ＢＳＫ第２０－２号

人的セキュリティ:脅威、挑戦、および対策

(PERSONNEL SECURITY : THREATS, CHALLENGES AND MEASURES(2007 年 12 月))

― 英国における人的セキュリティへの取り組み ―

平成２０年３月

財団法人 防衛調達基盤整備協会

はしがき

本出版物は、英国の政府機関である国家インフラストラクチャー保護センター（Centre for the Protection of National Infrastructure：以下 CPNI という。）が作成した「人的セキュリティ：脅威、挑戦、および対策（PERSONNEL SECURITY:：THREATS, CHALLENGES AND MEASURES)」（２００７年１２月）を翻訳したものである

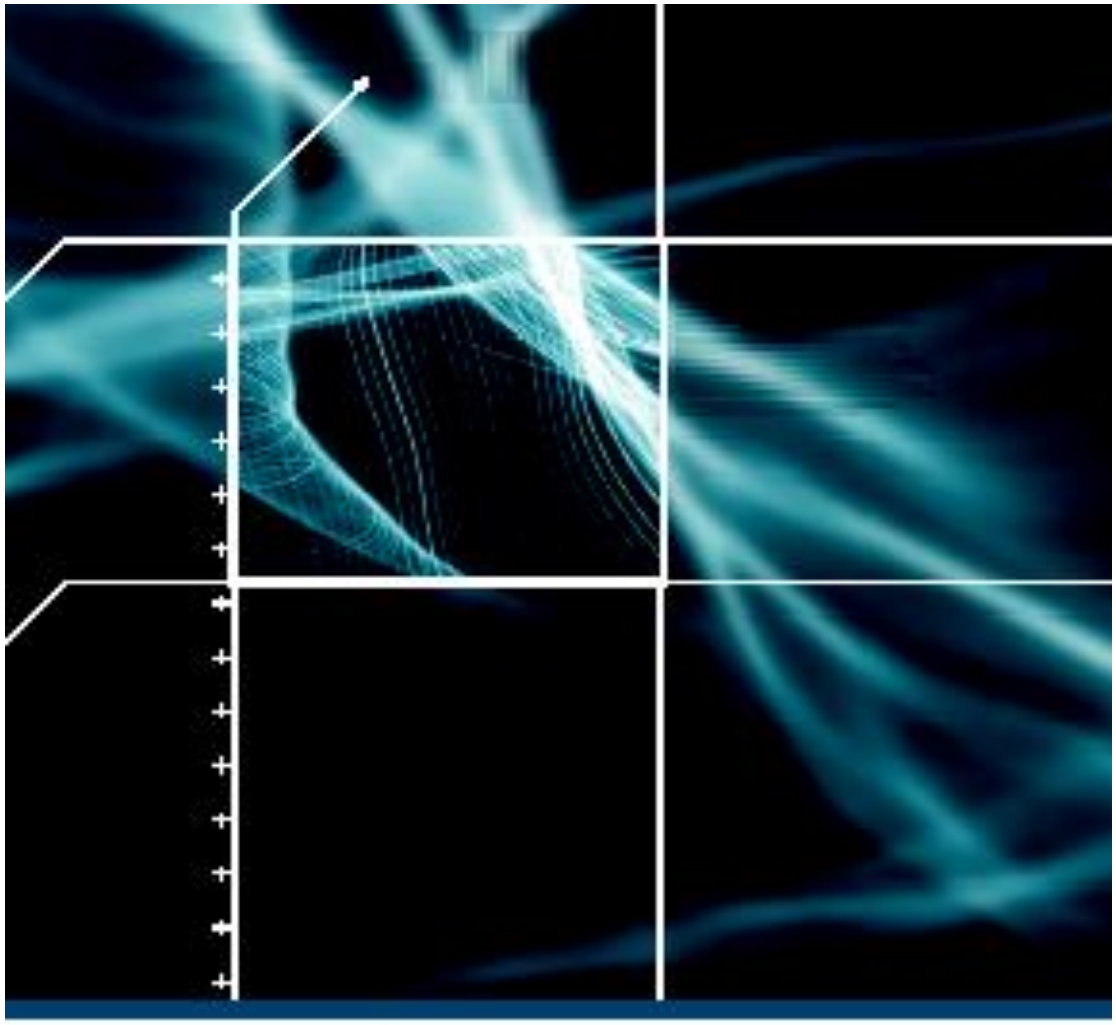
CPNI は、国家インフラストラクチャーに関連する組織に対して、キュリティ・アドバイスの提供を担当している機関である。

