サードパーティオプティクスによって変わるネットワーク設計構築運用

独立行政法人情報処理推進機構
産業サイバーセキュリティーセンター
専門委員 松本 智

自己紹介

- 松本 智
  - 産業サイバーセキュリティーセンターにてNWの設計構築運用を担当
    - 教育用研究ネットワークとサイバー技術調査分析基盤の設計構築運用研究開発を行う
      - NWに関連するあらゆることをやる
      - AS63770の運用、DFを用いた拠点間通信網の構築、無線LAN環境の設計構築
      - マルチスライスNWの構築とそれに関わるtoolの開発等
  - その他活動
    - InternetWeekプログラム副委員長(2017-2018)、同委員(2014～)
      - インターネットに関わる技術者/関係者向けに様々な技術の基礎知識や最新動向を伝えることを目的に、様々なプログラム（講演やハンズオン）の企画立案取りまとめを実施
      - 「社会を動かすモノのセキュリティに向き合おう」（2018）
      - 「オーバー100G時代を見据えた光イーサネット入門」（2018）
    - セキュリティーキャンプ（IPA）NOC講師
      - セキュリティー教育に必要なNW基盤の設計構築運用を実施
      - SOCチームの取りまとめ運用等も実施
    - その他
      - 複数の会社組織等にてネットワーク設計・構築・運用・コンサルティングに従事
      - L1～L3（internet）を主とした仕事をしています

本日の目的

- **ネットワークを取り巻くトレンドの変化から見えてくる次の時代の設計・構築・運用について解説**
  - 様々なトレンドの変化から、NW設計構築運用の新たなトレンドを紐解く
  - 今回は主としてEnterprise規模のネットワークを対象に解説
- **目次**
  - 産業サイバーセキュリティセンター紹介
  - NW装置を取り巻くトレンドの変化
  - Enterpriseネットワークを取り巻くトレンドの変化
  - 運用スタイルの変化
  - サードパーティオプティクスの広まりと影響
  - よくある不安
  - まとめ

産業サイバーセキュリティセンター紹介

1．サイバーセキュリティを取り巻く現状

2．産業サイバーセキュリティセンターの事業紹介

3．サイバー技術研究室のネットワークインフラ

1．サイバーセキュリティを取り巻く現状

社会インフラ・産業基盤を狙ったサイバー攻撃の世界的な増加

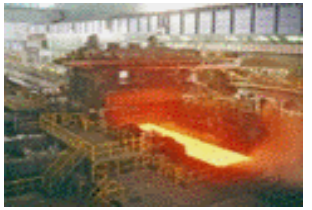
- 近年は社会インフラ・産業基盤に物理的なダメージを与えるサイバー攻撃のリスクが増大。海外においては、既に他国家などからなされるサイバー攻撃により、**社会インフラ・産業基盤の安全が脅かされる事案が発生**。

ロンドン五輪への攻撃（英国、2012年）

毎秒約１万件の不正通信。開会式会場の電力システムへの攻撃情報。手動に切り替え。

製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが製鉄所の制御システムに**侵入**し、不正操作をしたため、**生産設備が損傷**。



変電所へのサイバー攻撃（ウクライナ、2015年、2016年）

マルウェア感染により、変電所が**遠隔制御**された結果、数万世帯で3～6時間にわたる**大停電**が発生。

イスラエル電力公社（IEC)への（イスラエル、2016年）

イスラエルの電力発電を管轄する電力公社が**ランサムウェア**による攻撃を受け多数の**コンピュータシステムが停止**。

1．サイバーセキュリティを取り巻く現状

2017年度のインシデント事例

国内大手製造業

自己増殖型ランサムウェアである

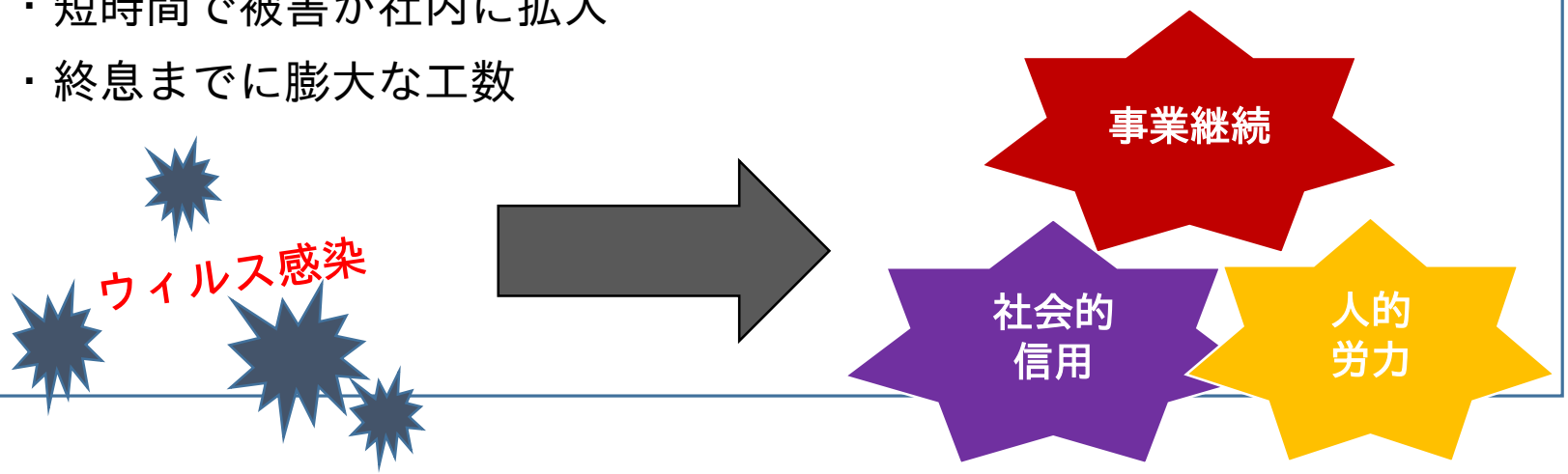
「WannaCry」ウイルスに感染

被害内容

・グループ社内ネットワークのWindowsサーバーが感染して、
　システム障害を起こす

・短時間で被害が社内に拡大

・終息までに膨大な工数



1．サイバーセキュリティを取り巻く現状

脅威の動向

2017年は大規模なインシデントこそ発生しなかったものの、今後、制御システムのサイバー脅威が高まる予兆となる事件や傾向を認知。

- 制御システムのマルウェア感染
  - ✓ 2017年1～6月に制御システムのランサムウェア感染を435件確認

    （Kaspersky Lab.Inc）
  - ✓ 制御システムに特化したマルウェア（TRITON、Stuxnet等）の出現
  - ✓ 内部関係者の過失によるウィルス感染

- 情報報機関からの高度なハッキングツールの流出
  - ✓ 米中央情報局、米国国家安全保障局保有の脆弱性や高度なハッキングツールが流出。今後出現するウィルスやサイバー攻撃の高度化の懸念。

- 国家の関与
  - ✓ 国家紛争やテロのドメインがサイバー空間に拡大。制御システムへのサイバー攻撃により重要インフラを損壊・機能停止に。相手国に簡単かつ効果的にダメージを与える攻撃手段へ。

