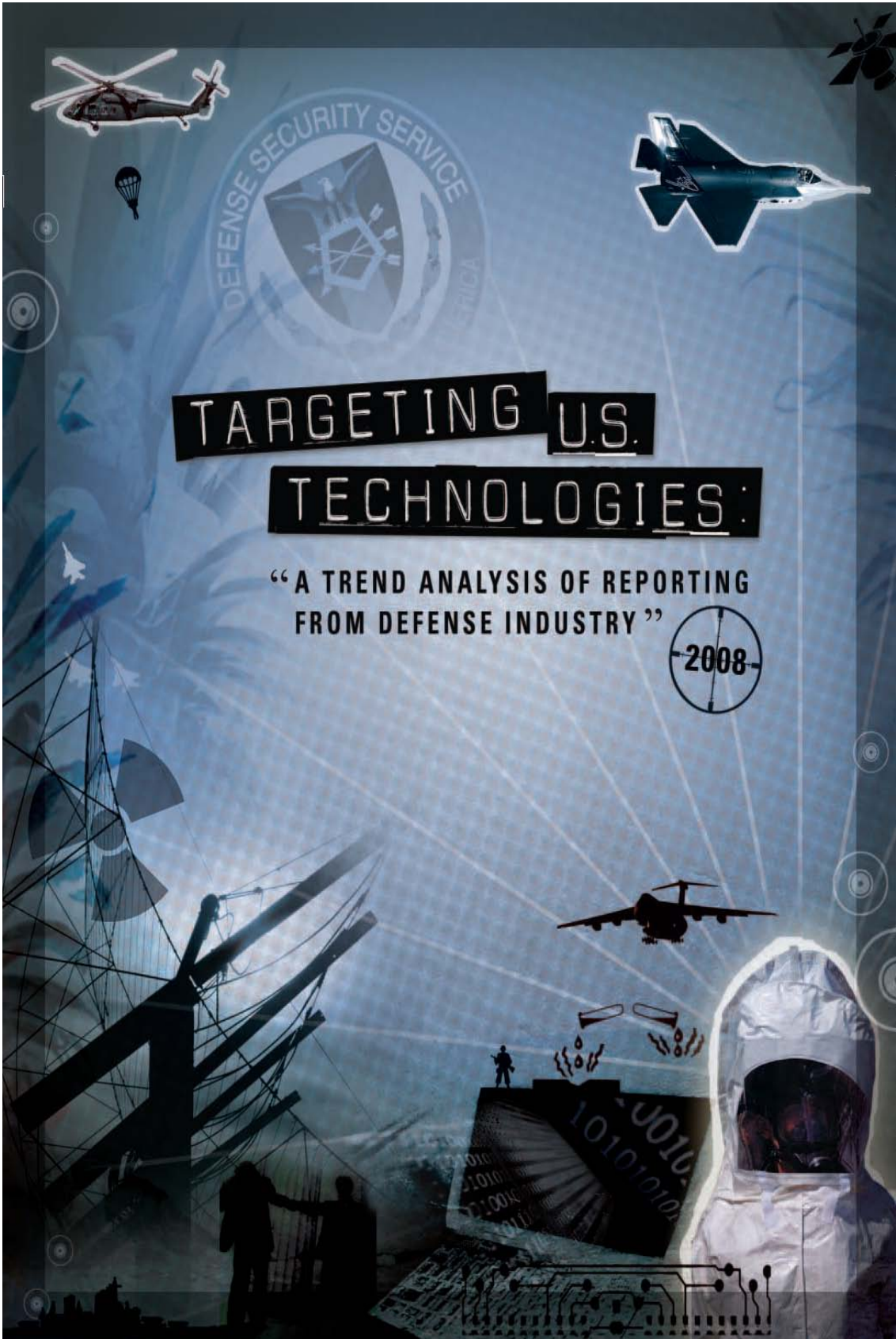


# 標的にされる合衆国技術 ( TARGETING U. S. TECHNOLOGIES ) — 防衛関連企業報告に基づく傾向分析 2008 — ( A TREND ANALYSIS OF REPORTING FROM DEFENSE INDUSTRY )

平成22年1月

財団法人 防衛調達基盤整備協会 ®





**TARGETING U.S.  
TECHNOLOGIES:**

**“A TREND ANALYSIS OF REPORTING  
FROM DEFENSE INDUSTRY”**

**2008**



出版：国防保全局カウンターインテリジェンス理事会

執筆者：

Ms. Sara DeWitz

Mr. Joseph

Mr. Timothy Deer O'Brien

Mr. John Parsons

Mrs. Erika Souliere

<http://www.dss.mil>

## は し が き

国防総省の国防保全局(DSS)には、防衛関連企業と協力の上、重要な技術及び情報を保護する任務が付与されている。国防総省と秘密区分指定情報を取り扱う契約を締結した防衛関連企業は、国家産業保全計画運用マニュアル(NISPOM)に基づき、同企業の情報及び従業員を標的とした外国の不審な実体の活動について、DSS に不審接触報告を行うことが求められている。

本出版物「標的にされる合衆国技術：防衛関連企業報告に基づく傾向分析-2008」は、DSS のカウンターインテリジェンス・オフィス(DSSCIO)が、防衛関連企業からの不審接触報告に基づき、外国からの不審な情報収集活動を分析した結果を示したものである。その目的は、国防総省のカウンターインテリジェンスに係わる政策立案及び意思決定は無論のこと、防衛関連企業のカウンターインテリジェンス活動における教育訓練や対策等に資することであり、内容としては、どの地域のどのような所属の不審な実体が、どのような手口を使用し、どのような技術情報の収集を企てたかを明らかにするとともに、それらの傾向分析を行ったものである。

我が国においても、外国のインテリジェンス機関が関係すると思われる民間企業からの重要技術情報の流出が散見されている。また、経済産業省が行った製造関連企業を対象とした技術情報流出アンケート調査では、38%の企業が、情報流出があったか又はあったと思われると回答している。

我が国の民間企業の先端技術を含む企業機密が、外国からの様々な手口を使用した収集活動の標的になっていることはこのような実態からも明らかであり、本出版物が示す米国における外国の不審な実体による収集活動の傾向分析情報は、我が国の民間企業に対しても有用な情報になり得るものと思われる。

本出版物が、我が国における技術情報管理の向上にいささかでも寄与貢献できれば、望外の幸せである。

平成 22 年 1 月

財団法人 防衛調達基盤整備協会  
理 事 長 宇田川 新一



## 目 次

序 論 .....	1
管理者向け要約.....	3
A. 主な成果.....	3
B. 地域別収集動向.....	4
C. サイバースペースの利用傾向 .....	5
D. 収集家の所属 .....	6
E. 収集手口.....	6
F. 標的にされた技術 .....	6
背 景 .....	9
A. 分析評価の対象範囲と手法 .....	10
B. 評価用語の説明.....	10
サイバーの利用動向 .....	13
地域別収集動向.....	17
A. 東アジア及び太平洋.....	17
B. 中近東 .....	21
C. 欧州及びユーラシア .....	25
D. 南及び中央アジア .....	28
事例研究 .....	33
見 解 .....	35
A. 結論.....	35
B. 予測.....	36
参照地図 .....	39
フィードバック様式 .....	43

本書においては、読者による読みやすさと理解を容易にするため、くり返し利用される用語の略号記述説明を各節の冒頭において示すこととした。



## 表目次及び図目次

表	図
サイバー	サイバー
表 1 発生地域……………13	図 1 所属……………14
表 2 標的にされた技術……………15	図 2 手口……………14
東アジア及び太平洋	東アジア及び太平洋
表 3 標的にされた技術……………19	図 3 所属……………17
	図 4 手口……………19
中近東	中近東
表 4 標的にされた技術……………23	図 5 所属……………21
	図 6 手口……………22
欧州及びユーラシア	欧州及びユーラシア
表 5 標的にされた技術……………26	
	図 7 所属……………25
	図 8 手口……………26
南及び中央アジア	南及び中央アジア
表 6 標的にされた技術……………30	図 9 所属……………28
	図 10 手口……………29



## 序 論

### 標的にされる合衆国技術 防衛関連企業報告に基づく傾向分析

国防保全局(Defense Security Service: DSS)には、防衛関連企業と協力の上、重要な技術及び情報を保護する任務が付与されている。この保護活動に不可欠なのが、秘密区分指定資料にアクセス権を持つ防衛関連企業、すなわち「施設保全適格証明書を持つ防衛関連企業(Cleared Defense Contractor: CDC)」に対する要求事項であり、CDC に対して不審な接触及び潜在的情報収集の企てを確認の上、報告することを求めている。その要点は、国家産業保全計画運用マニュアル(National Industrial Security Program Operating Manual: NISPOM)に述べられている。DSS は、防衛関連企業の情報及び従業員を標的とした不審な実体<sup>1</sup>の活動を示すこれら不審接触報告(Suspicious Contact Report: SCR)を CDC から受け、その分析結果に基づいて本報告書を出版した。

本報告書は、セキュリティ責任者、CDC、インテリジェンス専門家並びに国防総省の政策立案者及び意思決定者が、技術収集脅威を評価の上、適切なセキュリティ対策を講ずる助けとなることを意図している。本報告書は、防衛関連企業から受取った SCR を分析し、最も頻繁に標的とされた合衆国技術を明らかにするとともに、情報収集に最も利用された一般的手口の提示、情報収集を試みた組織及びそれら収集活動の発生地域の明確化を行ったものである。

DSS は、すべての施設セキュリティ責任者(Facility Security Office: FSO)が本報告書の情報を利用することにより、施設のセキュリティ意識向上及び教育プログラムの充実を図ることを奨励する。それぞれの企業内における脅威意識の向上に加え、確固たる訓練に基づく SCR の更なる提出は、本報告書の分析成果の完全性に貢献することになる。企業のセキュリティ・プログラムを効果的なものとするには、SCR を適時に DSS 支部へ提出することが不可欠である。

本報告書は、合衆国 CDC の FSO からの強力な支援を得て作成したものである。DSS は、合衆国 CDC の従業員に対し、NISPOM への継続的支援及び本報告書作成に当たっての貢献に謝意を表す。

DSS 局長

KATHLEEN M. WATSON

---

<sup>1</sup> 実体：本翻訳においては「entity」を「実体」とした。本報告書における実体とは、個人、グループ又は組織を意味する。



## 管理者向け要約

### A. 主な成果

本報告書は、DSS が国防総省(Department of Defense: DoD)のガイダンスに基づき、施設保全適格証明書を持つ防衛関連企業(Cleared Defense Contractor: CDC)コミュニティにおいて開発及び維持されている情報及び技術に対する外国からの標的行為の可能性について、その詳細と分析結果を述べたものである。本報告書の主な内容は、2006 年度及び 2007 年度(FY06-FY07)の間に、CDC コミュニティから報告された外国の不審な実体による不審接触について、DSS が行った分析から得られたものである。

