ＢＳＫ第２８－６号

訪問者：リスクとその軽減

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

［Visitors：Risks & Mitigations］

米国政府のためのサプライチェーンリスク管理（ＳＣＲＭ）ベストプラクティスについて

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

［Best Practices in Supply Chain Risk Management for the U.S. Government］

平成２８年１１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９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、“Visitors：Riaks & Mitigations”と”Best Practices in Supply Chain Risk Management for the U.S Government”を翻訳したものです。

前者は**「訪問者：リスクとその軽減」**と題して翻訳しましたが、ここでは企業を訪問することは、この企業の競争相手にとっては容易に入手できない情報を収集する良い機会であり、工場見学中、長期駐在者（訪問者）やジョイントベンチャー期間中、訪問後に企業からどのような手段で固有情報や秘密情報を盗み出すか、またその兆候について分かり易く説明し企業側が訪問者に対してセキュリティ対応することを求めています。例えば腕時計型マイクロカメラによる写真撮影や録音、靴底に両面テープを張り付けて生産プラント作業場の金属合金のかけらを収集する方法や会社内で社員に近づき情報を入手しようとする兆候について紹介し、警告している。我が国でも外国籍の従業員の雇用が増え、企業秘密の窃取等が行われるリスクがある中、企業や従業員を守るために役立つ資料であると思われます。

後者は**「米国政府のためのサプライチェーンリスク管理（ＳＣＲＭ）ベストプラクティスについて」**と題して翻訳しましたが、ここでは、米国ではグローバル化したサプライチェーンに起因する模造品、不法な改ざん、悪意のあるソフトウェア等の脅威について、国家標準技術院が策定したＳＣＲＭ基準に従い、各連邦政府機関ごとに戦略的かつ包括的な方法で管理しなければならないとして、サプライチェーンリスク管理のベストプラクティスについて紹介しています。市場のグローバル化に伴いサプライチェーンに対するリスクが高まり、我が国においても政府及び企業を含めたサプライチェーンリスク管理について取り組むための有益な資料であると思われます。

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２８年１１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）
[Visitors: Risks & Mitigations]

「訪問者：リスクとその軽減」

公益財団法人　防衛基盤整備協会　訳

はじめに

あなた方の施設に入った訪問者は、あなた方の知的財産や競争力に対して、セキュリティリスクを引き起こすかもしれません。訪問は、競争相手にとって、容易に入手できない情報を収集する良い機会です。ある訪問者は口頭で情報を引き出す訓練を受けているかもしれませんし、ある訪問者はその施設のセキュリティ制限を大胆に無視するかもしれません。その他に、制限された情報を入手するために、あらゆる種類の秘匿された記録装置を使う者がいるかもしれません。彼らが集めたいくつかの情報は、設備のレイアウトの様に当たり障りのないもののように思えるかもしれませんが、それらはあなた方の製品の秘密を解くカギを与えたり、自分たちの設備をより良く運営するのに非常に価値があるかもしれません。競争相手に、市場競争の中で自分たちがどうやってやりくりしているか教えないことです。そして泥棒があなた方の情報を盗むのを手伝わないことです。

一人の訪問者が自分の腕時計をいじっていた。そしてそれは、受け入れ側が腕時計にマイクロカメラが仕込まれているのではないかと疑うしぐさだった。

外国人の訪問者たちが、米国の軍用機の製造工場の床から銀色の金属合金の削りくずを集めるために、靴底に両面テープを張っていた。そして彼らは、その金属片を分析して飛行機に使われていた金属部品を特定した。

工場見学中のセキュリティ(Security during Facility Tours)

ペン、サングラス、ボタン、キーホルダー、タバコの箱などに偽装した音声・映像記録装置が、市販でたくさん出回っています。そのような装置をあなた方の施設に持ち込むのを阻止するのはほとんど不可能です。工場見学を計画するときは、このことを心に留めておいてください。

・訪問者に関係する脅威の事項について、全ての従業員に説明してください。
・訪問の範囲における適切な人物（エスコートする人、訪問者への説明者、見学される作業現場の人）に説明してください。

