ICT サイバーセキュリティ政策分科会（第７回）議事要旨

１．日　時）令和６年５月 10 日（金）13：00～15：00

２．場　所）WEB 開催

３．出席者）
【構成員】
後藤主査、新井構成員、上原構成員、栗原構成員、小山構成員、辻構成員、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整備準備室、デジタル庁、経済産業省、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（統括担当）、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

【発表者】
衛藤将史（国立研究開発法人情報通信研究機構（NICT））、須藤年章（NTT コミュニケーションズ株式会社）

４．配布資料
資料７－１　IoT 機器へのサイバー攻撃の観測と対策について（吉岡構成員）（一部非公開資料）
資料７－２　NOTICE の活動について（事務局）
資料７－３　新しい NOTICE における調査業務（NICT）（一部非公開資料）
資料７－４　電気通信事業者によるサイバー攻撃への効果的な対処を通じた安心・安全な情報通信ネットワークの実現に向けて（NTT コミュニケーションズ）

5. 議事概要
（１）開会

（２）議題
◆議題「通信分野におけるサイバーセキュリティ対策の取組について」、吉岡構成員より資料７－１、事務局より資料７－２を説明。NICT 衛藤氏より資料７－３を説明。

◆構成員の意見・コメント

辻構成員）

IoT 機器制御の奪い合いに参加してクリーンな状態に持って行くことはどの程度可能か。支配的な立場になることはかなりハードルが高いものなのか。

新井構成員）

ボットネット同士の攻防が IoT 機器の中でも確認できるという観測結果について、Telnet を止めれば Notice の観測結果に影響を与えることができるとの示唆があったが、一方、かつて Windows を狙うボットネットにて修正プログラムを適用し他のボットネットが同じ脆弱性を攻撃されることを妨げ、独占的に感染 PC を悪用するといった動きもあった。Telnet 停止以外にも特定のボットネットが独占的に感染 IoT 機器を悪用するための仕組みが他にもあれば詳しくお伺いし、NOTICE の観測結果を左右するような要因が他にもあれば確認したい。

蔦構成員）

クラウドボットネットについてクラウドサービスプロバイダーに通報等して止めることはできないのか。そもそもそれが現実的ではないなら、その旨教えていただきたい。

盛合構成員）

IoT 機器のセキュリティ対策について、ユーザーだけでなく IoT 機器メーカーや ISP/NW 事業者の対応も重要と考えている。今回クラウドボットネット事例で AWS に何らかの対策をしてもらえれば防げるものか。

小山構成員）

FOFA の性能が良い理由として考えられることがあれば教えていただきたい。また、信頼のおけるスキャナーを日本でも運用すべきと考えているが、御意見をお願いしたい。

上原構成員）

IoT 機器でも特に従来ネット接続しなかったものが後に接続するようになったものについては通信モジュールを自社開発していない例が少なくないように思う。その場合メーカーも通信モジュールの仕様を正しく理解しておらず、そもそもポートが何のために空いているのか分かっていない可能性があると思う

辻構成員）

昨今販売されているデバイスにてデフォルトパスワードのものはまだまだあるのか。
事実があればNOTICEのような注意喚起も行い、同時にNCSCが行ったような取り組みも必要になると考える。
（https://www.ncsc.gov.uk/blog-post/smart-devices-law）

上原構成員）

IoT 機器で攻撃が行われているものの多くがルーターであるということから、ISP の関わりが重要になると思う。例えばルーターのレンタル化を推進（特に家庭向き）してルーターの管理ごと ISP 側にお願いするという方法が考えられそうである。

吉岡構成員）

辻構成員への回答。機器の権限を奪い返すことについて、誰がどのような立場で実施するかの整理はあるが、技術的には非常に興味を持っている。現在この攻防は完全ではなく隙があり本気になれば奪い返せる目途が少し見えている。ハニーポット内で疑似戦を行い本当に奪い返せるか、権限を維持できるかを実験することができるので興味深く考えている。

