

防 衛 取 得 研 究 第四卷 第四号 平成23年3月

- | | | |
|---|---|-----|
| 1 | I SMSの有効性測定結果の分析とその活用について | 1 頁 |
| 2 | 米国のサイバー・カウンターインテリジェンスについて
—通信傍受の法的及び技術的側面— | 4 頁 |

1 ISMS の適合性の確認から有効性の確認へステップアップ

近年、構築した ISMS（情報セキュリティマネジメントシステム）が、適用規格に適合しているかのフェーズから、構築・運用している ISMS の PDCA のどのプロセスでどのような有効性を発揮しているか、具体的に確認できるようにしていくことが求められてきております。

2 有効性測定の目的

ISMS における有効性の測定及びレビューをしていくには、その目的・方法とその PDCA プロセスが、どのように展開・活用されていくべきなのかを理解し、その理解の適切性を実際の PDCA プロセスの中で確認していくことが重要です。

JIS Q 27001 情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—要求事項で要求している「4.2.3b) ISMS の有効性について定期的にレビューする。」という中身には、ISMS 基本方針及び目的を満たしていることのレビューとセキュリティ管理策のレビューとがあり、そのことにはどのような意味があるのか理解する必要があります。

ISMS 全体の有効性の測定は、構築した ISMS が ISMS 基本方針及び目的を満たしていることを確実にするために実施するものです。管理策又は一群の管理策の有効性の測定結果は、最終的には ISMS の有効性の測定のためのものであり、ISMS 全体の継続的な改善のために活用することになります。

3 有効性測定のプロセス

有効性の測定も一つのプロセスと考えることができることから、プロセスアプローチの考え方を適用することになります。どのように有効性を測定するか計画し、実行し、その結果について点検し、必要に応じ測定方法を見直すことになります。

4 有効性測定の PDCA

・ ISMS 全体の有効性測定の計画

インプットとしては、ISMS 基本方針・目的、セキュリティ監査の結果、インシデント、有効性測定の結果、提案及び利害関係者からのフィードバックの 6 項目のほかに「リスクアセスメントの結果」も役立つと考えられます。アウトプットとしては有効性測定の判定結果を考えることができます。フィードバック先としては、「リスクアセスメントプロセス」「マネジメントレビュー」へととなります。

・ 管理策の有効性測定の計画

管理策の有効性を測定する場合は、実施度及び達成度がポイントとなります。

・ 実行

セキュリティ要求事項を満たしていることを検証するために、管理策の有効性を測

定します。

・点検と処置

有効性測定のプロセスの中で監視し、課題を発見して改善処置をとることになります。

5 有効性測定の見直し

要求規格の 4.3.1g) 組織が必要とする文書化の手順としては、管理策有効性測定手順(概要、測定手法、有効性の評価)、管理策有効性測定票等の作成または組織で毎年度作成する ISMS 実施計画書への盛り込み等があります。

6 管理策の有効性測定の基本的考え方

管理策の有効性測定は、管理策が計画した管理目的をよく達成していることを判断する材料であり「有効性測定は管理目的とよく関係づけて」捉える必要があります。管理策は管理目的以上に「リスクと関係づけて」捉える必要があります。

7 管理策の有効性測定の具体例

管理策の有効性測定の具体例としては、①「リスク対応計画書」の進捗度 ②「入退出記録」の実施率 ③ネットワーク関連のインシデントの件数及び対応時間 ④情報セキュリティ苦情件数 ⑤データバックアップ実施率 ⑥情報セキュリティ関連投資額 ⑦システム要員の訓練実施率等の定期的な測定の方法が考えられます。

8 管理策の有効性測定実施方式の具体例

管理策の有効性測定実施方式の具体例としては、①管理策 133 項目を各部の業務内容に適した管理項目として割振り、分担して実施するセルフチェック方式。②管理策 133 項目を各部の業務内容に適した管理項目として割振るが、その組織にとって重要な項目については複数の部に測定させて実施する複数チェック方式。③半年あるいは 1 年毎にある部が担当した項目を他の部に測定させるクロスチェック方式等があります。

9 マネジメントシステムの有効性の確認

マネジメントシステムの有効性を確認する手法として、①組織を理解する。②該当する目的に照らして、重要となる分野を想定する。③目的の実現の程度、実績を評価する。④マネジメントシステムが有効に機能しているかどうか判断する等の方法があります。またそのためには、①組織のプロセスを理解できる。②適用規格の目的と意図を理解し、組織の活動の結果を規格の要求事項に結び付けて評価できる。③ビジネスの多様性を認識し、当該組織の背景や文化等を理解することができる。④円滑なコミュニケーションを図ることができる等の力量が求められることとなります。この力量は、組織の個人へ、そして組織全体へと求められるものです。

10 判定結果をどのように活用するか

このようにプロセス全体を考慮して、管理策または一群の管理策の有効性について判定を導き出すことは当然重要ですが、これら有効性測定結果をどのように活用するかを考慮することも重要です。その有効性測定結果のフィードバック先としては、次のように考えることが可能です。

(1) 先ずは、組織自身の ISMS へのフィードバック

- ・ ISMS 全体の有効性測定へインプットする一要素として活用する。
- ・ プロセス・システムの管理責任者等に報告し、リスクアセスメント結果の妥当性確認や必要に応じて再リスクアセスメントを実施し、追加の管理策の必要性等を検討する。
- ・ 測定する上で必要なモニタリングプロセスについて再検討する。
- ・ 測定結果を基に、インシデント対応をするための基準等のインシデント管理を再検討する。
- ・ 測定結果を基に、測定方法自体や測定頻度などの有効性測定プロセスについて再検討する。

