これまでの国内外における OTセキュリティの取り組み

株式会社テリロジー
OT/IoTセキュリティ事業部
執行役員　部長　御木 拓真

アジェンダ

- テリロジーって何している会社？
- 苦労話
- 現場第一主義
- 新たな取り組み
- 海外イベントに参加しました

アジェンダ

- テリロジーって何している会社？
- 苦労話
- 現場第一主義
- 新たな取り組み
- 海外イベントに参加しました

株式会社テリロジー　～サイバーセキュリティイネーブラー～

企業のデジタル革新を支える

IT/OT/IoT サイバーセキュリティ イネーブラー

テリロジー　取り扱い商材一覧

ネットワーク商材
- Infoblox — DNS/DHCPサーバ
- radware — ロードバランサー 回線マルチホーミング

OT/IoTセキュリティソリューション
- waterfall — 一方向セキュリティゲートウェイ（データダイオード）
- NOZOMI NETWORKS — OT/IoTセキュリティ（可視化/脅威検知:OT-IDS）
- txOne networks — OT向けIPS OT向けエンドポイントセキュリティ USB型ポータブルセキュリティ
- SALVADOR TECHNOLOGIES — サイバーリカバリソリューション
- FORTINET — FortiGate /OT/IT分離
- Tempered — OT-ZTNA セキュアリモートアクセス
- SecurityGate.io — OTリスクアセスメントプラットフォーム

ITセキュリティソリューション
- RAPID7 — 脆弱性スキャナー&Metasploit
- radware — DDoS対策ソリューション（DefenseProシリーズ）
- Infoblox — DNSセキュリティ
- TREND MICRO / TippingPoint — IDS/IPS専用装置
- OneSpan — ワンタイムパスワード 二要素認証
- TREND MICRO Deep Discovery Inspector

クラウドセキュリティ
- ORACLE Cloud
- sumo logic — Cloud Native-Log Analysis /SIEM/UEBA/SOAR
- aws / Microsoft Azure
- CATO NETWORKS — SASE solution
- TREND MICRO C1NS (Cloud IPS)
- Infoblox — DNSセキュリティ
- CORESTACK CSPM
- RAPID7 — 脆弱性スキャナー
- radware — Cloud WAF/DDos

CTI商材
- BITSIGHT — サイバーリスク スコアリングサービス
- DOMAINTOOLS — フィッシングサイト対策
- DARKOWL — クレデンシャル、カード情報、IPアドレス、機密情報漏洩検知
- TEAMT5 — エンドポイント セキュリティ ＊脅威ハンティング ＊メモリフォレンジック
- Cyabra — SNS分析プラットフォーム 風評被害・偽情報発見

RPA/運用管理/モニタリング商材
- RPA EzAvater（自社開発） — RPAツール プログラミングのナレッジ不要！
- CloudTriage（自社開発） — ユーザ体感品質の測定 M365のモニタリング エンドポイント挙動監視
- TechSee — 映像共有カスタマーサポート ツール
- THX（自社開発） — パケットキャプチャツール

TERILOGY Holdings

TERILOGY

平成元年設立
Terilogy HQ

JPX STANDARD TOKYO
5513

DX認定

bsi ISO 14001 Environmental Management CERTIFIED / ISO/IEC 27001 Information Security Management CERTIFIED
IS 97125 / ISO27001
EMS 513188 / ISO14001

TERILOGY SERVICEWARE

みえる通訳
96%
zoom
Biz翻訳

CONSTELLA SECURITY JAPAN

Cyber Threat Intelligence
momentum
THX
BITSIGHT The Standard in SECURITY RATINGS
KELA TARGETED CYBER INTELLIGENCE
DOMAINTOOLS

VN GLOBAL

政府認定SOC事業＆OTセキュリティ事業

OT/IoTセキュリティに取り組むお客様に対し活動実施

株式会社テリロジー
OT/IoTセキュリティ事業部　部長
御木 拓真

2017年:OT/IoTセキュリティ事業取り組み開始
2017年:Tempered Networks（現:Johnson Controls）取り扱い開始
2018年:Nozomi Networksディストリビューター開始
2022年:Security Gateディストリビュータ開始
2022年:Waterfall security Solutionsディストリビューター開始
2023年:TXOne Networksディストリビュータ開始
2024年:Salvador Technologies（OTバックアップ/リカバリ）開始

