資料5

意見書

2022 年 6 月 17 日
日本電気株式会社
取締役会長
遠藤　信博

1. 決定事項について

サイバーセキュリティ 2022(案)、重要インフラのサイバーセキュリティに係る行動計画(案)、サイバーセキュリティ関係施策に関する令和 5 年度予算重点化方針(案)に関して、いろいろな観点から深くご検討頂きありがとうございます。これらの案に賛成いたします。

特にサイバーセキュリティ 2022(案)では、国内で発生する多様なインシデントの多くが国際情勢の変化に起因としていることに留意し、その対策として情報共有・犯罪捜査・人材育成等における国際協力・連携の強化が重点施策の一つとされていることが重要だと思います。

また国内においては、地域や中小企業等のセキュリティ対策や重要インフラを中核としたサプライチェーンのセキュリティ強化にも配慮しており、重点施策としてバランスが取れていると思います。

令和 5 年度予算要求においても、サイバーセキュリティ戦略の 3 つの方向性を踏まえ、それに関連する「特に強力に取り組む重点 6 項目」の強化に努めて頂きたいと思います。

2. データから価値創造を行うバリューチェーン

DX の浸透とともに、今まで企業内で閉じていたデータの共有範囲が多くの関係する企業に拡大し、共創により価値を創造するバリューチェーンが形成されるようになりました。そこでは、生産や流通に必要なデータを、国境を越えた企業とリアルタイムで共有し、データを中心とした価値創造を行う「全体最適型のソリューション」を作り上げることが求められています。セキュリティに関しても、このオープンでダイナミックに変化する企業間バリューチェーンの中で、より厳密に、よりストレスなくデータが保護されることが要求されます。現在、脚光を浴びているス

マートシティやスマートヘルスケアといった分野が、まさにこういったバリューチェーンを必要とする領域だと思います。

バリューチェーンをセキュアに保つためには、個々の企業のセキュリティ能力を高め、全体としてのセキュリティ能力を高めることが重要になってきます。特に、全体組織でのセキュリティ強化で重要なのは、バリューチェーンで共有するあるいは共通化するデータやソフトウェア部品の安全性の確保で、米国のバイデン大統領も言及しているソフトウェア部品表(SBOM)などは、国際間協調がなければ実用化が難しいものの一つであり、米国や他の諸国と連携し一刻も早く実現することが必要です。

3. コレクティブセキュリティの重要性

近年、国際間のサイバー攻撃がますます活発化しており、従来のセキュリティ対策では対応が難しいケースが増加しています。サイバー攻撃対策には、「攻撃者の情報」「マルウェアの情報」「攻撃手法の情報」「ターゲット製品の脆弱性情報」など、地理的にも、分野的にも異なる情報の収集と分析が必要となり、国際的な情報共有、分野横断的な情報共有が不可欠となってきました。このため、防御側での協力態勢である「コレクティブセキュリティ」の概念の重要性が急激に増しており、今後短期間に、政府内・各種組織間や官民連携での多層的なコレクティブセキュリティの仕組みを構築していかなければならないと思います。

4. 我が国の弱点を知るためのサイバー防御力強化について

国際紛争の状況などを鑑みると、日本のサイバー防衛能力の抜本的強化が必要なことは言うまでもないと思います。不正アクセスや DoS 攻撃のようなサイバー攻撃では、相手の最も弱い部分を狙うのが常識・常道ですが、実際には防御する側が自身の弱点を正確には把握できていないことが多く、攻撃が容易に成功しているケースが多いように思います。これは、システムに対して攻撃者視点でのペネトレーションテスト(模擬攻撃)を実施しておらず、システムの本当の弱点を見逃していることが原因と考えられます。

日本では、ペネトレーションテストを実施できる技術者は、質・量に関しても米国などと比べると劣っていると言わざるを得ません。高度な専門技術者を育成するコースや研修サイトに関しても、本格的なものは国内には存在していないのが現状で、まずペネトレーションテスター育成の仕組みを作り、実際にペネトレーションテストで弱点を明確化することで、「高度なセキュリティ技術者の育成」と「サイバー防御力強化」を同時に実現できると考えます。

5. 事故調査委員会設置に向けた課題

最後に、サイバーセキュリティ 2022(案)の国民が安全で安心して暮らせるデジタル社会実現の取り組みの中の「サイバーインシデントに係る事故調査の体制整備に向けた実証事業」に関しては、「事故調査を行うために最低限必要とされる技術力」の確認と「実証事業の中で検討すべき二つの課題」の検討が必要であると思います。

事故調査のためには、各業種・業態に対応した「システム・運用の専門知識」に加えて、間違いなく正確に分析を行うために必要な「攻撃手法」「防御技術」「解析手法」「マルウェア技術」「インシデントの傾向」等の高度な知識が必要であり、必要な技術の整理と、これらを持った一定水準以上の技術者を分野毎に育成しておくことが最低限必要になると思います。

また実証事業における一つ目の課題は、民間企業から事故調査委員会への参加者に与える資格や権限に関するものとなります。事故調査者は通常は所属企業の技術者としての業務がありますが、事故調査委員会に招集されると公的機関の立場で企業秘密やインシデント情報に触れる必要があり、一定の資格や権限を付与する必要があるとともに、守秘義務なども明確に定義する必要があります。

二つ目の課題は、事故調査ノウハウの継承に関する課題です。事故調査委員会に招集されるメンバーは、中・長期に亘っての固定化が難しいですが、守秘義務があるため実際のインシデント調査から得られたノウハウの継承が難しいと予想されます。さらには、制御システムのインシデント調査で重要となる高度な解析ノウハウはドキュメントだけでは伝えきれない部分が多いため、ノウハウの継承方法に関しての仕組み作りを是非、検討していって頂きたいと思います。

以上