日本ユニシスにおける顧客情報システム開発のセキュリティ対策

Security Measures for Customer Information Systems Development in Nihon Unisys

山　口　　繁

要　約　社会では情報システムのセキュリティ事件および事故が後を絶たず，しかも年々増加する傾向にある．日本ユニシスの開発するシステムにおいてもセキュリティに関して十分な品質の維持を怠ると，セキュリティ事件および事故により金銭的，労力的損失を被るだけではなく，顧客に多大な迷惑をかけることになり，IT サービス企業として信用失墜の大問題につながる危険に晒されている．

日本ユニシスでは，顧客情報システム開発における管理標準「ISBP（Information Services Business Process）」を定め，開発業務に適用し，品質向上を目指している．

ところが，2001 年に日本ユニシスが開発した Web アプリケーションにセキュリティの脆弱性があることを外部から指摘され，大きな衝撃を受けた．これを契機に開発システムのセキュリティ品質向上策として「システム開発セキュリティプロセス」を定め，開発業務に適用し，一層のシステム品質向上を目指している．

システム開発セキュリティプロセスでは，基盤システム，アプリケーションシステムに対する技術的セキュリティ対策および開発環境における人的，物理的，制度的情報セキュリティ対策を定めており，開発業務の立上げから終結までの全過程に適用している．また，開発システムの技術的セキュリティ対策の必要十分性と開発作業中の情報セキュリティの管理状況についてレビューの実施を規定し，開発業務のセキュリティ品質の維持，向上を図っている．

Abstract　The security problems of information systems have kept rising for several years, getting attention as social issues. If the application system that Nihon Unisys has developed does not ensure sufficient level of security, it would cause serious security problems and damage to our reputation as an IT service company.

Nihon Unisys defined ISBP (Information Service Business Process), our management standard for customers' information systems development, and applied it to our development activities, attempting the improved quality of security.

In 2001, however, a specialized agency pointed out the security vulnerability in the Web application systems that Nihon Unisys developed. This triggered us to define Systems Development Security Process as security improvement measures and apply it to our systems development projects.

System Development Security Process defines our technical security measures for infrastructure/application systems and human-physical-institutional security measures for development environment, which have been applied to entire development phases from starting-up through release. It also mandates the review of requirements/sufficiency in technical security measures of developed system, and the status of information security management of the system under development, aiming at the maintenance and improvement of security quality of development project.

1. はじめに

近年情報システム，特にWeb系システムのセキュリティ脆弱性に対する攻撃は増加しており，個人情報漏洩等の事件および事故も多く発覚し，社会問題化している．受託開発したシステムやソリューションシステムで，いったんセキュリティ事故が発生した場合，リカバリコスト等の直接的損失を被る顧客に多大な迷惑をかけることになる．ITサービス企業としての信頼性失墜により被る会社の損失も計り知れない．

日本ユニシスでは，顧客情報システム開発において，管理標準「ISBP（Information Services Business Process）」を定め，開発業務に適用し，品質向上を目指している．セキュリティ品質も開発システムの重要な品質要素と捉え，「システム開発セキュリティプロセス」を定め，システムの品質向上を目指している．

本稿では，基盤システム，アプリケーションシステムに対する技術的セキュリティ対策および開発環境における人的，物理的，制度的情報セキュリティ対策を定めた「システム開発セキュリティプロセス」の規定と適用について紹介する．

2. セキュリティプロセスの策定

2001年，日本ユニシスが開発したWebアプリケーションにセキュリティの脆弱性があることを外部から指摘され，大きな衝撃を受けた．これを契機に，需要増加が見込まれるWebシステムのセキュリティ品質の改善を図るために，「開発システムセキュリティプロセス」を策定し，2002年から開発プロジェクトへの適用を開始した．この開発システムセキュリティプロセスでは，セキュリティ管理プロセスを明確にするとともに，基盤システムとWebアプリケーションの技術的セキュリティ対策ガイドを作成し，開発担当部門向けに具体的で役立つ技術情報を提供した．

同じ時期，日本ユニシスでは全社共通の情報セキュリティ管理策として，第一次情報セキュリティ総合戦略が策定された．これを受けて開発業務に特化した情報セキュリティ管理策として，ISMS[*1]に準拠した「開発環境セキュリティプロセス」を策定した．

この開発環境セキュリティプロセスと開発システムセキュリティプロセスを統合し，「システム開発セキュリティプロセス」と改め，2005年から受託システム，ソフトウェア商品および社内システムの開発業務へ適用している．

また，システム職全体のセキュリティスキルの底上げを図るため，開発業務経験度に合わせたセキュリティ教育コースを設け，研修受講を推し進めている．

3. システム開発セキュリティプロセス

システム開発セキュリティプロセスは，日本ユニシス内の開発プロジェクトがセキュリティに対する問題意識を高め，セキュリティ脅威とリスクを洗い出し，セキュリティ対策を実施するために作られており，次のことを目的としている．

