

外からの侵入ばかりに気をとれていませんか？

データ紛失や誤送信や持ち出し 内部情報漏洩対策

企業や組織の外部からのサイバー攻撃やランサムウェアなどの悪意ある攻撃や脆弱性によって発生する脅威への対策はもちろんですが、PC の誤操作やデバイスの紛失といった人為的なミスなど、企業や組織と関わる人に発生する脅威にも対策が必要です。

安全な運用管理を支援する各種機能・ソリューションを提供いたします。

気づいたときには、もう手遅れ

情報処理推進機構の行った「企業における内部不正防止体制に関する実態調査」では、内部不正のリスクについて十分に認識し、優先度の高い経営課題として捉えていると答えた割合は回答者の 40%。高い水準に達していないことと、個人情報以外の重要情報に対策を行っている企業は半数に満たないという結果が出ています。

企業や組織で発生する内部脅威とは



情報漏えい



マルウェア感染



DoS/DDoS 攻撃



迷惑・スパムメール



フィッシング



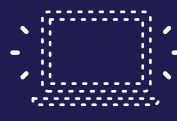
Web サイト改ざん



不正アクセス



ショルダーハック



PC などデバイスの
置き忘れ・盗難



社用 ID など
データの紛失・盗難



各機能のご紹介

サイバー攻撃対策

未知の脅威を検知し、素早い調査・駆除、エンドポイントへの対策に特化したさまざまな機能を搭載しています。

テレワーク運用

労働時間や業務状況の見える化、テレワーク中の従業員の状況把握や過重労働対策に活用いただけます。

資産管理

日々変動する資産情報を自動収集、運用の最適化やコストダウンなどに活用いただけます。

ログ管理

日々の PC の挙動をログとして管理、情報漏洩リスクの素早い発見を支援します。

セキュリティ管理

社内ポリシーに沿って不適切な操作を制限、ユーザーの情報セキュリティ意識向上に活用いただけます。

デバイス管理

デバイスやメディアの適正管理で、個人 / 機密情報の漏洩防止、組織の大切な情報を守るお手伝いをいたします。

ランサムウェア・IT セキュリティ対策強化

サイバー攻撃に多層防御による情報漏洩対策を可能にし、サイバー攻撃のリスク最小化を支援いたします。

レポート

日々蓄積されるデータを活用し、IT 資産運用の傾向を把握しながら変化を察知するツールとしても活用できます。

メンテナンス

離れた拠点の PC をリモート操作、メンテナンスや問い合わせ対応など作業の効率化にお役立ていただけます。

ソフトウェア資産管理 (SAM)

管理台帳でソフトウェア資産を複合的に管理し、導入・運用などの各フェーズでの業務を支援いたします。

サーバー監査

重要データが集まるサーバーのアクセス状況やデータベースの取扱い状況などの把握にもお役立ていただけます。

モバイル機器管理

スマートフォン、タブレット端末のビジネス活用を支援いたします。

その他にもリモート操作・送信メールログ・不許可端末遮断など
オプションで様々な対策が可能です。詳しくはお問い合わせください。