ボルト・タイフーン III

—— 米政府機関が実施したサイバースパイ活動と偽情報作戦の実態に迫る

要旨

「ボルト・タイフーン」に関する前の二つの調査報告書が発表された後、米連邦政府機関や主流メディア、マイクロソフト社は一斉に沈黙を守り続けている。一方、ロバート・ジョイス氏をはじめとする米情報機関、サイバーセキュリティを担当する部門の現・元官僚、一部の米サイバーセキュリティ企業、サイバーセキュリティメディアが声を上げて大いに反論していたが、前の二つの報告書で出された証拠に触れないようにしていた。こうした言動は、盗人猛々しい卑劣な真の姿をあらわにした。本報告書は、前の二つの報告書に基づき、米連邦政府や情報機関と「ファイブ・アイズ（Five Eyes）」が中国やドイツなどの国、および世界中のインターネットユーザーに対し共同で実施した通信傍受・機密情報窃取というサイバースパイ活動をさらに明らかにする。また、トレーサビリティ分析をミスリードする「ツールキット」を利用して「フォルスフラッグ（偽旗作戦）」を実施し、悪意あるサイバー攻撃行動を隠し、他国に濡れ衣を着せる確証を示す。さらに、サプライチェーン攻撃を実施し、ネットワーク関連製品の中にバックドアを仕掛け、「待ち伏せ」という事実を暴き出し、「ボルト・タイフーン」という米連邦政府による自作自演の茶番劇の真相を徹底的に解明していく。

一、まえがき

2024 年 4 月 15 日と 7 月 8 日、中国国家コンピューターウイルス緊急処理センターやコンピューターウイルス対策技術国家工程実験室、中国最大のインターネッ

トセキュリティ企業 360 が前後して、「ボルト・タイフーン――米国の議会と納税者に対する米情報機関の陰謀的詐欺キャンペーン」[1]「ボルト・タイフーン II――米国の議会と納税者に対する米政府機関の偽情報作戦の実態に迫る」[2]と題する調査報告書を発表し、次のように指摘した。米政府機関は「令状なしで通信監視を実施する権限」を確保し続けるため、世界中の通信・インターネットユーザーに対し無差別監視を実施し、またその裏にある利益集団のためにより大きな政治的利益と経済的利益を掠め取り、中国によるサイバー攻撃の脅威という偽情報をでっちあげ、米議会議員と納税者に対し他の組織と共謀して詐欺を実施する「ハウス・オブ・カード」式の茶番劇を演じている。報告書が発表された後、虚言を造った者、米「グローバルメディア局」（USAGM）および同機関にコントロールされる欧米の主流メディアは相変わらず沈黙を守っていたが、この「沈黙」は国際社会で広く注目された。米国や欧州、アジアなどの国・地域からの 50 人以上のサイバーセキュリティ専門家が各種の方法を通じて、当センターと連絡を取り、米国とマイクロソフト社が「ボルト・タイフーン」を中国政府とつなげたことには、有力な証拠に欠けていると述べた。また、米国が「ボルト・タイフーン」を操って偽情報作戦を展開していることへの懸念を表した。同時に、インターネットにおいて関連話題に対する注目度が持続的に上昇し、国際社会は米国およびそのサイバー覇権の真の姿と、米国がインターネットを利用して世界への無差別監視を実施しているという現実的な危

[1] https://www.cverc.org.cn/head/zhaiyao/news20240415-FTTF.htm

[2] https://www.cverc.org.cn/head/zhaiyao/news20240708-FTTFER.htm

害をよりはっきりと認識できるようになった。そうした事実を背景に、われわれは米政府機関が「ボルト・タイフーン」に関する偽情報を捏造し、「偽旗作戦」を組織・実施し、中国に対しサイバー攻撃を行っている客観的な証拠をより多く公開する必要がある。また、米国の「盗人猛々しい」姿や自作自演の茶番劇を引き続き暴き出さなければならない。

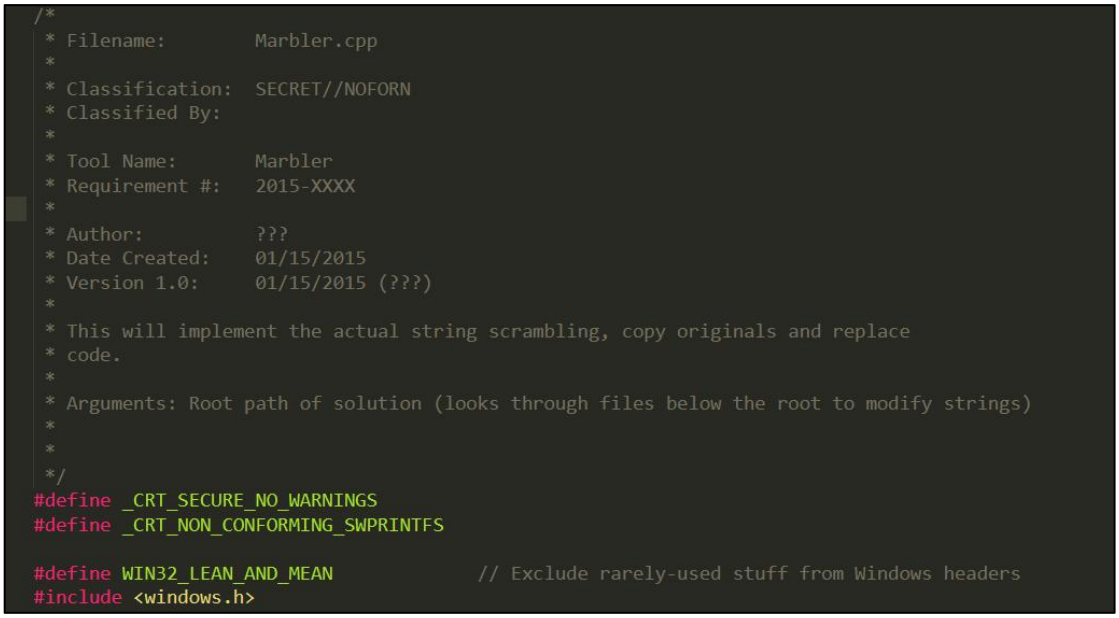
二、サイバー空間の「カメレオン」

周知のとおり、米国は世界最大の軍需品供給者である。大規模の軍事産業システムと力強い軍産複合体はすでに、米国の政治・経済・軍事政策を左右する基盤となっており、それによって築き上げられた米国のサイバー兵器庫は規模が大きく、形が多様であるとともに、複雑な機能と豊かな製品を持っている。この間、中国国家コンピューターウイルス緊急処理センターはすでに、米国家安全保障局（NSA）、中央情報局（CIA）が開発した複数のサイバー兵器を公表し、また、「中国西北工業大学がNSAによるサイバー攻撃を受けた事件に関する調査報告書」の中で、米国の関係情報機関がサイバー攻撃を仕掛ける際に利用した複数のサイバー兵器の機能や、高い隠ぺい性を持つ攻撃技術・戦術を詳しく分析したが、それらはあくまでも「ハッカー帝国」としての米国が有する巨大なサイバー兵器庫の「氷山の一角」にすぎない。

長期にわたり、米国はサイバー空間で「前方防御」戦略を積極的に推進し、「ハント・フォワード作戦(Hunt Forward)」を実施してきた。つまり、ライバル国の周辺

地域でサイバー軍を配置し、そうした国々のサイバー攻撃の対象に対し近接偵察と侵入テストを展開する。そういった戦術の需要に合わせて、米情報機関は別名「マーブル（Marble）」のツールキットを開発した。その役割は、自身の悪意あるサイバー攻撃行為を隠し、他国に濡れ衣を着せ、さらにトレーサビリティ分析をミスリードすることである。「マーブル」は、一種のフレームワークであり、その他のサイバー兵器開発プロジェクトと統合することができ、サイバー兵器開発者がプログラムのコードが持つ各種の識別可能な特徴を混乱させることをサポートし、サイバー兵器開発者の「指紋」を「ふき取る」ことができる。銃で喩えると、銃器のライフリングを変えることで、技術手段で弾丸がどの銃器から発射されたか追跡できないようにすることである。さらに、「マーブル」は、もう一つ「卑怯」な機能を持っている。それは、中国語やロシア語、朝鮮語、ペルシア語、アラビア語などの言語の文字列を自由に挿入できること。これは明らかに、調査員をミスリードし、中国やロシア、朝鮮、またはイランなどのアラビア国家に濡れ衣を着せる狙いである。

フレームワーク「マーブル」のソースコードとその注釈（図 1）によると、それは機密（しかも外国に漏らしてはいけない）武器研究開発計画に指定されており、遅くとも 2015 年からすでに始まっていた。明らかに、同計画は米情報機関が自身の需要に合わせて作り上げた「秘密兵器」であり、米国のいわゆる「同盟国」にさえ漏らしてはいけないものである。



```
/*
 * Filename:        Marbler.cpp
 *
 * Classification:  SECRET//NOFORN
 * Classified By:
 *
 * Tool Name:       Marbler
 * Requirement #:   2015-XXXX
 *
 * Author:          ???
 * Date Created:    01/15/2015
 * Version 1.0:     01/15/2015 (???)
 *
 * This will implement the actual string scrambling, copy originals and replace
 * code.
 *
 * Arguments: Root path of solution (looks through files below the root to modify strings)
 *
 *
 */
#define _CRT_SECURE_NO_WARNINGS
#define _CRT_NON_CONFORMING_SWPRINTFS

#define WIN32_LEAN_AND_MEAN             // Exclude rarely-used stuff from Windows headers
#include <windows.h>
```

図１　「マーブル」計画のソースコード

また、図 2・3・4・5 に示したように、フレームワーク「マーブル」は、100 種類以上の暗号化アルゴリズムを使って、ソースコードファイル内の識別可能な変数名や文字列を難読化し、また、特定の文字列を挿入し、ミスリーディングの役割を果たすことができる。

```
virtual int ScrambleW(wchar_t *wcToScramble, unsigned int iNumOfChars) = 0;

/*
    Args:
        cToScramble[in]: is the buffer containing a char string to scramble
        iNumOfChars[in]: the number of CHARs in the buffer

        Ret: > 0 == SUCCESS,  <=0 == FAILURE
*/
virtual int ScrambleA(char *cToScramble, unsigned int NumOfChars) = 0;


/*
    Args:
        cVarName[in]: the name of the variable being replaced
        cStringLiteral[in]: the string literal to be added to the insert (after scrambling)
        iNumOfChars[in]: the number of characters in the buffer
        cInsert[out]: the insert to replace CARBLE\BARBLE declaration in the c/cpp file

        Ret: > 0 == SUCCESS,  <=0 == FAILURE
*/
```

