令和７年度総務省行政事業レビュー公開プロセス

令和７年６月１６日

（３）IoTの安心・安全かつ適正な利用環境の構築

【阿南会計課長】　それでは、３つ目の「IoTの安心・安全かつ適正な利用環境の構築」について議論に入ります。

ここからは、株式会社コラボラボ代表取締役、横田響子先生に御参加いただきます。よろしくお願いします。

初めに、担当部局から１０分程度で資料に沿って説明をお願いします。よろしくお願いします。

【説明者】　サイバーセキュリティ統括官室でございます。

案件といたしましては、「IoTの安心・安全かつ適正な利用環境の構築」ということで、施策の概要について１０分程度で御説明を最初にさしあげたいと思います。

次、お願いします。IoTサービスの普及とサイバー攻撃の現状ということで、本施策におきましては、いわゆるIoT機器と呼ばれるような比較的ネットワークに接続されたユーザーに近い機器、これらを総称して、IoT機器と呼んでおりまして、その中に具体的には無線LANのルーターでありますとか、あとは監視カメラでありますとか、そういう幾つかの類型で分けられるような機器がありますけれども、それを総体としてIoT機器と呼んでおります。こうしたIoT機器のセキュリティの向上を目的としまして本施策を進めているわけでございますけれども、こうした機器を悪用した、我が国のみならず世界的にサイバー攻撃が起こっておりまして、本施策におきましてはその中の代表例でありますDDoS攻撃と呼ばれるものを対象に対策を講じているというところでございます。本施策におきましてはこうしたDDoS攻撃といったものに着目をいたしまして、この攻撃自体は、今御紹介したIoT機器を踏み台として、例えばスライドに書いてございますような、米国のDNSの事業者を対象とした攻撃でありますとか、国内でありますと、行政機関であります国交省の監視カメラでありますとか、こうしたものを具体的に踏み台とした攻撃といったものが実際に起こっているという状況でございます。

次、お願いします。そもそも、DDoS攻撃というのはどういうふうに起こるかということでございますけれども、左に書いてございます攻撃者が、ネットワーク上の中核であります、C&Cサーバと言われるサーバを自分のコントロール下に置くと。このサーバを経由しまして、

今御紹介をしたIoT機器を実際乗っ取っていくと。これを一つのグルーピングをいたしまして、攻撃対象に対してこうしたグルーピングをしたIoT機器から大量の情報を送りつけ、その対象となっている企業でありますとか団体でありますとかこうしたものを、情報を送りつけることによってネットワークを麻痺させるといった攻撃の類型でございます。

次、お願いします。こうしたIoT機器のセキュリティ上の課題ということで、現状、ネットワークに接続されているIoT機器の結構な割合ですね。ここに書いてございますが、ほぼ半分ぐらいという割合になりますけれども、こうしたネットワーク機器、IoT機器は、かなり古いものが多いといった現状があるということでございます。こうした古い機器というのは、設定上の不備でありますとか、実装されているソフトウェアがアップデートされないといった課題を抱えておりまして、今御説明をしたようなサイバー攻撃のいわゆる踏み台にされやすいといった状況になってございます。こうした状況の中、実際に利用者という観点で見ますと、個人であるとか法人であるとか幾つか類型は考えられるわけでございますけれども、いずれにしても、管理体制の不備があったりですとか、あるいは利用者の意識が低いですとか、こうしたものも併せ考えると、こうした意識の改善でありますとか、機器自体の設定ですとか、ソフトウェアのアップデートですとか技術的な対策、これらを複合的に行っていく必要があるというふうに考えられているところでございます。

次、お願いします。このDDoS攻撃の、実際にどういう形で起こるのかといった仕組みに着目をしまして、これに対してどういう対策を行うべきかという全体像を示したのがこのスライドでございます。攻撃の手法ですね。その仕組みを分解いたしますと、ネットワーク上に接続されているサーバの部分とIoT機器の部分、これは大きく２つ挙げられるということでございます。その意味におきまして、このサーバに対する対策、それからIoT機器に対する対策というのが２つ大きな対策の柱でございまして、このスライドに書いてございます、ネットワークとして分類されますC&Cサーバへの対処というのが１つ。それから、IoT機器の端末側として書いてございます、IoT機器に対する対策が１つと。それに加えて、いわゆる利用者の意識を高めていくという意味において、周知啓発というのも併せて行う必要があるということで、施策の柱としてはこの３つということを挙げているところでございます。

次、お願いします。１つ目のIoT機器への対処ということで、これは総務省の所管法人でありますNICTが実際にネットワークの観測を行いまして、IoT機器に内在するような設定の不備でありますとか、ソフトウェア上の脆弱性でありますとか、こうしたネットワーク上のセキュリティ上の弱点と呼ばれるようなところを観測によって洗い出しているということ

でございます。こうした観測の結果に基づきまして、具体的にはインターネットサービスプロバイダのような事業者を経由して、その事業者のサービスに加入しているような個々のユーザーに対する注意喚起を行ったりですとか、あとは実際に機器を製造しているメーカーでありますとか、システムを構築しているSIerでありますとか、こうしたその他の事業者を通じて技術的な修正を行ったりですとか、あとは一般的な広報によって意識を高めていただくですとか、幾つかの手法によってIoT機器の脆弱性を改善しようという取組を進めているということでございます。

次、お願いします。こうしたIoT機器への対処につきましては、具体的に実施主体でありますNICTの業務を定めたNICT法、この中で具体的に法定されている事業でございまして、NICTはこの法律に基づき、この事業を実施しているということでございます。具体的には、ID・パスワードの設定の脆弱性、こうしたものを観測によってあぶり出すと。加えまして、ファームウェア、いわゆるソフトウェアの脆弱性、こうしたものも発見をしていくと。加えて、実際にマルウェアに感染してしまっている機器、こうしたものも併せて、ネットワーク上に所在するこうした機器を実際に観測することによって発見をして対策を講じるということでございます。

