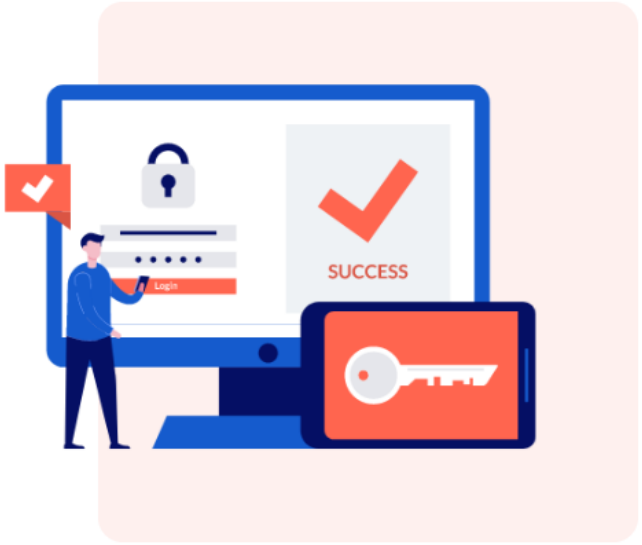


法人向けオールインワン
PCセキュリティソリューション

EXO セキュリティ

増大するセキュリティリスク、対策していますか？

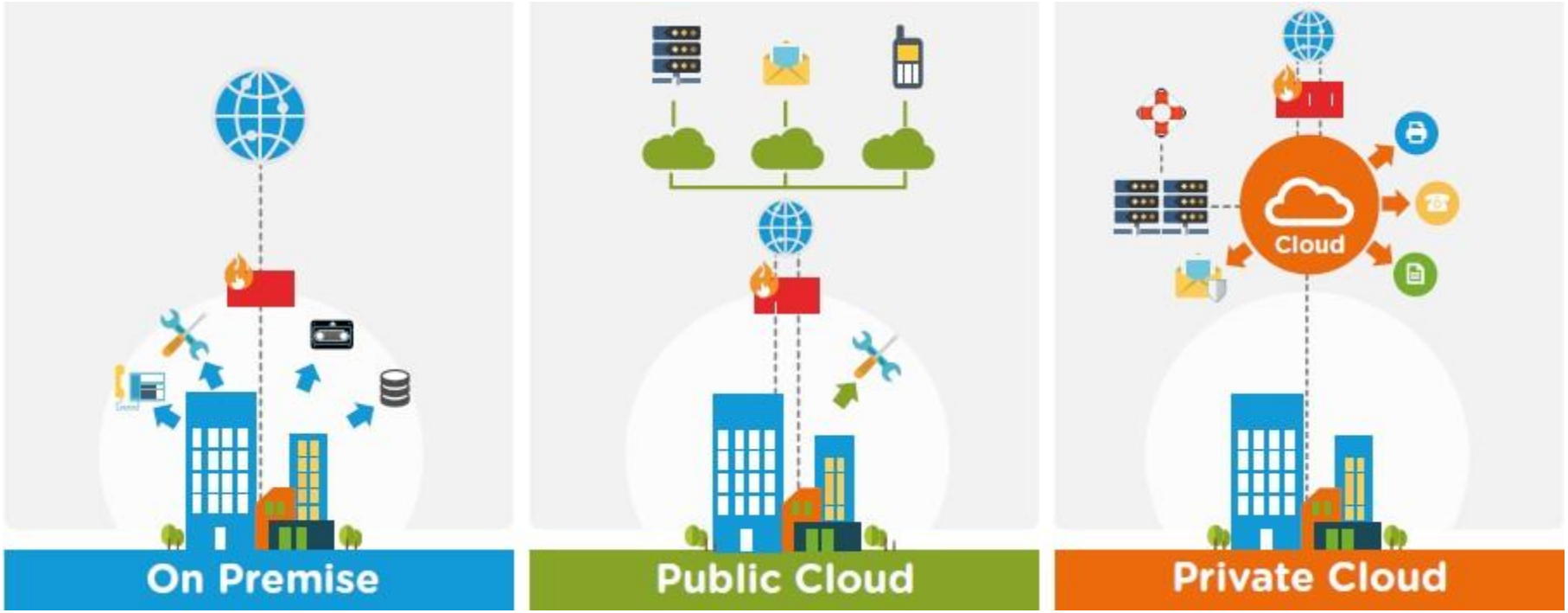
増加する企業向けサイバー攻撃

クラウド（SaaS）型 業務環境の拡大	リモートワークの増加	情報漏洩リスクの増加
		

しかし

セキュリティソフトだけでは
増大するセキュリティリスクをすべてカバーすることは不可能です。

クラウド時代、セキュリティ対策は揃えてますか？

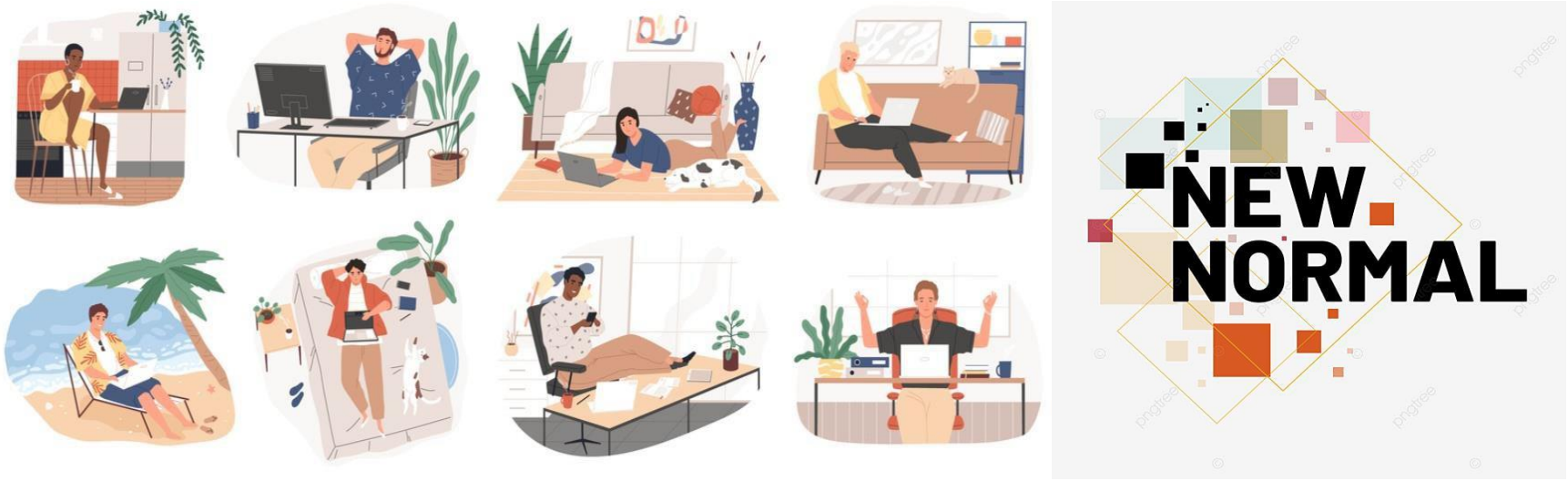


過去のITは「オンプレミス」環境で、境界のセキュリティが重要でした。
しかし、現在のクラウド環境では、
エンドポイントセキュリティ対策
つまりデバイスでのセキュリティ対策がもっとも重要です。

リモートワーク、新たなセキュリティリスクになる

Remote work is new normal.

特に、いつでもどこでも業務ができる環境で、
エンドポイントデバイスに対するセキュリティ対策が最大の課題です。



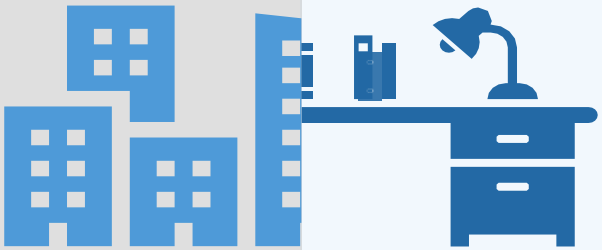
