警察庁 National Police Agency

重要インフラ専門委員会　警　察　庁　資　料

政府の情報セキュリティ対策における警察庁の貢献の在り方

平成20年7月18日

1. 警察庁の基本的な考え方
→ 警察の3つの特性

知見
- ◆ 国内外におけるインテリジェンス活動
- ◆ リアルタイム検知ネットワーク等監視活動
- ◆ 重要インフラ事業者との連携
  - → 個別訪問、共同対処訓練、サイバーテロ対策協議会
- ◆ 捜査活動を通じて得た情報等による犯罪及びその情勢の分析
- ◆ サイバー犯罪相談窓口での相談対応、サイバーセキュリティ・カレッジ等における防犯指導

技術
- ◆ 不正プログラム解析技術
- ◆ 各種機器の動作検証技術
  - → 各種OSのDoS攻撃防御機能の動作検証
  - → FW、ルータ等のDoS攻撃に対する負荷検証　等
- ◆ 各種サイバー攻撃に対する防御ツール等の活用・開発

捜査
- ◆ 国内における捜査活動
- ◆ 国際捜査
  - → ICPO、 G8・24時間コンタクトポイントを通じた捜査協力
- ◆ デジタルフォレンジックの確立に向けた取組み

未然防止
事態対処 に貢献

1. 警察庁の基本的な考え方
→ 重要インフラ事業者等と警察の連携強化

被害の拡大防止
- 被害の拡大防止策の検討
- 情報セキュリティ対策の強化
- 事案発生時の緊急対処活動の実施

“複眼的・有機的な対処”

