

平成 16 年度内閣官房
情報セキュリティ対策推進室委託調査

「情報セキュリティの基本問題に係わるテーマに関する調査研究」

報 告 書

【概要版】

株式会社 日立製作所

1. はじめに	3
1.1. 背景	3
1.2. 目的	3
1.3. 本報告書の取り扱う範囲	3
2. 重要インフラ概要	4
2.1. 重要インフラの定義	4
2.2. 重要インフラのサービス提供の維持について	4
2.3. 重要インフラを支える情報システムの概要	5
3. 重要インフラの機能継続に係わる脅威と対策及びその課題	7
3.1. 重要インフラに対する脅威	7
3.2. 重要インフラに係わる脅威に対する対策	10
3.3. 重要インフラ間の相互依存性とその問題点	12
3.4. 重要インフラ防護に係わる現時点の課題	14
4. 政府の政策・施策としての3年後の理想像	17
4.1. 情報共有政策の推進	18
4.1.1. 米国におけるISACの現状	18
4.1.2. 国内における情報共有の現状	23
4.1.3. 海外の重要インフラ防護機関との連携	24
4.1.4. 今後求められる情報共有政策のあり方	26
4.2. 重要インフラ防護のためのセキュリティ演習	30
4.2.1. セキュリティ演習の形態	31
4.2.2. 国内の状況	33
4.2.3. 海外の状況	35
4.2.4. 今後求められる演習のあり方	50
4.3. セキュリティに係わる標準策定の推進	51
4.3.1. 国内の状況	51
4.3.2. 海外の状況	52
4.3.3. 今後求められるセキュリティに係わる標準のあり方	57
5. 国家情報セキュリティセンター（仮称）の位置付けと役割に係わる弊社の提言	58
5.1. 国家情報セキュリティセンター（仮称）の位置付け	58
5.1.1. 重要インフラ事業者に対するセキュリティパスの強化	59
5.1.2. 重要インフラ分野の拡大と相互依存性を考慮した階層化	59
5.1.3. 国家情報セキュリティセンター（仮称）への評価機関の設置	59
5.2. 国家情報セキュリティセンター（仮称）に求められる役割	60
5.2.1. 情報共有を前提とした情報収集・分析技術の向上	60
5.2.2. 重要インフラに係わる公開情報の政府による監視	60
5.2.3. 緊急時対応演習の実施とそれに伴う体制整備	61
5.2.4. 「セキュリティのあり方」に関する研究の促進	62

6. 参考文献（順不同）	63
--------------------	----

1. はじめに

1.1. 背景

我が国における近年の高度情報化社会の進展は、国民の経済活動や生活そのものに対し利便性、効率性等の面で様々な恩恵をもたらしているが、それを実現化しているのは飛躍的な発展を遂げる情報通信システムの存在であると言える。

各々の情報通信システムは、電気・通信・輸送などの各重要インフラに依存している一方で、この重要インフラ自身の運用・維持においてもそれぞれ固有の情報通信システムが利用されており、それらが相互に依存しているのが現状である。

個々の重要インフラは、それぞれ高信頼性確保のため十分な対策を行ってはいるものの、万が一不測の事態によりそれらの一つでも継続不能に陥ると、それは多くの情報通信システムに影響を及ぼし、我が国における政治・経済の両面に対して極めて重大な影響を及ぼす可能性は否定できない。

その一方で、今般の新潟県中越大震災を初め大型台風の本土上陸などの多くの天災がライフラインを破壊し、またアメリカ同時多発テロや各種コンピュータウィルスなどの人為的要因によるトラブルも、重要インフラの運用に大きな影響を与えている。今後の技術革新に伴い、新たな脅威が生まれる可能性も大きい。

そこで、特にライフラインに係わる国内重要インフラの環境、役割、及び機能を考える上での問題点の抽出や、取り巻く環境の変化、脅威について客観的な観点から整理を行うことは、e-Japan 遂行の中間点を迎えた現在、政府として各重要インフラの横断的検証を実施し、中長期的かつ現実的な情報セキュリティ政策・施策を内外に明示し得る意味で、非常に意義深いものであると考えられる。

1.2. 目的

本調査研究では、「情報セキュリティの基本問題」を「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」と捕らえ、調査研究のテーマとする。特に、重要インフラの事業継続のために、政府として検討すべき政策・施策を導出することを目的とする。

1.3. 本報告書の取り扱う範囲

本報告書では、まずは重要インフラに関する現状分析を行い、それぞれの重要インフラが個々に又は相互依存して抱える問題点を洗い出した結果について記載する。そして、その脅威や問題点についての対策を検討し、政府の施策・政策としての重要インフラ防護とその官民連携のあり方結果について記載する。

本報告書で取り扱う重要インフラとは、各事業者が対外向けに機能を提供している部分のみとし、独自の専用線のような社内独自インフラは対象外とする。

2. 重要インフラ概要

2.1. 重要インフラの定義

まずは重要インフラを定義し、その提供する機能を明確化する。

重要インフラとは、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であり、情報通信、金融、航空、鉄道、電力、ガス、政府・地方公共団体の7分野をいう¹。重要インフラが提供するサービスについては、その維持と障害時の迅速な復旧が確保されることが最重要となる。本報告書で取り扱う重要インフラ7分野の定義を表 2-1 に示す。

表 2-1 本報告書で取り扱う重要インフラ分野の範囲

	本報告書で取り扱う範囲
情報通信	固定電話・携帯電話・インターネット事業者
金融	銀行、信用金庫、保険会社、証券会社等
航空	航空保安業務、航空各社
鉄道	JR を含む鉄道各社
電力	電力各社 ²
ガス	都市ガス各社(プロパン等は除く)
政府・地方公共団体	政府・地方公共団体が提供するサービス ³

2.2. 重要インフラのサービス提供の維持について

上述したとおり、重要インフラが提供するサービスについては、その維持と障害時の迅速な復旧が求められる。重要インフラのサービス提供の維持に関する考え方の違いを表 2-2 に示す。

¹ 「重要インフラのサイバーテロに係る特別行動計画」(平成 12 月 12 月 5 日情報セキュリティ対策推進会議)
http://www.bits.go.jp/sisaku/2000_1215/1215actionplan.html 参照

² ただし日本原子力発電株式会社、電源開発株式会社等は除く

³ ただし防災・消防・水道・警察・医療・交通等は除く

表 2-2 重要インフラのサービス提供の維持に関する考え方の違い

		当てはまる重要インフラ分野
サービスの継続性 に対する考え方	サービス提供の維持が最優先	電力、情報通信
	サービス提供よりも安全確保が優先	ガス、鉄道、航空、金融、政府・地方公共団体
一社のサービスが 停止した場合の代 替事業者の数	ほとんど無い	電力 ⁴ 、ガス、政府・地方公共団体
	場合によっては代替可能	鉄道、航空、金融
	代替手段が多数存在	情報通信
一社のサービス停 止時の影響度	甚大な影響を及ぼす可能性がある	電力、金融、航空（航空管制）、政府・地方公共団体
	代替手段等により被害拡大防止が可能	情報通信、鉄道、航空（輸送）、ガス

表 2-2 に示すように、サービス提供の維持については、電力及び情報通信分野がサービス提供の維持のために様々な対策を行っているのに対し、ガス、鉄道、航空、金融、及び政府・地方公共団体のように、サービス提供の維持よりも安全確保が最優先とされる分野も存在する。このことは分野の特性に依存している。例えば、電力は他の様々なサービスが依存している重要インフラであり、かつ、一事業者のサービスが停止してしまった場合の代替提供手段が殆どないことから、電力事業者のサービス停止は許容されない。従って、電力供給の一部が停止してしまった場合でも事業者間や周囲の区域間で互いに補完できるように設計されている。

これに対して、鉄道や航空などの輸送事業は、少しでも異常を検知した場合には、運転を停止してその安全を確保することが優先されている。また、そのサービス停止時の代替手段として、他鉄道事業者、バス、タクシー、他航空事業者、及び船舶等が利用可能であるため、サービスの継続性は比較的優先事項とはならない。情報通信分野も同様である。

また、金融機関の1社が事業停止した場合、一部の機能は他の金融機関で代替可能であるが、多くの場合、利用者の資金管理が不可能となり、その金融機関が被る被害は甚大なものとなる。特に、地方銀行は地方経済の中枢を担っていることが多く、結果として地域活動が麻痺することが想定される。

2.3. 重要インフラを支える情報システムの概要

ここでは、重要インフラが提供するサービスの維持と迅速な復旧を支える情報システムについて、その概要を記す。

重要インフラを支える情報システムの多くは、制御系と情報処理系に分離されている。制御系とは、金融分野における勘定系や電力分野における電力供給のための

⁴ 各電力事業者の供給地域を越えて相互に電力を供給しており、電力事業者1社の事業停止時に一度にすべての電力供給が止まることはない。

システムなど、重要インフラの根幹を支えるシステムを示す。情報処理系とは、航空分野や鉄道分野等における座席予約システムや発券システム、その他顧客管理、料金計算、営業支援などを行うシステムのことをいう。

一般的に、制御系システムはインターネット等の外部ネットワークとは切り離す、システムを多重化するなどの入念な情報セキュリティ対策を実施しているケースが殆どである。

これに対し、情報処理系システムの多くは、その特性上利用者数が膨大である事に加えて、インターネット等の外部ネットワークとの接続が必要となっている。情報セキュリティ対策を積極的に実施しているものの、情報漏洩やウィルス感染等の内部要因による障害発生等のリスクは、他の民間業者同様に存在すると言える。

3. 重要インフラの機能継続に係わる脅威と対策及びその課題

本章では、重要インフラの機能継続にかかわる脅威を示し、その脅威に対する対策及びその課題を明確化する。

3.1. 重要インフラに対する脅威

重要インフラに対する脅威を、偶発的なものか、故意によるものかという2つの観点で洗い出した。表 3-1 では、各観点に含まれる脅威を小分類化してあげ、小分類に含まれる脅威の例を示した。

表 3-1 脅威の分類

大分類	小分類とその例
偶発的脅威	自然災害（地震、雷、風水害、雪害、火災） 自然事故（機器の劣化・不良、バグ） 人的事故（操作ミス、要員の能力・適正不足、体制・マニュアルの不備）
故意による脅威	物理的攻撃（破壊、不正改造、盗難（情報漏えい）、設備の盗難） サイバー攻撃 ⁵ （外部からのDoS、不正侵入（漏えい、改ざん、破壊）） 人的攻撃（ソーシャルエンジニアリング（フィッシング詐欺等を含む） 組織内部の人間による不正行為（不正操作、情報の持ち出し））

脅威に対する対策は、時系列に沿って考えると「障害の未然防止」、「障害の拡大防止・迅速な復旧」、及び障害の要因等の分析・検証による「再発の防止」に分けられる。このうち、「障害の未然防止」、「再発の防止」については、それぞれ障害発生前あるいは障害復旧後の所謂定常状態で実施する対策である。これに対し「障害の拡大防止・迅速な復旧」は、まさに障害が発生している状況における対策である。

「障害の未然防止」、「再発の防止」のための対策としては「予防」「抑止」といった観点の対策が相当する。また、「障害の拡大防止・迅速な復旧」のための対策としては、「検知」「拡大防止」「回復」といった観点の対策が相当する。

一方、脅威に対する対策は、その手段の性質により、「物理的対策」「技術的対策」「人的対策」に分類できる。表 3-2 に、対策の分類と対策の例を示す。

⁵ サイバーテロよりも広い概念であり技術的攻撃一般を指す言葉としてサイバー攻撃とする

表 3-2 対策の分類

対応サイクルによる分類		手段の性質による分類		
大分類	小分類	物理的	技術的	人的
障害の未然防止、再発の防止	予防	耐防災環境、システムの多重化、緊急時の電力及び通信回線の確保、非公開、入退管理	ネットワーク経由等による不正侵入防止、アクセス制御、情報の保存	緊急時対応計画の作成、情報セキュリティ管理体制の整備、基準・手順類の作成、教育・訓練の実施、監査の実施
	抑止	災害及び事故の検知、監視	監視、緊急事態の検知	
障害の拡大防止・迅速な復旧	検知	災害及び事故の検知、監視	監視、緊急事態の検知	
	拡大防止	システムの多重化、緊急時の電力及び通信回線の確保、災害及び事故の検知、監視	監視、緊急事態の検知、ネットワーク経由等による不正侵入防止	
	回復		監視、緊急事態の検知、情報の保存	

なお、表 3-2 で示した対策の例を JIS X 5080:2002 で示される分類で整理すると表 3-3 となる。

表 3-3 対策例と JIS X 5080:2002 によるセキュリティ対策分類との対照

JIS X 5080 によるセキュリティ対策分類		対応する表 3-2 の対策例	
1	情報セキュリティ基本方針	人的	基準・手順類の作成
2	組織のセキュリティ	人的	情報セキュリティ管理体制の整備
3	資産の分類及び管理	物理的	非公開
		技術的	アクセス制御
		人的	基準・手順類の作成
4	人的セキュリティ	人的	緊急時対応計画の作成、基準・手順類の作成、教育・訓練の実施、
5	物理的及び環境的セキュリティ	物理的	耐防災環境、システムの多重化、緊急時の電力及び通信回線の確保、非公開、検知、入退管理、監視
6	通信及び運用管理	物理的	システムの多重化
		技術的	ネットワーク経由等による不正侵入防止、情報の保存
		人的	基準・手順類の作成
7	アクセス制御	技術的	監視、ネットワーク経由等による不正侵入防止、アクセス制御
		人的	基準・手順類の作成
8	システムの開発及び保守	物理的	システムの多重化
		技術的	ネットワーク経由等による不正侵入防止
		人的	基準・手順類の作成
9	事業継続管理	物理的	災害及び事故の検知、監視、緊急時の電力及び通信回線の確保
		技術的	緊急事態の検知、情報の保存
		人的	緊急時対応計画の作成
10	適合性	物理的	監視
		技術的	監視
		人的	基準・手順類の作成、監査の実施、

3.2. 重要インフラに係わる脅威に対する対策

脅威に対する対策は、手段の性質により物理的対策、技術的対策、及び人的対策に分類できる。

物理的対策とは、以下に示す脅威に対する対策のことである。

- ・ 地震、雷、水害（降雪を含む）、火災、等の自然災害、機器の故障、等の偶発的な脅威
- ・ テロ等の人為的な機器の破損、盗難、建物や施設への物理的な破壊等を含む脅威

