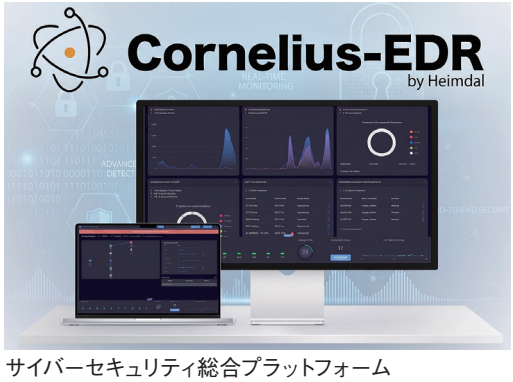
中小企業の経営リスクを解決

セキュリティサービスの包括提供で人材難・運用難をサポート

ディ・アイ・システム（4421・S）

サイバー攻撃の高度化により、企業規模を問わずセキュリティ対策は喫緊の経営課題となっている。ところが日本企業の大半を占める中小企業では、専任人材や運用ノウハウの不足から、高度な対策を導入・維持することは容易ではない。こうした背景のもと、ディ・アイ・システムは「運用できるセキュリティ」を軸に、ログ管理、特権ID管理、EDR運用支援までを包括的に提供する中小規模事業者向けサービスを強化している。



サイバーセキュリティ総合プラットフォーム

専門人材いなくても運用可能

2025年12月、ディ・アイ・システムはサイバーセキュリティ統合プラットフォーム「『Cornelius-EDR』by Heimdal」をリリースした。同サービスは、AIによる未知マルウェア検知、ランサムウェア暗号化防御、脆弱性管理、自動パッチ適用、DNSセキュリティなどを統合し、MSP型の運用支援まで提供するもの。従来のEDRは、高度な脅威検知が可能な一方、アラート分析や運用負荷の高さが課題だった。しかし同社は、初期設定支援、アラート対応、問い合わせ窓口、継続運用支援を包括提供することで、「専門人材がいなくても維持できるEDR環境」を実現した。

グループ力生かしたシステム群

現在ディ・アイ・システムでは、中小規模事業者向けセキュリティサービスを強化している。その背景には、日本企業特有の構造課題がある。近年、ランサムウェアや標的型攻撃などサイバーリスクは急速に高まっているが、多くの中小企業では情報システム部門が少人数体制であり、担当者が兼務しているケースも珍しくない。その結果、「必要性は理解しているが、運用できない」という問題が顕在化している。

実際、セキュリティ対策は導入後の運用が重要だ。ログ監視、脆弱性対応、アクセス管理、アラート分析などは継続的な対応が求められるが、専任人材を確保できる企業は限られる。

同社は、こうした中小企業の〝人材不足〟と〝運用負荷〟に着目し、「導入できるセキュリティ」ではなく、「運用し続けられるセキュリティ」の提供を成長戦略の一つに据えている。

高権限アカウントを守る

例えば子会社ウイーズ・システムズが開発する「WEEDS Trace」は、特権ID管理や操作ログ管理を中核としたセキュリティソリューションだ。システム管理者などが利用する高権限アカウントは、不正利用されれば重大インシデントにつながる可能性がある。そのため近年では、金融機関や大企業のみならず、中堅・中小企業においても特権ID管理の重要性が高まっている。

同製品では、申請承認ワークフロー、アクセス制御、ワンタイムパスワード発行、操作ログ記録などを一元的に提供。「誰が、いつ、何を行ったのか」を可視化することで、内部不正対策や監査対応を支援する。特に特徴的なのは、「申請→利用→監査」という運用フロー全体を統制できる点であり、単なるログ保存製品とは一線を画している。

また、ディ・アイ・システムはログ管理分野でもサービスを拡充。2024年に投入した「ため口グ」は、中小規模ネットワーク向けSyslog管理アプライアンスであり、ログ収集・保存・分析を低コストかつコンパクトに実現する製品だ。

サイバー攻撃や障害発生時にはログ分析が不可欠だが、中小企業では導入・運用ハードルが高かった。そこで同社は、導入時のパラメータ設定から運用保守までをワンストップで提供することで、〝ログ管理を外部化できる環境〟を構築した。

運用可能な基盤構築

ディ・アイ・システムグループの戦略は、単なるセキュリティ製品販売ではない。ログ管理、特権ID管理、EDR、脆弱性対策、監査対応までを包括的に支援し、中小企業が〝現実的に運用可能なセキュリティ基盤〟を構築することにある。

サイバー攻撃が日常化する現在、求められているのは「理想を振りかざし、現実的に運用負荷が高まるセキュリティ」ではなく、「限られた人員でも継続できるセキュリティ」だ。ディ・アイ・システムは、その〝現場起点の現実解〟を提供する企業として、存在感を高めつつある。

株式会社ディ・アイ・システム
本社　〒100-0005　東京都千代田区丸の内2-1-1　明治安田生命ビル15F
https://www.di-system.co.jp/