮想ネットワークの設定が、情報セキュリティ方針に整合することを確実にする仕組みを整備する。

13.2　情報の転送

目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。

13.2.1　あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。

13.2.1.1 / 13.2.1.2 / 13.2.1.3 / 13.2.1.4 / 13.2.1.5 / 13.2.1.6 / 13.2.1.7 / 13.2.1.8 / 13.2.1.9 / 13.2.1.10 / 13.2.1.11 / 13.2.1.12 / 13.2.1.13は、「情報セキュリティ管

理基準」の「管理策基準」に同じ。

13.2.3　電子的メッセージ通信に含まれた情報は、適切に保護する。

13.2.3.1 / 13.2.3.2 / 13.2.3.3 / 13.2.3.4 / 13.2.3.5 / 13.2.3.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14　システムの取得、開発及び保守

14.1　情報システムのセキュリティ要求事項

目的：ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む

14.1.1　情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。

14.1.1.1 / 14.1.1.2 / 14.1.1.3 / 14.1.1.4 / 14.1.1.5 / 14.1.1.6 / 14.1.1.7 / 14.1.1.8 / 14.1.1.9 / 14.1.1.10 / 14.1.1.11 / 14.1.1.12 / 14.1.1.13 / 14.1.1.14 / 14.1.1.15 / 14.1.1.16 / 14.1.1.17 / 14.1.1.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.1.1.19.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス利用者が利用する情報セキュリティ機能について、情報を提供する。

14.1.1.20.P　クラウドサービス提供者は、クラウドサービス利用者が利用する情報セキュリティ機能についてクラウドサービス利用者に提供する有益な情報が、悪意ある者にとって役立つ情報の開示にならないようにする。

14.1.2　公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。

14.1.2.1 / 14.1.2.2 / 14.1.2.3 / 14.1.2.4 / 14.1.2.5 / 14.1.2.6 / 14.1.2.7 / 14.1.2.8 / 14.1.2.9 / 14.1.2.10 / 14.1.2.11 / 14.1.2.12 / 14.1.2.13 / 14.1.2.14 / 14.1.2.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.1.3　アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。

- 不完全な通信
- 誤った通信経路設定
- 認可されていないメッセージの変更
- 認可されていない開示
- 認可されていないメッセージの複製又は再生

14.1.3.1 / 14.1.3.2 / 14.1.3.3 / 14.1.3.4 / 14.1.3.5 / 14.1.3.6 は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2　開発及びサポートプロセスにおけるセキュリティ

目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため。

14.2.1　ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。

14.2.1.1 / 14.2.1.2 / 14.2.1.3 / 14.2.1.4 / 14.2.1.5 / 14.2.1.6 / 14.2.1.7 / 14.2.1.8 / 14.2.1.9 / 14.2.1.10 / 14.2.1.11 / 14.2.1.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.1.13.PB　クラウドサービス提供者は、開示方針に反しない範囲で、セキュリティを保つための開発手順及び慣行についての情報を提供する。

14.2.2　開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。

14.2.2.1 / 14.2.2.2 / 14.2.2.3 / 14.2.2.4 / 14.2.2.5 / 14.2.2.6 / 14.2.2.7 / 14.2.2.8 / 14.2.2.9 / 14.2.2.10 / 14.2.2.11 / 14.2.2.12 / 14.2.2.13 / 14.2.2.14 / 14.2.2.15 / 14.2.2.16 / 14.2.2.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.3　オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。

14.2.3.1 / 14.2.3.2 / 14.2.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.9　新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。

14.2.9.1 / 14.2.9.2 / 14.2.9.3 / 14.2.9.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15　供給者関係

15.1　供給者関係における情報セキュリティ

目的：供給者がアクセスできる組織の資産の保護を確実にするため。

15.1.1　組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。

15.1.1.1 / 15.1.1.2 / 15.1.1.3 / 15.1.1.4 / 15.1.1.5 / 15.1.1.6 / 15.1.1.7 / 15.1.1.8 / 15.1.1.9 / 15.1.1.10 / 15.1.1.11 / 15.1.1.12 / 15.1.1.13 / 15.1.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.1.1.14B　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報、情報処理施設及び移動が必要なその他のものの移行の管理、並びにその移行期間全体にわたって情報セキュリティが維持されることの確実化を含める。

15.1.2　関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのIT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。

15.1.2.1 / 15.1.2.2 / 15.1.2.3 / 15.1.2.4 / 15.1.2.5 / 15.1.2.6 / 15.1.2.7 / 15.1.2.8 / 15.1.2.9 / 15.1.2.10 / 15.1.2.11 / 15.1.2.12 / 15.1.2.13 / 15.1.2.14 / 15.1.2.15 / 15.1.2.16 / 15.1.2.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.1.2.18.PB　クラウドサービス提供者は、クラウドサービス提供者とクラウドサービス利用者の間に誤解が生じないように、クラウドサービス提供者が実行する適切な情報

セキュリティ対策を、合意の一環として定める。

15.1.3　供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。

15.1.3.1 / 15.1.3.2 / 15.1.3.3 / 15.1.3.4 / 15.1.3.5 / 15.1.3.6 / 15.1.3.7 / 15.1.3.8 / 15.1.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.1.3.10.P　クラウドサービス提供者は、ピアクラウドサービス提供者[18]のクラウドサービスを利用する場合には、自身のクラウドサービス利用者に対する情報セキュリティの水準が維持されるか又は上回ることを確実にする仕組みを整備する。

15.1.3.11.P　クラウドサービス提供者は、サプライチェーンに基づきクラウドサービスを提供する際には、供給者に情報セキュリティの目的を与え、各供給者にその目的を達成するためのリスク管理活動を実施することを要求する。

15.2　供給者のサービス提供の管理

目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。

15.2.1　組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。

15.2.1.1 / 15.2.1.2 / 15.2.1.3 / 15.2.1.4 / 15.2.1.5 / 15.2.1.6 / 15.2.1.7 / 15.2.1.8 / 15.2.1.9 / 15.2.1.10 / 15.2.1.11 / 15.2.1.12 / 15.2.1.13 / 15.2.1.14 / 15.2.1.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.2.2　関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理する。

15.2.2.1 / 15.2.2.2 / 15.2.2.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16　情報セキュリティインシデント管理

16.1　情報セキュリティインシデントの管理及びその改善

目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

16.1.1　情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。

16.1.1.1 / 16.1.1.2 / 16.1.1.3 / 16.1.1.4 / 16.1.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.1.6.P　クラウドサービス提供者は、サービス仕様の一部として、クラウドサービス利用者とクラウドサービス提供者の間の、情報セキュリティインシデント管理の責任の割当て及び手順を定める。

16.1.1.7.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス提供者がクラウドサービス利用者に報告する情報セキュリティインシデントの範囲を

[18] ピアクラウドサービス提供者：一又は複数の他のクラウドサービス提供者が利用するために、その事業者のクラウドサービスの一環として、一又は複数のクラウドサービスを提供するクラウドサービス提供者（ISO/IEC 17789:2014 3.2.5 peer cloud service provider）

含む文書を提供する。

16.1.1.8.P　クラウドサービス提供者は、クラウドサービス利用者に、情報セキュリティインシデントの検知及び関連する対応策の開示レベルを含む文書を提供する。

16.1.1.9.P　クラウドサービス提供者は、クラウドサービス利用者に、情報セキュリティインシデントの発生を通知する目標時間枠を含む文書を提供する。

16.1.1.10.P　クラウドサービス提供者は、クラウドサービス利用者に、情報セキュリティインシデントの通知手順を含む文書を提供する。

16.1.1.11.P　クラウドサービス提供者は、クラウドサービス利用者に、情報セキュリティインシデント関連の問題に対処するための連絡先情報を含む文書を提供する。

16.1.1.12.P　クラウドサービス提供者は、クラウドサービス利用者に、特定の情報セキュリティインシデントが発生した場合に適用可能なあらゆる回復策を含む文書を提供する。

16.1.2　情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。

16.1.2.1 / 16.1.2.2 / 16.1.2.3 / 16.1.2.4 / 16.1.2.5 / 16.1.2.6 / 16.1.2.7 / 16.1.2.8 / 16.1.2.9 / 16.1.2.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.2.11.P　クラウドサービス提供者は、クラウドサービス利用者が、情報セキュリティ事象をクラウドサービス提供者に報告するための仕組みを提供する。

16.1.2.12.P　クラウドサービス提供者は、クラウドサービス提供者が、情報セキュリティ事象をクラウドサービス利用者に報告するための仕組みを提供する。

16.1.2.13.P　クラウドサービス提供者は、クラウドサービス利用者が、報告された情報セキュリティ事象の状況を追跡するための仕組みを提供する。

16.1.6　情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。

16.1.6.1 / 16.1.6.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.7　組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。

16.1.7.1 / 16.1.7.2 / 16.1.7.3 / 16.1.7.4 / 16.1.7.5 / 16.1.7.6 / 16.1.7.7 / 16.1.7.8 / 16.1.7.9 / 16.1.7.10 / 16.1.7.11 / 16.1.7.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.7.13.PB　クラウドサービス提供者は、クラウドサービス利用者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。

