6.2.2.11　テレワーキングを行う場合の条件及び制限は、適切と考えられ、かつ適法な場合には、マルウェアに対する保護及びファイアウォールの要件を考慮して定める。
6.2.2.12　テレワーキングを行う場合に考慮すべき指針及び取決めには、組織の管理下にない個人所有の装置の使用を許さない場合には、テレワーキング活動のための適切な装置及び保管用具の用意に関する事項を含める。
6.2.2.13　テレワーキングを行う場合に考慮すべき指針及び取決めには、許可した作業、作業時間、保持してもよい情報の分類、並びにテレワーキング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に関する事項を含める。
6.2.2.14　テレワーキングを行う場合に考慮すべき指針及び取決めには、安全な遠隔アクセス方法を含め、適切な通信装置の用意に関する事項を含める。
6.2.2.15　テレワーキングを行う場合に考慮すべき指針及び取決めには、物理的セキュリティに関する事項を含める。
6.2.2.16　テレワーキングを行う場合に考慮すべき指針及び取決めには、家族及び訪問者による装置及び情報へのアクセスに関する規則及び手引を含める。
6.2.2.17　テレワーキングを行う場合に考慮すべき指針及び取決めには、ハードウェア及びソフトウェアのサポート及び保守の用意を含める。
6.2.2.18　テレワーキングを行う場合に考慮すべき指針及び取決めには、保険の用意を含める。
6.2.2.19　テレワーキングを行う場合に考慮すべき指針及び取決めには、バックアップ及び事業継続のための手順を含める。
6.2.2.20　テレワーキングを行う場合に考慮すべき指針及び取決めには、監査及びセキュリティの監視に関する事項を含める。
6.2.2.21　テレワーキングを行う場合に考慮すべき指針及び取決めには、テレワーキングが終了したときの、権限及びアクセス権の失効並びに装置の返却に関する事項を含める。

7　人的資源のセキュリティ

7.1　雇用前

目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため

7.1.1　全ての従業員候補者についての経歴などの確認は、関連する法令、規制及び倫理に従って行う。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行う。
7.1.1.1　関連があるプライバシー、ＰＩＩの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、満足のいく推薦状（例えば、業務についてのもの、人物についてのもの）の入手の可否の確認を行う。
7.1.1.2　関連があるプライバシー、ＰＩＩの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、応募者の履歴書の確認（完全であるか及び正確であるかの確認）を行う。
7.1.1.3　関連があるプライバシー、ＰＩＩの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、提示された学術上及び職業上の資格の確認を行う。
7.1.1.4　関連があるプライバシー、ＰＩＩの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、公的証明書（パスポート又は同種の文書）の確認を行う。
7.1.1.5　関連があるプライバシー、ＰＩＩの保護及び雇用に関する法令の全てを考慮に入れ、許される場合には、信用情報又は犯罪記録のレビューのような、より詳細な確認を行う。
7.1.1.6　情報セキュリティに関する特定の役割のために雇用する場合、組織は、候補者が、情報セキュリティに関するその役割を果たすために必要な力量を備えていることを確認する。
7.1.1.7　情報セキュリティに関する特定の役割のために雇用する場合、組織は、特に、その役割が組織にとって重要なものである場合は、候補者が、その役割を任せられる信頼できる人物であることを確認する。
7.1.1.8　最初の発令で就く業務であるか、昇進して就く業務であるかにかかわらず、情報処理施設にアクセスすることがその担当者にとって必要になる場合、特にそれらの設備が秘密情報（例えば、財務情報、極秘情報）を扱っているときには、組織は、より詳細な確認も検討する。
7.1.1.9　手順には、確認のためのレビューの基準及び制約を定める（例えば、誰が選考するのか。また、この確認のためのレビューは、いつ、どのように、なぜ行うのか。）。
7.1.1.10　選考プロセスは、契約相手に対しても確実に実施する。
7.1.1.11　契約相手に対して選考プロセスを実施する場合、組織と契約相手との間の合意では、選考の実施に関する責任、及びその選考が完了していないとき又はその結果に疑念若しくは懸念があるときに従う必要がある告知手順を定める。
7.1.1.12　組織内である職位に付けることを検討している全ての候補者についての情報は、当該法域での適切な法令に従って収集し、扱う。
7.1.1.13　適用される法令によっては、選考活動について候補者へ、事前に通知する。

7.1.2　従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載する。
7.1.2.1　従業員又は契約相手の契約上の義務には、組織の情報セキュリティのための方針群を反映する。
7.1.2.2　従業員又は契約相手の契約には、秘密情報へのアクセスが与えられる全ての従業員及び契約相手による、情報処理施設へのアクセスが与えられる前の、秘密保持契約書又は守秘義務契約書への署名を行う。
7.1.2.3　従業員又は契約相手の契約には、従業員又は契約相手の法的な責任及び権利（例えば、著作権法、データ保護に関連して制定された法律に関するもの）を明確にする。
7.1.2.4　従業員又は契約相手の契約には、従業員又は契約相手によって扱われる情報の分類に関する責任、並びに従業員又は契約相手によって扱われる組織の情報、情報に関連するその他の資産、情報処理施設及び情報サービスの管理に関する責任を明確にする。
7.1.2.5　従業員又は契約相手の契約には、他社又は外部関係者から受け取った情報の扱いに関する従業員又は契約相手の責任を明確にする。
7.1.2.6　従業員又は契約相手の契約には、従業員又は契約相手が組織のセキュリティ要求事項に従わない場合にとる処置を含める。
7.1.2.7　情報セキュリティに関する役割及び責任は、雇用前のプロセスにおいて候補者に伝える。
7.1.2.8　組織は、従業員及び契約相手が情報セキュリティに関する雇用条件に同意することを確実にする仕組みを整備する。
7.1.2.9　雇用条件は、情報システム及びサービスと関連する組織の資産に対する、従業員及び契約相手によるアクセスの特性及び範囲に応じて、適切なものとする。
7.1.2.10　雇用の終了後も、定められた期間は、その雇用条件に含まれている責任を継続させる。