資料２

サイバーセキュリティ戦略本部
研究開発戦略専門調査会
第２回会合　議事概要

１　日時
平成 27 年 4 月 27 日（月）　14:00～16:00

２　場所
フレンドビルディング７階会議室

３　出席者（敬称略）

（会長）	後藤 滋樹	早稲田大学理工学術院教授
（委員）	上野 裕子	三菱 UFJ リサーチ&コンサルティング株式会社 政策研究事業本部 経済・社会政策部 主任研究員
	小松 文子	独立行政法人 情報処理推進機構 情報セキュリティ分析ラボラトリー長
	小山 覚	NTT コミュニケーションズ株式会社 経営企画部 マネージドセキュリティサービス推進室 担当部長
	新 誠一	電気通信大学 教授
	名和 利男	株式会社サイバーディフェンス研究所 理事／上級分析官
	松原 実穂子	インテル株式会社 サイバーセキュリティ政策部長
	宮地 充子	北陸先端科学技術大学院大学 教授

（外部発表者）	木下 剛	シスコシステムズ合同会社 専務執行役員 最高技術責任者（CTO） 戦略事業開発担当 兼 IoE イノベーションセンター担当
	三輪 浩史	株式会社小松製作所 ICT ソリューション本部 副本部長
	御井 敬	関西電力株式会社 経営改革・IT 本部 情報監理グループ チーフマネジャー

（事務局）	髙見澤 將林	内閣サイバーセキュリティセンター長
	谷脇 康彦	内閣審議官
	篠田 陽一	サイバーセキュリティ補佐官
	三角 育生	内閣参事官

（オブザーバー）　内閣府
総務省
文部科学省
経済産業省

4　議事概要

（1）IoT セキュリティに関する発表

資料 4-1～4-3 に沿って、以下 3 名の方からそれぞれ発表。その後質疑応答。

①シスコシステムズ　木下専務執行役員
②小松製作所　三輪副本部長
③関西電力　御井チーフマネジャー

① シスコシステムズ　木下氏の発表に関する質疑応答

○（名和委員）シスコはスウェーデンの会社を昨年買収している。また、CTO の方が書いた人材に特化したブログには、IoT に関する示唆も含まれている。この買収はシスコにどのような意味があったのかを、人材あるいは他の観点で教えていただければと思う。

○（シスコシステムズ 木下氏）買収したのは人工知能の会社である。今、サイバーセキュリティの世界は IPS や IDS を含め、ログ解析が主体である。昨今の APT に代表される複雑なセキュリティ脅威を、人的リソース主体で解析するには限界があるので、我々としては、比較的効率を上げることができるものについては人工知能等の技術を積極的に活用しようと考えている。かといって、サイバーセキュリティの専門家が不必要になるわけでは当然ない。セキュリティ脅威が高度化する中、シグネチャーの解析など、専門家ならではの知見を持って対処すべきところで活躍していただくという役割分担が必要であるということで買収した。

人材の育成に関しては、IoT のビジネスという新しいものが訪れている中で、人的リソースのミスマッチの一番大きなところはセキュリティ分野だと思っている。IoT セキュリティに精通した技術者育成は、従来は各企業とも IT 部門の中で行っていたが、IoT のシステムの利用が IT 部門の中だけではとどまらず事業部やユーザーといった方々にまたがることを考えると、IT の専門家というのが特定の分野だけで育成されるものではなくて、もっと幅広

く一般的に対処していく上で、人材の育成開発というものが我々非常に大きな問題だと捉えている。

② 小松製作所　三輪氏の発表に関する質疑応答

○（宮地委員）KOMTRAX というシステムを初めて伺ったので沢山聞きたいことがある。３点お伺いしたい。

１点目に、同業他社も KOMTRAX のようなデータ収集や活用を行っているのか。

２点目として、KOMTRAX で収集したデータは、どちらかというと自社内の利活用が目的に思えるが、例えば安全性という観点で、いろいろな故障や事故の発生情報を同業他社間で共有化して安全性基準を作っていくというような利活用もあるかと思う。そのようなデータベースの結合、あるいはデータマイニングの結合のような活用を考えているのか。

