セキュリティマネージドサービス説明資料

マイクロソフト
統合セキュリティ監視サービス
「Azure Sentinel」Ver.1.0

PSC SECURITY
すべてのオンラインビジネスに安心を

会社紹介

Company introduction

PSC
POWER
STAFF
COMMUNICATIONS

2022

会社概要

1996年創業
今年25年目を迎えるDX COMPANY

株式会社 ピーエスシー

POWER STAFF COMMUNICATIONS

設立	1996年9月
決算期	3月
社員数	701名（2021年4月1日現在）
住所	〒105-0011 東京都港区芝公園 2-2-18 オーク芝公園ビル TEL 03-3435-1044 / FAX 03-3435-1418
資本金	1億8,778万円
業績	売上高：11,750百万円（2021年3月期実績）
代表	鈴木 正之
関連会社	ピーエスシー琉球 ピーエスシースマイル ピーエスシーテクニカルサービス

会社概要

全てのステークホルダーに安心感と信頼を

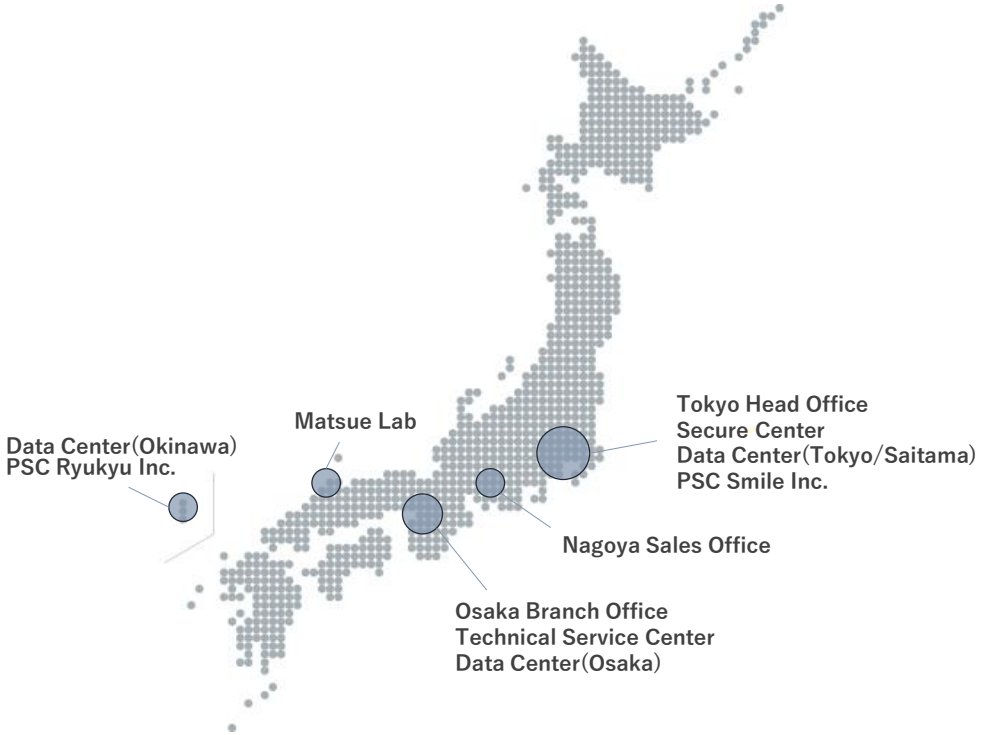
認証登録・資格・認定

・品質マネジメントシステム認証
・情報セキュリティマネジメントシステム（ISMS）認証
・プライバシーマーク
・健康経営優良法人 大規模法人部門認定
・データ適正消去実行証明協議会　消去プロセス認証
・くるみんマーク
・銀の認定マーク

加盟団体

・ 一般社団法人ソフトウェア協会（SAJ）
・一般社団法人日本コンピューターシステム販売店協会(JCSSA)
・一般社団法人 IT資産管理評価認定協会（SAMAC）
・ADEC データ適正消去実行証明協議会
・一般社団法人日本コールセンター協会（CCAJ）
・一般社団法人コンピュータソフトウェア著作権協会（ACCS）

拠点・事業所



東京本社

芝園DXフロア

■東京本社
東京都港区芝公園 2-2-18 オーク芝公園ビル
■西日本支社
大阪府大阪市中央区高麗橋3-2-7　ORIX高麗橋ビル4F
■名古屋営業所
愛知県名古屋市中区錦1-13-26 伏見スクエアビル12F

■ピーエスシー琉球（子会社）
■ピーエスシースマイル（特例子会社）

□芝園DXフロア
□PSCセキュアセンター
□PSCデータセンター
□テクニカルサービスセンター
□松江ラボ

ビジネスパートナー

・日本アイ・ビー・エム株式会社　ビジネスパートナー
・日本マイクロソフト株式会社認定ソリューションプロバイダー
・日本ヒューレット・パッカード合同会社
・グーグル合同会社 Google Cloud Partner
・SCSK株式会社
・デル・テクノロジーズ株式会社
・クエスト・ソフトウェア株式会社
・シスコシステムズ合同会社　プレミア認定パートナー
・株式会社エムアンドシーシステム
・Coltテクノロジーサービス株式会社
・ヴイエムウェア株式会社
・株式会社オプテージ

コラボレーション

ビジネスを互いに進化させるパートナーシップ

01

Azure Sentinelを活用したセキュリティ分析

セキュリティ運用のよくある課題

セキュリティ
人材不足

SIEMの導入・展開
コストが高額

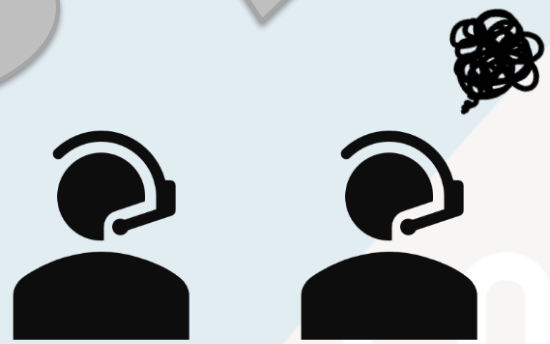
大量のアラート生成
によるバックログ
の増加

サイバー攻撃の
高度化

セキュリティログが増える
につれてインフラコスト
の増加

自動化の実装
が困難

セキュリティログを
入れる手間がか
かる

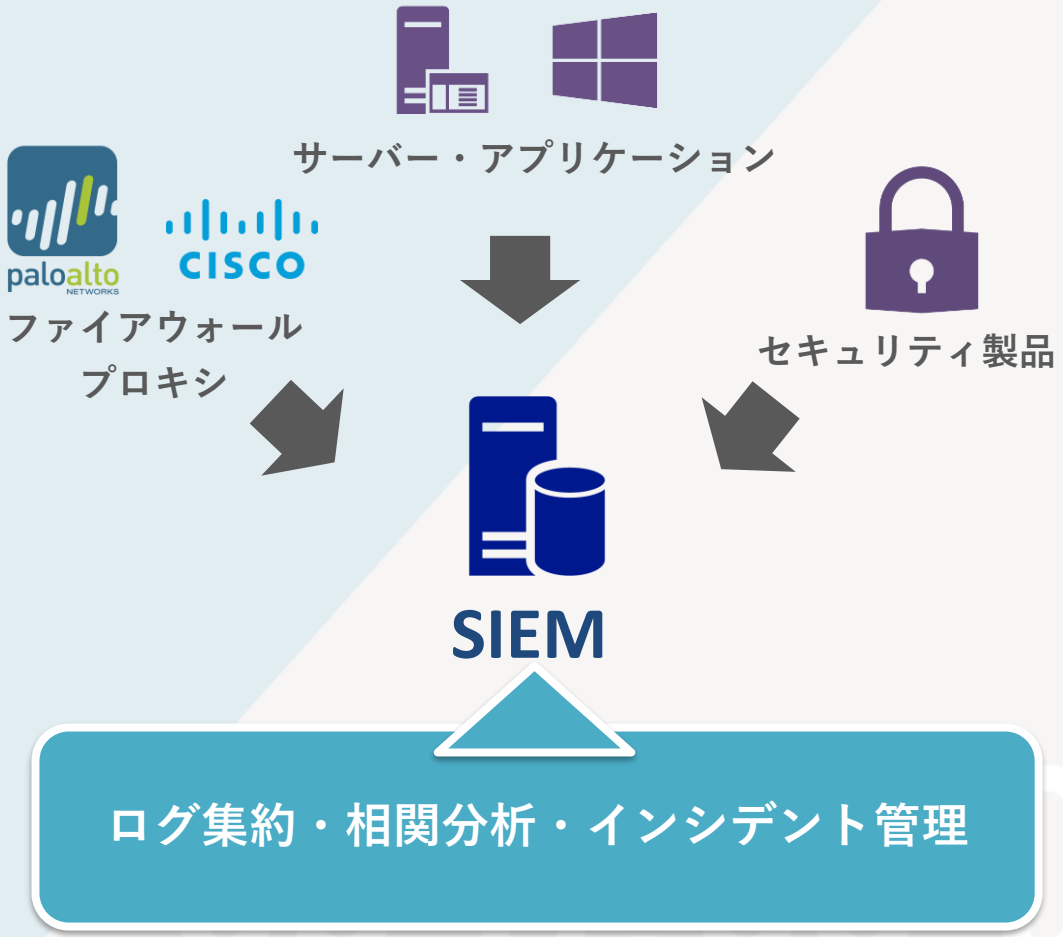


「Azure Sentinel」運用サービス –PSC インテリジェンスサービス-

分析

■なぜSIEMが必要か？

昨今の情報セキュリティにおける「脅威」及び「リスク事象」となる事項について，NIST SP800-30（情報セキュリティリスクアセスメントの実施の手引き），ISO/IEC 27005（情報セキュリティリスクマネジメント）等の複数のグローバルスタンダードのガイドラインでも見られる通り，攻撃者の攻撃パターンをシナリオにした「リスクシナリオ」がありますが、通常のセキュリティ製品だけではすべての攻撃シナリオに対応することが困難です。複数のシステムから収集されるログから相関的に見ることでリスクシナリオに沿ったセキュリティ運用を実施することができます。

