２０１８．１１．２１
（株）NSD コンサルティング

TechNet ASIA-PACIFIC 2018 参加報告

AFCEA（Armed Force Communication Electronic Association）が毎年この時期に開催する TechNet ASIA-PACIFIC 2018 に参加いたしましたので、ご参考のために報告いたします。

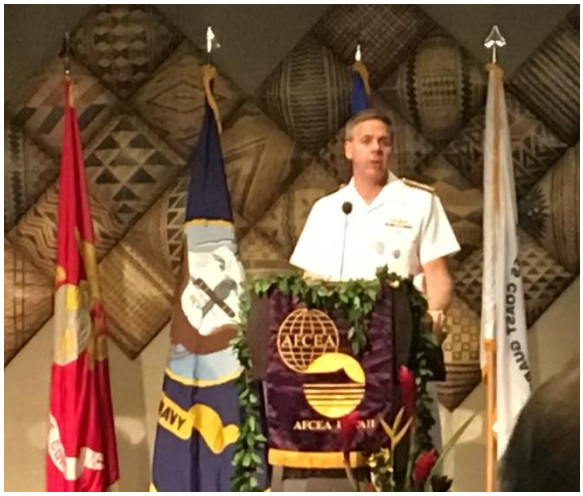
１．概　要

TechNet ASIA-PACIFIC は AFCEA International が毎年この時期に AFCEA ハワイ支部と共に開催している通信・IT・サイバーに関する会議（講演とパネル）及び展示会です。今回は 11 月 13 日（火）～15 日（木）まで、ホノルルのヒルトン・ハワイアン・ビレッジで開催されました。特筆すべきことは DISA（Defense Information System Agency）長官兼 JFHQ-DODIN（Joint Force Headquarter, DoD Information Network）司令官の VADM Nancy Norton が参加されたことです。 このことが象徴するように、主に Cyber Security に主眼が置かれている内容となりました。また、表題に「Sharpening the competitive edge for combined cyber operation」（統合されたサイバーオペレーションの競争力の向上）と名付けられているとおり、様々なパネルディスカッションや展示会においても「統合」「Cyber」を中心にされていました。展示会にブースを設けていた企業は 179 社であり、昨年よりも少しだけ多い展示となりました。

写真上左は開会式の様子、右は展示会場の様子です。

２．講演・パネルディスカッション

（１）インド太平洋軍司令官基調講演



左写真は基調講演をするインド太平洋軍司令官 ADM Philip S. Davidson。彼の講演の要旨は次のとおりです。

①　自由で開かれたインド太平洋の実現のため、我々はあらゆることにチャレンジしている。

②　インド太平洋司令部（INDOPACOM）は、広範囲の責任範囲において「フルスペクトルサイバーオペレーション」を実施する能力と可能な技術を模索している。

③　INDOPACOM で行っていることはすべて、同盟国やパートナーとのシームレスな統合作戦にあり、相互運用性に重点を置く計画的な方法を求めている。

③　サイバースペースの脅威に対処するには、社会全体のアプローチが必要である。指揮官の任務保証は、国のインフラと可用性に大きく依存しており、いずれかを標的とする攻撃は、国家と任務を脅かす可能性が大きくなる。

④　私たちのサイバー上の敵は、電気グリッドを含む重要インフラに浸透し、今後の紛争では、アメリカのエネルギーと生活の神経中心を閉鎖する可能性がある。

（２）Women in AFCEA Panel Session

表題「Women of Government, Industry and Academia Discuss Cyber Security Challenges」（産学官の女性がサイバーセキュリティ活動を語る。）

パネリスト

〇Ms. Linda Newton, former U.S. Pacific Fleet Chief Information Officer

〇Ms. Deborah Golden, Principal, Deloitte & Touche LLC

〇Ms. Ruth Youngs Lew, Principal Executive Officer
Enterprise Information Systems, Department of the Navy

〇Ms. Tracy Fu, National Account Manager, SANS Institute

〇VADM Nancy A. Norton, USN, Director, DISA and Commander, JFHQ-DODIN

このパネルセッションは弊社の米国協力会社である Caribou Technology LLC の Ms. Christina Ward の報告によるものです。主要な論議は次のとおりです。

