ICT-ISAC情報共有基盤の活動紹介
～脆弱性情報の取り扱いについて～

2022年7月22日

寺田真敏(ICT-ISAC情報共有WG主査)

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

ICT-ISAC情報共有基盤の活動紹介

目次

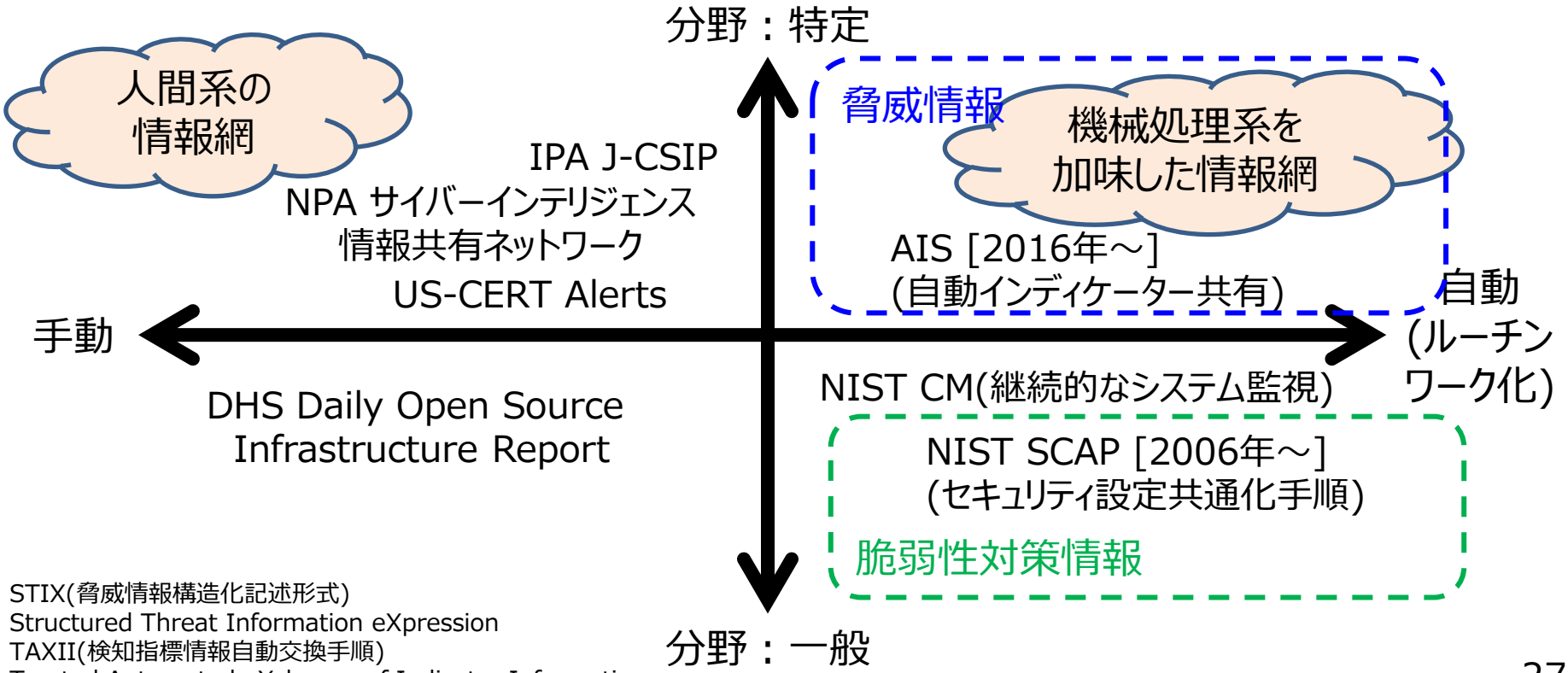
- 背景：情報共有と機械可読化の潮流
  - 米国での取り組み
  - サプライチェーン／ソフトウェアサプライチェーン
  - ソフトウェアサプライチェーンへのサイバー攻撃

- 脅威/脆弱性情報と資産情報との連携
  - ICT-ISAC Japan での取組み
  - 脅威情報：バンキングマルウェア情報
  - 脅威情報：ブロックリスト
  - 脆弱性情報：脆弱性深刻度評価システム(Vuldate)

背景：情報共有と機械可読化の潮流

米国での取り組み

- ルーチンワーク化(コンピュータ処理)による対処
  「ルーチンワーク化」の部分は、一般的にMachine Readableと言われている。
  直訳すると機械可読であるが、手順化してコンピュータ処理することを意味する。

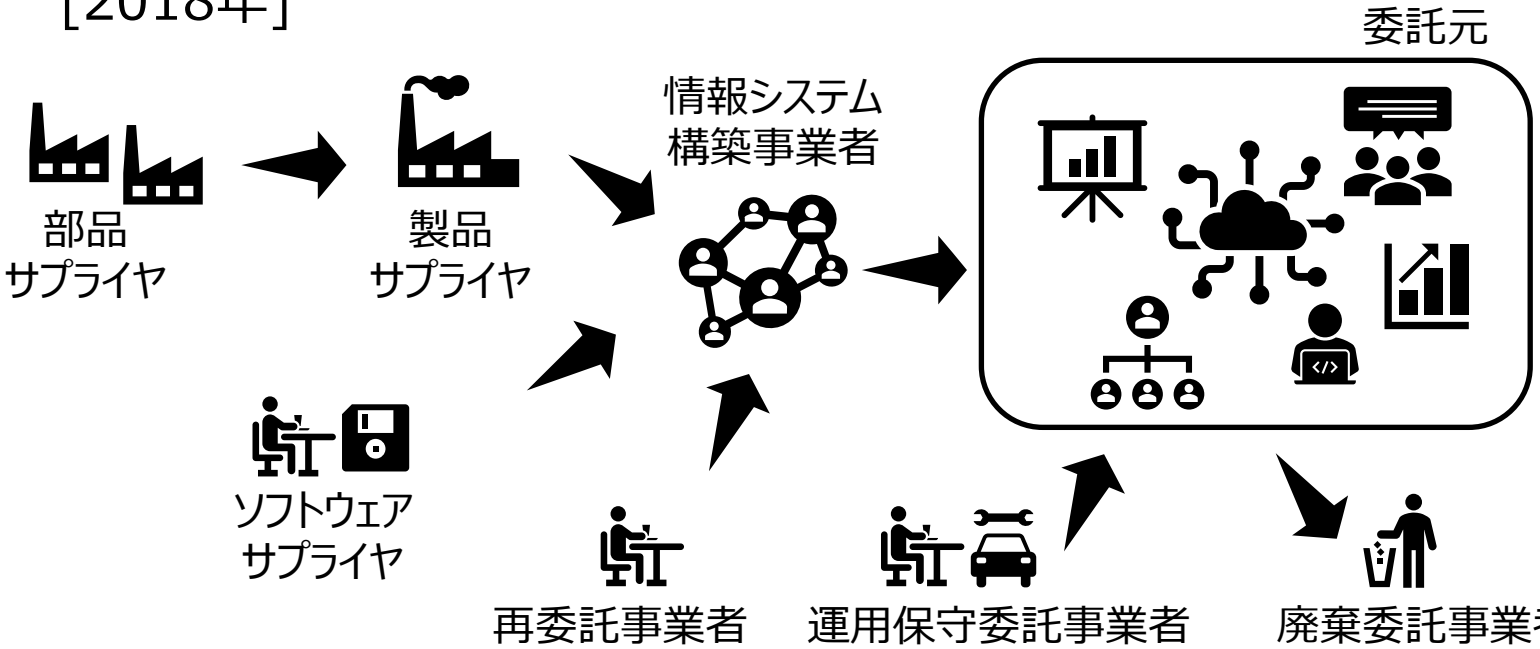


STIX(脅威情報構造化記述形式)
Structured Threat Information eXpression
TAXII(検知指標情報自動交換手順)
Trusted Automated eXchange of Indicator Information

