大規模国際イベントにおけるサイバーセキュリティ対策

Cybersecurity Solutions for Major International Events

● 太田大州　● 武仲正彦　● 加藤正顕　● 益岡竜介　● 佳山こうせつ
● 福島則哲　● 今井豊成

あらまし

IoTの発展が急激に進みサイバー空間が広がる中で，サイバー攻撃はますます増加・高度化していく。加えて，国家の威信をかけた大規模国際イベントでは，世界中から大規模なサイバー攻撃にさらされることが想定される。これを見据え，東京2020オリンピック・パラリンピック競技大会（以下，東京2020大会）に向けて，サイバーセキュリティ対応能力を向上させるためのエコシステム構築が日本の大きな課題となる。富士通はこのエコシステム構築のために，政府に対してセキュリティ技術の国産自給率の向上を提言している。そして自社でも，国産技術を開発するとともに，人材不足が論じられるセキュリティ技術者の育成に注力している。このような取り組みを通じて，レガシーとして2020年以降の社会を支えるべく，エコシステムの構築に貢献していく。

本稿では，東京2020大会およびその先を支えるセキュリティに必要な着眼点と，それを支える富士通の技術開発・人材育成について述べる。

Abstract

IoT has developed rapidly, resulting in an expanding cyberspace. There is thus a risk of an increase in the number and sophistication of cyberattacks. Major international events often act as vehicles for the host country's dignity, and are exposed to massive attacks from all over the world. In view of the Olympic and Paralympic Games Tokyo 2020, Japan is faced with the major challenge of establishing an ecosystem that enhances its cybersecurity capabilities. Fujitsu proposes that the Japanese government improve the self-sufficiency of cybersecurity technology in order to build up the ecosystem. Fujitsu itself focuses on developing technology domestically and training security engineers to counter the prospective shortage of talent. Through these efforts, we will contribute to the creation of the ecosystem in order to support society beyond 2020, aiming to leave a legacy. This paper describes the important perspectives for making the Tokyo 2020 and future society cyber-secure. It also presents Fujitsu's initiatives in technology and personnel development.

ま え が き

2020年に開催される東京2020オリンピック・パラリンピック競技大会（以下，東京2020大会）は，IoTやAI（人工知能）の活用によってデータが価値を生む「データ駆動型社会」形成の重要な基点となる。データが価値を生み出す前提として，サイバーセキュリティは不可欠なものとなっている。日本にとって，競技大会を通じた社会基盤の変革は，2020年以降のサイバーセキュリティの礎となる。

近年，サイバー攻撃による被害は情報漏えいだけにとどまらず，電力会社や交通機関などの重要社会インフラにも及んでいる。不特定多数のコンピュータを狙ったWannaCryのようなランサムウェアや，IoT機器の脆弱性を利用するボットネットMiraiを使用したDDoS（Distributed Denial of Service）攻撃などが急増している。特に，大規模な国際イベントでは世界中からの大規模なサイバー攻撃が考えられ，開催国に対するサイバー攻撃は増加する。過去には，リオ2016オリンピック開催期間中に4,000万回の脅威を観測し，223回もの大規模なDDoS攻撃が行われたとされる。[(1)] IoT機器が300億個に達し，急速にサイバー空間が拡大していくと予想される2020年は，サイバー攻撃が更に増加・高度化することを認識しなければならない。[(2)]

このような背景を踏まえると，全ての攻撃を防ぐことは困難である。特に，サイバー攻撃の増加が想定される大規模イベントにおいては，あらかじめ攻撃および事故を前提とした対応が必要となる。この観点から，今後は「検知・対処・復旧」「関連組織の情報共有」および「それらを支える人材育成」が必要であり，これらを連携させるエコシステムの構築が課題となる。富士通はこの領域を支えるための技術開発・人材育成を実践している（**図-1**）。更に，日本が東京2020大会およびその先のセキュリティ基盤を創造・育成していくために，政府に対してセキュリティ技術の国産自給率向上を提言している。