① サイバーセキュリティはできる限り自動化する必要がある。人に頼らざるを得なければ失敗するだろう。

② 産業界はサイバーセキュリティ革新に大きな役割を果たすが、その製品にサイバーセキュリティをうまく組み込んでいない。

③ セキュリティをシステムの最初から構築することは、私たちができる最も重

要なことである。
④ 原因とその結果から見れば、内部脅威こそが最も大きい脅威である。国防総省もその脅威への確実な対応が必要である。
⑤ 政府から始めて、誰もが情報をより多く共有する必要がある。政府全体で、より良い対応をしなければならない。

（３）J2 Panel Session

表題「Incorporating Cyber into Multi-Domain Operations」(マルチドメイン作戦へのサイバーの組込み)

パネリスト

〇BRIG Colin Karotam, Australian Army, Deputy Director for Intelligence U.S. Indo-Pacific Command
〇COL Jason A. Chung, USA, U.S. Army Pacific, G2
〇Col Andrew J. (A.J.) Moyer, USMC, Marine Corps Forces, Pacific G2
〇Col Michael (Mike) A. Boutet, USAF, Individual Mobilization Augmentee (IMA), Headquarters Pacific Air Forces Command, A3/6 Director of Air and Cyberspace Operations, Joint Base Pearl Harbor-Hickam, Hawaii
〇CAPT Jenna K. Hausvik, USN, Deputy Director, Intelligence and Information Operations Directorate (N2N39), U.S. Pacific Fleet

パネルでの主な発言は次のとおりです。

① サイバーを戦闘乗数（combat multiplier force）として見て、新しい能力と戦法が必要である。これらは既存の指揮統制の中で絡み合っていなければならない。インド太平洋軍の自由で開かれたインド太平洋実現への推進にはサイバースペースが含まれている。
② 強力なサイバー能力は、競合国（中国を念頭に言っていると思われます。）を抑止する。
③ マルチドメイン作戦では、新しい技術の使用が求められている。 弾力性のあるアーキテクチャ上を横断して攻撃（shooters）に直結するセンサを考える。また、マルチドメイン作戦センターの設立を検討したいと思うかもしれない。
④ サイバーに重点を置き過ぎている。サイバー自体が存在している訳ではない。これは広範な情報環境（活動）の一部である。
⑤ 制限された環境での作戦については、実際にそれを訓練するのに十分な時間

を費やしていることを知らない。これについての教訓はない。

⑥ 私たちの最大の課題は、変化への抵抗です。技術革新ではなく、私たちがすでに行っていることに技術を加える方法について考えるべきだ。

（４）Keynote Panel Session

表題「Achieving Cyber Resilience in the INDO-PACIFIC Region」

パネリスト

○Ms. Jodi Ito, Information Security Officer, University of Hawaii

○Mr. Jeff Watkins, Communications Director, Commercial Solutions for Classified, National Security Agency

○VADM Nancy A. Norton, USN, Director, DISA and Commander, JFHQ-DODIN

○Dr. John A. Zangardi, Chief Information Officer, Department of Homeland Security

パネルでの主な発言は次のとおりです。

① 太平洋地域では海底ケーブル、代替は衛星システムです。 これらは、この地域にとって絶対に重要です。さらに、広大な地域でのコミュニケーションの手段として、さらなる手段が必要です。

② 単一区画のみで構成された船は、その中のたった一つの穴が船を沈める。海軍はそのような船は持たない。しかし、私たちは単一区画構成のネットワークを持っています。そこでは、一つの穴がネットワーク全体に穴を開けます。

③ 政府の巨大システムの情報を請負業者、下請け業者、そのサプライヤーに提供すべきではない。

④ フィッシング攻撃は、データ漏洩の大きなドアです。フィッシングは大きな問題であり、そのことを人々に教えることが大切です。

⑤ ハッカーたちは、数年前のような大規模なデータ侵入から得られた情報をLinkedIn などで共有する方がより良くなっている。

⑥ 個人情報を無意識のうちに共有する危険性を認識すべきです。新しいアプリをダウンロードすると、携帯電話のすべての情報にアプリがアクセスすることに同意するのはなぜですか。なぜ携帯電話のカメラにアクセスする必要がありますか。利便性の前にセキュリティを考える必要があります。

⑦ サプライチェーンはますますサイバーセキュリティの問題となっています。誰かがネットワークのサプライチェーンに入ることができれば、そのネットワーク全体を掌握してしまいます。NSA はサプライチェーンマネジメントの問題に対処するために立ち上がっています。それは非常に重要です。
⑧ どのような措置がとられても、脅威は継続する。防御する最善の方法は自らの脆弱性を知ることです。これには、信頼できる真のハッカーの役割が大きい。Red Team（脆弱性を明らかにするために模擬攻撃を加えるチーム）は、システムそのもの、使用する人、その業務プロセスのどこギャップがあるかの発見に効果的です。