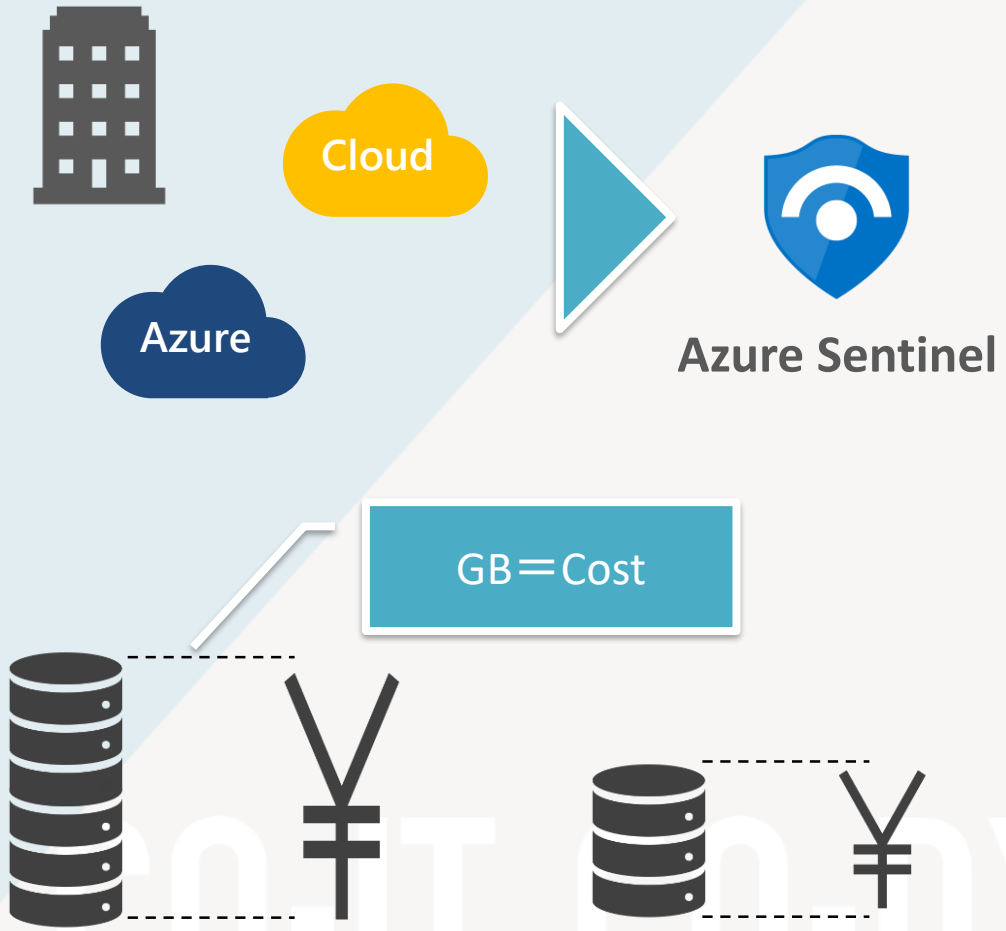


「Azure Sentinel」運用サービス　–PSC インテリジェンスサービス-

分析

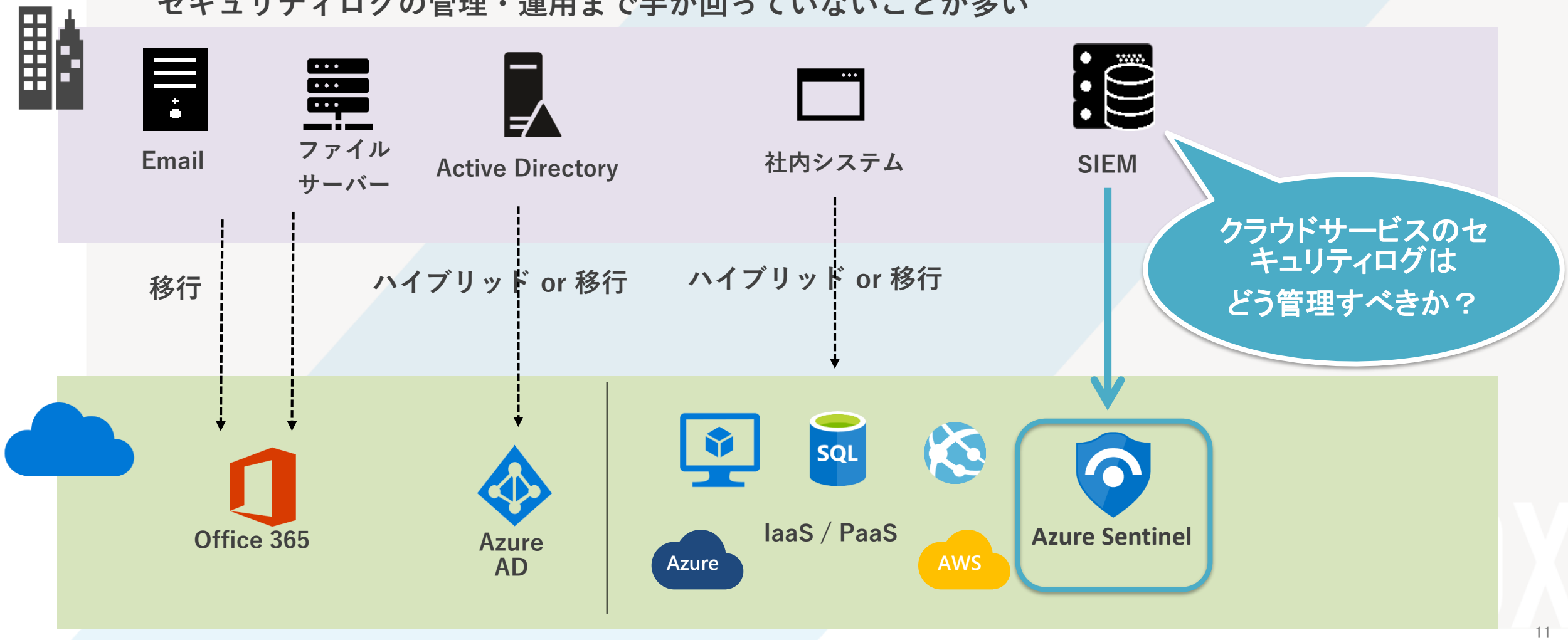
■なぜマイクロソフトなのか？

クラウドネイティブな SIEMとして、Azureはもちろんオンプレミス環境、他のクラウド環境のシステムなど、さまざまな環境のログ統合管理が可能です。
通常のSIEM製品と違い、ログの利用量に合わせた従量課金体系となっており、年間利用金額も比較的リーズナブルであるうえで、メンテナンスが不要なクラウドサービスという非常に強力なSIEM製品となっています。



ハイブリッドクラウド・マルチクラウドへの変化と SIEM

企業 IT がハイブリッドクラウド・マルチクラウドへ変化する中、クラウドサービスの
セキュリティログの管理・運用まで手が回っていないことが多い



Azure Sentinel の 4 つの基本機能

データ収集

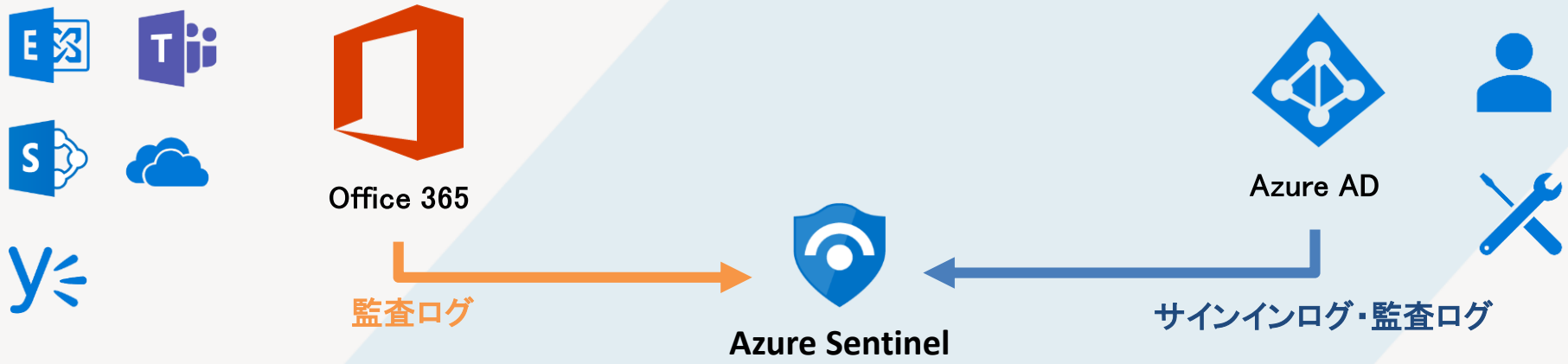
検知

調査

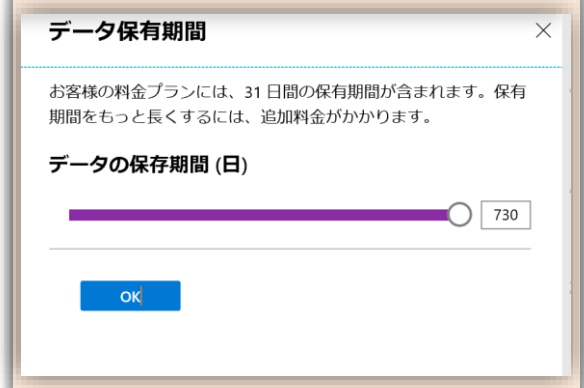
対処

Sentinelの役割① »» Office 365のログ管理ソリューションとして

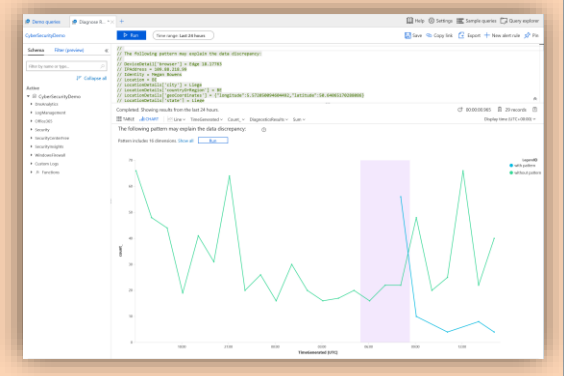
Office 365の管理ログと、Azure Active Directoryの
サインイン・監査ログを一括長期管理が可能



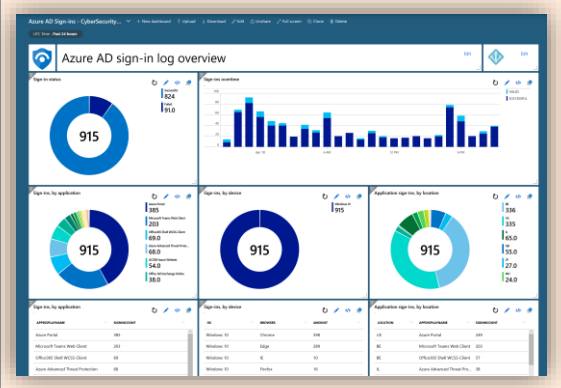
最長2年間の保存



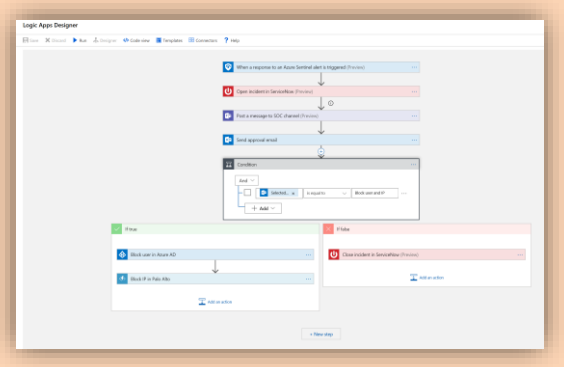
必要なデータの検索



ダッシュボードによる可視化



対処の自動化



Sentinelの役割② »»

