2024 年 5 月

シリーズ 「日本のサイバーセキュリティ政策史」第 7 回（連載全2回）

すべての人が「自分ごと」として向き合える行動計画を【前編】

～現場の声をすくい上げ、実効性を高める～

サイバーセキュリティ政策分野に詳しい三角育生氏が日本の同政策史をひもとくシリーズ。第 7 回は、2011 年から 2022 年の間にのべ 9 年間 NISC に在任された山内智生氏をお迎えし、政策立案・実施の現場の取組を明かしていただきます。3 つの重要インフラ行動計画、サイバーセキュリティ基本法の改正、そしてサイバーセキュリティ戦略のとりまとめなどを主導する中、日本の経済社会のサイバーセキュリティ課題をどうとらえ、解決を図ったか。東京オリンピック・パラリンピック競技大会を平和に終えられた陰でいかなる対策が講じられていたのか、そのレガシーとは何か。前編では第 3 次行動計画策定の背景や意図、意義をうかがいます。

【出席者】

山内 智生 氏
総務省 サイバーセキュリティ統括官（最高情報セキュリティ責任者）、
元内閣官房内閣審議官（内閣サイバーセキュリティセンター）

聞き手：
三角 育生 氏
東海大学情報通信学部長・教授

第 2 次行動計画改定――事業継続を主眼に

三角 山内さんが内閣サイバーセキュリティセンター（NISC）に在任されたのは、2011 年 8 月から 2014 年 7 月まで、および 2016 年 6 月から 2022 年 5 月までですね。その間、3 つの重要インフラ行動計画、サイバーセキュリティ基本法の改正、2020 年東京オリンピック・パラリンピック競技大会（以下、「TOKYO2020」という）における対応およびその準備のためのサイバーセキュリティ対策、そして 2021 年 9 月に閣議決定されたサイバーセキュリティ戦略のとりまとめなどを主導されました。本日は、そうした施策策定の背景や意図、意義をお聞かせいただければと思います。

まず、「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」（2014 年 5 月 19 日、情報セキュリティ政策会議。以下、「第 3 次行動計画」という）についてです。その前の「重要インフラの情報セキュリティ対策に係る第 2 次行動計画」（2009 年、以下、「第 2 次行動計画」という）改定の

主眼は何だったのでしょうか。

山内　第 2 次行動計画をいつ見直すかということは文書に書かれていませんでした。私が NISC に着任したのは、東日本大震災（2011 年 3 月 11 日）の 5 カ月後。ようやく灰神楽が収まりかけている時期で、東日本大震災を踏まえた事業継続についての気づきをとりまとめることがまず目前にありました。それで事業継続計画（BCP）の策定に頭を悩ませている最中に、わが国の重工企業へのサイバー攻撃事案（2011 年 9 月）、さらに衆議院・参議院両院へのサイバー攻撃事案（2011 年 10 月報道および同年 11 月発表）が発生しました。当時、重要インフラ事業者の方々の意識の中では、サイバー攻撃を受けた当事者の方々は大変だろうとは思っても、その他の者においては「自分ごと」としては考えられていなかったのではないかと思います。

三角　情報系への攻撃であって制御系ではないといった意識からでしょうか。

山内　それもありますし、同じ情報システムでも、自分たちに影響するものであるという実感はあまりお持ちではなかったのではないかと思います。

したがって、第 2 次行動計画改定の主眼とは何かを端的にいうと、BCP でした。つまり、データを複製して物理的に別の場所に保管しておく、バックアップを置いておくということ。当時、バックアップの議論こそありましたが、東京と大阪の双方に置いておけばいいだろう、というような認識でした。それは間違ってはいません。しかし、東日本大震災の震源域は 1,000 キロメートル以上にわたります。ということは、東京・大阪間の 400～500 キロメートルの距離だと両方被災をする可能性がゼロではありません。そういうことが当時わかったので、バックアップが同じリスク要因によって倒れることがないようにすべきということを訴求したいと考えました。

