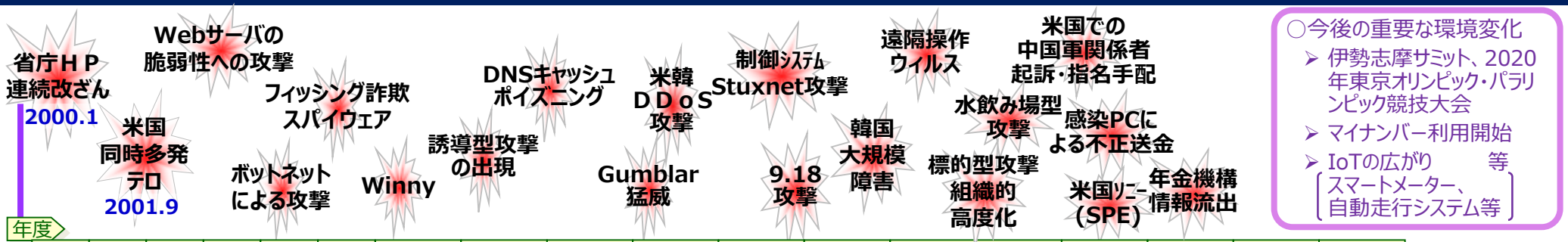
NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

重要インフラの情報セキュリティに係る第３次行動計画について

内閣官房　内閣サイバーセキュリティセンター(NISC)
重要インフラグループ　参事官
瓜生　和久

サイバーセキュリティ政策の経緯



第３次行動計画の基本的考え方・要点

「重要インフラ防護」の目的

重要インフラにおける**サービスの持続的な提供**を行い、**自然災害やサイバー攻撃等に起因するＩＴ障害**が国民生活や社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を**可能な限り減らす**とともにＩＴ障害発生時の**迅速な復旧を図る**ことで重要インフラを防護する。

「基本的な考え方」

情報セキュリティ対策は、**一義的には重要インフラ事業者等が自らの責任において実施**するものである。
また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- **政府機関は**、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して**必要な支援を行う**。
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、**他の関係主体との連携をも充実させる**。

～ 行動計画推進に当たって期待する関係主体、更には事業者等の経営層に期待すること ～

各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方

- **自らの状況を正しく認識**し、**活動目標を主体的に策定**するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、**相互に自主的に協力**する。
- ＩＴ障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、ＩＴ障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。

- 上記の目的達成に当たっての情報セキュリティを中心とする**リスク源の認識**。
- 上記のリスク源の評価及びそれに基づく**優先順位を含む方針の策定**。
- システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営**資源の継続的な確保**。
- システムの運用状況の把握等を通じた当該方針の**実行の有無の検証**。
- 演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の**検証及び改善策の有無の検証**。