内閣府主催
世界経済フォーラム協力

Cyber³ Conference Okinawa 2015

Crafting Security in a Less Secure World

2015年11月7日（土）～8日（日）沖縄県名護市

INDEX

I. 背景

インターネットよりも、効果的に人間とモノをつなげることができたテクノロジーはこれまであったでしょうか。しかし今、インターネットが私たちにもたらしてきた変化など、瞬く間に過去のものにしてしまうほど、広大で複雑な世界が広がってきています。それはコネクティビティです。この広大で目に見えない「サイバーコネクション」網は、インターネット・オブ・シングス（IoT）が規模、流通、機能の面で拡大を続けるなか、専門家の理解すら追いつかないスピードで、私たちの世界を変えようとしています。IoTは、変革をもたらす力を持った技術です。今後IoTによって、従来の競争基盤が変わり、産業の境界が刷新され、既存産業を破壊するような企業が次々と誕生してくるでしょう。しかしこれにより将来どのような影響があるのか、官民問わずあまり正しく把握できていないのが現状です。

理論的には、ネットワークが拡大し、ネットワーク・デバイスのスマート化が進めば進むほど、利便性が高まりそのメリットも大きくなるはずです。データは、このニューエコノミーの通貨です。膨大なデータを活用すれば、ユーザーはパワフルな分析が可能となり、意思決定をリアルタイムでより的確に行えるようになります。そうなれば、個人や企業はもちろん、産業全体がより良い結果を作り出すことができます。すでに商業・工業・医療・政府その他分野のアプリケーションで、このサイバー空間の活用が進んでおり、接続デバイスから送られてくるデータも増え続けています。今後数年でIoTの普及が進み、オンラインやオフラインという区別はどんどん曖昧になるでしょう。
つまり、このハイパーコネクテッド・ワールドは、人類全体にこれまでにない恩恵をもたらしてくれる可能性があるのです。しかしその実現のためには、ひとつ欠くことができない条件があります。それは、「サイバーセキュリティ」です。特にIoTデバイス環境において、サイバーセキュリティが果たす役割は非常に大きいと言えます。サイバーセキュリティがなくては、個々のシステムはもちろん、相互接続されたグローバル経済全体の安定・信頼性は確保できません。

コンポーネントがより大きい容量で接続されていくに従い、IoTは今後も幾何級数的に増加し、ますます複雑な仕組みになっていくはずです。しかし、数字だけでこの巨大ネットワークの成功を測ることはできません。この巨大ネットワークが社会に恩恵をもたらすなかで、いかにユーザビリティ・信頼性・信用性を提供できるかが、成功の基準となるはずです。そしてこの信用性を高めることこそ、サイバーセキュリティが担う役割なのです。世界中のあらゆるレベルの組織が、物理・論理ネットワークとアプリケーション環境の全域（デバイスレベルの認証、アプリケーションセキュリティ、システム全体の保証、レジリエンシー、インシデント対応モデル等）を網羅する、新しいセキュリティの枠組みを必要としています。脅威情報の共有や、ベストプラクティスの迅速な普及など、国際社会が一丸となってセキュリティに取り組むことこそ、来たるIoT社会の基盤となるはずです。これを成し遂げるためには、全ての関係者による真剣で継続的な、ハイレベルのコミットメントが求められます。

逆にこうした対応を行わなければ、「サイバークライム」は急増し、IoT社会の基盤はもろく崩れ去ってしまいます。すでにサイバー犯罪者は、現実世界の犯罪者を模倣しはじめています。しかもこうしたサイバークライムは、デジタルの形式を用いている分、実際の犯罪よりも洗練されています。周知のとおり、脅迫や重窃盗など国境を超えて行われている犯罪も多く、こうした犯罪が個人に対する暴力犯罪に発展するのは、もはや時間の問題なのです。それだけではありません。サイバークライムがテロリストによるサイバー空間の利用へと発展した場合、多くの人や重要インフラ（発電所、ダム、金融ネットワークなど）がターゲットとなり、重大な経済混乱や大規模な人命損失など、あらゆる被害を引き起こす可能性があります。これはますます「つながっていく」世界で、とりわけ恐ろしい一面です。デジタルの0や1は、ユーザーもターゲットも区別しません。テロリストが使用するツールや高度なサイバークライムは、最初こそ潤沢な資金を持った天才が開発する必要があっても、それを複製したり実行したりするだけなら、知性がなくてもできてしまいます。何も対策がされなければ、一人の人間が100万ドルかけて作ったサイバー攻撃ツールが、コピー・ペーストされて若者の玩具になってしまうのもすぐの話です。そして、私たちが住む相互接続社会では、ある場所にいる一人の犯罪者やテロリストが、デジタルシステムの非対称性を利用して、地球上どこへでも社会に大損害を与えることができてしまうのです。

この文書の内容は、本件会議で行われた議論の内容をまとめたものであり、日本政府としての見解を記したものではありません。なお、日本政府のサイバーセキュリティ政策に関しては、内閣官房内閣サイバーセキュリティセンターのウェブサイトに掲載された関連文書を参照してください。
http://www.nisc.go.jp/
http://www.nisc.go.jp/eng/index.html

II. 要旨
A) サイバーコネクション

教育

業界ステークホルダーや政府機関、消費者に対して、IoTが機会とリスクを伴うことについて教育することは、非常に重要です。現在、新しい技術パラダイムに関する一般的な不信感は広範囲に広がっていますが、避けることのできないリスク・メリットのバランスがあることを受け入れ、説明する必要があります。メリットが高まれば、リスクもまた高まるのです。

人工知能（AI）やオートメーション技術は、人々の生活をより安全且つ快適にするものですが、それを提供する企業側は、信頼を得て理解を育まなくてはなりません。2020年までには、シームレスなクラウドを通じて、150億から200億ものデバイスが繋ることになるでしょう。その現実が実際にどれほど巨大なものになるのか、完全に理解している人は技術者を含めて皆無です。有意義な形で、一般の人々に教育するにはどのようにすればよいでしょうか。人間は特に意識することもなくテクノロジーと接点を持ち、また個人データの量や性質は常に変化しているため、教育も変化する目標に向けられたものとなります。消費者が、新しい技術のメリットを明確に定義して理解することができるにつれて、その技術が受け入れられる比率も向上します（例えばウェブメール。導入当初は安全なものだと思う人はいませんでしたが、今ではメールなしでは生きることができないほどです）。IoTに関しても同じ流れが続き、ユーザーたちに関する新たなデジタルデータが次々と生成されることになるのです。

