b）利用者エンドポイント機器は、利用していない場合、物理的管理策及び論理的管理策を用いて、認可されていない利用から保護する。重要度の高い、取扱いに慎重を要する、又は影響の大きい業務情報が入っている機器を、無人の状態で放置しない。

c）公共の場所、オープンオフィス、集会所及びその他の保護されていない場所では、特別な注意を払って利用者エンドポイント機器を使用する。

d）利用者エンドポイント機器を盗難から物理的に保護する。

8a-8.1.7　利用者エンドポイント機器の盗難又は紛失に備えて、法令、規制、契約（保険を含む。）及び組織のその他のセキュリティ要求事項を考慮して、そのための手順を確立する。

【個人所有の機器の使用】

8a-8.1.8　個人所有の機器の使用を組織が許可している場合、この管理策に示している手引に加えて、次の事項を考慮する。

a）機器の個人使用と業務上の使用とを区別する。このような区別を可能とし、個人所有の機器に保存された業務データを保護するためのソフトウェアの使用も含む。

b）利用者が自らの義務（物理的保護、ソフトウェアの更新など）を受け入れた場合にだけ、業務情報にアクセスできるようにする。業務データについて帰属を主張しないこと、及び機器の盗難若しくは紛失があった場合又はサービス利用の認可が取り消された場合に組織が遠隔操作でデータを消去することへの合意を含む。こうした場合、ＰＩＩ保護に関する法令を考慮する。

c）個人所有の機器で開発された知的財産権に関する紛争を防止するためのトピック固有の方針及び手順

d）個人所有の機器へのアクセス（機械のセキュリティを検証する目的で、又は調査において）。これは法令で禁止されている場合がある。

e）要員又は外部組織の利用者が個人で所有する利用者エンドポイント機器上のクライアントソフトウェアについて、ライセンスを受ける責任を組織が負うことになる可能性があるソフトウェアライセンス契約

【無線接続】

8a-8.1.9　組織は、利用者エンドポイント機器のセキュリティのために次の事項に関する手順を確立する。

a）機器の無線接続の構成

b）関連するトピック固有の方針に従って適切な帯域幅の無線又は有線接続を使用すること

8a-8.2　特権的アクセス権

管理策：特権的アクセス権の割当て及び利用は、制限し、管理する。

目的：　認可された利用者、ソフトウェア構成要素及びサービスだけに特権的アクセス権が与えられることを確実にするため。

詳細管理策

8a-8.2.1　特権的アクセス権の割当ては、アクセス制御に関するトピック固有の方針に従って、認可プロセスによって管理する。

8a-8.2.2　この管理策の実施については、次の事項を考慮する。

a）各々のシステム又はプロセスの特権的アクセス権を必要とする利用者を特定する。

b）特権的アクセス権を、アクセス制御に関するトピック固有の方針に沿って、必要に応じて、かつ、事象ごとに、利用者に割り当てる（すなわち、特権的アクセスを必要とする活動を実行するために必要な力量をもつ個人に対してだけ、かつその個人の職務上の役割のための最小限の要求に基づいて）。

c）特権の認可プロセス（すなわち、誰が特権的アクセス権を承認することが可能かを決定するか、又は特権的アクセス権は認可プロセスが完了するまで許可しない。）及び割り当てた全ての特権の記録を維持する。

d）特権的アクセス権の終了に関する要求事項を定め、実施する。

e）利用者が、自らが特権的アクセス権をもっていること、及び自らがいつ特権的アクセスモードになっているかを認識することを確実にするための対策を講じる。考えられる対策としては、特別の利用者識別情報、利用者インタフェース設定、又は特別の装置の使用が含まれる。

f）特権的アクセス権における認証の要求事項は、通常のアクセス権における要求事項よりも要求が高くなる場合がある。特権的アクセス権を用いて作業を行う前に、再認証又は認証の格上げが必要になる場合がある。

g）定期的に、また組織に何か変更があった後に、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任及び力量の点で今も適格であるかどうかを検証する。

h）汎用の実務管理者ＩＤの使用を避けるため、システムの構成管理機能に応じて、具体的な規則を確立する。そのようなＩＤの認証情報を管理し、保護する。

i）特権的アクセス権を永続的に許可するのではなく、承認された変更又は活動を実施するのに必要な時間枠だけ一時的な特権的アクセスを許可する。これはしばしばブレークグラス手順（break glass procedure）と呼ばれ、しばしば特権的アクセス管理技術において自動化されている。

j）監査の目的で、システムへの全ての特権的アクセスのログを記録する。

k）特権的アクセス権をもつ識別情報を複数の人で共有又は連携することはせず、特定の特権的アクセス権の割当てが許可された個別の識別情報を各人に割り当てる。特権的アクセス権の管理を簡素化するために、識別情報をグループ化することが可能である。

l）特権的アクセス権をもつ識別情報は、管理作業を実行するためだけに使用し、日常の一般的な職務（すなわち、電子メールの確認、ウェブへのアクセス）には使用しない（利用者はこれらの活動のために別の通常のネットワーク識別情報をもつ。）。