セキュリティマネージドサービス説明資料

EDRマネージドサービス

Ver1.1

Microsoft Defender for End Point

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

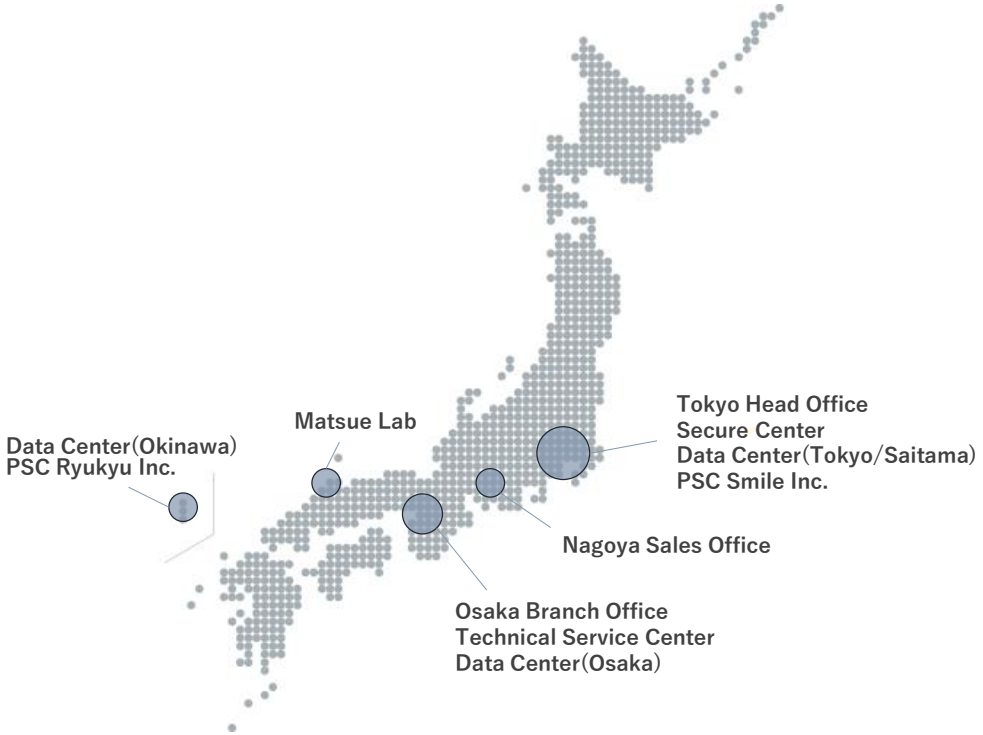
認証登録・資格・認定

・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

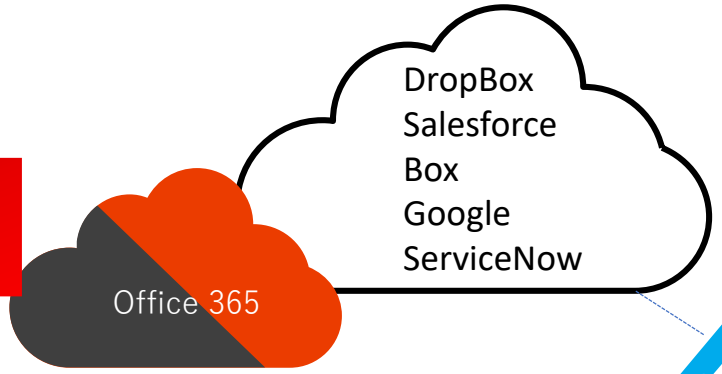
・日本アイ・ビー・エム株式会社　ビジネスパートナー
・日本マイクロソフト株式会社認定ソリューションプロバイダー
・日本ヒューレット・パッカード合同会社
・グーグル合同会社 Google Cloud Partner
・SCSK株式会社
・デル・テクノロジーズ株式会社
・クエスト・ソフトウェア株式会社
・シスコシステムズ合同会社　プレミア認定パートナー
・株式会社エムアンドシーシステム
・Coltテクノロジーサービス株式会社
・ヴイエムウェア株式会社
・株式会社オプテージ