もう一つは、東日本大震災で通信施設も被災をしたので、システムだけではなくて、ネットワークの多重化についてもあらためて考えてほしいと考えました。

加えて、石油製品の輸送が途絶すると、通信基地局などの機能も止まってしまいます。東日本大震災の際、太平洋側の石油製品の輸送ができなくなり通信基地局が 1 日半、つまり 36 時間機能がストップする事態に陥りました。石油製品の供給確保は、東日本大震災から現在に続く課題です。

三角　2024 年 1 月の能登半島地震でも通信基地局のバッテリーが切れて通信が途絶するといった同様のことが起こりましたね。

第 3 次行動計画の根底にあるもの――見るべきはサービス障害

山内　おっしゃるとおりです。それで 72 時間は持たせる必要がある、という話になりました。第 3 次行動計画を策定するときの根底には、われわれはシステム障害を防ぎたいのか、それともシステム障害を大きな要因とするサービス障害を防ぎたいのかということをしっかりと議論すべきということでした。

三角　第 1 次行動計画では、山口英先生（当時、内閣官房情報セキュリティ対策推進室情報セキュリティ補佐官、故人）はサービスを守ることだとおっしゃいました。

山内　そのとおりです。それが多分、どこかで変質していたのです。私が NISC に着任した直後、

当時は第 2 次行動計画に基づく政策が推進されていた時期でしたが、闘病に向かわれる山口補佐官が「俺はいなくなるけれど、お前、頑張れよ」と言われたときに、「重要インフラが重要インフラたるゆえんは、行っているサービス、提供している業務が重要だからである。システムを守るだけなら、その人たちは重要インフラ事業者ではないだろう」とおっしゃいました。そのとおりです。そして、分野によってシステムのサービスにおける位置づけはまったく異なります。例えば、金融や通信業界は、システムはきわめて重要です。それがダウンするリスクを想定してビジネスが組まれています。


山内氏

しかし、金融業界もすべて同じではありません。銀行・証券会社と、生命保険会社・損害保険会社は同じ金融業界でもまったく別の考え方をします。保険会社の方々は「システムがダウンしても、不便になるかもしれないけれど、ビジネスが止まるものではない」と明確に言われていました。

三角　当時はそのような感じだったわけですね。

山内　また、各業界において、システムを担当する部局を見るとスタンスがわかりやすかったものです。例えば当時、水道協会の担当部署は、いわばさまざまな業務を処理する部局である総務部総務課でした。担当の方は「システムが止まったとしても、水の供給を維持する方法はある」と言われていました。それは当時でいうとおそらく間違ってはいません。こうした考え方の違う方々に、共通してリスクとして何を見るのかというというとき、「あなた方の業務を止めてはならないですよね」という点は共通して同意を得られたわけです。こうした共通認識を改めて入れようとしたところが、第 3 次行動計画の出発点だったということではないかと思っています。

経営層へのメッセージ

三角　経営層という言葉が明確に書かれているのは第 3 次行動計画が初めてです。

山内　そうです。一方、経営という言葉は最初の行動計画（「重要インフラの情報セキュリティ対策に係る行動計画」2005 年 12 月 13 日、情報セキュリティ政策会議決定。以下、「第 1 次行動計画」という）から使っています。

三角　第 1 次行動計画から使われてはいますが、第 3 次行動計画ではかなり強調して書かれていますね。

山内　はい。第 1 次行動計画では「経営の問題でもある」という言い方をしていました。第 3 次行動計画で、経営層の方々に向けて「自分の問題として認識すべき」という言い方に変えたのは、われわれ NISC にいる人間もそう思っていた部分はあるのですが、どちらかというと、業界団体の方々からのご要望が大きかったことによります。すなわち、「行動計画などがつくられても、経営層に響いていない。ヒト、モノ、カネを持つ経営層に対して、自らの仕事であって、自分たちが関与して決めて、持続的に取り組まないといけないということがわかる文書にしていただきたい」ということを言われました。第 3 次行動計画の 10、11 頁に表裏で絵と文書を入れたのはそういう理由です。