重要インフラの物理的対策は、日本が古来より地震、水害等の自然災害が多い国であり、そうした自然災害等の経験により得たノウハウを結集することで、多くの重要インフラ事業者が既にある程度の対応をしている状況にあるといえる。また、金融分野における「金融機関等コンピュータシステムの安全対策基準（以下FISC安全対策基準と記す）」⁶及び「検査マニュアル（金融庁）」⁶、情報通信分野における「情報通信ネットワーク安全・信頼性基準」など、業界によっては業界向けの基準又はガイドライン等を作成し、その中で、推奨する或いは要求する物理的対策を示しているものあり、各事業者の物理的対策の充実度に貢献している。

技術的対策とは、脅威に対して主に重要インフラ機能継続に必要な情報システムに対して IT を用いて対策するものを指す。

重要インフラの技術的対策は、2000年2月に発生した官公庁への不正アクセス以降、適用が積極的に推進されている。「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⁷の報告を見ても、各重要インフラ分野とも重要な情報システムに関しては、基本的に外部ネットワークとの接続を避ける、接続する場合にも認証システムやファイアウォールの導入、ウィルス対策、セキュリティ監査による検証の実施などの対策がとられており、各事業者における技術的対策状況は、ある程度の水準まで達していると考えられることができる。

また、次章でペネトレーション・テストの国内における普及状況について報告するが、これも技術的対策がある程度の水準に達していることの一つの裏づけと考えることができる。ただし、大手事業者を含めて IT 障害が発生している状況や、技術の進歩による脅威の多様化等を踏まえると、そうした変化への対応策を継続して検証する必要がある。また、IT 障害等が発生した場合の拡大防止や迅速な復旧に関

⁶ 金融庁による検査で使用されるマニュアル。金融持株会社に係る検査マニュアル，投資信託委託業者・投資顧問業者に係る検査マニュアル，証券会社に係る検査マニュアル，保険会社に係る検査マニュアル，預金等受入金融機関に係る検査マニュアルなどがある。 <http://www.fsa.go.jp/manual/manual.html>

⁷ <http://www.bits.go.jp/active/sisaku/20021128suisin-1.html>

しては実効性等の検証が必要である。

人的対策とは、脅威に対して人的要因を対象に実施する対策を意味する。これには、職員及び外部委託業者といった内部の人員を適切に管理するための「役割・責任の明確化」⁸、「管理体制の整備・維持」などの対策、また、それらを方針・基準・規則などの形で明文化するなどの人員管理の仕組みを整備するための対策が相当する。加えて、各人員に対し教育・訓練等を実施し、情報セキュリティ対策について周知・徹底を行うといった個々の人員に対して直接行われる対策も相当する。

金融分野における「FISC安全対策基準」及び「検査マニュアル(金融庁)」⁸、政府・地方公共団体における「地方公共団体における情報セキュリティポリシーに関するガイドライン」⁸、情報通信分野における「情報通信ネットワーク安全・信頼性基準」⁸、電力分野における「電力におけるサイバーテロ対策危機管理ガイドライン」⁸など各事業分野において様々な基準やガイドラインが存在すること、また、「重要インフラのサイバーテロ対策に係わる特別行動計画」のフォローアップ等について⁹の記述により、基準の整備、緊急時対応、人材育成、及び普及・啓発等の観点での対策が実施されていること、等から判断して各重要インフラ事業者における人的対策はある程度の水準にあると言える。

また、昨今の個人情報漏えい事件発生以降、情報管理も積極的に推進されており、個人情報保護法の2005年4月施行に併せ、各事業者の情報管理対策がさらに進展するであろうことが予測される。

業界としての基準やガイドラインが存在しており、かつそれらに基づくセキュリティ運用状況の把握等が行われている分野においては、業界内のセキュリティ対策の標準化がある程度実現されていると言える。

業界内においてセキュリティ対策状況が標準化されている基盤があれば、その上で障害や脆弱性等のセキュリティに関する情報共有も行いやすくなる。こうした業界を束ねる体制のある分野とない分野とでは、比較すると、今後セキュリティ推進状況に決して小さくない差が生じてくることが想定される。

⁸ 「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」(URLは下記の脚注次項目を参照)に、「電力分野においては、事業者団体にて「電力におけるサイバーテロ対策危機管理ガイドライン」を作成。」との記述がある。

⁹ <http://www.bits.go.jp/active/sisaku/h140328followup.html>

3.3. 重要インフラ間の相互依存性とその問題点

重要インフラとは、国民生活・経済活動の根幹となるサービスを提供する基盤である。それらは相互に依存関係を有していると同時に、特に電力に対する依存性が高いことは明らかである。

各重要インフラの相互依存性を表 3-4 に示す。

表 3-4 各重要インフラの相互依存性

		依存する側						
		情報通信	金融	航空	鉄道	電力	ガス	政府
依存される側	情報通信							
	金融							
	航空							
	鉄道							
	電力							
	ガス							
	政府							

：影響する¹⁰

：多少影響がある¹¹

空欄：影響しない又は不明

この表によれば、電力は勿論、情報通信分野の事業者に対する依存度も高いことが判る。電力に関しては、障害により電力事業の継続性に影響が出た場合、全ての分野にわたる重要インフラ事業者に影響を及ぼす。このような状況は何れの事業者も認識しており、このため、電力事業者はその機能停止を防ぐためにあらゆる努力を行っている。一方、電力に依存している他の重要インフラ事業者は、バックアップ電源の設置や電源供給の多重化等を行うことで、リスクの低減化を図っている。

緊急時の復旧作業を行う際にも同様のことが言える。つまり、複数の重要インフラが同時に緊急事態に陥ってしまった場合においては、電力や情報通信の復旧が他の重要インフラ事業者の復旧作業に依存してしまうのである。

従って、重要インフラの効率の良い迅速な復旧作業を実施するという観点においては、業種及び事業者を横断した正確かつ迅速な情報共有を行う事が重要となる。被害状況の把握、復旧作業の優先順位付け、及びそれらに基づいた的確なスケジュー

¹⁰ 依存される事業者の機能低下又は停止が発生した場合、その事業者に依存している事業者も同様の機能低下又は停止してしまう場合

¹¹ 依存される事業者の機能低下又は停止が発生した場合、その事業者に依存している事業者の提供するサービスが一部低下する可能性がある場合

ール策定等を行うことが必須である。

また、日頃からこのような緊急時の情報共有の訓練等を行い、緊急時の体制の有効性を確認すると共に、定期的に見直しを行うことも重要である。しかし、残念ながらこれらの対策の実施度は必ずしも高くないのが現状である。阪神淡路大震災や新潟県中越大震災等の激甚災害発生時の教訓を元に、早急な対策が必要と考える。

特にヨーロッパやアメリカなどの海外においては、複数の国の重要インフラがそれぞれ相互依存している場合がある。その場合、複数の国にまたがった重要インフラ事業者に対する国際的なセキュリティ対策基準を定め、公開し、その基準に従ったセキュリティ対策を行うこととなる。日本は島国であり、他国の重要インフラ事業者との関連は殆どないものの、そのようなセキュリティ対策標準は様々なノウハウの集まりであり、日本特有の事案を考慮した上で活用すべきである。

3.4. 重要インフラ防護に係わる現時点の課題

「3.2 重要インフラに係わる脅威に対する対策」及び「3.3 重要インフラ間の相互依存性とその問題点」から、重要インフラ防護に係わる現時点の課題を分析する。

課題は、情報共有のあり方、緊急時対応に関する演習の必要性、及びセキュリティ対策の基準化推進、という3つの観点から整理し表 3-5 に挙げた。

表 3-5 個々の重要インフラ防護に係わる現時点の課題及び各重要インフラ間の相互依存性に係る現時点の課題

	個々の重要インフラ防護に係わる現時点の課題	各重要インフラ間の相互依存性に係る現時点の課題
情報共有	<ul style="list-style-type: none"> ・事業分野における情報共有に対する姿勢の差異 ・情報提供のための制度の不足 	<ul style="list-style-type: none"> ・業種を横断する情報共有制度が存在しない
演習	<ul style="list-style-type: none"> ・緊急時対応に関する演習の不足 	<ul style="list-style-type: none"> ・複数インフラ事業者における緊急事態発生への対応に関する演習の不足
対策の基準化	<ul style="list-style-type: none"> ・情報セキュリティ対策の業界内標準化に対する業界ごとの取り組み姿勢の差異 	<ul style="list-style-type: none"> ・相互依存項目に関するセキュリティ対策の業種間調整の不足

(1) 情報共有に対する現時点の課題

個々の重要インフラ防護に係わる現時点の課題として、事業分野によって情報共有に対する姿勢に差があること、情報提供のための制度が不足していることの2点が挙げられる。

例えば、過去に発生した事件事故等の情報共有を積極的に行うことにより、再発防止を積極的に推進している分野がある一方で、そうした情報共有実施に消極的な分野が存在する。

同一事業分野の事業者においては、想定される脅威や脆弱性について、事業者間で共通するものが多いと考えられるため、事故犯罪に関する情報収集・分析・提供などの情報共有により、重要インフラの機能継続に係わる対策の効率的な推進を期待できる。このため、いずれの分野においても、個々の重要インフラ事業者内だけに留まらず、事業者を横断した情報共有体制が整備されることが望ましい。

また、情報共有においては、情報提供事業者は脆弱性や事件事故の事例など、いわゆる組織にとってマイナスの情報を他事業者に提供することになる。各事業者が、同一事業分野の他事業者に対してこうした情報提供を行うことにためらいを感じずることは十分に想像できるが、一方この考え方は、情報共有化推進の大きな妨げとなる。また、提供した情報の提供先での取り扱い方法に関して明確な取り決めが無いことも、情報提供に消極的とならざるを得ない一因と考えられる。

従って、情報共有を活性化させるためには、情報提供者にとって情報提供を行いやすい環境の整備、提供する情報の内容や範囲に関する十分な事前検討が必要である。

各重要インフラ間の相互依存性に係わる現時点の課題としては、「業種を横断する情報共有制度が存在しない」ことが挙げられる。3.3 重要インフラ間の相互依存性とその問題点で述べたように、何れの重要インフラ分野も電力、及び情報通信分野への依存度が高い。こうした事実がある中で、事業分野を超えた障害や脆弱性等に関する情報共有は欠かせないものとする。

情報共有に関しては、個々の重要インフラ事業者に係わる課題、及び業種を横断した課題がそれぞれ存在する。これらの課題は、政府による情報共有組織を整備し、一元的に情報を収集・分析・提供すれば解決するという訳では決してない。重要インフラ防護のために必要な情報は様々なチャネルから収集することが望ましいが、それによって各重要インフラ事業者がバラバラの対策をとってしまっただけでは意味がない。

この一見矛盾している問題点を解決する一つの方法は、異なる役割を持った官民のそれぞれの情報共有に係わる組織間の連携である。情報共有政策、及び官民連携のあり方について、海外における事例等を参考にしながら次項で検討を行う。

(2) 緊急時対応に関する演習の必要性

管理者は、定常時におけるセキュリティに関する運用が各要員によって確実に実施されているかを把握するために、業務のリモート監視や監査などを実施する。しかし、緊急時において当該要員による適切な対処策が滞りなく実施されるかを想定することは難しい。

一方、緊急時対応計画は、緊急時の被害を少しでも抑えるために計画されており、緊急時に確実な対処が執られなければ意味をなさない。緊急事態発生という異常な状況下での的確な対応を実施することは、定常運用を確実に行うことよりも困難であり、これを実現させるためには、類似の状況を事前に模擬体験しておくことが有効である。

サイバーテロを含めた緊急時対応計画の策定が進められている中で、重要インフラ事業者においては、緊急事態発生に対する対応の事前演習としての「ペネトレーション・テスト」と呼ばれる、脆弱性を模擬的に攻撃しそれへの対応状況を評価する演習については普及の度合いが高まってきているが、それ以外の方策についてはあまり実践されていないのが現状である。今後は、緊急時をより幅広くシミュレーションし、対応を模擬的に体験する演習が行われることが望ましい。

また、現状実施されている演習の多くは各事業者内に閉じた状況で行われてい

るが、今後は事業者間の相互依存性を考慮した、複数業界に跨るシミュレーション演習も必要となる。これらを実施する場合は、その影響の大きさと有効性を鑑み、業界の枠を越えた実施体制についても検討することが必要である。

次に、演習そのもののあり方について、海外における事例等を参考にしながら検討を行う。

(3) セキュリティ対策の基準化の推進

セキュリティ対策における統一基準の策定は、各事業者におけるセキュリティ対策の取り組みを明文化する意味でも重要である。重要インフラ分野においては、多くの事業者において既に策定済の状況にあると言える。但し、それらは元々事業者単位での独立した取り組みであったことから、同一分野の事業者であってもセキュリティ対策に関する基準の内容が大きく異なっている場合がありうる。

ISO17799、BS7799-2:2002 といった情報セキュリティマネジメントに関する基準の普及により、近年、各事業者の作成するセキュリティ対策基準の内容は、標準化が進んでいるが、具体的な取り決めのレベルでは、各組織毎に異なっている状況にある。例えば、2つの事業者がセキュリティ対策基準項目として入退管理を規定している場合にも、入退管理をどのレベルで行うか、例えば個人単位の入退室記録を採るかといったことは組織毎に異なってくることが想定される。

前述のとおり、業界として取り組むべきセキュリティ対策について、基準やガイドライン等で示している事業分野については、ある程度の標準化が為されているものと見なすことができる。一方、業界標準のない事業分野においては、事業者間でセキュリティ対策の取り組み状況、セキュリティ対策に対する認識にある程度の差が生じる可能性がある。この差は、前述の情報共有推進における、情報提供が行いやすい環境整備実現の妨げともなり得るものである。例えば、共有した情報の取り扱いにばらつきが生じ、その結果予期しない情報の取り扱いに関する侵害が発生するなどが想定される。

また、現状、セキュリティ対策内容は事業者内に閉じている場合が多いが、相互依存性が多く見られる事業者間では、相互依存項目に関するセキュリティ対策内容については事業者間での調整が行われることが望ましい。これについても、業界における基準の標準化の中で検討・反映していくことが必要と考えられる。

4. 政府の政策・施策としての3年後の理想像

本章では、政府の今後3年間に渡る政策・施策としてどのようなものが考えられるのか、欧米及び国内における現状を考慮した上で提言する。具体的な項目としては、「情報共有政策の推進」、「重要インフラ防護のためのセキュリティ演習」、「セキュリティに係わる標準策定の推進」を挙げている。

「4.1 情報共有政策の推進」では、事業者が保有するインシデントに関する情報を効率的に吸い上げ、一元管理・配信を行うことにより、類似インシデント発生時における社会的影響の軽減を目指すための政策・施策を提言する。