新井構成員への回答。Telnet 以外でも機器を独占するような動きは見えており、典型的には WebUI からの攻撃はよくあり、例えばWebUIの待受ポートを変更すると他の攻撃者は入れなくなり自分だけアクセスできること、IP アドレスが変更されても追随できるようダイナミック DNS をセットしておくなど、明らかにその機器を自分が占有したいという意図が見える攻撃は他にもあると考えている。

蔦構成員、盛合構成員への回答。クラウドサービスプロバイダーへの通報は大いにあり得る。既にある程度実施してアビューズ対応している上で今の結果になっていると見ている。AWS 上のホスト数の全体を考えると少なく、かなりの対策を行った上で残ってしまっていると見るべきと思っている。一方で、それほどの規模感でないのに沢山いるプロバイダーは海外に存在するが対策が甘いかもしれない。また、防弾ホスティングの様に不正な活動を確信犯的に許容しているという可能性もあるかもしれないと考えている。

小山構成員への回答。FOFA は検知数が大きく違い驚いたが、重複している可能性も考え精査する必要がある。少なくとも Shodan や Censys は全世界向けのサービスで日本国内の機器に特化しているとは思えない。シグネチャーの作りなどが弱い気がするので、国内の機器を把握できるスキャナー等の仕組みはリスクを把握する上で非常に重要だと考えている。

上原構成員への回答。全く同感である。メーカーは全て自分たちで製作している訳ではないため、サプライチェーンの複雑化が明らかに問題である。実際、問題を指摘してもアウトソースしている等の話も多く、組込み機器の場合は、BSP で開発している側がパッケージ内容全てを把握していないことも関係していると思う。

辻構成員への回答。最近の機器について、国内の家庭用ルーターのパスワードは個体ごとに異なりしっかりと対応されている。またファームウェア更新も自動でオンとなっており、最近の脆弱性は攻撃を受けても収束が比較的早い印象を持っている。

蔦構成員）

NOTICE は流通後の製品についての対策で、これから発売する製品についての対策としては、平成 30 年に端末設備等規則にサイバーセキュリティに関する技術基準が追加されたと認識している。追加から数年経過した現在、どのような運用状況となっているのか、この技術基準が対策として十分か、もしくは何らかの課題・改善点はあるのかなどについて説明いただきたい。

栗原構成員）

機器のサポートはどこかで切れてしまうので、買い替えを促していかなければならない。この辺りについては何か施策等はあるか。

上原構成員）

レンタル型について、家庭向けの話だがルーターに脆弱性があった場合誰がどうやって責任を取るかという点について、一般家庭へ義務を負わせることは無理があるため、ISP へ責任を課す方向に促せる何かがあったほうが良いのでは。
また、新 NOTICE にベンダーが参加する場合、ベンダーのみが保有している情報と ISP が保有している情報を繋ぐ役割が新 NOTICE にあると考える。エンドオブライフを迎えてしまった機器に対し、本来ベンダーは買い替えを促したいが、ユーザー登録がされていない場合は伝えることができない。しかし、自動アップデート機能等で IP アドレスが分かる状況があり、その場合 NOTICE の枠組みを使用して知らせることが可能だと考えられないか、法的な整理は少し必要であるが、御意見をいただきたい。

小山構成員）

流量計の設置業者が判明し対策が進んだことについて、従来から特に法人設置の IoT 機器への対策が進まない課題は､ISP を通した回線契約者への注意喚起だけではリーチできないことの裏返しと考えていた｡新しいNOTICEを進めるにあたり、ベンダーや設置業者との関係性が構築できたところから順番に対策を強化していくといった優先順位も考えられるので御意見を伺いたい。

酒井参事官）

蔦構成員への回答。端末設備規則との関わりについて、規則改正後、ルーターの管理機能は、①アクセス制御機能を付けパスワードの変更を促すようにする、②ファームウェアのアップデートができるようにしておく、この 2 つが要件に入るが、本要件は機器製造時の責任として課すものではなく、ISP の設備に接続する際の要件となり、かつ接続時にこれを満たすこととなっている。規則が 100%守られるとしても、その後ユーザーが適切に管理する保証はない状況である。端末設備規則を満たした機器を接続してもらい、それ以外の機器が接続されないようにする努力により、脆弱な IoT 機器が一定数減ることを期待することに加えて、引き続きユーザーの適切な管理を求めていく必要があると考える。

