CLUTCH F.C.C. TECHNOLOGY × Next Read

自動車部品サプライヤーの情シスが考えた ひとり情シス向け セキュリティサービス

SecureQUEST

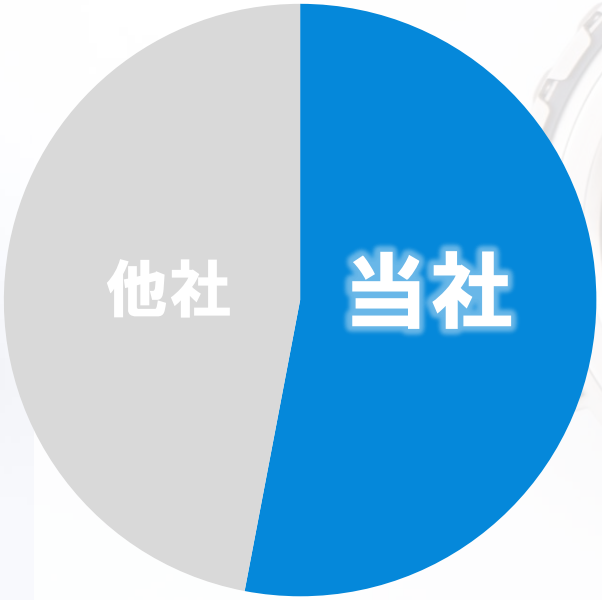
ご紹介資料

株式会社エフ・シー・シー

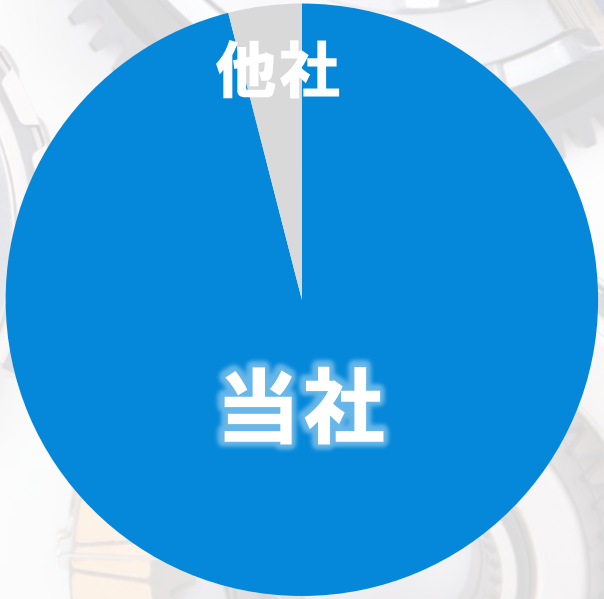
当社は自動車部品メーカーです

二輪車用クラッチのシェア

世界の半分以上



国内はほぼ全体をカバー



なぜセキュリティサービスを提供するのか

2020年
ネクストリード社のサポートを受け
当社グループ（海外含む）のセキュリティレベル統一に着手

2022年
海外のグループ子会社でランサムウェア被害が発生

2023年
サイバー攻撃被害の経験、自工会セキュリティガイドラインへの準拠により
良いセキュリティの仕組みが構築できた

当社グループ内だけではなく
サプライチェーン全体のセキュリティレベル底上げのため
この仕組みを社外に水平展開できないだろうか？

2023年 11月
自動車業界のみならず産業界ひいては社会全体に
当社のできる範囲で貢献すべく SecureQUEST サービス提供を開始

CLUTCH F.C.C. TECHNOLOGY　Next Read

組織のサイバーセキュリティを巡る状況

狙われているのは製造業と中小企業

個人情報や機密情報を狙ったサイバー攻撃は増加の一途を辿り、手口は巧妙化・ビジネス化しています。

ランサムウェアの被害件数は、業種では製造業、会社規模では中小企業で最も多くなっています。

サプライチェーンに及ぼす影響が甚大

事態は、一社への攻撃が大手顧客等を含むサプライチェーン全体に影響を及ぼすという点で深刻です。

復旧まで業務停止を余儀なくされる可能性もある為、中小企業にとっては死活問題です。

世界を悩ます脅威を相手にひとりでは不安

サイバー攻撃の増加に伴い業界や顧客からの要求はより高度に、対応範囲も拡大する一方で、ひとりで立ち向かうご担当者様も多いのではないでしょうか？

情報セキュリティ 10大脅威の変遷

順位	脅威の種類	2025	2024	2023	2022	2021
1	**ランサムウェアによる被害**	**1**	**1**	**1**	**1**	**1**
2	**サプライチェーンの弱点を悪用した攻撃**	**2**	**2**	**2**	**3**	**4**
3	システムの脆弱性を突いた攻撃	3	5、7	6、8	7、6	10
4	内部不正による情報漏えい	4	3	4	5	6
5	標的型攻撃による機密情報の窃取	5	4	3	2	2
6	リモートワーク等の環境や仕組みを狙った攻撃	6	9	5	4	3
7	地政学的リスクに起因するサイバー攻撃	7	–	–	–	–
8	分散型サービス妨害攻撃（DDoS攻撃）	8	–	–	–	–
9	ビジネスメール詐欺	9	8	7	8	5
10	不注意による情報漏えい等	10	6	9	10	9

