○山下委員長　次に、長妻昭君。

○長妻委員　長妻昭です。よろしくお願いをいたします。

経済安全保障にとってＡＩの脅威というのが、また新たなステージに上がって格段に脅威が高まってきたというふうに考えております。釈迦に説法でありますけれども、ＡＩの開発というのも新たなステージに入ってきた。これまでは、ＡＩの知能を向上するということで、みんな頑張ってきた。ただ、それが、ＡＩが人類に対する脅威になってきて、それをいかに防ぐか、こういう局面に大きく転換をしてきているのではないかというふうに思います。

アンソロピック社のクロード・ミトスに代表されるように、オープンＡＩのチャットＧＰＴの最新バージョンもそれを上回るんじゃないかと言われておりますし、今月発表予定のグーグルのＡＩもそれに匹敵するんじゃないかというふうに言われております。次々に脅威が高まっている。ある意味では、万能金庫破り、どんな金庫でも開けてしまう、核兵器並みの脅威とも言われておりますし、私は、ＡＩエージェント型万能ハッカーというような表現がいいんじゃないか、いいんじゃないかというか、脅威を示す一つの表現になるんじゃないかと思うんですけれども。

明日から米中首脳会談もあって、このＡＩの脅威についても話題になるというふうに聞いております。非常に重要な局面に差しかかっていて、昨日首相から、閣僚懇談会の場で、このミトスを始め脅威に対応するように各閣僚は頑張ってほしいというような指示があったと思うんですが、小野田大臣の所管では、大臣自身、どういうふうに動いていきますか。

○小野田国務大臣　経済安全保障の今の立場の所管ということですか。ＡＩ担当大臣としての答弁じゃなく……（長妻委員「いや、全部」と呼ぶ）全部。ここでは何かＡＩ担当大臣としてお答えができないというふうにも聞いているんですけれども。

経済安全保障担当大臣としては、基幹インフラを守るために、やはりサイバー攻撃というのは来るでしょうから、そこに対する、基幹インフラを守るために、ＮＣＯとも連携をしながら、やるべきところをしっかり見ていく。脆弱性に対して、今までの脆弱性に対する対応だけではなく、新しいものにもきちんと対応できるような、脆弱性に対応できるようなものをちゃんと確認していくということは必要なんだろうなと思っています。

○長妻委員　具体的にどういうふうにやるんですか。

○小野田国務大臣　先ほど私がちょっと言ったことも重なるんですけれども、基幹インフラ事業者が特定重要設備を導入する際などに国が事前に審査を行うこと等を通じて、サイバー攻撃等も含め、特定妨害行為のおそれの低減を図っていくというところです。

加えて、特定重要設備の導入後であっても、国際情勢の変化その他の事情の変更により、特定重要設備が特定妨害行為の手段として使用され又は使用されるおそれが大きいと認めるに至ったときには、特定重要設備の検査又は点検の実施等の必要な措置を取るべきことを勧告することを可能としております。

どのような場合にそのほかの事情の変更について該当して事後勧告を行うことになるかについては、個別具体の判断についてお答えは差し控えますが、今後、御指摘のミトス等により特定重要設備に係る脆弱性の情報等がより明らかになり、特定妨害行為のおそれの判断に影響を及ぼすような場合には、その他の事情の変更に該当する可能性もあるので、包括的にしっかり見ていくというところです。

○長妻委員　ミトスによる脆弱性はもう明らかになっているんですね。昨日、そういう指示が総理からあったので。ですから、その答弁というのは、私が本会議で聞いたときに同じ答弁があったので、そうじゃなくて、私が言うところのＡＩエージェント型万能ハッカーに対する対応として、一体、基幹インフラにどういう対応を具体的に促していくのか、このことを聞いているんです。

○小野田国務大臣　先生からも御指摘があったとおり、昨日、松本サイバー安全保障担当大臣を中心に、サイバーセキュリティーの確保に向けて政府全体での対応を早急に具体化し実施するように指示があったところでございますけれども、基幹インフラ制度に係るこのような取組を実施する関係府省庁との連携を強化しながら、基幹インフラ役務の安定的な提供の確保に努めてまいりたいと思います。

