参考資料２

ICT サイバーセキュリティ政策分科会（第２回）議事要旨

1. 日 時）令和 6 年 2 月 27 日（火）13：00～14：46

2. 場 所）WEB 開催

3. 出席者）

【構成員】
後藤主査、栗原構成員、小山構成員、篠田構成員、蔦構成員、盛合構成員、吉岡構成員

【オブザーバー】
内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制準備室、デジタル庁、地方公共団体情報システム機構

【総務省】
山内サイバーセキュリティ統括官、豊嶋大臣官房審議官（国際技術、サイバーセキュリティ担当）、小川サイバーセキュリティ統括官室参事官（総括担当）、酒井サイバーセキュリティ統括官室参事官（政策担当）、佐藤サイバーセキュリティ統括官室企画官、牧野サイバーセキュリティ統括官室統括補佐、井上サイバーセキュリティ統括官室参事官補佐、中尾情報流通行政局放送技術課課長補佐

【発表者】
取屋慶治（一般社団法人日本ケーブルラボ）

4. 配付資料

資料２－1　放送設備の安全・信頼性に関する技術基準の概要と最近の動向
資料２－2　ICT-ISAC 放送 WG の活動と放送局の設備、セキュリティ（一部非公開資料）（栗原構成員）
資料２－3　（一社）日本ケーブルラボとケーブルテレビ業界に向けたセキュリティの取組み
（日本ケーブルラボ）

5. 議事概要
（1）開会

（2）議題
◆議題（１）「放送分野におけるサイバーセキュリティ対策の取組ついて」、総務省より資料２－１、栗原構成員より資料２－２を説明。

◆構成員の意見・コメント
後藤主査）

資料２－２の 6 ページ目について、赤い枠の中が心臓部であり、それ以外の部分が変化している状況と説明いただいたが、赤い境界線はどの程度厳格に機能的に分かれているのか。例えば IP 化する際、赤い枠の中を一斉に切り替えるのか、あるいは少しずつ IP 化したものを作り、確かめながら IP 化していくのか。個別システムのマイグレーションを行うのかもしれないが、結構リスクがあると感じた。

栗原構成員）

送信設備は電波を出すものであるため、IP 化されることはあまり考えづらいが、赤枠内の送出バンクや最新の設備などは既にファイル化が進んでおり、現在でも IP 方式で最終段階に渡すことはできる。マスター設備と呼ばれているエンコーダーや多重化装置などについて、従来の専用機器からソフトウェア化されるかはわからないが、番組も既にファイル化されているので、どこまで IP でデータ送出するかなどは今後の動向を見ながら安定性やコストなどを考えていくことになると思うが、番組制作の設備の大部分が IP 化しているため、今後は番組をデータで送出設備に渡す形になっていくと思う。サブなどは別だが、カメラが IP でいきなり出ていくのかというのは、なかなか懐疑的である。

後藤主査）

赤い枠の外の部分で IP 化されたものに関して、大きな事故などは起きた例はあるか。

栗原構成員）

番組制作設備で大きな事故が起こったことはない。

蔦構成員）

まず 1 点目として、資料 2―1 の 10 ページの訓令と記載されている放送法関係審査基準と改定予定の技術基準は同じものという理解でよいか。それを前提に、訓令であれば行政機関内の上から下への命令・伝達であるから、基本的には民間企業は関係ないと認識している。ただし、あくまで審査基準として、審査するために内部でこのような基準に基づいて検討するということだと思う。行政手続法では、審査基準は基本的に公にしなければならないとされているが、これは公開されているのか、その辺りについてコメントいただきたい。2 点目が、参考となっているため意見を言う対象でもないと思うが、24 ページの 1 つ目のポツで具体的な措置内容としてお示しいただいた、サイバー事案による障害からの早期復旧を図るための措置として、バックアップの実施等の措置が記載されているが、これだけでいいのか疑問に思った。28 ページの枠内 2 つ目のポツについても、サイバー事案からの復旧に関することが記載されているので、これも復旧を図るための措置の一つなのだろうとは思ったが、24 ページの記述とのつながりが分かりづらかったので、今後の改定の参考としていただければと思う。加えて、総務省と栗原構成員への質問として、放送分野については、重要インフラの行動計画や安全基準等策定指針に基づいてガイドライン等を策定されていると伺った。似たような制度として経済安全保障推進法において、放送分野が基幹インフラ分野とされており、番組送出設備が特定重要設備に入っている。特定重要設備の導入については経済安全保障推進法との関係で届出をしなければならず、その際、リスク管理措置として様々なセキュリティ対策を含めた措置をとることになっていると思うが、どのように対応されているか御意見いただきたい。

