特集　サイバー攻撃の情勢と対策

インターネットが国民生活や社会経済活動に不可欠な基盤として定着する一方、平成23年中は、**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**しました。

情報通信技術を用いて政府機関や先端技術を有する企業から機密情報を窃取する**サイバーインテリジェンス**や、政府機関を含む重要インフラ事業者等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**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。

	サイバーインテリジェンス	サイバーテロ
用語の意味	サイバー空間における諜報活動	○ 重要インフラの基幹システムに対する電子的攻撃 ○ 重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いもの
目　的	機密情報の窃取	基幹システムの機能障害
対　象	政府機関や先端技術を有する企業等	重要インフラ事業者等 （情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流）
主な手口	・ 不正プログラムへの感染 ・ コンピュータへの不正アクセス	・ コンピュータへのアクセス集中 ・ 不正プログラムへの感染 ・ コンピュータへの不正アクセス

サイバー攻撃には、

① **攻撃の実行者の特定が難しいこと**

→ 攻撃者は第三者のコンピュータを「踏み台」にして攻撃することが可能

② **攻撃の被害が潜在化する傾向があること**

→ 不正プログラムへの感染や不正アクセスを被害者が把握できない可能性

③ **国境を容易に越えて実行可能であること**

→ コンピュータとインターネットへのアクセスさえ確保できれば容易に国境を越えて攻撃することが可能

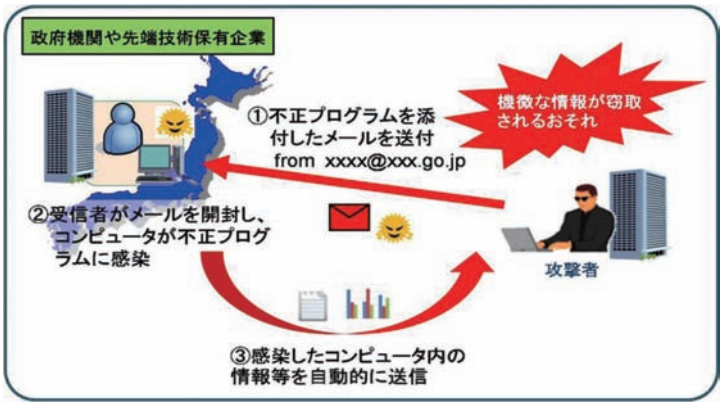
などの特徴があり、我が国においても、**サイバー攻撃への対処能力の強化が喫緊の課題**となっています。

サイバーインテリジェンスをめぐる情勢

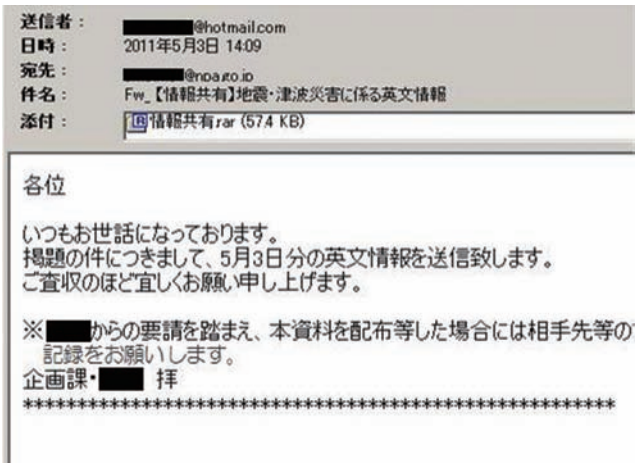
攻撃の手口

情報通信技術の普及に伴い、政府機関や民間企業では、情報を電子データで保有することが一般的となっています。平成23年中は、**我が国の政府機関・先端技術を有する企業から機密情報の窃取を狙ったとみられるサイバー攻撃**が発生しました。こうした活動によって機密情報が窃取されると、我が国の治安、外交や安全保障に重大な影響が生じるおそれがある上、重要インフラの基幹システムの設計や脆弱性に関する情報が窃取された場合、それらを悪用してサイバーテロが実行されるおそれもあります。