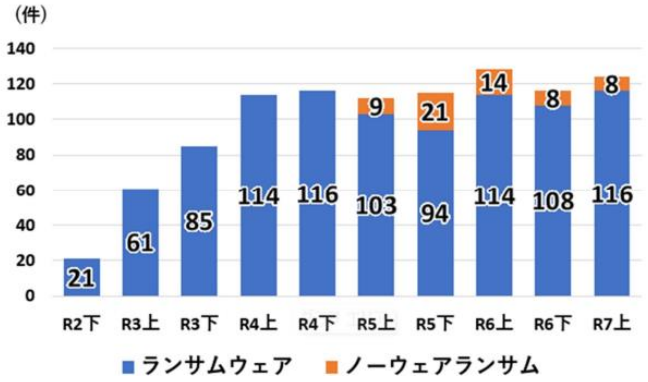
出典：IPA 情報セキュリティ10大脅威

中小企業に対するサイバー攻撃の現状

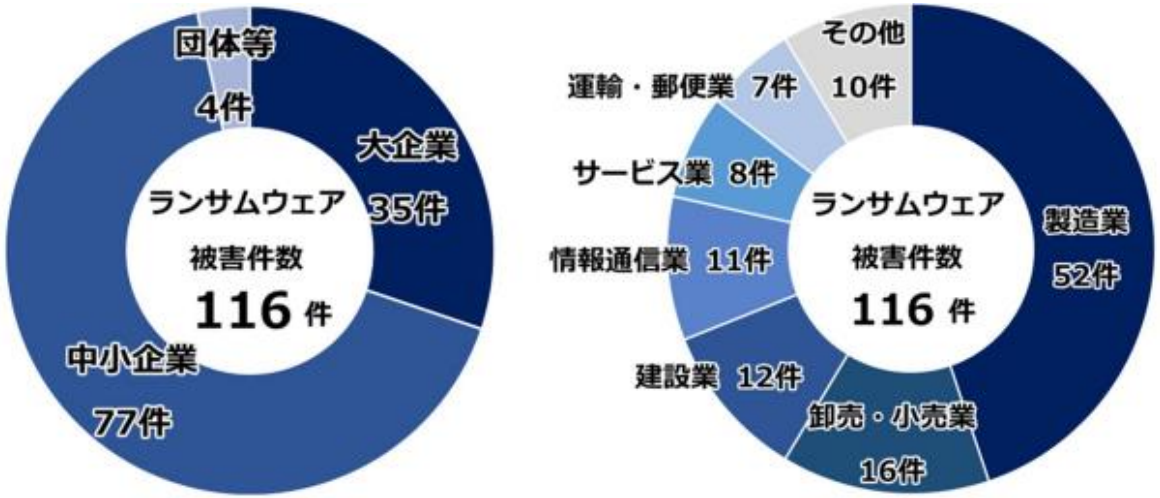
中小企業に対するランサムウェア攻撃

企業・団体におけるランサムウェア被害の報告件数は高い水準で推移

※ノーウェアランサムの被害については、令和５年上半期から集計。



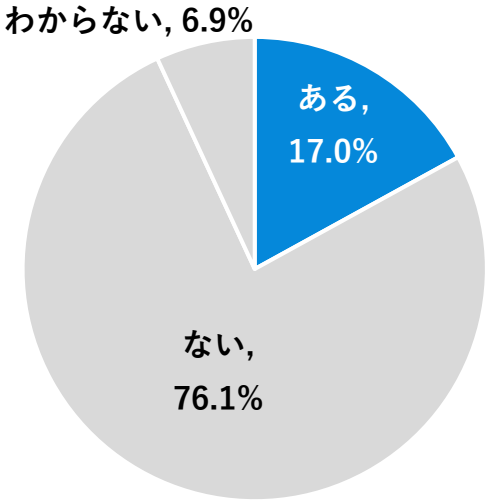
中小企業、製造業が狙われています



出典：令和7年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

取引先等を経由したサイバー攻撃被害

過去に取引先等がサイバー攻撃の被害被害を受け、それが自社に及んだ経験がありますか＜仕入・外注・委託先等の取引先＞



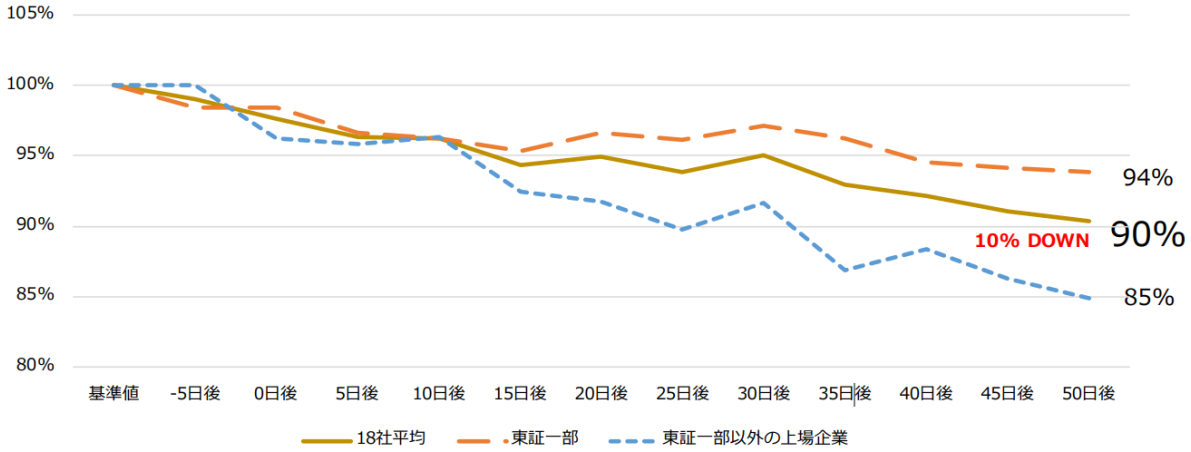
出典：企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査
（株式会社NTTデータ経営研究所）

経営リスクとしてのサイバーセキュリティリスク

図表 10　サイバーリスク指標モデル（**年商 1000 億円企業**における社内報告資料の例）【潜在損失額】

		想定損失額の目安	算出根拠
直接被害	①個人情報漏えいによる金銭被害	▲80億円	JNSA一人当たり損害賠償額より算出 （基礎情報価値×機微情報度×本人特定容易度×社会的責任度×事後対応評価×顧客数≒80億円）
直接被害	②ビジネス停止による機会損失	5営業日あたり ▲20億円	社内ヒアリングより算出 （1日あたりの生産量×商品単価≒2億円） （1日あたりのECサイト売上≒2億円）
直接被害	③法令違反による制裁金	▲40億円	EUデータ保護指令（GDPR）の制裁金 （全世界の売上高の4%≒40億円）
直接被害	④事故対応費用	▲0.6億円	過去事例や業者ヒアリングにより算出 （調査費用、データ復旧費用、応急処置費用等）
間接被害	⑤純利益への影響	▲10.5億円	JCIC調査実績より算出 （前期純利益50億円×21%≒10.5億円）
間接被害	⑥時価総額への影響	▲300億円	JCIC調査実績より算出 （時価総額3000億円×10%≒300億円）

