

# ビル制御システムのセキュリティと 経産省ガイドライン解説 (配布版)

2019年11月7日

森ビル株式会社

ALSOK 総合警備保障株式会社

NTTコミュニケーションズ株式会社 井上 裕司 / Yuji Inoue

佐藤 芳紀 / Yoshinori Sato

熊谷 拓実 / Takumi Kumagae

# 自己紹介

投影のみとさせていただきます

詳しくは <https://built.itmedia.co.jp/bt/articles/1907/29/news005.html>

# IPA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 (ICSCoE)

ICSCoE

検索

IPA Better Life with IT  
独立行政法人 情報処理推進機構  
Information Technology Promotion Agency, Japan

Industrial Cyber Security Center of Excellence

近頃は社会インフラ・産業基盤に物理的なダメージを与えるサイバー攻撃のリスクが増大し、海外においては、既に他国等からなされるサイバー攻撃により、社会インフラ・産業基盤の安全が脅かされる事案が発生しています。社会インフラ・産業基盤における、サイバー攻撃に対する防護力を強化することは、国家全体の喫緊の課題です。

## 人材育成事業

- 社会インフラ・産業基盤事業者において、自社システムのリスクを認識しつつ必要なセキュリティ対策を判断できる人材を育成するプログラムを提供。
- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家と共に安全性・信頼性の検証や早期復旧の演習を行う。
- 最新の技術・ノウハウを学び、産業界のセキュリティ責任者や専門家、海外との連携を促進するコミュニティなどを創出する。
- 海外との積極的な連携において、海外専門家との知見交換の場を創出し、グローバルな知見を蓄積していく。
- 企業等の経営層に対して、サイバー攻撃の実態や産業サイバーセキュリティ対策の必要性を啓発するためのトレーニング提供・情報発信を行う。

## 目標すべき産業サイバーセキュリティ人材像

- 自適・適應・技術理解
- プロジェクトを強力に推進していく力を要います。
- プロジェクトの強力な推進
- 将来の優先順位づけと事業計画への織り込み
- 改革推進のロードマップ化
- ビジネススキル
- プロジェクトの強力な推進
- サイバー攻撃による影響の度合い把握
- 監視対象の選出
- 対応の優先順位づけ
- テクノロジースキル (OT・IT)
- 産業インフラに対する脅威の特徴と防護措置の検討
- インシデント対応の対応とビジネス戦略との連携

## 実際の制御システムの安全性・信頼性検証事業

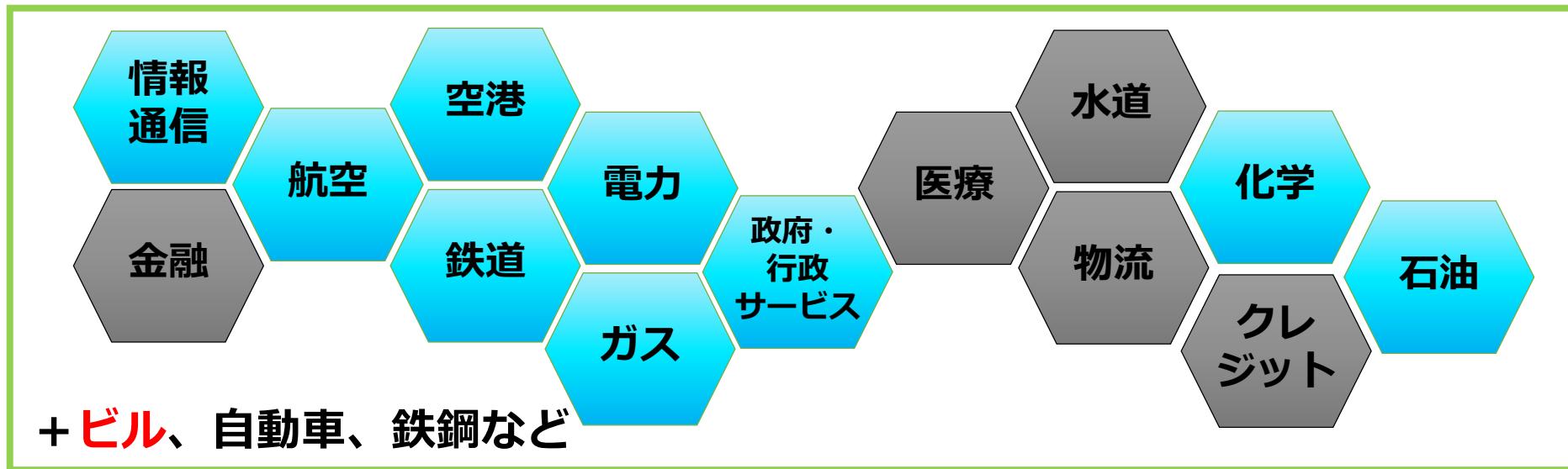
- 我が国の大規模な社会インフラ・産業基盤に係る制御システムの安全性・信頼性に関するリスク評価を行う。
- あらゆる改修可能性を検証し、必要な対策立案を行う。

## 攻撃情報の調査・分析事業

- 最新のサイバー攻撃情報を収集。(例えば、おとりシステムの観察や民間専門機関が持つ攻撃情報を収集)
- 新たな攻撃手法等を調査・分析し、人材育成事業やシステム検証事業に活用。

# IPA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

## プログラム2期生の出身元企業 一重要インフラ分野別ー（※水色表記）



日本の産業インフラのセキュリティを守るために、  
高度なトレーニングを受講

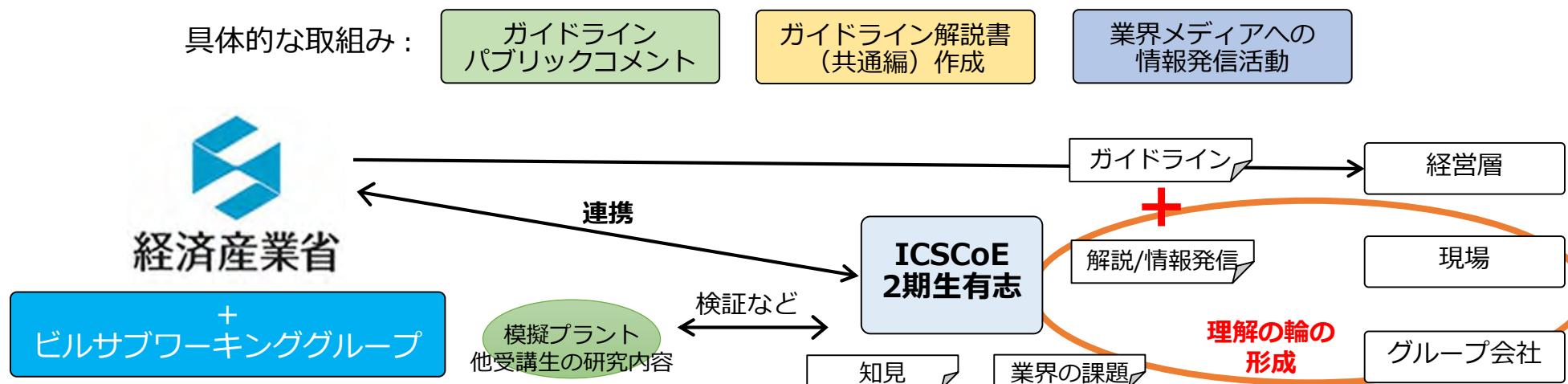
投影のみとさせていただきます

詳しくは [https://www.ipa.go.jp/icscoe/program/core\\_human\\_resource/index.html](https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html)

# ICSCoEでの卒業プロジェクト：ビル業界への貢献

## 「ビルセキュリティガイドライン（※）」をより普及させていくための施策

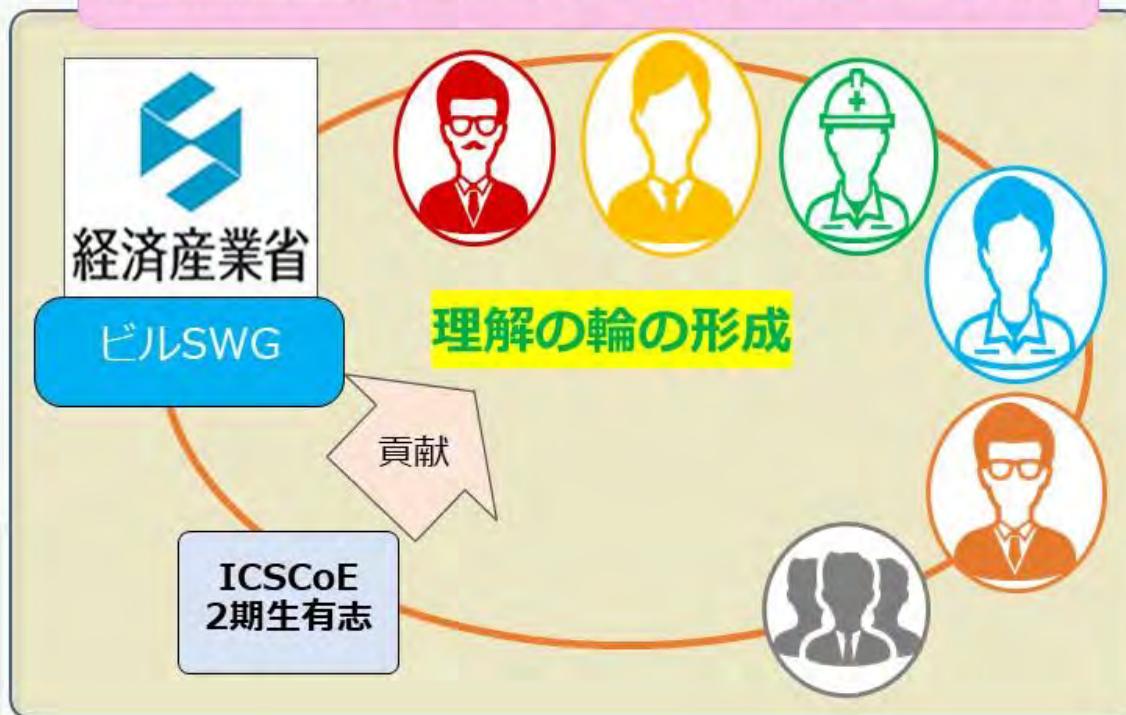
- 課題認識 : ビルシステムにおけるセキュリティ水準の向上  
ガイドラインやベストプラクティスをどのようにすれば  
経営層や現場、グループ会社へ浸透させることができるか？
- 取組み方針 : “経済産業省 サイバーセキュリティ研究会 ビルサブワーキンググループ”と連携し、
  - ①ガイドラインを現場/経営層双方の視点で解説
  - ②普及のための情報発信・啓発



※ 正式名：「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン 第一版」

# ICSCoEでの卒業プロジェクト：ビル業界への貢献

## 卒業後もビルSWGでの活動を継続



ガイドライン解説書の作成

ビル業界に向けた情報発信  
(業界誌 / Web記事)



# アジェンダ

1. 本セッションの論点・目的
2. 経産省 ビルセキュリティガイドライン解説
3. ケーススタディ “リスク分析から対策優先度をつけてみる”
4. まとめ

1. 本セッションの論点・目的

2. 経産省 ビルセキュリティガイドライン解説

3. ケーススタディ “リスク分析から対策優先度をつけてみる”

4. まとめ

# 本日お話ししたい内容

## ロビル制御システムの特徴及び環境変化

- ✓ 多様性、長いライフサイクル、マルチステークホルダー
- ✓ 環境変化 (IoT、2020)

## ロビルセキュリティガイドライン及び対策本質理解

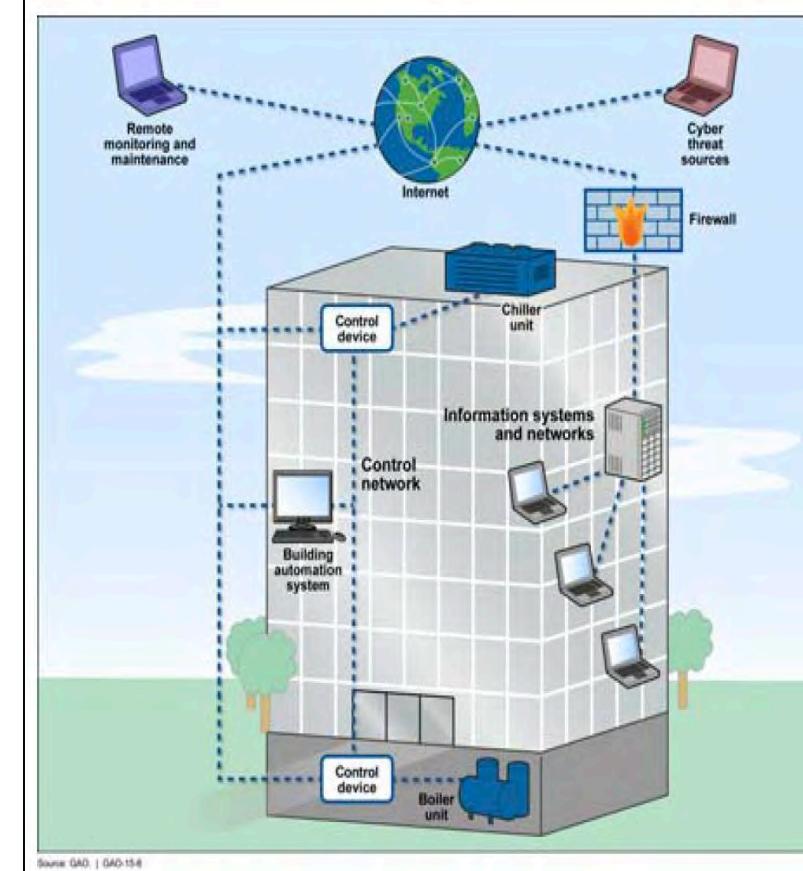
- ✓ なぜ今ガイドラインなのか
- ✓ 対策の本質とは

## ロビルセキュリティガイドライン解説

- ✓ ガイドラインの利活用シーン
- ✓ 具体的対策

## リスク分析

- ✓ リスクアセスメント : CCE  
お手元の「CCEリスク分析ワークシート」をぜひお使いください

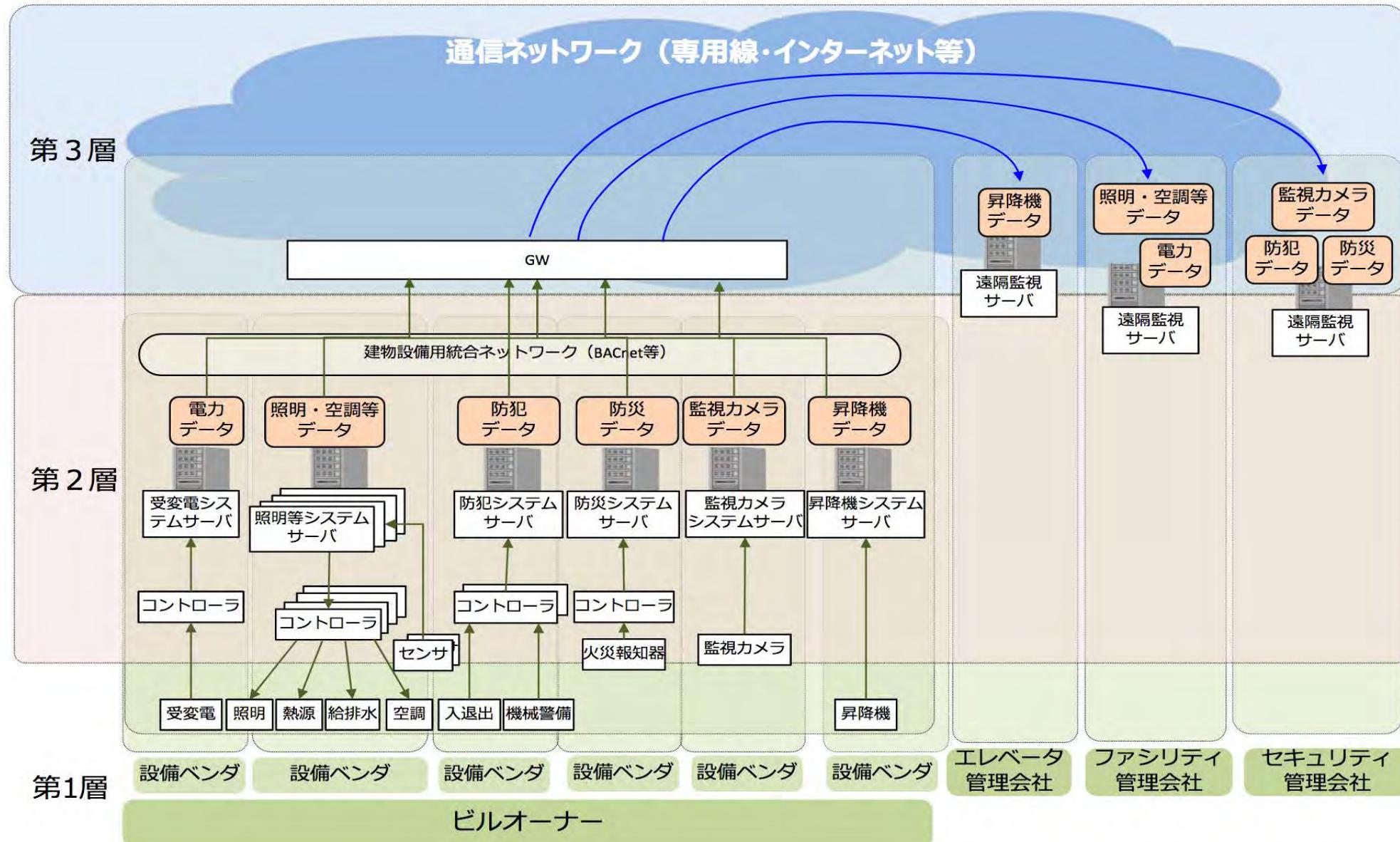


# (参考) 制御システムとは



出典) NISC, [https://www.nisc.go.jp/active/infra/pdf/infra\\_rt4\\_abst.pdf](https://www.nisc.go.jp/active/infra/pdf/infra_rt4_abst.pdf)

# ビル制御システムとは



出典) 経済産業省, 「サイバー・フィジカル・セキュリティ対策フレームワーク」

# ビル制御システムの特徴

## 超長期の運用

- ・ITシステムの倍以上の長期に渡る運用  
(ビルシステムでは**10~20年**)
- ・例. Windows7 延長サポート含めてリリース後から約10年間  
→ サポート期間にギャップがある

## 複数のフェーズに分かれた長いライフサイクルを持つこと

ビルの企画から建設、運用、そして最終的な撤去まで、幾つかのフェーズに分かれ た非常に長いライフサイクルを有している  
→ 例. 設計段階では、長期の運用を意識した上でのセキュリティ対策をどのように設計仕様に盛り込むかが課題

