物理・サイバーセキュリティで支えるOT環境
～建設業の実践アプローチ～

2025年5月9日

株式会社　竹中工務店

情報エンジニアリング本部
西園　健吾

デジタル室
鈴木　真徳

TAKENAKA

目次

1. はじめに
   - 自己紹介
   - 会社概要、当社の主な作品

2. OT環境における物理セキュリティの重要性について

3. 施設における脅威とその対策

4. 重要機能室の物理的防護

5. 建設業におけるサイバーセキュリティの現状と取り組み

自己紹介

氏名：西園　健吾（Nishizono Kengo）

所属：情報エンジニアリング本部
　　情報エンジニアリング2グループ

経歴：
- 化学メーカーの火力発電設備の計装設備の設備改修・保全工事を担当
- 2019年 竹中工務店入社　以下の業務に従事
  ー建設プロジェクトにおけるネットワーク(OA/BA/FA)・セキュリティ関連の設計・施工支援
  ースマートビル分野の技術開発（ビルOS(ビルコミ®)関連等）

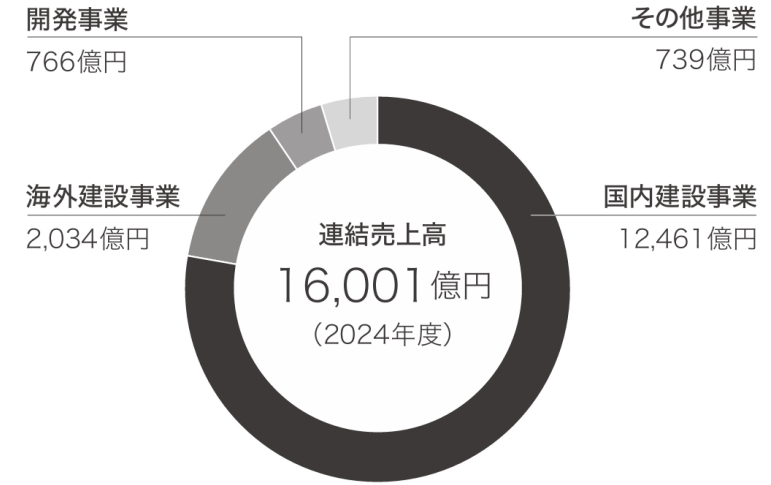
資格：
　ボイラー整備士、エネルギー管理士(電気)、プロジェクトマネージャ等

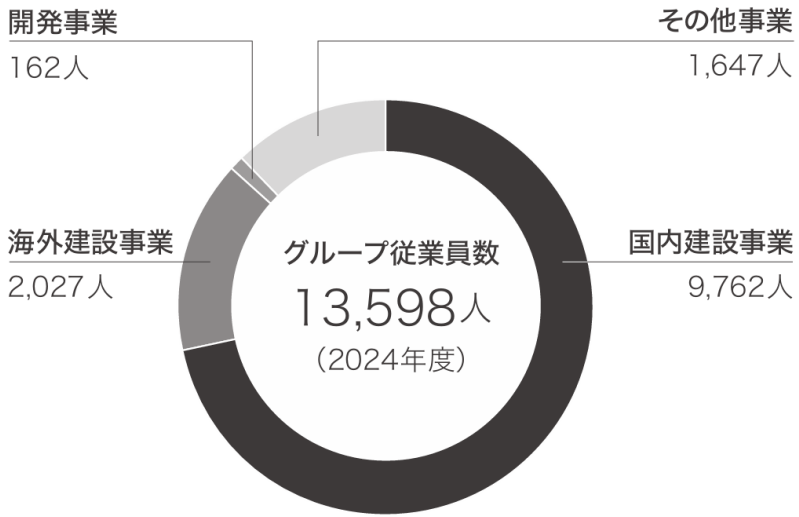
会社概要

竹中工務店

主要事業内容	**・建設工事に関する請負・設計及び監理** ・不動産の売買、賃貸、仲介、斡旋、保守、管理及び鑑定並びに不動産投資に関するマネジメント他
本社所在地	**大阪市中央区本町4-1-13**
従業員数 (2025年1月)	**単体：7,804名** （グループ全体：13,598名）
グループ会社	子会社55社、関連会社13社 その他関係会社1社
沿革	**創業1610年（慶長15年）** **創立1899年（明治32年）**

竹中グループの事業規模





TAKENAKA

当社の主な作品

近年

- 長崎スタジアムシティ（2024年）
- 大阪梅田ツインタワーズ・サウス（2022年）
- 東京ミッドタウン八重洲（2022年）
- 渋谷　パルコ・ヒューリックビル（2019年）
  など。

