

ET&IoT Technology 2018
IPA ブースプレゼンテーション

事業被害ベースのリスク分析シート

リスク	発生可能性	被害	対策	リスク	発生可能性	被害	対策
1	2	2	3	2	2	2	3
2	2	2	3	2	2	2	3
3	2	2	3	2	2	2	3
4	2	2	3	2	2	2	3
5	2	2	3	2	2	2	3
6	2	2	3	2	2	2	3
7	2	2	3	2	2	2	3
8	2	2	3	2	2	2	3
9	2	2	3	2	2	2	3
10	2	2	3	2	2	2	3
11	2	2	3	2	2	2	3
12	2	2	3	2	2	2	3
13	2	2	3	2	2	2	3
14	2	2	3	2	2	2	3
15	2	2	3	2	2	2	3
16	2	2	3	2	2	2	3
17	2	2	3	2	2	2	3
18	2	2	3	2	2	2	3
19	2	2	3	2	2	2	3
20	2	2	3	2	2	2	3

制御システムのセキュリティ

～サイバー攻撃の現状とリスク分析のすすめ～

2018年11月14日(水) 16:30 - 16:50

2018年11月15日(木) 14:30 - 14:50

2018年11月16日(金) 14:00 - 14:20

独立行政法人情報処理推進機構(IPA)

セキュリティセンター

セキュリティ対策推進部

福原聡／岡下博子



本日の内容

1. 制御システムとは
2. 制御システムのセキュリティ
3. 制御システムにおける脅威
4. 制御システムへのサイバー攻撃の分類
5. サイバー攻撃事例
6. リスク分析のすすめ
7. リスク分析の例
8. リスク分析ガイドのご紹介

1. 制御システムとは

- 制御システムとは
電力・ガス、石油・化学等のプラントにおける監視制御や、機械・食品の工場の生産ライン等で利用されているシステム
- 制御システムの特長
 - ✓ 社会基盤、産業基盤を支えており可用性が最重要。停止による社会的な影響・事業継続上の影響が大きい
 - ✓ システムのライフサイクルが10-20年と長期間



石油化学プラント



工場の生産ライン

2. 制御システムのセキュリティ

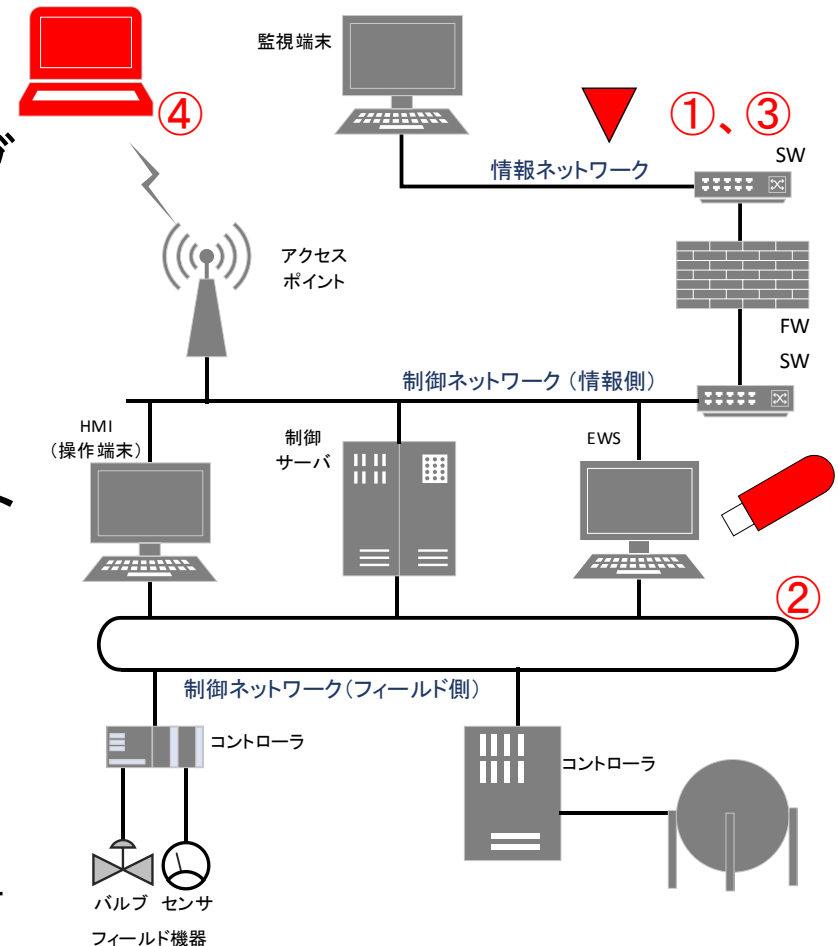
- セキュリティ対策の必要性
 - インターネット、リモート回線等外部ネットワークとの接続
 - 構成コンポーネントがWindowsやLinux等の汎用品
 - USBメモリの利用
- 制御システムに対する攻撃
 - 日本の20～40%の制御システムはサイバー攻撃を受けている
 - カスペルスキー <https://ics-cert.kaspersky.com/> から推定
 - 60%の制御ネットワークは外部から侵入可能
 - ポジティブテクノロジー
<https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ICS-attacks-2018-eng.pdf>

