「IoT・5G セキュリティ総合対策　2020（案）」に関する意見

2020 年 6 月 25 日

BSA ｜ザ・ソフトウェア・アライアンス（BSA）[1]は、「IoT・5G セキュリティ総合対策 2020（案）」（以下、「対策案」といいます）に関する意見募集の機会に感謝し、総務省（以下、「貴省」といいます）に対して、以下のとおり意見を提出します。

はじめに

BSA は国際市場において、世界のソフトウェア産業を代表する主唱者です。BSA の会員はソフトウェアが実現するイノベーションの第一線で活躍する企業で構成されており、5G ネットワーク・インフラやサービスを基盤とする、クラウド・コンピューティング、IoT（Internet of Things）、人工知能（AI）やその他の製品やサービスを通じて、世界の経済成長を加速化しています。データ駆動型の製品やサービスのグローバル・リーダーとして、また、サイバーセキュリティを促進する立場として、BSA は『Cybersecurity Agenda』[2]を策定し、世界中の政府に向けて、サイバーセキュリティ上の優先政策課題の解決にソフトウェアを活用すること、強靭な官民連携や広範囲な国際協力を通して、相互運用性を保ちながら、サイバーセキュリティ強化への取り組みを拡大することを提言しました。BSA は特に、以下の点における官民連携を強く支持します。

・業界標準を活用し、重要なセキュリティ情報を把握するための新たなツールを開発し、セキュリティに関する研究と脆弱性開示を強化することで、安全なソフトウェアのエコステムを促進する。
・相互運用性があり、リスクベースのサプライチェーン・セキュリティ政策を支持し、5G とソフトウェアのサプライチェーンを強化し、政府調達においてサイバーセキュリティを優先し、サプライチェーンの安全性を強化するための連携的な取り組みを促進する。
・国際規格の策定を支持し、セキュリティに関する国際法を連動させ、グローバルな規範に関する取り決めを促進することで、サイバーセキュリティ活動に関する国際的な合意形成を進める。
・STEM（科学・技術・工学・数学）教育を受けられる機会を増やし、サイバーセキュリティ分野のキャリア形成に向けた新たな道を開き、テクノロジー技能を持つ働き手を強化することで、21 世紀型のサイバーセキュリティ労働力開発をする。
・デジタル・トランスフォメーションを受け入れ、革新的なクラウド・セキュリティ・ソリューションを促進し、最先端技術の可能性を活用し、新たに出現するリスクに対抗するためのイノベーティヴな連携を育むことで、サイバーセキュリティを前進させる。

---

[1] BSA の活動には、Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software, Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday が加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] “Securing Tomorrow: BSA’s Cybersecurity Priorities and Software’s Essential Role” https://bsacybersecurity.bsa.org/wp-content/uploads/2020/02/02032020BSACybersecurityAgenda.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

上記の優先事項は、本対策案と一致しております。貴省が、労働力と人材開発、研究開発、官民連携、国際協力、国際規格、またセキュリティ・バイ・デザインの重要性を認識していることを我々は高く評価しています。

また、この機会に、日本政府が今回の世界的パンデミックにおいて、懸命に対応されていることに感謝を述べさせて頂きます。BSA 会員企業は世界中の政府を支援するために、救済と援助のための様々な取り組み[3]を始めています。エンタープライズ向けのソフトウェア企業は、教育者や事業者に向けてアドバイスや無償のリソースを提供し、緊急な医療研究のためのスーパーコンピューティングやアナリィテクス・ツールを運用し、緊急資金を寄付するなど、この難題に共に立ち向かうために連携をとっております。

この取り組みの一環として、BSA は『対応と回復に向けたアジェンダ』[4]（以下、「アジェンダ」といいます）を策定し、強靭で包括的なリモート・エコノミー（遠隔環境での経済活動）の構築のための提言をしました。アジェンダでは、強固なサイバーセキュリティの実践、強靭なインシデント対応力の支援、また、パンデミックからの回復期においては、5G ネットワークを含む、ユニバーサルで手頃で安全な高速インターネット・アクセス、そして、クラウドサービスへの責任ある移行を推進することを政府に求めています。