三角　それが従来と明確に変わった理由なのですね。

山内　とにかく1枚ビリッと破いて、「これはあなた方に向けてのメッセージです」と経営層の方々に渡していただける形にしています。そこが第 3 次行動計画の大きなポイントです。逆に言うと、それを念頭にいろいろ組み替えをしているのが第 3 次行動計画です。

5 つの柱

三角　第 3 次行動計画で示されている計画期間内に取り組む情報セキュリティ対策についてうかがいます。まず、第 2 次行動計画から対策の 5 本の柱が変わっているのはどのような意図でしょうか（図を参照）。

山内　変えたポイントがいくつかあります。第 3 次行動計画の 5 本の柱は「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント」、そして「防護基盤の強化」です。第 2 次行動計画の柱を見ると、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「共通脅威分析」、「分野横断的演習」、「環境変化への対応」となっています。

三角　「分野横断的演習」が第 3 次行動計画で抜けているのはなぜですか。

山内　私が NISC に着任して早々、皆さんの議論を見ている中で、なぜ NISC の施策が第 2 次行動計画の 5 本の柱の中に入っているのか、という話がありました。

三角　それはどういうことですか。

山内　分野横断的演習は NISC が行っている施策の名前です。本来的な目的は、分野横断的演習をやることそのものではなく、分野横断的演習を通じて達成するべきものです。そうであれば、私としては、なぜ NISC の施策名を柱の一つとして位置づけているのかという疑問を持ちました。内部での議論をした上で、事業者の方々に聞いてみたところ、皆さんも同様のご意見だったこともあり、議論し直しました。そうした中で、障害にどう対応するかということに対して、検証手段として分野横断的演習があるだろう、という結論でした。

三角　障害対応体制であれば、別段、分野横断だけではありませんね。

山内　そのとおりです。分野横断的演習といったときに、おそらく明示的に読めないのが、自分たち事業者で行っている訓練や演習です。こうした分野横断的演習以外のところで行っている訓練や演習は当然、役に立つはずですし、それらのマネジメントをどうするかという話もあるはずです。そこで、さまざまな準備を行うことも含めた体制を整え、その体制が実動するものであるかどうかを確かめましょう、ということが、この行動計画における目標であることを明示することにしたわけです。具体的に実施することが大きく変わるわけではないかもしれませんが、柱を書き換えました。

三角　見直しの背景、趣旨がよくわかりました。

行動計画の柱の変遷

1次行動計画	2次行動計画	3次行動計画	4次行動計画	現行行動計画
1. 安全基準等	1. 安全基準等の整備・浸透	1. 安全基準等の整備・浸透	1. 安全基準等の整備・浸透	1. 障害対応体制の強化
2. 情報共有体制の強化	2. 情報共有体制の強化	2. 情報共有体制の強化	2. 情報共有体制の強化	2. 安全基準等の整備・浸透
3. 相互依存性解析	3. 共通脅威分析	3. 障害対応体制の強化	3. 障害対応体制の強化	3. 情報共有体制の強化
4. 分野横断的演習	4. 分野横断的演習	4. リスクマネジメント	4. リスクマネジメント、対処体制の整備	4. リスクマネジメントの活用
	5. 環境変化への対応	5. 防護基盤の強化	5. 防護基盤の強化	5. 防護基盤の強化

