次世代の情報セキュリティ政策に関する研究会（第９回）議事要旨

１　日時

平成２０年６月１８日（水）１０：００～１２：００

２　場所

総務省 第３特別会議室

３　出席者

（１）構成員（敬称略、五十音順）

有村 浩一（テレコム・アイザック・ジャパン）、綾塚 保夫（㈱NTT ドコモ）、小倉 博行（三菱電機㈱）、木村 孝（ニフティ㈱）、小屋 晋吾（トレンドマクロ㈱）、小山 覚（㈱NTTPC コミュニケーションズ）、齋藤 衛（㈱インターネットイニシアティブ）、佐田 昌博（株ウィルコム）、篠田 陽一（北陸先端科学技術大学院大学）、下村 正洋（NPO 日本ネットワークセキュリティ協会）、高倉 弘喜（京都大学）、高橋 正和（マイクロソフト㈱）、手塚 悟（㈱日立製作所）、徳田 敏文（日本アイ・ビー・エム㈱）、中尾 康二（KDDI㈱）、原田 典明（日本電気㈱（則房構成員代理））、藤井 俊郎（松下電器産業㈱）、藤本 正代（富士ゼロックス㈱）、松隈 純（ソフトバンク BB㈱（福智構成員代理））、水越 一郎（東日本電信電話㈱）、村上 晃（㈱ラック（新井構成員代理））、持麾 裕之（NEC ビッグローブ㈱（飯塚構成員代理））、安田 浩（東京電機大学）、山内 正（㈱シマンテック総合研究所）、横田 孝弘（KDDI㈱）

（２）事務局

中田政策統括官、松井官房審議官、鈴木総合政策課長、柳島データ通信課企画官、河内情報セキュリティ対策室長、村上情報セキュリティ対策室課長補佐、長屋情報セキュリティ対策室対策係長

（３）発表者

NTT 情報流通プラットフォーム研究所、奈良先端科学技術大学院大学

４　議事

（１）開会

（２）議事

⑴情報セキュリティに関する調査研究・研究開発の動向について

⑵報告書（案）について

⑶自由討議

（３）その他

（４）閉会

５　議事概要

（１）開会

事務局より、第８回会合の議事要旨につき説明が行われた。

（２）議事

(1)情報セキュリティに関する調査研究・研究開発の動向について

ア.ボットネット実態調査（NTT 情報流通プラットフォーム研究所）

資料 9-2 に基づき説明が行われた。

（主な質疑）

・閉環境においては IRC を、開環境においては HTTP を利用したボットが多いとのことだが、閉環境の場合にはダウンロードが発生しないため、主に IRC となるのは当然ではないか。また、コマンドコントロールの通信とダウンロードの通信の区別がされていないようであり、単純に比較をした場合に誤解を招くような表現ではないか。

⇒HTTP を利用したボットのうち、ほとんどは BOBAX という HTTP の C&C サーバを用いたボットと同様のコマンド体系を持つものとなっている。他についても、挙動を見ると単に追加ボットをダウンロードするのではなく C&C サーバとの通信と思われるものが存在したため、ここでは 1226 個の検体が HTTP の C&C を利用しているという表現をさせていただいた。

・かなりの検体が収集されているが、世界中に蔓延しているボットのうち、どの程度をカバーしていると分析されているか。また、いろいろな挙動をする様々なタイプのボットが観測されているが、それらを集約するといくつくらいのタイプのボット群が存在すると認識されているか。

⇒国ごとや ISP ごとに蔓延している検体は異なるため、現時点では、全世界のカバー率というのは把握できていない。また、PC１台の中で解析した情報だけの分類では不十分と思われ、ダイナミックなボットの活動シーケンスをもとに分類していくというのは、１つの手段ではないかと思う。

イ.トレースバック技術への取り組み（奈良先端科学技術大学院大学）

資料 9-3 に基づき説明が行われた。

（主な質疑）

・IP トレースバックは比較的下位レイヤーの技術であるが、冒頭に記載がある Web サイトやｅメール等における本人確認のような、上位レイヤーで使えるモデルにまで発展する可能性はあるのか。

⇒技術的な話と法律を含んだ話の二面性がある。技術的には、NAT を経由したり踏み台を経由した通信のような、トランスポート層で変換のかかった通信であってもトレースは可能。この技術は、実際にはハッシュ値のようなユニークな値を問い合わせ、それを ISP 間で転送していくという仕組みのため、XML のスキームを少し拡張すれば、IP パケットのハッシュ値だけではなく、例えばユーザ ID のようなものの問い合わせも可能。ある意味、この仕組みをアプリケーション層まで一般化して拡張していくことも可能だと考えている。また、この仕組みは情報漏えい対策にも利用できると考えており、現在、NICT ではそのあたりについて取り組んでいる。しかし、法的な話となると全く違う話になり、通信の秘密との関係で調査・議論を行っているところだが、IP パケットのヘッダ部分のハッシュ値に限定すれば、これを無作為に計算し問い合わせることは問題ないだろうと考えている。しかしながら、ユーザ名やｅメールの本文のような、パケットのペイロードを対象に処理することは、現行の解釈の範囲においては法に抵触する可能性がある。このあたりについては、IP トレースバックというものが世の中に浸透しその必要性が認知されれば、もう少し違った法解釈がされるようになるかもしれない。

