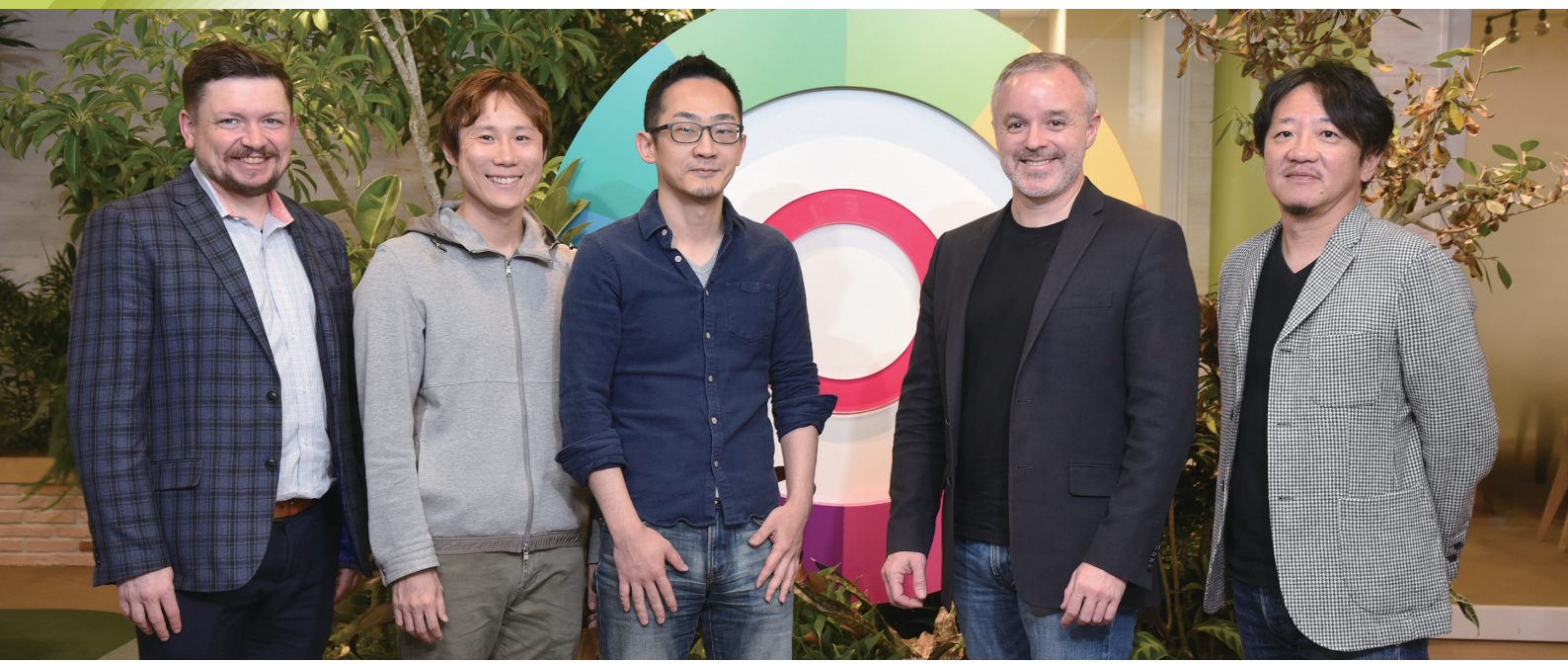
“ネットワークを記録する” Verizon NDRと
“物言うSOC” パロンゴManaged SOCで得られたメリット

ゲーム会社のアカツキが「Verizon NDR」を導入し、「きちんと活用できた」理由



モバイルゲームを中心に幅広いエンターテインメント事業を手がけるアカツキでは、「Verizon Network Detection and Response（Verizon NDR）」とパロンゴManaged SOCサービスを2018年に導入した。パブリッククラウド上のゲームサービス用プラットフォームから、海外子会社を含む社内の業務システムまで自社のITネットワーク全体を、パロンゴのフルタイムサポートを受けながらVerizon NDRで監視している。アカツキでCTO/CISOを務める田中勇輔氏と、同社 Corporate ITチーム マネージャーでセキュリティ専任部署の現場指揮も執る徳山文晟氏に、その背景を詳しく聞いた。