自然に受け入れられる順に

山内　そこで、さきほどお話ししたとおり、分野によって違うところがあるので、第 4 の柱で改めて「リスクマネジメント」の話を書いています。問題意識として、情報セキュリティマネジメントを考える上でのリスクを考えるときに、国際標準化機構（ISO）の規格 ISO/IEC27001（情報マネジメントシステム規格）でよいのかということがありました。今は少し変わっていますが、当時の ISO/IEC27001 はほぼ情報セキュリティに係る事項に限られていました。さきほど申したように、第 2 次行動計画のときにわれわれはリアルの障害を経験しています。リスクを考えるときにはそれも念頭に入れねばなりません。そうすると、まず ISO31000（リスクマネジメント規格）に基づき、われわれがサービスを継続するときに障害になりうるものとはなんぞや、ということを定義した上で、ISO/IEC27001 を引っ張っていくということを考えなければなりません。サービスの持続的な提供に対する不確かさ、という点を内部で議論して、こうした問題意識を投げかけていたところ、さまざまなリスクマネジメントのご専門の方々が知恵を貸してくださいました。ただし、議論が発散したときもあり、また、どちらにしても ISO の規格を用いるということなので、その点を問題視される方もいらっしゃいました。

三角　リスクマネジメントにはさまざまな方法論がありますね。

山内　一部の分野では、「自分たちは ISO の規格がつくられる前からリスクマネジメントをやっている。後発の規格に従うわけにはいかない」というようなご意見を述べる方もいらっしゃいました。実は第 3 次行動計画の最初のドラフトには ISO について書いていたのですが、これではまとまらないと考え、最終的には本文には ISO の規格に基づくものはほとんど入っておりません。

三角　今では、ISO31000 について多くの方が納得して用いていらっしゃると思いますが、当時は違ったということですね。

山内　今は、サイバーリスクもリスクの一つであり、全体のガバナンスの中で対応すべきものという考え方は、多くの方において共通認識があると思います。ISO31000 に基づくリスクマネジメントを実施するかどうかは別にしても、リスクマネジメントが必要だということについては、ほぼ疑いのない共通認識になっています。

三角　どのようなフレームワークにおいても、ISO31000 に記載されていることと同様のことは実質的にやっていますからね。

山内　おっしゃるとおりです。しかし、当時は、そこまでの認識があるように思えませんでした。ISO31000 とは何かということが周知されていない中で、ISO31000 という言葉が突然出てきたら、拒否反応は生じるでしょう。こうした考えから、一般的な概念である「リスクマネジメント」という言葉を使っています。

三角氏

一方で、「まずリスク分析をしないと、何に対応するかが決まらないでしょう」というご意見もありました。ごもっともなご意見なのですが、そもそもリスクとは何かということを十分に理解されていない方々がいらっしゃる中で、「まずリスク分析から始めましょう」といきなり言っても、リスクマネジメントは進みません。

そこで、第 2 次行動計画までで実行してきたことを念頭に、「これ

までやってきた対策をそのまま続けることで良いのかどうかについて検証する必要がありますよね。そのためにも、リスクマネジメントが必要ですよね」という言い方をしています。そうすると、今まで実施したことを否定されているのではないかといったことからの拒否感を示す方々においても、たしかにそれは必要、という話になります。それゆえ、あえてリスクマネジメントは第 4 の柱になっています。実は、第 4 次行動計画の最初のドラフトではリスクマネジメントを第 1 の柱にしました。しかし、内部で議論している中で、今お話ししたような理由から、第1の柱にはしないことにしようとなりました。

対策の柱は、自分たちができること、すなわち今までもやってきて、割と自然と受け入れられるものの順番に並んでいます。柱の第 1 から第 3 まではそれまでもあったわけです。第 3 の柱は、分野横断的演習から変わったとはいえ、中身は今までやってきたものの延長線上にあります。これらを支えるという観点で、リスクマネジメントをしっかりやろうという言い方になっています。

三角　リスクマネジメントが第 1 の柱にあるほうが自然であるように思えていましたが、事情を理解しました。

山内　ただし、第 3 次行動計画で示して、少なくとも 3 年間なり施策を実施しているうちに、リスクマネジメントの必要性自体はきっと共通に皆に理解されるだろう。そのときに、改めて柱としての位置づけをどこにするかを考えればよいと考えておりました。