3. 制御システムにおける脅威

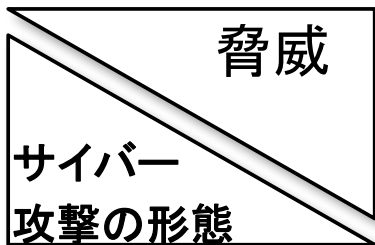
- 制御システムにおける脅威 (2016年 高い順)

- ① ソーシャルエンジニアリングとフィッシング
- ② USBメモリや外部のPCを介してマルウェア感染
- ③ インターネット/イントラネットからのマルウェア感染
- ④ リモートアクセス

- BSI Industrial Control System https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005E.pdf?__blob=publicationFile&v=3



4.制御システムへのサイバー攻撃の分類



インターネット/
イントラネット/
フィッシング

USBメモリ
持ち込み機器

リモートアクセス

バラマキ型
差別に
攻撃、破壊

日英仏 自動車メーカー
2017 WannaCry
1～数日の操業停止

米 発電所
2012 Mariposa
運転再開が3週間遅延

凡例:国 業界/施設
年 マルウェア名
事業被害

標的型
一つの目標に
突き進む

ウクライナ 電力
2015 BlackEnergy3
22.5万人停電3-6時間

イラン ウラン濃縮施設
2010 Stuxnet
8400台の遠心分離機
が破壊

中東 石化プラントSIS
2017 TRITON
フェールセーフでシス
テム停止

5.サイバー攻撃事例(1)

膨大な損失が発生する

- ランサムウェア感染による自動車工場の操業停止
 - 【被害】:2017年5月~6月、フランス、英国および日本の大手自動車メーカーの工場で、コンピュータがマルウェア WannaCry に感染し、1日~数日間操業が停止した。
 - 【原因】:外部ネットワークからの感染か隔離されたネットワークへの外部機器の持ち込みか



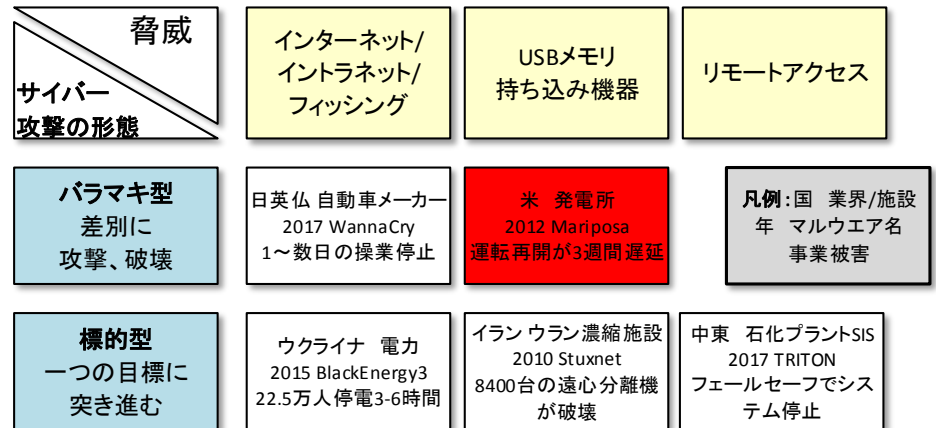
Wannacry感染による暗号化画面

脅威 サイバー 攻撃の形態	インターネット/ イントラネット/ フィッシング	USBメモリ 持ち込み機器	リモートアクセス
	パラキ型 差別に 攻撃、破壊	日英仏 自動車メーカー 2017 WannaCry 1~数日の操業停止	米 発電所 2012 Mariposa 運転再開が3週間遅延
標的型 一つの目標に 突き進む	凡例:国 業界/施設 年 マルウェア名 事業被害	ウクライナ 電力 2015 BlackEnergy3 22.5万人停電3-6時間	イラン ウラン濃縮施設 2010 Stuxnet 8400台の遠心分離機 が破壊
		中東 石化プラントSIS 2017 TRITON フェールセーフでシス テム停止	