本稿では，サイバーセキュリティにおけるエコシステムの構築という観点で，運用コスト低減や復旧時間の短縮，脅威情報の効果的連携，サイバー空間の破壊的拡大に順応するパケットキャプチャー，および新たな不正通信発見のための国産技術の開発について述べる。更に，これら技術の開発や運用の実践を支える人材育成について述べる。

東京2020大会を通じたエコシステム

攻撃者がサイバー空間を自由に使い，自らの目的を果たす現代において，個人の技術力向上とともに個人と個人のつながりを深めることが重要で

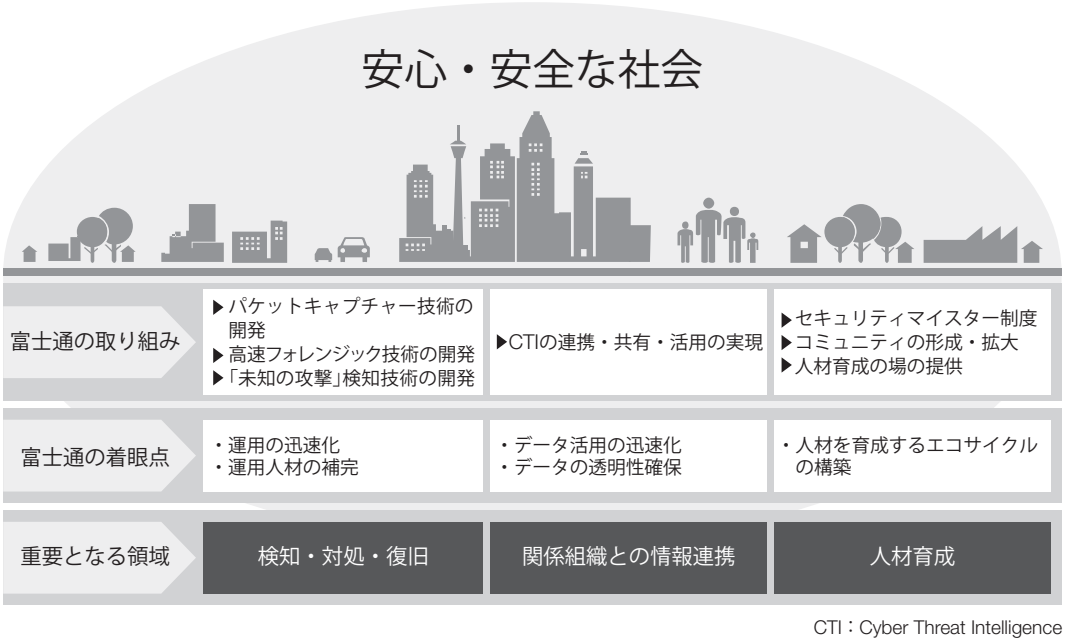

図-1　大規模イベントを支えるために重要となる領域

ある。サイバー空間を最大限に活用したデジタル革新を推進していくためにも，多くの個人がこのサイバー空間を安全にするために協力し合えるエコシステムを構築する必要がある。富士通は，国産技術の一層の進化と人材の育成，更には社会ルールの形成を通じて，東京2020大会の成功とともに2020年以降の安心・安全な社会の実現に貢献したい。

このエコシステムを構築するためには，東京2020大会に対するサイバー攻撃の目的を正しく理解する必要がある。オリンピックが国家の威信をかけて開催されるならば，その妨害には国家レベルで対策を講じる必要がある。また，犯罪組織や思想犯による攻撃の目的は，金銭や嫌がらせなどにとどまらず，テロ行為や脅迫にも及ぶことが想定される。

