8b-8.13.9　組織がクラウドサービスを利用する場合、クラウドサービス環境にある組織の情報、アプリケーション及びシステムのバックアップ情報を作成する。

8b-8.13.10　組織は、クラウドサービスの一部として提供されるバックアップサービスを利用する場合、バックアップの要求事項が満たされるかどうか、また、どのように満たされるかを特定する。

8b-8.13.11　重要な業務情報の保持期間は、複製の保存に関するあらゆる要求事項を考慮に入れて、決定する。

8b-8.13.12　組織は、情報の保持期間が終了したら、バックアップに使用している記憶媒体にある情報の削除、また、法令及び規制を考慮する。

8b-8.14　情報処理施設・設備の冗長性

管理策：情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入する。

目的：　情報処理施設・設備の継続的な運用を確実にするため。

詳細管理策

8b-8.14.1　組織は、業務上のサービス及び情報システムの可用性に関する要求事項を特定する。

8b-8.14.2　組織は、可用性の要求事項を満たすために、適切な冗長性をもってシステムアーキテクチャを設計し、実装する。

8b-8.14.3　組織は、冗長な構成要素及び情報処理施設・設備を作動させる手順を計画し、実装する。

（8b-8.14.3参考）　冗長性は、情報処理施設・設備の一部又は全体を二重化させることによって導入することが可能である。

8b-8.14.4　冗長な構成要素及び情報処理施設・設備を作動させる手順では、冗長な構成要素及び処理活動を常に作動させておくか、又は緊急の場合に自動若しくは手動で作動させるかを定める。

8b-8.14.5　冗長な構成要素及び情報処理施設・設備は、主たる構成要素及び情報処理施設・設備と同じセキュリティレベルをもつことを確実にする。

8b-8.14.6　情報処理施設・設備の故障を組織に警告し、計画した手順を実行できるようにし、情報処理施設・設備を修理又は交換している間も、継続して可用性の維持を可能とする仕組みを設ける。

8b-8.14.7　組織は、冗長システムを実装する場合、次の事項を考慮する。

a）インターネットサービス提供者など、ネットワーク及び重要な情報処理施設・設備の供給者、二者以上と契約する。

b）冗長性のあるネットワークを使用する。

c）冗長構成をとったシステムをもつ地理的に離れた二つのデータセンターを使用する。

d）物理的に冗長性のある電力供給装置又は電源を使用する。

e）ソフトウェア構成要素の複数の並列インスタンスを、同じデータセンター内又は異なるデータセンターのインスタンス間で自動負荷分散して使用する。

f）システムにおいて二重化した構成要素をもつ、又はネットワークにおいて二重化した構成要素をもつ。

8b-8.14.8　実施できる場合、できれば本番モードにおいて、一つの構成要素から別の構成要素への切替え（failover）が意図したとおりに動作することを確実にするために、冗長な情報システムを試験する。

8b-8.15　ログ取得

管理策：活動、例外処理、過失及びその他の関連する事象を記録したログを取得し、保存し、保護し、分析する。

目的：　事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。

詳細管理策

【ログ取得全般】

8b-8.15.1　組織は、ログを作成する目的、どのデータを収集し、ログに記録するか、及びログデータを保護し、取り扱うためのログ特有の要求事項を決定する。

8b-8.15.2　ログ特有の要求事項は、ログ取得に関するトピック固有の方針に文書化する。

8b-8.15.3　活動、例外処理、過失及びその他の関連する事象を記録したログを取得する場合には、各事象について、次の事項をイベントログに含める。

a）利用者ＩＤ

b）システムの動作

c）関係する事象の日時及び内容

d）装置・機器の識別情報、システムの識別子及び所在地

e）ネットワークアドレス及びプロトコル

8b-8.15.4　次の事象について、ログ取得を考慮する。

a）システムへのアクセスの、成功及び失敗した試み

b）データ及び他の資源へのアクセスの、成功及び失敗した試み

c）システム構成の変更

d）特権の利用

e）ユーティリティプログラム及びアプリケーションの利用

f）アクセスされたファイル、及び重要なデータファイルの削除を含むアクセスの種類

g）アクセス制御システムが発した警報

h）セキュリティシステムの起動及び停止

i）識別情報の作成、変更又は削除

j）アプリケーションにおいて利用者が実行したトランザクション

（8b-8.15.4参考）　インシデントの分析、警告及び調査のためにシステム間のログを関係付けられるように、全てのシステムが同期した時刻源をもつことが重要である。

【ログの保護】

8b-8.15.5　特権的アクセス権をもつ利用者を含め、利用者は自らの活動のログを削除又は停止する権限をもたない。

8b-8.15.6　特権を与えられた利用者に関するアカウンタビリティを維持するために、ログを保護及びレビューする。

（8b-8.15.6参考）　利用者は、その直接の管理下で、情報処理施設・設備に関するログを改変する可能性がある。