人手での対応は限界、5G時代のサイバー攻撃対策に「自動化」が必要な理由

企業にとって喫緊の課題は、サイバー攻撃対策だ。IoT（Internet of Things）デバイスの普及など、あらゆるモノがネットワークに接続する世界では、1つの脆弱性放置が企業の信頼と業績を失墜させることもある。A10ネットワークスは、今後の在るべきセキュリティ対策をテーマにしたカンファレンス「A10 Forum 2018」を開催。そのもようをダイジェストで紹介する。

年率平均2桁成長を維持するこれだけの理由

セキュリティの脅威が急速に高まっている。2016年にはマルウェアによる623 GbpsものDDoS攻撃が発生。欧州や北米などで極めて広範に主要なインターネットサービスが停止した事件は記憶に新しい。

A10ネットワークス 日本法人代表
兼 社長
米国本社バイスプレジデント 兼務
川口亨 氏

加えて、ITとビジネスとの密連携が進むことも相まって、セキュリティ脅威は企業経営に直接的、かつ甚大な打撃を与えるまでになった。脅威がECサイトで顕在化すれば、そこでの収益機会は根こそぎ奪われる。他システムでも業務停止は免れない。

こうした状況にあって、ネットワークのセキュリティと利便性を担保するさまざまなソリューションをフルラインナップで提供し、国内での存在感を増しているのがA10ネットワークスである。

同社ではDDoS防御やSSL可視化のための「Thunder TPS／SSLi」や、広範囲なセキュリティや負荷分散、大規模NAT（ネットワークアドレス変換）のための「Thunder CFW／ADC／CGN」といったアプライアンス群を提供している。

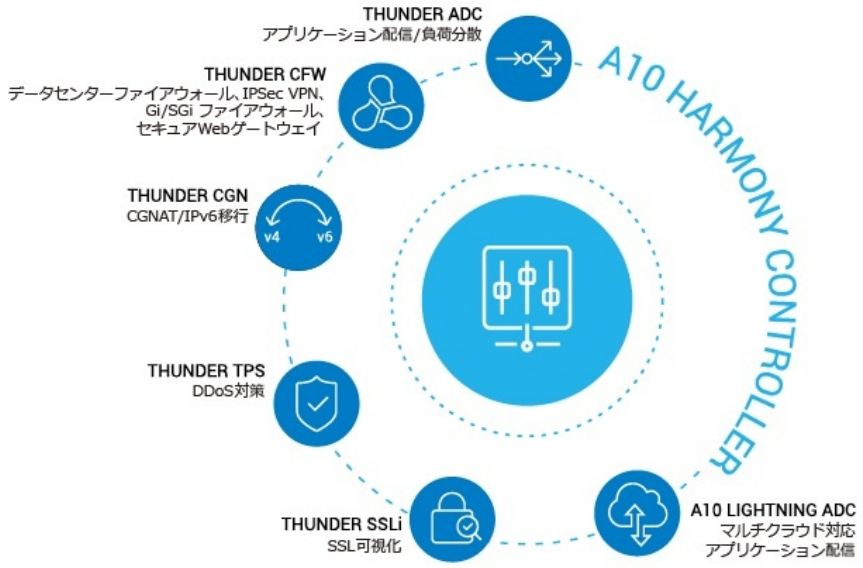
その高い処理性能とともに、「クラウドやオンプレミスを問わない」あらゆる環境下での、「アプライアンスからコンテナまで」の実装手法による柔軟性や拡張性、さらにライセンス形態の多様さが支持を集め、ネットワーク品質や要件にとりわけシビアな大企業を中心にユーザーのすそ野を拡大させてきた。

「我々のビジネスはグローバルで年率平均14%増の成長を続けています。中でも伸びが成長著しいのが日本です。国内のIT投資が総じて軟調にありながら、売上高は年率平均2桁増で推移しています。新規ユーザーも大手を中心に毎年約160社のペースで増加し、累計ですでに1000社を超えるほどです」ーー。A10ネットワークス 日本法