次、お願いします。２番目のサーバへの対処ということで、これは具体的に、サーバを流れるような、フロー情報と呼ばれる特定の情報、これを観測することによって、このサーバ自身が実際にサイバー攻撃に対して加担をしているかどうかというのを発見するということでございます。この事業自体は実際に実証事業として現在行っているところでございまして、実証事業の中で、実際に攻撃に対して加担をしている可能性があるかどうかといったことを検知したりですとか、こうした結果に基づいて、対策の全体像でお示しをしましたけれども、IoT機器の観測、あるいはその注意喚起と、こういった一連のフローの中にこうしたサーバに関する情報も加味をしながら注意喚起、あるいは結果的にはその対策の効果の確認といったところを試行的に進めているというところでございます。

次、お願いします。３番目は、意識向上ということで、リテラシーの向上でございます。これに関しては、主に無線LANが個人のユーザーが比較的多いということで、こうした方々に対する意識の啓発という意味におきまして、セキュリティのガイドラインを作成したりですとかということを通じて実際に意識向上を図っているということでございます。対象としては、具体的に個人のユーザーの方、あるいは専門家の通信事業者もいますけれども、その他、それぞれの業態の中で事業をしていらっしゃる方が通信サービスとして無線LANを

提供する場合、こうした方々も当然対象となるわけでございまして、幅広い対象の方に参照していただけるようなガイドラインの作成をして御活用いただいているという内容になってございます。

次、お願いします。こうした取組の今後の方向性でございます。１番目のIoT機器への対処ということで、これに関しては、以前はIDとかパスワードといった機器に対する設定の不備といったところが主体であったということでございますけれども、加えて、最近はソフトウェアの脆弱性といったところが主体になりつつあるということで、こうしたところを重点的に取組を進め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。

２番目のサーバの検知・対処につきましては、実際に実証実験の中で一定程度の効果が確認されたということで、こうした情報を積極的に事業者の方に利活用していただくといった方向性で進めていきたいというふうに考えてございます。

３番目のリテラシーの向上でございますけれども、これは引き続き周知啓発といったところを継続するということが柱でございますけれども、必要に応じて、技術が進んでまいりますので、技術のアップデートを重ねながら、内容の改訂も行いながら、こうした周知啓発といったところを継続して行っていくということを予定しておるということでございます。

こうした取組、今国会で御議論いただいて成立をいたしましたサイバー対処能力強化法、これはいわゆるネットワーク上のサイバー攻撃に対する機器を含めた脆弱性に対する対処といったところが内容として含まれているということでございまして、これに対する対処を官民連携を進めていく中で行っていくと。そういった意味において、こうした大きな流れの中で、総務省、NICTが取り組んできたこうした事業の整合を図りながら、NICTが獲得をした脆弱性の情報などを適切に共有を図りながら、注意喚起の業務、こうしたものも連携を図りながら今後も進め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。

以降、ちょっと参考の資料として幾つかつけてございますが、最後、事業レビューの短期あるいは長期のアウトカムということで、既にペーパーのほうに書いてございます。参考にしていただきますと大変幸いでございます。

説明は以上でございます。

【阿南会計課長】　ありがとうございました。

では、本事業の論点について説明させていただきます。

まず、１つ目の論点は、「適切なアウトカムが設定されているか」という点です。

まず、NOTICEの事業についてですが、４点記載しております。①のところですが、短期、

長期アウトカムとして、注意喚起の対象者以外も含めて実施したアンケートによって把握した安全対策の認知率や安全管理対策の実施率を指標としておりますけれども、これでは指標が改善しても悪化してもNOTICEの効果が他の要因か分からないので、NOTICEによる改善効果を測定できる指標を設定できないかという点でございます。例として２つ書いてありますが、１つ目は、例えば前の年に注意喚起したIoT機器が翌年は注意喚起の対象にならなかったら効果があったと考えられるのではないかということであります。２つ目ですが、アンケートの結果をもし使うということであれば、注意喚起の対象者のみの結果を見たり、それ以外の回答と比較することでNOTICEの効果が分かるのではないかということでございます。

それから次に、NOTICEの論点②ですが、説明資料に出てきたマルウェア感染IoT機器検知数やファームウェアに脆弱性を有するIoT機器数を指標または参考指標として取り入れられないかという点でございます。

次に、NOTICEの論点③ですが、調査対象IPアドレス数の目標である１．２５億件が妥当なものかという点であります。

次に、NOTICEの論点④ですが、成果指標の根拠としているIoT機器に関するアンケートは調査方法や回答数が公表されていないので、アンケートの信頼性が分からないと。また、レビューシートには注意喚起対象者以外も含めたアンケートと書いてありますが、注意喚起対象者がどの程度含まれるかという点も分からないので、調査方法や結果を明らかにすべきではないかという点でございます。

次に、無線LANセキュリティガイドラインに関する、論点の⑤としてありますが、短期アウトカムと長期アウトカムの目標値や達成率が適当かという点であります。ガイドラインの認知率や安全管理対策の実施率の指標が横ばいで、目標に達していない状況が続いているんですけれども、達成率９０％以上という高い評価になっているのは少し違和感があるのではないかという御指摘がありました。

それから、２つ目の論点ですけれども、サイバー攻撃の脅威が増大する中で今後どのようにセキュリティ対策に取り組んでいく必要があるかという、事業そのものの在り方の論点であります。

まず、NOTICEの事業についての①の論点ですが、プロバイダに任されている注意喚起の方法をしっかり把握すべきではないかという点であります。例えば、注意喚起の方法をどのように伝えているのかと。メールなのか、郵送なのかとか、どのような文面で伝えているのか

と。例えば、あなたの管理する機器は危険ですよというような具体的な注意喚起なのかというようなことが考えられるかと思います。その際、プロバイダによって注意喚起の方法が異なるのであれば、注意喚起による改善効果をプロバイダ別に比較できれば効果的な周知方法が分かるのではないかという点でございます。

次に、NOTICE事業の論点②ですが、担当部局から、事前勉強会で今後、プロバイダに加えて、機器の製造業者やシステム開発業者との協力を図ることも検討するという御説明がありましたけれども、どのように推進していくのかという点でございます。

