交通サイバーセキュリティXII

交通運輸分野における基幹インフラサービスの安定的な提供に向けた持続可能なサイバーセキュリティ体制の構築について

～総括ディスカッション～

情報セキュリティ大学院大学

後藤　厚宏

本日のご講演1

山下　雄史様：サイバーセキュリティに関する国土交通省の取組

- 「国家安全保障戦略」（令和4年12月16日閣議決定）に基づき、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、サイバー安全保障分野での対応能力の向上に向けた検討が行われている。こうした中で、サイバー安全保障に関する政府の検討状況について、また、サイバーセキュリティを巡る国土交通省の最近の取組状況について講演する

本日のご講演2

古川　文路様：社会インフラを支える製造業におけるサプライチェーンセキュリティの取組～サイバーレジリエンスの向上に向けて～

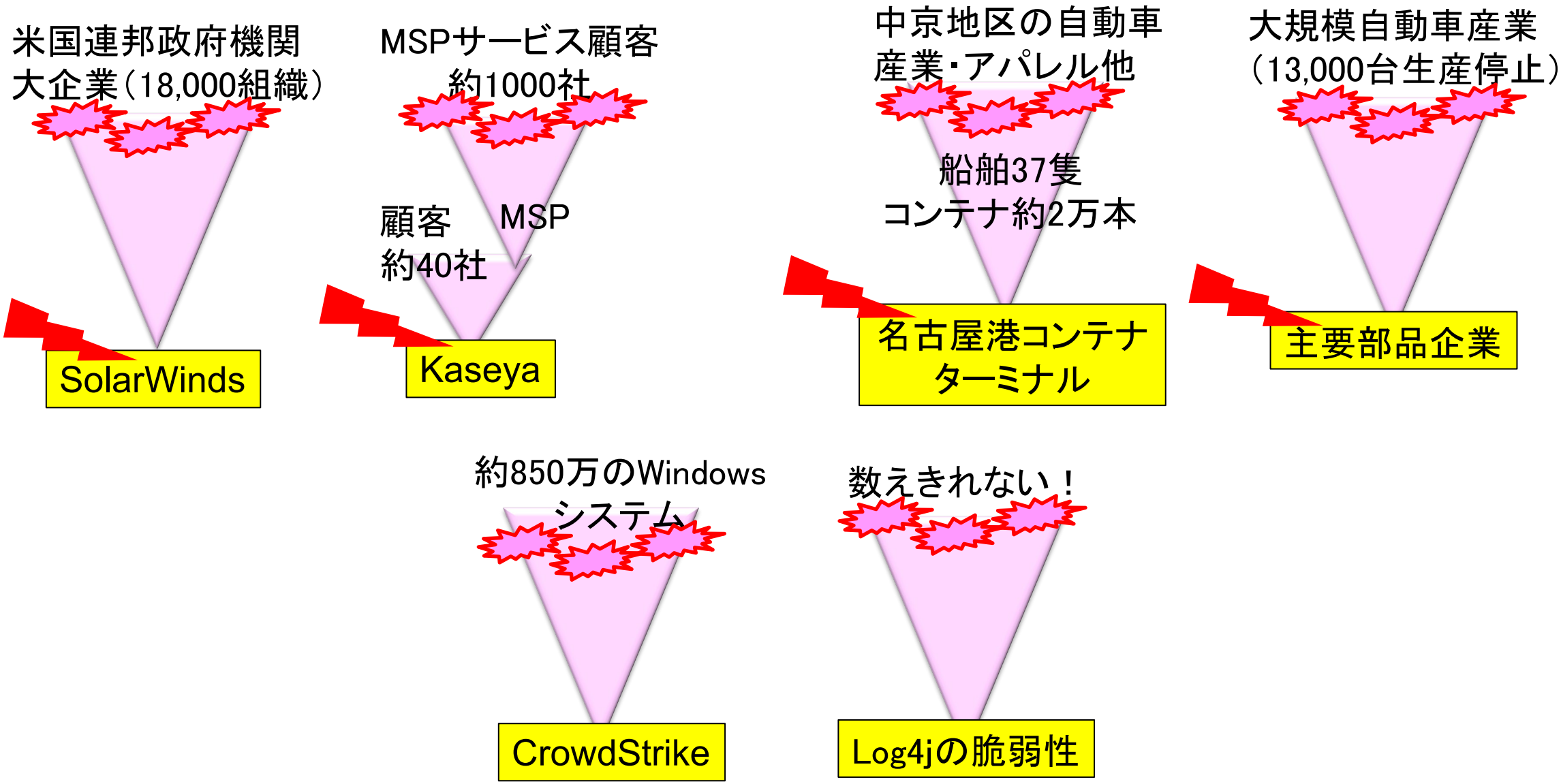
- 昨今、産業分野を狙ったランサムウェア攻撃やサプライチェーンに起因するサイバーインシデントが増加している。さらに、国内の経済安全保障推進法やEUのサイバーレジリエンス法など、サプライチェーンセキュリティ対策に関する規制も始まっている。このような状況を踏まえ、電力、水道や鉄道等の社会インフラに製品を納める東芝のサプライチェーンセキュリティ対策、サイバーレジリエンス向上のための取り組みをご紹介

