平成２８年４月２８日
（株）NSD コンサルティング

Defensive Cyber Operations Symposium 報告

Defensive Cyber Operations Symposium は AFCEA（Armed Force Communication and Electronics Association）主催により、４月２０日～２２日にワシントン DC のコンベンションセンターに於いて開催されました。本文書は同イベントに参加した株式会社 NSD コンサルティング（早野）の耳目を通じて得た Cyber 関係の米軍及び関係企業の動向等について報告するものです。

１．Defensive Cyber Operations Symposium の概要

本イベントは通常メリーランド州ボルティモア市において５月又は６月に開催されていましたが、昨年４月にボルティモア市で発生した暴動により昨年の開催が１か月順延した経緯もあり、本年については４月という早い時期にワシントン DC において開催されました。

本年は AFCEA 設立７０周年という節目の開催でもあり、実質的に DISA との共同開催に近い形で軍側が大きく関与した内容となりました。軍高官及び著名な民間人の参加者は以下のとおりです。

○LTG Alan R. Lynn, USA（DISA 長官兼 JFHQ-DODIN 司令官）
○Mr. Terry Halvorsen（国防総省 CIO）
○Ms. Margaret Whitman（HP Enterprise　CEO）
○Lt Gen James K. McLaughlin, USAF（米国サイバー軍副司令官）
○VADM Jan E. Tighe, USN（艦隊サイバー軍兼第１０艦隊司令官）

本イベントは主ホールで行われる基調講演及びパネルディスカッションの他、Theater Session と呼ばれる５つの分野毎の報告・教育と展示会で構成されています。Theater Session の５つの分野は次のとおりです。

Theater 1：Cyber Education
Theater 2：Leveraging Technology
Theater 3：Building Economies
Theater 4：Strengthening Practices
Theater 5：Mission Partner

展示会には約２２社のブース及び DISA の大きなエリアが設けられており、来場者数はトータル５０００人～６０００人という大規模なものでした。

２．DISA に関する若干の説明

２０１５年１月に Cyber Command Structure が大きく変革し、DISA（Defense Information Systems Agency）はネットワークとその安全性を保つシステム等を提供する顔と国防総省の情報ネットワークの運用（Cyber 防衛を含む）する顔とで性格を異にすることとなりました。つまり、JFHQ-DODIN（Joint Force Headquarter－DOD Information Networks）の任務を持つこととなり、DISA 長官は JFHQ-DODIN 司令官を兼務することとなりました。DISA における Cyber Operations は２０１８年までに完成する総勢６２００人の Cyber Mission Force（National Mission Teams 13、Cyber Protection Teams 68、Combat Mission Teams 27、Support Teams 25）の態勢が確立する予定です。

したがって、DISA としての指揮系統は DOD CIO に繋がり、JFHQ-DODIN としての指揮系統は US Cyber Command 司令官に繋がっています。彼らは、実際のネットワーク防御を実施しながら、それらに対応するネットワークの構築及び関連技術の開発等を行っています。特に Cyber Operation における関係は別図のとおりです。

３．イベントの細部

（１）基調講演（Keynote）

基調講演は次の方々が実施されました。特に防衛省・自衛隊に役に立つと思われるものについては、翻訳作業中です。

○LTG Lynn, USA（DISA 長官兼 JFHQ-DODIN 司令官）・・翻訳中

○Mr. Halvorsen（国防総省 CIO）・・翻訳中

○Ms. Whitman（HP Enterprise　CEO）

○Mr. Roesch（CISCO Security Business Group VP & Chief Architect）

○VADM Tighe, USN（艦隊サイバー軍兼第１０艦隊司令官）・翻訳中

基調講演に於いては、Cyber War が強調され、その対応の為に産業界との新たなパートナーシップの確立や迅速な対応の為に調達方式の見直しが提言されました。米軍としては、それほどの危機感と独自ではできない技術分野のために協力が欠かせないという表れであると思えました。さらに、米国サイバー軍が昨年６２００人のサイバー対処要員の増員を認められ、全１３３チームの内、準備できたものから逐次 JFHQ-DODIN の指揮下に投入している現状と、その投入が効果的であることが語られました。