過去

- 東京ドーム（1988年）
- 日本武道館（1964年）
- 東京タワー（1958年）
  など。

大阪梅田ツインタワーズ・サウス　渋谷 パルコ・ヒューリックビル

東京ミッドタウン八重洲　あべのハルカス・てんしば

竹中工務店　会社案内より

TAKENAKA

本講演のゴール

- 聴講者の皆様にご理解いただきたい内容

1. **物理セキュリティとサイバーセキュリティの関係性、多層防御の考え方を理解いただく**
2. **施設における脅威と対策立案の流れ、対策例を理解いただく（浸水対策・重要機能室防護）**
3. **建設業特有のセキュリティ課題と実践的な対応方法を理解いただく**

目次

最近の事例

- 近年工場などの敷地への侵入、現場資材の窃盗などの被害が増加

【いったい誰が?何の目的で?】火力発電所に何者かが侵入「北海道電力・苫東厚真発電所」で被害―"門の鍵"壊し車で忍び込む‥‥警察に被害届を提出、不審物は発見されず＜北海道厚真町＞

北海道文化放送　2025年5月7日 水曜 午前11:50

FNNプライムオンライン：【いったい誰が？何の目的で？】火力発電所に何者かが侵入
https://www.fnn.jp/articles/UHB/868107 2025.5.7

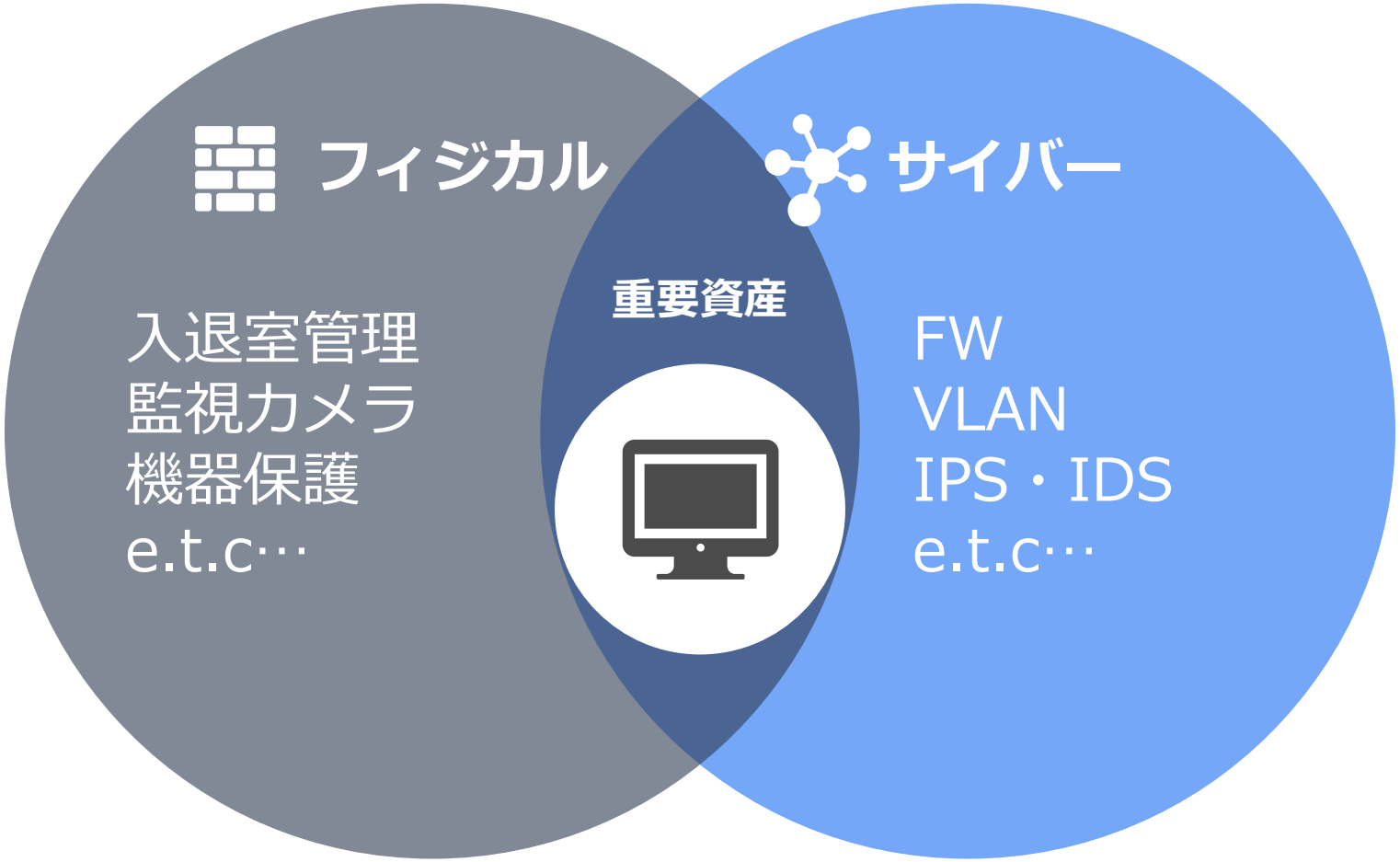
「チーム忍者」リーダー(23) らを逮捕　工事現場から銅線盗んだか…新築の建設現場狙い、総額2500万円相当の窃盗関与の可能性