17　事業継続マネジメントにおける情報セキュリティの側面

17.1　情報セキュリティ継続

目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。

17.1.1　組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。

17.1.1.1 / 17.1.1.2 / 17.1.1.3 / 17.1.1.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

17.1.2　組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。

17.1.2.1 / 17.1.2.2 / 17.1.2.3 / 17.1.2.4 / 17.1.2.5 / 17.1.2.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。。

18　順守

18.1　法的及び契約上の要求事項の順守

目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

18.1.1　各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。

18.1.1.1 / 18.1.1.2 / 18.1.1.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.1.4.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービスを管轄する法域を通知する。

18.1.1.5.P　クラウドサービス提供者は、自身の関連する法的要求事項（例えば、個人を特定できる情報（PII）を保護するための暗号に関するもの）を特定する。

18.1.1.6.P　クラウドサービス提供者は、自身の関連する法的要求事項を特定した情報を、要求するクラウドサービス利用者に提供する。

18.1.1.7.P　クラウドサービス提供者は、クラウドサービス利用者に、適用法令及び契約上の要求事項を現時点で順守していることの証拠を提供する。

18.1.2　知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。

18.1.2.1 / 18.1.2.2 / 18.1.2.3 / 18.1.2.4 / 18.1.2.5 / 18.1.2.6 / 18.1.2.7 / 18.1.2.8 / 18.1.2.9 / 18.1.2.10 / 18.1.2.11 / 18.1.2.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.2.13.PB　クラウドサービス提供者は、知的財産権の順守に対応するためのプロセスを確立する。

18.1.3　記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。

18.1.3.1 / 18.1.3.2 / 18.1.3.3 / 18.1.3.4 / 18.1.3.5 / 18.1.3.6 / 18.1.3.7 / 18.1.3.8 / 18.1.3.9 / 18.1.3.10 / 18.1.3.11 / 18.1.3.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.3.13.PB　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービスの利用に関して、クラウドサービス提供者が収集し、蓄積する記録の保護について、情報を提供する。

18.1.4　プライバシー及びPIIの保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。

18.1.4.1 / 18.1.4.2 / 18.1.4.3 / 18.1.4.4 / 18.1.4.5 / 18.1.4.6は、「情報セキュリテ

ィ管理基準」の「管理策基準」に同じ。

18.1.5　暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。

18.1.5.1 / 18.1.5.2 / 18.1.5.3 / 18.1.5.4 / 18.1.5.5 / 18.1.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.5.7.PB　クラウドサービス提供者は、クラウドサービス利用者に、適用する協定、法令及び規則を順守していることをレビューするため、クラウドサービス提供者が実装した暗号化機能の記載を、提供する。

18.2　情報セキュリティのレビュー

目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

18.2.1　情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。

18.2.1.1 / 18.2.1.2 / 18.2.1.3 / 18.2.1.4 / 18.2.1.5 / 18.2.1.6 / 18.2.1.7 / 18.2.1.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.2.1.9.P　クラウドサービス提供者は、クラウドサービス利用者に、クラウドサービス提供者が主張する情報セキュリティ管理策の実施を立証するための、文書化した証拠を提供する。

18.2.1.10.P　個別のクラウドサービス利用者の監査が実用的でない又は情報セキュリティのリスクを増加させる可能性のある場合には、クラウドサービス提供者は、情報セキュリティがクラウドサービス提供者の方針及び手続に従って実装及び運用されているという、独立した証拠を提供する。

18.2.1.11.P　クラウドサービス提供者は、情報セキュリティがクラウドサービス提供者の方針及び手続に従って実装及び運用されているという、独立した証拠を、クラウドサービス利用者となる見込みのある者が、契約に先立って入手できるようにする。

18.2.1.12.P　クラウドサービス提供者が選択する適切な独立した監査は、十分な透明性が提供されることを条件に、クラウドサービス提供者の運用に対するレビューへのクラウドサービス利用者の関心を満たすための、通常受入れ可能な手段とする。

18.2.1.13.P　独立した監査が実用的でない場合は、クラウドサービス提供者は、自己評価を実施し、クラウドサービス利用者に、そのプロセス及び結果を開示する。

付録１

クラウドサービス利用者向け管理策基準

付録1. クラウドサービス利用者向け管理策基準

「C」は、クラウドサービスにおける、クラウドサービス利用者向け管理策であることを示す。

管理策基準に記載される管理策[X.X.X]は、情報セキュリティリスクアセスメントの結果に基づき、適切に選択すべき事項である。詳細管理策[X.X.X.X]については、管理策を実装するために組織・環境・技術等に応じて必要とする事項を選択する。

5 情報セキュリティのための方針群

5.1 情報セキュリティのための経営陣の方向性

目的：情報セキュリティのための経営陣の方向性及び支持を、事業上の要求事項並びに関連する法令及び規制に従って提示するため。

5.1.1 情報セキュリティのための方針群は、これを定義し、管理層[*19]が承認し、発行し、従業員及び関連する外部関係者に通知する。

5.1.1.1 / 5.1.1.2 / 5.1.1.3 / 5.1.1.4 / 5.1.1.5 / 5.1.1.6 / 5.1.1.7 / 5.1.1.8 / 5.1.1.9 / 5.1.1.10 / 5.1.1.11 / 5.1.1.12 / 5.1.1.13 / 5.1.1.14 / 5.1.1.15 / 5.1.1.16 / 5.1.1.17 / 5.1.1.18 / 5.1.1.19 / 5.1.1.20 / 5.1.1.21は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

5.1.1.32.C クラウドサービス利用者は、クラウドコンピューティングのための情報セキュリティ方針を、クラウドサービス利用者のトピック別の方針として定める。

5.1.1.33.C クラウドサービス利用者は、クラウドサービス利用者のクラウドコンピューティングのための情報セキュリティ方針を、組織の情報及びその他の資産に対する情報セキュリティリスクの受容可能なレベルと整合して定める。

5.1.1.34.C クラウドサービス利用者は、クラウドコンピューティングのための情報セキュリティ方針を定める際には、クラウドコンピューティング環境に保管する情報は、クラウドサービス提供者によるアクセス及び管理下にあることを考慮して定める。

5.1.1.35.C クラウドサービス利用者は、クラウドコンピューティングのための情報セキュリティ方針を定める際には、アプリケーションプログラムなどの資産は、クラウドコンピューティング環境に保持される可能性があることを考慮して定める。

5.1.1.36.C クラウドサービス利用者は、クラウドコンピューティングのための情報セキュリティ方針を定める際には、情報の処理は、マルチテナントの仮想化されたクラウドサービス上で実行される可能性があることを考慮して定める。

5.1.1.37.C クラウドサービス利用者は、クラウドコンピューティングのための情報セキュリティ方針を定める際には、クラウドサービスのユーザ及びそのクラウドサービスのユーザがクラウドサービスを利用する状況を考慮して定める。

5.1.1.38.C クラウドサービス利用者は、クラウドコンピューティングのための情報セキュリティ方針を定める際には、クラウドサービス利用者の特権的アクセスのあるクラウドサービス管理者を考慮して定める。

5.1.1.39.C クラウドサービス利用者は、クラウドコンピューティングのための情報セキュリティ方針を定める際には、クラウドサービス提供者の組織の地理的所在地、及び

*19 管理層には、経営陣及び管理者が含まれる。ただし、実務管理者（administrator）は除かれる。

クラウドサービス提供者が（たとえ、一時的にでも）クラウドサービス利用者のデータを保管する可能性のある国々を考慮して定める。

5.1.2　情報セキュリティのための方針群は、あらかじめ定めた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当かつ有効であることを確実にするためにレビューする。

5.1.2.1 / 5.1.2.2 / 5.1.2.3 / 5.1.2.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6　情報セキュリティのための組織

6.1　内部組織

目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

6.1.1　全ての情報セキュリティの責任を定め、割り当てる。

6.1.1.1 / 6.1.1.2 / 6.1.1.3 / 6.1.1.4 / 6.1.1.5 / 6.1.1.6 / 6.1.1.7 / 6.1.1.8 / 6.1.1.9 / 6.1.1.10 / 6.1.1.11 / 6.1.1.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.1.14.C　クラウドサービス利用者は、クラウドサービス提供者と、情報セキュリティの役割及び責任の適切な割当てについて合意し、割当てられた役割及び責任を遂行できることを確認する。

6.1.1.15.C　クラウドサービス利用者は、自身とクラウドサービス提供者の情報セキュリティの役割及び責任について、合意書に明記する。

6.1.1.16.C　クラウドサービス利用者は、クラウドサービス提供者の顧客対応部門との関係を特定し、管理する。

6.1.2　相反する職務及び責任範囲は、組織の資産に対する、認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために、分離する。

6.1.2.1 / 6.1.2.2 / 6.1.2.3 / 6.1.2.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.3　関係当局との適切な連絡体制を維持する。

6.1.3.1 / 6.1.3.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.3.4.C　クラウドサービス利用者は、クラウドサービス利用者及びクラウドサービス提供者が併せて行う操作に関連する関係当局を特定する。

6.1.4　情報セキュリティに関する研究会又は会議、及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持する。

6.1.4.1 / 6.1.4.2 / 6.1.4.3 / 6.1.4.4 / 6.1.4.5 / 6.1.4.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.1.5　プロジェクトの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。

