ＢＳＫ第２９－４号

誘 導 質 問

「ＥＬＩＣＩＴＡＴＩＯＮ」

知的財産保護

「Ｉｎｔｅｌｌｅｃｔｕａｌ Ｐｒｏｐｅｒｔｙ Ｐｒｏｔｅｃｔｉｏｎ」

Ｕ．Ｓ．Ｄｅｐａｒｔｍｅｎｔ ｏｆ Ｊｕｓｔｉｃｅ
Ｆｅｄｅｒａｌ Ｂｕｒｅａｕ ｏｆ Ｉｎｖｅｓｔｉｇａｔｉｏｎ
（米国司法省　連邦捜査局）

平成２９年８月

公益財団法人　防衛基盤整備協会

はしがき

本小冊子は、２０１６年７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一般向けの啓発資料のうちの２件、「Elicitation」と「Intellectual Property Protection」を翻訳したものです。

前者は**「誘導質問」**と題して翻訳しましたが、産業スパイや海外の諜報員が、企業からどのようにして重要な情報を引き出すのか、特定の情報が探されているという疑いが上がることなく、情報を引き出す方法について記述されており、様々な誘導質問の手法とその脅威を理解することによって、産業スパイや諜報員の誘導質問に気付き、情報を引き出される危機を回避し、情報漏洩防止の一助になるものと思われます。

後者は**「知的財産保護」**と題して翻訳しましたが、企業からどのような方法で知的財産を盗み出すのか、また、その兆候について警告しており、企業の知的財産を保護するための一助になるものと思われます。

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２９年８月

公益財団法人　防衛基盤整備協会

理事長　鎌田　昭良

目　次

Ⅰ. 誘導質問

Ⅱ. 知的財産保護

U. S. Department of Justice
Federal Bureau of Investigation
（米国司法省　連邦捜査局）

「ELICITATION」
「誘　導　質　問」

公益財団法人　防衛基盤整備協会　訳

１．誘導質問

誘導質問は、目立たないように情報を収集するための手法です。特定の情報を狙っていることに気付かれることなく、簡単には入手できない情報を収集するための会話技術です。この手法は、押しつけ的ではなく、簡単に偽装や否定が可能な効果的な手法です。

この手法は差し向かいの対話だけでなく、電話経由や書面などにも応用できます。

熟練した攻撃者による誘導質問は、普通の会話や業務上の会話のように見えます。攻撃の対象者は、自分が標的になっていること、もしくは自分が価値のある情報を提供したことにまったく気付きません。

多くの産業スパイや海外の諜報員は、誘導質問技術の訓練を受けています。彼らの仕事は、非公開情報を入手することです。競合する会社は競争で勝ち抜くために情報を求め、海外の諜報員は米国の防衛技術に関する情報を狙っています。

２．誘導質問の定義

尋問されているような印象を与えることなく、情報を引き出すための会話の戦略的利用

誘導質問は、単純かつあからさまに実施されることもあります。そのような誘導質問には簡単に気付き、回避することも可能です。その一方、独創的な方法で、持続的かつ綿密な計画の下に行われ、時には共謀者を雇って行われるような場合もあります。質問者は、会話の話題や質問の理由のつじつまを合わせるために、作り話をするかもしれません。

誘導質問者は、攻撃の準備段階で、攻撃対象者やその同僚の情報を集めることもあります。

誘導質問は、社交の場面、カンファレンス、電話、街中、インターネット、誰かの家など、ありとあらゆるところで実施される可能性があります。

３．誘導質問は珍しいことではない

意図を知られず、情報を引き出すことは珍しいことではありません。サプライズパーティを開くために、本人に気付かれることなく、スケジュール、欲しいもの、食べ物の

嗜好などの情報を集めたことはありますよね？誘導質問と気づかないために質問を回避できず、提供すべきでない価値ある情報を、熟練した誘導質問者が聞き出そうとした場合には問題となります。