フジテレビ　社会部　2025年4月28日 月曜 午後0:15

FNNプライムオンライン：「チーム忍者」リーダー(23) らを逮捕　工事現場から銅線盗んだか
https://www.fnn.jp/articles/-/864160 2025.5.7

物理セキュリティの位置づけ

- 資産を保護するにはサイバー・物理の両輪での保護が重要
- サイバー・物理を一体化することでより強固なセキュリティ体制を構築可能



物理セキュリティにおける多層防御の考え方

- 物理セキュリティも考慮し、サイバー側と連動したセキュリティ対策が必要
- 外側から内側への段階的な防護層を形成し、重要資産を保護することが肝要

施設防護：最外層の防御

敷地境界のフェンス、ゲート、警備パトロール

建屋防護：建物内への侵入を制限

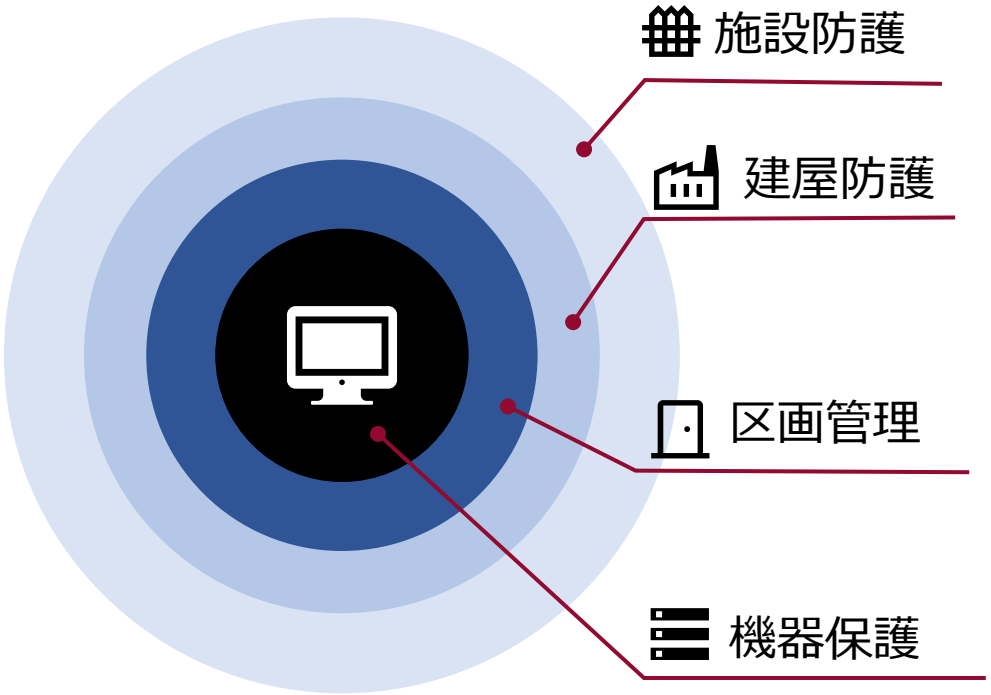
入退室管理、監視カメラ、生体認証など

区画管理：重要エリアへのアクセスを制限

権限に応じた入室許可・アクセス制御

機器保護：機器への物理アクセス制限・検知

サーバラックの施錠、機器取り外し検知器等



物理セキュリティが重要な理由

- DX推進・AI活用に加え、多発する災害、国際的・経済的な情勢から以下の３つを挙げる

1. サイバーセキュリティの基盤となる要素
2. 人為的なリスクも増加傾向
3. 物理的な保護が事業継続性（BC）に直結

工場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においても、
セキュリティ対策企画・導入の進め方のステップ2 対策立案「**物理面での対策**」として挙がっており極めて重要な要素

セキュリティ対策企画・導入の進め方(抜粋)

目次

施設における脅威の分類・対策立案の流れ

施設における脅威は大きく以下に分類される

1. 自然災害による脅威

- 水害（洪水・豪雨・台風など）
- 雷害（落雷によるシステム障害）
- 地震（建物損壊・設備破損など）
- その他（噴火・地すべりなど）

2. 人為的脅威

- 不正侵入（物理的な施設への侵入）
- 破壊行為（設備や機器の意図的な損壊）
- 情報窃取（媒体からの情報漏洩）
- 内部不正
  （産業スパイ、意図的な情報漏洩）

