



**「重要インフラの情報セキュリティ対策に係る行動計画」の見直し
(事務局案説明資料)**

個別論点(第1回)

2008年 6月 4日
内閣官房 情報セキュリティセンター
(NISC)

今回は、「4-2 行動計画の基本的枠組みに関する事項」を中心に検討し、採りうる方向性を確認したい
 なお、「4-1 本委員会の議論等を通じて認識された課題」については、全体にかかる論点であるため、今回のみならず、次回以降も随時議論し、最終的に基調となる方向性を設定したい

検討テーマ(論点整理における項目)	現行動計画における項目	該当ページ
4-1 本委員会での議論等を通じて認識された課題	(全体)	p2
4-2 行動計画の基本的枠組みに関する事項		
対策の目的(目標)、視点	1 目的と範囲	p3 ~ 5
「重要インフラ分野」の分類、位置づけ 枠組みの柔軟化 「重要インフラ事業者等」「重要システム」	2 重要インフラの定義と対象 別紙1 各重要インフラ分野において対象となる重要システム等	p6 ~ 11
IT障害への脅威の例示	2(2)ア IT障害への脅威の例示	p12
他の取組みとの関係の整理	1 目的と範囲	p13
評価の手法	8(1) 進捗状況の評価・検証	p14
4-3 安全基準等の整備		
4-4 情報共有体制の強化		
4-5 相互依存性解析・分野横断的演習		
4-6 その他		
自由討議		

今回の議論にて積み残った内容は、引き続き次回以降にて議論を継続

行動計画の見直しのとりまとめに際して、最終的に以下の点について採るべき方向性を示せるよう、個別の論点の検討を行う(資料4 見直しの背景と進め方 p13を再掲)

各重要インフラ分野において、ITへの依存度(ITの機能不全とサービス低下の距離感)、ITの観点での他分野との相互依存性などは様々である。それに応じた各分野における取組みにも多様性が存在する。

全分野・全事業者に一律の対策を求め平均を底上げするか、個別の進んだ対策を伸ばすか

情報セキュリティ対策を考える際には、経営(コスト配分・サービスの維持レベルなど)やコンプライアンス、内部統制の視点も踏まえるべき要素の一つである。

対策の対象はITのみに限定するか、ITを含めた経営全体か

重要インフラ事業者等の立場から見ると、「個々の利用者(顧客)」へのサービス提供と「公益」の観点から求められる対応の2つの側面があり、両者は必ずしも常に一致するものではない。

事業者等の自発的な取組みに重点をおくか、義務的な取組みに重点をおくか

IT障害から重要インフラを防護する観点からは、障害の未然防止だけでなく、障害発生時に影響を最小限に抑えるための対応(早期対応、応急対応など)も重要である。

緊急時対応を国や他事業者と連携して行うのか、事業者独自の取組みに任せるのか

個々の重要インフラ事業者等による情報セキュリティ対策については向上が進んでいるものと考えられるが、障害(リスク)の発生時の情報や、「経験」から得られる知見の共有については、今後の一層の取組みについて、検討を進めるべきである。

どのような知見を共有対象とすべきか

IT障害に至らない事象(ヒヤリ・ハット等)も重視すべきではないか

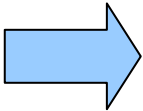
対策の目的(目標)、視点

【重要整理事項】

「重要インフラにおけるIT障害発生ゼロ」よりも適切な目標はあるか

- 第1次情報セキュリティ基本計画において、2009年度初めの目標として、以下が挙げられている
 - 政府機関:すべての政府機関において、政府機関統一基準が求める水準の対策を実施
 - 重要インフラ:重要インフラにおけるIT障害の発生を限りなくゼロに
 - 企業:企業における情報セキュリティ対策の実施状況を世界トップクラスの水準に
 - 個人:「IT利用に不安を感じる」とする個人を限りなくゼロに
- 現行動計画において以下の目的が挙げられている
 - 重要インフラ事業者等のサービスの維持
 - IT障害発生時の迅速な復旧等の確保

