①国境なきサイバー空間：年金機構事件の“Who done it?”

資料6

平成28年2月7日放送　NHKスペシャル
『サイバーショック　狙われる日本の機密情報』

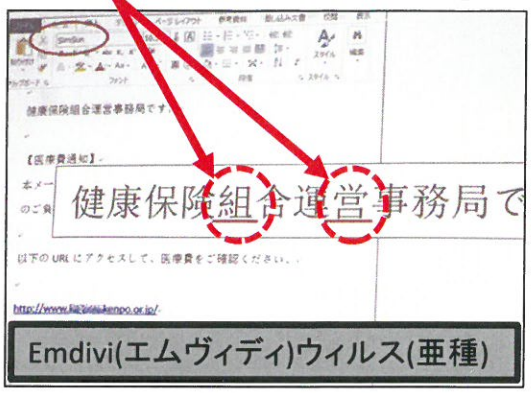
●年金機構事件で中継地点になったサーバを調べると、1000以上の企業・団体から2万件以上の情報流出が判明。（whoisコマンドでIPアドレス調査：カスペルスキー社分析）
●流出情報には、防衛産業の設計情報や日豪打合せメモ、JR北海道のセキュリティ体制など企業機密情報（UBIC社解析）。
●「サイバー攻撃は『史上最大の富の移転』で国の土台が水面下で知らぬ間に蝕まれている」と慶大・土屋大洋教授。
●今回の日本を狙った攻撃はどこから仕掛けられていたのか追跡。福岡の居酒屋、北海道の牧場HP経由ルートはIPアドレスが次々変わり追跡不能。九州歯大病院→上海企業→広東省IT企業(他の日本企業の情報もこの企業へ)。問いただすと「私たちは合法的な企業でそのようなこと（サイバー攻撃関与）はあり得ない」(解析はPwCサイバーサービス社)

年金機構が受信した不審メールの例

差出人：[redacted]excite.co.jp〉
件名：【医療費通知】
添付ファイル：医療費通知のお知らせ.lzh
〉本メールは、保険を利用して診察や診療を受けられた方に、医療費のご負担額等をお知らせしています。
〉Windows-PC で開けてください。

中国語の簡体字

2014年秋からバラ撒かれたEmdiviウィルスの偽メール



（出典）NHKスペシャル:『サイバーショック-狙われる日本の機密情報-』(平成28年2月7日放送)
（出典）日本年金機構「不正アクセスにyる情報流出事案に関する調査結果報告」(平成27年8月20日)
（出典）日経新聞「年金情報流出 解明進まず 被害全容や犯人不明」(2015年7月9日)、「年金機構へのサイバー攻撃 類似ウィルス11団体感染」(2016年1月3日)
（出典）IT PRO by 日経コンピュータ「長野県上田市を襲った標的型攻撃メール、住基ネット強制遮断の憂き目に」
http://itpro.nikkeibp.co.jp/atcl/column/15/082000199/082000001/?ST=security&P=4

②サイバー空間の利用をどうするか徹底的な議論・国際連携が必要

警察庁・公表資料（H28.3.17）

【違法中継サーバ対策】

インターネット接続を取り次ぐ中継サーバについては、利用者のIPアドレスが置き換わるなどの特性を有しており、その匿名性から犯罪インフラとなっている実態がある。

平成27年11月、15都道府県警察合同捜査本部において、他人の認証IDを不正利用してインターネット接続していた日本国内の中継サーバ事業者による不正アクセス事件を検挙した。被疑者らは、中国からのインターネット接続を取り次ぐための中継サーバ事業を日本国内で営む会社の経営者や社員であり、同年６月下旬ころ、インターネット接続事業者が第三者を正規利用権者として付与した認証ID・パスワードを不正利用して不正アクセス行為をしていた。

また、中継サーバ事業者の通信回線は、被疑者の検挙後も契約が継続されたままで、サーバを接続すれば直ちに事業が再開できる環境にあり、犯罪被害の拡大防止の観点から回線契約を解除する必要性があったことから、悪質な中継サーバ事業者への対策として、大手通信事業者に働き掛けを行った結果、同年12月、事業者が契約約款を改正し、契約解除に応じることとなった。

押収されたサーバには、不正入手されたID・パスワードが延べ1800万件も蓄積！

不正接続を自動で試みる専用プログラムも約百種類見つかる。中国製とみられ、昨年6～11月に大量の不正アクセスの形跡があった！

今年2月29日、米・カーター国防長官は記者会見で、サイバー部隊を使ってISの通信ネットワークに過重な負荷をかけ、ISが部隊の指揮をとれなくするようサイバー攻撃を加えていると明らかにした。専門家いわく「歴史的な瞬間」「能力行使だけでなく、サイバー攻撃をすると公言しているのであり、これでサイバー攻撃を戦争の一形態として位置付けることになる」。

米国『マンディアント報告書』

■61398部隊の存在

■本部と思われる上海のビル

この報告書によれば、人民解放軍の総参謀第三部の第二局が61398部隊とされ、この部隊は、従来、外国人が関与する外交・軍事・国際通信の監視を行い、信号・通信情報活動(SIGINT)も担当しており、単独の部門としては、中国のインテリジェンス機構の他のいかなるものよりも規模が大きいとされている。第三部には、十三万人の要員がいるが、そのうち第二局(61398部隊)は主な部局で、米国とカナダを対象として、政治、経済、軍事関連の情報を収集している。関連オフィスは上海に集中しているという。（「サイバー攻撃への注目と米中首脳会談」※出典・土屋大洋氏）

（出典）警察庁・広報資料「平成27年におけるサイバー空間をめぐる脅威の醸成について」(平成28年3月17日)
（出典）日経新聞夕刊「警視庁押収の中継サーバー 個人情報1800万件蓄積 中国のグループ 発信元隠し接続 国境超えた犯罪、摘発困難」(2016年3月25日)
（出典）(旧)マンディアント社報告書「APT1」http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
（出典）土屋大洋著「米国のサイバーセキュリティ政策-スノーデン事件のインパクト-」(拓殖大学『海外事情』2014年3月号)
（出典）朝日新聞朝刊「米中を追う機密・インフラ全て標的 サイバー交渉担当、特使に『中国の関与が疑われる主な米国へのサイバー攻撃』」(2015年9月22日)
（出典）日経新聞朝刊(FINANCIAL TIMES)「米、サイバー攻撃を宣言 まず対「イスラム国」世界に意志示す」(平成28年4月17日)

平成28年4月19日　参議院 総務委員会　民進党・新緑風会　石上俊雄