Microsoft Security

Microsoft Digital Trust Security

パートナー ソリューション カタログ

第 3 版

マイクロソフトは ワークスタイルの多様化が もたらす脅威に 高度なクラウド技術を 駆使したソリューションで 対応しています。

多様なワークスタイルや業務の効率化を実現するため、クラウドやモバイル活用が進み、自宅や外出先、サテライト オフィスなど、社外から企業のデータにアクセスする機会が増加しています。
マイクロソフトは、デバイスからクラウド上のデータまで、さまざまな脅威から企業を保護するソリューションとして、Microsoft 365 Enterprise の製品群と、AI を活用したセキュリティ分析をクラウド環境で提供する Microsoft Sentinel を提供しています。

セキュリティとコンプライアンス強化をご検討されているお客様には、信頼できるパートナー ソリューションがサポートいたします。Microsoft 365 E5 導入支援、Microsoft Sentinel 活用といったお客様のクラウド導入/活用へのサポートに加え、アセスメントや SOC 運用など、お客様の IT 環境全体も含めたセキュリティ コンプライアンス上の課題を解決するソリューションを掲載しております。
セキュリティの脅威が高度化し、自社のみでの対応が難しくなってきている昨今、本カタログ掲載の、経験豊富なパートナー ソリューションの導入をぜひご検討ください。

Microsoft Digital Trust Security Alliance とは?

企業のデジタル トランスフォーメーション (DX) を支える、クラウド ネイティブ時代の新しいセキュリティ対策への移行、実装を実現する環境を推進するため、マイクロソフトのクラウド サービス「Microsoft 365」や「Microsoft Azure」を基盤としたセキュリティ ソリューションを提供するパートナー企業と共に歩むコミュニティです。デジタル トラストを実現するセキュリティ ソリューション普及促進を目的とした企業間連携に取り組んでいます。

加入企業数 69 社 (2022 年 2 月現在)

Microsoft DIGITAL TRUST SECURITY Alliance

Microsoft Digital Trust Security Alliance パートナー (カタログ掲載企業)

企業名五十音順

株式会社アイネットテクノロジーズ

アバナード株式会社

株式会社インフォメーション・ディベロプメント

ウチダスペクトラム株式会社

エクシオグループ株式会社

SBテクノロジー株式会社

ＮＲＩセキュアテクノロジーズ株式会社

NTTコミュニケーションズ株式会社

株式会社大塚商会

株式会社Colorkrew

株式会社クラウドネイティブ

KPMGコンサルティング株式会社

株式会社サイバーセキュリティクラウド

株式会社シーイーシー

ＪＢサービス株式会社

JBCC株式会社

SoftwareONE Japan 株式会社

株式会社ソフトクリエイト

ソフトバンク株式会社

株式会社ソリトンシステムズ

TIS株式会社

株式会社TOSYS

日商エレクトロニクス株式会社

日本システムウエア株式会社

日本タタ・コンサルタンシー・サービシズ株式会社

日本電気株式会社

日本ビジネスシステムズ株式会社

ネクストリード株式会社

パーソルプロセス＆テクノロジー株式会社

富士通株式会社

三井物産セキュアディレクション株式会社

株式会社ラック

リコージャパン株式会社

Microsoft 365 Enterprise と Microsoft Sentinel の 2 つの手法で、セキュリティとコンプライアンス強化を実現

最高の生産性向上アプリと高度なセキュリティ、
コンプライアンス機能を提供する強力なソリューション

Microsoft 365 Enterprise

常に変わり、進化し続けるデジタル時代の基盤となるセキュリティ

インターネットであらゆるものがつながる世界でテクノロジーはかつてないスピードで進化し、私たちの生活や働き方は変わり続けています。会社の外から働くリモート ワークが進み、スマートフォンやタブレットなどのモバイル端末を含めて 1 人で複数のデバイスを使うことも珍しくなくなっています。
いつでも、どこでも、安全に働けることがかつてないほど重要になっています。
このように常に変わり、進化し続ける時代において、Microsoft 365 E5 は、企業が必要とするセキュリティとコンプライアンス機能を提供する強力なクラウド ソリューションです。

ID & アクセス管理
ユーザー ID の保護と
ユーザーリスクレベルに基づく
価値あるリソースへのアクセス制御

脅威からの保護
高度な脅威に対する
保護と攻撃された際の
即座の回復

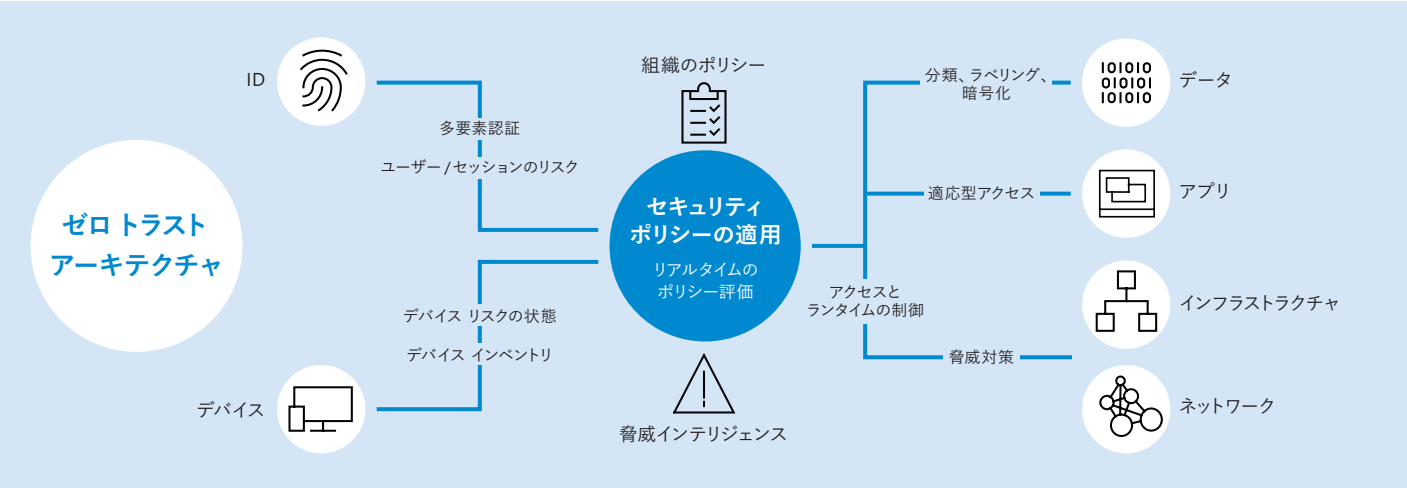
情報保護
機密情報の保護ファイル、
メールの暗号化など

デバイス管理
デバイスへの脅威防御と
脆弱性の可視化

セキュリティ管理
セキュリティ ツールを通じて
可視化と制御を実現

" 決して信頼せず、常に確認する" ことを前提にしたゼロ トラストでセキュリティ強化と利便性の向上を両立

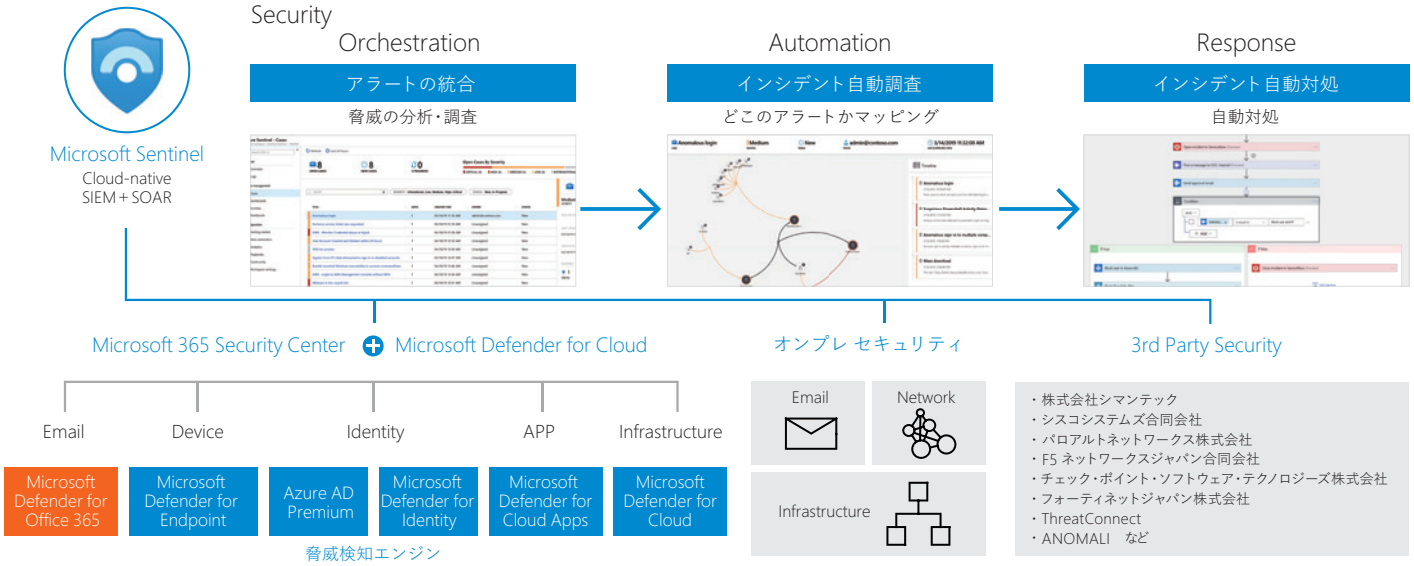
企業におけるクラウド サービスの利用は年々増加しており、組織内外の境界をベースにした従来型のネットワーク制御では安全性の確保が難しくなっています。そのため、組織の内側か外側かにかかわらずネットワーク上のすべてを疑い、検査や認証によって利便性を損なうことなく安全性を確保する "ゼロ トラスト" のアプローチが重要です。
Microsoft 365 E5 で提供するセキュリティ ソリューションもゼロ トラストに基づいています。



企業全体のセキュリティをインテリジェントに分析

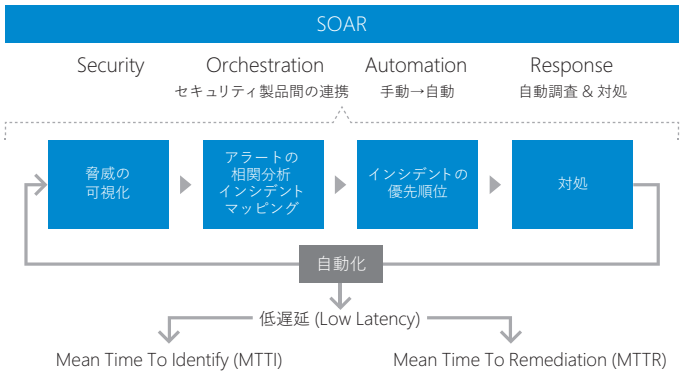
Microsoft Sentinel

クラウド ネイティブ型のセキュリティ情報イベント管理 (SIEM) およびセキュリティ オーケストレーション自動応答 (SOAR) ソリューションです。横断的な検索や AI を使ったインシデントの抽出、特定のアラートへのインシデントと対処の自動実行ワークフローの作成などが可能になります。



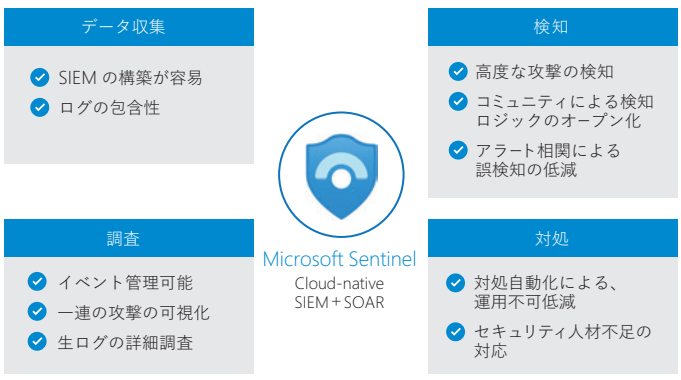
セキュリティ運用の負荷を軽減

Microsoft Sentinel により、脅威の可視化から各セキュリティ製品によるアラートの統合、インシデントの調査と対処を自動化できるため、セキュリティ運用の負荷が大幅に軽減されます。また、より迅速に脅威を特定し、短時間で対処できることで、感染の拡大や業務への影響を最小化できます。



Microsoft Sentinel を活用したセキュリティ運用

データ収集から検知、調査、対処までを自動化できる Microsoft Sentinel の活用により、高度なセキュリティ インフラの構築や保守が不要になります。組織のニーズと規模に合わせて、柔軟にスケーリングを行えるため、セキュリティにかかわる IT コストを削減できます。また、セキュリティ運用全般の自動化によって、セキュリティの専門家の人材不足も解決することが可能になります。



Index

企業名五十音順

■ 企業名/ソリューション名	■ 導入フェーズ	■ サービス対象	
SoftwareONE Japan 株式会社 SoftwareONE マネージド 365 セキュリティ	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	27
株式会社ソフトクリエイト Microsoft Defender for Endpoint 監視サービス	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	28
ソフトバンク株式会社 マネージドセキュリティ サービス	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	29
株式会社ソリトンシステムズ セキュリティ監視サービス for IoT/OT	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	30
TIS株式会社 Microsoft Sentinel 向け活用サービス	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	31
TIS株式会社 Microsoft 365 E5 Security 導入サービス	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	32
株式会社TOSYS セキュリティ デスク サービス Office 365 脅威対策アセスメント サービス	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	33
株式会社TOSYS Enterprise Mobility + Security (EMS) 導入サービス	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	34
日商エレクトロニクス株式会社 サイバー攻撃 & 内部脅威可視化アセスメント	コンサルティング / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	35
日商エレクトロニクス株式会社 MSS for EDR - Microsoft Defender for Endpoint -	コンサルティング / 運用	エンドポイント / ID / 情報資産 / 統合管理 / コンプライアンス	36
日商エレクトロニクス株式会社 MSS for SIEM - Microsoft Sentinel -	コンサルティング / 設計/構築 / 運用	マルチクラウド / ID / 情報資産 / 統合管理 / コンプライアンス	37
日本システムウエア株式会社 統合運用監視サービス「Managent」	コンサルティング / 設計/構築 / 運用	ID / 情報資産 / 統合管理 / コンプライアンス	38
日本タタ・コンサルタンシー・サービシズ株式会社 TCS Hαven for SOC	コンサルティング / 設計/構築 / 運用	ID / 情報資産 / 統合管理 / コンプライアンス	39
日本電気株式会社 脅威可視化アセスメント & 設定変更支援サービス	コンサルティング / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	40
日本ビジネスシステムズ株式会社 マネージドセキュリティサービス (MSS) シリーズ	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	41
日本ビジネスシステムズ株式会社 スマート スタート for Microsoft 365 セキュリティ	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	42
ネクストリード株式会社 脅威可視化アセスメント Light	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	43
パーソルプロセス＆テクノロジー株式会社 Office 365 脅威可視化 無料アセスメント	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	44

■ 企業名/ソリューション名	■ 導入フェーズ	■ サービス対象	
パーソルプロセス＆テクノロジー株式会社 「いつでも」「どこでも」「どのデバイスでも」を実現する Microsoft 365 MSS	コンサルティング / 設計/構築 / 運用	マルチクラウド / メール / エンドポイント / CASB / ID / 情報資産 / 統合管理 / コンプライアンス	45
パーソルプロセス＆テクノロジー株式会社 Azure Security ワークショップ (ネットワーク＆Hybrid Cloud Security)	コンサルティング / 運用	マルチクラウド / 情報資産 / 統合管理 / コンプライアンス	46
パーソルプロセス＆テクノロジー株式会社 Microsoft Endpoint Management ワークショップ	コンサルティング / 設計/構築 / 運用	エンドポイント / ID / 情報資産 / 統合管理 / コンプライアンス	47
富士通株式会社 FUJITSU Security Solution インテリジェンス マネージド セキュリティ サービス	運用	メール / エンドポイント / CASB / ID	48
三井物産セキュアディレクション株式会社 統合ログ監視サービス･Advanced SOC with Microsoft Sentinel セキュリティ監視サービス for Microsoft 365 Defender	コンサルティング / 設計/構築 / 運用	メール / エンドポイント / CASB / ID / 統合管理	49
株式会社ラック マネージドEDRサービス for Microsoft Defender for Endpoint	コンサルティング / 設計/構築 / 運用	エンドポイント	50
リコージャパン株式会社 Microsoft 365 脅威分析サービス	コンサルティング / 設計/構築 / 運用	メール / エンドポイント / CASB / ID / 統合管理	51

スタートアップ for Microsoft 365 Security

株式会社アイネットテクノロジーズ

INET-TECHNOLOGY'S
SECURITY AND OPERATION CONSULTING

Microsoft 365 セキュリティを今すぐ導入したいお客様に最適!

Microsoft 365 は導入したけど、今持っているライセンスで何ができる? どこまで守れる? といったお悩みをお持ちのお客様向けに特化したソリューションです。

こんな課題をお持ちの方におすすめ!

■ ライセンスは購入したが、何から始めればいいかわからない
■ テレワークでもセキュリティ対策がしたい
■ 専任がおらず、運用面で不安がある

解決

導入効果

■ 当社の豊富なナレッジに基づいたすばやい導入が可能です
■ セキュアでストレスフリーなテレワーク環境を実現します
■ 専任者不在でも安心なマニュアルをご提供します

【サービス内容】

■ スタートアップ for Microsoft 365 Security Basic

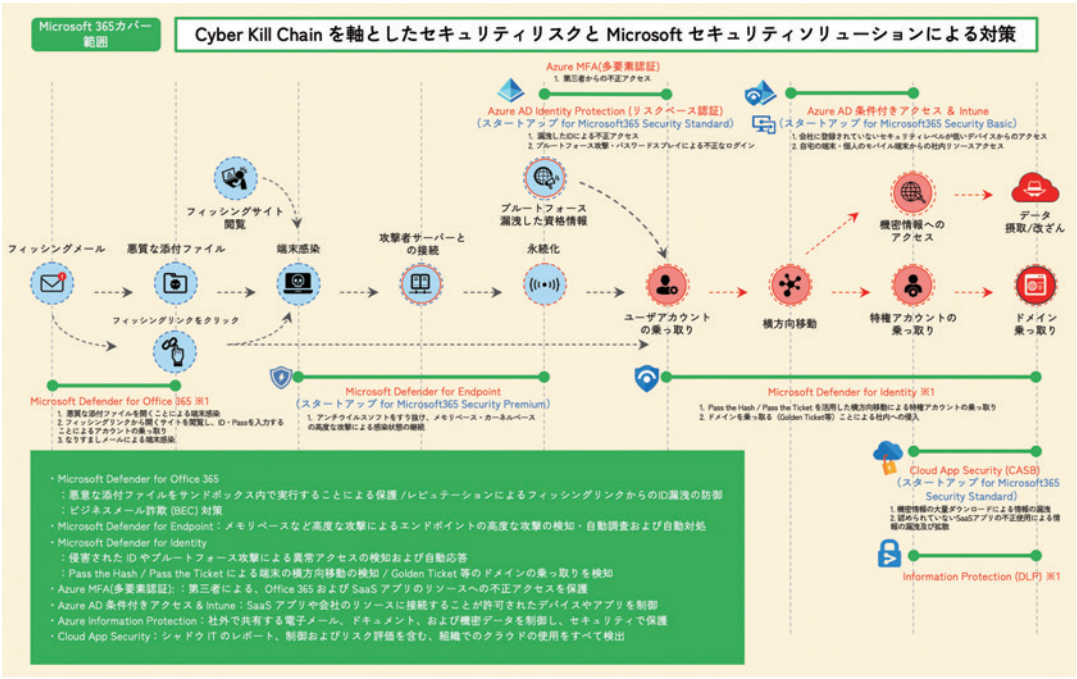
ライセンス: Microsoft 365 E3 または Enterprise Mobility + Security E3
スコープ: Microsoft Azure AD 条件付きアクセス + Intune デバイス認証

■ スタートアップ for Microsoft 365 Security Standard

ライセンス: Microsoft 365 E5 または Enterprise Mobility + Security E5
スコープ: (Basic プラン +) リスクベース認証 + MCAS 不正監視

■ スタートアップ for Microsoft 365 Security Premium

ライセンス: Microsoft 365 E5 または Enterprise Mobility + Security E5
スコープ: (Standard プラン +) MDE + リスクベース認証



【サービス提供エリア】

関東、中部、近畿地方

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先
株式会社アイネットテクノロジーズ
TEL 03-6264-9133 Microsoft Security 診断サービス 050-8881-5770 (受付時間 平日 9:00 ～ 17:30) e-mail info@inet-tech.jp
フォーム https://www.inet-technologys.com
所在地: 〒103 - 0005 東京都中央区日本橋久松町 11 - 8 REGRARD NINGYOCHO URL: https://www.inet-technologys.com

脅威可視化アセスメント

株式会社アイネットテクノロジーズ

Microsoft 365 の外部脅威に対する強化を支援します。

Microsoft 365 をご契約のお客様へ、日々進化するサイバー セキュリティの脅威可視化アセスメント をご提供します。お客様のテナントに対して不正アクセスや標的型攻撃、マルウェア感染等を検出して可視化し、その情報をもとにリスク回避、軽減を行うための最適な構成をサポートします。外部脅威リスクの有無および今後のセキュリティ強化ポイントを把握できます。

こんな課題をお持ちの方におすすめ!