1．サイバーセキュリティを取り巻く現状

近年のセキュリティ対策のトレンド

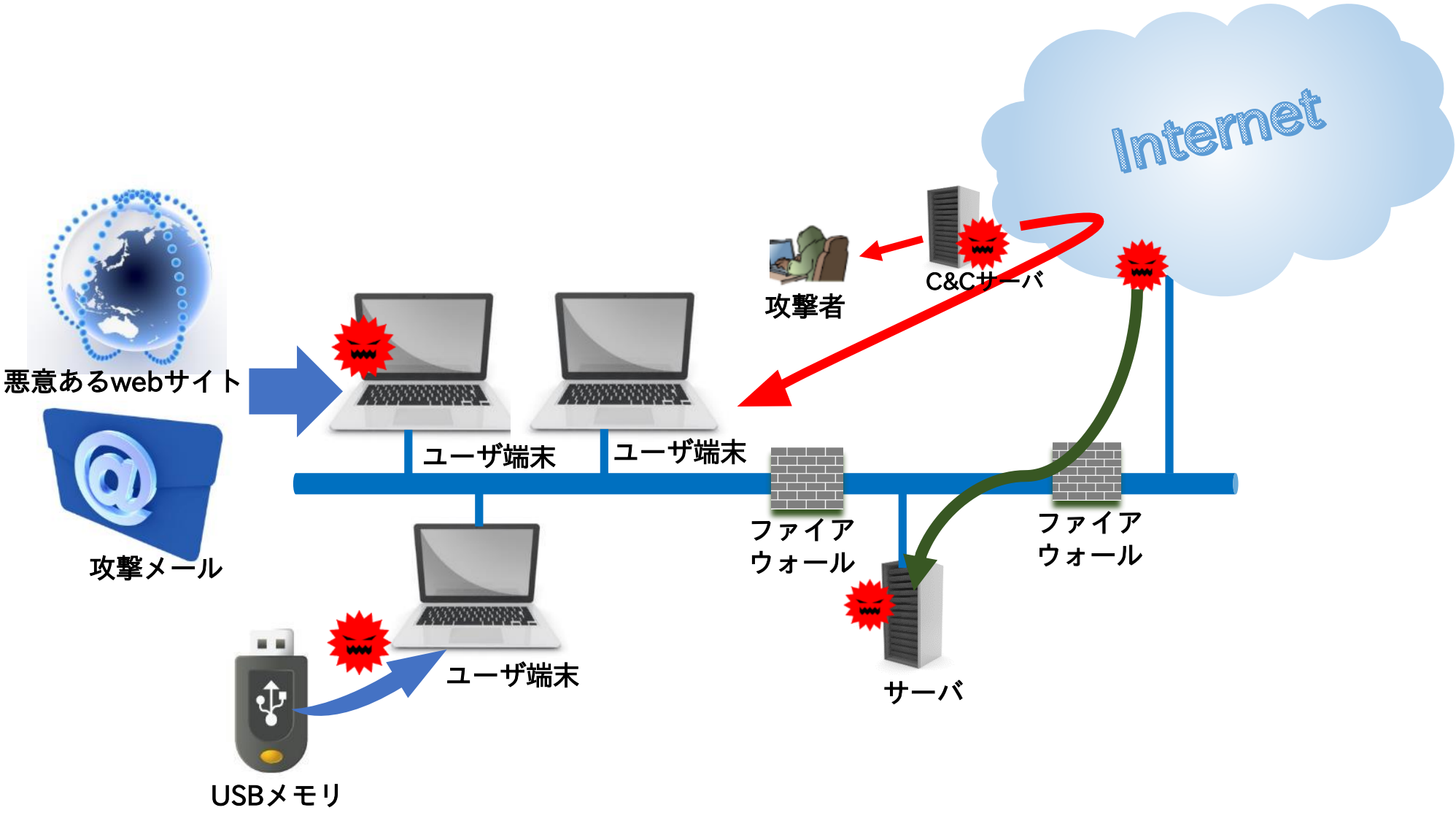
1. IT（Infomation Tecnology）からOT（Operasional Tecnology）へ
   →設備等の機能停止等で、社会の機能不全、経済的なダメージが現実に
2. 研修から演習へ
   →座学では、体得しきれず演習スタイルが主流に（攻守、実機の利用、etc）
3. 現場から経営へ
   →以前からの課題であるが、情報システム部門にとどまらない段階に

制御システムと情報システムにおけるセキュリティの考え方の違い

	制御システム	情報システム
セキュリティの優先順位	システムが**継続して安全に**稼働できることを重視	情報が適切に管理され、情報漏えいを防ぐことを重視
セキュリティの対策	モノ（設備、製品）サービス（連続稼働）	情報
技術のサポート期間	10年～20年	3年～5年
求められる可用性	24時間365日の安定稼働 （再起動は許容されないケースが多い）	再起動は許容範囲のケースが多い
運用管理	現場技術部門	情報システム部門

1．サイバーセキュリティを取り巻く現状

情報システムの構成例とリスク



1．サイバーセキュリティを取り巻く現状

制御システムの構成例とリスク

制御システム構成例

1．サイバーセキュリティを取り巻く現状

- 制御システムは、ウィルス感染や不正アクセス等のサイバー攻撃のリスクが増大
- セキュリティ被害の主原因は下記の4ケースに分類され、制御システムの運用状態において大きな脅威

被害事例の原因の多くは、こういった基本的な部分にある

USBメモリ

- USBメモリからのウィルス感染事例は頻繁に発生。
- しかしながら、USBポートは運用上なくすことは不可能なことが多く、メンテナンス上も不可欠。

リモートメンテナンス回線

- リモートメンテナンス回線の先の端末からの不正アクセス、ウィルス混入が発生。

操作端末の入れ替え/保守用端末の管理

- 操作端末は、汎用パソコンであることが一般的であり、入れ替え時にウィルス感染していた端末から被害が発生。
- システムに接続する保守用端末が原因となるケースも有。

内部犯行・工業用無線LAN等

- 内部犯行者は物理セキュリティを通過。
- 工業用無線LANからの侵入事例も有。
- パソコンのID、パスワードの共通化、メモ書きの貼り付けなどは、悪用されやすい、危険な運用。

- 多くの企業で制御システムのセキュリティ対策はあまり意識されておらず、端末や制御システムの大多数は脆弱性が修正されていない。
- そのため、工場の生産ラインの停止や設備損壊などを引き起こし、企業に甚大な損失を与える可能性が高まっている。

1．サイバーセキュリティを取り巻く現状

2．産業サイバーセキュリティセンターの事業紹介

3．サイバー技術研究室のネットワークインフラ

2．産業サイバーセキュリティセンターの事業紹介

日本政府における産業サイバーセキュリティ施策方針

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

OT(制御技術）とIT（情報技術）の知見を結集させた
世界レベルのサイバーセキュリティ対策の中核拠点
「産業サイバーセキュリティセンター」を2017年4月に発足

2．産業サイバーセキュリティセンターの事業紹介

人材・組織強化、技術、ノウハウを結集し、社会インフラ、及び産業基盤のサイバーセキュリティ対策抜本的強化を図るために、**３つの事業**を柱に推進。

人材育成事業

- 自社システムのリスクを認識し、必要なセキュリティ対策を判断できる人材の育成
- 模擬プラントを用いた実践演習による、現場で活きるスキルの醸成
- 国内外の有識者、専門家との連携を促進
- 企業等の経営層へ、サイバーセキュリティ対策の必要性、人材活用についての啓発