2004年 テリロジーに入社後、通信キャリア向けセールス/開発プロジェクトに従事し、2017年からOT/IoTセキュリティ対策、特にOT領域におけるセキュリティ対策ソリューションの開発に従事。

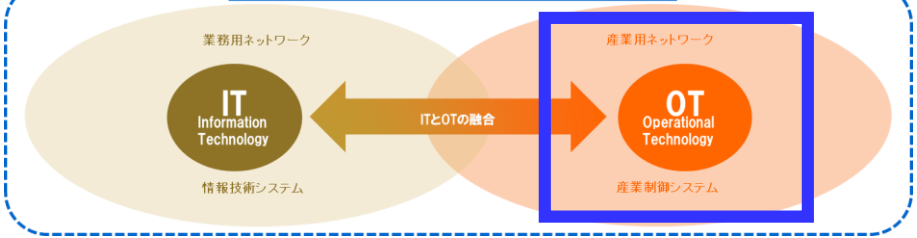
国内外の重要インフラ企業や製造業のお客様に、制御システムセキュリティの最新技術提案やソリューション含めたトレーニングなどを実施。

2018年/Nozomi Networks社とディストリビューター契約を交わし、国内の製造業・重要インフラのお客様にOTセキュリティの製品をご提供。製造/制御システムをサイバー攻撃から如何にして守り、安心・安全のお手伝いに取り組む

OT/IoTセキュリティに取り組むお客様に対し活動実施

情報ネットワーク（IT）と制御ネットワーク(OT)を安全に接続
～ネットワークの脆弱性とIoTのセキュリティ対策～

ITとOTをトータルで守る統合セキュリティ



サイバー攻撃

●重要インフラ14分野

・情報通信	・鉄道	・政府・行政サービス	・化学
・金融	・電気		・クレジット
・航空	・ガス	・医療	・石油
・空港	・水道	・物流	

- 電力（送配電/発電/需給）
- 石油 & ガス
- 製造業/ローカル５G
- 化学
- 製薬
- 交通機関
- ビル
- 水道/ダム
- 倉庫/物流
- 空港
- 船舶
- スマートシティ

狙われるOT・制御





私たちのミッション

重要インフラ/OT/IoTに対するセキュリティ

電力・ガス・石油・化学・船舶・鉄道・ビル・空港・食品/飲料・製造

安心・安全のお手伝い

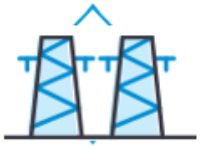
日本国内でも取り組みは進んできております。

私達【 テリロジー 】は、

実際に　　一緒に　　を考え

活動を実施しております

私達がOT/IoTセキュリティでご支援させて頂いた業種



電力

オイル/ガス

化学

食品/飲料

物流/倉庫

製造

製薬/医療

船舶

自動車メーカ
パーツメーカ

半導体

ビルディング

OTセキュリティのすゝめ:ステップごとに対策を実施

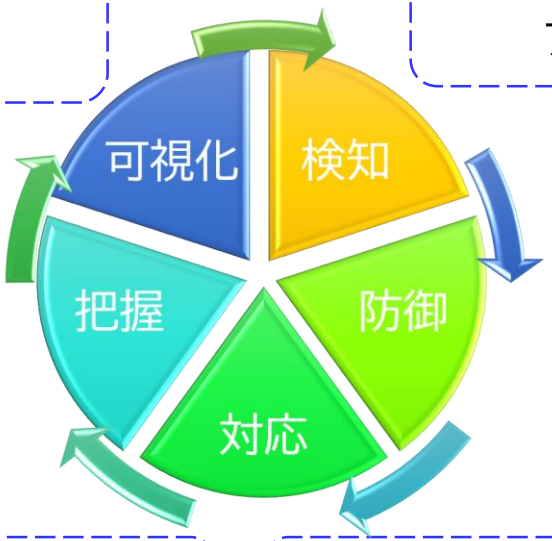
ビジネスリスクは何か？	✓ 自社にとっての最優先を考える。事業継続を脅かすリスクは？
企業/組織の理解・意識付け	✓ 組織として自分事に。役割を明確に。脅威を認識し現場と相互理解。
現状把握/リスク分析	✓ 自社の状況はどのような状況。どこにセキュリティリスクがあるか。
資産・通信・脆弱性の可視化	✓ 工場の資産は？ IT/OTはどのように接続？ 脆弱性の把握へ
IT/OT境界分離/脆弱性対応	✓ IT/OT分離を行い、直接繋げない。優先順位決め必要な対策を。
OTネットワーク対策_検知・防御	✓ OT環境に特化したソリューションを検討。専門家の知見と共に。
OTSOC運用・IT・OT統合管理	✓ セキュリティは運用が必須。監視・ログ取得・攻撃検知・報告実施
人材教育・体制強化・情報収集	✓ ログ解析・フォレンジック解析・マルウェア解析・

