IPA Better Life with IT

IT資産管理とセキュリティ
～リスク分析のすすめ～

2018/06/08

独立行政法人 情報処理推進機構 (IPA)
技術本部セキュリティセンター
情報セキュリティ技術ラボラトリー
寺田真敏

目次

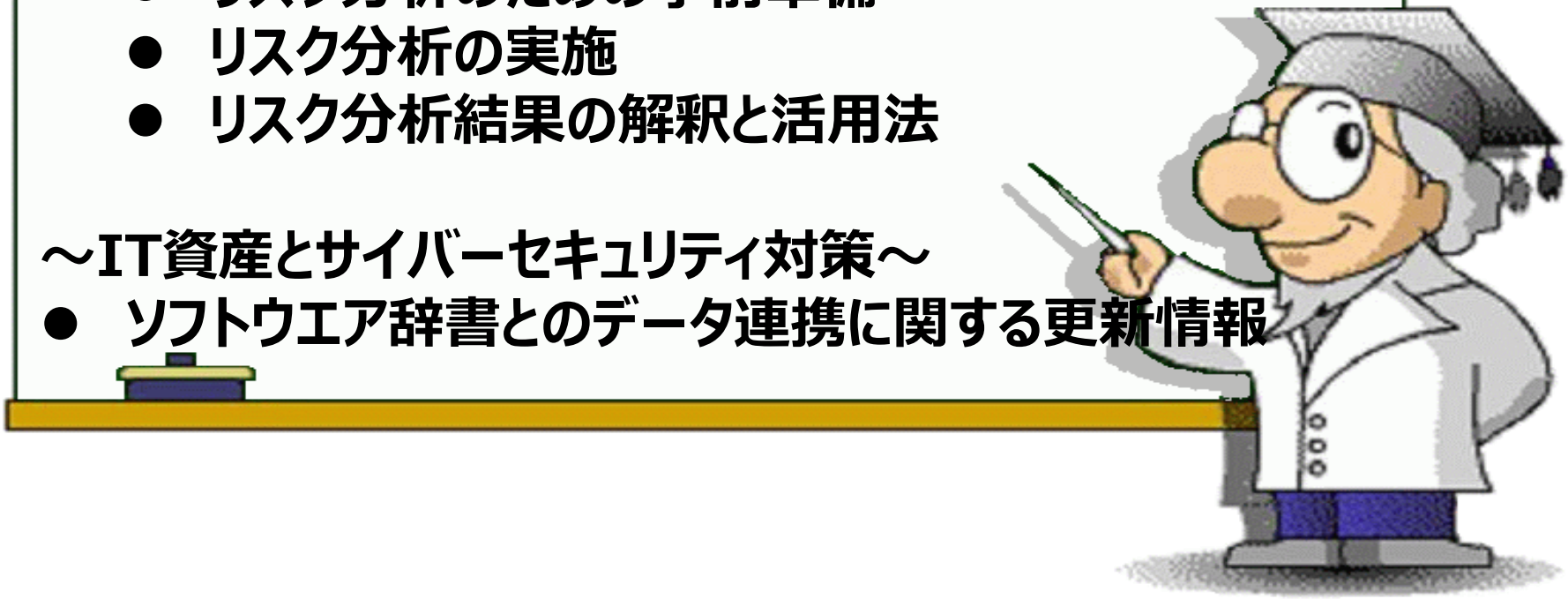
- 情報セキュリティ10大脅威 2018

～セキュリティ対策におけるリスク分析実施のススメ～

- リスク分析の作業手順
  - リスク分析のための事前準備
  - リスク分析の実施
  - リスク分析結果の解釈と活用法

～IT資産とサイバーセキュリティ対策～

- ソフトウエア辞書とのデータ連携に関する更新情報



情報セキュリティ10大脅威 2018

- 2017年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から選出

昨年	個人	順位	組織	昨年
1位	インターネットバンキングやクレジットカード情報等の不正利用	1位	標的型攻撃による被害	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	2位
7位	ネット上の誹謗・中傷	3位	ビジネスメール詐欺による被害	ランク外
3位	スマートフォンやスマートフォンアプリを狙った攻撃	4位	脆弱性対策情報の公開に伴う悪用増加	ランク外
4位	ウェブサービスへの不正ログイン	5位	脅威に対応するためのセキュリティ人材の不足	ランク外
6位	ウェブサービスからの個人情報の窃取	6位	ウェブサービスからの個人情報の窃取	3位
8位	情報モラル欠如に伴う犯罪の低年齢化	7位	IoT機器の脆弱性の顕在化	8位
5位	ワンクリック請求等の不当請求	8位	内部不正による情報漏えい	5位
10位	IoT機器の不適切な管理	9位	サービス妨害攻撃によるサービスの停止	4位
ランク外	偽警告によるインターネット詐欺	10位	犯罪のビジネス化(アンダーグラウンドサービス)	9位
	インターネット上のサービスを悪用した攻撃(10)	ランク外へ	ウェブサイトの改ざん(6) ウェブサービスへの不正ログイン(7) インターネットバンキングやクレジットカード情報の不正利用(10)	

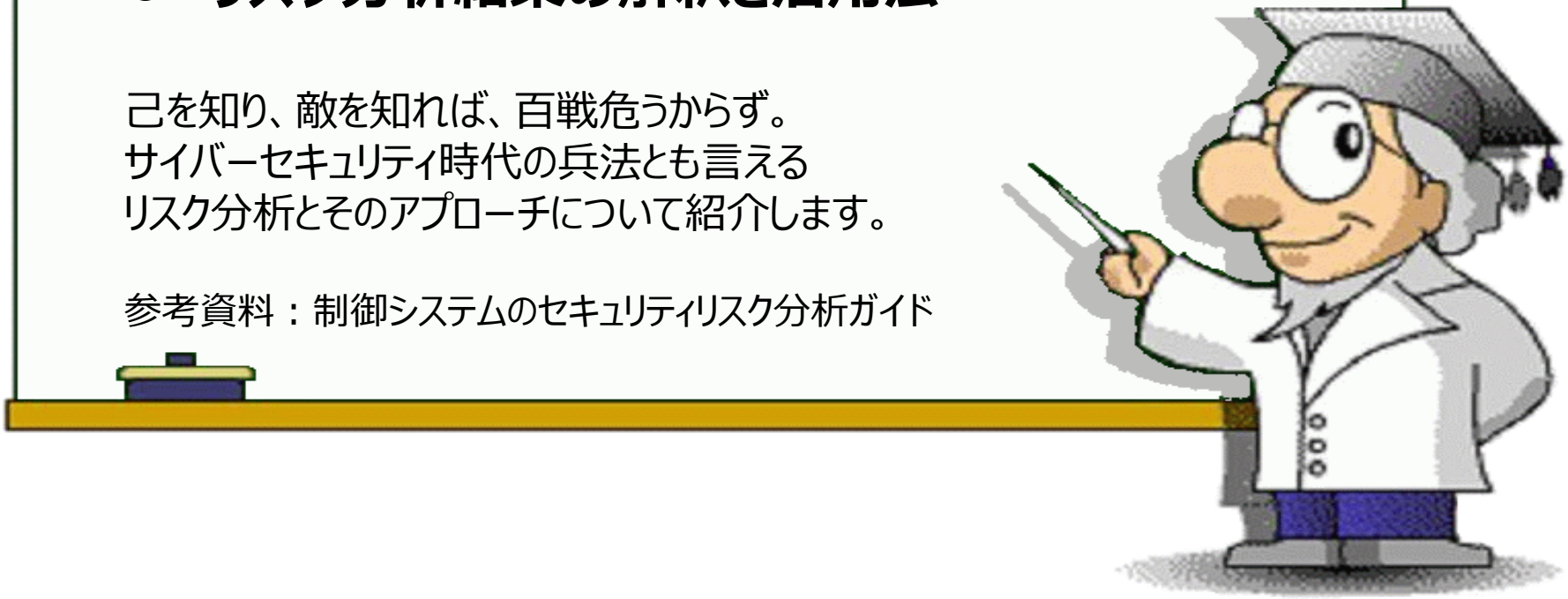
目次

～セキュリティ対策におけるリスク分析実施のススメ～

- **リスク分析の作業手順**
  - **リスク分析のための事前準備**
  - **リスク分析の実施**
  - **リスク分析結果の解釈と活用法**

己を知り、敵を知れば、百戦危うからず。
サイバーセキュリティ時代の兵法とも言える
リスク分析とそのアプローチについて紹介します。

参考資料：制御システムのセキュリティリスク分析ガイド



サイバー攻撃と戦う兵法
～セキュリティリスク分析の重要性～

IPA

中国、春秋時代の軍事戦略家、孫武の兵法書『孫子』に示された名句に「彼を知り己を知れば百戦殆うからず」がある。サイバー攻撃時代において、敵＝脅威(攻撃者を含む)、己＝自組織と置き換えてみると、セキュリティ対策において効果的な施策を実施するための教えとなる。
リスク分析は、
　己を知り、敵を知れば、百戦危うからず
を実践する、サイバーセキュリティ時代の兵法である。

「リスク分析」　＝　①②③を評価指標に、事業リスクを明確にするプロセス
① 評価対象(資産や事業)の価値(重要性)、想定される被害の規模・影響
② 評価対象に対して想定される脅威とその発生の可能性
③ 想定される脅威が生じた際の受容可能性(評価対象の脆弱性、対策不備)

リスク分析の重要性と有効性
① 実効的なリスクの低減の実現
② 効果的なセキュリティ投資の実現(追加対策、有効なテスト箇所の抽出)
③ PDCAサイクルの確立とセキュリティの維持向上を継続するためのベース

制御システムの
セキュリティリスク分析ガイド

- **具体的な手順を解説、テンプレート、チェックリスト等を提供**
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

