News Release

2019 年 3 月 28 日

世界初、FortiGate の PCAP データを活用した
セキュリティ高度分析サービスを提供開始

～Fortinet と共同開発し、サイバー脅威検知精度向上とセキュリティ業務効率化に貢献～

NTT コミュニケーションズ株式会社（以下 NTT Com）は、Fortinet, Inc.（以下 Fortinet）のセキュリティアプライアンスである FortiGate を活用したセキュリティ高度分析サービス（以下 本サービス）を、総合リスクマネジメントサービス「WideAngle」のマネージドセキュリティサービスの新メニュー（別紙）として、2019 年 3 月 28 日より提供開始します。

1. 背景

企業の ICT 環境においてサイバー攻撃を防御するには、インターネットゲートウェイに設置した UTM※1 や IDS※2、IPS※3、WAF※4、プロキシサーバーなどの ICT 機器から生成されるセキュリティアラート（以下 アラート）を分析してインシデント対応するのが一般的です。一方で、これらのアラートには、対応が不要な事象も数多く含まれているため、CSIRT やシステム管理者の分析業務負担が課題になっています。

NTT Com は、2003 年よりセキュリティオペレーションセンター（以下 SOC）を開設し、インシデント対応が必要なセキュリティ脅威のみをお客さまに通知するサービスを提供しています。今回、Fortinet との共同開発により、セキュリティアプライアンスの出荷台数で世界をリードする FortiGate において、PCAP データ※5 のリアルタイム分析を実現する世界初※6 の高度分析サービスを提供メニューに加えます。

2. 本サービスの特長

NTT Com は、セキュリティ脅威の迅速かつ的確な検知にあたっては、アラート前後の通信内容である PCAP データをリアルタイムに分析し、サイバー攻撃の有無や詳細な内容をすばやく突き止めることが極めて重要なプロセスと捉えています。本サービスにより、FortiGate を利用しているお客さまをはじめ、多くの企業において、サイバー脅威検知精度の向上と CSIRT やシステム管理者の業務効率化に貢献します。

（1）世界初となる FortiGate を活用したリアルタイムな PCAP データ分析

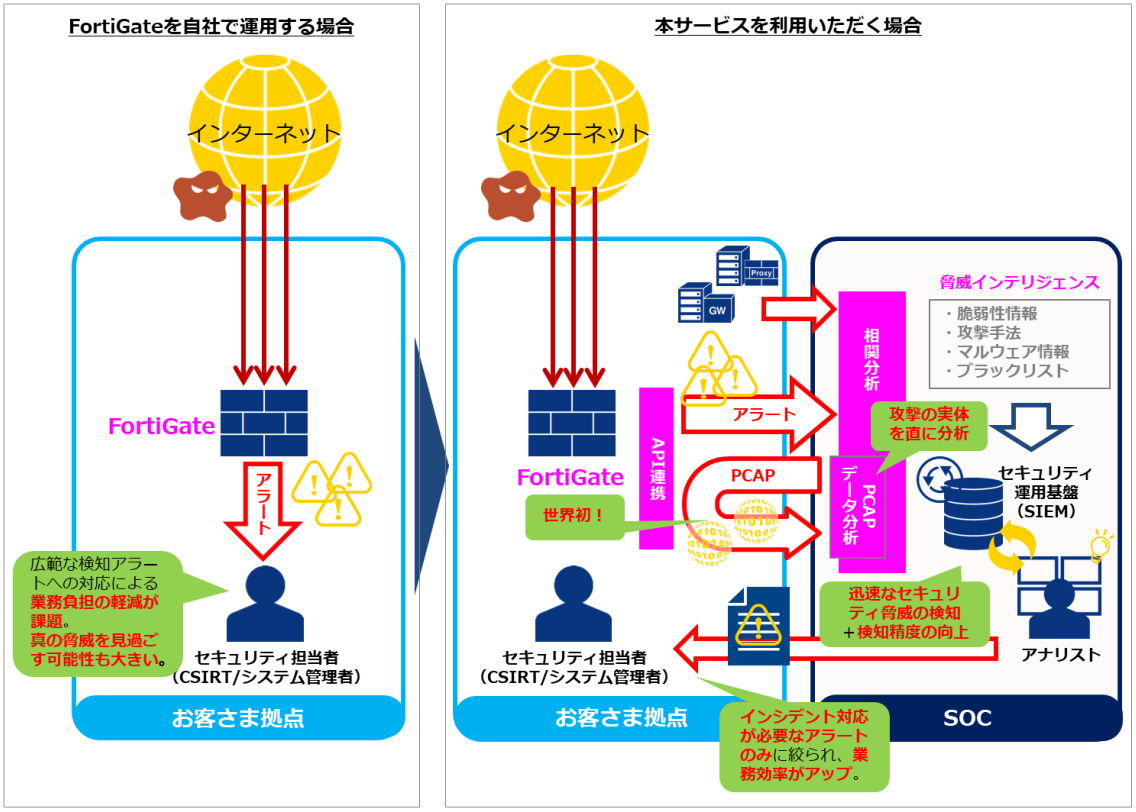
本サービスは、Fortinet との共同開発により、FortiGate において、アラートの原因となった PCAP データを API 連携にてリアルタイムに確認できます。これにより、サイバー攻撃の実体を直に分析し、サイバー攻撃の成否や内容の詳細な把握が可能となります。FortiGate の幅広い検知力と SOC の脅威インテリジェンス※7 を融合させ、セキュリティ脅威検知の迅速化と精度向上を実現します。