Microsoft 365 E5とサードパーティの セキュリティ製品の統合分析・可視化環境として

Microsoft 365 E5 セキュリティ製品のアラートとサードパーティ製品のアラートを管理・相関分析

Office 365 ATP
Email

Azure AD Identity Protection
ID

Microsoft Defender ATP
エンドポイント

Azure ATP
オンプレミスAD

Cloud App Security
SaaS

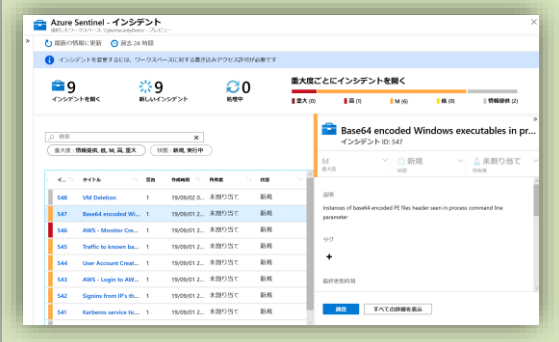
サードパーティ製品

セキュリティアラート

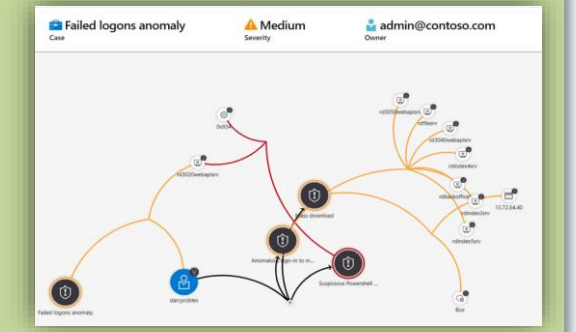
Azure Sentinel

セキュリティアラート

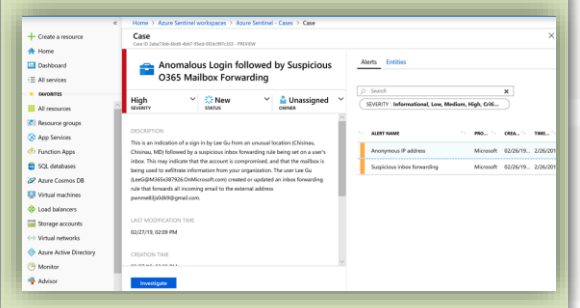
イベントの一元的な管理



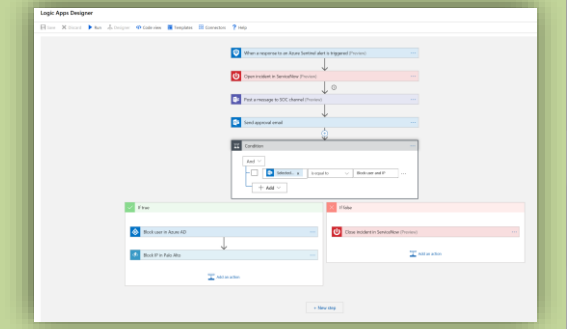
相関分析



Fusionによる 重要インシデント特定

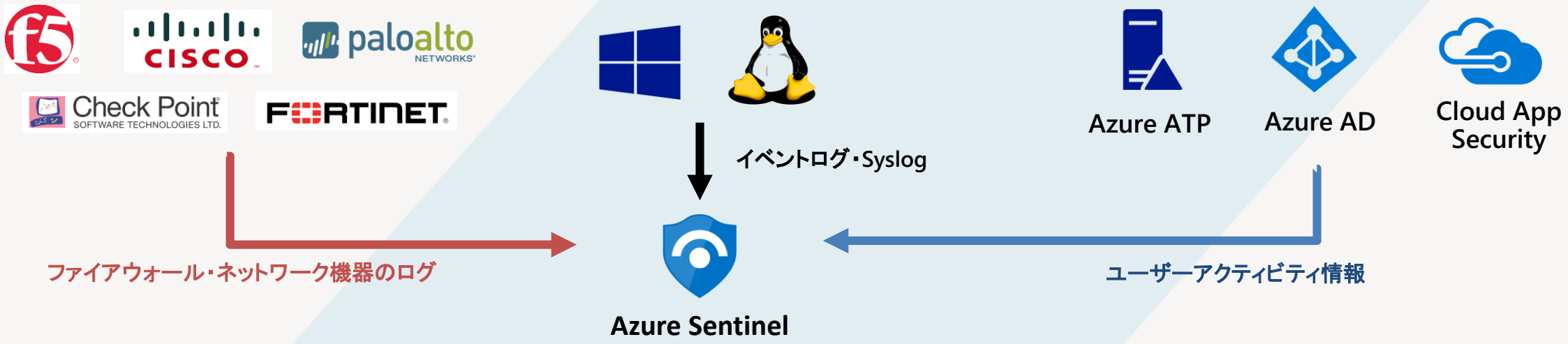


対処の自動化

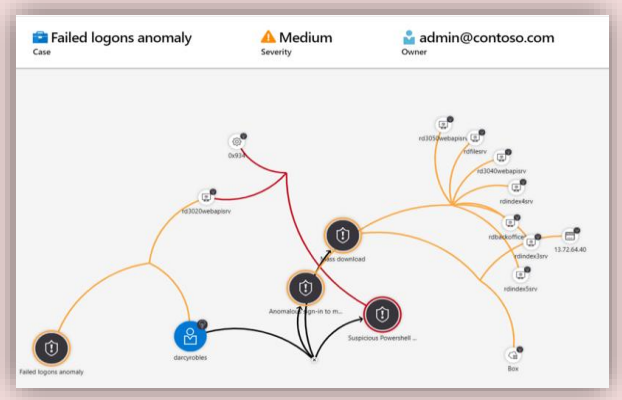


Sentinelの役割③ »» クラウド時代の SIEM として

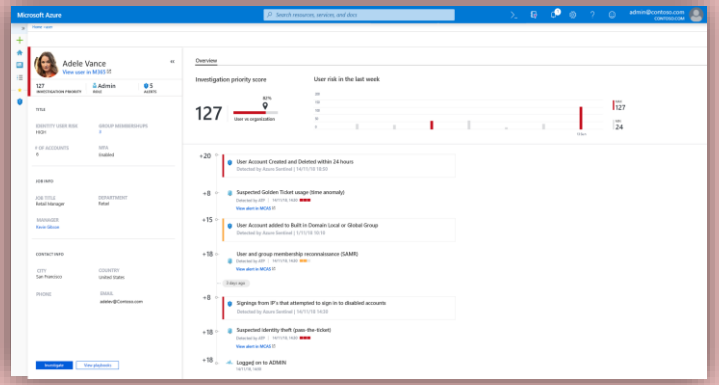
オンプレミス対象のSIEM & SOAR 機能に加え、クラウドのデータも扱えるSIEM & SOAR as a Service (UEBA coming soon)



