2023 年 2月

シリーズ 「日本のサイバーセキュリティ政策史」第 2 回

激動の時代に危機管理体制を構築して

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 2 回は、「国民を守る情報セキュリティ戦略」を策定し、大規模サイバー攻撃事態等への初動体制構築、情報集約体制整備を進めた元内閣官房副長官補（安全保障・危機管理担当）、内閣官房情報セキュリティセンター（NISC）長の西川徹矢氏をお迎えし、話をうかがいます。政権交代、東日本大震災など歴史的な出来事や危機に直面する中でサイバーセキュリティ政策をどのように舵取りしたのか――。

【出席者】

西川 徹矢 氏　笠原総合法律事務所 弁護士、
元内閣官房副長官補（安全保障・危機管理担当）、
元内閣官房情報セキュリティセンター（NISC）長

［聞き手］
三角 育生 氏.　東海大学情報通信学部長・教授

「国民を守る情報セキュリティ戦略」の策定背景

三角　本日（2022 年 11 月 29 日）は、2009 年 8 月～2011 年 8 月、内閣官房副長官補兼 NISC センター長を務めた西川徹矢さんをお迎えし、在任中に立案・実施されたサイバーセキュリティ（情報セキュリティ）政策の背景等についてお聞きします。

まず、「国民を守る情報セキュリティ戦略」（2010 年 5 月 11 日情報セキュリティ政策会議決定）の策定背景についてです。「はじめに」で、「本戦略は『第 2 次情報セキュリティ基本計画』を包含する、今後4年間（2010 年度から 2013 年度）を対象とした包括的な戦略である」と示されています。3年計画である「第2次情報セキュリティ基本計画」（2009 年 2 月 3 日、情報セキュリティ政策会議決定［以下、「第 2 次基本計画」という］）から 1 年 3 カ月で、大規模サイバー攻撃事態への対処態

勢の整備を中核とした新たな戦略が決定されたわけです。このように短期間で新たな戦略を決定した目的や背景には何があったのでしょうか。

西川　第 2 次基本計画では、大規模サイバー攻撃等の緊急事態に対する初動対処体制が明確になっていませんでした。対処の判断を下すには、各方面の現場の情報を的確に集約できる仕組みが不可欠です。個々の現場では特定の事象が発生していることを認識することはできても、それが国家レベルで重大なものか、そうでないのかはほとんど判断がつきません。それには、情報集約の全過程から収集された情報等を突合し、その危険性等を早期に把握し、その後の措置方針を決定する部署が不可欠です。私は、こうした仕組みづくりが必要だという問題意識を着任当初から強く持っていました。

というのも、長年、警察庁や警視庁、フェルディナンド・マルコス大統領退位の混乱期の在フィリピン大使館、県警察など、危機管理の現場、あるいはその総括責任者の立場にありました。そこでは、いささかなりとも、重大または危険性のありうる現場情報を瞬時に中央に上げて、それらの情報も踏まえて中央で判断しコントロールする仕組みで動いていました。危機管理の現場においてはそういう発想のもと、関連組織でそれぞれの役割や取るべき情報を明確にしておくことが必要なのです。

三角　同感です。ただ、そうした体制を構成する際、職員の資質や問題意識などによって差異が出てしまう、あるいは、せっかく熟度を上げた職員が異動してしまうと体制が弱くなることもあるのではないでしょうか。

西川　そのためにも、常に体制の構築を念頭に入れて、常日頃から計画的に人材の発掘・育成および訓練をすることが重要です。

人が異動したから機能しなくなる、という問題は起こしません。万一、個別の案件で情報の収集や報告に漏れがあったとしても、他地区担当者を臨時応援で派遣したり、補充したり、いろいろな代替措置を講じて作戦を実施するなどしておけばよい。そのような組織をつくろうとしました。

