

資料編  
(参考資料)

## 資料編

1. G 8 関連	3
(1) パリ会合プレスリリース	
(2) ベルリン会合プレスリリース	
(3) 東京会合プレスリリース	
2. 政府 I T 政策関連	11
(1) e-Japan 重点計画 (抜粋：6.高度情報通信ネットワークの安全性及び信頼性の確保)	
(2) e-Japan2002 プログラム (抜粋： 分野別施策 6. 高度情報通信ネットワークの安全性及び信頼性の確保)	
(3) 重要インフラのサイバーテロ対策に係る特別行動計画	
(4) サイバーテロ対策に係る官民の連絡・連携体制について	
3. 情報システム安全対策指針	36
4. 不正アクセス禁止法関連	51
(1) 不正アクセス行為の禁止等に関する法律	
(2) 不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規定	
(補遺)	
1. G 8 関連	60
(1) 国際組織犯罪対策に関する勧告(改訂版) (抜粋：Part Ⅰ：国境を越えた犯罪 SectionD：ハイテク・コンピュータ関連犯罪)	
(2) テロ・犯罪捜査における国境を越えたネットワーク通信追跡のための勧告	
(3) 公共の安全を保護するために不可欠なデータの利用可能性に関する原則	
(4) データ保全に関するチェックリスト	
(5) G 8 データ保護制度に関する声明	
2. 政府 I T 政策関連	77
(1) e-Japan 重点計画-2002 (抜粋： 重点政策 5 分野 5. 高度情報通信ネットワークの安全性及び信頼性の確保)	
(2) 緊急対応支援チームの設置について	

## 1. G8 関連

### パリ会合プレスリリース

G8 ハイテク犯罪対策政府・産業界合同会合：  
サイバー空間における安全性と信頼性に関する政府と産業界との対話

プレスリリース（仮訳）

2000 年 5 月 17 日

1. 全 G8 メンバー国から集まった政府及び産業界の代表者たちは、5 月 15 日?17 日、パリにおいて、G8 パリ会合：サイバー空間における安全性と信頼性に関する政府と産業界との対話を行い、ハイテク犯罪、インターネットの犯罪目的での使用に関連した、産業界・政府側共通の課題及びその課題の解決手段につき議論した。右会合は G8 リヨングループがイニシアティブを取り、運営された。以下の文は、会合に出席した政府団団長によって発出されたものである。
2. 情報・通信技術は、情報の入手、共有及び交換と経済の発展にとって、かつてない機会を提供している。全ての G8 諸国は、経済、プライバシー、人権、社会等の考慮と、サイバー空間における公共の安全と信頼性を維持する必要性とのバランスを取るにより、電子商取引の発展を促す環境を作ることの重要性の大きさを認識する。
3. ハイテク犯罪の進展は、サイバー空間の安全性と信頼性を脅かすものである。それは、企業や国家のみならず一般私人に直接影響を及ぼす。
4. 各種のシステムを通じてインターネット犯罪者の所在を確認し及びその身元を特定する能力は、電子的要素を帯びた犯罪の抑止、捜査及び訴追にとって極めて重要である。コンピュータ・ネットワークの越境的性質は、犯罪者が押収を逃れるために情報を外国に保存したり、それを素早く移動又は削除したりすることを比較的容易としている。多くのコンピュータ・ネットワークや通信網の越境的性質が、法的に認められる捜査にとって大きな課題となっていることから、G8 は、この問題に「国境を越えた犯罪」の文脈で率先して取り組んできた。
5. G8 諸国は、これら新しいネットワークの合法的利用者の保護を改善し、もって情報技術の持続可能な発展を保証するためには、一層迅速な或いは画期的な解決策を発展させるべきであり、また、そのためには政府と産業界が協力しなければならないと確信する。解決策の内の幾つかは、実施体制、法制度及び国際協力手続の適合を必要とする国家自身の事柄である。また、民間部門と政府との間の協力のための原則の発展を求めるものもある。一層の作業が必要であるが、既に政府と産業界とはサイ

バー犯罪に立ち向かう措置を取ってきている。

6. 政府と民間部門とは、情報・通信技術の不正なあるいは有害な使用との闘いにおいて共通の利益を有している。政府と民間部門との対話は、いくつかの理由により、明らかに必要不可欠なものである。即ち、企業自身が犯罪行為の被害者となることもしばしばであり、また、企業はサイバー犯罪対策を提案するに適している。
7. これらの課題の全てに応えるべく、G8 諸国は、初めて、政府と民間部門の双方からの上級代表者を一堂に集めた。こうして、犯罪の防止及び訴追に責任を有する公的機関は、情報技術分野の主要企業 130 社の代表と対話を開始することができた。実りある対話を通じて、彼等は、先端技術の使用がもたらす諸問題について討議し、可能な限り最善の解決策を発展させるための措置を講じることができた。
8. 3 日間の会議の中で、いくつかのテーマが討議された。サイバー犯罪者の所在及び身元の特定に際し、直面する問題点が特に留意された。参加者は、以下の要素を考慮に入れつつ、既存の規則を改善し、新たな解決策を発展させる必要性を強調した：
  - 個人の自由及び私生活の保護
  - 政府のハイテク犯罪への対策能力の維持
  - あらゆる関係者に対する適切な訓練
  - ハイテク犯罪対策に向けられた明白かつ透明性の高い枠組み
  - 自由・公正な経済活動、及び産業界の健全な発展の確保及び産業界の自発的イニシアティブに基づく行動規範と基準の支援
  - 実効性と結果の評価
9. また、参加者は、ハイテク犯罪に有効に対処するために、G8 内の、また、G8 を越えた国際協力が不可欠であるとの見解を共有した。情報技術の乱用に安全な避難所（セーフ・ヘーブン）がなくてはならない。
10. この会議の成果は、本年 7 月沖縄で会合する予定の G8 各国首脳の討議に資するものと期待される。

[http://www.mofa.go.jp/mofaj/gaiko/summit/ko\\_2000/genoa/crime.html](http://www.mofa.go.jp/mofaj/gaiko/summit/ko_2000/genoa/crime.html)

## ベルリン会合プレスリリース

G8 政府共同プレスリリース（仮訳）

G8 政府及び民間によるコンピューター犯罪対策会合

各国専門家がハイテク問題に焦点をおいたワークショップを開催（於：ベルリン）

2000 年 10 月 26 日

ベルリン?今週、全 G8 各国から政府及び民間の上級代表が集まり、ハイテク犯罪、コンピューター関連犯罪及び犯罪目的によるインターネットの悪用への対策についての議論を行った。この「サイバースペース上の安全性と信頼性に関する G8 政府・産業界合同ダイアログ」は、10 月 24 日から 26 日、G8 リヨングループとして知られる国際組織犯罪対策上級専門家会合の主催で行われた。

リヨングループは、本年 5 月、パリにおいて、初めてとなる G8 各国の政府及び民間の合同会合を開催した。パリ会合では、シニアレベルの政府代表者が、通信や先端技術関連分野に関係する 130 の大企業及びいくつかの団体の代表者と対話をもった。各国代表団は、先端技術が犯罪目的で悪用された手法について考察し、可能な解決策について検討した。

今週のベルリン・会合は、パリで始めた対話を継続し、パリでの成果を活用した。本会合では、リヨングループが前進するために特に重要視している以下の 3 つのテーマを中心に取り上げた。

市民的権利を尊重しつつ、

1. 脅威の分析や犯罪予防を通じ、電子商取引、重要インフラ及びサイバースペース上の信頼性を保護すること。
2. 情報通信技術を悪用する犯罪者を追跡・特定する能力を向上させること。
3. 政府、民間、利用者及びサイバースペース上の安全性と信頼性の促進に関心を有する他の関係者との生産的な関係の構築を継続させること。

本会合では以下のような作業が行われた。

- サイバースペース上の安全性と信頼性を促進する上で、政府、民間、利用者及びその他関心を有する者にとっての役割と責任について検討すること。
- 脅威及び犯罪行為についての情報交換に関する最良の方法について議論すること。
- 捜査上関連性の高い通信に関するデータ及びそのデータの保全/保存に関するコスト、利益、懸念を特定すること。
- オンライン上の犯罪者をまさに犯罪を敢行している最中に特定する最良のメカニズム及びその上での重大な障害について検討すること。
- 認証実務及び技術のサイバー犯罪対策上の有益性及び実用性について議論すること。

- 緊急事態に 24 時間対応可能であるような政府と産業界の重要なコンタクトポイントを発展させる可能性につき検討すること。
- 政府と民間、両者のための教育やトレーニングの機会を改善すること。
- この重要な対話から得られる利益を、非 G8 諸国にも享受させること。
- サイバースペースの安全性及び信頼性を向上させる取り組みが、先端技術の利用者の市民的権利（含プライバシーの権利）を尊重し、サービスプロバイダも含めた特定の集団に過重な負担を負わせることのないよう保証すること。

これらの作業の多くは小規模な「ワークショップ」において開催され、そこでは率直かつ非公式な意見交換に重点がおかれた。協力の阻害要因の軽減及び実用的な解決策を発展させることが強調された。現時点では、公式な同意の形成を目的とすることはなく、また有用なものともとらえられなかったが、一方、すべての参加者はこの対話の価値に関する認識を同じくした。

本会合に参加した各国政府代表団は、民間の代表者との協議後、次の見解を共有するに至った。

すなわち、コンピューター、電子メール、インターネット及び無線通信は、最近までは一般的なものではなかったが、今日、至る所に存在し、我々の重要インフラを支え、大抵の市民の日常生活に関わりを持つようになった。21 世紀の技術が、我々の生活様式に変化をもたらし、又無数の新たな機会を提供すると同時に、コンピューターとネットワークはもはや犯罪者が国境に制約されない新たな犯罪にとってのフロンティアを開いた。プライバシーを守りつつ、法執行機関、民間、消費者及びその他の者がサイバー犯罪者の先を行くためには、政府と民間が今までにないほど協力して取り組んでいかなければならない。

G8 首脳による沖縄コミュニケは、本分野における政府と産業界の緊密な協力の重要性を強調し、ベルリン会合を含め、より一層の対話を促した。

ベルリン G8 会合は、ハイテク犯罪、特に、コンピューター関連犯罪の対策及びサイバースペースでの安全性と信頼性の促進における新たな重要なステップを示している。実際、我々はサイバースペースにおける市民の繁栄、機会及び市民的権利を保護し続けるための土台を築いているところである。我々は、我々の協力関係が持続、改善されることを期待し、日本で開催予定のハイテク犯罪に関する産業界との第 2 回ハイレベル会合を歓迎する。

[http://www.mofa.go.jp/mofaj/gaiko/summit/ko\\_2000/genoa/lyon.html](http://www.mofa.go.jp/mofaj/gaiko/summit/ko_2000/genoa/lyon.html)

## 東京会合プレスリリース

### G8 ハイテク犯罪対策・官民合同ハイレベル会合 プレスリリース（仮訳）

2001年5月24日

今週、東京において、G8 各国の政府・民間及び欧州委員会の上級代表が集い、ハイテク犯罪対策及び犯罪目的でのインターネットの使用について議論を行った。そこでは、公共の安全、プライバシー及び他の社会的な諸価値の擁護、並びに情報社会と電子商取引の成長の促進を含んだ公共の利益を増進するような、あり得べき解決策が探求された。G8 ハイテク犯罪対策・官民合同ハイレベル会合は、リヨングループという名で知られる国際組織犯罪対策上級専門家会合が主催して、5月22日から24日まで開催された。

1. 情報・通信技術（IT）は、21世紀を形作る可能性を秘めた力である。われわれが目当たりしている経済的、社会的及び文化的変容は、疑いもなく重大である。しかし、ITの絶え間ない発展はまた、犯罪者に新たな技術を濫用して犯罪を犯す機会をも与えている。ハイテク犯罪は、異なった国々の複数の電気通信／コンピュータ・ネットワークを通じて瞬時に実行される可能性があり、世界中の企業や国家のみならず、一般個人にまで直接影響を及ぼす。ハイテク犯罪は、深刻な世界的な脅威となっている。

ハイテク犯罪に効果的に対抗するためには、国際的な協力が不可欠である。G8は、リヨングループの枠組み内で、この緊急課題の解決に努めてきた。しかし、政府間だけの協力では不十分である。政府・民間の間のパートナーシップが重要であり、このことは1998年のバーミンガム・サミット以来、G8各国の首脳により強調されてきた。

このような背景から、リヨングループは、2000年5月、パリにおいて、第1回のG8政府・民間代表者会合を開催した。パリ会合においては、G8各国の政府代表者は、主要な通信・新技術関連企業130社の代表者と対話を行った。出席者は、新技術の犯罪における使用が通信及びコンピュータ・システムの安全性を脅かす方法について議論するとともに、あり得べき解決策を模索した。

2000年7月の九州・沖縄サミットにおいて、G8各国の首脳は、パリ会合で生み出された成果及びモメンタムを歓迎し、民間との対話を促進する必要性を強調した。リヨングループは、官民の対話を進展させるため、2000年10月、ベルリン会合を開催した。ベルリン会合での作業の大部分はワークショップで行われ、政府と民間との協力を妨げる障害の除去、及び、ハイテク犯罪を予防、探知、捜査するための実務的な解決策の追求に重点が置かれた。

2. 今週の東京会合は、九州・沖縄サミットにおける G8 各国首脳のコミットメントを受けて、実質的な成果を生み出すことを目的として、民間との対話を更に促進するために開催されたものである。

この目的を達成するため、G8 各国の政府及び民間の上級代表（約 200 名）は、個別のプロジェクト・グループにおいては、主要な問題点について意見交換を行うとともに、一堂に会した全体会合においては、横断的な問題や官民間の将来の協力のあり方を模索した。

ベルリンで始められたワークショップでの議論を継続し、国内的及び国際的レベルでの成果に基づいて、5 つのプロジェクト・グループは、i) データの保存、ii) データの保全、iii) 脅威の分析及び予防、iv) 電子商取引の保護及びユーザー認証、v) トレーニング、の各問題を検討した。

データ保存?以下の事項について討議され、または、検討された。

- ? 資源( resources )及びビジネスチャンスの観点からのコスト及び優先事項に関する討議；
- ? 現在存在する様々なサービス、ビジネス・モデル及びサービス・プロバイダーに関する検討；
- ? 法的、技術的、財政的な問題及びプライバシーの問題に配慮した上でのデータ保存の実務に関する討議。

データ保全?以下の文書が作成され、以下の問題が検討された。

- ? 法執行機関がデータの保全を要請する際に用いるためのチェックリストの作成
- ? データ保全に関する法的枠組みを考えるに当たり検討されるべき事項に関するリストの作成
- ? データ保全の要請に対するプロバイダの協力を妨げる法の衝突及び裁判権の問題に関する討議
- ? データ保全に関する法執行及び産業界のためのベスト・プラクティスの作成

脅威分析及び予防?以下の勧告がなされた。

- ? コンピュータを利用した犯罪とコンピュータ・ネットワークへの攻撃の予防には官民の緊密な協力が必要である。
- ? 内容（コンテンツ）関連の脅威の予防は技術的または法的な理由により末端利用者のレベルにおいてはじめて対処可能となる。
- ? 政府は、IT 社会において、すべてのユーザーの意識を高めることにさらに関与されなければならない。
- ? G8 諸国及び非 G8 諸国における共通の慣行が定められるべきであり、かつ、国ごとの脅威の分類が相互に通用するものとなるべきである。



- ? 各国は、社会の様々な分野におけるハイテク犯罪とその影響の正確な構図を集積し、明確にする機構を設立すべきである。

電子商取引の保護とユーザー認証?以下の諸分野が討議され、勧告に至った。

- ? データ/ネットワークのセキュリティ・ポリシー
- ? データ/ネットワークのセキュリティモデルの要素についての提案
- ? より安全な電子商取引の指針についての提案
- ? G8 共通の電子商取引ウェブサイト
- ? 相互認証
- ? 情報共有
- ? 将来の討議

トレーニング?以下の文書が作成された。

- ? トレーニング戦略の概要表
- ? トレーニングと認識のための論理モデル
- ? 産業界のための戦略の概要表
- ? 政府・産業界協力のひな形
- ? 技能セット及び対象者のひな形

政府及び民間双方からの参加者の積極的な参画によって、全てのグループは自由、率直かつ実務的な討議を行った。パリ会合及びベルリン会合での成果に立脚して、各グループは実務的な解決策と具体的な結果を探求した。彼らの討議の成果物のうちいくつかは別添されている。更に、対話自体が価値のあるものであると証明された。

3. プロジェクト・グループ会合の後、参加者全員が全体会合に出席した。参加者はプロジェクト・グループで取り上げた分野について、より幅広い視野から議論を行い、とりわけ、関係者間での将来の協力、一般市民の意識および非 G8 諸国へのアウトリーチを含むより広範な問題についても考察した。

拘束力を有するような約束や、いかなる種類の公式な合意の形成は目指されていなかったが、関係者全員が、この対話の価値及び適当な場において対話を継続することの必要性を認識した。

4. ワークショップ会合に参加した各国政府代表は、民間代表との協議の後、以下の認識を共有した。

IT は、情報へのアクセス、共有及び交換並びに経済発展のための前例を見ない機会を与える一方で、

その濫用が国際社会にとってますます懸念材料となっている。IT がグローバルな社会の不可欠な基盤になればなる程、サイバー空間における安全性及び信頼性を確保することが、ますます重要になる。信頼性の欠如が、IT に導かれている社会のまさに根底を危険にさらすことにもなりかねない。この意味で、政府、民間および個人ユーザー全てが、ハイテク犯罪に対する闘いにおいて、共通の利害を有している。更に、IT の保護は、個人のプライバシーと安全を、ある面では増進することを可能にする。

個人のプライバシー、産業の健全な発展及びその他の社会的諸価値を尊重しつつ、サイバー空間における安全性と信頼性を確保するためには、脅威が特定されて、予防され、ハイテク犯罪者を追跡・特定できる法執行能力が維持される必要がある。これらの課題の解決策は、更なる官民協力の進展を必要とする。ハイテク犯罪を扱う教育の改善及びトレーニングの機会も、官民双方にとり死活的に重要である。

東京会合は、これらの分野における G8 の官民間の対話の深化における、新たな重要な 1 歩となった。21 世紀を迎え、われわれは、サイバー空間における繁栄、機会及び市民的権利の促進に努める。

今次会合の結果、ハイテク犯罪と戦うためには、官民間の協力関係を更に強化し、世界規模における国際協力を促進する必要があることが再確認された。

今次会合の成果は、2001 年 7 月、ジェノバに集う G8 首脳間の議論を促進することが期待される。

<http://www.mofa.go.jp/mofaj/gaiiko/hitech/01tokyo/press.html>

## 2. 政府IT政策関連

### e-Japan 重点計画（抜粋）

#### 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?

平成13年3月29日

IT戦略本部

#### 6. 高度情報通信ネットワークの安全性及び信頼性の確保

##### <目標>

我が国の高度情報通信ネットワークの安全性及び信頼性を世界最先端のIT国家にふさわしいものにするため、特に、電子政府、電子商取引、重要インフラ等のうち国民生活や社会経済活動に大きな影響を及ぼすものについて、情報セキュリティの不備により不正アクセス、コンピュータ・ウイルス、DoS攻撃(Denial of Service; サービス不能攻撃)等の高度情報通信ネットワークにおける脅威に起因するサービス提供機能の停止をゼロとすることを目標とする。

##### (1) 現状と課題

インターネット等の情報通信ネットワークにおいては、常に不正アクセス行為、コンピュータ・ウイルス、DoS攻撃<sup>1</sup>などの脅威にさらされており、超高速インターネット網の整備やインターネット常時接続の実現、電子商取引の発展や電子政府の実現等によって、これらの脅威は、政府機関や企業などに限らず、すべての国民にとっても、詐欺等の犯罪行為やプライバシー侵害等のかたちで、現実の差し迫ったものとして現れてくることが懸念される。

また、エネルギー供給、交通、政府・行政サービス等の国民生活や経済・社会活動に大きな影響を与えているいわゆる重要インフラ関連サービス活動の多くは、情報システムにますます依存するようになってきており、今後、更に加速的な情報化・ネットワーク化の進展が見込まれるなか、いわゆるサイバーテロの脅威が現実のものとなってきている。こうした状況は、自然災害等の緊急事態発生時の危機管理や国家安全保障に関わる事案についても同様であり、安全で信頼できる情報通信ネットワークの構築は経済社会全般の安全性・信頼性を確保する上で必須の課題である。

しかし、我が国の現在の情報セキュリティ水準は、不正アクセス防止に有効とされる一般的方法の一つ

---

<sup>1</sup> DoS攻撃： Denial of Service 攻撃(サービス不能攻撃)の略称。コンピュータやネットワークに不正に負荷をかけたり、セキュリティホールを突くなどして業務を妨害する攻撃。

であるファイアウォール<sup>2</sup>の設置率が 50%程度(米国では約 80%)にとどまっているなど、いまだ世界最高水準のものとは言い難いため、これを 2005 年までに世界最先端の IT 国家にふさわしい水準に引き上げることが必要である。

このため、情報の自由な流通と民間の自由な活動の確保を大前提としつつ、情報通信に関する安全性及び信頼性の確保とプライバシーの保護に万全を期する。あわせて、国際的な連携、治安、防災、安全保障、さらには、災害時等における情報システムのバックアップ体制や高度なセキュリティが求められる施設には、光ファイバー等を用いるなどの十分な配慮が必要である。

<主要指標(1999年12月)>	
政府・企業等における情報セキュリティポリシー策定率	18.9%
政府・企業等におけるファイアウォール設置率	50.7%
政府・企業等におけるバックアップシステム設置率	24.3%