総務省放送技術課　中尾課長補佐）

訓令であるということについて、省令の下位法令として御指摘のように審査基準として定めているが、放送事業者がこれを規範として自らの放送設備に対する措置を行うものであるため、改正案を公開した上で、意見募集・パブリックコメントを経て、提出があった意見を反映して改正を行っている。経済安全保障についての御質問については、直接的な担当ではないのでどこまで回答できるかわからないが、経済安全保障推進法と放送法の規定とは見る観点が異なると考えている。放送法の場合はあくまでも放送設備の安定的な運用、そして放送停止事故を起こさないことの観点から規定しているもので、経済安全保障推進法の規定は、例えば機器のサプライヤー等をチェックするなど、いわゆるナショナルセキュリティという観点から規定しているものと認識をしているので、

個別の対応となっている。

栗原構成員）

放送設備の直接の担当をしていないため、経済安全保障に関してどういう動きになっているのか分からないところではあるが、ICT-ISAC の放送 WG としては、そういったことも加味してガイドラインや参考資料等を今後検討していきたいと思っている。

蔦構成員）

重要インフラと基幹インフラがよく混ざると思っているので、お聞きした。

盛合構成員）

放送設備が IP 化されてきていることで、インターネットにつながる典型的な IoT 機器になってきたと思った。放送事業者の方は外部のネットワークには繋がないので安心とよく言われるが、ファイルでのやり取りではいくらでも入り込む余地があるので、安心してはいられないと思う。実際に米国でも大手のテレビ局のシンクレアなどがランサム攻撃を受けた例や、日本でも NICT がオリパラの際に情報セキュリティ関係機関としてご協力した際に、海外の放送局の方々がネットワークに繋いだ瞬間に様々な感染機器が見つかる等の事象があった。放送機器が感染してしまうと偽情報を流されるという可能性もあり、まさに放送事故になってしまうのではないかと危惧している。業界内ではあまり危機感がない、セキュリティが自分事とされていないといったお話もあったが、WG などで課題を持ち寄って議論をされていると思うが、サイバーセキュリティに関する研修などは受けているか。

栗原構成員）

スタッフにも放送の最後の送出を行っているスタッフと番組制作スタッフの 2 種類あり、仕事の内容が大きく分かれている。番組を送出する部門では、送出設備に張り付いて監視する業務を一人でできるようになるまでの研修を厳しくやっているなどにより守られていると思う。また、番組を受け取るという業務も比較的決まったスタッフが行っていることから、そういったところで守られているのだと思う。一方で、制作側については、先ほどのオリパラなどではスタッフが増員されるなど、スタッフが流動的な中で、いくつかのパソコンが感染するということはあると思うが、パソコンが使えなくなってしまったということは今のところ起きていない。EPP や EDR などで守っていることでパソコンが使えなくなったとしても放送そのものが止まるということはない。アノニマスの仮面のようなものがいきなり放送に流れてしまうといった、ファイルを入れ替えられてしまうといったことも現実にはなかなか考えられない。実際にはファイルは必ずプレビューもされている。一方でそのファイルが何かに感染していた場合に全体に影響する可能性があることは危惧しているが、映像ファイルのため、非常にファイルサイズが大きく、例えば 90 分 50GB のファイルサイズが納品された時に全てウイルスチェックをかけるのは現実的ではない。ただ、実行可能ファイルかというとそういうわけでもないと思っているので、現在は番組を送出するためのハードウェアに入れているので問題が起こっていないのかもしれないがそういう侵害はあまり考えられない。どちらかといえばメールから感染しているのに気づかず、奥の設備のメンテナンスのために接続することで中枢のサーバが被害を受けてしまう、あるいはインターフェイスより表にあるサーバが同様な方法で被害を受けた時に、インターフェイスの穴を通して内部のサーバまで被害を受けるようなことがあれば、全体が固まってしまうということもありうる。いずれにしても予定していた番組が流せなくなる可能性があるとは思うが、一昨年ほど前にアニメの会社が被害に遭い、新しいものがオンエアできず再放送や他の番組で埋めたことがあったように、納品しようとしたドラマがランサムウェアの被害でオンエアできなくなってしまうといったことが制作会社側で起こることはあったとしても放送は出ると信じている。

