BlackBerry

HITACHI
Inspire the Next

インシデントレスポンス付き CylancePROTECT®

| 導入事例 | 株式会社アシスト 様

アシスト

所在地	東京都千代田区九段北4-2-1 市ヶ谷スクエアビル
設立	1972年3月
従業員数	1,244名 （2022年4月現在 グループ会社含む）
事業内容	ソフトウェアパッケージ製品の販売、および、それに関わる技術サポート、教育など
URL	https://www.ashisuto.co.jp/

ゼロトラストをめざしてエンドポイントセキュリティを強化
AI方式の検出エンジンでマルウェアを高精度に検出

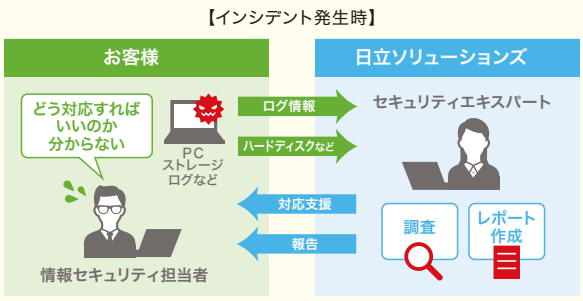
パッケージソフトウェア販売会社の老舗として知られるアシストは、ゼロトラストセキュリティ実現のための第一歩となるエンドポイントセキュリティの強化に着手。インシデント発生時の備えとして、サイバー保険が付帯された「インシデントレスポンス付き CylancePROTECT」を導入しました。AI方式の同製品の導入により、未知のマルウェアでも高精度に検出できるようになっています。

課題	効果
従来のパターンマッチング方式では 未知のマルウェアの検出が難しかった	AIを活用した検出エンジンにより、 高精度なマルウェア検出を実現
パターンファイル更新やバージョンアップなどの 運用管理の作業負荷が高かった	パターンファイルの更新や定期的なバージョンアップが 不要になり、運用管理の作業工数を大幅に削減
万一のインシデント発生に備え、調査や デジタルフォレンジックができる体制を強化したかった	サイバー保険により、インシデント発生時も セキュリティエキスパートによる支援を受けることが可能

SOLUTION

サイバー保険を活用したセキュリティサービス

- インシデント発生時の調査やデジタルフォレンジックの作業を支援するサイバー保険を「CylancePROTECT」に付帯
- AI方式のエンジンが未知のものを含むマルウェアを活動前に検知し、エンドポイントを保護
- クラウド上で一元管理できるため、セキュリティ運用管理の工数とコストを抑制



株式会社 日立ソリューションズ

| 導入事例 |

株式会社アシスト 様
INTERVIEW

経営企画本部
ITサービス企画部
課長
杉山 勝彦 氏

経営企画本部
ITサービス企画部
伊良皆 亮 氏

経営企画本部
ITサービス企画部
鈴木 康祐 氏

背景 ゼロトラストを意識してセキュリティを強化

1972年創立の株式会社アシストは、パッケージソフトウェア販売会社の老舗として知られる企業です。同社がエンドポイントセキュリティ対策の見直しに着手したのは2020年夏のことです。当時使っていた、パターンマッチング方式のマルウェア対策製品には、限界を感じていました。

「パターンマッチング方式は未知の脅威への対応に弱いのではないかと私たちは認識しており、中長期的にゼロトラストセキュリティの実現をめざすにはエンドポイントの保護を強化する必要がありました」（杉山氏）

さらに、運用管理工数の大きさも課題の1つでした。利用していたマルウェア対策製品では、全従業員のPC内のパターンファイルとエージェントを最新の状態に保つために、更新漏れの有無をITサービス企画部がチェックする必要があったのです。

「万が一、インシデントが発生したときに、社内要員だけで調査やデジタルフォレンジックを行えるのかという懸念もありました」（杉山氏）

取り組み 検知率が高い「CylancePROTECT」を選択

見直しにあたっては、パターンファイルでの検知に頼らない、AI方式のエンドポイントセキュリティ製品を導入する方針としました。自社での取り扱い商材を含む複数の製品・サービスの中から、マルウェア検知率が高いものを選び出し、2021年7月に「インシデントレスポンス付きCylancePROTECT」の採用を決めました。