セキュリティ事故適時開示後の株価傾向調査（n=18）



出典：JCIC取締役会で議論するためのサイバーリスクの数値化モデル～サイバーリスクの金額換算に関する調査～

SecureQUEST 2本の柱

監視サービス

ネクストリード社の
セキュリティのプロによる
アラート監視、ログ分析

- SOC
- EDR
- ファイアウォール
- 不正サインイン
- 相関分析

伴走サポート

当社がグローバル展開した
セキュリティ対策の知見、経験で
お客様をご支援

- 回数無制限の相談窓口
- アラート対応支援
- 月次レポート解説
- 自工会/部工会セキュリティガイドライン準拠
- 段階的なセキュリティ強化支援

Microsoft 365

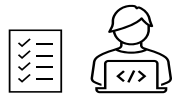
SecureQUEST のサービスイメージ

お客様の IT 環境（グローバル）

クラウド

ID、パスワード

ネットワーク、PC、サーバー



継続的なセキュリティ強化

監視サービス

- 24h365d アラート監視
- リスクレベルが高い
  - デバイスの自動隔離
  - アカウントの自動無効化

伴走サポート

- アラート対応支援
- 対策改善施策解説
- 改善実行支援
- 回数無制限の相談窓口
- 自工会ガイドライン準拠

セキュリティのプロによる分析

独自のリスク検知ロジック

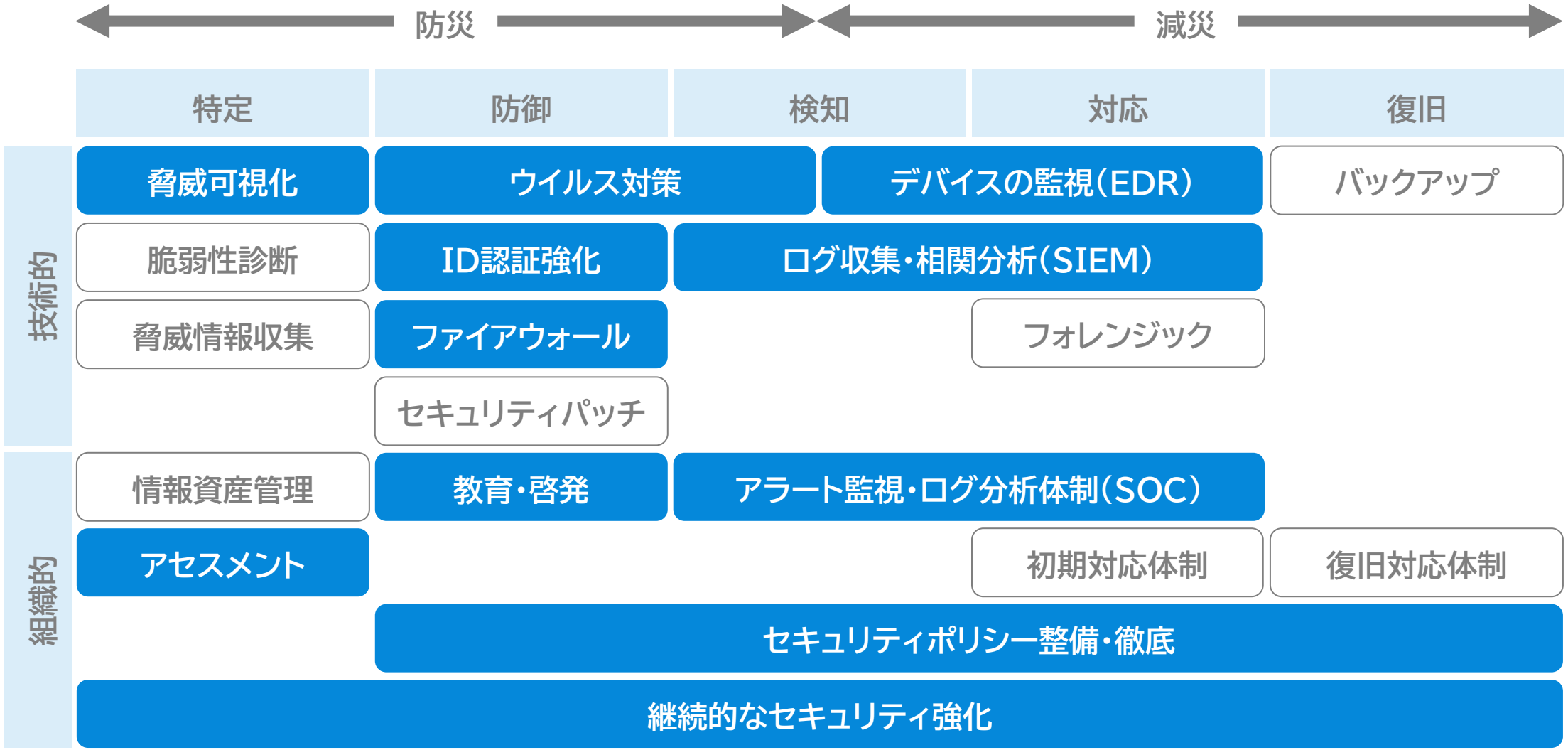
オペレーターのログ分析により誤検知、過検知を最小化

月次レポート

監視サービスにより
短期的なリスクに対応しながら

伴走サポートで**継続的なセキュリティ強化**の
サイクルをしっかり回し
中長期的なリスクに対応

SecureQUEST のサービス範囲



監視サービス／伴走サポート

SecureQUEST 監視サービス 3つの特長

1 アラート発報で終わらない監視サービス

アラート通知には確認、処置の観点も分かりやすく記載！ アラートのクローズまでしっかり伴走！

2 不正サインインもしっかり監視

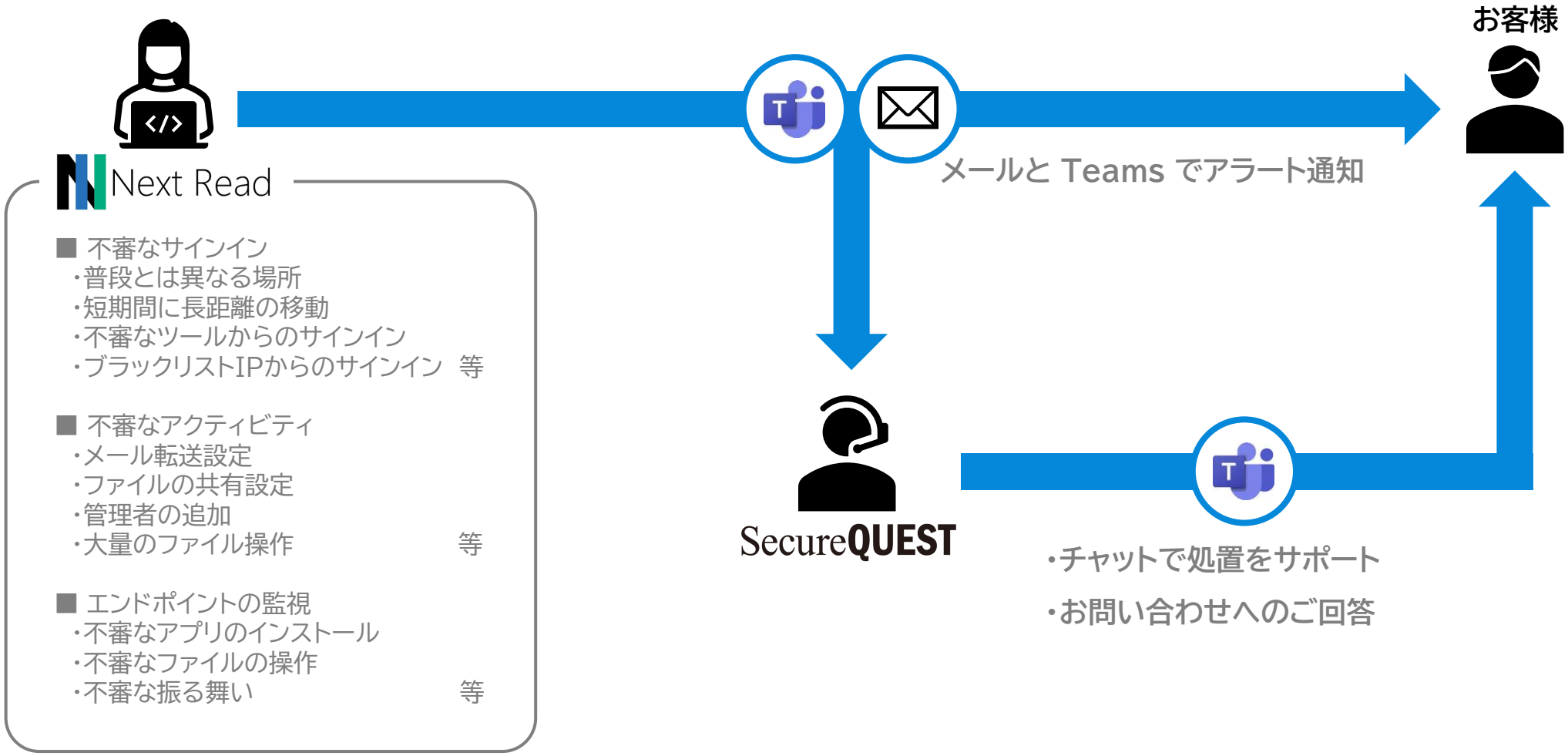
ID・パスワード漏えいをモニタリングしていますか？不正サインインされていない自信はありますか？

