8d-8.28.2　最低限のセキュリティに配慮したコーディングのベースラインを確立し、適用する。

8d-8.28.3　セキュリティに配慮したコーディングのためのプロセス及びガバナンスを、第三者から入手したソフトウェア構成要素及びオープンソースソフトウェアも対象とするように拡張する。

8d-8.28.4　組織は、組織のセキュリティに配慮したコーディングの原則を下記により方向付ける。

a）現実世界の脅威、並びにソフトウェアのぜい弱性に関する最新の助言及び情報を監視する

b）組織のセキュリティに配慮したコーディングの原則を継続的に改善する

c）組織のセキュリティに配慮したコーディングの原則に従うための学習を要員に施す

（8d-8.28.4参考）　これは、急速に変化する脅威の状況に対抗するために、効果的なセキュリティに配慮したコーディング慣行の実施を確実にするのに役立ち得る。

【計画及びコーディング前】

8d-8.28.5　セキュリティに配慮したコーディングの原則を、新規の開発及び再利用の両方で使用する。

8d-8.28.6　セキュリティに配慮したコーディングの原則は、組織内の開発活動並びに組織が他者に提供する製品及びサービスの両方に適用する。

8d-8.28.7　コーディング前の計画及び前提条件は、次の事項を含む。

a）組織内及び外部委託のコード開発の両方に使用する、セキュリティに配慮したコーディングに関する組織固有の期待及び広く認められた原則

b）情報セキュリティのぜい弱性につながる一般的及び歴史的なコーディング慣行及び欠陥

c）セキュリティに配慮したコードの作成を実施させるために、統合開発環境（ＩＤＥ）などの開発ツールを構成する。

d）該当する場合には、開発ツール及び実行環境の提供者が示す手引に従う。

e）更新された開発ツールの維持及び使用

f）セキュリティに配慮したコードを作成する際の開発者の資格

g）脅威モデリングを含むセキュリティに配慮した設計及びアーキテクチャ

h）セキュリティに配慮したコーディング標準、及び関係する場合はその使用を義務付けること

i）開発のための管理された環境の使用

【コーディング中】

8d-8.28.8　コーディング中の考慮事項は、次の事項を含む。

a）使用するプログラム言語及び手法に特有の、セキュリティに配慮したコーディング慣行

b）ペアプログラミング、リファクタリング、ピアレビュー、セキュリティイテレーション、テスト駆動開発など、セキュリティに配慮したプログラミング手法を使用する。

c）構造化プログラミング手法を使用する。

d）コードを文書化し、情報セキュリティのぜい弱性の悪用を許す可能性のあるプログラミングの欠陥を除去する。

e）セキュリティに配慮しない設計手法の使用を禁止する。

8d-8.28.9　セキュリティに配慮して作成するソフトウェアのテストは開発中及び開発後に実施する。

（8d-8.28.9参考）　静的アプリケーションセキュリティテスト（ＳＡＳＴ）プロセスで、ソフトウェアのセキュリティのぜい弱性を特定することが可能である。

8d-8.28.10　ソフトウェアの運用を開始する前に、次の事項を評価する。

a）攻撃対象領域（attack surface）及び最小特権の原則

b）最も一般的なプログラミングエラーの分析を実行し、これらが低減されたことを文書化する。

【レビュー及び保守】

8d-8.28.11　コードの運用が開始された後、次のことを行う。

a）更新はセキュリティに配慮してパッケージ化し、適用する。

b）報告された情報セキュリティのぜい弱性に対処する。

c）エラー及び攻撃の疑いのログを取得し、必要に応じてコードを調整するためにログを定期的にレビューする。

d）ソースコードを、認可されていないアクセス及び改ざんから保護する。

8d-8.28.12　外部ツール及びライブラリを使用する場合、組織は次の事項を考慮する。

a）外部ライブラリを管理し、リリースサイクルに合わせて規則正しく更新することを確実にする。

b）十分に検査された構成要素、特に認証及び暗号化の構成要素の選択、認可及び再利用

c）外部の構成要素の使用許諾、セキュリティ及び履歴

d）ソフトウェアが保守可能で、追跡することができ、実証された定評のある供給元に由来することを確実にする。

e）開発資源及び成果物の十分に長期的な可用性

8d-8.28.13　ソフトウェアパッケージを変更する必要がある場合、次のことを考慮する。

a）組み込まれた管理策及び完全性プロセスが危険にさらされるリスク

b）業者の同意を得るかどうか。

c）標準のプログラム更新として業者から必要な変更を得る可能性

d）変更の結果として、将来、組織がソフトウェアの保守に責任を負うようになった場合の影響

e）使用中の他のソフトウェアとの互換性

8d-8.29　開発及び受入れにおけるセキュリティテスト

管理策：セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施する。

目的：　アプリケーション又はコードを本番環境に導入するときに、情報セキュリティ要求事項が満たされているかどうかの妥当性確認をするため。

詳細管理策

8d-8.29.1　新規の情報システム、アップグレード及び新しい版は、開発プロセスにおいて綿密に試験し、検証する。