8　資産の管理

8.1　資産に対する責任

目的：組織の資産を特定し、適切な保護の責任を定めるため

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

8.1.1.1　組織は、情報のライフサイクルに関連した資産を特定し、その重要度を文書化する。

8.1.1.2　情報のライフサイクルには、作成、処理、保管、送信、削除及び破棄を含める。

8.1.1.3　文書は、専用の目録又は既存の目録として維持する。

8.1.1.4　資産目録は、正確で、最新に保たれ、一貫性があり、他の目録と整合していることを確実にする仕組みを整備する。

8.1.1.5　特定された各資産について、管理責任者を割り当て、分類する。

8.1.2　目録の中で維持される資産は、管理する。

8.1.2.1　資産の管理責任を時機を失せずに割り当てることを確実にするためのプロセスにおいて、資産が生成された時点、又は資産が組織に移転された時点で、適格な者（資産のライフサイクルの管理責任を与えられた個人及び組織）に管理責任を割り当てる。

8.1.2.2　資産の管理責任者は、資産のライフサイクル全体にわたって、その資産を適切に管理することに責任を負う。

8.1.2.3　資産の管理責任者は、資産の目録を作成する仕組みを整備する。

8.1.2.4　資産の管理責任者は、資産を適切に分類及び保護する仕組みを整備する。

8.1.2.5　資産の管理責任者は、適用されるアクセス制御方針を考慮に入れて、重要な資産に対するアクセスの制限及び分類を定め、定期的にレビューする。

8.1.2.6　資産の管理責任者は、資産を消去又は破壊する場合に、適切に取り扱う仕組みを整備する。

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

8.1.3.1　組織の資産を利用する又はアクセスできる従業員及び外部の利用者に対し、組織における情報や情報処理施設に関連する資産あるいは資源に関する情報セキュリティ要求事項について、認識させる。

8.1.3.2　従業員及び外部の利用者は、どのような情報処理資源の利用に対しても、また、利用者自身の責任の下で行ったいかなる利用に対しても、責任をもつ。

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

8.1.4.1　雇用の終了時の手続は、前もって支給された物理的及び電子的な資産（組織が管理責任をもつもの又は組織に委託されたもの）の全ての返却を含める。

8.1.4.2　従業員及び外部の利用者が組織の設備を購入する場合、又は個人所有の設備を用いる場合には、手順に従って、全ての関連する情報を組織に返却し、設備からセキュリティを保って確実に消去する。

8.1.4.3　従業員及び外部の利用者が継続中の作業に重要な知識を保有している場合には、その情報を文書化し、組織に引き継ぐ。

8.1.4.4　雇用の終了の予告期間中は、雇用が終了する従業員及び契約相手が認可を得ずに関連情報（例えば、知的財産）を複製することのないよう、組織が管理する。

8.2　情報分類

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

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

8.2.1.1　情報の分類及び関連する保護管理策には、情報を共有又は制限する業務上の要求、及び法的要求事項を含める。

8.2.1.2　情報資産の管理責任者は、その情報の分類に対して責任を負う。

8.2.1.3　分類体系には、分類の規則及びその分類を時間が経ってからレビューするための基準を含める。

8.2.1.4　分類体系における保護レベルは、対象とする情報についての機密性、完全性、可用性及びその他の特性を分析することによって評価する。

8.2.1.5　分類体系は、アクセス制御方針と整合させる。

8.2.1.6　それぞれのレベルには、分類体系の適用において意味をなすような名称を付ける。

8.2.1.7　分類体系は、組織全体にわたって一貫させ、全員が情報及び関連する資産を同じ方法で分類し、保護に関する要求事項について共通した理解をもち、適切な保護を適用できるようにする。

8.2.1.8　分類は、組織のプロセスに含め、組織全体にわたって一貫した論理的なものとする。

8.2.1.9　分類の結果は、組織にとっての取扱いに慎重を要する度合い及び重要性（例えば、機密性、完全性、可用性）に応じた資産の価値を含める。

8.2.1.10　分類の結果は、ライフサイクルを通じた、情報の価値、取扱いに慎重を要する度合い及び重要性の変化に応じて、更新する。

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

8.2.2.1　情報のラベル付けに関する手順は、物理的形式及び電子的形式の情報及び関連する資産に適用できるようにする。

8.2.2.2　ラベル付けは、8.2.1で確立した分類体系を反映する。

8.2.2.3　ラベルは、容易に認識できるようにする。

8.2.2.4　情報のラベル付けに関する手順では、媒体の種類に応じて、情報がどのようにアクセスされるか又は資産がどのように取り扱われるかを考慮して、ラベルを添付する場所及びその添付方法に関する手引を示す。

8.2.2.5　従業員及び契約相手に、ラベル付けに関する手順を認識させる。

8.2.2.6　取扱いに慎重を要する又は重要と分類される情報を含むシステム出力には、適切な分類ラベルを付ける。

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

8.2.3.1　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順を作成する。

8.2.3.2　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、各レベルの分類に応じた保護の要求事項に対応するアクセス制限に関する手順を含める。

8.2.3.3　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、資産の認可された受領者について、正式な記録を維持するための手順を含める。

8.2.3.4　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、情報の一時的又は恒久的な複製は、情報の原本と同等のレベルで保護するための手順を含める。

8.2.3.5　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、ＩＴ資産は、製造業者の仕様に従って保管するための手順を含める。

8.2.3.6　情報を分類に従って取り扱い、処理し、保管し、伝達するための手順には、媒体の全ての複製には、認可された受領者の注意をひくように明確な印を付けるための手順を含める。

8.2.3.7　他組織との情報共有を含む合意には、その情報の分類を特定し、他組織からの分類ラベルを解釈するための手順を含める。