6V-02

標的型攻撃の早期検知に向けたSTIX/TAXIIの活用に関する検討

岡田　周平†　　後藤　厚宏†

情報セキュリティ大学院大学†

１．はじめに

近年，APT やばらまき型メール攻撃による被害が相次いでおり，標的型攻撃の脅威が顕在化している．標的型攻撃の手口は，ソーシャルエンジニアリングの駆使，マルウェアの多様化，通信の隠蔽等，巧妙化が進んでおり，攻撃の早期検知が困難となっている[1]．

標的型攻撃には手口を使い回すものがあり，その情報を早期収集することにより，被害を阻止できるものがある．特に，メール送信元 IP アドレス，電子メールの件名等，標的型攻撃の攻撃そのものの有無を判定できる情報は，攻撃の早期検知に有用である．

これらの情報を自組織のみで収集することは，サイバーセキュリティ対策資源が有限であるなか，困難である．複数の組織が連携して，脅威情報を共有することにより，より多くの情報を低コストで収集することができる．

しかしながら，現状，脅威情報の収集は，組織毎の個別対応が中心であり，組織間における適時適切な情報共有が課題となっている．本課題を解決するため，組織間連携において必要となる要素を定義する必要がある．

そこで，本稿では，脅威情報共有の観点から標的型攻撃の主な特徴を分析し，情報共有の有効性を考察する．その後，脅威情報の早期共有を実現するモデルを提案し，組織間における適時適切な情報共有を行うための要素を定義する．具体的には，モデルの構成要素である，情報の早期共有，共有情報の定義，情報共有に関わる組織と共有範囲及び情報共有基盤の整備について検討を行うとともに，基盤の整備において STIX 及び TAXII を活用することについて示す．

２．脅威情報共有の観点から分析した標的型攻撃の主な特徴と情報共有の有効性

報道されている事例[2]を基に，脅威情報共有の観点から分析した標的型攻撃の特徴及び情報共有の有効性に関する考察は次のとおりである．

(1)標的型攻撃の手口

攻撃対象に固有の手口を使う部分がある一方で，標的型攻撃のツールやインフラを使い回す部分がある．使い回される手口を共有し，当該情報を基に，組織内のログ分析を行えば検知可能な攻撃がある（例：医療費通知を装った標的型メール）．

(2)執拗な攻撃

攻撃者はひとつの組織に対して，複数回に亘り，執拗に攻撃を行うことがある．例えば，1 回目と 2 回目の攻撃では From 電子メールアドレスが使い回される等の共通点があることがあり，それぞれの情報を組織内及び組織間で共有することは，手口が使い回される攻撃に対して有効である．

Feasibility study on the use of STIX/TAXII for the early detection of targeted attacks

Shuhei OKADA†, Atsuhiro GOTO†

†Institute of Information Security

(3)侵害の進行の早さ

攻撃者は，短期間で目的の実行までの行動を達成することがある．組織間における迅速な情報共有や取得した情報を基にした組織内の分析は，侵害の早い標的型攻撃に対して有効である．

(4)攻撃対象

特定の組織，業種を狙う一方で，幅広い組織，業種を狙うことがある．特定の組織，業種を狙う攻撃は，攻撃の手口が広く知られない．同一業種において攻撃の手口を情報共有することは，同一業種にのみ狙う攻撃に対して有効である．

３．脅威情報の早期共有モデルの提案

3.1. 脅威情報の早期共有モデル

組織間における脅威情報の早期共有モデルを図 1 のとおり提案する．

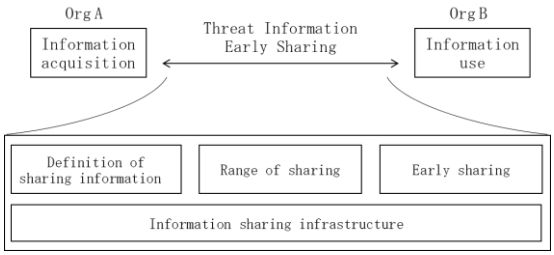


図１　脅威情報の早期共有モデル

早期共有モデルは，手口を使い回す標的型攻撃を早期に検知するため，組織間において適時適切に情報共有することを目的としている．具体的には，情報の早期共有，共有情報の定義，情報共有に関わる組織と共有範囲及び情報共有基盤の整備について定義する．

なお，早期共有モデルは，標的型攻撃に関する脅威情報源を拡充するものである．したがって，従来の検知方法を補完するものであり，本モデルに基づく情報共有により，検知力の向上に資するものである．

3.2. 情報の早期共有

(1)Cyber Kill Chain モデル

標的型攻撃対策モデルとして，Cyber Kill Chain が知られている[3]．本モデルでは，標的型攻撃のフェーズを，①偵察→②武器化→③デリバリ→④エクスプロイト→⑤インストール→⑥C&C→⑦目的の行動，に分解し，定義している．

標的型攻撃の被害規模は，攻撃フェーズの進展に応じて拡大するため，組織は標的型攻撃を早期に検知する必要がある．Cyber Kill Chain を有効に活用し，より早い攻撃フェーズで攻撃者の攻撃を適応的に検知できれば，被害を軽減することができると考えられる．

(2)情報の早期共有

本稿において定義する「早期共有」とは，標的型攻撃を早期検知するための情報共有を行うことである．「早期検知」とは，被害規模が拡大する前の③デリバリから

⑥C&C までの間に標的型攻撃を検知することをいう．組織間における脅威情報の早期共有の流れは，図 2 のとおりである．組織 B において早期検知を行うには，組織 A における標的型攻撃の検知後，組織 A は組織 B に対して，早期に情報共有する必要があると考えられる．