3. 事故

- 火災（電気系統からの発火・延焼）
- 設備故障（冷却装置の故障・電源喪失）
- システム障害（物理的要因によるもの）
- 環境問題（温度・湿度による障害）

⚠ 脅威への対策立案の流れ

ステップ1	ステップ2	ステップ3	ステップ4	ステップ5
守るべき対象を明確化	保護の目的を明確化	防護レベル目標の策定	対策の優先順位付け	対策の実行

TAKENAKA

自然災害（水害）：豪雨による河川氾濫事例

豪雨により河川氾濫が発生。工場の1階に設置されていたサーバ室が浸水

⚠ 被害状況

- 制御サーバが水没し完全に損壊
- バックアップも1週間前のものしかなかった
  最新データを喪失
  （担当者がHDDで取得した物）
- 復旧費用とダウンタイムによる損失が発生

✕ 問題点

- 浸水リスクがある1階にサーバ室を設置
- 電源設備やネットワーク機器も同 1 階に設置されていた
- 事前のバックアップ体制が不十分
  （頻度が低い。オフサイト保管なし）
- BCP（事業継続計画）が未整備で、復旧手順が明確でなかった
- ハザードマップの確認不足による立地リスク認識不足

TAKENAKA

脅威への対策立案の進め方（例）

ステップ1 守るべき対象を明確化

- 従業員、サーバ機器、生産データ、
  ネットワークインフラ、電源設備など…
  ※各資産の重要度と依存関係

ステップ2 保護の目的を明確化

- 浸水から人命・機器を守る
  ＝事業継続性の確保のため
- データを災害から守る
  ＝データの完全性維持のため

ステップ3 防護レベル目標の策定

- 水害リスクに対する対策の立案
- あるべき姿・目標・基準の検討

ステップ4 対策の優先順位付け

- 即時対応すべき重要課題
- コスト対効果の高い対策
- 長期的に取り組むべき対策

目次

サーバ室･計算機室等(重要機能室)の物理的防護・対策

- 産業制御システムや重要なOT機器は、一般のオフィス環境とは異なる物理的な保護が必須
- 特に**重要機能室**は設備インフラの保護、入退管理･アクセス制御など多角的な防護対策が求められる

空調・冷却対策

- 空調の最適方式の選定
- 空調機の冗長化設計
- 温湿度モニタリング
- キャッピング

効率的な空調・冷却により発熱防止

浸水対策

- 上層階に設置
- 防水扉・防潮板設置
- 空調用漏水検知機設置

開口部からの浸水・内部機器からの漏水の防止

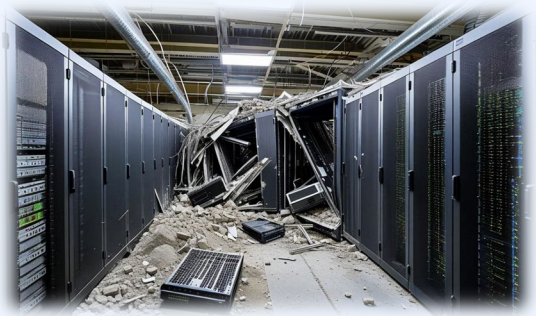
侵入対策

- 生体認証システム
- 入退室管理システム
- 監視カメラ

入退室管理・アクセス制御により入場者を限定

地震対策

- 建物耐震・制振・免震化
- ラック用耐震アンカー
- ラック免震化



免震・耐震対策により機器を保護

TAKENAKA

例：重要機能室への侵入対策

- 場等のOT環境下では内部関係者による不正アクセスのリスクにも注意が必要
- 従業員の役割・権限ベースのアクセス制御、アクセスログの記録・モニタリングを組み合わせ、物理的な不正アクセスの抑止と検知を両立

⚠ 各区域のレベル設定例

区　域	セキュリティレベル	アクセス制御方法
外　構	1：低	フェンス・ゲート+監視カメラ
事務所・執務エリア	2：中	ICカード(電気錠)
生産室	3：高	ICカード/PIN(電気錠)+監視カメラ
重要機能室	4：最高	ICカード+生体認証+監視カメラ

⚠ 重要機能室への対策例

- 生体認証システム（指紋、静脈、虹彩など）
- ＋
- 監視カメラシステム（死角のない配置）
- ＋
- 入退室管理システム（ログ記録と監査）
- ＋
- 電気錠・インターロックドア（自動施錠）

