ＮＴＴコミュニケーションズ
セキュリティ /SDx+Mソリューション

リスクを見渡し、企業情報システムの安全な利用環境を実現する WideAngle

NTTコミュニケーションズ（以下、NTT Com）は、企業向けのセキュリティサービスWideAngleを提供しています。迅速な対処が求められるサイバー攻撃の脅威に対し、新たに提供を開始した「プロアクティブレスポンス」では、SOC（セキュリティオペレーションセンター）からの指示でリスクある通信を自動遮断することが可能です。

広い視野でリスクを見渡す WideAngleのサービス

WideAngle とは、NTT Com が提供する総合リスクマネジメントサービスのブランドです。この名称には、サイバーセキュリティ上の未知の脅威に世界がさらされる中、広い視野でリスクを見渡し、安全・安心な社会を志す開拓者でありたいという思いを込めています。

NTT Com は企業向けのセキュリティサービスを 2 つのラインナップで提供しています。

1 つは WideAngle プロフェッショナルサービスです。CSIRT※1などを設置しセキュリティ管理体制を強化したい企業に対し、NTT Com のセキュリティ専門家の有する知識・経験を、総合コンサルティング、インシデントレスポンス、脆弱性診断、アドバイザリーサポートなどのメニューで提供しています。

プロフェッショナルサービス(PS)

サービス	サービスメニュー	メニュー
CSIRT運用支援ソリューション	総合コンサルティング	
	インシデントレスポンス	総合インシデントレスポンス
		インシデント初動対応パック
		インシデント対応駆付け保証
		標的型マルウェア感染端末調査
	脆弱性診断	プラットフォーム脆弱性診断
		Webアプリケーション脆弱性診断
		セルフ脆弱性診断
	アドバイザリーサポート	
	脆弱性マネジメントプラットフォーム(提供予定)	

マネージドセキュリティサービス(MSS)

サービス	サービスメニュー	メニュー
インフラストラクチャプロテクション	NWセキュリティ	ファイアウォール IPS/IDS
	コンテンツセキュリティ	E-mailアンチウィルス
		Webアンチウィルス
		URLフィルタリング
		アプリケーションフィルタリング
		WAF
リスクマネジメント&スレットプロテクション	リアルタイムマルウェア検知(RTMD)	RTMD ONSITE
		Cloud base RTMD
	エンドポイントスレットプロテクション バリデーション&アイソレーション(EPTP V&I)	
	CLA(Correlation Log Analysis) (非セキュリティ設備との総合ログ相関分析)	
	プロアクティブレスポンス	
個別メニュー	インターネットセキュリティUTM	

表1　WideAngleのサービスメニュー

脅威分析の実力で高い評価を得る アナリスト高度分析

もう 1 つは、WideAngle マネージドセキュリティサービス（WideAngle MSS）です。お客さま環境に設置した IPS/IDS※2などのセキュリティ機器と SOC を回線で結び、機器が検知したセキュリティログをリアルタイムに分析します。もしサイバー攻撃につながる脅威を発見した場合は、セキュリティインシデントレポートとしてお客さまに通知します。

とくに評価されているのが、SOC のリスクアナリストが専門家の目でログを追い脅威の特定を行う「SIEM 分析とアナリストによる高度分析」のオペレーションメニューです。国内で本格的に提供を開始して約 2 年半で 100 社以上の企業にご利用いただいています。

企業が遭遇した脅威に能動的な対処を行う プロアクティブレスポンス

それらの実績をもとに、WideAngle MSS において新たに提供を開始したアドオンメニューが「プロアクティブレスポンス」です。上述した「SIEM 分析とアナリストによる高度分析」にこのプロアクティブレスポンスを付加することで、企業情報システムがサイバー攻撃に見舞われた際に、不正アクセス拡大につながる端末の通信を、SOC の分析結果に基づき即座に抑止することができます。

最近話題になった WannaCry の事件でもわかるように、サイバー攻撃は巧妙化・悪質化する一方であり、被害の拡散を防ぐには脅威をいちはやく発見し迅速に対処すること

がカギとなります。従来型のSOCのサービスでは、脅威を察知しお客さまへのレポートを発行しますが、その後の対処は、業務の継続性への影響も考慮してお客さま企業の担当者に判断を預け、その指示を受けて改めてSOCが通信ブロックのためのポリシー変更を行う形になっていました。しかしこれではお客さま社内の確認・調整にかなりの時間を要してしまいます。