## (2) 施策の意義

情報セキュリティ対策の推進は、高度情報通信ネットワークの発展に必要不可欠なものであるが、ITに係る技術革新の速度が極めて速いなかで、ますますその攻撃手法等が進化を遂げていることや、国境が無いというサイバー空間の特徴により、国内のみならず世界のどこからでも瞬時かつ隠密にサイバー攻撃を受ける可能性があることなどから、その対応は困難さを増している。このため、それに対処するための安全対策についても不断の見直しが必要である。高度情報通信ネットワークの安全性及び信頼性の確保は、世界最先端の IT 国家構築の基盤となるものであり、国民一人一人が安心してネットワークを利用するための前提となるものである。

## (3) 具体的施策

### 1. 情報セキュリティに係る制度・基盤の整備

刑事基本法制、情報セキュリティに関する客観的な判断基準等、情報セキュリティ対策における制度・基盤の整備を推進する。

#### ア) 刑事基本法制の整備(法務省)

IT 経済社会における刑事の基本法制について、高度情報通信ネットワーク社会の安全性及び信頼性の確保に資するため、法的基盤の整備を行う。

i) 2001 年中に、支払用カードの偽造等の犯罪に関する罰則の整備について刑法の一部を改正する法律案を国会に提出する。

---

<sup>2</sup> ファイアウォール：主に内部ネットワークと外部(インターネット等)との境界に設置外部からの不正アクセス等の攻撃を防ぎ、内部ネットワークを保護するシステム。

ii) 2005年までに、各種のハイテク犯罪に対する罰則、情報通信ネットワークに関する捜査手続について、適切な処罰を確保するため必要に応じた法整備を行う。

イ) 情報通信ネットワークの安全・信頼性対策(総務省)

2001年中に、移動体通信のインターネット利用の急増に伴う新たな脅威等に対処するため、次世代移動通信ネットワークの安全・信頼性対策について検討を行い、所要の制度整備を行う。

ウ) 暗号技術の標準化の推進(総務省及び経済産業省)

客観的にその安全性が評価され、実装性で優れた暗号技術を採用するため、2002年度までに、ISO<sup>3</sup>、ITU等における暗号技術の国際標準化の状況を踏まえ、専門家による検討会の開催等を通じて電子政府利用等に資する暗号技術の評価及び標準化を行う。

エ) 情報セキュリティマネジメント規格の確立(経済産業省)

2001年度中に、情報セキュリティマネジメントに関する国際規格(ISO/IEC<sup>4</sup>13335、ISO/IEC17799)をJIS等へ国内規格化するとともに、情報処理サービス業を対象とした事業所認証制度を創設することにより、情報通信ネットワークの安全性及び信頼性を確保する。

2. 政府部内における情報セキュリティ対策

各府省において情報セキュリティポリシー<sup>5</sup>の継続的な評価・見直しを実施し、情報セキュリティポリシーの水準を一層向上させるとともに、電子政府の基盤構築に資する情報セキュリティ評価・認証基盤の整備を行う。

また、情報セキュリティ水準の高い製品等の利用、重要システムのバックアップ、擬似アタックを含めた情報セキュリティ評価の実施等、国民に信頼される電子政府の構築を推進する。

ア) 情報セキュリティポリシーの評価・見直しの実施(内閣官房及び全府省)

2003年度までに、「情報セキュリティポリシーに関するガイドライン」(2000年7月、情報セキュリティ対策推進会議決定)に基づき、全府省は、情報セキュリティポリシーの運用・評価・見直しを実施するとともに、必要に応じ重要システムのバックアップ、擬似アタックを含めた情報

---

<sup>3</sup> ISO: International Organization for Standardization(国際標準化機構)の略称。物資及びサービスの国際交換を容易にし、知的、科学的、技術的及び経済的活動分野における国際間の協力を助長するために、世界的な標準化及びその関連活動の発展開発を図ることを目的とした国際機関。

<sup>4</sup> IEC: International Electrotechnical Commission(国際電気標準会議)の略称。電気及び電子の技術分野における標準化のすべての問題及び関連事項に関する国際協力を促し、これによって国際的意志疎通を図ることを目的とした国際会議。

<sup>5</sup> 情報セキュリティポリシー: どのような情報資産をどのような脅威からどのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定。

セキュリティ評価を行い、電子政府の実現のための情報セキュリティを確保するのに十分な水準に引き上げる。

イ) 政府におけるセキュリティ水準の高い製品等の利用の促進(全府省)

2001年度より、政府における情報セキュリティに関する信頼性の高いシステムの構築のため、「各省庁の調達におけるセキュリティ水準の高い製品等の利用方針」(2001年3月、行政情報化推進各省庁連絡会議)を踏まえた政府調達を行う。

ウ) 情報セキュリティ技術評価・認証事業の実施(経済産業省)

2001年度中に、情報機器等の情報セキュリティ関連国際規格(ISO/IEC15408)に基づいた評価・認証事業を開始するとともに、2003年度までに、政府レベルでの認証に係る国際相互承認スキームへの参加を目指す。

3. 個人情報保護

<前掲(4.電子商取引等の促進)>

4. 民間部門における情報セキュリティ対策及び普及啓発

情報セキュリティ対策を推進するための税制、融資等の支援を実施し、民間部門の情報セキュリティ水準の一層の向上を図るとともに、情報セキュリティ対策に係る相談業務や情報交換・発信について機能の充実を行う。

ア) 情報セキュリティ意識の向上(警察庁)

2001年度中に、国民に対する情報セキュリティに関する研修・意見交換を実施するための情報セキュリティコミュニティセンター(仮称)を全都道府県警察に設置する。また、2004年度までに、ハイテク犯罪<sup>6</sup>に関する相談、広報啓発活動等に従事する情報セキュリティアドバイザーを都道府県警察に配置し、その能力向上のための研修を行う。

イ) 産業界との連携の強化(警察庁)

2001年度中に、産業界との連携を強化するため、産業界からの参加者を含む会議を警察庁において開催し、産業界との連携に関する基本方針を策定するとともに、全都道府県警察に、プロバイダー、民間企業等とのハイテク犯罪情勢や犯罪手口等の犯罪実態に係る情報交換を行うための協議会を設置する。

ウ) 電気通信システムの信頼性を向上する施設の導入支援の強化(総務省)

2001年中に、自然災害等の非常時における通信手段の確保及びコンピュータウイルス等に対する情報セキュリティの向上を図るため、電気通信基盤充実臨時措置法の改正法案を国会に提出し、

---

<sup>6</sup>ハイテク犯罪：コンピュータ技術及び電気通信技術を悪用した犯罪で、電子計算機使用詐欺、ネットワークを利用したわいせつ物頒布、不正アクセス禁止法違反等が挙げられる。

同法による支援対象となる「信頼性向上施設」に、新たに「コンピュータウイルス監視装置」等を追加することによって、これらの施設の導入を行う民間事業者に対する税制優遇措置等の支援を行う。

#### エ) 情報通信ネットワークにおける情報セキュリティ評価手法の確立(総務省)

2003年度までに、情報通信ネットワークに関して事業者の規模にあったセキュリティ評価項目等の検討を行い、ITUに対し国際標準提案を行うとともに、事業者における情報セキュリティ対策のレベルを的確に判断するための評価手法を確立する。

#### オ) 不正アクセス対策・ウイルス対策等に関する情報提供体制の強化(経済産業省)

2003年度までに、不正アクセス、ウイルス等に関する情報収集・分析に係る機能を具体的に担っている情報処理振興事業協会(IPA)及びコンピュータ緊急対応センター(JPCERT/CC)の充実強化・連携及び海外の関係機関との連携を図り、情報セキュリティ情報提供機能の向上を行うことにより、広く一般利用者がこれらの情報提供を享受できる環境を整備する。

### 5. 重要インフラのサイバーテロ対策

「重要インフラのサイバーテロ対策に係る特別行動計画」(2000年12月、情報セキュリティ対策推進会議決定)を踏まえ、重要インフラの基幹をなす情報システムについて、リスク評価、情報セキュリティポリシーの策定及びこれらに基づく情報セキュリティ対策を推進するとともに、政府や民間事業者等との連絡・連携体制の構築及び緊急対処能力の向上を行う。

#### ア) 官民の連絡・連携体制の構築(内閣官房及び全府省)

2001年中に、官民共同で、情報通信ネットワークの脆弱性を克服するため、既存の連絡体制を活用しつつ、重要インフラ(情報通信、金融、航空、鉄道、電力、ガス、政府及び地方公共団体)における連絡・連携体制の構築を行う。

#### イ) 内閣官房における緊急対処体制の整備(内閣官房)

2001年度中に、情報セキュリティ事案に対処するための緊急時対応マニュアルを作成するほか、2003年度までに、情報セキュリティ対策業務支援システムを整備するなど、内閣官房における緊急対処体制の整備を行う。

#### ウ) 警察における緊急対処体制の整備(警察庁)

i) 2001年度中に、いわゆるサイバーテロ発生時の被害防止や攻撃元の追跡等を行う機動的技術部隊の創設及びサイバー攻撃の発生を認知するためのリアルタイム検知ネットワークシステムの構築を行うほか、要員の訓練・研究環境等必要な装備資機材を整備するなど、いわゆるサイバーテロの未然防止及び発生時の緊急対処のための体制を構築する。

ii) 2003 年度までに、テロ組織等に関する情報収集体制の整備、警察と重要インフラ管理者との連携強化、要員の技術の向上を図る。

#### エ) 防衛庁における緊急対処体制の整備(防衛庁)

2003 年度までに、防衛庁・自衛隊の保有する情報システムについて、情報セキュリティを確保しつつ運用を行うための運用ガイドラインの策定等を行うほか、情報システムに対する常時監視、システム監査、緊急事態対処等の各種機能を有した組織(部隊)体系の構築を行う。

### 6. 情報セキュリティに係る研究開発

#### ア) 国防・治安に係る情報セキュリティ技術の研究開発の推進(警察庁及び防衛庁)

2002 年度までに、警察庁においては、強力なファイアウォールの研究開発を行い、警察が保有するネットワークの情報セキュリティを強化する。

また、2003 年度までに、防衛庁において、サイバー攻撃に対する対処手法の実証的研究等を行い、防衛庁が保有するネットワークの情報セキュリティを強化する。

#### イ) 情報セキュリティに関する基盤技術の研究開発の推進(警察庁、総務省及び経済産業省)

2005 年度までに世界最先端の IT 国家にふさわしい技術水準を確保するため、現在想定されているあらゆる脅威等に対する情報セキュリティ技術の研究開発を推進し、次の研究開発について 2005 年度までに実用化を目指すこととする。

##### i) 不正アクセスやいわゆるサイバーテロの予防、検知等に関する研究開発

不正アクセスやいわゆるサイバーテロ等の脅威から情報通信ネットワークを守るため、これらの脅威を検知し、迅速かつ適切な対処を可能とするために必要な技術開発を行う。

##### ii) 情報通信ネットワークの安全性及び信頼性の確保に関する研究開発

情報の自由な流通を確保するため、暗号技術、電子署名等の認証技術、セキュリティ評価・認証技術等の情報通信ネットワークの安全性及び信頼性の確保に必要な技術開発を行う。

### 7. 情報セキュリティに係る人材育成

研究開発、研修事業、資格制度の導入等を通じ、高いレベルの情報セキュリティ技術を有する人材を十分に確保するための多面的な育成を行う。

#### ア) ハイテク犯罪対策に係る人的基盤の整備

i) 2004 年度までに、ハイテク犯罪捜査官の配置、サイバーパトロールモニターの委嘱、ハイテク犯罪捜査に従事する全国の警察職員への部内外の研修の実施等、ハイテク犯罪対策に必要な人材の確保や民間との協力体制の整備を行う。(警察庁)



ii) 2001 年度中に、地方検察庁の捜査官のネットワーク及び情報セキュリティに関する高度な専門的知識の習得を促進し、複雑高度化するハイテク犯罪に適正かつ迅速に対応できる体制の整備を行う。(法務省)

イ) 防衛庁における情報セキュリティ等に係る人材教育(防衛庁)

2003 年度までに、防衛庁職員を米国等へ派遣を行い、緊急事態対処等の高度な情報セキュリティ技術等を習得した中核的な技術専門要員を確保し、部内における技術要員の教育及び作戦情報などの秘匿性の高い情報を扱う防衛庁のネットワークの情報セキュリティの確保を行う。

ウ) 情報セキュリティに関する資格制度の整備(総務省及び経済産業省)

2001 年度中に、電気通信主任技術者試験に情報セキュリティに関する試験科目の追加、情報処理技術者試験に情報セキュリティ・アドミニストレーター試験の導入を行うとともに、情報セキュリティに関する講習の実施等及び情報セキュリティ評価関係技術者育成のための研修事業に対する助成を実施する。

#### 8. 情報セキュリティに係る国際連携の強化

G8、OECD 等における情報セキュリティに係る取組に加え、開発途上地域への支援等国際的な取組に積極的な貢献を行う。

ア) ハイテク犯罪対策に係る国際連携の強化(警察庁、総務省、外務省、法務省及び経済産業省)

2001 年度に、我が国が主催予定である第 2 回 G8 ハイテク犯罪対策官民合同ハイレベル会合等の機会を通じて、国際的なレベルでの官民の協議を行うとともに、ハイテク犯罪に関する迅速な捜査協力のためのルール作りについて協議する。

イ) 各国警察機関との連携強化(警察庁)

2001 年度に、アジア・太平洋ハイテク犯罪対策担当実務者会議の開催、アジア諸国警察機関との連絡のための 24 時間コンタクトポイントシステムの有効活用等を通じ、各国警察機関との連携を強化するとともに、ハイテク犯罪対策に係る技術的指導等を行う。

ウ) 米国国防総省等との連携強化(防衛庁)

2003 年度までに、米国国防総省との間における政策協議等の意見交換(IT フォーラム等)を通じて、防衛庁としての情報保証<sup>7</sup>を確立するとともに、これらのノウハウ・技術等について、国防上支障のない限り部外に公表する。

---

<sup>7</sup>情報保証：ここでは、現在、米国国防総省が実施しているコンピュータ・システム等の安全に関する各種施策の総称(Information Assurance)。

エ) 情報セキュリティに関するグローバル情報交換ネットワークの構築 (経済産業省)

2003年度までに、不正アクセス・ウイルス等の発生状況・分析等情報セキュリティに関する情報集積を行っている CERT/CC 等諸外国の官民関係機関との情報交換のため、JPCERT/CC における関係諸機関との連携強化、民間各層におけるネットワーク構築の支援等を行い、情報セキュリティに関する迅速かつ正確な情報提供、対応及び施策への反映ができる環境を整備する。

<http://www.kantei.go.jp/jp/singi/it2/kettei/3siryou46.html>

e-Japan2002 プログラム

？平成14年度IT重点施策に関する基本方針？

平成13年6月26日

IT戦略本部

II 分野別施策

5. 高度情報通信ネットワークの安全性及び信頼性の確保

情報セキュリティの確保は、IT化を進める上での前提条件となるものである。一方、平成12年におけるコンピュータウイルスの届出件数は1.1万件（前年比約3倍）、不正アクセス被害の届出件数は143件（前年比約2.6倍）と増加してきている。平成14年度においては、特に、電子政府におけるセキュリティ体制やいわゆるサイバーテロに対する対応体制の構築、民間におけるセキュリティ水準の向上等を重点的に図る。

(1) 信頼性の高い「電子政府」の構築

1. 電子政府の情報セキュリティを確保するため、各省庁及び地方公共団体の情報セキュリティに関する支援、並びに各省庁の情報セキュリティの評価・監査、緊急事態への対応を一元的に行う体制を構築するための検討を開始する。（内閣官房）
2. セキュリティポリシーの継続的な評価・見直しを図るため、「擬似アタック」の実施等を含め、効果的な手法について検討を行う。（内閣官房）
3. 緊急対応体制の整備や地方財政措置の実施等、地方公共団体の情報セキュリティに関する支援を推進する。（総務省）

(2) サイバーテロ対策の強化（内閣官房、警察庁、防衛庁、金融庁、総務省、経済産業省、国土交通省）

官民間のいわゆるサイバーテロに係る情報の集約、伝達、蓄積及び官民での共有等を行うための「サイバーテロ対応データベース」（仮称）の構築・機能強化を行うとともに、緊急時に対処するための高度な技術を有する人材の育成、体制整備、国際連携を推進する。

(3) 情報セキュリティの意識の向上

義務教育レベルからの基礎教育、民間のイニシアティブを連携させる枠組の整備、各分野毎のニーズを踏まえた人材育成プログラムへの支援を推進する。（総務省、文部科学省、厚生労働省、

経済産業省)

(4) 民間部門における情報セキュリティ対策への支援

1. 情報セキュリティに係る関係機関・団体における民間への情報提供・受入・指導助言機能の強化、都道府県警察等における民間からの相談受付業務の充実及びハイテク犯罪対策のための体制の強化を行う。(警察庁、総務省、経済産業省)
2. 情報セキュリティに関する普及啓発活動を行うとともに高度な情報セキュリティ設備の導入や情報セキュリティ関連サービスの購入等を行おうとする民間企業等について、その促進のための支援を行う。(総務省、経済産業省)

(5) 情報セキュリティに係る基盤技術の開発(警察庁、防衛庁、総務省、文部科学省、経済産業省)

暗号技術、情報セキュリティ評価技術等の基盤技術の開発を行うほか、国防・治安関連技術について支障のない範囲内で政府他部門・民間にも公開する。

<http://www.kantei.go.jp/jp/singi/it2/kettei/010626.html>

## 重要インフラのサイバーテロ対策に係る特別行動計画 (概要)

### 1 目的

いわゆるサイバーテロなど、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いかなる攻撃からも重要インフラを防護する。

### 2 対象とする重要インフラ分野

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。）

### 3 官民におけるサイバーテロ対策

#### (1) 被害の予防（セキュリティ水準の向上）

被害を予防するため、その前提として、対象となる重要インフラの情報システムのリスク分析を行い、情報システムの重要度に応じた対策を講ずることによって、恒常的に各重要インフラ分野のセキュリティ水準の向上を図る。

#### (2) 官民の連絡・連携体制の確立・強化

セキュリティ情報（セキュリティ改善に必要な情報）及び警報情報（サイバー攻撃の発生情報等の警戒や緊急対処に必要な情報）の共有、予防・対処等を連携して行うための官民における体制の確立・強化を図る。

#### (3) 官民連携によるサイバー攻撃の検知と緊急対処

各重要インフラ分野においてサイバー攻撃を受けた場合又はそのおそれがある場合の対応策を定めるとともに、官民全体で対処能力の強化を行う。

#### (4) 情報セキュリティ基盤の構築

サイバーテロ対策を進めていくため、人材の育成、研究開発、普及啓発、法制度の整備等の情報セキュリティ基盤の構築を推進する。

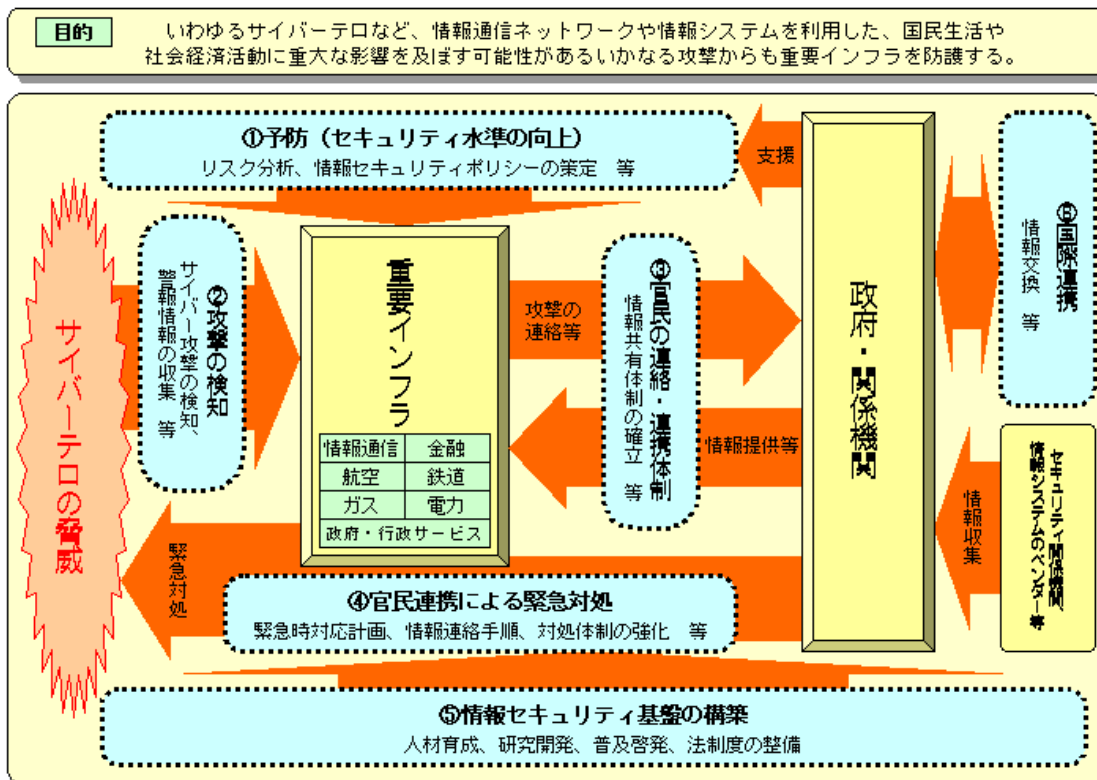
#### (5) 国際連携

サイバー攻撃は、国境を越えて行われる可能性があることから、このような攻撃に適切に対処するため、国際的な連携を推進する。

### 4 行動計画の見直し

この行動計画は、官民の連絡・連携体制の確立を中心としてとりまとめた初めてのものであり、政府は、この進捗を踏まえ、定期的及び必要に応じ見直しをする。

## 重要インフラのサイバーテロ対策に係る特別行動計画の概要



[http://www.bits.go.jp/taisaku/2000\\_1215/1215fig2.html](http://www.bits.go.jp/taisaku/2000_1215/1215fig2.html)

