c）認可された保守要員だけが、装置の修理及び保守を実施する。
d）故障と見られるもの及び実際の故障の全て、並びに予防及び是正のための保守の全てについての記録を保持する。
e）装置の保守を計画する場合には、この保守を、要員が構内で行うのか、又は組織の外で行うのかを考慮して、適切な管理策を実施する。保守要員に適切な秘密保持契約を結ばせる。
f）構内で保守を実施する場合は保守要員を監督する。
g）遠隔保守のためのアクセスを認可し、管理する。
h）情報を保有している装置を保守のために構外へ持ち出す場合は、構外にある資産のセキュリティの対策を適用する。
i）保険において課される全ての保守要求事項を順守する。
j）保守の後、装置を作動させる前に、その装置が改ざんされていないこと及び適切に機能することを確実にするために検査する。
k）装置を処分することに決定した場合、装置のセキュリティを保った処分又は再利用の対策を適用する。

7b-7.14　装置のセキュリティを保った処分又は再利用

管理策：記憶媒体を内蔵した装置は、処分又は再利用する前に、全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保てるよう上書きしていることを確実にするために、検証する。

目的：　処分又は再利用する装置からの情報漏えいを防止するため。

詳細管理策

7b-7.14.1　装置は、処分又は再利用する前に、記憶媒体が内蔵されているか否かを確かめるために検証する。

7b-7.14.2　秘密情報又は著作権のある情報を格納した記憶媒体は、物理的に破壊、又はその情報を破壊、消去若しくは上書きする。

7b-7.14.3　秘密情報又は著作権のある情報の消去又は上書きには、標準的な削除機能を利用するよりも、元の情報を媒体から取り出せなくする技術を利用する。

（7b-7.14.3参考）　記憶媒体のセキュリティを保った処分に関する詳細な手引については7b-7.10を、情報の削除に関する手引については8b-8.10を参照。

7b-7.14.4　組織を特定する、又は情報の分類、管理責任者、システム若しくはネットワークの区別を示すラベル及び表示は、再販又は慈善団体への寄付を含む処分を行う前に除去する。

7b-7.14.5　組織は、施設のリース終了時又は施設外への移転時に、アクセス制御、監視装置などのセキュリティ管理策の除去を検討する。

（7b-7.14.5参考）　これは、次のような要因に依存する。
a）施設を元の状態に戻すリース合意
b）次のテナントに対して、取扱いに慎重を要する情報を含むシステムが残されるリスクの最小化
c）移転先の施設で管理策を再利用できること

8　技術的管理策

8a　情報アクセスの管理

8a-8.1　利用者エンドポイント機器

管理策：利用者エンドポイント機器に保存されている情報、処理される情報、又は利用者エンドポイント機器を介してアクセス可能な情報を保護する。

目的：　利用者エンドポイント機器を使用することによってもたらされるリスクから情報を保護するため。

詳細管理策

【技術的管理策全般】

8a-8.1.1　組織は、利用者エンドポイント機器のセキュリティを保った構成及び取扱いに関するトピック固有の方針を確立する。

8a-8.1.2　利用者エンドポイント機器のセキュリティに関するトピック固有の方針は、関係する全ての要員に伝達し、次のことを考慮する。
a）利用者エンドポイント機器が取扱い、処理、保存又は支援をすることが可能な情報の種類及び分類レベル
b）利用者エンドポイント機器の登録
c）物理的保護についての要求事項
d）ソフトウェアのインストールの制限
e）利用者エンドポイント機器のソフトウェア（ソフトウェアの版を含む。）の要求事項及び更新の適用の要求事項
f）情報サービス、公衆ネットワーク、又はその他の構外ネットワークへの接続に関する規則
g）アクセス制御
h）記憶装置の暗号化
i）マルウェアからの保護
j）遠隔操作による機器の無効化、データの消去又はロック
k）バックアップ
l）ウェブサービス及びウェブアプリケーションの使用
m）エンドユーザーの行動の分析
n）取外し可能なメモリ装置を含む取外し可能な機器の使用、及び物理ポートを無効化できる可能性
o）利用者エンドポイント機器に分割機能がある場合は、その利用。これによって、組織の情報及びその他の関連資産を、機器上の他の情報及びその他の関連資産からセキュリティを保って分離することが可能である。

8a-8.1.3　ある情報が特に慎重な取扱いを要する場合に、利用者エンドポイント機器を用いてその情報にアクセスは可能とするが、その機器には保存はできないようにするかどうかを検討する。

（8a-8.1.3参考）　その場合、機器に追加の技術的保護手段が必要になる可能性がある。例としては、オフライン作業のためのファイルのダウンロードの無効化、及びＳＤカードなどのローカルストレージの無効化を確実にすることがある。

8a-8.1.4　可能な限り、利用者エンドポイント機器の管理策に関する推奨事項を、構成管理又は自動化されたツールによって強制する。

【利用者の責任】

8a-8.1.5　利用者エンドポイント機器を保護するためのセキュリティ要求事項及び手順、並びにそのセキュリティ対策を実施する自らの責任について、全ての利用者に認識させる。

8a-8.1.6　利用者エンドポイント機器のセキュリティに関して、利用者に、次の事項を実施するように助言する。
a）利用者エンドポイント機器を利用する必要がなくなったら、実行していたセッションからログオフし、サービスを終了する。