TechNet Asia Pacific 2016 参加報告書

2016.11.21

（株）NSD コンサルティング
代表取締役　早野禎祐

AFCEA TechNet Asia Pacific 2016 に弊社から参加いたしましたので、防衛省の皆様のご参考のために報告書を作成いたしました。

１．概要

AFCEA TechNet Asia Pacific 2016 は１１月１５日～１７日にハワイのホノルルに所在する Hilton Hawaiian Village で開催されました。規模的には昨年よりも一回り小さく、参加高官もハワイ在所の統合・陸・海・空司令官ではなく、副司令官レベルでした。ブース出展企業数も１７３社と昨年よりも２０社ほど少なくなっていました。今回のテーマは「MAXIMIZING COMBINED POWER THROUGH CYBER」であり、パネルディスカッションや基調講演もそのテーマに沿って実施されました。

基調講演は次の方々が実施しました。

○　太平洋艦隊副司令官　Phillip G. Sawyer 海軍少将
○　太平洋海兵隊副司令官　Brian W. Cavanaugh 海兵隊少将
○　ハワイ大学学長　David Lassner 博士
○　Pikey Way 有限責任会社社長　Cindy Moran 女史（元 DISA 副 CIO）
○　国防総省 CIO　Terry Halvorsen 氏・・・・翻訳中

また、パネルディスカッションは次のものが実施されました。

○　International and Interagency Coordination Panel
○　Operational Challenges J2/J3/J5 Panel（非公開）
○　Cybersecurity Panel・・・・翻訳中
○　C4 Capabilities (J6) Panel・・・・翻訳中

日本からの参加はNEC関連会社のC3Iシステムズ社から研修ということで、５名（引率者は、同社戦略アドバイザーの元空自の里村氏）のみであり、ハワイの米軍各司令部におられる自衛隊連絡官からは、航空総隊司令部付で米太平洋空軍 A3/A6 連絡官である小松３空佐（博士及び CISSP 保有者）が昨年に続き参加されていました。日本からのブース展示企業はなく、日本関連企業として米国 NEC（「日本とは別会社です。」とはブース担当者の発言。）、米国日立ケーブルが出展していました。

２．基調講演とパネルの議論の要旨

（１）太平洋海兵隊副司令官講演

「ミッションの成功を得るためには、米軍は、サイバースペースを通じて提供される技術的能力に大きく依存する分散型業務に重点を置かなければならない。」と強調していました。「また、分散型の運用により、よりスマートで効果的な兵器と今後の大きなミッションの成功が可能になる。」と指摘しました。

「センサとして機能する複数のプラットフォームを想像してみてください。陸、海、空、宇宙及びサイバー領域にわたる C4ISR が含まれます。ネットワーク対応のスマートな武器や画像、ビデオ、音声を無人の航空システムや F-35 の高度なネットワークとのアップリンクとダウンリンクでパトロールしている海兵隊員を想像してみてください。」と聴衆に訴えかけ、「無人航空機や F-35 の陸上砲撃調整センターや洋上の兵器調整センターなどのへの長距離ターゲティング施設へのデータダウンリンク」を提案していました。最後に「ロボットと海兵隊員が有人無人のチームに統合されたと想像してください。私はそのすべてを視覚化することができます。」さらに、「海兵隊員は、指揮統制と分散作戦を可能にする技術に興味を持っている。」と話を締めくくりました。

（２）国防総省 CIO 講演

細部は現在翻訳中ですが、彼は主に次の点について強調していました。

A. ハイブリッドクラウド環境の利用について

同氏は、電子メール、チャット、ビデオ、ファイル共有などの一連の基本的なエンタープライズサービスを提供するクラウドソリューションを持つことになると述べました。 「それらはモデル化され、おそらく商用プロバイダと提携するだろう。」と彼は語っていました。

B.　内部脅威について

同氏は内部脅威に関する聴衆からの質問に対し、「内部者によるサイバー脅威に懸念を抱いているが、隊員の自由意思を制限しないように。」とも警告しました。内部脅威については、それが「大きな被害をもたらした」ことを認め、「インサイダーの脅威を調べるために採用しようとしている技術はある」が「私たちは、周りの人が注意を払っていれば、ほとんどの内部脅威が特定できたと言えるでしょう。」として教育の重要性も強調していました。