構造構築

こうした理由により、IoTのアーキテクチャーの設定が必須となります。セキュリティ面で最も重大な点は、見知らぬ脅威に対する耐性を作ることです。登壇者の一人はこれを「想定できないことを想定すること」と呼びましたが、その意味は、止めることのできない脅威が存在するとして、全ての見知らぬ脅威に対して防御しようとするのではなく、侵入（ハッキング）に耐えることができ、不都合を最小限に抑えながら機能し続けるシステムが必要だというのです。

将来におけるネットワークユーザーは、もはや人間だけではなくなります。ロボットやAIシステムも、サイバー領域の一員となりつつあるのです。インターネットは、IoTデバイスとのインターフェースをスムーズに管理できるよう埋め込まれなければならず、その逆にはならないようにしなければなりません。自律システムが攻撃を受けて危険にさらされることも考えられるため、人間を介することなく、少なくともある程度は自己防衛可能なメカニズムが必須となります。

IoTというものは、そもそも、集積ないし送信されるデータ量が膨大に増加することを暗示しています。データ量が増加すると同時に増すのが脆弱性であり、IoTは多面的な脆弱性の時代の幕開けとなるでしょう。マルチステークホルダー間の意見交換が、如何にして真の協調を生み出し、問題ある関係に妨げられる国家的規制体制に向き合い、そして最終的に人々の信頼を深めることができるのか。IoTの規制やセキュリティ基準を策定するためには、同じ目標を共有する、マルチステークホルダーネットワークの構築が不可欠です。自由なアクセスと厳しい制約を受けるイノベーションの間で、均衡を見出す必要があるのです。そのためには、多様なステークホルダーが一丸となって、積極的に協力することが不可欠となります。

さらに、IoTは各種デバイスの機能性を最大限に活用することができるため、人々に様々な文脈上の体験や、マス・カスタマイゼーションという利益をもた

らします。同時に私たちは、これらの将来的なネットワークにおける一つ一つの要素に、セキュリティを組み込む必要性を検討しなくてはなりません。
「ハイパーコネクテッド・ワールド」はまた、保護された閉鎖的なイノベーションが、オープンイノベーションに取って代わられることを意味します。IoT時代において、データは新たな貨幣となり、かつてない程のデータ量が作り出され、その分析や活用は将来における重大課題となっています。
産業用IoTセキュリティについて言えば、多様なステークホルダーグループにより、チェーン全体のセキュリティを確保しなくてはなりません。レジリエンスは、IoTの安全な未来を準備するための鍵なのです。ハッキングされ得るものは、やがてハッキングされることになります。ネットワークに未接続のシステム（例えば電子投票システムなど）ですら、リスクに晒されているのです。リスクを緩和するために、バックアップシステムは不可欠です。バリアを用いた（あくまでも防御的な）システムは、既に過去のものとなりました。最善のモデルは、無数の攻撃に耐えながらも柔軟な反応により日々の活動への影響を最小限のものとしつつその機能性を維持する、複雑な人体の免疫システムのようなものでしょう。人体のように、健全な（耐性があって安定した）システムは、重大な悪影響やマルウエアの侵入にも屈することなく、何年にもわたって機能すべきなのです。

ヒューマンファクターと倫理的側面

IoTやAIに関して、プライバシーや人権、そして法的・倫理的責任について、重大な疑念があることは否定できません。IoTを規制するための、最善なアプローチの検討が必要です。規制なき世界は恐怖の世界となり、使い物にならない「ジャングル」になってしまいますが、他方で、規制だらけの「過保護国家」を作り上げてしまうことも簡単にできてしまいます。
自律型デバイスが引き起こす攻撃・事故があった場合に備え、予め責任の所在を明白にしなくてはなりません。人工知能を効果的なものにするためには、人間の意思決定・やりとりを研究し、人工知能の技術に応用する必要があります。究極的には、現状及び将来における課題の解決方法は、単に技術的なものだけでなく、社会的・政治的、そして経済的なものでもあるのです。
IoTはユーザーにとって、新興市場へのアクセスや自由を拡大させる可能性を秘めていますが、新興国ではテクノロジーが人件費以上に高コストで、またIT管理が緩慢である傾向にあります。知識の創造は、現状の経済的・社会的不平等を再生産するものとなってはなりません。知識の創造が、コストを負担できる者だけでなく全ての人に、具体的なメリットをもたらすようにしなくてはならないのです。IoTは、ユーザーベースのアプリケーション（例えば自宅やオフィスなど）が実行される際に、害を与えてはなりません。「ヒポクラテスの誓い」のIoT用デジタル版は、「初めに、害を及ぼさない」とするべきでしょう。

II. 要旨
B) サイバーセキュリティ

第5の戦争領域としてのサイバーセキュリティ

「比例性」や「相互確証破壊」といった従来からの戦争認識は、サイバー空間の領域における国家の活動に当てはめることが難しくなります。サイバー攻撃が、核兵器や生物化学攻撃と同等の大量破壊を成しうると想定はできるものの、これは起こり難い事態でしょう。サイバー攻撃は、核兵器や科学兵器による攻撃に比べて、遥かに集中的な攻撃が可能であり、なぜ国家が攻撃的なサイバー活動に従事してきたのかも、このサイバー攻撃の性質で説明がつきます。従来通りの戦争や戦略的な核兵器使用、その他の大量破壊兵器から手を引いた国家も、サイバー戦争を進んで検討するかもしれないのです。

他方で、軍と民間ユーザーによるインターネットインフラストラクチャーの共有は、軍事目標と民間施設の区別と、一般市民の巻き添え被害の程度の予測を難しくします。さらに、攻撃の二次的、三次的な影響があるかもしれないという不安が、問題をさらに難しくします。また、サイバー上の敵への対応策においては、オンライン攻撃の犯人を特定する技術的な難しさが、従来通りのリスク検討法の応用を困難にします。

多くの国家がサイバー手段による諜報活動や、限度はあるものの攻撃的な活動に積極的に従事しています。国家は、サイバー活動が何らかのアクシデントで本格的なサイバー戦争に発展することを避けたいのであれば、(冷戦時代の「紳士の諜報ゲーム」のような)共通ルールを策定することが重要です。サイバー攻撃ツールは非国家の主体が比較的容易に開発・導入できるため、許容可能な挙動について国家間で公式・非公式を問わず共通認識を策定する必要性が、ますます高まっています。

