サイバーセキュリティ戦略本部
第34回会合　議事概要

１　日時

令和４年６月１７日（金）　　８時３５分～９時００分

２　場所

総理大臣官邸２階小ホール

３　出席者（敬称略）

松野　博一	本部長（内閣官房長官）
牧島　かれん	副本部長兼デジタル大臣
二之湯 智	国家公安委員会委員長
金子　恭之	総務大臣
林　　芳正	外務大臣
萩生田 光一	経済産業大臣
岸　　信夫	防衛大臣
小林　鷹之	経済安全保障担当大臣
末松　信介	東京オリンピック競技大会・東京パラリンピック競技大会担当大臣
後藤　厚宏	情報セキュリティ大学院大学学長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原　佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	東京都立大学法学部客員教授
宮澤　栄一	株式会社デジタルハーツホールディングス取締役会長
村井　純	慶應義塾大学教授

（※遠藤本部員及び田中本部員はご欠席。）

木原　誠二	内閣官房副長官
磯﨑　仁彦	内閣官房副長官
栗生　俊一	内閣官房副長官
村田　隆	内閣危機管理監
髙橋　憲一	内閣サイバーセキュリティセンター長
藤井　健志	内閣官房副長官補
滝崎　成樹	内閣官房副長官補

4　議事概要

（1）本部長冒頭挨拶

本日はご多忙の中、お集まりをいただき、感謝申し上げる。

本日は、「サイバーセキュリティ2022」、「重要インフラのサイバーセキュリティに係る行動計画」、「令和５年度予算重点化方針」のそれぞれの案について、ご審議をいただきたいと考えている。また、先般のサイバーセキュリティ月間について報告がある。

ウクライナ情勢を含む昨今の様々な情勢を踏まえるまでもなく、サイバーセキュリティをめぐる情勢は、その脅威度が格段に高まってきていると言わざるを得ない。また、ランサムウェアやEmotetによる日本企業の被害も増えてきており、政府・民間を問わず、対策に取り組む必要性もますます高まっている。

こうした情勢の変化も踏まえ、セキュリティ政策の在り方について、本日も限られた時間となるが、活発なご討議をお願い申し上げる。

（2）討議

【決定事項】

・サイバーセキュリティ2022（2021年度年次報告・2022年度年次計画）（案）について

・重要インフラのサイバーセキュリティに係る行動計画（案）について

・サイバーセキュリティ関係施策に関する令和５年度予算重点化方針（案）について

【報告事項】

・2022年サイバーセキュリティ月間について

○牧島副本部長兼デジタル大臣

それでは、意見交換に移りたい。

まず、有識者本部員よりコメントをいただきたい。

○中谷本部員

３点の決定事項については、いずれも賛同する。その上で、４点、申し上げる。

一点目に、ロシアによるウクライナ侵略により、地政学的状況が一段と厳しくなっている中で、サイバーセキュリティについても、平時対応のみならず、有事対応についても考えておくことが不可欠であると考える。具体的には、サイバー攻撃とそれへの反応について、自衛隊法や武力攻撃事態・存立危機事態対処法といった安全保障法制における位置付けを明確にすべきだし、また、サイバー攻撃の主な反応である有責者の資産凍結と入国禁止は、それぞれ外為法と出入国管理・難民認定法を根拠とする

と思われるが、運用の在り方について明確化すべきであると考える。

二点目に、サイバー攻撃の標的の８割はIoTを狙ったものであると指摘されており、古いシステムを更新せずに使用し続ける企業も少なくないことが強く懸念される。そのような企業には、更新のコストは企業の社会的責任のための必要経費だと考えて更新していただきたく、また政府としても注意喚起を行う取組である「NOTICE」（注：National Operation Towards IoT Clean Environment。国立研究開発法人情報通信研究機構（NICT）がサイバー攻撃に悪用されるおそれのある機器を調査し、電気通信事業者を通じた利用者への注意喚起を行う取組）をはじめ、可能な限りの対応を進めていただきたいと考える。

三点目に、サイバーセキュリティに関する産学官の知見や情報の結節点であるCYNEX（注：NICTが構築を進めているサイバーセキュリティ統合知的・人材育成基盤）を一層推進することで、有機的に人材育成や研究開発を進めていただきたい。