以下に述べる事項は、DSS が CDC から FY06-FY07 の間に受け取ったデータ分析に基づく主な成果である。

- DSS が CDC から受け取った「不審」とされた外国の接触に係わる詳細報告数は、引き続き急激な増加状態にあることを示している。このことは、ある面では、爆発的なインターネット利用の拡大、そしてインターネットの持つ禁止されることも取捨選択されることもない、グローバルなアクセス機会がますます増加したことによるものと思われる。また、CDC における脅威意識の強化は、従業員の責任事項としての不審なインシデントの識別と報告の増加をもたらした一因であると考えられる。
- 東アジア及び太平洋地域が発生源となった不審接触数は、他の地域に比べ、最大かつ飛びぬけた値となっている。これら不審接触の特徴及び数値的に不均衡な様相は、市場の自由競争、経済的及び軍事的優位のため、同地域による一致団結した接触利用努力を示唆するものである。
- DSS は、不審接触行為に及ぶ実体の所属に変化があることを確認した。地域別分析における接触発生源のほとんどは、その数において商業所属の不審な実体が政府組織所属の不審な実体を圧倒している。このことは、接触をより当たり障りのないものとするため、関係する政府又は政府所属の実体代理として非政府所属の不審な実体を利用するという意図的な企てと思われる。また、この変化には、ますます成長及び相互に係わり合いをもつグローバル経済も、反映しているものと思われる。
- CDC データ・システムに保管されている情報への不正アクセス手段として、サイバースペースを利用する懸念がますます高まっており、この利用は DSS が「不審」と考える接触のかなり大きな割合を占めている。このような脅威の持続に対抗し、敵体制構成要素による情報戦場の支配を低減するセキュリティ対策を効果的なものとするには、不断の警戒を怠ってはならない。

## B. 地域別収集動向

合衆国国務省によれば、世界には200の独立国家が存在している。これら半数以上の国々の不審な実体が FY06-FY07 の間に、少なくとも一度は合衆国の防衛技術又は情報を不審な方法で取得することを企てた。DSS は、国務省が定義する6地域にこれらの企てをグループ分けした(国務省の各地域局内に存在するこれらの国々の情報は、本報告書の参照地図による)。DSS が FY06-FY07 において、最も多く不審接触報告(Suspicious Contact Report: SCR)に係った6地域を多いほうから順に並べると次図のようになる。

また、全 SCR の5%については、その発生源となった地域が不明であった。不審な要求に係る地域が、必ずしも標的となった技術の最終的なエンドユーザーでないことは注目に値する。収集家は、匿名性のプロキシ<sup>2</sup>の利用又は収集活動の根拠地を他の地域に置くことにより、彼らの意図又は最終的なエンドユーザーのアイデンティティを隠蔽するかもしれないのである。

提出された SCR 及びその分析の結果は、「東アジア及び太平洋」が最も積極的に合衆国防衛技術の不正な入手を企てた地域であることを示している。この地域は、FY06-FY07 における収集の企ての36%を占めており、歴史的にも最も積極的な収集家となっている。

この地域に係る報告数は、地域別 SCR 数の最も大きな割合を占めており、前年に比べ30%から36%へとわずかながら増加している。「東アジア及び太平洋」地域に係る報告数は増加しているものの、その他の地域に係る報告数は一定に留まっているか又はわずかながら減少している。

繰り返すが、FY06-FY07 における「中近東」地域に係る報告は、「東アジア及び太平洋」地域に次ぐ最も積極的な収集活動地域であることを示しており、全報告件数の20%を占めている。この地域の次に「欧州及びユーラシア」及び「南及び中央アジア」地域に係る報



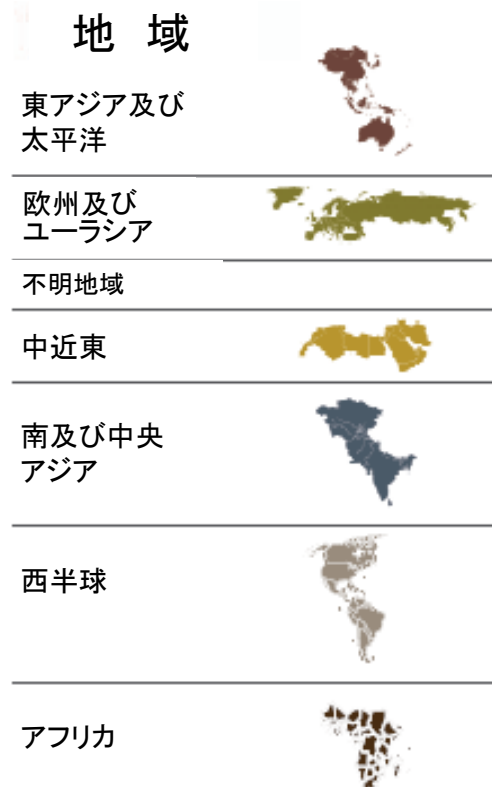
<sup>2</sup> プロキシ(proxy)とは、組織内部のネットワークと外部のインターネットの境界に設置され、直接インターネットに接続できない内部ネットワークのコンピュータに代わって、代理としてインターネットとの接続を行うコンピュータをいう。

告があり、それぞれ全報告件数の 17%及び 16%を占めている(注意：残るアフリカ及び西半球の 2 地域に係る SCR 件数はごくわずかであることから、今回の報告においては最も積極的な収集地域の対象外とした)。

さらに、FY06-FY07 を通じて最も不審な収集活動を行ったサイバー実体は、次に示す地域が発生源であると思わせるインターネット・プロトコル(IP)アドレスを持っており、多い順に示すと次図のようになる。

### C. サイバースペースの利用傾向

本報告書は、ますます蔓延の度合いを高めつつあるサイバースペース利用の収集脅威を認識し、それを特に別項として記述した。防衛関連企業から DSS に報告されたサイバー・インシデントは、外国の不審な実体が非秘密区分指定企業ネットワーク上で管理されている非秘密区分指定情報を標的にしていることについて詳細に述べている。しかしながら、DSS は、秘密区分指定ネットワークについての詳細な報告がないことが防衛関連企業を誤ったセキュリティ感覚に至らしめるのではないかと、とういことを懸念している。防衛関連企業は、秘密区分指定及び非秘密区分指定の両ネットワークをセキュアなものとするため、事前の対応策を講ずるべきである。



DSS は、FY06-FY07 の間において、防衛関連企業のコンピュータ・システムやネットワークに対する侵入すなわち「ハッキング」の企てを含むインシデント報告が、全報告の 52%を占めていることを確認した。これらのインシデントは、東アジア及び太平洋地域を発生源とするインターネット・プロトコル (IP) アドレスを持っていた。DSS の分析者は、ハッキングが特定の地域を示す IP アドレスを持つとはいえ、同地域内収集家の 96%の所属は「不明」とであると分類している。これらの所属については、IP アドレス (例：政府、大学、民間など) の特性、及びユーザーが匿名性のプロキシを介して真のアイデンティティを隠蔽すると思われることから、確定するのが困難な状態にある。FY06-FY07 の間、サイバーを利用した不審な実体が最も興味を抱いた標的は「情報システム」技術であった。かつ、彼らが好んだ手口は「侵入の企て」であり、全サイバー・インシデントの 61%がこの分類に属していた。

## D. 収集家の所属

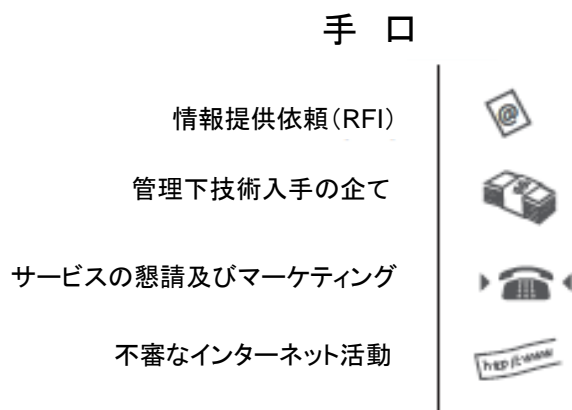
DSS は、収集家の所属を決定するとともに、どの外国の不審な実体が合衆国技術を標的にしているのかを確定するため、各 SCR を分析する。例えば、「政府」と分類された SCR は、外国の政府又は機関に所属する者又はその代理者の不審な活動を意味する。その他の収集家には、「商業」、「個人」又は「政府関連」所属の不審な実体がある。DSS は、FY06-FY07 における合衆国技術収集家のトップが「商業」所属の不審な実体であると判断した。この商業に分類された SCR は、2004 年度(FY04-FY05)統計値の 5%増となっており、結果として不審な収集実体の所属のトップが「政府関連」から「商業」へと置き換わった。この暗示的な増加は、民間の研究開発を捜し求めている外国の不審な実体が、政府又は政府関連の不審な実体を発生源とする収集活動の焦点を商業へシフトしたことによるものと思われる。

## E. 収集手口

DSS にとって、発生地域及び収集家の所属を確認した次の段階として、この不審な実体による制限された情報への収集の企てがどのようなものであったかを知ることが重要となる。DSS は、収集手口(Method of Operation: MO)の識別と分析結果に基づき、最も普及した収集テクニック及び指標を明らかにした上で、そのような MO の効果を無効化する対策を CDC に推奨している。

FY06-FY07 の間におけるトップ・フォーの収集手口は、外国による全収集企ての 70% 強を示している。

FY04-FY05 からトップの座を維持している「情報提供依頼(Request For Information: RFI)」は 12%も落ち込んだものの、「不審なインターネット活動」は 5%増となった。FY06-FY07 は FY04-FY05 と同様に、「RFI」と「管理下技術入手の企て」が引き続きトップ・ツーMO として留まっている。



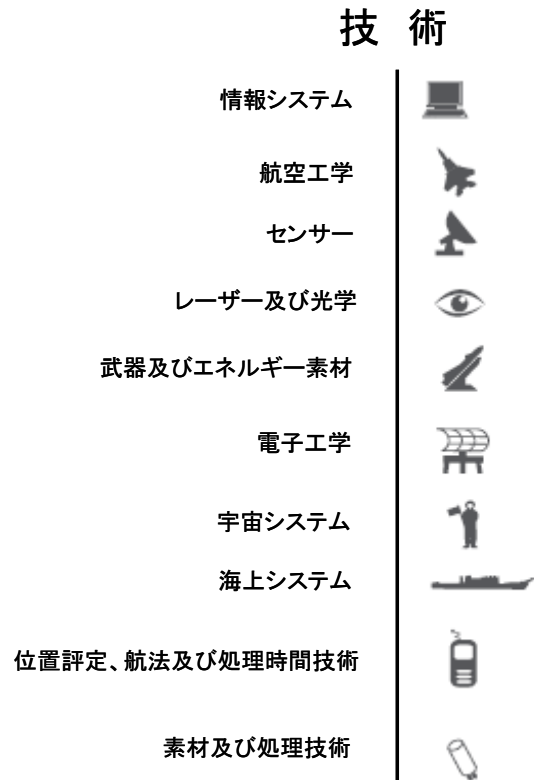
## F. 標的にされた技術

DSS は、外国が関心示している合衆国防衛技術について、開発科学技術リスト(Developing Scientist and Technologies List: DSTL)が示す 20 の分類に従って分析している。分析の重要な目的は、不審な実体が取得しようとする標的にしている技術が何かを明らかにすることである。そして、この収集技術の優先順位を知ることにより、合衆国の CDC

が技術及び秘密区分指定情報の漏えい低減のためのセキュリティ対策事項を確立する助けとなるのである。

DSS の FY06-FY07 における SCR 分析結果に基づき、標的となった技術を外国の不審な実体の関心の度合いの高いものから順に並べると次図のとおりとなる。これは、収集に当たっての優先順位を示すものと判断される。