関連コンテンツ


人手での対応は限界、5G時代のサイバー攻撃対策に「自動化」が必要な理由

人代表兼社長 米国本社バイスプレジデント 兼務の川口亨氏は好調な業績を強調する。



アプリケーションサービスゲートウェイ A10 Thunder シリーズ

インテリジェントオートメーション（IA）による自律学習で人手の作業リスクを一掃

海外に目を転じれば、評価の高さは一層際立つ。同社製品を採用するサービスプロバイダーは250社を突破した。クラウド大手のマイクロソフトも「Microsoft Azure」の保護のために、Thunder TPS（大規模DDoS防御専用アプライアンス）を採用しており、グローバルに展開する40ものデータセンターに導入済みである。またこれに加えて、最近ではDNSサービスを保護／拡張する「ノンストップDNSソリューション」も採用している。

A10ネットワークス 創業者 兼 CEO
Lee Chen氏

そんなA10ネットワークスは現在、セキュリティと利便性のさらなる向上に向けた新たなアプローチを推し進めている。それが、運用の「インテリジェントなオートメーション化」を目指す「IA（Intelligent Automation）」だ。

そして、その柱となる製品としてA10ネットワークス 創業者兼CEOのLee Chen氏が披露したのが、機械学習を活用した分析基盤の「Harmony Controller」だ。

Chen氏によると、同社のソリューション群は機能面ですでに群を抜くレベルにありながら、こと設定や設計などの運用面では他社製品と同様の課題が残されていたという。

「その根底にあるのは、人手の作業でミスは避けられないという残念な事実です。そ

のため、いくら製品やサービスが優れていても、運用フェーズで漏れが生じがちとなる状況を避けては通れなかったのです」とChen氏は打ち明ける。

対して、Harmony Controllerは、ADCやCGNなどのフロントソリューションで生じたあらゆるログを自動的に集約／分析した結果をフィードバックする（図1）。

図1：A10ネットワークスのソリューション

これにより、トラフィックの可視化や制御／対策の自動化を実現することで、設定や容量設計にまつわる人手作業のミスによるリスクを一掃。加えて、コンソールの一元化などによるソリューション群の統合を通じて、ネットワークの柔軟性や利便性が飛躍的に向上できるのだ。

「トラフィックを基に攻撃を学習して自律的な各種サービスの保護につなげる、これがIAで我々が目指す世界なのです」とChen氏は力を込める。

今のセキュリティでは5G／IoT対応に不十分

無論、既存ソリューションの強化／拡充にも余念がない。2018年の第4四半期に提供予定の「One-DDoSプロテクション」では、Thunder ADC／CGN／CFWの全てにDDoS攻撃検知機能を搭載するという。

A10ネットワークス
ワールドワイドマーケティング担当
副社長
Gunter Reiss氏

「これにより純然たるDDoS攻撃だけでなく、アプリケーションやLANなどに対する多様な攻撃への迅速な対応も実現され、ネットワークの効率的かつ効果的な保護も可能になります」（Chen氏）

また、2016年に日本でも提供を開始した「Thunder CFW」ではファイアウォールやサーバー負荷分散、SSL可視化、CGNATなどの機能を1つのアプライアンスで実現する。さらにOffice 365を最適化するクラウドプロキシなどを包含した高い機能性

が評価され、今年度上期で対前年同期比130%の売上増を記録しているという。

その上で、Chen氏が今後の注力を表明した技術領域が、ビジネス創造／革新や、社会システムの最適化で今後の急速な利用拡大が確実視されている5GとIoTだ。

A10ネットワークス ワールドワイドマーケティング担当副社長のGunter Reiss氏によると、その普及の兆しは産業界や政府の取り組みなどですでに顕在化しているという。

実際に、自動車業界の破壊的なイノベーションである自動運転技術では、ソフトウェアとIoT機器の塊となった自動車の制御基盤として、5Gが不可欠な存在という。

他業界でも、製造現場の高度化を皮切りに、多様な機器や場所に埋め込まれたIoT機器の制御による製品やサービスの高度化が進められている。同時に、通信業界ではすでに5GがWi-Fiに取って代わりつつある。

こうした動きを踏まえ、同社はこの4月に大容量ファイアウォールや大規模NAT、アプリケーションデリバリーコントローラー（ADC）によるトラフィックステアリング機能などを統合することにより、通信事業者の5G、IoT対応を支援する『5G Gi-LANソリューション』を発表。「すでに韓国の大手モバイルキャリアに採用されています」とChen氏は5Gでの実績を説明する。

5G普及による攻撃の凶悪化にIAで備えを！

もっとも、「5GとIoTの普及は、セキュリティリスクのさらなる増大も招きかねません」とReiss氏。IoTデバイスの普及は、DDoS攻撃の発生源の増加も意味し、5Gによる通信の広帯域化によって、攻撃データの飛躍的な増大も容易に予想される。