- 開発システムセキュリティ
  開発システムで扱う情報資産をセキュリティ脅威から保護するセキュアな情報システムを開発し，顧客に提供する．

- 開発環境セキュリティ
  セキュリティ上安全な環境で開発業務を実施し，開発で扱う顧客機密情報，開発成果物等の情報資産を安全に管理する．

このようにセキュリティを確保するべき範囲は，開発システムと開発環境の二つである．開発システムは更に基盤システムと，アプリケーションシステムに分かれる．

1）開発システムセキュリティプロセス

ⅰ）基盤システムセキュリティ

基盤システム構築では，システムの構成上のセキュリティ脆弱性を持たないように設計・構築することが重要である．基盤システム構築のセキュリティでは，ファイアーウォールや侵入検知システム（ISD）等のセキュリティ機器の組み込み，ネットワーク，サーバシステムのセキュリティ設定，OS や基本ソフトウェアへのセキュリティパッチ適用等のセキュリティ機能構築を行う．

ⅱ）アプリケーションシステムセキュリティ

アプリケーション開発では，意図しない利用方法や不正アクセス等に対し，セキュリティ脆弱性を持たないように設計し，プログラミングすることが重要である．アプリケーション開発のセキュリティでは，アプリケーション利用者の認証や機密データの暗号化，アクセスログ取得等のセキュリティ機能開発を行う．

開発システムセキュリティプロセスでは，各開発工程で実施すべきセキュリティ機能開発とその開発状況を確認するレビューの実施をプロセスとして定めている．

2）開発環境セキュリティプロセス

開発環境では，個人情報を含む顧客機密情報や設計書などの開発成果物，テストデータなど，開発作業で作成あるいは利用する情報を機密度に応じて安全に取り扱う（保管・移送・提供・消去）必要がある．システム開発の作業場所は，自社，客先，協力会社など多様である．これら開発環境における情報セキュリティ管理の実施と管理状況を確認するレビューの実施をプロセスとして制定している．

3.1　体制と役割

システムを開発する開発プロジェクトの役割に加えて，システム開発セキュリティプロセスを全社的に推進する役割をシステム開発セキュリティオフィスとセキュリティ技術主管部が担い，開発プロジェクトのセキュリティ機能開発を支援する．図１にシステム開発セキュリティプロセスの実施体制を示す．

1）開発プロジェクト

・開発システムのセキュリティレベル設定
  プロジェクトマネージャは，開発するシステムについて，顧客要求や取り扱う情報の機密度とシステム利用環境等を勘案して，セキュリティレベル（高・中・低）を設定する．

・セキュリティ機能開発
セキュリティレベルに応じたアプリケーションシステムのセキュリティ機能開発および基盤システムのセキュリティ構築を行う.
・情報セキュリティ管理の実施
プロジェクト内セキュリティ管理者が中心となって，情報セキュリティプロシージャの順守と情報セキュリティ管理を行う.
・セキュリティレビューの実施
セキュリティレベル「高」の案件は第三者セキュリティレビューを受ける.
セキュリティレベル「中」あるいは「低」の案件については，プロジェクト内でセキュリティレビューを行う.

2） システム開発セキュリティオフィス
・セキュリティプロセスの主管
セキュリティに関するプロセスの社内規程および運用ルールの策定と開発環境セキュリティ管理基準策定を行う.
・大/中規模開発プロジェクトのセキュリティレベル判定
プロジェクトが設定したセキュリティレベルの合理性，妥当性を客観的に評価し判定する.
・第三者セキュリティレビューの事務局
・社外セキュリティ情報の収集と社内向け情報発信

3） セキュリティ技術主管部
・開発者向け技術資料の提供
セキュリティ対策ガイド（基盤/アプリケーション）の発行とセキュリティ要件定義作成ガイドの提供.

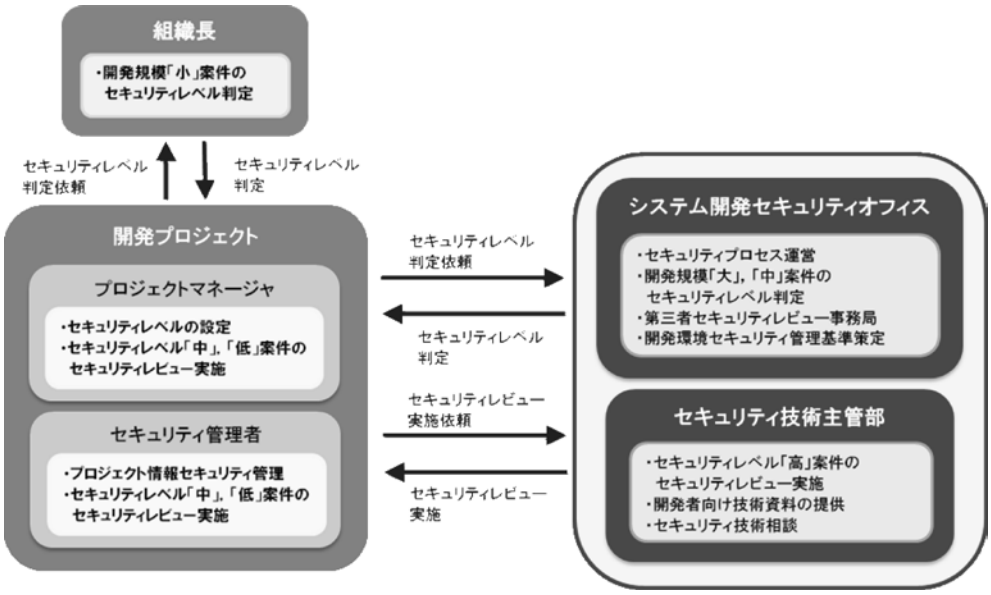

図1　システム開発セキュリティプロセスの実施体制

・第三者セキュリティレビューの実施
セキュリティレベルが「高」の案件について，第三者の立場でセキュリティレビューを実施する．
・技術相談による個別プロジェクトへの直接支援

