暗号化消去システム認証 for Cloud
CE-C 認証基準ガイドライン
第 1.0 版

データ適正消去実行証明協議会

はじめに

総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」では、ISMAP（政府情報システムのためのセキュリティ評価制度）と同様に、クラウドサーバ上の仮想サーバ（論理ボリューム）のデータ消去には、暗号化消化が要求されている。暗号化消去を成立させるためには、対象となる論理データや暗号鍵の管理が適切に行われいるかを確認及び証明することが求められる。

技術的な確認及び証明は、当検証・制度確立前に実施された実証実験により、ログ管理が有効であることが確認及び証明されたが、暗号化消去を成立させるための暗号化と鍵の管理プロセスに関しては問題が多く、解決のためには、当事者を中心とした検討が必要であった。

そこで、2023 年 3 月、クラウドサービス・プロバイダ認証基準ワーキンググループが組織され、暗号化消去を実運用するための暗号化及び鍵管理における、次の業務プロセスの定義を策定するに至った。

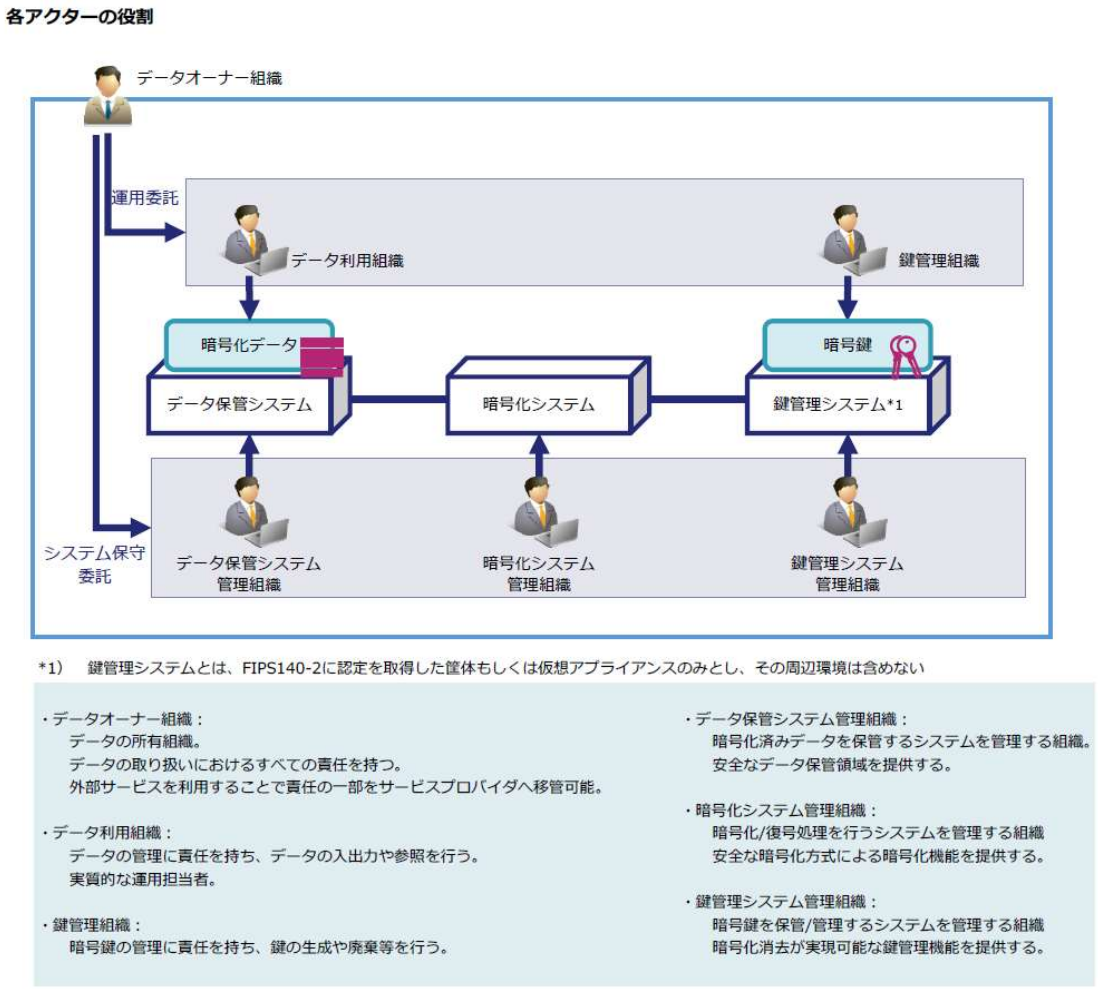
・クラウド仮想化サーバ上のデータ暗号化運用体制の標準化
・データ暗号化設定時の暗号鍵の管理方法及び運用体制の標準化
・上記を踏まえた、暗号鍵管理プロセスに関するチェックリスト策定

目次

各アクターの役割

暗号鍵消去を考える上で、データオーナー、データ保管システム、暗号化システム、鍵管理システムの各アクターの役割を考える必要がある。

下記の図は、当該各アクターの定義と役割を示したものである。



暗号化消去クラウドサービス・プロバイダ認証基準における各システムの定義

1. データ保管システムとは、暗号化された後のデータが保存されるためのシステムを指す。
2. 暗号化システムとは、データ保管システムの不揮発媒体にデータを書く前に暗号化処理を行うためのシステムを指す。
3. 鍵管理システムとは、暗号化システムが暗号・復号に利用する鍵を管理するシステムを指す。

A. データオーナー

審査要件

A.データオーナー

A.1.セキュリティポリシー **A.1.1.** **鍵管理システム管理組織はデータを保護するためのセキュリティポリシーを確立すること。セキュリティポリシーには以下を明記すること。** **a）組織の目的に対して適切である。** **b） 情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示す。** **c） 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。** **d）鍵情報や暗号化データに対するアクセス制御方針**

指針の解説

セキュリティポリシーは、データオーナー組織として、暗号化消去における最上位の考え方を組織の外部及び内部に向けた表明である。このような観点より、上記 a）～d）を考慮したセキュリティポリシーを策定することが望ましい。

適切性の確保：

セキュリティポリシーは、組織の目的に対して適切であり、鍵管理システムの目的と一致していることが望ましい。

情報セキュリティ目的の明示：

セキュリティポリシーは、情報セキュリティの目的を明示し、鍵管理システムがデータを保護し、機密性や完全性を確保するための枠組みを提供することが望ましい。

コミットメントの表明：

セキュリティポリシーには、情報セキュリティに関連する適用される要求事項を満たすことへの組織全体のコミットメントが含まれる。組織は、セキュリティポリシーの実施と遵守に必要なリソースやサポートを提供することを約束することが望ましい。

アクセス制御方針の定義：

セキュリティポリシーには、鍵情報や暗号化データに対するアクセス制御方針が明確に定義されることが望ましい。アクセス制御方針は、認証、認可、および監査のプロセスを含み、機密性を維持するための適切な手順を提供することが望ましい。

変更管理と監査：
セキュリティポリシーは、変更管理プロセスを定義し、セキュリティ要件の変化や新たな脅威に対処するためのメカニズムを提供する。ポリシーの監査と評価は定期的に行われ、ポリシーが効果的かつ適切に実施されていることを確認することが望ましい。

教育と啓発：
セキュリティポリシーは、組織内外の関係者に向けて教育と啓発を行うための資源やプログラムを提供する。全ての関係者がセキュリティポリシーを理解し、遵守することが重要であり、適切なトレーニングや情報提供をすることが望ましい。

A.2.システム構成、体制、役割

A.2.1.

データオーナー組織は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者または作業を委託する別組織の役割や責任及び体制について確認できる文書を用意すること。

指針の解説

システム構成、体制、役割は、データオーナー組織として、暗号化消去におけるシステム構成、体制、役割を明確にすることである。システム構成、体制、役割は、各種規程、体制図等で明確にすることが望ましい。このような観点より、以下を考慮したシステム構成、体制、役割を明確にすることが望ましい。

役割と責任の明確化：
データオーナー組織は、鍵情報や暗号化データに関する作業を行う自組織の作業者や、作業を委託する別組織の役割と責任を明確に定義すること。各作業者や組織が担当する業務内容や責任範囲、連絡先などを含む文書を用意することが望ましい。

体制の整備：
データオーナー組織は、鍵情報や暗号化データに関する作業やシステム設定を行うための適切な体制を整備する。体制には、必要な資源や権限、監督体制、連絡先情報などが含まれることが望ましい。

文書の作成：

鍵情報や暗号化データに関する作業やシステム設定に関する役割や責任、体制について確認できる文書を作成する。文書はわかりやすく、具体的な情報を含み、関係者が容易にアクセスできる場所に保管されることが望ましい。

定期的なレビューと更新：
文書は定期的にレビューされ、必要に応じて更新されること。変更があった場合や新たな要員が加わった場合など、文書の内容に変更が生じた際には、迅速に更新することが望ましい。

関係者への通知と教育：
関係者に対して、鍵情報や暗号化データに関する作業や体制についての文書を適切に通知し、説明すること。関係者が自らの役割や責任を理解し、適切に業務を遂行できるようにするために、必要な教育やトレーニングを実施することが望ましい。

A.2. システム構成、体制、役割
A.2.2.
データオーナー組織は、鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できる文書を用意すること。

指針の解説
データオーナー組織は、鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できる文書を用意すること。これらの文書は、該当システムの構成図等で明確にすることが望ましい。このような観点より、以下を考慮した鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できることを文書化することが望ましい。

システム構成の明確化：
データオーナー組織は、鍵情報や暗号化データを取り扱うシステムの構成を明確に文書化する。これらの文書には、システムのハードウェア、ソフトウェア、ネットワーク構成などが含まれていることが望ましい。

データフローの記述：
鍵情報や暗号化データの取り扱いに関するデータフローを記述する。データの生成元から保存、処理、転送、削除までの手順やプロセスが明確に記載されることが望ましい。

セキュリティ対策の説明：

システムの構成やデータフローに関連するセキュリティ対策が文書に含まれること。
アクセス制御、暗号化、監査ログの設定など、セキュリティを強化するための具体的な措置が記載されることが望ましい。

システム間の統合と依存関係の説明：
鍵情報や暗号化データを取り扱うシステムが他のシステムとどのように統合されているか、および依存関係があるかを明確に説明すること。他のシステムとのデータのやり取りや、データの共有方法などが示されることが望ましい。

文書のアップデートとレビュー：
文書は定期的にレビューされ、必要に応じてアップデートされること。システムの変更やアップグレード、新たなセキュリティ要件の追加などがあった場合には、文書も適切に更新されることが望ましい。

関係者への共有と教育：
システム構成やデータフローに関する文書は関係者に適切に共有され、理解されるようにすること。関係者がシステムの構成やデータフローを把握し、セキュリティ上の重要性を理解できるようにするために、適切な教育やトレーニングを提供することが望ましい。

A.2. システム構成、体制、役割
A.2.3.
データオーナー組織は、鍵情報や暗号化データを取り扱う以下のシステムについて、管理する組織が確認できる文書を用意すること。
・データ保管システム管理組織
・暗号化システム
・鍵管理システム管理組織

指針の解説
データオーナー組織は、鍵情報や暗号化データを取り扱うデータ保管システム管理組織、データ保管システム管理組織、暗号化システム、鍵管理システム管理組織システムについて、管理する組織が確認できる文書を用意することが望ましい。これらの文書は、各種規程、該当システムの構成図等で明確にすることが望ましい。このような観点より、以下を考慮したステム管理組織、データ保管システム管理組織、暗号化システム、鍵管理システム管理組織が確認できることを文書化することが望ましい。

文書の作成：
データオーナー組織は、鍵情報や暗号化データを取り扱う各システムに関する管理文書を作成すること。これには、データ保管システム管理組織、暗号化システム、鍵管理システム管理組織に関する情報が含まれることが望ましい。

各システムの役割と責任の明確化：
文書には、各システムが担う役割と責任が明確に記載されることが望ましい。データ保管システム管理組織の役割、暗号化システムの機能、鍵管理システム管理組織の責任などが含まれることが望ましい。

システムの構成とデータフローの説明：
各システムの構成やデータフローに関する情報が詳細に記述されること。データの流れ、処理手順、保管場所、システム間の相互作用などが明確に示されることが望ましい。

セキュリティ対策と規制遵守の確認：
文書には、各システムが採用するセキュリティ対策や遵守すべき規制が明確に記載されることが望ましい。アクセス制御、暗号化アルゴリズム、監査要件などが具体的に述べられることが望ましい。

文書の定期的な更新とレビュー：
管理文書は定期的にレビューされ、必要に応じて更新されること。システムの変更や新たなセキュリティ上の脅威に対処するために、文書が最新の状態に保たれることが望ましい。

関係者への共有と教育：
管理文書は関係者に適切に共有され、理解されるようにすること。関係者が各システムの役割やセキュリティ上の重要性を理解できるように、適切な教育やトレーニングを提供することが望ましい。

A.3. 経営陣の責任

A.3.1.

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者または作業を委託する別組織に対し、アクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備すること。

指針の解説

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者または作業を委託する別組織に対し、アクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備すること。整備方法としては、役割責任表などが考えられる。これらの役割責任の整備方法には、以下を考慮することが望ましい。

役割と責任の明確化：

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業を行う作業者や、作業を委託する別組織に対して、情報セキュリティの役割と責任を明確に伝えること。各作業者が担当する役割や責任範囲、セキュリティ上の重要性を理解するための具体的な要点が含まれることが望ましい。

教育と啓発のプログラム：

データオーナー組織の経営陣は、情報セキュリティの役割と責任に関する教育と啓発プログラムを整備すること。これには、定期的なセキュリティトレーニング、セキュリティ意識向上のキャンペーン、具体的なシナリオに基づいたトレーニングなどが含まれることが望ましい。

コミュニケーション手段の確立：

情報セキュリティの役割と責任に関する要点を適切に伝えるためのコミュニケーション手段を確立すること。これには、会議、ワークショップ、メール、社内ポータルなどのコミュニケーション手段が活用されることが望ましい。

アクセス権限の付与前の確認：

アクセスが許可される前に、情報セキュリティの役割と責任に関する要点が理解されたことを確認するためのプロセスを確立すること。アクセス権限の付与や特権の委任は、適切なトレーニングや認識確認の手順に基づいて行われることが望ましい。

遵守の強調：
データオーナー組織の経営陣は、情報セキュリティの役割と責任に関する要点を伝える際に、遵守の重要性を強調すること。適切な手順やポリシーに従うことが、組織のセキュリティと信頼性を確保する上で不可欠であることを明確に伝えることが望ましい。

A.3. 経営陣の責任
A.3.2.
データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備すること。

指針の解説
データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備すること。整備方法としては、データオーナー組織の経営陣が作業者に対して、経営方針などで明確にすることが考えられる。これらの整備方法には、以下を考慮することが望ましい。

期待される行動と責任の明確化：
データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業を行う自組織の作業者に対し、情報セキュリティに関する期待される行動と責任を明確に示すこと。これには、セキュリティポリシーと規定、ベストプラクティスへの遵守、機密性やデータの完全性の維持などが含まれることが望ましい。

役割と責任の説明：
各作業者の役割と責任が明確に定義され、情報セキュリティの観点から期待される役割が明示されること。作業者が自らの責任を理解し、適切な行動を取るための指針が提供されることが望ましい。

リスク管理と対応策の提案：
データオーナー組織の経営陣は、情報セキュリティリスクの認識と管理に関する期待を示すこと。リスクに対する適切な対応策やセキュリティ上の改善策の提案が作業者に提示されることが望ましい。

コミュニケーションと教育：
情報セキュリティに関する指針は、適切なコミュニケーション手段を通じて作業者に伝達されること。適切な教育とトレーニングが提供され、作業者が情報セキュリティに関する指針を理解し、実践できるように支援されることが望ましい。

フィードバックと改善のプロセス：
データオーナー組織の経営陣は、情報セキュリティに関する指針や期待に対するフィードバックを受け入れ、適切な改善のプロセスを確立すること。作業者からのフィードバックを活用し、指針やプロセスを改善していくための仕組みが整備されることが望ましい。

A.3. 経営陣の責任

A.3.3.

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備すること。

指針の解説

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備すること。整備方法には、以下を考慮することが望ましい。

方針の明確な伝達：
データオーナー組織の経営陣は、組織の情報セキュリティの方針群を明確に定義し、作業者に伝達すること。方針は簡潔で理解しやすく、作業者が容易に把握できる形式で提示されることが望ましい。

方針の重要性の強調：
情報セキュリティの方針の重要性を作業者に強調し、組織のセキュリティ文化を醸成すること。データ漏洩やサイバー攻撃などのリスクについての意識向上を促進し、方針の重要性を理解させることが望ましい。

動機付けと報奨制度の導入：
作業者が情報セキュリティの方針に従うように動機付けるために、適切な報奨制度やイン

センティブを導入することが望ましい。優れたセキュリティ実践に対する報酬や賞賛、昇進の機会などを提供し、方針への適合を奨励することが望ましい。

教育とトレーニングの提供：
情報セキュリティの方針に関する教育とトレーニングを作業者に提供すること。方針の理解と実践を支援するための継続的なトレーニングプログラムが実施されることが望ましい。

遵守の監視と評価：
方針の遵守を監視し、評価する仕組みを導入すること。リアルタイムの監視や定期的な評価を通じて、作業者が情報セキュリティの方針に適切に準拠していることを確認することが望ましい。

フィードバックと改善のプロセス：
作業者からのフィードバックを受け入れ、方針やプロセスの改善を促進すること。セキュリティ方針の改善により、作業者のモチベーションとセキュリティへのコミットメントを高めることが望ましい。

A.3. 経営陣の責任

A.3.4.

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備すること。

指針の解説

データオーナー組織の経営陣は、データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備すること。整備方法には、以下を考慮することが望ましい。

役割と責任の明確化：
データオーナー組織の経営陣は、自らの役割と責任が情報セキュリティに与える影響を明確に理解すること。役割と責任が定義され、情報セキュリティへの関与が明示されることが望ましい。

情報セキュリティのトレーニングと教育：
経営陣は、情報セキュリティに関するトレーニングと教育プログラムに参加し、適切な知識とスキルを身につけること。情報セキュリティの重要性や最善の実践方法についての理解を深めるための機会が提供されることが望ましい。

情報セキュリティ方針の策定と遵守：
経営陣は、情報セキュリティ方針の策定と遵守に積極的に関与すること。方針に従い、情報セキュリティに関連する決定を行い、その遵守を監督することが望ましい。

リーダーシップとモデルへの影響力：
経営陣は、情報セキュリティに対するリーダーシップを発揮し、組織内でモデルとなる行動を示すこと。モデルとなる行動は、作業者に情報セキュリティの重要性を示し、組織全体の文化を形成されることが望ましい。

情報セキュリティへのコミットメントの強調：
経営陣は、情報セキュリティへのコミットメントを強調し、組織内でその重要性を定期的に確認すること。情報セキュリティの課題や成果に関する定期的な報告を通じて、コミットメントを示すことが望ましい。

評価と改善のプロセス：
経営陣は、自らの情報セキュリティ認識の水準を評価し、改善するためのプロセスを確立すること。フィードバックを受け入れ、個人としての成長と組織全体のセキュリティ能力向上を目指すことが望ましい。

A.3. 経営陣の責任

A.3.5.

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備すること。

指針の解説

データオーナー組織の経営陣は、データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備すること。整備

方法には、以下を考慮することが望ましい。

情報セキュリティ方針の伝達：
データオーナー組織の経営陣は、情報セキュリティ方針を作業者に明確に伝達し、理解されるようにすること。方針は雇用条件の一部として提示され、作業者がそれに従うことが求められることが望ましい。

適切なトレーニングと教育：
作業者には、情報セキュリティに関する適切なトレーニングと教育が提供されること。方針に従うための具体的な指導や実践的なトレーニングが行われ、作業者が情報セキュリティに関するスキルを習得することが望ましい。

雇用条件の明確化：
雇用条件には、情報セキュリティ方針と遵守することが明記されること。作業者は、雇用契約や規則で情報セキュリティ方針に同意し、それに従うことが雇用の条件とされることが望ましい。

モニタリングと評価：
組織は、作業者の情報セキュリティ方針への遵守を定期的にモニタリングし、評価すること。適切な方針の遵守が保証されるよう、監視手段や評価プロセスが整備されることが望ましい。

フィードバックと改善：
作業者からのフィードバックを受け入れ、情報セキュリティ方針や適切な仕事のやり方に関する改善を実施すること。組織は、作業者が方針に関して疑問や提案を持つ場合に対処し、方針を改善していく仕組みを構築することが望ましい。

報酬と評価の連動：
作業者の報酬や評価には、情報セキュリティ方針への遵守や適切な仕事のやり方への貢献が考慮されること。情報セキュリティに対する適切な取り組みが報酬や昇進の要因として反映されるよう、評価システムが整備されることが望ましい。

A.3. 経営陣の責任

A.3.6.

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備すること。

指針の解説

データオーナー組織の経営陣は、データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備すること。整備方法には、以下を考慮することが望ましい。

技能と資格の要件の明確化：

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業を行う作業者に対し、適切な技能と資格を保持することを要件とすること。必要な技能や資格は明確に定義され、作業者がそれらを維持することが求められることが望ましい。

定期的な教育プログラムの提供：

経営陣は、定期的な教育プログラムを作業者に提供し、最新の情報セキュリティのトレンドやベストプラクティスを学ぶ機会を提供すること。教育プログラムは、情報セキュリティに関する基礎知識から高度なスキルまで包括的な内容をカバーし、作業者の能力向上を促進することが望ましい。

業界標準や規制に対する遵守：

経営陣は、業界標準や規制に基づいた情報セキュリティの要件を遵守するための教育プログラムを提供すること。作業者が業界の最新の規制や規制に関する変更に対応できるよう、定期的なトレーニングが実施されることが望ましい。

技能向上の奨励：

経営陣は、作業者の技能向上を奨励し、学習と成長を促進すること。優れた成果やスキル向上に対する報酬や昇進の機会を提供することで、作業者のモチベーションを高めることが望ましい。

定期的なスキル評価とフィードバック：

経営陣は、作業者のスキルレベルを定期的に評価し、フィードバックを提供すること。フィ

ードバックは、作業者が自己評価し、改善するための指針となることが望ましい。

A.3. 経営陣の責任

A.3.7.

