情報セキュリティ　～身近な危険に備えよう!～

研究の目的・背景・仮説（Introduction)

ネットワーク社会の今、サイバー攻撃に関するニュースがよく報道されている。2020年だけでも大手システム会社から国立大学、図書館運営会社など、被害を受けた場は多岐に渡り、攻撃手段も全く異なっていた。そういった報道の中で、日本のセキュリティに関心を持つようになった私たちは、更に調べていくうちに、「攻撃者の中には、独学で攻撃手法を学ぶ者も多い」ことを知り、本当に素人でも攻撃活動が出来るのか調べたいと思った。
よって、この研究の目的は日本のセキュリティ会社の現状を探るとともに、我々素人による攻撃手法の実験を行い、日本のセキュリティ事情について把握することにある。

材料と方法 (Materials andMethods)

材料　パソコン、スマートフォン

結果１　警察官の生活安全課の方から話を聞いたり、警察や公安の資料を見て、インターネットの危険性や詐欺について概要　特徴　事例　対策の４つに分けてまとめる。

結果２{嫌がらせファイルのプログラミング内容}
・やり方　YouTubeでウイルス作り方と検索を行う
①メモ帳を開く②@echo offと打つ③stertを自分の好きなだけ打つ④名前を付けて保存する

結果(Results)

今回の探究の結果は、「まったくの素人でも、インターネットで犯罪を行える」である。
私達の班では、現役警察官の生活班の方に話を伺ったり、警察庁や公安調査庁の資料について調べた。
実際に素人がインターネットで調べ、プログラミングを行った。

結果１

実際の警察官の方の話　公安　警察の資料について。
・現在インターネットは生活と密着しており、生活でのインターネットの危険は増加
・近年では、社会全体がネットを使っておりコロナなどでのテレワークでの危険性が増加
警視庁が発表してる　サイバー空間での脅威　主な事例と特徴　対策　（令和3年版）

	概要	特徴	事例	対策
①ランサムウェア	感染すると端末等に保存されているデータを暗号化して使用できない状態にした上でそのデータを復号する対価として金銭を要求する不正プログラム	暗号資産による金銭の要求が多くを占める	・復旧等に要した期間 １週間から2か月以上 費用　約1000万以上 ・感染経路　テレワーク　で利用されている機器　ネットに繋がる機器	・警察庁ウェブサイトにおける注意喚起 ・損害保険会社と連携した対策の推進 ・ダークウェブサイトの監視 ・医療機関の電子カルテの感染させないように厚労省と連携 ・中小企業や医療機関等を対象としたランサムウェアへの対策
②フィッシング等に伴う不正送金 不正利用	SNSを使いメールやwebなどで誘導し不正にパスワードなどをだまし取る	インターネットバンキングに係る不正送金事犯は、令和元年に、SMS等を用いて金融機関を装ったフィッシングサイトへ誘導する手口が急増し、ID・パスワード、ワンタイムパスワード等が窃取され、金融機関のインターネットバンキングから不正送金される被害等が多発	・同年には、発生件数 1,872件 被害額 約25億2,100万円 ・フィッシング対策協議会令和3年フィッシング　グ報告 件数　52万6,504件 一貫して増加傾向 ・クレジットカード不正利用 被害額 約223億9,000万円	・不正送金組織の検挙等指定暴力団構成員等を含む 男女29名を検挙した。 ・金融機関との連携強化 ・口座売買組織の検挙等令和3年10月までに、口座売買組織の犯行指役口座譲渡者等7名を検挙 ・関係団体と連携　金融機関への対策要請 ・注意喚起
③標的型メール攻撃	ターゲットを特定の組織やユーザー層に絞って行うサイバー攻撃	不審な点が少なく一見普通のメールと変わりない	・機械部品関連の製造業者に対する標的型メール攻撃新IDのお知らせと称して、不正プログラムが仕掛けられたファイルをダウンロードするよう誘導する標的型メールが機械部品関連の製造業者に送信された。 ・医薬品メーカーに対する攻撃 添付ファイルから偽のパスワード入力画面に遷移させ、業務で使用す るアカウントのパスワードを入力するよう誘導する標的型メールが医薬 品メーカーに送信された。	・サイバー攻撃に関する各種情報を集約 するとともに、これらの情報を総合的に分析して、事業者等に対し、分析 結果に基づく注意喚起を行っている ・NISCから提供を受けた政 府機関に対する標的型メール攻撃の分析結果についても、当該事業者等に対して情報共有を行っている。
④他国からの攻撃	サイバー攻撃	システムの弱点を突いた攻撃　人間の心の隙を突いた攻撃　例　メール　SNS	日本にサイバー攻撃する主な国 1**中国**　軍や情報機関による攻撃 2**ロシア**　中国と同様 3**北朝鮮**　金銭獲得 破壊活動	・破壊的団体等の調査 ・活動の制限や解散指定等を請求 ・公安調査庁のホームページでの情報公開