平成12年12月15日

情報セキュリティ対策推進会議

## 重要インフラのサイバーテロ対策に係る特別行動計画

### 1 特別行動計画の目的

この特別行動計画の目的は、いわゆるサイバーテロなど、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いかなる攻撃からも、重要インフラを防護することである。

政府は、内閣官房を中心として、官民の緊密な協力の下、この計画の実施に努めることとし、民間重要インフラ分野の事業者及び地方公共団体（以下「民間重要インフラ事業者等」という。）においては、この計画を指針として、自主的な取組の強化を図るものである。また、政府は、民間重要インフラ事業者等における計画の実施に当たっては、必要な協力を行うこととする。

### 2 いわゆるサイバーテロの脅威

産業や政府の活動の多くは、情報システムに依存するようになってきており、更に加速的な情報化・ネットワーク化の進展が見込まれている。重要インフラにおいても、電力供給、交通、電子政府等の国民生活や社会経済活動に不可欠なサービスの安定的供給や公共の安全の確保等に関する重要な役割を情報システムが果たすようになってきている。

このような重要インフラの基幹をなす重要な情報システムに対して、情報通信ネットワークや情報システムを利用した電子的な攻撃（以下「サイバー攻撃」という。）が行われた場合には、国民生活や社会経済活動の混乱、国民の生命の危険などの重大な被害が生ずるおそれがある。このような攻撃は、他の物理的攻撃と異なり、情報システムに侵入する技術を有する者であれば、一台のコンピュータによって行うことも可能な一方、国民生活や社会経済に混乱を引き起こすこと等を目的として組織的に大規模な攻撃が行われることも懸念されている。

外国においては、金融関係等の情報システムが被害を受けた事例や、個人がいわゆるハッカーとして、重要インフラ等の情報システムに対する侵入、サービス不能攻撃(DoS 攻撃)、コンピュータウイルスの流布等によって重大な被害を起こした事例もあり、このような脅威は現実のものとなってきている。米国においては、高度な技術を有する犯罪者集団やテロリスト集団などが重要なネットワークを攻撃することによる、経済的な被害、混乱、死傷者等をもたらす脅威に対して、国家計画の策定などに取り組んでいるところである。

また、インターネット等の他のネットワーク等との接続が進むことによって相互依存性が高まっていくこと及び情報システムの仕様の標準化や共通化が進展していることから、現時点では外部からの侵入の危険性が少ない情報システムについても、このような脅威は増大していくこととなる。さらには、内部関係者の関与等の脅威にさらされる可能性は常に存在しており、また、他のネットワークとは接続していないとされている情報システムであっても、外部からの侵入の危険性を排除することはできないことを認識しなければならない。

### 3 重要インフラ分野

いわゆるサイバーテロの脅威により、国民生活や社会経済活動に重大な影響を与えられとされる重要インフラ分野を、当面、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。）とする。ただし、新たな脅威等を踏まえ、本行動計画で対象とする重要インフラ分野について、適宜、見直しを行うこととする。

各重要インフラ分野を所管する省庁は、所管分野がこの計画を適切に実施できるよう協力することとする。

なお、いわゆるサイバーテロの脅威から、我が国の重要インフラを防護するため、これらの重要インフラ以外の分野においても、必要に応じ、この特別行動計画を参考として、対策の強化を図ることが重要である。

### 4 被害の予防（セキュリティ水準の向上）

被害を予防するためには、その前提として、対象となる重要インフラの情報システムのリスク分析を行い、情報システムの重要度に応じた対策を講ずることによって、恒常的に各重要インフラ分野のセキュリティ水準の向上を図ることが必要である。

#### (1) 民間重要インフラ分野等のセキュリティ水準の向上

- 民間重要インフラ事業者等は、「情報セキュリティポリシーに関するガイドライン」（平成12年7月18日、情報セキュリティ対策推進会議決定）や各省庁の情報セキュリティ関連ガイドライン、OECDのセキュリティガイドライン等を参考としてリスク分析や情報セキュリティポリシーを策定するなど、セキュリティ水準の向上に努める。
- 各民間重要インフラ分野及び地方公共団体（以下「民間重要インフラ分野等」という。）においては、仕様が共通する情報システムを使用する場合又は互いに情報システムを接続する場合において、分野に共通するリスクに対し適切な対処を行うため、各民間重要イン



フラ分野等における対策指針の策定について検討する。

- 政府は、民間重要インフラ事業者等のセキュリティ水準の向上に資するために、情報の提供、助言、指導等、民間重要インフラ事業者等の取組に対する支援の一層の推進に努める。

#### (2) 電子政府の構築に向けたセキュリティ水準の向上

- 各省庁は、平成15年度までに電子政府の基盤を構築することを踏まえ、「情報セキュリティポリシーに関するガイドライン」を踏まえて策定したポリシーに従い、セキュリティ水準の向上のため必要な措置を講ずる。
- 内閣官房の専門調査チームによる、各省庁の情報システムのセキュリティ対策に係る技術的調査・助言等を実施する。

### 5 官民の連絡・連携体制の確立・強化

各重要インフラ分野においては、セキュリティ情報（セキュリティ改善に必要な情報）及び警報情報（サイバー攻撃の発生情報等の警戒や緊急対処に必要な情報）の共有、予防・対処等を連携して行うための官民における体制の確立・強化を図ることが必要である。

特に、いわゆるサイバーテロの脅威が増大していくなか、サイバーテロ対策に関する官民の連絡・連携体制を確立することは急務であることから、各分野における状況を踏まえ、本計画決定後一年以内を目標として、次の体制を構築することが必要である。

#### (1) 各民間重要インフラ分野等における連絡・連携体制

各民間重要インフラ分野等において、次の役割を担うサイバーテロ対策に係る事業者間の連絡・連携体制を、既存の連絡体制を活用しつつ構築する。

- 各分野に共通するセキュリティ情報及び警報情報の収集、連絡及び共有
- サイバー攻撃が発生した場合又はそのおそれがある場合における連絡体制
- 政府及び関係機関との一元化された連絡の実施 等

#### (2) 他分野の重要インフラ事業者との連絡・連携体制

ネットワークを介して、他分野の重要インフラ事業者と情報システムを相互接続している場合には、サイバーテロ対策に関し互いの連絡・連携体制を必要に応じ構築する。

(3) 政府における連絡・連携体制の確立

政府においては、内閣官房を中心とし、次の役割を担う連絡・連携体制を構築する。

- セキュリティ情報及び警報情報の収集、連絡及び共有
- サイバー攻撃が発生した場合又はそのおそれがある場合における情報集約
- 政府部内、関係機関及び各民間重要インフラ事業者等との連絡 等

(4) 情報の取扱い

情報の収集及び共有に際しては、民間重要インフラ事業者等から適切に情報が提供されるよう、あらかじめ、情報の取扱いが厳正な管理の下で行われることなどを関係者間で合意するなど、関係者間における信頼関係の構築に努める必要がある。

(5) 民間重要インフラ事業者等に対する協力

政府は、セキュリティ情報及び警報情報の提供等、民間重要インフラ事業者等に対する協力を努める。

6 官民連携によるサイバー攻撃の検知と緊急対処

各重要インフラ分野においてサイバー攻撃を受けた場合又はそのおそれがある場合の対応策を定めるとともに、官民全体で対処能力の強化を行う必要がある。

(1) サイバー攻撃の検知

- 政府及び民間重要インフラ事業者等は、基幹をなす重要な情報システムに障害が発生した場合に、それがサイバー攻撃か否かを判断することが困難であることを前提に、想定される事態を十分に踏まえ、障害の内容、発生箇所、障害の範囲等、事案に対する適切な対処を行えるようあらかじめ手順を定める。
- 政府及び民間重要インフラ事業者等は、政府関係機関、情報セキュリティ関係団体、情報システムのベンダー等からセキュリティ情報及び警報情報の収集を行う。

(2) 緊急時対応計画の策定

- 各民間重要インフラ分野等においては、サイバー攻撃が発生した場合又はそのおそれがある場合の対策及び緊急時対応計画の策定について、5で定める連絡体制を活用しつつ検

討を行う。

(緊急時対応計画に想定される事項)

- ・連絡、被害拡大防止、証拠保全、復旧(応急)、再発防止等

また、この計画においては、迅速な対応を可能とするよう、サイバー攻撃の検知後の時間経過に応じた手順をとりまとめることが重要である。

- 緊急時における対処には、高度な判断を必要とする場合があることから、責任と権限を有する適切な者が速やかな判断を行うことができるよう、緊急時対応計画等の手続に定める。

### (3) 緊急時における情報の連絡手順

- サイバー攻撃を受けた場合又はそのおそれを示す情報を得た場合の緊急時における情報の連絡手順を次のとおりとする。

#### ア サイバー攻撃に関する情報の連絡

1. サイバー攻撃を受け、又はそのおそれを示す情報を得た省庁又は民間重要インフラ事業者等は、速やかな対処を講ずるとともに、分野内の他の民間重要インフラ事業者等、所管官庁、関係機関等の定められた連絡担当者に当該情報を連絡する。
2. 情報の連絡を受けた省庁は、当該情報を内閣官房に連絡するとともに、攻撃を受けた民間重要インフラ事業者等に対する指示、助言等を行う。
3. 内閣官房は、関係省庁等との連携を図り、情報収集等を行う。

#### イ 警報情報の連絡

1. 内閣官房は、攻撃又はそのおそれを示す情報の内容から必要な場合には、各省庁に警報情報を連絡する。
  2. 各省庁は、内閣官房から警報情報を受けた場合には、所管する民間重要インフラ事業者等に速やかに当該情報を連絡する。
- 政府及び民間重要インフラ事業者等は、必要に応じサイバーテロ対策の訓練を実施する。
  - 政府及び民間重要インフラ事業者等は、攻撃による被害によって国民生活や社会経済活動に影響を生じた場合には、関係者に対し、迅速かつ適切な情報の提供を行うよう努める。

#### (4) 政府における緊急対処体制の強化

- サイバー攻撃が発生した場合又はそのおそれがある場合において、内閣官房は、各省庁等との協力・連携を図り、情報集約を行うとともに、政府として対処が必要な場合には、対処方針について各省庁との調整を行う。
- 内閣官房は、このための所要の連携体制を各省庁等の協力を得て構築するとともに、各省庁は、サイバーテロ対策に係る情報収集体制及び対処体制を強化する。

### 7 情報セキュリティ基盤の構築

サイバーテロ対策を進めていくため、人材の育成、研究開発、法制度の整備等の情報セキュリティ基盤の構築を推進することが必要である。

また、重要インフラをサイバー攻撃から防護するためには、重要インフラのみならず、一般の情報システムを運用・利用する者が、いわゆるサイバーテロの脅威を認識し、セキュリティ対策の重要性についての理解を深め、必要なセキュリティ対策を講じることが重要であることから、広く一般に対して、普及啓発を行うことが必要である。

#### (1) 人材育成の推進

- 政府及び民間重要インフラ事業者等は、職員等に対する教育・訓練、セキュリティ技術の専門家の継続的な養成等に努める。

#### (2) 研究開発の推進

- 政府及び民間重要インフラ事業者等は、いわゆるサイバーテロの脅威に対して強固な基盤を構築するために必要な技術開発、脅威の分析、対策・技術に関する調査研究等を、官民の協力・連携を図りながら推進する。

#### (3) 普及啓発の推進

- 政府は、不正アクセス行為の発生状況等の公表、不正アクセス行為からの防御に関する啓発及び国内外のいわゆるサイバーテロの脅威に関する知識の普及等を行う。
- 政府は、民間重要インフラ事業者等の職員等を対象とした情報セキュリティに関する研修等を推進する。

#### (4) 法制度の整備

- 政府は、国際的動向との調和及び情報通信ネットワークにおける安全確保の観点から、関連する刑事基本法制など法制度の整備を検討する。

## 8 国際連携

サイバー攻撃は、国境を越えて行われる可能性があることから、このような攻撃に適切に対処するため、国際的な連携を推進することが必要である。

- 政府及び民間重要インフラ事業者等は、国外の情報セキュリティ関係団体等からの情報収集に努める。
- 政府は、OECDやG8におけるサイバーテロ対策に関連する国際的な取組に対する協力を推進する。
- 政府は、諸外国の関係機関との間の情報交換や共同訓練等、国際的な連携強化を推進する。

## 9 行動計画の見直し

この行動計画は、官民の連絡・連携体制の確立を中心としてとりまとめたサイバーテロ対策の初めてのものであり、政府は、この行動計画の進捗を踏まえ、定期的及び必要に応じ、この行動計画の見直しを実施する。

[http://www.bits.go.jp/taisaku/2000\\_1215/1215actionplan.html](http://www.bits.go.jp/taisaku/2000_1215/1215actionplan.html)

## サイバーテロ対策に係る官民の連絡・連携体制について

### サイバーテロ対策に係る官民の連絡・連携体制について

平成13年10月10日

「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15日、情報セキュリティ対策推進会議。以下「特別行動計画」という。)を踏まえ、以下の考え方にに基づき、サイバーテロ対策に係る官民の連絡・連携体制の構築を進めることとする。

#### 1 対象となる重要な情報システム等

特別行動計画に定める「重要インフラの基幹をなす重要な情報システム」(以下「重要システム」という。)及び特別行動計画の対象となる事業者については、いわゆるサイバーテロによって国民生活や社会経済活動に与える重大な影響を考慮し、重要インフラ分野ごとに定めることとする(別紙1参照)。

なお、具体的に対象となる重要システムの詳細については、別紙1に掲げる重要システムの例を踏まえ、各事業者において定めることとする。

#### 2 サイバー攻撃発生時等における連絡体制等

##### (1) 連絡体制

サイバー攻撃発生時等における政府と事業者との間の連絡は、重要インフラ分野ごとに、既存の事故、障害時等における連絡体制等の活用又は業界団体等におけるサイバーテロに関する連絡窓口の構築等により、各重要インフラ分野を所管する省庁(以下「所管省庁」という。)を通じて行うものとする(別紙2参照)。

また、各重要インフラにサービスを提供する情報サービス産業事業者については、個々の重要インフラ事業者を通じて行うものとする。

なお、各重要インフラ分野内における情報共有及び検討体制については、事業者間で共通する課題がある場合など、情報共有等が有効な場合に業界団体を中心として行うこととする。

##### (2) 情報連絡の対象となる事案

情報連絡の対象となる事案は、重要システムに重大な障害が発生した時、重要システムに対するサイバー攻撃を検知した時又は攻撃の予告があった時及び重要システムに対するサイバー攻撃による被害を検知した時とする(別紙3参照)。

この場合において、

の「重大な障害」とは、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして事業者が連絡を要すると判断したものを含むものとする。

の「重要システムに対するサイバー攻撃を検知した時」については、「被害は発生していないが、そのおそれが高い攻撃を検知した場合」に限ることとする（別紙4参照）。

なお、**ア**、**イ**及び**ウ**のいずれにも該当しない場合においても、サイバー攻撃の未然防止、被害の拡大防止等に資すると考えられる事案について情報の提供を行うこと並びに**エ**、**オ**に該当するかどうか不明な場合について所管省庁又は内閣官房に対して相談を行うことを妨げるものではない。

### （3）情報連絡の内容

情報連絡の内容については、事案発生時における利用可能な連絡手段、連絡担当者等の連絡を確保するための情報を必須とするほかは、その時点で判明している情報を随時連絡することとする。この際、当該情報が全容が解明するまえの断片的又は不確定なものであっても差し支えないものとする。

なお、以下に掲げる事項について、判明した範囲で随時連絡するように努めるものとする。

#### ア 対象システム

- ハードウェア、ソフトウェア（システムの名称、バージョン、パッチの適用状況等）

#### イ 事案概要

- 事案の分類（重要システムにおける障害、サイバー攻撃の検知、予告、サイバー攻撃による被害）
- 攻撃の種別（不正アクセス、サービス不能攻撃、情報漏えい・改ざん、システム破壊等）
- 原因（セキュリティホール、侵入経路、不正プログラム等）
- インフラサービスへの影響等被害の程度

#### ウ 対処状況

- 対策の概要（システムの停止・復旧、セキュリティ改善策等）
- その他の連絡先（警察・セキュリティ関係機関等）

#### エ 他の事業者に対する攻撃の可能性

#### オ その他

### （4）連絡手段

事案発生時の連絡手段については、事業者と所管省庁の間及び政府部内において事前に明確化することとする。この際、電話、FAX、e-mail等2以上の連絡手段を明示するものとする。

なお、e-mail等インターネットを用いて機密に関する情報の連絡を行う場合には、リスク分析や費用対効果などに応じて暗号等の導入の必要性について検討することとする。

## 3 政府及び事業者における対応

### （1）所管省庁における対応

所管省庁は、各事業者から2により連絡を受理した場合（重要システムに重大な障害が発生した時に行

われる連絡で、当該障害が設定ミス・操作ミスや業務の便宜のために行った行為等サイバー攻撃を原因とするものでないことが明らかである場合を除く。)には、速やかに内閣官房へ連絡するとともに、関係所管分野の事業者等からの情報収集、現状把握等に努めるものとする。

また、内閣官房からの指示、情報提供等を踏まえて、各事業者に情報の提供、対処方法、体制等についての助言、指導等を行うものとする。

#### (2) 内閣官房における対応

内閣官房は、各所管省庁からの情報、関係機関等からの関連情報等を収集・分析するとともに、事案の重要度に応じ、各所管省庁を通じた情報提供や助言、指導、対策支援等、関係省庁と連携した各種の緊急対処措置を講ずることとする。

#### (3) 事業者における対応

各事業者は、特別行動計画に定める緊急時対応計画に想定される事項(連絡、被害拡大防止、証拠保全、復旧(応急)、再発防止等)について、速やかに適切な措置を執るものとする。

### 4 情報の取扱い

#### (1) 情報共有に関する考え方

##### ア 共有の原則

本連絡・連携体制において連絡された情報の取扱いについては、法令等に定めがある場合又は連絡を行う事業者の了承がある場合を除き、連絡を受ける所管官庁及び内閣官房以外に提供しないものとする。

ただし、官民連携してサイバーテロ対策を進めるため、次の事項に該当する場合には他の事業者及び関係機関等との情報共有を行うものとする。

セキュリティホール等を発見した場合であって、他の事業者と同じ問題が生じるおそれがあると認められる場合

サイバー攻撃の発生又は攻撃の予告がある場合であって、他の事業者の重要システムが危険にさらされていると認められる場合

また、政府及び各事業者は、共有された情報につき、その保秘に十分留意しなければならないものとする。

##### イ 共有の範囲及び内容

情報共有(提供)は、注意喚起等として各事業者の対策に資するものとして行うものであることから、情報を共有(提供)するその範囲及び事項は次のとおりとする。

情報を共有(提供)する範囲は、当該情報に直接関係する事業者等(業界固有のシステムの場合には当該業界内、他の分野に関係する場合は関係するすべての分野)とする。

共有(提供)する情報の内容は、情報連絡を行った事業者が不利益を被らないよう、具



体的な対策を実施するために必要な事項に限るものとする。また、企業名や分野名を提供する必要がある場合については、原則として同意を得た上で行うものとする。

#### (2) 情報の公開に関する考え方

事業者から提供された情報は、原則として行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第5条第2号ロに規定する情報（任意提供情報）として取り扱うものとする。ただし、これは本官民連絡・連携体制の枠組みの中で情報を提供（共有）することを妨げるものではない。（なお、当該情報が情報公開法第5条第2号本文但し書きに規定する情報に該当する場合には、公開されることがある。）

### 5 その他

(1) 本連絡・連携体制の運用に関し必要な具体的事項については、年内を目途に政府及び各重要インフラで協議の上定めることとする。

(2) 本連絡・連携体制の効率的かつ効果的な運用を図るため、政府及び各事業者は訓練を実施するものとする。また、内閣官房は、平素より関係省庁及び関係機関の協力を得て、広くセキュリティ情報（セキュリティ改善に必要な情報）の収集、分析を行うとともに、これらを本連絡・連携体制の運用により得られた成果と併せて各重要インフラに随時提供するよう努めるものとする。

(3) 本申し合わせは、警報情報（サイバー攻撃の発生情報等の警戒や緊急対処に必要な情報）の共有に関する事項を中心として定めるものであるが、2(1)に定める連絡の体制は、セキュリティ情報についても、政府と重要インフラ分野各事業者間の情報共有、連絡、相談の枠組み等として活用し得るものとする。

