令和２年６月１６日

サプライチェーン・リスクに関するワーキングチーム 提言

自 由 民 主 党
政 務 調 査 会
情報通信戦略調査会

Ⅰ. はじめに

2020 年、世界は、新型コロナウイルス感染症（COVID-19）という未曾有の危機に直面している。我が国は、この大きな困難の中で、国民の生命身体を最大限に守りつつ経済社会を維持・発展するため、デジタル技術の積極的な活用を進めていかなければならない。すなわち、人との物理的な接触を最小限に止めるテレワークやオンライン会議等の手段の駆使、デジタルデータを集約・分析することで可能となる人流把握とクラスター早期発見への取り組み等である。

このような営みにより、デジタル技術に対する国民の意識に急速な変化がもたらされつつある。パラダイム・シフトとも言うべき価値観の変化は、COVID-19 による社会の変動を経た「コロナ後」の時代に、新世代の無線通信技術である 5Gの本格的展開の開始と相まって、社会全体のデジタル・トランスフォーメーションを劇的に推し進めることになるであろう。

そして、それは、我々が Society5.0 と呼ぶサイバー空間と実空間が高度に融合した社会の到来を加速させることに他ならない。同時に、このことはコロナ後の時代におけるサイバー空間の安全性の確保が、我が国の焦眉の課題となることを意味している。

とりわけ、情報通信機器やソフトウェア、サービス等の幅広いデジタル製品について、その開発・製造・設置・保守・管理・廃棄等の過程で、情報の窃取・破壊や情報システムの停止等の悪意ある機能が組み込まれる「サプライチェーン・リスク」への対応の必要性は論を俟たない。政府では、これまで、政府 IT 調達及び 5Gに関する許認可等の施策を通じ、サプライチェーン・リスク対策を進めてきた。しかしながら、このリスクは政府 IT 調達や 5Gに

とどまるものではなく、中小企業も含む社会全般に関連する課題であることを意識する必要がある。仮に、悪意ある機能を組み込まれたデジタル製品が我が国の重要インフラの情報システムや制御システムに浸透すれば、我が国は社会システムのコントロールを喪失し、国民の生命身体や財産の安全を確保することが困難になる。それゆえ、5Gをはじめ重要なシステムについては、導入時のみならず、運用の段階に於いても、脆弱性を検出し、その情報を関係者で共有するための体制の構築に取り組むとともに、サイバー攻撃者を探索し、攻撃を行っている指令を遮断する等の迅速な対応を可能とするための法制度も含めた対応等について検討していくことが喫緊の課題となっている。

特に、自ら気付かないうちに組み込まれるマルウェア等により、組織内の機器・システムに対する被害にとどまらず、ネットワークを介して他者の機器・システムにも感染を広げ、社会に大きな混乱をもたらす。これを如何に防止するかは大きな課題であり、まさに現在、我々が取り組んでいる対感染症の考え方をサイバー空間に於いても確立しなければならない。いわゆる「サイバー衛生」の観点に立ち、サプライチェーン・リスクへの対応に今この瞬間にも取り組みを進めていく必要がある。

本ワーキングチームにおいて行った有識者からのヒアリングの結果、後述するように我が国のサプライチェーン・リスクへの対応は極めて脆弱であることが明確となった。また、このサプライチェーン・リスクという重大なリスクに対して、国民の意識も必ずしも高いとは言えない状況にあり、あらゆる手段を総動員することによって、速やかにそのリスクの顕在化を防がねばならない。

喫緊の課題については早急に対策を講じていく必要があり、中長期的にはサプライチェーン・リスクを含むサイバーセキュリティへの対処能力の向上のために一元的な組織を実現し、我が国のサイバーセキュリティ体制の抜本的な強化を目指すべきである。

本ワーキングチームは、Society5.0 社会を迎えるにあたって必要となるサプライチェーン・リスク対策をはじめとするサイバーセキュリティ戦略を議論するため、2019年10月、自由民主党政務調査会により情報通信戦略調査会に設置された。ワーキングチームのメンバーは、COVID-19による難局の中でも、オンライン会議ツールも活用し、外部の専門家からのヒアリングや政府関係機関からの政策の推進報告を受けつつ、サイバーセキュリティ戦略についての集中的な討議を重ねてきた。

