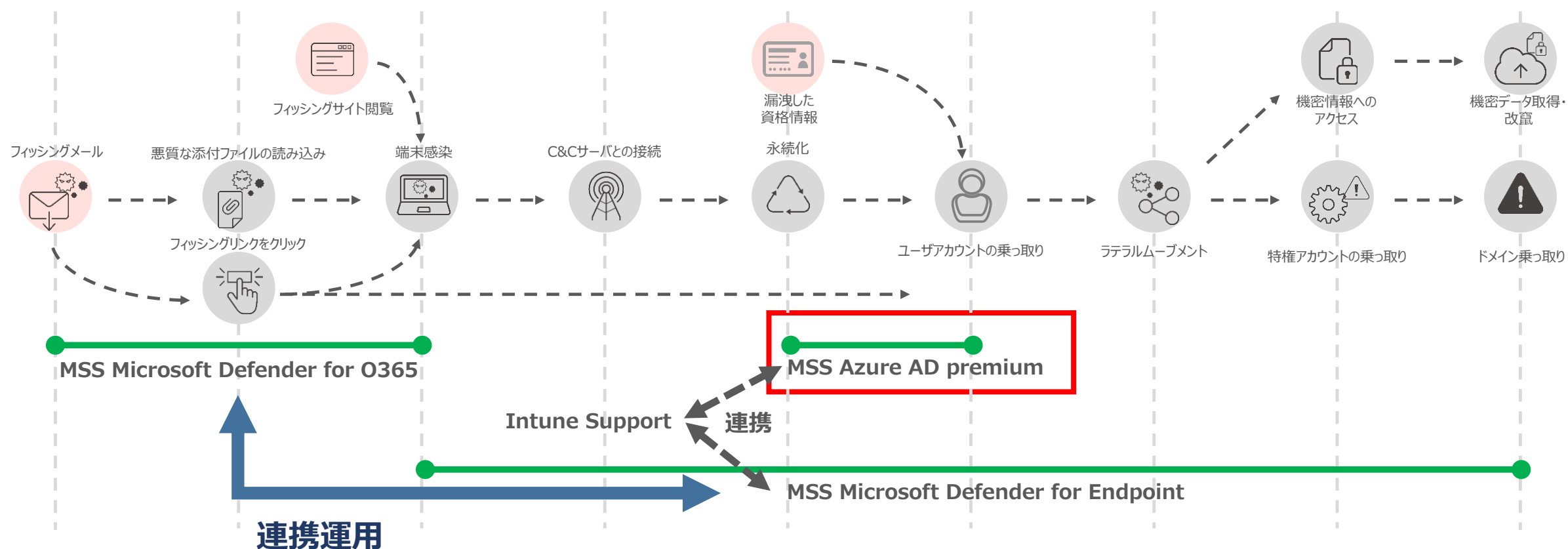
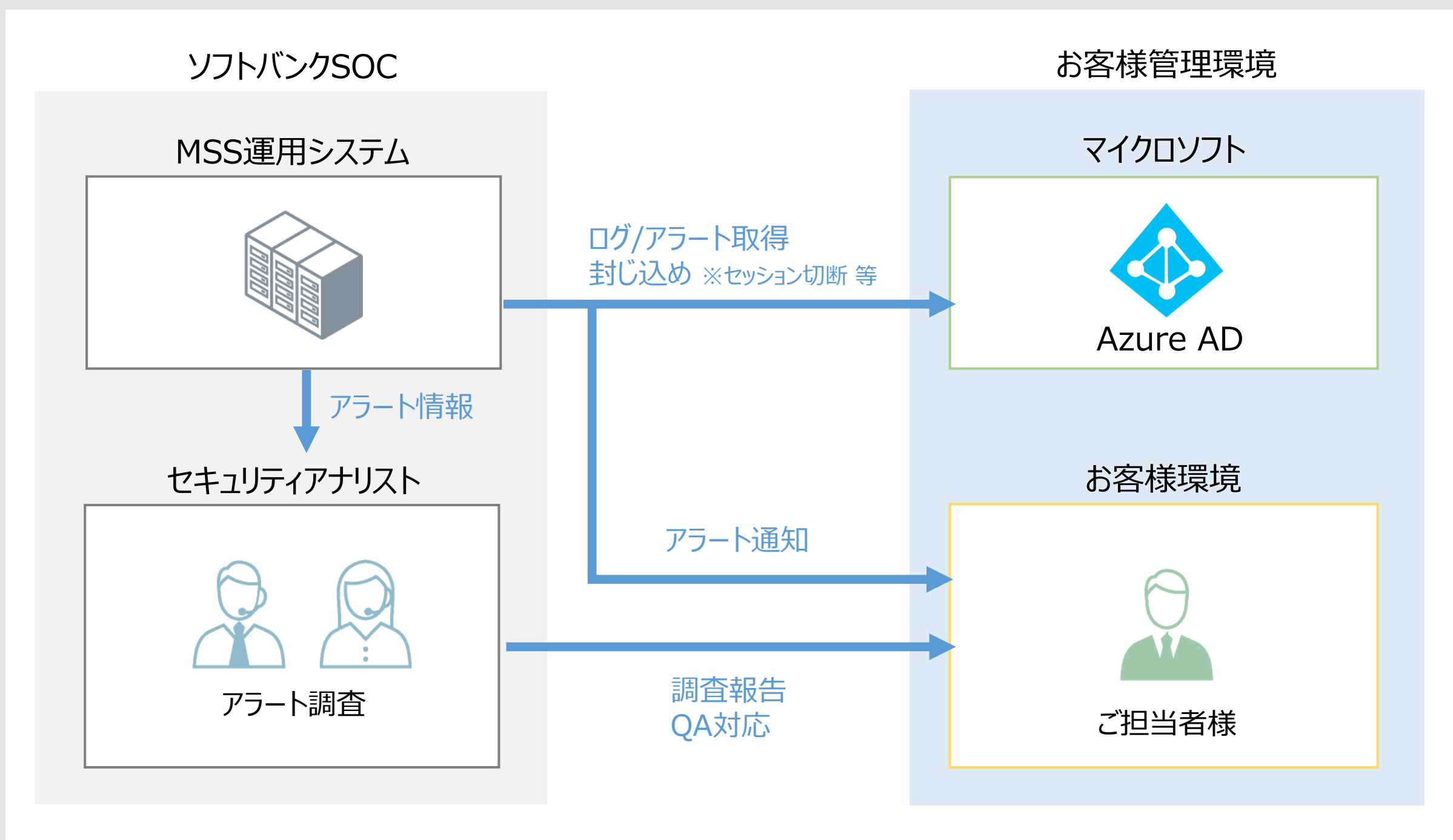


