9.2.4.5　秘密認証情報の割当ての正式な管理プロセスでは、仮の秘密認証情報は、セキュリティを保った方法で利用者に渡す。外部関係者を通して渡すこと又は保護されていない（暗号化していない）電子メールのメッセージを利用することは避ける。
9.2.4.6　秘密認証情報の割当ての正式な管理プロセスでは、仮の秘密認証情報は、一人一人に対して一意とし、推測されないものとする。
9.2.4.7　秘密認証情報の割当ての正式な管理プロセスでは、利用者は、秘密認証情報の受領を知らせる。
9.2.4.8　秘密認証情報の割当ての正式な管理プロセスでは、業者があらかじめ設定した秘密認証情報は、システム又はソフトウェアのインストール後に変更する。
9.2.5　資産の管理責任者は、利用者のアクセス権を定められた間隔でレビューする。
9.2.5.1　利用者のアクセス権は、定められた間隔で見直す。
9.2.5.2　利用者のアクセス権は、何らかの変更（例えば、昇進、降格、雇用の終了）があった後に見直す。
9.2.5.3　利用者のアクセス権は、利用者の役割が同一組織内で変更された場合、そのアクセス権についてレビューし、割当てをし直す。
9.2.5.4　特権的アクセス権の認可は、利用者のアクセス権より頻繁な間隔でレビューする。
9.2.5.5　特権の割当てを定められた間隔で点検して、認可されていない特権が取得されていないことを確認する。
9.2.5.6　特権アカウントを変更する際は、定期的なレビューのために変更ログをとる。
9.2.6　全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正する。
9.2.6.1　雇用の終了時に、アクセス権を削除する必要があるかどうかを決定し、情報並びに情報処理施設及びサービスに関連する資産に対する個人のアクセス権を削除又は一時停止を行う。
9.2.6.2　雇用を変更した場合、新規の業務において承認されていない全てのアクセス権を削除する。
9.2.6.3　削除又は修正が望ましいアクセス権には、物理的な及び論理的なアクセスに関するものを含める。
9.2.6.4　従業員及び契約相手のアクセス権を特定するあらゆる文書に、アクセス権の削除又は修正を反映する。
9.2.6.5　辞めていく従業員又は外部の利用者が引き続き有効な利用者ＩＤのパスワードを知っている場合、雇用・契約・合意の終了又は変更に当たって、これらのパスワードを変更する。
9.2.6.6　情報及び情報処理施設に関連する資産へのアクセス権は、雇用の終了又は変更の前に、雇用の終了又は変更が、従業員若しくは外部の利用者の側によるものか又は経営側によるものかどうか、及び雇用の終了の理由、従業員、外部の利用者、又は他の利用者の現時点の責任、現在アクセス可能な資産の価値のリスク因子の評価に応じて、縮小又は削除する。

9.3　利用者の責任

目的：利用者に対して、自らの秘密認証情報を保護する責任をもたせるため

9.3.1　秘密認証情報の利用時に、組織の慣行に従うことを、利用者に要求する。
9.3.1.1　全ての利用者に、秘密認証情報を秘密にしておき、関係当局の者を含む他者に秘密認証情報が漏えいしないよう助言する。
9.3.1.2　全ての利用者に、秘密認証情報を、例えば、紙、ソフトウェアのファイル、携帯用の機器に、記録して保管しなように助言する。ただし、記録がセキュリティを確保して保管され、その保管方法が承認されている場合には、この限りではない（例えば、パスワード保管システム（password vault））。
9.3.1.3　全ての利用者に、秘密認証情報に対する危険の兆候が見られる場合には、その秘密認証情報を変更するよう助言する。
9.3.1.4　全ての利用者に、秘密認証情報としてパスワードを用いる場合は、十分な最短文字数をもつ質の良いパスワードを選定するよう助言する（質の良いパスワードとは、次の条件を満たすものとする。①覚えやすい。②当人の関連情報（例えば、名前、電話番号、誕生日）から、他の者が容易に推測できる又は得られる事項に基づかない。③辞書攻撃にぜい弱でない（すなわち、辞書に含まれる語から成り立っていない。）。④同一文字を連ねただけ、数字だけ、又はアルファベットだけの文字列ではない。⑤仮パスワードを発行する場合、最初のログオン時点で変更する。）。
9.3.1.5　全ての利用者に、個人用の秘密認証情報を共有しないよう助言する。
9.3.1.6　全ての利用者に、自動ログオン手順において、秘密認証情報としてパスワードを用い、かつ、そのパスワードを保管する場合、パスワードの適切な保護を確実にするよう助言する。
9.3.1.7　全ての利用者に、業務目的のものと業務目的でないものとに、同じ秘密認証情報を用いないよう助言する。

9.4　システム及びアプリケーションのアクセス制御

目的：システム及びアプリケーションへの、認可されていないアクセスを防止するため

9.4.1　情報及びアプリケーションシステム機能へのアクセスは、アクセス制御方針に従って、制限する。
9.4.1.1　アクセスへの制限は、個々の業務用アプリケーションの要求事項に基づき、定められたアクセス制御方針に従う。
9.4.1.2　アクセス制限の要求事項を満たすために、アプリケーションシステム機能へのアクセスを制御するためのメニューを提供する。
9.4.1.3　アクセス制限の要求事項を満たすために、利用者がアクセスできるデータを制御する。
9.4.1.4　アクセス制限の要求事項を満たすために、利用者のアクセス権（例えば、読出し、書込み、削除、実行）を制御する。
9.4.1.5　アクセス制限の要求事項を満たすために、他のアプリケーションのアクセス権を制御する。
9.4.1.6　アクセス制限の要求事項を満たすために、出力に含まれる情報を制限する。
9.4.1.7　アクセス制限の要求事項を満たすために、取扱いに慎重を要するアプリケーション、アプリケーションデータ又はシステムを隔離するための、物理的又は論理的なアクセス制御を提供する。
9.4.2　アクセス制御方針で求められている場合には、システム及びアプリケーションへのアクセスは、セキュリティに配慮したログオン手順によって制御する。
9.4.2.1　利用者が提示する識別情報を検証するために、適切な認証技術を選択する。
9.4.2.2　強い認証及び識別情報の検証が必要な場合には、パスワードに代えて、暗号による手段、スマートカード、トークン、生体認証などの認証方法を用いる。
9.4.2.3　システム又はアプリケーションへログオンするための手順は、認可されていないアクセスの機会を最小限に抑えるように設計する。
9.4.2.4　ログオン手順では、認可されていない利用者に無用な助けを与えないために、システム又はアプリケーションについての情報の開示は、最小限にする。
9.4.2.5　システム又はアプリケーションの識別子を、ログオン手順が正常に終了するまで表示しない。
9.4.2.6　ログオン手順では、「コンピュータへのアクセスは、認可されている利用者に限定する」という警告を表示する。