2016年1月18日

サイエンティフィック・システム研究会
システム技術分科会　2015年度第2回会合

東工大CERTの立ち上げと現在の取り組み

東京工業大学　学術国際情報センター　准教授
松浦知史

・要旨
　組織内CSIRTの重要性が叫ばれている。攻撃手法は高度化/多様化し続けており、学内のサービス担当者が片手間でセキュリティ情報を収集し、適切な運用を行い、問題発生時には初動対応を行うといった事は到底望めない。情報セキュリティの専門チームと現場担当者が協力し安全な環境を構築して行く事が求められている一方で、実際の組織立ち上げには多くの課題が山積している。

　実行力のある組織を構築するためには、適切な権限、人材、機材、予算またそれを支えるトップ層を含む学内の理解が必要である。しかし権限一つ取っても、権限を規定するための学内規則の変更、権限の必要性に関する全学への説明が必須であり、場合に寄っては権限を定める過程で抵抗や反発も発生しかねない。新規のセキュリティに関する施策や予算獲得を行う際にも安全性、必要性、効果とコストのバランスなど幅広い観点でトップ層から現場担当者まで様々な立場の方々に説明し、説得する必要がある。

　本公演では東工大CERTの立ち上げ時期を中心に上記の様な課題に対して、どのように行動し、どのように説得してきたかを紹介する。また、インシデントレスポンスの事例や次世代型ファイヤフォールの導入など現在の活動内容も併せて紹介する。