「ハッカー対策等の基盤整備に係る行動計画」

平成１２年１月２１日
情報セキュリティ関係省庁局長等会議決定

Ⅰ　はじめに

近時、産業や政府の活動の多くは、コンピュータシステムに依存するようになっており、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。いわゆるハッカー*１によるコンピュータへの侵入やコンピュータ・ウィルス（以下、「ウィルス」）の問題をはじめ、情報セキュリティに関するさまざまな問題が発生する懸念が生じている。

このような中、官民を通じ我が国全体において、情報化・ネットワーク化の進展に見合った、適切な情報セキュリティ水準を確保していく必要がある。

---

*１　「ハッカー」は、さまざまな意味で用いられるが、本行動計画では、コンピュータに不正なアクセスを行う者を指す。

Ⅱ　これまでの取組

１．政府部内における取組

各省庁においては、これまでも、自らのシステムをハッカーやコンピュータウィルス等の情報セキュリティ上の脅威から守るため、各種の対策を講じてきている（以下、本行動計画において、「政府部内における取組」とは、このような政府自らのシステムに係る対策を意味する）。

主として、各省庁の情報システム部門を中心として、例えば、以下のような対策が講じられている。

なお、平成１１年、「行政情報システムの安全対策指針」（行政情報システム各省庁連絡会議幹事会了承）が策定されているところである。

①体制整備
- システム管理者の設定その他

②ユーザ（内部職員）の管理等に関する対策
- ユーザＩＤ管理（長期不在者のＩＤの停廃止等）
- パスワード管理（ユーザにパスワードを設定させるとともに、容易に推測しうるパスワードを設定しないこと、パスワードを随時変更すること等につきユーザを指導）
- 重要データへのアクセス権限の限定
- 重要施設に係る入退室管理

③システムの構築・運用に関する対策
- 不正アクセスを防止する機能（ファイアウォール等）の導入
- 機器、ソフトウェアの導入時におけるウィルス検査の実施
- ワクチンを用いた定期的なウィルス検査の実施
- アクセス履歴の保管、定期的分析

④その他
- 緊急時体制の整備（不正アクセス等の緊急事象発生時における組織内の連絡体制や復旧手順の確立等）
- ユーザに対する教育・啓蒙
- 第三者によるシステム監査の実施

２．民間に対する普及啓蒙等

関係省庁は、民間においても１．に掲げるような対策が進むよう、基準・指針等を策定し、民間に対する普及啓蒙を図っている。

（参考）関係省庁がこれまで公表している基準・指針等
（分野別・業種別等各種のものが存在）
- 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）
- コンピュータウィルス対策基準（平成７年・通商産業省告示）
- 情報システム安全対策基準（平成７年・通商産業省告示）
- コンピュータ不正アクセス対策基準（平成８年・通商産業省告示）
- システム監査基準（平成８年・通商産業省公表）
- 情報処理サービス業情報システム安全対策実施事業所認定基準（平成９年・通商産業省告示）
- 情報システム安全対策指針（平成９年・国家公安委員会告示）

また、普及啓蒙に止まらず、法的な基準を策定している例もある（電気通信事業法上の電気通信設備に関する技術基準、技術基準への適合に関する認証制度）。

３．技術開発の推進

更に、官民のシステムの防護に資するべく、不正アクセス関連（不正アクセスの自動検知や発信源追跡等の技術を含む）、ウィルス関連、暗号関連等、情報セキュリティに関する各種技術の開発を関係省庁において推進している。

４．法制度の整備と捜査体制の充実

以上のような防御面での対策を進める一方で、不正アクセス行為等を処罰するための法制度の整備、捜査体制の充実を進めている。

（１）法制度（罰則）の整備
①コンピュータ犯罪に係る刑法改正

昭和６２年の刑法改正において、電子計算機使用詐欺、電子計算機損壊等業務妨害、電磁的記録不正作出及び供用を処罰する規定を設けた。

②不正アクセス禁止法の制定

平成１１年８月６日、通常国会において「不正アクセス行為の禁止等に関する法律」が成立し、同８月１３日に公布された（施行は、一部条文を除き、平成１２年２月１３日）。

同法においては、特定電子計算機（電気通信回線に接続している電子計算機）のうち、アクセス制御機能によりその利用を制限されているものに、電気通信回線を通じて、他人の識別符号等を入力して作動させ、その制限されている利用をし得る状態にさせる行為（「不正アクセス行為」）の禁止等を定めている。

（２）捜査体制の充実

警察庁にハイテク犯罪に対応するためのナショナルセンターを設置し、都道府県警察の体制を強化する等、「サイバーポリス」とも呼ぶべき体制の整備を図っている。

５．国際的連携

ＯＥＣＤ（セキュリティ・プライバシー作業部会*２ 等）、Ｇ８国際組織犯罪対策上級専門家会合（リヨングループ）を始めとする国際フォーラムに参加しているほか、各省庁において国際的な連携を図っている。