最も一般的な感覚で検討すると、紛争中の国々がサイバー活動の許容範囲について合意することはなさそうです。しかしその問題を個々の課題ごとに細分化すれば、当事者にとって共通の関心事や共通の価値観が具体化され、まず初めにそこから取り組むことが可能になります。時間をかければ、全ての当事者はもちろんのこと、各々の市民の安全や安定に貢献することができる、国家のサイバー活動に関する多面的な対話の構築に向けて歩みを進めることは可能です。

国際法はサイバー戦争とその他の戦争を区別していないため、国境を越えた紛争に係る現行法を有効に活用することができます。サイバー攻撃に対して如何なる対応が求められるとしても、攻撃者の帰属を明らかにすることは非常に重要な要素です。そのため、国家がサイバー攻撃の発端を特定するにあたって役に立つ能力を開発することに、より力を注ぐべきです。国家が攻撃者の帰属を見分ける能力を高めるために重要な分野は、三つあります。より良いテクノロジー、より良い脅威データの共有、そして敵に関する分析情報の共有です。これらがなければ国家は、他国家による活動と非国家の主体による活動を区別することができず、また適切に対応することもできません。実際、非国家の主体による脅威を見分けることが、従来敵対している国家間の共通事項となり得ることになり、それによってルール策定へと進むこともできるのです。近い将来、これらの国家は、互いに脆弱な分野(例えば原発や金融システムなど)をサイバー攻撃から一切立ち入り禁止とする合意事項を見出すべきです。双方にとって最も脆弱なインフラを犯さないという合意は、より大きな展望のほんの一部に過ぎません。

サイバー領域における国家の第一の関心事は、サイバーディフェンスです。脅威データの共有メカニズム(政府間の共有及び官民間の共有)は、サイバー攻撃の発生を防ぐ国家の能力に貢献できます。しかしこうした共有メカニズムが効果的に機能するためには、行動へと繋がる、意味のあるデータが収集・

共有されなくてはなりません。さもなければデータ共有することは、ほとんど価値がなくなってしまいます。破壊的な報復というものは自立国家のみのツールであり続けるべきですが、民間企業がツールの開発やネットワーク管理を通じて、サイバー攻撃への対応に関して国家を支援する余地はあるのです。
ハッキング被害に遭った企業には自己防衛をする権利がありますが、しかしその権利が相手に対するハッキングまで拡大されるかどうか、特にハッカーの資産の破壊や無能化までを含むのかについては、明白ではありません。かつて海の領域では、敵の船を追跡し破壊することが許された私掠船も存在していましたが、現代のサイバー領域においてそのような行動が可能であるのか、また望まれるのかどうか、明らかではありません。必要なステップは他にもあります。最も脆弱あるいは最も不安定な要素が、重層的な防衛システムに守られて常に一定の場所にとどまらない、耐性あるシステムを構築することが必要です。
経済スパイについては、大国間で規範的な価値観が共有されていない中で国家間の合意が必要になるため、特に難しい課題です。経済スパイ活動の範囲そのものが一つの課題だと言えるでしょう。例えば、貿易交渉にあたる国が政府の支援を受けて行う経済スパイ活動は、競合相手の交渉スタンスへの特権的なアクセスや識見をうまく得ることができれば、当該国家で活動する企業にとって有益です。このように難しい課題の解決のためには、各々の国が二国間ないし多面的フォーラムに進んで参加し、合意点を見出す過程を始めるほかにありません。

五輪におけるセキュリティ

ロンドンオリンピック・パラリンピック組織委員会（LOCOG）のセキュリティチームは、それぞれ独自のセキュリティアーキテクチャーを必要とする、5つの別箇のネットワークと関わっていました。
・LOCOG運営企業の企業ローカルエリアネットワーク（LAN）
・試合スコアやデータ送信に使用されたスコアネットワーク
・プレスネットワーク
・放送ネットワーク
・一般アクセス用WiFiネットワーク
ネットワーク運営者は、通常のファイアーウォール・不正アクセス監視システム（IDS）・ウイルス防御対策を採用しましたが、これらに加えて、ビッグデータ分析機器を開発し、ネットワークトラフィックのサンプル抽出や、進行中であるにも関わらず発見されにくい侵入の痕跡を探し出すことが行われました。結果、一秒当たり1万1千におよぶ攻撃回数が記録され、膨大な処理能力が必要となりました。その無数の攻撃に対応するためには、処理能力だけでなく、選手村・各スポンサー・訪問中の要人・国家それぞれが、直面するリスクがどんな性質であるかをしっかりと把握し、計画・実行に移すことを必要としました。ロンドン五輪セキュリティチームは、計画の策定に多大な労力を費やし、何が防衛を必要とする事項か優先事項をまとめました。ガバナンスをじっくりと検討することや、会場セキュリティ・ネットワークセキュリティ・警察など、様々な現場の関係者に与えられる役割と責任に関して理解することも求められました。来場者や業者、プレスなど、五輪ネットワーク設備を利用する人数を把握するとともに、その利用がもたらす課題やリスクを明白にする必要もありました。例えば、記録によると、マルウエア活動は来場者が持ち込んだデバイスからだけでなく、プレスが持ち込んだデバイスからも見つかりました。このようなリスクを理解し、ネットワークセグメンテーションなどを通じて対応することが重要です。
LOCOGと英国政府はいくつもの新たな手段を活用することによって、発生する脅威に対して素早く効果的に対応する能力を高めました。五輪参加予定国のセキュリティサービスと確実なパートナーシップを組むことで、専門家集団から集めたベストプラクティスを活用し、英国におけるセキュリティや警察の規範を超えて対応能力を拡大させただけでなく、オリンピック連盟に一致団結の感覚を作り出したのです。これらの関係が大会において大きく奏功し、重要情報の提供やリアルタイム分析、行動計画策定がオリンピック関係者間で広くサポートされました。ホスト国の政府は、現地でフュージョンセンターを設置すべきです。フュージョンセンターにおいて、他国政府やステークホルダーらは活動拠点を設置し、問題が発生すると同時にデータを共有できるようになります。
LOCOGはまた、テクノロジーの一時的な使用停止などにも取り組み、新たな技術を導入すると新たな脆弱性も発生するという脅威を、最小限にとどめようとしました。残念ながらこの原理は、ユーザーたちのテクノロジーニーズが増加したことにより、断念せざるを得ませんでした。ロンドンの場合、公衆アクセス用のWiFiネットワークを追加するという決断が下されたのは、WiFiデバイスが爆発的に増加してからのことであり、決断が遅れました。ここでも、ガバナンスがうまく働かなければなりません。警察から民間セキュリティまで全ての関係者を含む、セキュリティチームの役割と責任が理解されると同時に、支援が必要な際は誰に問い合わせればよいか分かるよう、個人的な関係性が構築されなくてはなりません。ひとたび計画が出来上がれば、今度はセキュリティスタッフを十分に指導、訓練する必要があります。スタッフの対応をテストして、向上させるためには、レッドチーム（仮想敵）や攻撃シナリオを用いなければなりません。そして、物理的セキュリティとサイバーセキュリティの連携が必要です。IT資産に物理的に近づくには、IT資産を格納する建物への物理的立ち入りが必要ですが、ITによって建物への物理的立ち入りをコントロールしています。敵対する者はこの点を理解しています。物理的な進入・退出ポイントから不正認証・DDoSに至るまで、セキュリティチームは

