グローバルなセキュリティ脅威の動向

本稿では，グローバルなセキュリティ脅威の動向として，最近報告された非常に巧妙なサイバー攻撃の事例を2件，攻撃の詳細と対策について紹介します．また，グローバルなセキュリティ脅威に関するNTTグループとしての取り組みの1つ「GTIR（Global Threat Intelligence Report：グローバル脅威情報レポート）」を紹介します．このようなセキュリティ脅威情報を共有することで，セキュリティ意識を高め，セキュリティを強化することにつなげられると考えています．

荒金 陽助[†1] /小倉 賢治[†1]
遠藤 斉[†1] /高橋 健司[†2]

NTTセキュアプラットフォーム研究所[†1]
NTT Innovation Institute, Inc.[†2]

セキュリティ脅威の増大と情報共有の重要性

米国金融大手JPモルガン・チェースからの大規模な顧客情報流出，社内システムを破壊して窃取した内部情報を公開する等のソニー・ピクチャーズへの破壊的なサイバー攻撃，米国人事局からの政府職員情報大量流出，日本年金機構からの情報漏洩など，大規模でその被害の評価も困難なほどのサイバー攻撃が近年多数報告されています．このようなサイバー攻撃では，主に保安上の観点から，その詳細が報告されることはあまりありません．

しかし，このような事例を通して攻撃の手口や対応策を把握することで自らのセキュリティを強化することは可能であり，セキュリティ脅威の情報を共有することは今後ますます重要になっていくと考えられます．

本稿では，最近報告された巧妙なサイバー攻撃の事例と，情報共有を加速させるためのGTIR（Global Threat Intelligence Report：グローバル脅威情報レポート）の取り組みについて紹介します．

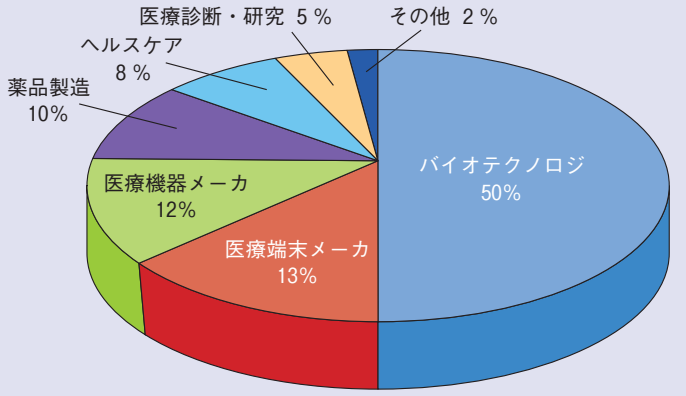
企業機密情報を秘密裏に窃取する「FIN4」

セキュリティ保護のソリューションを提供しているFireEye社（米国）は，顧客のネットワークにおけるインシデントへの対応や同社の製品が検出したデータから，株式公開企業の株価に影響を与えると考えられる内部情報に焦点を絞って秘密裏に情報を窃取しているグループを検出し，このグループを「FIN4」と名付けました．

FIN4は，そのメンバを特定できていないために攻撃の目的は明らかになっていません．しかしFireEye社では，FIN4は入手した内部重要情報を活用して株式の取引を有利に進めて利益を上げていると考えています．このようなサイバー攻撃は，標的の企業に直接的な損失がみられないために，攻撃を受けた標的の実態や被害範囲の把握は非常に困難です．

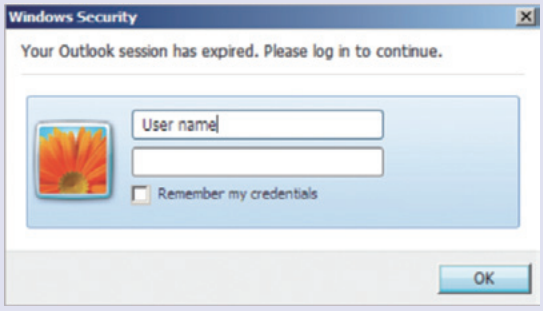
FIN4の活動は2013年半ばからみられ，FireEye社が把握している標的は約100社で，68％が医薬系企業，20％がM&Aコンサルティング会社，12％がその他の株式公開企業です．医薬系企業は，新薬などの開発や臨床試験，また国の認可などにかかわる情報が株価に大きな影響を与えます．またM&Aコンサルティング会社は，公開前のM＆A情報を多く扱っています．FIN4の標的となった医薬業界の中の分野別内訳を**図1**に示します．