これらの想定から，東京2020大会を妨害するために実行される攻撃は，DDoS攻撃が主流になると考えられる。その攻撃を成功させるために，攻撃者は関係機関や企業に対して，様々なAPT（Advanced Persistent Threat）攻撃による諜報活動を繰り返し行ってくると考えられる。これは，DDoS攻撃に参加させるコンピュータやIoT機器が十分な数になるまで繰り返されるであろう。

これに対抗するためには，攻撃によってボット化した機器を排除し，インターネットの安全性に貢献するためのエコシステムの構築が必要である。そのためには，以下の三つの要件を連携させて取り組んでいく必要があると考える。

(1) 新たな技術視点による攻撃の感知と迅速な対応の仕掛け
(2) 社会に発生している脅威に関する情報を迅速に共有する仕組み
(3) 適切なコミュニティの形成によるモラルを持った高度な技術者の育成

国産技術開発における富士通の取り組み

本章では，前述した三つの要件に対する，富士通の技術開発について述べる。

● 戦略的イノベーション創造プログラム（SIP）

東京2020大会を控え，内閣府が主導する戦略的イノベーション創造プログラム（SIP）に，国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）を管理法人として，「重要インフラ等におけるサイバーセキュリティの確保」が追加された。SIPは，府省横断，産官学連携の中，研究から社会実装までをトータルに実施することを特徴とするプログラムである。(3)

富士通は，その中で「情報・制御ネットワーク構成機器のトラフィック分析による健全性確認技術」を担当し，情報通信インフラを主な対象とした研究開発に取り組んでいる。昨今，重要なインフラに対する様々なサイバー攻撃が顕在化する中で，本研究開発は脅威の侵入を完全には防ぎきれないことを前提として，組織の内部で活動する脅威を検知し，推奨される対策を提示することを目指す。重要なインフラである情報通信基盤では，新旧多種多様な機器が運用されている中，汎用技術を採用することで仮想システム化・仮想ネットワーク化が急速に進んでいる。これに対して，運用中の機器に手を加えることなく最小限の機器の追加で容易に導入できるように，通信パケットをモニタして分析する手法を採る。

富士通は，以下に挙げる項目の研究開発に取り組んでいる。

(1) システムおよびネットワークの仮想化に対応した高性能な通信パケット収集技術により，仮想空間の見える化を実現する。
(2) 汎用サーバを並列利用する高速パケット蓄積・検索技術により，低コストかつ高いスケーラビリティを実現する。
(3) 通信の規則性や送受信の関係性に着目し，通信データ全体を正常とみなし，それらの特徴量との乖離（かいり）を判断する群挙動モデル解析技術により，大量の通信データの中から不審通信を行う少数の機器を効率的に抽出する。

更に，セキュリティ対策を実装する上での最重要事項として重要インフラサービス・業務の安定継続を掲げ，緊急度と業務重要度に対応する対策リコメンド技術によるセキュリティ対策プロセスとエスカレーションの支援にも取り組む。**図-2**に示す階層の中で，特に重要と考えているのは，レベル2 ～ 3に対応するSOC（Security Operation Center）およびCSIRT（Computer Security Incident Response Team）の活動である。人材不足や業務輻輳が課題となるこの階層に対して，推奨される対策を提示

図-2　脅威検知レベルと対策エスカレーション

し支援することを意図している。

これらの研究開発の中で，ネットワークの仮想化に対応したパケット収集技術においては，従来技術の約7倍となる10 Gbpsの速さで欠損なく収集する技術を世界で初めて開発した。また，高速パケット蓄積･検索技術においては，収集した通信データを種類に応じて格納先を振り分けることで，合計100 Gbpsでリアルタイムに蓄積する技術を開発するなど，成果を挙げてきた。[4] 今後，インフラ事業者との社会実装を進め，東京2020大会期間中の情報通信インフラの安定稼働に貢献することを目指している。

● 高速フォレンジック技術

現在，攻撃の侵入後に行う対処と言えば，人手によるマルウェア解析が中心である。マルウェア解析には高度な知識が必要であり，そのようなスキルを持つ人材は常に不足している。一般的なレベルでさえ情報セキュリティ人材の不足が深刻であり，2020年には不足数が19万人まで増加すると経済産業省は分析している。[5]