(4) 本申し合わせについては、運用の状況、情勢の変化等を踏まえ、随時見直しを行うものとする。

<http://www.bits.go.jp/suisinkaigi/dai4/terotaisaku.html>

## 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 (別紙1)

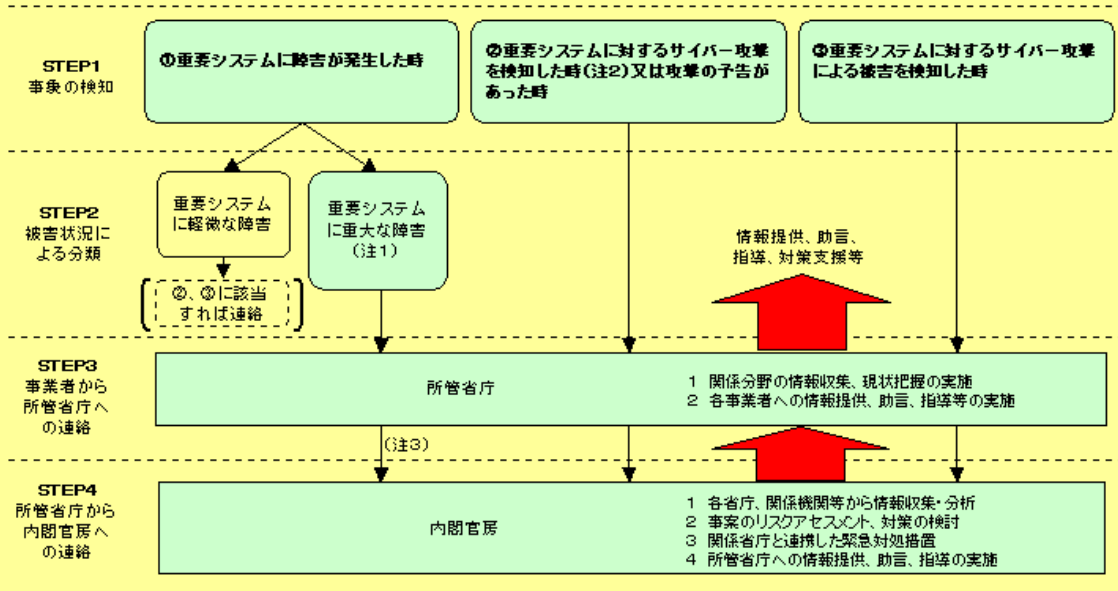
分野(注1)	サイバー攻撃による情報システムの障害、不正な処理などの質感・危険性	対象となる事業者(注2)	対象となる重要システム例(注3)
情報通信	<ul style="list-style-type: none"> <li>電気通信サービスの停止</li> <li>電気通信業務に関する通信の妨害</li> <li>番組制作・放送運行、緊急災害対応など情報発信機能の障害</li> </ul>	<ul style="list-style-type: none"> <li>第一種及び特別第二種等の主要な電気通信事業者</li> <li>放送事業者(NHK、衛星放送、ケーブルテレビを含む。)</li> </ul>	<ul style="list-style-type: none"> <li>電気通信事業用設備</li> <li>通信管理業務システム</li> <li>放送業務用システム群</li> </ul>
情報サービス	<ul style="list-style-type: none"> <li>情報システム共通のセキュリティホールによる広範な障害等</li> </ul>	<ul style="list-style-type: none"> <li>重要インフラにおける重要システムを管理・運営する情報サービス産業事業者</li> </ul>	
金融	<ul style="list-style-type: none"> <li>預金の払い出し、振込等資金移動、融資業務などの業務の停止等</li> </ul>	<ul style="list-style-type: none"> <li>銀行、信用金庫、信用組合、農業協同組合等</li> </ul>	<ul style="list-style-type: none"> <li>勘定システム</li> <li>資金証券システム</li> <li>国際システム</li> <li>海外接続システム(オープンネットワークを利用したサービスを含む。)</li> </ul>
航空	<ul style="list-style-type: none"> <li>運航の遅延、欠航</li> <li>航空機の安全運航に対する支障等</li> </ul>	<ul style="list-style-type: none"> <li>定期航空協会加盟事業者</li> <li>国土交通省(航空管制・気象)</li> </ul>	<ul style="list-style-type: none"> <li>運航システム</li> <li>予約・搭乗システム</li> <li>整備システム</li> <li>貨物システム</li> <li>航空管制システム</li> <li>気象情報システム</li> </ul>
鉄道	<ul style="list-style-type: none"> <li>列車運行の遅延、運休</li> <li>列車の安全安定輸送に対する支障等</li> </ul>	<ul style="list-style-type: none"> <li>JR及び大手民間鉄道事業者等の主要な鉄道事業者</li> </ul>	<ul style="list-style-type: none"> <li>列車運行管理システム</li> <li>電力管理システム</li> <li>座席予約システム</li> </ul>
電力	<ul style="list-style-type: none"> <li>電力供給の停止</li> <li>電力プラントの安全運用に対する支障等</li> </ul>	<ul style="list-style-type: none"> <li>一般電気事業者、日本原子力発電(株)及び電研開発(株)</li> </ul>	<ul style="list-style-type: none"> <li>制御システム</li> <li>運転監視システム</li> </ul>
ガス	<ul style="list-style-type: none"> <li>ガスの供給の停止</li> <li>ガスプラントの安全運用に対する支障等</li> </ul>	<ul style="list-style-type: none"> <li>主要なガス事業者</li> </ul>	<ul style="list-style-type: none"> <li>プラント制御システム</li> <li>遠隔監視・制御システム</li> </ul>
政府・行政サービス	<ul style="list-style-type: none"> <li>政府、行政サービスに対する支障</li> <li>個人情報保護の漏洩、盗取、改ざん</li> </ul>	<ul style="list-style-type: none"> <li>各省庁</li> <li>地方公共団体</li> </ul>	<ul style="list-style-type: none"> <li>各省庁及び地方公共団体の情報システム(電子政府への対応)</li> </ul>

注1) 対象とする重要インフラ分野については、医療分野等を定めることなど引を鑑み検討することとしている。  
 注2) ここに掲載している対象事業者は、重点的に対策を実施すべし事業者であり、各分野のこれら以外の事業者についても同様の対策を講ずることが望ましい。  
 また、主要な事業者としているものは、Y2K対策等における対象事業者に準じるものである。  
 注3) 対象となる重要システムの詳細については、質感・危険性を例を踏まえ、事業者において定める。

## サイバー攻撃発生時等における連絡体制等 (別紙2)

分野	報告の連絡体制	サイバー攻撃発生時等における連絡体制	情報セキュリティ関連連絡の共有各分野におけるセキュリティ対策等の連絡体制
情報通信	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>電気通信事業者に基づく急務の停止等の対応大臣への報告</li> <li>放送局等事業者に基づく放送局等に対する電気通信設備の障害状況等報告</li> <li>放送局等事業者、重要放送局等に対する緊急事への連絡</li> <li>(2) 政府→事業者、事業者間</li> <li>ウイルス発生等緊急情報を発着門及び関係省との間で通知・共有</li> </ul>	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>既許の連絡体制を活用して実施</li> <li>(2) 政府→事業者</li> <li>既許の連絡体制を活用して実施</li> </ul>	<ul style="list-style-type: none"> <li>ウイルス発生等の情報共有体制を活用して実施</li> </ul>
情報サービス		<ul style="list-style-type: none"> <li>重要インフラにサービスを提供する事業者は、各々のインフラ事業者を通じて対応。</li> <li>バンカー等の事業者は、情報の提供・公開を通じて対応を支援。</li> </ul>	
金融	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>銀行等に基づく(貸付)戻し、貸付等の決済業務に遅延・停止等の内容報告大臣(金融庁)への報告</li> <li>(2) 政府→事業者、事業者間</li> <li>特になし</li> </ul>	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>既許の連絡体制を活用して実施</li> <li>(2) 政府→事業者</li> <li>発着門を通じて実施</li> </ul>	<ul style="list-style-type: none"> <li>金融庁、FISCO等の発着門を通じて実施</li> </ul>
航空	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>航空機に基づく航空機の運航に関する国土交通大臣への報告</li> <li>(2) 政府→事業者、事業者間</li> <li>サイバーテロに関する連絡窓口を設置</li> <li>航空機安全情報の不具合に関する情報を関係機関で共有(空防軍団)</li> </ul>	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>事故時は事故処理関係に基づき実施</li> <li>遅延、飛行予告は連絡窓口を通じて実施</li> <li>(2) 政府→事業者</li> <li>連絡窓口を通じて事業者へ直接連絡</li> </ul>	
鉄道	<ul style="list-style-type: none"> <li>(1) 事業者→政府、政府→事業者</li> <li>鉄道事故等報告規則に基づく、鉄道運転事故等に関する国土交通大臣への報告</li> <li>サイバーテロに関する連絡体制を設置</li> <li>(2) 事業者間</li> <li>特になし</li> </ul>	<ul style="list-style-type: none"> <li>(1) 事業者→政府、政府→事業者</li> <li>事故時は既許の事故報告体制により実施。</li> <li>事故に至らないサイバーテロに関しては、サイバーテロの連絡体制により実施。</li> </ul>	
電力	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>防災関係計画、電気関係報告規則に基づくお電所事故等に関する総務大臣への連絡</li> <li>(2) 政府→事業者、事業者間</li> <li>特になし</li> </ul>	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>既許の連絡体制を活用して実施</li> <li>(2) 政府→事業者</li> <li>発着門を通じて実施</li> </ul>	<ul style="list-style-type: none"> <li>発着門を通じて実施</li> </ul>
ガス	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>ガス事業実施規則に基づく、一定規模のガス供給支障等の総務大臣への報告</li> <li>(2) 政府→事業者、事業者間</li> <li>災害によりガス供給支障が発生した場合等における、ガス協会「防災情報連絡」に基づく発着門連絡</li> </ul>	<ul style="list-style-type: none"> <li>(1) 事業者→政府</li> <li>既許の連絡体制を活用して実施</li> <li>(2) 政府→事業者</li> <li>発着門を通じて実施</li> </ul>	<ul style="list-style-type: none"> <li>発着門の発着門を通じて実施</li> </ul>
政府・地方公共団体	<ul style="list-style-type: none"> <li>(1) 各省庁→関係省庁</li> <li>政府機関の情報システムに関する緊急時の連絡等についてに基づく連絡</li> <li>(2) 関係省庁→各省庁</li> <li>政府機関の情報システムに関する緊急時の連絡等についてに基づく情報提供</li> </ul>	<ul style="list-style-type: none"> <li>政府毎の連絡体制で実施</li> </ul>	<ul style="list-style-type: none"> <li>政府毎の連絡体制で実施</li> </ul>

### 情報連絡の対象となる事案



- (注1) 「重大な障害」とは、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして事業者が連絡を要すると判断したものを含む。
- (注2) 「サイバー攻撃を検知した時」については、「被害は発生していないが、そのおそれが高い攻撃を検知した場合」に限ることとする(別紙4参照)。
- (注3) 重大な障害が設定ミス・操作ミスや業務の便宜のために行った行為等サイバー攻撃を原因とするものでないことが明らかである場合は、連絡を要しない。

### 「サイバー攻撃を検知した時」について

連絡の要否	例
連絡の対象となるもの (被害は発生していないが、そのおそれが高い攻撃を検知した場合)	<p>○重要システムへの影響が相当程度予想される攻撃を検知した場合(注)</p> <ul style="list-style-type: none"> <li>外部から侵入できないはずの内部ネットワークにある重要システムに不正アクセスの試みが行われた場合</li> <li>重要システム内で重要システムに障害を与えるおそれのあるコンピュータウイルスが発見された場合</li> <li>攻撃パターンや過去の事例等の状況から、重要システムに重大な影響を及ぼすおそれがあると思われる攻撃が行われた場合</li> </ul> <p>○重要システムに対して特定のグループ等から明らかな査問・目的を持って攻撃が行われたことを検知した場合</p>
連絡の対象とならないもの	<p>○重要システムに対する攻撃の予備行為として行われたおそれのあるものを検知した場合</p> <ul style="list-style-type: none"> <li>外部から重要システムに対するアクセスを可能とするバックドアを発見した場合</li> <li>外部から重要システムに対するアクセスを可能とする不審なモデム等が発見した場合</li> <li>重要システムに対する攻撃を行うプログラム(ツール)が仕掛けられているのを発見した場合</li> <li>メンテナンス用の接続口から第三者のアクセスを可能とする不正な設定を発見した場合</li> </ul>
	<p>○重要システムに対する攻撃に必要な情報を窃取する行為を検知した場合</p> <ul style="list-style-type: none"> <li>重要システムに関するシステム構成や設定情報などが盗まれた場合</li> <li>重要システムに関するパスワードや暗号鍵等が盗まれた場合</li> <li>重要システムに直接接続されたゲートウェイにスニファが仕掛けられた場合</li> </ul>
	<p>○重要システムに関係しないシステムへの攻撃を検知した場合</p> <ul style="list-style-type: none"> <li>インターネットに接続されたファイアウォールに対する単なるポートスキャンを検知した場合</li> <li>専ら宣伝広告用のホームページサーバに対する不正アクセス・改ざんを検知した場合</li> <li>専ら事務用の電子メールサーバへのコンピュータウイルスの到来を検知した場合</li> </ul>

注) 事例・情勢等の適切な判断が行えるよう、「重要システムに障害を与えるおそれのあるコンピュータウイルス」や「攻撃パターンや過去の事例等の状況から、重要システムに重大な影響を及ぼすおそれのあると思われる攻撃」については、政府から情報提供を行い、これらの情報を参考に連絡の対象となるか否かを事業者において判断する。

### 3. 情報システム安全対策指針

#### 情報システム安全対策指針

##### 情報システム安全対策指針

平成 9 年 9 月 18 日制定（国家公安委員会告示第 9 号）

平成 11 年 11 月 22 日一部改正（国家公安委員会告示第 19 号）

#### < 目次 >

##### 第 1 編 総則

##### 第 2 編 情報システムについて講ずべき安全対策

###### 管理者が講ずべき対策

###### 第 1 章 ネットワーク

###### 第 2 章 ホスト等

###### 第 3 章 施設

###### 第 4 章 攻撃等認知時における措置等

###### 第 5 章 個人情報保護

###### ユーザが講ずべき対策

###### コンピュータ・ウイルスに関し管理者及びユーザが講ずべき対策

##### 第 3 編 開放的なネットワークに接続する情報システムについて追加的に講ずべき安全対策

###### 管理者が講ずべき対策

###### 第 1 章 ネットワーク

###### 第 2 章 攻撃等認知時における措置等

###### コンピュータ・ウイルスに関し管理者及びユーザが講ずべき対策

##### 第 1 編 総則

#### 1 目的

本指針は、情報システムの関係者に対し、情報システムに係る犯罪、不正行為、個人情報の漏えい、災害等による被害を未然に防止し、又は最小限に抑えるために講ずべき対策及び犯罪発生時における警察との連携を確保するための措置を示すことにより、国民生活の安全を確保し、情報社会における秩序を維持することを目的とする。

#### 2 定義

- (1) 情報システム コンピュータ・システムを中心とする情報処理及び通信に係るシステム（人的組織を含む。）をいう。
- (2) ネットワーク 通信のために用いられる装置及び回線をいう。
- (3) ホスト等 クライアント・サーバ・システムにおけるサーバ及びクライアント、メインフレーム・システムにおけるホスト・コンピュータ及び端末並びにネットワークの接続を制御するコンピュータをいう。
- (4) 個人情報 個人に関する情報であつて、特定の個人を識別することができるものをいう。
- (5) セキュリティ 犯罪、不正行為、災害若しくは事故による被害を受けること又は情報システムが犯罪若しくは不正行為の用に供されることが防止されている状態をいう。
- (6) 管理者 情報システムの設置及び運営に関し責任及び権限を有する者をいう。
- (7) ユーザ 情報システムにより提供されるサービスを利用するためにアクセスする権限を有する者をいう。
- (8) 統括セキュリティ責任者 情報システムのセキュリティに関し責任及び権限を有する者をいう。
- (9) 監査責任者 監査に関し責任及び権限を有する者をいう。
- (10) 危機管理責任者 危機に対する対応に関し責任及び権限を有する者をいう。
- (11) 危機管理オペレータ 危機の状況を記録するとともに、危機管理責任者の指示を受け、具体的な対処を行う者をいう。
- (12) アクセス コンピュータ・システムを利用できる状態とすること又はその内部に電子的に存在する情報を取り扱うことをいう。
- (13) 不正アクセス 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）第3条第2項に規定する不正アクセス行為その他の不正な手段によりユーザ以外の者が行うアクセス又はユーザが行う権限外のアクセスをいう。
- (14) 危機 情報システムに被害が生じ、又は生ずるおそれがある状態をいう。
- (15) 攻撃 コンピュータ・システムのセキュリティを侵害することを目的として故意に行われるアクセスをいう。

### 3 対策の策定

#### (1) モデル・システム

本指針は、企業会計システム、顧客管理システムその他の次に掲げる要件を満たす情報システムをモデルとして、情報システムのセキュリティを確保するために必要と考えられる項目を列挙している。

ア ホスト等を回線により相互に接続したネットワーク・システムであること。

イ 当該情報システムの管理者がユーザを管理することができるものであること。

ウ 破壊、改ざん又は漏えいによる影響が小さくない情報を処理するものであること。

エ 当該情報システムが運用停止することにより受ける影響が小さくない業務を処理するものであること。

#### (2) 対策の策定方法

管理者は、対象とする情報システムについて、リスク分析に基づきセキュリティ方針を立て、当該方針に沿って本指針の示す項目から必要なものを選択するとともに、必要に応じ追加を行い、対策を策定する

必要がある。特に、社会的に重要な基盤を形成している情報システムについては、サイバーテロのリスクについても考慮する必要がある。

### (3) 他の基準の活用

対策の策定に当たっては、別表に掲げる他省により示された基準も活用することが重要である。

## 第2編 情報システムについて講ずべき安全対策

インターネット等開放的なネットワークとの接続の状況の有無にかかわらず、すべての情報システムについて講ずべき安全対策は、次のとおりである。

### I 管理者が講ずべき対策

#### 第1章 ネットワーク

管理者は、ネットワークに係る不正アクセス、他者のユーザIDを不正に利用したなりすまし等を防止するため、次に掲げる項目について対策を講ずること。

##### 1 監視

###### (1) ログ

ア ログを取得すること。ログの内容は、少なくともアクセスした者を特定可能なものであること。

イ ログ自体のセキュリティを確保すること。

ウ ログを定期的に監査すること。

エ ログは、次回の監査まで保管すること。

###### (2) 不正アクセス検出機能

不正アクセスが行われた場合に、これを検出し、危機管理責任者に知らせる機能を設けること。

###### (3) その他

ア ネットワーク及びホスト等の状態を監視する機能を設けること。

イ 端末を利用したアクセスについて当該端末を特定する機能を設けること。

ウ 異常がある場合に、ネットワーク及びホスト等の機能を停止させることができる機能を設けること。

##### 2 パスワード

パスワードにより認証を行うネットワークについては、次の対策を講ずること。

(1) ユーザには、必ずパスワードを設定させ、その秘匿に努めさせること。

(2) 他者が容易に推測できる語句等をパスワードとして設定しないようユーザを指導し、又は設定を拒否する機能をシステムに設けること。

(3) パスワードを適切な期間ごとに変更するようユーザを指導し、又は変更を促す機能をシステムに設けること。

(4) パスワードの再入力回数を制限するなど、他者によるパスワードの推測を困難にするための措置を

講ずること。

- (5) ユーザがパスワードを忘れたときなどに、パスワードを通知する場合に備え、本人確認の方法等について手続を定めておくこと。
- (6) パスワード・ファイルの暗号化等の措置を講ずるなど、パスワードの秘匿に努めること。

### 3 ネットワーク・アクセス

- (1) ログインに際し、識別及び認証を行うこと。
- (2) 認証の手段については、当該情報システムに求められるセキュリティに応じ選択すること。
- (3) 前回のログインの日時を確認できる機能を設けること。

### 4 ユーザID管理

- (1) 退職、異動、長期出張、長期留学等により、不要となり、又は長期間使用されないユーザIDについては、廃止等の措置を講ずること。
- (2) 長期間ログインが無いユーザに対して、文書等によりその旨を通知すること。
- (3) ユーザから要求があったときは、当該ユーザによる使用状況を開示すること。

### 5 暗号化

- (1) 通信を行うときは、必要に応じデータ等を暗号化すること。
- (2) 暗号鍵の保管を適切に行うこと。特に、ユーザの暗号鍵を集中的に管理する場合は、その保管の適正を図ること。

### 6 データ交換

- (1) データ交換に先立ち、意図する通信相手であることを確認するため、認証を行うこと。
- (2) デジタル署名等によりデータの完全性の確認を行うこと。
- (3) データが送信されたこと、受信されたこと等を証明し、これらの否認を防止できる機能を設けること。
- (4) (1)から(3)までを暗号を利用して行う場合であって、ユーザの暗号鍵を集中的に管理するときは、その保管の適正を図ること。

