２０１７年6月２６日
（株）NSD コンサルティング

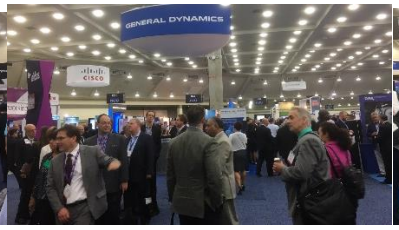
Defensive Cyber Operation Symposium 参加報告

本報告は、Cyber Operation や Cyber 関連ソリューションに興味を持たれる方々の参考のために、株式会社 NSD コンサルティング（代表取締役：早野）が見聞した内容をまとめたものです。

１．概　要

Defensive Cyber Operation Symposium は、AFCEA（軍通信電子協会）が毎年開催する Cyber Operation を中心とした講演と展示会です。昨年はワシントン DC で開催されましたが、本年は 6 月 13 日～15 日にメリーランド州ボルティモアでの開催となりました。講演は DISA 長官兼 JFH-DoDIN 司令官、国防総省 CIO 等の高官によるもの、実務担当者によるもの等が数多く計画されました。

展示会は Cyber 関連事業を営む会社 205 社がブースを構えて、来訪する米軍関係者にアピールをしていました。また、展示会場に 5 つのシアター（「Build」「Operate」「Defend」「Mission Partner」「Cyber Education」）が設けられ、実務担当者によるパネルデスカッションや方針の説明などが行われました。



（写真上は講演・パネルの状況、写真下は展示会場、右はDISA長官と筆者。）

２．講演・パネルデスカッション

主要な講演及びパネルデスカッションは次のとおりです。

○基調講演

LTG Alan R. Lynn, USA　DISA長官兼JFH-DoDIN司令官

Mr. John Scimone, Senior VP and CSO,Dell

Dr. John A. Zangardi,　Acting Department of Defense CIO

○パネルデスカッション

Partnering for Cyber Innovation

DoD Collaboration for Success in Cyber

Readiness in the Cyber Domain : The Fight for Talent and Resources

DISA長官兼JFH-DoDIN司令官のLynn中将の講演では、「スピードとセキュリティの両方が求められている。」と技術の方向性を示しました。また、軍用クラウド（Milcloud 2.0）の構築予算についても触れました。

John Scimone氏の講演（対談）では、企業における脅威の現状、特に内部脅威（Insider Threat）についてかなりの時間が割かれました。

国防総省CIOのZangardi氏の講演では、内部脅威に対応するサイバーセキュリティスコアカード2.0の話題や、Cyberに関する技術と人材の話題にまで及びました。国防総省では報酬の面では民間にかなわない、やはり「使命感と愛国

心に頼るところが大きい。」と認めていました。

Partnering for Cyber Innovation では、「企業がサイバー脅威の情報とインテリジェンスを共有することを躊躇していること、政府と分かち合う必要がある場合には悪化することを躊躇している。」という状況が語られ、業界として国防総省として Cyber イノベーションの促進を妨げるものの除去や考え方について議論が行われました。

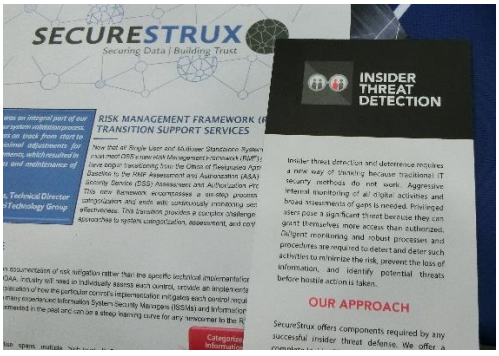
DoD Collaboration for Success in Cyber では、「サイバー戦闘が日常的になり、敵対者をよりよく理解し、異常を迅速に突き止めることができるサイバー戦士を必要としていること。」「サイバーでは機械の速度が必要なこと。」が語られました。また、「真の協力関係が築かれていない。」現状も紹介されました。