5.サイバー攻撃事例(2)

マルウェア感染はネットワーク経由だけではない

- 米 発電所のタービン制御システム
 - 【被害】:2012年、制御ネットワークに接続された約10台のコンピュータがマルウェア Mariposa に感染した結果、運転再開が約3週間遅延
 - 【原因】:システム管理会社がメンテナンス時にアップデートを行おうとして**USBメモリーを持ち込み感染**



5.サイバー攻撃事例(3)

制御専用のプロトコルを利用/広範囲で被害

ウクライナ 電力

- 【被害①】:2015年12月、3時間～6時間にわたり大規模停電が発生。22万5千人に影響を及ぼした。侵入にはマルウェア BlackEnergy3 が使われたが、停電を引き起こした最終的な攻撃は、**攻撃者による制御システムの不正操作**であったと言われる。
- 【原因】: 標的型メールによる感染
- 【被害②】: 翌2016年12月、30分～1時間15分にわたる大規模停電が発生。制御システムがマルウェア「Industroyer/CrashOverride」に感染し、**当該マルウェアが送電変電所の遮断機を不正操作**したと言われる。



1年で進化



サイバー 攻撃の形態	脅威	インターネット/ イントラネット/ フィッシング	USBメモリ 持ち込み機器	リモートアクセス
	パラミキ型 差別に 攻撃、破壊	日英仏自動車メーカー 2017 WannaCry 1～数日の操業停止	米 発電所 2012 Mariposa 運転再開が3週間遅延	凡例:国 業界/施設 年 マルウェア名 事業被害
標的型 一つの目標に 突き進む	ウクライナ 電力 2015 BlackEnergy3 22.5万人停電3-6時間	イラン ウラン濃縮施設 2010 Stuxnet 8400台の遠心分離機 が破壊	中東 石化プラントSIS 2017 TRITON フェールセーフでシ テム停止	

5.サイバー攻撃事例(4)

独自仕様の制御システムで発症し人知れず活動

- イラン ウラン濃縮施設

- 被害: マルウェア Stuxnet に感染したコンピュータの制御により、ウラン濃縮施設の8400台の遠心分離機が破壊された。このマルウェアは、管理者には全て正常に作動していると見せかけつつ、機器に高い負荷をかけて稼働不能としたとされる。
- 原因: USBメモリで持ち込まれたといわれる

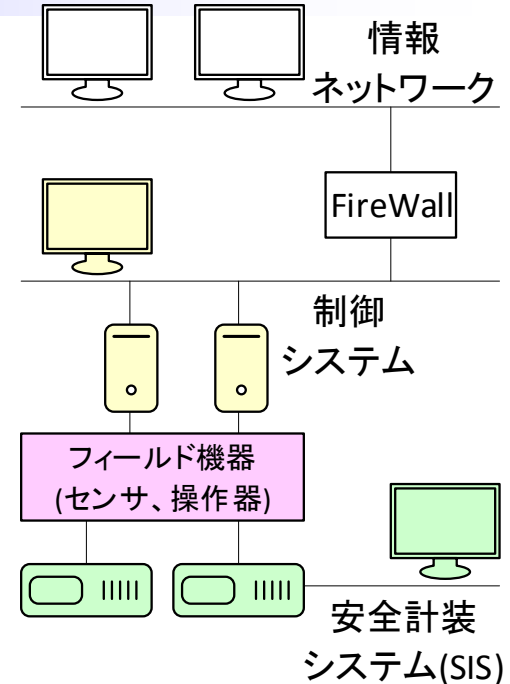


5.サイバー攻撃事例(5)

SIS (安全計装システム) さえも攻撃対象

- 中東 石化プラント

- 【被害】2017年 石油化学プラントの安全計装システム(SIS)のコントローラの制御プログラムをマルウェア TRITON が改竄し、プロセスが緊急停止。
- 【原因】マルウェアによるEWS(エンジニアリングワークステーション)へのリモートアクセス (詳細不明)



脅威 サイバー 攻撃の形態	インターネット/ イントラネット/ フィッシング	USBメモリ 持ち込み機器	リモートアクセス
	パラミキ型 差別に 攻撃、破壊	日英仏 自動車メーカー 2017 WannaCry 1~数日の操業停止	米 発電所 2012 Mariposa 運転再開が3週間遅延
標的型 一つの目標に 突き進む	ウクライナ 電力 2015 BlackEnergy3 22.5万人停電3-6時間	イラン ウラン濃縮施設 2010 Stuxnet 8400台の遠心分離機 が破壊	中東 石化プラントSIS 2017 TRITON フェールセーフでシ ステム停止

