ＢＳＫ第２６－５号

海外出張する企業専門家のための安全とセキュリティについて

FBI Counterintelligence brochure（ＦＢＩ対情報啓発資料）

[Safety and Security for the Business Professional Traveling Abroad]

インサイダー脅威
―インサイダースパイを発見し、阻止するために―

FBI Counterintelligence brochure（ＦＢＩ対情報啓発資料）

[The Insider Threat An introduction to detecting and deterring an insider spy.]

平成２６年１０月

公益財団法人　防衛基盤整備協会

はしがき

本小冊子は、２０１４年８月現在で米国連邦捜査局（ＦＢＩ）が対情報活動のためにウェブ上で公表している９件の一般向けの啓発資料のうちの２件、”Safety and Security for the Business Professional Traveling Abroad”と”The Insider Threat An introduction to detecting and deterring an insider spy”を翻訳したものである。

前者を、「海外出張する企業専門家のための安全とセキュリティについて」と題して翻訳したが、ここでは外国の企業、外国政府又は外国の犯罪者が、米国のビジネスマンや研究者から、どのような手段で企業秘密や個人情報などを盗み出すかの手口を解説している。そして、旅行前に準備すべきこと、旅行中に行うべきこと、帰国後に行うべきことと、時系列的に分かり易く説明している。例えば旅行前の準備では、携帯用パソコン等からは、税関等で検査と称して内容がダウンロードされる可能性があるので、それが絶対に必要だという場合以外は記憶させないことや、記憶させる場合は暗号化ソフトを使用することを求めている。また、旅行中の注意としては、携帯電話は、たとえ電源を切っていてもハッキングされてマイクとして利用されることや、いくつかの国では、Wi-Fi は治安機関によって管理されているので安全ではないことなどを警告している。

また、後者を「インサイダー脅威―インサイダースパイを発見し、阻止するために―」と題して翻訳した。この中で、外部からの攻撃にはしばしば気づくことが出来るが、発見するのがより難しくまた最も大きな損害を引き起こすのは、インサイダーつまり正当なアクセス権を持つ従業員であることを警告している。そして、インサイダー脅威の生起・増大要因を説明し、次に脅威となっている人物の行動の特徴を解説し、インサイダー脅威への対応策を述べている。

我が国では、中小企業に至るまで海外への企業進出が一般的となる中、海外出張に伴い企業秘密の窃取等が行われる脅威があることは知られておらず、また、我が国においてもインサイダーによる情報漏えい事件は後を絶たず、更に外国籍の従業員の雇用が増えている中、外国人による企業秘密の窃取事件も生起している。

本小冊子は、海外旅行者や海外出張者をターゲットとする情報セキュリティ攻撃が増大している中、またインサイダーによる脅威が増大している中、企業や個人を守るために役立つものと思われます。本小冊子が我が国の情報セキュリティ体制の向上にいささかでも貢献できれば幸いです。

平成２６年１０月

公益財団法人　防衛基盤整備協会

理事長　宇田川　新一

目　　次

FBI Counterintelligence brochure　（ＦＢＩ対情報啓発資料）
[Safety and Security for the Business Professional Traveling Abroad]

「海外出張する企業専門家のための安全とセキュリティについて」

公益財団法人　防衛基盤整備協会　訳

「学術交流に参加したいという意欲が高い米国の科学者や学者ほど、ホテルの部屋や会議室に設置されている標準的な電子的監視装置の前でのみならず、巧妙な質問を投げかけるように訓練された外国人による単純なアプローチに対して、特に脆弱になってしまう。」
（外国の経済上の情報収集及び産業スパイに関する年次議会報告２００３）

１．　はじめに

あなた又はあなたの会社は、ある国が、自分たちのマーケットシェアを伸ばすためや、自国の経済を発展させるため、あるいは自国の軍隊を近代化するために必要な、情報や技術を獲得するための、標的になっているかもしれません。標的に対して使う手段には、手荷物検査、広範囲に渉る質問、携帯用パソコンからの情報のダウンロードや携帯用パソコンに対する不必要な検査などがあります。

出張者は米国外を旅行中、自分たち自身の安全とセキュリティだけではなく、自分のビジネス情報のセキュリティを確実にするための手段を講じなければならなりません。

２．　良いセキュリティ習慣は、あなたとあなたの会社を守る助けとなります。

企業スパイは、業務で出張中の旅行者にとって、ますます深刻な脅威となっています。犯人は、競争相手、たまたま出くわした者、あるいは外国のインテリジェンスオフィサーかもしれません。多くの国では、国内企業は自国政府の援助や支援を受けながら、競争のためのインテリジェンスを収集しています。このリスクを軽減するために、あなたの所属する組織のクリティカルな情報や技術は、それが絶対に必要だという場合以外は、いかなるハードコピーにも電子装置にも記録してはいけません。もしそうだとしても、暗号化機能を使い、しかもそれを常時携行し目を離さないことで、情報に対する物理的アクセスを保持しなければなりません。ホテルの金庫による保護は、適切ではありません。