DISA 長官の LGN Lynn は、「世界は変わってしまった。Cyber の中は、以前は知能ゲームで、そっと静かに侵入してきたが、今や、ドアをけ破り、掴み取ろうとしている。それは Cyber Warfare であり、毎日、我々のネットワークの中で起こっている。」とも発言しています。

国防総省 CIO の Mr. Halvorsen は「文化の変化について語る時である、Cyber Culture と Tech Culture に関して。」という少し衝撃的な発言もして

います。彼は昨年の本イベントに於いて「国防総省のシステムからパスワードを無くす。」という大胆な提言をしましたが、今回も彼は「Identification」という言葉を使いながら、「CAC カード以上の効果的な認証を早急に導入すべき。」という趣旨の発言をしました。さらに、「Cyber に関して産業界を超えて、国家間の連携を強化するべきである。」とも述べました。

艦隊サイバー軍司令官である VADM Tighe は、「嘗て米軍が享受していた圧倒的な優位性は、ライバル勢力によって危険なほど低下した。特に、二国は重大な脅威をもたらしている。」とし、「ロシア」と「中国」を名指しして「米国に挑戦する脅威である。」との認識を表明しました。また、「我々は日々ネットワークを防衛するために戦っている。日々、彼らの侵攻を阻止するために戦っている。」との「Cyber War」を遂行していることを強調しました。

（２）パネルディスカッション（Panel）

Panel においては、次の内容が行われました。特に防衛省・自衛隊に役立つと思われるものについては、翻訳作業中です。

○Software Defined Everything（産業界による討議）
○DISA Business Enterprise Panel（DISA による諸計画を紹介する内容）
○Services CIO Panel（各軍の CIO 等による討議）・・・翻訳中
○Combatant Command and Joint Collaboration Panel
（Cyber 軍や各統合軍等の J6 等による討議）・・・・・翻訳中

各パネルにおいては、Cyber Operation における現状への厳しい認識が表明されました。特に米空軍副 CIO の Maj. Gen. Finan によれば、「軍務についている者の Cyber Baseline を底上げをしているが、その動きは遅い。敵は我々のループの中にいる。」という情報漏えいに纏わる鋭い分析を表明しました。

現在、IOT（Internet of Things）という言葉が流行っていますが、まさにそのことを捉えたデスカッションとして Software Defined Networks から一歩進んで Everything に変わるという認識が共有されています。DISA の説明資料の中にも、「Software Defined Networks」の「Networks」を赤線で消して「Everything」と書き換えた表現が用いられていました。

（３）Theater Session

分野毎のテーマについては別紙を参考にしてください。同じ時間帯に開催されるので、一つにしか参加できず、また展示会場の視察等もあり参加できたのはほんの一部にすぎません。当該 Session 等で使用されたプレゼン資料内、入手できた全ては別添の CD に格納しましたので、参考にしてください。

私が参加した中で参考となったのは Cyber Education の中の「External Dependencies and Supply Chain Risk Management」でした。（プレゼン資料は CD に格納）

（４）展示会

２２０社もの何等かCyberに係る企業が展示をしているのは相当に大きい展示会であると思われます。昨年のボルティモア市のコンベンションセンターでの展示に比べれば、スペース的に若干狭い印象を受けました。

主な展示を主要なKey Wordを用いて区分すると次のようなものになると思われます。

○内部脅威（Insider Threat）
○認識（Identify）
○一括（Simple）
○教育（Education）
○Big Data

簡単にそれらについて説明を加えます。

ア．内部脅威（Insider Threat）

写真は正にその標語を掲げたLockheed Martin社のブースの様子です。米空軍副CIOの発言にあるように「敵は内部にある。」とは、アメリカ外交公電ウィキリークス流出事件（２０１０年）やスノーデン事件（２０１３年）でも明らかなように、軍内部からの重大な情報流失は権限を持ったオペレータがその権限により入手したデータを内部から持ち出したものです。また、それらを許す倫理感やセキュリティ手順及び保護ツールを早急に改める必要があるとの認識です。

