JNSA セキュアシステム開発ガイドライン

「Web システム　セキュリティ要求仕様（RFP）」編　β版

2005 年 12 月 5 日

セキュアシステム開発ガイドライン WG

もくじ

Copyright (c) 2005 NPO 日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

1. はじめに

Web アプリケーションに対する企業と社会の需要と依存度はますます高まっているが、一方で Web アプリケーションの脆弱性をついた不正アクセスが後をたたない。

JNSA をはじめとするセキュリティ団体やソフトウェアメーカーの啓発により、ネットワークやホストレベルのセキュリティについては、ある程度、「ここまでは必須の対策」というレベルについての社会的なコンセンサスは醸成されてきている。たとえばデスクトップ PC であれば、アンチウイルスソフトのインストールと定義ファイルの更新、Windows Update を初めとした OS とソフトウェアを最新のバージョンに保つこと、見知らぬ人から届いたメールは不用意に開かない、等のユーザーレベルの対策は、いまや「常識」と言っても問題は無いであろう。ネットワークレベルの対策としては、FireWall の導入、無線 LAN アクセスポイントのセキュア化、等についても、発注者側も、機器を納入するベンダー側も当たり前の作業として実施しているはずである。むしろこれらの対策を施していなかったのであれば、ウイルスに感染したり、ネットワークに不正侵入されたとしても、その責任が発注者側にあるのか（コストをけちった？）、受注者側にあるのか（設定をミスした）はある程度明確であり、対策そのものが明示的に要求仕様に含まれていなかったとしても、社会的に必須の対策か、どうかという事が争点になることはまずないはずだ。

ところが昨今、増加の傾向にある Web アプリケーションの脆弱性を突いた攻撃は、その対策の必要性についての社会的コンセンサスが業界内でも構築されていないのが現状ではないだろうか。ここでいう Web アプリケーションに対する攻撃とその対策は、例えば SQL インジェクションやクロスサイトスクリプティング、およびセッション管理に関する問題や、アプリケーション固有の機能に関する問題を指している。これらは Web アプリケーションによって実現したい機能からみれば「非機能要件」ととらえられ、要求仕様として明示的にされていない現状にある。そのため、ベンダー側としても明示的に対策に関する提案と、そのコストを明示することが困難な状況にある。ユーザーにしてみれば社会的に必要十分な対策をとる意思があっても、その基準が無いためにベンダーの提案を検証することができない、という状況も作り出している。

こういった状況に鑑み、JNSA では発注者側（ユーザー）側と受注者（ソフトウェアベンダー）とが共有できる Web アプリケーションのセキュリティ要求仕様について整理・提示することを試みることにした。

本ドキュメントは、発注者（ユーザー）に対しては、RFP（提案依頼書）に盛り込むセキュリティ対策のサンプルとして参照していただけることを目指している。本ドキュメン

Copyright (c) 2005　NPO 日本ネットワークセキュリティ協会

トの作成にあたっては、JNSA の会員企業を中心とした、システム開発とネットワークセキュリティに携わる企業の方々によりレビューされているので、このドキュメントに記載されている内容を Web アプリケーションに実装することで、現時点で必要十分と言える対策を施していると考えていただいてよいだろう。受注者（ソフトウェアベンダー）にとっては、Web アプリケーションのセキュリティに関する要件を要件定義・基本設計の段階から盛り込んでいただくことにより、セキュリティに関する要件を「機能要件」として算出していただくことの裏付けの資料となるはずだ。また、本資料では要求仕様に対する「対策」については、それを記述することが目的ではないので、サンプルを記述するにとどめた。「対策」の提案については各ソフトウェアベンダーの特色を出していただき、大いに競争していただければよいと考えている。

本書の活用により、発注者（ユーザー）と受注者（ソフトウェアベンダー）間での Web アプリケーションに対するセキュリティ対策についての「常識」が醸成される事を願ってやまない。

メンバー一覧

エー・アンド・アイ システム株式会社　洞　昌伸
NEC ネクサソリューションズ株式会社　小峰 光
NEC ネクサソリューションズ株式会社　中西克彦
京セラコミュニケーションシステム株式会社　徳丸 浩
株式会社 シーエーシー　岩崎 貴行
新日鉄ソリューションズ株式会社　田京義英
大日本印刷株式会社　小野　潤
TIS 株式会社　塩田　英二
株式会社ディアイティ　山田　英史
日本アイ・ビー・エム株式会社　平山　敏弘
日本オラクル株式会社　北野晴人
株式会社日本システムディベロップメント　大鐘　博子
日本電信電話株式会社　廣瀬　洋一
日本ユニシス株式会社　森　駿
日本ユニシス株式会社　高橋 謙司
マイクロソフト株式会社　松岡正人
みずほ情報総研 株式会社　中山 和郎
株式会社ラック　倉持 浩明
株式会社ラック　大野祐一
株式会社ラック　丸山司郎（WG リーダー）