３点目として、KOMTRAX のセキュリティの部分もとてもよく考えられているとは思ったが、どちらかというと、収集した後のデータのセキュリティ確保の観点になっていると感じた。つまり漏えい防止であるとか、第三者の持ち逃げ防止という観点である。今、組込のセキュリティが問題になっている。つまり集められたデータが本当に正しいのかという観点である。例えば、機械側で誰かが既に攻撃していて、収集したデータがすでに正しくないというようなこともあるかもしれない。その辺りどのように考えているのか教えていただきたい。

○（小松製作所 三輪氏）１点目の御質問について、他社にも同じようなシステムはある。コマツの KOMTRAX は 2001 年からスタートしているが、同じ頃に車用のナビが出て GPS が安くなって、データ通信というものも手軽に使える状況になって来ており、各社一斉にこのようなシステムをスタートしている。車からどんな情報を取得するかに関しては、多少は差があるが各社そんなに違うことはないと思っている。コマツが先行した大きな理由は、KOMTRAX を標準装備にしてスタートしたということで、システムが付いている車の数はかなり大きな差がついている。当然、沢山の車からデータが取れると、どのように使うのかということに必死になるので、データを使ってどうビジネスに活かすかというところでは、コマツは先に進んでいるかと思っている。

２点目の同業他社とのデータの共同利用という話については、非常に難しい問題で、各社囲い込みに走っているような状況にある。ただ、複数社の車を使っているお客様が沢山いるので、お客様のシステムにコマツのサーバー

からデータを送って欲しいという動きもあり、データのフォーマットの標準化や国際標準化の検討がされている。ただ、ごく基本的なデータだけが対象になるので、今度はそれ以外のどこでメーカー同士が差を付けるかの競争になるのではないかと思う。

３つ目の御質問で、組込の方でデータの完全性についての話は、基本的には一旦出荷してしまって 2000 年から動いている車を後から検証するのは非常に難しく、車を作ったときの品質保証のレベルのセキュリティのままとなってしまう。但し、故意にお客様がいじってデータを改ざんしてしまうケースも見られる。端的なのは先程のサービスメーターに関する話である。昔は中古車を高く売るために、走行距離を意図的に短くするといったケースがあったが、今はそれができないようになっている。しかし逆にサービスメーターの１日の増分値をもとに賃金請求をしている所では、沢山働いたように見せたいためにサービスメーターを進ませるというケースが出ている。コマツ側から見ていると、なぜ一日に 25 時間働いているのだろうかという車が存在している。それをお客様自身がやっているのか、代理店が加担してはいないか、そのような非常にややこしい話ではあるが、そういう点に関しては、最近気を使っている。

○（小山委員）今例えば代理店がデータを変更・改ざんする可能性があるというお話があった。国の状況も違う中でどうやってその脅威の種を拾って検討してセキュリティ対策に反映していくか、いわゆる PDCA を回していくようなところについて、とても苦労されているのではないかと思うが、可能な範囲で御紹介いただけないか。

○（小松製作所 三輪氏）もぐらたたき状態というのが本当のところだと思う。先ほど紹介したようなことがなぜわかるかというと、データの不整合を見つけると、そこを糸口に探して調べているからである。そうでないとなかなか見つからないのが実態かと思う。

きちんとデータが取れればお客様が喜ぶかというと、そうとは限らない。KOMTRAX で見ていると、タンクからの燃料の盗難がわかるのでお客様に連絡すると、外部の人ではなくオペレータが盗んでいたという例が結構多い。お客様側は、オペレータを解雇し次のオペレータを探すことになる。お客様にまた盗まれていることを伝えると、３回目くらいに、オペレータを探すのが大変なのでもう言わないでくださいということがあったりする。正しいデータであることを求めざるを得ないが、今の話のように、客が何に価値を持ってくれるかというのは各国で少しずつ異なる。全部同じように最高レベルの品質を求めようとするとコストとの兼ね合いもあって、ここも頭を悩ませ