本日のご講演3

名和 利男様：対策から組織戦略へ：脅威の変化に応じた持続可能なセキュリティ体制の構築

- サイバー脅威は、一変して企業の事業活動に影響を与えるものとなっている。しかし、依然として私たちはレガシーな対策で被害を防ごうとし、ほとんどの企業で失敗している。この主要因は、「予算や人的リソースの不足」と言われているが、それ以上に、組織における「持続可能なセキュリティ対策の成熟が低レベル」であることを受け入れる必要がある。本講演は、今のサイバー脅威の特徴から、組織戦略の重要性を考えていく

サプライチェーンによる被害の「波及」と「増幅」



自組織への直接被害とサプライチェーンを介した波及被害

サプライチェーンのリスク（経営視点）⇒　サプライチェーン全体へ拡大

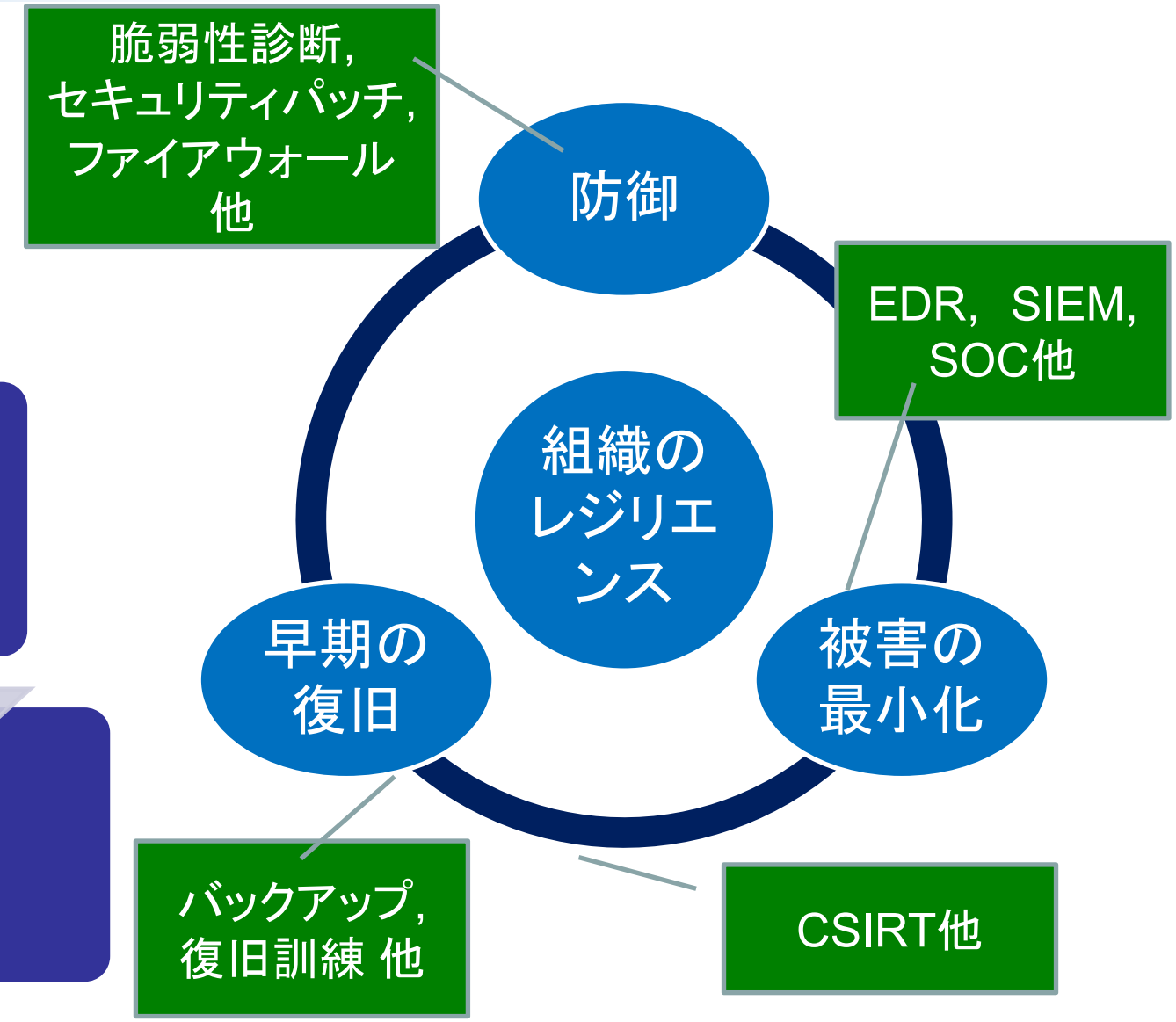
産業構造全体のリスク（政策視点）⇒　産業全体へ拡大

サイバー攻撃リスクとレジリエンス確保

ネットワーク社会のアタックサーフェスは広大・複雑（⇒要防御）

一方で、サイバー攻撃による被害をゼロにすることは困難

社会・産業・組織が回復不能にならない（破綻しない）**レジリエンス**



パネルディスカッション 「テーマ１」

■サプライチェーン対策とレジリエンスのあり方

サプライチェーンのリスクと対策

① 国内外の子会社、委託先等を踏み台にした攻撃対策

② 導入するITやネットワーク機器、ソフトウェア等への不正対策

③ メンテナンス時における不正ソフトウェアが混入したアップデートなどに対する対策

④ サプライチェーンにおける波及被害対策

とレジリエンスのあり方

パネルディスカッション 「テーマ２」

■持続可能なサイバーセキュリティ体制の構築について「テーマ１」の議論を受けて、

- 持続可能なサイバーセキュリティ体制の構築
- 官民連携の在り方と課題

ご質問・
コメント・
アドバイス
をお願いします