

高性能AIで分析・検知、クリーンアップまでを自動化

# IT管理者の負荷を低減する 高精度の予測対応型 セキュリティ

# はじめに

## 高速ディープラーニングで、 高精度の予測対応型セキュリティを実現

サイバー攻撃は日々巧妙化しており、ウイルスやマルウェアの侵入を完全に防ぐことは難しくなっています。そこで、侵入を防ぐ従来型の対策よりも、脅威の侵入を素早く検知し、被害が出る前に防御するセキュリティ対策が重要視されています。

Sophos Intercept X Advancedは、高性能AI（予測型ディープラーニング）でマルウェアを検出し、サイバー攻撃からエンドポイントを守ります。

本資料では、Sophos Intercept X Advancedにより、高精度の未知マルウェア攻撃予測・検知を実現し、IT管理者の負荷を低減させた企業の事例をご紹介します。

# INDEX

<b>はじめに</b>	1
高速ディープラーニングで、高精度の予測対応型セキュリティを実現	
<b>1. 導入の背景</b>	
サーバーセキュリティの強化と統合	4
課題1：セキュリティ対策ソフトが複数あり管理が困難	5
課題2：セキュリティの専任者がいない	6
<b>2. Sophos Intercept X Advancedが選ばれた理由</b>	
EDR機能における検知分析をAIで自動化、運用負荷を低減	8
メリット1：自動的にインシデント対応を行える	9
メリット2：高速ディープラーニング検知エンジンで、未知の脅威に対応	10
メリット3：包括的なセキュリティ対策を実現可能	11
<b>3. 導入の効果</b>	
効果1：検知から復旧まで自動化され、運用負荷を低減	13
効果2：予測・検知により、未知のマルウェア攻撃への対策を高精度で実現	14
効果3：多層防御型の包括的な対策が可能に	15
効果ビフォーアフター	16
<b>おわりに</b>	17
高性能AI(予測型ディープラーニング)でマルウェアを検出	