平成25年1月16日
サイバー空間の脅威に対する
総合対策委員会決定

サイバー犯罪対処能力の強化等に向けた緊急プログラム
～いわゆる遠隔操作ウイルス等による犯行予告事案を受けて～

一連の遠隔操作ウイルス等による犯行予告事案により、警察のサイバー犯罪捜査に対する信頼が大きく揺らぐとともに、情報通信技術の急速な発達に警察捜査が追いつけていないのではないかとの不安を国民に与える結果となった。これら一連の事案については、関係都府県警察において検証が行われ、サイバー犯罪捜査に関しては、捜査員間での知識レベルの差が大きく、本件捜査においても、第三者による遠隔操作について、知見は有していたものの、その可能性を見いだすことができなかったこと等が示された。

サイバー空間の安全・安心の確保は、警察として最優先で取り組むべき課題の一つであり、これまでも警察庁では「警察庁サイバーセキュリティ重点施策」等により各種施策を推進してきたところであるが、今回の一連の事案を受けて当面緊急に推進すべき施策をサイバー犯罪対処能力の強化等に向けた緊急プログラムとして取りまとめた。今後は、本プログラムを着実に実施し、サイバー空間の安全と安心を確保するよう努めるものとする。

第１　対処能力の向上

今後ますます高度化・複雑化するサイバー犯罪等に対処するため、次の施策により、サイバー犯罪等対処能力の向上を図る。

１　捜査力及び解析力の強化

(1)　専門的知識・能力を有する者の採用等

ア　官民人事交流

民間事業者の知見を活かし、最新の情報技術に対応した各種施策を実施していくため、警察と情報通信企業等との人事交流の実施を検討する。

イ　情報通信職員の採用拡大

インターネットやスマートフォンが普及し、多くの犯罪に悪用され、情報技術解析部門に持ち込まれる電磁的記録の解析業務が質・量共に増大していることから、解析対応力の向上のため、情報通信職員の新規採用の拡大に努める。

(2)　効果的な教育・訓練

ア　民間企業への講義委託等

捜査員一般のサイバー犯罪捜査に係る知識の底上げを図るため、民間企業に講義を委託するほか、捜査員の知識等に応じた効率的な教育の実施に努める。

イ　大学等への派遣

情報通信技術や情報セキュリティ等に関してより高度で専門的な知識を習得させるため、海外を含め、情報セキュリティ等に関する教育を行っている大学等への捜査員、解析担当職員等の派遣を検討する。

ウ　捜査員のための各種マニュアルの作成等

捜査員がサイバー犯罪に利用される情報通信技術の基礎を習得できるよう、情報通信技術に係る基礎的なマニュアルを作成するほか、デジタルフォレンジックによる犯罪捜査への技術支援を促進するため、捜査員及び捜査幹部向けのガイドブックを充実強化する。また、インターネット上の殺人予告等の事案に効果的に対応するため、これまでに発生した犯行予告事案の分析を踏まえた同種事案への対応マニュアルを作成し、捜査員に対する教育・訓練の実施に努める。

エ　高度かつ実戦的な訓練

サイバー空間の脅威への対処能力の向上や高度な技術・知識の習得のための情勢に対応した訓練環境を整備し、第一線で活動する警察職員に対し、高度な解析手法の習得等を目的とした実戦的な訓練の実施に努める。

(3)　捜査手法等

ア　捜査特別報奨金制度の効果的活用

匿名性が高く犯人に結びつく情報の収集が困難であるサイバー犯罪に関する警察への情報提供を促す手法の一つとして、一定の要件を満たしたこの種の事件等を捜査特別報奨金の対象事件として指定することができるよう、捜査特別報奨金取扱要綱を改正したところであり、同制度の効果的な活用を図る。

イ　おとり捜査の積極的活用等

サイバー犯罪捜査においては、事後的な犯人の追跡に困難を伴うケースが多

々あることから、買受け捜査を積極的に活用するとともに、新たな捜査手法について検討する。

ウ　ハッカーからの協力の確保

いわゆるハッカーは、ハッカーフォーラム等の場において、様々な情報交換を行っていることから、こうしたハッカーコミュニティーに積極的に警察職員が参加するなどしてハッカーとの関係を構築し、必要な情報収集を行う。

