令和２年 12 月 14 日

令和２年度サイバーセキュリティ政策会議（第３回）
発言要旨

１　開会

２　第三回会議における御発表等について

【事務局から、第一回及び第二回サイバーセキュリティ政策会議の指摘事項、第三回議事次第について発表】

３　サイバー犯罪者たちの動向観測

【委員から、サイバー犯罪者たちの動向観測について発表】

４　IoT サイバーセキュリティの現状

【有識者から、IoT サイバーセキュリティの現状について発表】

５　質疑

委　　員：　実空間においては、例えば暴力団から脅迫を受けた場合の一般的な対応として、付け込む隙を見せない、毅然とした態度で対応するといった認識の共有が啓発活動により広まっているが、ランサムウェアの二重恐喝等の場合、何をしてはいけないのかといったことの啓発がそれほど進んでいないように見受けられる。警察庁としてどのような対応を実施していくのか。

事 務 局：　御指摘のとおり、最近のランサムウェアに係る対策は、十分とは言えないと考えている。ワナクライ等の従来型のランサムウェアについては、感染への対処法として、警察への相談、バックアップの保存等を各関係機関と連携し注意喚起してきたところ。

　一方、ランサムウェアの二重恐喝等の対応としては、被害企業と連携し犯人の特定を進めるとともに、身代金の支払いによって被害を回復（暗号化ファイルの復号）することは確実ではなく、かつ、米国等の法令に抵触する場合もあることを説明している。

　ランサムウェアの二重恐喝等については、これからも注意喚起等の対応を考えていきたい。

委　　員：　ベストプラクティスの対外的共有をお願いしたい。

委　　員：　ランサムウェアの対策の１つとして、海外では No More Ransom という組織を活用し、データの復元が可能であるという話を聞いたことがあるが、当

該組織は信用に足るものか。

また、ランサムウェアで暗号化されたデータを復元する方法として、暗号鍵の断片情報の活用、消去された平文データの復元等、様々な対策が検討されていると考えるが、昨今の情勢について情報提供願う。

委　　員：海外のランサムウェアの被害対策組織については、組織があることは認知しているものの、詳細については把握していない。

暗号化されたデータの復旧については、バックアップサーバ等のデータも感染時に暗号化されることから、データの復旧は一筋縄ではいかない。また、Windows の自動バックアップ領域であるボリューム・シャドー・コピー・サービス（ＶＳＳ）についても、ランサムウェアがデータを削除し、バックアップからの復旧を妨げる手口も確認されており、復旧にはかなりの困難が伴う状況である。

対策手法としては、クラウド上にバックアップを保存することや、ネットワークに接続されていないオフライン端末等にバックアップを保存することが有効である。

暗号鍵の抽出に関しては、攻撃者も対抗措置として、毎回異なる暗号鍵を使用していることから、デジタルフォレンジックによりデータを復旧することは難しい。

事 務 局：委員御指摘の No More Ransom は、ユーロポールの主導で実施している取組であり、信用できるものと考えている。一方、暗号鍵をデジタルフォレンジックで取り出しデータを復元するという No More Ransom の取組について、最近は犯罪者等の手口の巧妙化により、復号が難しくなっている。

委　　員：新井委員の発表において、「あなたの能力が必要です。大金が欲しいですか。」といったランサムウェア攻撃の実行役の勧誘メールを引用していたが、当該メールアドレスの一部に怪しい文字列があり、それにも関わらず引っかかってしまう人がいるのであれば、やはりサイバーハイジーンが重要であると言えるのではないか。このようなメールに引っかかった人がどのぐらいいるのかご存じであればお伺いしたい。

また、コメントとしては、コロナに関わらず、シンプルな手口に騙される人が多くいることから、サイバーハイジーン（サイバー公衆衛生）の重要性が増していると考えている。

委　　員：国内に関しては、発表した事例しか把握していない。一方、海外に関しては、ベラルーシ、ポーランド等の東欧諸国において、実行役が検挙された事例を複数確認している。

委　　員：ＲａａＳ（Ransomeware as a Service）について、ダッシュボードでＩＤ、暗号鍵、身代金の支払い状況等について管理できるとお伺いしたが、暗号鍵

による復号をせず、単に業務妨害をしたいだけであれば多数の端末に感染させる意味も分かるが、身代金の回収に重きを置く場合、ランサムウェアの感染端末を限定した方が効率的と考えるが如何か。また、ランサムウェアの感染について、国家の関与が疑われるものもあるところ、御意見を頂戴したい。

吉岡様への質問として、総務省、ＮＩＣＴで実施しているＮＯＴＩＣＥの成果は、調査で明らかになってきているのか。

委　　員：ランサムウェアにより二重恐喝を行うグループに関しては、数万台規模のＰＣやサーバ内のデータを暗号化している。一連の暗号化に関する復号鍵は、ランサムウェアの開発・暴露サイト運用グループ、あるいは交渉を担っているグループが管理している。大規模なランサムウェアの感染についても、管理・交渉を支援するグループがあり、暗号化されたＰＣ、サーバ等の管理に対応している。攻撃者は、ランサムウェアグループの攻撃役、ランサムウェアの開発・暴露サイトの運用・交渉役とに役割を分担しており、攻撃役は多数のＰＣ等を暗号化することに特化、ランサムウェアの開発・暴露サイトの運用・交渉役は、暗号化されたＰＣ等の管理を実施し、一種のエコシステムを確立させている。

国家の関与が疑われるランサムウェアの感染としては、昨年、台湾において、国営の石油ガス会社に対する標的型攻撃が行われた事例がある。当該攻撃は、一般に政府が支援するサイバー攻撃グループによる犯行と言われているが、ランサムウェアと同様に暗号化が行われ国営企業の事業継続に支障をきたす被害が発生した。

