JNSA ワーキンググループ紹介

セキュア・システム開発 ガイドライン作成 WG

WG リーダー
株式会社ラック　丸山　司郎

■ 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ておりますが、具体的な項目やレベルなどの明確な基準は存在しておりません。

一方、開発システムのセキュリティ評価基準としてISO15408が存在しますが、どのレベルを選択すべきかが規定されていないことなどから、なかなか実装は難しいものがあります。

そのような中、現実にサイバー攻撃にあい、事業継続に影響のでる企業も発生していることから、システム開発におけるセキュリティ要件の定義は喫緊の課題であります。

そこで、JNSAに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提示し、広く公開することで、システムオーナがその妥当性（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る評価項目を提示するとともに、システム開発者や、運用者（SI/SO)が適切な競争を行うことで、IT社会の健全な発展の一助となることを目的として当WGを設立いたしました。

よって、当ガイドラインに期待する要件としては以下があります。

- 将来ISO15408等の国際標準への橋渡しとなる指標
- 段階的に分かりやすく実施できるガイドライン
- 利用者の財産などの保護対策内容を明示できる指標
- システムオーナがその妥当性を合理的に判断できる評価項目
- システム開発者や、運用者（SI/SO)が適切な競争を行えるセキュリティ基準

■ 想定成果物

システムオーナが、SI/SOを委託する際の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」作成を目指します。

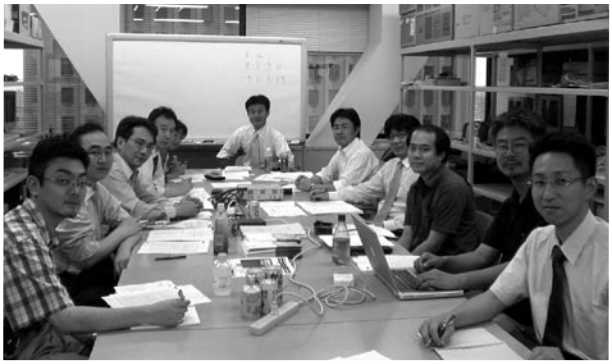
WGの中で成果物の形態について検討した結果、調達側・提供側の双方で使えるガイドラインとなるのが理想ではあるが、時間と体力の観点から、まずは調達側を意識した成果物を目指すべきだろう、という結論となりました。

つまり、『受注時の残留リスクに対する評価を、受注者側と発注者側が共通の基準で話せるもの』を目指して、発注者側のRFPという形で表現できればよいのではないかと考えております。

■ 目標レベル

「まずはJNSAとしての意思表示を」という観点から、当面は以下のようなレベルを想定し、濃度よりも速度を優先していきます。

ー 無いよりまし！（Better Than Nothing）
ー ボトムライン（最低限、実施すべきライン）の提示
ー 簡単・お手軽に使えるレベルの提示



■ セキュア・システム開発ガイドラインの全体像（イメージ）

ガイドライン		検討期間
システム開発		2005 年度のスコープ
インフラ構築		2006 年以降の検討課題
アウトソース		
	IDC	
	運用	
製品導入		
家電組み込み		

■ WGの運営方針

・1 ～ 2 回 / 月の会合を工学院にて行い、全体の意見調整を行う。
・成果物については、メーリングリスト上で検討して、今年度中の公開を目指す。
・当面は、発起人である丸山がリーダを務めるが、内容展開によってはＷＧの細分化やリーダの交代を検討していく。
・メンバー加入は随時受け付けておりますので、ご興味がある方はお気軽に会合にご参加いただくか、JNSA 事務局までお問い合わせください。

年間スケジュール