OTセキュリティポートフォリオ

OTセキュリティ人材育成　/　OTセキュリティ外部運用委託(OT-MSS)

サイバーセキュリティリスク評価
サプライチェーンリスク評価
企業のセキュリティリスクを可視化

OTリスクアセスメント
アセスメントプラットフォーム



可視化＆現状把握
資産の可視化/通信の可視化/経路の可視化

OT-IDS/ハイブリッド脅威検知

OTゼロトラストNWアクセス
デバイスクローキング
(見えない＝攻撃されない)

一方向
セキュリティゲートウェイ

レガシーOS/脆弱性を保護
/仮想パッチ

ランサムウェア対策
オフラインバックアップ/リカバリー

テリロジー
～OTセキュリティポートフォリオ～

サイバーセキュリティ評価
①Bitsight（EASM）
「 Bitsight 」

OTリスクアセスメント
②Security Gate
「SecurityGate」

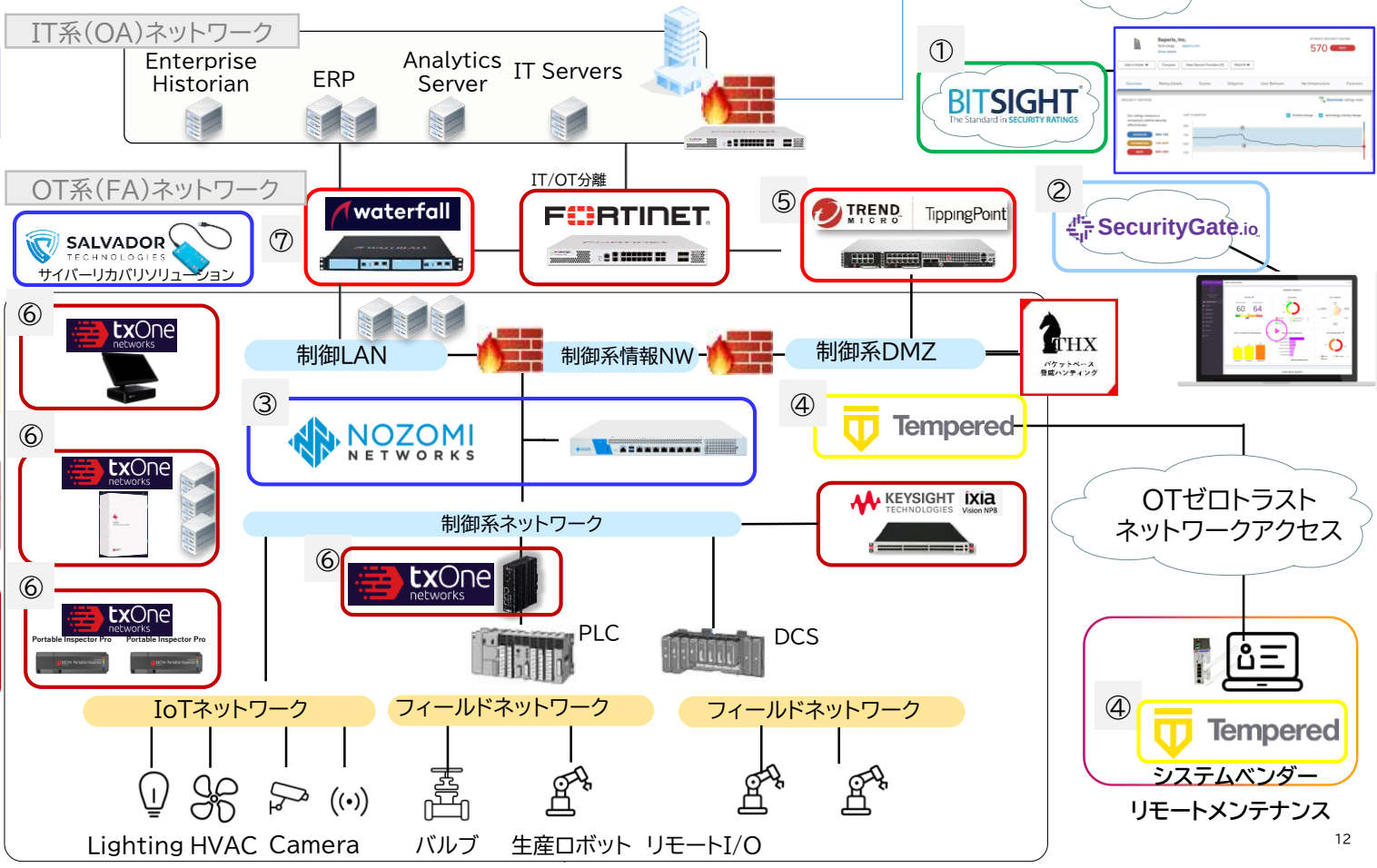
可視化/異常・脅威検知
③Nozomi Networks
「 Guardian 」

