大学 CSIRT におけるグループチャットツール活用事例

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

大阪大学

Case of using group chat tools at university CSIRT

Satoru Matsumoto, Kenji Ohira, Shigeto Tajima,

Takeshi Okuda, Atsuo Inomata, Ichiro Morihara

Osaka Univ.

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、迅速に対応しあえた。これら情報インシデント対応チームでの ICT 活用事例について以下に述べる。

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。従来は、メールとメーリングリストのみを用いて、インシデント疑いに対する対応を行っていた。 しかし、マルウエア等の攻撃情報や、インシデント要因を含んだ大容量の情報、発生している疑いの状況を分析する為のスクリーンショットの情報共有は、グループチャットの方が、より利便性が高い場合が多いと考えた。また、特に大阪大学では、CSIRT においては部門・部局を跨る分野横断的な人員により構成されている。その為、構成員間の物理的な距離は離れ、構成人員間で共有するストレージ装置も部門・部局を跨る管理が障壁となり、設置と配置が難しい状況であった。そこで、クラウド上に展開されているグループチャットツールを利用すると、迅速に対応しあえる成果を得た。これらインシデント対応チームでの ICT 活用事例について詳細を以下に述べる。

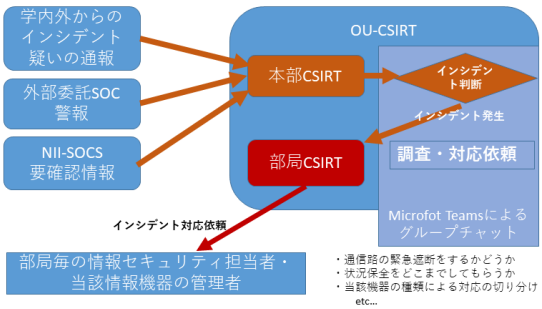

図１. インシデント疑い発生から判断までのチーム対応フロー図

2　課題点

情報インシデント疑いの発生から初動対応までに、従来のメールおよびメーリングリストのみを活用していた時点で課題となっていた事例を以下に述べる。

2.1 情報共有について

マルウエア等で攻撃された疑いの情報や、インシデント要因を含んだ情報は、分野横断的な人員で構成されている、他部局・他部門にて周知されるべきでない情報を含むことが多々ある。また、専門家でない方々に周知されるべきでないマルウエアの情報を含むことも多くある。時として、そ

の情報を元に追試し、2 次感染が発生し、個人情報を含む多くの情報が当事者以外に流出する場合もある。メールを利用したコミュニケーションにおいては、これら共有情報のアクセスコントロールが難しくなっていた。また、高度なサイバー攻撃を被った場合、要因の特定が困難となり、解析の為に情報機器のストレージ全てのディスクイメージや数ギガバイトに及ぶ大容量のアクセスログを扱う場合が多い。メールソフトの容量制限や多量のデータ伝送による回線輻輳により、情報共有が困難となっていた。また、大学全体で同時多発的に被っている攻撃の証拠となるスクリーンショット情報は、部局・部門毎、銘々に個人宛へと報告を受けていた場合、集約が困難となっていた。同時多発的にマルウエアの攻撃が各部署にばら撒かれた際、インシデント事案が並行して複数発生する。それぞれのインシデントに対する管理を多数のメールを全てどこまで進捗していたか読み返して対応する必要があり、混乱を招いた。

2.2 発生時点からの報告のまとめについて

情報インシデント疑いが、情報インシデントであると判定された場合、情報インシデントの初動対応に移り、原因を排除するべく要因を分析・特定するために、発生事象についてのタイムラインを直ちに作成する。この際、メール・メーリングリストを利用していた場合、各人が受け取ったメール・メーリングリストに流れた情報を持ち寄り、メールソフト内のデータについて多量の見返しを行わねばならず、また、添付ファイルの整理に多くの時間を要した。

3 活用事例の紹介

この度、大阪大学では、１で述べた構成員間の距離やストレージの配置問題や、２で述べた課題点を踏まえて、試験的にグループチャットツールを導入する事とした。Redmain [1]等のインシデント毎の管理ができる進捗管理ツール等を使う事も考慮したが、ソフトウエア開発の進捗管理や品質管理に特化したツールが多く、議論を行うチャット機能が不足していた。Slack [2], Yammer [3]等のメールと親和性の高い多機能のグループチャットツールも検討したが、既に大阪大学では Office365 の包括契約もなされていて、アカウントの流用と、情報コンテンツへのアクセスコントロールの移譲も行い易いと考え、Microsoft Teams [4]を活用する事とした。クラウドコンピューティング上のリソースを使う事で、部門・部局を跨る構成員にとって、共有情報コンテンツの管理が行い易くなることも、選定理由の 1 つであった。以下、活用した結果の事例を示す。

3.1 情報共有について

- Microsoft Teams のアカウントに従った情報アクセスコントロールがなされ、Web へのリンク，画像，参考資料が集約され、一元管理されるようになった。

3.2 発生時点からのタイムライン作成について

チャットツールにより、時刻が打刻され、纏め易くなり、Microsoft Teams の機能により Web へのリンク，画像，参考資料がタイムラインに従って一元管理される様になった。また、メール本文の転送もグループチャットの分類毎に行える。メールソフトを利用したグループチャットへの参加も可能となり、他部局から届いたメールに対しても本文をチャットのタイムラインに容易に組み込める事が可能となった。

4 主観的評価

表1. グループチャット活用の主観的な纏め

便利と感じた点	インシデント疑いに対する情報の即時一元管理化が可能となった。
	インシデント疑い発生からのタイムライン作成の効率化が行えている。
	Microsoft Teams の機能として「いいね」ボタンがあり、意見への賛同が携帯端末等から手短に行え、チーム判断が活性化した。
	主観として、メールを見返すことが無い等のインシデント対応速度の向上が見られた。
	同時多発的に発生したインシデントの管理を混乱せずに管理できた。
不便な点	Teams のチャット機能に引用の機能が無く、また、スレッドの管理機能に不足を感じた。
	Teams の機能として、メンバー構成の設定をするだけのためにシステム全体の管理者権限が必要となり不便に感じた。
	Teams の機能として、包括契約に参加しているユーザ全体を検索できてしまい、巨大組織として、部局間の境界や隠匿すべきユーザ情報が見えてしまう。この為限られた特権ユーザのみで試用する事となった。

表１に Teams をグループチャットとして利利用した際の、利用者（インシデント対応チーム）の主観的な評価を纏め、示す。利用期間は

2019 年 4 月 1 日～9 月２０までの期間の主観的な纏めであり、大阪大学 本部 CSIRT 構成員及び数名の教職員の 11 名でチーム対応を行った。高度な判断を要する、グループチャットツールを利用したインシデント疑いの件数は 47 件であった。26 ファイルの共有情報ファイルが共有された。

5 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（Computer Security Incident Response Team）において、グループチャットツールを活用した際に、メールのみでのコミュニケーションと比べて、情報共有の一元化が行え、タイムライン作成が効率よく行えるようになった。同時多発的に並行で発生する部局ごとのインシデント疑い事案が、個々に判り易く管理されるようになった。

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] ファーエンドテクノロジー株式会社, redmine.jp/ ， 2019 年 9 月 20 日時点
[2] Slack 社, https://slack.com/intl/ja-jp/，2019 年 9 月 20 日時点
[3] Microsoft 社 , https://products.office.com/ja-jp/yammer/yammer-overview，2019 年 9 月 20 日時点
[4] Microsoft 社 , https://products.office.com/ja-jp/microsoft-teams/group-chat-software ， 2019 年 9 月 20 日時点