### 7 災害等対策

災害、事故等による回線の途絶を避けるため、必要に応じ回線の二重化を図ること。

## 第2章 ホスト等

管理者は、ホスト等に係る不正アクセス、他者のユーザIDを不正に利用したなりすまし等を防止するため、次に掲げる項目について対策を講ずること。

### 1 監視

#### (1) ログ

ア ログを取得すること。ログの内容は、少なくともアクセスした者を特定可能なものであること。

イ ログ自体のセキュリティを確保すること。

ウ ログを定期的に監査すること。

エ ログは、次回の監査まで保管すること。

#### (2) 不正アクセス検出機能

不正アクセスが行われた場合に、これを検出し、危機管理責任者に知らせる機能を設けること。

### 2 パスワード

パスワードにより認証を行うホスト等については、次の対策を講ずること。

(1) ユーザには、必ずパスワードを設定させ、その秘匿に努めさせること。

(2) 他者が容易に推測できる語句等をパスワードとして設定しないようユーザを指導し、又は設定を拒否する機能をシステムに設けること。

(3) パスワードを適切な期間ごとに変更するようユーザを指導し、又は変更を促す機能をシステムに設けること。

(4) パスワードの再入力の回数を制限するなど、他者によるパスワードの推測を困難にするための措置を講ずること。

(5) ユーザがパスワードを忘れたときなどに、パスワードを通知する場合に備え、本人確認の方法等について手続を定めておくこと。

(6) パスワード・ファイルの暗号化等の措置を講ずるなど、パスワードの秘匿に努めること。

### 3 ホスト等へのアクセス

(1) ログインに際し、識別及び認証を行うこと。

(2) 認証の手段については、当該情報システムに求められるセキュリティに応じ選択すること。

(3) 前回のログインの日時を確認できる機能を設けること。

### 4 アクセス制御

セキュリティ方針に応じ、ホスト等へのアクセス制御のほか、データベースのデータ、ファイル等ごとにアクセス制御を行うこと。

### 5 オペレーティング・システム

アクセス制御機能等セキュリティを確保するために必要となる機能を有するオペレーティング・システムを選択すること。

### 6 セキュリティ・ホール

(1) 専用のソフトウェア等を用いて、セキュリティ・ホールのチェックを行うこと。



(2) セキュリティ・ホールが発見されたときは、それを無くすために必要な措置を講ずること。

#### 7 暗号化

(1) データを保管する際は、必要に応じデータ等を暗号化すること。

(2) 暗号鍵の保管を適切に行うこと。特に、ユーザの暗号鍵を集中的に管理する場合は、その保管の適正を図ること。

#### 8 ホスト等の管理

(1) 各装置を容易に取り外し、取り付け、又は持ち運ぶことができないよう措置を講ずること。

(2) ディスプレイは、表示された情報を利用者以外の者に直接に又は容易に見られないように設置すること。

#### 9 災害等対策

(1) 必要に応じ、装置を二重化し、代替運転機能を設けるなどの措置を講ずること。

(2) 自動回復機能を設けること。

### 第3章 施設

管理者は、ホスト・コンピュータ等コンピュータ・システムを構成する重要な装置を設置する施設を部外者の侵入、災害等から保護するため、次に掲げる項目について対策を講ずること。

#### 1 資格及び身分証明書等

(1) 資格

ア 施設立入資格（以下「資格」という。）を設けること。

イ 資格は、必要最小限の者に対して、有効期間を限って与えること。

ウ 資格は、個人に対して与えること。

エ 資格の付与に際しては、立入りが可能な施設の範囲及び立入りの目的を特定すること。

(2) 身分証明書等

ア 資格を与えた者には、次の事項が記録された身分証明用の文書、ICカード等（以下「身分証明書等」という。）を交付すること。

(ア) 資格の有効期間

(イ) 立入りが可能な施設の範囲及び立入りの目的

(ウ) 顔写真等の個人識別情報

イ 身分証明書等は、偽造等の困難な材質のものとする。また、身分証明書等の原紙等が流出することのないよう厳重な管理を行うこと。

ウ 資格を与えた者が、身分証明書等を紛失し、又はき損したときは、直ちに統括セキュリティ責任者に届け出させること。

エ ウの届出があったときは、直ちに当該身分証明書等を無効とすること。

## 2 入退管理等

### (1) 入退管理

ア 施設への立入りを許可するに当たっては、身分証明書等により、その都度資格を確認すること。

イ 施設への立入りを許可する期間を限定すること。

ウ 立ち入る者の氏名、許可の有効期間、立入りが可能な施設の範囲、立入りの目的等、施設立入許可（以下「許可」という。）に関する記録を作成し、保存すること。

エ 許可を与えた者には、記章等の施設立入票を貸与し、見やすい位置に着用させること。

オ 施設立入票については、1(2)イからエまでに準じ対策を講ずること。

カ 建物、コンピュータ室等の出入口において、資格及び許可の有無をチェックすること。

キ 施設に物資を搬出入するときは、その都度、当該物資、運搬用具等をチェックすること。

ク 物資の搬出入に際しては、担当者の氏名、物資の名称、数量、搬出入の日時等の記録を作成し、保存すること。

ケ 警備員を配置し、入退管理に当たらせること。

### (2) 防犯設備等

ア 敷地の出入口の数を制限し、資格の確認等を行うための施設を設けること。

イ 敷地内に侵入センサ、防犯カメラ等を設置するなど、侵入の発見及び抑止のための措置を講ずること。

ウ 建物、コンピュータ本体又は周辺機器が設置されている部屋、電源室、空調室、MDF（主配線盤）室、IDF（中間配線盤）室、データ保管室等の出入口及び開口部には、侵入センサを設置するなど、侵入の発見及び抑止のための措置を講ずること。

エ 警備員に施設内外の巡回に当たらせること。

## 3 災害等対策

(1) 施設の立地に当たっては、可能な限り自然災害の少ない場所を選定すること。

(2) 建物については、耐震構造とするとともに、防火構造とすること。

(3) 各種設備については、地震による移動、転倒及び震動防止の措置を講ずること。

(4) 内装については、不燃材料を使用するなど、防火措置を講ずること。

(5) 電源設備については、停電に対する措置を講ずること。

(6) 空気調和装置については、防火措置及び防水措置を講ずること。水冷式空気調和装置を使用する場合は、断水に対する措置を講ずること。

## 第4章 攻撃等認知時における措置等

管理者は、犯罪発生時における警察との連携を確保し、危機に対して的確に対応するとともに、セキュリティを確保するため、次に掲げる項目について対策を講ずること。

## 1 攻撃等認知時における措置

- (1) ユーザ等に対し、攻撃、事故その他情報システムのセキュリティを侵害する行為又は事態（以下「攻撃等」という。）を認知したときは、直ちに危機管理責任者に報告することを義務付けること。
- (2) 攻撃を受けた対象、不正アクセス検出の結果、ログイン時のログ等、その後の監査又は調査に必要な情報を、攻撃等を認知した時点の状態で作成すること。
- (3) 警察機関等への通報が必要なときは、直ちに通報すること（(4)に掲げる措置を除く。）
- (4) 攻撃が不正アクセス行為の禁止等に関する法律第3条第2項に規定する不正アクセス行為であり、同法に規定する都道府県公安委員会による援助が必要なときは、援助を受けたい旨の申出をすること。
- (5) 警察機関等の調査等が終了し、復旧を行うに当たっては、作業の経過を記録すること。

## 2 組織体制

- (1) 責任及び権限の明確化のため、次に掲げる体制をとること。

### ア 通常の体制

専任の統括セキュリティ責任者及び監査責任者を置くこと。

### イ 危機管理体制

専任の危機管理責任者及び危機管理オペレータを置くこと。

- (2) (1)ア及びイの責任者等のほか、責任及び権限の明確化のため、必要に応じ、その他の責任者等を置くこと。

## 3 情報システムの開発、運用及び保守

### (1) 開発

ア 開発に従事する者以外の者に、基礎データ等の情報が漏えいすることを防止する措置を講ずること。

イ システム設計等に関し、ドキュメントを作成すること。

ウ 運用及び保守のためのマニュアルを作成すること。

エ 運用のためのマニュアルには、危機の範囲及び危機に対する対応を定めること。

### (2) 運用

ア マニュアルに基づいて行うこと。

イ 運用記録を取ること。

### (3) 保守

ア マニュアルに基づいて行うこと。

イ 保守記録を取ること。

## 4 データ管理

- (1) 重要なデータを記録している記録物が不要となったときは、データの消去、記憶媒体の破砕等アクセスが不可能となるような措置を講じた後、当該記録物を直ちに廃棄すること。

- (2) 重要なデータを記録している記録物については、保管場所の入退管理、データの暗号化等の措置を講

ずること。

(3) フロッピー・ディスク等の容易に取り外すことができる記憶媒体については、必要に応じ、データの暗号化、物理的な書込み禁止の措置等所要の措置を講ずること。

## 5 バックアップ

(1) バックアップは、定期的に、かつ、可能な限り頻繁に行うこと。

(2) バックアップ・ファイルは、適切な保存方法、保存期間等を定め、原本と異なる場所に保管すること。

## 6 監査

(1) 監査は、情報システムの安全性、信頼性及び保全性並びに犯罪予防の観点から行うこと。

(2) 監査の方法を定めて、マニュアルを作成すること。

(3) 計画的かつ定期的に行うこと。ただし、重大な事故が発生し、又は発生するおそれがあると認められるときは、その都度行うこと。

(4) 監査報告書を作成すること。

(5) 統括セキュリティ責任者は、監査結果に基づき、速やかに所要の措置をとること。

## 7 教育及び訓練

(1) 危機発生時の措置について、マニュアルを作成してユーザに配布するとともに、定期的に訓練を行うこと。

(2) 危機が社会に与える影響の大きさ等をユーザに理解させること等により、モラルの向上を図ること。

(3) ユーザによる対策の実施状況を監視し、十分な措置が講じられていない場合は指導を行うこと。

## 第5章 個人情報保護

管理者は、情報システムにおいて処理される個人情報を保護するため、次に掲げる項目について対策を講ずること。

### 1 個人情報の収集等

(1) 個人情報の収集は、あらかじめ収集の目的を明確に定め、その目的を達成するために必要な範囲内で、適法かつ公正な手段によって行うこと。

(2) 本人以外からの個人情報の収集は、本人の権利利益が不当に侵害されるおそれのない場合に限って行うこと。

(3) 個人情報は、収集の目的に必要な範囲内で正確かつ最新の状態に保つこと。

(4) 個人情報の収集の目的及び範囲は、原則として、公開すること。

### 2 個人情報の利用及び提供

(1) 個人情報の利用及び提供は、原則として、収集の目的の範囲内で行うこと。

(2) 収集の目的の範囲を超える個人情報の利用及び提供は、原則として、本人の同意がある場合又は法律の規定による場合に限って行うこと。

### 3 自己情報の開示等

- (1) 本人から自己の個人情報の開示を求められたときは、原則として、これに応じること。
- (2) 本人から自己の個人情報の訂正、追加又は消去を求められたときは、その内容を確認の上、原則としてこれに応じること。

## II ユーザが講ずべき対策

### 1 パスワードの管理

パスワードにより認証を行うコンピュータ・システムを利用する場合は、次のことに留意すること。

- (1) メモを残さないなど、パスワードの秘匿に努めること。
- (2) 次のような、他者が容易に推測できる語句等をパスワードとして使用しないこと。

ア 短いもの又は単純なもの

イ 辞書に記載されているもの

ウ 家族の名前、生年月日等、ユーザ自身に関するもの

エ 過去に使用したもの

- (3) 適切な期間ごとにパスワードを変更すること。

### 2 暗号化

- (1) 通信を行うときは、経済取引にかかわる情報等の重要なデータ等を暗号化すること。
- (2) 暗号鍵の保管を適切に行うこと。

### 3 データ交換

- (1) データ交換に先立ち、意図する通信相手であることを確認するため、認証を行うこと。
- (2) デジタル署名等によりデータの完全性の確認を行うこと。

### 4 端末等の管理

- (1) 端末から離れるときは、次に掲げる措置のいずれかを講ずること。
  - ア 電源を切る。(電源キーを使用している場合は、電源キーを抜く。)
  - イ ログアウトする。
  - ウ パスワード付きスクリーン・セーバを使用する。
- (2) ディスプレイに表示された情報を、直接に又は容易に他者に見られないよう留意すること。
- (3) ユーザIDの不正な利用を発見するため、前回のログインの日時を確認すること。

## 5 身分証明書等の管理

身分証明書等を交付された場合は、次のことに留意すること。

- (1) 身分証明書等を厳重に管理し、紛失しないこと。
- (2) 身分証明書等を他者に貸与しないこと。
- (3) 身分証明書等を紛失したときは、直ちに統括セキュリティ責任者に届け出ること。

## 6 攻撃等認知時における措置

- (1) 攻撃等を認知したときは、危機管理責任者に報告すること。
- (2) 攻撃を受けた対象、不正アクセス検出の結果、ログイン時のログ等、その後の監査又は調査に必要な情報を、攻撃等を認知した時点の状態で作成すること。

## 7 データ管理

- (1) 重要なデータを記録している記録物が不要となったときは、データの消去、記憶媒体の破砕等アクセスが不可能となるような措置を講じた後、当該記録物を直ちに廃棄すること。
- (2) 重要なデータを保存するときは、データを暗号化すること。
- (3) フロッピー・ディスク等の容易に取り外すことのできる記憶媒体については、必要に応じ、データの暗号化、物理的な書き込み禁止の措置等所要の措置を講ずること。
- (4) 携帯端末等については、重要なデータを内蔵の記憶装置に保存することを避け、やむを得ず保存する場合は、データの暗号化等の措置を講ずること。

## 8 バックアップ

- (1) バックアップは、定期的に、かつ、可能な限り頻繁に行うこと。
- (2) バックアップ・ファイルは、適切な保存方法、保存期間等を定め、原本と異なる場所に保管すること。

## III コンピュータ・ウイルスに関し管理者及びユーザが講ずべき対策

### 1 システムの使用開始時に講ずべき措置

ホスト等を起動させるときは、始めにワクチン・プログラムを用いるなどして、コンピュータ・ウイルスのチェックを行うこと。

### 2 新たに入手したプログラムを使用するときに講ずべき措置

#### (1) 出所不明のプログラムの使用自粛

フリーウェア、シェアウェア等のうち、出所が不明のプログラムは、コンピュータ・ウイルスに感染しているおそれがあるため、可能な限り使用しないこと。

#### (2) コンピュータ・ウイルスのチェック

新たに入手したプログラムを使用するときは、あらかじめ、ワクチン・プログラムを用いるなどして、

少なくとも次の点を調べることにより、コンピュータ・ウイルスのチェックを行うこと。また、チェックを行った結果、陽性とされたもの及び陽性の疑いのあるものについては使用しないこと。

なお、オの点を調べるときは、端末等をネットワークから切り離して行うこと。

- ア ファイル（隠しファイルを含む。以下同じ。）に内容の不明なもの又は不必要なものが無いか。
- イ ファイルの作成日時又は変更日時が異常でないか。
- ウ ファイル・サイズが異常な値のファイルが無いか。
- エ ファイル名に拡張子を付加するオペレーティング・システムを使用している場合に、予定されていない拡張子を付加されたファイルが無いか。
- オ プログラムの各種機能を作動させることにより不正な命令が機能しないか。

### 3 システム使用中に講ずべき措置

#### (1) コンピュータ・ウイルスのチェック

ワクチン・プログラムを用いるなどして、少なくとも次の点を調べることにより、コンピュータ・ウイルスのチェックを行うこと。

なお、新たにファイルを入手したときは、ワクチン・プログラムによるチェックを行うこと。

- ア ファイルの作成日時又は更新日時が異常でないか。
- イ ファイル・サイズが異常な値になっていないか。
- ウ ファイルの内容に変化が無いか。
- エ 余計なファイルが増えていないか。
- オ 存在しているはずのファイルが無くなっていないか。
- カ 余計なプログラムが主記憶装置に常駐していないか。

#### (2) 作動状況の監視

ホスト等の作動状況を監視し、次のような異状が現れた場合は、ワクチン・プログラムを用いるなどしてチェックを行うこと。

- ア アクセスすることが想定されない装置にアクセスする。
- イ 記憶媒体へのアクセス時間が異常に長い。
- ウ 利用可能な記憶領域が通常より少ない。
- エ 記憶媒体の未使用領域が急激に小さくなる。
- オ 異常なメッセージが出る。
- カ 誤入力が多い。

### 4 コンピュータ・ウイルス発見時に講ずべき措置

#### (1) ネットワークからの切離し

使用中の端末等をネットワークから切り離すこと。

#### (2) コンピュータ・ウイルスの除去等

ワクチン・プログラムを用いるなどして、コンピュータ・ウイルスを除去し、又はその機能を停止させ

ること。

(3) ファイルの修復

ファイルの破壊又は改ざんが行われたときは、あらかじめ作成されたマニュアルに基づき、修復ツール等を用いて修復すること。

(4) 再起動

再起動は、システム・ファイルのバックアップ・ファイルにより行うこと。

(5) 危機管理責任者への報告

速やかに危機管理責任者に報告すること。

(6) ユーザへの通知

危機管理責任者は、ユーザに対し、とるべき措置を速やかに通知すること。

5 その他

(1) アクセス制御等

コンピュータ・ウイルスによるファイルの破壊又は改ざんを防止するため、必要に応じ、アクセス制御等の措置を講ずること。

(2) バックアップ

ア システム・ファイルのバックアップ・ファイルを作成し、保存すること。

イ バックアップに当たっては、ワクチン・プログラムを用いるなどしてチェックを行うこと。

(3) ワクチン・プログラムの更新等

ア 新種のコンピュータ・ウイルスに対応するため、必要に応じ、ワクチン・プログラムを更新すること。

イ ワクチン・プログラムを用いるときは、適切な条件設定を行うこと。

(4) 教育

管理者は、コンピュータ・ウイルス対策に関するマニュアルを作成してユーザに配布するとともに、マニュアルの内容をよく理解させておくこと。

第3編 開放的なネットワークに接続する情報システムについて追加的に講ずべき安全対策

情報システムのうち、インターネット等開放的なネットワークに接続するものについて、第2編に示した安全対策に加え、不正アクセス、コンピュータ・ウイルスの侵入等の防止の観点から講ずべき安全対策は、次のとおりである。

なお、開放的なネットワークに接続する情報システムについては、第2編に示した安全対策についても、不正アクセス、コンピュータ・ウイルスの侵入等のリスクの増加を考慮する必要がある。

1 管理者が講ずべき対策

第1章 ネットワーク

管理者は、開放的なネットワークを介した不正アクセス、コンピュータ・ウイルスの侵入等を防止する



ため、次に掲げる項目について対策を講ずること。

#### 1 接続等

- (1) 開放的なネットワークとの接続は、必要最小限の機能、回線及びホスト等に限定すること。
- (2) 開放的なネットワークと接続するときは、当該開放的なネットワークからの保有する情報への不正アクセスを防止する機能を設け、すべての通信を制御すること。
- (3) (2)をファイアウォール等を利用して行う場合は、適切な条件設定を行うこと。
- (4) (2)をコンピュータ・システムを利用して行う場合は、セキュリティ・ホールに関する措置を講ずるなど当該システムのセキュリティを確保すること。
- (5) ネットワークの構成等に関する重要な情報は、真に必要な場合を除き公開しないこと。

#### 2 監視

回線の負荷状況等を監視する機能を設けること。

#### 3 切離し

異状が発見された場合等必要がある場合は、接続された開放的なネットワークを切り離すことができるようにすること。

### 第2章 攻撃等認知時における措置等

管理者は、犯罪発生時における警察との連携を確保し、危機に対して的確に対応するとともに、セキュリティを確保するため、次に掲げる項目について対策を講ずること。

#### 1 攻撃等認知時における措置

- (1) 攻撃等を認知したときは、関係機関等と協力して被害の状況を把握すること。
- (2) 関係機関等と協力して被害の拡大を防止するための措置を講ずること。
- (3) 攻撃の分析及び原因の究明を行い、関係機関等と協力して再発防止のための措置を講ずること。

#### 2 ユーザの限定

開放的なネットワークを介してアクセスできるユーザは、可能な限り限定すること。

#### 3 情報収集

- (1) 開放的なネットワークを介してなされる不正アクセス等に関する情報について平素から収集すること。
- (2) 収集した情報については、必要に応じユーザに提供すること。

#### 4 教育

情報システムの安全対策が適当でない場合は、他者のユーザIDを不正に利用したなりすまし等を助長することとなり、その結果、開放的なネットワークに接続される他の情報システム等に被害を与える危険性があることをユーザに十分認識させること。

## II コンピュータ・ウイルスに関し管理者及びユーザが講ずべき対策

### 1 新たに入手したプログラムを使用するときに講ずべき措置

送信元が不明のプログラムは、コンピュータ・ウイルスに感染しているおそれがあるため、使用しないこと。

### 2 システム使用中に講ずべき措置

開放的なネットワークを介して、電子メール（添付ファイルを含む。）の受信又はファイルのダウンロードを行ったときは、ワクチン・プログラムによるチェックを行うこと。転送するときは、事前にチェックを行うこと。

別表（第1編の3(3)関係）

他省により示された基準

「コンピュータウイルス対策基準」（平成7年7月7日付け通商産業省告示第429号）

「情報システム安全対策基準」（平成7年8月29日付け通商産業省告示第518号）

「コンピュータ不正アクセス対策基準」（平成8年8月8日付け通商産業省告示第362号）

「情報通信ネットワーク安全・信頼性基準」（昭和62年2月14日付け郵政省告示第73号）

[http://www.npa.go.jp/hightech/antai\\_sisin/kokuji.htm](http://www.npa.go.jp/hightech/antai_sisin/kokuji.htm)

#### 4. 不正アクセス禁止法関連

##### 不正アクセス行為の禁止等に関する法律

不正アクセス行為の禁止等に関する法律（平成11年法律第128号）

###### （目的）

第一条 この法律は、不正アクセス行為を禁止するとともに、これについての罰則及びその再発防止のための都道府県公安委員会による援助措置等を定めることにより、電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与することを目的とする。

###### （定義）

第二条 この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者をいう。

2 この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。

一 当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号

二 当該利用権者等の身体の一部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号

三 当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

3 この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次条第二項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

###### （不正アクセス行為の禁止）

第三条 何人も、不正アクセス行為をしてはならない。

2 前項に規定する不正アクセス行為とは、次の各号の一に該当する行為をいう。

一 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二 アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三 電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（不正アクセス行為を助長する行為の禁止）

第四条 何人も、アクセス制御機能に係る他人の識別符号を、その識別符号がどの特定電子計算機の特定利用に係るものであるかを明らかにして、又はこれを知っている者の求めに応じて、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。ただし、当該アクセス管理者がする場合又は当該アクセス管理者若しくは当該利用権者の承諾を得てする場合は、この限りでない。

（アクセス管理者による防御措置）

第五条 アクセス制御機能を特定電子計算機に付加したアクセス管理者は、当該アクセス制御機能に係る識別符号又はこれを当該アクセス制御機能により確認するために用いる符号の適正な管理に努めるとともに、常に当該アクセス制御機能の有効性を検証し、必要があると認めるときは速やかにその機能の高度化その他当該特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとする。