- マルウェアの感染状況を知りたい
- アカウント情報は漏洩していないか?
- ファイルのアクセスに異常はないか?
- デバイスは感染していないか?

解決

導入効果

- マルウェア攻撃を受けている状況を可視化
- アカウント奪取の試行件数を可視化
- クラウド ストレージのデータアクセスの状況を可視化
- 端末の感染状況を可視化

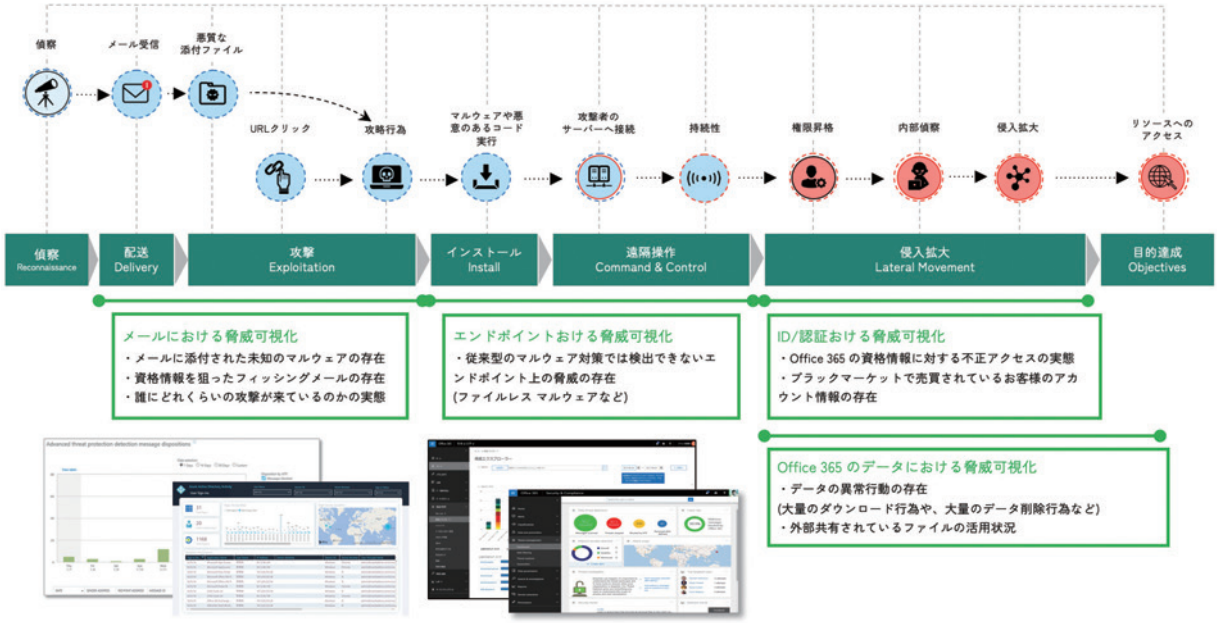
【サービス内容】

■ ヒアリング
サービスのご説明、ライセンスの状況や環境についてヒアリングを実施いたします。

■ 設定作業
ヒアリング内容をもとに設定作業を実施いたします。

■ データ収集、分析
設定作業後にデータ収集を行い、分析を行います。

■ ご報告、提案
結果についてのご報告と今後の対策についてご提案いたします。



【サービス提供エリア】

関東、中部、近畿地方

【価格】

お問い合わせください

□ お問い合わせ先
株式会社アイネットテクノロジーズ
TEL 03-6264-9133　Microsoft Security 診断サービス 050-8881-5770（受付時間 平日 9:00 ～ 17:30）　e-mail info@inet-tech.jp
フォーム https://www.inet-technologys.com
所在地: 〒103 - 0005 東京都中央区日本橋久松町 11 - 8　REGRARD NINGYOCHO　URL: https://www.inet-technologys.com

Microsoft 365 Secure Score Assessment

アバナード株式会社

avanade

Microsoft 365 におけるセキュリティを強化するための分析とロードマップを策定

Secure Score Assessment では、アバナードの優れた知見を元に開発されたアセスメント ツールと Microsoft 365 Secure Score Tool を組み合わせ、企業の Microsoft 365 利用におけるセキュリティ対策状況を可視化/スコアリングします。得られた結果を高度に評価/分析し、推奨される対応事項、および実装を行うまでのロードマップを提供します。

こんな課題をお持ちの方におすすめ!

■ Microsoft 365 をセキュアに利用できているか評価したい
■ M&A による組織のテナント統合に併せてガバナンスを強化したい

解決

導入効果

企業が抱えるリスクを明確にしたうえで、改善に向けて優先的にとるべきアクションとそのロードマップを策定できます。

【サービス内容】

■ ワークショップによるヒアリングで主要なリスクをスコアリング

Secure Score Assessment では、ワークショップを通じて組織の情報をヒアリングします。評価ツールによりリスクは自動でスコアリングされます。

■ 深いセキュリティ専門知識を活用した高度な分析

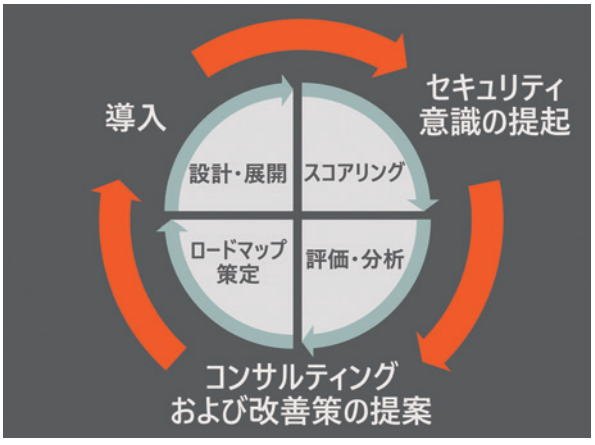
Microsoft エコシステムのソリューション プロバイダーとして培ってきた高度な知見と深い洞察により、組織が抱えるセキュリティ リスクをさらに評価/分析します。

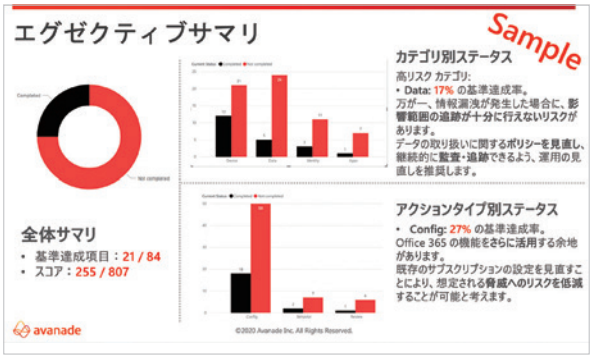
■ 迅速な成功に向けたロードマップを策定

セキュリティ対策はコストとのバランスが求められます。評価/分析により組織が抱えるリスクを明確にしたうえで、最大限に効果を引きだすロードマップを策定します。

■ セキュア ワークプレイスの実現に向けた Next Action

Microsoft 365 の高度なセキュリティ機能の実装、クラウド ID マネージメントの最適化、グローバルでのテナント統合などさまざまな課題に対し、アバナードが優れた技術力で支援します。





【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先

アバナード株式会社

TEL 03-6234-0150 (受付時間 平日 9:00 ～ 18:00) e-mail tokyo@avanade.com
フォーム https://www.avanade.com/ja-jp/contact
所在地: 〒106 - 6009 東京都港区六本木 1 - 6 - 1 泉ガーデンタワー 9F URL: https://www.avanade.com/ja-jp

Microsoft Defender for IoT 導入・運用サービス

株式会社インフォメーション・ディベロプメント

INFORMATION DEVELOPMENT

制御ネットワークの異常を即時検知、お客様へお知らせし、攻撃の拡散防止に寄与します。

制御ネットワーク用に開発された監視センサーを用い、特殊なプロトコル、デバイスが存在する環境の脆弱性を特定し攻撃経路を識別。異常な振る舞いをリアルタイムで検知します。本サービスではセンサーを導入し、運用するためのご支援をいたします。また、導入に向けた事前のアセスメントも実施。ミラーポートがあれば安価で容易に行うことが可能なため、事前調査としてご活用いただけます。弊社独自の遠隔監視サービスもメニューにございますので、ぜひご活用ください。

こんな課題をお持ちの方におすすめ!

工場や建物の DX を進めるための現状把握をし、制御システムへのサイバー攻撃に対する安全性の担保、攻撃に対する備えがあることを立証したいお客様。

解決

導入効果

- ネットワーク可視化、図面化
- 常時監視と攻撃発生の検知
- 脆弱性評価と攻撃経路予測による対策の提示
- 監視専門人材は不要

【サービス内容】

■ Microsoft Defender for IoT 導入・運用サービス “フェーズ 0”

PLC など制御機器が接続されたスイッチからのパケットを頂戴し、簡易的な調査結果をご提供します。

■ Microsoft Defender for IoT 導入・運用サービス “フェーズ 1”

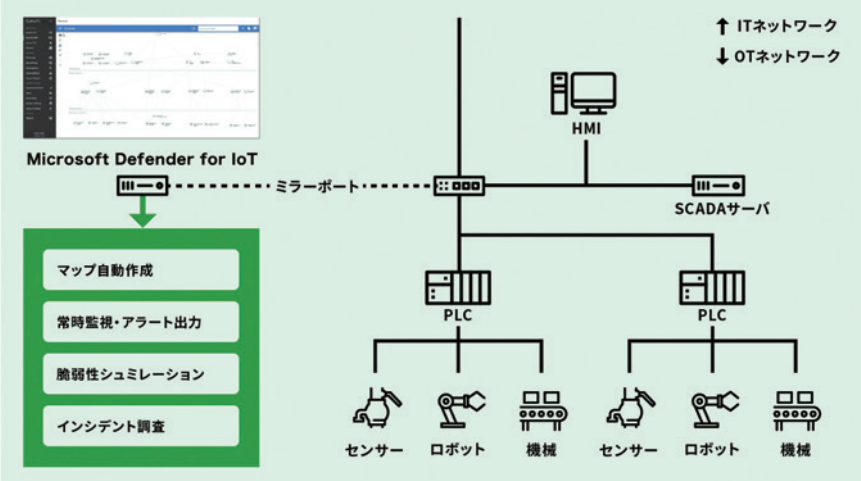
物理調査やリスクの特定を実施いたします。将来的な NW 更改などの準備にもご活用いただけます。

■ Microsoft Defender for IoT 導入・運用サービス “フェーズ 2”

累計十数件のお客様との案件実績を活かし、センサーの構築、導入、センサー学習後のチューニングを実施します。

■ Microsoft Defender for IoT 導入・運用サービス “フェーズ 3”

弊社監視センターが 24 時間 365 日監視し、アラート発生時はお客様にメールや電話にてお知らせします。



【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://www.idnet.co.jp/service/azure_defender_for_iot.html

□ お問い合わせ先

株式会社インフォメーション・ディベロプメント

TEL 03-3262-1734（受付時間 平日 9:00 ～ 17:30 祝日を除く） e-mail marketing@idnet.co.jp

フォーム https://www.idnet.co.jp/contact/service.html

所在地: 〒102 - 0076 東京都千代田区五番町 12 - 1 番町会館 URL: https://www.idnet.co.jp/

USILIS セキュリティ ソリューション

ウチダスペクトラム株式会社

安心/安全なモダン ワーク プレース環境の構築を支援し、時間や場所にとらわれない柔軟な働き方を実現

リモート ワークの導入など、働き方が多様化してきたことに伴い、セキュリティ対策の見直しが必要になっています。ウチダスペクトラムでは、組織の環境を可視化して、現状を評価し、セキュリティ強化やセキュリティ対策の最適化をご支援します。リモートワークにおける“ゼロトラスト”環境のセキュリティ対策で重視される「メール」、「ID / 認証」、「データ」の対策に重点を置いたサービスを提供します。

こんな課題をお持ちの方におすすめ!

- ■ リモート ワークのセキュリティ対策に不安がある
- ■ セキュリティ対策にかけられるコストに限りがある
- ■ セキュリティに詳しい担当者がいない など

解決

導入効果

- ■ リモート ワーク環境のセキュリティ向上
- ■ コンプライアンス ガバナンスの強化
- ■ 組織の状況に応じた柔軟な導入計画の立案
- ■ スピーディーなモダン ワーク プレースの構築

【サービス内容】

■ 脅威可視化アセスメント / レポーティング サービス

Office 365 環境を多角的な視点からアセスメントします。脅威実態 (標的型攻撃や ID 侵害の有無など) の把握により、効果的なセキュリティ対策の検討を支援します。

■ 機密情報可視化アセスメント / レポーティング サービス

Office 365 環境に存在する機密情報 (社外秘や個人情報など) を調査、分析します。機密情報の有無や属性などを明らかにすることで、情報漏えい対策の検討を支援します。

■ Microsoft 365 セキュア リモート ワーク環境構築支援サービス

リモートワーク環境の導入をご検討中のお客様に、Microsoft のセキュリティ機能を利用したセキュアなリモート ワーク環境の構築を支援します。

■ 条件付きアクセス環境構築サービス

Azure AD の条件付きアクセス制御を中心とした、セキュア ID 環境の整備を実現します。(リアルタイムなリスク評価の組み込みやマネージドデバイスのアクセス許可など)

【サービス提供エリア】

全国

【価格】

月額費用 240,000 円 ～

※税別、サービス内容により異なります。

ソリューションの詳細はこちら https://www.spectrum.co.jp/_1306.html

□ お問い合わせ先

ウチダスペクトラム株式会社

TEL 03-5543-6817 (受付時間 平日 9:00 ～ 17:00 土日祝日を除く) e-mail contact@spectrum.co.jp

フォーム https://www.spectrum.co.jp/contact/

所在地: 〒104 - 0033 東京都中央区新川 1 - 16 - 14 アクロス新川ビル アネックス URL: https://www.spectrum.co.jp/

ゼロトラスト
ネットワーク導入・運用サービス

エクシオグループ株式会社

Microsoft 365 でリモート ワークも安心・安全・快適
脱 VPN のゼロトラスト ネットワーク

ゼロトラスト ネットワークとは、VPN 経由の境界線防御のネットワーク構成に対し、VPN を使用せず「ネットワークはすべて危険」という考え方に基づいて、社内外のどこから来た通信であっても、データ アクセス時に必ず認証を行うネットワーク構成になります。
エクシオのゼロトラスト ネットワークは、Microsoft 365 と SIEM を活用して構築します。
セキュリティの不安、通信の不安、管理の不安を解決し、リモート ワークを安心安全快適に行うことができます。

こんな課題をお持ちの方におすすめ!

- セキュリティ不安でリモート ワークに踏み出せない
- リモート ワークに課題(セキュリティ/管理/通信遅滞) がある
- 社内ネットワーク更改を検討

解決

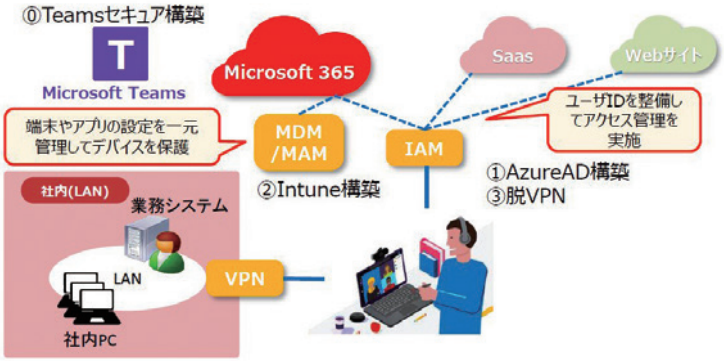
導入効果

- セキュアで快適なリモート ワーク環境構築
- 一元管理により管理者の運用負担を軽減
- AI で不正アクセスなどの脅威に迅速対応
- 専用線や VPN を廃止、運用コスト削減

【サービス内容】

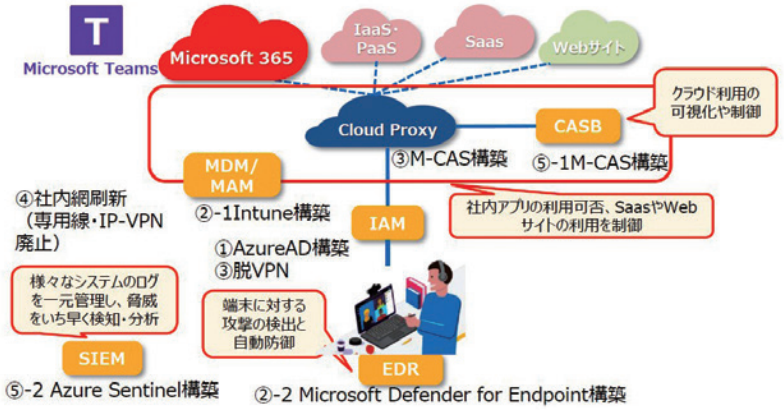
■ セキュア リモート ワーク環境 (脱 VPN : クラウドへ直接アクセス)

リモート ワークで社内ネットワークが遅く Microsoft Teams などを活用できない/リモート ワークをしたいがセキュリティ不安で踏み出せないお客様へ。
クラウドへ脱 VPN のリモート環境を構築し、ストレス フリーのネットワーク環境とシステム管理者の運用負担を実現します。



■ ゼロトラスト ネットワーク環境 (脱社内ネットワーク: すべてクラウド経由)

会社に行かず、社内外を意識せず、業務遂行したいお客様へ。
専用線や VPN を廃止し、すべてクラウド経由の環境を構築します。システムのログを常時監視・分析し、セキュリティ脅威検出を自動化します。



【サービス提供エリア】

全国

【価格】

サービス ① 5,000,000 円 ～
サービス ② 10,000,000 円 ～

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先
エクシオグループ株式会社
e-mail mpn-ict@hqs.exeo.co.jp
フォーム https://www.exeo.co.jp/info/
所在地: 〒150 - 0002 東京都渋谷区渋谷 3 - 29 - 20 URL: https://www.exeo.co.jp/

MSS for Microsoft 365

SBテクノロジー株式会社

SB Technology

メール、ID、エンドポイントをしっかり網羅した コーポレート IT 向けプロフェッショナル SOC サービス

Managed Security Service

当社の専門セキュリティ アナリストが、多岐に渡る Microsoft 365 E5 コンポーネント群から発生したさまざまなログやセキュリティ アラートの相関分析を行い、分析結果だけでなくどのように対応すればよいかといった推奨対策もご提示します。(当社サービス対象コンポーネントに対して) また、必要に応じて脅威の抑制も当社にて実施しますので、より安心できるセキュリティ対応を 24 時間 365 日利用いただくことが可能です。

こんな課題をお持ちの方におすすめ!

自社にセキュリティの専門家が不在で、Microsoft 365 のさまざまなセキュリティ ログの分析や対応を行うことが困難なお客様向け。

解決

導入効果

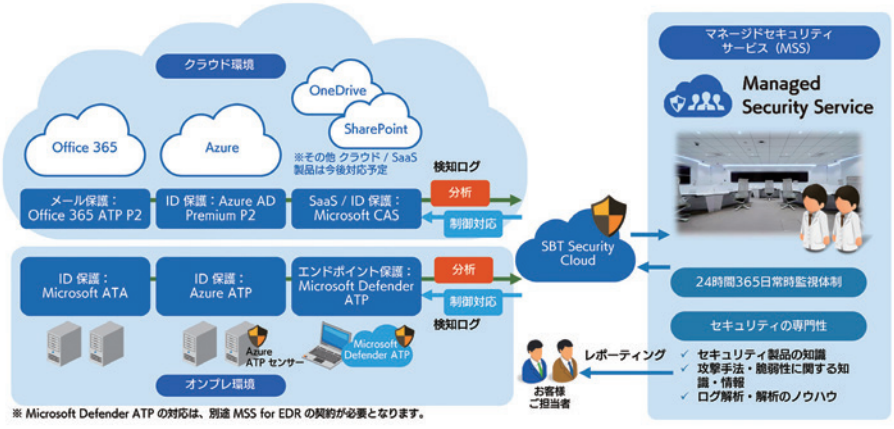
- Microsoft 365 に特化したアナリストによる高クオリティ SOC
- プロフェッショナル チームによる 24 時間 365 日のセキュリティ監視

【サービス内容】

■ MSS for Microsoft 365　～ コーポレート IT のセキュリティは SBテクノロジー にお任せください! ～

・当社のセキュリティ チームがお客様に代わり Microsoft 365 環境を 24 時間 365 日監視します。
・セキュリティ アラートが発生した場合にはその影響度レベルに応じてメールおよび電話にてご連絡します。
・Microsoft 365 コンポーネントで発生したさまざまなログを当社のセキュリティ専門アナリストが相関分析し、事象の報告だけでなく、どのように対応すればよいのか? といった推奨対策案もご提示します。
・単なるセキュリティ監視だけでなく『必要な処置』まで含んだマネージド ディテクション アンド レスポンス (MDR) サービスを提供します。

【サービス対象コンポーネント】
Defender for Office 365 P2、Defender for Cloud Apps、Azure AD Premium P2、Defender for Identity、Defender for Endpoint P2
※ Defender for Endpoint P2 の対応は、別途 MSS for EDR の契約が必要となります。



【サービス提供エリア】
全国

【価格】
オープン価格

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら　https://www.softbanktech.co.jp/service/list/managed-security-service/mss-for-m365/

□ お問い合わせ先
SBテクノロジー株式会社
TEL 03-6892-3154 (受付時間 平日 10:00 ～ 17:00)　e-mail sbt-ipsol@tech.softbank.co.jp
フォーム https://inquiry.softbanktech.co.jp/public/application/add/505?param=49
所在地: 〒160 - 0022 東京都新宿区新宿 6 - 27- 30 新宿イーストサイドスクエア 17F　URL: https://www.softbanktech.co.jp/

MSS for Microsoft Sentinel

SBテクノロジー株式会社

SB Technology

Microsoft Sentinel の利活用を支援する 24 時間 365 日体制のセキュリティ監視サービス

Managed Security Service

SBテクノロジーがこれまで培ってきたクラウドとセキュリティの知見を活かし、Microsoft Sentinel のセキュリティ監視に必要なさまざまな作業をサービスとして提供します。これにより、お客様企業は運用業務の負荷をかけずに Microsoft Sentinel を活用したセキュリティ監視が可能となり、24 時間 365 日いつでも安心できるセキュアな環境を実現することができます。

こんな課題をお持ちの方におすすめ!