本資料は、組織のセキュリティ、採用、およびライン部門の管理者を対象とした人的セキュリティに関する導入的説明書（ガイダンス）である。本ガイダンスには、組織をインサイダー脅威（本ガイダンスでは、合法的なアクセス権を悪用する従業員をインサイダーと定義する。）から保護するためのプロセスと対策が解説されている。この内容は公的機関のみならず、広く民間企業にとっても有用なものであると思われる。

本出版物が、我が国における人的セキュリティ体制の向上にいささかでも貢献できれば望外の幸せである。

平成２０年３月

財団法人 防衛調達基盤整備協会
理事長　宇　田　川　　新　一



PERSONNEL SECURITY:

THREATS, CHALLENGES AND MEASURES

２００７年１２月

免責事項

社名、商標などによる特定の商品、プロセス、またはサービスへの言及は、CPNI による支持、推薦、または好みを意味するものではない。本書に発表された著者の見解や意見は、広告または製品の推薦目的に使用してはならない。

CPNI は、法律が認める最大範囲において、本書の過失（誤り、脱落）、何人の不作為、もしくは行動の抑制によって引き起こされた、または、さもなければ本書の中の情報もしくは言及を使用することによって引き起こされた、如何なる人が被る如何なる損失もしくは損害（直接に、間接に、または必然であろうと、利益もしくは見込み利益の損失、データ、仕事、または営業上の信用の損失を含むが、これらには限定されない）に対する責任を一切負わない。利用者は、本書の使用に際しては、自分自身で判断をしなければならない。また、利用者の特定な状況については独立した専門家の助言を求めなければならない。

序　文

本書は、セキュリティ、採用、およびライン部門の管理に責任を有するものに対する人的セキュリティに関する導入的説明書（ガイダンス）となるものである。本書は、英国の国家基盤（Infrastructure）の一部である主要な資産、サービス、およびシステムを所有または運用する組織向けに作成されているが、本書に概説されたプロセスと対策は広く民間企業にとっても有用なものである。**図１は内容の要約である。**

