



技術部会活動報告と今年度の活動

技術部会長

住商情報システム株式会社 二木真明

2007年6月6日

- ネットワークセキュリティに関する技術をテーマに調査・研究、実証実験、意見集約、他組織とのコラボレーションなどを推進します。
 - 各種ワーキンググループ活動
 - プロジェクト(公的案件の受託など)
 - ワークショップ、BoFの開催

ワーキンググループ活動



- 成果物目的のワーキンググループ(WG)
 - 不正プログラム調査WG
 - リーダー: 渡部章氏 (株式会社アークン)
 - ハニーポットWG
 - リーダー: 園田道夫氏 (JNSA研究員)
 - WebアプリケーションセキュリティWG
 - リーダー: 加藤雅彦氏 (株式会社アイアイジェイテクノロジー)
 - 脆弱性定量化に向けての検討WG
 - リーダー: 郷間佳市郎氏 (JNSA研究員)
 - セキュアプログラミングWG
 - リーダー: 伏見諭氏 (株式会社情報数理研究所)
 - セキュアOS普及・啓発WG
 - リーダー: 澤田栄浩氏 (日本高信頼システム株式会社)

- 勉強会目的のワーキンググループ(WG)
 - 暗号モジュール評価基準WG
 - リーダー:小川博久氏(株式会社シーフォーテクノロジー)
 - PKI相互運用技術WG
 - リーダー:松本泰氏(セコム株式会社)
- プロジェクト(受託事業など)
 - Challenge PKIプロジェクト
 - リーダー:松本泰氏(セコム株式会社)

- 多様化する不正プログラム(マルウェア)の挙動、活動を研究し、対策に生かすことを目的としたWG
 - 昨年度の活動
 - 「増加しそうなマルウェアについて、ネットワークを組んで感染させ、その活動を監視・分析する。また、ソリューションの効果を研究する。」というテーマで、WG会合を8回実施。
 - マルウェアの挙動が確認できる環境を構築したが成果物の完成までには至らなかった。
 - 今年度の活動予定
 - 現在、WG内で今年の方角性を議論中

- 疑似サーバ環境をインターネット上に構築し、インターネット側から行われる攻撃やマルウェアの侵入などについての観察を行うことで対策に生かせる情報を収集することを目的としたWG
 - 今年度の活動
 - JNSAにて設置したハニーポットシステムの状態を継続的に観察した
 - 今年度の活動予定
 - 引き続き観察を継続し、その結果を報告書(観察日記)にまとめたい

Webアプリケーションセキュリティ WG



- 近年、Webサイトへの攻撃は、ユーザが開発したアプリケーションへの攻撃が主流になりつつある。こうした状況やその対策について啓発、技術的な研究を行うことを目的にスタートしたWG
 - 昨年度の活動
 - Webアプリケーションにとどまらず、そのインフラを含めた企画から導入・開発、運用までのライフサイクル全体にわたる安全管理について考察。啓発用コンテンツの製作を検討した。(後ほどリーダーより報告します)
 - 今年度の活動予定
 - 順次、啓発コンテンツを執筆、制作しJNSAバイヤーズガイドサイトに連載予定

脆弱性定量化に向けての検討



WG

- 脆弱性に対する「パッチ」は、網羅的なテストが省略されていることが多く、高い可用性を要求されるシステムにおいては、障害を恐れて検証なしでの適用がためらわれる場合が多い。「パッチ」の検証作業の緊急度や優先順位などを決められる「脆弱性の緊急度」のような指標値があれば・・・という現場レベルの発想からスタートしたWG
- 昨年度の活動
 - 脆弱性と脅威の程度をからめた指標値の計算式(一昨年の活動で作成)の改良と検証するための、アンケートを実施。
 - 調査結果を含めた報告書を作成し、WG活動としては一区切りとする。
 - 活動は一旦終了 (後ほどリーダーより報告します)

- ソフトウェア脆弱性の根本的な原因であるプログラミング問題を開発者の問題としてクローズアップし、様々な分野のソフトウェア技術者で問題意識を共有しつつ、解決策を探っていくWG
 - 昨年度の活動
 - セキュアプログラミングという切り口で、様々な分野における問題意識を整理、共有した。
 - 各分野にまたがる問題であり、技術マップを作成するためアンケート調査などを実施することを決定。
 - 今年度の予定
 - 細部の討議をさらに進め、成果物を作成の予定

