TLP:CLEAR

安定輸送を脅かす最新のサイバー脅威と事業継続のための要諦

2025年 12月

名和 利男

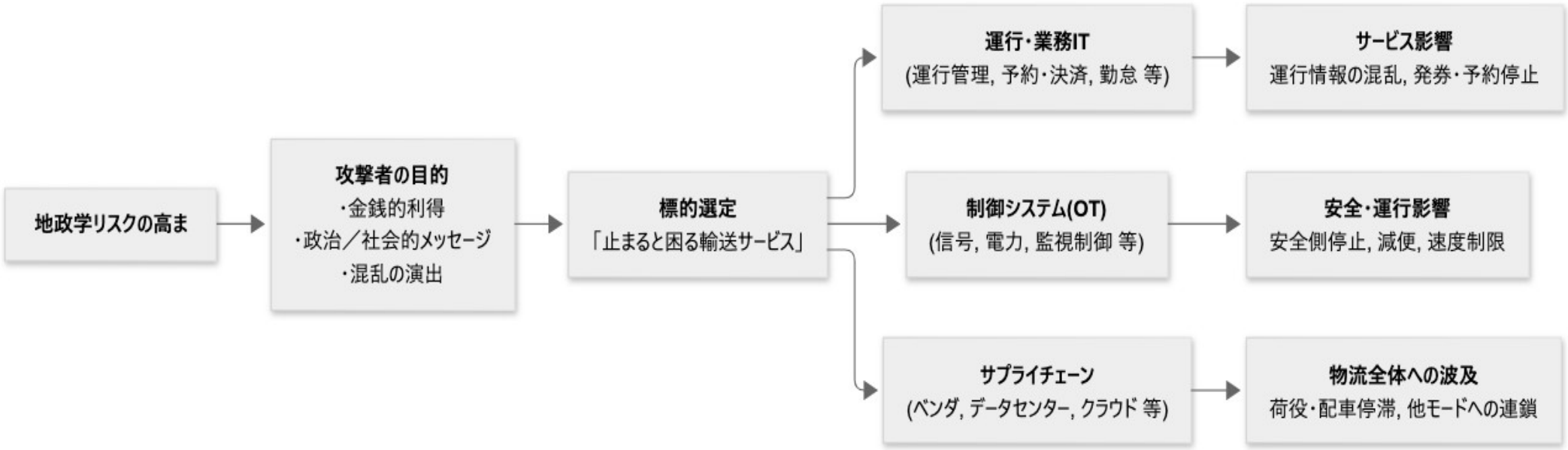
ねらい -「安定輸送を脅かす最新のサイバー脅威と事業継続のための要諦」

- サイバー攻撃が「**安定輸送**」とどのように結びつくのかを共有します。
- 単なるITトラブルではなく、「**安全・定時・正確**」という価値そのもののリスクとして捉えていただきます。
- そのうえで、各社で明日から見直せる**組織的・技術的なポイント**を持ち帰っていただくことを目指します。