ているところである。

○（新委員）KOMTRAX のサービスに 2001 年頃から取り組まれており、古い機種もあるとのことであるが、セキュリティ上の問題が出た場合には、機器のアップデートをする必要があると考える。アップデートの実施の有無や、アップデートが遠隔で出来るのか現地でするのかを、差支えない範囲で教えて欲しい。

○（小松製作所 三輪氏）仕組みとして遠隔で書き換える機能は持っているが、実際にはバグの修正くらいにしか使っていない。コマツの品質保証の考え方として、ソフトウェアは機器の品番と対応させて管理するので、そことの整合がまだついておらず、機能的には遠隔アップグレード出来るが、行っていないのが現状である。

もう一つは、配布資料の構成図でもお見せしたが、KOMTRAX は、自身が全てのセンサーを抱えているわけではなくて、基本的にはいろいろなコントローラーが抱えているセンサーのデータをコントローラーからもらってくるという仕組みである。古い機械でコントローラーが返答できないものは KOMTRAX だけアップグレードしても駄目なので、古い車について機能をアップデートしていくことは難しい。

○（松原委員）

２点お伺いしたい。１点目は、先ほどお話のあった KOMTRAX の件であるが、クラウド化はしていないが、2001 年からシステムの拡大を続けて来て、最近拡張が厳しくなってきているというお話があったと思う。仮にクラウドに切り替える場合、お客様からいろいろ懸念や質問があがってくると思うが、それに対して、どのように対応や説得をして行くのか。

２点目として、KOMTRAX をお客様に提供する際に、インターネットに接続している時点で抵抗感のあるお客様もいるかもしれない。インターネットに接続することで、データの改ざんの可能性以外に、外部からのサイバー攻撃などにより、システムが動かなくなる可能性について、懸念の声は出ているのか。この２点について教えて頂きたい。

○（小松製作所 三輪氏）１点目のクラウドにするとお客様がどういう反応するかというのはまだよくわからない。これから検証が必要と思っている。

クラウド移行によるセキュリティリスクよりも、個人情報保護の話やフォ

ースト・ローカリゼーション（Forced Localization）[1]の観点などから、世界中クラウドでシステムが成り立つのかという懸念がある。お客様自身が、機械から取得した情報の置き場がクラウドかどうかに関心を示すレベルにはないと思っている。

２点目の質問については、当初は、インターネット接続への不安よりも、コマツがデータを閲覧できることに対する不信感や懸念感があった。それは、実際に使ってもらってメリットを感じてもらった中で消えていった。

③ 関西電力　御井氏の発表に関する質疑応答

○（名和委員）制度面の件でお伺いしたい。計量ユニットについては、計量法に基づく検査・審査などがあるかと思うが、通信ユニットについて、第三者が評価するという仕組みづくりの検討は、セキュリティに限った話ではなく正しく動作するかといった観点を含め、今この業界であるのか。

○（関西電力 御井氏）計量ユニットは計量法で 10 年に 1 回検査するとなっているが、通信ユニットについては、定期的に検査する仕組みや第三者評価の制度はない。

○（後藤会長）家庭内の HEMS との連携などで、今後の展開が行われるということであるか。

○（関西電力 御井氏）そうである。これからいろいろな事業者が出てきて、30 分単位の計量データを使ったビジネスを展開されるかと思うので、そのような事業者にセキュリティを保った形でデータを提供するというのが、我々の使命かと思う。