ある県警察の本部長時代、特定の容疑者について、特定の課の捜査員に対し、個々人が保有するすべての情報をデータベースに入力させ再利用できるようにした上で、さらに、情報を集中的に収集分析した結果、初めて見えてくるものがあり、犯人を追い詰めたことがありました。サイバー分野でも同様な手法も使えると思います。特殊な分野ゆえ、携わる人間が限られていますが、その層を厚くし、そうした人間に、情報を集中的に監視させていると、「ふわっと」浮いて見えてくるクセや特徴のようなものがあります。それが大事なのです。

三角　なるほど。そうした組織をサイバー分野ではどのように構築されたのでしょうか。

西川　どういう組織体にするかについては、在任中に関係者と議論を重ね、最終的にその構想は、私の退任後に公表された「官民連携強化のための分科会における検討結果」（2012 年 1 月 19 日 CISO 等連絡会議に報告、同 24 日に情報セキュリティ政策会議に報告・公表）のかたちになっています。もちろん、これには長い期間がかかりますが、とにかく積み上げていくしかないと思います。この結果を踏まえて、政府機関等の情報システムに対するサイバー攻撃等が発生した際、技能

員による適格かつ機動的な支援が可能となる情報セキュリティ緊急支援チーム(CYMAT)を整備しようとしておりました。CYMAT は発生事象の正確な予測や把握、被害拡大防止、復旧、再発防止のための技術的な支援および助言、そして対処能力の向上に向けた特殊・専門的訓練等を行うこととなっていました。

緊急事態への対処態勢整備は自身の考えから

三角 「国民を守る情報セキュリティ戦略」では、策定の背景理由として、2009 年 7 月に米韓で大規模サイバー攻撃事態が発生したこと、大規模な個人情報漏洩事案の発生も後を絶たないことなどを述べています。米国から体制整備の必要性などの指摘があったのでしょうか。

西川 緊急事態に対する対処態勢整備の必要性は、自身の経験・考えから不可欠と考えたものです。米国等に対する大規模サイバー攻撃などは確かにありました。こうした事態の予兆や発生情報があれば、一般に国際的な情報交換は行われますが、それはギブアンドテイクの世界です。わが国としても、しっかりと現場の状況・情報を予兆段階から把握することが不可欠です。その意味でも、情報集約体制を強化することが不可欠でした。

政権交代の影響

三角 2009 年 9 月 16 日に自民党から民主党に政権が代わりました。このことが新たな戦略策定を促したということはありますか。

西川 私が着任したのは同年 8 月 11 日の自民党政権時代です。その段階から、私としては大規模攻撃への対応体制の強化を図るべきだとの考えでした。

着任して 1 カ月で民主党政権に交代したわけですが、私の立場としては、まずは、「平成 17 年度以降に係る防衛計画の大綱」(2004 年[平成 16 年]12 月 10 日安全保障会議決定・閣議決定。以下、「16 大綱」という)の見直し作業をどうするかが戦略的重要課題でした。16 大綱では、「5年後又は情勢に重要な変化が生じた場合には、その時点における安全保障環境、技術水準の動向等を勘案し検討を行い、必要な修正を行う」ことになっていました。

「防衛大綱においては、平成 21 年末までに検討の上必要な修正を行うとされて」いましたが、そのためには 9 月の時点では検討作業が十分に重ねられている必要があります。そこで、当時の官房長官に諮り、その後の手続き等を検討した結果、まずは安全保障会議を開くことにしました。会議ではさまざまな意見が出ましたので、官房長官は、もう少し時間をかけて議論をする必要があると判断され、その結果、鳩山内閣は「国家の安全保障にかかわる重要課題であり、政権交代を経て、新政権として十分な検討を行う必要がある」として、同年 10 月 16 日の関係閣僚委員会、基本政策閣僚委員会等において、現大綱の見直しおよび次期中期防衛力整備計画決定を 1年先送りし、2010 年中に結論を得ることになりました。

一方、実務政策性の強い情報セキュリティについては、同政権でも政権交代前からの大規模攻撃対応体制の強化の方針をそのまま進めることになりました。その具体的な措置としては、