（3）International and Interagency Coordination Panel

参加者は以下の方々でした。

○　モデレーター

太平洋軍 CIO　 Mr. Randall C. Cieslak

○　パネリスト

太平洋軍　副 DJ4-ILSC　Rory Copinger-Symes 英国海兵隊准将
太平洋軍　国際関与主任　James McAllister 米空軍大佐
アジア太平洋安全保障研究所　教授　William A. Wieninger 博士
国防総省 CFE-DM　部長　Joseph D. Martin 氏
パロアルトネットワーク Japan　松原千穂子氏

主な参加者の発言は次のとおりです。

★太平洋軍 CIO　Randall C. Cieslak 氏：「保護を重視すると、すべての安全対策と管理のためにユーザーにとっては苛立っています。相互運用性はより困難になる。」

★英国海兵隊　Rory Copinger-Symes 准将：「共有された情報、共有されたツールでお互いに信頼できるものでなければ、決して連立して活動するつもりはない。」と述べ、また、「教義、訓練、教育の必要性」を訴えていました。さらに司令部の構造そのものを情報化時代に合わせたものにする必要があると次のように述べました。「司令部のほとんどは、旧プロイセンモデルを中心に設計されています。私は J-6、J-4、J-5 について話しています。私たちがこの新しいサイバー時代に入った今、新しく構造化する必要がある。」

★Joseph Martin 氏：「国防総省の指揮統制システム、通信システムは、データを共有しないように設計されており、他の人々からそのデータを保護する

ように設計されている。」また、最近のニュージーランドの地震の例を引用し、「人道支援のために米空軍が高空から撮影した写真を利用できるように依頼した。データの機密を解除するまでにどれくらいの時間がかかるのか聞いたが、答えはまだ出ていません。」と共有が進まない現実を披露しました。

★William Wieninger 教授：「米国は、しばしばより安全なシステムを構築しようとしているが、実際にはシステムを使用する人々が安全の鍵である。」と語り、「重要な点は、情報を共有するのに十分な信頼感を感じている状況に人々を導くことだ。」と述べました。

（4）Cybersecurity Panel・・・現在翻訳中

参加者は以下の方々でした。

○モデレーター

サイバー軍太平洋軍連絡官　Jody Grady 海軍大佐

○パネリスト

NSA ハワイ技術部長　Robert Runser 氏

ハワイ電力　情報保証部長　Bryan Tepper 氏

海軍太平洋 NCTAMS　CSO　Eric Husher 氏

太平洋軍要求資源部　プロジェクトマネージャー　Ross Roley 氏

太平洋軍サイバー任務保証主任　Trevor Jones 氏

参加者は、共通情報システムまたは産業制御システムに対するサイバー攻撃がより致命的であるかどうかについて議論しました。

主な参加者の発言は次のとおりです。

★太平洋軍 Ross Roley 氏：「産業用制御システムに対する攻撃がより壊　滅的である。」と主張しました。 彼は「油パイプラインバルブが不用意に開いたままになって漏れを引き起こした少なくとも 10 年前の事例を引用しました。この地域で釣りをしている子供たちの一部が、マッチを水の中に投げ入れ 3 人の子供が死亡した。そのような種類の被害を引き起こす情報システムは見られない。」と事例を挙げていました。

★サイバー軍太平洋軍連絡官 Jody Grady 大佐：「状況による。」と反論し、「もしあなたがハッキングした情報システムが、私たちとイラク人の間でモルスルに軍隊が近づくのを手助けするシステムが共有されていれば、彼らの位置は喪失し、ISIL は彼らを襲うために私たちから奪った砲兵を使うことができました。それはかなり致命的だ。」と発言しました。「敵が正確な軍隊の

