遠隔操作ウイルス対策に関する提言

自　由　民　主　党
総　務　部　会
通信・放送政策小委員会
ＩＴ戦略特別委員会

平成２４年１１月１６日

遠隔操作ウイルス対策に関する提言

はじめに

本年発生した遠隔操作ウイルスによる被害は、高度なサイバー犯罪技術を駆使したもので、国民に与える脅威は重大なものである。

自由民主党は、すでに「情報セキュリティに関する提言（平成 24 年 2 月 24 日）」（以下、先の提言）を行っているが、今回の事案は、先の提言の中で指摘していた「国民の安心安全」の論点が、「遠隔操作ウイルス被害」と「誤認逮捕」により顕在化した形となった。

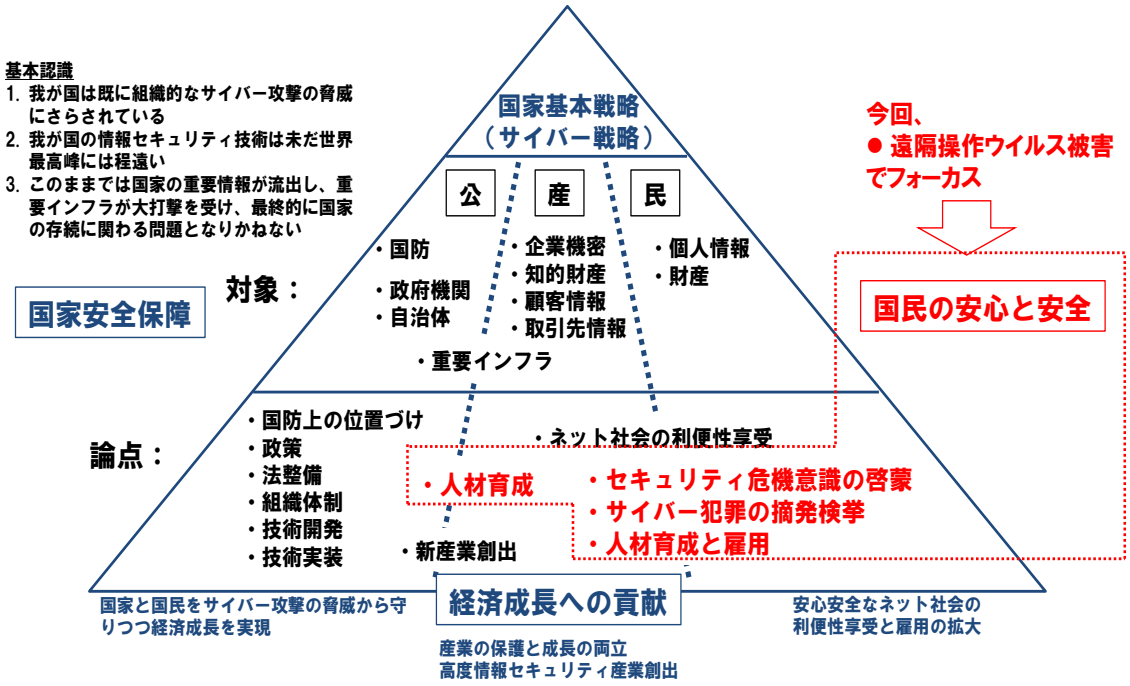
このような事案が発生した背景には、民主党政権が情報セキュリティ政策を国家的な重要課題と位置付ける事なく、国民に向けた対策を怠っていた事が根本にある。

今回の事案に関する国民向けの基本的な対策については、すでに政府の関係組織が発信しているが、未然防止、早期検挙、取り調べに渡る抜本的な官側の対策は、未だ議論の緒についたばかりである。

わが党は、昨年から連続して顕在化した一連のサイバー犯罪を国民及び国家の重大な脅威と認識し、先の提言とともにさらに遠隔操作ウイルスに関して抜本的な対策を打ち立て、より一層積極的な情報セキュリティ政策を推進していく。

