6a-6.7.1　リモートワーク活動を許可する組織は、関連する条件及び制限を定めたリモートワークに関するトピック固有の方針を発行する。

6a-6.7.2　適用可能な場合には、リモートワークに関するトピック固有の方針として、次の事項を考慮する。

a）要員が配置されている法域を含め、リモートワークの場所及び周辺環境の物理的セキュリティを考慮に入れた、リモートワークの場所における既存の又は新たに提案する物理的セキュリティ

b）施錠可能なファイリングキャビネット、場所間におけるセキュリティを保つべき移送、並びにリモートアクセス、クリアデスク、情報及びその他の関連資産の印刷及び廃棄、情報セキュリティ事象の報告に関する規則など、遠隔物理環境のための規則及びセキュリティの仕組み

c）期待される物理的なリモートワーク環境

d）次を考慮した、通信のセキュリティに関する要求事項
- ―組織のシステムへのリモートアクセスの必要性
- ―通信回線からアクセスし、通信回線を通過する情報の取扱いに慎重を要する度合い
- ―システム及びアプリケーションの取扱いに慎重を要する度合い

e）個人所有の機器での情報の処理及び保管を支援する、仮想デスクトップアクセスなどリモートアクセスの使用

f）リモートワークの場所における、他者による情報又は資源への認可されていないアクセスの脅威

g）公共の場所における、他者による情報又は資源への認可されていないアクセスの脅威

h）家庭のネットワーク及び公衆ネットワークの使用並びに無線ネットワークサービスの設定に関する要求事項又は制限

i）ファイアウォール及びマルウェアからの保護などのセキュリティ対策の使用

j）システムを遠隔で展開し、初期化するためのセキュリティに配慮した仕組み

k）組織のネットワークへのリモートアクセスを許可する場合に、単一要素認証の仕組みのぜい弱性を考慮に入れた、認証及びアクセス権限有効化のためのセキュリティに配慮した仕組み

6a-6.7.3　リモートワークに関し、考慮すべき指針及び対策には、次の事項を含む。

a）組織の管理下にない個人所有の機器の使用を許さない場合には、リモートワーク活動のための適切な機器及び保管用具の提供

b）許可した作業、保持することができる情報の分類、並びにリモートワークを行う者にアクセスを認可する内部システム及びサービスの定義

c）遠隔で作業する者及び支援を提供する者のための訓練の提供。これは、遠隔で作業しつつセキュリティに配慮した方法で業務を行う方法を含む。

d）機器画面のロック及び非アクティブ状態タイマー、機器の位置追跡の有効化、遠隔データ消去機能のインストールに関する要求事項など、セキュリティに配慮したリモートアクセス方法を含む、適切な通信機器の提供

e）物理的セキュリティ

f）家族及び訪問者による機器及び情報へのアクセスに関する規則及び手引

g）ハードウェア及びソフトウェアのサポート及び保守の提供

h）保険の提供

i）バックアップ及び事業継続のための手順

j）監査及びセキュリティの監視

k）リモートワークが終了したときの、権限及びアクセス権の失効並びに機器の返却

6a-6.8　情報セキュリティ事象の報告

管理策：組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設ける。

目的：　要員が特定する可能性がある情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。

詳細管理策

6a-6.8.1　情報セキュリティインシデントの影響を防止又は最小化するために、全ての要員及び利用者に、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ておく。

6a-6.8.2　全ての要員及び利用者に、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。

6a-6.8.3　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ものとする。

6a-6.8.4　情報セキュリティ事象には、インシデント、違反及びぜい弱性を含める。

6a-6.8.5　情報セキュリティ事象の報告を検討する状況には、次を含める。

a）効果のない情報セキュリティ管理策

b）情報の機密性、完全性又は可用性に関する期待に対する違反

c）ヒューマンエラー

d）情報セキュリティ方針、トピック固有の方針又は適用される標準の不順守

e）物理的セキュリティ対策に対する違反

f）変更管理プロセスを経ないシステム変更

g）ソフトウェア若しくはハードウェアの誤動作又はその他の異常なシステム挙動

h）アクセス違反

i）ぜい弱性

j）マルウェア感染の疑い