4)　開発プロジェクトの組織長
・小規模開発プロジェクトのセキュリティレベル判定

3.2　セキュリティプロセスの流れ

日本ユニシスの管理標準である ISBP では，「提案時」，「立ち上げ時」，「開発実行時」の三つのフェーズがある．システム開発セキュリティプロセスでも，ISBP の「提案時」，「立ち上げ時」，「開発実行時」の三つのフェーズと連携して，プロセスを定義している．図 2 にシステム開発セキュリティプロセスの流れを示す．

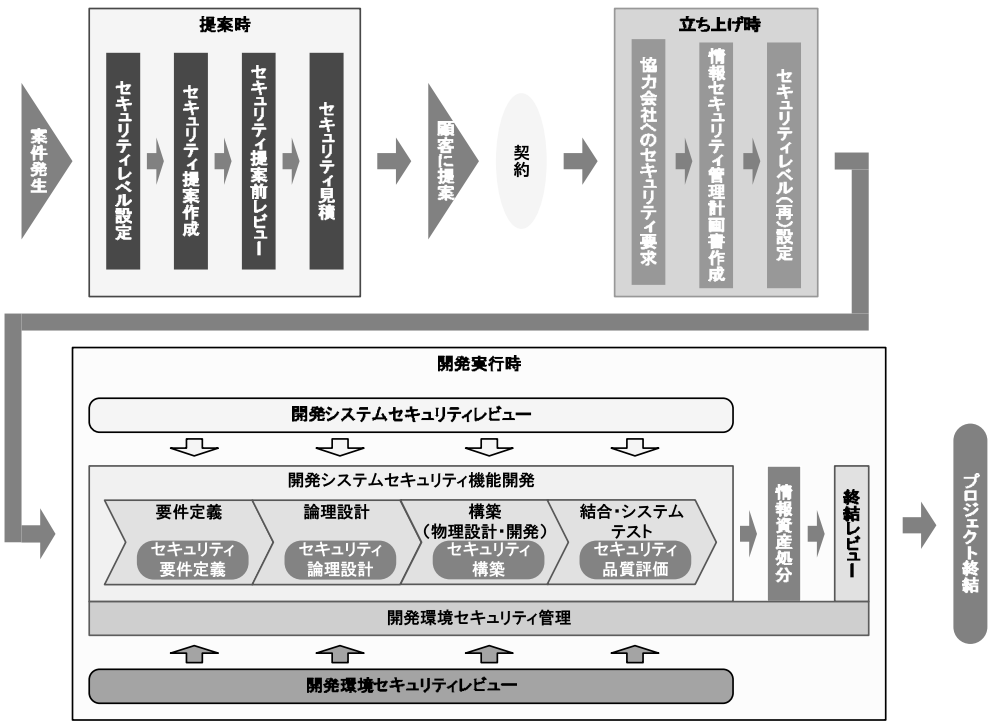

図 2　システム開発セキュリティプロセスの流れ

3.2.1　開発システムセキュリティレベルの設定

情報システムの提案，開発に先立ち，どの程度のセキュリティ提案，セキュリティ機能開発をするべきかの目安とするために，顧客のセキュリティ要求度合，開発システムで取り扱う情報の機密度を基にセキュリティレベルを設定する．機密度の「高」「中」「低」をそのままセキュリティレベル「高」「中」「低」としている．表 1 にセキュリティレベル設定基準を示すが，小規模なシステム開発であっても，セキュリティ対策の重要性を意識した開発を行うことができる．セキュリティレベルの設定手順を以下に示す．

1） プロジェクトマネージャが，開発システムの情報機密度「高・中・低」を判断する
2） プロジェクトマネージャが，セキュリティレベル設定基準を基にセキュリティレベルを設定する
3） 設定したレベルについて，第三者にレベルの妥当性の判定を受ける

表1　セキュリティレベル設定基準

セキュリティレベル		適用基準	取り扱う情報の例
高	開発するシステムのセキュリティ不備が，社会問題，顧客の損失かつ会社全体の信用失墜に繋がる恐れがある案件	情報機密度「高」の情報を扱うシステム	・企業にとって経営，信用に関わる極めて重要な情報（基幹システム情報） ・機微な個人情報 ・サイバーテロの対象となりうる情報（社会インフラ，公的機関，放送新聞，金融関連の基幹システムで扱う情報） ・国家的機密情報（政府，省庁，自治体等で扱う情報）
中	開発するシステムのセキュリティ不備が，会社の責任問題になる案件	情報機密度「中」の情報を扱うシステム	・ビジネス（オンラインショップ等）情報 ・一般企業のBtoB，BtoCで扱う情報 ・機微以外の個人情報
低	開発するシステムのセキュリティ不備が，会社の責任問題にはならないが，基本的なセキュリティの考慮を行う必要がある案件	情報機密度「低」の情報を扱うシステム	・不特定多数，特定多数に公開できる情報 ・一般的なWeb発信情報