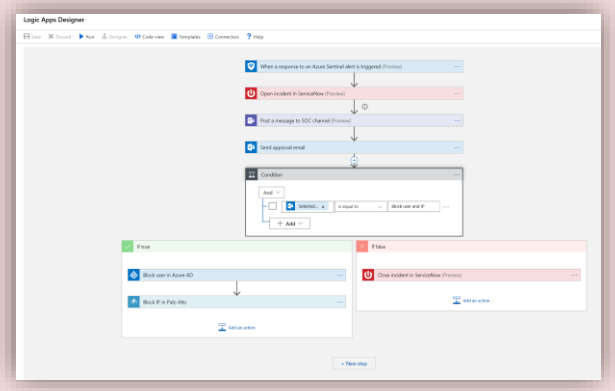
SIEM



ユーザー分析



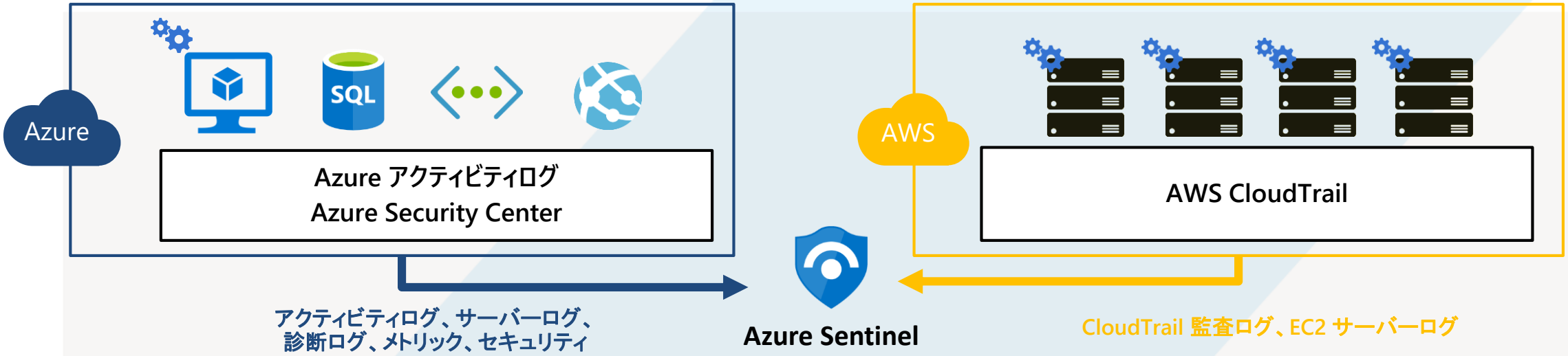
SOAR



Sentinelの役割④

マルチクラウド環境の統合監査ログ基盤として

Azure に加え、Amazon Web Service の監査ログ・サーバーログも統合管理が可能



クラウド監査ログ

- リソースの操作
- IAMの設定
- ユーザーアクティビティ
- クラウド正常性

サーバー・リソースログ

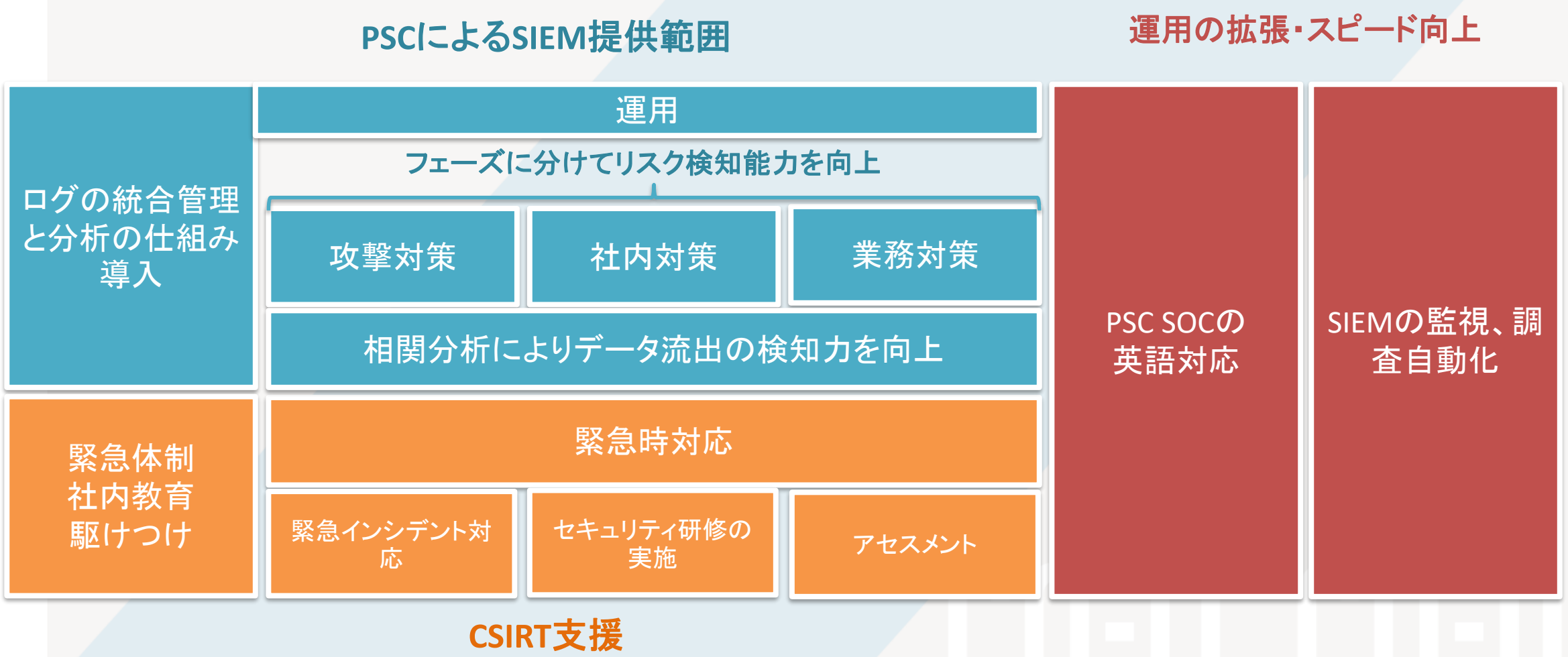
- イベントログ・Syslog
- 死活監視
- アクセスログ
- パフォーマンスログ

セキュリティ・コンプライアンス確保の高速化・一元化

02

Azure Sentinelを活用したセキュリティ運用

SIEMを活用した導入と運用の提供



進め方

1

貴社のセキュリティリスクと要件を明確にします。

総務省によって策定されたセキュリティリスクとその対応方法により貴社にとって重要な対策をチェックします。
運用を円滑に行うために必要な要望と製品機能について確認します。

2

最適な運用手法を実施・導入します。

総務省によって策定されたセキュリティリスクとその対応方法により貴社にとって重要な対策をチェックします。
運用を円滑に行うために必要な要望と製品機能について確認します。

3

製品導入後の効果検証とチューニングを行います。

不要なイベントの整理や、新たな脅威が発生した場合に検知ルールの追加を検討・実施してきます。検知精度を向上させるために、また導入製品を有効活用するために月ごとの改善を実施していきます。

1. 貴社のセキュリティリスクと要件を明確にします。

セキュリティリスクマネージメントの考え方①

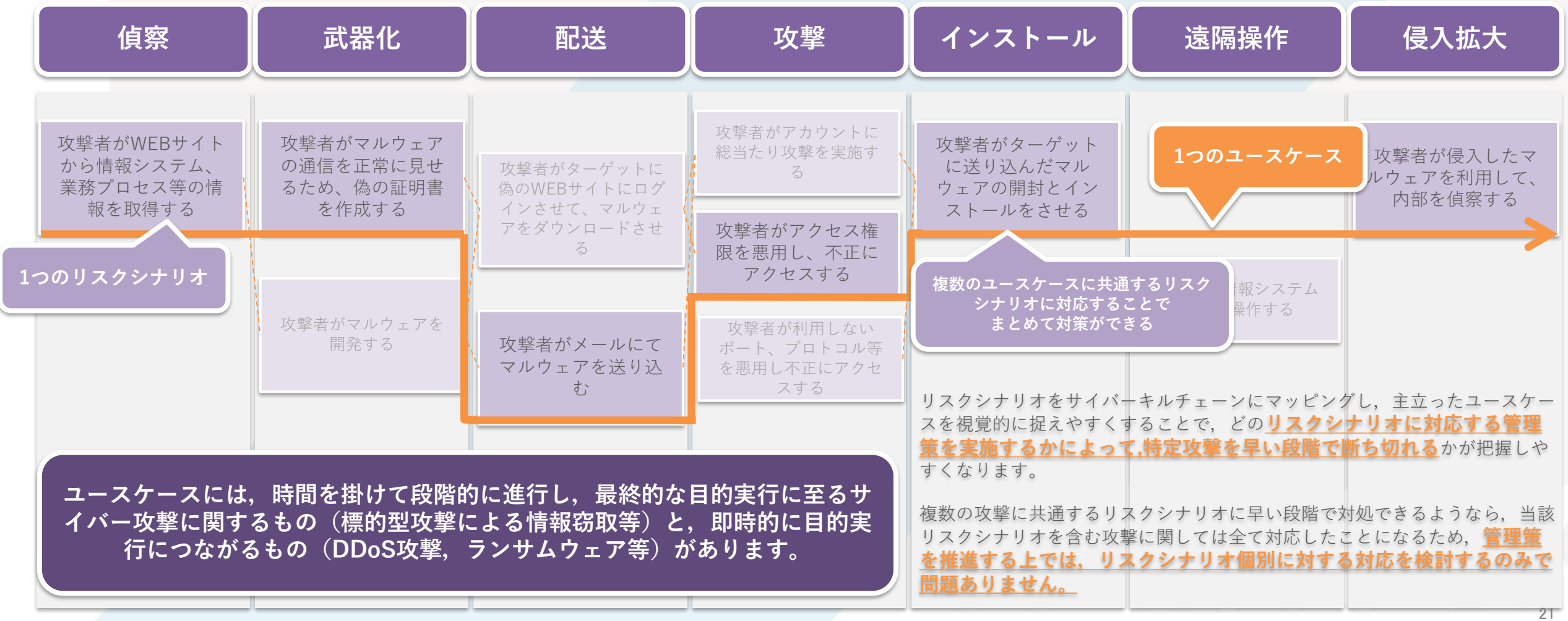
昨今の情報セキュリティにおける「脅威」及び「リスク事象」となる事項について，NIST SP800-30（情報セキュリティリスクアセスメントの実施の手引き），ISO/IEC 27005（情報セキュリティリスクマネジメント）等の複数のグローバルスタンダードのガイドライン等から精査・抽出し，サイバーセキュリティリスクマネジメントに関する「リスクシナリオ」を導出します。

リスクシナリオは，サイバー攻撃の工程を抽象的に切り出したものであり，サイバーキルチェーンの各段階にマッピングします。

1. 貴社のセキュリティリスクと要件を明確にします。

セキュリティリスクマネージメントの考え方②

サイバー攻撃はリスクシナリオの組合せによって構成されます。



ユースケースには，時間を掛けて段階的に進行し，最終的な目的実行に至るサイバー攻撃に関するもの（標的型攻撃による情報窃取等）と，即時的に目的実行につながるもの（DDoS攻撃，ランサムウェア等）があります。

リスクシナリオをサイバーキルチェーンにマッピングし，主立ったユースケースを視覚的に捉えやすくすることで，どの**リスクシナリオに対応する管理策を実施するかによって,特定攻撃を早い段階で断ち切れる**かが把握しやすくなります。

複数の攻撃に共通するリスクシナリオに早い段階で対処できるようなら，当該リスクシナリオを含む攻撃に関しては全て対応したことになるため，**管理策を推進する上では，リスクシナリオ個別に対する対応を検討するのみで問題ありません。**

1. 貴社のセキュリティリスクと要件を明確にします。

リスクシナリオの優先順位づけ

NIST SP800-30のリスクアセスメント手法を参考に，**リスクシナリオの脅威のレベルを評価する**ことで，優先的に対応すべきリスクシナリオを定義します。次ページに参考資料を掲載します。

脅威レベル評価結果例

		a1	a2	A	b1	b2	B		A×B
脅威/脆弱性分類	リスクシナリオ	発生頻度	発現可能性	発現度	影響範囲	復旧難易度	影響度	～	脅威のレベル
侵入拡大	攻撃者はマルウェアに感染した端末を利用して、不正アクセスや攻撃拡大をする	中間	高い	中間	中間	中間	中間	～	中間
侵入拡大	攻撃者は無線アクセスポイントを設置する	低い	中間	低い	低い	低い	非常に低い	～	非常に低い
目的実行	攻撃者は機密情報を取得し、外部に漏洩させる	中間	非常に高い	高い	中間	中間	低い	～	低い
目的実行	攻撃者は情報システム機能を低下させ、サービス妨害する	中間	非常に高い	高い	高い	非常に高い	非常に高い	～	非常に高い

NIST SP800-30 リスク評価 判断基準

定性的な値	説明(NIST原文)	プロジェクトごとの説明
非常に高い	非常に高いリスクとは、その脅威事象が組織の業務、組織の資産、個人……	脅威事象が発生し負の影響をもたらす可能性が非常に高く、負の影響が発生した場合には、膨大な情報資産に影響が及ぶ可能性がある
高い	高いリスクとは、その脅威事象が組織の業務、組織の資産、個人……	脅威事象が発生し負の影響をもたらす可能性が高く、負の影響が発生した場合には、膨大な情報資産に影響が及ぶ可能性がある
中間	中間のリスクとは、その脅威事象が組織の業務、組織の資産、個人……	脅威事象が発生し負の影響をもたらす可能性がある程度あり、負の影響が発生した場合には、広範な情報資産に影響が及ぶ可能性がある
低い	低いリスクとは、その脅威事象が組織の業務、組織の資産、個人……	脅威事象が発生し負の影響をもたらす可能性が低いが、負の影響が発生した場合には、多数の情報資産に影響が及ぶ可能性がある
非常に低い	非常に低いリスクとは、その脅威事象が組織の業務、組織の資産、個人……	脅威事象が発生し負の影響をもたらす可能性が非常に低いが、負の影響が発生した場合には、複数の情報資産に影響が及ぶ可能性がある

