JNSA ワーキンググループ紹介

セキュアプログラミング WG

WG リーダー
株式会社情報数理研究所　伏見　諭

当WGは、セキュリティに対処する上で、運用の立場ではなく、システム／ソフトウェアの開発の立場からの対処方策を検討する活動をしています。「セキュアプログラミングWG」という名ですが、ソフトウェアのコーディングということに的を絞っているわけではなく、システムのライフサイクル全般で開発サイドが関係する場面全体を対象と考えています。このWGの活動を開始した2006年頃には、多くの問題意識がプレゼンの発表の形で寄せられ、必ずしもフォーカスを絞るのが良いとは思えないとの考えから、しばらくはセキュアプログラミングに関わる技術マップの作成という形で活動しました。しかし、これも多忙なメンバーから継続的にインプットを得ることがむずかしく、足踏み状態となりました。

そこで、淡々とした活動スタイルの方が負担が軽く、また活動の灯を絶やさないで済むとの考えから、2008年頃からセキュアプログラミングに関係すると思われる国際規格の検討を中心とする活動に切り替えました。具体的には、ISO/IECの合同技術委員会JTC1の中でITセキュリティの標準化を担当しているSC27の活動の中で提案されていた「アプリケーションセキュリティ」の規格の内容を初期のドラフト段階から検討することとしました。そのため、日本のSC27委員会のこの規格を審議するワーキンググループであるWG 4に対してJNSA（のセキュアプログラミングWG）としてリエゾン要員を出すこととし、首尾よくSC27/WG4から受け入れてもらえました。リエゾンとは、ISOやJTC1の規格検討において、審議内容に関連する団体から臨時またはある程度恒常的に討議に参加する要員を受け入れる制度です。

アプリケーションセキュリティ規格は、ISO/IEC 27034という規格番号が予定されているもので、番号から推測されるように、ISMS規格の中でのアプリケーションセキュリティという位置づけもありますが、実際の規格内容はこの推測とは少し違っています。ITシステム、ソフトウェアの開発において、いろいろな環境からセキュリティに関する要求が存在し、またそれに対してどのようなアプローチでセキュリティを設計・実装・試験・運用設定していくかのソリューションも複数存在します。そこにはレベル感もあります。それらを適切に表現し、企業組織および個別の開発で適切に選択して実際のシステム、ソフトウェア開発を行っていくべきと考えられます。このようなセキュリティの表現と選択の仕組みを提案しているのが、この規格案です。規格案にはかなり難点があるため、日本の意見を反映させるべく、国内SC27/WG4とともに、規格案へのコメントを作成し、国際審議に役立てています。なおこの規格の第1部は、2010年1月付で、委員会レベルドラフトの最新版が発行された状態となっています。

3/3（水）拡大勉強会の様子

JNSA ワーキンググループ紹介

ところで、この国際規格検討とは別に、2009年9月開催のWGで、米国NIST国立標準局の脆弱性データベースNational Vulnerability Databaseで言及されている各種リスト(脆弱性等)の勉強会の構想が新たに提案されました。

リストには次のようなものがあります。

CVE:　ぜい弱性識別子による網羅的脆弱性カタログ
CWE:　CVE等をややカテゴリーわけしようという試み
CAPEC:攻撃パターンの列挙
CCE:　構成管理上の脆弱性のカタログ
SCAP:　システムのバリデーションテストのしくみ

これらについては先行的にIPAで研究しているとの情報があるため、IPAから講師を招いて勉強会を行うことが提案されました。その結果、3月3日(水)に拡大勉強会として実施しました。

WGメンバーリスト

氏　名	所　属
リーダー 伏見　諭	株式会社情報数理研究所
塩見　友規	オー・エイ・エス株式会社
岡崎　吾也	株式会社情報数理研究所
安田　直	株式会社ディアイティ
塩田　英二	ＴＩＳ株式会社
塚田　孝則	日立ソフトウェアエンジニアリング株式会社
奥原　雅之	富士通株式会社
福田　尚弘	パナソニック電工株式会社
武部　達明	横河電機株式会社