第四に、重要インフラに宇宙関連もカバーできるよう、適当な機会にご検討いただければと考える。

○野原本部員

本日の決定事項３点について、いずれも賛成する。

特に説明の冒頭にあった「サイバーセキュリティ2022」は、昨今の情勢の変化によるサイバーリスクの増大を踏まえた、今年度の重点施策が的確にまとめられていると評価している。その上で、３点申し上げる。

一点目に、ナショナルサート機能の強化については、「サイバーセキュリティ2022」の中でも最重要施策とされている。既に昨年度からNISCセンター長をヘッドとして、関係省庁等の局長級会合も立ち上げて、NISC内の体制を拡充し、「情報収集・共有」、「分析・集約」、「対処調整」、「政策対応」の４機能に対応した体制にし、これまでに既に４回、関係省庁合同の注意喚起を発出していると聞いている。しかし、我が国の注意喚起は米国のCISA（サイバーセキュリティ・インフラストラクチャー・セキュリティ庁）・NSA（国家安全保障局）・FBI（国家安全保障局）合同による注意喚起が、脅威評価、技術情報、防御策等から構成されることに比べると、まだまだ質的向上が必要であると考える。しっかりと取り組んでいただきたい。

二点目に、重要インフラ事業者をはじめとする民間部門におけるサイバーセキュリティの強化も重要な施策である。重要インフラ14業種については、既に行動計画もあり、体系的な取組がなされて効果が上がっているが、その周辺の、例えば食品、製薬、自動車等、それに準ずる業種に対するサイバーセキュリティの強化策についても、情報通信業界等を通してという間接的な方法だけでなく、直接的な施策を拡充する必要があると考える。

三点目に、アクティブ・サイバー・ディフェンスについての検討の必要性について、先ほど中谷本部員からもコメントがあったが、ウクライナ侵攻等の国際情勢の変化を

考えると、我が国のナショナルサートはインシデント発生以降の事後的な追跡と対応策のみであるが、サイバー攻撃に対して敵の攻撃の無力化のためのアトリビューションや通信の遮断などのアクティブ・サイバー・ディフェンスを可能とするよう、NSS（国家安全保障局）等と連携して検討する必要があると考える。

○前田本部員

まず、「年次計画」に異存ない。それから「重要インフラ行動計画」について、これはいわばNISCの原点であるが、着実に充実・進展していると考える。ガスも同様でエネルギーの話もあるが、サイバー攻撃によるインシデントの危険性については、再認識すべきである。「予算重点化方針」も的を射たものであると考える。サイバー警察局の発展、それからナショナルサートの重視など、全く異存ない。

ただ一点だけ、ナショナルサートに関連して申し上げたいのが、５月26日の衆議院の予算委員会で、議員の方から、アメリカの関係者から日本のサイバーセキュリティ能力は低いという指摘を受けたということに関してである。それに対してはもちろん官房長官がパーフェクトなお答えをされておられ､全くそのとおりであると考えるが、長年NISCのお手伝いをさせていただいてきた側としては、日本のサイバーセキュリティ能力はゼロであるという、アメリカの高官の指摘に関しては異論がある。特定秘密保護法も、以前からお手伝いをしてきて、アメリカの高官から、このままでは日本に情報を出せないという話も、それはそのとおりであると考えるが、日本もその後、不十分な面はあるが、法律を改正した。さらに、最近のEmotet、WannaCryなどのサイバー攻撃の被害に関しても、アメリカに比べてそこまで遜色があるのか。東京オリンピック・パラリンピック競技大会へのサイバー攻撃を完全に守り切ったではないか。世界一のサイバーセキュリティである。その点を、今日は是非申し上げたいと思った次第である。

もちろん議員が仰る､公務員により高度な守秘義務を､というのは全く賛成である。経済安全保障に舵を切った現在、例えばナショナルサートに関してもクリアランスという視点がサイバーセキュリティにとっては最も重要であるということを確認していただきたいと考える。

○宮澤本部員

決定事項３つについて、賛成する。

私からは二点申し上げる。一点目は、ウクライナ事案によって、明らかにサイバー攻撃は激増した。我が社の設置しているハニーポットと呼ばれる、ハッカーホイホイとも言えるトラップには、侵攻後、約10倍の数のハッカーがかかるようになった。ほぼ同時期に、トヨタの関連会社もハッカーに狙われ、全工場が生産停止するという被害も出た。今回、ハイブリッド戦争と言われるように、ハッカーはいまや表舞台に立

ったのだと考える。ウクライナには、世界中から30万人を超すハッカーが義勇兵として集まった。はたして日本は、有事の際、数十万人単位のハッカーを確保することができるのだろうか。いま一度、国内の人員を広く集め、教育を加速させ、サイバーの予備役なども考えた方が良いと考える。

