8.3　媒体の取扱い

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

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

8.3.1.1　取外し可能な媒体の管理のために、再利用可能な媒体を組織から移動する場合に、その内容が以後不要であるならば、これを復元不能とする。

8.3.1.2　取外し可能な媒体の管理のために、必要かつ実際的な場合には、組織から移動する媒体について、認可を要求する。

8.3.1.3　取外し可能な媒体の管理のために、組織から移動する媒体について、監査証跡の維持のために記録を保管する。

8.3.1.4　取外し可能な媒体の管理のために、全ての媒体は、製造業者の仕様に従って、安全でセキュリティが保たれた環境に保管する。

8.3.1.5　取外し可能な媒体の管理のために、データの機密性又は完全性が重要な考慮事項である場合は、取外し可能な媒体上のデータを保護するために、暗号技術を用いる。

8.3.1.6　取外し可能な媒体の管理のために、保管されたデータがまだ必要な間に媒体が劣化するリスクを軽減するため、読み出せなくなる前にデータを新しい媒体に移動する。

8.3.1.7　取外し可能な媒体の管理のために、価値の高いデータは、一斉に損傷又は消失するリスクをより低減するために、複数の複製を別の媒体に保管する。

8.3.1.8　取外し可能な媒体の管理のために、データ消失の危険性を小さくするために、取外し可能な媒体の登録を含める。

8.3.1.9　取外し可能な媒体の管理のために、取外し可能な媒体のドライブは、その利用のための業務上の理由があるときにだけ有効とする。

8.3.1.10　取外し可能な媒体の管理のために、取外し可能な媒体を用いる必要がある場合、媒体への情報の転送を監視する。

8.3.1.11　取外し可能な媒体の管理のための手順及び認可のレベルは、文書化する。

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

8.3.2.1　認可されていない者に秘密情報が漏えいするリスクを最小化するために、媒体のセキュリティを保った処分のための正式な手順を確立する。

8.3.2.2　秘密情報を格納した媒体の、セキュリティを保った処分の手順は、その情報の取扱いに慎重を要する度合いに応じたものとする。

8.3.2.3　秘密情報を格納した媒体は、セキュリティを保って、保管し、処分する（例えば、焼却、シュレッダーの利用、組織内の他のアプリケーションでの媒体の再利用のためのデータ消去）。

8.3.2.4　セキュリティを保った処分を必要とする品目を特定するための手順を定める。

8.3.2.5　取扱いに慎重を要する媒体類を選び出すことが困難な場合には、セキュリティを保って全ての媒体を処分する。

8.3.2.6　媒体の収集並びに処分のサービスを提供する外部業者は、十分な管理策及び経験を持つ適切な契約相手を選択する。

8.3.2.7　監査証跡を維持するために、取扱いに慎重を要する品目の処分を記録する。

8.3.2.8　処分のために情報を含む媒体を集める場合、それらの情報が集積されることによる影響に配慮し、手順に含める。

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

8.3.3.1　輸送される情報を格納した媒体を保護するために、信頼できる輸送機関又は運送業者を用いる。

8.3.3.2　輸送される情報を格納した媒体を保護するために、認可された運送業者の一覧について、管理者の合意を得る。

8.3.3.3　輸送される情報を格納した媒体を保護するために、運送業者を確認する手順を導入する。

8.3.3.4　輸送される情報を格納した媒体を保護するために、輸送途中に生じるかもしれない物理的損傷から内容を保護（例えば、媒体の復旧効果を低減させる場合のある、熱、湿気又は電磁気にさらすといった環境要因からの保護）するために、こん（梱）包を十分な強度とし、また、製造業者の仕様にも従う。

8.3.3.5　輸送される情報を格納した媒体を保護するために、媒体の内容、適用された保護、並びに輸送の責任窓口への受渡時刻及び目的地での受取り時刻の記録を特定するログを保持する。

9　アクセス制御

9.1　アクセス制御に対する業務上の要求事項

目的：情報及び情報処理施設へのアクセスを制限するため

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

9.1.1.1　資産の管理責任者は、資産に対する利用者のそれぞれの役割に対して、適切なアクセス制御規則、アクセス権及び制限を、アクセスに伴う情報セキュリティリスクを反映した制御の詳細さ及び厳密さで、決定する。

9.1.1.2　アクセス制御は、論理的アクセス制御と物理的アクセス制御の両面を考慮して決定する。

9.1.1.3　利用者及びサービス提供者には、アクセス制御によって達成する業務上の要求事項を明確に規定して提供する。

9.1.1.4　アクセス制御方針に、業務用アプリケーションのセキュリティ要求事項を反映する。

9.1.1.5　アクセス制御方針には、情報の伝達及び認可に対する方針（例えば、知る必要性の原則、情報のセキュリティ水準、情報の分類）を含める。

9.1.1.6　アクセス制御方針は、システム及びネットワークにおける、アクセス権と情報分類の方針との整合性を考慮して定める。

9.1.1.7　アクセス制御方針には、データ又はサービスへのアクセスの制限に関連する法令及び契約上の義務を反映する。

9.1.1.8　アクセス制御方針に、利用可能な全ての種類の接続を認識する分散ネットワーク環境におけるアクセス権の管理を含める。

9.1.1.9　アクセス制御方針に、アクセス制御における役割の分離（例えば、アクセス要求、アクセス認可、アクセス管理）の方針を含める。

9.1.1.10　アクセス制御方針に、アクセス要求の正式な認可に対する要求事項を含める。

9.1.1.11　アクセス制御方針に、アクセス権の定期的なレビューに対する要求事項を含める。

9.1.1.12　アクセス制御方針に、アクセス権の削除の方針を含める。

9.1.1.13　アクセス制御方針に、利用者の識別情報及び秘密認証情報の利用及び管理に関する、全ての重要な事象の記録の保管を含める。

9.1.1.14　アクセス制御方針に、特権的アクセスを認められた役割を含める。

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

9.1.2.1　ネットワーク及びネットワークサービスの利用に関し、方針を設定する。

9.1.2.2　ネットワーク及びネットワークサービスの利用に関する方針は、アクセスが許されるネットワーク及びネットワークサービスを対象にする。

9.1.2.3　ネットワーク及びネットワークサービスの利用に関する方針は、誰がどのネットワーク及びネットワークサービスへのアクセスが許されるかを決めるための認可手順を対象にする。