【ガイド本編の目次】

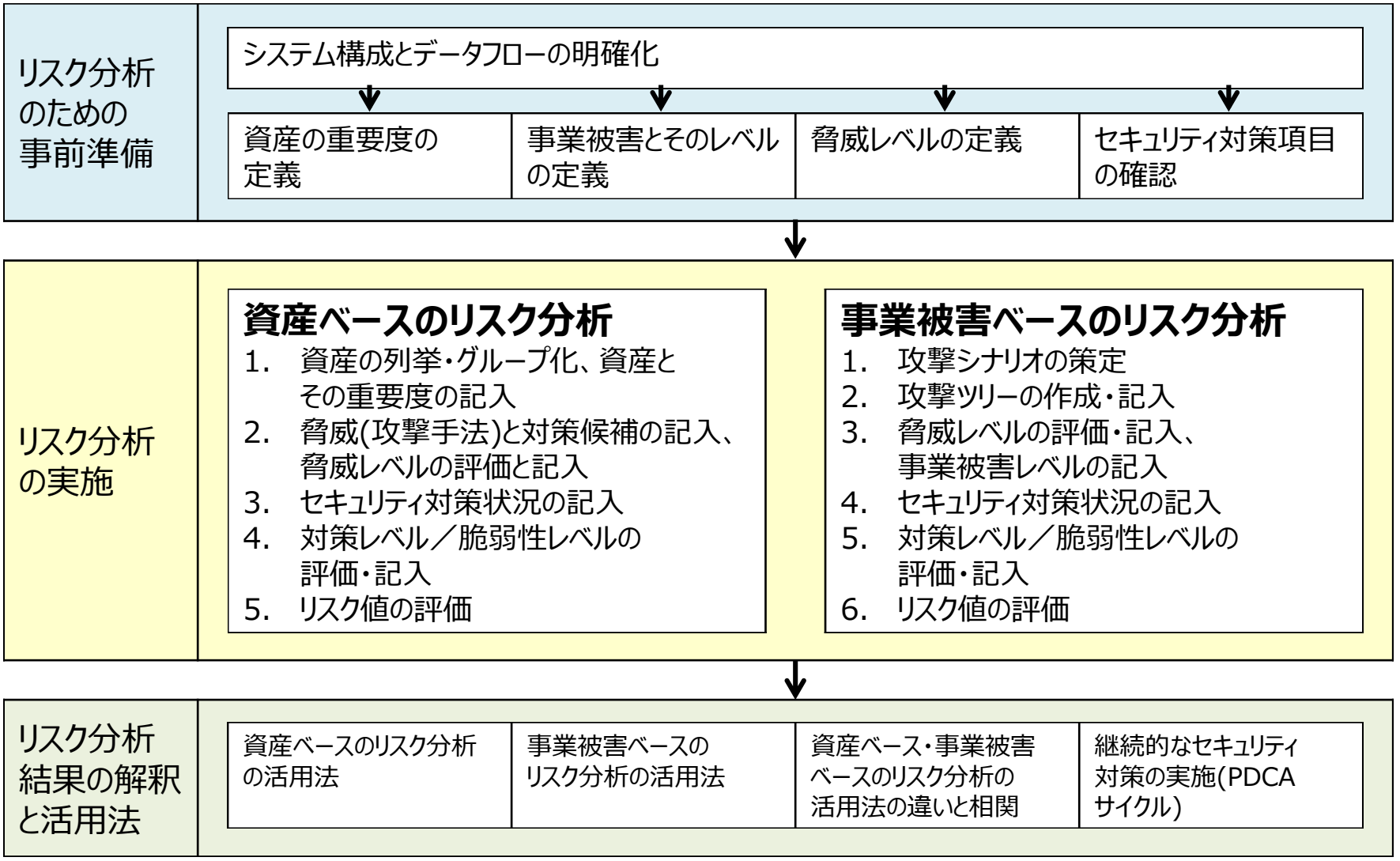
ガイド本編

350頁

別冊
(分析例フルセット)

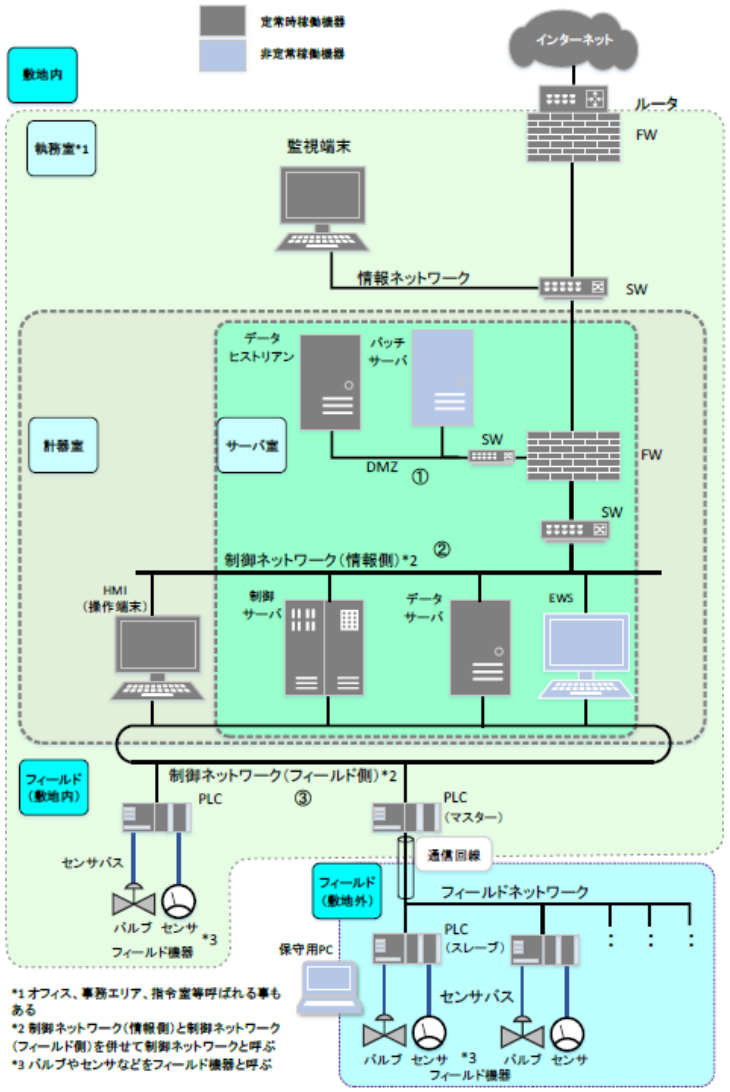
70頁

リスク分析の作業手順


リスク分析のための事前準備
システム構成とデータフローの明確化
資産の重要度の定義
事業被害とそのレベルの定義
脅威レベルの定義
セキュリティ対策項目の確認
リスク分析の実施
資産ベースのリスク分析
1. 資産の列挙・グループ化、資産とその重要度の記入
2. 脅威(攻撃手法)と対策候補の記入、脅威レベルの評価と記入
3. セキュリティ対策状況の記入
4. 対策レベル／脆弱性レベルの評価・記入
5. リスク値の評価
事業被害ベースのリスク分析
1. 攻撃シナリオの策定
2. 攻撃ツリーの作成・記入
3. 脅威レベルの評価・記入、事業被害レベルの記入
4. セキュリティ対策状況の記入
5. 対策レベル／脆弱性レベルの評価・記入
6. リスク値の評価
リスク分析結果の解釈と活用法
資産ベースのリスク分析の活用法
事業被害ベースのリスク分析の活用法
資産ベース・事業被害ベースのリスク分析の活用法の違いと相関
継続的なセキュリティ対策の実施(PDCAサイクル)

リスク分析の作業手順
~事前準備：システム構成とデータフローの明確化~

- 資産の洗い出し
- システム構成の明確化、論理化
  - 分析範囲の決定
  - 分析用アーキテクチャの明確化
  - 資産とその付帯情報の整理
  - 分析対象とする資産の絞り込み (グループ化と除外)
  - ロケーションと資産の配置
  - 各資産の接続情報の記述
- データフローの明確化
  - データの流れのシステム構成図へのマッピング



リスク分析の作業手順
~事前準備：資産の重要度の定義~

- 資産の重要度
  - 資産ベースのリスク分析における評価指標の一つ
  - システム資産としての価値、攻撃によって想定される事業被害や事業継続性への影響を考慮した評価点(1：低～3：高)

【資産の重要度の判断基準の定義例】

評価点	判断基準
3	・資産が攻撃された場合、システムが長期間停止する恐れ ・資産から情報が漏えいした場合、巨額の損失が発生する恐れ ・資産が攻撃された場合、大規模の人的／環境被害が発生する恐れ
2	・資産が攻撃された場合、システムが一定期間停止する恐れ ・資産から情報が漏えいした場合、ある程度の損失が発生する恐れ ・資産が攻撃された場合、中規模の人的／環境被害が発生する恐れ
1	・資産が攻撃された場合、システムが短期間停止する恐れ ・資産から情報が漏えいした場合、小額の損失が発生する恐れ ・資産が攻撃された場合、小規模の人的／環境被害が発生する恐れ

【資産とその重要度の定義例】

資産名	重要度レベル
監視端末	2
ネットワーク装置 ・スイッチ ・ファイアウォール(機器)	3
データサーバ	3
制御サーバ	3

リスク分析の作業手順
~事前準備：事業被害とそのレベルの定義~

- 事業被害レベル
  - 事業被害ベースのリスク分析における評価指標の一つ
  - 脅威によって生じる事業被害の評価点(1：小～3：大)
- 事業被害
  - 組織の事業の安定的な運営や継続を阻害する事象・状況
  - 発生時の被害範囲や会社経営上の打撃を基に各事業者にて定義

【事業被害レベルの判断基準の定義例】

評価点	判断基準
3	事業上の被害が大きい。 例：発生した場合、被害範囲はシステム全体に及ぶ、など
2	事業上の被害が中程度。 例：発生した場合、被害範囲がシステムの一部に限定される、など
1	事業上の被害は小さい。 例：発生した場合、被害範囲はシステムの極一部に限定される、など

【事業被害レベルの判断基準の定義例】

事業被害	概要	事業被害レベル
広域での○○供給停止	○○製造設備、○○供給設備等へのサイバー攻撃により、広域において供給停止が発生し、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。	3
大規模対策費用の発生	サイバー攻撃を受け、○○の供給停止の被害は発生しなかったものの、現行対策の脆弱性が明らかとなり、その解消のために膨大な対策費用が発生する。	1

リスク分析の作業手順
~事前準備：脅威レベルの定義~

- 脅威レベル
  - 2種類のリスク分析における評価指標の一つ
  - それぞれのリスク分析において、想定する脅威が発生する可能性の評価点(1：低～3：高)
- 脅威(攻撃手法)のリストアップとその分類

【脅威レベルの判断基準の定義例】

評価点	判断基準
3	発生する可能性が高い。 例：個人の攻撃者(スキルは問わない)によって攻撃された場合、攻撃が成功する可能性が高い、など
2	発生する可能性は中程度。 例：一定のスキルを持った攻撃者によって攻撃された場合、攻撃が成功する可能性がある、など
1	発生する可能性は低い。 例：国家レベルのサイバー攻撃者(軍隊及びそれに準ずる団体)によって攻撃された場合、攻撃が成功する可能性がある、など

【脅威(攻撃手法)とその分類の例】

攻撃対象	脅威(攻撃手法)
機器	不正アクセス、物理的侵入 不正操作 過失操作 不正媒体・機器接続 高負荷攻撃 窃盗
通信路	経路遮断 通信輻輳 無線妨害 盗聴 通信データ改ざん 不正機器接続