3 海外拠点もまとめて監視

海外拠点もまとめて監視！ 日本の IT 部門と海外拠点に同時にアラート発報！中国も！

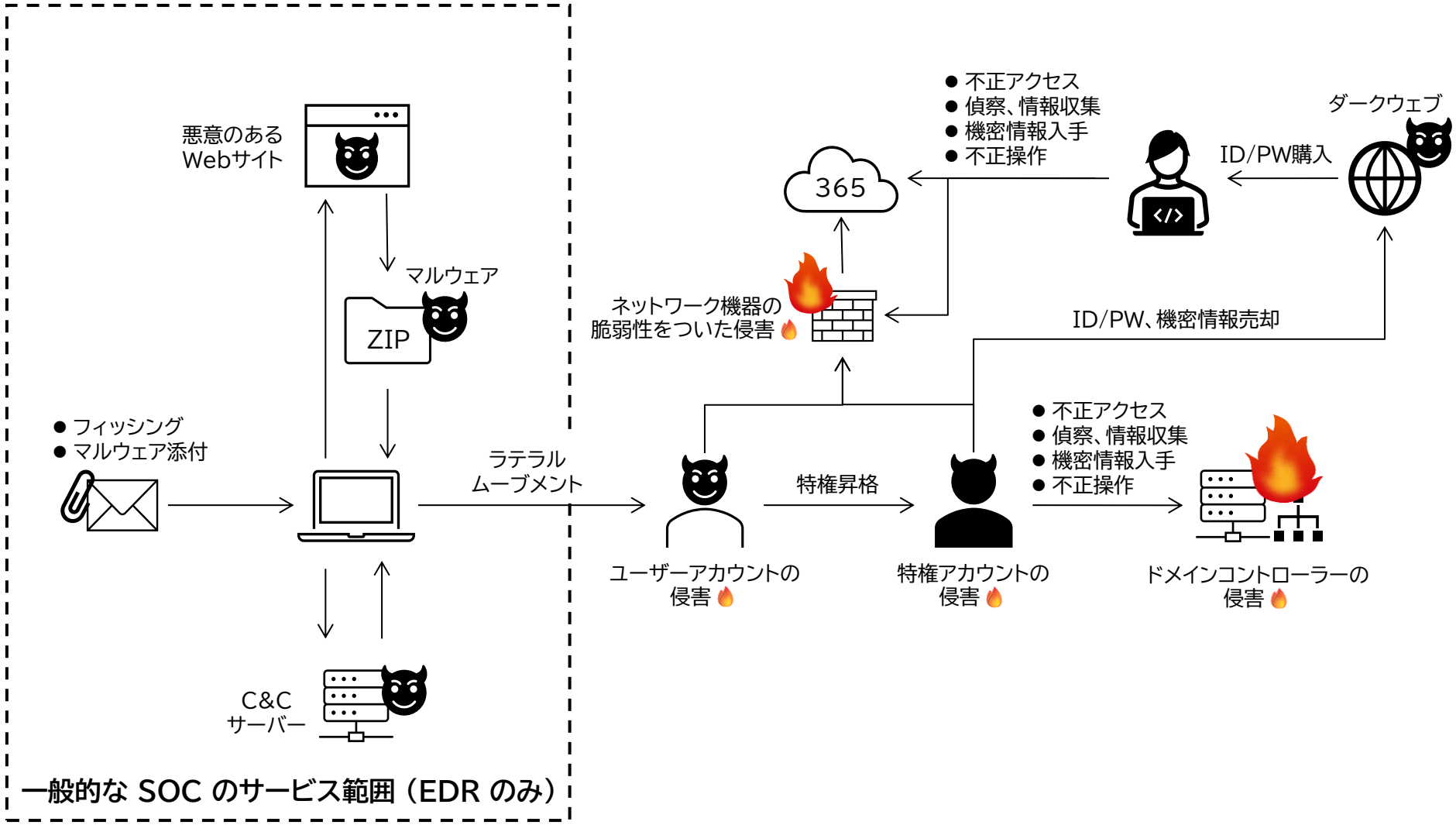
SecureQUEST の監視サービス

アラートのクローズまでしっかり伴走、アラート発報で終わりません

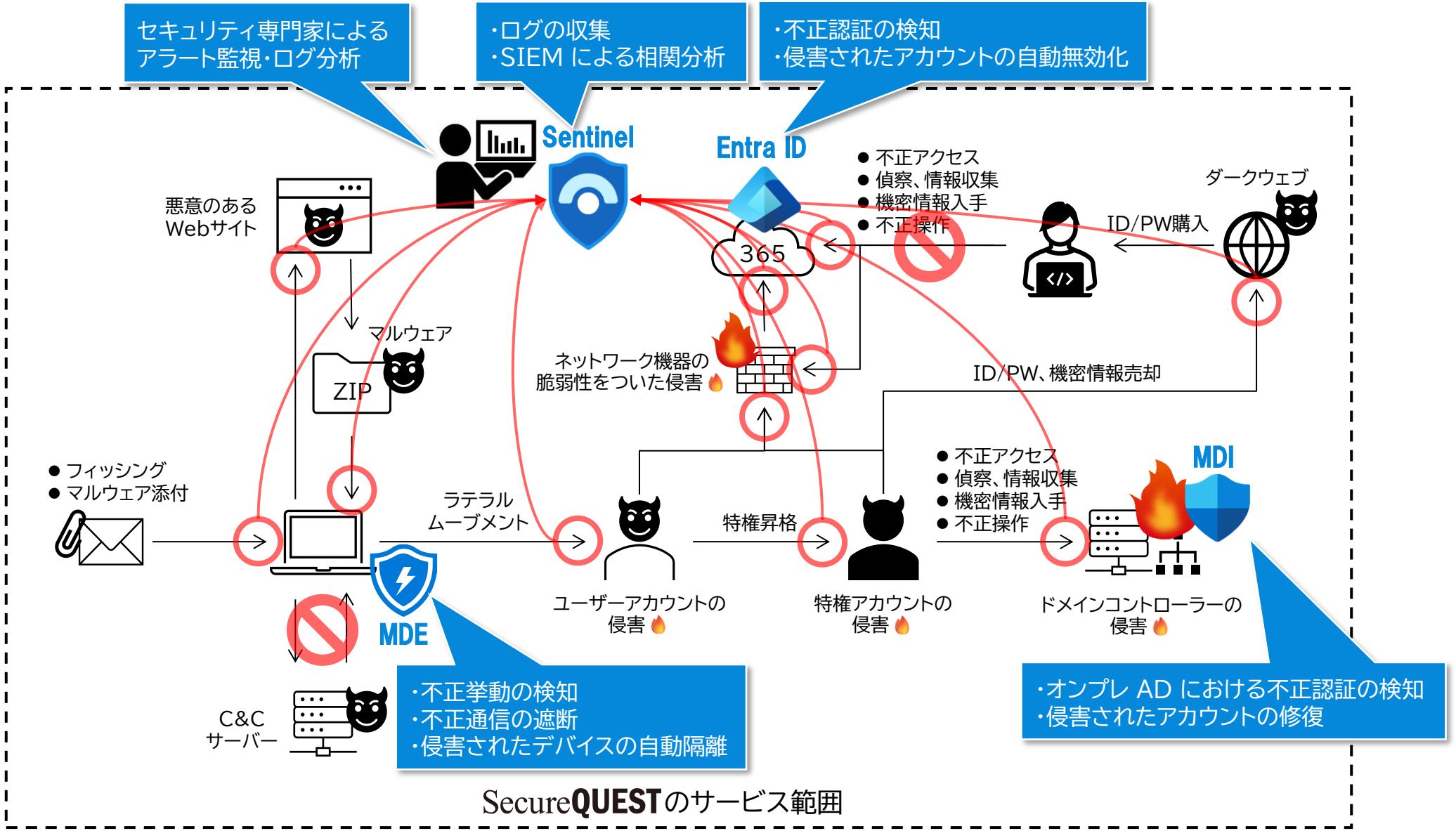


SecureQUEST の監視サービス

必要な監視はできていますか？

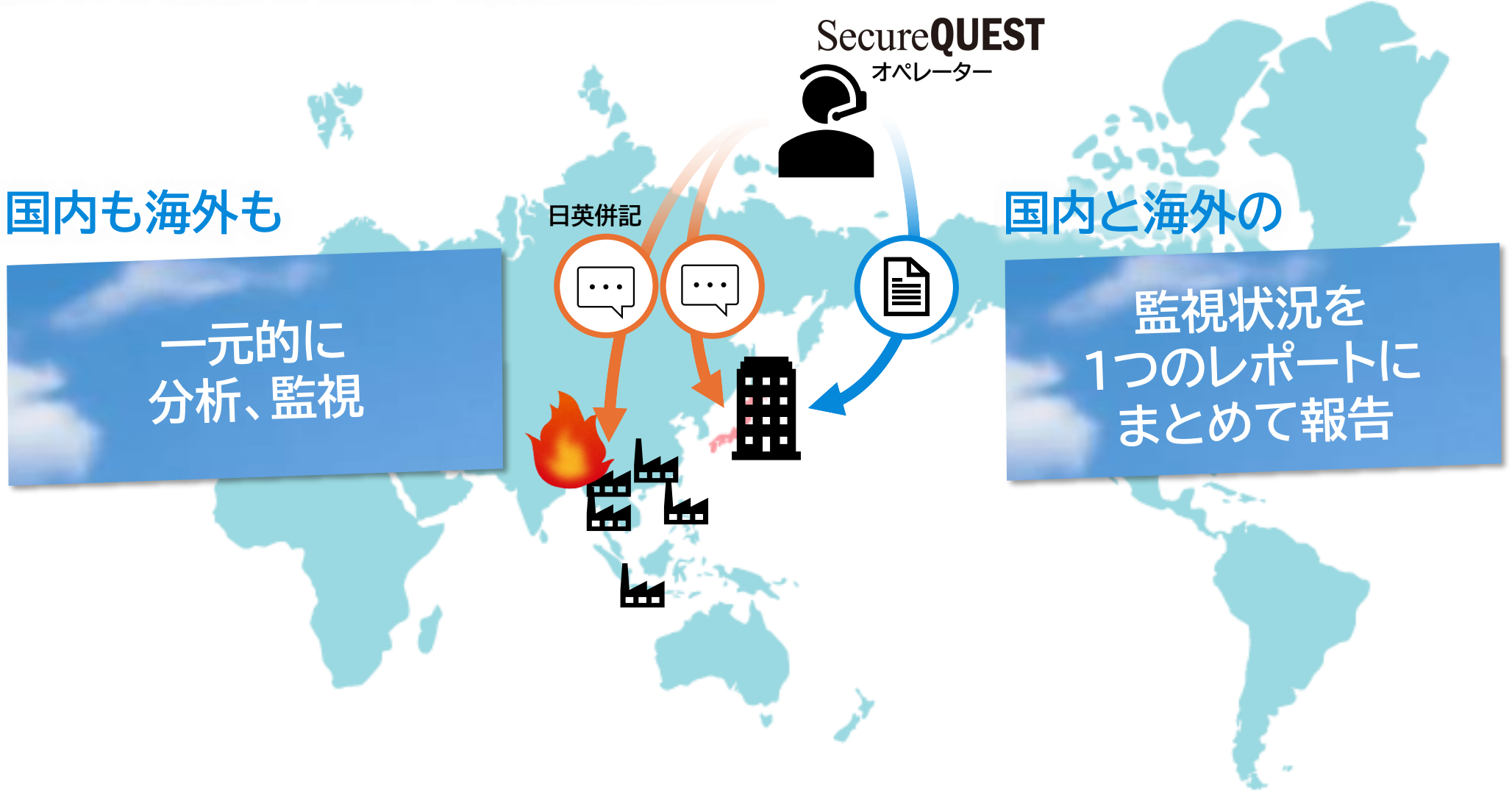


SecureQUEST の監視サービス



海外拠点もまとめて監視

海外拠点のリスク把握、セキュリティ統制を支援します



監視サービス / 伴走サポート

SecureQUEST 伴走サポート 3つの特長

1 段階的なセキュリティ強化に伴走

お客様の状況に応じて段階的かつ継続的なセキュリティ強化のサイクルを回します！

2 勝手に変わる Microsoft 365 への対応に伴走

勝手に増える、勝手に変わる Microsoft 365 の機能。把握も調査も実装も大変ではないですか？

3 となりの席の同僚のようにひとり情シスに寄り添う伴走

社内に相談相手はいますか？ SecureQUEST のご相談窓口は同僚と同じで回数無制限です！

SecureQUEST の伴走サポート

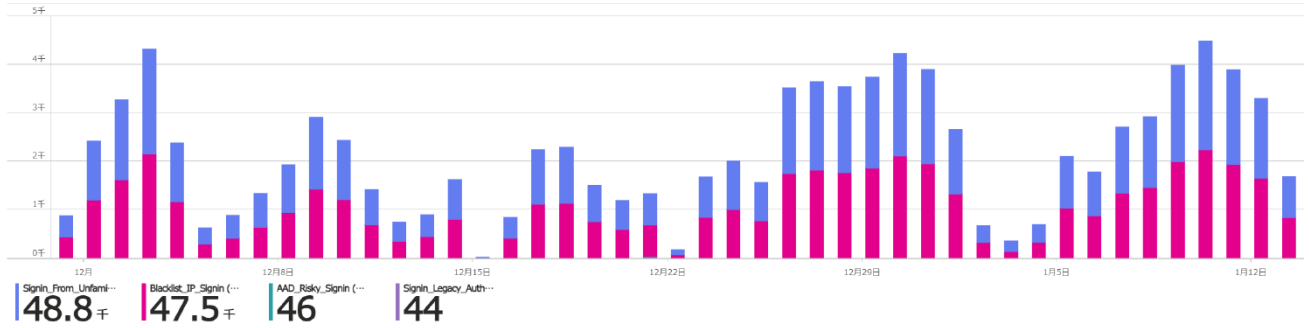
アラート監視を行い短期的なリスクに対応しながら
段階的かつ継続的なセキュリティ強化で中長期的なリスクに対応します

SecureQUEST の伴走サポート

月次レポートでは監視状況を丁寧に解説します

1-3. 不審なサインインの状況

正規アクセス以外の、不正アクセスや不審なアクティビティを成功・失敗を問わずグラフ化したものです。



■サマリ

- 一か月を通して、海外から Blacklist IPアドレス を用いた不審なサインイン試行が行われています。（下記ユーザーアカウント以外は全て認証失敗）