二点目は、今、一番取り組まなければならないことは何かというと、中小企業経営層への知識と覚悟を高めることである。日本の垂直統合型の企業群において、その末端の企業の経営層の認識はまだ低い。また意識はあっても、何を対策し、どう対応したら良いのか、予算の感覚もない。ハッカーに一度狙われると、最終的に100％の企業がウイルスメールを開いてしまう。回避は不可能である。最近では日本語も上手に使われており、昔のような変な日本語ではない。とあるセキュリティ企業の調査では、１台が感染すると、1.5時間で次のパソコンが感染するというデータもある。１時間が勝負で、すぐにパソコンをネットワークから切り離すしかない。EDR（注：Endpoint Detection and Response。エンドポイントセキュリティを担う仕組みの一つ。）という、感染を前提とした防御策が有効であるが、中小企業がこうした防御策を知っているのかどうか懸念がある。予算はウイルスソフトと同じ、月1,000～2,000円程度である。これが導入できていれば、トヨタの問題は完全に防げていた。また、被害の情報共有という点で日本人は不得手である。日本人特有の恥や外聞というプライドを捨てて、全てを包み隠さず公表する覚悟が必要である。被害金額も全てである。

その覚悟を促すためにも、まずは我々が我が国のサイバーセキュリティ対策において、他国の後塵を拝して後追いするのか、それとも日本独自の対策を世界に先駆けて行って、他とは違う一歩前進の行動を取るのか、今、官も民も大きな覚悟が必要な時代がやってきたと考えている。

○村井本部員

今日の議論の中で、重要インフラのことを少しお話ししたい。ウクライナ侵攻が起こった２月 24 日以前から､実はウクライナはパワーグリッドをロシア系からヨーロッパ系に切り替えるテストをしていた。その後、侵攻があり、予定では来年の６月までに完成させるということであったが、切替えを３週間で完成させた。その成果を見ると、ウクライナ全土で、ソーシャルネットワークが継続使用可能となっている。停電が起きていない。これはパワーグリッドがいかに大事かということを物語っている。我が国は地震の度に停電にみまわれている。ウクライナの場合は、事前に準備していたから、３週間で切り替えられた。

今回明確に分かったことは、サイバー空間というものは、全ての国民と全ての産業も合わせてデジタル社会が成り立っているが、電気がないと動かないということである。やはり重要インフラの中で、電力だけが重要というわけではないが、そもそも電力が確保されていないとサイバー空間、デジタル社会は動かない。したがって、電力

の優先度は、特にこの会議では特別に考えて良いのではないかと考える。

二点目は、これも今回のウクライナの事案で分かったことであるが、ほとんどのことがソーシャルネットワークの上で動いている。ソーシャルネットワークの分析、プロパガンダの偽情報の発見等は、全てソーシャルネットワークインテリジェンスである。問題はこの力が我が国のどこにあるのか。いわば昔でいう OSINT（オープンソースインテリジェンス）である。この力を我が国ではどこが責任を持ってやるのかということである。デジタル社会がこれだけ推進され、10 年前倒しということは 10 倍の速度で進む。また、今は報道機関が全て事件の発生を、警察からの連絡ではなく、ソーシャルネットワークの分析部隊を抱えて検知している。このようなことをサイバーセキュリティの上でも考えていく必要があると考える。

○後藤本部員

決定事項３点に賛同する。その上で４点申し上げたい。

一点目は、先ほどから出ているが、NISCの総合調整の役割であるナショナルサートの機能を、民間と連携しながら、先ほどもあったSNSの分析、グローバルな経済状況、国際競争、課題共有等、サイバーセキュリティ分野を超えた分析能力の強化を期待したい。

二点目は、「重要インフラの行動計画」では、サプライチェーンの観点が加わって、事業継続性重視の姿勢が明確になっており、高く評価したい。同様に、政府機関そのものについても、情報の機密性の観点だけではなくて、事業継続確保、といった観点からの施策も必要であると考える。

三点目は、「令和５年度予算重点化方針」についてである。民間も政府も日々、デジタル依存度が高まっていく現状にあることから、現状に合わせた施策ではなく、今後のデジタル依存度の高まりを先読みした施策が重要であると考える。その意味で、大規模サイバー攻撃事態等への対処では、その波及被害が広く社会に及ぶということを想定した対応策の強化が必要となるし、当然ながら研究開発、人材育成、普及啓発等の施策が大事であると考えている。ぜひ予算への反映をお願いしたい。