リスク分析の作業手順
~事前準備：脅威レベルの定義~

【資産(機器)に対する脅威(攻撃手法)の例(抜粋)】

#	脅威(攻撃手法)	説明	具体例
1	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	不正入手した認証情報の悪用(不正ログイン) 認証機構を持たない機器への侵入 機器に内在する脆弱性の悪用 設定不備(不要プロセス動作や不要ポート開放等)の悪用
2	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入 する。あるいは、物理的アクセスが制限された機器(ラックや箱内に設置され た機器等)の制限を解除する。	敷地内／計器室／サーバ室への不正侵入 ラック／設置箱の不正開放
3	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	不正入手した認証情報の悪用(不正ログイン) 認証機構を持たない機器への侵入 機器に内在する脆弱性の悪用
4	過失操作	内部関係者(社員や協力者のうち、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	メール添付ファイル開封 マルウェアに感染した正規媒体の持ち込み
5	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB 機器等)を接続し、攻撃を実行する。	不正媒体の接続 媒体からの読み込み／媒体への書き出し
⋮	⋮	⋮	⋮
14	窃盗	機器を窃盗する。	機器のネットワークからの切り離し、不正持出 保守用モバイル端末の盗み出し

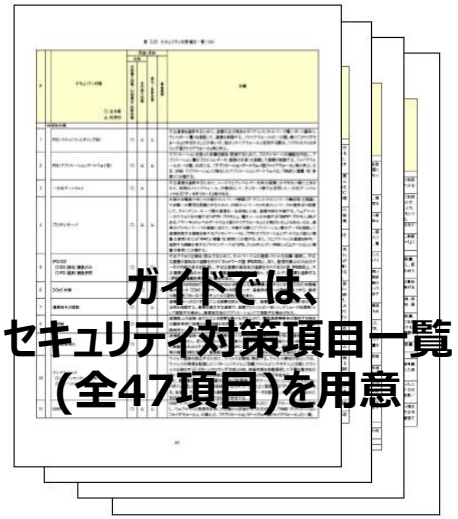
リスク分析の作業手順
~事前準備：セキュリティ対策項目の確認~

- 脆弱性レベル
  - 2種類のリスク分析における評価指標の一つ
  - それぞれのリスク分析において、発生した脅威を受け入れる可能性の評価点(1：低～3：高)
- セキュリティ対策の一覧とその分類

【脆弱性レベルと対策レベルの定義(評価点と判断基準)】

評価点		判断基準
脆弱性レベル	対策レベル	
3	1	脅威が発生した場合、容易に受けいれる可能性が高い。 例：過去の事例において、脆弱性を利用した攻撃が発生・成功し、被害が生じたことが確認されている、など
2	2	脅威が発生した場合、受け入れる可能性が中程度である。 例：一般的な対策を実施しており、攻撃が成功するか否かは攻撃者のレベルに依る、など
1	3	脅威が発生した場合、受け入れる可能性は低い。 例：効果的な対策や、多層的な対策を実施しており、攻撃が成功する可能性は低い、など

【セキュリティ対策一覧】



ガイドでは、
セキュリティ対策項目一覧
(全47項目)を用意

リスク分析の作業手順
~リスク分析の実施~

IPA

- リスク分析の手法と特徴

#	分析手法			工数	効果
1	ベースラインアプローチ			小	△
2	非形式的アプローチ			小	×
3	詳細リスク分析	資産ベース		中	○
		シナリオベース	アタックツリー・アナリシス(ATA)	大	○
			フォールトツリー・アナリシス(FTA)	大	○
4	組み合わせアプローチ			大	◎

- アタックツリー・アナリシス(ATA)：攻撃者視点で、トップダウンに、誰が、どこから、どのルートを経由して被害発生を引き起こしうるかのシナリオをツリーとして構成していく方法
- フォールトツリー・アナリシス(FTA)：被害(インシデント等)事象を起点として、ボトムアップに、その被害に至る１ステップ前の攻撃事象を想起しながらツリーとして構成していく方法

リスク分析の作業手順
~リスク分析の実施~

- **資産ベースのリスク分析　＜己を知る＞**

  保護すべきシステムを構成する資産を対象に、各資産(サーバ、端末、通信機器等)に対して、その重要度(価値)、想定される脅威、脆弱性の３つを評価指標として、リスク分析を実施。

  ⇒　資産に対して網羅的に脅威と対策状況を評価可能

- **事業被害ベースのリスク分析　＜敵を知る＞**

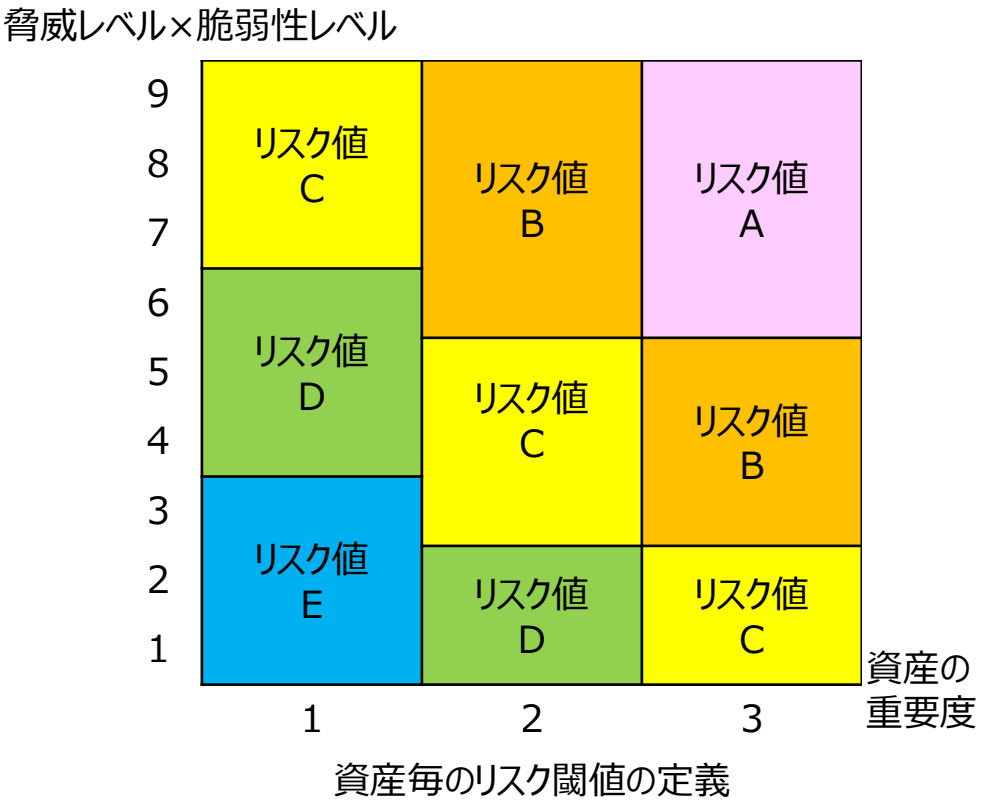
  保護すべきシステムにおいて実現されている事業やサービスに対して、回避したい事業被害を定義し、発生した際の事業被害のレベル、その被害を起こしうる攻撃シナリオによる脅威、そのシナリオに対する脆弱性(そのシナリオの受容可能性)の３つを評価指標として、リスク分析を実施。

  ⇒　一次攻撃脅威から、連鎖して事業被害に繋がる攻撃を、
  　　評価可能(ATAとFTAの利点を融合)

  ⇒　**机上でのペネトレーションテスト**

リスク分析の作業手順
~資産ベースのリスク分析~

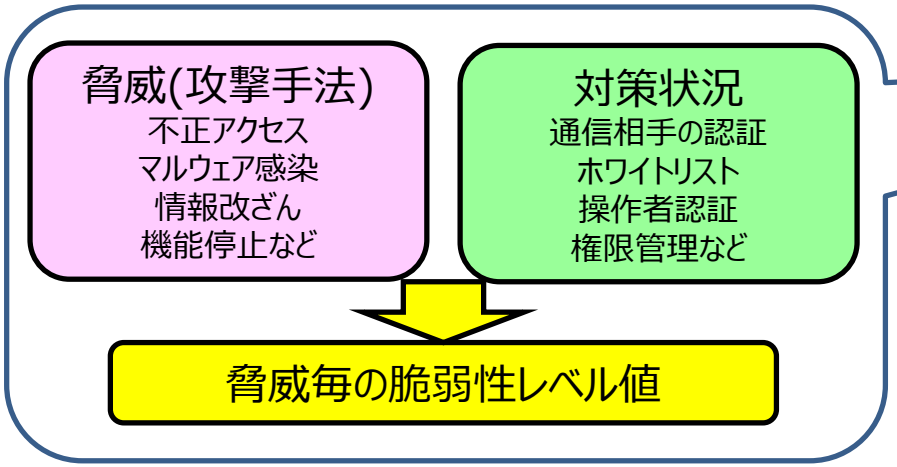
- 保護すべき制御システムを構成する資産群を対象に
- 各資産のリスクの大きさ(リスク値)を査定する。
  - ① 資産の重要度
  - ② 各資産に対する脅威レベル(脅威の発生可能性)
  - ③ 資産の各脅威に対する脆弱性レベル(発生した脅威を受け入れる可能性)