セキュリティ専任の担当者が確保できない、知見やノウハウがなく Microsoft Sentinel の導入後の監視が難しいと思っている方におすすめ。

解決

導入効果

Microsoft Sentinel 導入後の、24 時間 365 日体制のセキュリティ監視、セキュリティ専門家によるインシデント分析などの監視業務を提供します。

【サービス内容】

■ SBテクノロジーの運用ノウハウを分析ルールに適用

SBテクノロジーが培ってきたセキュリティ運用のノウハウそのものが Microsoft Sentinel の分析ルールに適用され、自動的に脅威の判定が行われるようになります。また継続的な追加、更新もサービスに含まれます。

■ Microsoft Sentinel の SOAR 機能を活用した自動抑制

Microsoft Sentinel の SOAR (Security Orchestration, Automation and Response) 機能を活用し、検出したアラートの影響度に応じて即時必要な抑制対応も自動的に行われるようになります。

■ セキュリティ アナリストによる詳細調査

アラート発生時の詳細調査をセキュリティ アナリストが実施し、影響範囲の見極め、推奨対応策などを報告いたします。

Microsoft Sentinel

クラウドネイティブな

- セキュリティデータ収集
- 脅威インテリジェンスを活用した脅威の検出
- AIを活用した脅威の調査

×

マネージドセキュリティサービス(MSS)

セキュリティの専門性

- セキュリティ製品の知識
- 攻撃手法・脆弱性に関する知識・情報
- ログ分析、解析のノウハウ

【サービス提供エリア】

全国

【価格】

オープン価格

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://www.softbanktech.co.jp/service/list/managed-security-service/mss-for-azure-sentinel

□ お問い合わせ先

SBテクノロジー株式会社

e-mail sbt-ipsol@tech.softbank.co.jp

フォーム https://inquiry.softbanktech.co.jp/public/application/add/505?param=ms_mss-for-microsoftsentinel

所在地: 〒160 - 0022 東京都新宿区新宿 6 - 27- 30 新宿イーストサイドスクエア 17F URL: https://www.softbanktech.co.jp/

マネージド EDR サービス (Microsoft Defender for Endpoint)

NRIセキュアテクノロジーズ株式会社

エンドポイントを 24 時間 365 日監視することで、Microsoft 製品によるセキュリティ対策を強化

マネージド EDR サービス (Microsoft Defender for Endpoint) は、Microsoft 365 E5 ライセンスにバンドルされる EDR 機能をお客様に代わって監視を行います。サイバー攻撃の能動的な可視化、防御やセキュリティ インシデント発生時の調査、対処を迅速に行うことで組織のサイバー攻撃発生時に検知から隔離対応まで一気通貫でサポートします。

こんな課題をお持ちの方におすすめ!

Microsoft 365 E5 を購入したが EDR 機能を有効活用できていない。EDR のアラートに対してどこまで調査するべきか判断に困る。

解決

導入効果

- セキュリティ専門家による調査と対処
- インシデント対応にかかる時間の削減
- セキュリティをアウトソースし、運用に専念

【サービス内容】

■ スピーディにセキュリティ監視体制を構築

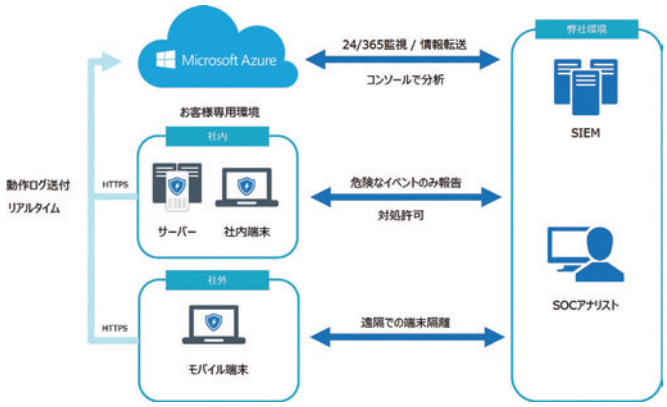
ご利用テナントへアクセス許可を設定いただくだけでマネージド サービス環境を構築することが可能になります。マネージド サービス環境を構築後、セキュリティ アナリストがお客様環境ごとにチューニングを実施します。

■ アラート発生時に何をすべきか明確に

アラートが検出された際に、どこまで調査すべきか判断にお悩みではありませんか。お客様に必要なアラートのみ通知を行うため、アラート対応に工数を費やす必要がなくなります。またリスクに応じた自動隔離や、遠隔からの手動隔離オペレーションを実施します。

■ 高度なスキルを保有した IT セキュリティ アナリストによる監視

セキュリティ モニタリングやインシデント ハンドリングは、セキュリティに関する情報収集と発信を 24 時間 365 日体制で行う、高度セキュリティ資格を保有したセキュリティ アナリスト チームが実施します。



【サービス提供エリア】

全国

【価格】

個別見積もり

ご利用のライセンス、ユーザー数、導入期間・内容などにより、見積もりが変動いたします。

端末 100 台 ～

ソリューションの詳細はこちら https://www.nri-secure.co.jp/service/mss/edr-microsoft

□ お問い合わせ先

NRIセキュアテクノロジーズ株式会社

フォーム https://www.nri-secure.co.jp/service/mss/edr-microsoft

所在地: 〒100 - 0004 東京都千代田区大手町 1 - 7 - 2　東京サンケイビル　URL: https://www.nri-secure.co.jp/

WideAngle マネージドセキュリティサービス

NTTコミュニケーションズ株式会社

Microsoft Defender for Endpoint を活用したエンドポイント セキュリティ対策サービス

サイバー攻撃自体の暗号化やファイルレス マルウェア攻撃などの新たなサイバー脅威の出現、インターネットに PC 端末を直接接続して業務を行うリモート ワークの拡大により、エンドポイントにおけるセキュリティ対策の強化が求められています。そのような中、当サービスでは、セキュリティ オペレーションセンター (SOC) にて、エンドポイント上の Microsoft Defender for Endpoint を活用し、24 時間 365 日、サイバー攻撃を監視、脅威を特定し、遠隔からの感染端末の隔離などの対処を行うことで、被害の拡大を防止します。

こんな課題をお持ちの方におすすめ!

エンドポイントでの脅威検知と分析に加え、侵害された PC 端末の隔離による被害拡大の抑制までを 24 時間 365 日行える運用体制を構築したい。

解決

導入効果

- サイバー攻撃からのエンドポイント保護
- 感染端末の即時隔離による被害拡大の防止
- 24 時間 365 日の高精度な検知と初動対応体制の確立
- サイバー攻撃の監視/特定/対処のお客様業務の負担軽減

【サービス内容】

■ サイバー攻撃からエンドポイントを保護

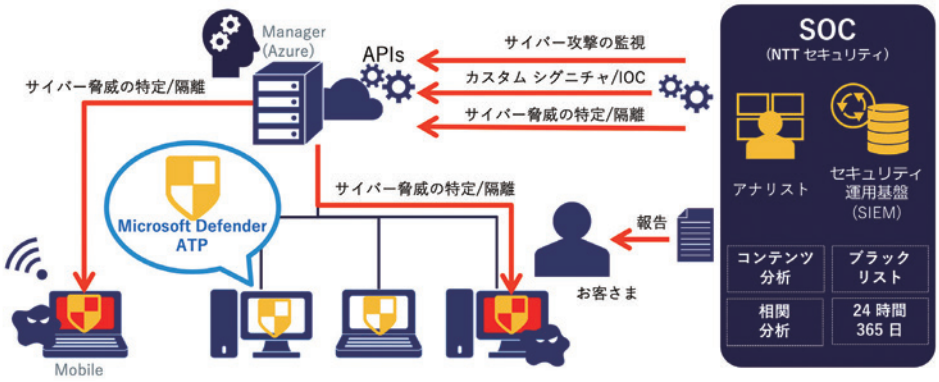
Microsoft Defender for Endpoint を活用し、SOC が PC 端末のアクティビティ (ファイルやプロセスの挙動、レジストリ変更、通信情報など) を監視/分析し、サイバー脅威からエンドポイントを保護します。

■ サイバー攻撃が確認された端末を遠隔から即時隔離

SOC 独自の脅威インテリジェンスや GW セキュリティ製品のアラートとの相関分析を用いた高度な分析により、速やかに感染端末を特定し、アナリストが遠隔から隔離します。これにより、お客様セキュリティ担当者が不在となる、夜間や休日における被害拡大を防止することができます。

■ 24 時間 365 日、サイバー攻撃の監視/特定/対処/報告を実施

経験豊富なアナリストが、独自の SIEM やブラックリスト、カスタム シグネチャ/IOC を駆使し、リアルタイムに相関分析/コンテンツ分析を行い、24 時間 365 日、サイバー脅威を特定、対処します。これにより、高精度な検知力と迅速な初動対応、お客様業務の軽減が実現できます。



【サービス提供エリア】

全国

【価格】

お問い合わせください

ソリューションの詳細はこちら https://www.ntt.com/business/services/security/security-management/wideangle.html?msatp2020

□ お問い合わせ先

NTTコミュニケーションズ株式会社

フォーム https://www.ntt.com/business/services/security/security-management/wideangle.html?msatp2020

URL: https://www.ntt.com

Office 365
アカウント脅威分析サービス

株式会社大塚商会

株式会社 大塚商会

まず狙われる! わかりやすいターゲットである、アカウントの確認から始めませんか?

Office 365 ご利用の際に必要で、狙われやすい Office 365 アカウント。このアカウントの基盤となっている Azure Active Directory への攻撃やリスクを分析し、ご報告します。

こんな課題をお持ちの方におすすめ!

Outlook on the Web をご利用、海外出張のメンバーが多い、など Office 365 アカウントの漏えい、管理が心配なお客様。

解決

導入効果

Office 365 アカウントの利用はもちろん、失敗の状況やリスクが確認できます。リスクに対し必要となる運用面での対策/適切なセキュリティ強化範囲やコスト検討が可能となります。

【サービス内容】

■ アカウント脅威分析　準備サービス

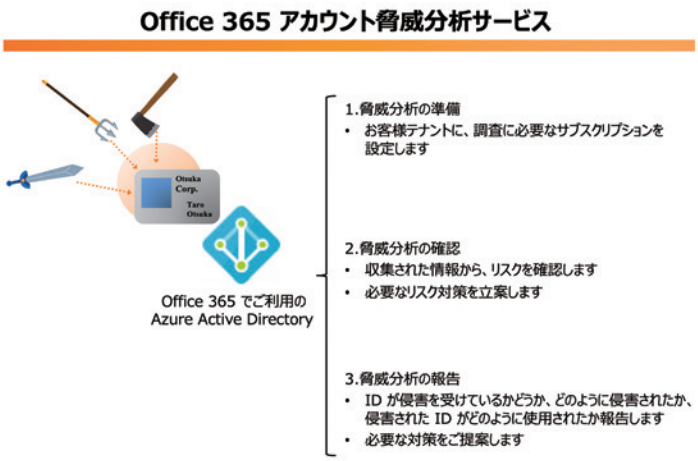
Microsoft 365 E5 (EMS E5) のトライアル ライセンスを、お客様テナントに適用します。

■ アカウント脅威分析　確認サービス

採取された情報から、リスクを確認するとともに、セキュリティ対策の提案を日々行う技術者が、お客様に必要と思われる対策を立案します。

■ アカウント脅威分析　報告サービス

お客様先に訪問し、分析結果および必要と思われる対策をご報告します。



【サービス提供エリア】

関東、近畿地方

【価格】

ID 数により、個別見積もり

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先

株式会社大塚商会

TEL 0120-579-215 (受付時間 平日 9:00 ～ 17:30)

フォーム https://www.otsuka-shokai.co.jp/contact/forms/products/tayoreru/office365/inquiry/index.php

所在地: 〒102 - 8573 東京都千代田区飯田橋 2 - 18 - 4　URL: http://www.otsuka-shokai.co.jp

Azure 振舞い監視サービス

株式会社Colorkrew

colorkrew

Microsoft Sentinel によるセキュリティ監視サービス

Sentinel を利用して、Azure 内で発生した「サイバー攻撃」、「不審な振舞い」、「重大な影響をおよぼす作業」、「VM の脆弱性」などを検知します。検知された情報は、ご指定のメールアドレスや Microsoft Teams / Slack などのチャンネルに通知されるほか、Colorkrew 認証システム Mamoru PUSH との連携 (オプション) により、不審な振舞いをしたユーザーの認証レベルを強化または利用停止することも可能です。

こんな課題をお持ちの方におすすめ!

■ セキュリティにおける、未知の脅威への対策を探している
■ Azure 環境で正しいコンプライアンスが保たれているか監視したい

解決

導入効果

■ ユーザーの振る舞いを分析することで、未知の脅威や内部犯行を監視します
■ 構成や設定情報、脆弱性の有無をチェックすることで、コンプライアンス レベルを監視します

【サービス内容】

■ Azure WAF が検知した危険なアクセス

WAF が攻撃者をブロックした場合、もしくは攻撃者のアクセスが成功した場合 (WAF でブロックされた攻撃者の IP アドレスが、別のアクセスに成功した場合)、アラートが上がります。

■ Azure での不審な振舞い

Azue Portal 上の不審な振舞い (普段利用しない IP からのアクセスなど) や、重大な影響をおよぼす作業 (リソース削除、サービス停止など) があった場合、アラートが上がります。

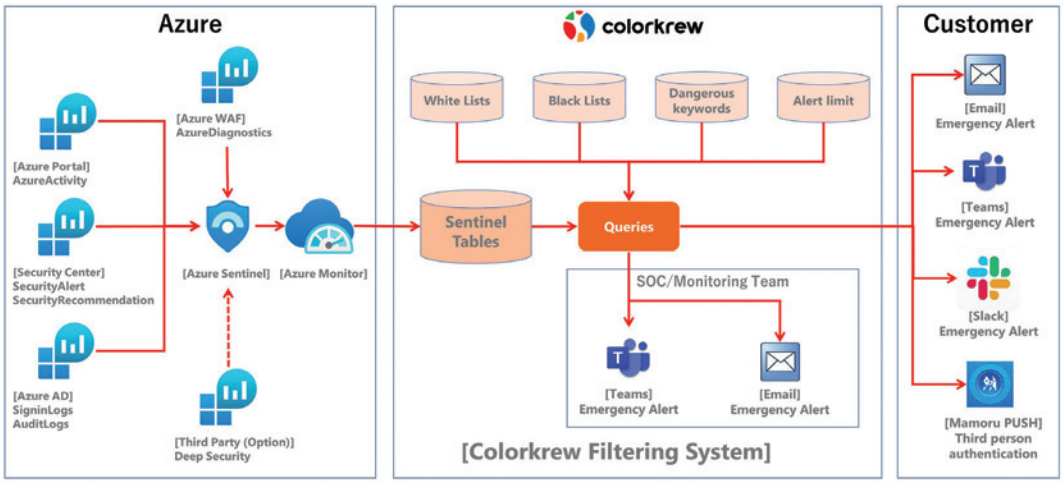
■ Mamoru PUSH によるセキュリティ レベルの強化

Colorkrew 認証システム Mamoru PUSH との連携 (オプション) により、不審な振舞いをしたユーザーの認証レベルを強化または利用停止することが可能です。

■ VM の脆弱性情報と対策

VM の脆弱性が発見された場合、アラートが上がります。

システム概要



【サービス提供エリア】

全国

【価格】

初期費用: 500,000 円 ～
運用費用: 400,000 円 ～

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://kuramane.colorkrew.com/logfilter/sentinel/

□ お問い合わせ先

株式会社Colorkrew

TEL 03-5825-9339 (受付時間 平日 10:00 ～ 18:00) e-mail salesproject_all@colorkrew.com
フォーム https://kuramane.colorkrew.com/mailform-pardot/
所在地: 〒111 - 0053 東京都台東区浅草橋 5 - 20 - 8 CSタワー7F URL: https://www.colorkrew.com/

Microsoft 365 E5 導入支援サービス

株式会社クラウドネイティブ

Microsoft 365 E5 を中心に、今実現できる最もセキュアで利便性の高いシステムの実装をご提案

「ゼロトラスト アーキテクチャ」の概念をもとに、Microsoft 365 E5 を中心として、今実現できる最もセキュアで利便性の高いシステムの実装をご提案します。お客様の Microsoft 365 E5 導入による価値を享受するまでの時間を圧縮することで導入企業のセキュリティ運用を加速させます。

こんな課題をお持ちの方におすすめ!

Microsof 365 E5 の導入を検討しているが、価値を享受するまでの学習コストによってビジネス速度への影響を懸念されているお客様。

解決

導入効果

Microsoft 365 E5 導入による価値を享受するまでの時間が圧縮され、導入企業にノウハウが蓄積されるため、導入以降のセキュリティ運用が加速します。

【サービス内容】

■ 実装の最適化に向けたサポート

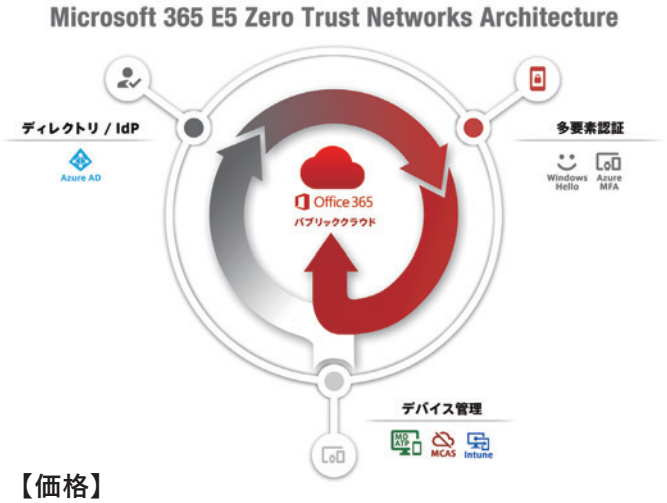
お客様環境と運用体制のヒアリングを通じて、Microsoft 365 E5 を活用することで実現できるセキュリティのカバレッジを意識共有します。
Microsoft 365 E5 の各種機能を実装するうえで必要な情報のご提供と、スムーズな運用開始に向けた作業工程を提示します。

■ 基本設定のサポート

Microsoft 365 E5 で利用可能な各機能が、事前に定義したセキュリティのカバレッジに対して十分に作用するよう、基本設定の実施をサポートします。
導入企業にノウハウとして蓄積されるよう、基本設定の実施を通じて、各種設定を理解していただきます。

■ 運用業務のサポート

Microsoft Sentinel を中心にした、アラーティングやチケット管理、インシデント/レスポンスを促進するインタラクティブなエンリッチメントの実装支援を行い、導入企業に運用ノウハウが蓄積されるようアラート対応の手ほどきを行います。



【サービス提供エリア】

全国

【価格】

月額費用 1,000,000 円 ～

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先

株式会社クラウドネイティブ

TEL 050-1744-0150 (受付時間 平日 10:00 ～ 19:00) e-mail info@cloudnative.co.jp
フォーム https://cloudnative.co.jp/contact/
所在地: 〒104 - 0053 東京都中央区晴海 3 - 10 - 1 Daiwa 晴海ビル 2F URL: https://cloudnative.co.jp/

Microsoft 365 を活用した セキュリティ態勢構築支援サービス

KPMGコンサルティング株式会社

多岐にわたるセキュリティ対策の高度化を支援します。

セキュリティの脅威は日々増大しており、どのように防ぐかに加え、いかに早期に検知して対応するかが喫緊の課題となっています。KPMG は、Microsoft 365 などの最新ソリューションを活用し、防御策の強化とともに、モニタリングやインシデント レスポンスの体制、プロセス改善を含めたセキュリティ オペレーション エクセレンスの確立を支援します。

こんな課題をお持ちの方におすすめ!