(2) 次に、組織自身の中に構築されている他の情報保全体制及び情報セキュリティ体制へのフィードバック

これはこのような ISMS 全体及び管理策または一群の管理策の有効性測定結果のフィードバック・分析を、その組織の中に構築されている他の情報保全体制及び情報セキュリティ体制の運用・管理にも活用することが可能であり、それぞれのマネジメントシステムの有効性測定結果のフィードバック・分析を相互に活用していくという発想と実行は、マネジメントシステムの有効性を高めていく上において重要であると考えられるものです。

具体的には、当該組織で展開している次のような情報保全体制及び情報セキュリティ体制の運用・管理に活用することが可能であります。

- ・ (独) 宇宙航空研究開発機構 (JAXA) の情報セキュリティ規程に基づく情報セキュリティ体制
- ・ 内部統制 (JSOX 法) における資産の保全体制
- ・ 防衛省の情報セキュリティ基準に基づく情報セキュリティ体制

これらの情報セキュリティの基本的な考え方・基準は、JIS Q 27001 と共通する部分が多く、JIS Q 27001 に基づき構築した ISMS の有効性測定結果をそれぞれの情報保全体制及び情報セキュリティ体制に水平展開し、相互に、その有効性を高めていくという発想とその実行が求められております。

11 ISMS の有効性測定の最終的目的

ISMS 全体の有効性の測定及びその結果のレビューは、管理策または一群の管理策の有効性の測定とその結果のレビューを受けて年度目的、あるいは中期的目的を満たしていることのレビュー、それらによる ISMS 基本方針を満たしていることのレビューを経て、ISMS 全体の有効性のレビューが段階的に成り立っていることです。

米国のサイバー・カウンターインテリジェンスについて

—通信傍受の法的及び技術的側面—

客員主任研究員 横山恭三

はじめに

「サイバー・カウンターインテリジェンス」という用語が米国政府の政策文書に登場したのは、2008年1月、ブッシュ大統領が発出した大統領令第54/第23号(National Security and Homeland Security Presidential Directive : NSPD54/HSPD23)「包括的国家サイバー・セキュリティ・イニシアチブ (Comprehensive National Cybersecurity Initiative : CNCI)」が最初である。そして、この大統領令に続き、同年7月30日に発出された行政命令13470号において「カウンターインテリジェンス」の定義が改訂された(拙稿「カウンターインテリジェンスの定義の改訂」(本防衛取得研究第三巻第二号)参照)。これまでのところ、米国の政策文書では、「サイバー・カウンターインテリジェンス」の定義がなされていないが、米軍統合用語集では、「(米国の)サイバー能力と意図を判断するための伝統的な手段を使用して行う外国諜報機関の情報収集活動のみならず、主たる手段としてコンピュータ・ネットワークを使用する外国の情報活動を、特定・浸透・無力化するための方策である」¹と定義されている。

ねずみが侵入する穴を塞ぐのがセキュリティであり、その穴を利用してねずみを捕まえることがカウンターインテリジェンスであるとすれば、「サイバー・カウンターインテリジェンス」は、敵対者(外国の情報機関、テロリスト、外国の犯罪組織、又はハッカー)が、コンピュータ・ネットワークを利用して侵入するならば、そのコンピュータ・ネットワークを利用して敵対者を探知し、敵対的活動を防止し、さらに法執行機関と協力して敵対者を逮捕する活動と言える。そのための主要な方法としては、電気通信の伝送路の途中に装置を取り付け、電話(固定及び移動)やファクシミリ、コンピュータ通信(Eメール、IP電話)などの通信を傍受し、あるいは、監視下にある容疑者のコンピュータにスパイウェアをインストールし容疑者の情報を収集するなどが考えられる。

本稿は、サイバー・カウンターインテリジェンスにおける主要な情報収集手段である通信傍受について米国の状況を紹介するものである。

以下、最初に、サイバー・スペースの脅威の実態を紹介し、次に、サイバー・カウンターインテリジェンスの中心的手段である通信傍受の法的側面を紹介し、最後に通信傍受の技術的側面を紹介する。

1. サイバー・スペースにおける脅威の実態

サイバー・スペース²として知られるグローバルに相互連結したデジタル情報と通信インフラは、現代社会のあらゆる側面を支えている。サイバー・スペースに対する脅威は、あらゆる国家の経済と安全保障に対する重大な挑戦となっている。特に重要インフラの運営をコンピュータ・ネットワークに大きく依存した近代国家に対するサイバー攻撃は、大きな打撃をもたらす。2007年のエストニアの政府機関等へのサイバー攻撃がこの例である。他方、政府業務や重要インフラの運営へのコンピュータ・ネットワークの利用の進んでいない国、例えば、北朝鮮などはサイバー攻撃にあってもほとんど被害がないであろう。

また、近代国家のコンピュータ・システムには大量のセンシティブな情報が内蔵されている。これらセンシティブな情報の漏洩は、特に国家主体によるものは、国家間の技術力の差を一気に縮めるこ

とが可能となり、被害国の経済的競争力や軍における技術的優位性の喪失に繋がるであろう。2009年の米国の国防産業企業からのF-35の設計や電子システムに関するセンシティブな情報の漏洩はこの例であろう。

