ＢＳＫ第２０－１号

対　情　報　訓　練　資　料

(Counterintelligence)

(企業秘密を盗み出す手口とその対策)

平成２０年２月

財団法人 防衛調達基盤整備協会

はしがき

本出版物「対情報訓練資料(企業機密を盗み出す手口とその対策)」は、米国防総省の国防保全局対情報室(Defense Security Service Counterintelligence Office)が、米国の防衛関連企業を対象にまとめた対情報訓練資料を翻訳したものである。国防保全局対情報室は、米国の企業や従業員を情報収集の標的とした外国の情報機関などによる活動を分析し、企業が取扱っている連邦政府の秘密情報や企業機密情報などを保護するため、企業に対する対情報活動支援を行っている。

本出版物は、次の３点についてまとめたものである。

(1) 外国の情報機関やその手先が、どのような情報収集の手口で連邦政府の秘密情報、企業の機密情報やセンシティブ情報にアクセスしているか

(2) そのような情報収集の疑念を抱かせる指標にはどのようなものがあるか

(3) 情報を保護するための基本的なセキュリティ対策事項にはどのようなものがあるのか

わが国においても外国からの情報収集活動による事件報道がしばしば行われているが、これは氷山の一角なのかもしれない、いやすべてかもしれない。しかしながら、わが国の先進技術を狙ったこの種情報収集活動が今後ますます増えるのは明らかであろうと思われる。そのような犠牲にならないためにも、わが国の企業及びその従業員が脅威意識をもって情報の保護を確実にする必要があるのではなかろうか。

本出版物が、わ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２０年２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

要　　約

本小冊子は、対情報活動に係わる次の訓練資料をまとめたものである。

- ✧　元従業員の引き込み：彼らは誰のために働くのか？
- ✧　対情報活動とセキュリティ対策事項
- ✧　外国人の訪問：何が不適切か？
- ✧　隠れ蓑会社：エンドユーザーは誰か？
- ✧　インターネット：勝手な情報収集に急速な拡大をもたらしている手口
- ✧　保全施設適格証明書を有する防衛関連企業から科学技術情報を収集するための学術的接近
- ✧　米国防衛関連企業に向けられた外国からの情報収集活動に係わる不審な指標及びセキュリティ対策事項
- ✧　情報の引き出しに利用される入札
- ✧　何を我々は保護しているのか？

元従業員の引き込み：彼らは誰のために働くのか？

この小論文は、外国の組織が米国の保全施設適格証明書を有する企業の元従業員を、情報収集作戦にとってなぜ卓越した有望な候補者と見るのかについて解説するものである。

対情報活動とセキュリティ対策事項

この小論文は、対情報活動に係わる基本的なセキュリティ対策事項について解説するものである。

外国人の訪問：何が不適切か？

この小論文は、外国人科学者や技術者の保全施設適格証明書を有する防衛関連企業への訪問が、情報収集活動のための様々な手口を利用した不適切行為に結びつく可能性を説明するものである。

隠れ蓑の会社：エンドユーザーは誰か？

この小論文は、会社を隠れ蓑として輸出制限及び通商禁止の回避に利用可能なことから、それらが米国政府及び防衛関連企業に対して重大な問題をもたらす可能性について考察するものである。

インターネット：勝手な情報収集に急速な拡大をもたらしている手口

この小論文は、外国の組織と保全施設適格証明書を有する米国の企業及びその従業員と

の間のコンピュータ引き出しを用いた勝手な通信手法として、インターネットがなぜ急速な成長を遂げているのかを説明する。

保全施設適格証明書を有する防衛関連企業から科学技術情報を収集するための学術的接近

この小論文は、1996 年及び 1997 年に起こったセンシティブ情報及び秘密情報の収集に学術的接近の手口を利用したインシデントについて、その具体的な事例及び関連する指標を示すものである。

米国防衛関連企業に向けられた外国からの情報収集活動に係わる不審な指標及びセキュリティ対策事項

1997 年に出版されたこの小冊子の目的は、セキュリティ専門家、対情報活動要員及び保全施設適格証明書を有する企業が不審な接触を認識し脅威に適切に対応するため、費用対効果があり、かつ、合理的なセキュリティ対策事項を導入するにあたっての助けとなる情報を提供するものである。

情報の引き出しに利用される入札

この小論文は、外国政府が契約意図を決して持つことなく米国の企業に対し詳細な入札を行わせ、技術情報、ある場合は企業機密に係わる情報を獲得することに関心を持っていると思われる可能性の存在について説明する。

我々は何を保護しているのか？

この小論文は、米国の企業が護ろうと努めるべき資産の概括的な種類を明らかにするとともに、資産が持つ脆弱性とセキュリティ対策事項の設置を企業が検討する際の助けとする情報を提供するものである。

1　元従業員の引き込み：彼らは誰のために働くのか？

1.1　序　論

国防保全局(Defense Security Service: DSS)は、情報収集の手口(Modus Operandi: MO)として注目すべき幾つかの報告を受けている。その報告の内容によれば、保全施設適格証明書を有する会社の元従業員が、外国の企業や研究所に働きに出かけており、その企業や研究所は保全施設適格証明書を有する米国の企業において彼らが以前に従事していたプロジェクトや技術と同様の事項に関心を持っているとされているのである。元従業員は情報収集目的で外国に雇われたのかもしれないし、そしてさらなる情報入手目的で米国との接触を期待されているのかもしれない。これらの報告は、外国の組織がこの情報収集の手口(MO)を利用して、秘密、センシティブ[1]又は企業機密に係わる情報を収集しようとしていることを明確に示している。外国の組織は、米国の元従業員を収集活動に、特に見込みがある者としてみているのである。なぜなら、これら米国の元従業員がいったん米国での雇用を終了すれば、彼らは米国政府や企業のセキュリティ要求事項に従う義務を感ずることがほとんどないと外国の組織は考えているからである。

1.2　テクニック

情報収集の手口(MO)の一つに、保全施設適格証明書を有する米国の企業の元従業員による訪問を利用する方法があるが、これは輸出制限に係わる情報やおそらくは秘密の技術情報を元の同僚から気付かれることなく収集するには都合の良い手法と考えられているからである。防衛装備品及びサービス(これには、秘密及び非秘密の両技術データが含まれる)の輸出は、武器輸出規制(ITAR)の管理下にある。外国の企業や研究所で働く米国市民は、気付いているか又は気付かずに「非秘密」の技術的な話をすることが適切又は許可されているのだから心配することはないと、元同僚に対して誤った説得をすることができる利点を持っている。

1.3　事例研究

ほとんどの国、特に米国と政治的かつ軍事的な同盟関係にある国は、国防総省重要軍事技術リスト(Department of Defense Militarily Critical Technology List: MCTL)に記載されている 18 の異なる技術区分の多くについて、同様の研究開発中のプログラムをもって

---

[1] センシティブ：sensitive の訳語である。本訓練資料では、企業等において取扱いに慎重を要する情報を「センシティブ情報」としている。
米国では、政府が秘密の情報として取り扱うのは国家の安全保障に係わる情報であり、これを「秘密情報(classified information)」とし、top secret(機密), secret(極秘)及び confidential(秘)に細区分して使用している。秘密の情報ではないが取扱いに慎重を要する政府の情報について、国防総省などでは「秘密でないセンシティブ情報(sensitive but unclassified: SBU)」としている。
一方、企業における情報については、企業機密に係わる情報を「企業機密情報(proprietary information)」とし、取り扱いに慎重を要する情報を「センシティブ情報(sensitive information)」としている。

いる。このようなことから幾つかの国々は、前述のとおり、この装置や技術を取得することに関心を抱いている。次に述べる 2 つの実例は、この種の情報収集の手口(MO)を利用した典型的な例である。

(1) 以前に秘密保護適格証明書を保持していた、ある米国市民は、センサーに係わる軍事重要技術を専門的に取り扱うエンジニアであったが、保全施設適格証明書を有する米国の企業を退職して外国に移住し、外国政府の研究補助金を取得するため外国の大学で同じ技術に係わる研究を開始した。彼は、この外国の大学に雇用されている間に重要軍事技術に係わる特定の情報を取得しようとして、米国にある保全施設適格証明書を有する元の会社及び同僚を訪問するため帰国する手はずをつけた。その情報は、輸出管理の対象として明確に国際武器取引規制(ITAR)下にあるものであった。幸いにも、この元同僚で米国市民による要請を「輸出管理情報に対する外国からの要求」であると米国の会社の従業員が認識し、いかなる情報についても話し合うことや開示することを拒否したのである。

(2) 他のインシデントの例では、保全施設適格証明書を有する企業で約 3 年もの間、主要な米国防衛プログラムに従事していた秘密保護適格証明書を有する米国市民が、外国にある会社に働きに行ったというのがある。この元従業員は、毎年帰国するつど、保全施設適格証明書を有する元の会社と同僚を訪問することを数回繰り返していたのであった。また、彼女は、帰国のつど、米国を離れるに前に元同僚達とディナーを共にすることが常であった。もっとも、これら類の関係は完全に悪意のないものではあったが、元従業員が居住し働いている国は、米国との間に企業機密協定を締結してなく、かつ、データ交換協定(Data Exchange Agreement: DEA)において制限されており、技術及び装置の技術転用及び悪用の経歴があったのである。このような状況から、その会社はセキュリティ上のリスクを感じ、関連するセキュリティ対策事項について見直しを行ったのである。