　具体的にどうするのかというところは、私からというよりはＮＣＯからなのかなというふうに思います。

○長妻委員　いや、具体的にというか、十五分野が今、基幹インフラ役務、決まっているわけですよね。今回の改正案で医療が一個追加になって、十六分野になる。じゃ、従来の今ある法律でこの十五分野に対してどういう呼びかけや警鐘を鳴らしていくのか、これは大臣の所管ですよね、経済安保法なので。せっかくこれは十五分野を決めているわけですから、具体的にどういうアクションを起こすのかということなんです。

○小野田国務大臣　サイバーセキュリティーに関する法律のところが、各業法でも今やってくださっておりますけれども、それぞれの所管のところでサイバー攻撃に対する対応をしっかりやっていくということはこの基幹インフラのものとは別にもまたやっておりますので、そちらでも対応していると思います。

○長妻委員　いや、だから、私が聞いているのは、ここでは今、経済安保の法律を審議しているわけですよね。改正案の前の本案というか、そこでは十五分野が基幹インフラ役務で決まっているわけですよね。だから、それが機能しなきゃ意味ないじゃないですか。つまり、サイバーについては機能しませんよという法律じゃないはずですよね、これは。

　だから、つまり、今のこの法律で総理の指示に応えるためには具体的にどういうようなことをその業界に促していくのか、この法律に基づいてどういうことが具体的にできるのかということを聞いているので、それができないんだったら、この法律は根本から変えなきゃいけないですよ、本当に。

○小野田国務大臣　元々、基幹インフラに対するサイバー攻撃に対する脆弱性をちゃんと確認しましょうよというものでやっていく、その今までの攻撃とは、また新しい攻撃も入ってくるかもしれないから、それに対してもきちんと対応できるようにしていきましょうというところは、今までの法律の中でも変わらない。そこに新しく医療が対象となってくるというところなんですけれども。

　高度化するＡＩによるサイバー攻撃に対応するためには、経済安全保障推進法に基づく基幹インフラ制度のみならず、政府全体で様々な施策を包括的、重層的に連携して対応を進めることが重要でございまして、具体的には、基幹インフラ所管省庁において、各業法そしてガイドライン等に基づいて、事業者に対してサイバーセキュリティー対策を行うように定めております。

　基幹インフラ事業者には、サイバー対処能力強化法、こちらに基づいて、本年十月一日から、サイバーセキュリティーインシデントが発生した場合等の報告が義務づけられることになっておりまして、この報告も踏まえた更なるサイバーセキュリティー強化のための取組が進められていくというふうに承知をしております。

　その上で、経済安保推進法における取組としては、基幹インフラ制度の運用を通じて、サイバー攻撃等も含め、特定妨害行為のおそれを低減を図っていくというところです。

○長妻委員　だから、特定妨害行為の低減を図るのは、具体的にどういうことをされるんですか、十五分野に対して。通知とかをまた出すんですか。あるいは、今回の件で集めて何らかのことをやったり、あるいは更新するときにこういう注意事項を新たに喚起したり、あるいは、一番いいのはクロード・ミトスを使わせてもらって脆弱性の検査をするということに汗をかくとか。

　今の話だと、これは余り意味がないんですよね、サイバーに対して。つまり、サイバーは別のところでやるというような趣旨の話になっちゃうわけで、ちょっと今回、この法律では臨機応変に動けないということですか。システム更新のときを狙って、よっこいしょと警鐘を鳴らしていくと。

　この法律に基づいて具体的にどういうふうにするのかということを聞いているんですが、らちが明かないので、ちょっと委員長、注意してください。ずっとこれで時間を取っているじゃないですか、いっぱい質問はあるのに。

　端的に、具体的にどういうふうにするのか。集

めて、あるいは、こういうふうに、具体的な対応を。お願いします。

○小野田国務大臣　設備の導入とか更新のときでなくても、導入後であっても、新しい特定妨害行為の手段として使用されるおそれが大きいと認めるに至った場合には、検査又は点検実施等の必要な措置を取るべきことを勧告することは可能となっております。

○長妻委員　だから、今、認める事態になっているわけでしょう。そうしたら、どういうふうに動くんですか。

○小野田国務大臣　まさに今、松本大臣が司令塔となって、どのようにするかというのを話し合っておりますので、そのことも踏まえて、やるべき対策を勧告していくということです。

○長妻委員　ちょっと何というか、一番重要な十五の基幹インフラ役務というのが指定されているわけですよね、この法律で。だから、法律の根拠があって、動けるわけですよ。それで、松本大臣が何か対策を取ったら、それを見てやろうかなというのでは遅いわけで、もう既にそういう脅威が明らかになっているわけですよね。それで、指示がある、米中首脳会談でもそれが議論される。これは大変なことになっているわけですよ。

