サイバーセキュリティタスクフォース
情報通信ネットワークにおけるサイバーセキュリティ対策分科会（第３回）議事要旨

1. 日 時）令和５年３月 16 日（木）10：00～12：00

2. 場 所）総務省 第１特別会議室(８F)及びオンライン

3. 出席者）

【構成員】
後藤主査、井上構成員、河村構成員、小塚構成員、小山構成員、田中構成員、藤本構成員、吉岡構成員、吉川氏（齋藤構成員代理）

【オブザーバー】
内閣サイバーセキュリティセンター、経済産業省

【総務省】
山内サイバーセキュリティ統括官、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、廣瀬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

【発表者】
岡田猛史（射水ケーブルネットワーク株式会社）、伊東健太郎（INC 長野ケーブルテレビ）、立石聡明（一般社団法人日本インターネットプロバイダー協会）、加藤雅人（一般社団法人デジタルライフ推進協会）、梶俊明（ヤマハ株式会社）、萩原雄一（株式会社ゼロゼロワン）

4. 配付資料

資料３－１	国内の IoT 機器が踏み台となった最近のサイバー攻撃事案について（非公開資料）
資料３－２－１	サイバーセキュリティ対策への取組み（射水ケーブルネットワーク）
資料３－２－２	サイバーセキュリティ対策への取組みについて（INC 長野ケーブルテレビ）
資料３－２－３	地域 ISP のサイバーセキュリティ対策の現状と課題（JAIPA）
資料３－３－１	DLPA におけるサイバーセキュリティ対策に向けた活動紹介（DLPA）
資料３－３－２	ヤマハにおけるセキュリティ対策の取り組みについて（ヤマハ）
資料３－３－３	Karma に見る IoT 機器の現状（ゼロゼロワン）
参考資料	情報通信ネットワークにおけるサイバーセキュリティ対策分科会（第２回）議事要旨

5. 議事概要
（1）開会

（2）説明
◆議題（１）「国内の IoT 機器が踏み台となった最近のサイバー攻撃事案について」について、事務局より資料３－１を説明。

◆構成員の意見・コメント
吉岡構成員）

資料３－１にあるような事例をお聞きして、ルータだけではなく、その先にある内部の別の機器に感染が拡大したローカルエリアネットワークも攻撃に曝されていると思った。技術的にはローカルネットワークにも攻撃を行うことは可能だとは思っていたのだが、それほど多いと考えていなかった。また内部の機器を狙うときに特定の脆弱性を狙ったということだが、Mirai のようなマルウェアが自律的に感染を広げる一環で行われたのか、ある程度機器や内部の脆弱性を狙って固定のポイントで行われたのか、攻撃側がどれくらい意図して攻撃を行ったのかが少し気になったため、もし情報があれば教えていただきたい。加えて外部に向けて攻撃を行ったのは DoS 攻撃かと勝手に想像しているが、複数台感染したとしても上流の回線は一つだと思われるところ、あまりこういった攻撃手法は意味がないとも思っているが、複数機器を感染させることで、アップリンクスキルぎりぎりまで帯域を使って攻撃ができるなど、どのような技術的な意味があってこのような攻撃をしているかも気になったので、もしご見解があればお伺いしたい。

河村構成員）

今回の場合、システムメンテナンス用に開かれて、アクセス制限の設定が適切にされていなかったルータのポートから侵入と書いてあるが、これはたとえその下の個々のアクセスポイントの脆弱性があったとしても、ルータの設定が適切になされていれば防げたと考えられるということで、これからの再発防止についてお教えいただきたい。

佐藤企画官）

まず吉岡構成員からのご質問については、実際に事業者の方にもヒアリングをしてみたが、攻撃元については C&C サーバも含めて中々特定ができていないようであり、データを分析すれば分かるかもしれないが、攻撃者がどのような意図でこのような攻撃を行ったのかについては分析がそこまでできていないと聞いている。次に河村構成員からのご質問については、再発防止という意味では、ご指摘の通り仮にアクセスポイントに脆弱性があっても、ルータで適切にアクセス管理を行うか、さらにはルータの手前に例えばもう一つゲートウェイを設置するなど、マルウェアが入ってこないように適切に対応を行っていれば防げたということで、当該事業者においても、ルータの手前に機器を設置するといった対応も現に行っているという話も聞いている。