・訪問者当たりのエスコートする人の数が、訪問者を適切に監督し管理するのに十分であることを確認してください。
・エスコートする人たちが、訪問時に使用される窃盗のための技術について知識があり、訓練を受けていることを確認してください。
・訪問者が何時、自分たちの作業場に立ち入るかを知っているかどうか従業員に確認するとともに、訪問者の視界から企業の固有情報を隠すように彼らに注意喚起してください。
・訪問者を、訪問者バッジや訪問者上着などで、簡単に識別できるようにしてください。
・訪問者に対して、セキュリティ上および安全上の決まりごとについて、事前に通知しておいてください。そしてそれには、違反した場合に引き起こされる結果についても含めておいてください。
・規則遵守上の問題やセキュリティ上の懸念がある場合に、工場見学を中止し訪問者を施設の外に退去させることを躊躇しないでください。

訪問者が工場見学の最中に制限された情報を入手しようと試みているかどうかの兆候(Indicators that a visitor may be trying to obtain restricted information during tour)

・間際での、訪問者名簿への追加や変更
・機微／禁止エリアへの許可を得ていない電子装置や記録装置の持ち込みの試み（または成功）
・携帯電話やマイクロカメラ（極小のもの或いは腕時計、ペン、又はその他の持ち物に偽装したもの）でアイテムの写真を撮ろうとする試み
・当初述べていた訪問目的にこだわらない（訪問目的を修正・変更する）
・許可された範囲外の質問をする。
・セキュリティ上や訪問規定上の問題が生じると、腹を立てたりけんか腰になる。
・工場見学中に、ルートから離れたり、はぐれたふりをする。
・機微又は秘密関係の工場見学申請が却下されると、もう少し緩やかな工場見学や民需部門の工場見学を申請してくる。
・特定の施設に繰り返し工場見学を行う。
・商業上の訪問と考えられているのに、外国からの訪問者が、自分の身分を隠そうとする外国の連絡官や大使館員によってエスコートされる。

長期駐在やジョイントベンチャー期間中のセキュリティ(Security during Long-term Visits and Joint Ventures)

長期駐在やジョイントベンチャーは、競争会社に制限された情報を入手するための一層大きな機会を提供する。それらはまた、訪問や駐在の期間中または将来に、制限された情報を収集する上で、手助け（喜んでであれ、しぶしぶであれ）する可能性のある従業員に目星をつけたり、評価したり、友人として近づく機会を訪問者に与える。

提携大学からの訪問者が、許可なく、もう一方の大学に設立された研究室にあるすべてのアイテムを、装置の製造元やモデルが映り込むように写真を撮った。二つの大学は共同研究していると思われていたが、その設立された研究室の室長は、結局のところ彼の研究室は一方的に情報を共有（提供）しただけだったということを知った。

・プロジェクトの範囲の観点から、広く従業員を教育し、またセキュリティ懸念事項をどのように報告するか教育してください。
・情報の聞き出しやリクルートの試みをどう察知するか従業員を訓練してください。
・訪問者の到着前に、従業員に対して、訪問者のアクセス制限、潜在的な収集テクニック、経済スパイの特徴、及びセキュリティ上の懸念を誰に報告すべきかについて、説明してください。
・従業員に対して、プロジェクトの範囲及び情報の聞き出しへの気づきについて、定期的でかつ継続的に思い出せるように、注意喚起してください。
・訪問者に対して、コンピュータ、コピー機、ファックスの使用やアクセス制限、及び建物や部屋へのアクセス制限を含む、義務と責任について説明してください。
・訪問者に対して、彼らが守るべきセキュリティ要求事項についての同意書に署名を求めてください。そしてその同意書には遵守しなかった場合の結果について記述すべきです。
・ジョイントベンチャーの範囲で共有される情報は、最小限の範囲にしてください。
・従業員及び訪問者による規則の不遵守や無視には、罰則があることを確実に周知するようにしてください。
・企業の固有情報や秘密情報には、分かるように表示してください。
・施設に不必要な代表者が立ち入ることを拒否してください。

