MITSUBISHI ELECTRIC
Changes for the Better

NEWS RELEASE

（開発 No.1615）

2016 年 2 月 17 日
三菱電機株式会社

数億種類のウイルスの活動を50個程度の「攻撃手口」に分類・検知し、情報流出を阻止

「サイバー攻撃検知技術」を開発

三菱電機株式会社は、一日あたり 100 万種以上増える※1 といわれる数億種類のウイルスの活動を、わずか 50 個程度※2 の攻撃手口に分類して検知する「サイバー攻撃検知技術」を開発しました。従来、種類が多く見逃していたサイバー攻撃を未然に検知することで、情報流出などの被害防止に貢献します。

※1　出典：シマンテック社「2015 年インターネットセキュリティ脅威レポート」
※2　2016 年 2 月 17 日現在

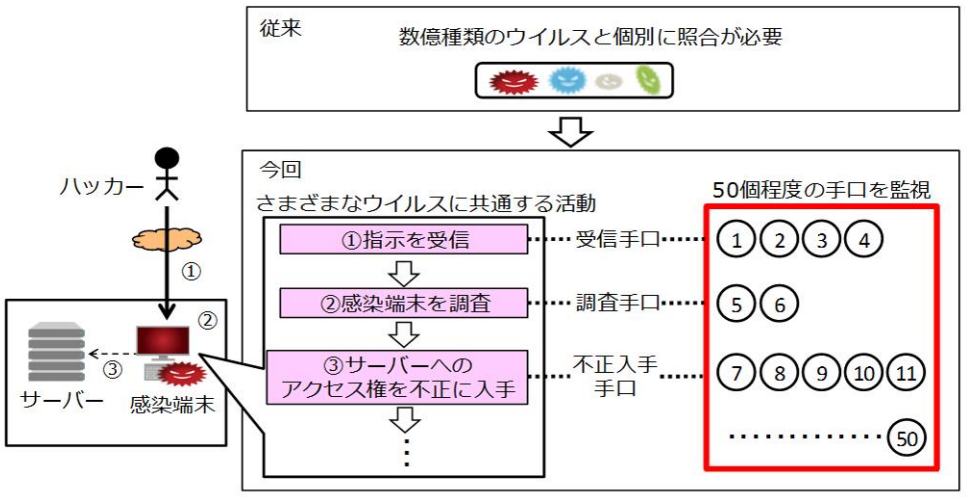

図 1.　攻撃手口を監視

開発の特長

1. ウイルスの攻撃手口を50個程度に分類・監視・検知し、情報流出を阻止
   - ハッカーが目的達成のために必ず実施する攻撃手口を 50 個程度に分類
   - 50 個程度の攻撃手口を監視し、感染したウイルスを検知することで情報流出を阻止

2. 攻撃シナリオを活用して、高精度にサイバー攻撃を検知
   - 検知した攻撃手口が、想定される攻撃シナリオに沿ったものかを相関分析でチェック
   - 攻撃手口と類似した正規ユーザーの活動を、攻撃シナリオに沿っていなければ正規ユーザーであると識別することにより、攻撃検知の高精度化を実現

開発の概要

	機能
今回	・ハッカーが必ず行う攻撃手口を 50 個程度に分類・監視・検知 ・攻撃シナリオを活用した相関分析により、サイバー攻撃を高精度に検知
従来	・サイバー攻撃に使われる数億のウイルスの種類をひとつひとつ見分けて検知

報道関係からのお問い合わせ先	〒100-8310 東京都千代田区丸の内二丁目 7 番 3 号　TEL 03-3218-2359　FAX 03-3218-2431 三菱電機株式会社　広報部

開発の背景

ネットワークを経由したサイバー攻撃により、企業の情報が流出する問題が深刻化しており、政府も対策を図るなど検知・防御強化に向けた動きが加速しています。

一方、1 日当たり 100 万種以上の新しいウイルスが登場※1 するといわれており、膨大な種類のウイルスをひとつひとつ見分ける従来のウイルス検知方法では感染を完全に阻止することは非常に困難であるため、ウイルスへの感染を前提として、情報流出自体は阻止することがセキュリティー業界の共通認識となっています。

当社は今回、ウイルスを操るハッカーの攻撃手法を分析し、情報窃取などの目的達成のために必ず実施される手口がわずか 50 個程度に集約されることに着目しました。これにより、ウイルスの検知を容易にし、情報流出を防ぐことができる「サイバー攻撃検知技術」を開発しました。

特長の詳細

1. ウイルスの攻撃手口を 50 個程度に分類・監視・検知し、情報流出を阻止

   サイバー攻撃におけるウイルスの活動は、攻撃対象の端末に感染し、ハッカーから指示を受信し、感染端末を調査し、さらに活動を広げるため不正にアクセス権を入手するという段階を踏みます。例えば、感染端末を調査する活動段階では、感染端末に保存されているドキュメントの検索、通信ルートの確認、セキュリティー対策設定の確認という攻撃手口により、何をどのように盗み出すかを決定します。

   当社は今回、ウイルスに共通の攻撃手口を活動全体でわずか 50 個程度に分類し、それぞれをログ分析で検知する分析ルールを定義化しました。それに基づきウイルスを監視・検出することでサイバー攻撃を防止します。

   また、この共通の攻撃手口は、1 年で十数件※3 しか増えません。新しい攻撃手口が 1 つ確認された段階で分析ルールを追加することで、この 1 つの攻撃手口を使う膨大な数のウイルスによるサイバー攻撃を検知できます。

   ※3　2013 年以降の 1 年間における増分

2. 攻撃シナリオを活用して、高精度にサイバー攻撃を検知

   これまで、正規のユーザーが行う攻撃手口と類似した活動が、攻撃ではないことを判断することも課題でした。そこで、この攻撃手口をいくつか連続させたサイバー攻撃シナリオを定義し、攻撃手口が、攻撃シナリオに沿って発生しているかをチェックする相関分析によって、攻撃手口に類似した正規ユーザーの活動とサイバー攻撃とを識別します（図 2）。

   ひとつの活動だけではなく、その活動の前後に何をしていたかも含めて判断することで、ハッカーの活動とハッカーではない正規ユーザーの活動を高精度に識別します。

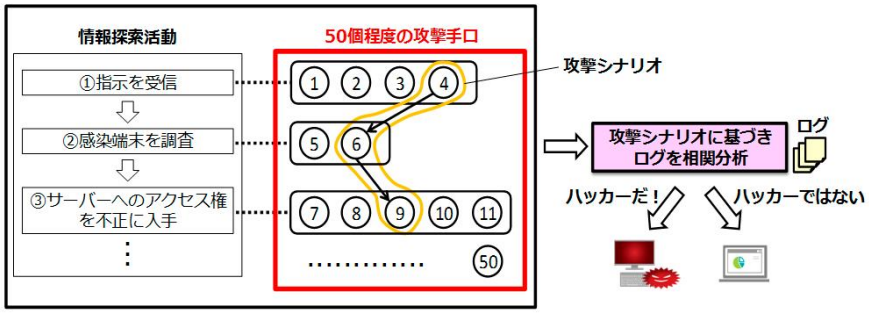

図 2.　攻撃シナリオに基づくサイバー攻撃検知

特許

国内 6 件、海外 6 件

開発担当研究所

三菱電機株式会社　情報技術総合研究所
〒247-8501　神奈川県鎌倉市大船五丁目 1 番 1 号
FAX 0467-41-2142
http://www.MitsubishiElectric.co.jp/corporate/randd/inquiry/index_it.html