３．クリティカルな企業情報としては、次のようなものがあります。
・顧客データ
・従業員データ

・下請け情報
・価格戦略
・企業資産である製造方法や工程
・技術の構成要素や図面
・企業戦略
・企業財務データ
・電話帳
・コンピュータ・アクセス・プロトコル
・コンピュータネットワーク設計図
・取得(購入)戦略
・マーケティング戦略
・投資データ
・交渉戦略
・パスワード(コンピュータ、電話、口座)

４.「旅行前」に行うべきこと

〇あなたが旅行しようと計画している地域におけるローカルな法律や習慣をよく知りなさい。あなたは現地の法律に従うことが求められています。そしてそれらには、服装の基準、写真撮影の制限、電話の制限、外出制限などが含まれます。

〇服装を考えなさい。そうすれば、現地の人の感情を害することがないばかりか、あなたに対する望まない注目を引くこともありません。米国人は金持ちだと思われており、スリやその他の犯罪のターゲットにされています。決して高価に見える宝石類を身に着けてはいけません、米国のチームスポーツのシャツを着たり、あなたが米国人であることを示すような野球帽はかぶってはいけません。

〇あなたが携行するパスポート、航空券、運転免許証、クレジットカードのコピーを作ってください。コピー１通を自宅に保存し、もう１通を原本とは異なるところにしまって携行してください。そうすれば、それらを落としたり盗まれたときに、再発行するプロセスをスピードアップするのに役立ちます。

〇必要でない身分証明書やクレジットカードは、持って行かないこと。それらは盗まれるかもしれないので、携行するのは、最小限にしてください。また、必要なら、トラベラーズチェックを用意してください。

○連絡先を確認してください。緊急時の家族の連絡先とホテルの連絡先です。また、国務省にあなたの旅行を登録してください。あなたが訪問する国にある米国大使館と領事館の電話番号と住所を入手してください。

○必要な薬を持参すること。薬は、フライトの間は、一時預けの手荷物ではなく、携行手荷物の中に入れて、元の包装のまま携行してください。適切な医療保険に入っていることも確認してください。

○特定の旅行前カントリーリスクの評価を入手してください。あなたが旅行しようと計画している国々に関して、あなたの会社のセキュリティ担当者、国務省、あるいはＦＢＩから入手してください。そこにはあなたが用心しなければならないことや準備しなければならない特定の事項が記述されているでしょう。そしてそれはあなたの安全と心の平安を約束してくれるでしょう。

○ウェブページ www.osac.gov を見てください。そこには、あなたが訪問しようと計画している国についてのセキュリティ上のニュースや報告があります。

○旅行前に、あなたの携帯用パソコン、携帯電話、ＰＤＡをきれいにしてください。つまり、それらに、機微な連絡先、研究成果、個人的なデータが入っていないことを確認してください。あなたが持って行くすべてのデータについてバックアップを取り、本国に残してください。もし可能なら、クリーンな携帯用パソコンと携帯電話及び旅行中に使う新しいＥメールアカウントを使ってください。あるいは、それらの装置を持って行かなくても済むならば、それらを持って行かないでください。

○携帯電話は、連絡先リスト(電話帳)、使用者名、パスワード、ブラウザー履歴を盗むために、ハッキングされます。

○アンチウィルス、スパイウェア、セキュリティパッチ、ファイアーウォールについて、最新の保護を使用してください。

○あなたのボイスメールを消去してください。あなたが自分のメッセージにアクセスするとき、パスワードが盗まれ、他人があなたのメッセージを調べるかもしれません。

５．「旅行中」に行うべきこと

〇あなたのパスポートを守ってください。米国人旅行者のパスポートの盗難は、増えています。パスポートは、ズボンの前ポケットか、服の中の見えないポーチに入れておくことを勧めます。しかも２４時間身に着けていてください。ホテルによっては、あなたの滞在中は、あなたのパスポートをフロントデスクに預けるように求めます。そして彼らは、あなたのことを地元の通常の警察に登録することでしょう。その場合、預かり証を受け取ってください。そして出発前に、確実に自分のパスポートを調べてください。もしパスポートを無くしたり盗まれたら、最寄りの米国大使館又は領事館に、速やかに状況を報告してください。