・訪問者がネットワーク接続されたコンピュータを使用することを許可してはいけません。もし必要ならスタンドアローンのコンピュータを提供してください。
・訪問者がファックスしたり、郵送したり、ｅメールした全ての文書をレビューしてください。そして必要なら翻訳してください。
・経済スパイや情報の聞き出し、リクルートなどの兆候がないかどうかチェックするために、訪問者と接触する機会の多い従業員を定期的に面接してください。
・訪問者や従業員による、彼らに許可されたコンピュータアクセスを超えるいかなる試みも検知するために、常続的なコンピュータ監査を実施してください。

テキストメッセージを読むという口実を使って、訪問者が携帯電話を使って、営業秘密の装置の写真を撮った。写真は技術者にｅメールされ、その技術者によって、後に類似の装置が設計され製造された。

長期駐在者（訪問者）が制限された情報の入手を試みるときの兆候(Indications that long-term visitors may be trying to obtain restricted information)

・ある会社は、競争入札の過程で、膨大な技術データを提供するようそそのかし、その上で契約はキャンセルされる。
・ジョイントベンチャー期間中の潜在的な技術共有契約が片務的である。
・提携企業が、その時期としては必要以上の代表者を送り込んでくる。
・訪問者は、プロジェクトの範囲外の情報を聞き出すために、会社の人間を選び出す。
・訪問者がローカルエリアネットワークにアクセスしたがる。
・訪問者が、施設への制限のないアクセスを求める。
・訪問者が、大使館や外国へ文書をファックスしたり、ｅメールする。
・訪問者が、コンピュータに許可されていないＵＳＢメモリやその他のデバイスを接続しようと試みる。
・訪問者が、頻繁にセキュリティ手順を忘れたり、彼に頻繁に禁止事項について注意喚起する必要がある。

制限された情報の入手を試みる訪問者に関する追加の指標(Additional Indicators that a Visitor is Trying to Obtain Restricted Information)

外国人の訪問者が製品のサンプルを入手するために、化学溶剤の中に自分たちのネクタイを浸した。彼らはまた、工場内で別々の方向に散らばり、施設の中でできるだけすべての写真を撮った。その訪問者たちを受け入れた会社は、その国での市場を見出すことはできなかった。

・不注意による、機微な、企業固有の、あるいはプロジェクトの情報の暴露。
・セキュリティＩＤバッジの不適切な着用。
・存在しないセキュリティＩＤバッジの使用やＩＤバッジの持参忘れ。
・セキュリティバッジを写真撮影したり、返却しない。
・彼らの訪問範囲を超えるエリアに対するアクセスをリクエストしたり立ち入ったりする。
・彼らのアクセスの範囲を超えた情報をリクエストする。
・秘密の、あるいはデュアルユースの、さもなければ制限された情報をリクエストする。
・装置や書類の紛失または所在確認ができない。
・彼らが知る必要のないプログラムに関する特有の略語を使って、プログラムに関する質問をする。
・さらに情報を得るために、ソーシャルエンジニアリングの手法あるいは聞き出しテクニックを使う。

訪問後の手続き(Post-Visit Protocols)

・長期駐在者（訪問者）が使用した、建物や部屋やコンピュータのためのパスワード、カギ、あるいはアクセスコントロールを変更してください。
・従業員に対して、一旦長期駐在やジョイントベンチャーが終了した場合に、その後どの情報が共有できてどの情報が共有できないか、説明してください。
・駐在者（訪問者）からのその後のコンタクトについての会社の方針について、教育してください。（職場へのｅメール、個人のｅメール、電話、直接の面会、ＳＮＳを介したコンタクトについてのガイダンスを提供するような会社の方針を示す必要があるかもしれません。）つまり、以前の訪問者とのコンタクトを適切に行うための訓練を従業員に行ってください。

あるジョイントベンチャー契約で、片方の会社からもう片方の会社に３人の従業員を派遣できることとなっていた。ジョイントベンチャーが終了したときに、３人の従業員たちは、受け入れ先の企業固有の情報を、私物と表示した箱の中に入れて持ち出そうと試みた。