○（後藤会長）その辺りは、ホームネットワークや、北陸先端大学の丹先生が色々コンソーシアムや標準化などを推進されていると思うので、そちらに期待したいと思う。

一つ質問がある。スマートメーターの導入は家庭向けの低圧受電顧客と、高圧である大口顧客へのどちらが先行するのか。

[1] 【Forced Localization】
情報セキュリティ、国家安全保障、自国産業の保護育成などを名目として排他的な独自政策を進める動きのこと。 自国で生成されたデータを直接海外サーバに送ることを禁じ、国内にサーバを置くことを求める動きなどもあり、ICT によるイノベーションを阻害する動きとして懸念されている。

○（関西電力 御井氏）高圧の方が低圧の展開計画よりも早い。

○（後藤会長）私の勝手な想像であるが、高圧のほうがユーザー側にもメリットが多いのではないか。

（２）IoT セキュリティに関するご議論

発表全体を通して、各委員からのご議論があった。

○（新委員）資料３に議論のポイント（１）にセキュリティ・バイ・デザインという言葉が出ているが、シスコの発表では個々の機器でセキュリティ機能を作り込むというよりも、監視し、その後は排除するという形の対策が重要ということで、個別の機器の対策だけでなくて、監視、継続的なアップデートというものを含めた形でのセキュリティ・バイ・デザインということだと思う。KOMTRAX も同じ話だと思うし、関西電力のお話の中でも委員の方からスマートメーター自身のセキュリティ、サイドチャネル攻撃についての質問があったわけである。つまり、このセキュリティ・バイ・デザインという中にいろいろな階層の作り込みがあるわけで、そこまで分解した形で議論していかないと話が食い違ってしまうのでないかと感じた。

また、関西電力の発表で標準化の話や、コマツ KOMTRAX のところでも ISO の話があったが、プレイヤーが多い場合には何らかの標準に基づいた形で進めることが重要で、そこのところが（２）の「関係者が協働を推進する方策」ということになるかと思う。

資料３の議論ポイントの四つのうちの二つについてコメントさせて頂いた。

○（上野委員）資料３のご議論いただきたいポイント（２）「多くの主体が関係する分野での、関係者が協働を推進していくための方策」や（３） 「IoT 製品に関わるセキュリティガイドラインを含む必要な指針や基準の整備はどうあるべきか」にかかわる部分について意見を申し上げたい。本日や前会合で、IoT セキュリティ分野の技術開発をしている方からの発表があったが、これらの技術を導入していくということになると、一言で企業といっても、技術を開発している企業、ユーザー、その間に立つサービスプロバイダーの３種類があるかと思う。ビジョンを示すのであれば、方向性や実現した場合の絵を示せばよいと思うが、これを「戦略」というもので示していくのであれば、誰が何をするのかも示すことが重要である。政府が全てを行うならい

いが、企業にも「協働」を働きかけるのであれば、ただ呼びかけても実現は難しく、ユーザー側にとって何のメリットがあるのかを示す必要がある。もしくはメリットがなくても脅威にさらされないためにセキュリティ上対応しなくてはならないというのであれば、国としてそれを示すとともに、誰が何をやらなくてはならないのかを戦略として議論していくことが重要と思う。

○（後藤会長）本日発表いただいたシスコシステムズ木下氏は、これまでも幅広くご活躍されていて、情報分野という面で幅広くお話されたと思う。また、KOMTRAX は大変有名で私も雑誌等で拝見し、クローズなものかと考えていたが、お話をお伺いしていると、登場する関係者が大変多く、また小松製作所のグループ会社の中でも別の視点から見ているという点は面白いと感じた。また、関西電力のお話では、それぞれの立場で視点が違い、それぞれのところにメリットがないとシステム導入の原動力となる動機づけが弱いということで、細かく見ていかないといけないと思った。