1.4 教 訓

会社のセキュリティ責任者は、元従業員が外国の組織に引き込まれる可能性があることを、従業員に確実に教育し認識させるべきである。このような情報収集の手口の指標として含まれるものには、外国での居住、外国の企業での勤務、同じ技術の研究、及び元の雇用会社への頻繁な訪問がある。このような指標に係わる状況に遭遇した者は、このインシデントについて会社を支援する立場にある国防保全局(DSS)企業保全代表部及び連邦捜査局(FBI)支部に報告すべきである。ここでの教訓は、秘密保護適格証明書を有するか又は秘密保護適格証明書を以前に有していた米国市民だからといって、秘密又は非秘密の輸出管理下にある情報を取り扱う資格を自動的に与えられることはないということである。

2　対情報活動とセキュリティ対策事項

2.1　序　論

より多くの米国企業の施設が外国の組織との係わりをもつにつれ、これら企業の多くが外国人の訪問、ジョイント・ベンチャー、共同研究などに関連した対情報活動(Counterintelligence: CI)に係わるインシデント報告が顕著なものとなっていることを、国防保全局(Defense Security Service: DSS)は注目している。外国人の訪問、ジョイント・ベンチャーや共同研究に関連する対情報活動の問題は、一般的にはいくつかの簡単なセキュリティ対策事項(Security Countermeasures: SCMs)によって軽減することができるのである。最近の経験によれば、外国組織に対処するいくつかのベスト・セキュリティ対策事項には次ぎあるが、それらに限定されるものではない。

- ✧　技術管理計画(Technology Control Plan: TCP)をもつこと。
- ✧　輸出管理問題に係わる知識を従業員に与えること。
- ✧　コンピュータ・セキュリティ監査を頻繁に実施すること。
- ✧　契約書を「英語」で記述すること。
- ✧　入国許可(visa)申請に応じないこと。

2.2　技術管理計画

技術管理計画(TCP)は、会社の輸出管理下にある技術のアクセス方法及び開示が許可されている特定情報について規定するものである。技術管理計画は、秘密及び輸出管理下の情報の保護、外国人訪問者に対するアクセス制御、並びに外国人従業員に対するアクセス制御に係わる計画である。技術管理計画は、セキュリティ対策事項の一つであるが、国際市場におけるビジネスの確保に努力するあまり、しばしば看過されることがある。ある種の状況下にあっては、技術管理計画が国家産業保全計画運用マニュアル(National Industrial Security Program Operating Manual: NISPOM)及び国際武器取引規制(ITAR)に求められることもある。技術管理計画は、すべての輸出管理下にある情報へのアクセス及び開示のためのガイドラインを示すとともに、企業の業務運営及び明らかにされた特定脅威との整合を図るべきである。国防保全局の対情報活動組織は特定脅威を明らかにすることについて企業を支援することができる。

2.3　輸出管理問題の知識

多くの中小企業は外国組織とのビジネスを急ぐあまり、しばしば武器輸出管理法(Arms Export Control Act: AECA)に気づかない場合がある。武器輸出管理法は連邦法であり、防衛装備品及びサービスの販売及び輸出について規制するものである。国防貿易管理局(Office of Defense Trade Controls: ODTC)は、国際武器取引規制(ITAR)に基づき武器輸出

管理法を履行する。国際武器取引規制は防衛装備品及び関連する技術データの輸出について規定し、企業に対してライセンス又は他の書面による輸出許可を求めるものである。米国の企業が国際武器取引規制に違反や輸出違反を犯していることにさえ気づかずに、防衛関連装備品又はサービスを輸出する可能性が正に現実なものとなっている。しかしながら、ことわざにあるように「法の無知は弁明根拠にあらず(ignorance of the law is no excuse)」である。輸出管理に係わる事項については、外国とのビジネス交渉の当初から考慮されるべきである。国防貿易管理局にはインターネット・ホームページがあり(www.pmdtc.org)、国務省通商停止参照表(State Department's Embargo Reference Chart)、武器輸出管理法に基づく輸出禁止国家、国際武器取引規制及び輸出ライセンス申請書に係わる情報が掲載されている。企業は輸出管理問題に関連する知識を得ることにより、多大の時間と金銭の節約を図ることができるのである。

2.4　頻繁なコンピュータ監査

（コンピュータ監査は）先進技術を取り扱う米国企業の施設に共通する問題である。このようなことから、ほとんどの政府職員や企業従業員がインターネットへのアクセス権を持っている。ビジネス上の取引さえも、インターネットの支援を得てより頻繁に行われている。インターネットの利用には潜在的な脆弱性があり、短時間に大量の情報を失う結果となることもある。さらに、施設の外部とのコンピュータ接続を行っているすべての会社は、ファイアウォールを設置していてもハッキングの脅威に曝されているのである。慎重に講じられたセキュリティ対策事項(SCM)は、毎日又は少なくとも毎週、コンピュータ・セキュリティ監査を行うことである。この監査の目的は、許可されていない侵入の試みを検知することである。しかしながら、コンピュータ監査は、コンピュータ侵入の検知による不正な活動の報告がなされ、かつ、改善又は是正処置が講じられない限り、単なる時間の浪費となるのである。不正な侵入の企てについては、各施設の情報システム・セキュリティ計画の規定に従い、各施設において取り扱われるべきである。少なくともこの不正侵入があった場合の取扱いには、一般的に施設セキュリティ責任者(Facility Security Officer: FSO)、国防保全局(DSS)企業保全代表部、国防保全局の情報システム・セキュリティ専門家､おそらくは連邦捜査局支部に対して侵入の企て報告が求められることになる。侵入の企てが現又は元従業員であると決定された場合は、コロンバスにある国防保全局の運用センターに有害情報報告を提出しなければならない。現又は元従業員が不正侵入の企てを行った場合、それらの者に対するコンピュータ・システムへのアクセスを除外すべきである。場合によっては、積極的なコンピュータ侵入の企てに対してコンピュータ・システムの施設外との接続を一時的に切断し、侵入の企てが継続するならば、切断したままでこの不正活動に対処するための特別計画を策定することになるであろう。他の慎重に講じられたセキュリティ対策事項には、従業員に対していかなるインターネット上の未知の要求にも対応しないこと、また、そのコンタクトについてセキュリティ責任者に報告するこ

とを求めたポリシーの確立がある。

2.5　契約書は「英語」で記述

外国組織と米国企業とのジョイント・ベンチャーにおいて、企業でやりとりされるコミュニケーションや往復書簡に結果として不合意が生じた事実を国防保全局(DSS)はこれまでに何度となく承知している。多くの米国企業は、外国の組織と頻繁に契約交渉を行うのであるが、翻訳のコスト節約に結びつくと思われる簡単なセキュリティ対策事項(SCM)を講ずるのを忘れている。契約書を「英語」で作成して双方が合意することになれば、米国の企業でやりとりするすべての往復書簡は英語で作成されることになる。企業が英語で契約書を作成しないとなると、米国の企業から輸出管理、企業機密又は秘密に係わる情報が流出して行くのを確実に防ぐには、通訳を採用する方法しかないことになってしまうのである。

2.6　入国許可申請に応じないこと

外国の市民は、「単に、そうしたいからといって」、不法に米国の領土に入ることはできない。ほとんどの外国の市民は、米国へ入国にあたってビザが求められる。多くの外国の科学者やエンジニアは、研究の実施目的で米国への訪問を望むのであるが、彼らは米国のスポンサーに対してビザを申請しなければならない。外国の組織が米国入国ビザの獲得目的でわれわれに支援を求めることに、米国の関係者は疑念を示すべきである。米国の企業や米国政府にとって明確な利益がないのであれば、ビザの求めに応じないことである。欲せざる外国人訪問のスポンサーとなることを穏やかに断ることにより、発生する可能性のある問題を未然に防ぐことができるのである。

2.7　要　約

国防保全局対情報室(DSS CI)の目的の一つは、企業の国際市場への参加機会が増えることから、合理的で費用対効果のあるセキュリティ対策事項を採用するにあたっての脅威情報の提供支援を行うことである。前述のセキュリティ対策事項は、外国の組織とのビジネスを行う企業に一般的な推奨対策事項の幾つかを示したものである。あなたの会社がなんらかの疑いを抱かせるような外部からの接触に遭遇した場合、その事象を国防保全局及び連邦捜査局に報告すべきである。

3　外国人の訪問：何が不適切か？

3.1　序　論

外国人による会社訪問中の不適切なふるまいに係わる事項について、国防保全局は米国政府の保全施設適格証明書を有する企業からの報告を継続して受けている。訪問中の不適切なふるまいは、外国の情報収集活動の手口(MO)として頻繁に報告されている。外国の組織にとって訪問は、よりコストがかかるとともに少しばかりリスクは高くなるが、たいてい訪問者たちは、標的とした企業施設へのアクセスによってなんらかの利益を得ているのである。このような理由からこの情報収集活動の手口は最も頻繁に利用されるものではないが、この訪問によりかなりの技術が奪われる結果となる可能性があり、米国にとっては外国の情報収集活動による最も損害の大きな手法となっている。優れた情報収集家は、いったん企業施設に入ると、訪問を巧みに利用して彼らの求める幾つか又はすべての目標とする情報に向かっているのである。外国の科学者やエンジニアは手続きが煩雑な情報入手手続を待つことなく、訪問することによって獲得した技術を本国に持ち帰り、その技術を直接彼らが必要とするものに応用するのである。