図1.「情報セキュリティ政策に関する基本的な考え方」

（情報セキュリティに関する提言（平成24年2月24日）より）



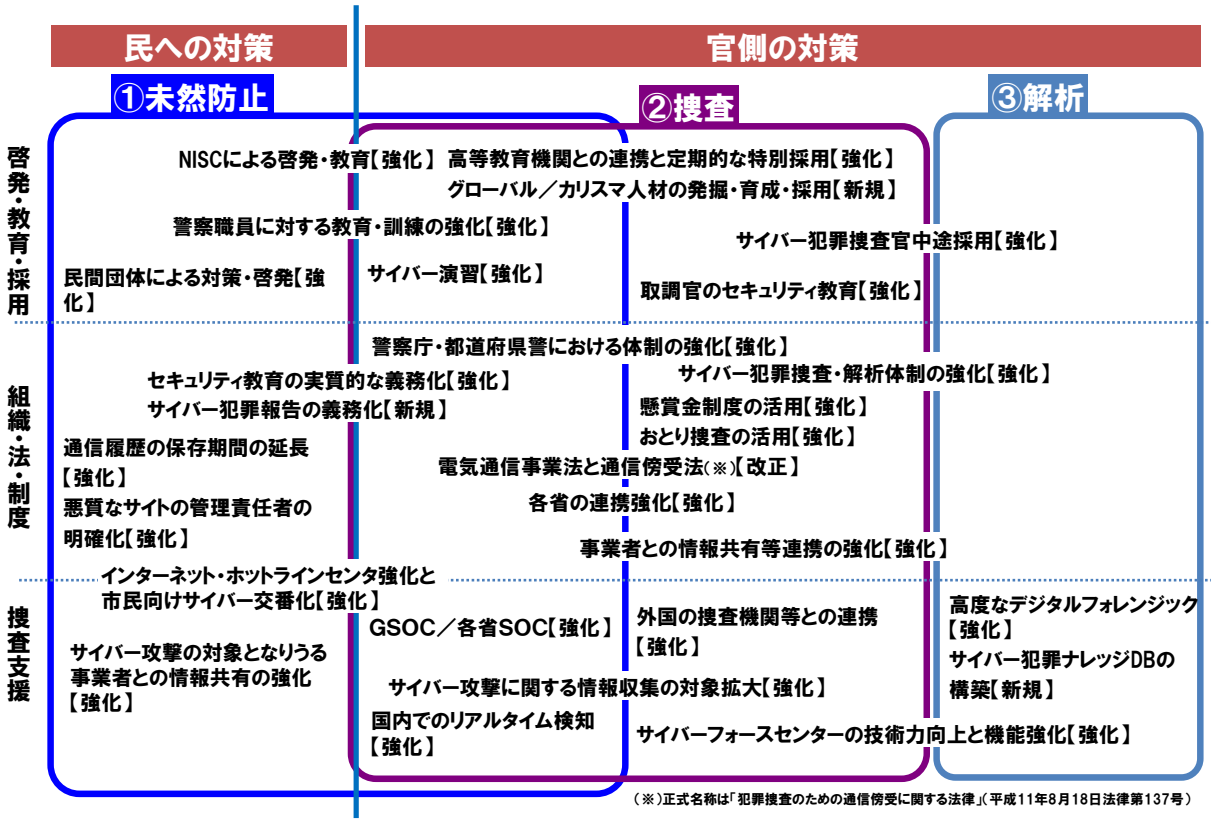
２．対策の全体像

遠隔操作ウイルスに関する抜本的な対策は、未然防止、捜査、解析の３段階のサイクルに分けて語られるべきであり、また政策分野として、啓発・教育・採用（サイバーセキュリティ技術者の雇用）、組織体制・法・制度の２分野があり、それらを支える技術的な捜査支援の施策とともに３重構造となっている。（図２）

