PRESS RELEASE

報道関係各位

デジタルアーツコンサルティング株式会社

デジタルアーツコンサルティング、NATO主要諸国の国防関連重要インフラ防衛等軍事関連の顧客を担当するNozomi Networksの専門家にサイバー防衛とOT/IoTに関するインタビューを実施

Nozomi Networksに聞くーサイバー防衛とOT/IoTセキュリティ

2022年2月24日にロシアがウクライナに侵攻して1年以上戦闘の舞台は地上だけでなく、サイバー空間でも繰り広げられていると言われています。特に、ウクライナの重要インフラに対するDDoSからはじまり、やがてエネルギー企業の産業制御システム（OT）が標的となり、大規模停電を誘発する事となりました。また、ウクライナ軍のドローン攻撃は日本でも頻繁に報道され、有事におけるその効果は周知のところとなっています。［1］

現在、日本は宇宙・サイバー・電磁波といった新領域を含み、防衛力の抜本的強化に向けて取り組んでおり、今回のロシアのウクライナ進行を受けて、OT/IOTのセキュリティ対策の重要性は国防という観点でも一層重要性が増していると言えるでしょう。
防衛力の抜本的強化を目指す日本は何が必要なのかを睨みつつ、EU兼NATO諸国およびアメリカへのロシアからのサイバー攻撃、並びにそれらの国が防衛としてOT/IOTのサイバーセキュリティにどのように取り組んでいるのかに関して、Nozomi Networksの専門家にインタビューを実施しました。

【Interviewee Profile | Nozomi Networks】

名前：Bill Aubin：VP of Federal Sales
・VP of Federal Sales
経歴：
Nozomi Networksの米国連邦ビジネスチームを先頭に立ちチームを率いている。過去には、サイバーセキュリティソリューションベンダであるImperva、HyTrust、Exabeamでの上級役職の経験があり、米国政府のセキュリティプログラムやセキュリティ規制に深い知識を持つ。また、アメリカ空軍での経験があり、米国政府にサービスを提供するIT企業の副社長役を務めてきた経歴を持つ。
出典：Nozomi Networks Inc.

名前：Michael Dugent
・IoT Sales Director
経歴：
Nozomi NetworksのIoTビジネス開発を先導している。過去にはICS（Industrial Control System)スタートアップ企業のIndustrial Defender並びにLockheed Martinの商用サイバーセキュリティ部門、そしてイスラエルの行動分析スタートアップFortscaleでの上級役職を含む、ICSおよびIoTサイバーセキュリティの背景を持つ。Nozomi Networksの導入プロジェクトを含み、多くの現場プロジェクトの監督を担当し、ICSおよび

IoTサイバーセキュリティの第一線で多くの経験もつ。
出典：Nozomi Networks Inc.

【INTERVIEW】

- ロシアによるウクライナ侵攻で展開されるサイバー攻撃

荒川素年：
2022年2月にロシアがウクライナへの軍事侵攻を開始してから、すでに1年以上が過ぎています。軍事進攻の裏側で、両陣営からサイバー攻撃が行われているとニュースで大きく報じられており、ウクライナの重要インフラへの攻撃があったと報道がありました。専門家の目には今回のサイバー攻撃はどのように映ったのでしょうか。
Michael Dugent：
ロシアによるサイバー攻撃の状況をより深く理解するためには、ロシアの行動をさらに遡って探るとよいです。具体的には、2008年のロシアによるジョージアへの侵攻、並びに2014年のロシアのクリミアへの進出などのロシアによる敵対行動が開始された以降で、いくつかのサイバー攻撃の事例が知られていると思います。これは2014年から2015年にかけて、重要なインフラを標的としたサイバー攻撃が東ヨーロッパでいくつか確認され、各国は対応が必要となりました。また、ウクライナ首都であるキーウの電力網に対するサイバー攻撃は大規模な停電を引き起こしたのですが、過去の事例を念頭に置くとウクライナの電力網へのサイバー攻撃は東ヨーロッパにおける重要インフラへの攻撃の一部だとみることができると思います。
2022年2月にロシアによる新たな侵攻が始まった際、サイバーセキュリティの専門家たちはウクライナおよび周辺地域でのサイバー攻撃の大幅な増加を確実に予見していました。しかし、実際はウクライナおよび東ヨーロッパ全体のサイバー防御の能力と成熟度が大幅に向上した結果として、予想されていたような攻撃は発生しませんでした。これは私たちNozomi Networksや他の専門家が予想していたものとは大きく異なりました。もちろん、私たちが把握できない何らかのサイバーインシデントがロシアによる侵攻の準備段階や実際の進行の最中に起こっていた可能性はあります。また、もし多くの攻撃の試みがあったとしても、ウクライナのサイバー防御力やそれを支援する同盟国の力により、サイバー攻撃を制御できたとすれば、詳細は公にされることはない可能性があります。しかしながら、サイバー活動の急増を念頭に考えると、2022年のロシアによる敵対行動の開始時に類似した状況は見られませんでした。