3.2　テクニック

外国人による大多数の訪問は無事に終了するが､そのかなりの者がなんらかの不適切な、又は疑われるような行動を結果として起こしているのである。報告された事例によれば、外国人の訪問中の不適切なふるまいとして､“問い詰めると腹を立てる｢ぶらつき｣訪問者”、“許可された話題の範囲を超えた質問”と“データ交換協定の不正利用を含む隠された議題”､“前ぶれなしの会社施設の訪問”､“写真撮影と記録”､米国政府から公式に訪問のスポンサーとなることを拒否された場合の“｢商用｣話題への切り替え”、並びに“訪問団員の直前又は前ぶれなしの追加”などがある。これら事例にあるテクニックの多くは、ホスト側が融和的に努めようとすることを利用して情報収集目的を達成しようとするものであり、ホスト側に潜在的に当惑させるインシデントとなるよう特に仕組まれたものである。

3.3　事例研究

外国人の訪問中における不適切なふるまいの報告の多くは、本来的にはセキュリティ対策事項で護られたことを逆手にとって、これを脆弱なものとした利用が関連している。このようなことは、訪問団の規模に比べセキュリティ対策事項が十分でない場に最も頻繁に起こるものである。他の事例は「何を保護すべきか」及び「質問にどのように答えるべきか」について、外国人訪問者の案内をする者が事前に適切な説明を受けていなかったというものである。ある航空会社施設への訪問時に、10 名からなる外国人訪問団に対して一人の案内人が割り当てられた。その訪問団は、案内人の態勢に脆弱性があることに気付き、この機会を利用してトイレ休憩の間に訪問団を分割させたのである。これにより、輸出管

理技術を取り扱っている区域で、訪問団の半分は案内人がいない状態になってしまったのである。

米国内に常駐する外国人駐在武官によってよく利用されるテクニックに、三つ揃えのスーツに名刺を携え、なんの前ぶれもなく企業の施設を訪問するというのがある。(本来ならば軍服姿の）駐在武官がビジネススーツで契約会社を訪れると、会社の従業員はあまり脅威を感じないのである。しかしながら、それ自身のテクニックは「前ぶれなし」であり、駐在武官の施設アクセス許可は、会社の管理者の好意に依存しているのである。ワシントン行政区内に分散している複数の施設において、頻繁に駐在武官が非秘密の論文及び小冊子を求めるとともに、話題を他の市場性のある開発事業を明らかにさせる内容に切り替えたというのがある。会社の従業員は気付いていないと思われるが、ほとんどの外国人駐在武官は、情報将校であるか又は情報将校として活動しているのである。

この他の普通によくあるテクニックとして、外国人訪問団の参加団員を訪問直前になって変更や追加するというのがある。このテクニックもまた、企業管理者の好意に依存するものであり、企業側が団員の変更や追加の施設訪問を許可することを期待するものである。この変更又は追加される人物は時おり、大使館又は領事館からの文官又は駐在武官ということがある。直前になっての訪問者の追加や変更の理由は、企業が当該訪問者の身元調査に要するに十分な時間がないことになるのを確信しているからであり、このことによって情報将校を企業施設に滑り込ませる可能性が高まるのである。

3.4　セキュリティ対策事項

これらの情報収集テクニックに関連する脆弱性を軽減するための幾つかの推奨セキュリティ対策事項は、相対的に簡単で、安価、そして実施されれば効果のあるものである。

- ✧　疑いを抱かせるような外国人訪問者の施設へのアクセスを許可しないこと。何人もアクセスすることはできないことと改めてアポイントメントを取るべきであることを彼らに告げること。
- ✧　施設へのアクセスを行わせるにあたっては、直前の追加や変更を許可しないこと。他の団員のアクセス許可の間、直前に追加や変更した訪問者はロビーに留まるよう求めること。これにより、情報将校を企業の施設外に潜在的に留まらせることができ、適切な公式訪問手順を促進することができる。
- ✧　外国人訪問者が到着したときに、提出されている訪問申請書と訪問者の識別照合を確実に実施し、彼らが言うように本当に当人かどうかを確認すること。
- ✧　訪問団が幾つかのグループに分かれたとしても、それらを管理するのに十分な数の案内人を確実に準備すること。

✧　案内人に対する十分な教育を確実に実施し、施設内の重要な箇所はどこか、及び外国人訪問団から防護すべきものが何かを周知徹底させること。

✧　施設内の従業員に対する説明を確実に実施し、外国人訪問団の訪問（視察）範囲を知らせるとともに、許可された事項以外はいかなる対話も行わせないようにすること。

✧　セキュリティ・インシデントを起こした訪問者が、問い詰められ腹を立てた場合、これは情報収集のテクニックであることを認識し、当該訪問者が規則に従った行動をしなければ施設から離れることを要求すること。

✧　施設内のある何かが「サイト・センシティブ(sight sensitive)」[2]に該当する場合、いかなる写真撮影又はノートへの記録をも許可しないこと。

[2] Sight sensitive：ちょっとした視察でセンシティブ情報をもたらすような物体をいう。

4　隠れ蓑会社：エンドユーザーは誰か？

4.1　序　論

国防保全局(DSS)は、不審な「隠れ蓑会社」に関連した多くの報告を毎年受領している。場合によってはこの様な報告が、連邦捜査局(FBI)や米国関税局の捜査に委ねられることもある。隠れ蓑会社は、米国政府や防衛関連企業に対し重大な問題をもたらすことができる。なぜなら、隠れ蓑会社は、輸出制限及び通商禁止を回避する目的で利用され得る潜在的可能性があるからである。

4.2　テクニック

隠れ蓑会社は、一般的にあたかもコンサルタントであるかのような営業を行っている。隠れ蓑会社は、一般的にエンドユーザーが誰であるかを隠す意図をもって、代理として活動している。隠れ蓑会社は、正規の方法で技術の所在を突き止めた上でこれを取得し、不正な受取人に対して不正輸出を行う目的で利用されるである。この種の疑いのある指標には次のようなものがある。

- ✧　米国の企業が「割合に知られていない」会社からファックス、郵便、電子メールや電話などで、軍事関連情報について一方的な提供依頼を受け取る。その依頼自身は、簡単で経費のかからない、脅威を抱かせず、なんのリスクもないものである。
- ✧　一方的な依頼
  - ➢　「怪しげな」英語で送られている。
  - ➢　「いいかげんな」ビジネス・レターヘッド[3]や標準的なビジネス慣行に比べると素人的なフォームで送られている。
  - ➢　たまには、デュアルユーズに属する技術（電子、航空、通信）を含んでおり、それらは利用目的によって輸出許可を必要とするものや必要としないものがある。
- ✧　その隠れ蓑会社は、
  - ➢　ほんの数人の従業員しかいない。そこの従業員は他のビジネスにも従事しているようである。
  - ➢　該当する装置について仕事をしている者であれば、当然あるはずの知識がない。
  - ➢　該当する装置の契約に際して、整備保証や操作員の訓練については断っている。
  - ➢　購入契約した以外の第三者にその装置を運搬するかのような印象があり、かつ、実際のエンドユーザーは未知である。
  - ➢　会社自身がコンサルティング又はブローカー・ビジネスであることを明らかにしているようである。

[3] 便箋上部に印刷された差出人名、事業署名、所在地など

- 外国大使館とのコネを持っているか又はビジネス上の関係にあると思われる。
- 外国銀行による資金供給を得ていると思われる。
- 通商禁止国にオフィスを持っていると思われる。
- 取引を速やかに終わらせ、前金で支払うことを望んでいる。

✧ その隠れ蓑会社の代表者は、

- 不法取引ができるかどうか見定めるため、米国企業やその代表者の誠実さをテストすることを企てていると思われる。
- 品物が運搬される第三国に米国企業のオフィスが存在しているか否かを尋ねることがある。
- 米国の企業が品物の運搬に気が進まないのを抑えようと、金銭的刺激（賄賂）を申し出ることがある。
- 不正取引の片棒を担がせるため、外国の当局担当者をすぐにも買収できると暗示することがある。

4.3 事例研究

カリフォルニアにある米国の有限会社が米国の防衛関連企業から電子妨害装置を購入するため、関連情報を一方的に求めてきた。その電子妨害装置は、国際武器取引規制(ITAR)の対象となっているものであり、米国外に輸出する場合は許可が必要となるものである。その電子妨害装置を求めているカリフォルニアにある会社の従業員数は数人だけであり、当事者である米国の防衛関連企業は、その社名さえも知らない組織であった。電子妨害装置を求めているカリフォルニアの会社は、明らかにエンドユーザーではなく隠れ蓑会社に近いものであった。

この他のインシデントには、南西アジアの国にだけに売却した航空機のシステム構成部品について、ある米国の会社が米国の防衛関連企業に対して見積要求（Request For Quote: RFQ）を提出したというのがある。その南西アジアの国は、米国の通商禁止国リストに以前から掲載されていた国であった。その見積要求を提出した米国の会社は、以前からあまり知られていないテキサスにある小さな会社であった。その部品のエンドユーザーとして指定されているのは、西ヨーロッパの国であった。見積要求書はおそらく自宅のコンピュータで作成されたものと思われ、ビジネス・レターヘッドは手書きで書き込まれたものであった。米国の防衛関連企業は、同じ航空機部品に関する同じような見積要求書をフロリダにある他の米国の会社から受け取ったときに不審に思ったのである。第 2 番目の見積要求書ではエンドユーザーがリストに掲げられていなかったものの、部品の番号、量及び物品番号は最初の見積要求書と全く同一であった。これらの見積要求書を提出した 2 つの米国内の会社は、南西アジアの国又はその代理人によって運営されている隠れ蓑会社のようであった。

