Webセキュリティ - 設計編:

Webシステムに必要なセキュリティ要件の組み込み

2006年1月30日

株式会社ラック
丸山司郎

index

- 背景
- 検討の経緯
- ユーザー目線でのセキュリティ要件
- RFPガイドラインの使い方

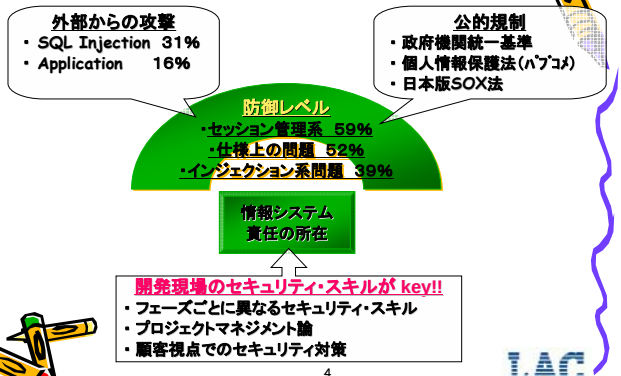
背景

- JNSAとは
  - 特定非営利活動法人（NPO）
  - 日本ネットワークセキュリティ協会
  - ネットワークセキュリティシステムに携わるベンダーが結集して、ネットワーク・セキュリティの必要性を社会にアピールし、かつ、諸問題を解決していく場として、2001年7月設立
- セキュアシステム開発ガイドラインWG
  - 2005年4月活動開始
  - 17名のメンバーによりβ版が完成（12/5）

2005年 事件のまとめ

- SQLインジェクション
  - 見過ごされていた弱点への攻撃
- スパイウエア
  - IT詐欺による金銭的な被害
- フィッシング
  - 金融機関を騙る詐欺で金銭的な被害
- Winny（Antinny）
  - アングラ領域における被害
- 人間系の犯罪
  - 元従業員や、委託先の社員による犯罪

セキュリティの実態と開発におけるセキュリティの重要性

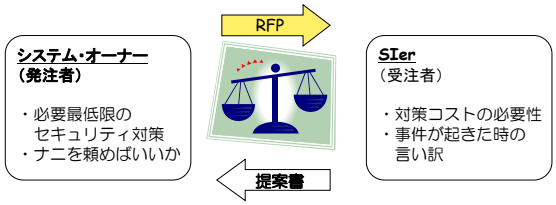


WGで目指すもの（表）

- 個人情報保護法施行を契機に、一般の情報システムへの管理責任が要求されるようになったが、そのレベルなどの明確な基準は存在しない。
- 開発システムのセキュリティ評価基準としてはISO15408が存在するが、どのレベルを選択すべきかが規程されていないことなどがから、実装は難しい。
- そこで、JNSAよりシステム開発に於けるセキュリティガイドラインを広く公開することにより、
  - 将来ISO15408等への国際標準への橋渡しをにらみながら、段階的に分かりやすく実施でき、
  - しかも、システムオーナもその妥当性（システムの社会的責任とマイナスリスクの除去）を合理的に判断でき、
  - 利用者の財産などの保護対策内容を明示でき、
  - システム開発者や、運用者（SI/SO)の適切な発展と競争により、
  - IT社会の健全な発展への貢献を、ねらうものである。

WGで目指すもの

- 簡単、お手軽で、わかりやすい指標・基準を、どこよりも早く、JNSAで公表したい。



RFP : Request For Proposal
情報システムを導入するに当たって、ユーザが納入を希望するベンダに提供する、導入システムの概要や調達条件を記述した文書。

index

- 背景
- 検討の経緯
- ユーザー目線でのセキュリティ要件
- RFPガイドラインの使い方

検討の経緯　1

- **記載するレベル**
  - Better Than Nothing（無いよりまし！）
  - ボトムライン（最低限、実施すべきライン）の提示。
  - RFPとして、コピペできるようなもの
- **検討の経緯**
  - ボトムラインの項目洗い出しでも膨大な量になるのでは？
  - 突き詰めていくと、15408になってしまう。
  - コスト（労力）の観点から、厚みを「薄く」するのはありだが、「なくす」のは×としたい。
  - 「脅威」を何処まで掘り下げるのか？
    - ウイルス、侵入、改ざん、といった大レベル
    - インターネットからの侵入、社員の悪用といった小レベル

検討の経緯　2

- **スコープ（検討対象）**
  - 「Webシステム開発」を今回の検討スコープとする。

	分類	概要
⇨	WEBシステム開発	ECサイトに代表されるWebシステムは、ほぼすべてカスタムメイドである。まずは、こちらについて、ガイドラインをつくりたい。
今後の検討課題	一般システム開発	
	ネットワークインフラ	
	アウトソース	
	製品導入	
	インターネット家電	

検討の経緯　3

- 「脅威」と「脆弱性」と「対策」の相関

脅威≒手口	脆弱性	対策
・なりすまし ・Dos ・侵入 ・改ざん ・漏えい ・ウイルス	・OS ・ミドルウエア ・アプリケーション ・ネットワーク ・ハードウエア ・人間	・システム的 ＋パッチ ＋アンチウイルス ＋FW ・人的 ＋ポリシー ＋教育 ＋監査