一方、情報共有はあくまで過去のインシデント情報を収集したに過ぎず、これらに基づいた対策を行ったとしても、未知の脅威に対しては有効に働かない。そこで、事業継続性の観点から、インシデントが発生したとしても適切に対処できるように日頃から訓練を行っておく必要がある。これらを踏まえて、「4.2 重要インフラ防護のためのセキュリティ演習」では、セキュリティ演習の形態を国内外の過去の事例を元に分類するとともに、今後政府及び重要インフラ事業者が取り組むべき演習形態、及びそれに伴う政策・施策について提言する。

「情報共有政策の推進」、「重要インフラ防護のためのセキュリティ演習」は、その実施自体も重要であるが、それ以上にこの施策から得られた教訓を事業者に根付かせることが重要となる。従って、「4.3 セキュリティに係わる標準策定の推進」では、国内外で制定されているセキュリティに係わる標準及びガイドライン等を洗い出すと共に、特に米国で積極的に制定されている「業界標準」の策定に焦点を置き、「情報共有政策の推進」、「重要インフラ防護のためのセキュリティ演習」で培われたノウハウを活用した標準策定・ブラッシュアップの必要性を提言し、「政府の政策・施策としての3年後の理想像」としてまとめるものである。

4.1. 情報共有政策の推進

異なる事業分野間で横断的に情報共有を行うことは、重要インフラ防護にとって重要であることは前に述べた。例えば、ある事業者でシステム障害が発生した場合、それが単なるプログラムの障害であるのか、或いは悪意を持った第三者による攻撃で引き起こされたのかを切り分けるためには、他の事業者や警察に問い合わせる等により、同様の現象の他部署での発生有無を確認しないと判断できない。他の事業者でも同様な障害が発生していることが判れば、ウィルスなどによる攻撃も疑われることになる。一方、そのような問合せが行えない場合には、あらゆる可能性の中から自力で原因を追究する必要があり、原因究明に多大な時間を要する。

このように、他所でのシステム障害の発生情報をいち早く入手することで、その障害の原因が第三者攻撃であった場合、その対策を迅速かつ適切に実施することが可能となる。このような情報は、インターネット上のコミュニティとして幅広く流通しているが、情報の信用性に欠けるものもあり、重要インフラという性格を考慮した場合には不適格なものも多い。そこで、政府主導で信頼のおける情報共有が行われることが求められる。

情報共有は、アメリカでは ISAC (Information Sharing and Analysis Center) (情報収集分析センター) として 1999 年頃から活動が行われている。一方国内においても 2002 年から Telecom-ISAC (通信分野の情報共有団体) が活動を開始しており、その活動はかなり定着している。以下では、米国及び国内での ISAC の現状を述べると共に、今後求められるであろう情報共有政策について言及する。

4.1.1. 米国における ISAC の現状

(1) ISAC の種類と産業分野

米国における ISAC は、民間セクターが重要インフラ保護 (CIP: Critical Infrastructure Protection) に関する様々な情報を共有し分析するための組織であり、2005 年 1 月 14 日現在、米国土安全保障省 (DHS: Department of Homeland Security) などの Web サイトで確認されるだけで 17 種類の ISAC がある。

ISAC Council (Information Sharing and Analysis Centers Council) は、ISAC 同士及び ISAC と政府間の相互作用を効率良く発揮させるための枠組みであり、北米地域の重要インフラに関するサイバー及びフィジカルセキュリティを強化することを目的として設立された。現在は 10 の ISAC が参加している。

これはもともと独立に活動していたものが、セクター間の情報共有が必要であるということから、当初 8 つのセクターがジョイントし、ISAC 活動の重要ポイントや目的を明確にするために作られたものである。

ISAC Council では毎月一回ミーティングを開催しており、ISAC 間での情報共有を図っている。

表 4-1 ISAC の種類と産業分野

(2005 年 2 月 10 日現在)

産業分野 ¹²	ISAC
農業	なし
食料	Food Industry ISAC
水道	Water ISAC*
公衆衛生	Healthcare Services ISAC (HCISAC)*
エマージェンシー サービス	Emergency Fire Service ISAC
	Emergency Law Enforcement ISAC
州政府	Multi-State ISAC (MS-ISAC)
国防産業	なし
情報通信	Information Technology ISAC (IT-ISAC)*
	Telecommunications ISAC (NCC-ISAC)*
	Research and Educational Network ISAC (REN-ISAC)
エネルギー	Electricity Sector ISAC (ES-ISAC)*
	Energy ISAC*
交通	Surface Transportation ISAC (ST-ISAC)*
	Public Transit ISAC (PT-ISAC)* ST-ISAC 内 ISAC
銀行及び金融	Financial Services ISAC (FS-ISAC)*
化学及び危険物	Chemical Industry ISAC*
不動産	Real Estate ISAC
郵便及び輸送	なし
グローバル	World Wide ISAC

*ISAC Council メンバー

¹² 産業分野の分類方法はDHSによる

(2) 重要インフラ分野の ISAC の活動内容

今回重要インフラとして定義した分野に相当する ISAC の活動内容について表 4-2 にまとめる。該当する ISAC は 8 団体であるが、これらの運営母体、運営資金の調達方法などはそれぞれ独自の方式をとっている。

例えば電力分野の ISAC である ES-ISAC (Electric Sector ISAC) は、北米 (カナダ、アメリカ、メキシコ) の電力会社で構成されている電力信頼度協議会 (North America Electric Reliability Council : NERC) が運営しており、NERC に加入しているメンバーはすべて ES-ISAC に加入している。そのため、ISAC として会費徴収は行われておらず、NERC 会員としての会費により運営が任されている。これは NERC が、1960 年代から電力業界における情報共有活動を実施しており、ISAC 設立の気運が高まった際に、既存の組織を活用して設立されたことに由来する。

一方金融分野の ISAC である FS-ISAC とエネルギー分野 (石油会社とガス会社、一部の電力会社が加入) の ISAC である Energy ISAC は、政府関連のセキュリティサービスを行っている民間の SAIC 社が運営している。同じ母体で運営されていながら、FS-ISAC は会員からの会費により運営費がまかなわれているのに対し、Energy ISAC は、エネルギー省 (DOE : Department Of Energy) からの援助資金 (\$600,000) を元に、中小事業者の会費を無料にしている (会費 (\$7,500 / 年) を納めている事業者に対しては、基本サービス以外に、オプションのサービスを提供している)。

ISAC の基本的な機能は、物理・サイバー両面に対する情報共有であるが、その運営方法や監督官庁の関わり方には大きな違いがある。これは、既存の組織を十分に活用し、業界の事情 (事業者の規模の違いなど) を十分に反映して ISAC が設立されたためである。

表 4-2 米国における重要インフラ分野の ISAC の活動内容 (1 / 2)

分野	ISAC	活動内容
情報通信	Information Technology ISAC (IT-ISAC)	2001年1月設立。非営利団体であるISS社が運営する。ソフトウェア、ハードウェア、サービスを含むIT業界全般を対象とする。会員からの情報は一旦ISSに集約された後、匿名化した上で会員に配信される。また重大情報はITAA (Information Technology Association of America) を通じて広報される。会員が納める会費により運営されている(サービスが限定された無料会員の制度もある)
	Telecommunications ISAC (NCC-ISAC)	NCC (National Coordinating Center for Telecommunications)が2000年3月に設立し運営にあっている。通信業者、ネットワークサービス、及びこれらを対象としたベンダーや、関連協会、省局が参加している。脆弱性、脅威、侵入、異常状態に関する情報を複数のソースから入手し分析して、警告の発令や通信インフラに与える影響を軽減することを目的とした活動を行っている。運営費は政府予算によりまかなわれている。
金融	Financial Services ISAC (FS-ISAC)	1999年10月設立。ISACの中で最初に設立された。セキュリティベンダーであるSAIC社が運営する。銀行、証券、保険業界を対象とし、業界向けの脆弱性、脅威、インシデントに関する情報をいち早く入手し、分析した上で、会員への情報提供を行っている。会員が納める会費により運営されている(サービスが限定された無料会員の制度もある)
航空	Public Transit ISAC (PT-ISAC) ¹³	2003年1月にST-ISAC内のISACとして設立。APTA(American Public Transportation Assn.)が運営する。基本的な活動はST-ISACと同じであるが、鉄道に限らず幅広く公共交通機関を対象としている。
鉄道	Surface Transportation ISAC (ST-ISAC)	2002年4月設立。AAR(Association of American Railroads)が運営する。貨物・旅客双方の鉄道事業者及び、陸上輸送事業者が加盟する。各国の政府やCERTが発行する情報及びベンダーの情報などを収集し、会員事業者に対して脆弱性情報などを提供する。情報の範囲としてはサイバー・物理両方を含む。

¹³ PT-ISACは航空・鉄道両分野を含む

表 4-2 米国における重要インフラ分野の ISAC の活動内容 (2 / 2)

分野	ISAC	活動内容
電力	Electricity Sector ISAC (ES-ISAC)	2000 年 10 月に設立。電力業界を対象としており、サイバー・物理両面での脅威・脆弱性に関する情報を収集し、メンバー間で共有している。もともと電力供給の信頼性確保を目的として設立された NERC が運営にあたっているため、NERC 設立から 30 年以上にわたって行われていた情報共有を引き継いだ形となっている。また情報共有にあたって会員との間に NDA を結んでいないなど、会員間の結束は非常に強く、最も成功した ISAC の一つであると言われている。運営費は NERC として会員から集められた会費によりまかなわれている。
ガス	Energy ISAC	FS-ISAC を参考に、2001 年 11 月に設立された。FS-ISAC と同様、SAIC 社が運営する。石油、ガス、パイプライン事業者を対象としており、サイバー・物理両面での脅威・脆弱性に関する情報提供を行っている。会員からの情報提供は期待しておらず、一方的な情報配信を目的としている。大事業者が多い石油業界と小事業者が多いガス業界の両方を対象としていたため、活動が石油業界中心となってしまう、ガス業界の中には活動に不満を漏らす事業者もある。また民間企業である SAIC 社に重要情報が漏れることを懸念する事業者もある。運営費に関しては、規模の小さなガス事業者の中には参加費を払えない事業者も存在したため、運営費を DOE からの補助によりまかなう(別途会費を支払うと、オプションサービスを受けることができる)方式に変更し、小事業者の参加を促している。
政府・地方公共団体	Multi-State ISAC (MS-ISAC)	2003 年 1 月設立。ワシントン DC も含めた全米 50 州が加盟する。メンバーは月に 1 回電話による会議を開いており、MS-ISAC は政府及び各州間の情報共有の中心的役割を果たしている。

4.1.2. 国内における情報共有の現状

2005年1月18日現在、国内において確認されているISACはTelecom ISACただ一つである。しかし、ISACという名称は使われていなくても、事業者間の情報共有を行っている業界団体はいくつか存在する。以下では、国内において確認できている重要インフラに係わる団体の現状について述べる。

「財団法人金融情報システムセンター(FISC)」のように、国内における業種別の情報共有は、ISACという名前はついていないが、業界団体レベルで米国のISACに近い活動が行われているケースもある。一部の活動は「重要インフラの安定稼働」に重点を置いたものであるが、米国の電力分野におけるISACであるES-ISACのように、従来、電力信頼度協議会(NERC)で行われていた情報共有をISACという形に発展させたものもある。また無理に複数の業界にまたがった情報共有を行おうとすると、米国のEnergy ISACの事例のように、石油業界、ガス業界の事業規模の違いやセキュリティに対する意識の相違から効率的に機能しなくなる可能性もある。よって、従来から業種別に情報共有が行われている業界であれば、新たな組織を設立せずに既存の枠組みを活用することも望ましい、と考えられる。

4.1.3. 海外の重要インフラ防護機関との連携

情報共有政策の一環として、各国政府の重要インフラ防護機関との情報共有を提案する。重要インフラのセキュリティが、主に物理面で重要視されていた時代には、国境での警備を強化することによりテロリストなどの侵入を阻止することができた。しかし、サイバーセキュリティも考慮しなければならない現代では、国境のない世界で如何に迅速にテロなどの行為を阻止するかが重要となる。そのためには、各国政府機関とのこれまで以上の密な連携が必要と考えられる。

以下では、主な国の重要インフラ防護機関とその活動内容を紹介する。

表 4-3 主な国における重要インフラ防護機関 (1 / 2)

国	機関名	活動内容
アメリカ	国土安全保障省(DHS) IA&IP (Information Analysis and Infrastructure Protection)	<ul style="list-style-type: none"> ・米国における重要インフラやキーリソースの安全保障に係わる包括的な国家計画を立案すること ・他の連邦機関との調整や、州及びローカル政府機関、公社、プライベートセクターなどとの協力を通し、米国における重要インフラ及びキーリソースを保護するための手段を推奨すること ・テロ攻撃に対する抑止、予防、先制、又は対応策を支援するために、DHS によって分析された情報を DHS 内に、また他の連邦機関、州及びローカル政府機関、プライベートセクターに対して広めること
イギリス	国家インフラストラクチャ安全調整局 (NISCC) (National Infrastructure Security Co-ordination Center)	<ul style="list-style-type: none"> ・兼任者によるバーチャルな組織形態である ・「産業セクション毎」「技術テーマ毎」の2層構造により構成されており、「産業セクション毎」の枠組みの中で、重要インフラへの対応が行われている ・大きな脅威が発生した際に、NISCC がコーディネーターとなって重要インフラ監督省庁との連携を行う
ドイツ	内務省 連邦情報技術安全局 (BSI) (Bundesamt für Sicherheit in der Informationstechnik)	<ul style="list-style-type: none"> ・IT セキュリティに関する最新動向の分析結果等を基に、IT に関する連邦政府の政策助言及び製品認証における国際協調の推進化を図る ・BSI は重要インフラ事業者とインフォーマルなミーティングを実施しており、また重要インフラ事業者に対して、監督省庁を通さないダイレクトなネットワークを持つ

表 4-3 主な国における重要インフラ防護機関 (2 / 2)

