「サイバーセキュリティ戦略」に基づき 2019 年度に実施すべき施策に関する意見

2019 年 2 月 25 日

BSA ｜ザ・ソフトウェア・アライアンス（BSA）[1]は、内閣官房　内閣サイバーセキュリティセンター（NISC）に対して、「サイバーセキュリティ戦略」に基づき 2019 年度に実施すべき施策（サイバーセキュリティ 2019）に関する意見提出の機会を歓迎します。BSA は、NISC が、日本及び地域においてサイバーセキュリティに関する継続的なリーダーシップを発揮し、サイバーセキュリティ政策策定に関して産業界のステークホルダーと誠実に協力いただいていることに感謝し、2018 年に取りまとめられたサイバーセキュリティ戦略を実施するための 2019 年に具体的な措置を定める NISC の取り組みに敬意を表します。

はじめに

BSA 会員企業は、データ駆動型のイノベーションの最前線に立って、グローバルな情報経済を推進し、また、日常生活をより良くするための重要なソフトウェア、セキュリティツール、通信デバイス、サーバー、コンピュータを開発し、提供しています。BSA 会員企業は、産業制御システムや IoT デバイスを含む重要な技術を開発しており、これらは、サイバーセキュリティ戦略の Society 5.0 のビジョンで議論されるデジタルにつながった産業のバックボーンを形成しています。また、サイバー脅威から利用者及び技術を保護するためのセキュリティ技術を提供することによって、利用者の信頼を獲得しています。よって、BSA 会員企業は、サイバーセキュリティ戦略の実施に重大な関心を有しており、日本のコネクテッド・エコノミー全体のセキュリティを向上させる効果的なアプローチを策定するため、NISC に協力させていただきたいと考えています。

サイバーセキュリティ戦略に基づき 2019 年度に実施すべき施策全般について

サイバーセキュリティ戦略は、日本及び世界においてサイバーセキュリティを強化するための説得力あるビジョンを示しています。マルチステークホルダーとの協働を重視することは、セキュリティを著しく進展させつつデジタル経済を強化する、賢明で実践的かつ効果的な政策策定への最適な道筋です。NISC はサイバーセキュリティ戦略を 2019 年にいかに実施するか検討しており、この点、私どものインターナショナル・サイバーセキュリティ・ポリシーフレー

[1] BSA ｜ The Software Alliance（BSA ｜ ザ・ソフトウェア・アライアンス）は、グローバル市場において世界のソフトウェア産業を牽引する業界団体です。BSA の加盟企業は世界中で最もイノベーティブな企業を中心に構成されており、経済の活性化とより良い現代社会を築くためのソフトウェア・ソリューションを創造しています。ワシントン DC に本部を構え、世界 60 カ国以上で活動する BSA は、正規ソフトウェアの使用を促進するコンプライアンスプログラムの開発、技術革新の発展とデジタル経済の成長を推進する公共政策の支援に取り組んでいます。BSA の活動には、Adobe, Akamai, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAS Institute, Siemens PLM Software, Slack, Splunk, Symantec, 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。

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

ムワーク[2]に記載されている6つの包括的原則に基礎を置いて実施することを、BSAは提言します。

1. 政策は、国際的に認められた技術標準と整合すべきです。国際的に認められた技術標準は、サイバーセキュリティに対する効果的なアプローチを定義し実施するための広く検証されたコンセンサスに基づく枠組みを提供し、共通の課題に対する共通のアプローチを促進し、これにより協力と相互運用性を可能にします。
2. 政策は、リスクベース、結果重視、技術中立的であるべきです。政策は、技術的状況の多様性と絶え間ない進歩を反映すべきであり、異なるレベルのリスクに対処し、ネットワークやシステムの所有者や運用者が、自らのインフラストラクチャを、自らが望むセキュリティのレベルを満たすために最善と考える技術や方法で守ることができるよう、アプローチに優先順位を付けるべきです。
3. 政策は、可能な限り、市場主導のメカニズムを信頼すべきです。市場の力を活用してサイバーセキュリティを推進する政策は、変化するセキュリティ環境に後れを取らずに最大限広範な効果を達成するのに最も成功する可能性が高いと言えます。
4. 政策は、イノベーションを促進するよう、柔軟で適応可能なものであるべきです。政策は、企業が新たな課題に対する新たなアプローチを開発し、それを信頼する顧客に対して革新的な製品を届けることができるよう、柔軟かつ適応可能でなければなりません。
5. 政策は、官民連携に根ざしたものであるべきです。サイバーセキュリティは、政府と民間の利害関係者間で共通の責任です。政府は、民間部門と緊密に協力することによってのみ、デジタル経済の活力を維持しながら、サイバーセキュリティの脅威に真に対処することができます。
6. 政策は、プライバシー保護を重視して策定すべきです。悪意あるサイバー活動に対して防御しようとするいかなるサイバーセキュリティへのアプローチも、データの完全性を損なうべきではありません。サイバーセキュリティ政策は、プライバシー上の考慮事項に慎重に適合させるべきです。

