制御システムにおける
セキュリティ対策優先順位付けガイド

2022年6月21日

独立行政法人 情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム 第 5 期受講生
対策優先順位付けプロジェクト

目次

1.はじめに

1-1. 課題背景

近年制御システムを狙ったサイバー攻撃は増加傾向にあり、対策導入の重要性や緊急性が高まっている。
速やかな対策が求められるが、計画して導入するまでには以下のようなハードルがある。

○リスクアセスメントを実施するスキルや時間がない。 課題(1)

○アセスメントを実施しても複数のリスクと複数の対策候補が挙がり、その中で優先順位付けが難しい。 課題(2)

○対策すべきリスクの優先順位はわかるが、企業固有の制約※1を加味すると優先順位付けが難しい。 課題(3)

※1 企業固有の制約例
- **現場の運用状況**によって導入しやすい対策とそうでない対策がある。
- 予算や納期によって導入しやすい対策とそうでない対策がある。

図. セキュリティ担当者が対策導入に向けて実施するタスクとハードルの対応イメージ

1-2. 本プロジェクトの狙い

リスク診断から対策の優先順位付けまで行うガイドとツールを作成し対策導入までのハードルを減らす。

ガイドの狙い

- どのようなリスクがあるか可視化しそれに対する対策を説明できる。
- 優先順位の付け方について議論の材料にできる。
- 企業固有の制約を加味した対策の優先順位付けを検討できる。

ネットワーク構成と重要資産を設定 セキュリティリスク診断	セキュリティ戦略を設定 優先順位付け	企業固有の制約を設定 導入する対策の決定

1-3. 想定利用シーン

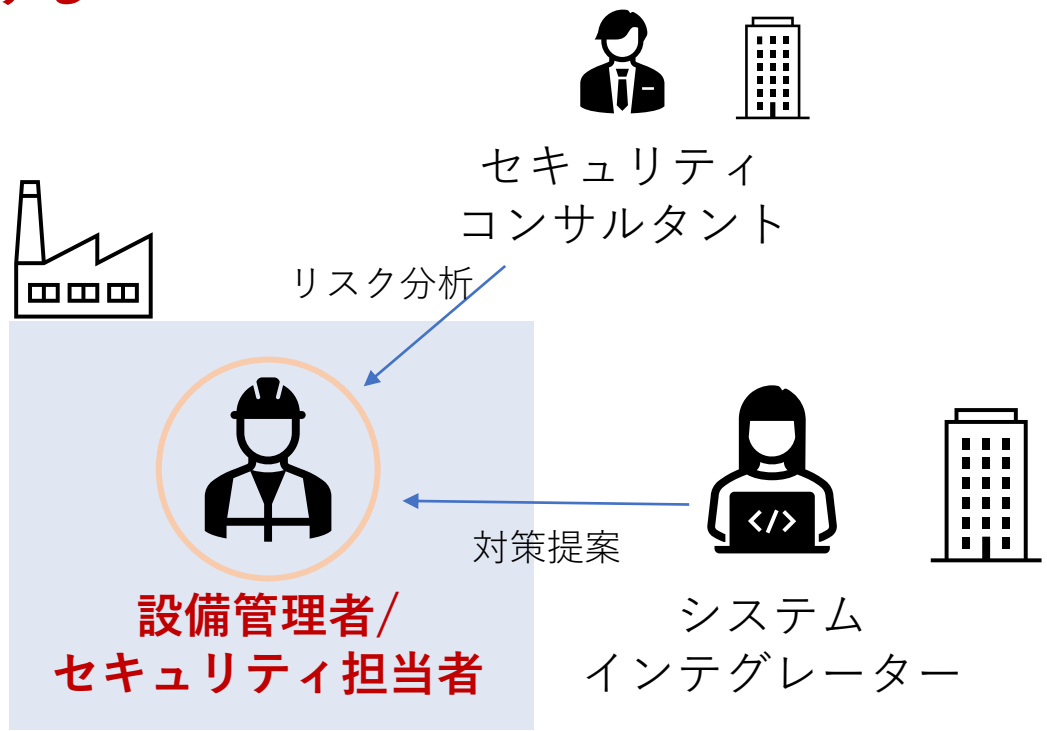
○ガイドの想定利用者

工場の設備管理者やセキュリティ担当者

特にセキュリティ対策がまだまだ十分でない企業を想定する

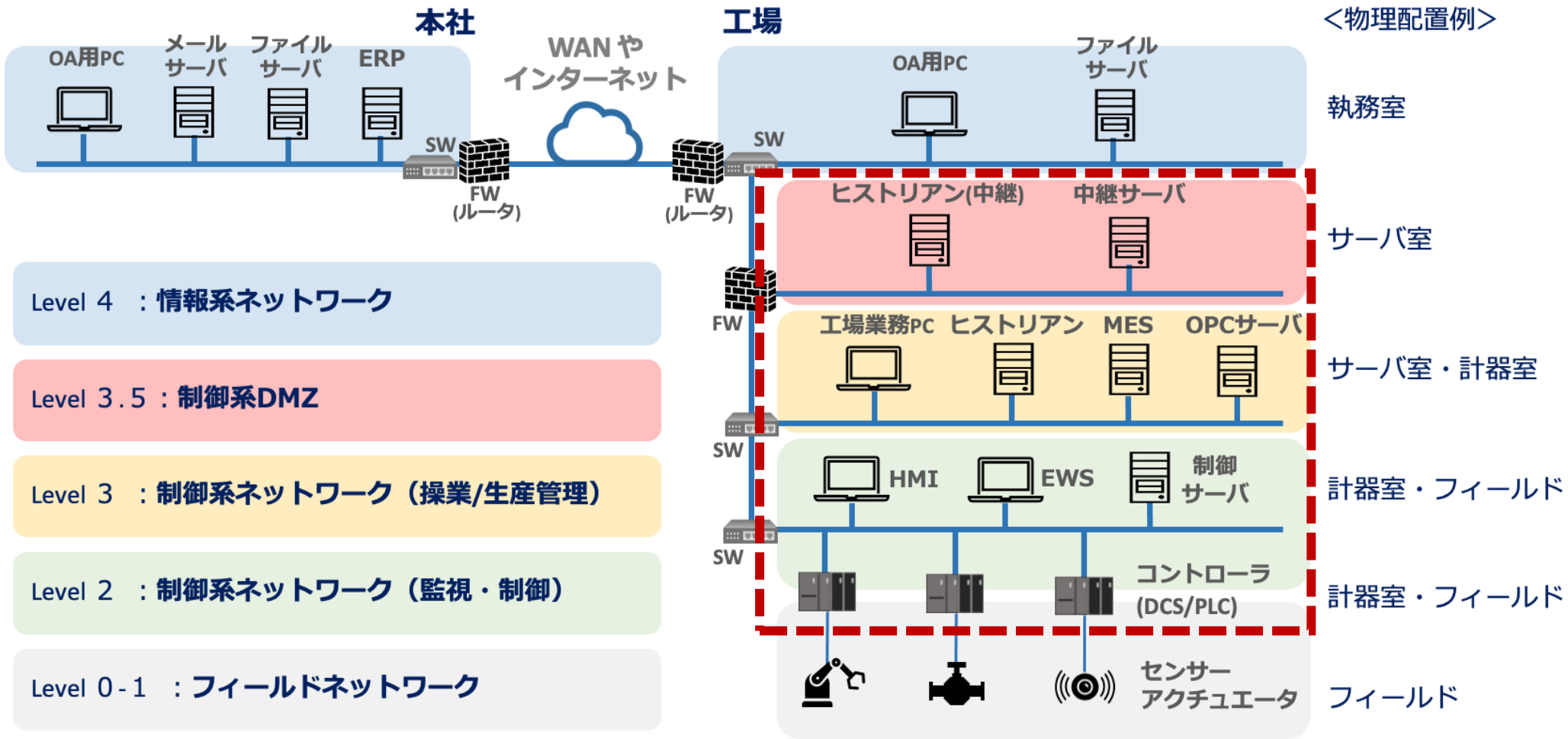
○ユースケース

- 工場の担当者が自発的に対策導入を検討する場合
- セキュリティコンサルタントによるリスク分析後に、どの対策から導入するか検討する場合
- システムインテグレータから複数の対策を提案され、どの対策から導入するか検討する場合



1-4. ガイドのスコープ

制御システム構成の制御系ネットワークから制御系DMZへのサイバーセキュリティリスクを対象とした、リスクアセスメントと対策の優先順位付けガイドを作成する。（情報系ネットワークはスコープ外とする）



1.5 制御システムを構成する資産の一覧

資産	機能
ERP	生産、物流、販売、会計データを一元化する基幹システムのサーバ。　※スコープ対象外
ファイルサーバ	制御系以外の情報を保存し業務で利用するサーバ。　※スコープ対象外
メールサーバ	制御系以外のOA用のメール送受信するサーバ。　※スコープ対象外
OA用PC	制御系以外の情報と業務に利用する端末。　※スコープ対象外
ファイアウォール(FW)	外部のネットワークからの攻撃や侵入を防ぐための機能を有する機器。
ルータ・スイッチ(SW)	複数のネットワークを集線、中継する機器。
データヒストリアン(中継)	長期間のプロセス値や管理パラメータを分析するためのサーバ。 制御ネットワークのデータヒストリアンのデータを中継して情報ネットワーク 側で参照する役割。
データヒストリアン	長期間のプロセス値や管理パラメータを分析するためのサーバ。 コントローラ、制御サーバからデータを収集した静的 なヒストリデータを扱う。
MES	生産工程を効率化するためERPの生産計画を元に制御サーバの設定値や指示を支援するサーバ。
制御サーバ	コントローラの制御機器に対し設定値やコマンドを送信し、制御機器 からのデータを集約するサーバ。
OPCサーバ	コントローラ、HMIとOPC通信でプロセス値を受信して制御サーバへ通信するサーバ。
EWS	コントローラのプログラムエンジニアリング及び改造やプログラムの変更等を行うための端末。
HMI(操作端末)	コントローラからの測定値を監視し、設定値(目標値)を入力する端末。
コントローラ	センサからの測定値が設定値に一致する様に、偏差から調節方式に応じて算出した操作量を調節するためアクチュエータに出力する機器。
フィールド機器	バルブやポンプ、電動機等の出力するアクチュエータの機器と、圧力計、温度計などプロセス値を計測するセンサー機器。

1-6. セキュリティ対策一覧（1/2）

対策名称	対策導入箇所	概要　実施内容
標的型メール訓練の定期実施	OA用PC	不正なメールを受信しても開封することないようにするために、OA用PCユーザに教育や周知を実施する。
OSやアプリケーションのバージョン最新化	OA用PC	脆弱性を悪用した攻撃を防止するためにパッチを可能な限り速やかに適用し脆弱性を 解消する。
アンチウイルスソフトによる検知、駆除	OA用PC	マルウェア感染を防止するために、アンチウイルス機能(製品)を利用してウイルス検知、除去する。
IDS（情報系）による不正通信検知	情報系ネットワーク	不正アクセスを検知、遮断するために、通信パケットを収集・解析・監視する機能を利用する。
FWやIPSによるIT/OT分離（制御系DMZ設置）	情報系ネットワークと制御系ネットワークの境界	外部から内部ネットワークへの侵入と侵攻拡散を防止するために、ネットワークを情報系ネットワーク、制御系DMZ、制御系ネットワークの3層のセグメントに分割して運用する。既に制御系DMZを構成している場合でも、FWやIPSの通信許可/不許可リストの見直しを定期的に行い、必要最低限の通信のみを許可することが重要である。
IDS（IT/OT境界）による不正通信検知	情報系ネットワークと制御系ネットワークの境界	不正アクセスを検知、遮断するために、通信パケットを収集・解析・監視する機能を利用する。
不正通信検知後の対応手順作成と定期訓練	情報系ネットワークと制御系ネットワークの境界	不正アクセスを検知後に対応できる手順書を作成することと一連の訓練を定期的に実施する。
ホワイトリスト型のプロセス起動制限	制御系ネットワーク内のサーバや端末	不要なプロセス起動を制限するため、ホワイトリスト作成しプロセス起動を禁止する。
IDS（制御系）による不正通信検知	制御系ネットワーク	不正アクセスを検知、遮断するために、通信パケットを収集・解析・監視する機能を利用する。
不正通信検知後の対応手順作成と定期訓練	制御系ネットワーク	不正アクセスを検知後に対応できる手順書を作成することと一連の訓練を定期的に実施する。
FWによるセグメント分割	制御系ネットワーク	不正通信を遮断するためにアクセス制御リスト（不要通信の禁止）を設定したファイアウォールを導入する。
複雑なパスワードの設定	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器	なりすましや不正アクセスを防止するために、初期パスワードの使用禁止、複数IDでの使い回しが内容に設定することと定期的な変更を行う。
通信の暗号化	制御系ネットワーク内	通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化し、内容を読めないようにする。

1-6. セキュリティ対策一覧（2/2）

対策名称	対策導入箇所	概要　実施内容
データの暗号化	制御系ネットワーク内 のサーバや端末	データ漏えいによる被害を最小化するために、暗号技術を用いてデータを暗号化し、データが漏えいしたとしても読み取りや不正利用できようにする。
インシデント対応手順の作成と定期訓練	―	インシデント対応する組織が適切に対応するために、対応手順やフローを作成して定期的に訓練を実施する。
操業の復旧手順の作成と定期訓練	―	制御に関わる組織（製造、計装）が適切に対応するために、対応手順やフローを作成して定期的に訓練を実施する。
ログ収集	制御系ネットワーク内 のサーバや端末、NW機器、 セキュリティ機器	攻撃の早期検知や被害の事後調査を行うため、システムのログ収集と分析（定期的or異常検知時）を行う。
データバックアップ	制御系ネットワーク内 のサーバや端末	データの物理的破壊や論理的破壊の攻撃時に回復するために、システムのデータバックアップ（コピー）を作成する。