（５）J6 Panel Session

表題「Achieving a Free and Open Indo-Pacific Through Combined Cyber Operations」

パネリスト

○ BG Paul H. Fredenburgh,III, USA, Director, Command, Control, Communications, and Cyber (C4) U.S. Indo-Pacific Command
○ BG Moses Kaoiwi, USA, Director, Joint Staff-(HI), Joint Force Headquarters (JFHQ)
○Col Joseph (Jay) Matos, USMC, Director, Information Environment Operations, Marine Corps Forces Pacific
○Col Glen M. Genove, USAF, Deputy Director, Air & Cyberspace Operations (A3/6), CIO, & DIRCYBERFOR, U.S. Pacific Air Forces
○Brigadier General J.R.P. (Patrice) Laroche, Royal Canadian Air Force Deputy Director for Operations, J3, U.S. Indo-Pacific Command
○Dr. John A. Zangardi, Chief Information Officer, Department of Homeland Security

パネルでの主な発言は次のとおりです。

① サイバーに焦点を当てることは、新しい国家安全保障戦略の推進力の一つです。今日、私たちはすべての単一ドメインで競争しなければならないと予想されており、それにはサイバースペースも含まれています。 我々の敵はサイバースペースを活用して紛争に至らない範囲で作戦を実施しています。
② 私たちは、陸、海、空、宇宙と連携して、全地域のサイバー作戦全般を提供

しなければなりません。 我々は、効果的な作戦のためのネットワークの構想と設計を検討する必要がありますが、単独では行えないなら、同盟国やパートナーとの相互運用が可能なネットワークを設計しなければなりません。

③ これらのパートナーの１つはカナダで、宇宙、サイバーは、多国籍活動では不可欠な部分となる。

④ 技術だけでは連合の相互運用性に対する解決策ではない。連立パートナーにとって、より多くのギアを投げ入れることは答えではない。パートナーが相互運用性をどのように備えているかを考えなければならない。

⑤ ハワイの重要なインフラストラクチャーは任務保証（ミッション・アシュアランス）にとって不可欠です。ハワイ州軍はサイバーミッションアシュアランスチーム（CMAT）を結成し、すでに確立された化学、生物、核（CBN）の緊急対応チームと同等のものです。CMAT は、政府機関と業界の間でハワイ内においてパートナーシップを発展させる予定です。

⑥ 緊急対応は物理的であろうとサイバーであろうと、そこに存在する脅威に対する対処の鍵となる。

⑦ ネットワークの仮想化は、私たちの多くの進歩を可能にした。現在では、1 台のマシンが複数のネットワークにアクセスできるようにしている。IT の観点からすれば、全ては接続性に関するものです。

（６）太平洋陸軍副司令官講演

写真は講演する太平洋陸軍副司令官 Maj. Gen. John P. Johnson。講演の要旨は次のとおりです。

① 太平洋陸軍は、自由で開かれたインド太平洋への政府の取り組み全体において重要な役割を果たしている。

② 中国の強制的かつ統制的な行動は、実際に米国とその同盟国にとって大きなチャンスを提供している。中国は物理的、経済的プレゼンスを積極的に拡大していることが、他の国々を米国へと押しやっている。

③ 例えば、ベトナムはこの５年間で、素晴らしいパートナーとなった。

④ 他の国々との演習ではパートナーシップが構築されており、相互運用性も向上している。互いにコミュニケーションする能力が大きく向上している。

３．展示会

展示会には 179 社のブースが設置されており、ホノルル駐在の陸・海・空及び海兵隊から多数見学や情報収集に参加していました。出展されているブースの内、約 7 割がセキュリティ関連、その他が通信、表示、コンポーネント器材という感じでした。主要な項目毎に報告します。

（１）Cyber Security と AI（人工知能）

今回の展示において、昨年とは大きく様変わりしたのがこの項目です。サイバーセキュリティに関係するブースで、AI（人工知能）を謳ったアピールは皆無でした。AI を使用していないのかと問われれば、使用している箇所もあることは事実です。攻撃（侵入）の判定、マルウェア（亜種）の判定、ユーザー活動の異常検知等、確かに使用されている部分はあります。したがって、その性能をアピールするのにわざわざ AI という用語は使わなくなったということではないかと解釈しています。

