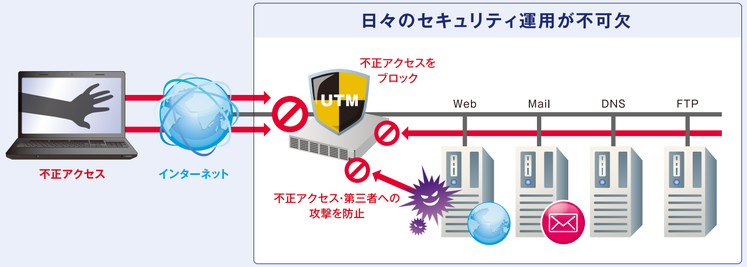
セキュリティ機器の自社導入。
設置して終わりになっていませんか？

近年、不正アクセス等のサイバー攻撃は、
急増していると共に手口が高度化・巧妙化し、
世界的な社会問題となっています。

ITシステムを構成するOSやアプリケーションの
脆弱性は次々と発見され、
それらを修正するための対応を行わなければ、
「対策」できていることにはなりません。

高度化するサイバー攻撃から情報やシステムを守るためには、
変化の激しい情勢を把握し、適時適切かつ迅速な対応が必要です！



本サービス機能一覧

セキュリティマネジメント		内　容
セキュリティインシデント対応	リアルタイムIPSイベント検知	危険度「Critical」かつIPSで遮断していない不正アクセスを検知した場合、お客さまへご連絡します。
	IPSイベント対応アドバイス	検知した不正アクセスに対して、お客さま環境に適したセキュリティ設定を検討し、検知内容と推奨対策内容をご連絡し、お客さま承認後、作業を実施します。
	セキュリティログ分析	ファイアウォールのアクセスログを分析し、セキュリティリスクの高い通信を検知した場合、お客さまへご連絡します。
セキュリティオペレーション	IPブラックリストチューニング	全世界で報告されているIPブラックリストに、当サービス検知実績をプラスした精度の高い情報を基に、定期的（3ヶ月に一度）にお客さま機器を最適化します。
	保護対象サーバー脆弱性診断	定期的(※1)にお客さまの公開サーバー（保護対象）に対して最新の脆弱性診断を実施し、発見された脆弱性に対する攻撃を防御するよう設定します。
	IPSシグネチャチューニング	保護対象機器メーカーより新たなシグネチャがリリースされた場合、お客さま環境を考慮し、シグネチャの有効/無効化作業を実施します。(※2)
ログ管理・分析	ログ収集	お客さま先にログ収集用サーバーを設置し、セキュリティログを収集します。収集したログはセキュアに保管します。ログ保管容量は1ヶ月あたり10GBを上限としています。(オプションで追加可能)
	Webポータル	お客さま専用の監視Webポータルをご提供します。1契約につき1アカウント（ID）を発行し、各レポートもポータルサイトを通じご提供します。
	セキュリティログレポート	専用ポータルで閲覧可能な基本サマリレポートをご提供します。
ヘルプデスク	ヘルプデスク	サービス内容、機器仕様などに関するお問い合わせに回答します。受付はメールまたは電話にて24時間365日、対応は平日9:00-17:00となります。
	運用報告会	年に1回監視サービスの結果をまとめ、報告会を実施します。オプションで、半期に1回など追加することも可能です。

システムマネジメント		内　容
性能監視	基本性能監視	トラフィック監視、CPU使用率監視、メモリ使用率監視、コネクション数監視を行います。それぞれに設定した閾値以上となった場合に、障害と判断し、ご連絡します。
	性能監視詳細通知・対応(※3)	「基本性能監視」で対象とする監視項目にて、障害の発生または復旧を検知した場合、発生原因等について調査を行い、調査結果をメールでご報告します。
稼働監視	基本稼動監視	ノード監視、ポートステータス監視、冗長化ステータス監視(※4)を行います。それぞれに設定した閾値以上となった場合に、障害と判断し、ご連絡します。
	セキュリティ機能監視	ファイアウォールフィルタリング監視、アンチウイルスパターンファイル更新監視、IPSシグネチャ更新監視、URLフィルタリングDB更新監視などを行います。
	保護対象サーバー監視	サービス対象機器のセキュリティポリシーにて保護される公開サーバーを監視します。標準で最大10台（10グローバルIPアドレス）までの監視が可能です。
	稼動監視詳細通知・対応(※3)	「基本稼動監視」で対象とする監視項目について、障害の発生または復旧を検知した場合、発生原因等について調査を行い、調査結果をメールにてご報告します。
システムオペレーション	設定変更	「定期シグネチャチューニング」「緊急シグネチャチューニング」「カスタムシグネチャ適用」の作業や、お客さまからご依頼の設定変更作業を回数無制限で対応します。
	設定情報バックアップ保管	それぞれの設定変更作業を実施する際には、設定情報のバックアップを取得し、過去2世代分を保管します。
	バージョンアップ(※5)	メーカーサポート終了および不具合解消を目的とした、バージョンアップ作業を原則年1回、リモート接続にて実施します。
障害復旧支援	障害復旧支援(※6)	障害発生時の復旧支援を行います。機器交換が必要となる場合は、機器交換手配、最新の設定情報バックアップファイルを用いた論理復旧などご一貫した対応を行います。 ※ただし、機器交換後のOSのインストール、最新コンフィグの投入は、本サービスに含まれていない為、保守ベンダーに実施いただきます。(最新コンフィグは保守ベンダーへ連携します。)