Copyright (c) 2005　NPO 日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

2. このドキュメントの目的

このドキュメントは、発注者（ユーザー）がベンダーに Web アプリケーションの提案依頼をかける際に、RFP（提案依頼書）に最低限、盛り込むべきセキュリティ対策について記述している。

従って、発注者（ユーザー）はこのドキュメントに記述されている要求仕様を自社の RFP に記載することができる。もちろん、このドキュメントに記載したのはベースラインとなる要求仕様なので、ここに書かれている内容を網羅したシステムを開発すれば、セキュリティ対策は万全、という訳では無いことに注意していただたい。

受注者（ソフトウェアベンダー）は、アプリケーションの提案の際に、このドキュメントに記載されている内容に対する対策を、具体的な対策案として提案に盛り込むことができる。本書に書かれているような内容について、ユーザーから明示的に提示が無かった場合は、実施するセキュリティ対策について、要件定義から基本設計の段階でユーザーと合意し、要求仕様として整理する際のガイドラインとして利用することができる。それは非機能要件を機能要件化することであり、詳細設計・開発・テスト工程の見積もりにも流用できるはずだ。また、なんらかの理由で対策を施さなかったものについては、対策を実施しないことによりアプリケーションに残存する脅威についてユーザーと合意しておくことで、免責事項とすることができるはずだ。

Copyright (c) 2005　NPO 日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

3. このドキュメントの対象読者

１）発注者（ユーザー）のうち、RFP を記載する・ベンダーの提案を評価する立場にある方

２）受注者（ソフトウェアベンダー）のうち、提案書を記載する立場にある方、マネージャの方、営業の方

4. このドキュメントに含まれていること、含まれていないこと

このドキュメントでは Web アプリケーションに関するセキュリティ対策のうち、アプリケーションの設計とプログラミングで回避可能な既知の脆弱性について、Web アプリケーションの要求仕様として一般的に盛り込むべきと考えられる内容について記載している。要求仕様に対する対策については、サンプルを提示しているが、これは要求仕様が意味する内容について理解していただく為に記載している。要求仕様に対する対策については、それぞれのベンダーが特色を出した提案を記載することを期待している。

反対に、ネットワークやホストレベルで対策すべきセキュリティ対策については記載していない。また、運用や人的セキュリティ対策についても対象外としている。また、RFP としては、契約面に関する事項や、プロジェクトの運営、開発プロセスに関しても記述があるべきだが、それらについては盛り込まれていない。

Copyright (c) 2005　NPO 日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

5. Web システム・セキュリティ要求仕様（RFP）

１）前提条件

この Web システム要求仕様は、イントラネットまたは、インターネットに公開し、利用される Web アプリケーションシステムを想定している。

システムの構成としては、一般的な三層構造（We サーバ/アプリケーションサーバ/DB サーバ）によって構成されるものを想定しているが、特定の言語／製品に限定はしていない。

２）Ｗｅｂシステムの類型化

システムを新たに作成するにあたって、「何を目的として、どのような機能のシステムを、いくらくらいの予算で作成するか。」を、ユーザの視点から作成し、開発業者に提案依頼を行うものを、ＲＦＰと考える。

この中の「機能」、「予算」という部分によって、個々のシステムに必ず盛り込まれなければならないセキュリティ要件は明らかに異なるが、ここでは、セキュリティ要件に影響を与える要因を抜き出し、システム構成を類型化したうえで、対応レベルを記載することとする。

Copyright (c) 2005　NPO 日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

6. セキュリティ対策への主要な影響要因

○ インターネットなど、**外部ネットワークへの公開**の有無

○ **機密情報取り扱い**の有無

個人情報（プライバシー情報）、決済情報、などを取り扱うか否か。

○ システムの利用者の類型化

- **「不特定多数」**：特に認証を必要としない。もしくは、認証は必要とするが、その ID を発行する際の個人の特定は行われない。

  例）

  - ✧ 認証を必要としない、インターネット上のポータルサイト、掲示板など。
  - ✧ ID は発行するが、個人の特定をせず、またメールでの存在確認を行うとしても、Free メールを許すなど、事実上その ID から個人の特定が困難な場合。
  - ✧ 認証がなされないイントラネットシステム
    - ・認証者のみ：利用者すべての顔が把握できる人数（数十人）
    - ・管理範囲内：アクセスを許可された範囲のシステム利用者のみ

