サイバーセキュリティ戦略本部
第６回会合　議事概要

日　時：令和８年７月 31 日（金）　　10 時 15 分～10 時 25 分
場　所：総理大臣官邸２階大ホール
出席者：別紙のとおり
議　題：

- サイバーセキュリティ 2026（2025 年度年次報告・2026 年度年次計画）
- 重要インフラ統一基準等
- 脅威ハンティングに係る基本方針
- サイバーセキュリティ関係施策に関する令和９年度予算重点化方針
- サイバーセキュリティ対策推進会議の構成員の変更
- 「Project YATA-Shield」の取組状況

議事概要：

○ 松本副本部長兼サイバー安全保障担当大臣より、決定を要する事項の各議題について説明が行われた。

○ また、松本副本部長兼サイバー安全保障担当大臣より、「Project YATA-Shield」の取組状況について、以下の旨の説明が行われた。

・サイバー攻撃にAIが悪用されることで、攻撃のスピード・規模が劇的に増加するなどの脅威に直面しております。

・本年５月、総理指示を踏まえ、我が国のサイバー対処能力を強化する「Project YATA-Shield」を取りまとめました。これに基づき、NCOが中心となって、関係省庁と連携しながら、取組を進めています。

・具体的には、取りまとめ後、ただちに、政府機関等、重要インフラ事業者等及びソフトウェア・ベンダに対して基本的な対策の確実な実施等を要請する注意喚起を行いました。また、政府機関等に対する取組として、政府統一基準群の改定を行うとともに、特定のAIモデルに依存するのではなく、種々のAIツールを活用し、政府機関等の重要システムにおける脆弱性のチェックを開始しております。重要インフラ事業者等に対する取組としては、重要インフラ統一基準の策定や、国内・海外のAI関係企業とのマッチング支援等を進めております。最後に横断的な取組として、外国政府機関やビッグテック等との更なる連携、AISIによる技術支援・評価、サイバー人材の育成支援、技術開発の推進も併せて進めてまいります。

・次に、各重要インフラ所管省庁における取組です。いずれの省庁も、大臣と、所管する重要インフラ分野の代表者との会合を開催し、対策の要請等を行うとともに、情報

提供やフォローアップ等を通じ、対策の強化に努めていただいております。

・また、金融庁は、５月に金融機関向けに「要請文」を発出し、例えば、左上の①にある通り、フロンティアAIへの対応について、経営トップのリーダーシップの下で経営課題として扱うこと、右下の⑧にある通り、ITシステムを能動的に停止させざるを得ない場合も選択肢に入れること、などの対応を求めています。こうした対応は、金融機関のみならず、政府機関や、他の重要インフラ事業者にもあてはまるものです。

・重要インフラの中には、例えば、地方公共団体、医療機関、規模の小さい事業者といった、一層の対策向上が必要な分野や事業者もあることから、所管省庁において、業界のニーズに応じ、寄りそった支援も行っていただいております。

・引き続き、官民の総力を挙げて、日本全体としてサイバーレジリエンスの強化に向けて取組を進めてまいります。

○ 審議の結果、議題のうち本部決定・本部長決定を要する事項については、原案のとおりに決定された。

○ 出席者からの発言は以下のとおり。

・片山財務大臣（兼金融担当大臣）から、「金融分野で取組を進める中で、他の分野にも応用できる気づきとして、以下５点申し上げます。①アクセス制限のないAIモデルを含めて様々なモデルを活用し、早期に対応を開始することが望ましいという点、②大量に発見される脆弱性に優先順位を付け、脆弱性発見からパッチ適用までの対応を加速化させることも重要、③こうしたAIの活用に加えて、基本的な対策を迅速かつ着実に進めるとともに、多層防御やインシデント発生時の備え等をしっかりと進めていく必要、④更に、データの安全な取扱いが重要な論点、⑤また、ITベンダー等における対応も重要であり、国家サイバー統括室（NCO）を中心に、政府全体として連携していく必要、こうした金融分野の先行的な取組で得られた知見・経験は、各分野においても参考にしていただきたいと思います。」といった発言があった。

・林総務大臣から、「AI性能の高度化を踏まえた総務省の対応としては、５月に、所管分野の代表に対して、私から注意喚起を行うとともに、経営層のリーダーシップの下で積極的に取り組むよう、対策の強化を要請しました。その要請を踏まえ、情報通信分野については、ICT-ISACにおいて、事業者が取り組むべき事項等をとりまとめ、対策を進めている。地方行政分野についても、全地方公共団体において情報資産の脆弱性管理に関する点検の実施を進めています。加えて、総務省では、所管の情報通信研究機構（NICT）とともに、サイバーセキュリティに関する人材育成支援や技術開発を推進しています。今後とも、所管事業者や関係機関と連携し、AIの進展を踏まえたサイバーセキュリティ対策の強化に取り組んでいきます。また、今般策定する重要イン

