重大な脅威に対するセキュリティ設計手法の考察

Consideration on Security Design Technique against Serious Threats

八津川　直伸，石　野　貴　子

要　約　企業が情報システムを設計するにあたり，非機能要件であるセキュリティ対策を組み込もうとする場合，システム開発の初期段階においては，システムやネットワーク等のソフトウェア構成および物理機器構成が未確定なため，セキュリティ要件が定まらず対策実施が後回しになりがちである．結果として，システム開発後半になって明らかになったセキュリティ要件への対応のために，基本設計のやり直し等の手戻りが発生することになる．このような事態を避けるため，重大な脅威に対する必要最小限のセキュリティ対策については，システム開発の初期段階において，可能な限り盛り込んでおくことが望ましい．

本稿では，インターネット等の不特定多数からの脅威にさらされる情報システムに必要な最小限のセキュリティ機能を見出すために，まず近年における重大なセキュリティ上の脅威とは何かを識別し，次にこれら脅威に対する技術的・運用的セキュリティ対策として，世の中に存在する主なフレームワークを参照しながらセキュリティ設計を行う手法について考察した．その結果，セキュリティ対策を確実に実装するために，システム開発の初期段階で考慮すべきポイントも明らかになった．

Abstract　When the company designs an information system and incorporates security countermeasures as nonfunctional requirements in it, the security requirements are not yet decided at the initial stage. Because software and physical equipment configuration such as the system and the network are unspecified at the initial stage of the system development, the security countermeasures tends to be postponed to the last moment. Therefore, to support the security requirements which became apparent at the second half of the system development, the system basic design sometimes has to be redesigned. To avoid these situations, it is desirable to implement necessary and minimum functions of security countermeasures against the serious threats beforehand into the system basic design at the initial stage of the system development as far as possible.

In this article, we try to find necessary and minimum of security functions for the information system which is exposed to the threats from the unspecified majority in the Internet and so on. To do this, we firstly identify the serious security threats in recent years. And next, we consider the design approach of security using the main framework which existed in the world as technical and operational security countermeasure against these threats. As a result, to ensure the implementation of security measures, some points to be considered at an initial stage of the system development were clarified, too.

1. はじめに

企業において，情報とそれを取り扱う情報システムは重要な情報資産である．今や社会活動のあらゆる局面において重要な役割を担う情報システムは，コンピュータを用いた不正行為，スパイ行為，妨害行為，過失行為等，様々なセキュリティ上の脅威に直面しており，適切なセ

キュリティ対策の実装は当たり前のこととして求められている．

しかしながら，システムの開発初期段階においては，システムやネットワーク等のソフトウェア構成および物理機器構成が未確定なため，どのようなセキュリティ対策を実施すればよいのかを判断できない場合が多い．一方で，セキュリティ機能はシステム機能と密接に絡むため，必要最小限のセキュリティ機能を，予め可能な限りシステム設計に盛り込んでおくことが肝要である．

本稿では，この必要最小限のセキュリティ機能を見出すために，まず近年における重大なセキュリティ上の脅威とは何かを識別し，次にこれら脅威に対する技術的・運用的セキュリティ対策を，世の中に存在する主なフレームワークを参照しながら設計する手法について述べる．

このような手順で導いたセキュリティ対策を予め開発初期段階で盛り込むことは，短期間で重大な脅威を重点的に解消するという意味において，企業から求められる「必要最小限のセキュリティ対策とは何か？」という問いに対する答えを示唆するものとして一考に値するものである．また，システム開発後半，例えば詳細設計段階以降で明らかになった脅威に対しては不足部分の追加的対応で済むことが多く，大幅な設計変更による手戻りを防止するという意味において合理性を有する．

2. セキュリティ対策設計上の問題点

通常，システム開発における情報セキュリティ対策は，以下の手順に従い行われる．

1） 調査・状況認識ステップ

まず，前提条件を確認し，保護すべきデータやシステム構成要素，およびシステムに関わる利用者等を正確に把握する．

a） 前提条件（準拠が必要な法令，基準，企業のセキュリティポリシー）の確認
b） システムが扱う保護すべきデータの洗い出し
c） システム構成要素の洗い出し
d） システム利用者の洗い出し
e） システムの物理的設置場所の洗い出し

2） 脅威分析検討ステップ

ステップ 1)で状況を正確に把握した後，システムの安全性の観点から，保護すべきデータやシステムに対する脅威を洗い出し，リスク分析を行い，その後，対策としてのセキュリティ要件を定める．

f） 脅威の洗い出し
g） リスク分析実施
h） セキュリティ要件の決定

3） 対策（セキュリティ設計/開発）実施・運用維持ステップ

ステップ 2)で定めたセキュリティ要件に対して，具体的な対策を決定し，システム設計に反映する．本番稼働後は，セキュリティ対策の適切な運用と維持継続がなされる．

i） セキュリティ対策の設計，開発・実装，テスト
j） セキュリティ対策の運用
k） セキュリティ対策の維持継続

以上のような手順において問題なのは，システムの開発初期段階において，システムやネッ

トワーク等のソフトウェア構成および物理機器構成が未確定なため，どのような情報資産が，どのような脅威にさらされ，またどのようなリスクが存在するのかについてシステム設計者が把握できず，セキュリティ要件が定まらないことである．また，非機能要件であるセキュリティ対策は，利便性の低下，開発費用の増大，運用効率の低下などの弊害を招くことが多く，開発プロジェクトにおいて対策実施が後回しにされることも多い．その結果，システム開発後半，例えば詳細設計以降において明らかになったセキュリティ要件への対応のために，基本設計のやり直し等の手戻りが発生することにもなる．このような事態を避けるためには，最終的にどのようなシステム構成になったとしても，重大な脅威に対しては予め開発初期段階において必要最小限のセキュリティ対策機能を可能な限り盛り込んでおくことが肝要である．

そこで次章以降では，インターネット等の不特定多数からの脅威にさらされる情報システムを対象として，重大なセキュリティ上の脅威を識別し，それらに対して世の中に存在する主なフレームワークを参照しながら，必要最小限の技術的・運用的セキュリティ対策設計の導出を試みる．

3. 重大なセキュリティ上の脅威の識別

重大なセキュリティ上の脅威の識別は，独立行政法人　情報処理推進機構（IPA）の「情報セキュリティ白書 2007 年版」[1]および「情報セキュリティ白書 2008 第Ⅱ部」[2]で公開された直近 2 年間の 10 大脅威を基に行う．この 10 大脅威とは，情報セキュリティ分野における研究者，実務担当者等 104 名から構成される「情報セキュリティ検討会」において，2006 年および 2007 年に「印象が強かったもの」，「社会的影響が大きいもの」等の観点から選択されたセキュリティ上の脅威である．

「情報セキュリティ白書 2007 年版」および「情報セキュリティ白書 2008 第Ⅱ部」における 10 大脅威を表 1 に示す．

表 1 「情報セキュリティ白書」における 10 大脅威

順位	情報セキュリティ白書 2007年版 10大脅威	情報セキュリティ白書 2008 第II部　10大脅威
1	漏えい情報のWinny[*1]による止まらない流通	高まる「誘導型」攻撃の脅威
2	表面化しづらい標的型（スピア型）攻撃	ウェブサイトを狙った攻撃の広まり
3	悪質化・潜在化するボット[*2]	恒常化する情報漏えい
4	深刻化するゼロデイ攻撃[*3]	巧妙化する標的型攻撃
5	ますます多様化するフィッシング詐欺[*4]	信用できなくなった正規サイト
6	増え続けるスパムメール	検知されにくいボット，潜在化するコンピュータウイルス
7	減らない情報漏えい	検索エンジンからマルウェア[*6]配信サイトに誘導
8	狙われ続ける安易なパスワード	国内製品の脆弱性が頻発
9	攻撃が急増するSQLインジェクション[*5]	減らないスパムメール
10	不適切な設定のDNSサーバを狙う攻撃の発生	組み込み製品の脆弱性の増加

2年分の情報セキュリティ白書の10大脅威には，重複している脅威や密接に関連する脅威もあるため，情報セキュリティ白書に書かれている脅威を表2のように分類し，各々の脅威を「重大なセキュリティ上の脅威」と位置付ける．