収拾つかず

検討の経緯　4

- 体系化＝分類＝目次

パターン	呼称	出展	サンプル
案1	対策ベース	MS社の資料より、Web アプリケーション セキュリティ 強化 - 脅威とその対策 http://www.microsoft.com/japan/msdn/security/guidance/secmod77.mspx	＊入力検証 ＊認証 ＊承認 ＊機密性の高いデータ ＊セッション管理
案2	脅威による分類	脅威が現実のものとなった場合の影響を「なりすまし、改ざん、否認、情報漏えい、DoS攻撃、権限昇格」の6つに分類する方法で、Microsoftの提唱によるものである。 http://www.microsoft.com/japan/technet/security/topics/architectureanddesign/ipsec/ipsecapd.mspx	＊Spoofing（なりすまし、ID 偽装） ＊Tampering（改ざん） ＊Repudiation（否認） ＊Information disclosure（情報の漏えい） ＊Denial of service（サービス拒否） ＊Elevation of privilege（権限の昇格）
案3	IPAの分類	ウェブサイトの脆弱性対策の緊急チェックポイントを発表 ～ウェブサイトの脆弱性悪用による被害回避のための緊急対策情報を発信～ http://www.ipa.go.jp/about/press/20050623.html	1）不要なエラーメッセージを返していないか 2）公開すべきでないファイルを公開していないか 3）ユーザからの入力値をチェックして無害化しているか ： 14）ファイアウォールを使用して、適切に通信を
案4	契約による分類	（WGの検討から）	＊自社で ＊外部委託 ＊システム・アウトソース ＊業務アウトソース
案5	フェーズによる分類	（WGの検討から）	＊提案 ＊運用中 ＊開発中（企画、設計、開発、テスト）
案6	個別対策	（WGの検討から）	＊ウイルス対策 ＊フィッシング対策 ＊メール不正中継 ＊DNS

検討の経緯　5

検討パターン	検討状況
1. 対策手法からの分類	・ベンダーの立場で見ると提案しやすい形態だが、ユーザがなぜそれを求めているのか（何を恐れているのか）が不明である ・「想定する攻撃」の列がそのままRFPになりそう。 ・網羅性に欠ける危険性がある。欠けていることに気が付かない可能性もある。その点STRIDのアプローチの方が良いのでは。
2. 現象（脅威）による分類	・起こっては困ること、起こらないような対策を示すのが目的。 ・アプローチ大項目だけで要求を出すと受注者側のリスクが高くなる。 → 想定する原因を明記。 ・漏れのないようにするのは提案側であり、RFPはそこまで必要ない。
3. STRIDE分類	・表を作成したところパターン2と見た目は似たものになった。 ・DFDがあるのであればRFPは不要なのでは。結局、STRIDEからのアプローチが間違っているという結論もうろ →既存システムには適用できるだろう。方法論として、既存システムに対する脅威を分析して考えていくというのはあるだろう。
4. ISMS管理基準から	・ISMSの127項目のどの項目を選択するか、選択した項目をどう読み解いたかが、読んだ人や組織によって解釈が変わる。 ・統括的な管理方法として抜粋してチェックリスト的使用法は可能であろう。

index

- 背景
- 検討の経緯
- ユーザー目線でのセキュリティ要件
- RFPガイドラインの使い方

パターン3：脅威視点のRFP

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。

パターン2：現象視点のRFP

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な対策を提案すること。
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の対策を提案すること。
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。
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。
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な対策を提案すること。
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の対策を提案すること。
7. **内部者対策**
   - 内部者による情報漏えい・改ざんを防止・抑止するための対策を提案すること。
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。
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

パターン1：対策視点のRFP

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。
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。
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。
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。
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。
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。

各パターンの特徴比較

	発注者		受注者	
	メリット	デメリット	メリット	デメリット
パターン1「対策手法の視点」	-	網羅性が不明	提案しやすい	他社との優位性を出しにくい
パターン2「現象面の視点」	分かりやすい	-	-	できないこの説明が必要
パターン3「脅威モデルの視点」	簡単であり、書きやすい	提案にばらつきがあり、評価が困難	-	提案内容によっては責任範囲が広くなる

index

- 背景
- 検討の経緯
- ユーザー目線でのセキュリティ要件
- RFPガイドラインの使い方

システムの類型化

- セキュリティ対策への主要な影響要因
  - コスト？
  - **外部ネットワークへの公開**
    - インターネットなどの信頼できないネットワークに、接続するか否か
  - **機密情報の保有**
    - 個人情報、プライバシー情報、決済情報などの機密情報を保有するか否か
  - **システム利用者の範囲**
    - 不特定多数 ： 特に認証を必要としない
    - 特定多数 ： 個人を特定する情報を元にIDなどで認証
    - 特定限定 ： 人的も管理可能な範囲内