本提言は、そうした討議の結果得られた我が国のサイバーセキュリティ政策

上の様々な課題を提示するとともに、それらに対して我が国が取るべき具体的な手段を指し示すものである。

政府においては、本提言の内容を今後のサイバーセキュリティ政策と予算策定に着実に反映するとともに人員の大幅な拡充を含む体制の抜本的強化を図ることで、コロナ後の時代における国家としてのサイバー能力の抜本的な強化に取り組むよう、ここに強く要請する。

II. 問題の所在

ワーキングチームが実施したヒアリングでは、サプライチェーン・リスク対策を中心とするサイバーセキュリティ確保に向けた多くの課題が指摘された。ワーキングチームとしては、かかる状態は極めて深刻であり、早急な対策が必要であると認識する。

1. サプライチェーン・リスク対策等における課題

(1) **検証能力の不足**：サプライチェーン・リスクの検証にあたっては、情報通信システムのハードウェア及びソフトウェアの脆弱性を検出し脅威分析を行う必要があり、極めて高度な技術力が求められる。我が国において、こうした能力を有する人材は限られている。昨年度より脆弱性検出技術の開発が途に就いた段階であり、技術的検証能力は不十分な状況にある。

(2) **運用者側のスキルの問題**：5Gはこれまで ICT が利用されてこなかった様々な分野や地域における導入が見込まれるが、それらの利用を支えるローカル5Gの運用者にあっては、ICT スキルが高度ではない可能性も想定される。したがって、5Gの機器やシステムにおいて何らかの脆弱性が発見された場合、運用者側のみで迅速・効果的な対策を図るのには限界がある。

(3) **ベンダと運用者の情報共有の不足**：ローカル5Gを含む5Gネットワークについて、ベンダと運用者の間で、5Gセキュリティに関する様々なリスク情報等が共有されないために的確な対応が取れず、インシデントが発生するおそれがある。

(4) **ソフトウェアに関する継続的リスク対策の必要**：５Ｇ特定基地局の開設計画の認定やローカル５Ｇに関する免許の交付、第201回国会で成立した特定高度情報通信技術活用システムの開発供給及び導入の促進に関する

法律に基づく措置を通じ、５Ｇ導入時におけるサプライチェーン・リスク対策の制度的枠組みが整備されつつある。他方で、システム運用開始後もソフトウェアのアップデートが継続的に発生するが、その際に悪意の攻撃により被害が生じる可能性がある。

(5) **政府調達に加えた横串的対応の必要**：政府では、政府機関の IT 調達や 5G におけるサプライチェーン・リスク対策を進めている。しかし、Society 5.0 におけるサイバー空間は、実空間と融合し、あらゆるシステムが複雑かつ有機的に相互に依存する関係を持つこととなる。現在も、政府調達や情報通信といった分野ではサプライチェーン・リスク対策の取り組みは実施されつつあるが、対応が不十分な分野においてインシデントが発生すれば、他分野にも影響が波及していくおそれがあり、安全保障の観点からも大きな課題である(注１)。しかしながら、現状では、国民生活や社会経済活動に大きな影響のある重要なインフラや情報について、分野横断的に横串を通したサプライチェーン・リスク対策は不十分な状況にある。

（注１）主なインシデント事例は別紙を参照。

(6) **少数のベンダによる寡占の問題**：5Gの機器やシステムについての市場シェアは、世界的にも少数の外国ベンダによって占められており（注２）、通信事業者にとってのベンダの選択肢は限られ、サプライチェーン・リスクが大きくなっている。

（注２）主要通信機器の世界シェア

2019年 サーバー世界シェア(出荷台数:1175万台)	
デル 【米国】	17.4%
HPE/新華三集団(ニューH3C)【米国/中国】	15.4%
浪潮集団(インスパー) 【中国】	8.7%
聯想集団(レノボ) 【中国】	6.4%
華為技術(ファーウェイ) 【中国】	5.2%
その他	46.8%