日本でも有名なサイバーセキュリティ企業は、ほぼ出展していました。出展を見て内容の話を聞くだけでなく、毎年通っているので既知の企業関係者も多く、それらの方々との意見交換ができたおかげで各社の強みやシェアについて情報を得ることが出来ました。例えば、シスコシステムズは（写真は掲載していませんが）ネットワークルーターやスイッチの世界最大手ですが、実はサイバーセキュリティ分野でもサンドボックス（マルウェアであるかどうかを判定する機能）で大きなシェアを占めていました。しかし、後発組に押されかなり苦戦を強いられているということです。また、ファイアーアイはサンドボックスを最初に世に出した会社ですが、現在は他社に押されて下位に低迷しているということでした。最後の右写真のパロアルトは次世代ファイアーウォール（この中に様々な機能が内包されており、一台で各種の機能を果たすことが出来ます。）を展開する企業で、ファイアーウォール及びサンドボックス市場では第 1 位に躍り出たということでした。

写真の solarwinds と ivanti は共に IT/ネットワーク管理及びモニタリングを提供する会社です。solarwinds は米空軍で大きなシェアを占めており、そのネットワークモニタリング機能が高く評価されているとのことです。

写真は共にエンドポイントセキュリティの会社ですが、全く異なるアプローチをしています。ENDGAME はエンドポイントへの攻撃（エクスプロイト、マルウェア、ファイルレス等による攻撃）を阻止・対処するプラットフォームを提供する会社です。名前も面白いですが、オールインワン機能ということでシェア

を伸ばしているようです。他方、Bronium という会社は、エンドポイントへのマルウェアの侵入はあり得るということを前提として、メール添付ファイル、Web 閲覧等、外部との接触は全てセグメント化（隔離）するというソリューションです。マイクロセグメントと言い、添付ファイルの Word 文書等はセグメント化してもそのファイルへの書き込み、切り貼り等全て普通の機能として使うことが出来ます。そのファイル等を保存しても、セグメント化されたまま保存されることにより、マルウェアやエクスプロイトが付いていても、そのセグメントから出ることが出来ず、マルウェアやエクスプロイトとしての機能を果たせなくすることで安全を保つというソリューションです。Web 閲覧はインターネットエクスプロラー等の閲覧ソフトで見ている状態でセグメント化されて安全が保たれています。

（２）Insider Threat（内部脅威への対応）

女性のパネルディスカッションにおいて、「結果から見れば内部脅威（Insider Threat）こそが、最も重大な脅威である。」と Ms. Deborah Golden（Deloitte & Touche）が言っていましたが、スノーデン事件やマニング上等兵事件などはまさにそれを証明しています。実際、2016 年の米国カーネギーメロン大学による調査「US State of Cybercriminal Survey」によれば、毎年５０％以上の企業が内部犯行によるサイバー被害を受けているとのことです。

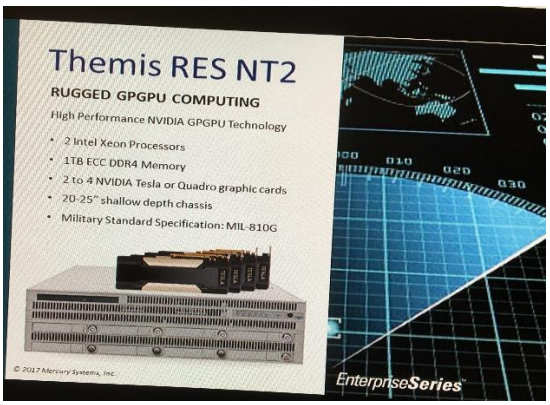
写真はエンドポイントの内部脅威対策のソリューションです。左写真の１０ZiG は Thin Client または Zero Client のエンドポイント器材によって、内部脅威への対策を行うものです。一般的な内部脅威対策として様々な所で活用されています。Thin Client 等は複数の端末の処理を一元的に特定のサーバー側で実施することにより端末にデータを渡さないことにより内部脅威に対抗します。しかし、ソフトウェアで処理することから沢山の端末からのアクセスが集中すると動きが鈍くなるなどの利便性の問題があることも事実です。