6.リスク分析のすすめ

様々なタイプのサイバー攻撃にいかに対応するか？

- 標的型かバラマキ型か？
- 侵入される経路は？
- どのような被害が想定されるか？
- システムのどこを強化すべきか？



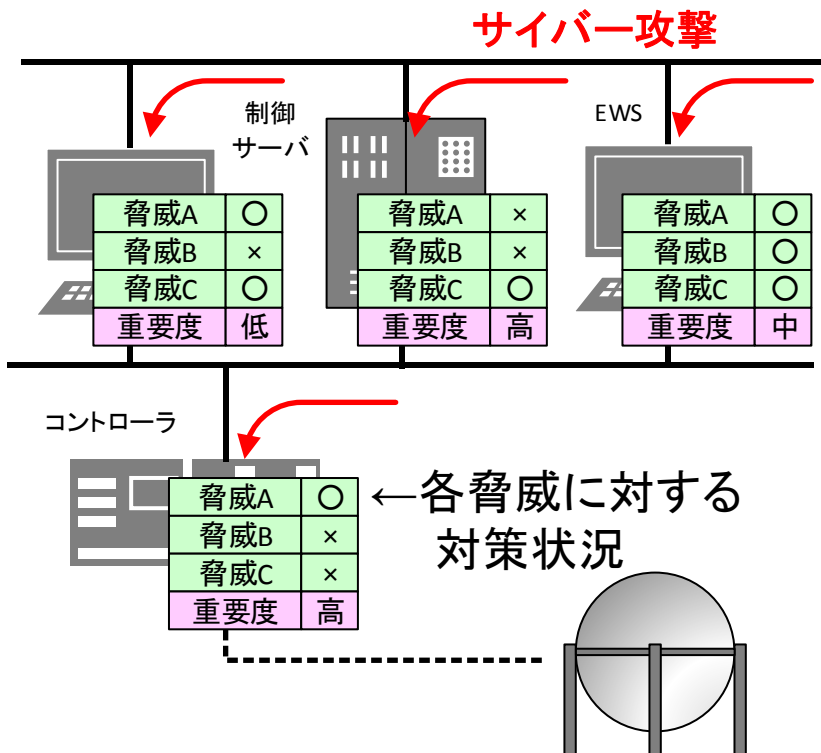
システム全体の俯瞰と効果的なセキュリティ対策の検討が必要 → 詳細リスク分析

6. リスク分析のすすめ

2つの詳細リスク分析

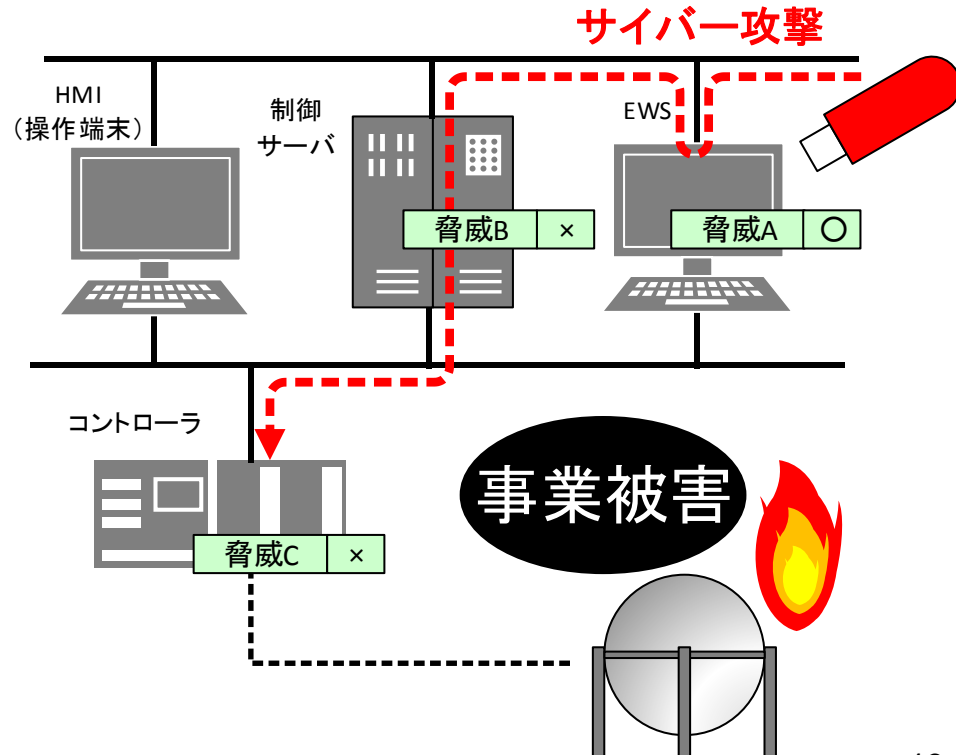