このように、情報システム、インターネット、及びその他のインフラの連結性の増大は、これを利用して情報を窃取しようとするあるいは重要インフラに対して電子的攻撃をしようとする敵対者に先例のない機会を提供する一方、これらに依存した国家には脆弱性をもたらしている。従って、これらの敵対者に対抗するカウンターインテリジェンスコミュニティには、あらゆる情報技術を駆使して敵対的活動を破砕することが求められる。これが、「サイバー・カウンターインテリジェンス」が生まれた背景である。

以下、サイバー脅威の実態を示す幾つかの事例を紹介する。

- ①2004年に、中国広東省を発信源とするハッカーが米軍関連の研究所、NASA、及び世界銀行などから大量のデータを窃取していたことが発覚した。この事例は、暗号名で「タイタン・レイン (Titan Rain)」と呼ばれた。³
- ②2007年4～5月に、エストニアで大規模なサイバー・テロが発生し、約3週間にわたり、大統領府や政府機関、銀行、新聞社などのウェブサイトが停止したほか、一時は携帯電話網や救急ネットワークも被害を受けた。この事例は、インターネットへの依存度が高まっている国々に対して重要な警告を発した。⁴
- ③2007年年6月に、米国の下院議員フランク・R・ヴォルフとクリス・スミス（中国の人権問題の批判者）は、彼らの議会オフィス・コンピュータが、中国を発信源とするハッカーに侵入されたことを明らかにした。⁵
- ④2007年年8月、ドイツのスピーゲル誌は、ドイツのアンゲラ・メルケル首相のオフィスの3つのコンピュータ・ネットワークが中国の情報機関と思われるハッカーに侵入されたと報じた。⁶
- ⑤2008年11月5日、ニューズウィーク紙は、オバマ氏とマケイン氏の大統領選挙戦のコンピュータ・システムが外国のハッカーに侵入されたと報じた。⁷
- ⑥2007年年12月、ニューヨークタイムズ紙は、中国を発信源とするハッカーがテネシーのオークリッジ国立研究所の核兵器研究室から機密情報を窃取しようとしたと報じた。⁸
- ⑦2008年、中東の米軍基地のラップトップ・コンピュータに、ウィルスに感染したフラッシュ・ドライブが挿入されたことにより、米軍の軍事用機密コンピュータ・ネットワークから大量の情報が盗み出された。このサイバー攻撃に対抗するペンタゴンの作戦計画は、「バックショット・ヤンキー作戦」と名付けられた。⁹
- ⑧2009年4月21日、ウォールストリートジャーナル紙は、現及び元政府職員の話として、身元不明のサイバースパイが、過去2年間にわたり、米国、英国及びその他の同盟国と共同開発している次世代戦闘／爆撃機F-35に関する情報を保管している国防産業企業のサーバーにハッキングし、F-35の設計や電子システムに関する数テラバイトのデータをダウンロードしたと報じた。火器管制装置やセンサーなどの最もセンシティブな情報はオフラインであったので無事であったもようである。¹⁰
- ⑨2009年4月8日、ウォールストリートジャーナル紙は、匿名の上級政府職員（インテリジェンス）の話として、中国とロシアのサイバースパイが、米国送電網を維持している企業のコンピュ

ータ・システムに侵入し、さらに悪いことには、システムを破壊することができるソフトウェアを残置していると報じている。さらに、この侵入を探知したのは企業でなくインテリジェンス機関であったと報じている。¹¹

⑩2009年3月29日に、カナダのシンクタンク「SecDev Group」とカナダのトロント大学の「Munk Center for International Studies」による共同研究プロジェクト「Information Warfare Monitor」が発表した「Tracking GhostNet : Investigating a Cyber Espionage Network」と題する報告書は、10カ月にわたる調査の結果、「GhostNet」により、103カ国の国際機関のコンピュータ1,295台が乗っ取られていることが判明したと発表した。中国政府がこの事件に関与していると疑われている。¹²

⑪2010年9月、イラン各地で産業用のコンピュータ・システムが、数週間にわたりサイバー攻撃を受け、約3万台のパソコンが「スタックスネット」と呼ばれるコンピューターウイルスに感染した。¹³

ボーダレスで匿名性の高いインターネットによる攻撃の発信源の特定は困難であることから、攻撃を疑われた国は、いつもその事実を否定している。また、被害側も様々な理由から被害の実態を公表しない場合が多い。従って、上記の幾つかの事例では発信源などから中国やロシアなど関与しているとの報道がなされているが真相は不明である。

2. 米国の通信傍受法

米国憲法の中には「通信の秘密」は明示的に書かれてはいないが、憲法修正第1条の「表現の自由」及び修正第4条の「プライバシーの保護」が援用され、通信の秘密は保護されるべきものとされている。

他方、通信傍受を合法とする幾つかの法律がある。1つ目は、1968年に成立した「通信傍受法 (Title III of the Omnibus Crime and Control Act of 1968)」(筆者注：電話盗聴法 (Wiretap Act) とも言われる)である。この法律では、(1) 捜査機関が行う通信傍受に際して判事から令状を取る必要があること、(2) 令状を取る際には「信じるに足る相当な理由 (probable cause)」を判事に示さなくてはならないとされている。