この収集の優先順位は、前年の評価結果と大体一致している。FY06-FY07 における不審な実体は、前年に引き続き「情報システム」技術を最も頻繁に標的としており、この技術に係る SCR の登録件数は前年に比べ 5%増となっている。また、残りの 9 分類もわずかな増加を示しており、これらの技術に引き続き関心があることを示している。しかしながら、DSS は、これらの SCR 増加要因の一部が、CDC における意識向上の強化及び外国の不審な実体が関心を示すこれら既知標的に係る不審なインシデント報告の積極性によるものと信じている。





## 背 景

2008年7月16日付けの国防総省訓令第5200.39号(DoDI 5200.39, July 2008)は、施設保全適格証明書を持つ防衛関連企業(Cleared Defense Contractor: CDC)コミュニティ内で発生した不審接触、すなわち合衆国 CDC 基盤の従業員、情報及び技術に対する外国の脅威を示す詳細報告書の出版を DSS に求めている。同訓令によれば、DSS は、脅威リスクの高い技術が何かを知らしめるとともに、適切な脅威対策を講ずる支援を行なうため、この報告書を DoD カウンターインテリジェンス・コミュニティ、国家組織(national entity)及び CDC コミュニティに配付することとされている。DSS は、2006年2月28日付けの国防総省マニュアル第5220.22号(DoD 5200.22-M, February 28, 2006)国家産業保全計画運用マニュアル(National Industrial Security Program Operating Manual: NISPOM)の第1章第3節に規定される報告要求事項に従い、CDC からの不審接触報告(Suspicious Contract Report: SCR)を受領し分析する。DSS は、これらの SCR 分析に基づき、本報告書「標的にされる合衆国技術：防衛関連企業報告に基づく傾向分析」を出版する。

先の年次報告書は単年度を対象としたものであったが、本報告書は2006年度及び2007年度に及ぶ複数年度を対象としている。したがって、DSS は2006年度を対象とした2007年度版報告書を出版しなかった。しかしながら、今後は毎年出版することとする。

本報告書の傾向分析は、単年度対象の2006年度版とは異なり FY06-FY07 の複数年度を対象とし、合衆国 CDC コミュニティを標的とした外国の脅威実体の発生様相を地域別に示すものである。DSS は、本報告書における脅威実体の国について、それらの国を所掌範囲とする国務省各地域局の地域名称を利用した。本報告書には、地域別の統計及び傾向上の分析、各地域に属する外国の不審な実体が CDC コミュニティ標的時に利用したこれまでの手口、及びそれら不審な実体が標的とした具体的な技術が含まれている。また、各節には、CDC コミュニティに対する今後の標的行為活動予測の分析評価結果が述べられている。

また、本報告書は、CDC コミュニティが直面したサイバー脅威の具体的な情報についても提供している。DSS はこれまで、不審なサイバー活動について、地域別収集傾向のサブ項目として含めていた。しかしながら、DSS は、CDC コミュニティに対するサイバー攻撃報告が増加したことから、この増加脅威に対応するには別項で取り扱うことが適切であると判断した。

本報告書は、DSS の継続活動の一部として出版したものであり、合衆国 CDC 基盤を標的にした外国の不審な実体についての意識向上を図るとともに、そのようなインシデント発生時には速やかに DSS に報告するよう推奨するものである。本報告書は、脅威実体が特定技術の情報取得に利用した手口の解明、脅威リスク下にある技術の明示及び外国の取

集家の将来活動予測について述べている。また、本報告書は、セキュリティ専門家が外国の標的行為を検知、抑止、低減又は無効化するに当たって、その利用に即座に供し得る参考ツールとなることを意図している。

#### A. 分析評価の対象範囲と手法

本報告書は、主に DSS が CDC コミュニティから収集した SCR に基づいているが、全インテリジェンス・コミュニティからの報告についても言及している。DSS は、企業から受領したすべての SCR を分析の対象とするが、DSS が潜在的なカウンターインテリジェンスの懸念事項と断言したものだけに基づいて本報告書は作成されている。DSS は FY06-FY07 の間に、総計 4,897 通の SCR を CDC コミュニティから受領した。DSS は、これらの SCR に対して分析プロセス及び DSS の外国インテリジェンス脅威評価手法を用い、2,269 通を分析評価対象として選定した。選定されたこれらの SCR は、CDC コミュニティに対して潜在的なカウンターインテリジェンス脅威となるか、又は DSS が合衆国の利益に対する敵対性として決定した構成分子とつながりがあると断言した脅威に係わる報告内容であった。

DSS は、FY06-FY07 間の SCR データに対する正確な統計分析を行うため、FY04-FY05 間のデータを分析に組み入れ、比較データとして掲載した。本報告書におけるすべての傾向、統計値及び分析結果は、FY04-FY05 及び FY06-FY07 間の比較データを示している。

DSS は、外国の脅威が関心を示す合衆国防衛技術について、開発科学及び技術リスト (Developing Scientific and Technologies List: DSTL) に示されている技術名称を用いた。DSTL は世界中で開発中の科学技術能力に係わる明細表であり、そこに掲載された技術は、将来における合衆国軍隊の能力を著しく強化又は低下させる可能性を持つものである。DSS は、各技術の分類及びサブ分類を定義する際に、この DSTL を分析目的に不可欠なひな型として利用している。

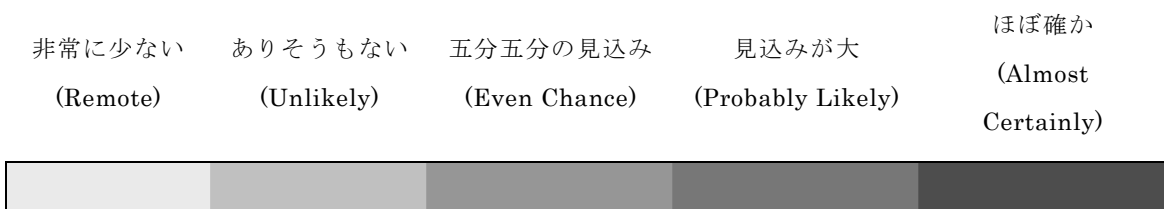
前述のとおり、DSS が SCR を分類・選定するのは、それらがカウンターインテリジェンスとの関連を持つか、又は CDC コミュニティに潜在的なカウンターインテリジェンス脅威をもたらすか否かを決定するためである。DSS の分析家は、SCR を吟味し、重要な合衆国技術、標的行為に及んだ不審な実体、収集の手口、並びに CDC コミュニティから以前提出された報告及び全インテリジェンス・コミュニティからの情報との関係について調査する。

#### B. 評価用語の説明

DSS は、本報告書「標的とされた合衆国技術：防衛関連企業報告に基づく分析傾向」における評価用語として、インテリジェンス・コミュニティの評価用語を採用した。「と思わ

れる」又は「示唆する」の用語は無論のこと、「我々は・・・と判定する」又は「我々は・・・と評価する」などの類語的表現法の利用は、我々の分析的な評価や判定努力を伝達するための表現である。不完全又は断片的な情報に基づくこれらの評価は、事実でも証拠でもなく又は経験則に基づく確証若しくは知識でもない。分析判定の中には収集した情報に直接基づくものもあるが、その他は以前の判定に委ねており、両判定とも今後の基礎データとなる。我々は、いずれのタイプの判定にせよ、何か事実であることを示すか又は2つの事項若しくは問題を絶対的に結びつける「証拠」を持っているわけではない。

「公算(見込み)(likelihood)」に属するインテリジェンス判定は、開発、事象又は傾向の蓋然性に係わる DSS の意向を示すものである。次に示す図は、各用語間の大まかな関係を示すものである。



我々は、事象が生起しないとする表現には「ありそうもない(unlikely)」の用語を利用しない。我々は、五分五分の見込みを上回る場合に「おそらく(probably)」及び「おそらく(likely)」の用語を利用する。我々がありそうもないか又は極めて少ない事象を示す場合で、かつ、その帰結がその言及を正当化する場合は、「我々は・・・だと片付ける(dismiss)ことはできない」、「我々は・・・を除外(rule out)することはできない」及び「我々は・・・を無視(discount)することはできない」の文言を利用する。我々は、「かもしれない(may)」、「・・・とそれとなく示す(suggest)」などの文言については、関連する情報が一般的に存在しないか、不完全又は断片的で評価不能の場合に、その見込みを示す用語として利用する。

また、我々は、判定の際の公算(見込み)度合を示す用語の利用に加え、我々の評価を支持する情報の範囲と質に基づき、「高(high)」、「中(moderate)」又は「低(low)」の信頼度レベルも利用する。



## サイバーの利用動向

### 1 全般

防衛関連企業からの報告に基づく DSS の分析結果は、施設保全適格証明書を持つ防衛関連企業(Cleared Defense Contractor: CDC)コンピュータ・ネットワークに対する標的行為の増加を示している。DSS が CDC から FY06-FY07 間に受領した不審なサイバー活動(Suspicious Cyber Activity: SCA)報告件数は 229 となっており、FY04-FY05 間の報告件数 80 に比べると大幅な増加となっている。コンピュータ・システムへの侵入の企て及び関連するサイバー・ベースの活動は、自国の研究開発(Research & Development: R&D)プログラムの促進及び合衆国先進技術の模倣を求める多くの外国の不審な実体にとって、魅力的で相対的に低リスクの選択肢となっている。DSS は、識別可能なコンピュータ・ネットワーク侵入活動のさらなる調査について、法の執行機関及びカウンターインテリジェンス機関に委ねている。

### 2 発生地域

CDC からの FY06-FY07 間における SCA 報告によると、東アジア及び太平洋地域の不審な実体が最も活発な収集家であること、及び同地域に属する報告件数が全 SCA 報告件数の 52% を占めていることを示している。報告は、この地域における不審な実体が自国の

表1:発生地域

地 域	FY2006-FY2007 (%)	FY2004-FY2005 (%)
東アジア及び太平洋	52	57
欧州及びユーラシア	21	16
不明	18	9
中近東	4	12
南及び中央アジア	4	3

指揮統制通信及びインテリジェンス活動の改善は無論のこと、R&D プログラムを促進するため、CDC を標的にしている公算が大きいことを示している。東アジア及び太平洋地域に次ぐ第二の活発な収集活動地域は、欧州及びユーラシアであり、全 SCA 報告件数の 21% を占めている。この%値は、FY04-FY05 の 16% に比べ、わずかな増加となっていることを示している。DSS はすべての侵入の企てについてその発生地域を明らかにすることを試みたが、実際の発生地域が未決定や不明のまま残された SCA が多々あった。このような報告は、件数別 SCA 報告の第 3 位となっている。表 1 の%値は、標的行為に及んだ不審な実体の発生可能地域を示すものであり、単に DSS の SCR 分析結果に基づくものである。また、この表は必ずしもサイバー活動の発生地域を確証付けるものでもない。

分析家の意見：報告件数の増加は、収集家によるサイバー不正利用戦術の使用増加は無論のこと、CDC によるサイバー意識の向上及び報告傾向の増加の両者を直接反映したものである。(信頼度レベル：高)

### 3 収集家の所属

DSS は、報告された情報の評価及び調査の実施、並びにこれまで実際にあった収集の企てとの関連付けを行った後、SCA 収集家の所属を明らかにする。DSS は、可能ならばすべての場合について、インターネット・プロトコル(Internet Protocol: IP)を SCA 発生元確定の基礎として利用する。DSS の分析家は、補足情報が入手可能な場合、ファイル・ネームや具体的なネットワーク侵入手法など