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、セキュリティに関することや、暗号鍵に対する教育、力量を定期的に実施していること。

指針の解説

データオーナー組織の経営陣は、データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、セキュリティに関することや、暗号鍵に対する教育、力量を定期的に実施していること。実施方法には、以下を考慮することが望ましい。

定期的なセキュリティ教育プログラムの実施：
データオーナー組織の経営陣は、作業者に対してセキュリティに関するトピックについて定期的な教育プログラムを実施すること。教育プログラムは、情報セキュリティの基本原則、セキュリティポリシー、最新の脅威や攻撃手法に関する知識を提供されることが望ましい。

暗号鍵に関する教育とトレーニング：
作業者には、暗号鍵の生成、管理、交換、保存などに関する教育とトレーニングが提供されること。暗号鍵の重要性や適切な取り扱い方法についての理解を深めるための具体的な指導が行われることが望ましい。

セキュリティ実践の定期的な評価：
経営陣は、作業者のセキュリティ実践力を定期的に評価し、向上のためのフィードバックを提供すること。評価は、実際の作業やシミュレーションを通じて行われ、作業者のセキュリティスキルの向上を支援されることが望ましい。

最新のセキュリティトレンドに関する教育：
作業者には、最新のセキュリティトレンドや脅威に関する教育が提供されること。新たな脅威や攻撃手法についての知識は定期的に更新され、作業者が常に最新の情報にアクセスできるようにすることが望ましい。

ポリシーと手順の継続的な強調：
経営陣は、セキュリティポリシーと手順の重要性を定期的に強調し、作業者がこれらを遵守することを促すこと。ポリシーと手順は、定期的に復習され、作業者が常に遵守することを確保することが望ましい。

A.3. 経営陣の責任
A.3.8.
データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組みを整備すること。

指針の解説
データオーナー組織の経営陣は、データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者に対し、情報セキュリティのための方針群又は手順への違反を報告するため、例えば、内部告発など、匿名の報告経路を提供する仕組みを整備すること。整備方法には、以下を考慮することが望ましい。

目的の明確化：
匿名の報告経路を整備する主な目的を明確に定義し、その目的を達成するための方針を策定することが望ましい。

法的要件の遵守：
匿名報告の仕組みを構築する際には、関連する法的要件や規制に従うことを確認すること。特に個人情報保護法などの適用を確認し、遵守することを重視することが望ましい。

報告プロセスの明確化：
匿名報告を行うためのプロセスを明確に定義すること。報告者がどのようにして報告を行うか、どのようにして匿名性が保たれるか、そして報告の受け手は誰かなど、プロセスのすべての側面を詳細に明記することが望ましい。

報告先の選定：
匿名報告を受け付ける組織内の担当者や部署を選定すること。報告先は信頼性が高く、情報を適切に処理し、適切な措置を講じることが期待される人物や部署であることが望ましい。

報告者の保護：
匿名報告者のプライバシーや安全を保護するための措置を講じること。これには、報告者の身元を特定できないような技術的手段の導入や、報告者への不当な処置を防ぐための法的保護の提供などが含まれることが望ましい。

報告の検証と対応：
受け取った報告を検証し、その内容に基づいて適切な対応を講じるプロセスを確立すること。報告された問題の深刻さや緊急性に応じて、迅速かつ適切な行動をとることが望ましい。

透明性と報告者へのフィードバック：
匿名報告プロセスの透明性を確保し、報告者に対して適切なフィードバックを提供することで、報告者が信頼を持って問題を報告し続けることを促すこと。報告の結果や対応策についての情報は、組織内で適切に共有されることが望ましい。

定期的な評価と改善：
匿名報告プロセスを定期的に評価し、必要に応じて改善を行うこと。報告された問題の解決やプロセスの効果を評価し、改善点を特定して、継続的なセキュリティの向上に取り組むことが望ましい。

A.3. 経営陣の責任

A.3.9.

データオーナー組織の経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動すること。

指針の解説

データオーナー組織の経営陣は、データオーナー組織の経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動すること。具体的な行動方法には、以下を考慮することが望ましい。

方針と手順の理解と支持：
経営陣は、情報セキュリティ方針や手順を十分に理解し、それらに対する明確な支持を表明すること。これには、情報セキュリティに関するトレーニングや教育プログラムへの参加を通じて、自身の理解を深めることを含むことが望ましい。

手本となる行動の実践：
経営陣は、情報セキュリティに関する最善の実践を自ら実践し、他の従業員に手本となる行動を示すこと。これには、パスワードの適切な管理、機密情報の適切な取り扱い、セキュリティポリシーへの遵守などを含めることが望ましい。

リーダーシップとコミュニケーション：
経営陣は、情報セキュリティに関するリーダーシップを発揮し、従業員に対してその重要性を常に強調すること。定期的なコミュニケーションや会議を通じて、情報セキュリティへの取り組みを推進し、関連する成功事例や重要なポイントを共有することが望ましい。

リスク管理と優先順位付け：
経営陣は、情報セキュリティリスクを理解し、それらに対する適切な優先順位付けを行うこと。リソースの配分や投資決定において、情報セキュリティの重要性を考慮し、適切な措置を講じることを求めることが望ましい。

透明性と責任：
経営陣は、情報セキュリティに関する透明性を確保し、関係者に対して責任を果たすことを約束すること。情報漏洩やセキュリティインシデントが発生した場合には、速やかに対処し、その結果や教訓を公正かつ透明に共有することが望ましい。

継続的な改善と学習：
経営陣は、情報セキュリティのプロセスと実践を継続的に改善し、組織全体のセキュリティ能力を向上させるために学び続ける姿勢を示すこと。業界の最新動向やベストプラクティスについて常に情報を収集し、組織に適用するための検討を行うことが望ましい。

A.4.委託先管理

A.4.1.

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を委託する別組織が、作業者に対して以下を整備していることを情報セキュリティのための方針群、手順及び管理策で確認すること。

- **組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組み**
- **組織の情報セキュリティのための方針群に従うように動機付ける仕組み**
- **組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組み**
- **組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組み**
- **適切な技能及び資格を保持し、定期的に教育を受けさせる仕組み**
- **情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組み**

指針の解説

データオーナー組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を委託する別組織が、作業者に対して、情報セキュリティについて期待することを示すための指針を提供する仕組みなどを整備すること。整備方法には、以下を考慮することが望ましい。

指針の提供：

別組織が作業者に対して情報セキュリティに関する役割や期待することを示す指針を提供していることを確認すること。これにより、作業者は自らの役割を理解し、適切なセキュリティプラクティスを遵守することが期待されることが望ましい。

動機付けの仕組み：

別組織や作業者が情報セキュリティ方針に従うように動機付ける仕組みを整備していることを確認すること。報奨制度や教育プログラム、適切なフィードバックメカニズムなどが含まれることが望ましい。

認識の向上：

別組織が作業者の情報セキュリティに関する認識を向上させるための仕組みを提供していることを確認すること。トレーニングや教育プログラム、評価や認定制度などが含まれるこ

とが望ましい。

雇用条件への準拠：
別組織や作業者が情報セキュリティ方針や適切な業務手順に従うようにするための雇用条件を整備していることを確認すること。これには、契約や規則、社内規程などが含まれることが望ましい。

教育と資格の提供：
別組織や作業者が適切な技能や資格を保持し、定期的に情報セキュリティに関する教育を受ける仕組みを提供していることを確認すること。これにより、作業者は最新のセキュリティプラクティスや技術について常に学び続けることが望ましい。

匿名報告経路の提供：
別組織が情報セキュリティ方針や手順への違反を報告するための匿名の報告経路を提供していることを確認すること。これにより、作業者はセキュリティに関する懸念や問題を匿名で報告しやすくすることが望ましい。

B. データ保管システム

B. データ保管システム

B. 1. セキュリティポリシー B. 1. 1. **鍵管理システム管理組織はデータを保護するためのセキュリティポリシーを確立すること。セキュリティポリシーには以下を明記すること。** **a) 組織の目的に対して適切である。** **b) 情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示す。** **c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。** **d) 鍵情報や暗号化データに対するアクセス制御方針**

指針の解説

セキュリティポリシーは、データ保管システムとして、暗号化消去における最上位の考え方を組織の外部及び内部に向けた表明である。このような観点より、以下を考慮したセキュリティポリシーを策定することが望ましい。

適切性の確保：
セキュリティポリシーは、組織の目的に対して適切であり、鍵管理システムの目的と一致していることが望ましい。

情報セキュリティ目的の明示：
セキュリティポリシーは、情報セキュリティの目的を明示し、鍵管理システムがデータを保護し、機密性や完全性を確保するための枠組みを提供することが望ましい。

コミットメントの表明：
セキュリティポリシーには、情報セキュリティに関連する適用される要求事項を満たすことへの組織全体のコミットメントが含まれる。組織は、セキュリティポリシーの実施と遵守に必要なリソースやサポートを提供することを約束することが望ましい。

アクセス制御方針の定義：
セキュリティポリシーには、鍵情報や暗号化データに対するアクセス制御方針が明確に定義されることが望ましい。アクセス制御方針は、認証、認可、および監査のプロセスを含み、機密性を維持するための適切な手順を提供することが望ましい。

変更管理と監査：
セキュリティポリシーは、変更管理プロセスを定義し、セキュリティ要件の変化や新たな脅威に対処するためのメカニズムを提供する。ポリシーの監査と評価は定期的に行われ、ポリシーが効果的かつ適切に実施されていることを確認することが望ましい。

教育と啓発：
セキュリティポリシーは、組織内外の関係者に向けて教育と啓発を行うための資源やプログラムを提供する。全ての関係者がセキュリティポリシーを理解し、遵守することが重要であり、適切なトレーニングや情報提供をすることが望ましい。

B.2. システム構成、体制、役割

B.2.1.

データ保管システム管理組織は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者または作業を委託する別組織の役割や責任及び体制について確認できる文書を用意すること。

指針の解説

システム構成、体制、役割は、データ保管システム管理組織として、暗号化消去におけるシステム構成、体制、役割を明確にすることである。システム構成、体制、役割は、各種規程、体制図等で明確にすることが望ましい。このような観点より、以下を考慮したシステム構成、体制、役割を明確にすることが望ましい。

役割と責任の明確化：
データ保管システム管理組織は、鍵情報や暗号化データに関する作業を行う自組織の作業者や、作業を委託する別組織の役割と責任を明確に定義すること。各作業者や組織が担当する業務内容や責任範囲、連絡先などを含む文書を用意することが望ましい。

体制の整備：
データ保管システム管理組織は、鍵情報や暗号化データに関する作業やシステム設定を行うための適切な体制を整備する。体制には、必要な資源や権限、監督体制、連絡先情報などが含まれることが望ましい。

文書の作成：
鍵情報や暗号化データに関する作業やシステム設定に関する役割や責任、体制について確

認できる文書を作成する。文書はわかりやすく、具体的な情報を含み、関係者が容易にアクセスできる場所に保管されることが望ましい。

定期的なレビューと更新：
文書は定期的にレビューされ、必要に応じて更新されること。変更があった場合や新たな要員が加わった場合など、文書の内容に変更が生じた際には、迅速に更新することが望ましい。

関係者への通知と教育：
関係者に対して、鍵情報や暗号化データに関する作業や体制についての文書を適切に通知し、説明すること。関係者が自らの役割や責任を理解し、適切に業務を遂行できるようにするために、必要な教育やトレーニングを実施することが望ましい。

B.2. システム構成、体制、役割
B.2.2.
データ保管システム管理組織は、鍵情報や暗号化データを取り扱うシステム及びその周辺環境の構成やデータフローが確認できる文書を用意すること。

指針の解説
データ保管システム管理組織は、鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できる文書を用意すること。これらの文書は、該当システムの構成図等で明確にすることが望ましい。このような観点より、以下を考慮した鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できることを文書化することが望ましい。

システム構成の明確化：
データ保管システム管理組織は、鍵情報や暗号化データを取り扱うシステムの構成を明確に文書化する。これらの文書には、システムのハードウェア、ソフトウェア、ネットワーク構成などが含まれていることが望ましい。

データフローの記述：
鍵情報や暗号化データの取り扱いに関するデータフローを記述する。データの生成元から保存、処理、転送、削除までの手順やプロセスが明確に記載されることが望ましい。

セキュリティ対策の説明：
システムの構成やデータフローに関連するセキュリティ対策が文書に含まれること。

アクセス制御、暗号化、監査ログの設定など、セキュリティを強化するための具体的な措置が記載されることが望ましい。

システム間の統合と依存関係の説明：
鍵情報や暗号化データを取り扱うシステムが他のシステムとどのように統合されているか、および依存関係があるかを明確に説明すること。他のシステムとのデータのやり取りや、データの共有方法などが示されることが望ましい。

文書のアップデートとレビュー：
文書は定期的にレビューされ、必要に応じてアップデートされること。システムの変更やアップグレード、新たなセキュリティ要件の追加などがあった場合には、文書も適切に更新されることが望ましい。

関係者への共有と教育：
システム構成やデータフローに関する文書は関係者に適切に共有され、理解されるようにすること。関係者がシステムの構成やデータフローを把握し、セキュリティ上の重要性を理解できるようにするために、適切な教育やトレーニングを提供することが望ましい。

B. 3. 経営陣の責任

B. 3. 1.

データ保管システム管理組織の経営陣は、作業者が鍵情報や暗号化データに関する作業、およびシステム設定へのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備すること。

指針の解説

データ保管システム管理組織の経営陣は、作業者が鍵情報や暗号化データに関する作業、およびシステム設定へのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備すること。整備方法としては、役割責任表などが考えられる。これらの役割責任の整備方法には、以下を考慮することが望ましい。

経営陣の役割と責任の明確化:
経営陣は情報セキュリティの重要性を理解し、その責任を認識すること。情報セキュリティポリシーの策定と維持に責任を持つことが望ましい。

作業者への教育と訓練:
作業者に対し、情報セキュリティの重要性と責任を定期的に教育し、訓練すること。鍵情報や暗号化データの取り扱い方法とシステムへのアクセス権限に関するガイドラインを提供することが望ましい。

情報セキュリティポリシーの普及:
情報セキュリティポリシーを組織内で普及させ、全ての作業者が理解し遵守することを確保すること。ポリシーの更新や変更があった場合は、適切に伝達し、理解を確認することが望ましい。

アクセスコントロールの強化:
鍵情報や暗号化データへのアクセスは、必要最小限の権限で制限すること。アクセス権限の与えられた作業者は、その権限の範囲内でのみ作業を行うことを徹底することが望ましい。

監査と評価:
情報セキュリティの実施状況を定期的に監査し、遵守状況を評価すること。監査結果に基づき、改善点を特定し、適切な対策を講じることが望ましい。

リスク管理と対応:
情報セキュリティに関連するリスクを評価し、適切な管理策を策定すること。セキュリティインシデントが発生した場合は、速やかに対応し、適切な措置を講じることが望ましい。

継続的な改善:
情報セキュリティの方針や手順を継続的に改善し、最新の脅威やベストプラクティスに対応すること。組織内の全てのメンバーが、情報セキュリティの向上に協力する文化を醸成することが望ましい。

B.3. 経営陣の責任

B.3.2.

データ保管システム管理組織の経営陣は、作業者に対し、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備すること。

指針の解説

データ保管システム管理組織の経営陣は、作業者に対し、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

経営陣のリーダーシップ:

経営陣は情報セキュリティの重要性を理解し、その重要性を従業員に示すことでリーダーシップを発揮すること。情報セキュリティに関する組織全体の方針や目標を明確に定義し、従業員に伝達することが望ましい。

情報セキュリティの期待の明確化:

経営陣は、従業員に対し、情報セキュリティに関する期待事項を具体的に示すこと。作業者には、データの取り扱い、アクセス権の管理、セキュリティポリシーの遵守などに関する具体的な指針を提供することが望ましい。

教育と訓練の提供:

情報セキュリティに関する教育と訓練プログラムを組織内で定期的に実施し、作業者の能力を向上させること。従業員が情報セキュリティポリシーを遵守し、セキュリティのベストプラクティスを理解するための機会を提供することが望ましい。

コミュニケーションの促進:

経営陣は、従業員とのコミュニケーションを通じて、情報セキュリティに関する重要な情報や変更事項を伝達すること。従業員は、情報セキュリティに関する懸念や提案を提出するための適切なチャネルを提供することが望ましい。

フィードバックと改善:

経営陣は、従業員からのフィードバックを受け入れ、情報セキュリティプロセスやポリシーの改善に活かすこと。継続的な監視と評価を通じて、情報セキュリティの効果を定期的に確認し、必要に応じて改善を行うことが望ましい。

遵守と報奨:

経営陣は、情報セキュリティポリシーの遵守を奨励し、従業員が適切なセキュリティ対策を実践することを評価すること。優れた情報セキュリティ実践に対する報奨制度を導入し、従業員のモチベーションを高めることが望ましい。

B.3. 経営陣の責任

B.3.3.

データ保管システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備すること。

指針の解説

データ保管システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

組織の情報セキュリティポリシーの明確化:

経営陣は、組織の情報セキュリティポリシーを明確に定義し、従業員に理解しやすい形で伝えること。ポリシーは、データ保管、アクセス管理、セキュリティプロトコルなどに関する具体的な方針を含むことが望ましい。

教育と意識向上の促進:

作業者に対し、情報セキュリティの重要性を定期的に強調し、意識向上を図る教育プログラムを実施すること。定期的なトレーニングやシミュレーションを通じて、セキュリティに関する最新の脅威や対策について従業員を啓発することが望ましい。

動機付けと報奨:

作業者が情報セキュリティポリシーに従うことを奨励する報奨制度を導入すること。遵守した場合の報奨や、セキュリティ違反を減らすことでチームや個人の評価に対するポジティブな影響を示すことが望ましい。

フィードバックと改善:

従業員からのフィードバックを受け入れ、ポリシーの実施に関する問題や提案を積極的に取り入れること。ポリシーの改善点や不明瞭な部分を特定し、適切な修正を行うことで、従業員の満足度と遵守率を向上させることが望ましい。

ロールモデルの示唆:

経営陣や管理職は、情報セキュリティポリシーを率先して遵守し、従業員に良いロールモデルを示すことが重要であること。従業員は、リーダーシップからのポジティブな影響を受け、ポリシーに積極的に従う傾向が高まることが望ましい。

継続的な監視と改善:
情報セキュリティポリシーの遵守状況を継続的に監視し、違反や問題を早期に検出すること。監視結果に基づいてポリシーの改善を行い、組織全体のセキュリティレベルを向上させることが望ましい。

B.3. 経営陣の責任
B.3.4.
データ保管システム管理組織の経営陣は、作業者に対し、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備すること。

指針の解説
データ保管システム管理組織の経営陣は、作業者に対し、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

役割と責任の明確化:
経営陣は、自らの情報セキュリティに関する役割と責任を明確に定義し、作業者に対して明示すること。各作業者の役割と責任が情報セキュリティの目標と一致していることを確認することが望ましい。

教育とトレーニングの提供:
情報セキュリティに関する教育プログラムやトレーニングを組織内で実施し、経営陣と作業者の両方に対して情報セキュリティに関する知識を向上させること。役割と責任に関連する情報セキュリティのトレーニングを提供し、一定の水準を達成するためのサポートを行うことが望ましい。

規定の策定と遵守の促進:
経営陣は、情報セキュリティポリシーと手順を策定し、それらの遵守を促進すること。自らの役割と責任に関連する情報セキュリティ規定を従業員に明確に伝え、その遵守を監視することが望ましい。

監査と評価:
情報セキュリティの実施状況を定期的に監査し、遵守水準を評価すること。監査結果に基づいて、必要な対策や改善点を特定し、適切な対応を講じることが望ましい。

透明性とコミュニケーション:
経営陣は、情報セキュリティに関する透明性を確保し、作業者とのコミュニケーションを促進すること。情報セキュリティに関する重要な変更や問題について、適切な情報を提供し、従業員からのフィードバックを受け入れることが望ましい。

継続的な向上:
経営陣は、情報セキュリティの向上に向けて継続的な取り組みを行い、一定水準を維持するだけでなく、常に向上を目指すこと。新たな脅威や技術の進展に対応するため、定期的な情報セキュリティの再評価と改善を行うことが望ましい。

B.3. 経営陣の責任

B.3.5.

データ保管システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備すること。

指針の解説

データ保管システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

情報セキュリティ方針の明確化:
経営陣は、組織の情報セキュリティ方針を明確に定義し、作業者に対して遵守を求めること。方針は、データの保護、アクセス管理、セキュリティ対策などに関する具体的なガイドラインを含むことが望ましい。

雇用条件への組み込み:
情報セキュリティ方針や適切な仕事のやり方を含む、情報セキュリティへの遵守が雇用条件として組み込まれること。作業者は雇用契約や規定を受け入れる際に、情報セキュリティ方針に同意することが求められることが望ましい。

教育とトレーニングの提供:
作業者に対し、情報セキュリティ方針や適切な仕事のやり方に関する教育プログラムやトレーニングを提供すること。新入社員や関連部署の従業員には、情報セキュリティの基本や方針に関する研修を実施することが望ましい。

遵守の監視と評価:
経営陣は、情報セキュリティ方針の遵守を定期的に監視し、適切な評価を行うこと。違反や問題が発生した場合には、適切な対応を講じ、必要に応じて改善を行うことが望ましい。

報奨とリワード:
情報セキュリティ方針への遵守や適切な仕事のやり方を実践する作業者には、報奨やリワードを与える制度を導入すること。優れた情報セキュリティ実践に対する認定や特典を提供し、作業者のモチベーションを高めることが望ましい。

継続的な改善:
情報セキュリティ方針や適切な仕事のやり方を継続的に改善し、組織のセキュリティレベルを向上させる取り組みを行うこと。ユーザーフィードバックや業界のベストプラクティスを活用して、常に最新の状況に適応することが望ましい。

B.3. 経営陣の責任
B.3.6.
データ保管システムを取扱う責任者及び作業者に対して、セキュリティに関することや、暗号鍵に対する教育、力量を定期的に実施していること。

指針の解説
データ保管システムを取扱う責任者及び作業者に対して、セキュリティに関することや、暗号鍵に対する教育、力量を定期的に実施していること。これらの実施方法には、以下を考慮することが望ましい。

教育プログラムの策定:
組織は、データ保管システムを取り扱う責任者及び作業者向けのセキュリティ教育プログラムを策定すること。プログラムは、セキュリティに関する基本的な原則から暗号鍵の重要性、セキュリティ脅威への対処方法までを網羅することが望ましい。

定期的なトレーニングの実施:
セキュリティ教育プログラムは、定期的に実施されるトレーニングセッションを含むこと。トレーニングは、責任者及び作業者が最新のセキュリティ手法やベストプラクティスについて理解を深めるために提供されることが望ましい。

暗号鍵に関する教育の強化:
教育プログラムは、暗号鍵の重要性や使用方法に焦点を当てた専門的なトレーニングを提供すること。責任者及び作業者は、暗号鍵の生成、管理、保護に関する基本的な知識とスキルを習得することが求められることが望ましい。

実践的なシミュレーションの実施:
セキュリティ教育プログラムには、実践的なシミュレーションや演習が含まれること。責任者及び作業者は、シミュレーションを通じて実際のセキュリティイベントに対処する能力を向上させることが望ましい。

評価とフィードバックの提供:
教育プログラムは、参加者の理解度や能力を定期的に評価し、フィードバックを提供する仕組みを備えること。参加者のフィードバックを収集し、教育プログラムの改善に役立てることが望ましい。

継続的な学習と向上:
組織は、責任者及び作業者が継続的に学習し、自己向上を促進するためのリソースを提供すること。最新のセキュリティトレンドや技術に関する情報へのアクセスを支援し、専門知識の向上をサポートすることが望ましい。

B.3. 経営陣の責任

B.3.7.

