攻撃者視点から見た OT環境の通信監視 スモールスタートから始めてみよう

サイバーディフェンス研究所
OTセキュリティグループ
プリンシパルコンサルタント　安井　康二

自己紹介

Caree

２０年以上、重要インフラのSCADA開発

- ミドルウェア・ネットワーク・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、攻撃者知見学ぶ

- 制御システムのペネトレーションテスト
- 模擬制御システム環境の構築と攻撃・検知・防御実験

知り得た知見を、制御業界の方へ還元したい

CyberDefense

対象者

自らが関わるOT環境において、侵入兆候があるのか知りたい方

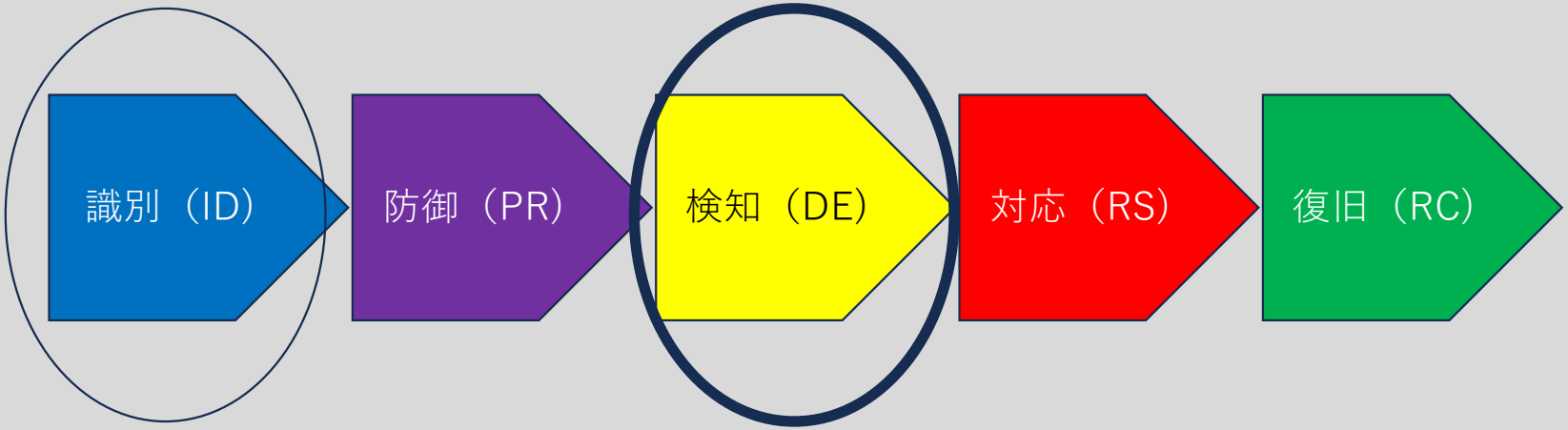
- 通信監視に興味がある
- OT IDS製品選定の前に基礎知識を得たい
- 侵入兆候の発見方法を実際に見てみたい
- パッチ未適用のLinux/Windowsへの攻撃が心配

CyberDefense

対象範囲

資産把握

通信監視



NIST サイバーセキュリティフレームワーク(CSF)

CyberDefense

通信監視は、OT環境と相性が良い理由

- セキュリティ対策の効果を見える化
  攻撃を仕掛けられているのか、防げているのか把握できる

- 可用性への心配なく監視可能
  受動的なパケットキャプチャで監視できるので運用への影響与えない

- 日々の点検の延長で監視可能
  一次診断であれば、無理なくOT現場の人が慣れ親しんだ設備異常点検の延長として運用可能（と思う）

CyberDefense

初期導入課題

- 費用が高く敷居が高そう
- どんな機能が必要なのかわからない

↓

どの製品を適用するかの判断基準がわからない

↓

- スモールスタートで始めてみる
  工夫すれば低いコストでも運用可能
  制御システムは、原則、特定の機器間で決まったプロトコルで通信を行うため、通常時と異なる侵入兆候をみつけやすい。

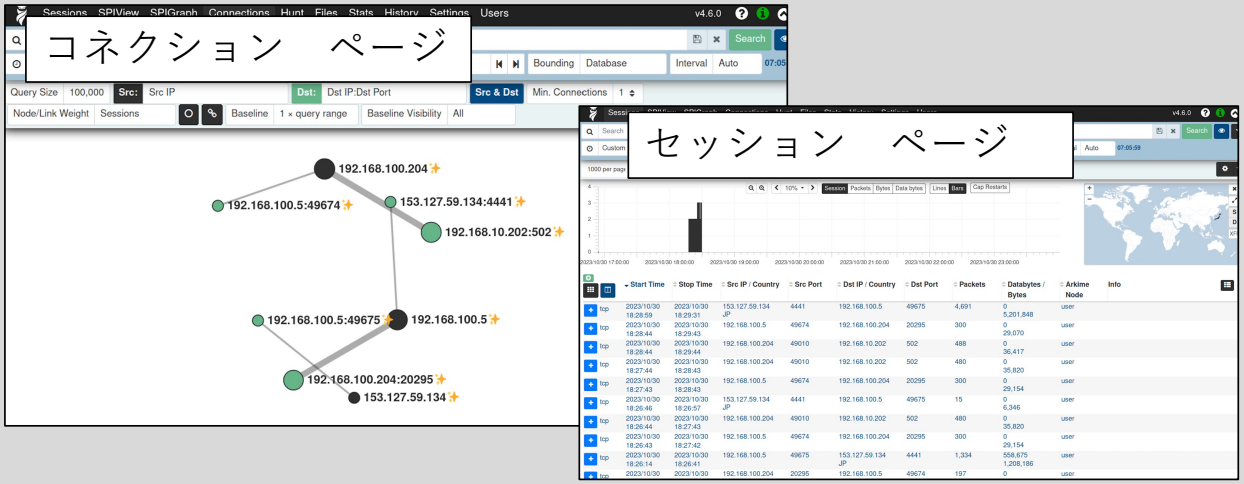
CyberDefense

スモールスタート

- 用意するもの
１０～２０万円程度のPC

- 手法
OSSツール： Arkime

- 手順
PCにArkimeをインストール設定
Switchにミラーポート設定しパケットキャプチャしてArkimeで監視



https://arkime.com/
CISAの通信分析ツール群Malcolmに採用。

詳細は、
「サイバーディフェンス研究所ブログ　DARKMATTER」で公開
https://io.cyberdefense.jp/entry/ot_ids_oss/