- 全体としては、下記 2 ユーザーアカウントに対して、攻撃と思われる不審なサインインのパスワード認証の成功を確認しています。多要素認証の要求設定や強固なパスワードが使用されているか、また攻撃者が狙いやすい命名を避けるなど、認証セキュリティの強化を推奨いたします。

➢ 対象ユーザー：

加えて

優先対応すべき対策を手順付きで推奨
Microsoft 365 の機能拡張にしっかり伴走

2.2 推奨事項 – 前項 No.1 手順

管理ロールのすべてのユーザーに対して多要素認証が有効になっていることを確認する

管理ロールを持つユーザーに対して多要素認証を必須にします。

名前 *
管理者 - すべてのクラウドアプリ - 多要素認証…

割り当て
ユーザー
組み込まれた特定のユーザー および 除外された特定のユーザー
ターゲット リソース
すべてのクラウド アプリ
条件
1 個の条件が選択されました

アクセス制御
許可
1 個のコントロールが選択されました
セッション
0 個のコントロールが選択されました

設定手順

1. Azure Portal にサインインし、
   Microsoft Entra ID → セキュリティ → 条件付きアクセス → ポリシー を開きます。
2. 「＋新しいポリシー」をクリックします。
3. ポリシーにわかりやすい名前を付けます（例：「管理ロールに対するMFA要求」）
4. 「ユーザーとグループ」を選択し、対象の管理ロールを持つユーザーまたはグループを選択します。
   「ディレクトリロール」をチェックし、必要な管理ロールを選択します。
   少なくとも次のロールを保護します。
   - グローバル管理者
   - 認証管理者
   - 課金管理者
   - 条件付きアクセス管理者
   - Exchange 管理者
   - ヘルプデスク管理者
   - セキュリティ管理者
   - SharePoint 管理者
   - ユーザー管理者

