5e-5.25　情報セキュリティ事象の評価及び決定

管理策：組織は情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定する。

目的：　情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため。

詳細管理策

5e-5.25.1　インシデントの結果及び優先順位を特定するために、情報セキュリティインシデントの分類及び優先順位付けの体系について合意する。

5e-5.25.2　体系には、事象を情報セキュリティインシデントに分類する基準を含める。

5e-5.25.3　連絡の窓口は、合意した体系を使用して、各情報セキュリティ事象を評価する。

5e-5.25.4　情報セキュリティインシデントの調整及び対応に責任を負う要員は、評価を実行し、情報セキュリティ事象に関する決定をする。

5e-5.25.5　評価及び決定の結果は、以後の参照及び検証のために詳細に記録しておく。

5e-5.26　情報セキュリティインシデントへの対応

管理策：情報セキュリティインシデントは、文書化した手順に従って対応する。

目的：　情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため。

詳細管理策

5e-5.26.1　組織は、情報セキュリティインシデント対応に関する手順を確立し、それを全ての関連する利害関係者に伝達する。

5e-5.26.2　情報セキュリティインシデントには、必要な力量をもつ指定されたチームが対応する。

5e-5.26.3　情報セキュリティインシデントへの対応策には、次の事項を含める。

a）インシデントの結果が拡がる可能性がある場合は、インシデントの影響を受けるシステムを含める。

b）情報セキュリティインシデントの発生後、できるだけ速やかに証拠を収集する。

c）必要に応じて、危機管理活動及び場合によっては事業継続計画の発動を含むエスカレーションを行う。

d）後で行う分析のために、関連する全ての対応活動を適正に記録することを確実にする。

e）知る必要性の原則に従って全ての関連する内部及び外部の利害関係者に対し、情報セキュリティインシデントの存在又は関連するその詳細を伝達する。

f）対応の有効性を改善し、他の組織への影響を最小限にする助けとするために、関係当局、外部の利益団体及び会議、供給者、顧客などの内部及び外部の関係者と調整する。

g）インシデントへの対処が滞りなく済んだ後、正式にそれを終了し、記録する。

h）必要に応じて、情報セキュリティのフォレンジック分析を実施する。

i）根本原因を特定するために、インシデント後の分析を実施する。それが定められた手順に従って文書化され、伝達されることを確実にする。

j）インシデントを引き起こし、インシデントの一因となり、又はインシデントの防止に失敗した管理策に関連するものを含む、情報セキュリティのぜい弱性及び弱点を特定し、管理する。

5e-5.27　情報セキュリティインシデントからの学習

管理策：情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いる。

目的：　将来のインシデントの起こりやすさ又は影響を減らすため。

詳細管理策

5e-5.27.1　組織は情報セキュリティインシデントの形態、規模及び費用を定量化し、監視するための手順を確立する。

5e-5.27.2　情報セキュリティインシデントの評価から得た情報は、次の目的で使用する。

a）インシデントのシナリオ及び手順を含むインシデント管理計画を強化する。

b）組織の情報セキュリティリスクアセスメントを更新し、将来の同様のインシデントの起こりやすさ又は影響を減らすために必要な追加の管理策を決定し、実施するために、再発する又は重大なインシデント及びそれらの原因を特定する。これを可能にする仕組みには、インシデントの形態、規模及び費用に関する情報の収集、定量化及び監視を含む。

c）発生し得るインシデントの事例、こうしたインシデントへの対応方法の事例、及び以後これらを回避するための方法の事例を示すことによって、利用者の意識向上及び訓練を強化する。

5e-5.28　証拠の収集

管理策：組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施する。

目的：　懲戒処置及び法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため。

詳細管理策

5e-5.28.1　懲戒処置及び法的処置のために情報セキュリティ事象に関連する証拠を取り扱う場合は、内部の手順を定めてそれに従う。

5e-5.28.2　法的処置のために情報セキュリティ事象に関連して取り扱われる証拠は、関連する法域において受容される可能性を最大にするために、異なる幾つかの法域の要求事項を考慮する。

5e-5.28.3　情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための証拠の管理に関する手順では、各種の記憶媒体、装置・機器及び装置・機器の状態（すなわち、電源が入っているか、切れているか）に従って、証拠の特定、収集、取得及び保存の指示を規定する。

5e-5.28.4　証拠は原則として、適切な国内法廷又は別の懲戒会議において受容される方法で収集し、次の事項を示す。

a）記録は完全で、いかなる方法でも改ざんされていない。

b）電子証拠の複製は原本と同一であることが推定される。

c）証拠の収集元である情報システムは、証拠を記録した時点で正しく機能していた。