〇税関を通るときは、丁重で協力的にふるまってください。あなたの荷物を手元から離してはいけません。油断してはいけません。

〇公認タクシーを利用してください。あなたがジプシータクシーを利用すれば、過大請求されるか、強盗に遭うか、誘拐されるかもしれません。

〇あなたの部屋に知らない人を招き入れてはなりません。一人で旅行するのは避けてください。特に暗くなった後は、自分の周囲に気を配ってください。そして、自分の安全を脅かすと思われる場所は避けてください。露天商や無垢に見える若者にも用心してください。一人があなたの注意を引いている間に、もう一人がスリを働くかもしれません。

〇高額の現金を持ち歩かないでください。常に信頼できる両替所を利用してください。さもなければ、偽札をつかまされる危険を冒すことになります。

〇列車の寝台コンパートメントでの盗難に気をつけてください。ここで被害に遭うことは、よくあることです。

〇飲み物から目を離してはいけません。誰かが、記憶喪失や眠気を引き起こす薬を入れるかもしれません。

〇もし可能なら、ロビーや駅で長時間待つのは避けてください。これらの場所は、スリ、盗人、暴力的犯罪者のたまり場かもしれません。特に、携帯用パソコンの盗難は、空港でよくあることです。

〇空港での盗人は、セキュリティチェックポイントで、あなたの前に並んでいるかもしれません。あなたがＸ線装置のベルトコンベアに携帯用パソコンを乗せた後、二人目の盗人が金属探知機に引っかかり、通過を遅らせます。その間に、最初の盗人が、Ｘ線装置を通過してきたあなたの携帯用パソコンを盗みます。

〇もしあなたが逮捕されたら、それがいかなる理由であろうとも、最寄りの米国大使館又は領事館に通知するよう頼んでください。

〇あなたのことをかぎまわる新しい知人や、あなたが困る状況に巻き込まれるように企てる新しい知人には用心してください。

〇暴動や騒乱を避け、現地の法律に従ってください。もしデモや集会に出くわしたら、注意深くしてください。混乱の中では、たとえあなたが、見物人であったとしても、あなたは逮捕されるか拘留されるかもしれません。多くの国では、政府やその指導者を軽蔑して話すことは、禁止されていることを、心にとどめておいてください。列車の駅、政府庁舎、宗教上のシンボル、軍事施設の写真を撮影するのは、違法行為かもしれません。

〇いかなる違法な、不適切な、又は軽率な行動も避けてください。性交渉の申し出は避けてください。それは部屋への踏み込み、写真撮影、脅迫へとつながるかもしれません。つきあいで飲むときに、ホストに追いつこうとはしないでください。闇取引に参加してはいけません。あなたの所持品を売ってはいけません。違法なドラッグやポルノを持ち込んでも購入してもいけなせん。政治的あるいは宗教上の反対者を、探し出してはいけません。他の土地へ配達する小包や手紙を頼まれてはいけません。

〇あるアメリカ人は、見知らぬ男から手紙を渡されました。アメリカ人はそれを返そうとしましたが、男は走り去ってしまいました。その夜そのアメリカ人は、国家保安機関の官憲の来訪を受け、手紙を受け取ったことに対して警告されました。

〇目立たないように心掛け、知名度が上がることを避けなさい。地元のニュースメディアに自分の個人的なことやビジネスに関することは話さないようにしてください。外国人とどんな情報を自分が共有しようとしているかについて、注意深く考えてください。彼らは、あなたとあなたの会社につけ込むために、あなたから情報を入手するよう指示されているかもしれません。丁寧に話題を変えてください。相手が人をだまして情報を聞き出そうとしていることをどうやって気づくかにつて

は、ＦＢＩは助言することができます。

〇あなたの周囲に気を配ることで、犯罪者やテロリストを避けてください。そして自分が監視されている可能性について敏感でいてください。誰であれあなたを尾行する人間がいたら、それを覚えて、すぐに適切な官憲及び／又は米国大使館あるいは領事館に報告してください。一般的に犯罪者は、彼らのターゲットが気を緩めた時に襲ってきます。もし誰かがあなたをつかんだら、大騒ぎしなさい。つまり、大声で叫び、蹴って、逃げなさい。もしあなたが誘拐されたら、警戒を続け、自分自身のための精神的及び肉体的プログラムを確立しなさい。つまり、平静を保ち、怯えないように心掛けてください。

〇あなた自身やアメリカ人の同僚の性格の欠点、財政的問題、恋愛関係、その他の困った問題についての噂話をしないでください。これらの情報こそ、あなたとあなたの同行者につけ込もうと考えている者にとって、最も欲しがっている情報です。