サイバーハッキング防止、情報漏洩管理、IT資産管理、
PCの脆弱性チェック、バックアップ、勤怠管理、セキュリティ誓約など
情報システム担当者の仕事と悩みは増える一方です。

リモートワーク、新たなセキュリティリスクになる

新型コロナウイルスは私たちの身の回りを大きく変化させました。
リモートワークは日常となり、
PCセキュリティは必ず解決しなければならない課題です。

従来

オフィスでの
セキュリティ環境への
投資だけで
セキュリティ対策が可能



現在

セキュリティが
脆弱な環境の増加で
ユーザ認証問題、情報流出の
課題が発生しているため
エンドポイント
セキュリティ対策が必要になる

新型コロナウイルスによる社会的変化により
デジタルへの転換が加速化し、
従来オフラインだけのビジネス環境は、
急速にオンラインに切り替わっています。

リモートワーク環境の増加で
オフライン環境のセキュリティに
投資されたシステムだけでは
不十分になっています。

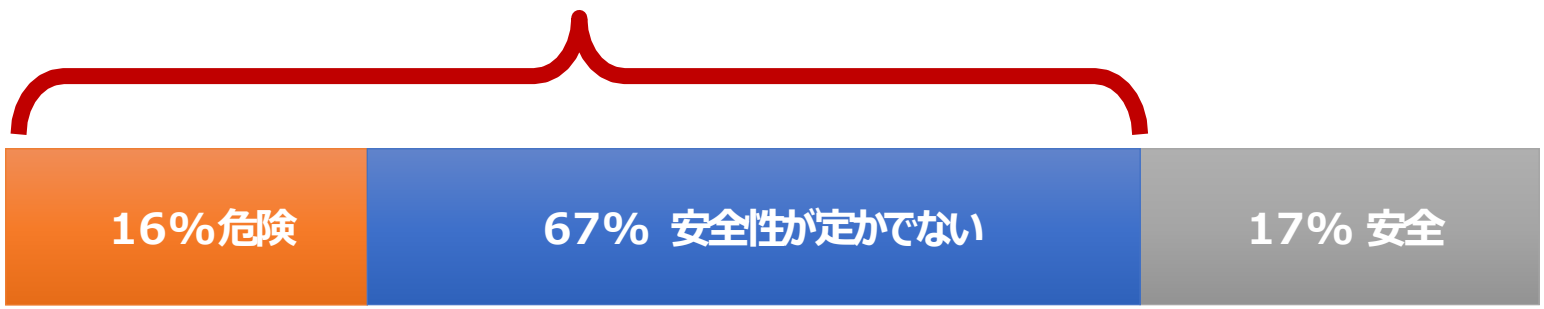
高コスト、柔軟な適用が難しい
ネットワークセキュリティより
エンドポイントのセキュリティ対策がより
重要になっていることを意味します。