データ保管システム管理組織の経営陣は、作業者に対し、情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組みを整備すること。

指針の解説

データ保管システム管理組織の経営陣は、作業者に対し、情報セキュリティのための方針群又は手順への違反を報告するため、例えば、内部告発など、匿名の報告経路を提供する仕組

みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

匿名報告経路の設置:
経営陣は、情報セキュリティの方針や手順への違反を匿名で報告するための専用の報告経路を設置すること。この報告経路は、作業者が安心して違反を報告できるよう、厳格な機密性と匿名性が確保されることが望ましい。

報告手順の明確化:
匿名報告経路の手順と方法を明確に定義し、作業者に周知すること。作業者が容易にアクセスできるよう、報告経路の情報を組織内の適切な場所に掲示することが望ましい。

報告者の保護:
投稿者の匿名性を保護するための措置を講じること。投稿者が報復や不利益を受けることなく、違反報告を行えるよう、経営陣は適切な対策を講じることが望ましい。

報告内容の処理と調査:
投稿された違反報告は適切に処理され、必要に応じて迅速かつ公正な調査が行われること。違反報告に対する対応は透明性が保たれ、関係者に適切に通知されることが望ましい。

報告者へのフィードバック:
匿名報告者に対し、報告内容が受領されたことや対応状況についてのフィードバックを提供すること。報告者に対する感謝の意を示し、組織としての報告に対する積極的な姿勢を示すことが望ましい。

継続的な改善と透明性:
匿名報告経路の効果と透明性を継続的に評価し、改善を行うこと。経営陣は報告経路の存在や活動について、定期的に組織内外に公表し、透明性を確保することが望ましい。

B.3. 経営陣の責任

B.3.8.

データ保管システム管理組織の経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動すること。

指針の解説

データ保管システム管理組織の経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動すること。これらの行動方法には、以下を考慮することが望ましい。

方針と手順の明確化:
経営陣は、情報セキュリティに関する方針群、手順、および管理策を明確に定義し、組織内での遵守を促すこと。方針と手順は、データ保管、アクセス管理、セキュリティポリシー遵守などに関する具体的な指針を含むことが望ましい。

支持の実証:
経営陣は、情報セキュリティ方針と手順への支持を実証するために、行動によってそれを示すこと。情報セキュリティへの積極的な関与や適切な対策の実施を通じて、経営陣が方針と手順に従っていることを明確にすることが望ましい。

透明性とコミュニケーション:
経営陣は、情報セキュリティに関する方針や手順についての透明性を確保し、従業員とのコミュニケーションを促進すること。方針や手順の目的や重要性を明確に説明し、従業員がその重要性を理解し、遵守するようサポートすることが望ましい。

リーダーシップの示唆:
経営陣は、情報セキュリティに関するリーダーシップを示し、従業員に良いロールモデルとなること。定期的な情報セキュリティの挑戦や成功に関する報告を通じて、経営陣が方針と手順に対するコミットメントを強調することが望ましい。

継続的な評価と改善:
経営陣は、情報セキュリティ方針と手順の効果を継続的に評価し、必要に応じて改善を行うこと。新たな脅威や技術の進展に対応するため、定期的な方針と手順の再評価を実施し、組織全体のセキュリティレベルを向上させることが望ましい。

B.4. 委託先管理

B.4.1.

データ保管システムの経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を委託する別組織が、作業者に対して以下を整備していることを情報セキュリティのための方針群、手順及び管理策で確認すること。

- **組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組み**
- **組織の情報セキュリティのための方針群に従うように動機付ける仕組み**
- **組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組み**
- **組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組み**
- **適切な技能及び資格を保持し、定期的に教育を受けさせる仕組み**
- **情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組み**

指針の解説

データ保管システムの経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を委託する別組織が、作業者に対して、情報セキュリティについて期待することを示すための指針を提供する仕組みなどを整備すること。整備方法には、以下を考慮することが望ましい。

指針の提供：

別組織が作業者に対して情報セキュリティに関する役割や期待することを示す指針を提供していることを確認すること。これにより、作業者は自らの役割を理解し、適切なセキュリティプラクティスを遵守することが期待されることが望ましい。

動機付けの仕組み：

別組織や作業者が情報セキュリティ方針に従うように動機付ける仕組みを整備していることを確認すること。報奨制度や教育プログラム、適切なフィードバックメカニズムなどが含まれることが望ましい。

認識の向上：

別組織が作業者の情報セキュリティに関する認識を向上させるための仕組みを提供していることを確認すること。トレーニングや教育プログラム、評価や認定制度などが含まれるこ

とが望ましい。

雇用条件への準拠：
別組織や作業者が情報セキュリティ方針や適切な業務手順に従うようにするための雇用条件を整備していることを確認すること。これには、契約や規則、社内規程などが含まれることが望ましい。

教育と資格の提供：
別組織や作業者が適切な技能や資格を保持し、定期的に情報セキュリティに関する教育を受ける仕組みを提供していることを確認すること。これにより、作業者は最新のセキュリティプラクティスや技術について常に学び続けることが望ましい。

匿名報告経路の提供：
別組織が情報セキュリティ方針や手順への違反を報告するための匿名の報告経路を提供していることを確認すること。これにより、作業者はセキュリティに関する懸念や問題を匿名で報告しやすくすることが望ましい。

B.5. 暗号化消去対象のデータ保管領域

B.5.1.

暗号化消去対象となるデータ保管領域と範囲が明記された文書を用意すること。

指針の解説

暗号化消去対象のデータ保管領域は、暗号化消去対象となるデータ保管領域と範囲が明記された文書を用意すること。文書化方法には、以下を考慮することが望ましい。

データ保管領域の明確な定義:
組織は、暗号化消去となるデータ保管領域とその範囲を明確に定義する文書を作成すること。この文書には、どのデータが対象となるか、どのような形式で保存されているか、どの場所に保存されているかなどが含まれることが望ましい。

対象データの詳細な記述:
文書は、暗号化消去となるデータの詳細な説明を提供すること。データの種類、形式、保存期間、アクセス権限などの情報が含まれることが望ましい。

範囲の明示:
データ保管領域の範囲が明確に定義され、文書内で詳細に説明されること。特定のサーバ、データベース、ファイルシステム、クラウドストレージなど、範囲に含まれるものが明確に示されることが望ましい。

管理責任の明確化:
文書は、データ保管領域の管理責任を明確に示すこと。責任者や管理者が誰であり、どのような権限と責任を持つかが明確に定義されることが望ましい。

更新とレビューのプロセス:
文書は、定期的な更新とレビューのプロセスを定めること。新しいデータ保管領域が追加された場合や変更があった場合には、文書が更新され、必要な場合にはレビューが行われることが望ましい。

アクセス制御と監視:
文書は、データ保管領域へのアクセス制御と監視に関するポリシーを含むこと。アクセス権の管理、ログの監視、不正アクセスの検出などが明確に定義されることが望ましい。

法的および規制要件の遵守:
文書は、法的および規制要件に従うように設計されること。データ保管領域に関連する法的および規制要件が含まれ、遵守するための措置が明示されることが望ましい。

B.5.暗号化消去対象のデータ保管領域
B.5.2.
使用する暗号化について以下を明記すること。
・暗号化レイヤ
・暗号アルゴリズム
・鍵の取得方法
・鍵の保持期間
・鍵の保護方法
暗号化には CRYPTREC リストに記載のある暗号アルゴリズムを使用すること。

指針の解説
暗号化消去対象のデータ保管領域における暗号化には、CRYPTREC リストに記載のある暗号

アルゴリズムを使用されることが望ましく、以下を考慮することが望ましい。

暗号化レイヤ:
使用する暗号化レイヤを明確に指定すること。通常、データの転送時にはトランスポート層暗号化（TLS など）が使用されることが望ましい。

暗号アルゴリズム:
使用する暗号アルゴリズムを明示すること。CRYPTREC リストに記載の暗号アルゴリズムを選択することが望ましい。

鍵の取得方法:
暗号化に使用する鍵の取得方法を明確に定義すること。鍵の生成や交換方法、管理手順などが含まれることが望ましい。

鍵の保持期間:
鍵の保持期間を指定すること。鍵の有効期限や再生成頻度などが明確に定義されることが望ましい。

鍵の保護方法:
鍵の保護方法を具体的に記述すること。鍵の保存場所、アクセス権限、バックアップ方法、物理的な保護などが含まれることが望ましい。

CRYPTREC リストの暗号アルゴリズムの使用:
暗号化には CRYPTREC リストに記載の暗号アルゴリズムを使用することを明示すること。CRYPTREC リストには信頼性の高い暗号アルゴリズムが含まれていることが望ましい。

法的および規制要件の遵守:
暗号化に関する法的および規制要件を遵守することを確認すること。特定の業界や国の規制要件に応じて、暗号化手法や鍵の管理方法を選択することが望ましい。

監査と評価:
暗号化の実装と運用に関する定期的な監査と評価を行うこと。セキュリティの脆弱性や改善点を特定し、必要に応じて対策を講じることが望ましい。

B.5.暗号化消去対象のデータ保管領域

B.5.3.

保管するデータは不揮発の媒体に書き込まれる前に自動で暗号化すること。

指針の解説

暗号化消去対象のデータ保管領域における保管するデータは、不揮発の媒体に書き込まれる前に自動で暗号化することが望ましく、以下を考慮することが望ましい。

自動暗号化の導入:

不揮発性の媒体にデータを書き込む前に、自動暗号化システムを導入すること。システムはデータが保存される前に、自動的に暗号化を実行するよう設定されることが望ましい。

暗号化アルゴリズムの選択:

使用する暗号化アルゴリズムを慎重に選択すること。安全性と性能のバランスを考慮し、信頼性の高い暗号化手法を選択することが望ましい。

鍵の生成と管理:

暗号化に使用する鍵は、自動的に生成されるか、または適切に管理されること。長期間使用する鍵は定期的に更新されることが望ましい。

暗号化の透過性:

自動暗号化はユーザーやアプリケーションにとって透過的であることが望ましく、データの書き込みおよび読み取り操作に対して影響を与えないように設計されることが望ましい。

暗号化キーの保護:

暗号化に使用される鍵は、適切に保護されること。不正アクセスやデータ漏洩を防ぐために、鍵の保存とアクセス制御に対する厳格なセキュリティ対策が実施されることが望ましい。

システムの監視と管理:

自動暗号化システムは、運用中に監視され、適切に管理されること。エラーや異常が検出された場合には、即座に対処されることが望ましい。

法的および規制要件の遵守:

自動暗号化は、適用される法的および規制要件に準拠すること。特に個人情報や機密データの保護に関する規制に従うように設計されることが望ましい。

継続的な改善:
自動暗号化の実装は継続的な改善の対象となること。技術の進化やセキュリティの脅威に対応するため、システムは定期的にレビューおよび更新されることが望ましい。

B.6. データ保管前の暗号化設定

B.6.1.

暗号化対象領域には暗号化前のデータを格納しないことを、ポリシーまたは手順に明記すること。

指針の解説

データ保管前の暗号化設定における暗号化対象領域には、暗号化前のデータを格納しないことを、ポリシーまたは手順に明記することが望ましく、以下を考慮することが望ましい。

データ暗号化の目的:
暗号化は、機密性を確保し、データの保護を強化するための手段であることが望ましい。

暗号化対象領域の定義:
暗号化対象領域は、機密性が保護されるべきデータが格納される領域を指すことが望ましい。

ポリシーの明記:
暗号化対象領域には、暗号化前のデータを格納しないことをポリシーまたは手順に明記すること。暗号化前のデータの格納は、機密性の侵害やセキュリティ上のリスクを招く可能性がある。

暗号化前のデータの取り扱い:
暗号化前のデータは、暗号化が適用された後、適切に消去または保管する必要がある。暗号化前のデータを不必要に保持することは、機密性の侵害や法的なコンプライアンスの違反につながる可能性があることに留意することが望ましい。

適切な暗号化手法の選択:
機密性を保護するために、適切な暗号化手法を選択すること。暗号化手法の選択は、データ

の機密性、性能、およびコストの要件に基づいて行われることに留意することが望ましい。

定期的な監査と評価:
暗号化対象領域のポリシーと手順は、定期的な監査と評価によって検証さる。ポリシーの実行状況やセキュリティ上のリスクに関する洞察を得るために、定期的な監査を実施することが望ましい。

B.6. データ保管前の暗号化設定
B.6.2.
利用開始時に暗号化対象領域にデータが格納されていないことを確認し記録すること。利用開始時とは暗号化対象領域に自動の暗号化設定を適用した日時を指す。

指針の解説
データ保管前の暗号化設定における暗号化対象領域には、利用開始時に暗号化対象領域にデータが格納されていないことを確認し記録することが望ましい。利用開始時とは暗号化対象領域に自動の暗号化設定を適用した日時を指すことが望ましく、以下を考慮することが望ましい。

暗号化対象領域の利用開始の定義:
暗号化対象領域の利用開始とは、暗号化設定が自動的に適用され、暗号化対象領域が利用可能になった日時を指すことが望ましい。

利用開始時の確認と記録:
利用開始時には、暗号化対象領域にデータが格納されていないことを確認し、その旨を記録する。データの格納状況を確認するために、暗号化対象領域の内容を監査またはスキャンする。利用開始時の確認と記録は、セキュリティの透明性と責任追跡のために重要であることが望ましい。

記録の内容:
利用開始時に行われた確認と記録には、次の情報が含まれることが望ましい。
・利用開始日時
・暗号化対象領域の名称または識別子
・データの格納状況（データが存在しないことを確認した場合、その旨を明記する）
・確認を実施した担当者の氏名または識別子

記録の保管:
利用開始時の確認と記録は、適切なセキュリティ標準に従って保管されることが望ましい。記録は、必要に応じて監査や法的な要求に対応するために容易にアクセス可能にすることが望ましい。

定期的な再確認:
利用開始後も定期的に暗号化対象領域の内容を監査し、データが適切に暗号化されていることを確認することが望ましい。再確認はセキュリティの継続的な確保と、ポリシーの遵守を保証するために重要であることが望ましい。

B.7.鍵管理システム外の暗号鍵保持を制限
B.7.1.
データ保管システムでは暗号鍵を不揮発状態で保持しないこと。
※本要件に対応できない場合、代替策としてB.8.8.～B.8.10.に準拠すること。

指針の解説
鍵管理システム外の暗号鍵保持を制限することにおけるデータ保管システムでは、暗号鍵を不揮発状態で保持しないことが望ましく、以下を考慮することが望ましい。

暗号鍵の不揮発状態での保持:
不揮発状態での暗号鍵の保持は、暗号化の強度と鍵の安全性を向上させるために避けるために、データ保管システムでは、暗号鍵を不揮発状態で保持しないことが望ましい。

鍵の一時的な利用:
暗号鍵は、必要に応じて一時的にメモリ内に読み込まれ、使用される。暗号鍵が使用された後は、できるだけ早くメモリから消去することが望ましい。

暗号鍵の生成と交換:
暗号鍵は、安全な乱数生成器を使用してランダムに生成される。暗号鍵の交換は、安全な通信経路または鍵交換プロトコルを介して行われることが望ましい。

暗号鍵の保管:
暗号鍵は、安全な鍵管理システムまたはハードウェアセキュリティモジュール（HSM）など

のセキュリティ機構を使用して保管される。暗号鍵は、物理的なアクセスや不正なアクセスから保護されることが望ましい。

暗号鍵の定期的なローテーション:
暗号鍵は定期的にローテーションされ、鍵の強度とセキュリティを維持すること。ローテーションは、セキュリティポリシーに基づいて定期的なスケジュールで行われることが望ましい。

鍵の適切な削除:
不要になった暗号鍵は、適切な方法で削除されること。鍵の削除は、機密情報の漏洩やセキュリティのリスクを最小限に抑えるために重要であることが望ましい。

B. 8. アクセス制御

B. 8. 1.

鍵情報や暗号化データに関する作業、およびシステム設定の権限の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理すること。

指針の解説

アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理することが望ましく、以下を考慮することが望ましい。

アクセス制御方針への準拠:
鍵情報や暗号化データに関する作業およびシステム設定の権限は、関連するアクセス制御方針に厳密に従うことが望ましい。

正式な認可プロセス:
鍵情報や暗号化データに関連する作業やシステム設定の変更は、正式な認可プロセスによって管理される。認可プロセスは、適切な管理者や責任者によって承認されることが望ましい。

アクセス権の割り当て:
鍵情報や暗号化データに関連する作業やシステム設定の実行に必要なアクセス権は、最小限の特権の原則に従って割り当てること。必要最低限の権限のみが付与され、原則として

「必要最小限の原則」に従うことが望ましい。

アクセス権のレビューと更新:
アクセス権は定期的にレビューされ、必要に応じて更新すること。レビューは、変更された役割や業務の要件、セキュリティ上のリスクに基づいて行われることが望ましい。

監査とトレーサビリティ:
鍵情報や暗号化データに関連する作業やシステム設定の変更は、監査可能でトレーサビリティのある方法で実行される必要がある。すべての変更は、適切なログに記録され、必要に応じて監査の対象とすることが望ましい。

教育と意識向上:
鍵情報や暗号化データの管理に関わるスタッフには、適切な教育と意識向上の機会が提供される。スタッフは、セキュリティポリシーやアクセス制御方針に従うことの重要性について教育されることが望ましい。

B.8. アクセス制御
B.8.2.
鍵情報や暗号化データに関する作業、およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割当てていること。
システム設定の権限を割り当てるアカウントはユーザー個人に紐づいたアカウントとし、複数ユーザーで共有利用するアカウントにはシステム設定権限を割り当てないことが望ましい。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割当てていること。システム設定の権限を割り当てるアカウントはユーザー個人に紐づいたアカウントとし、複数ユーザーで共有利用するアカウントにはシステム設定権限を割り当てないことが望ましく、以下を考慮することが望ましい。

最小限の要求事項に基づく権限の割り当て:
鍵情報や暗号化データに関する作業およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割り当てること。ユーザーに必要な権限のみが付

与され、原則として「必要最小限の原則」に従うことが望ましい。

個人に紐づいたアカウントの使用:
システム設定の権限を割り当てるアカウントは、ユーザー個人に紐づいた個別のアカウントとすること。個人に紐づいたアカウントを使用することで、個々のユーザーのアクションを追跡し、責任の所在を明確にすることが望ましい。

共有利用アカウントでの権限割り当ての回避:
複数ユーザーで共有利用するアカウントには、システム設定権限を割り当てないことが望ましい。共有利用アカウントでは、個々のユーザーのアクセス管理やトレーサビリティが困難になるため、個人に紐づいたアカウントの使用を推奨することが望ましい。

役割に応じた権限の定義:
各ユーザーの役割や責任に応じて、適切な権限が定義される。ユーザーの役割や業務の変更に応じて、権限の再評価と調整が行われることが望ましい。

権限のレビューと更新:
権限は定期的にレビューされ、必要に応じて更新すること。レビューは、変更された役割や業務の要件、セキュリティ上のリスクに基づいて行われることが望ましい。

B. 8. アクセス制御
B. 8. 3.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、アクセス権の変更・消去していること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、アクセス権の変更・消去していることが望ましく、以下を考慮することが望ましい。

人事異動や退職によるアクセス権の管理:
鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、速やかにアクセス権の変更または消去すること

が望ましい。

変更の手順:
アクセス権の変更または消去は、所定の手順に従って行うこと。変更手順は、組織のポリシーや手順に従い、必要な承認を得ることが望ましい。

アクセス権の変更:
人事異動や退職等によるユーザー交代の場合、新しいユーザーに適切なアクセス権を割り当てること。新しいユーザーの役割や責任に応じて、適切な権限を与えることが望ましい。

アクセス権の消去:
旧ユーザーのアクセス権は速やかに消去すること。消去手順は、情報セキュリティポリシーやアクセス制御方針に従って行われることが望ましい。

トレーサビリティの確保:
アクセス権の変更や消去の過程は、適切に記録され、トレーサビリティが確保すること。変更の理由や実行者、実施日時などの情報が記録されることが望ましい。

監査とレビュー:
アクセス権の変更や消去の過程は、定期的に監査され、必要に応じてレビューが行われること。監査とレビューにより、アクセス権の変更や消去が適切に実施されていることが確認されることが望ましい。

B.8. アクセス制御
B.8.4.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーやシステムを定められた間隔でレビューしていること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーやシステムを定められた間隔でレビューしていることが望ましく、以下を考慮することが望ましい。

レビューの頻度の定義:

鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てられたユーザーやシステムは、定められた間隔でレビューすること。レビューの間隔は、セキュリティポリシーや業界のベストプラクティスに基づいて定義されることが望ましい。

レビューの対象:
レビューの対象には、鍵情報や暗号化データに関する作業やシステム設定の権限を持つすべてのユーザーやシステムが含まれること。レビューの対象は、管理者やセキュリティチームによって明確に定義されることが望ましい。

レビューの手順:
レビューは、所定の手順に従って実施すること。レビュー手順は、アクセス権の確認、権限の適合性の評価、不正なアクセスの検出などを含むことが望ましい。

変更の必要性の評価:
レビューの結果、アクセス権の変更や更新が必要である場合は、適切な手順に従って変更が実施されること。変更が必要な場合、正式な承認プロセスに従い、変更が実行されることが望ましい。

トレーサビリティの確保:
レビューの過程や結果は、適切に記録され、トレーサビリティが確保されること。レビューの実行者や結果、変更が必要とされた理由などの情報が記録されることが望ましい。

改善の実施:
レビューの結果に基づいて、適切な改善策が実施されること。改善策は、セキュリティポリシーや業界のベストプラクティスに準拠して実施されることが望ましい。

B.8. アクセス制御
B.8.5.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てた全ての認可を記録していること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てた全ての認可を記録していることが望ましく、以下を考慮することが望ましい。

認可の記録:
鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てる際、全ての認可は正式に記録されること。認可の記録には、誰がどのような権限を得たか、ならびにその権限が割り当てられた日時などの情報が含まれることが望ましい。

記録の内容:
記録には、次の情報が含まれることが望ましい
・ユーザーまたはシステムの識別子
・割り当てられた権限やロール
・権限の有効期限（必要な場合）
・権限の割り当て日時
・認可を行った管理者の識別子

情報の保管:
認可の記録は、安全に保管されること。記録は、情報セキュリティの最高水準に従い、適切なアクセス制御が施された場所に保存されることが望ましい。

記録の追跡:
認可の記録は、変更履歴を追跡するために適切に管理されること。記録が変更された場合、変更の内容と理由が適切に文書化されることが望ましい。

監査とトレーサビリティ:
認可の記録は、定期的な監査やセキュリティ検証の対象とすること。記録の監査により、権限の割り当てが適切に実施され、セキュリティポリシーに準拠していることが確認されることが望ましい。

B. 8. アクセス制御
B. 8. 6.
認可プロセスが完了するまで、鍵情報や暗号化データに関する作業、およびシステム設定を許可しないこと。

指針の解説
アクセス制御は、認可プロセスが完了するまで、鍵情報や暗号化データに関する作業、およ

びシステム設定を許可しないことが望ましく、以下を考慮することが望ましい。

作業の禁止:
鍵情報や暗号化データに関する作業、およびシステム設定を許可する前に、認可プロセスが完了するまで、これらの作業を禁止することが望ましい。

認可プロセスの開始:
鍵情報や暗号化データに関する作業、およびシステム設定の変更を行う場合、まず認可プロセスを開始すること。認可プロセスには、必要な承認を得るための手続きが含まれることが望ましい。

承認の取得:
作業やシステム設定の変更に関連する認可を得るために、適切な管理者や関係者からの承認を取得すること。承認は、セキュリティポリシーや規制要件に準拠した形で行われることが望ましい。

プロセスの完了:
必要な承認が得られた後、作業やシステム設定の変更を実行する。認可プロセスが完了し、関連する手続きや承認がすべて確立されるまで、作業を許可しないことが望ましい。

監査とトレーサビリティ:
認可プロセスの完了までの間、作業の禁止や承認の取得のプロセスに関する情報は、適切に記録され、トレーサビリティが確保されることが望ましい。監査のために、関連する情報を必要に応じて提供できるようにすることが望ましい。

遵守と教育:
全ての関係者に対して、作業の禁止や認可プロセスの重要性を啓発し、遵守すること。適切な教育や意識向上活動を通じて、適切な手続きを実行するための理解を促進することが望しい。