〇あなた方の会話は、内輪のものでもなく、安全なものでもないことに、用心してください。米国とは違って、ほとんどの国においては、技術的な監視について、法的制限がありません。ほとんどの外国の治安機関は、インテリジェンスの観点から潜在的な価値を持つ人間を特定するために、旅行者を選別するための様々な手段を持っています。そして彼らはまた、あなたを監視するために様々な形で協力してくれるホテルや支配人達と良好な関係を持っています。盗聴器は、航空機の座席、ホテルの部屋、タクシー、及び会議室で、よく発見されています。

〇民間企業及び政府機関の出張者は、滞在する部屋番号を報告され、所持品は調べられています。

〇電子装置を手元から離してはいけません。それら(あるいはその他の高価なもの)を、一時預かりの手荷物として輸送してはいけません。パスワードは見えないように隠してください。可能なら、Wi-Fi ネットワークは避けてください。いくつかの国においては、それらのネットワークは、治安機関によって管理されています。つまり、いかなる場合においても、それらのネットワークは安全ではありません。

〇使用のたびごとに、あなたのインターネットブラウザをクリアにしてください。つまり、履歴ファイル、キャッシュ、クッキー、インターネットの一時ファイルを消去してください。

○もしあなたの携帯電話や携帯用パソコンが盗まれたら、速やかに地元の米国大使館又は領事館に報告してください。

○あなたの会社のネットワークにログインするために、会社から支給されたコンピュータではないコンピュータを使ってはいけません。たとえ暗号化されていようとも、会社から支給されたのではないコンピュータを経由した情報は、危険にさらされることを、常に考えてください。

○膨大な国々のサイバー犯罪者たちは、クレジットカードデータやログイン信用証明書(ユーザー氏名およびパスワード)を含む盗まれた財政情報を売買しています。

○あなたのコンピュータや携帯電話に、外国の電子的記憶媒体の接続を許してはいけません。それらの装置にはマルウェアが入っているかもしれませんし、それらはあなたの電子的データを自動的にコピーするかもしれません。あなたに渡されたＵＳＢメモリーを使ってはいけません。それらにはマルウェアが仕込まれているかもしれません。

○あなたは、ほとんどの国のインターネットカフェ、ホテル、空港、事務所、あるいは公共の場所で、プライバシーを期待することは出来ません。あなたが電子的に送るすべての情報、特に無線通信されたものは、傍受されます。もし、情報が外国政府、他の企業、あるいはグループにとって価値がある場合は、その情報は傍受されその手に落ちると推測すべきです。治安機関と犯罪者たちは、あなたの携帯電話を利用して、あなたの動きを追跡することもできますし、あなたが自分の電子装置のスイッチを切っていると思っているときであっても、マイクのスイッチを入れることができます。

○北京オリンピックの期間中、ホテル宿泊客のインターネット活動を法執行機関が監視することができるようなソフトウェアをインストールすることが、ホテルに求められました。

○「フィッシング」に注意しなければなりません。外国の治安機関や犯罪者たちは、あなたの個人情報又はセンシティブな情報を入手する目的で、あなたが信頼している誰かを装うことに熟達しています。

６.「帰国後」に行うべきこと

〇あなたの会社の情報セキュリティ担当者と一緒に、あなたのシステムアクセスを調べ直してください。説明のつかないアクセスは、調査されなければなりません。

〇あなたの帰国後に、外国人が、あなたにコンタクトしてくるのは一般的ではありません。ＦＢＩは、これらのコンタクトがあなたやあなたの会社にいかなる危険をもたらすかを、見極めるお手伝いができるかもしれません。

〇あなたのボイスメールを含むすべてのパスワードを変更してください。そして電子装置のマルウェアをチェックしてください。

〇旅行中に、何か通常ではない出来事や著しいインシデントがあった場合は、あなたの会社のセキュリティ担当者とＦＢＩに報告してください。ＦＢＩへの届け出は、将来の旅行に関する助言が、あなたの経験した出来事やインシデントを反映させたものとなる助けとなります。

〇追加の旅行の安全に関する助言及びカントリー脅威評価は、要請次第で、ＦＢＩで提供可能です。

(以上)

FBI Counterintelligence brochure （ＦＢＩ対情報啓発資料）
[The Insider Threat An introduction to detecting and deterring an insider spy.]