国	機関名	活動内容
フランス	国土保安局 (DST) (Direction de la Surveillance du Territoire)	<ul style="list-style-type: none"> ・フランス国内のセキュリティ (CIP 含む) に関して責任を負う ・サイバー犯罪への対応を目的とした情報システム部 (DSI) と、国防施設や社会インフラ施設の防護を目的とした国家財産監視保護経済部 (DESPPN) を有する ・ミッションとして、テロやサイバー犯罪対策が挙げられている
韓国	国家情報院 (NIS) (National Intelligence Service)	<ul style="list-style-type: none"> ・1961年に設立された韓国の諜報機関 (KCIA) を前身とする大統領の直轄組織 ・国家・公共部門を対象とした情報システムのセキュリティ対策支援、重要インフラ保護等をミッションとする
	情報通信部 情報保護振興院 (KISA) (Korea Information Security Agency)	<ul style="list-style-type: none"> ・上部組織である情報通信部 (MIC : Ministry of Information and Communication) は重要インフラ保護関連政策の総括・立案を行う ・情報セキュリティ政策の調査、重要インフラ保護、情報セキュリティ製品評価等、韓国情報セキュリティの中心的な役割を担う ・重要インフラ保護の支援として、重要インフラ保護対策立案・技術支援等を行う
オーストラリア	通信情報技術・芸術省 情報経済局 E-security 調整グループ (ESCG) (E-Security Co-ordination Group)	<ul style="list-style-type: none"> ・連邦政府の省庁横断組織で、関係省庁の代表者により構成され、官民双方の重要インフラ保護及び情報セキュリティに関する政策立案、調整を行う ・管轄下の重要インフラ防護グループ (CIPG : Critical Infrastructure Protection Group) で、電気通信、金融、電力、航空における脆弱性の評価を監督し、致命的な影響を与える重要インフラ保護に関する助言を行う

4.1.4. 今後求められる情報共有政策のあり方

今後重要インフラに求められる情報共有政策のあり方について、以下に述べる。

(1) 情報共有促進政策の必要性

ISAC の活動が活発な米国においても、事業者から提供される情報は未だ十分ではないのが現状である。DHS 等のヒアリングによれば、比較的活動が成功しているといわれる電力関連の ES-ISAC で 50%程度、ガス関連の Energy ISAC では 25%程度しか情報が把握できていないと言われている。以下では、米国で情報共有促進のために実際に導入されているか、又は導入が検討されている政策・施策の事例を紹介する。

(a) 情報の安全性の確保

米国では情報公開制度（FOIA : Freedom Of Information Act）があり、連邦政府が保有する情報に対して市民から情報開示を求められた場合、拒否することができない。これは、重要インフラに関するセキュリティ情報も例外ではなく、この制度が事業者からの情報提供を阻害していると指摘されていた。そこで CIP に係わる情報に限り、FOIA の適用除外にできるプログラム（PCII Program : the Protected Critical Infrastructure Information Program）を整備した。

事業者は連邦政府に提供する情報に対して、CII (Critical Infrastructure Information) であることを主張する権利が与えられている。このように主張された情報は、PCII Program Office が審査し、CII であるかどうかを判断する。もし仮に CII であると認められなかった場合は、事業者は提供した情報を返却あるいは破棄を要求することができる。

日本国内においても、事業者から提供された情報の安全性を確保する制度を整備することが必要であると考えられる。

(b) NDA (Non Discloser Agreement) の締結

米国において、ISAC に所属する事業者間での NDA の有無は、ISAC の成り立ちや運営方法により異なる。例えば、ES-ISAC ではメンバー企業との NDA は結ばれていない。これは、NERC の 30 年に及ぶ歴史の中で培われてきた信頼関係によりその必要がないためである。一方 Energy ISAC では、参加企業全てが NDA を結んでいる。これは Energy ISAC がガス業界及び石油業界など、業界にまたがって設立されていることと、運営母体が SAIC 社という民間の企業であることに由来している。事実ヒアリング調査により、SAIC 社のような民間企業に CII が流れることを懸念する声も聞かれた。なお ISAC Council においては、各 ISAC 間において NDA が締結されている。

このように、事業者から効率的に情報提供を促すためには、NDA の整備なども重要になると考えられる。

(c) TAX サービス

米国会計検査院（GAO：Government Accountability Office）が検討している政策であり、共有するのに有効な情報を積極的に提供した企業に対しては、税の軽減措置や情報提供活動に対する対価としての活動費用の負担を行えないか検討している。

どのような情報を有効であると認めるのか判断が難しい面もあるが、政府による情報提供促進のための一つの手法として考えられる。

(d) フィードバック

米国でのヒアリング調査により、情報提供に対するフィードバックの重要性が指摘された。特に政府機関は、提供された情報に対して何らかの付加価値を付けた形で事業者に戻すことが求められている。その一つの形として、事業者が提供した情報に、政府しかアクセスできないような情報を加えた分析を行い、フィードバックできないか検討されている。

情報共有は双方向で行われて初めて成り立つものであり、政府はどのような形で事業者にフィードバックできれば情報提供に対するインセンティブが向上するのか、検討する必要がある。

以上のように、情報共有を促進するにあたっては、事業者間における情報提供の仕掛け作りが重要となる。セキュリティに関する情報は、使われ方次第では逆に脅威ともなり得る。また、民間企業にとっては経営上外部に提供することが難しい情報でもある。よって、情報流通を促進するに当たっては、その情報の安全性及び提供のメリットを目に見える形にすることが、最低限求められるものとする。

(2) 情報共有組織間における連携の重要性

4.1.2 で述べたように、国内における情報共有は一部の業界で業種を中心とした枠組みで行われている。既存の枠組みを活用した活動という面からすると、これは望ましい形態であり、今後の他の業界への展開が期待される。しかしながら、セキュリティに関する情報共有は業界に閉じて行われるべきではない。そこで、情報共有組織間における連携の重要性を、以下の観点から述べる。

(a) 幅広い情報の結集

前述の通り、国内における情報共有は一部の業界で業種を中心とした枠組みで行われている。Telecom ISAC に(社)電気通信事業社協会がオブザーバとして参加しているケースはあるものの、組織間の積極的な情報共有を目的としているものとは言い難い。また一部の事業者では、地域毎に設けられている情報共有連絡会などに所属し、他の事業者と連絡を取り合っているケースも見られるが、事業者単独での取り組みに留まっており、重要インフラ全体としての情報共有の枠組み作りまでには至っていない。

米国においても、必ずしも当初から重要インフラとしての情報共有が行われていたわけではなかった。米国ルイジアナ州バトンルーージュ郡の East Baton Rouge Law Enforcement でのヒアリングによると、例えば 2001 年 9 月 11 日に起きた米国同時多発テロの犯人の 1 人は、連邦政府が運用する「ナショナルテロリスト」情報のデータベースに登録されている人物だった。しかし彼がフロリダ地区で駐車違反を犯した際に、地元の警察は反則切符を切っただけで釈放してしまった。これは連邦政府と地元警察との間で情報共有が行われていなかったがために起きてしまった問題である。

現在米国では、ISAC Council の活動などにより重要インフラ全体としての情報共有が進められている。同様に国内においても、重要インフラ相互間の情報共有を推進する枠組み作りが求められる。

(b) 情報管理の一元化

(a) で述べた、組織間における情報共有が活発になると、様々な情報がやり取りされるため内容が錯綜してしまう懸念が指摘されている。例えば、同じ内容の情報であっても、報告元の捉え方によって異なる情報として処理される可能性が生じる。このような状況が続くと、事業者のセキュリティ担当者に提供される情報は膨大な数となり、個々のインシデントに対する意識が低下する可能性がある。また、監督官庁と所属業界団体など、複数の経路から同一の情報が送られてくることにより、セキュリティ担当者が忙殺される可能性もある。

情報を幅広く結集するに当たっては、内容及び連絡経路の一元化を徹底することが必要となる。

(3) 重要インフラに係わる情報管理の徹底

インターネットの普及に伴い、様々な情報が容易に入手可能となっている。しかし米国では、重要インフラに係わる機密性の高い情報までも安易に流通される状況が危惧されており、2001年9月11日の米同時多発テロ以降、こういった重要インフラに係わる情報（CII：Critical Infrastructure Information）の管理を強化している。具体的には、米運輸省（DoT：Department of Transportation）のWebサイトで公開されていた送電システムのマップは、テロリストに悪用されるとの観点から掲載を取りやめている。

こういった情報の中には、公開されている情報そのものの機密性が高い場合もあるが、事業者が情報それ自体は機密性が高くないため、何気なく公開している情報があり、これらを集めて統合することにより機密性の高い情報が作成される例も報告されている。アメリカではこのような、機密扱いでない大量の情報から重要な機密情報を導き出す行為のことを「デリベーション(導出)」と呼んでいる。

また、事業者が公開する意図はないものの、そういった情報を入手した第三者が公開してしまっている事例もある。例えば、事業者の社員が講演した資料を入手した第三者が、Webサイトなどで公開してしまっている例などが挙げられる。

インシデント情報などを事業者や政府がお互いに共有していく必要がある一方で、今後は、インターネットや書籍などで公開されている、重要インフラに関する情報の管理を徹底していくことが必要と考える。

4.2. 重要インフラ防護のためのセキュリティ演習

国内の重要インフラ各社においては、その社会的責任の重大性から既に多くの投資がセキュリティ対策に対して行われている。しかし、従来型のセキュリティ対策は「過去のインシデント事例」に基づいたものが多く、ゼロデイ攻撃¹⁴や攻撃手法の多様化・高度化に対して迅速に対応することには困難が伴う。また、オープンソースなソフトウェアの利用が進展すると、ソフトウェアの中身を熟知した攻撃者による攻撃の可能性も考えられる。

このような状況を考慮すると、インシデントの発生を100%防ぐことは困難であり、従来型のセキュリティ対策を行うと共に、事業継続性の観点から、実際にインシデントが発生した際に迅速に対応すべく日頃から訓練を行う、「セキュリティ演習」の実施が必要であると考えられる。以下では国内外で実施されたセキュリティ演習を紹介し、その実施形態を分類するとともに、今後重要インフラ防護のために必要と思われるセキュリティ演習について提言する。

¹⁴ アプリケーションのセキュリティホールに関する情報が、一般に公開される前にそのセキュリティホールを狙って行われる攻撃

4.2.1. セキュリティ演習の形態

重要インフラを防護するためのセキュリティ演習としては、大きく分けて2つの演習が存在する。一つは「ペネトレーション・テスト」¹⁵と呼ばれるもので、もう一つはインシデントに対する「緊急時対応演習」である。ペネトレーション・テストは、システムの脆弱性をチェックする検査であり、いわば「被害に遭うことを最小限に留める」ためのテストであると位置付けることができる。一方緊急時対応演習は、インシデントが発生することを前提としており、シミュレーションや模擬システムなどを使用して、実際にインシデントを発生させ、担当者が適切に対応できるかテストする、いわば「防災訓練」的な演習である。

表 4-4 セキュリティ演習の形態

形態	ペネトレーション・テスト	緊急時対応演習
目的	被害に遭うことを最小限に留める	インシデント発生後の対応手順などを確認する
演習内容	システムの脆弱性をチェックする検査	想定されるインシデントを模擬システムやシミュレーション上で発生させ、その対応を訓練する
演習機器	実際に稼動しているシステム	・ 机上演習 ・ コンピュータ上でのシミュレーション ・ 実機をモデル化した模擬システム

¹⁵ 実際に稼動しているシステムに対して実際に攻撃を行い、脆弱性やセキュリティ上の問題がないかチェックすること。

また緊急時対応演習には大きく分けて表 4-5 に示す 4 つの実施形態が存在する。各々の内容と特長及び実施事例を表 4-5 に示す（事例の詳細に関しては、4.2.2、4.2.3 にて後述する）。

表 4-5 緊急時対応演習の実施形態

形態	概要	特長	事例
机上演習	関係者が会議室などに集まり、特定のインシデントに対する対応手順を確認する。	<ul style="list-style-type: none"> ・実際のインシデント発生を体験するわけではないため、リアリティに欠ける ・コスト面や準備が短期間である点でメリットがある 	表 4-9 表 4-11 ~ 表 4-18
シミュレーション演習	シミュレーション・システム上の仮想のインターネットに、自社のシステムと同じ構成の仮想システムを接続して行う演習。シミュレーション上でのインシデントの発生に対して、実際に担当者が対応して、手順を確認する。	<ul style="list-style-type: none"> ・数週間から数ヶ月といった長期にわたるシナリオを数日間で実施できるなど、時間的な短縮が図れる ・今後発生し得る仮想の脅威を表現できる ・インシデント発生時のシミュレーション上での反応と実機の反応に差が生じる可能性あり 	表 4-19 表 4-21
模擬システム演習	実際に稼動しているシステムと同じか、重要度の高い機器により構成された模擬システムを使用した演習。構築に要するコストが高く、事業者単独ではなく、政府レベルで企画されるケースが多い。	<ul style="list-style-type: none"> ・より実機に近い環境で演習を行うことができる ・システム構築費用がかかり、準備に時間を要する ・実際にウィルス等を発生させるため、インターネットには接続せず、閉じた環境で行うことになる 	表 4-8 表 4-20
実機演習	実際に稼動しているシステムを使用した演習。重要インフラ事業者ではリスクが高く、行われるケースは非常に少ない。	<ul style="list-style-type: none"> ・実際に稼動しているシステムが停止する可能性もあり、危険が伴う ・リアルな演習が行えるという点で優れている 	表 4-10

4.2.2. 国内の状況

(1) ペネトレーション・テスト

ペネトレーション・テストは、国内においても既に多くのテストが実施されている。このテスト内容に関しては、事業者個別の情報であるため触れることは難しいが、2003年9月～11月にかけて行われた住民基本台帳ネットワークシステム（住基ネット）に対するセキュリティ試験について表4-6にまとめる。

表4-6 住民基本台帳ネットワークシステムに対するペネトレーション・テスト

実施時期	2003年9月～2003年11月
実施主体	長野県（実際の作業は業者に委託）
演習の概要	インターネットから住基ネットへの侵入及びデータ改ざんの可否 町内情報通信網に接続したコンピュータや無線LANからの侵入及びデータ改ざんの可否
演習評価	総務省 住基ネットシステム調査委員会

出典：2003年9月25日付「東京読売新聞」朝刊30面

2003年12月17日付「日刊工業新聞」11面

表4-7 米電力会社におけるペネトレーション・テスト

実施時期	不明（2002年～2003年頃）
実施主体	ERCOT（Electric Reliability Council Of Texas （米テキサス地域の独立電力送電事業者））
演習の概要	ERCOTのインフラに対して、3日間に渡る“White Hat”攻撃を行う。
演習評価	トロイの木馬やウイルス、ワームから自社ネットワークを守ることができた。またDMZの使用やフィルタリング機能などの多段の防御装置が有効に機能していることがわかった。

出典：ERCOTによるプレゼン資料“ERCOT'S Defense in Depth Strategy”