※1 定期的に実施するには、サービス利用時に予め実施のお申し出をいただく必要があります。※2 作業はお客さまにご指示をいただいてから行います。※3 すべての事象について、確実に原因を特定することをお約束するものではございません。※4 本項目は、Active/Standbyの冗長化構成を採用している場合にのみご利用いただけます。※5 メジャーバージョンアップ、マイナーバージョンアップを問わず実施しますが、機器仕様及び当社検証結果より推奨バージョンとない場合は対象外とします。※6 すべての事象について確実に原因を特定することをお約束するものではございません。また、機器のLED点灯状況のご確認など、お客さまにてご対応いただく場合があります。

本サービス料金

本サービスは月額サービスとなっており、お客さまがご利用される監視対象機器の型番によってサービス料金が異なります。
また、サービス開始にあたり、初期費用が必要となります。詳しくは当社営業担当までお問い合わせください。

STNet
エスティネット　検索
eigyo@stnet.co.jp
TEL 087-887-2404（ビジネス営業本部）
※お問い合わせの回答は営業時間内（平日9:00～17:00）となります。

本店ビジネス営業本部 ／ TEL.087-887-2404　首都圏営業部 ／ TEL.03-4588-4211
香 川 支 店 ／ TEL.087-887-2480　愛 媛 支 店 ／ TEL.089-906-2480
徳 島 支 店 ／ TEL.088-635-2480　高 知 支 店 ／ TEL.088-879-2480

