9.4.2.7　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。
9.4.2.8　ログオン手順では、ログオン情報の妥当性検証は、全ての入力データが完了した時点でだけ行う。誤り条件が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを指摘しない。
9.4.2.9　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。
9.4.2.10　ログオン手順では、失敗した試み及び成功した試みのログをとる。
9.4.2.11　ログオン制御への違反又は違反が試みられた可能性が検知された場合には、セキュリティ事象として取り上げる。
9.4.2.12　ログオンが成功裏に終了した時点で、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、その詳細を表示する。
9.4.2.13　ログオン手順では、入力したパスワードは表示しない。
9.4.2.14　ログオン手順では、ネットワークを介してパスワードを平文で通信しない。
9.4.2.15　ログオン手順では、リスクの高い場所（例えば、組織のセキュリティ管理外にある公共の場所又は外部の区域、モバイル機器）では特に、あらかじめ定めた使用中断時間が経過したセッションは終了する。
9.4.2.16　ログオン手順では、リスクの高いアプリケーションのセキュリティを高めるために接続時間を制限し、認可されていないアクセスの危険性を低減する。
9.4.3　パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にするものとする。
9.4.3.1　パスワードの管理システムでは、責任追跡性を維持するために、それぞれの利用者ＩＤ及びパスワードを使用させるようにする。
9.4.3.2　パスワードの管理システムでは、利用者に自分のパスワードの選択及び変更を許可し、また、入力誤りを考慮した確認手順を組み入れる。
9.4.3.3　パスワードの管理システムでは、質の良いパスワードを選択させるようにする。
9.4.3.4　パスワードの管理システムでは、パスワードは、最初のログオン時に利用者に変更させるようにする。
9.4.3.5　パスワードの管理システムでは、パスワードは、定期的に及び必要に応じて変更させるようにする。
9.4.3.6　パスワードの管理システムでは、以前に用いられたパスワードの記録を維持し、再使用を防止する。
9.4.3.7　パスワードの管理システムでは、パスワードは、入力時に、画面上に表示しないようにする。
9.4.3.8　パスワードの管理システムでは、パスワードのファイルは、アプリケーションシステムのデータとは別に保存する。
9.4.3.9　パスワードの管理システムでは、パスワードは、保護した形態で保存し、伝達する。
9.4.4　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理する。
9.4.4.1　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用のための識別、認証及び認可手順を整備し、使用する。
9.4.4.2　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムは、アプリケーションソフトウェアから分離する。
9.4.4.3　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、可能な限り少人数の信頼できる認可された利用者だけに限定する。
9.4.4.4　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムを臨時に用いる場合の認可手順を整備する。
9.4.4.5　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用を制限する（例えば、認可されたシステム変更のための期間での利用）。
9.4.4.6　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの全ての使用に関するログを取得する。
9.4.4.7　システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの認可レベルを明確にし、文書化する。
9.4.4.8　不要なシステム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムは全て除去又は無効化する。
9.4.4.9　権限の分離が必要な場合には、システム上のアプリケーションへのアクセス権をもつ利用者に対して、システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用を禁止する。
9.4.5　プログラムソースコードへのアクセスは、制限する。
9.4.5.1　プログラムソースコード及び関連書類（例えば、設計書、仕様書、検証計画書、妥当性確認計画書）へのアクセスは、認可されていない機能が入り込むことを防止し、意図しない変更を回避し、価値の高い知的財産の機密性を維持するために、厳重に管理する。
9.4.5.2　可能な限り、プログラムソースライブラリは、運用システムの中に保持しない。
9.4.5.3　プログラムソースコード及びプログラムソースライブラリは、確立した手順に従って管理する。
9.4.5.4　サポート要員による、プログラムソースライブラリへの無制限のアクセスを許さない。
9.4.5.5　プログラムソースライブラリ及び関連情報の更新、並びにプログラマへのプログラムソースの発行は、適切な認可を得た後にだけ実施する。
9.4.5.6　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。
9.4.5.7　プログラムソースライブラリへの全てのアクセスについて、監査ログを維持する。
9.4.5.8　プログラムソースライブラリの保守及び複製は、厳しい変更管理手順に従う。
9.4.5.9　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、その完全性を保証するために役立つ追加的な管理策（例えば、ディジタル署名）を実施する。

10　暗号
10.1　暗号による管理策
目的：情報の機密性、真正性及び／又は完全性を保護するために、暗号の適切かつ有効な利用を確実にするため
10.1.1　情報を保護するための暗号による管理策の利用に関する方針は、策定し、実施する。
10.1.1.1　暗号の利用に関する方針は、業務情報を保護する上での一般原則も含め、暗号による管理策の組織全体での使用に関する管理の取組みを考慮して定める。
10.1.1.2　暗号の利用に関する方針は、リスクアセスメントに基づく、要求される暗号アルゴリズムの種別、強度及び品質を考慮に入れた、要求された保護レベルの識別を考慮して定める。
10.1.1.3　暗号の利用に関する方針は、持ち運び可能な若しくは取外し可能な媒体装置又は通信によって伝送される情報を、保護するための暗号の利用を考慮して定める。
10.1.1.4　暗号の利用に関する方針は、暗号鍵の保護手法、及び鍵が紛失、危険又は損傷した場合の暗号化された情報の復元手法を含む、鍵管理に対する取組み方を考慮して定める。

第明治三二十種五郵年三月三十一物三十一認可日