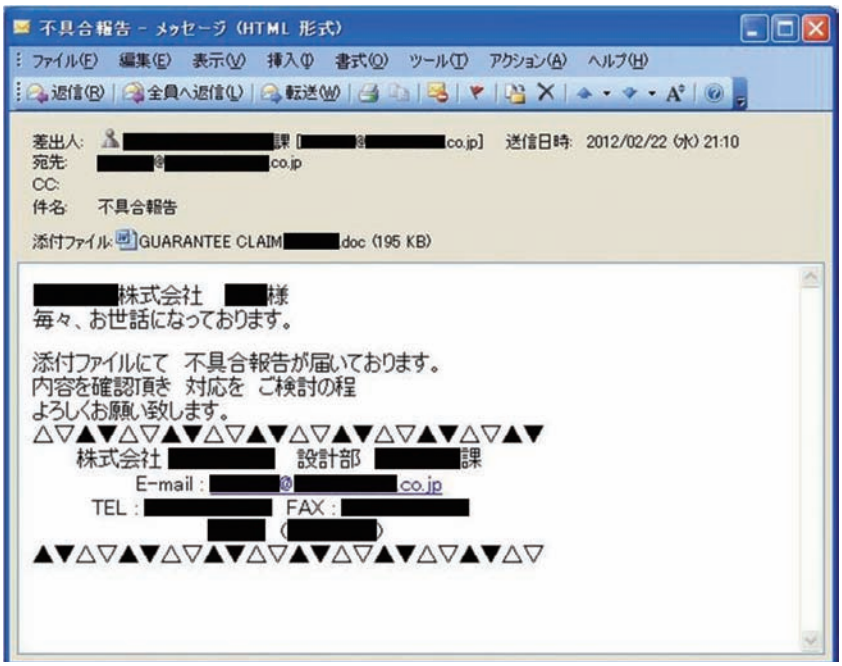
サイバー攻撃

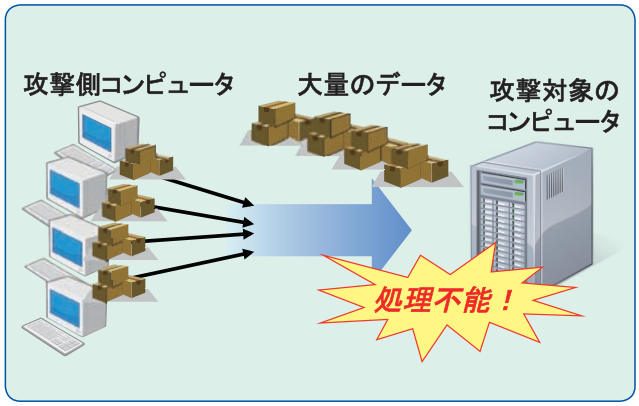
情　勢

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。

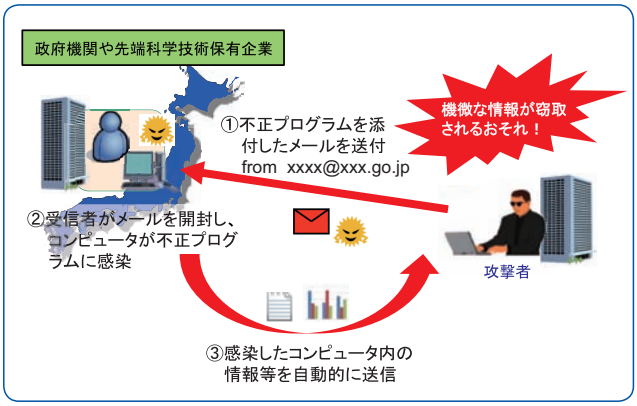


ある企業に実際に送付された標的型メール

サイバーテロに用いられる手口としては、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**が代表的です。また、サイバーインテリジェンスに用いられる手口としては、業務に関連した正当なものであるかのように装いつつ、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、これを受信したコンピュータを不正プログラムに感染させることによって、被害者の知らぬ間に機密情報を外部に送信させ、情報の窃取を図る**標的型メール攻撃**が代表的です。