これらの包括的な政策に加え、2019年に実施すべき優先事項について、BSAは、具体的に以下の通り意見を述べます。

サプライチェーン・リスクマネジメント

サイバーセキュリティ戦略で論じられている1つの重要な分野は、技術サプライチェーンのセキュリティと完全性の保護です。この戦略が発表されて以降、サプライチェーンにおける国家主導の介入、広く使用されているコンポーネントにおける重大な脆弱性の特定、サプライチェーンのリスクを緩和するための国家の行動が主張される中で、サプライチェーンにおけるセキュリティ問題が顕著になってきました。その一方で、産業界は、サプライチェーンの完全性に関するグローバルな原則を確立し、グローバルサプライチェーン全体のあらゆるレベルでのセキュリティを強化するイニシアチブを体系化することによって、サプライチェーンの確保に関するリーダーシップを発揮してきました。

グローバルサプライチェーンにおけるセキュリティ、完全性、信頼性は、デジタル経済を支え、日本のSociety5.0ビジョンを推進するイノベーションと相互連携を維持するために不可欠です。このため、BSAは、日本がサイバーセキュリティ戦略を実施する上で、サプライチェーン

[2] BSAインターナショナル・サイバーセキュリティ・フレームワークは、https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdfにおいてご覧になれます。更に詳しい情報は、https://bsacybersecurity.bsa.org/をご参照ください。

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

への脅威を低減し、悪意ある活動に対する防御を強化し、グローバルなデジタル商取引の成功に必要なイノベーションと相互運用性を可能にするよう、サプライチェーンリスク管理に対し洗練されたアプローチを優先的に採用することを推奨します。

具体的には、BSA は、日本におけるサプライチェーンセキュリティへのアプローチが以下の原則に従って策定されることを提案します。

- **裁量**　サプライチェーンセキュリティ強化策の一つには、責任ある行動を促す規範を認識し、悪意ある脅威に対抗する集団的防御を優先する、より安全なグローバルなサイバーセキュリティエコシステムの醸成があります。日本は、グローバルサプライチェーンにおいて組織的な介入を行わないことへのコミットメントを重要なメッセージとして発信することができます。

- **相互運用性**　サプライチェーンリスクを管理する政策の策定にあたり、デジタルサプライチェーン全体に渡り、国際的に認められた業界主導のセキュリティ標準を採用すべきです。このような標準に沿った政策を策定することにより、テクノロジープロバイダーによる国境を越えた革新的な製品を開発し、維持し、かつ確実にすることができ、重大なサイバー脅威に対する国境を越えた運用連携の促進を支援します。

- **協働**　政府によるサプライチェーンリスクの管理における取組みは、業界を含む主要な政府以外の関係者と協働して行うことが最も効果的です。産業界はサプライチェーンの懸念に対処するリーダーシップを強化しており、政府は、サプライチェーンセキュリティ確保とリスク管理のためのベストプラクティス策定を目的とした官民連携の協力機会を奨励すべきです。同様に、サプライチェーン脅威に関する情報共有と運用上の協力の拡大を通じて、主要国との政府間ベースでの協働が求められます。

- **透明性**　特定の外国ベンダーを、通知なしに購買プロセスから排除するといった、不透明なサプライチェーンリスク管理プロセスは、混乱を生み、他国政府による保護主義的介入を促し、グローバルビジネスの経済競争力を損なう可能性があります。例外的状況でない限り、サプライチェーンリスク管理プロセスは、影響を受ける利害関係者に対して具体的な措置を通知し、公衆に対して透明なものとすべきです。さらに、政府は、透明性の原則により、特定されたサプライチェーンの脆弱性を ISO/IEC 29147 に記載された脆弱性開示方法に従ってサプライヤーに開示する義務を負うべきです。

- **公平性**　サプライチェーンリスク管理プロセスは、決定に対して影響を受ける利害関係者が異議や不服を申し立て、申し立てられた違反に対する防御をし、過去の懸念を是正する機会を含め、紛争解決のための公正なメカニズムを確立すべきです。透明性の確保と同様に、公正な紛争解決メカニズムを確立することで、リスク軽減手法を制限することなく、確実性と予測可能性を備えた環境を整備できます。