所在地を取得しなくても、後日致命的となる情報を盗むことができます。私が使っているレーダーの周波数を入手すれば、もし私がラジオで話すのに使う周波数を得るなら、それは致命的になる可能性がある。」と述べました。
★太平洋軍サイバー任務保証主任 Trevor Jones 氏：「すべてのインフラストラクチャと情報コントロールシステムが害を引き起こすような方法で使用されています。」と指摘しました。
★ハワイ電力情報保証部長 Bryan Tepper 氏：「産業用制御システムに対する攻撃が最も致命的である。」ことに同意しました。同氏は、同社のシステムがランサムウェア攻撃のために数日または一週間閉鎖された場合、顧客に請求書を送付し、会社の請求書を払い、通信する能力に影響を及ぼすと述べました。「ここで軍隊は、自力で停電に対処しますが、ほとんどのバックアップシステムはそれほど長時間稼働することができず、それが問題になる可能性があります。」と述べています。
★NSA ハワイ Robert Runser 氏：「情報システムに対する攻撃は戦略的効果をもたらす可能性がある。」と指摘しました。同氏は、ソニー・ピクチャーズ・エンターテイメントに対する攻撃を引用し、辞任と会社再編につながったことを説明しました。「指揮統制について考えるなら、コマンドと制御システムに戦略的効果をもたらす非常に機敏な情報システムがある。それらは人々を殺したり、爆発を起こさないかもしれないが、非常に敏感な時期には重大なリーダーシップを損なう可能性がある。」
★海軍太平洋 NCTAMS Eric Husher 氏：「情報システムと産業制御システムの両方が同時に攻撃される可能性がある。」と述べました。

（細部は、翻訳語関係部署に配布の予定です。）

（５）C4 Capabilities (J6) Panel・・・現在翻訳中
参加者は以下の方々でした。
○モデレーター
太平洋軍 J6　Kathleen M. Creighton 海軍少将
○パネリスト
陸軍 311 通信旅団司令官　Lawrence F. Thoms 陸軍准将
太平洋空軍 A3/A6　Glen M. Genove 空軍大佐
太平洋海兵隊 G6　Joseph A. Matos Ⅲ海兵隊大佐
DISA 太平洋司令官　Joseph E. Delaney 海兵隊大佐
太平洋艦隊 N6　Ruth A. Youngs Lew 女史

参加者は、防衛技術産業に対し任務を達成するために最も必要なものについて語りました。この議論の中には、次世代の認証ツールから航空の指揮統制ネットワークモデリングまでの機能が含まれていました。

米太平洋軍の J6 である Kathleen Creighton 少将は、「任務を達成するために最も必要なもの」について参加者に問いかけたところ、参加者からは次のような意見が出されていました。

★DISA Pacific の司令官 Joseph Delaney 大佐:「シングルサインオン機能と次世代クレデンシャルが必要だ。」と示唆しました。「現在利用可能なものもありますが、ポリシーによって制限されており、引き続き前進するためにはそれを克服するためにあなたの助けが必要です。」とも聴衆に訴えていました。

★太平洋艦隊 Ruth A. Youngs Lew 女史:「傍受される確率が低く、内容検出確率の低いスペクトル管理ツールが必要である。」と述べていました。

★太平洋空軍 Glen Genove 大佐:「次世代衛星通信と高帯域幅だけでなく軽量でもあるその他の伝送経路の次世代技術である保護された通信」を挙げました。

★太平洋海兵隊 Joseph Matos 大佐:「軍隊は、すでに所有している技術をよりよく統合または使用するためのアイデアが必要になることもある。」と付け加えました。彼は HF 波通信を例に挙げて「次の新しいおもちゃを探し出すのではなく、時にはすでに在庫に入っている技術と能力があることがある。」と語りました。

★陸軍 311 通信旅団司令官 Larry Thoms 准将:「すでに利用可能なセンサーデータを理解する必要がある。」と業界の助けを求めていました。

（細部は、翻訳語関係部署に配布の予定です。）

３．展示内容について

今回のテーマに合わせて、コラボレーションツール（会議通信）、大型表示装置、ネットワーク管理ツール、Cyber Security ソリューション、野外（搭載）展開用堅牢型サーバー製品、簡易型通信装置等が１７３社から展示されていました。Northrop Grumman や General Dynamics 等の防衛大手、Hewlett Packard や Dell 等のコンピュータ大手､小さいながら特定分野の専業メーカーが特徴のある展示を行っていました。その中で、報告に値すると思われるものについて記載します。

（１）コラボレーション（会議通信）ツール

以前から自由な会議通信が良好な指揮を可能にするという観点から、各社が展示していましたが、今回は次の２点が興味を引きました。

Ａ．携帯型会議ツール

写真左は、Cisco システムズの携帯型ビデオ会議ツール。同製品は同社の子会社に移管されているが、125kbps でも良好なビデオ映像を送ることができ、接続先の自由な追加が可能な点が評価できます。（ちょうど、内線電話を使っている感覚で操作できます。）ケースは耐ショック処置と防水処置がされており、野外の使用可です。

