企業向けサイバーセキュリティソリューション

Palo Alto SOCサービス

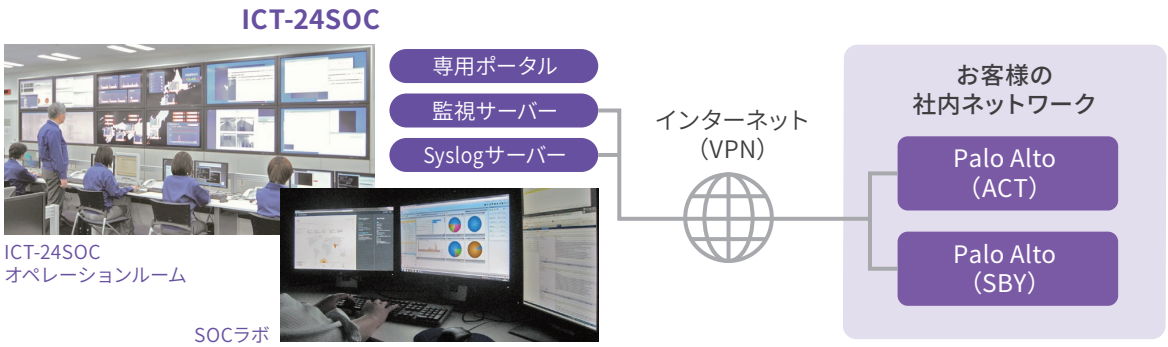
PaloAltoも、適切に管理しなければ

セキュリティインシデントのリスクが高まります。

お客様のPalo Altoを、当社のICT-24SOCが24時間365日監視することにより セキュリティインシデントの早期発見をサポートします。

セキュリティ対策のために設置したPalo Altoを、導入時のまま放置していませんか？ サイバー攻撃は常に進化しており、適切な管理を怠れば、PaloAltoを導入していてもセキュリティインシデントのリスクは確実に高まります。

Palo Alto SOCサービスは、24時間365日リアルタイム監視によってセキュリティインシデントの兆候をいち早く察知し、Palo Altoが持つポテンシャルを最大限に活用することで、御社のネットワークを安全に保ちます。