サイバーインテリジェンスに用いられるおそれのある攻撃の手口としては、業務に関連した正当なものであるかのように装いつつ、不正プログラムを添付した電子メール（**標的型メール**）を送付し、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り、被害者の知らぬ間に機密情報を外部に送信させる手口が代表的です。



標的型メール攻撃の仕組み


送信者：[redacted]@hotmail.com
日時：2011年5月3日 14:09
宛先：[redacted]@npa.go.jp
件名：Fw:【情報共有】地震・津波災害に係る英文情報
添付：情報共有.rar (57.4 KB)

各位

いつもお世話になっております。
掲題の件につきまして、5月3日分の英文情報を送信致します。
ご査収のほど宜しくお願い申し上げます。

※[redacted]からの要請を踏まえ、本資料を配布等した場合には相手先等の記録をお願いします。
企画課・[redacted] 拝
****


送信者：[redacted]@[redacted].go.jp
日時：2011年5月4日 20:04
宛先："[redacted]" <[redacted]@npa.go.jp>
件名：[redacted]対策基本法案
添付：[redacted]対策基本法案.zip (65.6 KB)

皆様

本件の概要
[redacted]対策基本法案

担当
[redacted]省[redacted]課 広報室

(See attached file: [redacted]対策基本法案.pdf)

==========
[redacted]省[redacted]課 広報室 [redacted]川 [redacted]子

実際に警察庁の職員宛に送付された標的型メール。送信者のアドレスやメール本文には実在する政府機関の職員の名前が使用されている上に、件名や添付ファイルもメールを受信した職員の業務に関する内容であるため、業務に関連した正当な電子メールのようにも見えます。しかし、分析の結果、添付ファイルを開封すると、そのコンピュータは不正プログラムに感染し、自動的に外部と通信を行うことが分かりました。このように、受信者にメールを開封させ、不正プログラムが仕込まれた添付ファイルを実行させるための工夫がなされている点が、標的型メールの特徴です。

機密情報の窃取

23年中、標的型メール攻撃により、防衛産業関連企業等のコンピュータが、外部からの情報窃取を可能とする不正プログラムに感染する事案が発生するなど、サイバーインテリジェンスの脅威は正に現実のものとなっています。

【事例1】三菱重工業株式会社に対するサイバー攻撃（23年9月）

9月、三菱重工業株式会社がサイバー攻撃を受け、最新鋭の潜水艦やミサイル、原子力プラントを製造している工場等で、約80台のコンピュータが**外部からの情報窃取を可能とする不正プログラムに感染**していたことが明らかになりました。同月30日、警視庁は三菱重工業株式会社から被害届を受理しました。現在、本件についての捜査が進められているところです。また、11月、同社は防衛及び原子力に関する保護すべき情報の流出は認められなかった旨の調査結果を発表しました。

攻撃を受けた三菱重工業神戸造船所
（読売新聞社）

【事例2】衆議院・参議院に対するサイバー攻撃（23年10月・11月）

10月、**衆議院のコンピュータが外部からの情報窃取を可能とする不正プログラムに感染**していたことが明らかになりました。11月には、全議員のID及びパスワードが流出し、**最大15日間にわたってメールが盗み見られていたおそれ**があるとの報告書が公表されました。

衆議院サーバー等ウイルス感染防止対策本部（時事）

また、11月、**参議院のコンピュータも不正プログラムに感染**していたことが明らかになり、12月には、**ネットワーク構成の変更等の対策が必要**であるとの報告書が公表されました。

【事例3】外務省の在外公館等に対するサイバー攻撃（23年10月）

10月、外務省の在外公館の職員が使用するコンピュータ等が、情報窃取を目的とする不正プログラムに感染していたことが明らかになりました。検出された不正プログラムは、**外務省のネットワークシステムを標的にした特殊なもの**であった旨が報じられています。