6a-6.4　懲戒手続

管理策：情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために、懲戒手続を正式に定め、伝達する。

目的：　要員及びその他の関連する利害関係者が情報セキュリティ方針違反の結果を理解すること、違反を抑止すること、及びそれを犯した要員及びその他の関連する利害関係者を適切に扱うことを確実にするため。

詳細管理策

6a-6.4.1　懲戒手続は、情報セキュリティ方針違反が生じたことの事前の確認を待って開始する。

6a-6.4.2　正式な懲戒手続は、次のような要素を考慮した段階別の対応を定める。

ａ）違反の内容（誰が、何を、いつ、どのように）及び重大さ、並びにその結果

ｂ）違反が意図的である（悪意がある）か、又は意図的でない(偶発的）か。

ｃ）最初の違反か又は繰り返されたものか。

ｄ）違反者は、適切に教育・訓練されていたかどうか。

6a-6.4.3　懲戒手続の対応は、関連する法令、規制、契約及び事業上の要求事項、並びに必要に応じてその他の要素を考慮に入れる。

6a-6.4.4　懲戒手続を、要員及びその他の関連する利害関係者が情報セキュリティ方針、トピック固有の方針、及び情報セキュリティの手順に違反することを防ぐための抑止力として使う。

（6a-6.4.4参考）　意図的な情報セキュリティ方針への違反には、直ちに処置をとることが求められる場合がある。

6a-6.5　雇用の終了又は変更後の責任

管理策：雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、施行し、関連する要員及びその他の利害関係者に伝達する。

目的：　雇用又は契約を変更又は終了する手続の一部として、組織の利益を保護するため。

詳細管理策

6a-6.5.1　雇用の終了又は変更を管理する手続では、終了又は変更後にどの情報セキュリティの責任及び義務を引き続き有効とすることが望ましいかを定める。

6a-6.5.2　雇用の終了又は変更後の情報セキュリティの責任及び義務に、情報の秘密保持、知的財産及び取得したその他の知識、並びにその他の秘密保持契約に含まれる責任を含める。

6a-6.5.3　雇用又は契約の終了後も引き続き有効な責任及び義務は、その個人の雇用条件、契約又は合意に含める。

（6a-6.5.3参考）　個人の雇用の終了後、定められた期間継続するその他の契約又は合意も、情報セキュリティの責任を含む場合がある。

6a-6.5.4　責任又は雇用の変更は、現在の責任又は雇用の終了と新しい責任又は雇用の開始との組合せとして管理する。

6a-6.5.5　職務を去る又は職務が変わる個人がもつ情報セキュリティの役割及び責任を特定し、別の個人に移す。

6a-6.5.6　変更及び運用の手順を要員、その他の利害関係者及び関連する連絡先担当者に伝達するための手続を確立する。

6a-6.5.7　雇用の終了又は変更の手続は、供給者の要員、供給者との契約若しくは組織との仕事の終了が生じる場合、又は組織内で仕事の変更がある場合に、外部の要員（すなわち、供給者）にも適用する。

6a-6.6　秘密保持契約又は守秘義務契約

管理策：情報保護に対する組織のニーズを反映する秘密保持契約又は守秘義務契約は、特定し、文書化し、定常的にレビューし、要員及びその他の関連する利害関係者が署名する。

目的：　要員又は外部の関係者がアクセスできる情報の秘密保持のため。

詳細管理策

6a-6.6.1　秘密保持契約又は守秘義務契約には、法的に強制できる表現を用いて、秘密情報を保護するための要求事項を取り上げる。

6a-6.6.2　秘密保持契約又は守秘義務契約は、利害関係者及び組織の要員との間で締結される。

6a-6.6.3　組織の情報セキュリティ要求事項に基づいて、契約の条件は、取り扱われる情報の種類、その分類レベル、その使用及び当事者に許可されるアクセスを考慮して決定する。

6a-6.6.4　秘密保持契約又は守秘義務契約に対する要求事項を特定するために、次の要素を考慮する。

ａ）保護する情報の定義

ｂ）秘密を無期限に又は情報が一般公開されるまで保持する必要がある場合も含めた、契約の有効期間

ｃ）契約終了時に要求する処置

ｄ）認可されていない情報開示を避けるための、署名者の責任及び行為

ｅ）情報、企業秘密及び知的財産の帰属、並びにこれらと秘密情報の保護との関係

ｆ）秘密情報の許可された利用範囲、及び情報を利用する署名者の権利

ｇ）高度に取扱いに慎重を要する状況における、秘密情報に関わる行為の監査及び監視の権利

ｈ）認可されていない開示又は秘密情報漏えいの、通知及び報告のプロセス

ｉ）契約終了時における情報の返却又は破棄に関する条件

ｊ）契約の不順守が発生した場合に講じるべき処置

6a-6.6.5　組織は、適用される法域における秘密保持契約又は守秘義務契約の順守を考慮に入れる。

6a-6.6.6　秘密保持契約又は守秘義務契約に関する要求事項は、定期的に及びこれら要求に影響する変化が発生した場合に、レビューする。

6a-6.7　リモートワーク

管理策：組織の構外でアクセス、処理又は保存される情報を保護するために、要員が遠隔で作業をする場合のセキュリティ対策を実施する。

目的：　要員が遠隔で作業をする場合の情報セキュリティを確実にするため。

詳細管理策

（6a-6.7参考）　リモートワークは、組織の構外から組織の要員が作業し、ハードコピーで又はＩＣＴ機器を通じて電子的に情報にアクセスするときに常に行われる。リモートワーク環境は、“テレワーキング”、“コンピュータ端末を用いた在宅勤務（telecommuting)”、“柔軟な作業場（flexible workplace)”、“仮想的な作業環境”、及び“遠隔保守”と呼ばれる環境を含んでいる。