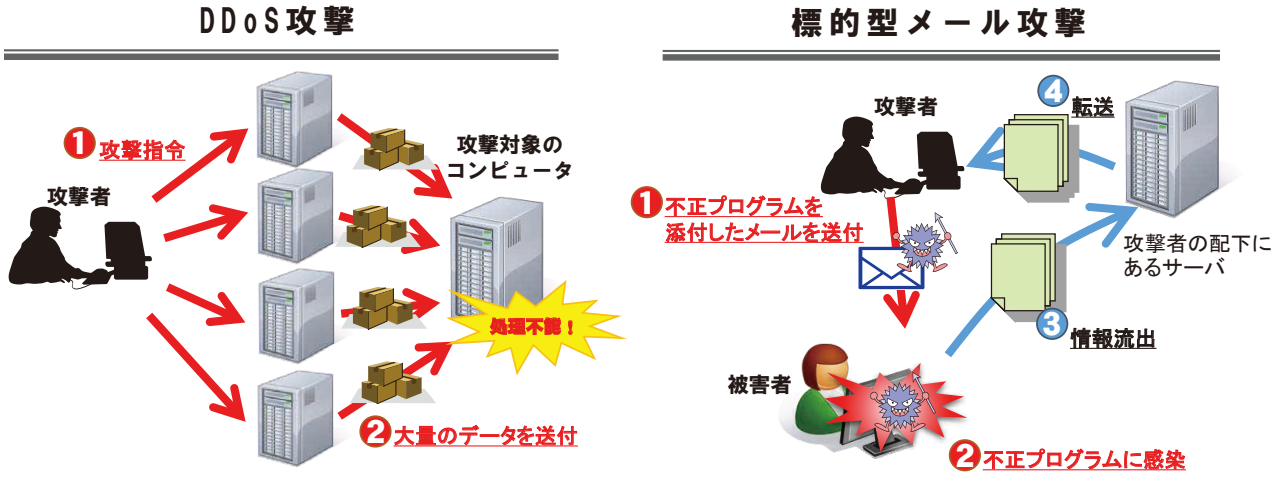
サイバー攻撃

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（サイバーエスピオナージ）**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**（注）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。



サイバー攻撃の手口

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。平成28年上半期に警察が把握した**標的型メール攻撃は1,951件であり、前年同期比で約1.3倍に増加しています。**このうち約８割を非公開のメールアドレスに対する攻撃が占めており、また、送信元メールアドレスについて攻撃対象の事業者等や実在する事業者等のメールアドレスを詐称したものが多数確認されるなど手口の巧妙化がうかがわれます。

（注）：Distributed Denial of Serviceの略。

【事例】ウクライナの電力会社に対するサイバー攻撃事案（27年12月発生）

27年12月、ウクライナにおいて大規模な停電が発生しました。ウクライナ政府は、停電がサイバー攻撃によるものとした上で、同国の電力会社の一社がシステムへの不正な侵入を受け、**30か所の変電所との通信を切断**されたことにより、**８万の顧客が停電の影響を受けた**と発表しました。

【事例】バングラデシュ中央銀行に対するサイバー攻撃事案（28年２月発生）

28年２月に発生したバングラデシュ中央銀行に対するサイバー攻撃により、**８千万ドル以上が同行から他行の口座に不正送金**されたと報じられました。米国セキュリティ会社は、この事案で使用された不正プログラムについて、「北朝鮮の犯行とされる2014年11月の米国ソニー・ピクチャーズ・エンターテインメントへのサイバー攻撃に使用されたものと同様の機能を有している」と指摘しました。

バングラデシュ中央銀行（ロイター/アフロ）

【事例】米国大統領選挙に関するサイバー攻撃事案（28年６月判明ほか）

28年６月、米国民主党全国委員会のコンピュータシステムに対するサイバー攻撃により、同国共和党大統領候補のドナルド・トランプ氏に関する**調査資料等が窃取**されたことが判明し、また、７月には、同民主党の大統領候補ヒラリー・クリントン氏の選挙陣営が使用するコンピュータシステムがサイバー攻撃を受けていたことが判明するなど、**同国大統領選挙に関連して複数のサイバー攻撃**が行われていたことが報じられました。

10月、同国政府は、ロシア政府が大統領選挙の妨害を企図して、政治団体に対するサイバー攻撃を指示していたという旨の声明を発表し、12月、同国大統領は、ロシア政府が米国大統領選挙を狙ったサイバー攻撃を行ったなどとして、ロシアに対する制裁措置を命じました。