セキュアリモートアクセス
④Tempered
「 Airwall 」

脆弱性対策攻撃対策
⑤ トレンドマイクロ
「 TippingPoint 」

⑥産業用向けIPS
TXOne Networks
「 Edge IPS」
「Portable Inspector」

一方向ゲートウェイ
⑦Waterfall
「 Unidirectional Security Gateways 」



アジェンダ

- テリロジーって何している会社？
- 苦労話
- 現場第一主義
- 新たな取り組み
- 海外イベントに参加しました

苦労話・・・

- 2016年　OTセキュリティ調査開始　　※当時は　ICS　セキュリティの呼び方主流
- 2017年　リモートアクセス＆セグメンテーション製品を展開。 興味頂けず。。。
- 2018年　**Air Gap**　神話が当たり前の時期・・・

「あっ。大丈夫。ウチは工場クローズドNWで安全だから」

「そもそも、工場の中がのモノが分からないのに、つなぐなんてありえないよ」

⇒ならば、工場の中がどうなっているのか分かる必要がある！

⇒そして、海外と違った文化を持つ日本に合うソリューションが必要！

⇒日本のお客様になじむ製品を探そう！

苦労話・・・

苦労

認知度向上

- 2018年 **Nozomi Networks 代理店契約/正式取り扱い開始！**
- 2018年 そもそもOTセキュリティ市場が形成されて無く、販売はほぼ「0」状態。

  ⇒ IT部門とOT部門が仲が悪い。セキュリティは投資。必要性感じられていない
- 2019年 以前商用導入無し、戦略切替,市場開拓では無く,「市場創造」及び「共創」へ
- 2020年 オリパラをきっかけに重要インフラ事業者様のセキュリティ対策活発化

  ⇒**電力・ガス・化学**のお客様と会話ができるようになる

  ⇒知ってもらう為に,「**OTセキュリティとは？**」を毎月100名以上にウェビナー実施
- 2021年 製造業のお客様でのニーズが掘り起こしされ始める。

  ⇒コロナ化における業務＆現場改革/製造DX/IoTの実装

当時のお客様の状況　2019年～21年

- 「実は、、、工場でマルウェアが見つかって。。。この間もHMIの動作が重くなって
  現場担当から連絡あって、実際に確認していたらその時にブルースクリーンに。。」

  ⇒緊急チームを作り対策乗り出すも、どんな資産が工場にあるか不明。。。
  まずは、手作業で台帳作成・整理から開始。。。。

- 「インターネットにつながっていなければ安全。」と仰られていたお客様。。。
  ウィルス感染。2000年代に流行したWindowsの脆弱性狙うウィルス。。
  ⇒USBからの感染。 しかもワーム。 Autorunを悪用