   ※ブレークグラスアカウントが存在する場合、必ずこれを「対象外」に設定します。
5. 「ターゲットソース」を選択肢、「すべてのクラウドアプリ」を選択します。
6. 「条件」を選択し、必要に応じて追加の条件を設定します。
   （例：場所、デバイス状態、リスクレベルなど）。
7. 「アクセス制御」を選択し、「許可」タブを開き、「多要素認証を要求する」をチェックします。
8. ポリシーの有効化を「オン」に設定し、「保存」をクリックします。

これで、選択した管理ロールを持つユーザーに対して多要素認証を要求する条件付きアクセスポリシーが作成されます。変更を有効にするには、しばらく時間がかかる場合がありますのでご注意ください。

※ネクストリード社およびエフ・シー・シー社のゲストユーザーは、各社テナントにおいて多要素認証を適用済みですので、本ポリシーの対象外として設定をお願いいたします。

Next Read

お客様 1社 1社に寄り添うご相談窓口

不確実な時代に必要なのは画一的なソリューションではなく、伴走するパートナーではないでしょうか

内部環境

- 組織ごとに
  - 経営課題が違う
  - システム環境も守るべき情報資産も違う
  - セキュリティに掛けられる予算、工数が違う
- DXによるデジタル利活用範囲の拡大
- 気軽に相談できる相手がいない

外部環境

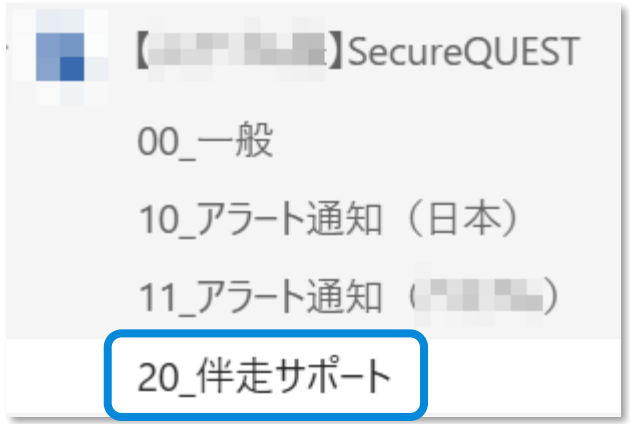
- サイバー攻撃の激化
- セキュリティ対策技術の進化の加速
- セキュリティ対策ソリューションの多様化
- 業界、顧客からの要求が難化、増加