インシデント調査のために導入、「わずか2分」で異常通信を検知

アカツキは2010年、モバイルゲームの開発と運営からスタートした会社だ。現在も同社ビジネスの主軸はモバイルゲーム事業であり、オリジナルのゲームタイトルに加えて、複数の大手ゲーム会社と共同開発したゲームタイトルでもヒットを連発している。また同社のゲームは海外でも人気が高く、台湾にはゲーム事業の子会社を設けている。

ただしアカツキの事業フィールドは “デジタル” だけではない。ビジネスのもうひとつの柱として、“リアル” のエンターテインメントを提供するライブエクスペエンス事業も展開している。たとえばアウトドアレジャーの予約サイト、サバイバルゲームフィールドの運営、オーダーメイドパーティの企画運営サービスなどだ。2019年3月には、横浜駅直通の複合型体験エンターテインメントビル「アソビル」もオープンさせた。

「ハートドリブンな世界へ」――。そんな企業ビジョンを持つアカツキがVerizon NDRを導入したのは、

「Verizon Network Detection and Response（Verizon NDR）」のダッシュボード画面

2018年夏のこと。ただしそれは、セキュリティインシデントの発生という苦い体験がきっかけだった。マルウェアが社内に侵入し、社外との通信を行っていることが確認されたのだ。

アカツキ社内ではすぐにインシデント対応委員会が組成され、田中氏、徳山氏もそこに加わった。対応委員会が中心となって、迅速にインシデントの原因や影響範囲を調査する必要がある。しかし、当時のアカツキにはインシデントの原因や攻撃の詳細を究明する経験値がなかった。

「何か異常が起きていることはわかったのですが、どこにどんな原因があるのか、その先をどう調査すればよいのか、われわれにはわかりませんでした。そのとき、以前試用したことがあったVerizon NDRのことを思い出したのです」（徳山氏）

アカツキではその2年ほど前に一度、パロンゴからVerizon NDRの紹介を受け、PoC（実証導入）を実施していた。そのときは特に異常は見られず、導入を見送っていたものの、接続されたPCやサーバーのネットワーク上の挙動を詳細かつわかりやすく可視化できるという製品の特徴は理解していた。

今回のインシデントについて、Verizon NDRならば何かわかるのではないか。そこですぐにパロンゴに連絡を取り、トライアル導入のかたちでインシデント調査を始めた。

「その効果はすぐに表れました。Verizon NDRを入れてわずか2分ほどで、怪しい通信が発生している端末を発見できたのです」（徳山氏）

Verizon NDRが発見したこの情報を足がかりに調査を進め、最終的には社内にカスタムマルウェアが侵入していたこと、その侵入経路はおそらく社員宛てのフィッシングメールであること、また通信先のC2サーバーなどの脅威情報から、ある有名攻撃グループの関与が疑われることなどが判明した。

インシデント対策委員会ではこの調査結果から、部分的な対応ではなく社内IT環境の刷新が必要であると判断。業務PCやネットワークの全面的な入れ替えを行い、完全にクリーンな環境を取り戻すことに成功した。

「もしもこのときVerizon NDRを入れていなければ、原因や影響範囲が特定できず、社内IT環境の刷新という大きな決断はできなかったと思います。部分的な対処にとどまって、その結果、今でも脅威にさらされ続けていたかもしれません」（田中氏）

アカツキではこの一件をきっかけに、セキュリティを維持するためにはネットワークの継続的な監視に加え、事後調査もできる手段を備えることが必要だと考え、そのままVerizon NDRとパロンゴManaged SOCの正式導入を決めた。社内の組織体制も見直し、田中氏がCISOに着任するとともに、SOC/CSIRTチームも設置して徳山氏が現場指揮を執ることにした。

調査にはパロンゴも参加、専門的な知見提供で迅速な対応へ

上述したインシデント調査にはパロンゴも参加し、セキュリティ専門家としての知見に基づいて、攻撃手法から考えられる攻撃者グループの実像や、予想される影響範囲などをアドバイスした。それに加えて米国VerizonのSOCチームからも、Verizon NDRが収集したデータに基づくレポートが提出された。