資産ベースのリスク分析

- 全資産を漏れなく分析



事業被害ベースのリスク分析

- 事業被害を生じさせる攻撃手順に沿って分析

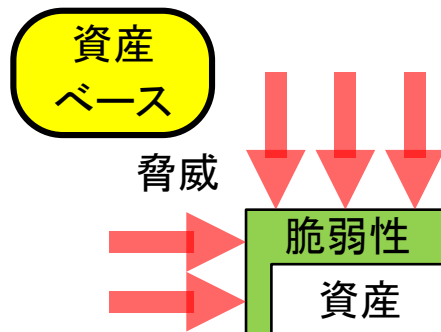


6.リスク分析のすすめ

2つの詳細リスク分析

資産ベースのリスク分析

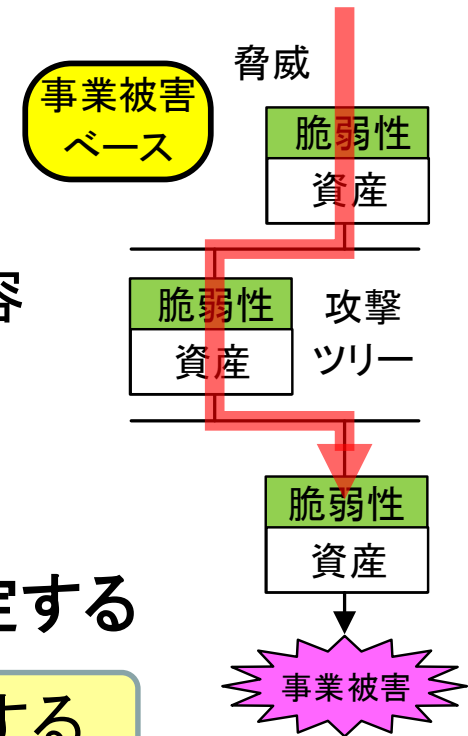
- 資産単体のさまざまな脅威に対する対策状況(脆弱性の裏返し)を分析
- 資産の重要度を分析