結果２

素人でもインターネットでの嫌がらせのファイルを作れるのかを実験してみた。
結論、作ることができた。その様子と写真　システムコード

写真１　メモ帳の様子

・ファイルを開いた状態　写真２３

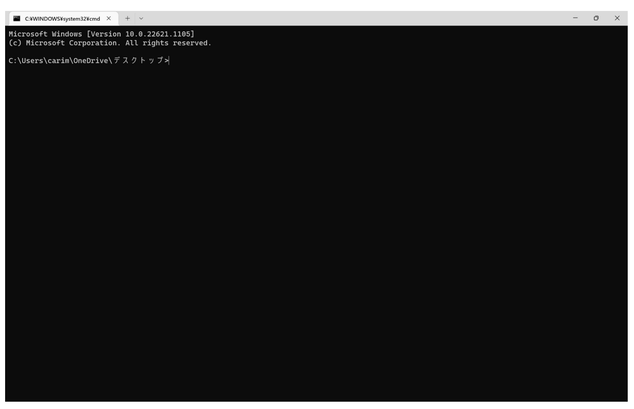

写真2　ページ画面

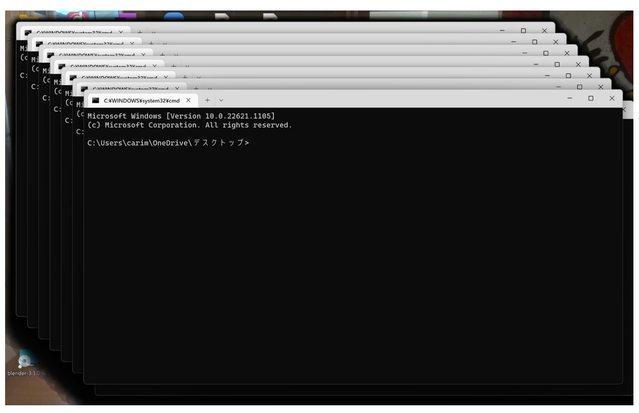

写真3　ファイルが動いている時

＊このウイルスファイルはUSBに保存出来、パソコンの セキュリティソフトでも危険性を察知出来なかった。

考察(Discussion)

私たちは2つの仮説を立てた。実験結果からまずコンピュータにおける嫌がらせや乗っ取り、ハッキングは1人で行うには中々難しい、という点において、実際は時間がかかっても素人でも簡単に操作できると分かった。特に簡単な動作に関しては、YouTubeなど、誰でも見ることができる動画で学ぶことができた。この実験を続けることで、攻撃者達の知識の入手先を知る手掛かりが見つかるかもしれない。
次に日本のセキュリティは緩いのではないか、という点について、日本の主なサイバーセキュリティ企業や、日本と海外でのセキュリティ意識の違いを調べたことで、日本には多種多様なセキュリティ企業が存在し、セキュリティに予算をかける会社も増えてきてはいるが、依然としてセキュリティ人材の育成やセキュリティ意識については、世界の中でも大きな遅れがあることが分かった。
また、重要視されている脅威について、アメリカなどの海外では「詐欺による金銭被害」や「攻撃によるサービス停止」などの外部的要因が上位に入ったのに対し、日本では「内部不正による被害」や「メールの誤送信」など、内部の脅威が上位に入っているという特徴が見られた。
今後の研究では、特に身近なWiFiを使った乗っ取りの仕方、またそれを防ぐ方法の研究と、これまでの学習で見えた日本のセキュリティの特徴について、もっと深く探究していきたい。

参考文献(Reference)

・警視庁　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf
・公安調査庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf
・YouTubeリグのPCチャンネル [目標100人]　https://www.youtube.com/watch?v=CG8fZJ_gLEM

謝辞(Acknowledgments)

多忙の中、我々の探究の為に情報を提供や資料提供本当にありがとうございます。