- NATO主要諸国におけるサイバー防衛対策

荒川素年：
ウクライナや東ヨーロッパでは過去の教訓から、着実にサイバーセキュリティ対策が実施されてきた可能性があると理解しました。防衛という意味では、ウクライナで発生した事例を他国事ではなく私事としてとらえ、着実にサイバーセキュリティ対策を講じることが重要だと思います。一方、ヨーロッパ全体で考えるとヨーロッパ連合(EU)や北大西洋条約機構(NATO)といった組織がありますが、それぞれではどのようなサイバーセキュリティ対策の取り組みがなされているのでしょうか。
Michael Dugent：
各国はそれぞれ独自のサイバー防御能力を保有しています。一方でサイバーセキュリティはNATO（北大

西洋条約機構）の重要な使命の一部でもあります。また、NATO非加盟国およびスイスのような中立国も含め、国家とNATOは一定程度のサイバーセキュリティに関して連携が行われています。NATOは積極的にサイバー防御の訓練を行っており、物理的な戦争演習と同等の重要性を持つものとして位置づけています。

荒川素年：

一方、アメリカにおいては重要インフラへのサイバー攻撃が大きなニュースとなりました。アメリカでは重要インフラに対するサイバー攻撃に対して、国家としてどのようなサイバーセキュリティ対策の取り組みがなされているのでしょうか。

Bill Aubin：

コロニアルパイプライン社がランサムウェア攻撃を受け、1週間にわたって操業停止に追い込まれた事件をきっかけに、アメリカでは重要インフラのサイバーセキュリティの重要性に対する認識が変わりました。2023年３月２日にバイデン政権は国家におけるサイバーセキュリティ戦略として５つの柱を掲げており、その柱の一つが「重要インフラの防衛」です。また、アメリカでは2022年度のNDAA（国防権限法：National Defense Authorization Act）の第1505条で、重要インフラのセキュリティ対策が国防総省の最優先事項となり、ネットワーク上のデバイスの可視化、脆弱性管理、継続的な監視と脅威検出が強調されています。

- Nozomi Networksに対するサイバー防衛需要の高まり

荒川素年：

政府、重要インフラ、軍隊などをお客様としているお二方は、2022年のロシアによる侵攻が始まって以降、Nozomi Networksのソリューションに関する問い合わせで何か気が付いたことはありますでしょうか。

Michael Dugent：

ロシアの侵攻が始まると、サイバーセキュリティ技術への需要が急増したことを確認しました。また、Nozomi Networksはウクライナの防衛を支援するために、すべてのNozomi Networksソフトウェアをウクライナ政府およびウクライナの重要なインフラ機関に無償で提供しました。また、他のヨーロッパの国々、特に東ヨーロッパの国々から大きな関心が示されました。Nozomi Networksは、東ヨーロッパの国々の防衛を最優先とし、利益追求よりも優先して彼らにできる限りのことをしました。これらの行動は、我々Nozomi Networksのミッションの一部として行われたものです。

当初の焦点は東ヨーロッパの政府とヨーロッパにおける重要インフラでしたが、その後、重要インフラやデータセンターなどに対するサイバーセキュリティ技術への需要が急激に高まりました。これらはすべて、Nozomi Networksが特に優れた能力を持っている分野です。また、今後数年間では、我々はさまざまなヨーロッパの軍と共同で、数々の大規模な国家防衛に不可欠な重要な環境に関連した様々なプロジェクトに取り組む予定です。

荒川素年：

お客様からはどんな要望があり、Nozomi Networksのソリューションに対する反応はどのようなものがありましたか。

Michael Dugent：

軍事関係のお客様からの要望の一つの例として、データセンターに関するものがあります。

軍事組織も他の産業と同様に、デジタル化が進む中で安全なデータ処理が重要となっています。しかし、政府を含めた多くの組織はクラウドサービスプロバイダーに完全に依存することはできず、自己所有

のデータセンターを持っています。
彼らの多くはインターネットトラフィックに対するサイバーセキュリティを有していますが、それだけでなく消火システムや冷却システムのセキュリティならびに、物理的なセキュリティシステムなどの側面も考慮に入れる必要があります。こうした領域において、私たちNozomi Networksのテクノロジーはソリューションを通じて支援を提供することができます。
Bill Aubin：
技術面の話をするとNozomi Networksは、ディープパケットインスペクション、機械学習、AIを使用することで、通常多くの人員を必要とする作業を簡略化できます。
Nozomi NetworksのソリューションであるGuardianをインストールすると、Guardianがアセットを評価し、セキュリティの脆弱性を把握し、正常なステータスと異常なステータスを学習した機械学習プロファイルが作成されます。プロファイル作成後、継続監視モードに移行されます。通常多くの人員が必要となる作業をGuardianに置き換えることで、施設内の熟練した作業者をセキュリティオペレーションセンターに集中させることができます。このアプローチはサイバーセキュリティにとどまらず、保守および運用の可視化にも関わります。私たちが使用するディープパケットインスペクション技術により、何かしらのシステムが通常のパラメータを超えて動作していることを特定できるので、サイバー攻撃や保守運用上のシステム障害であるかを示すことが可能です。この技術により、潜在的な問題に早急に対処することができ、より深刻な問題に発展する前に対処することが可能になります。Nozomi Networksの競合他社で、私たちと同様にディープパケットインスペクションを実施したり、アセットインテリジェンスを提供したりするものはありません。