参考1）SIEMによる相関分析で予測するリスク例

※灰色箇所は今回のご要望範囲対象外と考えますが、
対象範囲を拡大して監視は可能なものもあります。

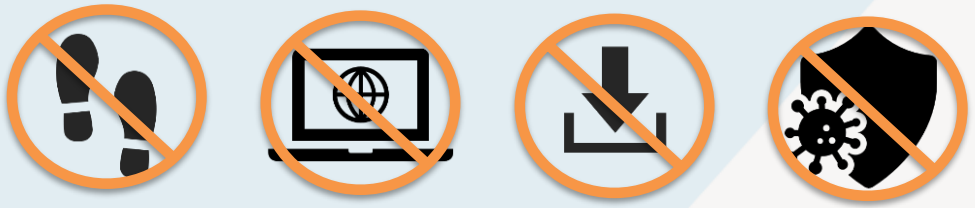
外部攻撃

情報漏洩

サイバー・キル・チェーンカテゴリ	リスクシナリオ
偵察	攻撃者はWebサイトをあさることで、情報システム、業務プロセス、ユーザまたは職員、外部との関係についての情報を取得する。
偵察	攻撃者はネットワーク上に存在するホストを検出するため、コマンド等を無造作に送り、その応答からホストの有無や状況、攻撃対象を特定する。
偵察	攻撃者は情報システムと社外との通信を盗聴する。
武器化	攻撃者はマルウェアの通信を正常にみせかけるため、偽の証明書を作成する。
武器化	攻撃者はアクセス者をマルウェアに感染させるため、偽のWebサイトを作成する。
武器化	攻撃者はマルウェアを開発する。
武器化	攻撃者はアクセスした職員から機密情報を取得するため、フィッシングサイトを作成する。
武器化	攻撃者は攻撃手法を検討し用意する。
武器化	攻撃者はフリーソフトウェアや市販のIT製品にマルウェアを埋め込む。
配送	攻撃者は偽のWebサイトに職員をアクセスさせ、マルウェアをダウンロードさせる。
配送	攻撃者はメールでマルウェアを送り込む。
配送	攻撃者はBYOD端末を狙いマルウェアを送り込む。
攻撃	攻撃者はアカウントに対し総当り攻撃を実施する。
攻撃	攻撃者はリモートアクセスを悪用し情報システムに不正アクセスする。
攻撃	攻撃者はアクセス権限を悪用し不正アクセスする。
攻撃	攻撃者は利用しないポート、プロトコル、サービスを悪用し不正アクセスする。
攻撃	攻撃者は脆弱性を悪用し情報システムに不正アクセスする。
攻撃	攻撃者は無線LAN通信を妨害する。
攻撃	攻撃者はソーシャルエンジニアリングを実施し、職員から機密情報を取得する。
攻撃	攻撃者は公開Webサーバに対しDoS/DDoS攻撃を実施する。
インストール	攻撃者は送り込まれたマルウェアを開かせ、マルウェアをインストールさせる。
インストール	攻撃者は盗聴ソフトウェアをインストールする。
インストール	攻撃者はシステム上に罠をしかけるとともに、ユーザの操作により不正プログラムを実行させる。
遠隔操作	攻撃者は侵入したマルウェアを利用して内部を偵察する。
遠隔操作	攻撃者は外部のC&Cサーバと通信させ新たなマルウェアを送り込む。
遠隔操作	攻撃者は情報システムを遠隔操作する。
遠隔操作	攻撃者は端末を遠隔操作する。
侵入拡大	攻撃者はマルウェアに感染した情報システムや端末を利用して、他の情報システムや端末に不正アクセスし、攻撃を拡大する。
侵入拡大	攻撃者は無線アクセスポイントを設置する。
目的実行	攻撃者はクラウド環境内のデータを改ざん・削除する。または、情報を取得する。
目的実行	攻撃者は機密情報を取得し、外部に漏えいさせる。
目的実行	攻撃者は情報システムの機能を低下させ、サービスを妨害する。
目的実行	攻撃者はWebサイト内の情報を改ざん・破壊する。
目的実行	攻撃者は情報システム内の情報を改ざん・破壊する。
目的実行	攻撃者は情報システムに使用されるソフトウェアを改ざん・破壊する。
目的実行	攻撃者はサイバー物理攻撃により暖房や空調の設定を変更する。

注意点）検知できないイベント

- 対象ログソースに痕跡の無いアクセスの検知



- サイバーキルチェーンの「武器化」工程となる、偽の証明書作成、偽のWebサイト作成などお客様先へのアクセスがない活動
- イベントログの取得が困難な対象機器（BYOD端末等）
- 公開WebサイトへのDdos攻撃については、検知可能だがDdos攻撃対策製品と違って検知、対策が遅くなる。Cloud型WAFのDdos対策機能や、キャリアによるDdos対策のように保護対象システムの前面での対策を行う必要がある。

具体的な運用開始のためのSIEMルールデザイン例

インターネット・ゲートウェイ

Proxy

Firewall

管理

Azure Active Directory

デバイス

Intune

Defender ATP

お客様
セキュリティ担当者

ログの集約

イベントログのチェック項目

【外部からの情報】
◆送信元確認
◆レスポンスコードチェック
◆攻撃の種別
◆内部からの通信

【情報の紐づけ】
◆ユーザー情報連携
◆端末、デバイス情報連携

【情報漏洩につながるログ】
◆マルウェア感染端末
◆マルウェア添付ファイル

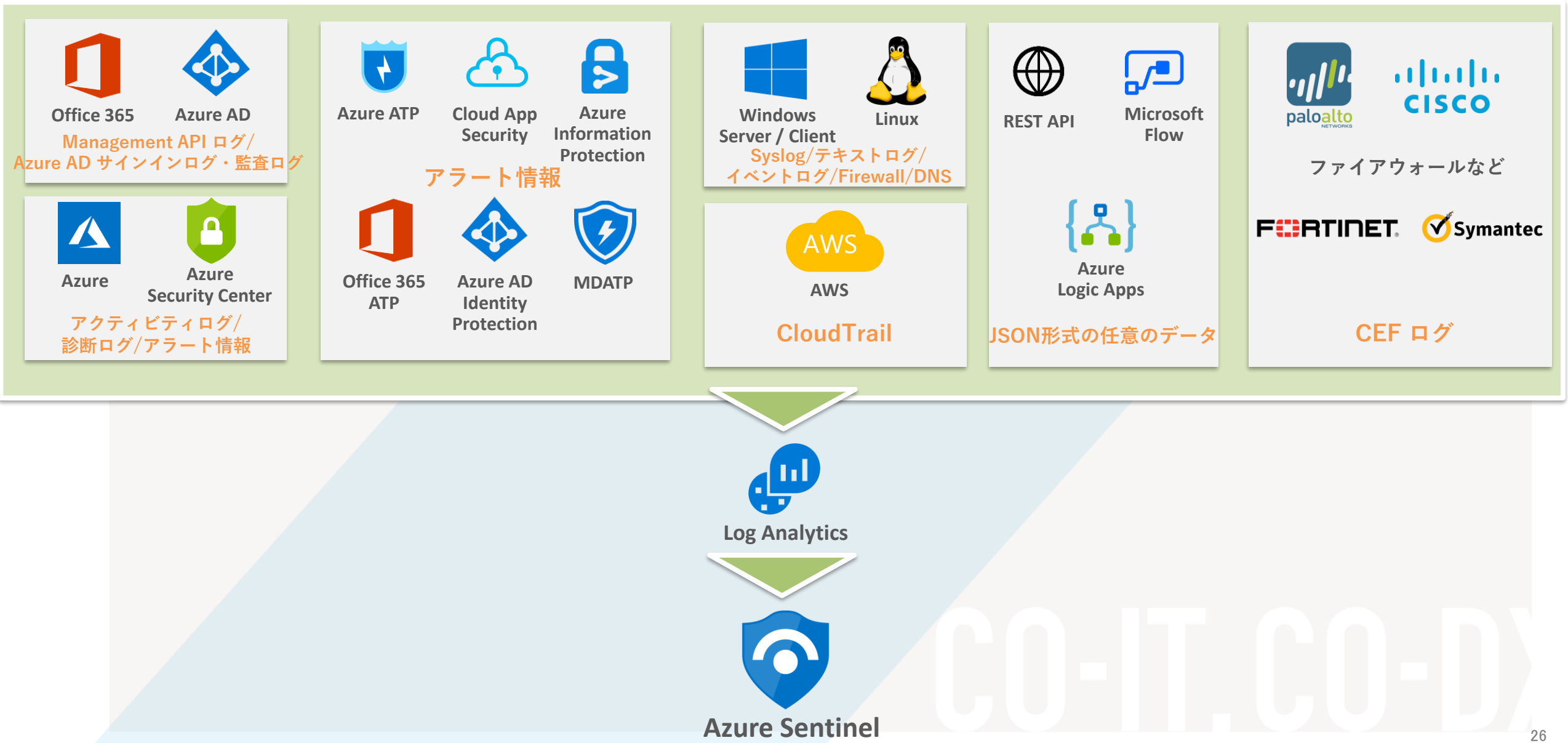
【情報漏洩につながるログ】
◆外付けストレージ及びインターネットストレージ使用有無
◆印刷履歴