中核となる3事業

制御システムの安全性・信頼性検証事業

- 実際の制御システムの安全性・信頼性に関するリスク評価・対策立案を行う

※IPAセキュリティセンターと連携して実施する事業

脅威情報の調査・分析事業（サイバー技術研究室）

- 脅威情報を収集、新たな攻撃手法など調査・分析
- 外部のホワイトハッカーの協力を得つつ、高度なサイバー技術の調査・研究

２．産業サイバーセキュリティセンターの事業紹介

１）人材育成事業 提供プログラム全体像

中核人材育成プログラム

- 1年間のカリキュラム

責任者向けプログラム

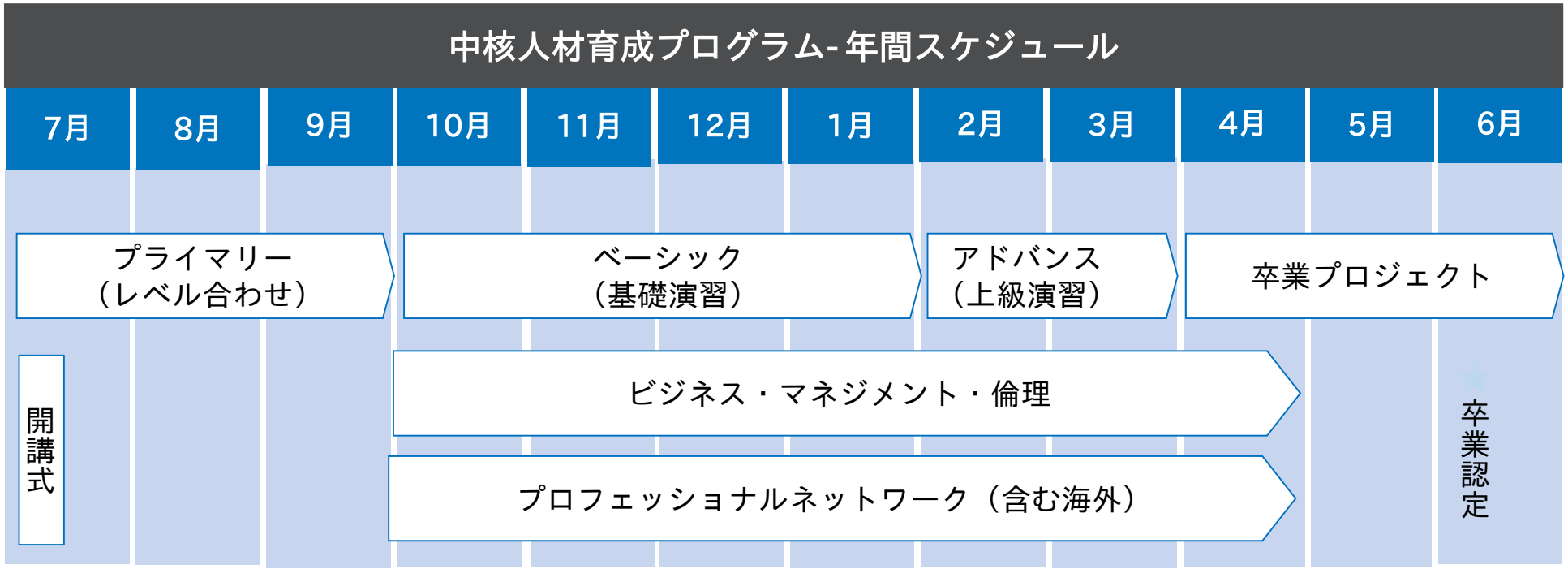
- 短期間のトレーニング
  - ✓ 業界別トレーニング（2日間）
  - ✓ 国際トレーニング（2日間）
  - ✓ 戦略マネジメント系セミナー（週次夕方開催全7回）