【事務局案】

- 
- ・ 基本計画検討委員会より、情報セキュリティ基本計画の全体的な視点からのインプットが想定されるため、その内容を受けてから後日検討
 - ・ 究極的な目標である「基本理念」と、合理的な達成水準を具体化した「政策目標」を分けて議論
 - ・ ひとまず現行基本計画の目標を「基本理念」、現行動計画の目的を「政策目標」として、それぞれ前提において議論

「未然防止」「拡大防止」「再発防止」のバランスをどう考えるか、いずれかに重点をおくべきか

- 現行動計画において上記3つの観点が書かれているが、次の一手を進めるためには行動計画にて予め重点をおくべき点を明らかにすべきという考え方がある
 - 一方、情報提供等を受けて対策する側が判断すべきこととして、特に重点を置くべきではないという考え方もある
- 以下2つの対応が考えられる
 - 案1:全てに取り組む
 - 案2:いずれかに重点をおく
 - 案2 - 1:4つの柱の施策毎に必要性等を踏まえて判断する
 - 案2 - 2:行動計画全体にかかるテーマを定める

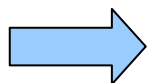


【事務局案】

- ・ 個別施策における具体的な取組みの検討を踏まえて議論することが望ましいため、後日検討

個人情報保護の観点をどう位置づけるべきか

- 一般に個人情報保護法において「個人情報保護取扱事業者」には、個人情報の適正な取扱いの確保が求められている
- 現行動計画は、「重要インフラ事業者等の自主的な対策について示す」こととしている



【事務局案】

- ・ 個人情報保護法が制定されていることを踏まえると、法令遵守の観点から当然対応が必要なものであり、重要インフラ事業者向けとして特に行動計画において求めるべきことは現時点では少ないのではないか

現行動計画「1 目的と範囲」より(抜粋)

- ・ (IT障害)から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重要インフラを防護し、重要インフラ事業者等の事業継続への取組みを強化するための取ることが望ましい**重要インフラ事業者等の自主的な対策**について示す

「重要インフラ分野」の分類、位置づけ

【重要整理事項】

現在の10分野の分類や位置づけは適切か、実態に即し見直し(分割・追加等)の必要はないか

- 諸外国における重要インフラの分類(次ページ)等を参考に、見直し(分割・追加等)が望まれる分野はないか
例) クレジットカード会社(消費者信用)、ITベンダー(情報技術) 等
- 現在の10分野とは別に、協力を求めるべき業界があれば、何らかの形で位置づけることも考えられる
- 現在の10分野についても、ITへの依存度等に応じて分類や位置づけを何段階かに整理することも考えられる
- 重要インフラの定義そのものについても、必要に応じて見直しを検討することが考えられる

【事務局案】

- ・ 新たな分野を加えるのではなく、現在の10分野を踏襲しつつより内容を充実させてはどうか

現行動計画「2 重要インフラの定義と対象」より(抜粋)

- ・ 重要インフラとは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの」と定義
- ・ 当面の対象分野は、「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)」、「医療」、「水道」、「物流」の10分野