図 2　暗号化関数

```
virtual int ScrambleW(wchar_t *wcToScramble, unsigned int iNumOfChars) = 0;

/*
    Args:
        cToScramble[in]: is the buffer containing a char string to scramble
        iNumOfChars[in]: the number of CHARs in the buffer

        Ret: > 0 == SUCCESS,  <=0 == FAILURE
*/
virtual int ScrambleA(char *cToScramble, unsigned int NumOfChars) = 0;


/*
    Args:
        cVarName[in]: the name of the variable being replaced
        cStringLiteral[in]: the string literal to be added to the insert (after scrambling)
        iNumOfChars[in]: the number of characters in the buffer
        cInsert[out]: the insert to replace CARBLE\BARBLE declaration in the c/cpp file

        Ret: > 0 == SUCCESS,  <=0 == FAILURE
*/
```

図 3　暗号化アルゴリズム

```
        {
            if (bHasBackSlash)
                wsprintf(pszFullPath, L"%s%s", pszRoot, FindFileData.cFileName);
            else
                wsprintf(pszFullPath, L"%s\\%s", pszRoot, FindFileData.cFileName);

            //Process File
            if (PathMatchSpec(pszFullPath, L"*.c") || PathMatchSpec(pszFullPath, L"*.cpp") || PathMatchSpec(pszFullPath, L"*.h")
            {
                if (!PathMatchSpec(FindFileData.cFileName, L"Marble.*"))
                {
                    BOOL bProcessed = ProcessFile(pszFullPath, pMarblerList);

                    //Global Flag for error
                    if (!bProcessed)
                    {
                        g_bModificationError = TRUE;
                        wprintf(L"Error modifying file\n");
                    }
                }
```

図 4　ファイル処理機能関数

```
        if (pNode->eStringType == stCHAR)
        {
            int iResult = g_pScram->ScrambleA((CHAR *)lpbLine, iLineLen);
            if (iResult > 0)
            {
                if (VerifyScramRatio(pNode->eStringType, (LPBYTE)pNode->cString, lpbLine, iLineLen))
                {
                    iResult = g_pScram->CreateStringLiteralA(lpbLine, iLineLen, cLiteral);
                    if (iResult > 0)
                    {
                        iResult = g_pScram->GenerateInsertA(cVarName, cLiteral, iLineLen, cInsert);
                        if (iResult <= 0)
                            bModError = TRUE;
                    }
                    else
                        bModError = TRUE;
                }
                else bModError = TRUE;
            }
            else
                bModError = TRUE;
        }
        else
        {
            int iResult = g_pScram->ScrambleW((WCHAR *)lpbLine, iLineLen);
            if (iResult > 0)
            {
                if (VerifyScramRatio(pNode->eStringType, (LPBYTE)pNode->cString, lpbLine, iLineLen))
                {
                    iResult = g_pScram->CreateStringLiteralW((WCHAR *)lpbLine, iLineLen, cLiteral);
                    if (iResult > 0)
                    {
                        g_pScram->GenerateInsertW(cVarName, cLiteral, iLineLen, cInsert);
                        if (iResult <= 0)
                            bModError = TRUE;
                    }
```

図 5　ファイル処理機能関数（その 2）

さらに、「マーブル」のテストコードの実例から、故意に挿入された「外国語」の文字列が見つかった。いわゆる「外国語」には、アラビア語や中国語、ロシア語、朝鮮語、ペルシア語しか含まれていない（図 6）。

```
//Add foreign languages
//Arabic
WARBLE wcArabic[] = L" لى بيناتقى ل ال فى ل انضى غ ثوي ح علاتع و عمت جمل ا علنش ل الك شل لم ءهzل ود ٣٠ يفى عيط فو آلم أ دي
sb.Append((LPBYTE)wcArabic, 380);


//Chinese
WARBLE wcChinese[] = L"洴洕沘 烕煓瑐 鹿楁楕 謌 钃躔, 篶鬗齵 逯郹幁荏恴 潬滮湤 麖 踶鞨 洋絜泛 螭蜮謕 崞愊慄 榼 趏趆, 嵥 逳婖 蟷蠉蟞 鍮
sb.Append((LPBYTE)wcChinese, 266);


//Russian
WARBLE wcRussian[] = L"Зыд нэ нонюмэш контынтёонэж. Видэ бландит ан квуй, дуо декам эпикюре эа. Йн дйкит мольлиз дэльякатезш
sb.Append((LPBYTE)wcRussian, 550);


//Korean
WARBLE wcKorean[] = L"사용할 수있는 구절 많은 변화가 있지만, 대부분의, 주입 유머로, 어떤 형태의 변경을 입었거나 조금이라도 믿을 보이ス
sb.Append((LPBYTE)wcKorean, 288);

//Farsi
WARBLE wcFarsi[] = L" لورم ایپسوم کل طحنمل ( به ا ن گلی سک Lorem ipsum) به م تیآز مل ی شکو بیمعنی در عصت چ پ رآخفص
sb.Append((LPBYTE)wcFarsi, 1710);

lpbData = (LPBYTE)malloc(sb.GetUsedSize());
dwDataLen = sb.GetUsedSize();
memcpy(lpbData, sb.GetBufferAddress(), sb.GetUsedSize());

return;
```

図 6　ファイルの中に挿入された「外国語」

フレームワーク「マーブル」は、米情報機関が世界中で無差別で際限のないサイバースパイ活動を展開しており、また、「偽旗作戦」を実施することによって、調査員や研究者をミスリードし、ライバル国に濡れ衣を着せる狙いをはっきりと証明している。

上述の「偽旗作戦」は、ソースコードの特徴を隠すことにとどまらない。サイバー犯罪集団の攻撃技術・戦術を上手に真似することによって、米情報機関はさまざまな完璧のように見える「ポケット」組織をでっちあげた。この点に関しては 2 回目の報告書の中ですでに説明されている。

このように、米サイバー軍と情報機関のハッカーは、カメレオンのようにサイバー空間で他の身分を装い、他の国を「代表」して世界中でサイバー攻撃を行い、機密を盗み取り、さらに、米国の非「同盟国」に濡れ衣を着せるような行為を続けてきた。

信頼できる情報源によると、「偽旗作戦」は実際、米情報機関の「ダークパワー」（イギリスは「Online Covert Action」と呼ぶ）の重要な部分だという。米国と他の「ファイブ・アイズ（Five Eyes）」加盟国の機密文書によると、「ダークパワー」は主に、「偽情報作戦」と「技術的妨害行動」といった二つの面に分けられている。「技術的妨害行動」について、米国家安全保障局（NSA）は特別に「実施マニュアル」を作成した。「偽旗作戦」はまさにそのうちの重要な一部である。同時に、米国と他の「ファイブ・アイズ（Five Eyes）」加盟国の内部文書では、「ダーク

パワー」を実施する際に、「否認」「妨害」「中傷」「欺く」といった四つの主要な原則（「4D」原則）を守らなければならないと指摘した。この「4D」原則はちょうど、「ボルト・タイフーン」行動のすべてのコアとなる要素をカバーしている（図 7、図 8）。

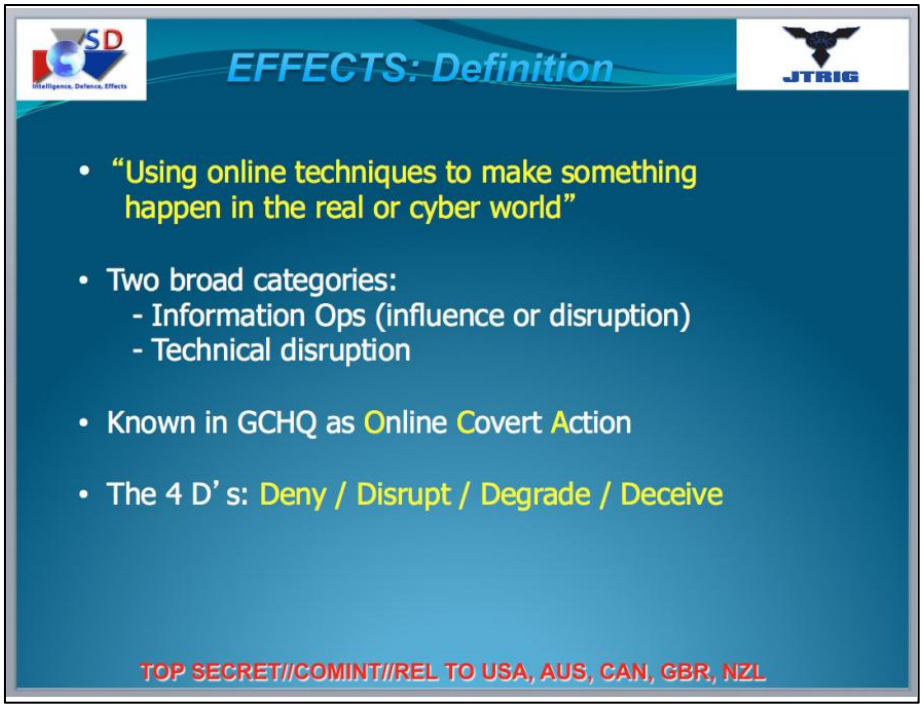


図 7　米国をはじめとする「ファイブ・アイズ（Five Eyes）」の「ダークパワー」に対する定義

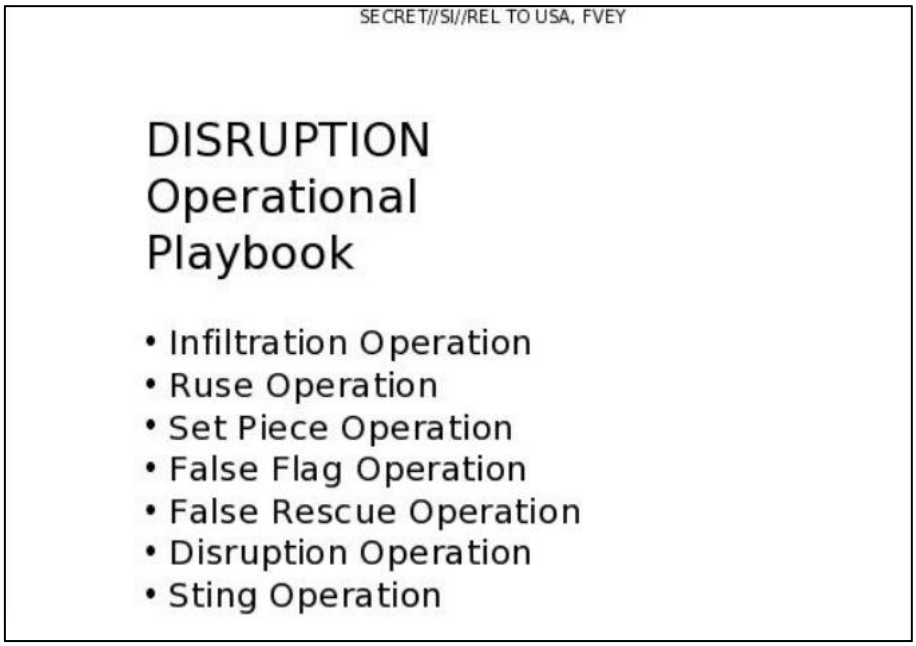


図 8　米国をはじめとする「ファイブ・アイズ（Five Eyes）」による「技術的妨害行動」に関する「実施マニュアル」

上述の証拠から、「ボルト・タイフーン」行動は典型的で巧妙に仕組まれた、米国の資本集団の利益に合致した偽情報作戦（いわゆる「偽旗作戦」）だという結論を導き出すことができる。その技術・戦術は米国をはじめとする「ファイブ・アイズ（Five Eyes）」加盟国の情報機関が「ダークパワー」で採った技術・戦術に完全に一致している。当然、そうした米国の国家レベルの情報機関によって巧妙に仕組まれた詐欺を見破るのはかなり難しい。判断を妨害する情報が多く存在するため、技術面の分析だけに頼っては絶対不十分であり、多方面の情報と関連資料を総合的に分析してこそ、米情報機関がうっかりしておかしたミスを見つけ、米国家安全保障局（NSA）と中央情報局（CIA）などの情報機関がでっち上げた陰険な計画を解明することができる。その経緯は、2024 年 4 月 15 日と 7 月 8 日に