目次

自己紹介

氏名：鈴木　真徳

所属：デジタル室　デジタル企画グループ

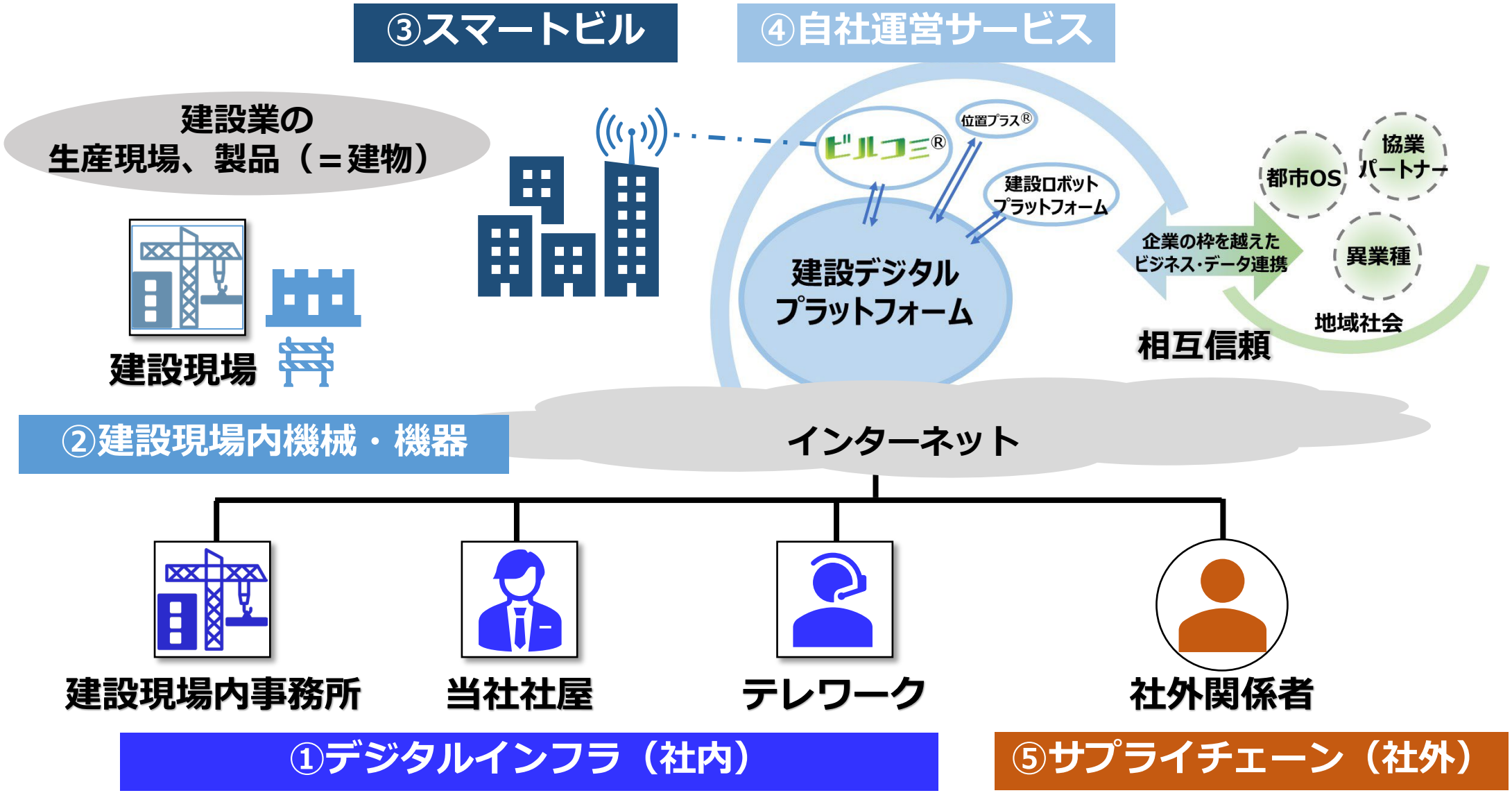
経歴：
製造業での研究開発や情報システム業務等を経て、竹中工務店に入社。
データサイエンス業務を担当後、サイバーセキュリティに関する企画管理を担当。

資格：
CISSP, CCSP, 情報処理安全確保支援士, 産業サイバーセキュリティエキスパート
エネルギー管理士、高圧ガス製造保安責任者、第一種衛生管理者

イベント登壇等：

Interop Tokyo Conference 2024　「AIインシデントへの具体策 ～ヒヤリハットと大事故を踏まえた対策～」
第9回重要インフラサイバーセキュリティコンファレンス（2025年）　「産業制御セキュリティにおける状況と対策は？」
など
AI、クラウド系が多いです。