(4)　新技術に関する研究等

ア　Ｔｏｒ等高度匿名化技術に係る調査・研究

Ｔｏｒ(Ｔｈｅ　Ｏｎｉｏｎ　Ｒｏｕｔｅｒ)等のインターネット上の高度匿名化技術の最新の状況について調査・研究を推進する。また、Ｔｏｒ等高度匿名化技術を利用した通信からのアクセス制限等を含め、高度匿名化技術を用いた犯罪に対する効果的な対策について検討する。

イ　諸外国の捜査手法に関する調査・研究

サイバー犯罪はその特性から容易に国境を越えて行われ、他国で用いられた手口が我が国において利用されることがしばしばあることから、外国捜査機関におけるサイバー犯罪捜査手法の調査・研究を推進する。

2　体制の整備

(1)　サイバー犯罪捜査員及び解析担当職員の増員

サイバー犯罪の高度化・複雑化に対応するため、サイバー犯罪捜査員及び解析担当職員の増員に努めるとともに、都道府県警察からの派遣要請に機動的に対応すべく各管区警察局等に設置されている都道府県(方面)情報通信部情報技術解析課への「機動解析班」の設置等により、サイバー空間の脅威に対処するための体制の充実を図る。

(2)　「全国協働捜査方式」の拡充

サイバー犯罪捜査を効果的・効率的に推進するための、いわゆる「全国協働捜査方式」について、警視庁に設置されている情報追跡班の体制を強化するなどして同方式の拡充を図る。

(3)　サイバー攻撃対策の強化

サイバー攻撃対策について、警察庁の情報収集・分析機能、都道府県警察に対する司令塔機能等を強化するため、「サイバー攻撃対策官」の設置に努めるほか、情報通信部門との連携の下、サイバー攻撃の被害防止及び初動捜査に従事すべく、主要都道府県警察への「サイバー攻撃対策隊」の設置に努めるなどしてサイバー攻撃対策の強化を図る。

(4)　サイバー犯罪に対処するための体制の在り方の検討

サイバー犯罪の形態が多様化している最近の情勢やサイバー犯罪に対する国民の不安感の増大等を踏まえ、高度化・複雑化するサイバー犯罪に対してより効果的な対処を可能とするための警察庁の体制の在り方を検討する。

(5)　「不正プログラム解析センター」の拡充等

不正プログラムの解析体制を充実するため、平成24年11月１日に設置した「不正プログラム解析センター」の体制強化、不正プログラム解析に係るデータベー

スの拡充、不正プログラム解析に関する外国関係機関との情報共有等を推進する。

3　資機材の整備

(1)　新種のウイルスを検知するためのシステムの高機能化

最新のパターンファイルを適用したウイルス対策ソフトであっても検知できない新種のウイルスの検知をより確実なものとするためのシステムの強化に努める。

(2)　解析用資機材の高機能化

情報通信技術や電子機器を利用した犯罪が巧妙化・複雑化している中で、新たな情報通信技術や電子機器が用いられた犯罪にも対応できるよう解析用資機材の更新・強化に努める。

(3)　インターネット観測用システムの高機能化

ＤｏＳ攻撃による被害観測やボットネット観測、Ｐ２Ｐ観測等の各種観測機能を高度化することにより、サイバー犯罪・サイバー攻撃手法の巧妙化・複雑化に対応する技術力を強化するため、現在運用中のリアルタイム検知ネットワークシステムの更新・強化に努める。

第２　民間事業者等の知見の活用

サイバー空間の脅威に対処するためには、警察による取締りのみならず、民間事業者等の知見を活用した取組が必要である。そこで、次の施策により、民間との協力の強化、各種抑止対策等を推進する。

１　情報共有枠組みの構築

(1)　アンチウイルスベンダーとの情報共有等

新種のウイルスに対して早急な対策を講じることができるよう、警察が把握した新種ウイルスに係る情報や、アンチウイルスベンダーが把握した新種ウイルスに係る情報を相互に交換するため、既存の枠組みを活用しつつ、新たな情報共有の枠組みの構築や、民間との協力によるウイルスに係るデータベースの構築を検討する。

(2)　各種情報共有枠組みの活用

「サイバーインテリジェンス対策のための不正通信防止協議会」、「サイバー犯罪に対する警察と民間事業者の共同対処に関する指針」を受けた関係企業との協力体制等の既存の枠組みを活用して、民間との協力による情報共有の取組の強化を図る。