- 脅威のトレンドに合わせて個別対応しているため、対策の重複や抜け漏れがある
- リモートワークを前提としたシステムへの移行に伴い、対策を再設計する必要がある
- 監視不足などにより、常にリアクティブなインシデント対応となってしまっている

解決

導入効果

- セキュリティ対策の最適化
- ユーザーと部門を巻き込んだセキュリティ改革
- 監視態勢、インシデント対応プロセスの高度化

【サービス内容】

■ Microsoft 365 導入効果のクイック アセスメント

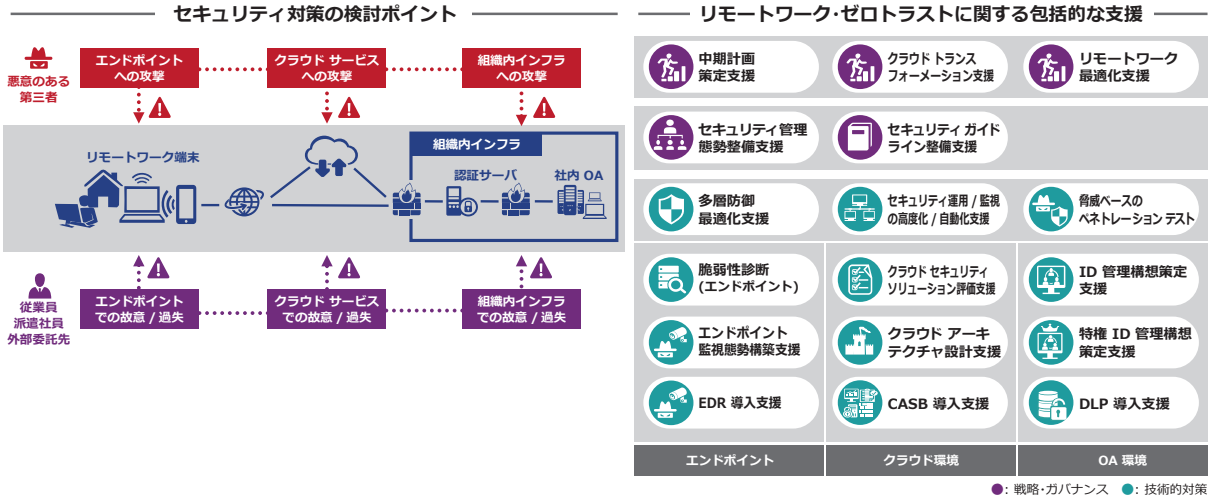
最新セキュリティ脅威を基に既存対策の課題を分析するとともに、Microsoft 365 を導入した場合の効果を、セキュリティ対策の有効性、コストの観点で短期間でアセスメントします。

■ Microsoft 365 を活用したゼロトラスト対策の構築支援

ゼロトラスト対策の導入計画の策定から、ポリシー設計、運用体制 / プロセス整備、インシデント対応態勢整備、ユーザー教育までトータルで支援します。

■ Microsoft 365 を活用したセキュリティ監視態勢の構築支援

Microsoft Defender や Microsoft Sentinel などを活用し、日々進化する脅威に対抗するためのセキュリティ監視態勢の強化を支援します。



【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先

KPMGコンサルティング株式会社

TEL 03-3548-5111 e-mail kc@jp.kpmg.com

所在地: 〒100 - 0004 東京都千代田区大手町 1 - 9 - 7 大手町フィナンシャルシティ サウスタワー URL: http://home.kpmg/jp/kc

WafCharm

株式会社
サイバーセキュリティクラウド

CYBER SECURITY CLOUD

Azure WAF の運用を自動化して、業務負荷を軽減!

WafCharm

WafCharm は、世界中の Web に対する攻撃パターンを学習し、Azure WAF をはじめとしたパブリック クラウドの WAF ルールを最適化させる WAF 自動運用サービスです。
専門的な知識がなく WAF のルール作りやルールの網羅性に不安がある方や、新規脆弱性に対応する余裕が無い方の運用の不安を解消します。

こんな課題をお持ちの方におすすめ!

Azure WAF 専任の運用人材を用意できなかったり、最適なルール作り、新規脆弱性対応のリソースがない方におすすめです。

解決

導入効果

- WafCharmが最適なルールを適用
- 新規脆弱性も、専任リサーチャーが監視
- 誤検知対応もサポートにお任せください
- 面倒な WAF 運用から解放されます

【サービス内容】

■ WafCharm が最適なルールを適用

自動で最適なルールを Azure WAF に適用するので、ルール作りはすべてお任せ。
カスタマイズや新規でルールの作成が必要な場合も、WafCharm が対応します。

■ 簡単導入で、充実の運用サポート

導入は簡単で即時可能。運用のサポートも充実しているので、専任の人材をご用意する必要はありません。
新規脆弱性にも、当社の専任リサーチャーが迅速に対応するので、安心。

■ 日本語サポートでいつでも安心

24 時間 365 日の日本語による技術サポートで、誤検知や万が一のトラブル発生時もすぐに対応するので安心。
(※エントリープランは、サポート時間に制限あり)

■ 初期費用 0 円、月額 5,000 円から利用可能

明確な定額の料金体系で月額 5,000 円から利用可能です。コストを抑えながらも強固なパブリック クラウドの WAF 運用を実現できます。
30 日間の無料トライアルも可能。

【サービス提供エリア】

全国

【価格】

月額 5,000 円 〜 (ウェブリクエスト数に応じて「エントリー」「ビジネス」「エンタープライズ」の 3 種類のプランがあります)　※ 初期費用 0 円

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら　https://www.wafcharm.com/

□ お問い合わせ先
株式会社サイバーセキュリティクラウド
フォーム https://www.wafcharm.com/contact/
所在地: 〒150 - 0011 東京都渋谷区東 3 - 9 - 19 VORT 恵比寿 maxim 3F　URL: https://www.cscloud.co.jp/

CEC SOC for Microsoft Defender for Endpoint

株式会社シーイーシー

CEC
Computer Engineering & Consulting

CEC SOC

Microsoft Defender for Endpointを 24 時間 365日監視 / 運用

24 時間 365 日対応可能な Microsoft Defender for Endpoint のセキュリティ監視 / 運用サービスです。Microsoft Defender for Endpoint だけではなく、Microsoft Defender for Endpoint のイベントと周辺機器 (サーバーやネットワーク機器など) のログを相関的に分析し、インシデント対応を迅速に行います。サービス内容についてはお客様ごとにカスタマイズ可能です。

こんな課題をお持ちの方におすすめ!

- ■ セキュリティのノウハウを持った人材がいない
- ■ 周辺機器も含めて監視してほしい
- ■ 自社にあった SOC サービスが見つからない

解決

導入効果

- ■ 専門アナリストによる解析と迅速な対応
- ■ 周辺機器のイベントと相関的に分析
- ■ サービスはお客様毎にカスタマイズ可能

【サービス内容】

■ 専門アナリストによる監視 / 運用

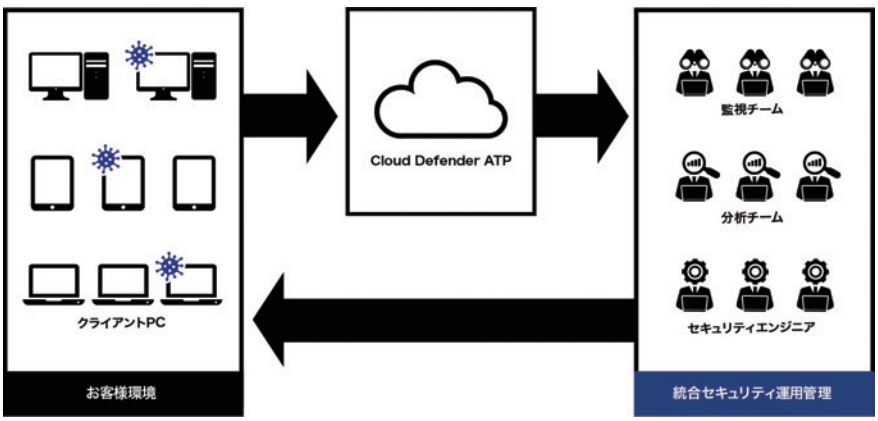
24 時間 365 日の監視 / 運用体制で、Microsoft Defender for Endpoint のセキュリティ イベントを監視します。お客様が不在の時間帯でもインシデント対象 PC をネットワークから隔離することが可能です。

■ セキュリティ インシデントの検出状況を月次レポートで報告

これまで把握することができなかった、セキュリティ インシデントおよびセキュリティ アラートの検出状況を詳細に分かりやすくレポート形式で報告します。

■ 賠償額最大 1 億円のサイバー リスク保険

賠償額最大 1 億円の「サイバー リスク保険」を、追加費用なしで付帯できます。
お客様は安心してサービスをお使いいただけます。



【サービス提供エリア】
全国

【価格】
オープン価格

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://security.cec-ltd.co.jp/soc_microsoft_defender_atp/

□ お問い合わせ先
株式会社シーイーシー
TEL 03-5783-3162 (受付時間 平日 9:00 ～ 17:45) e-mail pabg-marketing@cec-ltd.co.jp
フォーム https://security.cec-ltd.co.jp/contact/
所在地: 〒108 - 6012 東京都港区港南 2 - 15 - 1 品川インターシティA棟 12F URL: https://security.cec-ltd.co.jp/

Microsoft Defender for Endpoint 運用サービス

ＪＢサービス株式会社

Microsoft Defender for Endpoint が脅威を検知した際の「初動対応」をご支援します

Microsoft Defender for Endpoint が検知した脅威をお客様のご担当者様にお知らせし、該当端末をネットワークから隔離することで、セキュリティ インシデントに対する初動対応をご支援します。
また、隔離後はお客様にて安全が確認された後、ネットワークへの再接続作業を代行いたします。

こんな課題をお持ちの方におすすめ!

■ セキュリティ脅威が発生した場合に、すばやく初動対応を実施したい
■ セキュリティ脅威発見時にまずは危険な端末の隔離を実施したい

解決

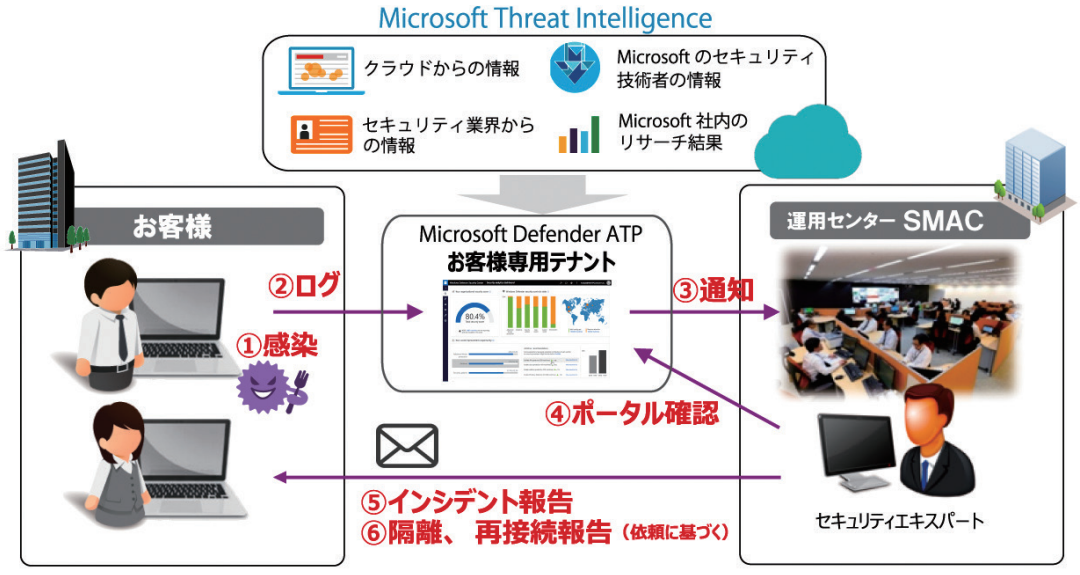
導入効果

Microsoft Defender for Endpoint が検知した脅威を正しく「知る」ことができ、適切な「初動対応」が可能になります。

【サービス内容】

■ 脅威を正しく「知る」ことと最初の「対応」をご支援します

Microsoft Defender for Endpoint が検知した脅威をお客様のご担当者様にすばやくお知らせし、お客様からの依頼に基づき、脅威が発見された端末をネットワークから隔離します。これによりお客様環境内におけるマルウェアの拡散を予防することで、安全に業務を継続することが可能となります。
また、お客様にて端末の再インストール等により、安全が確認された後、ネットワークへの再接続作業を代行いたします。



【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先
ＪＢサービス株式会社
e-mail jbs_security@jbsvc.co.jp
フォーム https://www.jbsvc.co.jp/contactus.html
所在地: 〒160 - 0022 東京都新宿区新宿 4 - 2 - 23 新四 curumu ビル 11F URL: https://www.jbsvc.co.jp/

セキュリティ最適化支援サービス

ＪＢＣＣ株式会社

セキュリティ環境調査と脅威 PoC にてリスクの洗い出しを行い セキュリティ全体最適化ロードマップを作成

お客様のセキュリティ環境をヒアリング、さらに Office 365 利用時における現状のリスクを「脅威可視化 PoC」にて実環境でアセスメントを実施します。リスクの洗い出しから対策の重要性と優先度を決め、お客様に適した対策ロードマップとしてご提案します。本サービスの提供後、ご要望に応じてマイクロソフト セキュリティを始めとするソリューションを活用した構築/運用支援までをワンストップでご支援することも可能です。

こんな課題をお持ちの方におすすめ!

自社の Office 365 利用状況、システム全体のリスク度合いを評価しセキュリティ対策検討を進めたいが、現状把握の手法や進め方が分からない。

解決

導入効果

■ 自社が抱えるセキュリティ リスクの現状理解と対策案の確立、中長期的なセキュリティ実装計画の策定
■ 対策優先度に則り計画的にセキュリティ対策を進めることができる

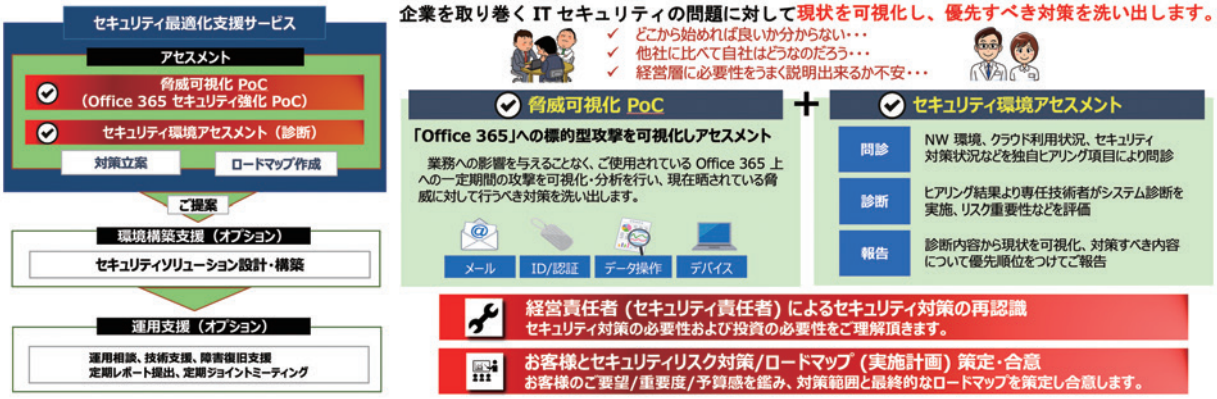
【サービス内容】

■ アセスメント サービス (脅威可視化 PoC & セキュリティ環境アセスメント)

ご使用されている Office 365 上への一定期間の攻撃を可視化/分析し、システム管理者が気付いていない現在晒されている脅威に対して行うべき対策をご提案します。
お客様システム環境全体のヒアリングとセキュリティ視点のアセスメントを実施。セキュリティ環境最適化へ向けた対策をロードマップを作成しご提案します。

■ [オプション] 環境構築支援/運用支援サービス

セキュリティ最適化支援サービスによるアセスメントの実施後、別途弊社にて構築/運用フェーズのご支援が可能です。
・マイクロソフト セキュリティを始めとするソリューションを活用した構築支援サービスをご提供
・導入後の運用相談、技術支援、障害復旧支援、定期レポート提出、定期ジョイント ミーティングなどを運用サービスとしてご支援



【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先
ＪＢＣＣ株式会社
TEL 03-5714-5346（受付時間 平日 9:00 ～ 17:00 土日祝日、および年末年始 12/30 ～ 1/4、その他会社休日などを除く）
e-mail service@web.jbcc.co.jp
所在地: 〒144 - 8721 東京都大田区蒲田 5 - 37 - 1 ニッセイアロマスクエア 15F URL: https://www.jbcc.co.jp/

SoftwareONE
マネージド 365 セキュリティ

SoftwareONE Japan株式会社

Microsoft 365 をご利用のお客様のセキュリティ運用をグローバルで実現

お客様のセキュリティ策定に応じ、Microsoft 365 でのセキュリティ対策をデプロイし、セキュリティ オペレーション センターでの 24 時間 365 日対応でセキュリティ専門のアナリストがログを分析し、的確な推奨対応事項を提示します。
多発する社内システム セキュリティ侵害を抑制し、ご担当者様の負担を軽減、メイン業務を圧迫しない運用づくりをお手伝いします。

こんな課題をお持ちの方におすすめ!

- ■ セキュリティに対応する人材が足りない
- ■ リスクを軽減し、セキュリティ課題への時間とコストを削減したい
- ■ グローバルでセキュリティを運用したい

解決

導入効果

- ■ 専門のアナリストがログを的確に分析します
- ■ セキュリティ課題への時間とコストを削減します
- ■ グローバル拠点でお客様をサポートします

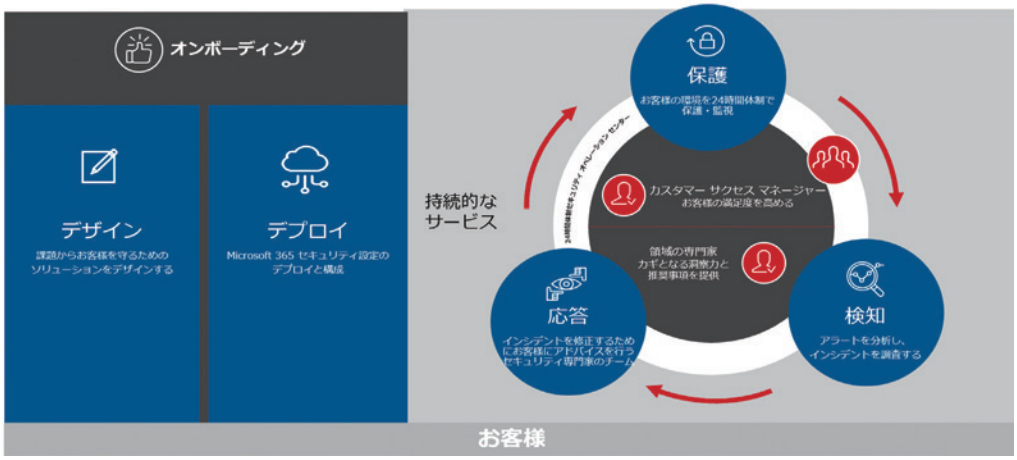
【サービス内容】

■ セキュリティ策定に応じたデプロイメント
お客様のセキュリティ策定から、セキュリティ ポリシー、ルール、設定、アラートを構成します。

■ セキュリティ オペレーション センターでの 24 時間 365 日対応
セキュリティ専門のアナリストがログを分析し、的確な推奨対応事項を提示します。

■ カスタマー サクセス マネジャーによるサポート
選任の担当者による定期的なレポートと推奨の提示をします。

マネージド365セキュリティのアプローチ



【サービス提供エリア】
全国

【価格】
お問い合わせください

ソリューションの詳細はこちら https://www.softwareone.com/ja-jp/solutions/managed-security/managed-365-security

□ お問い合わせ先
SoftwareONE Japan株式会社
TEL 03-5369-0140 (受付時間 平日 9:00 ～ 17:30) e-mail marketing.jp@softwareone.com
フォーム https://www.softwareone.com/ja-jp/solutions/managed-security/managed-365-security
所在地: 〒162 - 0067 東京都新宿区富久町 16 - 6 西倉LKビル 9F URL: https://www.softwareone.com/ja-jp/

Microsoft Defender for Endpoint 監視サービス

株式会社ソフトクリエイト

SOFT CREATE

Microsoft Defender for Endpoint を活用した エンドポイント セキュリティ監視サービス

サイバー攻撃自体の暗号化やファイルレス マルウェア攻撃などの新たなサイバー脅威の出現、コロナ禍によるテレワークの拡大により、エンドポイントにおけるセキュリティ対策の強化が求められています。
そのような中、当サービスでは、セキュリティ オペレーション センター (SOC) にて、エンドポイント上の Microsoft Defender for Endpoint を活用し、24 時間 365 日、サイバー攻撃を監視、脅威を特定し、影響度の高い脅威に対して端末の隔離 (対処) を行うことで、被害の拡大を防止します。

こんな課題をお持ちの方におすすめ!