「まずはその気になってもらわないと話にならない」

三角　第 5 の柱「防護基盤の強化」は、柱の第1から第 4 を支えるものとしてあるということですね。

山内　そうです。具体的には、まず「広報公聴活動」。第 2 の柱で「情報共有体制の強化」を挙げていますが、ここでは特に、自分たちがどういう情報発信をするか、逆に外で何をやっているかを知るということです。

また、「国際連携」についてですが、民間の活動において、例えば ISAC（Information Sharing and Analysis Center）の連携などがあります。そういうものについても、ぜひ意識を持っていただこうということが背景にあります。

さらに、「規格・標準及び参照すべき規定類の整備」について。結局のところ、例えば、分野横断的演習を一つやるにしても、突然「今からやります」と言ってなんとかなる問題ではありません。自分たちが何の規範に基づいて動くことになっているのか、それをやった後に得た気づきをどうやって反映していくのかという議論をするときに、何らかのドキュメント、リファレンスが必要になるわけです。そういうものをつくって、必要に応じて見直す、というサイクルも回す必要があるだろうと考えました。こうしたことをどこかに書く必要があるという話になり、柱の第 1、第 2、第 3 などにつながる部分もありますが、それを包括したものとして第 5 の柱の第 3 項に書いています。

今、申したような構造で、まずはそれまで自然発生的に行っていたものを、しっかりと体系立てて、目標に向かって進むためのツールがこれである、という表現にしたいというのが、第 3 次行動計画策定時の背景にあったテーマです。そういう意味で、柱の第 4 と第 5 は、私の目から見ると、大きく変えたというようには見えません。目標を実現するためのツールとして何があって、それをどうつ

くるのかという観点でまとめ直しているということではないかという風に思っています。

三角　その点は大切ですが、今まで明示的ではなかったですね。

山内　ええ。私が着任した当時、実はまだ私の席の後ろに第 1 次行動計画を策定する際の議論の資料が残っていました。CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response）をどうやってつくるか、山口補佐官に指摘されたことをどこまで入れるか、誰をどうお誘いをして何をしてもらうのか、といった議論の中で、ある意味、色濃く出ていたのが、まずはその気になってもらわないと進まないということです。当時の NISC の目標は、重要インフラ事業者の皆様が腑に落ちて取り組んでもらえるものを行動計画としてまとめることにあったようです。それらが情報セキュリティ確保に係る安全基準等の整備であり、また、自らの対策が大切であることに加えて、危機が発生したときには助け合うということ、すなわち情報共有体制の強化であり、分野横断的演習でした。第 1 次行動計画策定検討当時には、演習・訓練に体系立ったものがありませんでした。そういう意味で、分野横断的演習は、さきほど第 3 次行動計画の話題においては柱から外したと申しましたが、当時のスターターとしては重要であったわけです。

三角　本対談シリーズの第 6 回でお話をうかがった立石譲二さん（元内閣官房副長官補［安全保障・危機管理］付内閣参事官　内閣官房情報セキュリティセンター［NISC］重要インフラ防護担当）は分野横断的演習を実施する前に在任し、海外の状況も踏まえてそうした演習が必要だということを提唱されました。演習が実際に実施される前に離任されたのですが、演習はどのような意義があったでしょうか。

山内　自分たちが何か起きたと思ったときにどう対応するかという頭の体操をしなければいけないわけです。その習慣づけの施策という意味では、大きな意義があったと思います。その意義をさらに拡張して、自らの取組としていただくために位置づけを見直したものが第 3 次行動計画であったわけです。

重要インフラ分野拡大の意図

三角　第 3 次行動計画で重要インフラ分野が拡大しました。従来の情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）、医療、水道、物流の 10 分野に、新たに化学、クレジット、石油が加わり計 13 分野になりました。その背景や意図についておうかがいできますか。

山内　もっともわかりやすかったのは石油です。現実の世界で相互依存性の検討をすると必ず重要な業にあたります。しかし、なぜ石油関連事業者は重要インフラ事業者ではないのか。そういう視点で考えると、石油は、いわゆるサイバーセキュリティにおける重要インフラではありません。

