5c-5.16.2　組織は、利用者識別情報に関連する情報の変更を取り扱う支援プロセスをもつ。

（5c-5.16.2参考）　このプロセスは、個人に関連する信頼する文書の再検証を含む場合がある。

5c-5.16.3　第三者が提供し又は発行した識別情報を使用する場合、組織は、必要な信頼レベルが第三者の識別情報にあり、関連するリスクを知り、十分に対応する。

（5c-5.16.3参考）　この対応には、第三者に関連する管理策、及び認証情報に関連する管理策を含む場合がある。

5c-5.17　認証情報

管理策：認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理する。

目的：　適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。

詳細管理策

【認証情報の割当て】

5c-5.17.1　認証情報の割当て及び管理のプロセスは、次の事項を確実にする。

a）仮の秘密認証情報として登録プロセス中に自動的に生成される個人パスワード又は個人識別番号（ＰＩＮ）は、推測不可能であり、各人に対して一意で、かつ、利用者は最初の使用後にそれを変更することが要求される。

b）新規、更新又は仮の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。

c）仮の認証情報を含む認証情報は、セキュリティを保った方法で利用者に渡し、保護されていない（平文の）電子メールのメッセージをこの目的で利用することは避ける。

d）利用者は、認証情報の受領を知らせる。

e）業者があらかじめ定めた又は提供した初期設定の認証情報は、システム又はソフトウェアのインストール直後に変更する。

f）認証情報の割当て及び管理に関する重要な事象の記録を保持し、記録に機密性を付与する。記録保持方法は、承認を受ける。

【利用者の責任】

5c-5.17.2　認証情報にアクセスする又はそれを使用する者に、次の事項を確実に行うよう助言する。

a）パスワードなどの秘密認証情報は機密を保つ。個人の秘密認証情報を他人と共有しない。複数の利用者に、又は個人でないエンティティにひも（紐）付けられている識別情報に対して使用する秘密認証情報は、認可された人とだけ共有する。

b）影響を受けた又は侵害された認証情報は、侵害の知らせ又はその他の兆候があれば、直ちに変更する。

c）パスワードを認証情報として使用する場合、例えば、次のような最適な慣行の推奨事項に従った強力なパスワードを選択する。

1）パスワードは、当人に関する情報から、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。

2）パスワードは辞書の単語又はそれらの組合せに基づかない。

3）覚えやすいパスフレーズを使用し、英数字及び特殊文字を含めるようにする。

4）パスワードに最小限必要とする長さを定める。

d）異なるサービス及びシステム間で同じパスワードを使用しない。

e）ａ）～ｄ）の規則に従う義務が、雇用条件にも含まれている。

【パスワード管理システム】

5c-5.17.3　パスワードを認証情報として使用する場合、パスワード管理システムは、次の事項を行う。

a）利用者が自分のパスワードを選択及び変更できるようにし、入力エラーに対処するための確認手順を含める。

b）優良な慣行の推奨事項に従って強固なパスワードを使用させる。

c）パスワードは、最初のログイン時に利用者に変更させる。

d）必要に応じて、例えば、セキュリティインシデントの後に、又は有効な識別情報のパスワードを知っている利用者の雇用の終了若しくは変更の時に、パスワードを変更させる。

e）以前のパスワードの再利用を防止する。

f）一般的に使われるパスワード、並びにハッキングされたシステムで侵害された利用者名及びパスワードの組合せの使用を防止する。

g）パスワードは、入力時に、画面上に表示しない。

h）パスワードは、保護した形態で保存し、伝達する。

5c-5.17.4　パスワードの暗号化及びハッシュ化は、パスワードに関する承認された暗号技術に従って実行する。

5c-5.18　アクセス権

管理策：情報及びその他の関連資産へのアクセス権は、組織のアクセス制御に関するトピック固有の方針及び規則に従って、提供、レビュー、変更及び削除する。

目的：　情報及びその他の関連資産へのアクセスを、事業上の要求事項に従って定義し、認可することを確実にするため。

詳細管理策

【アクセス権の提供及び無効化】

5c-5.18.1　エンティティの認証された識別情報に対する物理的及び論理的アクセス権の割当て又は無効化のプロセスには、次の事項を含む。

a）情報及びその他の関連資産の利用についての、その情報及びその他の関連資産の管理責任者からの認可の取得

b）事業上の要求事項及び組織のアクセス制御に関するトピック固有の方針並びに規則の考慮

c）アクセス権の承認及び実施の役割の分離、並びに相反する役割の分離を含む、職務の分離の考慮

d）ある者が情報及びその他の関連資産にアクセスする必要がなくなった場合にアクセス権を削除する。特に、組織を去った利用者のアクセス権を時機を失せずに削除する。

e）臨時要員、又は要員が必要とする一時的なアクセスについて、限られた期間の一時的アクセス権を与え、期限の日に取り消すことの考慮