別紙

**＜共通攻撃手法と個別攻撃手法の流れ＞**

■　共通攻撃手法

①　インターネットや USB メモリを通じた情報システムへのウイルス感染

②　システムの脆弱性を利用することによる情報システム環境内部でウイルスの拡散

③　バックドアを作成し、外部の指令サーバ（C&C サーバ）と通信することにより、ウイルスの増強や新たなウイルスのダウンロードの実行

※ウイルスの増強やダウンロードは以降④⑤の手順でも実行される可能性あり。

■　個別攻撃手法：Stuxnet の場合

④　原子力システム等を制御する装置が配備してある、制御システムへの侵入

⑤　制御システム上にある装置に対する攻撃の実行

**＜『新しいタイプの攻撃』イメージ＞**

『新しいタイプの攻撃』をロケットの例で考えてみると、下記の図のように特定のシステムへの攻撃に特化した（個別攻撃手法）**ペイロード部**と特定のシステムに侵入する為の共通仕様部分（共通攻撃手法）の**ランチャー部**に分けることができる。一連の攻撃の流れで考えると、ペイロード部とランチャー部からなるロケットが、システムに侵入し、ペイロード部で特定のシステムに攻撃を加える。即ち、実際に目的を達成するためのペイロード部を積んだロケットが目的地に向けて、発射される形となる。

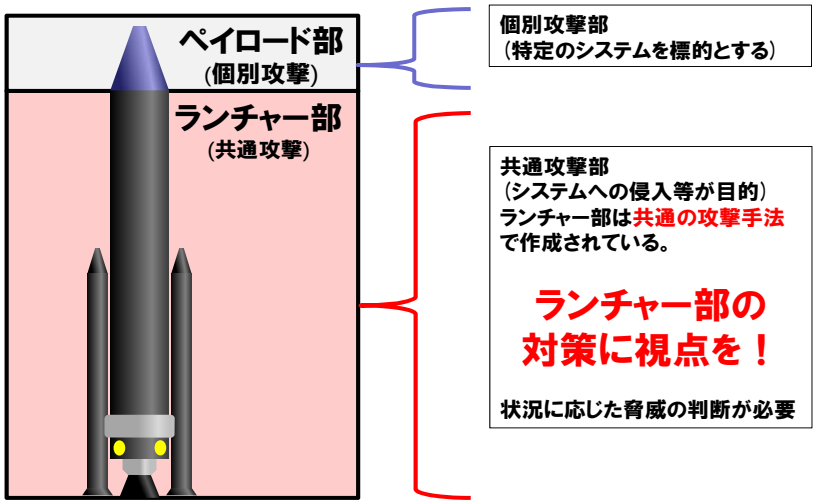


図１　ロケットを例にした『新しいタイプの攻撃』のイメージ

＜システム・ネットワーク設計における６つの推奨対策＞

表１　システム・ネットワーク設計対策要件

| No | 機能要件項目 | 機能要件内容 | 要件理由及び背景 | 設計事例 |
|---|---|---|---|---|
| 1 | プロキシの認証情報のチェック | 一般 PC の外部 Web アクセス時、認証プロキシによる認証アクセスを設計。 | ウイルスが、独自の通信メソッドを用いて搾取した情報を悪性サイトに送信する場合、認証情報を使用しない場合が多いことが確認されている。<br>※ウイルスが既認証状態を使用した攻撃仕様となった場合は、防止出来ない。 | ・認証プロキシ |
| 2 | HTTP,SSL 通信のヘッダーチェック | 外部通信（GET,POST コマンドのヘッダー等通信内容）の検出･遮断。 | ウイルスが窃取した情報を外部の悪性サイトに送付する場合、新たな攻撃コードをダウンロードする場合、C&C サーバからの指示を受信する場合に多くは 80/tcp,443/tcp が用いられる。 | ・NOC/SOC 監視 |
| 3 | 未知のウイルスを検出可能なソフトウェアの導入 | ゼロデイ脆弱性含む、ウイルスが脆弱性を使用した時の挙動検知。 | PC 上のウイルスの脆弱性利用等の挙動などから攻撃動作を検出することにより、未知ウイルスや、未知の脆弱性を突く「ゼロデイ攻撃」を検出し防御することが可能な製品が複数の企業から発表されてきている。<br>・ただし、従来のウイルス対策ソフトを補完するものとして、防御機能、管理工数等十分な評価の上で設計利用検討の可能性がある。 | ・振舞い検知タイプのウイルス対策ソフトの導入 |
| 4 | スイッチ等での VLAN ネットワーク分離設計 | ルータ、スイッチによる必要なアクセス範囲に限定した、VLAN 及びルーティング設定。<br>特に、管理系端末 LAN の分離設計。 | システムへの影響を最小化するため、攻撃時の影響範囲をネットワーク設計上分離できるようにする。<br>・Conficker、Stuxnet 事案等対処事例 | ・ネットワーク設計<br>・ルータ、スイッチの VLAN 設定 |
| 5 | 最重要部のインターネット直接接続の分離設計 | 最重要部の通常サービス（http,ssl）に関するインターネット直接接続を分離設計し、外部からの制御シーケンスの影響を回避する。 | 外部からの制御シーケンスは、http,ssl 等の通常通信を多用する。<br>USB 等を介し、最重要部にウイルスが侵入した場合でも、インターネットを介した環境等攻撃分析情報の搾取、攻撃ウイルス更新、攻撃指示の影響を回避する。 | ・ネットワーク設計 |
| 6 | システム内 P2P 通信の遮断と検知 | VLAN 設定において、P2P 通信の到達範囲を限定する。 | 外部のダウンロードサーバからアップデートされるウイルスは、外部接続可能な P2P 用に仕立てた内部 PC を経由して、内部システムに存在するウイルスの一斉バージョンアップやリモートコントロールを行う。 | ・ネットワーク設計 |