NTT西日本　セキュリティオペレーション（セキュリティ運用監視）サービス

ICT 環境における効率的なセキュリティ運用監視サービス

西日本電信電話（以下、NTT西日本）では、24時間365日、クラウドからオンプレミス、ネットワークの統合的な監視オペレーションを提供するとともに、セキュリティ専門家による脅威情報の収集による早期事象解析を実現するセキュリティオペレーションを提供し、お客さまのICT環境やシステム運用の管理負担を軽減します。

課題の顕在化について

「働き方改革」の実現に向けた各企業における取り組みが進められる中で、業務効率化や働き方の多様化（在宅勤務、リモートアクセス等）のためにICT環境の充実が図られるとともに、事業活動を支えている情報システムのセキュリティ対策についても並行して見直されるケースが多々あります。

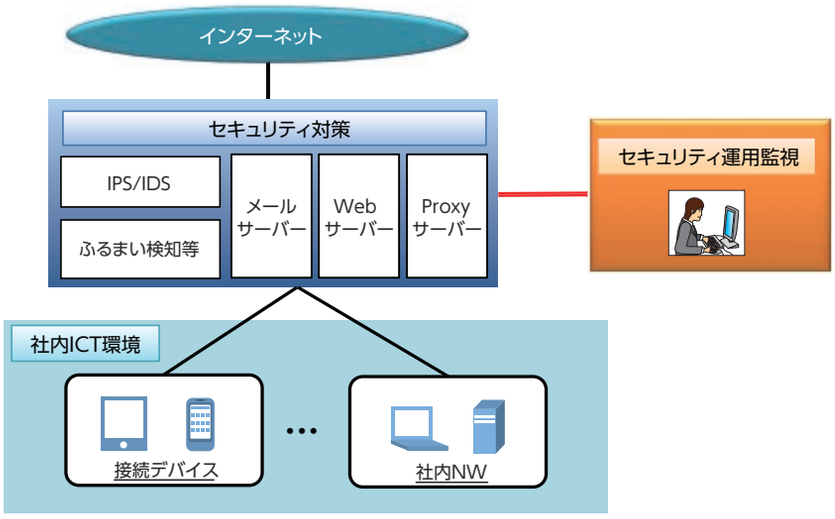


図１　一元的なセキュリティ対策とセキュリティ運用監視モデル

IPA（独立行政法人情報処理推進機構）の「情報セキュリティ10大脅威2018」(2018年1月30日発表)の「『組織』の10大脅威」において、セキュリティ対策や対応の遅れから実被害につながるリスクとして「セキュリティ人材の不足」が取り上げられており、システム運用コストの最適化やセキュリティ技術者確保の手段として、必要な機能をアウトソースすることが重要な選択肢となってきています。

また、経済産業省が策定（2017年11月改訂）している「サイバーセキュリティ経営ガイドライン」においても、企業において「検知」の対策が十分ではないと想定されている（サイバー攻撃を自分たちで気づけていないケースが多い）ことを背景とする改訂ポイントが取り上げられています。

これらは、日本の各企業におけるセキュリティ対策レベルの実態をあらわすとともに、サイバーセキュリティ脅威の高まりに合わせて、今後さらに課題が浮き彫りになると想定されます。

対策トレンドについて

マイナンバー制度導入に合わせて自治体が導入を推進したセキュリティ強化対策事業や、学校教育活動のICT活用における教育情報システムの強靭性向上などにおいて、セキュリティ対策のポイントとして一元管理が取り上げられています。これらは、社内のICT環境から外部のインターネットに接続する接続点を集約することにより、効率的なセキュリティ対策とセキュリティ運用監視を実現するなど、サイバーセキュリティ対策トレンドとして各企業も参考にすることができます（図１参照）。

脅威の可視化について

サイバーセキュリティ脅威は日々拡大し続けており、各企業の事業活動において考慮しなければならない状況は高まっています。拡大し続けるサイバーセキュリティ脅威に対応していくには、セキュリティ対策機器の導入にとどまらず、脅威情報をウォッチしながら自社の情報システム運用への影響確認や対応判断をする必要があります（図2参照）。そのためには、高度なセキュリティ専門スキルや膨大なシステム運用リソースが必要です。そのことから、効率的にサイバーセキュリティ脅威を可視化し、脅威の特定を行うセキュリティ運用監視（図3参照）が重要な機能に位置づけられています。