2．産業サイバーセキュリティセンターの事業紹介

2）中核人材育成プログラム

中核人材育成プログラム

- 将来、企業などの経営層と現場担当者を繋ぐ“中核人材”を育成
- 1年をかけてテクノロジー（OT・ＩＴ）、マネジメント、ビジネス分野を総合的に学習



２．産業サイバーセキュリティセンターの事業紹介

２）中核人材育成プログラム

施設紹介

模擬プラント

模擬プラント

大会議室

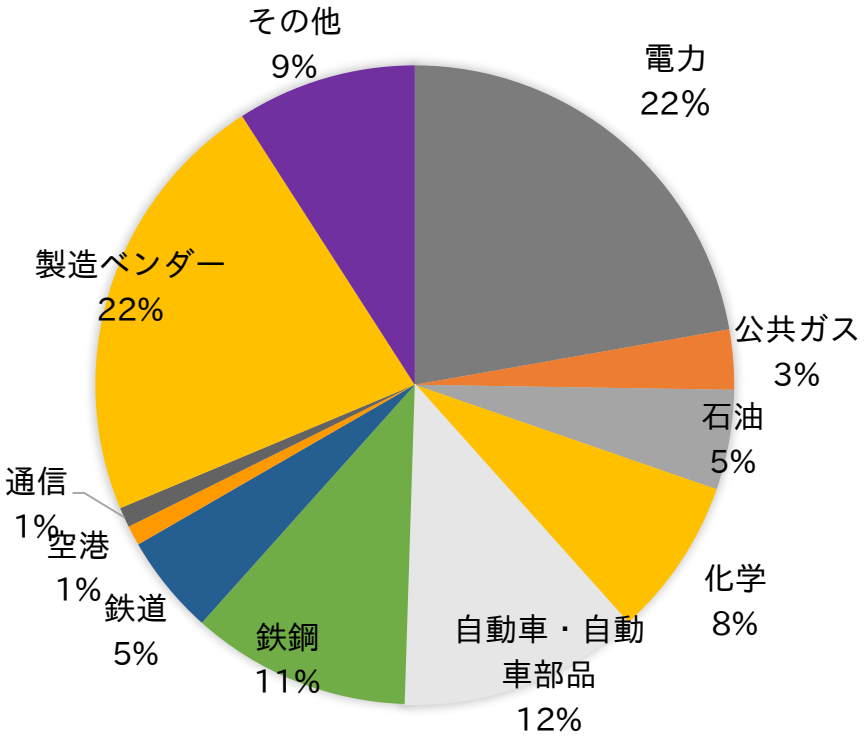
アクティブラーニング室

2．産業サイバーセキュリティセンターの事業紹介

2）中核人材育成プログラム

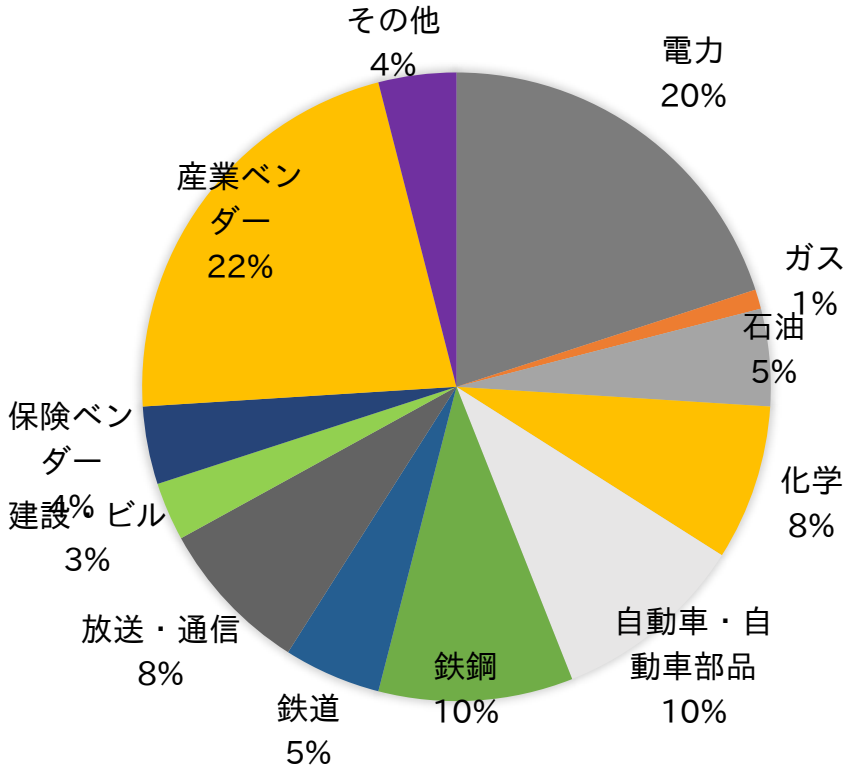
受講生の構成（平成29年度、平成30年度）

第1期中核人材育成プログラム受講生の構成
※平成29年度



受講者数：76

第2期中核人材育成プログラム受講生の構成
※平成30年度



受講者数：83

２．産業サイバーセキュリティセンターの事業紹介

２）中核人材育成プログラム
海外機関連携トレーニング（平成29年度、平成30年度の事業例）

海外における産業サイバーセキュリティを直に学ぶための派遣演習

- フランス（パリ）の学術機関や電力事業者等を訪問し、現地の産業界・大学の研究者や行政担当者による講演や、彼らとの意見交換を通じて、サイバーセキュリティの国際的標準を理解するとともに、現地キーパーソンとの人脈を構築（平成29年9月、平成30年9月）。

- 在日英国大使館のアレンジにより、英国の政府機関や金融・自動車関連事業者、ベンチャー企業等を訪問し、彼らとの意見交換等を通じて、英国における官民の取組を理解するとともに、現地キーパーソンとの人脈を構築（平成30年12月）。

enisa
European Union Agency for Network and Information Security

２．産業サイバーセキュリティセンターの事業紹介

２）中核人材育成プログラム
海外機関連携トレーニング（平成29年度、平成30年度の事業例）

米国国土安全保障省（DHS）とのASEAN等向け
日米サイバー共同演習（平成30年9月）

DHSの制御システムセキュリティの担当部門であるICS-CERTが提供するプログラムを、米国から招へいした講師の指導のもと、本場のトレーニングを体験。演習を通じて、プロセス制御システムに対する実際の攻撃手法や、制御システムネットワークのセキュリティ対策を向上する戦略を理解。

