## 【お客様情報】

システムインテグレーター
企業規模：2,300 名

## 【導入の背景】

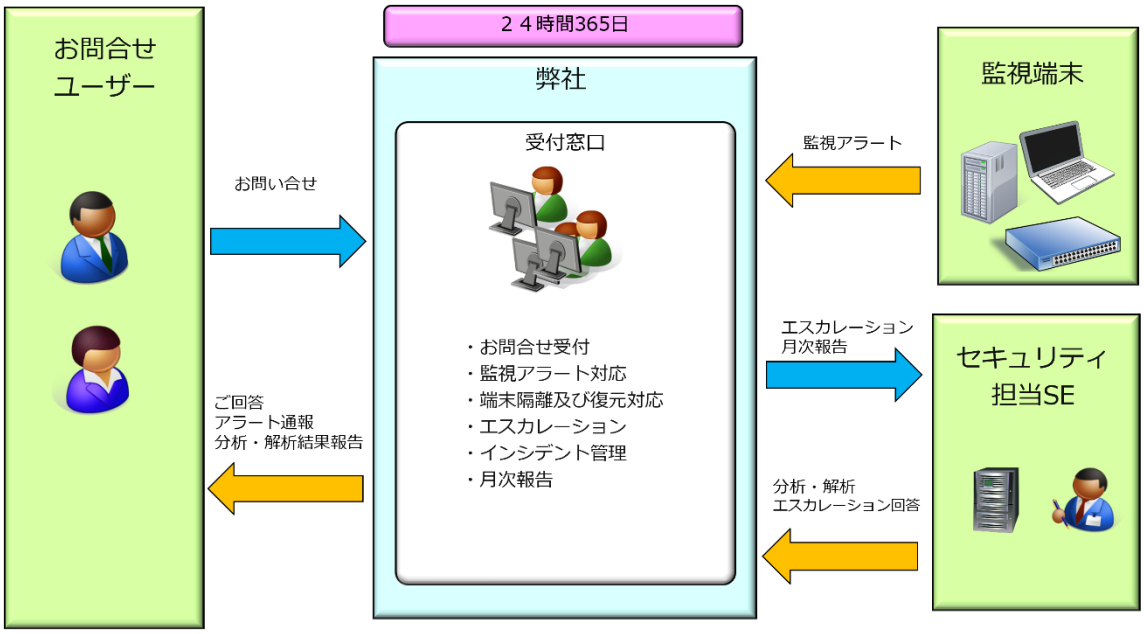
SOC（Security Operation Center）サービスを開始しようとしている。
開始するにあたって 24 時間 365 日対応可能なヘルプデスク窓口を探している。

## 【ヘルプデスク概要】

体制　　：弊社共用オペレータ
時間　　：24 時間 365 日
対応件数：500 件/月
監視対象：PC、サーバー、ネットワーク機器
作業内容：

① 受付対応（お問合せ番号を発行し、お問合せ内容を確認）
② 監視アラート対応（監視アラートの重要度に応じて、お客様へ電話またはメールにて通報）
③ 端末隔離及び復元対応（監視アラートの重要度に応じて、対象端末をネットワークより隔離及び対処後隔離端末の復元）
④ エスカレーション対応（関連部署及びご担当者様へエスカレーション）
⑤ インシデント管理（オープンからクローズまでお問い合わせの管理）
⑥ 報告（月次報告にてヘルプデスク作業報告）

サービス提供イメージ：




【具体的なお問い合せ】

・連絡先の変更をお願いします

・メンテナンスがありますので、〇〇までアラートの静観をお願いします

・監視下サーバーのホスト名変更について

・不審なメールを開いてしまった端末の解析依頼

・ウイルスが検知された場合の対処について

## 【導入効果】

既存の 24 時間 365 日のヘルプデスク体制を利用することにより、低コストにてヘルプデスク窓口が開設できた。IT 技術に強いオペレータが対応しているため、端末の切り離し等のオペレーション作業や監視アラート通知作業等手間のかかる作業を任せることができ、セキュリティ SE は、アラートの分析や解析等より高度な作業に専念することができた。