エンドポイントセキュリティ対策はなぜ必要なのか

ウイルスが検知されていなかったプログラムのうち
83%は持続的なセキュリティ管理が必要でした。

自社で調査・分析した結果、
発行元が確認できないプログラムの中で
(有効なデジタル証明書を使っていない、信頼できないプログラム)

17%だけが安全だと判断でき、
83%は継続的に管理すべきプログラムだと
確認されました。
(PCドキュメントファイルにアクセスしたしていた
プログラム基準)



エンドポイントセキュリティ対策はなぜ必要なのか

ユーザー操作と類似した悪性プログラムは簡単に作成できます。
すべてのウイルス対策プログラムはこのような
悪性プログラムを探知できませんでした。

ファイルの読み込み
によるドキュメント
ファイルの流出

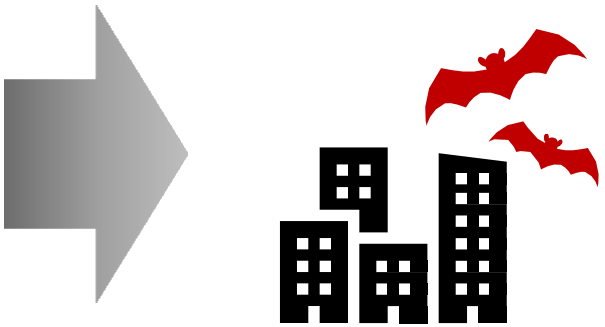
テキスト抽出を利用した
メッセンジャーの
会社内容の流出

ウイルス対策
ソフトが検知
できなかった脅威

画面キャプチャー
を利用した
パスワード流出

ユーザー操作と類似
した情報漏洩

情報漏洩を狙う悪性コード攻撃は、
ユーザーの行為と類似しているため、
検知が難しく、一度情報が漏洩してしまうと
企業の損失につながります。



企業のビジネスへ被害発生

中小企業のセキュリティ担当者の不在

セキュリティをしたくても、
セキュリティ専門家を採用することは難しいです。
セキュリティ上の問題は放置され、何も起こらないことを願うだけです。

セキュリティ対策が
必要と思われる中小企業な中、
35万社の企業を調査した結果、

セキュリティ担当者83%、
セキュリティ管制、侵害探知·対応など
セキュリティ対応専門の人は
わずか1.4%でした。

セキュリティ担当
66,646名
(83.4%)

統括セキュリティ対策・情報保護担当
1,152名
(1.4%)

35万社

製造業 89,340	建設業 27,887	卸売り及び小売業 74,425	金融及び保険業 28,219	専門、科学および技術サービス業 27,637
事業施設管理及び事業支援サービス業 12,721	協会、団体、修理及びその他個人サービス業 20,999	出版、映像、放送通信及び情報サービス業 74,425	運輸業 89,340	宿泊及び飲食店業 27,887

2016年情報保護人材需給実態調査、KISA

EXO セキュリティ

中小企業のセキュリティ担当者の不在

中小企業のセキュリティ担当者は、人事総務など管理部署の方がほとんどです。
セキュリティをどこから始めなければいいか分からない方も多いです。

業務過多

セキュリティ業務をどこからどうやって始めればいいか全くわかりません。
基本知識も必要ですし分野も多くて仕事の量も増えると思います。
今の仕事に加えて、セキュリティ業務で忙しくなるのは避けたいです。

大きな負担

セキュリティ業務を頑張ったところで、業務成果は分かりづらく目立たないです。
しかし、ランサムウェアのようなセキュリティ事故でも発生した場合、
責任は免れられず、複雑な復旧作業などの、
セキュリティ事故時の対応は行っていかなければなりません。

社員の敵

セキュリティー対策をきちんとするには、従業員への制限が多くなります。
従業員は、不満が多くなりセキュリティ担当者はいつのまにか「社内の敵」に…
それ故、セキュリティ対策を実行するに難しい環境になっていきます。