以前の駐在者（訪問者）が制限された情報を入手しようとするときの兆候(Indicators that previous visitors may be trying to obtain restricted information)

・以前の訪問者が、従業員を、訪問者の海外の会社に、講義を依頼したり表彰をするとして招待する。
・以前の訪問者の同僚から、他の部や他の従業員（つまり営業部など）に宛てるべき情報提供やサービスの提供を依頼する内容の望まないｅメールがくる。
・適切ではない、あるいは人を操作するようなソーシャルコンタクト（ｅメール、電話、ＳＮＳを介して、あるは直接に）がある。
・以前の訪問者が、頼み事をしてきたり、追加の情報をリクエストしてくる。
・以前の訪問者が、彼らの訪問の目的外のプロジェクトについての機微な情報をリクエストしてくる。
・訪問者または訪問者の会社が、調査や質問項目に答えるよう依頼してくる。
・以前の訪問者が、ｅメールなどの受領者に、セキュリティ上の懸念は心配ないと助言したり、もしセキュリティ上の懸念があっても無視するように依頼する。

一般的なガイダンス(General Guidance)

・機微な情報を放置してはいけません。
・機微な、又は企業固有のあるいはプロジェクトの情報は、それを共有する前に、管理者から許可を得てください。つまり、情報の受領者がそのような情報を受領することが許可されていることを確認してください。
・もし機微な、あるいは企業固有の情報を共有することが許可されていたとしても、それについて安全でないあるいはオープンな環境下では議論してはいけません。
・機微な情報は、安全な方法で廃棄してください。（シュレッダーするなど）
・席を離れる場合は、コンピュータワークステーションをロックしてください。
・ワークステーションにパスワードやログイン手順書を記憶させてはいけません。
・誰とも、アクセスコード、ユーザー名、あるいはパスワードを共有してはいけません。
・電子的記憶媒体（外部記憶装置、ＵＳＢメモリ、ノートパソコンなど）から目を離さないでください。
・文書による許可なくしては、個人的なソフトウェア及びハードウェア（ＵＳ

Ｂメモリ）を会社のネットワークにインストールしたり接続することを許可してはいけません。

もしあなたが疑わしい態度や行動に気が付いたなら、すぐにあなたの会社のセキュリティ担当者に報告してください。セキュリティ部門に、それが問題のないものかどうか判断させてください。追加の情報や訓練については、ＦＢＩにコンタクトしてください。

営業秘密(Trade Secret)：（１）所有者が適切な手段を用いて秘密にしている。（２）単独でも経済的価値のある。そのようなすべてのタイプの情報（財務上の、ビジネス上の、科学的な、技術的な、経済的な、あるいは無形の）
企業固有の情報(Proprietary Information)：公には入手できない情報で、所有者によって開発されたもので、所有者の資産と見なされるが、営業秘密までには至らないもの。
機微な情報(Sensitive Information)：公開されていない情報だが、企業の固有情報ではないもの。輸出管理の対象情報や出版制限の情報を含む。

FBI Counterintelligence brochure （ＦＢＩ対情報啓発資料）
[Best Practices in Supply Chain Risk Management for the U.S. Government]

「米国政府のためのサプライチェーンリスク管理（ＳＣＲＭ）ベストプラクティスについて」

公益財団法人　防衛基盤整備協会　訳

サプライチェーンリスク管理（ＳＣＲＭ: Supply Chain Risk Management）

サプライチェーンリスク管理（ＳＣＲＭ）は、製品とサービスのサプライチェーンのグローバルで分散した性質に関連したリスクを、特定し、評価し、無効化するプロセスです。

米国経済のグローバリゼイションは、新たに出現してきた脅威や脆弱性から、米国政府のサプライチェーンを保護するために、ＳＣＲＭ手法を適用するときに、ユニークで複雑な問題を惹起します。外国政府の存在と影響、製造や開発の不十分な実行、模造品、不法な改ざん、窃盗、悪意のあるソフトウェア等は、軽減すべきサプライチェーンリスクの例です。連邦政府機関、政府の契約相手方、供給者、インテグレータは、米国政府のサプライチェーンに対する脅威を、一貫して評価、測定、無効化することを難しくしている、様々なしかも標準化されていないプラクティスを使っています。

