脆弱性管理と資産管理との連携への取組み

寺田真敏 †1 †2

概要:サイバー攻撃の高度化・巧妙化に伴い，民間企業等の情報システムへの脅威が深刻化している．サイバー攻撃の被害を防ぐためには，日々公開される脆弱性に対して迅速に対応することが求められ，各組織で使用しているどのソフトウェアがどの脆弱性の影響を受けるかを判別することが重要となる．本稿では，サイバー攻撃への迅速な対応を可能にする環境を実現するため，多層防御のための情報活用基盤を提示すると共に，脆弱性情報とソフトウェア資産情報の管理における運用上の課題と解決の方向性について述べる．

1. はじめに

サイバー攻撃手法はますます複雑化・巧妙化しており，組織は日々新しい脅威情報を入手し，迅速に対応する必要がある．このようなサイバー攻撃の脅威に対応していくため，企業間・組織間で互いの持つ脅威情報を活用していくアプローチがある．

本稿では，このアプローチを拡張し，多層防御のための情報活用基盤を提示すると共に，この情報活用基盤を用いて解決したい課題について述べる．

2. 多層防御のための情報活用基盤

多層防御のための情報活用基盤では，攻撃スピードに追従するために，STIX/TAXII によるシステムを介した連携(機械処理系，machine readable)を想定し[1]，(1)脅威などの攻撃元情報だけではなく，脆弱性などの攻撃先情報を活用すると共に，(2)これら情報を資産や部品成分表(SBOM:Software Bill of Materials)[2]と紐付けて活用する(図 1)．ここで，攻撃元とは，攻撃者側のリソースに関するものであり，攻撃者自身，マルウェアや C2 サーバなどの攻撃者の代行となるものである．攻撃先とは，攻撃者が攻撃対象とするリソースに関するものであり，被害者となるユーザ自身，情報ならびに制御システムの設計・コード・設定などの脆弱性，情報ならびに制御システム上で流通するデータなどが該当する．

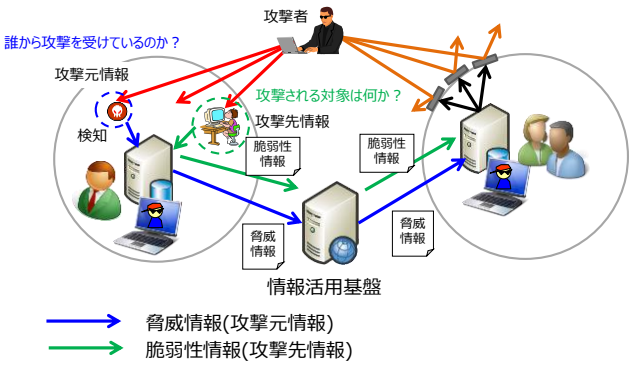


図 1:多層防御のための情報活用基盤

3. 情報活用基盤を通して解決したい課題

情報活用基盤を通して解決したい 4 つの課題について述べる．

【課題 1】脆弱性情報の件数は増加傾向

米国脆弱性対策データベース(NVD: National Vulnerability Database)に登録されている件数は，脆弱性を分担協力して登録する組織(脆弱性登録組織)の増加と共に増加している(図 2)．増加傾向にある脆弱性情報への対応を人手に依存した場合，その人の技量によってしまうことになる．

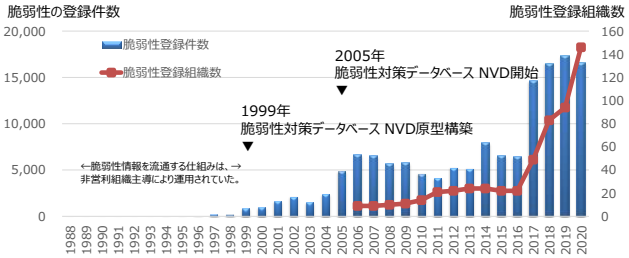


図 2:脆弱性報告件数の推移

【課題 2】インストール状況と脆弱性との紐付けは人手

攻撃元/攻撃先情報のいずれも，組織の保有する資産との紐づけを想定しておらず，多くの場合，インストール状況と脆弱性との紐付けを人手で実施している．すなわち，資産管理と脆弱性対策とが連携できているわけではない[3].

【課題 3】カスタムアプリ管理は整備途上

攻撃元/攻撃先情報のいずれも，委託などで開発したカスタムアプリを想定していない，あるいは部品成分表(SBOM)との紐づけを想定していない．これらカスタムアプリの場合には，資産管理や脆弱性管理を前提とした開発が行われていないこともあり，管理対象から漏れてしまうことになる．

【課題 4】脅威情報と脆弱性情報は個別に情報展開

脅威などの攻撃元情報と脆弱性などの攻撃先情報は，個別に情報展開されており，攻撃元情報と攻撃先情報との相互活用を想定する運用形態には至っていない．

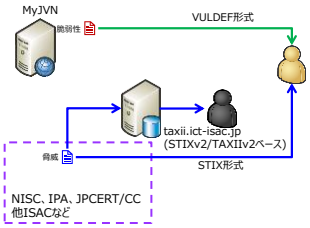
†1 東京電機大学, Tokyo Denki University.
†2 一般社団法人 ICT-ISAC, ICT-ISAC Japan