この認識に基づく展示品としては、データ全体を暗号化しておくもの、表示している時は見えていてもデータを何かに格納するときは自動的に暗号化されるもの、データ転送（メールを含め）する際はタイムスタンプや相手先の場所等数種類の特定因子を使って暗号化してマンインミドルによる盗聴を防止するもの等がありました。

写真は、作戦室等や会議室等の密室における情報漏えいリスク防止を上記製品のようなアプリケーション層（プログラム）による防止から、もっと簡単で確実にした物理層でPCと運用者を分離するKVM Extension技術の適用したThinklogical社のブースです。端末PCを全てデータセンター又はサーバールームに隔離することにより内部脅威（データを抜く、データを注入する）を除去し、幾種類もの端末に変化できる仮想端末機能をユーザー側からスイッチを操作することで物理的に連接することで

実現する機能を有しています。スノーデン事件以来、ほぼ全ての Intelligence 機関と全ての統合軍作戦室等で用いられている実績を有しているとのこと。

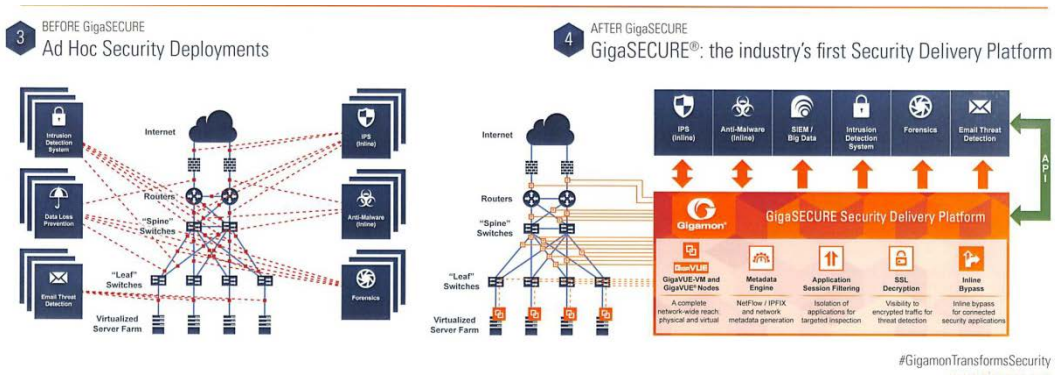
イ．認識（Identify）

Identify を謳った製品等としては、自らの脆弱性の認識を確認する試験を提供するもの、脅威の情報（Cyber Intelligence）や状況（Cyber Common Operational Picture）を表現するもの、自らのデータの書き込みや書き出しの状況を確認できるもの、リアルタイムログ分析で不正なことが起きていないかを確認できるもの等がありました。写真はそれらの一部です。

ウ．一括（Simple）

米海軍省 CIO の Mr. Robert Foster によれば、米海軍の IT 予算は全予算の４．７％凡そ８０００億円であり、その内、運用経費が６８００億円、新規議場への投資は１２００億円と制限があるとのことです。（２月の WEST における発言）今回も、CIO Panel で同様の発言がありました。このように日本に比べたら大きい予算ではあるものの、彼らにとってはかなり制限を受けている新規投資予算との認識です。

サイバーセキュリティに至っては、様々なセキュリティソリューションが複雑にネットワークに接続され、まるでタコ足配線のようになった状態が通常であり、そのためセキュリティは高コストであるとの認識があります。今回の展示ではそれら一連のサイバーセキュリティ製品を一括したトータル製品を提供しているブースが多くありました。このことによりコストパフォーマンスの高いサイバーセキュリティを実現し、予算の適正化を図ることを後押ししているようでした。図はその一例です。



エ．教育（Education）

写真は見事にその必要性を訴えたブースです。パネルディスカッションで発言があったように、「敵は内部ループにある。」と言う表現は、内部犯行の

みならず、知識不足による間違いであったり、ルール違反であったりということも指しているものであると思います。教育ビジネスは本当に多くの企業が参入しており、大きな変わらない市場と言えるでしょう。また、DISA 自身もそのビジネスを行っているようです。