４．なぜ誘導質問は有効なのか？

訓練された誘導質問者は、人や文化の特質を理解しており、それを悪用する技術を持ち合わせています。悪用される特質には、次のようなものがあります。

（１）たとえ赤の他人や最近の知り合いに対しても、礼儀正しく協力的でありたい傾向
（２）特に自分の専門分野には、精通しているように見せたい傾向
（３）感謝されていると感じ、なにか重要なことに貢献していると思いたい傾向
（４）賞賛や奨励を受けた場合に、話を誇張し見せびらかす傾向
（５）ゴシップを好む傾向
（６）人の間違いを正そうとする傾向
（７）情報がどのように利用されるかを知らない場合、相手が詮索している情報、与えてしまった情報の価値を低く評価する傾向
（８）人が正直だと信じ、人を疑うことを好まない傾向
（９）「正直」な質問をしたときに、正直に答える傾向
（10）誰かと意見を交換したい傾向

例えば、公共の場で誰か（攻撃者）と会い、自然に「相手と知り合う」ような会話の中で、質問が仕事に関連する内容に変わります。所属している組織の名称には一切触れません。別の人（攻撃者）が、自身の仕事への不満を話しながら、今度は会社の仕事の満足度について質問します。あなたは自分が何処で働き、どんな仕事をしているのか、彼は知らないだろうと思い、ただ、ちょっとした雑談をしているだけで害はないだろうと考えるかもしれません。

しかしながら、匿名性や、正直かつ博識のある人だと思われたいという性質、「情報を悪用される」とは疑わない人間の自然な特徴に付け込んで、必要な情報を得ているかもしれません。また、この自然な会話だけで、不満のある社員を見つけだし、インサイダー情報の提供候補者を、見定めることができてしまうかもしれません。

５．手法

誘導質問には様々な手法が存在し、実際には複数の手法を組み合わせて利用します。手法として次のようなものがあります。

（１）知識を装う（Assumed Knowledge）：知識を持っている、もしくは知識を持つ人と知り合いだと装う。「以前、一緒に働いていたネットワーク専門の人によれば...」

（2）ブラケッティング（Bracketing）：より具体的な数値を聞きだすために、高低の推定値を示す。「もうすぐ利率を上げると仮定すると、5 ドルから１５ドルの間だと予想します。」応答「おそらく 7 ドルぐらいでしょう。」

（3）これを超えられる？（Can you top this?）：超えることを期待しつつ極端な話を持ち出す。「M 社で～が可能なすごい製品を開発中と聞きました。」

（4）秘密の餌（Confidential Bait）：見返りに機密情報を受け取ることを期待して、機密情報を漏らす振りをする。「ここだけの話なんだけど...」「オフレコの話だけど...」

（5）批判（Criticism）：反論の中で機密情報を話してくれることを期待して、個人や組織を批判する。「どんな手を使ってその仕事を受注したんですか？B 社のエンジニアの方が、その種の仕事を得意としていることは周知の事実なのに」

（6）故意な偽の情報と自明の否定(Deliberate False Statements / Denial of the Obvious)：正しい情報で訂正されることを期待しつつ、間違った主張をして相手に訂正させる。「そのプロセスがうまく機能しないことは誰でも知っていますよ。それは DARPA（国防省国防高等研究計画局）の夢物語で、そのプロジェクトが開始されることはないでしょう。」

（7）無知を装う(Feigned Ignorance)：その分野について詳しくないことを装い、正しいことを教えてあげようとする人間の特徴を悪用すること。「私はこの分野では新米で、助けて欲しいんですよ。これは、どのように動くのでしょうか？」

（8）お世辞（Flattery）：情報を提供する人を丸め込むために褒め言葉を使う。「あなたは、この新製品を設計する上で鍵となる人物であったに違いありませんね。」

（9）よい聞き手（Good Listener）：忍耐強く耳を傾け、その人の感情（肯定的であれ否定的であれ）の妥当性を検証することによって、不平を言う、または自慢する本能を利用する。信用に値すると思われれば、より多くの情報を共有してくれる。