(2) 緊急時対応演習

事業者における緊急時対応演習は、防災訓練の一環として「情報システムが停止した場合」「情報システムが使用不能な場合」などを対象として実施されているケースが多い。一部の事業者では、不正アタックを想定した机上演習なども実施されているが、サイバー攻撃の再現は高度な技術を要するため、「連絡体制」や「初動手順」の確立が主な目的となっている。そのような状況の中で、電力業界を対象として経済産業省が主体となって実施した「サイバーテロ演習」は先進的な取り組みとして注目に値する。

表 4-8 電力業界を対象としたサイバーテロ演習

実施時期	2004年11月～2005年2月
実施主体	経済産業省 電力中央研究所 電気事業連合会
演習の目的	実際にサイバー攻撃を受けた際の防御ノウハウの蓄積
演習形態	模擬システムを構築 (電力会社が実際に使用している、料金などを管理する事務処理系システムと電力供給を制御するシステムの一部を再現)
演習の概要	外部から招く情報システムの専門家が中心となり、コンピュータウィルスのほか様々な不正侵入の手段を駆使して、模擬システムを実際に攻撃する。

出典：2004年8月14日付「日本経済新聞」朝刊3面
2005年3月16日付「東京読売新聞」朝刊1面

4.2.3. 海外の状況

海外においては、特に米国を中心に数多くの「緊急時対応演習」が実施されている。とりわけ、「机上演習」「シミュレーションによる演習」が多いことが特長として挙げられるが、表 4-20 に示すような実機及び実際の街を用いた大掛かりな演習も行われている。また、各事業者単位で模擬システムを使用した演習も行われていることが確認されている。

(1) 米国における演習の状況

重要インフラに関して米国で実施された主な演習を表 4-9～表 4-20 にまとめる。

表 4-9 米国における重要インフラに係わる演習(The Day After)

名称	【The Day After】						
実施時期	1996年3月						
実施主体	DoD (DARPA : Defense Advanced Research Projects Agency)						
演習の目的	<ul style="list-style-type: none"> ・米国の情報セキュリティ基盤を拡充するために必要となる研究開発議案への提言作成 						
演習の概要	<ul style="list-style-type: none"> ・約60名の政府、大学、報道などの情報インフラ関係者による約半日の机上演習 ・西暦2000年に起こると想定された中東危機を背景とし、重要インフラに対してサイバー攻撃の発生を想定 ・演習のプロセス <ul style="list-style-type: none"> - "The Day of" (STEP1): サイバー攻撃の発生 - "The Day After" (STEP2): 対応策の実践 - "The Day Before" (STEP3): 攻撃による被害を最小化するために対応策を改善 ・シナリオの抜粋 <table border="1" data-bbox="432 1043 1362 1675"> <tr> <td>5 / 11 夕方</td> <td>NCC がホワイトハウスへ以下の報告を行う カリフォルニア州北部とオレゴン州の電話回線にトロイの木馬が仕掛けられ、回線が不通になった ワシントン州フォートルイスの軍事基地の基幹回線が DOS 攻撃を受け、通信システムが数時間にわたり機能不全に陥った</td> </tr> <tr> <td>5 / 20 夕方</td> <td>全米ネット及び地方ネットのイブニングニュースが、「陸軍及び海軍の LAN や電話回線がサイバー攻撃されたため、湾岸地区における米軍の活動に支障をきたしている」と報道</td> </tr> <tr> <td>5 / 24 午後</td> <td>ワシントンで緊急に国家安全保障会議が開催されることになったが、電話回線が不通のため、大統領は関係者を招集できない</td> </tr> </table> 	5 / 11 夕方	NCC がホワイトハウスへ以下の報告を行う カリフォルニア州北部とオレゴン州の電話回線にトロイの木馬が仕掛けられ、回線が不通になった ワシントン州フォートルイスの軍事基地の基幹回線が DOS 攻撃を受け、通信システムが数時間にわたり機能不全に陥った	5 / 20 夕方	全米ネット及び地方ネットのイブニングニュースが、「陸軍及び海軍の LAN や電話回線がサイバー攻撃されたため、湾岸地区における米軍の活動に支障をきたしている」と報道	5 / 24 午後	ワシントンで緊急に国家安全保障会議が開催されることになったが、電話回線が不通のため、大統領は関係者を招集できない
5 / 11 夕方	NCC がホワイトハウスへ以下の報告を行う カリフォルニア州北部とオレゴン州の電話回線にトロイの木馬が仕掛けられ、回線が不通になった ワシントン州フォートルイスの軍事基地の基幹回線が DOS 攻撃を受け、通信システムが数時間にわたり機能不全に陥った						
5 / 20 夕方	全米ネット及び地方ネットのイブニングニュースが、「陸軍及び海軍の LAN や電話回線がサイバー攻撃されたため、湾岸地区における米軍の活動に支障をきたしている」と報道						
5 / 24 午後	ワシントンで緊急に国家安全保障会議が開催されることになったが、電話回線が不通のため、大統領は関係者を招集できない						
演習の結果	分散型の適応型セキュリティアーキテクチャ、早い回復力を有する戦略とシステム構築を提言						

出典：産業構造審議会情報セキュリティ部会報告書・情報セキュリティ総合戦略策定研究会報告書 情報セキュリティ総合戦略 世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上、(2003年10月10日 経済産業省)

表 4-10 米国における重要インフラに係わる演習(Eligible Receiver)

名称	【Eligible Receiver】
実施時期	1997年6月 3ヶ月の準備期間の後に約2週間の攻撃を実施
実施主体	NSA
演習の目的	<ul style="list-style-type: none"> ・アメリカ国内のすべての電力システム及び電話のシステムのスイッチを切る方法を見つけること ・国防省の中にあるコンピュータシステムに不正侵入を試みること
演習の概要	<ul style="list-style-type: none"> ・NSAのスタッフ35人がハッカーに扮し、合衆国内の3チームと太平洋上の船舶を拠点とする1チームの計4チームが実際にサイバー攻撃を実施
演習の結果	<ul style="list-style-type: none"> ・攻撃の成果 <ul style="list-style-type: none"> - 米国9つの市の送電網に侵入し、スイッチを切るサインを残した - DoDのネットワークへの侵入に成功した回数が36回 (スーパーユーザとしてアクセス権を得た) - DoDのシステムへの侵入のうち、DoDのシステム管理者が検知できたのは2回 ・演習後の対策(国防省) <ul style="list-style-type: none"> - コンピュータネットワークの24時間監視体制の確立 - 800あるネットワークすべてにIDS及びファイアウォールを設置 - コンピュータ犯罪について研究するための研究所の設置 - 最も機密性の高いネットワークに対する公開鍵インフラの整備

出典：産業構造審議会情報セキュリティ部会報告書・情報セキュリティ総合戦略策定研究会報告書 情報セキュリティ総合戦略 世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上、(2003年10月10日 経済産業省)

なお Eligible Receiver に関しては、民間ネットワークを直接テストしたものではないとの情報もある。

表 4-11 米国における重要インフラに係わる演習(Zenith Star)

名称	【Zenith Star】
実施時期	1999年10月13日～1999年10月14日の2日間
実施主体	IATAC (Information Assurance Technology Analysis Center)
演習の目的	<ul style="list-style-type: none"> ・ Computer Network Defense (CND) コミュニティが、組織間の調整等、その目的を達成するために必要となるプロセスと道具の洗い出し
演習の概要	<ul style="list-style-type: none"> ・ Eligible Receiver をベースに実施された机上演習 ・ 演習のプロセス <ul style="list-style-type: none"> - Eligible Receiver をベースに新CND組織化のルールや役割分担を理解する - Agency 間の要求事項の理解 - JTF-CND(Joint Task Force CND)と他のサポート機関 (例えば NIPC、Intel) に対する調整活動の試験 - 各チーム (インテリジェンス、法の執行、カウンターインテリジェンス、オペレーション) によって指摘されたポイントの改善・演習の構造 - 参加者は、機能的な4チームに分割された政府関係者55名 * Operations チーム (SPACECOM、JTF-CND 及びそのコンポーネント) * インテリジェンスチーム (CIA、DIA、NSA) * 法執行・スパイ防止活動チーム (Defense Criminal Investigative Operations、NIPC) * 他のチーム (Joint Staff、国防長官の[OSD]のオフィスチーム) <ul style="list-style-type: none"> - チーム間のコミュニケーションツールは安全な電話ユニット、STU- 、 Face to Face、ファックスと電子メールに限定

出典：産業構造審議会情報セキュリティ部会報告書・情報セキュリティ総合戦略策定研究会報告書 情報セキュリティ総合戦略 世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上、(2003年10月10日 経済産業省)

表 4-12 米国における重要インフラに係わる演習(Top Officials)

名称	【Top Officials】
実施時期	2000年5月
実施主体	DoS、米司法省（DoJ：Department of Justice）
演習の目的	<ul style="list-style-type: none"> ・大量破壊兵器（WMD：Weapons of Mass Destruction）による攻撃の様々な面に対する、効果的で協調的な戦略的対応を米国内外で行えるようにする ・危機管理において、従来の協調関係にはないような各組織の役割を調査し強化する ・連邦政府、州、各地域の危機管理システムをより幅広く運用するフレームワークを構築する ・権限、戦略、作戦、方針、手順、手段及び連携能力を有効的なものにする ・米国内における事前の戦略及び国際的な対応戦略をサポートするための継続的で系統的な演習プログラムを作成する
演習の概要	<ul style="list-style-type: none"> ・デンバー、コロラド、ポーツマス、ニューハンプシャーで実施。 ・連邦政府、州政府、及び各地域の危機管理を担当する職員が参加しWMDによる攻撃への対応を、ロールプレイングにより訓練した ・WMDによる攻撃の発生時に、以下のような様々な問題を関係者で協調して対応する <ul style="list-style-type: none"> 「法の執行」「国家安全保障」「重要インフラ防護」「情報公開」 「指揮統制」「危機管理マネジメント」「医療と健康」「資源管理」 ・デンバーでは化学攻撃に対するシミュレーションも行った ・ニューハンプシャーではバイオ攻撃への対応も行った
コメント	この3年後にTop Officials2が行われる（表4-18参照）

出典：米國務省（DoS：Department Of State）ホームページより

（2005年2月21日現在）

（URL：<http://www.state.gov/s/ct/rls/fs/2002/12129.htm>）

表 4-13 米国における重要インフラに係わる演習(Black Ice)

名称	【Black Ice】
実施時期	2000年11月
実施主体	<ul style="list-style-type: none"> ・ユタ州 ・スポンサー DoE、Utah Olympic Public Safety Command
演習の目的	<ul style="list-style-type: none"> ・2002年の冬季オリンピック(ソルトレークオリンピック)に備えたもの ・重大なテロ攻撃や自然災害による影響が、コンピュータへの同時サイバー攻撃によっていかに拡大されるかということを実証するため
演習の概要	<ul style="list-style-type: none"> ・演習参加者 連邦、州、地元自治体、民間など225名以上 ・演習のシナリオ：電力網の大規模な混乱 2002年2月14日(ソルトレークオリンピックの第2週)に始まる。 大規模な暴風雪がユタ州の七つの郡にまたがる電線を倒し、ソルトレークシティ周辺のマイクロ波通信が使えなくなる。また、ソルトレークシティの南北にある送電線と、複数の州に高圧送電線にも被害が出る。 送電システムの被害はそれほど大きくはないが、七つの郡に電力を送る能力は著しく低下し、電力不足により計画停電の実施を余儀なくされる。計画停電が始まると共に、電力網をコントロールするSCADAシステムがサイバー攻撃により広い障害が出る。その原因がハッカーなのか、テロリストなのか、内部犯行か、暴風雪によるダメージなのかは不明。
演習の結果	<ul style="list-style-type: none"> ・数時間以上の停電により、電力に依存するインフラすべてのパフォーマンスとサバイバビリティ(生存性)が低下することが判明 ・最初に電気通信ネットワーク、そして水道システム、天然ガス産業、天然ガス発電設備、インターネット、携帯電話、一般電話に障害をもたらしていく

出典：ダン・バートン著 星睦訳 「ブラックアイス サイバーテロの见えない恐怖」(2003年10月11日 インプレス)

表 4-14 米国における重要インフラに係わる演習(Dark Winter)

名称	【Dark Winter】
実施時期	2001年6月22日～23日
実施主体	戦略国際問題研究所(CSIS)、ジョンズ・ホプキンス大学
演習の目的	米国でバイオテロが発生したと想定した際に、州及び地方政府の対応、連邦政府の責任についてシミュレーションし、大統領役などに扮した現職又は元政府高官の対応を訓練する
演習の概要	<ul style="list-style-type: none"> ・オクラホマ、ジョージア、ペンシルベニア州の三つのショッピングセンターが天然痘による同時バイオテロ攻撃を受けたと想定 ・病院における情報通信機能の不足から、政府での情報収集が効率よく行えず、結果としてウィルス拡散防止対策が遅れることになる
演習の結果	<ul style="list-style-type: none"> ・官民の医療コミュニティを網羅する通信機能と早期警告機能を大幅に改善する必要がある ・メディアとの関係は政府のどのレベルにおいても重要であることが分かった ・医療関係は当時国家としては最もセキュリティ上重要な問題であることが分かった
コメント	2002年10月には同研究所により”Silent Vector”が実施される。(表4-17参照)

出典：CSIS ホームページより（2005年3月2日現在）

（URL：<http://www.csis.org/isp/darkwinter/index.htm>）

ダン・バートン著 星睦訳 「ブラックアイス サイバーテロの见えない恐怖」(2003年10月11日 インプレス)

2001年11月6日付「日本経済新聞」朝刊8面

表 4-15 米国における重要インフラに係わる演習(Blue Cascades)

名称	【Blue Cascades】
実施時期	2002年6月12日
実施主体	<ul style="list-style-type: none"> ・ Pacific North West Economic Region (PNWER) ・ スポンサー U.S. Navy、Federal Emergency Management Agency (FEMA Region 10) Canadian Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP)
演習の目的	<ul style="list-style-type: none"> ・ インフラ同士の結びつきが強いことに着目し、地域全体の重要インフラのセキュリティを増強するための共同戦略を構築するため
演習の概要	<ul style="list-style-type: none"> ・ 机上訓練 ・ 演習参加者 連邦、州、Bonneville Power Administration、BC Gas、BC Hydro、Boeing、Duke Energy、PG&E、Williams Gas Pipeline、Puget Sound Energy、Port of Seattle、Idaho Bureau of Disaster Services、U.S. Navy、National Infrastructure Protection Center、Telus、Verizon、Qwest、FEMA、BC Provincial Emergency Program、OCIPEP ・ 訓練対象 エネルギー（電力、石油、天然ガス）、電気通信、運輸、水道システム、金融ネットワーク、緊急サービス、行政サービスなど
演習の結果	<ul style="list-style-type: none"> ・ テロ攻撃や物理的災害により、地域の電力が数週間から数ヶ月にわたって途絶え、地域全体で停電が発生し、それが他の州にも広がる可能性を指摘。それに続き、地域の電気通信と、少なくとも二つの天然ガス輸送システムが破綻し、主要な水道システムと地域の港が麻痺すると指摘 ・ 電気通信の場合、被害をもたらすのは攻撃ではなく、長時間の停電によるシステム障害であった ・ 停電によりインターネット接続に障害が発生する事態が発生した