オ．Big Data

外部からの攻撃（或いは侵入）を防止し、阻止するには現状の分析が必須であり、データセンター化やクラウドサービス化が進んでいる米軍に於いては、それらシステムのログデータだけでも膨大なものになります。前年の本イベントにおける主要メッセージは正に Big Data でしたが、今年も変わらず Big Data は主要展示でもありました。写真は Ciena 社のコンテナ型データセンターが展示されているものです。

4．DCOS2016 で見える現状と方向性

（1）米軍は Cyber War を戦っている。

JFHQ-DODIN 司令官の LTG Lynn、国防総省 CIO の Mr. Halvosen、艦隊サイバー軍司令官の VADM Tighe、其々が発言しているように、「We are at War today in Cyber」として米軍は Cyber War を現に戦っていること。そしてその敵（増大する脅威）は「ロシア」と「中国」とする認識であること。米軍はこの戦いを勝ち抜くために、全力を投入する意思を感じることができました。

昨年から US Cyber Command においては、「Information Assurance」から「Mission Assurance」へという標語が提起され、現在、各軍の Cyber Command 及び IT やネットワークシステムを開発整備する部門や System Command などでは当然のこととなっていました。正に全ての戦いに勝つという目的の達成に寄与するためにこそ、「Assurance」はあるべきであるということと思われます。

そのために、様々な変革を構想していることが垣間見えてきました。Cyber と Intelligence を組み合わせ、市場として膨大な空間を創造し、産業界等を取り込んで、新たな協力関係の構築と、迅速さを要求される技術や製品の適用を進めるために調達のルールについても変革を迫ることを訴えているようでした。

（２）識別（資産とリスク）とリスク管理手法が行われている。

２月に行われた WEST でも報告しましたが、米軍（国防総省）は秘密の認識が適切にできており、COTS ハードウェアや COTS ソフトウェア及び計画の現状や不具合、今後の予定等については関連産業界にはオープンにされており、その結果、既存企業だけではなく様々な企業からより良い提案を受けることができる態勢となっていました。この流れは本イベントでも変わることなく、現在の計画の状況や今後の計画等が惜しげもなく披露されていました。これは、秘密の指定は実世界（Real World）の実データ（Real Data）、クリティカルな性能値であるということの認識ができている査証であると思われます。

Cyber Security と言うと、自らのネットワークやシステムの運用を含めた環境とそこで扱われる守るべき資産を評価せずに、一般的に考えられるものは予算の許す限り全て導入することを行いがちです。守るべき資産(データ)がどの程度の価値があって、何処に所在するのか、誰がその資産（データ）を何処で、どのように使っているか。そして、そのプロセスにおいて何処にどのようなリスクが存在し、それらのリスクはリスク管理の考え方の下で、「回避」できるか、「移転」できるか、「低減」できるか、そして漏えいや破壊等の被害に対してどこまで「許容」できるか。という評価とリスク管理の考え方が良く理解されていると感じることができました。この考え方によって、適切な方策を自ら評価して導入する自信ということも感じることができました。（例えば、DISA は６５００人の技術者と１５００人の軍人で構成され、其々のポストでは IT/ICT の明確な資格が要求されています。）

（３）調達手法で手詰まり感も見える。

国防総省 CIO の Mr. Halvosen も発言したように「The pace of change in cyber is what makes it different from every other war.」という変化するスピードに大きな違いがあります。最も効率の良い適切な技術を相手が対応できないうちに投入する必要がありますが、調達に於いてはルールによる制限があるようです。思うようには早いスピードで投入することができないことや同等機能で安い価格での調達（LPTA）が技術的に適切でないこともあるようである。パネルディスカッションや質問でも指摘等が行われていました。彼ら自身の焦りも感じられるものでした。

HP Enterprise CEO の MS. Whitman は「We have to change the way procurement is done. Government is losing out on the best of industry.」という言葉を用いて、調達改革を訴えていました。