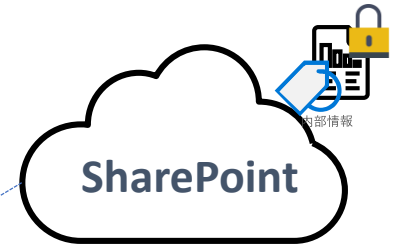
コラボレーション

ビジネスを互いに進化させるパートナーシップ

E5で実現するセキュリティ対策例

場所によらない、ID/デバイスの認証とデータアクセスを常に監視するセキュリティソリューション





悪質な添付ファイル / フィッシングリンク付きのメール

Defender for Office 365

悪質な添付ファイルの振る舞い分析
悪質なフィッシンリングリンクの書き換え

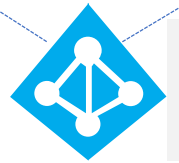
Threat Intelligence

O365 へのテナント攻撃を可視化
メールボックスに対して未読状態のマルウェア添付メールの削除可能

機密情報の漏洩

Azure Information Protection

機密情報の自動ラベリング
および暗号化



Azure Active Directory P2

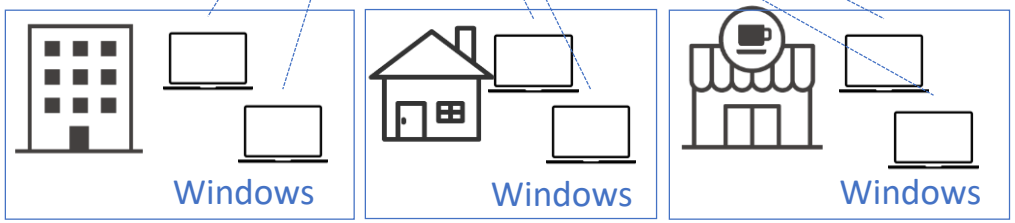
不正なIPからのサインインの検知・対処
異常な場所移動でのサインイン検知・対処

ブルートフォース攻撃
漏洩した資格情報でのログイン

Microsoft Cloud App Security

シャドーITの検出
SaaS内での機密情報の可視化
異常行動検知

SharePoint等からファイルの大量ダウンロード



Intune（M365 E3）
ポリシー違反を可視化
パッチ適用管理

必要なアクセス端末のみアクセス可能にする

Defender for Endpoint
エンドポイントの攻撃の検知・自動調査および自動対処

未知のマルウェア感染
高度なファイルレス攻撃

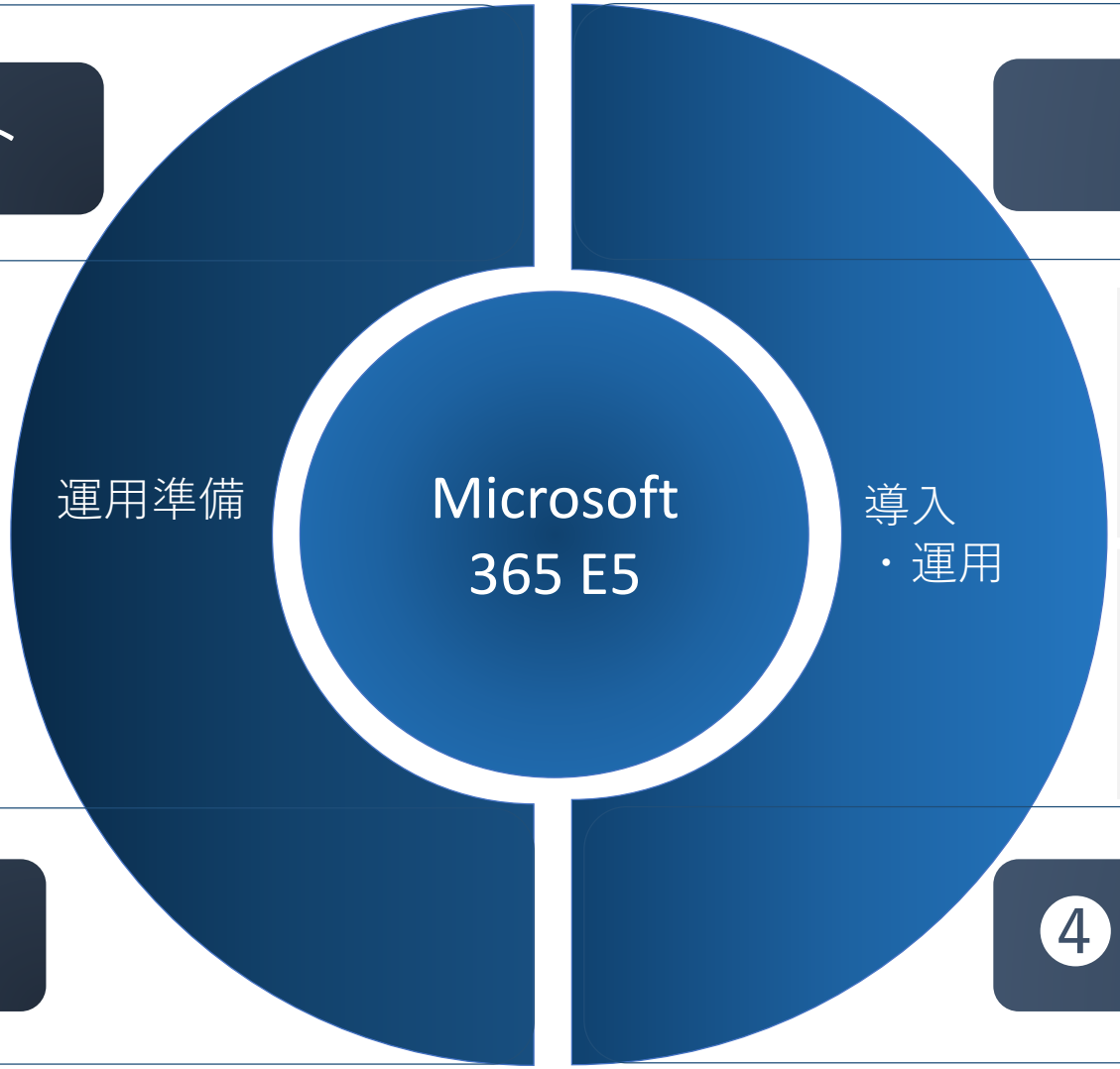
PSCの考えるMicrosoft 365 E5の活用ソリューション

①アセスメント

CIS Controlsのガイドラインに基づいた調査や、企業のセキュリティポリシーに基づいた調査・報告。

②運用デザイン

Azure Sentinelを活用したサードパーティー製品を含めた統合運用プランの策定とWorkShop開催



③導入支援

優先順位とE5製品の必要な連携を意識した導入スケジューリングとFastTrackを活用した導入支援

④マネージドサービス

多岐にわたる製品から相関分析された重要アラートの整理と月次で提案する強化対策

01
EDRマネージドサービス

EDR(Endpoint Detection & Response)機能の重要性

- 情報漏洩の有無は？
- 影響範囲は？
- 攻撃の経路は？
- 誰が、どこから？
- 利用されたマルウェア、手法は？

ー調査内容ー

- ☑ Win Rar/7-zipの痕跡
- ☑ アーカイブファイルの痕跡
- ☑ 侵害されたユーザー
- ☑ 侵害されたシステム
- ☑ タイムライン
- ☑ インテリジェンス情報
- ☑ マルウェア、スクリプト
- ☑ 横展開手法

インシデント対応の運用プロセスモデル

イベント確認・検知

・トリアージ分析
・重要度判定

インシデント分析

・影響範囲の特定
・侵入経路の特定
・情報漏洩の痕跡
・TTP（戦術/技術/手順）の特定

インシデント対応に向けた改善

・ポリシーチューニング
・人員増強

対　処

【短期的な対処】
・マルウェア削除
・データ復旧
・感染端末リプレース
【中・長期的な対処】
・社内ポリシー更新・改正
・ネットワーク再設計

応急処置

・対象システム隔離
・対象ユーザ利用停止

セキュリティ製品から上がるアラートを基に、お客様環境への影響報告、課題の抽出、セキュリティリスクに対する改善レポートを提供し、PDCAを回すことでよりセキュリティを強固にしていく活動を支援しています。