安定輸送とサイバーの関係を揃える

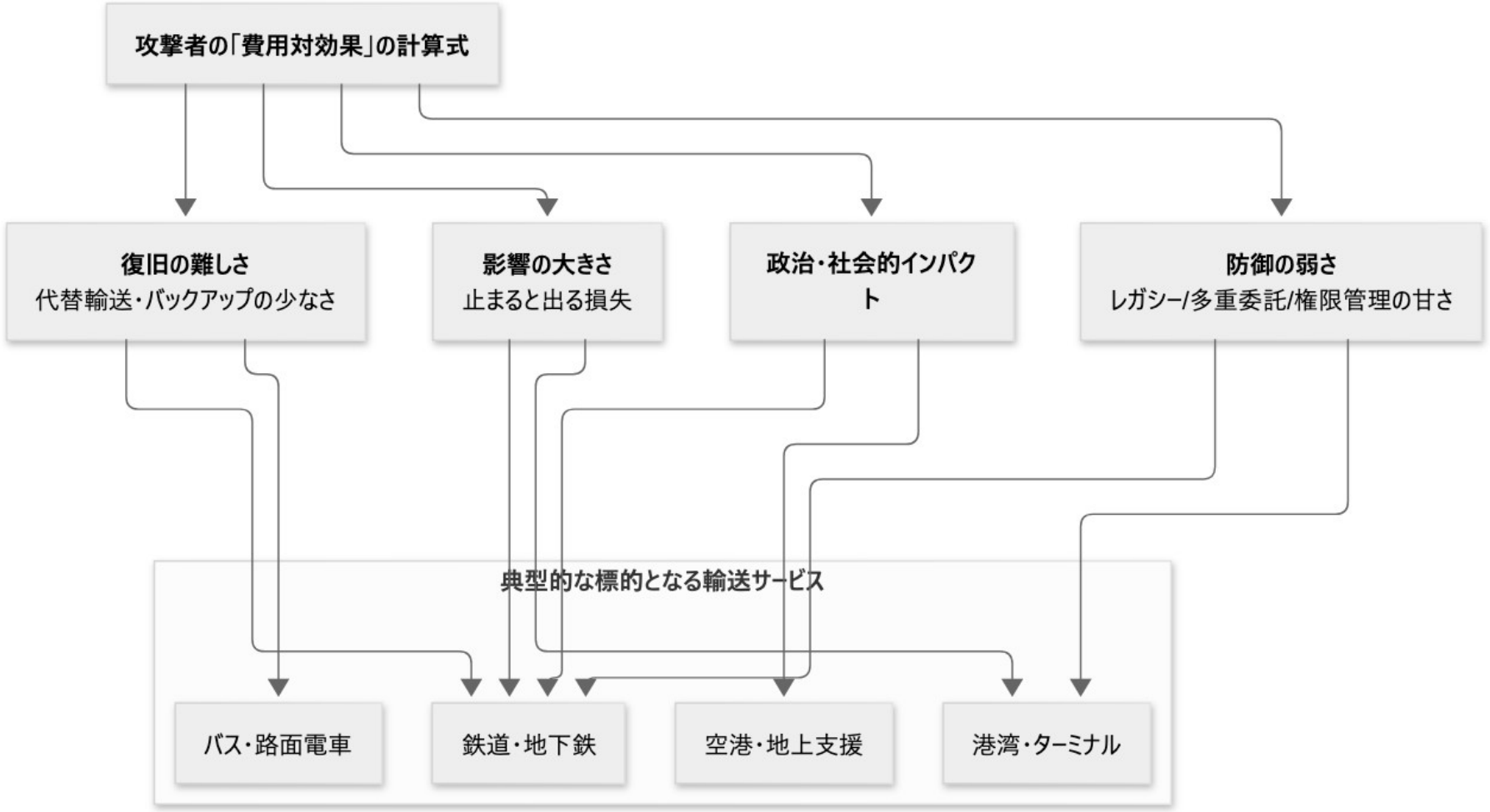
- 運輸事業者にとっての「**安定輸送**」とは
  - 人とモノを「安全」「定時」「正確」に運ぶという使命を継続することです。
  - サイバー攻撃が揺さぶるもの
- 運行管理・予約・決済といったITシステムを通じて、**サービス提供能力**そのものを揺るがします。
  - 場合によっては、制御システムまで含めて安全側停止や運休に追い込まれる可能性があります。
- 本講演の視点
  - 「サイバー＝情報システム部門の問題」という見方から一歩進めて、
  - 「**安定輸送を支える全体の仕組みへのリスク**」としてご一緒に整理していきます。

【図解】安定輸送に対するサイバーリスクの構造



TLP:CLEAR

輸送事業を狙う4つの攻撃パターン



TLP:CLEAR

セッション 1

事例で見る:
安定輸送を揺るがしたサイバー事案

海外事例：サプライチェーン経由で止まる輸送

- デンマーク鉄道事業者DSBの事例
  - 列車運行で必須となる**ソフトウェアを提供するベンダ**がランサムウェア被害を受けました。
  - その結果、保守のためにサーバが停止され、**全国的な列車運行停止**が数時間続いたと報告されています。

- 学べるポイント
  - 「**自社は直接狙われていないのに止まる**」というパターンが現実に存在します。
  - **サプライチェーンの一社の停止**が、国全体の輸送に波及し得ることを確認できます。

国内事例：港湾物流が止まったケース

- 名古屋港のランサムウェア事案の概要
  - コンテナターミナルのシステムが攻撃を受け、**積み下ろし管理システム**が停止しました。
  - トレーラーの受付・搬出入ができなくなり、数日間にわたり**港湾物流が大きく停滞**しました。

- 運輸全体への示唆
  - **一見「港湾のシステム障害」に見えても**、トラック輸送・鉄道・海運・サプライチェーン全体に影響が及びます。
  - 「一拠点のシステム停止」が、**上流・下流の運輸モードに連鎖する**ことを意識する必要があります。

事例から見える共通パターン

- 共通している点
  - デジタル化・効率化を進めた「**要のシステム**」が攻撃の標的またはボトルネックになっています。
  - 自社単体ではなく、**サプライチェーン全体で事業継続**を考えざるを得ない状況です。

