14.1.3.5　アプリケーションサービスのトランザクションでは、その詳細情報を、公開している環境の外（例えば、組織のイントラネット内に設置しているデータ保存環境）で保管すること、及びインターネットから直接アクセス可能な記憶媒体上にそれらを保持して危険にさらさないことを確実にする仕組みを整備する。

14.1.3.6　アプリケーションサービスのトランザクションでは、信頼できる専門機関を利用（例えば、ディジタル署名又はディジタル証明書の発行・維持の目的での利用）する場合、エンドツーエンドの証明書及び／又は署名管理プロセスを通じたセキュリティを統合し、組み込む。

14.2　開発及びサポートプロセスにおけるセキュリティ

目的：情報システムの開発サイクルの中で情報セキュリティを設計し、実施することを確実にするため

14.2.1　ソフトウェア及びシステムの開発のための規則は、組織内において確立し、開発に対して適用する。

14.2.1.1　セキュリティに配慮した開発のための方針には、開発環境のセキュリティを含める。

14.2.1.2　セキュリティに配慮した開発のための方針には、ソフトウェア開発のライフサイクルにおける、以下の２点の手引きを含める。

１．ソフトウェア開発の方法論におけるセキュリティ

２．用いる各プログラミング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

14.2.1.3　セキュリティに配慮した開発のための方針には、設計段階におけるセキュリティ要求事項を含める。

14.2.1.4　セキュリティに配慮した開発のための方針には、プロジェクトの開発の節目ごとにおけるセキュリティの確認項目を含める。

14.2.1.5　セキュリティに配慮した開発のための方針には、セキュリティが保たれたリポジトリを含める。

14.2.1.6　セキュリティに配慮した開発のための方針には、版の管理におけるセキュリティを含める。

14.2.1.7　セキュリティに配慮した開発のための方針には、アプリケーションのセキュリティに関して必要な知識を含める。

14.2.1.8　セキュリティに配慮した開発のための方針には、ぜい弱性を回避、発見及び修正するに当たっての開発者の能力を含める。

14.2.1.9　開発に適用される標準類が知られていない可能性がある場合、又は現行の最適な慣行に整合していなかった場合には、新規開発する場合及びコードを再利用する場合の両方に、セキュアプログラミング技術を用いる。

14.2.1.10　セキュリティに配慮したコーディングに関する標準類を確認し、その使用を義務付ける。

14.2.1.11　開発者は、開発に適用する標準類の使用及び試験について訓練を受け、また、コードレビューによって標準類の使用を検証する。

14.2.1.12　開発を外部委託した場合、組織は、その外部関係者がセキュリティに配慮した開発のための規則を順守していることの保証を得る。

14.2.2　開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理する。

14.2.2.1　初期設計段階からその後の全ての保守業務に至るまで、システム、アプリケーション及び製品の完全性を確実にするため、正式な変更管理手順を文書化し、実施する。

14.2.2.2　新しいシステムの導入及び既存システムに対する重要な変更は、文書化、仕様化、試験、品質管理及び管理された実装からなる正式な手続に従う。

14.2.2.3　新しいシステムの導入及び既存システムに対する重要な変更の際の手続には、リスクアセスメント、変更の影響分析及び必要なセキュリティ管理策の仕様化を含める。

14.2.2.4　新しいシステムの導入及び既存システムに対する重要な変更の際の手続は、既存のセキュリティ及び管理手順が損なわれないこと、サポートプログラマによるシステムへのアクセスはその作業に必要な部分に限定されること、並びにいかなる変更に対しても正式な合意及び承認が得られていることを確実にする仕組みを整備する。

14.2.2.5　変更管理手順には、実施可能な範囲でアプリケーション及びその運用に関する変更管理手順を統合する。

14.2.2.6　変更管理手順には、合意された認可レベルの記録を維持することを含める。

14.2.2.7　変更管理手順には、変更は、認可されている利用者によって提出されることを確実にすることを含める。

14.2.2.8　変更管理手順には、変更によって管理策及び完全性に関する手順が損なわれないことを確実にするために、管理策及び手順をレビューすることを含める。

14.2.2.9　変更管理手順には、修正を必要とする全てのソフトウェア、情報、データベース及びハードウェアを特定することを含める。

14.2.2.10　変更管理手順には、セキュリティ上の既知の弱点を最少化するために、セキュリティが特に重要とされるコードを特定し、これを点検することを含める。

14.2.2.11　変更管理手順には、作業を開始する前に、提案の詳細について正式な承認を得ることを含める。

14.2.2.12　変更管理手順には、変更を実施する前に、認可されている利用者がその変更を受け入れることを確実にすることを含める。

14.2.2.13　変更管理手順には、システムに関する一式の文書が各変更の完了時点で更新されること、及び古い文書類は記録・保管されるか又は処分されることを確実にすることを含める。

14.2.2.14　変更管理手順には、全てのソフトウェアの更新について、版数の管理を維持することを含める。

14.2.2.15　変更管理手順には、全ての変更要求の監査証跡を維持・管理することを含める。

14.2.2.16　変更管理手順には、操作手順書などの運用文書類及び利用者手順が、適切な状態であるように、必要に応じて変更することを確実にすることを含める。

14.2.2.17　変更管理手順には、変更の実施は最も適切な時期に行い、関係する業務処理を妨げないことを確実にすることを含める。

14.2.3　オペレーティングプラットフォームを変更するときは、組織の運用又はセキュリティに悪影響がないことを確実にするために、重要なアプリケーションをレビューし、試験する。

14.2.3.1　オペレーティングプラットフォームの変更によって、アプリケーションの機能及び処理の完全性が損なわれていないことを確実にするために、これらに関係する手続きをレビューする。

14.2.3.2　オペレーティングプラットフォームの変更の実施前に適切な試験及びレビューを行っても間に合うように、オペレーティングプラットフォームの変更を通知することを確実にする仕組みを整備する。

14.2.3.3　事業継続計画に対して、適切な変更がなされることを確実にする仕組みを整備する。

14.2.4　パッケージソフトウェアの変更は、抑止し、必要な変更だけに限る。また、全ての変更は、厳重に管理する。

14.2.4.1　可能な限り、そして実行可能な場合には、業者が供給するパッケージソフトウェアは、変更しないで用いる。

14.2.4.2　パッケージソフトウェアの変更が必要な場合は、組み込まれている機能及び処理の完全性が損なわれるリスクへの対応を行う。