i）クラウドサービスカスタマである組織が利用するクラウドサービスプロバイダが提供する機能に基づいて、該当する場合に、データ及び構成情報の必要なバックアップを提供し、セキュリティを保った方法でバックアップを管理する。

j）サービスの提供中又はサービスの終了時に組織が要求する場合、クラウドサービスカスタマである組織が所有する構成ファイル、ソースコード、データなどの情報を提出し、返却する。

5d-5.23.8　クラウドサービスカスタマである組織は、組織へのサービス提供方法に対して、実質的に顧客に影響を与える変更を行う前にクラウドサービスプロバイダが事前に通知することを合意において要求することが望ましいかどうかを、次の事項を含めて考慮する。

a）クラウドサービスの提供に影響する又はそれを変更するような技術インフラストラクチャの変更

b）新しい地理的又は法的区域での情報の処理又は保存

c）ピアクラウドサービスプロバイダ又はその他の下請負業者の利用（既存の業者の変更又は新しい業者の利用を含む。）

5d-5.23.9　クラウドサービスを利用する組織は、クラウドサービスプロバイダと緊密な連絡を維持する。

（5d-5.23.9参考）　こうした連絡によって、クラウドサービスプロバイダとクラウドサービスカスタマである組織との両方が各サービスの特性を監視し、合意に含まれるコミットメントの不履行を報告する仕組みを含む、クラウドサービスの利用についての情報セキュリティに関する情報の相互交換が可能になる。

5e　インシデント管理

5e-5.24　情報セキュリティインシデント管理の計画策定及び準備

管理策：組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定め、確立し、伝達することによって、情報セキュリティインシデント管理を計画し、準備する。

目的：　情報セキュリティ事象に関する伝達を含む、情報セキュリティインシデントへの迅速で、効果的で、一貫性があり、かつ、秩序のある対応を確実にするため。

詳細管理策

【役割及び責任】

5e-5.24.1　組織は、適切な情報セキュリティインシデント管理プロセスを確立する。

5e-5.24.2　インシデント管理手順を実行するための役割及び責任を決定し、関連する内部及び外部の利害関係者に効果的に伝達する。

5e-5.24.3　情報セキュリティインシデント管理プロセスを確立する際には、次の事項を考慮する。

a）連絡先を含む、情報セキュリティ事象を報告するための共通の方法を確立する。

b）管理、文書化、検知、トリアージ、優先順位付け、分析、伝達及び利害関係者の調整を含む、組織が情報セキュリティインシデントを管理する機能を備えるためのインシデント管理プロセスを確立する。

c）情報セキュリティインシデントを評価し、それに対応し、そこから学習する機能を組織が備えるためのインシデント対応プロセスを確立する。

d）組織内で、情報セキュリティインシデントに関連する事項は、力量のある要員だけが取り扱えるようにする。そうした要員には、文書化した手順及び定期的な訓練を提供する。

e）インシデントに対応する要員に必要な訓練、認証及び継続的な専門能力開発を特定するプロセスを確立する。

【インシデント管理手順】

5e-5.24.4　情報セキュリティインシデント管理の目的について、経営陣が同意している。

5e-5.24.5　情報セキュリティインシデント管理について責任ある人々が、潜在的な結果及び重大度に基づく解決の時間枠を含む、組織が決めた情報セキュリティインシデントの取扱いの優先順位を理解していることを確実にする。

5e-5.24.6　これらの目的及び優先順位を満たすようにインシデント管理手順を実施する。

5e-5.24.7　経営陣は、次の活動のためにそれぞれのシナリオ及び手順が作成され、実施されていることを考慮して、情報セキュリティインシデント管理計画の作成を確実にする。

a）何が情報セキュリティインシデントに該当するかに関する基準に従った情報セキュリティ事象の評価

b）情報セキュリティ事象及び情報セキュリティインシデントの監視、検知、分類、分析及び報告

c）インシデントの種類及びカテゴリに従った、対応及びエスカレーション、危機管理の発動及び継続計画の発動の可能性、インシデントからの管理された回復、並びに内部及び外部の利害関係者への伝達を含む、情報セキュリティインシデントの終結までの管理

d）関係当局、外部の利益団体及び会議、供給者、顧客など、内部及び外部の利害関係者との調整

e）インシデント管理活動のログ取得

f）証拠の取扱い

g）根本原因分析又は事後分析手順

h）学んだ教訓及びインシデント管理手順又は一般的な情報セキュリティ管理策についての必要な改善の特定

【報告手順】

5e-5.24.8　情報セキュリティ事象及び情報セキュリティインシデントの報告手順には、次の事項を含める。

a）情報セキュリティ事象が発生した場合にとる処置

b）情報セキュリティインシデントを報告する際に要員が必要な全ての活動を実行できることを支援するためのインシデント書式の使用

c）情報セキュリティ事象の報告者に、その件が対処され、終結した後で、可能な限り結果を知らせることを確実にするための適切なフィードバックの手続

d）インシデント報告書の作成

5e-5.24.9　インシデント管理手順を実施する際は、関連する利害関係者へ定められた時間内にインシデント報告する外部の要求事項を考慮する。