- ■ 自社にセキュリティ専門家が不在で、セキュリティログの分析や対応を行うことが困難なお客様
- ■ テレワーク環境におけるセキュリティ対策/強化が必要なお客様
- ■ 社員のリテラシーが浸透化できていないお客様

解決

導入効果

- ■ サイバー攻撃からのエンドポイント保護
- ■ 感染端末の即時隔離による被害拡大の防止
- ■ 24 時間 365 日の高精度な検知、脅威レベルにおける体制の確立
- ■ サイバー攻撃の監視 /特定 / 対処のお客様業務の負担軽減

【サービス内容】

■ サイバー攻撃からエンドポイントを保護

Microsoft Defender for Endpoint を活用し、SOC が PC 端末のアクティビティ (ファイルやプロセスの挙動、レジストリ変更、通信情報など) を監視 /分析し、サイバー脅威からエンドポイントを保護します。

■ サイバー攻撃が確認された端末を遠隔から即時隔離

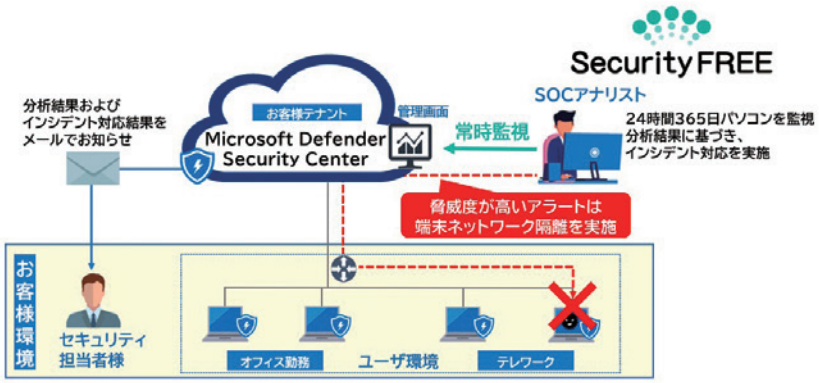
SOC 独自の高度な分析 (脅威レベルに応じた対処) により、速やかに感染端末を特定し、アナリストが遠隔から隔離します。これにより、お客様セキュリティ担当者が不在となる、夜間や休日における被害拡大を防止することができます。

■ 24 時間 365 日、サイバー攻撃の監視 / 検知 / 対処 / 報告を実施

経験豊富なアナリストが、独自の SIEM やブラック リスト、カスタム シグネチャ / IOC を駆使し、リアルタイムに相関分析 / コンテンツ分析を行い、24 時間 365 日、サイバー脅威を特定、対処します。これにより、高精度な検知力と迅速な初動対応、お客様業務の軽減が実現できます。

■ Active Directory 監視サービスとの併用可能

Active Directory監視サービスとの併用により、企業を狙った攻撃者の対策がより強固になり、被害拡大を防止することができます。



【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先

株式会社ソフトクリエイト

TEL 03-3486-1520 (受付時間 平日 9:00 ～ 18:00) e-mail sc-contact@softcreate.co.jp
フォーム https://www.softcreate.co.jp/solution/security/apply
所在地: 〒150 - 0002 東京都渋谷区渋谷 2 - 15 - 1 渋谷クロスタワー URL: https://www.softcreate.co.jp/

マネージドセキュリティサービス

ソフトバンク株式会社

SoftBank

セキュリティ監視 / 分析 / 対処の統合窓口

マネージドセキュリティサービス (MSS) は 24 時間 365 日体制で当社のさまざまなサービスに対するセキュリティ監視 / 分析 / 対処の統合窓口を提供するサービスです。

こんな課題をお持ちの方におすすめ!

サイバー攻撃が高度化する中で、ネットワークからエンドポイントまで横断的かつ実際に侵害を許した場合の検知、対処を想定した体制を構築したい

解決

導入効果

ネットワークからエンドポイントまで統合的に監視し、経験豊富なアナリストによる調査およびインシデントによる被害の封じ込めを実施いたします

【サービス内容】

■ ワンストップ提供

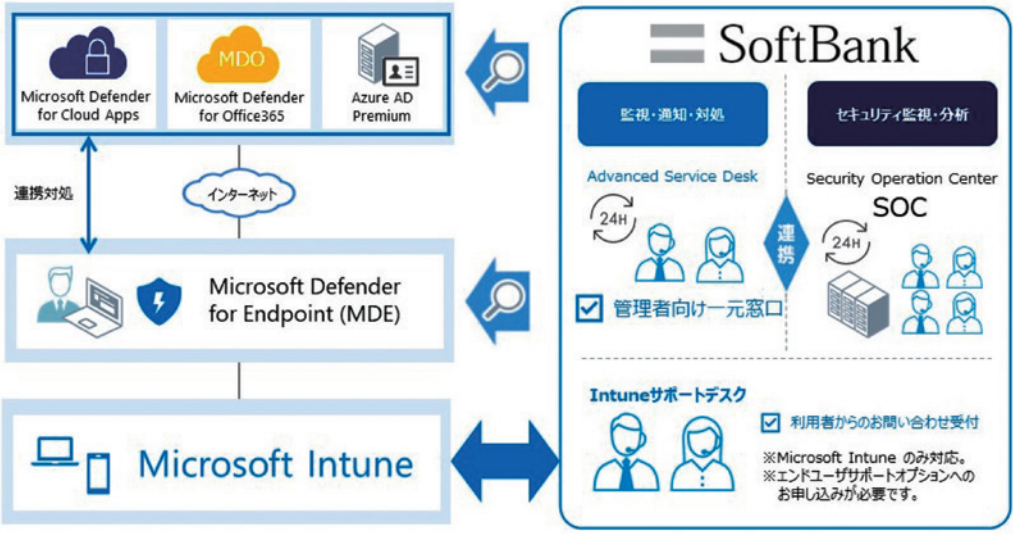
ネットワーク運用に加えてセキュリティ運用をソフトバンクの窓口にて一元対応

■ ゲートウェイ サービスとの統合窓口

Microsoft 365 に加え、ゲートウェイ サービスを含めた統合窓口を提供

■ 緊急遮断を含む初動対応を自動対処

アラート検知時、自動で緊急遮断対応や日本語での通知などの初動対応を実施することで、迅速な対応を提供



【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://www.softbank.jp/biz/security/mss/sbmss/

□ お問い合わせ先

ソフトバンク株式会社

フォーム https://tm.softbank.jp/form/security/mss/index.php

所在地: 〒105 - 7529 東京都港区海岸 1 - 7 - 1 東京ポートシティ竹芝オフィスタワー URL: https://www.softbank.jp/biz/

セキュリティ監視サービス for IoT / OT

株式会社ソリトンシステムズ

セキュリティ監視サービス for IoT/OT

IoT/OT 資産のアセスメントを実施し、脆弱性分析に基づきセキュリティ品質を向上、お客様の情報資産を守ります。

・可視化により課題が明確になります。
・PCAP ファイルを分析することにより、現状把握が簡単に実現できます。
・クラウド、オンプレ、エアギャップ ネットワークなど IoT/OT 環境の形態を問わず導入をサポートします。
・小規模 (監視対象 100 デバイス) から始めて段階的に監視対象を広げることができます。
・IoT デバイスのファームウェア脆弱性を洗い出し、開発サイクルの品質向上をサポートします。

こんな課題をお持ちの方におすすめ!

■ サプライチェーン攻撃や情報漏洩といった、組織のセキュリティリスクを排除したい
■ SOC / CSIRT を運用したいが人員の確保が難しい
■ 取扱製品のソフトウェア脆弱性を調べたい

解決

導入効果

■ アセスメントと継続監視により情報資産を保護
■ 経験豊富なエンジニアが SOC / CSIRT 運用を代行
■ ソフトウェアの脆弱性診断

【サービス内容】

■ IoT / OT 環境のアセスメントと継続監視

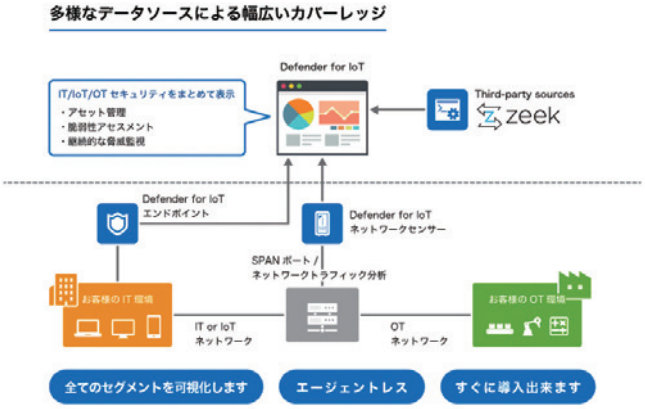
IoT/OT 環境のアセスメントを行い、ネットワークとそれにつながるデバイスを明らかにします。そして、継続監視を行い定常状態を把握することによって、インシデントの発生をリアルタイムに検知します。一連の作業はパッシブに行われ、既設のシステムを停止させるような心配はありません。

■ SOC / CSIRT 運用支援

日常の監視業務からインシデント発生時の対応まで、弊社の経験豊富なエンジニアが貴組織の SOC / CSIRT 運用を代行します。

■ ソフトウェア脆弱性診断

IoT / OT 機器のソフトウェア脆弱性診断を行います。機器のファームウェアを直接診断するので、ソースコードは不要です。CVE / CWE の検出、SBOM (ソフトウェア部品表) の自動生成などを行います。



【サービス提供エリア】
全国

【価格】
お問い合わせください (例: 100 デバイス年契約 200,000 円〜)

ソリューションの詳細はこちら https://www.soliton-cyber.com/all-services/defender-for-iot

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先
株式会社ソリトンシステムズ サイバー&コンサルティング事業部
e-mail public-safety@list.soliton.co.jp
所在地: 〒160 - 0022 東京都新宿区新宿 2 - 4 - 3 URL: https://www.soliton.co.jp/

Microsoft Sentinel 向け活用サービス

TIS株式会社

スピード導入/コスト最適化が実現する「次世代型クラウド ネイティブ SIEM」の活用をトータル支援

「Microsoft Sentinel 向け活用サービス」は、Office 365 や Microsoft Azure などのサービスを活用し「各種セキュリティ製品のログ監視/運用を検討している」「SIEM の有効活用やインシデント対応を自立運用したい」という課題を持つ企業向けに「Microsoft Sentinel」の導入に向けたアセスメント、設計、実装、運用の各フェーズで支援を提供するサービスです。

こんな課題をお持ちの方におすすめ!

SIEM 導入/運用する人材がいない、ログが際限なくたまる、大量のアラート ログからの脅威検出と対処が難しいなどの課題を持っている企業。

解決

導入効果

- 短期間での SIEM 導入が可能
- 検知ルールの最適解を提供することで運用工数を削減
- SIEM 運用だけでなく SOC や CSIRT 運用などお客様に合わせた支援が可能

【サービス内容】

■ アセスメント サービス

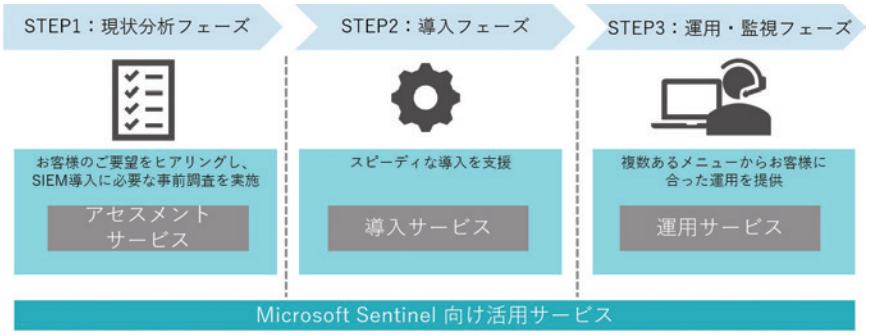
Microsoft Sentinel の導入検討企業に対し、TIS の技術コンサルタントが現状のセキュリティ運用状況や、導入で実現したい要件などをヒアリングし、要件に沿った導入や体制のイメージ、導入ステップの提示などのアセスメントを実施します。

■ 導入サービス

Microsoft Sentinel の導入支援を行います。自社運用をする場合は、構築や操作説明などのナレッジ トランスファーも行います。また、試用や検証を目的とした部分導入を希望する企業向けのパッケージもご用意し、個別の要件に柔軟に対応します。

■ 運用サービス

Microsoft Sentinel 導入後の運用を実施します。SIEM 運用で課題となるインシデント対応時のログの調査および状況の可視化を実現し、継続的なルールのアップデートを支援します。



【サービス提供エリア】

全国

【価格】

お問い合わせください

ソリューションの詳細はこちら https://www.tis.jp/service_solution/microsoftazure/azuresentinel/

□ お問い合わせ先

TIS株式会社

TEL 050-1702-4063 (受付時間 平日 9:00 ～ 12:00、13:00 ～ 17:00) e-mail ps-info@ml.tis.co.jp

フォーム https://www.tis.jp/inq/01_01/?solt=s0400

所在地: 〒135 - 0061 東京都江東区豊洲 2 - 2 - 1 豊洲ベイサイドクロスタワー URL: https://www.tis.co.jp

Microsoft 365 E5 Security 導入サービス

TIS株式会社

TIS INTEC Group

Microsoft 365 E5 ライセンスに含まれるセキュリティ機能で標的型攻撃のリスクを低減!

「Microsoft 365 E5 Security 導入サービス」では、Microsoft 365 E5 のライセンスで利用できる EDR (Endpoint Detection and Response)、CASB (Cloud Access Security Broker) といった先端のセキュリティ対策を導入することで、未知のマルウェアによる標的型攻撃のリスクを低減します。

こんな課題をお持ちの方におすすめ!

- マルウェアによる標的型攻撃への対策ができていない
- クラウドサービスの利用が統制できていない
- ゼロトラスト環境への移行を検討している

解決

導入効果

- EDR やメール セキュリティでマルウェアによる標的型攻撃に対策
- CASB でシャドー IT 対策
- 将来的なゼロトラスト環境の構築を想定した段階的な展開が可能

【サービス内容】

■ アセスメント サービス

Microsoft 365 E5 導入検討企業に対し、TIS の技術コンサルタントが現状のセキュリティ運用状況や、導入で実現したい要件などをヒアリングし、要件に沿った導入や体制のイメージ、導入ステップの提示などのアセスメントを実施します。

■ 導入サービス

Microsoft 365 E5 に含まれるセキュリティ対策の導入支援を行います。自社運用をする場合は、構築や操作説明などのナレッジ トランスファーを行います。

■ サポート サービス

運用開始後に発生する技術的な質問に回答する QA サービスを提供し、TIS が運用面を支援します。また、EDR や SIEM 製品に関しては、当社を窓口とした MSS (Managed Security Service) が提供可能です。

【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先

TIS株式会社

TEL 050-1702-4063 (受付時間 平日 9:00 ～ 12:00、13:00 ～ 17:00) e-mail ps-info@ml.tis.co.jp

フォーム https://www.tis.jp/inq/01_01/?solt=s0400

所在地: 〒135 - 0061 東京都江東区豊洲 2 - 2 - 1 豊洲ベイサイドクロスタワー URL: https://www.tis.co.jp

セキュリティ デスク サービス
Office 365 脅威対策アセスメント サービス

株式会社TOSYS

「セキュリティ強化」と「多様な働き方」を同時解決。
新時代のセキュリティ対策をご支援します。

国内でトップクラスの脅威対策アセスメント実施実績を誇る TOSYS が、Microsoft 365 E5 などに含まれるセキュリティ ツールを最適な状態で運用できるよう、モニタリング、セキュリティ分析対応、各種設定などを支援します。在宅勤務や BYOD など多様な働き方に対応したセキュリティ環境の整備や働き方改革の実現に寄与します。
お客様の Office 365 環境にて不正アクセスや標的型攻撃の状況チェックなど、セキュリティの健康診断を行います。

こんな課題をお持ちの方におすすめ!

■ 在宅ワークを推進したいが、社外 PC の盗難やサイバー攻撃に不安
■ Office 365 環境にて、どれだけ攻撃を受けているのか知りたい

解決

導入効果

■ 最小限の負荷で効果的にセキュリティ向上
■ ポリシーに合わせた現実的な環境実現
■ 脅威の状況を容易に把握

【サービス内容】

■ 定期的な健康診断で自社セキュリティ環境のチェックと対策
健康診断を通して、自社セキュリティの問題点洗い出しと対策を実施します。
定期的な診断にて PDCA を回し、継続的なセキュリティ強化を実現します。

■ フォレンジックで不正アクセスの経過とデータ漏えいの可能性を調査
セキュリティ インシデントやアラート発生時に、不正アクセスに至るまでの経過やデータ漏えいの可能性について、監査ログなどを調査しご報告いたします。

■ リアルタイム監視で不審なアクセス/振る舞いの早期調査
不審なサインインやアプリケーションを検知した際には、早期に TOSYS が原因を調査し、対策方法を提供します。当ご支援にてお客様の運用負荷を軽減いたします。

■ 各種セキュリティ設定相談を承ります
働き方改革のためのセキュリティ整備をはじめ、お客様の要望や課題の相談を承ります。
多角的視点で調査し、セキュリティ レベルを維持した設定のご提案が可能です。

【サービス提供エリア】
全国

【価格】参考価格一例: Microsoft 365 E5 をご契約の場合
セキュリティ デスク サービス: 140,000 円/月 (100 ユーザーまで)
情報セキュリティ脅威アセスメント診断サービス: 300,000 円 (エンドポイント診断除く、交通費別途)

ソリューションの詳細はこちら https://www.live-style.jp/managed-security/

□ お問い合わせ先
株式会社TOSYS
TEL 0120-742-500 (受付時間 平日 9:00 ～ 17:00) e-mail sales@team.live-style.jp
フォーム https://www.live-style.jp/contact/
所在地: 〒380 - 0935 長野県長野市中御所 3 - 13 - 7 中御所ビル 4F URL: https://www.live-style.jp

Enterprise Mobility + Security (EMS) 導入サービス

株式会社TOSYS

Office 365 のセキュリティ対策強化を支援します。

Livestyle

Office 365 の基本セキュリティ機能に加え、利用者の自由を維持しつつ管理を強化するためのサービスです。企業のポリシーに応じたID、データ、デバイスの統合的なセキュリティ ソリューションが可能です。機密ファイルを特別な権限をもつ人だけが閲覧でき、そのファイルを本人がメールなどで転送しても 転送先の人はファイルを見ることができないといったような、企業経営に欠かせない機密保持に役立ちます。

こんな課題をお持ちの方におすすめ!

- 会社全体のセキュリティを見直したい
- セキュリティを向上したい
- セキュリティを導入したいが何から始めたらよいかわからない

解決

導入効果

- 最小限の負荷で効果的にセキュリティ向上
- ポリシーに合わせた現実的な環境を実現
- 統一した管理画面で運用可能

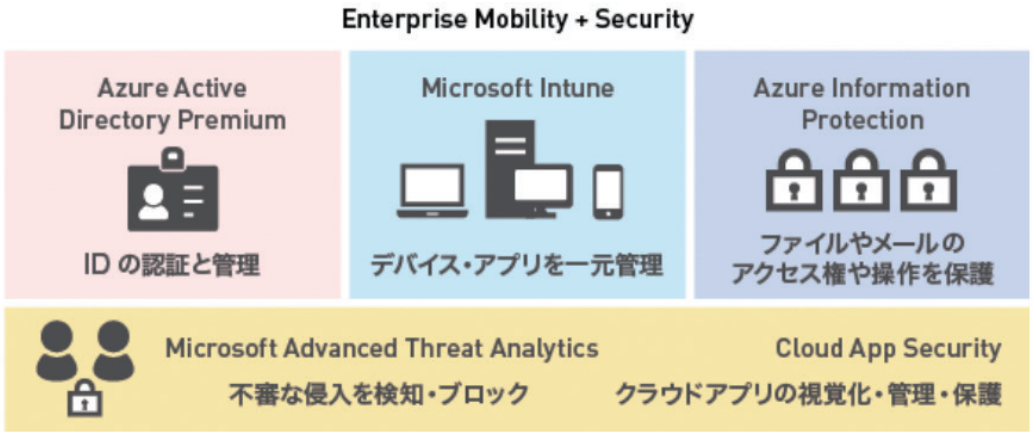
【サービス内容】

■ ID の認証と管理
・条件付きアクセス、多要素認証によるアクセス制限
・シングル サインオンによる認証 (SAML 認証)

■ デバイス アプリを一元管理
デバイス登録、デバイス管理、デバイスのアプリケーション制御

■ ファイルやメールのアクセス権や操作を保護
・機密情報の分類、ラベリング
・暗号化による保護
・ファイルの追跡とアクセス権の制御

■ クラウド アプリの視覚化、管理、保護
・シャドウ IT の検出、制御
・サイバー攻撃の脅威と異常に対する保護



【サービス提供エリア】
全国

【価格】参考価格一例: ID 認証と管理の設定　1,000,000円 ～
お気軽にお問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://live-style.jp/security/

□ お問い合わせ先
株式会社TOSYS
TEL 0120-742-500（受付時間 平日 9:00 ～ 17:00） e-mail sales@team.live-style.jp
フォーム https://www.live-style.jp/contact/
所在地: 〒380 - 0935 長野県長野市中御所 3 - 13 - 7 中御所ビル 4F URL: https://www.live-style.jp

サイバー攻撃 & 内部脅威可視化アセスメント

日商エレクトロニクス株式会社
"Your Best Partner"
NISSHO ELECTRONICS

Office 365 環境はもちろん、IT 基盤に潜むサイバー脅威を横断可視化。Hybrid 環境の可視化はお任せください!