表2　重大なセキュリティ上の脅威

No.	重大なセキュリティ上の脅威	情報セキュリティ白書の10大脅威
1	Webアプリケーションの脆弱性への攻撃	2008【 2 位】ウェブサイトを狙った攻撃の広まり
		2008【 5 位】信用できなくなった正規サイト
		2007【 5 位】ますます多様化するフィッシング詐欺
		2007【 9 位】攻撃が急増するSQLインジェクション
2	情報漏えい	2008【 3 位】恒常化する情報漏えい
		2007【 1 位】漏えい情報のWinnyによる止まらない流通
		2007【 7 位】減らない情報漏えい
3	標的型（スピア型）攻撃	2008【 4 位】巧妙化する標的型攻撃
		2007【 2 位】表面化しづらい標的型（スピア型）攻撃
4	誘導型攻撃	2008【 1 位】高まる「誘導型」攻撃の脅威
		2008【 7 位】検索エンジンからマルウェア配信サイトに誘導
5	ボット，コンピュータウイルス	2008【 6 位】検知されにくいボット，潜在化するコンピュータウイルス
		2007【 3 位】悪質化・潜在化するボット
6	スパムメール	2008【 9 位】減らないスパムメール
		2007【 6 位】増え続けるスパムメール
7	国内製品の脆弱性への攻撃	2008【 8 位】国内製品の脆弱性が頻発
		2007【 4 位】深刻化するゼロデイ攻撃
8	組み込み製品の脆弱性への攻撃	2008【10 位】組み込み製品の脆弱性の増加
9	脆弱なパスワードの利用	2007【 8 位】狙われ続ける安易なパスワード
10	DNSサーバの脆弱性への攻撃	2007【10 位】不適切な設定のDNSサーバを狙う攻撃の発生

4.　セキュリティ対策に用いられる主なフレームワーク

セキュリティ対策を検討する際，対策の抜け漏れを防ぐために既存のフレームワークを利用することが一般的である．フレームワークにはセキュリティマネジメントシステムを構築するもの，技術的対策に重点をおいたもの，セキュリティ監査視点のもの等がある．主なフレームワークを表3に示す．

これ以外にも，企業が属する業界や団体等で情報セキュリティに関する基準やガイドラインが定められている場合には，それを用いてセキュリティ対策を検討する必要がある．フレームワークの内容の全てを満たす必要性があるかについては，適用対象となる範囲，システムの種類によるため，場合によっては部分的に利用するという方法もある．本章では表3に示したフレームワークについて述べる．

表3　主なフレームワーク

基準・ガイドライン	制定・発行
JIS Q 27001：情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項 JIS Q 27002：情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範	日本規格協会
情報セキュリティ管理基準	経済産業省
政府機関の情報セキュリティ対策のための統一基準	内閣官房情報セキュリティセンター（NISC）
FISC（金融情報システムセンター）　安全対策基準等関連ガイドライン	金融情報システムセンター（FISC）
PCI DSS（Payment Card Industry Data Security Standard, ペイメントカード業界データセキュリティ基準）	PCISSC（PCI Security Standards Council LLC）

4.1　JIS Q 27001 と JIS Q 27002

セキュリティマネジメントシステム構築のフレームワークとして一般的な規格であり，ISMS（Information Security Management System）認証基準（JIS Q 27001）と，管理目的および管理策である附属書 A の手引き（JIS Q 27002）である．

JIS Q 27001 には，セキュリティ対策の本筋である「Plan-Do-Check-Act（計画－実行－点検－処置）」の PDCA サイクルの構築について書かれている．このフレームワークに則りセキュリティ対策を検討・実施し，定めた規則通りに運用することにより，セキュアな状態が保たれる．ただし，対策の具体例は書かれていないため，どのような対策を実施すればよいか，特に技術的対策をどのレベルまで実施すればよいかという疑問は残る．

4.2　情報セキュリティ管理基準

経済産業省が定め，2003 年 4 月 1 日から運用開始した「情報セキュリティ監査制度」で用いられる管理基準である．初版は JIS Q 27002 の前規格である JIS X 5080 を基に策定したものであり，2008 年 7 月 2 日に JIS Q 27001 および JIS Q 27002 の両規格に基づいた改正案が出されている．情報セキュリティ監査基準に従った監査において，監査上の判断の尺度として用いることを原則としているため，基にした両規格の各管理策に対して，より詳細に記述されている．

各規格と比較すると対策の具体例に触れられてはいるが，どのレベルまで実施すればよいかの判断は，採用する企業に任せられている．

4.3　政府機関の情報セキュリティ対策のための統一基準

政府機関の情報セキュリティ対策の整合化・共通化を促進し，政府機関全体としての情報セキュリティ水準の向上を図ることを目的とした基準であり，2005 年 12 月に全体版初版が定められ，2008 年 2 月 4 日で第 3 版となる．これにより，政府機関のセキュリティ対策のばらつきがなくなり，一般企業でも政府機関と同レベルのセキュリティ対策が実施可能となる．ただし，公務員法等の法律で定められている範囲の管理項目については定められていないため，政府機関以外の企業では，この基準だけを満たすのでは不充分といえる．

4.4 FISC（金融情報システムセンター） 安全対策基準等関連ガイドライン

重要な社会インフラである金融情報システムの安全性確保のための自主基準であり，コンピュータシステムの安全対策基準・解説書，システム監査指針等がある．コンピュータシステムの安全対策基準は，設備基準，運用基準，技術基準から成り，対策を適用する対象箇所および実施必須基準項目と推奨基準項目とを明確にしている．実装の具体例が記述されているため，金融機関だけでなく，他業種の企業も対策策定の参考とすることが可能である．

4.5 PCI DSS（Payment Card Industry Data Security Standard，ペイメントカード業界データセキュリティ基準）

国際ペイメントブランド5社が2004年に策定したカード情報セキュリティの国際統一基準であり，加盟店やサービスプロバイダー等，カード情報を保管，処理，伝送するすべての組織が，カード会員のカード情報や取引情報を保護するために実施しなければならない要件を定めている．カード情報保護のための実装レベルの要件が具体的に定義されているため，実装時の悩みは少ないが，自由度は低く，高レベルの要件については実装が困難な組織もあると思われる．

5. 重大なセキュリティ上の脅威と対策

本章では，3章で識別した重大なセキュリティ上の脅威への対策に関し，4章のどのフレームワークにおいても要求されている共通対策項目を抽出し，その具体化を図る．識別した脅威とセキュリティ対策の一覧を表4に示し，各々の脅威と対策について，各節にて詳細に述べる．

5.1 Webアプリケーションの脆弱性への攻撃

攻撃者は昨今，セキュリティ対策コードの実装が甘く，攻撃の労力に対し比較的得られるものが多いビジネスアプリケーション（主にWebアプリケーション）を攻撃の対象にすることが多い．正規サイトの脆弱性を利用したセッション乗っ取りやSQLインジェクション等による情報漏えい，マルウェア配信サイトへの誘導，多様化するフィッシング詐欺等枚挙にいとまがない．これらの脅威の原因は相互に関係しているものが多い．

5.1.1 脅威

1） クロスサイト・スクリプティング（Cross Site Scripting：XSS）

XSSは，Webアプリケーションの脆弱性を突いて利用者を狙う攻撃手法の一つである．Webサイトを閲覧した利用者のブラウザ内で悪意のあるスクリプトが実行され，偽情報の表示や，情報の漏えい，セッションの乗っ取り，フィッシング詐欺等の被害を引き起こす代表的な攻撃手法である．IPAが公表している「脆弱性関連情報に関する届出状況」においては，届出に基づくWebサイトの脆弱性全体の70%がこのXSSおよび次に述べるSQLインジェクションで占められており，依然として多くのWebサイトがこの脆弱性を抱えている．

2） SQLインジェクション

古くから存在する攻撃手法であり，同様なものにOSコマンドインジェクション，LDAPインジェクション等がある．2006年は2005年と比較しておよそ数倍から数十倍程度の攻撃

表4　重大なセキュリティ上の脅威とセキュリティ対策一覧

識別した脅威		セキュリティ対策	
1	Webアプリケーションの脆弱性への攻撃	1-1	XSS対策
		1-2	SQLインジェクション対策
		1-3	フィッシング詐欺対策
2	情報漏えい	2-1	ネットワークのセキュリティ対策
		2-2	ファイルの暗号化
		2-3	アクセス制御
		2-4	アカウント管理
		2-5	メールフィルタリング
		2-6	各種ログの監査
3	標的型（スピア型）攻撃	3-1	メールフィルタリングの実施
		3-2	ファイアウォールによる不要な通信の遮断
		3-3	ウイルス対策・脆弱性対策
4	誘導型攻撃	4-1	基本的に企業の従業員が使用するソフトウェアを最新の状態にしておく
		4-2	ウイルス定義ファイルを最新に保つ
		4-3	ボット・コンピュータウイルス対策の実施
		4-4	利用者の啓発
5	ボット，コンピュータウイルス	5-1	ファイアウォールによる不要な通信の遮断
		5-2	ネットワークの監視
		5-3	セキュリティパッチの適用
		5-4	ウイルス対策ソフトウェアの定義ファイルを最新の状態に保つ
6	スパムメール	6-1	スパムメール・フィルタリング
		6-2	送信ドメイン認証
		6-3	フロー制御
		6-4	第三者中継の無効化
7	国内製品の脆弱性への攻撃	7-1	使用しているソフトウェアの脆弱性対策およびゼロデイ攻撃対策の実施
		7-2	セキュリティパッチの適用
8	組み込み製品の脆弱性への攻撃	8-1	組み込みアプリケーションのアップデート
		8-2	組み込み機器への接続制限
9	脆弱なパスワードの利用	9-1	安全なパスワード認証機能を備える
		9-2	パスワード文字列の複雑性実現機能を備える
		9-3	パスワード認証の強化機能を備える
10	DNSサーバの脆弱性への攻撃	10-1	サービス妨害攻撃対策
		10-2	DNSキャッシュ汚染対策