B.8.アクセス制御
B.8.7.
<HYOK を実施できない場合の代替要件>
認可されていない状態又は検知されない状態で、一人で鍵情報に対してアクセス、操作ができないように管理策を適用する。
具体的な管理策には、操作ログの監視、二人体制作業ルール、パスワードの知識分割、管理者による承認後の作業などが挙げられる。

指針の解説

アクセス制御は、認可されていない状態又は検知されない状態で、一人で鍵情報に対してアクセス、操作ができないように管理策を適用すること。具体的な管理策には、操作ログの監視、二人体制作業ルール、パスワードの知識分割、管理者による承認後の作業などを考慮することが望ましく、以下を考慮することが望ましい。

アクセスおよび操作の制限:
HYOK の実施ができない場合でも、認可されていない状態や検知されない状態で、一人で鍵情報に対してアクセスや操作ができないように管理策を適用することが望ましい。

具体的な管理策:
以下の管理策を考慮することが望ましい。

- 操作ログの監視:鍵情報へのアクセスや操作が行われた際に、操作ログを監視して不正なアクセスや操作を検知すること。
- 二人体制作業ルール:鍵情報に対する重要な操作や変更は、二人以上の関係者による承認や監視のもとで行われる二人体制で行うこと。
- パスワードの知識分割:鍵情報へのアクセスに必要なパスワードを複数の関係者に分割して保持し、単独ではアクセスできないようにすること。
- 管理者による承認後の作業:鍵情報に対する重要な作業や変更は、管理者による承認が必要であり、承認後に作業が実行されること。

適切な監視とトレーサビリティ:
代替要件が適用された場合、アクセスや操作に関するログが適切に監視され、不正なアクセスや操作があった場合には迅速に対処されること。ログは適切に保管され、必要に応じて監査や調査のために提供されることが望ましい。

定期的な評価と改善:

代替要件の有効性は定期的に評価され、必要に応じて改善されること。改善は、セキュリティ上のリスクや業務上の要件に基づいて行われることが望ましい。

B.8.アクセス制御
B.8.8.
<HYOK を実施できない場合の代替要件>
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーと、その権限を認可する者を分離すること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーと、その権限を認可する者を分離することが望ましく、以下を考慮することが望ましい。

ユーザーと認可者の分離:
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーと、その権限を認可する者を明確に分離することが望ましい。

役割と責任の分離:
ユーザーと認可者の役割と責任を明確に定義し、混同を避けること。ユーザーは、作業や操作を実行するが、認可者はそれらの作業や操作を承認する役割を果たすことが望ましい。

認可プロセスの実施:
ユーザーに新しい権限を割り当てる前に、適切な認可プロセスを実施すること。認可プロセスには、必要な承認を得るための手続きが含まれることが望ましい。

承認の明確化:
ユーザーが新しい権限を取得する際には、その権限を認可する者が明確に識別されること。承認者は、適切な権限を持ち、役割と責任が明確に定義されることが望ましい。

二重管理体制の確立:
ユーザーと認可者の分離を強化するために、二重管理体制を確立すること。重要な操作や変更に関する承認は、複数の関係者によって行われることが望ましい。

監査とトレーサビリティ:
ユーザーと認可者の分離が適切に実施されていることを確認するために、定期的な監査を実施すること。監査の結果は適切に記録され、トレーサビリティが確保されることが望ましい。

B.8.アクセス制御
B.8.9.
<HYOK を実施できない場合の代替要件>
ユーザーまたは管理者が、鍵情報や暗号化データに関する作業、およびシステム設定を行う際は、活動の監視、監査証跡、管理層による監督などにより不正を防止する管理策を策定すること。

指針の解説
アクセス制御は、ユーザーまたは管理者が、鍵情報や暗号化データに関する作業、およびシステム設定を行う際は、活動の監視、監査証跡、管理層による監督などにより不正を防止する管理策を策定することが望ましく、以下を考慮することが望ましい。

活動の監視:
ユーザーまたは管理者が鍵情報や暗号化データに関する作業やシステム設定を行う際、その活動をリアルタイムで監視すること。監視により、不正行為や異常なアクティビティを早期に検知し、適切な対応を行うことが望ましい。

監査証跡の作成:
活動の監視によって生成されたログやイベントに関する監査証跡を作成すること。監査証跡には、誰が何を行ったか、いつ行ったかなどの情報が含むことが望ましい。

管理層による監督:
不正を防止するために、管理層がユーザーの活動や管理者の行動を監督すること。監督には、定期的なレビューや報告、必要に応じた調査や対応が含まれることが望ましい。

不正行為への迅速な対応:
監視や監査証跡の分析により不正行為が検知された場合、迅速に対応すること。不正行為の発生源を特定し、適切な措置を講じて被害を最小限に抑えることが望ましい。

トレーニングと教育:
ユーザーや管理者に対して、不正行為の防止に関するトレーニングや教育を提供すること。セキュリティ意識の向上や適切な行動規範の普及に努めることが望ましい。

定期的な監査と改善:
管理策の有効性を確認するために、定期的な監査と評価を実施すること。監査結果をもとに、管理策やプロセスを改善してセキュリティレベルを向上させることが望ましい。

B.8.アクセス制御
B.8.10.
<HYOK を実施できない場合の代替要件>
不正を防止する管理策が運用されていること。

指針の解説
アクセス制御は、不正を防止する管理策が運用されていることが望ましく、以下を考慮することが望ましい。

不正を防止する管理策の運用:
不正を防止するための管理策が適切に運用されていることを確認すること。管理策は、組織のセキュリティポリシーや規制要件に基づいて策定され、実施されることが望ましい。

管理策の明確化:
不正を防止するための管理策は、明確に文書化され、関係者に周知されること。文書化された管理策には、目的、対象、手順、責任者などが明確に記載されていることが望ましい。

運用手順の定義:
不正を防止するための管理策の運用手順が明確に定義されていること。運用手順には、誰が責任を持ち、どのようなプロセスやツールを使用して実施されるかが記載されていることが望ましい。

定期的な評価と改善:
不正を防止する管理策の有効性は定期的に評価されること。評価の結果をもとに、必要に応じて管理策やプロセスを改善することが望ましい。

トレーニングと意識向上:
適切なトレーニングや意識向上活動が実施され、関係者が不正行為の識別や報告方法を理解すること。意識向上活動は、セキュリティに関する最新の脅威やベストプラクティスに焦点を当てて行われることが望ましい。

報告と迅速な対応:
不正行為が発生した場合、関係者は適切な報告手順を知り、迅速かつ適切に対応されること。不正行為の報告と対応のプロセスは、適切に文書化され、周知されることが望ましい。

B.9.変更管理

B.9.1.

変更管理ルールと手順を定め、責任者及び開発及び保守の責任者が承認していること。

指針の解説

変更管理は、変更管理ルールと手順を定め、責任者及び開発及び保守の責任者が承認していることが望ましく、以下を考慮することが望ましい。

変更管理ルールの策定:
変更管理ルールは、変更の要求、承認、実装、監視、評価などの手順を包括的に定義すること。ルールは、組織のビジョン、目標、セキュリティポリシーに合わせて策定されることが望ましい。

変更管理手順の定義:
変更管理手順は、変更の要求から承認、実施、評価までの一連のステップを具体的に示すこと。手順には、誰が変更を要求するか、どのように承認が得られるか、実施方法やテスト手法、変更後の評価方法などが含まれることが望ましい。

責任者の任命:
変更管理ルールと手順における責任者は、明確に任命されること。責任者は、変更の要求や承認、実装、監視、評価などの各段階で責任を持つことが望ましい。

開発・保守責任者の承認:
変更管理ルールと手順は、開発および保守の責任者によって承認されること。承認された手順に基づいて変更が行われることで、変更の一貫性と安全性が確保されることが望ましい。

変更の文書化:
変更管理の各段階での重要な決定や活動は、適切に文書化されること。文書化には、変更要求書、承認書、実装手順書、テスト結果、評価報告書などが含まれることが望ましい。

監視と評価:
変更が実施された後も、定期的な監視と評価が行われること。変更の影響や成果を適切に評価し、必要に応じて手順やプロセスを改善することが望ましい。

B.9.変更管理
B.9.2.
変更管理要求が生じた場合、他システムの影響を考慮していること。

指針の解説
変更管理は、変更管理要求が生じた場合、他システムの影響を考慮していることが望ましく、以下を考慮することが望ましい。

変更要求の評価:
変更管理要求が発生した際には、まず他システムへの影響を評価すること。影響の範囲を正確に把握するために、関連する他システムやサービスを明確に特定することが望ましい。

影響範囲の分析:
変更が他システムに与える影響を詳細に分析すること。影響範囲には、データの整合性、システムの可用性、関連するプロセスやワークフローへの影響などが含まれることが望ましい。

関係者の連携:
変更管理プロセスに関連する他システムの所有者や関係者と綿密に連携すること。影響範囲や変更計画に関する情報を共有し、必要な合意や調整を行うことが望ましい。

変更計画の調整:
他システムへの影響を考慮して、変更計画を適切に調整すること。変更のタイミングや手順、テスト計画などが他システムと調和するように検討されることが望ましい。

変更の実施と監視:
変更が実施される際には、他システムへの影響を監視すること。変更の影響が予期せず拡大する可能性がある場合、迅速に対応策を講じることが望ましい。

リスク管理:
他システムへの影響を考慮して、変更に関連するリスクを適切に管理すること。リスクを最小限に抑えるための予防策や回避策を検討し、必要に応じて変更計画を修正することが望ましい。

B.9.変更管理
B.9.3.
緊急の変更要求は文書化され、変更管理手続にしたがっていること。

指針の解説
変更管理は、緊急の変更要求は文書化され、変更管理手続にしたがっていることが望ましく、以下を考慮することが望ましい。

文書化された要求:
緊急の変更要求が発生した場合、要求内容は適切に文書化されること。文書化には、変更の理由、範囲、影響、実施方法などが含まれることが望ましい。

変更管理手続に従う:
緊急の変更要求も、通常の変更と同様に変更管理手続に従うこと。変更管理手続には、要求の提出、評価、承認、実施、監視、評価などのステップが含まれることが望ましい。

優先順位の明確化:
緊急の変更要求の優先順位が明確に定義されること。優先順位は、変更の重要度や緊急性、影響度などを考慮して設定されることが望ましい。

速やかな対応:
緊急の変更要求は速やかに対応されること。変更管理手続の各段階で迅速な判断と行動が求められることが望ましい。

文書化の適正化:

緊急の変更要求が承認された後も、適切に文書化されること。実施された変更の詳細や結果、影響などが適切に記録され、トレーサビリティが確保されることが望ましい。

監視と評価:
緊急の変更が実施された後、変更の影響や成果が適切に監視され、評価されること。不適切な変更や影響の発生があれば、迅速に対処することが望ましい。

B.10. システムクロック

B.10.1.

時刻同期技術を用いてシステム内のシステムクロックの時間精度を確保する仕組みを用意すること。

指針の解説

システムクロックは、時刻同期技術を用いてシステム内のシステムクロックの時間精度を確保する仕組みを用意することが望ましく、以下を考慮することが望ましい。

時刻同期技術の選定:
システムクロックの時間精度を確保するために適切な時刻同期技術を選定すること。NTP（NetworkTimeProtocol）、PTP（PrecisionTimeProtocol）などの技術を使用することが望ましい。

時刻同期サーバの設置:
時刻同期技術を利用するための時刻同期サーバを適切な場所に設置すること。サーバは信頼性が高く、ネットワークへのアクセスが容易であることが望ましい。

クライアントの設定:
各システム内のクライアント（サーバ、ワークステーションなど）に対して、時刻同期サーバへの接続を設定すること。クライアントは定期的に時刻同期サーバから時刻情報を取得し、システムクロックを同期することが望ましい。

セキュリティ検討:
時刻同期技術のセキュリティに関する検討を行うこと。時刻同期通信の暗号化や認証の実施など、セキュリティ対策を講ずることが望ましい。

モニタリングとアラート:
時刻同期の状態をモニタリングし、異常が検知された場合には適切なアラートを発信すること。時刻同期の障害や遅延が早急に対処されることが望ましい。

定期的な評価と調整:
時刻同期の正確性と信頼性を保つために、定期的な評価と調整を行うこと。システムクロックと時刻同期サーバの間の時差を監視し、必要に応じて調整を行うことが望ましい。

B.10. システムクロック **B.10.2.** **時刻同期技術を用いてデータ保管システム内のシステムクロックの時間精度が維持されていること。** **上記を時刻同期設定やサンプリングしたログ等を確認できること。**

指針の解説
システムクロックは、時刻同期技術を用いてデータ保管システム内のシステムクロックの時間精度が維持されていること。これらを時刻同期設定やサンプリングしたログ等を確認できることが望ましく、以下を考慮することが望ましい。

時刻同期技術の選定:
データ保管システム内のシステムクロックの時間精度を確保するために適切な時刻同期技術を選定すること。NTP（NetworkTimeProtocol）、PTP（PrecisionTimeProtocol）などの信頼性の高い技術を選択することが望ましい。

時刻同期設定の構築:
時刻同期技術を利用するための適切な設定を行うこと。システム内のすべてのデータ保管システムが、時刻同期サーバに正しく接続されていることを確認することが望ましい。

ログの記録と監視:
時刻同期設定やシステムクロックの状態を監視するためのログを記録すること。ログには、時刻同期イベントやシステムクロックの変更履歴などが含まれることが望ましい。

定期的な確認と監査:
時刻同期設定やログを定期的に確認し、システムクロックの時間精度が維持されているこ

とを確認すること。監査により、設定が適切に実施されているかどうかを確認することが望ましい。

アラートの設定:
時刻同期の異常や問題が検知された場合には、適切なアラートが発信されるように設定すること。アラートにより、問題が早急に検知され、対応が行われることが望ましい。

トラブルシューティング手順の準備:
時刻同期の問題が発生した場合に備えて、適切なトラブルシューティング手順を準備すること。手順には、問題の特定方法や解決策が含まれることが望ましい。

C. 暗号化システム

C.暗号化システム

C.1.セキュリティポリシー

C.1.1.

鍵管理システム管理組織はデータを保護するためのセキュリティポリシーを確立すること。セキュリティポリシーには以下を明記すること。

a) 組織の目的に対して適切である。

b) 情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示す。

c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。

d) 鍵情報や暗号化データに対するアクセス制御方針

指針の解説

セキュリティポリシーは、暗号化システムとして、暗号化消去における最上位の考え方を組織の外部及び内部に向けた表明である。このような観点より、以下を考慮したセキュリティポリシーを策定することが望ましい。

適切性の確保：

セキュリティポリシーは、組織の目的に対して適切であり、鍵管理システムの目的と一致していることが望ましい。

情報セキュリティ目的の明示：

セキュリティポリシーは、情報セキュリティの目的を明示し、鍵管理システムがデータを保護し、機密性や完全性を確保するための枠組みを提供することが望ましい。

コミットメントの表明：

セキュリティポリシーには、情報セキュリティに関連する適用される要求事項を満たすことへの組織全体のコミットメントが含まれる。組織は、セキュリティポリシーの実施と遵守に必要なリソースやサポートを提供することを約束することが望ましい。

アクセス制御方針の定義：

セキュリティポリシーには、鍵情報や暗号化データに対するアクセス制御方針が明確に定義されることが望ましい。アクセス制御方針は、認証、認可、および監査のプロセスを含み、機密性を維持するための適切な手順を提供することが望ましい。

変更管理と監査：
セキュリティポリシーは、変更管理プロセスを定義し、セキュリティ要件の変化や新たな脅威に対処するためのメカニズムを提供する。ポリシーの監査と評価は定期的に行われ、ポリシーが効果的かつ適切に実施されていることを確認することが望ましい。

教育と啓発：
セキュリティポリシーは、組織内外の関係者に向けて教育と啓発を行うための資源やプログラムを提供する。全ての関係者がセキュリティポリシーを理解し、遵守することが重要であり、適切なトレーニングや情報提供をすることが望ましい。

C.2. システム構成、体制、役割

C.2.1.

暗号化システム管理組織は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者または作業を委託する別組織の役割や責任及び体制について確認できる文書を用意すること。

指針の解説

システム構成、体制、役割は、暗号化システム管理組織として、暗号化消去におけるシステム構成、体制、役割を明確にすることである。システム構成、体制、役割は、各種規程、体制図等で明確にすることが望ましい。このような観点より、以下を考慮したシステム構成、体制、役割を明確にすることが望ましい。

役割と責任の明確化：
暗号化システム管理組織は、鍵情報や暗号化データに関する作業を行う自組織の作業者や、作業を委託する別組織の役割と責任を明確に定義すること。各作業者や組織が担当する業務内容や責任範囲、連絡先などを含む文書を用意することが望ましい。

体制の整備：
暗号化システム管理組織は、鍵情報や暗号化データに関する作業やシステム設定を行うための適切な体制を整備する。体制には、必要な資源や権限、監督体制、連絡先情報などが含まれることが望ましい。

文書の作成：
鍵情報や暗号化データに関する作業やシステム設定に関する役割や責任、体制について確

認できる文書を作成する。文書はわかりやすく、具体的な情報を含み、関係者が容易にアクセスできる場所に保管されることが望ましい。

定期的なレビューと更新：
文書は定期的にレビューされ、必要に応じて更新されること。変更があった場合や新たな要員が加わった場合など、文書の内容に変更が生じた際には、迅速に更新することが望ましい。

関係者への通知と教育：
関係者に対して、鍵情報や暗号化データに関する作業や体制についての文書を適切に通知し、説明すること。関係者が自らの役割や責任を理解し、適切に業務を遂行できるようにするために、必要な教育やトレーニングを実施することが望ましい。

C.2. システム構成、体制、役割
C.2.2.
暗号化システム管理組織は、鍵情報や暗号化データを取り扱うシステム及びその周辺環境の構成やデータフローが確認できる文書を用意すること。

指針の解説
暗号化システム管理組織は、鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できる文書を用意すること。これらの文書は、該当システムの構成図等で明確にすることが望ましい。このような観点より、以下を考慮した鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できることを文書化することが望ましい。

システム構成の明確化：
暗号化システム管理組織は、鍵情報や暗号化データを取り扱うシステムの構成を明確に文書化する。これらの文書には、システムのハードウェア、ソフトウェア、ネットワーク構成などが含まれていることが望ましい。

データフローの記述：
鍵情報や暗号化データの取り扱いに関するデータフローを記述する。データの生成元から保存、処理、転送、削除までの手順やプロセスが明確に記載されることが望ましい。

セキュリティ対策の説明：
システムの構成やデータフローに関連するセキュリティ対策が文書に含まれること。アク

セス制御、暗号化、監査ログの設定など、セキュリティを強化するための具体的な措置が記載されることが望ましい。

システム間の統合と依存関係の説明：
鍵情報や暗号化データを取り扱うシステムが他のシステムとどのように統合されているか、および依存関係があるかを明確に説明すること。他のシステムとのデータのやり取りや、データの共有方法などが示されることが望ましい。

文書のアップデートとレビュー：
文書は定期的にレビューされ、必要に応じてアップデートされること。システムの変更やアップグレード、新たなセキュリティ要件の追加などがあった場合には、文書も適切に更新されることが望ましい。

関係者への共有と教育：
システム構成やデータフローに関する文書は関係者に適切に共有され、理解されるようにすること。関係者がシステムの構成やデータフローを把握し、セキュリティ上の重要性を理解できるようにするために、適切な教育やトレーニングを提供することが望ましい。

C.3.経営陣の責任

C.3.1.

暗号化システム管理組織の経営陣は、作業者が鍵情報や暗号化データに関する作業、およびシステム設定へのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備すること。

指針の解説

暗号化システム管理組織の経営陣は、作業者が鍵情報や暗号化データに関する作業、およびシステム設定へのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備すること。整備方法としては、役割責任表などが考えられる。これらの役割責任の整備方法には、以下を考慮することが望ましい。

経営陣の役割と責任の明確化:
経営陣は情報セキュリティの重要性を理解し、その責任を認識すること。情報セキュリティポリシーの策定と維持に責任を持つことが望ましい。

作業者への教育と訓練:
作業者に対し、情報セキュリティの重要性と責任を定期的に教育し、訓練すること。鍵情報や暗号化データの取り扱い方法とシステムへのアクセス権限に関するガイドラインを提供することが望ましい。

情報セキュリティポリシーの普及:
情報セキュリティポリシーを組織内で普及させ、全ての作業者が理解し遵守することを確保すること。ポリシーの更新や変更があった場合は、適切に伝達し、理解を確認することが望ましい。

アクセスコントロールの強化:
鍵情報や暗号化データへのアクセスは、必要最小限の権限で制限すること。アクセス権限の与えられた作業者は、その権限の範囲内でのみ作業を行うことを徹底することが望ましい。

監査と評価:
情報セキュリティの実施状況を定期的に監査し、遵守状況を評価すること。監査結果に基づき、改善点を特定し、適切な対策を講じることが望ましい。

リスク管理と対応:
情報セキュリティに関連するリスクを評価し、適切な管理策を策定すること。セキュリティインシデントが発生した場合は、速やかに対応し、適切な措置を講じることが望ましい。

継続的な改善:
情報セキュリティの方針や手順を継続的に改善し、最新の脅威やベストプラクティスに対応すること。組織内の全てのメンバーが、情報セキュリティの向上に協力する文化を醸成することが望ましい。

C.3. 経営陣の責任

C.3.2.

暗号化システム管理組織の経営陣は、作業者に対し、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備すること。

指針の解説

暗号化システム管理組織の経営陣は、作業者に対し、組織内での役割において、情報セキュ

リティについて期待することを示すための指針を提供する仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

経営陣のリーダーシップ:
経営陣は情報セキュリティの重要性を理解し、その重要性を従業員に示すことでリーダーシップを発揮すること。情報セキュリティに関する組織全体の方針や目標を明確に定義し、従業員に伝達することが望ましい。

情報セキュリティの期待の明確化:
経営陣は、従業員に対し、情報セキュリティに関する期待事項を具体的に示すこと。作業者には、データの取り扱い、アクセス権の管理、セキュリティポリシーの遵守などに関する具体的な指針を提供することが望ましい。

教育と訓練の提供:
情報セキュリティに関する教育と訓練プログラムを組織内で定期的に実施し、作業者の能力を向上させること。従業員が情報セキュリティポリシーを遵守し、セキュリティのベストプラクティスを理解するための機会を提供することが望ましい。

コミュニケーションの促進:
経営陣は、従業員とのコミュニケーションを通じて、情報セキュリティに関する重要な情報や変更事項を伝達すること。従業員は、情報セキュリティに関する懸念や提案を提出するための適切なチャネルを提供することが望ましい。

フィードバックと改善:
経営陣は、従業員からのフィードバックを受け入れ、情報セキュリティプロセスやポリシーの改善に活かすこと。継続的な監視と評価を通じて、情報セキュリティの効果を定期的に確認し、必要に応じて改善を行うことが望ましい。

遵守と報奨:
経営陣は、情報セキュリティポリシーの遵守を奨励し、従業員が適切なセキュリティ対策を実践することを評価すること。優れた情報セキュリティ実践に対する報奨制度を導入し、従業員のモチベーションを高めることが望ましい。

C.3. 経営陣の責任

C.3.3.

