❸「コンピュータフォレンジック」（インシデントの詳細調査）
マルウェア感染したPCのハードディスクやログなどに残る痕跡を解析し、感染や不正アクセス、情報の不正流出がないかなど、インシデントの詳細状況の調査を実施します。また、調査報告書を作成し、お客様が指定される場所で報告会を実施します。

これらのサービスは要望によって、必要なものだけを実施することも可能です。

「万が一」だからこそ、実績のあるセキュリティのエキスパートに

セキュリティインシデントは「万が一」の事態です。もちろん十分なセキュリティ対策は必要ですが、一般の企業においてまれにしか発生しないインシデントの被害調査のために専任の担当者を置くことはかなりの負担になります。だからこそ「MDRサービス インシデントレスポンス」のような外部の専門家を活用する形で対応するほうが効果的といえるでしょう。

日立ソリューションズには長年、いわゆるホワイトハッカーをはじめとするセキュリティのエキスパートが多数在籍しています。日立ソリューションズのホワイトハッカーは、国内外のセキュリティコンテストにも参加し優秀な成績を収めるなど、セキュリティ技術の向上のために日々研鑽しています。

「万が一」の事態に備え、火災発生時の消防士のように頼れる、「MDRサービス　インシデントレスポンス」の利用を検討してみてはいかがでしょうか。

マルウェアの被害から企業を守るために。
まずはお気軽にご相談ください。

万が一のセキュリティインシデント発生時に初動対応や原因調査を支援

インシデントが発生した際に、高度なセキュリティの知識を持つセキュリティエキスパートが対応方針策定やマルウェア感染範囲などの調査、コンピュータフォレンジックなどを行い、被害の深刻化を防ぐための適切なインシデント対応を支援します。

MDRサービス インシデントレスポンス
www.hitachi-solutions.co.jp/security/sp/solution/task/mdr_incident_response.html

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/vol12/

C19S-03-01　2020.03

HITACHI
Inspire the Next

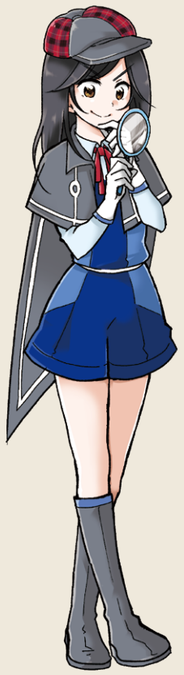
マルウェア感染!? 万が一の事態にはセキュリティエキスパートにお任せを

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。

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。



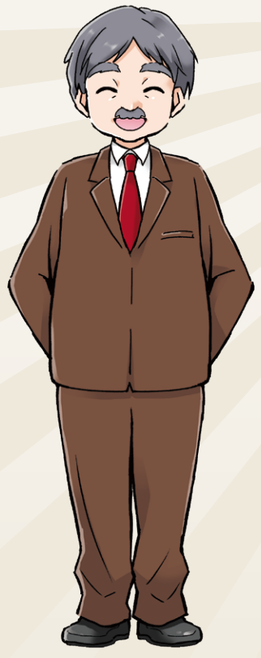
登場人物

土戸田 健治

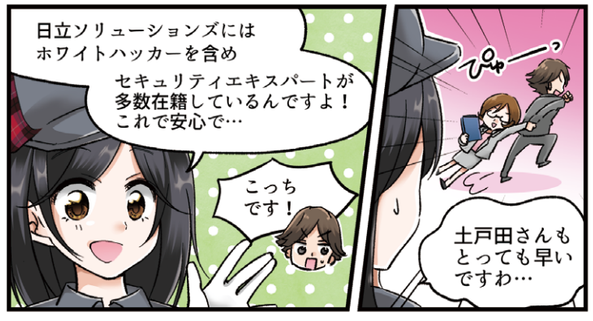
△×社の総務部兼情報システム担当。多忙な中、セキュリティ対策に日々奮闘している。
高校生のころは陸上の短距離選手として活躍していたらしい。

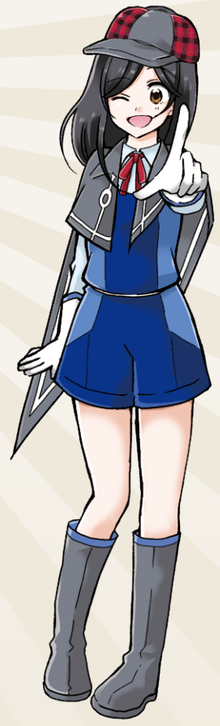
曾柳 好男

IT探偵事務所所長兼取締役を務める社長。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。



※移動時間やセキュリティエキスパートの空き状況により、すぐに訪問できない場合があります。





1T探偵しおんが解決!