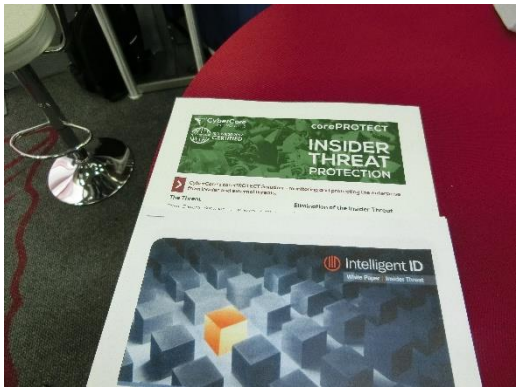
The Fight for Talent and Resources では、「サイバー・ドメインの進化は、指導者が新しい脅威や進化する脅威に対応できるような労働力の訓練と維持を再考する必要があることを意味すること。」「献身的な才能を持つ従業員と幹部との関係を築くという要求と課題」が語られました。また、サイバーコマンド内において、部下との年齢差が大きすぎること「部下の平均年齢が 25 歳」という中で、どのように働かせるかという話も出てきました。

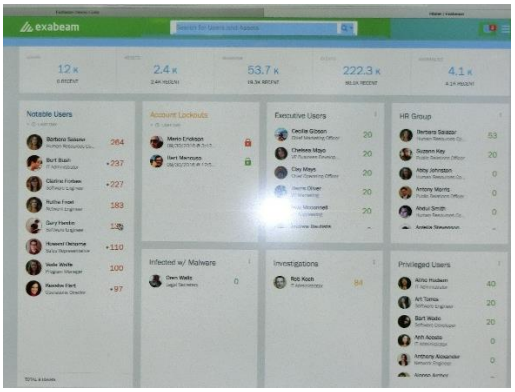
これら基調講演及びパネルデスカッションのうち、DISA 長官兼 JFH-DoDIN 司令官の講演、国防総省 CIO の講演、「DoD Collaboration for Success in Cyber」、「The Fight for Talent and Resources」の４篇は文章化して本報告に添付いたします。（申し訳ありませんが今回は翻訳はいたしませんでした。）

３．展示会

講演でも頻繁に登場した言葉「Insider Threat」に対応するかの如く、展示会場における主要なテーマは、①Insider Threat、②データ保護、③Cyber Intelligence の３点であったと思われます。今までも、AFCEA においては、軍を対象にしていることもあり、Insider Threat（内部脅威）は取り上げられてきていましたが、今回のように展示ブースの多くが Insider Threat 対策を強く打ち出しているのは初めてでした。また防衛大手のノースロップグラマンやゼネラルダイナミックスから従業員５名のベンチャー企業までが展示していました。



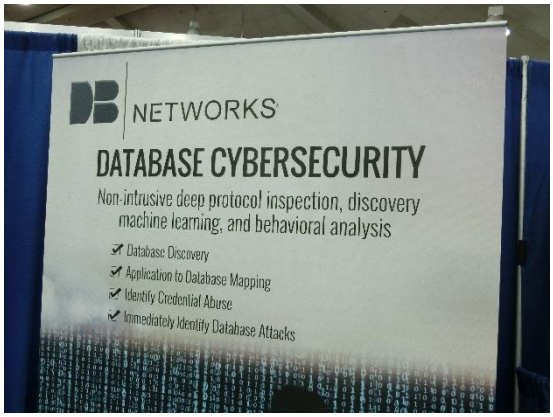




上記写真は①の「Insider Threat」対策を前面に出していたブースの一部です。それら対策の基本は「利用者の行動分析」による「内部脅威可能性の識別」、これらによる「脅威者の排除」と「警告」というソフトウェア的対応でした。ただし、「行動分析」には全て人工知能（AI）技術の適用を行っていました。それぞれの対策技術に一長一短はあるものの、単にシンクライアント（Thin Client）化すれば良いというような解決方法ではなく、システムの可用性の確保とシステムへの負担を軽減しながら、「行動分析」による内部脅威（「小さな正義の告発者」や「内通者」）を事前に特定して、Insider Threat を防止することは共通しているように思えました。さらに AI 技術の発展が加速すれば、このソリューションの競争がさらに激化するものと思われます。

上記写真のように Insider Threat 対策の前段階としてネットワークの「モニタリング」を主要なソリューションとしているブースもありました。「ネットワークマネージメント」という言葉で表現されている場合もありますが、定常時のネットワークのトポロジーを見える化して異常を早く検知し、マルウェアによる内部からの外部 C&C サーバーへの接続を阻止しようとするものも目立ちました。