標準サービスの進め方

事前準備：およそ2.5カ月

事前準備

1～2週間 現状確認

■確認内容
・ネットワーク構成、設定
・設定グループ
・セキュリティ要件
・スケジュール
・利用端末情報
・利用機能の確認

クイック導入サービスではヒヤリングシートによる確認のみ実施

1～2週間 設定シート作成

■作業内容
・設定ルールおよびグループをパラメータシートへ落とし込み
・グループ作成とグループ毎ルールの作成
・配布方法の策定

クイック導入サービスではカスタマイズができません

■お客様に対応いただく事項
・既存資料の閲覧許可/提供
・質疑対応
・作成資料の確認/一部記入いただく事項あり

配布支援

2～4週間 PoCおよび導入手順作成

■作業内容
・事前検証および切り替え手順書兼チェックシート作成
・ポリシーチューニング

クイック導入サービスではPoC対象端末は5台まで

2週間 配布作業支援

■作業内容
・スクリプト作成
・配布作業支援
・切り替え後サポート

クイック導入サービスではスクリプト作成等の支援はなく技術QA対応のみ

■お客様に対応いただく事項
・検証端末の選定
・アラート内容に関する確認事項回答
・最終決定ポリシーの確認
・本番導入の決定

条件

・各工程で打ち合わせを１，２回実施します。
・記載された期間は1000台を対象としたときの目安の期間となります。
・作業は基本自社で行い、必要に応じて現地訪問を行います。
・本サービスはユーザ数5,000ユーザまでを対象とします。それを超える場合は個別見積とします。
・既存ネットワーク機器の設定変更については、設定内容に関する支援は実施しますが、お客様にて対応いただきます。

運用準備サービスの進め方

事前準備

4週間

配布期間～モニタリング

■作業内容
・誤検知・過検知アラートの整理
・技術QA対応
・チューニング対応
・SOC接続準備
・障害時の設定変更
・管理対象端末確認

クイック導入サービスにおいても対応必要

■お客様に対応いただく事項
・SOCで判断が困難な誤検知判断についてのご確認
・インシデントが発生した端末のユーザへの連絡
・障害発生時の対応支援
・管理対象端末確認

運用開始

2～4週間

運用仕様の確定

■作業内容
・連絡体制、管理グループ、調査手順の合意など、運用設計及び監視準備
・月次レポートフォーマットの作成

■お客様に対応いただく事項
・運用仕様書、月次レポートフォーマットのご承認

運用サービス

■作業内容
・セキュリティアラート監視
・月次報告
・インシデントへのトリアージ
・ネットワーク遮断等設定変更
・感染端末調査、分析

条件

・各工程で打ち合わせを１，２回実施します。
・記載された期間は1000台を対象としたときの目安の期間となります。
・作業は基本自社で行い、必要に応じて現地訪問を行います。
・本サービスはユーザ数5,000ユーザまでを対象とします。それを超える場合は個別見積とします。
・既存ネットワーク機器の設定変更については、設定内容に関する支援は実施しますが、お客様にて対応いただきます。

初期費用

対象500台以下導入プラン

導入作業支援サービス　Pocサービス　クイック導入サービス

500台以下のお客様を対象とした標準導入プランです。適用されるセキュリティポリシーは選択できません。
当社推奨の固定設定となります。適用グループ数は2個までとなります。運用プランはエントリープランのみ選択できます。
※「導入作業支援サービス」もしくは、「Pocサービス」・「クイック導入サービス」のどちらかを選択できます。

初期費用	標準価格	備考
導入作業支援サービス	600,000円	ポリシー・ルール作成、エージェント配布支援、チューニング作業
運用準備サービス	250,000円	運用仕様書、レポートフォーマット作成