背景：情報共有と機械可読化の潮流

サプライチェーン

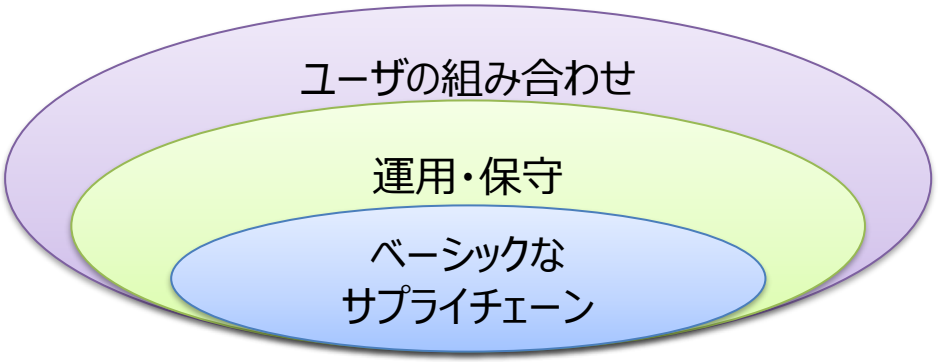
- ITにおけるシステム開発やサービス提供/利用に関する連鎖
- ビジネスパートナーや委託先企業も含めたサプライチェーン全体でのセキュリティ対策の必要性の高まり
  - サイバーセキュリティ経営ガイドラインv2.0 [2017年]
  - 米国立標準技術研究所(NIST) サイバーセキュリティフレームワークv1.1 [2018年]



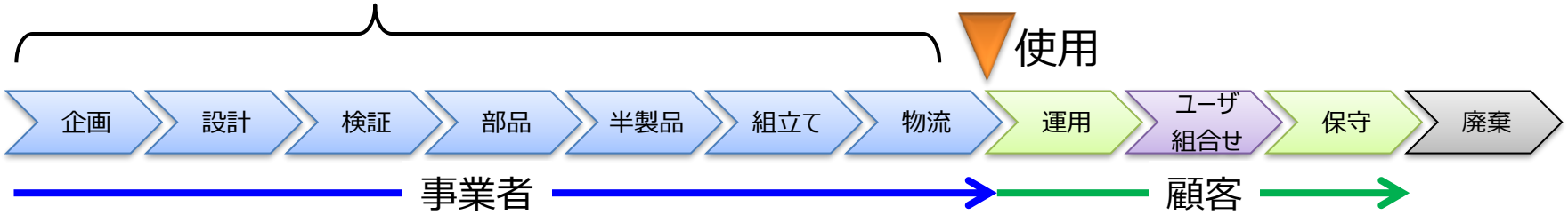
背景：情報共有と機械可読化の潮流

ソフトウェアサプライチェーン

- ソフトウェアの開発から、それがエンドユーザに使用されるまでの流通、その後の運用・保守、およびユーザが組合せて利用するまでの、それに関与する組織の活動、役割、情報、資源等を指すもの



ベーシックなサプライチェーン
個々の企業の役割分担にかかわらず、ソフトウェアの企画の段階からソフトウェア製品やサービスがエンドユーザの手に届くまでの全プロセスの繋がり