出典：ダン・バートン著 星睦訳 「ブラックアイス サイバーテロの見える恐怖」(2003年10月11日 インプレス)

表 4-16 米国における重要インフラに係わる演習(Digital Pearl Harbor)

名称	【Digital Pearl Harbor】
実施時期	2002年7月24日～2002年7月26日
実施主体	<ul style="list-style-type: none"> ・ Gartner ・ U.S Naval War College
演習の目的	<ul style="list-style-type: none"> ・ 重要インフラへのサイバー攻撃の実行可能性とそれによるダメージの程度を見極める
演習の概要	<ul style="list-style-type: none"> ・ 主催者から仮想シナリオ（予算、準備期間、人的ソース等）が与えられる ・ 仮想シナリオに基づいて、電力網システム、通信インフラストラクチャ、インターネット、金融サービスのそれぞれに対して、コンピュータセキュリティの専門家が4つのチームに分かれて攻撃手法を検討する ・ 実際にシステムに対して攻撃を実施するのではなく、実行可能な攻撃法と、攻撃が成功した場合に生じると予想されるダメージを机上で考察する
演習の結果	<ul style="list-style-type: none"> ・ 電力網システム SCADA システムから侵入して攻撃を実施することが可能であるが、実現性は低い ・ 通信インフラストラクチャ 攻撃に必要な情報が内部者以外には入手困難であることから、攻撃の実現性は低い。また内部者による攻撃が成功した場合でも、システムの冗長性によりダメージは限定される ・ インターネット peer-to-peer のファイル共有技術と同様の技術を用いた攻撃手法には現実性がある ・ 金融サービス 攻撃者がバックアップファイルをどれだけ破壊できるかによって、システムに重大なダメージを引き起こさせるかどうか決まる。インターネットチームが考案した攻撃手法を用いれば、バックアップファイルの破壊も可能

出典：産業構造審議会情報セキュリティ部会報告書・情報セキュリティ総合戦略策定研究会報告書 情報セキュリティ総合戦略 世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上、（2003年10月10日 経済産業省）

表 4-17 米国における重要インフラに係わる演習(Silent Vector)

名称	【Silent Vector】
実施時期	2002年10月17日～18日
実施主体	戦略国際問題研究所(CSIS)、ANSER 国土安全保障研究所
演習の目的	<ul style="list-style-type: none"> ・米国東海岸の重要なエネルギー関連施設やインフラに対して、2日後に大規模な攻撃が行われるという確かな情報が入手できた際に、これらの施設を防御するための情報が限られている中で、現職又は元政府高官がどのような行動を取るのかを演習する ・上記のような問題が生じた際の、メディアに対する新たな情報開示の手法を検討する ・政府の現在の情報収集システムが抱える欠点を明らかにする
演習の内容	<ul style="list-style-type: none"> ・大統領役、補佐官役、などの役割を、現職又は元政府高官が演じる ・参加者は、予想された攻撃に対する脅威分析、脆弱性の特定、発生した場合のインパクトを検討するとともに、対応プランを作成するために必要な情報や法律的なデータを収集した ・参加者は、想定される脅威があまりにもあいまいで、特別な対策を施すのは難しいと判断したが、警告レベルが次第に高まってきたため、一般的な防御策を行うことにした。 ・このことがメディアにリークされ、原子力発電所などのエネルギー関連施設周辺の住民がパニックに陥った ・結果として、参加者はより効果の高い対策を行うのか、このまま住民のパニックを放置するのかなかの決断を迫られた ・結局大規模攻撃は行われなかったが、参加者はこの情報がウソだったのか、それとも攻撃が遅れているだけなのかの判断を迫られた

出典：CSIS ホームページより（2005年3月2日現在）

（URL：<http://www.csis.org/isp/sv/>）

表 4-18 米国における重要インフラに係わる演習 (Top Officials2)

名称	【Top Officials2】
実施時期	2003年5月12日(午後3時に開始し5日間行う)
実施主体	DHS、DoS
演習の目的	<ul style="list-style-type: none"> ・ 非常事態に適切に対処するための能力の改善 ・ より専門性の高い危機管理システムのための幅広いフレームワークの構築 ・ 有事の際の権限、戦略、作戦、方針、手順、及び手段の有効性を確立する ・ 国土安全保障のための国家戦略をサポートするために、継続可能で系統的な演習プログラムを作成
演習の概要	<ul style="list-style-type: none"> ・ 19の連邦政府機関、イリノイ州、ワシントン州及びカナダ(ブリティッシュコロンビア州、バンクーバー市)の州及び地元の緊急時対応機関が参加し(一部の参加者は5日間の演習のうち初日のみ)、大量破壊兵器(WMD: Weapons of Mass Destruction)による攻撃を起きた場合に、国としてどのように対応すべきか訓練し、シミュレーションする ・ 演習シナリオ、損害の規模、脅威のレベルは仮定に基づいたものであり、将来のテロリストの攻撃を予測するものではないが、現状での米国に対する脅威を反映したものである
コメント	<ul style="list-style-type: none"> ・ 2005年4月にTop Officials3の計画があり、英国の支援を受け、コネチカット州及びニュージャージー州にて実施予定 ・ Top Officials4はアリゾナ州フェニックス及びオレゴン州ポートランドにて実施予定

出典：FEMA (Federal Emergency Management Agency) ホームページより

(2005年2月21日現在)

(URL: http://www.fema.gov/nwz03/nwz03_topoff2.shtm)

警察庁ホームページより(2005年3月14日現在)

(URL: http://www.cyberpolice.go.jp/international/north_america/20050310_211347.html)

表 4-19 米国における重要インフラに係わる演習(Livewire)

名称	【Livewire】
実施時期	2003年10月(5日間実施)
実施主体	Dartmouth 大学 ISTS (Institute for Security Technology Studies)
演習の目的	2003年にホワイトハウスにより発行された”The National Strategy to Secure Cyberspace”に記載されている「国家サイバーセキュリティ・レスポンスシステム」 ¹⁶ に必要な要件を特定すること。
演習の概要	<ul style="list-style-type: none"> ・金融、ユーティリティ、通信といった相互依存性のある重要インフラに対して、高度で十分な資金力がある攻撃者により30日間に渡るサイバー攻撃が行われたと想定(30日間分のイベントを5日間に短縮して実施) ・コンピュータ上に、参加組織の実際のネットワークをシミュレーション・モデルとして構築し、参加者に現実的で効果的な意思決定を行うリーダーと技術スタッフを配置してもらった(実際のネットワーク資産は一切使用されていない。つまりすべてシミュレーションとして実施) ・人的な緊急時対応に重点を置いた演習 ・エネルギー、金融、通信など50のプライベートセクターと、14地域の連邦、州政府関係者が約300人参加
演習の結果	連邦政府も含めた参加者の間では、サイバー攻撃によってもたらされる、複雑で変化の激しい状況に対応すべく、対応手続きの方法や規約の改正が始まった。
コメント	一部の事業者がシナリオの内容に不満を示し、演習の直前になって参加を辞退している。これは、演習シナリオの作成過程において、Dartmouth 大学のみで行い、事業者の参加を認めなかったことに起因している。

出典：ISTS Quarterly volume1, Number1, Spring 2004 (Dartmouth University)

¹⁶ サイバー攻撃を防御し、その影響の軽減、サービスの即時復旧のために、様々な組織における分析能力とインシデント対応能力を同等に高めるためのシステム

表 4-20 米国における重要インフラに係わる演習 (SCADA TEST)

名称	(SCADA TEST)(正式名称ではない)
実施時期	2003 年 ~ (8 年間の予定)
実施主体	SNL (Sandia National Laboratory) INEEL (Idaho National Engineering and Environmental Laboratory)
演習の目的	様々なメーカーが提供している電力会社向け SCADA(Supervisory Control And Data Acquisition)システムを一つ一つテストし、セキュリティ上問題がないか確かめる。結果をメーカーにフィードバックし改善を促す。
演習の概要	<ul style="list-style-type: none"> ・ INEEL が保有するアイダホの実験施設を使用。この施設は 1950 年頃原子力エネルギー政策をサポートする目的で作られ、その後送電線や事務所などが周辺に作られた。現在では研究所や事務所、高圧グリッド、原子炉、様々な無線、有線通信システムが存在し、施設関係者が実際に居住するなど、一つの街の機能を果たす。電力網は外部と全く遮断され、電力自給が可能な環境のため、この施設で発生した障害が外部の電力供給環境に影響を及ぼすことはない ・ 各メーカーの SCADA システムを一つずつインストールし、セキュリティ上の問題が発生した際に、SCADA にどのような問題が生じ、電力供給にどのような影響が発生するのかを実機ベースでテストする ・ 8 年間の計画で予算は 11,400 ドル

出典 : New Scientist Magazine (Saturday, May 15, 2004)

(2) 欧州における演習の状況

欧州においても、重要インフラに関する演習が実施されたとの情報がある。しかしその多くは未確認の情報であり、本報告書で記載するに十分な情報が得られていない。これら演習に関する情報が未確認である理由の一つとして、演習に関する費用が参加する事業者により負担されており、演習の結果はもとより、演習が実施されたという情報そのものが参加した事業者内でクローズされていることが指摘されている。

以下では、その中でも比較的確かな情報が得られている演習に関する状況を述べる。これは2001年にドイツで実施されたサイバーテロ演習である。

表 4-21 CYTEX

名称	【CYTEX】(CYber Terror EXercise at IABG)
実施時期	2001年11月12日～2001年11月14日
実施主体	IABG社 (1961年にドイツ政府によって設立された、航空業界と国防省のための分析・試験機関。現在は科学技術のサービスプロバイダ)
参加企業	<ul style="list-style-type: none"> ・ Federal Ministry of the Interior / German Information Security Agency (内務省情報セキュリティ室) ・ Federal Ministry of Economic Affairs (経済省) ・ Federal Ministry of Defense / Federal Office of Defence Technology and PBWB (国防省防衛技術室) ・ the Federal Academy for Security Policy ・ Police (警察) ・ Telekom (通信事業者) ・ der DFS, Deutsche Bundesbahn (鉄道事業者) ・ an energy facility(E.ON) (総合エネルギー会社：電力関連) ・ TÜV (セキュリティ産業) ・ EADS (主要産業の代表として参加)
演習の目的	ITシステムが攻撃を受けた際の状況評価と対応策の作成
演習の概要	連邦政府に対して揺さぶりをかけることを目的に、ベルリンに設置されている参加者の支店のITシステムに対して、国内外から攻撃が加えられたことを想定とした演習。上記参加企業から40名以上が参加。
演習の結果	<ul style="list-style-type: none"> ・ インフラ全体及び社会生活、産業界の一部の機能、そして政治的な活動が完全に停止されてしまうことが分かった ・ 通信トラフィックや銀行のトランザクションのキャパシティ、エネルギー施設や鉄道、航空は機能しつづけることができたが、大きなイベントは中止され、パニックが生じ、多額の経済損失が発生することが判明した ・ シナリオを習得するにあたって、インフラ間での協力が不可欠であった <p>以上のような状況を受けて、連邦政府により何が必要なのかが決定され、組織的、物質的な準備が整えられた。</p>

出典：IABG社ホームページより(2005年3月2日現在)

(URL：http://www.iabg.de/presse/aktuelles/mitteilungen/200111_cyber_terror_exercise_en.php)

4.2.4. 今後求められる演習のあり方

今後重要インフラに求められる演習のあり方について、以下に述べる。

(1) 緊急時対応演習の推進

これまでも、「ペネトレーション・テスト」は多くの事業者で既の実施されていると考えられ、これに基づくセキュリティ対策はかなり高いレベルに達しつつある。しかし「ペネトレーション・テスト」は実際に起きたインシデントに基づいて行われているケースが多く、過去の脅威に対しては有効に作用するが、未知の脅威に対する防御力が弱い。一方「緊急時対応演習」では、実際に演習をする以前の「シナリオ作成」というプロセスが重視されており、過去に起きたインシデントは当然のこと、今後起こると想定されるインシデントも含めた検討が参加者間で行われている。

こういった「今後起こり得るインシデント」には、現状では技術的に発生不可能と考えられていても、今後起こり得ると考えられているものも含まれており、机上演習やシミュレーションを活用して模擬的に発生させている。「インシデントは発生する」という前提のもとで、過去及び今後想定されるインシデントを体験し、事業継続性を考慮した上で、実際に起きた場合に何をすべきか、適切な処理が行えるかを確認する、防災訓練的な形態の演習の実施が求められる。

(2) 複数業界の参加による演習の実施

3.3 でみてきたように、重要インフラは相互間で依存する部分が存在する。このことは、あるインシデントが発生した際に、一つの業界だけではなく関連する複数の業界が協力して対処する必要があることを表している。米国や欧州においては、複数の重要インフラが参加した演習が実際に行われており、(1)で触れた演習におけるシナリオの作成過程においても、複数の業界で行うことにより、より効果的なシナリオを作成できると考えられる。国内においても、複数業界が参加した形での演習の実施が求められる。

(3) 演習に関する情報の共有化

演習を実施する際に、「シナリオ作成」の過程が重視されていることは(1)で触れた。しかし一方で、この過程が演習を実施する際に最も労力の要する過程であることも指摘されている。米国においては、このシナリオ作成の過程が十分ではないために、参加者の同意を得られなかったケースも報告されている。多分に、どのような枠組みで演習を実施するにせよ、このシナリオの多くは共通のものであると考えられる。過去の演習シナリオを共有化し、より効率的な演習実施に向けた制度作りが求められる。

4.3. セキュリティに係わる標準策定の推進

4.1、4.2 で述べた施策は、その実行もさることながら、そこから得られた知識・経験を業界に根付かせるべくセキュリティ標準の策定が重要となる。国内においては、後述する「ISMS 適合性評価制度」などが定着しているが、マネジメント面に重点がおかれており、「実際に何をすべきか」が書かれていないといった指摘もある。そこで本節では 4.1 及び 4.2 の実施により得られた情報を元に、「実際に何をすべきか」を特定したセキュリティ標準の策定について、国内外の状況をまとめると共に、今後の方向性を提言する。