捜査活動の実施
- 脅威原因の究明・除去、再発防止
- 通信ログ等の解析
- ICPO等を通じた国際捜査共助の実施
- 被疑者の検挙等による事案解明

事業継続性への配意
- 被害事業者の意向の尊重
- 事業者、警察のそれぞれが必要とする情報の共有

2. 北海道洞爺湖サミットに伴い講じた施策と課題

施　策

●　個別訪問

- 全国で延べ約900回実施
- 情報セキュリティ対策上の問題点の把握や緊急時の即応態勢を確立

●　共同訓練

- 全国で延べ約90回実施
- 実際に起こり得る様々な事態（大規模停電、ＤｏＳ攻撃、ＨＰの改ざん等）を想定した実践的なシナリオを作成

●　24時間監視

- サミットに関係する事業者等（洞爺湖町、ウインザーホテル洞爺等）のＨＰの24時間監視を実施

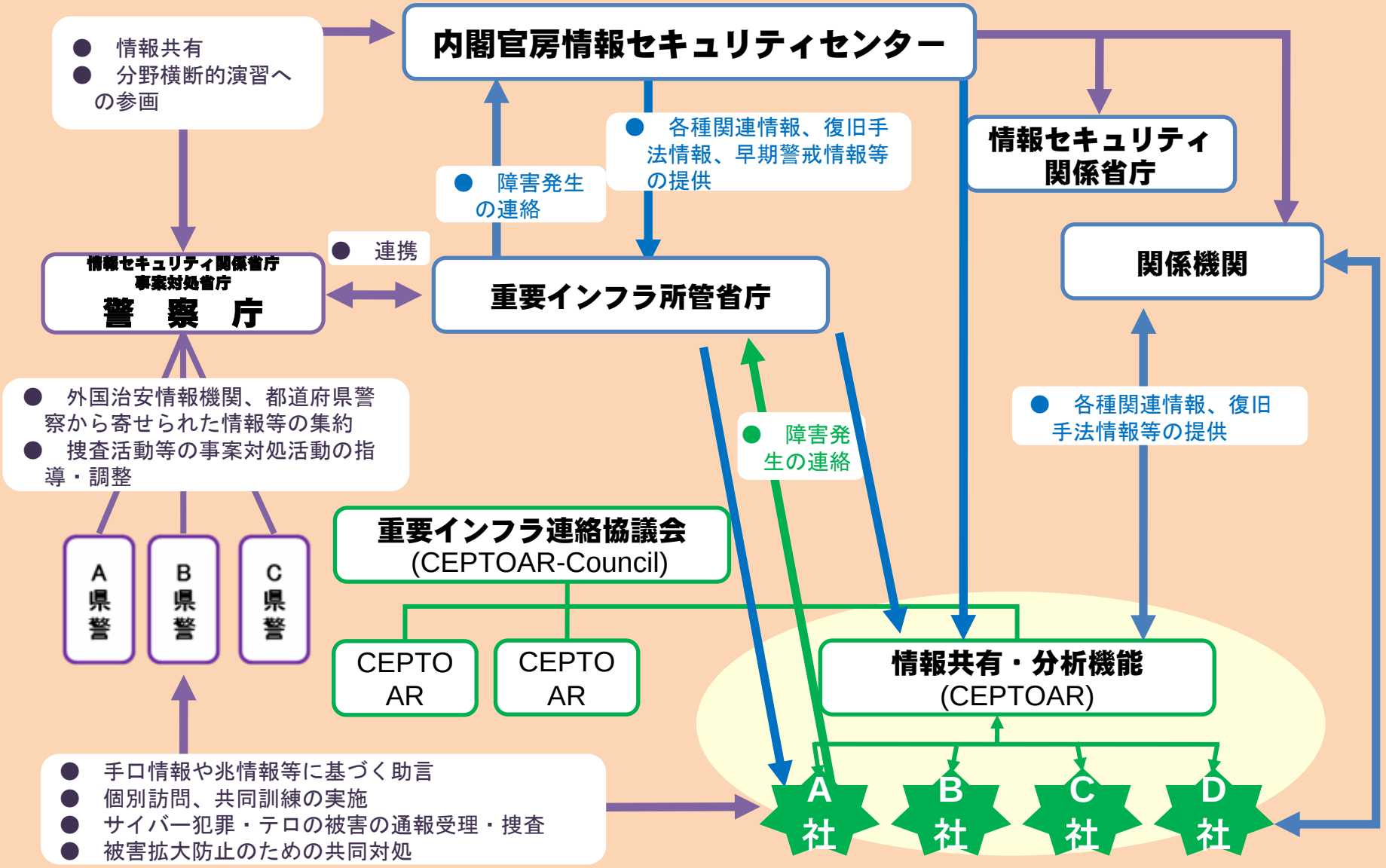
課　題

- ●　事業者間、地域間における情報セキュリティ対策の温度差
- ●　事業者がBCPを策定する際に必要となる知見の偏在
- ●　事業者における技術的知見の偏在

対　策

- ●　業種や地域に応じたキメの細かい情報提供
- ●　重要インフラ事業者がBCPを策定する際の助言・知見の提供
- ●　更なる技術的支援の充実
  - →　ボットネットやDoS攻撃の監視・早期検知を行うための機材・ソフトの開発等
  - →　サイバー攻撃の発信元調査を行うための機材・ソフトの開発、不正プログラム解析能力や暗号解析能力等の向上

3. 国が一丸となった情報セキュリティ体制



4. 諸外国の情報セキュリティ体制

全米サイバー対応調整グループ / NCRCG（National Cyber Response Coordination Group）

- DHS、DOJ/FBI、DODを共同議長として、連邦行政機関等の代表者で構成されたグループ
- 大規模なサイバー攻撃事案が発生した際に、国家的な対応方針を策定

活動調整・情報共有の促進

サイバー空間の防護及び事案対処関係機関

● 企画・調整官庁（Coordinating Agencies）

国土安全保障省（DHS）
国家サイバーセキュリティ課

司法省（DOJ）/FBI
- 他の法執行機関との協力によるサイバー犯罪の捜査活動を実施
- 民間企業との協力による未然防止を実施

国防総省（DOD）

● 支援官庁（Cooperating

- 商務省（DOC）
- エネルギー省（DOE）
- 国土安全保障省（DHS）
- 国務省（DOS）
- 運輸省（DOT）
- インテリジェンスコミュニティ
  - 他の事案対処機関との情報共有
  - 海外の脅威とサイバー攻撃の攻撃元を分析
- 国立標準技術研究所（NIST）
- 行政管理予算局（OMB）

● その他

- 科学技術計画局（OSTP）
- 国土安全保障会議 国家安全保障会議（HSC/NSC）

等

- 地方行政機関
- 非政府機関

５．北海道洞爺湖サミットのG8首脳声明

● テロ対策に関するＧ８首脳声明
G8 Leader's Statement on Counter-Terrorism

→ 我々は、G8の専門家から提出された国際テロリズム及び国際組織犯罪に関する報告書を歓迎し、以下を含むテロの脅威に対抗するための我々の協力を更に強化するとの我々の誓約を強調する。

→ テロリズムの多様化された脅威及び手段に照らし、（中略）情報通信技術の濫用を含む幅広い脅威に取り組むための我々の努力を強化する。

● テロ対策に関するＧ８首脳声明附属書

→ 我々は、国際的な重要情報インフラ施設の防護のための官民協力に関する好事例(Best Practices)を共有した。今後、これらの研究や取組の成果を踏まえ、重要インフラ施設の防護の更なる強化を図っていく。

（※ 以上は、外務省の仮訳による。）

【好事例(Best Practice)】

重要インフラ防護の責務を有する政府機関と法執行機関は、重要情報インフラ事業者との間に、事案発生時における機微な情報のやりとりを可能とする相互信頼関係を構築すること