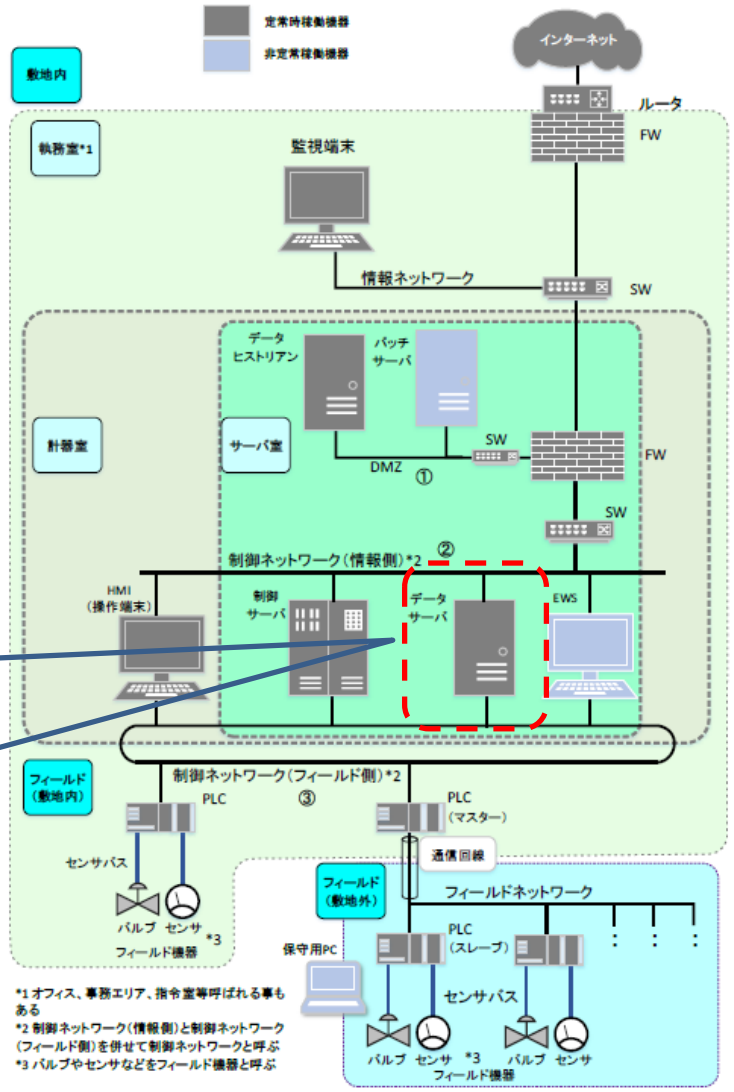


リスク分析の作業手順
~資産ベースのリスク分析~

- 保護すべき制御システムを構成する資産群を機能、種別等によってグループ化
- グループ化した資産群を対象に、
  - 脅威(攻撃手法)
  - 対策状況

  を記入→脆弱性レベルを評価





リスク分析の作業手順
~資産ベースのリスク分析~

【資産ベースのリスク分析シート】

凡例: ○ 対策実施　×　対策未実施　　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策					対策レベル
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			防御		検知/被害把握	事業継続		脅威毎
									侵入/拡散段階	目的遂行段階				
1	情報系資産	データサーバ	2	2		B	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 ○ IPS／IDS パッチ適用 脆弱性回避		IPS／IDS ログ収集・分析 統合ログ管理システム			2
2			2	1		C	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理　（ICカード、生体認証） 施錠管理					3
3			2	2		B	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証（ID/Pass）					2
4			2	3		A	過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング					1
5			3	3		A	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限					1
6			3	2		A	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認					2
7			3	1		B	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名					3
8			3	2				ソフトウェア、認証情報、構成設定情報、暗号	権限管理 ○ アクセス制御 データ暗号化 DLP	(同左) (同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム			2
9			3	3				ソフトウェア、認証情報、構成設定情報、暗号。	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ ○		1
10			2	2				ソフトウェア、認証情報、構成設定情報、暗号		権限管理 ○ アクセス制御	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ ○		2
11			3	3				コマンド（設定値変更、電源断等）や不正	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム			1
12			3	3							機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計		1
13			2	3				理能力以上の処理を要求し、機器の正常	DDoS対策		機器異常検知	冗長化		
14			1	2					施錠管理 ○	(同左)				
15			3	3		A	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。	耐タンパー 難読化 セキュア消去	(同左) (同左) (同左)				1
							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理　（ICカード、生体認証） ○ 施錠管理 ○		機器異常検知 機器死活監視	冗長化		

- 資産種別
- 対象装置
- 評価指標
  - 脅威レベル
  - 脆弱性レベル
  - 資産の重要度
  - リスク値
- 脅威(攻撃手法)
- 説明
- 対策
  - 防御
    - 侵入/拡散段階
    - 目的遂行段階
  - 検知/被害把握
  - 事業継続
- 脅威毎の対策レベル

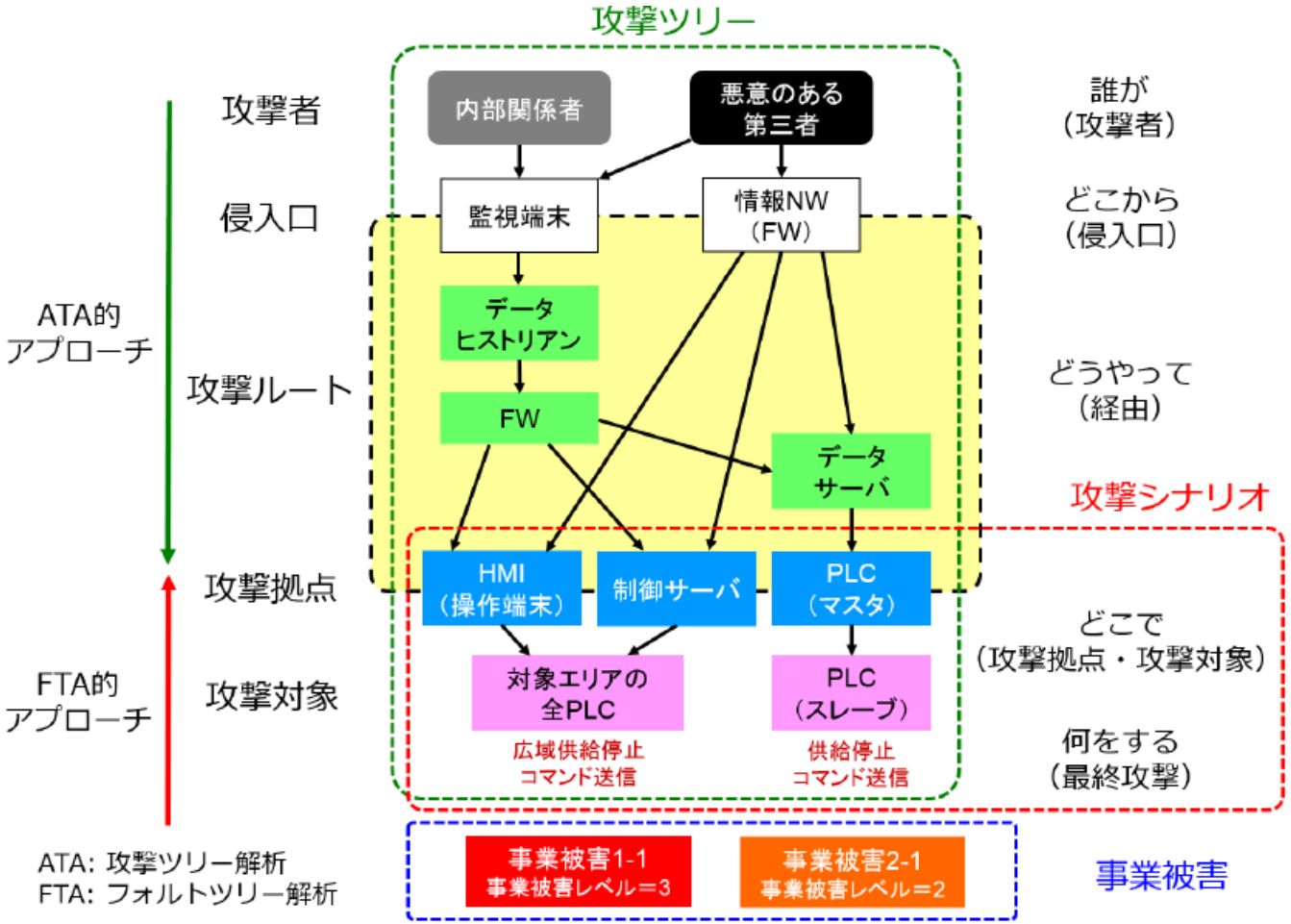
リスク分析の作業手順
~事業被害ベースのリスク分析~

- 攻撃シナリオ
  - 回避したい事業被害を引き起こす可能性のある攻撃拠点・攻撃対象・最終攻撃を具現化したシナリオ
- 攻撃ツリー
  - 攻撃シナリオに含まれる攻撃拠点・攻撃対象・最終攻撃に加えて、攻撃シナリオを実現する攻撃者・侵入口・経由を具体化した一連の攻撃手順
- 各攻撃ツリーのリスクの大きさ(リスク値)を、
  - 脅威レベル(脅威の発生可能性)
  - 脆弱性レベル(発生した脅威を受け入れる可能性)
  - 事業被害レベル(事業被害の大きさ)

  から算定

リスク分析の作業手順
~事業被害ベースのリスク分析~

- 事業被害ベースのリスク分析のアプローチ



リスク分析の作業手順
～事業被害ベースのリスク分析～

【事業被害ベースのリスク分析シート】

1．広域での○○供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	対策レベル 攻撃ステップ	攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	構成ステップ（項番）
	1-1	コマンドの不正送信により、広域に及ぶ供給が停止する。												
1		侵入口＝監視端末 悪意のある第三者が、情報ネットワーク上の監視端末に不正アクセスする。					FW（パケットフィルタリング型） パッチ適用 通信相手の認証 操作者認証	権限管理 ○ アクセス制御 ○	ログ収集・分析 ○		2			
4		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。					パッチ適用 通信相手の認証 操作者認証				2			
5		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。	2	2	3	B					1	2	#1	1,2,3,4,5
6		悪意のある第三者が、ファイアウォールから制御サーバに不正アクセスする。					パッチ適用	権限管理 ○ アクセス制御 ○	ログ収集・分析 ○					
7		悪意のある第三者が、制御サーバ上で広域供給停止操作を行い（広域供給停止コ し）、広域に及ぶ供給が停止する。					○	重要操作の承認	機器異常検知 ○ ログ収集・分析 ○					
8		悪意のある第三者が、ファイアウォールからデータサーバに不正アクセスする。						権限管理 ○ アクセス制御 ○	ログ収集・分析 ○					
9		悪意のある第三者が、データサーバからPLC（マスター）に不正アクセスする。					○	権限管理 アクセス制御	ログ収集・分析 ○					
10		悪意のある第三者が、PLC（マスター）上で供給停止コマンドを不正送信し、 が停止する。						重要操作の承認	機器異常検知 ○ ログ収集・分析 ○					
11		悪意のある第三者が、監視端末をマルウェアに感染させる。					アンチウィルス ○ パッチ適用 ○ ホワイトリストによるプロセスの起動制限リスト		機器異常検知 ログ収集・分析 ○					

- 攻撃シナリオ
  - 攻撃ツリー／攻撃ステップ対策
- 対策
  - 防御
    - 侵入/拡散段階
    - 目的遂行段階
  - 検知/被害把握
  - 事業継続
- 評価指標
  - 脅威レベル
  - 脆弱性レベル
  - 事業被害レベル
  - リスク値
- 対策レベル
  - 攻撃ステップ
  - 攻撃ツリー
- 攻撃ツリー番号
  - 攻撃ツリー番号
  - 構成ステップ(項番)