フラ統一基準では、『郵便』分野を新たに重要インフラの対象に加えています。総務省では、今般追加される郵便分野を含め、所管の重要インフラ分野について、重要インフラ統一基準を踏まえ、関係機関と連携し、各分野のガイドライン等の策定・修正を行うなど、サイバーセキュリティ対策を着実に進めてまいります。」といった発言があった。

・上野厚生労働大臣から、「当省では、５月18日の国家サイバー統括室からの注意喚起を受け、５月22日に医療機関・関係団体との意見交換を実施しました。会議では、高性能AIの悪用により、攻撃の高速化とそれによる脅威の増大への懸念を共有し、各機関に対し、経営層のしっかりとした関与の下、『医療情報システムの安全管理に関するガイドライン』を活用して、基本的な対策を確実に実施するよう要請しました。また、会議に出席していない医療機関等に対し、５月27日に、都道府県等を通じた注意喚起も行いました。６月29日には、アップデートした『医療情報システムの安全管理に関するガイドライン』と令和８年度版のチェックリストを発出し、その際、改めて資産管理の重要性等について周知の徹底を図りました。引き続き、高性能AIへの対応をはじめとする医療機関のサイバーセキュリティ対策の取組を着実に支援してまいります。」といった発言があった。

・赤澤経済産業大臣から、「クロード・ミュトスに代表される高度なAIが出現する中、高度化するAIによるサイバー攻撃の脅威を踏まえ、国家・国民の安全・安心を損なう様々なリスクに備えることが重要です。例えば、今月、開発中の最先端AIモデルが暴走し、他社のシステムに侵入する由々しき事態も発生しました。AI開発では、開発環境のセキュリティを高度に確保するなど、セキュリティの取組を凡事徹底していくことが重要です。このため、５月１日に私から直接、重要インフラ事業者のトップに対し、①トップ主導のリソース確保、②脆弱性情報の早期把握と対応、③内部システムのあらゆる挙動を常に確認する、いわゆる『ゼロトラスト』への移行を要請しました。電力業界には緊急点検の実施も求め、迅速なパッチ適用に向けたリソース確保など、更なる対応を要請しました。重要インフラ事業者におかれましては、一部に見られる『制御システムは閉域網だから安全』との誤った認識を改めていただくとともに、外部のベンダーと社内組織との間で役割と責任を明確化していただく必要があります。こうした課題の解決には、信頼できる人的リソースの質・量の確保や、日頃からの高いセキュリティ意識に基づいたマネジメントなどにしっかりと取り組むことが重要です。また、中小企業に向けては、異常監視やサイバー攻撃を受けた際の初動対応支援などをパッケージ化した『サイバーセキュリティお助け隊サービス』の普及にも取り組んでまいります。」といった発言があった。

・金子国土交通大臣から、「国土交通省では、『Project YATA-Shield』を踏まえ、５月28日、航空、水道等重要インフラ６分野の代表との官民対話を実施し、経営トップのリーダーシップの下で、サイバーセキュリティ対策を徹底・強化するよう、私から直接要請しました。また、交通事業者等からなる一般社団法人『交通ISAC』を始め関係事業者との意見交換を重ねているほか、新たに設置した相談窓口を通じた相談に対応するなど、事業者に寄り沿った対応を進めています。国土交通省としては、今後とも国家サイバー統括室（NCO）等の関係機関と緊密に連携しながら事業者の取組を支援するとともに、省内や所管独立行政法人のシステムについても、現在進めている基本的対策に係る総点検を含め、対策に万全を期してまいります。」といった発言があった。

・あかま国家公安委員会委員長から、「公共の安全と秩序の維持を責務とする警察は、これまでも、深刻なサイバー空間をめぐる脅威情勢に対処するため、サイバー攻撃の未然防止や被疑者の検挙に向けた取組を推進してきたところです。このような被害の未然防止や検挙のためには、サイバー脅威を幅広く認知することが必要不可欠であることから、警察においては、広報啓発活動や事業者との共同対処訓練等の官民連携を通じて、被害の通報・相談の促進を図ってきたところです。本日、基本方針が議論される脅威ハンティングは、より能動的にサイバー脅威を把握するための活動であり、サイバー攻撃の未然防止と被疑者の検挙に向け、警察が正にその責務として取り組むべきものです。AIの悪用等によりサイバー攻撃が一層高度化・巧妙化する情勢も踏まえ、全国警察において脅威ハンティングが着実に実施できるよう、警察庁を指導してまいります。また、公共の安全と秩序の維持の観点から行われるアクセス・無害化措置を含め、能動的サイバー防御を着実に実施するためには、内閣官房・内閣府、警察、防衛省・自衛隊が三位一体となって中核的な機能を果たす必要があることから、必要な体制整備に万全を期すよう、警察庁をしっかりと指導してまいります。」といった発言があった。