発表された二つの報告書で説明されている（詳しくは「ボルト・タイフーン――米国の議会と納税者に対する米情報機関の陰謀的詐欺キャンペーン」「ボルト・タイフーン II――米国の議会と納税者に対する米政府機関の偽情報作戦の実態に迫る」をご参照ください）。

三、サイバー空間の「覗き見者」

2回目の報告書の中で、米国の連邦政府機関、とりわけ情報機関が引き続き外国情報監視法（FISA）第702条が容認する令状なしでの監視権限を持ち続けるために、外部からのサイバー脅威をでっちあげ、偽情報作戦を起こし、無差別で際限のない大規模な傍受計画を継続してきた政治スキャンダルが指摘された。本報告書は、上述の令状なし・無差別・際限なしの傍受計画の具体的な状況について引き続き解明していく。

（一） インターネットの要路を抑える

米国家安全保障局（NSA）の内部極秘資料によると（図9）、米国はインターネットの構築・整備における技術的優位性と地理的優位性に頼って、世界中最も重要な大西洋横断光海底ケーブルと太平洋横断光海底ケーブルなどのインターネットの要路をしっかりと抑え、国家レベルのグローバル通信傍受施設を立ち上げ、米連邦捜査局（FBI）やイギリス国家サイバーセキュリティセンター（NCSC）と密接に連携し、光ファイバーで伝送された全量データに対しプロトコル解析とデータ窃盗を展開し、世界中のインターネットユーザーに対する無差別監

視を実現してきた。

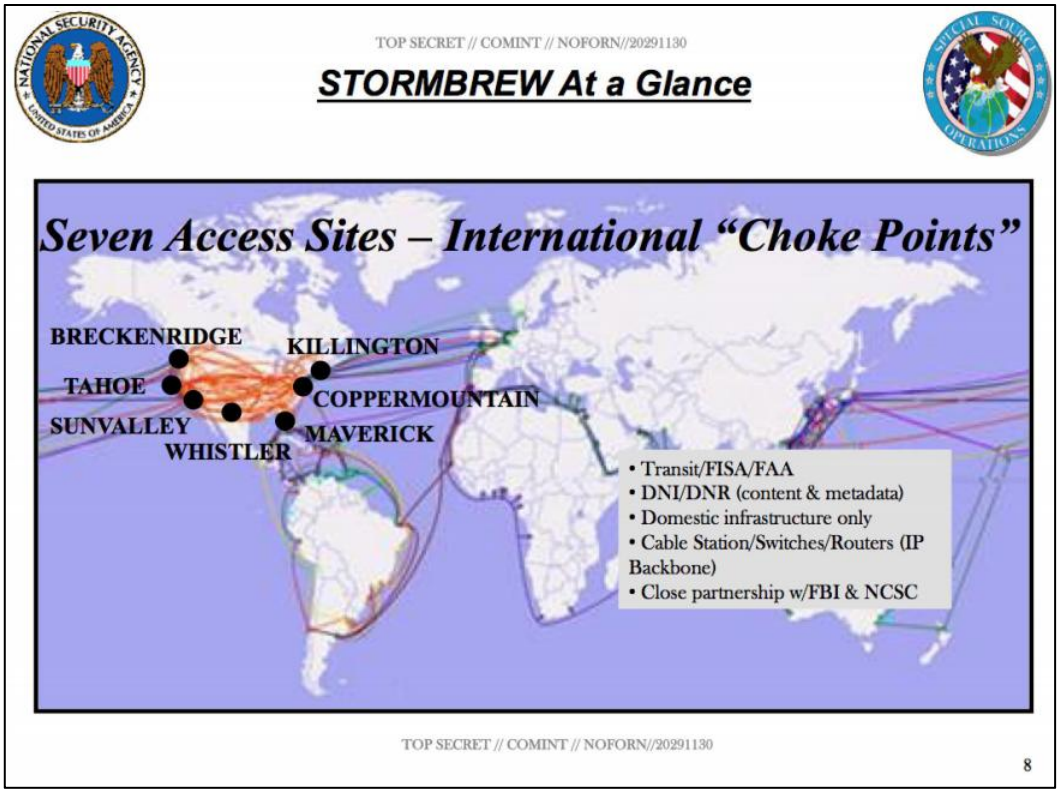


図 9　　NSA が運営する光海底ケーブル傍受施設

こうしたインターネットデータ傍受から利益を得た関係側が多い。米連邦政府情報機関や軍事組織のほかに、ホワイトハウスや内閣閣僚、在外公館、通商代表部、議会、さらに国務省、農務省、司法省、財務省、エネルギー省、商務省、国土安全保障省などの行政機関も含まれる。前回の報告書で指摘されたように、「ボルト・タイフーン」計画の参加者は、米情報機関に限らない。これは、米国資本の共通利益に奉仕するための計画であり、多くの米政府機関もそれを助長するような役割を果たしている（図 10）。

図 10　NSA 諜報サービスの「顧客」リスト

（二）インターネットデータを集積する「貯水池」

情報傍受の狙いは、識別可能なメッセージやデータを取得することである。そのため、光海底ケーブルで伝送されているデータをリアルに読み取り、検索できる情報に翻訳することは、米国家安全保障局（NSA）のもう一つの重要な活動である。だが、暗号化されたネットワーク通信データの占める割合の上昇を背景に、そうした活動は大きな困難に直面している。そのため、NSA は二つの重点プロジェクトを実施した。**一つ目は「上流（UpStream）」プロジェクト**。主な役割は前述の傍受施設で不正取得した光海底ケーブルの生の通信データをすべて保管し、巨大な規

模のデータの「貯水池」を作り上げること。この「貯水池」の中にある膨大なデータは、その後の情報処理作業プロセスの「上流」となっている。**もう一つは「プリズム（Prism）」プロジェクト。**主な役割は以下である。まずは「上流」プロジェクトの生データをインターネットアプリケーション別で分類し、通信内容を解析する。また、「上流」プロジェクトで取得した暗号化されたデータの解析難やデータの送受信される経路をすべてカバーできないことなど際立った課題を効果的に解決するため、「プリズム」プロジェクトが直接、米国の各大手インターネット企業のサーバーからユーザーのデータを取得するよう米政府は強制的に定めた。そのうち、マイクロソフト、ヤフー、グーグル、フェイスブック（現 Meta）、アップルなどの企業が含まれている。上述の二つのプロジェクトはいずれも、外国情報監視法（FISA）第 702 条の権限の下で実施されているものである。第 702 条は米情報機関が米連邦政府を代表して、世界中のインターネット回線データを合法で公開的、持続的に盗聴する公式的根拠となっている一方、米国が「盗聴帝国」であることの堅実で言い逃れることのできない証拠となっている（図 11）。

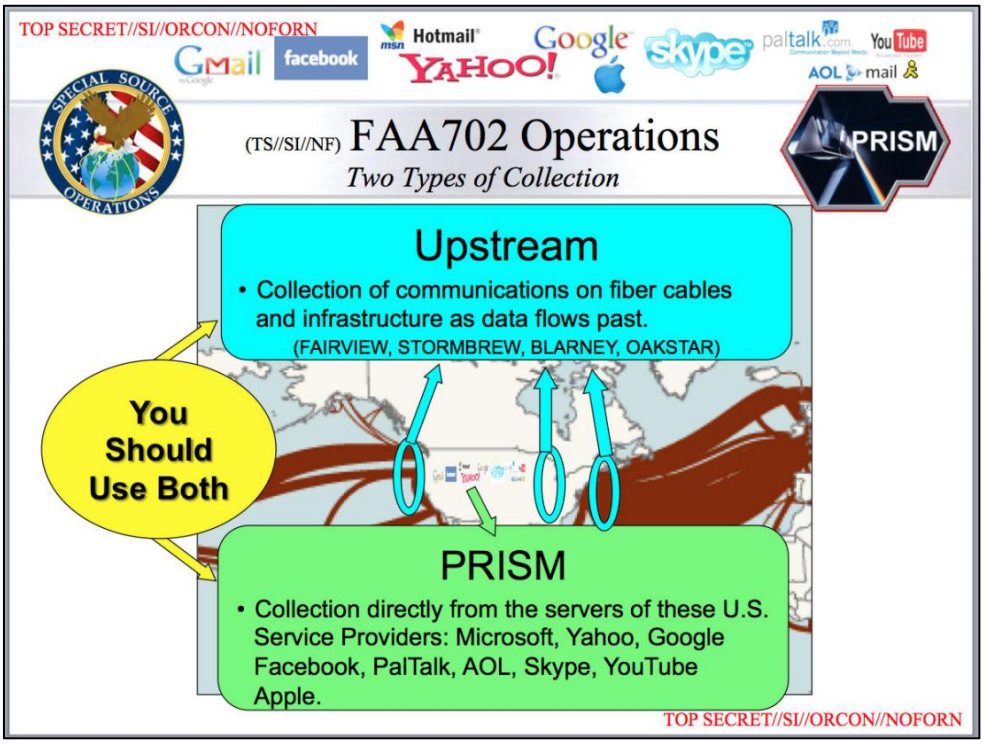


図 11　NSA が実施した世界中のインターネット通信を監視する二つの重点プロジェクト

（三）インターネットデータの「源」に潜入

米国家安全保障局（NSA）はすでにグローバルインターネットで大規模な傍受システムを配備したが、そうしたシステムの傍受対象とネットワーク通信内容は、光海底ケーブルがカバーした一定のエリアにとどまったら、収集したデータは NSA の情報活動の需要を全く満たせない。そのため、NSA は傍受システムの「死角」に位置する特定の対象に対し、「コンピューター・ネットワーク・エクスプロイテーション」（CNE）を実施している。NSA に所属する悪名高い「TAO」（Tailored Access Operations、タオ）はまさに、その作戦を実施する組織である。NSA の極秘文書