この課題に対して，富士通は一般的なレベルの情報セキュリティ人材でも高度な攻撃侵入後の対処が行える「高速フォレンジック技術」を開発した。[6], [7] サイバー攻撃によって組織に侵入したマルウェアは，Windowsの遠隔操作コマンドを利用して不正ログインや感染拡大などを繰り返すことが知られている。本技術は，通信内容からリアルタイムにWindowsの遠隔操作コマンドを再構成し，その操作を行ったユーザー情報とともに記録できる。そのため，組織内に本技術を搭載したセンサーを設置して組織内通信を監視することで，組織内に侵入した攻撃の進行状況を詳細に把握できるようになる。更に，このデータを基に，攻撃の影響範囲の全貌を表示することも可能である（**図-3**）。

このように，富士通の高速フォレンジック技術を使用すれば，組織に侵入した攻撃の状況や影響範囲を可視化できるため，一般的なレベルの情報セキュリティ人材でも高度な対処が可能となり，人材不足解決の一助となると同時に，ネットワークの健全性復旧時間を大幅に短縮できる。[8]

● サイバー脅威インテリジェンスの利活用：S-TIP

サイバー空間を安全にするためのエコシステムを構築する一つの鍵が，サイバー脅威インテリジェンス（CTI：Cyber Threat Intelligence）の利活用である。CTIとは，サイバー攻撃の5W1H，すなわちサイバー攻撃を誰が，いつ，何の目的で，どこに，何を使い，どのような攻撃を仕掛けたか？の知識である。CTIの利用により，攻撃者の意図に対抗して防御のリソースを配置したり，サイバー攻撃の動向を分析したりするなど，主体的な対処が可能となる。

CTIは，人間系CTIとシステム系CTIの大きく二つに分けられる。人間系CTIとは，人がセキュリティ専用SNSやメールなどを通じてやり取りする，サイバー攻撃に関する情報である。一方，システム系CTIは，サイバー攻撃の知識をコンピュータが理解できるSTIX（Structured Threat Information