・小野田経済安全保障担当大臣から、「我が国における基幹インフラに対するサイバー攻撃の脅威が増大する中、基幹インフラ役務の安定的な提供の確保を通じて、経済安全保障を推進するためには、サイバーセキュリティについての取組を不断に進めることが必要です。この点、今般の改正経済安全保障推進法で追加された医療分野も含め、基幹インフラ制度の運用に当たっては、本年10月から施行されるサイバー対処能力強化法とも緊密に連携してまいります。また、AI基本計画においても、AIがもたらすリスクが複雑化かつ深刻化する中、エージェント型AIの登場により、自律型サイバー攻撃の可能性も懸念されると指摘しています。人工知能戦略担当大臣としても、政府が高性能AIを用いて、脆弱性の発見・修正等の対応ができるよう、AISIによる技術支援

等を進めていきます。これらの取組を通じて、政府一体となって経済安全保障の更なる確保等に努めてまいります。」といった発言があった。

・小泉防衛大臣から、「国家を背景としたサイバーアクターによる組織化・洗練化されたサイバー脅威が国家安全保障上の脅威となるなか、国民の生活・経済活動を守ることは、我が国の『強い経済』の実現はもとより、有事において自衛隊の任務を確実に遂行する上で不可欠です。脅威ハンティングは、これらサイバー脅威情報を能動的に収集・蓄積・分析することで、サイバー攻撃キャンペーンの特徴や弱点を把握し、平時から有事に至るまで、サイバー攻撃をシームレスに抑止・防止することを可能とする取組です。防衛省・自衛隊は、今般策定する『脅威ハンティングに係る基本方針』に基づき、これまで自衛隊が運用する情報システムを対象に行ってきた脅威ハンティングに係る高度な能力を活用し、国民の生活・経済活動を守り、自衛隊の任務遂行を確実にする上で不可欠な重要インフラ等を防護していくため、国家サイバー統括室を中心とした政府一体の支援に積極的に貢献してまいります。また、日本成長戦略を下支えするサイバーセキュリティの確保のため、脅威ハンティングの能力活用や、政府として進める高機密ソブリンクラウド（仮）の導入などについても、防衛省・自衛隊として積極的に取り組み、防衛力の強化のみならず我が国の経済成長に寄与する『防衛と経済の好循環』に貢献してまいります。」といった発言があった。

・小林文部科学副大臣から、「現政権の目指す『新技術立国』の実現のためには、卓越した研究成果の社会実装が重要であります。そのような研究成果を創出する場として、大学等が果たすべき役割は極めて重要です。一方、多岐にわたる情報資産を保有する大学等においては、高性能AIの出現も踏まえサイバーセキュリティ対策の更なる強化が喫緊の課題となっております。文部科学省からは、政府全体を対象として発出されたAI性能の高度化を踏まえたサイバーセキュリティ対策の強化に関する事務連絡を大学等へ共有し、サイバーセキュリティ対策強化に向けた注意喚起を行っているところです。文部科学省としては、関係府省とも緊密に連携しながら、引き続き、大学等のサイバー対策強化に取り組んでまいります。」といった発言があった。

・金子内閣府大臣政務官から、「今月21日に閣議決定された日本成長戦略においては、世界共通の課題解決に資する製品・サービスを国内外に提供することで日本の成長につなげる17の戦略分野の一つとして『デジタル・サイバーセキュリティ』を選定しました。また、17の戦略分野における成長投資を下支えするため、官民連携でのサイバー脅威への対応を強化することが必要であるとの認識に基づき、８つの横断的課題の一つとしても『サイバーセキュリティ』を位置付けました。本日議題となったサイバーセキュリティ2026においても、日本成長戦略に盛り込んだサイバーセキュリティの

政策パッケージが、『特に強力に取り組むべき施策』として位置付けられました。17の戦略分野で先陣が切られる官民連携での国内投資を日本全国に拡げ、日本経済の更なる成長につなげていくため、その大前提となるサイバーセキュリティの強化を、成長戦略の観点から支えてまいります。」といった発言があった。

