サイバー攻撃に対する警察の取組状況

サイバー攻撃対策の推進体制

警察では、警察庁や各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いるほか、各部門が連携し、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。

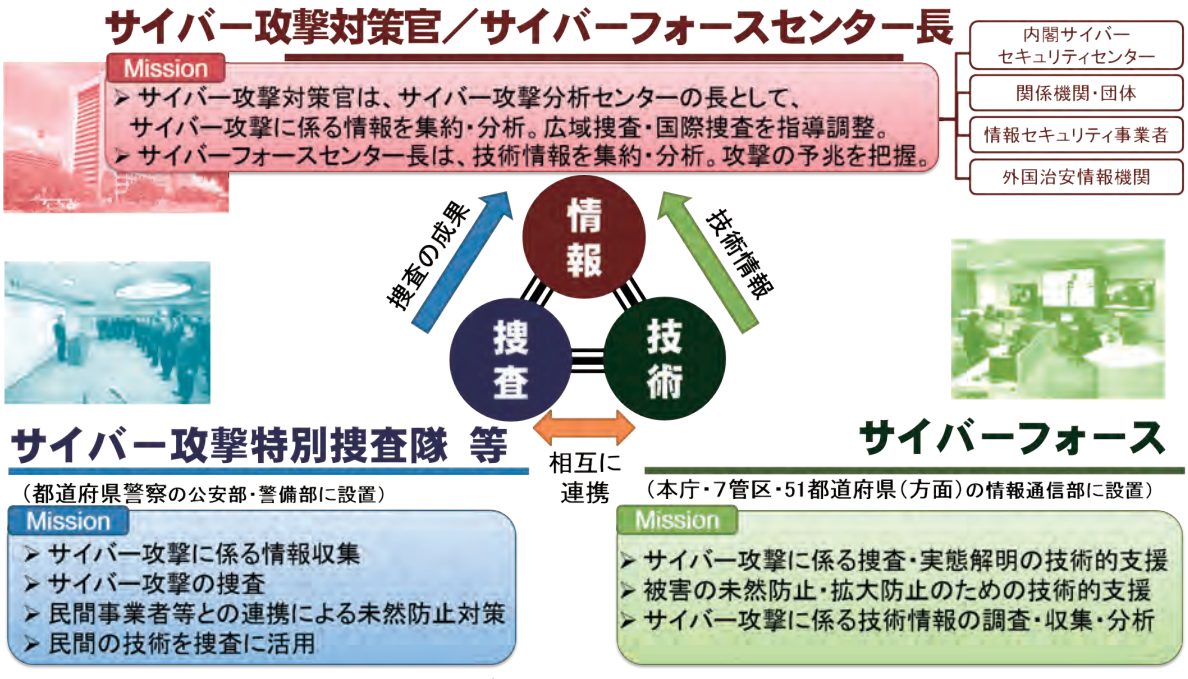
■　警察庁

警察庁では、**サイバー攻撃対策官**が、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るとともに、これを長とする**サイバー攻撃分析センター**において、サイバー攻撃に関する情報の集約・分析を実施しています。

■　都道府県警察

都道府県警察では、警備部門、生活安全部門及び情報通信部門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、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、サイバー攻撃に係る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におけるサイバー攻撃対策のみならず、他の都道府県警察に対して支援を行うことにより、全国の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。このほか、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。



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。

同人は、これまで1,000台以上のレンタルサーバを契約した上、主に海外に居住する利用者に転売して利益を上げていたとみられ、転売されたレンタルサーバのうち数台は、他のサイバー攻撃において踏み台として悪用されたとみられており、警視庁で実態解明を進めています。

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、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、24時間体制でのサイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラム等の分析、把握した情報や分析結果の都道府県警察の捜査員や重要インフラ事業者等への提供を行っています。

■　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。このシステムにより分析した結果を、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

■　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】ソフトウェアのぜい弱性に関する注意喚起

27年５月、サイバーフォースセンターにおいて、不審な通信の急増を検知しました。調査の結果、オンラインゲームで使用されるソフトウェアのぜい弱性を狙った通信である可能性が高く、このぜい弱性により、利用者のコンピュータが意図せずサイバー攻撃等の踏み台として悪用されるおそれがあることが判明しました。このため、警察では、関係機関へぜい弱性情報を提供するとともに、「@police」を通じて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