ここで設定したレベルについては，判定を受けなければならない．判定依頼先は，客観性を保つために開発規模によって異なってくる．大・中規模開発案件ならシステム開発セキュリティオフィスに，小規模案件なら開発プロジェクトの組織長に対して判定依頼を行い，判定を受ける．

セキュリティレベルの設定は原則として提案作成時に行うが，開発プロジェクト立ち上げ時に開発システムのセキュリティ要件の再確認を行い，提案時に設定したセキュリティレベルとレベルが異なる場合は，再設定を行う．

3.2.2　セキュリティ提案

顧客のRFP（提案依頼書）を受けて，これに応えるセキュリティ提案を行う．RFPにはセキュリティ要件が示されていないこともあるが，開発システムが取り扱うデータや利用環境等の特性からセキュリティ対応の必要性と重要性を考慮し，セキュリティ提案を作成する．

3.2.3　セキュリティ見積

セキュリティ見積では，以下に示すセキュリティ対策費用の見積りを行い，開発費用の見積りに反映する．また，セキュリティ対策漏れや開発中のセキュリティ事故等，今後開発中に起こりうるリスクも考慮する．

1） 基盤システム対策費用見積

セキュリティ機器（ファイアーウォール，IDS等）の導入・設計・テスト費用等

2）　アプリケーションシステム対策費用見積
セキュリティ機能要件（認証方式，アクセス制御，暗号化等）の設計・実装・テスト工数等
3）　開発環境セキュリティ対策費用
特別なセキュリティ設備を要求された場合の開発施設や入退室管理設備，施錠機器等の費用

3.2.4　協力会社へのセキュリティ要求

プロジェクト立ち上げ時の重要な作業は開発体制作りである．特にITスキルの高い協力会社を選定し，開発パートナーとしなければならない．協力会社選定時には，協力会社に対してSOW（作業範囲記述書）を提示する．このSOWに情報セキュリティ管理要求と委託開発システムのセキュリティ機能要件を記載して協力会社へのセキュリティ要求とし，通常の開発プロセスの中で情報セキュリティ管理要求とセキュリティ機能要件が満たされているかを確認する．

3.2.5　情報セキュリティ管理計画書作成

プロジェクト立ち上げ時に「プロジェクト管理計画書」を作成するが，その中に情報セキュリティ管理計画についても記述する．「情報セキュリティ管理計画書」は，プロジェクト管理計画書のセキュリティ部分の詳細編であり，以下の事項を記載する．

1）　情報セキュリティ管理の基本事項
秘密義務の厳守，開発環境セキュリティ管理，顧客機密情報保護，成果物・中間成果物の管理，開発システムセキュリティ機能開発管理について記載する．
2）　適用範囲と対象者
管理基準の適用範囲（対象プロジェクト，開発場所）と対象者を定義する．
3）　管理責任者と管理者/担当者
プロジェクトにおける情報セキュリティ全体の責任者，開発環境セキュリティ管理の責任者および担当者とそれぞれの役割について記載する．
4）　教育計画
プロジェクト要員に対する情報セキュリティ管理の方針と実施手順についての教育計画を記載する．
5）　レビューの計画
情報セキュリティ管理計画の順守状況のレビュー，開発システムセキュリティレビュー，開発環境セキュリティレビューの実施計画について記載する．

3.2.6　開発システムセキュリティ機能開発

ISBPでシステム開発の標準フェーズとして定義している「要件定義」「論理設計」「構築（物理設計・プログラム開発）」「結合・システムテスト」の各フェーズと連携し，「セキュリティ要件定義」「セキュリティ論理設計」「セキュリティ構築」「セキュリティ品質評価」をすること，これが開発システムセキュリティ機能開発である．表2に開発システムセキュリティ機能開発の作業項目一覧を示す．

表2　開発システムセキュリティ機能開発作業項目一覧

作業項目	作業内容
セキュリティ要件定義	顧客セキュリティ要求と提案書をインプットにして，開発システム（基盤/アプリケーション）のセキュリティ要件定義書を作成し，セキュリティ開発費用，セキュリティリスク費用を見積る．
セキュリティ論理設計	基盤システム，アプリケーションシステムのセキュリティ論理設計を実施する．
セキュリティ構築	ネットワーク，クライアント，サーバといった基盤システムのセキュリティ物理設計および実装を行う．また，アプリケーションシステムのセキュリティ物理設計およびプログラミングを実施する．
セキュリティ品質評価（テスト）	開発システムの結合テスト，システムテストの段階でセキュリティ対策品質評価として，ペネトレーションテストあるいはセキュリティ機能確認テストを実施する．