- ある半導体関連のお客様。 ネットワーク調査をさせて頂く。
  ⇒結果、、、SMBv1の通信が9割。 IT側とも通信可能なNW。。
  一番の問題は、、「　リスク　」と感じておらず。。。

導入ポイント　～背景・状況～

導入ポイント ： 資産台帳の不正確が露呈 ・ 海外工場でのインシデント ・ 経営層の理解

業種：製造業

規模：国内外50以上の拠点

状況：OT部門とIT部門で連携を図り、会社全体として工場セキュリティ/見える化PJを推進

■背景

① 生産設備部で資産台帳の管理はできていたが、**IT部門からの指摘により不完全に気付く**

② **海外拠点のIT端末インシデント発生**。 ウィルスチェックを実施したところ、OTネットワーク側のPCの感染も確認。

③ 影響範囲の特定に時間がかかった。 理由＝資産管理は不完全だが程度できていたが、ネットワークは把握できていなかった

■導入に向けて

✓ 上記インシデントを受けて、 **経営層から早急に対応するよう指示**のもと、本格検討を開始

✓ 各社製品の情報を収集し、比較検討を実施

✓ PoCを行い、自社のメンバー（IT側セキュリティ部隊）が操作を行い、**直観的操作が可能な製品**を重視のうえ選定

✓ 最終的に、数製品に絞りRFPを作成。 スモールスタートにて　Nozomi Networksを導入を実施　⇒現在10拠点以上に導入

3ヵ年計画 OTセキュリティプロジェクト：可視化・脅威検知

	POC/モデル工場選定				モデル工場本格運用				国内外工場への横展開			
	202X				202X				202X			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
テーマ	POC実施	ご提案フェーズ		課題抽出体制づくり	モデル工場での運用含めたテスト稼働				各工場横導入へ			
お客様	POC工場選定	モデル工場選定 OT-SECの検討		モデル工場へ導入	常設運用＆OT-SEC検討	各工場へ展開説明 各工場サイジング		各工場展開へ				
テリロジー	POCご提案 POC実施完了	OTSECご提案	導入に向けご提案	導入に向けサイジング・設計	お客様と共に課題に対しご提案を実施 (例) ①OT運用体制づくり支援 ②運用支援 ③OTセキュリティ教育							

※POC：有償POCにて、設置設定作業から簡易レクチャー、最終報告書レポート作成・報告会実施
※OT-SEC：お客様が必要とするOTソリューションやGuardian等を活用したOTNWの監視・脅威検知・レポート等
※OTセキュリティ教育：現場への工場セキュリティ知識の浸透を図る