主な対策としては、

- 国民への啓発と教育に関して、内閣官房情報セキュリティセンター（以下、ＮＩＳＣ）を中心に関連組織の官民への啓発と教育活動を大幅に拡充する。
- 未然防止と捜査の強化に必要な人材を確保するため、産官学連携で高度な情報セキュリティ人材を発掘・育成・雇用する。
- 国家として国民、企業、官をサイバー犯罪の脅威から守るため、各省の連携を強化し、総合力を発揮できる体制を整備する。
- サイバー犯罪の未然防止と捜査のため法・制度を積極的に改正・強化する。
- 官へのサイバー犯罪は国家安全保障にも関わるため、政府運用監視センター（以下、ＧＳＯＣ）を中心に官の防備を強化する。
- 捜査を支援するリアルタイム検知、デジタルフォレンジック等の技術を高度化しそのための投資を強化する。

図2．遠隔操作ウイルスに関する抜本的な対策の全体像



３．啓発・教育・採用（サイバーセキュリティ技術者の雇用）に関する抜本的な対策

未然防止、捜査、解析のサイクルに関する抜本的な対策として、啓発・教育・採用（サイバーセキュリティ技術者の雇用）の分野において、表１．のような対策を実施する。

表１．啓発・教育・採用の抜本的な対策

対策	内容
NISC による啓発・教育　【強化】	現在のＮＩＳＣの啓発・教育活動を他の関連機関の活動とも連携させて大幅に増強し、国民的なムーブメントとする。
民間団体による対策・啓発【強化】	例えば総務省管掌の Telecom-ISAC に継承された CCC の強化等、民間企業の団体を通した企業へのウイルス対策徹底を強化する。
警察職員に対する教育･訓練の強化【強化】	新しい技術の出現、サイバー犯罪・サイバー攻撃の巧妙化に対応する訓練環境の整備を行う。また、都道府県警察の捜査員には迅速に手法を習得できる環境、解析担当職員にはより高度な解析技術を習得できる環境を整備。
サイバー演習　【強化】	国並びに各都道府県警の「サイバー攻撃対策隊」を含むサイバー犯罪に関わる全ての職員を対象とした、専用環境による実践的な演習を実施する。
高等教育機関との連携と定期的な特別採用　【強化】	現在の官産学連携をさらに強化し、情報セキュリティの高等教育機関から毎年定期的に人材を官で雇用。（参考．韓国での対策の事例）
グローバル／カリスマ人材の発掘・育成・採用　【新規】	情報セキュリティキャンプやハッカーコンテスト等を強化し、グローバルに通用するカリスマ人材を発掘・育成し、官として雇用。
サイバー犯罪捜査官中途採用【強化】	現在進めているサイバー犯罪捜査官の中途採用の強化と効果的な研修の実施等により、捜査体制の質と量の拡充を図る。
取調官のセキュリティ教育【強化】	民間への講義・講習委託等により現在の教育を大幅に強化し、サイバー犯罪取調べのガイドラインを犯罪技術の進歩に合わせて徹底させる事で適正捜査を図る。