暗号化システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備すること。

指針の解説

暗号化システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

組織の情報セキュリティポリシーの明確化:
経営陣は、組織の情報セキュリティポリシーを明確に定義し、従業員に理解しやすい形で伝えること。ポリシーは、データ保管、アクセス管理、セキュリティプロトコルなどに関する具体的な方針を含むことが望ましい。

教育と意識向上の促進:
作業者に対し、情報セキュリティの重要性を定期的に強調し、意識向上を図る教育プログラムを実施すること。定期的なトレーニングやシミュレーションを通じて、セキュリティに関する最新の脅威や対策について従業員を啓発することが望ましい。

動機付けと報奨:
作業者が情報セキュリティポリシーに従うことを奨励する報奨制度を導入すること。遵守した場合の報奨や、セキュリティ違反を減らすことでチームや個人の評価に対するポジティブな影響を示すことが望ましい。

フィードバックと改善:
従業員からのフィードバックを受け入れ、ポリシーの実施に関する問題や提案を積極的に取り入れること。ポリシーの改善点や不明瞭な部分を特定し、適切な修正を行うことで、従業員の満足度と遵守率を向上させることが望ましい。

ロールモデルの示唆:
経営陣や管理職は、情報セキュリティポリシーを率先して遵守し、従業員に良いロールモデルを示すことが重要であること。従業員は、リーダーシップからのポジティブな影響を受け、ポリシーに積極的に従う傾向が高まることが望ましい。

継続的な監視と改善:
情報セキュリティポリシーの遵守状況を継続的に監視し、違反や問題を早期に検出すること。監視結果に基づいてポリシーの改善を行い、組織全体のセキュリティレベルを向上させることが望ましい。

C.3. 経営陣の責任

C.3.4.

暗号化システム管理組織の経営陣は、作業者に対し、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備すること。

指針の解説

暗号化システム管理組織の経営陣は、作業者に対し、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

役割と責任の明確化:
経営陣は、自らの情報セキュリティに関する役割と責任を明確に定義し、作業者に対して明示すること。各作業者の役割と責任が情報セキュリティの目標と一致していることを確認することが望ましい。

教育とトレーニングの提供:
情報セキュリティに関する教育プログラムやトレーニングを組織内で実施し、経営陣と作業者の両方に対して情報セキュリティに関する知識を向上させること。役割と責任に関連する情報セキュリティのトレーニングを提供し、一定の水準を達成するためのサポートを行うことが望ましい。

規定の策定と遵守の促進:
経営陣は、情報セキュリティポリシーと手順を策定し、それらの遵守を促進すること。自らの役割と責任に関連する情報セキュリティ規定を従業員に明確に伝え、その遵守を監視することが望ましい。

監査と評価:

情報セキュリティの実施状況を定期的に監査し、遵守水準を評価すること。監査結果に基づいて、必要な対策や改善点を特定し、適切な対応を講じることが望ましい。

透明性とコミュニケーション:
経営陣は、情報セキュリティに関する透明性を確保し、作業者とのコミュニケーションを促進すること。情報セキュリティに関する重要な変更や問題について、適切な情報を提供し、従業員からのフィードバックを受け入れることが望ましい。

継続的な向上:
経営陣は、情報セキュリティの向上に向けて継続的な取り組みを行い、一定水準を維持するだけでなく、常に向上を目指すこと。新たな脅威や技術の進展に対応するため、定期的な情報セキュリティの再評価と改善を行うことが望ましい。

C.3. 経営陣の責任
C.3.5.
暗号化システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備すること。

指針の解説
暗号化システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

情報セキュリティ方針の明確化:
経営陣は、組織の情報セキュリティ方針を明確に定義し、作業者に対して遵守を求めること。方針は、データの保護、アクセス管理、セキュリティ対策などに関する具体的なガイドラインを含むことが望ましい。

雇用条件への組み込み:
情報セキュリティ方針や適切な仕事のやり方を含む、情報セキュリティへの遵守が雇用条件として組み込まれること。作業者は雇用契約や規定を受け入れる際に、情報セキュリティ方針に同意することが求められることが望ましい。

教育とトレーニングの提供:

作業者に対し、情報セキュリティ方針や適切な仕事のやり方に関する教育プログラムやトレーニングを提供すること。新入社員や関連部署の従業員には、情報セキュリティの基本や方針に関する研修を実施することが望ましい。

遵守の監視と評価:
経営陣は、情報セキュリティ方針の遵守を定期的に監視し、適切な評価を行うこと。違反や問題が発生した場合には、適切な対応を講じ、必要に応じて改善を行うことが望ましい。

報奨とリワード:
情報セキュリティ方針への遵守や適切な仕事のやり方を実践する作業者には、報奨やリワードを与える制度を導入すること。優れた情報セキュリティ実践に対する認定や特典を提供し、作業者のモチベーションを高めることが望ましい。

継続的な改善:
情報セキュリティ方針や適切な仕事のやり方を継続的に改善し、組織のセキュリティレベルを向上させる取り組みを行うこと。ユーザーフィードバックや業界のベストプラクティスを活用して、常に最新の状況に適応することが望ましい。

C.3. 経営陣の責任

C.3.6.

暗号化システム管理組織の経営陣は、作業者に対し、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備すること。

指針の解説

暗号化システム管理組織の経営陣は、作業者に対し、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

技能と資格の要件の明確化:
作業者が持つべき技能や資格について明確な基準を設定する。これには、暗号化技術の専門知識、セキュリティ管理のスキル、および関連する業界の規制や規格に関する理解が含まれることが望ましい。

教育プログラムの設計:

定期的な教育プログラムを策定する。このプログラムは、新しい技術や脅威に関する最新の情報を提供し、作業者のスキルを向上させることを目的とする。教育プログラムは、オンサイトのトレーニング、外部のトレーニング機関との提携、オンラインリソースの利用など、さまざまな方法で提供することが望ましい。

定期的な評価と更新:
教育プログラムの効果を評価し、必要に応じて更新する。技術の進化や新たな脅威に対応するために、プログラムを定期的に再評価し、改善することが望ましい。

記録の管理:
作業者の教育履歴や資格情報を適切に管理し、追跡する。これにより、必要なトレーニングが受けられ、資格が維持されることを保証することが望ましい。

コミュニケーションとフィードバックの促進:
作業者と管理層の間で開かれたコミュニケーションを促進し、フィードバックを収集する。作業者が教育プログラムや資格要件に関する疑問や提案を提出できるようにすることが望ましい。

C.3. 経営陣の責任

C.3.7.

暗号化システム管理組織の経営陣は、作業者に対し、情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組みを整備すること。

指針の解説

暗号化システム管理組織の経営陣は、作業者に対し、情報セキュリティのための方針群又は手順への違反を報告するため、例えば、内部告発など、匿名の報告経路を提供する仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

匿名報告経路の設置:
経営陣は、情報セキュリティの方針や手順への違反を匿名で報告するための専用の報告経路を設置すること。この報告経路は、作業者が安心して違反を報告できるよう、厳格な機密性と匿名性が確保されることが望ましい。

報告手順の明確化:
匿名報告経路の手順と方法を明確に定義し、作業者に周知すること。作業者が容易にアクセスできるよう、報告経路の情報を組織内の適切な場所に掲示することが望ましい。

報告者の保護:
投稿者の匿名性を保護するための措置を講じること。投稿者が報復や不利益を受けることなく、違反報告を行えるよう、経営陣は適切な対策を講じることが望ましい。

報告内容の処理と調査:
投稿された違反報告は適切に処理され、必要に応じて迅速かつ公正な調査が行われること。違反報告に対する対応は透明性が保たれ、関係者に適切に通知されることが望ましい。

報告者へのフィードバック:
匿名報告者に対し、報告内容が受領されたことや対応状況についてのフィードバックを提供すること。報告者に対する感謝の意を示し、組織としての報告に対する積極的な姿勢を示すことが望ましい。

継続的な改善と透明性:
匿名報告経路の効果と透明性を継続的に評価し、改善を行うこと。経営陣は報告経路の存在や活動について、定期的に組織内外に公表し、透明性を確保することが望ましい。

C.3. 経営陣の責任
C.3.8.
暗号化システム管理組織の経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動すること。

指針の解説
暗号化システム管理組織の経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動すること。これらの行動方法には、以下を考慮することが望ましい。

方針と手順の明確化:
経営陣は、情報セキュリティに関する方針群、手順、および管理策を明確に定義し、組織内での遵守を促すこと。方針と手順は、データ保管、アクセス管理、セキュリティポリシー遵

守などに関する具体的な指針を含むことが望ましい。

支持の実証:
経営陣は、情報セキュリティ方針と手順への支持を実証するために、行動によってそれを示すこと。情報セキュリティへの積極的な関与や適切な対策の実施を通じて、経営陣が方針と手順に従っていることを明確にすることが望ましい。

透明性とコミュニケーション:
経営陣は、情報セキュリティに関する方針や手順についての透明性を確保し、従業員とのコミュニケーションを促進すること。方針や手順の目的や重要性を明確に説明し、従業員がその重要性を理解し、遵守するようサポートすることが望ましい。

リーダーシップの示唆:
経営陣は、情報セキュリティに関するリーダーシップを示し、従業員に良いロールモデルとなること。定期的な情報セキュリティの挑戦や成功に関する報告を通じて、経営陣が方針と手順に対するコミットメントを強調することが望ましい。

継続的な評価と改善:
経営陣は、情報セキュリティ方針と手順の効果を継続的に評価し、必要に応じて改善を行うこと。新たな脅威や技術の進展に対応するため、定期的な方針と手順の再評価を実施し、組織全体のセキュリティレベルを向上させることが望ましい。

C.4.委託先管理

C.4.1.

暗号化システム管理組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を委託する別組織が、作業者に対して以下を整備していることを情報セキュリティのための方針群、手順及び管理策で確認すること。

- **組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組み**
- **組織の情報セキュリティのための方針群に従うように動機付ける仕組み**
- **組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組み**
- **組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組み**
- **適切な技能及び資格を保持し、定期的に教育を受けさせる仕組み**
- **情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組み**

指針の解説

データ保管システムの経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を委託する別組織が、作業者に対して、情報セキュリティについて期待することを示すための指針を提供する仕組みなどを整備すること。整備方法には、以下を考慮することが望ましい。

指針の提供：

別組織が作業者に対して情報セキュリティに関する役割や期待することを示す指針を提供していることを確認すること。これにより、作業者は自らの役割を理解し、適切なセキュリティプラクティスを遵守することが期待されることが望ましい。

動機付けの仕組み：

別組織や作業者が情報セキュリティ方針に従うように動機付ける仕組みを整備していることを確認すること。報奨制度や教育プログラム、適切なフィードバックメカニズムなどが含まれることが望ましい。

認識の向上：

別組織が作業者の情報セキュリティに関する認識を向上させるための仕組みを提供していることを確認すること。トレーニングや教育プログラム、評価や認定制度などが含まれることが望ましい。

雇用条件への準拠：

別組織や作業者が情報セキュリティ方針や適切な業務手順に従うようにするための雇用条件を整備していることを確認すること。これには、契約や規則、社内規程などが含まれることが望ましい。

教育と資格の提供：

別組織や作業者が適切な技能や資格を保持し、定期的に情報セキュリティに関する教育を受ける仕組みを提供していることを確認すること。これにより、作業者は最新のセキュリティプラクティスや技術について常に学び続けることが望ましい。

匿名報告経路の提供：

別組織が情報セキュリティ方針や手順への違反を報告するための匿名の報告経路を提供していることを確認すること。これにより、作業者はセキュリティに関する懸念や問題を匿名で報告しやすくすることが望ましい。

C.5.提供する暗号化機能

C.5.1.

提供可能な暗号化について以下を明記すること。

・暗号化レイヤ

・暗号アルゴリズム

・鍵の取得方法

・鍵の保持期間

・鍵の保護方法

暗号化には CRYPTREC リストに記載のある暗号アルゴリズムを使用すること。

指針の解説

暗号化消去対象のデータ保管領域における暗号化には、CRYPTREC リストに記載のある暗号アルゴリズムを使用されることが望ましく、以下を考慮することが望ましい。

データ保管領域の明確な定義:

組織は、暗号化消去となるデータ保管領域とその範囲を明確に定義する文書を作成すること。この文書には、どのデータが対象となるか、どのような形式で保存されているか、どの場所に保存されているかなどが含まれることが望ましい。

対象データの詳細な記述:

文書は、暗号化消去となるデータの詳細な説明を提供すること。データの種類、形式、保存期間、アクセス権限などの情報が含まれることが望ましい。

範囲の明示:

データ保管領域の範囲が明確に定義され、文書内で詳細に説明されること。特定のサーバ、データベース、ファイルシステム、クラウドストレージなど、範囲に含まれるものが明確に示されることが望ましい。

管理責任の明確化:

文書は、データ保管領域の管理責任を明確に示すこと。責任者や管理者が誰であり、どのような権限と責任を持つかが明確に定義されることが望ましい。

更新とレビューのプロセス:
文書は、定期的な更新とレビューのプロセスを定めること。新しいデータ保管領域が追加された場合や変更があった場合には、文書が更新され、必要な場合にはレビューが行われることが望ましい。

アクセス制御と監視:
文書は、データ保管領域へのアクセス制御と監視に関するポリシーを含むこと。アクセス権の管理、ログの監視、不正アクセスの検出などが明確に定義されることが望ましい。

法的および規制要件の遵守:
文書は、法的および規制要件に従うように設計されること。データ保管領域に関連する法的および規制要件が含まれ、遵守するための措置が明示されることが望ましい。

C.6.暗号鍵は鍵管理システムでのみ保持し、鍵管理システム外には保持しない。
C.6.1.
暗号化システムでは暗号鍵を不揮発状態で保持しないこと。
※本要件に対応できない場合、代替策としてC.7.7.～C.7.10.に準拠すること。

指針の解説
暗号化システムでは暗号鍵を不揮発状態で保持しないことが望ましく、以下を考慮することが望ましい。

暗号鍵の不揮発状態での保持:
不揮発状態での暗号鍵の保持は、暗号化の強度と鍵の安全性を向上させるために避けるために、データ保管システムでは、暗号鍵を不揮発状態で保持しないことが望ましい。

鍵の一時的な利用:
暗号鍵は、必要に応じて一時的にメモリ内に読み込まれ、使用される。暗号鍵が使用された後は、できるだけ早くメモリから消去することが望ましい。

暗号鍵の生成と交換:
暗号鍵は、安全な乱数生成器を使用してランダムに生成される。暗号鍵の交換は、安全な通信経路または鍵交換プロトコルを介して行われることが望ましい。

暗号鍵の保管:
暗号鍵は、安全な鍵管理システムまたはハードウェアセキュリティモジュール（HSM）などのセキュリティ機構を使用して保管される。暗号鍵は、物理的なアクセスや不正なアクセスから保護されることが望ましい。

暗号鍵の定期的なローテーション:
暗号鍵は定期的にローテーションされ、鍵の強度とセキュリティを維持すること。ローテーションは、セキュリティポリシーに基づいて定期的なスケジュールで行われることが望ましい。

鍵の適切な削除:
不要になった暗号鍵は、適切な方法で削除されること。鍵の削除は、機密情報の漏洩やセキュリティのリスクを最小限に抑えるために重要であることが望ましい。

C.7.アクセス制御

C.7.1.

鍵情報や暗号化データに関する作業、およびシステム設定の権限の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理すること。

指針の解説

アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理することが望ましく、以下を考慮することが望ましい。

アクセス制御方針への準拠:
鍵情報や暗号化データに関する作業およびシステム設定の権限は、関連するアクセス制御方針に厳密に従うことが望ましい。

正式な認可プロセス:
鍵情報や暗号化データに関連する作業やシステム設定の変更は、正式な認可プロセスによって管理される。認可プロセスは、適切な管理者や責任者によって承認されることが望ましい。

アクセス権の割り当て:
鍵情報や暗号化データに関連する作業やシステム設定の実行に必要なアクセス権は、最小限の特権の原則に従って割り当てること。必要最低限の権限のみが付与され、原則として「必要最小限の原則」に従うことが望ましい。

アクセス権のレビューと更新:
アクセス権は定期的にレビューされ、必要に応じて更新すること。レビューは、変更された役割や業務の要件、セキュリティ上のリスクに基づいて行われることが望ましい。

監査とトレーサビリティ:
鍵情報や暗号化データに関連する作業やシステム設定の変更は、監査可能でトレーサビリティのある方法で実行される必要がある。すべての変更は、適切なログに記録され、必要に応じて監査の対象とすることが望ましい。

教育と意識向上:
鍵情報や暗号化データの管理に関わるスタッフには、適切な教育と意識向上の機会が提供される。スタッフは、セキュリティポリシーやアクセス制御方針に従うことの重要性について教育されることが望ましい。

C.7.アクセス制御
C.7.2.
鍵情報や暗号化データに関する作業、およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割当てていること。
システム設定の権限を割り当てるアカウントはユーザー個人に紐づいたアカウントとし、複数ユーザーで共有利用するアカウントにはシステム設定権限を割り当てないことが望ましい。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割当てていること。システム設定の権限を割り当てるアカウントはユーザー個人に紐づいたアカウントとし、複数ユーザーで共有利用するアカウントにはシステム設定権限を割り当てないことが望ましく、以下を考慮することが望ましい。

最小限の要求事項に基づく権限の割り当て:
鍵情報や暗号化データに関する作業およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割り当てること。ユーザーに必要な権限のみが付与され、原則として「必要最小限の原則」に従うことが望ましい。

個人に紐づいたアカウントの使用:
システム設定の権限を割り当てるアカウントは、ユーザー個人に紐づいた個別のアカウントとすること。個人に紐づいたアカウントを使用することで、個々のユーザーのアクションを追跡し、責任の所在を明確にすることが望ましい。

共有利用アカウントでの権限割り当ての回避:
複数ユーザーで共有利用するアカウントには、システム設定権限を割り当てないことが望ましい。共有利用アカウントでは、個々のユーザーのアクセス管理やトレーサビリティが困難になるため、個人に紐づいたアカウントの使用を推奨することが望ましい。

役割に応じた権限の定義:
各ユーザーの役割や責任に応じて、適切な権限が定義される。ユーザーの役割や業務の変更に応じて、権限の再評価と調整が行われることが望ましい。

権限のレビューと更新:
権限は定期的にレビューされ、必要に応じて更新すること。レビューは、変更された役割や業務の要件、セキュリティ上のリスクに基づいて行われることが望ましい。

C.7.アクセス制御
C.7.3.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、アクセス権の変更・消去していること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、アクセス権の変更・消去していることが望ましく、以下を考慮することが望ましい。

人事異動や退職によるアクセス権の管理:
鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、速やかにアクセス権の変更または消去することが望ましい。

変更の手順:
アクセス権の変更または消去は、所定の手順に従って行うこと。変更手順は、組織のポリシーや手順に従い、必要な承認を得ることが望ましい。

アクセス権の変更:
人事異動や退職等によるユーザー交代の場合、新しいユーザーに適切なアクセス権を割り当てること。新しいユーザーの役割や責任に応じて、適切な権限を与えることが望ましい。

アクセス権の消去:
旧ユーザーのアクセス権は速やかに消去すること。消去手順は、情報セキュリティポリシーやアクセス制御方針に従って行われることが望ましい。

トレーサビリティの確保:
アクセス権の変更や消去の過程は、適切に記録され、トレーサビリティが確保すること。変更の理由や実行者、実施日時などの情報が記録されることが望ましい。

監査とレビュー:
アクセス権の変更や消去の過程は、定期的に監査され、必要に応じてレビューが行われること。監査とレビューにより、アクセス権の変更や消去が適切に実施されていることが確認されることが望ましい。

C.7.アクセス制御
C.7.4.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーやシステムを定められた間隔でレビューしていること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーやシステムを定められた間隔でレビューしていることが望ましく、以下

を考慮することが望ましい。

レビューの頻度の定義:
鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てられたユーザーやシステムは、定められた間隔でレビューすること。レビューの間隔は、セキュリティポリシーや業界のベストプラクティスに基づいて定義されることが望ましい。

レビューの対象:
レビューの対象には、鍵情報や暗号化データに関する作業やシステム設定の権限を持つすべてのユーザーやシステムが含まれること。レビューの対象は、管理者やセキュリティチームによって明確に定義されることが望ましい。

レビューの手順:
レビューは、所定の手順に従って実施すること。レビュー手順は、アクセス権の確認、権限の適合性の評価、不正なアクセスの検出などを含むことが望ましい。

変更の必要性の評価:
レビューの結果、アクセス権の変更や更新が必要である場合は、適切な手順に従って変更が実施されること。変更が必要な場合、正式な承認プロセスに従い、変更が実行されることが望ましい。

トレーサビリティの確保:
レビューの過程や結果は、適切に記録され、トレーサビリティが確保されること。レビューの実行者や結果、変更が必要とされた理由などの情報が記録されることが望ましい。

改善の実施:
レビューの結果に基づいて、適切な改善策が実施されること。改善策は、セキュリティポリシーや業界のベストプラクティスに準拠して実施されることが望ましい。

C.7.アクセス制御
C.7.5.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てた全ての認可を記録していること。

指針の解説

アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てた全ての認可を記録していることが望ましく、以下を考慮することが望ましい。

認可の記録:

鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てる際、全ての認可は正式に記録されること。認可の記録には、誰がどのような権限を得たか、ならびにその権限が割り当てられた日時などの情報が含まれることが望ましい。

記録の内容:

記録には、次の情報が含まれることが望ましい

・ユーザーまたはシステムの識別子
・割り当てられた権限やロール
・権限の有効期限（必要な場合）
・権限の割り当て日時
・認可を行った管理者の識別子

情報の保管:

認可の記録は、安全に保管されること。記録は、情報セキュリティの最高水準に従い、適切なアクセス制御が施された場所に保存されることが望ましい。

記録の追跡:

認可の記録は、変更履歴を追跡するために適切に管理されること。記録が変更された場合、変更の内容と理由が適切に文書化されることが望ましい。

監査とトレーサビリティ:

認可の記録は、定期的な監査やセキュリティ検証の対象とすること。記録の監査により、権限の割り当てが適切に実施され、セキュリティポリシーに準拠していることが確認されることが望ましい。

C.7.アクセス制御

C.7.6.