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation Public Relations Office
〒100-8019　東京都千代田区大手町 2-3-1　大手町プレイスウエストタワー
OTEMACHI PLACE WEST TOWER 2-3-1 Otemachi, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

（2）機器単体では特定できないサイバー攻撃を相関分析により検知

巧妙なサイバー攻撃では、ICT 機器単体では脅威の特定が困難なケースがあり、複数の機器やアラートを複合的に分析する SOC の相関分析が効果的です。セキュリティアプライアンスの出荷台数で世界をリードする FortiGate において、相関分析を実現することで、より多くのお客さまに、他のセキュリティ機器を含めた全体的なセキュリティレベルの向上が可能となります。

<利用イメージ>



4. 提供範囲および提供開始日

2019 年 3 月 28 日より日本国内で提供開始

5. 利用料金

個別見積りにつき、詳しくは営業担当者までお問い合わせください。

6. フォーティネットジャパン株式会社　社長執行役員　久保田　則夫氏からのコメント

このたびの NTT Com による FortiGate を活用したマネージドセキュリティサービスの発表を心より歓迎します。デジタルトランスフォーメーションが進む中で、「攻め」の投資に見合った「守り」の投資も必要と考えます。NTT Com のセキュリティ高度分析サービスにおいて、世界および日本でセキュリティアプライアンスの出荷台数でシェア No.1[※8] を誇る FortiGate をフル活用するための開発を共同で成しえたのは、近年の巧妙化するサイバー脅威への対策を

より多くの企業に提供できる点で大変有意義なことだと思います。

Fortinet では脅威の状況や対策を調査・研究する FortiGuard Labs という機関を通して最新の情報を世界に発信しておりますが、今後も「革新性・高性能・簡易性・統合性」というミッションのキーワードにそって、使いやすく効果の高い製品作りに取り組み、NTT Com とともにお客さまのセキュリティ対策をサポートしていきます。

※1：「UTM」は、「Unified Threat Management」（統合脅威管理）の略。UTM 機器の略称としても使われる。ファイアウォールや VPN、ウイルス対策、不正侵入検知・防御（IDS/IPS）、Web コンテンツフィルタリングといったネットワークセキュリティに必要な機能が一通り実装されています。

※2：「IDS」は、「Intrusion Detection System」（不正侵入検知システム）の略。サーバーやネットワークの外部との通信を監視し、攻撃や侵入の試みなど不正なアクセスを検知して管理者に通報するシステムです。

※3：「IPS」は、「Intrusion Prevention System」（不正侵入防御システム）の略。サーバーやネットワークの外部との通信を監視し、侵入の試みなど不正なアクセスを検知する IDS の機能に加えて、攻撃を未然に防ぐシステムです。

※4：「WAF」は、「Web Application Firewall」（Web アプリケーションファイアウォール）の略。Web サーバーとインターネットなどの外部ネットワークとの間に設置され、サーバーへのアクセスを監視し、攻撃とみなされるアクセスパターンを検知するとブロックするシステムです。

※5：「PCAP」は、「packet capture」（パケットキャプチャ）の略。通信回線を流れるパケットを捕獲（キャプチャ）して中身を表示したり解析・集計などを行うことです。「PCAP データ」は、パケットキャプチャによって取得されたデータのことです。

※6：当社調べ

※7：脅威インテリジェンス（Threat Intelligence：スレットインテリジェンス）は、脅威の防止や検知に利用できる情報の総称です。脅威インテリジェンスの活用によって、従来のセキュリティ対策では見逃されていた高度なサイバー攻撃の検知、特定の業界・業種を標的とした巧妙なサイバー攻撃の防御が可能となります。

※8：出典 IDC’s Worldwide Quarterly Security Appliance Tracker – 2018Q4（出荷台数）

（別紙） WideAngle マネージドセキュリティサービス サービスメニュー

サービス	サービスメニュー	メニュー	提供機能
マネージドセキュリティサービス	ネットワークセキュリティ	ファイアウォール	• ファイアウォール
		IPS/IDS	• IPS/IDS
		ネットワークセキュリティ基本パック	• ファイアウォール • IPS/IDS
	コンテンツセキュリティ	コンテンツセキュリティ基本パック	• ファイアウォール • IPS/IDS • E-mail/Webアンチウイルス
		コンテンツセキュリティ拡張Aパック	• 基本パックの各提供機能 • URLフィルタリング
		コンテンツセキュリティ拡張Bパック	• 拡張Aパックの各提供機能 • アプリケーションフィルタリング • サンドボックス
		WAF	• Webアプリケーションファイアウォール
	リアルタイムマルウェア検知	RTMD ONSITE	• サンドボックス (Web/E-mail/マネジメント)
		Cloud base RTMD	• サンドボックス (Web/E-mail)
	エンドポイントセキュリティ	EDR	
		プロアクティブ レスポンス for SD-LAN	
	プロキシー分析		
	クラウドGWセキュリティ	WSS 基本パック	• コンテンツフィルタリング • Webアンチウイルス
		WSS RTMDパック	• 基本パックの各提供機能 • サンドボックス
	スレットインテリンジェンス	Active Blacklist Threat Intelligence (ABTI)	

サポートデバイスに
FortiGateを追加