量となり，Web アプリケーションに対する攻撃のうち，およそ 60% 程度が SQL インジェクション攻撃である[1]．この攻撃による被害の多くはデータベースからの情報漏えいであるが，その特徴として，攻撃されたことが発見されにくく，また被害が生じてもその事実に気がつくのが難しい，ということが挙げられる．

3)　フィッシング詐欺

何らかの偽メールで利用者をフィッシングサイトに誘導し，アドレスバーを隠したポップ

アップウィンドウに利用者のパスワードや個人情報を入力させるという単純な方法の他，Web サイトの脆弱性を突いた XSS により，本物の Web サイト上に内容を差し替えた偽情報を表示するという方法がある．後者の場合は，アドレスバーには本物のサイトのドメイン名が表示されるため，利用者がサイトのドメイン名や証明書を確認しても偽情報であることを見分けることができず，完璧なフィッシング詐欺サイトと言える．このような信用できなくなった正規サイトは，2006 年末に MPack[*7] や IcePack[*8] 等の攻撃ツールが登場して以降，増える傾向にある．前述のようにパスワードや個人情報を搾取されるだけでなく，書き換えられた Web ページに仕掛けられたインラインフレーム[*9] やスクリプト[*10] 等によって，閲覧した利用者の PC がマルウェアに汚染されてしまうこともある．

5. 1. 2　対策

Web アプリケーションのようにインターネット経由で接続されるシステムにおいては，外部から入力されるデータを信用してはならないのが鉄則である．アプリケーションへの入力パラメータ値の確認不徹底や外部アプリケーションへの出力パラメータ値の不適正な処理によって，5. 1. 1 項に述べた XSS や SQL インジェクション等の脅威が現実化する．これらは，開発者の理解不足によるところが大きく，正しい設計やコーディングを行えば防げる脅威であり，脆弱性というより，基本的なアプリケーションの要件を満たしていない，即ち適正な入力および出力を行うことができていないというバグに近いものである．このような脅威を防止するためには，図 1 に示すように入出力データの検査とそれらの適正化が必要である．

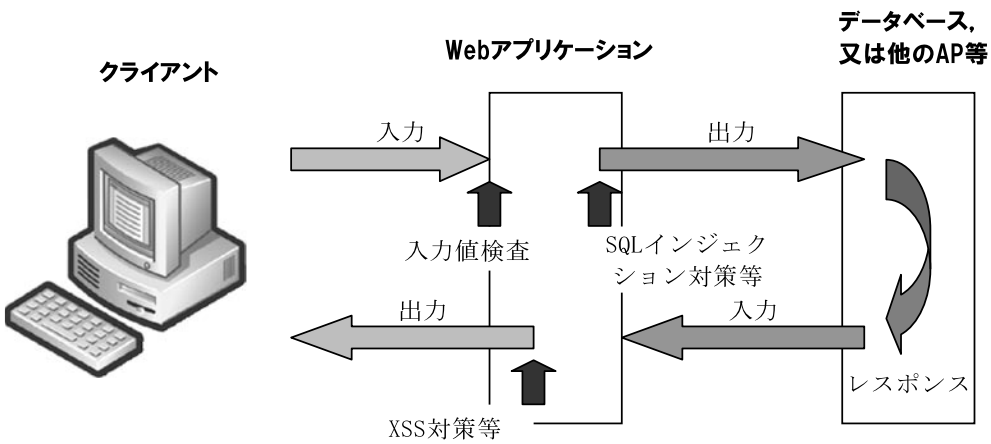

図 1　Web アプリケーションの入出力チェック

1）　XSS 対策

Web アプリケーションにおいて，クライアントからの入力を別の処理系への出力とする場合，不適正な出力によりシステムがセキュリティ上問題のある動作を起こすことを防ぐため，以下のように特殊な文字/文字列を完全に排除しクライアントからの入力を無害化する．

a）　HTML への出力を行う場合，XSS 対策として，予期しないスクリプトの動作（の割り込み）を防ぐため，「<」「>」「&」「”」「’」の文字は，それぞれ「<」「>」「&」「"」「'」と文字として扱われるようにエスケープ処理して出力する．

b) ダウンロードやファイル閲覧のため，ユーザの入力データをファイルアクセス時の引数（ファイル名）として利用する場合，PATH トラバーサル[*11] 対策として，「..」や「/」（あるいは「\」）等の文字をエスケープ処理してファイルを呼び出す．

c) クライアントからの入力データが，そのまま HTTP ヘッダに埋め込まれる（URL のリダイレクト先や Cookie）アプリケーションでは，HTTP レスポンス分割対策として，入力に「CR」や「LF」が含まれている場合はそれらを排除する．

2) SQL インジェクション対策

HTTP ベースの通信においては，利用者はそのリクエストを容易に改ざんすることが可能である．従って，クライアントから入力されるデータを受け取る Web アプリケーションは，HTTP リクエスト（ヘッダー，ボディ）が改ざんされている可能性を考慮して，毎回必ず，全ての入力データの正当性をチェックする．これにより，システムの誤動作や，データ汚染・破壊を防止する．

a) 入力値検査において業務要件上の許容範囲内で，文字種，不要な文字（群），サイズ等について，受け入れ範囲をできるだけ絞る．その上で，以下の処理を行う（サイズはバッファ・オーバーフロー対策）．

b) 入力されたデータの検証（基本的には，排除または拒否）を行う．
業務的な仕様等一定のルールの下で行う．置換が要求される場合もあるが，文字数が変わるとコードが煩雑になるので基本的に範囲外のデータは排除または拒否する．

c) 業務上，排除または拒否ができず受け入れる必要があるデータについては，下記 d)，e)のように，出力時にデータの検証（基本的には，無害化）を行う．

d) SQL によりデータベースへのアクセスを行う場合は，SQL インジェクション対策として，バインド変数を使ったアクセス（Java：Prepared Statement，.NET：ParameterizedQuery）を利用する．バインド変数が利用できない場合（order by 句，where 条件全体，対象 table が可変となる等）は，SQL 文を発行する際，SQL としての特殊文字（「'」「%」「_」等）をエスケープ処理する．
なお，LDAP や XML 等 RDB 以外のデータソース類にアクセスする場合でも，それらのインターフェイスで使用する特殊文字についてエスケープ処理する必要がある（LDAP インジェクション，XPATH インジェクション対策）．

e) d)と同様にクライアントからの入力データを OS コマンドの呼び出しの引数として使用する場合は，OS コマンドインジェクション対策として，呼び出し（出力）の際に，そのシステムで特別な意味を持つ文字をエスケープ処理して引き渡す．通常は，このサニタイジングによる対策以前に，汎用的にシェル，コマンドプロンプト等を呼び出すことを禁じ，想定した動作以外が起きないようインターフェイス設計を行う．

3) フィッシング詐欺対策

a) Web サイトにアクセスする利用者がパスワードや個人情報を入力する際に，入力しようとしている画面はどこのサイトなのか，アドレスバーに表示された URL のドメイン名で確認可能なようにサイトを設計する．
（例）アドレスバーを隠したポップアップウィンドウを使った画面設計は行わない．

b) Web アプリケーションに XSS の脆弱性が存在した場合，本物のサイト上に内容を差し替えた偽情報を表示できてしまうので，5. 1. 2 項の「1）XSS 対策」を確実に行う．

c） フィッシングサイト停止サービスを導入する．
フィッシングサイトの検出と停止を迅速に行う第三者サービスであり，正規の Web サイト運営者側にとって停止にかけるマンパワーと時間を節約できる．このサービス提供者は，徹底的なフォレンジックによって不正行為者を特定し，フィッシングサイトの迅速なシャットダウン，対抗策の導入，および将来の攻撃を防止する．また，世界各地の ISP（Internet Services Provider），CERT/CC（Computer Emergency Response Team/Coordination Center），およびサイバー・ポリスとの密接な連携に基づき，不正サイトのシャットダウンを促進している．

d） 利用者への注意喚起を行う．
フィッシング詐欺に遭わないためには，利用者自身が注意することが最も重要である．そのため個人情報等の重要な情報を取り扱う Web サイトでは，利用者に対し以下の点に注意すべきであることを掲載する．

ア） クレジットカード番号やパスワード等の，第三者に知られるべきでない情報を，メールで送信しない．

イ） 金融機関等からの緊急事態のメールは疑い，本物か迷う場合は電話で直接確認する．

ウ） 金融機関等の Web ページを開く場合には，メールに記載された URL からではなくブラウザのお気に入りから開くようにする．

エ） ブラウザのアドレスバーに表示された URL のドメイン名部分に，正しいドメイン名が表示されていることを確認する．

オ） クレジットカード番号やパスワード等の，第三者に知られるべきでない情報を入力する際には，ブラウザに鍵マークがあることを確認する．ブラウザが証明書に対して警告を出した場合は，入力を取り止める．