（都道府県公安委員会による援助等）

第六条 都道府県公安委員会（道警察本部の所在地を包括する方面（警察法（昭和二十九年法律第百六十二号）第五十一条第一項本文に規定する方面をいう。以下この項において同じ。）を除く方面にあっては、方面公安委員会。以下この条において同じ。）は、不正アクセス行為が行われたと認められる場合において、当該不正アクセス行為に係る特定電子計算機に係るアクセス管理者から、その再発を防止するため、当該不正アクセス行為が行われた際の当該特定電子計算機の作動状況及び管理状況その他の参考となるべき事項に関する書類その他の物件を添えて、援助を受けたい旨の申出があり、その申出を相当と認めるときは、当該アクセス管理者に対し、当該不正アクセス行為の手口又はこれが行われた原因に応じ当該特定電子計算機を不正アクセス行為から防御するため必要な応急の措置が的確に講じられるよう、必要な資料の提供、

助言、指導その他の援助を行うものとする。

2 都道府県公安委員会は、前項の規定による援助を行うため必要な事例分析（当該援助に係る不正アクセス行為の手口、それが行われた原因等に関する技術的な調査及び分析を行うことをいう。次項において同じ。）の実施の事務の全部又は一部を国家公安委員会規則で定める者に委託することができる。

3 前項の規定により都道府県公安委員会が委託した事例分析の実施の事務に従事した者は、その実施に関して知り得た秘密を漏らしてはならない。

4 前三項に定めるもののほか、第一項の規定による援助に関し必要な事項は、国家公安委員会規則で定める。

第七条 国家公安委員会、通商産業大臣及び郵政大臣は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に資するため、毎年少なくとも一回、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を公表するものとする。

2 前項に定めるもののほか、国は、アクセス制御機能を有する特定電子計算機の不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならない。

#### （罰則）

第八条 次の各号の一に該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。

- 一 第三条第一項の規定に違反した者
- 二 第六条第三項の規定に違反した者

第九条 第四条の規定に違反した者は、三十万円以下の罰金に処する。

#### 附 則

この法律は、公布の日から起算して六月を経過した日から施行する。ただし、第六条及び第八条第二号の規定は、公布の日から起算して一年を超えない範囲内において政令で定める日から施行する。

[http://www.npa.go.jp/hightech/fusei\\_ac1/houann.htm](http://www.npa.go.jp/hightech/fusei_ac1/houann.htm)

## 不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則

### 不正アクセス行為の再発を防止するための都道府県公安委員会による援助に関する規則

(平成11年国家公安委員会規則第12号)

#### (援助の申出)

第一条 不正アクセス行為の禁止等に関する法律(以下「法」という。)第六条第一項の申出(以下「申出」という。)は、別記様式の援助申出書を、当該申出に係る不正アクセス行為に係る特定電子計算機(次項において「当該特定電子計算機」という。)の設置の場所を管轄する都道府県公安委員会(道警察本部の所在地を包括する方面を除く方面にあっては、方面公安委員会。以下「公安委員会」という。)に提出してしなければならない。

2 公安委員会は、申出に添えられた書類その他の物件に次に掲げる事項に関する書類その他の物件で公安委員会が援助を行うため必要なものが含まれていないと認めるときは、その提出を求めることができる。

一 当該特定電子計算機に係るシステムの構成(当該システムを構成する当該特定電子計算機その他の特定電子計算機の機種、名称、機能及び識別情報(特定電子計算機相互間において電気通信を行う際に特定電子計算機を識別するために用いられる番号、記号その他の符号をいう。)、当該システムに用いられるプログラムの名称及び機能並びに他の特定電子計算機に係るシステムとの接続箇所及び接続方法を含む。)

二 当該特定電子計算機の特定利用の内容

三 当該特定電子計算機の特定利用を制限していたアクセス制御機能その他の機能の概要

四 前号のアクセス制御機能に係る識別符号を当該アクセス制御機能により確認するために用いる符号の内容及び管理状況

五 当該特定電子計算機に係るシステムを構成する当該特定電子計算機その他の特定電子計算機に入力された識別符号その他の情報又は指令に関する記録(当該情報又は指令が入力された日時、結果その他の入力履歴に関する記録を含む。)であって、当該申出に係る不正アクセス行為に関係があると認められるもの

六 当該申出に係る不正アクセス行為の再発を防止するために講じた措置その他の当該特定電子計算機に係るシステムに対して講じた措置

七 前各号に掲げるもののほか、当該申出に係る不正アクセス行為が行われた際の当該特定電子計算機の作動状況及び管理状況その他の参考となるべき事項であって、事例分析(法第六条第二項に規定する事例分析をいう。以下同じ。)の実施のために必要なもの

#### (公安委員会による援助措置)

第二条 公安委員会は、申出を受けた場合において、当該申出を相当と認めるときは、当該申出の内容に応じて、次に掲げる援助措置を採るものとする。

一 事例分析の結果に関する資料を提供すること。

二 当該申出をしたアクセス管理者が講ずることが適当であると認められる措置に関し必要な資料の提

供、助言又は指導を行うこと。

三 不正アクセス行為からの防御に資する事業を行うことを目的とする民間の団体その他の組織を教示すること。

四 不正アクセス行為から防御するための措置に関する事項を記載し、又は記録している書類、媒体その他の資料を教示すること。

五 その他不正アクセス行為からの防御に資すると認められる事項を教示すること。

(事例分析の実施の事務の委託)

第三条 法第六条第二項の国家公安委員会規則で定める者は、事例分析の実施に関する事務を適正かつ確実に行うことができる技術的能力を有し、かつ、十分な社会的信用を有すると公安委員会が認める者とする。

附 則

この規則は、法附則ただし書に規定する規定の施行の日（平成十二年七月一日）から施行する。

別記様式（第1条関係）

その1		受理年月日		受理番号	
<p><b>援 助 申 出 書</b></p> <p>不正アクセス行為の禁止等に関する法律第6条第1項の規定による援助を受けたいので、次のとおり申し出ます。</p> <p style="text-align: right;">年 月 日</p> <p>公安委員会 殿</p> <p style="text-align: center;">申出人の氏名又は名称及び住所</p> <p style="text-align: center;">?</p>					
申 出 人	(ふりがな)				
	氏名又は名称				
	住 所				
	(ふりがな)				
	法人にあっては、 その代表者の氏名				
申出に関する連絡先					
不正アクセス 行為に係る特 定電子計算機	設置場所				
	用 途				
不正アクセス行為 を認知した日時					
不正アクセス行為 が行われた日時					



<p>不正アクセス行為が 行われたと認める理由</p>	
---------------------------------	--

その2

申出書に添えて提出する資料

- 1 不正アクセス行為に係る特定電子計算機に係るシステムの構成に関する資料  
(資料名)
  
- 2 1の特定電子計算機の特定利用に関する資料  
(資料名)
  
- 3 2の特定利用を制限していたアクセス制御機能その他の機能の概要に関する資料  
(資料名)
  
- 4 3のアクセス制御機能に係る識別符号をそのアクセス制御機能により確認するために用いる符号の内容及び管理状況に関する資料  
(資料名)
  
- 5 1のシステムを構成する特定電子計算機に入力された識別符号その他の情報又は指令、それらの入力の日時、結果その他の入力履歴に関する資料  
(資料名)
  
- 6 不正アクセス行為の再発を防止するために講じた措置その他の1のシステムに対して講じた措置に関する資料  
(資料名)
  
- 7 不正アクセス行為が行われた際の特定電子計算機の作動状況及び管理状況その他の参考となるべき事項に関するその他の資料  
(資料名)

#### 記載要領

- 1 印欄には、記載しないこと。
- 2 申出人は、氏名の記載と押印に代えて、署名することができる。
- 3 該当する に? 印を付けるとともに、資料の名称を記載すること。
- 4 不正アクセス行為に係る特定電子計算機に係るシステムの構成には、システムを構成する特定電子計算機の機種、名称、機能及び識別情報、OS その他のプログラムの名称及び機能並びに他のシステムとの接続箇所及び接続方法を含む。
- 5 所定の欄に記載し得ないときは、別紙に記載の上、これを添付すること。

備考 用紙の大きさは、日本工業規格 A 4 とすること。

[http://www.npa.go.jp/hightech/fusei\\_ac3/enjyo\\_kitei.htm](http://www.npa.go.jp/hightech/fusei_ac3/enjyo_kitei.htm)

(補遺)

## 1. G 8 関連

### 国際組織犯罪対策に関する勧告(改訂版)(抜粋)

#### 国際組織犯罪対策に関する勧告(改訂版)

(仮訳)

Part : 国境を越えた犯罪

Section D : ハイテク・コンピューター関連犯罪

コンピューター及びコンピューターネットワークは、ますます、テロ行為その他の犯罪的攻撃の対象になってきているとともに、テロリスト及びその他の犯罪者が破壊的活動の計画及び実行のための通信媒体となってきた。多くのコンピューターネットワークが国境を越えることから、すべての国が十分な実体法及び手続法を有し、コンピューター及びコンピューターネットワークを利用して行われるテロ行為その他の犯罪活動を適切に防止し処罰するための捜査活動において協力することが肝要である。

1. 各国は、現代技術の乱用が刑事処罰に値する場合には的確に犯罪化し、その乱用に関する裁判権、法執行体制、捜査、訓練、犯罪防止、国際協力に関する問題に効果的に対処できるよう国内法を見直すべきである。
2. 各国は、上記見直しを行うに当たり、欧州評議会サイバー犯罪条約(2001年)、各種国際機関の作業及びG 8の作業、特に下記のを考慮に入れ、それらを指針とすべきである。
  - ・ ハイテク及びコンピューター関連犯罪に関する原則及び行動計画(1997年)
  - ・ 蔵置されたコンピューター・データに対する国境を越えるアクセスに関する原則(1999年)
  - ・ ネット上の犯人の追跡性に関する勧告(2002年)
  - ・ 公共の安全の保護に不可欠なデータの利用可能性に関する原則(2002年)
  - ・ 「データ保全のための法的枠組みにおいて考慮すべき事項」及び「法執行記録保全」という説明的前文から成るデータ保全パッケージ(2002年)
  - ・ データ保護体制に関する声明(2002年)各国は、ハイテク犯罪に対処するため、国際協定を含む国際的な解決策を目指して努力を継続することが奨励される。
3. 欧州評議会サイバー犯罪条約(2001年)がコンピューターシステムへの攻撃と闘うための重要な措置及びテロその他の犯罪の電子的証拠の収集を規定する措置を提供していることから、我々は、同条約に加盟する意向であり、また、他の国々に対しても、その資格があるなら同条約に加盟しその条項

のできる限り速やかな完全履行を確保することを求める。他の国々は、同条約への加入に努めるか、又は、少なくとも、同条約において求められている措置に近似した法的枠組みの有用性を確保すべきである。

4. 各国は、下記を含むハイテク犯罪防止及び抑止措置を講じるべきである。
  - ・ コンピューターネットワーク及び通信システムが安全であること並びにこれらのシステムが攻撃されたときに適切な対応体制が存在することの確保に努めるために、民間産業と協力すること。
  - ・ 知的所有権が偽造及び不正コピーから適切に保護されることを確保するための法律その他の措置を規定し履行すること。
  - ・ 将来の技術発展が提起する可能性のある問題を特定し及び最小化すること。
  - ・ ハイテク犯罪問題について一般の意識を高めること。
5. 各国は、犯罪の敢行にコンピューター技術を用いる犯罪者を追跡するために、適切な技術の取得並びに自国の捜査上及び訴追上の専門知識及び能力の継続的開発を支援すべきである。各国は、効果的な法執行技術の調査、さらには検証を促進すべきである。
6. 異なった国の間における法執行機関及び訴追機関間の連携が、ハイテク・コンピューター関連犯罪の問題に対処した際の経験の共有を含めて促進されるべきである。我々は、国際ハイテク犯罪24時間コンタクト制度の有効性の向上、及び他の国々のこの制度への参加奨励を確約する。
7. 各国は、自国において、また、国際協力の提供において、特に新技術の脅威を考慮したプライバシー権の保護と公共の安全及び他の社会的価値を保護する法執行能力の維持との間の適切な均衡を維持すべきである。各国は、この均衡を図る際には、民間部門の利害も考慮すべきである。

<http://www.g8j-i.ca/english/doc1.html> (英文)

## テロ・犯罪捜査における国境を越えたネットワーク通信追跡のための勧告

### テロ・犯罪捜査における 国境を越えたネットワーク通信追跡のための勧告

[ 仮訳 ]

1999年10月、G8各国の司法・内務閣僚がモスクワで会合を開き、犯罪の捜査において、国境を越えてネットワーク通信を追跡するための具体的なオプションを策定するよう、各代表者に指示した。閣僚のコミュニケには、以下のように示されている（抜粋）:

ネットワーク通信を違法な目的で使用する犯罪者の場所を確認して特定するために、各国は通信がなされている間及びその後、当該通信が複数国を通過する場合であっても、追跡を行う能力を高める必要がある。既存の手続きは、しばしば遅すぎるものであり、多くの国の迅速な援助を必要とする犯罪ではなく、二国間協力を指向する方向で作られている。より速く、斬新な解決策が見い出される必要がある。

2000年5月、専門家によりオプションの案が策定された。2000年7月、G8各国首脳は、日本の沖縄サミットにおいて、この作業を実施することを支持した。2001年2月、G8司法・内務閣僚はミラノで会合を開き、専門家に対して、特にプライバシーと個人の自由の保護等の関連する要素を考慮に入れた追跡性の勧告を策定するよう指示した。

閣僚はまた、モスクワにおいて、追跡性及び他のハイテク犯罪問題に関係した入力を探求するために、産業界の代表者と協議するよう指示している。それと同時に、会議やワークショップがパリ、ベルリン及び東京で開催され、世界中のハイテク関連企業から100名を超える代表者が出席した。

2001年9月11日の痛ましい出来事により、この作業の緊急性が増大した。テロリストは、電子メール、WWW上のサイト、携帯電話、その他の高度な通信手段を用いて、複数の大陸を跨った計画立案及び情報伝達を、追跡されるのを困難又は不可能にする方法で実施することができる。通信の近代化及び広域化によって、テロリストが利益を得るようなことがあってはならない。従って、我々はこの挑戦に対抗して、全政府のテロ及び他の犯罪行為に対処する能力を向上させるために、共同作業を行わなければならない。

同様の挑戦は、遠距離間で行われ得る国際ハイテク犯罪事案においても存在している。捜査官は成功するために、通信連鎖の中間に位置する他国のサービス・プロバイダと作業しながら、通信元のコンピュータから目的のコンピュータまでの通信の痕跡を追跡しなければならない。犯罪の発信源を特定するために、法執行機関はしばしば、幾つかの通信接続がいつ、誰によって行われたかを示す過去の記録に依存しな

ればならない。その他の場合には、法執行機関は通信接続が行われている最中に追跡を行う必要があるかもしれない。よくあるケースで、プロバイダが捜査官の管轄区域外に位置する場合には、その法執行機関は、他の管轄区域を担当するカウンターパートの支援を必要とするのが通例である。従来の捜査共助及び迅速化された捜査共助は一般的に、二国のみ（例、被害者所在国及び犯罪者所在国）を含んだ事案の過去データ及びリアルタイムデータを取得するよう設計されている。犯罪者が、通信を3乃至5カ国経由させた場合に、捜査共助のプロセスでは、法執行機関が通信連鎖上の各サービス・プロバイダからデータを収集できるまでには相当の期間を要し、その結果、データが使用できない、又は紛失される可能性を高め、犯罪者は特定されず、再度犯罪行為を犯す自由な身となる。

これらの勧告は、国際的なテロリスト及び犯罪通信をより効果的に追跡できるようにするために政府が迎えるステップを提案するものである。これらの勧告は、特定の捜査に関するデータの保全、迅速な捜査共助、複数のプロバイダを通じたリアルタイム追跡及びユーザレベル認証など、広範囲の問題を扱っている。これらの勧告は、既存の技術的能力の向上をプロバイダに要求することを意図しているものではない。最後に、これらの勧告の実施は、適切な人権の保護に関して、各国の国内法及び国際規約に従うものである。可能な範囲内において、これらレコメンデーションは、国内法における矛盾を防止又は最小限に留める形で実施されるべきであり、それは、国際的な法執行協力及び政府と産業界の協力の両方にとって、障害となり得る。

政府は、法執行機関がテロや他の犯罪活動を防止及び捜査する能力を向上させる以下の手法を考慮するものとする：

- 1 サービス・プロバイダ及びサービス・プロバイダ協会団体による行動規範の採用を支援することなどにより、サービス・プロバイダに対し、通信記録及び加入者記録の特定部分の保存を、合法的なビジネス及び公共の安全目的で許容する。<sup>1</sup>
- 2 ネットワークセキュリティ要求又は法執行捜査及び訴追において重要なインターネット及び他の技術に関係するデータの保存及び保全を許容するよう施行されたデータ保護法制が、公共の安全及び他の社会的価値を考慮することを保証する。
- 3 国内の法執行機関が、国内サービス・プロバイダに対して、国内の司法又は同類の命令の発付を迅速に得た後、国内法で要求されている場合には実質的なレビューを行ってから、外国からの（データ）保全指示を執行することを許容する。
- 4 国内法で許容されている場合に、一つの国内的な司法又は同類の命令を執行することを通じて、複数のサービス・プロバイダがその送受信に関与している特定の通信に関係した既存の通信記録の迅速な保

---

<sup>1</sup> データの種類については、各国で決定するものとする。

全、並びに、当該通信が伝達された経路及びサービス・プロバイダの特定を可能にするに十分な量の通信記録の迅速な開示を保証する。

- 5 国内の法執行機関に対して、被要請国における国内法の違反が存在しない場合であっても、前パラグラフに説明されたメカニズムを利用して、迅速化された共助を通じて外国からの要請に対応することを許容する。<sup>2</sup>
- 6 特定の通信の追跡要請を他国から受けた際に、国内法に対する違反が存在しない場合であっても、権限ある当局が、当該通信を追跡するために必要な全ての既存の国内データを保全するために、国内法で利用可能なメカニズムを用い、当該通信が第三国から来ていると認められる場合には、その旨要請国に告げ、要請国において当該第三国に援助を要請できるよう、十分なデータを要請国に提供できることを許容する。
- 7 国内の法執行機関に対して、各国の複数のプロバイダを通じて、通信経路、発信源又は宛先を特定するために、国内法で許容される場合には一つの国内的な司法又は同類の命令を用いて、特定された通信をリアルタイムで追跡することを許容する。
- 8 国内の法執行機関に対して、被要請国における国内法の違反が存在しない場合であっても、前パラグラフに説明されたメカニズムを利用して、迅速化された共助を通じて外国からの要請に対応することを許容する。
- 9 セキュリティを改善し、ネットワーク利用者のプライバシーを念頭に置きながら、適切な場合において、ネットワークの悪用を追跡できるネットワーク構成を奨励する。
- 10 技術的な中立性及びユーザーの選択の自由を尊重しながら、適切なアプリケーションにおける強力なユーザーレベル認証を奨励する。

<http://www.g8j-i.ca/english/doc2.html> (英文)

---

<sup>2</sup> “被要請国における国内法の違反が存在しない場合であっても”という文言は、その国において、問題となる犯行が犯罪となる要件を満たしていない、又は、犯罪として起訴できない場合であっても、被要請国は支援を提供しなければならないことを強調することを意図している。この文言及び一般的に勧告は、双罰性要件や被要請国の潜在的利益の例外等を含む、被要請国によって実施されるかもしれない支援を提供するための他の要件の実施可能性を制限することを意図するものではない。



## 公共の安全を保護するために不可欠なデータの利用可能性に関する原則

### 公共の安全を保護するために不可欠なデータの利用可能性に関する原則

(仮訳)

犯罪やテロリストの活動の捜査、防止、訴追のためには、法執行機関は、通信サービス提供者が保有する通信記録や加入者情報への適法なアクセスを必要とする。しかし、犯罪者やテロリストの捜査は、利用可能なデータや情報の欠如によって、ますます妨げられている。

このような理由により、プライバシー保護、産業界の考慮事項及び法執行機関による公共の安全に関する任務の遂行の間のバランスが保たれるよう、各国は通信記録や加入者情報の利用可能性に関する政策を考察すべきである。特に、バランスのとれた取り組みを作り上げるに当たっては、各国は、個人情報保護を含んだ人権を擁護すべきである。データ保護政策は、個人情報の保護、ネットワークの安全や詐欺の防止といった産業界の考慮事項及び犯罪やテロリストの活動と闘うための捜査を行う法執行機関の必要性との間のバランスを調整すべきである。

政府及び産業界は、技術や電子商取引の進歩はそれらの利用における公共の安全も含むものであることを認識すべきである。公衆とビジネスが安全で信頼できるものであることを確保することは、国家経済が継続して安定していることやインターネット上で事業を行うことに関する消費者の信頼の伸長にとって、不可欠である。

通信記録と加入者情報の利用可能性に関する政策を作成する際にバランスのとれた取り組みを促進するためには、データ保護やプライバシーに関する当局、産業界、法執行機関、ユーザーを含む全ての利害関係者との協議がなされるべきである。

政府及び産業界は、データの収集及び保存については、経済上の関連性があることを認識すべきである。これは、利用可能なデータの総量（すなわち、いかなる種類のいかなる記録か）、蔵置の期間、異なるビジネスモデルといった多数の要素に左右される。従って、政府は、公共の安全目的にとって有用であるかもしれないデータの類型を特定すべきである。ある記録、例えばネットワーク接続ログは、適法な捜査にとって、特に有用である。付録Aは、利用可能となり得る記録の一覧である。