- まとめ
  - 「ITの一部のトラブル」ではなく、「**輸送サービス全体の一時停止**」として現れることが多いです。
  - 以降のセッションでは、こうした事案の背後にある攻撃者の発想と、**壊され方のパターンを整理**していきます。

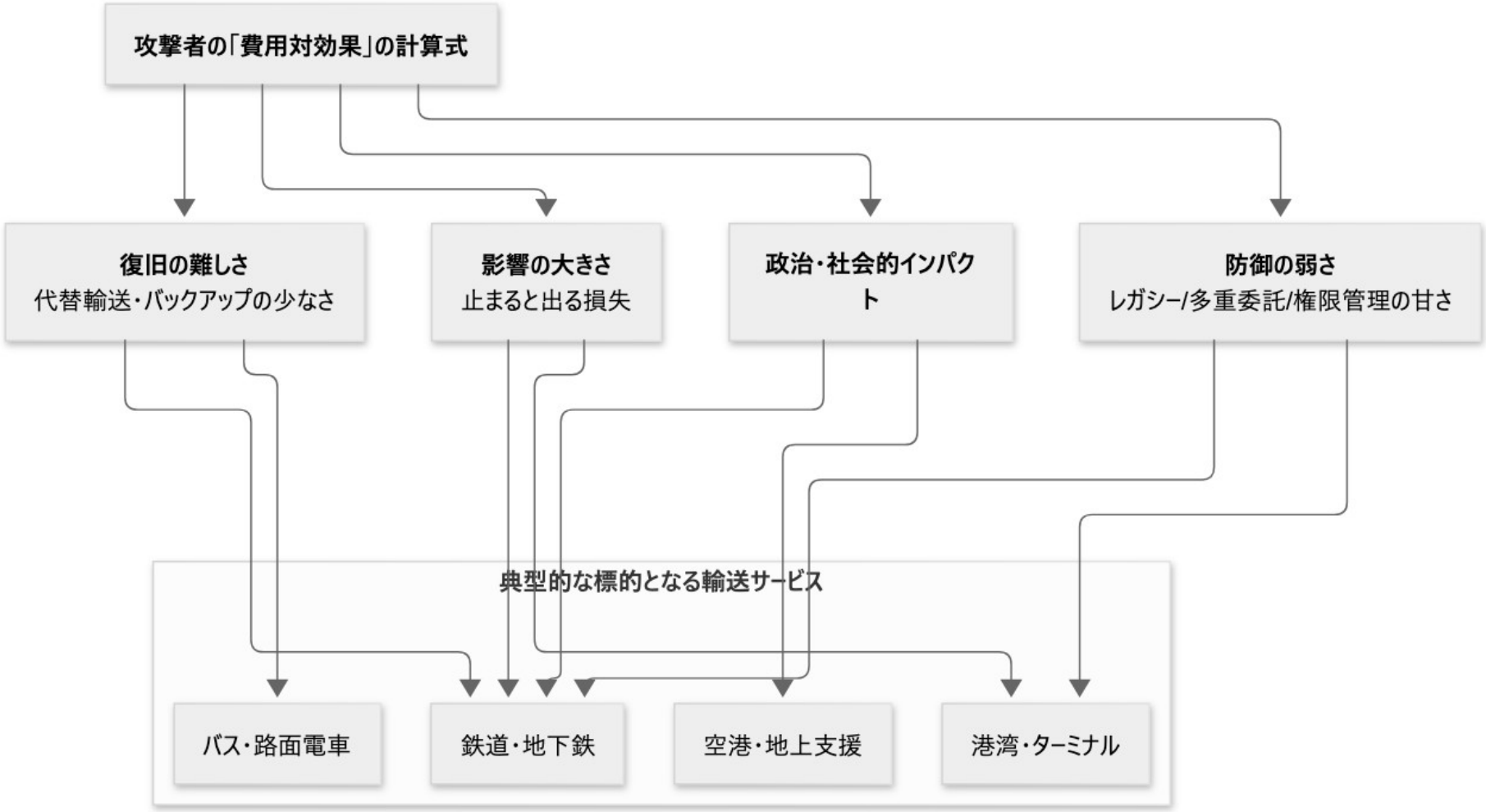
セッション 2

攻撃者の「計算式」と壊され方のパターン

攻撃者の費用対効果という発想

- 攻撃者は感情だけで動いているわけではありません。
  - 「**いかに少ないコストで、いかに大きな影響を与えられるか**」を常に考えています。
- 計算の要素
  - 止まったときの損失やニュース性（**影響の大きさ**）
  - 復旧に時間がかかるかどうか（**代替手段の有無**）
  - セキュリティの弱さ（**レガシーシステム、多重委託、権限管理の甘さ**など）
- 運輸業界が狙われやすい理由
  - 「止まるとすぐに社会問題になる」ため、攻撃者にとって“**費用対効果の高い標的**”になりやすい側面があります。

