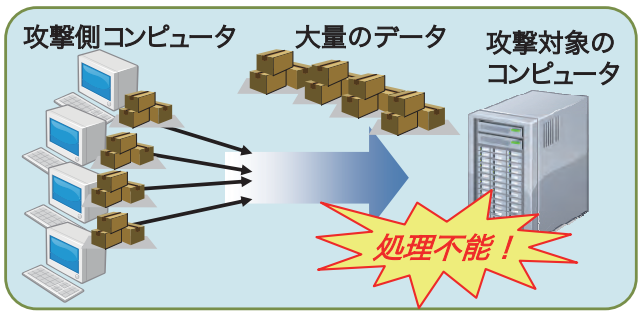
サイバー攻撃

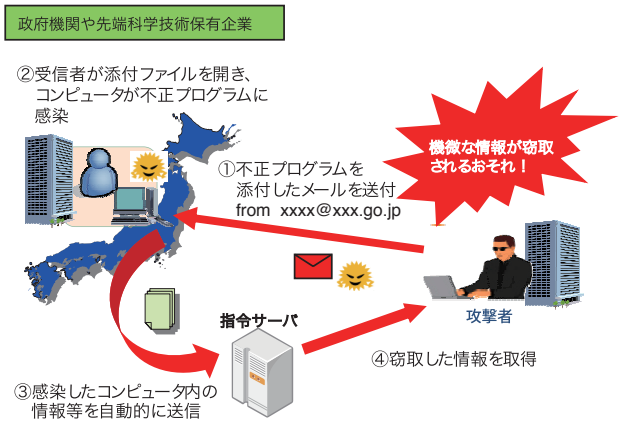
情　勢

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、安全保障及び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、攻撃対象のコンピュータに**不正プログラムを感染させる手口が巧妙化**しています。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」の攻撃件数が減少し、**対象を絞り込んだ攻撃が増加**したほか、**Windowsのショートカットファイルが添付されたメールが増加**しています。これに加えて、平成25年に確認された、対象組織の職員が頻繁に閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる**水飲み場型攻撃**のほか、**ソフトウェアの更新機能を悪用して不正プログラムに感染させるといった新たな手口**も確認されています。

【事例１】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、25年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。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。

【事例２】「もんじゅ」に対するサイバー攻撃事案（26年１月判明）

福井県に所在する独立行政法人日本原子力研究開発機構敦賀本部高速増殖炉研究開発センター（現：高速増殖原型炉もんじゅ）の中央制御室に設置されたパソコンが、**動画ソフトの更新機能を悪用した手口により不正プログラムに感染**し、外部のコンピュータと不正な通信を行っていたことが、26年１月に公表されました。その後の調査により、パソコン画面のキャプチャー画像**（注1）**、ネットワーク上にあるパソコンのアカウント名**（注2）**等のデータが窃取されていたことが判明しました。

（注１）パソコンのディスプレイに表示されている画面を画像データとして保存したもの。

（注２）パソコンを使用する上で必要となる識別情報。

【事例３】法務省に対するサイバー攻撃事案（26年９月発生）

法務省法務局の一般事務を処理するためのネットワークにつながれた端末と外部との不審な通信が確認されたため、当該通信内容等の調査を行っていたところ、**民事局及び法務局が保有する一部のサーバ及び端末に対して外部からの不正アクセス**があり、法務局の情報の一部が外部に送信された可能性があることが、26年９月に公表されました。

【事例４】米国の企業に対するサイバー攻撃事案（26年11月判明）

26年11月、米国ソニー・ピクチャーズ・エンタテインメントにおいて、**システムの破壊を伴うサイバー攻撃が発生**したことが判明しました。本攻撃により、**数千台のコンピュータが動作不能**となるとともに、**関係者の個人情報等が窃取**されました。米国当局は、本件攻撃に使用されたツールが、25年３月に発生した韓国の銀行等に対するサイバー攻撃事案において使用されたものと類似していることや、不正プログラム内に記録されていたIPアドレスと北朝鮮のインフラに関連がみられることなどから、北朝鮮政府が本件攻撃に責任を有すると結論付けたことを発表しました。

不正プログラムを実行した際に表示された画面

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、被害状況の早期把握、証拠資料の保全、被害拡大の防止、再発防止及び事件捜査を柱とした対応をとっています。

