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

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

岡田　周平・マネジメント分科会・情報セキュリティ大学院大学

Abstract：In recent years, APT and email spam attack have sparked incidents, threat of targeted attacks become obvious. Organizations can get more information at low cost by cyber threat information sharing. But currently cyber threat information acquisition is major way to deal with single organization, so it is the challenge to sharing threat information between organizations. To deal with this challenge, we propose a threat information early sharing model and to share signature using STIX and TAXII.

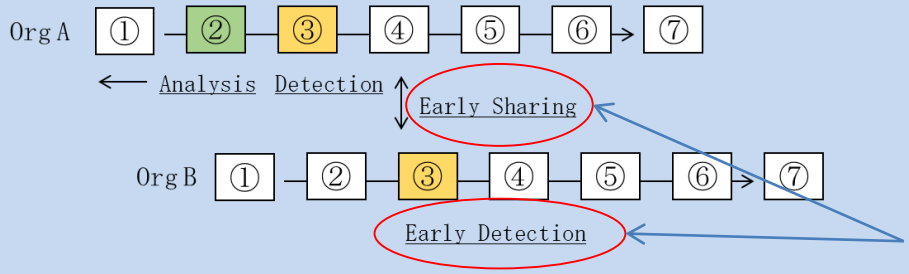
【方針①：脅威情報の早期共有モデル】

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（＝国際標準）を活用する．また，情報共有基盤の実装を行い，脅威情報を早期共有できるか検証し，本モデルの要件を満たしているか評価する．

【方針②：STIX及びTAXIIを用いたシグネチャの共有】

標的型攻撃を検知するための情報として，ネットワーク型IDS，ホスト型IDS，WAFで用いるシグネチャがある．これらは即時性も高く，特に有用であると考えられる．当該情報をSTIX及びTAXIIで共有できれば，組織間での利便性も高まると考えられる．そこで，（ⅰ）組織において有用なシグネチャを作成するために必要な項目を調査・検討し，（ⅱ）STIX及びTAXIIを用いたシグネチャの共有の実現性を調査，実装及び評価する．

【情報の早期共有とは】

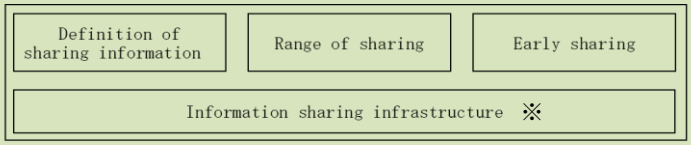


Exploit Phase

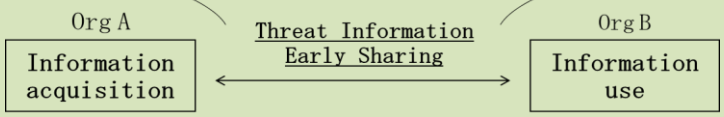
① Reconnaissance
② Weaponization
③ Delivery
④ Exploitation
⑤ Installation
⑥ C2
⑦ Actions on Objectives

この部分の早期化が目標！

【情報の早期共有モデル】



早期共有モデルの構成要素



※情報共有基盤が満たすべき要件
①フォーマットの統一，②アクセス制御，③情報共有の自動化，④機械判読性の高いデータタイプ，⑤共有情報のデータ管理，⑥STIX及びTAXIIの活用

① OrgA のフォーマットへの入力

title	mal IP
Indicator Type	IP Watchlist
From Mailaddr	
Mailsource Ipaddr	218.XX.XX.XX
Mail title	
Mail attachment	
C2 host	
C2 IPaddress	

➢ 即時性の高い脅威情報を定義

② STIXへの変換

③ OrgB のXMLデータの受領（STIX Expression）

```
<stix:Indicators>
  <stix:Indicator id="myNS:indicator-32ce10d9-b173-4fb0-8d7d-9b51419d14ae"
   timestamp="2016-02-05T22:50:42.336973+00:00" xsi:type='indicator:IndicatorType'>
    <indicator:Title>mal IP</indicator:Title>
    <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</indicator:Type>
    <indicator:Observable id="myNS:Observable-600d3ec9-db79-4d64-82a9-0317469003fc">
      <cybox:Object id="myNS:Address-a73463ec-6e13-4bf7-b513-3532fd07804c">
        <cybox:Properties xsi:type="AddressObj:AddressObjectType" category="ipv4-addr">
          <AddressObj:Address_Value
           condition="Equals">218.XX.XX.XX</AddressObj:Address_Value>
        </cybox:Properties>
      </cybox:Object>
    </indicator:Observable>
  </stix:Indicator>
</stix:Indicators>
```

➢ 国際標準であり，高汎用性を実現
➢ STIX及びTAXIIを用いたシグネチャの生成，共有を検討