・大西外務大臣政務官から、「高性能AIの悪用による越境サイバー攻撃の大規模化・巧妙化が懸念される中、深刻なサイバーインシデントへの対応に当たっては、各国と迅速かつ緊密に連携する必要があります。外務省としては、外国政府機関との更なる連携を推進する観点から、各国とのサイバー対話や国際会議に際し、このような脅威認識を共有しつつ、『Project YATA-Shield』を含む我が国の政策を適時適切に発信してきています。さらに、在外公館も活用し、各国の対応について情報収集するとともに、高性能AIへのアクセスを含め、同盟国・同志国との連携に取り組んでいます。外務省としても、NCOを始めとする関係省庁と連携し、各国との平素からの関係構築に引き続き務めてまいります。」といった発言があった。

○　高市内閣総理大臣より、以下のとおり発言があった。

・本日は、「サイバーセキュリティ2026」、「重要インフラ統一基準」、「脅威ハンティングの基本方針」などを決定しました。そのほか、AIの高度化を踏まえて５月に策定した「Project YATA-Shield」の取組状況を御報告いただきました。

・国家を背景としたものを始め、巧妙化・高度化するサイバー攻撃は、我が国の経済社会や国家安全保障に対する大きな脅威であり、AIの急速な高度化は、この脅威をさらに深刻なものとしております。
加速度的に脅威を増すサイバー攻撃は、我々の準備を待ってはくれません。

・サイバー脅威への対応の一層の強化と加速に向けて、本日、私から３点、指示をします。

・第１に、AIの高度化への対応の一層の強化です。
松本サイバー安全保障担当大臣を中心に、各大臣のリーダーシップの下、政府内の情報セキュリティ対策や、重要インフラ事業者等における脆弱性対応などを一層強化してください。

・第２に、「『サイバー対処能力強化法』などに基づく取組の加速」です。
官民連携の基盤となる「協議会の設置」や、「アクセス・無害化措置」について、松本サイバー安全保障担当大臣、あかま国家公安委員会委員長、小泉防衛大臣を始めとする関係大臣は、本年10月１日の施行に向けて、準備を加速してください。

・第３に、「社会全体のレジリエンス強化」です。
サイバー脅威への対応の強化は、『日本成長戦略』における17の戦略分野を始めとした、国内投資の成果を享受するための大前提です。各大臣は、サイバー分野における

官民の取組を、ギアを上げて推進してください。

・あらゆるサイバー脅威に切れ目なく対応することができますように、取組の不断の強化と見直しを行い、世界最高水準の強靱さの確保に向けて、全力で取り組んでいただきますようにお願いいたします。以上です。

（議了）

（別紙）

出席者一覧

高市　早苗	内閣総理大臣
木原　稔	内閣官房長官
	沖縄基地負担軽減担当
	拉致問題担当
松本　尚	デジタル大臣
	デジタル行財政改革担当
	行政改革担当
	国家公務員制度担当
	サイバー安全保障担当
	内閣府特命担当大臣（サイバー安全保障）
林　芳正	総務大臣
平口　洋	法務大臣
片山　さつき	財務大臣
	内閣府特命担当大臣（金融）
	租税特別措置・補助金見直し担当
上野　賢一郎	厚生労働大臣
鈴木　憲和	農林水産大臣
赤澤　亮正	経済産業大臣
	原子力経済被害担当
	ＧＸ実行推進担当
	産業競争力担当
	中東情勢に伴う重要物資安定確保担当
	内閣府特命担当大臣（原子力損害賠償・廃炉等支援機構）
金子　恭之	国土交通大臣
	水循環政策担当
	国際園芸博覧会担当
石原　宏高	環境大臣
	内閣府特命担当大臣（原子力防災）
小泉　進次郎	防衛大臣
あかま　二郎	国家公安委員会委員長
	領土問題担当
	内閣府特命担当大臣（防災　海洋政策）
小野田　紀美	経済安全保障担当

	外国人との秩序ある共生社会推進担当 内閣府特命担当大臣（クールジャパン戦略 知的財産戦略 科学技術政策 宇宙政策 人工知能戦略 経済安全保障）
小林　茂樹	文部科学副大臣
田所　嘉徳	復興副大臣
金子　容三	内閣府大臣政務官
古川　直季	内閣府大臣政務官
大西　洋平	外務大臣政務官
尾﨑　正直	内閣官房副長官
佐藤　啓	内閣官房副長官
露木　康浩	内閣官房副長官
増田　和夫	内閣危機管理監
市川　恵一	国家安全保障局長
阪田　渉	内閣官房副長官補
田中　利則	内閣官房副長官補
飯田　陽一	内閣サイバー官
井上　裕之	内閣府事務次官
佐伯　耕三	内閣広報官