作成シナリオ/ルール

外部攻撃の成否
ルール1
ルール2
ルール3

情報漏洩シナリオ
ルール4
ルール5
ルール6

Azure Sentinel によるログ収集対象



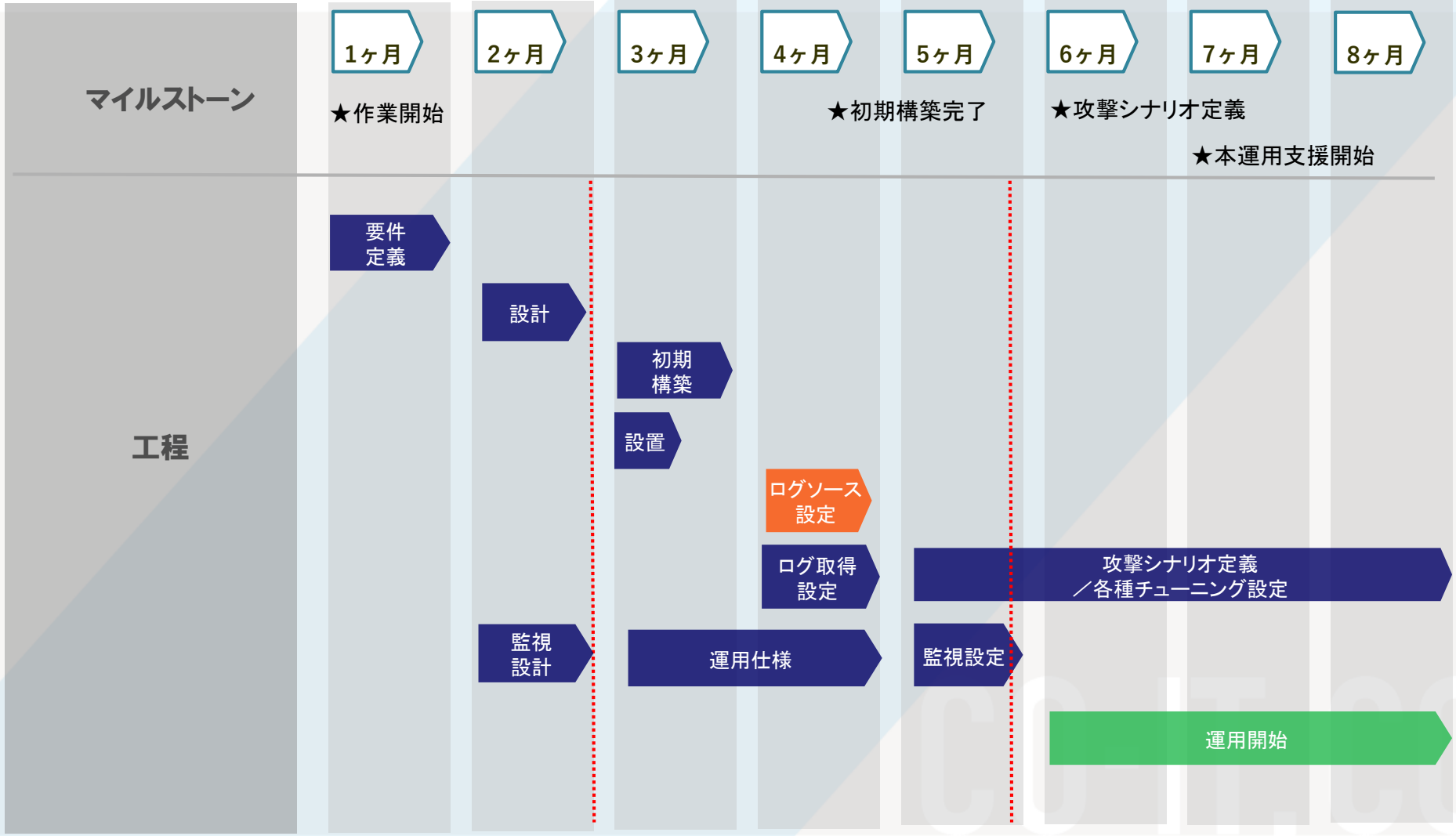
2. 最適な運用手法を実施・導入します。

進め方

1か月	1か月	3か月	
要件定義	設計	導入 運用準備	運用
サイバーセキュリティ対策としての要求仕様をまとめ、必要なリスクシナリオと対象ログソースを明確化します。また運用上必要な要件についてレポート提出いたします。 4回程度の打ち合わせを予定します。	リスクシナリオを実現するためのルール設計、必要サービスの導入設計、SOC対応するための運用設計を行います。	**■導入** プロジェクト計画書に基づき導入を進めます。 お客様には各工程での承認、及びネットワーク通信関連の許可、ログ取得対象製品のログ転送先設定を実施いただく予定です。 **■運用準備** 連絡体制、緊急連絡情報、インシデントレベル毎対応方法、運用タスクについて、手順と情報をまとめ運用仕様書を作成します。 また運用リハーサルを実施してSOCとの連絡が運用リリースから滞りがないようにします。	緊急インシデントに対しては2次分析まで実施し、対応方法をお知らせします。 初回のみルール稼働状況を確認し、チューニングに関する変更必要項目を月次報告書にて報告します。

2. 最適な運用手法を実施・導入します。

導入スケジュール



無償PoCの進め方

（準備期間～報告：1.5か月～2か月）

	1週間	1週間～2週間	2週間	1週間後
	ヒヤリング	事前準備	監視	分析レポート
内容	ヒヤリングシートに必要事項を記入	検証担当者がSentinelの設定をお客様環境に準備	即対応が必要、もしくは確認が必要な場合は、PSCがSOCとして連絡。	統計、課題、今後のアクションをレポート化して報告会を実施
実施項目	ターゲット決め シナリオ決め	アラートチューニング Azure設定	アラート通知/確認 QA対応	レポート提出 報告会
留意事項	対象はMS製品とサードパーティー製品2つまで DefenderATPは別途有償対応	Azure利用環境があることを前提。 ない場合は別途有償対応	定型的な暫定監視を提示 ・運用はオペレータ対応 ・QAは担当SE対応	延長要望ある場合は有償にて対応

3. 製品導入後の効果検証とチューニングを行います。

アイズオンモニタリングサービス　対応内容例

リスクカテゴリー	アクション	内容
コマンド実行（遠隔操作_目的実行）	検知	攻撃に使用されるコマンド・ツールの実行を検知
	アラート情報の収集	事象日時、該当端末IPアドレス、コマンド実行内容を確認
	報告	1次分析の調査結果を顧客へ一次報告。 該当端末が保守管理端末以外においての検知の場合（Critical） 該当端末が保守管理端末においての検知の場合(Medium) ※いずれの場合もユーザー操作によるものではないか確認頂くよう連絡する。
	各キルチェーンフェーズでのアラート検知がないか確認	セキュリティ監視装置から該当端末IPアドレスを基に別のアラートが発生していないかを確認。
	ログ情報の収集と調査☒害範囲の特定（通信成功可否）	FireWallログで該当PC(SourceIP)から外部への通信成否を確認。 ※ただし，別のアラートでC&C通信先が特定できている場合
	ログ情報の収集と調査☒害範囲の特定（通信確認）	Proxyログで該当PC(SourceIP)から外部へのPOSTの有無を確認。 ※ただし，別のアラートでC&C通信先が特定できている場合
レピュテーション検知_	検知	前科のある送信元のアクセスを検知
	アラート情報の収集	アラート内容、事象日時、通信元IPアドレス、通信先IPアドレスを確認する。
	報告	1次分析の調査結果を顧客へ一次報告(Medium)。
	宛先IPの特定☒Whois調査）	WHOIS調査でアクセス先のサイトのIPアドレスを特定する。
	影響調査（レピュテーション確認）	誤検知ではないか第三者の評価サイト(VirusTotal)で確認（検知の正確性の確認）、X-forceでのレピュテーション確認。
	ログ情報の収集と調査☒害範囲の特定（通信成功可否）	プロキシログで該当宛先ドメインに対して通信が成功しているかを確認。
	ログ情報の収集と調査☒害範囲の特定（通信成功可否）	通信元IPと宛先IP（通信先IP）と送信ポートを元にFireWallログで通信状況確認。
総当たり攻撃検知_	アラート情報の収集☒概要把握	アラート内容、事象日時、送信元IPアドレス、宛先IPアドレス、宛先ポートを確認する
	報告☒アリング依頼	1次分析の調査結果を顧客へ一次報告(High) 側に設定不備,或いは例外で許可していないかの確認を実施するよう依頼
	各キルチェーンフェーズでのアラート検知がないか確認	セキュリティ監視装置から該当端末IPアドレスを基に別のアラートが発生していないかを確認
	攻撃元IP調査	・送信元IP（攻撃元IP）をX-forceでのレピュテーション確認 、WhoisでのIP調査
	ログ情報の収集と調査☒害範囲の特定	・プロキシログより宛先IPアドレスが複数の内部IPに対して通信を実施していないか調査（内部偵察、侵入拡大の調査）
	ログ情報の収集と調査☒害範囲の特定	・プロキシログより宛先IPアドレスが外部へのPOST通信をしていないかの調査