## ビルシステムの特徴

ビルオーナー、設計会社、ゼネコン、サブコン、ビル管理会社、制御機器ベンダ等様々なステークホルダが存在している。  
→ 連携すべきステークホルダが多い

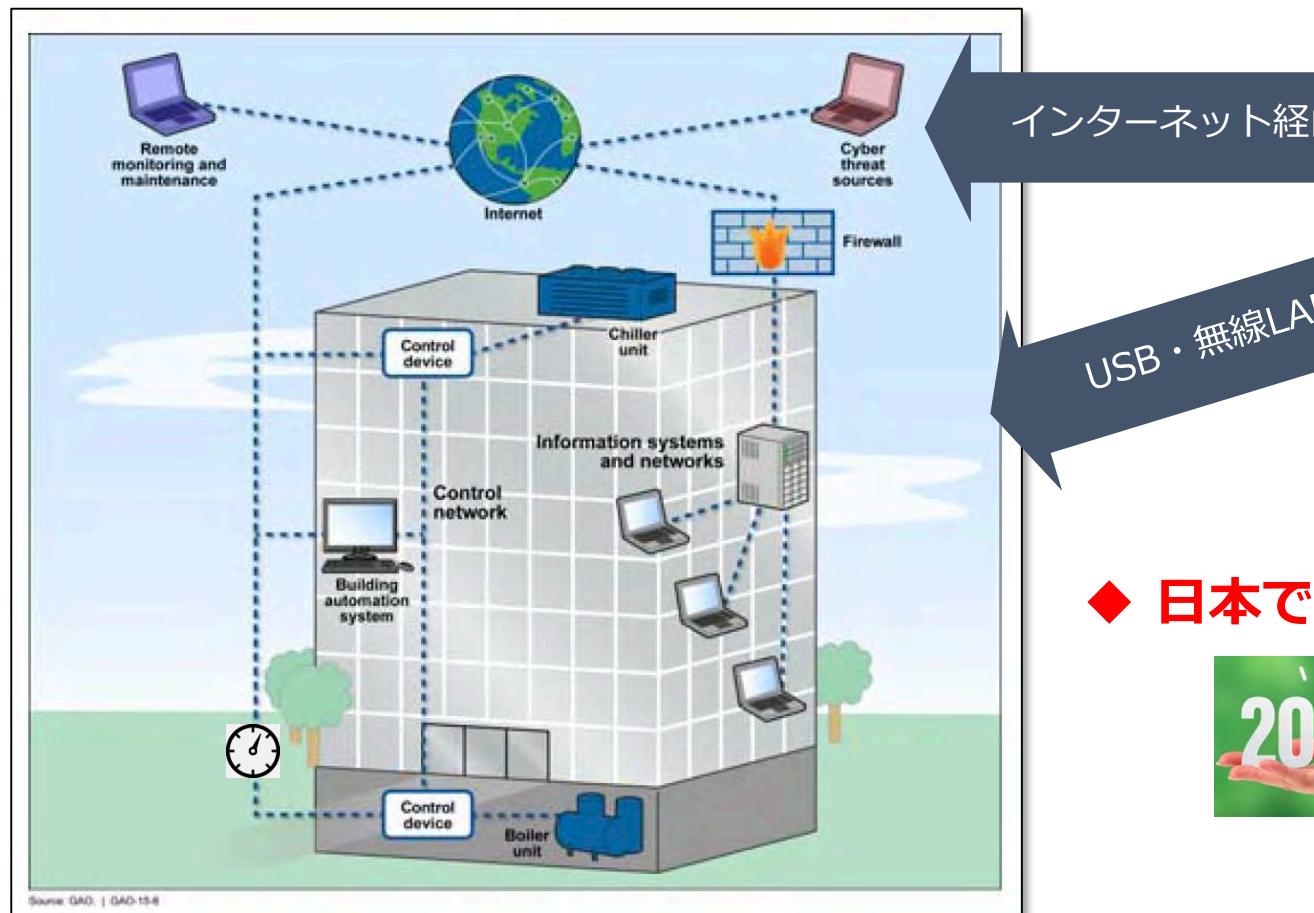
## マルチステークホルダであること

新築か既存か、自社ビルかテナントビルか、大規模か中小規模かなど、ビルの特徴が存在する  
→ セキュリティ対策をビルの特徴に合わせて選択していく必要がある

## 多種多様なビルの存在

# ビル制御システムの環境変化

システム運用を効率化するため、インターネットを経由したリモート監視やリモートメンテナンスを実施する例が増えてきている。



◆ 日本で控えている国際的イベントも



EXPO2025

出典/引用) 経済産業省, 2019/3/11, 『ガイドライン』パブコメ版 図2-3 空調等をインターネット経由で遠隔から管理する例

# 実際にビルも狙われている

国内でもビルシステムの攻撃リスクが顕在化

警視庁がインターネット定点観測システムにて、日本国内のビル管理システムに対する探索行為を検知し、注意喚起。（2014年7月）

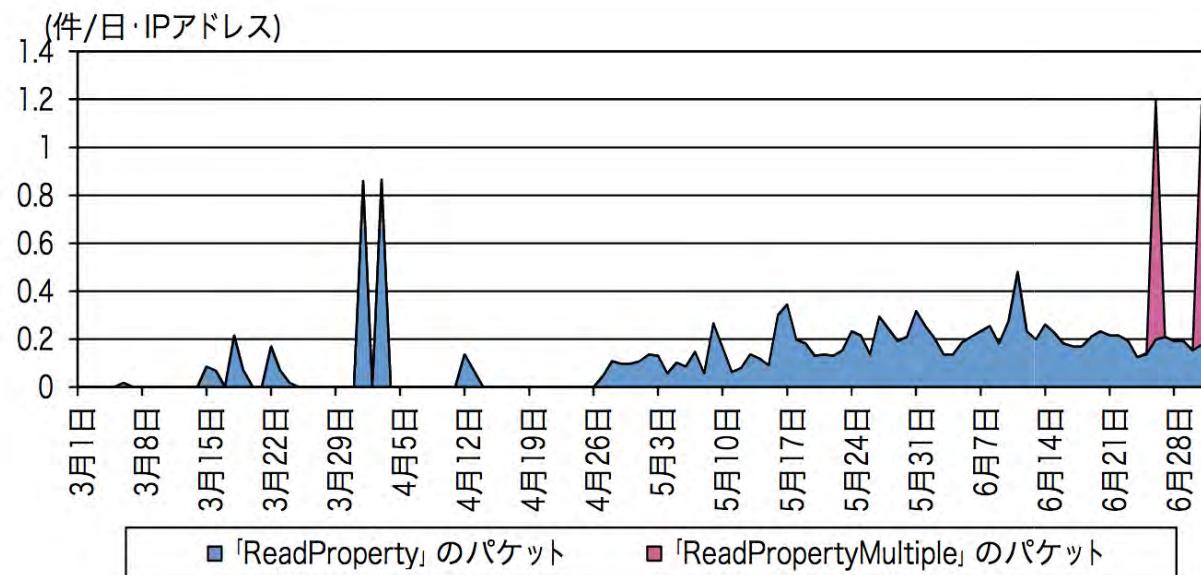


図 ビル管理システムの探索と考えられるアクセス (H26.3.1～H26.7.4)

「ReadPropertyMultiple」：  
BACnetシステムに接続された機器の情報をひとつの命令で複数確認できるパケットのこと

出典) 警視庁@police, 2014/7/6, 「ビル管理システムに対する探索行為の検知について」  
<https://www.npa.go.jp/cyberpolice/detect/pdf/20140706.pdf>

# (参考) ビル制御システムへの攻撃事例

## 事例：フィンランドのビル暖房停止



出典：

### 事例：オーストリアでのホテル宿泊客閉じ込め・閉め出し



出典：CNN

発生日	2017年1月
発生国・箇所	オーストリア・Romantik Seehotel Jaegerwirt
攻撃手法	ランサムウェア感染
影響	宿泊客の客室閉め出し

#### 概要

オーストリアの4つ星ホテルRomantik Seehotel Jaegerwirtで電子カードキーシステムがランサムウェアに感染した。

客室の扉はカード式のキーを使って施錠と開錠を行う仕組みだったが、サイバー攻撃によりこのカードキーのシステムがダウンしたため、宿泊客は自分の部屋に入れなくなった。新しいカードキーのプログラムもできなくなった。

ホテルの予約システムやキャッシュデスクシステムも含めてすべてダウンした。この日の宿泊客は約180人。攻撃側は、ビットコインで1,500ユーロの身代金を要求していた。

#### 参考 URL

■ CNN  
<https://edition.cnn.com/2017/01/30/europe/hackers-lock-out-hotel-guests-trnd/index.html>

■ ITmedia  
<https://www.itmedia.co.jp/enterprise/articles/1701/31/news068.html>

#### 概要

2016年11月、フィンランド東部ラッペーンランタの集合住宅の暖房・給湯システムが攻撃を受けて停止し、暖房と給湯の機能が利用不可になった。

インターネット経由で遠隔制御されていた暖房・給湯の制御システムに対してDDoS攻撃が行われた。その結果、システムの再起動が何度も引き起こされていた。

11月のフィンランドは既に外気温マイナス2度の環境であり、このような中で、数時間に渡って暖房が利用出来ない状況が継続した。

#### 参考 URL

- Metropolitan.fi  
<http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter>
- ETELA-SAIMAA  
<https://esaimaa.fi/uutiset/lahella/64208f0e-81b9-4a41-ad68-df8fa521224f>

後ほどリスク分析でも登場します

# (参考) shodan

Shodan Developers Monitor View All..

SHODAN BACnet Explore Pricing Enterprise Access

Exploits Maps

TOTAL RESULTS 8,043

TOP COUNTRIES

Country	Hosts
United States	5,599
Canada	1,183
United Kingdom	152
Australia	109
Germany	96

TOP SERVICES

Service	Count
BACnet	7,963
8083	10
8081	8
HTTP	8
Qconn	3

TOP ORGANIZATIONS

Organization	Count
Comcast Business	843
AT&T Internet Services	501
Verizon Wireless	370
Spectrum Business	253
AT&T U-verse	115

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

**108.66.218.140**  
108-66-218-140.uvs.lrvnca.sbcglobal.net  
**AT&T Internet Services**  
Added on 2019-06-08 09:01:31 GMT  
 United States

Instance ID: 50100  
Object Name: 6060 1st Floor Afterhours  
Location: 1st Floor mechanical room.  
Vendor Name: Delta Controls  
Application Software: V3.40  
Firmware: 329735  
Model Name: eBMGR-TCH

**24.37.73.2**  
modemicable002.73-37-24.static.videotron.ca  
**Videotron Ltee**  
Added on 2019-06-08 08:58:11 GMT  
 Canada, Sainte-julie

Instance ID: 100  
Object Name: 1\_AR\_4817\_Sherbrooke0  
Location: Grand Marche  
Vendor Name: Delta Controls  
Application Software: V3.40  
Firmware: 189697  
Model Name: DSC\_1146E

**94.205.143.10**  
Emirates Integrated Telecommunications Company  
**PJS**  
Added on 2019-06-08 08:59:17 GMT

Instance ID: 100  
Object Name: Was1\_PRP\_100

出典) shodan : インターネットに公開されているデバイスを探索できるサイト <https://www.shodan.io/>

# ビル制御システム（BA）と情報システム（IT）の違い

セキュリティの優先順位や環境に違いがある

	ビル制御システム（BA）	情報システム（IT）
セキュリティの 優先順位	<b>可用性</b> (システムが継続して安全稼動できること)	<b>機密性</b> (情報が適切に管理され、情報漏洩を防ぐ)
セキュリティの 対象	<b>ヒト(利用者の安心・安全)</b> モノ（設備） サービス（連続稼動や <b>リアルタイム</b> な提供）	情報
建設/構築 期間	<b>1~8年</b> ※小規模ビルから複合ビル、オフィスビルから商業ビルまで <b>多様</b>	<b>概ね1年以内</b>
技術の サポート期間	<b>10~20年</b> ※ビルの耐用年数は50年以上	<b>3~5年</b>
運用管理	ビル管理部門	情報システム部門

可用性、リアルタイム性、多様性

# なぜビル制御システムへのセキュリティ対策が難しいのか

	対策を講じる上での障害	影響を受ける対策
可用性	<ul style="list-style-type: none"><li>➤ 年一回の定期点検の時しかシステムを止められない</li><li>➤ システム更新は概ね10年周期</li><li>➤ インシデント発生時でも簡単にシステム停止できない</li></ul>	<ul style="list-style-type: none"><li>➤ システム停止を伴う対策はほぼ不可能（定期点検時は他のメンテ計画がたくさん）</li><li>➤ 被害拡大防止</li></ul>
リアルタイム性	<ul style="list-style-type: none"><li>➤ 稼働スケジュールに影響を及ぼす負荷はかけられない</li></ul>	<ul style="list-style-type: none"><li>➤ アンチウィルス製品（CPU負荷増）</li><li>➤ ログ強化（通信量増）</li></ul>
多様性	<ul style="list-style-type: none"><li>➤ 検証環境がない</li><li>➤ 多様なプロトコル</li><li>➤ マルチベンダー</li></ul>	<ul style="list-style-type: none"><li>➤ バージョンアップやパッチ適用時の影響調査、テストが困難</li><li>➤ IPS/IDSの導入が困難（正常パケットと異常パケットの判別困難）</li></ul>
その他	<ul style="list-style-type: none"><li>➤ セキュリティ対策意識がまだ醸成されていない</li><li>➤ BA（ビル現場）・IT双方の知識を持つ人材がない</li><li>➤ 対象機器が非常に多い・設置先が分散</li><li>➤ BAとITのライフサイクルの違い（設計時はXPが主流だったが、竣工時はWin10が主流）</li></ul>	<ul style="list-style-type: none"><li>➤ パスワードの定期的な変更が困難</li><li>➤ 資産管理が困難（全体把握が困難）</li></ul>

# そこでビルセキュリティガイドライン（1/2）

今年6月17日に経済産業省より公開。

## 1.1.1. ガイドラインの目的

近年のサイバー攻撃技術の高度化や様々なシステムが益々ネットワークに繋がっていく状況の中で、制御システムへのサイバー攻撃リスクも高まってきている。重要インフラ分野においては、国の政策としてサイバーセキュリティ対策を進めるとともに、各業界や個別の事業者においても取組が進んできているが、ビルシステムに関するサイバーセキュリティ対策はほとんど手付かずの状態と言ってよい。

本ガイドラインの目的は、これまで取組が遅れていたビルシステムのサイバーセキュリティについて、その確保のためのガイダンスを示すことである。ここでいうビルシステムには、ビルを運営するためのシステムを構成する全てのサブシステムが含まれており、このようなビルシステムの概念について概要を整理し、それに対する脅威を示すとともに、これらの脅威に対する対策について、設計、建設、竣工検査、運用、改修／廃棄のビルシステムのライフサイクルに係わる各段階において整理して示すものである。

ビルシステムにおける  
サイバー・フィジカル・セキュリティ対策ガイドライン  
第1版

令和元年6月17日

産業サイバーセキュリティ研究会  
ワーキンググループ1(制度・技術・標準化)  
ビルサブワーキンググループ

# そこでビルセキュリティガイドライン（2/2）

## 1.2.4. ガイドラインの位置づけ

ガイドラインを作成するにあたって、ビルサブワーキンググループでは、いくつかの方針を定めて検討を行ってきた。

- ガイドラインはマスト(レギュレーション)ではないものにする。ビルシステム関係者が何を優先して対策していくか決めるための情報を提供する。
- 対象者は、ビルオーナー、ゼネコン／サブコン、設計者、設備ベンダ、管理者等、ビルの企画・建設から運営管理に関わるステークホルダ全般とする。
- ガイドラインは共通編と個別編(詳細編)の2階建てにする。

- 共通編は初步的な対策をまとめたものであり、厳し過ぎず、ポイントを押されたものにする。
- 設計やテスト等の各段階のチェックプロセスについて、関係者間の共通リファレンスを作る。
- 個別編では、共通編を超える部分についての詳細な方策や、更なるセキュリティ投資に関する経営判断の材料を提供する。

ビルシステムにおける  
サイバー・フィジカル・セキュリティ対策ガイドライン

第1版

令和元年6月17日  
産業サイバーセキュリティ研究会  
ワーキンググループ1(制度・技術・標準化)

ビルサブワーキンググループ

# ガイドラインが示す対策の本質

	1.2.4 ガイドラインの位置付けにかかれているキーワード	持つ意味
ちゃんとリスク管理する	マスト（レギュレーション）ではない	リスクを正しく理解し、対策の優先順位付け、計画をしつかり立てる
みんなでやる	対象者はステークホルダー全般 関係者間の共通リファレンス	ビルオーナーだけ、ベンダーだけが対策するのではなく、関係者すべてが当事者意識、共通目的を持ち、正しく会話する

## 対策による効果

より安全・安心なビル設備を提供できるようになることにより

- 本来の事業に専念できるようになる
- ビルオーナーはもちろんのこと、ステークホルダー全般の社会的信用・企業価値向上につながる
- 万が一サイバー攻撃により被害が発生してしまった場合でも、次の効果が見込まれる
  - 被害や損失の最小化
  - 復旧にかかる費用の低減
  - 風評被害の低減

1. 本セッションの論点・目的

2. 経産省 ビルセキュリティガイドライン解説

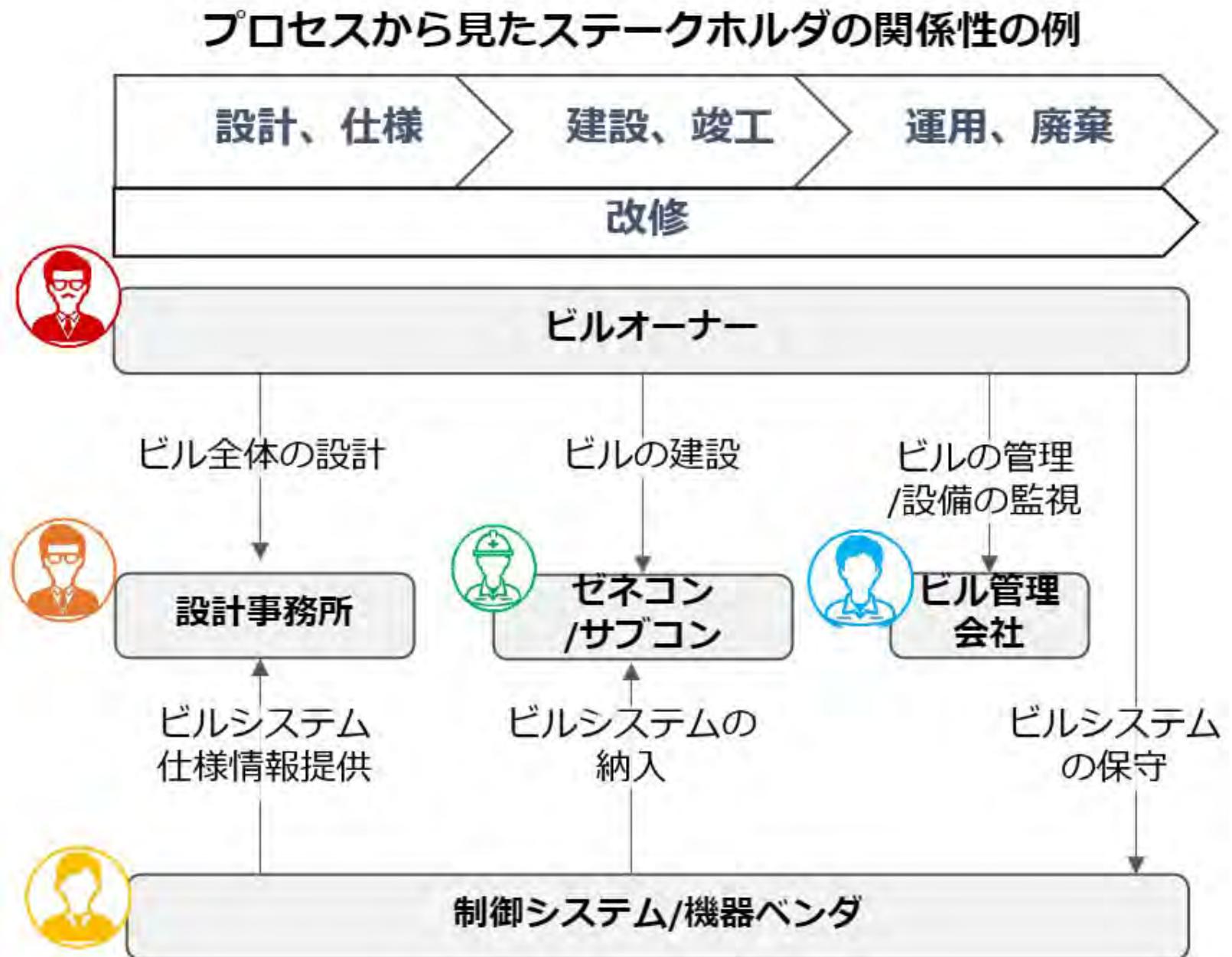
3. ケーススタディ “リスク分析から対策優先度をつけてみる”