次に、無線LANセキュリティガイドラインに関する論点③ですが、他の政府機関でも類似の取組があると思われるが、役割分担や連携はできているのかという点でございます。

それから最後、３つ目の論点ですけれども、調達の適正化の観点で、本事業は契約において一者応札が多く見受けられるが、改善の余地がないかという点でございます。

論点についての御説明は以上でございます。

それでは、論点に沿って議論に入らせていただきます。

まず、１番のNOTICEの論点①ですが、NOTICEによる攻撃抑制効果を把握するため、注意喚起したIoT機器の対策実施状況を把握できる指標を設定できないかという点。この点は横田先生から御指摘いただいたと思いますので、よろしくお願いいたします。

【横田先生】　ありがとうございます。

アウトカムをより踏み込んだ設定ができないかという考えの下、質問をさせていただきたいんですけれども、まず、現状を確認、カバーしているIPアドレスですね。アウトプットの中でIPアドレスのカバーがどんどん増えている、確認できる。要は、プロバイダを通じた検知する能力が高まっているという理解はしているんですけれども、現状、どれぐらいのカバー率なんでしょうかということが１点と、また、前年注意喚起を行ったものがどれぐらい次年度には改善がされているのかというのを、今、確認できる状況であればどれぐらいなのかというのをまず教えていただきたいんですが、いかがでしょうか。

【説明者】　１点目は、全体どれくらいIPアドレスがあって、それのどれぐらいカバーされるか。これは御質問というか、論点の中での、いわゆる指標の一つとして書いた、１．２億とか１．２５億と書いてございますが、これは前回少し御説明をしたところなんですが、一定規模以上のISPの事業者さんがこの事業に対して御協力をいただいている。その中で、その事業者さんがカバーしているIPアドレスを観測として使わせていただいているという形でございますけれども、ほぼ一定規模以上のIPアドレスは、我々の見積りでは大体１．３

億ぐらいなので、ほぼほぼ全てをカバーしているという状況でございます。その意味において、観測の対象としては、もちろん１００％ではないんですが、ほぼカバーしている中で、それらの、ある意味ではそこに所在するような脆弱性というのはほぼ洗い出しができているのではないかというふうに考えております。

その中で、一定割合でいわゆる脆弱性のある機器というのが出てくるわけでございますけれども、出てきた中で一部、注意喚起に値するようなものに対して実際の注意喚起行為を行っていく。具体的に申し上げますと、大体４分の１ぐらいが現状でございまして、脆弱性として感知されたものの中の４分の１ぐらいが注意喚起という形を行っているということでございます。それに対して実際に対策がされたり、されなかったりということで、具体的なアクションのフェーズに移っているということでございます。

【横田先生】　ありがとうございます。

改めて、カバー率、発見できる、カバーできている範囲も広いですし、NOTICE自体の能力というのも、協力いただいて注意喚起にも結びついているということで、やはり実施している事業としてはすばらしいんですけれども、それが改善につながっているのか。要は、最終的に攻撃をされないことが目的となりますので、今おっしゃっていただいた注意喚起をしたうちでどれぐらい改善しているかというのを確認できる状況にまずあるのかということと、やはりそれを改善できているかまでを追ってアウトカムとして設定することができないのかというのをぜひお考えいただきたいんですけれども、いかがでしょうか。

【説明者】　ありがとうございます。

現状は、御説明の中にもあったんですが、この事業自身がアンケート調査を行っておりまして、そのアンケートの対象というのは、まさに注意喚起にある意味では直接ひもづくわけではないんですが、広く一般的な機器から一定程度の割合を抽出して、それが具体的にどういう形、アクションを取る、意識啓発としてどれくらいの割合かですとか、あとはその中で実際に対策が行われたかどうかというのは一般的な形で行っているわけでございますが、それはこの施策自体が世の中のIoT機器のセキュリティのレベルを上げるというのが最終的な目標なので、そういう形に落とし込んでやっているというのが現状でございます。その意味において、まさに先生御指摘の、事業としてフォーカスをしたときに、事業として行っているプロセスがきちんと効果が上がっているのかという意味では、まさにISPに対して注意喚起をし、その注意喚起を母数としたときに、それに対してどれぐらいアクションが取られたかみたいな、その部分を切り取るというのは一つのやり方かなというふうに思ってお

ります。

ただ、一方で、事業自身が、注意喚起というのが一つの、まさにユーザーに対しての情報の届け方として有力な手法であることは間違いないんですが、それ以外に一般的な周知啓発みたいな形での意識啓発活動ですとか、違う形でも最終的な脆弱性の改善を行っていただくための努力というところも一応我々は踏まえておりまして、その意味で広く最終的にどうなったのかというところを指標としては捉えているということでございます。

加えて、具体的に効果がどれぐらい出たのかということでいいますと、少しまた切り口は変わるんですが、例えば、このNOTICE事業の中で実際にNICTが観測を行いまして、脆弱性のある機器とかメーカーとか、あとは型番ですとか、そういったものが世の中に広まっているもの、広まっていないもの、いろいろ出てくるわけでございますけれども、例えば影響度が非常に大きいと思われるもの、要は普及が進んでいるような機器、メーカーの機器ですとか、そういったものは時々あるわけです。こうしたものに着目をしたときに、そういうものが発見され、どれぐらい普及をしているかという推測がある時点であったときに、NOTICEのこうした活動を通じて、これはかなり具体的にフォーカスを当てているケースなんですが、どれぐらい時系列とともにその脆弱性が改善されたかというのを実は見ていたりするんです。そういう意味では、まさに先生が御指摘いただいた指標の設定の中でもさらに具体的なところを見ているみたいな活動を行っておりまして。ただ、それは特定の機器に着目をしているので、指標としてはちょっとなじまないですが、参考としてそういうふうな対策を講じることによって実際にセキュリティ上の脆弱性が改善しているみたいなデータの取り方もしているところもありますので、そういう意味では、このNOTICEの事業を行うことによって、最終的には世の中の機器のセキュリティレベルを上げていくという最終目標に向けての評価の仕方というのは我々もいろいろあり得るなと思っておりまして、まさに先生が御指摘いただいたところも一つ、まさに政策としての進め方の評価という意味では非常により効果を図るための切り口だなと思っておりますので、まさに幾つか視点がある中で、どういった形で改善を図るとNOTICEの事業がより透明性高く、効果がどれぐらい上がっているのかというのが見えるかというのを検討させていただければありがたいなと思っております。

