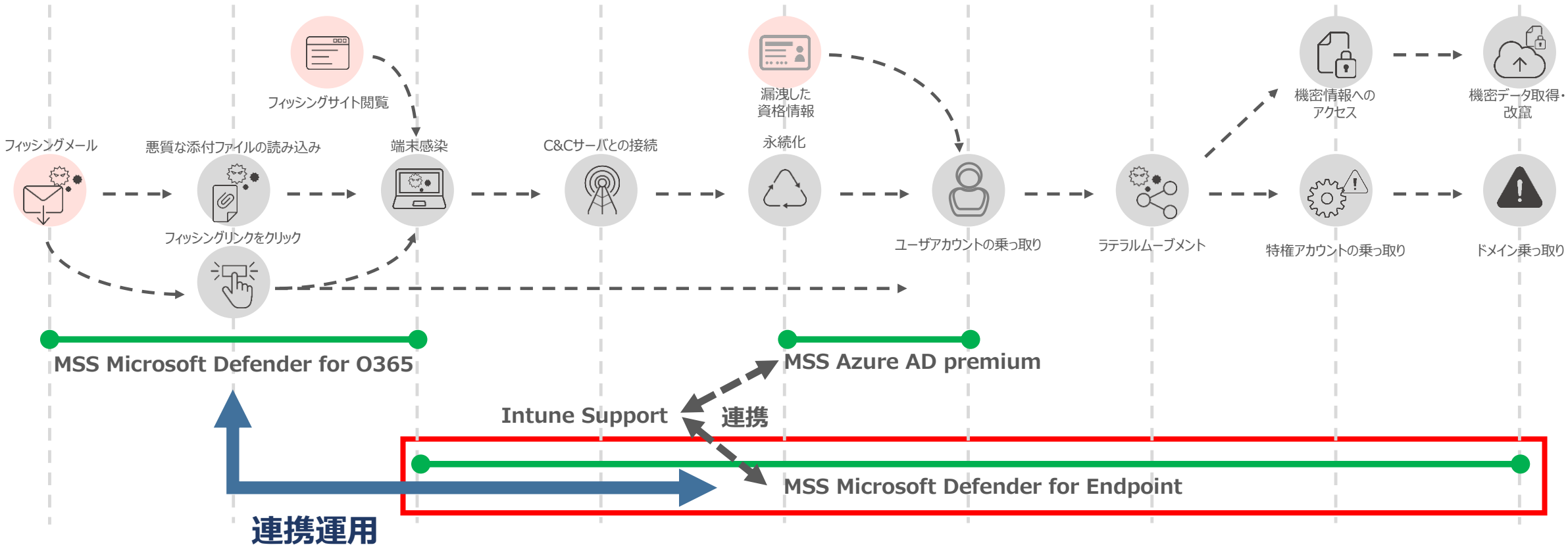
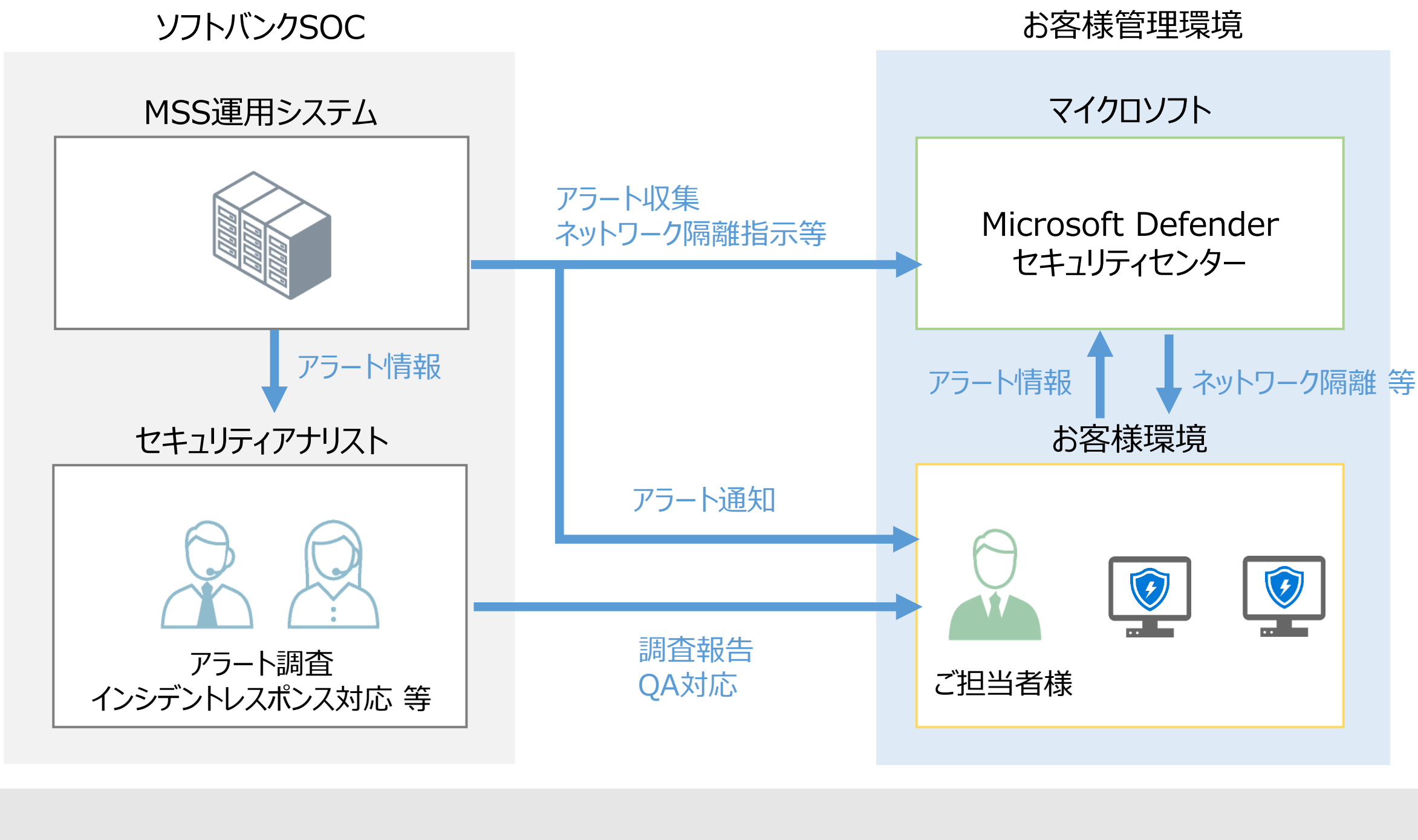
SoftBank for Biz