4. まとめ

# 『ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン』とは

章	タイトル	記載概要
1	はじめに	ガイドライン策定の目的、位置付け、ドキュメント構成
2	ビルシステムを巡る状況の変化	ビルシステムの特徴とビルシステムに対するサイバーセキュリティの脅威の現状を示す。
3	ビルシステムにおけるサイバーセキュリティ対策の考え方	ビルシステムにおけるサイバーセキュリティ対策の基本的考え方やビルの条件に合わせたガイドラインの活用の仕方を示す。
4	ビルシステムにおけるリスクと対応ポリシー	ビルシステムにおけるサイバーセキュリティリスクと対策ポリシーを示す。
5	ライフサイクルを考慮したセキュリティ対応策	ビルのライフサイクルを「設計・仕様」「建設」「竣工検査」「運用」「改修・廃棄」の5段階に大別。4章で示した脅威に対する対策について、ライフサイクルの各フェーズごとに実施すべきセキュリティ対策について示す。
付録A	用語集	
付録B	JDCC の建物設備システムリファレンスガイドとの関係	
付録C	CPS対策フレームワークの考え方と、CPS対策フレームワークの考え方を踏まえたビルシステムにおけるユースケース	
付録D	参考文献	

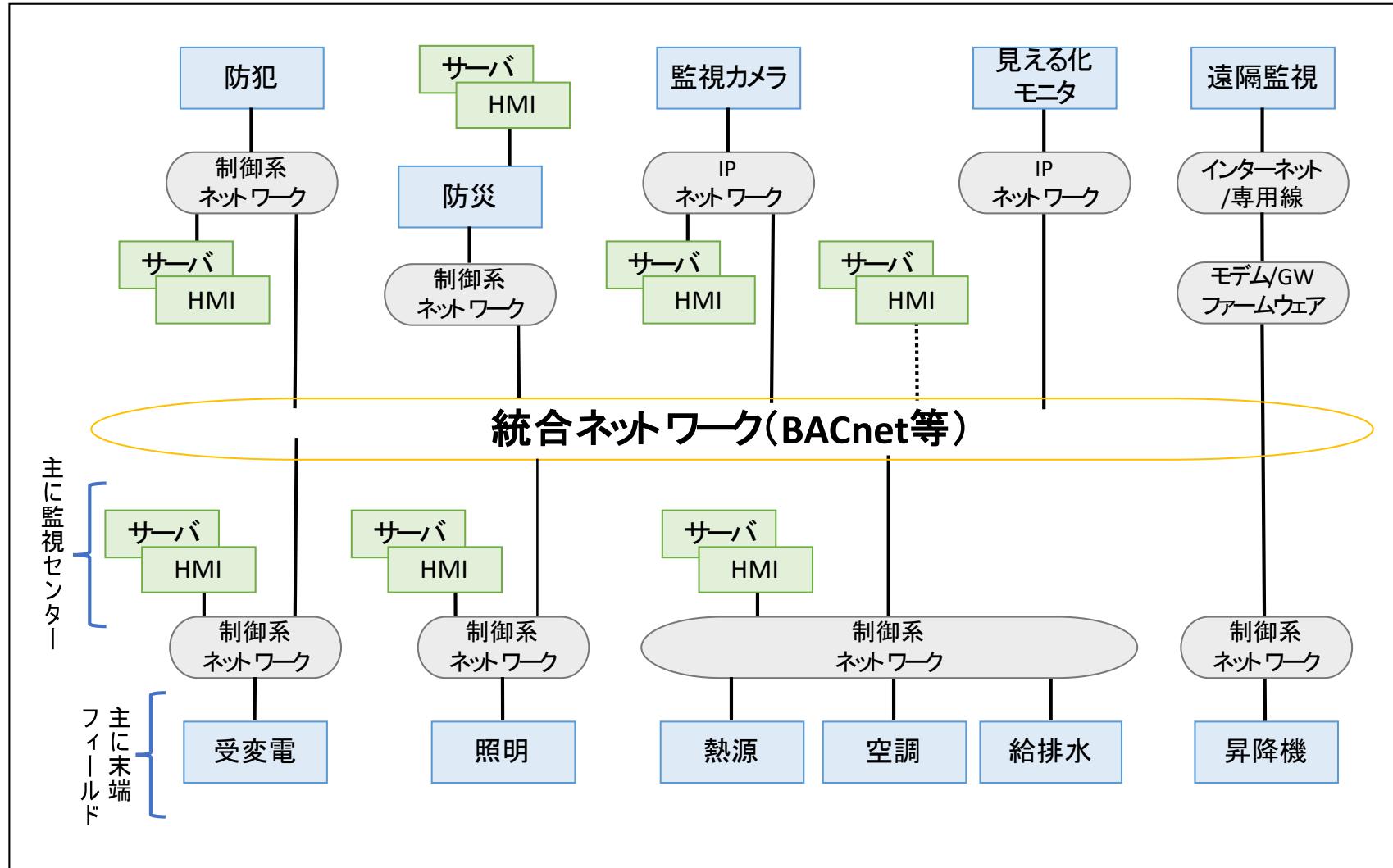
# 『ビルガイドライン』読み方：ビルライフサイクル、ステークホルダーを意識する



# 『ビルガイドライン』読み方：ビル制御システムが設置されている場所を意識する

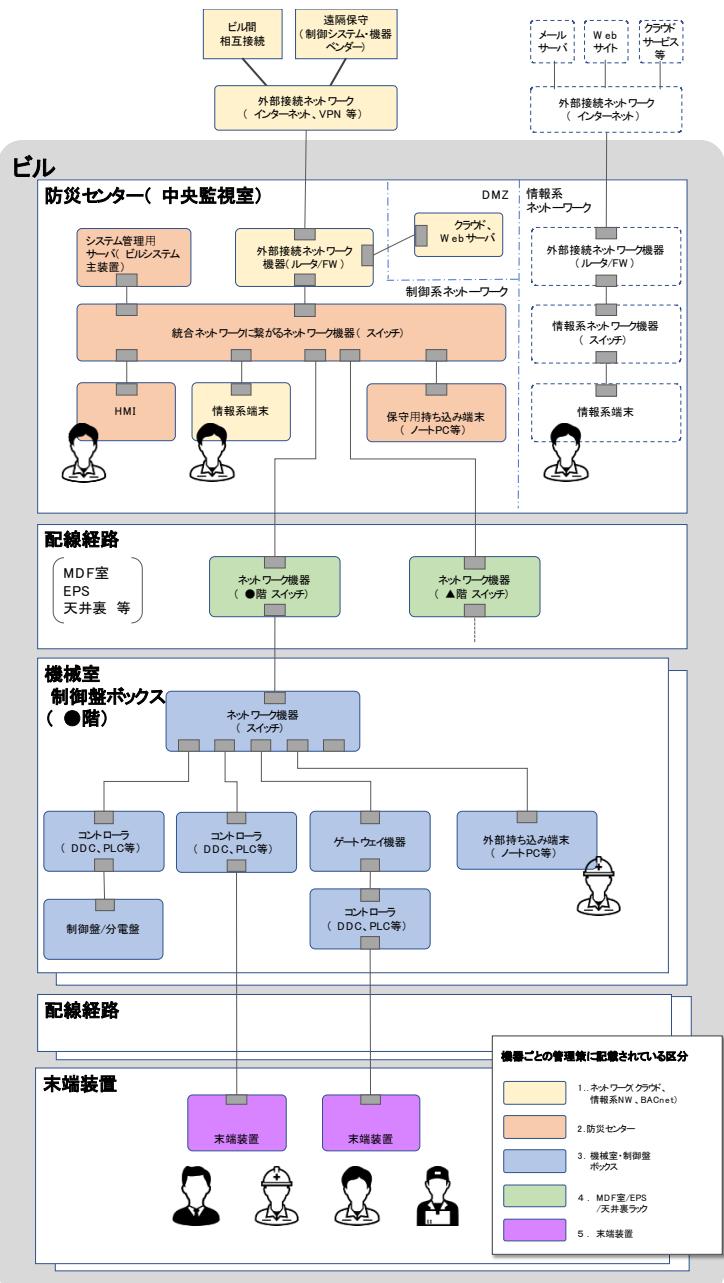
なぜ？

ビル運営の効率化のために、個別運用の各設備システムが統合ネットワークに接続されていることが多い。さらに、設備の末端は各フロアに散らばっており、管理の主体も様々。



出典/引用) 経済産業省, 2019/3/11,  
『ガイドライン』  
図3-3ビルシステムの標準的なモデル  
(全体像)  
を参考に作成

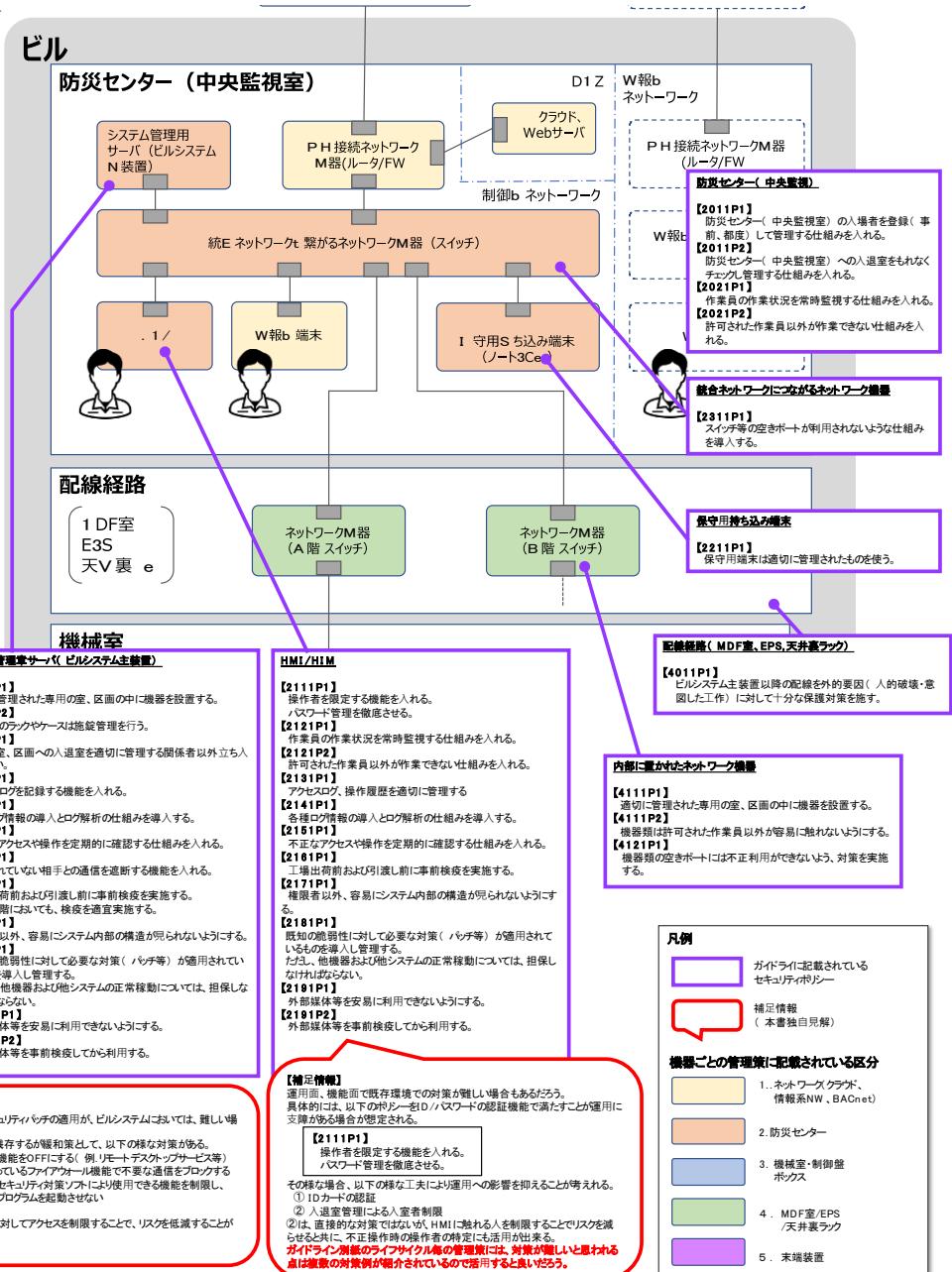
# 『ビルガイドライン』読み方：ビル制御システムが設置されている場所を意識する



## 対策マップ

構成図に  
ガイドラインの  
ポリシーをマッピング

対策の全体像を  
俯瞰することが重要



# ステークホルダー間で共通リファレンスになることの重要性



# 『ビルガイドライン』対策理解の近道

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン

## 「4. ビルシステムにおけるリスクと対応ポリシー」

### 全体管理

対策区分	ビルシステムにおけるリスクと対応ポリシー		
	インシデント	リスク源	ポリシー
1. 構成情報/管理情報			
2. バックアップデータ/事業継続			
3. 会社/要員の管理			
4. 体制構築等			

### 機器ごとの管理策

対策区分	ビルシステムにおけるリスクと対応ポリシー		
	インシデント	リスク源	ポリシー
1. ネットワーク			
2. 防災センター			
3. 機械室/制御盤ボックス			
4. 配線経路			
5. 末端機器が置かれる場所			

### 対応ポリシーをカテゴリ単位に分類

#### 【カテゴリ※】

- ・ 資産管理、構成管理
- ・ リスクアセスメント
- ・ サプライチェーン管理
- ・ 脆弱性管理
- ・ アクセス制御/ネットワーク分離/重要資産の保護
- ・ ログ管理
- ・ 検知プロセス/対応計画の策定
- ・ バックアップ

※カテゴリは、対応ポリシーの記載内容をNIST Cyber Security Framework を活用し分析した後、読みやすいように解説対象をグルーピングした区分

カテゴリ単位に対策のポイント（本質）を理解し、全体を俯瞰

# 『ビルガイドライン』対策の解説方法

**セキュリティポリシー** × **竣工時に資産情報、構成情報を把握する**

**カテゴリに関する対策ポリシー**

**資産管理、構成管理のポイント** = **資産情報、構成情報の把握**

**カテゴリに関する対策ポイント**

**どのようなリスクか？**  
ビルシステムの構成情報が把握できており、機器の接続関係がわからない状況です。

**リスクを放置するとどんな影響があるか？**  
適切にリスクの把握が出来ずに、対策漏れが発生してしまいます。

**対策の解説**

**新設ビルの場合**  
竣工時の引き渡し資料に以下を含める様に、設計時に関係者と認識を合わせておきましょう。

- ✓ システム構成図
- ✓ データフロー図
- ✓ 機器情報一覧  
(設置場所、IPアドレス等)
- ✓ 機器設定情報一覧
- ✓ ソフトウェア一覧
- ✓ 外部ネットワーク接続一覧

**既存ビルで資料がない場合**  
上記に記載している情報があるか確認をしましょう。

**リスク、リスクを放置した際に想定される影響、対策の解説**

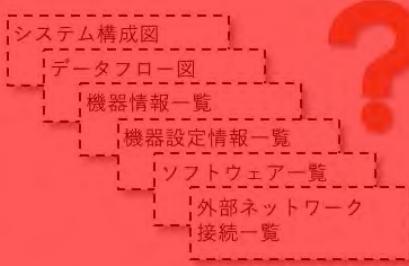
**【資産情報、構成情報の例】**

- システム構成図  
ネットワークの機器構成を示す図
- データフロー図  
機器同士の接続関係を示した図
- 機器情報一覧  
機器の資産情報をまとめた一覧  
(設置場所、IPアドレス等)
- 機器設定情報一覧  
機器の設定情報をまとめた一覧
- ソフトウェア一覧  
システムで使用しているソフトウェア情報(バージョン含む)をまとめた一覧  
(脆弱性の管理時に必要となる)
- 外部ネットワーク接続一覧  
ビルシステムから見た外部のネットワーク一覧  
(保守用回線、ITシステムとの相互接続、IoT機器向けのインターネット回線等)

**【インシデント発生時に、被害状況の把握に時間を要し、復旧の妨げとなります。】**

**【既存ビルで資料がない場合】**

まずシステム構成図、機器情報一覧、外部ネットワーク接続一覧を優先的に集めて整理しておきましょう。この情報を把握しておくことで、リスクアセスメントの際にで侵入経路の把握に活用することが出来ます。





構成管理

アセスメント

チェックリスト

カテゴリのインデックス

対応計画の策定

バックアップ

投影のみとさせていただきます

# 『ビルガイドライン』対策：アクセス制御

投影のみとさせていただきます

# 『ビルガイドライン』対策：アクセス制御

投影のみとさせていただきます

# 『ビルガイドライン』対策：検知プロセス・対応計画

投影のみとさせていただきます

# 『ビルガイドライン』対策：検知プロセス・対応計画

投影のみとさせていただきます

# 『ビルガイドライン』対策：検知プロセス・対応計画

投影のみとさせていただきます

1. 本セッションの論点・目的

2. 経産省 ビルセキュリティガイドライン解説

3. ケーススタディ “リスク分析から対策優先度をつけてみる”