セキュリティ担当者がEXOセキュリティを選ぶ理由

EXOセキュリティは、サイバーセキュリティ業務が負担だった担当者に愛されるサービスになることを目指します。

今までのセキュリティ会社は
中堅企業以上を対象に、
サービスを企画・提供してきました。

しかし、サイバーセキュリティ問題は
全ての企業にあり、
すべての企業に必要です。

我々は全世界のお客様のために
サービスを企画・提供していきます。

既存セキュリティ製品の Pain Point

セキュリティ知識がない
運営が難しい

高価な構築費用、
変動の激しい価格

複雑な政策設定の
承認、遮断など
非効率的な管理要素の発生

合理的な価格設定

優れた技術

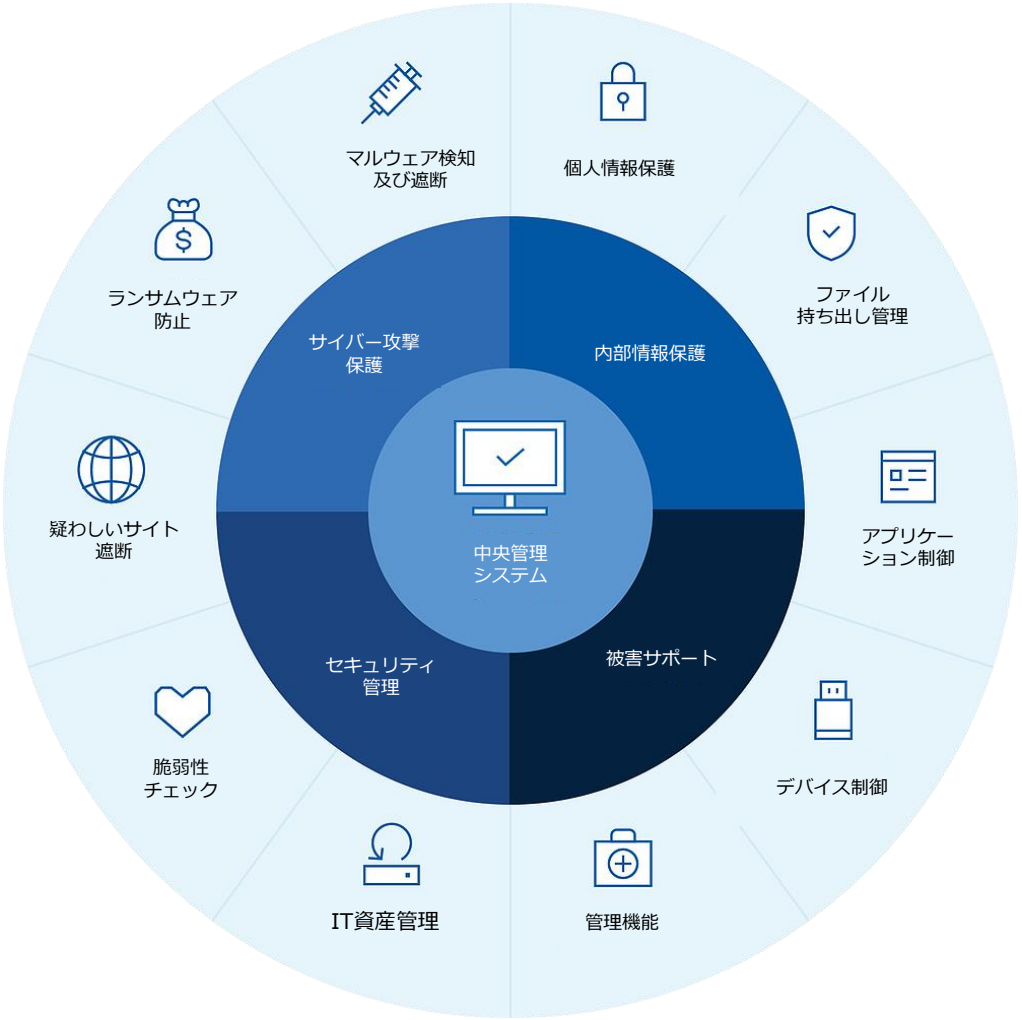
スピーディーな対応

- 社内セキュリティを技術的知識がなくても専門家のように運営することができます。
- コラボレーション企画が多い中小企業の担当者の手間を減らしてくれます。
- 専門用語の使用を最小限に抑えた親切なセキュリティサービスを提供します。

EXOセキュリティの特徴

ウイルス対策・情報漏洩対策を「EXOセキュリティ」一つで

中小企業に特化した オールインワン エンドポイントセキュリティ
EXOセキュリティ一つですべての対策ができます。



EXO セキュリティ

グローバルで立証された技術力

グローバルセキュリティソフト評価で優秀な成績で テストに合格しました。

グローバルセキュリティソフト性
能認証VB100獲得

独AVIRA社アンチウイルス
エンジン使用

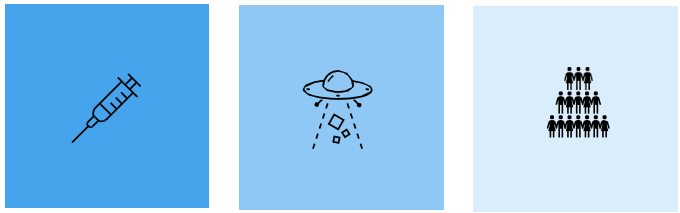
マイクロソフトウイルス
イニシアティブメンバー加入

- 2019年12月から2か月おきに
- グローバルウイルス対策性能テストVB100に参加し、全ての認証を獲得
- 信頼性の高い独AVIRA社アンチウイルスエンジン使用
- MVI(Microsoft Virus Initiative)メンバー加入
- 多様な顧客環境での製品動作検証完了

強い技術力と実績で信頼できるセキュリティソリューション

**Windows、MacOS対応のアプリケーション、
クラウド基盤の中央管理ができるプラットフォーム
を提供します。**

**現在約6000社以上のお客様を対象に安定的なサービスを
提供しています。**



**AI クラウド
セキュリティソフト提供**

**セキュリティログ収集
モジュール提供**

**約6000社の中小企業に
サービス提供**

- 安定的なカーネルモニタリング技術により、システム性能を低下させることなく、セキュリティログを収集することができます。
- MacOSのセキュリティソリューション及び情報流出管理が可能な製品は、韓国で唯一EXOセキュリティのみです。

情報システム担当者の負担を減らす簡単な操作

ユーザーデバイスにアプリケーションをインストールすると、
セキュリティログが自動的に収集され、
情報システム担当者は管理者ページで簡単に管理が可能になります。

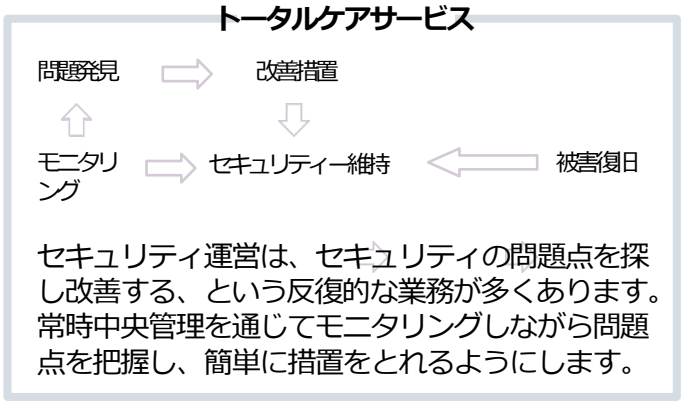
外部から侵入するウイルス、ランサムウェア、
PC に保存される個人情報、リムーバブルメディアへの
ファイルのコピー、ファイルの持ち出し、プリントなど、
すべてのログが記録されます。