「インサイダー脅威

―インサイダースパイを発見し、阻止するために―」

公益財団法人　防衛基盤整備協会　訳

１．はじめに

この資料は、管理者やセキュリティ担当者が、インサイダー脅威をどう検知するかの導入として、またどのようにあなたの会社の営業秘密を守るかのヒントを与えるものです。

会社は、部外者（非従業員）が、物理的にあるいは電子的に会社のデータにアクセスを試みるときには、しばしばそのことを検知しコントロールすることができます。そして部外者が会社の資産を盗もうとする脅威を軽減することができます。

しかしながら、発見するのがより難しくまた最も大きな損害を引き起こすのは、インサイダーつまり、正当なアクセス権を持つ従業員です。そのインサイダーは、個人的利益のためだけに盗むかもしれませんし、また他の組織や他の国の利益のために会社の情報や製品を盗むスパイかもしれません。

２．あなたの会社の知的財産を保護するために

知的財産の窃盗は、組織にとってますます脅威となっており、窃盗されてもそのことに数か月もあるいは数年も気づくことができません。

従業員が企業の専有情報を盗む事案は増加しており、彼らが、将来職探しをしなければならなくなると思った時、または職探しをしているときに、事案が発生しています。

合衆国議会は、発明を保護し、悪質又は継続的な知的財産権の侵害が、経営上の単なる標準原価（侵害による損害額をあたかも避けられない出費として捉えること[訳者注]）となることがないことを保証するために、知的財産権の侵害に対する刑法を拡張しまた強化してきました。

ある企業の専有情報や営業秘密を非合法に入手しようと企んでいる、国内のあるいは外国の競争企業もしくは外国政府は、非公開情報に対するアクセス権を手に入れるために、その企業にスパイを入社させたいと思っているでしょう。また

彼らは、その代わりに、同様のことを行わせるために、現在の従業員を取り込もうと試みるかもしれません。

３．インサイダー脅威の生起・増大要因

(1) 個人的要因

従業員の誰かが、雇用主に対してスパイになってしまう可能性を増加させる個人的な状況や動機には様々なものがあります。

・欲深さ又は経済的必要性：お金で何でも解決できるという思い込み。
過大な負債又は浪費癖。
・怒り／復讐：組織に復習したいと思っている点についての不満。
・仕事上の問題：功労に対する評価の欠如。
同僚やマネージャーとの不仲。
職務に対する不満。
解雇予定。
・イデオロギー／アイデンティティー：弱者を助けたいとの強い願望又は特別の理由
・引き裂かれた忠誠心：他の者や他の会社または合衆国以外の国への忠誠心
・冒険／スリル：生活への刺激を求める。
秘密の行為に好奇心をそそられる。
ジェームス・ボンド気取り。
・脅迫への脆弱性：不倫。
ギャンブル。
不正。
・エゴ／自己イメージ：規則を超越する態度。
自尊心が傷ついた時に修復したいとの願望。
お世辞やより良い仕事の約束に弱い。
しばしば、怒り／復讐あるいは冒険／スリルと連動。
・へつらい：見返りを期待しながら、インサイダー情報から利益を得ることのできる人物に一目置かれたいとか、喜ばせたいという願望。
・やむにやまれぬ破壊的な態度：薬物あるいはアルコール乱用あるいはその他の習慣性の行動。
・家庭問題：夫婦喧嘩あるいは愛する人との離別。

(2) 組織的な要因

組織の状況によっては、窃盗の容易さが増大する場合があります。

・企業の専有情報、秘密又は保護されている資料を入手することが可能であった

り、それが容易であったり、必要としない者へアクセス特権が付与されているかもしれません。
・企業の専有情報や秘密情報がそのように表示されていなかったり、正しく表示されていないかもしれません。
・企業の専有情報、秘密または他の保護資料を持って施設（あるいはネットワーク）を出ることが容易かもしれません。
・機微なあるいは企業専有の性質のあるプロジェクトに関して、自宅で作業することについてのポリシーが策定されていないかもしれません。
・セキュリティが緩いあるいは盗まれることの影響がほとんどないという認識があるかもしれません。
・時間的な圧力：急がされた従業員は、企業の専有情報や保護資産を適切に保護しなかったり、自分の行動の結果を十分に考えないかもしれません。
・従業員が、どのように適切に企業の専有情報を保護するか訓練されていないかもしれません。

４．インサイダー脅威への対応

(1) 行動の特徴

いくつかの行動は、従業員がスパイを行っているそして／又は組織から系統的に窃盗を行っていることの手掛かりとなる可能性があります。

・必要性や権限もなく、文書やＵＳＢメモリやコンピュータディスクやｅメールを経由して、企業の専有情報や資料を自宅に持ち帰る。
・職務に関係のないテーマの企業の専有情報又は秘密情報を不適切に探している。又は所持している。
・職務の範囲を超えた事柄に関心を持つ。特に外国企業や競争相手に対する関心がある。
・不必要に資料をコピーする。特にそれが企業の専有情報や秘密であればなおさらである。
・休暇中や病休中に、コンピュータネットワークにリモートアクセスする。あるいはそれが異常な回数である。
・個人的なソフトウェア又はハードウェアをインストールしたり、制限されているウェブサイトにアクセスしたり、無許可の検索を実行したり、秘密情報をダウンロードするなど、会社のコンピュータポリシーを無視する。
・許可なしに異常な時間数にわたって働く。つまり、残業をとてもしたがったり、週末に出勤したがったり、通常でないスケジュールで働きたがる。これらは、不法行為を最も実行しやすい時間帯である。
・報告なしで外国人（特に外国政府職員や情報機関職員）と接触したり、報告な