リスク分析の作業手順
~リスク分析結果の解釈と活用法~

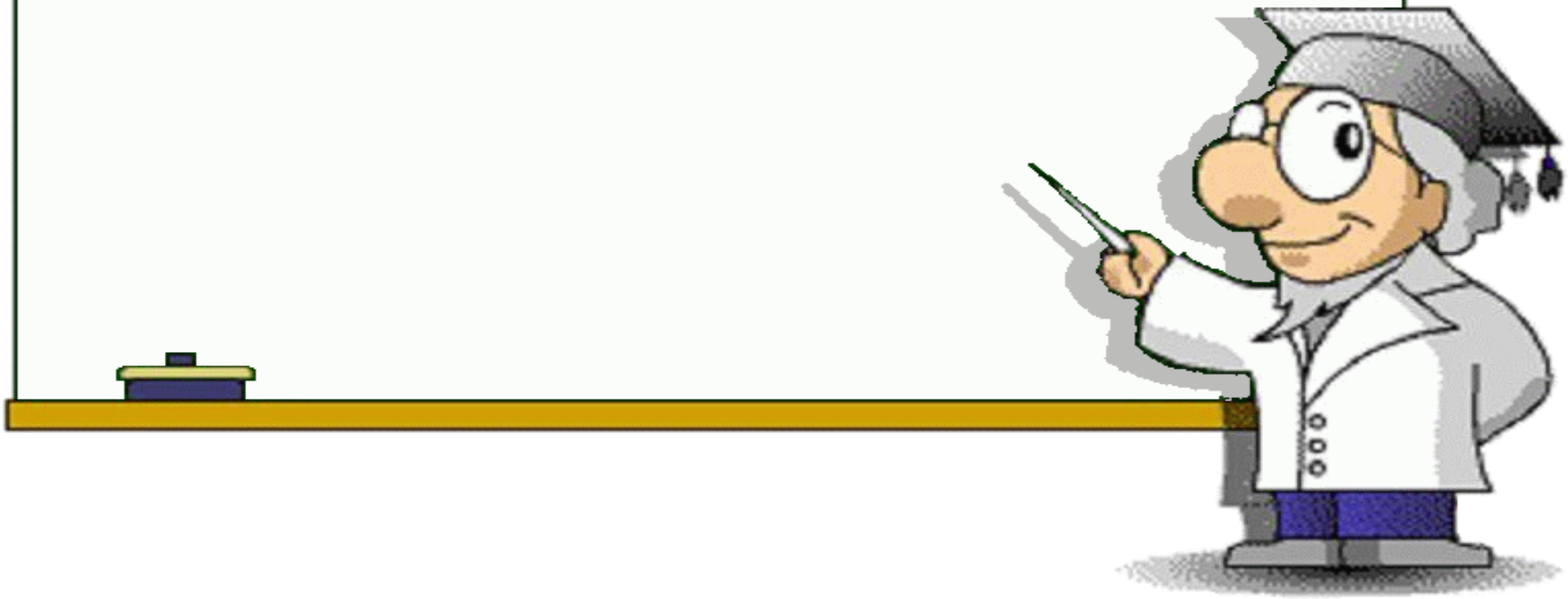
- リスク分析結果の解釈及び活用のねらい
  - セキュリティ上の弱点を発見し、サイバー攻撃に対するリスクを低減するため、分析結果として得られたリスク値を可能な限り低減する。

- リスク値の活用
  - リスクの把握
  - 改善箇所の抽出、選定
  - リスクの低減
  - リスクの低減効果の確認
  - セキュリティテストの対策箇所の抽出、特定

目次

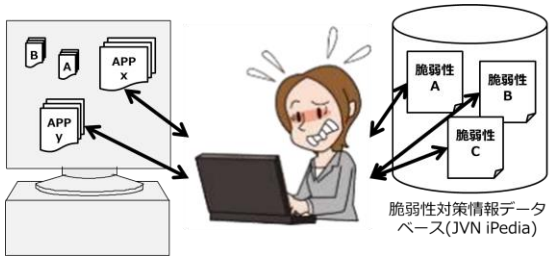
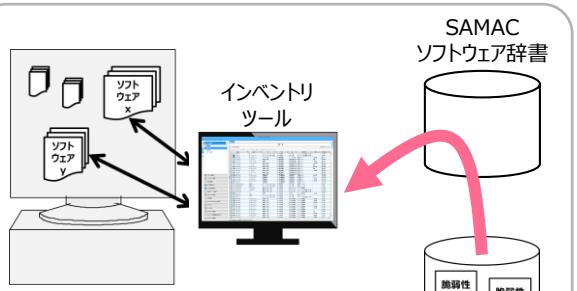
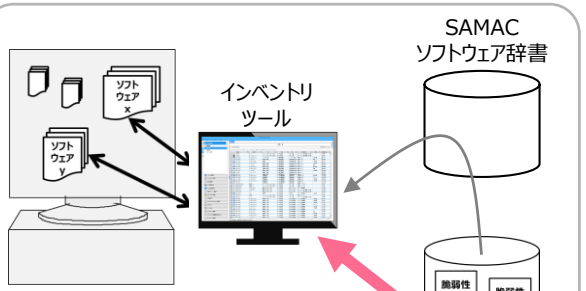
～IT資産とサイバーセキュリティ対策～

- ソフトウエア辞書とのデータ連携に関する更新情報



ソフトウエア辞書とのデータ連携
～IT資産管理と脆弱性管理の連携～

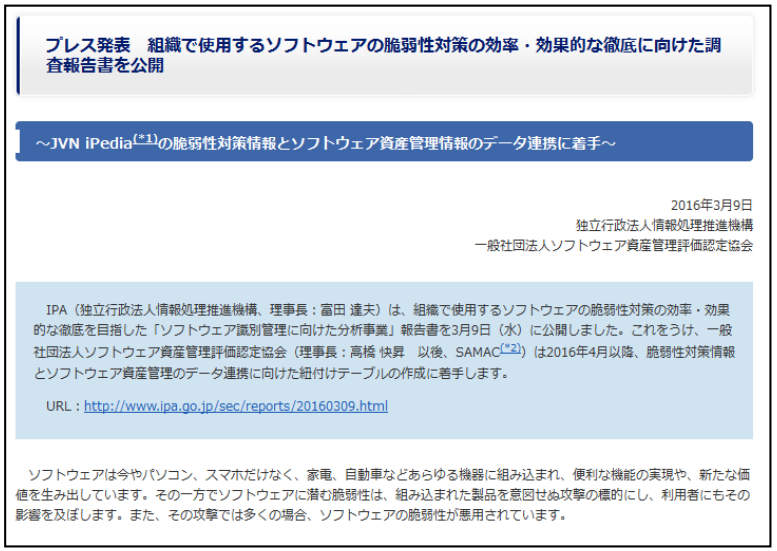
IPA

現在	① 現在の取組み 『JVN iPediaの活用』	② 将来的な連携 『JVN iPedia SWID連携』
		
人が脆弱性情報を検索し、各ソフトウェアを確認する。	SAMACソフトウェア辞書に脆弱性対策情報を連携する。	ソフトウェア識別タグが正式化すると直接インベントリツールと連携できる。
『全部なんて調べきれない！』	『辞書登録にあるものは、ツールの中で視覚的に分かる！』	『辞書登録に関わらず、SWIDがあればツールの中で視覚的に分かる！』
『いつの間にか脆弱性のあるソフトが入ってた！』	『でも直近の新しい情報は反映が遅くなってしまう･･･。』	『かなりリアルタイムに情報が反映される！』

ソフトウエア辞書とのデータ連携
～具体的な取り組み～

- 短期的
  - 製品識別子CPEを用いた脆弱性対策情報データベースJVN iPediaとSAMACソフトウェア辞書との連携

～JVN iPediaの脆弱性対策情報と
ソフトウェア資産管理情報のデータ連携に着手～
https://www.ipa.go.jp/about/press/20160309.html



プレス発表　組織で使用するソフトウェアの脆弱性対策の効率・効果的な徹底に向けた調査報告書を公開

～JVN iPedia(*1)の脆弱性対策情報とソフトウェア資産管理情報のデータ連携に着手～

2016年3月9日
独立行政法人情報処理推進機構
一般社団法人ソフトウェア資産管理評価認定協会

IPA（独立行政法人情報処理推進機構、理事長：富田 達夫）は、組織で使用するソフトウェアの脆弱性対策の効率・効果的な徹底を目指した「ソフトウェア識別管理に向けた分析事業」報告書を3月9日（水）に公開しました。これをうけ、一般社団法人ソフトウェア資産管理評価認定協会（理事長：高橋 快昇　以後、SAMAC(*2)）は2016年4月以降、脆弱性対策情報とソフトウェア資産管理のデータ連携に向けた紐付けテーブルの作成に着手します。

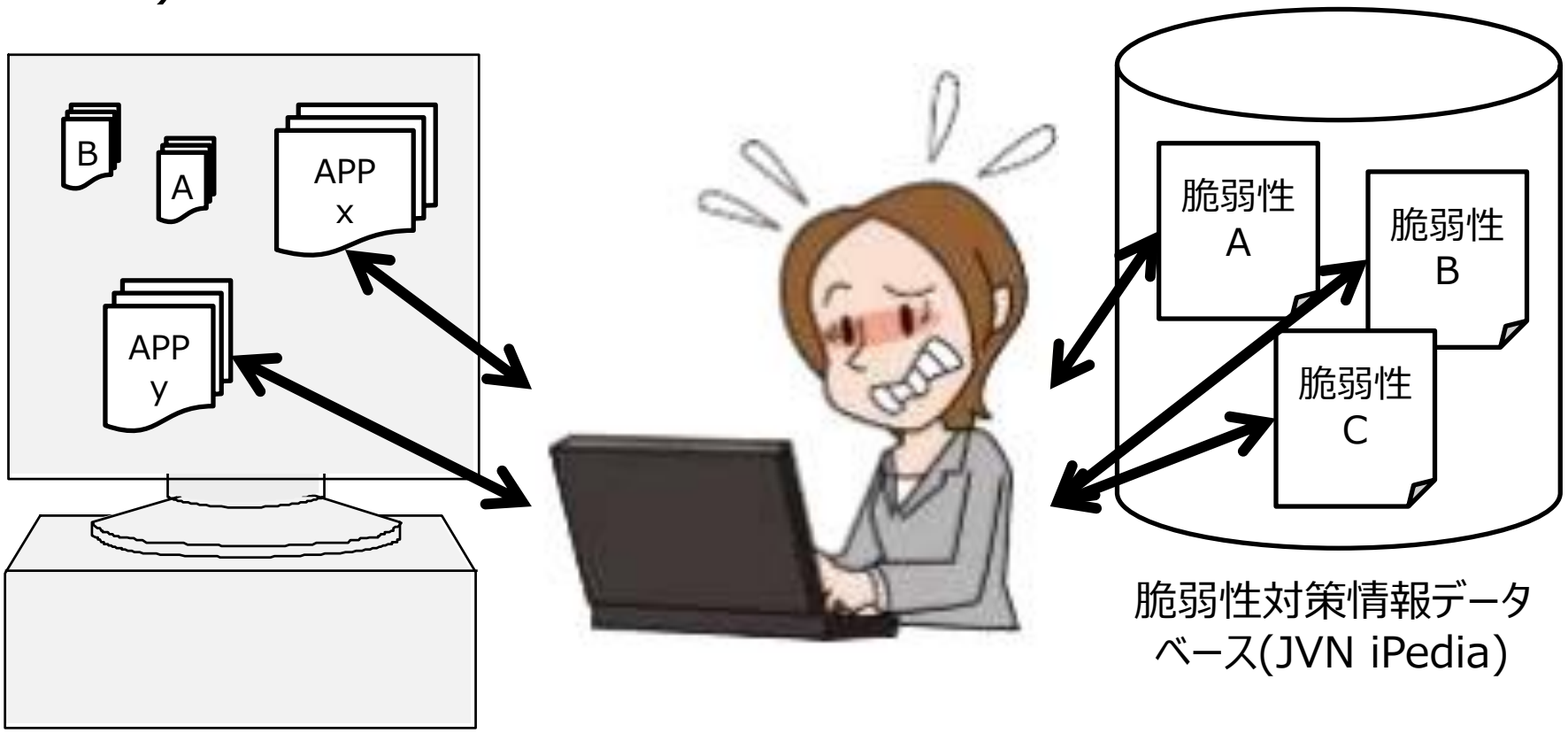
URL：http://www.ipa.go.jp/sec/reports/20160309.html

