資料18－1

前回までの御議論について

サイバーセキュリティタスクフォース事務局

令和元年12月５日

第16回、第17回で頂いた主な御意見について

【総論・その他】

- 東京2020大会まで間に合うものは実行するべきである。また、中長期的に法制度を含めて見直さねばならないものは何なのか、この場で認識の共有を行うとよい。
- 東京2020大会に向けて大会組織委員会の準備状況を報告してもらってはどうか。
- サイバー対策はネットの安全性を高めるので通信の秘密を強める、保護レベルを高める可能性があることを踏まえ、（通信の秘密について）議論をすべきではないか。
- 通信インフラ事業者（ISP）だけでなく巨大IT企業など上位レイヤーが有する情報にも意識して対策を考える必要がある。

【IoTのセキュリティ対策】

- IoT機器の調査結果を、ユーザーの啓発や、これから重要になる端末の安全性確保などに活用すべき。
- 「NOTICE」の取組について、技術的知識が十分でない一般の利用者に対してIoTセキュリティの重要性の周知啓発のための検討が必要。
- 短期的な取組と長期的な取組に分けて、短期的な重要IoT機器に対する対策はできれば東京2020大会までに実施すべき。
- 動的IPアドレスにつながる機器が外からのアクセスを期待してポートを開けることはあまりないので、対策について中長期的に取り組んでいくべき。
- 中長期的な課題として、C&Cサーバと通信しているIoT機器への対処について、制度面も含めて検討すべき。
- 大規模停電からの復電時などにIoT機器が一斉に通信を行うことで障害とならないよう十分な検討を行うべき。
- オープン情報を集約して脅威検知を行う仕組みや、攻撃側が有する情報を陳腐化するような技術が必要。
- 重要IoT機器の脆弱性調査が実施できるよう、予算化を含む必要な対応を行うべき。

【クラウドサービスのセキュリティ対策】

- 中小企業に係るサプライチェーンリスクの問題については、クラウド化・アウトソーシングによって端末管理にリソースを集中する仕組みの導入が必要。

【重要インフラとしての情報通信分野のセキュリティ対策】

- 大規模災害に対する通信設備の可用性について点検が必要。
- 未然防止だけでなく、事後の対処についても、特に重要インフラの１つである自治体では重要。

【研究開発の推進】

- ソフトウェアとハードウェアの両方にぜい弱性があるということ、及びそれらの課題について産学が連携して研究開発で取り組んでいるということを広く周知すべき。
- 広域ネットワークスキャンの研究開発の成果を、「NOTICE」を含めた様々な分野で活用することが重要。

【人材育成・普及啓発の推進】

- 人材育成については、技術と制度を掛け合わせたハイブリッドな人材の育成が必要。
- セキュリティの知識の全体的な底上げのため、戦略マネジメント層人材の育成が非常に重要。
- そもそもセキュリティに興味を持ってもらうための入口の取組が必要。
- 理工系以外の組織を含め社会全体でマインドを育成していくことが重要。
- 重要インフラ事業者について、CYDERへ参加を促す必要がある。

【情報共有・情報開示の促進】

- 人材育成については、インシデントなどの積極的な情報共有や情報発信が重要。

（※）項目は総合対策の想定箇所又は関連箇所、赤字は第17回で頂いた御意見

第17回で御議論いただいた内容と今後の方向性について①

■ 重要インフラ事業者等が設置するIoT機器のセキュリティ確保に向けて取り組むべき事項はないか？

（Ⅲ(1)IoTのセキュリティ対策）

主な現状と課題

- IoT機器について、**公知、未知のネットワーク探索システムの活動が活発化**し、IoT機器の所在やセキュリティ状態が全世界的に把握されつつある。また、探索システムの悪用については不明だが、**明らかに不要なアクセスを誘発するケース**が存在。
- 広域スキャン等による調査から、国内の重要施設を遠隔監視するシステムにも**セキュリティ不備がある可能性**が示されている。ハニーポットの観測結果を見る限り、セキュリティ不備のあるシステムは**不正アクセスのリスク**がある。
- 従来よりISPからマルウェアに感染等している機器の利用者に対して注意喚起を行っているが、IoT機器の場合は機器の数が膨大になり、**利用者も当事者意識が希薄**であるため、注意喚起の効果が日増しに薄れてきている。