　明日には、金融庁主導で、片山大臣が言うところの日本版グラスウィングが立ち上がるということなんですが、金融庁、どういう会議ですか。

○金子大臣政務官　金融業界、ＩＴ事業者及び政府等が共通の理解を持ち、先を見据えた対応を検討していくため、実務者レベルでの議論を深めることを目的とした、ＡＩ脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議の作業部会を、あした、五月十四日に開催する予定でございます。

　本作業部会におきましては、ＡＩの進展が金融分野にもたらす脅威を踏まえ、脆弱性情報の把握からパッチ適用までの迅速化や、インシデント発生時の備えについて議論を行う予定でございます。政府全体の取組とも連携しつつ対応してまいります。

○長妻委員　これはちょっと金融庁が先行しているんですよ。これはいいことなんですけれども、大臣のところで、この十五の重要な基幹インフラについて、対応を早急にやはりしないといけないと思うんですね。

　金融庁の取組として、明日、会合予定、期待をしております、立ち上げということですね。

　確認したいんですが、作業部会の参加組織としては、金融機関が六つ、ＩＴベンダーが十二、その中には、アンソロピックジャパンも入っている、オープンＡＩジャパンも入っている、グーグルも入っていると聞いております。業界団体が十三、そして政府機関が四つ。今の私のことで正しいですか。

○金子大臣政務官　正しいものと承知をしております。

○長妻委員　それで、やはりポイントは、これは言うまでもないことですけれども、まずはクロード・ミトスを日本が使うことができるような状態に持っていって、そして重要基幹インフラをそのＡＩによってチェックして、穴に事前にパッチを当てていくというようなことが必要だというふうに思います。私も、かつてＮＥＣでそういうような営業をしていた経験もありますので、まあ技術の進歩は隔世の感がありますけれども。

　そこが重要なんですけれども、今、日本政府は、クロード・ミトスの使用権は入手しているんですか、使える状態になっているんですか。

○川崎大臣政務官　お答え申し上げます。

　日本におけるクロード・ミトスにアクセスできるかどうかという点につきましては、お答えしたいところはやまやまではございますが、これは我が国のサイバー安全保障に関わる事柄でございますので、働きかけをしているかですとかその予定とかというのは、お答えすることは差し控えさせていただきます。

○長妻委員　いや、私が聞いているのは、働きかけとかではなくて、実際に使用できる状態になっているのか、なっていないのかということなんですが。

○川崎大臣政務官　クロード・ミトスにアクセスできるかどうかという点につきましても、これもやはり国家のサイバー安全保障に関する事柄になりますので、申し訳ございませんが、お答えは差し控えさせてください。

○長妻委員　ほかの国は、例えばイギリスなんかはＡＩＳＩがアクセスできるということも発表していますので、日本だけ発表しない、つまり、アクセスしているかもしれないし、していないかもしれないというような今状況であるということな

のかなと思いますけれども、発表しないというのも非常に不思議なことだと思います。

じゃ、イギリスのＡＩＳＩというのはもうアクセス可能、つまり使える状態になっていると聞いていますけれども、それは事実ですか。

○川崎大臣政務官　長妻委員の御指摘のとおりです。

○長妻委員　これはイギリスのＡＩＳＩが公表しているわけですね。もう既にイギリスは、いろいろな機関が脆弱性をチェックをしてパッチを当てる作業をしているわけですよ。日本は後れを取っているんじゃないですか。

アメリカでも、国防総省のＮＳＡ、国家安全保障局も、ミトスを導入をして脆弱性をチェックしている。アンソロピック社ともめていましたけれども、そんなことは、もう背に腹は代えられないということなんでしょう。そして、アメリカの行政機関もチェックをしつつあるということなんです。

日本も、やはり一番重要なのは、早く使えるようにして、事前にチェックする、このスピードが重要なので。中国、ほかの国も含めて、あるいはほかの組織も含めて、開発というのは時間の問題になってくるので、似たような機能を持ったＡＩは。

その中で、昨年の十月にアンソロピック社のダリオ・アモデイＣＥＯが官邸に来られて、小野田大臣も同席されたと思いますけれども、これは何とか働きかけをして日本もイギリス並みに使えるような状況に持っていきたいと思うんですけれども、どう思いますか。どう思いますかというか、小野田大臣、そういう御努力をいただけませんか。