カ） 初めて利用する Web サイトは，鍵マークのある Web ページで鍵マークより証明書を表示し，運営者を確認する．

キ） フィッシング対策ソフトを導入する．Web アクセスの際，フィッシングサイトを検知できる仕組みを備え，個人情報等の入力を行う前，あるいは詐欺画面が出る前等に自動的に画面をブロックし警告を表示する．

5. 2 情報漏えい

情報漏えいは，毎年，年間を通じて問題となっている．情報漏えいには故意によるもの，紛失，操作ミス等，様々な原因があり，対策もそれぞれに応じて行う必要がある．

5. 2. 1 脅威

1） 記憶媒体の紛失・盗難

情報を記録した記憶媒体の紛失や盗難は，携帯時の置き忘れや机上放置，ルールで禁止されている情報の持ち出し等の利用者の不注意，セキュリティ意識の低さから起こるルール違反や管理体制の不備が原因となって起こる．

2007 年 7 月に NPO 日本ネットワークセキュリティ協会（JNSA）が公開した調査結果によると，記憶媒体の紛失・盗難が情報漏えいの原因の中心である．

2）　P2P（Peer to Peer）ネットワークの利用

Winny/Share[*1] 等のファイル交換ソフトにより漏えいした情報は，P2P ネットワーク上を流通し続ける．紙媒体と異なりコピーしても情報が劣化しないため，大量の複製が作成される．

3）　誤送信・誤公開

電子メールの宛先を間違えることによる情報の誤送信や担当者の操作ミスによる誤公開等は，意図しない相手に対し情報をアクセスできる状態にしてしまう．誤公開は，担当者が気付かない場合，長期間に亘り誰もが参照できる状態で放置される．

4）　不正アクセス

外部から主にネットワークを経由して不正に企業内部に侵入し，情報を盗み出す．その手段には，正規アカウントを使用した「なりすまし」や，OS やアプリケーションの脆弱性の悪用等がある．一度企業内のサーバ等に不正侵入した後，それを踏み台としてさらに内部の重要な情報を持ったサーバ類にアクセスし，情報を盗み出すこともある．

5）　不正プログラム

ワーム・コンピュータウイルス等の不正プログラムにより，意図しない情報の公開や外部へのメール送信で情報が漏えいする．5.5 節「ボット・コンピュータウイルス」でも，不正プログラムを原因とした脅威を述べている．

6）　内部不正行為

正当なアクセス権を持った従業員による，情報の不正持ち出しが原因となる情報漏えいでは，その企業の従業員だけでなく，委託先企業の従業員による情報漏えいも問題となっている．また，アクセス権限のない従業員が，権限のある者のアカウントを不正に使用し情報を持ち出すことも，内部不正行為とされる．

5.2.2　対策

1）　ネットワークのセキュリティ対策

技術的対策の基本として，組織と外部との境界にファイアウォールを設置する．ファイアウォールでは業務に必要な通信のみを許可し，それ以外の通信は遮断することにより，外部からの単純な侵入を防ぐことができる．ファイアウォールを設置する際には，外部からアクセス可能な通信経路，通信機器は最小限とするようネットワークを設計する．その際，サーバ類は役割や扱うデータに応じて分類し，異なるネットワークセグメントに設置する．また，不正侵入検知システム/不正侵入防御システム（Intrusion Detection System/Intrusion Prevention System：IDS/IPS）を導入し，不正侵入を検知・防御する．

2）　ファイルの暗号化

操作ミスや紛失・盗難により情報が流出してしまった際に，その内容を見られないようにするための対策として，ファイルを暗号化する．サーバや記録媒体へ情報を書き込む際に自動的に暗号化するアプリケーションを利用することにより，従業員が意識せずともファイルが暗号化され，機密性が保たれる．クライアント PC 上のファイルの自動的な暗号化の実装が困難である場合は，クライアントに情報を保存しないよう，シンクライアント端末を導入することも有効である．

3） アクセス制御

内部からの不正アクセスを防ぐために，アクセス制御を実施する．アクセス権設定の際には，情報，サーバ，ネットワーク機器等へのアクセスを必要最小限とし，アクセス権の付与・変更・削除等の手順を明確に定め，設定状況について定期的に見直すことが重要である．

4） アカウント管理

アクセス制御を有効に機能させるために，アカウント管理を実施する．アカウントの登録・変更・削除等の手順を定め，一元管理を行う．アカウントの属性については，現状とあっているかを定期的に見直し，特別に高い権限（以下，特権という）を与えたアカウントについては，特権付与の審査を厳しくするとともに，より高い頻度で見直しを実施する．

5） メールフィルタリングの実施

重要情報の誤送信や意図的な外部への送信等を監視するため，組織外とのメール送受信内容をフィルタリングし，情報漏えいの可能性があると判断したメールを遮断する．メールによる情報漏えいの抑止のため，メールフィルタリングを実施していることを従業員に通知することも効果的な対策である．

6） 各種ログの監査

ファイアウォール，サーバアクセス，IDS/IPS，端末操作履歴等のログを取得し，ログに記録されている事象からセキュリティ事件・事故の兆候を見つけ出す機能を実装する．複数のログを用いて解析する必要があるため，NTP（Network Time Protocol）サーバを利用しログ収集対象機器の時刻同期を行い，各ログに記録される時刻のずれを防ぐ．

7） その他

紙媒体や記録媒体，サーバ機器等の盗難・紛失や情報の盗み見等防止の物理的対策として，持ち出し管理，施錠管理，入退室管理も重要である．

5.3 標的型（スピア型）攻撃

標的型（スピア型）攻撃とは，マルウェアを使い特定の企業や個人を狙って行われる攻撃であり，不特定多数を狙って行われる攻撃と区別されている．攻撃者は攻撃対象を充分調査した後攻撃するため成功率が高く，また，攻撃対象が限定されるため話題になりにくいという特徴がある．

5.3.1 脅威

攻撃者は攻撃対象を充分調査し，イントラネットのシステムを攻撃する．例えば，攻撃を受けた企業の従業員が信用してしまうような内容のメールを送ったり，つい開いてしまうような名前のファイルをメールに添付したりする．添付ファイルには今まで安全とされていたファイルが使われるため，マルウェアを送り込むことに成功しやすい．攻撃側は常に新しいプログラムを送り込むことを可能とするようにし，感染事実を隠蔽する巧妙な工夫や，セキュリティベンダーによる解析を妨害する措置も仕掛けている．

5.3.2 対策

業種に関係なく標的型攻撃を受ける可能性があるため，まずは攻撃メール等を社内へ入れないこと，入ってしまった場合拡散させないことが重要である．

1）　メールフィルタリングの実施

「.exe」「.com」「.scr」「.pif」「.bat」等の拡張子に代表される実行プログラム形式のファイルを開くと，危険なプログラムが実行される場合がある．日頃からこのような形式のファイルをやり取りしていると，受け取った者は躊躇なく開く可能性がある．これを防ぐため，関係者間でやり取りするファイルを，「.txt」「.doc」「.pdf」等の拡張子を持った実行できない形式のファイルや，「.zip」「.lzh」「.cab」等の拡張子を持ったアーカイブ形式のファイルのみとするような添付ファイルのルールを策定，メールフィルタリングソフトを導入し，ルールに沿わない添付ファイルをフィルタリングする．アーカイブ形式ファイルの場合，その内部にも実行プログラム形式のファイルを含まないようにフィルタリングする．

2）　ファイアウォールによる不要な通信の遮断

標的型攻撃に用いられるマルウェアは，プログラムが攻撃側のサーバから多段階にダウンロードされて実行するという特徴があり，攻撃側は常に新しいプログラムを送り込むことが可能となっている．攻撃側サーバからのダウンロードを避けるために，組織と外部との境界にファイアウォールを設置，不要な外向けの TCP ポートを閉じ，Web サイトへのアクセス（HTTP/HTTPS アクセス）をプロキシサーバ経由に限定する等の通信制限を実施する．

3）　ウイルス対策・脆弱性対策

「開いても安全である」という認識が高いファイルを処理するアプリケーションの脆弱性や，ベンダーからの対策が情報公開されていないゼロデイ脆弱性が，標的型攻撃においてはよく利用される．ウイルス対策ソフトウェアやスパイウェア[*12]対策ソフトウェアを導入することは重要であるが，製品選択する際に，既知のウイルス以外にプログラムの振る舞いに基づく方法等で未知の悪意あるソフトウェアを検出できる製品であるかを考慮する．また，使用していないサービスを無効化し，攻撃や悪意あるソフトウェアに利用されるのを防ぐことも有効である．