四点目は、ロシアのウクライナ侵攻に関する注目点として、サイバー空間における民間企業、特に巨大IT企業の役割についてである。マイクロソフトのブラッド・スミス会長がブログや講演で発信しているが、ウクライナ政府に向けた民間企業としての行動をどう理解するか。いろいろな議論があると思うが、私はITビッグテックによるサイバーセキュリティサービスの影響は、国同士の協力関係以上に大きな役割を持ち得るということを意識する。言い換えれば、国の影響力よりも、ITビッグテックの影響度が高い、これをどのように考えるべきか。これについて我が国としても議論を深めていきたいと考える。

【閣僚本部員発言】

○牧島副本部長兼デジタル大臣

サイバーセキュリティ戦略に基づく施策の実施に関しては、政府機関や、本日議題となっている行動計画に基づく、重要インフラ事業者に対する取組を強化することに加え、昨今の情勢の変化等も踏まえ、NISCを中心として関係の各政府機関のリソースを結集し、インシデント対応から政策的な措置までを一体的に推進するナショナルサートの取組をはじめ、関係者間の連携を更に加速してまいる。

また、サイバーセキュリティ対策では国際連携が不可欠である。Ｇ７デジタル大臣会合では、東京オリンピック・パラリンピック競技大会の運営経験・ノウハウを、今後開催を控える各国に引き継いでいく旨発信したほか、デジタル人材の不足、地域・中小企業に対する取組の必要性等､各国と様々な課題を共有していることを実感した。今後も、諸外国との緊密な連携により、サイバーセキュリティの確保に万全を期してまいる。

○二之湯国家公安委員長

サイバー空間の公共空間化が進む一方、近年、サイバー空間の脅威は極めて深刻な情勢が続いている。

こうした情勢を踏まえ、「特に強力に取り組む施策」にも掲載していただいているように、警察ではサイバー事案への対処能力の強化を図るため、警察庁にサイバー警察局を､関東管区警察局にサイバー特別捜査隊を､本年４月１日にそれぞれ設置した。

今回の組織改正により民間事業者、外国捜査機関等を含む国内外の関係機関との連携を強化し､サイバー事案への厳正な対処や実態解明を一層強力に進めることにより、サイバー空間における安全・安心の確保に努めてまいる。

○金子総務大臣

本日の決定事項である「サイバーセキュリティ2022」など３点については、昨今の国際情勢や国内でのリスクの高まりを踏まえた、必要な施策が盛り込まれていると考える。

総務省としては、

・電気通信事業者における積極的なサイバーセキュリティ対策を推進すること等による、情報通信ネットワークの安全性・信頼性の確保
・NICT（国立研究開発法人情報通信研究機構）に、情報収集・分析及び人材育成の基盤を構築すること等による、サイバー攻撃への自律的な対処能力の向上

などを柱とする「ICTサイバーセキュリティ総合対策2022（案）」を今般取りまとめたところであり、引き続き、我が国のサイバーセキュリティの確保に貢献してまいる。

また、総務省は、重要インフラとして、電気通信、放送、地方公共団体を所管しており、本日決定される「行動計画」に基づいて、官民連携に基づく重要インフラ防護を一層強化してまいる。

○林外務大臣

国際社会全体において、サイバー空間に対する依存度が一層高まる中、ウクライナにおける政府機関や重要インフラに対するサイバー攻撃に見られるように、国家の関与が疑われるものを含め、組織的かつ周到に準備された高度なサイバー攻撃の脅威が増大している。堅牢なサイバーセキュリティの確保は抑止力の強化や安全保障の確保に直結している。

こうした状況の中、同盟国・同志国間との連携が今まで以上に重要。先月の日米豪印首脳会合では、重要インフラ防護やインド太平洋地域における能力構築支援の協調等の取組を強化することを確認したほか、日米首脳会談でも協力の加速化で一致した。

引き続き、米国をはじめとした同志国と緊密に連携しつつ、サイバーセキュリティ上の課題に対応していきたい。

○萩生田経済産業大臣

今回のサイバーセキュリティ2022において、特に強力に取り組む施策として、「地域・中小企業のサイバーセキュリティ対策促進」を選出いただいた。

昨今のサイバー攻撃の高度化に伴い、サプライチェーンの中でもセキュリティが脆弱な部分が狙われるようになってきており、３月に起きた自動車工場の稼働停止の例に見られるように、脆弱な部分を起点として、サプライチェーン全体が影響を受ける事例が顕在化している。