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。

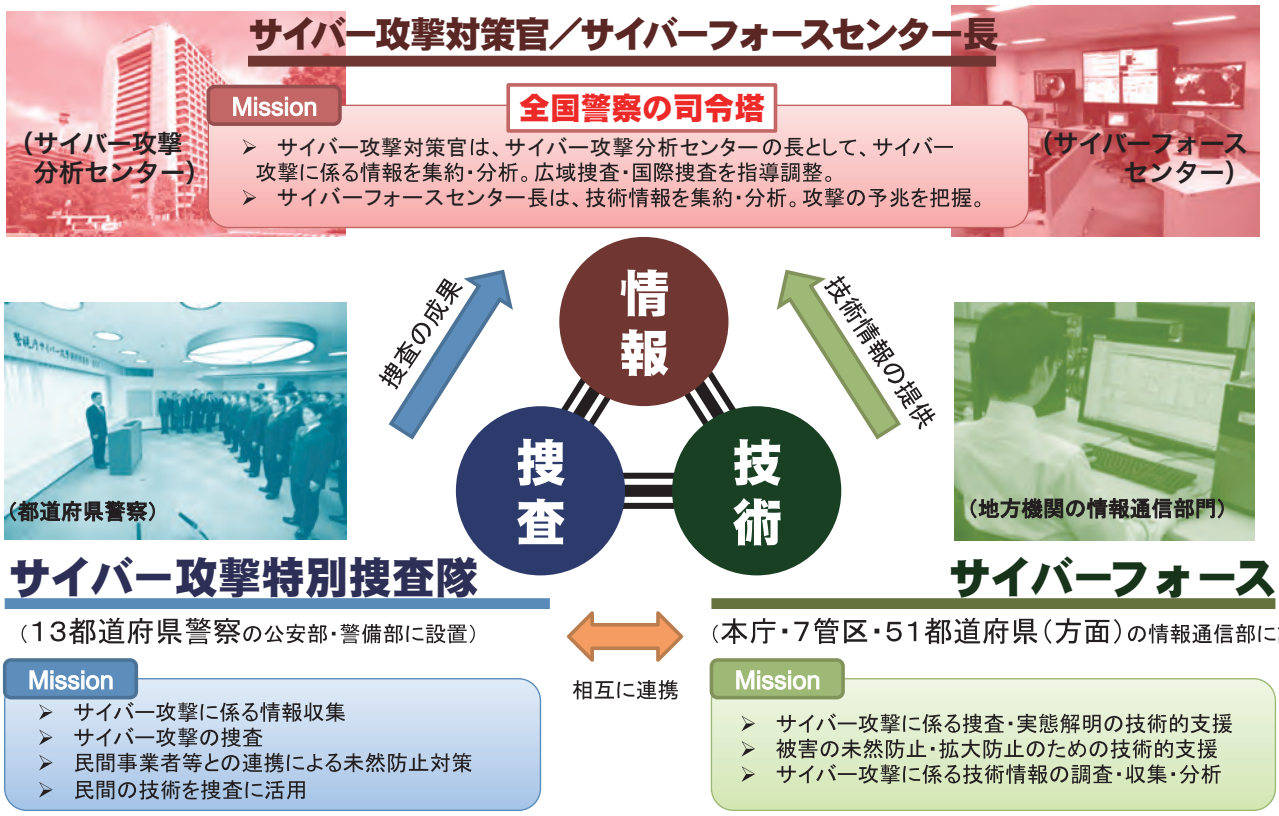
警察庁には、**サイバー攻撃対策官**を設置しており、都道府県警察が行う捜査に対する指導・調整、官民連携や外国治安情報機関との情報交換に当たっています。また、サイバー攻撃対策官を長とする**サイバー攻撃分析センター**を設置し、サイバー攻撃に係る情報の集約・分析機能を強化しています。

さらに、サイバー空間の脅威への対処は、警察のいずれの部門にとっても大きな課題となっていることから、26年４月、警察庁では、サイバーセキュリティ対策全般の司令塔としての機能を強化するため、サイバーセキュリティに関する各種取組の総括・調整を行う長官官房審議官（サイバーセキュリティ担当）及び長官官房参事官（サイバーセキュリティ担当）を設置しました。

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、技能及び経験をいかし、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るほか、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。26年は重要インフラ事業者等がサイバー攻撃を受けたとの想定の下、共同訓練を複数の都道府県警察において実施しました。

共同訓練（11月、東京）



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。

【事例】民間事業者等に対するサイバーインテリジェンス事案の実態解明

民間事業者や政府機関を標的としたサイバーインテリジェンス事案について捜査を進めた結果、高度なスキルを持つ一定規模の組織により、周到な準備の上で、長期間にわたり行われた攻撃であった可能性があることを解明し、公表しました。（６月、警視庁）

■　予兆把握と技術的対処

○　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、警察庁情報通信局並びに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。

○　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

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、ＤＤｏＳ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。

○　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】各種ソフトウェアのぜい弱性に係る注意喚起

26年中は、インターネットサーバで広く使われているソフトウェアに次々とぜい弱性が発見されました。これらのぜい弱性を悪用され、サイバー攻撃が発生するおそれがあったことから、警察では、「@police」等を通じて推奨する対策を広報し、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

○　重要インフラ事業者等との連携


サイバーテロ対策協議会

警察は、サイバーテロの標的となるおそれのある重要インフラ事業者等の間で構成される**サイバーテロ対策協議会**を全ての都道府県に設置しています。また、この協議会の枠組み等を通じ、個別訪問によるサイバー攻撃の脅威や情報セキュリティに関する情報提供、民間有識者による講演、参加事業者間の意見交換や情報共有等を行っています。さらに、サイバー攻撃の発生を想定した共同訓練やサイバー攻撃対策セミナーを実施し、サイバー攻撃のデモンストレーションや事案対処シミュレーション等を行うことにより、緊急対処能力の向上に努めています。

このほか、警察では平素から、事業者等に対し、事案発生時における警察への通報を要請するとともに、我が国の事業者等を対象とするサイバー攻撃の呼び掛け等を警察が認知した場合は、攻撃対象とされた事業者等に対して速やかに注意喚起を行い、被害の未然防止を図っています。

○　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6,833（平成27年1月1日現在）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等を総合的に分析し、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。

○　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、我が国の事業者等による不正な接続先への通信の防止を図るなど、官民連携した諸対策を推進しています。