マネージドセキュリティサービス
Microsoft Defender for Endpoint

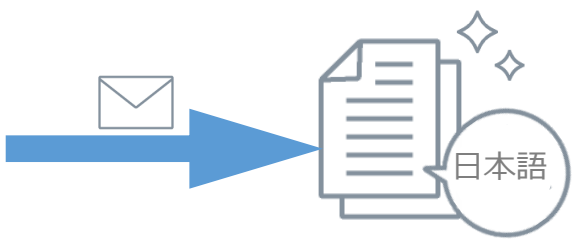
Microsoft Defender for Endpoint（以下、MDE）は、Microsoft 365 E5などに含まれるEDR（予防的な保護、侵害後の検出等）を行うエンドポイントセキュリティソリューションです。ソフトバンクではMDEを利用するお客様環境に対して、監視、調査、封じ込め、根絶といったお客さまの環境をより堅牢にするセキュリティ監視運用サービスを提供します。



サービス概要

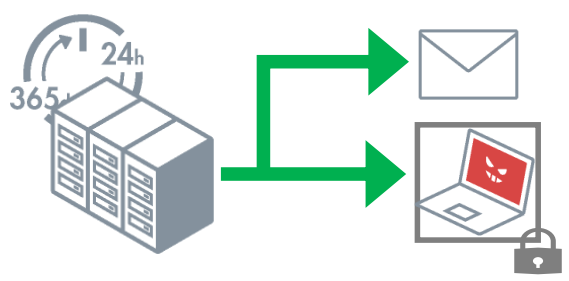


本サービスの特徴



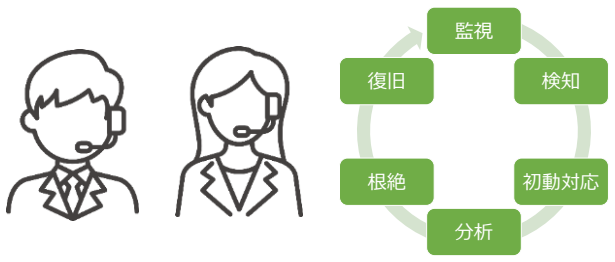
Point.1 詳細なアラート通知の提示と日本語化

・アラート発生時に通常のMDEが出力するアラートに
「いつ」、「誰に」、「何が起こったのか」などの情報を追加し、
日本語でアラート通知を実施します。



Point.2 自動化による迅速な初動対応

・アラート監視から通知、情報取得、MSS判定に合わせて
その後の封じ込めまでを自動化させることで、迅速な初動対応を実現



Point.3 検知から対処までサポートを提供

・アラート検知から初動対応、調査、インシデントレスポンス
(根絶、復旧)まで提供します。

メニュー一覧

メニュー	内容	概要
標準メニュー	アラート監視	MDEのアラートを監視し、出力したアラート内容に情報を付与し、通知します。
	アラート調査	MDEのアラートに対して調査を行い、結果をお客さまにご報告します。
	インシデントレスポンス	MDEのアラート発生時、MSSで判定した重大度に応じて対象端末のネットワーク隔離を行います。 端末に対してクリーンアップ処理を行います。
	接続状況監視	Defender Security Centerとセンサー間で一定期間通信が無かった場合、通知します。
	問い合わせ対応	本サービスの仕様やアラート調査に関する問い合わせ受け付け窓口を開設し対応します。
オプションメニュー	導入支援	MDEのオンボーディング支援を提供します。
	月次報告会	月次レポートを作成し、リモートでの報告会を実施します。
	アクティブディフェンス	定期クエリやスレットハンディングなどを行います。
	リモートフォレンジック	特定の感染被疑端末に対して侵害調査を行います。

お問合せ先
MSS：Microsoft Defender for Endpointに関するお問合せはこちら
https://tm.softbank.jp/form/security/mss/index.php