Information-technology Promotion Agency, Japan

プレスリリース
2011 年 10 月 18 日
独立行政法人情報処理推進機構

脅威を増す標的型のサイバー攻撃に関する注意喚起

～セキュリティ対応状況の確認と対策の徹底を～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、組織における機密情報や個人情報を狙ったサイバー攻撃事件の増加、更に国内基幹産業への標的型攻撃メールによるウイルス感染事件とその脅威の拡がりを受け、組織におけるセキュリティ対応状況の確認と対策の徹底を再度呼びかけます。
URL：http://www.ipa.go.jp/security/topics/alert20111018.html

昨年発覚した Stuxnet [(*1)] による攻撃に続いて、今年に入って海外では、航空機メーカーへの攻撃やインターネットを介した大量の個人情報漏えい事件などが発生し、9 月 19 日には、国内で、大手総合重機メーカーへのサイバー攻撃事件が報道されました。

このような事態を受け、IPA では、脅威を増す「新しいタイプの攻撃」への対策 [(*2)] や、標的型攻撃メールの分析と対策 [(*3)] を公開してきました。

10 月 15 日には、今回の大手総合重機メーカーの事件は防衛関連産業界を狙った標的型の攻撃であったという報道がありました。初めに業界団体に侵入（感染）し、その団体のメールを窃取、そのメールを悪用してウイルスファイルを傘下の事業者に送りつけ、目的の事業者への侵入を図っていたということです。従って、自組織のセキュリティ面で弱い所をいかに無くすかが、一組織だけでなく、業界としての喫緊の課題となっています。また、攻撃の情報を業界として共有することが、攻撃の回避や拡大防止に重要となります。

組織のシステム管理者は、下記の対応策および別紙のチェックリストを活用し、日頃からの対策を徹底することが必要です。また、不正アクセスや侵入、ウイルス感染の検知時は、IPA への早急な届出が望まれます [(*4)]。

対応策

組織においては、改めて、セキュリティ対策を検証し、組織システムと情報の保護に向けた継続的な尽力が求められます。対策の基本的な観点は以下のとおりです。この中で【対策 4】は IPA が先日公開したガイドで解説しています [(*2)]。

検討にあたっては、取り扱う組織情報の重要度、機密度を精査し、企業の社会的責任と事業継続性の観点から、相応の対策を選択することが重要となります。また、グループ企業や連携している組織では、統制されたポリシーと対策が必要となります。

【対策 1】：入口（ネットワーク経路）をしっかり守る
【対策 2】：ファイアウォールを抜けてもシステムにつけ入られる隙（脆弱（ぜいじゃく）性）を与えない
【対策 3】：標的型攻撃のルートとなる箇所を防御する
【対策 4】：ウイルスの活動（組織内蔓延（まんえん）や外部通信）を阻害、抑止する＜出口対策＞
【対策 5】：重要な情報はその利用を制限（アクセス制御）する
【対策 6】：情報にアクセスされても保護するための鍵（暗号）をかける
【対策 7】：操作や動き（ログ証跡）を監視・分析し不審な行為を早期に発見する
【対策 8】：万一被害が発生したら早急な対応（ポリシーと体制）をとる

■ 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／金野／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) 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)「新しいタイプの攻撃」の対策に向けた設計・運用ガイド　http://www.ipa.go.jp/security/vuln/newattack.html
(*3)『標的型攻撃メールの分析』に関するレポート　http://www.ipa.go.jp/about/technicalwatch/20111003.html
(*4) 情報セキュリティ安心相談窓口　http://www.ipa.go.jp/security/anshin/