6.1.5.1 / 6.1.5.2 / 6.1.5.3 / 6.1.5.4 / 6.1.5.5 / 6.1.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.2　モバイル機器及びテレワーキング

目的：モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

6.2.1　モバイル機器を用いることによって生じるリスクを管理するために、方針及びその方針を支援するセキュリティ対策を採用する。

6.2.1.1 / 6.2.1.2 / 6.2.1.3 / 6.2.1.4 / 6.2.1.5 / 6.2.1.6 / 6.2.1.7 / 6.2.1.8 / 6.2.1.9 / 6.2.1.10 / 6.2.1.11 / 6.2.1.12 / 6.2.1.13 / 6.2.1.14 / 6.2.1.15 / 6.2.1.16 / 6.2.1.17 / 6.2.1.18 / 6.2.1.19 / 6.2.1.20 / 6.2.1.21 / 6.2.1.22は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.2.2　テレワーキングの場所でアクセス、処理及び保存される情報を保護するために、方針及びその方針を支援するセキュリティ対策を実施する。

6.2.2.1 / 6.2.2.2 / 6.2.2.3 / 6.2.2.4 / 6.2.2.5 / 6.2.2.6 / 6.2.2.7 / 6.2.2.8 / 6.2.2.9 / 6.2.2.10 / 6.2.2.11 / 6.2.2.12 / 6.2.2.13 / 6.2.2.14 / 6.2.2.15 / 6.2.2.16 / 6.2.2.17 / 6.2.2.18 / 6.2.2.19 / 6.2.2.20 / 6.2.2.21は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

6.3.C　クラウドサービス利用者及びクラウドサービス提供者の関係

目的：情報セキュリティマネジメントのための、クラウドサービス利用者及びクラウドサービス提供者間の共同責任の関係を説明するため。

6.3.1.C　クラウドサービス利用者及びクラウドサービス提供者の両者は、クラウドサービスの利用における情報セキュリティの共同責任について、文書化し、公表し、伝達し、実装する。

6.3.1.1.C　クラウドサービス利用者は、クラウドサービスの利用に応じて、既存の方針及び手順を定義、又は追加し、クラウドサービスの利用において、クラウドサービスのユーザが、自身の責任を意識させる。

7　人的資源のセキュリティ

7.1　雇用前

目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。

7.1.1　全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。

7.1.1.1 / 7.1.1.2 / 7.1.1.3 / 7.1.1.4 / 7.1.1.5 / 7.1.1.6 / 7.1.1.7 / 7.1.1.8 / 7.1.1.9 / 7.1.1.10 / 7.1.1.11 / 7.1.1.12 / 7.1.1.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.1.2　従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。

7.1.2.1 / 7.1.2.2 / 7.1.2.3 / 7.1.2.4 / 7.1.2.5 / 7.1.2.6 / 7.1.2.7 / 7.1.2.8 / 7.1.2.9 / 7.1.2.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.2　雇用期間中

目的：従業員及び契約相手が、情報セキュリティの責任を認識し、かつ、その責任を遂行することを確実にするため。

7.2.1　経営陣は、組織の確立された方針及び手順に従った情報セキュリティの適用を、全ての従業員及び契約相手に要求する。

7.2.1.1 / 7.2.1.2 / 7.2.1.3 / 7.2.1.4 / 7.2.1.5 / 7.2.1.6 / 7.2.1.7 / 7.2.1.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.2.2　組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受ける。

7.2.2.1 / 7.2.2.2 / 7.2.2.3 / 7.2.2.4 / 7.2.2.5 / 7.2.2.6 / 7.2.2.7 / 7.2.2.8 / 7.2.2.9 / 7.2.2.10 / 7.2.2.11 / 7.2.2.12 / 7.2.2.13 / 7.2.2.14 / 7.2.2.15 / 7.2.2.16 / 7.2.2.17 / 7.2.2.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.2.2.20.C　クラウドサービス利用者は、関連する従業員及び契約相手を含む、クラウドサービスのビジネスマネージャ、クラウドサービスの管理者、クラウドサービスのインテグレータ及びクラウドサービスのユーザのための、意識向上、教育及び訓練のプログラムに、クラウドサービスの利用のための標準類及び手順を追加する。

7.2.2.21.C　クラウドサービス利用者は、関連する従業員及び契約相手を含む、クラウドサービスのビジネスマネージャ、クラウドサービスの管理者、クラウドサービスのインテグレータ及びクラウドサービスのユーザのための、意識向上、教育及び訓練のプログラムに、クラウドサービスに関連する情報セキュリティリスク及びそれらのリスクをどのように管理方法を追加する。

7.2.2.22.C　クラウドサービス利用者は、関連する従業員及び契約相手を含む、クラウドサービスのビジネスマネージャ、クラウドサービスの管理者、クラウドサービスのインテグレータ及びクラウドサービスのユーザのための、意識向上、教育及び訓練のプログラムに、クラウドサービスの利用に伴うシステム及びネットワーク環境のリスクを追加する。

7.2.2.23.C　クラウドサービス利用者は、関連する従業員及び契約相手を含む、クラウドサービスのビジネスマネージャ、クラウドサービスの管理者、クラウドサービスのインテグレータ及びクラウドサービスのユーザのための、意識向上、教育及び訓練のプログラムに、適用法令及び規制上の考慮事項を追加する。

7.2.2.24.C　クラウドサービス利用者は、クラウドサービスについての情報セキュリティの意識向上、教育及び訓練のプログラムを、経営陣及び監督責任者（事業単位の経営陣及び監督責任者を含む）に提供する。

7.2.3　情報セキュリティ違反を犯した従業員に対して処置をとるための、正式かつ周知された懲戒手続を備える。

7.2.3.1 / 7.2.3.2 / 7.2.3.3 / 7.2.3.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

7.3　雇用の終了及び変更

目的：雇用の終了又は変更のプロセスの一部として、組織の利益を保護するため。

7.3.1　雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、その従業員又は契約相手に伝達し、かつ、遂行させる。

7.3.1.1 / 7.3.1.2 / 7.3.1.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8　資産の管理

8.1　資産に対する責任

目的：組織の資産を特定し、適切な保護の責任を定めるため。

8.1.1　情報、情報に関連するその他の資産及び情報処理施設を特定する。また、これらの資産の目録を、作成し、維持する。

8.1.1.1 / 8.1.1.2 / 8.1.1.3 / 8.1.1.4 / 8.1.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.1.7.C　クラウドサービス利用者は、資産目録に、クラウドコンピューティング環境に保管される情報及び関連資産を明確にする。

8.1.1.8.C　クラウドサービス利用者資産目録の記録に、資産が保持される場所（例えば、クラウドサービスの所在の特定）を示す。

8.1.2　目録の中で維持される資産は、管理する。

8.1.2.1 / 8.1.2.2 / 8.1.2.3 / 8.1.2.4 / 8.1.2.5 / 8.1.2.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.3　情報の利用の許容範囲、並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は、明確にし、文書化し、実施する。

8.1.3.1 / 8.1.3.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.4　全ての従業員及び外部の利用者は、雇用、契約又は合意の終了時に、自らが所持する組織の資産の全てを返却する。

8.1.4.1 / 8.1.4.2 / 8.1.4.3 / 8.1.4.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.1.5.C　クラウドサービス提供者の領域上にあるクラウドサービス利用者の資産は、クラウドサービス利用の合意の終了時に、時期を失せずに返却ままたは除去する。

8.1.5.1.C　クラウドサービス利用者は、クラウドサービス提供者に、クラウドサービス利用者の資産の返却及び除去に続き、クラウドサービス提供者のシステムからクラウドサービス利用者の資産の全ての複写の削除に至るサービスプロセスの終了についての文書化された記載を要求する。

8.1.5.2.C　クラウドサービス利用者は、全ての資産を列挙し、サービス終了のスケジュールを記録し、時期を失せずに記載する。

8.2　情報分類

目的：組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

8.2.1　情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類する。

8.2.1.1 / 8.2.1.2 / 8.2.1.3 / 8.2.1.4 / 8.2.1.5 / 8.2.1.6 / 8.2.1.7 / 8.2.1.8 / 8.2.1.9 / 8.2.1.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.2.2　情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定

し、実施する。

8.2.2.1 / 8.2.2.2 / 8.2.2.3 / 8.2.2.4 / 8.2.2.5 / 8.2.2.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.2.2.8.C　クラウドサービス利用者は、採用したラベル付けの手順[20]に従って、クラウドコンピューティング環境において保持する情報及び関連資産にラベル付けする。

8.2.3　資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施する。

8.2.3.1 / 8.2.3.2 / 8.2.3.3 / 8.2.3.4 / 8.2.3.5 / 8.2.3.6 / 8.2.3.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.3　媒体の取扱い

目的：媒体に保存された情報の認可されていない開示、変更、除去又は破壊を防止するため。

8.3.1　組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施する。

8.3.1.1 / 8.3.1.2 / 8.3.1.3 / 8.3.1.4 / 8.3.1.5 / 8.3.1.6 / 8.3.1.7 / 8.3.1.8 / 8.3.1.9 / 8.3.1.10 / 8.3.1.11は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.3.2　媒体が不要になった場合は、正式な手順を用いて、セキュリティを保って処分する。

