Information-technology Promotion Agency, Japan

プレスリリース
2011 年 9 月 20 日
独立行政法人情報処理推進機構

組織の重要情報の窃取を目的としたサイバー攻撃に関する注意喚起

～組織システムのリスク把握と、日頃からのセキュリティチェックと対策の徹底を～

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正）は、組織における知財や個人情報を狙ったサイバー攻撃事件が目立っており、昨今も攻撃を受けていた事件が報道されたことを受け、組織のシステム管理者に対し、広く対策の徹底を呼びかけるため、注意喚起を発することとしました。

近年、組織の知財情報や個人情報等の窃取を目的とした攻撃が増加しています。サイバー攻撃は、公開されているサーバーへの攻撃だけではなく、特定企業や公的機関を狙い、ソフトウェアの脆弱（ぜいじゃく）性を悪用し、複数の攻撃を組合せ、人間の心理・行動の隙を突く手法を用い、対応が難しいサイバー攻撃（IPA ではこのような攻撃を「新しいタイプの攻撃」(*1) と呼びます）が問題になっています。

「新しいタイプの攻撃」は、端末がウイルスに感染してしまうと、組織内に拡散するだけでなく、攻撃者との通信によるウイルスの機能増強や、組織内の情報探査を行い、それらの情報を攻撃者へ送信したりします。場合によっては、組織の活動に関わる秘密情報や設計図などの知財情報などが攻撃者に窃取されてしまいます。これらの攻撃は、いわゆるインターネットに直接つながっていないシステムに対しても USB メモリー等の外部メディアを通じて行われるものもあります。

このような昨今のサイバー攻撃への対策では、**組織全体のネットワークシステムを把握し、外部からの攻撃を防御する対策だけではなく、たとえ侵入されたとしても組織の情報を窃取されないための対策（出口対策等）、早期発見の備え、事後対応など、トータルなセキュリティ対策で備える**ことが重要です。

組織のネットワーク管理者は、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してください。また、不正アクセスや侵入、ウイルス感染の検知時は、IPA への早急な届出をしてください (*2)。

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をお願いします。対策の基本的な観点は以下のとおりです。この中で【対策 3】は IPA が先日公開したガイドで解説しています (*3)。

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（脆弱性）を与えない
【対策 3】：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 4】：重要な情報はその利用を制限（アクセス制御）する
【対策 5】：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 6】：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 7】：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／相馬
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) 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
http://www.ipa.go.jp/about/technicalwatch/20101217.html
(*2) 情報セキュリティ安心相談窓口　http://www.ipa.go.jp/security/anshin/
(*3)「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

別紙

＜チェックリスト＞

それぞれの関門における多段の防御が有効となります[1)]。それぞれの組織におけるシステムやネットワークにおいて、下記の対策状況をチェックし、不足している部分を改善してください。

1. ネットワークの入口と経路での防御

- □ ファイアウォール
- □ 最新のウイルス対策ソフト　（ネットワーク、サーバー、クライアント）[2)]
- □ 侵入検知システム／防止システム
- □ 通信路の暗号化（Virtual Private Network などの利用）
- □ ネットワーク構造／設計　（重要なサーバーに対するルート制御やネットからの隔離）

2. 脆弱性対策

- □ OS やサーバーソフトウェアの定期的な脆弱性診断
- □ ウェブサイトで使用している OS やサーバーソフトウェアに関する脆弱性情報の、時期を逸しない収集とパッチの反映[3)]
- □ ウェブアプリケーションへの脆弱性の作り込みの回避[4)]
- □ ウェブアプリケーションファイアウォール（WAF）[5)]

3. ウイルス活動の阻害および抑止 (出口対策)[6)]

□ 端末間、他部署間のネットワーク通信の制限（ウイルスの組織内蔓延抑止）

- □ 組織の端末からの外部通信はプロキシを経由させる等の経路制御
- □ 組織内ネットワーク量の監視（異常さを早期に検知しウイルスの蔓延を早期に発見）
- □ 知財等のある重要なサーバーはインターネットから隔離

4. アクセス制御

- □ ユーザ認証
- □ アクセスするプログラムの特定（ホワイトリスト化）

5. 情報の暗号化

- □ 暗号
- □ 暗号鍵管理

6. システム監視、ログ分析

- □ ネットワークログ取得・分析
- □ サーバログ取得・分析
- □ アクセスログの監査（DB 監査ツールなど含む）

7. 管理統制およびコンテンジェンシープラン (事前準備・事後対応)

- □ セキュリティポリシー
- □ 海外を含むグループ会社間でのセキュリティガバナンス
- □ 危機対応体制の整備

【参考資料】

1). 2011年版 10大脅威　http://www.ipa.go.jp/security/vuln/10threats2011.html
2). コンピュータウイルス対策基準　http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm
3). 脆弱性対策情報データベースJVN iPedia　http://jvndb.jvn.jp/
4). 安全なウェブサイトの作り方 / 安全なSQLの呼び出し方
http://www.ipa.go.jp/security/vuln/websecurity.html
5). Web Application Firewall（WAF）読本　http://www.ipa.go.jp/security/vuln/waf.html
ウェブサイト攻撃の検出ツール iLogScanner　http://www.ipa.go.jp/security/vuln/iLogScanner/
6). 「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