【横田先生】　ありがとうございます。参考指標だけでも、ぜひ、おっしゃっていただいたように、具体的に改善につながっていくことが見えるものが追加されればよいなと思います。

【阿南会計課長】　ありがとうございます。

審議途中ですけども、有識者の先生方におかれましては、御議論いただきつつ、コメントシートの御記入もお願いいたします。１６時３０分めどで回収させていただきます。

ただいまの論点①に関連して、ほかの先生方、何かありますでしょうか。

よろしければ、論点の②に行かせていただきます。西出先生です。今、回答が少しあったかもしれませんが、他の観測結果を参考指標として取り入れられないかという御指摘でございます。よろしくお願いします。

【西出座長】　今の御指摘の中に回答もあろうかと思いますが、私がこれをお話しさせてもらったものの一番は、NOTICEの観測実績の中での一番最後の、ファームウェアに高リスク脆弱性を有するIoT機器、月４，１３８件というのを見つけまして、これはこれの数が減るに越したことはないだろうというのが直感的にありまして、こういうのを減らす努力をしていくみたいな意味合いでアウトカム指標的なモニタリングができないかというふうに疑問を持ったものですから、御質問させていただいた次第です。この１点についてお答えいただければと思います。

【説明者】　ありがとうございます。

最初の施策の説明の中で、今スライドの一部が出ておりますけれども、まさに左下に書いてございます、４つの数字を掲げさせていただいておりますが、実はNOTICE事業自身はホームページをつくっておりまして、いろんな観測データというのは皆さんが御覧いただけるような環境を少しずつ整えているという状況でございまして、実はここの数字はそうした周知啓発の一環として御確認をいただけるような形で公表している数字でございます。そういった意味で、観測の前提となるような件数、一番上に書いてございますが、観測総数から始まりまして、そうした対象となる１．２５億件を観測した結果、実際にマルウェアに感染したIoT機器の数がどれぐらい出ているかですとか、あとはID・パスワードのような脆弱性を抱えているような機器がどれぐらいですとか、まさに先生が御指摘いただいたような、これから取組を強化していかなきゃいけないのはファームウェアの部分ですね。そのファームウェアの部分で非常にリスクの高いものがどれぐらいあるかというのがそれぞれ数字として出てきていると。これはまさにある時点での観測の結果として、これぐらいありますよというのを情報としては出そうということで確認をいただけるような形になっていると。その中で、具体的にそれぞれ注意喚起をしたりですとか、あとは一般的な周知広報をしたりですとかという取組を進めたりですとか、あとは特定の、先ほどちょっと御説明さしあげたんですが、特に何か着目すべきメーカーの機器ですとか型番ですとか、影響が非常に大きい

ものというのは個別に着目をして、時系列でトレースをして、どれぐらい減ったかですとかというのは個別の取組としては追加的にやっているという状況でございます。

【西出座長】　どうですか、これ。アウトカム指標として成立しそうなところはありますか。ファームウェアに高リスク脆弱性を有するIoT機器を指標として考えたらということです。

【説明者】　ある時点での観測の結果ですので、参考指標としては当然あり得るかなというふうには思っております。というのは、ある時点での観測というのは、まさに中身の部分が、以前に観測をされた脆弱性を持つ機器については当然時間の経過とともに対策をすれば数が減っていくということになりますし、要するに発見された脆弱性を持つ機器がそれ以上種類として増えなければ徐々に減っていくということは当然確認をされるわけでございますが、時系列上の観測点が変わると、また新たな脅威というのは当然出てくるわけでございまして、その瞬間の数字というのはそれらの合算値という形になりますので、その意味において、そこを減らす努力は当然している中で、過去に発見されたものは当然その対策をして減っていくということは確認されながらも、時間がたった、観測点が時系列とともに移っていったときのそれぞれの瞬間での数字というのは実は中身が大分変わってしまっているので、そこを指標とすると、それが指標としてどういう形で評価できるかというのはなかなかちょっと難しいかなと思っておりまして。いわゆる注意喚起、あるいはワーニングの意味を込めて、こうした数字を広く提供するということは必要かなと思いますが、それは指標は指標として、現行あるいはアップデートした形での指標を設定した上で、こうした観測データを追加的に、世の中に対するワーニングの意味を込めて、併せて公表する、あるいは参考指標として掲載をするという形であれば、全体としての施策の効果の検証、あるいは観測データの公表をすることによっての世の中に対するワーニング、双方の意味合いを込めた形での設定ができるんじゃないかというふうには考えております。

【阿南会計課長】　ただいまの議論に関連して、ほかの先生方、よろしいでしょうか。

そうしましたら、論点の③について、先ほど話が出てしまったようですが、調査対象のIPアドレスの目標１．２５億の妥当性、カバー率ということで、鈴土先生、追加でありますでしょうか。

【鈴土先生】　ありがとうございます。

僕の基本的な問題の認識というのは、要するに、極論すれば、国内にこれだけIPアドレスが全体であります。そのうち、調査の対象としているのはこれだけです。調査の対象として

いるこれだけのIPアドレスに対して毎月どのぐらいの比率で調査をかけています。その調査の結果、これだけ危ないのが見つかって、それを追跡調査していったら、我々のワーニングのおかげでこれだけ直っていましたというのを追えると、国民としては、ある意味安心できる。ああ、これだけしっかりやっているんだなということで安心できるわけですが、今まで僕が聞いていた説明の中でちょっと誤解している部分もあるかもしれないと危惧を持ったので、幾つかその関連で質問させていただきたいんですが、まず、NOTICE参加団体９５、実績としての９５。一定規模以上の団体というのは大きなところをカバーしているという意味で非常に安心できる数字だなと思うんですが、その一定規模というのは具体的に表現できるのかというのが１点。そうすると、国民としては、ああ、そうねとすごくよく分かる。一定規模と言われると、それ、何だというふうになっちゃうかなというのが１点。