様々な攻撃ベクトルにまたがって、連携可能でなくてはなりません。これらの作業によって、実際に直面するであろう問題を事前に学び、インシデントを解決するために共に取り組むことになるカウンターパートと協働するのです。

軍隊と違ってオリンピック委員会の場合は、全てのセキュリティ資産が委員会の管理下にあるわけではありません。そのため、警察であろうと外国セキュリティチームであろうと、外部チームは目的意識を共有しなければなりません。信頼し合うことのできる個人的関係性の構築が、指揮系統に取って代わり、問題が発生した場合の素早いチーム間連携に繋がります。リオデジャネイロは、2016年五輪に向けてセキュリティチームの訓練のため、前回W杯大会を利用しました。東京は、2019年ラグビーW杯に投入するセキュリティ資産が、2020年に投入するものと同じであるようにするべきです。

次の五輪では確実に、想定可能なあらゆるサイバー脅威に直面することでしょう。そのため、ハクティビストや組織犯罪、インサイダー、政府を背景に持つハッカー、テロリストといった、広範囲の脅威を想定し計画を策定することが重要です。それぞれの敵の心理をプロファイリングし、潜在的な攻撃ベクトルを可能な限り洗い出し、無効にしなくてはなりません。今年初めのジャーマンウイングス機の墜落事故で見られたように、攻撃を防ぐための安全措置（この場合はキャビンドアの施錠）は、致命的な攻撃ベクトルへの扉を新たに開くこともあります。敵が何をする可能性があるのか予測し、適切な対応策を講じることはもちろん必要ですが、自己満足に陥ってはなりません。私たちの想像を超える、新たな予想外の攻撃ベクトルが出てくると想定し、そのような場合に備えて最善の計画を策定し、発生または発見と同時に対応していかなくてはなりません。五輪大会は世界における開催国の知名度を劇的に上げるため、セキュリティチームは、エネルギー供給網などのインフラやスポンサーの資産、政府ウェブサイトなど、様々なターゲットに向けられた攻撃に対応する準備をしなくてはなりません。これは五輪ウェブサイトや、選手村ネットワークに限られたものではないのです。サイバー攻撃への模擬訓練及び「レッドチーム」は、対応の効率を高めることができます。

敵の考え方の一歩先を行っていた例として挙げられるのが、前回のユーロピアン・フットボール・チャンピオンシップで実際に行われたフーリガン対策です。大会スポンサーたちは巧みにも、フーリガンによる暴力行為の歴史がある様々なEU加盟国の警察を招き、通常の制服姿で警備に当たらせました。驚くことに、この計画はうまくいきました。自国の警察が姿を現すと、フーリガンたちの暴力行為は、遥かに消極的なものとなったのです。主催国の警察と隣国の警察が、脅威データをリアルタイムで共有することも検討する価値があるでしょう。共に計画を策定し、訓練・協働することによって、イベント管理者たちはイベントに対する脅威を最小限のものとし、全ての人にとって安全で楽しめる五輪を保証できることでしょう。

サイバー規制

サイバー規制は、大きな概念（国家が目標とするセキュリティなど）と、日々発生する一時的な問題（大規模スポーツ大会の運営など）とを結びつける、ミドルウェアを指します。サイバー規制が、インターネットの安全に積極的に貢献できるものだということを、日本において証明することが可能でしょう。日本は、国民がインターネットにアクセスできるように努めていますが、このアクセスが安全なものであり、かつ社会の繁栄に貢献するようにしたいと望んでいます。EU諸国の視点から見ると、インターネットを価値あるものにするための成功の鍵は、規制の適用を受ける加盟国の規範的価値観や優先事項を具現化した、規制基準を策定することです。具体的には、レジリエンスの構築、国境を越えた協力メカニズムの採用、インフラの保護、リスク管理などが含まれます。また同時に、個人のプライバシーや利便性も尊重されなくてはなりません。そのため、ネット中立性やデータ漏洩通知などの問題も、検討されることが必要です。既存の価値観・法的手続きと一致しながら、衝突する必要性と利害の間で均衡をとることが、規制策定にあたっての目標となるでしょう。

米国企業がEU市民のデータ保存にあたって適用される「セーフハーバー協定」を無効とした、最近の欧州司法裁判所の判決に米国やEUは対応しようとしていますが、EUとしてはイノベーションを阻害せず、むしろ促進させる形で自らの域内におけるルールを策定しなくてはなりません。政府の役割は引き続き重要なものですが、民間企業も同時に積極的にルール作成に関わる必要があります。脅威に対する初期対応から新たなセキュリティツールの開発まで、様々な分野で主導的な役割を果たすためには、政府は民間セクターに頼らなければなりません。プライバシーは重要な関心事ですが、プライバシーのみが関心事であってはなりません。脅威に関するデータへのアクセスや、官民の間でデータを共有する能力も、極めて大事なのです。

サイバー関連ニュースについてメディアは最悪の事態をクローズアップする傾向にあり、これが誤解やヒステリックな反応を招くことがあります。最悪の事態に対応するためだけに策定されたサイバー規制は、的外れなものになるでしょう。規制措置は、慎重かつ合理的な、脅威に関する評価を反映したものでなければなりません。既に把握されている脅威の場合は、政府機関は、こうした脅威を防ぐためもしくは軽減するために、必要な措置をとるよう要求することが可能です。APT攻撃やゼロデイ攻撃による脅威への対策はさらに困難ですが、しかしそれだけの理由では、把握している脅威に対して既存の対応策があるにもかかわらず、行動をとれないことが正当化されるものではありません。