田中氏は、インシデントの調査や対応を進めるうえで、こうした専門的な知見が「非常に役立った」と振り返る。

パロンゴ CEOの近藤氏は、アカツキの調査に取りかかってすぐ、それがよく知られた攻撃者グループによるものだと予想したという。こうした攻撃者グループは、特定のターゲット業種に対して一斉に、共通する攻撃手法を用いて攻撃キャンペーンを仕掛ける。すでに同業種の顧客から攻撃の情報を得ていた近藤氏は、攻撃者の手口や狙いも容易に想定できた。

またVerizon側でも、グローバルレベルで多くの顧客企業から攻撃の情報を収集し、そこから最新の脅威インテリジェンスを構築している。元ProtectWise CTOで、現在はVerizonのグローバルセキュリティプロダクト担当ディレクターを務めるEugine Stevens氏、Verizon NDR担当シニアマネージャーのDavid Gold氏は、「このインシデントは日本のエンターテインメント業界を専門に狙う攻撃者グループによるものだった」と説明する。

「Verizonはグローバルのあらゆる地域で、広範な業界のお客様企業に対してSOCサービスを提供しています。そこで得られたデータから、世界のどこで、どんな業界に対して攻撃が発生しているのかを俯瞰し、脅威インテリジェンスを提供できます。これはお客様単独の情報ではわからないことですから、大きなメリットです」（パロンゴ 近藤氏）

また、Verizon NDRは過去のトラフィック情報も蓄積する仕組みなので、新たに見つかった攻撃の情報（ゼロデイ攻撃のインディケーター）を使い、過去にさかのぼって攻撃の発生時点を検出することもできる。「いつから攻撃が始まったのかという情報は、リスク管理上で有益です」と、近藤氏は説明する。

良い製品を「活用」するには“物言うSOC”が必要だった

前述のとおり、アカツキでは現在、社内ネットワーク（福岡や台湾の子会社を含む）や、ゲームサービスプラットフォームを支えるパブリッククラウドの管理レイヤーネットワークにVerizon NDRのセンサーを導入し、サーバーやPC、モバイルデバイスなどの異常なふるまいを早期に検知できる体制を整えている。すべてのパケット情報を収集／蓄積しているため、リアルタイムに異常を検知するだけでなく、過去にさかのぼってその端末がどんな通信をしていたのかを詳細に調査できる点も強みだ。

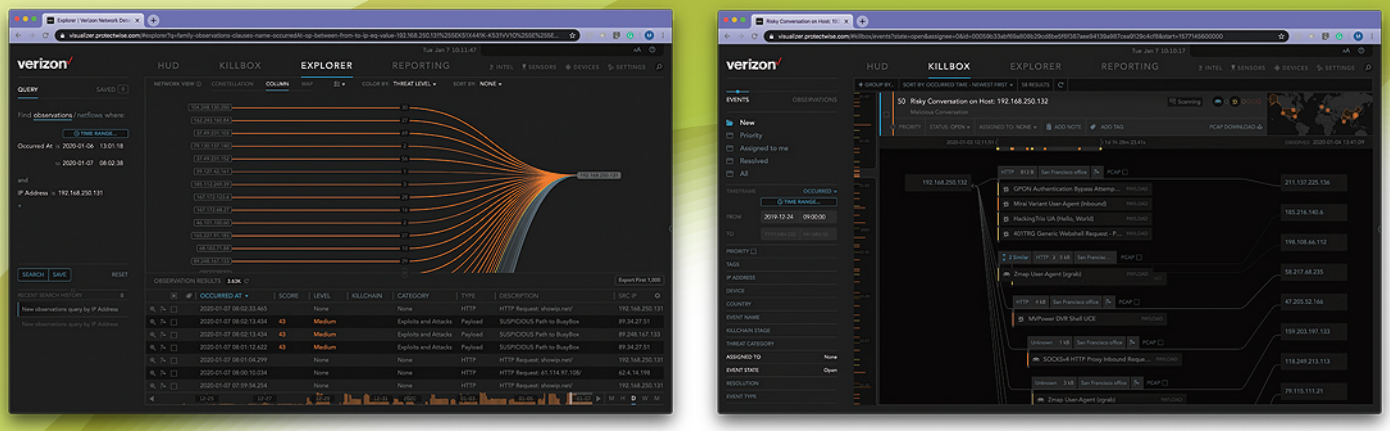
ただし田中氏は、プロダクトの機能や品質も大切だが、運用するうえで最も重要になるのは「密なコミュニケーションが取れる、良いパートナーが見つかるかどうか」だと語る。現場を率いる徳山氏もそれに同意し、次のように説明する。

