[標的型サイバー攻撃の手口と対策] 出典「標的型サイバー攻撃の対策セミナー」(TREND MICRO：平成 28 年 6 月 24 日開催)を編集　　文責：河東岩夫

活動	段階	目的	手口	対策
侵入前	1.偵察	事前準備	攻撃先を決定、初期潜入用不正プログラムを準備する	-
侵入時	2.侵入 感染	初期潜入	メールや Web サイトへのアクセスにより内部ネットワークに侵入、マルウェア等の不正プログラムを端末に感染させる	メールや Web サイト経由で侵入する不審なファイル・通信を検知・防御、マルウェア等の不正プログラムを検知・駆除・隔離する
	3.C&C	端末制御	C&C サーバとの通信を隠蔽・遠隔操作し、感染環境を確認する	C&C サーバとの通信を検知・防御する
内部	4.拡散	情報探索	PC 以外の端末やサーバに正規ツール・コマンドの使用により拡散し、LAN 内情報を探索する	感染端末から内部サーバや端末に感染拡大を行う通信を検知・防御する
	5.収集	情報集約	感染した端末やサーバの重要情報(社員・顧客・取引先・業務関連情報等)を収集する	感染した端末内での情報収集の行動を検知する
最終	6.奪取	情報送出	収集した重要情報を奪取し、イベントログやファイル等の潜入痕跡を消去する	ファイルを不正に外部に送信する通信を検知・防御する

注)

標的型サイバー攻撃の多くはメール攻撃(93%)や水飲み場型の改ざんされた Web サイト(7%)を通じて不正プログラムを企業に侵入させる。被害企業(90%)が侵入 5 カ月後に外部の指摘で攻撃に初めて気付く(同一攻撃者の 31 カ月間に及んだ攻撃もある)と言われている。それ故にメールや Web の入口・出口対策に注力しても脅威は排除できない。そのために「脅威の侵入ありき」の前提で多層に対策・防御を行い、内部ネットワーク全体を可視化し、不審な動きを早期にあぶり出すことがポイントであり、上記の対策に対応する以下の事例のような機能の具備が必要である。

①標的型攻撃やランサムといった攻撃を検知する機能

②脅威を継続的に検知する機能

③大量のログから危険な兆候を検知する機能

④各種のログの相関関係を把握し、相関分析を行う機能

⑤サンドボックス等の仮想環境での動的解析を行う機能

又、攻撃された場合に備えて以下の URL に記載する CSIRT 事例(出典：日本シーサート協議会)のような社内体制(平時・有事)の整備が必要である。

http://internet.watch.impress.co.jp/docs/news/745804.html