8.3.2.1 / 8.3.2.2 / 8.3.2.3 / 8.3.2.4 / 8.3.2.5 / 8.3.2.6 / 8.3.2.7 / 8.3.2.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

8.3.3　情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。

8.3.3.1 / 8.3.3.2 / 8.3.3.3 / 8.3.3.4 / 8.3.3.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9　アクセス制御

9.1　アクセス制御に対する業務上の要求事項

目的：情報及び情報処理施設へのアクセスを制限するため。

9.1.1　アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。

9.1.1.1 / 9.1.1.2 / 9.1.1.3 / 9.1.1.4 / 9.1.1.5 / 9.1.1.6 / 9.1.1.7 / 9.1.1.8 / 9.1.1.9 / 9.1.1.10 / 9.1.1.11 / 9.1.1.12 / 9.1.1.13 / 9.1.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.1.2　利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供する。

9.1.2.1 / 9.1.2.2 / 9.1.2.3 / 9.1.2.4 / 9.1.2.5 / 9.1.2.6 / 9.1.2.7 / 9.1.2.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.1.2.9.C　ネットワークサービス利用のためのアクセス制御方針は、、利用されるそれぞれ別のクラウドサービス毎にユーザアクセスのための要求事項を明記する。

9.2　利用者アクセスの管理

目的：システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため。

---

[20]適用可能な場合には、クラウドサービス利用者は、クラウドサービス提供者の提供するラベル付けを支援する機能を採用できる。

9.2.1　アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施する。

9.2.1.1 / 9.2.1.2 / 9.2.1.3 / 9.2.1.4 / 9.2.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.2　全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。

9.2.2.1 / 9.2.2.2 / 9.2.2.3 / 9.2.2.4 / 9.2.2.5 / 9.2.2.6 / 9.2.2.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.3　特権的アクセス権の割当て及び利用は、制限し、管理する。

9.2.3.1 / 9.2.3.2 / 9.2.3.3 / 9.2.3.4 / 9.2.3.5 / 9.2.3.6 / 9.2.3.7 / 9.2.3.8 / 9.2.3.9 / 9.2.3.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.3.12.C　クラウドサービス利用者は、クラウドサービスの管理能力にあわせたクラウドサービス利用者の管理者認証に、特定したリスクに応じた、十分に強固な認証技術（例えば、多要素認証）を利用する。

9.2.4　秘密認証情報の割当ては、正式な管理プロセスによって管理する。

9.2.4.1 / 9.2.4.2 / 9.2.4.3 / 9.2.4.4 / 9.2.4.5 / 9.2.4.6 / 9.2.4.7 / 9.2.4.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.4.10.C　クラウドサービス利用者は、パスワードなどの秘密認証情報の割当てのための、クラウドサービス提供者の管理手順が、クラウドサービス利用者の要求事項を満たすことを検証する。

9.2.5　資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。

9.2.5.1 / 9.2.5.2 / 9.2.5.3 / 9.2.5.4 / 9.2.5.5 / 9.2.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.2.6　全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。

9.2.6.1 / 9.2.6.2 / 9.2.6.3 / 9.2.6.4 / 9.2.6.5 / 9.2.6.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.3　利用者の責任

目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため。

9.3.1　秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。

9.3.1.1 / 9.3.1.2 / 9.3.1.3 / 9.3.1.4 / 9.3.1.5 / 9.3.1.6 / 9.3.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4　システム及びアプリケーションのアクセス制御

目的：システム及びアプリケーションへの、認可されていないアクセスを防止するため。

9.4.1　情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。

9.4.1.1 / 9.4.1.2 / 9.4.1.3 / 9.4.1.4 / 9.4.1.5 / 9.4.1.6 / 9.4.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.1.9.C　クラウドサービス利用者は、クラウドサービスにおける情報へのアクセスを、ア

クセス制御方針に従って制限できること[21]、及びそのような制限を実現することを確実にする仕組みを整備する。

9.4.2　アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。

9.4.2.1 / 9.4.2.2 / 9.4.2.3 / 9.4.2.4 / 9.4.2.5 / 9.4.2.6 / 9.4.2.7 / 9.4.2.8 / 9.4.2.9 / 9.4.2.10 / 9.4.2.11 / 9.4.2.12 / 9.4.2.13 / 9.4.2.14 / 9.4.2.15 / 9.4.2.16は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.3　パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。

9.4.3.1 / 9.4.3.2 / 9.4.3.3 / 9.4.3.4 / 9.4.3.5 / 9.4.3.6 / 9.4.3.7 / 9.4.3.8 / 9.4.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.4　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。

9.4.4.1 / 9.4.4.2 / 9.4.4.3 / 9.4.4.4 / 9.4.4.5 / 9.4.4.6 / 9.4.4.7 / 9.4.4.8 / 9.4.4.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.4.4.12.C　クラウドサービス利用者は、ユーティリティプログラムの利用を許可する場合には、クラウドコンピューティング環境において利用するユーティリティプログラムを特定し、クラウドサービスの管理策を妨げないことを確実にする仕組みを整備する。

9.4.5　プログラムソースコードへのアクセスは、制限する。

9.4.5.1 / 9.4.5.2 / 9.4.5.3 / 9.4.5.4 / 9.4.5.5 / 9.4.5.6 / 9.4.5.7 / 9.4.5.8 / 9.4.5.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

9.5.C　共有化された仮想環境におけるクラウドサービス利用者のデータのアクセス制御

目的：共有化されたクラウドコンピューティング上の仮想環境における情報セキュリティを確実にするため。

9.5.1.C　クラウドサービス利用者のクラウドサービス上の仮想環境は、他のクラウドサービス利用者及び認可されていない者から保護する。

9.5.2.C　クラウドコンピューティング環境における仮想マシンは、事業上のニーズを満たすため、要塞化する。

9.5.2.2.C　クラウドサービス利用者は、仮想マシンを設定する際には、適切に要塞化し(例えば、クラウドサービスを実行するのに必要なポート、プロトコル及びサービスのみを有効とする）、利用する各仮想マシンに適切な技術的管理策(例えば、マルウェア対策、ログ取得）を実施する。

10　暗号

10.1　暗号による管理策

目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため。

[21] これには、クラウドサービス、クラウドサービス機能及びクラウドサービス内で保持されるクラウドサービス利用者のデータに対するアクセス制限が含まれる。

10.1.1　情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。

10.1.1.1 / 10.1.1.2 / 10.1.1.3 / 10.1.1.4 / 10.1.1.5 / 10.1.1.6 / 10.1.1.7 / 10.1.1.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

10.1.1.11.C　クラウドサービス利用者は、リスク分析により正当化された場合には、クラウドサービスの利用のための暗号による管理策を実施する。

10.1.1.12.C　クラウドサービス利用者は、その管理策を提供するのがクラウドサービス利用者であれ、クラウドサービス提供者であれ、暗号による管理策は、特定したリスクを低減するために十分な強度とする。

10.1.1.13.C　クラウドサービス利用者は、クラウドサービス提供者が暗号を提供する際には、クラウドサービス提供者が供給する全ての情報をレビューし、暗号機能がクラウドサービス利用者の方針の要求事項を満たすことを確認する。

10.1.1.14.C　クラウドサービス利用者は、クラウドサービス提供者が暗号を提供する際には、クラウドサービス提供者が供給する全ての情報をレビューし、暗号機能がクラウドサービス利用者の利用する他の暗号による保護と互換性があることを確認する。

10.1.1.15.C　クラウドサービス利用者は、クラウドサービス提供者が暗号を提供する際には、クラウドサービス提供者が供給する全ての情報をレビューし、暗号機能が、保存データに適用される、若しくは、クラウドサービスへの転送中のデータ、クラウドサービスからの転送中のデータ及びクラウドサービス内で転送中のデータに適用されることを確認する。

10.1.2　暗号鍵の利用、保護及び有効期間（lifetime）に関する方針を策定し、そのライフサイクル全体にわたって実施する。

10.1.2.1 / 10.1.2.2 / 10.1.2.3 / 10.1.2.4 / 10.1.2.5 / 10.1.2.6 / 10.1.2.7 / 10.1.2.8 / 10.1.2.9 / 10.1.2.10 / 10.1.2.11 / 10.1.2.12 / 10.1.2.13 / 10.1.2.14 / 10.1.2.15 / 10.1.2.16 / 10.1.2.17 / 10.1.2.18 / 10.1.2.19は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

10.1.2.20.C　クラウドサービス利用者は、各クラウドサービスに利用する暗号鍵を特定し、鍵管理手順を実施する。

10.1.2.21.C　クラウドサービス利用者は、クラウドサービス利用者が利用する鍵管理機能をクラウドサービス提供者が提供する場合には、クラウドサービスに関連する鍵管理手順における鍵の種類の情報を要求する。

10.1.2.22.C　クラウドサービス利用者は、クラウドサービス利用者が利用する鍵管理機能をクラウドサービス提供者が提供する場合には、クラウドサービスに関連する鍵管理手順における鍵のライフサイクル、すなわち、生成、変更又は更新、保管、無効化、取り出し、保持及び破壊の各段階の手順を含む鍵管理システムの仕様の情報を要求する。

