資料5

第2分科会について

～重要インフラにおける情報セキュリティ対策強化のあり方の検討～

2004年10月26日

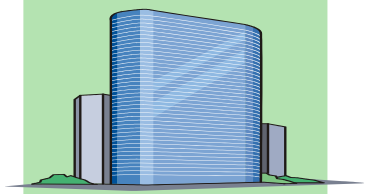
情報セキュリティ基本問題委員会事務局

1．第2次提言の射程（情報セキュリティ問題全体における位置付け）

情報セキュリティのグランドデザインの確立
実効性のある対策と施策の実施

重要インフラにおける情報セキュリティ対策のあり方

政府組織



- 民間のカウンタパートとしての信頼足り得る存在
- 国際的な信頼醸成
- バランスある技術投資の実施
- 透明性の確保

第1次提言

重要インフラ

- 依存可能な基盤としての機能提供
- 検証可能な機能設計と事業継続性確保
- 重要インフラ相互間の連携と協力

第2次提言

企業

個人

- 「セキュリティ文化」の参加者としての積極的な取り組み
- 個人情報保護問題やプライバシー問題に対するコンセンサスの形成

第3次提言

2．重要インフラにおける最近の主な関連事案（報道ベース）

サイバー攻撃	人為的ミス等
・豪クイーンズランド州で、市の水道施設の制御システムに侵入した犯人が、未処理の汚水100万リットルを河川および沿岸部に流し込んだ(2000/03) ・米カリフォルニア州の電力会社の送電網システムに外部者が不正侵入(2001/06) ・世界のルートDNSサーバ13箇所に対するDDoS攻撃が行われ、うち9箇所が一時影響を受けた(2002/10) ・SQL slammerワームが猛威を振るい、韓国では一時インターネットに障害が発生(2003/01) ・米鉄道の信号システムがコンピュータウイルスに感染、ワシントン周辺3路線で列車が停止したりダイヤが乱れるなどした(2003/08)	・大手銀行の合併に伴うシステム統合において、口座振替の未処理など大規模なシステム障害が発生、復旧に時間を要した(2002/04) ・インターネットバンキングのサービスがデータベースサーバの障害により全面的にダウン(2003/05) ・飛行計画情報処理システムがプログラムミスによりダウンし、200便近くが遅れるなど、航空ダイヤが全国的に混乱 (2003/03) ・注文件数の増加により証券取引所の売買システムや株価情報システムの処理が遅延(2003/07) ・航空路レーダー処理システムのトラブルでメインシステムを停止、国内便約130便に影響(2004/04) ・通信制御プログラムの不具合が原因で、金融機関同士のATMをネットワークで結ぶ「統合ATMスイッチングサービス」に障害発生。全国約20の金融機関のATMで他行カードを利用した取引が不可に(2004/01)

（報道発表資料を基に内閣官房にて作成。国名の明記がないものは国内事案。）

3．これまでの主な施策の流れ（重要インフラのサイバーテロ対策）

時期	施策内容
2000年　1月	ハッカー対策等の基盤整備に係る行動計画
2000年12月	重要インフラのサイバーテロ対策に係る特別行動計画 ○重要インフラとして以下を定義 情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）
2001年　3月	e-Japan重点計画 －高度情報通信ネットワーク社会の形成に関する重点計画－
2001年10月	サイバーテロ対策に係る官民連絡・連携体制について
2002年　3月	「重要インフラのサイバーテロ対策に係る特別行動計画」のフォローアップ等について
2002年　6月	e-Japan重点計画 －2002
2002年11月	「重要インフラのサイバーテロ対策に係る特別行動計画」に基づく取組みの推進について
2003年　8月	e-Japan重点計画 －2003
2004年　2月	e-Japan戦略Ⅱ加速化パッケージ
2004年　6月	e-Japan重点計画 －2004