「IoTデバイスの普及により、2030年には攻撃者のツールとして『武器化』される可能性があるデバイスが1250億に達すると見込まれます。この2年でDDoS攻撃は4倍に増えましたが、今後のデバイスの急増を勘案すれば、攻撃の規模はそれとは比較にならないほど拡大すると見て間違いありません」（Reiss氏）

しかも、アプリへの攻撃や複数の手口を組み合わせた攻撃など、「攻撃の複雑化に伴い、対応も込み入らざるを得ない」（Reiss氏）という状況だ。A10ネットワークスがIAを推し進める狙いは、まさにその点への迅速かつ的確な対応にあるという（図2）。

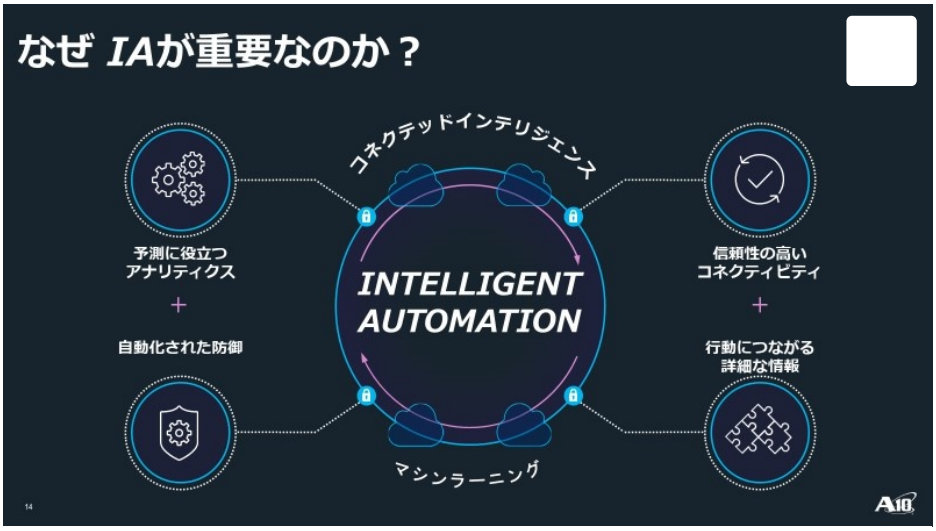


図2：A10ネットワークスがIAを推し進める狙い

「攻撃がいつ起こり、どう防御したのか。IAによりポイントソリューションを統合し一元管理することで、集約したデータを基に攻撃と防御が可視化され、レポート作成も自動化されます。かつ、機械学習による各種のログ分析などを通じ、ネットワーク全体における対応までの時間と精度を向上でき、得られた知見から将来を予測し、ポリシーの設定にまでつなげられます。これも一重に、ソリューション同士をIAでつなぎ、連携させたからこそ可能なことなのです」（Reiss氏）

そのための専門家を同社ではグローバルに配置。攻撃方法や攻撃対象などのデータを基にセキュリティマップを常時、更新するとともに、機械学習による分析結果を管理ツールのaGalaxyや分析基盤のHarmony Controllerに転送する取り組みにつなげている。

こうした仕組みをより広く展開することで、セキュリティの脅威を社会全体で抑え込むことが可能となる。その実現に向けReiss氏が期待を寄せるのが、同社の多様なパートナーだ。

ノンストップDNSソリューションのユーザーであるマイクロソフトもその1社だが、エリクソンやNEC、テクノロジーパートナーにはシスコシステムズやヴイエムウェアなど、錚々（そうそう）たる企業がパートナーに名を連ねる。

「ポリシー設定などの自動化を目指すためには、クラウドやSDN、DevOpsなどでの各種技術との連携も不可欠です。そこで、HCI（Hyper-Converged Infrastructure）分野ではニュータニックスやレノボ、自動化分野ではオープンソースの構成管理ツール Ansibleを展開するレッドハットなど、技術の進化に応じてパートナーを拡大しており、今後もその方針は変わりません」（Reiss氏）

5GとIoTデバイスの普及で、ネットワークの利用環境は大きく異なるだろう。その際にIAが大きな意味を果たすのは間違いない。A10のセキュリティソリューションは今後、サイバー攻撃に対する重要な役割を担うはずだ。