ソフトウェアは今やパソコン、スマホだけなく、家電、自動車などあらゆる機器に組み込まれ、便利な機能の実現や、新たな価値を生み出しています。その一方でソフトウェアに潜む脆弱性は、組み込まれた製品を意図せぬ攻撃の標的にし、利用者にもその影響を及ぼします。また、その攻撃では多くの場合、ソフトウェアの脆弱性が悪用されています。

- 長期的
  - ソフトウェア識別タグ(SWID)ISO19770-2を用いた資産管理と脆弱性対策の連携

ソフトウエア辞書とのデータ連携
～インストール状況と脆弱性との紐付け～

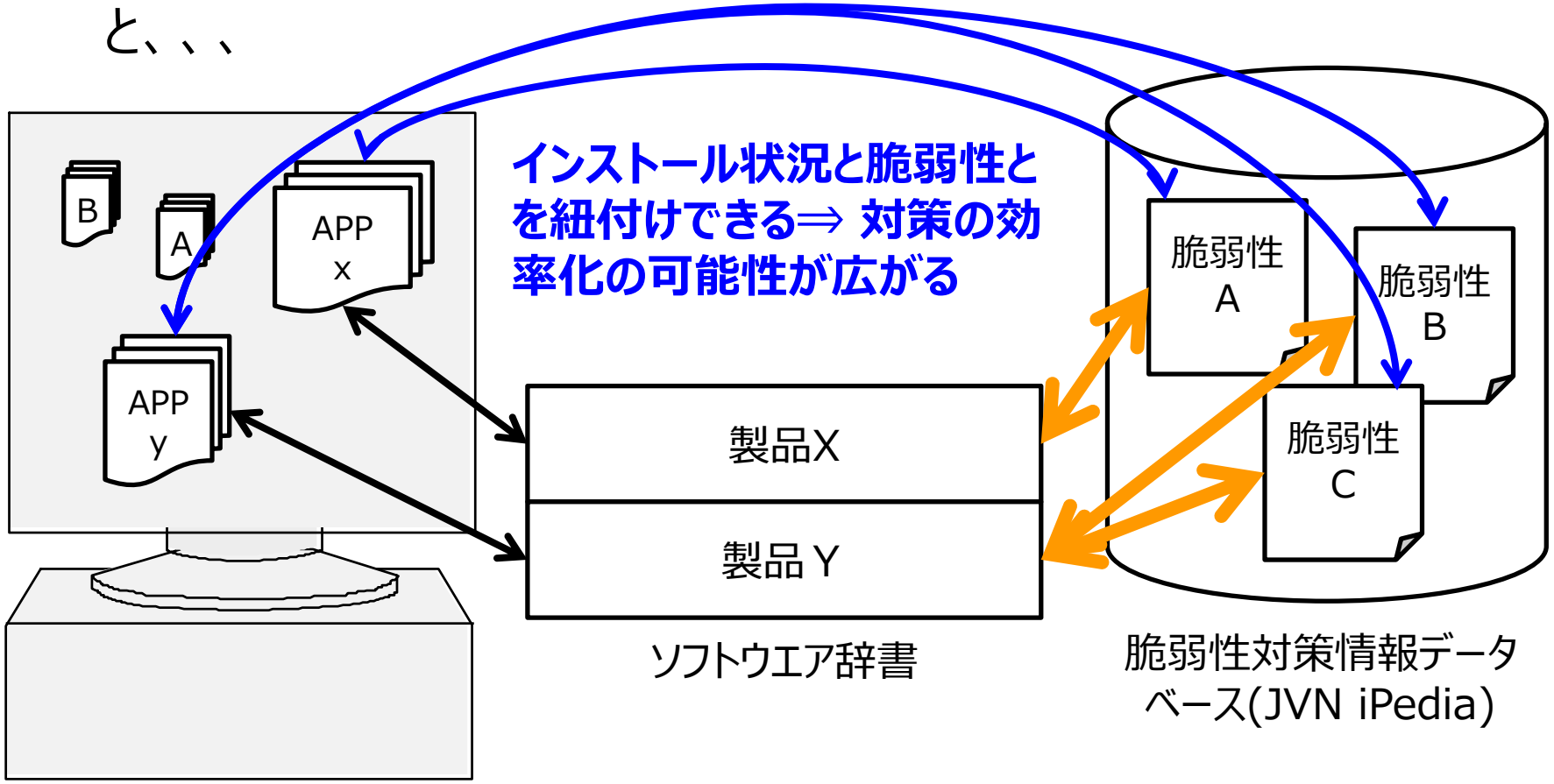
- 多くの場合、インストール状況と脆弱性との紐付けを人手で実施している(資産管理と脆弱性対策とが連携できているわけではない)。



ソフトウエア辞書とのデータ連携
～インストール状況と脆弱性との紐付け～

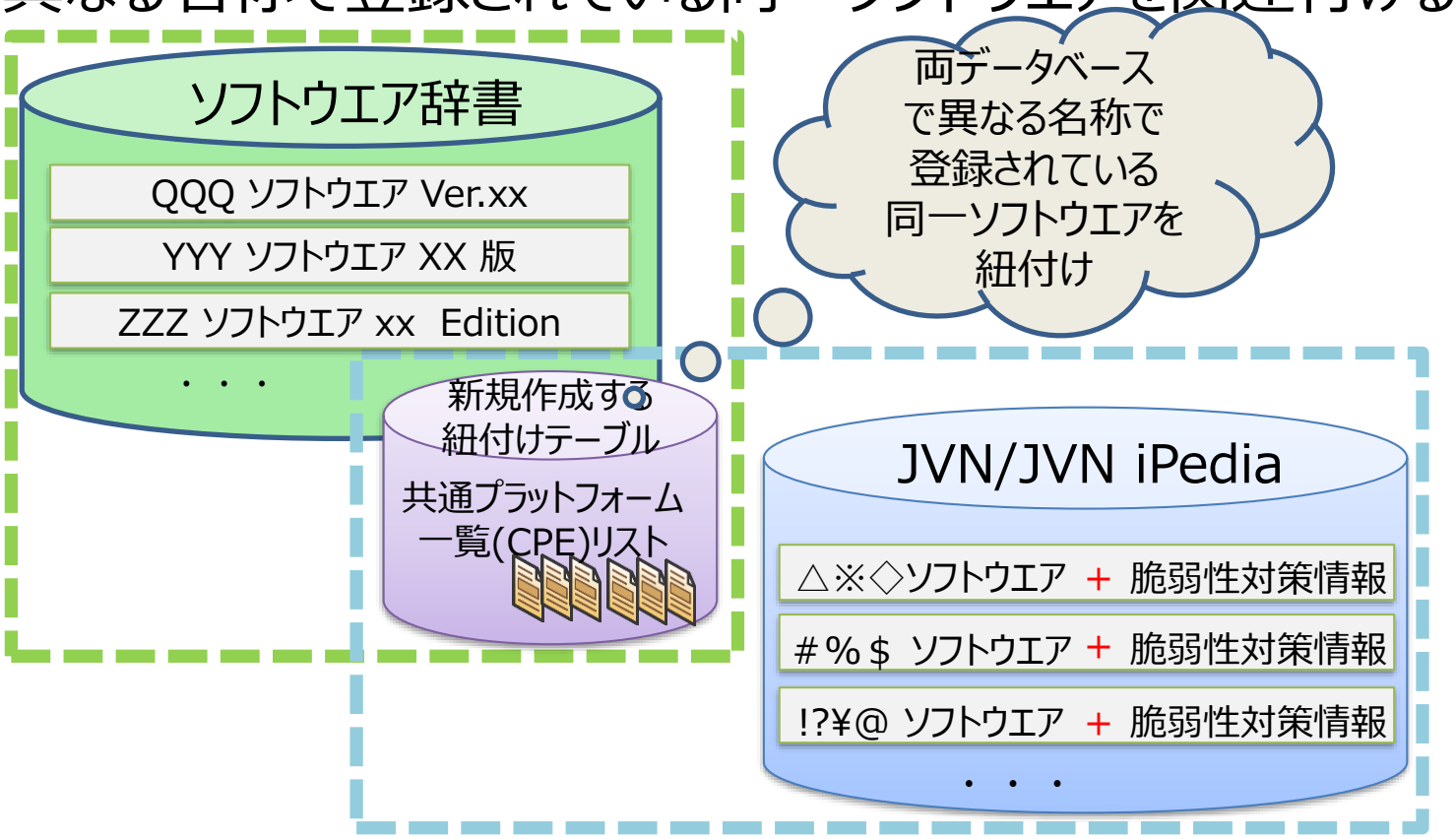
IPA

- もし、インストール状況を把握できるソフトウエア辞書と脆弱性対策情報サイト(JVN/JVN iPedia)とを紐付け[橙色の線]できると、、、



ソフトウエア辞書とのデータ連携
～インストール状況と脆弱性との紐付け～

- 紐付けとは
  ソフトウエア辞書と脆弱性対策情報サイト(JVN/JVN iPedia)で異なる名称で登録されている同一ソフトウエアを関連付けること



ソフトウエア辞書とのデータ連携
～SAMACソフトウエア辞書～

- SAMAC(一般社団法人ソフトウエア資産管理評価認定協会)が保守提供しているインストール状況を把握できるデータベース
  - インベントリ収集ツールで収集可能な[プログラムの追加と削除]に表示されているインストール名称をベースに作成
  - ソフトウエア辞書に登録されている項目は、ベンダ名、ソフトウエア名、エディション、バージョン、ソフトウエア種別(有償ソフトウエア・フリーウェア、HOTFIX、ドライバ・ユーティリティ等)