それから、これは多分僕の誤解だったかと思うんですけど、１．２５億について、毎月、悉皆で一定のＩＤ・パスワードの組合せでチェックしているというふうに思っていたんですが、もしそれが間違っていたら、これぐらいの率でと。明示できないんだったらその旨を教えていただければいいんですけど、どのぐらいの比率でチェックしていますということ。

そして、今の御説明の中で、検知したものの中で４分の１注意喚起と言っておられたような気がするんですけど、僕は全数だと思ったんですけど、何で４分の１なのかよく分からないなと。そこのところを教えていただきたいなというところですかね。

あとは、横田先生も言っておられるように、本当は検知した中で。でも、今の御説明でいくと、多分注意喚起した中でどれだけ直っていますという指標を明示すると、ああ、効果があるんだなということはよく分かると思うんですけども、取りあえず質問のほうへのお答えをよろしくお願いいたします。

【説明者】　ありがとうございます。

一定以上のということなんですが、加入者としては大体５万加入以上の規模のISP事業者ということでございます。それから、チェックという意味では、対象としている１．２５億ぐらい、現状IPアドレスがあるんですが、これは毎月全数チェックをしているということでございます。加えて、その１．２５億をチェックした上で一定比率で脆弱性が見つかりますと。その中で、４分の１ぐらいなんですが、それを注意喚起しているということなんですが、要するに、脆弱性は重大と思われるものから軽微なものまでいろんなものがあると。それを延べ単で注意喚起をしてしまうと、受け取る側のことを考えると、この機器は危ないですよ、この機器は危ないですよと次々来るわけです。いわゆる狼少年みたいになって、何もやらな

いということが生じてしまうので、優先順位の高いものを一定程度抽出した上でとにかく対策をしてくださいというやり方の方が実効性が上がるという観点で、今、そういうやり方をしているということでございます。

それから、ISP事業者に対する注意喚起に対して、最終的にアクションが取られたかどうかと、まさに先ほどの御指摘なのかなと思いますけれども、そこはちょっと我々のほうでも、まさに御指摘をいただいた視点もあろうかと思いますし、ほかの切り口でも情報をどうやって出したらユーザーの方が現状を把握し、対策を取ろうと思うのかと、そういう研究も今しておりますので、御指摘をいただいた点を含めて、指標の設定の仕方については検討させていただきたいなというふうに考えてございます。

【鈴土先生】　ありがとうございます。

これは意見というか、希望ですけれども、４分の１を選ぶところの表現として、例えばレビューシートを作るときとかの表現として、言ってみれば、優先度の高いものと言っちゃうと結構裁量が出てきちゃうので、例えばこれ以上の重要度のあるものみたいな表現ができると、読む側からするとすごく安心できるなと思いますので、御検討いただければと思います。

【阿南会計課長】　よろしいですか。論点の④ですが、アンケートの信頼性、公表すべきじゃないかという点につきまして、これも鈴土先生、横田先生にお話しいただきましたが、いかがでしょうか。じゃあ、横田先生、お願いします。

【横田先生】　アンケートは、すみません、誰向けのアンケートでしたっけ。注意喚起した方にでしょうか。

【説明者】　最終的に、この施策自体が、そういう方々、一般的にセキュリティレベルが上がっているかというところを最終目標としているので、それを前提としたアンケートの取り方になっています。だから、無作為というかに抽出をして、一定程度抽出をした上で、その方がセキュリティに対するどういう意識を持っているのか。その意識の下で対策を取る、取らないみたいな話が出てくる。最後のアクションにつながるかどうかというところをアンケートとして取っているということです。

【横田先生】　ありがとうございます。

このアンケートは、これを公表することで、よりセキュリティ意識を高めていくための材料とすることもできると思うんですけれども、現状、この扱いをどのようにお考えで、今後どのようにされる予定か、お伺いできますか。

【説明者】　現状、このアンケートがどういうふうに行われていたかというのを対外的には出していないんですが、具体的にどういう形でやっていくか、どこまで出せるかは検討させていただきたいんですが、対象として、こういう方々に対してこういう形でアンケートを取った結果がこういうふうになっていますという要所要所のところは、まさに注意喚起とか周知啓発みたいな形でいろんな情報を出していく中で役立っていただけるようであれば、公表することはやぶさかではないというふうに思っております。方法、どこまでというのはあると思うので、その出し方については検討させていただきたいと思います。

【横田先生】　単なる感想ですけど、出せるところの範囲が限られているというのは、何のための、何のアンケートなのか、ちょっと分からないんですけど、できるだけ透明性を高めて、皆さん、情報が多ければ多いほど活用していただけるかと思いますので、幅広にお考えいただきたいと思います。

【阿南会計課長】　では、続きまして、無線LANセキュリティガイドラインのところで論点⑤ですけども、短期アウトカム、長期アウトカムの目標値及び達成率は適切かというところで、これは鈴土先生、お願いします。

【鈴土先生】　ありがとうございます。

元の資料、説明用の資料の最後のページをちょっと見ていただけるとありがたいなと思います。活動・成果目標のフローが出ているところですね。「３０３：短期アウトカム」ということで、セキュリティ対策に係るガイドラインの認知度の向上、あるいはその下で、セキュリティ対策への理解の向上というのがあるんですが、これを、レビューシートで実際どうなっているかというのを見てみると、例えば無線LANのセキュリティ対策に係るガイドラインを知っているという回答の割合をアンケートで取っていて、目標は、５０％が知っているよという回答をすること。実績はどうなるかというと、２０２２年度は４４％、２０２３年度は４２％、２０２４年度は４３％。だから、あんまり向上はしていない。基本的に向上はしていない。達成率は５０に対して４０幾つなので、８８、８４、８６となっているんですけど、率だけ取り上げると何か大変よろしいような状況に見えちゃう。でも、さっきのように、もともとの目標は認知度の向上なので、それを表現するような形での指標を考えていただけないかなと。もしそれが何か向上がしていなくて難しいんですというんだったら、そもそも事業として効果があるんですかみたいな話になっちゃうかと思うんですが、いかがなものでしょうか。