- **「特定多数」**：個人を特定する情報を元に発行された ID などで認証を行う場合。

  例）

  - ✧ インターネットショッピングサイト、オンラインバンキング、社内ワークフローなどの業務システムなど。

- **「特定限定」**：前述の「認証者」であり、かつ人的にも管理可能な範囲内。

例）

- ✧ システム以外の人的な手段（目で見える範囲であるなど）において、そのユーザの行動を把握できる範囲。比較的少数のユーザを想定

○ 対応要件の定義

類型化したシステムによって、対応すべきレベルを 3 レベルで定義する。

- 必須
- 推奨
- 任意

Copyright (c) 2005　NPO 日本ネットワークセキュリティ協会

パターン１：対策手法からの RFP 記載例

1. 入力検証および不正データ入力時の無効化

ユーザが悪意のある文字列を組み込んでアプリケーションを攻撃し、本来権限のないユーザがデータにアクセス（情報の入手、情報の改ざんなど）できないように、以下を考慮した対策を提案すること。

- 悪意ある文字列の入力チェックもしくは無害化
- SQLインジェクションの防御
- コマンドインジェクションの防御
- パストラバーサルの防御
- パラメータ改ざんの防御
- クロスサイトスクリプティングの防御
- バッファオーバフローの防御

2. 認証と承認

なりすましや管理者権限の不正取得などができないような措置を講ずること。

- パスワード等を用いてユーザを認証することにより、各ユーザに対して許可されない行為は防止すること。

3. 適切なパスワード、セッション情報

パスワードやセッション情報を不正に使用されないよう、適切な措置を講ずること。

- パスワード、セッション情報は、有効期限、推測されにくに文字列、一定以上の桁数などの制限を設けて不正使用を防止すること。
- 高い頻度でパスワード照合に失敗するなど不正使用の可能性が疑われる場合は、アカウントをロックする等して不正使用を防止すること。

4. 機密データの暗号化

機密データを暗号化し、万一のデータ流出時にもデータ内容を保護できるように、以下を考慮した対策を提案すること。

- 個人情報や社外秘などの重要なデータについての暗号化
- 万一の盗聴や盗難および紛失の際のデータ解読の不可能

Copyright (c) 2005　NPO 日本ネットワークセキュリティ協会

5. 機密情報へのアクセス制御と情報漏えい防止

機密情報やアカウント情報にアクセスできないようにアクセス制御を実施し、機密情報の漏えいや　データの改ざんが行なわれないように、以下を考慮した対策を提案すること。
また印刷物の持ち出しや外部メディアへの情報取り込み等の物理的な情報漏えいを防止するため、プリントアウト制御・外部メディアへの制御等についての対策についても提案すること。

- 社員や派遣社員および協力会社などの内部の人間による機密情報漏えいの防止
- 機密情報に対する、不正な変更・改ざんの防止または抑止
- 本来権限のないユーザによる機密情報へのアクセスを防止
- 本来権限のないユーザによるアカウント情報へのアクセスを防止
- プリントアウト後に、紙を持ち出す等による物理的な機密情報漏えいの防止および抑止
- テープ・CDやUSBメモリーなどの外部媒体にコピーすることによる機密情報漏えいの防止および抑止
- 内部情報の記録された外部媒体を物理的に持ち出すことの防止および抑止

6. 監査とログ記録

各種ログ記録を確実に取ることにより、万一事故が発生した場合に追跡の基礎情報を取得可能な様に、以下を考慮した対策を講じること。またログへのアクセスは権限者のみに限定される対策についても提案すること。

- ユーザの操作実行の否認を、ログの分析により防止。
- 攻撃者が痕跡を残さずにアプリケーションを悪用することを防止。
- 攻撃者によるログの改ざん、消去を防止。
- 各種ログの時系列整合性のために時刻同期をおこなうこと。