CyberDefense

制御システムでためす

CyberDefense 模擬制御システム　MAP

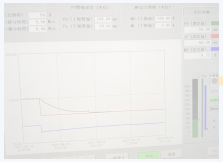
SCADA HMI

SCADA Server

仮想工場

Soft PLC

工場制御システム



SCADA HMI

SCADA Server

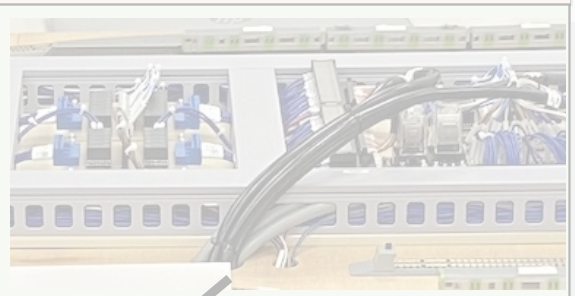
水ポンプ

コントローラPLC

水量制御システム

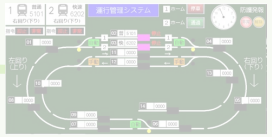
SCADA HMI

SCADA Server



鉄道

PLC



PLCのHMI

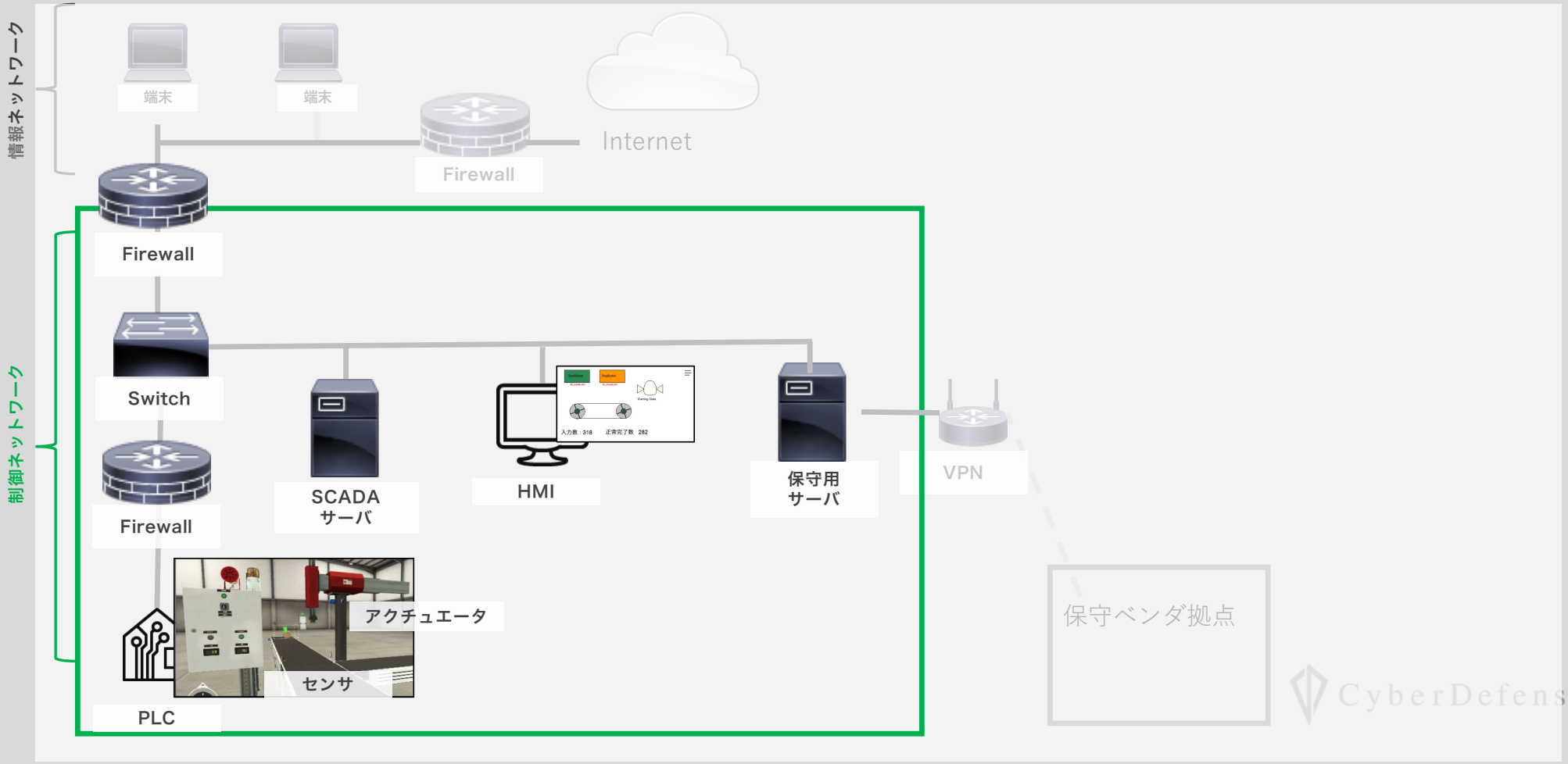
鉄道制御システム

判例

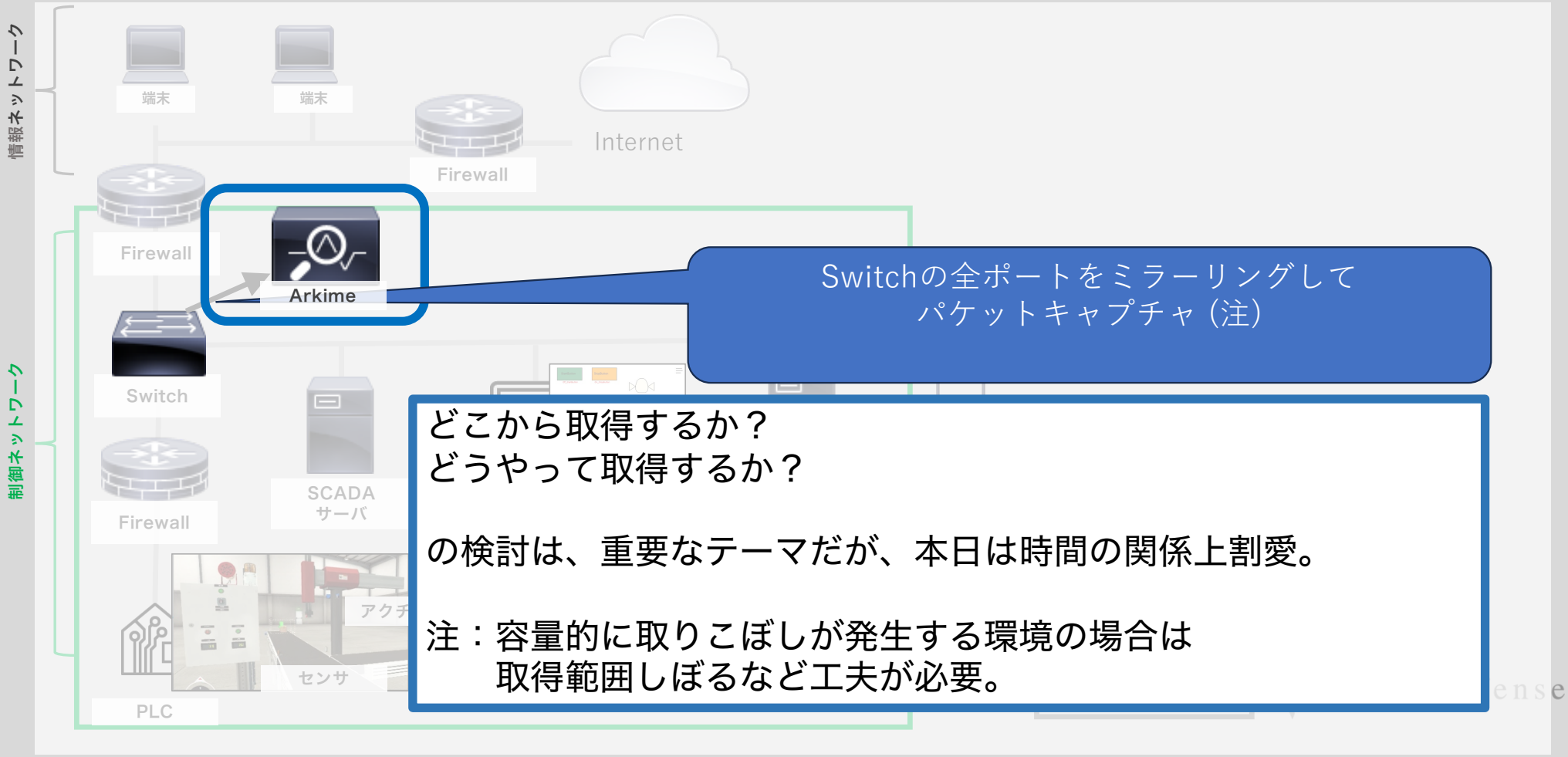
- :LAN(Modbus/TCP)
- :LAN(Melsec/UDP)
- :LAN(Melsoft/UDP)
- :LAN(独自 over TLS)
- :LAN(X11/TCP)
- :シリアル
- :電線

