大学 CSIRT におけるグループチャットツール活用事例 2

松本　哲, 大平　健司, 田島　滋人, 奥田　剛, 猪俣　敦夫, 森原　一郎

国立大学法人 大阪大学

Case 2 of using group chat tools at university CSIRT

Satoru Matsumoto, Kenji Ohira, Shigeto Tajima,
Takeshi Okuda, Atsuo Inomata, Ichiro Morihara
Osaka University.

概要

部門・部局を跨る、分野横断的な人員で構成されている大学 CSIRT（Computer Security Incident Response Team）において、情報インシデントの疑いが発生した時点から初動対応までの限られた時間内に、正確に要因を分析し、切り分け、対応を行う事が、後の対応フェーズにとって重要となる。メールとメーリングリストのみを用いて行っていたチーム対応をクラウドコンピューティング環境上にあるグループチャットツールにかえて行い、その成果を AXIES2019 年次大会にて報告した。その後の活用の変遷について再び報告する。

1　はじめに

部門・部局を跨る、分野横断的な人員で構成されている大学 CSIRT（Computer Security Incident Response Team）において、情報インシデントの疑いが発生した時点から初動対応までの限られた時間内に、正確に要因を分析し、切り分け、対応を行う事が、後の対応フェーズにとって重要となる。本学における、インシデント疑い発生からその判断のフロー概略を図 1 に示す。これらの対応を分野横断的な人員で構成されている距離的にも構内に散在する大学 CSIRT 構成員により、メールとメーリングリストのみを用いて従来行っていたチーム対応をクラウドコンピューティング環境上にあるグループチャットツールにより行う事で、様々な情報資源を相互に提示しあい、迅速に対応し合えた[1]。昨年度からインシデントの内容やトレンド、チーム構成に変化があり、それぞれについてのその後の活用について、事例紹介を行う。

2　課題点

2.1 インシデント内容の変遷について

CSIRT 業務に於いては、インシデントの内容や計算機器への攻撃手法のトレンドが絶えず変遷してゆき、それに伴い、初動対応パターンや対応ル

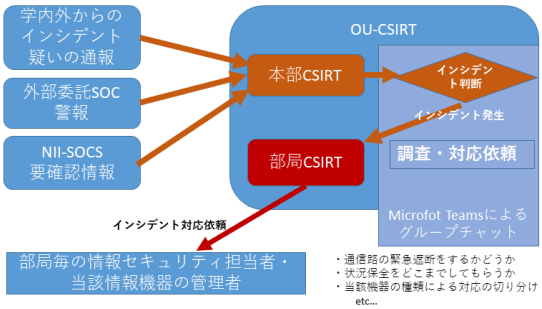

図1.　インシデント疑い発生から判断までのチーム対応フロー図

ールも変遷してゆくことが、様々な所に波及し課題を生む。マルウエアなどの攻撃手法は、以前行われていた攻撃手法の改良や、全く新しい攻撃の手法が用いられる等、様々な変遷を遂げる。それに伴い、新たな CSIRT 対応についての議論やコミュニケーションがグループチャットツールにて行われる。新たな対応については、各部局のチャットに参加していない事務職員にまで波及する事があり、メールからの移行を推進するために、チャットツール利用者のグループ範囲の拡張や、利用の呼びかけを行う必要があった。

