CyberDefense

ペネトレーションテスト事業者から見た制御システムセキュリティ対策の惜しい点

サイバーディフェンス研究所
技術部 安井　康二

自己紹介

安井　康二

Career

２０年以上、SCADAのインフラ開発に従事

- セキュリティ専任者という概念がない時代からセキュリティ担当
- FW, IDS, ログ管理（SIEM）, アプリケーションホワイトリスト
- リスクアセスメント

対策の有効性を知るには、攻撃手法を知らねば

2019

セキュリティ企業に転職、攻撃者側へ

- 制御システムのペネトレーションテスト
- 模擬環境の構築と攻撃実験

CyberDefense

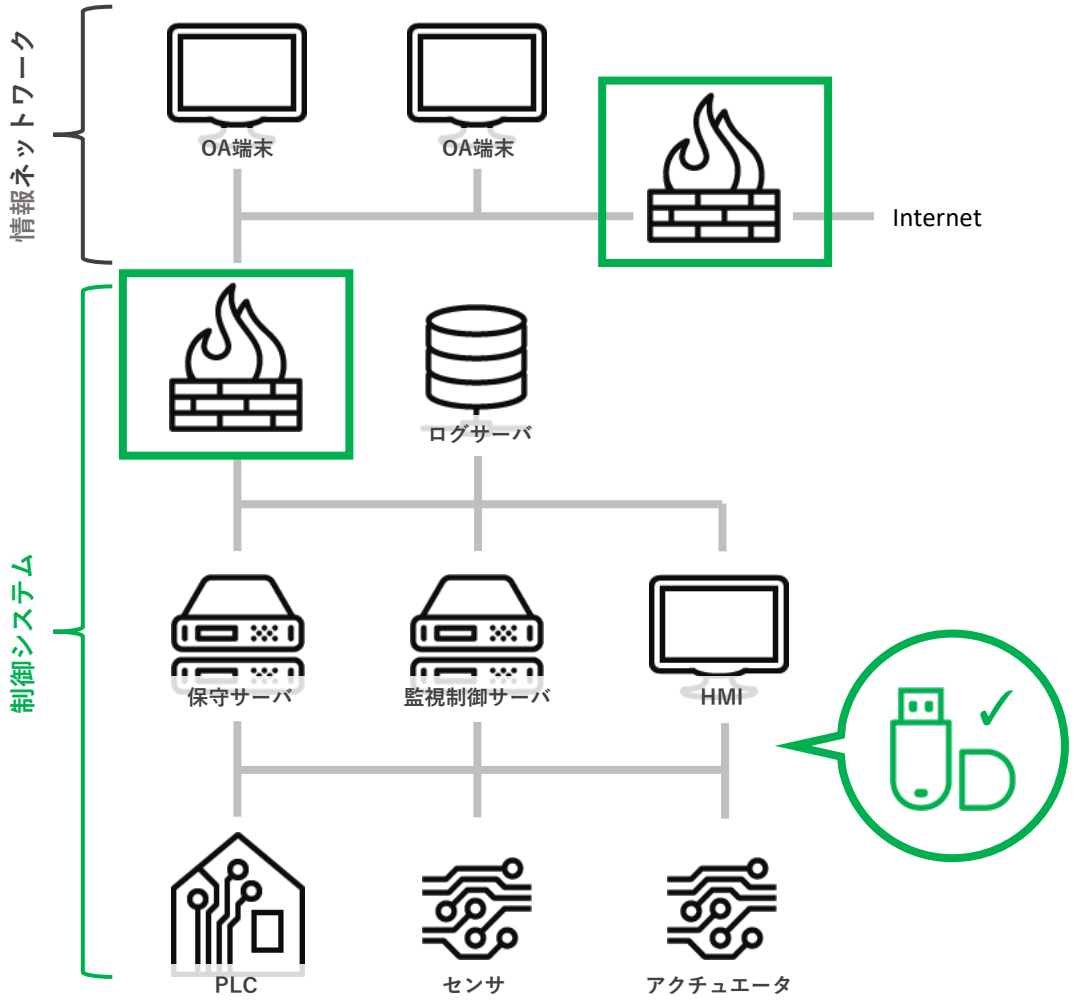
本日お話すること

- 「敵を知り、己を知る」ことで実現できる、費用対効果の高い納得感のあるセキュリティ対策
- 想定対象者：ユーザ、仕様検討・設計を担当するシステムベンダの現場担当者

