資料5

重要インフラにおける情報セキュリティ対策の今後の方向性に係る論点整理

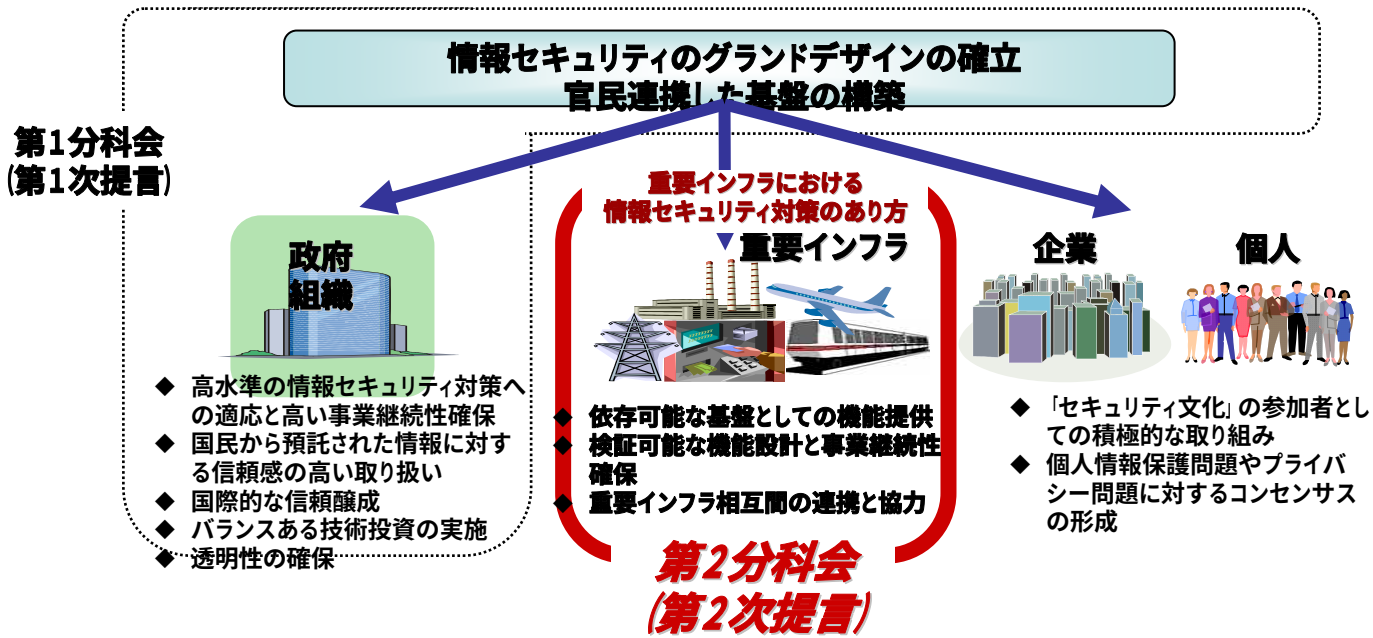
－　現在までの検討状況報告　－

平成17年1月31日
情報セキュリティ基本問題委員会
第2分科会

目次

はじめに　－　本論点整理の位置付け

- 当分科会は、「重要インフラにおける情報セキュリティ対策の強化」について検討を行うことを、情報セキュリティ基本問題委員会より付託され（下記図参照）、その具体的な方策を明らかにするべく検討を行っているところ。
- 昨年１２月９日に検討を開始し、以後、（1）全体の論点整理及び（2）重要インフラ事業者委員及び関係各省庁の取り組みについてのヒアリング等、現在までに４回の検討を行ってきたところ。
- 今回、当分科会としては、現在までの検討の状況を論点整理の形でとりまとめ、基本問題委員会に報告することとしたもの。
- 今後、当分科会としては、基本問題委員会からの指摘を受け、３月末までにさらに検討を加え、最終報告を行う予定。