盛合構成員）

色々なシナリオを考えて対策、ファイヤードリルを定期的にやるのがよさそうだと思った。

吉岡構成員）

放送事業者向けならではの要素もあり、一方で事例としては国内ではまだ大きな問題はないという話もあったが、放送事業者ならではの課題や問題をどのように抽出されているか、それに合ったような訓練を行うときにどうされているか。また、対策の観点で他の重要インフラと異なる点もあると思うが、プロの目から見てどういった点での違いが一番大きいか伺いたい。

小山構成員）

通信事業者として、過去から現在まで外部とのネットワークを切り離して、境界防御でセキュリティを確保してきたが、その反省点として、閉域網の中は安全といった過信から、IT の資産管理が疎かになる傾向があり、セキュリティパッチを当てることが十分に行えない場合や、例えば EOL のサーバの更改で多額の設備投資が必要になり、思うようにセキュリティ対策が進まないなど、大変な苦労をした経験がある。通信事業者の事例が放送事業者に当てはまるとは限らないが、今後放送設備の IP 化やクラウド化を進める際に、総務省が放送事業者向けに行う政策として、脆弱性対策を推進したほうが良いのではないか、総務省にお考えをお伺いしたい。また、事業者として現在どのような取組をされているか栗原構成員にお伺いしたい。

栗原構成員）

吉岡構成員から御質問のあった他の業界と性質が違う点について、放送設備の点では結構しっかりやっているつもりではいるが、制作現場はそれほど意識が高くない。良い番組を作るということが一義になっているため、例えば取材のために危ないサイトも閲覧し、アラームが出ても取材のためと言われてしまうとすぐにパソコンを閉じろとは中々言えないという特質はある。また、制御用の IT にはパッチが当てられないという課題がある。当ててしまうとメーカーが保証しないといった言い方をよくされる。メーカー側としてもどのようなパッチが当てられるか分からないため動作の保証はできないというのが基本で、パッチを当てたいと言うと、見積の話から始まってしまうというところもある。大きな脆弱性があればもちろんパッチを当てるが、中々IT の世界では当てにくい。放送機器となると動作保証の観点から、放送に傷がつかないようにパッチを当てるということはあえて行わず、攻撃者が入らないようにするしかないというのが現状である。今できている対策としてはホワイトリスト型の対策ソフトでの対応や、運用上でつながないようにするということぐらいまでである。今後、ネットワークを監視するというのが重要だと思っているが、出入口でどのようなトラフィックが流れていて、いつもと違うトラフィックがないかを確認する、あるいはどこかに通信しようとする際にいつもないはずのようなものを探すということをサーバ本体側ではなく、ネットワーク側で監視していくということが今後重要かと思う。

小山構成員）

IP 化やクラウド化を前提に考えると、パッチを当てたくらいで異常な動作を起こすような IT 機器や放送設備ではあってはならないと思う。システムの信頼性や安全性ついて、総務省の関与が必要かもしれないが、可用性の高いシステムをクラウド上に作り、その上でセキュリティパッチを迅速に当てられるような運用体制を構築していくことが必要ではないか。

総務省放送技術課　中尾課長補佐）

総務省からは制度の面について発言させていただく。現行の設備については放送専用の伝送規格が用いられることもあって外部ネットワークに原則つながないことと、境界防御型の防御策によって措置するという規定になっており、現在のところも大きな問題はなく運用されているものと考えている。一方で IP 化の場合には放送事業者が隔離して使うと言っても、通信方式が IP となった場合には外部ネットワークと接続されたことを前提とした対策が必要ということで、様々なセキュリティ強化の策を検討してきた。パッチについては小山構成員から貴重な御助言をいただいたので、放送設備自体の堅牢化という点について、今後の検討において参考とさせていただきたい。