建設業におけるサイバーセキュリティの俯瞰



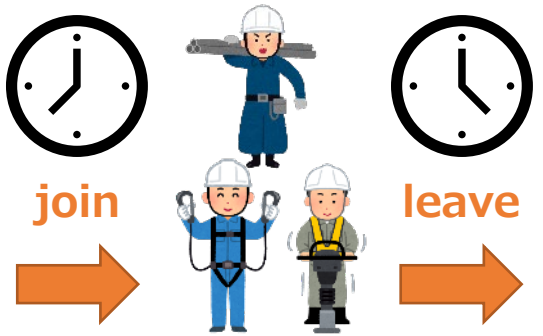
TAKENAKA

建設業におけるセキュリティの特徴

“むき出し”IT資産

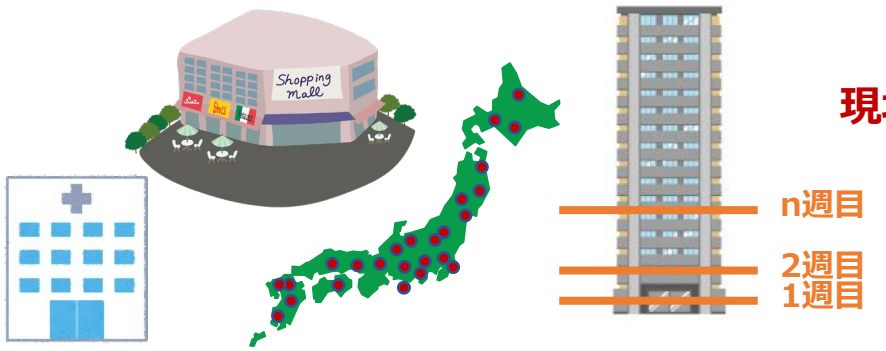
・振動、粉塵、直射日光等
・物理アクセスが容易
（当然、保護はしています）

短期間労働者



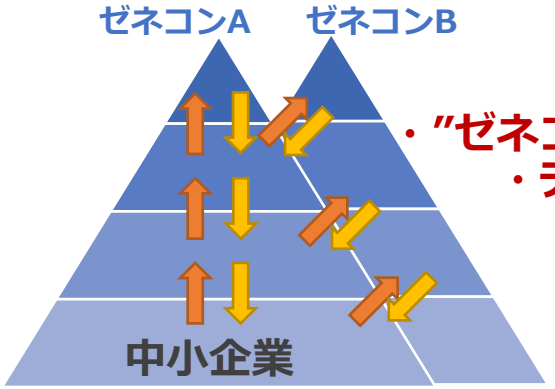
IDセキュリティ
の運用が難しい

多数・多様・変化する現場



現場特性に応じた柔軟な
ITインフラが必要

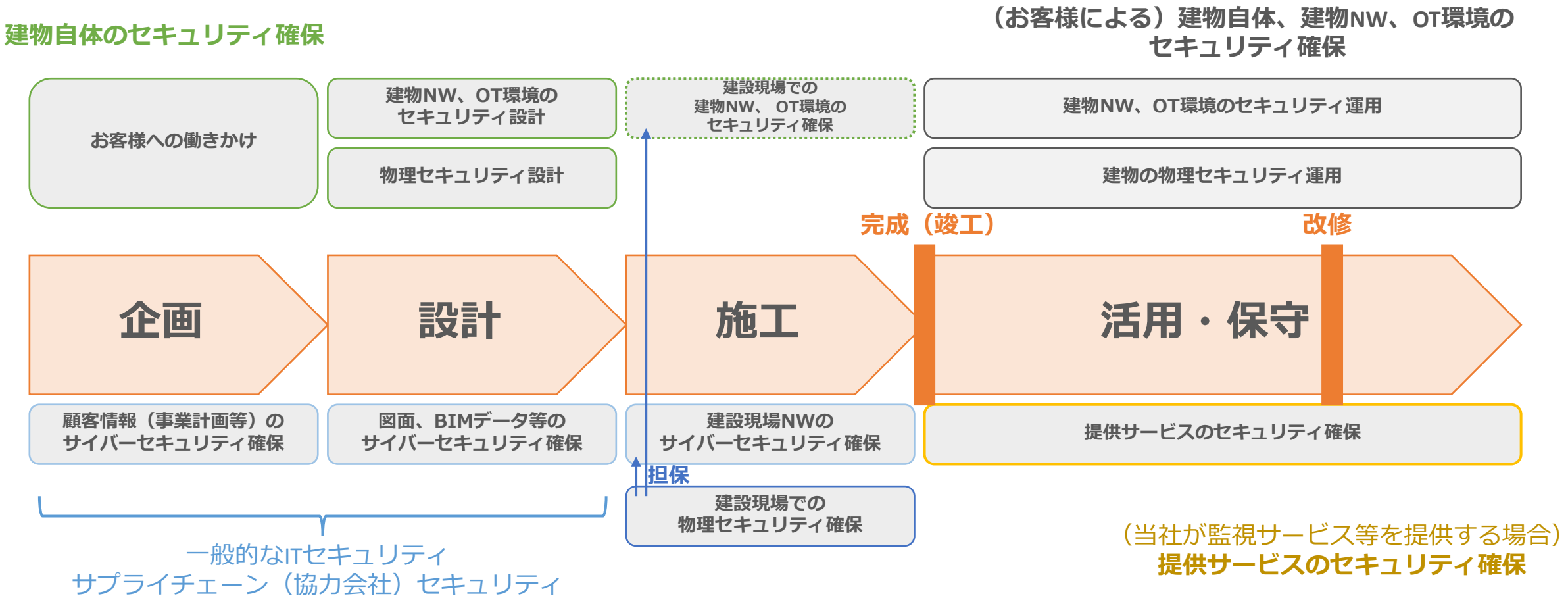
多層・非系列的サプライチェーン



・”ゼネコン個別の対策”に対する反発感
・データ共有先が多数・多層

TAKENAKA

建築プロセスにおけるセキュリティ



TAKENAKA

設計、施工段階のセキュリティ確保

対象と対策

①設計・施工データ（図面、BIM、等）、設計・施工システム

✓ 基本的なITセキュリティ確保の徹底

②建設現場のNW、現場で利用されるIoT機器通信

✓ ネットワークセキュリティの確保（SASE適用）

③建設現場で利用されるIoT機器

✓ 機器導入時の独自審査

④サプライチェーン（協力会社）

✓ 協力会社向け教育

いずれも完全な対策は不可能。
取り得る対策を講じながら、徐々にリスクを低減させていく。

①設計・施工データ（図面、BIM）、設計・施工システムの保護

システムをセキュアにする ▶ できる

保護対象	対策
クラウドインフラ	クラウド設定監査（CSPM） NWセグメンテーション
サーバ	脆弱性スキャン/パッチ、EDR
アプリ	脆弱性診断、WAF
ID・認証	ID連携、二要素認証
データ	日本リージョンに保存、暗号化

