サイバー攻撃対策

政府の取組

政府は、これまでも、内閣官房情報セキュリティセンター（NISC）を中心として、「国民を守る情報セキュリティ戦略」を策定するなど、情報セキュリティ対策の強化のための取組を推進してきました。

防衛産業関連企業等を標的としたサイバー攻撃の顕在化を踏まえ、政府は、**情報セキュリティ政策会議**の下に**官民連携の強化のための分科会**を設置し、情報セキュリティ対策における官民連携の在り方について取りまとめるなど、情報セキュリティ対策の更なる強化のための取組を推進しています。

情報セキュリティ政策会議（議長：内閣官房長官、出席者：国家公安委員長等）（共同）

警察の取組

■ サイバー攻撃事案の実態解明

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。

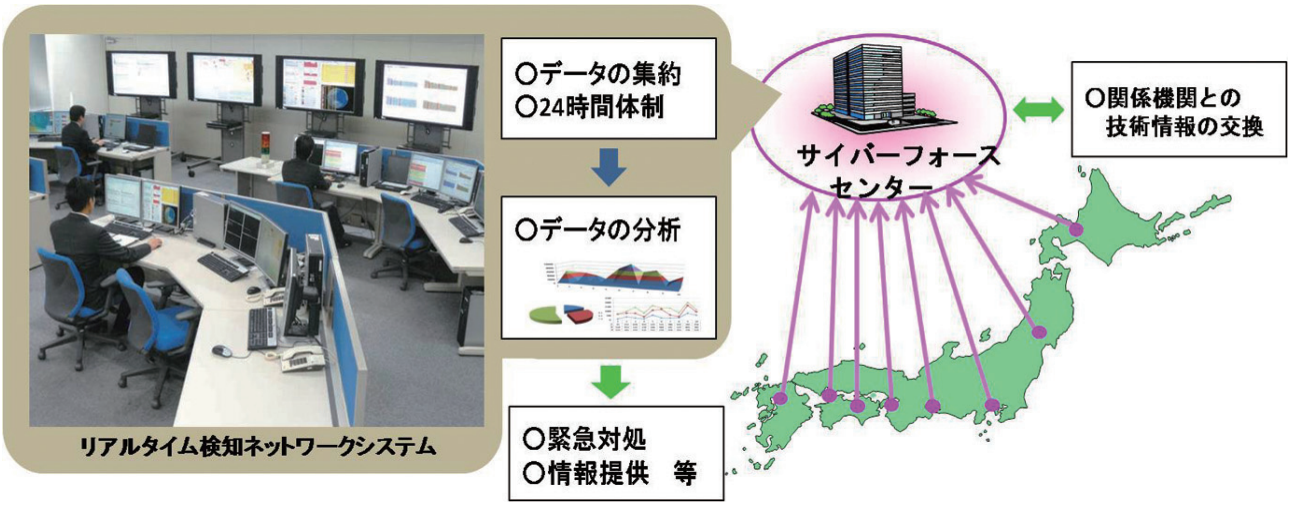
また、外国治安情報機関との情報交換を行うとともに、ICPO（国際刑事警察機構）を通じて、海外の捜査機関との間で**国際捜査協力を積極的に推進**しています。

■ 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**サイバーフォースセンター**を設置しています。

このセンターでは、**リアルタイム検知ネットワークシステム**と呼ばれる大規模なシステムを運用し、**24時間体制でサイバーテロの予兆把握**に努めるとともに、集約された情報を分析し、その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るほか、標的型メールに添付された不正プログラムの分析を行うなどしています。

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の機能

【事例1】社団法人の職員になりすました標的型メール

警察では、事業者等から提供された情報を基に、23年**4月から12月までの間に約1050件の標的型メール**が、我が国の民間企業等に送付されていたことを把握しました。下記の標的型メールは、その中の一例です。

社団法人のA氏が甲社職員等に送付した実際のメール

送信者：[redacted]@[redacted].or.jp>
日時：2011年8月26日 11:21
宛先：[redacted]
CC：[redacted]
件名：〈資料事前送付〉【8/31(水)10:30～@[redacted]：開催の連絡】 部品一括調達[redacted]
添付：一括調達における前提条件の整理_e.pdf ([redacted])

関係各位

[redacted]です。
首題打ち合わせにおける調整用資料を事前に送付させて頂きます。
ご確認のほど宜しくお願い致します。

なお、8/31(水)の当日は、弊方より印刷版を用意致しますので、
添付ファイルは事前の確認用としてご活用頂ければ幸いです。

以上。

社団法人のA氏になりすまし乙社職員等に送付された標的型メール

送信者：[redacted]
日時：2011年8月26日 21:44
宛先：[redacted]@[redacted].co.jp
件名：〈資料事前送付〉【8/31(水)1
添付：[redacted]用共通部品一括調達に係るコメント.pdf (529 KB)

