IPA Technical Watch

2010 年 12 月 17 日
独立行政法人情報処理推進機構

IPA テクニカルウォッチ：『新しいタイプの攻撃』に関するレポート

～Stuxnet（スタックスネット）をはじめとした新しいサイバー攻撃手法の出現～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、2010 年春ごろから海外を中心に発生している社会インフラをターゲットとした攻撃に関して、国内の実情に応じた影響・脅威を分析し、課題および対策方法を含めて、技術レポート（IPA テクニカルウォッチ 第 1 回）として公開しました。

昨今、海外で APT（Advanced Persistent Threats）と呼ばれる、ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組合せ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗なサイバー攻撃が発生しています。このような攻撃は、システムへの潜入等の「共通攻撃手法」と、情報窃取等の目標に応じた「個別攻撃手法」の、2 種類の手法で構成されています。IPA では、このように「共通攻撃手法」と「個別攻撃手法」を組み合わせた攻撃を『新しいタイプの攻撃』と呼称します。

IPA では、この『新しいタイプの攻撃』の一種であり、本年 7 月に世界中で話題となったコンピュータウイルス Stuxnet[1]を解析し、その結果を踏まえ本年 12 月に発足した「脅威と対策研究会[2]」にて、『新しいタイプの攻撃』が日本の社会インフラに与える影響について分析しました。

『新しいタイプの攻撃』では、「個別攻撃手法」の対象を変化させることで、幅広い各種システムが攻撃対象となりますが、その特性から、設定された対象以外のシステムについては影響が限定的となります。

例えば、Stuxnet の例においては、ネットワーク構成の違いや、攻撃対象となった制御システムの製品ベンダーの違いによって、日本の社会インフラへ影響を与える可能性は低いものとなっています。

ただし、いつ「個別攻撃手法」の対象を日本の社会インフラに設定されるかは分かりません。そのため、攻撃の前段階である「共通攻撃手法」への対策を日常的に行う必要があります。

ところが「共通攻撃手法」は、複数の攻撃の組合せや対策が行えない未知の脆弱性（ゼロデイ攻撃）が利用されており、既存のセキュリティ製品を導入した対策には限界があります。

IPA では、分析で得られた上記の事実から、『新しいタイプの攻撃』に対する対策として、「共通攻撃手法」から「個別攻撃手法」に移行する前にネットワークを介した動きを封じることで、攻撃を停止できることを確認し、システム・ネットワーク設計における 6 つの対策を提案しています。

■ 本件に関するお問い合わせ先
IPA セキュリティセンター　小林／中野／大森
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] 2010 年 7 月に発見された、制御システムを標的としたコンピュータウイルスの一種。
[2] 大学研究機関、セキュリティベンダー、システムベンダーなどからなる約 20 組織、約 30 名で構成する研究会。
目的は「知見の集約の場」。特定の組織に特化した攻撃については、汎用的なサイバーセキュリティ技術と、その組織に特化した対策技術が必要であることから、攻撃に応じた連携としての位置づけを高めていく。