<参考> 諸外国における重要インフラの分類



国名	我が国10分野との対応関係(各国における名称)										
	情報通信	金融	航空	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	その他
オーストラリア	通信	銀行・金融	交通		エネルギー		-	健康	水道	-	食料供給、緊急時対応、名所と公の集会
カナダ	通信・情報技術	金融	交通		エネルギー・設備		政府	公衆衛生	水道	-	食料、製造、安全保障
フランス	通信	銀行・金融	交通システム		エネルギー・電力、原子力発電所		-	公衆衛生	水道供給	-	化学・バイオ産業、公安秩序
ドイツ	情報通信・情報技術	金融・保険	交通・運輸		エネルギー		行政・司法	-	-	-	サービス、危険物、その他
韓国	情報通信、メディアサービス	金融サービス	交通		ガス・エネルギー		電子政府・国家行政	-	-	-	緊急時対応、国家防衛
シンガポール	情報・通信	銀行・金融	陸上・航空・海上輸送		エネルギー		-	健康	水道	輸送	極めて公的な場所、注目を集めるイベント
ロシア	情報・通信システム、マスメディア	クレジット・金融	交通		エネルギー		連邦政府関連情報	-	-	-	国内産業、軍事
スウェーデン	情報通信システム、インターネット	金融システム	航空管制	-	-	-	-	-	水道・輸送・産業における監視・制御	-	国家指令システム
英国	通信	金融	交通		エネルギー		政府	衛生	水道	-	食料、緊急時対応
米国 KR(Key Resources: 重要資産)含む	通信	銀行・金融	交通		エネルギー		政府施設	公共衛生・医療	水道	郵便・宅配	農業・食料、化学、商業施設、ダム、防衛産業基盤、緊急時対応、情報技術、国家象徴・モニュメント、核物質取扱・廃棄設備

重要情報インフラ防護(CIIP)の観点に限らない点注意

(出典)CIIPハンドブック2006 [http://cipp.gmu.edu/archive/5 IntlCIIPHandbook 2006 Vol I Switz.pdf](http://cipp.gmu.edu/archive/5%20IntlCIIPHandbook%202006%20Vol%20I%20Switz.pdf) 及び各国ホームページ

枠組みの柔軟化

【重要整理事項】

ITへの依存度、インターネットとの接続(直接・間接)、維持すべきサービスレベル、社会や利用者への影響の度合い、分野間の依存関係、事業規模等を踏まえ、対策の優先度を分野や事業者等单位などで柔軟に考えるべきではないか

- 現行動計画では「重要インフラ」の定義はあるが、対象とするサービスについての利用側と提供側のギャップが存在している
- 多くの論点についての方向性を整理する軸として、まずは行動計画の対象とする重要インフラの「サービス」を定義し、その範囲と水準を洗い出す必要があるのではないか