基盤システムおよびアプリケーションシステムの双方に対して，セキュリティ機能開発を実施しなければならない．基盤システムでは，悪意のある不正攻撃や不正侵入から基幹システムを防護することが重要である．また，アプリケーションシステムでは，情報漏洩につながる脆弱性を作り込まないようにする必要がある．

1）　基盤システムセキュリティ構築

基盤システムセキュリティでは，外部からの悪意ある不正攻撃や不正侵入から基幹システムを防護することが重要である．

システム開発セキュリティプロセスでは，情報システム基盤における情報セキュリティ構築の指針として「基盤セキュリティ対策ガイド」を用意しており，情報システム基盤を構築する場合のセキュリティ対策技法として参考にできる．当ガイドは，「情報システム基盤のセキュリティ対策の検討方法」と「情報システム基盤の脅威に対する対策」で構成している．

ⅰ）情報システム基盤のセキュリティ対策の検討方法

ア）調査・状況認識ステップ

前提条件を確認し，開発システムが扱うデータを洗い出す．また，システムを構成する要素および関わる人員を正確に認識する．

イ）脅威分析検討ステップ

調査/状況認識が明らかになったところから，システムの安全の観点で，守るべき情報やシステムへのセキュリティ脅威を洗い出し，その中でシステム構築時に対策を行うべきものを検討する．

ウ）対策・運用維持ステップ

脅威分析検討ステップで示されたセキュリティ要件に対して，具体的な対策を決定する．作成された対策は，システム設計（運用設計も含む）とシステムの本番稼働後に適用される．

ⅱ）情報システム基盤の脅威に対する対策

ア）ネットワークのセキュリティ対策

アクセス制御，通信の暗号化，ファイアーウォール，負荷分散機能，冗長化，侵入検知システム（IDS）と侵入防止システム（IPS）等

イ）機器に対するセキュリティ対策
ネットワーク機器（スイッチングハブ，ルータ等），各種サーバ，クライアントのセキュリティ対策やウィルス対策，認証，暗号化等
ウ）セキュリティ運用
ログの管理，バックアップ
エ）セキュリティ監査
第三者機関によるセキュリティ監査，脆弱性診断
オ）物理セキュリティ
監視カメラ，入退室管理，災害対策等
カ）教育
管理者教育，利用者教育，委託先社員・派遣社員教育

また，システムを設計する際，基盤セキュリティ要件として盛り込むべき項目の遺漏を防ぎ，適確なセキュリティ要件定義書を容易に作成できるように，「基盤セキュリティ要件定義書作成ガイド」と「基盤セキュリティ要件定義書（サンプル）」を用意している．

2）　アプリケーションシステムセキュリティ機能開発

アプリケーションシステムでは，認証等のセキュリティ機能の開発だけでなく，セキュリティ攻撃で突かれる脆弱性を作り込まないプログラミングが重要である．アプリケーション開発においても基盤システム開発と同様にセキュリティ対策の指針として，「アプリケーションセキュリティ対策ガイド」を用意している．当ガイドは，Web アプリケーションにおけるアプリケーションレベルでのセキュリティ対策に関する知識の普及を目的としており，Web アプリケーションに対する代表的なセキュリティ上の脅威（攻撃手法）と，その対策について解説している．

ｉ）セキュリティ脅威の種類
ア）不正アタック（システム攻撃）
DoS 攻撃，強制ブラウズ，バッファ・オーバーフロー，書式文字列攻撃，ファイルアップロード機能の悪用
イ）不正侵入
推測，ブルートフォースアタック，アカウントの不正取得，バックドアとデバッグオプション
ウ）不正アクセス（不正利用）
機能への不正アクセス，データへの不正アクセス
エ）不正入力
クロスサイト・スクリプティング，OS コマンドインジェクション，SQL インジェクション，クロスサイト・リクエスト・フォージェリ等
オ）盗聴・改ざん
盗聴，送信データの改ざん，HTTP・HTML の偽造
カ）なりすまし
Referer の悪用，セッション・ハイジャック，セッション・フィクセイション

キ）情報漏洩

サーバのデフォルトセットアップ，DBMS 上の重要情報，メール同時配信，システム内容推測，ハードディスク上の Cookie，キャッシュの悪用，URL 履歴

ク）その他の脅威

フィッシング詐欺

ii）脆弱性のカテゴリとその対策

ア）構成管理（サーバの適切な設定と運用）

デフォルト設定の排除，ディレクトリ参照の禁止，非公開ファイル・不要ファイルの排除

イ）認証

推測困難なパスワードの設定，ロックアウト，パスワード・リマインダー，オートコンプリート対策

ウ）認可

機能へのアクセス制御，データへのアクセス制御，ランダムな値の発番

エ）入力検証

サーバでのパラメータチェック，サニタイジング

オ）機密データの格納

パスワードの格納，クレジットカード番号の格納

カ）セッション管理

HTTP メソッドの選択，HTTP セッションの安全な使い方，パスワードの再確認，派生データの使い回し禁止

キ）暗号化

Cookie の安全な使い方，HTTPS の適切な使い方

ク）表示および出力

システム情報の隠蔽，キャッシュの制御，エラーハンドリング，監査とログ記録

ケ）その他の対策

メールヘッダ，電子署名付きメール，ファイルアップロード機能，適切なリリース等

なお，基盤システムと同様にシステムを設計する際，アプリケーションセキュリティ要件として盛り込むべき項目の遺漏を防ぎ，適確なセキュリティ要件定義書を容易に作成するために「アプリケーションセキュリティ要件定義書作成ガイド」の作成を進めている．