後藤主査）

詳細はまだ分からないところも多いので、今後情報があったところでまたご報告いただければと思うが、全体としてはアウトバウンドの問題が引き起こした例として捉え、今後の対策の議論の一例として参考にしていきたい。

◆議題（２）「地域 ISP 等によるサイバーセキュリティ対策の取組状況と課題について」について、射水ケーブルネットワーク岡田氏より資料３－２－１、INC 長野ケーブルテレビ伊東氏より資料３－２－２、JAIPA 立石氏より資料３－２－３を説明。

◆構成員の意見・コメント
井上構成員）

まずは資料３－２－１へのコメントだが、情報としてこういう一定年数経過した機器や高リスク端末の情報があると良いと思う。今のところ NOTICE からの注意喚起を受けていないということで非常にセキュアな状況が保たれていると思うが、万一 NOTICE から注意喚起が出された場合は、どのベンダーのどの機種のものかまで特

定できた機器が注意喚起対象になり、注意喚起を受け取った場合には同時に通知される具体的な機器の型番等の情報から、発売からの経過年数や過去の脆弱性情報等も辿れるためご参考にしていただきたい。次に資料３－２－２へのコメントだが、ユーザー宅の機器の脆弱性に関する情報がユーザサポートにおいて有用ということは非常に参考になった。以前本分科会でも発表したが、NOTICE の調査の付帯業務として、弱い ID とパスワードにも、付帯業務として可能な範囲で脆弱性情報も集めているので、その活用の一環として検討させていただきたい。

小山構成員）

資料３－２－２－の発表の中に、防犯カメラが攻撃の踏み台になっていたことに気づいた後から、手間をいとわず現場対応をされて素晴らしいです。私は通信事業者と ICT-ISAC の立場の両方で IoT のセキュリティ対策に課題を感じている。その中で、今日の冒頭の事務局からの説明と資料３－２－２のご発表について、監視カメラのような機器などが踏み台になっている件は、日本以外の地域でも同時に同じような攻撃が行われている可能性があるため、今後はメーカーとも連携した対策を行っていく必要があり、例えばポートスキャンをした時に判明する特徴のあるバナーや特定の C&C サーバと通信している他の監視カメラといった存在に絞り込んだ上で対策を打っていくべき。メーカーと連携して対策を打ち、通信事業者がフロー情報を確認する形で効果を確認していくことが出来れば、JAIPA の立石氏もおっしゃっていたような HEMS や火事・物損・人命というようなところにまで影響が及ぶ可能性がある IoT を確実に無くしていくことが出来る可能性がある。

後藤主査）

立石氏にお伺いしたい。今回事業者アンケートを取っていただいたが、非常に価値が高く分析の余地があると思われ、この元データを公開いただけると嬉しい。特に NOTICE の参加割合について参加 ISP の数からユーザー数を換算する等非常に重要なデータとなると思う。

JAIPA 立石氏）

公開は難しいかもしれないが、構成員限りで可能かどうかなど確認する。

◆議題（３）「メーカー等によるサイバーセキュリティ対策の取組状況と課題について」について、DLPA 加藤氏より資料３－３－１、ヤマハ梶氏より資料３－３－２、ゼロゼロワン萩原氏より資料３－３－３を説明。

◆構成員の意見・コメント
小山構成員）

資料３－３－１のご説明の中で、法人ルータは今日の説明の対象外ということで、ひょっとしたらその部分に該当するかもしれないが、ルータ等の IoT 機器にマルウェアが侵入することの１つのトリガーとして、遠隔保守のあえてポートを開けることやウェブ画面を見えるようにすることが考えられる。または防犯カメラなど、リモートからアクセスする必要性がある際にどういった対策が必要なのかを周知しなければならない。もし DLPA でリモート保守やリモートでアクセスの際の機器設定上の注意点などを公開・啓発を行っているなどあれば教えていただきたい。また、そのような活動の中での課題として、ヤマハ梶氏からの発表にもあった、法人向けルータは責任の所在が曖昧という点に関し、ご意見や現場の課題といった感じのところがあれば教えていただきたい。

