16.1.2　情報セキュリティ事象は、適切な管理者への連絡経路を通して、できるだけ速やかに報告する。
16.1.2.1　全ての従業員及び契約相手に、情報セキュリティ事象をできるだけ速やかに報告する責任のあることを認識させる。
16.1.2.2　全ての従業員及び契約相手に、情報セキュリティ事象の報告手順及び情報セキュリティ事象を報告する連絡先を認識させる。
16.1.2.3　情報セキュリティ事象の報告には、効果のないセキュリティ管理策を含める。
16.1.2.4　情報セキュリティ事象の報告には、情報の完全性、機密性又は可用性に関する期待に対する違反を含める。
16.1.2.5　情報セキュリティ事象の報告には、人による誤りを含める。
16.1.2.6　情報セキュリティ事象の報告には、個別方針又は指針の不順守を含める。
16.1.2.7　情報セキュリティ事象の報告には、物理的セキュリティの取決めに対する違反を含める。
16.1.2.8　情報セキュリティ事象の報告には、管理されていないシステム変更を含める。
16.1.2.9　情報セキュリティ事象の報告には、ソフトウェア又はハードウェアの誤動作を含める。
16.1.2.10　情報セキュリティ事象の報告には、アクセス違反を含める。
16.1.3　組織の情報システム及びサービスを利用する従業員及び契約相手に、システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は、どのようなものでも記録し、報告するように要求する。
16.1.3.1　全ての従業員及び契約相手は、情報セキュリティインシデントを防止するため、情報セキュリティ弱点をできるだけ速やかに連絡先に報告する。
16.1.3.2　情報セキュリティ弱点の報告の仕組みは、できるだけ簡単で使いやすく、いつでも利用できるようにする。
16.1.4　情報セキュリティ事象は、これを評価し、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。
16.1.4.1　連絡先の者は、合意された情報セキュリティ事象・情報セキュリティインシデントの分類基準を用いて各情報セキュリティ事象を評価し、その事象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。
16.1.4.2　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する。
16.1.5　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。
16.1.5.1　情報セキュリティインシデントには、指定された連絡先、及び組織又は外部関係者の他の関係する要員が対応する。
16.1.5.2　対応策には、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ことを含める。
16.1.5.3　対応策には、必要に応じて、情報セキュリティの法的分析を実施することを含める。
16.1.5.4　対応策には、必要に応じて、段階的取扱い（escalation）を行うことを含める。
16.1.5.5　対応策には、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ことを含める。
16.1.5.6　対応策には、知る必要性を認められている内部・外部の他の要員又は組織に対し、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ことを含める。
16.1.5.7　対応策には、インシデントの原因又はインシデントの一因であることが判明した情報セキュリティ弱点に対処することを含める。
16.1.5.8　対応策には、インシデントへの対応が滞りなく済んだ後、正式にそれを終了し、記録することを含める。
16.1.5.9　インシデントの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。
16.1.6　情報セキュリティインシデントの分析及び解決から得られた知識は、インシデントが将来起こる可能性又はその影響を低減するために用いる。
16.1.6.1　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及び監視できるようにする仕組みを備える。
16.1.6.2　情報セキュリティインシデントの評価から得た情報は、再発する又は影響の大きいインシデントを特定するために利用する。
16.1.7　組織は、証拠となり得る情報の特定、収集、取得及び保存のための手順を定め、適用する。
16.1.7.1　懲戒処置及び法的処置のために証拠を取り扱う場合は、内部の手順を定め、それに従う。
16.1.7.2　懲戒処置及び法的処置のために証拠を取り扱う手順では、各種の媒体、装置及び装置の状態（例えば、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、取得及び保存のプロセスを規定する。
16.1.7.3　懲戒処置及び法的処置のために証拠を取り扱う手順では、管理状況の一連の履歴を取得するプロセスを規定する。
16.1.7.4　懲戒処置及び法的処置のために証拠を取り扱う手順では、証拠の保全を行うプロセスを規定する。
16.1.7.5　懲戒処置及び法的処置のために証拠を取り扱う手順では、要員の安全を確保するプロセスを規定する。
16.1.7.6　懲戒処置及び法的処置のために証拠を取り扱う手順では、関与する要員の役割及び責任を定める。
16.1.7.7　懲戒処置及び法的処置のために証拠を取り扱う手順では、要員の力量を定める。
16.1.7.8　懲戒処置及び法的処置のために証拠を取り扱う手順では、文書化することを定める。
16.1.7.9　懲戒処置及び法的処置のために証拠を取り扱う手順では、要点説明を行うことを定める。
16.1.7.10　保存された証拠の価値を強化するために、要員及びツールの適格性を示す証明書又はその他適切な手段を追及する。
16.1.7.11　懲戒処置及び法的処置に必要な法的証拠が、組織の枠又は法域を越える場合、組織は必要とされる情報を法的証拠として収集することが法的に認められていることを確認する。
16.1.7.12　懲戒処置及び法的処置に関連する幾つかの法域にまたがる証拠の利用の可能性を最大にするために、それらの異なる法域の要求事項を確認する。

17　事業継続マネジメントにおける情報セキュリティの側面
17.1　情報セキュリティ継続
目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むため
17.1.1　組織は、困難な状況（adverse situation）（例えば、危機又は災害）における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定する。
17.1.1.1　組織は、情報セキュリティの継続が事業継続マネジメント（以下「ＢＣＭ」という。）プロセス又は災害復旧管理（以下「ＤＲＭ」という。）プロセスに織り込まれているか否かを判断する。
17.1.1.2　組織は、事業継続及び災害復旧に関する計画を立てる場合に、情報セキュリティ要求事項を定める。
17.1.1.3　事業継続及び災害復旧に関する正式な計画が策定されていない場合に、通常の業務状況とは異なる困難な状況においても、情報セキュリティ要求事項は変わらず存続するよう定める。