FIN4は，標的の企業を絞り込むと，まずその標的企業と取引のある企業をねらいます．そして，標的企業と取引のある企業のメールアカウントから，進行中の取引案件に関する情報を標的企業にメールで送信します．メール送信先は，標的企業の企業機密情報を扱う経営幹部や法務関係者，顧問弁護士などです．このメールには実際の取引でやり取りされるオフィスドキュメントが添付されており，これを開くと仕込まれているマクロにより偽のOutlookログインプロンプトが表示され[(1)]（**図2**），ここで入力されたログイン情報がFIN4のサーバに送信されます．マクロが無効化されているような環境に対しては，メール本文に偽のOWA（Outlook Web App）ログイン画面へのリンクを記載し，偽画面でログイン情報を窃取します．FIN4は，窃取したOutlook認証情報を使って標的企業の機密情報取扱者のメールアカウントにアクセスし，メール本文を盗み読むことで機密情報を入手します．



出典：https://www2.fireeye.com/fin4.htmlより作成

図1　FIN4が標的とする医薬系企業の分野別内訳



出典：https://www2.fireeye.com/fin4.html

図2　ログイン情報を窃取するための偽ダイアログ

またFIN4は，侵害を気付かれないように，「ハッキング」「フィッシング」「マルウェア」といった単語を含むメールを標的者のOutlookアカウントから自動的に削除する設定を行います．これにより，外部からの「あなたの企業がねらわれている」といったアドバイスが標的者の目に届かないように工夫しています．

米国証券取引委員会（SEC）が，FIN4の標的となった企業少なくとも8社に対して詳細の報告をするように求めているという報道[(2)]がありますが，2015年6月末時点でSECは公的には見解を出していません．

FIN4の犠牲者とならないためには，Microsoft Officeのマクロを無効化しておく，OWAに二要素認証を取り入れる，といったことが挙げられます．また，FIN4はログイン情報を送信するサーバとの通信を隠蔽するためにTor*1を使用するので，社内のアクセスログを監査して既知のTorノードとの通信がないか確認することも有効な手段です．

中国の新しい攻撃システム「Great Cannon」

2015年4月10日のトロント大学シチズンラボの調査により，中国のネット検閲システムGFW（Great FireWall）*2に併設された攻撃システムが存在することが明らかになりました．シチズンラボはこの攻撃システムをGC（Great Cannon）と名付けました．2015年3月のGreatFire.orgとGitHub*3への大規模なDDoS（Distributed Denial of Service）攻撃が，観測されたGCによる最初の攻撃となります．以下，GCの基盤となるGFWの仕組み，GCの仕組み，GCによる攻撃の順に解説します．

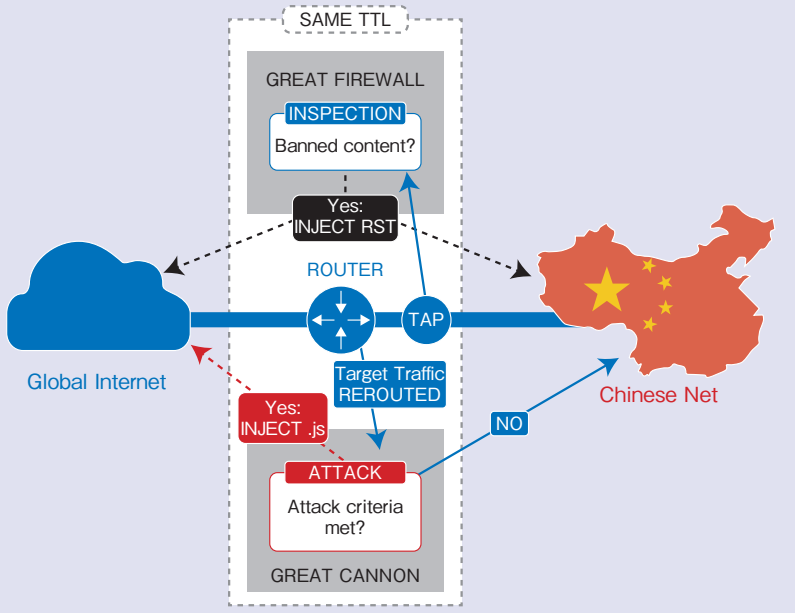
■GFWの仕組み

図3の上部がGFWとなります[(3)]．中国内から中国外への通信と中国外から中国内への通信はGFWを通り，「TAP」と示された部分で通信内容を傍受し，「INSPECTION」と書かれた部分で規制・遮断対象のアクセスかどうかを識別します．ここで規制・遮断対象と識別されると，「INJECT RST」の部分でアクセス元およびアクセス先サーバに対して，通信を中断・拒否をする際に使用するRST（リセット）パケットを送信し，接続を遮断します．GFWはロードバランスの機構を導入することにより，並行して複数の通信に対処することができます．このようにGFWは通信を常に監視することにより，中国当局が望まないアクセスを遮断することができます．

