8d　情報システム開発／導入の管理

8d-8.25　セキュリティに配慮した開発のライフサイクル

管理策：ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用する。

目的：　情報セキュリティを、ソフトウェア及びシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため。

詳細管理策

(8d-8.25参考)　セキュリティに配慮したサービス、アーキテクチャ、ソフトウェア及びシステムを構築するには、セキュリティに配慮した開発が必要となる。

8d-8.25.1　セキュリティに配慮した開発を達成するために、次の側面を考慮する。

a）開発環境、テスト環境及び本番環境の分離

b）ソフトウェア開発のライフサイクルにおける、次に関わるセキュリティに関する手引

1）ソフトウェア開発の方法論におけるセキュリティ

2）用いる各プログラム言語について定めた、セキュリティに配慮したコーディングに関する指針

c）仕様策定及び設計段階におけるセキュリティ要求事項

d）プロジェクトにおけるセキュリティの確認項目

e）回帰テスト、コードスキャン、侵入テストなどのシステム及びセキュリティのテスト

f）ソースコード及び構成ファイルのためのセキュリティが保たれたリポジトリ

g）版の管理におけるセキュリティ

h）アプリケーションセキュリティに関して必要な知識及び訓練

i）ぜい弱性を防止し、発見し、修正するに当たっての開発者の能力

j）ライセンスに関する将来の問題を回避しつつ、費用対効果の高いソリューションを確実にするための、ライセンスの要求事項及び代替案

8d-8.25.2　開発を外部委託した場合、組織は、供給者がセキュリティに配慮した開発のための組織の規則を順守していることの保証を得る。

8d-8.26　アプリケーションセキュリティの要求事項

管理策：アプリケーションを開発又は取得する場合、情報セキュリティ要求事項を特定し、規定し、承認する。

目的：　アプリケーションを開発又は取得する場合、全ての情報セキュリティ要求事項を特定し、対応することを確実にするため。

詳細管理策

【アプリケーションセキュリティの要求事項全般】

8d-8.26.1　アプリケーションセキュリティの要求事項をリスクアセスメントを通じて特定し、規定する。

8d-8.26.2　アプリケーションセキュリティの要求事項は、情報セキュリティの専門家の支援を受けて作成することを考慮する。

(8d-8.26.2参考)　アプリケーションセキュリティの要求事項は、アプリケーションの目的に応じて、幅広いトピックにわたることがある。

8d-8.26.3　アプリケーションセキュリティの要求事項には、該当する場合には、次の事項を含める。

a）エンティティの識別情報の信頼のレベル

b）アプリケーションで処理する情報の種類及び分類レベルの特定

c）アプリケーション内のデータ及び機能へのアクセス及びアクセスのレベルを分離することの必要性

d）悪意のある攻撃又は意図しない事業の中断・阻害に対するレジリエンス

e）トランザクションが生成、処理、完結又は保管される法域における法令及び規制上の要求事項

f）関与する全ての当事者のプライバシーの必要性

g）秘密情報の保護に関する要求事項

h）処理、転送及び保持するデータの保護

i）関与する全ての当事者間の通信をセキュリティを保って暗号化する必要性

j）完全性の確認及び入力の妥当性確認を含む入力の管理策

k）自動化した管理策

l）出力にアクセスできる人及びその認可も考慮した出力の管理策

m）“自由記述”欄の内容に関する制限、これは、機密データを管理されずに保存することにつながり得るため。

n）トランザクションのログ取得及び監視、否認防止の要求事項など、業務プロセスに由来する要求事項

o）他のセキュリティ管理策によって必要となる要求事項

p）エラーメッセージの取扱い

【トランザクションサービス】

8d-8.26.4　組織とパートナーとの間でのトランザクションサービスを提供するアプリケーションの場合、情報セキュリティ要求事項を特定する際には、次の事項を考慮する。

a）各当事者が提示する自らの識別情報について、それぞれが互いに要求し合う信頼のレベル

b）交換又は処理する情報の完全性に必要な信頼のレベル、及び完全性の欠如を特定するための仕組み

c）重要な取引文書の内容の承認、その発行、又はその文書への署名を誰が行えるかについての認可プロセス

d）重要な文書の機密性、完全性及び発送・受領の証明、並びに否認防止

e）トランザクションの機密性及び完全性

f）トランザクションの機密性を維持する期間に関する要求事項

g）保険及びその他の契約上の要求事項

【電子注文及び支払いアプリケーション】

8d-8.26.5　電子注文及び支払いを伴うアプリケーションの場合、次の事項を考慮する。

a）注文情報の機密性及び完全性を維持するための要求事項

b）顧客から提供された支払い情報を検証するための、適切な検査の度合い