4．第2分科会の立ち上げについて（案）

（1） 「情報セキュリティ基本問題委員会第２次提言」においては、国民生活及び経済活動の基盤となる重要インフラの情報セキュリティ対策のあり方（基本問題委員会第１回会合にて「重要インフラ防護のための中長期的政策と官民連携のあり方」としてテーマ設定されたもの）について提言を行うことを予定。

（2） したがって、今後、「第２分科会（重要インフラ対策検討分科会）」を立ち上げ、従来から「重要インフラのサイバーテロ対策」として行われている取り組みを踏まえながら、昨今の環境変化に応じた重要インフラにおける情報セキュリティ対策の強化の必要性及び具体策について検討を実施。その際、以下の視点に留意。

【視点１】重要インフラを取り巻く環境の変化と脅威についての再整理

重要インフラにおける様々な局面でのIT活用が進む中で、これを取り巻く環境の変化と脅威についての再整理が必要。

（例）複数重要インフラ間での相互依存性の増大
（例）サイバーテロ対策と非意図的な障害等の脅威に対する対策

【視点２】重要インフラにおける我が国の特性を踏まえた英知の共有等のあり方

我が国の重要インフラが持つ特性（元来から有する高い信頼性や自由化の進展度等も含む）を踏まえ、インフラ横断的に英知を共有するためのあり方についての検討が必要。

（例）事業継続性の確保における高い知見の共有のあり方
（例）早期警戒のための優先的な情報提供のあり方及び関係機関との連携のあり方
（例）その情報システムが最低限満たすべき技術的水準及び運用基準のあり方

（3） なお、第２分科会の検討に関しては、その特質上、重要インフラ所管省庁及び情報セキュリティ関係４省庁（情報セキュリティ対策推進会議及び情報セキュリティ専門調査会の庶務協力４省庁）等の協力を得ることが不可欠であり、適切な委員の選定などの立ち上げ段階から本委員会への報告の段階まで、当該省庁等と十分な相談をしつつ、検討を進めること。