2.2 議論内容や方法の変遷について

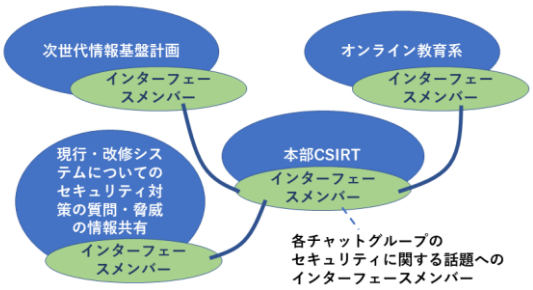

図2.　複雑なコミュニティー間の連携の概念図

２年目の利用となり、計算機器への攻撃対応の議論はノウハウの蓄積が進み、チャット内容の質的変遷が行われた。チャットツールへの投稿者の定常メンバーも変化があった。別途、大学 CSIRT へのセキュリティ対策についての質問やセキュリティ脅威に関する情報共有のチャットグループも作成された。他、コロナ禍の影響もあり、本学内で、テーマの違う計算機システム運用に関するグループチャットツール活用が活性化した。各グループに共通に包含される一部の利用者がセキュリティに関わる話題の橋渡しとなり、インターフェースメンバーを要する複雑なコミュニティに発展して、対応の複雑化が起きていた。

3　活用事例の紹介

２．の課題点についてインシデント内容の変遷への対応について、議論の内容や方法の変遷についての詳細とその対応について以下に述べる。

3.1 インシデント内容の変遷への対応

本年度は情報機器への攻撃や脅威の話題がノウハウの蓄積によって減り、インシデントについては、人為的な小規模のミスや、フィッシングサイトの話題が見受けられるようになり、内部監査や外部監査による情報機器の脆弱性問題への相談が CSIRT のチャットグループに多く寄せられるように傾向が変遷した。インシデント当該部局へのインターフェースとなる事務職員の方々により、チャットへの書き込みが多くみられた。フィッシングサイトに関するインシデント対応については、議論の結果、不審なサイトへの通信遮断結果のみをグループチャットシステムへ自動転送する仕組みを施し、対応の迅速化と省力化を行った。

3.2 議論内容や方法の変遷への対応

システム運用について稟議中の内容もあり、混乱を避けるため、システム運用に関する事項と CSIRT 業務のチャットグループは独立して設置さ

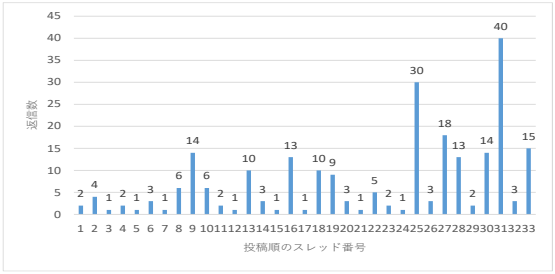

図3.　セキュリティ対策の質問・脅威情報共有

れている。本年度は図２に示した、複雑なコミュニティ間の連携が行えた。システム運用のコミュニティと本部 CSIRT のコミュニティ間にて、システム運用のセキュリティに対する伺いがあれば、両コミュニティに属するモデレータ的存在となるメンバーが連携の運用努力を行った。それにより、チャットグループ間をオブジェクティブにブリッジし、複数のグループチャットが円滑に運用された。本年度のセキュリティ対策の対話数の分布例を図３に示す。内訳詳細は守秘の為伏せる。特徴として、システム改善提案でのセキュリティについての伺いでは、対話数が多くなり、脆弱性情報共有については、概ね対話数が少ない傾向であった。コロナ禍の影響により、遠隔コミュニケーションに関するセキュリティへの質問については、対話数が多い傾向にあった。

4　まとめ

部門・部局を跨る分野横断的な人員で構成されている、大学 CSIRT において、グループチャットツールを活用の際、情報共有内容の変遷があった。それに対して、メンバーの再編や運用方針の変更で対応した。メインテーマが違うチャットグループ間でも、インターフェースとなるメンバーのモデレート努力により円滑にチャットグループ間でのコミュニケーションが図れた。

謝辞

平素より、ご多用の所、情報インシデント対応を行って戴いているすべての大阪大学構成員の皆様、関係各位の方々へ感謝の意を表します。

参考文献

[1] 松本　哲, 大平　健司, 田島　滋人, 奥田剛, 猪俣　敦夫, 森原　一郎、大学 CSIRT におけるグループチャットツール活用事例、AXIES2019 年次大会、AXIES、2019.