の技術データと比較することにより、発生地域及び所属組織を決定する。もともと、いわゆる「サイバー・ハクティビスト(hacktivist)」、多様な国際的活動家、特定地域独特の様々な不審な実体などがこれらサイバー活動の陰に存在していることもあり、このようなサイバースペースの特徴が政府又は民間の所属特定を著しく困難なものにしている。例えば、外国の不審な実体は、自由に利用可能な匿名性プロキシを利用するか又は全地球に及ぶオープン WiFi ホットスポット<sup>3</sup>のいずれかから攻撃を行うことで、IP アドレスを容易に隠すこと(IP マスキング)ができる。これらの資源、とりわけオープン匿名性プロキシ利用可能性のますます増加及びそれに伴う IP マスキングの容易さが、セキュリティ及びカウンターインテリジェンス・コミュニティによる発生地域内における所属の断定を複雑なものとしている。DSS は、FY06-FY07 の間に報告された事象の 96% について、SCA の背後にある明確な所属を決定付けることができなかった。

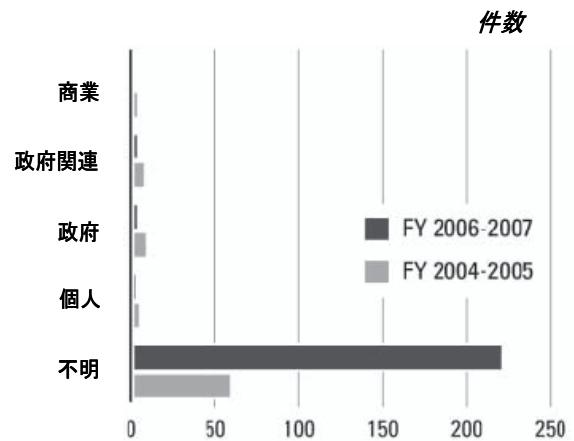


図1: 所属

### 4 収集の手口

サイバー収集家は、最も一般的な手口(Method of Operation: MO)として「侵入の企て(Attempted Intrusion)」を採用した。この MO は FY06-FY07 の間において、全 SCR の 61% を占めた。CDC ネットワークに不正アクセスを行うためのこれら企ての大部分は、ソーシャル・エンジニアリング手法を用いたものであり、悪意のある資料又はソフトウェアを添付し、人気のある商用ソフトウェア・プログラムを利用させようとした電子メールを利用するものであった。最も利用された第 2 番目の MO は「確認された侵入(Confirmed

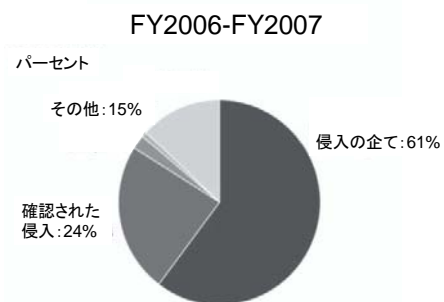


図2: 手口

<sup>3</sup> 無線 LAN 接続ポイント

Intrusion)」活動であった。FY06-FY07 の間に報告された全 SCR の 24%は、CDC の非  
 秘密区分指定ネットワークに対する確認された侵入であった。

FY06-FY07 におけるサイバーSCR の残余 15%は、「ボットネット」活動(ボットネット  
 とは、「ゾンビ・コンピュータ」と言われる危うい状態にされたコンピュータの集合体に対  
 する一般的な用語であり、ありふれた指揮統制インフラの下で悪意のあるソフトウェアを  
 走らせる)、不審なサービス妨害攻撃及びファイアウォール・ログである。

## 5 標的にされた技術

CDC からの FY06-FY07 間における報告は、開発科学及び技術リスト(DSTL)に掲載さ  
 れている全 20 技術が外国の不審な実体の標的となったことを示している。サイバー収集  
 家が最も頻繁に求めた技術は「情報システム」であり、全サイバー関連収集の企での 40%  
 強を占めている。「武器及びエネルギー素材」は、第 2 番目に最も頻繁に標的とされた技  
 術分野であり、全 SCA 報告の 9%を占めている。東アジア及び太平洋地域の不審な収集実  
 体は、この分野における最も活動的な収集家であった。「航空工学」技術は、第 3 番目に  
 最も標的とされた技術分野であり、全 SCA 報告の 7%を占めている。

表 2：標的にされた技術

開発科学及び技術リスト (DSTL) コード	FY06-FY07		FY04-FY05	
	事例数	%	事例数	%
航空工学	22	7	5	5
武器及びエネルギー素材	26	9	8	8
応用生物学	6	2	1	1
生物医学	2	1		
化学	4	1	1	1
指向性運動エネルギー	1	<1		
エネルギー・システム	1	<1		
電子工学	18	6	7	7
地上システム	1	<1		
情報システム	131	43	23	24
レーザー及び光学	19	6	5	5
製造及び組み立て	1	<1	2	2
海上システム	12	4	18	19
素材及び処理	6	2		
核	3	1	2	2
位置評定、航法及び処理時間	2	1		
センサー	15	5	9	9
シグナチャー・システム	1	<1	1	1
宇宙システム	17	6	1	1
兵器効果	3	1		
不明	12	4	15	15

## 6 予測分析

非秘密区分指定ネットワークを標的にしたサイバー攻撃が近年ますます増加することは、ほぼ確かなことである。攻撃ツールの利用が容易なことと同ツールによるネットワーク攻撃成功確率の高いことが、CDCのネットワークをアクセスの上、操る技術能力を持つ収集家にとって、サイバー標的行為を魅力的なMOに位置づけている。ネットワークに対する侵入の企て件数は、CDC側の強化された検知手法の開発及び設置は無論のこと、脅威に対する意識向上及び報告傾向の増加に伴って増加することはほぼ確かである。さらに、ますますのコンピュータ・ネットワークの複雑化及び防衛関連企業のグローバル化に伴い、サイバー標的行為及び収集活動は、防衛関連企業による脅威の識別及び対処を強化させることになると思われる。(信頼度レベル：高)

## 地域別収集動向

### A. 東アジア及び太平洋

#### 1 概観

前述の評価のとおり、東アジア及び太平洋地域からの不審な実体が FY06-FY07 間における最多の合衆国技術収集家の地位を維持している。これは、第 2 の最多の収集家地域として名高い中近東を発生源とする収集活動をはるかに凌駕するものである。しかしながら、東アジア及び太平洋地域内のどのような種類の不審な実体が頻繁な収集活動を行っているかについては、大きな変化がある。FY04-FY05 の間における最多の不審接触報告 (Suspicious Contact Report: SCR) は、同地域に所在する「政府」所属の不審な実体から発生したものであった。しかしながら、FY06-FY07 においては、「商業」所属の不審な実体が最も活動的な収集家の位置にあった。東アジア及び太平洋地域の不審な実体は、制限された情報を入手する際、「管理下技術入手の企て」収集手口を主に利用した。また、東アジア及び太平洋地域の不審な実体はこの報告期間に、収集活動の焦点を「情報システム」技術、とりわけ軍事用「指揮・統制・通信・コンピュータ・インテリジェンス・捜索及び偵察(Command, Control, Communication, Computer, Intelligence, Surveillance, and Reconnaissance: C4ISR)アプリケーション」に当てた。

#### 2 収集家の所属

DSS は、東アジア及び太平洋地域の収集家に係る 696 件の SCR 分析を行い、制限された技術、秘密区分指定の技術及び企業機密技術に対する入手の企てにおいて、同地域の「商業」所属の不審な実体が「政府」所属の不審な実体を大幅に上回っていることを明らかにした。

東アジア及び太平洋地域内の「商業」所属の不審な実体による FY06-FY07 の間の SCR 件数は、全報告件数の 42% を占めている。FY04-FY05 間の数値を上回るこの著しい増加は、様々な所属の不審な実体が全般にわたって収集活動を継続する中で、合衆国が最も頻繁に直面した不審な実体の所属が「政府」から「商業」に置き換わったことによるものである。実際、図から明らかのように、「政府」所属の収集家に



図3: 所属

よる SCR 件数は大きな変化がないにもかかわらず、FY04-FY05 における第一位の座から FY06-FY07 では第三位に落ち、「政府関連」所属をわずかに下回っている。「商業」所属による収集の企ては、一般的には「政府」所属の収集活動を反映した代理の役を担うものであり、これにより政府の収集要求事項が満足されることになる。また、この増加の一因として、合衆国の施設保全適格証明書を持つ企業(CDC)の職を希望する大卒や院卒生など、従来とは異なった「商業」所属による収集活動の増加がある。

(分析者の意見：我々は、グローバル市場への参加がますます盛んなことから、非在来型収集家の増加を認めないわけにはいかない。しかしながら、収集家の所属が政府から商業へシフトしたことについては、政府所属の不審な実体が管理下技術を手に入れる代わりとして、十中八九、正当又は不法なフロントカンパニーをうまく利用していると判断される。東アジア及び太平洋地域に第三国の商業所属が増加しているが、(政府所属の不審な実体が)小規模な商業行為の代理としてこれらを利用し、輸出入制限手続をうまくかわそうとしているようである。(信頼度レベル：中))

### 3 手口

FY06-FY07 における東アジア及び太平洋地域のトップ・スリーの収集手口(MO)は、その順位が変更となったものの、FY04-FY05 に同じである。CDC からの報告によれば、最も頻繁に利用された収集手口は「管理下技術入手の企て」であり、全 SCR 件数の 35% を占めている。「情報提供依頼」は、第 2 位に下落し全報告の 28% となったが、「サービスの懇請及びマーケティング」は、最も有効な手口として選ばれ第 3 位を維持している。また、収集傾向は「管理下技術入手の企て」又は「情報提供依頼」の手口と「外国人本土訪問の利用」の手口を組合せたものとなっている。例えば、合衆国本土に訪れる代表団が CDC 訪問の間に補足的な秘密区分指定情報を求める、というのが一般的となっている。

(分析者の意見：この管理下技術入手の手口がトップになった理由の一つには、合衆国技術に直接アクセスする許可を与えた合意事項に係わる共同覚書に中で、CDC に押し寄せたエンジニアによるものが考えられる。これらの収集家は、ただ単に情報を求めるだけではなく、多様な軍事及び民事のプログラムにおける開発に必要な特定製品の入手を企てていると思われる。(信頼度レベル：高))