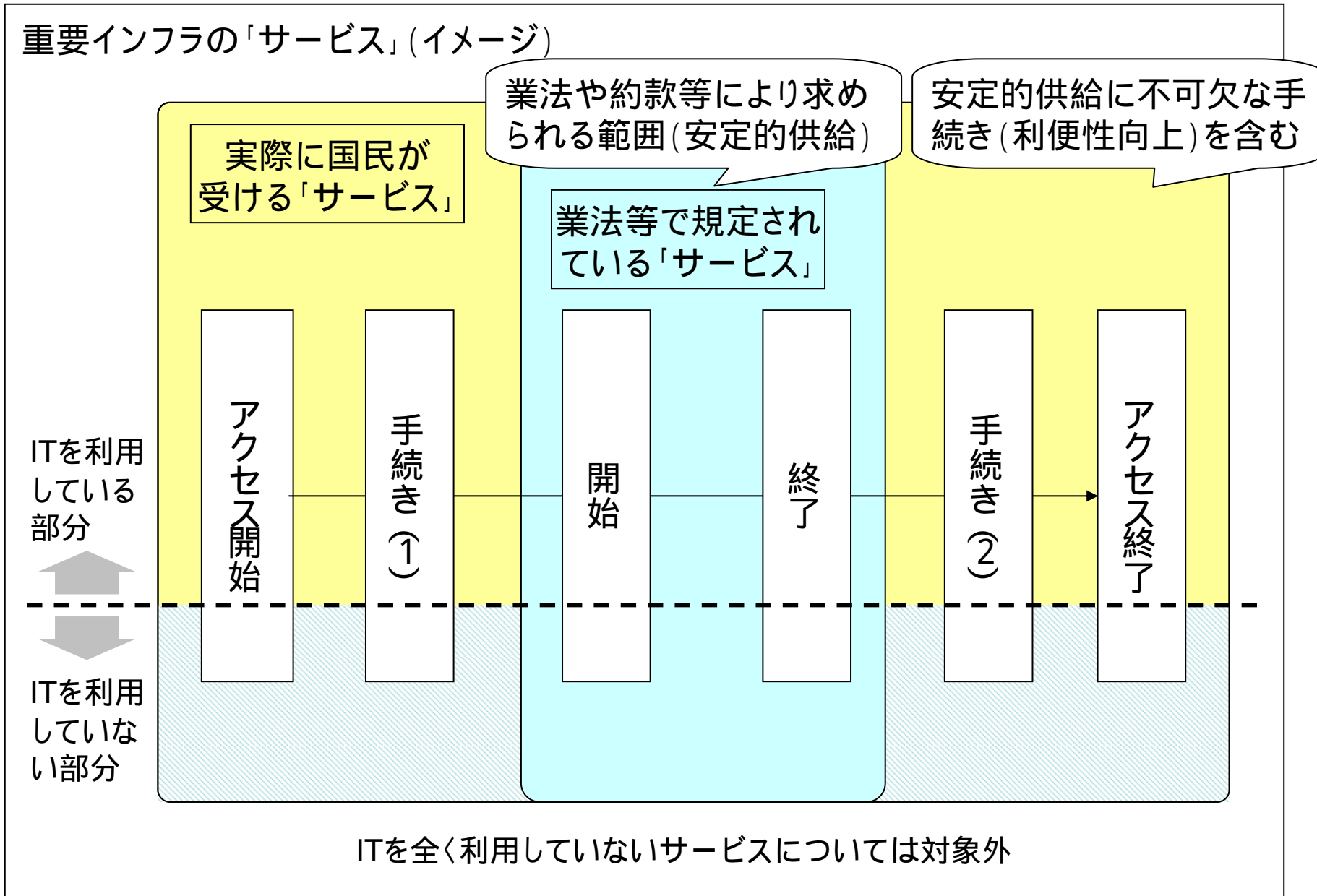


【事務局案】

- ・サービスのITへの依存は、時代とともに変化することを踏まえ、現時点でのITへの依存度に拘らず、一旦広くサービスを洗い出してはどうか
- ・従来より事業者等(提供側)が対策を取っている業法等で規定されている「サービス」に限らず、その周辺サービスを含め実際に国民(利用側)が受ける「サービス」を対象としてはどうか
- ・防護対象とする「サービス」を具体化して、行動計画に盛り込むこととしてはどうか

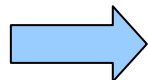
現行動計画「1 目的と範囲」より(抜粋)

- ・重要インフラ事業者等のサービスの維持及びIT障害発生時の迅速な復旧等の確保を図るため、内閣官房を中心とした政府及び各重要インフラ分野において実施することが望ましい施策を既存の法令、防災計画等の枠組み等との整合を図りつつ具体化



「分野」単位よりも「事業者等」単位の方が進捗しやすい事項もあるのではないか

- 現行動計画は、「重要インフラ事業者等の自主的な対策について示す」こととしている
 - 分野単位で考えると、事業規模の小さい事業者等を含め、全事業者が対応しうる最低限の対策になりがちではないか
 - 分野内のいわゆるトップランナー的な事業者にて行われる取組みも含めるべきではないか
- 個別施策の中で検討するという考え方もある



【事務局案】

・対策の優先度を分野や事業者等单位などで柔軟に考え、分野の一部の事業者等がとりうる対策事項についても、行動計画の取組みとして検討してはどうか

「重要インフラ事業者等」「重要システム」

【重要整理事項】

行動計画の別紙1に掲載されている「重要インフラ事業者等」や「重要システム」について、実態や利用者の観点に即した修正の必要はないか

- 一般企業としてではなく、重要インフラとして位置づける事業者の範囲をどこにおくか
 - 分野によって事業者を一部の範囲に限定してよい場合があるのではないか
 - 事業者のサービス停止・機能低下の影響が多方面に及ぶ場合、当該事業者が対象事業者に含まれているか
 - 例えば判断基準としては、市場占有率が一定以上ある場合や指定公共機関等として公共的な役割が求められている場合などが考えられないか
- 2007年度の指針の見直しでは、「安全基準等の適用対象とならないシステムも含めて、我が国の国民生活や社会経済活動に影響をおそれが生じる障害が発生」していることが明らかとなっている
 - 行動計画の対象範囲は、例示された重要システムに限定できないのではないか（例えば、バックオフィスのシステム障害がサービスへ影響する場合はないのか）



