Viewpoint

在日米国商工会議所意見書

日本のサイバーセキュリティにおける新たな計画の推進
Implementing Japan's New Cybersecurity Strategy

インターネット・エコノミー・タスクフォース
Internet Economy Task Force

2015年7月まで有効
Valid Through July 2015

英語正文

在日米国商工会議所 / The American Chamber of Commerce in Japan

〒106-0041, 東京都港区麻布台 2-4-5, メソニック39MTビル10階
Masonic 39 MT Bldg. 10F, 2-4-5 Azabudai, Minato-ku, Tokyo 106-0041

Tel +81 3 3433 7358
Fax +81 3 3433 8454
external@accj.or.jp

http://www.accj.or.jp/en/advocacy/viewpoints

ACCJ Viewpoint

RECOMMENDATIONS

The "2014 Cybersecurity Strategy" (2014 Cybersecurity Strategy) document, released in May 2014 along with the "International Strategy on Cybersecurity Cooperation," separately released in October 2013, offer a roadmap and timetable for the Government of Japan's (GOJ) planning with respect to the mounting cybersecurity threat. We understand that they reflect the Abe administration's concern with the dramatic increase in cyber-attacks and its commitment to take active steps to protect Japanese security and economic interests. More recently, the Liberal Democratic Party (LDP) with the support of most other parties has announced plans to introduce legislation in the Diet to establish a "Cybersecurity Center" in the Cabinet Secretariat and to give the new organization formal authority to create and implement a unified cybersecurity strategy across the government as the executive agency for the Information Security Policy Council.

The American Chamber of Commerce in Japan (ACCJ) welcomes these strategy documents and the proposed new legislation as the start of what should be a vibrant and open debate on possible measures Japan may be taking unilaterally and in cooperation with the United States and other nations to protect our common cyberspace. We urge quick implementation of the proposals contained in these documents, following broad consultation among public and private sector stakeholders. And in this context, we urge the GOJ to:

- Centralize planning and administration in the "Cybersecurity Center";
- Adopt an information security management "baseline";
- Take a coordinated approach to cybersecurity standards;
- Introduce an accreditation framework for government cloud computing;
- Ensure new security measures are non-discriminatory; and
- Increase cooperation with the United States on cybersecurity.

In the sections below, we elaborate on the key recommendations that we believe would further

提言

2014年5月に公表された年次計画「サイバーセキュリティ2014」と、2013年10月に公表された「サイバーセキュリティ国際連携取組方針」は、高まるサイバーセキュリティの脅威に対する日本政府の取組みに関し、行程表とその予定を提示している。これらの計画は、安倍政権のサイバー攻撃の劇的な増加に対する懸念と日本の安全保障と経済的利益を守るための積極的なコミットメントを反映したものであるといえる。さらに最近では、「サイバーセキュリティセンター」を内閣官房に創設し、情報セキュリティ政策会議の執行機関として新設されるセンターに、政府機関全体の統一された戦略の立案と実行の法的権限を与える法案が、自民党など与野党6党によってへ提出された。

在日米国商工会議所(ACCJ)は、サイバー空間を保護するために日本単独または米国や他国と協力してとり得る措置に関する活力あるオープンな議論の出発点として、これらの計画と新たな法案を歓迎する。ACCJは、官民のステークホルダーとの幅広い協議を通じて、本意見書に含まれる提案の早期実施を求める。以上を踏まえ、ACCJは日本政府に以下の取組みを提案する。

- 「サイバーセキュリティセンター」に関する政策の企画と運営の集約化
- 情報セキュリティマネジメントにおける「ベースライン」の導入
- 政府におけるサイバーセキュリティの基準設定について、調和のとれたアプローチの採用
- 政府のクラウドコンピューティングについての認証枠組みの導入
- 新たなセキュリティ対策における内外無差別性の保証
- 米国と日本のサイバーセキュリティ協力の強化

以下にACCJが、日本政府の取組みが成功裡に実現するために役立つと考えている主要な提言を詳述する。

問題点

「サイバーセキュリティセンター」に関する政策の企画と運営の集約化

ACCJは、内閣官房の下にサイバーセキュリティセンターが創設される案に敬意を表すと共に、同機関が多面的なミッションを遂行するために、必要な予算と人員が確保さ

contribute to the successful realization of the GOJ's objectives.