(10) 質問を誘導する (The Leading Question)：少なくてもひとつの前提を含んだ、YES/NO で答えられる質問をする方法。「前の仕事を辞める前、統合テストに関する仕事をしていたことがありますか？(真意：「あなたは前の職場では何を担当していましたか？」)

(11) マクロからミクロ（Macro to Micro）：マクロなレベルから会話を開始し、徐々に実際に興味があるトピックに対して会話を誘導していくこと。最初に経済のことから会話を始め、政府の支出、国防予算の削減に話を移し、その後「予算削減があった場合、X プロジェクトにはどんな影響があるんでしょうか？」などと話を進めていく。優れた誘導質問者は、情報を聞きだした後、逆のプロセスをたどり、会話をマクロな話題に再度誘導する。

(12) 共通の話題（Mutual Interest）：趣味・経験など共通の興味があることを利用して親密性をアピールして、情報の引き出しまたは情報を引き出すためのラポール（心理学用語：主として二人の間にある相互信頼の関係）を形成すること。「あなたのお兄さ

んは、イラク戦争に参加したんですか？私もそうでした。どの部隊に所属していましたか？」

（13）遠まわしの言及（Oblique Reference）：別のトピックへの推察を与えるようなトピックを議論します。例えば、パーティのケータリングに関する質問は、実は部外の業者がアクセスする方法を知る手段である場合があります。

（14）見せかけの反対・不信感（Opposition/Feigned Incredulity）：反論や不信感を表明することによって、立場を守るために追加の情報の提供を期待する。「そんなスピードで設計し製造できるはずがありません。」「理論的にはいい方法だが、しかし...」

（15）挑発的な表明（Provocative Statement）：続く会話を誘導するために、質問が自分へ向くように誘導すること。「仕事のオファーを受けなかったことに後悔しているよ。」応答「なんで受けなかったのよ？」ほかの人が質問することになるので、続く会話の中であなたの立場が、より無害となる。

（16）アンケートや調査（Questionnaires and Surveys）：アンケートのための無害な目的を述べる。目的に沿った質問の中へ、自分が本当に知りたい質問をいくつか混ぜる。もしくは、会話を開始するための口実としてアンケートを利用します。

（17）引用された事実（Quote Reported Facts）：真実または嘘の情報を引用することによって、情報が公開情報であると思わせる手法。「会社がリストラをしているという報道についてコメントをいただけませんか？」「アナリストが予測している記事を読みましたか？」

（18）偽のインタビュー（Ruse Interviews）：ヘッドハンティングを装って電話し、経験や資格、最近のプロジェクトについて聞き出します。

（19）部外者を狙う（Target the Outsider）：ターゲットが所属していないグループの人たちへ質問を行う。多くの場合、友人・家族・ベンダー・子会社・競合他社は（なにかしらの）情報をもっていますが、共有すべきでない情報が何かについてはきちんと理解していないかも知れません。

（20）情報の提供と見返り（Volunteering Information / Quid Pro Quo）：見返りを期待して情報を提供する。「当社の赤外線センサーは、その距離では 80%の正確性しか保障できません。御社のセンサーはそれより優れていますか？」

（21）単語の繰り返し（Word Repetition）：重要な単語や概念を繰り返し、既に述べたことについてより詳細な情報を提供させようとすること。「3000 メートルのレンジね？興味深い。」

６．誘導質問を避けるためには

どんな情報が共有すべきではないかを理解し、そのような情報を収集している人を疑うことが重要です。情報を知るべき立場でない人に対しては、自身の個人情報、家族、同僚に関する情報などを含め、いかなる情報も提供すべきではありません。

以下のような対抗策で、誘導質問を逸らすことができます。

（1）公開情報を参照するように伝える。（ウェブサイト、プレスリリース）
（2）不適切と感じた質問や主張は無視して話題を変える。
（3）自分自身で質問を逸らす。
（4）質問の理由は？と聞き返す。
（5）特徴のない答えを返す。
（6）知らないと答える。
（7）このような議論には、セキュリティ担当の承認が必要と答える。
（8）これについては、お話できないと伝える。