この状況は、道路に関する法律に類似しています。それぞれの国にはそれぞれのルールがありますが、共通項もまた多く存在しているのです。それぞれの国が国際運転免許を発行・交付するために、完全なルールの調和は求められ

ません。国際運転免許で運転するドライバーは、当該国家の法律に従うために運転の仕方を多少修正する必要はありますが、国際運転免許のプロセスは非常にうまく機能しています。それぞれの国は、独自の規範を阻害しない形で道路の安全性を維持しつつ、海外旅行者は、多くの国の道路を利用することができるのです。サイバー空間の法的枠組み・規制枠組みにおいても、同様の手法が検討されるべきですが、これは特に民間セクターに関して言えることでしょう。それぞれの国には独自のルールを実行する自由がありますが、しかしどの場所であっても当てはまり起こりうる、中核となるコンセプト（多重防衛）や基本的な実態（既知の脅威ベクトル）があるのです。

企業（特に多国籍企業）は、各国が共通の戦略や基準を策定するにあたって、支援をするのに適した立場にあります。世界保健機関（WHO）は流行病やその他の健康危機に対応するための安全基準を策定しますが、マルチステークホルダーから成る多国籍組織は、国家に対して、異なる市場においてある程度の一貫性を持つビジネスを提供しつつ、国内ルールを策定するのに役立つベストプラクティスや最低限の基準を提案することができるのではないでしょうか。マルチステークホルダーが参画しなければ、サイバーセキュリティ産業は障害なく発展し、後で規制をしようと思っても効果が薄いということになりかねません。つまり、国家と多国籍組織は、その価値観や優先事項を象徴するルールを策定しなくてはなりませんが、共通の解決策や連携メカニズムを発見するために協働することは、世の中の利益になるのです。

II. 要旨
C) サイバークライム

サイバークライムに対抗する国際的枠組みの必要性

国内法の調和と研究技術の進歩によって、インターネットとコンピュータ犯罪に対処しようとする最初の国際条約であるブダペスト条約は、サイバークライムに対して国際的に対抗するための強固な枠組みです。ただし刑事共助条約（MLAT）のプロセスでは、スピードや対応面で不十分です。既存のプロセスを改善するために、様々な実行可能な取り組みを実施すべきですが、それだけでなく、現在のアプローチを進化させる必要もあります。新たなアプローチ開発を推進するために認識を高める必要がありますが、新たなアプローチはそれまでのアプローチとは異なるものであり、また文化的制約を受ける可能性があります。社会的に受け入れられるアプローチにするには、マルチステークホルダー間で早急に協議する以外にありません。国家安全保障と法執行機関の結び付きが強化されると、必然的に複雑化してしまいます。

政策や法的枠組みを技術革新のスピードと整合させることの難しさ

政府機関は、技術革新のスピードに対応すべく苦慮しているため、官民のパートナーシップや、成果目標を柔軟に設定すること（目標達成方法は特定せずに、目標のみを指定）が好まれています。サイバー空間において国家の活動が増える中で、新たな課題が発生しています。攻撃者の帰属が（技術的・政治的要因によって）複雑化しており、当事者に対して告訴や規範徹底など、確実な制裁を加えることが困難になっています。サイバーリスクを全社的リスクマネジメント（ERM）に組み込み、（IT部門責任者にとどまらず）経営幹部レベルにも責任を負わせ、企業と政府機関の両者が、リスクマネジメントのために連携を推進する必要があります。

官民のパートナーシップと情報共有体制を確立してサイバーリスクを管理

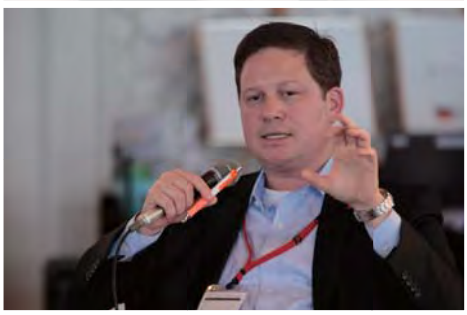
情報共有は重要なツールではありますが、目標とする成果でもなければ、すべての問題の解決策でもありません。産業界から政府機関だけではなく、産業界間、政府機関から産業界、政府機関同士の連携も重要です。情報共有や、情報共有に有効なモデルに関してはかなり進歩してきました。これらモデル（たとえばインターポール、ユーロポール、Microsoft Cybercrime Center など）から学び、さらに進化させる必要があります。会議参加者の多くは、「5 Eyes」と呼ばれるモデルは陳腐化しており、世界規模のマルチステークホルダーによる協力という観点から、コラボレーションがなされるべきと感じています。世界中の全ての問題に万能なモデルは存在せず、多様性を受け入れる必要があります。政府機関は単なる番人ではなく、当事者として参加する必要があります。情報共有の最終目標は、市民とシステムを保護することです。

民間セクターの参加を促すには、具体的な目標を明確にし、どの種類のどんなレベルの情報を共有できるか、また共有すべきかを特定することが必要です。脅威情報を共有し、今後の動向を先読みして手を打つことは、社会が将来の起こりうる脅威に対して耐性を持つことに役立つのです。

セキュリティとプライバシーに関する新たな課題

将来のイノベーションによって、セキュリティやプライバシー上の課題が発生すると同時に、それらに対処する新たな方法も登場します。組織（企業と政府の両方）が脅威に対して効果的に対応することを確実にするためには、準備と練習が必要です。このプロセスには経営幹部レベルを含める必要があります、なぜなら経営幹部レベルは、組織における全てのサイバーインシデントが特定されたことを確認しなければならないのです。

情報技術（IT）や運用技術（OT）が活用されたことを通じて得られた経験（セキュリティを考慮した設計、認証など）を、再検証して拡大し、この種の知識をIoTにも転用することが重要です。優れたサイバークライム対策スタッフを、政府機関向け（調査と告訴の専門家など）と業界向け（セキュリティアーキテクトなど）に、引き続き育成する必要があります。情報共有に関しては（あるいはサイバーセキュリティも）、「リーダー」はいないことを認識しなければなりません。皆、間違いを犯した経験があります。世界中での成功事例を基に、ベストプラクティスを開発する必要があります。