5－1．参考～米国の事例①

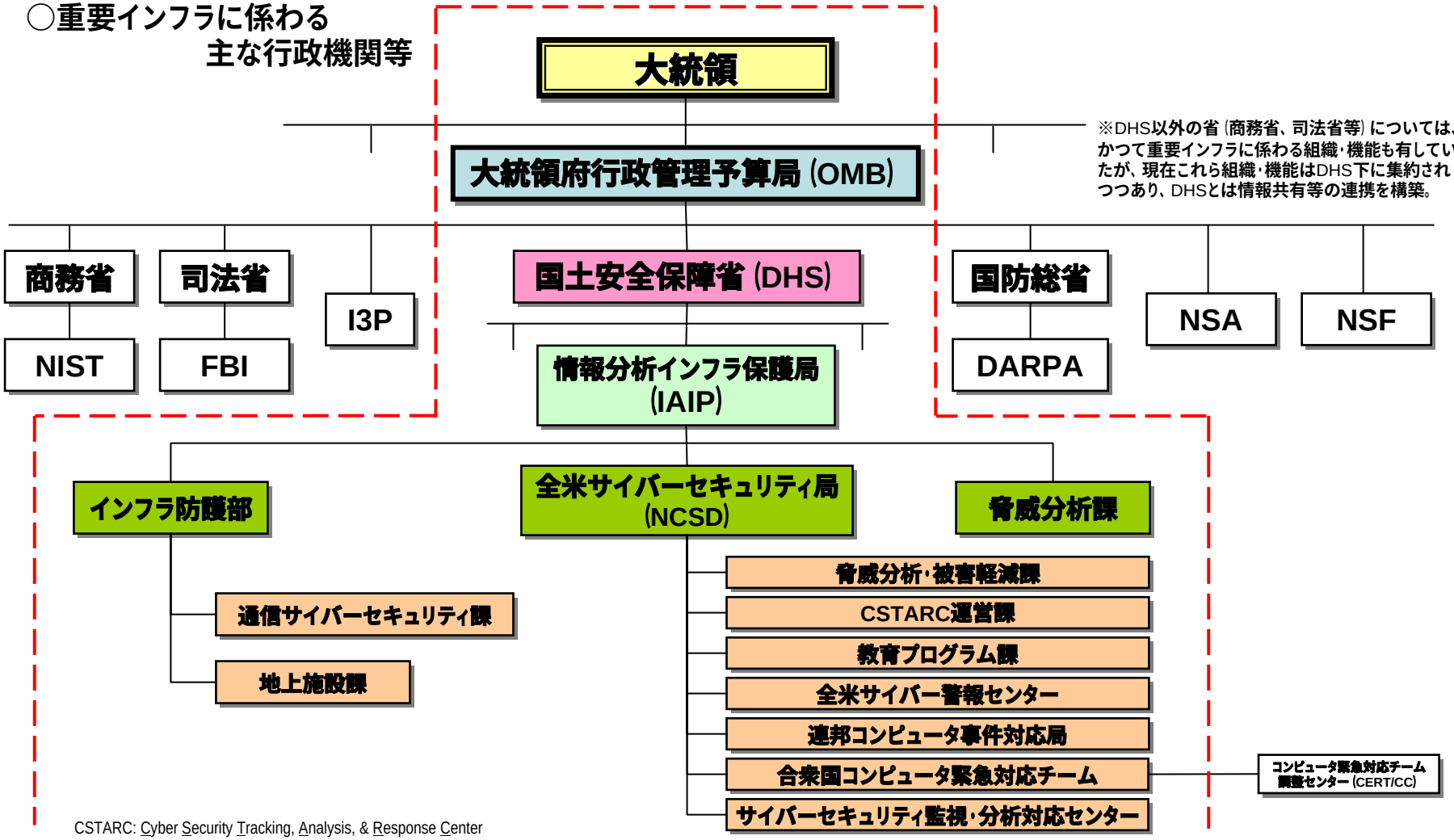
時期	事項
1995年4月	オクラホマシティ連邦政府ビル爆破事件
1995年6月	重要インフラ作業グループ（CIWG）設置
1996年7月	重要インフラに関するEO（Executive Order）13010発布
1996年7月	大統領重要インフラ防衛委員会（PCCIP）等設置
1997年10月	PCCIPによる最終報告
1998年5月	重要インフラ防護に関する大統領決定指令第63号（PDD63）発布
2000年1月	情報システム防護のための国家計画（Ver1.0）策定
2001年9月	NY世界貿易センタービルおよび国防総省で同時多発テロ勃発
2001年10月	国土安全保障局（OHS）および国土安全保障会議（HSC）設置
2001年10月	重要インフラに関するEO（Executive Order）13231発布
2001年10月	大統領重要インフラ防護会議（PCIPB）、全国インフラ諮問会議（NIAC）等設置
2003年1月	国土安全保障省（DHS）発足
2003年6月	内局の情報分析・インフラ保護局（IAIP）に全米サイバーセキュリティ局（NCSD）設置
2004年6月	重要インフラ国土安全保障情報ネットワーク（HSIN-CI）構築