---

*２　ＯＥＣＤのセキュリティ・プライバシー作業部会とは、情報・コンピュータ・通信政策委員会（ICCP）の下の作業部会。正式名称は、「情報セキュリティとプライバシーに関する作業部会（WPISP）」。

Ⅲ　取組強化に関する基本的考え方

１．政府部内における取組

政府は、平成１５年度までに電子政府の基盤を構築することとしている（「経済新生対策」平成１１年１１月１１日経済対策閣僚会議）ところ、この電子政府が、国民及び海外の信頼を得るだけの情報セキュリティ水準を確保するよう図ることは重要な課題である。

また、これまでの政府部内の取組は、主として、各省庁の情報システム部門における取組に止まっていたところ、政府内での連携を強め、情報セキュリティ関連の技術開発や、現在検討中のセキュリティ評価といった政策を、より有機的に政府部内の対策に組み込んでいくことにより、一層のセキュリティ水準向上が期待できる。

このため、本行動計画では、平成１５年度を当面の目標年限とし、また、政府部内の情報セキュリティ対策を、情報システム部門のレベルに止まらず、政府全体として取り組むべき課題と位置づけて、施策の推進を図る。

２．民間等における取組

民間、地方公共団体といった国以外の者（以下、「民間等」）における情報セキュリティ対策については、本来的に、各者の自己責任において実施されるべきものであるが、政府としても、これまで、広く我が国経済社会全体の利益を図る観点から、各主体が自主的に取組を進めるための環境整備（各種基準・指針等の普及をはじめとする情報提供）を行ってきている。

本行動計画においては、以下の２つの観点から、取組の強化を図る。

① １．のような政府部内における取組強化について、民間等にモデルとして提示するため、積極的に情報の公開を行う。

② 経済社会の根幹をなす民間重要インフラや地方公共団体といった特定分野については、万一問題の発生した場合、国民生活に重大な影響が及ぶ危険性（いわゆるサイバーテロの危険性）が考えられることから、「自主的な取組の環境整備」から一歩踏み出し、特に取組の推進を図る。

３．国際的連携

上記のような政府全体としての取組を推進するにあたり、各省庁が行っている既存の連携を一層強化するとともに、関係省庁で協力して、諸外国との必要な協力体制の構築を図る。

４．その他

（１）法制度の整備について

コンピュータにより処理・保存される情報（以下「コンピュータ情報」）の不正入手・漏示については、現行法制上、各種罰則の適用により相当程度までは処罰の対象となり*３ 、また、当然ながら、他者に経済的な損失を与えた場合には民事上の損害賠償等の対象とはなり得るものの、不正入手・漏示自体を一般的に処罰の対象とする規定は設けられていない。

一方、コンピュータ情報の保護に係る罰則について、諸外国の立法例は、各国ごとに相当の差異があり、必ずしもコンピュータ情報の不正入手等を一般的に処罰の対象としているものではない。

・ドイツ：　保護されている電子情報の不正入手一般を処罰の対象としている。

・アメリカ：　無権限でコンピュータにアクセスし、国家の国防又は外交上の秘密情報、一定の金融機関の金融情報等を入手することを処罰の対象としている。

・フランス：　情報の不正入手等を一般的に処罰の対象とする規定はない。

この問題については、昭和６２年の刑法改正の際にも、処罰の対象とす

---

*３　例えば、不正アクセス行為を行った上で情報を不正入手した場合には、「不正アクセス行為の禁止等に関する法律」に基づく処罰の対象となる。

このような、コンピュータ情報の保護に関連する罰則として、同法のほか、以下のようなものがある。

・刑法上の罰則（電子計算機及び電磁的記録に関する罪のほか、秘密を侵す罪、名誉に対する罪等。また、窃盗罪、背任罪等の財産罪が成立する場合もある）

・無体財産権の侵害に対する罰則（著作権法、特許法等）

・通信の秘密の侵害に対する罰則（有線電気通信法、電気通信事業法等）

・公務員の秘密を保持すべき義務違反に対する罰則（国家公務員法、地方公務員法等）　等

る規定を設ける必要がないか検討されたが、多様な情報の取扱いや、コンピュータ以外で用いられる情報の取扱いとの均衡等について更に検討を重ねることが必要とされたところ*4 であり、以上を踏まえつつ、引き続き検討を行う。

（２）サイバーテロ対策について

サイバーテロ対策については、本行動計画に基づき基盤的な政策を推進しつつ、更に検討を行い、平成１２年１２月を目途に、「サイバーテロ対策に係る特別行動計画」としてとりまとめることを予定している。