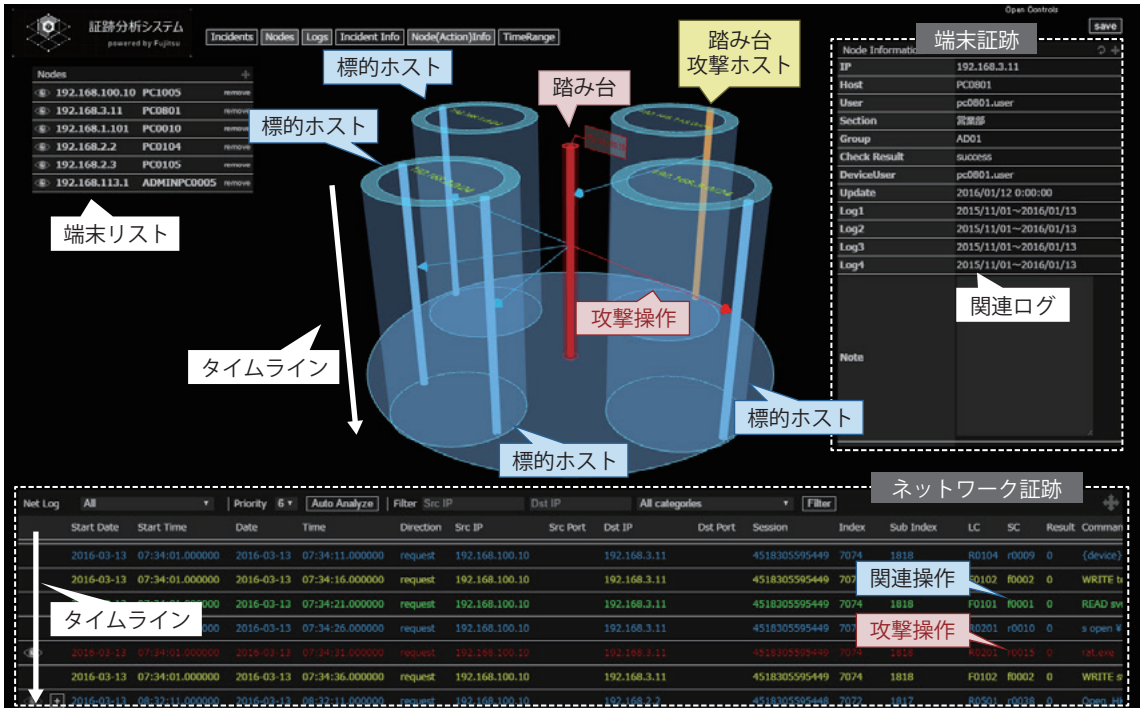

図-3　標的型攻撃の進行状況を可視化

eXpression）形式に変換し，システムに提供するものである。[9]−[11] 人間系CTIには文脈情報が多く，サイバー攻撃の全体を把握するのに有効である。システム系CTIはコンピュータ同士のやり取りであるため，共有は非常に高速であり，CTIに含まれる悪性のIPアドレスをプロキシサーバなどのセキュリティ機器へ自動設定することも可能である。

人間系CTIとシステム系CTIの共有および活用が重要であるが，それら二つがほぼ分断されていることが問題である。例えば，セキュリティ専用SNSに蓄積された人間系CTIをシステムで活用するためには，STIX形式に変換する手間と時間が必要となる。一方，システム系CTIは人の目に触れないものであるため，人の行動には結びつかず，人が評価することもない。

富士通は，デジタル技術によって人間系CTIとシステム系CTIを境目なく共有・活用して次の段階に導くS-TIP（Seamless Threat Intelligence Platform）を実現した。人は今までと同様にセキュリティ専用SNSやメールなどを通じてCTIをやり取りするが，それらは自動的にSTIX形式に変換され，システム系CTIとしても共有・活用される。システム系CTIは，セキュリティ専用SNSのタイムラインの中に人間系CTIと混じって分かりやすい形で表示される。これによって，セキュリティ専用SNSを見た人がシステム系CTIも共有・活用・評価できるようになる。このように，S-TIPは人間だけではなくコンピュータやセキュリティ機器などのシステムをも，CTIを利活用するエコシステムにシームレスに取り込み，新たな次元でサイバー攻撃への対処を実現する。

- **新たな技術視点での攻撃の感知：標的型サイバー攻撃検知技術「Malicious Intrusion Process Scan」**

既存の標的型サイバー攻撃検知技術は，標的型サイバー攻撃に使用されるマルウェアを検知対象としている。シグネチャと呼ばれる手配書とマルウェアを見比べたり，仮想環境で動作を確認したりして，マルウェアを検知している。つまり，マルウェアを検知することで標的型サイバー攻撃を発見しようとしている。しかし，これらの方法では，シグネチャの更新よりもマルウェアの進化が早くて検知できない事例や，マルウェアが仮想環境を検知して動作を止めてしまうために，すり抜けが発生する事例が起こっている。

また，シグネチャや仮想環境での検知だけでは

なく，ネットワークに設置されている様々な機器のログを収集して，相関分析ルールを適用して検知する方法も存在する。しかし，こうした運用を行うためには，機器が発信するアラートに対して危険と判断する基準の設定など，かなり高度な知識や技術が必要となるため，運用できる人員が限られている。

富士通グループが新しく開発した標的型サイバー攻撃検知技術「Malicious Intrusion Process Scan」は，マルウェアを見ることなくネットワーク上の攻撃者の行動を相関分析し，脅威をリアルタイムに検知することが可能である。[12), 13)] この技術は，以下の二つの特徴を持つ。