【説明者】　ありがとうございます。

まさに御指摘の点はあろうかと思っておりまして、現行の目標設定は年度一定程度のラインを維持するみたいな設定の仕方にしておるんですが、これはこの場合ですと無線LANの機器を対象としていて、その無線LANの機器の技術的な中身は結構変遷をしている関係で、セキュリティに対する捉え方というのも変わっているので、一定程度のラインを維持するというのが一つあるかなと思いつつ、事業を継続する中でそれを向上させないと、何のためにやっているのという、まさに御指摘のとおりだと思いますので、そこは設定の仕方を検討させていただいて、よりよい形の指標の設定というのを改善をさせていただければと思います。

【阿南会計課長】　論点の２つ目の①ですが、注意喚起の方法はプロバイダごとに任されているようですが、プロバイダ別の実施方法や改善状況について把握や検証をしているのかという点について、横田先生、お願いします。

【横田先生】　ありがとうございます。

そもそもなんですけど、注意喚起後の改善状況において、プロバイダごとに差異というのは結構改善結果にあったりするものなのかというのをぜひお伺いしたいのと、その結果、改善状況がよいプロバイダが何を行っているのかなどを把握していたらぜひ教えていただきたいと思います。

【説明者】　ありがとうございます。

プロバイダによって手法というか、インターネットサービスプロバイダなので、当然顧客に対してメールを流すというのは通常あり得る形なので、そういう形が通常のケースであることが多いということです。方法によって、どういう形で利用者が受け取って、それがアクションにつながっていくのかというのは、まさに御指摘をいただいたとおり、それぞれの事業者のやり方というのはいろいろありますし、把握の仕方というのもいろいろあるというのが正直現状でございます。そういった意味で、やり方とも連動はすると思うんですが、そのやり方に応じて、ユーザーの受け取りがどうなっていて、意識がどこまで高まるとか、その意識の高まりとともに最終的に改善が必要なセキュリティに対するアクションが取られるかどうかにどこまでつながるのかというのは、今まさに研究を行っているところで。要するに、やり方を変えることでより最終的なアクションの率が上がるのであれば、そういう形で促していき、事業者のやり方の改善を促していくということになろうかと思うんですが、実はそこのところはあまり明確には現状分かっていないところがあって、そこを今ちょっと。最後、ユーザーがアクションをどういう形で担保していただけるのかというのを今ち

ょっと精査して、そこの研究をしているというのはまさに途上なので、その研究の結果を踏まえて、より注意喚起自体が最終的なセキュリティに対するアクションにより効率的につながるような方法というのをこれからまさに確立をしていこうかなと、改善を図っていこうかなということをしています。

【横田先生】　ありがとうございます。

正直、今、何か詐欺メールもたくさんあったりとかして、どれが本当の注意喚起なのか否かというのも非常に分かりづらかったりとかするので、恐らく事業者さんもかなり工夫をなされているんじゃないかなというふうに思います。研究がどの場でなされているのか分かりませんけれども、ぜひ、事業者さん同士の共有はもちろんですし、アンケート等々もうまく公開して、早く改善につながるようにお努めいただければと思います。

【説明者】　役所から送るか、企業から送るかみたいな、主体によって捉え方が違うとかというのは、まさに今出てきているところでして、先生御指摘のとおり、そういった伝え方をどういう形でやると受け手側が信頼感を持って対策をしようとするかというところも結構機微な部分があるので、そこを含めて、まさに今、研究をしているというところでございます。

【阿南会計課長】　ありがとうございました。

では、次の論点②ですけども、プロバイダに加えて、機器の製造業者、システム開発業者、販売店との協力をどのように推進していくのかという点について西出先生、よろしいですか。

【西出座長】　これはまさしくプロバイダ以外の様々な関係業者の方々に対してアウトリーチすると、より効果が出るんじゃないのかということですよね。ここに書いてあるとおり、機器の製造、また、システム開発等々の各関連の方々にお話をいろいろ、注意喚起等々も含めてアウトリーチしていくといいますか、そういうことをしていくことが非常に効果があるのではなかろうかという趣旨で説明をさせてもらっている。ある意味、そういうのをやっていくとよろしいんじゃないのか。もっと強く言うと、やってくださいという話ですがね。そういう趣旨を込めてお話をさせていただいております。

【説明者】　ありがとうございます。

まさに御指摘のとおりかなと思っておりまして、我々は通信業界を所管しておりますので、ISPというところから始めていますと。その上で、まさにメーカーに対しても少し今アプローチを始めていますし、もっと言うと、製造の段階と、最後の、ユーザーがサービスを

受けるISPの段階ですね。その間に、流通の過程でいうと販売業者みたいなのがいて、幾つかのポイントがあるわけで、それぞれ対策を講じることでより重層的な対策になるというのはまさに御指摘のとおりで、その意味において、今、関係省庁と話をし始めているところで、所管するそういう業界に対する何か情報を提供するような機会などを通じて、こういったセキュリティ機器に対するセキュリティの対策の必要性であるとか、それに対する具体的なアクションを取ってくださいですとかということの、そういった違う情報提供の場を活用させていただくようなところからまず始めていこうということで、具体的な話を、今、始めているところですので、そういう形でプラスアルファの機会でこういった取組を紹介して実効性を上げていこうということは今まさに進めているところでございます。

【阿南会計課長】　ありがとうございます。

続きまして、無線LANセキュリティガイドラインについて、③の論点ですけど、他の政府機関との役割分担・連携はできているのかという点について、鈴土先生からお願いします。

