資料6

意見書

2022 年 6 月 17 日
KDDI 株式会社
代表取締役会長
田中　孝司

１．決定事項について

決定事項 3 件について、異論はありません。

サイバーセキュリティ 2022 は、戦略の事項に沿って良く整理され、令和 3 年度の評価と令和 4 年度の計画が包括的にまとめられていると思います。また、特に強力に取り組む施策として取り上げられた 6 件はいずれも重要な施策であり、現在の時流に合ったものが適切に選定されていると考えます。

重要インフラのサイバーセキュリティに係る行動計画について、現行の第 4 次行動計画における有効な取組を継続することに賛同します。サイバー攻撃等の増加については、重要インフラ事業者も例外ではないため、施策などが具体化されたことは評価できます。

サイバーセキュリティ関連施策に関する令和 5 年度予算重点化方針についても、重要インフラ事業者向けの施策を含め、6 件を特に強力に、かつ確実に取り組むという意図で、予算を重点的に割り振る方針に賛同します。

２．国主導の包括的な防御対策について

次に、具体的な案件に対する意見を以下に示します。

国際情勢の変化によるサイバーリスクが増大するとともに、国内でも多様なインシデントが発生し、ランサムウェアや Emotet による被害が拡大している状況です。このような状況を踏まえると、特に強力に取り組む施策として挙げられた「ナショナルサート機能の強化」は非常に重要な施策です。国民の安全・安心を守るため、NISC を中心に、国が主体的に関係機関と連携を図りつつ、包括的なサイバー防御を講ずることが急務であると考えます。

東京オリンピックでは NISC が中心となり業界横断で対応して頂いたこともあり、成功裏に閉幕しました。これまでのオリンピックの中で、東京大会が一番成功した事例であると思います。オリンピックに限らず、日本では、世界を震撼させるような大きなセキュリティ事案は起きていないのも事実です。これらは、NISC を中心とした関係の皆様の成果です。今後は、この成果であるオリンピックなどの対応で得た知見、ノウハウなどのアセットをさらに有効に活用する、昇華させていくなどの意識、取組が重要であると考えます。東京オリンピックで構築した情報共有プラットフォームの利活用など、次につなげていく施策をぜひお願いしたい。

日本のサイバーセキュリティ能力は、インテリジェンス能力や攻撃能力が欠如しているとの評価もあり、英国機関 IISS では Tier3 の最低評価となっております。一方で、上述させて頂いたとおり、東京オリンピ

ック開催時を含めて大きなセキュリティ事案が発生していない事実もあります。当然、全てに対応できておらず、対応が不十分のところ、対応できるところがありますが、成果がでているところ正確に認識頂く必要があるかと思います。

正しい情報を正確に理解して頂くという意味で、日本もサイバーセキュリティ対策をしっかり講じている点を発信していくべきと考えます。サイバーセキュリティ分野は一般国民にとって難しいことも事実ですが、外部環境が激しく変化している中、専門ではない方々にも理解してもらえるように、丁寧な広報活動が必要です。

３．サイバーセキュリティ戦略の実行フェーズについて

サイバーセキュリティ戦略は実行フェーズに入っています。サイバーセキュリティ戦略のフレームワークは良くできており、これを確実に実行・運用していくことが今後重要となってきます。そのためには、先を見据えて先手を打つ、想定リスクを抽出し対処していくことが必要となります。

今後、特に重要となるのが DX の推進で、そのコアとなるのが 5G・IoT 通信です。これらのコア技術に対してプロアクティブな取組みが必要と考えます。

例えば、5G 通信サービスにおいては、一昨年の 2020 年に提供開始しましたが、より高機能なサービスが提供できるシステムも進化しますし、オープン化も進んでいきます。技術の進化にあわせて、フレームワークの一つとなるガイドラインなどもアップデートが必要ですし、実運用を意識した取組みが必要となります。

以上より、サイバーセキュリティ戦略のフレームワークの実行フェーズを成功させるべく、国主導の包括的な防衛対策を進めるとともに、正しい情報を正確に把握・理解して頂くための広報活動と、外部動向変化に応じた臨機応変、かつプロアクティブな対応・取組みを期待します。

以上