情報システム担当者は、セキュリティ設定を通じて
ファイルのコピー、ファイルの持ち出しなどを
事前にブロックすることもできます。

攻めと守りを同時に強化したワンストップサービス

中小企業にとって必要な
統合的なセキュリティ、中央管理、事故対策までが
ワンストップで叶うサービスです。

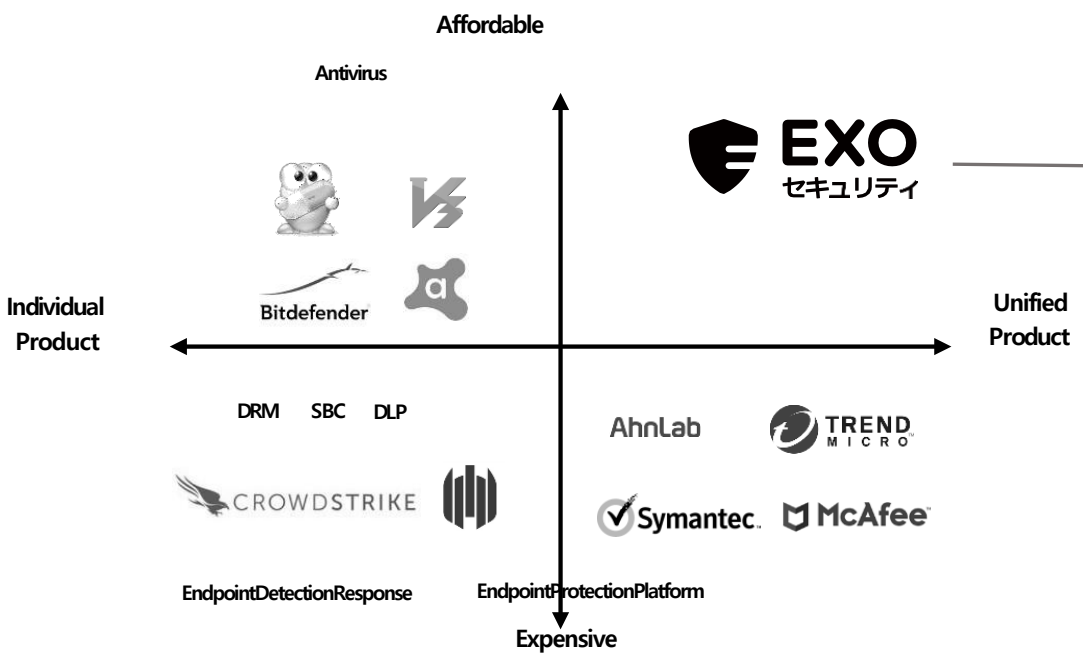
中小企業のセキュリティ担当者の業務負担を軽減できる



- **統合セキュリティ**：セキュリティソフト、情報流出管理、セキュリティ点検、資産管理まで一貫して解決することでセキュリティを強化します。
- **中央管理**：セキュリティプログラムの配布、リスク通知、スケジュールに基づいて精密検査を行います。

業界TOPレベルのオールインワンセキュリティソリューション

独歩的なオールインワン
PCセキュリティソリューションをリーズナブルな価格でご提供します。



- アンチマルウェア
- ランサムウェア対策
- ウェブ保護（疑わしいサイトブロック）
- 個人情報検出
- リムーバブルメディア制御
- アプリケーション制御
- PCの脆弱性チェック
- ソフトウェアのインストール状況照会
- ウェブアクセス制御（メール、SNSブロック）
- ファイル持ち出し記録
- ファイル持ち出しブロック
- 画面キャプチャブロック
- プリント制御（ウォーターマーク）
- ウイルス対策終了/削除防止（無力化防止）

EXOセキュリティ機能紹介

アンチマルウェア

さらに向上したマルウェア探知

人工知能とクラウドの分析技術を追加して、探知性能がさらに向上しました。
(AVIRA最高等級エンジン使用)

リアルタイム検査

システムをリアルタイムに監視しながら、ウイルスやマルウェアの流入を防止することで、ユーザーのシステムと個人情報を保護します。
リアルタイムスキャンが有効の場合、PCにリムーバブルストレージデバイスが接続されると該当デバイスに対して自動的にスキャンが実行されます。