栗原構成員への回答。昔は特に大量に流通している機器のエンドオブライフはアナウンスされず、メーカーのエンジニアが可能な限りサポートすることがユーザーサービスとの認識で取組んでいたが、昨今はサポート終了をお伝えすることで､「ユーザー側が適切なセキュリティ対策を選択できるようにする」ことがユーザーにとって良いサービスだという意識が徐々に広がってきている。一方、ユーザー側は、自分の使っている機器がエンドオブライフに達しているかを簡単に判断できる状況ではないので、今後は NOTICE の HP などを活用し、エンドオブライフ、エンドオブサービスを迎えた機器に対しての対処方法などを伝えていければと考えている。また、メーカーがエンドオブライフはサービス低下と考えてユーザーに対して伝えることを躊躇すると伺うが、NOTICE の HP で「適切なセキュリティ対策とは時には古い機器の買い替えも含む」と明確に記載し、案内を伝えやすくなるように期待している。

上原構成員への回答。ISP ルーターレンタルの推奨による問題の解決について、そのとおりであると考える。大手プロバイダーがレンタルで提供している機器は、大部分で遠隔管理が可能であり、ユーザー側も楽である。また、ISP 側で新たな脆弱性が発見された場合、遠隔で全て対処ができるという点でも有効であるため、当該ルーターの安全性及び推奨を伝えていくべきであると考えている。一方、ユーザー側での設定変更は禁止していない会社もあり、自ら設定を変更される方もいるため、こうしたユーザーへのセキュリティ対策の情報提供も重要であると考える。
ベンダーとの情報共有により新しい注意喚起が行える件について、現在はベンダーとコミュニケーションを開始していく段階である。メーカーから ISP への情報提供により、IP アドレスから ISP を使用しユーザーを特定できる可能性があるが、現行の制度運用上は違法性阻却が可能な場合にのみ ISP によるユーザー特定が許可されているので、今後はリスクなども考慮し引き続き評価をしていきたい。

小山構成員への回答。御指摘の通り、ISP の皆さまには協力をいただいているところだが、必ずしも全ての方に注意喚起が届くわけではないことを踏まえ、ひたすら注意喚起をするというだけではなく、SI やベンダーを通じて、より効果的で直接的な対処も考えている。現時点で具体的には進んでいないが、今後ご指摘いただいたことを念頭にメーカー、SI、その他メーカー系業界団体との意見交換を続けていきたい。

NICT　衛藤氏）

新井構成員への回答。国内の一般企業や病院、港湾施設などに置かれている VPN 装置への対策も必要という指摘は全くその通りである。ベンダー、設置業者に限らず、港湾や病院をはじめとする重要インフラにも直接リーチし、結果として対策が進み、通信インフラのセキュリティ向上に寄与することは NOTICE の目的に資する活動だと考える。そういった方向性で積極的に取組んでいきたい。

小山構成員への回答。フロー活用による通信フロー分析により侵害されている機器を確認していく点に関して、現状総務省において委託事業の中で通信フロー分析の調査事業というのをやってきたが、そのような結果等を参考に通信フローの活用は積極的に取組みたいと考えている。また、通信フローに限らず外部の様々なセキュリティサービスを積極的に活用し、NCO 調査能力の向上に取組んでいきたい。

上原構成員）

NOTICE の日本での役割の大きさについて、不正アクセス禁止法の中で民間サービスが Shodan の様なものを持つことが難しく、責任ある体制で行える点で、責任ある特定アクセスを行うことが出来る組織 NICT とそのサービスである NOTICE がその代わりになり、セキュリティ上も安全保障上も重要なサービスであると認識しており、今後に期待している。