から、「TAO」が世界中でCNEを無差別に実施し、5万件以上のマルウェアを送り込んだ。被害者は主に、アジア、東ヨーロッパー、アフリカ、中東、南米に集中していることがわかった。また、NSA の内部文書から、中国の主要都市はほとんど、CNE の範囲内にあり、大量のインターネット資産が侵入された。当然、前回の報告書で言及された中国西北工業大学と武漢市地震観測センターの所在地も含まれている。前述のマルウェアの指令統制センターの多くは、日本や韓国、**グアム**、ハワイなど米国外の米軍事基地に位置している。**グアム**について、前の二つの報告書を読んだ読者にはなじみがあるはずだ。米政府がでっちあげた「ボルト・タイフーン」にまつわるデマの発祥地で、「ボルト・タイフーン」偽情報作戦によってサイバーセキュリティ発展の歴史に記録されている。だが実際、**グアム**の米軍事基地はそもそも「ボルト・タイフーン」サイバー攻撃の被害者ではなく、逆に、中国や東南アジアの多くの国に対するサイバー攻撃を起こした者であり、不正取得されたデータの回収センターでもある（図 12、13）。

その他の国の防御レベルの高く、侵入が難しく、価値の高い攻撃対象に対し、NSA の「TAO」は直接、サプライチェーン攻撃を実施している。これは、サイバーセキュリティ技術や製品の分野における米国の優位性に基づき、米大手インターネット企業や設備サプライヤーの協力の下で、配送ルートで攻撃対象を傍受し、また攻撃対象にインターネット接続サービスを提供する業者が仕入れたネットワーク関連製品を捕獲し、その製品を解体してバックドアを仕掛けた後、配送ルートに戻して攻撃対象に届ける方法である。この方法は普通、他国のプロバイダーに対する攻

撃活動に使われており、攻撃対象となるプロバイダーの通話料金管理システムなどへの侵入を実現することで、攻撃対象の携帯の通話内容への傍受を実現することができる。中国の西北工業大学がNSAの「TAO」によるサイバー攻撃を受けた事件の中で、中国国内に位置するプロバイダーは前述のような攻撃を受けていた。攻撃対象の通話内容やネット閲覧履歴、現実世界での行動軌跡はすべて、NSAの「TAO」にリアルタイムで監視されていた（図 14）。

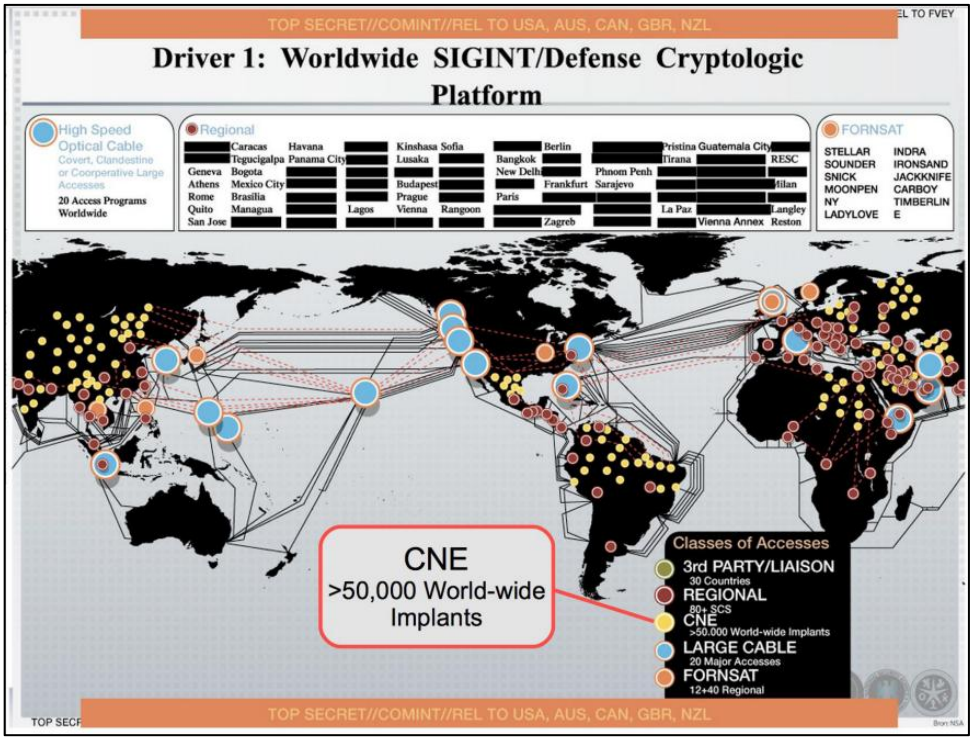


図 12　NSA に所属する「TAO」によるグローバルネットワークへの侵入行動の見取図

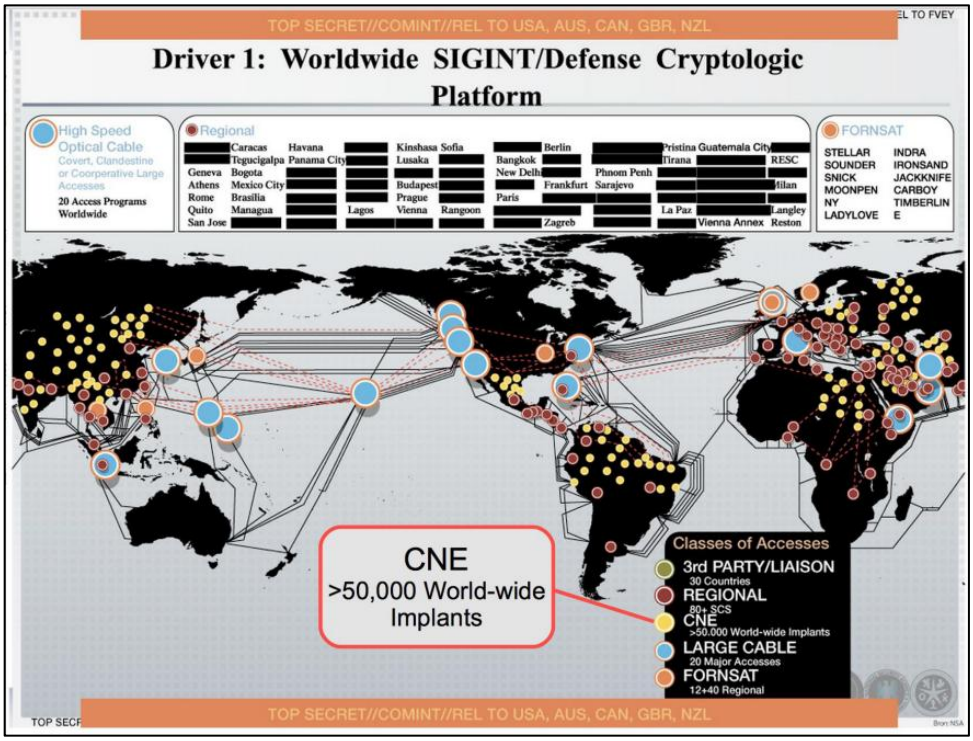


図 13　NSA に所属する「TAO」による中国のネットワークへの侵入行動の見取図

(TS//SI//NF) Such operations involving **supply-chain interdiction** are some of the most productive operations in TAO, because they pre-position access points into hard target networks around the world.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

図 14　攻撃対象が購入した米通信大手「シスコシステムズ」の

ネットワーク関連設備を開けて、バックドアを仕掛ける「TAO」の

技術者たち

皮肉にも、NSA がこうしたサプライチェーン攻撃を説明する際に、戦術用語「待ち伏せ」を意味する「pre-position」という表現を使った。これは、傍受対象が使用するインターネット製品でバックドアを仕掛けることを指しており、NSA のその後の攻撃やとコントロール、機密の不正取得活動に伏線を張った。また、「ボルト・タイフーン」組織がグアムなどに位置する米国の「重要インフラ」にサイバー攻撃を実施した際に使われた戦術を説明する時、米連邦政府機関も「pre-position」という表現を使っていた。では、いったい誰が世界中で整備された重要インフラの中で「待ち伏せ」をしたのか。その真相はもはや言うまでもないものである。

（四）インターネット情報を際限なく取得

第 702 条により、米情報機関は大規模のグローバルなインターネット監視網を築き上げ、米政府機関に大量の価値の高い情報を提供してきた。これによって米国政府はたびたび、外交・軍事・経済・科学技術などの分野で先手を取ることができた。第 702 条と関連するインターネット監視システムはすでに、現段階において米国が自らの覇権地位を守る「秘密兵器」となっている。こうした技術面の大きな先発優位性を持った米連邦政府と情報機関はますます大っぴらに悪事を働くようになり、いかなる目標でも「重点監視対象リスト」に入れられる恐れがある。以下、事実をまとめてながら説明していく。

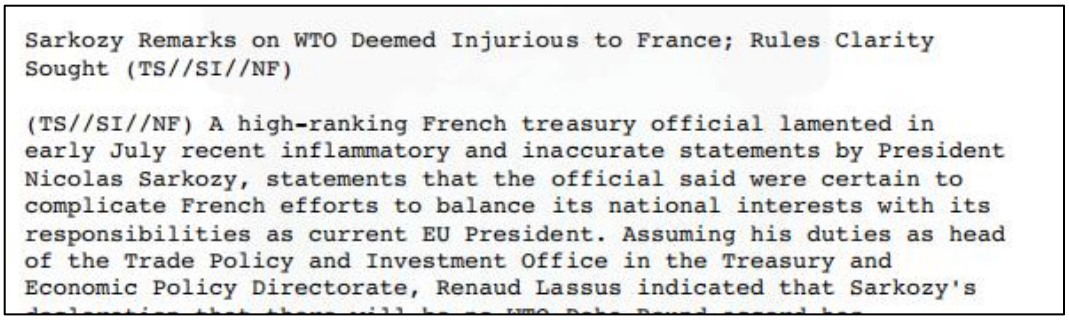
１．フランス

2004 年から 12 年にかけて、米国はフランスに対し長期的なスパイ活動を実施していた。傍受の内容はフランス政府の政策や外交、金融、国際交流、インフラ整備、ビジネス、貿易活動など多岐にわたっていた。そのうち、一部の重要な情報は米国の承認の下で、他の「ファイブ・アイズ」加盟国に共有された。つまり、「ファイブ・アイズ」加盟国も米国のスパイ活動から利益を得たことを証明している。米国によるフランスへのスパイ活動の傍受記録で、フランスのコアとなる政治部門や経済部門の電話や、フランス大統領官邸の電話などが含まれていた。暴かれた米情報機関の機密文書の中で、フランス政府高官の対話や通信内容を傍受して取得した極秘情報のダイジェストが複数盛り込まれている。傍受対象には、フランスの元大統領（図 15）や財務相、外務相、上院議員、財務と経済政策省官僚、在米フランス大使、EU の貿易政策を直接担当する官僚などがいた。