2010 年 12 月 27 日、情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議で、「情報セキュリティ対策推進会議・危機管理関係省庁連絡会議合同会議申合せ」として、大規模サイバー攻撃事態等における政府の初動対処態勢の整備、平素からの情報収集の強化と情報共有の徹底について府省庁の合意が確認されました。

三角　ところで、政府機関の対策に関して、2011 年4月 21 日（同 26 日改定）、情報セキュリティ政策会議で「政府機関の情報セキュリティ対策のための統一管理基準」に、規範（「政府機関の情報セキュリティ対策のための統一規範」）も新たに設けられました。その趣旨は何だったのでしょうか。

西川　情報セキュリティ対策推進会議で府省庁の官房長等を集めて、大規模サイバー攻撃事態等の初動対処を決めましたが、セキュリティポリシーを政府方針のもとに責任を持って実施していくのは府省庁の最高情報セキュリティ責任者（CISO）たる官房長等の任務です。官房長等に、具体的に何をやるべきかをしっかりと認識してもらうために規範として簡潔に示しました。

東日本大震災の勃発

三角　安全保障・危機管理担当官房副長官補の任にあって、2011 年 3 月 11 日の東日本大震災発生後、危機管理・初動対処の体制整備は大変であったと承知しています。さりとて、平素からグローバルな情報セキュリティの防護体制の重要性は変わりません。情報セキュリティ体制と危機管理体制とのバランスをどう取られたのでしょうか。

西川　東日本大震災の初動時点で原発対策等についての責任者は内閣危機管理監で、私は地震・津波被害対策を担当する責任者として主任務を手分けしました。地震・津波被害対策の初動体制は2週間ほどである程度目途が立ったので、その後は情報セキュリティ体制についても並行して対応することができました。

3 月 11 日 14 時 46 分の地震発生後、2 分間で私は官邸危機管理センターに駆け付けました。その後約1週間は着の身着のまま、それ以降も昼夜を問わず常駐しました。その時点で人命の救出に次いで大事だと考えた一つは、道路の復旧です。和歌山県警本部長時代、私は阪神・淡路大震災を経験しています。道路・鉄道網が壊滅的な被害を受けて、緊急車両も動きが取れず、救助や支援活動が困難な状況でした。そこで、東日本大震災の被災地復旧においては、少なくとも片側一車線の復旧などを迅速に行うことに腐心しました。また、併せて、救助要請のない、救命の声すら届いてこないエリアを特定しようと努めました。そこはつまり、最も被害の深刻なエリアということであり、優先的に救助が必要だからです。

東日本大震災は年度末に発生したことも大問題でした。なぜなら、役所は4月1日から翌年3月 31 日までの1年間を4期に分けて予算管理をしています。最後の第四 4 半期の3月となると、たいていの場合ほとんど予算を執行してしまっている。しかも、今回の災害では、予算執行を実際に担当する現場の役所が震災のために機能できない。そうした困難な状況の中での復旧作業でした。

三角　東日本大震災発生以降しばらくの間、日本では顕著なサイバー攻撃は見られませんでした。

震災後、最初の顕著な事件は 2011 年 9 月の三菱重工業への標的型メール攻撃ではなかったかと思います。

西川　そうですね。同事件を受けて、2011 年 10 月 7 日、情報セキュリティ政策会議議長である官房長官の談話として「情報セキュリティ対策の強化について」が発出されました。国の重要な情報を扱い国の安全に深く関わる企業に対して、企業の情報セキュリティのいっそうの強化と政府・民間双方向の情報共有等の官民連携への協力を、また、一般企業等に対して、職員の情報セキュリティ意識の向上、感染時に被害を最小限にとどめる対策の実施を、さらに、国民全般に向けてパソコンやスマートフォン等のセキュリティ関連ソフトウエアを常に最新の状態にするよう呼びかけました。