(1)「見つからない攻撃を見つける」検知技術

新たな着眼点による検知技術は，「攻撃者行動遷移モデル」を活用している。このモデルは，攻撃者により送り込まれたマルウェアの行動の遷移を整理したもので，実際のネットワーク通信を当てはめることによって攻撃活動を発見できる(**図-4**)。これによって，従来のセキュリティ対策をすり抜ける標的型サイバー攻撃もリアルタイムに検知し，情報漏えいのリスクを低減する。

(2)「見つけた後が違う」攻撃プロセスの見える化

攻撃を発見した後の対処については，対処の優先順位付けやログの収集・分析などの調査に必要な作業を自動化することで，容易に攻撃プロセスの見える化が可能である。これにより，対処の際に必要となる情報を的確に把握でき，SOC運用の大幅な効率化を実現する。

富士通のセキュリティ人材育成

本章では，富士通が考える人材育成の意味とアプローチについて紹介し，富士通が人材育成を通して成し遂げたい「つなげるセキュリティ社会」のエコサイクルについて述べる。

セキュリティの人材育成が盛んに叫ばれる中，富士通では2014年にセキュリティマイスター認定制度を立ち上げ，人材育成に取り組んでいる。700名を目標に制度設計し，3年半が経過した2017年12月現在，2,700名を超えるセキュリティマイスターが育まれた。

その一方で，育成ばかりに目がいき，育成された人材の活用や雇用，継続的なスキルアップや支援がないまま語られるケースも散見する。そもそも，人材育成の意味とは何なのか。富士通が3年半の実践で得た一つの答えは，「人と人をつなげるもの」である。そのような人材育成によって，セキュリティを共通の言語で語ることができ，共通の問題意識を持ち，そしてセキュリティの全体像を語れる人的ネットワークを作ることができる。

人と人がつながれば組織がつながる。普段，それぞれのミッションで縦割りになりがちな組織が，人のつながりにより情報を巡らせるようになる。そして，情報が巡れば相互理解が芽生える。デジタルデータを利活用する現場がセキュリティを理解し，セキュリティ部門がデジタルデータの利活