1-7. 優先順位付けガイドの流れ

セキュリティリスク診断から対策の優先順位付けは大きく分けて3つのステップで決定する。

①セキュリティリスク診断

フレームワークを取り入れたリスク分析

・自組織の制御システムに対する攻撃シナリオ(リスク)とその対策を決定できる。

②導入すべき対策の優先順位付け

攻撃の発生可能性やセキュリティ戦略を考慮して優先順位付け

・防御対策と検知対応対策のどちらを優先するか企業の方針により決定できる。

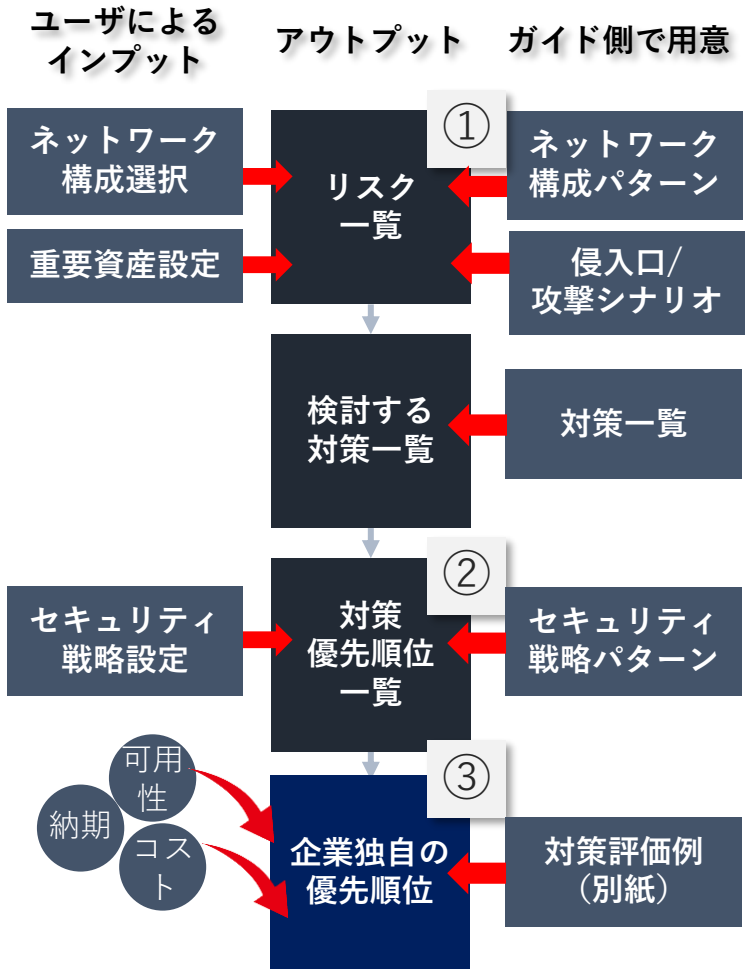
③企業固有の制約による優先順位付け

予算や制御システムの運用状況などの企業固有の制約を考慮して優先順位付け

- 各対策のコスト感や導入時のハードルについての評価を確認できる。

参考：優先順位付けガイドのロジック

ガイドの各ステップでユーザによるインプットとガイドのアウトプットで図を示す



2.セキュリティリスク診断

2. セキュリティリスク診断

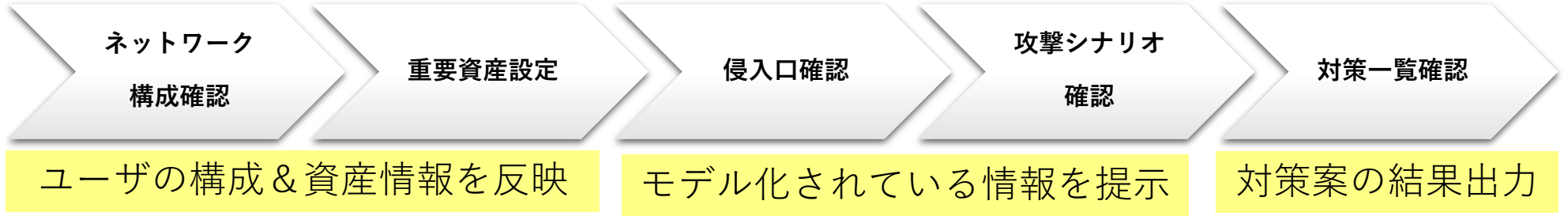
セキュリティリスク診断は５つの手順を実施する。

セキュリティリスク診断

フレームワークを取り入れたリスク分析

・自組織の制御システムに対する攻撃シナリオ(リスク)とその対策を決定できる。

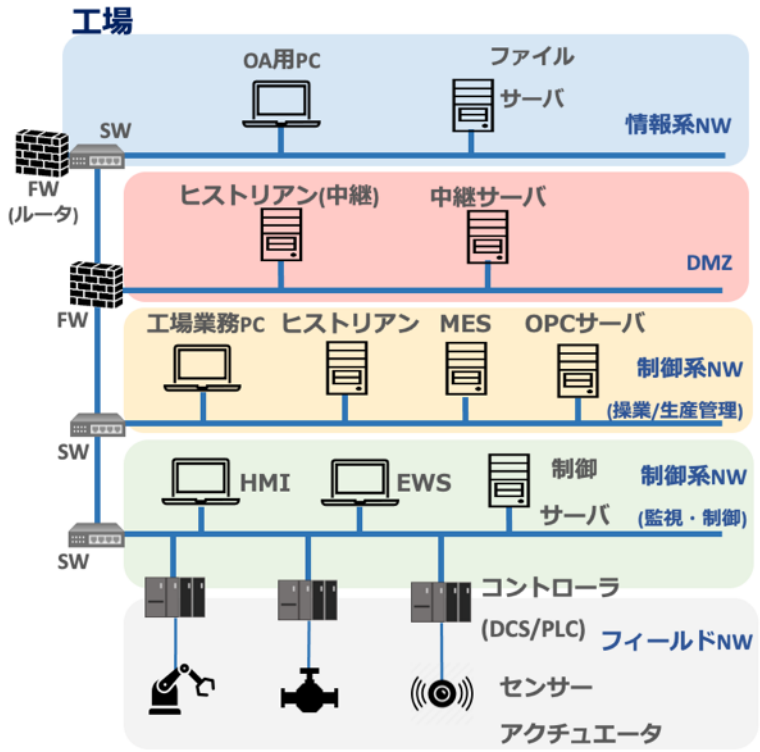
ガイド機能分類	概要
ネットワーク構成確認	構成図と資産をパターン化したものを提示して選択する。
重要資産設定	構成図から守るべき重要な資産を選択する。
侵入口確認	重要資産が攻撃対象となる侵入経路を決定する。
攻撃シナリオ確認	キルチェーンでモデル化された攻撃フェーズを決定する。
対策一覧確認	攻撃フェーズ別の対策検討案を提示する。