4）　その他

管理面で必要な対策として，従業員に対するセキュリティ教育も重要である．従業員には，偽メールを発見できるようにするために，メールでのなりすましが可能であることを意識させる．また，二重拡張子やアイコンの偽装等，害のない形式のファイルへの見せかけにも注意する必要がある．

5. 4　誘導型攻撃

この攻撃は，攻撃を受ける側が悪質なサイトへの誘導メールや悪質な掲示板/Web サイトを閲覧することで成立する．ほとんどの場合が OS やアプリケーションの脆弱性を利用する攻撃である．Web サイトへのアクセスやメールは，通常ファイアウォールにおいて通過が許可されているので，どのような企業や個人に対しても誘導型攻撃は容易に成立し得る．

5. 4. 1　脅威

誘導された利用者は悪質なサイトへアクセスするだけで，ボットやウイルスを PC にインストールされてしまう攻撃にさらされる．昨今では，検索エンジンからマルウェア配信サイトに誘導する方法も見られる．よく用いられる単語をキーとして SEO（Search Engine Optimization：サーチエンジンによる Web サイトの検索結果の表示順位を向上させる施策）対策が施

されたマルウェア配信サイトは，その単語による検索結果の上位に表示されるので，利用者が無造作にそれをクリックするとマルウェアに汚染されてしまうことになる．この誘導型攻撃は，直接マルウェア配信サイトやフィッシングサイトへの誘導の他，5.1節で述べたXSSの前段階としても利用される．

5.4.2　対策

前述のように，Webサイトへのアクセスやメールは，通常ファイアウォールで通過が許可されているので，防御する企業側としては誘導された悪質なサイトからボットやウイルス等を企業内にダウンロードしないよう，あるいはダウンロードしてしまった場合には迅速に駆除するよう対応するしかない．2007年は，ワープロソフトや圧縮解凍ソフトウェアに脆弱性が発見された結果，メールに添付された文書ファイルや圧縮ファイルを悪用する攻撃が多発した．誘導型攻撃への対策としては，以下が挙げられる．

1）　企業の従業員が使用するソフトウェアを可能な限り最新の状態にしておくこと
2）　ウイルス定義ファイルを最新に保つこと
3）　平行して5.5節で述べるボット・コンピュータウイルス対策を実施すること
4）　利用者の啓発を図ること

5.5　ボット・コンピュータウイルス

ボットは，同じようにネットワークを通じて感染するウイルスとは違い，感染に成功してコンピュータへ侵入し，ボットネットワークと呼ばれる独自のネットワークに自動的に参加し，拡大していく．

5.5.1　脅威

ボットをインストールされたコンピュータは，迷惑メールの送信や第三者への攻撃の踏み台として悪用されるため，知らないうちに加害者となり第三者に被害を与えてしまう．JPCERT/CC（Japan Computer Emergency Response Team/Coordination Center）によるボットの調査によると，侵入経路として5.1節で示したようなWebサイトの脆弱性を狙う傾向があることがわかっている．これは，ファイアウォールに阻まれずに感染が可能であるためと分析されている[2]．また，ボットネットワークの構成も変化し，指令サーバの冗長化や自立分散型のボットが出現している．

ウイルスの感染経路は多様化が進み，2007年はインスタントメッセンジャーを経由して感染するものが増加した．

5.5.2　対策

1）　ファイアウォールによる不要な通信の遮断

5.3.2項でも述べたが，ボットの外部との通信を防ぐために，組織と外部との境界にファイアウォールを設置，不要な外向けTCPポートを閉じ，Webサイトへのアクセス（HTTP/HTTPSアクセス）をプロキシサーバ経由に限定する．また，ボットは本来組織内で行われるべき通信とは異なる通信を行う場合があるため，本来行われるべき通信のみを許可する運用を行うことにより，ボットが行う通信を遮断，ボットの活動を抑える．

2)　ネットワークの監視

前述のファイアウォールによる対策と同様の理由により，組織内ネットワークを監視し，ボットが行う通信を検知，遮断する．

3)　セキュリティパッチの適用

ソフトウェアの脆弱性対策として，セキュリティパッチを適用する．しかし，これは実運用環境の変更にあたるため，パッチ適用後の動作確認は必須である．セキュリティパッチのリリース情報を入手してから実運用環境に適用するまでの動作確認を含めた手順を定めておき，手順に則り実施することが必要である．

4)　ウイルス対策ソフトウェアの定義ファイルを最新の状態に保つ

ウイルスの感染経路が多様化しているため，通信経路へのウイルス対策ソフトウェアの導入だけではウイルス感染を防御できない．各サーバやクライアントへウイルス対策ソフトウェアを導入し，定義ファイルを最新の状態に保つとともに，ボット駆除ツール等での定期的なチェックが必要である．

5.6　スパムメール

スパムメールは迷惑メールとも呼ばれ，広告やフィッシング詐欺，マルウェア配布等の目的で，受信者の意図に反して無差別かつ大量に送信され，受信者本来の利用を妨げているものである．

5.6.1　脅威

2007年のスパムメールの数は，海外セキュリティベンダーの統計によれば，2006年と比較しておよそ2.5倍になっている．また，メール全体に占めるスパムメールの割合は，調査方法によるばらつきがあるものの，おおよそ70%～95%程度であると報告されており[2]，このような大量のスパムメールにより，クライアントPCやサーバへの負荷が増え，受信者側は対応に時間を取られる，配送の遅延やフィルタの副作用で本来受け取るべきメールを見逃す等の被害が生じている．

5.6.2　対策

スパムメールを受け取らないようにするには，状況に応じて以下の対策を選択する．

・スパムメール・フィルタリング
・送信ドメイン認証
・フロー制御

また上記に加え，スパムメールの踏み台となる第三者中継の無効化を行う必要がある．

1)　スパムメール・フィルタリング

なんらかの規則（フィルタ）により，受信メールを検査する．スパムメール（迷惑メール）と判定した場合は，そのメールを隔離あるいは削除する．フィルタには以下の種類がある．

a)　ルールフィルタ

本文や件名に特定の文字列があるかをフィルタリングのルールとして設定しておき，設定したルールに従って判定する機能．例えば，メールの「本文に《出会い》が含まれる」，「件名に《格安》が含まれる」等．

b） シグネチャフィルタ

メールの本文やヘッダを一定の方法に従って計算したデータ（シグネチャ）と比較し，迷惑メールかどうかを判定する機能．対策ベンダーが既に流通している迷惑メールを収集してシグネチャを作成し，データベース化しておく．届いたメールに含まれる要素からシグネチャを作成し，ベンダーが提供するデータベースと照合することで迷惑メールかどうかの判断を行う．

c） ベイジアンフィルタ

過去に迷惑メールと判定されたメールに含まれる単語を解析し，迷惑メールの特徴や傾向を自動的に学習させ，その学習した情報を基に新しいメールが迷惑メールかどうかを判定する機能．

d） レピュテーションフィルタ

SMTP で接続を要求してきた相手の IP アドレスやドメイン名等の情報を，レピュテーション（評判）情報を提供するサーバにインターネット経由で問い合わせて，評判の悪い相手なら接続を拒否する機能．

e） ヒューリスティックフィルタ

予め設定した複数のルールで判定した結果を総合し，迷惑メールかどうかを判断する機能．例えば，「本文に大文字が入っていたら 1 点」，「疑わしいリンクがあったら 2 点」等，疑わしい条件に該当したら予め決めておいた点数を加算していき，一定のしきい値を超えると迷惑メールと判定する．

2） 送信ドメイン認証

迷惑メール送信者は，メールソフト等で送信元を簡単に詐称することができる．そこで，送信されてきたメールが，送信元と名乗っているアドレスに示されるドメイン（送信ドメイン）から本当に送られているかどうかの確認（送信ドメイン認証）を行う．これにより，正しい送信元と判断されたメールのみ受信することができる．送信ドメイン認証は大きく分けて二つの方式がある．

a） IP アドレスベースによる認証（SPF：Sender Policy Framework）

受信側メールサーバでは，SMTP での接続の際に相手が通知してきたドメイン名を使って，送信者側が送信側 DNS に予め公開した SPF レコードの問い合わせを行う．SPF レコードの IP アドレスと SMTP のソース IP アドレスとを照合し，それらが同一であれば認証成功とする．

b） 電子署名ベースによる認証（DKIM：DomainKeys Identified Mail）

送信者はメール本文に電子署名を付し，受信側メールサーバでは，SMTP での接続の際に相手が通知してきたドメイン名を使って，送信者側が送信側 DNS に予め公開した公開鍵を取得する．受信者はこの公開鍵を使用して電子署名を検証し，正規の送信者からのメールか否かを判断する．

3） フロー制御

スパムメールは，不特定の送信元から短時間に大量に配信されるという特徴がある．この特徴を検知し，企業への入り口部分でスパムメールをフロー制御する．これにより，メールサーバへの負荷を低減できる．例えば，以下のようなフロー制御がある．

a) 1秒間に同じ送信元（IPアドレス）から一定数以上のメールを受信した場合，その送信元からのメールを一定時間受け取らないようにする．

b) 1分間に同じ送信元（IPアドレス）から受信したメールの受信者の80%以上がUser Unknownなら，その送信者からのメールを一定時間受け取らないようにする．