田中構成員）

資料３－３－２の 11 ページ、デフォルトパスワードの廃止に関してはユーザーあるいは SIer にパスワードの変更を求めているということと理解。資料３－３－１スライド 6 では、DLPA 推奨ルータはウェブ設定ログイン

ID・パスワードが個体ごとに異なり変更不可であり、提供時に強固なID・パスワードを設定することでSIer含め利用者側ではそれらを変更することを想定していないとの認識だが、その点個人利用者と法人利用者とで考え方の違いはあるか補足いただきたい。

吉川氏）

１点目にDLPA加藤氏への質問だが、資料３－３－１最終ページについて、バッファローではファームウェアの修正ができない古い製品については利用者へ利用停止の案内を行ったとのこと、案内の結果どういう効果があったのか教えていただきたい。２点目に資料３－３－２ヤマハの梶氏への質問として、10スライド目にあるインプット・アウトプットについて、脆弱性と紐付いている機器については優先して対応をいただけると理解したが、脆弱性として特定される前の、IoTボットネットの不審な動きや流行しているマルウェアの情報等の曖昧な情報が共有された際にはどういった対応をするのか。ISPの立場からすると、脆弱性情報と紐付かない事象としてそのような曖昧な情報が先に共有されるため、同様の情報がメーカーにも共有された際の対応を伺いたい主旨。

井上構成員）

１点目に資料３－３－１DLPA様へのコメントと質問で、DLPAの推奨ルータがNOTICEでこれまで検出されていないことは非常に素晴らしい結果であり、セキュリティの視点でDLPAや各社からさらにこの点アピールしていただければ心強い。また、NOTICEの取組は、現在は実際に調査をしているNICTとISPと総務省の枠組みでの活動となっているが、今後は機器を実際に製造しているメーカーの皆さまも含めた一体的なこの活動となることを希望している。質問としてはDLPAの推奨のWi-Fiルータのリストは公開されているかを教えていただきたい。２点目に資料３－３－２ヤマハ様へのコメントだが、NOTICEからの指摘を受けセキュリティ機能を実装した点非常に素晴らしい取組であり、NOTICE業務を行っている側からすると非常にやって良かったと感じる。コメントだが、セキュリティ改善が製品の付加価値となるようなマーケットが形成され、セキュリティが高い製品がある程度値段が高くてもきちんと売れるような形になっていければと思っている。繰り返しになるが、機器メーカーも含めた次期の体制を検討していきたい。

吉岡構成員）

ISP、機器メーカーまたは攻撃を観測している関係者からの話を聞き、それぞれが独立して行うのではなく連携が大事であることを改めて感じ、特に機器メーカーについては、ルータが第１の攻撃対象になっている事情がある中で、業界の連携が進んでいることが明確に分かって大変素晴らしいと思った。一方で、冒頭事務局からLAN内の機器への攻撃事例の説明や、ルータそのものではなくそこに無線接続されていたカメラへの攻撃またはその乗っ取られたカメラからの外部への攻撃事例の説明があったものと理解しているが、ルータではなくその先の機器も攻撃される事例が発生している点、今後そのような機器にも対策を広げていく必要があると思う。ルータ等のメーカーは既に様々な活動や連携をしていてモデルケースになっていると思うので、対策の活動が広がっていけばよいと思った。

DLPA加藤氏）

小山構成員からのリモート保守やリモートでアクセスの際の機器設定上の注意点に関するご質問については、DLPAとしては個人向けルータを主としているため、リモート保守の形態は、現在はDLPA4社とも取っていない。一部の法人向けルータや、個人向け法人向け双方に近いようなルータに関しても、メーカーが保守を行うかということについてもあまり聞いておらず、ISPや導入する機器を設置・設定する企業側でリモート保守をして