マルウェアによるサイバー攻撃は高度化しており、セキュリティの知識がないと「いざ」攻撃を受けた際に、適切な判断ができません。インシデント発生時には速やかに原因と被害状況を把握し、適切な初動対応をする必要があります。
その一方で、一般の企業がセキュリティに精通した人材を育成・確保するのは難しい状況もあります。
日立ソリューションズが提供する「MDR*1サービス　インシデントレスポンス」は、マルウェア被害が発生した際に、お客様のもとにセキュリティエキスパートが駆け付け、インシデント対応を行います*2。具体的には、セキュリティインシデントであるかどうかの判断、インシデント対応体制やお客様が実施された暫定対策についてのアドバイス、被害状況の把握、コンピュータフォレンジック*3などを実施し、お客様のインシデント対応の支援を行います。

*1 MDR: Managed Detection and Response　*2 日立ソリューションズ営業日、最大2日間。訪問場所は日本国内全域（島嶼、僻地を除く）で、公共交通機関で訪問できる場所とします
*3 コンピュータなどに残る侵入の痕跡を調査すること

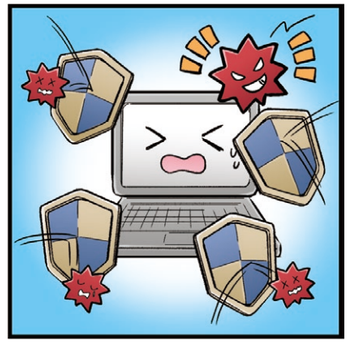
厳重なセキュリティ対策を講じても“100%”はない

日々巧妙化、高度化するサイバー攻撃。攻撃者は、常にシステムの脆弱性を見つけ出し、さまざまな防御手段をかいくぐって被害を与えることを狙っています。

そのため、セキュリティ対策を強化するだけではなく、万が一セキュリティ被害を受けた場合の備えをしておくことが重要です。

これを火災に例えると、火災報知器の設置や、コンロの近くに燃えやすいものを置かないなど、日頃から備えることが必要です。しかし、実際に火災が発生した場合には、消防に連絡し、火災による被害の拡大を食い止める必要があります。

情報システム部門の担当者はマルウェア感染を防ぐ対策だけでなく、もし感染してしまった場合、いかに適切な対応ができるか、ということも考慮しておかなくてはなりません。



「いざ」というときに、適切な対応ができるか

では、マルウェア感染による被害が発生した場合に、社内の担当者だけで適切な対応ができるでしょうか。

冒頭にも述べたように、サイバー攻撃はますます巧妙化・高度化しています。知らない間にマルウェアに感染して情報が不正に流出させられ、外部機関や顧客からの連絡によって被害が判明した、ということも珍しくありません。

最近では、EDR*4によって、マルウェアの侵入原因や影響範囲の調査・分析を行うことも可能ですが、その調査・分析には非常に高度で専門的なセキュリティ知識に精通している必要があります。さらに、担当者が日々の管理業務を行いながら高いセキュリティ知識を維持することは難しいのが現実です。こうした人的要因から、EDRの必要性を理解していても、導入に踏み切れない企業も少なくありません。

また、インシデントの際の適切な対応は、経営面においても悪影響を及ぼしかねない重要な課題です。マルウェア被害が実際に発生していたのか、その被害範囲はどれぐらいなのかを把握し、速やかな初動対応を行い、被害の拡大を防ぐこと。そして、株主、顧客、取引先、従業員などの、いわゆるステークホルダーに対し、適切な情報発信が行えないと、企業の信用を大きく失うことになります。

*4 Endpoint Detection and Response：エンドポイントでのマルウェア感染後の調査などにフォーカスした機能を持つ製品

インシデント発生時に必要な対応を支援

そこでこのようなセキュリティインシデントの発生時に火災発生時の消防士のように対応するのが、日立ソリューションズの「MDRサービス インシデントレスポンス」です。このサービスは3つのメニューで構成されています。

❶「対応方針策定支援」（インシデント発生時の初動対応）
お客様からマルウェア被害発生の連絡を受けると、まずは日立ソリューションズのセキュリティエキスパートが現場に駆けつけます。お客様による事象の確認に立ち会い、セキュリティインシデントか否かの判断の支援をします。また、インシデント対応体制やお客様が実施した暫定対策についてアドバイスを行います。

❷「侵害調査支援サービス」（インシデントの影響範囲調査）
マルウェア被害発生時に侵入状況の調査・報告を行います。調査用スクリプトを使って、感染の可能性がある端末のログデータなどを収集し、解析、調査を行います。また、端末の調査で不審なファイルが発見された場合には、そのファイルがマルウェアかどうかの脅威判定や、脅威の可能性が高いファイルの潜伏範囲の調査を行い、感染端末を洗い出します。