○（名和委員）私は、以前 NISC が進めていた行政機関に対するセキュリティ・バイ・デザインというところを２年半請け負った者であるが、かなりのバリアや障害があり、かなり大変だったという思いがある。今後を考えていく上で、CSIRT（Computer Security Incident Response Team）の構築において内部犯行というのがかなりある。内部犯行対策は情報システムだけでなくで、設計開発段階から意識しないといけないと言われている。海外もしくは他社からのコンポーネントについて、利益や個人の利ざやのために格安なものを使用したり、某国ではかなりパフォーマンスの低いものを不正に導入して、完成したものが動かなかったといったことも聞いている。不正なコンポーネントについても以前と違った考えで不正アクセスと考えた方がよいと思う。

○（小山委員）ソフトウェア開発現場のクオリティをどうあげていくかという視点も今の名和委員のご発言の中に含まれていると思う。今のソフトウェア、セキュリティの開発現場は、１つの例であるが、時給 2,000 円の人の書いたプログラムの穴を時給１万円の人が見つけているという状況となっている。本来は時給の高い優秀な方がプログラムの開発に携わるべきにも関わらず、仕組みの悪さがある。セキュリティ・バイ・デザインをたとえ作ったとしても、企業の経営者からするとスピードとコストが求められるということで、組み込みソフトウェアも容易に使ってしまうというのも背景にあるのではないか。よって、企業の理解を深めて、腕のあるプログラマーに本当にプログラミングさせるような、素晴らしい施策を推進していただきたいと思う。

○（新委員）今の小山委員の話に関連して発言させていただく。本日３名の方に発表いただいたが、ソフトの開発に関してはデバックやメンテナンスのための API が必ずある。小学生の子供でもゲーム機の API を探すのに一生懸命になったりするように、API は完全に攻撃対象となるし、また開発者は API を知っている状態である。API を悪用するようなことがあっても大丈夫、または露見するようなシステムまで考えないということを小山委員は御指摘になっていると思う。完璧なものはない、必ず攻撃されるということを前提に対策を練っていかないと意味のある対策はできないと思った。

○（小松委員）関西電力とコマツの話を踏まえると、権限が強いので情報を集められると見える。実際これから先 IoT を考えるとき、集中と分散というとありふれているが、権限が集中していない方にも情報を共有していくことが重要と思うので、そこが越えなければいけないところと思う。また、情報を集めるために標準的なインターフェイス、かつセキュアなインターフェイスが必要だと思った。

○（後藤会長）インターネットというのは分散というのがキーワードとなっているが、論理的には集中しているところがある。結構そういうところが攻撃の標的になっているという話がある。集中しているところが叩かれた例もあるし、守る方も注意深くやっているが、万全かと言われると危ういのでないかと考えている方もいる。そういったこともあり、スケールを考えた時のアーキテクチャは十分考えなければいけないのだろうと思う。

○（宮地委員）セキュリティ・バイ・デザインという観点で、今回３業種からお伺いした事例を考えたい。先ほどコマツの発表の際に業界内での情報共有ということを発言したが、業界というよりもセキュリティという点でデータベースを共有できるとよいと思う。スマートメーターへの攻撃の説明があったが、同じような攻撃がトラック車両に対しても適用される可能性がある。上手く異なる業界にも横串を組むことで、業界内の事例は少なくても集めるとスモールデータがミドルデータとなる可能性がある。セキュリティ・バイ・デザインとして、一般的な形でセキュリティに関するデータの提供や収集を行う仕組みができると、日本全体として、各種業界のセキュリティ向上に繋がると思う。

○（名和委員）資料３の議論ポイント（４）「IoT の特徴を加味したセキュリティ技術の開発・実証はどうあるべきか」に関して発言させていただく。

「IoT の特徴を加味したセキュリティ技術の開発・実証がどうあるべきか」というのは、人材にかかってくるのではないかと思う。まさにシスコでの人工知能の会社の買収などのように。

最近、米国の有名な検索エンジンを作っている会社が、日本の有名大学の新卒学生を、非常に高額な報酬でヘッドハンティングするというニュースがあった。他のところにもヘッドハンティングが来ているのではないかと思う。どのくらいの数の日本人が釣られていってしまうのかなと思った。