携帯型ビデオ会議ツールの左の電話は Cisco8865 であり、同電話でビデオ会議通信ができる。（上部に小型カメラがあります。）接続先の追加等の使用感は同様に内線電話を使っているのと変わらない。太平洋軍の軍人から CENTRIX－J にこの電話が使われ始めたとの情報を得ました。

Ｂ．遠隔医療支援用精密映像ツール

遠隔医療支援にビデオ通信を用いるケースは多いが、上の写真はソフトウェアによる映像鮮明化技術を適用した製品です。（IRON BOW 社の製品）右のカメラ（対象物により取り換え可能）で撮影し、専門医のいる左の施設へ伝送した場合に鮮明化処理を行っています。左の写真は腕を右のカメラで撮影して送った（リアルタイム）ものですが、皮膚の皺や体毛が鮮明に映し出されています。HD 程度の映像では 2～５Mbps の通信帯域が確保できれば良いとのことで、これだけの鮮明画像にしては意外と狭帯域でも可能なことが理解できます。

（２）大型表示装置

人間の意思決定には状況認識（Situation Awareness）が必須ですが、如何に状況を表示するかが最後には問われることになります。ハードウェアとしての表示装置やソフトウェアによる制御など、様々な製品群が展示されていました。

A. LED 大型表示装置

上部写真は PLANAR 社（現在は RAYARD 社の傘下）の LED 大型表示装置で、埋め込まれた LED ライトの間隔が非常に小さく、非常にきれいな画像が細かく綺麗に表示できます。上部右写真は同左の裏側ですが、上下左右に４台の小モジュールで構成されています。LED 製品は、振動、衝撃、降水等の悪環境でも使用できることから、価格が安くなれば、今後は艦船内の表示装置として主流を占めることになるかも知れません。

同社の通常型（液晶）大型表示装置は米軍の様々な作戦室等のビデオウォールとして採用されています。発熱部が切り離されていることから、ほとんど壁に直接つける形での設置が可能であり、設置工事費を安く上げることが可能です。

B. ４K ビデオウォール

写真左は Extron 社の４K ビデオウォールです。４K のニーズは UAV のカメラの進化と共に軍内の作戦室や監視室で高まっているとのことであり、他の企業も４K 高精細表示を売り文句にしている展示が目立ちました。

C. ビデオコントローラー

展示では前述の PLANAR 社のビデオコントローラーを使用しているものが多く見かけました。同社のコントローラーは PC の画面操作と同じよ

うに、複数の画面を自由に拡大縮小、配置換え、最大化最小化等がまるでWindows の操作と同様にできることが評価されていると思われました。同等の機能は表示装置のコントローラーメーカーとして名高いハンガリーの DEXON 社の製品のみではないかと思われます。

D. 注意事項（中国資本の会社に関して）

上記で紹介した PLANAR 社（米国）は本年初めに同業種の RAYARD 社（中国資本：本社は北京）に買収され、現在は RAYARD 社の傘下企業となっています。米軍及び米国連邦政府機関では、両社（PLANAR 社も RAYARD 社も）も調達上の規制は TAA（Trade Agreement Act：指定された国での生産品のみを認める規定あり。）により、米国内の工場での生産されたことを証明していることで、以前から RAYARD 社も米軍へ納入しています。PLANAR 社も現在も工場は米国内にあり、部品レベルから生産国等の開示をしていることから米軍の調達も以前と変わることなく続けられています。（上記の解説は米国内の弊社の協力会社の役員（元米海軍軍人）によるものです。）

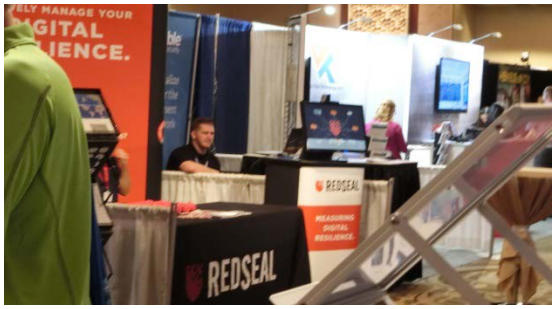
左のマークが付いた製品は TAA に適合していることを証明しています。(国防総省への納入が認められたという証明にもなります。) 中国資本の会社のみならず、中国に大きな工場を持つ DELL 社なども国防総省等への納入は米国または指定国内による生産品としています。（DELL 社の説明）