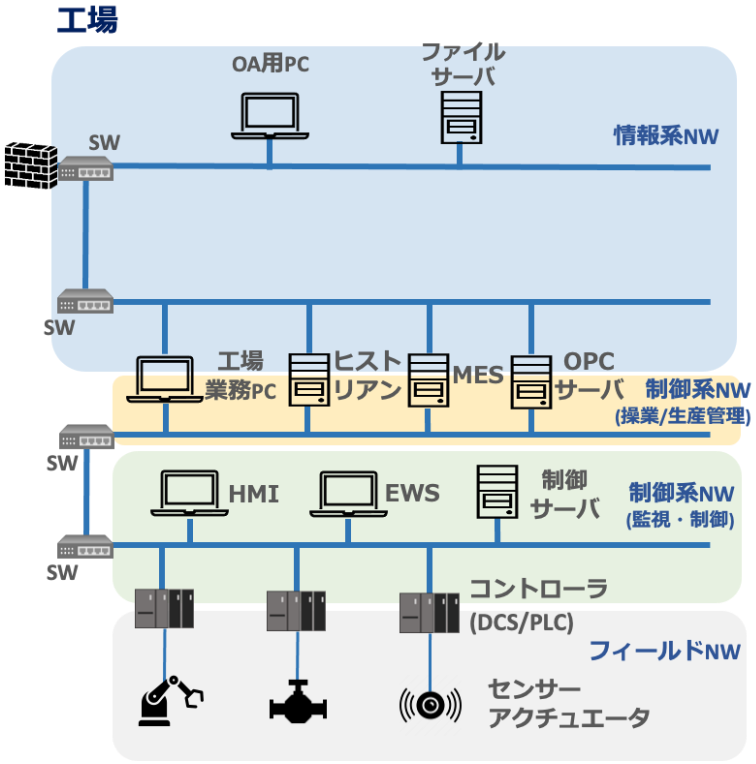
2-1. ネットワーク構成確認

ネットワーク構成は３つのパターンからユーザが選択する。

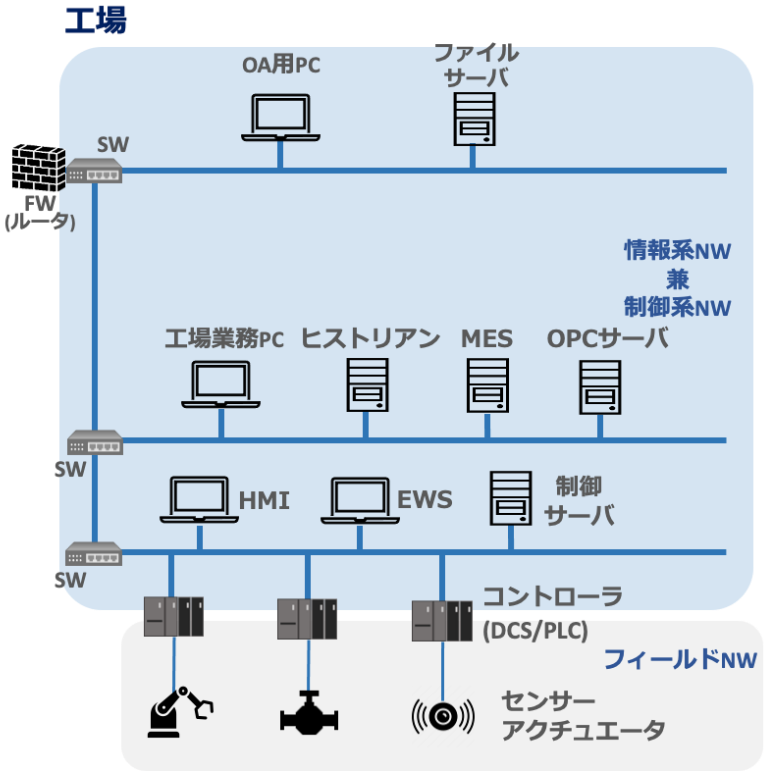
DMZによるIT/OT分離構成



NIC2枚挿しによるIT/OT分離構成



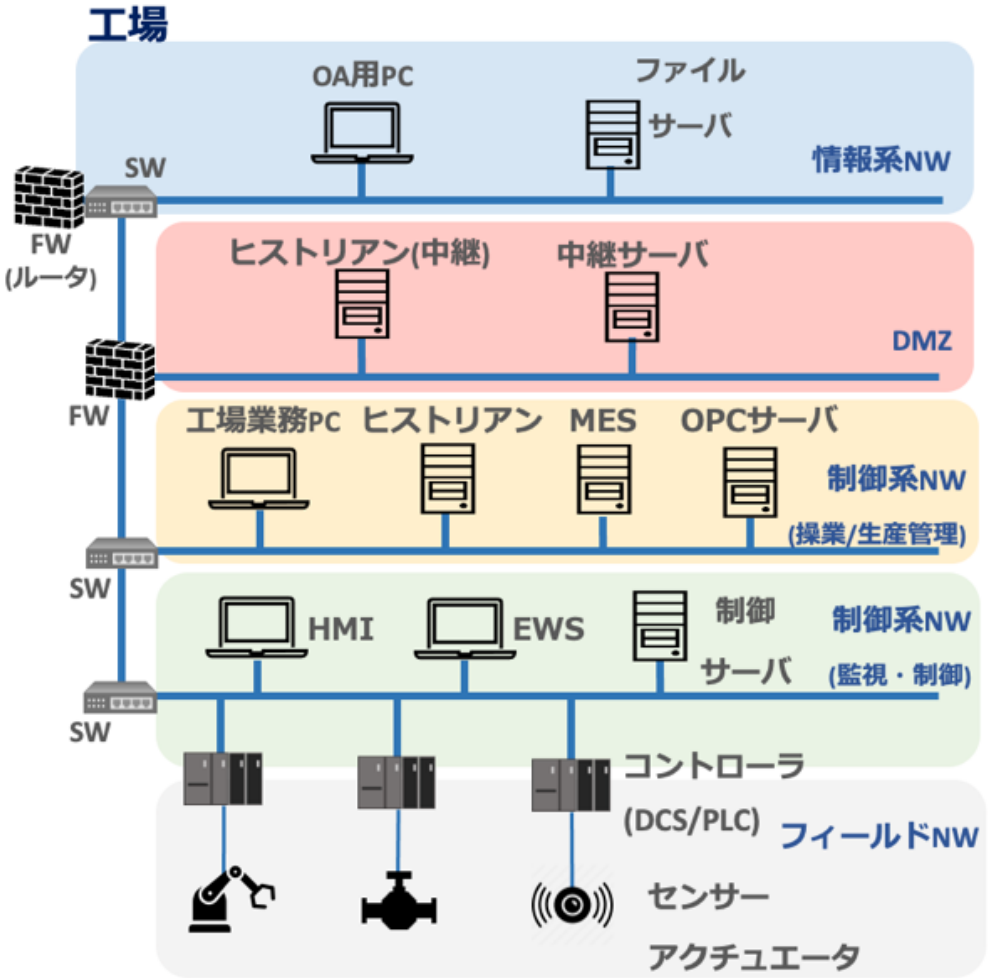
IT/OTがフラット（同一セグメントにIT/OTが混在）



2-1. ネットワーク構成確認

ユーザが選択したネットワーク構成には資産情報は既に設定されている。

DMZによるIT/OT分離構成

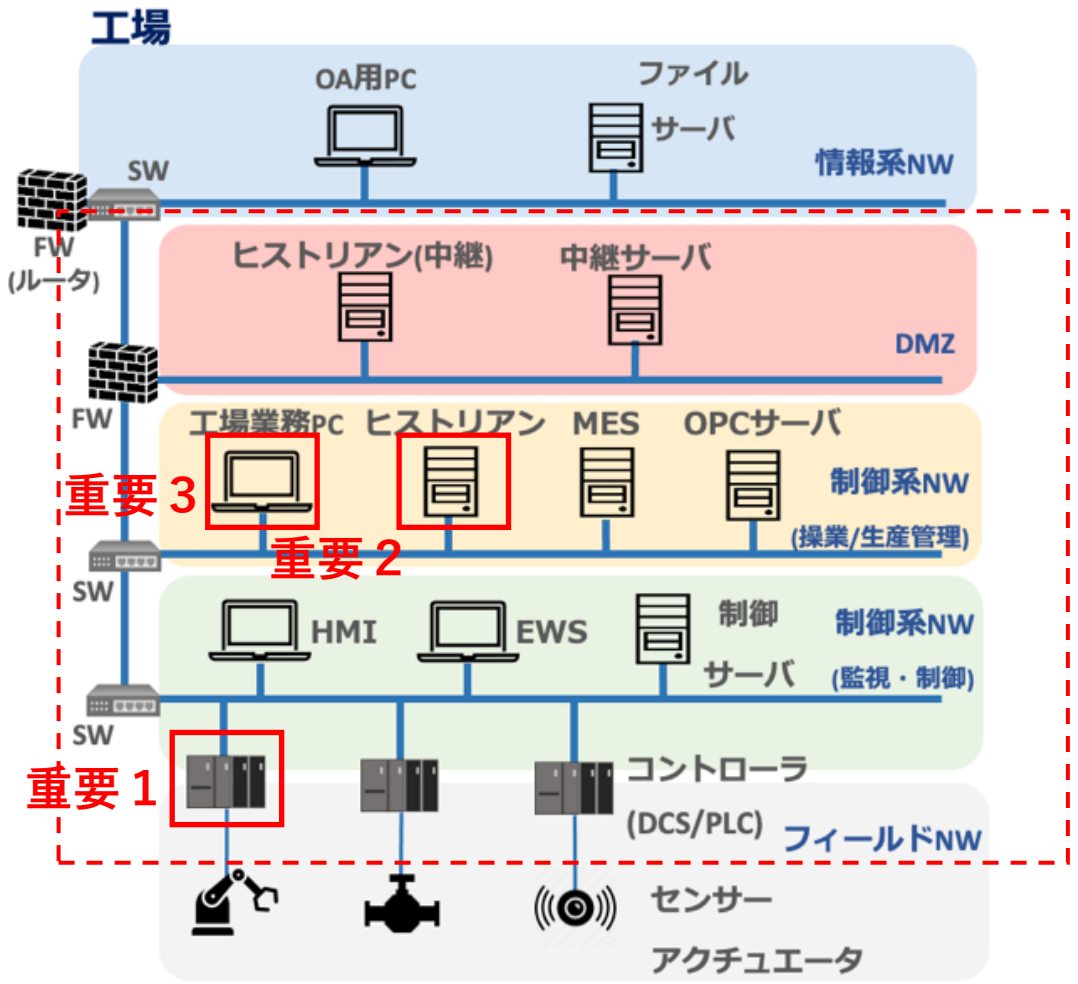


- ネットワーク構成確認

例：DMZによるIT/OT分離構成　が選択される。
次の手順、重要資産設定に進む。

2-2. 重要資産設定

重要資産は制御系NWにある資産8つから3つ。理由は下記2つから1つ選択する。



- 重要資産設定

例：３つの重要資産と理由が選択される。

	重要資産	理由（被害影響）
1	コントローラ	操業停止
2	ヒストリアン	機密情報漏洩
3	工場業務PC	機密情報漏洩

次の手順、侵入口確認に進む。

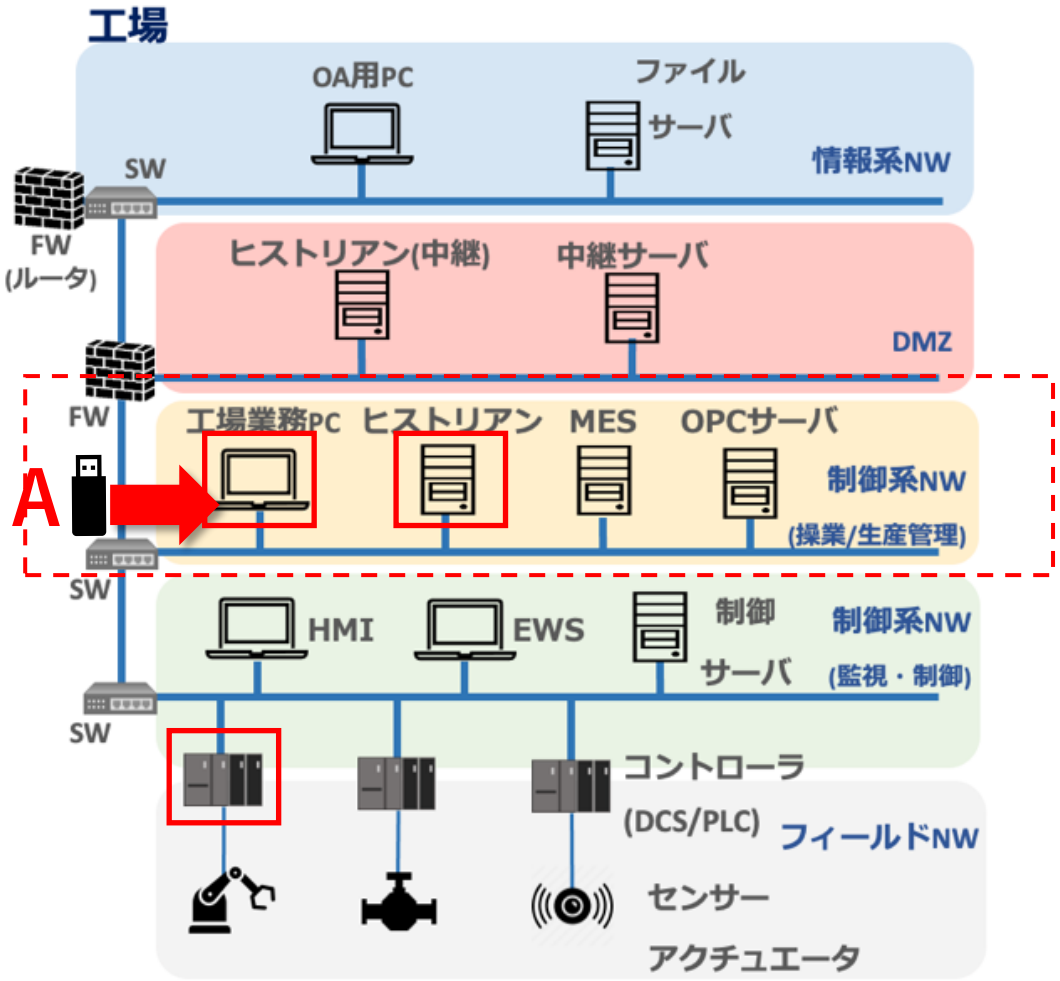
補足：理由となる被害影響の想定

- 制御機能や制御に関わる設定値やプログラムを保有しており、**工場停止や異常動作に影響する**ため。
- 製造・設計に関わる機密情報を保有しており**情報漏洩**に影響するため。