【図解】攻撃者の「費用対効果」の計算式と輸送サービス

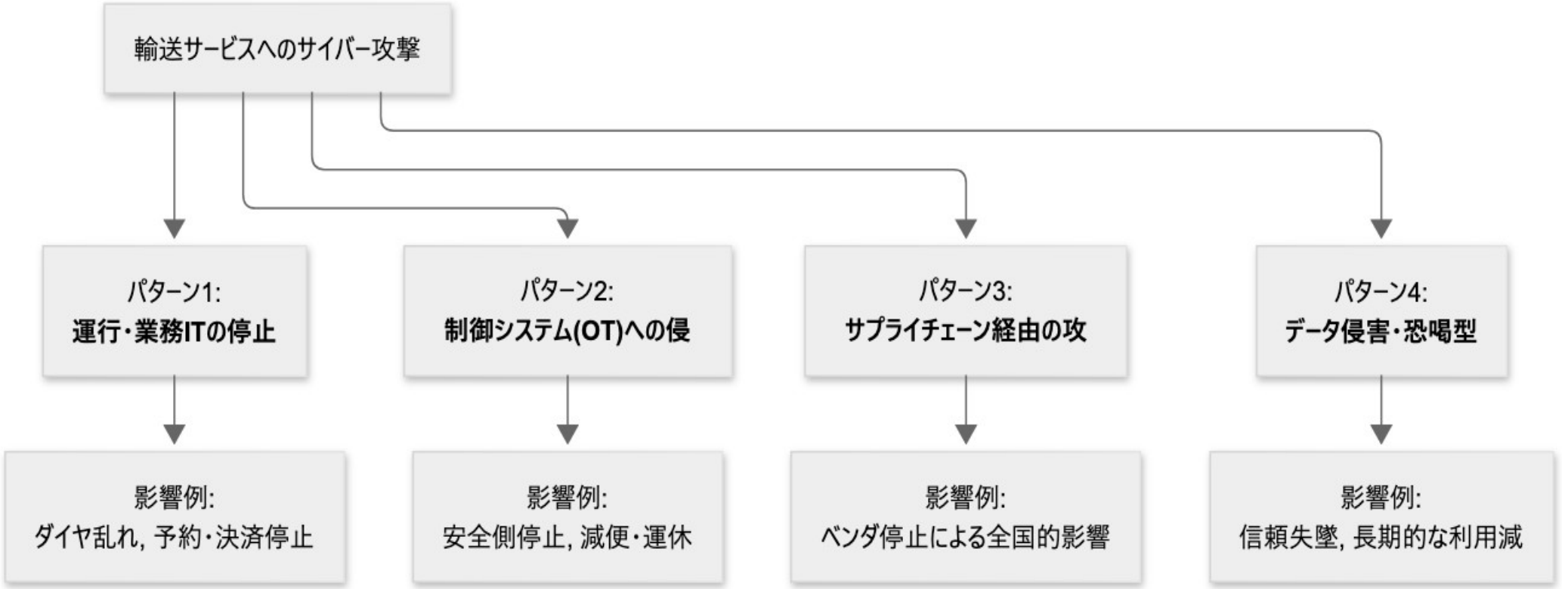


TLP:CLEAR

輸送事業を狙う4つの攻撃パターン

- パターン1：**運行・業務ITを止める攻撃**
  - 運行管理、予約・決済、人員配置などが停止し、運行計画どおりに動けなくなります。
- パターン2：**制御システム（OT）に侵入する攻撃**
  - 信号・監視制御・電力制御などに影響し、安全側停止や減便・運休が長引くおそれがあります。
- パターン3：**サプライチェーン／ベンダを経由する攻撃**
  - 自社ではなく、必須ソフト・クラウド・データセンターが止まることで、結果的に輸送が止まります。
- パターン4：**データ侵害による信頼失墜型攻撃**
  - 顧客・荷主情報や運行データの流出により、ブランドと長期の信頼にダメージを与えます。

【図解】輸送事業を狙う4つの攻撃パターン



TLP:CLEAR

「どこが壊れると一番困るか」を可視化する

- 自社の業務に当てはめてみると
  - **どのシステムが止まると、何時間後に「重大な輸送影響」が出るのか**を洗い出しておくことが重要です。

- 可視化のポイント
  - 運行・現業・IT・経営が**同じ図を見て議論**できるレベルの粗さで構いません。
  - 「止めると**危険**」「止めると**困る**」「止めても**なんとかなる**」を分けて整理します。