5－2．参考～米国の事例②

	PCCIP	PDD63	情報システム防護のための国家計画 (Ver1.0)	EO13231
位置付け	■ 重要インフラに対する脅威と脆弱性のスコープと性質の評価 ■ 重要インフラ保護における法的問題及び、ポリシーに関わる問題の明確化 ■ 重要インフラを**物理的攻撃及びサイバー攻撃から保護**するための包括的な国家政策と導入戦略の推奨	■ PCCIPの推奨を利用した重要インフラ防衛の枠組みの規定 ■ 本枠組みに従い任命された関連政府機関は民間セクターと協力し、2005年までに指定された重要インフラに対し脅威となる事象に確実に対応	■ PDD63に基づいたサイバーセキュリティに関する最初の国家計画 ■ サイバー攻撃の回避･検知･対応およびサイバー攻撃からの早期回復に主眼	■ PDD63の活動の多くを引き継ぎ、重要インフラに対するサイバー上の脅威に焦点
内容	■ 重要インフラ所有組織と重要インフラ利用組織のそれぞれを対象にインタビュー調査を行い、意見を収集 ■ **情報通信、銀行･金融、エネルギー、物資輸送 (商品･ガス･石油･水等)、生活必須サービス (水道･緊急サービス･政府サービス)** の各セクタを対象とした研究グループを発足させ、それぞれのセクタに存在する脆弱性とそれに対する推奨策を提示 ■ 国家インフラ保全局 (CIAO),全国インフラ防護センター (NIPC), 情報共有分析センター (ISAC) の設置、研究開発の推進、および法律の整備を勧告	■ 議会との協調 ■ 重要インフラの所有者、運営者と政府で責任を分担 ■ 評価を頻繁に実施 ■ 経済的インセンティブの提供と慎重な規制の適用 ■ 全ての政府の権限、能力、人材の活用 ■ プライバシーの尊重 ■ 政府がインフラ保護の最善の達成法に関するモデルを担う ■ 民間セクタの自発的な参加の要請と緊密な連絡 ■ CIAO、 NIPC、国家インフラ防護委員会 (NIAC) の設立及び ISAC、重要インフラセキュリティパートナーシップ (PCIS) の発足	■ 国家の重要インフラ保護という視点において行政と連邦議会との密接な協力の提言 ■ 法の執行を含む民間および連邦政府機関の重要インフラ保護プログラムについて記述 ■ 連邦政府規模で実施中の政策の概略及び被害規模を縮小する能力を強化するための政策例の提示 ■ 特定の省における最も重要なインフラの把握、潜在的弱点の評価･修正、独自の重要システムに対する計画的攻撃を認知･回避するための手段 ■ 重要インフラ保護のための枠組み、防衛インフラの範囲、具体的方策等、国防総省が実施してきた連邦政府計画と民間部門に対する模範政策の詳細を提示 ■ 各政府機関は、安全保障、研究開発、技術･対策の標準化、人材育成、情報提供･分析等、様々な角度から重要インフラ保護に取り組む	■ 大統領重要インフラ防護会議 (PCIPB) の設置 ■ PCIPB の活動を補佐する10 の常設委員会の設置 ■ 全国インフラ保全会議 (NIAC) の設置 ■ 連邦機関の重要インフラの保護および政府･州･地方自治体･民間企業･学術機関の間での情報共有体制の確立 ■ インシデントのハンドリングならびに危機対応 ■ セキュリティプロフェッショナルの採用と育成のための戦略策定 ■ 研究開発における関係省庁との協調 ■ 国際インフラストラクチャの保護に向けた協調 ■ 重要インフラ保護に関わる法律の制定