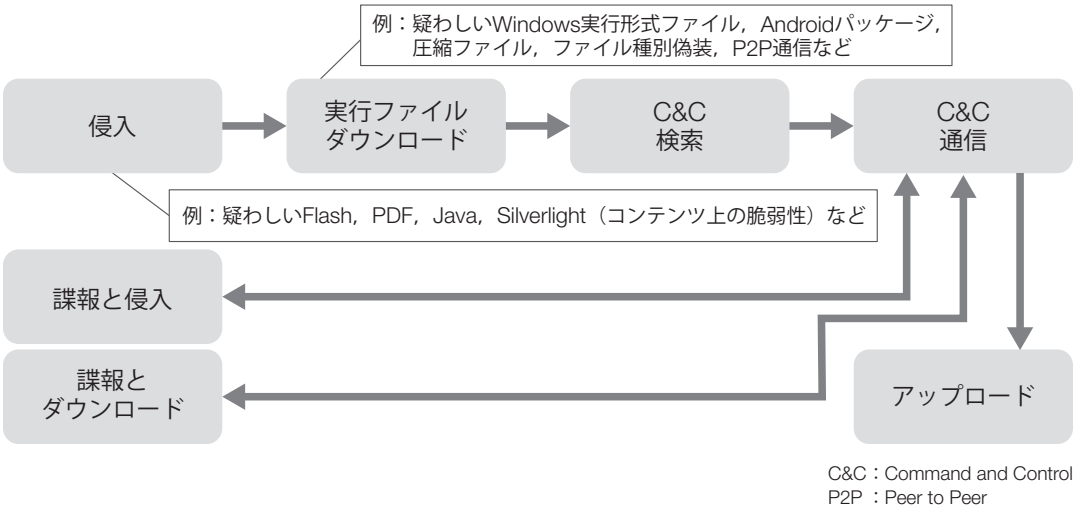

図-4　攻撃者行動遷移モデル

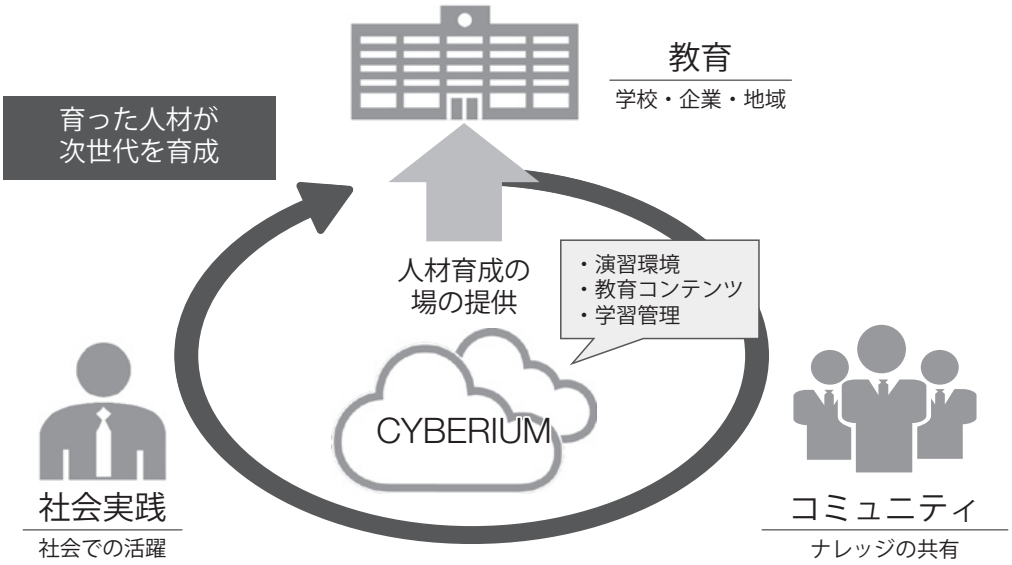

図-5　CYBERIUMを中心とした人材のエコサイクル

用を理解することで，セキュリティが付加価値となり，競争力を高めることができる。

人材育成を富士通だけにとどめることなく，お客様や地域，学生などの若者とともに実現するために，富士通は国産のサイバーレンジ（仮想演習場）CYBERIUMを開発した。これは，セキュリティを学び，体験し，考える場であるとともに，先人の失敗や成功を共有する場でもある。更には，仲間を作りコミュニケーションする場でもあり，育成されたセキュリティマイスターたちとともに育んでいる（**図-5**）。

これからも，育まれたセキュリティマイスターが安心・安全なデータの利活用を実践し，東京2020大会を新たな一歩として，人々が安心して暮らせる社会を実現していく。

むすび

本稿では，運用コストの増大，高度セキュリティ人材の不足という課題を解決する観点で，必要な着眼点とそれを支える技術開発，および人材育成について述べた。

大規模イベントを開催するに当たってサイバーセキュリティへの対応を充実させ，レジリエンス（復元力）のある社会に移行することが重要である。

本稿で記載した内容は，既に社会実装可能な状況にある。大規模イベント開催に向けて，直接の攻撃対象となる組織・施設への導入はもとより，サイバー空間を利用する多くの企業・団体・組織の積極的な導入を期待する。また，Society 5.0デジタル革新推進の横断的課題としてのサイバーセキュリティを，2020年以降に向けたエコシステム構築と同期させ，産官学による社会実装が急速に進むことを期待するところである。

本稿で述べた研究の一部は，総合科学技術・イノベーション会議の戦略的イノベーション創造プログラム（SIP）「重要インフラ等におけるサイバーセキュリティの確保」（管理法人：NEDO）によって実施されました。