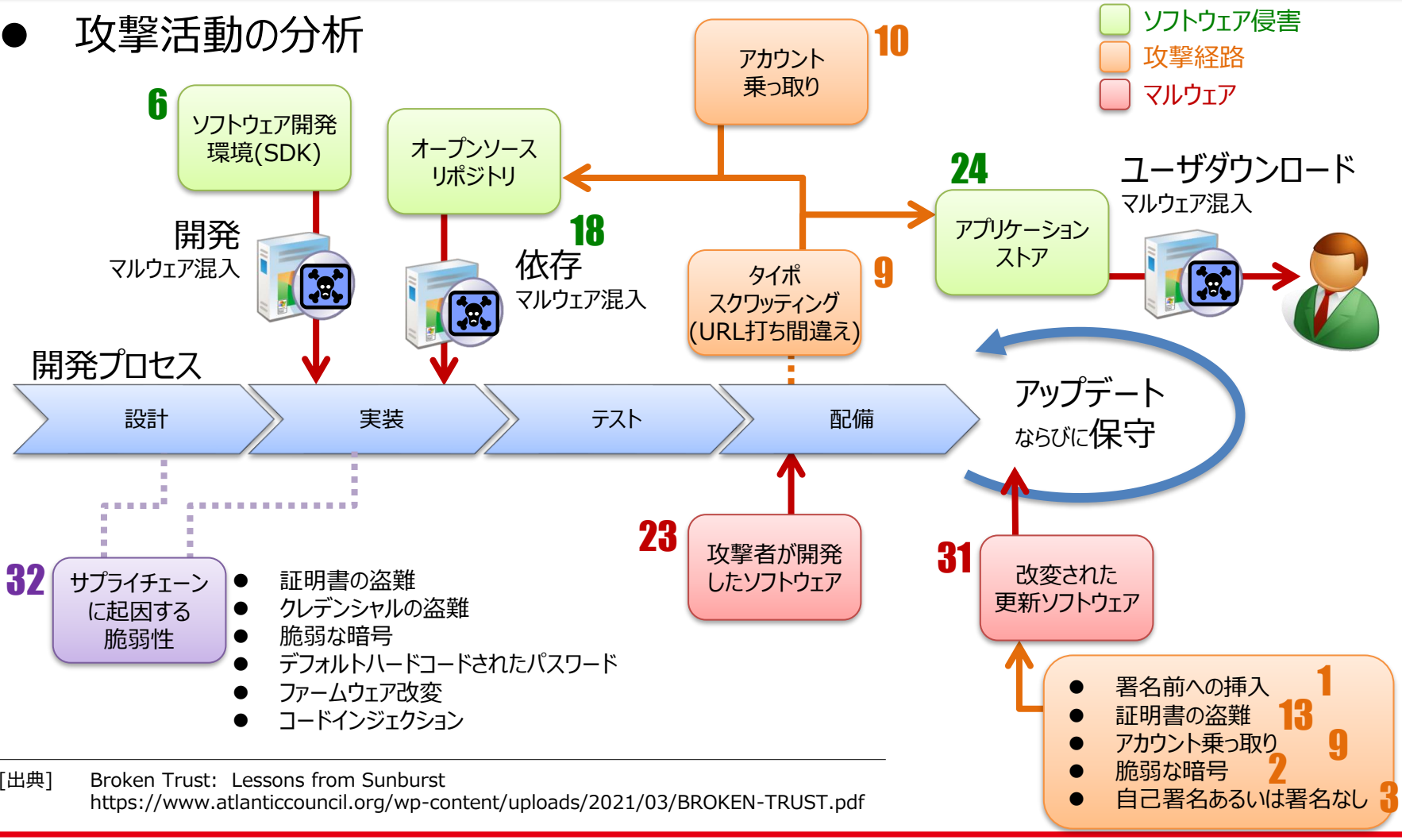


[出典]　ソフトウェアサプライチェーンにおける変化と課題 [2014年]
https://www.ipa.go.jp/files/000040879.pdf

背景：情報共有と機械可読化の潮流

ソフトウェアサプライチェーンへのサイバー攻撃

- 攻撃活動の分析

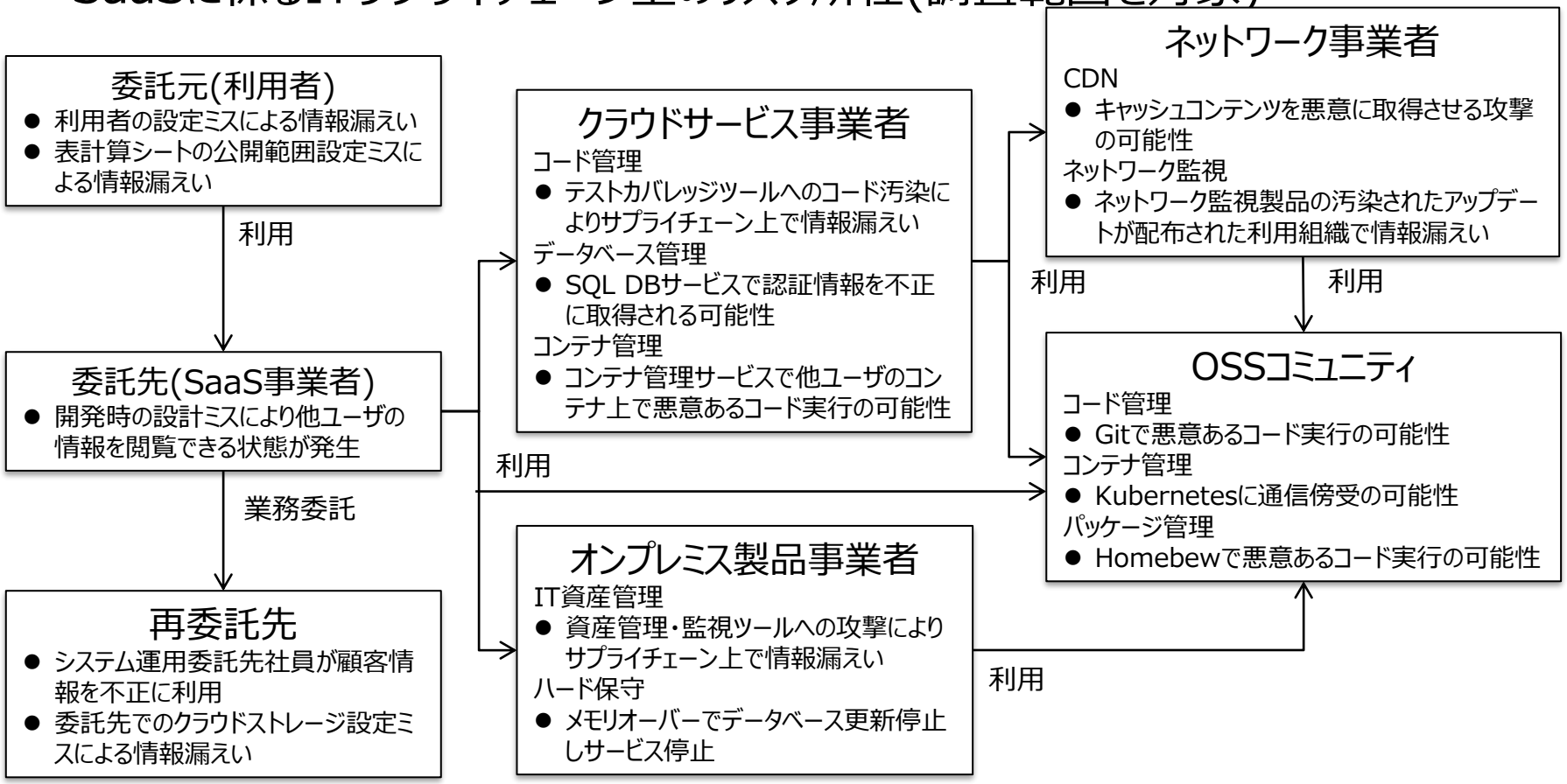


[出典] Broken Trust: Lessons from Sunburst
https://www.atlanticcouncil.org/wp-content/uploads/2021/03/BROKEN-TRUST.pdf

背景：情報共有と機械可読化の潮流

ソフトウェアサプライチェーンへのサイバー攻撃

- SaaSに係るITサプライチェーン上のリスク所在(調査範囲を対象)

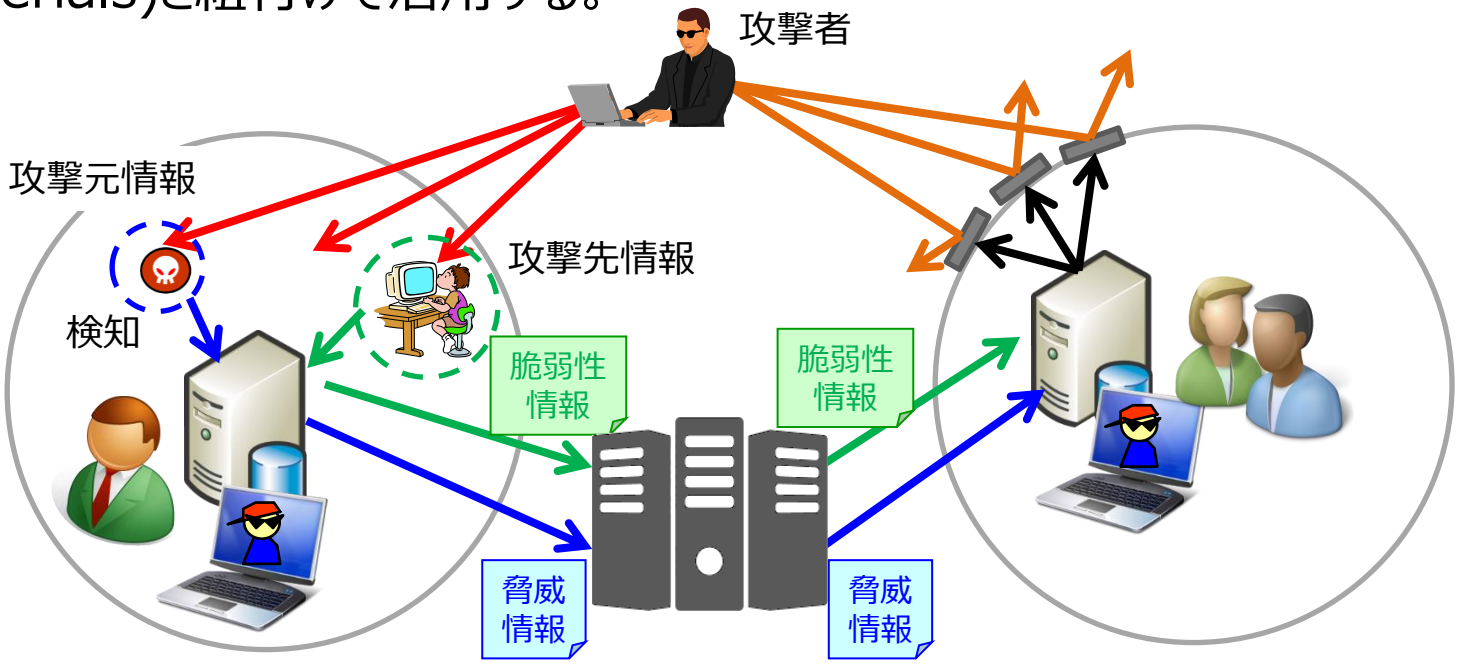


[出典] クラウドサービスのサプライチェーンリスクマネジメント調査 [2022年]
https://www.ipa.go.jp/security/fy2021/reports/scrm/index-cloud.html

背景：情報共有と機械可読化の潮流

脅威情報と脆弱性情報の連携

- 多層防御としての(情報活用＋対策)
- 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ソフトウェア部品表(SBOM:Software Bill of Materials)と紐付けて活用する。