もし、誰かが、特に仕事に関連した情報を引き出そうとしていると気が付いたら、セキュリティ担当者へ報告しましょう。

さらなる情報またはトレーニングについては FBI へコンタクトしてください。
www.fbi.gov

U. S. Department of Justice

Federal Bureau of Investigation

（米国司法省　連邦捜査局）

「Intellectual Property Protection」

「知的財産保護」

公益財団法人　防衛基盤整備協会　訳

１．はじめに

国内外の企業が、会社の情報を違法に取得する可能性があります。自国の経済や軍を強化するために、米国のテクノロジー企業を標的にしています。

企業の業績・独自性に寄与する企画やシステムを保護しましょう。企業が先進的な技術を保有している場合は、技術やその技術にアクセスできる人物が標的になる可能性があります。企業が他社よりも低コストで製造できるプロセスを開発している場合は、その製造プロセスも対象となります。 企業が他社や他国と交渉している場合は、交渉者や交渉戦略も対象となります。あなたの会社が製品やアイデアの開発のために時間やリソースを投資したのであれば、これを保護しましょう！

２．標的となる情報

（１）独自の製法やプロセス
（２）プロトタイプまたは青写真
（３）研究
（４）技術的コンポーネントと計画
（５）機密文書
（６）コンピュータアクセスプロトコル
（７）パスワード
（８）従業員データ
（９）製造計画
（10）装置仕様
（11）ベンダー情報
（12）顧客データ
（13）アクセス制御情報
（14）コンピュータネットワーク設計図
（15）ソフトウェア（ソースコードを含む）
（16）電話帳

（17）採用／解雇の手順や計画
（18）交渉の戦略
（19）販売予測
（20）価格戦略
（21）企業戦略
（22）マーケティング戦略
（23）買収戦略
（24）予算見積もり／支出
（25）企業財務データ
（26）投資データ

３．よくある戦術

（１）コンピュータのハッキング！　（電子デバイスハッキング）
　ア　訪問者が USB ドライブなどの電子デバイスを接続し、マルウェアの追加や情報をダウンロード
　イ　標的型攻撃によるネットワークのハッキング
　ウ　放置されたラップトップのアクセスまたは盗難
（２）企業の訪問者
　ア　許可されない写真撮影またはコンピュータのアクセス
　イ　制限区域への不正な立ち入り
　ウ　訪問目的を超えた質問
（３）公開情報の見直し。過剰な情報を公開していないか？
（４）余剰機器の入手。コピー機、プリンター、FAX マシンなどのメモリーに何千ページもの情報が残っている可能性
（５）雇用の勧誘（主要な従業員の雇用の試み）
（６）展示会における盗難または不正な撮影
（７）盗難（原本が社内に残されたまま、制限された書類のコピーを含む）
（８）ダンプスターダイビング（会社のゴミ箱から情報を見つける）
（９）合弁企業
（10）フロント企業
（11）迷惑な情報依頼
（12）情報の引き出し（制限されたデータや製品の入手を目的として、従業員と友好関係を築く。従業員からは、自分の仕事に興味を抱いた無害な人に見えるかもしれない。）
（13）電子的な監視（ホテルの部屋の盗聴器、携帯電話のハッキングなど）