CyberDefense

制御システム



通信監視環境



Switchの全ポートをミラーリングして
パケットキャプチャ（注）

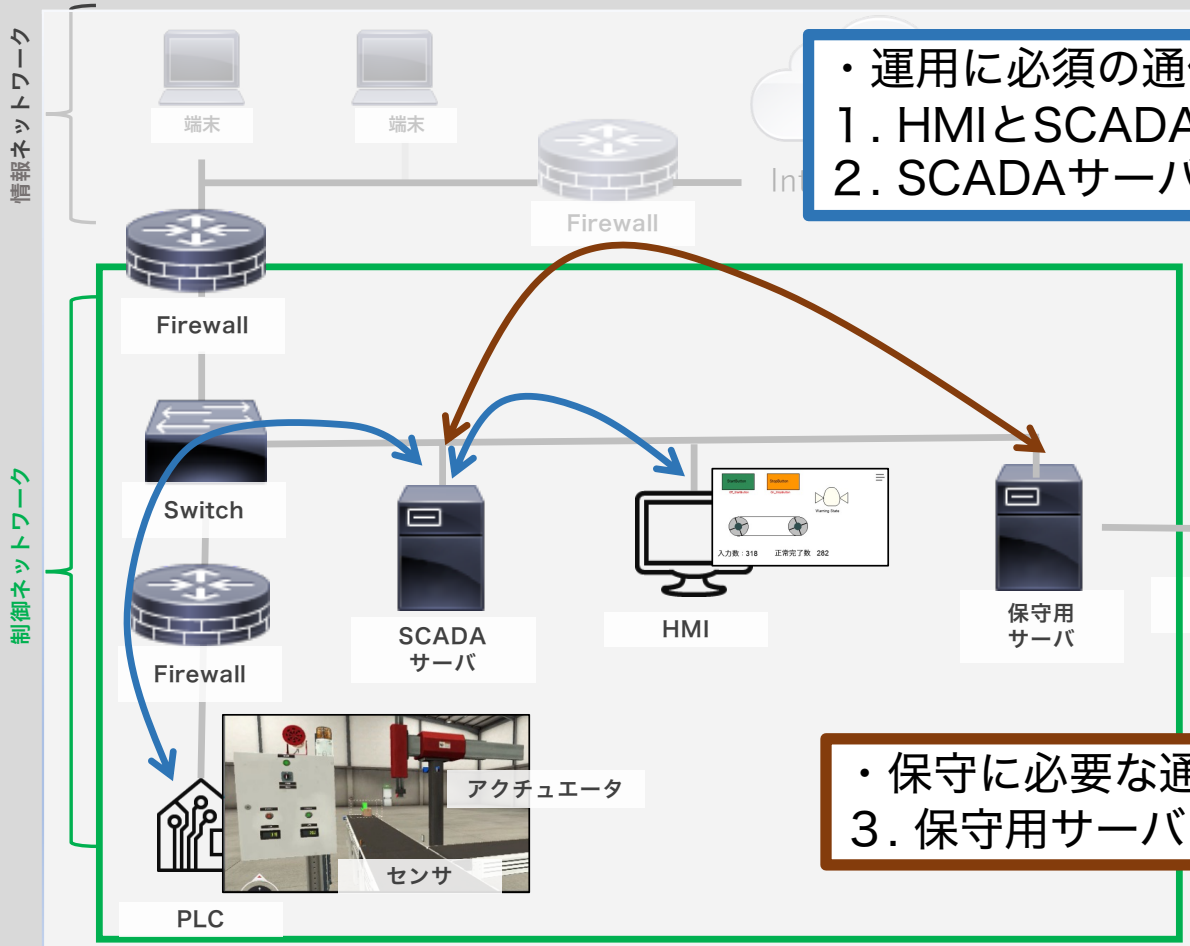
どこから取得するか？
どうやって取得するか？

の検討は、重要なテーマだが、本日は時間の関係上割愛。

注：容量的に取りこぼしが発生する環境の場合は
　　取得範囲しぼるなど工夫が必要。

平常時の監視

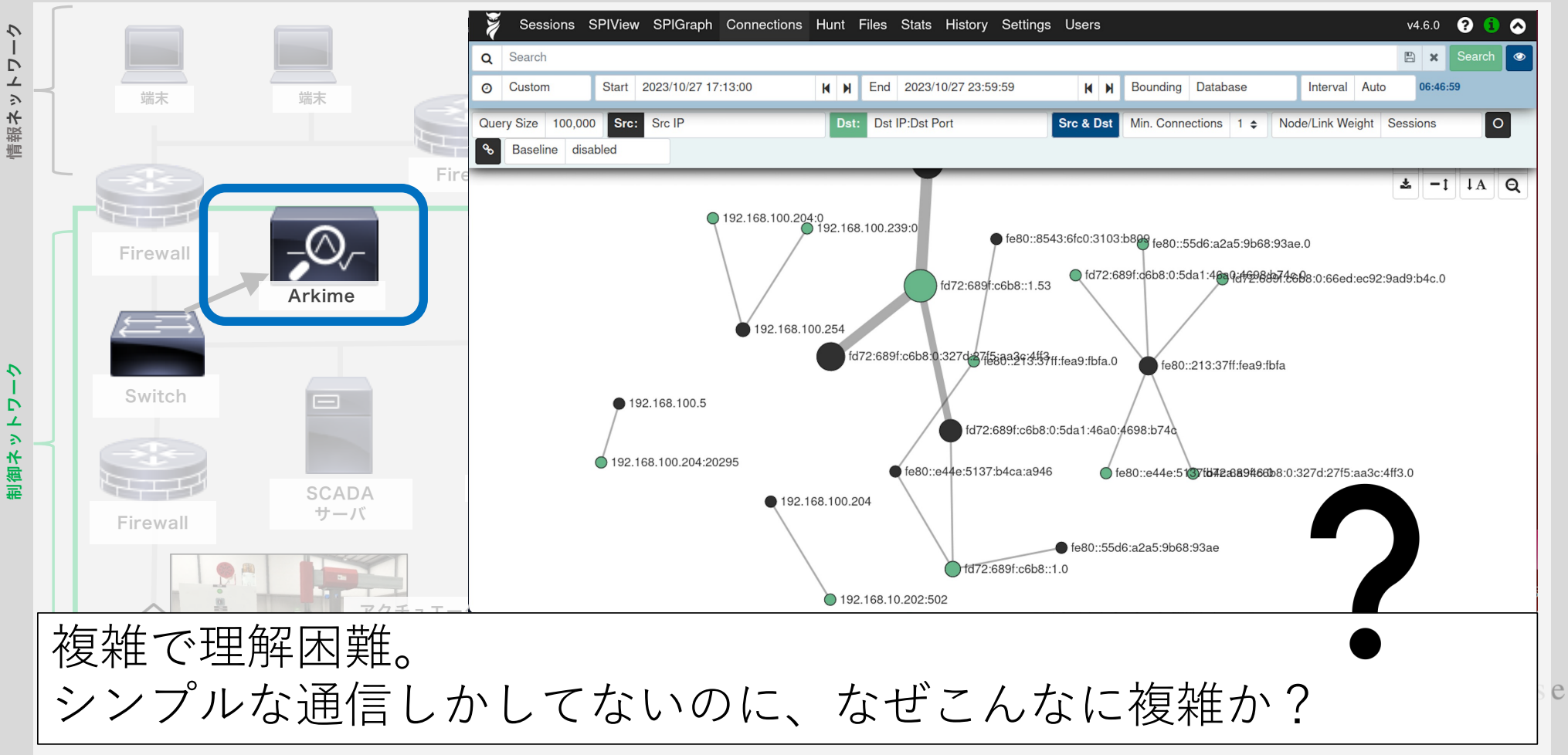
制御システムの必須通信



・運用に必須の通信
1. HMIとSCADAサーバの通信（TCP/20295）
2. SCADAサーバとPLCの通信（TCP/502）

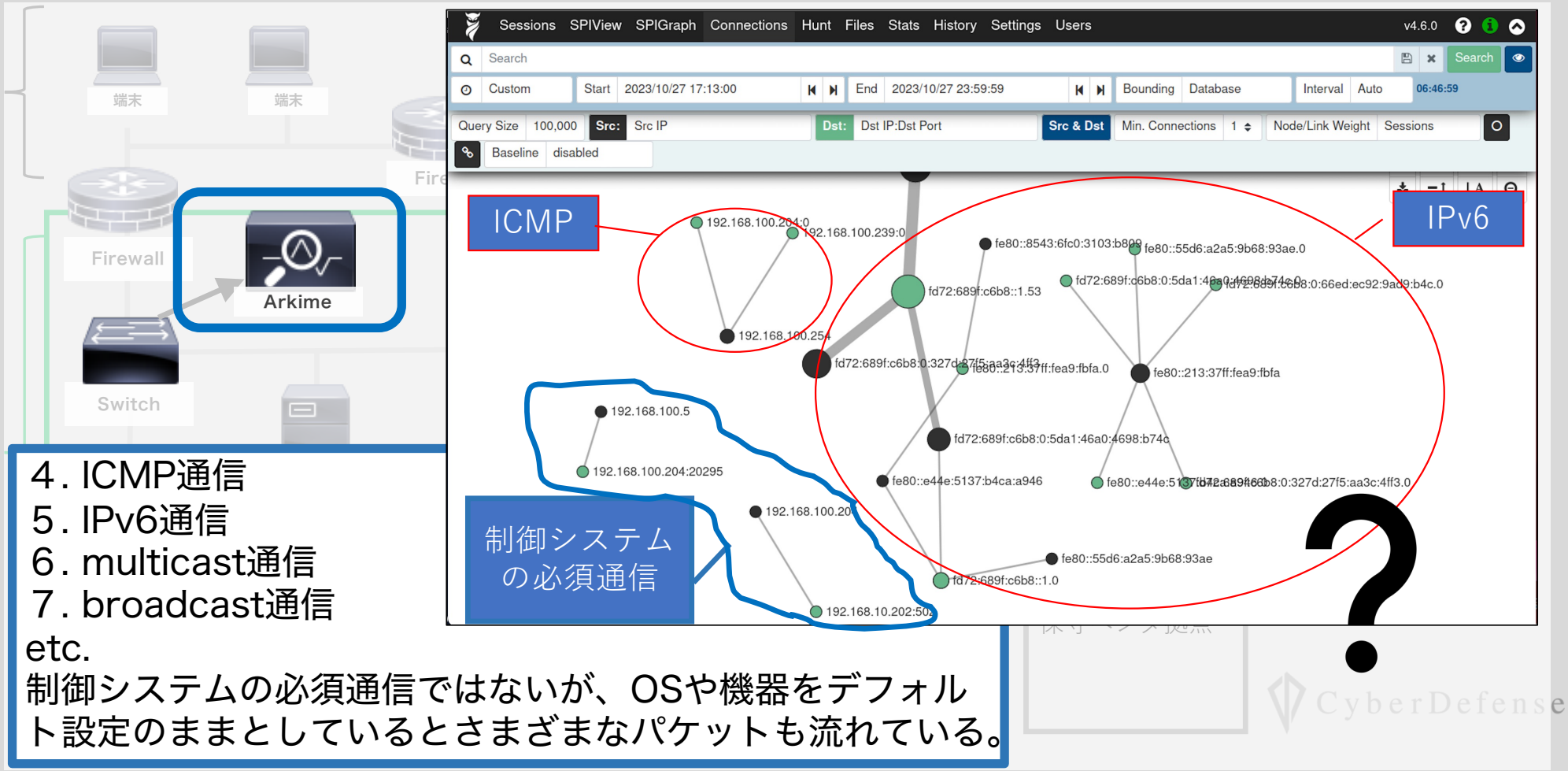
・保守に必要な通信
3. 保守用サーバとSCADAサーバ（TCP/22）

通信監視結果



複雑で理解困難。
シンプルな通信しかしてないのに、なぜこんなに複雑か？

通信監視結果　解説１



4. ICMP通信
5. IPv6通信
6. multicast通信
7. broadcast通信

etc.