（４）JFHQ-DODIN 運用への自信の表明

JFHQ-DODIN が発足してまだ１５カ月しか経っていないが、指揮官である LTG Lynn はその効用に強い自信を漲らせていました。Cyber Operation に関しては直接的に US Cyber Command の指揮を受ける統合実動部隊であ

り、最も大切な国防総省のネットワーク（NIPRNet/SIPRNet を含む全て）上でCyber Warを戦う部隊として今までのDISAのネットワーク運用部門にはない性格と Cyber 要員の増員をされています。各陸海空軍のコンポーネント毎に個別に行うのではなく、「海軍基地に空軍兵のサイバー要員がいる。」というような表現まで使って、当該 Cyber War の分野で統合化を進めるべきであるというメッセージが込められている自信であると思われました。

（５）Software Defined Everything と Simple 化へ

CISCO はハードウェアベースのルーター及びスイッチで世界シェアの約７割を支配していますが、その CISCO さえ、今回は「SDN (Software Defined Networks)」を大々的に展示していました。DISA の発表でも Networks に限らず全てのものを定義するのに Software を使用するという「Software Defined Everything」が表明されていますので、米国における軍民限らずこの方向性に進むものと思われます。

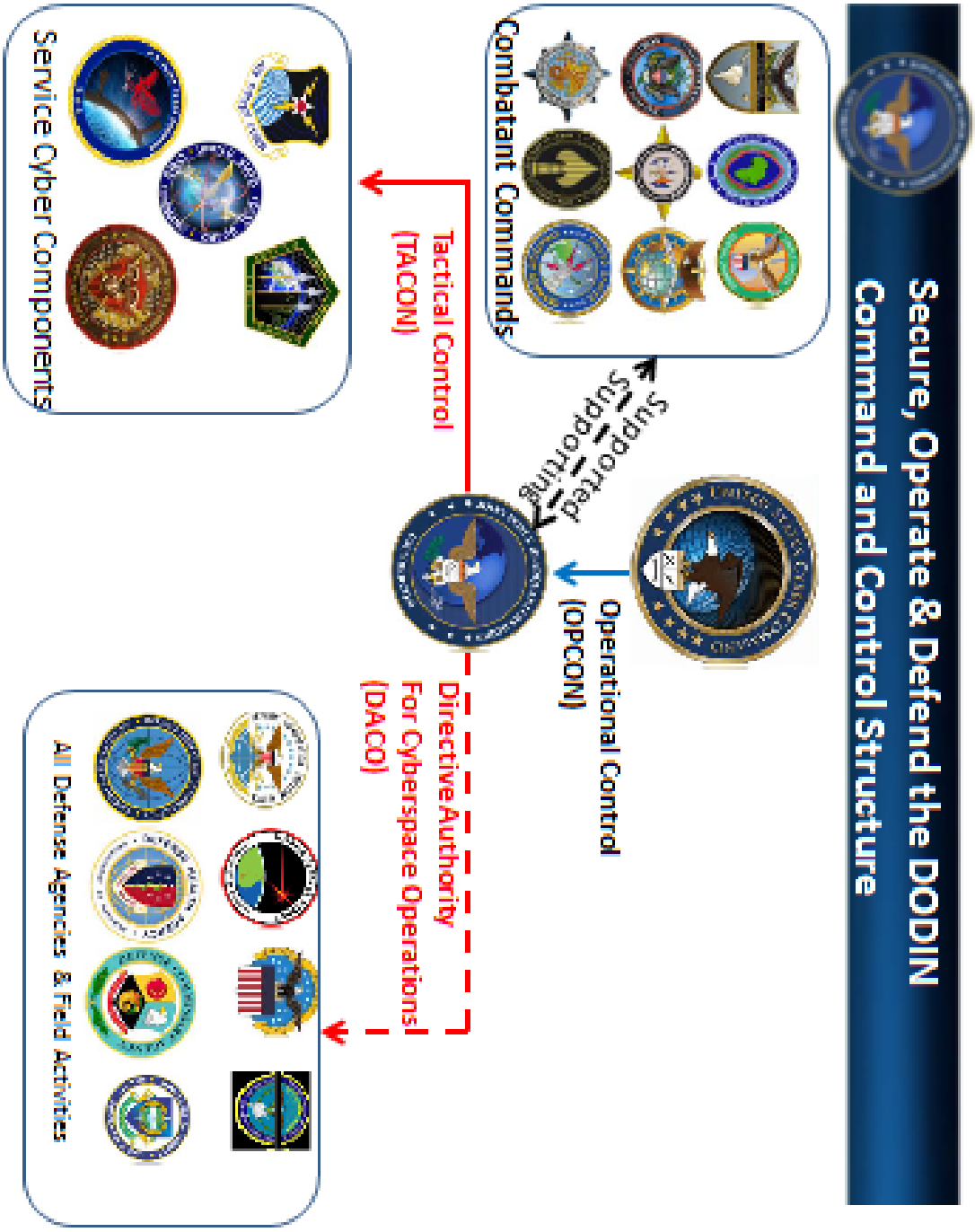
また、既存の Cyber Security の製品群は様々な機能のものを組み合わせて全ての穴を防ぐ「タコ足配線」のような接続をされていましたが、これは費用が掛かり、同じデータを集め重複することのあり、人間の管理能力が追い付かなくなる恐れもあることから、Software Defined Everything が進めば進むほど、一括した Security Solution を提供する製品で Simple 化が進むものと思われます。