２．産業サイバーセキュリティセンターの事業紹介

２）中核人材育成プログラム

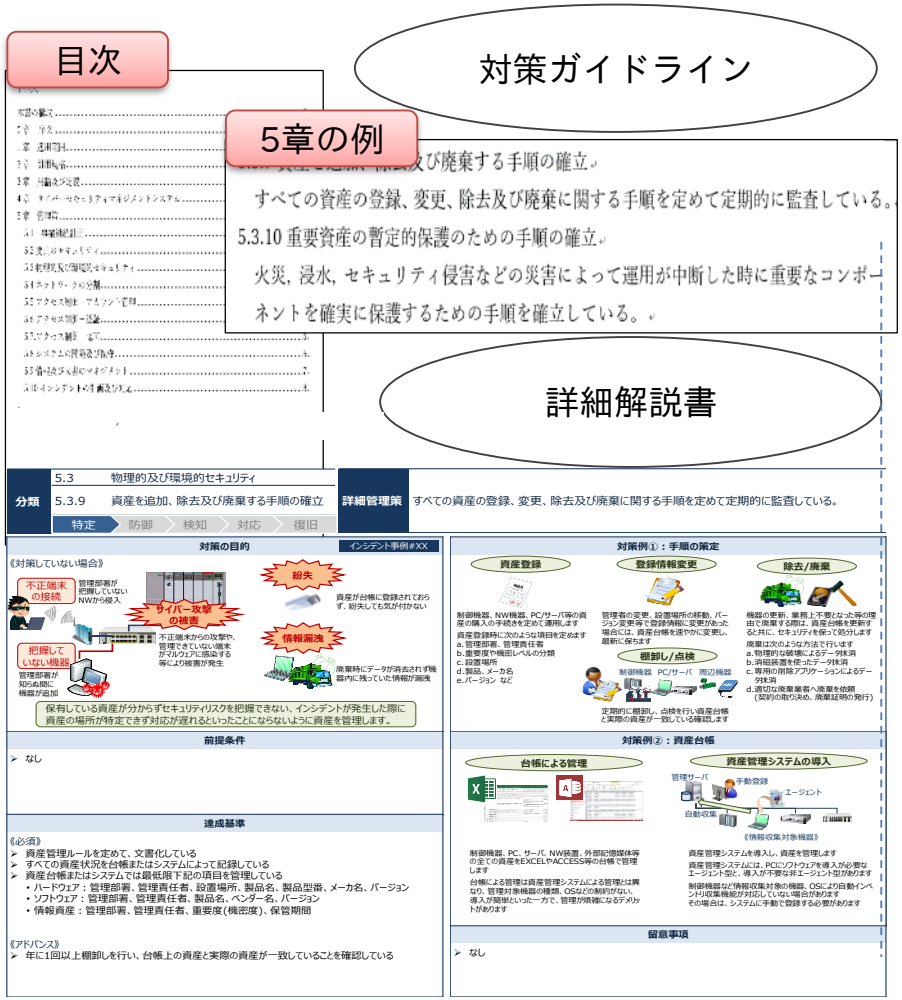
卒業プロジェクト

第１期では２３件のチーム卒業プロジェクト、４件の個人卒業プロジェクトを実施。

自動車業界の受講者チーム

＜工場セキュリティ対策要件の
グッドプラクティス検討＞

国際規格やガイドラインを踏まえて、実際の現場において利用可能な実装例を伴う詳細な解説書を作成



２．産業サイバーセキュリティセンターの事業紹介

２）中核人材育成プログラム

修了者コミュニティ

【名 称】

叶会（かなえかい）

【目 的】

・卒業後も知見をアップデート
・卒業年次を超えた人脈
・修了者の知見の社会還元

業界を横断した制御システムのセキュリティに係る連携体制の構築

【主な活動】

・総会（今年度は11月9日）で最新動向と演習・発表

・サイバーセキュリティ情報提供活動
　→　情報共有ツールを使い、ICSCoEが入手した脆弱性情報等を修了者に提供

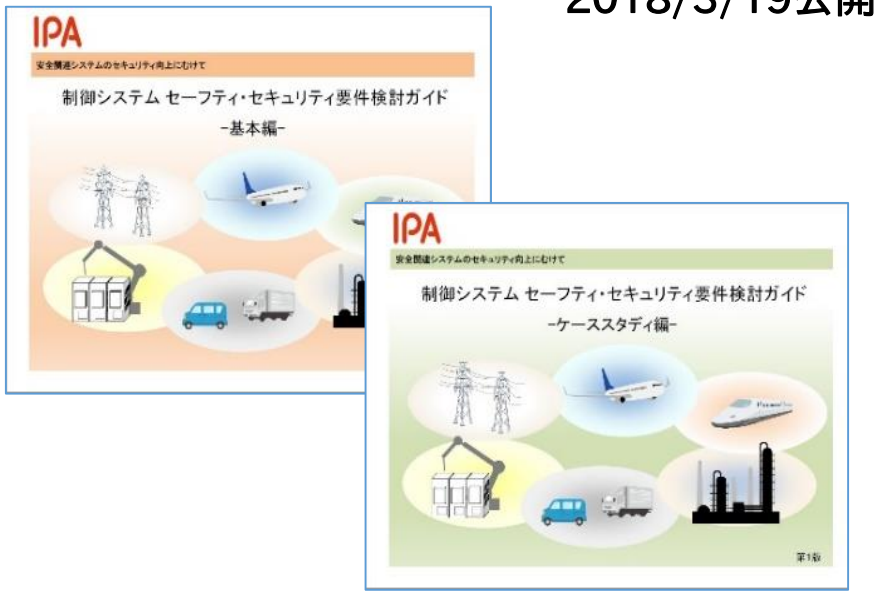
2．産業サイバーセキュリティセンターの事業紹介

3）制御システムの安全性・信頼性検証事業

- 制御システムのセキュリティに関する国際規格の活用の推進
- 実際の制御システムの安全性・信頼性に関する情報収集・対策立案を実施

「制御システムのセキュリティリスク
分析ガイド 第2版」
2018/10/15公開

「制御システム セーフティ・
セキュリティ要件検討ガイド」
2018/3/19公開



２．産業サイバーセキュリティセンターの事業紹介

４）脅威情報の調査分析事業（サイバー技術研究室）

- 国内のホワイトハッカーのコミュニティの協力を得つつ、

  高度なサイバー技術の研究開発

- 人材育成事業の受講生がサイバーセキュリティ分野の研究者との

  協働により研究活動を実施

サイバー技術研究室の風景

２．産業サイバーセキュリティセンターの事業紹介

５）責任者向けプログラム　平成30年度実績

責任者向けプログラムー年間スケジュール	
業界別 トレーニング	8月24,25日 業界別(1回目） （金属、石油、化学、製薬、製造） 11月16,１７日業界別(2回目) （電力、ガス） 2月15,16日業界別(3回目) （鉄道、交通）
国際トレーニング	11月2,3日 国際トレーニング(1回目)　2月1,２日 国際トレーニング(2回目)
戦略 マネージメント系 セミナー	11～12月、週次夕方開催全7回

1．サイバーセキュリティを取り巻く現状

2．産業サイバーセキュリティセンターの事業紹介

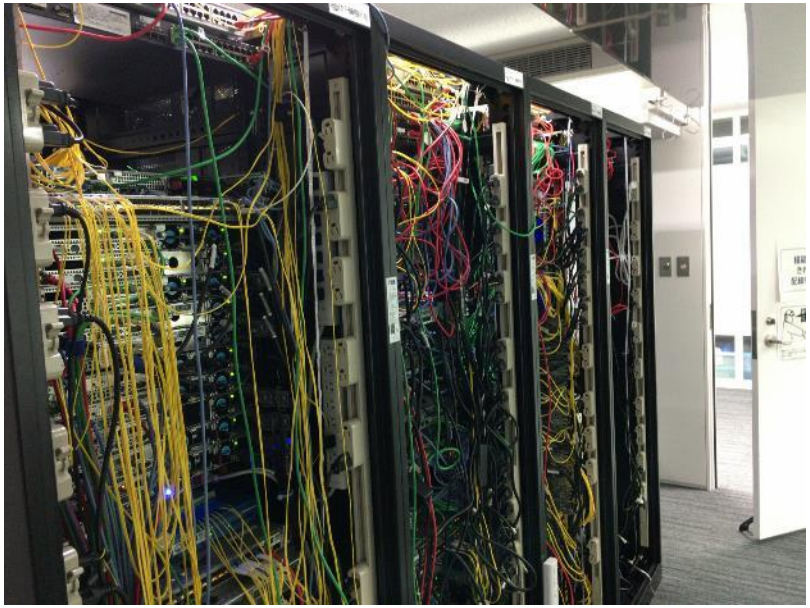
3．サイバー技術研究室のネットワークインフラ

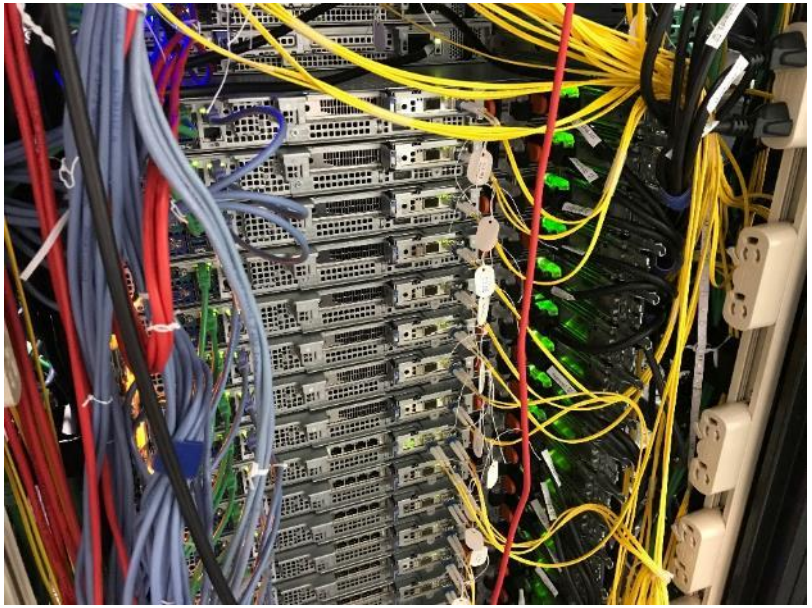
３．サイバー技術研究室のネットワークインフラ

■ 求められる機能・役割

- ■リアル環境を活用した、最新のサイバー攻撃情報の調査分析
- ■国内ならびに国際セキュリティ機関同士の、調査分析における連携強化
- ■普遍的なサイバー脅威の分析と、その対処方法の知識化