制御システムの必須通信ではないが、OSや機器をデフォルト設定のままとしているとさまざまなパケットも流れている。

通信監視の工夫

PC、監視結果を見る人間の能力・労力にリソース制限ないのであれば全てのパケットをキャプチャした方がセキュリティ上好ましい。しかし、限られた予算では非現実。

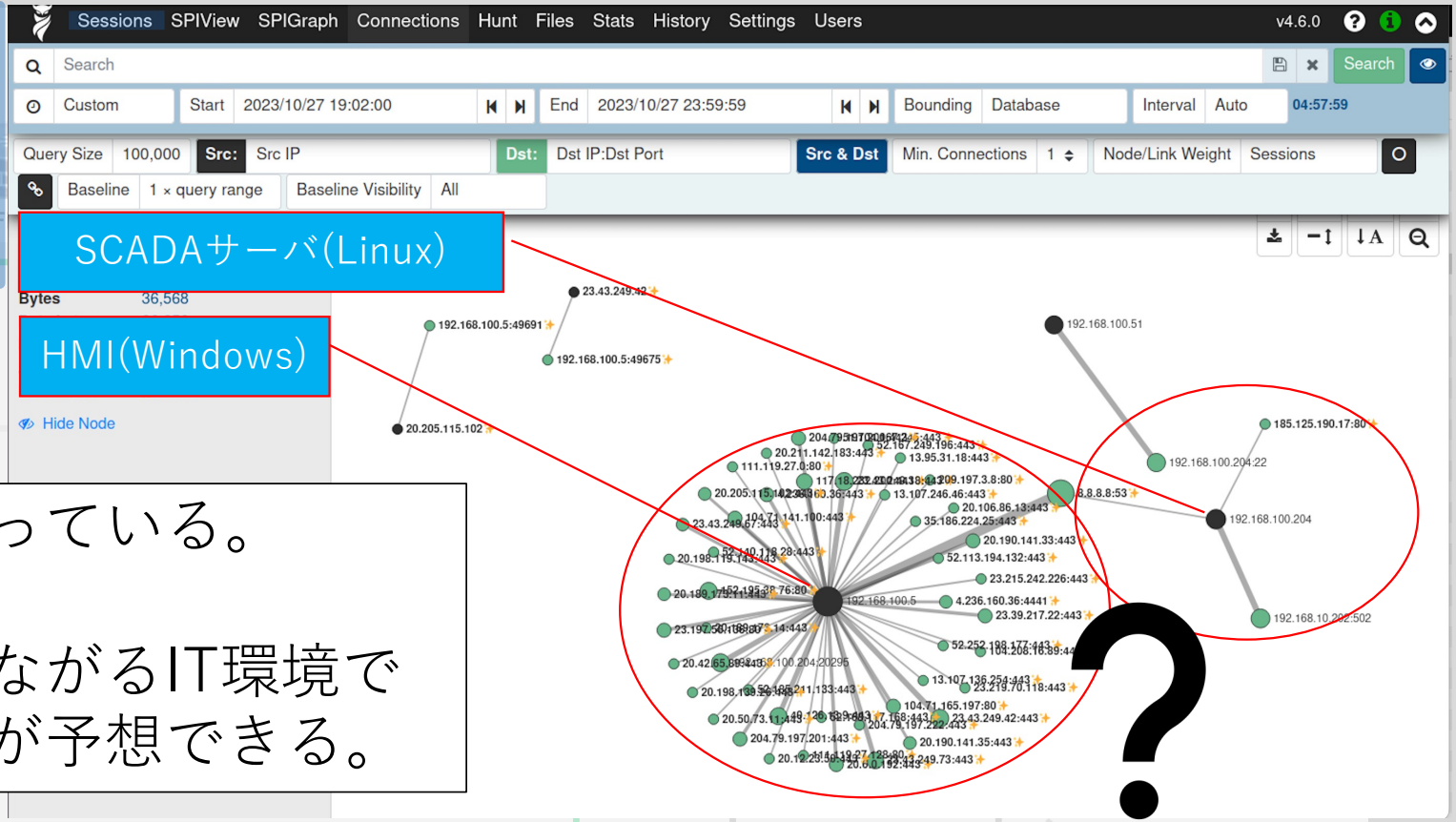
→ 妥協策　最低限見たいところを見る
当該制御システムで、攻撃可能性の低そうなプロトコルや、過去の制御システムにおけるインシデント事例ではあまり見かけない通信プロトコルをキャプチャ対象外とする。
４. ICMP通信
５. IPv6通信
６. multicast通信
７. broadcast通信
残るのは、IPv4のtcp or udp の unicast通信