４．組織体制・法・制度に関する抜本的な対策

未然防止、捜査、解析のサイクルに関する抜本的な対策として、組織体制・法・制度の分野において、表２．のような対策を実施する。

表２．組織体制・法・制度に関する抜本的な対策

対策	内容
セキュリティ教育の実質的な義務化 【強化】	国民の情報セキュリティリテラシーを強化するため、学校や職場でのセキュリティ教育を義務化する。
警察庁･都道府県警における体制の強化 【強化】	警察庁におけるサイバー攻撃対策官の新設 及びサイバー犯罪捜査の技術的支援を行う解析担当職員の増強。都道府県警察における全国協働捜査方式のさらなる推進、サイバー犯罪捜査官の増強及びサイバー攻撃対策隊の新設と増員。
サイバー犯罪報告の義務化【新規】	一般企業と国民にサイバー犯罪、インシデント情報を報告する事を義務付け、インシデントＤＢを公開する。
通信履歴の保存期間の延長【強化】	サイバー犯罪を抑止する等の観点から通信履歴の保存期間を延長する。
悪質なサイトの管理者責任の明確化 【強化】	違法・有害な書き込みの削除等に関するサイト管理者の責任の明確化を図る。
サイバー犯罪捜査･解析体制の強化 【強化】	現在進めているサイバー犯罪捜査官の中途採用の強化を始め、サイバー犯罪捜査員及び解析担当職員の増員、効果的な研修の実施等により、捜査体制の質と量の拡充を図る。
各省の連携強化 【強化】	国家として国民、企業、官をサイバー犯罪の脅威から守るため、各省の連携を強化し、総合力を発揮できる体制を整備する。
懸賞金制度の活用 【強化】	米国の事例を参考に、サイバー犯罪に対する懸賞金制度の活用を図る。
おとり捜査の活用 【強化】	米国の事例を参考に、サイバー犯罪に対するおとり捜査の活用を検討する。
電気通信事業法と通信傍受法（※） 【改正】	通信を傍受できる対象となる犯罪の項目に、「サイバーテロ、サイバー犯罪」を追加する。
事業者との情報共有等連携の強化 【強化】	情報セキュリティ事業者等との連携を大幅に強化し、サイバー犯罪の抑止のための官民共同の枠組みを構築する。

（※）正式名称は、「犯罪捜査のための通信傍受に関する法律」

５．技術的な捜査支援施策

未然防止、捜査、解析のサイクルに関する抜本的な対策として、技術的な捜査支援施策として、表３．のような対策を実施する。

表３．捜査支援に関する抜本的な対策

対策	内容
インターネット・ホットラインセンター強化と市民向けサイバー交番化【強化】	既存の「インターネット・ホットラインセンター」に加えて、都道府県警察における一般市民向けの相談窓口を強化し、住民サービスの向上を実現する。
サイバー攻撃の対象となりうる事業者との情報共有の強化　【強化】	先端技術を有する企業を対象とした「サイバーインテリジェンス情報共有ネットワーク」や重要インフラ事業者等から成る「サイバーテロ対策協議会」を始めとする官民の情報共有の枠組みについて、その構成事業者数や対象業種を拡大するとともに、共有する情報の更なる高度化を図る。
ＧＳＯＣ／各省ＳＯＣ　【強化】	各府省庁の運用監視センター（ＳＯＣ）を強化すると共にＮＩＳＣのＧＳＯＣ機能を大幅に増強。
サイバー攻撃に関する情報収集の対象拡大　【強化】	サイバー攻撃の予告、謀議、煽動、請負等に関する国内外の公開情報やサイバー攻撃の実行を容易にする匿名性の高いサービス、攻撃ツール等に関する情報の収集を強化するなど、情報収集の対象を拡大する。
国内でのリアルタイム検知　【強化】	標的型攻撃等の新たな攻撃に対応できるよう、リアルタイム検知ネットワークシステムの観測機能の強化を継続的に実施。
サイバーフォースセンターの技術力向上、機能強化　【強化】	国内のリアルタイム検知【強化】とともに、観測結果の分析能力を大幅に強化。
高度なデジタルフォレンジック【強化】	合理的な捜査実施のために、タイムライン分析（いつ、何をしたか）や統計的分析等の手法を用いた詳細なログ解析や「不正プログラム解析センター」を中心に、より高度な解析を実施。また、そのための高度な技術を有する職員(国)の確保を図る。 民間の専門解析事業者に対して業務を委託することも検討し､サイバー攻撃に関する情報分析体制を強化する。
サイバー犯罪ナレッジDBの構築【新規】	米国の事例を参考に、全国の捜査員の連携強化のためにサイバー犯罪に関わるあらゆる情報を蓄積する基盤を構築。将来的には他関連省庁との連携も視野に入れる。
外国の捜査機関等との連携強化【強化】	各種国際会議への積極的参画等を通じて、外国捜査機関等との連携を強化する。