4. まとめ

# リスク分析手法

- ✓ ガイドラインに記載の対策は、もちろんすべてを実施できることが望ましい。
- ✓ しかしながら、ビルの規模や特性、対策にかかる費用によってはそれが難しい場合もある。（セキュリティはどうしても費用として見られてしまう）
- ✓ セキュリティ専門家は“対策は全部すべき”とよく言うが“全部”なんて不可能。

**セキュリティ対策の優先度付けが有効**

## リスク分析の必要性

「許容できない事象／許容できる事象の見極め」  
「許容できない事象に関して、費用をかけて断ち切るべきポイント（優先度の高い対策）の設定」

「許容できない事象」を起こさないための対策を考える手法を採用

## Consequence-driven Cyber-Informed Engineering(CCE)

### STEP 1

#### Consequence Prioritization

許容できない事象を設定する

### STEP2

#### System of Systems Analysis

許容できない事象の発生条件を、システム構成  
(資産) ベースに要素分解する

### STEP3

#### Consequence-Based Targeting

許容できない事象の発生条件が成立するシナリオを、  
"サイバーキルチーン"をもとに洗い出す

### STEP4

#### Mitigation and Protection

許容できない事象の発生条件を断ち切るポイントを  
設定し、その実現策（防御対策）を整理する

# 事例：オーストリアでのホテル宿泊客閉じ込め・閉め出し



出典：CNN

発生日	2017年1月
発生国・箇所	オーストリア・Romantik Seehotel Jaegerwirt
攻撃手法	ランサムウェア感染
影響	宿泊客の客室閉め出し

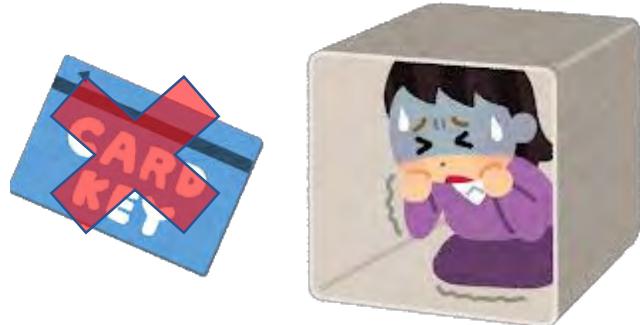
概要	<p>オーストリアの4つ星ホテルRomantik Seehotel Jaegerwirtで<b>電子カードキーシステムがランサムウェアに感染</b>した。</p> <p>客室の扉はカード式のキーを使って施錠と開錠を行う仕組みだったが、サイバー攻撃によりこのカードキーのシステムがダウンしたため、<b>宿泊客は自分の部屋に入れなくなった</b>。新しいカードキーのプログラムもできなくなった。</p> <p>ホテルの予約システムやキャッシュデスクシステムも含めてすべてダウンした。この日の宿泊客は約180人。攻撃側は、ビットコインで1,500ユーロの身代金を要求していた。</p>
参考URL	<ul style="list-style-type: none"><li>■ CNN <a href="https://edition.cnn.com/2017/01/30/europe/hackers-lock-out-hotel-guests-trnd/index.html">https://edition.cnn.com/2017/01/30/europe/hackers-lock-out-hotel-guests-trnd/index.html</a></li><li>■ ITmedia <a href="https://www.itmedia.co.jp/enterprise/articles/1701/31/news068.html">https://www.itmedia.co.jp/enterprise/articles/1701/31/news068.html</a></li></ul>

# 事例：オーストリアでのホテル宿泊客閉じ込め・閉め出し

サイバー攻撃者により、  
ホテルの電子カードキー  
システムへランサムウェア感染

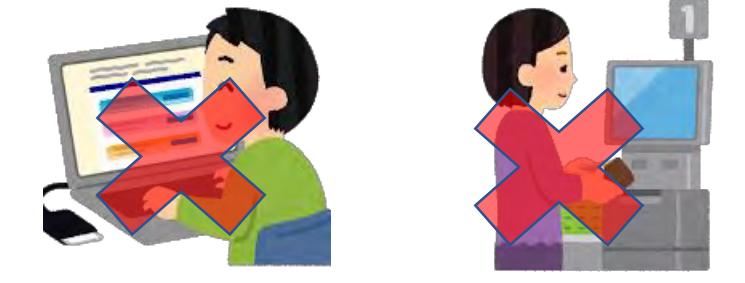


一切のシステム操作が不可能  
→客室扉の施錠、開錠が不可能  
→結果、宿泊客が閉じ込め・閉め出し



客室の電子カードキーシステム

攻撃は拡大し、予約システムや  
キャッシュデスクシステムも停止



予約システム

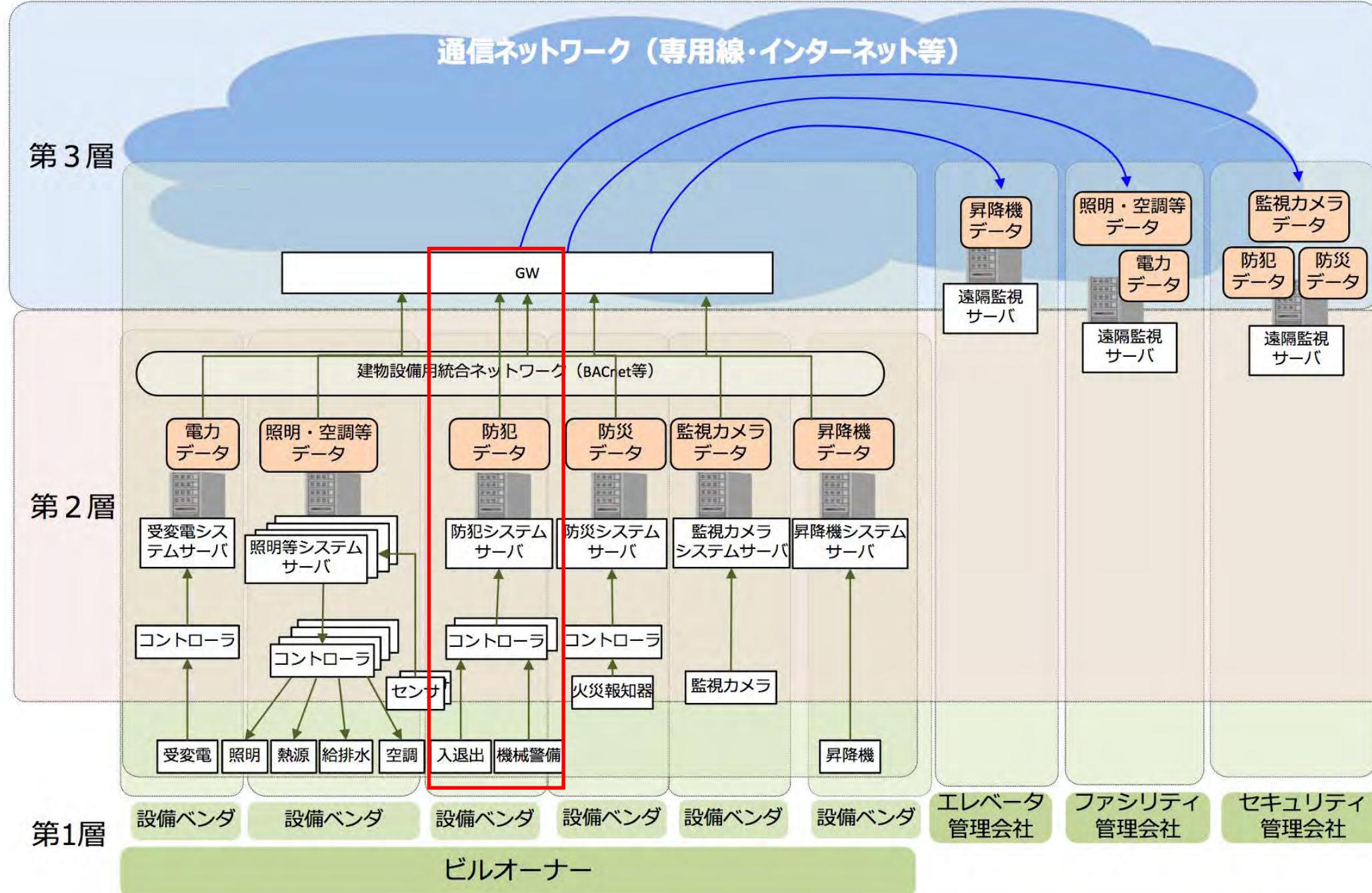
キャッシュデスク  
システム

攻撃者の要求に応じて  
身代金を支払い、制限  
を解除した



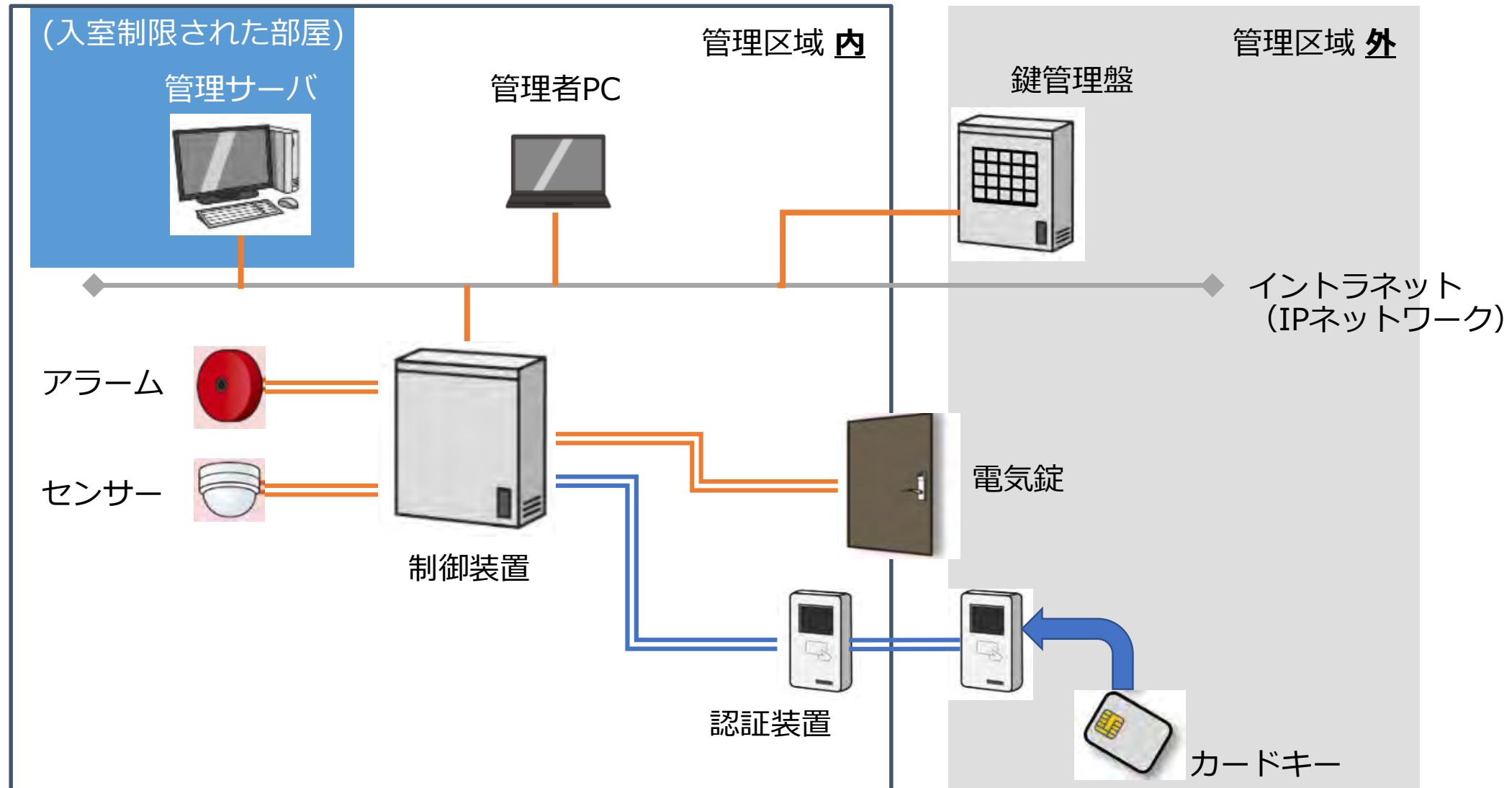
ランサムウェアとは：

マルウェアの一種。感染したコンピュータは、利用者のシステムへのアクセスを制限。制限解除のため、被害者がマルウェアの作者に身代金（ランサム）を支払うよう要求。



出典) 経済産業省、「サイバー・フィジカル・セキュリティ対策フレームワーク」

# 入退室管理システムの構成を整理



出典) IPA, 2019年5月20日, 「入退管理システムにおける情報セキュリティ対策要件チェックリスト」  
[https://www.ipa.go.jp/security/jisec/choutatsu/ecs/checklist\\_ecs.pdf](https://www.ipa.go.jp/security/jisec/choutatsu/ecs/checklist_ecs.pdf)

# リスク分析アプローチ

## 電子キーシステムの機能停止（ビルのお客様閉め出し）

を許容できない事象と設定

現状分析

弱いところを見る化  
(ビルガイドライン等とのマッピング)  
✓ 求める姿とギャップを明確化  
✓ 対策方針検討

リスク分析

リスクベースのシナリオから  
具体的対策を検討 (CCE<sup>※1</sup>)

対策検討

✓ 実現性に応じて対策レベルを設定（松・竹・梅）  
✓ 攻撃成立条件(サイバーキルチェーン)のどこで断ち  
切るか判断

解説範囲

「許容できない事象」を起こさないための対策を考える手法を採用

## Consequence-driven Cyber-Informed Engineering(CCE)

### STEP 1

#### Consequence Prioritization

許容できない事象を設定する

### STEP2

#### System of Systems Analysis

許容できない事象の発生条件を、システム構成  
(資産) ベースに要素分解する

### STEP3

#### Consequence-Based Targeting

許容できない事象の発生条件が成立するシナリオを、  
"サイバーキルチーン"をもとに洗い出す

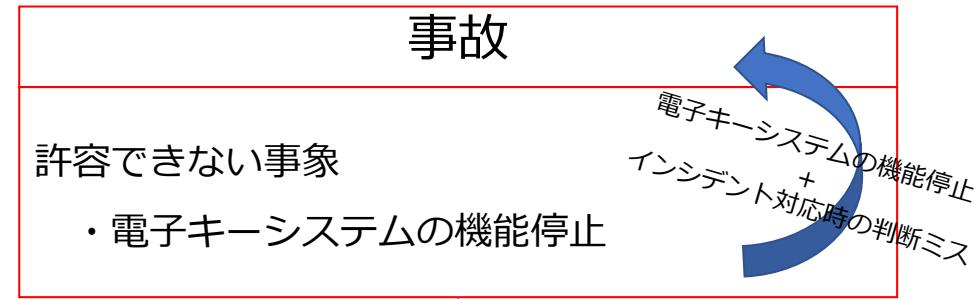
### STEP4

#### Mitigation and Protection

許容できない事象の発生条件を断ち切るポイントを  
設定し、その実現策（防御対策）を整理する

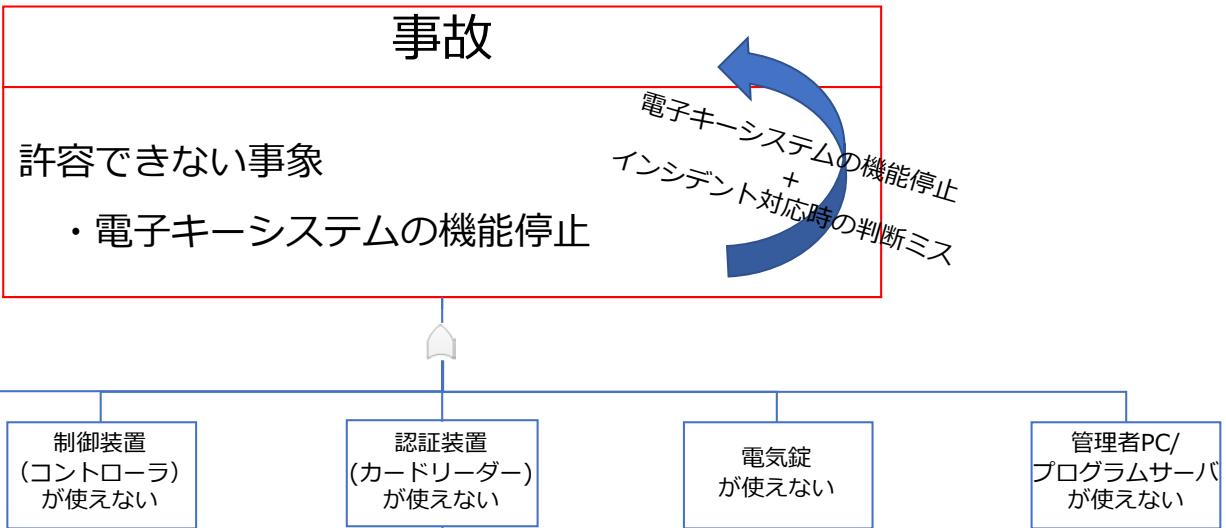
# STEP 1

Consequence  
Prioritization



## STEP 1

Consequence  
Prioritization

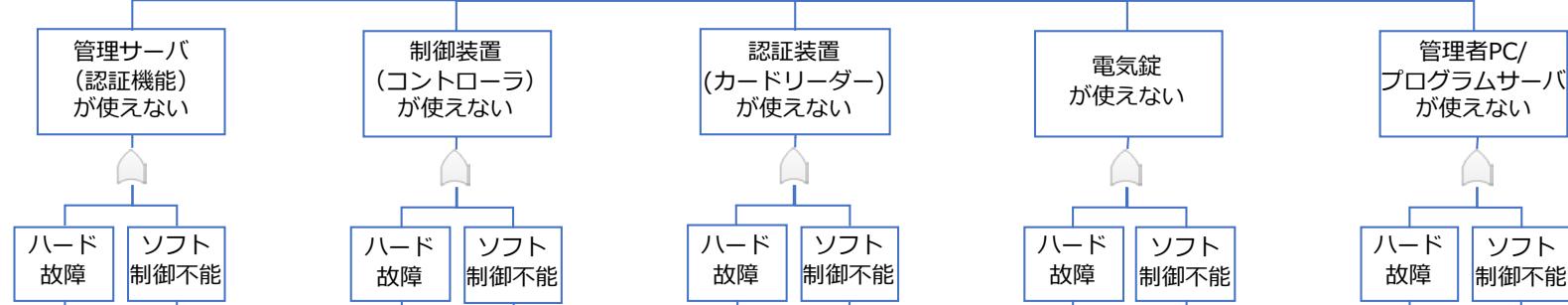
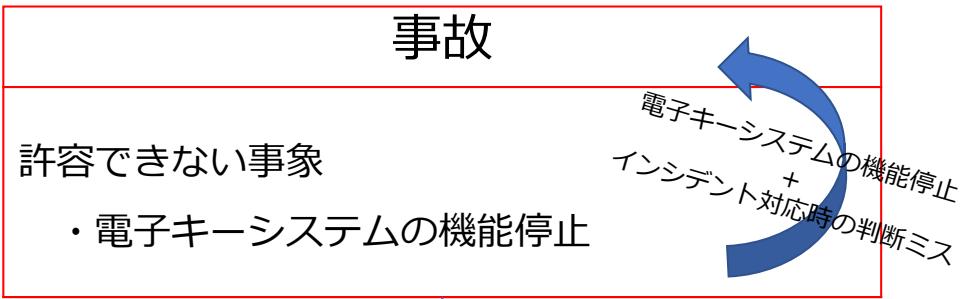


