cybereason 導入事例　　アルプスアルパイン株式会社

EDRの導入によりインシデントを可視化
グローバル規模、3万台以上のセキュリティ対策を統合・強化

2019年1月に経営統合し、新たなスタートを切ったアルプスアルパイン株式会社。同グループの企業は100社を超え、ネットワークは広く世界に拡大しています。従来、同グループでは国別／リージョン別にセキュリティ対策を実施していました。しかしサイバー攻撃が一段と高度化・複雑化する中、バラバラに対応していては不安があります。そこで同社はセキュリティ対策をグローバル規模で統合・強化するため、サイバーセキュリティ分析プラットフォーム「Cybereason（サイバーリーズン）　EDR」を採用しました。今回は導入の経緯と効果、将来の展望について、情報システム部 部長の清水直樹氏にお話をうかがいました。

従来の入口対策には限界、グローバル規模でセキュリティ対策を統一したい

―「Cybereason EDR」の導入を検討された背景について教えてください。

清水氏　大きく2つの理由があります。1つ目の理由は、従来の入口対策に限界を感じていたことです。これまでは侵入させないことを前提とした対策をとってきましたが、サイバー攻撃の技術が日に日に高まる中、いくら多層防御を導入しても100%の対策は不可能だと考えたのです。実際、2017～18年ごろはフィッシング詐欺被害拡大が報道されるようになり、弊社にも巧妙なねりすましメールなどが届くようになってきていました。

幸いなことに、当グループでは問題となるようなインシデントは発生していませんでしたが、いずれは対策をすり抜けてしまうだろうという危機感がありました。仮に一度でも内部ネットワークへの侵入を許してしまうと、攻撃者に好き勝手なことをされてしまう危険性があります。しかもそれは実害が発生するまで発覚しません。何をされたのか調査するにも相当な時間と手間を要し、すべて把握できるかどうかもわからないのです。

もう1つの理由は、国別／リージョン別にセキュリティ対策を導入していたため、統一がとれていなかったということです。それぞれのポリシーが違っていたため、たとえ同じ製品を使用していても、設定が異なるケースもありました。実際、それが原因で危ない思いをしたこともあり危機感を抱いていました。

こうした課題を解決するため、侵入を前提にした対応が可能なEDR（Endpoint Detection and Response）を、グローバル規模で導入できないか検討することにしました。サイバー攻撃の兆候を即座に検知し、適切な対処を迅速に行うことで万一の際のダメージを最小化するとともに、従来は点にとどまっていたセキュリティ対策を面でカバーしたいと考えたのです。

優れた機能と管理負荷の低さ、わかりやすいインターフェースを評価

―「Cybereason EDR」を採用した理由についてお聞かせください。

清水氏　EDRの導入について具体的な検討を開始したのは2018年初頭のことでした。ただ、当時は経営統合を控えてバタバタしていたこともあり、正式に採用を決めたのは2019年になってからです。

選定に際しては複数のEDRソリューションについて比較・検討したのですが、Cybereason EDRは攻撃の兆候をいち早く洗い出し、わかりやすく可視化してくれる点に魅力を感じました。また、実際の機能を比べても、攻撃の検知や特定において他ソリューションより優れていました。

さらに、マネージド・セキュリティ・サービスであることから、管理負荷がほとんどないことも大きなポイントでした。加えて、インターフェースのわかりやすさも良かったですね。これなら侵入箇所や経路、感染の原因などを正確に把握でき、攻撃の全体像が容易に可視化できると思いました。

コスト面も、他製品ではオプション扱いになっているような機能を標準で備えているので、トータルで考えればリーズナブルであると考えました。国内市場シェアでトップという実績への信頼感もありましたね。

―万単位と非常に多くのライセンスを導入されていますが、導入はスムーズに進んだのでしょうか。

清水氏　2019年春、テストを兼ねて国内に1000ライセンス分を先行導入しました。これで特に問題が起きなかったことから、海外への展開も進めることになり、2020年1月から世界中の全拠点の全ての端末に導入を開始しました。

導入自体は容易に進んだのですが、唯一問題となったのが欧州におけるGDPR（EU一般データ保護規則）への対応です。EDRはさまざまなログを取得しますが、これがクラウドを通じて欧州外に出ることが問題になったのです。これにより一部の地域で展開が遅れましたが、7月中にはなんとか完了させることができました。