上記写真は、②「データ保護」を打ち出していたブースの一部です。ランサムウェアを含むデータ及びシステム設定破壊するマルウェアに対抗するため、端末 PC を含むシステム全体のデータを隔離保管するソリューションを出していました。設定データ、ファイル、その他業務上の全てのデータは自動で Cloud 上のデータセンターに格納され、その Cloud は一か所のデータセンターに有る訳ではなく、分散格納されるという全てを破壊されることを避けている構成になっていました。万が一、ランサムウェア等によってローカルデータが破壊されても（利用できなくなっても）Cloud 上のデータセンターからバックアップできるという機能をもっています。AWS（Amazon Web Service）のブースも基本的にシステム全体をこれらのランサムウェアやデータ破壊から守ることを訴えていました。



ユーザーはデータの格納場所を意識することなく、このような専用ソリューションが自動でデータを隔離してくれるという便利な機能を有していました。これらは、外部と接続しているシステムはマルウェアに感染するリスクをゼロには

出来ないという前提に立ち、「リスク移転」による有効な対策として伸びているということでした。

上記写真は③「Cyber Intelligence」を主にアピールしていたブースの一部です。一部のソリューション（右上）では、OSINT の情報を活用し、防護するシステムが何処に繋げられようとしているかを国や都市レベルではなく、サーバーが置かれたビル（建物名）まで特定して表示することも可能なものもありました。

Cyber Command の以前のパネルデスカッションにおいても、Cyber ISR という言葉は一般化しており、敵（Cyber 上の）はどのような攻撃を行ってきたか、何処に拠点を持っていたか、どのような方法を使ったか、様々な情報を得た上で自らの Cyber PPT（Cyber に関連する People・Process・Technologies）を常に変化させるとしていました。関連企業の技術とソリューションはその要望に適合しようとしていることが理解できる展示になっていました。

その他の展示としては、Cyber 教育ビジネスのブースが沢山ありました。

前頁の写真はその一例ですが、沢山のブースが教育ビジネスをアピールしていました。前項に掲載したCyber Rangeの写真は、世界で初めてCyber Rangeを提供した会社のブースです。7つの訓練セルを一度に訓練させることができ、ネットワーク構成も仮想的に様々な状況で作ることができるとともに、訓練チームの練度に合わせてシナリオを簡単に生成できることなどをアピールしていました。また、そのCyber Range（システム）の価格も驚くほど安いものでした。

著者はDISA長官兼JFH-DoDIN司令官のLTG Lynnに展示会場のDISAブースにおいて直接お会いし、「Cyber兵士の能力維持向上はどのようにしているのか？」と質問しました。その答えは、「①民間に預けて教育してもらう。②Cyber Range等を使ってチーム同士の対抗戦を行う。③現場で経験させる。この３つを組み合わせて行っている。」というものでした。また、DoD Directive 8570.1等でIT/Cyber/Securityに関係するCIO/CISO等の配置とその必要資格が規定されていることから、CISSP/CISA/CISMなどの資格教育ビジネスは大きな市場を持っていると言えます。米軍においては、関連する配置（上級者）がこのような資格を有する（一定の知識と能力がある）ことが、Cyber/Security分野においての判断や意思決定の速さ及びリーダーシップを発揮することができる根源になっているとも言えるでしょう。

４．その他

今回のDefensive Cyber Operation Symposiumには、陸上自衛隊から米陸軍Cyber Center of Excellence（Fort Gordon：ジョージア州）に連絡官として派遣されている辻洋平２等陸佐が遠路はるばる参加されていました。また、民間からは株式会社ラックから佐藤雅俊氏（空自出身：前サイバー防衛隊長）及び日立製作所から坪倉恭司氏（海自出身：最終配置C4SC司令）が研修・情報収集のために参加されていました。これら３名の方々は素晴らしい姿勢であると感じました。

このようなイベントは現役の米軍関係者と親しく接する機会があり、関連米国企業の動向が理解できる格好の情報収集と人的コネクション作りができる場でもあります。開催場所に近い所に赴任されている連絡官や防衛駐在官などの皆様が参加されることは、大きな成果を生むものと思います。さらに、日本のIT/Cyber/Security企業は自らの製品や技術が世界的に見てどのレベルかを判定するためにも、是非、出展参加されることを望みます。また、世界で評価されてこそ、防衛省・自衛隊に自信をもって提供できるものと思います。弊社は今後もこのようなイベントに参加して情報や技術を皆様にお届けしたいと思います。