## STEP2

System of  
Systems Analysis

# STEP 1

Consequence  
Prioritization



# STEP2

System of  
Systems  
Analysis

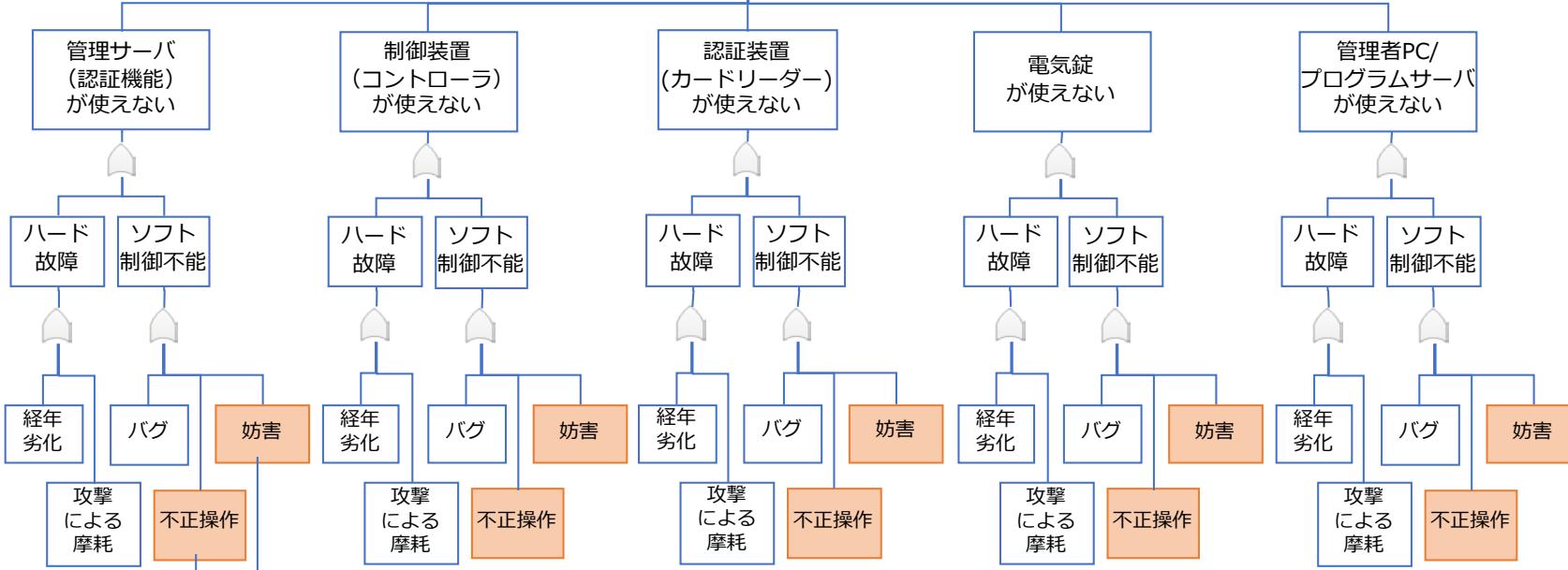
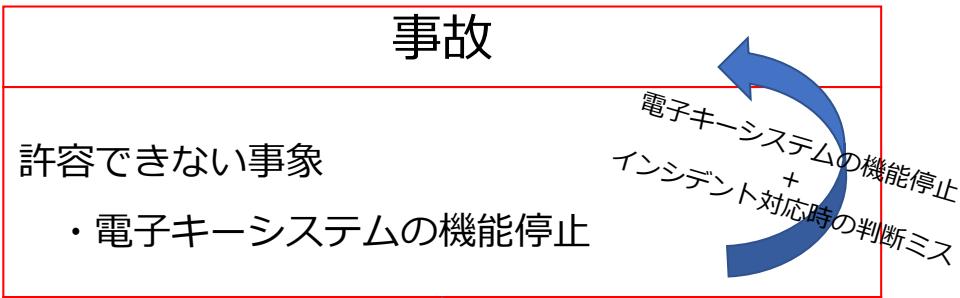
# STEP 1

Consequence  
Prioritization



# STEP2

## System of Systems Analysis

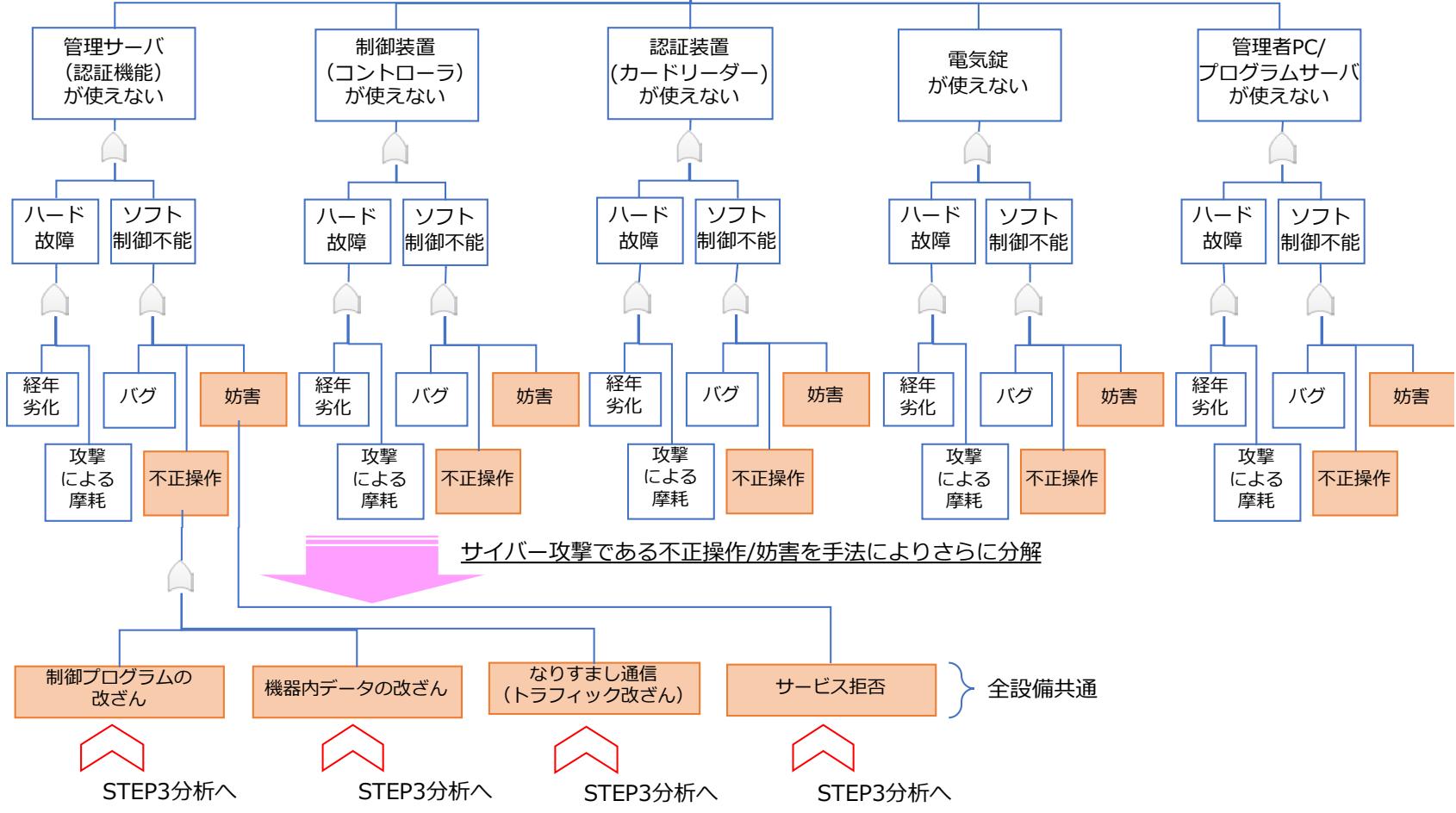
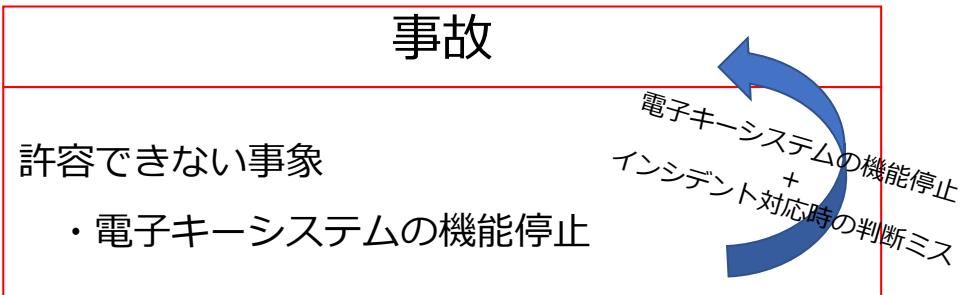


# STEP 1

## Consequence Prioritization



## STEP2 System of Systems Analysis



## STEP2

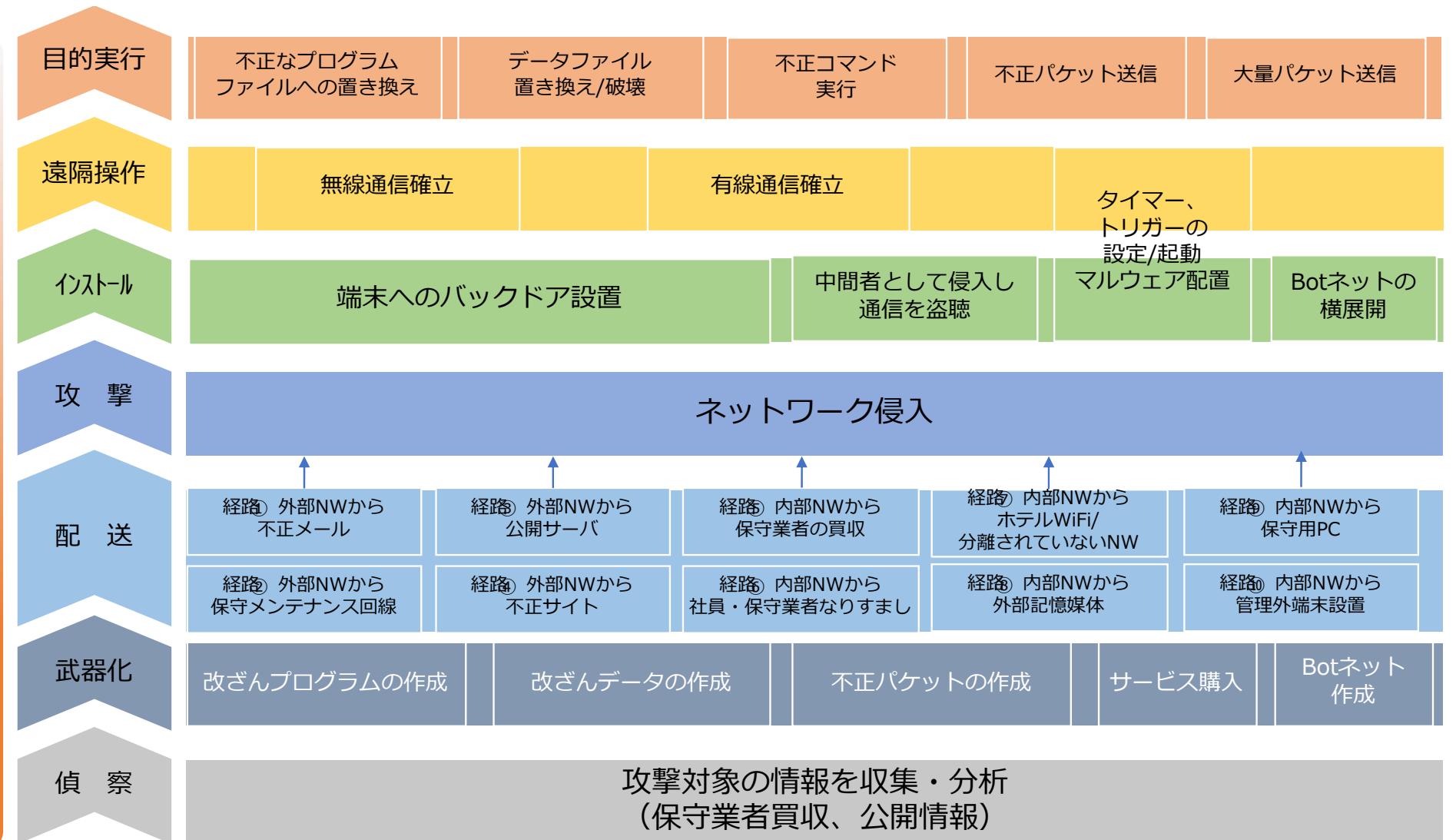
### System of Systems Analysis



STEP2 :  
不正操作/妨害へ

## STEP3

### Consequence-Based Targeting



# ネットワーク侵入の前で攻撃を断ち切る/検知することを、組織として設定（赤点線）

解説

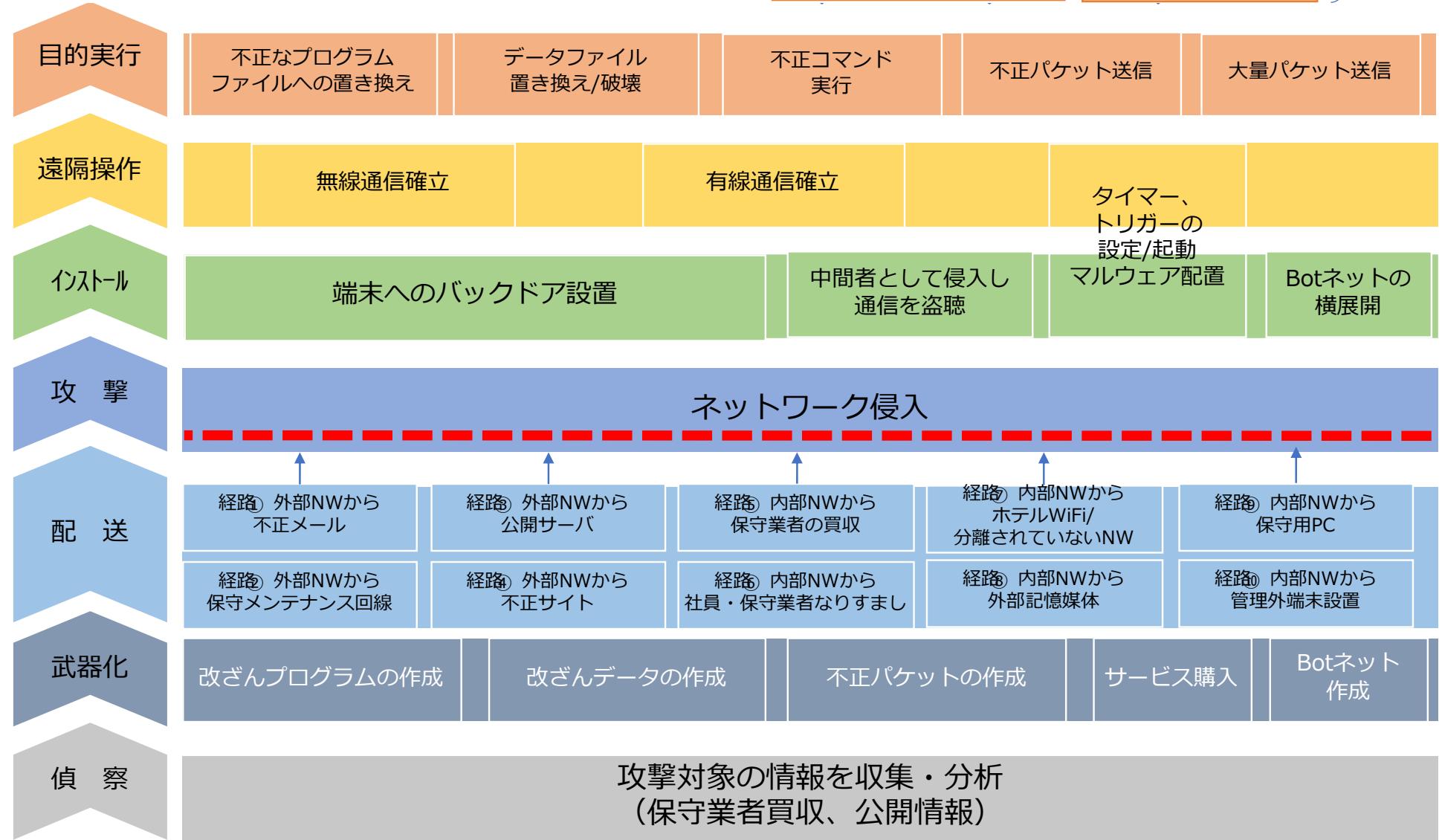
制御プログラムの改ざん

機器内データの改ざん

なりすまし通信  
(トラフィック改ざん)