3. 製品導入後の効果検証とチューニングを行います。

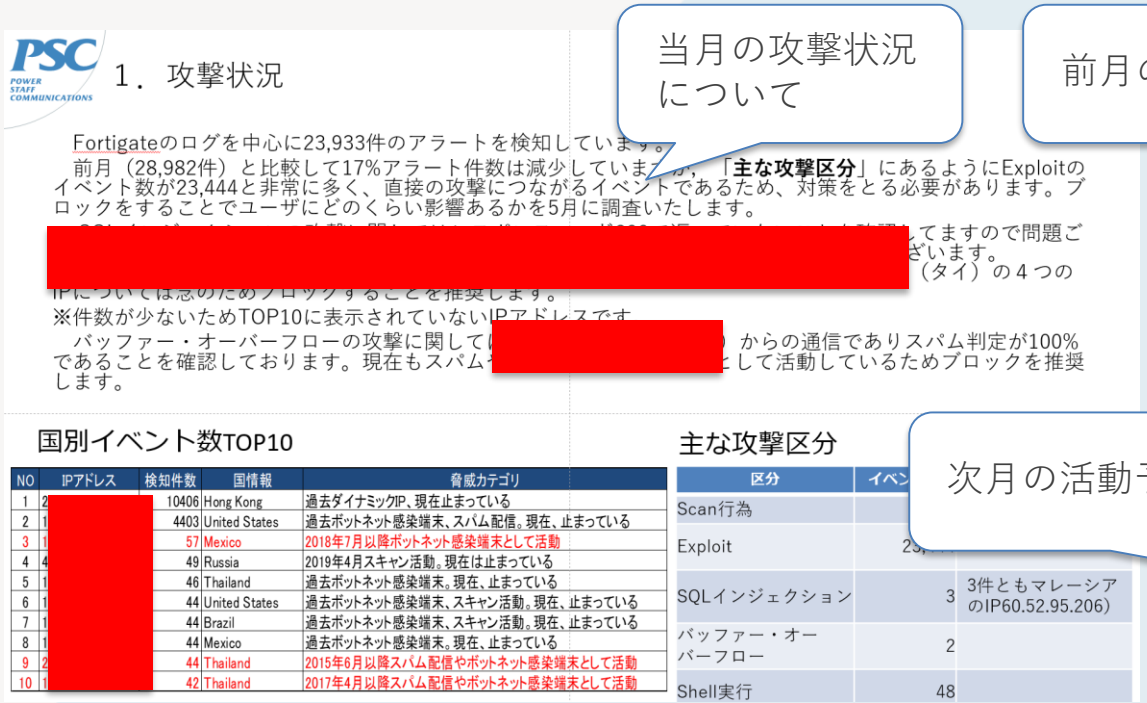
アイズオンモニタリングサービス　対応内容例

ビジネスセキュリティ	ログ情報の収集と調査☒害範囲の特定（通信確認）	Proxyログより不審な通信（マルウェアによる通信が発生していないか、定期的に通信が発生していないか、規則的な特徴がないか）を確認。
	情報漏洩観点調査	プロキシログからPOST通信がないかの確認
	影響調査（レピュテーション確認）	過検知ではないか第三者の評価サイト(VirusTotal)で確認（検知の正確性の確認）、X-forceでのレピュテーション確認。
不正アクセス（認証攻撃）	アラート情報の収集☒概要把握	アラート内容、事象日時、送信元IPアドレス、宛先IPアドレス、ユーザIDを確認する
	報告	1次分析の調査結果を以下のように顧客へ一次報告 K1-1での検知（Medium） K5-1での検知（High） ※報告時に作業によるログイン施行ではないか確認頂く 第一報告では送信元IPアドレスが外部IPアドレス或いは内部IPアドレスかの連絡実施
	各キルチェーンフェーズでのアラー[illegible]知がないか確認(K1-1	セキュリティ監視装置から該当端末IPアドレスを基に別のアラートが発生していないかを確認 ・特に総当たり攻撃（K4-1）が発生していないかを確認 送信元IPが内部IPアドレスの場合は侵入拡大が発生していないかを確認
	攻撃元IP調査(K1-1、K5-1共通)	・送[illegible]元IPが外部IPであった場合はX-forceでのレピュテーション確認 、Whois[illegible]のIP調査
	ログ情報の収集と調査(K5-1の場合)☒害範囲の特定	DMZか[illegible]内部に向かおうとしている通信が発生していないか
侵入拡大検知_	アラート情報の収集☒概要把握	アラート内容、事象日時、送信元IPアドレス、宛先IPアドレス、を確認する DMZ機器がの管理端末（メール中継セキュリティ対策装置，外部DNS）であるかを確認
	報告	1次分析の調査結果を顧客へ一次報告(Medium) （送信元IPが[illegible]の機器かどうかを報告する）
	各キルチェーンフェーズでのアラート検知がないか	セキュリティ監視[illegible]当端末IPアドレスを基に別のアラートが発生していないかを確認 ※侵入拡大フェーズのため前段階のフェーズでの検知がないか再確認
	宛先IP調査(宛先IPがインターネットの場合)☒	・宛先IPが外部IPであった場合はX-forceでのレピュテーション確認 、WhoisでのIP調査
	ブラックリスト登録確認	宛先IPアドレスがGSOCブラックリスト，貴省独自IPブラックリストに登録されていないかを確認する。
	ログ情報の収集と調査☒害範囲の特定	・踏み台にされていないかの調査 FWのログからDNSとメールセキュリティをキーとして不整合なフラグパケットのログが出ていないかを確認し、そのフラグの出方が短時間に複数件、同一の宛先に対して発生していないかを確認 （一般国民に対してDOS攻撃をしていないか等） パターン１の確認

3. 製品導入後の効果検証とチューニングを行います。

月次レポートについて

下記分析概況から、活動報告、チューニング提案、課題管理を実施します。



PSC POWER STAFF COMMUNICATIONS

1．攻撃状況

Fortigateのログを中心に23,933件のアラートを検知しています。
前月（28,982件）と比較して17%アラート件数は減少していますが、「**主な攻撃区分**」にあるようにExploitのイベント数が23,444と非常に多く、直接の攻撃につながるイベントであるため、対策をとる必要があります。ブロックをすることでユーザにどのくらい影響あるかを5月に調査いたします。
[redacted]してますので問題ございます。
[redacted]（タイ）の４つのIPについては急のためブロックすることを推奨します。
※件数が少ないためTOP10に表示されていないIPアドレスです
バッファー・オーバーフローの攻撃に関して[redacted]からの通信でありスパム判定が100%であることを確認しております。現在もスパム[redacted]として活動しているためブロックを推奨します。

国別イベント数TOP10

NO	IPアドレス	検知件数	国情報	脅威カテゴリ
1	[redacted]	10406	Hong Kong	過去ダイナミックIP、現在止まっている
2		4403	United States	過去ボットネット感染端末、スパム配信。現在、止まっている
3		57	Mexico	2018年7月以降ボットネット感染端末として活動
4		49	Russia	2019年4月スキャン活動。現在は止まっている
5		46	Thailand	過去ボットネット感染端末。現在、止まっている
6		44	United States	過去ボットネット感染端末、スキャン活動。現在、止まっている
7		44	Brazil	過去ボットネット感染端末、スキャン活動。現在、止まっている
8		44	Mexico	過去ボットネット感染端末。現在、止まっている
9		44	Thailand	2015年6月以降スパム配信やボットネット感染端末として活動
10		42	Thailand	2017年4月以降スパム配信やボットネット感染端末として活動

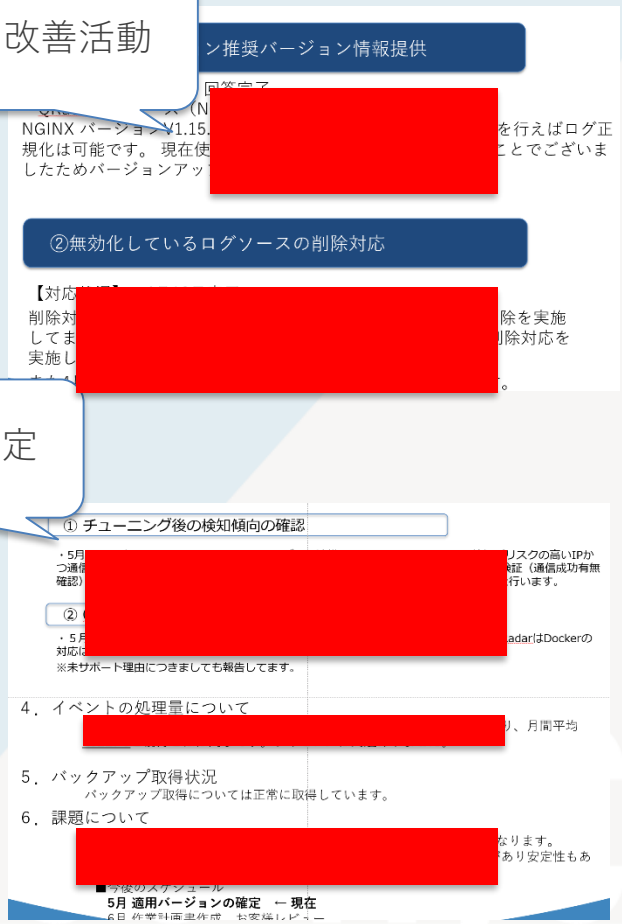
主な攻撃区分

区分	イベン	
Scan行為		
Exploit	23,	
SQLインジェクション	3	3件ともマレーシアのIP60.52.95.206）
バッファー・オーバーフロー	2	
Shell実行	48	

当月の攻撃状況について

前月の改善活動

次月の活動予定



ン推奨バージョン情報提供

[redacted]

②無効化しているログソースの削除対応

[redacted]

① チューニング後の検知傾向の確認

[redacted]

4．イベントの処理量について

[redacted]

5．バックアップ取得状況
バックアップ取得については正常に取得しています。

6．課題について

[redacted]

■今後のスケジュール
5月 適用バージョンの確定 ← 現在

上記のほか、ライセンス状況、対象製品の脆弱性情報、
通常運用報告を実施

料金

導入作業見積

項目	料金	備考
アセスメント	120万円～	情報セキュリティ監査対応、Poc
構築作業	260万円～	設計、構築、ルール設計、監視設計
運用準備	60万円～160万円	SOC接続環境構築、運用仕様書作成

月額見積（単価）

項目	料金	備考
基本監視サービス	30万円	※次ページ参照
調査・分析サービス	40万円～	40時間/月で対応。超過については10時間単位。

基本サービス内容

NO	費用項目	説明
1	**セキュリティイベント監視/通知**	24時間365日対応。対象機器で発生したセキュリティイベントを監視する。攻撃検知時の条件付け連絡対応を行う。
2	**インシデント発生時設定変更作業の実施**	対象製品においてセキュリティインシデントが発生した場合に設定変更を実施する。
3	**セキュリティ月次レポート提供**	当該月稼動に関する調査分析を交えたセキュリティ運用状況を報告レポート化し、報告する。
4	**セキュリティ月次報告会の実施**	セキュリティ月次レポートおよび課題に関する対応状況について、月次定例会にて対面報告する。
5	**死活監視**	対象製品へPSC SOCからICMPへの応答を監視する。
6	**通常時ルール、ポリシー設定変更作業の実施**	対象製品のルール、ポリシー設定変更作業を実施する。 月10回を限度とする
7	**お客様依頼に基づくシグネチャーの修正/適用**	お客様依頼に基づくシグネチャ修正/適用を実施する。
8	**セキュリティログ保管**	月次報告書として対象機器のログを12か月間保管する。
9	**【OPTION]】送信元遮断対応**	シグネチャプロックではなく、送信元に対するIP遮断対応。お客様承認の元実施する。※シグネチャブロックは項番６にて対応。
10	**【OPTION]】セキュリティ監視に関する技術QA対応。アイズオンモニタリング**	セキュリティ監視に関するチューニング提案、技術QA対応を行う。

03

PSC SECURITYサービス

SOC（セキュリティオペレーションセンター）

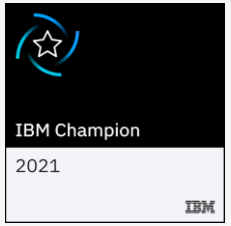
Security DX 実績

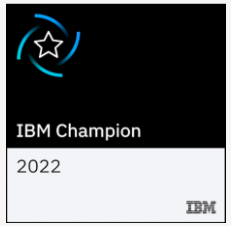
1. 自社保有施設

PSC SOC

世界水準のSecurity対策、BCP対策完備のデータセンター（某都内）

2. 日本初セキュリティ部門





IBM Champion（3年連続）

3.脆弱性診断

社数**432**社　未然防止**11,400**リスク

IBM社と共に多くのSecurity DXをプロデュース

SMC
Security Management Center

セキュリティサービス体制

経験豊富な技術者と蓄積されたナレッジ
ネット環境に潜むあらゆる危険を防御

オペレーションチーム

■役割

•24時間365日セキュリティ監視、運用
•ログアラート検出時15分以内に連絡

■業務

•ログ監視
•Firewall運用サービス
•死活監視サービス
•脆弱性診断自動スキャンサービス
•セキュリティパッチ定期通知サービス
•改ざん検知運用サービス
•障害切り分け