参考文献

(1) 公益財団法人東京オリンピック・パラリンピック競技大会組織委員会テクノロジーサービス局長 舘 剛司：リオ2016大会の振り返りと東京2020大会へ向けたサイバーセキュリティの取組み．JAIPAクラウドカンファレス2017，2017年7月19日．
https://cloudconference2017.jaipa.or.jp/pdf/doc_rio.pdf
(2) 総務省：「2017年版情報通信白書」の概要．平成29年7月．
http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/summary/summary01.pdf
(3) 内閣府:戦略的イノベーション創造プログラム(SIP)．
http://www8.cao.go.jp/cstp/gaiyo/sip/
(4) 国立研究開発法人新エネルギー・産業技術総合開発機構，富士通株式会社：ネットワークの通信データを

欠損なく収集・蓄積する技術を開発.
http://www.nedo.go.jp/news/press/AA5_100893.html
(5) 経済産業省：IT人材の最新動向と将来推計に関する調査結果．平成28年6月10日.
http://www.meti.go.jp/press/2016/06/20160610002/20160610002-7.pdf
(6) 海野由紀ほか：標的型攻撃の全貌をひと目で把握する高速フォレンジック技術．FUJITSU，Vol.68，No.5，p.69-77（2017）.
http://www.fujitsu.com/jp/documents/about/resources/publications/magazine/backnumber/vol68-5/paper09.pdf
(7) 富士通研究所：サイバー攻撃の全貌をひと目で把握する高速フォレンジック技術を開発．2016年5月13日.
http://pr.fujitsu.com/jp/news/2016/05/13-2.html
(8) 富士通：「グローバルマネージドセキュリティサービス」を拡充し，イントラネットやエンドポイントのセキュリティの強化を実現．2017年5月12日.
http://pr.fujitsu.com/jp/news/2017/05/12.html
(9) OASIS：サイバー脅威インテリジェンス技術委員会.
https://www.oasis-open.org/committees/cti/
(10) IPA：脅威情報構造化記述形式STIX概説.
https://www.ipa.go.jp/security/vuln/STIX.html
(11) IPA：検知指標情報自動交換手順TAXII概説.
https://www.ipa.go.jp/security/vuln/TAXII.html
(12) 寺田成吾ほか：高度標的型サイバー攻撃検知技術～ Malicious Intrusion Process Scan ～．PFU Tech. Rev.，Vol.27，No.1，p.33-40（2016）.
https://www.pfu.fujitsu.com/about/technology/no49/images/49-5.pdf
(13) PFU：攻撃者の行動から標的型サイバー攻撃を検知する新技術を開発．2015年10月28日.
https://www.pfu.fujitsu.com/news/2015/new151028.html

著者紹介

太田大州（おおた　たいしゅう）
富士通（株）
サイバーセキュリティ事業戦略本部
国産技術の醸成・普及，人材育成支援に関する活動に従事。

武仲正彦（たけなか　まさひこ）
（株）富士通研究所
セキュリティ研究所
情報セキュリティ，暗号実装，サイバーセキュリティの研究開発に従事。

加藤正顕（かとう　まさあき）
富士通（株）
ネットワークソリューション事業本部
大規模ネットワークのセキュリティビジネスに従事。

益岡竜介（ますおか　りゅうすけ）
（株）富士通システム統合研究所
サイバーセキュリティ技術，特にサイバー脅威インテリジェンス（CTI）の利活用の研究開発に従事。

佳山こうせつ（かやま　こうせつ）
富士通（株）
サイバーセキュリティ事業戦略本部
外郭団体との協働，およびグループ会社と連携した人材育成業務に従事。

福島則哲（ふくしま　のりあき）
（株）PFU
セキュリティビジネスユニット
セキュリティ商品企画に従事。

今井豊成（いまい　ほうせい）
富士通（株）
サイバーセキュリティ事業戦略本部
サイバーセキュリティに関わる国際動向調査に従事。