10.1.2.23.C　クラウドサービス利用者は、クラウドサービス利用者が利用する鍵管理機能をクラウドサービス提供者が提供する場合には、クラウドサービスに関連する鍵管理手順におけるクラウドサービス利用者が利用するために推奨される鍵管理手順

の情報を要求する。

10.1.2.24.C　クラウドサービス利用者は、クラウドサービス利用者が自ら鍵管理を行う場合、又は分けられた別個の鍵管理サービスを利用する場合、暗号の運用のための暗号鍵を、クラウドサービス提供者が保管及び管理することを許可しない。

11　物理的及び環境的セキュリティ

11.1　セキュリティを保つべき領域

目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。

11.1.1　取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いる。

11.1.1.1 / 11.1.1.2 / 11.1.1.3 / 11.1.1.4 / 11.1.1.5 / 11.1.1.6 / 11.1.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.2　セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護する。

11.1.2.1 / 11.1.2.2 / 11.1.2.3 / 11.1.2.4 / 11.1.2.5 / 11.1.2.6 / 11.1.2.7 / 11.1.2.8 / 11.1.2.9 / 11.1.2.10 / 11.1.2.11 / 11.1.2.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.3　オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。

11.1.3.1 / 11.1.3.2 / 11.1.3.3 / 11.1.3.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.4　自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用する。

11.1.4.1は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.5　セキュリティを保つべき領域での作業に関する手順を設計し、適用する。

11.1.5.1 / 11.1.5.2 / 11.1.5.3 / 11.1.5.4 / 11.1.5.5 / 11.1.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.1.6　荷物の受渡場所などの立寄り場所、及び認可されていない者が施設に立ち入ることもあるその他の場所は、管理する。また、認可されていないアクセスを避けるために、それらの場所を情報処理施設から離す。

11.1.6.1 / 11.1.6.2 / 11.1.6.3 / 11.1.6.4 / 11.1.6.5 / 11.1.6.6 / 11.1.6.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2　装置

目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。

11.2.1　装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し、保護する。

11.2.1.1 / 11.2.1.2 / 11.2.1.3 / 11.2.1.4 / 11.2.1.5 / 11.2.1.6 / 11.2.1.7 / 11.2.1.8 / 11.2.1.9 / 11.2.1.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.2　装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。

11.2.2.1 / 11.2.2.2 / 11.2.2.3 / 11.2.2.4 / 11.2.2.5 / 11.2.2.6 / 11.2.2.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.3　データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。

11.2.3.1 / 11.2.3.2 / 11.2.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.4　装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。

11.2.4.1 / 11.2.4.2 / 11.2.4.3 / 11.2.4.4 / 11.2.4.5 / 11.2.4.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.5　装置、情報又はソフトウェアは、事前の認可なしでは、構外に持ち出さない。

11.2.5.1 / 11.2.5.2 / 11.2.5.3 / 11.2.5.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.6　構外にある資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。

11.2.6.1 / 11.2.6.2 / 11.2.6.3 / 11.2.6.4 / 11.2.6.5 / 11.2.6.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.7　記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証する。

11.2.7.1 / 11.2.7.2 / 11.2.7.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.7.5.C　クラウドサービス利用者は、クラウドサービス提供者が資源のセキュリティを保った処分又は再利用のための方針及び手順を有することの確認を取る。

11.2.8　利用者は、無人状態にある装置が適切な保護対策を備えていることを確実にする仕組みを整備する。

11.2.8.1 / 11.2.8.2 / 11.2.8.3 / 11.2.8.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

11.2.9　書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。[*22]

11.2.9.1 / 11.2.9.2 / 11.2.9.3 / 11.2.9.4 / 11.2.9.5 / 11.2.9.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12　運用のセキュリティ

12.1　運用の手順及び責任

目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため。

12.1.1　操作手順は、文書化し、必要とする全ての利用者に対して利用可能とする。

12.1.1.1 / 12.1.1.2 / 12.1.1.3 / 12.1.1.4 / 12.1.1.5 / 12.1.1.6 / 12.1.1.7 / 12.1.1.8 / 12.1.1.9 / 12.1.1.10 / 12.1.1.11 / 12.1.1.12 / 12.1.1.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

[*22] クリアデスクとは、机上に書類を放置しないことをいう。また、クリアスクリーンとは、情報をスクリーンに残したまま離席しないことをいう。

12.1.2　情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理する。

12.1.2.1 / 12.1.2.2 / 12.1.2.3 / 12.1.2.4 / 12.1.2.5 / 12.1.2.6 / 12.1.2.7 / 12.1.2.8 / 12.1.2.9 / 12.1.2.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.2.12.C　クラウドサービス利用者の変更管理プロセスにおいて、クラウドサービス提供者による変更の影響を確認する。

12.1.3　要求された主要なシステム資源の使用を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測する。

12.1.3.1 / 12.1.3.2 / 12.1.3.3 / 12.1.3.4 / 12.1.3.5 / 12.1.3.6 / 12.1.3.7 / 12.1.3.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.3.10.C　クラウドサービス利用者は、クラウドサービス提供者が提供する合意した容量が、クラウドサービス利用者の要求事項を満たすことを確実にする仕組みを整備する。

12.1.3.11.C　クラウドサービス利用者は、クラウドサービスの性能を長期的に満たすことを確実にするため、クラウドサービスの利用を監視し、その容量の需要を予測する。

12.1.4　開発環境、試験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離する。

12.1.4.1 / 12.1.4.2 / 12.1.4.3 / 12.1.4.4 / 12.1.4.5 / 12.1.4.6 / 12.1.4.7 / 12.1.4.8 / 12.1.4.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.1.5.C　クラウドコンピューティング環境の、管理のための操作手順を定義し、文書化し、監視する。

12.1.5.2.C　クラウドサービス利用者は、一つの失敗がクラウドコンピューティング環境における資産に回復不能な損害をもたらしうる場合には、重要な操作[23]の手順を文書化する。

12.1.5.3.C　クラウドサービス利用者は、文書には、重要な操作を監督者が監視することを定める。

12.2　マルウェアからの保護

目的：情報及び情報処理施設がマルウェアから保護されることを確実にするため。

12.2.1　マルウェアから保護するために、利用者に適切に認識させることと併せて、検出、予防及び回復のための管理策を実施する。

12.2.1.1 / 12.2.1.2 / 12.2.1.3 / 12.2.1.4 / 12.2.1.5 / 12.2.1.6 / 12.2.1.7 / 12.2.1.8 / 12.2.1.9 / 12.2.1.10 / 12.2.1.11 / 12.2.1.12 / 12.2.1.13 / 12.2.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.3　バックアップ

目的：データの消失から保護するため。

---

[23] 重要な操作には、例えば、次のものがある。
- サーバ、ネットワーク及びストレージなどの仮想化されたデバイスのインストール、変更及び削除
- クラウドサービス利用の終了処置
- バックアップ及び復旧

12.3.1　情報、ソフトウェア及びシステムイメージのバックアップは、合意されたバックアップ方針に従って定期的に取得し、検査する。

12.3.1.1 / 12.3.1.2 / 12.3.1.3 / 12.3.1.4 / 12.3.1.5 / 12.3.1.6 / 12.3.1.7 / 12.3.1.8 / 12.3.1.9 / 12.3.1.10 / 12.3.1.11 / 12.3.1.12 / 12.3.1.13 / 12.3.1.14 / 12.3.1.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.3.1.25.C　クラウドサービス利用者は、クラウドサービス提供者がクラウドサービスの一環としてバックアップ機能を提供する場合には、クラウドサービス提供者にバックアップ機能の仕様を要求する。

12.3.1.26.C　クラウドサービス利用者は、クラウドサービス提供者がクラウドサービスの一環としてバックアップ機能を提供する場合[24]には、その機能がクラウドサービス利用者のバックアップの要求事項を満たすことを検証する。

12.4　ログ取得及び監視

目的：イベントを記録し、証拠を作成するため。

12.4.1　利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。

12.4.1.1 / 12.4.1.2 / 12.4.1.3 / 12.4.1.4 / 12.4.1.5 / 12.4.1.6 / 12.4.1.7 / 12.4.1.8 / 12.4.1.9 / 12.4.1.10 / 12.4.1.11 / 12.4.1.12 / 12.4.1.13 / 12.4.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.1.16.C　クラウドサービス利用者は、イベントログ取得のための要求事項を定義し、クラウドサービスがそれらの要求事項を満たすことを検証する。

12.4.2　ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護する。

12.4.2.1 / 12.4.2.2 / 12.4.2.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.3　システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。

12.4.3.1 / 12.4.3.2 / 12.4.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.4.3.4.C　クラウドサービス利用者は、クラウドコンピューティング環境における特権的な操作がクラウドサービス利用者に委任されている場合には、その操作及びその操作のパフォーマンスを記録する。

12.4.3.5.C　クラウドサービス利用者は、クラウドサービス提供者が提供するログ取得機能が適切かどうか、又はクラウドサービス利用者が追加のログ取得機能を実装すべきかどうかを決定する。

12.4.4　組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは、単一の参照時刻源と同期させる。

12.4.4.1 / 12.4.4.2 / 12.4.4.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