標準導入プラン

501台以上のお客様を対象とした導入プランです。ポリシーのカスタマイズが必要な場合においても本プランにてご提供します。運用は次ページの3つのプランから選択できます。

初期費用	標準価格	備考
導入作業支援サービス	1,200,000円	ポリシー・ルール作成、エージェント配布支援、チューニング作業
運用準備サービス	500,000円	運用仕様書、レポートフォーマット作成

月額料金表

ベンダー様価格

ご提供価格	エントリープラン（１台あたり）	スタンダードプラン（１台あたり）	エンタープライズプラン（１台あたり）	備考
＜簡易パッケージ＞ 500台まで（定額）	240円/月	320円/月	-	単価×台数により 月額料金が決まります。 運用時10%の増減は 金額変更が発生しません。
1000台まで（定額）	150円/月	200円/月	380円/月	
2500台まで（定額）	100円/月	140円/月	280円/月	
5000台まで（定額）	80円/月	130円/月	220円/月	
10000台まで（定額）	70円/月	120円/月	150円/月	
10001台以上（定額）	50円/月	80円/月	120円/月	

実施項目

実施項目およびご提供価格について	エントリープラン（１台あたり）	スタンダードプラン（１台あたり）	エンタープライズプラン（１台あたり）	備考
1 セキュリティイベント常時監視	○	○	○	
2 セキュリティ脅威検知・通知	○	○	○	
3 セキュリティ月次レポート提供	○	○	○	優先度の低いアラート報告も含む
4 脅威トリアージ（重要度/優先順位）	○	○	○	
5 ポリシー設定変更(ブラックリスト登録、ホワイトリスト登録、アラートのDismiss等)	○	○	○	
6 緊急性および重要性が高い脅威の即時通知・対象調査	○	○	○	
7 対象端末のネットワーク隔離対応	○	○	○	
8 セキュリティ月次定例報告会実施	×	○	○	
9 セキュリティインシデント発生時の設定変更実施	×	○	○	
10 標準機能を使ったアプリケーションやプロセス、ファイルの現状調査　※	×	○	○	製品管理コンソール機能にて対応
11 セキュリティ監視に関するアラートおよび技術的なお問い合わせ　※	○	○	○	
12 アプリケーションやプロセス、ファイルの詳細調査、脅威の削除/駆除　※	×	×	○	製品管理コンソール機能にて対応
13 フォレンジックやインシデントレスポンス(IR)、その他復旧対応　※	×	×	○	製品管理コンソール機能にて対応

※10～13は製品により対応できない場合があります。

見積条件

・報告時間の計算起点は1次報告はアラート着信から15分、2次報告は1次報告メール送付後から4時間となります。
・追加契約については前月までのご連絡にて対応いたします。
・監視対象となるデバイス数の変動は3か月単位でチェックを行い報告します。数量が既存契約の範囲を超過している場合は翌月から追加オプションの適用といたします。
・契約締結にあたり、「PSCセキュリティサービス契約書」の取り交わしを行います。

オプションサービス

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」

平日営業時間帯9時-17時／月４０時間までの
PSC アナリスト稼動。

【内　容】
①アラート内容の調査・分析業務、送信元の調査、対象マルウェアやURLの影響調査。
② 各設定変更提言や、ルール設計、追加の提案、システム追加時の各種打ち合わせ参加。

360,000円/月（40時間）

※時間超過の場合、
10時間単位で追加可能です。
※ 90,000円（10時間）

月次レポート

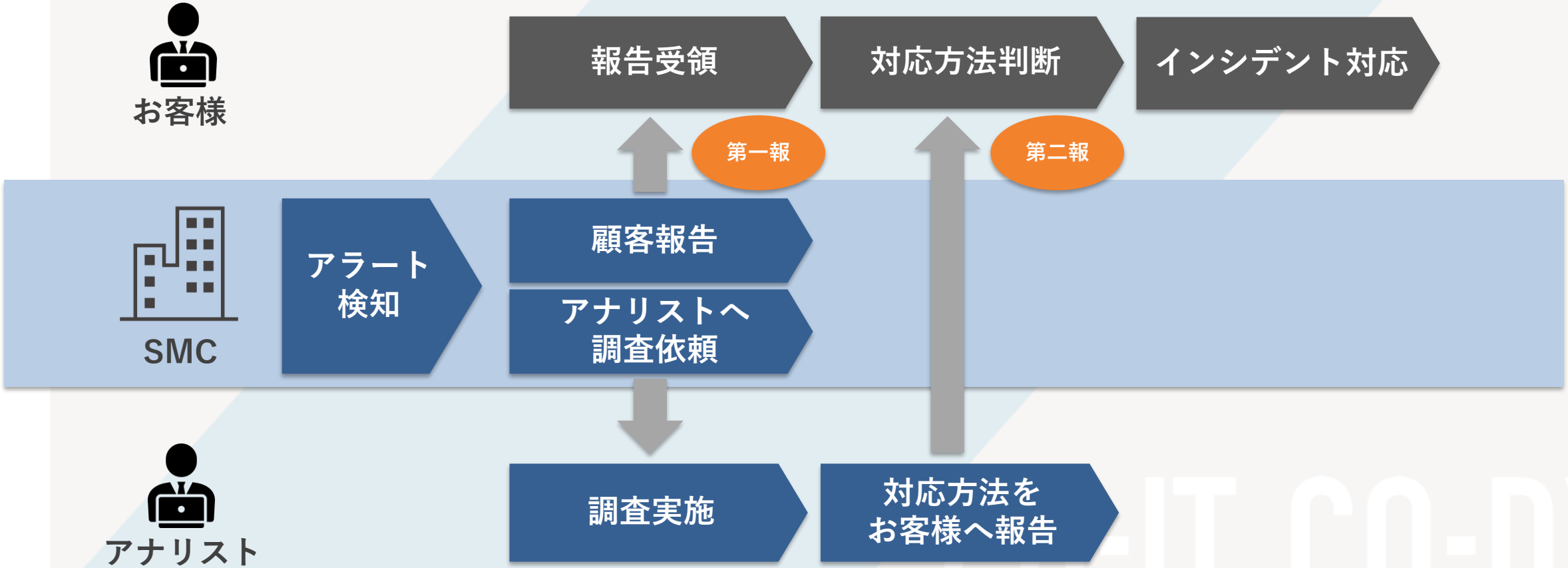
月次統計、攻撃元情報、アラート検知されたURL、添付ファイルの第3者機関による確認報告、インシデント対応報告、改善事項についての提言を行います。