ISSUES

Centralize Planning and Administration in the "Cybersecurity Center"

The ACCJ applauds the recommendation to establish the "Cybersecurity Center" under the Cabinet Secretariat and urges that be given the budget and human resources necessary to accomplish its multi-faceted mission. We agree that reorganization of the GOJ's planning and administrative approach to cybersecurity is urgently required in the light of the growing existential threat to Japan's economy and the security of its citizens presented by the cybercrime, cyber espionage and cyber targeting of critical infrastructure. We recommend that the legislation provide the new Center with a clear mandate to oversee (not merely coordinate) the diverse responsibilities and programs of existing ministries, thereby creating a strong and accountable focal point for the protection of domestic infrastructure, the promotion of cyber research, the training of key personnel and the implementation in and out of government of relevant standards. The new Center should take the lead in cooperation with national and local police forces in countering cybercrime threats domestically. This will allow the Self Defense Forces (SDF) to concentrate their limited resources on responding to national security threats as directed by competent civil authority.

Adopt an Information Security Management "Baseline"

In parallel with the creation of a "Cybersecurity Center," Japan needs to strengthen the legal basis for government information security management and adopt a framework that sets a consistent approach for baseline risk management. An example is the Federal Information Security Management Act (FISMA) in the United States, which has driven both greater accountability and cooperation across all U.S. government agencies in cybersecurity matters. At the same time, agencies need the flexibility to manage their infrastructures in line with mission requirements. In today's online environment, different agencies may take different approaches to implementation, using on-premise technology, hybrid models or entirely cloud-based solutions. Security cannot be achieved through a one-size-

れることを要望する。ACCJは、サイバー犯罪、サイバー諜報活動、重要インフラに対するサイバー脅威といった日本経済や国民の安全に対する脅威が増大する中で、日本政府によるサイバーセキュリティ政策の企画と管理に関し、アプローチの再調整が急務であることに同意する。ACCJは、法案によって、新たなセンターに既存の各省庁における多様な責務とプログラムを(単に調整だけでなく)監視する権限が付与されることで、このセンターが、国内の重要インフラ防護、サイバーセキュリティ研究の促進、サイバーセキュリティ人材の育成、政府内外への適切な国際標準の適用のため強固で権限のある中心機関になることができると考える。さらに国内のサイバー脅威に対処する上で、新設されるセンターは、警察庁と都道府県警察との協力を主導すべきである。この取組みによって、自衛隊は、管轄権を有するしかるべき機関の指示のもと国家安全保障上の脅威に対応するために、限られた資源を集中させることができる。

情報セキュリティマネジメントにおける「ベースライン」の導入

「サイバーセキュリティセンター」の設立と並行して、日本政府は政府情報のセキュリティマネジメントの法的基盤の強化と、リスクマネジメントに関するベースライン(組織の対策基準)における一貫したアプローチを設定する枠組みの導入が必要である。例としては、サイバーセキュリティに関して米国の政府機関全体にわたり、より広範囲な責務を与え、協力を促進させた、連邦政府情報セキュリティマネジメント法(FISMA)が挙げられる。同時に各省庁は、政策目的に沿って自身が管轄するインフラを管理するために、柔軟性を保つ必要がある。現在のオンライン環境の中で各省庁は、オンプレミス、ハイブリッドモデル、またはクラウドベースのソリューションといった、異なるシステムを利用することが想定される。したがって、セキュリティの確保は、画一的アプローチでは実現されない。そのため、秘密情報の共有に関する新たなルールを策定する上で、既に合意されている国際標準に基づくリスクマネジメントのアプローチが役立つ。さらにこれらのルールには、民間セクターの企業が攻撃報告をしても罰則を受けない保証として「セーフハーバー」の機能や、情報共有の障壁となる情報の「過剰な秘密指定」に対する安全措置(セーフガード)も含めるべきである。2009年から、ACCJは、日本政府に多様性とイノベーションを阻害しない一貫性のある政府の調達ガイドラインを要請しており、情報セキュリティのベースラインアプローチは、この目標達成のサポートとなると考えている。政府機関全体を対象としたサイバーセキュリティ対策のモニタリングと実施も、政府機関全体の調達戦略を設定する