ソフトウェア名	ベンダ名	エイリアス	バージョン	エディション	種別
Adobe Flash Player 10 ActiveX	ADOBE SYSTEMS	Flash Player	10	ActiveX	フリーウェア
Realtek High Definition Audio Driver	Realtek Semiconductor	High Definition Audio Driver	-	-	ドライバー・ユーティリティー等
Microsoft .NET Framework 3.5 SP1	Microsoft	.NET Framework	3	-	フリーウェア
IP Messenger for Win32	白水 啓章	IP Messenger	32	-	フリーウェア
Microsoft Office Personal 2007	Microsoft	Office	2007	Personal	有償ソフトウェア
JUSTSYSTEMｱﾌﾟﾘｹｰｼｮﾝの追加と削除	JUSTSYSTEMS	アプリケーションの追加と削除	-	-	ドライバー・ユーティリティー等
Google Toolbar for Internet Explorer	Google	Google Toolbar	-	-	フリーウェア
Intel(R) Graphics Media Accelerator Driver	Intel	Graphics Media Accelerator Driver	-	-	ドライバー・ユーティリティー等

ソフトウエア辞書とのデータ連携
～製品識別子CPEを用いた製品の紐付け～

IPA

- Common Platform Enumeration
  (共通プラットフォーム一覧)
  情報システムを構成するハードウェア、ソフトウエアの名称を、プログラムで(機械)処理しやすい形式で記述するための仕様
- MyJVN APIでは、CPE v2.2をサポート

cpe:/a:ipa:myjvn

cpe:/{種別}:{ベンダ}:{製品}:{バージョン}

:{アップデート}:{エディション}:{言語}

種別：h=ハードウェア、o=OS、a=アプリケーション

ソフトウエア辞書とのデータ連携
～製品識別子CPEを用いた製品の紐付け～

IPA

- インストール状況を把握できるSAMACソフトウエア辞書に連携用項目に製品識別子CPEを用いた製品を追記

SAMAC ソフトウエア 辞書

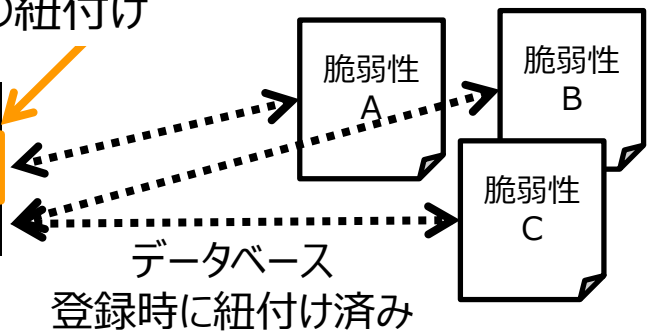
SAMACソフトウエア辞書の既存登録項目(9項目)				連携用項目(1項目)
sw_id	sw_vendor	sw_name	その他項目	CPE v2.2
・・・	・・・	Adobe Acrobat 8.2.0 Professional	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.0 Standard	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 - CPSID_50570	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 Professional	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 8.2.1 Standard	・・・	cpe:/a:adobe:acrobat
・・・	・・・	Adobe Acrobat 9.3.0 - CPSID_52073	・・・	cpe:/a:adobe:acrobat