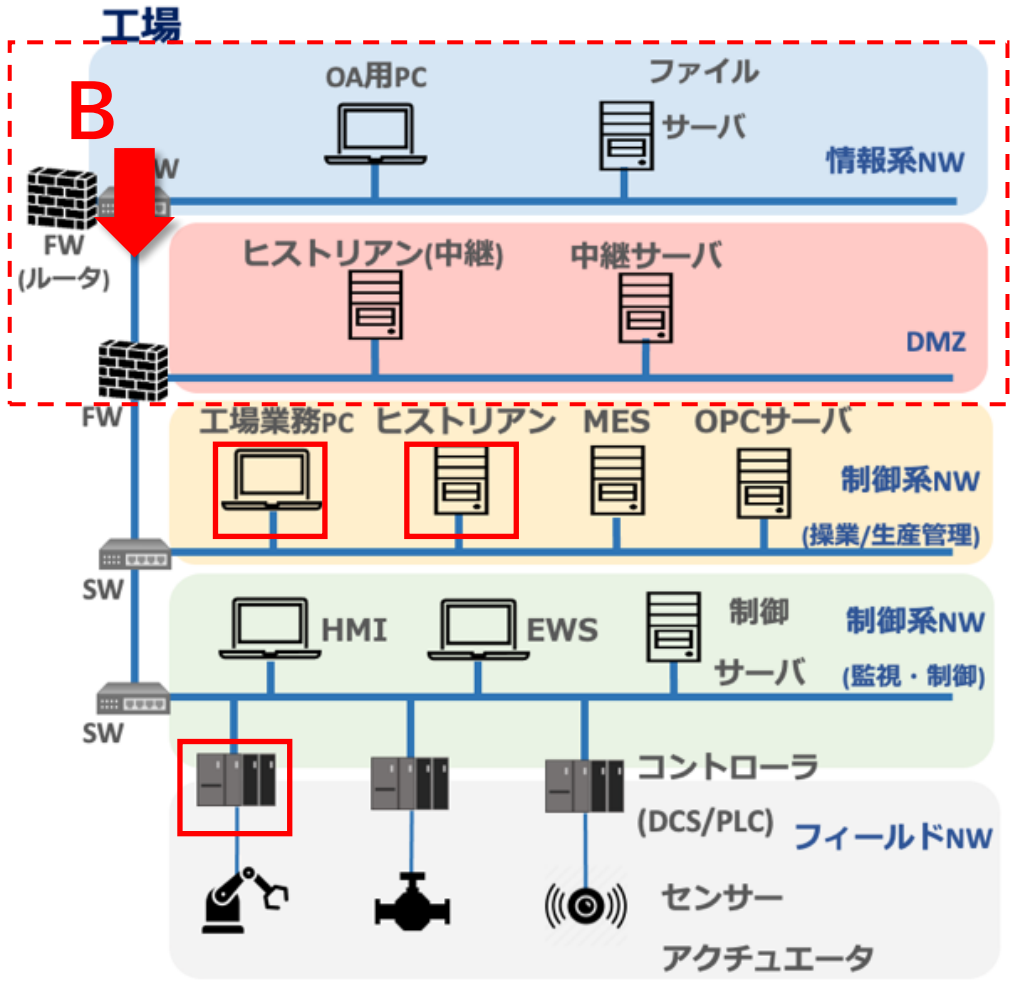
2-3. 侵入口確認

侵入口のパターンは以下２つをガイド側で提示している。

侵入口A　USBメモリからマルウェア感染

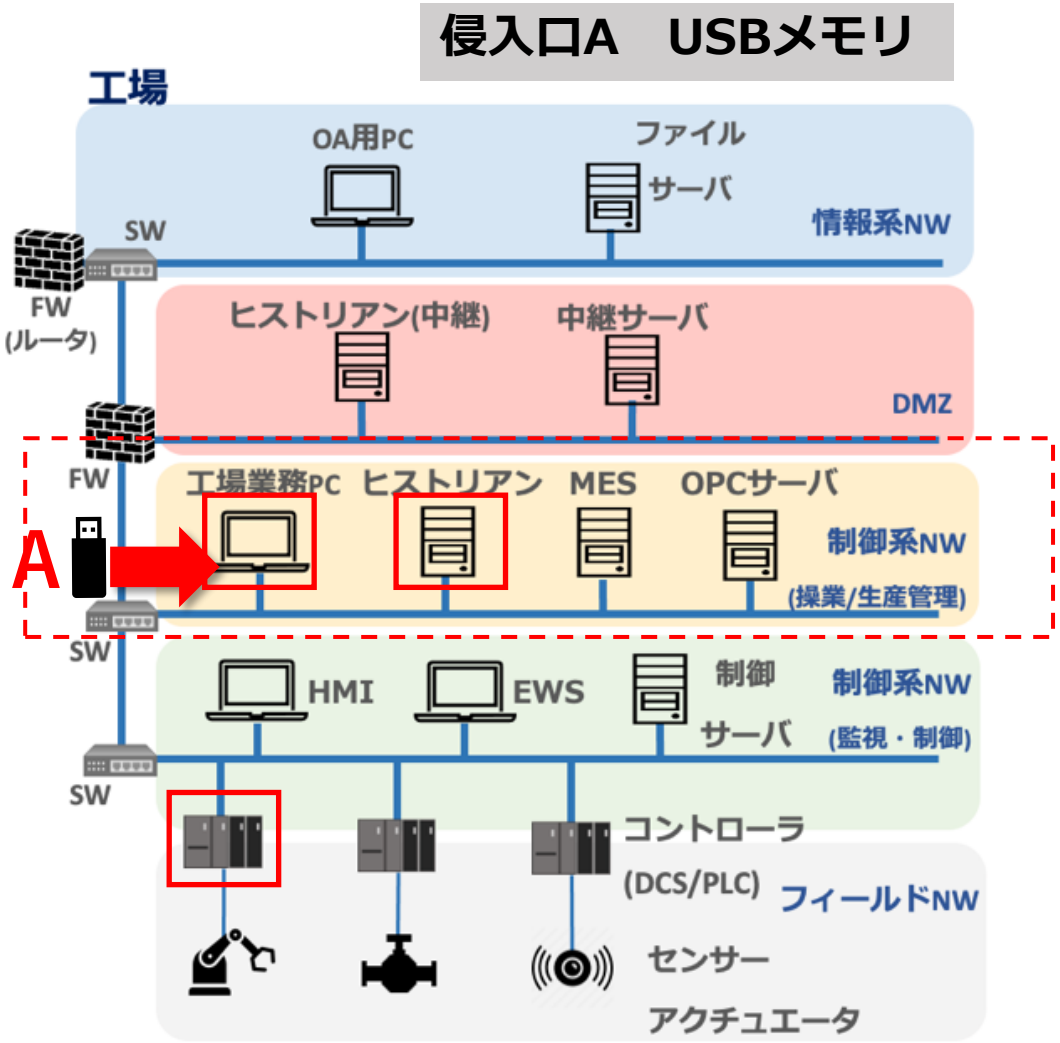


侵入口B　情報ネットワークからマルウェア感染



2-3. 侵入口確認

Aパターンは、重要資産に対してUSBメモリ接続を侵入口とした攻撃シナリオとなる。

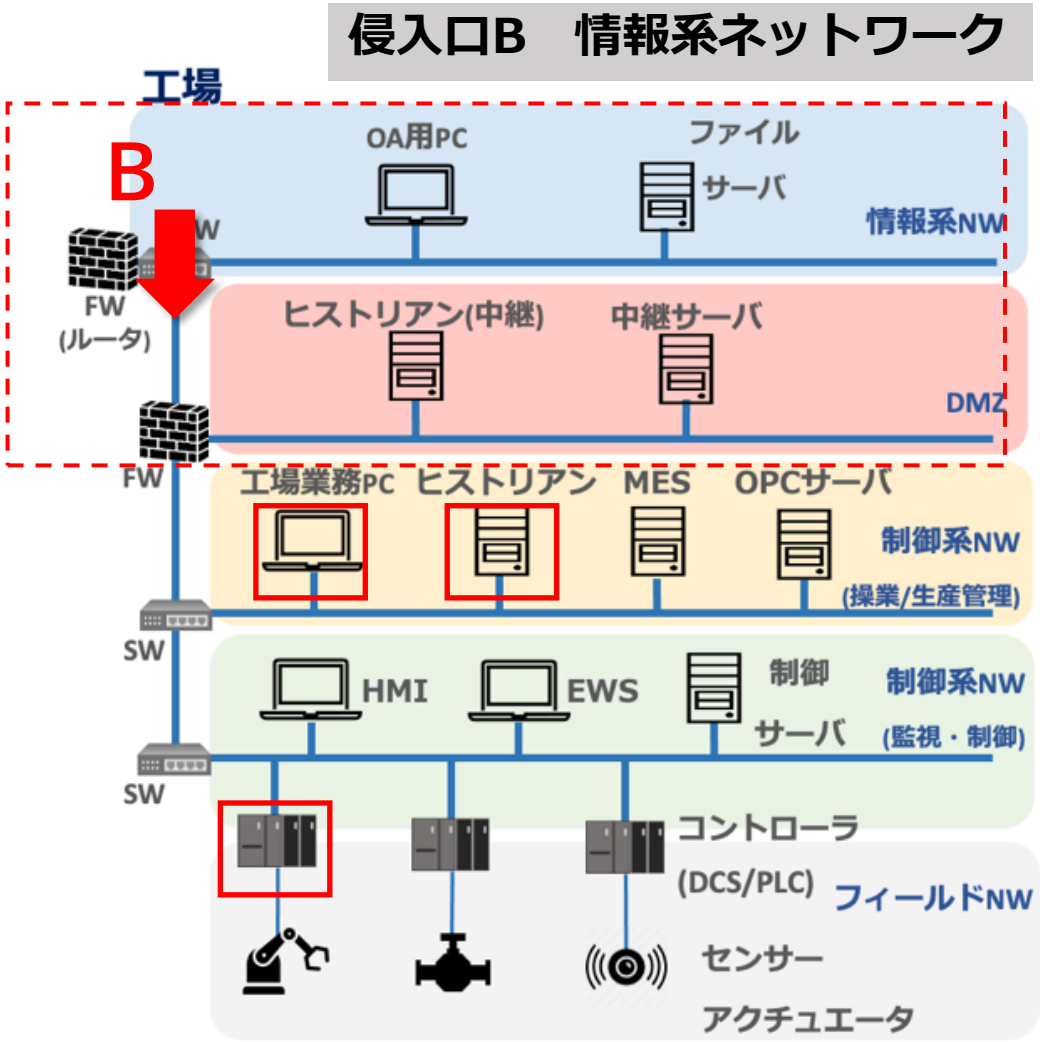


- 侵入口確認

例：USBメモリから工場業務PCに接続される。

2-3. 侵入口確認

Bパターンは、重要資産に対して情報ネットワークを侵入口とした攻撃シナリオとなる。



- 侵入口確認

例：情報系ネットワークから工場業務PCに接続される。

次の手順、攻撃シナリオ確認に進む

2-3. （参考）制御システムの１０大脅威

制御システムの１０大脅威の代表的な２つのパターンである。

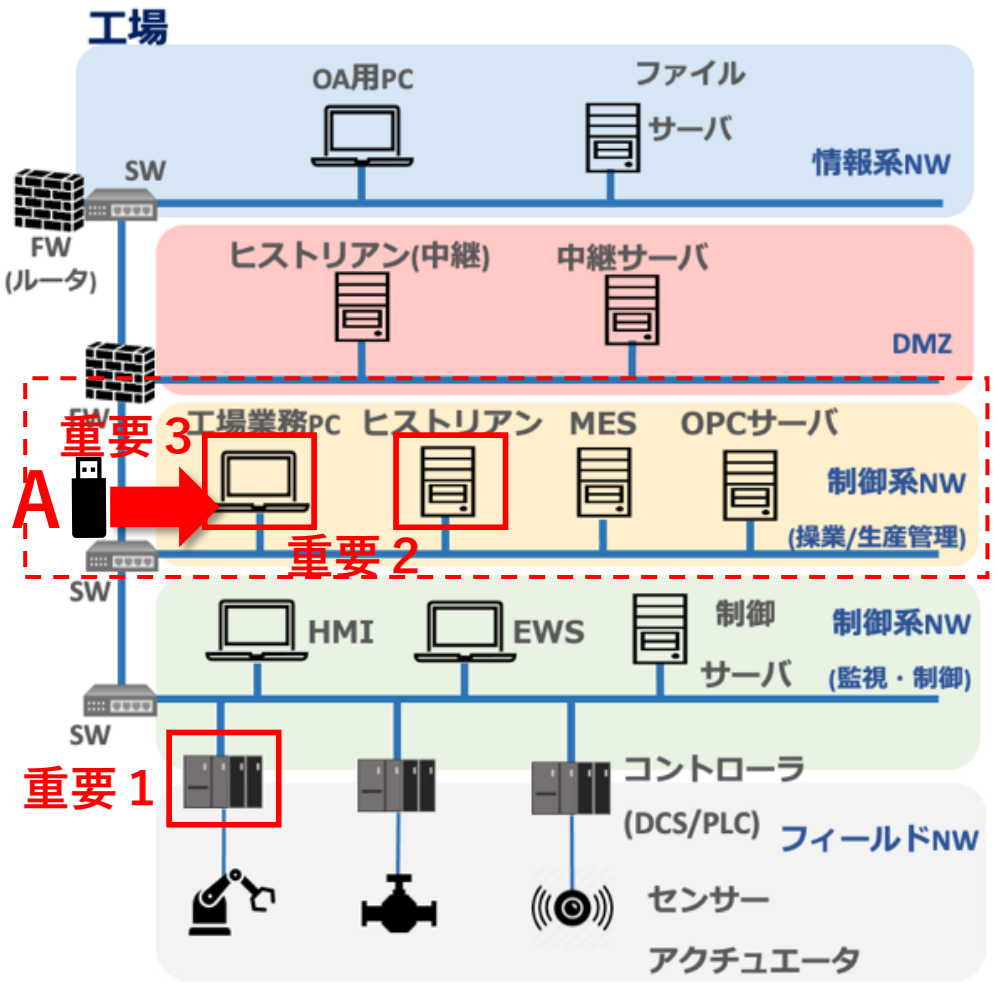
産業用制御システムのセキュリティ 10大脅威（2019年）		2016年
1位	リムーバルメディアや外部機器経由のマルウェア感染	2位
2位	インターネットやイントラネット経由のマルウェア感染	3位
3位	ヒューマンエラーと妨害行為	5位
4位	外部ネットワークやクラウドコンポーネントの攻撃	8位
5位	ソーシャルエンジニアリングとフィッシング	1位
6位	DoS/DDoS攻撃	9位
7位	インターネットに接続された制御機器	6位
8位	リモートアクセスからの侵入	4位
9位	技術的な不具合と不可抗力	7位
10位	スマートデバイスへの攻撃	10位

引用：IPA, 産業用制御システム（ICS）のセキュリティ -10大脅威と対策2019-
https://www.ipa.go.jp/security/controlsystem/bsi2019.html

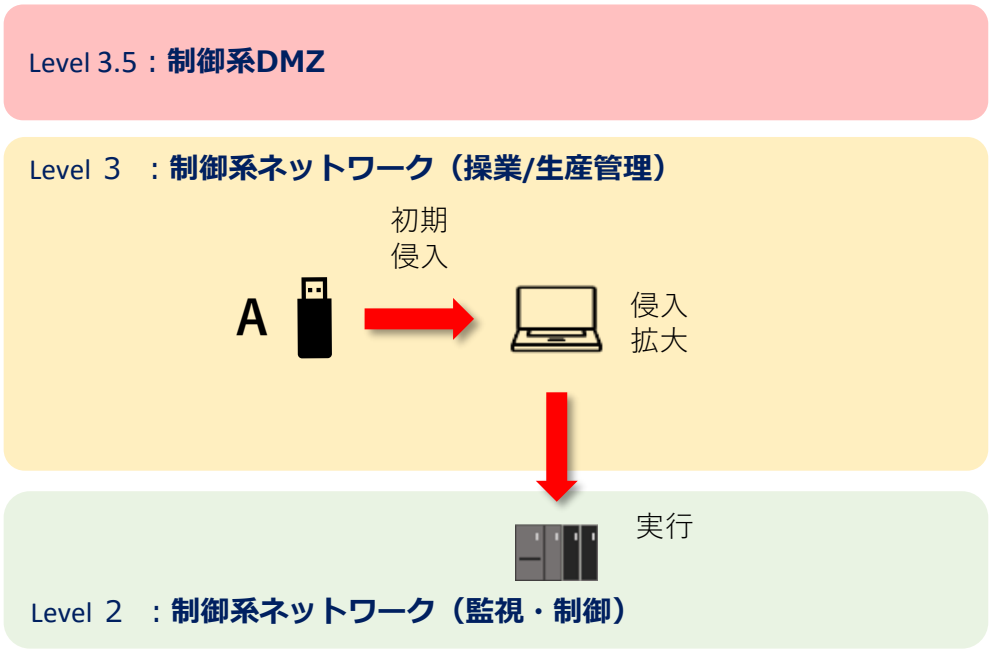
2-4. 攻撃シナリオ確認

設定した重要資産を攻撃対象として各侵入口からの攻撃シナリオを洗い出し、モデル化する。

例：侵入口・・・USBメモリ(Aパターン)
重要資産・・コントローラ、ヒストリアン、工場業務PC

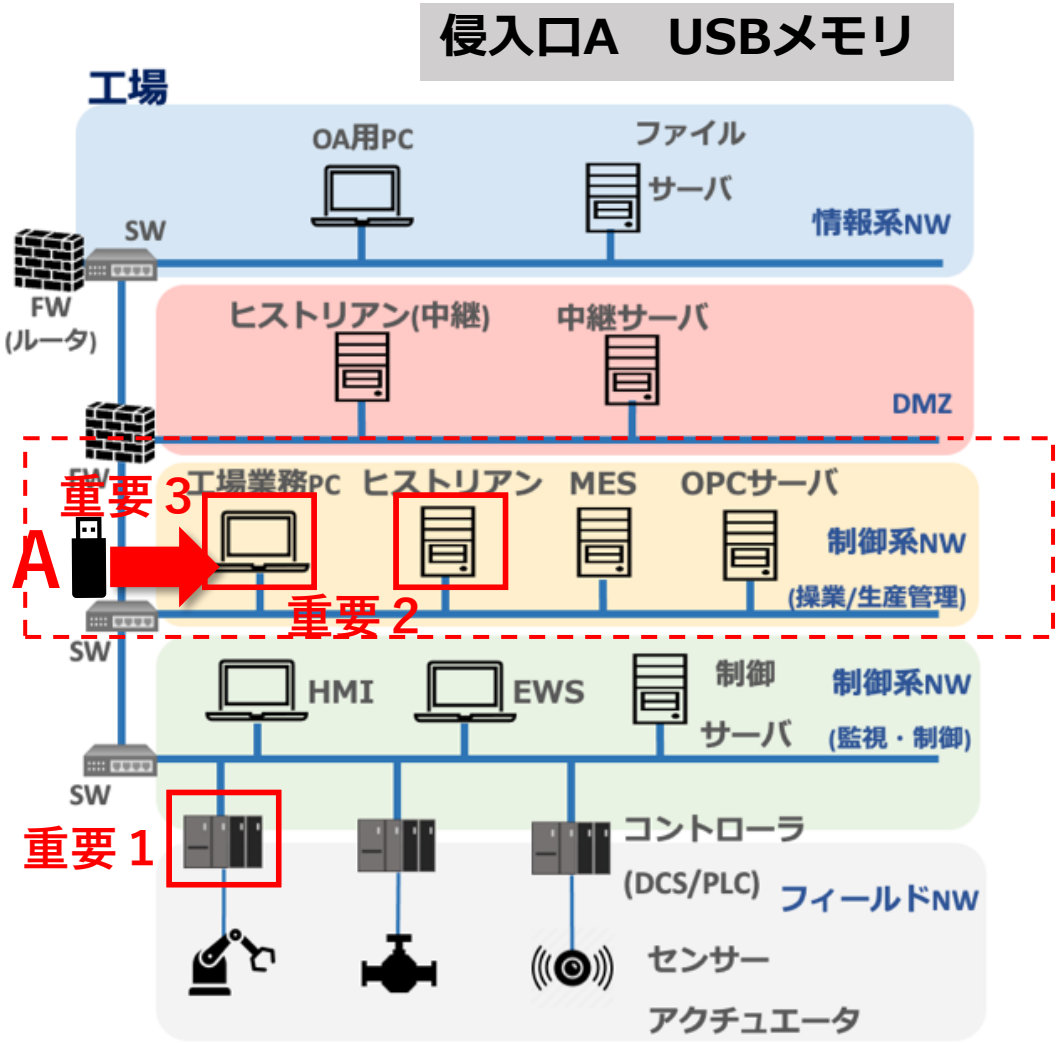


モデル化の例



2-4. 攻撃シナリオ確認

侵入口Aから、設定した重要資産３つに対しての攻撃シナリオを洗い出す。（Aパターン）



- 攻撃シナリオ確認

例：侵入口・・・USBメモリ(A)
　　重要資産・・コントローラ(1),ヒストリアン(2),
　　工場業務PC(3)

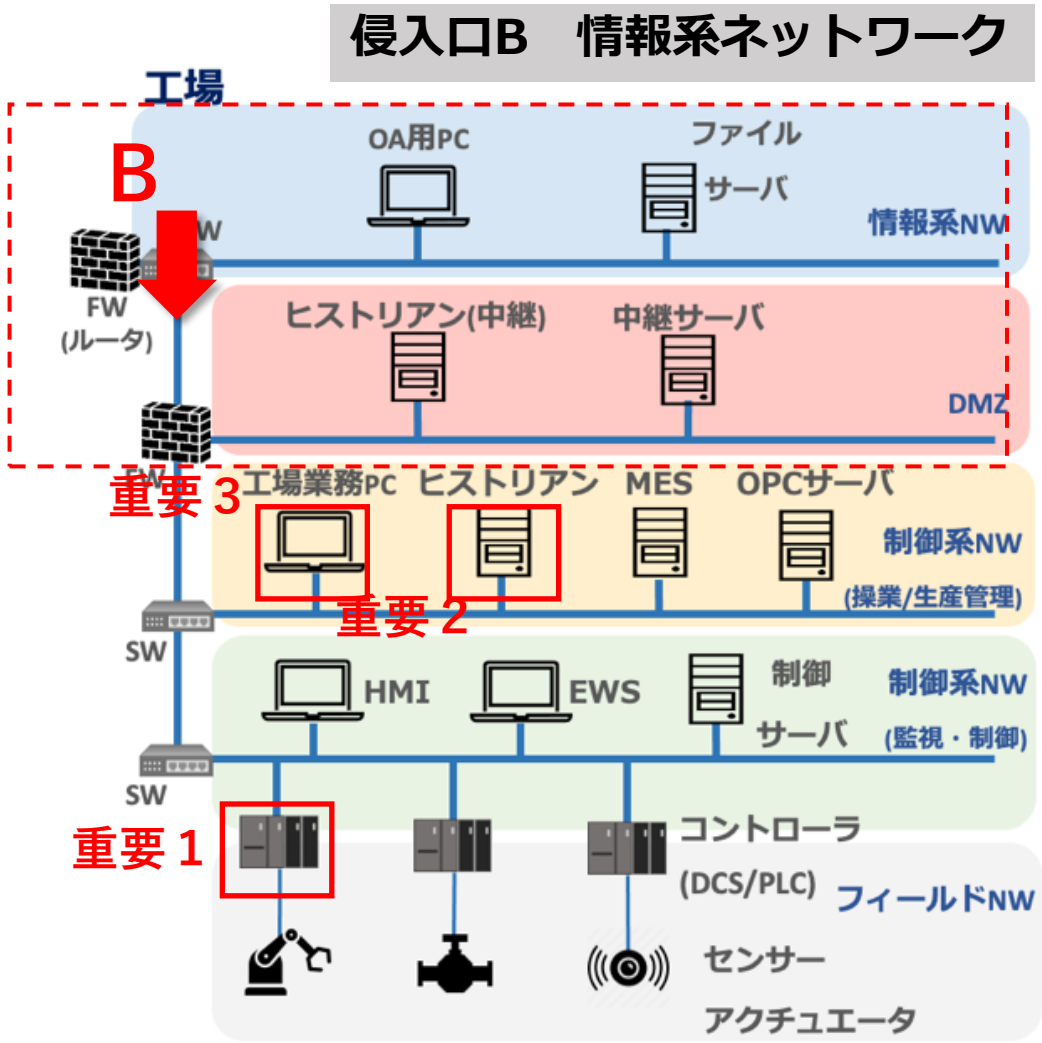
シナリオ

侵入口		重要資産	想定被害
A	→	1	操業停止
A	→	2	機密情報漏洩
A	→	3	機密情報漏洩

次にBパターンも同様にシナリオを設定する。

2-4. 攻撃シナリオ確認

侵入口Bから、設定した重要資産３つに対しての攻撃シナリオを洗い出す。（Bパターン）



- 攻撃シナリオ確認

例：侵入口・・・情報系ネットワーク(B)
　　重要資産・・コントローラ(1),ヒストリアン(2),
　　工場業務PC(3)