右写真は弊社が日本に紹介し事業支援している Thinklogical 社で恐縮ですが、発想が全く違い、端末 PC（シンクライアント用の接続器材でも含む）を保全が確保されたサーバー室へ隔離し、その端末から使用者のモニターやキーボード及びマウスを光ケーブルで延伸するものです。使用者側には USB ポートやネットワークポートが存在しないことにより、内部脅威をサーバー室に閉じ

込めるというものです。また、サーバー室の端末 PC（様々なシステムの PC）をマトリックススイッチに接続し、そのマトリックススイッチから使用者側に複数のモニター画面に複数のシステムの表示を出すことが出来るため、内部脅威を排除しながら情報共有を進めるものとして、米国統合軍司令部作戦室や情報機関の作戦モニター室等で全面的に使用されています。今回の展示会においても他社とは全く違う発想ということから異色の存在でした。

（３）Rugged Server（耐環境搭載型コンピュータ）

毎回のようにこの種の製品についてはご紹介していますが、今回も 1 年前とはラインナップが大きく違っていました。コンピュータそのものですから、製品の更新が早いということの表れでもあります。これらの製品に共通していることは、耐衝撃、耐振動、耐温度、耐電磁干渉等の能力が MIL-SPEC を満足しているということ。コネクター等の接続口の仕様を Mil-connector 等の特殊仕様に対応可能ということです。



上の写真は米国マサチューセッツ州に本社を置く mercury 社（元 Themis 社）のブースです。Themis 社の Rugged Server は陸・海・空の装備品（飛行機や艦船及びミサイル装置等）に導入されています。米海軍 DDG51 の最新バージョン（Baseline 9）の AWS（Aegis Weapon System）の表示装置のコンピュータとして同社の製品が採用されています。（海上自衛隊の「まや」には FMS でイージスシステムの一部として導入されているはずです。）

上写真は Dell コンピュータ社の耐環境性端末 PC と搭載用サーバーです。一般的なコンピューターメーカーであっても、このような搭載用の特殊仕様の製品も供給しています。今回の展示ではヒューレットパッカード社は同種の製品の展示はありませんでしたが、同社も Rugged Server を生産提供しています。

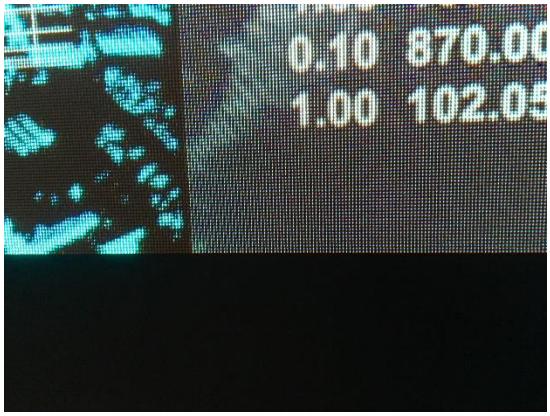
上写真はアイオワ州に本社及び工場を置く CRYSTAL 社のブースです。同社は 1987 年創業という老舗の Rugged Server メーカーです。左写真の奥にあるサーバーは 1.5U（高さの単位）という特殊な仕様になっていますが、米海軍潜水艦からの冷却効率を上げたいという要望に合わせて昨年作られたばかりです。海軍水上艦艇や潜水艦及び哨戒機（P-8）の様々なシステム（沢山使用されているのは映像処理系のシステムだそうです。）で使用されています。

左写真は KLAS　TELECOM 社の陸軍や海兵隊が使用する野外通信用の通信システム用の Rugged Server 及びスイッチです。同社はハンディというものに特化して前述他社の搭載型とは違いますが、適用されている MIL-SPEC は同様のものです。

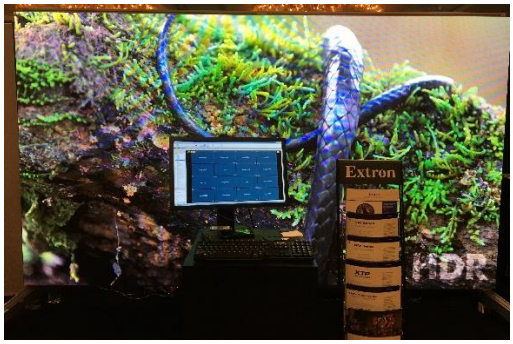
今回の展示では4社と少ないものでしたが、米国には10社以上のRugged Serverを生産する会社があり、互いに競っています。したがって、米軍等の様々なニーズに合わせた製品のラインナップが多彩なこと、一般使用のサーバー市場と連動して（使用されている部品は全てCOTS品）CPUやメモリー等が常に最新の性能を持っていること、価格が安い（日本の艦船・航空機搭載の同種製品と比べて）ことが特徴です。また、防衛省で懸念される部品の枯渇に対しては、全てがオープンアーキテクチャに基づいているため、ある部品が枯渇しても、必ず代替部品が存在することにより代替性は確保されています。（だから、世界の軍で使われているものと思います。）また、Rugged Serverの専業企業であるmercury社（元Themis社）もCRYSTAL社も日本に代理店もあり、技術部門も存在することから技術支援体制もあり整備性についても問題はないと思われます。