ソフトウエアの 脆弱性 データベース

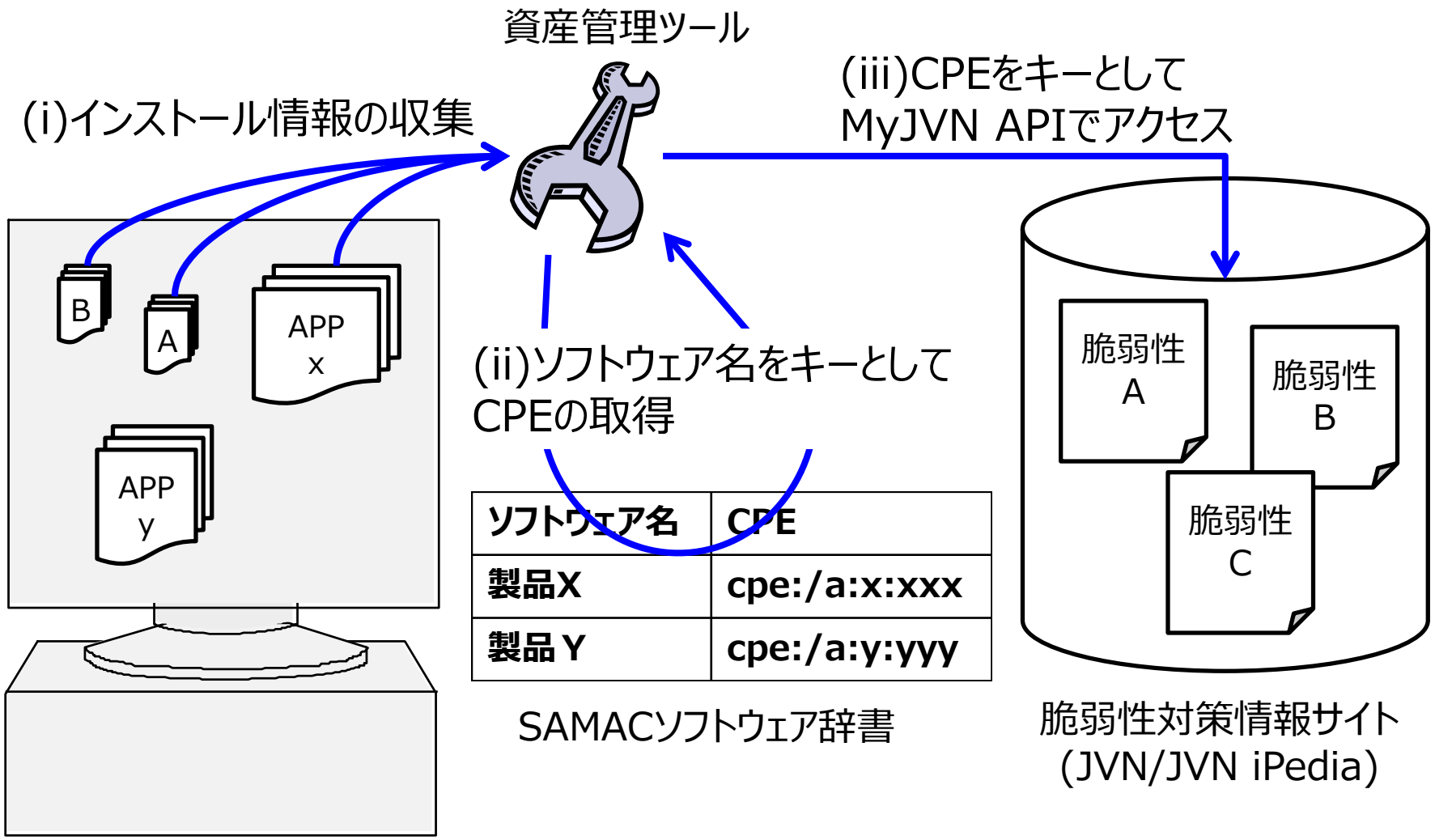
製品識別子CPEを用いた製品の紐付け

ソフトウエア名	CPE v2.2
Adobe Acrobat	cpe:/a:adobe:acrobat
製品Y	cpe:/a:y:yyy

JVN製品データベース



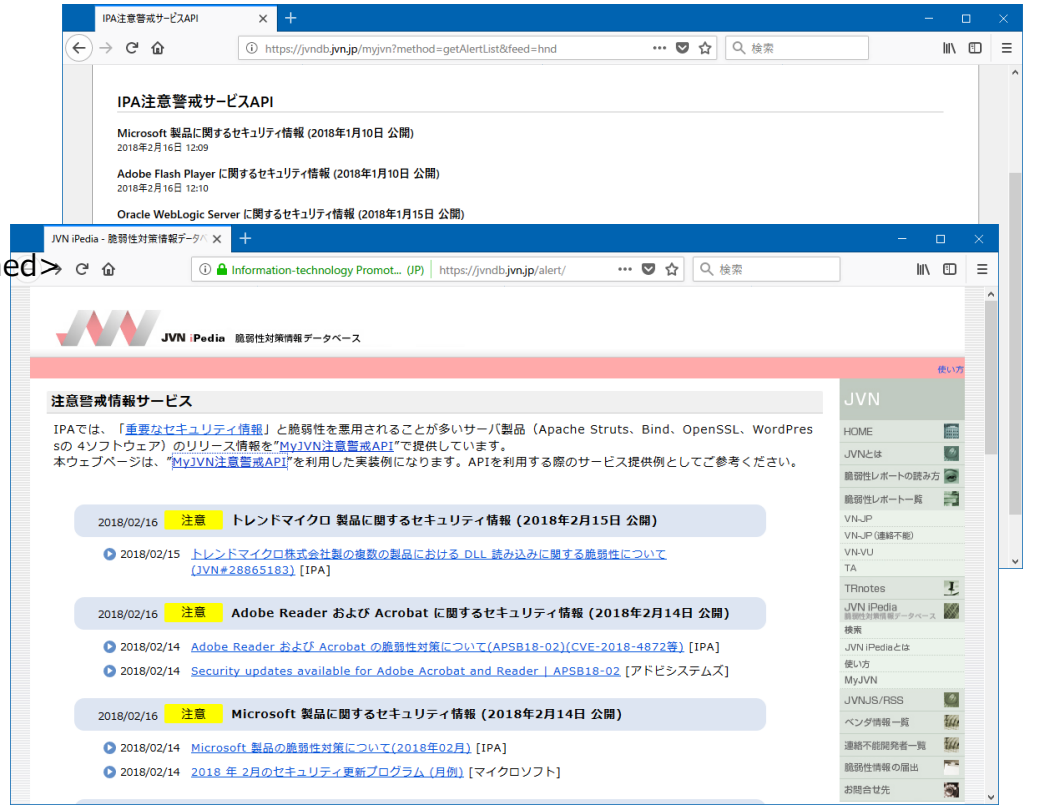
ソフトウエア辞書とのデータ連携
～脆弱性対策情報参照までの流れ～



ソフトウエア辞書とのデータ連携
～<新規>MyJVN API 注意警戒情報一覧取得～

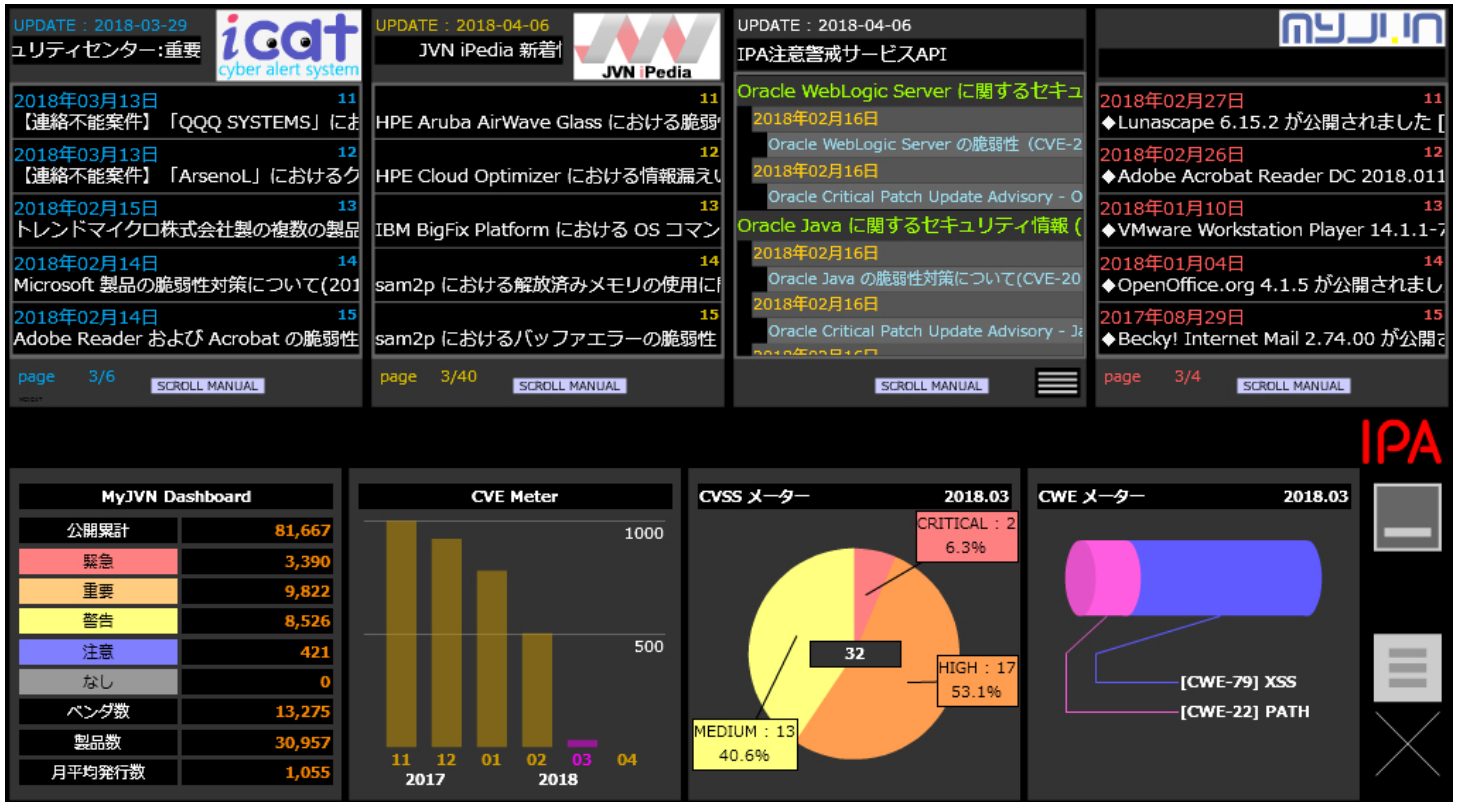
- 注意警戒情報一覧取得 getAlertList
  https://jvndb.jvn.jp/alert/
  - 脆弱性対策の動きの見える化の試みとして、関連情報をグループ化しながら追記
  - 製品識別子CPE(OpenSSL、BIND、Apache Struts、WordPress)を記載

```
<entry>
  <title>注意警戒のタイトル</title>
  <id>注意警戒の識別子</id>
  <summary>注意警戒の概要</summary>
  <link href="https://www.ipa.go.jp/" />
  <published>2017-07-13T08:29:29-04:00</published>
  <updated>2017-07-03T12:29:29Z</updated>
  <category term=" /Critical" label=" 緊急" />
  <sec:items>
    <sec:item>
      <sec:title>関連情報のタイトル</sec:title>
      <sec:identifier>関連情報の識別子</sec:identifier>
      <sec:summary>関連情報の概要</sec:summary>
      <sec:link href=" 関連情報の概要のURL" />
      <sec:cpe>製品識別子</sec:cpe>
    </sec:item>
    sec:item ノードを繰り返します。
  </sec:items>
</entry>
```



ソフトウエア辞書とのデータ連携
～<新規>MyJVN 脆弱性対策情報ダッシュボード～

- MyJVN 脆弱性対策情報ダッシュボード (mjdashboard)
  https://jvndb.jvn.jp/apis/myjvn/mjdashboard.html
  - JVN iPedia に登録されている脆弱性対策情報をMyJVN APIなどを利用して表示するためのツール



脆弱性対策に関わる基盤の整備
～JVN脆弱性対策機械処理基盤～

- 自動化などの脆弱性対策利活用基盤として、JVNを活用し、必要とされる新たなサービスを提供できる環境を整備していく

MyJVN

バージョン
チェッカ

セキュリティ設定
チェッカ

脆弱性対策
情報収集ツール

JVN Japan Vulnerability Notes
情報セキュリティ早期警戒
パートナーシップに報告された
脆弱性対策情報

JVN iPedia
国内外で報告された
脆弱性に対する
国内製品開発者の
脆弱性対策情報

共通脆弱性識別子CVEが
付与されている脆弱性対策情報

国内外で報告された
全ての脆弱性対策情報

MyJVN
JVNとJVN iPediaに登録されている脆弱性対策情報を対策実施に直結したサービスに繋げるための仕組みを提供する

JVN iPedia
国内で利用されている製品を対象にした脆弱性対策情報を広く蓄積する

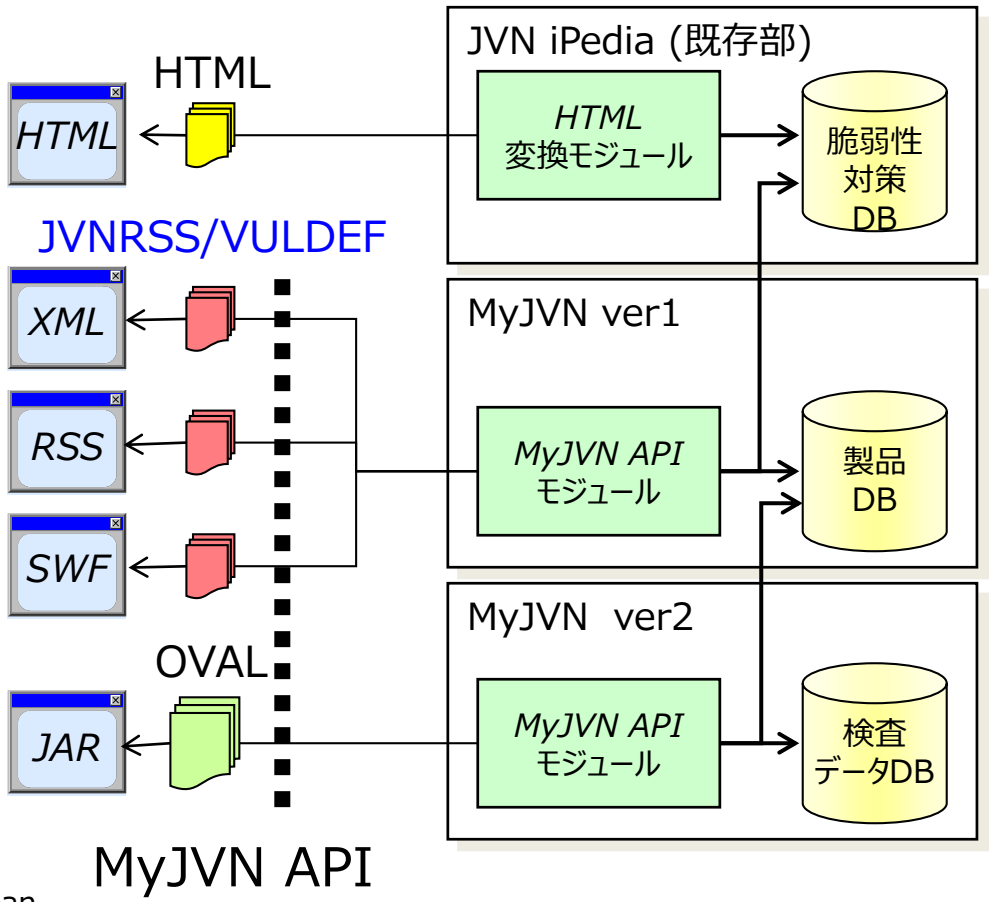
JVN
製品開発者と調整した脆弱性対策情報をタイムリーに公開する

脆弱性対策に関わる基盤の整備
～JVN脆弱性対策機械処理基盤～

- MyJVN API (http://jvndb.jvn.jp/apis/)
  - JVN iPediaの情報をウェブを通じて利用するためのソフトウエアインタフェース⇒ユーザ側でツール開発も可能

フィルタリング型情報提供
⇒ MyJVN脆弱性対策
情報収集ツール
⇒ JPCERT/CC VRDA連携

検査データ提供
⇒ MyJVNバージョンチェッカ
⇒ MyJVNセキュリティ設定チェッカ



脆弱性対策に関わる基盤の整備
～JVN脆弱性対策機械処理基盤～

- 注意警戒情報一覧取得 getAlertList
  https://jvndb.jvn.jp/apis/getAlertList_api_hnd.html

  - リクエスト形式
    https://jvndb.jvn.jp/myjvn?method=getAlertList&feed=hnd

  - レスポンス形式
    - XML：Atom+mod_sec
      - https://jvndb.jvn.jp/schema/atom.xsd
      - https://jvndb.jvn.jp/schema/mod_sec_3.0.xsd
        - グループ化記述用フィールドをサポート
    - JSON
      - https://jvndb.jvn.jp/schema/getalert1.json

最後に

日々の脆弱性関連情報の収集だけではなく、セキュリティリスク分析や資産管理と連携させた対策を進めることで、サイバーセキュリティリスクの管理を加味した脆弱性対策を実現していく必要があります。
JVN脆弱性対策機械処理基盤では、共通基準／共通仕様の活用、データ連携により、IT資産と脆弱性対策との一元的な管理を支援する基盤の整備を進めています。
脆弱性に対して適切な対応をとっていきましょう。


IPA
Better Life
with IT