- **イノベーション**　グローバルサプライチェーンのセキュリティ確保は、継続的な課題であり、セキュリティ技術は、新技術と新脅威によって絶えず変化する環境に適応し続けなければなりません。日本は、サプライチェーンの完全性の向上に向けた新たな技術的アプローチへの研究開発投資を通して、サプライチェーンリスクを効果的に管理する手法とテクノロジーにおける先駆的地位を維持することができます。有望な研究分野としては、ブロックチェーンベースの技術の利用、サードパーティー部品のセキュリティ問題の検査プロセス開発、サプライチェーンデータの分析及び異常検出への AI の適用などがあげられます。

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

- **執行**　国家が高度に洗練された脅威対策を提示できていても、サプライチェーンは、国家以外の者から、悪意あるサイバーセキュリティ活動、偽造、その他関連する活動による圧力を常に受けています。管轄内において、法執行を悪意ある行為者に対して積極的に継続して行うことは、日本のサプライチェーンリスク管理戦略における重要な要素です。

本原則は、日本のサイバーセキュリティ戦略のみならず、より広範でグローバルなサプライチェーンセキュリティの取組みに対して適用可能です。 BSA は、日本が、本原則を自国の政策において、また、グローバルリーダーとしての役割を通して、採用していくことを推奨します。日本は、例えば、2019 年 G-20 サミット開催国としての主導的立場、二国間及び多国間の貿易協定、国連、その他の多国間のフォーラムを通じ、本原則を推進する機会を有しています。BSA は、これらの今後の機会を有効に活用するため、日本政府に協力していく所存です。

Internet of Things

サイバーセキュリティ戦略における 2 つ目の重要な事項は、Internet of Things（IoT）のセキュリティ確保です。 IoT 機器は、個人の消費者向け技術と産業技術の双方の状況に変化をもたらし、生産性の改善、生活の質の改善、対応力の高いガバナンス及び驚くような技術的進歩を解き放つ大きな可能性を有しています。しかし、これらの機器は新たなリスクももたらすため、IoT セキュリティリスクへの対処につき、BSA は日本政府と協働していきたいと考えています。BSA は、必須セキュリティ機能、安全設計及びライフサイクル保守のためのベストプラクティス、その他関連機能に関するガイダンスを提供する IoT 機器セキュリティ基準の確立を支援しています。

実際、BSA は既に、推奨 IoT セキュリティ基準の公表を目指している米国国立標準技術研究所（NIST）及び IoT デバイス認証スキームの開発を目指している欧州ネットワーク・情報セキュリティ機関（ENISA）を含む、基準策定に向けた取組みに対して情報提供を行っています。これらが示唆するように、IoT セキュリティ基準策定に向けた取組みにとって重要かつ必要なことの 1 つは、当該基準が世界中における同様の取組みと継続的に整合性を保っていることです。相互運用性は、グローバルな商取引及びサイバーセキュリティ促進上、基礎的な役割を果たすものです。IoT 分野におけるガイダンスや規制に矛盾があると、デジタル貿易及び機器のセキュリティの両面において悪影響を及ぼします。また、IoT 機器は、機能、能力及びリスクに関して極めて幅広い多様性があることを考慮し、IoT セキュリティ基準は、リスクベースで柔軟性を有するものであることが重要です。

これらの優先順位に従って IoT 機器セキュリティ基準を策定していくよう、BSA は日本政府と協力していきたいと考えています。

セキュリティ強化に向けたクラウドコンピューティングの推進

サイバーセキュリティ戦略は、政府機関における業務の効率性とセキュリティ強化のためにクラウドコンピューティングを推進することの重要性を認識しています。この点に関し、BSA は、NISC に対して、政府のメッセージに一貫性があり、関係する政府機関や他の利害関係者において誤解がないことを確実にするため、クラウドコンピューティングに関する過去のガイダンスの一部を再検討していただけるよう求めます。特に、政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）における記載（4.1.4「クラウドサービスの利用」の箇所等）は、クラウドコンピューティング及び関連サービスがリスクを高めているような記述になっており、これについて引き続き懸念を有しています。このような記述は、クラウドコンピューテ

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

ィングのリスクがオンプレミスの IT システムよりも大きいという誤った印象を生み出す可能性があります。また、プライベートクラウド、パブリッククラウド、ハイブリッドクラウドなど様々なクラウドサービスモデルを考慮に入れることも重要であり、オンプレミスシステム同様、具体的なリスクは、どのような状況で使用されるかに基づいて評価されなければなりません。