→ 長期的な対策
システム企画段階から不要なパケットは流さない方針とする。
発注者：発注要件
設計者：基本設計思想

工夫後の通信監視結果

参考比較：インターネットと通信していた仮定の監視結果

以下はキャプチャ対象外
4. ICMP通信
5. IPv6通信
6. multicast通信
7. broadcast通信



一目瞭然で複雑になっている。

インターネットとつながるIT環境で
の通信監視の大変さが予想できる。

攻撃してみて侵入兆候の監視

CyberDefense

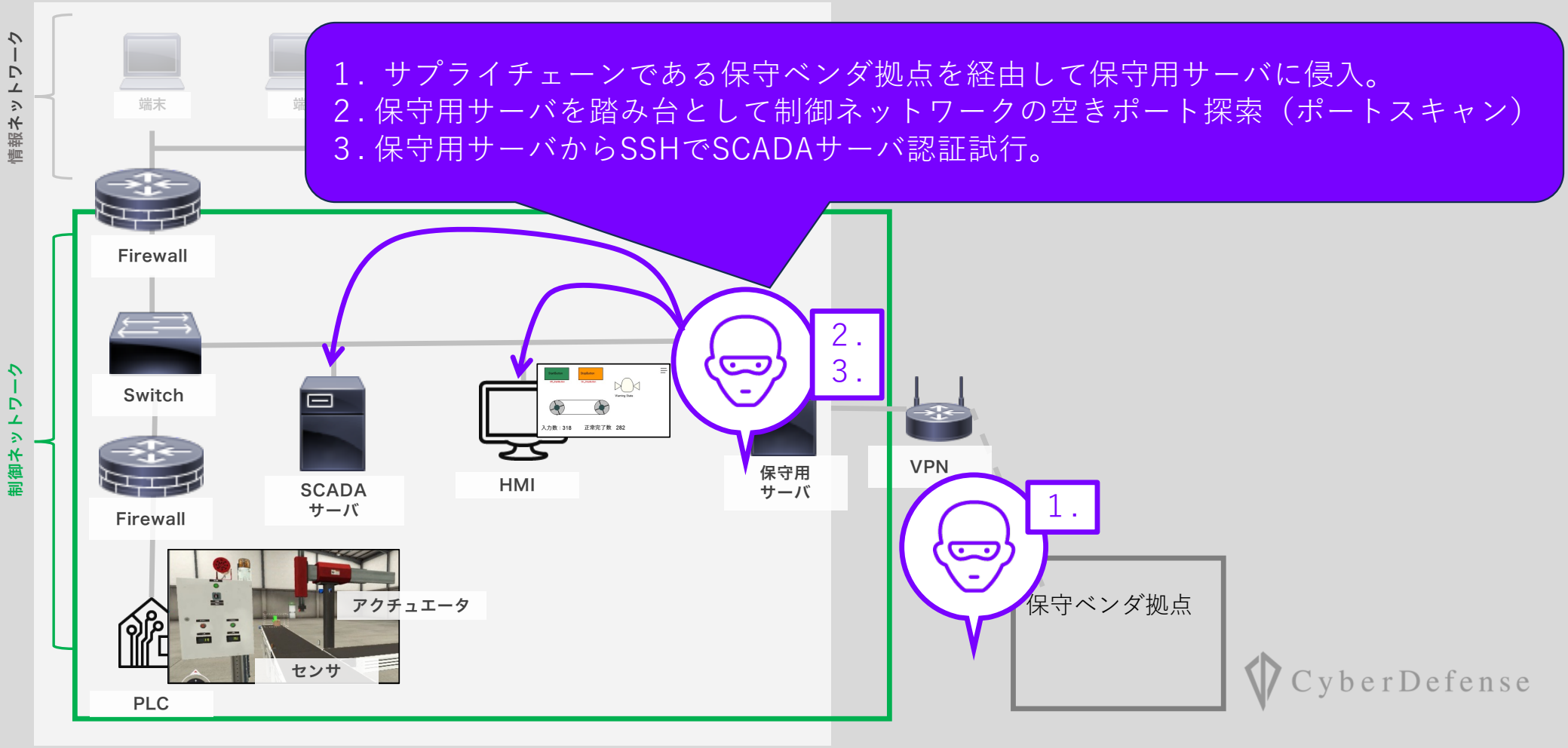
ありえそうな攻撃を想定

- 攻撃シナリオ１
  サプライチェーンから保守用サーバに侵入

- 攻撃シナリオ２
  BadUSBをHMIの空きUSBポートに挿す

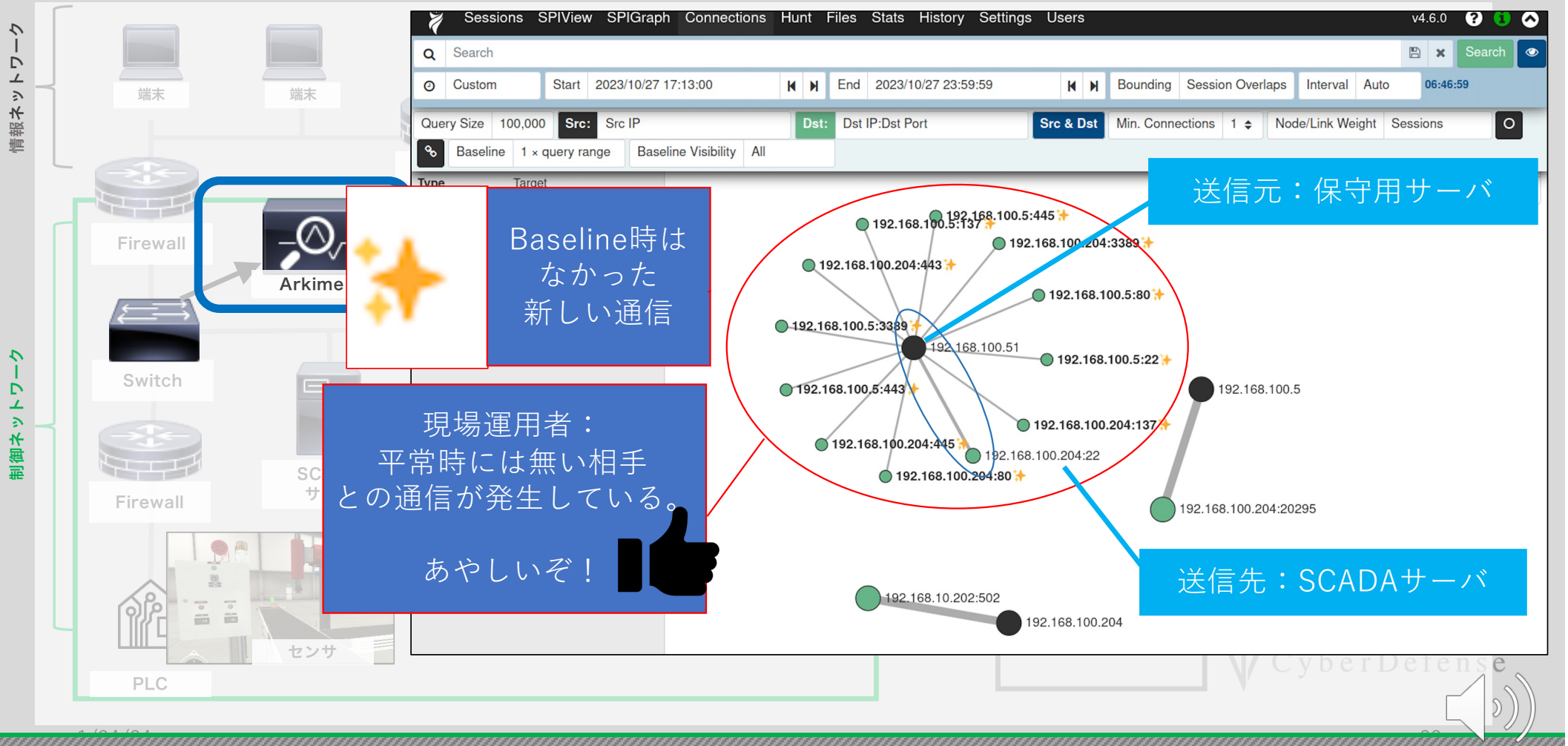
CyberDefense