出所: 米IDC

2018年 ルーター世界シェア(売上高:39.6億ドル)	
シスコシステムズ 【米国】	60.1%
華為技術(ファーウェイ) 【中国】	16.1%
中興通訊(ZTE) 【中国】	3.9%
新華三集団(ニューH3C) 【中国】	3.1%
ジュニパーネットワークス 【米国】	2.5%
その他	14.3%

出所: 米 Gartner

2018年 携帯基地局世界シェア(売上高:327億ドル)	
華為技術(ファーウェイ) 【中国】	30.9%
エリクソン 【スウェーデン】	27.0%
ノキア 【フィンランド】	21.9%
中興通訊(ZTE) 【中国】	10.9%
サムスン電子 【韓国】	4.7%
その他	4.6%

出所: 英 IHS Markit

(7) **検証体制の問題**：サプライチェーン・リスクについて、総合的・戦略的に検証できる体制が未整備である。

2. サイバーセキュリティ関連情報の取扱いについての課題

(1)「通信の秘密の保護」等のクリアーが課題に：様々なサイバー攻撃に適切に対応するためには、通信事業者等において、通信メタデータを効率的に活用し、迅速に積極的なサイバー防護措置（アクティブ・ディフェンス）を講じていくことの重要性が指摘されている。他方、我が国では、サイバーセキュリティの確保が目的であっても、通信メタデータを活用するには、個々の対策手法ごとに通信の秘密に関する解釈の整理が必要である。通信の秘密の保護は極めて重要である一方で、我が国ではこのような整理に時間を要するために、攻撃者の攻撃手法の進化に対して防護を行う通信事業者側が迅速に対応できないおそれがあり、国際連携によるサイバーセキュリティ確保のための対応にも支障が生じる事態に陥ることも懸念される。

(2) サイバー攻撃事案に係る情報共有のためのインフラが未整備：昨今の相次ぐ民間企業を狙った高度なサイバー攻撃事案に関連し、その情報共有や公表のあり方が様々な場で議論されている。攻撃者に係る情報を迅速かつ的確に共有し、我が国全体で高度なサイバー攻撃に対応するためには、情報共有を行う相手の信頼性を保証する仕組みが必要となるが、我が国では民間を対象としたクリアランス制度が整備されていないために、機密性の高い情報の共有が進んでいない。また、被害拡大防止のために、技術情報の共有を推進すべきである一方、事案対処中等の対策が十分に講じられていない段階で技術情報以外の様々な被害関連情報が広く公表されれば、攻撃者を利する結果に繋がる場合があるとの指摘もあり、考え方の整理が求められている。

3. サイバーセキュリティ研究開発と人材育成についての課題

(1) 研究開発や人材育成の遅れ：巧妙化・多様化するサイバー空間の脅威に対抗するためには、国家として、サイバーセキュリティ分野の研究開発の強化と人材の増強が必須である。しかし、海外のサイバーセキュリティ先進国と比べ、我が国のサイバーセキュリティ製品の自給率は低く（注３）、研究開発や人材育成の水準も、質・量ともに十分とは言えない。

（注３）ヒアリング先の有識者によれば「我が国のサイバーセキュリティ製品の自給率は 10%以下であると感じている。」とのことである。

(2) 実データの不足による「データ負け」：優れたサイバーセキュリティ製品の研究開発には、優れたエビデンスである実データの活用が必要である。我が国を対象にするサイバー攻撃情報の多くは、海外ベンダのセキュリティ製品を通じて海外に流出しているのが現状である。このために優れた国