CyberDefense

今回紹介する
攻撃シナリオと前提条件

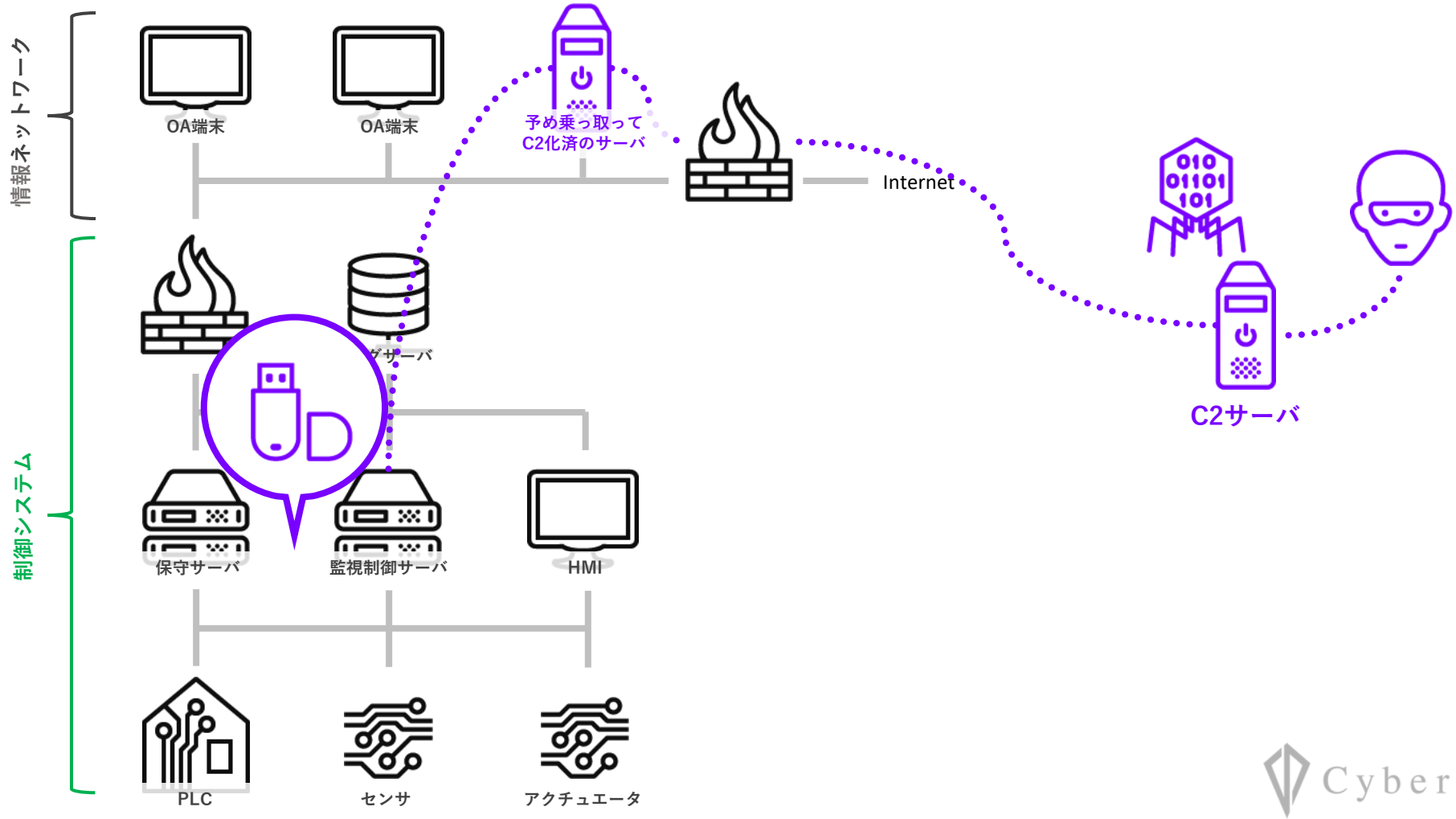
システムと対策の前提条件



- **外部からの侵入には？**
  - FWで防御する
- **内部からの侵入には？**
  - ウイルスチェック済みのUSBメモリのみ使用を許可する
  - 保守用端末、リモート保守は経由の侵入はシナリオ対象外

