「CylanceOPTICS」は端末上の疑わしい振る舞いからサイバー攻撃の予兆を検知し、マルウェアの動作を阻止、侵入経路の把握など、マルウェアによるダメージを最小限に抑えます。「CylancePROTECT」の検知技術を応用し、従来型のマルウェア対策製品では検知が難しい、WindowsのPowerShellスクリプトを悪用したファイルレス攻撃などをリアルタイムで検知し、プロセスを停止。潜伏しているランサムウェアの確認や、検知した端末のネットワークからの切り離し、そしてマルウェアの侵入経路を把握して、再発防止に役立てることができる機能などを持っています。

「CylancePROTECT」と「CylanceOPTICS」を併用することで、より高精度なマルウェア検知を実現するだけでなく、共通のコンソールで運用できるため、管理者の負担も大幅に軽減します。

メーカーとの密接な連携による日立ソリューションズの高いサポート力

Cylance社が日本に初めて進出した2016年4月から、日立ソリューションズはCylance製品を取り扱い、さまざまな業種で多くのお客さまに導入いただいています。

Cylance社とは定例のミーティングで機能リクエストなどをフィードバック。ロードマップや新技術の情報もいち早く共有し、協調体制を組んでいます。

また、保守ではWebにて24時間受付の対応や、技術情報の配信、技術資料の提供などの手厚いサポートを実現しています。その結果、お客さまへのサポート力が高く、顧客満足に寄与したことを評価され、2016年、2017年と2年連続でCylance社より「Japan Excellence Support Partner of the Year」を受賞しています。

エンドポイントのマルウェア対策ソリューションとして必要十分な機能を持つ「CylancePROTECT」と「CylanceOPTICS」のコンビネーション。企業が直面するセキュリティリスクを低減する強力な味方として、導入を検討してみてはいかがでしょうか。

未知のマルウェアからエンドポイントを守るために。まずはお気軽にご相談ください。

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/shion/vol4/

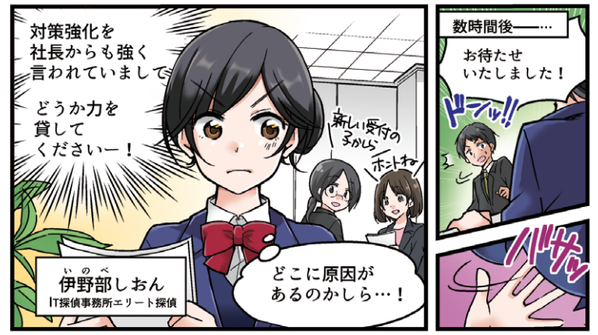
C18K-05-02 | 2019.05

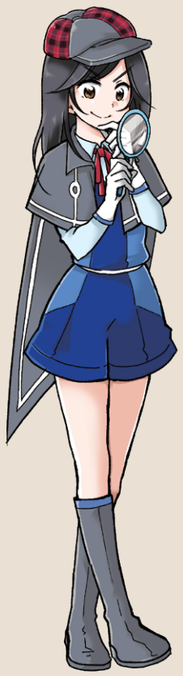
HITACHI
Inspire the Next

経営をも脅かすサイバー攻撃。十分な事前・事後対策を

プロローグ

都内某所に、ITを駆使して企業の悩みを解決するという、特別な探偵事務所がある。そこで働くエリートIT探偵の「伊野部しおん」は、企業が悩むセキュリティや業務効率化の課題を次々と調査・解決していく。





登場人物

前後 泰作（ぜんご たいさく）

□□商社、情報システム部部長。マルウェア感染の対応に追われており、今後の対策強化をどうするか悩んでいる。

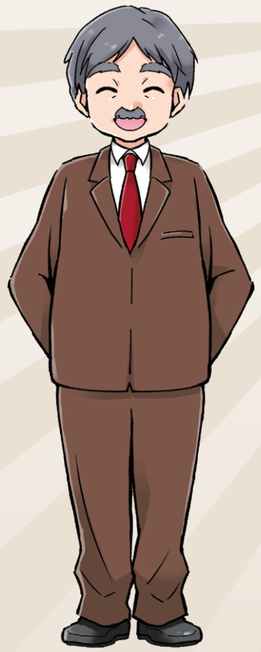
伊野部 しおん（いのべ）

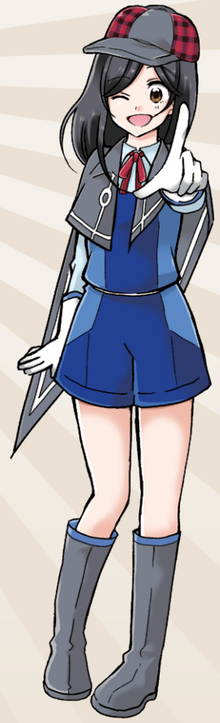
IT探偵事務所に勤めるエリート探偵。3年前までは某企業のスーパーエンジニアだったらしい。依頼先の関係者に変装をして、ITの課題を探し出して解決していく変装調査型の仕事を得意とする。

曾柳 好男（そりゅう よしお）

IT探偵事務所所長兼取締役を勤める社長。さまざまな企業に監査などの内部調査を依頼され、しおんを送り込んでは企業課題を解決させている。

しおんが解決!
経営をも脅かすサイバー攻撃。
十分な事前・事後対策を





1T探偵しおんが解決!