第2分科会委員名簿

浅野正一郎（座長）	情報・システム研究機構　国立情報学研究所教授
石幡　吉則	電気事業連合会情報通信部長
板橋　功	財団法人　公共政策調査会第一研究室長
稲垣　隆一	弁護士
大場　満	東京地下鉄株式会社　鉄道本部安全・技術部長
雄川　一彦	日本電信電話株式会社　第二部門担当部長
喜入　博	KPMGビジネスアシュアランス株式会社　顧問
郡山　信	財団法人　金融情報システムセンター監査安全部長
小林　俊徳	社団法人　日本ガス協会技術部長
土居　範久	中央大学　理工学部教授
中尾　康二	KDDI株式会社　技術開発本部情報セキュリティ技術部長
廣川　聡美	横須賀市企画調整部情報政策担当部長
前川　徹	早稲田大学　国際情報通信研究センター客員教授 ／株式会社　富士通総研主任研究員
松尾　明	中央青山監査法人代表社員
三輪　信雄	株式会社　ラック代表取締役社長
森田　元	株式会社　日本航空IT戦略企画室部長
渡辺　研司	長岡技術科学大学　経営情報系助教授

（五十音順、敬称略）

1．重要インフラにおける情報セキュリティ対策の視点①

➢ 今回の検討の前提として、重要インフラにおける情報セキュリティ対策の視点を、以下のように再整理する必要があるのではないか。

(1) 重要インフラの位置付けと求められる対策

- 国民生活･経済活動の根幹であるサービスを提供する基盤。
- したがって、重要インフラの提供するサービスについては、その維持と迅速な復旧が確保されることが最重要。
- 具体的には、現実のサービスの停止又は機能の低下等を引き起こす原因となる障害について、①未然防止、②拡大防止と迅速な復旧、③要因等の分析･検証による再発の防止の3つの側面全てについて、万全の措置が講じられることが不可欠。その際、適切な官民の役割分担が必要。

(参考) 重要インフラの定義例

「物理的施設、物資供給システム、情報技術、情報通信ネットワークなど、ある期間にわたって破壊、機能の低下、利用不可能な状態にされた場合に、国家の社会及び経済活動に多大なる影響を及ぼす恐れがあり、また防衛及び安全保障を確保するための国家の能力に影響を及ぼしかねないインフラストラクチャー」

(出所：豪州「重要インフラ防護に関する国家指針~Trusted information sharing network for critical infrastructure protection」平成16年3月)

1．重要インフラにおける情報セキュリティ対策の視点②

(2) 重要インフラにおける情報セキュリティ対策の視点

- 重要インフラにおいて、情報技術 (IT) が果たす役割が近年、急速に拡大。この傾向はいわゆる制御系においても同様。
- 各重要インフラの情報技術 (IT) の機能不全が、現実のサービス提供の停止または機能低下等の障害 (「情報技術 (IT) の機能不全が引き起こす障害」) の原因となり得るという認識は重要。

【「情報技術 (IT) の機能不全が引き起こす障害」の想定例】

例1) 特定の政治的意図を持った集団が、サイバー攻撃により証券取引システムを数分間停止させ、それにより株式取引による期待損失が数千億円に膨らむ状況が発生。

例2) 銀行システム再編に伴う大規模な統合システムで障害が発生し、現金支払い、公共料金等口座振替、カード決済等が長期間にわたって出来ない状況が発生。

例3) 大規模台風の来襲により、地方自治体が有するコンピュータルームが浸水し、情報化されている行政サービスの復旧に多大な時間がかかり、長期にわたり住民サービスが受けられない状況が発生。

- この観点から、重要インフラにおける情報セキュリティ対策の強化は必須。1)未然防止、2)拡大防止と迅速な復旧、3)要因等の分析・検証による再発の防止、の3つの側面全てについて万全の措置が講じられるべきとの視点が出発点。
  - なお、重要インフラにおける情報セキュリティ対策として、個人情報漏えいに係る対策も重要課題であるが、ここで検討すべきは、現実のサービス提供の停止または機能低下等の障害に係る対策。したがって、重要インフラにおける個人情報漏えいに係る対策については、他の民間企業等における対策のあり方と同時に検討することが適当 (第3分科会の検討課題として想定)。