連邦政府機関は、既知のあるいは新たに出現してきた脅威、脆弱性、及び組織的なインパクトを説明するＳＣＲＭ戦略を策定すべきです。連邦政府機関のサプライチェーンは、各連邦政府機関ごとにユニークです。一つのＳＣＲＭ戦略を連邦政府全体にわたって適用することはできないし、連邦政府機関は、各機関自分自身の戦略の基礎として、米国国立標準技術研究所（ＮＩＳＴ）が策定したＳＣＲＭ基準に従うべきです。ＳＣＲＭは、米国政府機関にリスクを受け入れ可能なレベルまで軽減するためのサプライチェーンリスクと必要な行動を評価するために調整チームアプローチを設置するように要請します。チームのバックボーンは、サプライチェーンマネジメント、セキュリティ、調達、契約及び行政法、監査と財務、並びに施設管理の各分野の専門知識を持った専門的学問分野の多様なグループで構成されるべきです。ＳＣＲＭは、下請けになりうる会社の法的履歴や財務的支払い能力、納税履歴、他社との会社関係を含むリスク評価ベースラインを作成するために、オープンソースコマーシャル製

品も含めて、多様な資源をてこの様に利かすべきです。最初の調査は、対情報脅威に焦点を当てた詳細リスク評価と一体化して評価されるべきです。以下のガイドは、ＳＣＲＭプロセスの中でレビューする詳細のリスク評価質問項目を提供します。

サプライチェーンリスクアセスメントを作成するための推奨(Recommendations for Developing a Supply Chain Risk Assessment)

効果的なリスクアセスメントは、省庁による自分たちのサプライチェーンとその脆弱性に対する理解から始まります。リスクアセスメントは、調達された製品や役務のセキュリティ、完全性、品質、及び回復力を調査し、特定し、評価するメカニズムです。

製品と役務の提供者(Providers of Products and Services)

役務提供者の所在地を特定しなさい。もし外国にあるのであれば、外国政府とその提供者（サプライヤー、ベンダーなど）との潜在的な関係を特定しなさい。提供者から機微なビジネス情報を国に提供させる法律や政策があるかどうか特定しなさい。関係している外国人又は提供者にアクセスしている社員の氏名、住所、役割を要求しなさい。

○提供者の本社の所在地、製造施設及び役務施設の所在地（つまり、米国か、外国か）
○提供者は、外国政府と関係があるか？
・提供者に対する外国政府の所有権は何パーセントか？
・提供者は、外国政府から補助金や優遇措置を受けているか？

提供者が外国籍の人間を雇用しているかどうか特定しなさい。誰がビザのスポンサーになっているか、各個人の滞在期間は許可されているものか、各外国籍の人間の技術的技能や能力の重要性を判断しなさい。そして、外国が（特にその従業員の母国に特別な焦点を当てて）同様の技能を持った働き手を必要としていると表明していないかどうか、判断しなさい。また、製品や役務を利用する米国政府について、それを外国政府が知った場合のインパクトについて検討しなさい。外国政府は、彼らの情報機関を使って、提供者の脆弱性につけこもうとしているかもしれません。

○提供者は、どれだけ綿密に従業員の身元調査をしているか。
・彼らは、外国籍の従業員を雇用しているか？
・彼らは、バックグラウンドチェックあるいは前職確認を行っているか。
◆犯罪歴､以前の職やスキルレベルについての嘘や誇大のような不適格要件を考慮しなさい。
・その提供者は、外国の情報機関とのいかなる関係も知られていないか。

知的財産窃盗に関する提供者の履歴に関する公開されている情報（そして入手できるなら秘密に情報）をレビューしなさい。何が危殆化されたり盗まれたのか、それがいつ、そして可能なら誰によってなされたものか特定しなさい。米国政府の国家安全保障に対して、潜在的なインパクトがあるかどうか検討しなさい。そして更に、米国政府や危殆化した製品や役務との関係での外国政府の国家安全保障上の利益についても検討しなさい。もし知的財産窃盗の履歴が不明ならば、サプライヤーやベンダーが、どのように自分たちの知的財産を保護しているかに関連する情報提供を要請しなさい。

