2015年9月3日

「サイバーセキュリティ２０１５（案)」に関する意見

BSA｜ザ・ソフトウェア・アライアンス

BSA｜ザ・ソフトウェア・アライアンス[1]（以下「BSA」）は、「サイバーセキュリティ２０１５（案)」（以下「本計画案」という。）に対し、以下の通り意見を提出します。

日本において、サイバー攻撃へのレジリアンシーを高め、強化することは重要な目標です。BSAの会員企業にとってもサイバーセキュリティは極めて重要であり、我々は、日本政府の上記目標及び取組を共有し賛同します。

BSAの会員企業は、民間向けか政府向けを問わず、製品及びサービスの全てについて、最高水準の完全性を維持することを目指しています。また、サイバーセキュリティ製品及びサービスの提供者でありかつユーザーとして、世界中の政府機関と協働した経験を数多く有し、各政府のサイバーセキュリティポリシーに対する取組みに貢献してきました。BSAは、本件に関する適切な支援を日本政府に対してさせていただいと考えております。

以下、本計画案に対するコメントを提出致します。

I. 総論

1. 官民連携

サイバーセキュリティの体制が効果的であるためには、国内及び世界の民間団体との協力が、明確な役割として組み込まれている必要があります。この点、グローバルなソフトウェア、IT企業は、最先端のソフトウェア・ソリューションや、企業向けベストプラクティスを開発する豊富な経験を有しております。

日本政府は、現在、業界ごとのサイバーセキュリティ・ガイドラインを策定していますが、私たちは、その過程において、官民連携を活用すること、及び国際調和を達成するために国際基準

[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, Altium, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, PTC, salesforce.com, Siemens PLM Software, Symantec, Tekla, The MathWorks, Trend Micro 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。

を採用することを強く要望します。内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）が本計画案を完成し、実行し、日本のサイバーセキュリティを高めるために各政府機関・団体の責任範囲について取り決める際、民間団体が必要に応じた役割を十分に担うことができるよう要望します。

2. サイバーセキュリティに関する国際的アプローチ

どのような国又は政府であっても、単独でサイバーセキュリティリスクを解決することはできません。非政府組織や国際的な連携先と協働することは、サイバーセキュリティの効果的なアプローチにおける欠かせない要素です。国際市場において成長し続けられるよう日本企業の競争力を維持しつつ、サイバースペースにおける安全確保の運用効率を高めるためには、国内ポリシーを策定する際に、グローバルな視点を持つことが重要です。

従って、日本政府においては、地域間及びグローバルでの情報共有及び保護を最大化するために、国際的、自主的かつ市場主導の基準を活用することを強く求めます。

3. 情報共有

BSAメンバー企業は、堅牢な情報ネットワークの確保とサイバー攻撃からの回復を確実とすることに全力を傾けています。この目標を達成するためには、脅威とアタックへの防御の備えに注力した、包括的なリスク・ベースのアプローチをとること、また、影響を受けたネットワークの早期かつ適切な復旧のメカニズムを策定することが必要です。サイバーセキュリティに対する脅威、脆弱性、インシデントといった情報につき、影響を受ける者と攻撃からの防御手段を開発する者が共有できるようにすることは大変重要です。攻撃は、民間か政府機関かを問わず、また、国を超えてなされるため、情報共有に関する政策は、官民で又は民間企業・政府機関のそれぞれの間での情報共有を促進するものとすべきです。この観点から、BSAは、政策決定者に対し、有効なサイバー脅威情報共有のために以下の６つの基本原則を推奨しています。

(1) 適切な目標を定めた政策を通じて、情報の共有及び受領に対する法律又は規制上の潜在的影響を明示的に限定することにより、民間機関が、国内及び海外において、サイバー脅威の指標に関する情報を他の民間機関又は政府と自発的に情報共有できる権限を付与すること
(2) サイバー脅威の指標を適時に共有することを妨げずに、サイバー脅威情報の共有により影響を受ける者のプライバシーを保護する適切な政策を策定すること
(3) 関連するサイバー脅威の情報を民間部門と共有する権限を政府機関に付与し促進すること、及び当該情報共有の期間を早めること（自動メカニズムによる場合を含む）
(4) 民間機関による政府及び民間双方との間の情報共有を促進すること、共有される情報について義務づけられる契約上の条件を最小限にすること、並びに、影響を受ける当事者が適切な取引上の合意を締結できるような柔軟性を提供すること
(5) 官民の情報共有のための民間のポータルを構築すること、及びこれらの情報共有及びその

他の状況に対する賠償保険が提供されるようにすること。

(6) 共有されたサイバー脅威の情報は、受領者によりサイバーセキュリティ促進にのみ用いられ、その他の目的に用いられず、及び、政府と情報を共有した場合にはその情報はサイバーセキュリティ促進又は限定された法の執行にのみ用いられることを保証すること