ＳＥ/アナリストチーム

■役割

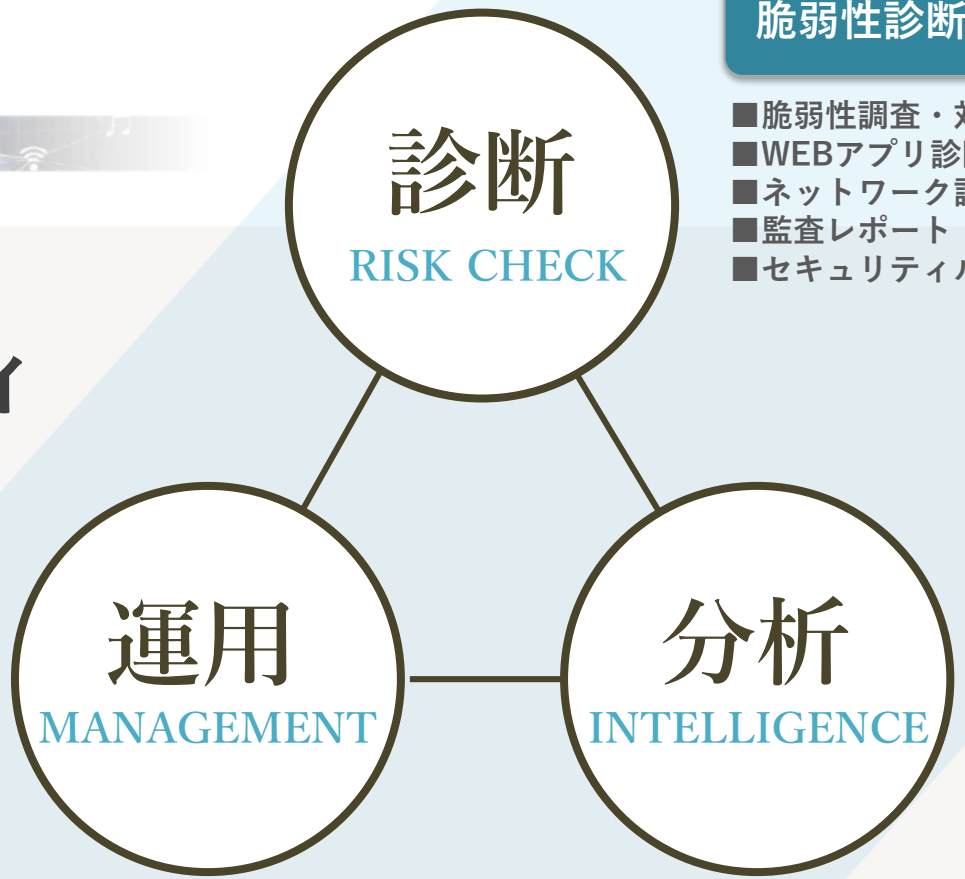
•お客様毎にコンサルティング、SI、分析/報告を対応
•Security Management Centerの品質向上、体制強化
•webサイトセキュリティ強化コンサルティング

■業務

•ログ分析
•web/NW脆弱性診断レポート
•セキュリティ機器導入
•顧客別サポート(日次/月次)
•障害対応

PSCのセキュリティソリューション

ネット環境に潜むあらゆる危険を防御



脆弱性診断

■脆弱性調査・対応
■WEBアプリ診断
■ネットワーク診断
■監査レポート
■セキュリティルール策定

ログ分析

調査/解決

■ログ統合・相関分析
■検知ルール作成
■ネットワーク分離
■ネットワーク可視化

ログ調査

防御の施策

■月次レポート/報告会
■セキュリティ監視
■脆弱性情報提供
■シグネチャチューニング

お客様の状況やステイタスそしてニーズに合わせて、
3つのサービスをトータルでセットアップ。
今の対策から未来の対策まで一気通貫でコンサルティング提供します。

沿　革

プロから頼られる技術力

PSCのセキュリティソリューション

～2013
・Web脆弱性診断

2014
・ネットワークセキュリティ
・IBM/MSS（不正侵入検知）
・ファイヤーウォールログ分析

2015
・改ざん検知/防御
・WAF運用サービス
・サンドボックス（FireEye）

2016
・ログ統合＆相関分析サービス
・TrendMicro/F5Networks MSP

2017
・セキュリティ対策チーム支援サービス（オンサイト）
・クラウドセキュリティサービス

2018
・エンドポイントセキュリティ
・AWS WAF

2019
・データベースセキュリティ

2020
・Microsoft Sentinel
・Microsoft Defender ATP

2021
・Microsoft E5 Security

2022
・西日本SOC開設「西日本マルチサポートセンター」

成功事例

自社施設で24時間365日
緊急対策から恒久対策まで総合提案。

月間延95社　月間延161PJ

導入～運用まで
ワンストップ

設備

セキュリティ監視ルーム

- 24 時間 365 日運用を行う監視ルーム
- カード認証、指紋認証等マルチ認証が必要な入館作業
- 金融機関にフォーカスした世界水準の設備
- 冗長化された電源、空調
- 3段階のセンサー、充実の消火設備
- 人口用水路による洪水対策
- 震度6弱に耐えうる、堅牢な建物構造
- 高速な光ファイバーネットワークに直結した快適なブロードバンド環境
- 大手町から15分以内の好立地

認証登録・資格

- プライバシーマーク
- 品質マネージメントシステム認証
- 情報セキュリティマネージメントシステム認証
- 日本カード情報セキュリティ協議会 会員
- 日本セキュリティ監査協会 セキュリティ監視運用サービス部門認定
  ＳＳＳマーク（サービス登録番号：019-0019-40）

10820219(06)

登録番号：019-0019-40

日本カード情報セキュリティ協議会
安全なカード社会の実現を目指して

対応拠点

東京と大阪に拠点を置き、東西でサービスを提供できる体制をとっています。
また、PSC琉球（PSC子会社）が沖縄でDR 拠点として、万一の際のお客様窓口となります。

幅広いお客様へ迅速に対応する、
東西に配した
セキュリティサービス体制。

セキュリティサービス@東京

- コンサルティング
- SOC業務
- 分析、調査

セキュリティサービス@大阪

- ユーザサポート
- SOC業務
- 分析、調査

ピーエスシー琉球

- お客様窓口

SOC提供サービス

PSC マネージドセキュリティサービス

SOC セキュリティオペレーションセンター業務

検知 → 切り分け → 報告 → 遮断・隔離

- 切り分け：・重要度判定 ・過検知/誤検知の切り分け
- 報告：・一次報告
- 遮断・隔離：・端末隔離 ・ユーザ利用停止依頼

PSCインシデントレスポンスサービス

情報システム部門業務

経路調査 → 影響調査 → 最終報告

- 経路調査：・情報漏洩確認

緊急度に応じて、一次報告・二次報告を実施し、推奨対応方法を連絡します。

危険度の把握から対応策の実施までに要する時間を最小限にすることで、被害の最小化をトータルでサポートします。

PSC セキュリティコンサルティング

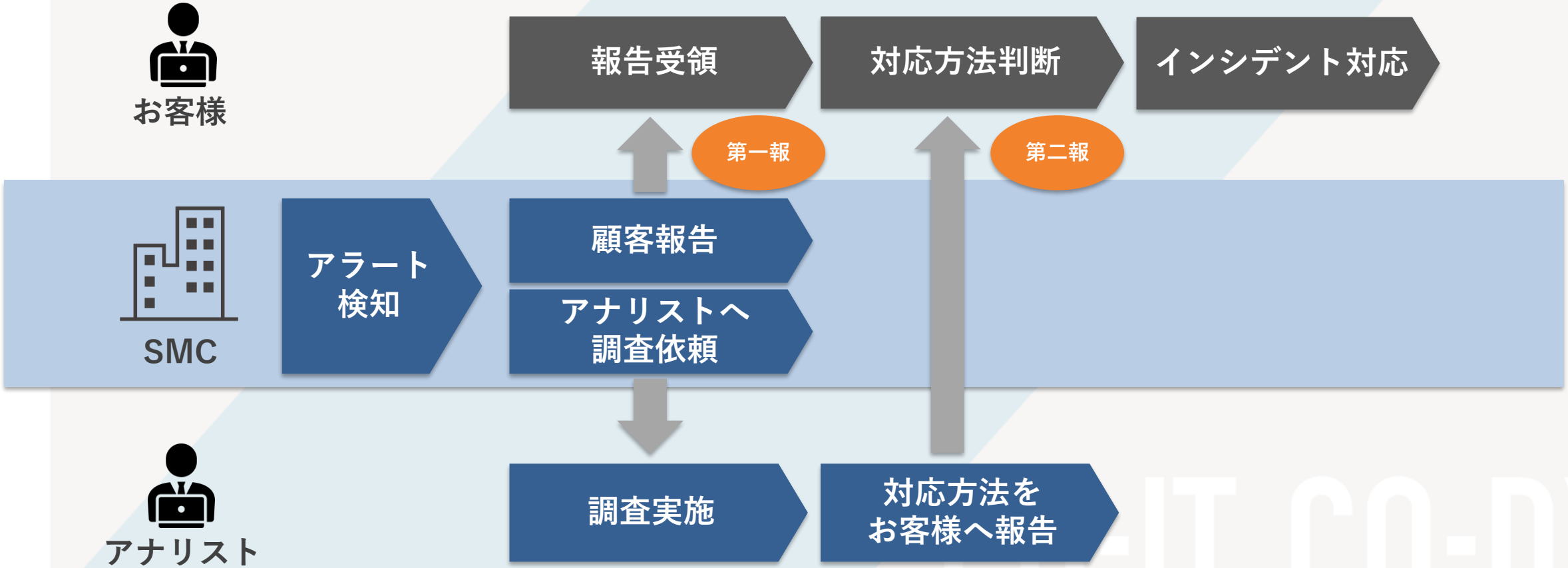
アフターフォロー業務

情報システム暫定対処 → 恒久対処

- 情報システム暫定対処：・マルウェア抽出、調査 ・重要データ復旧 ・端末リプレース ・ユーザーアカウント再発行
- 恒久対処：・社内ルールの見直し ・セキュリティポリシーの更新、改訂 ・全社通知 ・セキュリティ教育

連絡からの作業フロー

検知からの対応については、事前にフローテンプレートを提示し、お客様に合ったフローにカスタマイズしていきます。
カスタマイズしたフローは「運用仕様書」として規定し、その後の運用にて必要に応じて修正していくことが可能です。



脅威度別対応表

脅威度	対　応	対応期間
CRITICAL	検知した場合、第一報として「運用仕様書」の記載に則り、検知概要の報告を行う。 その後、上位SEが調査を実施し、推奨対応等がある場合「運用仕様書」の記載に則り、報告をする。	24時間365日 ※上位SEの調査、 報告対応は営業時間のみ
HIGH		
MEDIUM	検知した場合、第一報として「運用仕様書」の記載に則り、検知概要の報告を行う。 検知結果については月次報告会にてまとめて報告を行う。	24時間365日
LOW	検知した場合、第一報として「運用仕様書」の記載に則り、検知概要の報告を行う。 検知結果については月次報告会にてまとめて報告を行う。	
INFORMATIONAL		

EOF