手動検査

マルウェアの流入が疑われる場合、
ユーザーがコンピュータの一部または全体を選択して手動で検査することができます。

フルスキャン

管理者がフルスキャンを強制的に行うことも可能です。
また予約設定もできるので、予約した時間に自動的にPCの全体スキャンが実行されます。

マルウェア検出と措置検知

マルウェアを検出したら、自動で治療・隔離措置を行い、その後ユーザーへ通知します。

PCの異常検知とフルスキャン必要通知

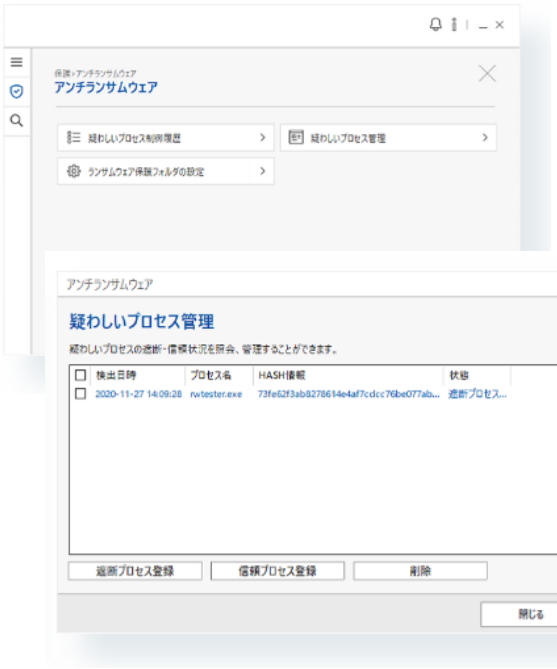
一日に複数種類のマルウェアが流入した場合、
PCの潜在的な脅威と全体スキャンの必要性をユーザーに通知します。

EXO セキュリティ

ランサムウェア防止

アンチランサムウェア機能で重要データを保護

疑わしいプロセスを制限して、PCをラムサムウェアから保護します。 (新型ランサムウェアの予防)



リアルタイム検査

システムをリアルタイムで監視します。
疑わしいプロセスがアクセスすることを遮断し、ユーザーPCの重要データを保護します。

疑わしいプロセスの制御履歴

疑わしいプロセスのアクセスおよび実行を検知し、制御した履歴を確認することができます。

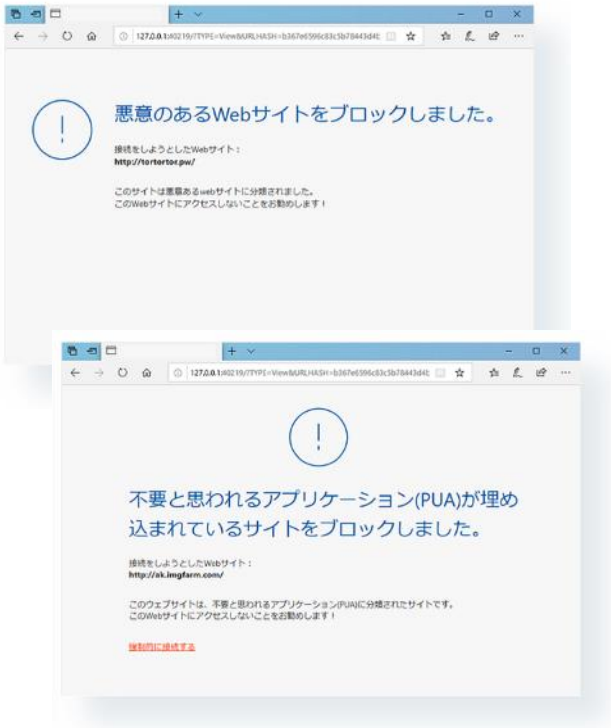
ランサムウェア防止環境設定

疑わしいプロセスから保護するべき重要ファイルの
ファイル拡張子やフォルダを登録して保護することができます。

Web保護

疑わしいサイトへのアクセスを遮断

疑わしいサイトや悪性コード流布サイト、
悪質サイトへのアクセスを遮断します。
社内で必要のないサイトを個別に指定して、遮断することもできます。



リアルタイム検査

システムをリアルタイムで監視しながら、
ユーザーが悪意のあるサイトや疑わしいWebサイトに
アクセスすることを遮断・警告することで、ユーザーのPCの重要データを保護します。

悪意のあるWebサイトの検出と遮断通知

ユーザーが悪意のあるWebサイトにアクセスすることを検出・遮断し、ユーザーに通知します。

疑わしいWebサイトへのアクセス検知と警告通知

疑わしいWebサイトにアクセスすることを検知・警告し、ユーザーに通知します。

脆弱性チェック

脆弱性が発生する原因となる主要項目についてリアルタイムにチェックします。

リアルタイム検査

オペレーティングシステム、ファイアウォール、主要ソフトウェアのアップデートなど、
必須脆弱点のチェック要素をリアルタイムでチェックし、
セキュリティリスクがある項目をユーザーに通知します。

脆弱項目に対する検知通知

リアルタイム検査で脆弱項目を検知すると、ユーザーへ通知します。
「PCセキュリティチェックを開く」ボタンで脆弱な項目の詳細を確認し、
早急に措置を行うことができます。

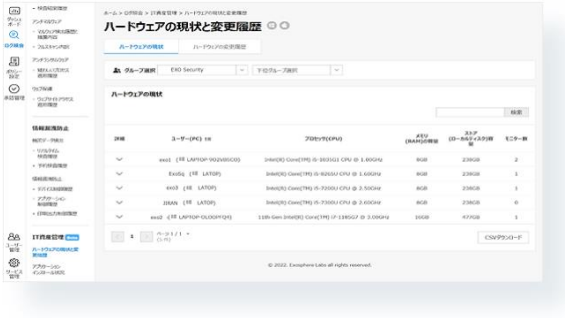
管理者はチェック状況を簡単に管理

管理者は、PCの脆弱性チェック状況を管理者ページで確認でき、
各PC別の脆弱性を確認後、素早く措置をとることができます。

IT資産管理(BETA)