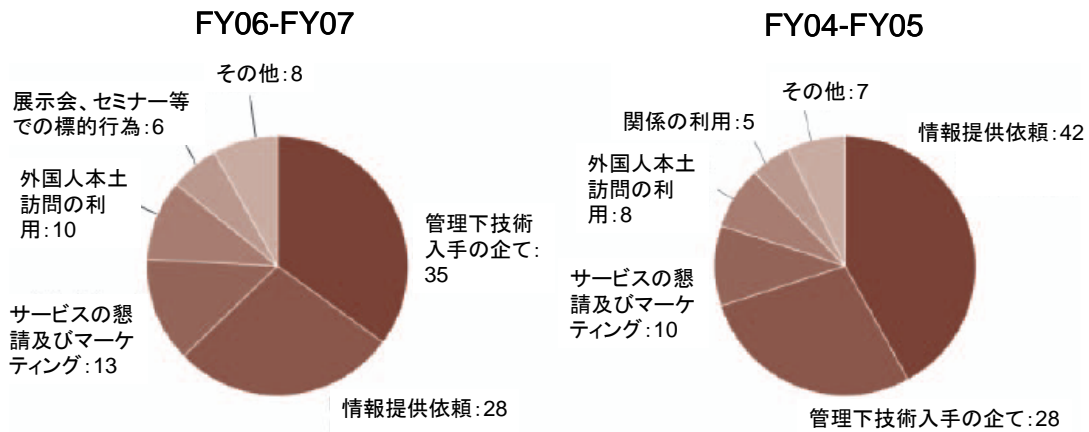


図4: 手口

#### 4 標的にされた技術

東アジア及び太平洋地域が標的とした技術のトップ・ファイブは、FY04-FY05 に比べ大きな変化がなく、その大部分が同じか、又はわずかばかり増加しただけである。しかしながら、「武器及びエネルギー素材」技術は第2位から第5位へと下落した。「情報システム」技術は、最も標的にされた技術として突出しており、C4ISR 及び軍事システム技術に収集焦点を当てたことと一致している。トップ・ファイブの各標的技術分野は、研究開発の近代化及び進展を目的とした現在の「商業」及び「政府」活動を示すものである。

(分析者の意見：情報システムの増加は、収集家が研究開発上の欠落事項に焦点を当てるとともに、軍事及び C4ISR 能力の近代化を望んだためと思われる。(信頼度レベル: 高))

表 3：標的にされた技術

開発科学及び技術リスト (DSTL) コード	FY06-FY07		FY04-FY05	
	事例数	%	事例数	%
航空工学	91	11	53	9
武器及びエネルギー素材	64	8	57	9
応用生物学	12	1	12	2
生物医学	3	<1	2	<1
化学	10	1	17	3
指向性運動エネルギー	3	<1	3	<1
エネルギー・システム	7	1	14	2
電子工学	52	6	40	7
地上システム	11	1	5	<1
情報システム	186	23	133	22
レーザー及び光学	90	11	53	9
製造及び組み立て	24	3	9	1
海上システム	49	6	22	4

素材及び処理	14	2	18	3
核	5	1	5	<1
位置評定、航法及び処理時間	38	5	16	3
センサー	101	12	54	9
シグナチャー・システム	7	1	28	5
宇宙システム	34	4	45	7
兵器効果	7	1	2	<1
不明	15	2	25	4

## 5 予測分析

東アジア及び太平洋地域の不審な実体が、彼らの国の研究開発プログラムを強化するため、先進技術を手に入れることに焦点を当て続けることはほぼ確実である。政府と政府関連に所属する収集家は、軍事システム技術収集活動の増加に伴い、商業所属の不審な実体に圧力をかけ、その収集活動の継続と増加を求めるものと思われる。また、収集の企ては、東アジア及び太平洋地域に課せられた貿易制限による輸出入制限を回避するため、第三国の商業所属の収集家を介したより巧妙なものとなろう。商業所属の不審な実体が、共同合意事項及び合衆国会社の買収を介して、デュアル・ユーズ技術取得に関与することはほぼ確実である。技術取得の焦点となるのは、研究開発上の短所、とりわけ C4ISR 技術とそのサブセットであると思われる。このように繁殖する脅威に立ち向かうためには、合衆国企業内における最高度の意識向上及び警戒が求められる。(信頼度レベル：高)

## B. 中近東

### 1 概観

中近東地域の不審な実体から発生したとする 453 の報告件数は、FY06-FY07 における最も積極的な収集活動地域の第 2 位を維持している。「政府関連」及び「商業」所属の収集家の数は、企業からの報告において抜きんできた値を示しており、これらに「政府関連」所属の収集家による収集の企てが続いている。不審な実体が主に求めた技術には「情報システム」が含まれているが、この地域の収集家は「航空工学」及び「センサー」技術に対しても関心を示している。この地域の収集家に好まれた収集スタイルすなわち手口(MO)の第 1 位は「情報提供依頼」であり、これに僅差で第 2 位の「管理下技術入手の企て」が続き、第 3 位は%値が大分下がるものの「サービスの懇請及びマーケティング」となっている。この地域の収集家は広範多岐にわたるものであり、学生、企業家から政府官吏に及んでいる。

### 2 収集家の所属

前項で特に言及したように、中近東地域からの接触は様々な収集家によって行われている。DSS は、FY04-FY05 の報告事例と同様、全報告の 34%を占める「政府関連」所属の不審な実体が最多の収集家であると評価した。しかしながら、FY06-FY07 報告における顕著な変化は、もしかすると「商業」所属の不審な実体から発生したと評価された 5%増であり、FY04-FY05 において抜きんできていた「政府関連」と「商業」が事実上同点になったことかもしれない。

(分析者の意見：商業所属の不審な実体の増加は、合衆国 CDC の先端技術を突きとめようとした商業及び政府関連の不審な実体間の結託によるものと思われる。大学、公共機関、研究開発センターなどの商業所属の不審な実体が、これら政府関連収集家と連携し収集活動を行ったことはほぼ確実である。したがって、政府が様々な政府機関を介してすべての外部通信を監視し、公式に許可された通信伝送に限定するということもあり得る。(信頼度レベル：中))



図5:所属

### 3 手口

この地域における不審な収集実体は、「情報提供依頼」手口がロー・リスク・ハイ・リターンのもつことから、これを最も一般的な手口として好んで利用し続けている。また、収集家は、合衆国 CDC から所望の情報を得るため、「管理下技術入手の企て」を不当に利用し続けている。「情報提供依頼」は人気のある手口として使用し続けているが、その他の収集家は中立国を介して合衆国の管理技術を手入又は迂回させようと企てている。

(分析者の意見：中近東地域の不審な実体が、合衆国技術に対する標的行為のアプローチとして、非在来型の収集家及びあらゆる利用可能な手段に依存することはほぼ確実である。この直接的な標的行為は、標的機会数を増加させるとともに、合衆国のセンシティブ技術、秘密区分指定技術及び輸出管理下技術の入手成功確率を高めるものと思われる。(信頼度レベル：高) )

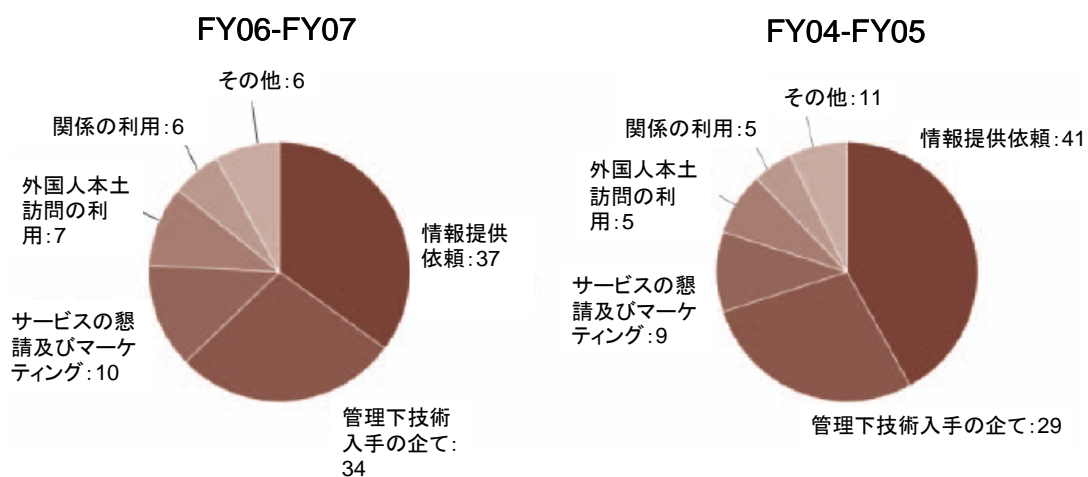


図6: 手口

### 4 標的にされた技術

中近東地域の不審な実体は、「情報システム」に対する標的行為を継続し続けている。「航空工学」及び「センサー」技術への関心の増加は、無人偵察機(Unmanned Aerial Vehicle: UAV)及び関連システムに対して特に関心を集中させたことによっても認められる。イラク戦争の UAV 分野に係わる報告件数は、FY04-FY05 以来 6 倍強となっており、中近東地域の不審な実体の関心の増加に伴ったものとなっている。UAV 技術が常に効率性と効果性の増加をもたらすものとして進化していることから、関連する兵器プラットフォーム・セットは無論のこと、これら新生技術の取得願望も増加することとなる。また、イラク及びアフガニスタンにおける戦争は、とりわけ戦闘能力に係わることから、「指揮・統制・通信・コンピュータ及び偵察 (C4ISR)」プログラムに関連した最先端技術の入手に対する注目を増加させている。

(分析者の意見：合衆国の防衛関連企業が航空工学分野における進歩を継続しているこ

とから、中東地域の不審な実体がこの分野について積極的な収集を企てることはほぼ確実である。収集家は、これらの航空システム、とりわけ UAV が研究開発における重要かつ継続的役割を担っていることから、UAV を標的にすることはほぼ確実である。さらに、テロリズムとの戦い(War on Terrorism)に係わる報道は、航空システム能力を強調するとともに、その関心を高めているように思われる。また、不審な実体も、プラットフォームの効率性、延長された飛行時間及び研究開発関連の C4ISR プログラムに注目している。(信頼度レベル：高))

表 4：標的にされた技術

開発科学及び技術リスト (DSTL)コード	FY06-FY07		FY04-FY05	
	事例数	%	事例数	%
航空工学	68	12	46	9
武器及びエネルギー素材	50	9	40	8
応用生物学	12	2	18	3
生物医学	6	1	4	1
化学	17	3	24	5
指向性運動エネルギー	4	1	5	1
エネルギー・システム	16	3	6	1
電子工学	30	5	52	10
地上システム	10	2	5	1
情報システム	121	22	116	22
レーザー及び光学	37	7	41	8
製造及び組み立て	28	5	14	3
海上システム	8	1	15	3
素材及び処理	27	5	20	4
核	5	1	3	<1
位置評定、航法及び処理時間	18	3	12	2
センサー	56	10	59	11
シグナチャー・システム	7	1	21	4
宇宙システム	15	3	11	2
兵器効果	1	<1	1	<1
不明	10	2	13	2

## 5 予測分析

中近東地域を発生源とする不審な実体は、既存技術の改善は無論のこと、自身の戦力倍加要素(force multiplier)の伸展を目的として、合衆国製品の収集を継続するようである。彼らが、センシティブな合衆国技術を手に入れる企てとして、Eメール利用の情報提供依頼を継続することはほぼ確実である。さらに、このような要求については、輸出規制を回避するため、他の国を介して収集の道を開き、という標的行為手法が継続すると思われる。

この地域の政治、経済状況などがより不安定となるにつれ、不審な実体が収集活動の関心を政府関連技術に向け続けることはほぼ確実である。そのような技術としては、とりわけ C4ISR 及び UAV に代表される情報システム及び航空工学である。(信頼度レベル：高)