→ リスク値を算定する

事業被害ベースのリスク分析

- 攻撃のシナリオを想定して攻撃ツリー(攻撃手順)の対策状況を分析
- 事業被害の内容と大きさを分析

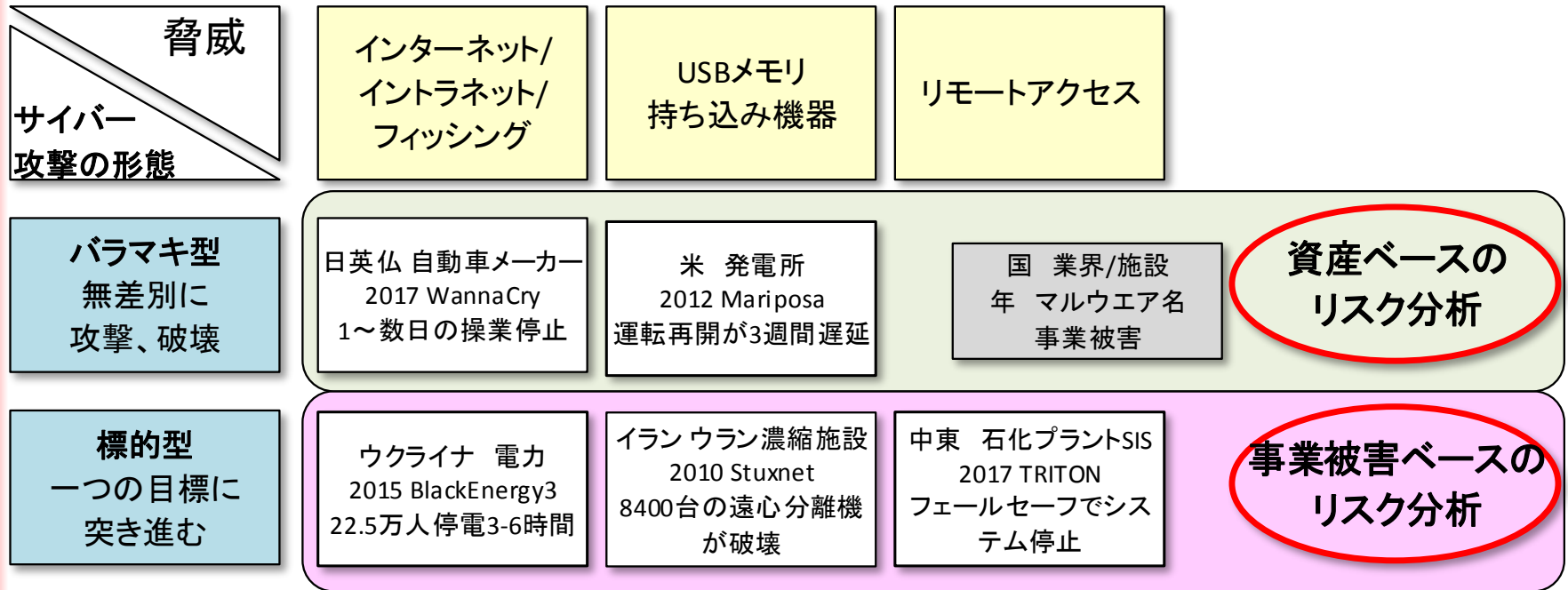


→ リスク値を算定する

高いリスク値に対策を検討する

6. リスク分析のすすめ

サイバー攻撃への対応



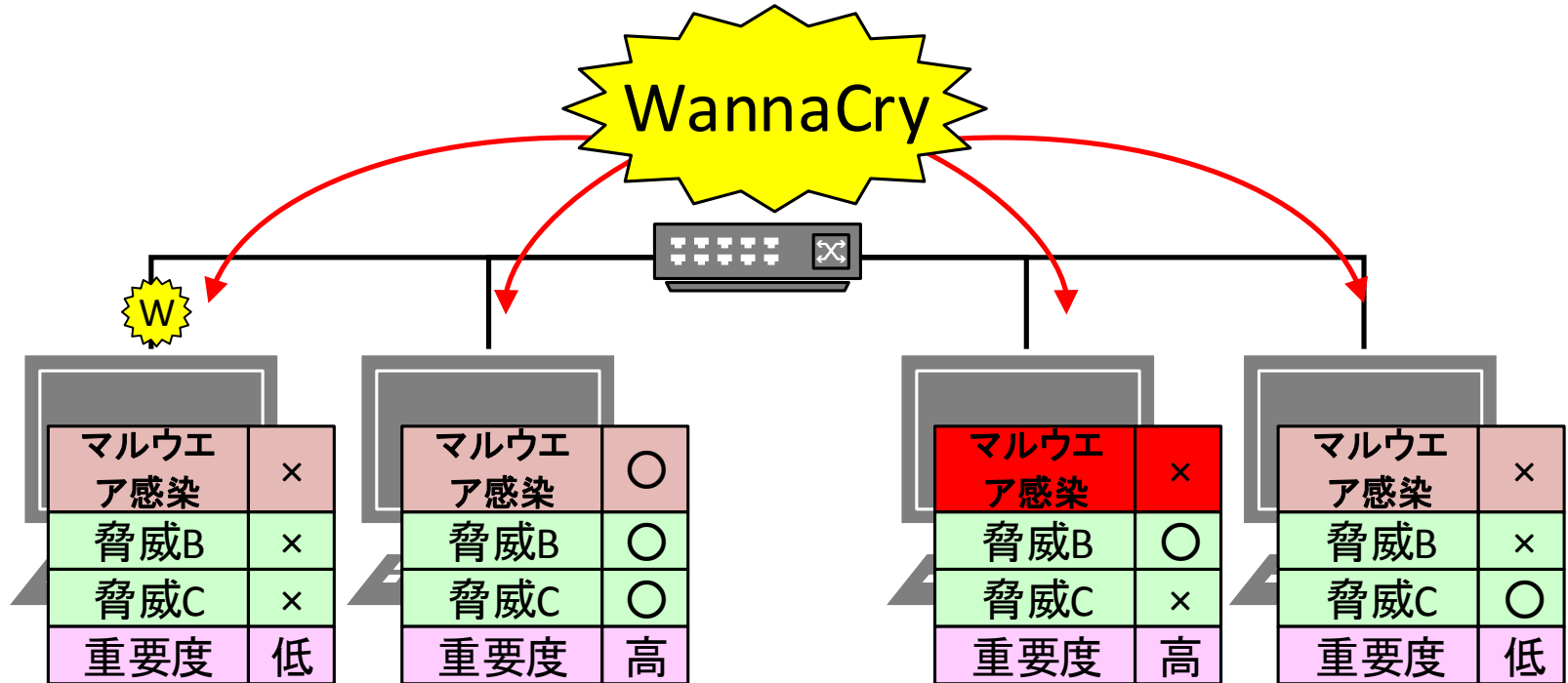
2つの詳細リスク分析は幅広く様々な脅威/攻撃に対応

7. リスク分析の例

資産ベースのリスク分析

- WannaCry

資産ベースのリスク分析

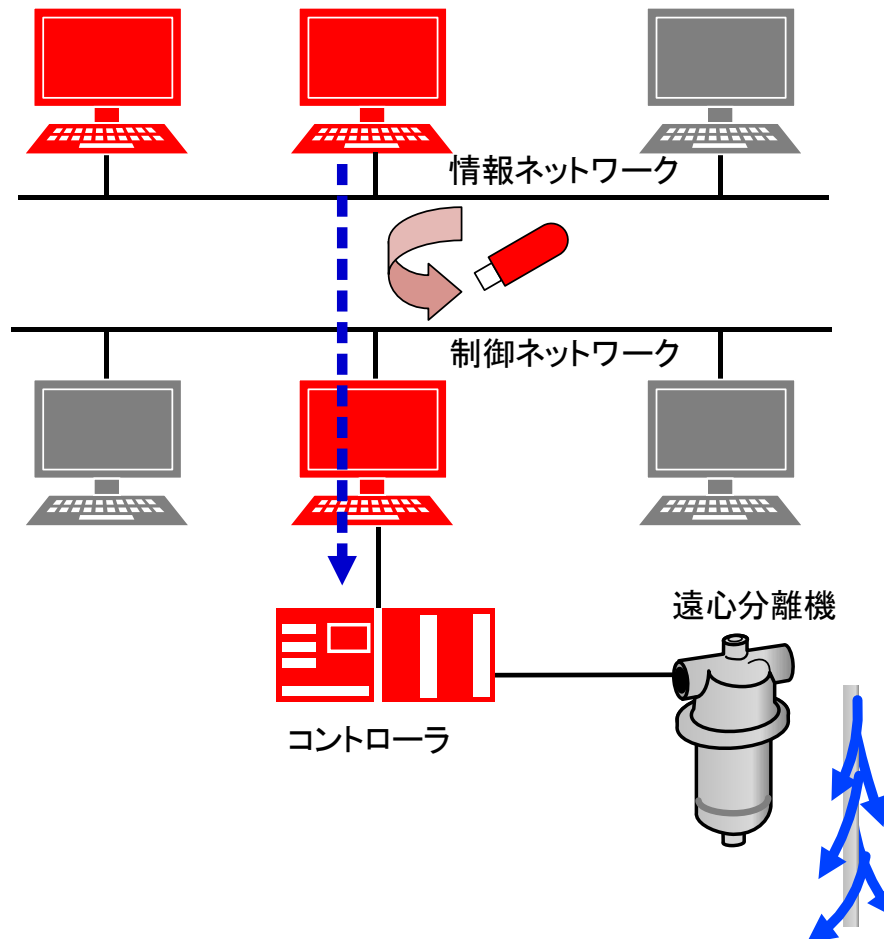


7. リスク分析の例

事業被害ベースのリスク分析

- Stuxnet

事業被害ベースのリスク分析



シナリオ：
制御ネットワーク上の
コンピュータシステム
にUSBメモリ経由でマ
ルウェアが侵入し、制
御ロジックを書き換え
る事で遠心分離機を
過負荷にて破壊した。

8. リスク分析ガイドのご紹介

制御システムのセキュリティリスク分析ガイド 第2版

2018年10月15日公開

• 制御システムのセキュリティ

－ 詳細リスク分析

- 資産ベース分析/事業被害ベース分析
- **セキュリティ投資の優先順位**等、組織として戦略的に検討可能
- 一度実施するとそれをベースに継続的セキュリティレベルの向上可能