脅威/脆弱性情報と資産情報との連携

ICT-ISAC Japan での取組み

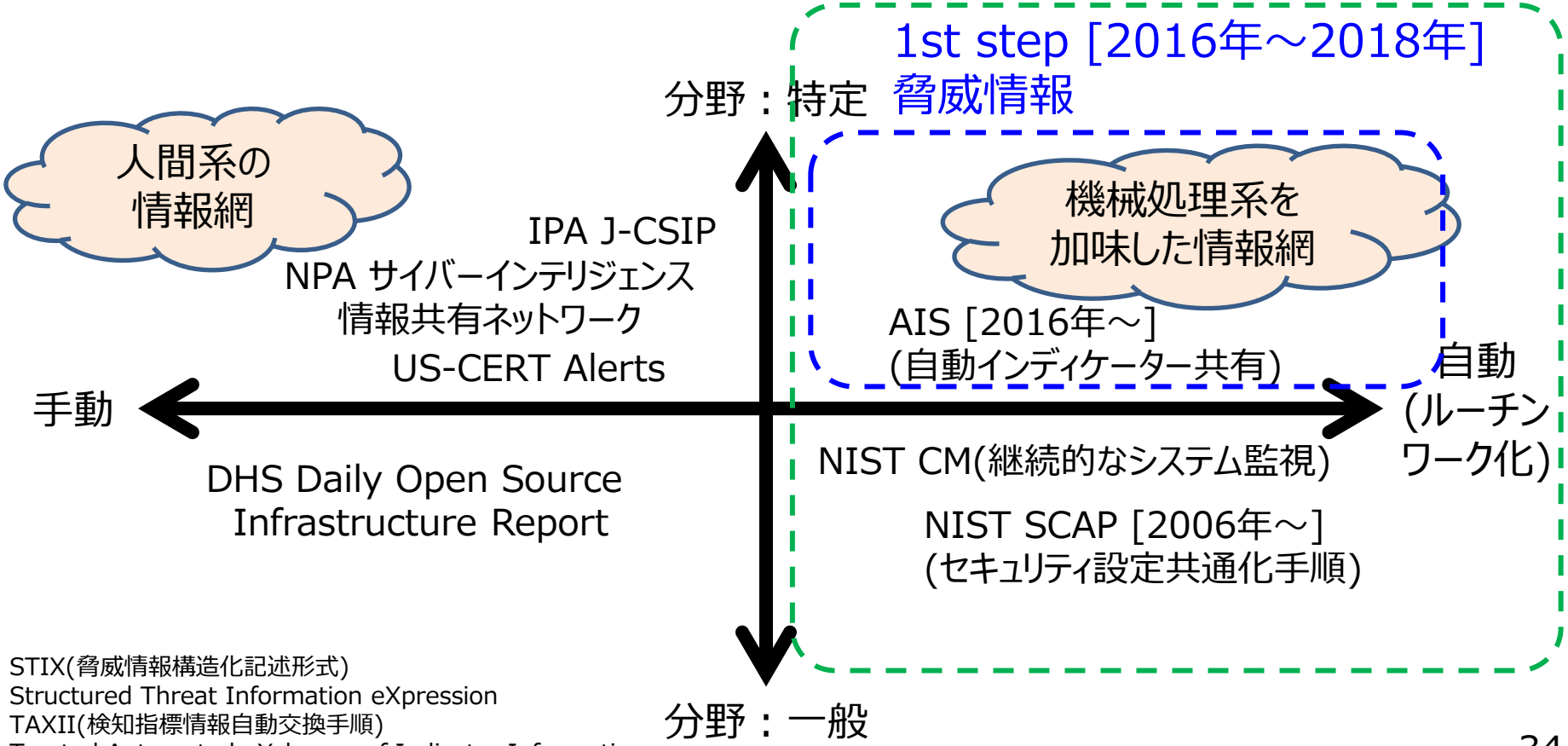
- 1st step [2016年～2018年] 多層防御としての情報活用
  - 脅威情報
  - 脅威情報(IPアドレス、ドメイン、URL、ハッシュ値)を交換するための場として、STIX v1/TAXII v1環境であるtaxii.ict-isac.jpをSoltraを使用して構築し、試行運用した。
  - 総務省「サイバー攻撃への集団防御に向けた情報共有基盤に関する実証事業」との連携
- 2nd step [2019年～] 多層防御としての情報活用
  - (脅威情報＋脆弱性情報)*資産管理連携
  - 脅威情報(IPアドレス、ドメイン、URL、ハッシュ値)と脆弱性情報とを関連付け、資産管理と連携するための場として、STIX v1+v2/TAXII v1環境であるtaxii.ict-isac.jpをOpenTAXIIを使用して構築し、試行運用中
  - 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」との連携
  - 総務省「脆弱性情報の高精度な深刻度・信頼度評価に関する実証実験」において構築した脆弱性評価システムとの連携

脅威/脆弱性情報と資産情報との連携

ICT-ISAC Japan での取組み

- 1st step [2016年～2018年]
- 2nd step [2019年～]

2nd step [2019年～]
(脅威情報＋脆弱性情報)×資産管理連携

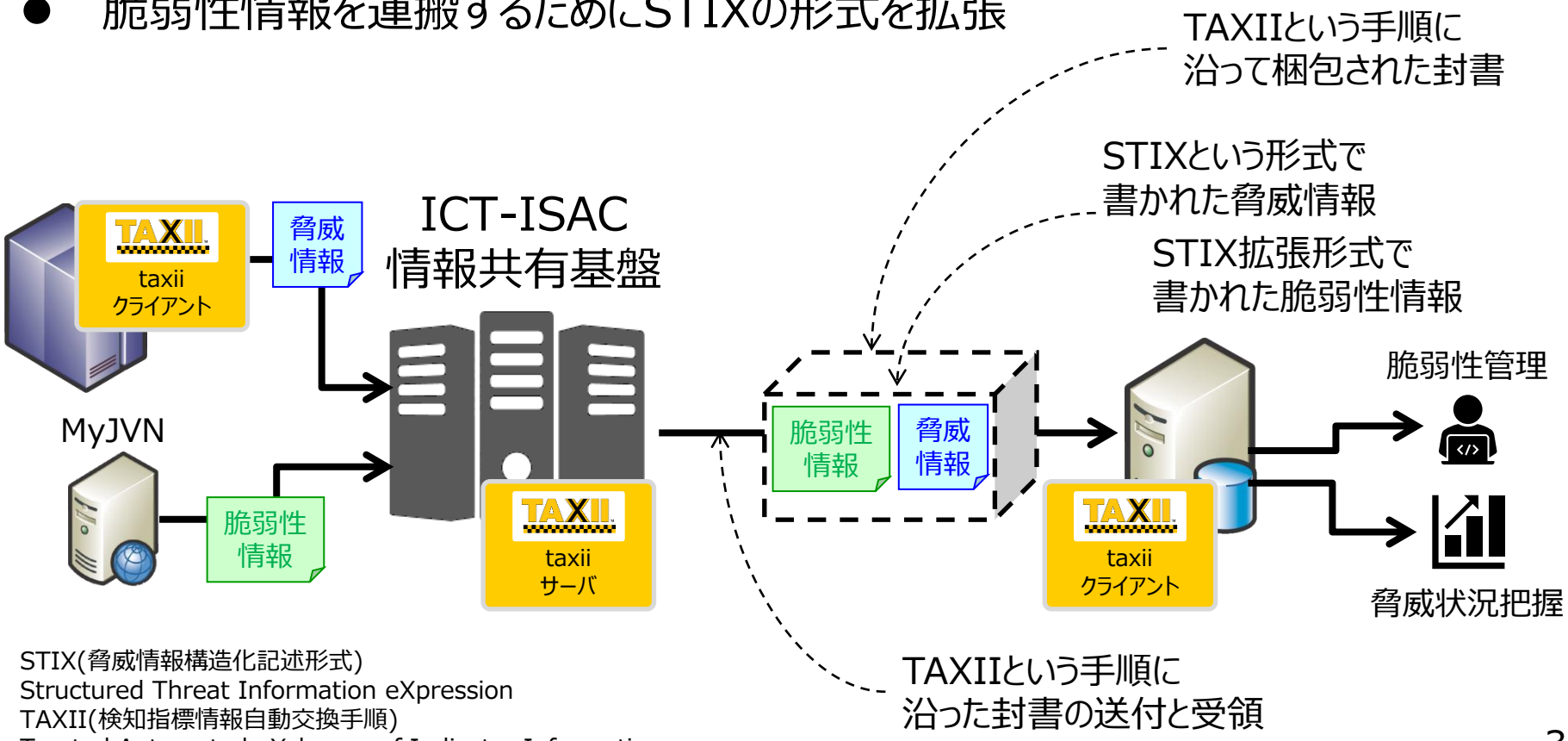


STIX(脅威情報構造化記述形式)
Structured Threat Information eXpression
TAXII(検知指標情報自動交換手順)
Trusted Automated eXchange of Indicator Information

脅威/脆弱性情報と資産情報との連携

ICT-ISAC Japan 情報共有基盤

- 多層防御としての情報活用を実現するために、STIXという形式で書かれた脅威情報をTAXIIという手順を使って交換
- 脆弱性情報を運搬するためにSTIXの形式を拡張