■これらを支える柔軟性のあるNW/サーバ基盤が重要





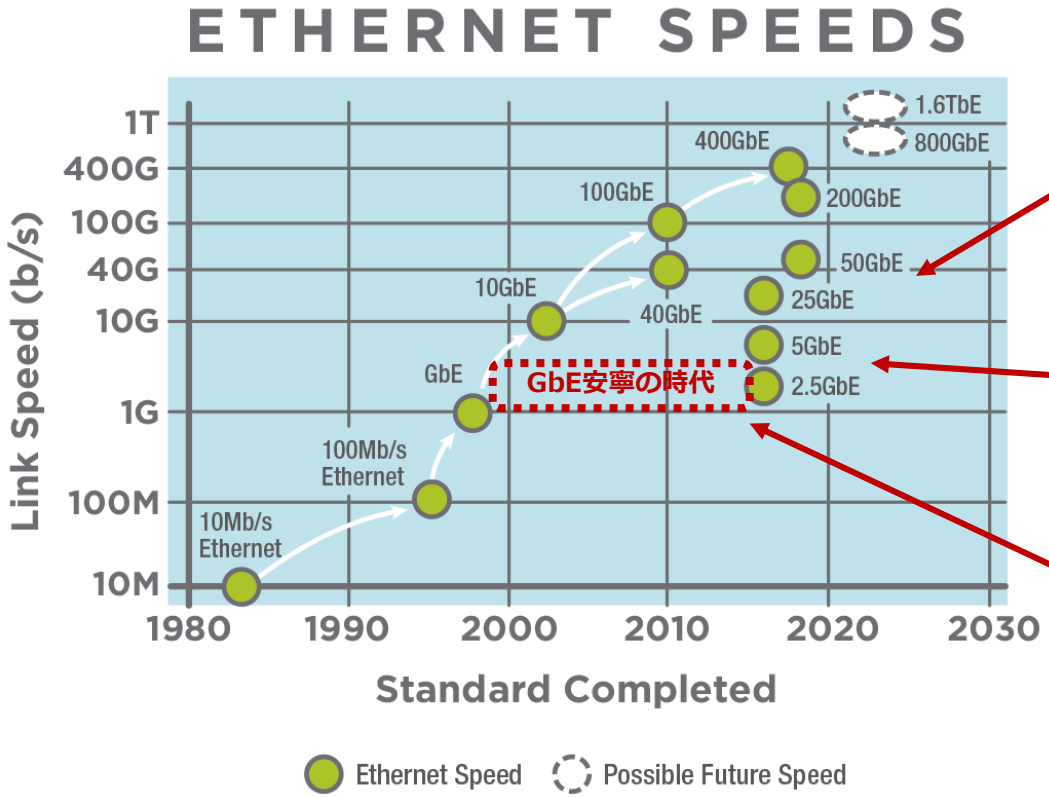
NW装置を取り巻く
トレンドの変化

NW装置を取り巻くトレンドの変化

- **Ethernetの高速化**
  - **~00年台、マルチレート多メディアだった規格の争いが終結**
    - ギガビット・イーサネットが覇権を獲得
    - 以降 1000BASE-T/LX/SX が Enterprise NW における主役の座に
    - 物理メディアとしての Cat5e、SMF、MMF(OM2)が鉄板に
    - **安寧の時代が到来**
  - **10Gbit Ethernet の台頭**
    - 00年代後半に Ethernet が WAN に進出
      - SONET/SDH より安価な 10G Ethernet専用線が大普及
    - それに伴い LANにも普及を開始
      - 10G BASE-T/LR/SR が登場、価格が高く普及が伸び悩む
      - 10年代前半～中盤にかけて価格も安くなり普及が進む
        - この頃からサーバにオンボード 10G が搭載され始める
    - **10年台後半、40G/100G Ethernet が登場　⇦ｲﾏｺｺ**
      - 当初から比較的安価な選択肢が揃っていたため一気に広まる
      - Enterprise NW でも真剣に考えないといけない時代が到来
      - **マルチレートイーサネット激動の時代が始まる！**

NW装置を取り巻くトレンドの変化

- Ethernetの高速化の今後
  - Enterprise NW においても、メディア選択の戦略が必要に



高速サーバの需要を満たす 25GbE/50GbE は 100GbE の普及を後ろ盾に伸びていきそうな気配

10GbE と 1GbE の間を埋める規格が登場するも、実需ベースでは 1GbE と 10GbE の棲み分けになりそう。

10GbE は規格の策定から安価な製品の登場までのタイムラグが長かったため 1GbE が覇権を握った

https://ethernetalliance.org/the-2019-ethernet-roadmap/ より

NW装置を取り巻くトレンドの変化

- **新興ベンダーの台頭と merchant silicone の普及**
  - **~2010頃まで：数社のNWベンダーが大きく幅を利かせていた**
    - NW装置に係るすべてをベンダーが自社で製造・コントロール
      - **トランシーバモジュールもベンダー純正品が基本**
    - 保守や運用体制、ビジネスモデルもこの頃に確立していく
    - 社内NWの単一ベンダー化が進んでいく
  - **2010年頃から：第三勢力のベンダーが徐々に台頭**
    - 用途と需要の細分化に伴った隙間企業が勢い付いてくる
      - **フルライン戦略からニッチ戦略への業界シフト**
    - NWプロセッサーの汎用化が進んだことが大きな要因
      - ～2010年頃まで：NWプロセッサー、筐体、基盤を自社で製造
      - 2010年頃～：汎用化した部品を組み合わせて製造
        - アセンブリ主体のベンダーが登場
        - 汎用NWプロセッサー(**merchant silicone**)が一気に普及
        - 汎用NW装置：汎用NWプロセッサーで構成されるNW装置

NW装置を取り巻くトレンドの変化

- **merchant silicone 普及の影響**
  - **汎用NWプロセッサーが主体となった製品ラインナップ**
    - **様々なベンダーが同じ汎用プロセッサーを使う**
      - ベンダーが違ってもチップが同じというのが当然に…
      - 価格も似たようなものに…
    - 画一的なNW製品が多ベンダーから販売
      - ポート構成やスループット、対応プロトコルで差がつきにくい
      - ベンダー間の差：**ネットワークOSの違いが一番大きな差別化要素**
  - **NW機器ベンダーはより厳しい価格競争環境に晒される**
    - 構成部品の汎用化で凌ぐようになる
      - ベンダーによるコストカット競争が激化
      - トランシーバモジュールの自社生産から汎用品の利用へのシフト
  - **サードパーティオプティクス時代の到来**
    - 安価で高品質な部品を求めるNW機器ベンダー
    - トランシーバメーカーの製造技術の進化

NW装置を取り巻くトレンドの変化

- **玉石混交時代に求められるNWエンジニアのスキル**
  - **ベンダー品と汎用品が入り乱れる時代**
    - **歴史は繰り返す…（DOS/V, *NIX, OPEN系/汎用系…）**
    - 汎用NWプロセッサーを用いた汎用NW装置の利活用が鍵
      - 単一ベンダーでNWを作ればいい時代の終焉
      - **単一ベンダーでNWを作る理由を正しく考え向き合う必要性**
    - 数多ある汎用NW装置から適切なものを選ばないといけない
      - 様々な規格を理解し、NWの要求と向き合う必要性が増す
      - 製品ありきのNW作りからの脱却
        - 要求を満たすチップの製品をどう選ぶかが重要
        - ベンダーの事情も把握して総合的に判断
  - **汎用部品の利活用でのコスト削減が鍵を握る**
    - 様々なベンダーが同じ汎用プロセッサーを使う
      - 様々な汎用部品が動く汎用NW装置が当たり前になりつつある
      - **汎用部品をうまく組み合わせてコスト削減するというセンス**

Enterpriseネットワークを取り巻くトレンドの変化

Enterpriseネットワークを取り巻くトレンドの変化

- **10Gbit Ethernet の普及が本格化**
  - **フロア内へ普及開始**
    - 基幹NW以外でも 10Gbit Ethernet の利用が普及
    - 10G NAS 等の普及でフロア内での利用が本格化
  - **10G 以上では non メタル が主流の世界**
    - 脱ツイストペアケーブル
    - 光ケーブルを利用するシチュエーションが増加
      - **利用するトランシーバモジュールの数が増える**
    - 10G BASE-T(IEEE 802.3an-2006)との棲み分け問題は根が深い
  - **サーバ収容におけるUTPケーブルから光ファイバーへの変化**
    - オンボード 10G SFP+ なサーバの増加
  - **UTPケーブルは光ファイバーより取扱が面倒**
    - 10G BASE-T(IEEE 802.3an-2006)では Cat6 ケーブル以上が必須
      - 細径UTPケーブル起因のトラブル
      - 200Mhz(25G BASE-T では 500Mhz)
      - STPケーブルの利用は非現実的
      - 取り回しや既設構内線張替え発生等で問題が起こることも

Enterpriseネットワークを取り巻くトレンドの変化

- **サーバアプリケーションや仮想化基盤が 10G 以上を要求**
  - **ストレージのネットワーク化**
    - ミドルエンドのNASで10G当然の時代
    - エンド端末にも 10G が必要になるパターン
  - **仮想化基盤の大規模化に伴う 10G 化**
    - Hypervisorに乗せる仮想マシン数の増加によるトラフィックの増加
    - ストレージのネットワーク化に伴うストレージトラフィックの増加
  - **上流向けで 10G*n LAG や 40G が必要に**
    - アグリゲーションSW以上の基幹部では 10G では足りなくなる
    - LAGをするか 40G/100G を採用する必要あり
  - **パッチシステムの消費を考えると 40G 有利の場合も**
    - 既設ファイバーの芯数によっては 40G-LR が最適となるパターン
    - 階やフロアをまたぐMPOケーブル問題