しで海外旅行を行う。
・説明なしのあるいは奇妙な理由による短期の外国旅行を行う。
・説明のつかない資産：家計収入では購入不可能な物品を購入する。
・競争相手方あるいはビジネスパートナーあるいは他の許可されていない個人といった疑わしい人物との個人的接触を行う。
・生命の危機あるいはキャリア上の失望による苦しみを味わっている。
・同僚の個人的生活に異常な関心を持つ：経済状態や恋愛関係についての踏み込んだ質問をする。
・自分が調査されているのではないかと心配している：職場や自宅が捜索されているかどうかを発見するために、髪の毛やひもなどを置いて点検する。：盗聴器やカメラを探す。

多くの人々は、上述のうちのいくつかあるいはすべてを程度の差はあれ、経験したり行っています。しかしほとんどの人々は、一線を越えることはありませんし、犯罪を犯すこともありません。

(2) 差がつく方策

組織は、知的財産窃盗を防ぐために、やるべきことがあります。

・セキュリティやその他の手順について、従業員を教育し、定期的に訓練してください。
・堅固とまでは言わなくても、企業の専有情報が適切に保護されていることを確実に確認してください。
・新しい従業員を採用するにあたって、適切な選別プロセスを用いてください。
・従業員に、疑わしい者を報告させるための手軽で恐れを感じない方法を提供してください。
・疑わしい行動を見つけるために、常日頃からコンピュータネットワークを監視してください。
・セキュリティ（コンピュータセキュリティを含む）担当者に必要な手段を確実に与えてください。

セキュリティ上の懸念について報告することは、会社の知的財産、会社の評判、会社の健全な財政状況、及び会社の将来を守り、致命的な事態を防ぐために重要なものであることを従業員に徹底してください。そうすれば従業員は自分の仕事として報告するようになります。従業員が何かを見たらそれを報告すべきだと従業員に徹底すべきです。

(3) 支援を受けること

潜在的な問題に気が付くこと、良い判断を行うこと、複数の別々の調査を行うことは、内部にスパイがいるかどうかをあなたが突き止めるのに役立ちます。しかしながら、もしあなたが従業員の一人がスパイであるまたは会社の営業秘密を盗んでいると睨んだならば、その人物が疑われていることを警告することなく、ＦＢＩのような訓練を受けた対情報活動の専門家の支援を求めてください。ＦＢＩは、そのような脅威を突き止めたり減らすための器材と経験を持っています。ＦＢＩは、調査依頼があれば、あなたのビジネスへの悪影響を最小化し、あなたのプライバシーとデータを守ります。ＦＢＩは、必要な場合、営業秘密や企業秘密を保護するために、保護命令を請求します。ＦＢＩは米国企業の秘密と競争力を維持することに努めています。ＦＢＩはまた、求めに応じて、あなたとあなたの従業員に対して、セキュリティと対情報活動の訓練あるいは啓発セミナーを提供します。

５．最近のインサイダーによる情報窃盗事件

(1) 刘　文 树　（リュウ・ウェンチュウ）

引退した科学研究者である彼は、２０１２年１月に、５年の懲役、２年の保護観察、２万５０００ドルの罰金と６０万ドルの没収を言い渡された。刘は、元の雇用主から営業秘密を盗み、それを中国の会社に売却した罪で、２０１１年２月に有罪となった。刘は、少なくとも４人の現従業員及び元従業員と共謀して、盗んだ情報を売るために中国全土を旅行し、物件と情報の見返りに現職と元従業員に金を支払い、プロセスマニュアルと他の情報を提供するよう当時の従業員を５万ドルで買収した。

(2) 黄 科 学（ホアン・ケキュ）

彼は別々の２つの米国企業に雇われていた。彼は、２００７年から２０１０年にかけて、両方の企業から盗まれた営業秘密を、ドイツと中国の個人に提供したことを認めた。盗まれた物件は、中国の大学に利益をもたらす不正な研究を行うために利用された。また黄は、中国で営業秘密を開発し生産することを追求した。両社の合計損失は、７００万ドルから２０００万ドルの間である。黄は、経済スパイと営業秘密の窃盗の罪を認め、２０１１年１２月に、７年３か月の懲役と３年の保護観察処分を言い渡された。