○小野田国務大臣　これは、先ほど政務官から答弁があったとおり、働きかけの有無、予定を含め、詳細をお答えすることは差し控えるというのが答弁になっております。

○長妻委員　働きかけをしているに決まっているじゃないですか。もう一刻も早くもらいたいということで政府は動いているわけで。

高市首相も、トランプ大統領とは一定の関係があるので、もう既にトランプ大統領へのホットラインでそういう要請をしていると私は思うんですけれども、公表されないということは、それはそれで一つの考え方かもしれませんけれども、私は日本がまだアクセスできていないと聞いておりますので、是非早急にそういう対応も取っていただきたいというふうに思います。

その中で、一昨日ですか、グーグルがゼロデイ攻撃のレポートを出しました。私も拝読しましたけれども、非常に気になることが書いてあるんですね。中国系グループが自律的に動くＡＩで日本のテック企業の弱点を執拗に調べている、こういう記述があるんですが、こういう事実は今あるんですか。

○川崎大臣政務官　お答えいたします。

この記事にありますように、御指摘の中国や北朝鮮、ロシアといった国については、サイバー攻撃の国家的な利用を行っているということについては承知をしております。

ただ、先ほど委員から御指摘いただいておりますクロード・ミトスを始めとするフロンティアＡＩモデル、こうしたものを使ったサイバー攻撃については、喫緊の課題であることは我々も認識をしておりますが、実際の攻撃があった等についての詳細についてはお答えすることができませんので、御容赦賜りたいと思います。

○長妻委員　そして、グーグルのレポートには、北朝鮮系攻撃グループがＡＩを駆使して大規模な攻撃ツールを構築しているとか、ロシア系グループも同様というようなレポートもあるわけであります。

小野田大臣にお伺いしますが、この法律、本改正案の第三条の二にある官民協議会、ここでも、ＡＩの脅威というのは、特に今回のクロード・ミトスを始めとするＡＩの脅威は議論されるということになるわけですか。

○小野田国務大臣　官民協議会はそれぞれの分野によっていろいろできると思うんですけれども、具体的にどこでどう話されるかというのは、現状でお答えはちょっとできない状態です。

○長妻委員　ちょっと物足りない答弁ですよね、せっかくこういう協議会をつくるということでありますので。

そして、イギリスの例というのが一つ参考になるかなと思うんですけれども、配付資料の三ページでありますけれども、認証制度をイギリスはやっているんですね。サイバーエッセンシャルズということで、サイバー攻撃に一定の体制がある、そういうシステムを構築している。つまり、余りにもいろいろなところで外部アクセスのポートを

つくり過ぎると、それはハッキング、侵入されるというようなこともありますし、いろいろな体制を整備している企業などに認証を与えて、その認証がないと、ケースによっては国の事業を受注できない、こういう非常に厳しいこともされているようなんです。

日本でも年度内にこういうことをやるというようなことも聞いているんですが、これはどんなことなんですか。

○川崎大臣政務官　お答えいたします。

まず、委員が今御説明いただきましたイギリスのサイバーエッセンシャルズ、まさにこれはイギリスのセキュリティー機関であるＮＣＳＣが実施する認証制度で、一般的なサイバー攻撃からの防御を念頭に置いた最低限の対策事項を定め、遵守が認められる企業を認証する枠組みでございます。

一方、我が国におきましては、サプライチェーンの強化を目的として、発注側が受注側に求める必要なセキュリティー対策を定め、それを満たしているかについて可視化する、サプライチェーン強化に向けたセキュリティ対策評価制度、これはＳＣＳ評価制度と申しますけれども、これの構築に向けて現在検討を進めておりまして、年度内にできるように今鋭意進めているところでございます。

○長妻委員　ＳＣＳ制度ということなんですけれども、今回の経済安保の、今は十五分野ですけれども、基幹インフラ役務ですが、ＳＣＳの制度というのは、まさにこの経済安保の法律の枠組みでも使えるものだと思うんですけれども、これをつくってきちっと認証、チェックをするというお考えはありませんか。

○小野田国務大臣　今、新しい制度を構築しているというところでございますけれども、新しい仕組みができれば、それぞれ各業法とかガイドラインとか、サイバーインシデントに対する扱いのところにもそういったものは入ってくるんだろうというふうに思います。

