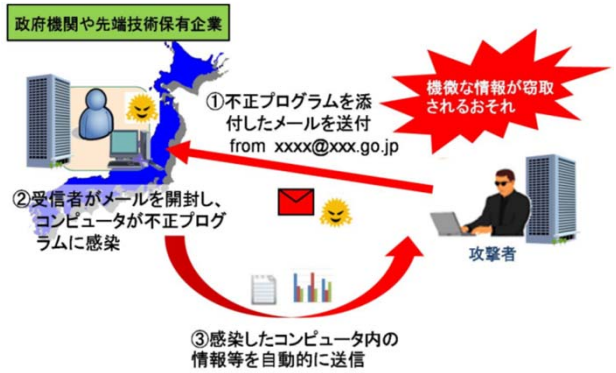
警察のサイバーインテリジェンス対策

参考3

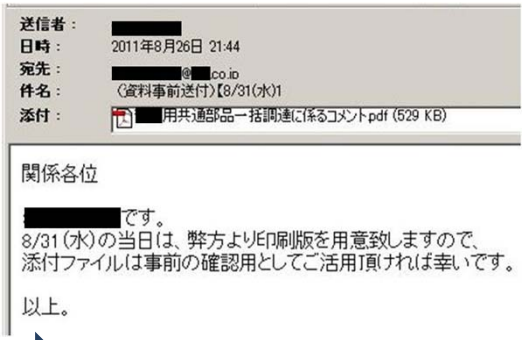
情　勢

政府機関や先端技術保有企業に対するサイバーインテリジェンス事案が続発

（標的型メール攻撃の仕組み）



（標的型メールの実例）



⇨ 23年４～９月で約890件把握

警察の取組

緊密に連携

民間事業者・団体

- **情報窃取の標的となるおそれのある事業者**
  （ｻｲﾊﾞｰｲﾝﾃﾘｼﾞｪﾝｽ情報共有ﾈｯﾄﾜｰｸ）

  先端技術を保有する全国約４千の事業者等との間でネットワークを構築し、サイバー攻撃事案に関する情報の集約・分析・注意喚起

- **情報セキュリティ関連事業者**
  （ｻｲﾊﾞｰｲﾝﾃﾘｼﾞｪﾝｽ対策のための不正ﾌﾟﾛｸﾞﾗﾑ対策協議会）

  不正プログラムや脆弱性に関する情報をウイルス対策ソフト開発企業等に提供し、社会全体の情報セキュリティを向上

警察庁・都道府県警察

サイバーフォースセンター

- 攻撃の発生状況や手口に関する情報収集・分析
- 外国治安情報機関等との緊密な情報交換
- 攻撃事案の実態解明、厳正な取締り

緊密に連携

関係機関

- **関係省庁との連携**
  （情報セキュリティ政策会議等）

  官房長官が議長を務める会議において、政府と企業等との連絡・連携の在り方等について検討

- **衆議院・参議院事務局等との連携**
  （衆議院ｻｰﾊﾞ等ｳｲﾙｽ感染防止対策本部）
  （参議院サイバー攻撃対策本部）

  衆議院・参議院事務局がそれぞれ対策本部を設置し、事実関係を調査。警察庁もオブザーバーとして積極的に参画。

警察のサイバーテロ対策

サイバーテロの未然防止

◆ サイバーテロの予兆の把握
- サイバー攻撃の自動検知
- 海外治安情報機関との情報交換

◆ 重要インフラ事業者等の管理者対策
- 個別訪問の実施
- サイバーテロ対策協議会の設立

サイバーテロ対策協議会

事案対処能力の向上

◆ 訓練の実施
- 重要インフラ事業者等との共同訓練の実施

◆ 装備資機材の整備

重要インフラ事業者等との共同訓練

サイバーテロの脅威

重要インフラ事業者等の基幹システムに対してサイバー攻撃が行われた場合、**国民生活や社会経済活動に甚大な支障**が生じるおそれがある。

重要インフラ事業者等（10分野）

①情報通信　②金融　③航空　④鉄道
⑤電力　⑥ガス　⑦政府・行政サービス
⑧医療　⑨水道　⑩物流