14.2.7.7　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、既知のぜい弱性が含まれないよう、十分な試験が実施されていることを示す証拠の提出を契約に含める。

14.2.7.8　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、預託契約に関する取決め（例えば、ソースコードが利用できなくなった場合）を契約に含める。

14.2.7.9　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、開発のプロセス及び管理策を監査するための契約上の権利を契約に含める。

14.2.7.10　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、成果物の作成に用いたビルド環境の有効な文書化を契約に含める。

14.2.7.11　システム開発を外部委託する場合には、組織の外部のサプライチェーン全体にわたり、適用される法令の順守及び管理の効率の検証については、組織が責任を負うことを契約に含める。

14.2.8　セキュリティ機能（functionality）の試験は、開発期間中に実施する。

14.2.8.1　組織内でシステムを新規に開発、更新するプロセスにおいては、詳細な活動計画及び一定範囲の条件下での入出力試験の準備を含めた綿密な試験及び検証は、最初に開発チームが実施する。

14.2.8.2　システムが期待どおりに、かつ、期待した形でだけ動作することを確実にするために、組織内で開発するもの及び外部委託したものの両方について、開発チームから独立した受入れ試験を実施する。

14.2.8.3　試験は、そのシステムの重要性及び性質に見合った程度で実施する。

14.2.9　新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立する。

14.2.9.1　システムの受入れ試験は、情報セキュリティ要求事項の試験及びセキュリティに配慮したシステム開発の慣行の順守を含める。

14.2.9.2　受け入れた構成部品及び統合されたシステムに対して、試験を実施する。

14.2.9.3　組織は、コード分析ツール又はぜい弱性スキャナのような自動化ツールを利用してセキュリティに関連する欠陥を修正した場合は、この修正を検証する。

14.2.9.4　試験は、システムが組織の環境にぜい弱性をもたらさないこと及び試験が信頼できるものであることを確実にするために、現実に即した試験環境で実施する。

14.3　試験データ

目的：試験に用いるデータの保護を確実にするため

14.3.1　試験データは、注意深く選定し、保護し、管理する。

14.3.1.1　ＰＩＩ又はその他の秘密情報を含んだ運用データは、試験目的に用いない。

14.3.1.2　ＰＩＩ又はその他の秘密情報を試験目的で用いる場合には、取扱いに慎重を要する詳細な記述及び内容の全てを、消去又は改変することによって保護する。

14.3.1.3　運用データを試験目的で用いる場合は、運用アプリケーションシステムに適用されるアクセス制御手順を、試験アプリケーションシステムにも適用する。

14.3.1.4　運用情報を試験環境にコピーする場合は、その都度認可を受ける。

14.3.1.5　運用データを試験目的で用いる場合は、運用情報は、試験が完了した後直ちに試験環境から消去する。

14.3.1.6　運用データを試験目的で用いる場合は、運用情報の複製及び利用は、監査証跡とするためにログを取得する。

15　供給者関係

15.1　供給者関係における情報セキュリティ

目的：供給者がアクセスできる組織の資産の保護を確実にするため

15.1.1　組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化する。

15.1.1.1　組織は、供給者による組織の情報へのアクセスに具体的に対処するため、方針において情報セキュリティ管理策を特定し、義務付ける。

15.1.1.2　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、組織が、自らの情報へのアクセスを許可する供給者の種類（例えば、ＩＴサービス、物流サービス、金融サービス、ＩＴ基盤の構成要素などの供給者）の特定及び文書化を含める。

15.1.1.3　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、供給者関係を管理するための標準化されたプロセス及びライフサイクルを含める。

15.1.1.4　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、様々な供給者に許可される情報へのアクセスの種類の定義、並びにそのアクセスの監視及び管理を含める。

15.1.1.5　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報の種類及びアクセスの種類ごとの最低限の情報セキュリティ要求事項で、組織の事業上のニーズ及び要求事項並びに組織のリスクプロファイルに基づく供給者との個々の合意の基礎となるものを含める。

15.1.1.6　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、それぞれの供給者及びアクセスに関して確立した情報セキュリティ要求事項が順守されているか否かを監視するためのプロセス及び手順（これには第三者のレビュー及び製品の妥当性確認も含まれる。）を含める。

15.1.1.7　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、各当事者が提供する情報又は情報処理の完全性を確実にするための、正確さ及び完全さの管理を含める。

15.1.1.8　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、組織の情報を保護するために供給者に適用する義務の種類を含める。

15.1.1.9　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、供給者によるアクセスに伴うインシデント及び不測の事態への対処（これには、組織及び供給者の責任も含める。）を含める。

15.1.1.10　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、各当事者が提供する情報又は情報処理の可用性を確実にするための、対応力に関する取決め、並びに必要な場合には、回復及び不測の事態に関する取決めを含める。

15.1.1.11　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、調達に関与する組織の要員を対象とした、適用される方針、プロセス及び手順についての意識向上訓練を含める。

15.1.1.12　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、供給者の要員とやり取りする組織の要員を対象とした、関与及び行動に関する適切な規則（これは、供給者の種類、並びに組織のシステム及び情報への供給者によるアクセスのレベルに基づく。）についての意識向上訓練を含める。

15.1.1.13　組織が実施する、並びに組織が供給者に対して実施を要求するプロセス及び手順には、情報セキュリティに関する要求事項及び管理策を、両当事者が署名する合意書の中に記載する条件を含める。