実は、最初にお話ししたように、2011 年

に NISC に着任して BCP の議論をしているとき、等しく重要インフラ事業者の方々が懸念を抱いていたことがありました。石油です。当時から首都直下地震、あるいは東南海・南海地震がいつ発生してもおかしくないという話があったわけです。であるがゆえに、優先供給契約を皆が結びました。そうなると、ほんとうに自社に優先的に供給されるのか、大丈夫なのかと心配する人からのご相談が多く寄せられました。

そこでの気づきは、卸や元売りの事業者と個別に直接、供給契約を結ぶのかどうかということでした。コーディネートできないなら、何らかの形で、業界間のつながりをつくらなければなりません。災害対応としてだけでなく、システムとしての問題としても、それが止まったときに油がないと動きません。TOKYO2020 に向けた準備の際も同様の課題がありました。また、2024 年1月の能登半島地震においても同様ですね。こうした業界間のつながりの重要性を考え、第 3 次行動計画検討の際に、石油業界にも重要インフラ分野としてお入りいただく必要があるというものでした。

三角　化学についてはいかがですか。

山内　化学はプラント系で気になっていました。実は、無機化学の事業者も石油化学の事業者と同様に気になっていました。しかし、実際に重要インフラ事業者として指定したのは、石油化学のみでした。

三角　それはどういうことでしょう。

山内　2 つ課題がありました。一つは、無機化学のプラント系を包含する業界団体がないこと。もう一つは、無機化学関連の団体としてはないこともないのですが、その団体は、プラスチック製品を扱う小売までが含まれていることでした。

三角　そうすると重要インフラとはいえませんね。

山内　はい。そこで、経済産業省とも協議を行い、石油化学を対象としました。石油化学工業会がいらっしゃるのですが、石油と同様に、ケミカルとしてのプラントを抱える事業者の団体です。

三角　外から見ると、石油を原材料とするプロセスとして石油産業と石油化学産業は上流と下流といえますよね。下流が滞れば上流も滞ってしまうから、全体を保証するために石油化学を入れたともいえますね。

山内　それは結果論です。

三角　クレジットはいかがですか。

山内　クレジットはまったく違うところに着目をしていました。当時から、資金流通量的に莫大だったのです。当時、クレジット決済額は約 50 兆円に上っていました。それだけの金額を扱っている業界が重要インフラ事業者として入っていないのはおかしいということです。この件で日本クレジットカード協会にお声をかけたとき、初めて政府に認めてもらい感謝する、と言われました。確かに当時、政府の政策文書に、クレジット業界とは何かということを明確に示したものは見当たりませんでした。

構造的には、アクアイワラー、つまり加盟店契約会社の話をするのか、それとも、イシュア、つまりクレジットカード発行会社の話をするのかというところがあるのですが、そこは今後の議論として、クレジット分野を重要インフラとしたわけです。

第 3 次行動計画の意義──障害対応体制の構築

三角　結局、イシュアだけが入りましたね。

山内　はい。最近の事例と対比すると、金融が重要インフラだといえば、皆さん同意されるでしょう。その中に全国銀行データ通信システム（全銀システム）と日銀ネットが重要インフラ事業者に入っているのかというと、実は日銀ネットは入っていないのです。

三角　日銀は情報セキュリティ対策推進会議オブザーバーであり、政府関係でカバーされるからですね。

山内　そういうことになります。ただ、全銀システムは直接的には入っていません。全国銀行協会（全銀協）のものだからです。全銀協は重要インフラのオブザーバーです。いわゆる重要インフラ事業者視点から見たら、CEPTOAR には全銀協は代表としては入っています。ただ、全銀協という事業者が全銀システムを運営している組織として見えているのかと質問されたら、そうはなっていません。

三角　システム自体は対象になっていないのですね。

山内　明示的には入っていません。ただし、システムがダウンしたらすぐに連絡が来ますし、どうなっているのか、とはなります。しかし、一つひとつの銀行のシステムがダウンしたときと同じような情報連携体制とはなっていません。