自社のIT資産現状把握

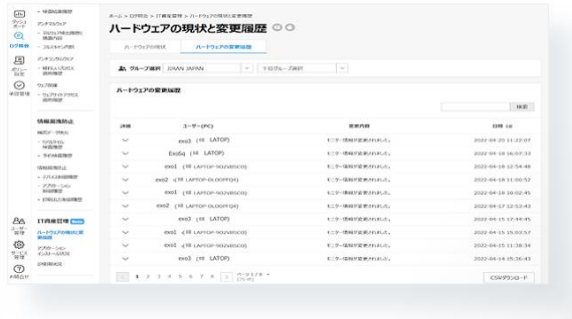
EXOセキュリティをインストールするだけで、
社内PCのすべてを把握（スペック、アプリケーション状況）でき、管理者の資産管理負担を減らします。



社内のデバイス状況を確認

エージェントがインストールされたデバイスの詳細情報を確認することができ、
社内PC管理が簡単にできます。

デバイスにインストールされたプログラム状況の確認



各PCにインストールされたプログラム状況の把握およびユーザー別での確認ができます。

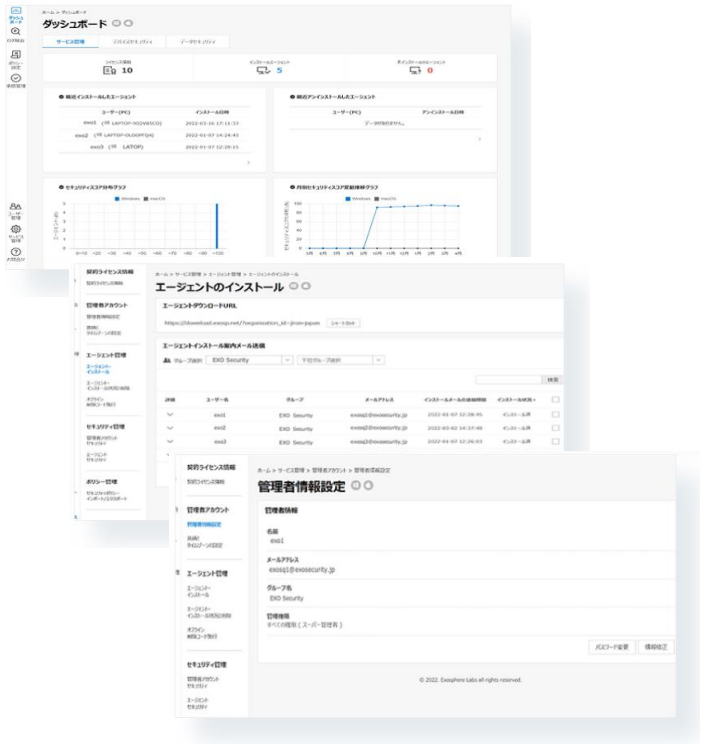
IP使用状況の確認

IP使用状況を確認することができるため、不正アクセスを把握することもできます。

その他の管理機能

サーバーや中央管理プログラムが必要ない管理者機能を使用

別途、構築や設置の必要がありません。(WEBベース)



わかりやすく簡単なポリシー設定

難しい用語の使用やポリシーを最少化し、ウイルス対策を簡単に構成できます。

アンチウイルスソフトを合理的な価格で

中小企業に必須のセキュリティ対策ソフトを合理的な価格でご利用いただけます。

#中央管理アクセス制御　#エージェントの削除防止　#セーフモードブート防止

#マルチブート防止　#OSのタイムゾーン変更を防止　#エージェントインストールステータス

個人情報保護

暗号化されていない個人情報を検出して暗号化し、顧客情報保護はもちろん、
個人情報保護法の遵守における自社のリスクも低減させることができます。

個人情報検出

個人情報を検出することができます。
管理者が設定したポリシーに沿った個人情報をリアルタイムでスキャン・検出することで、
個人情報を暗号化しないまま取り扱っているユーザーを確認することができます。

個人情報の強制暗号化

個人情報を検索し、社内セキュリティポリシーに従って暗号化・保護します。

手動暗号化・暗号化の解除

重要なデータや個人情報などをユーザーが手動で暗号化したり、
また暗号化を解除することも可能です。

リアルタイム検査・予約検査

管理者は個人情報が含まれたデータをリアルタイム検査もしくは予約検査(フルスキャン)
することで、個人情報データの現状を把握することができます。

デバイス制御機能

USBでのファイル持ち出しを防止

許可されていないUSBや外付けハードディスクなどのリムーバブルメディアの
ファイル持ち出しを防止できるデバイス制御機能を提供します。

リムーバブルメディア制御

管理者はリムーバブルメディアの接続を遮断したり、
読み取り・接続許可設定もできます。

読み取り専用

読み取り専用設定することで、リムーバブルメディアの接続はできても、
データの持ち出しはできなくなります。

リムーバブルメディア制御

デバイスを個別に設定することもできるため、社内指定デバイスを登録をしたり、
ユーザーは管理者にデバイス承認を依頼することも可能です。

アプリケーション制御機能

アプリケーション遮断

社内セキュリティやネットワークに影響を及ぼすアプリケーションを遮断できます。
(例：P2P、個人メッセンジャーなど)

