セキュア・システム開発
ガイドライン作成 WG
設立報告

（株）ラック
丸山　司郎
2005年6月１３日

もくじ

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、
  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。

 Page 3

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。

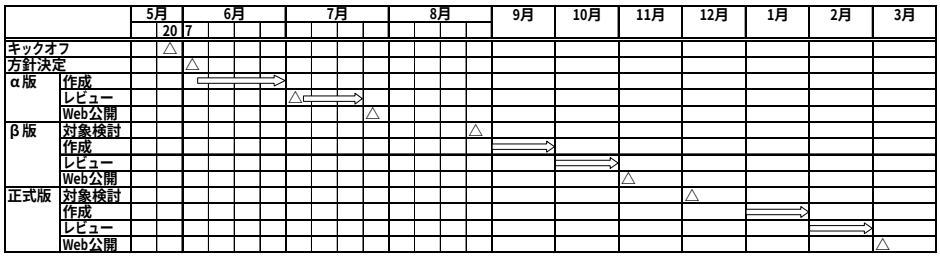
 Page 4

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。

- 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

4．活動計画



5．メンバー紹介

- CAC
  - 岩崎様
- 日本システムデベロップメント
  - 大鐘様
- 大日本印刷
  - 小野様
- 京セラコミュニケーションシステムズ
  - 徳丸様
- TIS
  - 塩田様
- A&I
  - 洞様
- DIT
  - 山田様
- NECネクサソリューションズ
  - 中西様
  - 小峰様
- 新日鉄ソリューションズ
  - 田京様
- 日本オラクル
  - 北野様
- NTT
  - 広瀬様
- みずほ情報総研
  - 中山様
- ラック
  - 倉持様
  - 大野様
  - 加藤様
  - 丸山

合計17名