産セキュリティ製品の研究開発が進まない「データ負け」のスパイラルに陥っている。

(3) 能力開発のコストの問題：サイバーセキュリティ能力は、サプライチェーン・リスクに関する技術的検証も含め、才能のある個人に依存しているが、産業界だけで人材育成を体系的に進めていくのは困難である。また、海外では、企業と政府系研究機関とが密接に連携しながら、アクティブ・ディフェンス能力に優れた人材の育成や、攻撃者視点を踏まえたサイバーセキュリティ製品の研究開発を進めているが、我が国ではそのような機会に乏しい。

4. 推進体制の問題

我が国では、内閣サイバーセキュリティセンターが政府内のサイバーセキュリティ政策の総合調整を行っているが、1.～3.で指摘するようなサプライチェーン・リスク対策を中心とするサイバーセキュリティに係る対処を一元的に実行するための体制とはなっていない。

III. 講ずるべき対策

前節で指摘したそれぞれの課題の解決に向けて、ワーキングチームとして、政府において講ずるべきと考える対策は次の通りである。政府は、これら各項目について、政府内の主管省庁や実施の期限を明確化しつつ、速やかに実行すること。

1. サプライチェーン・リスク対策の充実・強化

政府は、サプライチェーン・リスク対策を中心としたサイバーセキュリティ確保のため、次の施策を講ずるべきである。

(1) 検証能力の構築：情報通信分野で用いられる機器やサービスのサプライチェーン・リスクに関し、我が国独自の検証能力を獲得するため、国家戦略上の重要な施策として位置づけ、NICT 等の公的セクターが主体となって、研究機関や産業界と連携して高度な技術的検証能力の構築を進める。

(2) ベンダによる運用者支援・運用者との情報共有の仕組みの構築：

① 5Gの機器やシステムについてサプライチェーン・リスクを含むセキュリティ・リスクの存在が明らかになった場合、それらのベンダが、当該

機器やシステムを運用する全国系携帯事業者及びローカル5Gの運用者に対し、明らかになったセキュリティ・リスクを遅滞なく通知するとともに必要な対策を講じるよう、ガイドライン等により、その仕組みを早急に確立する。特にローカル5Gについては、運用者側のサイバーセキュリティに関する知識が不十分である可能性を踏まえ、ベンダが運用者を適切に支援する体制を構築する。

② ローカル5Gを含む5Gネットワークについて、ベンダと運用者の間で、5Gセキュリティに関するリスク情報等を迅速かつ効果的に共有する仕組みを早急に構築する。

(3) ソフトウェアに係るサプライチェーン・リスク対策の強化：5G時代のネットワークはソフトウェア化・仮想化していくことから、導入時のハードウェアを中心とした取り組みだけではなく、アップデート等によって継続的に機能の改善等が行われるソフトウェアのサプライチェーン・リスクも重要となることに留意し、（1）で獲得された検証能力を最大限に活用し、導入後の運用・管理を視野に入れたソフトウェア中心のサプライチェーン・リスク対策を進める。

(4) 分野横断的サプライチェーン・リスク対策の取組みの推進：政府調達や5Gにおける対策の経験と成果を踏まえ、我が国の国民生活や社会経済活動に大きな影響のある重要なインフラや情報について、脆弱性を把握し、信頼のおけない機器やシステムへの依存を避けるよう、サプライチェーン・リスク対策を確立することが重要である。具体的な検討を行う際には、分野ごとに個別に検討するのではなく、分野横断で横串を通した取組を推進し、経済安全保障の確立を図る。

(5) 我が国事業者による代替機器・システムの開発・展開に対する支援：信頼のおけない機器やシステムの提供を代替しうるポテンシャルを持つ我が国の事業者について、その技術開発や国際展開等の活動を支援する。その際、官民ファンドや基金等による委託研究等、従来とは異なるスキームによる支援を推進するべきである。また、早急に成果を得るためには我が国と同様の認識を持つ各国との連携が必要であり、政府全体での戦略的視点も踏まえて検討・推進する。

(6) 総合的な検証体制の構築：上記（1）～（5）の成果を基礎に、我が国の官民の能力や持てる情報を結集し、サプライチェーン・リスクを総合的・戦略的に検証できる体制の構築に向けて、政府横断的に取り組む。当面は、