それを受けて、「新たなサイバーセキュリティ戦略について（イメージ）」の資料に記載のある「人材の発掘・育成」の「育成」の記載に少し違和感がある。「確保」等のほうがよい表現ではないか。日本にも組み込みシステムで、すばらしい技術者がいる。日本だけが丁寧に育成していき、外資系がどんどん取って行くという構図があまりよくないのではと感じた。人材の「発掘・育成」ではなく、「発掘・確保」の重みが重要かと思った。

○（小山委員）資料３の議論ポイント（４）について、別の観点で発言させていただく。IoT の機器などで、後からファームフェアのアップデートが難しいものについて、今日調べて安全なものでも、時間の経過により、新しい脆弱性が発見されるということがある。毎年、今年の攻撃の手法で見たときに、果たして安全かどうかということを継続的に見ていく仕組みもしくは組織がいるのではないかと思う。

よく米国では車を壊してレポートしているような、コンシューマーレポートのようなことをしている仕組みもある。そういったものが良いかは別として、情報の発信を含めて対応を行う必要があるのではないか。

特に組み込みシステムは、外観だけみても何が入っているかわからない状況であり、良かれと思ってシステム組んだ瞬間からもうセキュリティ的にアウトというものも、今後出てくるかと思う。

そこで、名和委員に質問がある。組み込みなど、セキュリティチェックが難しいもの情報共有というのはとても難しいと思う。まさか自分の買った製品の中に、最初から脆弱なチップが使われていて、使うだけで危ないという情報を、ユーザーはどう知るのかということも含めた、情報共有に関する、先進的な取り組みなどをご存じあれば御紹介頂けないか。

○（名和委員）小山委員の御質問の点について、いくつか事例を紹介する。

１つめに、各国 CISRT の国際会議である FIRST の６月頃にある年次会合において、各々が飲み物を持参して集まる BYOB（Bring Your Own Bottle）形式のコミュニティがあり、それぞれのお酒を持ち合い、お酒を活用して皆で信頼関係を醸成している。コンプライアンス的な要素もあるが、個人を信

頼して、ぎりぎりまたはプラスアルファで情報交換し、持ち帰って課題をどうするかということを毎年行っている。

２つめに、組み込み系では、組織を横断した技術者コミュニティが複数ある。その一つの組織には、実は組み込み系企業のトップエンジニアの方々が集まっている。車業界の方もいれば家電業界の方、情報システム業界の方もいる。個人的なつながりで信頼関係を構築している。

３つめに、信頼関係の実現について、欧州では Trusted Introducer（CERT の認定サービスを提供する組織）という仕組みがある。信頼段階を３段階にわけて管理している事例がある。この専門調査会に参加しているうちの何人かもそこに加入頂いて、いろいろな情報共有をしている。

これらの３つの取組では、信頼をどう築くかに注力しており、その違いは、お酒かまたは仕組みかと思っている。

○（新委員）情報共有について補足させて頂きたい。

小松委員の所属する IPA では脆弱性ハンドリングを以前から行っており、脆弱性情報を共有化している。また、経済産業省では、去年の５月に告示を少し改正して、制御システムも脆弱性届出の範囲に入ったと理解している。今の小山委員の情報共有についてのご発言について、実質的にどうかという問題はさておき、一応枠組みは政府として用意されていると私は理解している。

○（小山委員）情報共有の仕組みがあることは、情報共有のフレームワークの一員として、十分理解している。

一方、通信事業者の立場では、家庭用のルータが悪さしたり不正送金の温床となったりしており、あなたの端末が問題になっていますよと注意喚起することが時々ある。注意喚起の対象が例えばパソコンとかご自宅のルータであれば、自分のものであるという認識もあると思うが、いわゆる IoT や IoE（Internet of Everything）になってくると、自分が該当すると認識することすら難しいと思う。現在の情報共有の枠組みでは不十分かなと思っており、発言させていただいた。