隠れ蓑会社のあるものは、より露骨で明らかに不正な申し出を行うこともある。フロリダに所在するある会社は、米国の防衛関連企業に手紙を送ったあと、数週間後には電話をして秘密の航空機搭載用赤外線妨害システム販売のためのビジネス協定の締結を申し出た。米国の防衛関連企業は、この国に対する輸出許可を得ることができず、ビジネス協定を推し進めることについて辞退したのであった。このビジネス協定の締結を求めた会社は、その後また、輸出許可の承認が下りる国に所在するオフィスや子会社を介して、当該妨害装置を輸出することについて米国の防衛関連企業に申し出たのであった。

4.4　セキュリティ対策事項

最良のセキュリティ対策事項は、あなたの顧客を知ることである。米国の多くの防衛関連企業は、日々、同じ会社とビジネスを行っている。センシティブ又は秘密の情報及び技術を求める「新しい」会社が登場した場合、当該会社の社歴をチェックすることが賢明なリスク管理といえる。対象となる会社が上記の指標のいずれかに該当して疑いをもたらすのであれば、御社の施設保全責任者(FSO)は国防保全局企業保全代表部、連邦捜査局及び米国関税局に通知すべきである。

5　インターネット：勝手な情報収集に急速な拡大をもたらしている手口

国防保全局(DSS)に提出された外国人による不審な接触報告によれば、米国の保全施設適格証明書を有する会社及びその従業員と外国組織との間において、インターネットがコンピュータを利用した情報引き出しの勝手な通信手口として最も急速に拡大しているとされている。物事に精通した様々な人を対象に、外国の組織がインターネットを利用した情報収集の手口を利用して接触を行っているという報告が、次から次へと国防保全局に提出されている。外国の組織は様々な断片情報を収集する意図を持って、これら専門家との接触を行っているのである。その後これらの断片情報が集められて驚くばかりのはっきりとしたモザイクとなり、誰しもが提供できなかったと思われるような詳細な情報を明らかにするのである。

インターネットの利用は、外国人収集家にとって様々な利益をもたらしている。外国の組織が秘密、企業秘密やセンシティブな情報を収集するにあたって、インターネットの利用は簡単かつ低コストであり、相手に脅威を与えることもなく、しかも比較的リスクが少ない情報収集の手口となっているのである。これらの外国の組織は、標的とした米国の企業やその従業員に何百という情報収集のための依頼と要望及び支援要請の通信を送り続けている間、彼らの国境内にあって安全に留まっていることができるのである。情報に対する勝手な要求は、インターネットの利用を含め「閉鎖国家(closed country)」に最もよく利用されている情報収集の手口であり、文化の共有をアピールするものであるとしばしば言われることもある。

外国の組織から米国の保全施設適格証明書を有する企業に送られた最近のインターネット利用の一つに、目に余る勝手な要求がある。それは、ネットワーク化されたリアルタイム・オペレーティング・システムのソフトウェア・ツールを利用した軍事プロジェクト（航空、宇宙、ミサイル、戦術、情報など）に関連する問い合わせを行ったというものである。外国の組織は、その要求の中で、ほとんどの情報がおそらく秘密であろうことを認めている。彼はまた、自国の「軍の顧客」がインターネットを利用した要求の送付に直接関与するには余りにも機密扱いにしすぎることも認めた上で、外国政府に対するサービスとして要求しているとしているというのである。

インターネット利用に係わる不審な活動報告に、東ヨーロッパの国における情報組織や保安組織に対する情報活動機能関連のアプリケーション・ソフトウェア・プログラムの売り込み要求を受け取ったというのがある。そのソフトウェア・プログラムは、複数のデータ資源や無数の文書を驚異的な速さで統合することができ、様々なウェッブサイトを検索する捜査ツールとして利用することができるのである。少なくとも、そのソフトウェア・プログラムは、外国の会社がインターネットを通じて競合するビジネス情報の取得に利用することができるのである。

多くの外国において、インターネットへのアクセスは、政府がホストとなっている可能性がる。これらの国々とのインターネットを介した外国人による接触のすべては、情報機関及び保安機関による監査及び監視の対象となっており、技術的秘密事項の漏えい防止及び西側技術の収集に利用されている。インターネット検索ソフトウェアへのアクセスが、外国の情報機関及び保安機関によるインターネット捜査及び監視により、情報及び対情報活動の両目的を支援していることは疑う余地もない。ある東ヨーロッパの国では過去 2 年間、幾何級数的に多くのインターネット・ホストが増加し、情報当局による米国のコンピュータ・システムへの侵入にどのインターネットが利用されているのか、その識別を困難なものとしている。外国の情報機関が情報入手のために初歩的なオンライン検索を行っていることは知られており、これにはインターネット上にある政府及び防衛関連企業のオンライン掲示板やウェッブサイトが含まれている。おそらく、先進のインターネット検索ソフトウェア・プログラムへのアクセスは、彼らの収集要求を満足させる一助となっているものと思われる。

外国の情報及び保安機関による先進ソフトウェア・ツールの利用は避けられないが、国防保全局に報告されたこれらのインシデントから、我々はセキュリティ上の教訓を得ることができる。そして、我々は明らかにされた脆弱性を軽減するため、セキュリティ対策事項を導入することができるのである。情報要求の手段としてのインターネットの利用が簡単で、低コスト、そしてリスクがないことから、我々は外国の組織がこれを利用していることを知っている。我々はまた、外国の情報機関や保安機関がインターネットを監視しているとともに、彼らの検索と捜査をより容易にする先進のソフトウェア・ツールを持っていることも知っている。

インターネットを介して受け取ったすべての情報要求について、我々は疑いの目をもって審査すべきである。個人への回答は、その要求者が個人として知られた人物であり、かつ、身元及び住所が確認された後にだけ行うこと。外国の組織は、彼ら自身の名を偽って存在している可能性があることから、このような確認は重要なものとなる。要求が知らないところから送られてきた、又は知られているところからの通常の要求とはどことなく異なる場合は、要求文の写しをセキュリティ責任者に提出するとともに、その要求に決して応えるべきではない。

下記は、コンピュータ利用の引き出しによる外国からの収集活動に係わる不審な指標である。

- ✧ 住所が外国になっている。

✧　受取人は、差出人に会ったことはない。
✧　差出人は、自身の身元を学生またはコンサルタントであるとしている。
✧　差出人は、自身の雇用者を外国政府であるとしているか、又は外国政府若しくは外国政府のプログラムの仕事をしていると明言している。
✧　差出人は、防衛関連のプログラム、プロジェクト又は契約に係わる技術について尋ねている。
✧　差出人は、プログラムに特定の略号を使用して、その防衛関連プログラムについて質問している。
✧　差出人は、第三者の「秘密の」又は「センシティブな」仕事をしているとほのめかしている。
✧　差出人は、要求が秘密又は管理下にある情報であることから、他から入手できなかったことを認めている。
✧　差出人は、受取人に対して、セキュリティ上の問題となる又は要求がセキュリティ上の秘密区分、輸出管理などに抵触することから情報の提供ができないのであれば、無視してもよいと言ってきている。
✧　差出人は、受取人に対して、セキュリティ上の問題を心配しなくてもよいと言っている。
✧　差出人は、受取人に対して、輸出許可は必要でない又は問題はないと断言している。

6　保全施設適格証明書を有する防衛関連企業から科学技術情報を収集するための学術的接近

ここ数十年間、米国の関係者から科学技術(Scientific and Technical: S&T)情報を引き出す手口として、外国の政府及び外国の民間商業組織の関係者が学術的接近を利用している。大学及び研究センターに所属する外国人が、国防総省(DoD)及び政府当局担当者、保全施設適格証明書を有する防衛関連企業、並びに軍事プログラムの従業員に対して、調達プログラム、資材及びシステム構成品、並びに設計及びエンジニアリング・プロセスと進捗状況に係わる科学技術情報について質問している。一般的に、このような情報は秘密、企業機密、輸出管理を必要とする重要軍事技術や秘密区分には属さないがセンシティブなものであり、民間の商用プログラムは無論のこと軍事にも適用されるものである（デュアルユーズ)。

保全施設適格証明書を有する企業から国防保全局(DSS)に提出された報告は、保全施設適格証明書を有する国防総省の企業に対する外国組織からの情報収集の手口(MO)として、勝手な情報要求が最も頻繁に利用されることを示している。各年とも、保全施設適格証明書を有する会社からのインシデント報告に、学術的接近の指標を見出すことができる。1977 年以来、国防保全局は保全施設適格証明書を有する企業に対する学術的接近の傾向を観察しており、(最近の傾向としては) 修士論文のデータ収集であると記述した外国からの勝手な要求がある。

国防保全局に提出された報告は、米国企業に対して行われた様々な学術的接近を示している。ある外国の大学は保全施設適格証明書を有する防衛関連の航空及び宇宙会社に対し、データは学術的研究だけに利用することを保証して調査項目に記入することを要求してきた。とりわけ疑念を抱かせる質問には次のようなものがあった。