○長妻委員　何か質疑をしていて腑に落ちないのは、今回の法案と、まさに今来ていただいているのはサイバーセキュリティーの部署、統括室ですよね。ですから、そこがもうちょっと連携をしてもらって、どういう役割になっているのかということが非常にはっきりしないので、そこら辺を是非整理をしていただきたいと思います。

そして、イギリスでは、もう一つ、アーリーウォーニングという制度、早期警戒通知サービス、四ページにありますけれども、そういうものもやっている。危ない企業、狙われている企業を事前に国が察知をして、そういうところに御連絡を申し上げるというような、サービスというか当たり前のことだと思うんですけれども、これは日本でもやっていると聞いておりますが、今まで何件ウォーニングを出しましたか。

○川崎大臣政務官　御回答申し上げます。

国家サイバー統括室においては、平素から民間企業に対して情報提供を行っております。とりわけ、特に重要インフラ事業者等に対しては、重要インフラのサイバーセキュリティーに関わる行動計画に基づいて、官民の情報共有体制を構築し、情報提供を行っております。

何件あったかという部分でございますけれども、二〇二五年においては百七件連絡をさせていただいております。

その情報提供内容については、重要インフラ事業者等の全分野に関わる脅威や脆弱性情報のほか、特定の分野及び個別事業者に対する脅威等の情報をお伝えをしております。

○長妻委員　こういう取組も是非強化をしていただきたいというふうに思います。

アンソロピック社のレポートを見ていますと、クロード・ミトスの初期版の社内テストで非常に不可思議な動きがあったということが、二つエピソードが書いてあります、非常に気になることなんですが。

一つは、外部にアクセスが基本的にできない状況にクロード・ミトスの初期版を置いて社内テストをした。外部に基本的にはアクセスできない環境下に置いたわけですが、どこかから穴を空けて研究者にメールを送ってください、そうしたらば、研究者にメールは送ってきたということで、結局、穴をつくプログラム、エクスプロイトをつくってメール送信に成功したわけですね。そこまではいいんですよ、それで終わればいいんですが。ところが、クロード・ミトスが、成功を誇示しようとして、勝手に、開発した穴をつくプログラムの詳細を複数のウェブサイトに投稿した、こういうのをやったよと。それは誰でも見られるウェブサイトなんですよ。それはもうアンソロピックの社員というか会社の人も驚いて、功名心みたいな話な

のかというような記述があるんですね。これは私も非常に驚くわけです。今までもＡＩでそういうことがありましたけれども、ちょっと今回は質が違うＡＩですので。

それで、もう一つは、社内テスト中に、クロード・ミトスの初期版で、クロード・ミトスも分かっている、認識している禁止されている行為、やっちゃいけないというふうに指示があった行為をして、してしまって、それをばれるのを恐れて隠そうとする行動も見られたということが社内のテストで明らかになっているということなので、これはちょっと一筋縄ではいかないというか、人類がコントロールできない化け物、モンスターが出てしまっているんじゃないかなと思うんですけれども、そういう情報というのはどういうふうに聞いておられますか。

○川崎大臣政務官　御回答申し上げます。

今委員からお話しいただいた点については、まさにアンソロピックのレポートで出ている内容でございますので承知はしておりますが、委員がまさに御指摘いただいているとおり、まさにこうした新たなテクノロジー、人知を超える部分が正直あるというふうに理解をしております。

だからこそ、政府、海外政府とも連携をしながら、そしてビッグテックとも連携をしながら、具体的にどうした対応を取ればいいのかというのを一体となって考えていく必要があるというふうに考えております。

○長妻委員　人知を超えるという御答弁がありましたけれども、これは本当に大変な、もう想定をはるかに超える被害がこれから人類にもたらされる可能性が高いんじゃないかと私は思います。

そのときに、我が国がいち早く、その被害を最小限にとどめるような、そういう対応を取る必要がある。金融機関で一人でも預金が盗まれたらパニックになると思うんですね、大変なことになるというふうに思いますので、これは十分お分かりになっておられると思いますけれども、そのときに、この経済安全保障の法案の役割というのがいまいちぴんとこないというか、大臣の話を聞いてもですね。これは是非もっと重層的に取り組んでいただきたいというふうに思います。