○（後藤会長）前回の会合でも次のような話があった。

・脆弱性管理などに、誰がどう責任をもつか。
・問題があったときに、誰に連絡すればよいのか。
・何か問題があった時に、当事者にうまく連絡がつかないと情報が活きない。

先進的な KOMTRAX や関西電力のスマートメーターのように、ユーザー

との通信がある意味双方向で出来ているシステムに関しては、取得できる情報量の多少はともかく、通信の生死確認や、異常かどうかの反応はある程度とれるかと思う。一方、古い機器は、孤立しているのに、一方的にデータの取得が必要なものがあると大問題となる。

そういった点について、これから先にシステムを作る人が、どのような設計をすべきかや、それでも注意が必要であるという点について、今回ご議論いただいているのではないかと思う。

○（小松委員）シスコ木下氏の発表資料４－１の P.10 にあるフォグコンピューティングというものが、IoT のアーキテクチャの中で鍵となるような役割を持つと思ったが、その辺はいかがか。

○（シスコ木下氏）我々は、フォグ（霧）コンピューティングと呼んでいるが、フォグコンピューティング自体は、分散協調するインテリジェンスのことである。従来クラウドサーバなどの中で実現していた機能をどのように分散させるかということである。単に分散させるだけではなく、インテリジェンスの元となるところと協調しないといけないと思っている。その対象となる機能の１つがセキュリティの分野だと考えている。

IoT の世界は、分散協調の仕組みで対処せざるを得ないと思っている。集中型だと IoT のスケールを考えたときに必ずしも対処できないので、分散協調が鍵になると思っている。セキュリティのところも、分散協調でやる必要があると私たちは考えている。

今日ご紹介した配布資料４－１　P.11 の pxGrid（Platform Exchange Grid）というコンテキスト（コミュニケーションの状況）をベースにした、セキュリティのポリシーを交換する仕組みが、まさに分散協調の一つの仕組みである。脅威がわかった人がそれを周知し、またはセキュリティ情報を必要とする人がその情報を入手できるという、リアルタイムにセキュリティ情報を交換する仕組みづくりであり、それにシスコは取り組んでいることを御紹介したつもりであった。その旨補足させていただく。

○（松原委員）１点コメントと、１点質問がある。

コメントであるが、議論ポイント２の「関係者が協働を推進していくための方策」のところで、ポイントとなるのは、どれだけ素晴らしいセキュリティであっても、使ってもらえなければ何にもならない。使用にあたってはユーザー側、それから提供側の情緒的なハードルもかなりあると思う。技術だけではなく、お互い抱えている人間的な感情の部分もセキュリティの中で対処していく必要があると思うので指摘しておきたいと思う。

次にシスコの木下氏に質問がある。配布資料４－１ P.６の IIC（Industrial Internet Consortium）についての説明の中で、システムの標準化という話があったが、IIC は必ずしもセキュリティの標準化に特化したコンソーシアムではないと思う。IIC では、今後セキュリティについて、どのように推進していくのか。

○（シスコ木下氏）IIC では、IoT のシステムのあるべき姿を議論している。セキュリティに特化して議論しているわけでない。

セキュリティの取り組みについては、２つポイントがある。

１つめのポイントは、今あるもので活用できるものは活用していこうというアプローチである。セキュリティに関しては、既存の標準化団体や、既存のサイバーセキュリティの指針というものを活用していこという考えである。

２つめのポイントは、IIC の中でのシステムの標準化を行っている目的は、セキュリティを IoT のビジネスの価値を高めるイネイブラーとして整備していこうということである。比較的従来のセキュリティ対策は、防御するという視点でのセキュリティ技術開発が中心であったが、IIC や IoT World Forum では、セキュリティをビジネスのイネイブラーとして積極的に活用するのに何が足りていないのか、そして、足りていないものを整備しようということで、皆が検討している。

以　上