【報告事項】

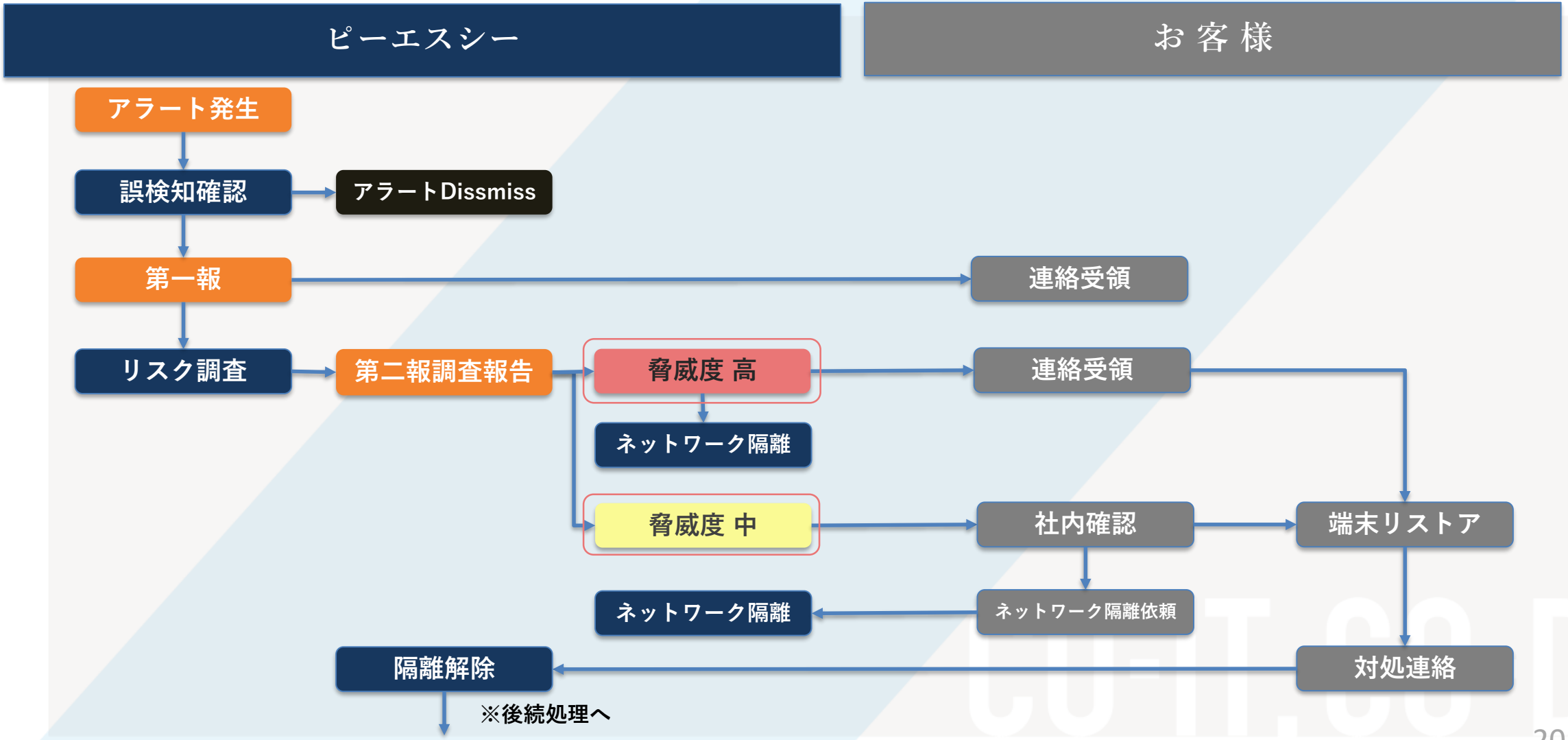
1．当月の概要
2．攻撃状況統計
3．インシデント対応履歴
4．重要度「高」の
　　インシデント詳細
　※マルウェア情報・対処報告
5．チューニング確認事項
　※URL等遮断許可依頼
6．セキュリティ強化対策事項
7．運用報告
8．脆弱性情報トピックス