サービス拒否

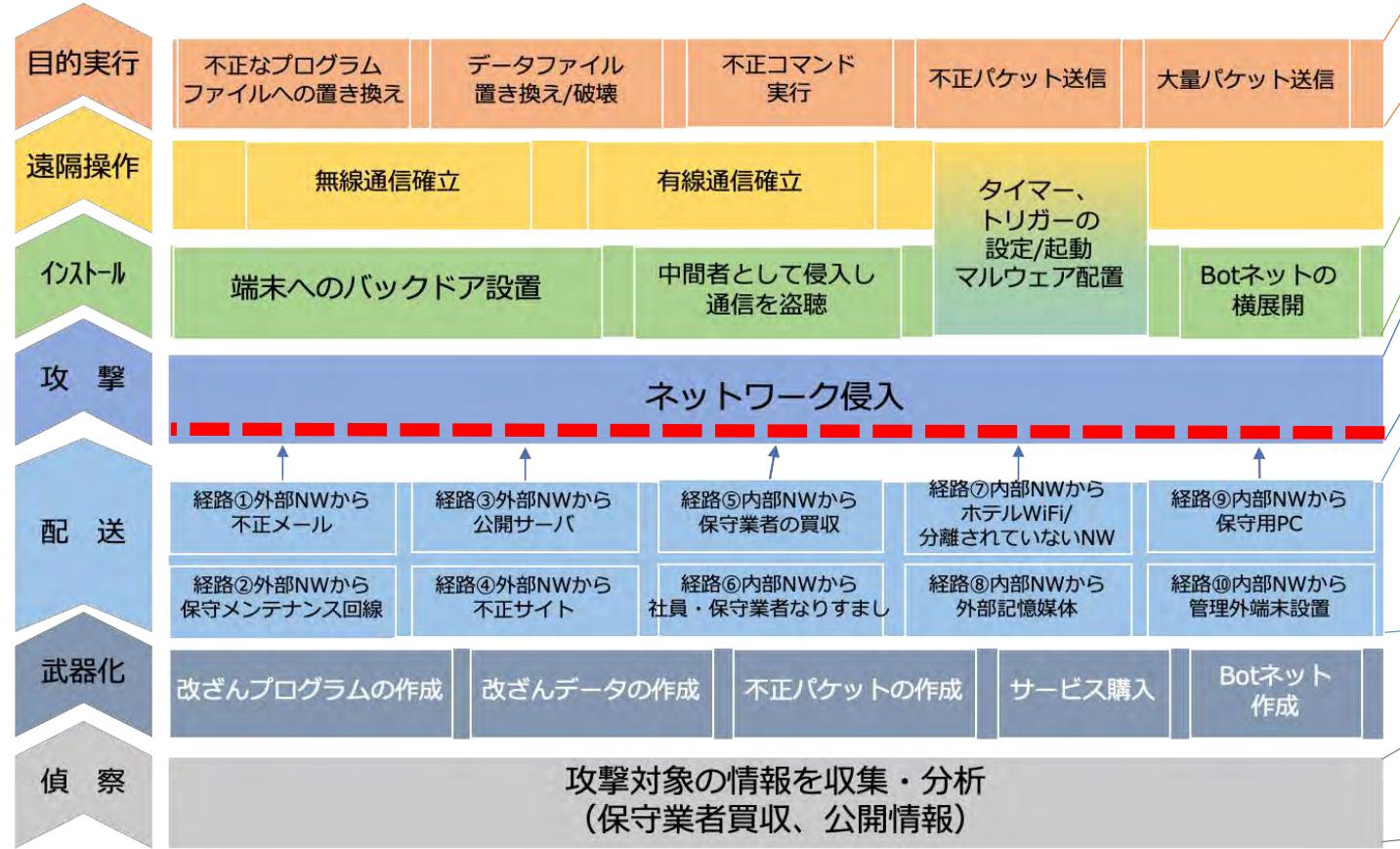
全設備共通



# STEP4の実施結果例

「サイバーキルチーン」のフェーズに沿ってセキュリティ対策を検討する。  
それぞれの対策にレベルを設定し、自社の経営方針に合わせた対策計画を立案する。

- 松 : ビルガイドラインに具体的に記載はないが、対策効果が大きいもの。  
ただし導入や運用にかかるコストが大きい等の負荷もある
- 竹 : ビルガイドラインに記載があり、導入・変更でBA構成への影響が大きいもの
- 梅 : ビルガイドラインに記載があり、導入・変更でBA構成への影響が軽微なもの



対策内容(例)	レベル
バックアップ	
セキュアSW導入	
通信暗号化	
IDS	
IPS	
ふるまい検知	
NW接続認証	
アンチウィルスソフト導入	
メールフィルタ	
URLフィルタ	
資産管理	
VPN接続	
FW導入	
WAF導入	
立入制限/施錠	
入退室ユーザー登録	
NWセグメント分割	
機器接続ポートブロック	
管理外USBメモリ禁止	
脆弱性情報収集	
ハニー波特設置	
セキュリティ啓発	
設備構成把握の徹底	
(共通の対策)ログの記録	

投影のみとさせていただきます

Cyber Kill Chainでのフェーズ	対策内容	対策レベル			該当するビルガイド イン"対策ポリシー"
		梅	竹	松	
目的実行	早期に復旧できるように定期的なバックアップ(データ、システム)を実施しておく。	<input type="radio"/>			・ 0211P1
	防御機能を備えたネットワークスイッチを導入し、サイバー攻撃を遮断する。		<input type="radio"/>		・ 2141P1 ・ 2151P1 ・ 2441P1 ・ 2451P1 ・ 3111P1 ・ 3121P1 ・ 3131P1
遠隔操作	-				-
インストール	通信プロトコルの内、データを暗号化する仕様のものを優先的に活用する。		<input type="radio"/>		-
攻撃	ネットワーク監視ツール導入(IDS)により、不審な通信を早期に検知できるようにする。	<input type="radio"/>			・ 2151P1 ・ 3131P1
	ネットワーク監視ツール導入(IPS)により、不審な通信を早期に遮断できるようにする。		<input type="radio"/>		-
	ネットワーク監視について、未知の脅威のために検知・遮断できないようなサイバー攻撃についても、その挙動などにより対応できるようにする(ふるまい検知)		<input type="radio"/>		-
	自社のセキュリティポリシーを満たせない機器については、ネットワークに接続しても通信ができないようにする。(検疫ネットワーク、RADIUS認証など)		<input type="radio"/>		・ 0221P1 ・ 1411P1 ・ 2181P1 ・ 2491P1 ・ 3171P1
	各機器にアンチウィルスソフトを導入しマルウェア感染を防ぐ。さらに、パターンデータ配信などの更新機能にも適応し、最新のマルウェアに対応できるようにする。	<input type="radio"/>			・ 1411P1
	不審な電子メールを隔離するメールフィルタ機能を設けて、メールを利用したサイバー攻撃を抑止する。	<input type="radio"/>			・ 1211P1 ・ 1311P1
	自社ネットワークからインターネットへ接続する際に、フィッシングサイトなどの危険なWebサイトの閲覧を制限できるようにする(URLフィルター)。	<input type="radio"/>			・ 1211P1 ・ 1311P1
	資産管理ツール導入により、不正な接続機器の把握や各機器での変更操作履歴の収集、アプリインストール制限をすることで、攻撃活動を把握・分析したり、バックドアプログラムの設置を抑止したりする。		<input type="radio"/>		・ 1031P1 ・ 2131P1 ・ 2141P1 ・ 3111P1 ・ 3121P1

Cyber Kill Chainでのフェーズ	対策内容	対策レベル			該当するビルガイドライン“対策ポリシー”	立入制限/施錠を徹底する。	○	・2021P2 ・2021P1 ・2021P2 ・2111P1 ・2411P1 ・2411P2 ・2421P1
		梅	竹	松				
目的実行	早期に復旧できるように定期的なバックアップ(データ、システム)を実施しておく。	○			・0211P1	配送	○	・2011P2 ・2021P1 ・2021P2 ・2111P1 ・2411P1 ・2411P2 ・2421P1 ・3161P1
	防御機能を備えたネットワークスイッチを導入し、サイバー攻撃を遮断する。		○		・2141P1 ・2151P1 ・2441P1 ・2451P1 ・3111P1 ・3121P1 ・3131P1			
遠隔操作	-				-			
インストール	通信プロトコルの内、データを暗号化する仕様のものを優先的に活用する。		○	-				
攻撃	ネットワーク監視ツール導入(IDS)により、不審な通信を早期に検知できるようにする。	○			・2151P1 ・3131P1	事業・業務に応じてネットワークセグメントを分割し最低限の通信のみ許可することで、サイバー攻撃による悪影響が拡がることを抑制する。	○	・1011P1 ・1021P1
	ネットワーク監視ツール導入(IPS)により、不審な通信を早期に遮断できるようにする。		○	-				
	ネットワーク監視について、未知の脅威のために検知・遮断できないようなサイバー攻撃についても、その挙動などにより対応できるようにする(ふるまい検知)		○	-				
	自社のセキュリティポリシーを満たせない機器については、ネットワークに接続しても通信ができないようにする。(検疫ネットワーク、RADIUS認証など)		○		・0221P1 ・1411P1 ・2181P1 ・2491P1 ・3171P1			
	各機器にアンチウイルスソフトを導入しマルウェア感染を防ぐ。さらに、パターンデータ配信などの更新機能にも適応し、最新のマルウェアに対応できるようにする。	○			・1411P1			
配送	不審な電子メールを隔離するメールフィルタ機能を設けて、メールを利用したサイバー攻撃を抑止する。	○			・1211P1 ・1311P1	武器化	・2191P1 ・2191P2 ・24101P1 ・24101P2 ・3181P1 ・3181P2	
	自社ネットワークからインターネットへ接続する際に、フィッシングサイトなどの危険なWebサイトの閲覧を制限できるようにする(URLフィルター)。	○			・1211P1 ・1311P1			
	資産管理ツール導入により、不正な接続機器の把握や各機器での変更操作履歴の収集、アプリインストール制限をすることで、攻撃活動を把握・分析したり、バックドアプログラムの設置を抑止したりする。		○		・1031P1 ・2131P1 ・2141P1 ・3111P1 ・3121P1			
	リモートで自社ネットワークへ接続する際はVPN機能を導入して、接続認証とデータ暗号化を行う。	○			・2461P1 ・3141P1			
	公開サーバなど、インターネットから接続される機器については、その境界にサイバー攻撃への防護や通信先を制限する機能を設ける。(FW導入)	○			・1031P1 ・1111P1 ・1211P1 ・1311P1			
	Webアプリケーションファイアウォールを導入する。(WAF)		○		・1111P1 ・1211P1 ・1311P1			
	立入制限/施錠を徹底する。	○			・2011P1 ・2011P2 ・2021P1 ・2021P2 ・2111P1 ・2411P1 ・2411P2 ・2421P1			
共通的考え方						運用する機器のログを記録し解析する。 入退室や、ユーザー操作などの履歴を記録し解析する。	○ ○	・2011P1 ・2011P2 ・2021P1 ・2121P1 ・2131P1 ・2141P1 ・2151P1 ・2431P1 ・2441P1 ・2451P1 ・3011P1 ・3111P1 ・3121P1 ・3131P1

# 事例：フィンランドのビル暖房停止



出典：  
Metropolitan.fi



出典：  
ETELA-SAIMAA

発生日	2016年11月
発生国・箇所	フィンランド・ラッペーンランタ
攻撃手法	DDoS攻撃
影響	ビル暖房停止

## 概要

2016年11月、フィンランド東部ラッペーンランタの集合住宅の暖房・給湯システムが攻撃を受けて停止し、**暖房と給湯の機能が利用不可**になった。

インターネット経由で遠隔制御されていた暖房・給湯の**制御システムに対してDDoS攻撃**が行われた。その結果、システムの再起動が何度も引き起こされていた。

11月のフィンランドは既に外気温マイナス2度の環境であり、このような中で、数時間に渡って暖房が利用出来ない状況が継続した。

## 参考 URL

- Metropolitan.fi  
<http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter>
- ETELÄ-SAIMAA  
<https://esaimaa.fi/uutiset/lahella/64208f0e-81b9-4a41-ad68-df8fa521224f>

# 事例：フィンランドのビル暖房停止

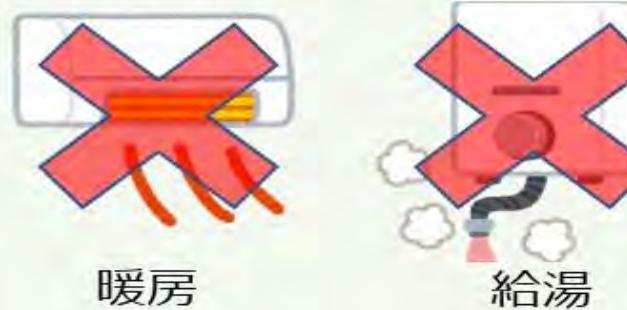
2016年11月、フィンランドのラッペーンランタで集合住宅の暖房・給湯システムがサイバー攻撃を受け、停止に追い込まれた。

攻撃者がインターネット経由で遠隔集中制御されていたビル暖房・給湯システムに対して  
**DDoS攻撃**を実施



制御系システムがシステム停止に追い込まれた  
→暖房・給湯を使えない状態が発生

住宅の暖房・給湯



DDoS攻撃とは：  
複数のコンピューターから標的のサーバーに、  
ネットワークを介した大量の処理要求を送ることでサービスを停止させてしまう攻撃

臨時措置として、ネットワークの通信量を制限した



# リスク分析手法は他にも



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

「IPA 制御システムガイド」で検索

★以下2つのリスク分析手法について、手順を掲載

- 資産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
  - \* 攻撃ツリーを用いた、事業被害シナリオを想定

ATA (Attack Tree Analysis) 、FTA (Fault Tree Analysis)についても補完的に採用されている。

1. 本セッションの論点・目的
2. 経産省 ビルセキュリティガイドライン解説
3. ケーススタディ “リスク分析から対策優先度をつけてみる”
4. まとめ

# まとめ

- ✓ ビル制御システムは、IT系と同じようなセキュリティ対策を講じることが難しい背景をご説明いたしました。
- ✓ セキュリティガイドラインに記載されている対策に関して、  
ビル制御システムのリスクを正しく認識いただけるようご説明したうえで解説いたしました。
- ✓ だからこそ、ビルセキュリティガイドラインには基本的なことが書かれており、その読み方や内容について解説いたしました。
- ✓ どこから対策すれば良いかを明確にするために、CCEという手法を用いたリスク分析作業を追体験していただきました。  
→ビル制御システムでは、「ネットワーク侵入」段階に至るまでに防ぐことが重要
- ✓ ビル業界におけるセキュリティ対策のファーストステップを踏み出すため、お手元の「CCEリスク分析ワークシート」を、ぜひご活用いただけすると幸いです。

ご清聴ありがとうございました

問合せ先

E-mail: [c18gpr\\_bagl@ml.icscoe.jp](mailto:c18gpr_bagl@ml.icscoe.jp)

IPA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  
2期修了生有志 ビルチーム一同

次ページ以降は、  
制御システムのリスク分析のために  
付属したワークシートです。

ぜひ、ご活用ください。

# MPOWER19ワークシート1 (CCEリスク分析)

# リスク分析手法

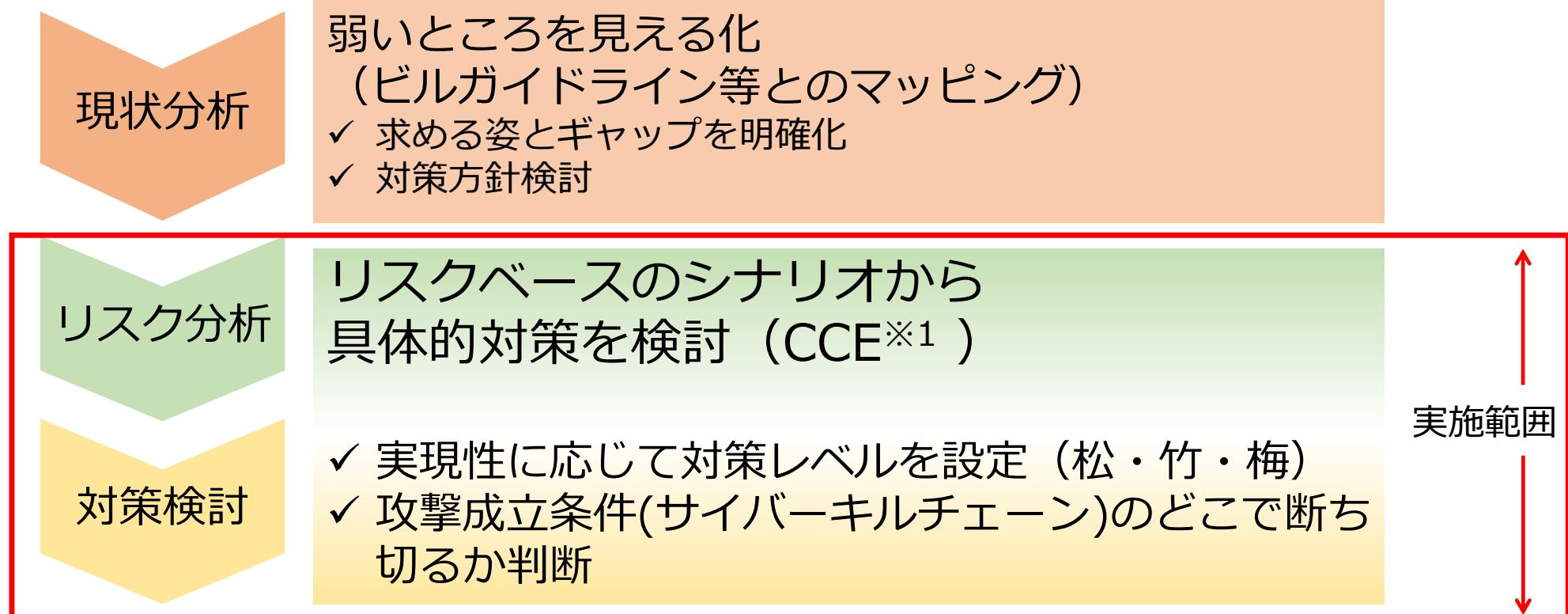
- ✓ ガイドラインに記載の対策は、もちろんすべてを実施できることが望ましい。
- ✓ しかしながら、ビルの規模や特性、対策にかかる費用によってはそれが難しい場合もある。（セキュリティはどうしても費用として見られてしまう）
- ✓ セキュリティ専門家は“対策は全部すべき”とよく言うが“全部”なんて不可能。

**セキュリティ対策の優先度付けが有効**

## リスク分析の必要性

「許容できない事象／許容できる事象の見極め」  
「許容できない事象に関して、費用をかけて断ち切るべきポイント（優先度の高い対策）の設定」

# リスク分析アプローチ



※1 CCE: Consequence-driven Cyber-Informed Engineering (The Idaho National Lab (INL))

