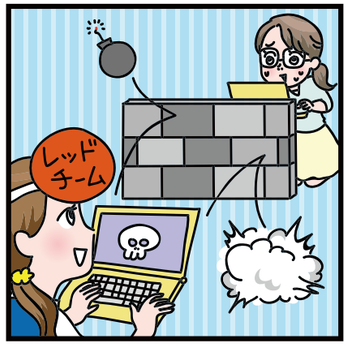
擬似マルウェアを使った攻撃で、第三者評価を実施



日立ソリューションズでは、セキュリティのエキスパートで構成されたレッドチームにより、擬似マルウェアを使って実際の標的型攻撃を再現する、「標的型攻撃対策評価サービス」を提供しています。

IPAが発行する「『高度標的型攻撃』対策に向けたシステム設計ガイド」で定義されている攻撃シナリオにもとづき、特に入口対策以降の技術的な対策を評価する擬似攻撃を実施します。

たとえば、不正URLからマルウェアをダウンロードした想定で、擬似マルウェアがバックドアを設置できるか、感染端末の情報を収集できるか、感染を広げるためのポートスキャンや、共有フォルダへの不正ファイルのアップロードができるか、マルウェアが取得した情報を社外のC&Cサーバにアップロードできるかといった攻撃を行い、各時点でのログを調査・確認。各攻撃フェーズにおいて検知や対策が有効に働いているかを評価します。

また、その結果に基づき、どのような対策が必要であるかをまとめた「セキュリティリスク評価報告書」を提示・納品します。

このように、日立ソリューションズが実際の標的型攻撃と同様の攻撃を行うことで、自社ネットワークにおける標的型攻撃対策の第三者評価を行うことができます。

セキュリティ対策に頭を悩ませている管理者の方々を トータルでサポートいたします。

情報資産を守るには、さまざまな「道（手段、方法）」があります。
日立ソリューションズは、セキュリティ対策のガイド役として、
お客さまに最適な「道」をご提案。
日々、高度化、巧妙化するさまざまな脅威から企業を守る、
確かなセキュリティ対策を提供します。

いま、本当に必要な情報セキュリティ対策をガイドする

トータルセキュリティソリューション

トータルセキュリティソリューション　検索

http://www.hitachi-solutions.co.jp/security/sp/

※本カタログ中の会社名、商品名は各社の商標、または登録商標です。
※本文中および図中では、TMマーク、®マークは表記しておりません。
※製品の仕様は、改良のため、予告なく変更する場合があります。
※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。
なお、ご不明な場合は、当社担当営業にお問い合わせください。
※本カタログ中の情報は、カタログ作成時点のものです。

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/column/kaiketsu/vol22/

S17S-13-01　2017.12

HITACHI
Inspire the Next

ITのお悩みをソリュっと解決！
特命課ソリュートくんがいく！

今のままで大丈夫!? 標的型攻撃対策評価サービスで 自社セキュリティの見直しを!

プロローグ

都内某所にある日立ソリューションズのビルの一室に古くから存在しているが誰にも知られていない特命課が存在する。
ソリュートくんのアンテナにキャッチされるさまざまなITのお悩みを特命課社員、甲斐結子とソリュートくんの二人で日々解決していく!

*詳しくは『99%以上の検知率!! CylancePROTECTで既知・未知の区別なくマルウェアを捕まえろ!』の巻をご覧ください

甲斐 結子（かい ゆいこ）

3年前なぜか特命課に配属されソリュートくんに振り回されていた日々だったが人々の課題を解決していくうちに仕事にやりがいを見出していくオペレーター。

生真面目な性格のため、ソリュートくんの言動や行動には少し頭を悩ませている。

登場人物

名屋見紫野美（なやみ しのみ）さん

情報システム部のキャリアを積み、将来はECサイトを立ち上げて独立をめざしている。そのステップとして前より規模は小さくても全体の業務に携われる会社に転職したものの、社長に振り回されがちになっている。

ソリュートくん

身長はアポストロフィ1.5個分だが通常時は40cm程度。アンテナを頼りに日々課題解決に燃えている。課題を持った人をみつけると興奮して早口になってしまうことがタマに傷。

結子の事をからかうのが日々の楽しみ。

株式会社 日立ソリューションズ

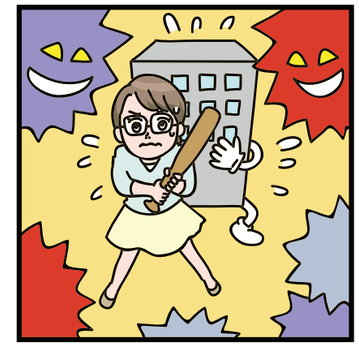
今のままで大丈夫!? 標的型攻撃対策評価サービスで
自社セキュリティの見直しを!

ソリューションと解決！

日立ソリューションズがセキュリティをトータルでサポート

日立ソリューションズではサイバー攻撃対策のPDCAサイクルにもとづき、コンサルテーションからシステム構築、運用支援までの幅広いメニューを用意しております。特定の製品によらず、お客さまによりよい製品・解決策を提案し、新たなサイバー攻撃にも対応できるソリューションを提供いたします。

その標的型攻撃対策、本当に大丈夫ですか?



重大な情報漏洩にもつながりかねない「標的型攻撃」の被害は後を絶ちません。2017年1月にIPA（独立行政法人情報処理推進機構）より発表された「情報セキュリティ10大脅威2017」でも、「標的型攻撃による情報流出」が1位となっていました。

一方で、ここ数年の標的型攻撃に対するリスク啓発もあり、多くの企業で、多層防御やユーザー教育など、標的型攻撃に有効とされるセキュリティ対策に取り組むようになってきています。

しかし、攻撃者も手を緩めることなく、続々と新しい手法を編み出し、攻撃を行っています。そのため、導入したセキュリティ対策も定期的に見直さなければ、新たな攻撃に対応できない可能性も出てきます。

日立ソリューションズでは、セキュリティのプロが、擬似的な標的型攻撃を実際のお客さまネットワークに行い、どれほど対応できるのかを診断・評価する「標的型攻撃対策評価サービス」を提供しています。実際の標的型攻撃を再現し、評価することで、お客さまの対策状況を把握し、改善につながる支援をしています。

ますます巧妙化が進む標的型攻撃

警察庁が2017年3月に発表した「平成28年中におけるサイバー空間をめぐる脅威の情勢等について」においても、標的型メールによる攻撃が過去3年連続で増加していると報告されています。その攻撃手法はますます巧妙化し、インターネット上には公開されていないメールアドレス宛の標的型メールが84%を占め、送信元アドレスが偽装されるなど、攻撃者の用意周到さが伺われる状況です。

また、標的型攻撃対策が進む中で、2016年にはこれまでほとんど報告のなかった「.js」形式ファイルが添付されたメールが急増するなど、次々と対策の盲点をつく攻撃が行われています。

標的型攻撃対策には現状把握が不可欠

このように増加する標的型攻撃に対し、各企業も、入口・出口・内部対策による多層防御に加え、怪しい添付ファイルやURLにアクセスをしないといったユーザー教育での対策を進めています。

しかしながら続々と新しい手法を繰り出してくる攻撃者に対抗するには、継続的に対策を見直すことが必要です。

そのためには、自社のネットワークが標的型攻撃に対して、どの程度検出や遮断といった対応ができるのか、現状を把握し、必要に応じて改善していくことが重要となります。

そこで効果的なのが、実際のネットワークに擬似的な標的型攻撃を実施して評価する手法です。