- ✧　主契約又は下請負契約の別を付して、会社の米国防衛関連プログラムを明示
- ✧　下請負企業としての取引パーセンテージ
- ✧　主な防衛関連製品及びサービス
- ✧　「わが国との取引促進にあたっての関心事は何か？」及び「そのような取引をどのように促進するのか？」

これらのうち「　」書きで示した最後の 2 つの調査質問事項は、外国の組織が米国の企業に再接触を望む場合、どのように、そしてどの優先順位で行うかを決定する際に利用できる答を回答者から引き出すものなのである。これらの調査質問事項に対する回答は、外国の関係者がどの保全施設適格証明書を有する企業に接触して、どのように標的を追い求

めるかを確証する際の助けとなるのである。それらには、文化的共通性の開拓、書面若しくは人を介した販売アプローチ（例：軍事又はデュアルユーズ製品に対する商業ライセンス）、旅行の間の接触、又は米国の企業若しくは従業員に合わせた接触手法などがある。

通商禁止国家から郵送されたある手書きの手紙は女性からのもので、「ミサイル誘導システムの精度計算における統計的分析」に係わる修士論文作成の助けとなる情報を求めるものであった。手紙を受け取った当事者は、どこの大学からなのか明らかにすることはできなかった。彼女への返送先は、郵便局の私書箱であった。そして、「単に、共分散分析手法に、・・・利用することに焦点を当てて」や「敬愛する・・・様」、また「自国に対する米国の通商禁止国指定が参考文献の欠如に影響を及ぼしている」などと記述して同情を引き出し、テーマの軍事上の重要性を目立たなくさせようとしていた。

他のインシデントは、米国外からの手紙、葉書及びファックスに関連したものである。手紙では、海軍工科大学に入学を命じられた外国の海軍将校が、熱線画像化及び捜索に係わる科学技術(S&T)情報を求めてきたというのがある。また、ある外国の研究機関の教授は、ガスタービン・ストレス・レシオに係わる方程式を求めてきた。電子光学(EO)技術の軍事への応用として知られている外国の大学が葉書を送ってきて、衛星搭載用画像化及び鮮明化装置に係わる電子工学情報を求めてきた。外国の国立大学の無線通信科の代表者が、マイクロ波吸収材に係わる情報をファックスで求めてきた。他の国の電子及び自動化研究所からの印刷した同文の手紙は、同様なデータを求めてきた。外国のビジネス・スクールからの印刷した同文の手紙は、センサー・データの融合について、競合する製造方式に係わるソフトウェア開発及び統合情報を求めてきた。最後に、ある中央研究機関が米国の企業に空気力学データについて問い合わせを行うとともに、機体空気抵抗削減のための国際科学技術プロジェクトにおいて共同研究を行うことを提案してきた。

これらの話題は、重要軍事技術、輸出管理下にある米国技術そのもの、又はこれらに関連したものである。企業が要求された情報を漏らすことになると、外国の関係者は彼らの軍事及び国防能力を増大又は拡張することができるのである。これらのインシデントは、様々な接触手段、標的対象及び外国の収集組織の存在を明らかにしているものであるが、その指標となっているものは首尾一貫している。つまり、要求の受取人は要求者に会ったことが決してなく、かつ、差出人が通商禁止国、軍事的危険地域及び経済的競合国となっていることである。

学術的接近の半数は差出人自身の身元を学生だとして明らかにし、その大部分は「修士論文」に利用するとして彼らの要求を正当化している。保全施設適格証明書を有する企業の従業員は、「論文要求」による標的となることが一般的である。差出人が学術的接近を行

った時点で、標的となった(宛先人の)従業員がその企業に在籍していたのは確かであるとされている。学生は常に、「(秘密保全適格証明書を有する従業員が) 提供できる助けとなるものは何でも」と求めている。要求は、米国に滞在している外国人学生からは無論のこと、海外からもやってくるのである。それらは先進ミサイル/バイオメトリクス・アクセス制御装置(「建物の中におけるセキュリティ及び安全のため」)、暗号におけるニューラル・ネットワーク(脳神経をモデルにした情報処理システム)、集積回路、全地球方位システム(GPS)などの重要軍事技術に関するものである。これら科学技術情報のすべては、軍事への適用を行っているものであり、かつ、輸出管理下にあるものである。これらインシデントに基づく不審な指標には論文のテーマが含まれているが、それらテーマは特定の結論を導き出すには余りにも広範なものであり、かつ、修士論文担当の学科長によって承認されるべきものと思われるようなテーマでもある。

グローバルな市場及び国際的なビジネス傾向から、国防保全局(DSS)はこれらの学術的接近が増加し続けるものと予想し、中でもインターネットの電子メールを介した接近が顕著であるとしている。学生や学生を装った者は、ネット上の情報源及び研究参考文献をますます捜し求め続けている。外国の情報収集組織は、彼らの意図を隠すためにこの手段を利用していると思われる。国防保全局は「海外の修士論文テーマ」及び「共感の誘い出し」について、次の出版物としている「米国防衛関連企業に向けられた外国からの情報収集活動に係わる不審な指標及びセキュリティ対策事項」[4]の不審な指標リストに掲載する予定である。このパンフレットは、外国からの既知及び不審な収集活動の発見及び無効化の方法を明らかにするものである。

4 本小冊子の付録がこれに該当する。

7　米国防衛関連企業に向けられた外国からの情報収集活動に係わる不審な指標及びセキュリティ対策事項

この項については、付録「米国防衛関連企業に向けられた外国からの情報収集活動に係わる不審な指標及びセキュリティ対策事項」を参照されたい。

8　情報の引き出しに利用される入札

米国防衛関連企業の担当者からのインシデント報告に、ある西ヨーロッパ政府の航空電子システムに係わる外国の防衛関連契約について、提案書の作成及び入札の要請を受けたというのがある。その米国防衛関連企業の担当者は、外国の政府契約に対し彼らが他のすべての入札者よりも最良かつ最も詳細であると確信する提案書を作成した。このような努力にもかかわらず、すべての入札が終了すると、その外国の政府は彼ら自身がシステムを構築することを決定してしまったのである。

米国の防衛関連企業は、外国の政府が当初から米国の会社と契約を締結する意図はなかったのではないか、つまり、外国の政府はなんらかの技術的情報をだまされやすい会社から入手することに関心があっただけではなかったのかと今になって思っている。その後、米国の防衛関連企業の従業員が国際貿易展示会に出席した際に外国製の航空電子システムを見たが、それは入札目的で米国から提出した彼ら自身のシステムと同じようなものであった。米国の防衛関連企業を慎重にだますことによって、外国の政府は企業機密を収集することができたと思われる。このようなごまかし行為によって、その外国政府は実証されたシステムから予備概念及び設計を取得することができたと思われ、かくして研究開発プロセスにおける金と時間を節約したのである。

米国防衛関連企業は、一方で外国政府に技術的企業機密を提供する際のリスクを心配したかもしれないが、他方では誠実な競争プロセスを期待したのであった。他の政府や外国の会社も、このような情報収集の手口(MO)を利用して企業機密を手に入れるかもしれない。米国の防衛関連企業は、次のような処置を講ずることによってセンシティブな企業機密情報を失うリスクを削減することができるのである。つまり、米国防衛関連企業は、将来パートナーとなる外国の組織について調査するとともに、企業の費用便益分析に企業スパイの犠牲者となる潜在的可能性の要素を加えることである。対象となる特定の国又は外国政府が、これまでに経済スパイ又は産業スパイを行ったという経歴を証拠書類で立証されるのであれば、そのような国又は外国の会社とビジネスを行うことは米国防衛関連企業の利益にはならないのである。米国防衛関連企業は少なくとも契約獲得競争のために必要となる絶対最小限の情報量を提供する方を選ぶことができるのである。

国防保全局(DSS)は、企業の将来のパートナー又は顧客が企業機密技術の収集脅威となるか否かを調査するのを支援することができるであろうか？直接にはできない。国防保全局は、保全施設適格証明書を有する企業がセキュリティ態勢全般を改善するのを支援することにより、企業機密保護を(間接的に)支援することになる。しかしながら、その外国の顧客又はパートナーは、会社間の相互訪問、及び引き続くその外国の組織の要員と米国の企業の秘密保全適格証明書を有する従業員との間の接触を介して、米国の輸出管理下にあ

る情報又は秘密情報に対する脅威となり得ることもある。外国組織の要員の訪問に情報取得の権利を与えるものではないが、訪問によって情報の直接観察及びそこからなんらかの情報が引き出されることになるのを許してしまうのである。訪問による触れ合いは、何らかの利用目的での社交的接触の基礎を築くものであり、情報の引き出し活動及びスパイ活動をする両者にとって重要なものとなるのである。このような理由から、外国人に関連する活動が秘密のプログラムに影響を及ぼす潜在的可能性を有することに関して、国防保全局の代表者は、保全施設適格証明書を有する会社との密接な連絡を取ることが重要となっている。国防保全局は対情報(CI)室を介して外国組織が属する国の情報収集の手口や収集要求を調査し、なんらかの知り得た情報があれば、秘密のプログラムに対して潜在的な脅威を有する保全施設適格証明書を有する企業に対して助言を行うことができるのである。この調査の成果は、秘密にしておくものであり、保全施設適格証明書を有する企業の知る必要性のある従業員に対してだけ開示されることになっている。この秘密の調査成果の導入を企業機密技術の情報収集の引き出しにどのように利用するかは、企業自身の判断に委ねられている。さらに、米国政府の他の機関も、国防保全局の任務との関連性がない場合でも、このような事例にある企業を支援することができるのである。このような機関には、連邦捜査局(FBI)や米国関税局及び商務省が含まれる。国防保全局は、これらの機関と密接な連携関係を確立しており、これら機関と連絡を取りながら企業を支援することができるのである。