NISC、総務省・NICT 及び経産省が中心となって体制を構築することとなろうが、総合的なサプライチェーン・リスク対策を推進する体制について、役割分担を含め早急な検討を行い、2～3 年を目途にその構築を目指す。その際、（信頼の置ける海外の主体も含め）あらゆる民間企業や研究機関等の総力を結集する。

2. サイバーセキュリティ関連情報の取扱の明確化

サプライチェーン・リスク対策は、サイバー攻撃への対策強化と切り離して語ることはできない。政府は、サイバーセキュリティ関連情報の取り扱いに関し、以下の点を速やかに検討し、その結果を具体的に実施するべきである。

(1) **アクティブ・ディフェンス推進等のためのインフラの整備**：通信事業者等におけるアクティブ・ディフェンス推進等の観点から、通信の秘密の保護を図りつつ、サイバー攻撃者の探索や攻撃指令通信の遮断等の一層のサイバーセキュリティを確保する方策を確立することが必要である。このため、総務省はじめ関係省庁は、連携を図りながら、関係法令等の改正を視野に、スピード感を持った多面的な検討を行うとともに、通信事業者等を支援し、連携を促進する枠組みについて早急に検討すべきである。

(2) **サイバー攻撃発生時の対応の強化**：個人情報や企業等における機微情報の漏洩の有無等について、サイバー攻撃の特性等を踏まえ、サイバー攻撃発生時に関係者間で情報共有と被害の拡大防止を図ることが必要である。このため、情報の取り扱いに係る民間セクターのクリアランス制度や被害公表のあり方について、NISC はじめ関係省庁は、サプライチェーン・リスク対策強化に資することも視野に、重要インフラを担う民間セクターと連携を図りながら、関係法令やガイドラインのあり方について、スピード感を持って多面的な検討を図るべきである。また、その際、サイバーセキュリティに係る体制の拡充や民間セクターへの支援に配慮すべきである。

3. オープン・イノベーションによるサイバーセキュリティ能力（研究開発・人材育成）の向上

政府は、我が国のサイバーセキュリティ能力の向上のため、産業界と政府系研究機関等とのオープン・イノベーションを促進し、サイバーセキュリティ分野の研究開発と人材育成を抜本的に進めるべきである。

(1) サイバーセキュリティ分野の「知」を結集する国家拠点の創設：1.（6）の総合的な体制の構築と並行し、サイバーセキュリティ分野の研究開発及び人材の育成に関する能力と知見について、信頼性が確保された国内の研究機関及び産業界で共有を進めるため、サイバーセキュリティ分野の産官学の「知」を結集する国家拠点の基盤を整備し、提供する。政府は、サイバーセキュリティ分野の産官学の「知」を結集する国家拠点（Center of Excellence）を政府系研究機関に創設し、信頼の置ける諸外国との戦略的連携も視野に、サイバーセキュリティに関する研究開発と人材育成を抜本的に強化すべきである。

(2) 「国家拠点」において集約すべき「知」：「国家拠点」においては、以下の観点を中心に、「知」の集約を行い、オープン・イノベーションを促進すべきである。

① 攻撃者が我が国のサイバー空間に残す膨大な情報を集約・蓄積・分析し、その成果を国産の実データに基づく高品質なエビデンスとして関係機関へ提供するとともに、産業界における国産サイバーセキュリティ製品の開発に活かすための統合的環境を整備し、**「敵に関する知」**の集約を行うこと。

② サイバーセキュリティ人材育成に関する様々な蓄積を大学や産業界等に開放するため、サイバーセキュリティ人材育成基盤を整備し、**「育てるための知」**の集約を行うこと。

③ 産業人材のアクティブ・ディフェンス能力の向上や、いわゆるバックドア対策を含む攻撃者視点を踏まえたサイバーセキュリティ製品の研究開発の促進を図るため、産業界との人的交流を活発化させるとともに、高い自由度を持つ研究開発環境を産業界へ開放することで、**「攻めるための知」**の集約を行うこと。