---

*４　コンピュータ情報の不正入手・漏示を一般的に処罰する規定を設けることには、以下のような問題点がある。

・コンピュータ情報には多種多様なものがあり、秘密としての要保護性や重要性においても軽重がある上、秘密情報、プライバシーに関わる情報、財産的価値のある情報等様々なものがあり、それぞれの特質に応じた取扱いを検討する必要がある。

・コンピュータによって処理・保護されていない情報にも要保護性や重要性において高いものがあり、これらに対する保護との間で均衡を失する。

・関連する諸規定との関係をどのように考えるかについて、慎重な検討が必要である。

Ⅳ　取組強化のための具体的措置

１．政府部内における取組の強化

（１）セキュリティに関する信頼性の高い政府システムの構築

【概要】

各省庁におけるシステムの構築について、セキュリティ評価や技術開発といったプロセスを有機的に組み込み、よりセキュリティ水準の高い政府システムの構築を図る。

【具体的措置】

①セキュリティ水準の高い製品や技術等の利用

・各省庁は、新たなコンピュータシステムを構築する際、それぞれのシステムに応じた十分なセキュリティ水準の製品や技術等を利用するよう留意する。

・通商産業省は、情報機器等の政府調達におけるセキュリティ関連国際規格（ＩＳＯ／ＩＥＣ１５４０８）*５の活用等の方針について、関係省庁と連携し、平成１３年５月までを目途に検討を行う。検討の結果については、行政情報システム各省庁連絡会議（総務庁を事務局とする各省庁会議）の場で提示し、同連絡会議において「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」の合意を目指す。

②セキュリティ水準の高い製品や技術等の開発

・通商産業省、郵政省等関係省庁は、経済新生対策における決定事項（「平成１５年度までに電子政府を実現させるために不可欠な技術開発を行う」）を踏まえ、情報セキュリティ関連分野においても、必要な製品、技術（特に、ハッキングの監視・検知、追跡等の技術を含む）等の開発を推進する。

・警察庁、防衛庁をはじめ、特にセキュリティ水準の高いシステムを構

---

*５　米国をはじめ一部欧米諸国では、10年程度前から、軍事上の調達基準を出発点として、セキュリティ評価・認証制度（情報機器等のセキュリティ水準を評価・認証するための制度）を整備・運用しており、認証結果の国際相互承認の動きも進展しているところ。ＩＳＯ／IEC15408は、こうした流れを前提として、セキュリティ評価基準に係る国際規格として合意されたもの。

築する必要のある省庁は、自らのシステムの必要に応じて、セキュリティ水準の高い製品、技術等の開発を引き続き推進する。
・以上を含め、上記の省庁が推進する情報セキュリティ関連の技術開発の成果については、その他各省庁も、必要に応じて活用する。
・上記における技術開発は、国際規格も念頭に置きつつ推進する。

（２）監視・緊急対処体制の整備・強化

【概要】

不正アクセスやウィルス発生等の緊急事象について、監視を行うとともに、事象発生時に緊急情報連絡、侵害の検知、システム閉鎖等の対処を迅速に行う体制（以下、「監視・緊急対処体制」）の整備・強化を図る。*6

【具体的措置】

・警察庁は、ハイテク犯罪、不正アクセス手法に関する分析等を活用するなどして、既存の監視・緊急対処体制の強化・拡充を行う。また、防衛庁は、保有するシステムについて、情報セキュリティを確保しつつ運用を行うためのシステム運用ガイドラインを平成１５年度までに策定するほか、各種の脅威動向等のノウハウを蓄積し、これらノウハウを踏まえて、当該システムの監視・緊急対処体制の整備に取り組む。
・各省庁は、それぞれ、または共同して、以上の取組及び平成１１年から１２年の越年時における経験を適宜参考にしつつ、監視・緊急対処体制の整備の方策について検討する。検討に当たって必要があれば、本局長等会議（幹事会を含む）等の場を適宜活用する。

なお、平成１１年から１２年の越年時においては、コンピュータ西暦２０００年問題に係る情報連絡体制の一環として、不正アクセスやウィルス発生等の緊急事象について、官邸を中心とし、外部専門家も活用しつつ、各省庁・民間の情報を集約する等の体制をとったところである。

---

*6　なお、米国政府では、政府内の各行政機関や産業界が連携して、緊急事象に係る警報発出、侵害の検知等を行うための体制を整えつつあり、また、軍においては、常時、監視・緊急対処を行うための体制が既に整備されている（国防情報システム局等）。