（３）Cyber Security ソリューション

Cyber Security は TechNet での展示の主流となっています。Symantec や Trend Micro 等専業メーカーとして有名な会社から、防衛大手の Raytheon 社や General Dynamics 社なども Cyber Security に関するもの（サービスを含めて）出展していました。紹介する主要なものとしては、Management 系の Security、民間技術を秘密保持に使う Commercial Solution for Classified（CSFC）と Insider Threat 対策です。

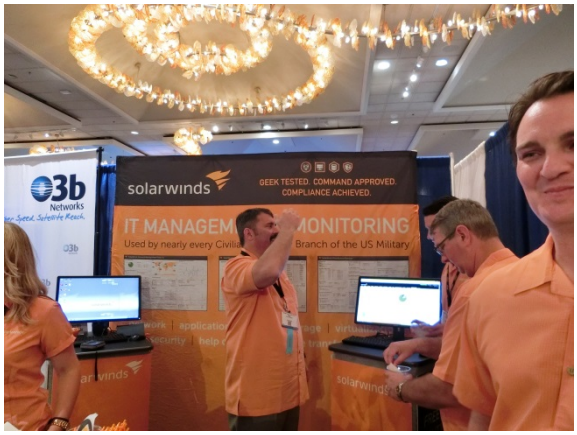
A. Management 系の Security

今回の展示の主流を占めていると思われるのが、この Management 系の Security 製品群であろうと思われました。



左の写真は REDSEAL 社のブースであり、同社の Security Solution はネットワーク内の結合を自動で図式化し、安全上問題のあるルーターの設定を警告することができる機能があります。新規にネットワークに加入する

システムや新設されたビル等のネットワーク加入時などに探索するために導入されるケースが多いようです。通常時はネットワーク内の流れをモニターし、許可されない流れを警告することで安全を保つ機能を持っているとのことです。新規機能として外部から侵入された場合にどのような経路でどこまで辿れるのか（侵入が可能なのか）を検査する機能を追加したと説明していました。同製品は JIE（Joint Information Environment）のセキュリティ機能である JRSS（Joint Regional Security Stack）に採用されているとのことです。



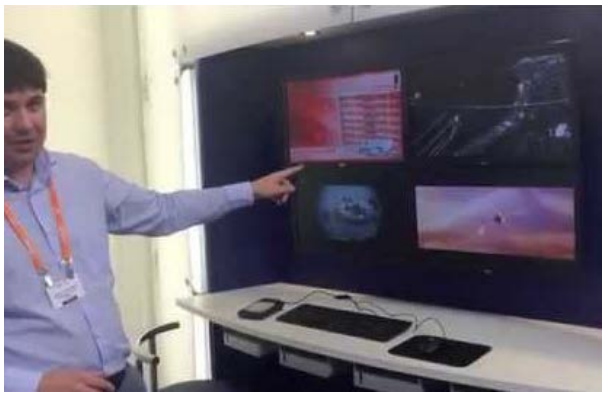
写真左は Solarwind 社のブースです。同社のソリューションは幕のロゴに記載されている MANAGEMENT と MONITORING で成り立っているようです。主は SIEM（Security Information and Event Monitoring）機能であり、セキュリティポリシーの監視と発生するイベント管理をリアルタイムのログ解析を通じて行います。空軍等に強みを持っています。

左の写真は LogRhythm 社のブースで、同社のソリューションも SIEM を主要な機能として展開していました。
他の企業も細かな違いはあるものの、リアルタイムログ分析からセキュリティリスクを低減することを謳っていました。

B. CSFC

General Dynamics のブースに大きく記載された Commercial Solutions for Classified（CSFC）は、軍や政府機関の増大するセキュリティと利便性の両立から、NSA／CSS（中央セキュリティサービス）が商用製品のうち基準を満たしたものを National Security Systems 内で使用することを認めたものです。この基準の適用により、商用製品群によって今までよりも早くシステムやネットワークがユーザーの使用できる環境に届くこととなりました。GD に限らず各社も GOTS の暗号体系や保全基準ではなく、最も近代的な商用ハードウェアおよびソフトウェア技術を即座に使用することができるように、当該分野に力を入れているとのことです。
（上記解説は GD 社の説明によるものです。）