9　我々は何を保護しているのか？

スパイ行為関連の裁判において、優れた弁護士が被告を弁護するために最初の段階で行う事の一つは、「盗まれた情報又は装置が秘密の情報又は企業機密情報であることを被告は知らなかった」と裁判官及び陪審員団を説得することである。弁護士は会社の従業員やセキュリティ責任者を証人席に座らせ、秘密の情報又は企業機密情報の明確な識別及びその確実な保護のため、どのように適切な対策が会社内に講じられたかを証人に訊ねることが許されている。証人が秘密の情報又は企業機密情報保護に利用されている適切な保護手段や対策について十分明確な説明をすることができなければ、その訴えは却下されることになる。

米国内においては、「秘密の」米国政府情報の保護を確実なものとするための様々な連邦法がある。これらの法律は、米国政府に対してスパイ行為を働いた米国及び外国の市民を訴追するため、これまでに何度となく適用されてきた。しかしながら我々には、最近に至るまで、米国の民間会社が保有する秘密指定をしていない企業機密情報を保護する連邦法がなかったのである。このような手抜かりを埋めるため、1996 年の経済スパイ法(Economic Espionage Act of 1996)は米国の会社にかなりの保護を提供することを目的として、特に制定されたものである。

どの会社の責任者も持たなければならない責任事項の一つは、従業員に対してどの情報が秘密又は企業機密なのかを明確に識別することである。言い換えれば、会社は秘密の米国政府情報や会社の企業機密を保護するための適切な対策を講ずる責任があるということである。

「企業機密」の用語は、財務、ビジネス、科学、技術、エンジニアリング、経済情報などに係わるすべての資産を意味する。これらには、図案、計画、編纂物、プログラム装置、試作品、製法、設計、手順、手法、技法、コード、プロセスや有形若しくは無形及びその記憶方式を問わず物理的、電子的、図式的、写真によってコンパイル若しくは記憶されたプログラムが含まれるか、さもなければ次の事項が書面で明らかにされた場合である。

- ✧　所有者が、このような情報を秘密として保護するための適切な手段を講じており、かつ、
- ✧　その情報は、一般人には通常知られておらず、まともな手段では即座に確定することができない独自の経済的価値を引き出すものである。

企業は、すべての資産及び活動に対して、同一レベルの保護を保証するとは限らないことを認識した上で、保護が必要な資産はどれか及びそれらの相対的価値又は重要性を明ら

かにする必要がある。資産価値を必ずしもドルで評価する必要はない。しかしながら、資産保護のために講じられるセキュリティ対策事項の経費は、それら資産の価値に関連付けられた適切なものでなければならない。資産の価値は、それらが失われた場合の潜在的な影響の度合いに関連付けることができる。国防総省内では、資産が失われたことによる影響に人命や国家利益を含めていると思われる。

米国政府にとっての資産とは、すべての職員、施設、資材、情報又は活動であり、米国政府や会社にとって現実的な価値のあるものである。これらの資産は、米国政府や会社と同様に、情報収集を目論む者にとっても価値を持つものであろう。もっとも、それら資産価値の中味及び大きさは異なるであろうが。

下記に示す分類は、米国の企業に関連した一般的な資産の種類を明らかにするにあたっての助けとなるものである。5 つの基本的な分類には次のものがある。

- ✧ 人
  - ➢ 政府職員
  - ➢ 企業
  - ➢ 軍人
- ✧ 活動/作業
  - ➢ 情報収集/分析
  - ➢ 事業/要員/財産のセンシティブな移動
  - ➢ センシティブな訓練の実施
  - ➢ 通信/ネットワーキング
  - ➢ 研究開発試験及び評価（RDT&E）とセンシティブな技術
  - ➢ センシティブな技術の生産物
  - ➢ 核/化学/生物資材の保護
  - ➢ 武器、爆発物及び装置の保護
- ✧ 情報
  - ➢ 秘密の情報
  - ➢ センシティブ・コンパートメンテッド(compartmented)情報[5]
  - ➢ 機密(top secret)
  - ➢ 極秘(secret)
  - ➢ 秘密(confidential)

[5] センシティブ・コンパートメンテッド情報：Sensitive Compartmented Information (SCI)。国家安全保障に係わる特定の情報であり、なんらかの秘密区分(機密、極秘、秘)に指定されているが、その情報の存在については公表されておらず、特別な取り扱いが求められる情報をいう。

- 秘密に指定されていない情報
- システム設計
- 知的財産
- 特許
- システム能力/脆弱性
- センシティブな手法
- センシティブな財務データ

✧ 施設

- 事業場
- 本部
- 現地事務所/管理建物
- 訓練施設
- 企業施設
- 保管施設
- 製造施設
- 研究開発(R&D)研究所
- 発電所
- 駐車施設
- 航空機格納庫
- 邸宅

✧ 装置/資材

- 運搬装置/車両
- 整備機材
- 運転装置
- 通信装置
- セキュリティ装置
- 武器
- 情報処理装置

重要な資産についての情報は、様々な情報源から集めることができる。「資産所有者」やプログラム・マネージャ（たいていは会社の幹部）は、資産の保護について一般的に最も精通している人物である。時として、それらの人物はエンジニアであったり、科学者であったりもする。これらの人物は、どの資産がセンシティブかつ価値があるかに関して一般的には最も優れた考えを持っているのである。

セキュリティ専門家は、保護している資産の特性や価値を理解することにより、関連す

る脆弱性やセキュリティ対策の設置箇所についてより合理的な決定を下すことができる。また、理解することは、第一に保護されるべき重要資産及び最も効果的に保護すべき資源を配置する場所を確実なものとする助けとなるのである。

付　録：米国防衛関連企業に向けられた外国からの情報収集活動に係わる不審な指標及びセキュリティ対策事項

国 防 保 全 局

対 情 報 室

米国防衛関連企業に向けられた外国からの

情報収集活動に係わる不審な指標及びセキュリティ対策事項

目　　次

1　外国からの情報提供依頼

米国防衛関連企業の科学技術(S&T)プログラム情報に関する外国からの種々の提供依頼は、標的行為に関連した情報収集の手口(MO)として最も頻繁に報告されているものである。この提供依頼にはファックス、郵便、電子メールや電話が一般的に利用されるが、それらは米国の企業の販売部門よりもむしろ社員個人宛に送られている。その提供依頼には、調査又は質問事項が含まれており、多くはインターネットを介して送られている。

1.1　指　標

- ✧　提供依頼者
  - ➢　外国の電子メール・アドレスがある。
  - ➢　通商禁止指定国家に関連しているかもしれない。
  - ➢　彼の身分を学生又はコンサルタントとしている。
  - ➢　彼自身を「学生」であると明らかにしたうえで、彼の国ではこの種の科学や技術情報が欠落しているとして同情を求めている。
  - ➢　彼の雇用者は外国政府か、又は彼の仕事が外国政府若しくはプログラムのためのものか明らかにしている。
  - ➢　防衛関連のプログラム、プロジェクト又は契約に係わる技術について質問している。
  - ➢　防衛関連のプログラムについて、そのプログラム固有の略号を利用して質問している。
  - ➢　彼の雇用者の身元は、「秘密である」ことを遠回しに言っている。
  - ➢　提供依頼されたものが秘密の情報又は輸出管理下にある情報であることから、ほかでは入手できなかったことを打ち明けている。
  - ➢　提供依頼された情報がセキュリティ上の問題をもたらすか又はセキュリティ上の秘密区分、輸出管理規制に属するなどにより提供できないと判断した場合、提供依頼を取り下げることを打ち明けている。
  - ➢　提供を受けた人に対して、(その情報に係わる) 輸出許可は不要であるか又は問題にならないことを保証している。
- ✧　提供依頼を受けた人は、依頼相手と一度も会ったことがないか又はビジネスを行ったこともない。
- ✧　提供依頼された技術は、国際武器取引規制(ITAR)管理下にある秘密の情報、重要軍事技術リスト掲載の情報、又は商用及び軍事の両者に使用可能な情報である。
- ✧　提供依頼先は企業の販売部門ではなく、個人に対してファックスや郵便で送られている。
- ✧　提供依頼は、一般的に受け入れ可能な情報の要件を超えている。
- ✧　外国の競合会社が「調査屋(surveyor)」を雇ったという強い疑念がある。

1.2　推奨セキュリティ管理策

- ✧　技術管理計画をもつこと。
- ✧　情報提供依頼に係わる企業ポリシーを文書化し、保持すること。
- ✧　不審な情報提供依頼に応じないよう従業員に指示すること。
- ✧　不審なインシデントについては、施設セキュリティ責任者(FSO)に報告するよう従業員に指示すること。
- ✧　公開領域にどの程度の情報を掲載しているか見直すこと。
- ✧　外国人にその情報の必要理由、誰の代理人か、及び米国の情報や製品が何の目的で利用されるかを訊ねること。

