e）プログラムリストは、セキュリティが保たれた環境で保持する。その環境では、読取り及び書込みアクセスを適切に管理し、割り当てる。
f）ソースコードへの全てのアクセス及び全ての変更について、監査ログを維持する。

8a-8.4.6　プログラムソースコードの公開を意図している場合には、その完全性に保証を与える追加の管理策の使用を考慮する。

8a-8.5　セキュリティを保った認証

管理策：セキュリティを保った認証技術及び手順を、情報へのアクセス制限、及びアクセス制御に関するトピック固有の方針に基づいて備える。

目的：　システム、アプリケーション及びサービスへのアクセスを許可するときに、利用者又はエンティティをセキュリティを保って認証することを確実にするため。

詳細管理策

8a-8.5.1　利用者、ソフトウェア、メッセージ、及びその他のエンティティ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。

8a-8.5.2　認証の強度は、アクセスする情報の分類に適したものを選択する。

8a-8.5.3　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、ディジタル証明書、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。

8a-8.5.4　重要な情報システムにアクセスするために、認証情報に追加の認証要素を加える。

（8a-8.5.4参考１）　知識、所持物、生体情報など、複数の認証要素を組み合わせて使用することで、認可されていないアクセスの可能性を減らすことが可能である。

（8a-8.5.4参考２）　特定の状況下においては、多要素認証に他の手法も組み合わせて、あらかじめ定義したルール及びパターンに基づく追加の要素も条件として要求することが可能である。このルール及びパターンには、通常と異なる場所からのアクセス、通常と異なる装置・機器からのアクセス、通常と異なる時間でのアクセスなどがある。

8a-8.5.5　生体認証情報は、機密性が損なわれた場合は無効化する。

8a-8.5.6　使用の条件によっては、生体認証が利用できないことに備えるため、生体認証は少なくとも一つの代替の認証手法をもつ。

8a-8.5.7　システム又はアプリケーションにログオンする手順は、認可されていないアクセスのリスクを最小限に抑えるように設計する。

8a-8.5.8　ログオンの手順及び技術は、次の事項を考慮して実装する。

a）認可されていない利用者に不必要な手助けを提供することを避けるために、取扱いに慎重を要するシステム又はアプリケーションの情報を、ログオン手順が正常に終了するまで表示しない。
b）“システム、アプリケーション、又はサービスへのアクセスは、認可されている利用者に限定する”という一般的な警告を表示する。
c）ログオン手順中に、認可されていない利用者の助けとなるようなメッセージを表示しない。
d）ログオン情報の妥当性確認は、全ての入力データが完了した時点でだけ行う。
e）利用者名及びパスワードに関する総当たり攻撃でログオンしようとする試みから保護する。
f）失敗した試み及び成功した試みのログをとる。
g）ログオン制御への違反又は違反が試みられた可能性を検知した場合には、セキュリティ事象として取り上げる。
h）ログオンが成功裏に終了した時点で、次の情報を別の手段で表示又は送信する。
　1）前回成功裏にログオンできた日時
　2）前回のログオン以降、失敗したログオンの試みがある場合は、その詳細
i）入力したパスワードを平文で表示しない。場合によっては、利用者のログオンを容易にするため、この機能を無効化する必要がある可能性がある。
j）ネットワーク“スニファ”プログラムで捕捉されることを避けるため、ネットワークを介してパスワードを平文で通信しない。
k）リスクの高い場所では、特に、使用せずにあらかじめ定めた時間が経過したセッションを終了する。
l）リスクの高いアプリケーションのセキュリティを高め、認可されていないアクセスの危険性を低減するために、接続の継続時間を制限する。

8a-8.6　容量・能力の管理

管理策：現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し調整する。

目的：　情報処理施設、人的資源、オフィス及びその他の施設で必要とされる容量・能力の確保を確実にするため。

詳細管理策

8a-8.6.1　事業におけるシステム及びプロセスの重要度を考慮に入れて、情報処理施設、人的資源、オフィス及びその他の施設の容量・能力に関する要求事項を特定する。

8a-8.6.2　システムの可用性及び効率性の確保を確実にするため、また、必要な場合には、改善のために、システムの調整及び監視を適用する。

8a-8.6.3　組織は、最大性能の要求事項を満たすのに十分なシステム容量・能力が利用できることを確認するために、システム及びサービスの負荷テストを実施する。

8a-8.6.4　適切な時点で問題を知らせるために、検知のための管理策を備える。

8a-8.6.5　将来必要とされる容量・能力の予測では、新しい事業及びシステムに対する要求事項並びに組織の情報処理の能力についての現在の傾向及び予測される傾向を考慮する。

8a-8.6.6　入手に長い期間又は高額な費用がかかる資源については、特別な注意を払うため、管理者、及びサービス又は製品の管理責任者は、主要なシステム資源の使用を監視する。

8a-8.6.7　システムセキュリティ又はサービスに脅威をもたらす可能性のある、潜在的な資源の制限及び主要な要員への依存度合いを特定し、回避するために、管理者は、容量・能力に関する情報を用い、また、適切な処置を立案する。

（8a-8.6参考）　十分な容量・能力の提供は、容量・能力の増強又は需要の低減によって達成することが可能である。