４．知的財産の盗難は、次のような結果をもたらす。

（１）利益の減少

（２）雇用の喪失

（３）評判の失墜

（４）模造品による健康や安全への懸念

（５）研究開発に対する投資の減少

（６）製造の遅延や中断

５．知的財産を盗む者は誰？

（１）国内または海外の競合他社

（２）国内または海外の新興企業（スタートアップ）

（３）外国の情報機関員（スパイ）

（４）不満をもつ従業員

（５）オポチュニスト（一匹狼）

（６）組織犯罪者

６．内部に潜む脅威

従業員が、会社の情報を集めて社外へ渡すかもしれないという兆候を探しましょう。

７．海外旅行

（１）外国に旅行する場合、あなたとあなたの会社の情報はより大きなリスクにさらされます。

（２）多くの外国では、技術的な監視に法的規制はありません。

（３）一部の外国政府は、国内企業が競合他社の情報を収集するのを手助けしています。

８．保護戦略

（１）企業における情報セキュリティの脆弱性を評価し、その脆弱性に関連するリスクを是正、または緩和しましょう。

（２）会社にとって重要な個人情報を、インターネットに接続するあらゆるデバイスに保存しないでください。

（３）最新のソフトウェアセキュリティツールを使用しましょう。多くのファイアウォールは､外部から侵入しようとする脅威を阻止できますが､送信データは制限しません。競合他社の情報のハッカーは、ネットワーク上に格納されたデータを取得しようとします。

（４）標的型メールの仕組みについて従業員を教育しましょう。不審な電子メールを開かないようにするための手順を確立しましょう。

（５）従業員が意図しない情報漏洩に加担しないよう訓練しましょう。
（６）研修やセミナーを通じて、従業員に定期的にセキュリティポリシーを教育しましょう。掲示やコンピュータバナーを使用して、セキュリティポリシーを強化しましょう。
（７）知的財産を保護するため、従業員教育や他のすべての措置を明文化しましょう。
（８）セキュリティと企業ポリシーを強化するための具体的な人事施策を確実に実施しましょう。会社のセキュリティポリシーを遵守させるために、明確なインセンティブを設けましょう。
（９）FBI やその他のセキュリティ専門家に、追加の意識啓発トレーニングを提供するよう依頼しましょう。 FBI は、脆弱性の自己評価ツールを提供することができます。

９．法執行機関への連絡

（１）知的財産保護の最終的な責任は、あなたにあります。 議会は、イノベーションを保護するための知的財産権侵害の刑法を、継続的に拡大し強化してきました。しかし、知的財産や製品を保護するための措置やその文書化など、当事者が合理的な手段を講じる必要があります。
（２）適用される違反
　経済的スパイ活動、企業秘密の盗難、メール詐欺、電子通信手段による詐欺、盗まれた財産の州間輸送、輸出管理、そして知的財産権
（３）これらの犯罪の被害者であると思われる場合は、FBI または国家知的財産権調整センターに連絡してください。調査官は、問題を認識していない場合は行動できません。FBI は、お客様のビジネスの混乱を最小限に抑え、調査中にお客様のプライバシーとデータを保護します。 必要に応じて、FBI は営業秘密やビジネスの秘密保持のための保護命令を追求します。

会社の営業秘密、機密情報や研究を守ろう！

www.fbi.gov　　www.ice.gov/iprcenter

平成２９年発刊資料
ＢＳＫ第２９－２号『企業が国際共同開発に参加する場合の契約制度上の課題等（その４）（平成２８年度）』
ＢＳＫ第２９－１号『中国のサイバー攻撃の実態（平成２８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。

誘導質問、知的財産保護（平成２９年度）

平成２９年８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
電　話　：　０３－３３５８－８７５４　　ＦＡＸ　：　０３－３３５８－８７３５
メール　：　koueki@bsk-z.or.jp
ホームページ　：　https://ssl.bsk-z.or.jp

平成27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

最優秀賞
友好が 写真アップで 絶交に
ペンネーム 友情報

佳作
そのサイト 白雪姫も 実は魔女
ペンネーム 三郎

佳作
「同意する」 規約長すぎ ついボタン
ペンネーム 楓すず

佳作
四季問わず 国境超えて サギの群れ
ペンネーム 三郎

佳作
『重要』の 疑似餌が踊る 詐欺メール
ペンネーム ばいなりい

ヤング奨励賞
詐欺かもよ そのワンタッチ 考えて
ペンネーム 頭川成葉