- この作業が、後ほどお話しする「優先度の高い対策」と「事業継続計画」の土台になります。

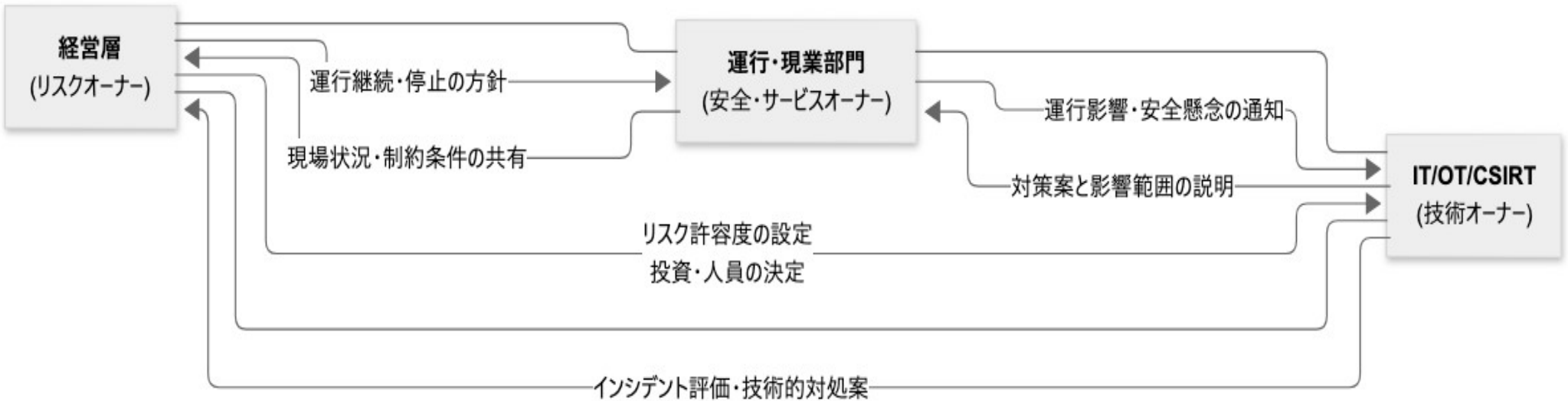
セッション 3

事業継続のための組織的要諦

三位一体の体制：経営・現場・技術

- サイバー事案は、**技術部門だけでは完結しません。**
  「止める・止めない」の判断には、経営と現場の視点が必須です。
- 三位一体の役割イメージ
  - **経営層**：リスク許容度と優先順位、投資判断を担います。
  - **運行・現場**：安全とサービスを守る観点から、現場状況と制約条件を示します。
  - **IT/OT/CSIRT**：技術的な評価と止血策、復旧プランを提示します。
- この3つが「横並び」で議論できる場を、**平時から用意しておく**ことが大切です。

【図解】経営・現場・技術の三位一体体制



TLP:CLEAR

初動24時間で「誰が何を決めるか」を明文化する

- 初動で迷わないために
  - どのレベルの事象で、誰が何分以内に報告するのかを**あらかじめ決めて**おきます。
  - 「運行影響の有無」「安全への懸念の有無」を、**早期に経営が把握できる**ようにしておきます。

- 決めておきたい項目
  - システム停止・手動運転・減便などの**決定権限**
  - 対策本部の**立ち上げ条件**と、**招集するメンバー**
  - 国交省・警察・関係自治体・ISAC等への**連絡ルート**と**優先順位**