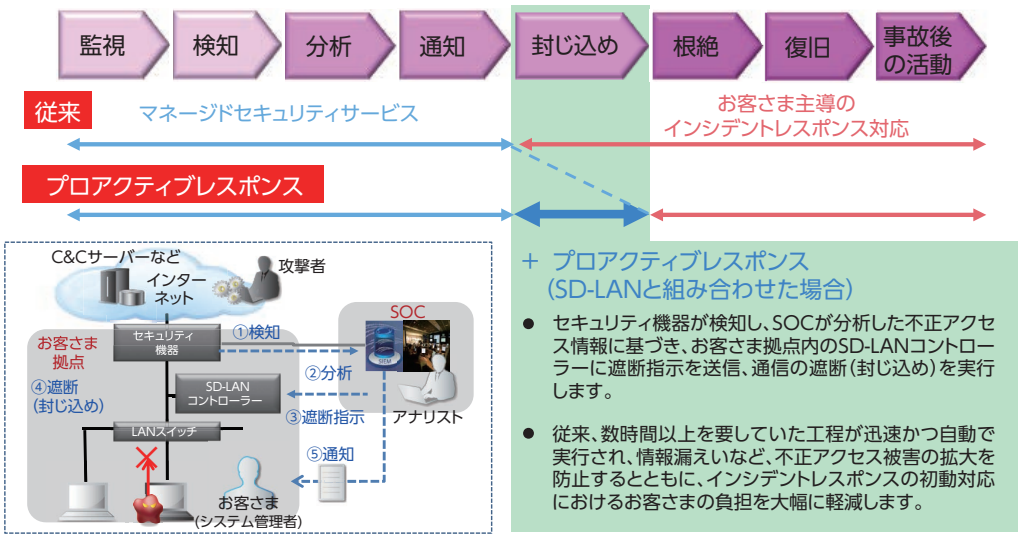

図1　プロアクティブレスポンスの概要とSD-LANとの組み合わせによる提供イメージ

プロアクティブレスポンスでは、SOCのアナリストがレポートを発行すると同時に、マルウェア※3感染が疑われる通信等の遮断指示をお客さま環境のネットワーク機器等に自動的に送信する機能を提供します。これにより、従来お客さま社内のプロセスを含め数時間以上かかっていた対処が、最短の場合数分程度で完了します。

SD-LANとの組み合わせで端末単位の通信遮断が可能

この機能は、NTT Comが推進するSDx+Mソリューション※4と組み合わせることで、より効果的な封じ込めを行うことが可能です。具体的には、端末のIPアドレス単位で通信を遮断することが可能になります。

お客さまのLAN環境に設置されたSD-LANコントローラーとSOCの間を結び、SOCの遮断指示がコントローラーに届くように構成します。遮断指示を受け取ったコントローラーは、SD-LAN配下のLANスイッチを制御し、該当するIPアドレスの端末をネットワークから切り離します。

これによりお客さま企業のセキュリティ管理者は、業務全体への影響を最小限にした上で、侵入経路・被害状況の調査や復旧などのインシデントレスポンスの対応を進めることができるのです。

WideAngle MSSでは、プロアクティブレスポンスの自動連携の対象機器を今後拡大していく予定です。

NTT Comは、企業が直面するサイバーセキュリティ上のリスクに対し能動的な対処と的確な運用支援を提供できる事業者として、WideAngleのもと提供する総合リスクマネジメントサービスの充実に努めていきます。

WideAngleのサービス企画を担当しています。お客さまが安全・安心にインターネットを利用するためのサービスを引き続き検討していきます。

ＮＴＴコミュニケーションズ
経営企画部
マネージドセキュリティサービス推進室
大水 祐一

※1　企業においてサイバーセキュリティに対処する組織の総称。
※2　不正侵入検知・防御システム。
※3　コンピューターウイルスなどの不正プログラムのこと。
※4　Software Defined技術を活用し、ICT環境全体の一元的・効率的な運用管理を実現するNTT Comのソリューション。

お問い合わせ先
NTTコミュニケーションズ株式会社 経営企画部 マネージドセキュリティサービス推進室
TEL:03-6733-0853　E-mail:mss-sp-cp@ntt.com

※http://www.bcm.co.jp/でも閲覧できます。