システムの類型化

外部ネットワークへの公開	機密情報の保有	システム利用者の範囲		対策レベル
有り	有り	－	⇒	必須
	無し	不特定多数		
		特定多数		推奨
		特定限定		
無し	有り	－		任意
	無し	不特定多数		
		特定多数		
		特定限定		

パターン2：現象視点のRFP

セキュリティインターネットなどの外部公開	有り				無し			
要件 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をシステムダウン	必須	必須	必須	必須	推奨	必須	推奨	推奨
・故障／過失による重要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. なりすまし対策								
・認証防止策								
・ユーザIDやパスワードの漏洩、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ェリ	必須	推奨	必須	必須	必須	推奨	必須	推奨
・重複処理の防止	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
・データ・データ蓄積が紛失し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
・正常な操作と推測でき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								
・通信経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
・データベースデータの改ざん	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（未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. 前弱性対策								
・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環境・対策	必須	必須	必須	必須	必須	必須	必須	必須
・脆弱なサービスを設定による不正アクセス防ぐ（最適化）	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・改ざん等の防止	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								
・不審検知・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されそれの記録・保存について取得するか明確化すること。	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管策	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体制を行うこと。	必須	必須	必須	必須	必須	必須	必須	必須

サンプル事例

- A社 『Webシステムの全面改訂』
- 概要：
  - A社は、売上高10億円、従業員数50名の製造業である。
  - 元々社内のシステムに詳しい人間が、社内システムの運用管理とあわせ、自社のWeb サイトも作成運用してきた。
  - しかし、システムの償却期限到来にあわせ、外部の開発業者に委託して、Webシステムを刷新するとともに、自社製品の紹介、販売にも可能なシステムの構築を検討することとなった。

サンプル事例

外部ネットワークへの公開	機密情報の保有	システム利用者の範囲
有り	有り	－
	無し	不特定多数
		特定多数
		特定限定
無し	有り	－
	無し	不特定多数
		特定多数
		特定限定

サンプルの選択例

セキュリティ要件	インターネットなどの外部公開	有り
	機密情報（個人情報、決済情報など）	有り
	システムの利用者	-
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
	・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
	・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
	・不正侵入による悪意あるシステムダウン	必須
	・故意／過失による高負荷処理に耐えられる構成	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
	・セッションハイジャック	必須
	・クロスサイトリクエストフォージェリ	必須
	・事後否認の防止	推奨
3. 漏えい対策		
	・通信経路上の盗聴	必須
	・万一、データ盗難が起きた場合における安全策	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
	・人的ミスによる情報漏えい	推奨

RFPに対する提案（例）

起こらないようにすべき事象・脅威	<- の説明	想定する原因	対策例
システムダウン	外部から攻撃されても、一定時間異以上のシステムダウンを起こさないような対策が採られていること。	DoS攻撃	DoS対応のF/W、ルータなどの機器で経済策をとる。 クラスタ構成、ロードバランサ等で負荷分散を行う。
		Webサイトの改ざん	改ざん検知・復旧システムの導入。 スタンバイ機を用意する。 改ざん具体的対応は「改ざん」の対応項目を参照。
		システム侵入等による、復旧のための停止	スタンバイ機を用意する。 侵入具体的対応は、不正アクセスの項目参照。
		ウィルス・ワーム・スパイウェア等	アンチウィルスソフト等の導入
レスポンスの低下	外部から攻撃されても、サービスが維持できないようなレスポンスの低下を防ぐ対策が採られていること。	DoS攻撃	DoS対応のF/W、ルータなどの機器で経済策をとる。 クラスタ構成、ロードバランサ等で負荷分散を行う。
		故意／過失による高負荷処理要求	画像・ファイルアップロードサイズなどの制限を行う。
情報漏えい	外部または内部からの情報漏えいを防止する対策が採られていること	万一データが盗まれた場合の安全性を確保する	重要なデータは暗号化もしくはハッシュ化（認証情報など）して保管する。
		ミスオペレーションによる非公開ファイルの公開、履歴ブラウジング	適切な権限設定がなされているか、監視・検出する仕組みを導入する。
		大量の情報漏えいの防止	一覧出力機能等で一度に出力可能な件数を制限するなどの機能を盛り込む。
改ざん	攻撃をうけても、コンテンツやデータ・通信内容の改ざんを防ぐ対策が採られていること	通信経路上での通信データの改ざん	重要なデータの通信にはSSLを利用する。
		静的コンテンツの改ざん	改ざん検知・復旧システムを導入し、継続的な監視・運用を行う。
		ログの改ざん	改ざん検知ツールを導入する。 ログに電子署名やタイムスタンプを施す。
なりすまし	攻撃者が正規ユーザの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	ユーザIDやパスワードを推測・盗聴される	パスワードポリシーの設定。 認証時におけるセキュアな通信路の確保。 セキュアなパスワードリカバリの方式。 ワンタイムパスワード、PKIなど、強固な認証手段の採用。
		セッションハイジャック	Cookieのセキュア属性、推測困難なセッションID、タイムアウトの設定など、セッション管理を適切に行う。
		クロスサイトリクエストフォージェリ	既知の攻撃手法に対応したセキュアプログラミングを行う。