STNetのサービスが、皆さまのビジネスの力に。
データセンター・クラウド　ネットワーク　システム開発

(S)SOC2-1

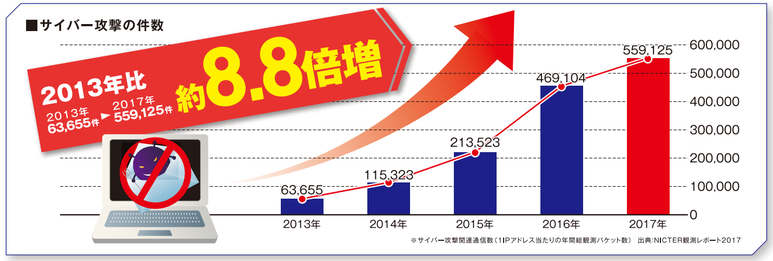
STNet
STNetのサービスが、皆さまのビジネスの力に。

急増するサイバー攻撃や企業のセキュアなネットワーク環境維持･･･
これらに対応できるセキュリティ人材の確保はできていますか？

STNetセキュリティ運用監視サービス

『NetStare』（ネットステア）supported by SecuAvail

■サイバー攻撃の件数



※サイバー攻撃関連通信数（1IPアドレス当たりの年間総観測パケット数）　出典:NICTER観測レポート2017

多くの企業が抱える課題

リソース確保　セキュリティ予算確保　専門スキル判断力醸成

課題解決

セキュアなネットワークシステムの維持を
NetStare® で サポート！

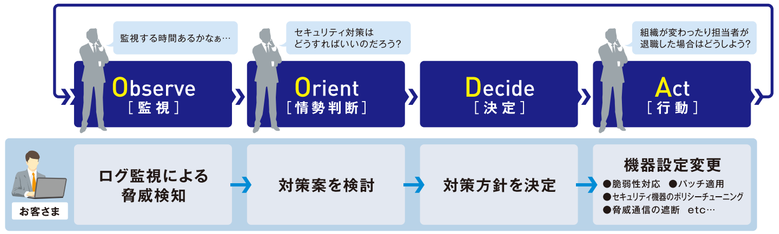
STNetセキュリティ運用監視サービス

NetStare®［ネットステア］ supported by SecuAvail

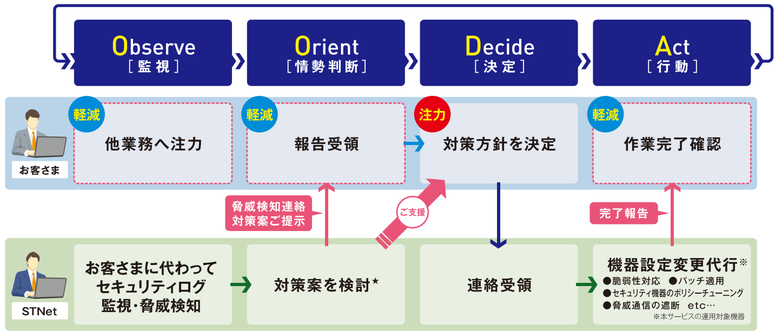
企業を取り巻くセキュリティ環境は厳しさを増しており、ITシステムを構成するOSやアプリケーションの脆弱性は次々に発見され、それらを修正するための対応業務は、多くの手間と時間がかかります。人的リソースはもちろんのこと、高度な専門知識も必要となり、インシデントが起こった場合には、即座に対処することが求められます。本サービスは、これらのセキュアな環境維持に必要な『OODAループによるセキュリティ運用』をサポートします。

セキュリティ運用に必要な「OODA（ウゥーダ）ループ」の実現をサポート

OODAループ（ウゥーダ・ループ）とは　アメリカ空軍のジョン・ボイド大佐によって提唱された意思決定理論。朝鮮戦争の航空戦についての洞察を基盤にして、指揮官のあるべき意思決定プロセスを分かりやすく理論化したもの。



STNet supported by SecuAvail の NetStare®［ネットステア］サービスご利用の場合



★危険度「Critical」かつIPSで遮断していない不正アクセスを検知したとき、お客さまの環境に適したセキュリティ設定を検討します。セキュリティログ分析の通知は1時間に一度閾値を超えた通信を自動通知します。

「OODAループ」の業務負荷を軽減し、迅速なセキュリティ運用対策の対応を可能にします。

サービス概要

本サービスは、お客さまシステム（UTM機器・ファイアウォール等）の稼動状態、不正アクセスをネットワーク・セキュリティ運用監視のプロフェッショナルが24時間365日監視し、インシデント発生時には直ちに攻撃内容を調査の上、お客さま環境を考慮した最適な設定を検討します。また、障害発生時には復旧支援だけでなくセキュリティポリシーの改善策まで実施※します。※作業はお客さま承認後の実施となります。

本サービスは、以下セキュリティマネジメント（SOC）とシステムマネジメント（NOC）を統合してご提供するサービスです。※SOC（Security Operation Center）　NOC（Network Operation Center）

セキュリティマネジメント　ネットワークセキュリティの脅威から保護

不正アクセスを検知して緊急対応（セキュリティインシデント対応）
外部からの攻撃の有無をセキュリティの専門家が24時間365日体制で監視し、インシデント発生時には直ちに攻撃内容を調査します。保護対象の環境を考慮した最適な設定を検討・対応します。

様々な攻撃を防御（セキュリティオペレーション）
セキュリティ機器の設定パラメータやシグネチャのチューニングにより、常に最新の状態でシステムを維持します。また、定期的※な脆弱性診断で、セキュリティリスクに対し事前対応を行います。
※定期的に実施するには、サービス利用時に予め実施のお申し出をいただく必要があります。

問題発生のリスクを洗い出す（ログ管理・分析）
システムやセキュリティ機器から得られるシステム・セキュリティログ・各種イベント情報を日常的に監視・解析し、問題が発生するリスクを早期に発見することで、インシデントを未然に防ぎ、脅威の拡散を防止します。

お客さまの悩みを解消（ヘルプデスク）
ヘルプデスクの体制は、SOCオペレーター、アナリストで構成され、ネットワーク・セキュリティの専門チームでお客さまのシステムを24時間365日体制でサポートします。対応は、平日9:00～17:00となります。

システムマネジメント　ネットワークシステムを統合的に運用管理

常に最適なパフォーマンスを維持（性能監視）
システムを構成する機器が本来の性能を発揮できているかどうかを把握し、最適なパフォーマンスを発揮できるよう監視します。これにより、システムダウンを未然に防ぐことができます。