2つ目に、1978年に成立した「外国インテリジェンス監視法 (Foreign Intelligence Surveillance Act : FISA)」である。ニクソン大統領によるウォーターゲート事件を受けて1975年に連邦議会に設置された所謂チャーチ委員会の提言を受けて成立したのがこの法律であり、また同法に基づき新たに設置されたのが「外国インテリジェンス監視裁判所 (Foreign Intelligence Surveillance Court : FISC)」である。外国インテリジェンス監視法 (FISA) が、国内の犯罪捜査の場合と異なるのは、外国インテリジェンス監視裁判所 (FISC) が発行する令状取得の要件には、犯罪性の有無は含まれず、監視対象が外国勢力 (Foreign power) によるスパイ活動であるかどうか問われるのみである。特に、米国人を監視下に置く場合には外国勢力の工作員 (エージェント) であると信じる十分な理由がなければならないとされた。

3つ目に、1986年の「電子通信プライバシー法 (ECPA : Electronic Communications Privacy Act)」である。この法律は、当時普及してきていた電子通信システムに対応し、電子メールの内容やプロバイダのログ (記録) を捜査対象とするために、1968年の通信傍受法を修正したものである。

4つ目に、1994年に成立した「通信傍受支援法（Communications Assistance for Law Enforcement Act : CALEA）」である。これは、捜査目的のための通信傍受における通信事業者の義務を明確化したもので、通信事業者は捜査当局から要求があった場合にはその要求に応じなくてはならない。そして、通信傍受を可能にする機器を通信事業者の設備の中に設置しなくてはならないと定めた。そのための技術標準は連邦通信委員会（FCC）が設定することになっている。この法律はしばしば議論の対象となった。例えば、連邦通信委員会（FCC）は、2006年5月にブロードバンドサービス・プロバイダおよびIP電話サービス・プロバイダに対する警察等法執行機関への協力・支援に関する規則の強化を図る命令を採択した。これに対して、人権保護団体やプロバイダ団体などは、通信傍受支援法（CALEA）はあくまで公衆電話交換網における通信傍受の規制法であり、IP電話等新たなインターネット通信に適用することに反対する運動を起こした。現在は、IP電話を含むブロードバンド回線で提供される通信サービスも通信傍受支援法の適用対象となっている。

5つ目に、2001年の「米国愛国者法（Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism : USA PATRIOT Act）」である。2001年の9.11同時テロを受けて制定された本法は、個人のプライバシーより安全保障を優先し通信傍受の要件を大幅に緩和した。本法成立以前は、捜査当局は傍受の対象とする電話一つ一つについて傍受申請をしていたが、本法は、対象者が使用している電話であれば、すべて傍受できるようにした。通信傍受のための令状については、以前は司法府の裁判所へ行って申請することが必要だったが、同じ行政府の中で検事総長や連邦検事が令状を出せるようになった。また、電子メールの内容について、インターネット・サービス・プロバイダ（ISP）に記録を求めることができるようになった。本法は、4年間の時限立法であったが、捜査権限に関する幾つかの条項は最初からもしくは延長の際に恒久化されている。

6つ目に、2007年に成立した「アメリカ保護法(Protect America Act of 2007)」である。この法律は、アメリカの通信網を介した外国人との通信を令状なしの通信傍受も認めるなど政府に大きな権限を与えた。この法律成立の背景を簡単に説明する。2005年12月、ニューヨークタイムズ紙は、9.11同時多発テロ以降、ブッシュ大統領の指示のもとで、令状なしで通信傍受が行われてきたと報じた。これにより、政府がテロ容疑者等の不審者の通信秘密を正規の令状なしに傍受していたことが明らかになり、国民のプライバシー保護と国家の安全保障をめぐる問題がクローズアップされた。これに対し、ブッシュ大統領は、国家の安全を保障するために必要な場合、令状なしの通信傍受も認めるとともに、政府を手助けする通信会社に対しても、過去に遡って免責を与えるべきであるとして、「外国インテリジェンス監視法」の改正を議会に促した。このような背景で成立したのが「アメリカ保護法」である。しかし、この法律は180日間の時限立法であった。この法律は、2008年の「改正外国インテリジェンス監視法（FISA Amendments Act of 2008）」の成立に繋がった。

7つ目に、2008年7月に成立した「改正外国インテリジェンス監視法（FISA Amendments Act of 2008）」である。同改正法は裁判所の令状無しで海外との電話・電子メールなどの傍受を合法化するもので、さらに情報提供に協力する通信会社の免責事項を、法成立前に遡って有効にする条文も盛り込まれている。旧法では、米国内に住む住民に対し、大統領は司法長官を通じて72時間以内の令状なしの監視を行うことができるが、その場合、司法長官はできるだけ早期に外国インテリジェンス監視裁判所（FISC）にその旨を報告し、事前に令状を得られなかった理由を説明しなければならず、その時間的余裕がないときは傍受行為を開始してから遅くとも3日後に事後令状を要求しなければ

ならないとされていた。

以上のように米国では、国民のプライバシー保護よりも国家の安全保障が優先されている。

3. 米国における通信傍受技術

通信は、アナログの電話から、音声もデジタル化するデジタル・データ通信の時代になった。特に、通信の多くがインターネットを利用した電子メールで行なわれるようになったことにより、カウンターインテリジェンス側の通信傍受は、次の様により困難なものとなった。

①人物の特定が難しい。

発信者が分かっても、多数宛に送信されていれば受取人が分からない。

②パレット通信であるためメッセージの捕捉が困難である。

メッセージがどのルートを通れるかは分からない。極論すれば、すべてのパケットが別々のルートを通って目的地に着くことも理論上はありえる。

③暗号化により解読が困難となった。

個人が PGP（電子メールやファイルを暗号化するためのソフトウェア）を使用できるようになった現状では、解読は不可能である。従って、カウンターインテリジェンスとしては、解読よりも、誰と誰が暗号通信をやっているという事実が重要になる。