有 識 者：ＮＯＴＩＣＥのページにおいて、Ｔｅｌｎｅｔの機器観測結果等を公表しているところ、顕著な効果はまだ明確に出ていない。

理由の１つとしては、ログインできるパスワードの種類が限られていることが挙げられる。現在、パスワードの種類を増やしたことで、検知されるＴｅｌｎｅｔ等の件数が増加しており、今後、効果が出てくると考えている。

また、最近は、Ｔｅｌｎｅｔ以外のサービスが標的となっているため、検査対象サービスを増やすことで効果は出てくると考えているが、現時点で顕著な結果が出ているという状況ではない。

参考として、ＮＯＴＩＣＥはルーター、ＩＰカメラなどが対象になっているところ、これとは別に外部から重要施設のシステムに不正侵入可能な点については、注意喚起まで含めてかなり内部のところまでお手伝いさせていただいている。当該取組は、非常に効果があり、しっかり対応していただいている。

委　　員：ランサムウェアの攻撃グループの動機についてお伺いしたい。最近、二重恐喝のランサムウェアが主流になっているところ、金銭を窃取できる可能性

について疑問に感じる。被害側は、既に窃取されているデータについて、身代金を支払ってもデータを暴露されない保障がない。攻撃側の目的としては、本当に金銭目的なのか、あるいは、単に業務を停止させることが目的なのか。現状の分析やデータがあればお伺いしたい。

委　　員：ランサムウェアグループの主犯格が、Ｙｏｕｔｕｂｅのインタビュー番組で話していたところによれば、彼らの運営するランサムウェアグループは、ランサムウェアに感染した企業が、１０件あれば３件は支払いに応じている。同時に、二重恐喝の手口を取ることにより、１件当たりの身代金額が３割程度上昇しているとのことである。さらに、従来型のランサムウェアに関して、パソコン１台あたり、４万円程度の被害額であったことから、例えば１,０００台感染すると、４,０００万円ぐらいの被害額になるといったところ、本年の４月にイギリスの両替業Ｔｒａｖｅｌｅｘ社が約２億円の身代金、本年６月にアメリカのカリフォルニア大学サンフランシスコ校が、約１億円の身代金を支払っており、従来に比べ高額な支払いを企業側が行っていることが確認できる。

委 員 長：研究成果について、他国にも情報共有を行うのか。

有 識 者：１００組織程度にＩｏＴマルウェアの検体、解析結果を共有しているところ、研究者との関係性によって提供するデータセットの内容に差をつけている。

委　　員：今回の発表を拝聴し、日本においても、専門家の先生方が分析・研究をされているということが分かり、心強い。一方で、消費者や中小企業、大企業であっても情報システム部門以外の経営者においても、サイバーセキュリティにとどまらない防衛意識、危機感を持った方がよいと考えており、具体的な犯人像を含め知識を共有するためにどうすればよいか考えていかなければならない。

委　　員：重要施設の点検等も積極的に行われていると認識しているところ、オリパラが近づく中で、当該事業者の不正アクセス事案が発生しているのか確認したい。

　また、ＩｏＴ機器等の様々な機器に脅威があるとお伺いしたが、どのような機器に特に危険性があるかお伺いしたい。

有 識 者：重要施設については、注意喚起により脆弱性の修正をしていただいているところ、重大インシデントに繋がった事例は確認していない。機械学習等も活用して探査しており、攻撃者よりも効率的に脆弱性を探査できている可能性がある。

　危険性に係る事例としては、ＮＡＳに対するランサムウェア攻撃が確認されており、データ復旧事業者にサイバー攻撃を認知せずに相談が行くケース

がある。特に、ＮＡＳは、いわゆるランサムノートと呼ばれる誰でも分かる形で警告文を提示できないことから、データ復旧事業者が調査した結果、ランサムウェアの感染が発覚する例が見られる。そのため、ＮＡＳ、ＶＰＮ等の設定不備や脆弱性により、不正侵入されるケースが増えてきていることから、注意が必要。

委　　員：脆弱性を発見した後、重要インフラ事業者のように限定された対象であれば個別に対応を求めるやり方もできるが、様々なメーカー・ユーザーに効率的に対応していただけるような注意喚起方法があれば、お伺いしたい。

有 識 者：オランダの事例として、ハニーポット等で検知した脆弱性がある機器について、検疫ネットワークに強制的に接続し、外部から接続できないようにすることで、感染を防止する取組を実施した。当該取組において、ユーザーは、インターネットに接続できなくなり、その理由を確かめるためにブラウザ等を立ち上げた場合、注意喚起のページに強制的に飛ばされる。ユーザーに対策を講じて頂いた場合、検疫ネットワークから元のネットワークに戻す手法を講じたところ、高い確率で対応して頂いた。ただし、ユーザー等の利用規約等の問題があることから、そこまでできる組織ばかりではないため、対応が難しくなっているところである。

現在、効果を上げるための取組として、エンドユーザーが自らセキュリティチェックを行うサイトを開発している。当該サイトでは、自分のアドレスから外部への攻撃の有無を調査できる。

ユーザー側が能動的にアクセスすることで、通信の秘密に係る問題も発生しないことから、当該サイトに多くの人がアクセスして貰えるように、ＳＮＳ等を活用したセキュリティチェックのキャンペーンを考えている。

委 員 長：被害企業が警察に相談に来ているということは、単に何とかして欲しいというだけでなく、被害を根絶して欲しいという方向に世の中が進んでいると思う。

６　報告書骨子のイメージ等について

【事務局から、報告書骨子のイメージ等について発表】

７　閉会