広　報　資　料

平成 24 年 3 月 1 日
警備企画課・情報技術解析課

サイバーインテリジェンスに係る最近の情勢

1　標的型メール攻撃事案の把握状況

警察では、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ものを始めとする標的型メールが我が国に合計 891 件送付されていたことを把握していたところであるが、10 月から 12 月までの３ヶ月間では、合計 161 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。

2　事業者等における新たな対策の状況

「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、防衛産業関連事業者等に対する標的型メール攻撃事案の顕在化を受け、新たに講じた対策の実施状況について聴取した結果、全職員に対し、標的型メール攻撃に関する注意喚起を実施するなど、全体の約 90%の事業者等が新たな対策を講じたと回答した。

3　情報窃取を企図したとみられるサイバー攻撃事案に係る分析

平成 23 年中に警察で分析した標的型メール攻撃に使用された不正プログラムはほぼ全て、感染するとコンピュータが外部への接続を行うものであった。接続先は、約 23%が中国、約 18%が米国、約 14%が韓国であり、外部への接続を行う際、IP アドレスやコンピュータ名等の情報システムに関する情報を送信するものも確認している。

また、攻撃者は、標的型メール攻撃により特定の端末に不正侵入が可能となった後、当該端末と同一のネットワーク内で稼働する ID・パスワードを管理するサーバへの不正侵入を行う例があったことから、不正侵入の拡大を防止するためには、ID・パスワードを管理するサーバの管理者権限を厳重に管理することが重要である。

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、平成 23 年８月に情報窃取の標的となるおそれのある全国約 4,000 の事業者等と構築した「サイバーインテリジェンス情報共有ネットワーク」を順次拡大しており、平成 24 年１月１日現在約 4,300 の事業者等が参画。また、内閣官房を始めとする関係省庁と連携し、今後、政府機関に対する標的型メール攻撃に関する情報と本ネットワークを通じて得られた情報を関係者の了解を得た上で共有するなど、更なる情報の集約を図る。