大学 CSIRT 体制に対する考察と新潟大学への適用 I

青山茂義 †, 三河賢治 †

aoyama@cais.niigata-u.ac.jp, mikawa@cais.niigata-u.ac.jp

新潟大学　情報基盤センター 新大 CSIRT†

概要

新潟大学では，2003 年から学内 CSIRT 運営を開始し，15 年間の実績がある．これまでに、セキュリティインシデントが発生した際の対応を速やかに行うため、各種情報セキュリティシステムの導入, インシデント対応手順や対応体制の整備を行ってきた．この間に, 検討・適用を行ってきたセキュリティインシデント対応体制の中で, 今回の報告では, 主に，外部 SOC と連動した 365 日 24 時間体制でのセキュリティレスポンスとそのシステム設計についての報告を行う．

キーワード

CSIRT，セキュリティインシデント対応

サイバーセキュリティ基本法成立（2014 年）やその改定（2016 年）に見られるように，現在，国をあげたセキュリティ強化が行われている．その一方で，国立大学を含む国の関係機関からの情報漏洩やウェブ改竄等のセキュリティインシデントは，依然として多数発生しており，セキュリティインシデント体制構築は急務である．

新潟大学は，10 学部，6 研究科，附属病院，附属学校，附属研究所等からなる総合大学である．教員・事務職員・学生のみならず，看護師や嘱託職員などと職種も多岐にわたっており，約 20,000 人の情報セキュリティポリシーの対象者がいる．新潟大学では, 2000 年の沖縄サミット開催に伴う国家をあげたセキュリティ体制構築の時流にも乗り, 2002 年 12 月にセキュリティポリシーが策定され，セキュリティ対応体制強化が行われた．その一貫として, 2003 年度から, 情報基盤センター (旧総合情報処理センター）セキュリティ相談室を中核とする CSIRT 体制の構築が行われてきた．発足当初は, セキュリティ担当教員 1 名, セキュリティ技術者（外注常駐者）1 名, セキュリティ担当事務職員（兼任数名）であったが, 現在では, 図 1 右下のような専任 4 名相当（教員, 技術職員, 事務職員, セキュリティ技術者）の体制に強化されている．

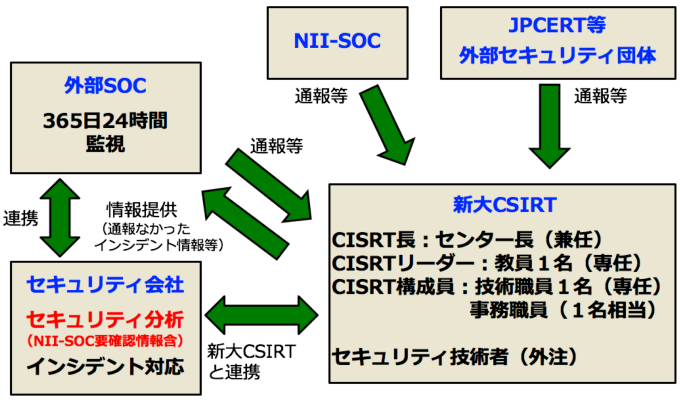

図- 1: 新大 CSIRT 体制 (2018 年)

セキュリティインシデントは，必ずしも，通常の勤務時間の平日の日中に起きるわけではない．サイバー犯罪者の立場からみて，むしろ，時間外や休日を狙って侵入を試みると考える方が自然である．そのため, 365 日 24 時間体制をどのように組むのかが課題となる．大学の技術職員等でローテーションを組むというのも考え方の一つではあるが，平日だけ考えでも、通常勤務の 8 時間に加えて、夜間の 16 時間分の人員確保が必要であり，多くの大学における人員不足や予算不足の現状を考えると，現実的ではない．また，セキュリティシステムによる自動遮断を使うというのも考え方の一つではあるが、誤検知も多く，メール等の重要インフラを長時間止めてしまうリスクも高い．そこで，本学では，外部 SOC(セキュリティオペレーションセンター）とセキュリティ会社と契約し，365 日 24 時間監視・通報・遮断体制を組むことにした．不正侵入検知装置 (IDS) やファイヤウォールのログから，外部 SOC が不正侵入の疑いがあると判断した場合は，本学 CSIRT の担当者、又は、セキュリティ会社に電話での直接連絡（外部 SOC の分析後、ほぼ確実に、インシデントが発生している場合のみ）があり，原則的にそのままネットワーク遮断を行う（外部 SOC 技術者、又は、本学 CSIRT 技術者）.

その後は，遮断を行った部局やユーザに連絡を取り，インシデント対応を行うが，当初は，全学で IP アドレスを管理しているデータベースに未登録であったり，登録内容が古かったりで, 速やかなインシデント対応が行えないという状況であった．そこで，全学的な認証ネットワークの導入 (2008 年度）[1] をすることに決め，認証データベースと連動した IP 管理データベース (IP 管理 DB) の開発・拡張 [2, 3] を行ってきた，本 IP 管理 DB に登録されていないネットワーク端末は，学内 LAN に原則的に接続できないので、インシデント発生時の端末（ユーザ）特定能力が大幅に向上した．最近になって起こってきた問題として、研究用ネットワークの高速化により、セキュリティ監視契約の費用（契約帯域で課金）が無視できなくなりつつある．そこで、図 2 にようにインフラ的通信とウィルス感染の疑い等が低い研究用データを分けて、インフラ的通信のみ監視するようにシステム変更を行った．本報告では、主に以上の点について、より詳細の議論と事例紹介を行う．

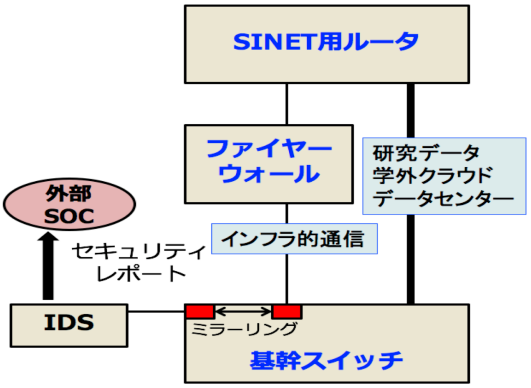

図- 2: セキュリティ監視対象

参考文献

[1] 浜元信州, 青山茂義, 三河賢治, 全学ネットワークアクセス認証システムの導入, インターネットと運用技術シンポジウム 2009, IPSJ Symp. Series Vol. 2009, No.15, pp.1-8 (2009).

[2] 浜元信州, 五十嵐瑛介, 青山茂義, 三河賢治, ホスト登録システムを利用したネットワークアクセス認証システムの運用, 情報処理学会研究報告,Vol.2010-IOT-9 ,No.4,pp.1-6 (2010).

[3] 青山茂義, 山本一幸，宮北和之，三河賢治, ホスト登録システムへの非利用 IP アドレスの特定機能実装と IP 棚卸し, 学術情報処理研究,No.22(2018), 出版予定.