④光ファイバーの使用により、隠密に傍受することが困難となった。

光回線は、電気信号で通信するケーブルと異なり電磁波が発生しない。従って、1970年代から1980年代にかけて、米海軍と国家安全保障局(NSA)がオホーツク海でソ連軍の海底ケーブルを傍受していた「アイビー・ベル (Ivy Bells) 作戦」のような隠密作戦が不可能となった。しかし、光回線でも通信傍受が可能であるという主張もある。玉川大学学術研究所・量子情報科学研究センターの二見史生准教授は、「2010年、光通信ネットワークから情報が盗聴される危険性を実験で確認したところ、電子メールの中身やパスワードを盗み見た。盗聴実験はタップと呼ぶ通信機器を光回線に取り付けて実施した。光信号を30%分岐したうえ、この光信号を電気信号に変換し、ソフトウェアを使ってパケット（情報の束）の中身を解析した。¹⁴」と学界で発表した。

次に、米国のカウンターインテリジェン・コミュニティが実施している具体的な通信傍受について、インターネット上に公開されている事例を紹介する。

(1) カーニボー

米連邦捜査局 (FBI) は、電子メール監視システム（通称：カーニボー (Carnivore)）を、インターネット・サービス・プロバイダー(ISP)のシステム内に設置し、ネットワークを移動するインターネット・トラフィックを収集している。捜査の対象となった人物が伝送したメッセージを探すため、何百万ものメールを厳重に選別する。FBI は、監視下にある容疑者のインターネット通信を監視するために同ツールを開発したとされる。

1999年頃に開発され FBI が開発したカーニボーは、特殊な設定を施した Windows コンピュータで、ISPのネットワーク上に設置され、データ通信をモニターし、特定の情報を記録する。記録された情報はリムーバブル・ハードディスクに記録され、FBI へ提供される。

2000年2月に FBI はカーニボー の名称を DCS (digital collection system) と変更したようである。また、2005年から、FBI は、カーニボーを使用しておらず、民間によって開発された別

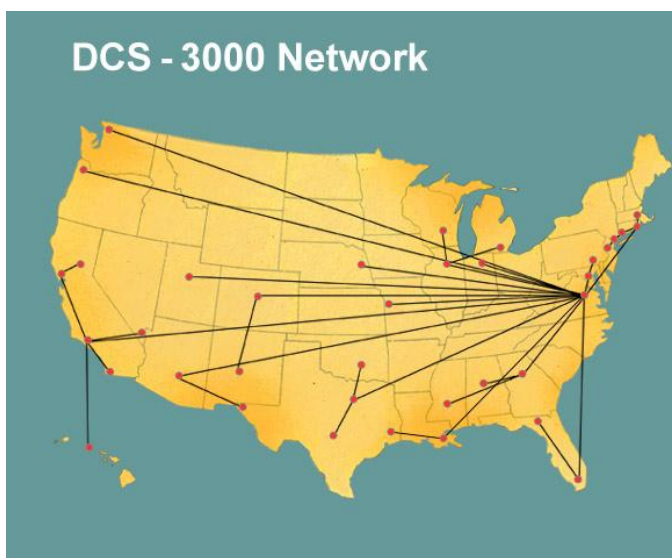
の製品を利用していると言われている。

因みに、我が国で使用されている通信傍受用の電子メール監視システムは、「通信事業者貸与用仮メールボックス装置」と呼ばれる。¹⁵

(2) DCSnet (Digital Collection System Network)

2007年に情報自由法(FOIA)の下で公開された文書により、FBIが、全米の携帯電話や固定電話を傍受する高度な監視システム(DCSNet)を開発していたことが明らかになった。この監視システムは、固定電話事業者やインターネット電話事業者や携帯電話事業者が管理するシステムと、FBIの傍受ルームとを接続している。この大規模な通信傍受システムはWindowsマシンで作動する三つの主要なサブシステムから成っている。「DCS-3000(別称Red Hook)」という第一のシステムはペンレジスター(発信者情報の分析と記録)とトラップ・アンド・トレース(受信者情報の分析と記録)を担当するもので、通信内容の監視には関わらない。「DSC-6000(別称Digital Storm)」と呼ばれる第二のシステムは、各種通信内容やテキストメッセージの収集記録と分析の機能をもち、通信傍受命令に直接的に対応する。第三の「DCS-5000」は高度な機密システムで、スパイやテロリストを対象とする通信傍受に用いられているという。¹⁶

図第1は、DCS-3000の通信網である。FBIの傍受ルームは、米国内の地方事務所や非公開の場所に設置されている。これらの傍受ルームは、インターネットとは異なった暗号化された独自の基幹回線で互いに結ばれている。この回線は米Sprint Nextel社が、政府から依頼されて運営している。



図第1 DCS-3000の通信網¹⁷

(3) スパイウェア(CIPAV)による情報収集

FBIは、電子監視下にある容疑者のコンピュータにスパイウェア(Computer and Internet Protocol Address Verifier : CIPAV)をインストールし、容疑者の情報を収集する。CIPAVは、IPアドレス、オープンポート、使用しているプログラムなどの情報を自動送信する。さらに、CIPAVは密かに隠れて、すべての送信メールを監視するとともに、接続したすべてのIPアドレスを記録する。