「当時は社内に専門家がいなかったので、Verizon NDRが異常なふるまいを検知してアラートを上げたとしても、その重要度がどの程度なのか、どう対処すればよいのか、われわれだけでは判断できませんでした。そこをパロンゴのManaged SOCが補ってくれたことで、きちんと『活用できている』実感が生まれました」（徳山氏）

アカツキの場合、Verizon NDRが発するアラートは徳山氏らセキュリティ専任部署が監視しているが、そのアラートについて何か対応を行うべきかどうかの判断（トリアージ）はパロンゴ側に任せているという。

アカツキ CTO／CISOの田中勇輔氏

アカツキ Corporate ITチーム マネージャーの徳山文晟氏



Verizon NDRのデモ画面。すべてのパケット情報から「ネットワークで何が起きたか／起きているか」をわかりやすくビジュアライズする

「Slackにアラートが上がったら、そのままSlackでパロンゴさんの判断を待つ感じですね。対応すべきかどうか、たいていは数分程度でトリアージ結果の連絡が来ます。ほとんどは『対応の必要なし』と判断されますから業務負担は少ないですし、緊急の対応が必要な場合でも、何をすべきか具体的に指示してもらえるので助かります」（徳山氏）

パロンゴの近藤氏は、Managed SOCのサービスでは顧客企業に対して“物言うSOC”であることを心がけていると話す。単にアラートが出たことを通知するだけでなく、対応が必要かどうか、対応が必要ならば何をすべきなのかまでを積極的に発言するスタンスだ。田中氏は、こうした専門的な知見の共有は顧客側としても有益だと考えている。

「重要度の高いアラートだけを知らせてくれるタイプのSOCサービスもあり、それを必要とする企業もあると思います。ただし、それだけだとこちら側に専門的な知見がたまりません。アカツキとしては“物言うSOC”のほうがありがたいですね」（田中氏）

今後の期待は自動化機能の拡充、そして「顧客を増やすこと」？

Verizon NDRの良い点について、田中氏、徳山氏は、ビジュアライズや検索の機能が強力であることを挙げた。たとえば怪しいふるまいを繰り返す端末は自動的にピックアップされ、その端末が過去にどの端末と、どんな通信をしていたかもわかりやすく可視化できる。

VerizonのStevens氏は、まさにそれがVerizon NDRの開発コンセプトであることを説明した。ネットワーク上のふるまいを過去にさかのぼって調査するためには、強力な検索機能に加えて「大量の情報を整理して伝える、ビジュアライズの能力も欠かせないからだ」と強調する。

それでは今後、ユーザーとしてVerizon NDRにどんな進化を求めるか。田中氏は、ファイアウォールやIDS／IPSといった他のセキュリティ機器とのAPI連携を強化してほしいと語る。具体的には、Verizon NDRが発見した高リスク端末の通信を、そうした機器で自動ブロックできるような仕組みだ。現状でもいくつかのセキュリティオーケストレーター製品（SOAR）とAPIを介して実現できるが、API連携は今後もさらに拡充を図りたいとStevens氏は答えた。

また徳山氏は、EDR（Endpoint Detection and Response）セキュリティとの連携強化を挙げた。Verizon NDRはネットワークの視点から、EDRは個々のエンドポイントの視点から、それぞれふるまいを監視している。それらの情報をより統合的に見ることができれば、不審な端末が検知された場合のトリアージやインシデント調査に役立つはずだ。

一方で、パロンゴのManaged SOCに期待することはあるだろうか。田中氏は「お客さんをさらに増やすこと」だと語り、笑った。

「パロンゴさんにはさらにお客さんを増やして、そこで情報収集した他業界での脅威の傾向などもぜひ教えてほしいと思っています。もちろん、Verizonとの連携で得られる海外、アジア地域での動向もですね。これからも良きパートナー、“物言うSOC”として、密なコミュニケーションをお願いしたいと考えています」（田中氏）

お問い合わせ

PARONGO — internet security company —
株式会社パロンゴ
https://www.parongo.com/
info@parongo.com

※このパンフレットは(株)角川アスキー総合研究所のニュースサイト「ASCII.jp」に掲載された記事を再編集したものです。