STIX(脅威情報構造化記述形式)
Structured Threat Information eXpression
TAXII(検知指標情報自動交換手順)
Trusted Automated eXchange of Indicator Information

脅威/脆弱性情報と資産情報との連携

ICT-ISAC Japan 情報共有基盤

- 多層防御としての情報活用を実現するために、利用目的に合わせてグループ化

区分	名称	用途
脅威	AIS	米国政府が運用するAIS(Automated Indicator Sharing)から提供されている情報の一部
	C2	動的解析装置が検知した不正接続先(IPアドレス、ドメイン、URL)で、ダウンローダサイトを含む広義のC２情報
	BKMW_CONF	バンキングマルウェア情報(マルウェアの設定ファイル配布サイト)
	BKMW_ATTK	バンキングマルウェア情報(攻撃対象となる金融機関サイト)
	BKMW_MANU	バンキングマルウェア情報(攻撃操作サイト)
	BLOCKLIST	組織で適用している不正接続先遮断リスト交換
脆弱性	VULS2	脆弱性情報 (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」、「脆弱性情報の高精度な深刻度・信頼度評価に関する実証実験」)

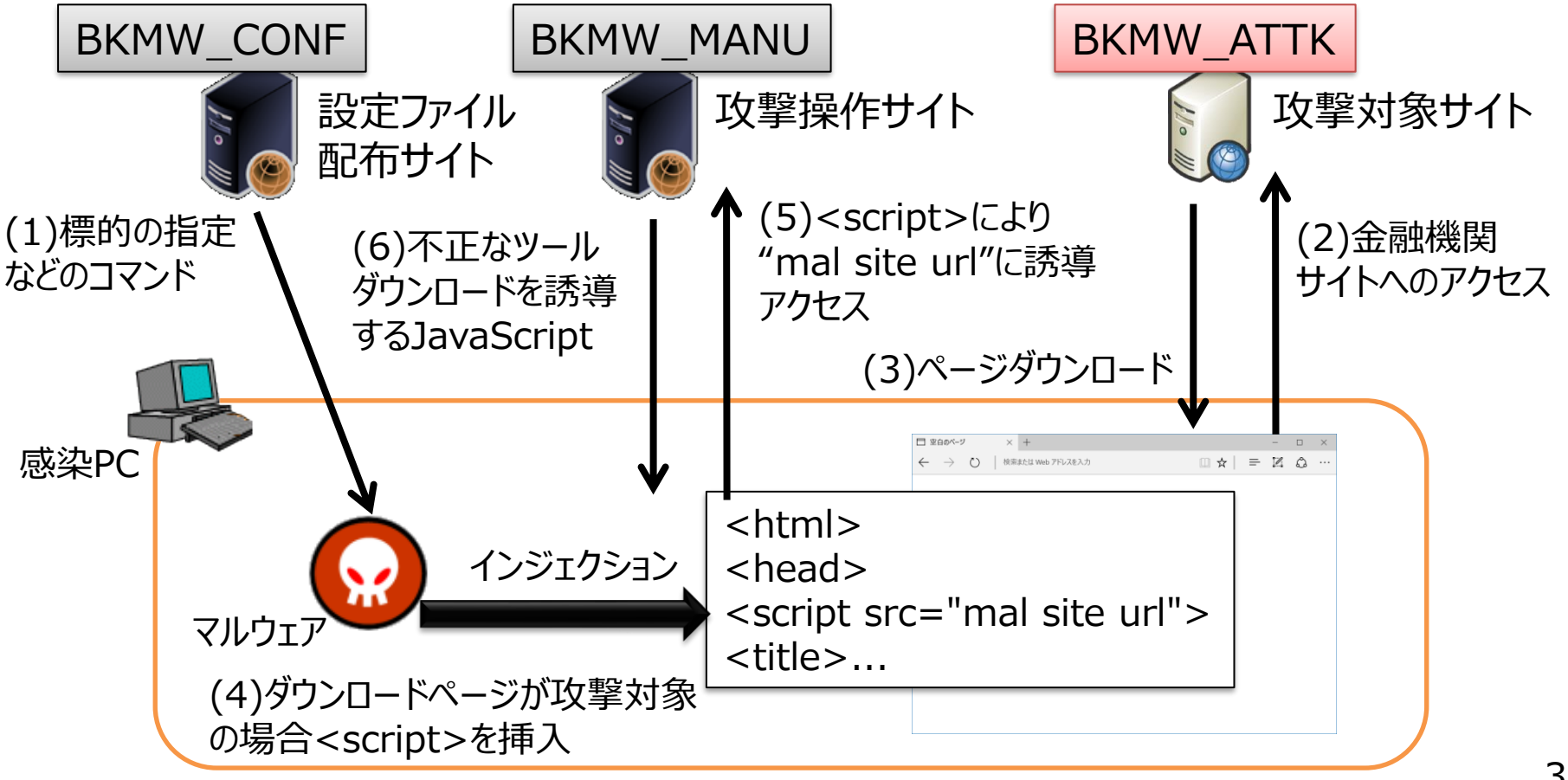
脅威情報
バンキングマルウェア情報

- 分野間連携への可能性
- 攻撃先情報の記述表現の強化

攻撃先情報：バンキングマルウェア

バンキングマルウェアによるサイバー攻撃活動

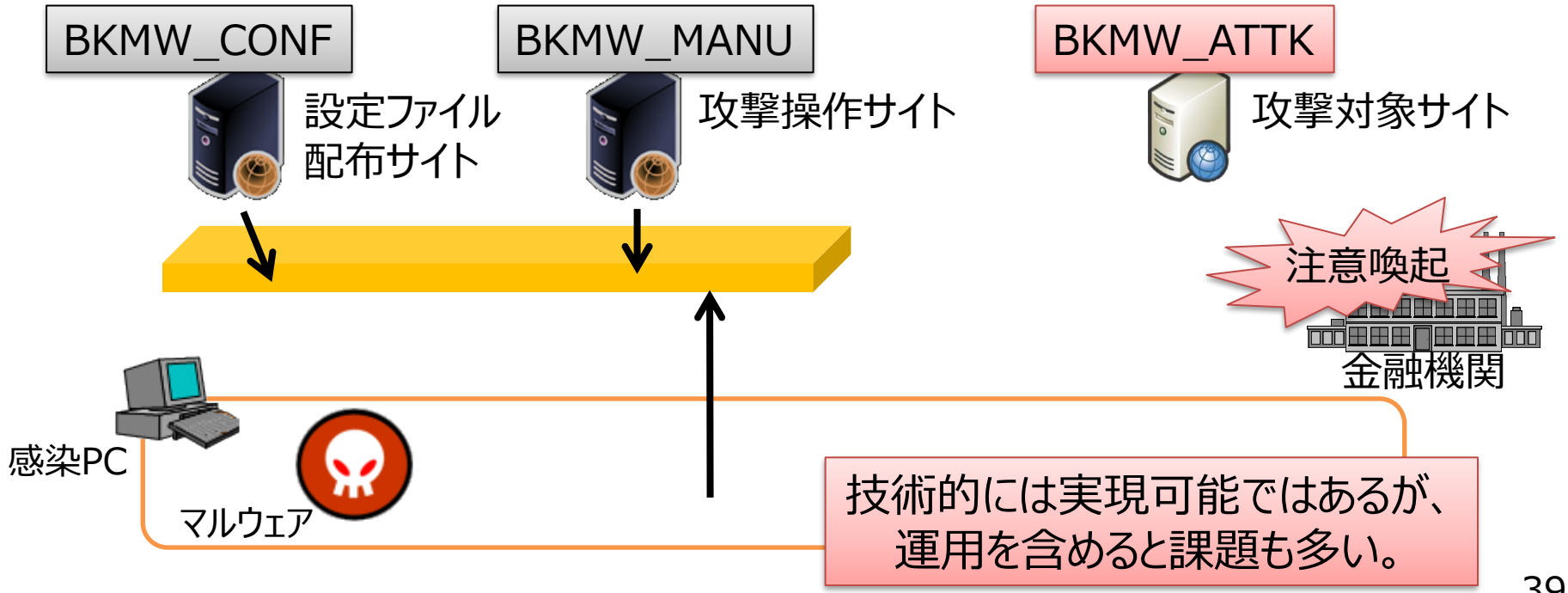
- 複数サイトが連携してサイバー攻撃を仕掛けている。



攻撃先情報：バンキングマルウェア

バンキングマルウェアによるサイバー攻撃活動への対処可能性

- 情報共有基盤として、接続ブロックや注意喚起などの対策につなげる。
  - マルウェアの設定ファイル配布サイト、攻撃操作サイトなど、不正接続先であるサーバのドメイン、IPアドレスを通知し、接続ブロックなどの対策へ
  - 攻撃対象となる金融機関サイトを通知し、注意喚起などの対策へ