## C. 欧州及びユーラシア

### 1 概観

欧州及びユーラシア地域は、FY06-FY07 間、施設保全適格証明書を持つ防衛関連企業 (Cleared Defense Contractor: CDC) からセンシティブ情報又は制限技術入手する企ての可能性があると判断された発生地域別の不審接触報告 (Suspicious Contact Report: SCR) 件数において、第 3 位となっている。FY06-FY07 の間に報告された 348 件のインシデントは、FY04-FY05 に DSS が当該地域からの収集の企てだとした 364 件からほんのわずかに減少している。CDC からの報告は、そのほとんどが「政府関連」及び「商業」所属の不審な実体による標的行為であることを示している。これらの不審な実体は、制限情報、秘密区分指定情報及び企業機密情報を手に入れる最も際立った収集手口として「情報提供依頼」を利用した。さらに、欧州及びユーラシア地域の不審な実体は、彼らの収集活動を「情報システム」技術、とりわけ情報通信サブ項目に焦点を当てた。

### 2 収集家の所属

FY06-FY07 における CDC からの報告によれば、「政府関連」及び「商業」所属の収集家が標的活動を行った大勢を占めている。これら 2 つの所属は、合計すると全欧州及びユーラシア地域における収集活動の 60% を占めている。

(分析者の意見: DSS は、他の地域全般における収集家の所属について、商業所属の増加に注目している。しかしながら、これとは異なり、欧州及びユーラシア地域を発生源とする政府関連所属の収集家の増加については、政府高官が軍事技術の開発を国家任務として公的に掲げていることに関連しているからだと思われる。(信頼度レベル: 中))



図7: 所属

### 3 手口

FY06-FY07 において、欧州及びユーラシアの収集家が利用したトップ・スリーの手口は、不審な実体を含む全インシデント報告のほぼ 80% を占めている。FY06-FY07 におけるトップ・スリーの手口は、「情報提供依頼」、「管理下技術入手の企て」及び「サービスの懇請及びマーケティング」であった。欧州及びユーラシア地域を発生源とする不審な実体は「情報提供依頼」を好みの手口として利用し続けた。けれども、FY06-FY07 の「情報

提供依頼」の占有率は、FY04-FY05 の 47%から 36%へと下落した。これとは逆に、「管理下技術入手の企て」は、大幅に増加して 30%に達した。一方で、「サービスの懇請及びマーケティング」は、12%からほんのわずかながら増加して 13%となった。

(分析者の意見：欧州及びユーラシア地域の収集家が、彼らの収集テクニックを変更することはほぼ確実にないと思われる。インターネットと Eメール・アカウント利用の劇的な増加は、国境をほとんど取り除き、「情報提供依頼」を実質的にリスク・フリーの選択肢としている。(信頼度レベル：高))

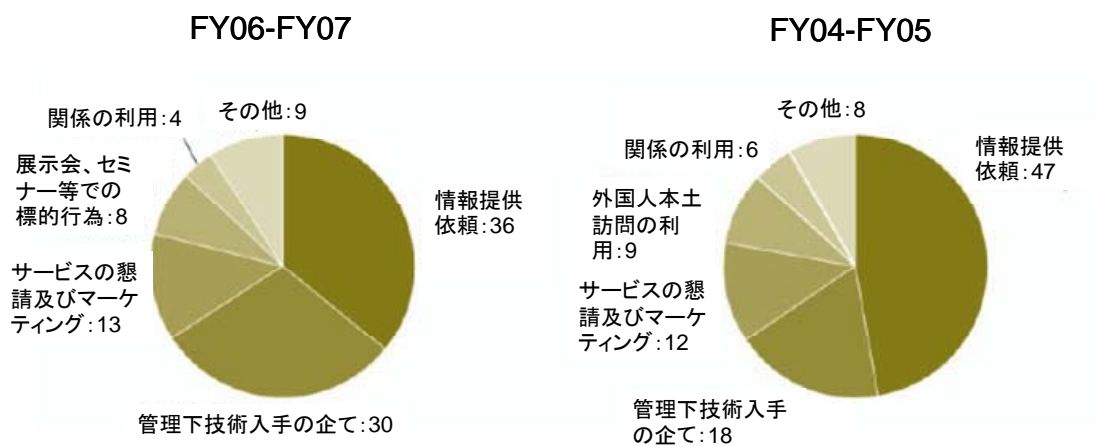


図8: 手口

#### 4 標的にされた技術

欧州及びユーラシアが標的にした技術のトップ・ファイブは、FY04-FY05 と比べ大幅な変化はない。「電子技術」を除き、ほとんどの技術分野は同じままである。「電子技術」は 5 位から 6 位へと下った。「情報システム」技術は、同技術の情報通信サブ項目に焦点を当てた収集活動であり、最も需要がある技術として 1 位に留まった。興味深いのは「航空工学」技術が穏やかな上昇に転じたことであるが、これは欧州及びユーラシア地域の不審な実体が積極的に航空機/搭載工業技術を求めた結果であると思われる。

表 5 : 標的にされた技術

開発科学及び技術リスト (DSTL) コード	FY06-FY07		FY04-FY05	
	事例数	%	事例数	%
航空工学	78	18	51	11
武器及びエネルギー素材	37	8	55	12
応用生物学	11	3	13	3
生物医学	2	<1	4	1
化学	10	2	14	3

指向性運動エネルギー	3	1	1	<1
エネルギー・システム	3	1	4	1
電子工学	21	5	45	9
地上システム	6	1	2	<1
情報システム	98	22	80	17
レーザー及び光学	46	10	32	7
製造及び組み立て	4	1	6	1
海上システム	16	4	15	3
素材及び処理	9	2	15	3
核	3	1	3	1
位置評定、航法及び処理時間	19	4	15	3
センサー	51	12	53	11
シグナチャー・システム	2	<1	22	5
宇宙システム	13	3	16	3
兵器効果	1	<1	1	<1
不明	6	1	28	6

## 5 予測分析

欧州及びユーラシア地域を発生源とする不審な実体は、彼らの研究開発を強化するため、先進技術の入手に焦点を当て続けるものと思われる。国内の防衛関連企業の活力を取り戻すとする願いは、政府関連及び商業所属の不審な実体を促し、所望の西側の技術を手に入る目的で合衆国の会社とのビジネス・ベンチャー探しを求めるものと思われる。さらに、欧州及びユーラシア地域の収集家は、先進兵器システムの開発や指揮・統制・通信・コンピュータ・インテリジェンス・搜索及び偵察(C4ISR)アプリケーションの更なる向上に資するものとして、潜在的可能性をもつデュアル・ユーズ技術を求め続けるであろう。(信頼度レベル：中)

## D. 南及び中央アジア

### 1 概観

南及び中央アジアは、最も技術収集活動が盛んな地域の第4番目を依然として維持している。「商業」所属の収集家は、他の地域における傾向と同様に、企業からの報告の第1位を占めている。収集家は「情報システム」技術を最も頻繁に求め、「レーザー及び光学」、「センサー・システム」及び「航空工学」技術がこれに次いでいる。企業からの主要な手口に係わる報告は、他の地域における順番に同じであり、第1位が「管理下技術入手の企て」で、「情報提供依頼」及び「サービスの懇請及びマーケティング」がこれに次いでいる。

### 2 収集家の所属

DSS が不審な接触判定基準を満足したとして確認した 348 件の報告に基づく最も劇的な傾向は、「商業」所属の不審な実体を発生源とした接触数の大幅な増加である。これら不審な実体の数は全報告の 52% を占めており、FY04-FY05 の 39% から大きく変わっている。また、「商業」又は「政府」所属の不審な実体に属さない「個人」による接触も、FY04-FY05

における報告数のほぼ倍となって 25% に上昇し、FY06-FY07 における全接触の四分の一を占めている。「政府」及び「政府関連」所属の不審な実体は、同じ時期にそれぞれ 10% 及び 11% に下落した。「政府関連」所属の不審な実体による収集活動は、前の時期の三分の一以下となり、FY04-FY05 から大幅な下落となった。

分析者の意見：商業所属の不審な実体による接触の増加及び対応する政府及び政府関連所属の

不審な実体による接触の下落は、DSS が FY06-FY07 に確認した傾向を忠実に描写したものとなっている。この傾向は、グローバルな市場経済の第三世界へのシフト及び国際的なインターネット・アクセスの増加に起因するものと思われる。このアクセスは、小規模な商業所属の不審な実体が大規模な国際的技術入手分野に参入し、最終的に特定の近代化活動に加わることを可能にしている。(信頼度レベル：中)



図9: 所属

### 3 手口

DSS の分析は、最も積極的に活動した収集家としての「商業」所属の不審な実体の増加傾向、及びこれに伴って最も広く利用された収集手口選択肢としての「管理下技術入手

の企て」テクニックの出現、という両者間の一致について注意深く観察した。「政府」所属の収集家は、情報入手手段として「情報提供依頼」を最も利用しているが、「商業」所属の収集家は、さらなるビジネス利益を得ると称して、実際に当該技術そのものの入手を好んで企てる傾向にあった。このような結果として、FY06-FY07における「管理下技術入手の企て」の増加は「情報提供依頼」の手口を上回り、FY04-FY05における手口の順位と完全に逆転した。最も利用された収集手口の第3位「サービスの懇請及びマーケティング」も若干増加したが、「管理下技術入手の企て」の手口に比べると見劣りがする。

(分析者の意見：FY06-FY07間の企業報告における手口の変化は、研究開発目的で技術を求める政府所属の不審な実体と販売目的で技術を求める商業所属の不審な実体間の違いを示している。商業所属の不審な実体が当該地域における技術契約を果たし続ける限り、管理下技術の入手要求はより積極的に拡大するものと思われる。(信頼度レベル：中))

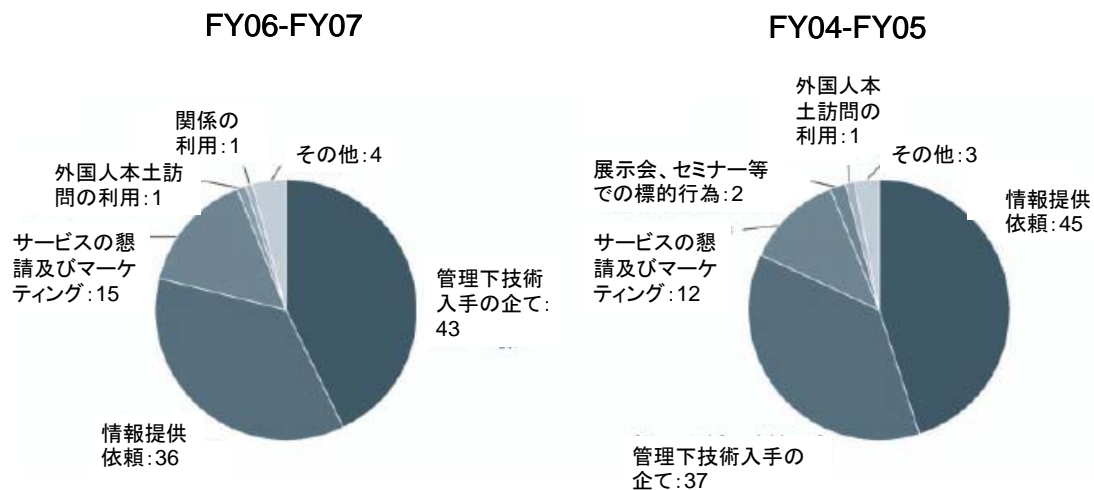


図10:手口

#### 4 標的にされた技術

過去4年間にわたり南及び中央アジア地域を発生源とする不審な標的行為は、最多の標的対象となった技術トップ・フォーに若干の増加が見られるものの、比較的動きがないまま推移してきた。この地域の不審な実体は「情報システム」技術、明確には「指揮・統制・通信・コンピュータ・インテリジェンス検索及び偵察 (C4ISR)」システムを第1位の標的技術として求め続けており、全報告の約四分の一を占めている。第2位は「レーザー及び光学」、具体的にはレーザー標的指示器及びレーザー距離測定器となっている。しかしながら、「レーザー及び光学」は「情報システム」を7%下回っている。第3位は「センサー」技術であり、改良爆発装置(Improvised Explosive Device: IED)、動体センサー及び侵入検知センサーに関心の的としている。第4位は「航空工学」のままであり、無人偵察機(UAV)及びその関連システムに関心を集中している。これらトップ・フォーの増加は、「化学」、「素材及び処理」及び「シグナチャー・システム」技術の実質的削減の結果である。