III. 会議の意義と今後の見通し

本会議で扱った3つのテーマは、１つずつ独立したテーマに見えるかもしれません。しかし実際には、これら3つのテーマは、それぞれ密接に関連し、持ちつ持たれつの関係にあります。とどまることを知らないサイバーコネクションの成長は、社会にとって有益なものとなる可能性を秘めていますが、他方で、新たなる極めて深刻な問題の元凶にも簡単になり得ます。どちらに転じるかは、国際社会が一丸となってサイバーセキュリティに取り組んでいけるかどうかにかかっています。新しいセキュリティパラダイムを形成し、真の国際協力体制を築くことができなければ、サイバークライムの増加に歯止めをかけることは不可能です。

今回の会議には、おおよそ30カ国から400人以上（政策担当者、企業経営者や学会リーダー等）が出席し、こうした課題について議論しました。議題の難しさはもちろんのこと、これら参加者が様々な知識や経験レベルを持った、異なる背景や視点の代表者として参加していたため、議論は非常に複雑なものでした。

これには理由があります。なぜなら、実行可能な解決策を見つけるためのカギは、まさにこのような多様性と反対意見がぶつかり合う状態を作り上げることにしばしばかかってくるからです。様々なバックグラウンドを持つ参加者が共通の議題を議論することは、議論に異なる視点をごく自然にもたらします。偏見なく意見交換をし、お互いの見解を真摯に聞き合えば、白か黒かで割り切れるものだと最初は思われていた問題が、実際には、有効な意見と考え方を広く包摂する問題であることが、判明するようになるのです。国境や文化境界、民族境界を越える複雑な問題を扱うときは特に言えることですが、包括的な解決策にたどりつくためにマルチステークホルダー対話を活用するこのようなプロセスは、かつてないほど重要になっています。

この手法は新しいものではありませんが、今日、非常に重要なものです。活発なマルチステークホルダーの参画は多様な意見を保証しますが、その様々な意見こそが価値ある一歩になるのです。言うまでもなく、同様の手法やイベントは、今後も繰り返されるべきです。今回の会議で話し合われたこと、また本ドキュメントに要約されたことは紙上で変化しない言葉ではありません。継続的な議論・討論を経て進化するべき、有機的存在なのです。今回のような取り組みは重要な始まりです。今回の議論は、ここで止まってはならず、別のフォーラムで別の参加者によって深められ、増進され、拡大されるべきものなのです。

サイバーセキュリティトラックで見られたように、日本においては今後数年間にわたり、2016年の伊勢志摩サミットや2020年の東京オリンピック・パラリンピックなど、重要なイベントが開催されます。特に東京オリンピック・パラリンピックの成功のためには、サイバーセキュリティの更なる向上が不可欠となります。会議で話し合われたことに基づき、官民の更なる協力、より高いレベルでの国際協力を推進していくべきことが、オリンピック・パラリンピックの成功を保証するために必要なのです。

IV. 付録：Plenary Sessionで議論された内容

サイバーセキュリティの重要性の認識

認識があるかないかにかかわらず、私たちはネットワークへの接続が高まる世界で生きています。IoTは地域経済とグローバル経済にこれまでにない大きな機会を与え、生活の質を向上させているものの、チャンスがある領域には遅かれ早かれ犯罪も付随します。サイバーセキュリティの専門家がいうには、企業は2つに分類できます。ハッキングされたことを知っている企業と、ハッキングされたことにまだ気づいてない企業の2種類です。サイバーセキュリティや他分野の専門家は、テクノロジーが進化してサイバークライムが増加・巧妙化する中で、将来の課題を予測して対応しなければなりません。現在、サイバーセキュリティの進化は、ネットワークへの接続が増大するスピードに追いついておらず、この状況を変える必要があります。

経済としてのインターネット

インターネットはただ単に経済成長に不可欠であるだけでなく、実際の感覚として、インターネットが経済そのものとなっています。すなわち、現在もしくは未来において、グローバル経済を考えるときは、インターネットがなくてはならない中核インフラとして必ず含まれるのです。企業はこれまで財務的な観点からリスクに着目してきましたが、サイバークライムのリスクを完全には理解していないため、サイバーセキュリティに十分に注力していません。また、情報の漏えいやハッキングが、企業の信頼性とブランドの価値を棄損することについて理解できていません。サイバーリスクの正確な評価が増加するなか、サイバースペース上の責任に関する保険市場が、サイバーセキュリティ経済の新たな領域となるかもしれません。

情報共有

情報共有によって、情報共有する当事者の一般的なセキュリティレベルを高めることができますが、機密情報を過度に使用すると脅威を招く可能性があります。企業は、セキュリティリスクを防止するために情報共有の重要性を認識する必要があり、他の競合企業との情報分離だけに注意を払うべきではありません。政府機関と企業の間の情報共有も不可欠です。政府機関は情報共有の監督者ではなく、情報共有の参加者として関与する必要があります。企業が情報提供を求められるものの、何の見返りも受けないということがあってはなりません。また、人工知能を通じて情報共有の革新が発生するものと考えられます。

暗号化したデータ

政府機関はサイバーセキュリティの専門家の声に耳を傾ける必要があります。アメリカ合衆国上院による暗号化に反対する法案は、セキュリティリスクを発生させる可能性があり、政府機関は暗号化されたデータに対して秘密裡にアクセスを求めることがあってはなりません。政府機関は市民と国家の安全を守るために最善の努力を行うべきでありますが、包括的かつ綿密な

戦略を策定し、サイバーセキュリティのコミュニティと自らの組織内のサイバーセキュリティの専門家の声に耳を傾けなくてはなりません。

健全なサイバー環境の促進に関する政府の役割

将来のサイバーセキュリティにとって、新たな形の官民パートナーシップが必要です。サイバーセキュリティは技術的なツールの問題ではなく、人的な問題です。そのため、人的な観点からの戦略的な検討が必要となります。市民は自らの生活がいかにネットワークに接続されているかさえも認識していないため、専門家は市民を保護するためのロードマップを作成し、また市民が自らを保護できるよう支援する必要があります。また、市民は体系的な攻撃や副次的な攻撃の可能性についても認識する必要があります。政府機関は、個人プライバシーを提唱する専門家の声に耳を傾けなくてはなりません。個人を特定することは重要であるものの、インターネット上で匿名性を保つ機能も必要です。

サイバークライムの発生

サイバークライムは個人と集団によって実施されますが、多くのサイバー犯罪者が発展途上国で活動しています。サイバークライムの脅威から逃れることは不可能であり、インターネットでは地理的な境界は存在しません。国家が攻撃（物理的な攻撃と非物理的な攻撃の両方）に関与することもあります。したがって、あらゆる種類の攻撃について明確に理解することが必要です。経済的な影響をもたらす例としては、証券市場の処理の遅れの発生や、銀行の取引への介入が挙げられます。実際に発生した例として、サウジアラビアで発生したサイバー攻撃があります。また、2012年に発生したグローバル・ブラックアウト作戦では、インターネット全体をダウンさせる旨のメッセージが出されました。この結果、これまでにないレベルの国際的な協力と情報共有が実現しました。