Enterpriseネットワークを取り巻くトレンドの変化

- **BOX型SWでのForwardingとTransportの分離**
  - **Forwarding処理とTransport変換処理の役割分離が進む**
    - Forwarding処理：いわゆるSwitchingやRoutingに必要な処理
      - NWプロセッサーがL2より上の処理を集中的に行う
        - L1の面倒を見なくて良くなり設計が容易に
    - Transport処理：メディアタイプ変換処理
      - SFP(Small Form Factor Pluggable)+ポート
      - メディアタイプへの変換はトランシーバモジュールが行う
        - SFP+ポートのみを搭載し メタル (*BASE-T) 変換もトランシーバモジュールに任せる場合も
      - 基盤からはデジタル信号線が出るだけ
  - **Forwarding処理とTransport変換処理の分離のメリット**
    - **ベンダーの利点：コスト圧縮、製品に幅をもたせやすい**
    - **ユーザの利点：都合の良いトランシーバモジュールを選べる**

Enterpriseネットワークを取り巻くトレンドの変化

- **BOX型SWでのメディアタイプ変換処理**
  - **信号のO/E, E/O 変換処理**
    - 電気信号と光信号を相互変換
    - レーザ光の調整など物理メディアに特化した処理を行う
      - **SW側からみたら（ほぼ）透過的な処理**
  - **トランシーバモジュールの選択で自由なNW設計が可能に**
    - 特殊なトランシーバモジュールを使うことで特殊環境を安価に
      - 長距離 BiDi モジュール や *WDM モジュール
    - ブレークアウトケーブルによる柔軟なIF運用
      - 1port:1速度 から 1port:多速度 運用へ
      - サーバ分野では 100G = 25G*4 のブームがきそう
        - 32*100G 時に 25G*128 構成が可能
    - **ベンダー利用者双方にとって構成の工夫がしやすくなった**

https://jp.finisar.com/active-optical-cables/fcbn510qe2cxx

Enterpriseネットワークでの運用の変化

Enterpriseネットワークでの運用の変化

- **～1Gの世界**
  - ツイストペアケーブル
  - LANケーブルを適当に挿せばリンクが上がる
  - 光ファイバーはフロア間、ビル間等限られた利用に留まる
  - トラブル：LANケーブルの劣化
- **Over10Gの世界**
  - ツイストペアケーブルと光ファイバーケーブルが入り乱れる
  - 光ファイバーケーブルを正しく挿さないとリンクが上がらない
  - フロア内へ光ファイバーの利用が到来
  - トラブル：光信号の損失、光ファイバーケーブル、コネクタの劣化

Enterpriseネットワークでの運用の変化

- **異速度異メディアの混在と既設ケーブル負債可**
  - **同じ物理層に多様なメディアタイプが共存**
    - SMF上に 1000BASE-LX/10G-LR/40G-LR/100G-LR4 が混在
    - メディアタイプと速度の管理
  - **敷設済みUTPケーブルの負債化**
    - フロア内NWには 1000BASE-T が残る
    - フロア間のUTPケーブルが使えなくなる
    - LANコンセントにも注意

SMFを多様なメディアタイプで使う

https://jp.finisar.com/
https://img-en.fs.com/images/products/550x550/40191.B.jpg

Enterpriseネットワークでの運用の変化

- **光ファイバーケーブルに関する知識が新たに必要**
  - **物理層で発生するトラブルが変化**
    - 大半が光配線やトランシーバモジュールへの理解不足によるもの
    - 誤った光ファイバーケーブルの取扱
  - **正しく理解し扱えばUTPケーブルと同等に扱うことができる**
    - パワーメータでレベルチェックする習慣をつける
    - 専用の測定器が必要になるが、取扱は簡単
    - 測定器の低価格により1式揃えても投資効果が高い
      - 最低限必要：光コネクタークリーナー、パワーメーター、パワーソース

https://www.nttrec.co.jp/product/category0204/11257100

ここまでのまとめ

- **マルチレートイーサネット時代が到来**
  - メディア選択の重要性が増し、失敗すると将来に大きな禍根を残す
- **BOX側SWの設計思想が変化しつつある**
  - 製品選択の戦略が今まで以上に重要に
- **サーバ室/フロア内の両方で 10GbE の利用が本格化**
  - 実利用とともに将来性を踏まえたL1設計がポイント
- **光ファイバーケーブルの取扱が必須に**
  - UTPケーブルのように適当に扱えない
  - 光ファイバーケーブルに関する知識が新たに必要

サードパーティオプティクスの広まりと影響

サードパーティオプティクスの広まりと影響

- **サードパーティオプティクス（モジュール）とは**
  - **NW機器ベンダー以外のメーカ（third party メーカ）が作ったトランシーバのこと**
    - NW機器ベンダーから見れば「**非純正/互換トランシーバ**」
    - （例）カメラメーカのレンズとレンズメーカのレンズの関係
  - **用語としてのサードパーティオプティクス**
    - 「トランシーバモジュール」と「オプティクスモジュール」
      - 意味に差異は無く、SFPなどに取り付けるモジュールを指す
      - 同じメーカのサイトでも機種によって用語が混ざってる場合も…
    - 本セッションでは特に**モジュール全般のことを「トランシーバモジュール」**、**third party メーカ が製造し販売するモジュールのことを「サードパーティオプティクス / サードパーティオプティクスモジュール」**と呼び分ける

サードパーティオプティクスの広まりと影響

- トランシーバモジュールに対する考え方の違い
  - **製品が登場した歴史的背景が影響**
  - ネットワーク機器ベンダーの考え方
    - トランシーバモジュールは**ベンダー専用製品を使用**
      - **NW機器の歴史はトランシーバモジュールの歴史とほぼ等しい**
      - 規格の策定とともに製品が進化
    - ベンダーロック
      - 他社製トランシーバモジュールは認識するも link-up しない
    - 保守体制も含めた厳密な管理
      - NW機器との組み合わせも厳密に管理
    - NW機器とトランシーバモジュールはセットと言う考え方
      - **100Mの頃から光化**しており、長い歴史と文化が醸成されている
      - 有機的な運用を行うということがあまりなかった

サードパーティオプティクスの広まりと影響

- **オプティクスモジュールに対する考え方の違い**
  - **サーバ・セキュリティー機器ベンダーの考え方**
    - 多くの部品がコモディティ化しておりトランシーバモジュールも該当
    - **光化が始まった時期がNW機器に比べ遅い**
      - **NW装置に比べ最新の規格からワンテンポ遅れている**
      - 1GbE の時代は 1000BASE-T が主流
      - 10GbE の普及に伴い徐々に光化（SFP/SFP+ポートを搭載）
    - メーカー固有のオプティクスモジュールを作るという文化が無い
      - サードパーティオプティクスを利用するケースが多い
      - 専用型番もなく、サードパーティメーカの型番のまま利用
    - ベンダーロックもほとんど無い
      - 例外的に一部NICではベンダーロック/専用型番があることも
        - オプティクスモジュールが認識しない/光が出るが Link-up しない等の事象が起こる