(分析者の意見：南及び中央アジア地域からの不審な実体は、当該地域に発生する暴動に対抗するため、経済及び軍事の近代化を追求し続けている。このような近代化要求に伴う標的行為は、当該国の軍事及び法の執行組織のために、不審な実体を最高の技術(C4ISR、標的指示及び検知システム)の入手に駆り立てると思われる。(信頼度レベル：中))

表 6：標的にされた技術

開発科学及び技術リスト (DSTL)コード	FY06-FY07		FY04-FY05	
	事例数	%	事例数	%
航空工学	49	12	40	10
武器及びエネルギー素材	28	7	32	8
応用生物学	5	1	6	2
生物医学	4	1	5	1
化学	3	1	14	4
指向性運動エネルギー	1	<1	4	1
エネルギー・システム	2	<1	5	1
電子工学	34	8	34	9
地上システム	10	2	6	2
情報システム	84	21	67	17
レーザー及び光学	59	14	48	12
製造及び組み立て	7	2	3	<1
海上システム	9	2	3	<1
素材及び処理	14	3	22	6
核	3	1	1	<1
位置評定、航法及び処理時間	4	1	7	2
センサー	55	14	41	10
シグナチャー・システム	5	1	31	8
宇宙システム	30	7	23	6
兵器効果			1	<1
不明	1	<1	4	1

## 5 予測分析

防衛関連企業との接触開始に際して、商業所属の不審な実体を最多の収集家として利用することは、次年度にもほぼ確実に継続されると思われる。収集手口選択肢として管理下技術入手の企てを利用することは、NATO パートナーとの共同及び接触の拡大につれ、同地域の商業及び軍事所属の不審な実体が新たな技術にさらされることから、継続されるであろう。情報システム、とりわけ C4ISR システムは、技術収集の主たる関心の的に留まるものと思われる。また、レーザーと光学技術の入手の企ても、C4ISR システムの入手の企てと相俟って拡大するものと思われる。航空工学を対象にした収集は、UAV システムが関心の的となっていることから、センサー技術の収集を上回ると思われる。その理由は、

UAVが高有用性かつ複数任務達成能力を備えていることから、NATO及び多国籍軍がUAVをC4ISRシステムに不可欠なコンポーネントであると支持しているからである。(信頼度レベル：中)



## 事例研究

外国会社の代表と目される人物が、施設保全適格証明書を持つ防衛関連企業(Cleared Defense Contractor: CDC)の軍事技術に係る職場で働いている従業員に対して、Eメールで接触してきた。しかしながら、DSSは、接触を働きかけた人物の会社名がEメールのアドレスと一致しなかったことに気付いた。Eメールの発信者は、彼の会社でCDCが開発した軍事技術が緊急に必要なになったと主張し、CDCとのビジネス関係を築くことを申し出たのであった。DSSにおける引き続き分析から、発信者が利用したメール・アドレスは、エンドユーザー証明書詐欺行為の前歴を持つ別の外国の会社のものであることが明らかとなった。

外国の調査センターの代表が合衆国のCDCに接触し、明らかに輸出管理素材の取得を正当化しようと企て、製品設計図を示した。その調査センターの設計図をレビューしたところ、それは重要軍事技術プログラムに係るものであることが明らかとなった。同調査センターは最初、同設計図の製品は何ら軍事に応用するものではないと否定していたが、ついに撤回し、製品設計図は実際のところ軍事目的に利用できることを認めたのである。外国の調査センターの代表は、このようなごまかしが明らかにされたにもかかわらず、最終製品を軍事目的に利用する意図はないと主張し続けたのである。

あるCDCが、人をだますような複数のEメールを受け取った、とDSSに報告してきた。そのEメールには添付資料があり、(それを開くと)悪意のあるソフトウェアが会社の内部コンピュータ・システムに自動的にインストールされてしまうものであった。このCDC内の非常に多くの従業員が、この策略の犠牲者となった。合衆国CDCの分析者が、この悪意のあるソフトウェアがインストールされたパソコンの一つを抽出し分析したところ、さらなる悪意のあるコードが「.gif」及び「.jpg」イメージファイル・ソフトウェアに組み込まれていることを発見した。

外国の会社がここ数か月間にわたり、合衆国CDCのある従業員に繰り返し接触し、同社で使用するコンポーネントの調達支援を求めてきた。もともと、接触は最初、非輸出管理規制コンポーネントを対象に、当たり障りがないと思える要求から始まったのであるが、その外国の会社は、後になって要求のリストを修正し、デュアル・ユーズの輸出管理品目を含めたのである。そしてついに、その外国の会社はCDC従業員との接触情報を同じ外国会社内の複数の部署と共有し、結果として、同従業員に対するさらなる要求の洪水となったのである。一か月以内に、この同じ外国の会社が標的行為を第二のCDCにシフトし、同社の国の軍事研究開発活動に係る技術を要求し始めたのである。

明らかに外国人学生を装った人物が、CDCにおいて航空力学研究を担当している従業員に接触し、同CDCにおけるUAV開発にどの程度の秘密区分指定情報が適用されているかを尋ねた。その「学生」は、外国の一流大学においておそらく航空力学専攻しているらしく、CDC航空力学研究部署におけるインターンとしての勤務の可能性を尋ねた。その「学生」は、実際に同学生の国が捜し求めている秘密区分指定及び輸出制限技術に係る情報及び研究の重要性を教えてくれるよう頼んだのである。

ある合衆国 CDC のエンジニアリング・チームが、外国のカウンターパート・チームとの意見交換会に参加した。その間、両チーム間で非秘密区分指定技術情報を共有することが許可されていた。合衆国の会社の代表はこの交換会プログラムの後で、外国のエンジニア・チームが交換会の場に置いたままの大量の印刷資料の中に、いくつかの輸出制限文書を発見した。合衆国の会社の代表は、外国のチームが放置した印刷物をさらに調べ、外国のチームが軍事プログラムに係る大量のオープン・ソース情報を取得していることを発見した。これらのプログラムは、合衆国 CDC との非秘密区分指定契約には明らかにあり得ないものであった。

## 見 解

### A. 結論

不審な依頼を地域別に分けると、ここ 2 年間の地域別順位傾向が同じであることを示している。しかしながら、その割合には変化がある。DSS は、最大の不審接触数となった地域が東アジア及び太平洋であり、FY04-FY05 の 30%に比べると 36%に増加していることを確認した。DSS は、これら東アジア及び太平洋地域による頻繁な収集活動に係る報告が、第 2 の最大の合衆国技術外国収集家である中近東地域を発生源とする報告に比べ、約 2 倍となっていることに気づいた。これらに次ぐのは、欧州及びユーラシアと南及び中央アジア地域の不審な実体であり、以上の 4 地域で最も頻繁に遭遇した収集家の階層を完成している。これらトップ・フォーの収集家が標的とした合衆国技術、とりわけ「情報システム」は 23%に及ぶ収集活動の関心の的となっている。

今回の収集期間において、不審な収集家の実体が政府所属から商業所属に係るものへとシフトしていることが認められた。最も頻繁に収集活動を行う不審な実体は、「商業」所属の収集家を利用して合衆国の技術を取得しようとしており、この分野の収集家の所属は全不審接触報告(SCR)の 40%を占めている。報告は、東アジア及び太平洋と中近東地域からの政府が管理下技術を手に入れようとして、正当な商業所属の実体及び不正なフロントカンパニーの両者を利用したことを示している。一方、南及び中央アジア地域の収集家は、学生などの非在来型収集家を利用して合衆国の制限技術にアクセスしようとしている傾向にある。また、トップの収集家が合衆国技術を標的にする際には、「政府関連」所属の不審な実体にも大きく依存しており、この分野の SCR は全収集活動の 24%を占めている。

FY06-FY07 におけるトップの収集家は、合衆国技術を取得する主要な手口 (MO) として「情報提供依頼」及び「管理下技術入手の企て」を利用した。これらに加え「サービスの懇請及びマーケティング」の手口を利用している不審な実体は、全収集企ての 70%強を占めている。また、このことは、「情報提供依頼」及び「管理下技術入手の企て」を当該地域におけるトップ・ツーの手口としている不審な実体とも一致している。さらに、トップの収集家は、合衆国技術を収集する手口として「不審なインターネット活動」を利用している。この手口の利用は 4%から 10%へと著しく増加しており、最も頻繁に利用された収集テクニックの第 4 位を占めている。

FY06-FY07 における最多の収集家に係る報告には、サイバー関連の報告が含まれている。東アジア及び太平洋地域が発生源となっている IP アドレスをもつ不審な実体は、全サイバー収集活動の 52%を占めている。このようなインシデントの発生地域の第 2 位は欧州及びユーラシアであるが、その占有率は 21%であり、大きく引き離されている。DSS 及びインテリジェンス・コミュニティの報告は、東アジア及び太平洋地域の収集家が「情報

システム」技術収集活動の一環として、研究開発及び「指揮・統制・通信・コンピュータ・インテリジェンス・搜索及び偵察（C4ISR）」に係る情報を入手するため、施設保全適格証明書を持つ防衛関連企業(CDC)のネットワークを標的にしていることを指摘している。同様に、最多のサイバー収集家は、最も人気があるサイバー技術として「情報システム」を標的にしており、この分野に適用する情報の取得に焦点を当てた不審接触活動の43%を占めている。収集家はこの技術を手口として「侵入の企て」を最も利用している。同手口は、情報システム技術を標的としたサイバー収集活動の61%を占めている。サイバー収集家は、IPアドレスの特性及び匿名性のプロキシを利用することで、彼らのアイデンティティを隠蔽している。このことが、収集家の真の所属を決定的に確認づけることを困難にしている。FY06-FY07において、DSSの分析がその発生地域の不審な実体を特定することができたのは、全サイバー関連SCRの4%だけであった。真のサイバー所属を明らかにするのが困難であるにもかかわらず、グローバル市場の拡大及び技術の進展に伴い、ネットワーク攻撃や侵入の企てが増加しつつある。

## B. 予測

CDCの従業員が脅威に対して、より敏感になるにつれ、CDCからのサイバー・インシデントを含むSCRの数が比例して増加することはほぼ確実である。同様に、防衛関連企業が新興の第三世界市場と取引するにつれ、非在来型収集家の利用もほぼ確実となり、それに伴って不審接触の数が増加することになる。