情報の内容は、世界貿易機関（WTO）や環太平洋パートナシップ協定（TPP）、G7、G20 に関わるフランス政府の関係政策と考慮、またはフランスの財政予算やフランス自動車産業の衰退状況、フランスの企業がイラクの石油食料交換プロジェクト（Oil-for-Food）計画に参加した状況などが含まれている。

米国は、上述の行動を実施する経済スパイに出した指示の中で、電気通信・電力・天然ガス・石油・原子力・再生可能エネルギー・環境技術・医療技術に関するフランスのすべての重要プロジェクトの販売と融資情報を収集するよう明確に

要求した。また、価値が 2 億ドルを超えるすべてのフランス企業の契約や交渉を遮断（窃取）するよう求めた。BNP パリバ銀行（BNP Paribas）や生命保険会社アクサ（AXA）、クレディ・アグリコル、プジョー（Peugeot）、ルノー（Renault）、トータルエナジーズ（Total）、電気通信事業者オレンジ（Orange）などのフランスの大手企業とフランスの主要な農業協会に直接影響を与えた。表 1 は、米国家安全保障局（NSA）がフランスに対するスパイ活動の中で取得した一部の情報のダイジェストを示している。



Sarkozy Remarks on WTO Deemed Injurious to France; Rules Clarity Sought (TS//SI//NF)

(TS//SI//NF) A high-ranking French treasury official lamented in early July recent inflammatory and inaccurate statements by President Nicolas Sarkozy, statements that the official said were certain to complicate French efforts to balance its national interests with its responsibilities as current EU President. Assuming his duties as head of the Trade Policy and Investment Office in the Treasury and Economic Policy Directorate, Renaud Lassus indicated that Sarkozy's

図 15　フランスのサルコジ元大統領に対する NSA の傍受記録

表 1 当時在任中のフランス政府関係者に対する米国家安全保障局（NSA）の一部の傍受記録

時期	情報種類	情報内容

時期	情報種類	情報内容
2004 年	ワシントン駐在フランス大使の情報	ワシントン駐在フランス大使は Oil-for-Food（OFF）計画から利益を得たとされる米国企業のリストを公表する予定だった。
2006 年	フランス政府上層部の通信情報	当時のシラクフランス大統領とフランス外相は、国連の任命に関する事項について話し合った。
2008 年	フランス政府上層部の通信情報	フランス経済・財務相は、当時のサルコジフランス大統領が「WTO 交渉の合意がフランスに悪影響を与える可能性がある」と述べたことに不満を抱いていた。
2008 年	フランス政府上層部の通信情報	当時のサルコジフランス大統領は、世界経済危機の責任を米国に帰し、フランスが先頭に立って世界金融システムの改革を求める考えを示した。

時期	情報種類	情報内容
2010年3月24日	フランス政府上層部の通信情報	ワシントン駐在のフラン大使とフランス大統領の外交顧問との対話：当時のサルコジフランス大統領が2010年3月31日にオバマ米大統領との会談で、次のいくつかの敏感な話題を提起しようとしていた。 具体的には、米国がフランスへの傍受能力を制限させる懸念がある二国間情報協力協議から離脱すること、フランスがアフガニスタンに軍事訓練機の提供を約束する可能性があること、欧州航空防衛宇宙会社（EADS）が米国軍側と空中給油機提供契約を締結する可能性があること、フランスのスピリッツメーカーであるペルノ・リカール（Pernod Ricard）に関する商標トラブルなど。

時期	情報種類	情報内容
2011 年 6 月 10 日	フランス政府上層部の通信情報	当時のサルコジフランス大統領とフランス外相との談話：サルコジ大統領はイスラエルとパレスチナ問題について強硬な発言をした。
2011 年 8 月 2 日	フランス政府上層部の通信情報	ワシントン駐在のフランスと EU の官僚との談話：米国の貿易政策を強く批判し、TPP（環太平洋パートナーシップ協定）は中国に対抗するものであると主張していた。

時期	情報種類	情報内容
2012 年 5 月 22 日	フランス政府上層部の通信情報	フランス政府内部では、持続的なユーロ圏危機がフランスの利益とフランス企業の景況に悪影響を与えることが懸念されており、特にギリシャのユーロ圏離脱問題に対する心配があった。当時のオランドフランス大統領は、当時のメルケルドイツ首相の危機問題に対する強硬な姿勢に不満を示し、メルケル氏が知らない状況の下に、フランスの官僚がドイツの野党議員と秘密会議を開催し、危機問題について議論することに賛成した。
2012 年 7 月 31 日	フランス政府上層部の通信情報	フランス財務相とフランス議会上院議員の対話：フランス財務相が「フランス経済が苦境に陥っており、今後 2 年間の状況は非常に厳しいと見込まれる」と述べた。

時期	情報種類	情報内容
2012 年	フランスに対する米国のスパイ命令	フランスに対して長期にわたる経済スパイ活動が行われると要求し、フランス会社の経済活動の詳細やフランス政府の経済政策、決定などの情報を入手しようとしていた。その内容は、フランスと米国やその他の国、国際機関との経済関係、フランスの金融・貿易政策、主要 8 カ国首脳会議（G8）や主要 20 カ国首脳会議（G20）の議事に対するフランスの見解などに及んでいた。

時期	情報種類	情報内容
2012 年	フランスに対する米国の経済スパイ命令	フランスの電気通信・電力・天然ガス・石油・原子力・再生可能エネルギー、さらには環境技術および医療技術に関するすべての重大なプロジェクトの販売や融資情報を収集しようと米スパイに指示し、価値が 2 億ドルを超えるすべてのフランス企業の契約と交渉を遮断し、関連情報を報告するよう求めた。関連情報は米国の各貿易、政治、情報機関に送付される。
2012 年	フランス政府関係者会議の議事情報	フランス財務省は経済・財務・産業相のために、主要 7 カ国首脳会議（G7）と主要 20 カ国首脳会議（G20）での発言要項を起草し、その内容には米国銀行業改革への督促や、戦略石油備蓄に関する米国のイニシアチブへの支持計画などが含まれていた。

2．ドイツ

米国家安全保障局（NSA）の機密文書によると、ドイツ連邦情報局（BND）やドイツ連邦憲法擁護庁（BfV）などの情報機関は、何度も米国の情報機関と協力し、欧州ひいてはドイツ国内での傍受活動[3]を展開してきた。また、米中央情報局（CIA）と共同でスイスにある暗号化技術会社 Crypto AG を買収・経営し、傍受の対象にバックドア付きの暗号化製品[4]を提供しているにもかかわらず、米国は依然としてドイツを「ファイブ・アイズ」から除外し、「利益パートナーでもあり、傍受の対象でもある」という第三レベルのパートナーに位置づけ、ドイツに対して深い不信感を抱いている。

実際、米陸軍、空軍、海軍および米国家安全保障局(NSA)は、ドイツや他の欧州諸国を監視するため、大量の秘密情報ステーションをドイツに設置している（図 16）

[3] https://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

[4] https://www.theguardian.com/us-news/2020/feb/11/crypto-ag-cia-bnd-germany-intelligence-report

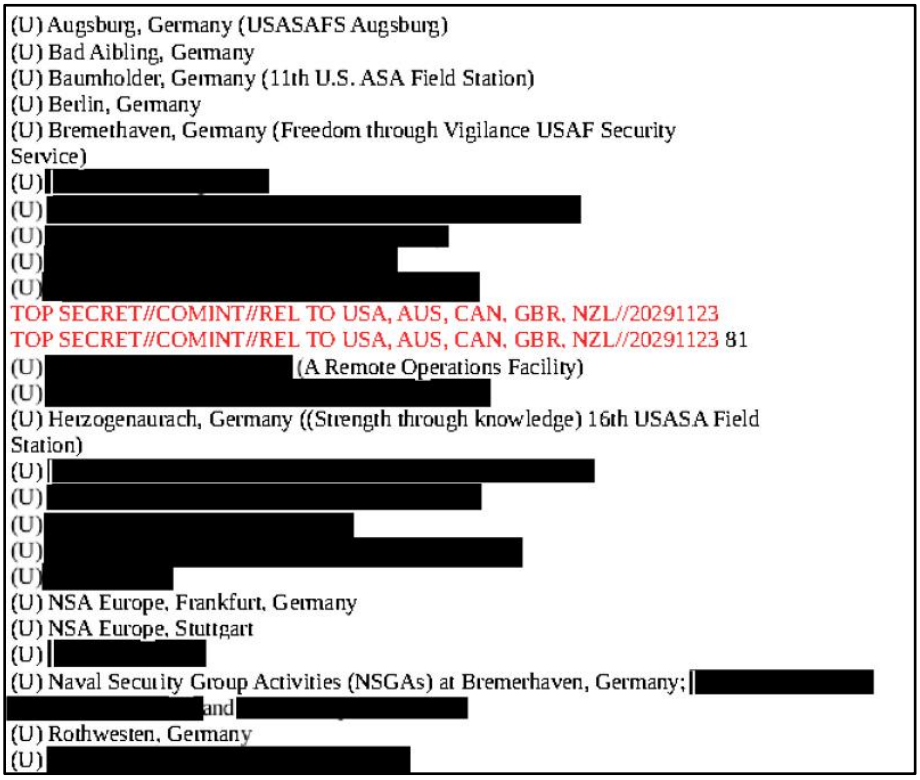
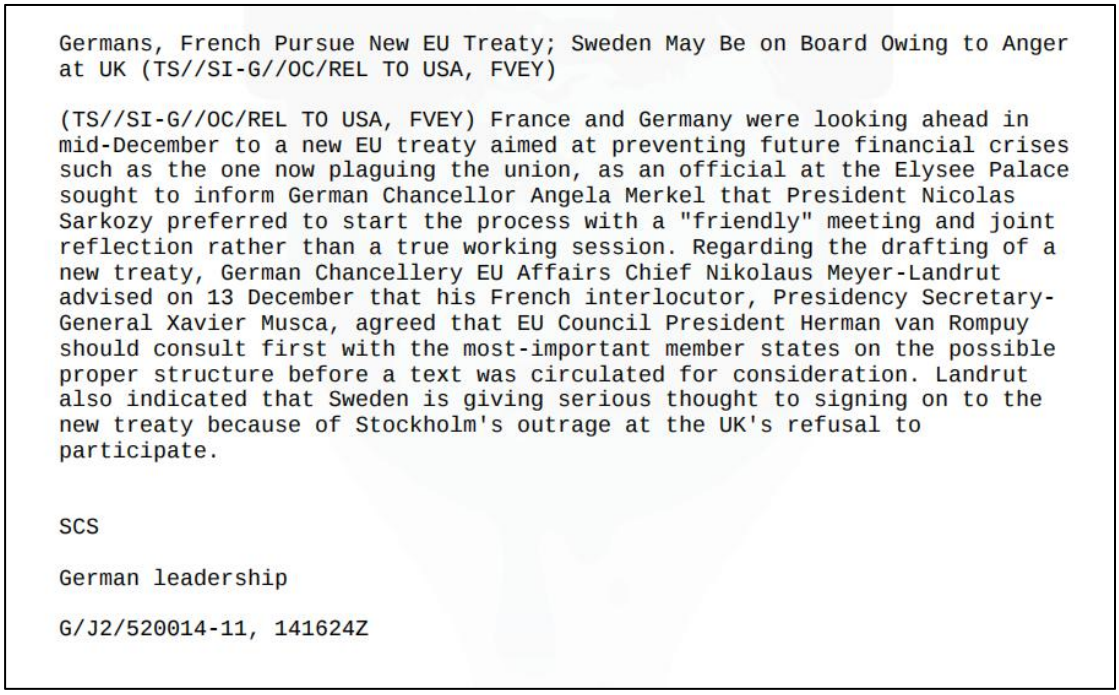