上記の見解は貴省の対策案とも一致しており、加えて、以下の意見を述べさせて頂くことで、日本政府が COVID-19 からの回復においてセキュリティをさらに強化し、日本経済の回復力を強化し、2021 年の東京オリンピック・パラリンピック競技大会に備えることに貢献したく考えています。

提言

I-(2) 改訂に当たっての主要な政策課題　① COVID-19 への対応を受けたセキュリティ対策の推進
1) テレワークの利用の増加への対応 / III-(5 トラストサービスの制度化と普及促進

貴省がテレワークや時差出勤を促進し、社員が請求書や押印や印刷等の処理のために事務所に通わずに済むよう、文書や業務のデジタル化を進めていることを歓迎します。この点で、タイムスタンプ、リモート署名、e シールを含むトラストサービスを促進し、また、これらのサービスを認証する公的枠組みの検討は大変重要となります。また、電子署名及び認証業務に関する法律が、民間においてクラウドサービスが広く普及していなかった 2000 年に制定されていることを踏まえ、本法を更新されることを奨めます。日本政府は、関連する基準適合の要件が現代の技術を利用できるようにし、民間企業が文書を認証するのにデジタル署名や電子タイムスタンプを全面的に活用をできるようにすべきです。COVID-19 を受けての緊急事態宣言時には、リモート署名やタイムスタンプが認証の公式な法的手段として認めらていなかったことから、勤務者が事務所に通わざるをえない事態となりました。

対策案においては、二年以内にトラストサービスに関する認定制度、認定基準、また現行法上の位置づけの検討が進むと記されておりますが、その検討過程においては、民間も積極的に関与させ、本取り組みを加速化させることを奨めます。社会において、これらのサービスが広く普及するには、誰もが、どのような端末からも、簡単にアクセスし、使用できるようにし、又、省庁内においても、本サービスが広く導入されるようにすべきです。また、これらのサービス導入を促進するために、様々な活用事例を政府から提示し、遠隔を軸とした活動の主要基盤となるクラウドサービスの積極的な導入も引き続き促進することを奨励します。

III - (3) クラウドサービスのセキュリティ対策

対策案においては、「政府情報システムのためのセキュリティ評価制度（ISMAP）」の導入により、省庁間のクラウド導入を促進することが記されています。その中には、セキュリティを含むクラウド

[3] 詳しくはこちらをご覧ください。https://www.bsa.org/covid19
[4] https://bsa.or.jp/bsa20200604-2/

環境の管理責任がサービスの提供者と利用者・調達者間で分担されるという、共通認識である「責任共有モデル」が明記されています。また、対策案においては、サービスの提供者側だけでなく、利用者・調達者側のリテラシー向上の重要性についても触れています。クラウドサービスが IoT や 5G ネットワークにますます不可欠となり、支えるアプリケーションやサービスが増えるにつれ、クラウド環境はより複雑でダイナミックになっていきます。クラウドサービス提供者は組込み型 ID 管理や脅威監視サービス等、顧客が自身のクラウド環境内で使う様々なセキュリティ・サービスを提供しています。また、IaaS（Infrastructure-as-a-Service）や SaaS（Software-as-a-Service）といった異なるクラウド・モデルによって役割や責任は変わります。

このことからも、クラウドの総合的なセキュリティ対策を策定する際には、このような多様な環境における役割や責任を慎重に区別し、この責任共有モデル下におけるのセキュリティへの意識向上が必要であることを強調しなくてはなりません。