サードパーティオプティクスの広まりと影響

- **近年のトレンド**
  - **ネットワーク機器にもサードパーティオプティクスの波到来**
    - 前述の通り、**後発ベンダーでの採用が増えつつある**
  - **エンドユーザが直接サードパーティオプティクスを調達可能に**
    - 取り扱う商社が増えたことで流通が改善
    - 国内の商流に完結して入手できることで急速に普及
    - 箱（SW）とトランシーバモジュールの**別買い**が可能に
      - 柔軟性のあるNW設計と調達が可能に
      - 規模に応じて段階的にトランシーバを買い足す
  - **トランシーバモジュールの運用をベンダーやNI/SIに丸投げしていた時代から自ら行う時代に**
    - ノウハウの蓄積が必要になる反面メリットは大きい
    - 測定器の進化・低価格化で自前運用も十分可能になった

サードパーティオプティクスの広まりと影響

- **運用スタイルの違い**
  - **純正トランシーバモジュールの運用**
    - 装置ごとに数量を管理、紐付いた装置にのみ取り付ける運用
    - **装置と合わせて保守に入る**
    - ウォーターフロー的手法で設計・機器選定をし、固定的に購入、運用
    - 装置間での**柔軟なトランシーバモジュールの運用に難あり**
  - **サードパーティオプティクスモジュールの運用**
    - 総量を管理し、利用形態に合わせて様々な装置に取り付ける運用へ
    - トランシーバモジュール単独で保守に入る
      - 装置側の保守の枠組みを**サードパーティオプティクスモジュールの利用を前提とした保守に変更**する必要あり
    - アジャイル的な手法で設計・機器選定をし、流動的に購入、運用
    - 装置間での**柔軟なオプティクスモジュールの運用が可能**
      - 予備部材を予め購入しておくことでトラブルに備える
      - 故障後の保守交換対応のタイミングを制御
      - 故障問い合わせや交換する人的負担を軽減

サードパーティオプティクスの広まりと影響

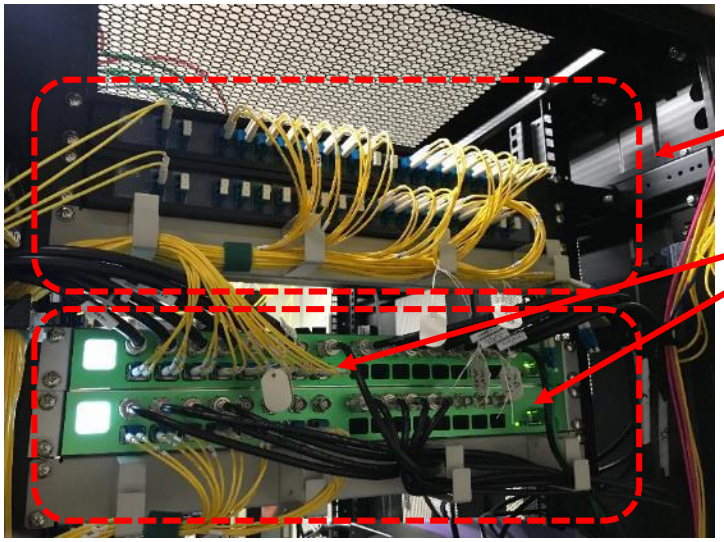
- **柔軟な買い方と運用がポイント**
  - **純正品オプティクスモジュールが適している場合**
    - 純正品は製品の出来・保守の側面で信頼度が高い
    - ほぼ変更が発生しない構成やコア部分で使う
    - **枯れてない規格のトランシーバで安定度を求めなければならない場合**
      - 100G/100Gや長距離用トランシーバの様に特殊なもの
  - **サードパーティオプティクスモジュールが適している場合**
    - 変更が発生しやすい構成やエッジ部分で使う
    - 研究開発のように流動性や即応性が求められる場合
      - 事前に使う総量が決定できない
      - まとめて在庫を持ち一括管理
    - 枯れてきている規格については積極的に導入しても良い
      - 10Gでは積極的に採用しコスト削減に寄与
      - 25G/50G の様に既にサードパーティ製が多い規格は要注意
  - **特徴を理解し組み合わせて運用することが重要**
    - **フロアで使うLANケーブルと、フロア間の固定配線の関係に近い**

サードパーティオプティクスの広まりと影響

- **運用を通して**
  - **トランシーバモジュールへの理解の促進**
    - トランシーバモジュールを扱える人が増えた
      - 今まではNWを専門に扱っていた人しか扱えなかった
      - Not-NWエンジニア でも光トランシーバが扱えるようになった
    - 実際に使ってもらい経験することで理解が進んだ
      - サーバサイド/アプリ開発エンジニアにとっては未知の領域
      - 実際に使ってもらったことで**垣根がなくなり運用しやすくなった**
  - **特殊トランシーバモジュールの活用**
    - Bi-Directional トランシーバモジュールの導入
      - 1芯で双方向通信が可能なトランシーバモジュール
      - 少ない構内配線や拠点間通信で活用
      - **純正品ラインナップに存在しない種別のトランシーバ**
        - サードパーティオプティクスモジュールを頼る形に

サードパーティオプティクスの広まりと影響

- **サードパーティの応用例**
  - **サードパーティオプティクスのCWDMシステムへの応用**
    - 拠点間で大容量通信を行う必要があった
      - 3G SDI 信号 と 10G Ethernet 信号の混合（180Gbps*2）
    - DF + サードパーティオプティクスによる自前CWDMシステム構築へ
      - Open Optical Line System の考え方
      - SDI信号の処理の都合で DWDMを採用できないため CWDM へ
    - 大量の専用線調達を回避し、極めて大幅なコスト削減に成功



光合分波モジュール

3G SDI　E/O トランスポンダー
MSA Video Transceiver

10G Ether用のCWDMトランシーバは各SWのポートに直接取り付け（トラポンレス）

サードパーティオプティクス
に対するよくある不安

サードパーティオプティクスに対する よくある不安

- **自前で運用保守できる自身がない場合はどうすれば…**
  - **正しくエンジニアリングをするためにはある程度知識が必要**
    - Over 10G の世界では、**知識の正しさと量が重要**
    - オプティクスの世界は奥が深い、深く知ることで正しい対応ができるようになる
  - **運用負担が低い部分からサードパーティオプティクスを使い始める**
    - 1G,10Gは製品も枯れてきており、比較的簡単に導入が可能
      - NWでもいきなりCoreに入れずEdgeから徐々に初めて見る
      - 使うことでサードパーティオプティクスに対する構えが整う
    - 40Gも間もなく10Gの様に扱える領域に入る
      - ただし**MPOケーブルに対する知識が新たに必要**
      - 100G以降は複雑化が更に進むためノウハウの蓄積と製品が枯れてくるまで時間がかかりそう

サードパーティオプティクスに対する よくある不安

- **自前保守の道具高いんじゃないの？**
  - **そんなことないです**
    - 最低限必要：クリーナー、パワーメーター、パワーソース
      - 近年安価になり、10万円程度で揃えられる
    - あると便利：ファイバースコープ
    - 詳しくなるとほしい部品が沢山
      - 高価な測定器等はレンタルするという手も
  - **長距離伝送システムを構築しない限り、比較的低コストで可能**
  - **正しい知識が手に入ること＝担当者の成長というメリット**

まとめ

まとめ

- **Ethernetの進化に伴い、メディア選択の重要度が増す**
  - マルチレートイーサネットへ向き合おう
- **サードパーティオプティクスの波が本格的に到来**
  - 乱立する規格に対する情報収集はこまめに
  - 正しい知識情報に基づいたNW設計へ
- **NW機器に対する考え方を改めよう**
  - 自らNW機器を選別して望むNWを作り上げる
- **柔軟な物品管理**
  - 運用と向き合い柔軟な運用の実現へ
  - 保守のあり方も見直そう

ご清聴ありがとうございました

I C S C o E

Industrial Cyber Security Center of Excellence