Basic プラン: お客様の Office 365 環境にて標的型攻撃が行われていないか、既に感染されていないかをメール、ID/データの振る舞い、エンドポイントの観点から多角的、網羅的にアセスメント。
Advanced プラン: 増え続ける IoT 機器が攻撃の踏み台になり、攻撃者の侵入経路は多様化し、網羅的な脅威防止対策が難化傾向。
Advanced プランでは、AI によるトラフィック分析をプラス。エージェントレスのため、手軽により広範囲の脅威可視化をご提供。

こんな課題をお持ちの方におすすめ!

- ■ 既存のセキュリティ対策では不安があるとお考えの経営者様
- ■ 自社インフラの実態を把握できていないと認識されている情報システム部門の担当者様

解決

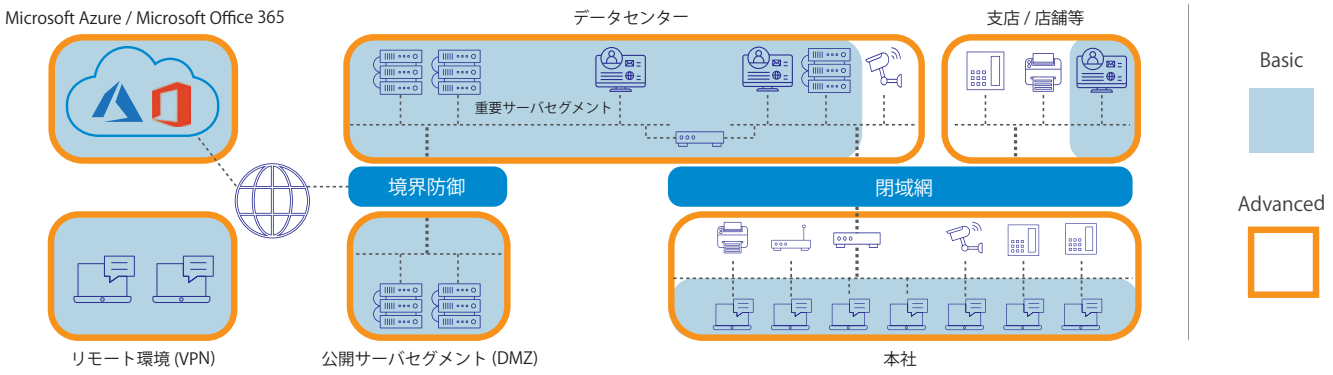
導入効果

- ■ 標的型攻撃メールの受信状況を可視化
- ■ 組織内部に侵入後、潜伏中の攻撃を可視化
- ■ Microsoft 365 E5 の導入効果を体感
- ■ 可視化結果に基づいたセキュリティ対策の検討

【サービス内容】

■ 既にお使いの Office 365 に評価用設定を追加するだけ。利用者に影響なくご利用いただけます。
■ 約 1 か月のモニター結果のレポートをご提出。また、オンサイトでの報告会もセットでご提供します。
■ Advanced プランでは、Basic プランに加え、調査用機器の貸出/設置からレポートまで一気通貫でご提供。調査用機器はミラーポートに接続するだけ! 利用者に影響なく容易にご利用いただけます。
■ Basic/Advanced プランをご利用いただいたお客様には、弊社の経験豊富なセキュリティ コンサルタントによる 2 時間のセキュリティ トレンド情報交換ミーティングを 1 回無償でご提供いたします。

サービス適用範囲



【サービス提供エリア】

全国

【価格】

Basic プラン: 無償※ ～
Advanced プラン: 750,000 円※ ～
※ 提供エリア、可視化対象規模など、条件によって個別見積もりとなる場合がございます。詳細はお問い合わせください。

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先
日商エレクトロニクス株式会社
TEL 03-6272-3980 (受付時間 平日 9:00 ～ 17:30) e-mail ss-inq@nissho-ele.co.jp
所在地: 〒102 - 0084 東京都千代田区二番町 3 - 5 URL: https://www.nissho-ele.co.jp/

MSS for EDR
- Microsoft Defender for Endpoint -

日商エレクトロニクス株式会社
"Your Best Partner"
NISSHO ELECTRONICS

セキュアなエンドポイント環境を実現。
EDR の運用はお任せください!

日商エレクトロニクスのエンジニアが 24 時間 365 日体制でお客様のMicrosoft Defender for Endpoint のテナントを運用担当者様に代わって監視します。アラート発生時には内容を分析し、必要に応じてエンドポイントの隔離から脅威の除去や推奨対応案の提示を行います。また、3 種類 (Basic、Standard、Premium) のサービスプランを用意しており、お客様のご要望に合わせて選択が可能です。

こんな課題をお持ちの方におすすめ!

■ 24 時間 365 日体制で監視ができないお客様
■ セキュリティ人材が不足しているお客様

解決

導入効果

■ 24 時間 365 日体制でお客様環境を監視し、隔離対応などを行います
■ アラート内容をアナリストが詳細に分析し、推奨対策案を提示します

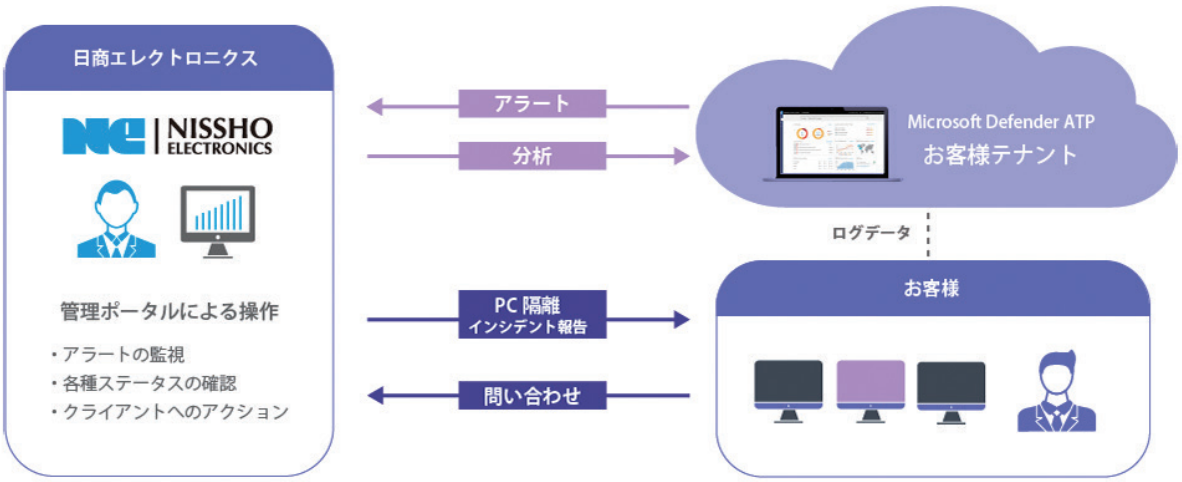
【サービス内容】

■ 簡易分析および通知
危険度に応じてアラートの内容を分析し、分析結果を推奨対策案とともに通知します。

■ エンドポイントの隔離
危険度が高いと判断したエンドポイントをリモートで隔離します。

■ 詳細分析
詳細な調査が必要と判断した場合には影響範囲や発生経緯などの特定に向けた分析を実施します。

■ 脅威除去 / 回復支援
エンドポイントに存在する脅威の除去や環境の復旧に向けた推奨対策案を提示します。



【サービス提供エリア】
全国

【価格】
月額費用 40,000 円 ～ (100 台 ～)
※ 税別、初期費用別途

ソリューションの詳細はこちら https://www.nissho-ele.co.jp/solution/ncpfcybersecurity/mssfordefenderatp/index.html

□ お問い合わせ先
日商エレクトロニクス株式会社
TEL 03-6272-3980 (受付時間 平日 9:00 ～ 17:30) e-mail datp-mktg@nissho-ele.co.jp
所在地: 〒102 - 0084 東京都千代田区二番町 3 - 5 URL: https://www.nissho-ele.co.jp/

MSS for SIEM - Microsoft Sentinel -

日商エレクトロニクス株式会社

"Your Best Partner"

サイバー攻撃対策をはじめとした Microsoft Sentinel 運用サービスを提供いたします

日商エレクトロニクスのエンジニアが 24 時間 365 日体制でお客様の Microsoft Sentinel のテナントを運用担当者様に代わって監視します。弊社では、MITRE ATT & CK の中でも特に SIEM で検知することが有効なタクティクスに対する監視 /分析サービスの推奨パッケージを提供しており、具体的な要件が決まっていないお客様でも、スモール スタートすることが可能です。

こんな課題をお持ちの方におすすめ!

■ サイバー攻撃対策として SIEM を導入したいお客様
■ 自社環境に合わせた SIEM の活用を検討しているお客様

解決

導入効果

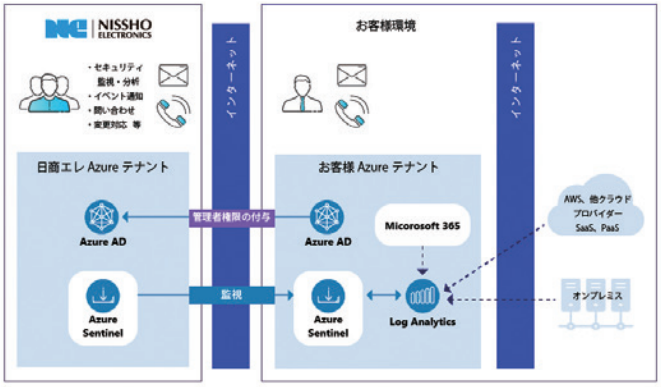
■ サイバー攻撃対策を主眼に置いた、推奨パッケージによるクイック スタートを実現
■ お客様環境に合わせたカスタム ルールやログソースの追加などに柔軟に対応可能

【サービス内容】

■ MSS for SIEM - Microsoft Sentinel -

SIEM はログを集約し分析を行うことでさまざまなアラートを検知できるソリューションです。しかし、その実現には要件の定義 / それに基づいたルールの選定 / 作成や必要なログソースの決定、また運用においては検知したアラート内容の調査、必要に応じて対応策の実施など高度な専門性が求められます。
MSS for SIEM - Microsoft Sentinel - はこれらの課題を解決します。迅速かつ効率的な SIEM 導入を実現し、標的型攻撃の検知を目的とした運用をお客様に提供いたします。

・ルール策定: 検知ルールの選定及びカスタム ルールの作成 / 追加を行います。
・分析及び通知: アラートの分析を行い、推奨対応案を通知します。必要に応じて、影響範囲など詳細分析を実施します。
・ルール作成 / 更新: セキュリティ状況の変化に合わせ、ルールの追加 / 更新を行います。
・チューニング: 誤 / 過検知のチューニングを実施します。
・月次レポート: Microsoft Sentinel からの情報にアナリストのコメントを付けて提供します。



【サービス提供エリア】

全国

【価格】

個別見積もり

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://www.nissho-ele.co.jp/solution/ncpfcybersecurity/mssforazuresentinel/index.html

□ お問い合わせ先
日商エレクトロニクス株式会社
TEL 03-6272-3980 (受付時間 平日 9:00 ～ 17:30) e-mail sentinel-mktg@nissho-ele.co.jp
所在地: 〒102 - 0084 東京都千代田区二番町 3 - 5 URL: https://www.nissho-ele.co.jp/

統合運用監視サービス「Managent」

日本システムウエア株式会社

NSW

Managent

AI 活用など最新デジタル テクノロジーを取り入れたシステム運用サービスを提供

「Managent (マネージェント)」は、クラウドとオンプレミスのハイブリッド環境に対応し、運用監視の設計構築、テクニカルサービス、サービスデスク、セキュリティ運用などのさまざまなサービスをワンストップで提供する統合運用監視サービスです。
AI 技術などの最新デジタル テクノロジーを取り入れることで、運用/監視業務やセキュリティ対策に関して、コストの削減/導入期間の短縮など、人手を最小限にした IT 運用を可能にし、お客様の DX 実現を支援します。

こんな課題をお持ちの方におすすめ!

- IT 運用人材不足を改善したい
- システム運用の負荷が特定の人に集中している
- 作業ミス/ヒューマン エラーを抑止して運用品質を向上させたい

解決

導入効果

- 大幅な工数圧縮での人材不足解消
- システム運用の自動化により大幅な負荷軽減
- 運用標準化により属人化、運用品質のバラツキ解消

【サービス内容】

■ 運用オートメーション

自動収集されたログデータ (対応履歴、システム/セキュリティログなど) を一元管理し、さらに AIOps を連携することにより、障害原因の早期特定や障害予兆、自動復旧を行います。

■「Microsoft Sentinel」連携

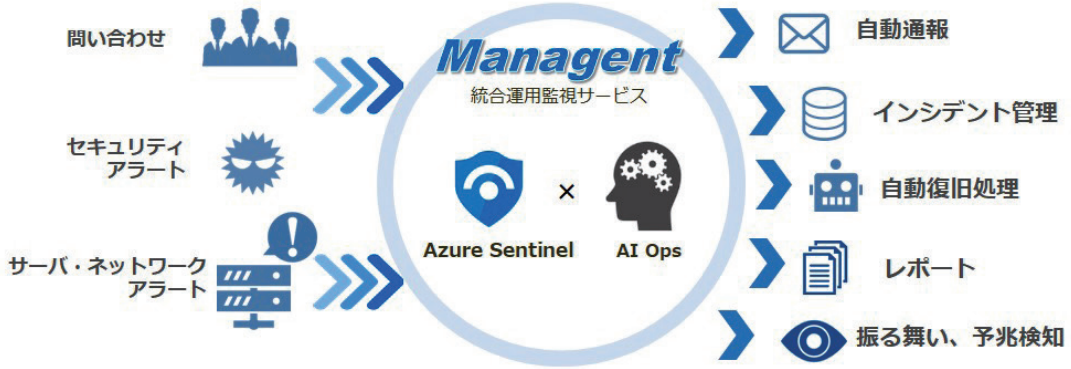
日本マイクロソフトが提供するセキュリティ監視クラウド サービス「Microsoft Sentinel」と「Managent」を融合したセキュリティ運用を提供します。

■ AI ハイブリッド脆弱性診断

機械学習/AI の応用とホワイト ハッカーによる診断のハイブリッド手法で、最新＆多数のガイドラインに準拠した診断を 3 倍≪早く/安く/高品質に≫提供する脆弱性診断サービスです。

■ AI ヘルプデスク ソリューション

24 時間 365 日対応可能なヘルプデスクとして、言語解析 AI アルゴリズムをチャットボット インターフェイスに組み込んだ AI ヘルプデスク サービスなど、お客様に最適なコール対応を提供します。



【サービス提供エリア】

全国

【価格】

自動監視通報サービス	5,000 円 ～
運用監視 + 個別運用	10,000 円 ～
運用監視 + 個別運用+テクニカル サービス	30,000 円 ～

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://nsw-dc.jp/aiops/

□ お問い合わせ先

日本システムウエア株式会社

TEL 03-3770-0096 (受付時間 平日 9:00 ～ 18:00) e-mail nsw-dc@gw.nsw.co.jp
フォーム https://nsw.smktg.jp/public/application/add/120
所在地: 〒150 - 8577 東京都渋谷区桜丘町 31 - 11 URL: https://www.nsw.co.jp/

TCS Hαven for SOC

日本タタ・コンサルタンシー・サービシズ株式会社

Microsoft Sentinel を用いた 24 時間 365 日のグローバル SOC サービス

グローバルにお客様専用かつ 24 時間 365 日 のチームを組むことで、お客様のセキュリティ ポリシー、セキュリティ標準や手順に準拠した SOC サービスを提供します。そのうえで Microsoft Sentinel を用いて機器が出力するログを集約し、監視/分析/初動対処/報告をします。これにより監視対象や機器ベンダーごとにサイロ化した非効率な運用の解消、リージョンごとのセキュリティ成熟度格差の是正などを実現し、よりセキュアな環境の創造を目指します。

こんな課題をお持ちの方におすすめ!

世界中のビジネス リージョン、国、拠点などのセキュリティ オペレーションを Microsoft Sentinel で統合したいが運用の担い手がいない。

解決

導入効果

- インドから世界中を 24 時間 365 日で管理
- 集中管理による標準化されたサービス品質
- 各国の拠点を活用することで多言語対応可
- お客様ビジネスに沿ったサービスの拡張

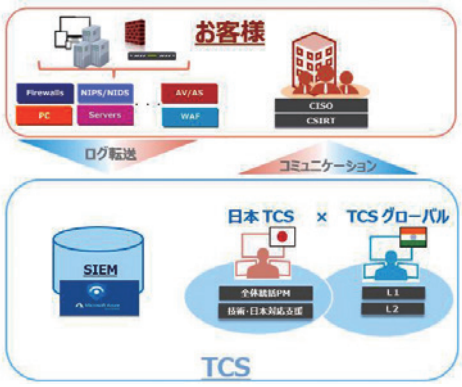
【サービス内容】

■ TCS Hαven for Security Operation Center

TCS は今まで培ってきたマネージド・セキュリティ・サービス プロバイダーとしての経験と知見を活用し、Microsoft Sentinel を用いたサービスを提供いたします。Microsoft Azure や Microsoft 365 からのログはもちろん、オンプレミスでもサード パーティが提供するアプライアンスやソフトウェアからのログも集約し、監視/分析/対処/インシデント管理をご支援いたします。

グローバルにお客様専用かつ 24 時間 365 日でサービス提供可能なチームを組むことにより、お客様のセキュリティ ポリシー、セキュリティ標準や運用手順に準拠したサービスを設計し提供することを可能としています。これにより機器ベンダーごとにサイロ化した運用監視サービスが引き起こす監視/分析/対処などにおける非効率な運用の解消、リージョンごとのセキュリティ成熟度格差の是正などを実現し、よりセキュアな環境の創造を目指します。

英語によるサービス提供が困難なリージョンにおいては、現地法人の TCS がお客様の窓口となり、言語や商習慣の差による障壁の緩和をいたします。また、お客様のビジネス拡張に沿ったサービスの拡張も容易です。



対応時間
- L1/L2 24 時間 365 日
- 技術・日本対応支援 平日 9:00-18:00 (JST)

サポート言語
- L1：日本語・英語
- L2：英語
- 技術・日本対応支援：日本語

サービス内容
- セキュリティログ監視
- ログ分析
- 初動対処
  *定型作業に限る
- お客様報告
- レポート
- 問合せ対応

【サービス提供エリア】

全国

【価格】

初期構築費用 15,000,000 円 ～
月額運用費用 4,300,000 円 ～

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://www.tcs.com/jp-ja/DTS/Cyber_sec

□ お問い合わせ先
日本タタ・コンサルタンシー・サービシズ株式会社
フォーム https://www.tcs.com/jp-ja/connect-with-tcs/contact-us
所在地: 〒105 - 8508 東京都港区芝公園 4 - 1 - 4 URL: https://www.tcs.com/jp-ja/home

脅威可視化アセスメント＆設定変更支援サービス

日本電気株式会社

Orchestrating a brighter world

NEC

デジタルシフトに伴う環境変化に対し、サイバー攻撃の脅威可視化から対策提案・導入までの一連の流れを支援

急速なデジタルシフトに伴い守るべき情報がオンプレミスからクラウド上へ移行しています。またテレワークが普及し、働く場所が多様化したことによって、従来のネットワーク境界中心の従来型のセキュリティ対策では限界を迎えております。セキュリティ対策においても、時代に適した「ゼロトラストモデル」での対策が必要です。そのためにもまずは現状のセキュリティ対策における脅威を可視化し、優先度付けした対策の提案から導入までの一連の流れをご提供します。

こんな課題をお持ちの方におすすめ!