実は、クレジット業界でも同じ議論がありました。事業者間決済を行っているアクワイアラーは入っておらず、イシュアの方々に入っていただきました。CEPTOAR に日本クレジットカード協会の方々が入っているので、実質的には、そのシステムに何か生じたら当然わかる仕組みになっています。責任関係が明確にわかる組織を入れて、そのシステム全体が何らかの障害が生じたときに実質的にわかる構造を担保するというのが当時の整理です。

われわれが到達したいと考えていたレベルまで実現できることが整理できたので、以上の石油、化学およびクレジットの 3 業種に入っていただきました。

三角　第 3 次行動計画の意義をどうとらえていらっしゃいますか。

山内　今申したとおり、その目標からさかのぼってどういうことをやるかということについて、体系立てることができたということが大きいのではないかと思っています。

三角　今、電子決済等がこれだけ普及しているので、クレジットは重要インフラ分野に入ってないと世の中の経済は回りません。その意味では、この時期に重要インフラ事業者となっていただいた意義は大きかったと思います。

山内　第3次行動計画策定後、障害対応体制の意義はますます大きくなっています。経済社会のサイバー空間への依存関係がどんどん高まってきました。システムがダウンしたときの影響は、策定当時から比べてもどんどん大きくなっていきます。したがって、ダウンしたときにどうするのかというマネジメントの確立は不可欠です。リスクの大きさを考えると、障害対応体制をしっかり構築する必要があるわけです。そして、今日、障害対応体制の確立・運用が最重要事項となってきていると思っています。

（後編につづく）

（2024 年 2 月 2 日収録。取材・構成:一般社団法人　日本サイバーセキュリティ・イノベーション委員会[JCIC]）

【出席者略歴】

山内 智生（やまうち ともお）氏

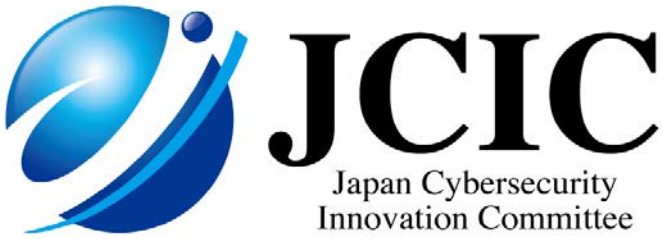
総務省 サイバーセキュリティ統括官（最高情報セキュリティ責任者）、元内閣官房内閣審議官（内閣サイバーセキュリテイセンター）

1989 年京都大学大学院工学研究科修了、郵政省（現総務省）入省。情報通信国際戦略局技術政策課研究推進室長などを経て、2011 年 8 月内閣官房情報セキュリティセンター参事官（重要インフラ担当）。2014 年 7 月総務省情報通信国際戦略局宇宙通信政策課長を経て、2016 年 6 月内閣官房内閣参事官（内閣サイバーセキュリティセンター、基本戦略担当）、2018 年 8 月同審議官（内閣サイバーセキュリティセンター） 内閣サイバーセキュリティセンター副センター長・内閣官房国家安全保障局・内閣官房副長官補付[事態]、2021 年 10 月総務省大臣官房審議官（国際技術、サイバーセキュリティ担当）・内閣官房内閣審議官（内閣サイバーセキュリティセンター）などを歴任し、2022 年 6 月より現職。

三角 育生（みすみ いくお）氏

東海大学情報通信学部長・教授

1987 年通商産業省(現経済産業省)入省。内閣サイバーセキュリティセンター(副センター長等)や経済産業省(サイバーセキュリティ・情報化審議官等)等において、サイバーセキュリティ、安全保障貿易管理といった行政に長く携わり、サイバーセキュリティ戦略の策定、サイバーセキュリティ基本法制定・改正、日本年金機構のインシデント対応等に従事。2020 年 7 月退官。2022 年 4 月より現職。博士(工学)、MA in Management。



[本調査に関する照会先]

JCIC 事務局　info@j-cic.com