III-(7) 重要インフラとしての情報通信分野のセキュリティ対策

また我々は、貴省において「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下、「ガイドライン」といいます）の更新に向けた検討がされていることを歓迎します。業務における利便性をさらに向上させ、政府のクラウド・バイ・デフォルト方針やデジタル手続法を反映し、地方公共団体におけるテレワークを促進させる目的で本検討がなされる時、本ガイドラインにおいては、クラウドサービス事業者（CSP）が、リージョナル又グローバルなインフラを活用してデータを蓄積・処理できるよう、データセンターの場所ではなく、CSP が準拠法に従い、データを安全かつ適切に扱うことに焦点をあてた改正をして頂くことを希望します。また、クラウドサービスを最大限活かし、より良いデジタル・サービスを市民に提供するために、物理的なネットワーク分離に関する記載をガイドラインから削除する、もしくは、分離の範囲を狭めることを推奨します。

また、地方公共団体の自主性を認め、各々の要件に合わせて商業的に交渉されたクラウドサービス契約に基づいて、最良の IT ソリューションと情報セキュリティへのアプローチが実現できるようにすることを強く奨めます。また、これに加え、地方公共団体間で積極的にベスト・プラクティスの共有がされることを奨めます。可動性、サービスの選択性、自主性を可能とする柔軟なガイダンスにより、市民を効率的に支援する上で必要なシステムを、地方公共団体が最適に選択することが可能となります。

III - (1)IoT のセキュリティ対策 / IV - (3) 国際連携の推進 - ③国際標準化の推進

IoT のセキュリティ対策を策定する上では、世界で進む同様の取り組みを考慮し、また、可能な限り、連携させることを奨めます。この緊急な課題に各国政府が着目する中、政策の分断のリスクが高まっています。IoT ソリューションが本質的に相互連携・依存していることから、政策の分断は問題となります。IoT セキュリティへの政府のアプローチが形成されるにつれ、国内、又、国際的な政策が互いに相容れず、矛盾し、一貫性が無くなると、多国籍なテクノロジー企業は、最善のセキュリティ・ソリューションの提供を阻まれ、苦しむことになります。これはイノベーションや競争を抑制することにもなります。IoT セキュリティに関して相互運用性のあるアプローチをとることは、日本、ひいては、グローバル経済にとって不可欠です。

この点において、国際的に認められた規格を軸に、貴省が IoT のセキュリティ政策を策定することを奨めます。相互運用性を促進することに加え、産業界、政府、学識者間の合意に基づくことにより、継続的なセキュリティ成果を生むことが可能となります。合意に基づいた国際規格を代替することはできなくとも、IoT 機器や部品の製造業者を指導する上では、産業界のベスト・プラクティスも参考となるでしょう。また、貴省は IoT 機器に着目したセキュリティの検討を拡張し、ネットワークや通信インフラも活用し、IoT 機器を保護する対策を考慮すべきです（例：安全な搭載、アクセスの方針、脅威監視、ドメイン・ネーム・サービス層のセキュリティ等）。

BSA は産業界の合意形成に向けた取り組みに関わっており、広く普及しているセキュリティに関するガイダンスを策定しました。例えば、BSA の『Framework for Secure Software』[5]では、IoT ソリューションや 5G を強化するソフトェアも含む、ソフトウェアのライフサイクルにおいてセキュリティを評価・促進する上で、エンタープライズ・ソフトウェア会社が実践しているベスト・プラクティスをまとめました。セキュリティへのアプローチを検討する上で、これらの資料を貴省が参照することを奨めます。また、20 の主要なサイバーセキュリティとテクノロジー団体をまとめている、C2 Consensus[6] on IoT Security Capabilities では、市場が求めるセキュリティへの期待に応えるために IoT 機器が備えるべき重要な性能について、また、世界的にセキュリティの相互運用性を保つために、IoT 機器製造者に向けたガイダンスをまとめています。

そして、対策案において触れているセキュリティ・バイ・デザインへのアプローチに関してですが、長期に亘りセキュリティを確保するには、ソフトウェア、ハードウェア、ファームウェア部品のライフサイクルにおける管理が大事であり、導入後の脆弱性への対応も求められているということを、ここに付け加えておきます。