■GCの仕組み

GCは，　図3の「Target Traffic REROUTED」の部分で対象となる通信の経路を変更し，「ATTACK」の

＊1　Tor：ネットワーク接続における経路を匿名化するソフトウェア．通信内容の秘匿化は行われません．
＊2　GFW：中国国内からのインターネット通信と，中国国内から中国国内へ向けて行われるインターネット通信に対して接続規制や遮断を行う，中国当局による大規模な検閲システム．
＊3　GitHub：GitHub社によって提供されている，ソフトウェア開発プロジェクトのための共有Webサービスであり，基本機能は無償で利用できますが，拡張機能の利用は有償となります．



出典：https://citizenlab.org/2015/04/chinas-great-cannon/

図３　模式化したGFWとGCの仕組み

部分で攻撃対象に該当するか識別します．該当する場合はアクセス元に対して攻撃コードを送り，該当しない場合はリクエスト先のサーバに接続します．攻撃コードを受け取ったアクセス元は踏み台となりGCの攻撃に加担させられます．GFWと同様に中国内から中国外への通信と中国外から中国内への通信はGCを通過するため，GCに利用される通信がごくわずかの割合であっても大規模な攻撃を行うことができます．GCは通信を乗っ取るため，中間者（MITM: Man In The Middle）攻撃が可能です．GCは大量の通信に対応するため，アクセス元が制御対象のIPアドレスに対する通信のみを横取りします．また，過去の通信を一定量保存（キャッシュ）することで同じ通信に対して何度も処理を行うような無駄を排除する仕組みも備えています．シチズンラボの試験の結果，最大約１万6000の直近のアクセス元IPを保存しているとみられます．

シチズンラボによると，GCおよびGFWそれぞれが作動するように設定された通信を送り，その反応を解析した結果からは，GCとGFWが攻撃設備を共有している形跡はなく，両者は独立したシステムであると考えられるとのことです．ただし，両者には通信パケットを書き換えた内容に共通点があり，プログラムコードの一部を両者で共有しているものとみられ，非常に密接な関係があると考えられるとのことです．GCはGFWと類似したロードバランスの機能を持っており，アクセス元のIPアドレスによって振り分けを行っているものと思われます．

シチズンラボがGFWとGCが作動するまでの通信経路を調査したところ，到達したネットワークが両者で同一であったことから，GCはGFWのすぐ近くに設置されているものとみられます．１つの試験環境からは両者ともにChina Telecomに到達し，別の試験環境では同様にChina Unionに到達しました．Robert Graham氏の過去の研究によると，GCはChina Unionのインフラ上にあると結論付けています．

■GreatFire.orgとGitHubへの攻撃

2015年３月14～25日にかけてGreatFire.orgに対して大規模なDDoS攻撃が行われ，通常の2500倍にあたる毎時26億回のリクエストが送られました．GreatFire.orgはAmazon CloudFront CDNサービスを利用してGFWを迂回して規制サイトを閲覧できる機能を提供しています．なお，中国政府機関 CAC（The Cyberspace Administration of China）は，すでにGreatFire.orgを外国の反中国組織（foreign anti-Chinese organization）として指定しています．

また，2015年３月25日～４月７日にかけてGitHubに対する大規模なDDoS攻撃が行われ，サイトのレスポンスタイムが通常の数倍に増大しました[4]．GreatFire.orgはGitHubに２つのリポジトリを持っており，中国の検閲の回避を希望する利用者に技術提供を行っています．GitHubへの攻撃は，GitHubにこれらのリポジトリの削除を強いる目的で行われたものとみられます．

GreatFire.orgおよびGitHubへの攻撃において，GCはBaiduの共通基盤として使われるBaidu analyticsやBaidu advertisingにアクセスする通信を横取りし，攻撃に利用していました．ただし該当するすべてのトラフィックが攻撃に使われるのではなく，シチズンラボの観測では大半の約98.25%の通信はそのままBaiduに送信され，約1.75%の通信が攻撃に利用されていました．攻撃に利用されたアクセスはBaiduから広告が配信されているサイトの閲覧などであり，サイト閲覧者は無自覚のうちにGreatFire.orgやGitHubへの攻

