

「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、協働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、導入を検討してみたいかでしょうか。



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。

まだマルウェア対策を
「既知」「未知」で
区別していますか!?

CylancePROTECT

詳しくは製品情報サイトへ
www.hitachi-solutions.co.jp/cylance/sp/

※本資料にはCylance Inc.の著作物が含まれています。※Cylance, CylancePROTECT, CylanceOPTICSは、Cylance Inc.の米国およびその他の国における商標または登録商標です。※その他、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、®マークは表記していません。※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/shion/vol4/



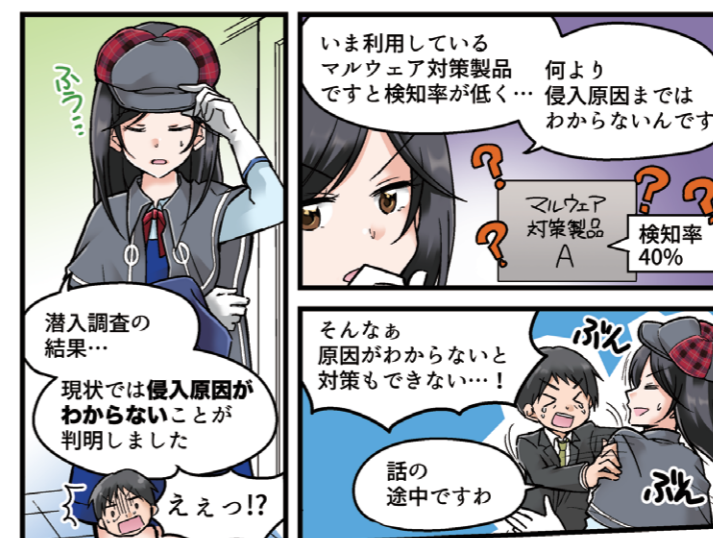
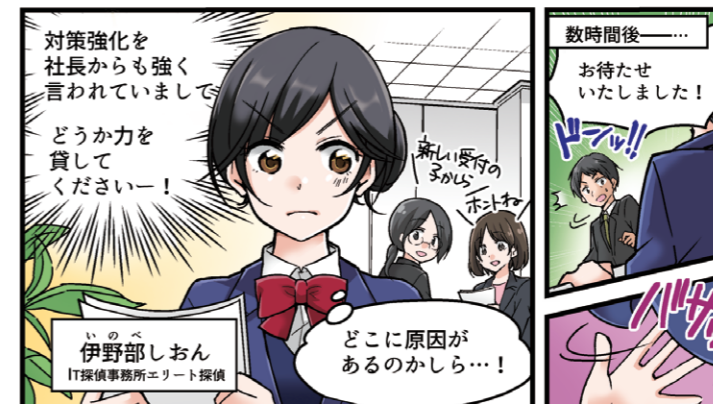
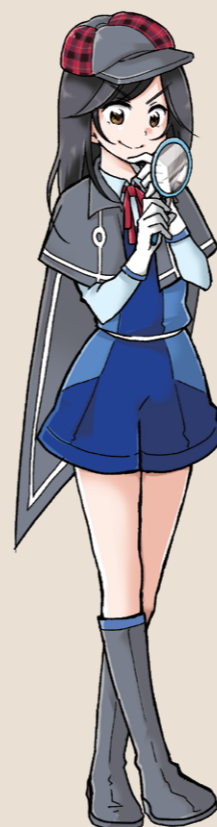
経営をも脅かすサイバー攻撃。十分な事前・事後対策を

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。

いのべ 伊野部 しおん

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。



登場人物

ぜんご たいさく 前後 泰作

□□ 商社、情報システム部部长。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。



そりゅう よしお 曾柳 好男

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

マルウェア対策なら
Cylanceに
おまかせ!

その検知率は
99%以上*
ですわ
※2018年4月NSS Labs調べ

CylancePROTECTの
AI技術によって
未知のマルウェアも
予測検知!

これでしっかり
「感染を防ぐ」ことが
できます!

きゅ…
99%!?

更に
CylanceOPTICSも
組み合わせれば、
「万が一の被害」の
対処も可能!

被害の拡大防止

会社としても
再発防止に
つなげることが
できるな!

原因分析

AIを活用し
侵入原因・経路・
影響範囲も
突き詰められます!

クラウド
クラウド!
容易な導入・管理

●日本初のCylance代理店

●さまざまな業種への
豊富な導入実績!

●2017 Japan Excellence
Support Partner of the Year受賞

何より
日立ソリューションズが
提供していますので
サポートも安心ですわ!

なるほど!!

導入後

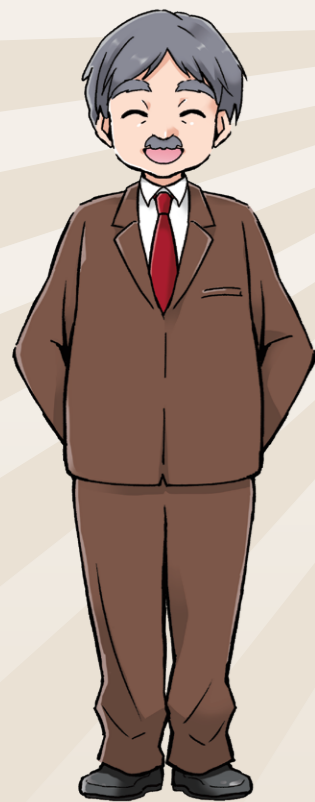
あの後には
感染もなく
毎日過ごして
います!

万が一検知した場合も
侵入経路が分かるので
対策がうてるように
なりました!

ところで…
あなたは
どこから潜入を?

お役に立てて
よかったです!

企業秘密
ですわ!



IT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えます*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」

こんなに
狙われている!

サイバー攻撃を受けた企業
その中でも被害
26%
約50%

社長の
(〇〇商社)

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えます*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 Ver.2.0」

侵入経路は…

影響範囲は…

「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

99%以上
検知!

万が一の
事後対応も
支援!!

AI活用!!