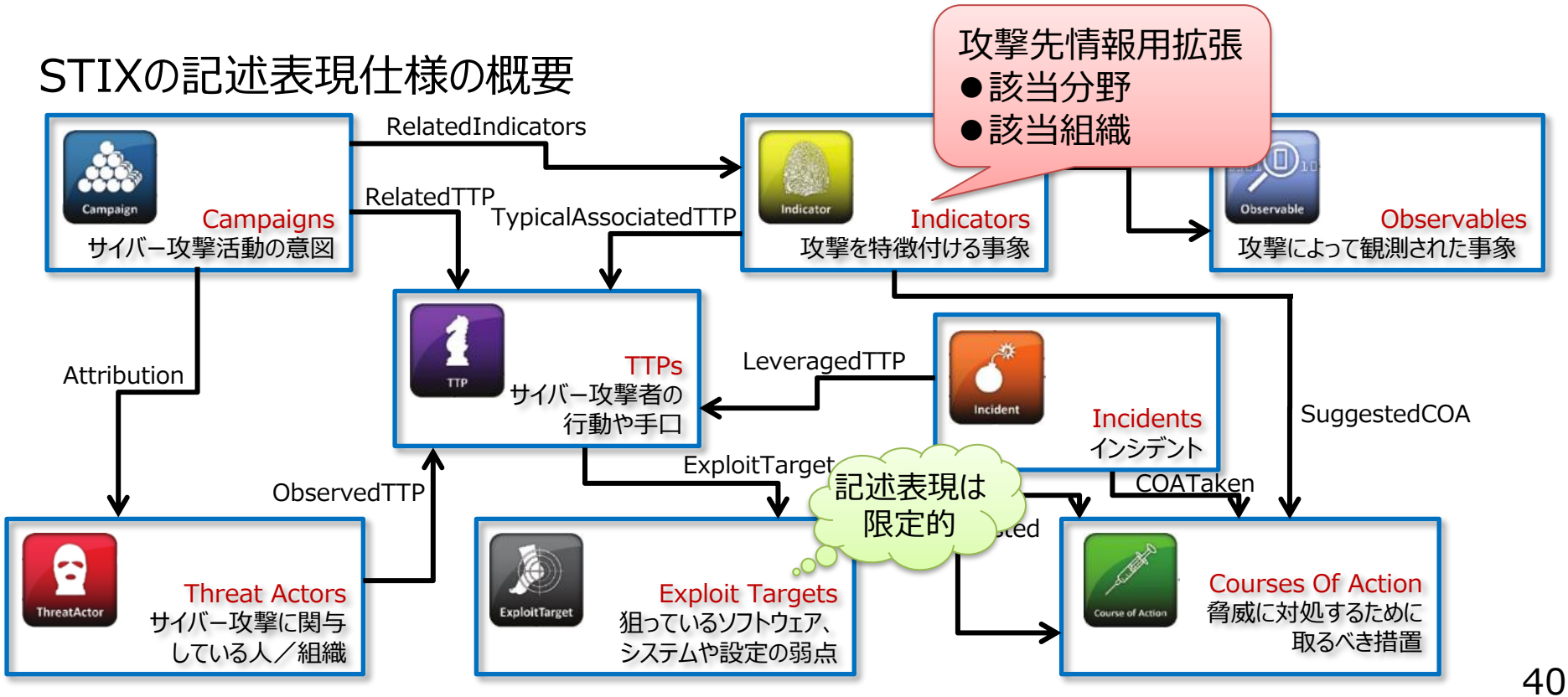


攻撃先情報：バンキングマルウェア

バンキングマルウェアによるサイバー攻撃活動への対処

- STIXで脅威情報を記載する際、攻撃先に関する記述表現仕様が不十分
  - 攻撃先情報を運搬するためにSTIXの形式を拡張
  - 今後、URL、ドメイン、IPアドレスによる記述表現仕様も必要

STIXの記述表現仕様の概要



脅威情報
ブロックリスト

- 評価済情報の活用

攻撃元情報：ブロックリスト

1st step [2016年～2018年]で学んだこと

- 情報共有が普及しない原因の一つは、分析と配信機能との不明瞭な役割分担
- 情報共有基盤の主機能は、配信機能とし、分析機能は外付けとすべき

受信者は、自分に必要となる情報が付いていないと欲しいとは思わない。

区分	概念図	事例
分析機能		ICOAST(インテリジェンスコミュニティの分析・シグネチャ情報共有ツール)
配信機能		AIS(自動インディケーター共有) STIX/TAXII環境

攻撃元情報：ブロックリスト

1st step [2016年～2018年]で学んだこと

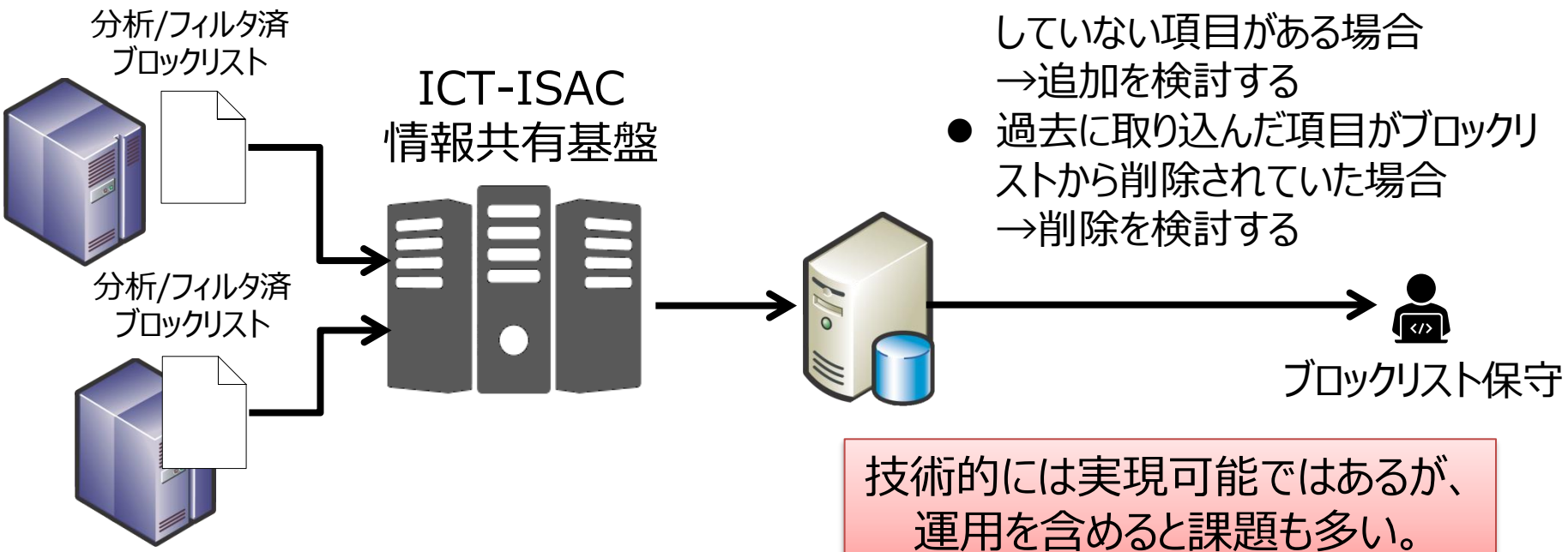
- 情報共有基盤の普及には、まずは配信型への適用
- 次に、相互利用型&&分析/フィルタ済に相当する情報流通の可能性へ