DDoS攻撃



標的型メール攻撃

【事例1】宇宙航空研究開発機構に対するサイバー攻撃（24年1月、11月）

平成24年1月、宇宙航空研究開発機構（ＪＡＸＡ）において、職員のコンピュータが不正プログラムに感染したことにより、23年7月から8月までの間、**当該端末の中に入っていた情報、業務中に表示した画面情報及び米国航空宇宙局（ＮＡＳＡ）等のシステムにアクセスするためのＩＤ・パスワードが外部に流出**していたことが判明しました。

さらに、11月にも、職員のコンピュータが不正プログラムに感染し、**ロケットの仕様や運用に関わる情報が流出**した可能性があることが判明しました。

【事例2】アノニマスによるものとみられるサイバー攻撃（24年6月）

6月、国際ハッカー集団「アノニマス」を名乗る者が、改正著作権法の成立を受け、日本の政府機関等に対するサイバー攻撃を示唆する書き込みを行いました。これに伴い、財務省及び国土交通省関東地方整備局の**ウェブサイトが改ざん**されたほか、裁判所、自民党、民主党及び日本音楽著作権協会のウェブサイトが**アクセス集中により閲覧が困難**になるなど、関連が疑われる被害が発生しました。

改ざんされたウェブサイト

【事例3】尖閣諸島情勢と関連したとみられるサイバー攻撃（24年9月）

9月には、尖閣諸島の国有化を始めとした一連の情勢を受け、中国のハッカー集団の掲示板等において、日本に対するサイバー攻撃が呼び掛けられ、攻撃対象として日本の行政機関や重要インフラ事業者等が名指しされました。その後、裁判所、重要インフラ事業者等の**ウェブサイトが改ざん**されたほか、総務省統計局、政府インターネットテレビ等のウェブサイトが**アクセス集中により閲覧が困難**になるなど、関連が疑われる被害が発生しました。

中国のチャットサイトにおける謀議状況

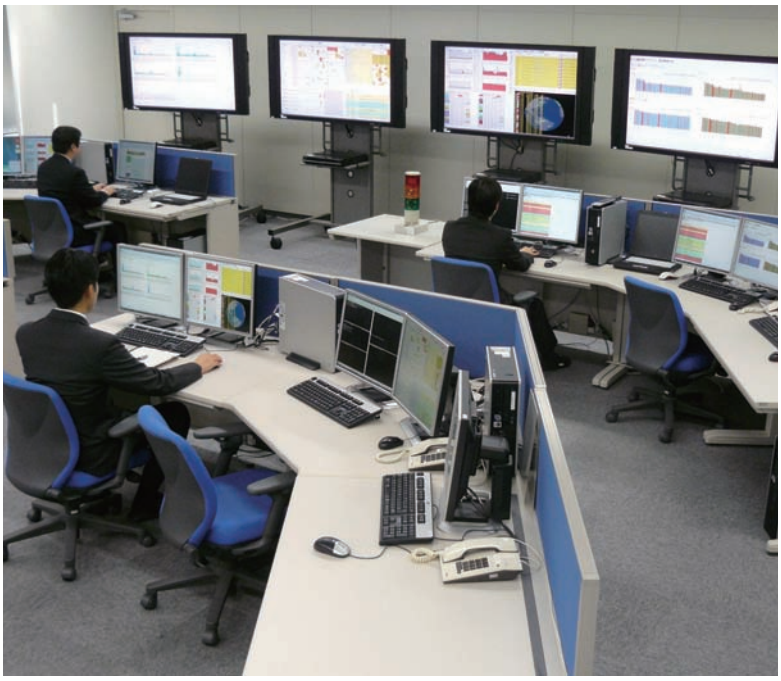
対　策

■ 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、ＩＣＰＯ（国際刑事警察機構）を通じて、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

警察では、各管区警察局等に専門の技術部隊である**サイバーフォース**を設置するとともに、その司令塔として警察庁に**サイバーフォースセンター（ＣＦＣ）**を設置しています。ＣＦＣでは、**24時間体制でのサイバーテロの予兆把握**や**標的型メールに添付された不正プログラムの分析**を実施し、集約された情報の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。また、サイバーテロ発生時には、緊急対処の技術支援の拠点として機能します。



