8d-8.29.2　セキュリティテストは、システム又は構成要素のテストに統合し、その一部とする。

8d-8.29.3　セキュリティテストは、機能的又は非機能的に表現することができる一連の要求事項に照らして実施する。

8d-8.29.4　セキュリティテストは、次の事項のテストを含む。
ａ）セキュリティ機能
ｂ）セキュリティに配慮したコーディング
ｃ）オペレーティングシステム、ファイアウォール及びその他のセキュリティ構成要素の構成を含む、セキュリティに配慮した構成

8d-8.29.5　セキュリティテスト計画は、一連の判定基準を使用して決定する。

8d-8.29.6　セキュリティテストの程度は、システムの重要性、性質及び導入する変更の潜在的影響に見合ったものにする。

8d-8.29.7　セキュリティテスト計画には次の事項を含める。
ａ）活動及びテストの詳細スケジュール
ｂ）一連の条件の下での入力及び予想される出力
ｃ）結果を評価する基準
ｄ）必要な場合、更なる処置の決定

8d-8.29.8　組織は、セキュリティに関係する欠陥の修正を検証する。

（8d-8.29.8参考）　検証には、コード分析ツール又はぜい弱性スキャナなどの自動化ツールを利用することができる。

8d-8.29.9　組織内で開発するソフトウェアについてのセキュリティテストは、次の順に行う。
ａ）最初に開発チームが実施する。
ｂ）その次に、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、独立した受入れテストを実施する。

8d-8.29.10　セキュリティのテストにおいて、次の事項を考慮する。
ａ）セキュリティの欠陥のテストに関連して、予期しない入力及び条件を含め、コードのレビュー活動を実施する。
ｂ）セキュリティに配慮していない構成及びシステムのぜい弱性を特定するために、ぜい弱性スキャンを実施する。
ｃ）セキュリティに配慮していないコード及び設計を特定するために、侵入テストを実施する。

8d-8.29.11　外部委託した開発、及び購入した構成要素については、取得プロセスに従う。

8d-8.29.12　供給者との契約では、特定したセキュリティ要求事項に言及する。

8d-8.29.13　外部から調達する製品及びサービスは、取得前に供給者との契約で特定したセキュリティ要求事項に基づく判定基準に照らして評価する。

8d-8.29.14　セキュリティテストは、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テストが信頼できるものであることを確実にするために、対象の本番環境に可能な限り一致するテスト環境で実施する。

8d-8.30　外部委託による開発

管理策：組織は、外部委託したシステム開発に関する活動を指揮し、監視し、レビューする。

目的：　組織が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため。

詳細管理策

8d-8.30.1　システム開発を外部委託する場合には、次の事項を行う。
ａ）要求事項及び期待を伝達する。
ｂ）要求事項を満たし、期待に応えることを合意する。
ｃ）外部委託から提供された作業及び成果物がこの期待を満たすかどうかを継続的に監視する。
ｄ）開発されたシステムをレビューする。

8d-8.30.2　組織の外部のサプライチェーン全体にわたり、次の事項を考慮する。
ａ）外部委託した内容に関する使用許諾の合意、コードの帰属及び知的財産権
ｂ）セキュリティに配慮した設計、コーディング及びテストの実施についての契約上の要求事項
ｃ）外部の開発者が考慮すべき脅威モデルの提供
ｄ）成果物の質及び正確さに関する受入れテスト
ｅ）受け入れられる最低限のセキュリティ及びプライバシー機能を実現していることを示す証拠の提出
ｆ）引渡しに当たって、悪意のある内容（意図的なもの及び意図しないもの）の存在を防ぐために、十分なテストを実施していることを示す証拠の提出
ｇ）既知のぜい弱性が含まれないよう、十分なテストを実施していることを示す証拠の提出
ｈ）ソフトウェアソースコードの預託契約
ｉ）開発のプロセス及び管理策を監査する、契約に基づく権利
ｊ）開発環境のセキュリティ要求事項
ｋ）適用される法令の考慮

8d-8.31　開発環境、テスト環境及び本番環境の分離

管理策：開発環境、テスト環境及び本番環境は、分離してセキュリティを保つ。

目的：　開発活動及びテスト活動による危険から本番環境及びそのデータを保護するため。

詳細管理策

8d-8.31.1　本番環境における問題を防ぐために必要な、本番環境、テスト環境及び開発環境の間の分離レベルを特定し、それに従って分離する。

8d-8.31.2　開発環境、テスト環境及び本番環境の分離をする際には、特に、次の事項を考慮する。
ａ）開発システムと本番システムとを適切に分離し、それらを異なる領域で運用する。
ｂ）開発段階から本番段階へのソフトウェアの導入に関する規則及び認可を、明確に定め、文書化し、実施する。
ｃ）本番システム及びアプリケーションに対する変更は、本番システムに適用する前に、テスト環境又はステージング環境でテストする。
ｄ）特定し、承認された状況を除いて、本番環境ではテストを行わない。
ｅ）コンパイラ、エディタ、及びその他の開発ツール又はユーティリティプログラムは、必要がないときには、本番システムからアクセス可能としない。