9.1.2.4　ネットワーク及びネットワークサービスの利用に関する方針は、ネットワーク接続及びネットワークサービスへのアクセスを保護するための運用管理面からの管理策及び管理手順を対象にする。

9.1.2.5　ネットワーク及びネットワークサービスの利用に関する方針は、ネットワーク及びネットワークサービスへのアクセスに利用される手段（例えば、ＶＰＮ、無線ネットワーク）を対象にする。

9.1.2.6　ネットワーク及びネットワークサービスの利用に関する方針は、様々なネットワークサービスへのアクセスに対する利用者認証の要求事項を対象にする。

9.1.2.7　ネットワーク及びネットワークサービスの利用に関する方針は、ネットワークサービスの利用の監視を対象にする。

9.1.2.8　ネットワークサービスの利用に関する方針は、組織のアクセス制御方針と整合させる。

9.2　利用者アクセスの管理

目的：システム及びサービスへの、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止するため

9.2.1　アクセス権の割当てを可能にするために、利用者の登録及び登録削除についての正式なプロセスを実施する。

9.2.1.1　利用者ＩＤを管理するプロセスに、利用者と利用者自身の行動とを対応付けすること、及び利用者がその行動に責任をもつことを可能にする、一意な利用者ＩＤの利用を含める。

9.2.1.2　利用者ＩＤを管理するプロセスに、共有ＩＤの利用は、業務上又は運用上の理由で必要な場合にだけ許可し、承認し、記録することを含める。

9.2.1.3　利用者ＩＤを管理するプロセスに、組織を離れた利用者の利用者ＩＤの、即座の無効化又は削除を含める。

9.2.1.4　利用者ＩＤを管理するプロセスに、必要のない利用者ＩＤの定期的な特定、及び削除又は無効化することを含める。

9.2.1.5　利用者ＩＤを管理するプロセスに、別の利用者に重複する利用者ＩＤを発行しないことを確実にするよう定める。

9.2.2　全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施する。

9.2.2.1　利用者ＩＤに対するアクセス権の割当て及び無効化のプロセスに、情報システム又はサービスの利用についての、その情報システム又はサービスの管理責任者からの認可を得ていることの点検を含める（アクセス権について、管理層から別の承認を受けることが適切な場合もある。）。

9.2.2.2　利用者ＩＤに対するアクセス権の割当て及び無効化のプロセスに、許可したアクセスのレベルが、アクセス制御方針に適していることの点検を含める。

9.2.2.3　利用者ＩＤに対するアクセス権の割当て及び無効化のプロセスに、許可したアクセスのレベルが、職務の分離などのその他の要求事項と整合していることの検証を含める。

9.2.2.4　利用者ＩＤに対するアクセス権の割当て及び無効化のプロセスに、認可手順が完了するまで、（例えば、サービス提供者が）アクセス権を有効にしないことが確実になるよう定める。

9.2.2.5　利用者ＩＤに対するアクセス権の割当て及び無効化のプロセスに、情報システム又はサービスにアクセスするために利用者ＩＤに与えられたアクセス権の、一元的な記録の維持を含める。

9.2.2.6　利用者ＩＤに対するアクセス権の割当て及び無効化のプロセスに、役割又は職務を変更した利用者のアクセス権の変更、及び組織を離れた利用者のアクセス権の即座の解除又は停止することを含める。

9.2.2.7　利用者ＩＤに対するアクセス権の割当て及び無効化のプロセスに、情報システム又はサービスの管理責任者による、アクセス権の定期的なレビューを含める。

9.2.3　特権的アクセス権の割当て及び利用は、制限し、管理する。

9.2.3.1　特権的アクセス権の割当ては、関連するアクセス制御方針に従って、正式な認可プロセスによって管理する。

9.2.3.2　特権の割当ての正式な認可プロセスでは、各々のシステム又はプロセス（例えば、オペレーティングシステム、データベース管理システム、各アプリケーション）に関連した特権的アクセス権、及び特権的アクセス権を割り当てる必要がある利用者を特定する。

9.2.3.3　特権の割当ての正式な認可プロセスでは、特権的アクセス権を、アクセス制御方針に沿って、使用の必要性に応じて、かつ、事象に応じて、利用者に割り当てる。すなわち、利用者の職務上の役割のための最小限の要求事項に基づいて割り当てる。

9.2.3.4　特権の割当ての正式な認可プロセスでは、割り当てた全ての特権の認可プロセス及び記録を維持する。

9.2.3.5　特権の割当ての正式な認可プロセスでは、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。

9.2.3.6　特権の割当ての正式な認可プロセスでは、特権的アクセス権の終了に関する要求事項を定める。

9.2.3.7　特権の割当ての正式な認可プロセスでは、特権的アクセス権は、通常業務に用いている利用者ＩＤとは別の利用者ＩＤに割り当てる。特権を与えられたＩＤからは、通常業務を行わない。

9.2.3.8　特権の割当ての正式な認可プロセスでは、特権的アクセス権を与えられた利用者の力量がその職務に見合っていることを検証するために、その力量を定期的にレビューする。

9.2.3.9　特権の割当ての正式な認可プロセスでは、汎用の実務管理者ＩＤの認可されていない使用を避けるため、システムの構成管理機能に応じて、具体的な手順を確立及び維持する。

9.2.3.10　特権の割当ての正式な認可プロセスでは、汎用の実務管理者ＩＤに関しては、共有する場合に秘密認証情報の機密性を維持する（例えば、頻繁にパスワードを変更する、特権を与えられた利用者が離職する又は職務を変更する場合はできるだけ早くパスワードを変更する、特権を与えられた利用者の間で適切な方法でパスワードを伝達する。）。

9.2.4　秘密認証情報の割当ては、正式な管理プロセスによって管理する。

9.2.4.1　秘密認証情報の割当ての正式な管理プロセスでは、個人の秘密認証情報を秘密に保つ旨の文書への署名を、利用者に要求する。この署名文書は、雇用契約の条件に含める場合もある。

9.2.4.2　秘密認証情報の割当ての正式な管理プロセスでは、グループの（すなわち、共用の）秘密認証情報はグループのメンバ内だけの秘密に保つ旨の文書への署名を、利用者に要求する。この署名文書は、雇用契約の条件に含める場合もある。

9.2.4.3　秘密認証情報の割当ての正式な管理プロセスでは、利用者に各自の秘密認証情報を保持することを求める場合、最初に、セキュリティが保たれた仮の秘密認証情報を発行し、最初の使用時にこれを変更させる。

9.2.4.4　秘密認証情報の割当ての正式な管理プロセスでは、新規、更新又は仮の秘密認証情報を発行する前に、利用者の本人確認の手順を確立する。