C. Insider Threat 対策と物理的リスク対策

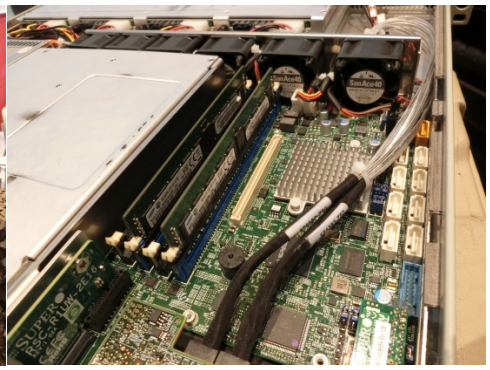


写真左は米国 Thinklogical 社の KVM Extension の展示。同社の技術は PC 操作員の周りから PC 本体をサーバー室に隔離し、必然的にオペレーターによるデータ持ち出しやマルウェア挿入を防止するものです。同時に秘区分の違うシステムも権限のある席においては自由に切り替えて複数のシステムを使うことができる利便性を両立させています。また、PC 本体からオペレーター席への延伸距離は５０マイルまで可能で、遅延と圧縮なしに４K の映像を運べる高い技術があります。同社の製品を展示する東京のデモセンターが豊洲センタービルアネックスの NTT データ内に設置されましたので、東京で体験することができます。

Cyber や Network は見えないものと思いがちですが、実際は光回線や銅線ケースブルによって物理的に繋がれています。左写真はその物理的な回線を構内において物理的に破壊されることの警報を出すために、マンホール等の解放できる所に光回線とセンサーを組み合わせ危険を知らせる警報ネットワークです。このような対策も必要でしょう。

（４）堅牢型サーバー等

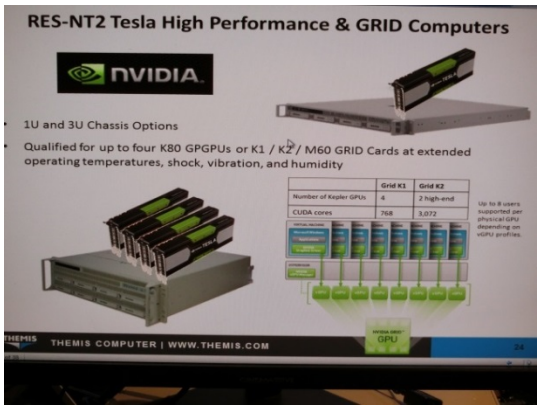
Rugged Server（衝撃、振動、温度などの耐環境性を MIL-SPEC に合致させた堅牢なコンピュータ）の市場は大きく、専業メーカーから HP や DELL などの一般のコンピュータ会社まで、この Rugged Server を展開しています。



上記の写真は Rugged Server 専業メーカーの THEMIS 社の製品の一部と Server 本体の中を覗いたものです。設置場所や要求性能によって様々な品揃えがあります。

この写真は同様の専業メーカーである CRYSTAL 社の Rugged Server と右はそれを陸軍の展開場所における Storage（データの格納場所）として使用した事例（別会社の展示）です。

両社の Rugged Server は、耐衝撃（MIL-STD-901）、耐振動（MIL-STD-810）、耐 EMI（MIL-STD-461：電磁気影響対策）、温度環境（－１５～＋５５C）に適合しており、野外の戦場、航空機内、艦船内、戦闘車両内で稼働できるように保証されています。市場規模が大きいため、種類及び部品在庫も豊富であり、価格も約２００万円台と海上自衛隊艦艇及び P-１哨戒機が搭載している搭載用 COTS コンピューター（MIL-SPEC 適合無し）の半額以下の価格帯となっています。



左写真は THEMIS 社の Server を米海軍 DDG51 の近代化計画としてイージス CIC コンソールとして採用し、仮想化処理により Server は全て Server 室内に集約され、コンソール本体は PC も Server も無く、表示装置（Monitor）と Keyboard、Joystick 等だけで構成された様子を GPU と共に図式化したものです。