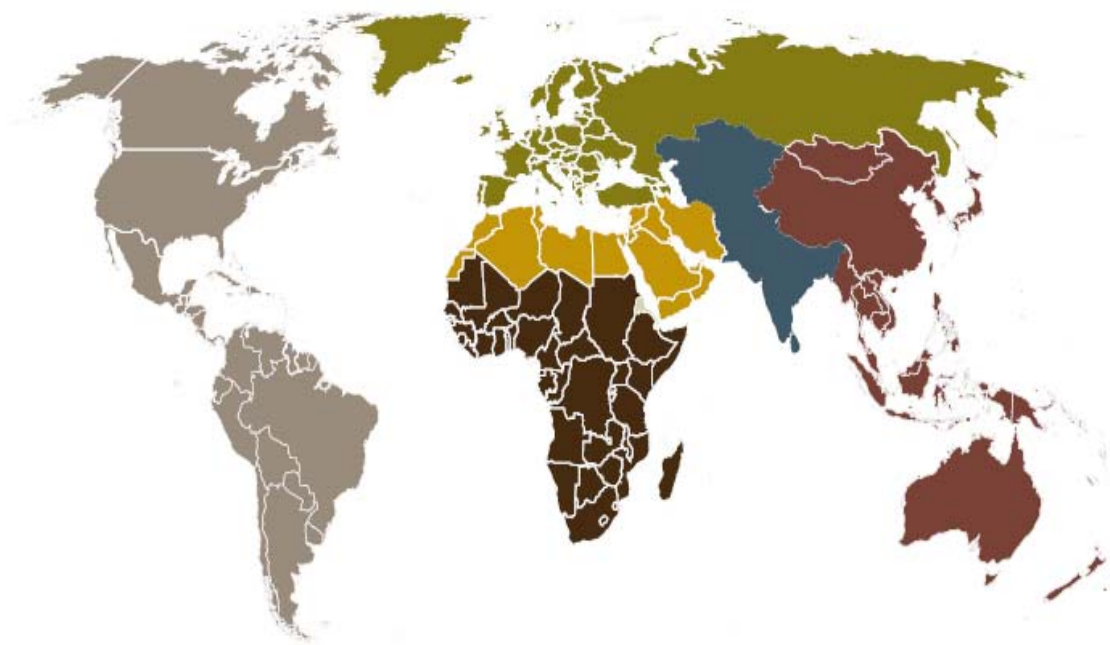
情報システム技術、とりわけC4ISRシステムに最多の収集家が優先的に標的とする技術に留まることはほぼ確実である。これには、モデリング・アンド・シミュレーション技術の収集増も含まれる。兵器技術開発、とりわけミサイル及びミサイル防衛技術は、中近東と欧州及びユーラシア地域の不審な実体にとって、優先的収集対象として継続するものと思われる。一方で、レーザー及び光学技術、素材及び処理技術並びに造船技術は、東アジア及び太平洋地域における優先的収集対象として継続するものと思われる。航空工学技術、とりわけ先進UAVシステムは、すべての地域収集家の主要な関心の的として継続するものと思われる。

不審な実体がCDCへの標的行為にインターネット利用の手口を増加させるであろうことは、ほぼ確実である。その理由は、他の手口に比べローリスク・ハイリターンであることから、不正な収集家が合衆国のコンピュータ・ネットワークに保管されているセンシティブ情報及び企業機密情報を取得する際に、格好の機会を提供するからである。また、インターネット利用の標的行為は、潜在的収集家の目には即座に明らかとならない標的機会を明示するツールとしても利用することができる。これにより敵対性構成分子は、その収集活動の的を絞り、あらゆる収集テクニックを用いた標的行為計画を立案することができる。

外国の商業所属の不審な実体が、センシティブな合衆国技術にアクセスしようとして共同商業活動を着実に推し進めるだけでなく、CDCによる開発技術の調達を企てを増加させることは、ほぼ確実であると思われる。これらの活動は、正当なグローバル・ビジネス慣行と合衆国技術の不正取得の企て間の区別を行う合衆国の治安及びカウンターインテリジェンス・コミュニティ能力を困難にすると思われる。さらに、ほぼすべての収集家が、自国の商業及び軍事アプリケーション技術基盤の両者を引き上げるため、いずれか又はすべてのデュアル・ユーズ技術の取得を、それらの重要性にかかわらず継続するであろう。この多次元に及ぶ脅威環境が、合衆国の国防保全要員及び CDC 側に、革新的かつ先見性のある警戒を求めることはほぼ確実であると思われる。(信頼度レベル：高)



## 参照地図





アフリカ	東アジア及び 太平洋	欧州及び ユーラシア	中近東	南及び中央 アジア	西半球
アンゴラ	オーストラリア	アルバニア	アルジェリア	アフガニスタン	
ベニン	ブルネイ	アンドラ	バーレーン	バングラデシュ	アルゼンチン
ボツワナ	ビルマ	アルメニア	エジプト	ブータン	アルバ
ブルキナファソ	カンボジア	オーストリア	イラン	インド	バハマ
ブルンジ	中国	アゼルバイジャン	イスラエル	カザフスタン	バルバドス
カメルーン	フィジー	ベラルूस	ヨルダン	キルギス共和国	ベリーズ
ケープベルデ	インドネシア	ベルギー	クウェート	モルジブ	バーミューダ
中央アフリカ共和国	日本	ボスニアヘルツェゴビナ	レバノン	ネパール	ボリビア
チャド	キリバス	ブルガリア	リビア	パキスタン	ブラジル
コモロ	南朝鮮	クロアチア	モロッコ	タジキスタン	カナダ
コンゴ共和国	北朝鮮	キプロス	オマーン	トルクメニスタン	ケイマン諸島
コンゴ民主共和国	ラオス	チェコ共和国	パレスティナ	ウズベキスタン	チリ
コートジボワール	マレーシア	デンマーク	カタール		コロンビア
ジブチ	マーシャル群島	エストニア	サウジアラビア		コスタリカ
赤道ギニア	ミクロネシア	ヨーロッパ連合	シリア		キューバ
エリトリア	モンゴル	フィンランド	チュニジア		ドミニカ
エチオピア	ナウル	フランス	アラブ首長国連邦		ドミニカ共和国
ガボン	ニューゼーランド	グルジア	イエメン		エクアドル
ガンビア	パラオ	ドイツ			エルサルバドル
ガーナ	パプアニューギニア	ギリシャ			グラナダ
ギニア	フィリピン	グリーンランド			ガテマラ
ギニアビサウ	サモア	ローマ教皇			ギニア
ケニア	シンガポール	ハンガリー			ハイチ
レソト	ソロモン諸島	アイスランド			ホンジュラス
リベリア	台湾	イタリア			ジャマイカ
マダガスカル	タイ	コソボ			メキシコ
マラウイ	チモール	ラトビア			オランダ諸島
マリ	トンガ	リトアニア			ニカラグア
モーリタニア	ツバル	ルクセンブルグ			パナマ
モーリシャス	バヌアツ	マケドニア			パラグアイ
モザンビーク	ベトナム	マルタ			ペルー
ナンビア		モルドバ			聖キッツ・ネビス
ニジェール		モナコ			聖ルシア
ルワンダ		モンテネグロ			聖ビンセント・グレナディス
サトマリシハ		オランダ			スリナム
セネガル		ノルウェー			トリニダード・トバゴ
セイシェル		ポーランド			合衆国
シエラレオーネ		ポルトガル			ウルグアイ
ソマリア		ルーマニア			ベネズエラ
南アフリカ		ロシア			
スーダン		サンマリノ			
スワジランド		セルビア			
タンザニア		スロバキア			
トーゴ		スロベニア			
ウガンダ		スペイン			
ザンビア		スウェーデン			
ジンバブエ		スイス			
		トルコ			
		ウクライナ			
		イギリス			



## フィードバック様式

(U)本出版物に関する意見又は質問事項のあて先は次のとおりである。

VA22314 アレキサンドリア ブラドックプレース 1340

国防保全局 カウンターインテリジェンス(CI)部長気付け

ウェブサイト : <http://www.dss.mil>

施設保全適格証明書を持つ防衛関連企業名称 : \_\_\_\_\_

CAGE コード<sup>4</sup> : \_\_\_\_\_

連絡先 : \_\_\_\_\_

住所 : \_\_\_\_\_

Eメール/電話 : \_\_\_\_\_

問題点 : \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

論考 : \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

推奨 : \_\_\_\_\_

\_\_\_\_\_  
\_\_\_\_\_

---

<sup>4</sup> CAGE: Commercial And Government Entity。国防総省が民間企業を識別する目的でコード化(5桁)したもの。



## 平成20年・21年度発刊・発刊予定資料

- BSK 第20-1号『対情報訓練資料(企業秘密を盗み出す手口とその対策)』  
BSK 第20-2号『人的セキュリティ：脅威、挑戦、および対策』  
— 英国における人的セキュリティの取り組み —  
BSK 第20-3号『我が国をめぐる兵器技術情報管理の諸問題(平成19年度)』  
BSK 第20-4号『技術情報セキュリティの現状と動向(平成19年度)』  
BSK 第20-5号『米国における情報セキュリティ関連のユーザー教育、資格付与及び管理について(平成19年度)』  
BSK 第20-6号『インサイダー犯罪防止のための監視・監査体制の在り方(平成19年度)』  
BSK 第20-7号『新しい防衛調達モデルの探索的調査研究(総論)』  
BSK 第20-8号『国の安全保障に係わる装備品等を生産している企業に対する外国資本による買収に関する各国の法規制の状況』  
BSK 第20-9号『管理者用情報セキュリティ・ハンドブック』(保全講習受講用)  
BSK 第20-10号『効果的な意識向上促進の取組み方』『携帯電話、携帯用パソコン、携帯情報端末(PDA)、その他電子装置を携帯する海外旅行』  
BSK 第20-11号『雇用中の人的セキュリティ：優れた実践事例ガイド』
- BSK 第21-1号『我が国をめぐる兵器技術情報管理の諸問題(平成20年度)』  
BSK 第21-2号『米国における情報システムの不測事態対応計画について(平成20年度)』  
BSK 第21-3号『外国の経済情報収集および産業スパイ活動に関する議会への年次報告(2007年度)』  
BSK 第21-4号『新しい防衛調達モデルの探索的調査研究(その2)』  
BSK 第21-5号『中央政府における究極の省庁別財務責任者である会計官、主席財務官等の役割に関する国際比較研究』  
BSK 第21-6号『多層防衛：セキュアで弾力性のあるIT組織の礎』(保全講習受講用)  
BSK 第21-7号『インサイダー脅威の防止・探知のための共通ガイド第3版』『米国の国家対情報戦略(2008年)』  
BSK 第22-1号『標的にされる合衆国技術』  
BSK 第22-2号～ 平成21年度調査研究

### 標的にされる合衆国技術

(TARGETING U.S. TECHNOLOGIES)

— 防衛関連企業報告に基づく傾向分析 2008 —

(A TREND ANALYSIS OF REPORTING FROM DEFENSE INDUSTRY)

平成22年1月 発行  
非売品 禁無断転載・複製  
発行：財団法人 防衛調達基盤整備協会  
編集：防衛調達研究センター刊行物等編集委員会  
〒160-0003 東京都新宿区本塩町21番3-2  
電話：03-3358-8754  
FAX：03-3358-8735  
メール：hozen@bsk-z.or.jp  
BSKホームページ：<http://www.bsk-z.or.jp>