・ITU での国際標準化という記載があるが、例えば OSI の参照モデルを見ると、通信を機能毎に分け、機能モジュールをサービスインターフェースとプロトコルインターフェース、そのサービスの機能をどう処理するかというプロセスのモデルに分類している。トレースバックとしてご提案されている BTM(Border Traceback Manager)等のモジュールは、一般化した機能モジュールになり得るものか。日本と他の国が全く違う方式でやっていた場合、このモデルが全然違うとやりにくいと思うが。

⇒トレースバックに限らずということであれば、今の DTM(Domain Traceback Manager)や BTM といったもののモジュール化は使えるのではないかと思っている。組織内を探査するモジュールとプロバイダ境界を切り分けるところは、大抵違うオペレーションであるため、それはトレースバックに限らず適用できる可能性はある。もう１つ、各国でトレースバックの仕組みを作り持ち寄った際、案外似ているということであれば、標準化は容易なのではないか。しかし、各国が作ったものが全く違った場合には、それをマージして標準化するのは困難であると思う。

・ITU での国際標準化活動として、「OSI７階層モデルを手本として」ということだが、これはトレースバックは別の階層ということなのか、それとも階層をまたがる機能として定義されるという意味なのか。

⇒NICT の研究センターでいろいろなモジュールを作っているが、そこでの大ざっぱな感覚として参照モデルが作れるのではないかということを考えている。そ

れはトレースバックに限った話ではなく、例えばボット対策プロジェクトのような検知系システムや、解析系システム、それらを連携させるような連携モジュールといったように、人間の体に例えるならば、目にあたるモジュール、手にあたるモジュール、頭脳にあたるモジュールといったものがあるのではないかと考えている。

(2)報告書（案）について

事務局より、資料 9-4 に基づき説明が行われた。

(3)自由討議

主に報告書（案）に関する議論が行われた。

・高度な ICT 知識がないと分からない言葉が出てきており、想定読者に一般の人も入るのであれば、用語の解説を付けるといった配慮も必要なのではないか。
⇒用語集を別添資料として付けるか、脚注に用語解説を付けるといった形でまとめさせていただきたい。

・P.59「③暗号・認証技術等の基盤的な研究開発の充実」のところで、「国産技術の開発に継続的に取り組むべき」との記載があるが、このような技術は国際性がないと製品に搭載されないといったことがあるので、併せて「国際的な標準化を進める」「国際的な普及に努める」といった文言を加えたほうが良いのではないか。

・P.38 の図表 3-10 は、様々な国から攻撃が来ているというよりも、特定の国から攻撃が集中しているというように読める。他に適切なデータがあるので、差し替えたほうが良いのではないか。

・P.2 に記載のある「ICT サービス提供事業者」には、製品の提供者も含まれるのか。一読すると含まれているようには見えないため、書きぶりを修正したほうが良いのではないか。

・P.63「(情報セキュリティ対策に係る人材育成の推進)」のところで、産と学の協働という部分があまり強く書かれていない。もう少し、「推し進める必要がある」といった書きぶりにしたほうが良いのではないか。

・大人たちは ICT が普及してきた経緯を知っているのに対し、今の子供たちは生まれつき携帯電話や PC といったものに囲まれて育ってきている。利用者にある程度リスクを認識させるような教育等の取組みが必要ではないか。

・P.32 に「攻撃ターゲットとしての旨みが増大する」という記述があるが、表現として不適切ではないか。

・P.20 に示されている脅威は、ICT に限ったものではなく、社会全体のものと考えられるが、P.67「６．終わりに」では、「安心・安全な ICT 環境」という形になっている。本報告書の目指すところは、ICT 環境だけなのか、社会インフラ的なもの

なのか、明確にしたほうが良いのではないか。

⇒脅威としては、外部脅威も含め様々なものがあるが、本研究会においては、特に「ボット等マルウェアによる脅威」と「ソーシャルエンジニアリングを駆使した脅威」に着目し、検討を行ってきたところ。P.21 にも、「本研究会では、主にこうしたネットワークを介してもたらされる脅威に着目して検討を行っている。」と記載しており、検討のターゲットは明確にされているものと認識。

・トレースバック技術に関して、P.63 に「最先端のセキュリティ技術の利用」ということで触れられてはいるが、発信元が分かることによる抑止力等、トレースバック技術の必要性という部分についても記載したほうが良いのではないか。

・本報告書は、どのようなセットで公表することをお考えか。

⇒報告書本体に用語解説等の参考資料を添付したものと、報告書の概要版の２点セットを考えている。

・現状の書きぶりであると、「永遠のビギナー」は国が守ってあげるので安心しなさいという流れになってしまうように感じるが、永遠のビギナーを 100%守ってあげられるわけではなく、「自分だけで守れとは言わないが、全て守ってあげられるわけではない」ということを利用者に認識してもらうユーザ教育や、伝える枠組みが必要ではないか。

（３）その他

事務局より、今後のスケジュールにつき説明が行われた。

（４）閉会