---

[24] クラウドサービス提供者がバックアップ機能を提供しない場合には、クラウドサービス利用者にバックアップ機能の実装の責任がある。

12.4.4.5.C　クラウドサービス利用者は、クラウドサービス提供者のシステムで利用されるクロックの同期について、情報を要求する。

12.4.5.C　クラウドサービス利用者は、利用するクラウドサービスの操作を監視する機能を有する。

12.4.5.6.C　クラウドサービス利用者は、クラウドサービス提供者に、各クラウドサービスに利用可能なサービス監視機能の情報を要求する。

12.5　運用ソフトウェアの管理

目的：運用システムの完全性を確実にするため。

12.5.1　運用システムに関わるソフトウェアの導入を管理するための手順を実施する。

12.5.1.1 / 12.5.1.2 / 12.5.1.3 / 12.5.1.4 / 12.5.1.5 / 12.5.1.6 / 12.5.1.7 / 12.5.1.8 / 12.5.1.9 / 12.5.1.10 / 12.5.1.11 / 12.5.1.12 / 12.5.1.13 / 12.5.1.14 / 12.5.1.15 / 12.5.1.16 / 12.5.1.17 / 12.5.1.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.6　技術的ぜい弱性管理

目的：技術的ぜい弱性の悪用を防止するため。

12.6.1　利用中の情報システムの技術的ぜい弱性に関する情報は、時機を失せずに獲得する。また、そのようなぜい弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。

12.6.1.1 / 12.6.1.2 / 12.6.1.3 / 12.6.1.4 / 12.6.1.5 / 12.6.1.6 / 12.6.1.7 / 12.6.1.8 / 12.6.1.9 / 12.6.1.10 / 12.6.1.11 / 12.6.1.12 / 12.6.1.13 / 12.6.1.14 / 12.6.1.15 / 12.6.1.16 / 12.6.1.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.6.1.19.C　クラウドサービス利用者は、クラウドサービス提供者に、提供されるクラウドサービスに影響を及ぼす可能性のある技術的ぜい弱性の管理について、情報を要求する。

12.6.1.20.C　クラウドサービス利用者は、管理責任のある技術的ぜい弱性を特定し、それらを管理するためのプロセスを明確に定める。

12.6.2　利用者によるソフトウェアのインストールを管理する規則を確立し、実施する。

12.6.2.1 / 12.6.2.2 / 12.6.2.3 / 12.6.2.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

12.7　情報システムの監査に対する考慮事項

目的：運用システムに対する監査活動の影響を最小限にするため。

12.7.1　運用システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意する。

12.7.1.1 / 12.7.1.2 / 12.7.1.3 / 12.7.1.4 / 12.7.1.5 / 12.7.1.6 / 12.7.1.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13　通信のセキュリティ

13.1　ネットワークセキュリティ管理

目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。

13.1.1　システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御す

る。

13.1.1.1 / 13.1.1.2 / 13.1.1.3 / 13.1.1.4 / 13.1.1.5 / 13.1.1.6 / 13.1.1.7 / 13.1.1.8 / 13.1.1.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.2　組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、ネットワークサービス合意書にもこれらを盛り込む。

13.1.2.1 / 13.1.2.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.3　情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離する。

13.1.3.1 / 13.1.3.2 / 13.1.3.3 / 13.1.3.4 / 13.1.3.5 / 13.1.3.6 / 13.1.3.7 / 13.1.3.8 / 13.1.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.1.3.13.C　クラウドサービス利用者は、クラウドサービスの共有環境におけるテナントの隔離を達成するネットワーク分離のための要求事項を定義し、クラウドサービス提供者がそれらの要求事項を満たすことを検証する。

13.1.4.C　仮想ネットワークを設定する際には、クラウドサービス提供者のネットワークセキュリティ方針に基づき、仮想ネットワークと物理ネットワークの設定の整合性を検証する。

13.2　情報の転送

目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。

13.2.1　あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備える。

13.2.1.1 / 13.2.1.2 / 13.2.1.3 / 13.2.1.4 / 13.2.1.5 / 13.2.1.6 / 13.2.1.7 / 13.2.1.8 / 13.2.1.9 / 13.2.1.10 / 13.2.1.11 / 13.2.1.12 / 13.2.1.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.2.2　合意では、組織と外部関係者との間の業務情報のセキュリティを保った転送について、取り扱う。

13.2.2.1 / 13.2.2.2 / 13.2.2.3 / 13.2.2.4 / 13.2.2.5 / 13.2.2.6 / 13.2.2.7 / 13.2.2.8 / 13.2.2.9 / 13.2.2.10 / 13.2.2.11 / 13.2.2.12 / 13.2.2.13は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.2.3　電子的メッセージ通信に含まれた情報は、適切に保護する。

13.2.3.1 / 13.2.3.2 / 13.2.3.3 / 13.2.3.4 / 13.2.3.5 / 13.2.3.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

13.2.4　情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化する。

13.2.4.1 / 13.2.4.2 / 13.2.4.3 / 13.2.4.4 / 13.2.4.5 / 13.2.4.6 / 13.2.4.7 / 13.2.4.8 / 13.2.4.9 / 13.2.4.10 / 13.2.4.11 / 13.2.4.12 / 13.2.4.13 / 13.2.4.14 / 13.2.4.15 / 13.2.4.16は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14　システムの取得、開発及び保守

14.1　情報システムのセキュリティ要求事項

目的：ライフサイクル全体にわたって、情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。これには、公衆ネットワークを介してサービスを提供する情報

システムのための要求事項も含む。

14.1.1　情報セキュリティに関連する要求事項は、新しい情報システム又は既存の情報システムの改善に関する要求事項に含める。

14.1.1.1 / 14.1.1.2 / 14.1.1.3 / 14.1.1.4 / 14.1.1.5 / 14.1.1.6 / 14.1.1.7 / 14.1.1.8 / 14.1.1.9 / 14.1.1.10 / 14.1.1.11 / 14.1.1.12 / 14.1.1.13 / 14.1.1.14 / 14.1.1.15 / 14.1.1.16 / 14.1.1.17 / 14.1.1.18は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.1.1.21.C　クラウドサービス利用者は、クラウドサービスの情報セキュリティ要求事項を決定し、クラウドサービス提供者が提供するサービスが、これらの要求事項を満たすことができるか評価する。

14.1.1.22.C　クラウドサービス利用者は、クラウドサービス提供者が提供するサービスが、クラウドサービスの情報セキュリティ要求事項を満たすことができるか評価するために、クラウドサービス提供者から情報セキュリティ機能の情報を取得する。

14.1.2　公衆ネットワークを経由するアプリケーションサービスに含まれる情報は、不正行為、契約紛争、並びに認可されていない開示及び変更から保護する。

14.1.2.1 / 14.1.2.2 / 14.1.2.3 / 14.1.2.4 / 14.1.2.5 / 14.1.2.6 / 14.1.2.7 / 14.1.2.8 / 14.1.2.9 / 14.1.2.10 / 14.1.2.11 / 14.1.2.12 / 14.1.2.13 / 14.1.2.14 / 14.1.2.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.1.3　アプリケーションサービスのトランザクションに含まれる情報は、次の事項を未然に防止するために、保護する。

- 不完全な通信
- 誤った通信経路設定
- 認可されていないメッセージの変更
- 認可されていない開示
- 認可されていないメッセージの複製又は再生

14.1.3.1 / 14.1.3.2 / 14.1.3.3 / 14.1.3.4 / 14.1.3.5 / 14.1.3.6 は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2　開発及びサポートプロセスにおけるセキュリティ

目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため

14.2.1　ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。

14.2.1.1 / 14.2.1.2 / 14.2.1.3 / 14.2.1.4 / 14.2.1.5 / 14.2.1.6 / 14.2.1.7 / 14.2.1.8 / 14.2.1.9 / 14.2.1.10 / 14.2.1.11 / 14.2.1.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.1.14.C　クラウドサービス利用者は、クラウドサービス提供者に、セキュリティを保つための開発手順及び慣行について、情報を要求する。

14.2.2　開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。

14.2.2.1 / 14.2.2.2 / 14.2.2.3 / 14.2.2.4 / 14.2.2.5 / 14.2.2.6 / 14.2.2.7 / 14.2.2.