4.3.1. 国内の状況

国内で主に採用されているセキュリティに係わる標準等について以下に述べる。

(1) ISMS (Information Security Management System) 適合性評価制度

我が国では昭和 56 年より、情報処理システムが十分な安全対策を実施しているかどうかを認証する制度として、通商産業省告示 342 号による「情報システム安全対策実施事業所認定制度」(以下、安対制度という)があった。安対制度では、情報処理施設が設置された設備における物理的な安全対策(火災対策など)がメインであり、技術面や人的面での対策に関してはあまり触れられていなかった。

そこでこれらを総合的にマネジメントする制度が必要とされるようになり、経済産業省では従来の安対制度を廃止し、英国標準である BS7799 を元に作成された ISMS を利用した評価制度を創設した。

ISMS では技術的及び組織全体のマネジメントに対して第三者が評価する。国際的な信頼を得た基準であるが、実際に何をすべきか、という点に関しては採用する事業者にゆだねられている。

(2) 金融機関等コンピュータシステムの安全対策基準

FISC において金融業界等の合意のもと、金融機関等の自主基準として策定された。その後 4 回の改訂を経て、現在まで金融情報システムに関する安全対策の共通のよりどころとして活用されている。

最新版では、安全対策に関する経営層の関与、コンティンジェンシープランの重要性、アウトソーシングへの対応、サイバーテロの脅威、設備関連技術の進展、関連ガイドライン等との整合性、コンピュータ関連事故・犯罪動向等に関する記述等、ISMS よりもかなり幅広く記載されており、金融情報システムに関する安全対策の具体的指針となっている。

(3) 地方公共団体における情報セキュリティポリシーに関するガイドライン

地方公共団体において情報セキュリティ対策を推進するために必要となる、セ

セキュリティポリシーに関する基本的な考え方、策定、運用及び見直し方法について記述したものの。基本的な構成は国におけるガイドラインに準拠している。

(4) ITIL (IT Infrastructure Library)

英国政府が「IT を活用して業務の遂行を適切に手助けする」ための方法論をまとめたもので、非営利団体である itSMF(IT Service Management Forum)が普及・啓発を行っている。システム運用に係わる業務全般を整理・体系化した「お手本」のようなものであり、ベストプラクティス集である。ISO などの基準をクリアするためのプロセスを記したものであり、厳密に言えば基準とは異なるものであるが、実際のところ、セキュリティ管理に関する項目も含まれている。重要インフラ事業者においても、採用もしくはプロセス改善のために参考にするケースが増えてきている。

4.3.2. 海外の状況

海外で主に採用されているセキュリティに係わる標準等について以下に述べる。

(1) 国際標準

ISO/IEC に代表される国際標準は、主に欧州・アジアを中心に採用されている。重要インフラのセキュリティに係わる国際標準を以下に示す。

(a) ISO/IEC 17799 (BS7799 Part1, JIS X 5080)

英国標準である BS7799 の Part1 が ISO によって国際規格化されたもの。「情報システム」と情報システム上でやり取りされる「情報」とを包含した広い範囲の情報セキュリティの管理基準である。10 の主な大項目と約 130 の中項目に区分けされた要求事項を定めている。

(b) 制御機器一般 (IEC61508)

IEC61508 は制御機器一般に当てはまる規格であり、主に欧州で採用されている。また国内でも JIS-C0805 として登録されている。これは工作機器や化学プラントなど「コンピュータ制御機器」の安全上の働き、つまり安全機能を、電気/電子/プログラム可能な「電子系」で構成する場合の遵守事項を定めた国際規格である。計装を使った安全装置の信頼性をいかに維持するかを定めた国際規範であり、設計から保守、廃棄に至るまでの全安全ライフサイクルに適用される。

この中で、安全度水準 (SIL) というものが定められており、4 段階の規定がなされている。これは基準とする許容リスクまでのリスク遞減量を示しており、業界レベル或いは企業レベルにおいて、目標とする許容リスクを定めるものである。

(c) 鉄道 (IEC62278 ~ 62280、EN50129)

IEC62278 ~ 62280 は、(b)で触れた IEC61508 をベースとし、国際鉄道連合 (UIC : International Union of Railways) の技術指針や各国の鉄道信号システムの技術要件を組み込んだものである。また、EN50129 は現在欧州規格だが、今後 IEC 規格として提案されると考えられている。以下に詳細を述べる。

(i) IEC62278 : Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS) (信頼性、可用性、保守性、安全性に係わる規格)

本規格は、鉄道の安全に係るシステムを開発・運用していく際の、信頼性(Reliability)、可用性(Availability)、保守性(Maintainability)、安全性(Safety)、及び経済性に関するマネジメントの規格であり、IEC61508 で導入された「安全性のライフサイクル」「安全性インテグリティレベル(安全度水準 : SIL)」の概念が反映されている。

IEC62278 は、地上・車上を問わず、鉄道の構成要素となるシステムのうち安全性に少しでも関係があり、且つ、この規格発効以降に新設された路線や延伸区間の設備、及び既設線区内で大規模改修を受ける設備、さらには新規開発製品、大きな設計変更を受けた製品の全てが適用対象となっている。

但し、本規格には、適用対象システムの位置付けや、範囲に関する規定が無く、適用対象が広域で大規模なシステム全体の場合もあれば、1 台の装置の場合もありえる。また、鉄道事業者や鉄道関連システムメーカーがそれぞれ単独に、また合同で準拠することとなる。

(ii) IEC62279 : Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems (制御及び防御システム用ソフトウェアに係わる規格)

本規格は、鉄道信号におけるソフトウェアの安全性規格であり、
ソフトウェアのライフサイクルにおける安全性確保のための要求事項

その要求事項が満たされていることを明らかにするプロセス、を規定している。具体的な規定内容を以下に示す。

- ・ の要求事項を明らかにするために必要な方法と管理
- ・ 作成すべき書類
- ・ のプロセスにおける関係組織と関係者の役割及び資格

- (iii) IEC62280 : Railway applications - Communication, signalling and processing systems : Safety-related communication in open/closed transmission systems (オープン又はクローズドな通信システムの安全性に係わる規格)

本規格は 2 部からなる鉄道信号における安全関連伝送 (通信) の規格である。表 4-22 に IEC62280 の主な内容を示す。

表 4-22 IEC62280

	第 1 部 (IEC62280-1)	第 2 部 (IEC62280-2)
対象	従来からの物理的に独立した専用の有線回線	無線やインターネットなどを中心とする物理的に独立になっていない伝送回線
内容	伝送における安全性を確保するために必要な 18 の技術要件を規定 ・通番管理 ・チェックコードによる伝送誤り検出 など	セキュリティ上の危険について解析することを求めており、必要なセキュリティ対策を実施することを規定 ・発信元の特定 ・暗号の使用 など
特徴	日本の鉄道信号において広く採用されている安全性技術と変わりはない	故意の妨害などに対して、より厳格なセキュリティ対策を規定している

- (iv) EN50129 : Railway applications – Safety related electronic systems for signalling (信号に関する電子システムの安全性にかかわる規格)

本規格は、信号システムの承認および受け入れのための必要な安全性要件 (信頼性管理、安全性管理、機能及び技術的安全性) とその書類管理について規定したものである。この文書による安全性の立証をセーフティケースと呼び、本規格の中心概念となっている。

また本規格は、安全性に特に重点をおく鉄道信号を対象としたものであるため、安全性インテグリティレベル (安全度水準 : SIL) と許容リスクの値を定めているが、ヨーロッパ内でも国ごとに事情が異なるため、現実的な対応として、安全性インテグリティの決定方法については特に定めていない。また、安全性の検証、妥当性検査、承認についても、その実施組織は明記されていない。

(2) 米国の状況

米国では、各業界に特化した標準が策定されているのが特長である。逆に(1)で述べたような国際標準は、参考にはされているもののそのままの形では適用されていない。主な業界別標準を表 4-23 に示す。

表 4-23 米国における業界別標準 (1 / 2)

業界	標準名	内容
制御システム	ISA SP99 (the Instrumentation, Systems, and Automation society)	ISA (国際計測制御学会) は、SP99 (制御システム・セキュリティ規格委員会) を設置し、製造 / 制御システムのセキュリティに関する技術報告書 2 編を刊行している。両報告書は定期的に更新されており、第 1 編(TR1)では、現在のセキュリティ技術やツールが評価され、第 2 編(TR2)では、セキュリティの改善・管理の取り組みが列挙されている。なお現在、製造システムに特化したセキュリティを扱う第 3 編の発行が予定されている。
電力	CSS1200 (Cyber Security Standard)	NERC が制定した米国の電力業界向けセキュリティガイドラインの一部。BS7799 等を元に作成された。セキュリティガイドラインはベストプラクティスとして書かれているためレベルはかなり高く、必ずしも全ての事業者が守れるものではない。しかし CSS1200 では、電力事業者が守るべき 16 の最低限必要な事項がかかれており、守られていない場合にはペナルティが課される制度となっている。「セキュリティポリシーの策定」「重要サイバー資産の特定」「サイバー / 物理アクセスコントロール」「職員のチェック」「サイバー / 物理アクセスのモニタリング」「情報保護」「訓練」「システムマネジメント」「試験方法」「サイバー / 物理インシデント発生時の対応」「復旧プラン」で示されるそれぞれの項目に対しては、対処方法や適用範囲、地域による特性、及び事業規模などによる達成レベルが記載されている。米国の電力事業者は事業規模が大小様々なため、事業規模による達成レベルを制定している点に特徴がある。なお現在では、適用範囲を広げ内容をブラッシュアップした CSS1300 の策定が行われている。

表 4-23 米国における業界別標準 (2 / 2)

業界	標準名	内容
ガス	AGA12 (American Gas Association)	<p>AGA が、ガス会社が使用する SCADA システムと DCA (Distributed Control Systems)を保護する目的で策定したガイドライン。主な目的を以下に示す。</p> <ul style="list-style-type: none"> ・ SCADA 使用者が、自社の特性に合った SCADA サイバーセキュリティ・ソリューションを選ぶ際に、セキュリティ上必要とされる事柄を確認する ・ システム・インテグレータが、SCADA サイバーセキュリティを的確に捉え、製品テスト時にセキュリティ上必要な要件をすべて満たせるようにする ・ SCADA を構成するハード、ソフト、ファームウェアがこの標準を満たすことにより、SCADA 製品が提供する機能が、SCADA サイバーセキュリティにおけるオープン・スタンダードとなることを目指す
	CSCSP (Chemical Sector Cyber Security Program)	<p>化学業界全般のサイバーセキュリティを改善するプログラムであり、ガス業界も一部含まれる。CIDX(Cheical Industry Data Exchange)がサイバーセキュリティ・グループを設置し、CSCSP における 5 つの活動分野のうち 2 つ (実施方法と規格、技術とソリューション開発) に取り組んでいる。化学分野のサイバーセキュリティに取り組む戦略 / ガイダンス文書が作成され、現在も作業が続けられている。</p>
政府	FIPS (Federal Information Processing Standards)	<p>米国連邦政府における情報処理標準。NIST (National Institute of Standards and Technology)が発行している。米国連邦政府では、FIPS で定められたアルゴリズムが存在する場合、原則としてはそれを用いなければならないと定められているので、実質調達要件となっている。暗号技術など、コンピュータセキュリティに関する標準を多数定めている。</p>

4.3.3. 今後求められるセキュリティに係わる標準のあり方

今後求められるセキュリティに係わる標準のあり方について、以下に述べる。

(1) セキュリティに係わる標準のブラッシュアップ

セキュリティの確保においては、常に技術の発展との攻防が繰り返されてきた。これまで多くのセキュリティ対策が施され、その度にそれを上回る技術が開発されてきた。セキュリティに係わる標準も、こういった技術の発展に伴ってブラッシュアップされていく必要があると思われる。4.1 で述べた情報共有、及び 4.2 で述べた演習におけるシナリオを元に、セキュリティに係わる標準を常に見直す体制を整える必要がある。

(2) 業種別セキュリティスタンダードの検討

4.3.2 でみてきたように、欧米においては業種別のセキュリティ基準が制定されている。これは各業界の特長を反映させて作られたものである。例えば、NERC が制定した米国の電力会社に適用した基準では、通信に関する部分は適用対象外とされている。これは、米国の電力会社の多くが、通信網を通信会社から借用しており、電力会社が通信網のセキュリティにまで関与できないという業界事情を反映している。

全く逆の状況であるが、同様の考え方が国内の事業者においても適用できる。例えば、国内の電力会社は通信に全て電力会社の自社網を使用している。このような状況においては、この通信網に対して不正アクセスが発生する可能性は非常に少ない。よって適用する基準に対しても、通信部分の不正アクセスは省略することが可能であると考えられる。

一方鉄道関連の国際規格である IEC62280 では、通信に関して専用線を使用した場合とインターネットを使用した場合の 2 通りを定めている。これは一部の事業者が制御用の通信にインターネットを使用していることを反映させたためと考えられる。このように、通信一つを取り上げても、業界によって標準の定め方は様々である。

業種別セキュリティスタンダードでは、業界の状況に合わせた標準の策定が可能であると言える。場合によっては、不必要な部分を省略しスリムな基準を適用する事により、事業者における円滑なセキュリティ対策の実施を推進していくことも検討に値する。

5. 国家情報セキュリティセンター（仮称）の位置付けと役割に係わる弊社の提言

「情報セキュリティ基本問題委員会」の第1次提言では、「国家情報セキュリティセンター（仮称）」の創設が提言された。そこで本章では、重要インフラ分野での情報セキュリティ対策として、「国家情報セキュリティセンター（仮称）」に求められる位置付けと役割について、弊社の提言を述べる。

5.1. 国家情報セキュリティセンター（仮称）の位置付け

図5-1に弊社が想定する「国家情報セキュリティセンター（仮称）」の位置付けを示す。この図では、特に以下の3点について着目したい。

- ・重要インフラ事業者に対するセキュリティパスの強化
- ・重要インフラ分野の拡大と相互依存性を考慮した階層化
- ・国家情報セキュリティセンター（仮称）への評価機関の設置

