平成２３年１０月

警　　察　　庁

三菱重工業(株)における不正プログラム感染事案について

１　事案の概要

三菱重工業(株)では、本年８月中旬に同社サーバが不正プログラムに感染している可能性を認知し、詳細調査した結果、本社を含む複数の事業所のサーバやパソコンが不正プログラムに感染していることが判明したもの。

２　捜査

本年９月３０日、警視庁において、三菱重工業(株)から被害届を受理し、現在、捜査中。

３　サイバー攻撃への対処

サイバー攻撃への対処は、国家の安全保障、危機管理上重要な課題であり、警察としては、今回の事案も踏まえ、未然防止の取組を一層推進するとともに、内閣官房等の関係省庁や海外治安情報機関等とも連携し、実態解明及び厳正な取締りを推進してまいる所存。

平成２３年１０月
警　　察　　庁

警察のサイバーインテリジェンス対策

１　情勢

政府機関や先端技術保有企業に対し、標的型メール等によるサイバー攻撃が続発している。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が現実のものとなっている。

２　対策

(1)　警察の取組

警察庁のサイバーフォースセンターは、サイバー攻撃の発生状況や手口に関する情報収集や分析を実施し、被害の未然防止対策に活用している。

また、外国治安情報機関等との間で緊密に情報交換を実施するとともに、サイバー攻撃事案の実態解明や取締りを推進しているところ。

(2)　官民の連携

○　サイバーインテリジェンス情報共有ネットワーク

情報窃取の標的となるおそれのある全国約4,000の事業者等からサイバー攻撃事案に関する情報を集約するとともに、その分析結果を事業者等に提供して注意を喚起している。

○　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

ウイルス対策ソフト提供事業者等に対し、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、社会全体における情報セキュリティの向上を図っている。

(3)　関係機関との連携

○　情報セキュリティ政策会議（議長：官房長官）の下、内閣官房情報セキュリティセンター（ＮＩＳＣ）を始めとする関係省庁との間で、官民連携の強化のための検討を実施。

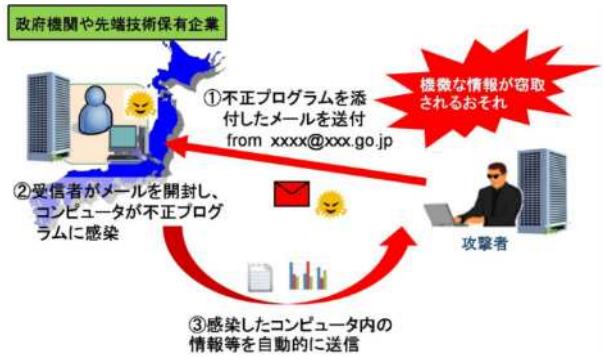
○　衆議院サーバ等ウイルス感染防止対策本部における事実関係の調査や情報セキュリティ対策の検討に対し、警察庁もオブザーバーとして参画。

警察のサイバーインテリジェンス対策

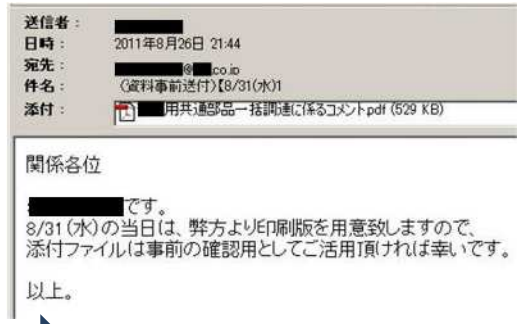
情　勢

● 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

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

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

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

- 衆議院事務局との連携
  （衆議院ｻｰﾊﾞ等ｳｲﾙｽ感染防止対策本部）

  衆議院事務局が対策本部を設置し、事実関係を調査。警察庁もオブザーバーとして対策本部の検討に積極的に参画。