

サイバーインテリジェンスに係る最近の情勢 (平成 23 年 4 月～ 9 月)

1 標的型メール攻撃事案の把握状況

平成 23 年 4 月から 9 月までの間に、震災や原発事故に関する情報の提供を装った標的型メールが我が国の民間企業等に合計約 540 件送付されていたことを把握。また、震災と関連のない標的型メールも合計約 350 件送付されていたことを把握。

2 事業者等におけるサイバーインテリジェンス対策の状況

「サイバーインテリジェンス情報共有ネットワーク」を構成する約 4,000 の事業者等に対し、対策の実施状況について聴取した結果は以下のとおり。

ウイルス対策ソフトは同ネットワークを構成する全ての事業者等が導入しており、約 92% の事業者等が週 1 回以上定期的なフルスキャンを実施。

組織内のコンピュータが不正な接続先と通信していないか調査を行うため、全体の約 95% の事業者等が通信状況に関する記録を保存。

標的型メール等のサイバー攻撃に関する職員教育については、全体の約 92% が実施していた一方、不審なメールに関する報告規定があるのは全体の約 16% であった。

3 情報窃取を企図したとみられるサイバー攻撃事案の例

標的型メール攻撃事案の一例を分析した結果、攻撃者は、標的とする事業者に関係する事業者等のうち、情報セキュリティ対策の進んでいない組織のパソコンをのっとり、盗み出したメールの情報を利用して標的型メールを送信していたことが判明。

4 警察のサイバーインテリジェンス対策の取組

警察では、本ネットワークの更なる拡大を図るとともに、サイバー攻撃に係る実態解明を推進し、更なる情報の集約を図る。

また、関係省庁と連携し、より実効性の高い情報共有に取り組むとともに、本ネットワークの構成員に対して対策の実施状況を踏まえた助言を行うほか、関係する社団法人や事業者等に対しても、セキュリティの向上についての働き掛けを実施。