※ 本RFPで求められない事項に関しても、本システムに採用すべき対策等があれば追加で提案してください。

Copyright (c) 2005　NPO 日本ネットワークセキュリティ協会

パターン２：現象面からの RFP 記載例

1. システムダウン･レスポンス低下防止策

外部から攻撃されても一定時間以上のシステムダウンを起こさないように、以下を考慮した対策を提案すること。

- DoS、DDoS攻撃によるシステムダウン、レスポンス低下
- アクセス集中によるシステム／サービスのダウン、レスポンス低下
- OSのバグやセキュリティホールを利用した攻撃によるシステムダウン、レスポンス低下
- 不正侵入による悪意あるシステムダウン
- 故意／過失による高負荷処理に耐えられる構成

2. なりすまし･否認防止策

正規ユーザのIDを不正に取得するなどしてなりすましを行い、システムを利用することを防ぐ対策、行った注文処理などを事後に否認されないため、以下を考慮した対策を提案すること。

- ユーザIDやパスワードの推測、盗聴
- セッションハイジャック
- クロスサイトリクエストフォージュリ
- 事後否認の防止

3. 漏えい対策

情報漏えいを防止するため、以下を考慮した対策を提案すること。

- 通信経路上の盗聴
- 万一、データ盗難が起きた場合における安全策
- 正常な操作（権限を有する操作）における情報漏えい
- 人的ミスによる情報漏えい

4. 改ざん防止対策

コンテンツやデータ、通信内容の改ざんを防ぐため、以下を考慮した対策を提案すること。

- 通信系路上での通信データの改ざん
- コンテンツやデータの改ざん
- 各種ログファイルの改ざん

Copyright (c) 2005　NPO 日本ネットワークセキュリティ協会

5. ユーザへの被害対策

システムのユーザやサイトの閲覧者が、当サイトの直接的・間接的原因により、被害を受けることのないように、以下を考慮した対策を提案すること。

- クロスサイトスクリプティング
- フィッシング
- ウイルス・ワーム・スパイウェア等のユーザ・閲覧者への感染
- 迷惑メール対策（本システムが迷惑メールの発信に悪用されないこと）

6. 脆弱性対策

サーバやネットワーク機器、アプリケーションの脆弱性に起因する情報漏えいや改ざん・なりすましなどの脅威に対抗するため、以下を考慮した対策を提案すること。

- Webアプリケーションの脆弱性を利用した不正アクセス
- OSやミドルウェア等のパッチを適用するための適切な構成・対策
- 脆弱なサービスや設定による不正アクセスを防ぐ（要塞化）

7. 内部者対策

内部者による情報漏えい・改ざんを防止・抑止するため、以下を考慮した対策を提案すること。

- 内部者による故意の情報漏えい・改ざん等の防止
- 内部者による故意の情報漏えい・改ざん等の抑止
- 内部者のミスオペレーションに起因する漏えいや設定ミス等の防止

8. 全般的な対策

前出の脅威個々の対策ではなく、全般にわたる以下のような対策を提案すること。

- 攻撃検知・防御機能
- ログ・監査証跡の取得。システムのログ、アクセスログ、操作ログなどについてそれぞれどの項目・操作について取得するかを明確化すること。
- バックアップデータの保護策