2．重要インフラにおける情報セキュリティ対策につき検討すべき側面

- 1．の視点を前提とすると、重要インフラにおける情報セキュリティ対策について、以下の3つの側面から検討する必要があるのではないか。

(1) 障害の未然防止

- 重要インフラにおいて、まず、「情報技術（IT）の機能不全が引き起こす障害」が発生しないよう、未然に障害を防止する措置が必要。
- そのためには、①重要インフラのサービスの維持に資する情報の適切な収集・提供・共有、②広く「情報技術（IT）の機能不全が引き起こす障害」を未然に防止するための対策の実施、③障害の分類や事業継続計画の策定等が必要。

(2) 障害の拡大防止・迅速な復旧

- (1) の未然防止が最も重要であることは言うまでもないが、万が一障害が発生した場合でも、その障害の拡大を防止し、迅速な復旧を図ることが必要。
- そのためには、①重要インフラのサービスの維持・復旧に資する情報の適切な収集・提供・共有、②広く「情報技術（IT）の機能不全が引き起こす障害」を局限化し、迅速に復旧するための対策の実施が必要。

(3) 障害の要因等の分析・検証による再発の防止

- また、万が一障害が発生した場合には、(1) (2) に継続的に役立てていくとの観点を前提に、その障害の要因等を分析・検証することが必要。

3．3つの側面を検討するにあたっての前提（対象範囲等の見直し）①

- 2．で示した3つの側面を検討するにあたり、「情報技術（IT）の機能不全が引き起こす障害」の範囲及び「重要インフラ分野」について、「重要インフラのサイバーテロ対策に係る特別行動計画」（平成12年12月情報セキュリティ対策推進会議決定）が対象とした範囲を見直す必要があるのではないか。

（1）「特別行動計画」が想定したリスク

- 平成１２年以降の「特別行動計画」に基づく政府の取り組みは、情報通信ネットワークや情報システムを利用した、国民生活や社会経済活動に重大な影響を及ぼす可能性がある全ての攻撃を対象。
- 重要インフラとして、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）の7分野を設定（新たな脅威等を踏まえ適宜見直しを行うことを明示）。

3．3つの側面を検討するにあたっての前提（対象範囲の見直し）②

（2）想定するリスクの見直しの方向性

- サイバー攻撃に加え、人為的なミス等の非意図的要因に起因するものや、地震、津波などの自然災害などの多種多様なリスクに対する総合的な対応が必要であり、それに相応しい体制の構築に向けた検討を行っていくべきではないか。
  - 従来から人口に膾炙している「サイバーテロ」の概念に関しては、そもそも「サイバーテロ」の脅威としていかなるものがあり得るかという点に関し、継続的に研究する機能が必要ではないか。
  - また、従来から、「重要インフラのサイバーテロ対策」と呼んできたところであるが、「情報技術（IT）の機能不全が引き起こす障害」の防止等を図るものであることを表す用語として、新たな用語を設定するべきではないか。

（3）対象事業及び分野の見直しの方向性

- 国民生活・経済活動の根幹であるサービスの維持と迅速な復旧の確保を図るとの大目的を前提とすると、「特別行動計画」が設定した7分野について、既存7分野の対象事業の見直しや対象分野の見直しを行うべきではないか（ex.政府・行政サービスの範囲の見直し／医療、水道等の追加等）。
  - なお、この点については、分科会の委員の中でも、「既存分野に対しての重点化の視点から、対象範囲を拡大すべきでない」との意見と、「より、国民生活を直視した判断から対象分野を拡大すべき」との意見の両論がある。