西川氏

情報セキュリティに関する認識

三角　官民双方に具体的対策を呼びかけていたわけですね。

西川　そういうことです。

日本の情報セキュリティや安全保障の戦略のあり方について、根幹から考え直すべき点がいくつかあると感じています。たとえば、日本での情報セキュリティの関心が企業機密情報や個人情報等の漏洩が中心となっている点です。これに対し、米国等 IT 技術先進諸国ではサイバーテロやサイバースパイ等の国防機密情報や政府機密情報等への攻撃に重点をおいています。

かつて、2000 年（Y2K）問題では、コンピューターが一斉に誤作動を起こすかもしれないことばかりがクローズアップされました。マスコミも大きく取り上げました。しかしそれは使用しているソフトや OS のバージョンを上げるなど手を打っておけばよい話で、むしろネットワークセキュリティの方が問題だったのではないでしょうか。実際、2000 年1月 24 日に科学技術庁等多数の省庁のホームページが改ざんされる事件が発生し、ネットワークセキュリティの重要性が認識されるようになりました。

三角　そうでしたね。

サイバー攻撃に備えて

西川　また、サイバー被害を受けたことが新聞等で報道されると株価に影響するから情報開示をしたくない、という声を聞くことがあります。しかし、株価が下がることもさることながら、国の重要インフラが停止・破壊されることのほうが社会的に甚大な影響を及ぼすことが多いと思います。サイバー攻撃を防ぐ手立てを講じてさえいれば大丈夫ということでもありません。被害を受けたらすみやかに情報開示をする。国は中央で対処することと各企業で対処してもらうことをいち早く手分けして、被害の拡大や社会生活に混乱の起こらないようにハンドリングする、ということがきわめて重要です。

三角　事案が発生した際、意図して隠そうとするのではなく、サイバー事案ではないから報告する必要はないと判断されるケースもあります。西川さんが最初に指摘されたように、個々の事案がサイバー攻撃を原因とするのかどうかの判断は難しいものです。全体を見る中で、同様のケースが同時多発的に発生することを認識して、はじめてサイバー攻撃によるものだと判断できる、といったようなことになるわけですね。

西川　件数の多寡だけが問題ではなく、基本的には、わからないと思った瞬間に情報を上げることです。

三角　西川さんが在任中に、「国民を守る情報セキュリティ戦略」が策定され、大規模サイバー攻撃事態等への初動体制の構築、情報集約体制整備が進み、東日本大震災後も具体的な体制の実施が着実に行われていたことをあらためてお聞きすることができました。ありがとうございました。

（2022 年 11 月 29 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］）

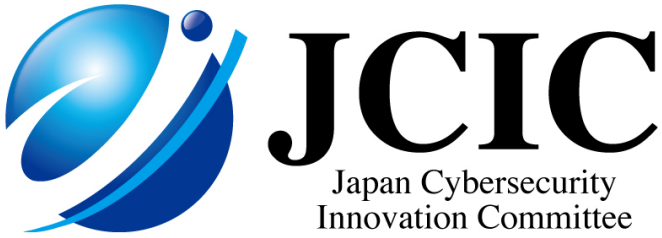
【出席者略歴】

西川　徹矢（にしかわ　てつや）氏

1972 年京都大学法学部卒業、警察庁入庁。在フィリピン大使館一等書記官、警視庁捜査第二課長、和歌山県および新潟県警察本部長、警察庁情報通信企画課長等を経る間に数々の事件捜査、危機管理、行政施策、組織運営を行い、1999 年防衛庁（省）に異動。防衛参事官（IT、施設、環境担当）等を歴任する中で、国際テロ対策、自衛隊イラク派遣、サイバー・情報戦対策、国会対応等に取り組み、2007 年退官。2009～2011 年内閣官房副長官補（安全保障・危機管理担当）兼内閣官房情報セキュリティセンター長を務める。現在、笠原総合法律事務所　弁護士。

三角　育生（みすみ　いくお）氏

1987 年通商産業省入省。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～東海大学情報通信学部長・教授。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