DIGITALEUROPE | ITI Information Technology Industry Council | JEITA

【仮訳】
グローバルな情報通信技術（ICT）業界の声明
サイバーセキュリティに対する望ましい政府の取り組み
2012 年 6 月

サイバーセキュリティは、全世界の政府、社会、ならびに産業界が最優先に掲げる事項である。サイバーセキュリティを進展させる政策的アプローチは、セキュリティのニーズに応えると同時に、相互運用、情報の開示性、およびグローバル市場の維持にも対応しなければならない。そのようなアプローチがセキュリティを向上させる結果となる。適切な政策環境があれば、サイバースペースの成長および発展により生じる社会的利益を維持しつつ、セキュリティを高めることが可能である。

政府がサイバーセキュリティ関連の法律、規制その他の政策を推し進める上で、我々は政府に対し以下を順守するよう要請する。

- **透明性のある方法で、さらにサイバーセキュリティに関する利害関係者の情報を取り入れてサイバーセキュリティ政策を展開する。**政府は、透明性の高い開かれた政策決定プロセスによって、サイバーセキュリティに関連する法律、規制その他の政策すべてを展開すべきである。このことは、草案文面を公開すること、法律の公示および意見公募を可能にすることを含むがこれらに限定されない。
- **リスクマネジメントおよびイノベーションを可能にする。**政府は、市場の変化に適応でき、企業および消費者がリスクを正しく理解し、評価し、対応への措置を講じることのできる政策的アプローチを採用すべきである。リスクマネジメントへのアプローチにより、民間企業関係者が自らのネットワーク、サービスおよび資産を管理し保護するために最適な立場に立ち、市場の力や企業責任、倫理規範によってそうした活動を行うことが奨励されるようになる。
- **民間企業と協力してサイバーセキュリティ政策を展開および実行する。**ICT 業界には、サイバーセキュリティのあらゆる側面においてリーダーシップとリソースを提供できる豊富な経験がある。こうした民間企業の主導および投資を踏まえてサイバーセキュリティ政策を行えば最大の効果が生まれるだろう。政策の適応性および有効性を高めることにもつながる。
- **世界的に認識された、産業主導型の自発的合意セキュリティ基準、ベストプラクティス、保証プログラム、適合性評価計画の展開および使用を促進する。**これらのアプローチは、以下の理由でセキュリティを向上させるだろう。1)自国のみに限定した取り組みでは、世界標準規格団体に伝統的に見られる最良の専門家による評価プロセスを利用できない場合がある。2)グローバルなデジタルインフラ全体に、実績のある効果的なセキュリティ方策を配備する必要がある。3)複数の法的管轄区域における複数の矛盾するセキュリティおよび適合性評価要件を満たす必要性から、有益な安全保障が要求されるため、企業のコストが上がる。
- **国際的に標準化された評価認証の使用に努める。**政府はリスクアセスメントに基づくコンプライアンス要件を認めるべきである。また、評価結果の国際的な transportability を支持するべきである。

- **サイバーセキュリティ要件は技術を問わないよう努める。**国内製の技術を優先させるなど特定の技術を要求する指令は、その国が世界のどこかで開発されうる最先端のセキュリティソリューションにアクセスできなくなることを意味するため、セキュリティを低下させる。
- **サイバーセキュリティ要件のためには、技術の発端となる国や技術ベンダーの国籍に関わらず、技術を調達できるよう努める。**製品の安全性とは、その製品がどのように製造され、使用され、保守されるかに関連しており、誰が何処で製造するかは関係ない。政府は、サイバー空間のサプライチェーンにおけるリスクに係る認識を再検討し、ICT ベンダーが ICT サプライチェーンを管理し保護するために最適な立場に立つことを認めるべきである。また、問題解決においては、排他的貿易障壁によらず調停による解決を図るべく、産業界と連携すべきである。
- **いかなるサイバーセキュリティ要件においても、ソースコードなどの知的財産（IP）の強制的な移動または審査を回避するよう努める。**このような知的財産は事業場の機密情報であり、企業の技術革新と経済的競争力の維持にとっても重要である。
- **規範的要件は政府の機密情報や軍事ネットワークなど敏感な経済領域に限定する。**多くの政府は、機密情報および軍事ネットワークに売り込まれるセキュリティ技術に対し非常に厳しい要件を正当的に提示する場合がある。このようなシステムのための政府の入手要件を政府の他のネットワークや政府の認可したネットワーク、あるいは、民間インフラや一般企業へ拡大すべきではない。
- **機関強化、危機管理計画およびサイバーセキュリティ戦略の展開を行う。**政府は効果的なサイバーセキュリティを実現するために、CERT など独自の強い独立機関を持つべきである。政府は、可能なときはいつでも民間企業と協力し、国内、地域、および国際的なセキュリティの目的を包括的に反映させ、準備および予防を共有し、有事の際には診断および対応を行い、教育と研究のギャップに対処するという重要な役目を持っている。
- **犯人およびその脅威に集中する。**政府は、国内外を問わずサイバースペース上の動き、脅威、出来事に対応する努力をすべきであり、適切な場合には可能な限り、国境を越えた協力体制により対処すべきである。
- **教育および認知度向上に注力する。**政府は、すべての利害関係者がサイバーリスクへの対処に協力するという自らの重要な役割を認識するよう努めるべきである。政府は、サイバーセキュリティに関わるあらゆる年齢層の市民に対し、教育システムを通じて認知度を上げるよう努めるべきである。

DIGITALEUROPE(DE)

Information Technology Industry Council (ITI)

Japan Electronics and Information Technology Industries Association (JEITA)