通信記録や加入者情報の利用可能性の確保に関し、政府は、異なるISP（注：インターネット・サービス提供者）のビジネスモデルに対し不合理な運用上、財政上の負担を回避するよう努めるべきである。

各国は、国境を越えてサービスを提供するサービス提供者に対する過度の負担を避けるため、適用可能性

のある国際通商義務を考慮に入れつつ、データの利用可能性に関する協動的取り組みを発展させるべきである。

通信記録や加入者情報の利用可能性に関して国内レベルで形成される政策は、犯罪者やテロリストによる国境を越えたネットワーク上の通信の迅速な追跡を可能とするため、国際的協力の必要性を考慮に入れるべきである。

## 付録A

以下は、典型的なインターネット・サービスにおいて利用可能な幾つかのサービスに関連したログの詳細の一覧である。これらのログのコンテンツについては、関係するビジネス的、技術的及び法的条件に従うものであり、全てのログにおいて以下のデータ要素が利用可能であるとは限らないことを特記する必要がある。

### (1) ネットワーク接続システム (NAS)

- ・ TACACS+ や RADIUS (ユーザー・サービスにおけるリモート認証ダイヤル) 等の認証及び認証サーバーに特化したアクセスログであり、IP ルータやネットワーク接続サーバーへのアクセスを制御するために使用される。
- ・ クライアントがサーバーに接続した日付及び時刻<sup>1</sup>
- ・ ユーザーID
- ・ 割り当てられたIPアドレス
- ・ NASのIPアドレス
- ・ 送信及び受信されたバイト数
- ・ 着信回線特定 (CLI)<sup>2</sup>

### (2) 電子メール・サーバー

- ・ SMTP (単一メール転送プロトコル) ログ
  - ・ クライアントがサーバーに接続した日付及び時刻
  - ・ 送信したコンピュータのIPアドレス
  - ・ メッセージID (msgid)
  - ・ 送信者 (login@domain)
  - ・ 受信者 (login@domain)
    - ・ POP (ポスト・オフィス・プロトコル) ログ又はIMAP (インターネット・メッセージ接続プロトコル) ログ
  - ・ クライアントがサーバーに接続した日付及び時刻
  - ・ サーバーに接続されたクライアントのIPアドレス
  - ・ ユーザーID

---

<sup>1</sup> 捜査及び訴追のためには、異なるコンピュータシステムやネットワークにおける、信頼できる時刻記録が重要である。同期をとるためのネットワーク時間プロトコル (NTP) の利用は、ISPの行動規範とするべきである。

<sup>2</sup> CLIは、通話が発信された電話番号を提供するものであるが、ISPで得られるかどうかはわからない。CLIの回収は、与えられたソフトウェアとハードウェアの組み合わせに依存している。

“LINXの行動規範 - 追跡性” セクション10.2 参照

- ・ 特定の場合においては、回復された電子メールの特定情報

(3) アップロード及びダウンロード・サーバー

- ・ F T P (ファイル転送プロトコル) ログ
  - ・ クライアントがサーバーに接続した日付及び時刻
  - ・ I Pソースアドレス
  - ・ ユーザー I D
  - ・ アップロード又はダウンロードされたデータのパス名及びファイル名

(4) ウェブ・サーバー

- ・ H T T P (ハイパーテキスト転送プロトコル) ログ
  - ・ クライアントがサーバーに接続した日付及び時刻
  - ・ I Pソースアドレス
  - ・ オペレーション (即ち G E T コマンド)
  - ・ オペレーションのパス名 (html ページ又はイメージファイルの回復)
  - ・ “最後に訪問されたページ”

(5) ユーズネット (U s e n e t )

- ・ N N T P (ネットワークニュース転送プロトコル) ログ
  - ・ クライアントがサーバーに接続した日付及び時刻
  - ・ プロトコル処理 I D (nnrpd[nnn...n])
  - ・ ホスト名 (割り当てられた動的 I P アドレスの D N S 名)
  - ・ 基本的なクライアントの活動 (コンテンツではない)
  - ・ ポストされたメッセージの I D

(6) インターネット・リレー・チャット

- ・ I R C ログ
  - ・ クライアントがサーバーに接続した日付及び時刻
  - ・ セッションの継続時間
  - ・ I R C 接続中に使用されたニックネーム
  - ・ ホスト名及び I P アドレス

<http://www.g8j-i.ca/english/doc3.html> (英文)

## データ保全に関するチェックリスト

### データ保全に関するチェックリスト

(仮訳)

1999年10月にモスクワで開催されたG8司法内務閣僚会合において、閣僚は、犯罪捜査を行う法執行機関は、一定の状況において、地理的境界を越えて捜査を行う能力を有すべきであることを認識した。第一歩として、モスクワコミュニケには「蔵置されたコンピュータデータに対する国境を越えるアクセスに関する原則」が含まれている。本原則は、公にアクセス可能なデータや同意に基いて取得できるデータに関し、法執行機関が外国に蔵置されたデータに緊急にアクセスすることを可能とするための実用的な手段が詳述された。

さらに、コミュニケは、G8の専門家に対し、「産業界との協議の上で、犯罪捜査において国境を越えたネットワーク上の通信の追跡のための具体的な選択肢を策定する」こと及び「インターネット犯罪について、殊にインターネット犯罪者の探知及び特定の問題につき重点的に、G8と産業界がアイデアを共有することができるような会議を開催する」ことを指示した。現在までに、G8は3つの「サイバー空間における安全と信頼性に関する政府・産業界の対話」を開催してきた：パリ(2000年5月15~17日)、ベルリン(2000年10月23~25日)及び東京(2001年5月22日~24日)。これらの対話は、ハイテク犯罪や犯罪目的でのインターネットの悪用に関連する共通の問題について議論が行われ、解決策を検討する機会を提供した。これらの対話の中で扱われた主な問題は、データ保存、データ保全、リアルタイム・トレーシング、脅威評価と防止、トレーニングである。

一連の協議の中で、ハイテク犯罪サブグループは、「テロ・犯罪捜査における国境を越えたネットワーク通信追跡のための勧告」を作成した。本勧告は、複数の管轄が関係する場合のデータ保全に関する部分を含んでいる。

データ保全は、データの収集や保存を強制するものではない；すなわち、データ保全は、本質的には、存在するデータに関する「削除するな」という命令である。データ保全制度は、法的に正当性のある要求により、特定の事件における事実に基き、すでに収集された特定のデータが削除されることの防止を提供するものである。後の時点で、権限ある機関による法的な要求によってデータの開示を強制することができる。

33カ国が欧州評議会サイバー犯罪に関する条約に署名をした。本条約は、データ保全に関する条文を含んでおり、多くの国が現在新しい立法の必要性について検討を行い、あるいは、データ保全に関する国内制度を実施するための法的方策を模索している。

このような作業を行っている国を支援するため、ハイテクサブグループは、以下のような実務的な道具を作成してきた：データ保全のための現在又は将来的な法的枠組みにおいて考慮されるべき事項のリスト及び法執行機関によるデータ保全要請のための行為規範のチェックリスト。これらのツールは、東京におけるG8官民対話の成果物である。G8ハイテク犯罪サブグループは、これらの文書が各国に対して拘束力を有するものとなることは意図していないが、データ保全法制を検討している国やデータ保全要請を実施する法執行機関に対して指針や援助を提供するものである。

## データ保全のための法的枠組みにおいて考慮されるべき事項

目的： この文書の目的は、現在又は将来的なデータ保全のための法的枠組みにおいて考慮され得る一連の質問を明らかにするためのものである。

注意： この文書において、「保全」とは、(a)権限ある機関による法的な要請により、(b)特定の事件における事実に基き、(c)特定の過去のデータが、その削除を防止するために、保全され得るものであり、(d)権限ある機関からのデータ開示のための法的要求の発出に係らしめられているものをいう。「保全」は、将来のデータ収集を含むものではなく、また、サービスプロバイダに対し現存しないデータの作成を義務付けるものではない。

### 1 法律の根拠

- 1.1 保全命令のための手続き法上の根拠は何か。
- 1.2 保全命令の発出のための実体法上の記述はあるか。
- 1.3 特定の種類のデータに関する保全命令のための実体法上の記述はあるか（例：トラフィックデータ対コンテンツ）。

### 2 対象

どのような記録が保全命令の対象とされるべきか。

### 3 保全命令の期間

どのくらいの期間記録が保全されるべきか。

### 4 保全命令の形式

- 4.1 保全命令のための標準化された形式があるべきか。
- 4.2 保全命令の送達はいずれによるべきか。
  - ・ 書面のみによる
  - ・ 口頭による
  - ・ 口頭及び後の書面による確認
  - ・ 電子メール

### 5 権限のある発行者

- 5.1 いかなる権限のある機関（「発行者」）が保全命令を発出できるか
- 5.2 発行者によって開始された伝達を特定するための証明手段が存在すべきか。

### 6 地理的範囲

保全命令は次のものに適用され得るか。

- ・ 発行者の管轄外に位置する記録
- ・ 発行者の管轄外に位置する受領者

### 7 秘密性

- 7.1 発行者は受領者に対して、(a)保全命令の秘密性を保つこと、かつ/又は、(b)捜査の対象に

- 対して保全命令を秘密にしておくことを要求できるか。
- 7.2 違法な開示に対する制裁は何か。
- 7.3 秘密性の要求について期限や失効時点を設けるべきか。
- 8 受領者への償還  
受領者への償還は可能か。受領者はいかなる費用を回復できるか。
- 9 受領者の種類
- 9.1 いかなる者（「受領者」）が保全命令の発出の対象となり得るか。
- 9.2 受領者においていかなる個人や部署が保全命令を受領すべきか。
- 9.3 一つの保全命令は一つの管轄内の複数の受領者に適用可能か。同じ国の中で複数の管轄にある受領者に適用可能か。
- 10 受領者の免責  
適法な保全命令に従ったことに関し、受領者は法的措置について免責を受けることができるか。特に、それらの免責は次のものか。
- 10.1 刑事免責
- 10.2 民事免責
- 10.3 海外に関する免責
- 11 不遵守に対する制裁  
権限に基づく保全命令に従わなかった受領者にはいかなる制裁が（もし存在すれば。）科されるのか。
- 12 受領者の拒否権  
いかなる状況下で、受領者は、保全命令に関して説明や変更を求め、その他遵守しないことが正当化されるのか。
- 13 取消義務  
関連する開示命令が後に発出されることを発行者が信じることができなくなった場合、発行者は開示命令を取り消す義務を負うか。
- 14 使用範囲  
保全されたデータは他の法的手続（例えば民事召喚令状）に従って開示されかつ用いられることができるのか、又は、開示及び使用は保全命令の起訴となった特定の犯罪捜査に限定されるのか。
- 15 捜査共助義務との相互作用
- 15.1 保全命令の手続きは捜査共助の手続きと整合しているか。
- 15.2 海外の権限ある機関からの要求により保全命令を発出するかを決定する際に考慮すべき基準は、もしあるとすれば、どのようなものか。
- 15.3 保全が海外の権限ある機関からなされ、受領した権限ある機関が捜査の対象となっている事件について明確な双罰性が存在しないかもしれないと考えた場合、保全命令は適切又は可能なものであるか。
- 16 部分開示



当該捜査に関するデータを保有している可能性のある他の潜在的な保全命令の受領者を特定するため、一定の形式の部分開示は認められ、又は、要求されるべきか。

17 潜在的濫用

いかなる行為や結果が保全手続きの濫用と考えられるのか。

18 潜在的な法律の抵触

いかなる法律が保全命令の要件と抵触する可能性があるか。

19 開示基準

適法は保全命令に従って保全されたデータの開示を律する基準は何か。

20 紛争解決

いかなる当局（裁判所、委員会等）が保全命令の有効性や適用範囲に関する紛争を解決できるか。

法執行の記録  
保全チェックリスト

目的：このチェックリストは、特定の犯罪捜査において、保全命令の発出が可能である場合に、権限ある機関に勤務する個人によって使用されることを想定している。

注意：この文書において、「保全」とは、(a)権限ある機関による法的な要請により、(b)特定の事件における事実に基き、(c)特定の過去のデータが、その削除を防止するために、保全され得るものであり、(d)権限ある機関からのデータ開示のための法的要求の発出に係らしめられているものをいう。「保全」は、将来のデータ収集を含むものではなく、また、サービスプロバイダに対し現存しないデータの作成を義務付けるものではない。

- 1 保全要求の出所の確認
  - 1.1 国内
  - 1.2 海外
- 2 保全命令の根拠の特定
  - 2.1 保全命令の発出権限を与えている法
  - 2.2 保全命令の根拠を形成する刑事犯罪
- 3 保全命令の適切及び範囲の特定
  - 3.1 保全命令の発出及び命令の範囲は適切か。例えば、発出命令と保全が求められている記録とは(a)比例しているか、(b)捜査に関連しているか、(c)受領者にとって不合理に負担となっていないか。
  - 3.2 記録は一般に入手可能か。
- 4 法執行機関がすでにいかなる情報を保有しているかの特定
  - 4.1 個人の特定（例：氏名）
  - 4.2 アカウント名（例：joe@internetmail.com）
  - 4.3 通信（例：AからBへの電子メール）
  - 4.4 ファイル（例：画像、文書等）
- 5 保全命令の受領者の特定
  - 5.1 いかなる者（「受領者」）が保全命令を受領すべきか。
  - 5.2 受領者におけるいかなる部門の者が保全命令の写しを受領すべきか。
- 6 保全されるべき記録の特定

以下の種類の記録は典型的なインターネットサービスにおいて入手可能である可能性がある。全ての受領者からこれら全ての記録が入手できるわけではないこと、実際に入手可能な記録は受領者のビジネスモデル及び記録保存の形態に依存することが留意されなければならない。

  - 6.1 契約者の記録（例：契約者の氏名、現住所）

- 6.2 通信記録（例：ユーザーID、割り当てられたIPアドレス）
- 注：欧州評議会サイバー犯罪条約に関する条約には通信記録の定義が規定されている。
- 6.3 蔵置されている通信内容（例：蔵置されている電子メール、蔵置されているFTPファイル）
- 6.4 その他の関連情報
- 7 保全命令の適用範囲の決定
  - 7.1 受領者による保全の期間
  - 7.2 関連記録の期間
- 8 受領者の費用償還
  - 費用償還の法、政策、取り決めはあるか。
- 9 保全命令の受領者への適切な送達手段の特定
  - 9.1 書面
  - 9.2 口頭
  - 9.3 口頭及び書面による確認
  - 9.4 電子メール
- 10 開示するための事後計画の準備

<http://www.g8j-i.ca/english/doc4.html>（英文）

## G 8 データ保護制度に関する声明

### G 8 データ保護制度に関する声明

( 仮訳 )

テロリストやその他の犯罪者によるコンピュータネットワーク利用の増加を考えると、テロリストによる攻撃や他の犯罪活動を防止し、これらが発生した際に捜査を行うためには、過去の通信記録が重要である。特に、通信記録の解析は、テロリストとその共犯を結びつける唯一の方法である可能性がある。一つの国で活動するテロリストや他の犯罪者が他国にいる者と連絡を取ったり、援助を受けたりすることはよくあることなので、上記のことは国際的な影響を有する。

いかなるデータ保護制度も、個人情報の保護と刑事捜査やテロ捜査における法執行機関にとっての通信記録の必要性とのバランスをとったものでなければならない。G 8 は、データ保護制度は異なった社会的利益の間のバランスを反映したものでなければならないと信じる。例えば、ネットワークの安全確保や詐欺の防止は、公共の安全や電気通信システム内の個人情報の秘密性と完全性を向上させるものであることから、データを保存するための正当な理由である。ここにおいて、法執行機関とプロバイダーは共通の利益 - - 正規の顧客のためにインターネットを安全なものにすること を有している。データ保護法制が課金目的のみのためのデータ保存しか認めていかない限り、このような立場は、重要かつ正当な社会的利益 特に定額料金サービスや無料インターネット、無料電子メールサービスによって課金目的でのデータ保存が不要とされているインターネットサービスプロバイダーに適用された場合 - - を見過ごし、その結果公共の安全を著しく損なうことになる。G 8 はまた、データ保護法制が特定の根拠に基づいて一般的な制度に対する特例を認める場合、当初の規則が破棄を要求するものであることもあるので、その特例がこれら他の利益を認識する唯一の手段になってはならないと信じる。

<http://www.g8j-i.ca/english/doc5.html> ( 英文 )

## 2. 政府IT政策関連

### e-Japan 重点計画-2002 (抜粋)

e-Japan 重点計画-2002

平成14年6月18日

IT戦略本部

#### 重点政策5分野

#### 5. 高度情報通信ネットワークの安全性及び信頼性の確保

##### <目標>

我が国の高度情報通信ネットワークの安全性及び信頼性を世界最先端のIT国家にふさわしいものにするため、特に電子政府、電子商取引、重要インフラについては、情報セキュリティの不備による不正アクセス、コンピュータ・ウイルス、DoS攻撃<sup>1</sup>等がなされた場合に、国民生活や社会経済活動に大きな影響を及ぼすものであることから、そうした脅威に起因するサービス提供機能の停止をゼロとすることを目標とする。

##### (1) 現状と課題

情報通信ネットワークにおいては、常に不正アクセス、コンピュータ・ウイルス、DoS攻撃などの脅威にさらされており、超高速インターネット網の整備やインターネット常時接続の実現、電子商取引の発展や電子政府の実現等によって、これらの脅威は、政府機関や企業などに限らず、すべての国民にとっても詐欺等の犯罪行為等のかたちで、一層重大な脅威として現れてくることが懸念される。同時に、情報通信技術を活用した個人情報の流通・利用が拡大する中、その不適正な取扱いによって、プライバシーを始めとする個人の権利利益が侵害されるおそれも高まっている。

また、エネルギー供給、交通、政府・行政サービス等の国民生活や経済・社会活動に大きな影響を与え、これらの脅威は、政府機関や企業などに限らず、すべての国民にとっても詐欺等の犯罪行為等のかたちで、一層重大な脅威として現れてくることが懸念される。同時に、情報通信技術を活用した個人情報の流通・利用が拡大する中、その不適正な取扱いによって、プライバシーを始めとする個人の権利利益が侵害されるおそれも高まっている。

このような脅威は、今後、更に情報化・ネットワーク化の進展が見込まれるなかで、一層深刻なものになっていくことが見込まれる。こうした状況は、自然災害等の緊急事態発生時の危機管理や国家安全保障に関わる事案についても同様であり、安全で信頼できる情報通信ネットワークの構築は国家・社会全体の

<sup>1</sup> DoS攻撃：Denial of Service 攻撃（サービス不能攻撃）の略称。コンピュータやネットワークに不正に負荷をかけたり、セキュリティホールを突くなどして業務を妨害する攻撃。

安全を確保する上で必須の課題である。

さらに、最近のネットワークを取り巻く内外の情勢の変化、例えば、昨年9月の米国同時多発テロに見られるような国外からの脅威の増大や、サイバー犯罪に関する条約<sup>2</sup>の署名などの国際的な取組の進展等の状況の変化も踏まえれば、従来以上に国際調和のとれた情報セキュリティ対策を推進していくとともに、いわゆるサイバーテロ対策など緊急事態への対処能力の向上を進め、情報セキュリティに係る人的・技術的基盤の層を厚くするほか、セキュリティに関する知識の普及啓発を推進していくことが必要である。

我が国の情報セキュリティ対策は、昨年の重点計画策定以来着実な進展を見せているものの、こうした新たな課題を受け、更に取組を強化していくことが求められている。

このため、情報の自由な流通と民間の自由な活動の確保を大前提としつつ、情報通信に関する安全性及び信頼性の確保並びに個人情報の保護に一層の努力を行う。こうした取組は、治安、防災、安全保障等においてとりわけ強力に推進される必要があり、国際的な連携の下で行われることが重要である。具体的には、災害時等における情報システムのバックアップ体制や、高度なセキュリティが求められる施設における光ファイバ等の活用などの十分な配慮が必要である。

#### < 主要指標 >

	1999年	2001年
政府・企業等における情報セキュリティポリシー策定率（注1）	18.9%	24.0%
政府・企業等におけるファイアウォール設置率（注1）	50.7%	69.1%
政府・企業等におけるバックアップ実施率（注1，2）	24.3%	43.8%
情報セキュリティ関連有資格者数（注3）	-	2,340人

（注1）（財）日本情報処理開発協会（調査回答件数 1999年：867件 2001年：718件）

（注2）調査項目の相違のため、1999年はバックアップ用のコンピュータ設置率、2001年はサーバのバックアップ用ファイルの保管率となっている。

（注3）情報セキュリティアドミニストレータ試験<sup>3</sup>及びネットワーク情報セキュリティマネージャ<sup>4</sup>の合格・取得者数

#### （2）施策の意義

<sup>2</sup> サイバー犯罪に関する条約：サイバー犯罪に関する刑事実体法、同手続法及び国際捜査協力に関する規定を含んだ世界初の包括的な国際条約。欧州評議会において作成作業が進められ、2001年11月8日に正式採択、同月23日に我が国を含む30か国が署名した。

<sup>3</sup> 情報セキュリティアドミニストレータ試験：（財）日本情報処理開発協会が実施している情報処理技術者試験の試験区分の一つ。

<sup>4</sup> ネットワーク情報セキュリティマネージャ：ネットワーク情報セキュリティマネージャー推進協議会（略称はNISM推進協議会：（社）電気通信事業者協会など7団体において設立）が実施している資格認定講習。

高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護は、世界最先端のIT国家構築の基盤となるものであり、国民一人一人が安心してネットワークを利用するための前提となるものである。

