8b-8.11.6　データマスキング、仮名化又は匿名化を利用する場合、次の事項を考慮する。

a）処理するデータの使用法に応じた、データマスキング、仮名化又は匿名化の強度のレベル

b）処理するデータへのアクセス制御

c）処理するデータの使用法に関する合意又は制限

d）ＰＩＩ主体を識別するために、処理するデータを他の情報と照合することの禁止

e）処理するデータの提供及び受領の追跡

8b-8.12　データ漏えい防止

管理策：データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存又は送信するシステム、ネットワーク及びその他の装置に適用する。

目的：　個人又はシステムによる情報の認可されていない開示及び抽出を検出し、防止するため。

詳細管理策

8b-8.12.1　組織は、データ漏えいのリスクを減らすために、次の事項を考慮する。

a）漏えいから保護する情報の特定及び分類

b）データ漏えいの経路・手段の監視

c）情報の漏えいを防止するための処置

8b-8.12.2　データ漏えい防止ツールを、次の目的で使用する。

a）認可されていない開示のリスクがある取扱いに慎重を要する情報を特定し、監視する。

b）取扱いに慎重を要する情報の開示を検出する。

c）取扱いに慎重を要する情報を漏えいする利用者の行為又はネットワーク送信を阻止する。

8b-8.12.3　組織は、組織の外部のサービス、装置・機器及び記憶媒体にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する必要があるかどうかを判断する。

8b-8.12.4　組織の管理外にデータをコピーして貼り付ける、又はアップロードする利用者の権限を制限する場合、データ漏えい防止ツール又は既存のツールの組合せなどの技術を導入する。

8b-8.12.5　データの取り出しが必要な場合、利用者による取り出しを許可し、利用者に自らの行動にアカウンタビリティをもたせる役割を、データの管理責任者に与える。

8b-8.12.6　画面のスクリーンショット又は写真を撮ることには、利用条件、訓練及び監査によって対応する。

8b-8.12.7　データをバックアップする場合、暗号化、アクセス制御及びバックアップを保持する記憶媒体の物理的保護などの対策を使用して、取扱いに慎重を要する情報の保護を確実にする。

8b-8.12.8　データ漏えい防止は、ちょう報活動の対象となる可能性がある、又はコミュニティにとって重要な可能性がある秘密情報を敵対者が情報収集活動によって取得することに対する保護も考慮する。

8b-8.12.9　データ漏えい防止活動は、独立の活動又は敵対者の情報収集活動への対応のいずれかとして、敵対者の決定を混乱させる方策を講じる。

8b-8.13　情報のバックアップ

管理策：合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査する。

目的：　データ又はシステムの損失からの回復を可能にするため。

詳細管理策

8b-8.13.1　組織のデータ保持及び情報セキュリティの要求事項に対応するために、バックアップに関するトピック固有の方針を確立する。

8b-8.13.2　インシデント又は記憶媒体の故障若しくは損失の後に、全ての重要な情報及びソフトウェアの回復を確実にするために、適切なバックアップ設備を備える。

8b-8.13.3　バックアップに関するトピック固有の方針に対応するため、組織は、情報、ソフトウェア及びシステムをバックアップする方法について計画を作成し、実装する。

8b-8.13.4　バックアップ計画を策定するときは、次の事項を考慮に入れる。

a）バックアップ情報の正確かつ完全な記録及び文書化したデータ復旧手順を作成する。

b）バックアップの範囲、及びバックアップの頻度は、組織の事業上の要求事項、関係する情報のセキュリティ要求事項、及びその情報の組織の継続的な運用に対する重要度を考慮して決定する。

c）バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。

d）バックアップ情報に対して、主事業所に適用されている標準と整合した、適切なレベルの物理的及び環境的保護を実施する。

e）バックアップに用いる媒体は、必要になった場合の緊急利用について信頼できることを確実にするために、定期的に試験する。バックアップデータで復旧する機能のテストは、バックアップ又はデータ復旧プロセスに失敗して、データに修復不能な損傷又は損失が生じることがないように、テストシステム上で行い、原本の記憶媒体に上書きしない。

f）特定したリスクに応じて、暗号化によってバックアップ情報を保護する。

g）バックアップを作成する前に、不注意によるデータ損失の検出を確実にするように注意する。

8b-8.13.5　バックアップの運用手順では、バックアップに関するトピック固有の方針に従って、バックアップの完全性を確保するために、その実行を監視し、計画したバックアップの失敗に対処する。

8b-8.13.6　個々のシステム及びサービスに関するバックアップ対策は、インシデント対応及び事業継続計画の目的を満たすことを確実にするために、定期的に試験する。

8b-8.13.7　定期的な試験は、これを復旧手順のテストと組み合わせて、事業継続計画において必要とされる復旧時間に照らして確認する。

8b-8.13.8　重要なシステム及びサービスに関するバックアップ対策は、災害に際してシステム全体を復旧させるために必要となる、システム情報、アプリケーション及びデータの全てを対象とする。