【事務局案】

・実態や利用者の観点に即した修正に加え、論点整理に対するこれまでの方向性を踏まえ、サービスの観点を切り口として、別紙1の項目立てを見直してはどうか

現行動計画 別紙1 「各重要インフラ分野において対象となる重要システム等」より(抜粋)

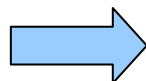
分野	情報システムの障害、不正な処理などの脅威・危険性	対象となる重要インフラ事業者等	対象となる重要システム例

IT障害への脅威の例示

【重要整理事項】

現在の脅威の例示は、実態に即して適切か

- 各事業者の取組みにおいて、脅威の例示は適切であったと評価できるか
 - 昨今の社会状況等を踏まえ、新たに加えるべき脅威はないか
例) パンデミック(新型インフルエンザの世界的流行)
- 各事業者毎に脅威に対する対策が可能か、あるいは分野横断的な対応が必要になるか



【事務局案】

- ・対応主体別の分類や優先付けをすべきではないか
- ・個別事業者で対策可能なものと、個別事業者では対策不可能なものを峻別して扱うべきではないか
- ・分野横断的な対応が必要な脅威については、行動計画における官民連携の枠組みを最大限活用して具体的な対応を進めるべき

現行動計画「2 重要インフラの定義と対象」より(抜粋)

サイバー攻撃によるIT障害への脅威

不正侵入、データ改ざん・破壊、不正コマンド実行、ウィルス攻撃、サービス不能攻撃(DoS: Denial of Service)、情報漏えい、重要情報の搾取 等

非意図的要因によるIT障害への脅威

操作・設定ミス、プログラム上の欠陥(バグ)、メンテナンス不備、内部・外部監査機能の不備、外部委託、マネジメントの欠陥、内部不正 等

災害によるIT障害への脅威

地震、水害、落雷、火災等の災害による電力供給の途絶、通信の途絶、コンピュータ施設の損壊等、重要インフラ事業者等におけるITの機能不全

他の取組みとの関係の整理

【重要整理事項】

情報共有や連携の部分で、防災担当機関や事案対応省庁、その他関係機関の取組みと競合する部分はあるか、補完しあえる部分はどこか

- 分野横断的演習において、「事案対応」の観点からの課題検証について」として個別に論点があげられている
- 基本計画検討委員会においても、他の関係機関との連携について検討の予定がある

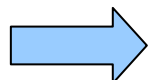


【事務局案】

・個別施策における具体的な取組みの検討や基本計画検討委員会での検討を踏まえて議論することが望ましいため、後日検討

個々の事業分野における業法との関係で競合する部分はあるか

- 他分野の事業継続のために、自分野の業法で規定される以上の対応を求められる場合があるのではないか



【事務局案】

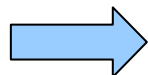
・個別施策における具体的な取組みの検討を踏まえて議論することが望ましいため、後日検討

評価の手法

【重要整理事項】

目標、評価指標、対策の進捗度合いの把握方法等について、どう設定すべきか

- 現行動計画では、プロセス評価(目標に対する実施状況の把握)を中心に実施
 - 上記に加え、2007年度は補完調査(参考となるデータの補足、具体的事例の検証)を実施
- 現行動計画は、「重要インフラ事業者等の自主的な対策について示す」こととしている
- 行動計画の取組みの内容を固めることが先決であるという考え方もある



【事務局案】

・基本計画検討委員会より、情報セキュリティ基本計画の全体的な視点からのインプットが想定されているため、その内容を受けて後日検討