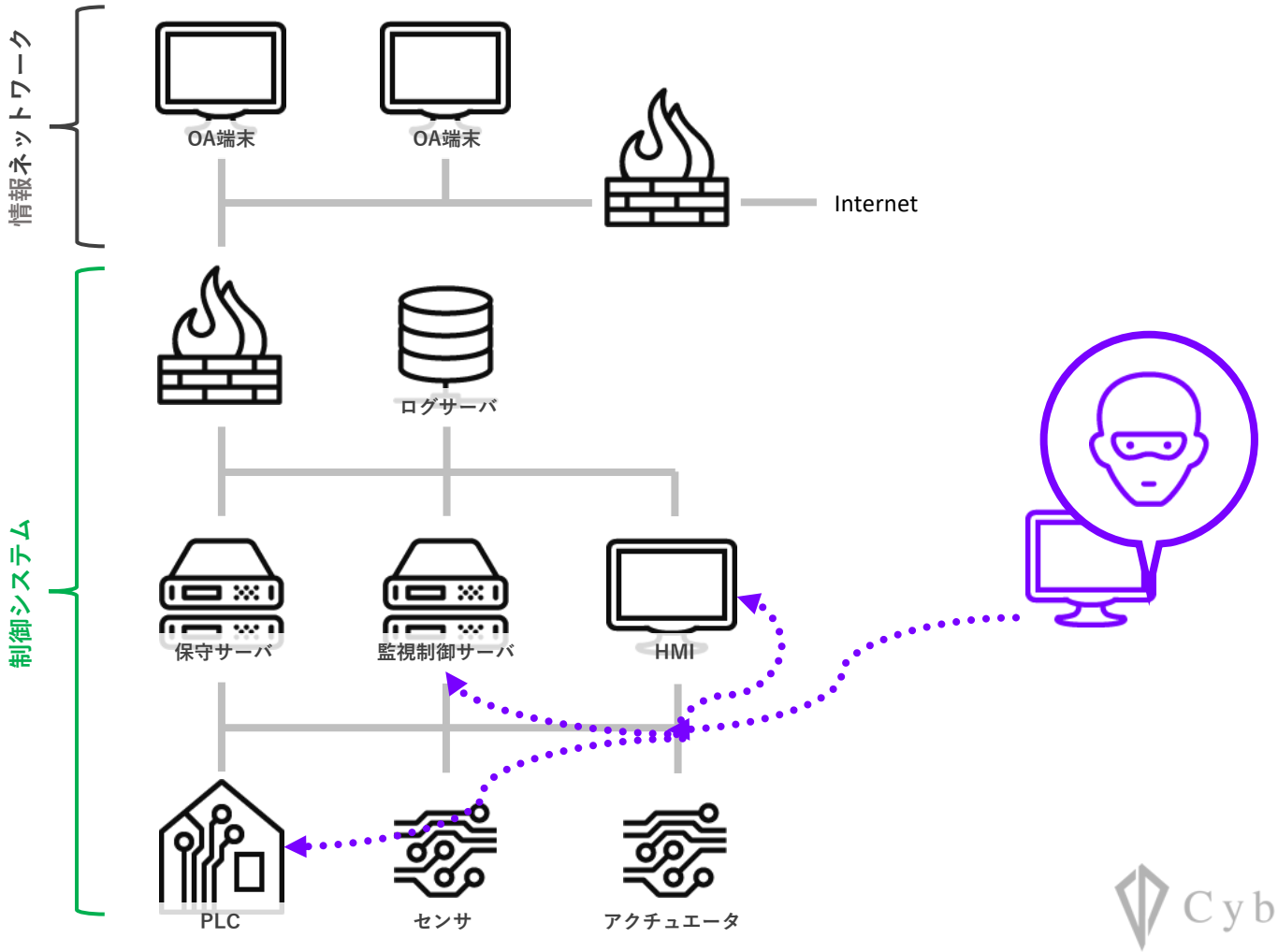
CyberDefense

シナリオ1 – USB経由で侵入



CyberDefense

シナリオ2 – 制御ネットワークから侵入



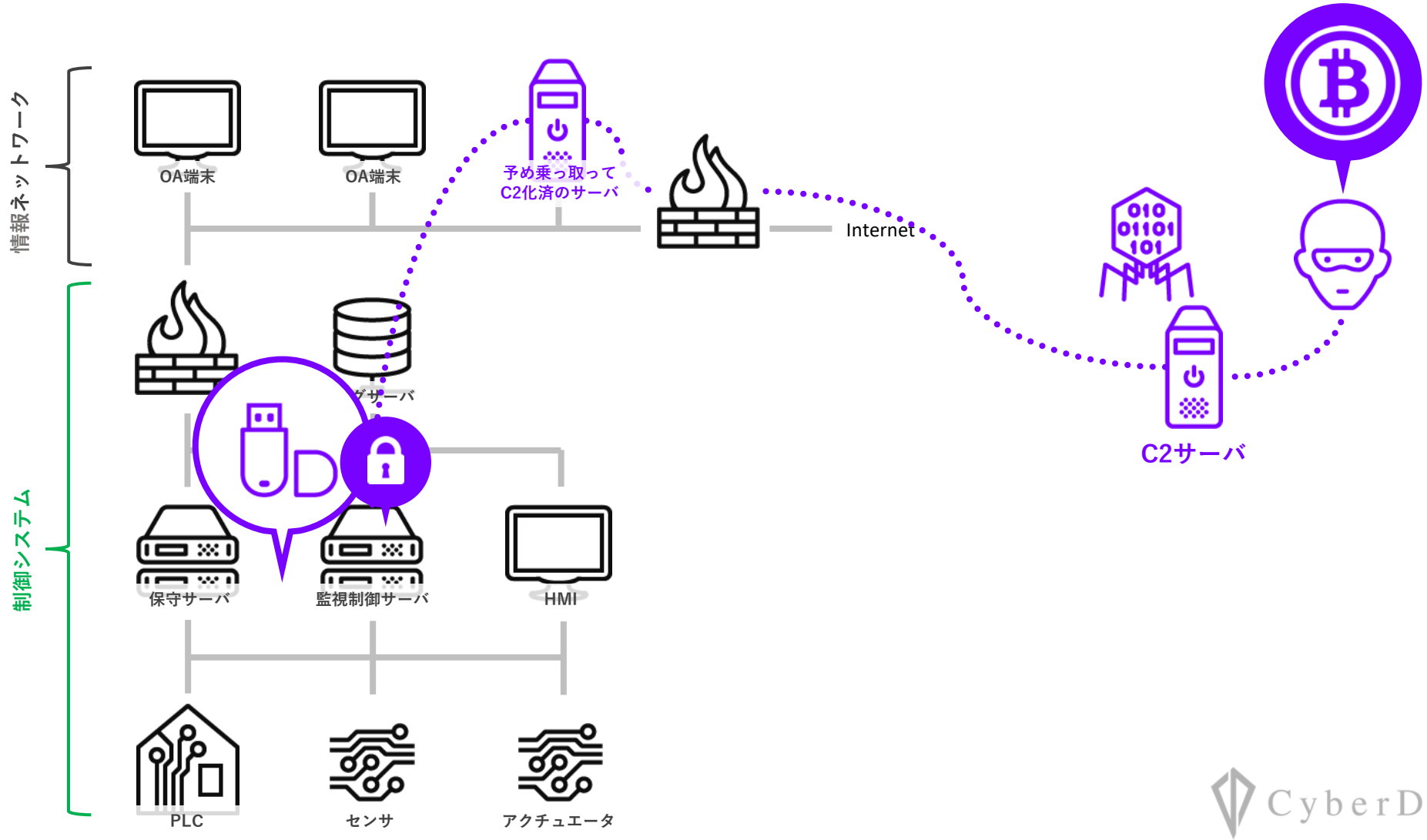
CyberDefense

シナリオ1 | USB経由の侵入

脅威の想定・対策・リスク分析

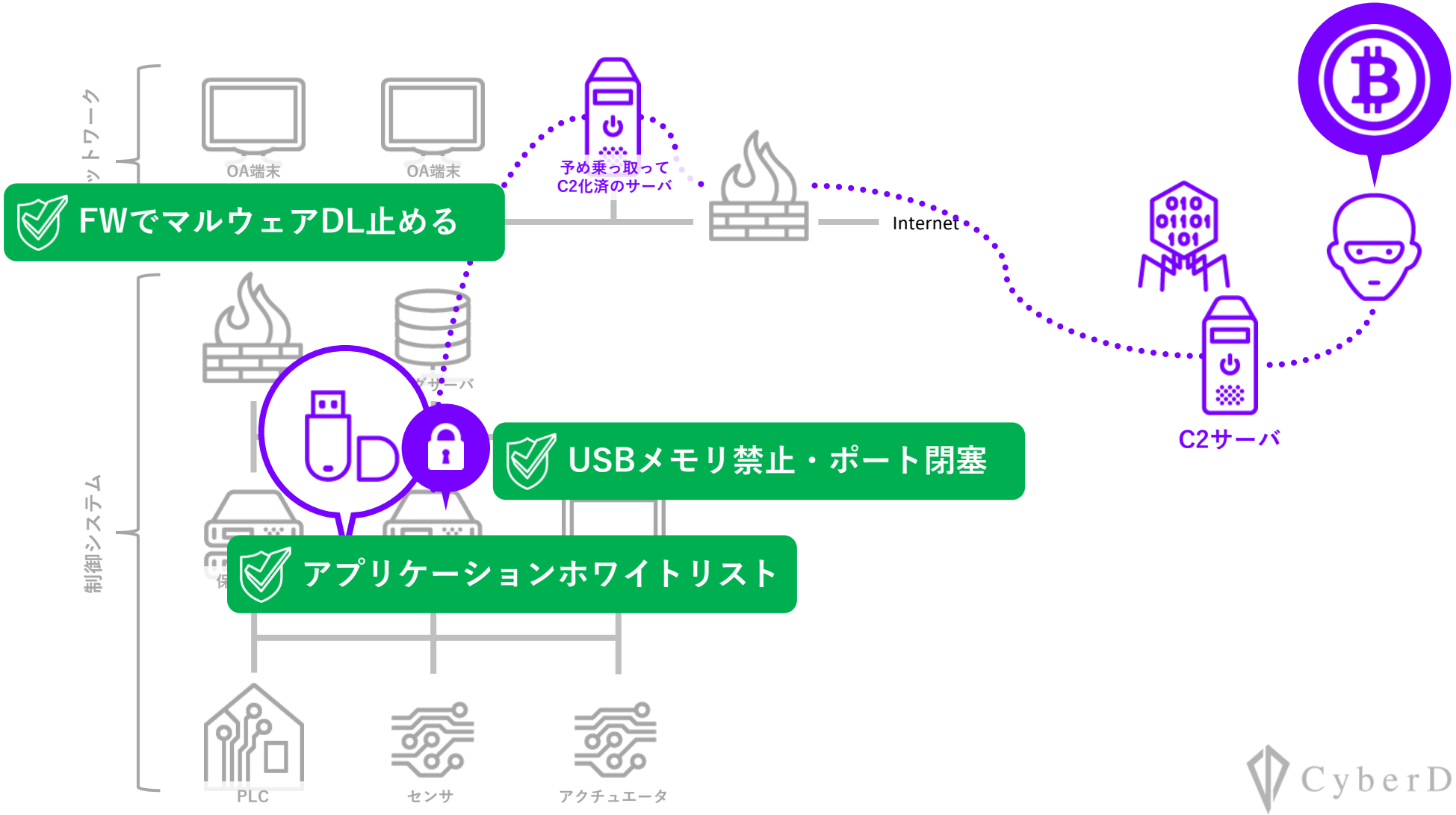
CyberDefense

シナリオ1 – 脅威の想定



CyberDefense

シナリオ1 – 対策



CyberDefense

シナリオ1 –事業被害ベースリスク分析

制御システムのセキュリティリスク分析ガイド　第２版
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

リスク分析してみると

攻撃シナリオ		評価指標				対
	攻撃ツリー／攻撃ステップ	脅威レベル	脆弱性レベル	事業被害レベル		防御
						侵入／拡散段階 / 目的遂行段階
1−1	USBメモリでマルウェア感染し監視制御不能					
	侵入口=サーバ 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。					使用USBポート閉塞 ○
	マルウェアが、C2サーバからランサムウェアをダウンロードする。					ホワイトリストによるプロセスの起動制限 ○ FW ○
	ランサムウェアが制御プログラムを暗号化し監視制御不能となる。	2	1	2	D	ホワイトリストによるプロセスの起動制限 ○