攻撃シナリオ１：サプライチェーンから保守用サーバ侵入

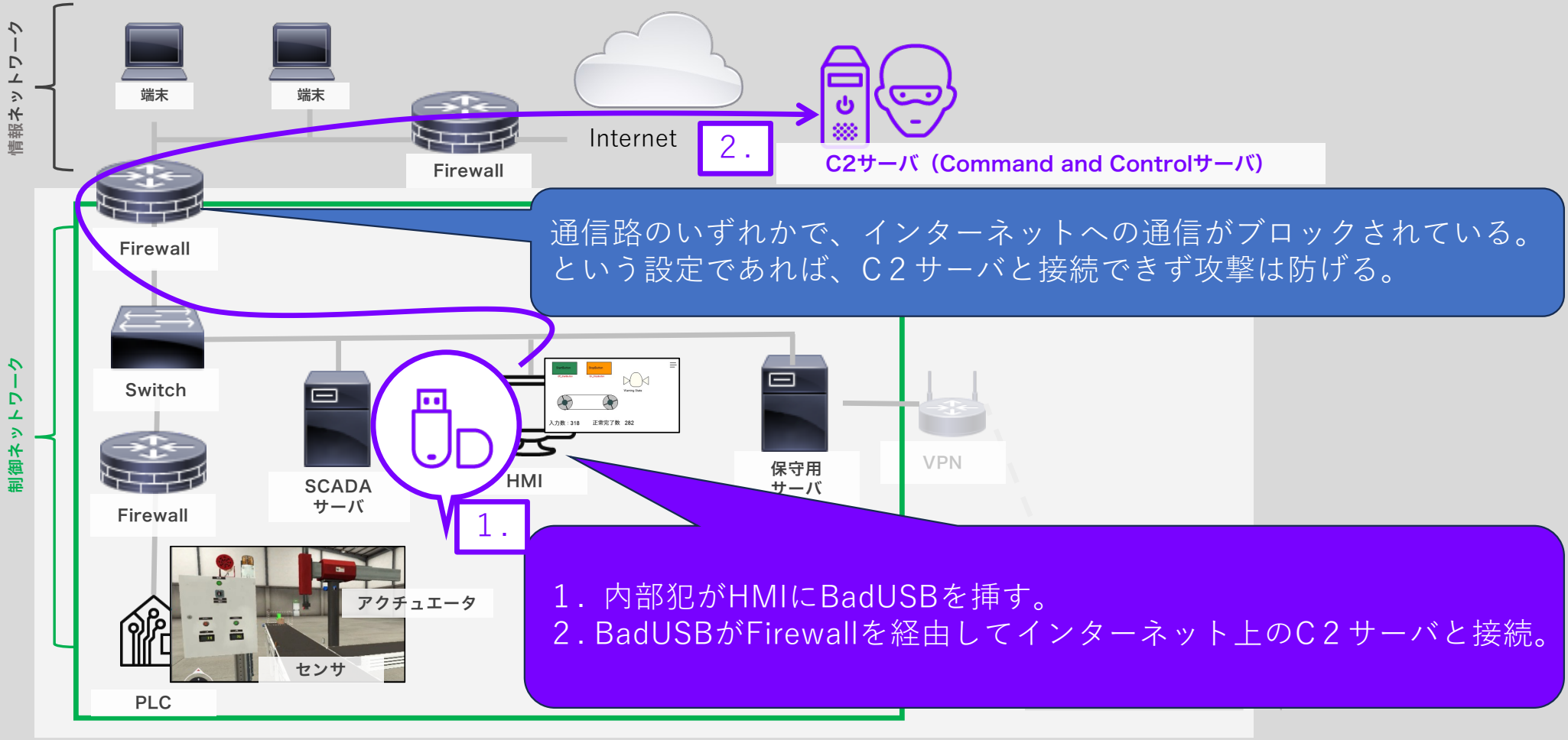


CyberDefense

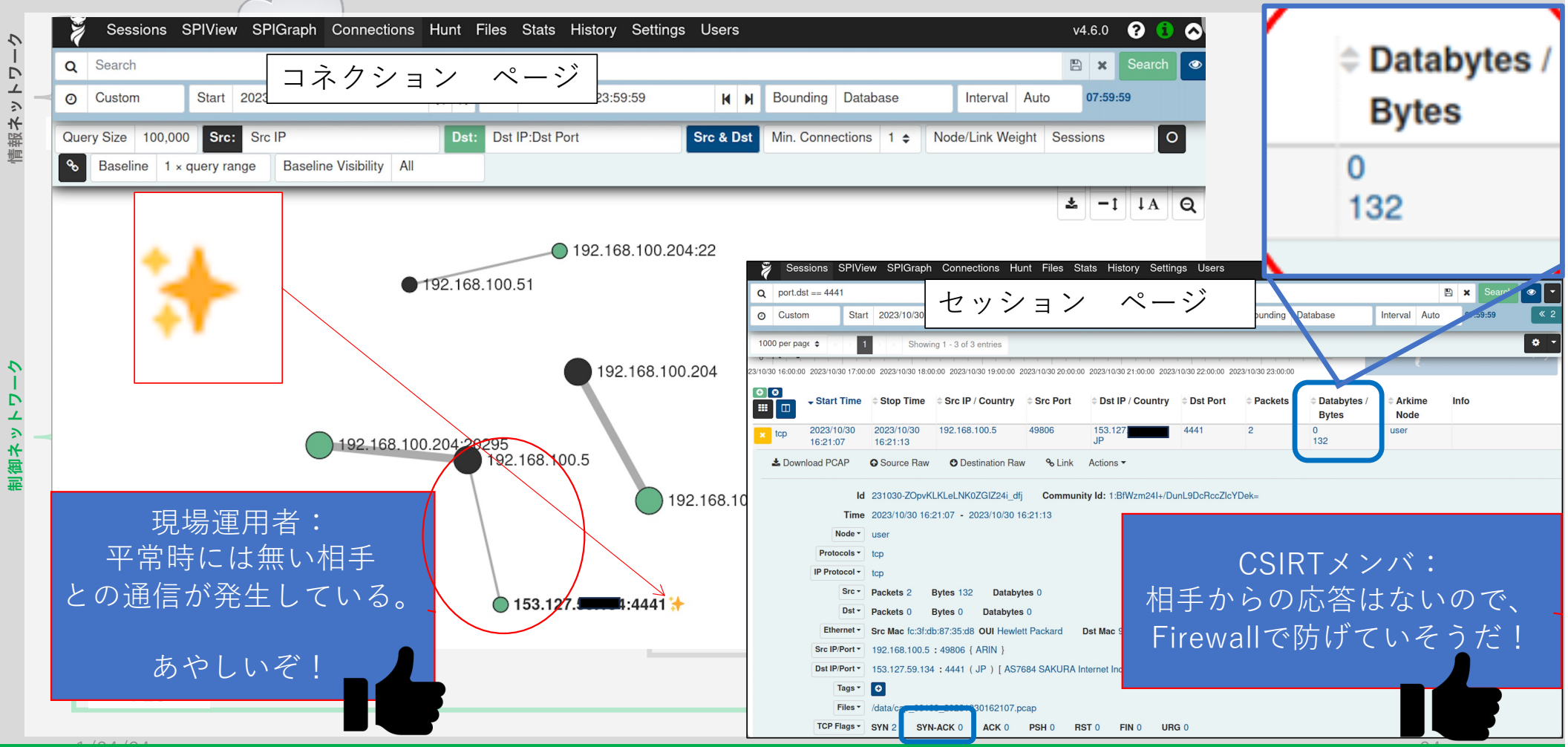
攻撃シナリオ１後の通信監視結果



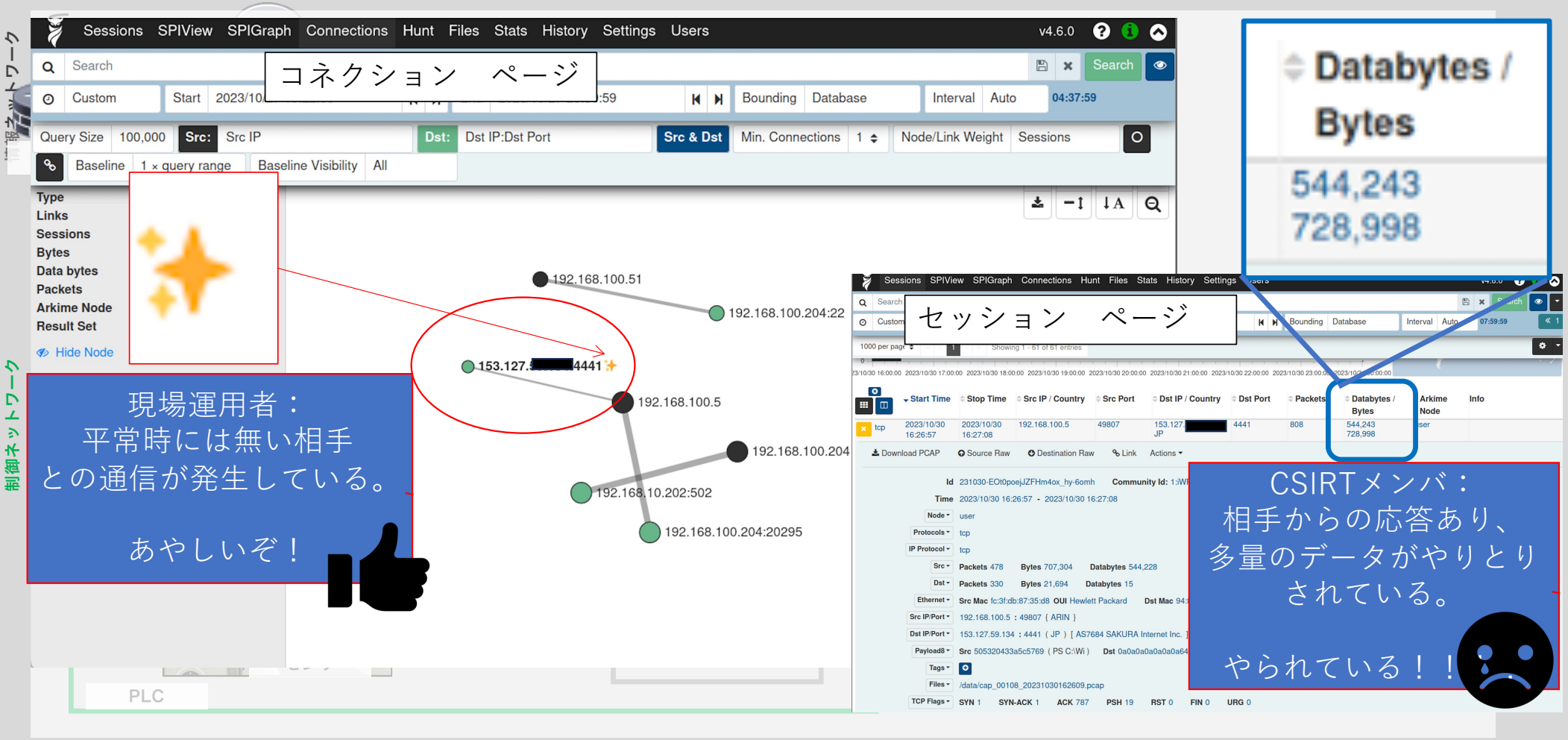
攻撃シナリオ2：BadUSBを挿してC2サーバへ接続



攻撃シナリオ２後の通信監視結果（C2接続防げる場合）



攻撃シナリオ２後の通信監視結果（C2接続された場合）

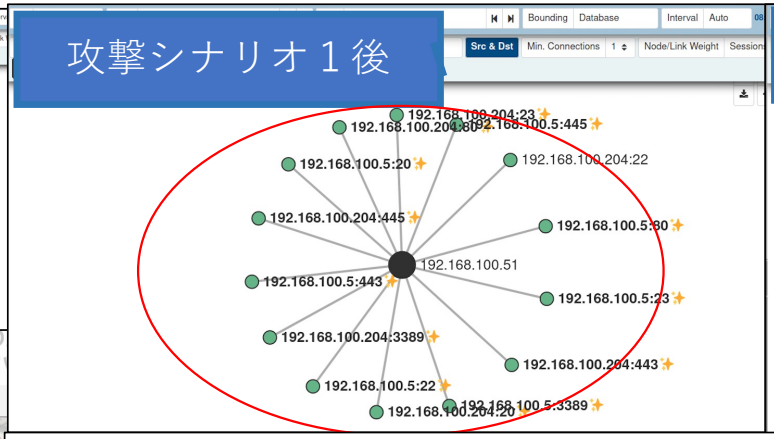


通信監視をもっと工夫

適用する上で問題がありそうな事
・機器が多くてチェックが大変。
・平常時のパケットが多すぎてPCリソース足りない。
→ もっと妥協案　制御システムの運用に必須な通信も　キャプチャ対象外とする。
平常時で残るのは、保守の通信のみ