8 / 14.2.2.9 / 14.2.2.10 / 14.2.2.11 / 14.2.2.12 / 14.2.2.13 / 14.2.2.14 / 14.2.2.15 / 14.2.2.16 / 14.2.2.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.3　オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。

14.2.3.1 / 14.2.3.2 / 14.2.3.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.4　パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。

14.2.4.1 / 14.2.4.2 / 14.2.4.3 / 14.2.4.4 / 14.2.4.5 / 14.2.4.6 / 14.2.4.7 / 14.2.4.8 / 14.2.4.9 / 14.2.4.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.5　セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、全ての情報システムの実装に対して適用する。

14.2.5.1 / 14.2.5.2 / 14.2.5.3 / 14.2.5.4 / 14.2.5.5 / 14.2.5.6 / 14.2.5.7は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.6　組織は、全てのシステム開発ライフサイクルを含む、システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し、適切に保護する。

14.2.6.1 / 14.2.6.2 / 14.2.6.3 / 14.2.6.4 / 14.2.6.5 / 14.2.6.6 / 14.2.6.7 / 14.2.6.8 / 14.2.6.9 / 14.2.6.10 / 14.2.6.11 / 14.2.6.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.7　組織は、外部委託したシステム開発活動を監督し、監視する。

14.2.7.1 / 14.2.7.2 / 14.2.7.3 / 14.2.7.4 / 14.2.7.5 / 14.2.7.6 / 14.2.7.7 / 14.2.7.8 / 14.2.7.9 / 14.2.7.10 / 14.2.7.11は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.8　セキュリティ機能（functionality）の試験は、開発期間中に実施する。

14.2.8.1 / 14.2.8.2 / 14.2.8.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.2.9　新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。

14.2.9.1 / 14.2.9.2 / 14.2.9.3 / 14.2.9.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

14.3　試験データ

目的：試験に用いるデータの保護を確実にするため

14.3.1　試験データは、注意深く選定し、保護し、管理する。

14.3.1.1 / 14.3.1.2 / 14.3.1.3 / 14.3.1.4 / 14.3.1.5 / 14.3.1.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15　供給者関係

15.1　供給者関係における情報セキュリティ

目的：供給者がアクセスできる組織の資産の保護を確実にするため

15.1.1　組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ

要求事項について、供給者と合意し、文書化する。

15.1.1.1 / 15.1.1.2 / 15.1.1.3 / 15.1.1.4 / 15.1.1.5 / 15.1.1.6 / 15.1.1.7 / 15.1.1.8 / 15.1.1.9 / 15.1.1.10 / 15.1.1.11 / 15.1.1.12 / 15.1.1.13 / 15.1.1.14は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.1.1.15.C　クラウドサービス利用者は、供給者の一類型として、クラウドサービス提供者を供給者関係のための情報セキュリティ方針に含める。

15.1.2　関連する全ての情報セキュリティ要求事項を確立し、組織の情報に対して、アクセス、処理、保存若しくは通信を行う、又は組織の情報のためのIT 基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意する。

15.1.2.1 / 15.1.2.2 / 15.1.2.3 / 15.1.2.4 / 15.1.2.5 / 15.1.2.6 / 15.1.2.7 / 15.1.2.8 / 15.1.2.9 / 15.1.2.10 / 15.1.2.11 / 15.1.2.12 / 15.1.2.13 / 15.1.2.14 / 15.1.2.15 / 15.1.2.16 / 15.1.2.17は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.1.2.19.C　クラウドサービス利用者は、サービス合意書に記載された、クラウドサービスに関する情報セキュリティの役割及び責任[25]を確認する。

15.1.3　供給者との合意には、情報通信技術（以下「ICT」という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含める。

15.1.3.1 / 15.1.3.2 / 15.1.3.3 / 15.1.3.4 / 15.1.3.5 / 15.1.3.6 / 15.1.3.7 / 15.1.3.8 / 15.1.3.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.2　供給者のサービス提供の管理

目的：供給者との合意に沿って、情報セキュリティ及びサービス提供について合意したレベルを維持するため。

15.2.1　組織は、供給者のサービス提供を定常的に監視し、レビューし、監査する。

15.2.1.1 / 15.2.1.2 / 15.2.1.3 / 15.2.1.4 / 15.2.1.5 / 15.2.1.6 / 15.2.1.7 / 15.2.1.8 / 15.2.1.9 / 15.2.1.10 / 15.2.1.11 / 15.2.1.12 / 15.2.1.13 / 15.2.1.14 / 15.2.1.15は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

15.2.2　関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理する。

15.2.2.1 / 15.2.2.2 / 15.2.2.3は、「情報セキュリティ管理基準」の「管理策基準」に同

---

[25] 役割及び責任には、次のプロセスを含むことができる。
- マルウェア防御
- バックアップ
- 暗号による管理策
- ぜい弱性管理
- インシデント管理
- 技術的順守状況の点検
- セキュリティの試験
- 監査
- ログ及び監査証跡を含む証拠の収集、維持及び保護
- 認証及びアクセス制御
-本人確認及びアクセス管理

じ。

16　情報セキュリティインシデント管理

16.1　情報セキュリティインシデントの管理及びその改善

目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

16.1.1　情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。

16.1.1.1 / 16.1.1.2 / 16.1.1.3 / 16.1.1.4 / 16.1.1.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.1.13.C　クラウドサービス利用者は、情報セキュリティインシデント管理の責任の割当てを検証し、クラウドサービス利用者の要求事項を満たすことを確実にする仕組みを整備する。

16.1.2　情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。

16.1.2.1 / 16.1.2.2 / 16.1.2.3 / 16.1.2.4 / 16.1.2.5 / 16.1.2.6 / 16.1.2.7 / 16.1.2.8 / 16.1.2.9 / 16.1.2.10は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.2.14.C　クラウドサービス利用者は、クラウドサービス提供者に、クラウドサービス利用者が検知した情報セキュリティ事象をクラウドサービス提供者に報告するための仕組みについての情報を要求する。

16.1.2.15.C　クラウドサービス利用者は、クラウドサービス提供者に、クラウドサービス提供者が検知した情報セキュリティ事象をクラウドサービス利用者に報告するための仕組みについての情報を要求する。

16.1.2.16.C　クラウドサービス利用者は、クラウドサービス提供者に、クラウドサービス利用者が報告された情報セキュリティ事象の状況を追跡するための仕組みについての情報を要求する。

16.1.3　組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。

16.1.3.1 / 16.1.3.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.4　情報セキュリティ事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定する。

16.1.4.1 / 16.1.4.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.5　情報セキュリティインシデントは、文書化した手順に従って対応する。

16.1.5.1 / 16.1.5.2 / 16.1.5.3 / 16.1.5.4 / 16.1.5.5 / 16.1.5.6 / 16.1.5.7 / 16.1.5.8 / 16.1.5.9は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.6　情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。

16.1.6.1 / 16.1.6.2は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.7　組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。

16.1.7.1 / 16.1.7.2 / 16.1.7.3 / 16.1.7.4 / 16.1.7.5 / 16.1.7.6 / 16.1.7.7 / 16.1.7.8 / 16.1.7.9 / 16.1.7.10 / 16.1.7.11 / 16.1.7.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

16.1.7.14.C　クラウドサービス利用者は、クラウドサービス提供者と、クラウドコンピューティング環境内の潜在的なディジタル形式の証拠、又はその他の情報の要求に対応する手順を合意する。

17　事業継続マネジメントにおける情報セキュリティの側面

17.1　情報セキュリティ継続

目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため。

17.1.1　組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。

17.1.1.1 / 17.1.1.2 / 17.1.1.3 / 17.1.1.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

17.1.2　組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持する。

17.1.2.1 / 17.1.2.2 / 17.1.2.3 / 17.1.2.4 / 17.1.2.5 / 17.1.2.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

17.1.3　確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で妥当かつ有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証する。

17.1.3.1 / 17.1.3.2 / 17.1.3.3 / 17.1.3.4は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

17.2　冗長性

目的：情報処理施設の可用性を確実にするため。

17.2.1　情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。

17.2.1.1 / 17.2.1.2 / 17.2.1.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18　順守

18.1　法的及び契約上の要求事項の順守

目的：情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

18.1.1　各情報システム及び組織について、全ての関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組みを、明確に特定し、文書化し、また、最新に保つ。

18.1.1.1 / 18.1.1.2 / 18.1.1.3は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.1.8.C　クラウドサービス利用者は、関連法令及び規制が、クラウドサービス利用者の法的管轄区域のものに加え、クラウドサービス提供者の法的管轄区域のものもある可能性について確認する。

18.1.1.9.C　クラウドサービス利用者は、クラウドサービス利用者の事業に要求される関連規制及び標準類を、クラウドサービス提供者が順守している証拠[26]を要求する。

18.1.2　知的財産権及び権利関係のあるソフトウェア製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするための適切な手順を実施する。

18.1.2.1 / 18.1.2.2 / 18.1.2.3 / 18.1.2.4 / 18.1.2.5 / 18.1.2.6 / 18.1.2.7 / 18.1.2.8 / 18.1.2.9 / 18.1.2.10 / 18.1.2.11 / 18.1.2.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.2.14.C　クラウドサービス利用者は、使用許諾のあるソフトウェアをクラウドサービスにインストールする[27]ことを許可する前に、クラウド固有の使用許諾に関する要求事項を特定する手順を備える。

18.1.2.15.C　クラウドサービス利用者は、クラウドサービスに柔軟性や拡張性があり、ソフトウェアが、使用許諾によって許可された以上のシステム又はプロセッサコアの上で動作可能な場合には、特に注意して確認する。

18.1.3　記録は、法令、規制、契約及び事業上の要求事項に従って、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護する。

18.1.3.1 / 18.1.3.2 / 18.1.3.3 / 18.1.3.4 / 18.1.3.5 / 18.1.3.6 / 18.1.3.7 / 18.1.3.8 / 18.1.3.9 / 18.1.3.10 / 18.1.3.11 / 18.1.3.12は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.3.14.C　クラウドサービス利用者は、クラウドサービス提供者に、クラウドサービスの利用に関して、クラウドサービス提供者が収集し、蓄積する記録の保護について、情報を要求する。

18.1.4　プライバシー及びPIIの保護は、関連する法令及び規制が適用される場合には、その要求に従って確実に行う。

18.1.4.1 / 18.1.4.2 / 18.1.4.3 / 18.1.4.4 / 18.1.4.5 / 18.1.4.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.5　暗号化機能は、関連する全ての協定、法令及び規制を順守して用いる。