4) 第三者中継の無効化

メールサーバを第三者中継に利用されないように，メールサーバに以下の設定を行う．

a) メールクライアントとして許可しているIPアドレスの範囲を指定し，そのアドレスからの電子メール配信要求についてのみ中継を行う．

b) 自社のドメインが宛先となっているメールのみを受信する．

5.7 国内製品の脆弱性への攻撃

これまでは世界的に利用されているソフトウェアに対する脆弱性攻撃が多かったが，2007年は国内で開発および販売されているソフトウェアの脆弱性が多数発見され，ゼロデイ攻撃のターゲットとされた．

5.7.1 脅威

世界的にみると利用者数は少ないが，国内でみると利用者数の多いソフトウェアに対する攻撃は，国内での影響範囲が広い．国内製品は，まだ脆弱性が発見され始めてから日が浅いため，多数の脆弱性が潜んでいる可能性があり，ゼロデイ攻撃の対象とされる危険性がある．

5.7.2 対策

1) 使用しているソフトウェアの脆弱性対策およびゼロデイ攻撃対策の実施

国内製品の脆弱性の中には，技術的に新しい種類の脆弱性ではなく，世界のソフトウェアで日々発見されている脆弱性と同種のものが多い．国内で利用されるソフトウェアの脆弱性情報を公開するデータベース等を利用し，利用しているソフトウェアの脆弱性やゼロデイ攻撃情報を収集，公開されている対策を実施する．

2) セキュリティパッチの適用

製品の脆弱性への対策は，セキュリティパッチを適用することである．その際，5.5節のセキュリティパッチ対策と同様の考慮が必要である．

5.8 組み込み製品の脆弱性への攻撃

近年，携帯電話や携帯ゲーム機等の組み込み機器を対象としたウイルスが出現しており，脆弱性対策が必要な状況が続いている．

5.8.1 脅威

2007年にJVN（Japan Vulnerability Notes）で公開された組み込み機器の脆弱性は3件であり[2]，それらはルータ等のネットワーク機器のWeb設定画面に対するクロスサイト・スクリプティング等の典型的なWebアプリケーションの脆弱性であった．攻撃技術は日々進化しているため，リリース時点でのセキュリティ対策だけでは不充分であり，組み込みアプリケーションに潜んでいる脆弱性が発見されることもある．

5.8.2 対策

1） 組み込みアプリケーションのアップデート

新しい攻撃や組み込みアプリケーションに潜んでいる脆弱性に対しては，ベンダーが公開する情報を収集し，組み込みアプリケーションのアップデートを行う．現在は，組み込みアプリケーションの更新機能を持った機器もありアップデートが容易になっているが，5.5節のセキュリティパッチ対策と同様の考慮が必要である．アップデート版のリリース情報を入手してからアップデートするまでの動作確認を含めた手順を定めておき，手順に則り実施することが必要である．

2） 組み込み機器への接続制限

ネットワーク構成や接続許可設定等を行って，組み込み機器への接続を必要最小限の機器に限定する．ただし，外部と接続するルータのWeb設定画面に脆弱性が発見された場合は，接続制限対策が有効とならないこともある．

5.9 脆弱なパスワードの利用

パスワード認証は比較的導入が容易なため，依然多くのシステムで利用されているが，不適正なパスワードの取扱いによるセキュリティ上のリスクは大きい．従って，パスワードで利用者を認証するシステムを開発する際には，システムの安全を守るため，パスワードに関する様々なポリシーを実現する機能を盛り込む必要がある．

5.9.1 脅威

脆弱（簡単）なパスワードを使用すると，他人がパスワードを容易に類推可能である．また総当り攻撃や辞書攻撃によってパスワードを入手し，本人になりすまして不正アクセスを行い，情報漏えいやシステム破壊等の様々な不正行為を引き起こす恐れがある．

IPAへの不正アクセス届出状況によると，2008年4月以降においても，不正アクセスの原因の約30%は，IDおよびパスワードの管理不備である．

5.9.2 対策

安全なパスワード管理を実現するための要件を以下に示す．

1） 安全なパスワード認証機能を備える

a） システムの全ユーザに対して認証機能を提供する．

b） ユーザIDは一人につき一個付与する．

c） 入力されたパスワードは非表示（アスタリスク等）にする．

d） ユーザIDまたはパスワード誤入力時のエラーは，正当な値が類推できる内容を表示しない．

e） 同一ユーザIDによるマルチログインを抑止する．

f） 初期パスワードは初回ログイン時に強制変更させる．

g） 一定回数連続して認証に失敗した場合，アカウントをロックアウトする．

h） パスワードの有効期限を設定し，有効期限が到来したら強制変更させる．

2） パスワード文字列の複雑性実現機能を備える

a） パスワードの最小桁数を設定する．

b) パスワードの文字種（英・数・記号）混在を必須とする．
c) 以前使用したパスワード文字列の再設定を一定世代禁止（履歴管理）する．
d) パスワードの変更が可能になるまでの最短日数を指定する．
e) 簡易な文字列（1234，password 等）を禁止する．
f) パスワードの設定および利用時に，利用者が遵守するべきセキュリティ要求事項（類推しづらい文字列にする，定期的に変更する等）を表示する．

3) パスワード認証の強化機能を備える
a) パスワードの盗聴対策（OTP[*13]，CHAP[*14] 等）
b) 二要素認証によるユーザ認証精度の向上（トークン所持とパスワード等）
c) 生体認証との組み合わせによる認証精度の向上（指紋，手形，網膜パターン，静脈パターン，顔認証，筆記パターン，キーストローク等）

例えば，システムのパスワードポリシーとして
- パスワードは 8 文字以上とし，英数字と記号を混在させること．また，辞書に載っている単語でないこと．
- パスワードは 90 日毎に変更し，以前に使用したパスワードは三世代の間使用しないこと．

等があった場合，上記 1)～3)の機能が実装されていれば，このポリシーを利用者に強制的に適用させることができる．

ここで忘れてはならないのが，パスワード失念対策である．パスワード管理者が失念者の本人確認を行った上，初期パスワードを発行する等の措置が必要になるが，本人確認の方法，初期パスワードの伝達方法等運用に依存する部分が多く，運用手順を備える必要がある．

5. 10　DNS サーバの脆弱性への攻撃

DNS とは，人が覚えやすいドメイン名と，コンピュータが他のコンピュータと通信する際に使用する IP アドレスとを相互に変換するシステムであり，インターネット通信において必須のシステムである．それゆえ常に攻撃対象となりやすい．

5. 10. 1　脅威

1) サービス妨害攻撃

2006 年に大規模な攻撃が観測されたもので，公開されている DNS キャッシュサーバを踏み台として，その何十倍ものデータを攻撃対象の DNS に送信し，攻撃対象をサービス不能状態にする．DNS の停止により，企業の Web サイトにおいて，ビジネス機会の損失が発生する等の被害が生じる．

2) DNS キャッシュ汚染

2008 年前半に世界中が大騒ぎになった DNS の脆弱性である．DNS の「トランザクション ID」および「UDP ソースポート番号」の使用方法に設計上の欠陥が存在し，この脆弱性を突いた攻撃により DNS キャッシュが汚染され，フィッシング詐欺に利用された．

DNS キャッシュ汚染とは，偽装したドメイン情報を DNS サーバのキャッシュに記憶させることを指す．想定される被害としては，悪意のあるユーザにより不正なサイトに誘導され，フィッシング/ファーミング[*15] に利用されることが挙げられる．この脆弱性は，「トランザ

クション ID」の乱数が予測可能であること，「UDP ソースポート番号」が固定されていることに起因する．これを悪用し，攻撃者は DNS サーバへ偽装した応答情報を送信することにより，不正な IP アドレスを DNS サーバのキャッシュに登録することが可能となる．