fits-all approach. A risk-management approach, based on agreed international standards, can help shape new rules for the sharing of sensitive information. Such rules should also allow for a "safe harbor" mechanism to ensure that private sector entities are not punished for reporting attacks and include safeguards against "over classification" of information, which can create barriers to sharing. The ACCJ has been on record since 2009 in calling for a consistent government procurement guideline that would not stifle diversity and innovation, and we believe an information security "baseline" approach will help achieve this objective. The monitoring and enforcement of government-wide cybersecurity measures will also greatly strengthen the hand of the government Chief Information Officer (CIO) in setting a government-wide procurement strategy.

Take a Coordinated Approach to Cybersecurity Standards in Government

Any new administrative and legal framework for cybersecurity will require a strong technological basis. The 2014 Cybersecurity Strategy appears to assign a central role in research and standards development to the Ministry of Economy, Trade and Industry's (METI) Information Technology Promotion Agency (IPA). We believe that a coordinated approach to developing cybersecurity standards is essential and that adequate budgetary and personnel resources are required for success. For this reason, it is important for the GOJ to clarify the respective roles in setting standards for cybersecurity of the new Cybersecurity Center in the Cabinet Secretariat and METI's IPA, as well as the part to be played by the Japan Industrial Standards Committee (JISC), which is also under METI. We are concerned about unnecessary duplication of activities and lack of cooperation among agencies with differing mandates. These problems have already arisen. In addition, while new and strengthened security standards are important, the GOJ must guard against mandating the use of technologies and standards unique to Japan for achieving its cybersecurity goals. Technology in the security area is evolving very rapidly and premature standardization, particularly when conducted in isolation from international trends, can stifle innovation and lead to a lagged and ultimately ineffective response to security threats. We note that the October 2013 International Strategy document pledges GOJ

上で、政府情報化統括責任者（政府CIO）の権限を大幅に強化することにつながる。

政府におけるサイバーセキュリティの基準設定についての調和のとれたアプローチの採用

いかなるサイバーセキュリティの新たな法的枠組みも、強固な技術基盤が必要となる。サイバーセキュリティ2014では、経済産業省所管の情報処理推進機構（IPA）に、評価基準の推進における中心的な役割を担わせている。サイバーセキュリティの評価基準の推進において、調和的なアプローチは不可欠であり、十分な予算と人的資源も成功には必要となる。以上のような理由から、日本政府にとって、内閣官房におけるサイバーセキュリティセンター、IPA、同じ経済産業省下の日本工業標準調査会（JISC）といった、サイバーセキュリティの評価基準を設定する各組織の役割の明確化が重要になる。ACCJは、既に顕在化している活動の不必要な重複や、異なった権限による省庁間協力の欠如について懸念している。さらに、新しく強化されたセキュリティ評価基準は重要であるが、日本政府は、サイバー目標を達成するために、日本独自の標準や技術の利用を義務化することを、避けなければいけない。セキュリティ領域における技術は急速に進展しており、とりわけ国際標準から離れた未成熟な基準はイノベーションを妨げ、セキュリティの脅威に対して遅延しかつ有効でない対応をもたらす。ACCJは、2013年10月の国際連携取組方針で、日本政府がサイバーセキュリティにおける国際的な技術基準策定への協力を掲げていることを、全面的に賛同すると共に注目している。