【表】初動24時間の RACI マトリクス

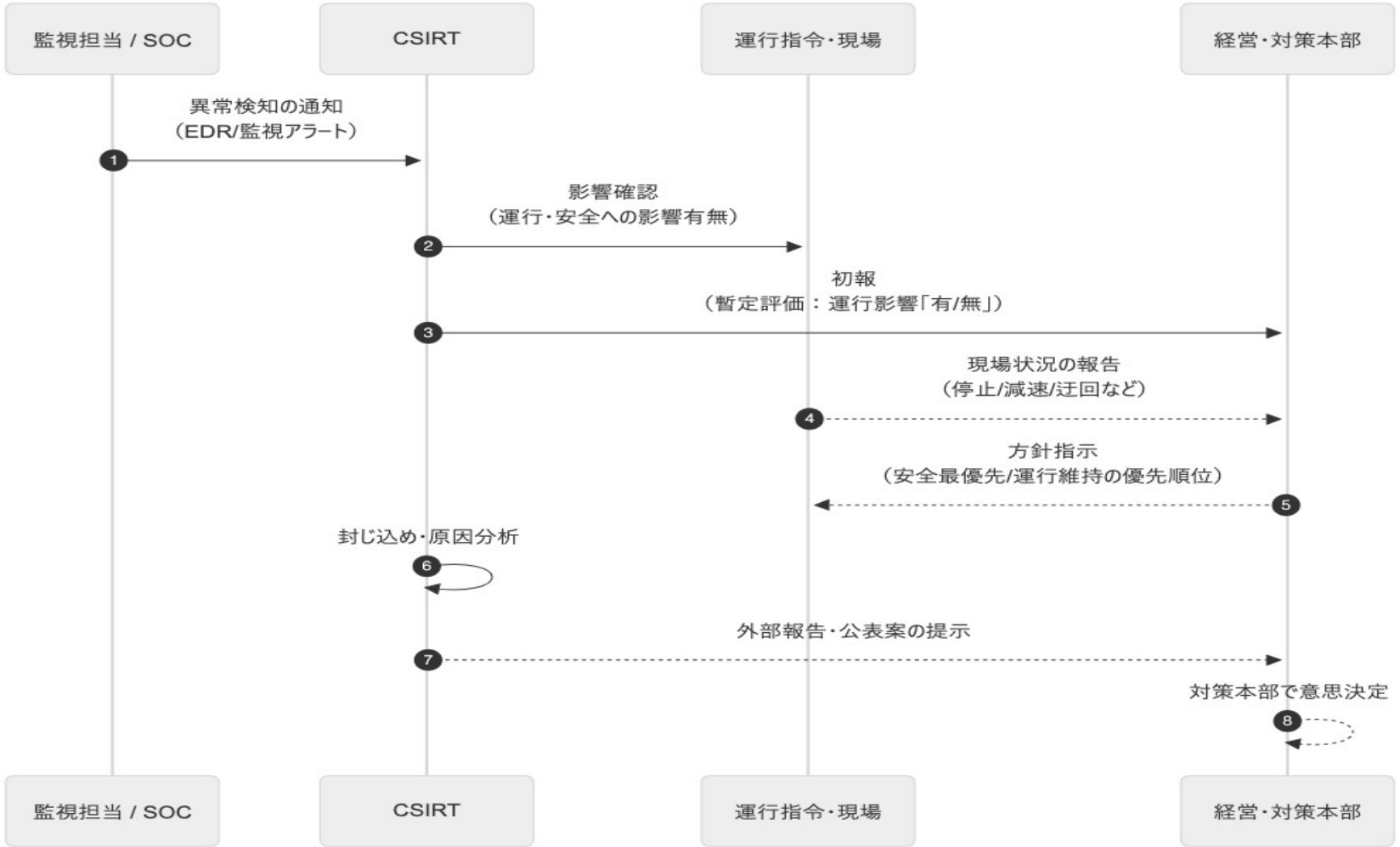
フェーズ / 行為	経営層	運行・現場部門	IT/OT部門	CSIRT・SOC
異常検知・一次解析	**I** (報告を受ける)	**I**	**C** (技術支援)	**R/A**
運行・安全への影響評価	**C**	**R/A**	**C**	**C**
初報（暫定評価）の経営層への共有	**I**	**C**	**C**	**R**
システム停止/減便/運休の意思決定	**A**	**C**	**C**	**I**
外部機関（国交省・警察 等）への連絡方針	**A**	**C**	**C**	**C**
技術的封じ込め・原因究明	**I**	**I**	**C**	**R/A**
再開条件の整理と合意	**A**	**R/C**	**C**	**C**

R：実務上の実行責任（ Responsible ）
A：最終決定責任（ Accountable ）
C：助言・協議（ Consulted ）
I：情報提供（ Informed ）

初動の情報連携イメージ

- 監視・CSIRT・現場・経営の連携は、**具体的な流れで共有しておく**と動きやすくなります。例として、次のとおり。
  - 監視担当が異常を検知し、CSIRTにエスカレーションします。
  - CSIRTが運行への影響を現場と確認し、速報として経営に報告します。
  - 経営と現場が、安全確保とサービス継続のバランスを議論し、方針を決定します。
- この流れを**机上演習などで何度か試しておく**ことで、実際の初動がスムーズになります。

【図解】初動24時間の情報連携イメージ（シーケンス）



TLP:CLEAR

演習と教訓の「BCPへの織り込み」

- 机上演習の目的
  - 現実に起こり得るシナリオで、**「止める・止めない」「どこまで公表するか」を議論**しておくことです。
- 演習後に必ず行いたいこと
  - BCP、インシデント対応手順、連絡体制などの文書に、**決まったことをきちんと反映**します。
  - 「次回までの宿題」を明文化し、**担当と期限を決める**ようにします。
- このサイクルを回すことで、「計画があるだけ」から「**実際に動ける計画**」へと成熟させていくことができます。