2　ウェッブベースの情報提供依頼

ウェッブベースの情報提供依頼は、米国防総省の技術を標的にした外国の重要な情報収集源として継続的に行われている。かつては保護されていた沢山の情報が、今日ではウェッブの利用により世界中の人々によって検索可能となっている。外国の組織は、標的となる可能性のある情報を明らかにすることや実際の情報収集を容易にするため、ウェッブベースの情報提供依頼を急激に増加させているように思える。ウェッブベースの情報提供依頼は、簡単、低コストで、相手に脅威を感じさせず、かつ、リスクのない手段であることから、米国防総省の技術を手に入れようとする手段として広く利用されているのである。ウェッブベースの情報提供依頼は、注意を引くことなく、かつ、従来から講じられてきた多くのセキュリティ対策事項を迂回できることから、標的に直接手を伸ばして取ることができるのである。

2.1　指　標

- ✧　保全施設適格証明書を有する防衛関連企業は、外国の情報提供依頼者と一般的にはビジネスを行わない。
- ✧　情報提供依頼が通商禁止国から発信されている。
- ✧　情報提供依頼が、一方的であるか又は正当なものではない。
- ✧　情報提供依頼者は、公式の政府機関を代表する者であると主張しているが、情報提供依頼にあたって正規手続きの利用を避けている。
- ✧　最初の情報提供依頼は、提供依頼人が誰であるかを知らない販売又は市場売買部門の従業員を依頼先にしている。
- ✧　情報提供依頼者は情報を漁っている。
- ✧　情報提供依頼者は、確認不明の第三者の代表者であるとしている。
- ✧　情報提供依頼者は、米国の保全施設適格証明書を有する防衛関連企業にかつて情報

収集行為を働いた経歴のある国に在住している。

- ✧ 情報提供依頼者は「規制回避(skirting control)」をしているように思える。
- ✧ これまでにも同様の情報提供依頼が幾つかあった。

2.2 推奨セキュリティ対策事項

- ✧ 技術管理計画をもつこと。
- ✧ ウェッブの設計及び公表にセキュリティを組み込むこと。
- ✧ ウェッブサイトの監視に有効な解決策を導入すること。
- ✧ 情報提供依頼があった場合、施設セキュリティ責任者(FSO)に報告するとともに、国防保全局の対情報室(CIO)のデータベース化のために報告すること（幾つかの状況において、同様の情報提供依頼が米国の複数の保全施設適格証明書を有する施設に対して行われている)。

3 サービスの懇願及び市場調査

過去の報告で終始変わらないものに、米国の研究施設、学術機関及び保全施設適格証明書を有する企業に、外国の人物、会社及び研究施設が彼らの技術やビジネス・サービスを申し出ているというのがある。

3.1 指 標

- ✧ 外国人「科学者」がセンシティブな防衛技術に係わる職を求めている。
- ✧ 海外拠点でのソフトウェア支援を提供している。
- ✧ 外国の政府や事業者（企業）がスポンサーとなって外国人をインターンとして勤務させる。
- ✧ 文化交流、個人対個人交流又は使節プログラムに招待する。
- ✧ 外国における販売又は取得代行者としての活動を申し出る。

3.2 推奨セキュリティ対策事項

- ✧ 技術管理計画をもつこと。
- ✧ 相手が求めているものが秘密又は管理下にある研究及び技術に係わる場合、その外国人科学者及びエンジニアの氏名を報告すること。
- ✧ 外国の地でソフトウェア支援受ける場合、推奨セキュリティ対策事項を入手するとともに、リスク評価を行うこと。
- ✧ 交流や使節プログラムで出発するに先立って、国務省の旅行ブリーフィングを受けること。

4　外国による米国技術/企業の取得

外国の組織は、米国の技術やセンシティブな技術/製品を所有する米国の企業を取得することによって、センシティブな技術にアクセスしようとしている。

4.1　指　標

- ✧　政治的及び軍事的同盟国の企業は、十中八九この種の活動に関連している。
- ✧　外国の競合相手は、技術にアクセスすることが可能な米国の企業で有利な立場を求めている。
- ✧　外国の親会社や外国のパートナーから雇った新入従業員が、秘密のデータにアクセスすることを求めている。
- ✧　外国の親会社はセキュリティ協定事項の回避を試みているか、より間単に、外国人の所有、管理若しくは影響(Foreign Ownership, Control or Influence: FOSI)プロセスの回避さもなければ混乱若しくは妨害を行っている。
- ✧　外国の親会社の従業員が、セキュリティ協定事項の除外を求めている。
- ✧　セキュリティ協定事項などの許可は不要であると明言している。
- ✧　外国の会社が情報又は製品を海外に輸送するのに、米国の会社に対して米国に本拠地を置く他の会社に送るよう、又は Fedex 若しくは UPS を介して海外のあて先に送るよう求めてくる。

4.2　推奨セキュリティ対策事項

- ✧　技術管理計画をもつこと。
- ✧　プログラム室に対して脅威評価を依頼すること。
- ✧　外国組織のしつこい要請で採用した従業員を吟味すること。
- ✧　外国人訪問者に対するチェックを頻繁に実施して、外国人関係者がセキュリティ協定事項の回避を試みていないか確認すること。
- ✧　外部重役やユーザー代理店に対し、脅威ブリーフィングを定期的に実施すること。
- ✧　米国に本拠地を置く会社は何をするのか尋ねること。なぜその会社が外国の組織と協力し合うのか尋ねること。外国人がなぜ速達便で製品を送ることを望むのか尋ねること。情報/製品が、輸出管理下にあるのか否かを輸出管理責任者に尋ねること。

5　外国人の米国施設訪問

米国の保全施設適格証明書を有する防衛関連企業への外国人訪問は、確固たるリスク管理が実践されていない場合、潜在的なセキュリティ・リスクをもたらすことになる。

5.1　指　標

- ✧　外国の連絡将校や大使館の担当者が随伴する訪問者が、建前としては商用訪問にもかかわらず、公式の身分を隠そうとする。
- ✧　明確な訪問目的とは対照的な秘密の目論見がある。
- ✧　直前になって、事前に知らされていなかった人物が訪問団に追加された。
- ✧　「コース逸脱」訪問者が、そのことを問い詰められたときに腹を立てた。
- ✧　代替手法を利用する。例えば、秘密を取り扱う施設への訪問が許可されなかった場合、その外国組織は商用訪問を企てる。
- ✧　訪問先の好意や自発的な対応を期待して、ブリーフィングの間に訪問者が許可された訪問目的範囲外の質問をする。
- ✧　訪問者はビジネス上の関心があることを主張しているが、この技術に関する研究や開発経験が欠落している。

5.2　推奨セキュリティ対策事項

- ✧　技術管理計画をもつこと。
- ✧　外国人の訪問に関係する全従業員に対して、当該国の脅威について説明すること。情報部に当該国の脅威評価を依頼すること。
- ✧　案内人及び訪問者との会合に加わる従業員両者に対して、訪問の範囲について事前に十分な情報を与えること。
- ✧　訪問者グループあたりの案内人の数は、訪問者の移動及び案内の管理に適切に対応できるものであること。

6　展示会、大会及びセミナー

これらの行事は、プログラムや技術とそれらに精通した人物を結び付けるものである。したがって、これらの行事は、外国の組織が後で利用することが可能な標的情報を提供するおそれがある。

6.1　指　標

- ✧　セミナーや大会において、秘密の情報又は輸出管理下の情報、及びそれら情報の利用の両者又はいずれかに係わる内容が話題となった。
- ✧　セミナーや大会の後援者となっている国又は組織は、過去、米国の施設訪問を試みたが失敗に終わったことがある。
- ✧　外国におけるブリーフィングや講演に全額外国側負担の招待状を受け取った。
- ✧　セミナーの 6 か月～12 か月前にプレゼンテーション要約の提出を求められた。
- ✧　写真撮影及び映画撮影が怪しいと思われる。

✧　出席者が偽造の名札を装着している。
✧　これら行事の間及び後で、思いがけない会話及び討論が行われた。

6.2　推奨するセキュリティ対策事項

✧　技術管理計画をもつこと。
✧　行事後に引き続く要求事項に注意すること。
✧　何の情報がどこで、誰に、いつ曝されるかをよく考えること。
✧　脅威､講ずべき事前対策､及び情報の引き出しにどのように対応すべきかについて、十分な旅行前ブリーフィングを従業員に対して実施すること。
✧　実際の装置の代わりに模型展示品を持参すること。
✧　プログラム室[6]による脅威評価を要求すること。
✧　情報の提供は、旅行/ホテル宿泊設備にさしあたり必要なものに限定すること。
✧　装置やソフトウェアが適切に保護されるか十分に検討すること。

7　インターネットの利用

インターネットの利用は、ハッキング、プローブ、スキャニング及びピニングから構成される。この区分は､インターネット・ベースの情報提供依頼に関連するものではないが、ほとんどの場合にプロービング活動が含まれている。システムのプロービングは、合法的なものではあるが、いったんポートにたどり着けば犯罪に着手したことになる。

7.1　指　標

✧　コンピュータ・プローブは､インターネット利用に際してシステムの脆弱性を探すのに十中八九利用される手口である。
✧　ネットワーク攻撃は､外国のインターネット・サービス・プロバイダーにその源を発している。
✧　攻撃が終日継続した。
✧　複数のパスワードの利用に数百回もの試みが行われた。