【鈴土先生】　ありがとうございます。

もともと、ほかにもIPAさんとかがあるので、そちらとの連携はどうなっているんですかということで御質問申し上げたところなんですけど、それぞれの業務をやっておられるということかと思うんですが、特にガイドラインみたいなダウンロード資料についてはということで申し上げると、主としてIPAさんかもしれないんですけど、あちらのページも見たときに、資料がいっぱいあって、どういうときにどれを使えばいいのか、さっぱり分からないので。こちらにもガイドラインがあるわけですけれども、そちらとの関係性もよく分からないので、希望的な意見としては、何か政府ワンストップで、ここに行けば何でもある、最初はこれを見るんだ、こういうときにはこれを見るんだということが利用者にとって分かりやすい形で提示していただけると非常にありがたいなと。コメントと受け取っていただければ結構かと思います。

以上です。

【阿南会計課長】　ありがとうございました。

よろしいですか。答えはいいですか。

【説明者】　前回も御質問いただいて、それぞれ、経済産業省、IPAとか、我々総務省ですとか。我々は、いわゆるネットワークとしてのセキュリティが大事ですよと。経済産業省さんはIT機器であるとかの安全性みたいな意味で、入り口は違いますが、最終的には割と似通ったところに行くということで、まさに御指摘のとおり、一般の方からすると、同じよう

な資料が違うところにあるといった捉え方をされるようなケースというのは当然あり得るのかなと思っております。そういった意味で、今々の状況ですと、それぞれがつくったマテリアル、ガイドラインみたいな資料というのは、事前に関係者で共有をしながら、相互チェックをしながら、どういう形でどっちが情報を出していくのかというところはやっているんですが、それは最終的に利用者の方に対して出していく段階ですと、捉え方は当然利用者視点で捉えていくわけですので、ちょっとそこはどこまで整理ができるか分からないんですが、関係者がそれぞれつくっているものをどういう形で共有して、どういうふうに整理をしてというところは検討させていただけたらと思います。

【阿南会計課長】　ありがとうございます。

最後の論点３ですけども、契約において、一者応札が多く見受けられるが、改善の余地はないかということです。これはアトキンソン先生、よろしいですか。

【アトキンソン先生】　いろいろ落札情報を見てみますと、単純平均で９８．５％の落札率が平均になっていまして、１００、９９．１ですとか、一番低いものは９１．７なんですけど、ちょっと異常に高いという感じはしますけども、これは何か改善の余地があるような印象を受けますけども、いかがでしょうか。

【説明者】　ありがとうございます。

一般論として、一者入札ですと、なかなか競争によって値段が下がりにくいという御指摘をまさに受ける状況かと思います。そういった意味において、この事業全体の中で特にIoTの関係、NOTICEの事業の関係ですと、中心的な事業になりまして、その中に幾つかの要素、例えば一般的な周知啓発みたいな、いわゆる広報事業みたいなものですとか、プロジェクト全体のマネジメントの事業ですとか、あとは注意喚起を行う事業ですとか、幾つかのパーツに分けることができると。その意味において、より競争を促していくという観点においては、複数社が公表した指標に基づいて競争して値段を下げるというインセンティブが働くほうがいいということでございますので、今々進めておりますのは、例えばNOTICEの事業でしたら各パーツ、広報とか、あとはプロジェクトマネジメントみたいなものというのはコンサルティング会社ですとか、あと、広報関係の会社というのは複数あって、割と裾野が広いと。そういうところはきちんと切り出した上で、それに対して入札を行うことでより適正な競争が働いていくというふうに考えておりますので、現にその一部は今そういう形で移行していて、まさに競争を行う中で実際の落札額がなるべく下がるような形での入札の形式というのを今、模索をしていて、具体的に進められるところはそういう形で進めておりますの

で、引き続き、事業の性格にもよると思うんですが、なるべくそういう形でできるものについてはよりそういう方向で進めていきたいと考えてございます。

【アトキンソン先生】　ほかのものに関してはちょっとコメントしないんですけど、６０％云々だとか何をもってそういう目標を設定しているのか。というのは、ほかの事業とみんな一緒なんですけど、あんまり落札率が下がると品質がどんどんどんどん下がっちゃいますので、あまりにも下げ過ぎるのはよくないんですけど、大体いいところとして９５％ぐらいがいい落札ラインなのかなという気がしないでもないんですけど、今は数ポイントぐらい上回っていて、そのバランスを取るような形はちょっとだけ改善の余地があるのかなと、私の感触です。

以上、コメントだけです。

【阿南会計課長】　ほかの方、よろしいでしょうか。

コメントシートが出そろいましたので、瀧川先生から事前にお預かりしているものも含めまして、提出していただいたコメントシートやこれまでの議論を踏まえまして、西出先生に取りまとめのコメント案の作成をお願いいたします。よろしくお願いします。

（コメントシート取りまとめ）

【阿南会計課長】　それでは、取りまとめ役の西出先生から、取りまとめコメント案の発表をお願いします。

【西出座長】　それでは、各委員の皆様におかれましてはありがとうございます。たくさんのコメントを頂戴しました。

それでは、まとめて御報告をさせていただきます。このようなIT機器の急増、多様化、このような状況下で、サイバー攻撃の問題は非常に増大しています。セキュリティの対策って非常に重要な事業じゃないかと位置づけられていると思います。その中で、さらにこの効果を踏まえることを考えた上で、やはり指標というものを含めて、いろいろと改善を検討していくところはあるのではなかろうかというような形でコメントをさせていただくことになります。

まずは指標の問題ですね。指標の問題のことを少しお話しします。まずは適切な成果指標というところに皆さん関心がございまして、例えば、代表的な機器における結果推移の公表等々いろいろあろうかと思うんですが、より具体的な成果が見える成果指標というものの検討をお願いしたいというものが１つ。それから、議論にも出ていました、様々な観測指標があったと思いますけども、ああいうのもしっかりとアウトカム、もしくは参考指標という