基本的な対策を確実に実施

システムをセキュアに使う ▶ 大変

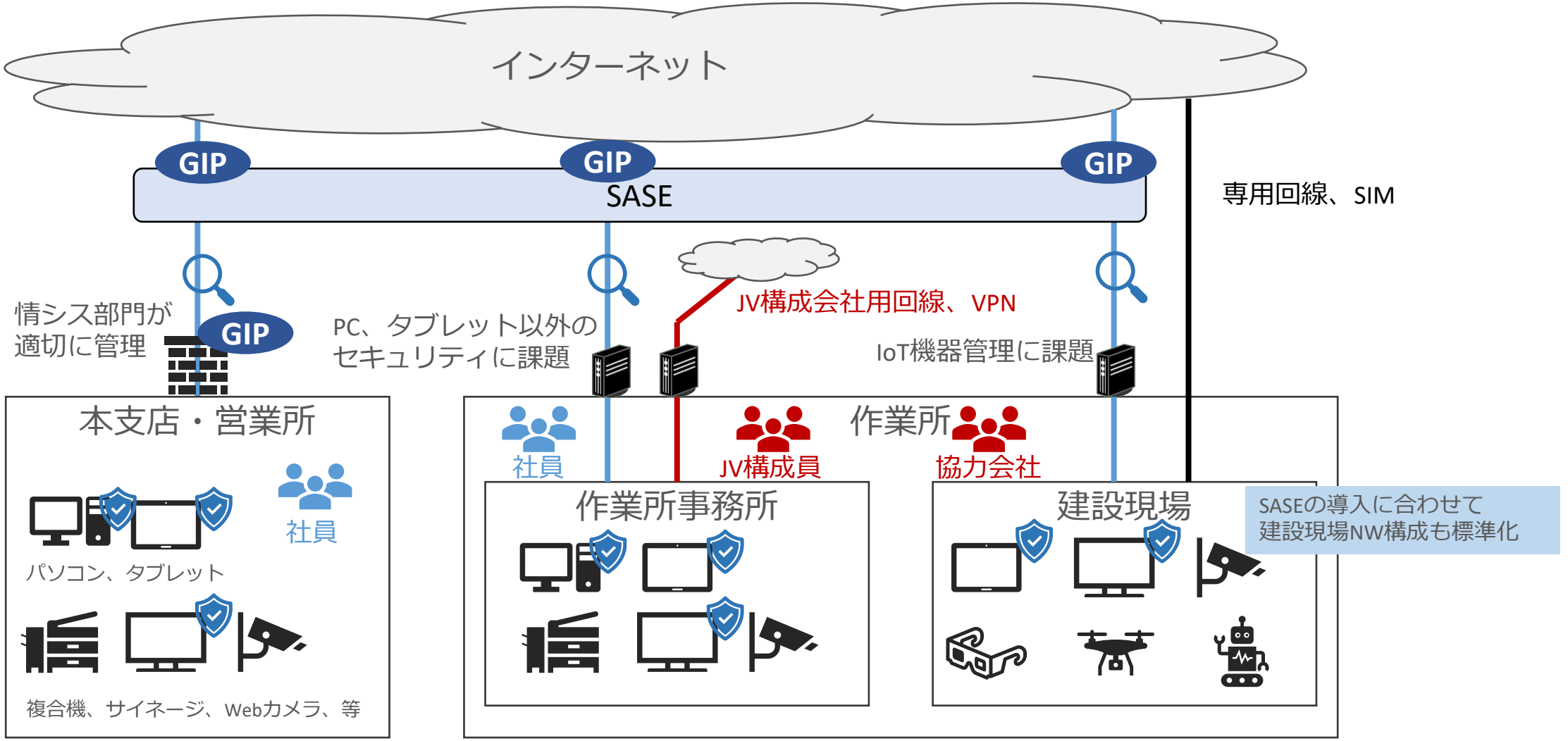
特に、社外ユーザーの取り扱いが課題

・ユーザーの拡大（社員⇒協力会社の職長⇒職人）
・アクセス端末の多様化（自社支給⇒他社支給⇒私有）
・アクセス場所の制約
（作業所≒仮囲いの中　以外では、アクセスして欲しくない）

・アクセス権限・制御設計の難しさ
・アカウントライフサイクル管理の難しさ

「ルール・契約」「IT」「教育」を組み合わせてリスク低減

②建設現場のNW、現場で利用されるIoT機器通信のリスク低減



SASEの導入により、不正通信ブロック、IoT機器可視性の向上を目指す

TAKENAKA

③建設現場で利用されるIoT機器のセキュリティ確保

明らかに不適な機器の排除

※内規レベルの運用

米国（連邦通信委員会）で指定されている、特定（某国の通信メーカー等）のベンダー製機器の排除

機器の基本的な仕様・セキュリティ機能の確認

※カタログスペック評価

（評価項目の例）
・OS種類、ネットワーク接続形態、重量・寸法
・内部ストレージ有無
・USBポート等の有無
・EDRやSASEエージェントの導入可否
・初期PW変更可否、パッチ提供の有無、ログ取得有無、、等
・付随するクラウドサービス
⇒ **JC-STAR制度も上手く活用し、社内のIoT機器評価スキームの整備**を行って評価の均一化と作業負荷削減

機器の使い方の確認

（評価項目の例）
・扱う情報の種類（予定表の表示だけなのか、図面を扱うのか、等）
・内部ストレージ、USBポート利用の有無
・設置場所、機器固定の有無
・会社アカウント、Office用アカウント利用有無