認可プロセスが完了するまで、鍵情報や暗号化データに関する作業、およびシステム設定を許可しないこと。

指針の解説

アクセス制御は、認可プロセスが完了するまで、鍵情報や暗号化データに関する作業、およびシステム設定を許可しないことが望ましく、以下を考慮することが望ましい。

作業の禁止:

鍵情報や暗号化データに関する作業、およびシステム設定を許可する前に、認可プロセスが完了するまで、これらの作業を禁止することが望ましい。

認可プロセスの開始:

鍵情報や暗号化データに関する作業、およびシステム設定の変更を行う場合、まず認可プロセスを開始すること。認可プロセスには、必要な承認を得るための手続きが含まれることが望ましい。

承認の取得:

作業やシステム設定の変更に関連する認可を得るために、適切な管理者や関係者からの承認を取得すること。承認は、セキュリティポリシーや規制要件に準拠した形で行われることが望ましい。

プロセスの完了:

必要な承認が得られた後、作業やシステム設定の変更を実行する。認可プロセスが完了し、関連する手続きや承認がすべて確立されるまで、作業を許可しないことが望ましい。

監査とトレーサビリティ:

認可プロセスの完了までの間、作業の禁止や承認の取得のプロセスに関する情報は、適切に記録され、トレーサビリティが確保されることが望ましい。監査のために、関連する情報を必要に応じて提供できるようにすることが望ましい。

遵守と教育:

全ての関係者に対して、作業の禁止や認可プロセスの重要性を啓発し、遵守すること。適切な教育や意識向上活動を通じて、適切な手続きを実行するための理解を促進することが望ましい。

C.7.アクセス制御
C.7.7.
<HYOK を実施できない場合の代替要件>
認可されていない状態又は検知されない状態で、一人で鍵情報に対してアクセス、操作ができないように管理策を適用する。
具体的な管理策には、操作ログの監視、二人体制作業ルール、パスワードの知識分割、管理者による承認後の作業などが挙げられる。

指針の解説

アクセス制御は、認可されていない状態又は検知されない状態で、一人で鍵情報に対してアクセス、操作ができないように管理策を適用すること。具体的な管理策には、操作ログの監視、二人体制作業ルール、パスワードの知識分割、管理者による承認後の作業などを考慮することが望ましく、以下を考慮することが望ましい。

アクセスおよび操作の制限:
HYOK の実施ができない場合でも、認可されていない状態や検知されない状態で、一人で鍵情報に対してアクセスや操作ができないように管理策を適用することが望ましい。

具体的な管理策:
以下の管理策を考慮することが望ましい。
・操作ログの監視:鍵情報へのアクセスや操作が行われた際に、操作ログを監視して不正なアクセスや操作を検知すること。
・二人体制作業ルール:鍵情報に対する重要な操作や変更は、二人以上の関係者による承認や監視のもとで行われる二人体制で行うこと。
・パスワードの知識分割:鍵情報へのアクセスに必要なパスワードを複数の関係者に分割して保持し、単独ではアクセスできないようにすること。
・管理者による承認後の作業:鍵情報に対する重要な作業や変更は、管理者による承認が必要であり、承認後に作業が実行されること。

適切な監視とトレーサビリティ:
代替要件が適用された場合、アクセスや操作に関するログが適切に監視され、不正なアクセスや操作があった場合には迅速に対処されること。ログは適切に保管され、必要に応じて監査や調査のために提供されることが望ましい。

定期的な評価と改善:

代替要件の有効性は定期的に評価され、必要に応じて改善されること。改善は、セキュリティ上のリスクや業務上の要件に基づいて行われることが望ましい。

C.7.アクセス制御
C.7.8.
<HYOK を実施できない場合の代替要件>
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーと、その権限を認可する者を分離すること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーと、その権限を認可する者を分離することが望ましく、以下を考慮することが望ましい。

ユーザーと認可者の分離:
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーと、その権限を認可する者を明確に分離することが望ましい。

役割と責任の分離:
ユーザーと認可者の役割と責任を明確に定義し、混同を避けること。ユーザーは、作業や操作を実行するが、認可者はそれらの作業や操作を承認する役割を果たすことが望ましい。

認可プロセスの実施:
ユーザーに新しい権限を割り当てる前に、適切な認可プロセスを実施すること。認可プロセスには、必要な承認を得るための手続きが含まれることが望ましい。

承認の明確化:
ユーザーが新しい権限を取得する際には、その権限を認可する者が明確に識別されること。承認者は、適切な権限を持ち、役割と責任が明確に定義されることが望ましい。

二重管理体制の確立:
ユーザーと認可者の分離を強化するために、二重管理体制を確立すること。重要な操作や変更に関する承認は、複数の関係者によって行われることが望ましい。

監査とトレーサビリティ:
ユーザーと認可者の分離が適切に実施されていることを確認するために、定期的な監査を実施すること。監査の結果は適切に記録され、トレーサビリティが確保されることが望ましい。

C.7.アクセス制御
C.7.9.
<HYOK を実施できない場合の代替要件>
ユーザーまたは管理者が、鍵情報や暗号化データに関する作業、およびシステム設定を行う際は、活動の監視、監査証跡、管理層による監督などにより不正を防止する管理策を策定すること。

指針の解説
アクセス制御は、ユーザーまたは管理者が、鍵情報や暗号化データに関する作業、およびシステム設定を行う際は、活動の監視、監査証跡、管理層による監督などにより不正を防止する管理策を策定することが望ましく、以下を考慮することが望ましい。

活動の監視:
ユーザーまたは管理者が鍵情報や暗号化データに関する作業やシステム設定を行う際、その活動をリアルタイムで監視すること。監視により、不正行為や異常なアクティビティを早期に検知し、適切な対応を行うことが望ましい。

監査証跡の作成:
活動の監視によって生成されたログやイベントに関する監査証跡を作成すること。監査証跡には、誰が何を行ったか、いつ行ったかなどの情報が含むことが望ましい。

管理層による監督:
不正を防止するために、管理層がユーザーの活動や管理者の行動を監督すること。監督には、定期的なレビューや報告、必要に応じた調査や対応が含まれることが望ましい。

不正行為への迅速な対応:
監視や監査証跡の分析により不正行為が検知された場合、迅速に対応すること。不正行為の発生源を特定し、適切な措置を講じて被害を最小限に抑えることが望ましい。

トレーニングと教育:
ユーザーや管理者に対して、不正行為の防止に関するトレーニングや教育を提供すること。セキュリティ意識の向上や適切な行動規範の普及に努めることが望ましい。

定期的な監査と改善:
管理策の有効性を確認するために、定期的な監査と評価を実施すること。監査結果をもとに、管理策やプロセスを改善してセキュリティレベルを向上させることが望ましい。

C.7.アクセス制御
C.7.10.
<HYOK を実施できない場合の代替要件>
不正を防止する管理策が運用されていること。

指針の解説
アクセス制御は、不正を防止する管理策が運用されていることが望ましく、以下を考慮することが望ましい。

不正を防止する管理策の運用:
不正を防止するための管理策が適切に運用されていることを確認すること。管理策は、組織のセキュリティポリシーや規制要件に基づいて策定され、実施されることが望ましい。

管理策の明確化:
不正を防止するための管理策は、明確に文書化され、関係者に周知されること。文書化された管理策には、目的、対象、手順、責任者などが明確に記載されていることが望ましい。

運用手順の定義:
不正を防止するための管理策の運用手順が明確に定義されていること。運用手順には、誰が責任を持ち、どのようなプロセスやツールを使用して実施されるかが記載されていることが望ましい。

定期的な評価と改善:
不正を防止する管理策の有効性は定期的に評価されること。評価の結果をもとに、必要に応じて管理策やプロセスを改善することが望ましい。

トレーニングと意識向上:
適切なトレーニングや意識向上活動が実施され、関係者が不正行為の識別や報告方法を理解すること。意識向上活動は、セキュリティに関する最新の脅威やベストプラクティスに焦点を当てて行われることが望ましい。

報告と迅速な対応:
不正行為が発生した場合、関係者は適切な報告手順を知り、迅速かつ適切に対応されること。不正行為の報告と対応のプロセスは、適切に文書化され、周知されることが望ましい。

C.8.変更管理

C.8.1.

変更管理ルールと手順を定め、責任者及び開発及び保守の責任者が承認していること。

指針の解説

変更管理は、変更管理ルールと手順を定め、責任者及び開発及び保守の責任者が承認していることが望ましく、以下を考慮することが望ましい。

変更管理ルールの策定:
変更管理ルールは、変更の要求、承認、実装、監視、評価などの手順を包括的に定義すること。ルールは、組織のビジョン、目標、セキュリティポリシーに合わせて策定されることが望ましい。

変更管理手順の定義:
変更管理手順は、変更の要求から承認、実施、評価までの一連のステップを具体的に示すこと。手順には、誰が変更を要求するか、どのように承認が得られるか、実施方法やテスト手法、変更後の評価方法などが含まれることが望ましい。

責任者の任命:
変更管理ルールと手順における責任者は、明確に任命されること。責任者は、変更の要求や承認、実装、監視、評価などの各段階で責任を持つことが望ましい。

開発・保守責任者の承認:
変更管理ルールと手順は、開発および保守の責任者によって承認されること。承認された手順に基づいて変更が行われることで、変更の一貫性と安全性が確保されることが望ましい。

変更の文書化:
変更管理の各段階での重要な決定や活動は、適切に文書化されること。文書化には、変更要求書、承認書、実装手順書、テスト結果、評価報告書などが含まれることが望ましい。

監視と評価:
変更が実施された後も、定期的な監視と評価が行われること。変更の影響や成果を適切に評価し、必要に応じて手順やプロセスを改善することが望ましい。

C.8.変更管理
C.8.2.
変更管理要求が生じた場合、他システムの影響を考慮していること。

指針の解説
変更管理は、変更管理要求が生じた場合、他システムの影響を考慮していることが望ましく、以下を考慮することが望ましい。

変更要求の評価:
変更管理要求が発生した際には、まず他システムへの影響を評価すること。影響の範囲を正確に把握するために、関連する他システムやサービスを明確に特定することが望ましい。

影響範囲の分析:
変更が他システムに与える影響を詳細に分析すること。影響範囲には、データの整合性、システムの可用性、関連するプロセスやワークフローへの影響などが含まれることが望ましい。

関係者の連携:
変更管理プロセスに関連する他システムの所有者や関係者と綿密に連携すること。影響範囲や変更計画に関する情報を共有し、必要な合意や調整を行うことが望ましい。

変更計画の調整:
他システムへの影響を考慮して、変更計画を適切に調整すること。変更のタイミングや手順、テスト計画などが他システムと調和するように検討されることが望ましい。

変更の実施と監視:
変更が実施される際には、他システムへの影響を監視すること。変更の影響が予期せず拡大する可能性がある場合、迅速に対応策を講じることが望ましい。

リスク管理:
他システムへの影響を考慮して、変更に関連するリスクを適切に管理すること。リスクを最小限に抑えるための予防策や回避策を検討し、必要に応じて変更計画を修正することが望ましい。

C.8.変更管理
C.8.3.
緊急の変更要求は文書化され、変更管理手続にしたがっていること。

指針の解説
変更管理は、緊急の変更要求は文書化され、変更管理手続にしたがっていることが望ましく、以下を考慮することが望ましい。

文書化された要求:
緊急の変更要求が発生した場合、要求内容は適切に文書化されること。文書化には、変更の理由、範囲、影響、実施方法などが含まれることが望ましい。

変更管理手続に従う:
緊急の変更要求も、通常の変更と同様に変更管理手続に従うこと。変更管理手続には、要求の提出、評価、承認、実施、監視、評価などのステップが含まれることが望ましい。

優先順位の明確化:
緊急の変更要求の優先順位が明確に定義されること。優先順位は、変更の重要度や緊急性、影響度などを考慮して設定されることが望ましい。

速やかな対応:
緊急の変更要求は速やかに対応されること。変更管理手続の各段階で迅速な判断と行動が求められることが望ましい。

文書化の適正化:

緊急の変更要求が承認された後も、適切に文書化されること。実施された変更の詳細や結果、影響などが適切に記録され、トレーサビリティが確保されることが望ましい。

監視と評価:
緊急の変更が実施された後、変更の影響や成果が適切に監視され、評価されること。不適切な変更や影響の発生があれば、迅速に対処することが望ましい。

C.9. システムクロック

C.9.1.

時刻同期技術を用いてシステム内のシステムクロックの時間精度を確保する仕組みを用意すること。

指針の解説

システムクロックは、時刻同期技術を用いてシステム内のシステムクロックの時間精度を確保する仕組みを用意することが望ましく、以下を考慮することが望ましい。

時刻同期技術の選定:
システムクロックの時間精度を確保するために適切な時刻同期技術を選定すること。NTP（NetworkTimeProtocol)、PTP（PrecisionTimeProtocol）などの技術を使用することが望ましい。

時刻同期サーバの設置:
時刻同期技術を利用するための時刻同期サーバを適切な場所に設置すること。サーバは信頼性が高く、ネットワークへのアクセスが容易であることが望ましい。

クライアントの設定:
各システム内のクライアント（サーバ、ワークステーションなど）に対して、時刻同期サーバへの接続を設定すること。クライアントは定期的に時刻同期サーバから時刻情報を取得し、システムクロックを同期することが望ましい。

セキュリティ検討:
時刻同期技術のセキュリティに関する検討を行うこと。時刻同期通信の暗号化や認証の実施など、セキュリティ対策を講ずることが望ましい。

モニタリングとアラート:
時刻同期の状態をモニタリングし、異常が検知された場合には適切なアラートを発信すること。時刻同期の障害や遅延が早急に対処されることが望ましい。

定期的な評価と調整:
時刻同期の正確性と信頼性を保つために、定期的な評価と調整を行うこと。システムクロックと時刻同期サーバの間の時差を監視し、必要に応じて調整を行うことが望ましい。

C.9.システムクロック C.9.2. **時刻同期技術を用いてデータ保管システム内のシステムクロックの時間精度が維持されていること。** **上記を時刻同期設定やサンプリングしたログ等を確認できること。**

指針の解説
システムクロックは、時刻同期技術を用いてデータ保管システム内のシステムクロックの時間精度が維持されていること。これらを時刻同期設定やサンプリングしたログ等を確認できることが望ましく、以下を考慮することが望ましい。

時刻同期技術の選定:
データ保管システム内のシステムクロックの時間精度を確保するために適切な時刻同期技術を選定すること。NTP（NetworkTimeProtocol）、PTP（PrecisionTimeProtocol）などの信頼性の高い技術を選択することが望ましい。

時刻同期設定の構築:
時刻同期技術を利用するための適切な設定を行うこと。システム内のすべてのデータ保管システムが、時刻同期サーバに正しく接続されていることを確認することが望ましい。

ログの記録と監視:
時刻同期設定やシステムクロックの状態を監視するためのログを記録すること。ログには、時刻同期イベントやシステムクロックの変更履歴などが含まれることが望ましい。

定期的な確認と監査:
時刻同期設定やログを定期的に確認し、システムクロックの時間精度が維持されているこ

とを確認すること。監査により、設定が適切に実施されているかどうかを確認することが望ましい。

アラートの設定:
時刻同期の異常や問題が検知された場合には、適切なアラートが発信されるように設定すること。アラートにより、問題が早急に検知され、対応が行われることが望ましい。

トラブルシューティング手順の準備:
時刻同期の問題が発生した場合に備えて、適切なトラブルシューティング手順を準備すること。手順には、問題の特定方法や解決策が含まれることが望ましい。

D. 鍵管理システム

D. 鍵管理システム

D.1. セキュリティポリシー

D.1.1.

鍵管理システム管理組織はデータを保護するためのセキュリティポリシーを確立すること。セキュリティポリシーには以下を明記すること。

a) 組織の目的に対して適切である。

b) 情報セキュリティ目的を含むか、又は情報セキュリティ目的の設定のための枠組みを示す。

c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。

d) 鍵情報や暗号化データに対するアクセス制御方針

指針の解説

セキュリティポリシーは、暗号化システムとして、暗号化消去における最上位の考え方を組織の外部及び内部に向けた表明である。このような観点より、以下を考慮したセキュリティポリシーを策定することが望ましい。

適切性の確保：

セキュリティポリシーは、組織の目的に対して適切であり、鍵管理システムの目的と一致していることが望ましい。

情報セキュリティ目的の明示：

セキュリティポリシーは、情報セキュリティの目的を明示し、鍵管理システムがデータを保護し、機密性や完全性を確保するための枠組みを提供することが望ましい。

コミットメントの表明：

セキュリティポリシーには、情報セキュリティに関連する適用される要求事項を満たすことへの組織全体のコミットメントが含まれる。組織は、セキュリティポリシーの実施と遵守に必要なリソースやサポートを提供することを約束することが望ましい。

アクセス制御方針の定義：

セキュリティポリシーには、鍵情報や暗号化データに対するアクセス制御方針が明確に定義されることが望ましい。アクセス制御方針は、認証、認可、および監査のプロセスを含み、機密性を維持するための適切な手順を提供することが望ましい。

変更管理と監査：
セキュリティポリシーは、変更管理プロセスを定義し、セキュリティ要件の変化や新たな脅威に対処するためのメカニズムを提供する。ポリシーの監査と評価は定期的に行われ、ポリシーが効果的かつ適切に実施されていることを確認することが望ましい。

教育と啓発：
セキュリティポリシーは、組織内外の関係者に向けて教育と啓発を行うための資源やプログラムを提供する。全ての関係者がセキュリティポリシーを理解し、遵守することが重要であり、適切なトレーニングや情報提供をすることが望ましい。

D.2. システム構成、体制、役割

D.2.1.

鍵管理システム管理組織は、鍵情報や暗号化データに関する作業およびシステム設定を行う自組織の作業者または作業を委託する別組織の役割や責任及び体制について確認できる文書を用意すること。

指針の解説

システム構成、体制、役割は、鍵管理システム管理組織として、暗号化消去におけるシステム構成、体制、役割を明確にすることである。システム構成、体制、役割は、各種規程、体制図等で明確にすることが望ましい。このような観点より、以下を考慮したシステム構成、体制、役割を明確にすることが望ましい。

役割と責任の明確化：
鍵管理システム管理組織は、鍵情報や暗号化データに関する作業を行う自組織の作業者や、作業を委託する別組織の役割と責任を明確に定義すること。各作業者や組織が担当する業務内容や責任範囲、連絡先などを含む文書を用意することが望ましい。

体制の整備：
鍵管理システム管理組織は、鍵情報や暗号化データに関する作業やシステム設定を行うための適切な体制を整備する。体制には、必要な資源や権限、監督体制、連絡先情報などが含まれることが望ましい。

文書の作成：
鍵情報や暗号化データに関する作業やシステム設定に関する役割や責任、体制について確

認できる文書を作成する。文書はわかりやすく、具体的な情報を含み、関係者が容易にアクセスできる場所に保管されることが望ましい。

定期的なレビューと更新：
文書は定期的にレビューされ、必要に応じて更新されること。変更があった場合や新たな要員が加わった場合など、文書の内容に変更が生じた際には、迅速に更新することが望ましい。

関係者への通知と教育：
関係者に対して、鍵情報や暗号化データに関する作業や体制についての文書を適切に通知し、説明すること。関係者が自らの役割や責任を理解し、適切に業務を遂行できるようにするために、必要な教育やトレーニングを実施することが望ましい。

D.2. システム構成、体制、役割
D.2.2.
鍵管理システム管理組織は、鍵情報や暗号化データを取り扱うシステム及びその周辺環境の構成やデータフローが確認できる文書を用意すること。

指針の解説
鍵管理システム管理組織は、鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できる文書を用意すること。これらの文書は、該当システムの構成図等で明確にすることが望ましい。このような観点より、以下を考慮した鍵情報や暗号化データを取り扱うシステムの構成やデータフローが確認できることを文書化することが望ましい。

システム構成の明確化：
鍵管理システム管理組織は、鍵情報や暗号化データを取り扱うシステムの構成を明確に文書化する。これらの文書には、システムのハードウェア、ソフトウェア、ネットワーク構成などが含まれていることが望ましい。

データフローの記述：
鍵情報や暗号化データの取り扱いに関するデータフローを記述する。データの生成元から保存、処理、転送、削除までの手順やプロセスが明確に記載されることが望ましい。

セキュリティ対策の説明：
システムの構成やデータフローに関連するセキュリティ対策が文書に含まれること。アク

セス制御、暗号化、監査ログの設定など、セキュリティを強化するための具体的な措置が記載されることが望ましい。

システム間の統合と依存関係の説明：
鍵情報や暗号化データを取り扱うシステムが他のシステムとどのように統合されているか、および依存関係があるかを明確に説明すること。他のシステムとのデータのやり取りや、データの共有方法などが示されることが望ましい。

文書のアップデートとレビュー：
文書は定期的にレビューされ、必要に応じてアップデートされること。システムの変更やアップグレード、新たなセキュリティ要件の追加などがあった場合には、文書も適切に更新されることが望ましい。

関係者への共有と教育：
システム構成やデータフローに関する文書は関係者に適切に共有され、理解されるようにすること。関係者がシステムの構成やデータフローを把握し、セキュリティ上の重要性を理解できるようにするために、適切な教育やトレーニングを提供することが望ましい。

D.3.経営陣の責任

D.3.1.

鍵管理システム管理組織の経営陣は、作業者が鍵情報や暗号化データに関する作業、およびシステム設定へのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備すること。

指針の解説

鍵管理システム管理組織の経営陣は、作業者が鍵情報や暗号化データに関する作業、およびシステム設定へのアクセスが許可される前に、情報セキュリティの役割及び責任について、要点を適切に伝える仕組みを整備すること。整備方法としては、役割責任表などが考えられる。これらの役割責任の整備方法には、以下を考慮することが望ましい。

経営陣の役割と責任の明確化:
経営陣は情報セキュリティの重要性を理解し、その責任を認識すること。情報セキュリティポリシーの策定と維持に責任を持つことが望ましい。

作業者への教育と訓練:
作業者に対し、情報セキュリティの重要性と責任を定期的に教育し、訓練すること。鍵情報や暗号化データの取り扱い方法とシステムへのアクセス権限に関するガイドラインを提供することが望ましい。

情報セキュリティポリシーの普及:
情報セキュリティポリシーを組織内で普及させ、全ての作業者が理解し遵守することを確保すること。ポリシーの更新や変更があった場合は、適切に伝達し、理解を確認することが望ましい。

アクセスコントロールの強化:
鍵情報や暗号化データへのアクセスは、必要最小限の権限で制限すること。アクセス権限の与えられた作業者は、その権限の範囲内でのみ作業を行うことを徹底することが望ましい。

監査と評価:
情報セキュリティの実施状況を定期的に監査し、遵守状況を評価すること。監査結果に基づき、改善点を特定し、適切な対策を講じることが望ましい。

リスク管理と対応:
情報セキュリティに関連するリスクを評価し、適切な管理策を策定すること。セキュリティインシデントが発生した場合は、速やかに対応し、適切な措置を講じることが望ましい。

継続的な改善:
情報セキュリティの方針や手順を継続的に改善し、最新の脅威やベストプラクティスに対応すること。組織内の全てのメンバーが、情報セキュリティの向上に協力する文化を醸成することが望ましい。

D.3. 経営陣の責任

D.3.2.

鍵管理システム管理組織の経営陣は、作業者に対し、組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組みを整備すること。

指針の解説

鍵管理システム管理組織の経営陣は、作業者に対し、組織内での役割において、情報セキュ

リティについて期待することを示すための指針を提供する仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

経営陣のリーダーシップ:
経営陣は情報セキュリティの重要性を理解し、その重要性を従業員に示すことでリーダーシップを発揮すること。情報セキュリティに関する組織全体の方針や目標を明確に定義し、従業員に伝達することが望ましい。

情報セキュリティの期待の明確化:
経営陣は、従業員に対し、情報セキュリティに関する期待事項を具体的に示すこと。作業者には、データの取り扱い、アクセス権の管理、セキュリティポリシーの遵守などに関する具体的な指針を提供することが望ましい。

教育と訓練の提供:
情報セキュリティに関する教育と訓練プログラムを組織内で定期的に実施し、作業者の能力を向上させること。従業員が情報セキュリティポリシーを遵守し、セキュリティのベストプラクティスを理解するための機会を提供することが望ましい。

コミュニケーションの促進:
経営陣は、従業員とのコミュニケーションを通じて、情報セキュリティに関する重要な情報や変更事項を伝達すること。従業員は、情報セキュリティに関する懸念や提案を提出するための適切なチャネルを提供することが望ましい。

フィードバックと改善:
経営陣は、従業員からのフィードバックを受け入れ、情報セキュリティプロセスやポリシーの改善に活かすこと。継続的な監視と評価を通じて、情報セキュリティの効果を定期的に確認し、必要に応じて改善を行うことが望ましい。

遵守と報奨:
経営陣は、情報セキュリティポリシーの遵守を奨励し、従業員が適切なセキュリティ対策を実践することを評価すること。優れた情報セキュリティ実践に対する報奨制度を導入し、従業員のモチベーションを高めることが望ましい。

D.3. 経営陣の責任

D.3.3.