## 事例：● ●

状況がわかる写真やイメージ図を貼付

出典：出典箇所を記載

発生日

発生国・箇所

攻撃手法

影響

### 概要

リスク分析対象とする事業被害を引き起こすセキュリティインシデントの概要を記述してください。

- ・サイバー攻撃内容
- ・事業インパクト
- ・対処内容

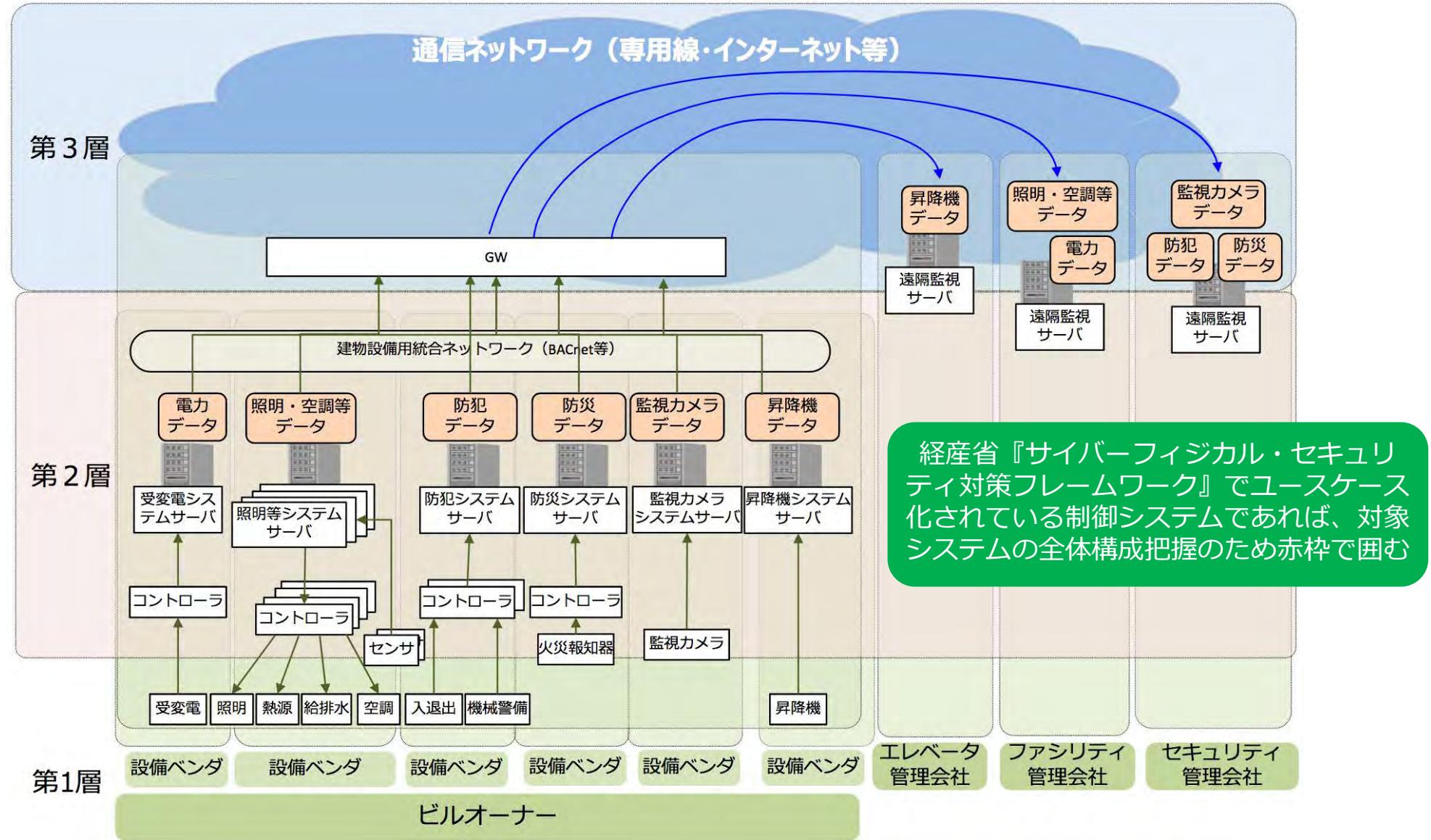
### 参考 URL

リスク分析にあたり、類似した事例などの公開情報参照先を記載。  
可能な限り2サイト以上記載。

## 事例： ● ●

図解

- ・リスク分析対象の事業被害を引き起こすための具体的な攻撃手法が分かっている場合は、その解説を記載する。
- ・分からぬ場合は概要からイメージを作成する。

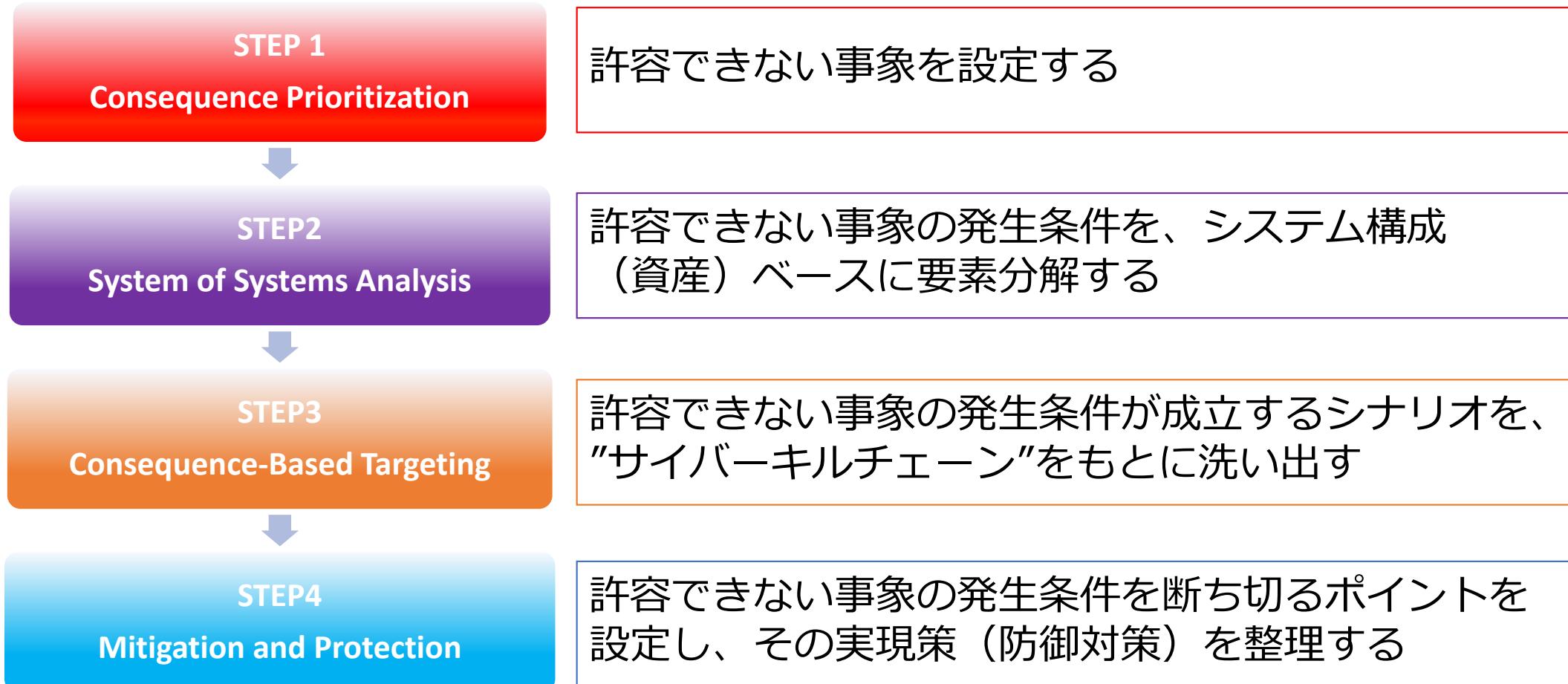


## ● ● システムの構成を整理

CCE STEP2で構成物品ごとに分解していくため、  
構成図を貼付

「許容できない事象」を起こさないための対策を考える手法を採用

## Consequence-driven C<sub>yber</sub>-Informed E<sub>ngineering</sub>(CCE)



## STEP 1

Consequence  
Prioritization

事故

許容できない事象

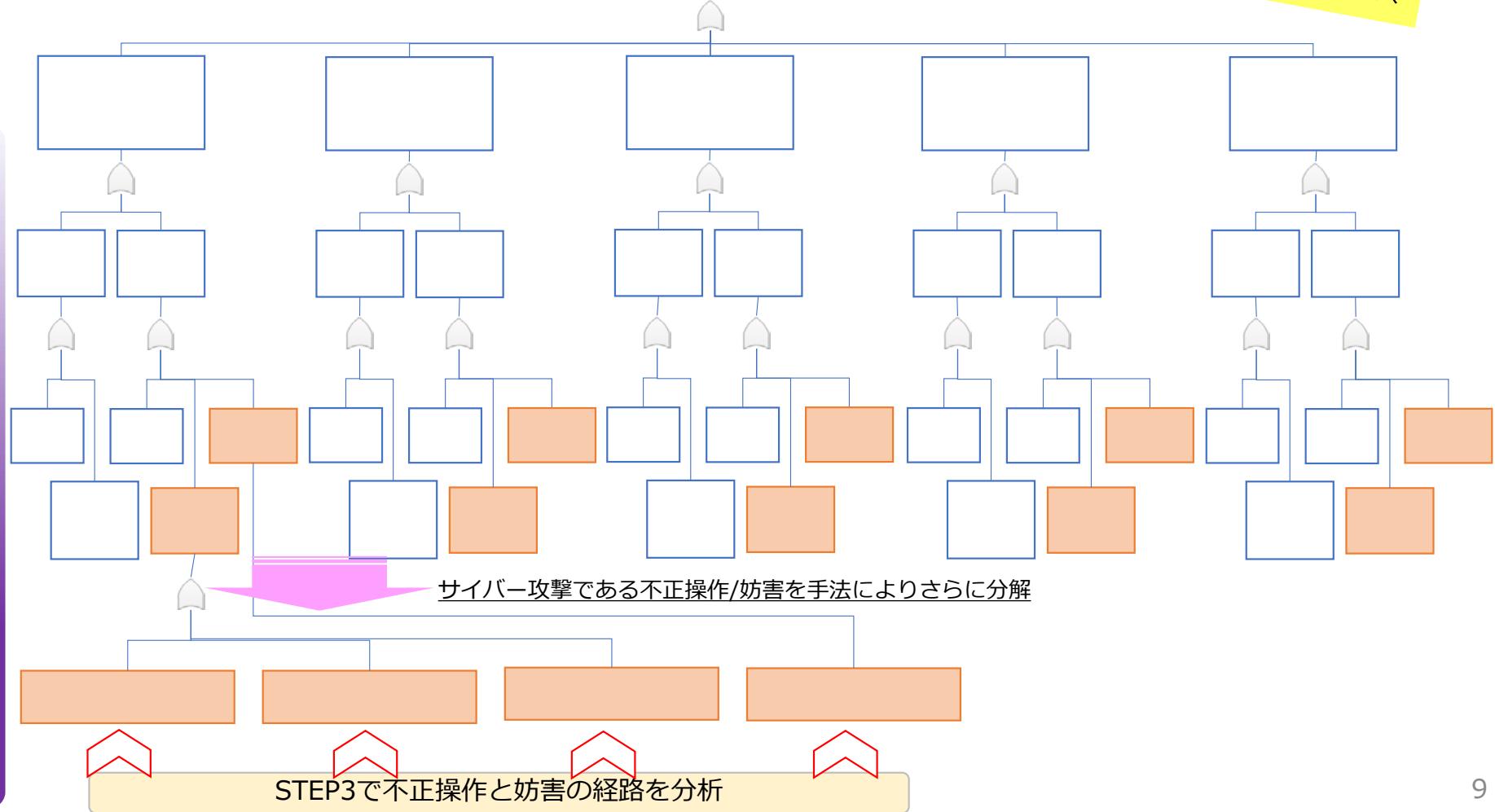
- ● の機能停止

● ● の機能停止  
+  
インシデント対応時の判断ミス



## STEP 2

System of  
Systems  
Analysis



## STEP2

System of  
Systems Analysis

STEP2 :  
不正操作/妨害へ

攻撃手法A

攻撃手法B

攻撃手法C

攻撃手法D

目的実行

遠隔操作

インストール

攻撃

配 送

武 器 化

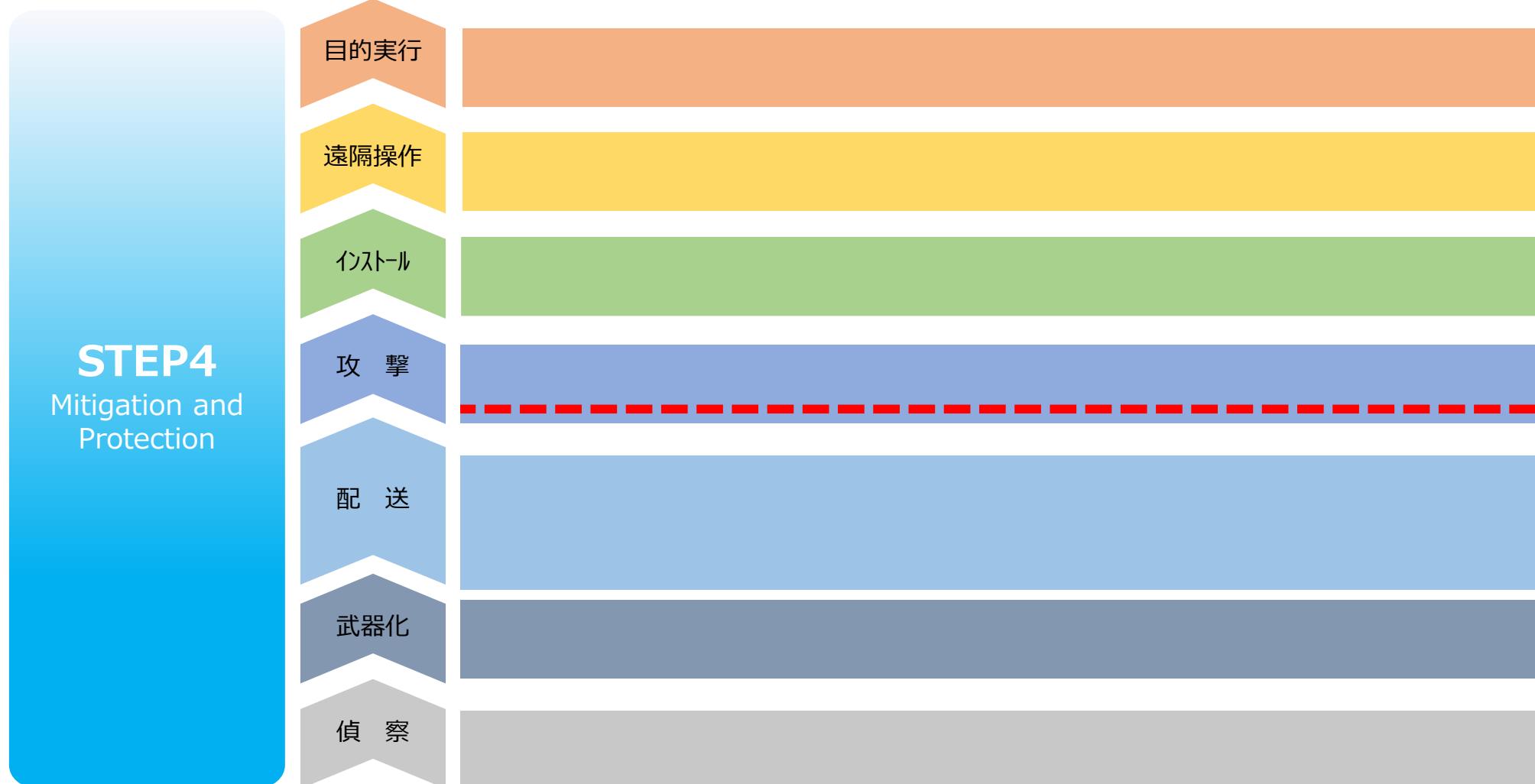
偵 察

## STEP3

Consequence-  
Based Targeting

0

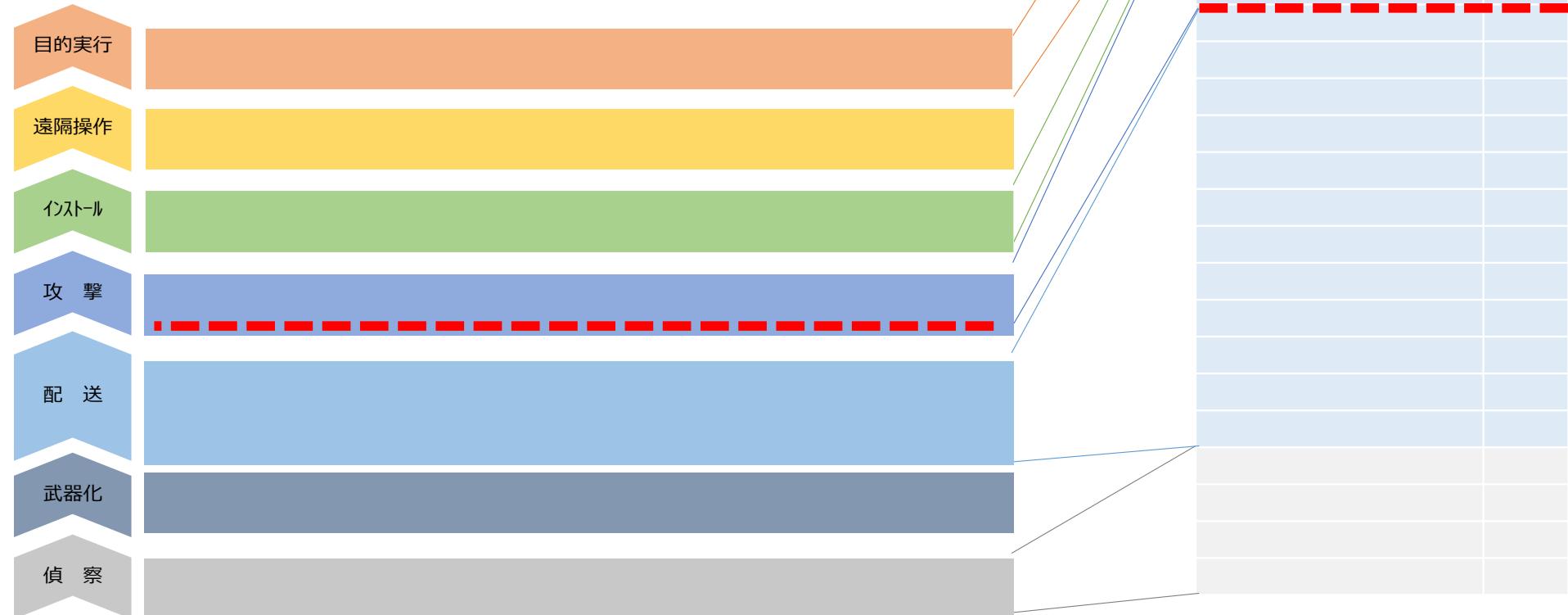
“〇〇”(サイバーキルチェーンの攻撃段階名称)の前で攻撃を断ち切る/検知することを、組織として設定（赤点線）



## STEP4の実施結果例

「サイバーキルチーン」のフェーズに沿ってセキュリティ対策を検討する。  
それぞれの対策にレベルを設定し、自社の経営方針に合わせた対策計画を立案する。

- 松  : ビルガイドラインに具体的に記載はないが、対策効果が大きいもの。  
ただし導入や運用にかかるコストが大きい等の負荷もある
- 竹  : ビルガイドラインに記載があり、導入・変更でシステムへの影響が大きいもの
- 梅  : ビルガイドラインに記載があり、導入・変更でシステムへの影響が軽微なもの



## STEP4の実施結果例

- ①『MPOWER19ワークシート2（リスク分析\_対策一覧例）.xlsx』 -> 「Worksheet」に、対策一覧を記載する。  
※参考：同ファイル  
「オーストリアでのホテル宿泊客閉じ込め・閉め出し」シート  
「フィンランドのビル暖房停止」シート
- ②松・竹・梅の基準に従い優先度付けを行う。
- ③設定した対策が、ビルガイドラインの対策要件No.のどれに該当するか、マッピングする。

## MPOWER19ワークシート2（リスク分析\_対策一覧例）.xlsx

## Worksheet

## 対策レベルの概観

&lt;松&gt;

ビルガイドラインに具体的に記載はないが、対策効果が大きいもの。ただし導入や運用にかかるコストが大きい等の負荷もある

&lt;竹&gt;