連絡からの作業フロー

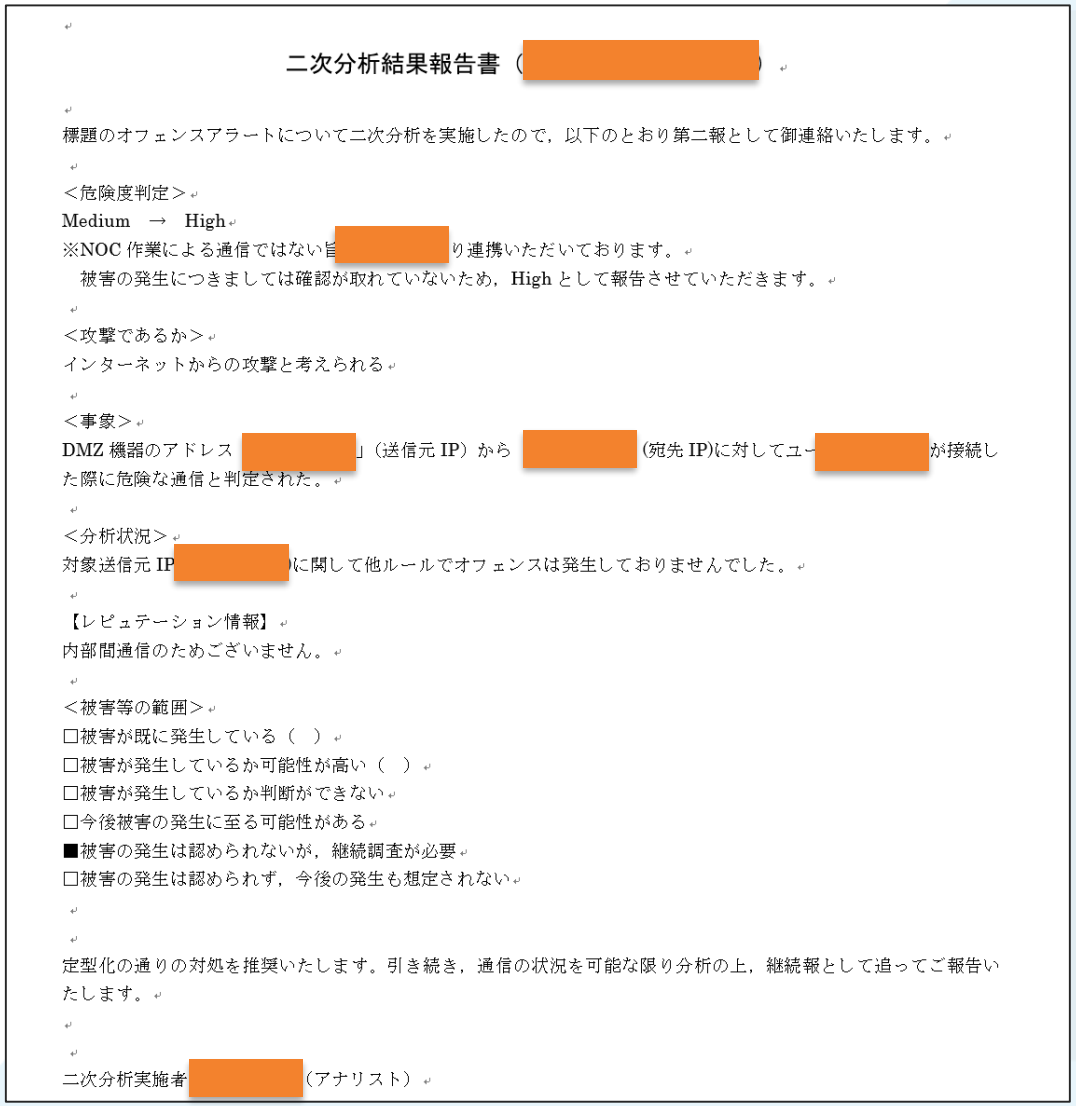
検知からの対応については、事前にフローテンプレートを提示し、お客様に合ったフローにカスタマイズしていきます。
カスタマイズしたフローは「運用仕様書」として規定し、その後の運用にて必要に応じて修正していくことが可能です。



基本監視フロー（ネットワーク隔離の場合）



分析内容例



二次分析結果報告書（[redacted]）

標題のオフェンスアラートについて二次分析を実施したので，以下のとおり第二報として御連絡いたします。

＜危険度判定＞
Medium → High
※NOC 作業による通信ではない旨[redacted]り連携いただいております。
被害の発生につきましては確認が取れていないため，High として報告させていただきます。

＜攻撃であるか＞
インターネットからの攻撃と考えられる

＜事象＞
DMZ 機器のアドレス[redacted]」（送信元 IP）から[redacted](宛先 IP)に対してユー[redacted]が接続した際に危険な通信と判定された。

＜分析状況＞
対象送信元 IP[redacted]に関して他ルールでオフェンスは発生しておりませんでした。

【レピュテーション情報】
内部間通信のためございません。

＜被害等の範囲＞
□被害が既に発生している（ ）
□被害が発生しているか可能性が高い（ ）
□被害が発生しているか判断ができない
□今後被害の発生に至る可能性がある
■被害の発生は認められないが，継続調査が必要
□被害の発生は認められず，今後の発生も想定されない