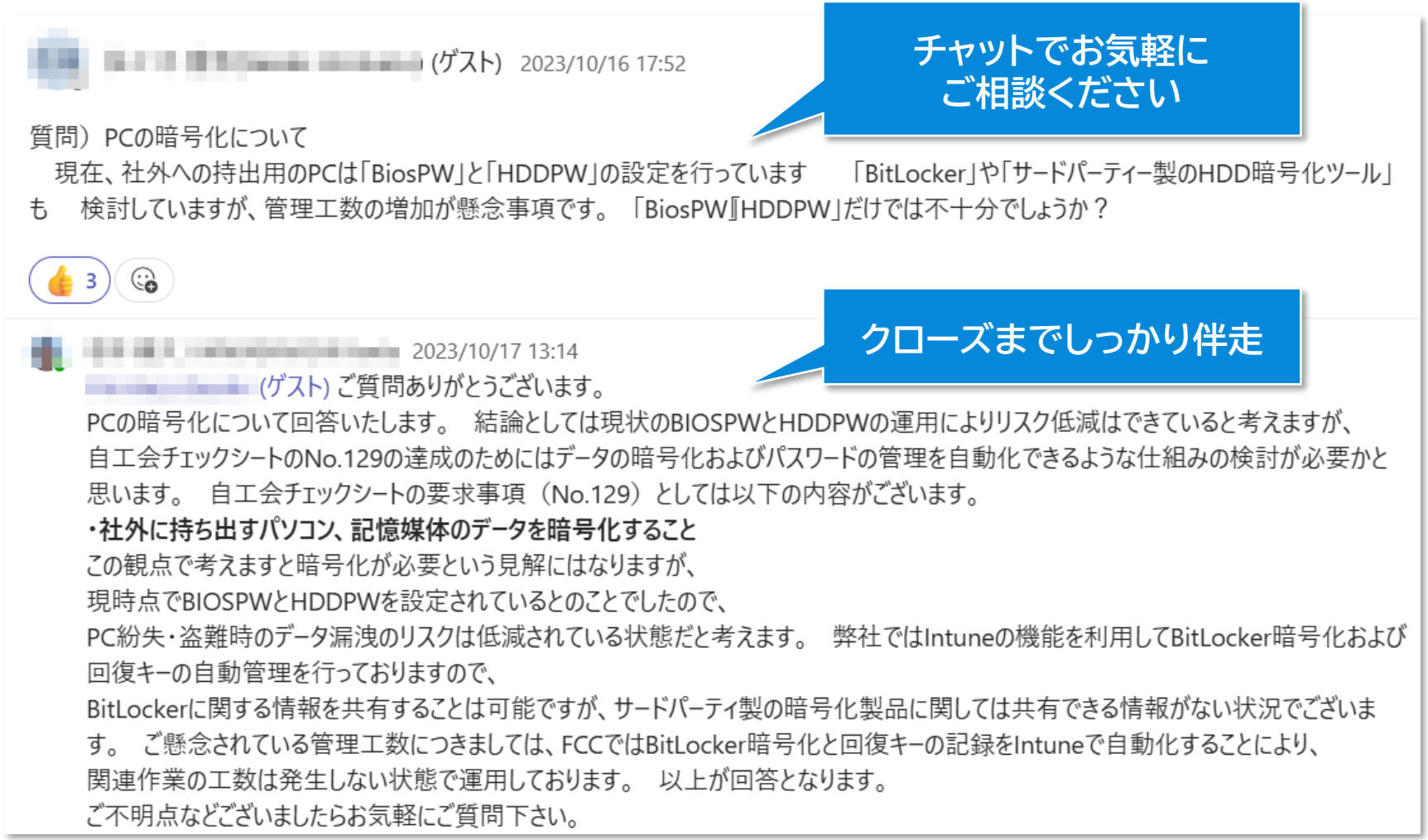
残念ながら、どの組織にも適合するマスターキーのような「答え」はありません

ベンダーではなく、コンサルタントでもない
自動車産業サプライヤーの情報システム部門の当事者である私たちが
お客様と一緒に悩み、一緒に考え、仲間として伴走します

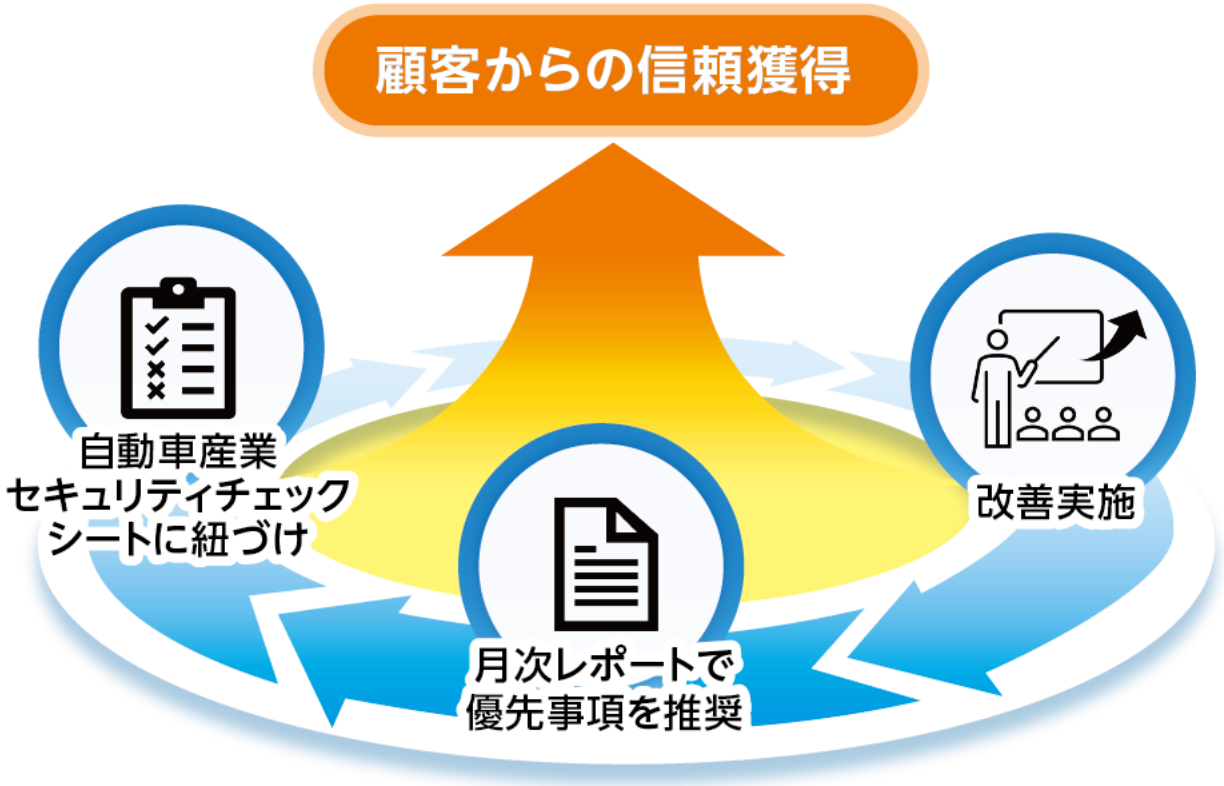
お客様 1社 1社に寄り添うご相談窓口

お気軽にご相談ができるよう、回数無制限のご相談窓口を Teams チャットにご用意しています





自動車産業セキュリティチェックシートに準拠してレベル上げ



対応項目の一例

17	Lv.2	サイバー攻撃や予兆を監視・分析をする体制を整備している
117	Lv.1	ユーザーID及びシステム管理者IDは定期的、または必要に応じて棚卸を行ない、不要なIDを削除している
122	Lv.3	認証ログのモニタリングを実施している
142	Lv.2	通信内容を常時監視し、不正アクセスや不正侵入をリアルタイムで検知/遮断および通知する仕組みを導入している
145	Lv.2	ログを分析し、サイバー攻撃を検知する仕組みを導入している
146	Lv.2	社内に侵入したマルウェアと不正なサーバーとの通信を遮断する対策を実施している

自動車産業サイバーセキュリティガイドラインとは？

自動車産業は多くのサプライヤーと連携して製品を製造しており、サプライチェーン全体を通じてセキュリティを確保するための対策が盛り込まれています。
情報資産の管理、アクセス権の制御、マルウェア対策などの基本的なセキュリティ対策やリスク管理の考え方はあらゆる業界に共通する課題です。

SecureQUEST プラン

Basic プラン

アカウント認証のセキュリティ対策、
監視を強化したいお客様

◆ 監視サービス

100 ユーザーまで
50,000円/月
（税込 55,000円/月）

101 ユーザー以降は 1 ユーザー当たり
500円/月
（税込 550円/月）

監視対象：
・アカウント認証

◆ 伴走サポート

150,000円/月
（税込 165,000円/月）

Standard プラン

アカウント認証に加え、エンドポイントを
監視したいお客様

◆ 監視サービス

100 ユーザーまで
74,000円/月
（税込 81,400円/月）

101 ユーザー以降は 1 ユーザー当たり
740円/月
（税込 814円/月）

監視対象：
・アカウント認証
・EDR（PC）
・EDR（サーバー） **※別途費用**

◆ 伴走サポート

150,000円/月
（税込 165,000円/月）

オプション

★ **ネットワーク機器監視**

★ **別テナントの監視**

★ **ログ保管 1年間**
（標準では 3か月間）

★ **ログ保管 日本リージョン**
（標準では U.S. リージョン）

ご相談ください

※ 表示価格は全て税抜きです。
※ 契約上のユーザー数はサインインの可能性がある自社テナントで作成されたユーザー数です。
※ 契約期間中にユーザーが増加した場合は再計算となりますが、+10% までの増加分は次回契約更新まで猶予します。
※ 契約後のプラン変更も可能です。
※ 監視サービスは 24 時間 365 日監視、リスクレベル【高】のアラートが発報された場合、対象デバイスの通信を自動で遮断し被害拡大を防ぎます。
※「伴走サポート」の受付時間は月–金曜 9:00 – 17:00 です。弊社休業日を除きます。

伴走はご契約前から始まります

ご検討にあたり各種情報提供、お試し、ご相談をすべて無償で承ります

STEP 1

資格情報漏えい診断

貴社のID・パスワードがダークウェブに漏えいしていないか診断します

STEP 2

脅威可視化アセスメント Light

貴社の Microsoft 365 環境の生のログを分析し、貴社に実際に迫っている脅威を可視化
セキュリティ強化の推奨事項も記載した簡易レポートをご提供し web 会議で解説します

STEP 3

無料体験版（1か月間）

本番とほぼ同等のサービスを1か月間無料でお試しください
月次レポートのご提供と web 会議での解説も付いています

STEP 4

Microsoft ライセンスのご相談

どのライセンスで何がどこまでできるのか？いちばんお得な買い方は？
お客様の課題を伺い、分かりづらい Microsoft ライセンスをコーディネートします

STEP 5

コストシミュレーション

現状と比較したコストシミュレーションを行います
コストだけでなく、セキュリティ強化のシナリオ作りもサポートいたします

敵を知り己を知れば百戦殆からず

まずはお気軽にお問い合わせください

SecureQUEST お問い合わせフォーム

公式HP：https://securequest.world/

APPENDIX

脅威可視化アセスメント Light 簡易レポート

[redacted]株式会社　様のポイント

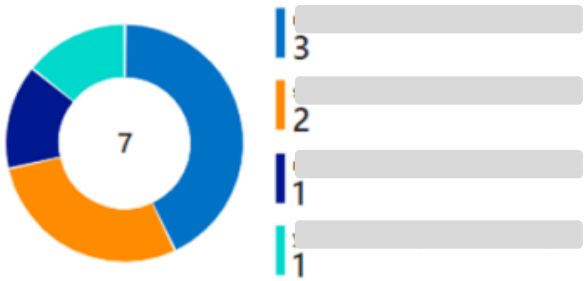
外部からの攻撃が確認されました。セキュリティ構成の強化や継続的なモニタリングによってさらに安心な環境を構成できます。

●IP 許可ポリシーにより配信されたメールの IP アドレス

- 18.177.156.1
- 18.177.156.2
- 18.177.156.10
- 18.177.156.11

※すべて ISP は Amazon.com（東京）

●リスク判定されたサインイン

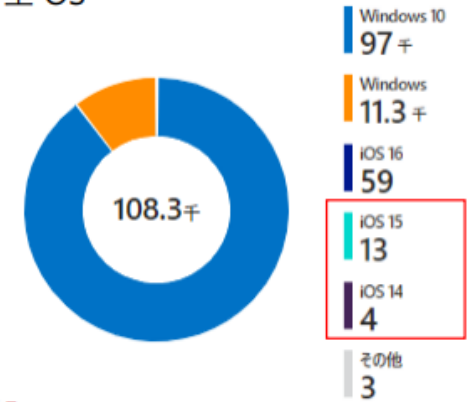


●漏洩した資格情報

UserId	Sources
[redacted]	[]
[redacted]	["bmifm.com"]
[redacted]	["lube.co.jp"]
[redacted]	[]
[redacted]	["shusyoku.net"]
[redacted]	["lube.co.jp"]
[redacted]	[]
[redacted]	[]