POINT 1

重要アラートのみのお知らせが可能

POINT 2

インシデント初動対応支援が可能

POINT 3

イベントログの保存が可能

セキュリティ Security

https://www.ntt-at.co.jp/product/paloalto-soc/

サービスメニュー

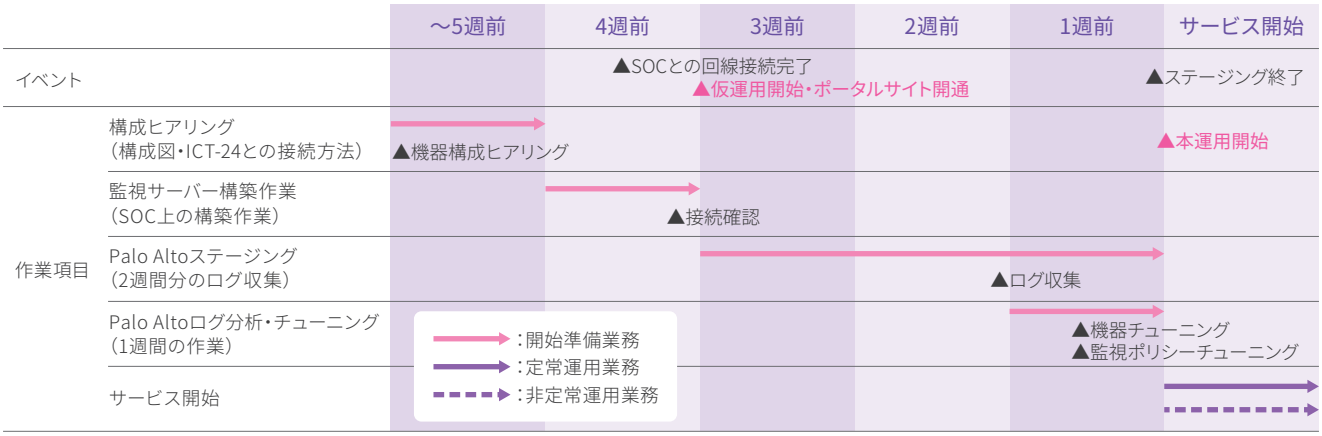
● お客様のニーズに応じたサービスプランをご用意しています。

サービスプラン①・・・・・稼働監視、アラーム通知といった必要最低限のメニューを含むベーシックプラン
サービスプラン②・・・・・脅威の動向や影響度分析が知りたいお客様向けのレポート付プラン
サービスプラン③・・・・・重要性の高いアラートに絞った通知、インシデント対応支援、月次レポート等、すべてを含んだマネージドプラン

サービスメニュー		サービス内容	①	②	③
基本サービス	コンテンツアップデート	最新シグネチャへの定期的な更新確認	○	○	○
	設定等チューニング	検知イベントを監視して検知・防御を最適化	―	―	○
	ソフトウェアアップデート	最新ソフトウェアの更新（安定をバージョン優先）	○	○	○
	正常稼働監視	機器の正常稼働を監視／トラブル時の切り分けと原因の調査	○	○	○
	イベント保全	Syslogサーバーへの自動転送による保全	○	○	○
	設定バックアップ	設定変更時はすべてバックアップ	○	○	○
	ポリシー設定変更	ユーザーからのリクエストを受けて実施（弊社業務時間帯・チケット制）	○	○	○
イベントハンドリング	アラーム分析・通知	未知の攻撃・不審な通信を分析し、インシデントの可能性がある場合はメールで通知	○	○	○
	設定変更	定期アラーム分析からのフィードバックによる設定変更	―	―	○
	問い合わせ対応	お客様からの申告に基づきオペレーターが対応	○	○	○
アナリティクス	レポート提供	月次で傾向分析および影響度分析結果を提示	―	○	○
	インシデント初動対応	リモートでインシデント初動対応を支援（弊社業務時間帯・チケット制）	―	―	○

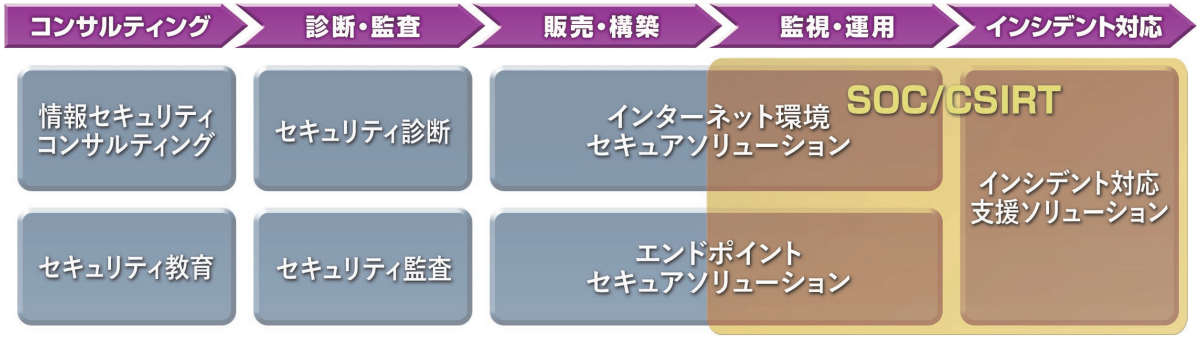
サービス開始までの流れ

● サービス開始まで準備期間は約5週間、ステージング（ログ分析含む）は約3週間です。



・Palo Altoの構築／設置／SOC接続設備は、お客様側でご用意下さい。
・サービス費用以外に別途、初期費用が掛かります。 ・ご利用最短期間は1年です。 ・価格は下記までお問い合わせ下さい。

NTT-ATのトータルセキュリティソリューション



お問い合わせ **https://www.ntt-at.co.jp/product/paloalto-soc/**

NTTアドバンステクノロジ株式会社 セキュリティ事業本部 マネージドサービスビジネスユニット
〒220-0012 神奈川県横浜市西区みなとみらい3-6-3 MMパークビル