○提供者が、知的財産窃盗の履歴があるか又は告訴されているか。
○提供者が、知的財産窃盗の被害者になったことがあるか。
・従業員が機微情報を不適切に共有したのか、あるいは施設へのアクセスを提供したのか。
・コンピュータネットワークへの侵入があったのか。
○提供者は、どのようにコンピュータネットワークを防護していたか。
○提供者は、コンピュータネットワーク侵入の被害者になったことがあるか。

提供者が、自分たちの製品やサードパーティ製品及び役務の品質を確証するためのプロセスと手順を特定してレビューしなさい。もし危殆化された製品が取得され、連邦政府のシステムや施設がそれを組み込んだ場合、米国政府に与えるインパクトを検討しなさい。

○確証された製品の品質はどうであるか。
○製品が要求事項を満たすことを確実にするためにどのようなメカニズムが設けられているか。
○政府機関は、物件・役務をレビューするために、検査プロセスを設けているか。

提供者の現在の財務状況と生産能力を検討して、現行の及び増加した場合の需要に応えられるかどうか検討しなさい。提供者の財務的なバックグランドをレビューし、提供者が要求に応えられなくなった場合の米国政府にとってのインパクトを検討しなさい。

〇提供者は、財務的に健全か。
〇提供者は、外国政府から補助を得ていないか。
・資金提供が減らされても成長し続けられるか。
・政府からの資金に、規定があるか。

流通と輸送(Distribution and Transportation)

製品がどのように提供者から米国政府へ輸送されるかをレビューしなさい。荷物の積み替え地点と保管施設を特定しなさい。それぞれの地点にアクセスすることのできた個人または政府職員を特定しなさい。そして、出荷の途中で製品にコンタクトした可能性のある個人が所属する運送会社の名前と住所を特定しなさい。輸送の形態及びルート、及びその国が国境警備隊や税関を通じて輸送を妨害することのできる能力、並びに積み替えや保管施設の物理的セキュリティ環境を、レビューしなさい。製品や役務が輸送の途中で危殆化された場合の米国政府へのインパクトについて検討しなさい。

〇製品がどのように、生産者、製造者、あるいは役務提供者から米国政府へ輸送されたか。
・海外輸送されたか。
・積み替え地点はどこか。
・輸送の途中で倉庫に保管されるか、されるとすればどこか。
・誰がその施設を所有しており、アクセスできるか。
・輸送には、どの輸送会社を使うか。

取り付け、組み上げ、メンテナンス(Installation, Integration, and Maintenance)

製品や役務がどのように取り付けられ、時が経つにつれ維持されるのかを、レビューし評価しなさい。装置の取り付け前あるいは取り付け後に遠隔アクセスするかもしれない個人の名前と住所を特定しなさい。さらに、米国政府の管轄下で装置に直接アクセスするかもしれない人物あるいは直接アクセスする必

要のある人物の名前と住所を特定しなさい。もし外国籍の者がアクセスするのであれば、それぞれの者がアクセスする情報の程度と範囲と個人の名前を特定しなさい。もし機微な情報や人物や施設が危殆化された場合の国家安全保障へのインパクトや結果について検討しなさい。

○製品や役務が、現行のシステムや手順にどのように組み込まれたり取り付けられるのか。
○誰が、機微な業務情報やユーザーや施設にアクセスするか。

廃棄及び退役(Disposal and Retirement)

電子装置を廃棄あるいは退役させる前に、機微な情報を消し去るべき、電子装置を決定しなさい。ハードドライブから機微な情報を取り除く責任を負う者の名前を特定しなさい。そして米国政府の資産から装置を物理的に取り外す責任を負う者の名前を特定しなさい。装置を廃棄あるいは退役させた後にそれをどうするか決定しなさい。もしそれが再生されて販売されるのであれば、それを購入あるいは取得する可能性のある会社の名前と住所を特定しなさい。