形で積極的にレビューシートの中でも表示をしていくことが大切じゃないかということでございます。

それから、指標としては、これは③に当たるんですよね。IPアドレス数の目標である１．２５億件の妥当性という話で出ている中で、やはり参加団体９０というところが分かりにくいというところからの話だったと思うんですけども、このIPアドレス１．２５億件という数字、これが全体に対するカバー率として妥当であるという情報を積極的にレビューシートの中で明示しておくほうがいいだろうという趣旨のコメントを頂戴しております。

あと、さらに、成果指標の評価に使用しているアンケート調査についてお話があったと思うんですけども、全体的に申し上げられるのは、多分この調査結果の信頼性というものをより読み手といいますか、国民に明示する必要があるというところがあろうかと思うんです。信頼性の確保だと思うんですけど、そういう意味で、調査の方法及び結果等々も積極的に開示していく、公表していくことが大事じゃないかというようなコメントを頂戴しております。

次です。次は無線LANのセキュリティガイドラインのことに関しましてコメントを頂戴しております。これもまとめてお話しさせてもらえれば、ガイドラインにおける短期アウトカムや中期アウトカムの問題ですね。ここについてのしっかりとした目標値や達成率等々、アウトカムとして、我々といいますか、読み手が分かるような指標をしっかりと検討して設定していくことが大事ではなかろうかということでございます。

続きまして、次のほうに移りますが、次はIT機器の注意喚起の方法等についてと申し上げたらいいのかなと思うんですけども、いろいろとプロバイダ別に様々な注意喚起を行っているという話でございますけども、プロバイダ別の実施方法や改善の状況、そのようなものをしっかり確認して注意喚起に生かしてほしいというようなコメント。それから、プロバイダのみならず、機器の製造業者やシステム開発業者、販売店等々の話があったかと思うんですけども、そのような他の業者におかれても、既にコメントとして頂戴していますけども、もう既に動かれているということなので、この連携協力をより進めていっていただきたいということでございます。

そして、これがセキュリティガイドラインですね。今から申し上げるのがセキュリティガイドラインとして申し上げたいことですけども、リテラシーの向上という意味でのガイドラインの策定という話になりますが、サイバーセキュリティ対策に取り組む他の政府機関等々も含めて連携協力を推進することや、このようなガイドラインの使い方ということが、

アクセシビリティと言ったらいいんですか、ユーザビリティと言ったらいいんですか、ユーザーのためのワンストップサービスというところを検討していく必要があるのではなかろうかと。より使いやすく、より注意喚起が届きやすくするという趣旨でのコメントとして頂戴していると私は認識しておりますが、それも検討してもらいたいということでございます。

最後でございます。最後は一者入札の件でございます。一者入札が多いということを踏まえての議論でございますが、単純平均落札率が９８．５％と、こういうような数字を踏まえて、契約において、より改善、原因分析等々を取り組んでいっていただきたいということでございます。

以上、コメントです。

【阿南会計課長】　ありがとうございました。ただいまのコメント案について御意見はありますでしょうか。よろしいですか。

では、特段御異論ないようなので、御提示いただいた取りまとめコメントのとおりとしたいと思います。後ほど書き起こしたものを共有させていただきます。活発な御議論、ありがとうございました。

では、先生方からの御指摘を踏まえ、担当部局から一言お願いします。

【説明者】　御指摘ありがとうございます。

１点目、色々議論をいただいた指標に関してでございます。これは事業レビューの中での指標の設定の仕方、あるいはそれに加えての参考指標とか、それ以外の形でデータの公表の在り方ですとか、それらトータルとして、どういう形で情報を提供し、あるいはその政策効果を測るかどうかといったところですね。全体像としてどういう形で見せるかということなのかなというふうに理解をしました。御指摘を踏まえて、まさに持ち得る観測のデータですとか、幾つか客観的に指標として使えるようなものがありますので、これをどういう形で公表するか、あるいは指標として設定するか、トータル検討させていただいて、改善を図っていきたいと思います。

それから、２点目はいわゆる連携の話でございます。施策を進める上で、より効率的に、あるいは実効性が上がるようにということで、他省庁ですとか他業界ですとかというところとの連携という意味では、一部御説明の中で進めておるところはあるというふうに御説明さしあげましたけれども、こういったところを今以上に進める形で、施策の実効性が上がるようにという形で取り組んでまいりたいと思います。

３点目は入札の関係でございますけれども、これも一部始めておりますが、まさに競争を適正に行う中で、適正な落札額の下でよりコストパフォーマンスのいい形で事業が進められるようにということで、引き続き入札に関しても努力を進めてまいりたいと思います。

引き続き御指導いただきますと非常にありがたいなと思っております。本日はありがとうございました。

【阿南会計課長】　ありがとうございます。

本日予定しておりました議論は全て終了しました。

最後に、総務省行政事業レビュー推進チーム副統括責任者の官房政策立案総括審議官、北川より御挨拶を申し上げます。

【北川官房政策立案総括審議官】　北川です。

本日はお忙しい中、長時間にわたりまして大変精力的に御議論いただきまして、誠にありがとうございました。また、西出先生にはコメントの取りまとめをいただきまして、誠にありがとうございました。

本日の議論の中で、事業の目的に照らした適切な成果指標の設定や事業の実施方法の見直しや入札の改善など、大変多くの貴重な御指摘、御示唆を頂戴いたしましたので、頂きました御指摘等を踏まえまして、より一層事業の質を上げてまいりたいと思います。総務省では、これまでのレビュー等を通じまして、ＥＢＰＭに対する省内の理解の浸透を図ってきているところでございますが、まだまだ、本日の御議論も踏まえ、さらなる検証が必要な点はあるなと感じたところでございます。先生方におかれましては今後とも引き続き御指導のほどよろしくお願いいたしたいと思います。

本日は誠にありがとうございました。

【阿南会計課長】　これをもちまして本日の予定は全て終了しました。長時間にわたり御議論ありがとうございました。

本日の議事の模様及び取りまとめコメントにつきましては、準備が出来次第、総務省のホームページに掲載させていただきます。

今後とも総務省の行政事業レビューの取組につきまして、御指導のほどよろしくお願いいたします。本日はありがとうございました。