7.2　推奨セキュリティ対策事項

✧　技術管理計画をもつこと。
✧　ファイアウォール監視ソフトウェアを導入し､すべての侵入の試みやすべての悪意のある活動のログをとること。
✧　このような攻撃を撃退するため、適切なレベルの保護対策を講ずること。

---

[6] プログラム室：原文は“program office”であるが、国防保全局(DSS)の対情報活動(CI)組織に属し、脅威評価を担当する室と判断される。

✧　プローブに気づいた場合は、セキュリティ警戒態勢のレベルを上げること。

8　ジョイント・ベンチャー/研究

共同生産や様々な交換協定は、制限された技術を標的にする外国の関係者に重要な機会を提供する可能性がある。

8.1　指　標

✧　常駐している外国の代表者が：

- 大使館又は他の国に外国語で文書をファックスしている。
- ローカル・エリア・ネットワーク(LAN)へのアクセスを望んでいる。
- 施設への無制限アクセスを望んでいる。
- プロジェクト範囲外の情報を引き出すため、企業従業員を物色している。

✧　入札プロセスの一環として、米国の企業をそそのかして大量の技術データを提供させる。結局その契約は解除される。

✧　ジョイント・ベンチャー間の技術共有協定が、一方の当事者だけに有利となっている。

✧　外国の組織が、プロジェクトに必要以上の代表者を送り込む。

8.2　推奨セキュリティ対策事項

✧　技術管理計画をもつこと。

✧　ファックスや郵送されるすべての外国語の文書を翻訳させ、審査すること。

✧　外国の代表者にはネットワークに接続されていないコンピュータを提供すること。

✧　情報の共有は、ジョイント・ベンチャー/研究の範囲に適切で最小限なものに限定すること。

✧　プロジェクトの範囲と情報の引き出しへの対処及び報告要領について、従業員に詳しく教育すること。

✧　不必要な外国代表者の施設への受け入れを拒否すること。

9　海外出張をする米国企業従業員への標的行為

情報収集者の母国を訪問する米国の旅行者に対しては、当該国において利己的に利用される不審な活動発生の潜在的可能性があり、これには外国の情報機関(Foreign Intelligence Service: FIS)によるものが含まれている。一般的に、外国の情報機関は、国際大会に関与する米国の旅行者を共同軍事作戦やジョイント・ベンチャーを支援する者と認識しているのである。

9.1　指　標

- ✧　技術的手段（例えば、電子的監視）を利用する。
- ✧　ハニートラップ(色仕掛け)、闇市場、強要行為などのわなによる陰謀を利用する。
- ✧　同じホテルの同じ部屋に繰り返し滞在させる。
- ✧　ホテルのサービス係が幾度となく部屋を訪れる。
- ✧　過度の有益な支援を受ける。
- ✧　通関当局による不当な質問を受ける。

9.2　推奨セキュリティ対策事項

- ✧　技術管理計画をもつこと。
- ✧　保全施設適格証明書を有する企業は、提供する情報の種類や量を検討し、ホストから要求されたとしても本質的に不要な経歴データ、その他のデータを与えずにおくこと。

10　労働力の提供

外国の科学者、学生、エンジニアなどは、米国の研究施設、学術機関、そして保全施設適格証明書を有する企業にさえも、彼らのサービスを申し出ているのである。これは、所望の技術に係わる情報の収集のため、情報収集する者を米国内の施設内部に置くという手口(MO)の一つであろうと思われる。

10.1 指　標

- ✧　外国人の応募者は、ある技術分野の科学やエンジニアリングの経歴の持ち主であるが、彼の国はその分野について情報収集要求をしたことが明らかとなっている。
- ✧　外国人の応募者は、外国の政府機関、軍事組織体、大学又は企業が経費を負担することを明らかにし、「無償」でのサービス提供を申し出ている。
- ✧　外国人のインターン（修士又は博士課程で勉学している）が、たいていは２年～３年の間、科学技術分野などに精通した人物の下に無償で働くことを申し出る。
- ✧　一般的に外国人が働きたい又は研究を行いたいと望んでいる技術は、秘密の情報、国際武器取引規制(ITAR)、重要軍事技術(MCTL)又は輸出管理下にある情報に関連している。

10.2 推奨セキュリティ対策事項

- ✧　技術管理計画をもつこと。
- ✧　外国人の長期訪問者について、従業員に対する意識向上のブリーフィングを定期的に実施すること。

✧　外国人の仕事、研究及びインターンの募集にあたって、応募者の経歴及び推薦者をチェックすること。

✧　外国の関係者が係わるプログラムについては、プログラム室の脅威評価を求めること。

11　元従業員の引き込み

センシティブ情報、企業機密情報や科学技術(S&T)プログラム情報へのアクセス権を保有していた元従業員が、相変わらず対情報活動における潜在的な懸念事項となっている。文化的共通性に標的を定めて関係を築きあげようとする行為は、情報収集の企てに関連していると考えるが一般的である。元従業員は、収集活動の有望な候補者として見られている可能性があり、かつ、米国政府や元の会社のセキュリティ要求事項への遵守義務をほとんど感じていないと思われているのである。

11.1 指　標

✧　元従業員が、外国の会社で元の会社と同じ技術に係わる仕事をしている。

✧　元従業員が、元の会社やその従業員との接触を継続している。

✧　ある従業員は、米国の企業と外国の企業とを数年ごとに替えて働いている。

11.2 推奨セキュリティ対策事項

✧　技術管理計画をもつこと。

✧　元従業員が企業の施設に戻ってきた場合の警戒行動について、従業員に前もって十分な指示を与えておくこと。

✧　元従業員による現従業員への訪問や接触に関し、会社としてのポリシーをもつこと。

✧　雇用終了の従業員に対し、秘密の情報、企業機密情報及び輸出管理下の情報などを保護する法的責任に係わる遵守事項について十分な説明をすること。

12　文化的共通性を利用した標的行為

外国の組織は、企業の従業員、訪問者及び滞在者の文化的背景を利用して情報を引き出すのである。

12.1 指　標

✧　従業員が、大使館、外国の会社又は家族の祖国から一方的に送られた挨拶状、その他の通信文を受けとった。

✧　従業員が、家族の祖国から講演や受賞目的の訪問を望む招待状を受けとった。

✧　外国人の訪問者が、同じ文化的背景をもつ企業の従業員を選び出し、仲良く働くか

又は交際する。

12.2 推奨セキュリティ対策事項

- ✧ 技術管理計画をもつこと。
- ✧ 全従業員に対しこの手口(MO)を前もって十分説明するとともに、会社の報告ポリシーに記載すること。
- ✧ 外国人訪問者の活動を監視し、彼らが会社従業員を標的にする指標を明らかにすること。
- ✧ 潜在的な問題を極小化するため、不審な標的行為については可及的速やかに報告させること。

平成１８･１９年の発刊・平成２０年発刊予定資料

ＢＳＫ 第１８－１号 『米 国 の 国 家 対 情 報 戦 略』
ＢＳＫ 第１８－２号 『米大統領に対する 2004 年度秘密区分指定状況の報告』
ＢＳＫ 第１８－３号 『わが国をめぐる兵器技術情報管理の諸問題(平成 17 年度)』
ＢＳＫ 第１８－４号 『技術情報セキュリティの現状と動向(平成 17 年度)』
ＢＳＫ 第１８－５号 『秘 密 保 護 の 法 的 枠 組 み と 具 体 的 対 策』
ＢＳＫ 第１８－６号 『米国連邦政府省庁の情報セキュリティ管理策の評価手法と手順』
ＢＳＫ 第１８－７号 『ｾｷｭﾘﾃｨ･ｶﾞｲﾄﾞ(Sec に対する技術収集動向(2006 年)』urity Guide 2006)』 （保全講習受講企業用）
ＢＳＫ 第１８－８号 『合 衆 国 防 衛 関 連 企 業

ＢＳＫ 第１９－１号 『米連邦政府サイバー・セキュリティ研究開発の調整態勢』
ＢＳＫ 第１９－２号 『外国の経済情報収集及び産業スパイ活動に関するホワイトハウス年次報告(2005 年)』
ＢＳＫ 第１９－３号 『情 報 セ キ ュ リ テ ィ の 現 状 と 動 向(平 成 18 年 度)』
ＢＳＫ 第１９－４号 『米 国 に お け る イ ン サ イ ダ ー 脅 威 へ の 取 り 組 み』
ＢＳＫ 第１９－５号 『わが国をめぐる兵器技術情報管理の諸問題(平成 18 年度)』
ＢＳＫ 第１９－６号 『2006 年 米国の情報コミュニティ年次報告』『米国の国家対情報戦略(2007)』

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』(予定)
ＢＳＫ 第２０－３号 『わが国をめぐる兵器技術情報管理の諸問題(平成 19 年度)』(予定)
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)』(予定)
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)』(予定)
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)』(予定)
ＢＳＫ 第２０－７号～ 『未定(米国会計検査院年次報告、国家対情報局年次報告ほか)』

対 情 報 訓 練 資 料
(Ｃｏｕｎｔｅｒｉｎｔｅｌｌｉｇｅｎｃｅ)
(企業秘密を盗み出す手口とその対策)

平成２０年２月 発行
非 売 品 禁 無 断 転 載・複 製
発 行 者 ： 財団法人 防衛調達基盤整備協会
〒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