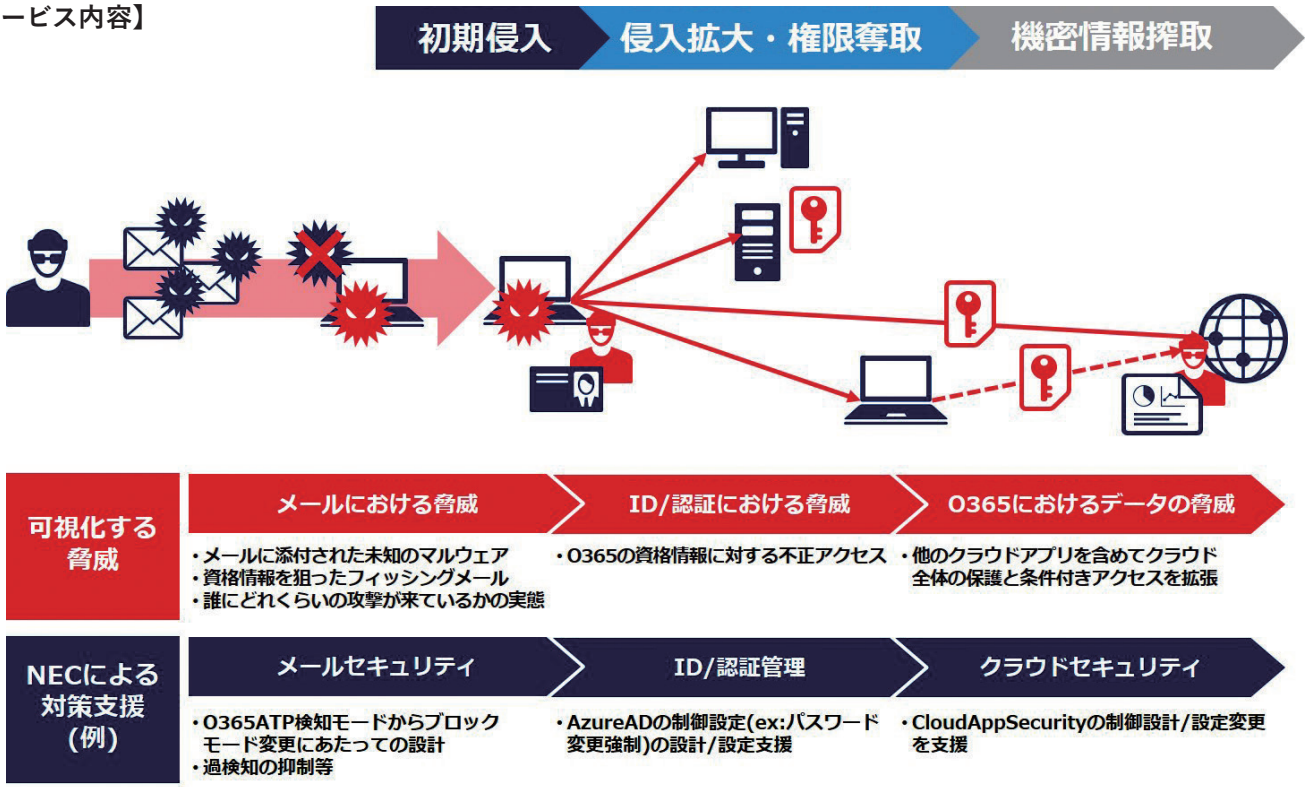
- 現状のセキュリティ対策の効果を可視化したいお客様
- セキュリティ対策の優先度付けにお困りのお客様
- セキュリティ設定についてお困りのお客様

解決

導入効果

- 対策状況と脅威を把握できる
- 適切な対策方法がわかる
- 設定支援により確実なセキュリティ設定が行える

【サービス内容】



【サービス提供可能地域】
全国

【価格】お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先
日本電気株式会社
e-mail sec-ms@security.jp.nec.com
所在地: 〒108 - 8001 東京都港区芝 5 - 7 - 1 (NEC 本社ビル) URL: https://jpn.nec.com/

マネージドセキュリティサービス (MSS) シリーズ

日本ビジネスシステムズ株式会社

JBS

Microsoft 365 E5 セキュリティの機能を活用した運用サービスで貴社の負担を軽減

検知したアラートに関する情報と、マイクロソフト パートナーとして JBS が長年培ったナレッジを併せて提供します。これにより、システム/セキュリティ担当者がアラートの対処が必要かをスムーズに判断できるようになり、お客様の負担軽減に寄与します。

＜サービス内容＞

■ 識別されたアラートの意味、トリガー、検出経緯を相関的に調査しすばやい脅威の絞り込み (悪意のあるアクティビティの抽出)

■ 排除 (誤検知対応)

■ 再発防止 (ポリシー反映など)

こんな課題をお持ちの方におすすめ!

■ アラートが脅威かどうかの適正な判断ができず、対応が遅れがち
■ アラートが多すぎて対応が遅れがち
■ 最新の脅威に対して最適な対策を打てない

解決

導入効果

■ 脅威を絞り込みスムーズなインシデント対応を実現できる
■ 対応すべきアラートを選別し適切な通知をユーザへ行える
■ 常に最適な対策を維持しセキュリティ レベルを高める

【サービス内容】

■ JBS の 提供する MSS シリーズ

すべての Microsoft 365 E5 セキュリティに対応しています。

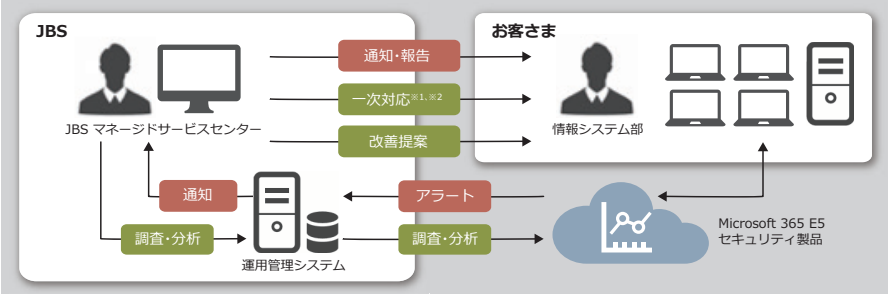
・Microsoft Defender for Endpoint　・Azure Active Directory Identity Protection　・Microsoft Defender for Cloud Apps
・Microsoft Defender for Office 365　・Microsoft Defender for Identity

■ セキュリティ運用を支援

インシデント対応支援と定期的な報告により、貴社のセキュリティ運用を支援します。

■ 最新の脅威への対策

日々アップデートされるマイクロソフト製品情報をキャッチアップし、貴社環境に合わせたポリシーを定期的に更新することで最新の脅威に対応します。



※ 1… Microsoft 365 E5 セキュリティ製品の自動対応機能による対応も含みます。 ※ 2… 特定のアラートのみ対応となります。

【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://pages.jbs.co.jp/service_managedsecurity01.html

□ お問い合わせ先

日本ビジネスシステムズ株式会社

TEL 03-4540-6478（受付時間 平日 9:00 ～ 17:00 土日祝日を除く）
フォーム https://pages.jbs.co.jp/contact_solution.html
所在地: 〒105 - 6316 東京都港区虎ノ門 1 - 23 - 1 虎ノ門ヒルズ森タワー 16F　URL: https://www.jbs.co.jp/

スマート スタート
for Microsoft 365 セキュリティ

日本ビジネスシステムズ株式会社

JBS

Microsoft 365 E5 セキュリティを始めませんか?
1 か月で開始できます!

Microsoft 365 環境のセキュリティ対策で、何から始めたら良いかお悩みのお客さま向けのサービスです。
多くの構築 / 運用実績に基づく設計で Microsoft 365 E5 セキュリティ製品を短期間で導入します。

こんな課題をお持ちの方におすすめ!

■ どういう点を考慮してセキュリティを導入すれば良いか分からない
■ セキュリティ対策を短期で導入したい
■ セキュリティ知識がないため、導入後の運用に不安がある

解決

導入効果

■ 豊富な実績に基づく設計でスムーズに導入できます
■ 1 か月で運用を開始できます
■ 基本操作から対応フローまで網羅した運用マニュアルを提供します

【サービス内容】

■ Microsoft 365 E5 セキュリティ全製品をカバー

すべての Microsoft 365 E5 セキュリティ製品に対応しています。
各製品の単体提供から製品間連携に対応したシナリオ ベースでの提供まで用意しております。

■ 1 か月で導入完了

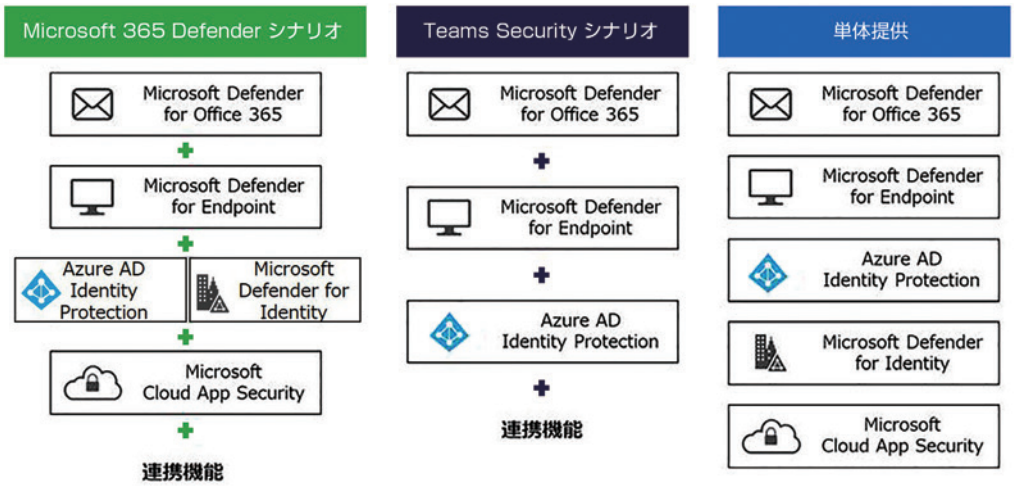
個別アセスメントは不要で、ヒアリング シートにご記入いただくだけで 1 か月で導入が完了します。

■ ベスト プラクティスに基づく設計

当社の構築 / 運用実績から得た知見をベースに、Microsoft 365 環境に必須となるセキュリティ設計の標準化を実現しました。

■ 実用的な運用マニュアルを提供

引き渡し後に即運用を開始いただけるように、製品の基本操作から実際のインシデント対応例を記載した運用マニュアルを提供します。



【サービス提供エリア】
全国

【価格】
お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

□ お問い合わせ先
日本ビジネスシステムズ株式会社
TEL 03-4540-6478（受付時間 平日 9:00 ～ 17:00 土日祝日を除く）
フォーム https://pages.jbs.co.jp/contact_solution.html
所在地: 〒105 - 6316 東京都港区虎ノ門 1 - 23 - 1 虎ノ門ヒルズ森タワー 16F URL: https://www.jbs.co.jp/

脅威可視化アセスメント Light

ネクストリード株式会社

所要時間 3 分で Microsoft 365 テナントの『リアルな脅威』を可視化

弊社独自の脅威インテリジェンスを基に貴社 Microsoft 365 テナントの脅威を可視化します。
企業規模に関わらず弊社がこれまで DX を支援してきた多くのお客様で Microsoft 365 環境の深刻なセキュリティ侵害をあぶり出すことに成功しています。『リアルな脅威』を可視化しながら、セキュリティに関するさまざまな疑問にお答えいたします。

こんな課題をお持ちの方におすすめ!

Microsoft 365 を利用中の以下のお客様
- ■ セキュリティに漠然とした不安
- ■ 環境の健康診断をしたい
- ■ 認証セキュリティを強化したい

解決

導入効果

自社環境の『リアルな脅威』を可視化し、リスクを把握できます。
また、専門家とのディスカッションを通じて今後重点的に取り組むべきセキュリティ施策のヒントを得られます。

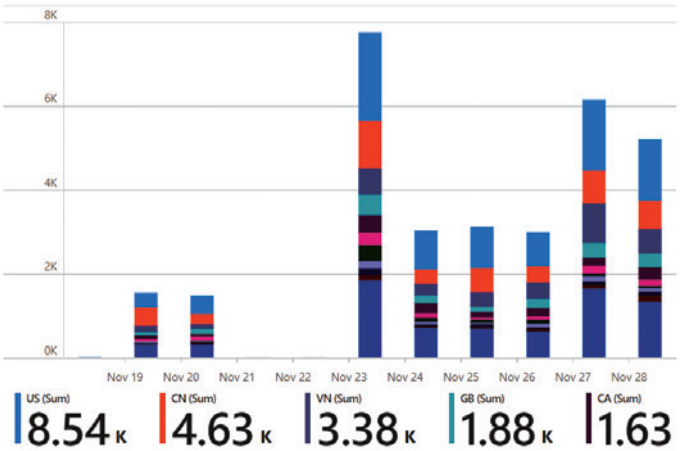
【サービス内容】

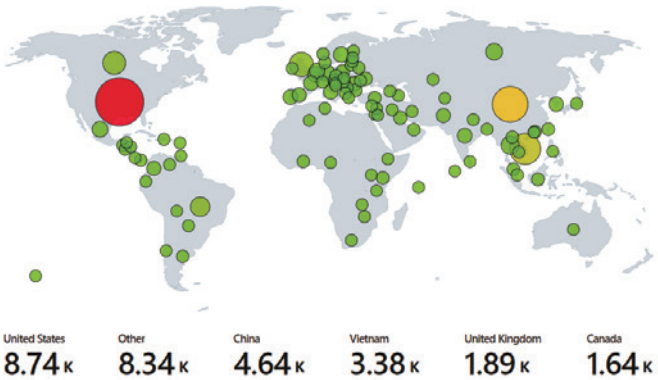
■ シンプルなのに高精度、高い評価実績を持つクイック アセスメントを無償で提供

本サービスを実施したお客様の 85% で Azure AD に対する継続的な攻撃が確認され、うち 38% は実際のアカウント侵害が見つかっています。
たった 3 ステップで簡単に申し込みができ、認証セキュリティの専門家による実施効果の高いアセスメントを無償で提供します。

■ サービスの申し込みは 3 STEP

STEP 1: 弊社分析アプリに対して Microsoft 365 テナントへのアクセスを委任します。(所要時間 1 分)
STEP2: Azure AD Premium P2 試用版ライセンスを有効化します。(所要時間 1 分)
STEP3: 1 か月後を目途にアセスメント結果の報告会日程を予約します。(所要時間 1 分)





【サービス提供エリア】
全国

【価格】
無償

ソリューションの詳細はこちら https://nextread.co.jp/nrassessment/

□ お問い合わせ先
ネクストリード株式会社
TEL 03-6869-5974 e-mail contact@nextread.co.jp
フォーム https://nextread.co.jp/contact/
所在地: 〒106 - 0032 東京都港区六本木 4 - 3 - 11 六本木ユニハウス 223 号 URL: https://nextread.co.jp/

Office 365 脅威可視化 無料アセスメント

パーソルプロセス＆テクノロジー株式会社
PERSOL
パーソル プロセス＆テクノロジー

すでに侵入されているかも、、、自社のリスク把握できてますか?
貴社のリスクを可視化し把握できます。

今なら、無料で貴社ご利用の Office 365 環境を診断し、安心して利用できる環境かどうかを可視化し、リスク度をレポートしすぐに把握できます。可視化されたリスクに関しては、安心してご利用できる提案までを弊社がご提案いたしますので、どこに脅威があるの? どんな対策をしなければ? などの不安を解消できます。Office 365 脅威可視化 無料アセスメントは、ご利用環境に影響なく、短期間で社内工数や調整などのご担当者様の手間なく実施できます。

こんな課題をお持ちの方におすすめ!

■ 診断は、「忙しくて時間が取れない」や、「社内調整がたいへん」「お金がかかる」
■ 自社のリスク把握ができてない
■ いつ、セキュリティ事故が起こるのか不安

解決

導入効果

■ 保有ライセンスを活用でき、追加コストなく診断できた
■ リスクへの提案があり、安全な環境にでき安心した
■ 危機意識が高まり、セキュリティ対策への実施計画が行えた

【サービス内容】

■ 脅威可視化アセスメント (リスク可視化と対処方法とご提案を今なら無料でご提供)

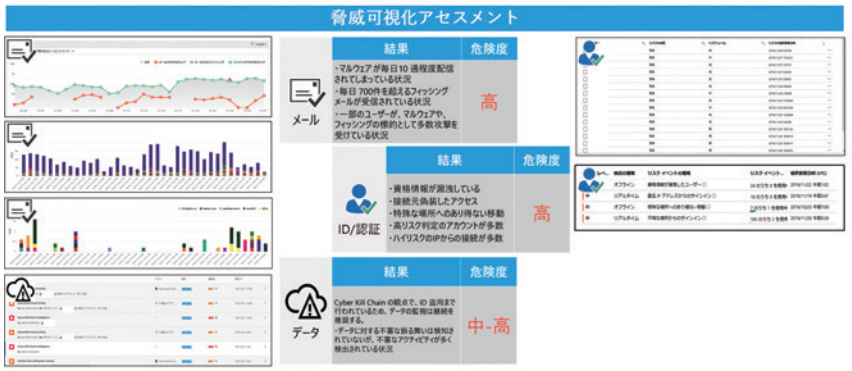
Office 365 E1/E3/E5 ご利用のユーザー様 (1,000 名以上) を対象にメール入り口、ログイン ID の不正利用、Office 365 上の不審なアクティビティを元に脅威の可視化を行います。その後、可視化した情報から弊社専門部門で分析を行い、貴社のリスクと対処方法をご提案いたします。

■ (有償オプション) Microsoft 365 ご利用者向け運用支援アウトソーシング サービス

Microsoft 365 のセキュリティ製品をご利用のお客様向けに設定などに関する管理者向け QA、追加された機能に関する導入計画策定 (ワークショップ含む)、インシデント発生時の一時対処 (方法の提案) までをアウトソーシングするサービスとなります。

■ (有償オプション) Microsoft Sentinel POC サービス

昨年発表された Microsoft Sentinel 利用を検討しているユーザー様向けに Microsoft Sentinel の開設手順、サーバーの登録、Agent 登録、オンボード作業をハンズオン形式でサービス提供します。3 回程度のワーキング想定。



【サービス提供エリア】

全国

【価格】今なら、無料 ※1 ※2 ※3

※1 脅威可視化アセスメント実施に必要なライセンスについてはお客様にてご用意いただく場合がございますので、お問い合わせください。※2 東京都内、大阪府内以外の場合、リモート (Microsoft Teams) での対応となります。なお、オンサイトをご希望される場合には、別途交通宿泊費が発生いたします。※3 無料アセスメントはできるだけ多くの方にご提供する予定ですが、当社側の都合により終了となる場合がございますので、できるだけ早くお申し込みください。

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://cloudsteady.jp/

□ お問い合わせ先
パーソルプロセス＆テクノロジー株式会社
TEL 03-6386-8297 (受付時間 平日 10:00 ～ 17:00) e-mail cloud-sales@cloudsteady.jp
フォーム https://www.persol-pt.co.jp/inquiry/cloud/
所在地: 〒135 - 0061 東京都江東区豊洲 3 - 2 - 20 豊洲フロント 7F URL: https://www.persol-pt.co.jp/

「いつでも」「どこでも」「どのデバイスでも」を実現する Microsoft 365 MSS

パーソルプロセス＆テクノロジー株式会社

PERSOL
パーソル プロセス＆テクノロジー

「いつでも」「どこでも」「どのデバイスでも」安心 / 安全にお客様の重要データにアクセスできるマネージド セキュリティ ソリューション

「いつでも」「どこでも」「どのデバイスでも」データやアプリケーションに安心 / 安全にアクセスできる IT 運用を支援します。
パーソルプロセス＆テクノロジー は長年 Microsoft 製品、Office 365 および Microsoft Azure などのクラウド ソリューション導入および運用の豊富な経験を活かし、お客様の業務に適したセキュリティおよびコンプライアンス対策運用を支援します。

こんな課題をお持ちの方におすすめ!

■ 最近猛威を振るっているランサム ウェアなどの脅威が怖い
■ 活発なクラウド サービス利用によるインサイダー、機密情報漏えい対策、シャドウ IT 対策ができていない
■ ニュー ノーマル時代のセキュア リモート ワークへのシフトができていない

解決

導入効果

■ お客様の業務形態を理解し適切なセキュリティおよびコンプライアンス対策を実施
■ クラウド サービス内で取り扱われる機密情報、インサイダー、シャドウ IT を可視化しシャットアウト
■ セキュア リモート ワークへのシフトを実現し、ゼロトラスト セキュリティを実現

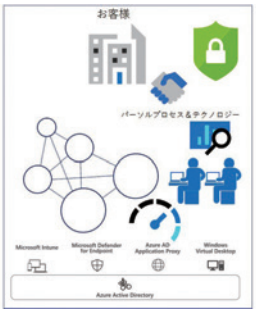
【サービス内容】

■「いつでも」「どこでも」「どのデバイスでも」を実現する「Microsoft 365 SOC Service」
クラウド サービスの利用拡大に伴う会社の重要なデータに「いつでも」「どこでも」「どのデバイスでも」アクセスすることを実現しながら、外部からの脅威、インサイダー、機密情報漏えい対策運用を支援します。

■ Microsoft の AI & 機械学習によるセキュリティ インテリジェンスを活用したエンドポイント運用ソリューション「Microsoft Defender for Endpoint MSS」
マイクロソフトの最新セキュリティと AI テクノロジーを組み合わせたエンドポイントへの自動対処機能を活用したマネージド セキュリティ ソリューションを提供します。

■ 定期的な企業の健康診断「セキュリティ＆コンプライアンス リスク可視化アセスメント」
セキュリティ / ハラスメント リスクを軽減するために定期的な可視化アセスメントを実施し必要な各種ポリシー作成の機会を提供します。

■「いつでも」「どこでも」「どのデバイスでも」を実現するための実証支援ソリューション「セキュアリモート PoC」
ご利用中の Office 365 環境にてセキュアで快適なリモートワーク環境の実現に向けてゼロトラスト セキュリティに基づいた PoC を実施します。



【サービス提供エリア】

全国

【価格】

Microsoft 365 マネージド セキュリティ サービス
※ID 数により、個別見積もり
【参考価格：1,000 ID / 平日営業時間対応】初期費用：500,000 円 ～、
月額費用：350,000 円 ～

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://cloudsteady.jp/solution/m365soc/

□ お問い合わせ先
パーソルプロセス＆テクノロジー株式会社
e-mail cloud-sales@cloudsteady.jp
所在地：〒135 - 0061 東京都江東区豊洲 3 - 2 - 20 豊洲フロント 7F URL：https://www.persol-pt.co.jp/

Azure Security ワークショップ (ネットワーク＆Hybrid Cloud Security)

パーソルプロセス＆テクノロジー株式会社

PERSOL
パーソル プロセス＆テクノロジー

クラウド上で稼働しているシステムのセキュリティ対策は万全でしょうか?