BSAは、本計画案を最終化する際、日本政府が上記の原則を考慮するよう求めます。

II. 各論

1. 経済社会の活力の向上及び持続的発展

(1) 1.1. 安全なIoTシステムの創出 (3)IoTシステムのセキュリティに係る制度整備(2-3頁)

IoTシステムのセキュリティに係る制度整備に関しては、脅威モデルを定義することなくして、開発側が脅威を軽減することは不可能であるため、(3)に記載される全ての項目は、各省により軽減すべき脅威モデルを定義した上で実行されるべきです。従って、「各省により、下記各項目において軽減すべき脅威モデルを定義した上で」との文言を、(ア) の項目が始まる前に追加して記載するのが良いと考えます。

1.1.(3)の(ア) では、「経済産業省において、IPAを通じて、IoTシステムに含まれる機器等に関して、攻撃事例や利用形態を基に整理を行い、総合的なガイドラインと基準の確立に向け、脅威分析とセキュリティ対策の明確化を図る。」と記載されています。この点、日本政府が国内向け独自基準を策定するのではなく、国際的、自主的かつ市場主導的な基準を活用することを強く求めます。サイバー脅威がグローバルなものであることを鑑みれば、効果的なサイバーセキュリティ戦略は、その効果を確実にするために国際的な視点が必要です。従って、本項目を以下のように修正することを要望します。

「経済産業省において、軽減すべき脅威モデルを定義した上で、IoT及びサイバーフィジカルシステムへの脅威シナリオ及び攻撃についての国際的なベストプラクティス及び評価を参考にしつつ、IPAを通じて、IoTシステムに含まれる機器等に関して、攻撃事例や利用形態を基に整理を行い、国際的かつ自主的基準に基づいた総合的なガイドラインの確立に向け、脅威分析とセキュリティ対策の明確化を図る。また、その際には、製品開発側にも調査を行い、脅威軽減に向けた努力に関する背景知識を得るものとする。」

(イ)についても国際的な経験が有益であることは同様です。従って、(イ) の記載について、「総務省において、軽減すべき脅威モデルを定義した上で、国際的なベストプラクティス及び評価を参考にしつつ、IoTシステムに関する横断的な取組の1つとして、ウェアラブル端末等のM2M機器の運用の実装上のセキュリティに係る横断的なガイドライン策定の検討を実施する。」と修正することを要望します。

(ウ)についても、「経済産業省において、軽減すべき脅威モデルを定義した上で、国際的なベストプラクティス及び評価を参考にしつつ、エネルギー分野におけるIoTのセキュリティガイドラインとして、スマートメーターのセキュリティの評価技術・手順の実証を行う。」と修正することを要望します。

(エ)についても、「厚生労働省において、軽減すべき脅威モデルを定義した上で、国際的なベストプラクティス及び評価を参考にしつつ、医薬医療機器法上の医療機器のサイバーセキュリティについて検討を進める。」と修正することを要望します。

(2) 1.1. 安全なIoTシステムの創出 (4)IoTシステムのセキュリティに係る技術開発・実証(3頁)

1.1.(4)の(ウ)では、「経済産業省において、CSSCにおける制御システムのテスト環境を用いシステム全体の脅威分析、リスク評価を行う技術を開発し、評価・認証制度やサイバー演習へと活用する。」と記載されています。この点、日本が国際的、自主的で、かつマルチステークホルダープロセスを通じて開発された認証制度を採用することを強く求めます。そして、そのような基準の一つが世界の共通基準（Common Criteria） であり、これを採用するのが本件においても有益と思われます。また、IoTの分野毎(例えば、ウェアラブル機器、原子力施設等)に求められる評価・認証制度に留意し、それぞれ異なったアプローチにより開発することが重要です。

従って、本項目の記載は、「経済産業省において、世界的でスケーラブルな認証制度及び基準に則した制御システムのテスト環境を用い、システム全体の脅威分析、リスク評価を行う技術を開発し、評価・認証制度やサイバー演習へと活用する。その際には、Common Criteriaのような国際的アプローチを採用し、世界の知見を活用するとともに、世界規模での脅威低減に貢献できるようにする。また、IoTの分野毎に求められる異なる評価、脅威モデルの定義及び認証制度に留意するものとする。」と修正することを要望します。

経済産業省は、日本及びグローバル企業が参加する「ロボット革命イニシアブ協議会」の「IoTによる製造ビジネス変革ワーキンググループ」を通じて、IoT事業の利用事例に関して、日本及び海外からの情報共有を図っています。しかしながら、本計画案には、この経済産業省の重要な取組みが盛り込まれていません。世界的な競争力を実現するには、日本の産業界がIoT分野における専門知識を有する国際的なIoTコンソーシアムと連携し協働することが重要です。