平常時
保守の通信のみ

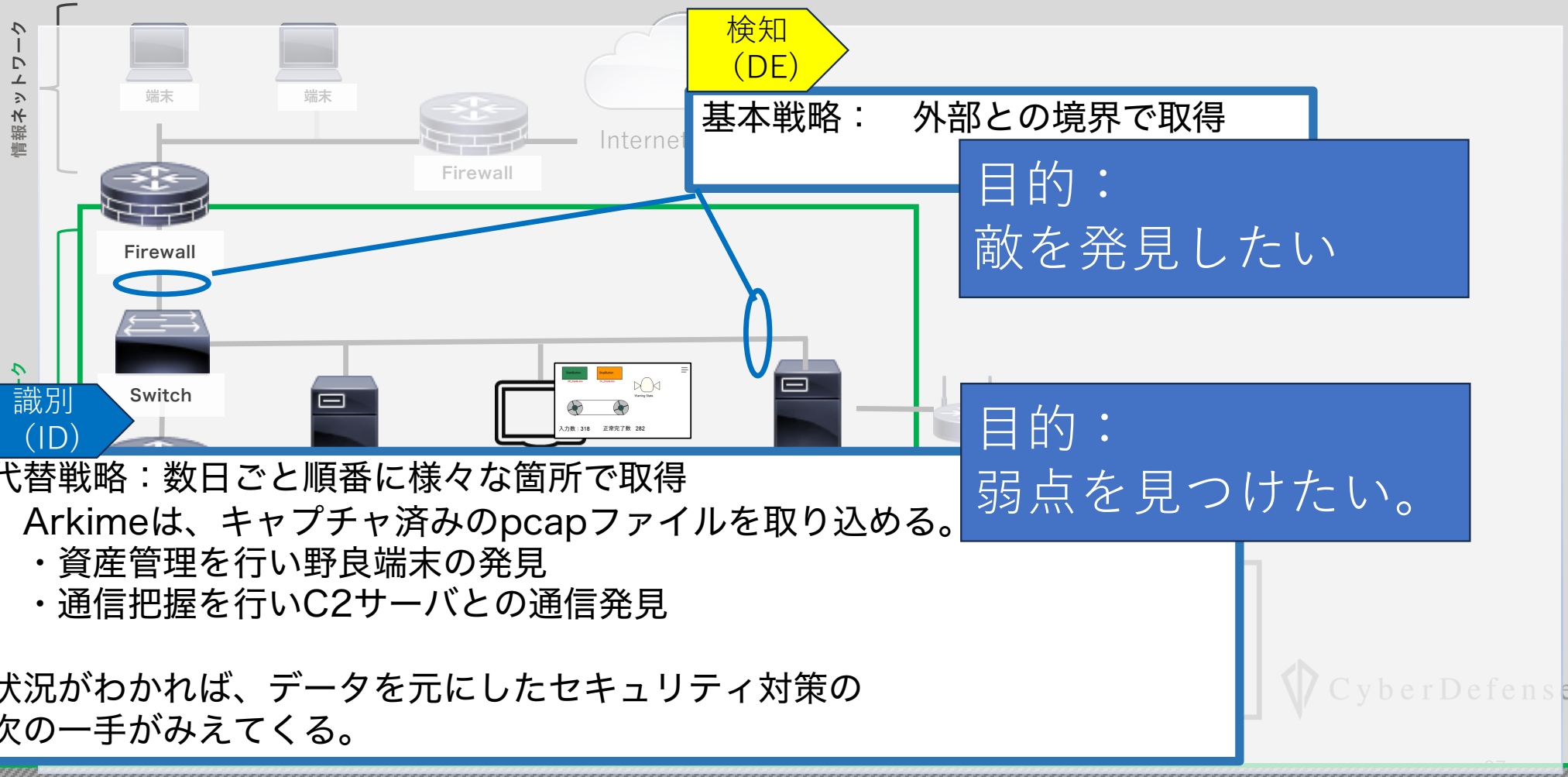
攻撃シナリオ１後



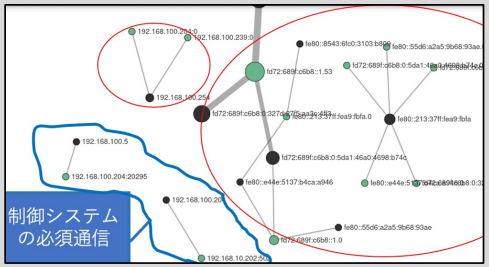
攻撃シナリオ２後

保守の通信以外が発生していることが、一目瞭然

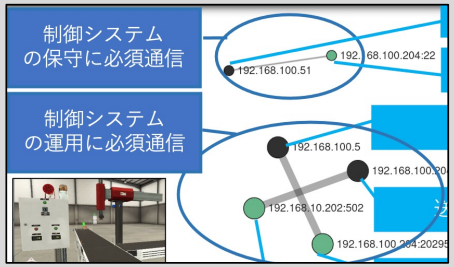
常時キャプチャできない時、弱点把握としての使い方



システムを開発・提供する方へ



従来：考慮なし



将来：必須通信のみ

参考：最新　2023年9月28日発行 NIST SP800-82 Rev.3
OTセキュリティへのガイドの抜粋

•5.2.3.1 Network Architecture
- OT-Specific Recommendations and Guidance
  One area of considerable variation in practice associated with firewall rules is the control of outbound traffic from the control network. Allowing outbound connections from lower levels, tiers, or zones could represent a significant risk if unmanaged. Organizations should consider making outbound rules as stringent as inbound rules to reduce these risks.

•5.2.3.3. Network Monitoring
- OT-Specific Recommendations and Guidance
  OT system traffic is typically more deterministic (i.e., repeatable, predictable, and designed) than IT network traffic, which can leveraged to support network monitoring for anomaly and error detection.

OT固有の推奨

防御
（PR）
アウトバウンドはインバウンドと同じくらい厳格に！

検知
（DE）
OTトラフィックはITより予測可能、異常検知に活用！

まとめ

まとめ

・通信監視は、OT環境と相性が良い理由を説明
・スモールスタートとしてOSSのArkimeを紹介
・どのような侵入兆候を検知できるかを模擬制御システムをつかって紹介
・OT環境での監視における運用方法のヒントを紹介

ぜひ自らためしてみてください

CyberDefense

今回紹介した事例は、スモールスタートの基本的な内容です。

見えないから分からなかった事でも

　一歩踏み出すことで

　　比較的容易に見えてくるものです

今回紹介した内容を試すことで、自分達のシステムの資産と通信を把握でき、通信監視製品を選定するための基礎知識を得ていただければ幸いです。

CyberDefense

インストール設定詳細は、

「サイバーディフェンス研究所ブログ　DARKMATTER」で公開

https://io.cyberdefense.jp/entry/ot_ids_oss/

以上

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

CyberDefense

参考：通信監視運用の前にやっておきたい対策

監視するなら、基本セキュリティ対策もやっておきたいものです。

・ファイアウォールの設定
　インバウンド・アウトバウンドともに必要最小限の通信のみ許可
・認証情報の保護
　平文で保存しない。パスワードの使い回しはしない。
・復元できるバックアップ
　ランサムウェア対策としてシステム復元できるように

パッチ適用できない環境でも行える効果的な対策はある。

CyberDefense

参考：紹介した方法で検知できない攻撃

こんな攻撃が心配で検知必要と考えるなら更なる対策を考えて

- 制御システムに必須の通信をつかった攻撃

例１：サプライチェーンから保守サーバに侵入した攻撃者が、保守サーバ上に平文保存されていたSCADAサーバの認証情報を取得。保守作業員がメンテナンス作業をおこなうスケジュールにあわせ、SSHでSCADAサーバに侵入。制御に関わるプログラムや設定情報を改ざん、もしくは、SCADAサーバからPLCに制御命令を送信。

例２：サプライチェーンから保守サーバに侵入した攻撃者が、中間者攻撃で監視・制御に関する通信を盗聴・改ざん

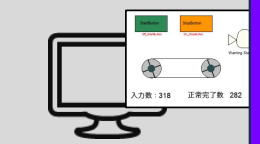
ここまで守りたいとなると、より豊富な監視機能をもつツールを導入するのがよいかもしれません。