関係各位

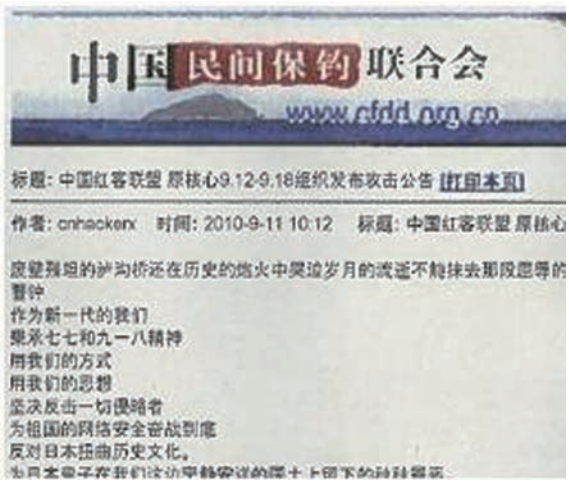
[redacted]です。
8/31(水)の当日は、弊方より印刷版を用意致しますので、
添付ファイルは事前の確認用としてご活用頂ければ幸いです。

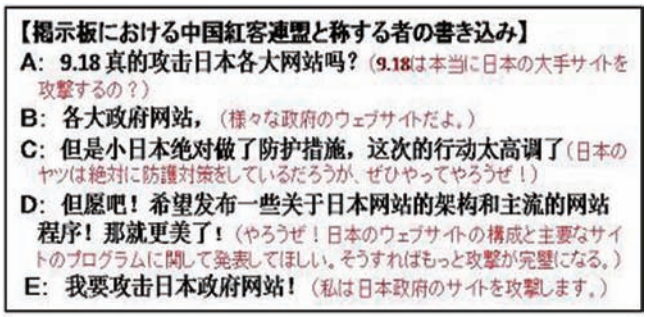
以上。

両者を比較すると、送信日時から分かるとおり、**実際のメールが送付された約10時間後にそのメールの本文をほとんどそのまま引用した標的型メールが送付**されています。社団法人のA氏が甲社に実際のメールを送付した際に、**参考送付をしていた同社団法人B氏のコンピュータが何者かにのっとられ、メールの情報が窃取された模様**です。

【事例2】「中国紅客連盟」による警察庁へのサイバー攻撃（22年9月）

22年9月、「中国紅客連盟」と称する者が、尖閣諸島の中国領有を主張する民間団体「中国民間保釣連合会」のウェブサイト上で我が国に対するサイバー攻撃を呼び掛けました。9月16日から18日にかけ、3次にわたりサイバー攻撃（DDoS攻撃）が行われ、**警察庁のウェブサイトの閲覧に支障**が生じました。





【上】掲示板における書き込みの状況
【左】「中国民間保釣連合会」のウェブサイト

攻撃の予兆を把握した警察庁では、初動対処として、攻撃対象とされたウェブサイトの**管理者に対し個別に注意喚起**を行って防御策を指導したほか、警察庁のウェブサイトの**閲覧に障害が生じた際には、これを早期に復旧**させました。

攻撃に利用されたツール

その後、警察では、改めて攻撃に利用されたコンピュータから約2万にわたる発信元を分析し、**攻撃元と思われるIPアドレスを抽出**しました。これらのうち国内のものについては「踏み台」となり、攻撃に利用されていたことが判明したことから、再度攻撃に利用されないように無害化措置を講じました。また、国外のものについては、9割が中国経由であったことから、ICPOを通じて**中国当局に捜査共助と再発防止を要請**するとともに、サイバーテロ対策協議会等を通じて**重要インフラ事業者等に本事案に関する情報を提供**し、同種の事案が発生した場合の対応について相互に情報を共有しました。