セッション 4

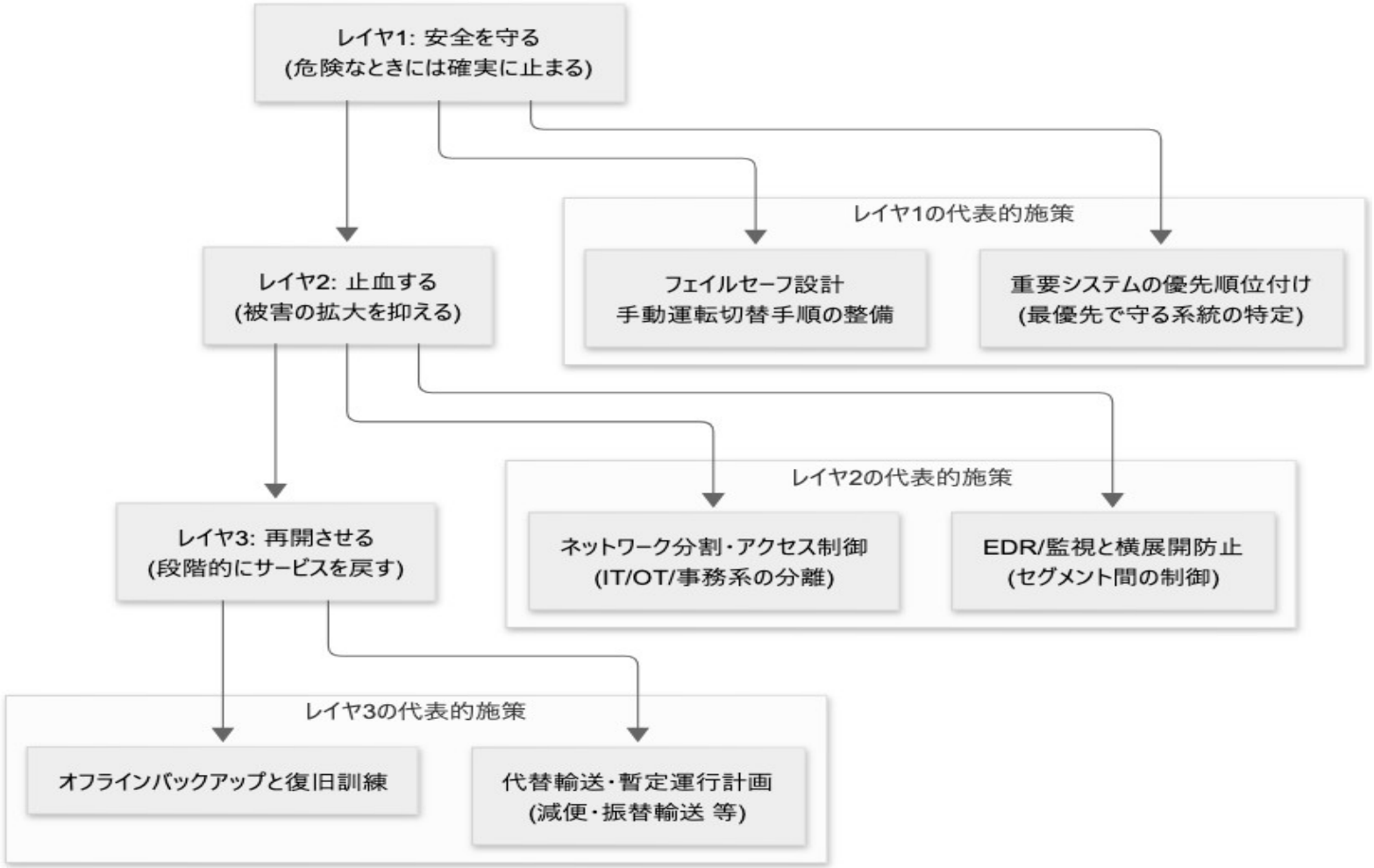
事業継続のための技術的要諦

安全・止血・再開の三レイヤーで考える

- 技術的な対策を三つのレイヤーで整理すると、優先度が見えやすくなります。
  - レイヤ1 = **安全を守る**（危険なときには確実に止まる）
  - レイヤ2 = **止血する**（被害の拡大を抑える）
  - レイヤ3 = **再開させる**（段階的にサービスを戻す）

