15.2.1.3　供給者のサービスの監視及びレビューは、供給者の作成したサービスの報告をレビューし、合意で求めている定期的な進捗会議を設定することを含める。

15.2.1.4　供給者のサービスの監視及びレビューは、独立した監査人の報告書が入手できれば、供給者の作成したサービスの報告のレビューと併せて供給者の監査を実施し、特定された問題の追跡調査を行うことを含める。

15.2.1.5　供給者のサービスの監視及びレビューは、合意書並びに全ての附属の指針及び手順書の要求に従い、情報セキュリティインシデントの情報を提供し、その情報をレビューすることを含める。

15.2.1.6　供給者のサービスの監視及びレビューは、供給者の監査証跡、情報セキュリティ事象の記録、運用上の問題の記録、故障記録、障害履歴及び提供サービスに関連する中断記録をレビューすることを含める。

15.2.1.7　供給者のサービスの監視及びレビューは、特定された問題の解決及び管理を実施することを含める。

15.2.1.8　供給者のサービスの監視及びレビューは、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ことを含める。

15.2.1.9　供給者のサービスの監視及びレビューは、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とともに、供給者が十分なサービス提供能力を維持することを確実にすることを含める。

15.2.1.10　供給者関係を管理する責任は、指定された個人又はサービス管理チームに割り当てる。

15.2.1.11　組織は、供給者が、順守状況のレビュー及び合意書における要求事項の実施についての責任を割り当てる。

15.2.1.12　組織は、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する。

15.2.1.13　組織は、サービスの提供において不完全な点があった場合に適切な処置をとる。

15.2.1.14　組織は、供給者がアクセス、処理又は管理する、取扱いに慎重を要する又は重要な情報・情報処理設備に対して、全てのセキュリティの側面についての十分かつ包括的な管理及び可視性を維持する。

15.2.1.15　組織は、報告プロセスを規定することで、セキュリティに関連した活動（例えば、変更管理、ぜい弱性識別、情報セキュリティインシデントの報告及び対応）の可視性を維持する。

15.2.2　関連する業務情報、業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して、供給者によるサービス提供の変更（現行の情報セキュリティの方針群、手順及び管理策の保守及び改善を含む。）を管理する。

15.2.2.1　供給者のサービス提供の変更に対する管理は、供給者との合意に対する変更を考慮して実施する。

15.2.2.2　供給者のサービス提供の変更に対する管理は、以下の４点を実施するために組織が行う変更を考慮して実施する。

1．現在提供されているサービスの強化
2．新しいアプリケーション及びシステムの開発
3．組織の諸方針及び諸手順の、変更又は更新
4．情報セキュリティインシデントの解決及びセキュリティの改善のための、新たな又は変更した管理策

15.2.2.3　供給者のサービス提供の変更に対する管理は、以下の７点を実施するための供給者サービスにおける変更を考慮して実施する。

1．ネットワークに対する変更及び強化
2．新技術の利用
3．新製品又は新しい版・リリースの採用
4．新たな開発ツール及び開発環境
5．サービス設備の物理的設置場所の変更
6．供給者の変更
7．他の供給者への下請負契約

16　情報セキュリティインシデント管理

16.1　情報セキュリティインシデントの管理及びその改善

目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため

16.1.1　情報セキュリティインシデントに対する迅速、効果的かつ順序だった対応を確実にするために、管理層の責任及び手順を確立する。

16.1.1.1　情報セキュリティインシデント管理に関する管理層の責任及び手順について、組織において、以下の６点の手順が策定され、十分に伝達されることを確実にするために、管理層の責任を確立する。

1．インシデント対応の計画及び準備のための手順
2．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を監視、検知、分析及び報告するための手順
3．インシデント管理活動のログを取得するための手順
4．法的証拠を扱うための手順
5．情報セキュリティ事象の評価及び決定のための手順、並びに情報セキュリティ弱点の評価のための手順
6．対応手順（段階的取扱い、インシデントからの回復の管理、並びに内部及び外部の要員又は組織への伝達のための手順を含む。）

16.1.1.2　情報セキュリティインシデント管理に関する管理層の責任及び手順について、確立する手順においては、以下の３点を確実にする。

1．組織内の情報セキュリティインシデントに関連する事項は、力量のある要員が取り扱う。
2．セキュリティインシデントを検知及び報告する場合の連絡先を定める。
3．情報セキュリティインシデントに関連した事項を取り扱う関係当局、外部の利益団体又は会議との適切な連絡を保つ。

16.1.1.3　情報セキュリティインシデント管理に関する管理層の責任及び手順について、報告手順においては、以下の４点を含める。

1．情報セキュリティ事象が発生した場合に、報告作業を助け、報告する者が必要な全ての処置を忘れないよう手助けするための情報セキュリティ事象の報告書式の作成
2．情報セキュリティ事象が発生した場合にとる手順。例えば、詳細全て（不順守又は違反の形態、生じた誤動作、画面上の表示など。）の記録を直ちにとる、直ちに連絡先に報告し、協調した処置だけをとる。
3．セキュリティ違反を犯した従業員を処罰するために確立された正式な懲戒手続への言及
4．情報セキュリティ事象の報告者に、その件の処理が終結した後で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

16.1.1.4　情報セキュリティインシデント管理の目的について、経営陣の同意を得る。

16.1.1.5　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に対し、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確実に理解させる。