米国大統領選挙の様子（AP/アフロ）

【事例】米企業Ｄｙｎに対するＤＤｏＳ攻撃事案（28年10月発生）

28年10月、ドメインネームシステム（ＤＮＳ）サービスを提供する米企業ＤｙｎがＤＤｏＳ攻撃を受けました。これに伴い、**Twitter、Amazon、米国の主要メディア等のウェブサイトに接続できない状態が断続的に発生**したと報じられました。攻撃には、「Mirai」と呼ばれる不正プログラムに感染した**ＩｏＴ機器が使用された**とされています。

【事例】富山大学水素同位体科学研究センターに対するサイバー攻撃事案（28年10月判明）

28年10月、富山大学水素同位体科学研究センターに対するサイバー攻撃により、同センターのパソコンが不正プログラムに感染し、**外部のサーバとの不審な通信**が発生していたことが公表されました。

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。

(1)　警察庁

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、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長官官房審議官及び長官官房参事官を設置し、部門の垣根を越えて全体を俯瞰する立場からサイバーセキュリティに関する各種取組の総括・調整を行っています。

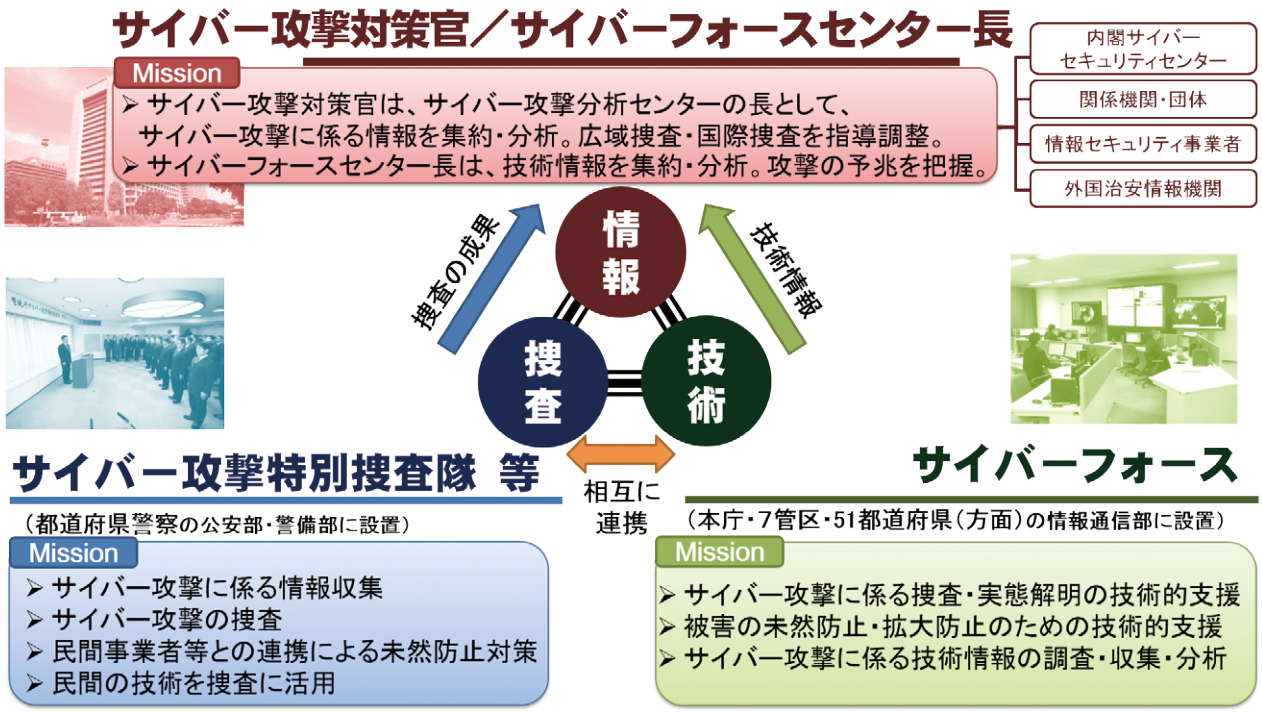
(2)　都道府県警察

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推進しています。

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する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。28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、共同対処訓練を複数の都道府県警察において実施しました。

共同対処訓練



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】政府機関に対するサイバー攻撃事件に関する捜査

我が国の政府機関に対する不正アクセス事件に関して警視庁が捜査を進めたところ、本件犯行に使用されたレンタルサーバの契約に際し、当時日本に留学生として在留していた中国籍の男性が、虚偽の氏名、住所、生年月日等の情報により会員登録を行っていた事実が判明したことから、27年11月、同人を私電磁的記録不正作出・同供用罪により検挙しました。

【事例】地方公共団体に対するサイバー攻撃事件に関する捜査

27年11月、大量のアクセスにより地方公共団体が管理していたホームページが閲覧不能になる事案（ＤｏＳ（ドス）攻撃(注)事案）が発生しました。大阪府警察は同地方公共団体から被害の申告を受け、所要の捜査を行った結果、28年５月、電子計算機損壊等業務妨害容疑で高校生（16）を検挙しました。