サイバーフォースセンター

■ 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。

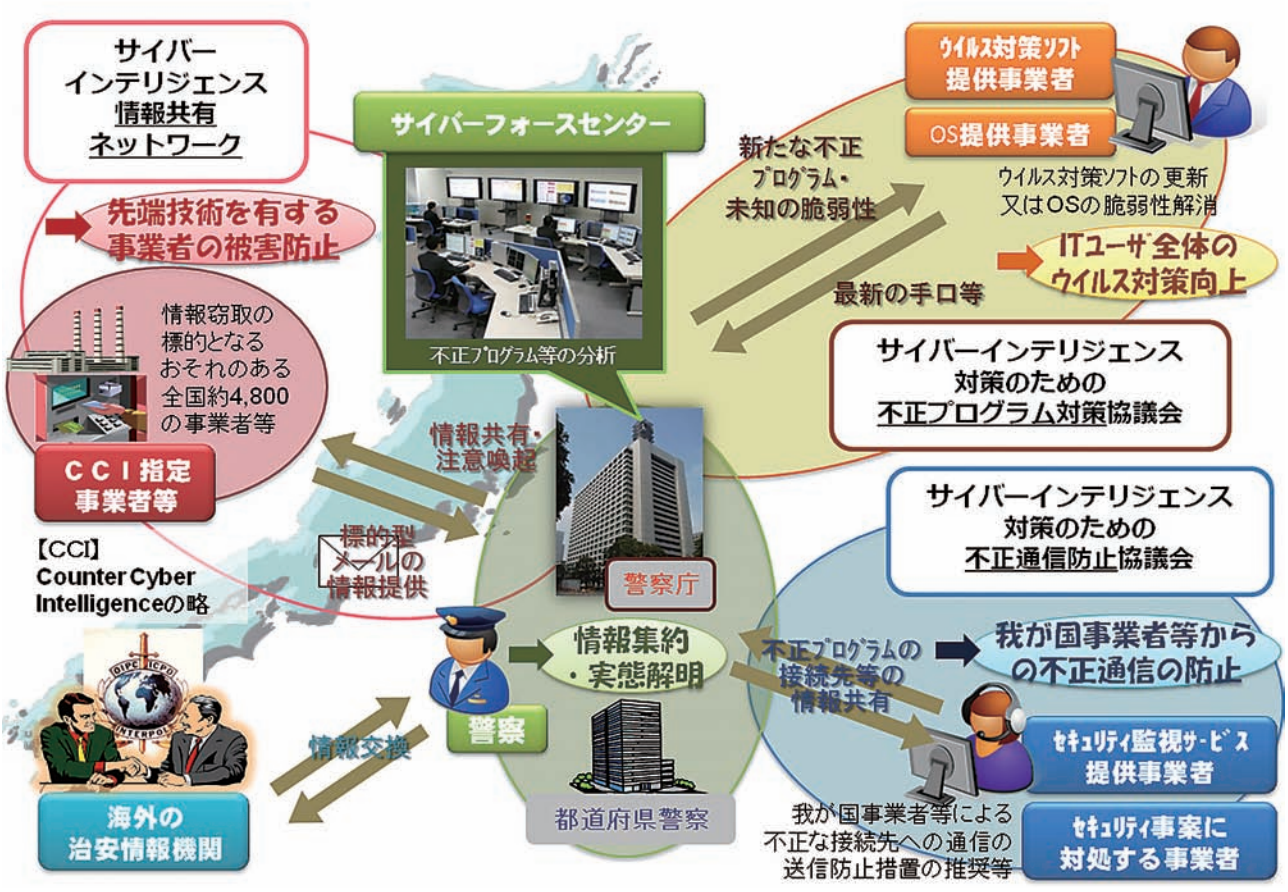
事業者との共同訓練

(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 4,800 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**サイバーインテリジェンス対策のための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、民間事業者等と連携した諸対策を推進しています。



サイバーインテリジェンス対策に係る警察の取組