政府のクラウドコンピューティングについての認証枠組みの導入

ACCJは日本と米国が、サイバーセキュリティにおけるグローバル・ベストプラクティスを促進させるために、新たな協力方法が検討されることを期待する。その協力機会の一つとして、政府機関のクラウド移行を支援するための、日本における認証枠組みの協同構築が考えられる。ACCJは、民間セクター全体に認証枠組みの基準およびベストプラクティスの導入を推進させるためにも、この認証システムが国際標準と一致されることを要望する。また認証システムの基準は、基準化の過程が公開された上で設定されることも重要である。これに関連して、ACCJは、官民連携のもとでサイバー攻撃に関する情報と技術を共有する日本版NCFTA創設の提言を歓迎する。日本版NCFTAによって、サイバー脅威への日米共同対処や、民間セクターのサイバー脅威への準備体制を強化するような取組みで、日本政府の主導力発揮を支援する機会が生み出されることになる。

cooperation in the creation of international technological standards for cybersecurity, which we fully support.

Introduce an Accreditation Framework for Government Cloud Computing

We believe that the United States and Japan should consider new ways of working together in developing global "best practices" for cybersecurity. One such opportunity is a possible collaboration in building an accreditation framework in Japan, which could assist government agencies in transitioning to the cloud. We urge that such an accreditation system be consistent with international security standards, as this would help encourage adoption of those standards and best practices across the private sector. It is also important that such standards be set through an open standardization process. In this connection, we welcome the recommendation to establish a Japanese version of the U.S. National Cyber Forensics and Training Alliance (NCFTA), which focuses on a public/private partnership to share threat information and cyber technologies. This will create an additional opportunity for the two countries to work together in responding to the cyber threat and support the GOJ role in providing leadership by example to private sector efforts in Japan to improve cybersecurity threat readiness.

Ensure New Security Measures are Non-Discriminatory

The ACCJ appreciates the recognition in the 2014 Cybersecurity Strategy of the need to act in ways consistent with Japan's World Trade Organization (WTO) obligations in setting new security standards and rules for procurement. We equally support the recognition of the requirement to actively consult with international cloud computing services providers in developing measures to protect critical infrastructure and promote industry best practices. To this end we recommend that the GOJ encourage the adoption of international standards and lead the way in promoting the principle of "certify once, use many times," similar to the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) for computer security certification. U.S. and Japanese companies share concerns that in India, China and other markets, new cybersecurity measures are routinely used to exclude foreign products and services and to undermine intellectual property protections. For

新たなセキュリティ対策における内外無差別性の保証

ACCJは、サイバーセキュリティ2014の中で日本政府が、新たなセキュリティ評価基準や調達ルールの設定を世界貿易機関（WTO）における協定と整合させると言及したことを高く評価する。同じく、重要インフラのための防護措置の推進と産業のベストプラクティスを向上するために、国際的なクラウドコンピューティングサービスのプロバイダと協議する取組みについても賛同する。これらの目的を達成するためにも日本政府は、国際標準の導入促進や情報技術セキュリティのためのコモンクライテリア（ISO/IEC 15408）のような、「認証は一回、利用は何度でも」という原則の普及を促進させなくてはならない。日米の企業は、インド・中国・他国の市場におけるサイバーセキュリティの新たな措置が、常に海外の製品やサービスの排除や知的財産権の保護を後回しにするための口実として利用されていることについての懸念を共有している。以上のような理由から、ACCJは、知的財産権を適切なレベル以下へと弱体化させ、データセンターの設置場所が国内外かによって、提供されるクラウドサービスの扱いを区別するような行為を避けることを、日本政府に要請する。

米国と日本のサイバーセキュリティ協力の強化

ACCJは、日本政府による情報セキュリティ技術における研究開発への多大な支援や、新たな市場セクターにおける投資や雇用を促進させようとする取組みを歓迎する。ただし、これらの取組みで透明性が確保され、海外関係者への情報公開がなされ、適切な安全措置（セーフガード）の条件が満たされるよう要望する。これらは、NATO加盟国との協定に類似したサイバーセキュリティに関する秘密情報の共有などの協力を可能にする将来の二国間協議で構築される日米間の枠組みを通して達成することができる。上記の認識により、ACCJは、サイバーセキュリティ2014でも掲げられているように、昨年度の国会で成立した特定秘密保護法に関する指針の迅速な推進と実施に賛同する。ただし、ACCJは日本政府に、透明性の確保と、今後のプロセスについて、さらに意見を述べる機会が提供されることを希望する。また、同時に、他の政府データ（例　オープンデータ）を、強固なプライバシー保護との調和のもとで、産業界が、国民や商用目的のために広く使用できることを保証する取組みについても賛同する。