いる場合が多いように認識している。田中構成員からの DLPA 推奨ルータにおける個体ごとに異なる ID・パスワードの考え方に関するご質問について、個体ごとに異なる ID・パスワードが設定されていることは申し上げたとおりだが、利用者が意図的にそれを変更することを禁止しているわけではない。利用者が変更するということはきちんとパスワードを認識して変更しているので、それを阻害するような仕様にはしていないということは訂正したい。ご質問の個人利用者に関する考え方としては、個人向けルータについては、ルータやネットワークについて詳しくない利用者も安心安全に使用できる点を重視した ID・パスワードの設定・設置・考え方をしている。吉川様の古い製品の利用停止の利用者への案内に関するご質問については、ファームウェアアップデート対応が困難になった成否についてはその旨をサイトで公表しているが、DLPA として現時点ではその案内の効果のとりまとめは行っていない。実際の効果検証は難しいと考えられるが、その点上手く関係者が連携してできるような仕掛けも考えていく必要があると思う。井上構成員からの DLPA 推奨 Wi-Fi ルータリストの公開に関するご質問については、今後販売するすべての機器に対してセキュリティ要件を適用するのがメーカーとしての責任であるという観点から、2019 年 12 月以降に DLPA4 社から提供しているルータはすべて DLPA 推奨ルータになっている。加えて井上構成員からは次期 NOTICE の活動はメーカーも連携して取り組むべきとご発言があったが、メーカーとしても責任のある対応を取っていきたいと思っているため引き続き協力していきたい。吉岡構成員のコメントに関しても、宅内の機器が感染し、カメラ、スマートフォンや PC など、フィッシング等から何か感染が広がる可能性があることをメーカーとしても懸念している。現時点では具体的事例をわれわれ自身もキャプチャできている訳ではないが、今後どういう対応をするべきかを引き続き検討し実行に移していきたい。

ヤマハ梶氏）

田中構成員からのログイン ID・パスワードの仕様に関するご質問について、業務用の機器ルータでは SIer がそれらを設定する関係で、一度に数台から数十台ほどの機器を扱うため、手作業で直接入力するのではなく設定ツール・設定機器から設定を流し込む形になる。このため DLPA 様が提唱されているように、最初から機器ごとに個別の設定することで一つ手間が発生してしまうので、どうしてもヤマハからの出荷時には共通のパスワードを設定することになる。この共通のパスワードをそのまま使われてしまうと NOTICE 注意喚起対象になってしまっている。このため、使用開始時には ID・パスワード設定を変更しないとネットワークに接続できないように変更した。その結果、必ずパスワードを変更してからネットワークにつながることになり、セキュリティの向上につながると考えている。吉川様からの脆弱性以前の情報共有下でのヤマハの対応に関する質問について、弊社は脆弱性もファームウェア不具合の一つと考えている。利用者から情報共有を受けた際、何かおかしな動作をした部分とセキュリティの問題とを紐付けて調査を進めていくところが第一歩になるかと思う。ヤマハでは新しいファームウェアを公開する度に 100 個ほど不具合を修正している。誰かに脆弱性と指摘されていなくても実質脆弱性に該当する不具合もたくさん含まれている。報告されている情報の中から、セキュリティに関わる不具合を判断し優先して対応しているというのが実情です。井上構成員からの次期 NOTICE への取り組みについてはメーカーとして参加すべきと考えている。

河村構成員）

資料３－３－１の DLPA の発表に関し、DLPA 推奨 Wi-Fi ルータの仕様はとても良いと思う。質問だが、10 ページに保証期間が 1 年と書いてあるが、DLPA のメーカーはそれぞれファームウェアの自動更新に対応しているとのことだが、それはこの 1 年間だけかそれとも何年間も自動更新が行われるか教えていただきたい。

DLPA 加藤氏）

ファームウェアの自動更新に関しては、申し上げた通り 2019 年 12 月以降の DLPA4 社の製品であれば商品の機

能として自動更新という機能が付いているので、1 年間だけの自動更新というよりも、その商品が今後販売され続ける限り、またメーカーが対応可能なファームウェア更新を続けられる限り、その機能は有効である。