(U) Augsburg, Germany (USASAFS Augsburg)
(U) Bad Aibling, Germany
(U) Baumholder, Germany (11th U.S. ASA Field Station)
(U) Berlin, Germany
(U) Bremethaven, Germany (Freedom through Vigilance USAF Security Service)
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123 81
(U) [redacted] (A Remote Operations Facility)
(U) [redacted]
(U) Herzogenaurach, Germany ((Strength through knowledge) 16th USASA Field Station)
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) [redacted]
(U) NSA Europe, Frankfurt, Germany
(U) NSA Europe, Stuttgart
(U) [redacted]
(U) Naval Security Group Activities (NSGAs) at Bremerhaven, Germany; [redacted] and [redacted]
(U) Rothwesten, Germany
(U) [redacted]

図 16 米国情報機関がドイツに設置した秘密情報ステーション

米国家安全保障局（NSA）は長期にわたりドイツの首相、外相、在外公使、総領事らの政府高官の通信内容を傍受しており、その傍受内容は多岐にわたる。その中には、ドイツ政府の国際情勢や突発事件に対する見解、およびドイツ政府関係者が対米国際交流に参加した後のプライベートな会話も含まれており、政治、軍事、経済、外交、政策、民族、安全、資源などの重要な分野に関わる。特に注目すべきは、米国の情報収集部門が EU 諸国の内部事情、特に金融リストの防止策に強い関心を持っていることだ。（図 17）



Germans, French Pursue New EU Treaty; Sweden May Be on Board Owing to Anger at UK (TS//SI-G//OC/REL TO USA, FVEY)

(TS//SI-G//OC/REL TO USA, FVEY) France and Germany were looking ahead in mid-December to a new EU treaty aimed at preventing future financial crises such as the one now plaguing the union, as an official at the Elysee Palace sought to inform German Chancellor Angela Merkel that President Nicolas Sarkozy preferred to start the process with a "friendly" meeting and joint reflection rather than a true working session. Regarding the drafting of a new treaty, German Chancellery EU Affairs Chief Nikolaus Meyer-Landrut advised on 13 December that his French interlocutor, Presidency Secretary-General Xavier Musca, agreed that EU Council President Herman van Rompuy should consult first with the most-important member states on the possible proper structure before a text was circulated for consideration. Landrut also indicated that Sweden is giving serious thought to signing on to the new treaty because of Stockholm's outrage at the UK's refusal to participate.

SCS

German leadership

G/J2/520014-11, 141624Z

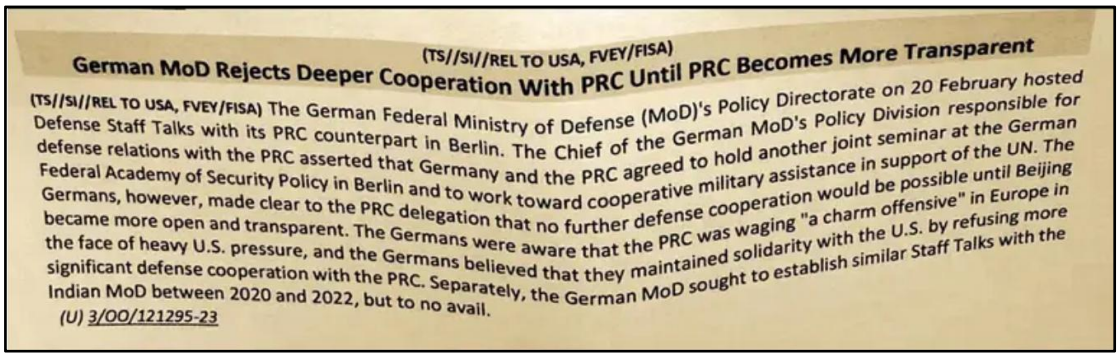
図 17 ドイツ政府指導者に対する米国家安全保障局（NSA）の傍受記録

スノーデン事件発生後も、米国はドイツへの傍受を緩めることなく、より隠れた方法を採用している。2021 年 5 月、デンマークメディア[5]は、米国家安全保障局（NSA）がデンマーク国防情報局（FE）と協力し、デンマーク経由のインターネット回線に対する通信傍受を暴露した。傍受の対象には、ドイツやスウェーデン、ノルウェーとフランスの国家指導者、高級政治家と高級官僚が含まれていた。その中には、当時のドイツ首相メルケル氏や外相のフランク・ワルター・シュタインマイヤー氏、野党党首のベルシュタインブリュック氏などが含まれ、彼らはすべて米国家安全保障局の米・デンマーク協力傍受プロジェクトの主要な傍受対象であった。また、

[5] https://www.dr.dk/nyheder/indland/forsvarets-efterretningstjeneste-lod-usa-spionere-mod-angela-merkel-franske- norske

この傍受プロジェクトを主宰していたのは、当時の米国副大統領で、今の大統領であるジョー・バイデン氏だ。

この傍受プロジェクトがメディアに暴露された後、再びドイツやフランスなどの欧州諸国の不満を引き起こした。当時のメルケルドイツ首相とマクロンフランス大統領は、同盟国に対する米国の傍受活動について「受け入れられない」と公に表明した。しかし、米国は明らかにこれらのいわゆる「同盟国」の感情を気にかけていないようだった。2023 年 4 月には、ドイツ連邦国防省に対する米国の傍受活動が再び暴露された[6]。



(TS//SI//REL TO USA, FVEY/FISA)

German MoD Rejects Deeper Cooperation With PRC Until PRC Becomes More Transparent

(TS//SI//REL TO USA, FVEY/FISA) The German Federal Ministry of Defense (MoD)'s Policy Directorate on 20 February hosted Defense Staff Talks with its PRC counterpart in Berlin. The Chief of the German MoD's Policy Division responsible for defense relations with the PRC asserted that Germany and the PRC agreed to hold another joint seminar at the German Federal Academy of Security Policy in Berlin and to work toward cooperative military assistance in support of the UN. The Germans, however, made clear to the PRC delegation that no further defense cooperation would be possible until Beijing became more open and transparent. The Germans were aware that the PRC was waging "a charm offensive" in Europe in the face of heavy U.S. pressure, and the Germans believed that they maintained solidarity with the U.S. by refusing more significant defense cooperation with the PRC. Separately, the German MoD sought to establish similar Staff Talks with the Indian MoD between 2020 and 2022, but to no avail.

(U) 3/OO/121295-23

図 18 ドイツ連邦国防省に対する米国家安全保障局の傍受情報記録

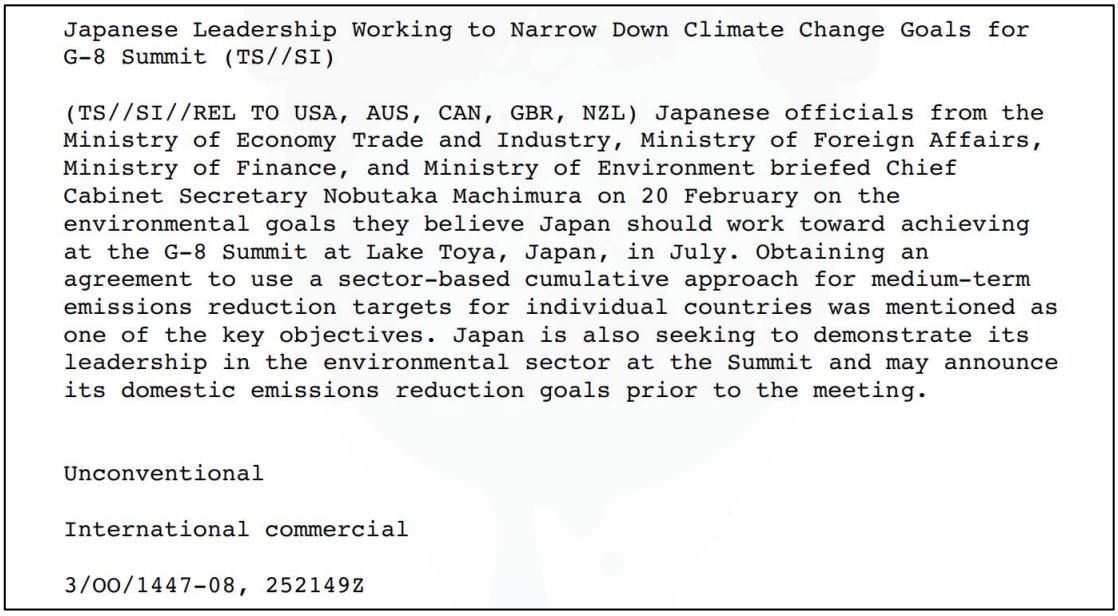
米国家安全保障局の極秘文書（図 18）が示すように、この傍受活動は、2023 年 2 月 20 にドイツ連邦国防省と訪問中の中国国防部代表団との間で行った軍事的外交会議に関わる。傍受記録によると、米国はドイツが中国との軍事分野における協力についてどのような見解や立場を持っているかに重点を置いてい

[6] https://www.tagesschau.de/investigativ/kontraste/pentagon-papiere-leaks-bundesverteidigungsministerium- 100.html