(注)：Denial of Serviceの略。特定のコンピュータに対し、大量のアクセスを繰り返し行い、コンピュータのサービス提供を不可能にするサイバー攻撃。

■　予兆把握と技術的対処

(1)　サイバーフォース


サイバーフォースセンター

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、**サイバーフォース**と呼ばれる技術部隊を設置し、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。

(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」**（https://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。

警察庁セキュリティポータルサイト「@police」

【事例】不正プログラム「Mirai」に関する注意喚起の実施

28年９月、サイバーフォースセンターにおいて、「Mirai」と呼ばれる不正プログラムに感染したIoT機器が発信元と考えられるアクセスの増加を検知しました。一般的にネットワーク機器が同様の不正プログラムに感染した場合、感染拡大を狙った更なる探索やＤＤｏＳ攻撃の踏み台となる可能性があることから、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

(1)　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

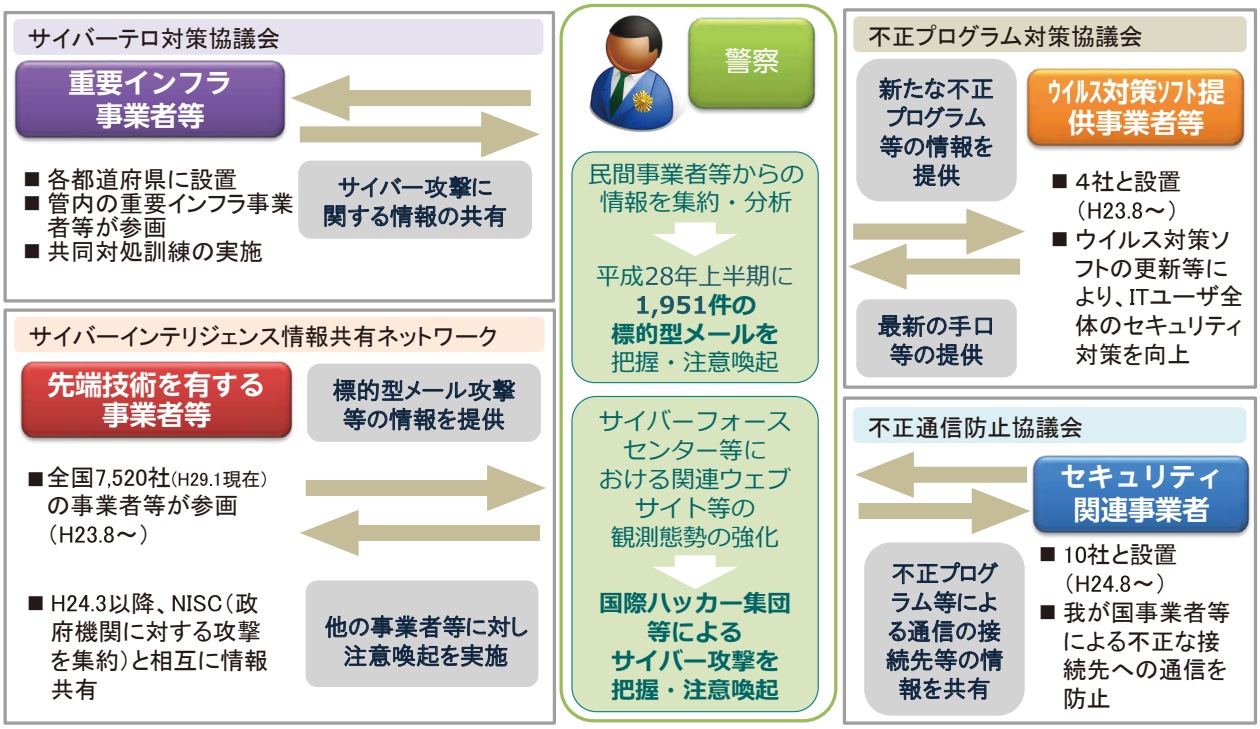
警察では、サイバー攻撃の標的となるおそれのある重要インフラ事業者等との間で構成する**サイバーテロ対策協議会**を全ての都道府県に設置しています。また、この協議会の枠組み等を通じ、個別訪問によるサイバー攻撃の脅威やサイバーセキュリティに関する情報提供、民間有識者による講演、参加事業者間の意見交換や情報共有等を行っています。さらに、重要インフラ事業者等とサイバー攻撃の発生を想定した共同訓練を実施し、緊急対処能力の向上に努めています。

(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7,500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、官民連携による諸対策を推進しています。



サイバー攻撃対策に係る民間事業者等との連携