5. 10. 2　対策

1）　サービス妨害攻撃対策

この攻撃は，多数のリカーシブ・クエリー（再帰問い合わせ）を攻撃対象の DNS サーバに送りつけることで行われる．これを防ぐために，企業ネットワークに設置する DNS サーバに対し，以下の基本的な設定を行う．

a）　外部 DNS サーバ（インターネットに公開する情報のみ保持）と内部 DNS サーバ（内部の情報のみ保持）を用意する．

b）　企業（DMZ）に設置する DNS は，不要であればインターネットからのリカーシブ・クエリーは受け付けない．

c）　DNS サーバの障害対策として，セカンダリ DNS サーバを用意する．

・プライマリ DNS サーバ側から，予め指定されたセカンダリ DNS サーバ以外へはゾーン転送を行なわないようにする．

・外部 DNS のセカンダリは，自社とは異なる ISP 等に設置されている DNS サービスを利用する．

2）　DNS キャッシュ汚染対策

この脅威は，リカーシブ・クエリーに対する正しいトランザクション ID および UDP ソースポート番号を含んだ偽装応答を受け取ることにより発生する．よって以下の対応を行う．

a）　DNS 製品のベンダーが提供する以下の修正パッチを適用する．

・トランザクション ID に用いる乱数を予測困難にする．

・送信クエリに使用する UDP ソースポート番号を乱数化する．

b）　a)の根本的な対応策として，DNSSEC（DNS Security Extension）を導入する．

DNSSEC とは，DNS のセキュリティを向上させるための拡張仕様である．サーバとクライアントの間で交わされるメッセージが改ざんされていないことを保証するため，メッセージのハッシュ値を公開鍵暗号方式で暗号化しメッセージとともに送る．届いたメッセージからハッシュ値を求め，復号したハッシュ値と比較することで，偽りのメッセージか否かを判定する．ハッシュ値が一致すれば，改ざんが行なわれていないことが証明できる．

6.　セキュリティ対策実装上の留意点

6. 1　セキュア・プログラミングの組織的な実施

システム開発にあたっては，セキュリティ対策コードをしっかりと実装すべきと 5. 1 節で述べたが，どのような開発者でも一定水準のセキュア・プログラミングが行えるようにするためには，セキュア・プログラミングのポイントを体系立ててまとめた開発基準や開発ガイドを予め作成し，開発関係者が共有できるようにすること，また，このような基準やガイドを備えても開発者が実践しなければ意味がないので，企業内でセキュア・プログラミングに関する教育

を実施し，開発関係者にその重要性を周知徹底することが必要である．さらに開発管理プロセスにおいて，セキュア・プログラミングが遵守されているか否かを，基本設計終了段階あるいは詳細設計終了段階等のチェックポイントでレビューするための体制を備える必要がある．最後に，システム統合テスト段階において脆弱性診断ツール等でセキュア・プログラミングがなされていることを検査し，脆弱性が検出された際には速やかに対応する．これらを開発初期段階から組織的・計画的に行うことが肝要である．

6.2　内部犯罪，過失への対応

5章で重大な脅威に主眼を置いたセキュリティ対策の技術的・運用的対策を述べたが，セキュリティ対策全般に亘って忘れてはならないのが悪意の内部犯罪や過失等への対応である．これらは，J-SOX法に基づく監査等においても，比較的，監査人から指摘されやすいポイントとなっている．

因みに「2007年 情報セキュリティインシデントに関する調査報告書」[11]によると，個人情報の漏えい原因比率（漏えい人数比率）は，「内部犯罪・内部不正行為」によるものが28%，「管理ミス」によるものが64%を占めており，内部犯罪や過失の割合は依然大きな比率を占めている．

以下に考慮すべき対策のポイントを述べる．

1)　特権を有するシステム利用者の統制を厳密に行う

システム利用者の中でも特権を有するシステム管理者等は，あらゆるファイルを閲覧，変更することが可能であり，その結果，特権を有する一人の人間が悪意を持てば，正規の権限での不正行為が実行可能である．また，操作ログ等をも削除できるので，不正行為の発見も困難となる．悪意がなくても，不注意でデータを変更してしまう可能性もある．従って，特権を有するシステム利用者に対しては以下の統制が必要である．これらの統制は，表3で示した各種フレームワークにおいても求められているところである．

a)　重要な処理における権限を分離（職権分離）する．例えば，ユーザIDの権限付与承認者と登録実施者を分離し，それぞれの職権毎に異なるユーザIDを付与する．

b)　特権的アクセス権限の設定は，責任者の承認に基づいて行い，付与の理由および権限者は適切かを確認する．

c)　特権的アクセス権限の必要性の見直しを定期的および人事異動や組織改編時に行う．

d)　特権的アクセス権限の使用状況は厳格に管理する．例えば，ログ等（下記項番3）参照）により定期監査を実施する．

2)　変更管理を適切に行う

どんなにシステムのセキュリティ対策を万全に行っても，不正なプログラムや誤ったデータを容易に本番環境に載せることができるのであれば，全てのセキュリティ対策は水泡に帰する．そこで，プログラムの修正やOS，データベース等に対する各種パッチの本番リリースにあたっては以下を考慮する．

a)　間違った，あるいは不正なプログラムやデータが責任者の承認なしに本番環境にリリースされないこと．

b)　変更管理プロセスにおいて，内部の意図的な不正または意図的なプロセスの迂回等を検知できること．

3） 誤った行為あるいは不正行為を検知，追跡できるような管理プロセスを備える

企業システムに係る処理が適切に実行されていることをモニタリングすることは，不正行為の検知のみならず予防，抑止にも繋がる．また，デジタルフォレンジックを正しく行うためにも必要である．

a） ログシート，処理報告，日誌等の作業記録は管理者の検証を受け，一定期間保管する．

b） 監視ログを分析，レビューし，報告する運用手順を確立する．特に注意すべき監視項目の例を以下に示す．

・失敗アクセス
・長期間使用されていないユーザ ID の再使用
・特権 ID の割当てと使用状況
・外部からの不正なネットワークアクセス

c） ログの保全（不正消去，改ざん防止）機能を備える．

・ログファイル，作業記録へのアクセス制御
・追記・更新不可な記録媒体への記録

6.3 運用やパフォーマンスへの影響

セキュリティ対策と利便性はトレードオフの関係にあることから，セキュリティ対策の実装は，ほとんどの場合運用やパフォーマンスに影響をおよぼすが，その中でも特に影響が大きいものとして，暗号化とログ採取がある．

暗号化は，アプリケーションで行うか基盤で行うかの検討が必要である．遵守しなければならない基準やポリシーにおいてアプリケーションでの暗号化を求めている場合は，セキュア・プログラミングガイド等に反映し，確実に暗号化が行われるようにしなければならない．基盤で実施する場合は，ハードウェアやソフトウェアの選択時に，システムが求めるパフォーマンスを保証できるかを検証する必要がある．

ログ採取は，対象とするログの種類，ログ採取レベル等によりパフォーマンスに大きな影響をおよぼすため，そのログの必要性を考慮し，採取するログやレベルを決定する必要がある．また，ログのアーカイブや保管場所等の運用を考慮した収集方法の検討も重要である．さらに，ログの集中管理，保管用の機器やソフトウェアの選定も早期に行うことにより，システムの基盤構築に大きな影響を与えるネットワーク構成等の設計の手戻りや，機器やソフトウェアの購入による追加費用の発生を防ぐことができる．

6.4 セキュリティ対策によって発生する別のリスク

あるリスクの軽減のために実施したセキュリティ対策が，新たなリスクを発生させることがある．その例として，6.3 節で述べた暗号化とログ採取，セキュリティパッチやウイルス定義ファイルの適用，組み込みアプリケーションのアップデートが挙げられる．

暗号化を行った際に発生する新たなリスクとしては，復号に係わるもの，暗号鍵に係わるものがある．暗号化した情報の保管期間中は，その内容を確認するために復号可能であることが求められるが，保管期間が長くなればなるだけ，復号可能状態を維持することが難しくなる．開発初期段階では，暗号化の対象や方法を安易に決めることなく，情報の重要度と保管する媒体の特徴を考慮することが求められる．また，暗号化した情報を権限のない者に閲覧させない

よう，暗号鍵の安全な保管方法や，暗号鍵の有効期間を考慮した運用の検討が必要である．

ログについても，保管期間中は内容確認が可能となるような対策の検討が必要である．ログの保管期間が長期になる場合，ログを保管している媒体に対応した機器がベンダーのサポートを受けられなくなることが起こりうる．ログの保管媒体を決定する際には，このようなリスクが発生することを考慮することが必要である．

セキュリティパッチやウイルス定義ファイルの適用および組み込みアプリケーションのアップデートは，これを行うことにより実運用環境を変更することになるということを意識する必要がある．実運用環境の変更であるため，ベンダーから提供されたセキュリティパッチ等を適用する前に，検証環境での動作確認が必要である．開発初期段階で運用時の検証環境をどの程度まで準備しておくかを検討することにより，機器やソフトウェアの購入および設置場所の確保に伴う追加費用の発生を防ぐことができる．

7. セキュリティ対策の追加検討

5章および6章において，システムやネットワークのソフトウェア構成や機器構成の情報資産およびシステムの脅威が明確になっていない開発初期段階で設計に盛り込むべきセキュリティ対策とその実装上の留意点について述べた．この段階でセキュリティ設計を行うことにより，システムの機能要件からは導き出されない，セキュリティ対策を実施するためだけに必要な機器やソフトウェアを早期に追加できる．