9. セキュリティ運用

上記すべての対策に関して、セキュリティを維持・向上するための運用設計を行うこと。

※ 本RFPで求められない事項に関しても、本システムに採用すべき対策等があれば追加で提案してください。

Copyright (c) 2005　NPO 日本ネットワークセキュリティ協会

パターン３：脅威モデルからの RFP 記載例

1．なりすまし、データの改ざん、情報の漏えいに関して

なりすまし、データの改ざん、情報の漏えいの発生を軽減する方法と発生した場合に検知できうる仕組みの提供を提案してください。

2．サービスの低下、アクセス権の昇格に関して

悪意のDOS攻撃などによるサービスの低下やアクセス権の昇格による影響を軽減する方法に関して提案してください。

3．否認の防止に関して

更に記録として残す部分に関しては否認を防止するために必要な手段の提供を提案してください。

Copyright (c) 2005　NPO 日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

パターン１：　対策手法の視点からの必須度マトリクス

セキュリティ要件	インターネットなどの外部公開	有り				無し			
	機密情報（個人情報、決済情報など）	有り	無し			有り	無し		
	システムの利用者	-	不特定多数	特定多数	特定限定	-	不特定多数	特定多数	特定限定
1．入力検証および不正データ入力時の無効化									
	・悪意ある文字列の入力チェックもしくは無害化	必須	必須	必須	必須	必須	必須	推奨	推奨
	・SQLインジェクションの防御	必須	必須	必須	必須	必須	必須	推奨	推奨
	・コマンドインジェクションの防御	必須	必須	必須	必須	必須	必須	推奨	推奨
	・パストラバーサルの防御	必須	必須	必須	必須	必須	必須	推奨	推奨
	・パラメータ改ざんの防御	必須	必須	必須	必須	必須	必須	推奨	推奨
	・クロスサイトスクリプティングの防御	必須	必須	必須	必須	必須	必須	推奨	推奨
	・バッファオーバフローの防御	必須	必須	必須	必須	必須	必須	推奨	推奨
2．認証と承認									
	・パスワード等を用いてユーザを認証することにより、各ユーザに対して許可されない行為は防止すること。	必須	任意	必須	必須	必須	任意	必須	推奨
3．適切なパスワード、セッション情報									
	・パスワード、セッション情報は、有効期限、推測されにくに文字列、一定以上の桁数などの制限を設けて不正使用を防止すること。	必須	任意	必須	必須	必須	任意	必須	推奨
	・高い頻度でパスワード照合に失敗するなど不正使用の可能性が疑われる場合は、アカウントをロックする等して不正使用を防止すること。	必須	任意	必須	必須	必須	任意	必須	推奨
4．機密データの暗号化									
	・個人情報や社外秘などの重要なデータについての暗号化	推奨	任意	任意	任意	推奨	任意	任意	任意
	・万一の盗聴や盗難および紛失の際のデータ解読の不可能	推奨	任意	任意	任意	推奨	任意	任意	任意
5．機密情報へのアクセス制御と情報漏えい防止									
	・社員や派遣社員および協力会社などの内部の人間による機密情報漏えいの防止	必須	推奨	推奨	推奨	必須	推奨	推奨	推奨
	・機密情報に対する、不正な変更・改ざんの防止または抑止	必須	推奨	推奨	推奨	必須	推奨	推奨	推奨
	・本来権限のないユーザによる機密情報へのアクセスを防止	必須	推奨	推奨	推奨	必須	推奨	推奨	推奨
	・本来権限のないユーザによるアカウント情報へのアクセスを防止	必須	必須	必須	必須	必須	必須	必須	推奨
	・プリントアウト後に、紙を持ち出す等による物理的な、機密情報漏えいの防止および抑止	必須	任意	任意	任意	必須	任意	任意	任意
	・テープ・CDやUSBメモリーなどの外部媒体にコピーすることによる機密情報漏えいの防止および抑止	必須	任意	任意	任意	必須	任意	任意	任意
	・内部情報の記録された外部媒体を物理的に持ち出すことの防止および抑止	必須	必須	必須	必須	必須	必須	必須	必須
6．監査とログ記録									
	・ユーザの操作実行の否認を、ログの分析により防止。	必須	任意	推奨	推奨	必須	任意	推奨	推奨
	・攻撃者が痕跡を残さずにアプリケーションを悪用することを防止。	必須	必須	必須	必須	必須	必須	必須	推奨
	・攻撃者によるログの改ざん、消去を防止。	必須	必須	必須	必須	必須	必須	必須	推奨
	・各種ログの時系列整合性のために時刻同期をおこなうこと。	必須	必須	必須	必須	必須	必須	必須	推奨