- 必要性が叫ばれ、様々な形でリリースされながらも、なかなか使い切れていないセキュアOS。その本来の使い方、導入方法など様々な技術的課題について啓発していくことを目的としたWG
 - 昨年度の活動
 - メンバーの意識あわせと活動方針の設定、テーマの抽出を行った
 - 今年度の活動予定
 - 様々なタイプのセキュア基盤(OS)を利用したソリューションモデルについての検討を行い、それを啓発していく
 - セキュアOSを利用することで産業界のインフラにまで発展したインターネットを少しでも安全に利用できるようになることを目標に活動を進める

- 米国及び、カナダの暗号モジュールのセキュリティ要件及び、評価制度、同要件の国際標準化、日本国における同要件及び評価制度などの動向把握及び、ベンダーとしての取組み方を議論し、必要に応じて提言などを行う。
 - 昨年度の活動
 - 主に国内動向について観察を行ったが、活動は比較的低調だった。
 - 今年度の活動予定
 - 年間の活動としては、独立行政法人 情報処理推進機構 (IPA) により 運用されている暗号モジュール試験及び認証制度 (JCMVP: Japan Cryptographic Module Validation Program) に関する 意見交換などを行う予定

- PKIにおける相互運用の問題を解決するための検討を行うWG
 - 昨年度の活動
 - IETFの参加(年3回)
 - 及びセミナー「PKI day - PKIの展開と最新技術動向」を6月に実施し、200名の集客があった。
 - 今年度の活動予定
 - 本年同様にIETFへの継続的な参加、セミナーの開催などを行う予定

Challenge PKIプロジェクト



- PKIに関する調査、研究を受託し、実行するためのプロジェクト。2001年から毎年、様々な課題で活動を行ってきた
 - 昨年度の活動
 - 独立行政法人情報処理推進機構 (IPA) の「IC・IDカードの相互運用可能性向上に係る基礎調査」の公募で採択され、調査を実施した。オープンでセキュアで相互運用可能なIDカードを目指して、PKIから見たICカードの相互運用性を調査するとともに、公的な目的で利用されるIDカード等に関わる問題点を探るため、行政府等のヒアリングも行った。
 - 今年度の活動予定
 - Multi-domain-PKIのRFC化 (IETFへの提案) と、今までのChallengePKI関係の報告書を中心に出版する企画の調整を行う予定。

BoF, ワークショップ活動



- WG活動に継続的に参加することは難しいが、興味のある課題について、とことん議論して見たい、というニーズに応じて昨年度から試行しはじめたイベント。今後、さらに様々なテーマで開催していきたい
 - (例) インシデントレスポンス BoF
 - インシデントレスポンスにおける問題、悩み、その他持ち寄って議論しようというBoF。昨年度、2回開催
 - ワークショップ
 - WGまたは個人が研究成果を発表し、広く意見を求める場として活用

その他、今年度の課題

- **家電、組み込み系システムのセキュリティ**
 - ゲーム機、ネット家電などの普及に伴って、リスクも高まっている組み込み系ソフトウェアの問題にJNSAとして各方面と連携しながらどのように取り組んでいくかを考えていく。
- **セキュリティ技術者の育成、技術継承**
 - JNSAセキュリティ道場、といった形で会員企業の若手技術者育成に貢献する方法を考える。
- **他の組織との技術面での協力、連携**
 - 共催セミナー、イベント等を通じての技術協力の推進
 - Internet Weekでの Security Day (昨年までJPCERT/CC, Telecom ISACと共催で実施)のようなイベントの模索。(技術的な観点からの協力、支援)

- 脆弱性定量化に向けての検討WG
 - 金岡 晃氏 / 筑波大学
- PKI相互運用技術WG
 - 松本 泰氏 / セコム株式会社
- WEBアプリケーションセキュリティWG
 - 加藤雅彦氏 / 株式会社アイアイジェイテクノロジー