サイバーセキュリティと日本

日本は、世界トップレベルを誇るテクノロジー領域（自動走行や医療技術など）において、サイバークライムが発生する可能性を認識しています。2015年1月にはサイバーセキュリティ基本法が成立し、2015年9月にはサイバーセキュリティ戦略を決定しました。オリンピックを控えた日本は、有効なサイバーセキュリティ戦略の発展にあたって世界の規範となるチャンスがありますが、これらの政策や活動は実行されなければ意味がなくなってしまいます。

サイバースペース上の規範

サイバースペースの安定を確保するためには、官民の関係が重要です。自浄機能を備える民主的な政府が市民の認識を促進することによって、サイバーセキュリティ領域における改善が容易に実行できます。企業や組織の幹部

が、サイバー攻撃のリスクを正しく理解することは困難な状態です。政府と明確な議論を行い、原則に基づくアプローチを設定することで、2者間の関係を改善できます。単一グループのリソースと情報には限りがあるため、連携の強化が重要となります。

マイナンバー（社会保障・税番号）

2016年1月には日本に住む人は、個人番号カードを保有することでオンラインで本人確認が可能となります。将来的にはマイナンバーをクレジットカードや健康保険証として使用することも可能になります。医療に関するビッグデータを活用することで医薬品・医療機器に関する研究開発がさらに発展します。個人情報を扱うため、プライバシーの保護がさらに重要となります。

サイバースペース上の情報収集と共有

インターネットは社会基盤の一種として確立していますが、機密情報は常に脆弱な状態にあります。情報の収集と共有を強化することで、警察はより多くの問題（不正活動を行うWebサイトの取り締まりなど）に対応することができます。日本はサイバーセキュリティに関する人的リソースと予算が不足しているものの、民間部門のリソースの活用によってこの状態に対抗できます。公共部門と民間部門の協力がこの領域における日本の強みです。

教育

サイバーセキュリティでは教育が重要なポイントになります。ITセキュリティのエンジニアは、世界をより安全にするために必要な存在であり、サイバーセキュリティの教育への投資が不可欠です。

法の執行と国際協力

現代の法制度のスピードは、サイバークライムのスピードに追い付いていません。効率をさらに高めるために、強固な国際連携が必要です。消費者のデバイスに関する規制は企業間の競争をなくしてしまいますが、重要インフラに関する政府規制は重要です。

テクノロジーの動向

基礎研究を効率的にアプリケーションと関連付ける必要があります。大学において知的好奇心を喚起する環境を構築することで、イノベーションと研究を改善することができます。


Day 2: Plenary Sessions
KASPERSKY


Telecoms
Finance
Transportation
KASPERSKY

V. スピーカー

Aiko SHIMAJIRI
Minister of State for Okinawa and Northern Territories Affairs; Minister in Charge of Information Technology Policy;
Minister in charge of "Cool Japan" Strategy, Government of Japan

William H. SAITO
Special Advisor, Cabinet Office - Government of Japan; Global Agenda Council - Cyber security, World Economic Forum

Richard SAMANS
Head of the Centre for the Global Agenda, Member of the Managing Board, World Economic Forum

Cyber Connection Track

Track Chair
Toshiyuki SHIGA
Chairman and CEO, Member of the Board, Innovation Network Corporation;
Vice Chairman, Member of the Board of Directors, Nissan Motor Co., Ltd.

Policy Lead
Rod BECKSTROM
Former President and CEO of Internet Corporation for Assigned Names and Numbers (ICANN); Former Director of U.S. National Cybersecurity Center

Technology Lead
Jarno LIMNÉLL
Professor, Cybersecurity, Aalto University; Vice President of Cybersecurity, Insta Group Ltd.

Academic Lead
Christopher TREMEWAN
Secretary General, Association of Pacific Rim Universities

Secretariat
James KENDALL
Fellow for the Common Challenges Program, Executive Director, Japan-US Military Program (JUMP), Sasakawa Peace Foundation USA

Cyber Security Track

Track Chair
Dennis BLAIR
Chairman of the Board and CEO, Sasakawa Peace Foundation USA; Former Director of National Intelligence, USA

Policy Lead
Linton WELLS II
Distinguished Senior Research Fellow, Monterey Cyber Security Initiative (MCySec) at the Monterey Institute of International Studies; Former Acting Assistant Secretary of Defense / Chief Information Officer (CIO), US Department of Defense

Technology Lead
Phillip MORRIS
CTO, BT Japan

Academic Lead
Jim FOSTER
Professor of Political Economy, Graduate School of Media and Governance, Keio University

Secretariat
William "Bud" ROTH
Senior Manager, Cyber & National Security of Public Sector, Deloitte Tohmatsu Consulting LLP

Cybercrime Track

Track Chair
Noboru NAKATANI
Executive Director, INTERPOL Global Complex for Innovation

Policy Lead
Angela MCKAY
Director of Cybersecurity Policy and Strategy, Global Security Strategy and Diplomacy (GSSD) team, Microsoft Corporation

Technology Lead
David BURG
Principal, PwC Global and U.S. Cybersecurity Leader, PricewaterhouseCoopers LLP

Secretariat
Lena RYUJI
External & Community Affairs Manager, Microsoft Japan

Other Speakers and Discussants
(by alphabetical order)

Akira AMARI
Minister in charge of Economic Revitalization;
Minister in charge of Total Reform of Social Security and Tax;
Minister of State for Economic and Fiscal Policy, Government of Japan

Michael CHERTOFF
Co-Founder and Executive Chairman, Chertoff Group; Former Secretary of Homeland Security (USA)

Raman Jit Singh CHIMA
Policy Director, Access Now

Alan COHN
Of Counsel, Steptoe & Johnson LLP; Former Assistant Secretary, U.S. Department of Homeland Security

Mike FLYNN
Former Director, Defense Intelligence Agency (USA)

John Michael FOLEY
President, CEO and Founder of Danish Centre of IT and Cybersecurity (COPITS)

Ross FOWLER
Vice President, Digital Transformation & IoE Acceleration, Asia Pacific & Japan Cisco Systems, Inc.