CIPAV の存在は、2007 年 7 月に法廷の文書を通じて知られるようになった。この文書には、ワシントン州オリンピア近郊の高校に爆弾脅迫のメールを送った 10 代の容疑者を、FBI が CIPAV を使って逮捕した経緯が示されていた。2007 年 6 月のメモには、FBI の要員に対する以下のような指示が書き込まれている。「CIPAV を仕込んで、ワシントン州レイシーの高校に爆弾脅迫を行った容疑者の地理的な位置を突き止めよ。CIPAV は、捜査対象者が使用している MySpace.com のプライベートチャットルームに掲載された URL アドレスを通じて仕込むように。」 FBI 特別捜査官の Norman Sanders 氏が当時作成した宣誓供述書によると、CIPAV は、標的となるコンピュータの IP アドレス、イーサネット MAC アドレス、環境変数、直前に訪問したウェブサイトのほか、コンピュータの登録済み所有者の名前や OS のシリアルナンバーといったレジストリ情報を含む、「ネットワークレベルのメッセージ」を送信できるという。¹⁸

FBI は、当初「Internet Protocol Address Verifier」と呼ばれる単純な技術を使用していたが、その後、「Magic Lantern」というソフトウェアを開発して乗り換え、さらに CIPAV へ乗り換えたようである。「Internet Protocol Address Verifier」(IPAV) は別名「ウェブバグ」とよばれ、ウェブページの閲覧者を識別する仕組みで、「Magic Lantern」は、キー・ストローク・ロギング・ソフトウェア(パソコンへのキー入力を監視してそれを記録するソフトウェアもしくはハードウェア)であり、電子メール又は OS の脆弱性を利用してインストールされる。

(4) NSA のテロリスト監視プログラム

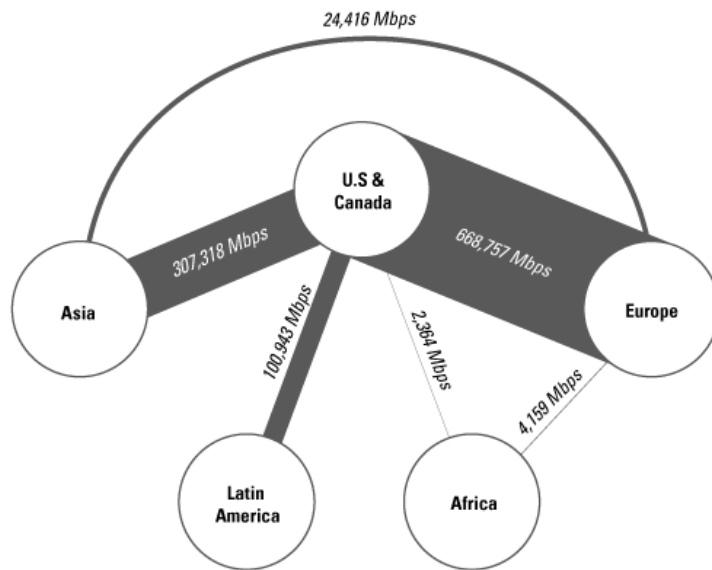
現在、米国では国家安全保障局 (NSA) によって「テロリスト監視プログラム」が実施されている。これは、2001 年の同時多発テロを受けて、2002 年にジョージ・ブッシュ大統領が承認したものである。このプログラムは、NSA が裁判所の令状なしに国際テロ組織アルカイダとの繋がりが疑われる人物のみならず、海外のテロ容疑者と通信した米国内居住者に対しても、裁判所の令状なしでの傍受権限を NSA に与えるものとなっていることから、適法性を巡って議論が戦わされてきた。また NSA に協力したとして、AT&T などの通信事業者らが提訴された。しかし、結果は、既述したとおり、「改正外国インテリジェンス監視法」に、情報提供に協力する通信会社の免責事項の条文が盛り込まれた。

土屋大洋氏の論文『ブッシュ政権の令状なし通信傍受をめぐる課題』¹⁹には次のように記述されている。「もともと、米国の通信業者は、法律によって政府に協力することが求められているが、このプログラムでは、NSA はこれまでない規模で通信会社の協力を仰ぐことになった。つまり、NSA の傍受ネットワークが、各通信会社の設備と直結され、大量のデータが NSA に流れることになった。NSA が使っているとされる Narus 社の「NarusInsight」という傍受用機器は、DSL(Digital Subscriber Line) 回線 39,000 本にあたる OC-192(北米の同期型光ネットワークのデータ伝送レート: 約 10Gb/s) のネットワーク回線をリアルタイムでモニターする能力がある。しかし、こうした大規模な通信傍受は、業界の協力がなくてはできない。ブッシュ政権の令状なし傍受の要請に応じた通信会社は、AT&A、Verizon、Bellsouth の大手三社だったといわれている。」

図第 2「国際インターネット回線の帯域(2005 年)」は、大陸間の帯域幅は、どれだけの量のデータを送受信できるかを表している。図第 2 のとおり、ほとんどのデータが米国を中継していることを示している。即ち、米国での通信傍受の機会が多い。