結論

サイバーの脅威は、過去10年で、単独のハッカーや犯罪集団によるものから、ビジネスや経済における安全だけでなく国家の安全保障の問題へと劇的に拡大している。広範なICTの製品やサービスを日本の企業や消費者へと提供して

this reason, we urge the GOJ to avoid actions that may weaken intellectual property safeguards below an appropriate level or make a distinction between cloud services offered from data centers within Japan and those outside of Japan.

Increase U.S.-Japan Cooperation on Cybersecurity

We welcome the efforts of the GOJ to support greater research and development of security technologies and to promote investment and employment in this new market sector. However, we urge that these programs be transparent and also open to foreign participants, fulfilling appropriate safeguards. This could be achieved through a framework between Japan and the United States established in future bilateral consultation that would permit this kind of collaboration and the corresponding sharing of sensitive cybersecurity information along the lines of similar arrangements with NATO countries. In this context, we support the recommendation found in the 2014 Cybersecurity Strategy pledging quick development and implementation of guidelines for government secrecy approved by the Diet last year. We urge transparency however, and hope to be able to comment further on the process going forward. We also support parallel efforts to assure that other government data (i.e. open data) can be made widely available to citizens and for commercial use by business, consistent with strong privacy protections.

CONCLUSION

Over the past decade, cyber threats have expanded dramatically from the activities of just a few individual hackers and criminal organizations to become a matter not just of business and economic security, but of national security. ACCJ members include companies that offer a wide range of ICT products and services to Japanese enterprises and consumers, and over the years, those companies have developed innovative technologies and have acquired substantial experience for mitigating the cybersecurity challenge in many technological and regulatory environments. The ACCJ looks forward to sharing this expertise with our Japanese partners and to many opportunities for further investments in this area.

Balancing the common interest in a robust legal framework and free flow of information

いる企業を含むACCJの会員企業は、長年にわたり革新的な技術を開発し、様々な技術・規制環境の中でサイバーセキュリティの問題を軽減してきた経験を持っている。ACCJは、これらの専門的知識を日本のパートナーと共有し、この分野においてさらなる投資機会を期待している。

強固な法的枠組みと、情報の自由な流れ、言論および表現の自由における共通の利益の均衡を図ることは継続して取り組んでいる課題である。サイバーの脅威は、サイバー犯罪、ビジネス・政府によって支援された諜報活動だけでなく、エネルギーや情報ネットワークという重要インフラを標的として破壊する敵対勢力の能力向上などによっても引き起こされるように多面的な課題である。このような理由から、効果的な対応のためには、官民の緊密な連携が必要不可欠であり、情報の安全と共有の適正なバランスに関する国内での幅広い議論が求められている。情報の自由な流れ、言論の自由への日本政府のコミットメントと効果的なサイバーセキュリティ政策において、プライバシー保護とイノベーションと成長の促進は主要方針であるとの日本政府の認識をACCJは歓迎する。

ACCJ Viewpoint

and freedom of speech and expression remains an ongoing challenge. Cyber threats represent a multi-faceted challenge, stemming not just from cybercrime or business or government-sponsored espionage, but the growing ability of sophisticated adversaries to target and destroy critical infrastructure, such as energy and communications networks. For this reason, a close partnership between the public and private sectors is essential for effective response and a broad national discussion on the appropriate balance between securing and sharing information is required. The ACCJ welcomes the GOJ's commitment to the free flow of information and freedom of speech and its recognition that privacy protection and the promotion of innovation and growth also need to be core objectives for an effective cybersecurity policy.