♪

本当に大丈夫なのか？

CyberDefense

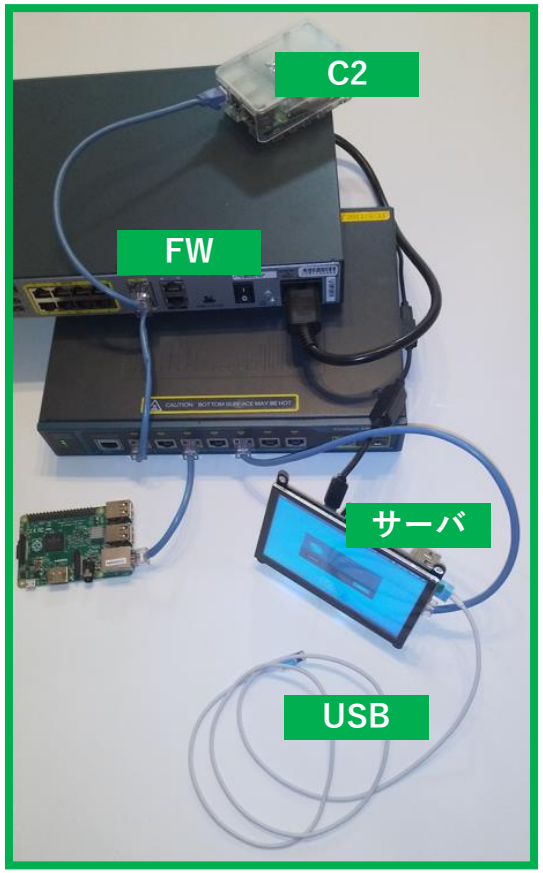
Demonstration 1

USB経由の侵入

USBケーブルからの侵入　デモ動画

CyberDefense

デモについて



CyberDefense

対策のポイント

情報ネットワーク

制御システム

USBメモリ禁止・ポート閉塞

「USBはあらゆるタイプの機器を疑う」

アプリケーションホワイトリスト

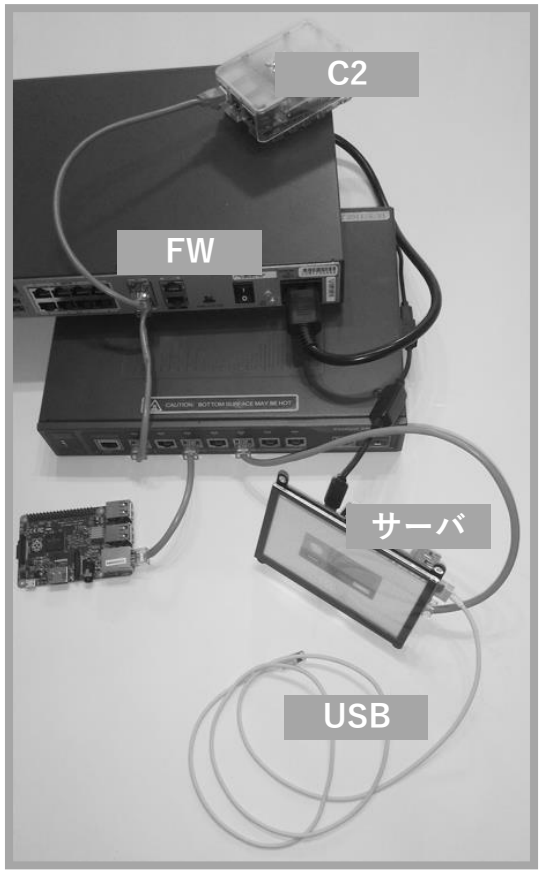
「ホワイトリストは万能ではない」

保守に使用する正規コマンドが使用されると検出できない場合がある。

FWでマルウェアDL止める

「アウトバウンドを制限する」

アウトバウンドとその戻りをブロックしていなければ、リバースシェルで任意操作可能。



CyberDefense

バックアップは重要

バックアップの仕様策定にあたって

- 何をバックアップするのか
  - システム初期イメージ
  - 運用設定データ
  - …
- 復元できなくても許容できるものは何か
- 復元テスト（せめて机上検討を）

復元テストをやっていれば

- 有事への備えに
- 日常の保守においても自信に
  - 最悪の場合は復元できる自信
- セキュリティ試験
  - 「壊れるかもしれないのでテストできません」
  - 「それに備えるにはコストがかかります」

