JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

【成果 報告】
セキュア･システム ガイドライン
策定 WG

㈱ ラック

丸山　司郎

2006年5月30日

もくじ

1. 設立趣旨
2. 想定成果物
3. 活動の方向性
4. スコープ
5. 活動実績
6. 宣伝活動
7. 効果
8. メンバー紹介

1．設立趣旨

- **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、**
  1. 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、
  2. 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、
  3. 利用者の財産などの保護対策内容を明示でき、
  4. 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、
  5. IT社会の健全な発展への貢献を、ねらうものである。

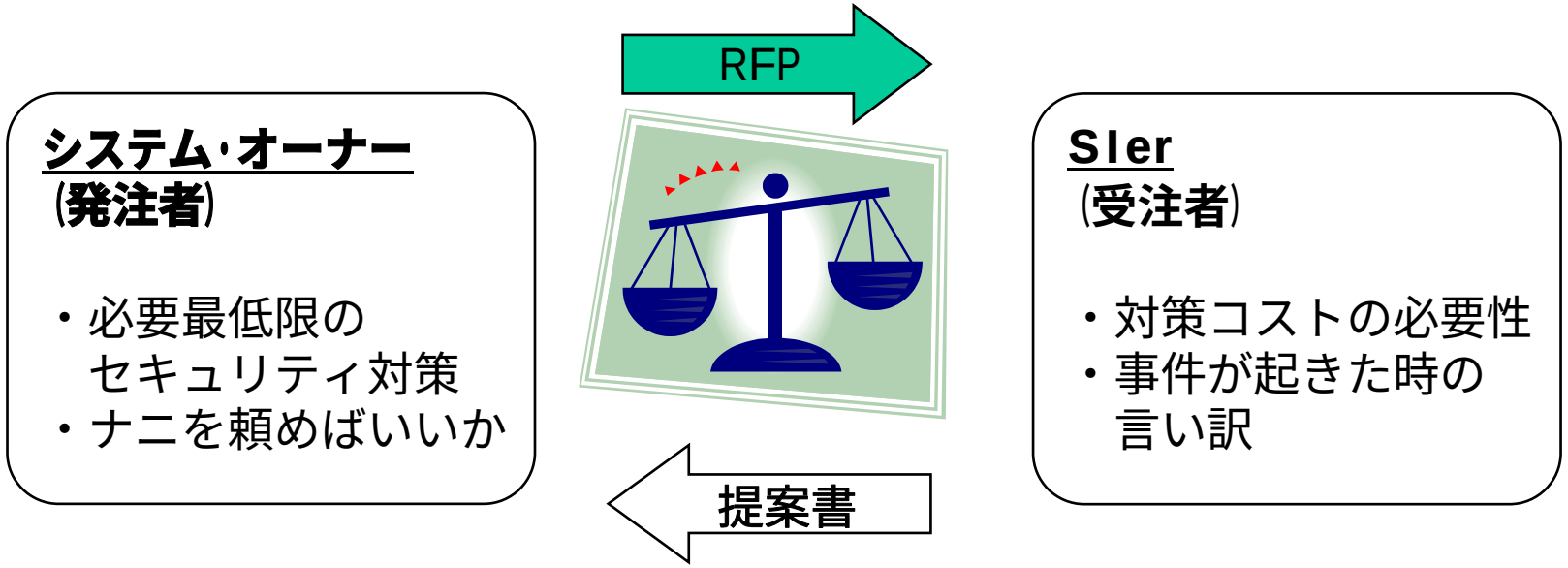
2．想定成果物

- システムオーナが、RFPに記載すべきセキュリティ要件としての、「セキュア・システム開発ガイドライン」作成をめざす。

- 検討の経緯
  - 本WGは　発注者側のＲＦＰに対するガイドラインを目指すのか、それとも　システム提供側の実装方法に対するガイドラインの提供を目指すのか？
  - 調達側・提供側の双方で使えるガイドラインとなるのが理想ではあるが、時間と体力の観点から、まずは調達側を意識した成果物を目指すべきだろう。
  - 受発注の合意（例：クロスサイトスクリプティングが無い事⇒何？）意思疎通が現時点ではあいまい。
  - 受注時の、残留リスクに対する評価が受注者側と発注者側が共通の基準で話せるものができればよいのではないか。

2．想定成果物

- 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。

3．活動の方向性

- **作成目標**
  - **発注者側のＲＦＰに対するガイドラインを目指す。**
  - **受注時の、残留リスクに対する評価が受注者側と発注者側が共通の基準で話せるものが理想。**
    ※リスク＝価格換算＆格納されている情報の重要度
- **作成レベル**
  - 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。**
  - **簡単･お手軽に使えるレベル**
- **進め方**
  - **被害調査WGのモデルケースを参考にモデル･システムを想定**
  - **モデルシステムの構築、**
    アウトソースに際して必要となるセキュリティ要件を洗い出す。

4．スコープ

- セキュアシステムの分類（案）
  - システム開発　⇐ α版のスコープ
    （例：ECサイト）
  - インフラ構築
  - アウトソース
    - データセンター
    - システム運用
  - 製品導入
  - インターネット家電

5．活動実績

- 第1回WG　5月20日　　キックオフ
- 第2回WG　6月7日
- 第3回WG　7月7日
- 第4回WG　8月9日
- 第5回WG　9月1日
- 第6回WG　9月15日
- 拡大WG　10月5日　　26名参加のワークショップ
- 第7回WG　10月24日
- 第8回WG　12月5日　　公開前レビュー

- 一般公開　12月　6日　　JNSAのWebサイトに掲載

6．宣伝活動

- **取材対応**
  - **日経BP社**　ITpro　**6月10日**
  - **現場担当者がホンネで語る「セキュリティ対策，ここが課題」**
  - http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20050802/165735/

- **取材対応**
  - **日経BP社**　ITpro **10月24日**
  - **提案依頼書に盛り込むべき**Web**セキュリティ項目**，JNSA**がサンプル提供**
  - http://itpro.nikkeibp.co.jp/article/NEWS/20051207/225830/

- **記事執筆**
  - **@**IT　**連載** Web**システムのセキュリティ要件**
  - http://www.atmarkit.co.jp/fbiz/cbuild/serial/securerfp/01/01.html

- **記事執筆**
  - **アスキー社　ネットワークマガジン6月号**
  - 「Web**セキュリティ完全防御マニュアル**」

7．効果

- 「セキュア・ジャパン２００６」（案）
  - 平成１８年４月２８日　内閣官房情報セキュリティセンター（ＮＩＳＣ）
- 第２章　対策実施４領域における情報セキュリティ対策の強化
  - 第３節　企業　【具体的施策】
    - イ）安全なWebサイトが備えるべき基準の検討（経済産業省）
      - **Webサイトの安全性を確保するため、２００６年度中に、発注者がウェブアプリケーション構築時に開発者（受注者）に対して示すべきセキュリティ要件に関する基準の検討を開始する。**

8．メンバー紹介

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

パターン1：対策視点のRFP

- **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）できないような対策を提案すること。
- **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。
- **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。
- **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な対策を提案すること。
- **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な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。
- **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な対策を講じること。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。

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の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の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。