定型化の通りの対処を推奨いたします。引き続き，通信の状況を可能な限り分析の上，継続報として追ってご報告いたします。

二次分析実施者[redacted]（アナリスト）

以下の項目について、二次分析フローを作成、対応しています。

- ◆ マルウェア感染の危険度
- ◆ 攻撃の有無
- ◆ 侵入拡大検知
- ◆ 分析状況
- ◆ 送信元評価
- ◆ 対処方法

分析結果報告書はWordファイルにて提出いたします。（左図参照）

実績（エンドポイントセキュリティ）

全体契約数 161契約 99社
※各セキュリティ製品（WAF、SandBox、IDPS含む）

Microsoftセキュリティサービス事例

■某製造系販売会社様
規模　　：1200ユーザ
提供サービス：MDE、MIP、MDO構築、運用設計、運用
期間　　：2022年で5年目

■某理系大学様
規模　　：1500ユーザ
提供サービス：MDO構築、保守、ヘルプデスク、 その他
期間　　：2022年で1年目

■セキュリティベンダー（OEM）
対象　　：3社
提供サービス：Sentiel、E5サポート
期間　　：2022年で１年目

■SIベンダー様
規模　　：製造系グローバル
提供サービス：Sentinel 構築
期間　　：2020年4月から1年間

■某大手製造業様
規模　　：14,000ユーザ
提供サービス：MDE 運用設計、運用サービス
（国内　※夏以降国外予定）
期間　　：2022年2月より開始

■某大手証券会社様
規模　　：6,000ユーザ
提供サービス：MDE 構築、運用設計、運用サービス
期間　　：2021年12月より開始

統合SOC事例

■某電力会社様
規模　　：本社、グループ企業のユーザ認証攻撃対策
提供サービス：SIEMアセスメント、再構築
サービス形式：コンサルティング

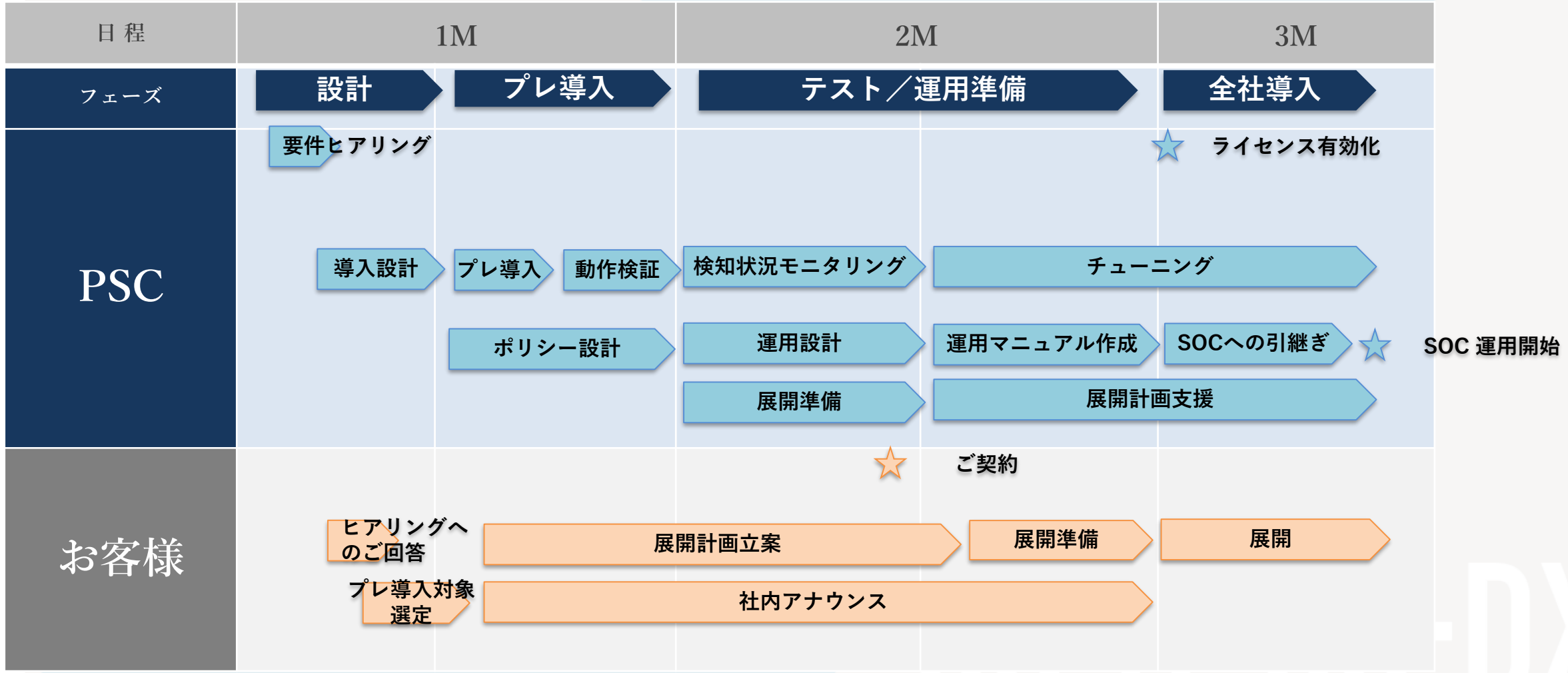
■省庁関係
規模　　：5万人の職員のインターネットアクセスを監視
提供サービス：SIEM運用サービス
サービス形式：弊社SOCよりサービス提供