18.1.5.1 / 18.1.5.2 / 18.1.5.3 / 18.1.5.4 / 18.1.5.5 / 18.1.5.6は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.1.5.8.C　クラウドサービス利用者は、クラウドサービスの利用において適用する暗号による一連の管理策が、関連する協定、法令及び規制を順守していることを検証する。

18.2　情報セキュリティのレビュー

目的：組織の方針及び手順に従って情報セキュリティが実施され、運用されることを確実にするため。

18.2.1　情報セキュリティ及びその実施の管理（例えば、情報セキュリティのための管理目的、管理

---

[26] そのような証拠は、第三者の監査人によって提出された証明書としてもよい。

[27] 商用の使用許諾のあるソフトウェアをクラウドサービスにインストールすることは、そのソフトウェアの許可条件の違反をもたらしかねない。

策、方針、プロセス、手順）に対する組織の取組みについて、あらかじめ定めた間隔で、又は重大な変化が生じた場合に、独立したレビューを実施する。

18.2.1.1 / 18.2.1.2 / 18.2.1.3 / 18.2.1.4 / 18.2.1.5 / 18.2.1.6 / 18.2.1.7 / 18.2.1.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.2.1.14.C　クラウドサービス利用者は、クラウドサービス提供者に、クラウドサービスの情報セキュリティ管理策及び指針の実施がクラウドサービス提供者の主張と一致することを示す文書化された証拠を要求する。

18.2.2　管理者は、自分の責任の範囲内における情報処理及び手順が、適切な情報セキュリティのための方針群、標準類、及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューする。

18.2.2.1 / 18.2.2.2 / 18.2.2.3 / 18.2.2.4 / 18.2.2.5 / 18.2.2.6 / 18.2.2.7 / 18.2.2.8は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

18.2.3　情報システムを、組織の情報セキュリティのための方針群及び標準の順守に関して、定めに従ってレビューする。

18.2.3.1 / 18.2.3.2 / 18.2.3.3 / 18.2.3.4 / 18.2.3.5は、「情報セキュリティ管理基準」の「管理策基準」に同じ。

付録２

クラウドコンピューティングのリスク

付録2　クラウドコンピューティングのリスク

下表は、経済産業省委託事業 平成２３年度企業・個人の情報セキュリティ対策促進事業 （グローバルなクラウドセキュリティ監査の利用促進）によるものである。

番号	リスクの識別名	リスクの具体的内容
H01	リソース・インフラの高集約によるインシデントの影響の拡大	・仮想化技術は、１台の物理ホストにｎ台の仮想マシンを集約することで、リソースの利用効率をｎ倍に高める一方、障害発生時の影響もｎ倍に拡大する。また、データセンタの大規模利用は、１か所のデータセンタに多数の利用者を収容することで、インフラの利用効率を高める一方、データセンタ内の障害発生時の影響も拡大する。例えば、データセンタ内のネットワークの設定ミスが、クラウドシステムの大半の機能を停止させ、大規模障害が発生するリスクがある。
H02	仮想／物理の設計・運用の不整合	・仮想化技術は、キャパシティのオーバーサブスクリプションを可能にするため、仮想リソースの総和と物理リソースの総和は一致するとは限らない、ソフトウェアと物理ホストが一対一対応しない、 仮想スイッチと物理スイッチのVLAN設計が異なるなど、従来のコンピュータ、ネットワークの設計・運用管理のノウハウが通用しないことが多い。仮想/物理にまたがるコンピュータとネットワークの大規模化・複雑化によって、予期せぬ不具合、大規模障害が発生するリスクがある。
H03	他の共同利用者の行為による信頼の喪失	・他のユーザの活動により、同じクラウドサービスを利用するユーザのIPアドレスが外部サービスによりブロックされる。 ・他のユーザの活動により、利用していたストレージが押収されてサービスの継続が困難になる。
H04	リソースの枯渇	・クラウドサービス提供者の予想を超えるユーザの需要増により、インフラやリソースがユーザの需要を満たせずサービスに支障が生ずることで、ユーザの減少や評判の低下を招く。 ・上記のリスクを回避するためにリソースを増強することで、場合によっては過剰投資として収益性を低下させる。
H05	隔離の失敗	・クラウドサービスを構成するメカニズムの不備・欠陥や脆弱性への攻撃により、異なるユーザやサービス間の隔離が失われることで、ユーザの機密情報の漏えいなどが生じ、事業者の評判が失墜する。
H06	サービスエンジンの侵害	・脆弱性等を通じてサービスエンジンの制御を奪われることで、クラウドサービスに特化した攻撃（サービスエンジン経由の情報漏えい、リソースの逼迫化によるサービスのマヒ等）が行われる可能性がある。
M07	クラウドプロバイダでの内部不正－特権の悪用	・クラウドサービス提供者における従業員の悪意の行動が、あらゆるクラウドサービスに影響を及ぼす。 ・従業員が犯罪組織の標的とされ、上記の行動を行う。
M08	管理用インタフェースの悪用	・クラウドサービスのユーザ向けに、インターネットからリソース制御を可能とするインタフェースが悪用され、サービス全体に影響を及ぼす。 ・クラウドサービス提供者の管理者の制御用インタフェースも同様に悪用されることで、さらなる影響を及ぼす。

M09	データ転送途上における攻撃、データ漏えい	・ユーザ環境とクラウドサービス、もしくは分散されたクラウドサービス相互間でのデータ転送機会が生ずることで、その転送中のデータの漏えいのリスクが生じる。
M10	セキュリティが確保されていない、または不完全なデータ削除	・ストレージやバックアップテープ等の物理媒体を他のユーザと共用する場合、媒体には常時複数ユーザのデータが記録されるため、特定ユーザのデータだけを消去する目的で、その媒体を物理的に破壊することはできない。
M11	クラウド内DDoS/DoS攻撃	・悪意のユーザもしくはユーザ環境の乗っ取り等を通じて同じクラウドサービス内を起点とするDDoS/DoS攻撃が行われることで、インターネット経由の場合よりも大きな被害がユーザに発生する。
L12	ロックインによるユーザの忌避	・クラウドプロバイダが、外部リソースを利用してユーザデータを保護する必要性が生じても、相互接続性がないために、データ移行ができない。 （注）本リスクはENISAではユーザにとっての「ロックインされてしまう」リスクとして整理されているが、ここではクラウドサービス提供者視点で扱う。
L13	ガバナンスの喪失	・クラウドを利用することで、ユーザが下位層を対象としたガバナンス（自社ポリシーに基づくアクセス制御、ログ管理、監査実施等）を失うことのリスクを憂慮し、クラウド利用を躊躇する。 （注）本リスクはENISAではユーザにとっての「ロックインされてしまう」リスクとして整理されているが、ここではクラウドサービス提供者視点で扱っている。
L14	サプライチェーンにおける障害	・クラウドサービスにおける認証等のサービスを外部委託することで、その委託先サービスに脆弱性が存在するとクラウドサービス全体に影響が及ぶ可能性がある。 ・どの部分を外部委託しているかを明示しないことで、ユーザによるクラウドサービスへの信頼度が低下する。
L15	EDoS攻撃（経済的な損失を狙ったサービス運用妨害攻撃）	・悪意のユーザによるユーザアカウントの乗っ取り、従量制リソースの浪費等を通じて、ユーザに経済的損失をもたらす。 （注）ENISAガイドラインにない追記： 同様の被害は、ユーザの過失（プログラムの欠陥、設計ミス）によっても生じる可能性がある。
L16	事業者が管理すべき暗号鍵の喪失	・悪意の関係者により、クラウドサービス提供者が管理すべき暗号鍵が不正利用されることで、ユーザの機密データの漏えいが生ずる。 ・クラウドサービス提供者が暗号鍵を喪失することでデータの復号が困難となり、ユーザのデータにおける完全性が損なわれる。
L17	不正な探査・スキャンの実施	・攻撃のためのデータ収集が、クラウドサービスの環境を通じて、より容易に行われる可能性がある。
L18	証拠提出命令と電子的証拠開示	・クラウドサービス上にデータが集中することで、司法当局によるデータの押収が行われた場合に、開示したくないデータまで開示されるリスクが増大するため、ユーザによるクラウドサービス利用を躊躇させる要因となる可能性がある。
L19	司法権の違い	・クラウドサービスの物理的インフラが設置される地域（国、州など）によっては、異なる司法上の解釈や独裁的な警察権力、国際的取り決めが遵守されないなどの影響がユーザに及ぶ可能性がある。

L20	データ保護	・クラウドサービス事業者が、ユーザが許可していないデータの処理を行う可能性があることで、ユーザがクラウド利用を躊躇する可能性がある。 ・ユーザが合法的でない方法で収集したデータが、クラウドサービス上に蓄積される可能性がある。
L21	ライセンス	・同一期間内に同じ数のマシンを使用していた場合でも、他のソフトウェアに比べてクラウドサービス利用者のライセンス費用は飛躍的に増大することがある。 ・PaaSやIaaSの場合は、クラウド内部で発生した独自の成果物（新しいアプリケーションやソフトウェア等）がユーザの知的財産として保護されない可能性がある。