3. 2. 7　開発環境セキュリティ管理

開発作業で作成する「開発ドキュメント」「ソースプログラム」等の開発成果物や，開発現場で扱う重要な情報である「顧客機密情報」「個人情報」およびこれらを含むテストデータを不正アクセスから保護し，情報漏洩しないように，また不正アクセスされないように管理することが重要である．

日本ユニシスグループにおける全業務を対象とした「情報セキュリティ管理」に対し，日本ユニシスの開発業務を実施するプロジェクトに特定した情報セキュリティ管理を「開発環境セキュリティプロセス」として規定し，開発プロジェクトの立上げからプロジェクト終結までの

全過程に適用している.

開発環境セキュリティプロセスでは，ISMS に準拠し，一部日本ユニシス独自の管理基準を追加した「開発環境セキュリティ管理基準」を策定し，開発プロジェクトに適用している．開発環境における情報セキュリティ管理には以下の五つのポイントがある.

1)　情報セキュリティ管理の実施
- ・開発成果物（含む知的財産），顧客機密情報等を情報資産管理台帳に記載し，管理する
- ・情報セキュリティプロシージャの遵守，プロジェクトの情報資産保護を行う

2)　機密情報管理
- ・日本ユニシスの顧客機密情報取扱基準に準拠し，開発する上で顧客から預かる機密情報を厳密に管理する

3)　個人情報管理
- ・個人情報保護関連規定に準拠し，開発現場で扱う個人情報を管理する
- ・顧客から個人情報の取扱を委託された場合，さらに協力会社に委託する場合は，日本ユニシスの顧客機密情報取扱基準に準拠する

4)　プロジェクト内月次レビューの実施
- ・セキュリティ管理者は，情報セキュリティプロシージャの遵守状況を月次でチェックし，プロジェクトマネージャに報告する

5)　情報資産の適切な処分
- ・顧客受入と検収が完了したら，プロジェクトで作成および利用した情報資産を適切に処分する．日本ユニシス社員はもちろんのこと，オフショアを含む協力会社社員による開発ドキュメント等の情報漏洩防止と，守秘義務の遵守を徹底させる
- ・プロジェクト終結レビュー時には，情報資産処分結果について確認する．また，開発委託した協力会社から開発文書等の処分結果を文書で報告させるなど結果を明確にする

3.2.8　セキュリティレビュー

システム開発セキュリティプロセスでは，セキュリティレベルに応じたレビューをルール化している．セキュリティレビューには，開発システムに対して行う「開発システムセキュリティレビュー」と開発プロジェクトでの情報セキュリティ管理状況をレビューする「開発環境セキュリティレビュー」がある.

セキュリティレビューは，開発のフェーズ毎に実施することを原則としているが，現実的な運用では，要件定義フェーズと結合・システムテストフェーズでのレビュー実施を必須としている．他のフェーズでのレビュー実施はオプションとし，プロジェクト側からの要請に基づいて実施する．要件定義フェーズと結合・システムテストフェーズのレビュー実施を必須としている理由は，要件定義フェーズでのレビューでセキュリティ要件の必要十分性を確認し，結合・システムテストフェーズでのレビューで開発においてセキュリティ要件を満足しているかを確認するためである.

また，セキュリティレビューはプロジェクト内で実施することを基本とするが，セキュリティレベルに応じてセキュリティ技術主管部による第三者レビューを実施する．表 3 にセキュリティレビュー形式を示す.

表3　セキュリティレビュー形式

セキュリティレベル	レビュー形式	レビュア
高	第三者レビュー	セキュリティ技術主管部
中	プロジェクト内レビュー	プロジェクトマネージャまたはプロジェクト内セキュリティ管理者
低	プロジェクト内レビュー	プロジェクトマネージャまたはプロジェクト内セキュリティ管理者

1）　開発システムセキュリティレビュー

レビューでは，システム開発セキュリティプロセスで提供している基盤，アプリケーションそれぞれのセキュリティ対策チェックシートに基づき，開発システム（基盤，アプリケーション）において必要十分なセキュリティの要件定義，設計，構築，テストが行われているかを確認する．

基盤セキュリティ対策チェックシート，アプリケーションセキュリティ対策チェックシートは，それぞれ「基盤セキュリティ対策ガイド」，「アプリケーションセキュリティ対策ガイド」に記載されている対策項目をチェック項目としている．各チェック項目には，チェック内容に対する対策事項が記載されている．また，各チェック項目に対してレビューガイドが記載されており，セキュリティの専門家ではないプロジェクトマネージャやプロジェクト内セキュリティ管理者が容易にセキュリティレビューを実施できる構成となっている．図3に基盤セキュリティ対策チェックシートを，図4にアプリケーションセキュリティ対策チェックシートを示す．