壊れるのが怖いからテストできない、は本末転倒では？

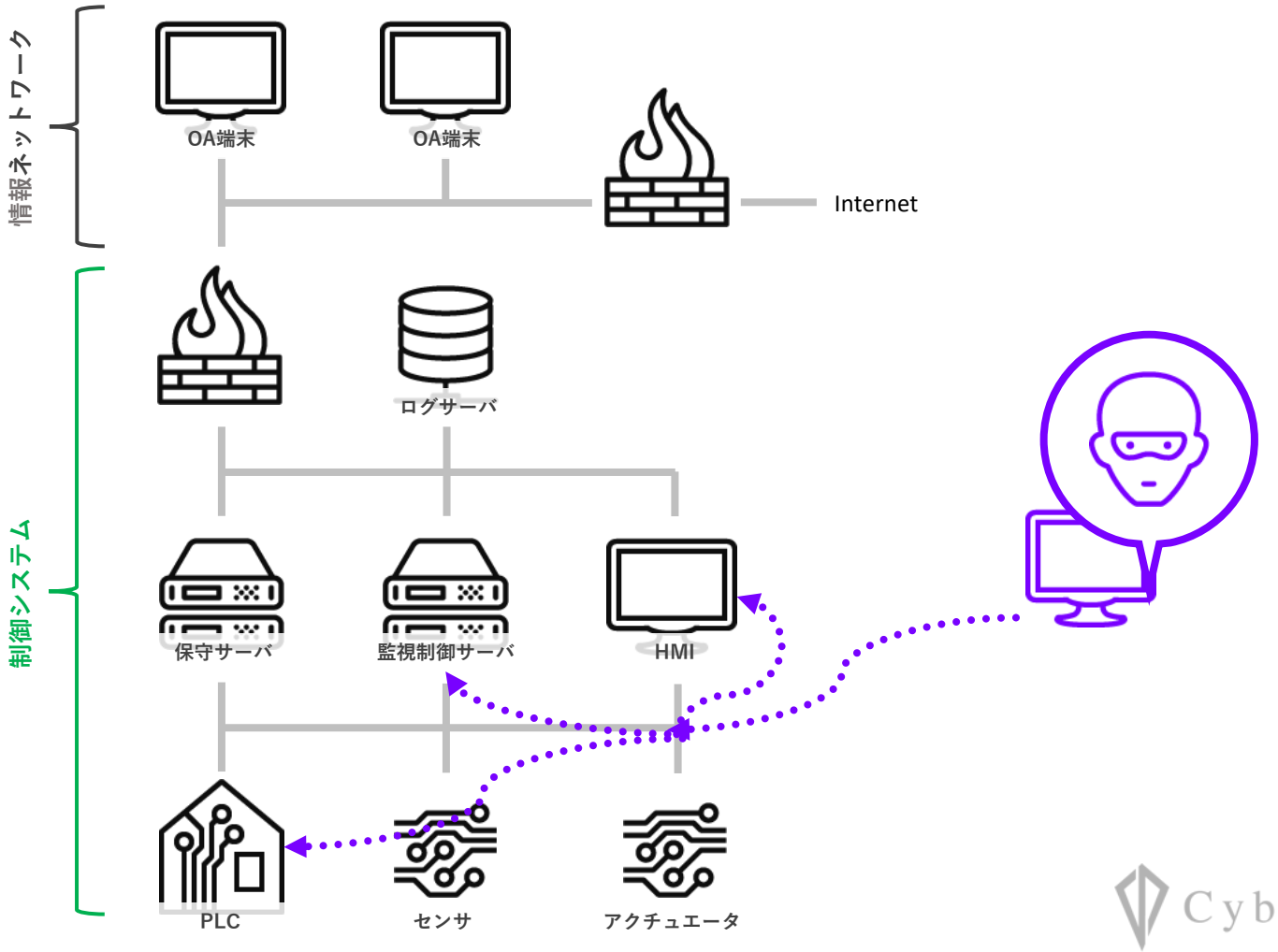
CyberDefense

Demonstration 2

制御ネットワークからの侵入

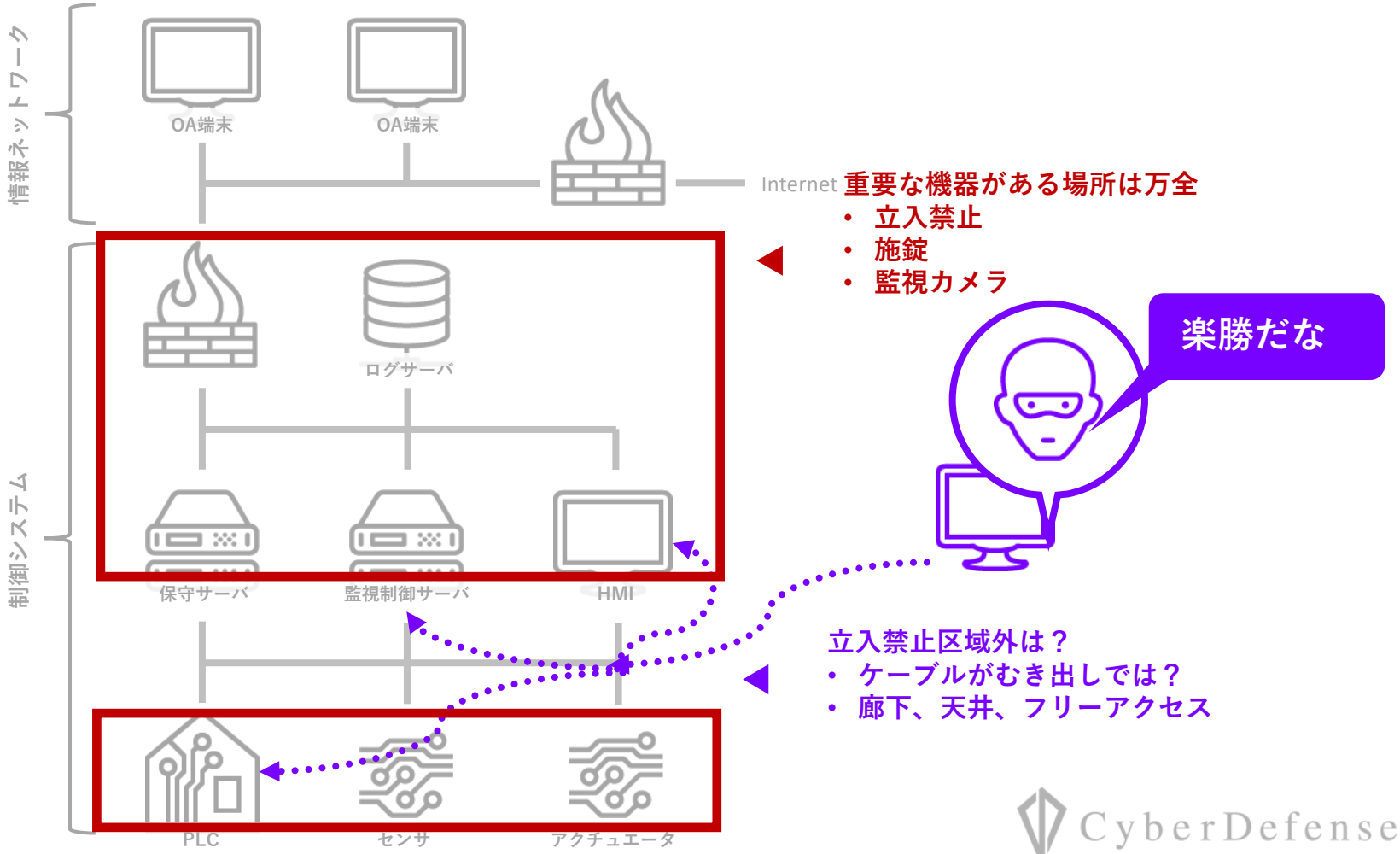
CyberDefense

制御ネットワーク侵入の概要



CyberDefense

制御ネットワーク侵入の概要



CyberDefense

LANケーブルからの侵入　デモ動画

資料元：弊社ブログ　DARK MATTER