従って、1.1.(4)に（キ）として、下記を追加することを要望します。

「経済産業省において、国際的IoTコンソーシアムにより開発された事業モデル及び利用事例を実現するIoTアーキテクチャに基づいた実用的なセキュリティフレームワークに関する調査を実施し、これら国際的IoTコンソーシアムとの共同実証実験の実施について検討する。」

(3) 1.2. セキュリティマインドを持った企業経営の推進 (3)組織能力の向上(4-5頁)

1.2.(3)の(エ)では、「経済産業省において、情報システム開発・運用に係るサプライチェーン全体のセキュリティ向上のため、リスクの高い丸投げ下請や発注者が把握できない多重の再委託などを防止し、情報システム開発・運用に係る取引の適正化を図るための制度整備を行う。」と記載されています。

しかしながら、現在の世界規模の供給モデルの中で、多重の再委託を禁止することは不可能であり、一社に全ての清算を要求することは現実的でないことから、本記載について懸念を有しま

す。コスト削減効果と効率を高めるために必要な委託と再委託から生じるサプライチェーンリスクの管理については、リスクベースアプローチを採用するべきです。従って、本項目について、以下の文言に修正することを要望します。

「経済産業省において、情報システム開発・運用に係るサプライチェーン全体のセキュリティ向上のため、情報システム開発・運用に係る取引の適正化を図るための制度整備を行う。」

(4) 1.3. サイバーセキュリティに係るビジネス環境の整備 (1)サイバーセキュリティ関連産業の振興(5頁)

2020年に開催する東京オリンピック・パラリンピックを控え、日本ではサイバーセキュリティに関する関心と懸念が高まっています。しかし、これらの懸念は、未だ、日本のサイバーセキュリティに係る課題を革新的な製品とサービスにより解決していくために業界と活発な議論を行うまでには至っていません。サイバーセキュリティ問題に適切に取組むためには、政府が、官民連携の構築と強化を促進し、リードしていく必要があります。従って、1.3.(1)に、(オ)として以下を追加することを要望します。

「経済産業省において、2020年の東京オリンピック・パラリンピック及びそれ以降に向け、日本のサイバーセキュリティの進展を妨げているセキュリティにおける障害について理解し、効率的で革新的なサービスと製品によりこれらの障害を克服するため、民間との対話及び連携を推進する。」

2. 国民が安全で安心して暮らせる社会の実現

(1) 2.2. 重要インフラを守るための取組 (1) 重要インフラ防護の不断の見直し (13頁)

2.2.(1)の(ウ)では、「内閣官房において、需要インフラ分野以外の民間企業をサイバー攻撃から保護するために、既存の重要インフラ分野いかんに関わらず情報共有等の取組の対象とすべき企業の範囲について検討を行う。」と記載されています。

日本政府が、サイバーセキュリティ上の懸念を解決するために情報共有が重要であることを十分に認識されていることは大変素晴らしいことですが、本記載のままですと、重要インフラ分野以外において、任意・匿名ではなく、強制的な情報共有の対象となるようにも読み得るため、任意・匿名であることを明確化すべきと考えます。即ち、流動的な脅威環境においては、パートナーシップ、信頼及びインセンティブの上に成り立つ情報共有が最も効果的であり、企業等がサイバーリスクを管理する上で最も良く機能すると考えます。また、上記のとおり（情報共有についての詳細意見は本意見I.3.を参照)、情報共有に関して適切な賠償責任の制限が提供されることは非常に重要です。

(2) 2.3. 政府機関を守るための取組(15頁-16頁)

2.3. の(ア)では、「内閣官房において、新たに直面した脅威・課題への対応について、政府統一基準を始めとした規程に適時反映するため、政府統一基準等の次期改定に向けた検討を順次進める。」と記載されています。

上記のとおり、BSAは、日本政府が、政府機関の保護のために、世界的なベストプラクティス

及び国際基準を採用すべきであると考えており、最新の脅威から防御するために世界中から最も優れた技術を日本において展開することを困難とするような日本独自の基準を策定することがないよう要望します。

2.3.(1)の(オ)、(カ)では、経済産業省において、政府調達推進のために又は暗号化モジュールに関し、評価及び認証手続の改善又は試験及び認証制度の普及を図る旨記載されています。これらの試験、評価及び認証手続についても上記同様、各政府機関において試験済みや認証済みの製品の迅速な展開が可能となるよう、国際的なベストプラクティス及び基準に則したものとしていただけるよう要望します。

III. 結び

BSAは、本意見提出の機会に感謝致します。ＮＩＳＣ、本件の関連省庁及び関係者の方々にとって、政策、ルール及びガイドラインを策定する上で本意見が有益であれば幸甚です。なお、BSAが意見を提出した懸念事項や要望について、いつでも更に説明や補足をさせていただきますので、そのような機会をいただければ幸いです。

以　上