シナリオ

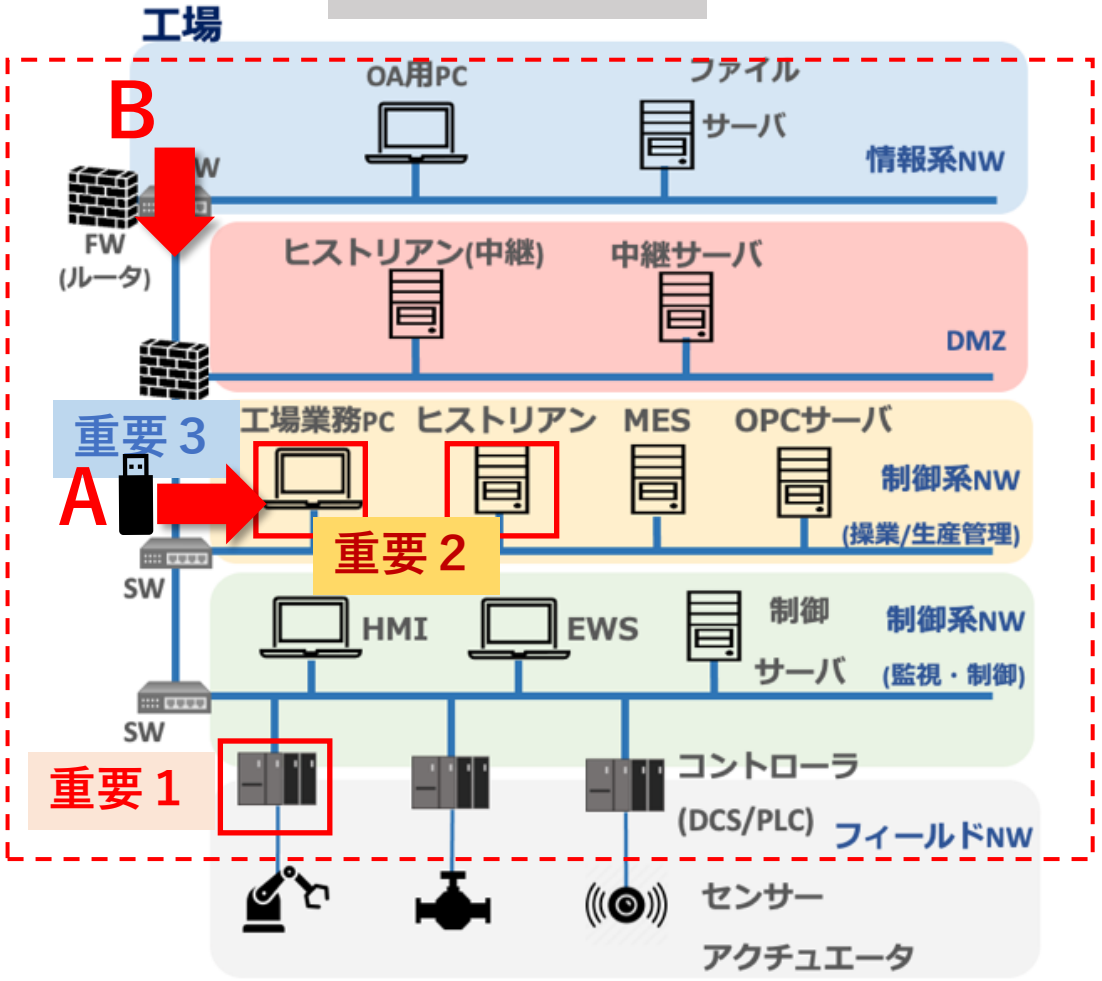
侵入口		重要資産	想定被害
B	→	1	操業停止
B	→	2	機密情報漏洩
B	→	3	機密情報漏洩

次にパターンAとBパターンを合わせて順位付けする。

2-4. 攻撃シナリオ確認

洗い出された６つの攻撃シナリオを資産の重要度で順位付けし、上位２つについてはモデル化する。

６シナリオ設定



- 攻撃シナリオ確認

例：侵入口・・・USBメモリ(A),情報系ネットワーク(B)
重要資産・・コントローラ(1),ヒストリアン(2),
工場業務PC(3)

シナリオ

侵入口		重要資産	想定被害	
A	→	1	操業停止	モデル化する
B	→	1	操業停止	モデル化する
A	→	2	機密情報漏洩	
B	→	2	機密情報漏洩	
A	→	3	機密情報漏洩	
B	→	3	機密情報漏洩	

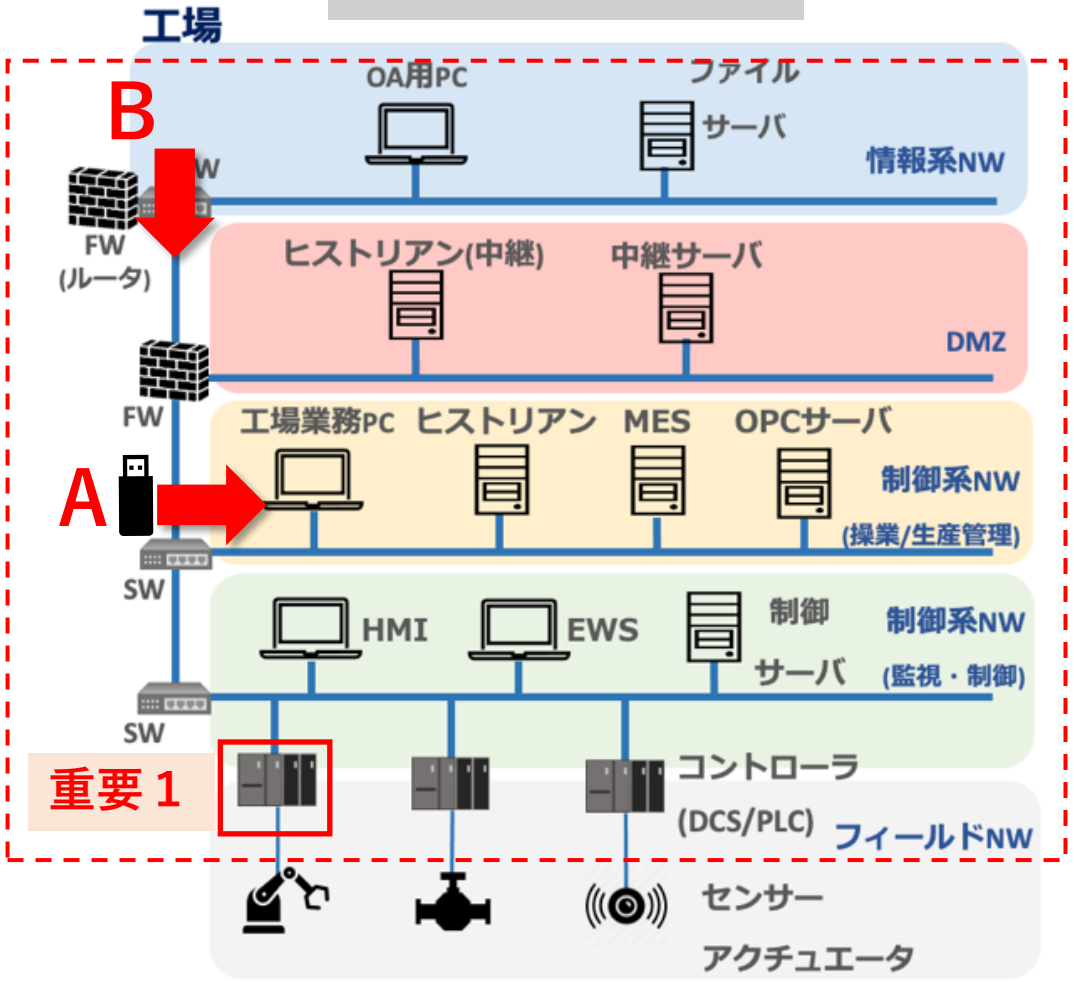
次に上位２シナリオをモデル化する。

※その他の攻撃シナリオのモデル図は別紙１「モデル図一覧」を参照。

2-4. 攻撃シナリオ確認

順位付けした上位２シナリオを攻撃段階にモデル化してリスク分析する。

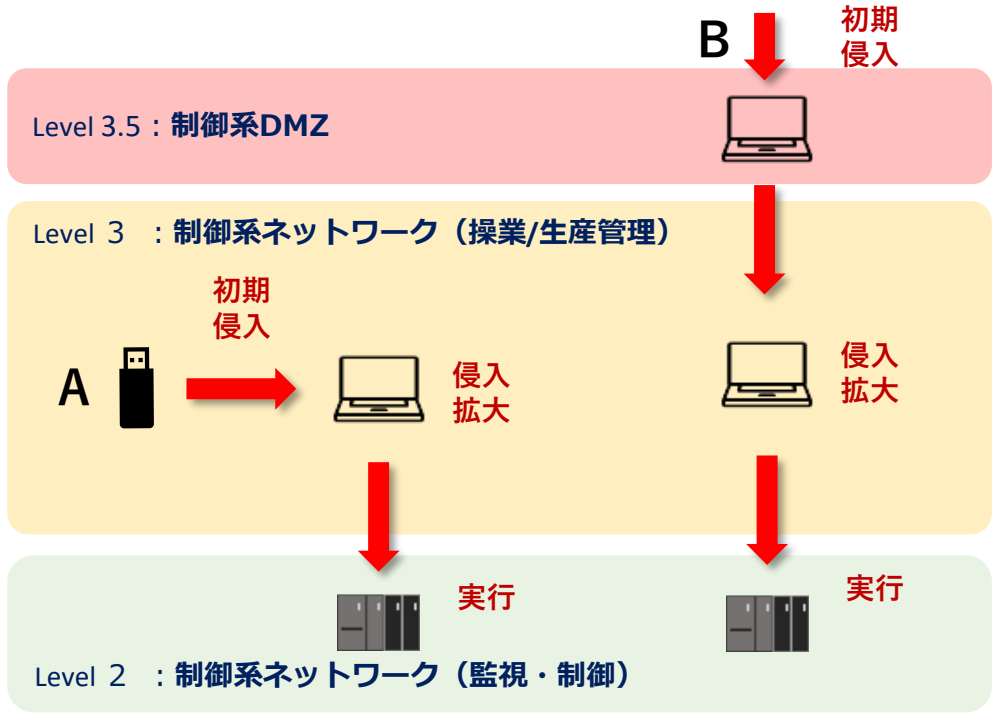
上位２シナリオ設定



- 攻撃シナリオ確認

シナリオ別に「初期侵入・侵入拡大・実行」の３段階にモデル化してリスク分析する。

次の手順、対策案を提示して確認する。



2-4. 攻撃シナリオ確認(補足)　例：侵入口A～操業停止

攻撃段階	サイバーキルチェーン
初期侵入	不正なUSBを工場業務PCに接続する。 外部保守PCを制御系ネットワークに接続する。
	工場業務PCにマルウェアが感染する。
侵入拡大	マルウェアが外部の攻撃者サーバと通信確立する。
	攻撃者が内部のネットワークを探索し情報収集する。
	発見したサーバや端末にマルウェアが感染拡大する。
	サーバや端末からコントローラの通信経路を確立する。
実行	コントローラのサービス妨害を実行する。 コントローラのプログラムや通信の改ざんを実行する。
	制御不具合により操業停止となる。　被害想定

USB/外部PCから侵入

工場業務PC　侵入口 A

↓

ヒストリアン
MES
制御サーバ
EWS
HMI

↓

コントローラ（PLC/DCS）　重要資産 1

2-4. 攻撃シナリオ確認(補足)　例：侵入口B～操業停止

攻撃段階	サイバーキルチェーン
初期侵入	オフィスPCで不審メールの添付ファイルを開く
	オフィスPCにマルウェアが感染する
侵入拡大	マルウェアが外部の攻撃者サーバと通信確立する。
	攻撃者が内部のネットワークを探索し情報収集する。
	発見したサーバや端末にマルウェアが感染拡大する。
	サーバや端末からコントローラの通信経路を確立する。
実行	コントローラのサービス妨害を実行する。 コントローラのプログラムや通信の改ざんを実行する。
	制御不具合により操業停止となる。　被害想定

情報系から侵入

オフィスPC　侵入口 B

↓

ヒストリアン中継
ヒストリアン
MES
制御サーバ
EWS
HMI

↓

コントローラ（PLC/DCS）　重要資産 1

2-4. 攻撃シナリオ確認(補足)　例：侵入口A～情報漏洩

攻撃段階	サイバーキルチェーン
初期侵入	不正なUSBを工場業務PCに接続する。
	外部保守PCを制御系ネットワークに接続する。
	工場業務PCにマルウェアが感染する。
侵入拡大	マルウェアが外部の攻撃者サーバと通信確立する。
	攻撃者が内部のネットワークを探索し情報収集する。
	発見したサーバや端末にマルウェアが感染拡大する。
	サーバや端末から機密情報を保持する機器に接続する。
実行	機密情報データの窃取や破壊を実行する。
	機密情報データが社外に漏えいする。

被害想定

USB/外部PCから侵入

工場業務PC

侵入口 A

ヒストリアン

MES

制御サーバ

EWS

HMI

MES

重要資産 1

2-4. 攻撃シナリオ確認(補足)　例：侵入口B～情報漏洩

攻撃段階	サイバーキルチェーン
初期侵入	オフィスPCで不審メールの添付ファイルを開く
	オフィスPCにマルウェアが感染する
侵入拡大	マルウェアが外部の攻撃者サーバと通信確立する。
	攻撃者が内部のネットワークを探索し情報収集する。
	発見したサーバや端末にマルウェアが感染拡大する。
	サーバや端末から機密情報を保持する機器に接続する。
実行	機密情報データの窃取や破壊を実行する。
	機密情報データが社外に漏えいする。 被害想定

情報系から侵入

オフィスPC

侵入口 B

↓

ヒストリアン中継

ヒストリアン

MES

制御サーバ

EWS

HMI

↓

MES

重要資産 1

2-5. 対策一覧確認

モデル化したシナリオ２つの対策案を提示する。シナリオ１の優先順位付けする基本の対策とする。

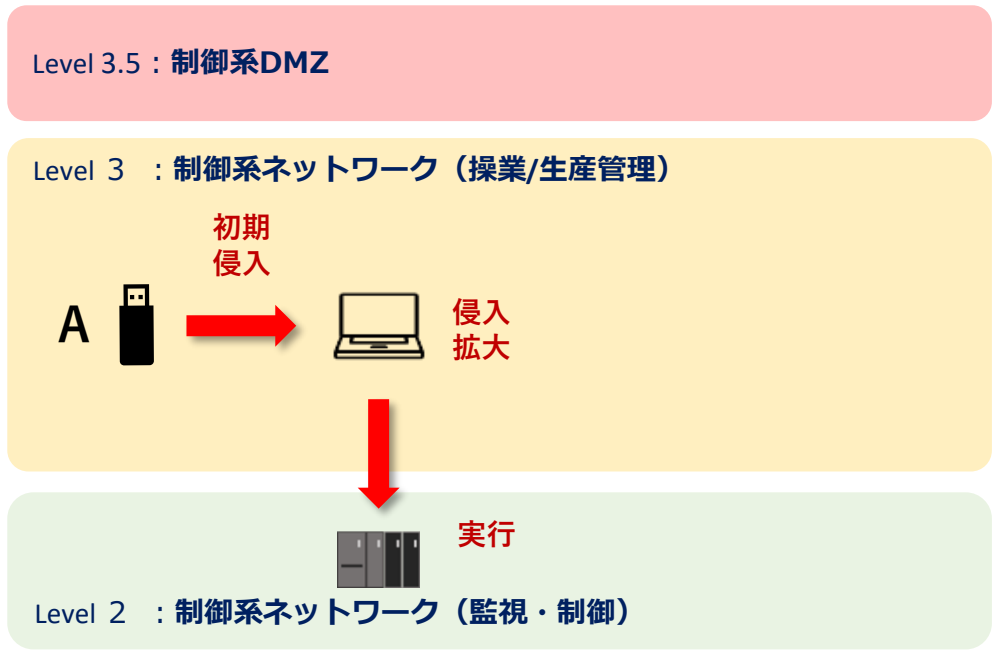
シナリオ１

攻撃段階	対策案
初期侵入	USBポートの物理ブロック
	デバイス接続制限の設定
	アンチウイルスソフトによる検知、駆除
侵入拡大	ホワイトリスト型のプロセス起動制限
	IDS(制御系)による不正通信検知
	不正通信検知後の対応手順作成と定期訓練
	FWによるセグメント分割
	複雑なパスワードの設定
	通信の暗号化
実行	インシデント対応手順の作成と定期訓練
	操業の復旧手順の作成と定期訓練
	ログ収集
	データバックアップ