システムの開発初期段階を過ぎると，システムやネットワークのソフトウェア構成や物理機器構成も決定し始め，情報資産の特定が可能となる．また，システムの機能要件が明確になってくると，想定する脅威も特定される．情報資産や脅威が特定されると，一般的なセキュリティ対策の検討時に行われるリスク分析が可能となる．そこで，リスク分析を実施し導き出されたセキュリティ対策と，開発初期段階で対応したセキュリティ対策とを比較し，不足している対策を追加する．この段階でリスク分析を行うことで，開発初期段階に検討したセキュリティ対策を実施するための機器やソフトウェアについても，リスク分析の対象にできる．リスク分析は，新しい情報資産が追加になった場合や考慮していなかった新たな脅威が追加された場合等にも再度実施し，現在のセキュリティ対策が有効であるか確認する必要がある．しかしながら，開発初期段階において重大な脅威に対する必要最小限のセキュリティ機能は盛り込み済みのため，新たな脅威に対しては不足部分の追加的対応で済むことが多い．

本稿で述べた重大な脅威に焦点をあてたセキュリティ設計手法は，必要最小限のセキュリティ機能を確保しつつ，システムの大幅な設計変更による手戻りを防止できるという観点において合理的である．

8. お わ り に

本来のセキュリティ対策は，企業において守るべき情報資産を洗い出し，次にシステムの構成要素，利用者，物理的現況等を加味しながら想定される脅威を洗い出し，脅威毎のリスク分析を経て，リスクに見合った適切なセキュリティ要件を決定，それに基づきセキュリティ設計を行い，構築，運用，維持継続していくものである．

しかしながら，システムを開発する場合，未だ形になっていないシステムに対して，守るべき情報資産やその重要度，想定される脅威を洗い出すのは困難であり，過去の経験や思いつき

で過剰なセキュリティ対策を実施するか，またはセキュリティ対策の考慮を後の工程に回すという事態に陥りやすい．結果として，過剰なセキュリティ対策を実施した場合は利便性低下，開発費用の増大，運用効率の低下等の弊害が生じ，セキュリティ対策の考慮を後工程に回した場合はシステム開発後半における大幅な設計変更による手戻り発生等の結果を招く．別の問題として，根拠のないセキュリティ対策では，経営陣が対策を実施しなかった場合のリスクを認識しづらく，セキュリティ対策にかかる費用が多すぎて承認されないということも起こりうる．

本稿では対象をシステム開発の初期段階と限定したが，本稿で述べたセキュリティ設計手法を応用することにより，現状のセキュリティ対策が重大な脅威に対抗できているのかを確認することにも利用できる．特にセキュリティ対策が充分に行われていない企業にとっては，この手法で導き出された対策を実施，その後守るべき情報資産に対するリスク分析を行い，その企業固有のセキュリティ対策を実施することにより，脆弱な箇所を放置する期間を短くしつつ，適切なセキュリティ対策を実施することが可能となる．

本稿が，システムへのセキュリティ対策を検討する際の参考になれば幸いである．

＊1　P2P ファイル交換ソフトウェアの一つ．同ソフトウェアを利用するユーザ間でファイルをお互いに交換することができる．
＊2　コンピュータを遠隔操作することを目的に作成されたソフトウェアで，ウイルスのように他のコンピュータに感染する機能のあるもの．ボットに感染したコンピュータは，外部からの指示に従い，他のサイトへの攻撃や，スパイウェアとしての活動などを行う．
＊3　製品開発者による脆弱性の修正前に行われる攻撃．
＊4「銀行からのお知らせメール」などと嘘をついて偽の Web サイトに誘導し，口座番号やパスワードを利用者に入力させて盗む，詐欺の手法．
＊5　データベースと連携した Web アプリケーションにおいて，問い合わせ命令文の組み立て方法に問題があるとき，Web アプリケーションへ宛てた要求に悪意を持って細工した SQL 文を埋め込み（Injection），データベースを不正に操作する攻撃．
＊6　コンピュータウイルス・スパイウェア等の悪意あるソフトウェア．
＊7　Web サイトに設置し，Web アクセスしてきた PC にマルウェアを強制的にインストールするソフトウェア．攻撃者は，XSS を用いて正規の企業が運営する Web サイトを改ざんし，MPack を設置した Web サイトに誘導するコードを仕掛けるケースが多い．
＊8　Mpack と基本機能は同じであるが，攻撃者が簡単に操作できるようにする仕組みを備えているのが特徴．
＊9　一つの Web ページ内に別の Web ページを表示させる仕組み．
＊10　Web ページ上で，HTML だけではできない様々な機能を実行するための簡易的なプログラムコード．
＊11　ユーザから入力可能なデータ（ファイル名や，ディレクトリ・パス名）を使って URL が構成される場合，その入力データに開発者側が予期していない絶対パスや相対パスを含んだファイル名や，ディレクトリ・パス名を指定して，本来公開する意図のないファイル等に不正にアクセスする攻撃手法のこと．
＊12　利用者や管理者の意図に反してインストールされ，利用者の個人情報やアクセス履歴などの情報を収集するソフトウェア．キーボードで入力された文字や画面イメージを記録する機能を持つものもある．
＊13　One Time Password（ワンタイムパスワード）の略．一回限り有効なパスワード認証システムのことでパスワードの盗聴対策に用いられる．
＊14　Challenge Handshake Authentication Protocol の略（チャップ）．クライアントがサーバからのチャレンジに対するレスポンス生成し，それをパスワードとしてサーバに返信する認証プロトコルのことで，パスワードの盗聴対策として用いられる．
＊15　フィッシング詐欺の手口の一つ．フィッシングは偽の案内メール等でユーザを誘導するが，ファーミングは，DNS サーバのキャッシュに偽装したドメイン情報を記憶させ，そのサーバを利用するユーザを丸ごと偽のサイトに誘導する．

参考文献
［1］「情報セキュリティ白書　2007年版　―10大脅威　「脅威の“見えない化”が加速する！」―」，独立行政法人　情報処理推進機構　セキュリティセンター，第2刷，2007年9月
［2］「情報セキュリティ白書　2008　第Ⅱ部　10大脅威　ますます進む『見えない化』」，独立行政法人　情報処理推進機構　セキュリティセンター，2008年5月
［3］「JIS Q 27001：情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項」，日本規格協会，2006年5月
［4］「JIS Q 27002：情報技術―セキュリティ技術―情報セキュリティマネジメントの実践のための規範」，日本規格協会，2006年5月
［5］「情報セキュリティ管理基準」，経済産業省，2003年4月
［6］「政府機関の情報セキュリティ対策のための統一基準」，内閣官房情報セキュリティセンター，第3版，2008年2月
［7］「安全対策基準・解説書」，金融情報システムセンター，第7版，2006年3月
［8］「システム監査指針」，金融情報システムセンター，第3版，2007年3月
［9］「Payment Card Industry (PCI) Data Security Standard PCI データセキュリティ基準」，国際ペイメントカードブランド（American Express/JCB/MasterCard/Visa），バージョン1.1（日本語暫定版），2007年2月
［10］「2006年　情報セキュリティインシデントに関する調査報告書」，NPO日本ネットワークセキュリティ協会，Ver.02.1，2007年10月
［11］「2007年　情報セキュリティインシデントに関する調査報告書」，NPO日本ネットワークセキュリティ協会，Ver.1.2，2008年6月
［12］「標的型攻撃について」，有限責任中間法人　JPCERT　コーディネーションセンター，2007年6月
［13］「近年の標的型攻撃に関する調査研究　―調査報告書―」，独立行政法人　情報処理推進機構　セキュリティセンター，2008年3月
［14］「複数の組み込み機器の組み合わせに関するセキュリティ調査報告書」，独立行政法人　情報処理推進機構　セキュリティセンター，2008年1月
［15］「財務報告に係る内部統制の評価および監査の基準並びに財務報告に係る内部統制の評価および監査に関する実施基準の設定について（意見書）」，金融庁企業会計審議会，2007年2月
［16］「複数のDNS実装にキャッシュポイズニングの脆弱性」，Japan Vulnerability Notes，http://jvn.jp/cert/JVNVU800113/index.html

執筆者紹介
八津川　直伸（Naonobu Yatsukawa）
1980年福井大学工学部電子工学科卒業．同年日本電信電話公社入社，大容量光ファイバー伝送システムの施設設計を担当．1985年日本ユニシス株式会社（当時，日本ユニバック株式会社）入社．以来，電気通信の自由化に伴い，コモンキャリアとしての電気通信事業（U-netサービス）の企画推進，汎用機用通信制御装置ソフトウェア（DCP/TELCONシリーズ）の開発および保守，セキュリティ商品の開発および保守，J-SOX対応支援等を経て，セキュリティシステム構築支援を担当．現在，共通利用技術部に所属．CISSP.

石　野　貴　子（Takako Ishino）
1989年日本ユニシス(株)入社．金融システム開発，インターネット接続環境における技術的セキュリティ対策適用業務，ISMSおよび個人情報保護等の情報セキュリティマネジメントシステム構築支援業務を経て，技術・マネジメント両観点からの情報セキュリティコンサルティング業務を担当．現在，共通利用技術部システム管理技術室に所属．CISSP.