このため、経済産業省では、地域・中小企業におけるセキュリティ対策を進めるため、IT導入補助金に「セキュリティ対策推進枠」を新たに設けるなど、中小企業のセキュリティ対策を支援する取組を強力に進めていく。

また、「サイバー・フィジカル・セキュリティ対策フレームワークの社会実装」に向けては、

①「工場ガイドライン」や「ビルガイドライン」など、業種別・業種横断的なサイバー攻撃のリスクや対策を整理したガイドラインの普及促進や、

②ソフトウェアの脆弱性管理に有効な、言わばソフトウェアの成分表示表である、SBOMの活用促進に向け、実証事業を通じた効果的な活用モデルの検討

等の取組も進めていく。

引き続き、中小企業や地域を含めた、産業界のセキュリティ対策の強化に取り組んでまいる。

○岸防衛大臣

国家主体が関与するサイバー攻撃が行われる中、今後、インフラの制御系システムやサプライチェーン等の脆弱性を狙った攻撃によって、安全保障上極めて重大な事案が引き起される可能性も否定できず、我が国全体としてサイバーセキュリティを強化することが急務と考える。

本日の決定事項である、重要インフラ行動計画、令和５年度予算重点化方針においては、いずれも国全体や政府機関としての対策の方向性がしっかりと示されており、極めて意義のあるものと認識しており、防衛省としても我が国全体のサイバーセキュリティを強化する取組に対して、引き続き積極的に協力してまいる。

○小林経済安全保障担当大臣

今国会で成立した「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」においては、国際的にサイバー攻撃等の脅威が増大している状況も踏まえ、情報通信や電力、金融をはじめとする基幹インフラ役務の安定的な提供に対する妨害を防止する観点から、基幹インフラ事業者における重要設備の導入等を国が事前審査する制度を措置している。

サイバーセキュリティに関するリスクへの対応は、経済安全保障の観点からも極めて重要であり、特に国際情勢の変化等を踏まえたサイバーセキュリティの確保に向けた官民連携や分析能力の強化について､政府全体として取組を進めていく必要がある。成立した法律の円滑かつ可能な限り速やかな施行に向けて取り組むことを含め、関係大臣と連携してまいりたい。

（３）決定事項の決定

○牧島副本部長兼デジタル大臣

それでは、本日お諮りした３件の決定事項について、異議はないか。

（「異議なし」と声あり）

○牧島副本部長兼デジタル大臣

異議なしということで、本案を決定させていただく。

（４）本部長締め括り挨拶

本日の会合では、昨年９月にサイバーセキュリティ戦略を決定してから初めてとなる年次報告・計画である「サイバーセキュリティ 2022」のほか、「重要インフラのサ

イバーセキュリティに係る行動計画」、「令和５年度予算重点化方針」について決定した。

「サイバーセキュリティ 2022」において、「特に強力に取り組む」とされた６つの施策を中心に、関係省庁において着実に取組を進めていただくよう、お願いする。

これに関連して、私からは２点、皆さんにお願い申し上げる。

１点目は、インシデントの未然防止を図るための、幅広い情報共有・緊密な連携の促進である。具体的には、ナショナルサートを通じて、全省庁横断的に情報共有の徹底を図ることにより、インシデント対応から政策的な措置までを、政府としてより一体的に推進をしていくこと、また、クラウドをはじめとする様々なサイバー関連の事業者との、より一層の緊密な連携を図ることなどの取組が必要不可欠であると考えており、省庁間、そして、官民間の情報共有・連携体制の更なる強化に向けた検討を深めていただきたい。

２点目は、我が国の取組の積極的な発信、国際協調・連携の強化である。例えば、我が国では、東京オリンピック・パラリンピック競技大会において、各種施策を講じることにより、運営に支障をきたすようなサイバー攻撃を防ぎ、無事に大会を開催したという実績を作った。関係省庁におかれては、こうした、我が国のサイバー能力や大会の運営経験・ノウハウ等を、各国に向けてしっかりと発信していっていただくことなどを通じて、サイバーセキュリティ分野における各国との協調・連携をより一層深めていただきたい。

みなさまには、いま申し上げたほか、サイバーセキュリティ戦略に基づく様々な施策を着実に実施いただくことをお願い申し上げる。

－ 以上 －