アプリケーション制御

アプリケーションの実行を遮断、ファイルの持ち出しを許可・遮断することができます。

アプリケーション制御ポリシー設定

管理者は管理者ページでアプリケーション制御ポリシー設定ができます。
アプリケーションごとの設定やユーザー例外設定が可能です。

利用料金

利用料金

合理的な価格、基本に忠実な法人向けエンドポイントセキュリティ

プラン	Endpoint protection	All-in-one protection
おすすめ	リーズナブルな価格で基本に忠実な 企業専用PCウイルス対策	ウイルス対策と情報漏洩予防が同時に叶う All-In-One PCセキュリティ
料金	**5,000円** (税別) /月	**10,000円** (税別) /月
ライセンス数	50まで使い放題	50まで使い放題
50ライセンス以降	1 ライセンス当たり200円	1 ライセンス当たり400円
主な機能	◦ アンチマルウェア、アンチランサム、ウェブ保護 ◦ 人工知能分析の次世代アンチウイルス ◦ 新型ランサムウェアも防止	◦ 人工知能分析の次世代アンチウイルス ◦ 個人情報の検出・強制暗号化 ◦ デバイス制御(USBなど)、アプリケーション制御

プラン別機能表

プラン		Endpoint protection		All-in one protection	
機能名	機能説明	OS別対応		OS別対応	
		Win	Mac	Win	Mac
アンチマルウェア	リアルタイムスキャン・検査	○	○	○	○
	USB自動スキャン・検査	○	○	○	○
	手動スキャン・検査	○	○	○	○
	フルスキャン・検査	○	○	○	○
	マルウェア検出および隔離通知	○	○	○	○
	潜在的な脅威の検知とフルスキャン・検査必要通知	○	○	○	○
	AI、クラウド分析	○	○	○	○
	ログ閲覧	○	○	○	○
	例外設定	○	○	○	○
ランサムウェア防止	リアルタイムスキャン・検査	○	○	○	○
	疑わしいプロセス制御原則(フォルダへのアクセス・実行検知、制御原則登録)	○	○	○	○
	ランサムウェア防止環境設定(ファイル拡張子・フォルダパス登録)	○	○	○	○
	安全未確認プログラムを遮断	○	○	○	○
	ログ閲覧	○	○	○	○
	例外設定	○	○	○	○
悪質サイト遮断（Web保護）	リアルタイムスキャン・検査	○	-	○	-
	悪質のあるWebサイトの検出・遮断通知	○	-	○	-
	不審と思われるWebサイトへのアクセス検出・警告通知	○	-	○	-
	不正サイトへのアクセス制御	○	-	○	-
	ウェブ保護例外設定	○	-	○	-
	ログ閲覧	○	-	○	-
ファイル保護	ファイルの手動暗号化	○	-	○	-
	ファイル完全削除	○	-	○	-
PCセキュリティチェック	リアルタイムスキャン・検査(オペレーティングシステム、ファイアウォール、主要ソフトウェアの	○	○	○	○
	脆弱な項目に対する探知通知	○	○	○	○
	管理者は点検状況を簡単に管理	○	○	○	○
	ログ閲覧	○	○	○	○
IT資産管理(BETA)	社内デバイス状況を確認	○	○	○	○
	デバイスにインストールされたプログラム状況の確認	○	-	○	-
	許使用状況の確認	○	-	○	-
個人情報保護	個人情報保護・検出	-	-	○	-
	個人情報の強制暗号化	-	-	○	-
	手動暗号化・暗号化の解除	-	-	○	-
	リアルタイムスキャン・検査	-	-	○	-
	予約スキャン・検査	-	-	○	-
	ログ閲覧	-	-	○	-
デバイス制御	デバイス接続遮断	-	-	○	○
	読み取り専用	-	-	○	○
	デバイス例外設定	-	-	○	○
	管理者承認機能	-	-	○	-
	ログ閲覧	-	-	○	○
アプリケーション制御	プログラム遮断	-	-	○	○
	アプリケーションの実行遮断	-	-	○	○
	ファイルの持ち出し許可・遮断	-	-	○	○
	アプリケーション例外設定	-	-	○	○
	ユーザー例外設定	-	-	○	○
	ログ閲覧	-	-	○	○
情報漏洩防止	ファイルの添付監視	-	-	○	○
	ファイルの添付遮断	-	-	○	○
その他管理機能	中央管理アクセス制御	○	○	○	○
	エージェントの削除防止	○	○	○	○
	セーフモードブート防止	○	-	○	-
	マルチブート防止	○	-	○	-
	OSのタイムゾーン変更を防止	○	-	○	-
	エージェントインストールステータス	○	○	○	○
	テクニカルサポートチャット対応	○	○	○	○

EXO セキュリティ

ご利用開始までの流れ

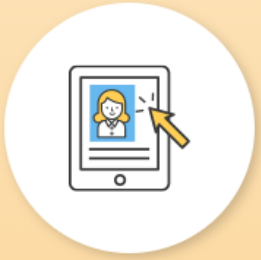
STEP 01

無料トライアル
もしくは
お問合せ

STEP 02

お申込み

STEP 03



アカウント
発行

STEP 04

ご利用開始

お申込み後、**5営業日以内**にご利用開始可能

お問い合わせ	exo@jiransoft.jp

会社概要

会社名	株式会社JIRAN JAPAN	
設立	2011年 7月 1日	
資本金	1,995,000円	
代表取締役	代表取締役　呉 治泳	
住所	〒105-7510 東京都港区海岸1-7-1　東京ポートシティ竹芝10階	
連絡先	TEL：03-6555-2991 (代)	
ホームページ	https://jiran.jp/	
事業内容	情報セキュリティ事業、クラウドストレージ事業、ビッグデータソリューション事業、顧客モニタリング事業を行う子会社等の事業支援、およびコーポレートガバナンス業務、Webサイトのデザイン・制作・運営	
主要取引先	・ソースネクスト株式会社 ・BBソフトサービス株式会社	子会社

JIRAN JAPAN

ありがとうございました。

お問い合わせ

03-6555-2991
exo@jiransoft.jp

EXO セキュリティ