以下では上記3点について具体的に説明する。

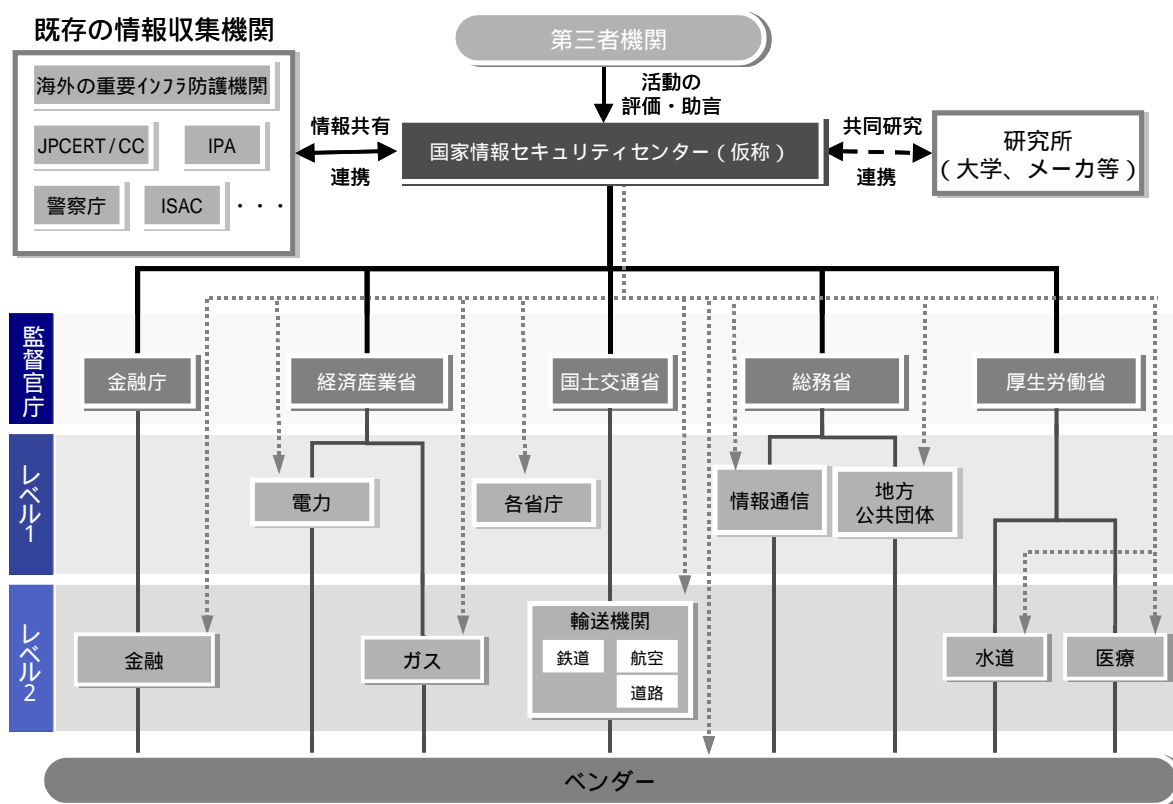


図 5-1 国家情報セキュリティセンター（仮称）の位置付け

5.1.1. 重要インフラ事業者に対するセキュリティパスの強化

これまで、政府の重要インフラ事業者に対するアプローチは、監督省庁を經由して行われてきた。しかしこういったアプローチでは、セキュリティ面においては、重大なインシデントが発生した際に迅速な処置が行えない可能性が懸念される。

また 4.1.4(a)(b)で述べた「幅広い情報の結集」「情報管理の一元化」や、4.2.4(2)で述べた「複数業界の参加による演習の実施」を「国家情報セキュリティセンター（仮称）」が実現していくにあたっては、事業者各社に対して直接やり取りのできるルートを確保することが必要になると考えられる。

5.1.2. 重要インフラ分野の拡大と相互依存性を考慮した階層化

現在、重要インフラの対象として本報告書で取り上げた7分野が指定されているが、これ以外にも「道路」「水道」「医療」などは、特にインシデント発生時の「インフラの確保」「防護すべきインフラ」という観点から、重要インフラに加えるべき分野として考えられる。

しかし、重要インフラの対象分野が増えるということは、限られた資源（人・物・金）が分散化してしまう可能性がある。そこで、重要インフラの中においてもレベル分けを行い、より重要度の高い分野については資源を優先的に配分していく必要がある。3.3でも指摘したように、多くの重要インフラ事業者は「電力」と「通信」に依存しており、その社会的責任は他の重要インフラ分野より大きく、また「政府・地方公共団体」は、インシデント発生時の「意思決定者」としての役割から、人的面も含めた緊急時の機能確保が必要になると考えられる。

弊社では、「国家情報セキュリティセンター（仮称）」が、このより重要度の高い「電力」「通信」「政府・地方公共団体」分野を「レベル1」として位置付け、重点的な施策を行う必要があると考えている。

5.1.3. 国家情報セキュリティセンター（仮称）への評価機関の設置

国家情報セキュリティセンター（仮称）の活動は、既存のどのセキュリティ関連機関も行ってこなかったような広範囲に及ぶと想定される。よって、その活動内容を評価し、適切な助言を与える第三者機関も同時に必要となる。4.1.4(1)(c)でも述べたように、米国では会計検査院（GAO:Government Accountability Office）にIT専門の検査員がおり、このような評価・助言を与える役割を担っている。国内においても、国家情報セキュリティセンター（仮称）の設立とともに、評価機関及び評価する人材の確保が必要であると考えられる。

5.2. 国家情報セキュリティセンター（仮称）に求められる役割

「情報セキュリティ基本問題委員会」の第1次提言では、「国家情報セキュリティセンター（仮称）」の常勤職員は60名程度と提言されていた。しかし、国家の情報セキュリティを包括的に担う機能をこの人数で担うには無理がある。そこで、既存の調査機関及び研究機関と連携し、効率良く業務をこなしていく必要がある。具体的には、警察庁やJPCERT/CC、IPAなどの国内のインシデント情報収集機関及び米国のDHSや英国のNISCCといった海外の重要インフラ防護機関と情報共有を行うとともに、大学や独立行政法人、メーカなどの研究機関と共同研究を活性化させていくことが求められる。

そこで4.1.4、4.2.4、4.3.3で挙げた政策提言に対し、具体的にどのような施策が考えられるのか、「国家情報セキュリティセンター（仮称）」の役割として、以下に述べる。

5.2.1. 情報共有を前提とした情報収集・分析技術の向上

4.1.4(2)で述べたように、今後は重要インフラ事業者間で効率良くインシデント情報を共有していくことが求められる。これまでも多くの企業で、インシデント発生時の情報収集・分析を目的としてアクセスログ等のログ収集・分析が行われてきた。しかし、これらの収集・分析は、自社内か、自社とベンダーとの間でのみ行われているケースが多く、幅広く共有するには以下のような問題が考えられる。

- ・ 機器によりログのフォーマットが異なる
- ・ ログの収集方法、分析結果の表示方法に統一性がない

こういった問題を解決するためには、収集・分析した情報を共有できるような仕組みが必要であり、具体的には、異なるログから得られる収集・分析結果を、ある一定の標準フォーマットに統一することや、そもそもシステムのログを異なる機器間でも標準化してしまうことが考えられる。

一方、裁判時の証拠保全を目的として、システム内のあらゆる情報を収集・分析する証跡管理技術が注目されている。この技術の状況保存力の高さは、インシデント情報の収集・分析という目的でも大いに活用できると考えられる。

5.2.2. 重要インフラに係わる公開情報の政府による監視

4.1.4(3)では、重要インフラに関する公開情報を監視する必要性について述べた。こういった情報の管理を事業者各社の自主管理とした場合、以下の点において限界があると考えられる。

- ・ 第三者によって公開されている情報のチェックには膨大な労力を要する
- ・ 発見した情報の削除を要請する法的な強制力がない
- ・ 政府と事業者とのテロや犯罪に関する意識の違いによる情報の価値の差によって、政府としてこういった重要インフラに関して公開されている情報（CII）

を常にチェックし、関係者に対して必要に応じて掲載削除を促して、重要な情報がテロリストや犯罪者に渡らないようにする機能が必要となる。「国家情報セキュリティセンター(仮称)」が、法的強制力も含めてこの機能を担うことが求められ、監視のために必要とされる要員、費用の確保を行うとともに、監視手法の技術開発、監視システムの構築・運用を行う必要があると考えられる。

5.2.3. 緊急時対応演習の実施とそれに伴う体制整備

4.2.4 で指摘したように、重要インフラ事業者は定期的に緊急時対応演習を行うことが求められる。しかし、こういった演習の実施を事業者のみに委ねるには、以下の点で問題があると考えられる。

- ・ 複数の事業者が参加する枠組みがない

重要インフラ相互間の調整機能を有する必要性

- ・ 演習実施費用の経営への負担度合い

前者では、「国家情報セキュリティセンター(仮称)」が実施する演習においては、相互依存性を有する重要インフラ各社が参画しやすい枠組みの策定と、相互間の調整を含めた役割を担うことが求められる。

また実施に当っては、その社会的影響を考慮すると、実際に稼動している機器を使用する演習は望ましくないことから、事業者各社がお互いに共有できるような演習システム・施設の構築が求められる。民間事業者のセキュリティ対策に、政府が関与することの是非を問う声も聞かれるが、重要インフラの社会生活における重要性を考慮すれば、結果としては国民の福祉に還元される事業であると考えられる。

「国家情報セキュリティセンター(仮称)」には、重要インフラ事業者以外の企業等にもこのシステム・施設を無償又は低料金で貸与する代わりに、4.2.4(3)の演習に関する情報共有化への協力や、4.1.4(1)で述べたインシデント情報共有化への協力を求め得ることが期待される。

しかしながら、後者として示したように、実際に演習施設を構築するとなると、膨大な種類の機器を揃えるために莫大な費用が必要となる。また、重要インフラ事業者の中には、既に製造が行われていないレガシーシステムを使用しているケースも想定される。そこで、演習施設には、事業者が一般的に使用している機器に関しては実機をそろえるものの、事業者が実際に使用していても市場シェアの低い機器や現時点での購入が難しいような機器に関しては、シミュレーションを用いた演習を併用して行い、費用対効果を高める必要がある。

表 4-5 でも述べたが、シミュレーションを用いた演習を行う際には、インシデント発生時のシミュレーション上での機器の反応を、いかに現実に近いかが重要となる。そのためには、メーカーが保有する機器別の障害情報や保守員の経験などを利用して、シミュレーション上でも現実により近い反応を引き出せるようなシステムの研究・開発を同時に行う必要があると考えられる。

5.2.4. 「セキュリティのあり方」に関する研究の促進

4.3.3 では、セキュリティ係わる標準に関する政策提言を行った。ここで述べた「セキュリティに係わる標準のブラッシュアップ」業種別セキュリティスタンダードの検討」は、今後 3 年間にわたる短期的な課題としては重要であると考えられるが、以下のような問題を抱えていることもまた事実である。

- ・セキュリティ対策として求められる最低基準を示したに過ぎない
- ・セキュリティ対策の上限が見えず、中長期的な目標が立てにくい

これは、セキュリティポリシーや標準が、過去に起きたインシデントや今後想定されるとされる脅威を元に作成された、ボトムアップ的なアプローチによるものであることにその要因がある。多くの重要インフラ事業者は、その社会的重要性から、この最低基準を大幅に超えたセキュリティ対策を施していると考えられる。

一方、ベストプラクティスと呼ばれるものは、現状の技術、法律制度など様々な環境を考慮した上で、最も先進的な事業者が採用している対策例であり、業界内や関連事業者にとっては、一つの指針とはなり得る。しかし、たとえベストプラクティスのセキュリティ対策を行っている事業者であっても、今後取るべき方策を継続して検討していかなければならないことには変わりなく、その意味では、ベストプラクティスであっても最終目標として位置付けられるわけではない。

このような状況から、そもそも重要インフラのセキュリティはどうあるべきか、標準やベストプラクティスを越えてはるかにレベルの高い位置に位置付けられる、トップダウン的なセキュリティ対策のあり方を検討することが、長期的には重要であると考えられる。ベストプラクティスのさらに上部に存在するため、現状の環境で事業者が達成することはほぼ不可能であるかもしれない。しかし、このトップダウン的なセキュリティ対策は、そこに到達すること自体が重要なのではなく、自社の現状との乖離を正しく認識し、その乖離が発生している原因(人的、技術、費用、等)を追求することに意義がある。事業者がこの原因を正しく認識することによって、短期、又は中長期的なセキュリティ対策の目標を設定することができる。例えば、仮に費用の問題で到達することができないのであれば、費用が確保でき次第対策を施せるため、短期的な目標として位置付けることができるが、技術的な面で到達できないのであれば、技術の発展を待つ必要があり、中長期的な目標として位置付けられる。

欧米では、こういった「セキュリティ対策のあり方」に関する研究が、一部の研究機関で行われ始めている。日本国内においても、「国家情報セキュリティセンター(仮称)」において、このような研究が今後行われていくことを期待するものである。

6. 参考文献（順不同）

- ・ 電力重要インフラ防護演習に関する調査報告書（2004年8月 独立行政法人 情報処理推進機構）
- ・ 金融機関等コンピュータシステムの安全対策基準・解説書（平成15年10月 財団法人 金融情報システムセンター）
- ・ 平成17年度版 金融情報システム白書（2004年12月 財団法人 金融情報システムセンター）
- ・ 米国情報セキュリティ関連オフィス訪問報告書（平成15年9月 日本ネットワークセキュリティ協会）
- ・ 産業構造審議会情報セキュリティ部会報告書・情報セキュリティ総合戦略策定研究会報告書 情報セキュリティ総合戦略 世界最高水準の「高信頼性社会」実現による経済・文化国家日本の競争力強化と総合的な安全保障向上、（2003年10月10日 経済産業省）
- ・ 実践セキュリティポリシー（平成12年2月 ISACA 大阪支部・監査基準分科会）
- ・ 鉄道と電気技術（社団法人 日本鉄道電気技術協会）
- ・ セキュリティ用語辞典（平成14年12月12日 日経BP社）
- ・ ダン・バートン著 星睦訳 「ブラックアイス サイバーテロの见えない恐怖」（平成15年10月11日 インプレス）
- ・ 土居範久監修 情報セキュリティ事典（平成15年7月10日 共立出版）
- ・ 地方自治情報管理概要（平成16年10月 総務省自治行政局地域情報政策室）
- ・ 情報セキュリティに関する実態調査（平成16年7月 総務省）
- ・ ISTS Quarterly volume1, Number1, Spring 2004 (Dartmouth University)
- ・ New Scientist Magazine (Saturday, May 15, 2004)
- ・ Microsoft Security Overview (ARC Advisory Group, August 2004)
- ・ JIS X 5080:2002 情報技術 - 情報セキュリティマネジメントの実践のための規範
- ・ 情報通信ネットワーク安全・信頼性基準（昭和62年郵政省告示第73号）
- ・ 地方公共団体における情報セキュリティポリシーに関するガイドライン（平成13年3月30日策定，平成15年3月18日一部改訂 総務省）