Copyright (c) 2005　NPO 日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会

パターン２：　現象面の視点からの必須度マトリクス

セキュリティ要件	インターネットなどの外部公開	有り				無し			
	機密情報（個人情報、決済情報など）	有り	無し			有り	無し		
	システムの利用者	-	不特定多数	特定多数	特定限定	-	不特定多数	特定多数	特定限定
1．システムダウン・レスポンス低下防止策									
	・DoS、DDoS攻撃によるシステムダウン、レスポンス低下	任意	任意	任意	任意	任意	任意	任意	任意
	・アクセス集中によるシステム／サービスのダウン、レスポンス低下	任意	任意	任意	任意	任意	任意	任意	任意
	・OSのバグやセキュリティホールを利用した攻撃によるシステムダウン、レスポンス低下	推奨	推奨	推奨	推奨	推奨	推奨	推奨	推奨
	・不正侵入による悪意あるシステムダウン	必須	必須	必須	必須	推奨	必須	推奨	推奨
	・故意／過失による高負荷処理に耐えられる構成	推奨	推奨	推奨	推奨	推奨	推奨	推奨	推奨
2．なりすまし・否認防止策									
	・ユーザIDやパスワードの推測、盗聴	必須	任意	必須	必須	必須	任意	必須	必須
	・セッションハイジャック	必須	任意	必須	必須	必須	任意	必須	推奨
	・クロスサイトリクエストフォージュリ	必須	推奨	必須	必須	必須	推奨	推奨	推奨
	・事後否認の防止	推奨	任意	推奨	推奨	推奨	任意	推奨	推奨
3．漏えい対策									
	・通信経路上の盗聴	必須	任意	必須	必須	必須	任意	必須	必須
	・万一、データ盗難が起きた場合における安全策	推奨	推奨	推奨	推奨	推奨	推奨	推奨	推奨
	・正常な操作（権限を有する操作）における情報漏えい	必須	必須	必須	必須	必須	必須	推奨	推奨
	・人的ミスによる情報漏えい	推奨	推奨	推奨	推奨	推奨	推奨	推奨	推奨
4．改ざん防止対策									
	・通信系路上での通信データの改ざん	必須	必須	必須	必須	必須	必須	必須	必須
	・コンテンツやデータの改ざん	必須	推奨	推奨	推奨	必須	推奨	推奨	推奨
	・各種ログファイルの改ざん	必須	必須	必須	必須	必須	必須	必須	必須
5．ユーザへの被害対策									
	・クロスサイトスクリプティング	必須	必須	必須	必須	必須	必須	必須	必須
	・フィッシング	必須	任意	推奨	推奨	-	-	-	-
	・ウイルス・ワーム・スパイウェア等のユーザ・閲覧者への感染	必須	必須	必須	必須	必須	必須	必須	必須
	・迷惑メール対策（本システムが迷惑メールの発信に悪用されないこと）	必須	必須	必須	必須	必須	必須	必須	必須
6．脆弱性対策									
	・Webアプリケーションの脆弱性を利用した不正アクセス	必須	必須	必須	必須	必須	必須	必須	必須
	・OSやミドルウェア等のパッチを適用するための適切な構成・対策	必須	必須	必須	必須	必須	必須	必須	必須
	・脆弱なサービスや設定による不正アクセスを防ぐ（要塞化）	必須	必須	必須	必須	必須	必須	必須	必須
7．内部者対策									
	・内部者による故意の情報漏えい・改ざん等の防止	推奨	任意	任意	任意	推奨	任意	任意	任意
	・内部者による故意の情報漏えい・改ざん等の抑止	必須	必須	必須	必須	必須	必須	必須	必須
	・内部者のミスオペレーションに起因する漏えいや設定ミス等の防止	必須	推奨	推奨	推奨	必須	推奨	推奨	推奨
8．全般的な対策									
	・攻撃検知・防御機能	推奨	推奨	推奨	推奨	任意	推奨	任意	任意
	・ログ・監査証跡の取得。システムのログ、アクセスログ、操作ログなどについてそれぞれどの項目・操作について取得するかを明確化すること。	必須	必須	必須	必須	必須	必須	推奨	推奨
	・バックアップデータの保護策	推奨	推奨	推奨	推奨	推奨	推奨	推奨	推奨
9．セキュリティ運用									
	・上記すべての対策に関して、セキュリティを維持・向上するための運用設計を行うこと。	必須	必須	必須	必須	必須	必須	必須	必須

Copyright (c) 2005　NPO 日本ネットワークセキュリティ協会

パターン３：　脅威モデルの視点からの必須度マトリクス

セキュリティ要件	インターネットなどの外部公開	有り				無し			
	機密情報（個人情報、決済情報など）	有り	無し			有り	無し		
	システムの利用者	-	不特定多数	特定多数	特定限定	-	不特定多数	特定多数	特定限定
1．なりすまし、データの改ざん、情報の漏えいに関して									
	・なりすまし	必須	必須	必須	必須	必須	必須	必須	必須
	・データの改ざん	必須	必須	必須	推奨	必須	必須	必須	推奨
	・情報の漏えい	必須	必須	必須	推奨	必須	必須	必須	推奨
2．サービスの低下、アクセス権の昇格に関して									
	・サービスの低下	必須	必須	必須	推奨	必須	推奨	推奨	任意
	・アクセス権の昇格	必須	必須	必須	推奨	必須	必須	推奨	推奨
3．否認の防止に関して									
	・否認の防止	必須	任意	推奨	推奨	必須	任意	任意	任意

Copyright (c) 2005　NPO 日本ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨ協会