アジェンダ

- テリロジーって何している会社？
- 苦労話
- 現場第一主義
- 新たな取り組み
- 海外イベントに参加しました

私達は、、、

OTセキュリティソリューションのお客様先評価　件数　50件以上/年間

⇒共創パートナー様とご一緒　や　テリロジー単独で実施！

◆そこで得たことは、各業種業界により・・・・・

:リスク(＝守りたいモノ/コト)がちがう

:言葉がちがう

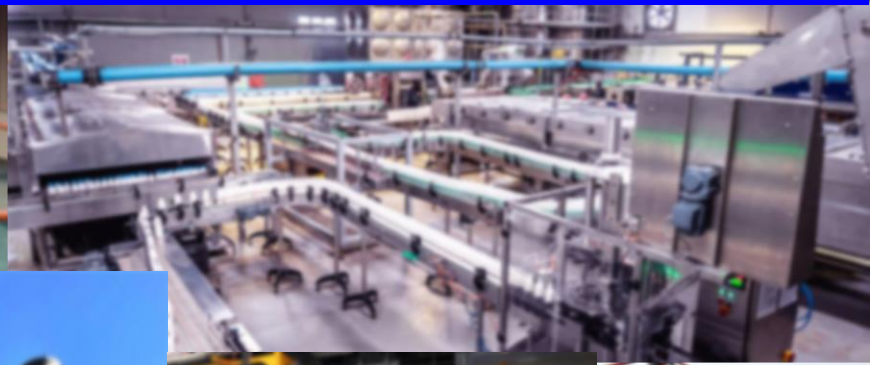
:設備がちがう

:優先順位がちがう

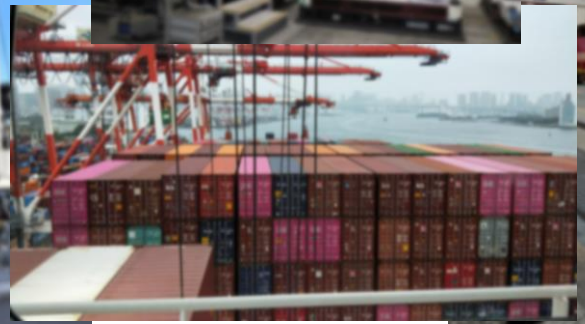
:コストの考え方がちがう

私達がOT/IoTセキュリティでご支援させて頂いた業種

2018年 ～ 2025年現在 これまで多くのお客様の現場に訪問



例えば・・・

- 電力業界・・・・・　何が一番優先順位高いネットワークでしょうか？
- 化学業界・・・・・　インシデントですぐに爆発しますでしょうか？
- ビル業界・・・・・　脅威はなんでしょうか？　何が引き起こされると一番困りますか？
- 船舶業界・・・・・　これからの課題は何でしょうか？
- 物流倉庫・・・・・　どのような機器が使われていますでしょうか？
- ガス業界・・・・・　どのようなことをDCS周りで気にしますでしょうか？
- 食品/飲料・・・・　どのような設備・ネットワークを持っていますでしょうか？

OT/IoTネットワークにおける課題

可視化＆現状把握、継続監視することで把握ができる！

You cannot protect what you don ‘t see !

Source: 405 CIO respondents, Sep 2023, Frost & Sullivan

各お客様のお取り組み（2023年）

時期	業種	
23年4月	ガス/エネルギー様	各プラントにOT/IoTセキュリティ導入　※12台
23年5月	製薬関連企業様	複数拠点　　※順次、国内拠点・海外拠点導入へ
23年5月	化学企業様	国内複数拠点導入　　※2024年海外各拠点導入へ
23年9月	薬品関連様	製品比較実施後導入　※各制御LANにリモートコレクター導入
23年9月	重要インフラ事業様	侵入検知システム　3拠点追加導入　　※監視体制内製
23年9月	半導体関連様	可視化目的で導入　※設備に対するアセスメントを実施
23年10月	飲料メーカ様	評価導入後、国内工場への展開決定　※DX推進を実施へ
23年11月	ビルディング関連様	ビルにおけるOT/IoTセキュリティに関する評価導入
23年12月	製造業様	3ヵ年プロジェクト　※国内複数拠点・特殊生産工場向け導入
23年12月	自動車関連企業	海外拠点に対するOT/IoTセキュリティ導入プロジェクト

アジェンダ

- テリロジーって何している会社？
- 苦労話
- 現場第一主義
  ～教えてもらったこと、見てきたこと、実際におこっていること～
- 新たな取り組み ～Leading the way from Japan to ASEAN emerging markets～
- 海外イベントに参加しました

ASEAN Global Strategy

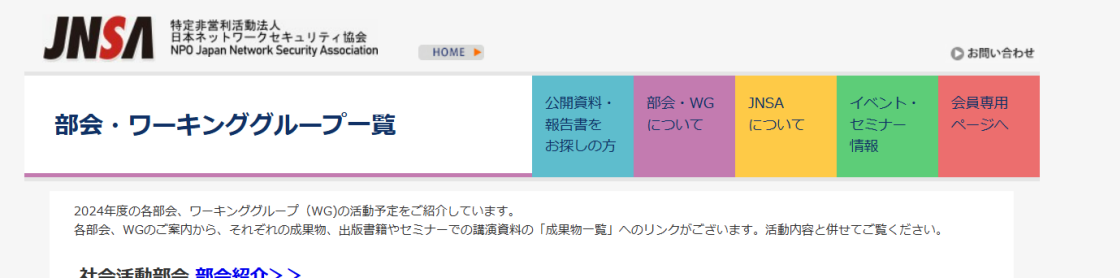
Based on our knowledge and experience accumulated over the past 30 years, we will deploy cyber security solutions to local and Japanese companies in Vietnam and ASEAN countries.