CyberDefense

こんな攻撃が心配で検知必要と考えるなら更なる対策を考えて

- **エアーギャップ越しの攻撃**

例３：内部犯が、USBを悪用しエアーギャップ越しにHMIをC2サーバと接続し、C2サーバからHMIをリモートデスクトップ操作。



HMI

制御ネットワークがインターネットと接続するルートがない（エアーギャップ）環境と仮定

１．内部犯が、LTE回線モデムをHMIに挿す
２．内部犯が、 BadUSBをHMIに挿す
（LTE回線を経由してC２サーバとセッション確立する。）

以降のながれは、攻撃シナリオ２と同じ。

このような攻撃手法を知ると、未使用のUSBポートを閉じる対策が、それなりの効果があることがイメージつきやすいかもしれません。

CyberDefense

検知だけでは心配と考えるなら更なる対策を考えて

- **検知されてもよい前提での攻撃**

例４：短時間で自律的に感染をひろげて被害発生させるマルウェア

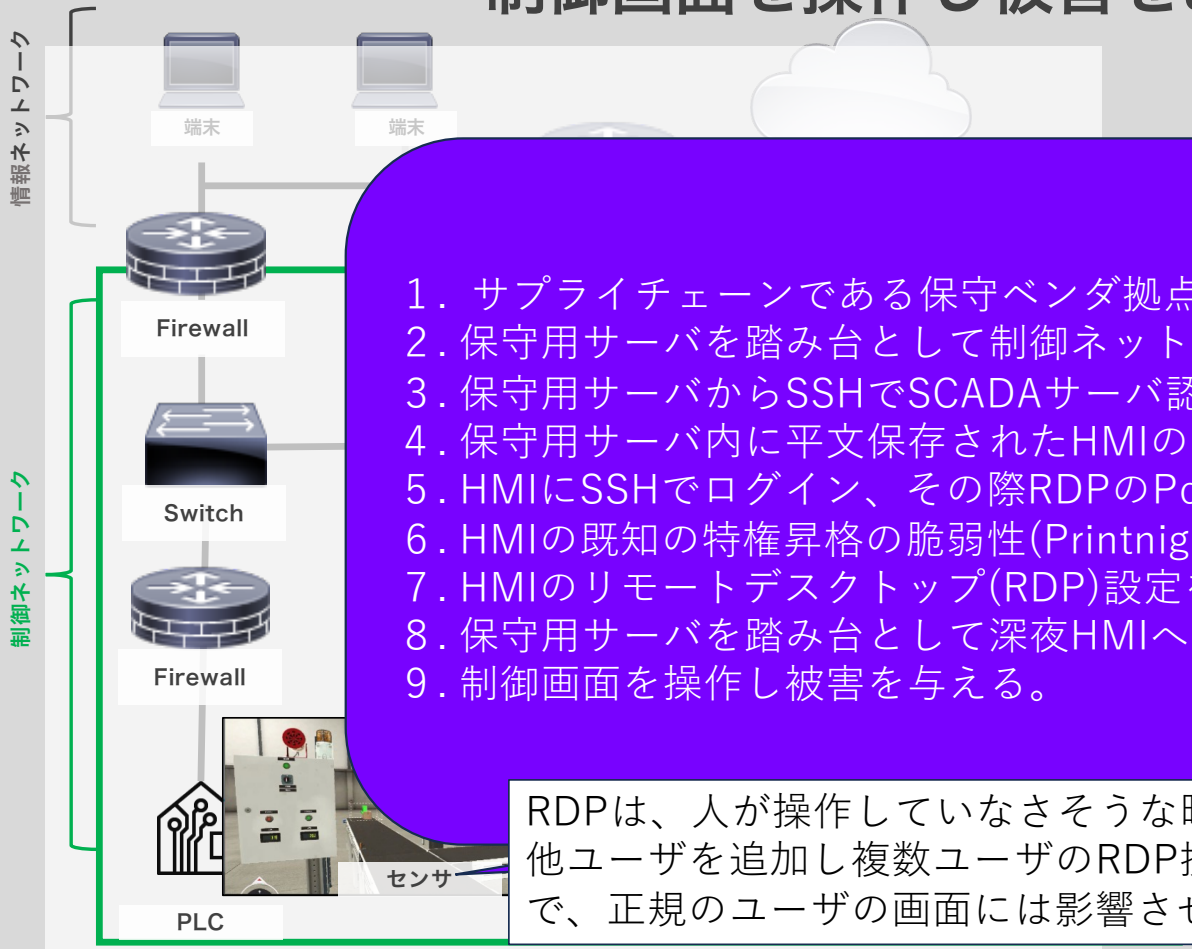
当然ながら検知対策は、検知した上で何かしらのアクションを起こさなければ防御とはなりません。

検知対策が被害を防げるのは、検知してから被害発生までの間に、対策を行える時間がある場合となります。

CyberDefense

参考：制御画面を操作するまでのシナリオ例

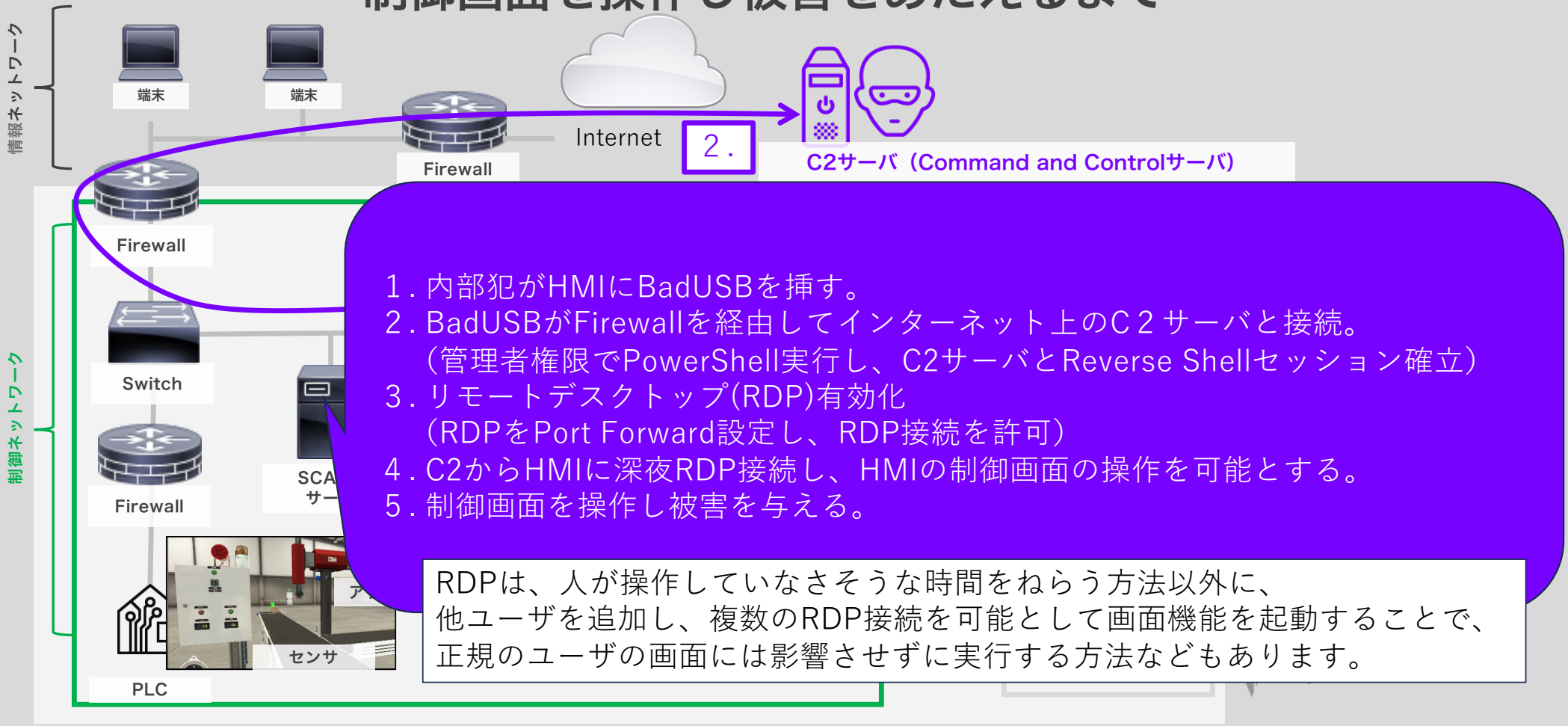
攻撃シナリオ１：サプライチェーンから保守用サーバ侵入後、制御画面を操作し被害をあたえるまで



1. サプライチェーンである保守ベンダ拠点を経由して保守用サーバに侵入。
2. 保守用サーバを踏み台として制御ネットワークの空きポート探索（ポートスキャン）
3. 保守用サーバからSSHでSCADAサーバ認証試行。
4. 保守用サーバ内に平文保存されたHMIのSSHユーザ・パスワードを窃取
5. HMIにSSHでログイン、その際RDPのPort Forwardを設定。
6. HMIの既知の特権昇格の脆弱性(Printnightmare)を発見し管理者権限取得
7. HMIのリモートデスクトップ(RDP)設定を有効化
8. 保守用サーバを踏み台として深夜HMIへRDP接続し、HMIの画面の操作を可能とする。
9. 制御画面を操作し被害を与える。

RDPは、人が操作していなさそうな時間をねらう方法以外に、
他ユーザを追加し複数ユーザのRDP接続を可能として画面機能を起動することで、正規のユーザの画面には影響させずに実行する方法などもあります。

攻撃シナリオ2：BadUSBを挿してC2サーバへ接続した後、制御画面を操作し被害をあたえるまで



1. 内部犯がHMIにBadUSBを挿す。
2. BadUSBがFirewallを経由してインターネット上のC２サーバと接続。
（管理者権限でPowerShell実行し、C2サーバとReverse Shellセッション確立）
3. リモートデスクトップ(RDP)有効化
（RDPをPort Forward設定し、RDP接続を許可）
4. C2からHMIに深夜RDP接続し、HMIの制御画面の操作を可能とする。
5. 制御画面を操作し被害を与える。

RDPは、人が操作していなさそうな時間をねらう方法以外に、
他ユーザを追加し、複数のRDP接続を可能として画面機能を起動することで、
正規のユーザの画面には影響させずに実行する方法などもあります。


ONLY
HUMANS CAN
COUNTER
HUMAN-DRIVEN
THREATS
CyberDefense
お問い合わせはこちらへ
https://www.cyberdefense.jp/contact/