貴社で稼働しているシステムを最新のマイクロソフトのセキュリティ技術で保護できるように導入方法を丁寧に説明します。
また、Microsoft Defedner for Cloud を活用したセキュリティ保護、管理、ガバナンス強化をハンズオン形式で説明します。

こんな課題をお持ちの方におすすめ!

- Azure 環境のインターネット ブレイク アウト時にセキュリティ強化をお考えの方
- Azure 上で外部公開 Web サーバーのセキュリティ強化をお考えの方
- オンプレミス、Azure、AWS などの複数クラウド上で稼働しているサーバーのセキュリティおよびガバナンス強化をお考えの方
- オンプレミス、マルチクラウド環境での統合管理を検討されている方

解決

導入効果

- Microsoft クラウド環境を最新セキュリティ機能で強化
- オンプレミス、マルチクラウド、マルチ OS 環境を統合管理
- Azure Firewall、Azure WAF を体感
- Microsoft Defedner for Cloud を体感

【サービス内容】

■ Azure WAF PoC 支援

外部公開 Web サーバーを Azure WAF で保護する方法、導入方法 (基本 / 既定値 / MS 推奨値) を理解いただくハンズオン＋座学形式の支援サービスです。

■ Azure Firewall PoC 支援

Azure Firewall 活用方法、導入方法 (基本 / 既定値 / MS 推奨値) を理解いただくハンズオン＋座学形式の支援サービスです。

■ Hybrid Cloud Security ワークショップ

貴社が運用するオンプレミス サーバー、Azure、AWS などのクラウド上で稼働するサーバーなどを Microsoft が提供する Microsoft Defedner for Cloud、Azure ARC 機能を活用して統合的なセキュリティ保護、ガバナンス強化を行う方法をワークショップで提供します。

【サービス提供エリア】

全国

【価格】

Azure WAF PoC 支援:　300,000 円[※1]
Azure Firewall PoC 支援: 300,000 円[※1]
Hybrid Cloud Security ワークショップ 350,000 円 ～ [※1]

※1 本サービスは Azure サービスの契約が必要になります。Azure サービスは従量課金で費用が発生いたしますので予めご了承願います。

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら　https://cloudsteady.jp/seminar/azure-security/

□ お問い合わせ先
パーソルプロセス＆テクノロジー株式会社
e-mail cloud-sales@cloudsteady.jp
所在地: 〒135 - 0061 東京都江東区豊洲 3 - 2 - 20 豊洲フロント 7F　URL: https://www.persol-pt.co.jp/

Microsoft Endpoint Management ワークショップ

パーソルプロセス＆テクノロジー株式会社

PERSOL
パーソル プロセス＆テクノロジー

お客様の Microsoft 365 環境でモダンなエンドポイント管理の可能性を体験!

働く環境の変化に伴い、これまでのエンドポイント管理では対応が難しく頭を悩ませているお客様が多く見受けられます。お客様自身で Microsoft 365 環境にてモダンなエンドポイント管理を実現できるようにするためのワークショップを提供します。

こんな課題をお持ちの方におすすめ!

■ 場所やデバイスを問わず、生産性高く仕事がしたい
■ 多様なデバイスを管理しつつ、ユーザーの利便性を落とすことなくセキュリティも確保する必要がある

解決

導入効果

■ 製品の理解向上: Microsoft Endpoint Manager の製品理解と管理能力の向上
■ デバイス管理の実装: お客様の環境にて可能な範囲でデバイスやアプリの保護を実装
■ ID 保護の実装: お客様の環境にて可能な範囲で ID 保護を実装

【サービス内容】

■ モバイル デバイス管理ワークショップ

本ワークショップでは、Microsoft Endpoint Manager の機能全般の理解を目的としています。
・学習: Microsoft Endpoint Manager の機能理解
・ハンズオン: Microsoft 製品を活用したエンドポイント管理と ID 保護の実装
・ディスカッション: モダンなエンドポイント デバイス管理を行うための議論

■ モバイル アプリケーション保護ワークショップ

本ワークショップでは他社の MDM をご利用の企業様で Office 365 のメール、Microsoft Teams を安全に利用するためのアプリケーション保護機能の理解を目的としています。

■ Microsoft Endpoint Manager ワークショップ for iPhone (DEP)

Apple で提供している iPhone の DEP と Microsoft Endpoint Manager を組み合わせた MDM / MAM 機能導入方法をワークショップ形式で提供します。

ワークショップを通して、お客様と協力し以下のことを実現します

製品の理解向上
Microsoft Endpoint Managerの製品理解と管理能力の向上

ID保護の実装
お客様の環境にて可能な範囲にてID保護を実装

デバイス管理の実装
お客様の環境にて可能な範囲にてデバイスやアプリの保護を実装

【サービス提供エリア】

全国

【価格】

お気軽にご相談ください

※1 本サービスは Microsoft Endpoint Manager (EMS E3 / E5) をお客様にてご用意いただく必要があります。
※2 Apple Business Manager の ID および iPhone 端末をお客様にてご用意いただく必要があります。

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://cloudsteady.jp/seminar/mem/

□ お問い合わせ先
パーソルプロセス＆テクノロジー株式会社
e-mail cloud-sales@cloudsteady.jp
所在地: 〒135 - 0061 東京都江東区豊洲 3 - 2 - 20 豊洲フロント 7F URL: https://www.persol-pt.co.jp/

FUJITSU Security Solution インテリジェンス マネージド セキュリティ サービス

富士通株式会社

Microsoft 製品をはじめとするセキュリティ機器、デバイスをご利用のお客様に対し、セキュリティ専門家が常に護るマネージド サービス

Microsoft 製品をはじめとするセキュリティ機器、デバイスをご利用のお客様に対し、お客様自身では対応が難しい 24 時間 365 日のリアルタイム監視、的確なインシデント対応といった継続的なセキュリティ運用強化支援など、サイバー攻撃に対応するためのセキュリティ運用サービスを提供します。また、重大インシデント発生時には、高い技能を有するエキスパートが課題解決に向けてサポートいたします。

こんな課題をお持ちの方におすすめ!

セキュリティ機器、デバイスが発するアラートへの日々の対応、および今後の改善対応についての悩みをお持ちのお客様。

解決

導入効果

- お客様のセキュリティ運用負荷軽減
- セキュリティ人材の保有コスト低減
- 投資根拠となる運用の客観的データ取得
- セキュリティ専門家の知見による安心感

【サービス内容】

■ リアルタイムのセキュリティ運用支援

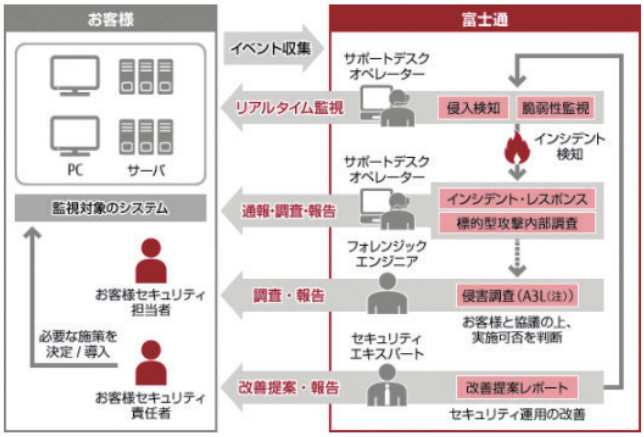
クラウドベースで稼働する「次世代セキュリティ監視基盤」に、膨大なセキュリティ アラートの対処、分析を自動的に実行する SOAR (Security Orchestration Automation and Response) の技術を実装し、24 時間 365 日自動でセキュリティ監視や通報を行います。

■ セキュリティ専門家による調査、報告、ならびに改善提案

巧妙化する国境を越えたサイバー攻撃などに対して、当社のセキュリティ アナリストがグローバル拠点で蓄積されたサイバー攻撃の傾向や痕跡情報などにもとづき、インシデントの原因究明や対処案の提示などの対応を支援します。

■ セキュリティ製品の幅広いサポート

Microsoft セキュリティ製品のほか、業務システムをはじめクラウドやネットワーク、パソコンなどのエンドポイントで発生したアラートやインシデントを集約し、当社の SOC を通じてセキュリティの統合的な監視、運用を行っています。



【サービス提供エリア】

全国

【価格】

お問い合わせください

Microsoft DIGITAL TRUST SECURITY Alliance

ソリューションの詳細はこちら https://www.fujitsu.com/jp/solutions/business-technology/security/secure/global-managed-security/globalmanaged-securityservice/

□ お問い合わせ先

富士通株式会社

セキュリティに関するお問い合わせフォーム https://contactline.jp.fujitsu.com/contactform/csque04701/821681/

所在地: 〒105 - 7123 東京都港区東新橋 1 - 5 - 2 汐留シティセンター URL: https://www.fujitsu.com/jp/

統合ログ監視サービス Advanced SOC with Microsoft Sentinel
セキュリティ監視サービス for Microsoft 365 Defender

三井物産セキュアディレクション株式会社

MBSD Threat Intelligence / Hunting 技術を融合させた MDR サービス

三井物産株式会社のグローバル ネットワークを活かし、提携した脅威情報ベンダーの情報に MBSD マルウェア研究部門の情報を加えた混合型 Intelligence、ならびに 2014 年から EDR のマネージド サービスをグローバル顧客へ提供してきた Threat Hunting 技術をベースに、Microsoft 社の先進的セキュリティ機能をフル活用した MDR (Managed Detection and Response) サービスを提供します。

こんな課題をお持ちの方におすすめ!

- セキュリティ機能やツールの進化に対応が追い付かない
- 検知アラートの専門的な分析 / 対応が難しい
- セキュリティ知識のある人材が不足している

解決

導入効果

- 「E5 セキュリティ ×Threat Intelligence ×Hunting」によるセキュリティ耐性向上
- 日々の対応業務から解放され業務の選択と集中を実現

【サービス内容】

2001 年に Security Operation Center を開設して以来、約 20 年の間、官公庁からエンタープライズまで幅広い業種の IT 環境のセキュリティ対策を担ってきた MBSD-SOC が、お客様のニーズに合わせて 3 つのレベルで MDR サービスを提供いたします。

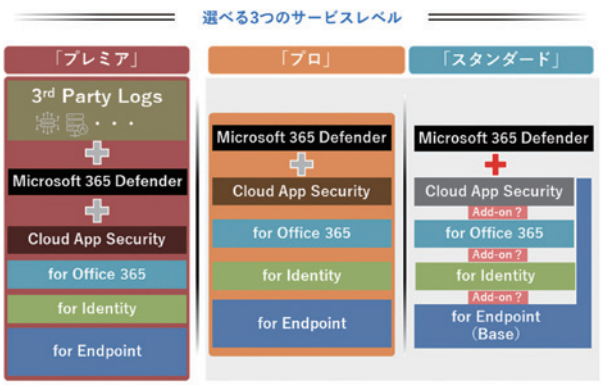
- プレミア: Microsoft 365 Defender ファミリーに加え、3rd パーティ ログ (Microsoft 社製品 / サービス以外のログ) を加えたトータル ソリューション (フルカスタム)
- プロ: Microsoft 365 Defender ファミリーのエンドポイント対策全体ソリューション
- スタンダード: Microsoft 365 Defender for Endpoint 中心のセキュリティ ソリューション (E5 ユーザー以外にも提供可)

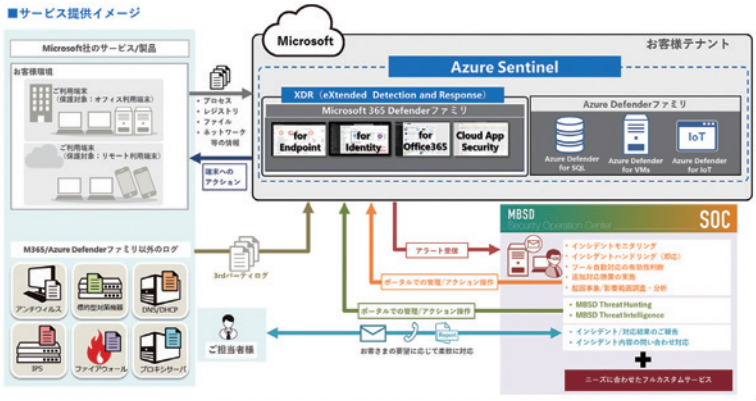
■ 万が一の事態でも安心

経験豊富なアナリストによる「マルウェア解析サービス」、「フォレンジックサービス」もワンストップでご提供します。

■ フルカスタム (プレミア) での提供

Microsoft Sentinel を利用し、SOC アナリストが能動的に攻撃を調査 / 分析 (Threat Hunting) することで、個々のセキュリティ機器だけでは検知が困難な脅威の早期発見と対処を実現します。





【サービス提供エリア】

全国

【価格】

お問い合わせください

ソリューションの詳細はこちら https://www.mbsd.jp/solutions/mss/

□ お問い合わせ先

三井物産セキュアディレクション株式会社

TEL 03-5649-1965 (受付時間 平日 9:30 ～ 17:45) e-mail sales-info@mbsd.jp
所在地: 〒103 - 0013 東京都中央区日本橋人形町 1 - 14 - 8 郵船水天宮前ビル 6F URL: https://www.mbsd.jp/

マネージドEDRサービス for Microsoft Defender for Endpoint

株式会社ラック

Microsoft Defender for Endpoint の監視、隔離、調査、駆けつけ対応までをトータル サポート

ラックがご提供する「マネージドEDRサービス for Microsoft Defender for Endpoint」は、お客様に代わって、検知したログに対して、24 時間 365 日のエンドポイント監視やリモートからの論理隔離などのオペレーションを実施します。さらに、アラートに関する調査として、これまで多数の事件/事故への対応実績を誇るサイバー救急センターのセキュリティ スペシャリストによる脅威分析およびインシデント レスポンスを提供します。

こんな課題をお持ちの方におすすめ!

より深く EDR のアラート分析を行うにはアラートの真偽判断やインシデントの原因調査が必要となるが、そのようなフォレンジック調査の知見やリソースが不足している。

解決

導入効果

- 24/365 のアラート監視で運用負荷を軽減
- 感染した PC は隔離して感染の拡大防止
- スペシャリストによる専門調査をご提供
- 調査レポートでは復旧や対策のアドバイスも

【サービス内容】

■ 24/365 のアラート監視と端末隔離

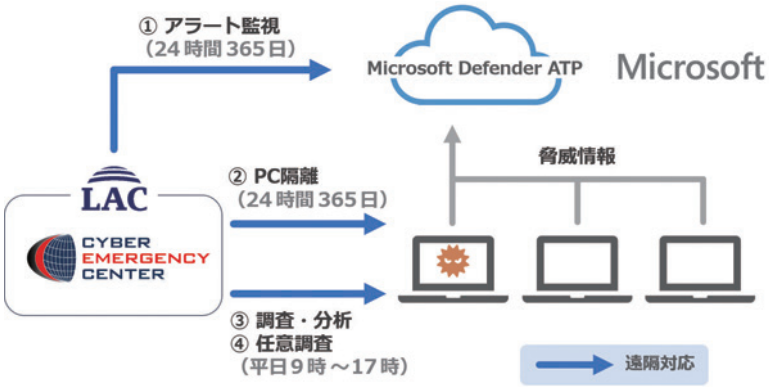
24/365 で発生したアラートを常時監視します。また、High レベルのアラートが発生した場合は、対象端末を即時ネットワーク隔離します。隔離対象から除外する端末を設定することも可能です。

■ アラート調査/任意調査

「侵入原因」「影響範囲」「情報漏えい」などについて EDR 機能を利用した調査を実施します。調査には、EDR で検知したアラート調査を実施するほか、EDR 以外の検知 (ネットワーク監視製品など) をきっかけに、EDR 機能を利用した任意調査も実施します。

■ 現状回復に向けたアドバイスを実施

調査結果をレポートとして報告します。レポートにはアラートの調査結果だけではなく、対象端末の復旧や対策に関するアドバイスが含まれます。また、別サービスとして、インシデント発生後の対応支援依頼 (C119 サービス) も承っております。



【サービス提供エリア】

全国

【価格】

月額費用 200,000 円 ～

※台数や条件により大きく変動しますので、価格についてはお問い合わせください。

ソリューションの詳細はこちら https://www.lac.co.jp/service/operation/edr.html

□ お問い合わせ先

株式会社ラック

フォーム https://www.lac.co.jp/contact.html

所在地: 〒102 - 0093 東京都千代田区平河町 2 - 16 - 1 平河町森タワー URL: https://www.lac.co.jp/

Microsoft 365 脅威分析サービス

リコージャパン株式会社

セキュリティ リスクは一過性のものではありません!
定期的なチェックとタイムリーな予防が必要です

お客様のご希望に合わせたスパンで Microsoft 365 脅威に関わる情報を収集 / 分析し、報告会を開催します。レポートの報告会では脅威に応じたベスト ソリューションの提案はもとより、最新情報の提供や今後のアクション プラン策定の支援も行います。
また、報告会以外でもお問い合わせいただける窓口を案内いたしますので、いつでもご質問、相談いただけます。

こんな課題をお持ちの方におすすめ!

定期的にセキュリティ状況を把握したいが、自社に Microsoft 365 に詳しい技術者がいないため、分析が難しいとお悩みのお客様

解決

導入効果

データ収集から分析まで弊社 SE が対応しますので、お客様で専門家をご用意いただく必要はありません

【サービス内容】

■ アセスメント サービス
Microsoft 365 E5 トライアル版を使用し、短期の情報収集をおこない、分析した結果を報告します。分析結果を受けて、実施するサービス内容を決定することも可能です。

■ 定期レポート サービス
お客様のご要望に合わせたスパンで、定期的に Microsoft 365 の情報を収集し、分析レポートを提出します。

■ 定例会サービス
分析レポートを対面で報告、運用や今後の展開についての相談を承ります。

■ 問合せ窓口サービス
Microsoft 365 セキュリティ関連のご質問、ご相談を受け付ける窓口を開設し、調査および情報提供を行います。

【サービス提供エリア】
全国

【価格】
別途見積り

Microsoft DIGITAL TRUST SECURITY Alliance

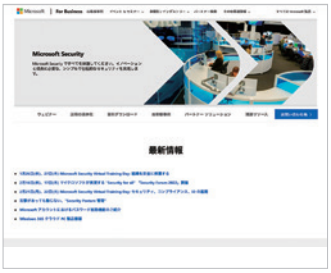
□ お問い合わせ先
リコージャパン株式会社
e-mail zjp_managed_shoudan@jp.ricoh.com
所在地: 〒105 - 8503 東京都港区芝 3 - 8 - 2 芝公園ファーストビル URL: http://www.ricoh.co.jp/

Microsoft 365 関連リソース

Microsoft 365 製品サイト

Microsoft 365 に関する最新情報はこちらをご覧ください。

https://www.microsoft.com/ja-jp/microsoft-365



Microsoft 365 E5 Security & Compliance

セキュリティとコンプライアンス対策に関する最新情報を
集約してお届けします。

https://www.microsoft.com/ja-jp/biz/security/default.aspx

Digital Trust Security Alliance 紹介ページ

Microsoft Digital Trust Security Alliance に関する情報をお届けします。

https://www.microsoft.com/ja-jp/partner/biz/mwp_sec_alliance.aspx

Microsoft Cloud Accelerator プログラム | Microsoft Partners

お客様の課題とニーズにマッチした Microsoft 365 の利活用を
ご支援するプログラムです。

https://www.microsoft.com/ja-jp/biz/security/microsoft-365-accelerator.aspx

ソリューションの詳細は各パートナーの公式サイトをご参照いただくか、または各パートナーにお問い合わせください。

Microsoft Security に関する最新情報はこちらをご覧ください。**https://www.microsoft.com/ja-jp/security/business**

製品に関するお問い合わせは、次のインフォメーションをご利用ください。

■ インターネット ホームページ　https://www.microsoft.com/ja-jp/
■ マイクロソフト購入相談 窓口　0120-167-400 (9:00 ～ 17:30 土日祝日、弊社指定休業日を除きます)

※ 電話番号のおかけ間違いにご注意ください。

Microsoft

日本マイクロソフト株式会社

〒108-0075 東京都港区港南 2-16-3 品川グランドセントラルタワー