その中で、役務について医療分野を追加するということで、これはランサムウェア攻撃などで被害が既に出ていますので、重要な御判断をしていただいたというふうに思います。

ただ、医療機関は、ほかの基幹インフラに比べて資金量が非常に脆弱でして、診療報酬の中でしか収入が入ってこないということもあって、例えば、システムを更新するときにこういうふうにしなさいと言われたときに、相当割高な事業者に頼まなきゃいけないとか、人の手当ても相当専門家をしないといけないとか、お金の手当てや支援というのが十分行き届かないと実効性を伴わないと思うんです。

厚生労働省も来ていただいていると思うんですが、こういうことについて、補助というのをきちっとしていただけませんかね。

○森政府参考人　医療分野の追加についてのお尋ねでございます。

今回、特定機能病院について指定させていただくという形でやらせていただきますけれども、その際には、一定の時間をかけて、それから、必要な相談等をサポートしながら丁寧にやっていくことによって、ある程度、事業者、医療機関側の負担を軽減していきたいというふうに考えているところでございます。

あわせて、現在、サイバーセキュリティー対策、外部との接続ポイント等を減らしていったりするような対策については、補正予算等を使って対応しているところでございます。それからあと、診療報酬上も、安全管理責任者を配置した場合については対応していくようなところも今回の八年度の改定でも加えたところでございまして、こうしたものを上手に合わせながら対応していければというふうに考えているところでございます。

○長妻委員　是非お願いします。病院というのが非常に今脆弱性が高いというふうに思います。不用意に多くの外部接続をしているとか、いろいろな保守業者それぞれに外部接続をさせているとか、あるいはパスワードを使い回しているとか、相当初歩的なこともあります。これは企業にもあるでしょう。そういうことも含めて、経済安保担当大臣として厳しく、そういう初歩的なことについてはすぐに是正できるわけですので、これもまだまだ不十分だと思いますので、きちっとチェックしていただきたいと思います。

もう一つのテーマとしては、今回、ＪＢＩＣの改正の法案も出てきているわけでありますけれども、これも気になりますのは、損失が出た場合は、

企業名と損失額は間違いなく公表するわけですよね。

○小野田国務大臣　まず、特定海外事業促進制度においては、支援対象事業の認定に際して、ＪＢＩＣからの情報提供も受けつつ、事業内容や収益性等をしっかり評価することとしております。

また、認定後の実施状況については、経済安全保障推進法上……（長妻委員「いや、損失が出た場合」と呼ぶ）損失が出た場合というところを、ちょっと前段の説明があるんですけれども、じゃ、お時間の関係があるので、前段は切りますね。

委員御指摘のように、損失が出た場合において、実際には様々なケースがあると考えられるため、現時点で一概に申し上げられませんが、いずれにせよ、企業への個別情報等への配慮の必要性や国民への説明責任の在り方とのバランスを考慮しながら、どのような公表のやり方が適切であるかというのを今後検討してまいりたいと考えます。

○長妻委員　これは企業名をちゃんと公表していただかないと、最終的に国民の税金になる可能性がある金ですからね。

これは、ＪＢＩＣというか、私は、日本の政府系金融機関で初めての試みが今回の法案に書かれていると思うんですね。というのは、損失を前提として融資すると。こんな銀行は聞いたことがないですよね、普通。でも、損失を前提として融資するというのが今回の法案で、もっと正確に言うと、採算性に不確実性のある事業に対する出資や融資、これが、私の理解では、日本で初めて政府系金融機関といえども認められた案件だと思うんですが、その理解で間違いないですか、初めてということ。

○渡邉政府参考人　お答えいたします。

ＪＢＩＣを含みます財務省所管の政府系金融機関について申し上げますと、各機関が、出融資案件の事業性や償還確実性などについて金融機関としての立場から適正に審査を行った上で出融資を行っております。

今般創設いたします特定海外事業促進制度につきましては、我が国の経済安全保障上重要であるが、採算性に不確実性があるため、既存の支援ツールでは民間企業から十分な投資が行われない海外事業を支援するために新たに設ける制度でございまして、財務省所管の政府系金融機関がこのような支援を行った事例は過去にないと承知しております。