荒川素年：
実際にNozomi Networksのソリューションが活躍している政府、軍事、重要社会インフラ関係で紹介できる実例はございますか。
Bill Aubin：
政府や軍事のプロジェクトに関しては公に公開できません。ただNozomi Networksのソリューションはアメリカ政府のペンタゴンが資金提供するサイバーセキュリティのプログラムであるMOSAICS(More Situational Awareness For Industrial Control Systems)でアーキテクチャの一部として選ばれています。Nozomi Networksは競合他社とのテストの結果、このプログラムに選ばれました。

・MOSAICSとは
国防総省（Department of Defense、DOD）による取り組みであり、サイバー攻撃などの非物理的攻撃に対して、制御システムの状況把握能力を向上させ、対応能力を実証することを目指したプロジェクトです。このプロジェクトのシステムアーキテクチャでは公共インフラの制御プロセスを管理するために使用されるネットワークへのサイバー攻撃の検出、軽減、回復が組み合わされており、意思決定の支援、分析、可視化、情報共有ツールも利用可能な状態で組み込まれます。Nozomi Networksのソリューションを含め、統合されたツールセットを用いた実証の結果、リアルタイムでサイバーアタックを検出・特定し、自動的なレスポンスと回復を可能にする能力を持つことが確認され、アメリカ海軍でのテストでは、1%未満の誤検知率を実現し、そのMOSAICSの実用性が確認された。[2][3]

かつて、サイバー空間が戦場になるだろう、と言われた時代がありました。ロシアのウクライナ侵攻以降、それはもはや現実（リアル）となっています。そして、サイバー防衛には重要インフラ等のOTという側面と、戦場におけるドローンや統合戦術ネットワークといったIoTの2つの側面を持っていることを認識することになりました。そしてそれらは既に対岸の火事などではなく、我が国においても最も重要な課題の一つとして認識し、取り組むべき時に来ているのではないでしょうか。

【Interviewer Profile /デジタルアーツコンサルティング】

文責：荒川 素年（あらかわ　もととし）
デジタルアーツコンサルティングにおいては、ガバナンス領域からテクノロジー領域まで幅広い案件を担当。アメリカの大学を卒業した背景を持ち、英語力活かし様々なグローバル案件を支援。
過去にはグローバル企業のSOC構築支援から、SIEM構築、情報セキュリティの監査など多くの案件に携わる。また、DACにおいても、サイバーセキュリティソリューションの調査なども担当し、世界中のソリューションに関しても広い知識を持つ。

編集：吉田 卓史（よしだ たくし）
17年間にわたり、一貫してサイバーセキュリティに携わる。ガバナンス構築支援からセキュリティ監査、ソリューション導入等、上流から下流まで幅広い経験を有する。また、複数の企業において、セキュリティのコンサルティングチーム立ち上げを0から担い、数億円の売上規模にまで成長させる。DACにおいても、セキュリティコンサルティングチームの立ち上げを担い、急速なチーム組成、案件受注拡大を行っている。

【参考文献】

[1] “ウクライナ情勢と連動して発生したサイバー攻撃から得るべき教訓.” 第5回 産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化）宇宙産業サブワーキンググループ, July 2022. https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/005_04_02.pdf.
[2] “With Mosaics, Johns Hopkins APL Brings the Future of Industrial Cybersecurity into Focus.” Johns Hopkins University Applied Physics Laboratory, May 4, 2022. https://www.jhuapl.edu/news/news-releases/220405-mosaics-future-ics-cybersecurity.
[3] Parkes, Harley. “More Situational Awareness for Industrial Control Systems (Mosaics ...” Rdp-21, November 2021. https://rdp21.org/wp-content/uploads/2021/11/MOSAICS-JCTD-OVERVIEW-10.19-1.pdf.

デジタルアーツコンサルティング株式会社のプレスリリース一覧
https://prtimes.jp/main/html/searchrlp/company_id/115624

【本件に関する報道関係者からのお問合せ先】
デジタルアーツコンサルティング株式会社
https://con.daj.jp/

CISOサービス事業部　セキュリティソリューショングループ
加藤博文