4．3つの側面を実現するための具体策の方向性①

➢ 2．で示した3つの側面を実現するためには、3．で示した範囲の見直しを前提とし、以下の問題点を解決すべく、現在の体制等の見直しが必要なのではないか。

(1) 現在の問題点

- 「特別行動計画」に基づく、現状の官民の連絡・連携体制等の下では、対象が「重要システムにおける重大な障害あるいはサイバー攻撃の検知と被害」に限定されており、重要システムの影響については、個々の重要インフラ事業者が自主的に判断することになっている。
- しかし、各重要インフラにおける情報システムの利用が進展し、重要インフラ相互の依存がサービス維持のために必須となっている状況の下で、
  (1)個別事業分野又は各重要インフラ事業者が単独で状況を把握しても、障害の未然防止、拡大防止等のためには不足。
  (2)相互依存性に基づくリスク評価による適切な優先度設定等も不足。

(2) 今後の方向性

①重要インフラ横断的な状況把握機能の強化

- 各重要インフラにおける情報システムの利用が進展し、重要インフラ相互の依存がサービス維持のために必須となっている状況を踏まえ、我が国全体として重要インフラの対策を向上させていく観点から、重要インフラ間の相互依存性解析等を行い、横断的な状況把握機能を強化すべきではないか。

4．3つの側面を実現するための具体策の方向性②

②重要インフラのサービスの維持･復旧に資する情報の適切な収集･提供･共有

- 未然防止の観点から、早期警戒情報提供･共有の枠組みを強化し、事業者個別の自主保安、障害の防止能力向上を促進していくべきではないか。
- 障害の拡大防止、迅速な復旧の観点から、障害が発生した場合には、当該障害が違法行為（過失を含む）による場合があることも視野に、警察への通報、捜査への協力等が重要であることも念頭におきつつ、現在の「特別行動計画」に基づき連絡の対象となっている「情報」の充実･質の向上も含めた官民の連絡･連携体制の強化を図るべきではないか。
- 障害の要因等の分析･検証による再発防止の観点から、1)分析のための情報収集のあり方に関する検討、2)重要インフラ間での分析･検証結果の共有、3)官民の連絡･連携体制の強化という視点等が重要ではないか。
- なお、この際、1)①の相互依存性解析の結果を踏まえるという視点、2)平時から非常時を意識した対応を行うという視点、3)関係機関が現在有する機能との連携を図るという視点、4)情報技術（IT）によって担われた社会的機能及び権利利益の回復という視点、5)情報共有の担い手とその役割の明確化を行うという視点等が重要ではないか。

③総合的な対策の強化

- 「情報技術（IT）の機能不全が引き起こす障害」に総合的に対応できるよう、各重要インフラ事業者における安全基準の作成や対策の促進を実施することが重要ではないか。
- なお、この際、1)①の相互依存性解析の結果を踏まえるという視点、2)重要インフラ所管省庁の対応能力を向上させるとの視点、3)各府省庁が有する情報セキュリティに関する機能や取組みを最大限に活用するという視点等が重要ではないか。

（参考1）重要インフラ事業者委員に対するヒアリング結果の概要整理①

1．個々の重要インフラにおける情報セキュリティ対策及び「IT事故」（仮称）注経験等について

- 各事業者とも、情報セキュリティ対策を、制御系と情報系（業務系／事務処理系）とに分けて実施。
- 制御系については、外部ネットワークとの分離による防護を基本とし、対策を入念に行っている事業者が太宗。
- 情報系（業務系／事務処理系）については、情報セキュリティ対策を積極的に実施しているものの、情報漏洩や内部要因による障害発生などのリスクを強く意識している事業者が太宗。
- 「IT事故」（仮称）の経験については、サイバー攻撃の被害経験は少ないが、地震等の自然災害によるもの、内部的なワーム感染などの経験の指摘もあり。
- 「サイバーテロを想定した演習」については、業界として取り組んでいる事例がある一方、災害時等を想定した一般的な訓練の一環として行っているとの事業者が太宗。また、重要インフラ間の横断的な演習の実施が有効との事業者もあり。

