資料７

意見書

2021 年 9 月 27 日
日本電気株式会社
取締役会長
遠藤　信博

1. オリンピック・パラリンピックについて

オリンピック・パラリンピックに関係しましては、大会運営や国民生活に影響を及ぼすインシデントは発生しませんでした。国民の皆様の高い意識、重要インフラ事業者の徹底した対策、組織委員会を始め大会関係者の準備と運用があって成しえたことで快挙だと思います。一方、無観客で競技が行われた状況でも、チケット販売に関してサイバー犯罪の兆候が見られたことは、今後の各種イベント開催における対策に生かしていただきたいと思います。

大会の準備のため、かつてないほどのセキュリティ対策の準備を重ねてきましたが、そのノウハウを、今後の日本のみならず「海外の国々」のデジタル社会発展のために生かしていただければと思います。また、本大会に向けて実施したリスクアセスメントや関係者・専門家との議論を通じて、社内インフラ以外のまだ明確にはなっていなかった日本のウィークポイントが明らかになったと思います。これらに関しては大会後、速やかに改善に着手していただきたいと思います。なお、インシデントには至りませんでしたが大会期間中に得られた多数のサイバー攻撃に関するデータは、日本の財産として産学含めて共有しサイバー攻撃解析技術の向上や人材育成に活用されることを希望します。

2. 次期サイバーセキュリティ戦略(案)について

次期サイバーセキュリティ戦略(案)が、パブリックコメントにより多くの方から御意見をいただき確定しました。「Cybersecurity for All」では、DX と歩調をあわせ「中小企業」「高齢者」「若年層」をサポートし、経営者の意識改革もさらに進める方向です。また推進体制としては、新たに「デジタル庁」が加わることでより強固な体制になるとともに、ナショナルサートの整備で対外的な窓口の強化も重要です。安全保障の観点は、今までタブー視されることもありましたが、この領域での取り組み

の強化を図るとともに、刑事訴追等の手段を積極的に展開することに期待します。今後 3 年間、これらの戦略を確実かつスピィーディーに達成することが大切だと思います。

また、最近活発化している「ランサムウェア」に関しては、一部の二重恐喝型のランサムウェアを除きインシデントの発生状況、身代金の支払い状況が把握できていないと思います。日本政府としては、被害に遭った企業が相談するメリットが得られる仕組みを作り、これらの状況把握・情報共有に努めていただきたいと思います。これは「ランサムウェア」に限定せず、今後発生すると予想される新しい攻撃に対しても柔軟かつ迅速に対応可能なことが重要だと思います。

過去十年間のサイバーセキュリティの動向を振り返ると、標的型攻撃、BEC(Business Email Compromise)、マイニングマルウェア、ランサムウェアなど、次々と新しい攻撃方法が編み出されてきました。特定の攻撃手法の中でも、攻撃者によって技術革新が繰り返し行われてきました。一方 2020 年代は、これらに加えて、「サプライチェーン」や「制御系システム」などの新領域が既にねらわれ始めており、「安全保障」がより重要視されるようになり、量子コンピュータ、量子暗号通信、耐量子計算機暗号などの量子技術や人工知能技術が急速に発展すると予想されます。また、近年企業経営で重視される「バリューチェーン」も今後サイバー攻撃のターゲットとなる可能性が極めて高いと考えています。例えば、複数の企業間で形成されるバリューチェーンに参加するためのセキュリティ要件、データ改ざん等への対応等の検討をこの戦略期間に始めていく必要があります。最近の十年間は攻撃組織や被害組織が主役となる「戦術の闘い」が主流でしたが、今後の十年間は国家としての「サイバー戦略」の良し悪し、その実行力、産学官の情報連携が国家の趨勢を左右する「戦略の時代」が来ると思います。

以上