鍵管理システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備すること。

指針の解説

鍵管理システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティのための方針群に従うように動機付ける仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

組織の情報セキュリティポリシーの明確化:
経営陣は、組織の情報セキュリティポリシーを明確に定義し、従業員に理解しやすい形で伝えること。ポリシーは、データ保管、アクセス管理、セキュリティプロトコルなどに関する具体的な方針を含むことが望ましい。

教育と意識向上の促進:
作業者に対し、情報セキュリティの重要性を定期的に強調し、意識向上を図る教育プログラムを実施すること。定期的なトレーニングやシミュレーションを通じて、セキュリティに関する最新の脅威や対策について従業員を啓発することが望ましい。

動機付けと報奨:
作業者が情報セキュリティポリシーに従うことを奨励する報奨制度を導入すること。遵守した場合の報奨や、セキュリティ違反を減らすことでチームや個人の評価に対するポジティブな影響を示すことが望ましい。

フィードバックと改善:
従業員からのフィードバックを受け入れ、ポリシーの実施に関する問題や提案を積極的に取り入れること。ポリシーの改善点や不明瞭な部分を特定し、適切な修正を行うことで、従業員の満足度と遵守率を向上させることが望ましい。

ロールモデルの示唆:
経営陣や管理職は、情報セキュリティポリシーを率先して遵守し、従業員に良いロールモデルを示すことが重要であること。従業員は、リーダーシップからのポジティブな影響を受け、ポリシーに積極的に従う傾向が高まることが望ましい。

継続的な監視と改善:
情報セキュリティポリシーの遵守状況を継続的に監視し、違反や問題を早期に検出すること。監視結果に基づいてポリシーの改善を行い、組織全体のセキュリティレベルを向上させることが望ましい。

D.3. 経営陣の責任

D.3.4.

鍵管理システム管理組織の経営陣は、作業者に対し、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備すること。

指針の解説

鍵管理システム管理組織の経営陣は、作業者に対し、組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

役割と責任の明確化:
経営陣は、自らの情報セキュリティに関する役割と責任を明確に定義し、作業者に対して明示すること。各作業者の役割と責任が情報セキュリティの目標と一致していることを確認することが望ましい。

教育とトレーニングの提供:
情報セキュリティに関する教育プログラムやトレーニングを組織内で実施し、経営陣と作業者の両方に対して情報セキュリティに関する知識を向上させること。役割と責任に関連する情報セキュリティのトレーニングを提供し、一定の水準を達成するためのサポートを行うことが望ましい。

規定の策定と遵守の促進:
経営陣は、情報セキュリティポリシーと手順を策定し、それらの遵守を促進すること。自らの役割と責任に関連する情報セキュリティ規定を従業員に明確に伝え、その遵守を監視することが望ましい。

監査と評価:

情報セキュリティの実施状況を定期的に監査し、遵守水準を評価すること。監査結果に基づいて、必要な対策や改善点を特定し、適切な対応を講じることが望ましい。

透明性とコミュニケーション:
経営陣は、情報セキュリティに関する透明性を確保し、作業者とのコミュニケーションを促進すること。情報セキュリティに関する重要な変更や問題について、適切な情報を提供し、従業員からのフィードバックを受け入れることが望ましい。

継続的な向上:
経営陣は、情報セキュリティの向上に向けて継続的な取り組みを行い、一定水準を維持するだけでなく、常に向上を目指すこと。新たな脅威や技術の進展に対応するため、定期的な情報セキュリティの再評価と改善を行うことが望ましい。

D.3. 経営陣の責任
D.3.5.
鍵管理システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備すること。

指針の解説
鍵管理システム管理組織の経営陣は、作業者に対し、組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

情報セキュリティ方針の明確化:
経営陣は、組織の情報セキュリティ方針を明確に定義し、作業者に対して遵守を求めること。方針は、データの保護、アクセス管理、セキュリティ対策などに関する具体的なガイドラインを含むことが望ましい。

雇用条件への組み込み:
情報セキュリティ方針や適切な仕事のやり方を含む、情報セキュリティへの遵守が雇用条件として組み込まれること。作業者は雇用契約や規定を受け入れる際に、情報セキュリティ方針に同意することが求められることが望ましい。

教育とトレーニングの提供:

作業者に対し、情報セキュリティ方針や適切な仕事のやり方に関する教育プログラムやトレーニングを提供すること。新入社員や関連部署の従業員には、情報セキュリティの基本や方針に関する研修を実施することが望ましい。

遵守の監視と評価:
経営陣は、情報セキュリティ方針の遵守を定期的に監視し、適切な評価を行うこと。違反や問題が発生した場合には、適切な対応を講じ、必要に応じて改善を行うことが望ましい。

報奨とリワード:
情報セキュリティ方針への遵守や適切な仕事のやり方を実践する作業者には、報奨やリワードを与える制度を導入すること。優れた情報セキュリティ実践に対する認定や特典を提供し、作業者のモチベーションを高めることが望ましい。

継続的な改善:
情報セキュリティ方針や適切な仕事のやり方を継続的に改善し、組織のセキュリティレベルを向上させる取り組みを行うこと。ユーザーフィードバックや業界のベストプラクティスを活用して、常に最新の状況に適応することが望ましい。

D.3. 経営陣の責任

D.3.6.

鍵管理システム管理組織の経営陣は、作業者に対し、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備すること。

指針の解説

鍵管理システム管理組織の経営陣は、作業者に対し、適切な技能及び資格を保持し、定期的に教育を受けさせる仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

技能と資格の要件の明確化:
作業者が持つべき技能や資格について明確な基準を設定する。これには、暗号化技術の専門知識、セキュリティ管理のスキル、および関連する業界の規制や規格に関する理解が含まれることが望ましい。

教育プログラムの設計:

定期的な教育プログラムを策定する。このプログラムは、新しい技術や脅威に関する最新の情報を提供し、作業者のスキルを向上させることを目的とする。教育プログラムは、オンサイトのトレーニング、外部のトレーニング機関との提携、オンラインリソースの利用など、さまざまな方法で提供することが望ましい。

定期的な評価と更新:
教育プログラムの効果を評価し、必要に応じて更新する。技術の進化や新たな脅威に対応するために、プログラムを定期的に再評価し、改善することが望ましい。

記録の管理:
作業者の教育履歴や資格情報を適切に管理し、追跡する。これにより、必要なトレーニングが受けられ、資格が維持されることを保証することが望ましい。

コミュニケーションとフィードバックの促進:
作業者と管理層の間で開かれたコミュニケーションを促進し、フィードバックを収集する。作業者が教育プログラムや資格要件に関する疑問や提案を提出できるようにすることが望ましい。

D.3. 経営陣の責任

D.3.7.

鍵管理システム管理組織の経営陣は、作業者に対し、情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組みを整備すること。

指針の解説

鍵管理システム管理組織の経営陣は、作業者に対し、情報セキュリティのための方針群又は手順への違反を報告するため、例えば、内部告発など、匿名の報告経路を提供する仕組みを整備すること。これらの整備方法には、以下を考慮することが望ましい。

匿名報告経路の設置:
経営陣は、情報セキュリティの方針や手順への違反を匿名で報告するための専用の報告経路を設置すること。この報告経路は、作業者が安心して違反を報告できるよう、厳格な機密性と匿名性が確保されることが望ましい。

報告手順の明確化:
匿名報告経路の手順と方法を明確に定義し、作業者に周知すること。作業者が容易にアクセスできるよう、報告経路の情報を組織内の適切な場所に掲示することが望ましい。

報告者の保護:
投稿者の匿名性を保護するための措置を講じること。投稿者が報復や不利益を受けることなく、違反報告を行えるよう、経営陣は適切な対策を講じることが望ましい。

報告内容の処理と調査:
投稿された違反報告は適切に処理され、必要に応じて迅速かつ公正な調査が行われること。違反報告に対する対応は透明性が保たれ、関係者に適切に通知されることが望ましい。

報告者へのフィードバック:
匿名報告者に対し、報告内容が受領されたことや対応状況についてのフィードバックを提供すること。報告者に対する感謝の意を示し、組織としての報告に対する積極的な姿勢を示すことが望ましい。

継続的な改善と透明性:
匿名報告経路の効果と透明性を継続的に評価し、改善を行うこと。経営陣は報告経路の存在や活動について、定期的に組織内外に公表し、透明性を確保することが望ましい。

D.3. 経営陣の責任

D.3.8.

鍵管理システム管理組織の経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動すること。

指針の解説

鍵管理システム管理組織の経営陣は、情報セキュリティのための方針群、手順及び管理策に対する支持を実証し、手本となるように行動すること。これらの行動方法には、以下を考慮することが望ましい。

方針と手順の明確化:
経営陣は、情報セキュリティに関する方針群、手順、および管理策を明確に定義し、組織内での遵守を促すこと。方針と手順は、データ保管、アクセス管理、セキュリティポリシー遵

守などに関する具体的な指針を含むことが望ましい。

支持の実証:
経営陣は、情報セキュリティ方針と手順への支持を実証するために、行動によってそれを示すこと。情報セキュリティへの積極的な関与や適切な対策の実施を通じて、経営陣が方針と手順に従っていることを明確にすることが望ましい。

透明性とコミュニケーション:
経営陣は、情報セキュリティに関する方針や手順についての透明性を確保し、従業員とのコミュニケーションを促進すること。方針や手順の目的や重要性を明確に説明し、従業員がその重要性を理解し、遵守するようサポートすることが望ましい。

リーダーシップの示唆:
経営陣は、情報セキュリティに関するリーダーシップを示し、従業員に良いロールモデルとなること。定期的な情報セキュリティの挑戦や成功に関する報告を通じて、経営陣が方針と手順に対するコミットメントを強調することが望ましい。

継続的な評価と改善:
経営陣は、情報セキュリティ方針と手順の効果を継続的に評価し、必要に応じて改善を行うこと。新たな脅威や技術の進展に対応するため、定期的な方針と手順の再評価を実施し、組織全体のセキュリティレベルを向上させることが望ましい。

D.4.委託先管理

D.4.1.

鍵管理システム管理組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を委託する別組織が、作業者に対して以下を整備していることを情報セキュリティのための方針群、手順及び管理策で確認すること。

- **組織内での役割において、情報セキュリティについて期待することを示すための指針を提供する仕組み**
- **組織の情報セキュリティのための方針群に従うように動機付ける仕組み**
- **組織内における自らの役割及び責任に関連する情報セキュリティの認識について、一定の水準を達成する仕組み**
- **組織の情報セキュリティ方針及び適切な仕事のやり方を含め、雇用条件に従うようにする仕組み**
- **適切な技能及び資格を保持し、定期的に教育を受けさせる仕組み**
- **情報セキュリティのための方針群又は手順への違反を報告するための、匿名の報告経路を提供する（例えば、内部告発）仕組み**

指針の解説

鍵管理システム管理組織の経営陣は、鍵情報や暗号化データに関する作業およびシステム設定を委託する別組織が、作業者に対して、情報セキュリティについて期待することを示すための指針を提供する仕組みなどを整備すること。整備方法には、以下を考慮することが望ましい。

指針の提供：
別組織が作業者に対して情報セキュリティに関する役割や期待することを示す指針を提供していることを確認すること。これにより、作業者は自らの役割を理解し、適切なセキュリティプラクティスを遵守することが期待されることが望ましい。

動機付けの仕組み：
別組織や作業者が情報セキュリティ方針に従うように動機付ける仕組みを整備していることを確認すること。報奨制度や教育プログラム、適切なフィードバックメカニズムなどが含まれることが望ましい。

認識の向上：
別組織が作業者の情報セキュリティに関する認識を向上させるための仕組みを提供していることを確認すること。トレーニングや教育プログラム、評価や認定制度などが含まれることが望ましい。

雇用条件への準拠：
別組織や作業者が情報セキュリティ方針や適切な業務手順に従うようにするための雇用条件を整備していることを確認すること。これには、契約や規則、社内規程などが含まれることが望ましい。

教育と資格の提供：
別組織や作業者が適切な技能や資格を保持し、定期的に情報セキュリティに関する教育を受ける仕組みを提供していることを確認すること。これにより、作業者は最新のセキュリティプラクティスや技術について常に学び続けることが望ましい。

匿名報告経路の提供：
別組織が情報セキュリティ方針や手順への違反を報告するための匿名の報告経路を提供していることを確認すること。これにより、作業者はセキュリティに関する懸念や問題を匿名で報告しやすくすることが望ましい。

D.5.アクセス制御

D.5.1.

鍵情報や暗号化データに関する作業、およびシステム設定の権限の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理すること。

指針の解説

アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理することが望ましく、以下を考慮することが望ましい。

アクセス制御方針への準拠:
鍵情報や暗号化データに関する作業およびシステム設定の権限は、関連するアクセス制御方針に厳密に従うことが望ましい。

正式な認可プロセス:
鍵情報や暗号化データに関連する作業やシステム設定の変更は、正式な認可プロセスによって管理される。認可プロセスは、適切な管理者や責任者によって承認されることが望ましい。

アクセス権の割り当て:
鍵情報や暗号化データに関連する作業やシステム設定の実行に必要なアクセス権は、最小限の特権の原則に従って割り当てること。必要最低限の権限のみが付与され、原則として「必要最小限の原則」に従うことが望ましい。

アクセス権のレビューと更新:
アクセス権は定期的にレビューされ、必要に応じて更新すること。レビューは、変更された役割や業務の要件、セキュリティ上のリスクに基づいて行われることが望ましい。

監査とトレーサビリティ:
鍵情報や暗号化データに関連する作業やシステム設定の変更は、監査可能でトレーサビリティのある方法で実行される必要がある。すべての変更は、適切なログに記録され、必要に応じて監査の対象とすることが望ましい。

教育と意識向上:
鍵情報や暗号化データの管理に関わるスタッフには、適切な教育と意識向上の機会が提供される。スタッフは、セキュリティポリシーやアクセス制御方針に従うことの重要性について教育されることが望ましい。

D.5.アクセス制御
D.5.2.
鍵情報や暗号化データに関する作業、およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割当てていること。
システム設定の権限を割り当てるアカウントはユーザー個人に紐づいたアカウントとし、複数ユーザーで共有利用するアカウントにはシステム設定権限を割り当てないことが望ましい。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割当てていること。システム設定の権限を割り当てるアカウントはユーザー個人に紐づいたアカウントとし、複数ユーザーで共有利用するアカウントにはシステム設定権限を割り当てないことが望ましく、以下を考慮することが望ましい。

最小限の要求事項に基づく権限の割り当て:
鍵情報や暗号化データに関する作業およびシステム設定の権限は、ユーザーの職務上の役割のための最小限の要求事項に基づいて割り当てること。ユーザーに必要な権限のみが付与され、原則として「必要最小限の原則」に従うことが望ましい。

個人に紐づいたアカウントの使用:
システム設定の権限を割り当てるアカウントは、ユーザー個人に紐づいた個別のアカウントとすること。個人に紐づいたアカウントを使用することで、個々のユーザーのアクションを追跡し、責任の所在を明確にすることが望ましい。

共有利用アカウントでの権限割り当ての回避:
複数ユーザーで共有利用するアカウントには、システム設定権限を割り当てないことが望ましい。共有利用アカウントでは、個々のユーザーのアクセス管理やトレーサビリティが困難になるため、個人に紐づいたアカウントの使用を推奨することが望ましい。

役割に応じた権限の定義:
各ユーザーの役割や責任に応じて、適切な権限が定義される。ユーザーの役割や業務の変更に応じて、権限の再評価と調整が行われることが望ましい。

権限のレビューと更新:
権限は定期的にレビューされ、必要に応じて更新すること。レビューは、変更された役割や業務の要件、セキュリティ上のリスクに基づいて行われることが望ましい。

D.5.アクセス制御
D.5.3.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、アクセス権の変更・消去していること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、アクセス権の変更・消去していることが望ましく、以下を考慮することが望ましい。

人事異動や退職によるアクセス権の管理:
鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てられたユーザーが、人事異動や退職等により交代した場合は、速やかにアクセス権の変更または消去することが望ましい。

変更の手順:
アクセス権の変更または消去は、所定の手順に従って行うこと。変更手順は、組織のポリシーや手順に従い、必要な承認を得ることが望ましい。

アクセス権の変更:
人事異動や退職等によるユーザー交代の場合、新しいユーザーに適切なアクセス権を割り当てること。新しいユーザーの役割や責任に応じて、適切な権限を与えることが望ましい。

アクセス権の消去:

旧ユーザーのアクセス権は速やかに消去すること。消去手順は、情報セキュリティポリシーやアクセス制御方針に従って行われることが望ましい。

トレーサビリティの確保:
アクセス権の変更や消去の過程は、適切に記録され、トレーサビリティが確保すること。変更の理由や実行者、実施日時などの情報が記録されることが望ましい。

監査とレビュー:
アクセス権の変更や消去の過程は、定期的に監査され、必要に応じてレビューが行われること。監査とレビューにより、アクセス権の変更や消去が適切に実施されていることが確認されることが望ましい。

D.5.アクセス制御
D.5.4.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーやシステムを定められた間隔でレビューしていること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーやシステムを定められた間隔でレビューしていることが望ましく、以下を考慮することが望ましい。

レビューの頻度の定義:
鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てられたユーザーやシステムは、定められた間隔でレビューすること。レビューの間隔は、セキュリティポリシーや業界のベストプラクティスに基づいて定義されることが望ましい。

レビューの対象:
レビューの対象には、鍵情報や暗号化データに関する作業やシステム設定の権限を持つすべてのユーザーやシステムが含まれること。レビューの対象は、管理者やセキュリティチームによって明確に定義されることが望ましい。

レビューの手順:
レビューは、所定の手順に従って実施すること。レビュー手順は、アクセス権の確認、権限

の適合性の評価、不正なアクセスの検出などを含むことが望ましい。

変更の必要性の評価:
レビューの結果、アクセス権の変更や更新が必要である場合は、適切な手順に従って変更が実施されること。変更が必要な場合、正式な承認プロセスに従い、変更が実行されることが望ましい。

トレーサビリティの確保:
レビューの過程や結果は、適切に記録され、トレーサビリティが確保されること。レビューの実行者や結果、変更が必要とされた理由などの情報が記録されることが望ましい。

改善の実施:
レビューの結果に基づいて、適切な改善策が実施されること。改善策は、セキュリティポリシーや業界のベストプラクティスに準拠して実施されることが望ましい。

D.5.アクセス制御
D.5.5.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てた全ての認可を記録していること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てた全ての認可を記録していることが望ましく、以下を考慮することが望ましい。

認可の記録:
鍵情報や暗号化データに関する作業やシステム設定の権限を割り当てる際、全ての認可は正式に記録されること。認可の記録には、誰がどのような権限を得たか、ならびにその権限が割り当てられた日時などの情報が含まれることが望ましい。

記録の内容:
記録には、次の情報が含まれることが望ましい
・ユーザーまたはシステムの識別子
・割り当てられた権限やロール
・権限の有効期限（必要な場合）

・権限の割り当て日時
・認可を行った管理者の識別子

情報の保管:
認可の記録は、安全に保管されること。記録は、情報セキュリティの最高水準に従い、適切なアクセス制御が施された場所に保存されることが望ましい。

記録の追跡:
認可の記録は、変更履歴を追跡するために適切に管理されること。記録が変更された場合、変更の内容と理由が適切に文書化されることが望ましい。

監査とトレーサビリティ:
認可の記録は、定期的な監査やセキュリティ検証の対象とすること。記録の監査により、権限の割り当てが適切に実施され、セキュリティポリシーに準拠していることが確認されることが望ましい。

D.5.アクセス制御
D.5.6.
認可プロセスが完了するまで、鍵情報や暗号化データに関する作業、およびシステム設定を許可しないこと。

指針の解説
アクセス制御は、認可プロセスが完了するまで、鍵情報や暗号化データに関する作業、およびシステム設定を許可しないことが望ましく、以下を考慮することが望ましい。

作業の禁止:
鍵情報や暗号化データに関する作業、およびシステム設定を許可する前に、認可プロセスが完了するまで、これらの作業を禁止することが望ましい。

認可プロセスの開始:
鍵情報や暗号化データに関する作業、およびシステム設定の変更を行う場合、まず認可プロセスを開始すること。認可プロセスには、必要な承認を得るための手続きが含まれることが望ましい。

承認の取得:
作業やシステム設定の変更に関連する認可を得るために、適切な管理者や関係者からの承認を取得すること。承認は、セキュリティポリシーや規制要件に準拠した形で行われることが望ましい。

プロセスの完了:
必要な承認が得られた後、作業やシステム設定の変更を実行する。認可プロセスが完了し、関連する手続きや承認がすべて確立されるまで、作業を許可しないことが望ましい。

監査とトレーサビリティ:
認可プロセスの完了までの間、作業の禁止や承認の取得のプロセスに関する情報は、適切に記録され、トレーサビリティが確保されることが望ましい。監査のために、関連する情報を必要に応じて提供できるようにすることが望ましい。

遵守と教育:
全ての関係者に対して、作業の禁止や認可プロセスの重要性を啓発し、遵守すること。適切な教育や意識向上活動を通じて、適切な手続きを実行するための理解を促進することが望しい。

D.5.アクセス制御

D.5.7.