５．まとめ

本 Defensive Cyber Operations Symposium では、記載しました Key Word や方向性（現状）などを知る良い機会であったと思います。そして、本イベントでも感じたことですが、軍将官はじめ関係者は関連技術情報に限らず関連情報に良く精通していることです。IT/ICT の関係職位に配置されるには、国防総省の規則によって、その保有する関連資格や経験等が規定されていることは大きいとは思いますが、良く勉強しているという姿に驚かされます。

また、本イベントに限らず、数多くの軍産学のイベントが開催されます。その場は、Keynote、Panel 及び展示会を注意深く見聞することにより、彼らの方向性を探り、彼らの問題点を浮き彫りにし、また新しい技術や製品を見出すチャンスがあるものであると思います。特に駐在官の所在する近くで開催されるイベントには是非積極的に派遣されることをお勧めいたします。もちろん、弊社としては今までどおり防衛省・自衛隊の役に立つ情報の取得と、このような配布に務めてまいりたいと思います。

別　図


Secure, Operate & Defend the DODIN
Command and Control Structure
Combatant Commands
Supported
Supporting
Operational Control
(OPCON)
Tactical Control
(TACON)
Directive Authority
For Cyberspace Operations
(DACO)
Service Cyber Components
All Defense Agencies & Field Activities

別　紙

Theater Session の内容について

Theater　1　：Cyber Education
○External Dependencies and Supply Chain Risk Management
○International Implications of Defensive Cyber Operations
○The Internet of Things (IoT) – A New Frontier in Cybersecurity
○NIST 800 – 171, DFARS, and Contractor Responsibilities for Covered Defense Systems
○CYBER Command and Control：What your data wants you to know

Theater 2：Leveraging Technology
○SATCOM：ASIR, Right Sizing and COMSATCOM
○Secure Host Baseline Windows 10 Migration
○Security Standards：Getting the Protections in Place
○Software Defined Networking
○Cyber Security Range 2.0 Architecture & Capability

Theater 3：Building Economies
○Computing and Cloud Services
○Unified Capabilities and Defense Enterprise Office Solutions
○DoD Mobility
○Managing Risk Through the Cloud Provisional Authorization Process
○Update on Cloud Cyber Defense CONOPS

Theater 4：Strengthening Practices
○Joint Regional Security Stack and Multi – Protocol Label Switching (MPLS)
○NIPRNet/SIPRNet Cyber Security Architecture Review (NSCSAR)
○Cyber Servies
○Big Data Platform (BDP) and Cyber Situational Awareness Analytic Capabilities
○Service Support Environment, Change Configuration and Asset Management Update

Theater 5：Mission Partner
○JFHQ – DODIN
○DISA Small Business Panel
○C2 of DISA's Enterprise
○Mission Partner Engagement Office (MPEO)
○Mission Partner Environment (MPE) Panel