■某自動車会社様
規模　　：従業員約3万人を対象とした情報流出の監視を実施
提供サービス：SIEM運用サービス
サービス形式：弊社SOCよりサービス提供

■某組合様
規模　　：日本全国の組合員の社内ネットワークの相関分析サービス
提供サービス：SIEM運用サービス、WAF運用サービス
サービス形式：弊社SOCよりサービス提供

■某私立大学様
規模　　：岡山県の某私立大学の職員及び学生の利用するインターネットゲートウェイにあるF/W、IPSをSIEMで監視
提供サービス：クラウド型SIEMサービス
サービス形式：弊社SOCよりサービス提供

個別対応EDR導入スケジュール



02

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

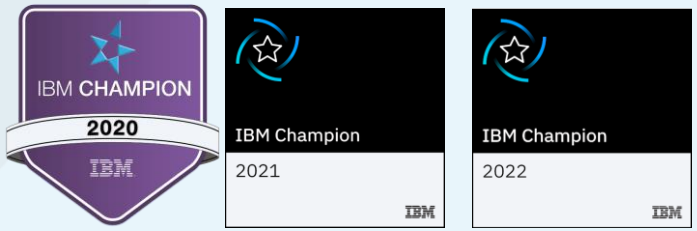
1. 自社保有施設

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

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

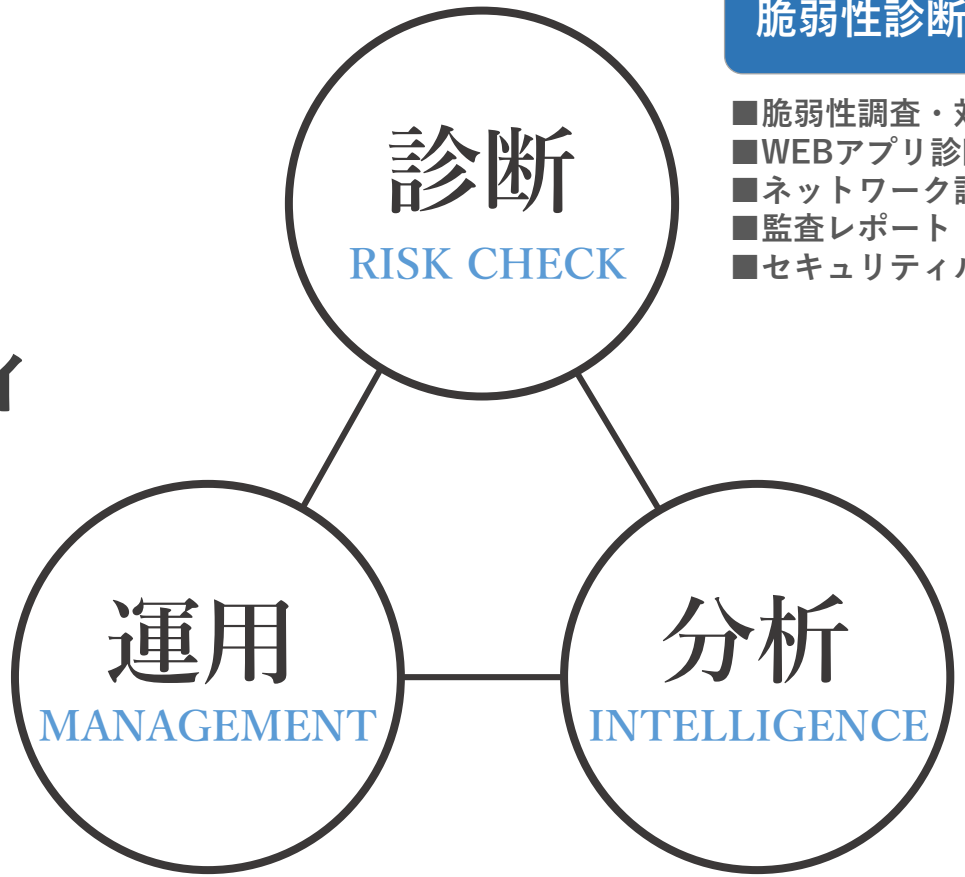
セキュリティサービス体制

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

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。

取り扱い製品

One Stop Solution

診　断	AppScan NESSUS	
監視/防御 （サイバー攻撃対策）	IBM XGS Imperva WAF Barracuda WAF Microsoft Firewall	Fire EYE Palo Alto Trend Micro Microsoft/AWS WAF
		Web Argus F5 Networks AKAMAI
監視/防御 （端 末・SWG）	Trend Micro MS Defender for Endpoint Carbon Black	iBoss Akamai ETP/EAA
分　析	IBM QRadar SPLUNK MS Sentinel	
調　査	MS Defender for Endpoint Carbon Black	

お客様の環境に合わせてサービスを提供する
マネージドセキュリティサービスを
アセスメント、構築からワンストップで提供します。

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。

導入～運用まで
ワンストップ

月間延95社　月間延161PJ

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

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

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。

脅威度別対応表

脅威度	対　応	対応期間
CRITICAL HIGH	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
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 INFORMATIONAL	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。	

EOF