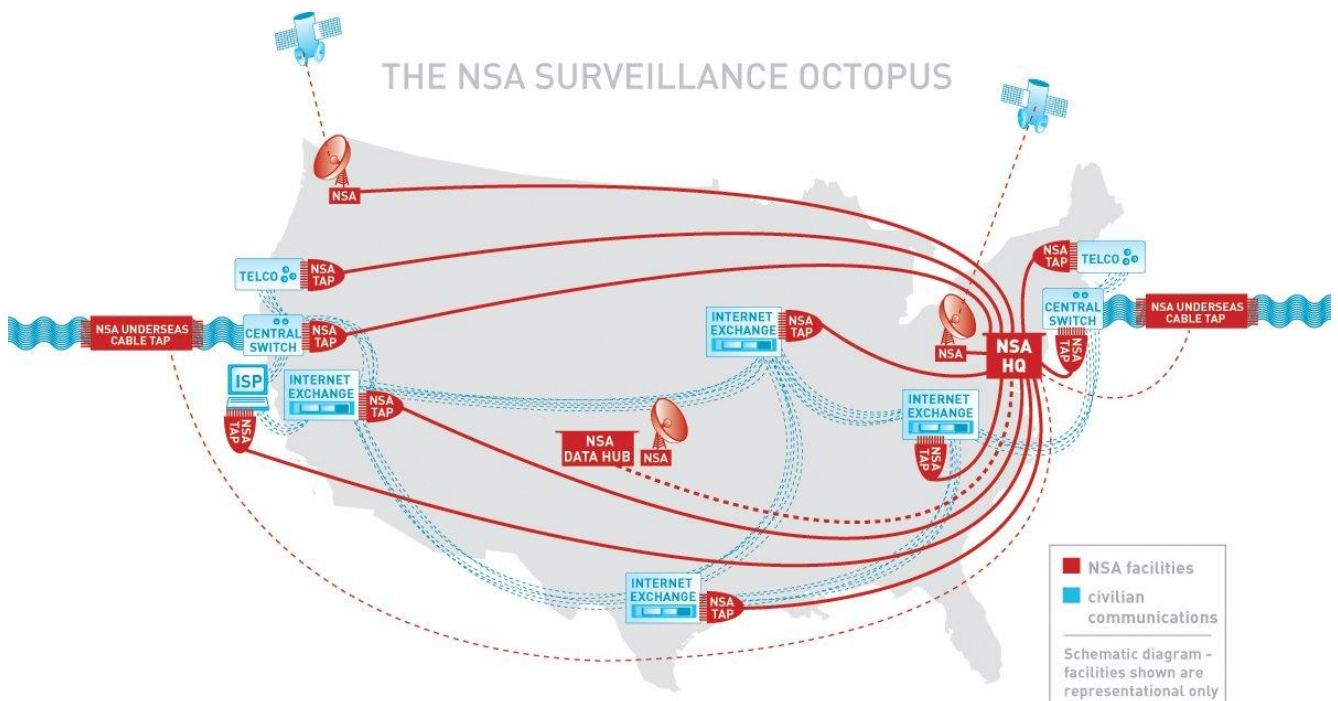
図第 3「NSA の通信傍受網」は、NSA の傍受装置がインターネット・ネットワークのアイエク ス (IX) に設置されていることを示している。また、通信衛星、海底ケーブルにも傍受装置が設置

されていることが分かる。



© PriMetrica, Inc. 2005

図第2 「国際インターネット回線の帯域（2005年）」²⁰



図第3 「NSAの通信傍受網」²¹

(5) 「ロービング・バグ (roving bug)」による盗聴

2006年に、「FBIは、携帯電話の通話口についているマイクを遠隔操作でオンにし、それを利用して付近の会話を盗聴するという『ロービング・バグ (roving bug)』と呼ばれる方法を使用している」との報道²²がなされた。

この盗聴手法は、2006年11月27日に発表された、米連邦地裁のLewis Kaplan 裁判官による意見書の中で明らかになった。裁判の文書では「携帯電話内に入れられた盗聴器」と言及されており、この表現はハードウェアともソフトウェアともとれるが、2005年には、「端末の所有者の知らないうちに、離れたところから携帯電話にソフトウェアをインストールできる。このソフトにより、所有者が通話していない時にもマイクをオンにできる」という内容の記事がFinancial Times 紙に掲載されていることなどからソフトウェアをダウンロードした可能性が大きい。

次の2件は、開発途中で中止となった興味あるプログラムである。

(6) ライフログ・プログラム (Life Log) ²³

国防高等研究計画局 (DARPA) が開発していたプログラム。DARPA の計画では、個人の生活で把握可能なあらゆる要素を収集し、データベースに保存し、それらを連結して脈絡を与え、関係や出来事、経験をたどる。そのため、送受信した電子メール、撮影した写真、閲覧したウェブページ、通話、視聴したテレビ番組、読んだ雑誌などあらゆる行動を1つの巨大なデータベースに取り込み、個人の生活における『脈絡』を追跡する。それにより、日課、人間関係、習慣など、個人に特有の行動パターンが得られれば、集団の中から個人を区別したり、その個人を監視したりすることが容易になるという。しかし、2003年5月に公表された途端に猛烈な批判を招き、2004年1月末にひそかに中止された。

(7) 全情報認知システム (Total Information Awareness System : TIA) ²⁴

国防高等研究計画局 (DARPA) が開発していたテロリストの情報につながる痕跡を探知し、テロ発生前にそれらを解明しようとするデータ・マイニング・システム。具体的には、パスポート申請、ビザ、労働許可、運転免許、レンタカー利用記録、航空券の購買記録、逮捕歴、クレジットカードの履歴、学歴、医療や居住の記録などから、浮かび上がるパターンを見付け出し、テロリストによる攻撃を予想するというものだった。