◆議題（1）「放送分野におけるサイバーセキュリティ対策の取組ついて」、日本ケーブルラボ　取屋氏より資料２－3 を説明。

◆構成員の意見・コメント
吉岡構成員）

11 枚目のスライドで、守備範囲と書かれているが、ケーブル事業者の守備範囲はこの図のどこまでが対象となるのか確認させていただきたい。

日本ケーブルラボ　取屋氏）

この図の中で示している部分全体としての守備範囲と考えているが、特に調査報告書の内容の中で触れたかったことは、現在ほどリモートワークやクラウドの活用が進む前は、社内情報システムとケーブルテレビシステムが業界内で守られていた中で情報の資産が扱われていたことから、境界だけある程度守っていれば大丈夫という考え方が主流であったが、残念ながら現在は境界の外に情報の資産が持ち出され保管されている状況が発生しているという現状である。最終的に本当に守らなければいけない本丸は社内情報システムにある各種データベースや機関システム、ケーブルテレビシステムの中にある放送や通信の送出設備だが、そこに至るエンドポイントや攻撃の対象となるポイントがリモートワークで持ち出されている端末やサプライチェーンのパートナーと接続しているシステム、接続の VPN など、そういった領域にまで広がっている。今までの考え方だけでは収まらなくなっていることをこの資料で説明していた。

吉岡構成員）

同じ図の右側に FTTH など末端の顧客側の絵も記載されているが、そのあたりも含めて監視や防御の対象になるのか。

日本ケーブルラボ　取屋氏）

実際のお客様の宅内の端末の部分に関しては、各事業者において監視している状況や対策している状況が少し異なってくるが、お客様の宅内の端末が何らかの侵害で攻撃の起点になってしまうことも十分あり得る話であり、ラボとしては宅内の端末のセキュリティを保っていくことも重要なポイントと考えている。今回はケーブルセキュリティ調査報告書の内容の御紹介をさせていただいたが、一方で宅内 IoT 機器に関してのセキュリティのガイドラインも出して、その中で機器を設置する時には初期パスワードを変えていくなどの最低限のセキュリティを確保するといった内容に関して報告しており、執筆中のセキュリティガイドライン（技術者編）の中ではその部分も少し触れていこうかと考えている。

蔦構成員）

IT 関係と OT 関係に関する取組が重なるところについて、10 ページの被害事例を見ていると、専ら IT 関係の

事例と見えるが、OT 関係についてはこういった被害事例は発生していないのか。もしそうなのであれば、今後 OT 周りの脅威としてどのようなものがありうるかお伺いしたい。また、14 ページに挙げていただいたセキュリティガイドラインは IT 関係を対象にしているのか、OT 関係も対象にしているのか、先ほどあった宅内の機器も対象にしているのかもお伺いできればと思う。

日本ケーブルラボ　取屋氏）

まず 10 ページについて、直近に発生した事例を特に取り上げていることから、やはり IT 系の部分の被害事例に寄っているが、OT 系でも実際の事例はあったと認識しており、具体事例として、放送設備のメンテナンスのために事業者が持ち込んだ USB ディスクが感染していて、中に入っていたものはパッチが当たっていなかったことから、それが感染して復旧対応が発生したという事例がケーブル事業者の中で発生しており、過去のワークショップの中でも事業者様からも報告いただいている。IT 系と OT 系の中に結節点にファイヤーウォールを置いているが、いくら隔離しているといっても 100%スタンドアローンになっているわけではない。どこかのタイミングで外部のものが入りこんできてしまうことがあることはきちんと伝えていかなければならないと考えており、様々なところでその点について触れている。セキュリティ調査報告書の中でもその点をしっかりと守っていくことがポイントと記載されている。14 ページのガイドラインでは、IT 系だけではなくて OT 系もしっかり守っていくことが、ケーブルテレビ事業者がやっていかなければならないセキュリティ対策としており、OT 系の部分に関しても範疇としている。また、宅内端末のセキュリティをきちんと保っていくことも最終的にはケーブルテレビサービス全体でのセキュリティを守っていくことになるということに関しても記載に触れていく予定である。

後藤主査）

ケーブルラボが普及活動に努めているが非常に分かり、放送局の方にも参考になると思われることが多くあった。

（3）閉会

以上