河村構成員）

大変安心した。というのも、私はファームウェアの更新を自分でしたことが一度もないが不具合などは起こったことがなく、更新を促すお知らせも見たことが今までないため、メーカー品だったからなのかと思う。そうすると 10 ページ 1 行目から書いてある 1 年から後のダウンロード提供というのは、自動更新であるとするなら何のことを指しているのか。

DLPA 加藤氏）

製品に瑕疵がある場合にそれを公開したり保守対応したりという意味では、本当に古い機種まで壊れたから交換や保証してくれと言われてもメーカーとしては難しい部分があるので、一般的に保証期間というのは 1 年となっている。しかし、脆弱性は特に特別扱いをしており、古い機器の脆弱性もこのように対応しているというところを意図して記載している。

河村構成員）

資料３－３－２のヤマハの資料について、19 ページに様々提言があるが、知識・手段・動機・コストの改善という点、動機の部分に記載がある強力な法規制に関しては、私も何らかのルール明記が必要だと思っている立場なのだが、どのようなルールを現時点で想定してこの言葉を書かれたのか。どのような法規制、何に向かって何を規制するかということの想定があれば現時点でのイメージで結構なので教えていただきたい。

吉岡構成員）

河村構成員からのご質問でもあった通り、いつまでファームウェアアップデートという面倒を見てもらえるのかというところがユーザーとしてはかなり気になるところかと思うので、EOS の観点が非常に重要だと思っている。利用者側からすると、いつまで更新が続くということが明示されている、または自分が使っている機器がすでに更新の対象ではないということが明示されていることがありがたいと思う一方で、機器メーカーの立場からすると、決定や公開・周知する方法というのは十分な検討が必要であると認識している。少なくとも一つ言えることは、情報を発信していく時に、そもそもルータのような機器にはセキュリティ寿命といった考え方があって、あまりにも古いものを使っていること自体にはある程度ユーザー側にも責任があるというか、それを選んでいかなければいけないという認識が醸成された上で併せて進んでいくものなのかと感じた。

ヤマハ梶氏）

河村構成員の質問について、一つは現行では JATE（電気通信端末機器審査協会）でセキュリティ規制がある。元々はアメリカのカリフォルニア州の IoT 機器に関するセキュリティ規制を参考にしたものかと思う。これによりインターネットにつながる新しい製品は JATE 認証を取得することで、セキュリティ規制が適用されるが、すでに発売済みのものは対象となっていない。一方で、今イギリスで制定されようとしているサイバーセキュリティ法規制では、新製品だけではなく、ある期日以降に発売するすべての製品が対象となる。日本でも同様に新製品だけではなく、既存製品も含めて規制が必要かと思われる。また、これらはすべてメーカー側への規制となるが、利用者側ないしは設置・管理者側に対しても何らかの規制が必要ではないかと思う。また、通信の安全保証のために妨害・傍受が規制されているが、調査目的ではもう少し踏み込んで通信の内容を調べることができるような法改正があると良いかと思われる。

小山構成員）

今回の説明を受け個人向けルータなどはしっかり対策されているが、法人に提供あるいは法人が利用する際にリスクが高まるというような認識を持ったので、どのように対策を進めたらいいかというメーカーの立場や団体の立場、あるいはゼロゼロワン様の立場でご意見いただきたい。

田中構成員）

DLPA 様の資料の中でも、個人使用と業務使用の 2 つの軸で責任の所在を整理されていた表があったと思うが、NOTICE の活動の中では注意喚起対象が個人ではなく中小の法人である案件が多いところもあり、表で言えば中間になるのかもしれないが、そういった中小企業、特に最初にネットワーク構築をした時と担当が変わってしまいルータの存在を失念しているといったことが個人よりも起きやすい部分があるかと思う。こういった部分のをフォローしていくというのが今後の課題になるかというのを感じた。