撃に参加していたことになります．

■GCは誰がつくったか

シチズンラボは，GCによるあからさまな攻撃は中国政府当局に無断で実行できるものではないレベルのものであるため，GCの構築や攻撃は中国政府当局の承認を受けているものと考えています．シチズンラボはなぜGCがつくられたのかは明確ではないとしながらも，GreatFire.orgの活動と中国共産党のイデオロギーとの対立の結果により構築された可能性や，このような破壊的な行為は党の望まないコンテンツへのアクセスをブロックするだけでなく，同様の活動を行う他の組織への「みせしめ」の効果をねらった可能性を推測しています．

■今後の予測

GCにはアクセス元に基づいた攻撃が可能であることは明らかであるため，まだ観測されていないものの，潜在的に後述するようなDDoS攻撃以外のサイバー攻撃を行うことが可能とみられます．例えばGCに簡単な設定変更を加えるだけで，中国国内のサーバに暗号化なしでアクセスしてくる特定のアクセス元に対してマルウェアを送ることができます．また，GCは完全な中間者であることから，暗号化されていないE-mail通信の添付ファイルをマルウェアに置き換えることもできます．

GCによる攻撃に対しては組織や利用者レベルで自身の防御対策を行うのは非常に困難です．しかし，GCはその機構上，HTTPなどの暗号化を行っていない通信の内容に基づいて攻撃を行っており，HTTPSなどの暗号通信に対しては対応できていません．したがってGCの効力を弱めていくには，多くの組織や利用者で通信やコンテンツの暗号化を推進させていくことが有効であると考えます．

GTIR

NTTグループ・グローバル脅威情報レポート（GTIR）の2015年版は，NTTグループ各社（NTTコムセキュリティ，Dimension Data，Solutionary，NTTセキュアプラットフォーム研究所，NTTデータ）の協力を得て，NTT Innovation Institute, Inc.（NTT I^3）により作成されました．2014年を通じてNTTグループが観測した約60億の攻撃データを基にして，以下の重要な傾向を詳説しています．

- 金融セクタが最大のターゲットで，検出された攻撃全体の18％に相当．コンサルなどの専門家サービスに対する攻撃は9％から15％に増加
- 74％の組織では正式なインシデント対応計画が欠如
- マルウェアの脅威に関するインシデント対応は2013年に比べ9％増加し，43%から52％へ．企業内で発見された脆弱性の76%は2年以上経過，同9%は10年以上経過
- エクスプロイト・キットがねらう脆弱性の80%以上は2013～2014年に公表．アドビ・フラッシュ対象のものが急増
- NTTのグローバル顧客に対する攻撃のうち56％は，米国内のIPアドレスが起点．攻撃者は米国内に在住しているとは限らないが，米国内の豊富なクラウドサービスを活用
- DDoS攻撃のうち，UDP（User Datagram Protocol）ベースの攻撃が全体の約3分の2

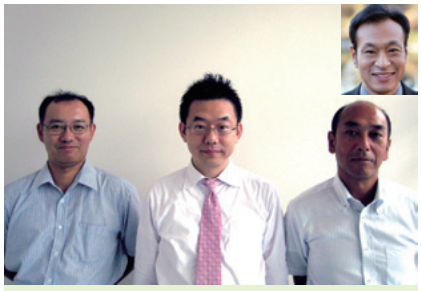
今後の展開

NTTセキュアプラットフォーム研究所に属するNTT-CERT（NTT Computer Security Incident Response and Readiness Coordination Team）は，NTTグループおよび情報ネットワーク社会のセキュリティ向上に貢献するために，情報セキュリティに関する相談窓口を提供するとともに，セキュリティにかかわる情報の配信も行っています．

NTTグループ会社のインシデント対応を継続して支援していくとともに，これからはよりグローバルな展開を意識して，情報の配信も行っていきたいと考えています．

■参考文献

(1) https://www2.fireeye.com/fin4.html
(2) http://www.reuters.com/article/2015/06/23/us-hackers-insidertrading-idUSKBN0P31M720150623
(3) https://citizenlab.org/2015/04/chinas-great-cannon/
(4) http://www.zdnet.com/article/google-says-chinese-great-cannon-shows-need-to-encrypt-web/



（左から）荒金　陽助/ 遠藤　斉/
小倉　賢治/ 高橋　健司（右上）

NTT-CERTは，NTTグループ内外の組織や専門家と協力して，セキュリティ脅威情報などを収集して分析しています．これからも積極的に情報を共有することで，セキュリティ向上に貢献し続けていきます．

◆問い合わせ先

NTTセキュアプラットフォーム研究所
NTT-CERT
TEL　0422-59-7800
FAX　0422-59-7801
E-mail　cert@ntt-cert.org