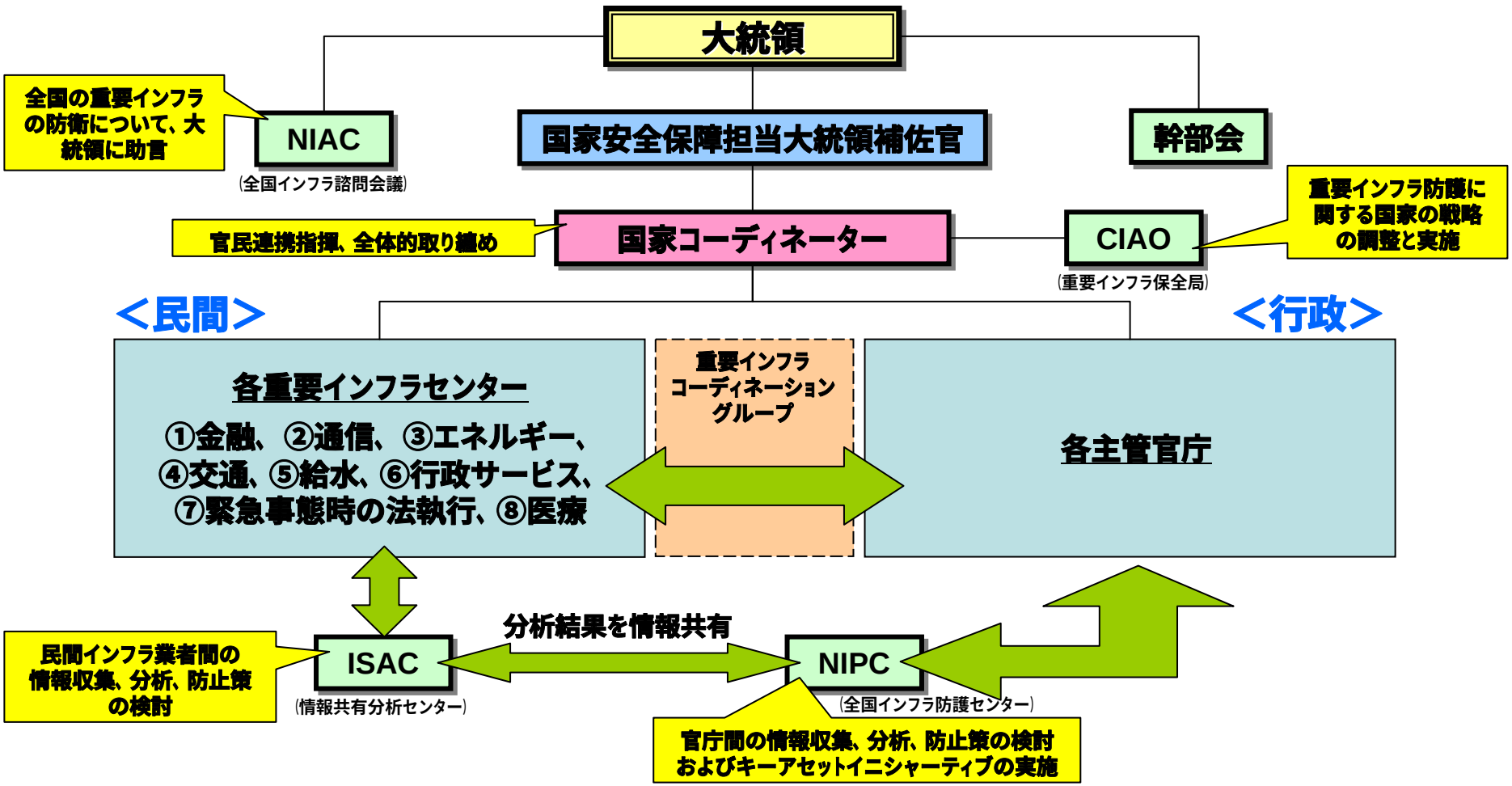
5－3．参考～米国の事例③

○重要インフラに係わる
主な行政機関等



CSTARC: Cyber Security Tracking, Analysis, & Response Center

5－4．参考～米国の事例④


大統領
全国の重要インフラの防衛について、大統領に助言
NIAC
（全国インフラ諮問会議）
国家安全保障担当大統領補佐官
幹部会
官民連携指揮、全体的取り纏め
国家コーディネーター
CIAO
（重要インフラ保全局）
重要インフラ防護に関する国家の戦略の調整と実施
＜民間＞
＜行政＞
各重要インフラセンター
①金融、②通信、③エネルギー、
④交通、⑤給水、⑥行政サービス、
⑦緊急事態時の法執行、⑧医療
重要インフラ
コーディネーション
グループ
各主管官庁
分析結果を情報共有
民間インフラ業者間の情報収集、分析、防止策の検討
ISAC
（情報共有分析センター）
NIPC
（全国インフラ防護センター）
官庁間の情報収集、分析、防止策の検討
およびキーアセットイニシャーティブの実施

6. 検討スケジュール (案)

- １０月２６日　第３回
  - 第２分科会活動方針承認
- １１月中～下旬
  - 第２分科会立ち上げ
- 来年１月中～下旬　第４回
  - 第２分科会の検討状況報告
- 来年３月末　第５回
  - 第２分科会の最終報告収受とその内容検討