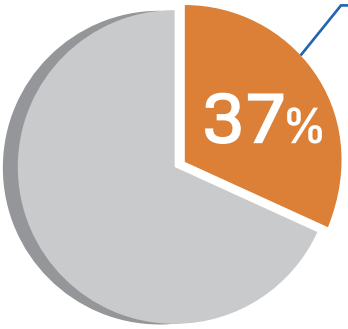
IT部門の悩み・寝不足の原因は
セキュリティ対策やIT管理の複雑化にあり!?

近年、ネットワークや IT システムは複雑化の一途をたどっており、企業に甚大な被害を与えるサイバー攻撃も高度化・複雑化しています。しかしながら、IT管理者はセキュリティ対策、ランサムウェア、管理の負荷など対応すべきことが膨大なため、企業側の対策が困難になっています。

ランサムウェアの脅威

ランサムウェア攻撃を受けた組織の割合



※調査会社 Vanson Bourne 社 30 か国にわたる 5,400 人の IT 管理者を対象に調査
※ランサムウェアの現状 2021 年版
https://secure2.sophos.com/ja-jp/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

データが暗号化された組織の割合 **54%**

暗号化されたデータを復旧できた組織の割合 **96%**

支払われた身代金の平均額 **17百万円**

身代金を支払って暗号化されたデータを復旧できた割合 (平均) **65%**

ダウンタイム、復旧のための人件費、人件費、デバイスのコスト、ネットワークのコスト、逸失利益、支払った身代金などを考慮したランサムウェア攻撃の影響を修復するための平均被害総額 **185百万円**

脅威と共に高まる、ITシステムと管理の複雑化

サイバー攻撃の脅威が迫っている一方で、複雑化するITシステム自体の把握やその管理も困難になってきている企業が増えています。

ITシステムの複雑化

ビジネス環境の変化に合わせて迅速に環境を整備するため、マルチベンダーマルチシステムとなることが多く、ITシステムが複雑化。全てを把握することが難しい状態に。

復旧時に発生する煩雑な作業

ランサムウェアなどのマルウェアに感染した場合、感染PCの特定、PCをネットワークから隔離、駆除、ネットワークへの復旧など対応事項が多く、復旧までに時間を要してしまう。

次ページ
昼夜を問わず迫りくる脅威との決別
アズムが提案するセキュリティ対策

実績と信頼のアズムが提案するSophosセキュリティ対策

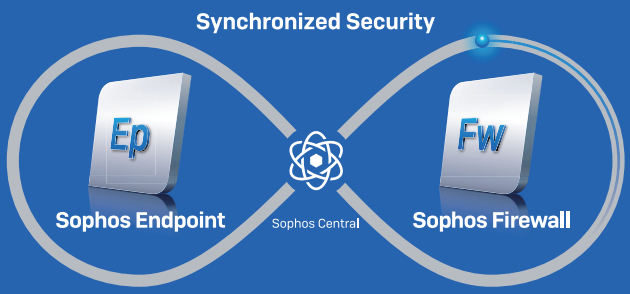
サイバー攻撃もインシデントも「Synchronized Security」が自動対応。

昼夜問わず迫りくる脅威と決別！

「Sophos Intercept X」と「Sophos Firewall XGS」が連携する「Synchronized Security」 で自動でインシデント対応が可能。昼夜問わず、脅威の検出からネットワーク隔離、駆除、ネットワーク復旧を自動化するため、インフラを保護するための時間と経費を大幅に節減。脅威からの解放とイノベーションに専念できる環境に貢献します。

Synchronized Security

ソフォスの製品がリアルタイムに情報を共有し、インシデント対応を自動化する能力。



たとえば、Sophos Intercept X が感染を検知すると、Sophos Firewall と通信し、感染したエンドポイントを自動的に隔離し、サイバー攻撃者によるネットワーク内の移動 (ラテラルムーブメント)を防ぎます。

Sophos Central

一元管理を実現したプラットフォームで複数のシステム管理から解放。
データは日本国内で保管。

Sophos Intercept X

未知の脅威も AI による検知や Exploit 対策で安心。
万が一のランサムウェアもロールバック機能で対応。

Sophos Firewall XGS

世界最高の可視性、保護、対応を実現。外部から組織への攻撃の侵入口を検査。

各ソリューション詳細はこちらからご確認いただけます ❯❯❯

枕を高くして眠るなら…

Sophosの導入検討を！

経済産業省認定
Smart SME Supporter
第13号-21040147

お問い合わせ先
株式会社アズム
〒107-0062　東京都港区南青山2丁目2番15号
Tel:03-5413-5411　Email:sophos@azm.co.jp
支店および事業所：札幌支店 Tel:011-596-6575 / 松本支店 Tel:0263-38-0930 /いわみ事業所 Tel:0854-86-8730