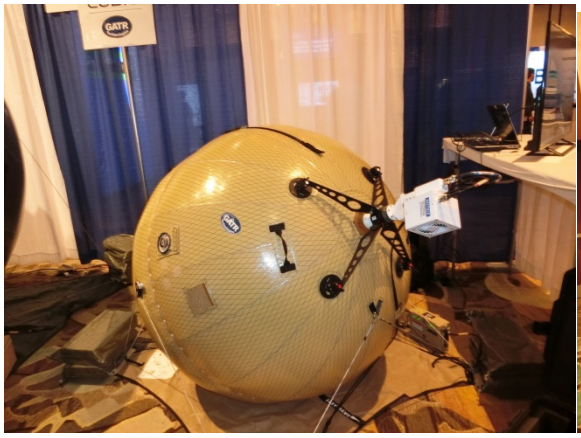
左写真は DELL の Rugged PC です。Server と同様に MIL-SPEC 適合ですが、価格は 4000 ドル～2000 ドルで、Panasonic の Tough Book とほとんど変わりません。市場の大きさで価格が下がることの証左を示しています。

（５）LINK-22 への対応

米海軍の戦術データリンクは LINK-16（UHF 帯域のみ）を使用していますが、NATO では HF 帯域が使用できる LINK-22 を使用しています。相互運用性を担保するために、米海軍も LINK-22 の適用計画を進め、太平洋艦隊の艦船にも LINK-22 対応艦が出現してきます。このため、LINK 支援器材または処理器材についても LINK-22 対応が出てくるという情報でした。

左写真は Ultra Electric 社の ADSI（航自の DC 内や海自 SF 作戦室に設置済み）ですが、来年内には ADSI－LINK-22 対応版をリリーズするとのことでした。今まで CDLMS で行っていた LINK-11／LINK-16 のマルチリンク処理を、この新 ADSI を艦艇に搭載することにより LINK-16／LINK-22 のマルチリンク処理も可能になるかも知れません。

（６）簡易型通信装置



写真はキャリーケース（人が持てる大きさと重さ）に入れて持ち運べる風船型衛星通信アンテナを展開（膨らました）して展示された様子です。

左透視図は同社のパンフによるものですが、風船内の電波反射板の構造が良く理解できます。右に置かれている黒い箱がキャリーケースです。

同アンテナはKu、Ka、C及びXバンド通信に対応できるものです。ケースから取り出して展開する様子は下記のYouTubeのURLでご覧ください。凡そ２０分～３０分で展開可能だそうです。また、同アンテナは防弾仕様になっており、流れ弾によって風船がしぼむことは無いようです。その様子もYouTubeで確認してください。

（展開及び防弾）https://www.youtube.com/watch?v=bQ17RQvKTJg

４．その他

（１）自衛官の参加

今回も参加された自衛官は虚空自衛隊からの連絡官である小松３空佐のみでしたが、せっかく沢山の自衛官が勤務されているハワイですので、是非、このような展示会と講演会を見ていただき、状況などを自衛隊内の関係各部に配信していただくことが望ましいと思います。また、このような沢山の米国を中心とする関係企業が参加していますので、その方々と名刺を交換するだけでも以後の情報交換ができるものと思います。

（２）責任のある者の参加

国際協力を話し合うパネルディスカッションに日本からは民間会社からパネリストとして参加（招待）されていました。他のパネリストが公的な立場（または関係国軍人）を持って発言していましたが、彼女は単なる民間人であり、軍（自衛隊）を代表するものではありません。英国が太平洋軍に勤務する英国海兵隊員（准将）を出しているのと同様に、太平洋軍への連絡官等（１佐クラス）が出演されるのが望ましいものと思います。

もちろん、語学の問題もあり、特定領域の知識の問題もありますが、自衛隊から（または内局から）出演する方が良いと思われます。（彼女の場合は、AFCEA会員でもあり、語学も堪能で、AFCEA International会長のShea退役海兵隊中将と懇意であることから、AFCEA側から依頼しやすかったという事情もあるとは思いますが。）

（３）日本企業の参加

日本企業からもっと沢山来訪して、米国の情報通信関連企業がどのような技術や製品を展示しているのかを確認していただき、国内での開発や改善につなげていただくことが必要であると思います。

弊社は自衛隊に直接情報をお届けして、要求に繋げていただくことを願っているのですが、受け手である日本企業がその内容等が理解できなければ、良いものは作れないと思います。今回、C3Iシステム社から５名の研修員を出されたことに敬意を表したいと思います。

以上