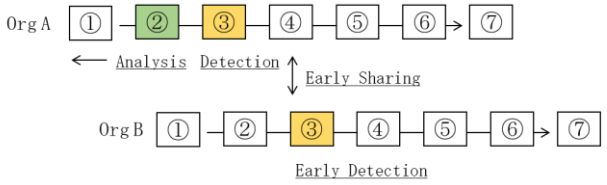


図 2　組織間における脅威情報の早期共有の流れ

3.3. 共有情報の定義

組織間で共有する情報としては，主に標的型攻撃の攻撃そのものの有無を判定できる情報，標的型攻撃の事案に関する知見，早期警戒情報等が考えられる．早期共有モデルでは，手口を使い回す標的型攻撃を早期に検知することを目的とするため，標的型攻撃の攻撃そのものの有無を判定できる情報の共有が適切である．「標的型攻撃そのものの有無を判定できる情報」とは，ログ分析が可能な情報であり，主にファイアウォール，メールサーバ及びプロキシサーバ等のログがあり，具体的には，次のものが挙げられる．

・メール送信元 IP アドレス
・From 電子メールアドレス
・電子メールの件名
・電子メールの添付ファイル名
・C&C 接続先ホスト名
・C&C 接続先 IP アドレス

3.4. 情報共有に関わる組織と共有範囲

(1)情報共有関連組織

本稿において定義する情報共有関連組織は，次のとおりである．

①情報提供組織

脅威情報を情報共有基盤へ提供する．

②情報利用組織

脅威情報を情報共有基盤から取得・利用する．

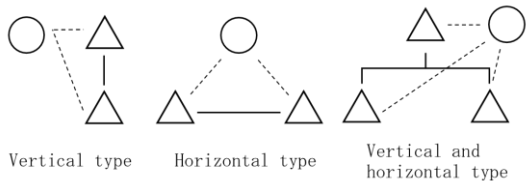
③情報共有組織

脅威情報を情報提供組織から受領する．また，脅威情報を情報利用組織へ提供する．情報共有基盤を管理する．

(2)情報共有の形態

情報共有の形態は，情報共有関連組織を踏まえ，図 3 の形態が考えられる．

①垂直連携型(例：本社・支社間)
②水平連携型(例：別の組織間)
③垂直水平連携型(例：グループ会社間)



(注)△は情報提供組織及び情報利用組織を指す．○は情報共有組織を指す．

図 3　情報共有の形態

(3)情報共有の範囲

共有情報は秘匿性の高い情報であるため，組織間で情報共有する場合，信頼できる相手方と共有することが原則である．信頼できない組織と情報共有した場合，虚偽の情報が共有される可能性もある．したがって，信頼の基盤となる情報管理の前提条件を定める必要がある．

3.5. 情報共有基盤の整備

情報の早期共有，共有情報の定義及び情報共有に関わる組織と共有範囲を満たす，情報共有基盤の要件は，次のとおりである．

(1)フォーマットの統一

情報提供組織が脅威情報を入力するフォーマットが必要である．当該フォーマットには，前述で定義した情報や情報提供組織に関する情報が含まれる．

(2)アクセス制御

情報共有基盤では，秘匿性の高い情報を共有するため，情報提供組織と情報利用組織の範囲でのみアクセスを許可する機能が必要である．

(3)情報共有の自動化

情報共有基盤において，早期に情報共有を行うため，情報の提供・利用を自動的に行う必要がある．

(4)データタイプ

脅威情報の受領時，情報利用組織が即座に分析できるように，機械判読性の高い状態で提供する必要がある．

(5)共有情報のデータ管理

共有情報について，登録，更新及び抹消に関するデータ管理を行う必要がある．正規の Web サイトを改ざんされた場合，情報共有時は悪性 URL であった先が後日，正常 URL に状態が遷移することがある．このような場合，登録情報を更新する必要がある．

(6) STIX 及び TAXII の活用

上記(1)～(5)の要件を満たす情報共有基盤を整備するため，脅威情報を共有するための標準化された仕様である，STIX[4]及び TAXII[5]を活用することが考えられる．

4．まとめ

本稿では，脅威情報共有の観点から標的型攻撃の主な特徴を分析し，情報共有の有効性を考察した．その後，脅威情報の早期共有モデルを提案し，モデルの構成要素について検討を行うとともに，情報共有基盤の整備において STIX 及び TAXII を活用することについて示した．今後，本モデルの有効性を評価するため，早期共有モデルの実装を目指す．

参考文献

[1] 独立行政法人情報処理推進機構：「高度標的型攻撃」対策に向けたシステム設計ガイド，https://www.ipa.go.jp/files/000046236.pdf（参照 2015-08-04）
[2] サイバーセキュリティ戦略本部：日本年金機構における個人情報流出事案に関する原因究明調査結果，http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf（参照 2015-08-26）
[3] Eric Hutchins, Michael Cloppert, Rohan Amin： Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 6th International Conference on Information Warfare and Security, pp.113-125 (2011)
[4] The MITRE Corporation：Structured Threat Information eXpression，https://stixproject.github.io/（参照 2016-01-05）
[5] The MITRE Corporation：Trusted Automated eXchange of Indicator Information，https://taxiiproject.github.io/（参照 2016-01-05）