分類	配信型 情報は一旦分析機関に集められ、分析機関での分析/フィルタ適用されたものが情報利用者に展開される。		相互利用型 情報は利用者同士が交換する。利用者同士で共通の分析機能を利用した場合、配信型に近い運用形態となる。	
	分析/フィルタ未済	分析/フィルタ済	分析/フィルタ未済	分析/フィルタ済
例	AIS セキュリティベンダの脅威情報	JPCERT/CCからの脅威情報(CISTA) IPAからの脅威情報(J-CSIP)	金融ISACが運用するSIGNAL ICT-ISACが運用するtaxii.ict-isac.jp	左記のシステムにおいてISACが分析機能を持った場合
展開性 分析機能	低 (分析処理が必要)	高 (そのまま適用できる)	低 (分析処理が必要)	高 (そのまま適用できる)
即時性 配信機能	高 (形式変換が不要) Machine-Readable	低 (形式変換が必要) Human-Readable	中 (形式変換が要/不要が混在) Machine/Human-Readable	
関係性		高 (自分たちに関連したものである)	高 (自分たちが検知したものである)	

攻撃元情報：ブロックリスト

ブロックリストの活用

- ブロックリスト＝不正接続先へのアクセスを阻止する一覧表 && 分析/フィルタ済
  - ブロックリストの差分情報(追加/削除)を投稿
    - いつ、何を追加(add)したか?
    - いつ、何を削除(del)したか?



- 取得したブロックリストの中に適用していない項目がある場合
  →追加を検討する
- 過去に取り込んだ項目がブロックリストから削除されていた場合
  →削除を検討する

技術的には実現可能ではあるが、
運用を含めると課題も多い。

脆弱性情報
脆弱性深刻度評価システム(Vuldate)

- CVSS(共通脆弱性評価システム；Common Vulnerability Scoring System)との違いが分かりにくいので、個人的には、CVSS現状評価支援システムと呼びたい

脆弱性情報：Vuldate

CVSS(共通脆弱性評価システム)

- 脆弱性の技術的な特性、攻撃活動の状況やシステムの重要度を加味して、脆弱性の深刻度を0.0～10.0のスコアで評価する。

JVN、製品・セキュリティベンダが提供

継続して集めるのは意外と難しい

利用者自身が集める情報

CVSS = 基本評価基準 × 現状評価基準 × 環境評価基準

基本評価基準	現状評価基準	環境評価基準
脆弱性そのものの技術的な特性	時間と共に変化する攻撃活動の状況	影響を受ける情報システムの状況

何が起きるのか?

既に攻撃は発生している?
対策は出ている?

システムの重要度は?

脆弱性情報：Vuldate

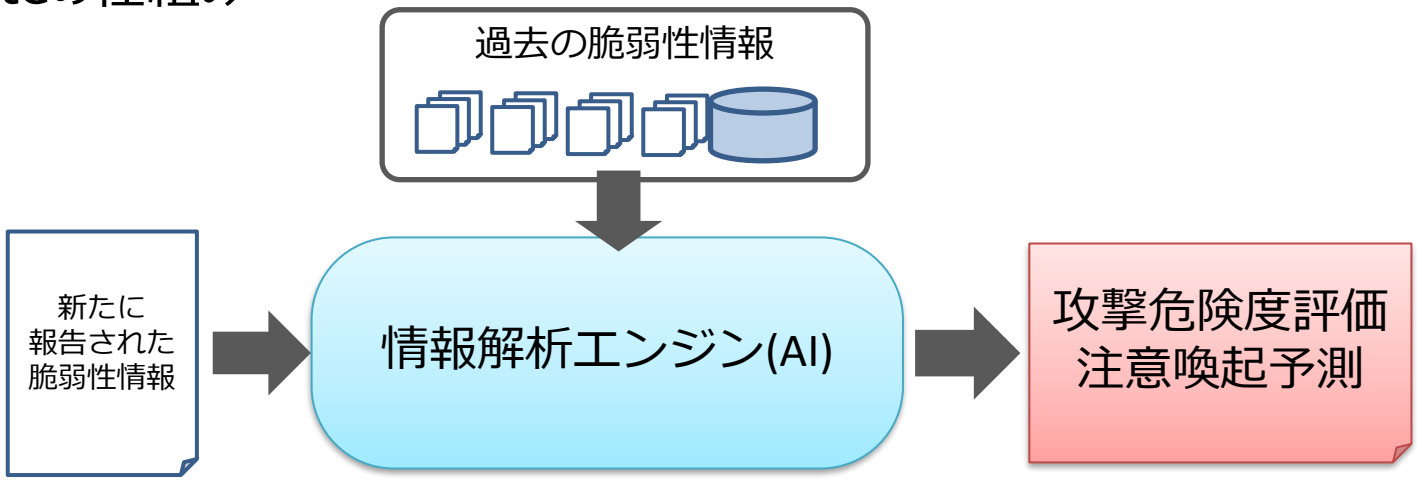
CVSS現状評価基準

- ある時点における脆弱性を取り巻く状況を評価
  - 攻撃可能性 (E: Exploitability)
    攻撃手法が実際に利用可能であるか
  - 利用可能な対策のレベル (RL: Remediation Level)
    対策がどの程度利用可能であるか
  - 脆弱性情報の信頼性 (RC: Report Confidence)
    脆弱性情報の信頼性は

脆弱性情報：Vuldate

現状評価を支援するVuldate

- Vuldateの仕組み



- Vuldateを使ってできること！
  - 攻撃危険度評価
    攻撃コードが生成される危険性：High,Medium,Low
    攻撃コードが生成されるとインシデント発生につながる可能性が高い
  - 注意喚起予測
    注意喚起に相当するような脆弱性かどうか：High,Medium,Low
    注意喚起になるような脆弱性は深刻度が高い