2）　開発環境セキュリティレビュー

開発プロジェクトでの情報セキュリティ管理状況を確認するためのレビューである．システム開発セキュリティプロセスで提供している開発環境セキュリティ対策チェックシートに基づき，情報セキュリティ管理状況を確認する．また，要件定義フェーズでは情報セキュリティ管理計画書の確認も行う．

開発環境セキュリティ対策チェックシートは，ISMSの情報セキュリティ管理項目に準拠しており，その項目の中から開発プロジェクトにとって守らなければならない必須の項目を抽出し，チェック項目としている．特に顧客機密情報，個人情報，開発成果物の管理に重点を置いた内容となっている．図5に開発環境セキュリティ対策チェックシートを示す．

対策ガイドの章、節、項				要件・対策検討時の確認項目			セキュリティ対策レベル（○：実施推奨）			対応状況			
										提案書／要件定義フェーズ			
章	大項目	中項目	小項目	・認識 ・確認 ・実装 ・運用 ・物理	チェック項目	内容詳細	高	中	低	確認事項	はい or いいえ	補足事項	更新日
2 情報システム基盤の脅威に対するセキュリティ対策について													
	2. 2.　ネットワークへの対策												
		2. 2. 2.　ネットワークアクセス制御											
				実装	①外部ネットワークと内部ネットワークの境界でアクセス制御を行なう《11.4.2》《11.4.5》【8.2.A.8】。	(1)外部ネットワーク（オープンネットワーク、リモートアクセス等）との接続箇所に不正侵入防止策を講じる。 （例） (a)ファイアウォールの設置 (b)プロキシサーバーの設置 (c)リモートアクセスサーバーの設置 (d)コールバック機能の組込み 等 以下にアクセス制御の例を示す。 (a)未使用のプロトコルをブロックする。 (b)未使用のポートをブロックする。 (c)診断用及び環境設定用ポートのアクセスを制限する。 (d)アプリケーションレベルでのアクセス制御を行なう。 (e)送信元IPアドレス、宛先IPアドレスによるフィルタリングを行なう。 (f)入力および出力についてフィルタリングを行なう。 (g)アドレス変換（グローバルIPアドレスとプライベートIPアドレスの変換）を行なう。 (h)リモートアクセスサーバにおいて、チャレンジレスポンス認証、ワンタイムパスワード認証等の強力な認証方式を用いる。 (i)コールバックによりアクセス者を限定する。				●リモートアクセス環境を構築しますか？ その他に公開サーバ等は、アドレス変換を実施していますか？ ※2.2.6.2（リモートアクセスの方式）と併せて確認する。			
				実装	②内部ネットワークの境界でアクセス制御を行なう。《11.4.5》【8.2.A】	(1)内部ネットワークのセグメントの境界でファイアウォール（または、ルータ、スイッチ等）を使ってアクセス制御を行なう。	○	○	○				
				実装	③外部ネットワークからのアクセス可能時間帯をシステム的に設定する《11.4.6》【8.2.A.10】。	(1)外部ネットワークからのアクセス可能時間帯をシステム的に設定する。 (a)物理的にネットワークを切断する。 (b)論理的（ソフトウェアの設定等）にネットワークを切断する。							
				運用	④アクセス状況監視を行う。《10.6.1》	(1)ネットワーク管理システムを導入する。 (a)監視する対象を定める。 ・負荷の異常な高まり ・サーバの障害 ・ネットワーク接続障害 ・ネットワーク機器障害 等 (b)障害等発生時のアクションを定める。 ・電子メールやポケットベル等で警報を通知 ・パトランプで通知 ・自動的にフェイルオーバーして問題のあるサーバを切断 等							

図3　基盤セキュリティ対策チェックシート

客先名	0	PM氏名	0	
プロジェクト名	0	記入担当者氏名	0	
開発責任部署	0	記入日／更新日	1900/01/00	

No.	対策カテゴリ	対策項目		回答	備考	レビュー結果と改善・指摘
2-1	システム情報の隠蔽	公開不要なページや、ファイル（データファイル、制御ファイル、バックアップファイルなど）が公開フォルダに置かれていない。また、不必要に公開フォルダが作られていない。	①はい ②いいえ（理由を備考へ記入）			
2-2		DBエラー情報やStackTraceなどの内部情報を含んだエラーメッセージが、一般利用者向けエラーページに表示されないように、適切なエラー処理を行っている。	①はい ②いいえ（理由を備考へ記入）			
2-3		処理ロジックが推測できたり、攻撃の糸口となったりするような冗舌なエラーメッセージを使用していない。	①はい ②いいえ（理由を備考へ記入）			
2-4		システム情報など、公開する必要のない情報がHTMLソース中にコメントとして出力されていない。	①はい ②いいえ（理由を備考へ記入）			
2-5		URL、URLパラメータ、httpヘッダなどに、秘匿しておくべき内容の文字列が含まれていない。	①はい ②いいえ（理由を備考へ記入）			

図4　アプリケーションセキュリティ対策チェックシート

No	開発環境セキュリティチェック項目 開発環境セキュリティ管理項目	セキュリティ 必須	セキュリティ 推奨	プロジェクト選	チェックポイント	レビューすべき証跡、資料関連文書	回答（答えの選択と「いいえ」の場合その理由または対応）		レビュー結果と改善指摘
	1.開発環境セキュリティ管理体制								
1	プロジェクト・セキュリティ責任者・管理者・担当者を決定する	○			・プロジェクト規模に見合ったセキュリティ管理体制が取られているか？大規模プロジェクトでは責任者、管理者各1名、サブシステムグループ毎に担当者1名。小規模プロジェクトでは責任者兼管理者をアサイン。	・セキュリティ管理計画書	①はい ②いいえ		
					・管理計画書にセキュリティ管理体制が明記されているか？		①はい ②いいえ		
	1.1セキュリティ管理の役割り及び責任								
	1.1.1プロジェクト・セキュリティ責任者の役割り								
2	情報セキュリティポリシーの遵守状況、セキュリティプロシージャの実施状況のレビューを行う。	○			・管理計画書にセキュリティ管理の役割、および責任がセキュリティ管理計画書に明記されているか？	・セキュリティ月次報告書 ・点検リスト	①はい ②いいえ		
3	情報セキュリティ・ポリシー、プロシージャ教育の計画、実施およびレビューを行う。	○				・セキュリティ教育計画書	①はい ②いいえ		
						・教育実施記録	①はい ②いいえ		
	1.2プロジェクト・セキュリティ管理者								
4	プロジェクトにおける情報セキュリティの維持・確保に関する管理を行う。 ①情報資産の台帳管理 ②情報セキュリティプロシージャの周知徹底、プロシージャ遵守の確認 ③情報資産アクセス権限の設定	○			・管理計画書にセキュリティ管理の役割、および責任がセキュリティ管理計画書に明記されているか？	・情報資産管理台帳 ・情報資産貸出し台帳 ・アクセス権管理台帳	①はい ②いいえ		
	1.3プロジェクトメンバー								
5	情報セキュリティポリシー、プロシージャに定められた規定、手順、関連法令の遵守。	○			・管理計画書に情報キュリティポリシー・プロシージャに定められた規定、手順の遵守が明記されているか	・セキュリティ管理計画書	①はい ②いいえ		

図5　開発環境セキュリティ対策チェックシート

4. プロセス適用の効果

2002年に開発プロジェクトへのシステム開発セキュリティプロセスの適用を開始してから，情報漏洩等の開発システムにおけるセキュリティ事件および事故発生の報告はされていない．この結果から，システム開発セキュリティプロセス適用の効果は出ていると言える．

しかしながら開発プロジェクトでのセキュリティ事故は，残念ながら報告されている．具体的な事故例は紹介しないが，可搬メディアやIDカードの紛失といった事故が発生している．セキュリティの規定や対策を策定しても，尽きるところは人の問題であり，セキュリティ意識の向上と維持を図らなければならない．

また，一般的にセキュリティ対策の費用対効果が明確になりにくいと言われているが，セキュリティ事件または事故の発生を抑えることで，事件，事故が発生した場合に顧客が被るリカバリコスト等の直接的損失，企業としての信頼性失墜による営業損失など，多大なる損失を防げることから，セキュリティ対策の費用対効果は大きなものであると言える．ただ発生確率を考慮しなければならないので，品質保証保険への投資効果相当と考えている．

5. お　わ　り　に

日本ユニシスでは，開発者向けにセキュリティに関する社内教育と基盤・アプリケーションのセキュリティ対策ガイド，開発環境の管理基準を提供してきた．

前章では開発システムでのセキュリティ事件および事故発生の報告はされていないと述べたが，開発時点では既知のセキュリティ脅威への対策を施すだけであり，新たなウィルスやセキュリティ攻撃手法が日々作成されているインターネット世界を考えれば，情報システムの運用・保守におけるセキュリティ対策の実施が，より重要である．

今後は，開発者がセキュリティ要件定義の考え方と必要性の程度を理解しやすいように，脅威の洗い出しと対応実施策について，開発プロジェクト寄りの実践的な指針をまとめる予定である．また開発環境セキュリティに関しては，日本ユニシスグループ全社ISMSの運用が開始されたことに伴い，システム開発セキュリティプロセスで策定した開発環境セキュリティ管理基準等は廃止し，ISMSベースの開発環境セキュリティプロセスに改変する予定である．保守業務を対象としたセキュリティプロセスの策定是非の検討を予定している．

＊1　ISMS：Information Security Management System の略．：情報セキュリティマネージメントシステム：組織が情報資産を適切に管理し守るための包括的な枠組みのこと．

参考文献　［1］ ISMS 認証基準 (Ver2.0)，財団法人日本情報処理開発協会，2003 年 5 月，http://www.isms.jipdec.jp/std/index.html
［2］ 独立行政法人　情報処理推進機構 (IPA)　セキュリティセンター HP，http://www.ipa.go.jp/security/

執筆者紹介　山　口　　繁（Shigeru Yamaguchi）
2001 年日本ユニシス(株)入社．電力関係のセキュリティミドルインフラ制作に取り組む．2005 年より独立行政法人向けのシステム開発に参加，2007 年より品質保証部にてシステム開発セキュリティオフィスの業務に従事．