令和8年第24回原子力委員会
資料第１号

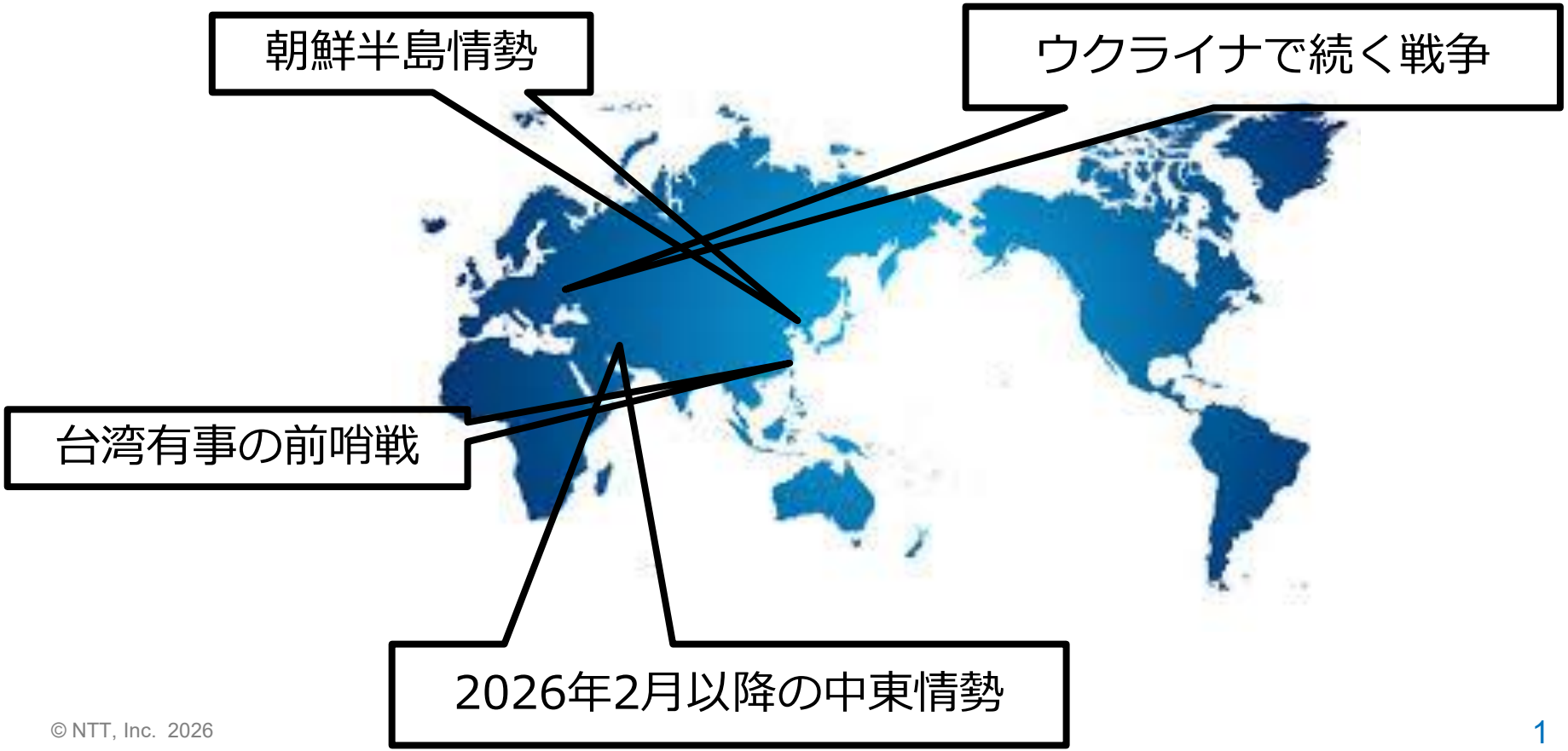
重要インフラへの攻撃事例とレジリエンスの教訓

原子力委員会　定例会議

松原　実穂子
NTT　チーフ・サイバーセキュリティ・ストラテジスト

令和8年6月16日（火）1400～1510

地政学的緊張関係とサイバー攻撃



ウクライナの民間企業がサイバー攻撃＋に直面

- 軍事侵攻前から金融など重要インフラサービスへのサイバー攻撃
- 軍事侵攻後は、業務妨害目的のサイバー攻撃＋ミサイル・ドローン攻撃
  - 2025年12月時点で想定修理総額は、**GDPの3倍相当の5880億ドル（92兆円）**
  - 2025年の**勤務中の負傷者は1,000人以上**、**殉職者は200人以上**

重要インフラのレジリエンス

■ 平時の備え

- 軍、規制当局、企業の連携と事業継続計画
- 能動的サイバー防御関連法
- 「国家防衛戦略」：「重要インフラに対する攻撃に際しては実効的な対処を行」う

■ 中東情勢と東アジア情勢

■ 目指す国のかたち

- 「たたかい」の再定義と個々の当事者意識＝強い和