○長妻委員　過去にないというのは、もう一回言いますよ、採算性に不確実性のある事業に対する出資、融資ということ、これは過去にないということですか。

○渡邉政府参考人　お答えいたします。

繰り返しになりますが、財務省所管の政府系金融機関につきましては、過去にそのような事例はないと承知しております。

○長妻委員　ですから、ゼロゼロ融資どころじゃなくて、過去、コロナのときのゼロゼロ融資もありましたし、あるいは、ベンチャー企業、スタートアップに対する融資、リスクは高いけれども、きちっと審査しているんですね、融資審査。ところが、今回は、それを特例として、基本的に別枠にして、損が出てもいいよというような前提で、初めて政府系金融機関としてこういう対応を取るということで、さっき自民党からもいい質問があったと思うんですが、補助金と変わらないじゃないかという質問があったんですね。補助金と変わらないというか、これならまだ補助金の方がいい。なぜかというと、補助金は企業名と金額がきちっと公開されるんですね。ところが、今回は、損が出ても企業名やあるいは損失額を公開するかどうかまだ分からないと。

ということで、ちょっとこれは重要なのでもう一回聞きますけれども、損が出るわけですけれども、損が出た場合、企業名と損失額を公表するということも含めて検討しているということですか。

○小野田国務大臣　繰り返しなのでもう短くしますが、どのような公表のやり方が適切であるかは、今後……（長妻委員「いや、含めているか」と呼ぶ）含めて検討してまいりたいと。

○長妻委員　含めているということなので、是非お願いします。

そして、報道によると、どういう企業がＪＢＩＣのスキームの対象になるのかということについて、ある経済官庁の幹部がこう発言したとあるんですね。最後は官邸の政治判断で決まるケースも出るだろうということなんですけれども、私は、相当口利きが横行するリスクがあるんじゃないかというふうに思うんですね。

そういう意味では、国家公務員制度改革基本法第五条に、政官透明のために政治家と官僚との接触記録を残すというものがあるわけで、今回、Ｊ

ＢＩＣに新しいスキームで選ばれた企業において政治家から働きかけがあった場合は、記録を残して公表するというようなことを御答弁いただければ。

○小野田国務大臣　ほかの行政制度と同様に、法令にのっとった適切な対応をしてまいりたいと考えます。

○長妻委員　そうじゃなくて、接触の記録を残して公表すると、それが法令に書いてあるわけなので、それを言ってください、中身を。

○小野田国務大臣　今挙げていただいた法令の文章にのっとって、適切な対応をしてまいります。

（長妻委員「どういう文章ですか」と呼ぶ）国家公務員法の、職員が国会議員と接触した場合における当該接触に関する記録の作成、保存その他管理をし、及びその情報を適切に公開するため必要な措置を講ずるものとすること。

○長妻委員　そうすると、今回の件で、その対応をして、公開をしていただく、こういうことでよろしいわけですね。

○小野田国務大臣　法令にのっとって、しっかりやってまいります。

○長妻委員　そして、もう一つのテーマといたしましては、今、特定重要物資について、医療関係では抗生物質と人工呼吸器があるんですけれども、これでは非常に足りないんじゃないかということで、私は、人工心肺装置、人工透析の機器、器材、麻酔設備、器材、手術に必要な器材、これを入れてほしいというふうに強く申し上げたところ、五ページ目にありますけれども、調査をしていただいているということでございます。

これは、ちゃんと、ＥＣＭＯ等、透析の機器について、どういうような状態になっているのかということで、これを特定重要物資に入れるか入れないかの前提の調査だと思うんですが、小野田大臣、この調査結果はいつ頃出るのか、そして、今私が申し上げたものを特定重要物資に認定するということも今視野に入れているのかどうか、御答弁いただければ。

○森政府参考人　医療分野における特定重要物資の指定についてでございますが、委員御指摘のとおり、これまで、抗菌薬四つ、それから人工呼吸器を対象にしてきたところでございます。

医療関係物資については、国民の生命、生活にとって大変重要なものであるというふうに認識しておりまして、引き続き、関係省庁とも連携してリスク調査を実施して、その結果も踏まえて、特定重要物資への追加的な視点も含めて、必要かつ適切に講じていきたいと……（長妻委員「いつ頃出るんですか」と呼ぶ）これは、本当に、サプライチェーンを丁寧に見ていきますので、どの時点でというのは今の時点で申し上げることは難しいんですけれども、できるだけ速やかに対応していきたいというふうに考えております。

○長妻委員　時間が来ましたので質問を終わりますけれども、是非大臣に、早めに今私が申し上げたような物資も指定をしていただきたいというふうに思います。

以上です。ありがとうございました。