4. 課題解決のアプローチ

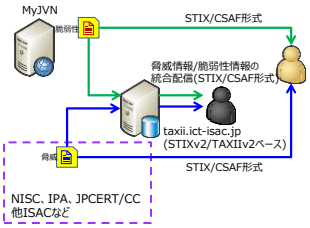
課題の情報活用基盤における課題解決のアプローチは，次の通りである．

- 脅威情報/脆弱性情報の統合配信【課題 1】【課題 4】

一つの情報展開ストリームに攻撃元ならびに攻撃先情報を重畳させることで，ここにアクセスさえすれば，攻撃元ならびに攻撃先情報が入手できる情報活用基盤を作ることができる．また，脅威などの攻撃元情報と脆弱性などの攻撃先情報との有機的な連携も容易となる(図 3).



脅威情報と脆弱性情報を異なるフォーマット，いろいろなサイトから受信している．

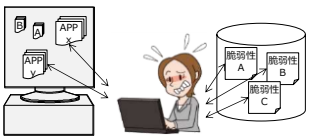


脅威情報と脆弱性情報を同じフォーマット，ひとつのサイトから受信できる．

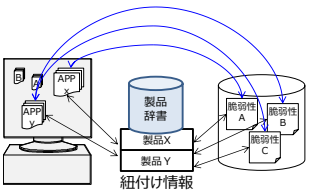
図 3:脅威情報/脆弱性情報の統合配信

- 資産と紐付けられる脅威情報/脆弱性情報の配信【課題 2】【課題 4】

攻撃元ならびに攻撃先情報を資産と紐付け，さらに資産管理ツールと連携することで，攻撃元/攻撃先情報の選別だけではなく，影響有無などの対策につなげることができる(図 4).



インストール状況と脆弱性との紐付けを人手で実施している．

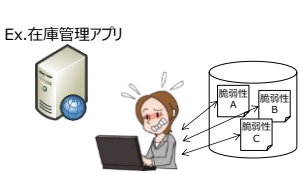


製品辞書(製品識別子とインストール名との対応表)を使用し，インストール状況を把握できる情報と脆弱性情報とを紐付ける．

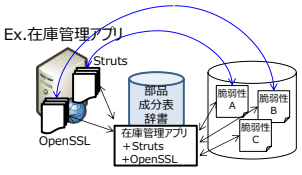
図 4:製品辞書による紐付け

- 部品成分表と紐付けられる脅威情報/脆弱性情報の配信【課題 3】【課題 4】

カスタムアプリの部品成分表(SBOM)を管理し，攻撃元ならびに攻撃先情報をカスタムアプリの部品成分表(SBOM)と紐付け，さらに資産管理ツールと連携することで，攻撃元ならびに攻撃先情報の選別だけではなく，影響有無などの対策につなげることができる(図 5).



カスタムアプリ(SI で開発したアプリケーションなど)は，資産管理や脆弱性管理の対象に含まれていないことがある．



カスタムアプリの部品成分表辞書(カスタムアプリで使用しているアプリケーション一覧)を整備し，アプリケーション一覧と脆弱性対策情報とを紐付ける．

図 5:部品成分表による紐付け

5. おわりに

本稿では，多層防御のための情報活用基盤を提示すると共に，この情報活用基盤を用いて解決したい課題について述べた．今後，個々の課題を解決していくことで，脅威などの攻撃元情報と脆弱性などの攻撃先情報との有機的かつ連携可能な情報配信(図 6)を検討していきたいと考えている．

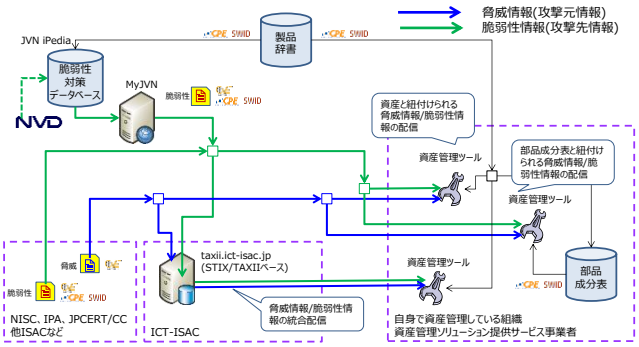


図 6:多層防御としての情報活用基盤と想定する将来像

謝辞

本研究にあたって，有益な助言を頂いた総務省「ソフトウェア脆弱性を狙ったサイバー攻撃の防御に向けた情報共有基盤に関する実証実験」の関係者各位に深く感謝いたします．

参考文献

[1] (一社)ICT-ISAC，サイバー攻撃の防御に向けた情報共有基盤に関する実証事業について https://www.ict-isac.jp/news/news20180629.html (参照 2021-05-10)

[2] National Telecommunications and Information Administration, SOFTWARE BILL OF MATERIALS, https://www.ntia.gov/SBOM, (参照 2021-05-10)

[3] 寺田真敏，他: 製品識別子を用いた脆弱性対策情報データベースと資産管理との連携に関する検討，情報処理学会 研究報告コンピュータセキュリティ(CSEC),2016-CSEC-72(3), (2016-02-25)