２　官民一体となったサイバー犯罪抑止対策の推進

(1)　通信履歴(ログ)の保存

サイバー犯罪捜査では、通信履歴が必要不可欠であるが、通信履歴が保存されていないために犯人の特定に支障が来す例が少なくないところ、サイバー犯罪抑止等の観点から通信履歴が一定期間保存されるよう、民間事業者等の取組の促進を図る。

(2)　インターネット・ホットラインセンターの拡充

インターネット上に氾濫する違法情報・有害情報に対処するため、サイバー犯罪をめぐる情勢の変化を踏まえて、違法情報・有害情報類型の見直しを図るとと

もに、インターネット・ホットラインセンターの体制の拡充に努める。

(3)　サイト管理者の管理責任の明確化

インターネット上には、インターネット・ホットラインセンターからの違法情報・有害情報の削除依頼にも応じない悪質なサイト管理者等が存在しているところ、違法情報・有害情報の書き込みに関するサイト管理者の管理責任を明確化するとともに、当該責任を果たしていない場合の措置を検討する。

(4)　サイバーパトロール強化

一般のインターネット利用者からの通報が期待されない、登録サイト内等の違法情報・有害情報やウイルスに関する情報を把握するため、サイバーパトロールを強化する。

(5)　スマートフォン用アプリに係る被害防止対策

スマートフォン利用者が悪意のアプリ(プログラム)のダウンロードにより個人情報流出等の被害に遭うケースが多発していることから、事業者等と協力して、スマートフォン用アプリに係る被害防止対策を推進する。

(6)　データ通信カード契約時における本人確認徹底要請等

事業者に対して、データ通信カード契約時における公的書類による本人確認の実施やインターネットカフェ利用者の本人確認の徹底等を要請する。

３　民間の知見の捜査等への活用

(1)　手口分析等の嘱託

民間の極めて高度かつ特殊な知見や技術を活用することが必要とされる事案について、守秘義務等に関する措置を講じた上で、民間事業者等に手口分析等を嘱託することを検討する。

(2)　解析対象となる電子機器等の技術情報に関する協力強化

効率的な解析の実施のため、解析対象となる携帯電話等の各種電子機器やソフトウェアの仕様等の技術情報の共有に関し、民間有識者、民間事業者、業界団体等との協力を強化する。

第３　国際連携の推進

地理的・時間的制約が少なく容易に国境を越えて敢行されるサイバー犯罪に効果的に対処するべく、次の施策により、国際連携を推進する。

１　外国捜査機関等との情報共有の強化

常時、外国捜査機関等とのサイバー犯罪に関する情報の交換に努めるほか、サイバー犯罪に対する最新の捜査手法を学び、外国捜査機関との連携を強化するため、米国ＮＣＦＴＡ（National Cyber-Forensics & Training Alliance）の捜査実習への職員の派遣等に努める。また、外国関係機関の解析技術部門への職員の派遣を検討する。

２　国際捜査の推進

サイバー犯罪は容易に国境を越えて敢行されることから、証拠の収集等のため外国捜査機関からの協力を得る必要がある事案については、外国の捜査機関に対して積極的に捜査共助を要請し、的確に国際捜査を推進する。

３　サイバー犯罪に係るリエゾンの派遣

主要国にサイバー犯罪捜査に係る連絡調整を任務とするリエゾンの派遣を検討する。

第４　広報啓発

インターネット空間の自由と開放性を背景に、サイバー犯罪の手口は日々変化し、高度化・複雑化しているところ、このような情勢を踏まえ、被害の未然防止等の観点から次の施策により広報啓発を推進する。

１　総合的な広報啓発

政府により毎年２月に実施される「情報セキュリティ月間」や毎年10月に実施される全国地域安全運動等の機会を捉え、不正アクセス防止対策に関する官民意見集約委員会やサイバー防犯ボランティアの活用を図るなどして国民各層の幅広い参加を得た取組を集中的に推進する。

２　民間事業者との会議等の開催

民間事業者との会議や各種講習会、都道府県警察のウェブサイト等のあらゆる機会・手段を通じ、一般のインターネット利用者、民間企業等対象の違いに応じた広報啓発活動を推進していく。

３　警察庁ウェブサイトの活用等

警察庁ウェブサイトを活用し、事件広報、新たな手口の注意喚起、被害に遭った際の対応要領等の紹介を行うほか、民間団体が管理するウェブサイトに対して、各種コンテンツの提供を行うなどの取組を推進する。