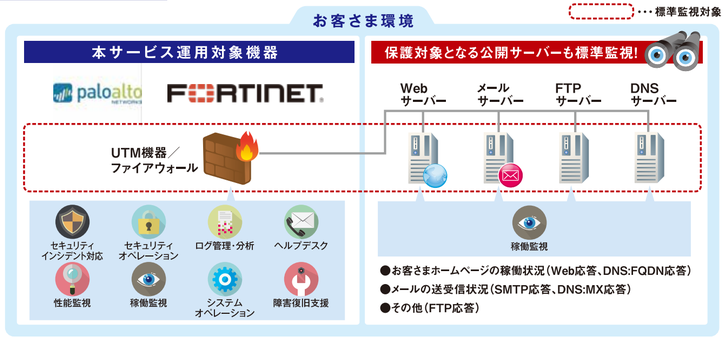
機器とサイト全体を監視（稼働監視）
ノード監視、トラフィック監視、プロセス監視、ポートステータス監視及びシステムの稼働状況を常に監視します。

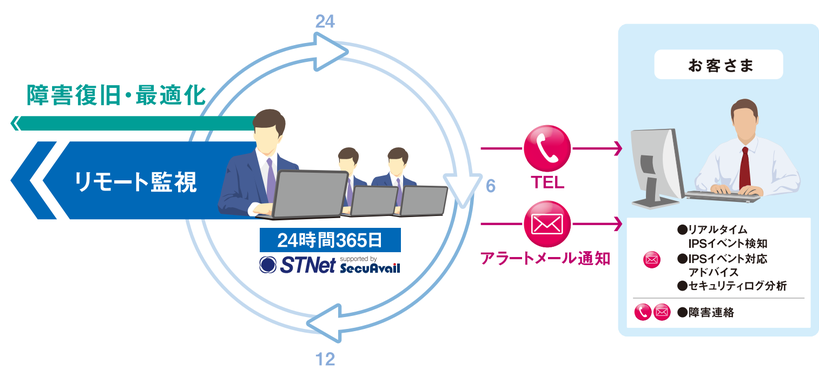
安心安全な環境を維持（システムオペレーション）
ポリシーの追加・変更・削除など、お客さま機器の設定変更作業を実施します。設定変更後はバックアップを実施し、障害復旧に備えます。また、運用対象機器のバージョンアップを年1回行います。

障害の原因を調査分析して復旧（障害復旧支援）
24時間365日体制でお客さまのシステムを監視し、万一システムに障害が発生した場合には、お客さまに代わってシステムを復旧します。

サービスの提供範囲

サービス対象のセキュリティ機器だけではなくサイト全体を標準監視します。



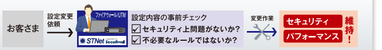


サービスの強み

本サービスでは、以下の内容も標準サービス範囲内でご提供します。

ポイント　ファイアウォールのポリシー変更作業は無制限で対応

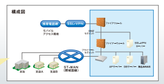
拠点追加やNW構成変更などによるポリシー追加・変更・削除などご要望に応じて変更作業を実施します。依頼内容は、論理的矛盾がないかを精査し、設定作業を行います。



ポイント　今の状態や分析結果をわかりやすいWebポータルで提供

どこで問題が発生しているかをビジュアルで確認ができるため、保守員と顧客など復旧方針を協議し、迅速な対応が行えます。

お客さまのネットワーク全体の構成図を専用ポータルに表示。



ポイント　脆弱性診断を3ヶ月ごとに実施※

対象機器に対して擬似アタックによる検査を行い、システムの脆弱性や想定されるセキュリティリスクを検出し、診断結果に基づき必要となる対策などについてご報告します。

※検出された脆弱性はレベルを区分し、分かりやすいレポートをご提出します。

警告	この項目に示される情報は、一般的に対策の実施が強く推奨されるもので、放置した場合には非常に危険であると考えられるものを示します。
注意	将来的に問点となりそうな項目や改善点に対して有益な情報を公開してしまっている設定上の問題点を示します。

※定期的に実施するには、サービス利用時に予め実施のお申し出をいただく必要があります。

ポイント　機器交換の調整・手配、保守ベンダーとも直接折衝

お客さまの機器に障害や故障が発生した場合に、論理障害に関する問い合わせや物理障害に伴う機器交換の調整・手配など、保守ベンダーとの折衝も代行します。