Joint project in Vietnam (OT Security)

Strictly Confidential

ベトナム工業団地でセミナー実施

JNSA



調査研究部会 部会紹介＞＞

セキュリティ市場調査WG ＞＞

組織で働く人間が引き起こす不正・事故対応WG ＞＞

IoTセキュリティWG ＞＞

脅威を持続的に研究するWG ＞＞

インシデント被害調査WG ＞＞

NEW データベースセキュリティWG ＞＞

NEW ＯＴセキュリティWG ＞＞

OTセキュリティWG　2024年8月より活動開始

リーダー：佐々木 弘志（フォーティネットジャパン合同会社）
サブリーダー：藤原 健太（フォーティネットジャパン合同会社）

1．WGの活動目的

（1） OTセキュリティ文化醸成のための調査・研究
（2） JNSA西日本支部工場セキュリティWGとの連携による取組み標準化
（3） AJCCA/JNSA活動支援窓口

2．WGの年間活動予定

（1）ユーザーへの啓発、方策
（2）各種ガイドライン理解度向上と標準化検討
（3）各種OTセキュリティ演習支援、モデレーター支援等の勉強ツールの策定検討
（4）AJCCAリードのASEAN企業に対するOTセキュリティ支援 上記より、JNSAの会員/非会員で工場セキュリティに興味があるメンバーを募り活動を開始する。GUTP/Edgecrossでも同様のWG座長を務めておられる東京大学 江崎先生からのご支援を賜り本WGとの連携活動を模索する。具体的な活動計画は今後の本WG定例MTGコアメンバーにて計画予定。

アジェンダ

- テリロジーって何している会社？
- 苦労話
- 現場第一主義
- 新たな取り組み
- 海外イベントに参加しました

2025年2月:S4x25参加

S4とは　～OTとICSセキュリティの未来を創造する～

- 2008年から開催されている世界最大級のOT/ICSセキュリティカンファレンス
- 業界のリーダーや先駆者が集まり、新しいアイデアや技術を共有し、ICSセキュリティの未来を創造する場。 ※OTセキュリティメーカやスタートアップメーカ多数参加
- 毎年マイアミで開催　※2025年今回は　タンパ　で開催
- S4カンファレンスの創始者＝Dale Peterson氏(ICS/OT分野の世界的先駆者)

S4x25　スポンサー

S4 Prime Sponsors

cisco　CLAROTY　FORTINET　NOZOMI NETWORKS　OPSWAT. Protecting the World's Critical Infrastructure　paloalto NETWORKS　SEL SCHWEITZER ENGINEERING LABORATORIES　servicenow　txOne networks

S4 Big Party

ARMIS　DRAGOS　Phosphorus　waterfall

Vulnerability Management Pavilion

CyBeats　EXIGER　FINITE STATE　FORESCOUT　Fortress　foxguard　INDUSTRIAL DEFENDER　OTORIO　VulnCheck

Lunch Sponsor

DARKTRACE　ELISITY　PSYMETIS　RUNSAFE SECURITY　splunk> a CISCO company　SUBNET SOLUTIONS INC.

S4 Lounge

1898 & CO. PART OF BURNS & MCDONNELL　HEXAGON　pwc　Security Compass THE SECURITY BY DESIGN COMPANY　xage SECURITY　xona

Startup Pavilion

bastazo　cyber energia　Cyolo　FRENOS PROACTIVE DEFENSE. ZERO IMPACT.　KLOCH　OPSCURA　SALVADOR TECHNOLOGIES

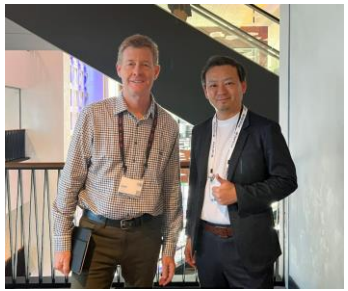
Craft Beer Bash

DISPEL Remote Access Systems　Google Cloud Security　gravwell　Insane Cyber

会場の様子　～3日間開催～

S4×25　基調講演　Dale Peterson氏

OT セキュリティの役割の再構築「OT セキュリティの専門家として、あなたの価値は何ですか？」



・what to do and, equally important, what not to do.
：何をすべきか、そして同様に重要な、何をすべきでないかに関して情報に基づいた決定を下す能力にある