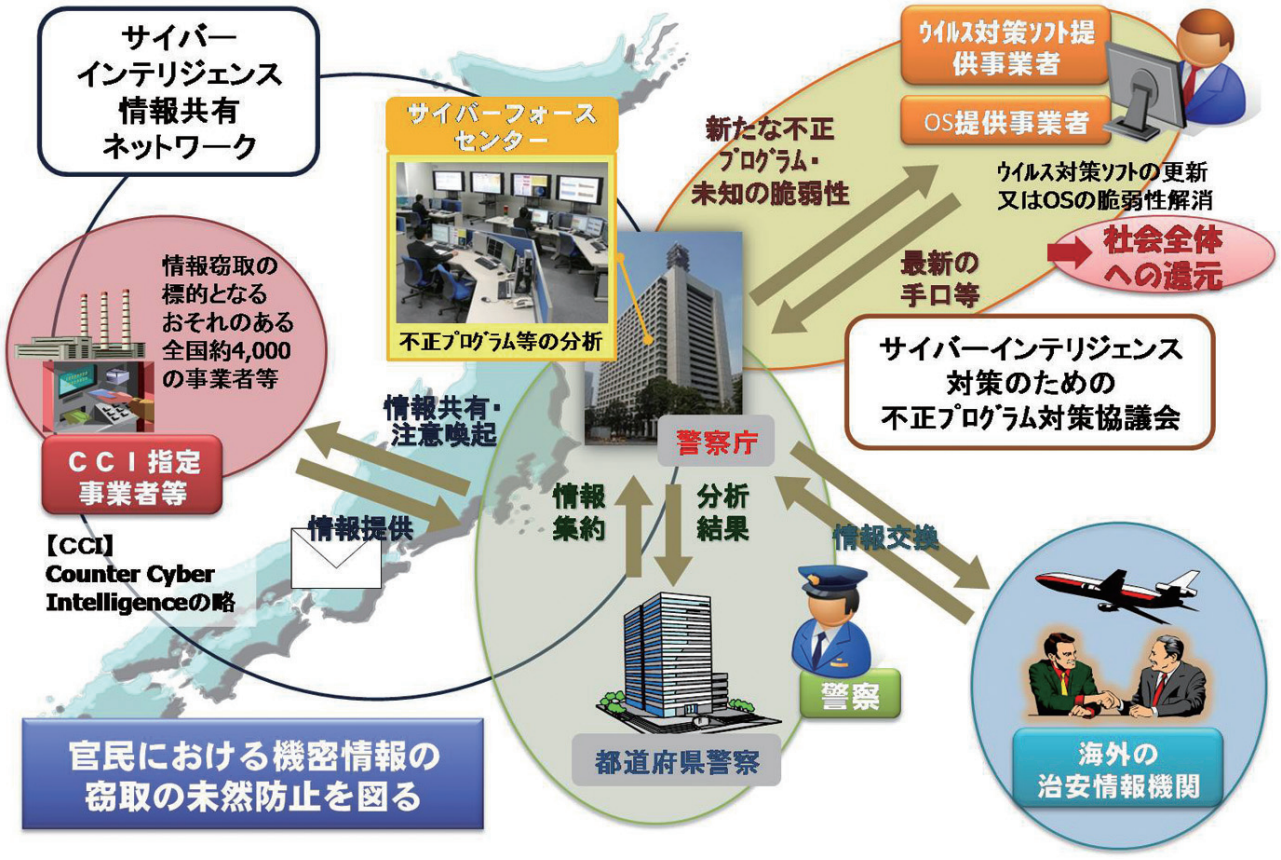
■ 官民連携の推進による被害の未然防止

(1) 先端技術を有する企業等との連携

23年8月、情報窃取の標的となるおそれのある**約4千の先端科学技術保有事業者**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。

(2) ウイルス対策ソフト提供事業者等との連携

23年8月、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、不正プログラム対策に係る情報共有を実施しています。特に、警察からは、**市販のウイルス対策ソフトで検知できない新たな不正プログラムに関する情報や未知の脆弱性に関する情報を提供**し、ITユーザ全体のセキュリティの向上を図っています。



(3) 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。

重要インフラ事業者への個別訪問

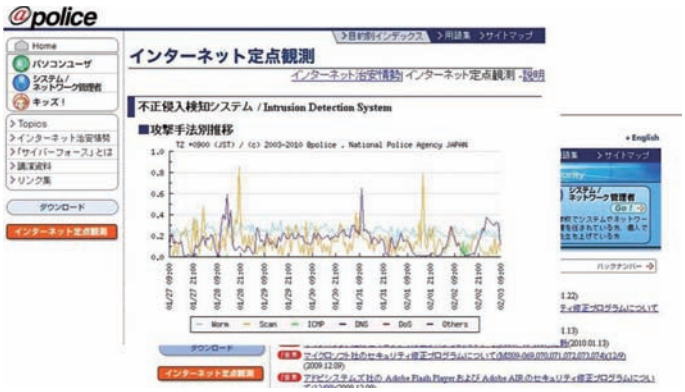
広報用パンフレット

サイバーテロ対策協議会

事業者との共同訓練

(4) インターネット利用者に対する情報提供

警察庁では、セキュリティポータルサイト「@ police」を開設し、不正プログラムの情報やインターネット上の観測データの集計・分析結果等の**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。(http://www.npa.go.jp/cyberpolice/)



警察庁セキュリティポータルサイト「@police」