2002年8月に計画が発覚後、物議を醸し、批判をかわすためにテロ情報認知 (Terrorism Information Awareness : TIA) に改名したが、2003年、米議会の反対に遭って計画は中止され、さらに、米議会上下院の合同委員会(House and Senate negotiators)は、2003年9月18日に、本計画の中心機関であった DARPA の情報認知局(Information Awareness Office : IAO)の閉鎖を決定した。

おわりに

我が国や諸外国においては、犯罪の捜査・防止という公共の福祉の要請に基づき、一定の要件の下での通信傍受などの強制処分は、憲法あるいは法律上全く許されないものではないと解されている。2000年11月に成立した我が国の「犯罪捜査のための通信傍受に関する法律」も、この様な趣旨に基づき法制化されたものである。しかし、この法律は通信傍受の対象となる犯罪を“薬物関連犯罪、銃器関連犯罪、集団密航の罪、組織的殺人”に限定し、さらに、“犯罪が行われたと疑うに足りる十分な理由”がなければ、地方裁判所の裁判官から傍受令状は発布されない。これでは、コンピュータ・ネットワークを使用する外国の情報活動を探知・防止することはできない。

我が国で行なわれている通信傍受は「司法的傍受」であり、他方、米国や英国などでは「司法的傍受 (裁判官が発布する令状に基づく刑事犯罪捜査のための傍受)」と「行政的傍受 (内務大臣などの

許可状に基づくスパイやテロリストの企てを未然防止するための傍受」が行なわれている。大森義夫氏は著書『日本のインテリジェンス機関』の中で、「行政的傍受は日本では認められていない。しかし、この制度のない先進主要国は存在しない。中略 そんな制度を認めれば行政府がめっちゃめっちゃ乱用するのではないか、との懸念を日本人一般は持つだろう。だが、米国でも英国でもそうした乱用の批判は全くない。なぜならば、制度の監督は国民の代表たる議会の権能である。行政府は議会の情報委員会に行政的傍受を実施した件数を報告する。求められれば委員会の秘密会で内容を説明する。」と述べている。「乱用の批判は全くない」は言い過ぎだと思うが、各国では議会が監視しているのは事実である。

米国では、1980年情報監視法(Intelligence Accountability(Oversight) Act of 1980)に基づき上院情報特別委員会(Select Committee on Intelligence)と下院情報特別委員会(Permanent Select Committee on Intelligence)が監視を行なっており、英国では1994年情報サービス法(Intelligence Services Act of 1994)に基づき、情報委員会(Intelligence and Security Committee : ISC)が監視を行なっている。

急速に進歩した情報通信技術は、国家主体のサイバー・テロやサイバー・エスピオナージ(ネットワーク上でのスパイ活動)という安全保障上の新しい脅威を生み出した。ともすれば我が国ではこれらをサイバー犯罪として捉えがちであるが、これらを国家安全保障上の重大な脅威と捉えた取組みが早急に必要である。(了)

¹米軍統合用語集(JP 1-02)「Measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions.」

²サイバースペースとは、重要な産業における情報技術インフラの相互依存したネットワークである。それにはインターネット、電気通信、コンピュータ・システム、並びに組み込み型のプロセッサ及び制御装置が含まれる。」BSK第23-2号「サイバースペース政策の再検討」(2011年)7頁

³<http://www.time.com/time/magazine/article/0,9171,1098961,00.html>

⁴<http://www.time.com/time/magazine/article/0,9171,1626744,00.html>

⁵

<http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20HPSCI%20White%20Paper%20on%20Cyber--Final%20DEC%2008.pdf>

⁶同上

⁷同上

⁸同上

⁹フォーリン・アフェアーズ・レポート、ウィリアム米国防副長官 2010年10月号「ペンタゴンの新サイバー戦略—なぜアメリカはサイバー軍を立ち上げたか」

<http://www.foreignaffairsj.co.jp/essay/201010/Lynn.htm>

¹⁰<http://online.wsj.com/article/SB124027491029837401.html#mod=article-outset-box>

¹¹<http://online.wsj.com/article/SB123914805204099085.html>

¹²<http://www.computerworld.jp/topics/vs/139989.html>

¹³読売オンライン、2010年9月27日(読売新聞)

<http://www.yomiuri.co.jp/net/news/20100927-OYT8T00458.htm>

¹⁴<http://www.naoru.com/esyuron.htm>

¹⁵<http://www.jiten.com/dicmi/docs/k18/19036s.htm>

¹⁶<http://wiredvision.jp/news/200709/2007090323.html>

- ¹⁷ http://www.wired.com/politics/security/multimedia/2007/08/gallery_wiretaps?slide=1&slideView=4
- ¹⁸ <http://japan.zdnet.com/news/sec/story/0,2000056194,20391941-2,00.htm>
- ¹⁹ <http://www.officepolaris.co.jp/icp/2006paper/2006007.pdf>
- ²⁰ http://www.telegeography.com/ee/free_resources/figures/gig-02.php
- ²¹ http://www.nsawatch.org/nsa_octopus.jpg
- ²² <http://itpro.nikkeibp.co.jp/article/MAG/20061205/255997/>
- ²³ <http://www2.nsknet.or.jp/~azuma/d/darpa.htm>
- ²⁴ <http://www.jiten.com/dicmi/docs/t/11568s.htm>