(3) 李　苑（リ・ユアン）

世界的な製薬会社で働いていた元化学研究者は、２０１２年１月に、彼女の雇用者から営業秘密を盗み、アビー・ファーマテック社を通じて販売可能なように

それを加工した罪を認めた。李はアビー社の５０％出資者であった。２００８年１０月から２０１１年6月までの間、李は彼女の勤務先の部内データベースにアクセスし、情報を彼女の自宅コンピュータにダウンロードして、アビー社を通じて販売するよう加工した。彼女は、１年６か月の懲役刑を言い渡された。

(4) エリオット・ドクサー

彼は、イスラエル領事館宛にｅメールを送り、イスラエルに役立つであろう情報を自分の勤務先の会社から喜んで持ち出すつもりであることを伝えた。イスラエルの情報オフィサーに扮したＦＢＩのおとり捜査官が、ドクサーと接触して、二人が情報を交換する場所（「デッドドロップ」）を決めた。その後１年半に、ドクサーはデッドドロップを少なくとも６２回訪れた。ドクサーは、顧客リスト、従業員リスト、契約情報、及びその他の営業秘密を提供した。彼は、１件とみなされる外国経済スパイ罪を認め、２０１１年１２月に6か月の懲役、6か月の自宅監禁、及び2万５０００ドルの罰金を言い渡された。

(5) セルゲイ・アレイニコフ

彼は、ウォール・ストリートにある会社でコンピュータプログラマとして働いていた。その会社に勤務していた最後の数日間の間に、彼は３２メガバイトものその会社が知的財産権を有するコンピュータ・コードを転送したが、それは会社に数百万ドルの被害を与える窃盗であった。彼は自分の行動を隠そうとしたが、会社は日常のネットワーク監視システムから異状に気が付いた。２０１０年１２月に営業秘密窃盗が発覚した。

(6) マイケル・ミッチェル

彼は会社に不満を持っており、勤務成績不良で解雇された。しかし彼は、会社の営業秘密を含む膨大なファイルを持っており、韓国のライバル企業とコンサルティング契約を結び、盗んだ営業秘密を渡した。２０１０年3月、彼は1年6か月の懲役刑と元雇用主である会社に１８万７０００ドル以上支払うように命じられた。

(7) シャリン・ジャーベリ

彼は、インドのベンチャー企業に融資したがっている投資家と信じていた人物に、営業秘密を渡した。そして会社から盗んできた情報が、自分が会社を興すのに必要なものであることを念押ししていた。２０１１年1月に、未決拘留（1年１５日）、保護観察3年、罰金５０００ドル、及び１００ドルの特別課税が言い渡された。

(8) 金韩娟（ジン・ハンジャン）

彼女は、２００６年に自分の勤める米国企業から長期休暇を取った。休暇期間中に金は、中国で、同業の企業で働いた。１年後、金は米国に戻ってきた。彼女は帰国１週間以内に、中国への片道切符を購入し、会社に対して長期休暇を終了する用意ができたことを伝えた。金は、２００７年２月に職場に復帰し、最初の二日間で数百件の技術資料をダウンロードした。２００７年２月２８日に、空港での通常の検査の際に、金の荷物から１０００件以上に及ぶ電子的又は紙ベースの、彼女の雇用主である会社の専有情報の文書が発見された。２０１２年に４年の懲役と２万ドルの罰金が言い渡された。

(9) 鐘东 蕃（チュン・ドンファ）

彼は、１９７９年から２００６年の間、中国のためにスパイを働いた。鐘は、スペースシャトル、デルタⅣロケット、Ｃ－１７軍用輸送機に関する営業秘密を中国政府のために盗んだ。鐘の動機は、母国のために貢献するということであった。鐘は、数十万点の文書を自分の勤める会社から盗んだ。彼は、中国のエージェントと秘密に面会するために、講義を行うためと見せかけて中国へ旅行した。彼は、中国へ情報を送るために、次に述べる麥も使った。２０１０年２月、懲役１５年以上を宣告された。

(10) 麥 大 志（マク・チ）

彼は、米国の軍事秘密を盗む目的を持って、米国の軍事産業に就職するために１９７８年に米国に送り込まれ、それを２０年以上にわたり行っていたことを認めた。彼は、米国潜水艦の静音電気推進システム、イージスレーダーシステムの詳細、米海軍で開発中のステルス艦に関する情報を、中国に流した。中国政府は、麥に、他の軍事技術の情報も入手するよう命じた。麥は、情報を暗号化したり、中国にこっそりと情報を手持ちで持ち込むために、一族の中から協力者をリクルートした。２００７年３月、麥は、外国政府のエージェントであることの登録を怠ったこと及び、共謀罪並びにその他の違反で有罪を宣告された。彼は２４年以上の懲役刑を言い渡された。