警察は、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、サイバー攻撃の発生を想定した共同対処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、我が国の事業者等に対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。

サイバーテロ対策協議会

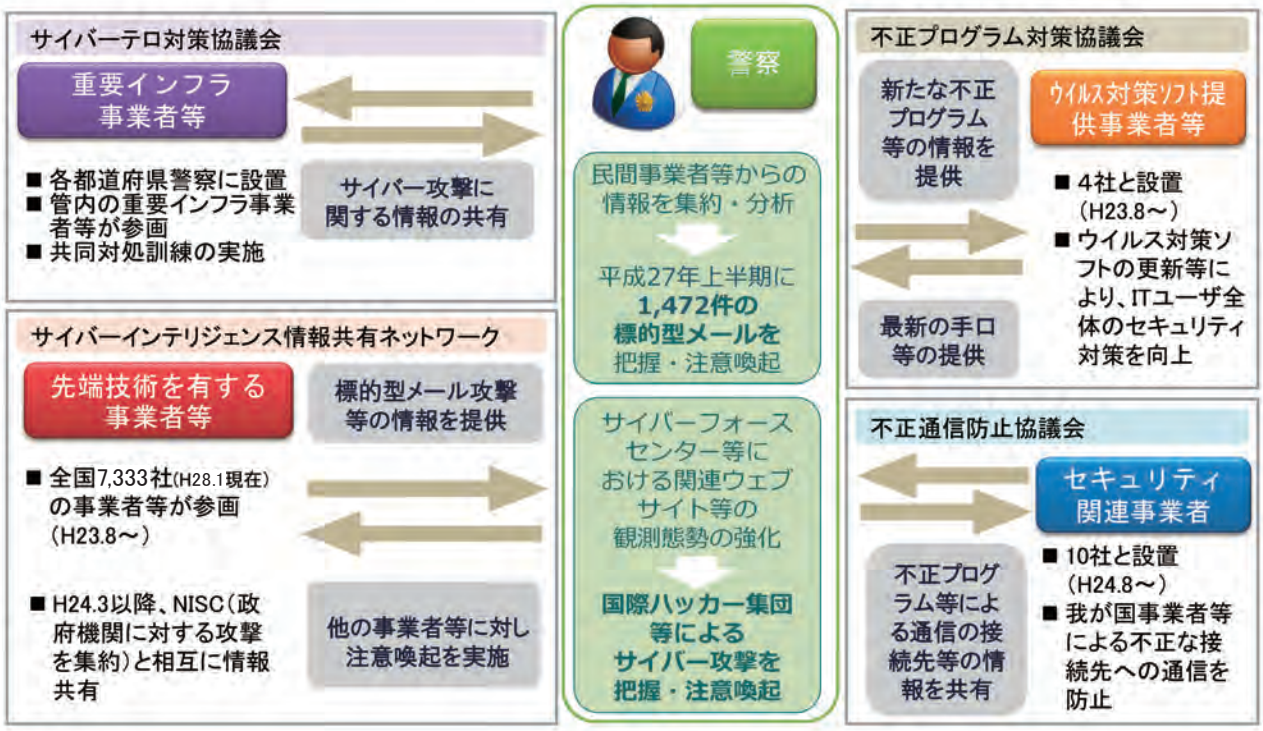

共同対処訓練

■　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高い先端技術を有する全国7,333の事業者等（平成28年１月現在）との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行う**サイバーインテリジェンス情報共有ネットワーク**を構築しています。警察では、このネットワークを通じて事業者等から提供された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、事業者等に対し、分析結果に基づく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

警察では、ウイルス対策ソフト提供事業者等との間で、**不正プログラム対策協議会**を設置しており、不正プログラム対策に関する情報共有を行っています。また、セキュリティ監視サービス又はセキュリティ事案に対処するサービスを提供する事業者との間で、**不正通信防止協議会**を設置しており、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っています。



サイバー攻撃対策に係る民間事業者等との連携