注：ここでは、サイバー攻撃に加え、情報資産に係るその他のリスク（コンピュータウイルス、不正アクセス、災害などの外部要因、従業員及び委託先の過失・犯行、システム障害などの内部要因）に起因する事件や事故を「IT事故（仮称）」と定義する。なお、情報資産とは、重要インフラ事業者にとって価値を有する情報そのもの（企画、運転計画や営業などの情報、稼働状態逐次情報、緊急時対応情報、バックアップデータ、顧客情報、知的財産などのデータベース、資料など）と、その情報を可用化する環境（ソフトウェア（アプリケーション、システムソフトウェア、ユーティリティ）、ハードウェア（コンピュータ装置、通信装置、メディアなど）等）を指している。

(参考1) 重要インフラ事業者委員に対するヒアリング結果の概要整理②

2. 重要インフラにおける相互依存性及び事業継続性の確保について

- 多くの事業者が、特に電力事業に対し、依存性が高いと認識。事業継続性の確保のために、UPS装置の設置やバックアップ電源の確保等の対策を行っている事業者が多い。更なる対策として、手動操作（運転員）による対応を手当てしている事業者もあり。
- 災害等が起こった場合に、移動電源車の配備計画や電源復旧計画等の情報が共有されていると、自らの事業の迅速な復旧に役立つとの指摘もあり。
- 情報通信事業への依存性の指摘もあり、事業継続性確保のために、自営回線の確保による対応を行っている事業者がいる一方で、NTT等との契約による回線の多重化で対応している事業者もあり。
- 「地域単位」で重要インフラ相互の情報共有等を行うことは、全体として事業の継続性の向上を図るために有効であるとの指摘あり。

3. 汎用システムの利活用度について

- 基本的に、特に制御系のシステムについては、汎用システムではなく独自システムを構築している事業者が太宗。一方で、1）部分的に汎用システムを活用している事業者が既に存在するとともに、2）今後、経営効率化の観点から、独自のシステムから汎用システムへの切り替えの必要性についての認識を指摘する事業者もあり。
- 情報系（業務系／事務処理系）については、インターネットの活用も含め、汎用製品によるシステム構築を行っている事業者が太宗。

（参考1）重要インフラ事業者委員に対するヒアリング結果の概要整理③

4．想定する脅威の範囲について

- 自然災害、障害、不正行為に至るまで、サイバー攻撃以外にも様々な脅威を想定している事業者が太宗。
- 外部からの攻撃等の外部的脅威に対しては、物理的入退室管理や外部ネットワークとの分離を理由に、そのリスクは小さいと認識している事業者が太宗。
- 内部的脅威に対しては、実際に事故を経験している事業者もあるとともに、制御系のシステムに対する脅威も含め、常にそのリスクは起きる可能性があると認識している事業者が太宗。

5．重要インフラにおける早期警戒情報等の必要性について

- ソフトウェアの脆弱性情報等についての「早期警戒情報」については、外部ネットワークとの分離を理由に、その必要性は小さいとする事業者がある一方で、可能な限り早期に情報を入手することが対策の実施上有効であるとする事業者もあり。
- 情報の信頼性と重要度の評価、情報の早期公表によるリスク評価等についての検討が必要であるとの事業者もあり。
- 「早期警戒情報」ではないが、プラント系システムのトラブル事例等整理された情報提供が行われることは有効との事業者もあり。
- 「早期警戒情報」に限らず、重要インフラ事業者間、自治体間、同一地域等において、情報の共有のみならず、脅威や対策を評価する仕組み、対策を助言する仕組みが重要であるとの指摘もあり。

(参考2) 検討の経緯

12月　9日　　第1回会合

本分科会での討議について

12月24日　　第2回会合

重要インフラ事業者委員／各府省庁からのヒアリング①

→金融、情報通信、自治体（3分野）

→防衛庁、法務省

1月12日　　第3回会合

重要インフラ事業者委員／各府省庁からのヒアリング②

→鉄道、航空、電力、ガス（4分野）

→警察庁、総務省、経済産業省、国土交通省

1月21日　　第4回会合

第4回基本問題委員会への中間報告案の検討