複数のセキュリティインテリジェンスで検知

●全 OS



Point 1. IP 許可ポリシーによるメール配信

IP 許可ポリシーによるフィッシングメール配信のアラートが 34 件検出されました。
このアラートは、信頼性の高いフィッシングメッセージが IP 許可ポリシーによりメールボックスへ配信されたことを示します。

IP許可リストにIPアドレスを指定しますと、登録範囲内からのすべてのメッセージが強制的に配信されるため、フィッシングやマルウェアの脅威のあるメールも配信されることが懸念されます。

実際に脅威があるメールかの確認と、この IP 許可ポリシーを無効化した際の業務影響を調査する必要があります。

Point 2. AI がリスク判定したサインイン

Entra ID がリスクを検知したサインインが 9 件検出されました。このリスク判定は Entra ID 側で普段の傾向と比較して判断されるため、普段使用しない IP アドレスやデバイスからアクセスがあった場合にそれを知ることができます。
今回はすべてが「低リスク」であり、調査の結果ユーザー本人による問題のないサインインと考えております。

リスクは「低」「中」「高」の三段階で判定され、攻撃で使用されている既知の IP アドレスからのサインインやアカウントが乗っ取られている可能性が高い場合などは「高」として検出されます。リスクの状態をすぐに知ることができれば、当該ユーザーのパスワード変更などの対応をスムーズに行うことができます。

漏えいした資格情報

ブラックマーケットに漏えいした資格情報 (ID とパスワードの組み合わせ) が 8 件検知されました。
現在の Office 365 の資格情報が同じ場合は不正サインインの対象になる可能性があります。
また、現在の資格情報と異なる場合であっても、攻撃のユーザー リストとして再利用されるため不正なサインインがないか注意する必要があります。

その他のリスク

- 古いバージョンの iOS からのサインイン
- メール転送設定 5 件
- OAuth アプリへの権限委任の同意 2件
- クラウドプラットフォームからのサインイン（失敗）1件

推奨事項

短期的な実施
- リスクがあるユーザーのパスワードリセット
- サインインや Office 365 不正利用の監視

中長期的な検討（例）
- メール配信ポリシーの見直し
- メール転送設定のフローの整備
- OAuth アプリの登録フローの整備
- iOS のバージョンアップデートフローの整備
- MFA およびパスワードレス認証の推進

ランサムウェア被害事例をもとにした機能説明

平時(侵入前)における主なリスクと対策機能

RISK 1 資格情報がダークウェブに漏えい

- 機能 ダークウェブへの漏えいをモニタリングし検知次第情報を提供
- 機能 30日間以上サインインされていないアカウント情報の棚卸

RISK 2 不正サインインの試み

- 機能 普段アクセスのない国、アプリ等からのサインインの監視
- 機能 多要素認証、デバイス認証、条件付きアクセス等によるアクセス制御
- 機能 30日間以上チェックインされていないデバイス情報の棚卸

RISK 3 一般ユーザーによる不審なアプリへの権限付与

- 機能 新規登録されたアプリの不審性調査、アラート発報
- 機能 ポリシーにより新規アプリの登録を制限

ランサムウェア被害事例をもとにした機能説明

侵入時における主なリスクと対策機能

RISK 1 不正な侵入の試み

- 機能 ファイアウォールのログ、Entra ID サインインログ、エンドポイントのログのアラート監視、相関分析
- 機能 高いリスクレベルを検知した際のデバイス自動隔離、アカウント自動無効化
- 機能 多要素認証、デバイス認証、条件付きアクセス等によるアクセス制御

RISK 2 誤検知、過検知が多い場合のアラート見逃がし

- 機能 オペレーターによる相関分析の結果、必要と判断されたアラートのみ発報
- 機能 過検知の場合、都度チューニング
- 機能 アラート発報後、事務局による対応状況確認、管理表による進捗管理

ランサムウェア被害事例をもとにした機能説明

侵入後における主なリスクと対策機能

RISK 1 ラテラルムーブメント(水平移動)による探索、アカウント侵害

- 機能 Entra ID および オンプレの Active Directory でのアカウント侵害の監視
- 機能 認証ログ、エンドポイントのログの相関分析

RISK 2 エンドポイントへの侵入

- 機能 EDR により不審な振る舞いを検知、検疫、アラート発報

RISK 3 EDR の無効化

- 機能 無効化の試みを検知、アラート発報

アラート通知例

Teams 内 お客様専用チームのアラートチャネル / SharePoint リストを活用したアラート管理表

Confirmation

下記デバイスにおいて、下記の不審なファイルが検知されました。

ファイルは Defender によってブロックされ検疫されているため問題はございません。

しかし、今回検知したファイルは WEB 検索するとゲームアプリとして確認ができたため、
業務利用であるか判断いたしかねましたので念のため、ご連絡いたしました。

フリーソフトにはマルウェアが混入するものや望ましくない振る舞いをするものがありますので、
業務で必要な場合は組織で許可されたソフトウェアのご利用をご検討いただけますと幸いです。

なお、下記のファイルは 製品 Tetris の一部でした。

確認いただきたいこと
■ファイルの入手元は明確になっている問題ないファイルでしょうか。不要な際はファイルの削除をお願いいたします。

なお、ファイルパスより USB などの外付けデバイスかと存じますので、
ご使用の場合はフォーマットを実施いただいてからご利用いただければと存じます。

もし、意図的にファイルの操作を行っていない場合は、端末のフルスキャンの実施をお願いいたします。

※Windows 設定 > プライバシーとセキュリティ > Windowsセキュリティ（を開く）
ウィルスと脅威の防止 > スキャンのオプション > フルスキャン

・アラート検知日時：2024/07/03 10:34 頃
・ユーザー：[redacted]@worldfcc.com
・デバイス名：[redacted]
・ファイル名：[redacted]
・ファイルパス：D:\Part control Sale\รถบรรทุก การจัดรถ\นพดล\New Folder (4)[redacted]
（SHA1：7371b2c1eabab38dd70cad3a42f4cda0228236c1）Virustotal 検出：39/74

お手数ですが、ご確認よろしくお願いいたします。

ConfirmationEn

The following suspicious file was detected on the device below.

There is no problem as the file has been blocked and quarantined by Defender.

However, the file detected this time could be identified as a game application when searched on the web, so we could not determine whether it was for business use and decided to contact you just in case.

Free software often contains malware or behaves in undesirable ways, so if necessary for your work, we would appreciate it if you could consider using software approved by your organization.

Moreover, the file below was part of the product Tetris.

What we would like you to confirm
■Is the source of the file clear and is there no problem with the file? If not necessary, please delete the file.

From the file path, it seems to be an external device such as a USB, so if you are using it, we would appreciate it if you could format it before using it.

If you have not intentionally manipulated the file, please perform a full scan of the terminal.

※Windows Settings > Privacy and Security > Open Windows Security
Protection Against Viruses and Threats > Scan Options > Full Scan

---
・Alert detection date and time: Around 10:34 on July 3, 2024
・User:[redacted]@worldfcc.com
・Device name:[redacted]
・File name:[redacted]
・File path: D:\Part control Sale\รถบรรทุก การจัดรถ\นพดล\New Folder (4)
(SHA1: 7371b2c1eabab38dd70cad3a42f4cda0228236c1) Virustotal dete
---

We apologize for the inconvenience, but we appreciate your confirmatio