インシデントを即時に可視化、具体的な対処方法までわかるように

―Cybereason EDR導入の効果についてお聞かせください。

清水氏　導入の効果で最も大きなものは、インシデントの可視化が実現したことですね。これまでは、仮に侵入されたとしても被害が出るまでは実態の把握は困難でした。つまり漠然とした対応しかとれなかったわけです。しかしCybereason EDRを導入していれば、異常を検知した時点で実際に何が起きているのか一目で状況を把握でき、さらに具体的にどのような対応をとればいいかまで教えてくれます。感染したおそれがある端末はリモートで容易に隔離できるため、感染がそれ以上拡大することもありません。

実際、テスト中に緊急の対応を要するインシデントが発生してしまったことがあったのですが、Cybereason EDRをテスト導入していた端末ではCybereasonのMSS（マネージド・セキュリティ・サービス）から分析レポートが上がってきて、すぐに的確な対応をとることができました。一方、テスト対象ではない端末では状況を追跡することができず、不十分な対応しかできなかったのです。この一件により、Cybereasonの有用性を実感しましたね。

さらに、これは管理者としての立場からの感想ですが、管理負荷が軽減されたのは大きいですね。現在グループ全体で3万台以上のPCを運用していますが、すべての状況が1か所で把握できるメリットは大きいです。また、たとえインシデントが発生してしまっても、レポート機能を活用することで、正確な報告ができるようになりました。

グループ全体のリスクを把握、ハンティングサービスの導入も検討

―将来の展望についてお聞かせください。

清水氏　今回の導入によりグローバル規模で統合されたセキュリティ対策が実現しましたので、次の段階としてグループ全体におけるリスクの可視化を実現したいと考えています。イントラネット上に攻撃の手口やリスクの状況を表示することで、従業員のセキュリティ意識啓発にも役立てていきたいと思います。

サイバーリーズン社が提供するハンティング・サービス（侵害調査）の実施も考えています。サイバー攻撃の侵入経路、流れを詳しく解析することで、システムや端末上のセキュリティホールや、抜け穴を根絶するとともに、より効果的なセキュリティ対策の立案に役立てることができればいいですね。

―ALSIへの評価、要望についてお聞かせください。

清水氏　今回の導入にあたっては、無償でトレーニングを実施していただくなど、サポート面には非常に満足しています。

ALSIは当社の子会社ということもあり、システムを長年にわたり見てもらっています。また、ALSIでも全社でCybereason EDRを導入しているので、顧客への導入・運用だけでなくユーザー側の視点も持っています。そういうこともあって、現場の困りごとを理解できる点が大きな強みでしょうね。また、セキュリティのスペシャリストとして高度な技術や豊富なノウハウを持っているだけでなく、サーバーやネットワーク、クラウドなど広くインフラ周りについても知見があります。そのため、ソフトウェアまで含めて全体をカバーしたソリューションが提供できるのが高く評価できる点ではないでしょうか。今後もいろいろとご助力願えればと思います。

問題が起きている端末の特定と問題への対処のスピードが大きく改善しました（清水氏）

アルプスアルパイン株式会社

〒145-8501
東京都大田区雪谷大塚町1-7
https://www.alpsalpine.com/

2019年1月の経営統合により、アルプス電気、アルパインは「アルプスアルパイン株式会社」として新たにスタートしました。大変革期にある自動車産業をはじめ、モバイル、民生機器、更にはエネルギーやヘルスケア、インダストリーなどさまざまな市場へ、これまで培ってきた「HMI（Human Machine Interface）」「SENSORING™」「コネクティビティ」の3つのコアデバイス技術とシステム設計力およびソフトウエア開発力を融合・進化させた新たな価値を創造しつづけることで、世界中の人々の豊かな暮らしに貢献してまいります。

開発・販売元

ALSI アルプス システム インテグレーション株式会社
〒145-0067　東京都大田区雪谷大塚町1-7
TEL 03-5499-8045　FAX 03-5499-0357
●詳しい情報は　https://www.alsi.co.jp/

■お問い合わせ先