ITに係る技術革新が急速に進むに伴い、ネットワークに対する攻撃手法等が進化を遂げていることや、サイバー空間においては国内のみならず世界のどこからでも瞬時かつ隠密にサイバー攻撃を受ける可能性があることなどから、ネットワークの安全性及び信頼性を確保することは困難さを増している。このため、これらの問題に対処するための対策についても不断の見直しを行うことにより、ネットワークの安全性及び信頼性が一層高められることとなる。

### (3) これまでの主な成果

2001年度において予定していた施策については、着実に実施された。特に、重要インフラのサイバーテロ対策に係る官民の連絡・連携体制の構築、政府の緊急対応支援チームの創設など、情報セキュリティに関する事案に備えた基本的な体制を整備した。主な施策は以下のとおりである。

#### 政府部内における情報セキュリティ対策

- ・ 電子政府の実現に対応した政府のとるべき措置について、「電子政府の情報セキュリティ確保のためのアクションプラン」としてとりまとめ（内閣官房及び全府省）（2001年10月10日、情報セキュリティ対策推進会議決定）
- ・ 緊急対応支援チーム（NIRT）を創設し、同チームの運営マニュアル等を整備（内閣官房）（2002年4月1日）
- ・ 情報機器等の情報セキュリティ国際規格（ISO/IEC15408）に基づいた評価・認証事業を開始（経済産業省）（2002年2月より独立行政法人製品評価技術基盤機構において民間評価機関の認定事業を開始）

#### 重要インフラのサイバーテロ対策

- ・ 重要インフラ（情報通信、金融、航空、鉄道、電力、ガス）における連絡・連携体制を構築（内閣官房及び関係府省）（「サイバーテロ対策に係る官民の連絡・連絡体制について」、2001年10月2日、情報セキュリティ専門調査会決定）
- ・ 機動的技術部隊（サイバーフォース）を整備（警察庁）（2001年4月1日「サイバーテロ対策技術室」設置）

#### 民間部門における情報セキュリティ対策及び普及啓発

- ・ 「コンピュータ・ウイルス監視装置」の導入を行う民間事業者に対する税制上の優遇措置を実施（総務省）（2001年8月13日告示改正）
- ・ 小学校及び中学校において情報モラルなどの学習を実施（文部科学省）（2002年度の新学習指導要領から実施）

#### 情報セキュリティに係る制度・基盤の整備

- ・ 支払用カードの偽造等の犯罪に関する罰則を整備（法務省）（2001年6月26日「刑法の一部を改正する法律」成立、同年7月24日施行）

- ・ 携帯電話等を用いたインターネット利用の急増に対処するための安全性・信頼向上策、迷惑メールへの技術的対策等について基準を策定（総務省）（2002年3月7日「情報通信ネットワークの安全性・信頼性基準」改正）
- ・ 情報セキュリティマネジメントに関する国際規格（ISO/IEC17799）を国内規格化（経済産業省）（JIS X 5080を2002年2月20日公示）

#### 個人情報の保護

- ・ 個人情報の保護に関する法律案提出（内閣官房）（2001年3月27日）
- ・ 行政機関の保有する個人情報の保護に関する法律案、独立行政法人等の保有する個人情報の保護に関する法律案、情報公開・個人情報保護審査会設置法案、行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律案提出（総務省）（2002年3月15日）

#### 情報セキュリティに係る人材育成

- ・ 電気通信主任技術者試験に情報セキュリティに関する試験科目を追加（総務省）（2001年4月）
- ・ 情報処理技術者試験に情報セキュリティアドミニストレータ試験を導入（経済産業省）（2001年10月）
- ・ 米CERT/CCへ専門技術要員の派遣（防衛庁）（2001年3月～9月）

#### 情報セキュリティに係る国際連携

- ・ 第2回G8ハイテク犯罪対策官民合同ハイレベル会合を開催（警察庁、総務省、外務省、法務省及び経済産業省）（2001年5月22日～24日、東京）
- ・ アジア・太平洋ハイテク犯罪対策担当実務者会議を開催（警察庁）（2002年2月26日～28日、東京）
- ・ アジア太平洋地域のCSIRT（Computer Security Incident Response Team）による国際会議を開催（経済産業省及び防衛庁）（2002年3月24日～26日、東京）
- ・ 米国防総省との間においてITフォーラムを開催（防衛庁）（2002年2月14日、東京）

### （4）具体的施策

#### 政府の情報セキュリティ確保

各府省において情報セキュリティポリシー<sup>5</sup>の継続的な評価・見直しを実施し、その水準を一層向上させるとともに、政府の情報セキュリティ確保のための体制を整備する。また、情報セキュリティ水準の高い製品等の利用、重要システムのバックアップ、擬似アタックを含めた情報セキュリティ評価の実施等、国民に信頼される電子政府及び電子自治体の構築を推進する。

#### ア）情報セキュリティポリシーの実効性の確保（内閣官房及び全府省）

<sup>5</sup> 情報セキュリティポリシー：どのような情報資産をどのような脅威からどのようにして守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含めた規定。



i) 2002年度中に、内閣官房において各府省の情報セキュリティポリシーに関する再評価、「情報セキュリティポリシーに関するガイドライン」(2000年7月、情報セキュリティ対策推進会議)の改定及び実施手法の模範例の提示を行うとともに、これを受けて各府省において情報セキュリティポリシーの見直しを行う。

ii) 2002年度中に、各府省は、各府省の情報セキュリティポリシーの実効性を確保するため、ポリシー運用の徹底を図るとともに、ポリシーに基づき、安全なネットワーク設計、監視・防護対策の強化、バックアップ、外部監査、訓練の実施等の情報セキュリティ確保のために必要な措置を行い、電子政府にふさわしいセキュリティ水準を確保する。

#### イ) 電子政府の情報セキュリティ確保のための体制の整備(内閣官房)

i) 2003年度までに、訓練の実施等による政府の緊急対応支援チーム(NIRT)の緊急時対応能力の向上、平時における情報収集・分析能力の強化、海外関係機関との連携の推進等体制の強化を行う。

ii) 2002年度中に、内閣官房を中心として実効性のある重層的な24時間監視体制の在り方について検討及び実証実験を行う。

#### ウ) 地方公共団体の情報セキュリティ確保の支援(総務省)

2002年度中に、緊急対応体制の整備への支援や地方財政措置の実施等、地方公共団体の情報セキュリティに関する支援を推進する。

#### 重要インフラのサイバーテロ対策

「重要インフラのサイバーテロ対策に係る特別行動計画」(2000年12月、情報セキュリティ対策推進会議決定)を踏まえ、重要インフラの基幹をなす情報システムについて、リスク評価、情報セキュリティポリシーの策定及びこれらに基づく情報セキュリティ対策を推進するとともに、政府の緊急対処能力の向上を図る。

#### ア) 特別行動計画における取組の強化(内閣官房及び関係府省)

2002年度中に、民間重要インフラ事業者等のサイバーテロ対策に関する取組を一層促進するため、各事業者等における情報セキュリティ対策状況の把握や実効性確保等について、重要インフラ分野ごとに具体的方策の確立を図る。

イ) 内閣官房における緊急対処体制の整備(内閣官房)

2002年度中に、サイバーテロ対応データベースの運用の開始、緊急対応支援チーム(NIRT)のサイバーテロ等への対応能力向上のための研修の実施など、内閣官房における緊急対処体制の強化を行う。

ウ) 警察における緊急対処体制の整備(警察庁)

i) 2003年度までに、サイバーテロ発生時の被害を最小限に抑えるための機動的技術部隊(サイバーフォース)において、対応能力の強化、サイバーテロに係る電磁的攻撃の手法の収集・分析能力の強化等サイバーテロに対する緊急対処体制の強化を行うとともに、2002年度中に、重要インフラ事業者等に対し、技術情報の提供、講習会の開催のほか、要請に基づき脆弱性試験の実施の協力や緊急連絡手段の提供など、サイバーテロ対策に係る支援を行う。

ii) 2003年度までに、テロ組織等に関する情報収集体制の整備、警察と重要インフラ管理者との連携強化、要員の技術の向上を図る。

エ) 防衛庁における緊急対処体制等の整備(防衛庁)

2003年度までに、防衛庁・自衛隊の保有する情報システムについて、情報セキュリティを確保しつつ運用を行うための運用ガイドラインの策定等を行うほか、情報の重要度に基づいた強固なネットワークを設け、それらの一元的な監視・統制等を行う組織を新設するとともに、情報システムに対する常時監視、システム監査、緊急事態対処等の各種機能を有した組織(部隊)の構築を行う。

民間部門における情報セキュリティ対策及び普及啓発

情報セキュリティ対策を推進するための税制、融資等の支援を実施し、民間部門の情報セキュリティ水準の一層の向上を図るとともに、情報セキュリティ対策に係る相談業務や情報交換・発信について機能の充実を行う。

ア) 情報セキュリティ意識の向上(警察庁)

2004年度までに、ハイテク犯罪<sup>6</sup>に関する相談、広報啓発活動等に従事する情報セキュリティアドバイザーを都道府県警察に配置し、その能力向上のための研修を行う。また、セキュリティポータルサイト及び情報セキュリティコミュニティセンターを活用し、消費者団体、学校関係者等と連携した

---

<sup>6</sup> ハイテク犯罪: コンピュータ技術及び電気通信技術を悪用した犯罪で、電子計算機使用詐欺、ネットワークを利用したわいせつ物頒布、不正アクセス禁止法違反等が挙げられる。

広報啓発活動を推進するとともに、ハイテク犯罪等に関する相談に迅速かつ的確に対応するためのネットワーク相談対応システムを構築する。さらに、ハイテク犯罪等に関する相談や事件に関する情報、ベンダーや関係機関からの情報等を集約・分析し、一元的に都道府県警察に提供するとともに、これらの情報を都道府県警察を通じて民間等へも提供する体制を確立する。

イ) 産業界との連携の強化(警察庁、総務省及び経済産業省)

2002年度中に、民間部門におけるセキュリティ水準の向上、ハイテク犯罪対策等の情報セキュリティ対策を効果的に推進するため、情報通信関連事業者、情報セキュリティ専門事業者、情報セキュリティ関連団体、コンピュータに関する有識者等と連携して、情報セキュリティに関する情報を収集・分析するための枠組みを構築する。

ウ) 信頼性向上施設等の導入支援(総務省)

i) 2002年度中に、自然災害等の非常時における通信手段の確保及び情報セキュリティの向上を図るため、電気通信基盤充実臨時措置法による支援対象となる「信頼性向上施設」によって、これらの施設の導入を行う民間事業者に対する税制優遇措置等の支援を行う。

ii) 2003年度まで、法人又は個人事業者が「ファイアウォール装置」を購入した場合の税制優遇措置を行う。

エ) 情報通信ネットワークにおける情報セキュリティ評価手法の確立(総務省)

2003年度までに、情報通信ネットワークに関して事業者の規模にあったセキュリティ評価項目等の検討を行い、ITUに対し国際標準提案を行うとともに、事業者における情報セキュリティ対策のレベルを的確に判断するための評価手法を確立する。

オ) 電気通信事業における情報セキュリティ対策の認定(総務省)

2002年度中に、セキュリティの高いプロバイダに関する民間認定事業の開始に係る支援を通じ、プロバイダの情報セキュリティ対策の向上及び利用者によるプロバイダの選択に資する。

カ) 不正アクセス対策・ウイルス対策等に関する情報提供体制の強化(経済産業省)

2003年度までに、不正アクセス、ウイルス等に関する情報収集・分析を行っている情報処理振興事業協会(IPA)及びコンピュータ緊急対応センター(JPCERT/CC)について、その充実強化・相互の連

携及び海外の関係機関との連携への支援を行い、情報セキュリティ情報提供機能の向上を行うことにより、広く一般利用者がこれらの情報提供を享受できる環境を整備する。

キ) 情報セキュリティマネジメント規格の普及啓発 (経済産業省)

2002年度中に、情報セキュリティマネジメント規格 (ISO/IEC17799、JISX 5080) に基づいたマネジメント実施のためのガイドラインを整備し、普及啓発を行う。

情報セキュリティに係る制度・基盤の整備

刑事基本法制、情報セキュリティに関する客観的な判断基準等、情報セキュリティ対策における制度・基盤の整備を推進する。

ア) 刑事基本法制等の整備 (警察庁、総務省、法務省、外務省及び経済産業省)

高度情報通信ネットワーク社会の安全性及び信頼性の確保に資するため、2005年までのできるだけ早い時期に、各種のハイテク犯罪に対する罰則、情報通信ネットワークに関する捜査手続について、適切な処罰を確保するため必要に応じた法整備を行う。

イ) 電気通信事業における安全・信頼性対策 (総務省)

i) 2003年度までに、電気通信事業における情報セキュリティに関して進められている国際規格の策定に対応した国内における電気通信事業用ネットワークの安全・信頼性対策基準について、所要の制度整備を行う。

ii) 2002年度中に、関係府省とも協力し、非常時における多数の事業者間の連携の強化や重要通信を効果的に確保するためのシステムの在り方について検討し、具体的方向性の確立を図る。

ウ) 暗号技術の標準化の推進 (総務省及び経済産業省)

客観的にその安全性が評価され、実装性に優れた暗号技術を採用するため、2002年度中に、ISO、ITU等における暗号技術の国際標準化の状況を踏まえ、専門家による検討会の開催等を通じて電子政府利用等に資する暗号技術の評価及び標準化を行う。

エ) 情報セキュリティ評価・認証事業の国際相互承認 (経済産業省)

2003年度までに、我が国の情報機器等の情報セキュリティ関連国際規格（ISO/IEC15408）に基づいた評価・認証事業について、政府レベルでの認証結果に関する国際相互承認スキームへの参加を目指す。

#### 個人情報の保護

高度情報通信ネットワーク社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、官民を通じた個人情報の適正な取扱いを確保することにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護する。

##### ア) 個人情報の適正な取扱いに関する基本法制の整備（内閣官房、内閣府及び全府省）

個人情報の適正な取扱いに関し、基本原則及び政府による基本方針の作成その他施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定める「個人情報の保護に関する法律案」の成立後公布の日から2年以内の施行に向けて、上記基本方針を作成するなどにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護する。

また、全ての分野を包括的に対象とする「個人情報の保護に関する法律案」の動向を勘案し、法案成立後公布の日から2年以内に、個別分野での個人情報の適正な取扱いが担保されるよう必要な措置を講じ、法の適切かつ有効な施行を図る。

##### イ) 行政機関及び独立行政法人等の保有する個人情報の適正な取扱いに関する法制の整備（総務省及び全府省）

国の行政機関、独立行政法人等に関し、個人情報の保護に関する法律案に則って公的部門にふさわしい個人情報の適正な取扱いを定める「行政機関の保有する個人情報の保護に関する法律案」及び「独立行政法人等の保有する個人情報の保護に関する法律案」その他関連法案の成立後公布の日から2年以内の施行に向けて、行政機関の保有する個人情報のあらましを記載した個人情報ファイル簿を調製することなどにより、行政の適正かつ円滑な運営を図りつつ、個人の権利利益を保護する。

#### 情報セキュリティに係る研究開発

##### ア) 国防・治安に係る情報セキュリティ技術の研究開発の推進

- i) 2002年度中に、強力なファイアウォールの研究開発を行い、警察が保有するネットワークの情報セキュリティを強化する。また、2004年度までに、司法手続きのための電子的記録の解析技術に関する

る系統的な調査研究等を行い、「コンピュータ法科学」分野の確立を目指す。（警察庁）

ii) 2003年度までに、サイバー攻撃に対する対処手法の実証的研究等を行い、防衛庁が保有するネットワークの情報セキュリティを強化する。（防衛庁）

イ) 情報セキュリティに関する基盤技術の研究開発の推進（警察庁、総務省及び経済産業省）

2005年度までに世界最先端のIT国家にふさわしい技術水準を確保するため、現在想定されているあらゆる脅威等に対する情報セキュリティ技術の研究開発を推進し、次の研究開発について2005年度までに実用化を目指す。

i) 不正アクセスやいわゆるサイバーテロの予防、検知等に関する研究開発

不正アクセスやいわゆるサイバーテロ等の脅威から情報通信ネットワークを守るため、これらの脅威を検知し、迅速かつ適切な対処を可能とするために必要な技術開発を行う。

ii) 情報通信ネットワークの安全性及び信頼性の確保に関する研究開発

情報の自由な流通を確保するため、暗号技術、電子署名等の認証技術、セキュリティ評価・認証技術、自然災害等の非常時通信機構等の情報通信ネットワークの安全性及び信頼性の確保に必要な技術開発を行う。

情報セキュリティに係る人材育成

研究開発、研修事業、資格制度の導入等を通じ、高い水準の情報セキュリティ技術を有する人材を十分に確保するための多面的な育成を行う。

ア) ハイテク犯罪対策に係る人的基盤の整備（警察庁）

2004年度までに、ハイテク犯罪捜査官の配置、サイバーパトロールモニターの委嘱、ハイテク犯罪捜査に従事する全国の警察職員への部内外の研修の実施等、ハイテク犯罪対策に必要な人材の確保や民間との協力体制の整備を行う。

イ) 防衛庁における情報セキュリティ等に係る人材教育（防衛庁）

2003年度までに、防衛庁職員を米国等へ派遣し、緊急事態対処等の高度な情報セキュリティ技術等を習得した中核的な技術専門要員を確保し、部内における技術要員の教育及び作戦情報などの秘匿性の高い情報を扱う防衛庁のネットワークの情報セキュリティの確保を行う。

ウ) ITセキュリティ技能標準の策定・普及(経済産業省)

2004年度までに、高度なITセキュリティ技術者の育成・活用を推進するため、ITセキュリティ関連業務に必要とされる技能に関する標準を策定するとともに、当該標準に基づく人材育成プログラム作りを支援する。

エ) 情報セキュリティ評価技術者の育成(経済産業省)

2004年度までに、情報セキュリティ評価基準(ISO/IEC15408,JIS X 5070)に基づく評価等を行う情報セキュリティ評価技術者及び情報セキュリティ設計技術者を育成するため、研修事業に対する助成を実施する。

情報セキュリティに係る国際連携

情報セキュリティに関する国際的な取組の推進に加え、開発途上地域への支援等国際的な取組に積極的な貢献を行う。

ア) ハイテク犯罪対策に係る国際連携の強化(警察庁、総務省、外務省、法務省及び経済産業省)

2002年度中に、G8の枠組みにおいてハイテク犯罪に関する迅速な捜査協力のためのルール作り等について協議する。

イ) 各国警察関係機関との連携強化(警察庁)

2002年度中に、アジア・太平洋ハイテク犯罪対策担当実務者会議の開催、アジア諸国警察機関との連絡のための24時間コンタクトポイントシステムの拡張等を通じ、各国警察機関との連携を強化するとともに、ハイテク犯罪対策に係る技術的指導等を行う。

ウ) 米国国防総省等との連携強化(防衛庁)

2003年度までに、米国防総省との間における政策協議等の意見交換(ITフォーラム等)等を通じて、防衛庁としての情報保証<sup>7</sup>を確立するとともに、これらのノウハウ・技術等について、国防上支障のない限り部外に公表する。

---

<sup>7</sup> 情報保証:ここでは、現在、米国防総省が実施しているコンピュータ・システム等の安全に関する各種施策の総称(Information Assurance)。

エ) 情報セキュリティに関するグローバル情報交換ネットワークの構築(経済産業省)

2003年度までに、不正アクセス・ウイルス等の発生状況・分析等情報セキュリティに関する情報集積を行っているCERT/CC等諸外国の官民関係機関との情報交換のため、JPCERT/CCにおける関係諸機関との連携強化、民間各層におけるネットワーク構築の支援等を行い、情報セキュリティに関する迅速かつ正確な情報提供、対応及び施策への反映ができる環境を整備する。

<http://www.kantei.go.jp/jp/singi/it2/kettei/020618honbun.html>



## 緊急対応支援チームの設置について

平成 14年 3月 28日

内閣官房

情報セキュリティ対策推進室

### 緊急対応支援チームの設置について

#### 1. 設置の趣旨

「電子政府の情報セキュリティ確保のためのアクションプラン」(平成13年10月10日、情報セキュリティ対策推進会議決定)等を踏まえ、電子政府や民間重要インフラ事業者等の情報システムへのサイバーテロ等の国民生活に重大な影響を与えるおそれのある情報セキュリティに係る事案に対し、各省庁等における情報セキュリティ対策の立案に必要な調査・助言等を行うための体制を内閣官房に整備する。

#### 2. 組織

内閣官房情報セキュリティ対策推進室内に「緊急対応支援チーム」(通称NIRT; National Incident Response Team)を設置。

#### 3. 人員構成

発足時においては、官民のコンピュータセキュリティ専門家15名から構成

(総括・指導担当:通信総合研究所非常時通信研究室長 大野 浩之氏)

メンバーのうち国家公務員については情報セキュリティ対策推進室への兼務辞令を発令、民間からのメンバーについては非常勤国家公務員として同室勤務を発令。

#### 4. 活動の対象となる事案

サイバー攻撃等による電子政府や民間重要インフラ事業者等の情報システムに係る障害の発生又はそのおそれがある事案等政府として危機管理対応が必要となる情報セキュリティに係る事案

#### 5. 活動の概要

NIRTは、情報セキュリティ対策推進室長の命により、事案発生時に次のような活動を行う。

事案の正確な把握

事案関連情報の収集、分析、被害拡大の予測等

被害拡大防止、復旧、再発防止のための技術的対応策の検討

事案対処方法の分析、各省庁等でとるべき対応策のとりまとめ

対策の実施に係る支援

各省庁等からの相談対応、要請に応じた対策実施支援活動

6. 今後の予定

本年4月1日付けで発足予定。

<http://www.bits.go.jp/taisaku/h140328nirt.html>