⇒JC-STAR制度ではカバーできない。**利用機器と利用方法を標準化**して負担削減

IoT機器の使い方に起因するリスク

- 機器の盗難
- 外部ポート経由の被害
- クラウド経由の被害

④サプライチェーン（協力会社）のセキュリティ確保

建設業のサプライチェーンである協力会社の多くは、1～50人規模の会社である。
IT担当がいない（総務・管理部門の社員が兼務である）ケースもあり、丁寧かつ地道な支援が必要。

セキュリティウェビナーの開催（2023年～、年1回実施）

- 世の中のセキュリティ脅威（警視庁やIPAの情報の周知）
- 建設業の状況、当社事例の共有
- **VPN装置へのパッチ適用、保守ベンダーとの契約確認の推奨**
- **EDRの導入推奨**
- ビジネスメール詐欺の注意喚起
- アンケート結果の周知
- お役立ち情報（各組織が出している中小企業向け資料等）の共有
- **IPAサイバーセキュリティお助け隊の案内**
- **竹中工務店　相談窓口の案内**

実際に被害にあった協力会社にも出演いただき、
被害の壮絶さを語ってもらった

まとめ

- ✓ OT環境を支える、という観点から、竹中工務店における、建物物理セキュリティ設計、建設現場を中心としたサイバーセキュリティを紹介した。
- ✓ OT環境の物理的保護では、単一の対策に依存せず、複数の防護層を重ねることで総合的なセキュリティレベルを高めることが重要である。
- ✓ 建設業の生産現場＝建設現場は、多数・多様・変化する現場であり、社外の関係者も多い。IoT機器や協力会社のID管理、データの取り扱いに課題がある中で、完全な対策は不可能だが、ルール・契約、IT、教育を組み合わせながらリスク低減を進めている。