ゼロゼロワン萩原氏）

ご質問にあった法人向けルータに対するリスクが高まる点については、大企業は基本的に SIer など機器導入をしっかり行っている印象が強く、中小の会社であまり IT のシステム屋といわれる人たちがいない企業や、とりあえず機器を導入して動けば大丈夫だという形になっている企業に古い機器が多く残っていくケースがあると思っている。対処すべきこととしては、機器導入時に担当の方にきちんと説明する、サポート期間を追っていくことが大事なのではないかと思っている。一部のレンタルルータ等に対しては製品のサポート終了通知を ISP が行っていることは聞いているが、似たようなことを SIer も行っていかないといけない。一方で SIer はいろいろな製品を抱えているため、情報をメーカーから下ろすなどの仕組みを共同で作っていく必要があるのではないかとも思っている。ヤマハさんの方の説明であったが、特に企業では責任者が誰なのか曖昧というようなご指摘もあり、その定義付けや機器導入のフレームワークを行政がチェックシートのような形で出せると良いのではないかと思っている。

ヤマハ梶氏）

法人使用の場合は責任の所在が曖昧になりやすい。何らかの強い前例があれば、それに従って責任の所在を注意喚起するような案内ができると思う。一方で、自由度とセキュリティ度合がどうしてもトレードオフになる。多少使いにくくなったとしてもセキュリティ向上を意識して製造することがメーカーとしての責任かと思った。田中構成員からのコメントにあった、個人と企業との区分の中間の部分は、仰るとおり、SIer がいなくて中小企業が自ら設置して使用している場合もたくさんあると思う。そこも含めて何かあったときに誰が責任を取ることになるかという明確な指針があると、その責任者に対してメーカーからもアプローチしやすくなり、かつ対応していただくための動機になるのではないかと思う。

DLPA 加藤氏）

吉岡構成員がおっしゃったセキュリティ製品の寿命の件は、個人向け・法人向けどちらもある話だと思っており、これをいかに利用者に伝えていく必要があるのかについては、メーカーとしても DLPA としても非常に喫緊の課題だと思っているが協会として各メーカーの意思統一というのが難しい部分もある。対応を断念せざるをえなかった機器に関しては DLPA4 社それぞれ持っているので、これが個人向けであり法人双方向けそれぞれのもの

について、どこにその情報をまとめて提供し、それがどう SIer や企業で導入される方に情報を回していくかというフローを作っていかなければならないと思った。

JAIPA 立石氏）

中小企業の話があったが、私の問題意識としては、大手の企業でも、大手 SIer でも、地方にリテラシーが高い人が少ないということが非常に問題かと思っているので、大手に任せたから大丈夫かというと、実はそうではないという現実が地方にあるということをご理解いただけたらと思う。

射水ケーブルネットワーク岡田氏）

立石さんのお話にもあったように、当社としても地方のケーブル局として対応しており、社内ではどうしても技術力が足りないところもあって、アウトソーシングしている部分もあることも申し上げた。アウトソーシングしている会社自体も技術者がだんだん不足してきているという所も結構あるようで、その対応のため県内のケーブル局等で連携を取りながら技術陣の構築を目指す話もしているような現状であるが、全体的に技術員が少ない点は課題としてある。

INC 長野ケーブルテレビ伊東氏）

弊社では新しいルータはファームアップを自動で適用しているということについても訪問して実際に確認しているので、大変ありがたい取り組みだと思っている。ルータ以外にも、このような機能が載ってくると、こちらとしても効果的な対応と思っているので、例えばウェブカメラといった他の機器にもこのような動きが広がっていくといいと思う。

藤本構成員）※会議後コメント
JAIPA 様のプレゼンにもあったが、地方のセキュリティ人材不足の状況が気になった。サイバーセキュリティタスクフォース親会のテーマでもあるかと思うが、自社人材を育成しようとしても教育機会の提供が不足しているのか、外部から専門人材を雇用しようとしていてもリクルーティングが難しいのか、何か他の理由があるのかなど、もう少し現場でどのようなことが起きているのか知りたいと思った。

（3）閉会

以上