今後の方向性（案）

- **攻撃者より先にIoT機器の設定等のセキュリティ不備を見つけ、迅速に通知して対策を行う取組**が重要ではないか。また、取組は東京2020大会までに実施すべきではないか。
- またその際は、**機械学習や人工知能**の利用によって発見の効率を高めることも検討すべきではないか。
- NOTICEの取組なども踏まえつつ、**IoT機器の利用者周知の在り方**について検討すべきではないか。
- 探索システム等の情報を集約して脅威検知を行う等、そのような情報を用いた攻撃への対応案について検討すべきではないか。
- 不要なポートを閉じる方策について、中長期的に検討すべきではないか。
- 中長期的な課題として、C&Cサーバと通信しているIoT機器への合理的な対応方法について、制度面も含めて検討すべきではないか。

第17回で御議論いただいた内容と今後の方向性について②

■ 地方公共団体や重要インフラ事業者等の人材育成を強化する必要はないか？

（ Ⅳ(2)人材育成・普及啓発の推進）

主な現状と課題

- 国立研究開発法人情報通信研究機構（NICT）の実施する実践的サイバー防御演習CYDERにより、情報システム担当者等を中心に**インシデントの検知から事案の対処・復旧までの実践的な学習機会**を提供。
- 受講者アンケートでは概ね好意的な反応であり、参加状況についても、国の行政機関等については未受講組織数が過去３年間で急減。一方、**地方自治体**については、依然として**半数近くが未受講**。
- 未受講の理由としては、業務多忙のほか、**開催日程、開催場所**が合わないという声が多い。
- 開催地を県庁所在地から変更・追加する等の事業運営上の工夫により、一定の効果は認められるが、課題の抜本的な解決には至っていない。

今後の方向性（案）

- 東京2020大会の開催に先立ち、社会的なセキュリティ対応力を強化するため、**特に未受講の地方自治体を対象とした集中的な受講機会を設けるなど、より効果的な取組**を検討する必要があるのではないか。
- 開催場所が遠方にあることを主な理由として挙げる未受講組織も多いことから、その対策として、オンライン受講環境の整備等、**受講場所に依存しにくい訓練機会の検討**も進める必要があるのではないか。
- その他の重要インフラ事業者にもCYDERの参加をより一層促すべきではないか。

第17回で御議論いただいた内容と今後の方向性について③

■ サイバーセキュリティの質の向上のため実効的な情報共有体制が構築・運営されているか？

（Ⅳ(4)情報共有・情報開示の促進）

主な現状と課題

- ISAC（Information Sharing and Analysis Center）は、リスクマネジメントの活動の一環であり、協業事業者、パートナー、競争事業者などの情報連携により、**サイバー攻撃からの防御コストの低減**に寄与。サイバー攻撃や事故への事前の対処だけでなく、**障害発生時の事案対処や復旧に関する情報**も共有。
- 国内では平成14年のTelecom ISACの設立を皮切りに、業界ごとに様々なISACが立ち上がり始めている。
- ISAC同士の連携が進むことで、例えば各ISACが有する情報のうち、類似した事例や国・業界横断的な対処方法を共有するなど、**業種ごとの共通課題を踏まえた情報共有の進展による対応能力の高度化が期待**される。
- 一方、業態によっては、**ISACを立ち上げる事務局人材もいない場合もある**ことが想定される。

今後の方向性（案）

- 情報共有体制については、官民においてはサイバーセキュリティ協議会、「重要インフラの情報セキュリティ対策に係る第4次行動計画」、サイバーセキュリティ対処調整センターなど、**既存の情報共有体制の枠組みの着実な実施**を図るべきではないか。
- その上で、東京2020大会及びその後に向け、我が国の様々な産業のサイバー攻撃への対応力を強化するため、NISC等と連携し、**国内のISAC間の連携を支援**するとともに、**先進的な取組を行っている米国のISAC等との連携も支援**するべきではないか。
- また、情報共有体制が未整備な国における**ISACの構築を支援**するべきではないか。
- さらに、人材が不足している分野については、ICT-ISACの有する知見やノウハウを活用し、**ISACの構築等を支援**するべきではないか。