（３）総合的・体系的な情報セキュリティ対策の検討

【概要】

各省庁の情報システム部門における技術的対策に止まらず、より総合的・体系的な情報セキュリティ対策の推進を確保するため、具体的方策について引き続き検討を行う。*7

【具体的措置】

- **本局長等会議（幹事会を含む）において、関係省庁からの協力を得て、総合的・体系的な情報セキュリティ対策推進を確保するための具体的方策について、引き続き検討し、平成１２年１２月までを目途に、各省庁向けの「情報セキュリティポリシーに関するガイドライン」（仮称、参考参照）を策定する。**
- **関係省庁は、上記ガイドラインを国際的にも信頼されうるものとするため、海外における取組動向等を十分に調査し、上記の本局長等会議における検討に貢献する。**
- **各省庁は、上記ガイドラインを踏まえ、平成１４年度中を目途に、情報セキュリティポリシーを策定し、これに基づく総合的・体系的な対策推進を図る。**

（参考）ガイドラインの内容として想定される事項（例）

- **総合的・体系的な情報セキュリティ対策推進に向けての基本的考え方（情報セキュリティポリシー策定の意義その他）。**
- **各省庁において策定すべき情報セキュリティポリシーの体系・項目（組織・責任体制、適用範囲、リスク分析の手法、対策決定・監査・緊急対処等の各段階における具体的手続ルール等）。**

---

*７　情報セキュリティ対策については、「システム構築」、「監視・緊急対処」といった個々の局面での断片的な対策実施に止まらず、

・対策検討の前提としてリスク分析をどのように行い、どのように対策の優先順位を決定するか

・対策を決定・実施した後、これをどのように監査し、その後の対策改善に活かしていくか

等を含め、セキュリティ対策のプロセスを踏まえた、総合的・体系的な方法論を確立することが重要である。

ＩＳＯ／ＩＥＣにおいても、ＩＳＯ／ＩＥＣ１５４０８とは別途、情報セキュリティの全体的なマネジメントのガイドライン作りを含む議論が行われているところ。

・情報セキュリティポリシーの策定体制（策定チームの設置及びメンバー、省庁内での策定手順等）
・情報セキュリティポリシーの例

（４）その他

【具体的措置】

・各省庁は、上記に掲げる対策を含め、情報セキュリティ対策を推進する基盤として、政府部内の人材につき研修等を通じて能力向上を図るとともに、秘密保全上問題がない範囲で、民間の技術専門家をはじめ外部人材の積極的活用を推進する。
・各省庁内部の情報セキュリティ対策については、継続的に評価・検証を行う体制整備を検討する必要があると考えられるところ、本局長等会議において引き続き検討し、平成１２年１２月までに結論を得ることを目指す。*8（なお、当面の本行動計画のフォローアップについては４．参照。）

*８　なお、米国政府では、各政府機関における対策推進のレビュー等を行うため、省庁横断的な「専門家レビューチーム」を設置。

２．民間等における取組の推進

（１）国以外の者一般への情報提供

【具体的措置】

・各省庁はそれぞれ、１．に掲げる自らの取組推進における経験や所管分野における施策等を踏まえ、所管分野の民間企業等が情報セキュリティ対策を実施するに際して参考となる事項を随時とりまとめ、公開する。

（２）民間重要インフラ等に係る取組の推進

【具体的措置】

・各省庁において、金融、エネルギー、情報通信、交通、医療等経済社会インフラとして重要な民間分野、地方公共団体（警察、消防を含む）その他、情報通信ネットワークを通じた事件が発生した場合に国民生活に重大な影響を与える可能性（いわゆるサイバーテロの対象となる可能性）が考えられる分野から、平成１２年４月までに、「重要分野」を選定し、本局長等会議に報告する。これを受けて、本局長等会議の下で、「重要分野」の関係者と政府関係者が参加し、官民で必要な情報交換等を行うための会議を開催する。各省庁は、このために、必要に応じて、ネットワーク化の進展状況等に関する調査・検討を実施する。

・本局長等会議（幹事会を含む）において、上記の情報交換等の状況も踏まえつつ、今後講ずべき対策について検討し、その結果を平成１２年１２月を目途に、「サイバーテロ対策に係る特別行動計画」としてとりまとめる。

・関係省庁は、それぞれの所管分野において、情報セキュリティ関連の各種施策（各種基準の見直し等を含む）に係る検討を引き続き推進・強化し、適切な場合には、その成果を本局長等会議（幹事会を含む）に報告して、「サイバーテロ対策に係る特別行動計画」の検討に貢献する。

３．国際的連携の強化

【概要】

・上記１、２に掲げると同様の対策推進を担う外国政府機関との連携・協力等を図る。

【具体的措置】

・外務省は、関係省庁と連携して、米国等この分野における体制整備が進んでいる国の関係部局からの情報収集を行い、あわせて、双方の対策推進状況について情報交換を行い、必要な協力体制の構築（例えば、緊急事象発生時における政府間の緊急連絡体制の確立、多数国間のフォーラムにおける連携等）を図る。

４．行動計画のフォローアップ

・上記に掲げる諸施策の実施状況については、平成１２年１２月を目途に、本局長等会議においてフォローアップを行う。