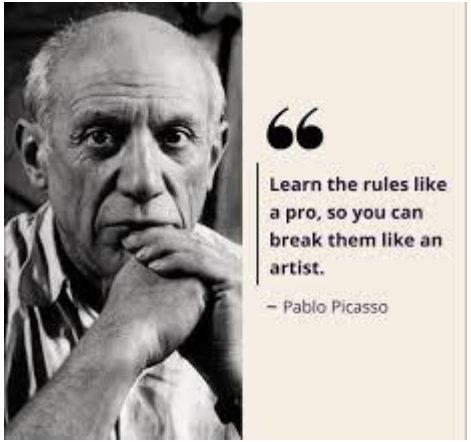
・From Visibility to Actionable Risk Mitigation : 単なる可視性の確保から、リスクを軽減するための具体的なセキュリティ対策の実施へ

・Barbell theory of OT cyber risk management
：OTサイバーリスク管理のバーベル理論 /コストと労力に見合った最も大きなリスク軽減を実現する対策を

・Not all security measures are created equal. : 全てのセキュリティ対策が同等に実施されているわけではない.

S4×25　基調講演　Dale Peterson氏

OT セキュリティの役割の再構築「OT セキュリティの専門家として、あなたの価値は何ですか？」



「プロのようにルールを学べば、芸術家のようにルールを破れるようになる」
これこそが OT セキュリティの未来であり、専門家が単なる実務家ではなく、
カスタマイズされたリスク管理戦略を策定できる**セキュリティ アーティスト**である

OTセキュリティリーダーにとっての重要なポイント

1. **徹底的に優先順位を付ける** :最小限のコストと労力で最大限のリスク軽減を実現するアクションに重点を置く
2. **アプローチのバランスをとる** :結果の管理を犠牲にして可能性の低減を過度に重視しない
3. **現状に挑戦する** :業界のベスト プラクティスに盲目的に従わないでください。自分の判断力を使って、何が最も重要かを判断してください。
4. **価値を明確に伝える** :自分が何を行っているか、また、なぜ特定のことを行わないかを考え、自分の決定を関係者に効果的に伝える方法を学ぶ
5. **継続的な学習を受け入れましょう**： OTセキュリティの基礎を習得するとともに、適応し、革新し、従来の常識に疑問を投げかける準備をする

その他主なテーマ

- セグメンテーションとアクセス制御への新たな焦点
- セキュリティ投資を定量化する業界のアプローチの進化
- AIと自動化：両刃の剣
- **クラウドにおける OT セキュリティ: Chevron の視点**

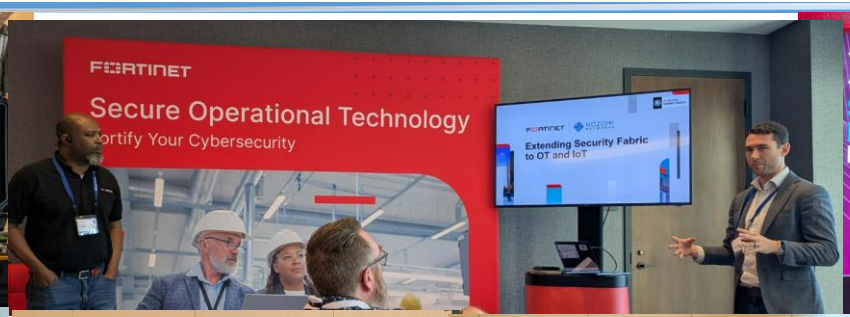
  :クラウド セキュリティの課題:ゾーン＆コンジット

  :クラウドベースのサービスを OT 環境に統合することに伴う課題と機会
- NVIDIA のサイバーセキュリティ AI プラットフォーム（・・・製品紹介？）

  :ITとOTの融合の中、新たな脅威に対処するため、AIと高速コンピューティングを活用したスケーラブルなソリューション
- 脆弱性パビリオン　12社でそろう

  :可視化・防御　そして、事前に把握しておくべき脆弱性、さらには見えない脆弱性にどう把握するのか。。。

様々なOTセキュリティソリューションベンダが集う



企業のデジタル革新を支える

IT/OT/IoT サイバーセキュリティ イネーブラー