◆議題「通信分野におけるサイバーセキュリティ対策の取組について」、NTT コミュニケーションズ株式会社須藤氏より資料７－４を説明。

◆構成員の意見・コメント

新井構成員）

通信インフラの健全性を維持するために C２などのサイバー犯罪者のインフラを把握することも非常に重要だと考える。その上で C2 のような特に大きいボットネットになると、多層構造を持っており、C2 の生存期間は１日が非常に多かったということが結果で出ていたが、これは Tier1 が大多数だったとの理解で良いか。
また、今後のグルーピングについて、マスターC2 である Tier2、３2、３を把握して遮断を効果的に行う検討をしているのか、もしくはこれから検討を考えているか。ボットネットの全容を把握して効果的に打撃を与え、通信事業者が持っている通信設備に対して影響を与えないようにするには、どの程度の範囲で適用すれば効果的なのかを検討する上で、上位構造も把握しておかないと効果判定ができないと考えており、そういった取組は今後計画・予定されているのかについて伺いたい。

NTT コミュニケーションズ　須藤氏）

今回の調査では C&C 単独機能で動いているものがあるが、多くはそのフロントにいる明らかに Tier1 かつプロキシーボットネットの様なものが非常に多く、今回の結果は主に Tier1 の C&C サーバの挙動が見えている。上位にいるマスターC2 を対策すればこの下のコントロールもどうにかなるので検討対象になっているが、国内通信事業者によるフロー分析で現状見えているところは、通信路と呼ばれているところで、もちろんマスターC&C サーバと子 C&C サーバとの通信を把握してここを対処することは効果的なので検討していく対象であると考える。この Tier1C&C サーバが国内にいた場合は見つけることができるが、今回の分析結果では非常に少数であり、定量的な成果が出せなかったところが今回の課題である。Tier1 の C2 サーバ自体がほぼ 99.99%海外である状況である。過去に Trickbot や Emotet 系のマスターC2 を見つけた実績もある技術なので重要ではあるが、現状の国内の網ではどうしても漏れてしまうというのが現実である。

小山構成員）

トライアルを進めていく上で、ユーザーの理解等の観点も重要で、ICT-ISAC もここに関わっていただきたい。その際は他の業界 ISAC との連携も視野に入れる。もう一方の課題は C2 の通信をブロックした場合、ボットネットが DoS 攻撃を行っていると攻撃が止まったように見えるが、その成果の測定をどのように行い、KPI を何に設定すべきなのかについては皆さんの御意見をいただきながら考えていきたい。

後藤主査）

先程の話で別の ISAC や海外の同じような取組など連携する仲間を増やしていくという観点での難しさは。

小山構成員）

こういった取組は日本で始まって間もなく、通信の秘密の情報共有に関して ISP 連携の中では許されているが、外に対してまだ条件などが整理できてない部分がある。まずは国内の連携、そして海外の連携と順番に課題を整理していきたい。

吉岡構成員）

基本的に国内の多少なりともボットが検知できるという理解は正しいか。またどれくらいいれば C2 として紛れないで認識ができるか、何か目安があれば教えていただきたい。

NTT コミュニケーションズ　須藤氏）

国内の ISP にボットが存在していることが前提で、挙動を踏まえた機械学習やグラフマイニングを使い C&C を特定することが今回の技術である。ボット数はチューニングやスレッショルド値の話となるので、今は答えることが非常に難しい。非常にアグレッシブ、大規模なものであるものは当然見つけやすいが、一般のサードサービス等と混ざってしまう。小規模で非常に静かに動いているものだが、ある瞬間から攻撃を発生するところは、機械学習系の技術だとスレッショルド値を下回ってしまって検出できない。グラフマイニングの方を用いることで少し違う観点から少数のものを拾えるような技術開発をしていく。

吉岡構成員）

規模以外に例えば何か同期性が強いとか弱いとか、そういうのも関係するのか。

NTT コミュニケーションズ　須藤氏）

おっしゃる通り同じような挙動をするところの同期性なども観点に入れて分析を行っている。

(3)閉会

以上