脆弱性情報：Vuldate

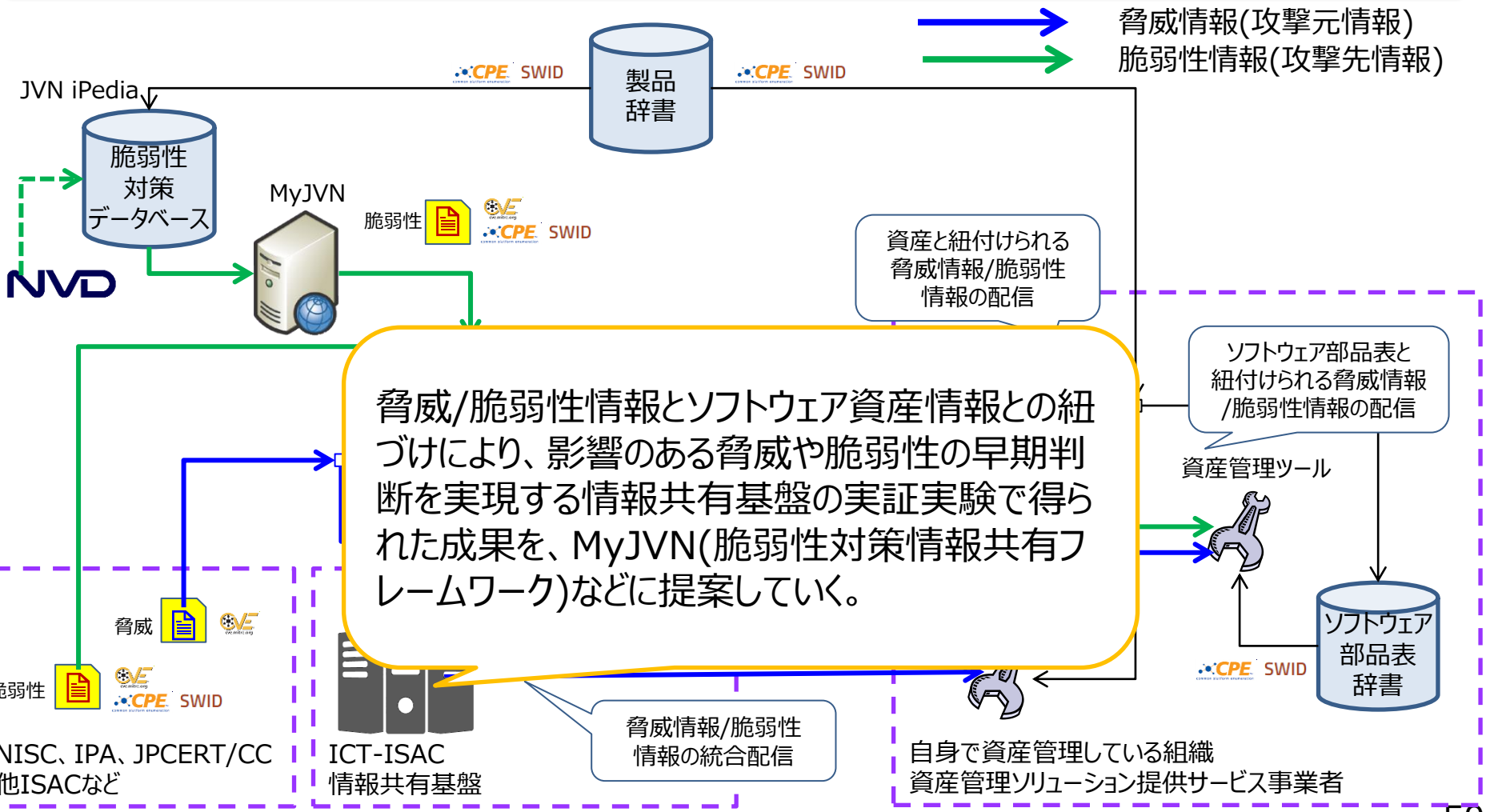
現状評価を支援するVuldate

https://www.vuldate.com/_jvn_summary

JVNDB-ID	CVE-ID	タイトル	CVSSv3	攻撃危険度評価	注意喚起予測	最終更新日
JVNDB-2022-000015	CVE-2022-25355	EC-CUBE における HTTP Host ヘッダの処理に脆弱性	3.1	Low	Low	2022-02-22
JVNDB-2022-000013	CVE-2022-21179	EC-CUBE 用プラグイン「メルマガ管理プラグイン」におけるクロスサイトリクエストフォージェリの脆弱性	3.1	Low	Low	2022-02-22
JVNDB-2021-007809	CVE-2021-25386	Android における古典的バッファオーバーフローの脆弱性	9.8	High	Low	2022-02-22
JVNDB-2021-007808	CVE-2021-25385	Android における古典的バッファオーバーフローの脆弱性	9.8	High	Low	2022-02-22
JVNDB-2021-007807	CVE-2021-25384	Android における入力確認に関する脆弱性	9.8	Low	Low	2022-02-22
JVNDB-2021-007806	CVE-2020-12288	複数の Intel(R) Thunderbolt(TM) コントローラにおける脆弱性	5.5	Medium	Low	2022-02-22
JVNDB-2021-007805	CVE-2020-12289	複数の Intel(R) Thunderbolt(TM) コントローラにおける境界外書き込みに関	5.5	Medium	Low	2022-02-22

情報共有基盤の実証

今後の活動

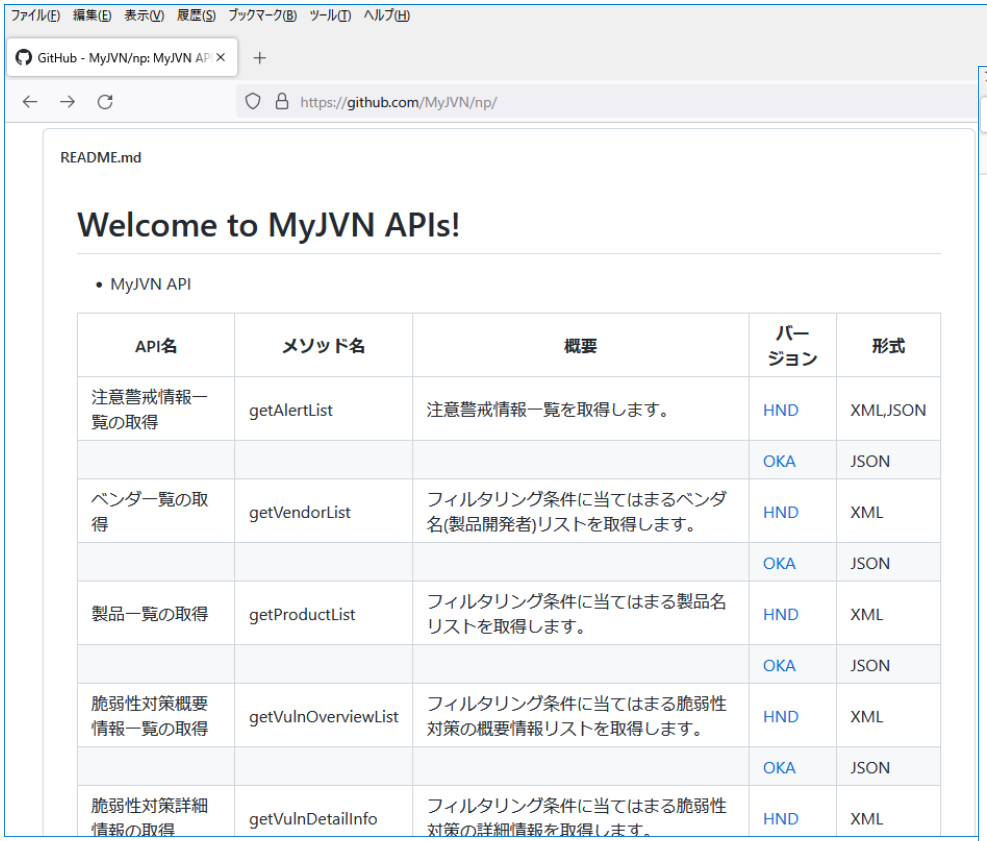


脆弱性対策情報共有フレームワーク MyJVN APIs!

- 実証実験から得られた知見の展開

今後の活動

- 実証実験から得られた知見の展開



README.md

Welcome to MyJVN APIs!

- MyJVN API

API名	メソッド名	概要	バージョン	形式
注意警戒情報一覧の取得	getAlertList	注意警戒情報一覧を取得します。	HND	XML,JSON
			OKA	JSON
ベンダー一覧の取得	getVendorList	フィルタリング条件に当てはまるベンダ名(製品開発者)リストを取得します。	HND	XML
			OKA	JSON
製品一覧の取得	getProductList	フィルタリング条件に当てはまる製品名リストを取得します。	HND	XML
			OKA	JSON
脆弱性対策概要情報一覧の取得	getVulnOverviewList	フィルタリング条件に当てはまる脆弱性対策の概要情報リストを取得します。	HND	XML
			OKA	JSON
脆弱性対策詳細情報の取得	getVulnDetailInfo	フィルタリング条件に当てはまる脆弱性対策の詳細情報を取得します。	HND	XML

- MyJVNデータフィード

データフィード名	概要	バージョン	形式
JVNDBRSS	脆弱性対策情報の概要	HND	XML
		OKA	JSON
脆弱性対策情報詳細	脆弱性対策情報の詳細	HND	XML
		OKA	JSON
ベンダー一覧	ベンダ名(製品開発者)リスト	HND	XML
		OKA	JSON
製品一覧	製品名リスト	HND	XML
	バージョンなし	OKA	JSON
	バージョンあり	OKA	JSON

- SBOM

タイプ	形式
SWID	XML
CycloneDX	JSON
SPDX	JSON

- 謝辞

本サイトでは、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」の成果を活用しています。

Collaborate
together
to make our
Internet
secure.

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan