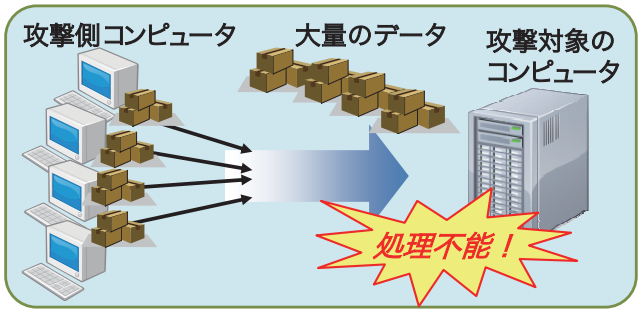
サイバー攻撃

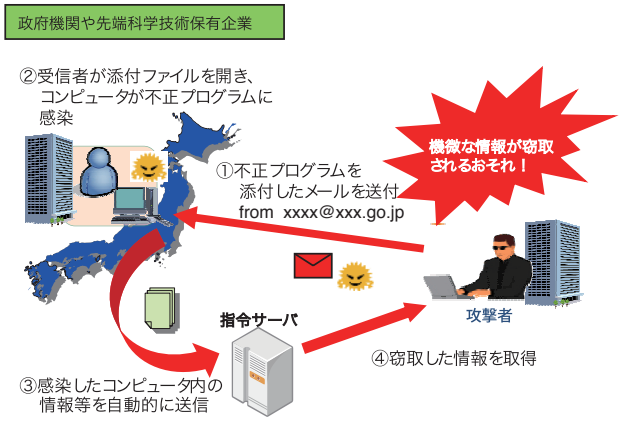
情　勢

近年、国内外において政府機関等に対する**サイバー攻撃**が続発しています。重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させてしまう**サイバーテロ**や、情報通信技術を用いた諜報活動である**サイバーインテリジェンス**の脅威は、国の治安、安全保障、危機管理に影響を及ぼしかねない問題となっています。サイバー攻撃には、**①攻撃の実行者の特定が難しい、②攻撃の被害が潜在化する傾向がある、③国境を容易に越えて実行可能である**といった特徴があり、我が国においても、サイバー空間の脅威に対する対処能力の強化が求められています。

サイバー攻撃の手口としては、攻撃対象のコンピュータに複数のコンピュータから一斉に大量のデータを送信して負荷を掛けるなどして、そのコンピュータによるサービスの提供を不可能にする**ＤＤｏＳ攻撃**や、セキュリティ上のぜい弱性を悪用してコンピュータに不正に侵入し、又は不正プログラムに感染させることなどにより、管理者や利用者の意図しない動作をコンピュータに命令する手法等があります。不正プログラムに感染させる手口として、業務に関連した正当な電子メールを装い、市販のウイルス対策ソフトでは検知できない不正プログラムを添付した電子メール（**標的型メール**）を送信し、受信者のコンピュータを不正プログラムに感染させる**標的型メール攻撃**があり、我が国においても多数発生しています。



ＤＤｏＳ攻撃



標的型メール攻撃

近年、標的のコンピュータに不正プログラムを感染させる手口の巧妙化が進んでいます。例えば、標的型メール攻撃については、多数の送信先に同一の文面及び不正プログラムを添付したメールを一斉に送信する**「ばらまき型」**の攻撃件数が減少する一方で、業務等に関係する内容を装って複数回にわたりメールのやり取りを行い、標的を信用させた後に不正プログラムを添付したメールを送信する**「やり取り型」**の攻撃件数が増加しています。

また、受信者に不正プログラムを実行させるため、一般的な文書ファイルや画像ファイルに偽装したものが増加しています。こうした標的型メール攻撃のほか、標的が頻繁に閲覧するウェブサイトに不正プログラムを蔵置し、標的がウェブサイトの閲覧に使用したコンピュータを不正プログラムに感染させる、**「水飲み場型攻撃」**と呼ばれる手口も出現しています。

【事例１】農林水産省における情報流出事案（25年１月判明）

農林水産省のコンピュータが不正プログラムに感染し、平成23年から24年までの間、ＴＰＰ交渉に関係するものを含む内部文書等が外部に流出した可能性があることが、25年１月に報じられました。その後、同年５月には、同省が設置した第三者委員会の中間報告において、24年１月から４月までに５台のパソコンから124点の文書が流出した痕跡が確認されたことなどが発表されました。

【事例２】宇宙航空研究開発機構における情報流出事案（25年４月発生）

４月、宇宙航空研究開発機構（ＪＡＸＡ）が管理するサーバが不正アクセスを受け、国際宇宙ステーション日本実験棟「きぼう」及び宇宙ステーション補給機「こうのとり」の運用準備に係る技術情報並びに関係者の個人メールアドレス等が流出したことがＪＡＸＡの調査により明らかになりました。

【事例３】韓国の銀行等に対するサイバー攻撃事案（25年３月及び６月発生）

韓国では、３月、複数の金融機関及び放送局において、不正プログラムが同時多発的に作動し、数万台に及ぶコンピュータが機能不全を起こしました。その結果、ＡＴＭやオンラインバンキングが停止したほか、ニュース原稿の作成や編集作業に影響が生じ、社会経済活動に大きな影響が生じました。

機能不全を起こした韓国金融機関のＡＴＭ
（ロイター／アフロ）

また、６月には複数の政府機関等のウェブサイトが、改ざん及びＤＤｏＳ攻撃の被害を受けたほか、政府関係者等の個人情報が流出しました。

これらの事案について、韓国政府は北朝鮮の関与を指摘しています。

対　策

■　サイバー攻撃への対処態勢

サイバー攻撃事案が発生した場合、警察は、どのような攻撃が行われたのかを明らかにし、被害を最小限にとどめ、被疑者を追跡するとともに、国民の平穏な社会生活を取り戻さなければなりません。そのために、次の事項を柱とした対応をとっています。

○　被害状況の早期把握
○　証拠資料の保全
○　被害拡大の防止
○　再発防止
○　事件捜査

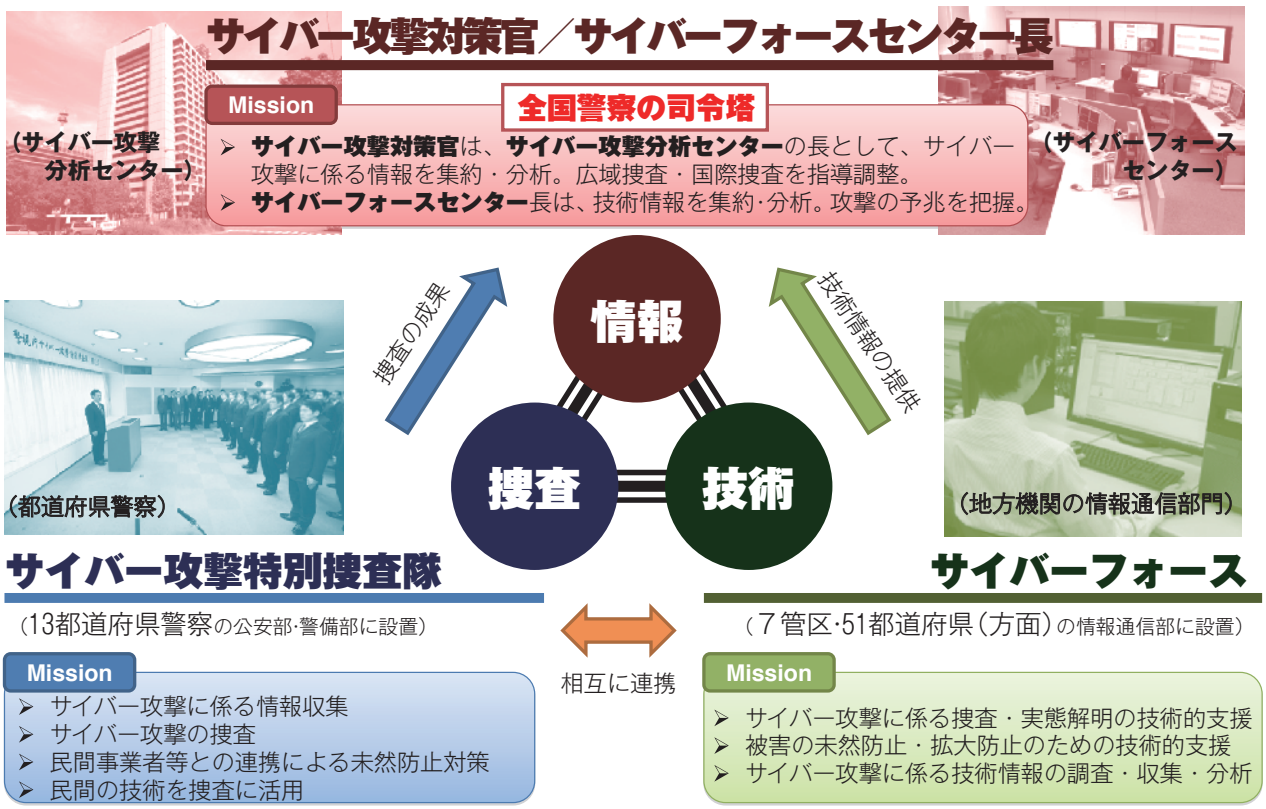
サイバー攻撃分析センター発足式

このため、警察では、警察庁や都道府県警察にサイバー攻撃対策を担当する組織を設置しており、サイバー攻撃の実態解明や被害の未然防止等の総合的なサイバー攻撃対策を推進しています。

警察庁には、**サイバー攻撃対策官**を設置しており、都道府県警察が行う捜査に対する指導・調整、官民連携や外国治安情報機関との情報交換に当たっています。また、サイバー攻撃対策官を長とする**サイバー攻撃分析センター**を設置し、サイバー攻撃に係る情報の集約・分析機能を強化しています。

都道府県警察には、警備部門、生活安全部門及び情報通信部門の職員により構成されるサイバー攻撃対策プロジェクトを設置しており、組織が一体となって対策を行っています。また、政府機関、重要インフラ事業者、先端技術を有する事業者等が多く所在している13都道府県警察には、**サイバー攻撃特別捜査隊**を設置しています。サイバー攻撃特別捜査隊は、サイバー攻撃捜査に関する専門的な知識、技能及び経験を生かし、設置された都道府県だけでなく、他県警察に対する支援を行うことにより、全国で発生し得るサイバー攻撃事案に対する対処能力の向上を図っています。また、情報収集活動の推進や民間事業者等との協力関係の確立においても、中核的な役割を果たしています。

さらに、警察では、サイバーテロへの対処態勢を強化するために、各種訓練に取り組んでいます。25年は、銀行のシステムがサイバー攻撃を受けたとの想定の下、初動対処のための机上訓練を全国の都道府県警察において実施しました。



サイバー攻撃対策の推進体制

■　サイバー攻撃の実態解明

警察では、違法行為に対する捜査を推進するとともに、サイバー攻撃を受けたコンピュータや不正プログラムを解析するなどして、攻撃者及び手口に係る実態解明を進めています。また、外国治安情報機関との情報交換を行うとともに、国際刑事警察機構（ＩＣＰＯ）を通じるなどして、海外の捜査機関との間で国際捜査協力を積極的に推進しています。

■　予兆把握と技術的対処

(1)　サイバーフォース

警察では、サイバー攻撃対策の技術的基盤として、警察庁情報通信局、各管区警察局及び各都道府県（方面）の情報通信部に、技術部隊である**サイバーフォース**を設置し、都道府県警察に対する技術支援を行っています。

また、警察庁のサイバーフォースは、**サイバーフォースセンター**として全国のサイバーフォースの司令塔の役割を担っており、サイバー攻撃発生時には緊急対処への技術支援の拠点として機能するほか、サイバー攻撃の予兆・実態把握を24時間体制で行うとともに、標的型メールに添付された不正プログラム等の分析を実施し、把握した情報や分析結果を都道府県警察の捜査員や重要インフラ事業者等に提供しています。

(2)　リアルタイム検知ネットワークシステム

サイバーフォースセンターでは、インターネットとの接続点に設置したセンサーに対するアクセス情報等を集約・分析することで、ＤｏＳ攻撃の発生や不正プログラムに感染したコンピュータの動向等の把握を可能とする**リアルタイム検知ネットワークシステム**を24時間体制で運用しています。26年１月には、情報の集約・分析能力の一層の強化を図るため、同システムの更新・高度化を行いました。このシステムで検知した情報を集約し、分析した結果を、重要インフラ事業者等への情報提供に活用しています。


サイバーフォースセンター

(3)　インターネット利用者への情報提供

警察庁では、警察庁セキュリティポータルサイト**「@police」**（http://www.npa.go.jp/cyberpolice/）を開設し、各種プログラムのぜい弱性や不正プログラムに関する情報等を公開しているほか、インターネット観測結果等の情報セキュリティの向上に資する情報を提供しています。

【事例】ウェブサイト改ざん事案の多発に係る注意喚起

25年１月以降、重要インフラ事業者等のウェブサイトに係る改ざん事案が多発しました。改ざんされたウェブサイトを閲覧するだけで不正プログラムに感染する可能性があることから、ウェブサイトの改ざん防止及び不正プログラムの感染防止のための推奨対策について「@police」で広報し、注意喚起を行いました。

■　民間事業者等との連携による被害の未然防止

(1)　重要インフラ事業者等との連携

警察では、重要インフラ事業者等に対する個別訪問を実施し、サイバーテロの脅威や情報セキュリティに関する情報の提供を行うとともに、事案発生時における警察への速報を要請するなどしています。また、警察及び重要インフラ事業者等で構成される**サイバーテロ対策協議会**を全ての都道府県に設置し、官民相互の情報共有に努めています。さらに、重要インフラ事業者等とサイバー攻撃の発生を想定した共同訓練を実施し、緊急対処能力の向上に努めています。

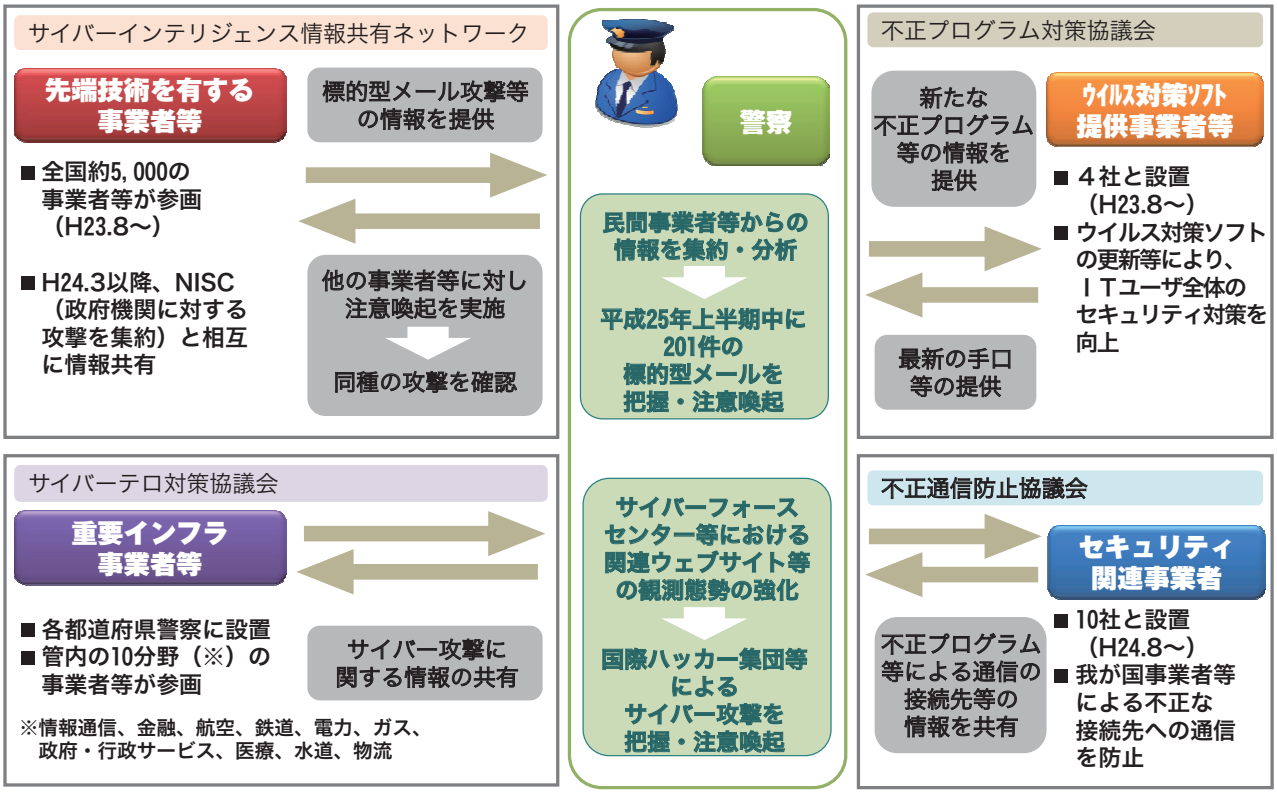
サイバーテロ対策協議会

(2)　先端技術を有する事業者等との連携

情報窃取の標的となるおそれのある約5,000の先端技術を有する事業者等との間で**サイバーインテリジェンス情報共有ネットワーク**を構築し、サイバー攻撃に関する情報を集約するとともに、これらの事業者等から提供された情報及びその他の情報を総合的に分析し、分析の結果を事業者等に提供するなどして注意喚起等を実施しています。

(3)　ウイルス対策ソフト提供事業者、セキュリティ関連事業者等との連携

警察とウイルス対策ソフト提供事業者等から成る**不正プログラム対策協議会**を設置し、警察が把握した不正プログラム対策に係る情報共有を行うとともに、警察とセキュリティ関連事業者から成る**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**を設置し、我が国の事業者等が不正な接続先に通信を行うことの防止を図るなど、官民連携した諸対策を推進しています。



サイバー攻撃対策に係る警察の取組