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が大きいもの

&lt;梅&gt;

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が軽微なもの

Cyber Kill Chainでのフェーズ	対策内容	対策レベル			該当するビルガイドライン”対策ポリシー”
		梅	竹	松	
目的実行					
遠隔操作					
インストール					
攻撃					
配送					
武器化					
偵察					
共通的考え方					

MPOWER19ワークシート2（リスク分析\_対策一覧例）.xlsx  
オーストリアでのホテル宿泊客閉じ込め・閉め出し（サンプル1）

対策レベルの概観

<松>

ビルガイドラインに具体的に記載はないが、対策効果が大きいもの。ただし導入や運用にかかるコストが大きい等の負荷もある

<竹>

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が大きいもの

<梅>

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が軽微なもの

Cyber Kill Chainでのフェーズ	対策内容（例）	対策レベル			該当するビルガイドライン”対策ポリシー”
		梅	竹	松	
目的実行	早期に復旧できるように定期的なバックアップ(データ、システム)を実施しておく。	<input type="radio"/>			<ul style="list-style-type: none"> <li>・ 0211P1</li> <li>・ 2141P1</li> <li>・ 2151P1</li> <li>・ 2441P1</li> <li>・ 2451P1</li> <li>・ 3111P1</li> <li>・ 3121P1</li> <li>・ 3131P1</li> </ul>
	防御機能を備えたネットワークスイッチを導入し、サイバー攻撃を遮断する。			<input type="radio"/>	
遠隔操作	-				-
インストール	通信プロトコルの内、データを暗号化する仕様のものを優先的に活用する。			<input type="radio"/>	-
攻撃	ネットワーク監視ツール導入(IDS)により、不審な通信を早期に検知できるようにする。	<input type="radio"/>			<ul style="list-style-type: none"> <li>・ 2151P1</li> <li>・ 3131P1</li> </ul>
	ネットワーク監視ツール導入(IPS)により、不審な通信を早期に遮断できるようにする。			<input type="radio"/>	-
	ネットワーク監視について、未知の脅威のために検知・遮断できないようなサイバー攻撃についても、その挙動などにより対応できるようにする(ふるまい検知)			<input type="radio"/>	-
	自社のセキュリティポリシーを満たせない機器については、ネットワークに接続しても通信ができないようにする。(検疫ネットワーク、RADIUS認証など)			<input type="radio"/>	<ul style="list-style-type: none"> <li>・ 0221P1</li> <li>・ 1411P1</li> <li>・ 2181P1</li> <li>・ 2491P1</li> <li>・ 3171P1</li> </ul>
防御	各機器にアンチウィルスソフトを導入しマルウェア感染を防ぐ。さらに、パターンデータ配信などの更新機能にも適応し、最新のマルウェアに対応できるようにする。	<input type="radio"/>			<ul style="list-style-type: none"> <li>・ 1411P1</li> </ul>
	不審な電子メールを隔離するメールフィルタ機能を設けて、メールを利用したサイバー攻撃を抑止する。	<input type="radio"/>			<ul style="list-style-type: none"> <li>・ 1211P1</li> <li>・ 1311P1</li> </ul>
	自社ネットワークからインターネットへ接続する際に、フィッシングサイトなどの危険なWebサイトの閲覧を制限できるようにする(URLフィルター)。	<input type="radio"/>			<ul style="list-style-type: none"> <li>・ 1211P1</li> <li>・ 1311P1</li> </ul>
	資産管理ツール導入により、不正な接続機器の把握や各機器での変更操作履歴の収集、アプリインストール制限をすることで、攻撃活動を把握・分析したり、バックドアプログラムの設置を抑止したりする。		<input type="radio"/>		<ul style="list-style-type: none"> <li>・ 1031P1</li> <li>・ 2131P1</li> <li>・ 2141P1</li> <li>・ 3111P1</li> <li>・ 3121P1</li> </ul>
	リモートで自社ネットワークへ接続する際はVPN機能を導入して、接続認証とデータ暗号化を行う。	<input type="radio"/>			<ul style="list-style-type: none"> <li>・ 2461P1</li> <li>・ 3141P1</li> </ul>
	公開サーバなど、インターネットから接続される機器については、その境界にサイバー攻撃への防御や通信先を制限する機能を設ける。(FW導入)	<input type="radio"/>			<ul style="list-style-type: none"> <li>・ 1031P1</li> <li>・ 1111P1</li> <li>・ 1211P1</li> <li>・ 1311P1</li> </ul>
	Webアプリケーションファイアウォールを導入する。（WAF）		<input type="radio"/>		<ul style="list-style-type: none"> <li>・ 1111P1</li> <li>・ 1211P1</li> <li>・ 1311P1</li> </ul>

MPOWER19ワークシート2（リスク分析\_対策一覧例）.xlsx  
オーストリアでのホテル宿泊客閉じ込め・閉め出し（サンプル1）

対策レベルの概観

<松>

ビルガイドラインに具体的に記載はないが、対策効果が大きいもの。ただし導入や運用にかかるコストが大きい等の負荷もある

<竹>

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が大きいもの

<梅>

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が軽微なもの

Cyber Kill Chainでのフェーズ	対策内容（例）	対策レベル			該当するビルガイドライン“対策ポリシー”
		梅	竹	松	
配送	立入制限/施錠を徹底する。	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	・2011P1 ・2011P2 ・2021P1 ・2021P2 ・2111P1 ・2411P1 ・2411P2 ・2421P1
	社内外の作業者について入退室管理を行うため、ユーザー登録を行う。				・2011P2 ・2021P1 ・2021P2 ・2111P1 ・2411P1 ・2411P2 ・2421P1 ・3161P1
	事業・業務に応じてネットワークセグメントを分割し最低限の通信のみ許可することで、サイバー攻撃による悪影響が拡がることを抑制する。	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	・1011P1 ・1021P1
	不正操作のリスクが考えられる機器のポートを物理的または論理的にブロックする。	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	・2311P1 ・3211P1 ・4121P1
	管理外USBメモリの利用を禁止する。	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	・2191P1 ・2191P2 ・24101P1 ・24101P2 ・3181P1 ・3181P2
武器化		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	
偵察	社内外の作業者に対するセキュリティ教育を行う。	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	・0311P1 ・0461P1
	セキュリティ脆弱性情報を収集し、必要に応じて対策を検討する。	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	・0221P1
	脆弱なサーバなどを意図的に設置して、サイバー攻撃者のやり口を分析したり、攻撃されたくない対象を分かりにくくしたりする(ハニーポット)。	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	-
	ビル内の外部接続回線の把握漏れがないように管理する。	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	・1041P1

MPOWER19ワークシート2（リスク分析\_対策一覧例）.xlsx  
オーストリアでのホテル宿泊客閉じ込め・閉め出し（サンプル1）

対策レベルの概観

<松>

ビルガイドラインに具体的に記載はないが、対策効果が大きいもの。ただし導入や運用にかかるコストが大きい等の負荷もある

<竹>

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が大きいもの

<梅>

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が軽微なもの

Cyber Kill Chainでのフェーズ	対策内容（例）	対策レベル			該当するビルガイドライン“対策ポリシー”
		梅	竹	松	
共通的考え方	運用する機器のログを記録し解析する。 入退室や、ユーザー操作などの履歴を記録し解析する。	○	○		・ 2011P1 ・ 2011P2 ・ 2021P1 ・ 2121P1 ・ 2131P1 ・ 2141P1 ・ 2151P1 ・ 2431P1 ・ 2441P1 ・ 2451P1 ・ 3011P1 ・ 3111P1 ・ 3121P1 ・ 3131P1

## MPOWER19ワークシート2（リスク分析\_対策一覧例）.xlsx

## フィンランドのビル暖房停止（サンプル2）

## 対策レベルの概観

&lt;松&gt;

ビルガイドラインに具体的に記載はないが、対策効果が大きいもの。ただし導入や運用にかかるコストが大きい等の負荷もある

&lt;竹&gt;

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が大きいもの

&lt;梅&gt;

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が軽微なもの

Cyber Kill Chainでのフェーズ	対策内容（例）	対策レベル			該当するビルガイドライン"対策ポリシー"
		梅	竹	松	
目的実行	ネットワーク監視ツール(IDS等)の導入により、DDoS攻撃を早期に検知できるようにする。	○			・2141P1 ・2151P1 ・2441P1 ・2451P1 ・3111P1 ・3121P1 ・3131P1
	ネットワーク監視ツール(IPS等)の導入により、DDoS攻撃を遮断できるようにする。				・2141P1 ・2151P1 ・2441P1 ・2451P1 ・3111P1 ・3121P1 ・3131P1
	防御機能を備えたネットワークスイッチを導入し、サイバー攻撃を遮断する。				・2141P1 ・2151P1 ・2441P1 ・2451P1 ・3111P1 ・3121P1 ・3131P1
遠隔操作	-				
インストール	-				
攻撃	外部との通信について、不要な通信先やポートでの通信を許可しない。	○			・1031P1 ・1111P1 ・1121P1 ・1311P1
	遠隔制御の通信元を認証する。（特定の通信元からの指示しか受け付けない）				・1111P1 ・1411P1 ・2461P1 ・3141P1 ・3311P1
	インターネットに公開する制御部分と、フィールド設備をネットワーク分割し、インターネットに公開するものののみDMZに配置する。				・1011P1 ・1021P1 ・1111P1 ・1311P1
配送	制御機器のパスワードをデフォルトID、パスワードから変更する。		○		・3151P1
武器化	-				
偵察	社内外の作業者に対するセキュリティ教育を行う。	○			・0311P1 ・0461P1
	ネットワーク監視ツール(IDS等)の導入により、スキャン行為を早期に検知できるようにする。				・2171P1 ・2481P1
	ネットワーク監視ツール(IPS等)の導入により、スキャン行為を遮断できるようにする。				・2171P1 ・2481P1
	セキュリティ脆弱性情報を収集し、必要に応じて対策を検討する。				・0221P1

MPOWER19ワークシート2（リスク分析\_対策一覧例）.xlsx  
フィンランドのビル暖房停止（サンプル2）

対策レベルの概観

<松>

ビルガイドラインに具体的に記載はないが、対策効果が大きいもの。ただし導入や運用にかかるコストが大きい等の負荷もある

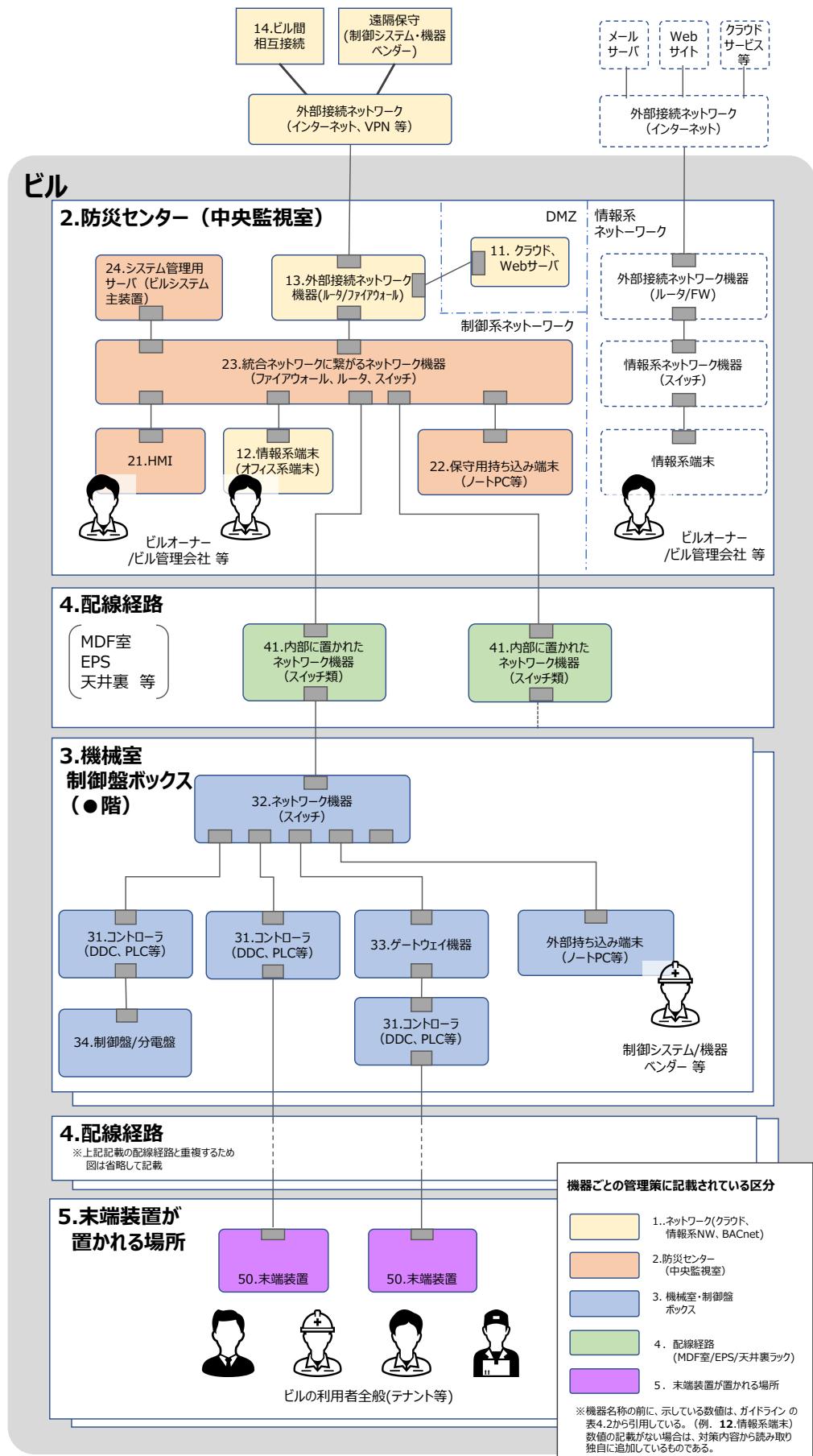
<竹>

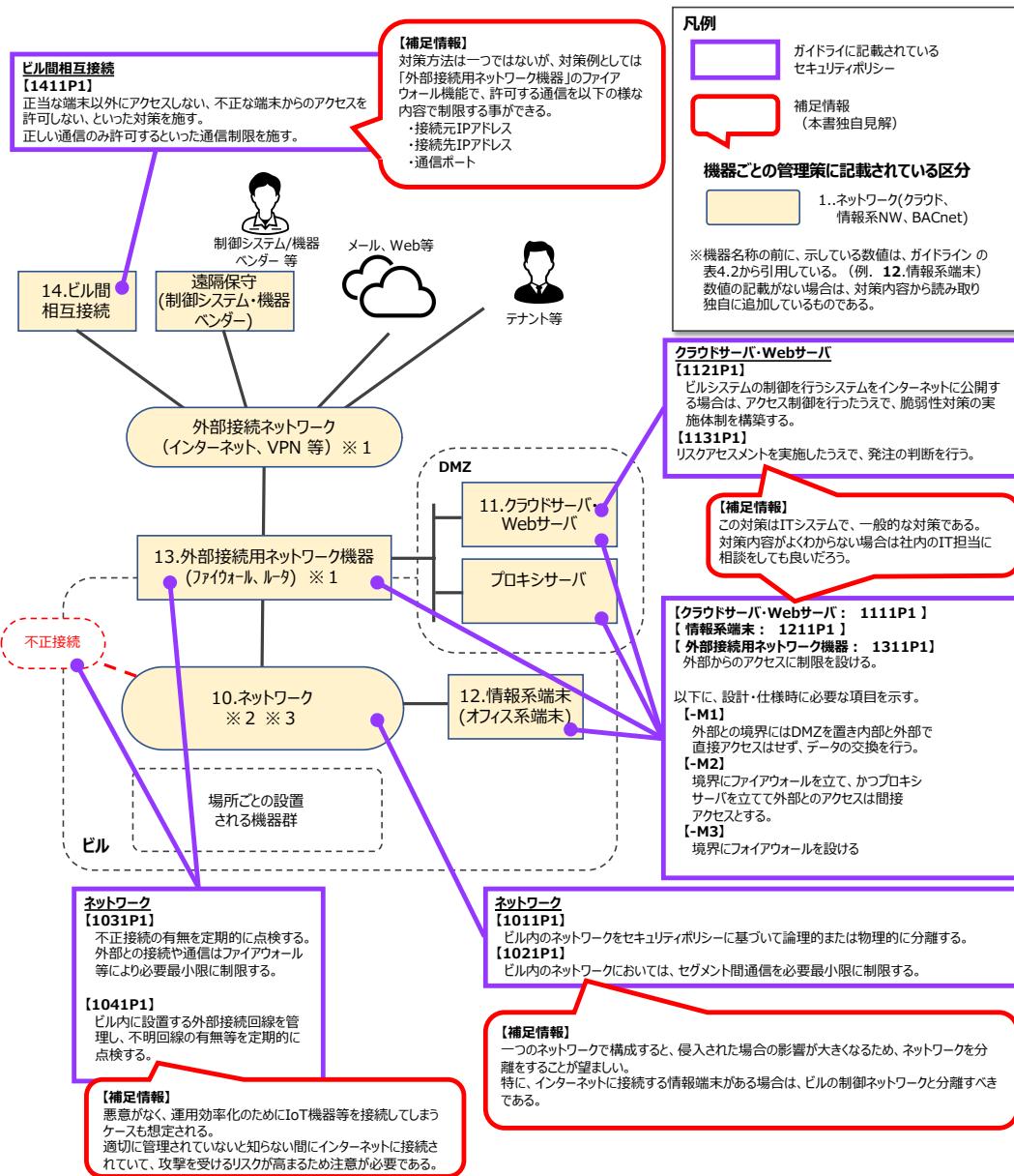
ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が大きいもの

<梅>

ビルガイドラインに記載があり、設備導入・変更でシステム構成への影響が軽微なもの

Cyber Kill Chainでのフェーズ	対策内容（例）	対策レベル			該当するビルガイドライン“対策ポリシー”
		梅	竹	松	
共通的考え方	運用する機器のログを記録し解析する。 入退室や、ユーザー操作などの履歴を記録し解析する。	○	○		・ 2011P1 ・ 2011P2 ・ 2021P1 ・ 2121P1 ・ 2131P1 ・ 2141P1 ・ 2151P1 ・ 2431P1 ・ 2441P1 ・ 2451P1 ・ 3011P1 ・ 3111P1 ・ 3121P1 ・ 3131P1





※1：外部に接続する回線（インターネット、専用線等）、外部接続用ネットワーク機器は、一つの様に図示しているが、実際は複数ある場合もあるため、ビル毎の環境にあわせて読みかえること。

※2：ビル内ネットワークには、様々な機器が繋がれ、実際はより複雑な構成となると想定される。

ガイドライン「図3-3 ビルシステムの標準的なモデル」を参考にしビル毎の環境にあわせて読みかえること。

※3：ここで示しているネットワークは、論理的な表現となっているため、物理的には複数のネットワーク機器（ファイアウォール、ルータ、スイッチ等）で構成される。