企業のシステム停止を狙ったり、企業内情報を窃取しようとしたりと、ますます巧妙化、高度化するサイバー攻撃。多くの企業がサイバー攻撃を受けており、中には甚大な損害を受けている企業もあります。

これまで、エンドポイントのマルウェア対策としては、マルウェアに感染させないソリューションが主流でしたが、亜種や新種のマルウェアが登場するなど100%の防御を実現することは困難です。万一のマルウェア感染を前提に、感染後の対処まで行うことも重視されつつあります。

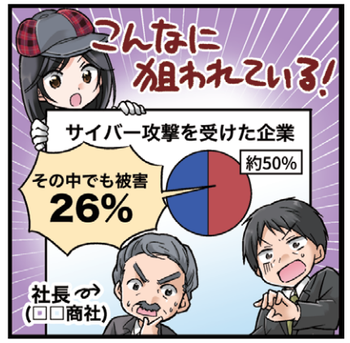
日立ソリューションズの「CylancePROTECT®」と「CylanceOPTICS™」は、AI技術を活用した高精度な検知エンジンにより、マルウェアの感染を未然に防ぎながら、万一の際も侵入経路の特定など、事後調査も支援できます。

サイバー攻撃対策は、もはや経営課題です

マルウェアによるサイバー攻撃により、企業が持つ個人情報や社内情報の流出といったいわゆる「サイバーインシデント」は増加する一方です。IPA（独立行政法人情報処理推進機構）の調査によれば、約50%の企業が何らかのサイバー攻撃を受けており、26%の企業においては被害を受けているといいます[*1]。

この状況を受けて、経済産業省は2017年11月に「サイバーセキュリティ経営ガイドライン」を改訂、企業経営者に対し、「サイバーセキュリティ」は経営リスクの一つだと明確に警告しています。また、2017年5月の改正個人情報保護法に続き、欧州でもGDPR（General Data Protection Regulation：一般データ保護規則）が2018年5月に施行され、企業に対する個人情報保護責任を求める動きは強くなっています。もはや、サイバー攻撃対策は、情報システム部門だけが責任を負うものでなく、企業全体の経営課題として取り組むべき状況にあると言っても過言ではありません。

*1 出典:独立行政法人情報処理推進機構「企業のCISOやCSIRTに関する実態調査2017」



企業に求められる、インシデント対応体制

標的型攻撃などのサイバー攻撃は、発覚までに時間がかかり、約半数が外部からの指摘で発覚するといいます[*2]。これを受けて「サイバーセキュリティ経営ガイドライン Ver 2.0」では、感染防止などの事前対策だけでなく、攻撃の「検知」、「対応」、「復旧」などの「事後対策」を求めています。

従来型のマルウェア対策製品は感染を未然に防ぐことに注視した製品が中心でしたが、事後対策に対応したEDR（Endpoint Detection & Response）製品も注目されるようになってきました。

*2 出典:経済産業省「サイバーセキュリティ経営ガイドライン Ver2.0」

「サイバーセキュリティ経営」に最適なCylanceのエンドポイントセキュリティ

エンドポイントのマルウェア対策ソリューションとして定評のあるCylance社では、事前対策として未然の感染防止を図る「CylancePROTECT」に加え、事後対策をカバーするEDR機能「CylanceOPTICS」をリリースしました。

「CylancePROTECT」はAI技術（機械学習）を使った独自のアルゴリズムで、未知のマルウェアであっても検知。マルウェアへの感染リスクを大きく低減します。

従来のパターンマッチング方式によるマルウェア対策ソフトと異なり、ファイルの特徴からマルウェアを予測して検知でき、既知・未知を問わず99%以上の検知率を誇ります[*3]。また、マルウェアが実行される前に検知できるため、マルウェアによる被害を最小限に抑えることが可能です。

パターンマッチング方式の場合、パターンにない未知のマルウェアを検知できず、感染のリスクが高まります。

EDR製品を併用していたとしても、対策をすり抜けるマルウェアが多いと、影響範囲の確認など管理者への負担は大きいものとなります。まずは既知・未知の区別なく高精度にマルウェアを検知し、感染リスクを減らすことが重要です。

*3 2018年4月NSS Labs調べ