- どのレイヤーも重要ですが、順番と役割を整理することで、**限られたリソースを有効に投下**できます。

【図解】安全・止血・再開の3レイヤー



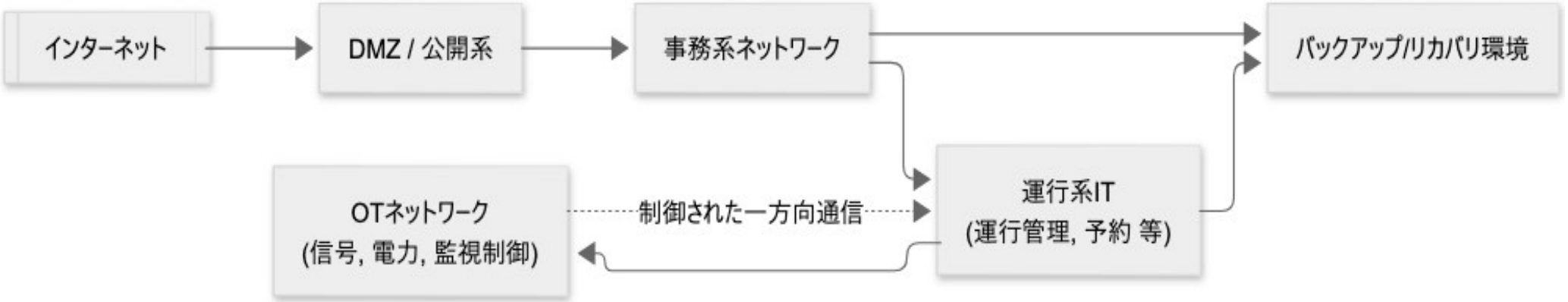
TLP:CLEAR

ネットワークとバックアップを「BCPの視点」で見直す

- **ネットワーク分割**の再確認
  - ITとOT、事務系と運行系など、どこまで論理的・物理的に分かれているかを改めて確認します。
  - ランサムウェアが横展開しにくい構造になっているかどうかも重要です。

- バックアップと**復旧手順**
  - オフラインを含むバックアップが、どこに、どの頻度で存在するのかを整理します。
  - 復旧手順がドキュメント化されているだけでなく、実際にリハーサルされているかどうかがポイントです。

【図解】IT・運行IT・OT・バックアップの全体像(簡易ネットワーク)



TLP:CLEAR

サプライチェーンと「共通運命体」としての備え

- 委託先・共同事業者との関係
  - 重要なシステムを担うベンダやクラウド事業者と、「インシデント発生時の連絡・情報共有・復旧協力」の枠組みを確認しておきます。
  - SLAや覚書などに、最低限の情報共有やタイムラインの期待値を明記しておくと安心です。

- **合同演習・情報共有**の勧め
  - 可能であれば、主要なベンダと合同で小さな机上訓練を実施しておくと、実際の連携が格段にスムーズになります。

セッション 5

最初のアクションとまとめ

経営・ガバナンスの「最初の一歩」

- 経営として明確にすること
  - 「**サイバーは安定輸送・安全の問題である**」と、社内向けにメッセージを出します。

- 最初に着手したい事項
  - サイバーインシデント時の決裁権限表を、**初動24時間の動き方**の観点で点検・改訂します。
  - 次回のBCP改訂サイクルで、「**サイバー攻撃前提のシナリオ**」を少なくとも1本は組み込むことを決めます。

現場・技術・サプライチェーンの「アクション」

- 現場とCSIRTの連携強化
  - 運行指令・現場とCSIRTが一緒に「**インシデント初動カード**」を作成し、簡潔なチェックリストとして共有します。
  - 過去の障害事例を「**もしサイバーだったら**」という観点で振り返るミニワークを行います。

- 技術・サプライチェーンの見直し
  - 主要システムごとに「**何時間止まると重大な影響か**」を整理し、優先度マップを作成します。
  - 重要ベンダとの間で、インシデント時の連絡先・連絡手段・初動情報の範囲を確認し、**文書化**します。

本日のまとめとメッセージ

- 今日お伝えしたかったこと
  - サイバー攻撃は、**安定輸送・安全・事業継続を同時に揺さぶるリスク**であるということです。
  - **攻撃者の「費用対効果」の発想**から見ると、運輸業界は決して他人事ではない標的となっています。

- 明日から実行していただきたいこと
  - 自社の「どこが壊れると一番困るか」を、**経営・現場・技術が同じ図で共有**することです。
  - そのうえで、**「止める・止めない・再開させる」の3レイヤー**で、組織と技術の備えを一歩ずつ前に進めていただければと思います。

本資料に関する連絡先

名和 利男（ Toshio NAWA ）

SITE: www.nawa.to

PGP: 0xFCFE14E1E38B4E01

TLP:CLEAR