対策一覧確認

シナリオ：侵入口　重要資産　想定被害
A　→　1　操業停止

シナリオ２も同様にモデル化する。



2-5. 対策一覧確認　詳細

シナリオ１

攻撃段階	対策案	対策導入箇所
初期侵入	USBポートの物理ブロック	制御系ネットワーク内のサーバや端末
	デバイス接続制限の設定	制御系ネットワーク内のサーバや端末
	アンチウイルスソフトによる検知、駆除	制御系ネットワーク内のサーバや端末
侵入拡大	ホワイトリスト型のプロセス起動制限	制御系ネットワーク内のサーバや端末
	IDS(制御系)による不正通信検知	制御系ネットワーク
	不正通信検知後の対応手順作成と定期訓練	制御系ネットワーク
	FWによるセグメント分割	制御系ネットワーク
	複雑なパスワードの設定	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器
	通信の暗号化	制御系ネットワーク内
実行	インシデント対応手順の作成と定期訓練	ー
	操業の復旧手順の作成と定期訓練	ー
	ログ収集	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器
	データバックアップ	制御系ネットワーク内のサーバや端末

2-5. 対策一覧確認

モデル化したシナリオ２つの対策案を提示する。シナリオ２の優先順位付けする基本の対策とする。

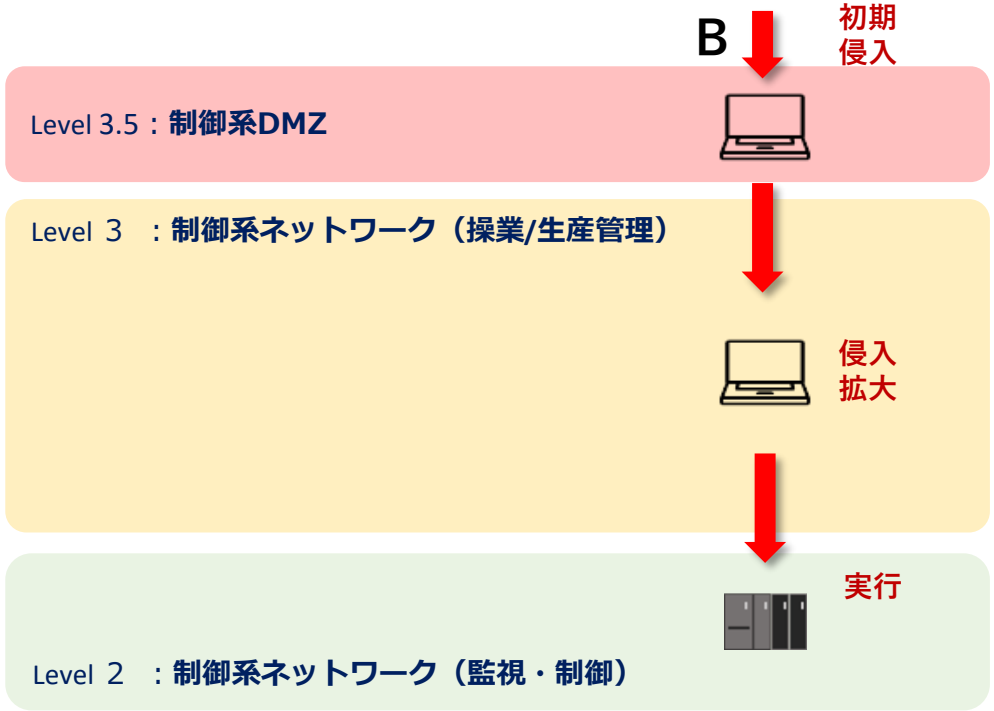
シナリオ２

攻撃段階	対策案
初期侵入	標的型メール訓練の定期実施
	OSやアプリケーションのバージョン最新化
	アンチウイルスソフトによる検知、駆除
侵入拡大	IDS(情報系)による不正通信検知
	FWやIPSによるIT/OT分離（制御系DMZ設置）
	IDS(IT/OT境界)による不正通信検知
	不正通信検知後の対応手順作成と定期訓練
	ホワイトリスト型のプロセス起動制限
	IDS(制御系)による不正通信検知
	不正通信検知後の対応手順作成と定期訓練
	FWによるセグメント分割
	複雑なパスワードの設定
	通信の暗号化
実行	インシデント対応手順の作成と定期訓練
	操業の復旧手順の作成と定期訓練
	ログ収集
	データバックアップ

対策一覧確認

シナリオ：侵入口　重要資産　想定被害
B　→　1　操業停止

セキュリティ診断の手順１から５まで完了した。
次のステップ優先順位付けに進む。



2-5. 対策一覧確認　詳細

シナリオ２

攻撃段階	対策案	対策導入箇所
初期侵入	標的型メール訓練の定期実施	OA用PC
	OSやアプリケーションのバージョン最新化	OA用PC
	アンチウイルスソフトによる検知、駆除	OA用PC
侵入拡大	IDS(情報系)による不正通信検知	情報系ネットワーク
	FWやIPSによるIT/OT分離（制御系DMZ設置）	情報系ネットワークと制御系ネットワークの境界
	IDS(IT/OT境界)による不正通信検知	情報系ネットワークと制御系ネットワークの境界
	不正通信検知後の対応手順作成と定期訓練	情報系ネットワークと制御系ネットワークの境界
	ホワイトリスト型のプロセス起動制限	制御系ネットワーク内のサーバや端末
	IDS(制御系)による不正通信検知	制御系ネットワーク
	不正通信検知後の対応手順作成と定期訓練	制御系ネットワーク
	FWによるセグメント分割	制御系ネットワーク
	複雑なパスワードの設定	制御系ネットワーク内のサーバや端末、 NW機器、セキュリティ機器
	通信の暗号化	制御系ネットワーク内
実行	インシデント対応手順の作成と定期訓練	ー
	操業の復旧手順の作成と定期訓練	ー
	ログ収集	制御系ネットワーク内のサーバや端末、 NW機器、セキュリティ機器
	データバックアップ	制御系ネットワーク内のサーバや端末

2-5. 対策一覧確認(補足)　例：侵入口A～操業停止

攻撃段階	サイバーキルチェーン	対策案
初期侵入	不正なUSBを工場業務PCに接続する。	USBポートの物理ブロック
	工場業務PCにマルウェアが感染する。	デバイスの接続制限を設定
		アンチウイルスによる検知、駆除
侵入拡大	マルウェアが外部の攻撃者サーバと通信確立する。	ホワイトリスト型のプロセス起動制限
	攻撃者が内部のネットワークを探索し情報収集する。	IDSで不正通信を検知
	発見したサーバや端末にマルウェアが感染拡大する。	検知後の対応手順作成と定期訓練
	サーバや端末からコントローラの通信経路を確立する。	FWでセグメント分割
		複雑なパスワードの設定
実行	コントローラのサービス妨害を実行する。 コントローラのプログラムや通信の改ざんを実行する。	インシデント対応手順の作成と定期訓練
		操業復旧手順の作成と定期訓練
	制御不具合により操業停止となる。	ログ収集機能の追加
	被害想定	データバックアップ定期実施

2-5. 対策一覧確認(補足)　例：侵入口B～操業停止

攻撃段階	サイバーキルチェーン		対策案
初期侵入	オフィスPCで不審メールの添付ファイルを開く		標的型メール訓練の定期実施
	オフィスPCにマルウェアが感染する		OAやアプリのバージョン最新化
			アンチウイルスによる検知、駆除
侵入拡大	マルウェアが外部の攻撃者サーバと通信確立する。		IDSで不正通信を検知（情報系）
	攻撃者が内部のネットワークを探索し情報収集する。		FWやIPSにて情報系・制御系の分離(制御系DMZ設置含む)
	発見したサーバや端末にマルウェアが感染拡大する。		IDSで不正通信を検知（制御系）
	サーバや端末からコントローラの通信経路を確立する。		検知後の対応手順作成と定期訓練
			複雑なパスワードの設定
実行	コントローラのサービス妨害を実行する。 コントローラのプログラムや通信の改ざんを実行する。		インシデント対応手順の作成と定期訓練
	制御不具合により操業停止となる。	被害想定	操業復旧手順の作成と定期訓練
			ログ収集機能の追加
			データバックアップ定期実施

2-5. 対策一覧確認(補足)　例：侵入口A～情報漏洩

攻撃段階	サイバーキルチェーン		対策案
初期侵入	不正なUSBを工場業務PCに接続する。		USBポートの物理ブロック
	工場業務PCにマルウェアが感染する。		デバイスの接続制限を設定
			アンチウイルスによる検知、駆除
侵入拡大	マルウェアが外部の攻撃者サーバと通信確立する。		ホワイトリスト型のプロセス起動制限
	攻撃者が内部のネットワークを探索し情報収集する。		IDSで不正通信を検知
	発見したサーバや端末にマルウェアが感染拡大する。		検知後の対応手順作成と定期訓練
	サーバや端末から機密情報を保持する機器に接続する。		FWでセグメント分割
			複雑なパスワードの設定
			機密データの暗号化
実行	機密情報データの窃取や破壊を実行する。		インシデント対応手順の作成と定期訓練
	機密情報データが社外に漏えいする。	被害想定	ログ収集機能の追加
			データバックアップ定期実施

2-5. 対策一覧確認(補足)　例：侵入口B～情報漏洩

攻撃段階	サイバーキルチェーン	対策案
初期侵入	オフィスPCで不審メールの添付ファイルを開く	標的型メール訓練の定期実施
	オフィスPCにマルウェアが感染する	OAやアプリのバージョン最新化
		アンチウイルスによる検知、駆除
侵入拡大	マルウェアが外部の攻撃者サーバと通信確立する。	IDSで不正通信を検知（情報系）
	攻撃者が内部のネットワークを探索し情報収集する。	FWやIPSにて情報系・制御系の分離(制御系DMZ設置含む)
	発見したサーバや端末にマルウェアが感染拡大する。	IDSで不正通信を検知（制御系）
	サーバや端末から機密情報を保持する機器に接続する。	検知後の対応手順作成と定期訓練
		複雑なパスワードの設定
		機密データの暗号化
実行	機密情報データの窃取や破壊を実行する。	インシデント対応手順の作成と定期訓練
	機密情報データが社外に漏えいする。 被害想定	ログ収集機能の追加
		データバックアップ定期実施

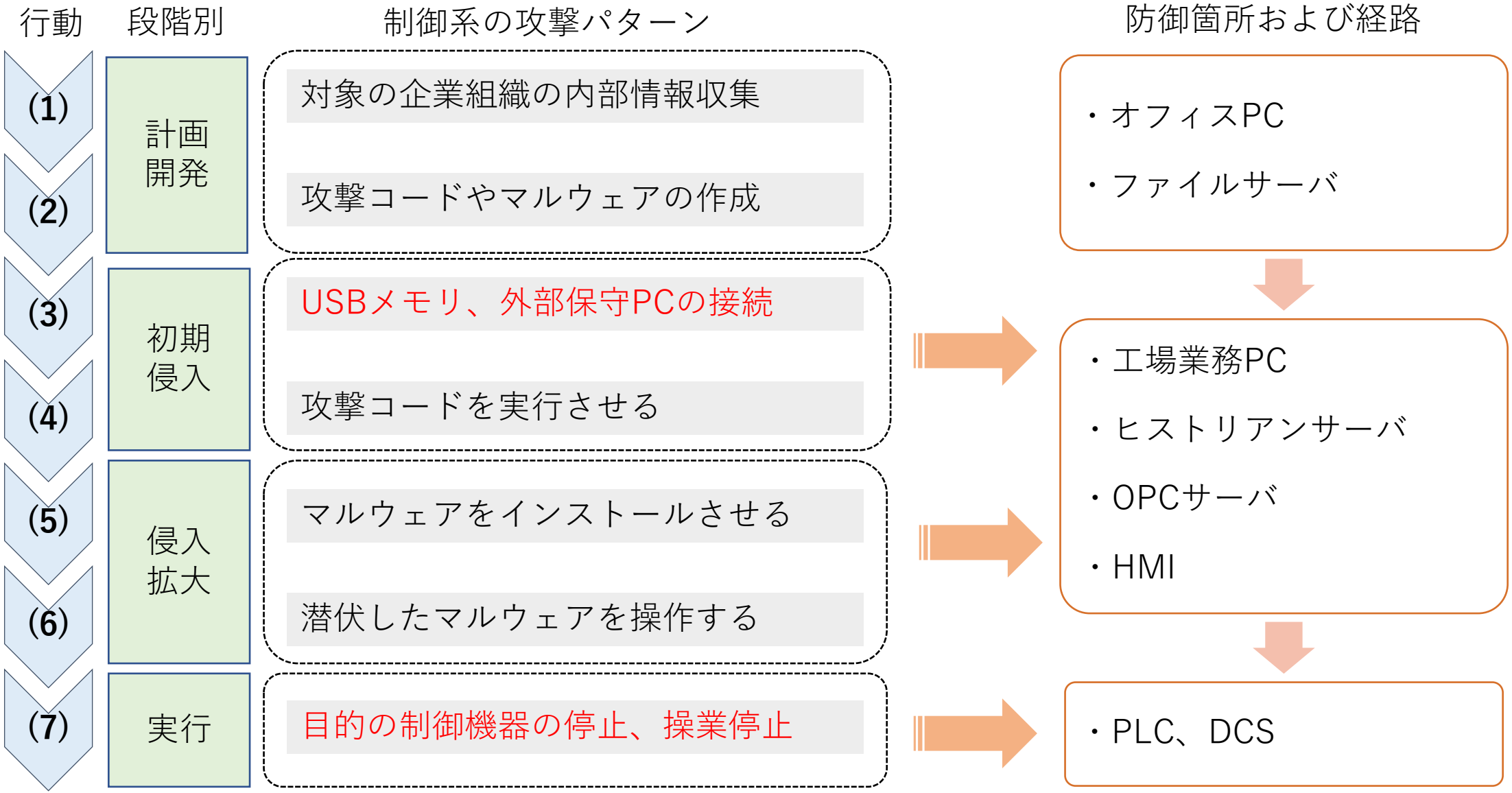
（参考）キルチェーンと攻撃シナリオ

攻撃者の行動を７つに分類したキルチェーンに対して、制御系の侵入経路を適用

攻撃者の行動分類	一般的なパターン（情報系資産）	制御系のパターン
(1) ・偵察	対象の企業組織の内部情報収集	対象の企業組織の内部情報収集
(2) ・武器化	攻撃コードやマルウェアの作成	攻撃コードやマルウェアの作成
(3) ・配送	標的型メールで攻撃サイトへ誘導	USBメモリや外付けディスクの接続
(4) ・攻撃	攻撃コードを実行させる	攻撃コードを実行させる
(5) ・インストール	マルウェアをインストールさせる	マルウェアをインストールさせる
(6) ・リモート操作	潜伏したマルウェアを操作する	潜伏したマルウェアを操作する
(7) ・目的の実行	目的のデータを盗む、破壊する	目的の制御機器の停止、操業停止

（参考）攻撃シナリオ　USB侵入＋操業停止

７つの行動に対して段階別に防御する箇所と経路を適用する。



（参考）攻撃シナリオ　情報NW侵入＋情報漏洩

７つの行動に対して段階別に防御する箇所と経路を適用する。

行動	段階別	制御系の攻撃パターン	防御箇所および経路
(1)	計画開発	対象の企業組織の内部情報収集	・オフィスPC ・ファイルサーバ
(2)		攻撃コードやマルウェアの作成	
(3)	初期侵入	オフィスPCから工場業務PCに侵入	・工場業務PC ・ヒストリアンサーバ ・OPCサーバ ・HMI
(4)		攻撃コードを実行させる	
(5)	侵入拡大	マルウェアをインストールさせる	
(6)		潜伏したマルウェアを操作する	
(7)	実行	機密情報やデータを盗む、破壊する	・ヒストリアンサーバ ・MES