マネージドセキュリティサービス Azure AD Premium

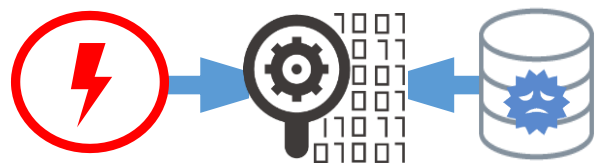
Azure ADは統合認証基盤の機能だけでなく、管理するIDへの不正アクセスを検知、保護する機能が提供されるサービスです。ソフトバンクでは、Azure AD Premium P1、Premium P2をご利用のお客さまに対して、ソフトバンクが持つ脅威インテリジェンスによる不正アクセスの監視や、封じ込め等、お客さま環境をより堅牢にするセキュリティ監視運用サービスを提供します。



サービス概要

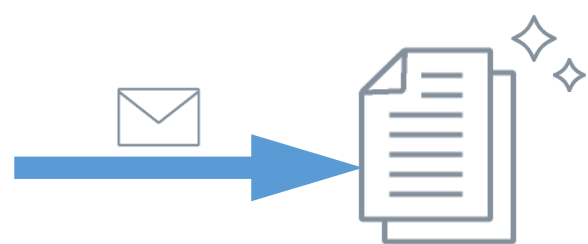


本サービスの特徴



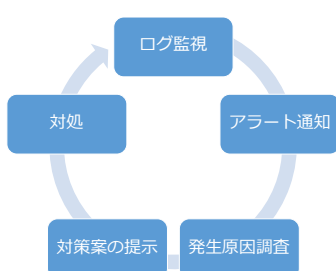
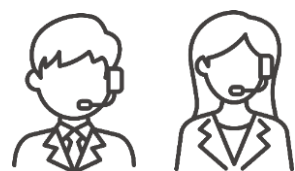
Point.1 独自の脅威情報から不正アクセス検知

- AzureADが出力するサインログに対して弊社が持つ脅威情報を基に不正アクセスの検知を行います。



Point.2 詳細なアラート通知と推奨対応策の提示

- アラート発生時には侵害されたユーザーIDや、侵害の発生時間等「いつ」、「誰に」、「何が起こったか」をお客様へ提示することで、対応判断をスムーズに行うようにします。
- アラート内容に応じて推奨となる対応策を提示します。



Point.3 検知から対処までサポートを提供

- サインログ監視からインシデントの発生原因の調査、対応案の提示、ログインセッションの取り消しといった対処までのサポートを提供します。

メニュー一覧

メニュー	内容	概要
標準メニュー	ログ監視	Azure ADのログを監視し、ログ内容をMSSで判定した重大度に基づき、アラート通知を行います。 重大度については、Azure ADのログ内容を弊社SIEMによる脅威インテリジェンスでの分析やAzure AD P2をご利用の場合、Identity Protectionのリスクレベル含め、MSSの重大度判定を行います。
	アラート調査	• 初動調査：アラート通知後に該当ユーザーに対しサインインログの調査を行い、調査結果を報告します。 • 詳細調査：封じ込め対処の後に調査対象ログでの調査を行い、調査結果を報告します。
	封じ込め	ソフトバンク設定の重大度に応じてセッション取り消しの自動対処を行います。また、お客さまのご了承のもとAzure ADの条件付きアクセスへ、攻撃元特定IPからの接続拒否設定を行います。
	問い合わせ対応	本サービスの仕様に関する問い合わせ受付窓口の対応を提供します。

お問合せ先

MSS : Azure AD Premiumに関するお問合せはこちら

<https://tm.softbank.jp/form/security/mss/index.php>