III-(2)5G のセキュリティ対策 - ① 脆弱性の検証手続き等の確立と体制整備/
② 5G の脆弱性情報や脅威情報等の共有の枠組みの構築

脆弱性は、研究者コミュニティにおける独立したセキュリティ専門家等により識別され、製品ベンダーに報告されます。このような協調的な脆弱性の公開（coordinated vulnerability disclosure、以下、「CVD」といいます）プログラム[7]について、セキュリティの専門家はガイダンスと規格を策定し、この重要なニーズについて伝えています。このようなプログラムは全て国際的に認知されている ISO/IEC29147[8]や 30111[9]と連動すべきです。

IoT のライフサイクルにおいて、セキュリティ成果を改善するには、政府は事業者が自主的に以下のような CVD プロセスを確立するように奨励すべきです：（1）国際規格、特に ISO/IEC29147 と 30111 と連動している（2）人工的な軽減適時性等、非生産的な要件を避ける（3）IoT ソリューションのライフサイクルにおける脆弱性管理に関する相対的なアプローチを反映している。

対策案ではハードウェア上に故意に組み込まれた不正なチップによって生じるセキュリティ上の課題に関して記していますが、サプライヤーは、インフラやサービス改ざんを探知・軽減するために、ベンダー・サプライチェーンを認証するセキュリティ性能開発を強化しています。トラストアンカーやソフトウェア・イメージ・サイニングのような改ざんに防止技術は真正性やハードウェアの完全性を確実にします。対策案に記されているリスクに対応する上でも、これらの対策を取り入れ、産業界と協働することを推奨します。

III-(2) 5G のセキュリティ対策

5G ネットワークの基盤として、革新的でソフトウェアで強化されたツールや技術は、5G ネットワークがどのように作用するか、そして、それをどのように守るかを根本的に作り変えます。政府はセキュリティの課題に対応するために、ソフトウェアによって可能となるソリューションの導入を促進す

---

[5] BSA Framework for Secure Software https://www.bsa.org/reports/bsa-framework-for-secure-software

[6] https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf

[7] For more on software vulnerability disclosure, see the BSA Guiding Principles for Coordinated Vulnerability Disclosure, https://www.bsa.org/files/policy-filings/2019globalbsacoordinatedvulnerabilitydisclosure.pdf. On hardware vulnerability disclosure, see Center for Cybersecurity Policy and Law, "Improving Hardware Component Vulnerability Disclosure," https://centerforcybersecuritypolicy.org/improving-hardware-component-vulnerability-disclosure.

[8] https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-2:v1:en

[9] https://www.iso.org/standard/69725.html

べきです。特に、ネットワーク機能を仮想化する技術への投資、サイバーセキュリティを強化するための新たなソフトウェア・イノベーションの活用、そして、5G の研究開発のセキュリティを優先させることは、5G ネットワークに関連するセキュリティの取り組みを強化することになります。これらは貴省が対策案で認識しているアプローチです。

この点で、我々はオープンスタンダード、又、オープンソース主導のアーキテクチャーを強調することを特に推奨いたします。無線アクセスネットワーク（RAN）技術は、セキュリティ課題に対応するためにソフトウェアを有効活用した一つの重要な事例となります。RAN 市場は現在、ごく少数のベンダーが独占しており、そのうちのいくつかにはサプライチェーン上のリスク懸念があがっています。仮想無線アクセス・ネットワーク（V-RAN）やオープン無線アクセス・ネットワーク（O-RAN）によって RAN を仮想化することは、競争を広げ、ネットワークのエッジにおけるセキュリティを前進させることになります。

同様にソフトウェアを軸とした SDN（Software－Defined Networking）、ネットワーク・スライシング、NFV（Network Function Virtualization）のような技術はサイバーリスクを軽減する新たな機会をもたらします。政策立案者はガイダンスを策定し、研究開発に投資し、期待できるアプローチを試し、これらの新しい技術を新しいセキュリティ手法に適用することで、疑わしい通信を分離し、機密情報を保護し、ユーザーを認証し、その他のセキュリティ要件に対応すべきです。ゼロ・トラスト・アーキテクチャー（全領域の全アセットの間に明確な認証を設定）を導入するアプローチを採用し、完全性を確実にし（改ざんを継続的に監視し、軽減する信頼性の高い製品を採用）、完全な可視化を実現し（異常な動作や通信の探知を可能にする）、セグメンテーションを実施し（いかなるセキュリティー侵害の影響も最小限におさられるようにアセットのグループを適切に分割）、また効果的な脅威からの保護を採用（機械学習機能による防御的セキュリティ制御と継続的監視を提供）することで、安全な 5G セキュリティ環境を構築でき、運用を開始することができます。