る。

3．日本

米国家安全保障局（NSA）の対外盗聴データベースには、日本に関する重要な政治・経済分野の傍受対象者リストが含まれている。このリストから、NSA が日本内閣、政府部門および大手財団に対してスパイ・傍受活動を行ったのは、安部政権に遡ることができると読み取られる。電話盗聴の対象者には、日本内閣オフィスの交換台、当時の内閣官房長官であった菅義偉氏の行政秘書、日本中央銀行内部の多くの官僚、三菱商事の天然ガス部門、三井物産の石油部門などが含まれている。その中で、「日本が G8 サミットで発表する予定の気候変動対応の機密提案」（図 19）という情報には、「REL TO USA，AUS，CAN，GBR，NZL」というマークが付けられており、この情報が「ファイブ・アイズ」同盟国と共有できることを米政府上層部から正式に許可されていることを示している。これは、「ファイブ・アイズ」同盟国が日本を対象とした専門的な計画を策定するための条件を整えていることを意味している。日本政府機関からひそかに盗聴された疑いがある関連情報は、米政府が日本政府に対する傍受活動の幅広さを示している。具体的な内容としては、農産物輸入や貿易紛争、世界貿易機関(WTO)ドーハ交渉における日本の立場、日本の気候変動対策、原子力とエネルギー政策、炭素排出計画、日本と国際エネルギー機関（IEA）などの国際機関との通信、および安倍晋三元首相官邸で行われた首相記者会見などの重要な情報が含まれている。実際の状況はそれだけではない。



Japanese Leadership Working to Narrow Down Climate Change Goals for G-8 Summit (TS//SI)

(TS//SI//REL TO USA, AUS, CAN, GBR, NZL) Japanese officials from the Ministry of Economy Trade and Industry, Ministry of Foreign Affairs, Ministry of Finance, and Ministry of Environment briefed Chief Cabinet Secretary Nobutaka Machimura on 20 February on the environmental goals they believe Japan should work toward achieving at the G-8 Summit at Lake Toya, Japan, in July. Obtaining an agreement to use a sector-based cumulative approach for medium-term emissions reduction targets for individual countries was mentioned as one of the key objectives. Japan is also seeking to demonstrate its leadership in the environmental sector at the Summit and may announce its domestic emissions reduction goals prior to the meeting.

Unconventional

International commercial

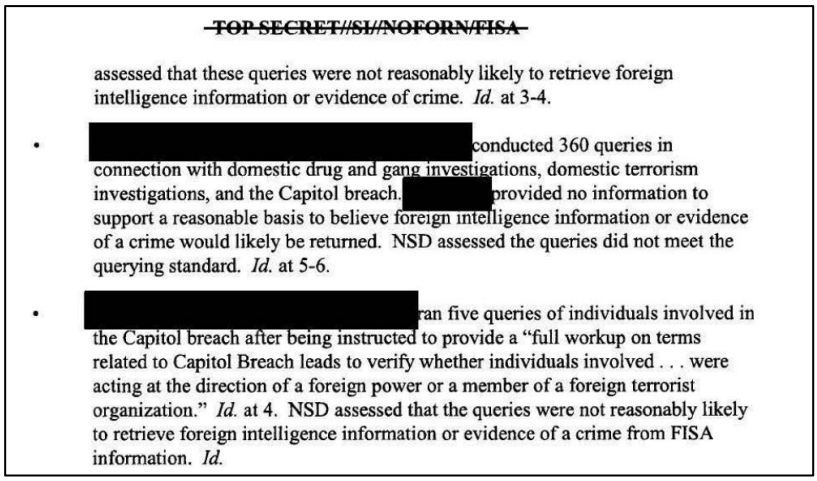
3/OO/1447-08, 252149Z

図 19 日本の指導者に対する NSA の傍受記録

4．米国の一般市民

私たちは 2 回目の調査報告書で、米国民間において外国情報監視法第 702 条に反対する正義の声がよく聞かれることを明らかにした。一見すると、NSA などの情報機関の情報収集活動は、米国外の外国人のみを対象としていると第 702 条は主張しているが、上述した NSA の傍受計画の技術的な方針からは、これらの傍受計画の全体的な目標が、世界中のインターネットユーザーのすべての通信データを不正に取得することであり、米国国内の一般市民を含むことが明らかだ。ただし、NSA などの情報機関は、情報分析者に対して「情報検索スクリーニング条件（Selector）」を設定する際には、「できるだけ」米国国内の一般市民や外国に滞在する米国民に関与しないよう求めている。しかし、このような措置はほぼ完全に「自律」に任せているため、実質的には形骸化されたものだと言えるだろう。

2023 年 5 月 19 日、米外国情報監視裁判所は一つの文書[7]を公開し、米情報機関がかつて数千回にわたり第 702 条に違反した行動（図 20）を実施していたことを明らかにした。特に、米連邦捜査局（FBI）は外国情報を収集する際、何度も通信とネット傍受ツールを濫用し、2021 年 1 月 6 日に勃発した「米議事堂襲撃事件」や 2020 年に発生した「米国ブラック・ライヴズ・マター自発的権利擁護抗議活動」に関与する米国民に対して傍受活動を行っていたことが摘発された。この裁判所の文書はその後メディアによって公開され、人々の疑念[8]を引き起こした。実際、当時の米国の「ウォール街占拠運動」では、FBI、NSA、中央情報局（CIA）などが平和集会の場にいるすべての人々や連絡者を対象とし、無差別に傍受を行っていた。その後、これらの手段は中国台湾地区の「太陽花」学運や中国香港地区の「セントラル（中環）占拠」不法集会に応用された。このことから、米国の一般市民に対する傍受は決して欠けていないことが分かった。



~~TOP SECRET//SI//NOFORN/FISA~~

assessed that these queries were not reasonably likely to retrieve foreign intelligence information or evidence of crime. *Id.* at 3-4.

- [redacted] conducted 360 queries in connection with domestic drug and gang investigations, domestic terrorism investigations, and the Capitol breach. [redacted] provided no information to support a reasonable basis to believe foreign intelligence information or evidence of a crime would likely be returned. NSD assessed the queries did not meet the querying standard. *Id.* at 5-6.
- [redacted] ran five queries of individuals involved in the Capitol breach after being instructed to provide a "full workup on terms related to Capitol Breach leads to verify whether individuals involved . . . were acting at the direction of a foreign power or a member of a foreign terrorist organization." *Id.* at 4. NSD assessed that the queries were not reasonably likely to retrieve foreign intelligence information or evidence of a crime from FISA information. *Id.*

[7] https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf

[8] https://thehill.com/policy/national-security/4012650-fbi-misused-surveillance-tool-fisa-section-702/

図 20 米外国情報監視裁判所の公開文書に記録された第 702 条に違反した事例

このようなネット上の傍受問題が頻発している要因は、米国の情報機関が第 702 条を実行する際、非常に緩やかな姿勢を維持していることにある（図 21）。米情報機関の内部トレーニング資料によれば、情報分析者が業務中に一般市民の個人情報を「偶然」に発見した場合、それは規定違反とは見なされず、報告する必要すらもないことが明らかにされている。

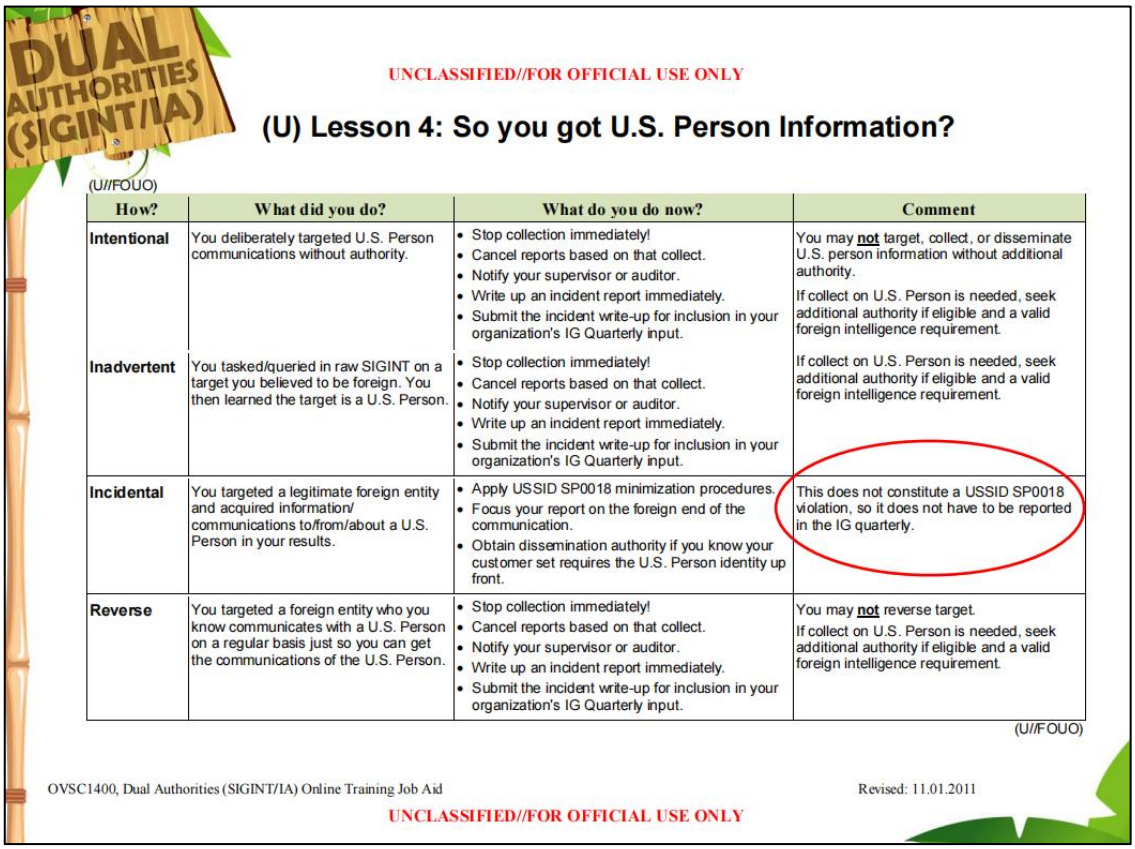


図 21 米情報機関の第 702 条のコンプライアンス要求に関するトレーニング材料

上述したケースから見ると、米国のグローバルネットワーク傍受計画と傍受ステーションは、ネットワークスペースのどこにでも存在する「覗き見者」のように、リアルタイムで世界中のインターネットユーザーのデータを盗み取っている。この傍受能力は、米国が「マトリックス」と「窃盗帝国」を構築するために不可欠な礎となっていることが分かった。このような膨大な傍受計画を維持するためには、毎年の必要な経費予算は驚くべきものとなり、インターネットデータの爆発的な増加に伴って、米国のグローバルネットワーク傍受計画の必要な経費も間違いなく急騰していくと考えられる。これは、米連邦政府とその情報機関と連携して「ボルト・タイフーン」計画の捏造行動を策定・推進する原動力となっている。