さらに、物理的ネットワーク分離は、リアルタイムでのセキュリティ更新による恩恵を妨げることになって多くの場合よりリスクを増大させる可能性があるにもかかわらず、物理的ネットワーク分離がセキュリティ上の解決策であると示唆する同対策基準における推奨（5.2.1「情報システムの企画・要件定義」（2）a 項 参照）についても、BSA は、引き続き懸念しています[3]。

これに関連して、我どもは、政府機関全体でのクラウド導入を加速し、かつ、クラウドサービスの安全性評価の手続きを改善しようとする日本政府による取り組み、特に経済産業省及び総務省によって現在行われている取組みを評価しています。また、CIO 連絡会議が決定した「政府情報システムにおけるクラウドサービスの利用に関する基本方針」において「クラウド・バイ・デフォルト原則」を推進していることは大変意義ある取組みであり、経済産業省及び総務省におけるクラウドサービスに関する取組も、この方針に適合し、かつ、最大限に活かしたものとなるようにしていただきたいと私どもは考えております。経済産業省と総務省が現在検討している政府機関が利用するクラウドサービスの安全性評価の仕組みに関し、BSA は、当該制度が世界的に他の政府機関クラウド安全性評価及び認証スキームと相互運用可能であり、国際的に認められた標準に適合するように制度設計する重要性を、今一度強調したいと思います。また、政府機関全体において、確実に、統一的に、リスクベースのアプローチと多層的な防御システムが適用されるようにすべきです。このようにすることによって、日本が提案するクラウド安全性評価の仕組みは、将来当該評価に従う公共部門の組織において、安全で効果的なクラウドコンピューティングサービスの採用を促進することになると考えます。

国際的なキャパシティ・ビルディング

BSA は、サイバーセキュリティ戦略で示された国際的なサイバーセキュリティ・キャパシティビルディングに対する日本のコミットメントを強く支持します。サイバーセキュリティは、国際的な協調的解決を必要とする国境を越えた課題です。サイバー空間の安全性確保は、各国がインターネット・エコシステム全体の強化のために共に協力し合うことによってのみ実現されます。そのために、開発途上の国々によるサイバー防衛能力とサイバーガバナンス能力強化に目的を絞った支援は重要であり、BSA は日本のリーダーシップを歓迎します。BSA は、日本政府が、多くの国々が未だ新たなサイバーセキュリティ法の策定又は施行の初期段階にある東南アジア地域に注力した国際的なキャパシティ・ビルディング支援活動を維持し拡大していただけるよう、希望します。

また、日本は、特定のサイバーセキュリティ脅威への対処を目的とした多国間運用協力への参加、国際的なサイバーセキュリティ規範の策定や信頼形成に向けた手段の確立の支援、国際的サイバーセキュリティ標準策定への参加、多国間ガバナンスメカニズムへの参加等を通じて、世界的なデジタルエコシステムの強化を支援することができます。特に、日本は、今年の G20 開催国であることから、国際的規範や信頼形成に向けた手段を推進する主導的地位にあります。

人材 5.0

[3] BSA の政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）に対する意見の詳細は、https://bsa.or.jp/wp-content/uploads/bsa_20160704.pdfをご参照ください。

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

サイバーセキュリティ戦略は、戦略に示された広範な政策目標を達成するためには人材育成が必要な基盤であることを正しく認識しており、2019 年の戦略の実施において、強力なサイバーセキュリティ人材の育成を優先事項とすべきです。日本の「Society 5.0」のビジョンは、経済分野を横断する技術革新を支え、コネクテッド・エコノミーの恩恵を確実に得ることができるよう、サイバーセキュリティ専門家に対して急速に高まる需要を満たすことができる人材、即ち人材 5.0 を基盤として構築されなければなりません。

現状及び将来のニーズを満たすサイバーセキュリティ人材の育成は、長期の世代に渡って将来の実務家を教育することから始まります。特に重要なのは、現在の人材における著しい不均衡に対処するために、より多くの女子学生がサイバーセキュリティを含むコンピューターサイエンス教育の道を進むインセンティブを与えることです。BSA 会員企業は、サイバーセキュリティ能力開発のための代替的なコースを提供し、ソフトウェア業界において多数派ではない女性等の更なる参加を促進するプログラムに対して多額の投資を行っています。政府が、これらの取組みに対して投資を行うことで、その規模と有効性が大幅に拡大する可能性があります。

結び

BSA は、サイバーセキュリティにおける NISC のリーダーシップに敬意を表するとともに、NISC が協力的なマルチステークホルダー・アプローチを取られていることについて感謝します。サイバーセキュリティ戦略に基づき 2019 年度に実施すべき施策の検討において BSA 及び会員企業の本意見が有用なものであること、また、本取組みについて引き続き NISC と協力していけることを願っております。ご質問やご意見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