（4）Video Wall（大型表示装置）

艦艇等の衝撃や振動が加わる場所において、Video Wall（大型スクリーン）を使用することは、外枠を強固にしたり、ショックアブソーバーを付けたりして、機能以外の所に大きな出費を伴います。



上写真はPLANAR社のLED大型Video Wallです。小型のLED画面を８つ組み合わせて、写真の大型画面を作っています。LEDですので衝撃や振動に強く、万が一故障しても故障の小型画面のみを取り換えればよい構成となっています。右写真は画面を拡大したものですが、LEDの間隔は1.3mmとなっており、ハイビジョンまで表現できるということです。



写真はChristie Digital Systems社のLED大型Video Wallです。表示

制御は Extron 社のもので行われていました。この LED の間隔は 1.9mm であり、それでも右写真のように素晴らしい精細な表現が可能です。何故、1.9mm 間隔にしているかとの質問に対し、「価格も顧客の求めるもの」という回答でした。

（５）Cross Domain

クロスドメインと言えば、陸・海・空・宇宙・サイバーという戦闘空間を横断するもの、あるいは統合するものという定義で語られますが、ソリューションでクロスドメインという定義は違います。それは、違うセキュリティレベルを繋ぐものというものです。（例えば、秘区分無しシステムと極秘システムを接続するための機材というものです。）

左写真は TRIDENT SYSTEMS 社のブース、右写真は OWL Cyber Defense Solution 社のブースです。簡単に言えば、右写真に示されているように下位のセキュリティレベルのシステムから上位のセキュリティシステムのシステムへ一方通行でデータ（ビデオ、メール、その他）を流すものです。何を流すことができるか、逆方向へは流れないのかなどが、性能の良し悪しとなります。何故、このようなソリューションが必要かと言えば、例えば、一般のビデオ映像を秘匿システムで解析している分析官の所へ渡して他の情報と照らし合わせて、総合分析を行うためなどに用いられます。なお、これらの Cross Domain ソリューションは ITAR（International Traffic in Arms Regulations）対象に指定されており、同盟国への輸出は FMS 取引に限られます。

（６）その他

写真は、米海兵隊システムコマンドの正式プログラムに基づいて製作されたTRIDENT SYSTEMS社のSCC(Secure Communication Controller)v1.1です。これは違う無線機同士を繋ぐ他国軍(又は別系の無線等を使用する別軍種間)とのインターオペラビリティ確保手段として用いられます。写真はSCCの最新バージョンであり、個人携帯型を示しています。バッテリーが乾電池式となり、長期間の使用に耐えられるようになっています。車載型も旧バージョンより小型になっており、持ち運びが簡便となっています。10月に沖縄で新バージョンのテストを見せたとのことで、来年に沖縄駐屯の海兵隊に100セットほど納入されるそうです。

４．所　見

今回の講演やパネルディスカッションでは、新たな国防戦略の下、「Free and Open Indo-Pacific」という言葉が随所に使われました。また、名指しこそしていませんが、中国を対象にした内容であることも多く、このような公開の場を通じてメッセージを送っているようにも思えました。

このようなイベントに毎回(年に数回)参加しているお陰で、ある意味、定点観測をしているようなもので、展示物やブースのメッセージから変化を見ることが出来ます。また、既知の人たちと会話を通じて表面には出ていない情報を得ることが出来ます。

また、今回のTechNet Asia-Pacificには、航空自衛隊からの太平洋空軍司令部への連絡官と第747通信中隊への交換幹部の2人が参加されていました。陸・海の連絡官は通信職域ではないことから参加していないのではないかということでした。たとえ通信(又はIT)に精通していなくとも、見るべき展示品や聞くべき講演及びパネルディスカッションは沢山ありますから、このようなイベントには参加されることを期待いたします。自らの目と耳で行う情報収集が最も大切であると思っています。