h）特定された情報セキュリティ事象又はインシデントに対応し、管理する。
i）情報セキュリティのぜい弱性を特定し、管理する。
j）供給者とその供給者との間の供給者関係における情報セキュリティの側面をレビューする。
k）供給者が、十分なサービス提供能力を維持すること、及び重大なサービスの不具合又は災害の後においても合意したサービス継続レベルが維持されることを確実にするように設計された実行可能な計画を維持する。
l）供給者が、順守をレビューし、合意の要求事項を実施する責任を割り当てる。
m）供給者が適切な情報セキュリティレベルを維持していることを定期的に評価する。

5d-5.22.3　供給者関係を管理する責任は、指定された個人又はチームに割り当てる。

5d-5.22.4　合意書における要求事項、特に情報セキュリティに関する要求事項を満たしているかどうかを監視するために、十分な技術力及び人的資源を確保しておく。

5d-5.22.5　サービスの提供において不完全な点があった場合は、適切な処置をとる。

5d-5.23　クラウドサービスの利用における情報セキュリティ

管理策：クラウドサービスの調達、利用、管理及び利用終了のプロセスを、組織の情報セキュリティ要求事項に従って確立する。

目的：　クラウドサービスの利用における情報セキュリティを規定し、管理するため。

詳細管理策

5d-5.23.1　組織はクラウドサービスの利用に関するトピック固有の方針を確立し、全ての関連する利害関係者に伝達する。

5d-5.23.2　組織は、クラウドサービスの利用に伴う情報セキュリティリスクを管理する方法を定め、伝達する。

(5d-5.23.2参考)　これは、外部関係者が提供するサービスを、組織が管理する方法の既存の取組の拡張又はその一部である可能性がある。

(5d-5.23参考)　クラウドサービスの利用は、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間の、情報セキュリティに関する責任の共有及び分担、並びに共同作業を伴う可能性がある。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の責任を適切に定義し、実践することが不可欠である。

5d-5.23.3　組織は次の事項を定義する。
a）クラウドサービスの利用に伴う全ての関係する情報セキュリティ要求事項
b）クラウドサービスの選定基準及びクラウドサービス利用の範囲
c）クラウドサービスの利用及び管理に関する役割及び責任
d）どの情報セキュリティ管理策をクラウドサービスプロバイダが管理し、どの情報セキュリティ管理策をクラウドサービスカスタマとしての組織が管理するか。
e）クラウドサービスプロバイダが提供する情報セキュリティ機能を取得し、利用する方法
f）クラウドサービスプロバイダが実施する情報セキュリティ管理策に関して保証を得る方法
g）組織が複数のクラウドサービス、特に異なるクラウドサービスプロバイダのクラウドサービスを利用する場合に、管理策、インタフェース及びサービスの変更を管理する方法
h）クラウドサービスの利用に関連して発生する情報セキュリティインシデントを取り扱うための手順
i）情報セキュリティリスクを管理するため、クラウドサービスの継続的な利用を監視し、レビューし、評価する組織の取組
j）クラウドサービスの出口戦略を含め、クラウドサービスの利用を変更又は停止する方法

(5d-5.23参考)　クラウドサービスの合意は、多くの場合、事前に定義されており、交渉の余地はないことを踏まえ、全てのクラウドサービスについて、組織は、クラウドサービスプロバイダとのクラウドサービスの合意をレビューする。

5d-5.23.4　クラウドサービスの合意は、機密性、完全性、可用性及び情報の取扱いについての組織の要求事項、並びに、適切なクラウドサービスレベル目標及びクラウドサービスの定性的目標に言及する。

5d-5.23.5　組織は、クラウドサービスの利用に関連するリスクを特定するために、関連するリスクアセスメントも実施する。

5d-5.23.6　クラウドサービスの利用に関連する残留リスクは、組織の適切な管理層が明確に特定し、受容する。

5d-5.23.7　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間の合意は、組織のデータ及びサービスの可用性を保護するために次の規定を含む。
a）アーキテクチャ及びインフラストラクチャに関する業界で認められた標準に基づくソリューションを提供する。
b）組織の要求事項を満たすためにクラウドサービスのアクセス制御を管理する。
c）マルウェア監視及び保護ソリューションを実装する。
d）組織の取扱いに慎重を要する情報を、承認されている場所、又は特定の法域内若しくは特定の裁判権の下で処理し、保存する。
e）クラウドサービス環境で情報セキュリティインシデントが発生した場合に専用の支援を提供する。
f）クラウドサービスが、更に外部の供給者へ下請負契約されている場合に、組織の情報セキュリティ要求事項が満たされることを確実にする（又はクラウドサービスの下請負を禁止する。）。
g）異なる法域にわたるディジタル証拠に関する法令及び規制を考慮して、ディジタル証拠を収集する際に組織を支援する。
h）組織がクラウドサービスの利用を終了したいときに、適切な期間にわたって、適切な支援及びサービスを提供する。