訳者より：読者に分かり易いよう、原典に無い一部の表題を付けたり、項目番号を付与しました。

平成２６年発刊資料

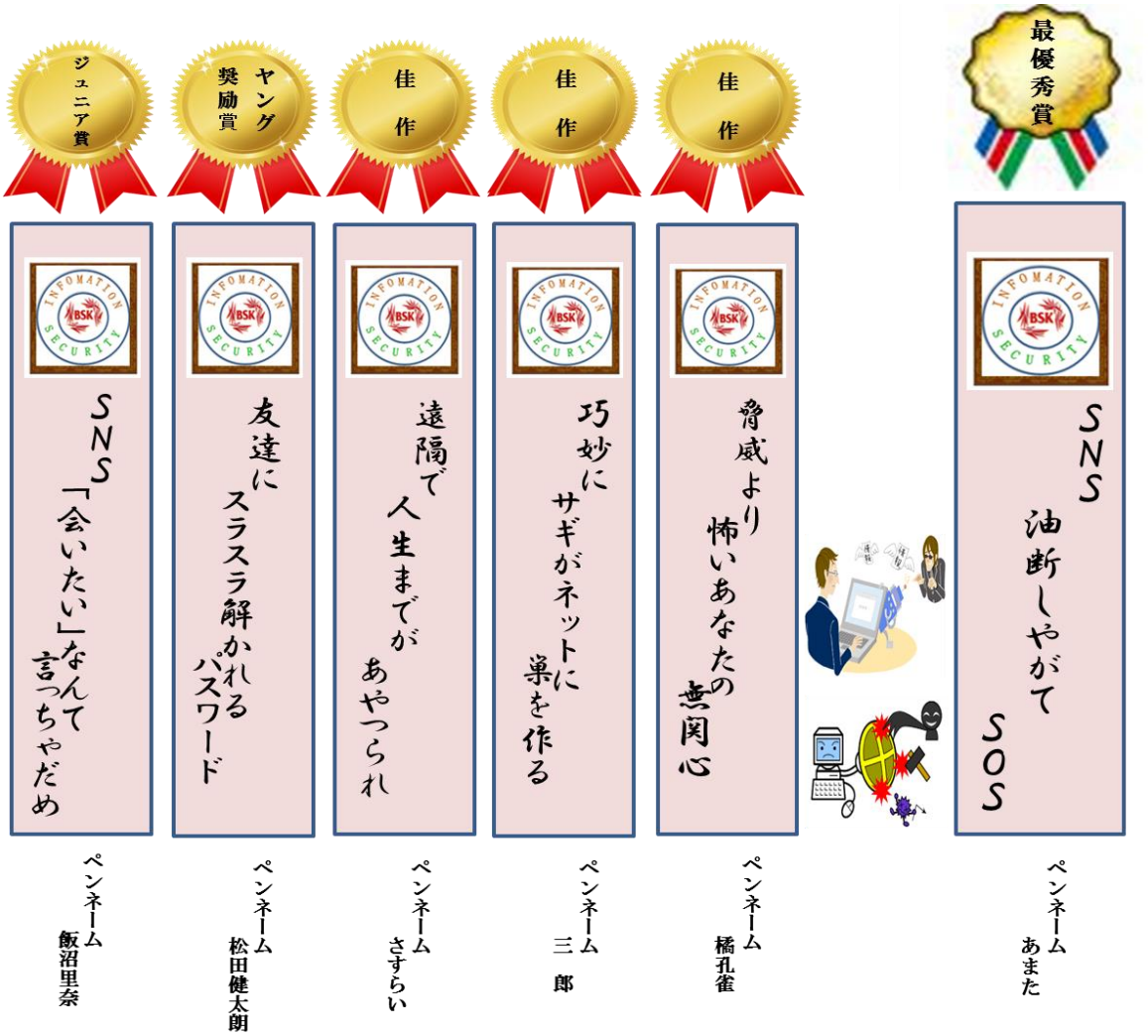
ＢＳＫ 第２６－　３号『情報セキュリティの現状と動向について（平成２５年度）』
ＢＳＫ 第２６－　４号『外国においても活用可能な、米国におけるインサイダー脅威に対する最善の対応策』（平成２５年度）

本報告書の中で意見にわたるものは、委託研究先の見解であることをお断りしておきます。

海外出張する企業専門家のための安全とセキュリティについて
インサイダー脅威
―インサイダースパイを発見し、阻止するために―

平成２６年１０月　発行
非　売　品　　禁 無 断 転 載・複 製
発　　行　：　公益財団法人　防衛基盤整備協会
編　　集　：　防衛基盤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　：　koueki@bsk-z.or.jp
ＢＳＫホームページ：　https://www.bsk-z.or.jp

平成26年度情報セキュリティ川柳入選作品



主催　公益財団法人　防衛基盤整備協会