3.導入すべき対策の優先順位付け

3. 導入すべき対策の優先順位付け

ガイドが提示する攻撃の発生可能性による対策の基本優先順位付けから、企業のセキュリティ戦略を反映するステップにより優先順位を決定する。

導入すべき対策の優先順位付け

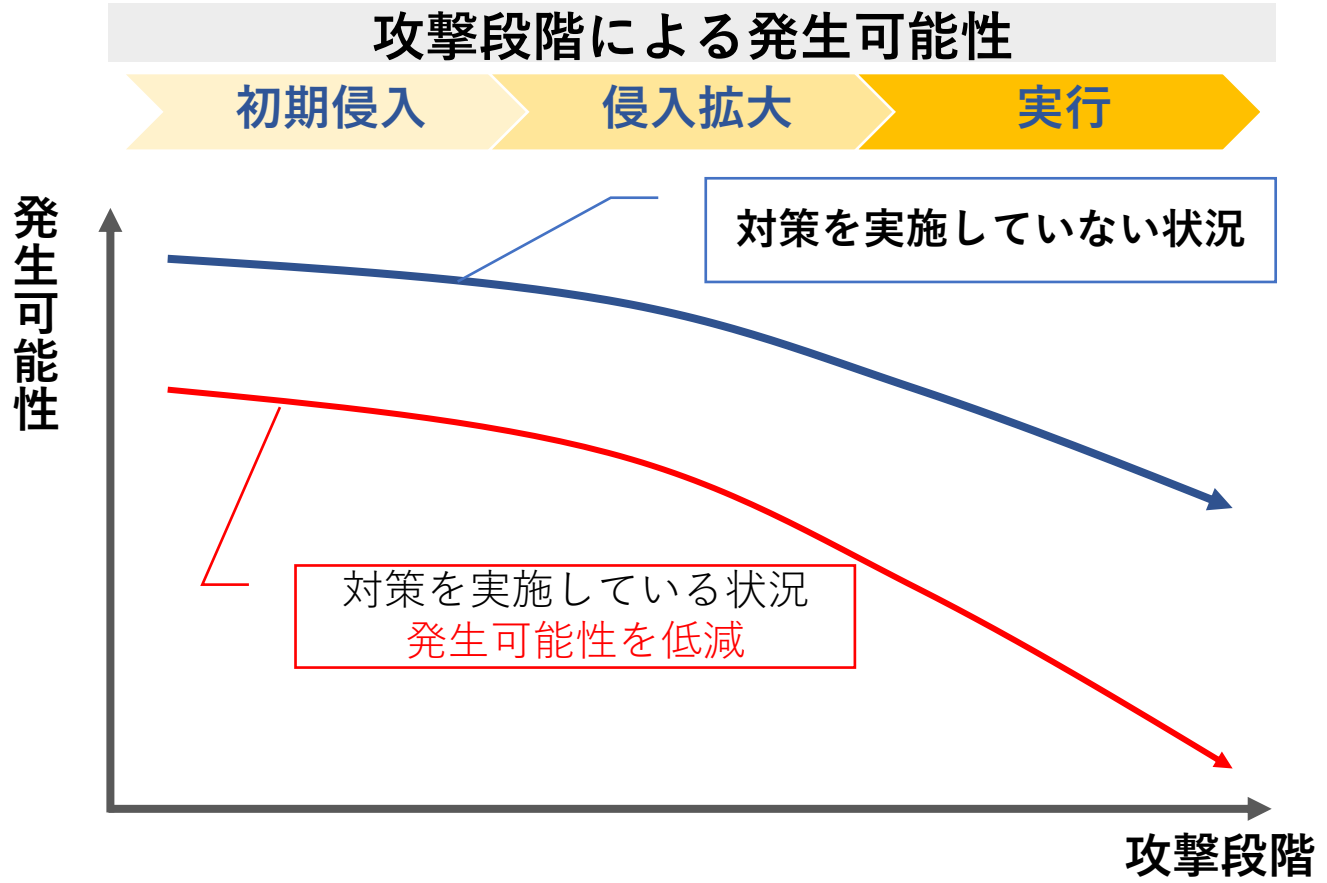
攻撃の発生可能性やセキュリティ戦略を考慮して優先順位付け

・防御対策と検知対応対策のどちらを優先するか企業の方針により決定できる。

ガイド機能分類	概要
優先順位付けの考え方提示	ガイドとして基本の優先順位付けとする攻撃段階の考え方を提示する。
対策案のカテゴリ分類	リスク分析した対策案を防御対策と検知対応対策で分類する。
セキュリティ戦略確認	方針にて防御対策と検知対応対策のどちらを重視するか選択する。
対策優先順位決定	攻撃シナリオと対策案の優先順位を決定する。

3-1.優先順位付けの考え方提示

攻撃段階が初期であるほど発生可能性が高く、進行するほど防御者に気づかれやすく攻撃者のスキルが問われるため攻撃の発生可能性は低くなる。



本ガイドでは攻撃段階の初期から対策を実施していくことを基本的な優先順位付けの考え方として実行段階（インシデント発生）の発生可能性リスクを低減することを目指す。

3-1.優先順位付けの考え方提示

各シナリオの対策の優先順位は「初期侵入、侵入拡大、実行」の順番で優先順位をつける。（シナリオ１）

シナリオ１

侵入口　重要資産　想定被害
A　→　1　操業停止　　侵入口A：USBメモリ　重要資産１：コントローラ

優先順位

攻撃段階	対策案	対策導入箇所
1 初期侵入	USBポートの物理ブロック	制御系ネットワーク内のサーバや端末
	デバイス接続制限の設定	制御系ネットワーク内のサーバや端末
	アンチウイルスソフトによる検知、駆除	制御系ネットワーク内のサーバや端末
2 侵入拡大	ホワイトリスト型のプロセス起動制限	制御系ネットワーク内のサーバや端末
	IDS(制御系)による不正通信検知	制御系ネットワーク
	不正通信検知後の対応手順作成と定期訓練	制御系ネットワーク
	FWによるセグメント分割	制御系ネットワーク
	複雑なパスワードの設定	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器
	通信の暗号化	制御系ネットワーク内
3 実行	インシデント対応手順の作成と定期訓練	ー
	操業の復旧手順の作成と定期訓練	ー
	ログ収集	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器
	データバックアップ	制御系ネットワーク内のサーバや端末

3-1.優先順位付けの考え方提示

各シナリオの対策の優先順位は「初期侵入、侵入拡大、実行」の順番で優先順位をつける。（シナリオ２）

シナリオ２

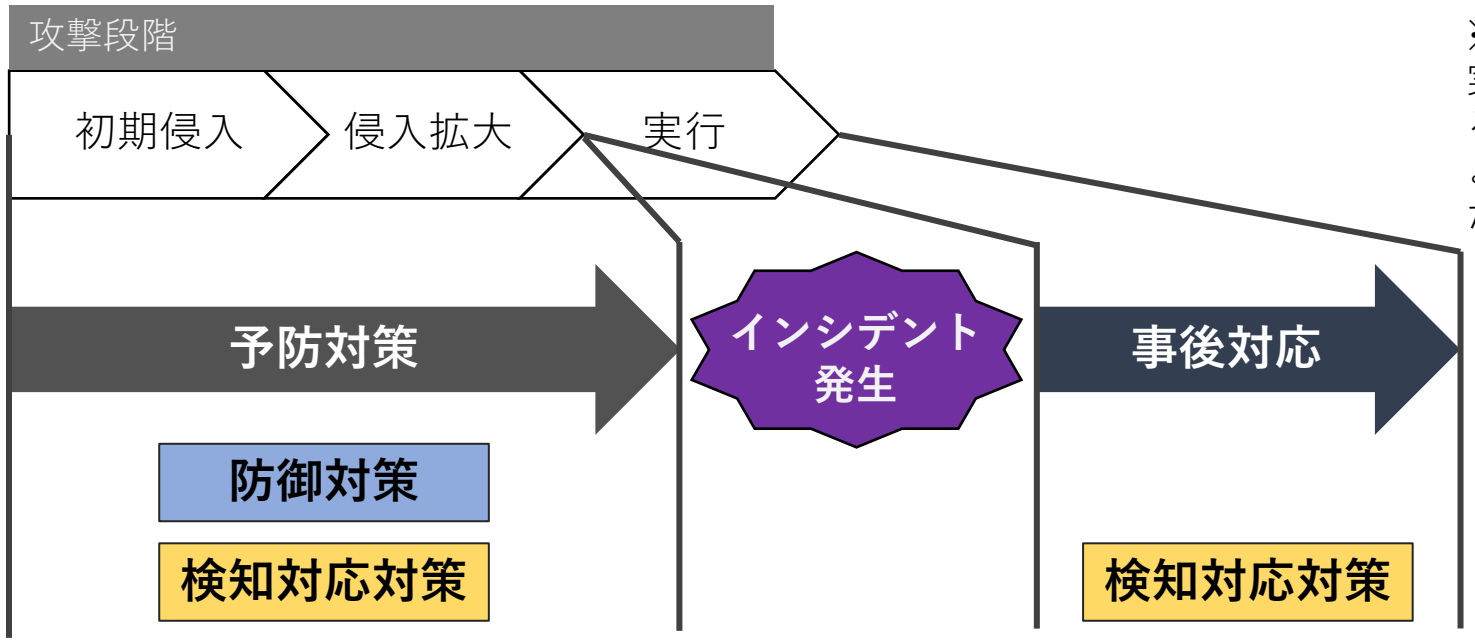
侵入口　重要資産　想定被害
B　→　1　操業停止　侵入口B：情報系NW　重要資産１：コントローラ

優先順位

攻撃段階	対策案	対策導入箇所
1 初期侵入	標的型メール訓練の定期実施	OA用PC
	OSやアプリケーションのバージョン最新化	OA用PC
	アンチウイルスソフトによる検知、駆除	OA用PC
2 侵入拡大	IDS(情報系)による不正通信検知	情報系ネットワーク
	FWやIPSによるIT/OT分離（制御系DMZ設置）	情報系ネットワークと制御系ネットワークの境界
	IDS(IT/OT境界)による不正通信検知	情報系ネットワークと制御系ネットワークの境界
	不正通信検知後の対応手順作成と定期訓練	情報系ネットワークと制御系ネットワークの境界
	ホワイトリスト型のプロセス起動制限	制御系ネットワーク内のサーバや端末
	IDS(制御系)による不正通信検知	制御系ネットワーク
	不正通信検知後の対応手順作成と定期訓練	制御系ネットワーク
	FWによるセグメント分割	制御系ネットワーク
	複雑なパスワードの設定	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器
	通信の暗号化	制御系ネットワーク内
3 実行	インシデント対応手順の作成と定期訓練	ー
	操業の復旧手順の作成と定期訓練	ー
	ログ収集	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器
	データバックアップ	制御系ネットワーク内のサーバや端末

3-2. 対策案のカテゴリ分類

対策の分類としてインシデント防止の「予防対策」と発生後の「事後対応」がある。また、対策の機能により「防御対策」と「検知対応対策」で分類する。



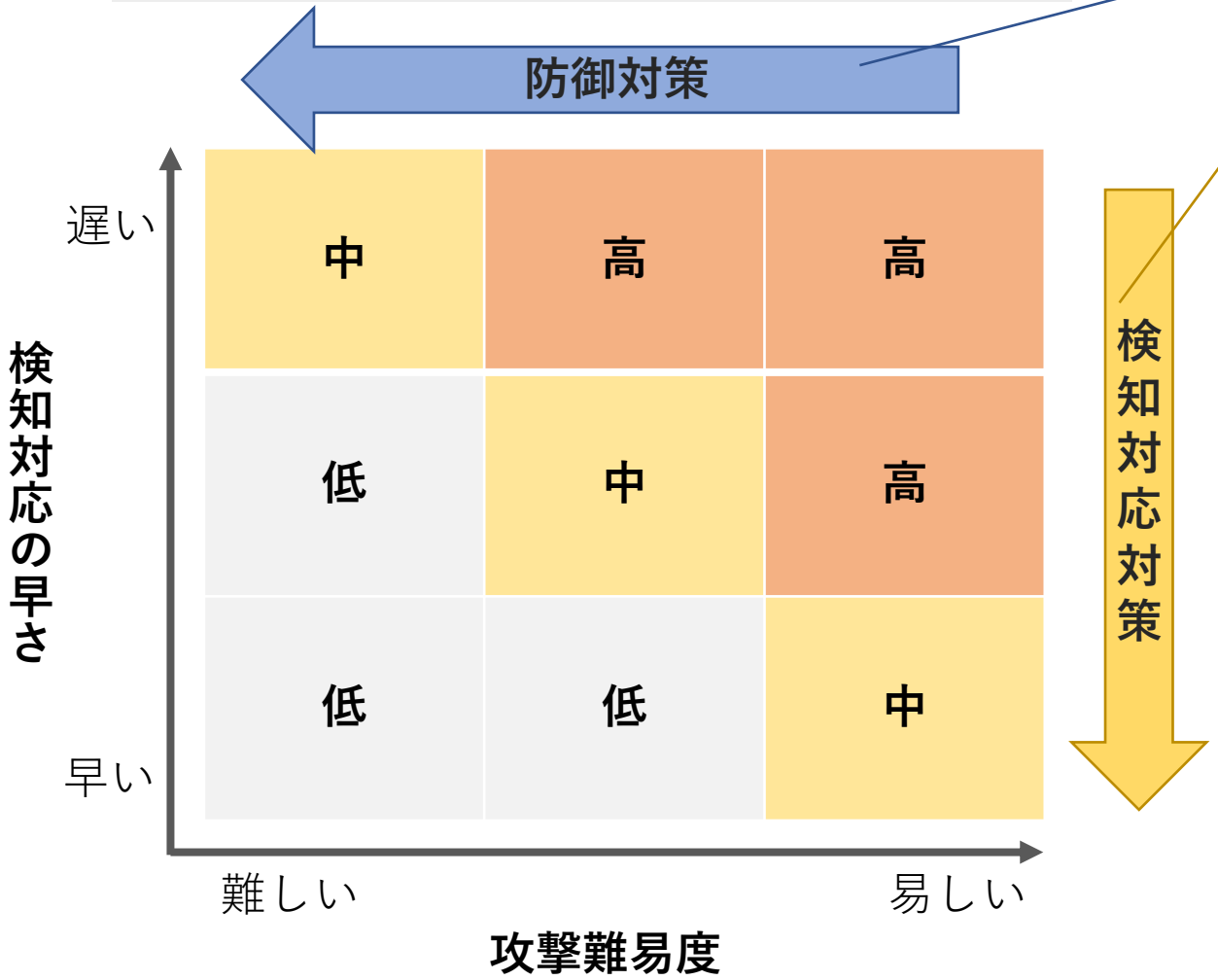
※「実行」段階の対策について
実行段階の直前まで攻撃が侵入拡大している場合、「実行」段階の攻撃を防御対策によって防ぐことは難しいため、事後対応のための検知対応対策に投資すべきである。

予防対策	防御対策	防御対策を事前に講じて侵入や拡大を予防すること。 （FW導入、アンチウルスの製品導入）
予防対策	検知対応対策	検知機能を利用して防御対策の設定見直しや改善対応で侵入や拡大を予防すること。 （FW導入、アンチウルスのログチェック、設定見直し）
事後対応	検知対応対策	インシデント発生後の障害検知と対応手順、復旧機能などで事後対応すること。 （IDSの異常検知、手順通りにインシデント対応、バックアップからリストア）