－ 第2版の特徴

- 実際に分析を行った数業種の分析のフィードバックを含む
- よりわかりやすくシンプルにすることで分析工数を削減



<https://www.ipa.go.jp/security/controlsystem/riskanalysis.html>

12/10にIPAにて事業者向け有料セミナー開催予定

8. 制御システムに対するリスク分析の実施例

制御システムのセキュリティリスク分析ガイド 別冊

- 典型的なモデルシステムに対するリスク分析の完全な実施事例
 - ① データフローマトリックス
 - ② 資産の重要度の判断基準
 - ③ 各資産に対する重要度一覧
 - ④ 事業被害レベルの判断基準
 - ⑤ 事業被害とそのレベルの検討
 - ⑥ 脅威レベルの判断基準
 - ⑦ 脅威レベルの検討
 - ⑧ 資産ベースのリスク分析シート
 - ⑨ 攻撃シナリオ一覧の作成
 - ⑩ 攻撃ルート作成
 - ⑪ 事業被害ベースのリスク分析シート
 - ⑫ 制御システムのリスク分析結果(リスク低減のための改善策)

事業被害ベースのリスク分析シート



リスク分析シート一式(Excelファイル)は、以下のURLからダウンロード可能。

<https://www.ipa.go.jp/security/controlsystem/riskanalysis.html>

8.早わかり 活用の手引き

- 制御システムのセキュリティリスク分析ガイド(本体380ページ、別冊94ページ)のエッセンスをまとめた全36ページの紹介資料
- 活用の手引きは、以下のURLからダウンロード可能。
<https://www.ipa.go.jp/security/controlsystem/riskanalysis.html>

IPA Better Life with IT

早わかり

制御システムのセキュリティリスク分析ガイド
～セキュリティ対策におけるリスクアセスメントの実施と活用～

【活用の手引き 第2版】

独立行政法人情報処理推進機構(IPA)
セキュリティセンター
2018年10月

Copyright © 2018 独立行政法人情報処理推進機構

The image shows the cover of a guidebook. At the top left is the IPA logo with the tagline 'Better Life with IT'. Below it is a green oval with the text '早わかり' (Early Understanding). The main title is '制御システムのセキュリティリスク分析ガイド' (Control System Security Risk Analysis Guide) with a subtitle '～セキュリティ対策におけるリスクアセスメントの実施と活用～' (Implementation and Utilization of Risk Assessment in Security Countermeasures). A small screenshot of a risk assessment table is shown in the top right corner. Below the title is a blue horizontal line, followed by the text '【活用の手引き 第2版】' (Usage Guide, 2nd Edition). At the bottom, it says '独立行政法人情報処理推進機構(IPA) セキュリティセンター 2018年10月' (IPA Security Center, October 2018). A circular collage of various industrial and IT-related icons is positioned on the left side of the bottom section. The copyright notice 'Copyright © 2018 独立行政法人情報処理推進機構' is at the very bottom.

展示ブースにもお立ち寄りください。

制御システムの情報セキュリティ

制御システムへのサイバー攻撃の脅威

- ・ 制御システムの安全神話の崩壊
 - 汎用プラットフォーム (Windows, UNIX) や標準プロトコルの採用
 - 外部ネットワークとの接続 (遠隔監視 / 遠隔管理、リモートメンテナンス)
 - 記憶媒体の持ち込みによる外部とのデータ交換
 - 攻撃者による制御用通信プロトコルの理解
- ・ 最近のインシデント事例
 - 2015年、2016年 ウクライナ: 電力システムへのサイバー攻撃による大規模停電
 - 2017年 日・英・仏: 自動車の生産管理システムのランサムウェア感染による生産停止
 - 2017年 サウジアラビア: 安全計装システムへの攻撃

制御システムを保有する事業者向けのリスクアセスメントガイド

☞ 「制御システムのセキュリティリスク分析ガイド 第2版」

- ・ 自組織でリスクアセスメントを実施し、セキュリティ対策を向上するための**実践的な分析手法の解説書**
 - リスク分析の**全体像**の理解向上と取り組みを促進
 - リスク分析を具体的に実施するための**手順や手引き**
 - 2通りの**詳細リスク分析の手法** (資産ベース、事業被害ベース) を解説 【早分かり 活用の手引き】
- ・ **リスク分析のための素材**を提供
 - リスク分析シート (フォーマット、実施例)
 - 脅威 (攻撃方法) や対策の一覧
 - 特定対策に関する詳細チェックリスト
- ・ リスク分析結果の**活用例**の提示
 - リスク低減の対策強化策の検討方法
 - セキュリティテストの解説

経営者・管理者向けガイド

☞ 「制御システム利用者のための脆弱性対応ガイド 第3版」

- ・ リスクに対する**考え方の理解**
- ・ セキュリティ対策の**ポイントの把握**
- ・ 管理者が把握すべき脆弱性対応の**解説**

独立行政法人 情報処理推進機構
IPA 制御 セキュリティ

関連する展示ブースのご案内 (制御システムセキュリティ)