「『CylancePROTECT』はマルウェアの検知率が高く、PC側のCPUやメモリーを大量に消費することもありません。今回採用した『インシデントレスポンス付き CylancePROTECT』は、『CylancePROTECT』にインシデント発生時の調査などを支援してもらえるサイバー保険が付帯していることも魅力的でした」（杉山氏）

導入作業は8月にスタートし、4カ月をかけてPoCによる検証・ITサービス企画部内の1つの課でのテスト・経営企画本部に在籍する約100名による試行を実施しました。

これらの作業を担当した鈴木氏は、「テストと試行の際に、業務に必要なものでも怪しいファイルと判断されてしまうケースがかなりあることが判明しました」と振り返ります。

そこで対策を講じ、「本稼働後も同じ傾向になると考えられましたので、エンドユーザーからの申し出に応じてセーフリストに登録する運用にしました」と伊良皆氏は語ります。

効果 クラウドサービスのため運用管理工数が大幅減少

試行の完了を受けて、ITサービス企画部は「CylancePROTECT」の運用開始を全社にアナウンスしました。マルウェアの検出のみ実施し隔離しない検出モードで2週間の試験運用をした後、2021年12月にはマルウェアの検出だけでなく、隔離まで実現する隔離モードへと切り替え、本番稼働を開始しました。

「正確な効果を把握するにはまだ時間がかかりそうですが、すでにかなりの数のマルウェアを検出できており、エンドポイントセキュリティを強化するという当初の目的は十分に達成できたと思います。ゼロトラストセキュリティへと向かう道のりの1～2割のところに、まずは到達したと思います」（杉山氏）

管理も、クラウド上で一元的に行う「CylancePROTECT」を利用することによって、運用管理工数も大幅に削減することができました。PCに組み込むエージェントを更新する際も、システム管理者が管理用Webサイトから配信を指示するだけで作業は完了します。エージェントのアップデートは自動的に行われるので、エンドユーザーにも負担はかかりません。

「従来は検査に引っかかったPCは必ずフルスキャンするというルールになっており、とても時間がかかっていました。『CylancePROTECT』では初回のフルスキャン以降、差分スキャンが自動的に行われるため、都度フルスキャンを行う必要がなくなり、管理者だけでなくエンドユーザーにとっても使い勝手がよく、満足感が高まっています。また、今回サイバー保険も付帯しているため、万が一インシデントが発生した場合であっても、対応をエキスパートに支援してもらえるということはとても大きいと思っています」（伊良皆氏）

展望 他製品との連携でゼロトラストをめざす

ゼロトラストセキュリティの実現をめざすアシストにとって、「CylancePROTECT」は目標を達成するための手段の1つというポジションです。エンドポイントセキュリティの強化に続けて、ITサービス企画部は「CylancePROTECT」とほかのセキュリティ対策ツールとの連携を深化させようと考えています。

別に導入しているクラウド型のWebプロキシ「Zscaler Internet Access」が出力するログと「CylancePROTECT」のログを集約・分析し、業務をより効率化できるようにする計画を進めています。また、EDR*ツールの導入も検討しています。

「日立ソリューションズは20年来のパートナー企業です。今回の『CylancePROTECT』導入にあたっても、設定方法やセーフリストの作り方まで協力してもらい、とても助かりました。今後、デジタルフォレンジック対応が必要になったときにも相談したい相手です」（杉山氏）

安全・安心なデジタル社会を実現するための前提となるセキュリティ対策。日立ソリューションズはこれからも、幅広いソリューションで同社を支援していきます。

＊EDR：Endpoint Detection and Response

本事例のwebページはこちら
www.hitachi-solutions.co.jp/cylance/case15/

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/cylance/sp/product/incidentresponse/

J21S-16-00 | 2022.06