5b　資産管理

5b-5.9　情報及びその他の関連資産の目録

管理策：情報及びその他の関連資産の目録を、それぞれの管理責任者を含めて作成し、維持する。

目的：　組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。

詳細管理策

【目録】

5b-5.9.1　組織は、情報及びその他の関連資産を特定し、情報セキュリティの観点からそれらの重要度を決定する。

5b-5.9.2　文書は、必要に応じて専用の目録又は既存の目録として維持する。

5b-5.9.3　情報及びその他の関連資産は、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。情報及びその他の関連資産の目録の正確性を確実にするための選択肢は次のものを含む。

a）資産目録に照らして、特定した情報及びその他の関連資産の定期的なレビューを実施する。

b）資産の設置、変更又は除去のプロセスにおいて目録の更新を自動的に適用する。

5b-5.9.4　資産の場所を、必要に応じて目録に含める。

（5b-5.9参考）　目録は、情報及びその他の関連資産の単一のリストである必要はない。目録は組織において関係する機能が維持することが望ましいことを考えると、情報資産、ハードウェア、ソフトウェア、仮想マシン（ＶＭ）、施設、要員、力量、機能及び記録に関する目録などの、動的な目録の集まりとみることが可能である。

5b-5.9.5　各資産は、それに関係する情報の分類に従って分類する。

5b-5.9.6　情報及びその他の関連資産の目録の粒度は、組織のニーズに適したレベルである。

（5b-5.9.6参考）　資産の性質上、情報のライフサイクルにおいて資産の特定のインスタンスが文書化できない場合がある。短期間だけ存続する資産の例として、ライフサイクルが短いＶＭインスタンスがある。

【管理責任】

5b-5.9.7　特定した情報及びその他の関連資産について、各々の資産の管理責任を個人又はグループに割り当て、その上で分類を特定する。

5b-5.9.8　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を実施する。

5b-5.9.9　資産を生成した時点、又は資産を組織に移転した時点で、管理責任を割り当てる。

5b-5.9.10　現在の資産の管理責任者が職務を離れる又は変わる場合は、必要に応じて資産の管理責任を再割り当てする。

【管理責任者の義務】

5b-5.9.11　資産の管理責任者は、次の事項を確実にして、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。

a）情報及びその他の関連資産の目録を作成する。

b）情報及びその他の関連資産を適切に分類し、保護する。

c）分類を定期的にレビューする。

d）データベース、ストレージ、ソフトウェアの構成要素、サブ構成要素など、技術資産の構成要素を一覧表示し、ひも（紐）付ける。

e）情報及びその他の関連資産の許容される利用に関する要求事項を確立する。

f）アクセス制限が分類に対応し、有効であり、これを定期的にレビューする。

g）情報及びその他の関連資産は、削除又は破棄する場合、セキュリティに配慮した方法で処理し、目録から削除する。

h）資産の管理責任者が、資産に関連するリスクの特定及びマネジメントに関与する。

i）資産の管理責任者が、情報を管理する役割及び責任をもつ要員を支援する。

5b-5.10　情報及びその他の関連資産の許容される利用

管理策：情報及びその他の関連資産の許容される利用に関する規則及び取扱手順は、明確にし、文書化し、実施する。

目的：　情報及びその他の関連資産を適切に保護し、利用し、取り扱うことを確実にするため。

詳細管理策

5b-5.10.1　組織の情報及びその他の関連資産を利用する、又はそれらにアクセスする要員及び外部の利用者に対し、情報及びその他の関連資産を保護し、取り扱うための情報セキュリティ要求事項を認識させる。

5b-5.10.2　要員及び外部の利用者は、どのような情報処理施設・設備の利用に対しても、責任をもつ。

5b-5.10.3　組織は、情報及びその他の関連資産の許容される利用に関するトピック固有の方針を確立し、情報及びその他の関連資産を利用する又は取り扱う全ての人にそれを伝達する。

5b-5.10.4　許容される利用に関するトピック固有の方針では、個人に期待する情報及びその他の関連資産の利用方法について、明確に指示をする。

5b-5.10.5　トピック固有の方針には、次の事項を記載する。

a）情報セキュリティの観点から見た、個人に期待する行動及び許容できない行動

b）情報及びその他の関連資産について許可する利用及び禁止する利用

c）組織が実行している監視活動

5b-5.10.6　許容される利用の手順は、情報の分類及び特定したリスクに従って、情報のライフサイクル全体にわたって立案する。

5b-5.10.7　許容される利用の手順の立案においては、次の項目を考慮する。

a）分類のレベルに応じた保護の要求事項に対応するアクセス制限

b）情報及びその他の関連資産の認可された利用者についての、記録の維持

c）情報の一時的又は恒久的な複製についての、情報の原本の保護と整合性のあるレベルでの保護

d）情報に関連する資産の、製造業者の仕様に従った保管

e）記憶媒体（電子的又は物理的な）の全ての複製についての、認可された受領者の注意をひくような明確な表示

f）情報及びその他の関連資産の破棄、並びにサポートされている削除方法の認可