4. 中長期的な体制の強化

サプライチェーン・リスク対策を推進する総合的な体制については、2～3年を目途にその構築を目指すことを提言した（1.（6））が、中長期的には、サイバーセキュリティに係る対応、具体的には、IT 戦略本部を抜本的に強化し、政府全体のデジタル・トランスフォーメーションを加速させた上で、サイバー攻撃の検知・分析・判断・対処を行うとともに、人材育成や関連産業の育成等も併せて一元的に実行するための組織の実現を目指すことが必要

である。このため、政府においては、このような中長期的な体制の強化も視野に、当面のサプライチェーン・リスク対策を早急に進めるべきである。

Ⅳ. おわりに

「はじめに」において、人類が COVID-19 を経験したことにより、社会全体のデジタル・トランスフォーメーションが劇的に推進されること、及び、このような変化の中にあって、「サイバー衛生」の観点に立ち、サプライチェーン・リスクへの対応が喫緊の課題となっていることを述べた。

しかしながら、その一方で、COVID-19 が企業業績に極めて深刻な影響を与えつつあることも明らかになった。

サプライチェーン・リスクをはじめとしたサイバーセキュリティの分野は、攻める側よりも守る側のコストが高く、短期的に利益を得るビジネスとしては成り立ちにくいことが指摘されていることに加え、今回の COVID-19 禍で、我が国の事業者の研究開発・人材育成意欲が大幅に減退することも懸念される。

本提言では、政府における体制の強化、サプライチェーン・リスク対策推進等のための法制面でのインフラや研究開発・人材育成の強化等に加え、多くの項目において、民間事業者への支援の必要性を述べたが、現下の経済状況等にかんがみれば、税制等従来の枠組みの支援を拡充するのは勿論のこと、官民ファンド、基金等を活用した委託研究、政府保有株式の売却益や配当金なども視野に入れたより前向きの支援策を推進するべきである。

本 WT においては、今後の経済や企業の研究開発意欲の状況を踏まえつつ、引き続き、必要な対策の検討を進めていくこととする。

以上

（別紙）サプライチェーンに起因するインシデント事例

1. **暗号化通信に使われるソフトウェアに脆弱性（2014 年）**：UNIX 系 OS で暗号化通信に使われる、オープンソースで開発・提供されているソフトウェア「OpenSSL」の拡張機能に、外部からの要求に対して必要以上に情報が流出してしまう脆弱性「Heartbleed」があった。

2. **スマートフォン用アプリに悪意あるコードが含有（2015 年）**：iPhone 等で使用される iOS アプリの開発環境「Xcode」のコピー版に悪意あるコードが仕込まれており、この環境を用いて開発されたアプリには、開発者も気づかずに悪意あるコード「XcodeGhost」が含まれてしまった。「XcodeGhost」に汚染されたアプリは、情報窃取や遠隔操作が可能であった。

3. **PC のプリインストールソフトウェアに脆弱性（2015 年）**：Lenovo 製の一部 PC にプリインストールされていた広告ソフトウェア「Superfish Visual Discovery」に脆弱性があり、SSL 通信が盗聴可能となる可能性があった。

4. **スマートフォン用ファームウェアがユーザ情報を送信（2016 年）**：BLU Products 製スマートフォンが採用する Shanghai Adups Technology 製ファームウェアがユーザ情報の一部を中国のサーバに無断で送信していた。

5. **ビジネス上のサプライチェーンによる脆弱性（2017 年）**：ワーム型ランサムウェア「WannaCry」の世界的な蔓延の際、取引先が踏み台となって、我が国企業にも被害が発生した（デジタル製品に悪意ある機能が組み込まれた事案ではなく、ビジネス上のサプライチェーンが問題となった事案）。

6. **PC のアップデートサーバ経由でマルウェア送付（2019 年）**：ASUS 社のソフトウェア・アップデートサーバが攻撃者の侵入を受け、ASUS 製の一部 PC を対象に、ソフトウェア・アップデート・ツールを介してマルウェアが送付可能な状態となっていた。