https://io.cyberdefense.jp/entry/lan-cable-intrusion

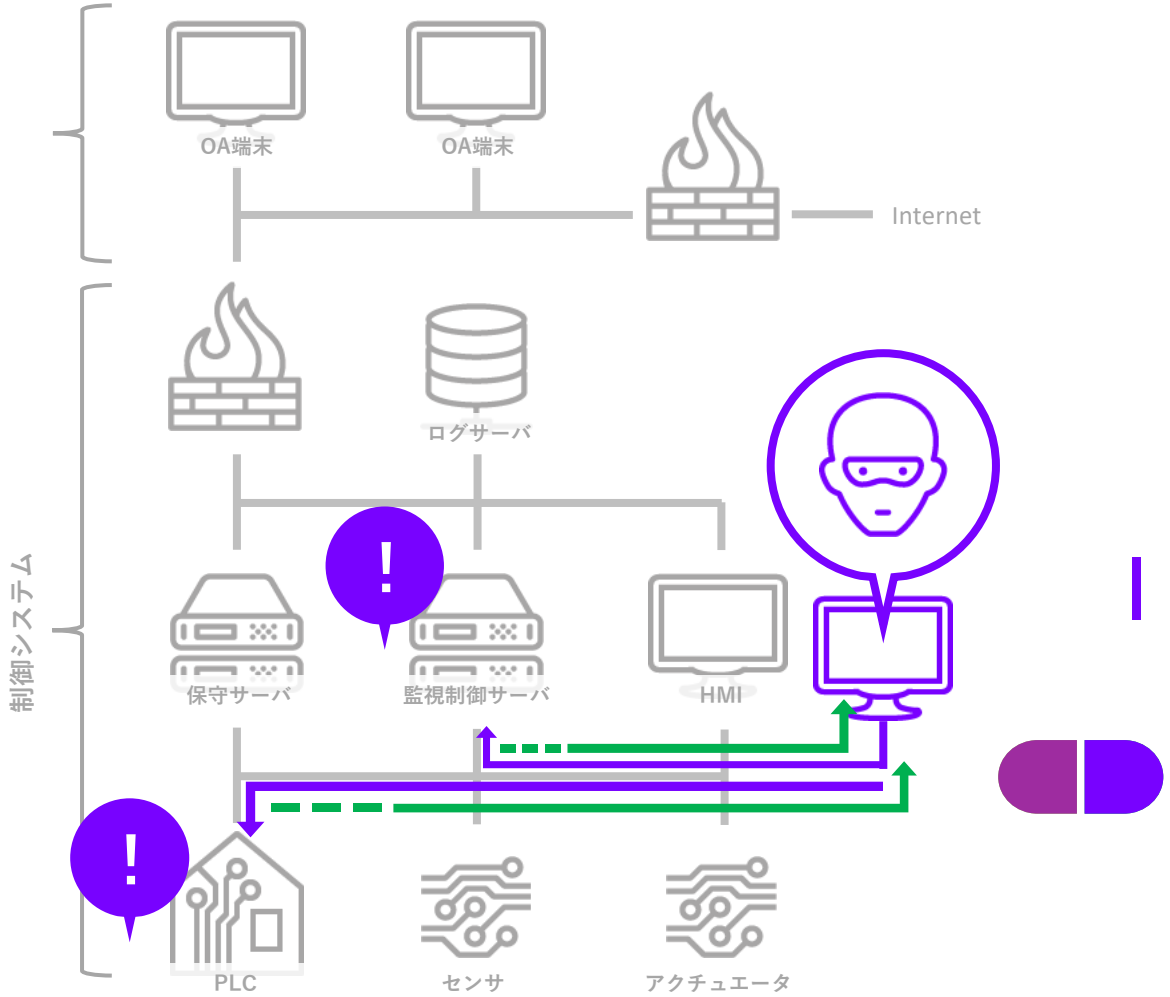
CyberDefense

Demonstration 3

中間者攻撃

CyberDefense

制御ネットワーク侵入の概要



CyberDefense

中間者攻撃　デモ動画

CyberDefense

まとめ

まとめ

本日ご紹介した攻撃手法に有効な対策

- USBはあらゆる機器に注意
- FW設定は外部向け通信も塞ぐ
- バックアップ
  - バックアップが必要なもの必要ないもの
  - テストの実施、復元できることの確認
- 物理侵入口は通信路も確認する

制御システムのセキュリティで重要なこと

- リスク分析は有効、しかし
  - リスク分析結果の盲信は危険
- 攻撃手法の理解が重要
  - 本当に有効な対策がわかる
  - 過剰にコストを掛けずにすむ
- なぜ大丈夫なのか？を知る姿勢

CyberDefense

ONLY HUMANS CAN COUNTER HUMAN-DRIVEN THREATS

CyberDefense

お問い合わせはこちらへ
https://www.cyberdefense.jp/contact/