認可されていない状態又は検知されない状態で、一人で鍵情報に対してアクセス、操作ができないように管理策を適用する。
具体的な管理策には、操作ログの監視、二人体制作業ルール、パスワードの知識分割、管理者による承認後の作業などが挙げられる。

指針の解説

アクセス制御は、認可されていない状態又は検知されない状態で、一人で鍵情報に対してアクセス、操作ができないように管理策を適用すること。具体的な管理策には、操作ログの監視、二人体制作業ルール、パスワードの知識分割、管理者による承認後の作業などを考慮することが望ましく、以下を考慮することが望ましい。

アクセスおよび操作の制限:
認可されていない状態や検知されない状態で、一人で鍵情報に対してアクセスや操作がで

きないように管理策を適用することが望ましい。

具体的な管理策:
以下の管理策を考慮することが望ましい。
・操作ログの監視:鍵情報へのアクセスや操作が行われた際に、操作ログを監視して不正なアクセスや操作を検知すること。
・二人体制作業ルール:鍵情報に対する重要な操作や変更は、二人以上の関係者による承認や監視のもとで行われる二人体制で行うこと。
・パスワードの知識分割:鍵情報へのアクセスに必要なパスワードを複数の関係者に分割して保持し、単独ではアクセスできないようにすること。
・管理者による承認後の作業:鍵情報に対する重要な作業や変更は、管理者による承認が必要であり、承認後に作業が実行されること。

適切な監視とトレーサビリティ:
代替要件が適用された場合、アクセスや操作に関するログが適切に監視され、不正なアクセスや操作があった場合には迅速に対処されること。ログは適切に保管され、必要に応じて監査や調査のために提供されることが望ましい。

定期的な評価と改善:
代替要件の有効性は定期的に評価され、必要に応じて改善されること。改善は、セキュリティ上のリスクや業務上の要件に基づいて行われることが望ましい。

D.5.アクセス制御
D.5.8.
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーと、その権限を認可する者を分離すること。

指針の解説
アクセス制御は、鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザーと、その権限を認可する者を分離することが望ましく、以下を考慮することが望ましい。

ユーザーと認可者の分離:
鍵情報や暗号化データに関する作業、およびシステム設定の権限を割り当てられたユーザ

ーと、その権限を認可する者を明確に分離することが望ましい。

役割と責任の分離:
ユーザーと認可者の役割と責任を明確に定義し、混同を避けること。ユーザーは、作業や操作を実行するが、認可者はそれらの作業や操作を承認する役割を果たすことが望ましい。

認可プロセスの実施:
ユーザーに新しい権限を割り当てる前に、適切な認可プロセスを実施すること。認可プロセスには、必要な承認を得るための手続きが含まれることが望ましい。

承認の明確化:
ユーザーが新しい権限を取得する際には、その権限を認可する者が明確に識別されること。承認者は、適切な権限を持ち、役割と責任が明確に定義されることが望ましい。

二重管理体制の確立:
ユーザーと認可者の分離を強化するために、二重管理体制を確立すること。重要な操作や変更に関する承認は、複数の関係者によって行われることが望ましい。

監査とトレーサビリティ:
ユーザーと認可者の分離が適切に実施されていることを確認するために、定期的な監査を実施すること。監査の結果は適切に記録され、トレーサビリティが確保されることが望ましい。

D.5.アクセス制御
D.5.9.
ユーザーまたは管理者が、鍵情報や暗号化データに関する作業、およびシステム設定を行う際は、活動の監視、監査証跡、管理層による監督などにより不正を防止する管理策を策定すること。

指針の解説
アクセス制御は、ユーザーまたは管理者が、鍵情報や暗号化データに関する作業、およびシステム設定を行う際は、活動の監視、監査証跡、管理層による監督などにより不正を防止する管理策を策定することが望ましく、以下を考慮することが望ましい。

活動の監視:
ユーザーまたは管理者が鍵情報や暗号化データに関する作業やシステム設定を行う際、その活動をリアルタイムで監視すること。監視により、不正行為や異常なアクティビティを早期に検知し、適切な対応を行うことが望ましい。

監査証跡の作成:
活動の監視によって生成されたログやイベントに関する監査証跡を作成すること。監査証跡には、誰が何を行ったか、いつ行ったかなどの情報が含むことが望ましい。

管理層による監督:
不正を防止するために、管理層がユーザーの活動や管理者の行動を監督すること。監督には、定期的なレビューや報告、必要に応じた調査や対応が含まれることが望ましい。

不正行為への迅速な対応:
監視や監査証跡の分析により不正行為が検知された場合、迅速に対応すること。不正行為の発生源を特定し、適切な措置を講じて被害を最小限に抑えることが望ましい。

トレーニングと教育:
ユーザーや管理者に対して、不正行為の防止に関するトレーニングや教育を提供すること。セキュリティ意識の向上や適切な行動規範の普及に努めることが望ましい。

定期的な監査と改善:
管理策の有効性を確認するために、定期的な監査と評価を実施すること。監査結果をもとに、管理策やプロセスを改善してセキュリティレベルを向上させることが望ましい。

D.5. アクセス制御
D.5.10.
不正を防止する管理策が運用されていること。

指針の解説
アクセス制御は、不正を防止する管理策が運用されていることが望ましく、以下を考慮することが望ましい。

不正を防止する管理策の運用:

不正を防止するための管理策が適切に運用されていることを確認すること。管理策は、組織のセキュリティポリシーや規制要件に基づいて策定され、実施されることが望ましい。

管理策の明確化:
不正を防止するための管理策は、明確に文書化され、関係者に周知されること。文書化された管理策には、目的、対象、手順、責任者などが明確に記載されていることが望ましい。

運用手順の定義:
不正を防止するための管理策の運用手順が明確に定義されていること。運用手順には、誰が責任を持ち、どのようなプロセスやツールを使用して実施されるかが記載されていることが望ましい。

定期的な評価と改善:
不正を防止する管理策の有効性は定期的に評価されること。評価の結果をもとに、必要に応じて管理策やプロセスを改善することが望ましい。

トレーニングと意識向上:
適切なトレーニングや意識向上活動が実施され、関係者が不正行為の識別や報告方法を理解すること。意識向上活動は、セキュリティに関する最新の脅威やベストプラクティスに焦点を当てて行われることが望ましい。

報告と迅速な対応:
不正行為が発生した場合、関係者は適切な報告手順を知り、迅速かつ適切に対応されること。不正行為の報告と対応のプロセスは、適切に文書化され、周知されることが望ましい。

D.6.鍵のライフサイクル管理

D.6.1.

鍵の保管にはFIPS140-2またはFIPS140-3 レベル1準拠の製品を使用すること。

指針の解説

鍵のライフサイクル管理は、鍵の保管にはFIPS140-2またはFIPS140-3 レベル1準拠の製品を使用することが望ましく、以下を考慮することが望ましい。

FIPS140-2 または FIPS140-3 レベル 1 の準拠性確保:
鍵の保管には、FIPS140-2 または FIPS140-3 規格に基づいたレベル 1 の準拠性を確保することにより、鍵のセキュリティが確保され、規制要件を満たすことが望まれる。

適切な鍵管理システムの選択:
FIPS140-2 または FIPS140-3 に準拠した製品を使用して、適切な鍵管理システムを導入する。これには、鍵の生成、保存、分配、および削除に関する手順が含まれることが望ましい。

鍵の安全な保管場所の確保:
鍵を保管する物理的な場所やデジタル環境を選定し、適切なセキュリティ対策を実施する。これには、アクセス制御、監視、ログの記録、および適切なバックアップ手順の確立が含まれることが望ましい。

定期的な監査と評価:
鍵の保管プロセスを定期的に監査し、セキュリティポリシーと規制要件に準拠していることを確認する。また、鍵管理システムの性能やセキュリティの評価を実施し、必要に応じて改善を行うことが望ましい。

継続的なトレーニングと教育:
鍵管理担当者に対して、適切なトレーニングと教育を提供し、FIPS 規格に基づくベストプラクティスを理解させる。これにより、鍵の適切な保管とセキュリティの確保が維持されることが望まれる。

D.6.鍵のライフサイクル管理
D.6.2.
データオーナー組織が鍵の生成ログの提示を要求した際は、生成ログをデータオーナー組織に提示すること。

指針の解説
データオーナー組織が鍵の生成ログの提示を要求した際は、生成ログをデータオーナー組織に提示することが望ましく、以下を考慮することが望ましい。

要求の受付と評価:
データオーナー組織から鍵の生成ログの提示要求を受けた場合、すぐに受け付け、要求内容

を評価する。要求が妥当であるかどうかを確認し、必要な場合は追加情報を要求することが望ましい。

適切なログの抽出と提供:
鍵の生成ログが必要とされる場合、適切な手順に基づいてログを抽出し、データオーナー組織に提供する。ログの提供は、安全で適切な方法で行われることが望ましい。

機密情報の保護:
鍵の生成ログには機密情報が含まれる場合があるので、ログの提供時には、適切なセキュリティ対策を実施して情報漏洩のリスクを最小限に抑えること。これには、ログの暗号化、安全な送信手段の選択、アクセス制御の実施などを含むことが望ましい。

要求の文書化と記録:
データオーナー組織からの鍵の生成ログの提示要求に対する対応を適切に文書化し、記録を保持する。これには、要求内容、提供されたログの詳細、および対応日時などの情報が含まれることが望ましい。

適切なコミュニケーションとフィードバック:
データオーナー組織とのコミュニケーションを確保し、要求の適切な対応を行ったことを確認する。また、必要に応じて、提供されたログに関するフィードバックを収集し、適切な改善を行うことが望ましい。

D.6.鍵のライフサイクル管理
D.6.3.
データオーナー組織が鍵の廃棄を要求した際は、鍵を廃棄したのち、廃棄ログをデータオーナー組織に提示すること。

指針の解説
データオーナー組織が鍵の廃棄を要求した際は、鍵を廃棄したのち、廃棄ログをデータオーナー組織に提示することが望ましく、以下を考慮することが望ましい。

要求の受付と評価:
データオーナー組織から鍵の廃棄要求を受けた場合、すぐに受け付け、要求内容を評価すること。要求が妥当であるかどうかを確認し、必要な場合は追加情報を要求することが望まし

い。

適切な廃棄手順の実施:
鍵の廃棄要求が承認された場合、適切な廃棄手順を実施すること。これには、鍵の削除、破壊、またはその他の廃棄方法が含まれる。鍵を廃棄する際には、セキュリティリスクを最小限に抑えるために、適切な手順と標準に従うことが望ましい。

廃棄ログの作成:
鍵の廃棄が完了した後、廃棄ログを作成する。このログには、廃棄された鍵の識別情報、廃棄日時、および廃棄手順の詳細が含まれることが望ましい。

ログの提供:
廃棄ログが作成されたら、データオーナー組織に対してログを提示する。ログの提供は、安全で適切な方法で行われることが望ましい。

機密情報の保護:
廃棄ログには機密情報が含まれる場合があるので、ログの提供時には、適切なセキュリティ対策を実施して情報漏洩のリスクを最小限に抑えること。これには、ログの暗号化、安全な送信手段の選択、アクセス制御の実施などを含むことが望ましい。

要求の文書化と記録:
データオーナー組織からの鍵の廃棄要求に対する対応を適切に文書化し、記録を保持すること。これには、要求内容、提供されたログの詳細、および対応日時などの情報が含まれることが望ましい。

適切なコミュニケーションとフィードバック:
データオーナー組織とのコミュニケーションを確保し、要求の適切な対応を行ったことを確認する。また、必要に応じて、提供されたログに関するフィードバックを収集し、適切な改善を行うことが望ましい。

D.6.鍵のライフサイクル管理
D.6.4.
鍵情報の鍵管理システム外への持ち出しがある場合、鍵管理システム外で持ち出した鍵情報を使用して鍵が復元できないようにすること。

指針の解説

鍵情報の鍵管理システム外への持ち出しがある場合、鍵管理システム外で持ち出した鍵情報を使用して鍵が復元できないようにすることが望ましく、以下を考慮することが望ましい。

外部持ち出しの制限と管理:
鍵情報は原則として鍵管理システム内で保持されるべきだが、特定の状況下で外部に持ち出す必要がある場合には、事前に管理者より許可を受けることが必要である。外部持ち出しの許可は、適切な権限を持つ管理者が承認し、記録されることが望ましい。

外部持ち出しの目的と期間の明確化:
外部持ち出しの目的と持ち出しの期間を明確に定義すること。これには、外部での作業や特定のプロジェクトへの参加などの正当な理由が含まれることが望ましい。

持ち出し時のセキュリティ対策の実施:
鍵情報が外部に持ち出す際には、適切なセキュリティ対策が実施される必要がある。これには、鍵情報の暗号化、安全なデータ転送手段の利用、およびアクセス制御の実施が含まれることが望ましい。

鍵情報の一時的な利用の許可:
外部で持ち出した鍵情報が一時的に利用される場合には、その利用期間が終了した後、鍵情報が自動的に無効化されるようにする必要がある。これにより、鍵情報の不正利用や漏洩のリスクを最小限に抑えることが期待できる。

復元不能な鍵情報の確保:
外部で持ち出した鍵情報を使用して鍵を復元することができないようにするために、適切な技術的手段を実施すること。これには、鍵情報の一時的な変更や一度使用した鍵情報の自動的な無効化などが含まれることが望ましい。

監視とログの記録:
外部で持ち出された鍵情報の利用を監視し、必要な場合はログを記録する。これにより、鍵情報の不正利用や漏洩が発生した場合に迅速な対応が期待できる。

D.6.鍵のライフサイクル管理

D.6.5.

鍵情報の鍵管理システム外への持ち出しがある場合、鍵管理システムにて鍵を廃棄した後は、持ち出した鍵情報も廃棄し、鍵情報からの鍵の復元を禁止することをポリシーに明記すること。

指針の解説

鍵情報の鍵管理システム外への持ち出しがある場合、鍵管理システムにて鍵を廃棄した後は、持ち出した鍵情報も廃棄し、鍵情報からの鍵の復元を禁止することをポリシーに明記することが望ましく、以下を考慮することが望ましい。

外部持ち出しの制限と管理:

鍵情報は原則として鍵管理システム内で保持されるべきだが、外部への持ち出しは必要最小限に限定すること。外部持ち出しの許可は、適切な権限を持つ管理者が承認し、目的と期間が明確に定義されることが望ましい。

廃棄後の鍵情報の廃棄:

鍵管理システムにて鍵が廃棄された後、外部で持ち出した鍵情報も同様に廃棄されるべきである。これにより、外部に持ち出した鍵情報からの鍵の復元が禁止されることが期待される。

廃棄ポリシーの明記:

鍵管理システムのポリシードキュメントに、鍵情報の持ち出しに関するポリシーが明記されるべきである。具体的には、鍵管理システムにて鍵が廃棄された後は、持ち出した鍵情報も廃棄し、鍵情報からの鍵の復元を禁止するよう述べられることが望ましい。

セキュリティ意識の向上:

鍵管理システムの利用者や関係者に対して、外部持ち出しのリスクとポリシーの重要性について教育を行うことが重要である。セキュリティ意識の向上により、ポリシーの遵守が促進されることが望ましい。

監視と監査:

鍵情報の持ち出しと廃棄に関する活動は監視され、定期的な監査が実施されるべきである。これにより、ポリシーの遵守状況が確認され、必要に応じて改善措置が講じられることが望ましい。

D.6.鍵のライフサイクル管理

D.6.6.

鍵情報(鍵や鍵のメタデータ)を鍵管理システム外へ持ち出す場合、業界のベストプラクティスやガイドラインで定められた安全な方法で配送すること。

指針の解説

鍵情報(鍵や鍵のメタデータ)を鍵管理システム外へ持ち出す場合、業界のベストプラクティスやガイドラインで定められた安全な方法で配送することが望ましく、以下を考慮することが望ましい。

持ち出しの目的と許可:

鍵情報を持ち出す必要が生じた場合は、その目的を明確にし、適切な権限を持つ管理者からの許可を得ることが必要である。持ち出しの目的や期間を適切に文書化し、承認プロセスを確立することが望ましい。

業界のベストプラクティスやガイドラインの遵守:

鍵情報の持ち出しに関する業界のベストプラクティスやガイドラインを遵守すること。これには、業界団体や規制機関が提供するセキュリティに関するガイドラインやベストプラクティスを参照することが望ましい。

安全な配送方法の選択:

鍵情報を安全に配送するために、業界標準の安全な方法を選択する。これには、暗号化された通信チャネルの利用、安全なデータ転送プロトコルの使用、および信頼性の高い運送業者の利用が含まれることが望ましい。

データの暗号化:

鍵情報を外部へ持ち出す前に、必要に応じてデータを暗号化すること。これにより、データが不正アクセスから保護され、機密性が確保されることが期待される。

送信時のアクセス制御:

鍵情報を外部に送信する際には、送信先を厳密に制限し、送信された情報にアクセスできる人物を制限すること。これにより、情報漏洩や不正利用のリスクを最小限に抑えることが期待される。

送信時の監視とトレース:
鍵情報の送信プロセスを監視し、送信された情報が適切な受信者に届いたことを確認すること。また、送信時のログを記録し、トレース可能な情報を保持することが望ましい。

D.7.変更管理

D.7.1.

変更管理ルールと手順を定め、責任者及び開発及び保守の責任者が承認していること。

指針の解説

変更管理は、変更管理ルールと手順を定め、責任者及び開発及び保守の責任者が承認していることが望ましく、以下を考慮することが望ましい。

変更管理ルールの策定:
変更管理ルールは、変更の要求、承認、実装、監視、評価などの手順を包括的に定義すること。ルールは、組織のビジョン、目標、セキュリティポリシーに合わせて策定されることが望ましい。

変更管理手順の定義:
変更管理手順は、変更の要求から承認、実施、評価までの一連のステップを具体的に示すこと。手順には、誰が変更を要求するか、どのように承認が得られるか、実施方法やテスト手法、変更後の評価方法などが含まれることが望ましい。

責任者の任命:
変更管理ルールと手順における責任者は、明確に任命されること。責任者は、変更の要求や承認、実装、監視、評価などの各段階で責任を持つことが望ましい。

開発・保守責任者の承認:
変更管理ルールと手順は、開発および保守の責任者によって承認されること。承認された手順に基づいて変更が行われることで、変更の一貫性と安全性が確保されることが望ましい。

変更の文書化:
変更管理の各段階での重要な決定や活動は、適切に文書化されること。文書化には、変更要求書、承認書、実装手順書、テスト結果、評価報告書などが含まれることが望ましい。

監視と評価:
変更が実施された後も、定期的な監視と評価が行われること。変更の影響や成果を適切に評価し、必要に応じて手順やプロセスを改善することが望ましい。

D.7.変更管理
D.7.2.
変更管理要求が生じた場合、他システムの影響を考慮していること。

指針の解説
変更管理は、変更管理要求が生じた場合、他システムの影響を考慮していることが望ましく、以下を考慮することが望ましい。

変更要求の評価:
変更管理要求が発生した際には、まず他システムへの影響を評価すること。影響の範囲を正確に把握するために、関連する他システムやサービスを明確に特定することが望ましい。

影響範囲の分析:
変更が他システムに与える影響を詳細に分析すること。影響範囲には、データの整合性、システムの可用性、関連するプロセスやワークフローへの影響などが含まれることが望ましい。

関係者の連携:
変更管理プロセスに関連する他システムの所有者や関係者と綿密に連携すること。影響範囲や変更計画に関する情報を共有し、必要な合意や調整を行うことが望ましい。

変更計画の調整:
他システムへの影響を考慮して、変更計画を適切に調整すること。変更のタイミングや手順、テスト計画などが他システムと調和するように検討されることが望ましい。

変更の実施と監視:
変更が実施される際には、他システムへの影響を監視すること。変更の影響が予期せず拡大する可能性がある場合、迅速に対応策を講じることが望ましい。

リスク管理:
他システムへの影響を考慮して、変更に関連するリスクを適切に管理すること。リスクを最小限に抑えるための予防策や回避策を検討し、必要に応じて変更計画を修正することが望ましい。

D.7.変更管理
D.7.3.
緊急の変更要求は文書化され、変更管理手続にしたがっていること。

指針の解説
変更管理は、緊急の変更要求は文書化され、変更管理手続にしたがっていることが望ましく、以下を考慮することが望ましい。

文書化された要求:
緊急の変更要求が発生した場合、要求内容は適切に文書化されること。文書化には、変更の理由、範囲、影響、実施方法などが含まれることが望ましい。

変更管理手続に従う:
緊急の変更要求も、通常の変更と同様に変更管理手続に従うこと。変更管理手続には、要求の提出、評価、承認、実施、監視、評価などのステップが含まれることが望ましい。

優先順位の明確化:
緊急の変更要求の優先順位が明確に定義されること。優先順位は、変更の重要度や緊急性、影響度などを考慮して設定されることが望ましい。

速やかな対応:
緊急の変更要求は速やかに対応されること。変更管理手続の各段階で迅速な判断と行動が求められることが望ましい。

文書化の適正化:
緊急の変更要求が承認された後も、適切に文書化されること。実施された変更の詳細や結果、影響などが適切に記録され、トレーサビリティが確保されることが望ましい。

監視と評価:

緊急の変更が実施された後、変更の影響や成果が適切に監視され、評価されること。不適切な変更や影響の発生があれば、迅速に対処することが望ましい。

D.8. システムクロック

D.8.1.

時刻同期技術を用いてシステム内のシステムクロックの時間精度を確保する仕組みを用意すること。

指針の解説

システムクロックは、時刻同期技術を用いてシステム内のシステムクロックの時間精度を確保する仕組みを用意することが望ましく、以下を考慮することが望ましい。

時刻同期技術の選定:

システムクロックの時間精度を確保するために適切な時刻同期技術を選定すること。NTP（NetworkTimeProtocol)、PTP（PrecisionTimeProtocol）などの技術を使用することが望ましい。

時刻同期サーバの設置:

時刻同期技術を利用するための時刻同期サーバを適切な場所に設置すること。サーバは信頼性が高く、ネットワークへのアクセスが容易であることが望ましい。

クライアントの設定:

各システム内のクライアント（サーバ、ワークステーションなど）に対して、時刻同期サーバへの接続を設定すること。クライアントは定期的に時刻同期サーバから時刻情報を取得し、システムクロックを同期することが望ましい。

セキュリティ検討:

時刻同期技術のセキュリティに関する検討を行うこと。時刻同期通信の暗号化や認証の実施など、セキュリティ対策を講ずることが望ましい。

モニタリングとアラート:

時刻同期の状態をモニタリングし、異常が検知された場合には適切なアラートを発信すること。時刻同期の障害や遅延が早急に対処されることが望ましい。

定期的な評価と調整:
時刻同期の正確性と信頼性を保つために、定期的な評価と調整を行うこと。システムクロックと時刻同期サーバの間の時差を監視し、必要に応じて調整を行うことが望ましい。

D.8.システムクロック D.8.2. **時刻同期技術を用いてデータ保管システム内のシステムクロックの時間精度が維持されていること。** **上記を時刻同期設定やサンプリングしたログ等を確認できること。**

指針の解説
システムクロックは、時刻同期技術を用いてデータ保管システム内のシステムクロックの時間精度が維持されていること。これらを時刻同期設定やサンプリングしたログ等を確認できることが望ましく、以下を考慮することが望ましい。

時刻同期技術の選定:
データ保管システム内のシステムクロックの時間精度を確保するために適切な時刻同期技術を選定すること。NTP（NetworkTimeProtocol）、PTP（PrecisionTimeProtocol）などの信頼性の高い技術を選択することが望ましい。

時刻同期設定の構築:
時刻同期技術を利用するための適切な設定を行うこと。システム内のすべてのデータ保管システムが、時刻同期サーバに正しく接続されていることを確認することが望ましい。

ログの記録と監視:
時刻同期設定やシステムクロックの状態を監視するためのログを記録すること。ログには、時刻同期イベントやシステムクロックの変更履歴などが含まれることが望ましい。

定期的な確認と監査:
時刻同期設定やログを定期的に確認し、システムクロックの時間精度が維持されていることを確認すること。監査により、設定が適切に実施されているかどうかを確認することが望ましい。

アラートの設定:

時刻同期の異常や問題が検知された場合には、適切なアラートが発信されるように設定すること。アラートにより、問題が早急に検知され、対応が行われることが望ましい。

トラブルシューティング手順の準備:
時刻同期の問題が発生した場合に備えて、適切なトラブルシューティング手順を準備すること。手順には、問題の特定方法や解決策が含まれることが望ましい。

データ適正消去実行証明協議会
CSP 認証基準 WG メンバー

リーダー：税所　達朗（さくらインターネット㈱）［運営実行委員会委員長］
メンバー：吉川　大亮（キヤノン IT ソリューションズ株式会社）
：岡部　淳一（ISACA 東京支部　副会長　兼　理事）
：村上　輝暁（P マーク主任審査員/ISMS 審査員補）
：坂本　哲也（株式会社ウルトラエックス）
：沼田　理（デジタル・フォレンジック研究会）［技術顧問］
：大泰司　章（合同会社ＰＰＡＰ総研）
：井谷　寛（ネットアップ合同会社）
：神沢　剛史（ネットアップ合同会社）
オブザーバ：上原　哲太郎（立命館大学　情報理工学部　教授）
：神田　雅透（独立行政法人情報処理推進機構）

発行元：データ適正消去実行証明協議会　CSP 認証基準 WG メンバー
発行日：2024 年 12 月 17 日