米国の政治家が私利のために連邦議会を欺く事例はしばしば見受けられる。「ボルト・タイフーン」計画捏造行動で重要な役割を果たした米連邦捜査局（FBI）のクリストファー・レイ局長はまさにその常習者である。2022 年 7 月、クリストファー・レイは米司法省長官のメイリック・カーランと共に、現職の米大統領バイデンの息子の犯罪の証拠を隠滅したため、上院議員からの質問[9]を受けた。2023 年 8 月には、クリストファー・レイは再び連邦議会に偽造のメモ[10]を提出したため、複数の下院議員から質問を受けた。2024 年 7 月、トランプ前大統領の銃撃事件に関する米議会の公聴会において、クリストファー・レイはまた偽証し、トランプ氏が弾丸

[9] https://nypost.com/2022/08/31/fbi-agents-say-christopher-wray-has-got-to-go-report/

[10] https://nypost.com/2023/08/10/fbi-head-chris-wray-lied-about-targeting-catholics-he-owes-america-answers/

に撃たれていない[11]と主張し、現職のバイデン大統領の本当の健康状態を議会に隠した。そのため、トランプ氏はクリストファー・レイの即時辞任を強く求めた。

四、異常なことに必ず裏がある

私たちが2回目の「ボルト・タイフーン」に関する調査報告書を発表した後、米国の公式機関やその主流メディアは沈黙を守っていたが、米政府機関の一部の前任者や現職者、また一部のサイバーセキュリティ会社は、SNS や米国のサイバーセキュリティ業界メディア、独立系ニュースメディアを通じ、私たちの調査報告書に対する見解や考えを発表した。その中には、米政府と歩調を合わせて、私たちの調査報告書が米関連企業の研究成果を「歪曲」や「濫用」したと主張する否定的な声も少なくなかった。これらの米国企業は先を争って「身の潔白」を訴えた。ここで説明しなければならないのは、サイバー攻撃事件の調査研究を行う際、他の専門機関の研究成果を引用・参考することは正常な業界慣行であるということだ。しかし、私たちが異なる研究結論を出したことで、一部の米国企業から「歪曲」や「濫用」と見なされることは、米国のネットワーク覇権の影響力の強さを実感させられると同時に、これらの企業が発言する際には必ず大きな外部からの圧力を受けていたと確信した。

国際的にサイバー脅威情報を共有する米非営利団体「Cyber Threat Alliance（CTA）」の言い直し行為も特に味わい深いものである。同団体はメディアの取

[11] https://www.nbcnews.com/politics/donald-trump/republicans-rip-fbi-directors-testimony-trump-might-not-hit-bullet-rcna163653

材に対し、後続研究における前期の「ボルト・タイフーン」報告書で提供された感染指標に誤りが見つかったため、元報告を修正したと主張している。このごまかしの説明は、まさに疑念を招くではないだろうか。報告書の修正時間はさておき、最も大きな疑問点は、元報告書から削除されたページ全体には、IP アドレスリストだけでなく、C＆C サーバアドレスやランサムウェアの暗号通貨ウォレットアドレスなどの重要な証拠も含まれているという点である。これらの証拠の収集過程に間違いだらけとは考えられない。さらに、もしその後の研究が詳細で厳密なものであったなら、修正された報告にはなぜその旨の説明がなかったのか、また、報告書の目次はなぜ同時に修正されなかったのかという疑問も残っている。Cyber Threat Alliance（CTA）のこうした異常な行為は、元報告書に対する改ざんは、巨大な「外圧」に押されて急いで完成させたものでしか考えられない。もちろん、私たちはすでに最新の報告書の中で、米情報機関が中国、ロシア、イラン、アラブ諸国に対してサイバースパイ活動を行っていると同時に、米議会および納税者に対して偽情報を提供している証拠をより多く提出し、米情報機関のこれらの行動は揺るぎない事実であることを示した。

マイクロソフト社の対応も注目すべきだ。8 月 11 日、マイクロソフト社脅威インテリジェンス戦略部長である Sherrod DeGrippo 氏は、2024 年に世界最大級の国際サイバーセキュリティカンファレンス BlackHat の開催期間中に、いわゆる「ボルト・タイフーン」組織は終焉の兆しが見られず、依然として活動していると述べたが、「この組織は中国政府に支えられている」という発言には決定的な証拠も示していな

かった。実際、2023 年以降、マイクロソフト社の動きには一連の疑問点が付きまとっている。私たちが前の二つの報告書で指摘したように、マイクロソフト社は米国軍側や情報機関との協力を著しく強化しており、2024 年にはこの協力がさらに深化し続けている。2024 年 5 月 7 日、米ブルームバーグ社[12]は、「マイクロソフト社はすでに米情報機関のためにオフライン版の人工知能モデルとヘルパープログラムを配備しており、米情報機関はこれらの技術を極秘レベルの情報の補助分析に用いる」と伝えた。

さらに懸念すべきのは、マイクロソフト社がユーザーの「プライバシー情報」に異常な関心を示していることだ。マイクロソフト社は 5 月 21 日、新しい人工知能ソリューションの「Copilot + PC」を発表し、「Recall」機能をリリースした。これにより、Windows オペレーティングシステムはユーザーが行った各操作のデータを記録し、人工知能アシスタントの学習に利用できるようになる。マイクロソフト社は、この機能はローカル実行に限られ、保存されたデータも暗号化されていると主張しているが、この機能の悪用によるプライバシーの漏洩に対するユーザーの懸念を払拭することはできない。結果として、この論争を受けてマイクロソフト社は「Windows 更新に伴いこの機能をプッシュする計画」を延期せざるを得なかった。また、6 月 13 日には、マイクロソフトホールディングスの OpenAI 社が、米国家安全保障局の中曾根元局長を取締役会のメンバーに招へいした。マイクロソフト社のこの一連の動きから、第 702 条関連の傍受プロジェクトの重要なパートナーとして、マイクロソフト社が米情報機関の

[12] https://nypost.com/2023/08/10/fbi-head-chris-wray-lied-about-targeting-catholics-he-owes-america-answers/

影響を受け、コントロールされる程度がいっそう甚だしくなるという事実が十分に伺える。その見返りとして、米政府機関の黙認のもとで、マイクロソフト社が市場の優位性を濫用し、Windows と Office の更新をきっかけにソフトウェア製品をバンドルプッシュすることで、間接的な独占を実現させることができるようになった。

ここでは、7 月 19 日に発生したインターネットセキュリティ事故について触れざるを得ない。米国の有名なネットワークセキュリティ企業である CrowdStrike 社の製品の更新ミスにより、世界中の数百万台の Windows オペレーティングシステムをインストールしたコンピューターが「ブルースクリーン」の故障で使えなくなり、多くの国の公共交通や衛生健康などの重要な情報インフラに深刻な損失がもたらされたということだ。類似した事故は、全世界のネットワーク安全に関わる人々が見たくないものであろう。特にコンピューターウイルスの予防と治療に関わる者として、このような事故は、第三者のウイルス対策ソフトに対する信頼にダメージを与え、さらに全世界のネットワーク安全業界の生態にも影響を及ぼすことになる。しかし、このような深刻な結果をもたらしたサイバーセキュリティ事故に対して、米国の最も重要なサイバーセキュリティ主管部門である米国サイバーセキュリティ・インフラストラクチャセキュリティー庁（CISA）は、マイクロソフト社と CrowdStrike 社に対して異常に甘い態度を示している。何も行動を取らないだけでなく、その局長であるジェーン・エフストリーは、今回の事故を「ボルト・タイフーン」組織を攻撃するための予行演習と呼び、マイクロソフト社と CrowdStrike 社から公衆の目をそらそうとしている。この常識に反する厚かましい言論と行為の背景には、当然、深刻な原因が存在する。実際、

今回の事故は米国の IT サプライチェーンにおける大きな優位性を反映しており、マイクロソフト社と CrowdStrike 社は米情報機関の重要なパートナーとして、米政府機関に保護されているのは当然のことだ。マイクロソフト社と CrowdStrike 社は処罰を受けるどころか、米政府機関の「護衛」の下で「サイバー攻撃めぐる中国脅威論」を掲げ、引き続き世界市場を開拓しながら、第 702 条のために情報を次々と輸送している。

同時に、われわれはアメリカ州、ヨーロッパ、アジア、アフリカから多くの著名なメディア、国際的に有名な人物、業界の専門家たちが、「ボルト・タイフーン」の真相を求めて正義の声を上げていることに気づいた。特にオーストラリアの専門家は「サイバー・スパイ活動の地政学」[13]というテーマで評論を発表し、米政府とマイクロソフト社の報告書には確かな証拠がないことを明確に指摘した。さらに、米国の情報機関が令状なしでの監視権限を更に拡大するために、「ボルト・タイフーン」サイバー攻撃の脅威を捏造し、公共の支持を得ることで政策立案者に圧力をかける邪悪な行為を明らかにした。このような国際的視野を持つ人々の発言に、私たちは深く敬意を表する。

五、結語

数年来、米連邦政府の機関は、自らの利権を追求するため、サイバー攻撃のトレーサビリティ問題を政治的に利用してきた。マイクロソフト社と CrowdStrike 社

[13] https://johnmenadue.com/the-geopolitics-of-cyber-espionage/

などの一部の企業は、米国の政治家や政府機関、情報機関に迎合し、自社の商業利益を拡大する手段として、十分な証拠や厳密な技術分析が欠如しているにもかかわらず、「アンサンブル」や「ハリケーン」「コアラ」ではなく、「タイフーン」や「パンダ」「龍」といった奇妙でありながら明確な地政学的な色彩を持つ名前でハッカー組織を命名することに躍起になっており、自分のいわゆる「高度な技術」と文化的背景を示しようとしている。結局、最も基本的な製品の品質問題を無視し、業界全体の風潮を損なう事態を引き起こしている。われわれは前回の報告書で、中国が常にサイバーセキュリティ事件における技術調査の政治的関与に反対し、サイバー攻撃の起源を政治化することに反対していることを何度も強調してきた。一方、米連邦政府機関は裏で煽動し、虚偽のサイバー攻撃の脅威をでっち上げることで大量の議会予算を騙し取った結果、その野心はますます膨れ上がっている。このままではいつか「自分の首をしめる」ことになるだろう。クリストファー・レイをはじめとする無責任な米国の政治家たちは、不正な利益を追求するために、繰り返して「ボルト・タイフーン」という虚構の物語を操り、米国の議会や国民を欺いているが、こうした行為は必ずや米国民からの正義の審判を受けることになるだろう。

最後に、地政学的な対立がますます激化する今日、国際的な正常な交流こそがサイバーセキュリティ業界に最も必要である。私たちは改めて呼びかけるが、サイバーセキュリティには広範な国際的な協力が不可欠であり、さまざまなサイバーセキュリティ企業と研究機関は、サイバー脅威への対抗技術の研究に専念し、利用者に対してより高品質な製品やサービスを提供する方法を追求すべきである。そうす

ることで、インターネットは人類社会の共同発展と進歩を促進する中で、着実に進むことができる。

中国国家コンピューターウイルス緊急処理センター

コンピューターウイルス対策技術国家工程実験室

2024 年 10 月 14 日