3-2. 対策案のカテゴリ分類（補足）

インシデントの発生可能性を下げる対策として「防御対策」と「検知対応対策」がある。

インシデント発生可能性のマトリクス



防御対策は**攻撃難易度を難しくする**ことで発生可能性を減らす。

検知対応対策は**検知対応の早さを向上する**ことで発生可能性を減らす。

※昨今はサイバー攻撃の巧妙化により防御策だけでは完全に防御しきれないため、異常や攻撃を検知する対策を活用して対応対策、復旧対策に繋げることが重要となる。

また検知対応を早期に行うことで、インシデントの発生可能性を低減することができる。

3-2. 対策案のカテゴリ分類

対策を「防御」「検知対応」に分類する。

シナリオ１

侵入口　重要資産　想定被害
A　→　1　　操業停止　　侵入口A：USBメモリ　重要資産１：コントローラ

優先順位

	攻撃段階	対策案	分類
1	初期侵入	USBポートの物理ブロック	**防御（予防対策）**
		デバイス接続制限の設定	**防御（予防対策）**
		アンチウイルスソフトによる検知、駆除	**検知対応（予防対策）**
2	侵入拡大	ホワイトリスト型のプロセス起動制限	**防御（予防対策）**
		IDS(制御系)で不正通信検知	**検知対応（予防対策）**
		不正通信検知後の対応手順作成と定期訓練	**検知対応（予防対策）**
		FWによるセグメント分割	**防御（予防対策）**
		複雑なパスワードの設定	**防御（予防対策）**
		通信の暗号化	**防御（予防対策）**
3	実行	インシデント対応手順の作成と定期訓練	**検知対応（事後対応）**
		操業の復旧手順の作成と定期訓練	**検知対応（事後対応）**
		ログ収集	**検知対応（事後対応）**
		データバックアップ	**検知対応（事後対応）**

3-2. 対策案のカテゴリ分類

対策を「防御」「検知対応」に分類する。

シナリオ２

侵入口　重要資産　想定被害
B　→　1　操業停止　　侵入口B：情報系NW　重要資産１：コントローラ

優先順位

攻撃段階	対策案	分類
1 初期侵入	標的型メール訓練の定期実施	**防御（予防対策）**
	OSやアプリケーションのバージョン最新化	**防御（予防対策）**
	アンチウイルスソフトによる検知、駆除	**検知対応（予防対策）**
2 侵入拡大	IDS(情報系)による不正通信検知	**検知対応（予防対策）※情報系**
	FWやIPSによるIT/OT分離（制御系DMZ設置）	**防御（予防対策）**
	IDS(IT/OT境界)による不正通信検知	**検知対応（予防対策）**
	不正通信検知後の対応手順作成と定期訓練	**検知対応（予防対策）**
	ホワイトリスト型のプロセス起動制限	**防御（予防対策）**
	IDS(制御系)で不正通信検知	**検知対応（予防対策）**
	不正通信検知後の対応手順作成と定期訓練	**検知対応（予防対策）**
	FWによるセグメント分割	**防御（予防対策）**
	複雑なパスワードの設定	**防御（予防対策）**
	通信の暗号化	**防御（予防対策）**
3 実行	インシデント対応手順の作成と定期訓練	**検知対応（事後対応）**
	操業の復旧手順の作成と定期訓練	**検知対応（事後対応）**
	ログ収集	**検知対応（事後対応）**
	データバックアップ	**検知対応（事後対応）**

3-3.セキュリティ戦略確認

対策の戦略として重視するパターンを選択する。

スタンダード（予防対策重視）

攻撃段階の早い段階から防御対策と検知対応対策をバランスよく実施する方針

検知対応重視

素早く検知対応しインシデントを未然に防いだり、インシデントが発生してしまった場合に復旧を早める方針

防御重視

多層防御の考えでインシデントの発生可能性を低減する方針

各方針による攻撃段階と対策分類ごとの優先順位例

優先順位	攻撃段階	対策分類
1	初期侵入	防御(予防対策)
2		検知対応(予防対策)
3	侵入拡大	防御(予防対策)
4		検知対応(予防対策)
5	実行	検知対応(事後対応)

優先順位	攻撃段階	対策分類
1	初期侵入	検知対応(予防対策)
2	侵入拡大	検知対応(予防対策)
3	実行	検知対応(事後対応)
4	初期侵入	防御(予防対策)
5	侵入拡大	防御(予防対策)

優先順位	攻撃段階	対策分類
1	初期侵入	防御(予防対策)
2	侵入拡大	防御(予防対策)
3	初期侵入	検知対応(予防対策)
4	侵入拡大	検知対応(予防対策)
5	実行	検知対応(事後対応)

3-3.セキュリティ戦略確認

バランスタイプを選択したで優先順位を決定する

スタンダード（予防対策重視）

シナリオ１

優先順位

優先順位	攻撃段階	対策案	分類
1	初期侵入	USBポートの物理ブロック	防御（予防対策）
2		デバイス接続制限の設定	防御（予防対策）
3		アンチウイルスソフトによる検知、駆除	検知対応（予防対策）
4	侵入拡大	ホワイトリスト型のプロセス起動制限	防御（予防対策）
5		FWによるセグメント分割	防御（予防対策）
6		複雑なパスワードの設定	防御（予防対策）
7		通信の暗号化	防御（予防対策）
8		IDS(制御系)で不正通信検知	検知対応（予防対策）
9		不正通信検知後の対応手順作成と定期訓練	検知対応（予防対策）
１０	実行	インシデント対応手順の作成と定期訓練	検知対応（事後対応）
１１		操業の復旧手順の作成と定期訓練	検知対応（事後対応）
１２		ログ収集	検知対応（事後対応）
１３		データバックアップ	検知対応（事後対応）

3-3.セキュリティ戦略確認

検知対応重視タイプを選択したパターンで優先順位を決定する。

検知対応重視

シナリオ１

優先順位

優先順位	攻撃段階	対策案	分類
1	初期侵入	アンチウイルスソフトによる検知、駆除	検知対応（予防対策）
2	侵入拡大	IDS(制御系)で不正通信検知	検知対応（予防対策）
3		不正通信検知後の対応手順作成と定期訓練	検知対応（予防対策）
4	実行	インシデント対応手順の作成と定期訓練	検知対応（事後対応）
5		操業の復旧手順の作成と定期訓練	検知対応（事後対応）
6		ログ収集	検知対応（事後対応）
7		データバックアップ	検知対応（事後対応）
8	初期侵入	USBポートの物理ブロック	防御（予防対策）
9		デバイス接続制限の設定	防御（予防対策）
１０	侵入拡大	ホワイトリスト型のプロセス起動制限	防御（予防対策）
１１		FWによるセグメント分割	防御（予防対策）
１２		複雑なパスワードの設定	防御（予防対策）
１３		通信の暗号化	防御（予防対策）

3-3.セキュリティ戦略確認

防御重視タイプを選択したパターンで優先順位を決定する

防御重視

シナリオ１

優先順位

優先順位	攻撃段階	対策案	分類
1	初期侵入	USBポートの物理ブロック	防御（予防対策）
2		デバイス接続制限の設定	防御（予防対策）
3	侵入拡大	ホワイトリスト型のプロセス起動制限	防御（予防対策）
4		FWによるセグメント分割	防御（予防対策）
5		複雑なパスワードの設定	防御（予防対策）
6		通信の暗号化	防御（予防対策）
7	初期侵入	アンチウイルスソフトによる検知、駆除	検知対応（予防対策）
8	侵入拡大	IDS(制御系)で不正通信検知	検知対応（予防対策）
9		不正通信検知後の対応手順作成と定期訓練	検知対応（予防対策）
１０	実行	インシデント対応手順の作成と定期訓練	検知対応（事後対応）
１１		操業の復旧手順の作成と定期訓練	検知対応（事後対応）
１２		ログ収集	検知対応（事後対応）
１３		データバックアップ	検知対応（事後対応）

4.企業固有の制約による優先順位付け

4. 企業固有の制約による優先順位付け

3章までで優先順位付けした各対策についてコストや導入ハードルを評価し、各企業の制約（予算や制御システムの運用状況など）を考慮して最終的な優先順位付けを行う。

企業固有の制約による優先順位付け

予算や制御システムの運用状況などの企業固有の制約を考慮して優先順位付け

・各対策のコスト感や導入時のハードルについての評価を確認できる。

ガイド機能分類

各対策の評価を提示

概要

各対策の導入/運用コストや導入ハードルについて評価例を提示する。
↓
次ページ以降の評価例を参考に3章までで挙がった対策案について
予算や運用状況等の企業固有の制約を考慮して最終的な優先順位付けを
行ってください。

※当プロジェクトにて評価した例は別紙２「各対策の評価例」を参照。

4. 企業固有の制約による優先順位付け

各対策の「導入コスト」「運用コスト」「導入時のハードル」について、予算や制御システムの運用状況等を考慮して導入の難易度を評価する。

対策の評価例（シナリオ２の対策一覧から抜粋）

優先順位	対策名称	対策箇所	導入コスト	運用コスト	導入時のハードル
1	標的型メール訓練の定期実施	OA用PC	◎	◎	◎
2	OSやアプリケーションのバージョン最新化	OA用PC	◎	◎	◎
3	アンチウイルスソフトによる検知、駆除	OA用PC	◎	◎	◎

例：対策１「標的型メール訓練の定期実施」の評価コメント

導入コスト	テスト用のメール作成や、e-Learningの整備などに社内人件費や社外委託費を要する。
運用コスト	訓練の実施内容の定期点検や定期実施に社内人件費や社外委託費を要する。
導入時ハードル	制御システムへの影響なし。

4. 企業固有の制約による優先順位付け(補足)

例ではコスト感/導入ハードルについて、導入の難易度を「◎、○、△」の3段階で評価している。

導入が容易 ⟷ **導入が難しい**

	◎	○	△
導入コスト	・製品の導入コストが少ない ・導入に要する作業が少ない	・製品の導入コストが中程度 ・導入に要する作業が中程度	・機器コストが多い ・導入に要する作業が多い
運用コスト	・製品の運用保守コストが少ない ・年数回の定期作業がある程度	・製品の運用保守コストが中程度 ・イベントに応じて運用保守作業がある	・製品の運用保守コストが多い ・日々一定の運用保守作業がある
導入時のハードル(制御システムの可用性への影響)	・制御システムへの影響が少ない 情報系ネットワークへの対策導入やミラーポート接続による導入など	・制御システムへの影響が中程度 制御システムへの影響を考慮してサービス一時停止の調整を要する	・制御システムへの影響が大きい 製造業務に関わるMES、HMI、コントローラの機器停止や制御システムの停止への影響がある

4. 企業固有の制約による優先順位付け(補足)

シナリオ２の対策の評価例　（1/2）

※詳細は別紙２「各対策の評価例」を参照。

優先順位	対策名称	対策箇所	導入コスト	運用コスト	導入時のハードル
1	標的型メール訓練の定期実施	OA用PC	◎	◎	◎
2	OSやアプリケーションのバージョン最新化	OA用PC	◎	◎	◎
3	アンチウイルスソフトによる検知、駆除	OA用PC	◎	◎	◎
4	IDS(情報系)による不正通信検知	情報系ネットワーク	△	○	◎
5	FWやIPSによるIT/OT分離（制御系DMZ設置）	情報系ネットワークと制御系ネットワークの境界	○	○	○
6	IDS(IT/OT境界)による不正通信検知	情報系ネットワークと制御系ネットワークの境界	△	△	◎
7	不正通信検知後の対応手順作成と定期訓練	情報系ネットワークと制御系ネットワークの境界	◎	◎	◎
8	ホワイトリスト型のプロセス起動制限	制御系ネットワーク内のサーバや端末	○	○	△
9	IDS(制御系)で不正通信検知	制御系ネットワーク	△	△	◎

4. 企業固有の制約による優先順位付け(補足)

シナリオ２の対策の評価例　（2/2）

※詳細は別紙２「各対策の評価例」を参照。

優先順位	対策名称	対策箇所	導入コスト	運用コスト	導入時のハードル
１０	不正通信検知後の対応手順作成と定期訓練	制御系ネットワーク	○	○	◎
１１	FWによるセグメント分割	制御系ネットワーク	△	○	△
１２	複雑なパスワードの設定	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器	◎	○	◎
１３	通信の暗号化	制御系ネットワーク内	△	○	△
１４	データの暗号化	制御系ネットワーク内のサーバや端末	△	○	△
１５	インシデント対応手順の作成と定期訓練	ー	○	○	◎
１６	操業の復旧手順の作成と定期訓練	ー	○	○	◎
１７	ログ収集	制御系ネットワーク内のサーバや端末、NW機器、セキュリティ機器	○	○	○
１８	データバックアップ	制御系ネットワーク内のサーバや端末	○	○	○

5.利用規約

5-1. 著作権及びその他すべての知的所有権

「制御システムのセキュリティ対策優先順位付けガイド及び制御システムのセキュリティ対策優先順位付けツール（以下、「本作品」）」に関する著作権及びその他すべての知的所有権は、「情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラム 5期生 制御システムのセキュリティ対策優先順位付けガイドプロジェクト（以下、「本プロジェクト」）」及び本作品中に利用した下記各イラスト制作者等に帰属します。
・ICONFINDER（https://www.iconfinder.com/）

5-2. 免責事項

本プロジェクトは、本作品について品質的にも法律的にも何らの保証もしません。また、本プロジェクトは、本作品の使用に起因して生じるすべての直接的、間接的、付随的又は結果的損害、利益の損失等に関し、法的原因の如何を問わず何らの責任も負いません。

5-3. 注意事項

本作品の内容は本プロジェクトの見解に基づいております。独立行政法人情報処理推進機構（IPA）及び作成者の所属企業の見解を反映するものではありません。

5-4. 利用条件・範囲

本作品は、個人、法人組織における非営利、非商業的態様でのセキュリティ対策優先順位付けの目的でのみ、かつ健全な社会通念に反しないことを条件として、本書面の定めにしたがって事前連絡せずに無償で使用出来るものとします。その他の利用（内容の改変等を含みます）は一切認めませんので、その場合には改めて本プロジェクト及び上記各イラスト制作者等の許諾を得る必要があります。

6. 謝辞

本プロジェクトの推進に際し、以下のICSCoE講師の皆様にはサイバーセキュリティの専門家としてご指導・ご鞭撻を賜りましたこと、感謝申し上げます。

越島 一郎 教授　　名古屋工業大学
満永 拓邦 准教授　東洋大学
佐々木 弘志 氏　　フォーティネットジャパン株式会社

本プロジェクトの推進に際し、以下のICSCoE1期生の皆様には現場視点の貴重なご意見・ご指摘をいただきましたこと、感謝申し上げます。（順不同）

飯塚 禎彦 氏　JFEコムサービス株式会社
木村 修明 氏　東ソー株式会社
松髙 聡史 氏　三菱地所株式会社
安元 智司 氏　旭化成株式会社
佐々木 誠 氏　東京エレクトロン株式会社
金杉 将幸 氏　三菱重工業株式会社
花田 高広 氏　産業技術総合研究所
堀江 剛史 氏　株式会社UACJ
本田 英之 氏　株式会社中電シーティーアイ
横江 智昭 氏　株式会社トヨタシステムズ
他1名

その他本プロジェクトに関わっていただいた全ての皆様に感謝申し上げます。

7. プロジェクトメンバー

【リーダー】

大久保 佑　　三菱電機株式会社

【メンバー】（50音順）

宇山 大貴　　ダイキン工業株式会社
木村 太祐　　コスモエネルギーホールディングス株式会社
杉生 雅樹　　株式会社日立システムズ

8. 参考文献

- 制御システムのセキュリティリスク分析ガイド第二版
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
- NIST Cybersecurity Framework Version 1.1
  https://www.nist.gov/cyberframework/framework
- Consequence-driven Cyber-informed Engineering (CCE)
  https://inl.gov/cce/
- Cyber Kill Chain
  https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
- MITRE ATT&CK for Industrial Control Systems
  https://collaborate.mitre.org/attackics/index.php/Main_Page