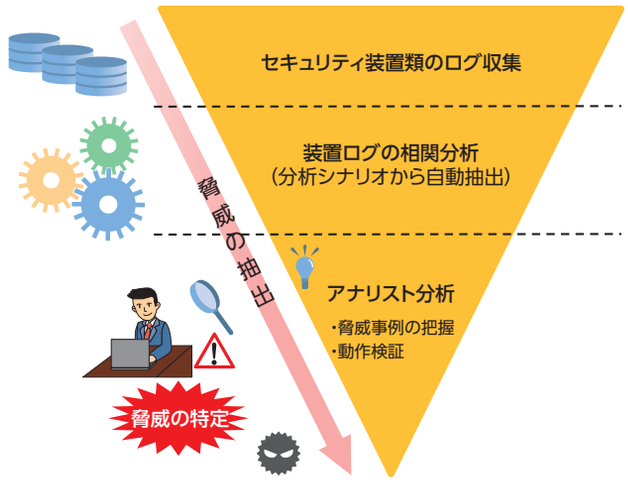
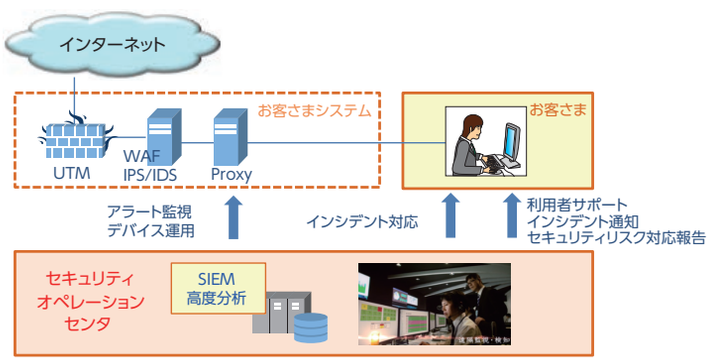


図2　セキュリティ脅威可視化までの分析イメージ

求められる対応策

一般的なセキュリティ対策（セキュリティゲートウェイ機器、アンチウィルスソフトウェア等）をしているにも関わらず、企業情報を公開するサーバーへの不正侵入や社員の業務端末でのマルウェア感染など、事業継続を脅かすセキュリティインシデント事例がマスメディア等で多く取り上げられています。そのような現状において求められる対応策としては、ICT環境における社内外の通信状況を監視し、セキュリティ脅威の発生に素早く気づくことが重要になってきます。

NTT西日本では、前出の「対策トレンド」において述べた自治体や教育委員会での一元的なセキュリティ運用監視の実績に加え、長年のセキュアで安定的なネットワークインフラ運用やセキュリティ環境構築実績で積み重ねたノウハウ、約400名のセキュリティ人材（NTT西日本グループ）、西日本エリア（富山県、岐阜県、静岡県以西の30府県）に約200ヶ所あるサポート拠点などの経営資源を活用したセキュリティサービスを提供することにより、お客さまのICT環境における「サイバーセキュリティ脅威＝経営課題」を解決するサポートをさせていただきます。



セキュリティオペレーション	サービス概要	サービス詳細
セキュリティ管理	セキュリティ監視	24時間365日、セキュリティアナリスト有人監視
	高度ログ分析	ログ相関分析+高度アナリスト分析による真の脅威の抽出
	緊急対応	影響拡大防止のための通信緊急遮断（FW、Proxy等）
	通知・レポート	インシデントの通知、定期レポーティング
セキュリティデバイス管理	障害監視	24時間365日、機器障害監視、稼働監視
	セキュリティ機器の設定変更	ポリシー変更、ブラックリスト、ホワイトリスト追加等
	パッチ・シグネチャの最新化	必要に応じたパッチ・シグネチャー適用
CSIRT支援	CSIRT立ち上げ支援	CSIRT立ち上げコンサル、専門家による相談会
	セキュリティ診断	Webセキュリティ/ NWセキュリティ診断（リモート/オンサイト）レポート
	教育支援	エンドユーザーへの定期研修、標的型メール訓練等

図3　セキュリティ運用監視サービスの概要

お問い合わせ先
西日本電信電話株式会社
ビジネス営業本部 クラウドソリューション部 ソリューション担当
TEL：06-6469-4137　E-Mail：sec-info-ml@west.ntt.co.jp
※電話番号をお確かめのうえ、お間違いのないようお願いいたします。

審査：17-2630-1