Information-technology Promotion Agency, Japan

プレスリリース
2012 年 1 月 20 日
独立行政法人情報処理推進機構

標的型サイバー攻撃の事例分析と対策レポートを公開

～攻撃の流れを把握し、複数の視点から総合的な対策を～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、標的型サイバー攻撃 (*1) に関する事例を分析し、攻撃に対応する上での課題の考察と総合的な対策をまとめた「標的型サイバー攻撃の事例分析と対策レポート」を、1 月 20 日（金）から IPA のウェブサイトで公開しました。
URL：http://www.ipa.go.jp/security/fy23/reports/measures/index.html

2011 年は、国内の大手重工メーカーや衆議院・参議院が情報窃取型の標的型サイバー攻撃を受け、社会の関心を集めました。これらの攻撃では、標的型攻撃メールにより送付されたコンピューターウイルスがシステム内部に侵入し、スパイ活動をすることで、システム内部の組織情報や個人情報が抜き取られました。
IPA は、このような被害の大きい標的型サイバー攻撃について典型的な事例を分析し、標的型攻撃に対応する上での課題の考察や、総合的な対策をレポートとしてまとめました。

このような標的型サイバー攻撃では、特定の情報窃取を目的として、同業種や業界に狙いを定め巧みで執拗（しつよう）な攻撃が行われることが想定されます。そのようなケースでは、ある組織が検知した攻撃情報を迅速に共有することで、全体の被害の低減や早期の対応を実現することが可能であると考えられます。
それを実現する仕組みとして、2011 年 10 月 25 日に経済産業省の主導の下にサイバー情報共有イニシアティブ（J-CSIP (*2)）が発足しました。IPA は情報ハブ（集約点）の機能を担い、重工業 9 社の間で情報共有を実施する試みを進めており、本レポートの中でその概要を紹介しています。

＜対策レポートのポイント＞

2011 年に大手重工メーカーに対して行われた攻撃の事例分析と考察を概説しているほか、標的型サイバー攻撃の流れと課題を整理し、総合的なセキュリティ対策について解説しています。このような攻撃を防ぐためには、事前対応、早期警戒、攻撃を受けた際の検知と防御、最終被害の回避、それぞれが重要となります。本レポートの中では早期警戒の新たな取組みとして、業界内でサイバー攻撃情報を共有する取組み（J-CSIP）を紹介しています。また、事前対応に活用できるコンテンツとして、攻撃対象となる主要なソフトウェアの更新状況を一括チェックできる「MyJVN バージョンチェッカ」および注意喚起情報をリアルタイムに配信する「icat」を、最終被害の回避を目的として「出口対策」を紹介しています。

本レポートによる事例紹介を機に、標的型サイバー攻撃に対する理解が深まり、また「MyJVN バージョンチェッカ」、「icat」、「出口対策」等の活用が促進され、標的型サイバー攻撃の被害の回避・低減に資することを期待します。

■本件に関するお問い合わせ先
IPA　技術本部　セキュリティセンター　金野／相馬／入澤
Tel: 03-5978-7527　Fax: 03-5978-7518　E-mail: vuln-inq@ipa.go.jp
■報道関係からのお問い合わせ先
IPA　戦略企画部　広報グループ　横山／大海
Tel: 03-5978-7503　Fax: 03-5978-7510　E-mail: pr-inq@ipa.go.jp

(*1) ここでは、特定の組織・個人に対してインターネット経由で情報窃取やサービス妨害などを行なう攻撃。
(*2) Initiative for Cyber Security Information sharing Partnership of Japan。「早期警戒のための情報共有による攻撃の検知と回避」、「標的型サイバー攻撃の実体調査と共有情報による早期対策の推進」を目的としている。
http://www.ipa.go.jp/security/J-CSIP/index.html