大学CSIRT体制に対する考察と新潟大学への適用II
—部局CSIRT—

青山茂義, 三河賢治, 宮北和之

aoyama@cais.niigata-u.ac.jp, mikawa@cais.niigata-u.ac.jp, miyakita@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，16 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．2018 年の AXIES 年次大会では，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った．今回の報告では，2018 年度に導入を行った部局 CSIRT について，考察と報告を行う．

キーワード

CSIRT，セキュリティインシデント対応

国立大学では，情報漏洩やウェブ改竄等のセキュリティインシデントが多数発生しており，セキュリティインシデント体制構築は急務である．多くの国立大学では，2016 年度に情報セキュリティ対策基本計画（三カ年計画）を策定し，CSIRT 体制の見直しや再構築を行った．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．そのため，大規模で多様な職種の構成員の組織で速やかなセキュリティインシデントレスポンスを実現する必要がある．

中央集約型 CSIRT は，比較的構築も容易なので，JPCERT の CSIRT ガイド [1] や各種 CSIRT 講習会などでも解説されることが多いが，本学のような総合大学の実運用には向かないと思われる．そこで，中央集約・分散ハイブリッド型 CSIRT モデル（図- 1 参照）を考えながら，組織構成や各種規定・手順の整備，セキュリティ体制の変更を 2017~2018 年度に行った．その目玉は，部局 CSIRT の設置であるが，本学に限らず，大阪大学の OU-CSIRT[2] など，他大学でも導入が進みつつある所である．

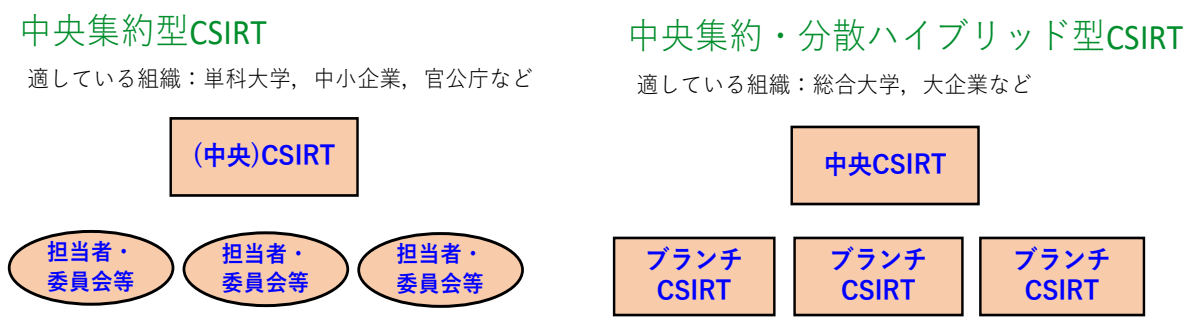

図- 1: CSIRT 体制の型

図- 2 では，では，部局 CSIRT の概略を表しているが，部局 CSIRT 長は，部局のセキュリティ維持等に責任を持つ部局長である．また，実際のセキュリティ実務を行うための部局 CSIRT リーダーを部局 CSIRT 長とは別においている．部局 CSIRT リーダーとして想定しているのは，部局内のコンピュータ管理に詳しい中堅教員である．ただ，教員がリーダーの場合は，出張等も多く，セキュリティインシデント対応を速やかに行えない場合があるので，副リーダー（複数名可）も配置している．また，これまでの委員会ベースの運用の大きな問題点の一つは，部局内での事務系の連絡体制等をうまく活用できない場合が多いことであった．そのため，部局 CSIRT には，部局 CSIRT 運用に必要な事務作業や連絡を担当する事務職員を含めていただき，事務系 CSIRT 業務を担当職員の公式職務とした．

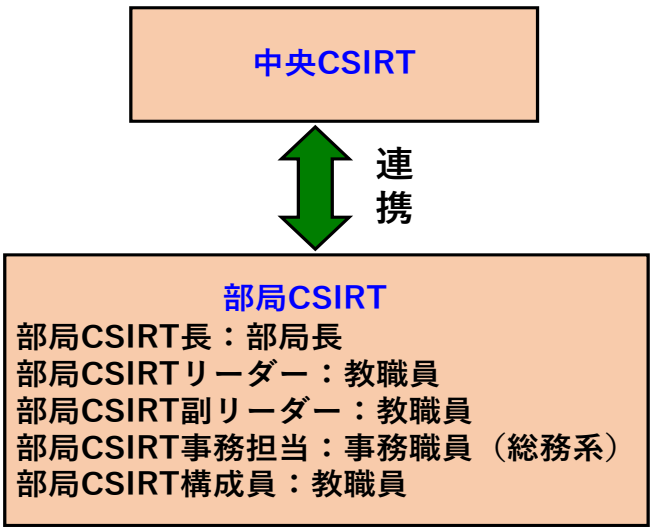

図- 2: 中央 CSIRT と部局 CSIRT

2019 年度 AXIES 年次大会では，上記の部局 CSIRT 構築に関して，本学で行った考察・検討，部局 CSIRT を含む CSIRT 体制に関する詳細の報告を行う．

参考文献

[1] JPCERT コーディネーションセンター, CSIRT ガイド, https://www.jpcert.or.jp /csirt_material/files/guide_ver1.0_20151126.pdf.

[2] 日本 CSIRT 協議会 OU-CSIRT(大阪大学 CSIRT) 情報; https://www.nca.gr.jp/member/ou-csirt.html