様々な分野において 5G の導入が増すにつれ、一貫性のない、重複するガバナンスのリスクが生じます。5G は以下の分野において不可欠なテクノロジーとなります：通信分野（5G は超高信頼低遅延通信を提供します）、交通分野（5G は高度な交通管理を可能とします）、医療分野（5G が生命にかかわる医療機器や遠隔手術を支えます）、製造分野（5G が遠隔操作での支援ロボットによりスマートマニュファクチャリングを可能とします）等。前世代型の通信ネットワークが電気通信サービスに限定して規制することができたのに対し、5G が依存する中核となるインフラ（例えばクラウドサービス）は多数の機能やクライアントに同時にサービス供給するため、従来の電気通信に限定した規制には適合しません。ガバナンスを成功させるには、分野や省庁をまたがった統一的なアプローチが必要です。そのようなガバナンスの仕組みは、柔軟性があり、5G ネットワーク特有の利用法や脅威に対応し、個別のコンプライアンス要件に合わせたリスクベースのアプローチを構築しなくてはいけません。統一性をもたらすためにも、貴省が他の省庁との連携を促進する効果的な仕組みを構築することを推奨します。

I-(2) 改訂にあたっての主要な政策課題 － ④ 我が国のサイバーセキュリティ自給率向上に向けた産学官連携の加速 / IV －（1）研究開発の推進 － ① サイバーセキュリティ統合知的基準の構築

サイバーセキュリティの脅威は性質上、グローバルであり、国境によって隔てられているわけではありません。効果的な分析と調査のためには、サイバー攻撃に有効な脅威情報が広く可視化されていなくてはなりません。可視化は様々な情報源から可能となります。対策案に記載されている、オプンソースな情報（OSINT）（IV(1)①）や ISAC（III(1)③、IV（3）②）のような特定分野ごとの情報共有や分析センターのような選択肢に加え、顧客のインストール先、発表されている脆弱性、脅威を共有するネットワーク等から得ることも可能です。意義ある分析のために脅威情報を集めることは、脅威の調査が実施される場所には関係しません。日本国内のベンダーは海外の事業者同様、日本の情報源だけでなく、世界中の情報源から脅威情報を得て、研究することができます。国内と海外ベンダー間の脅威情報共有の取り決めは、有効な脅威データを集め、国内の能力開発を可能とし、対策案に記されている「データ負けのスパイラル」を防ぐことができます。BSA 会員企業の多くはそのような情報

共有の取り決めを促進しています。貴省が情報共有を強化し、エンジニアをグローバルな規模で育成することを奨めます。日本特有のサイバーセキュリティ・モデルが世界と相容れなくなることは、日本が国際的にサイバーセキュリティをリードすることを妨げることになります。

結び

BSA は、上記が対策案をまとめるに参考となることを願います。データ・フリー・フロー・ウィズ・トラスト（DFFT）を支えるために貴省がサイバーセキュリティにおいて、リーダーシップを発揮するのを我々は支援します。また、今後は、政策提言に関して意見募集をする際は、長めの期間を設けることを奨励します。19 日間ではなく 60 日間であれば、対策案を検討・分析し、高い関心を持つ利害関係者間で調整し、我々の立場や提案をまとめ、思慮深く、建設的な提言を、政策策定においてすることが可能となります。また、BSA は現在、セキュリティ政策において世界中の政府を支援するために、IoT や 5G のセキュリティに関する指針を策定しております。本意見に関してご質問等があれば、いつでもご連絡下さい。

以　上

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office