○装置を廃棄したり退役させたときに、機微な情報が不適切に暴露されないことを確かなものとするために、政府機関にとっては、どのレベルの綿密な検査が必要か。
○廃棄した装置に何が起こるのか。
・それが再生されて再び販売されるのか。

米国政府のサプライチェーンのリスクを無効化する(Neutralize Risks to the USG Supply Chain)

米国政府の調達職員は、脅威、脆弱性、そしてそれらのインパクトに関して調査することに一丸となって取り組むべきです。適切なレベルでリスクを無効化するための取るべき必要な行動を推奨すべきです。これらの推奨事項は、現行の連邦政府機関の政策手続きと同様に、連邦政府調達規則に則ったものでなければなりません。

共通リスク軽減テクニック(Common Mitigation Techniques)

○米国政府は、米国政府への提供者と常続的なコミュニケーションを取り、協力的な関係を維持すべきです。
○米国政府は、提供者の製品開発、製造施設、及び物理的並びにサイバーセキュリティ基準を監査するために、現地監査をリクエストすべきである。
○米国政府は、提供者に、訪問者の記録を取り始め、それを維持するようリクエストすべきである。
○米国政府は、提供者の所有者や製品開発に変更がある場合は、事前の通知をリクエストすべきである。
○米国政府は、提供者が知的財産、製造プロセス、あるいはその他の機微な物件の保護を確実に行えるように、契約書や合意書を認証された法的権威者にレビューさせるように、促すべきである。

追加の情報(Additional Information)

商務省：Department of Commerce
米国国立標準技術研究所：National Institute of Standards and Technology(NIST)
ＳＰ８００－１６１連邦情報システムのためのサプライチェーンリスク管理実務
http://scrm.nist.gov

国家情報長官室： Office of the Director of National Intelligence(ODNI)
インテリジェンスコミュニティ指令７３１
http://dni.gov

国防セキュリティ局：Defense Security Service(DSS)
国家産業セキュリティプログラム
http://www.dss.mil/isp/index.html

連邦捜査局：Federal Bureau of Investigation(FBI)
http://fbi.gov

統合任務付与(Joint Duty Assignments)

ＦＢＩは、参加を希望する政府機関とより良い連携を図り、ＳＣＲＭに関係するインテリジェンスを共有するために、統合任務付与機会を設けています。興味のある方は、ＦＢＩの（２０２）３２４－２３７６に連絡ください。

情報を提供する会合(Informational Sessions)

ＦＢＩは、国家情報長官室（ＯＤＮＩ）の国家対情報及びセキュリティセンター（ＮＣＳＣ）サプライチェーン局の活動メンバーです。国家対情報及びセキュリティセンター（ＮＣＳＣ）の任務は、米国政府、米国インテリジェンスコミュニティ、及び米国の民間部門（外国及びその他の敵から、情報収集、浸透、あるいは攻撃のリスクに晒されている）の対情報活動やセキュリティ活動を指導あるいは支援することです。国家対情報及びセキュリティセンター（ＮＣＳＣ）は、その任務を支援する中で、サプライチェーンリスク管理を含む、機能分野横断的な統一されたインテリジェンス戦略を開発し、実行しています。国家対情報及びセキュリティセンター（ＮＣＳＣ）は、関心のある政府機関に対して、要請があれば、ＳＣＲM情報提供会合を提供します。その情報提供会合は、政府機関に対して、ＳＣＲM軽減テクニックについてさらに学ぶ機会を与え、ＳＣＲM軽減テクニック、及びＳＣＲMのキーとなる人脈を共有する機会を提供します。情報を提供する会合のスケジューリングや国家対情報及びセキュリティセンター（ＮＣＳＣ）のワーキンググループについてもっと知りたい場合は、（２０２）３２４－１７３５にお電話ください。

平成２８年発刊資料

ＢＳＫ 第２８－５号『セキュリティより始めよ』
ＢＳＫ 第２８－４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３)』
（平成２７年度）

訪問者：リスクとその軽減
米国政府のためのサプライチェーンリスク管理（ＳＣＲＭ）ベストプラクティスについて

平成２８年１１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