Nik GOWING
International Broadcaster; Former BBC Main Presenter; Global Agenda Council on Geo-Economics, World Economic Forum; Visiting Professor, Kings College School of Social Science and Public Policy (UK)

Joseph Lorenzo HALL
Chief Technologist, Director, Internet Architecture project, Center for Democracy & Technology

Jerry HOFF
Principal Security Strategist, Vice President, Static Code Analysis Division, WhiteHat Security

Rick HOWARD
Chief Security Officer (CSO), Palo Alto Networks

Rex B. HUGHES
Co-Director, Cyber Innovation Network, The Computer Laboratory, Cambridge University

John C. (Chris) INGLIS
Distinguished Visiting Professor in Cyber Studies, US Naval Academy; Former Deputy Director, NSA

Steve INGRAM
Partner and National Cyber Leader, PwC Australia

Jazi Eko ISTIYANTO
Chairman, Nuclear Energy Regulatory Agency (BAPETEN), Republic of Indonesia; Professor of Electronics and Instrumentation, Gadjah Mada University

Toshinori KAJIURA
Chair, Cyber Security Working Group, Japan Business Federation (Keidanren)

Eugene KASPERSKY
Chairman and CEO, Kaspersky Lab

Yoshihiro KAWAHARA
Associate Professor, Department of Information and Communication Engineering, University of Tokyo

Noboru KIKUCHI
President, Toyota Central R&D Labs, Inc., Japan; Director, Toyota Research Institute of North America (TRINA)

Erka KOIVUNEN
Cyber Security Advisor, F-Secure Corporation

Taro KONO
Chairperson of the National Public Safety Commission, Government of Japan

Noboru KOSHIZUKA
Professor, Interfaculty Initiative in Information Studies, University of Tokyo; Vice Director, YRP Ubiquitous Networking Laboratory

Maoko KOTANI
Chief News Anchor, "Nikkei Plus 10" on TV Tokyo BS (satellite) Network

Yu-chuang KUEK
Vice-president, Stakeholder Engagement - Asia, Internet Corporation for Assigned Names and Numbers (ICANN)

Glyn LEWIS
Director, National Coordinator, Cyber Crime Operations, Australian Federal Police (AFP)

Clive LINES
Coordinator, Australia Cyber Security Centre; Deputy Director, Cyber & Information Security; Deputy Director, Australian Signals Directorate

Miroslaw MAJ
Founder and President, Cybersecurity Foundation; CEO, ComCERT

Cheri MCGUIRE
Vice-President, Global Government Affairs and Cyber Security Policy, Symantec Corporation

Francisco García MORÁN
Chief IT Advisor, European Commission

Carlos MOREIRA
Chairman, Chief Executive Officer, and Founder, WISeKey SA

Jeff MOSS
President and Founder, DEF CON Communications; Member, U.S. Department of Homeland Security Advisory Council

Jun MURAI
Dean and Professor, Faculty of Environment and Information Studies, Dean, Environment and Information Studies Faculty, Keio University

Soichiro MURATA
Director, Internet of Things/Fourth Industrial Revolution, SAP Japan K.K.

Toshio NAWA
Executive Director, Senior Security Analyst, Cyber Defense Institute, Inc. (Japan)

Christophe NICOLAS
Senior Vice-President and Head of Cyber Services and Technologies, Kudelski Security, Kudelski Group

Tsuguo NOBE
Chief Advanced Service Architect and Director, Intel K.K.; Visiting Associate Professor, Nagoya University

Brian D. NORDMANN
Senior Advisor, Bureau of Arms Control, Verification and Compliance, U.S. Department of State

Nohyoung PARK
Professor of Law; Director, Cyber Law Centre, Korea University

Jim PENROSE
Senior Vice-president for Cyber Intelligence, Darktrace Limited; Former Technical Director of Intelligence Operations, National Security Agency (USA)

Reinhard POSCH
Chief Information Officer, Government of Austria; Professor, Graz University of Technology

Harry D. RADUEGE, Jr.
Senior Advisor and Director for Cyber Risk, Deloitte & Touche LLP; CEO, Network Centric Operations Industry Consortium (NCOIC); Chairman, Deloitte Center for Cyber Innovation; Former Director, Defense Information System Agency (DISA)

Yoshihiro SATOH
Asia Regional Chief Privacy Officer, HP, Inc.; Former Assistant Councillor, National center of Incident readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat, Government of Japan

Stein SCHJOLBERG
Chair of The International Think Tank on Justice, Peace and Security in Cyberspace

Howard A. SCHMIDT
Partner, Ridge-Schmidt Cyber; Former Cyber-Security Coordinator, Executive Office of the President of the United States

Alexander SEGER
Executive Secretary, Committee of the Parties to the Budapest Convention on Cybercrime, Head of Cybercrime Program Office (C-PROC), Council of Europe

Makita SHIMOKAWA
Deputy Director-General, Foreign Policy Bureau; Ambassador in Charge of Cyber Policy, Government of Japan

Toshiaki SHIRAI
Director for Cyber Security, National Police Agency, Government of Japan

Tomotaka TAKAHASHI
Founder and CEO, Robo Garage (Kyoto University); Research Associate Professor, University of Tokyo; Visiting Professor, Osaka Electro-Communication University

Jun TAKEI
Director of Global Internet Policy and Standards, Intel Japan Corporation; Visiting Professor, Keio University

Tatsuhiro TANAKA
Research Principal, National Security Laboratory, Fujitsu System Integration Laboratories, Ltd.; Former head of JSDF communications networks

Yasu TANIWAKI
Deputy Director-General, National center of Incident readiness and Strategy for Cybersecurity (NISC), Cabinet Secretariat, Government of Japan

Giuseppe TARGIA
Vice-President, Security Business Unit, Nokia

Hideyuki TOKUDA
Dean, Graduate SCHOOL OF MEDIA AND GOVERNANCE; Director, Ubiquitous Computing and Communications Laboratory, Keio University

Paul WARD
Cyber Intelligence Manager, National Crime Agency (UK), currently seconded to INTERPOL Global Complex for Innovation

Makiko YAMADA
Director-General, Global ICT Strategy Bureau, Ministry of Internal Affairs and Communications (MIC), Government of Japan

Shunichi YAMAGUCHI
Former Minister for Okinawa Affairs and Information Technology Policy, Government of Japan

Ichita YAMAMOTO
Member, House of Councillors; Former Minister for Okinawa Affairs and Minister for Science and Technology Policy, Government of Japan


C3
CONFERENCE
OKINAWA 2015