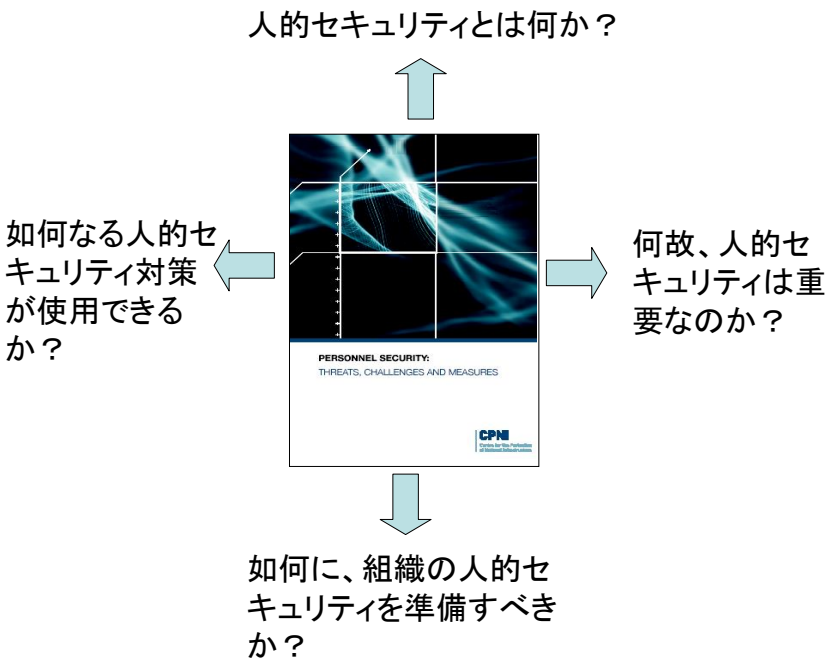


図１：本ガイダンスが取り組む主要な論点

効果的な人的セキュリティ体制には、採用プロセスと契約プロセスのみならず、その後の継続的した監督（コントロール）が必要である。本ガイダンスは、使用可能な対策と各組織が規模等に応じて実行できるプロセスを概説している。本ガイダンスは、英国国家インフラストラクチェー（National Infrastructure）内の各組織の経験から直接情報を得て作成されており、英国情報局保安部（Security Service：一般に MI5 として知られている。）の人的セキュリティに関する出版物（「リスクの管理：Managing the Risk」）に取って代わるものである。 今後、 必要に応じ、より詳細なガイダンスに関する文献が提供されるであろう。

本小冊子のｐｄｆ版は www.opni.gov.uk から入手可能である。

目　次

1. 要　旨

人的セキュリティとは何か？

人的セキュリティとは､正社員あるいは契約社員が､彼らの合法的アクセス権を悪用し、不正な目的で組織の資産へアクセスするリスクを管理する指針と手順のシステムである。“資産”とは、従業員、建物、システム、情報など組織が価値あると判断するもの全てである。合法的なアクセス権を悪用するものは“インサイダー”と呼ばれる。

一部の企業では、人的セキュリティ（personnel security）に正社員の物理的保護（physical protection）を包含しているが、CPNI の見解では、これは別個の活動であり、それは個人的セキュリティ（personal security）（注１）と称される。

（注１）組織は従業員に対しある程度の個人的セキュリティを与えるべきであるが、CPNI はこの点に関する助言には言及しない。人的セキュリティの一部として実施される多くの対策は、従業員に対し必要以上の保護を提供するので、結果として個人的セキュリティ対策として機能するであろう。

何故、人的セキュリティは重要なのか？

人的セキュリティは次の理由により組織の保護のために重要である。

① それは、あらゆる範囲のインサイダー脅威に対する組織の脆弱性を低減させる。インサイダー事件は、有害であり、損失が大きく、厄介であり、かつ、チームワークを乱すものである。効果的な人的セキュリティによって、組織はこれらからの痛手を回避することができる。

- 一部の組織が、増大するテロリストに関連したインサイダー活動の脅威に直面していることを示唆する証拠が存在する。
- 不正行為や機微な情報を売り渡すなどの人的セキュリティ違反の結果、組織が毎年、相当の経済的損失や社会的信用を失うという明白な証拠が存在する。

② 組織の保護能力は、幾つかの保護対策の中の最も弱い要素（エレメント）と同程度のものでしかない。しかし、人的セキュリティは、より具体的な物理的・電子的セキュリティ対策が優先されることにより、しばしば無視されている。

③ 人的セキュリティは労働力の信用と健全性に関する一定レベルの保証を提供する。そして、それは、良好な組織管理全般の基礎となる。

如何に、従業員は彼らの合法的アクセス権を悪用するのであろうか？

従業員の取る行動には、次のようなものが考えられる。

- 無許可の情報開示
- 物理的または電子的破壊活動
- 第３者によるアクセスの補助
- 金銭的または処理上の不正（着服等）
- 窃盗

人的セキュリティは何を達成しようとするのか？

人的セキュリティは次のことに努力している。

① 新しい採用者や契約社員から提供された個人情報（例えば、身分証明書や履歴書）が本物であることを保証する。

② セキュリティに関し懸念がない人物だけが採用されていることを保証する。

③ 従業員が組織資産へのアクセス権を悪用する可能性を局限する。

④ セキュリティに関し懸念がある従業員を発見し、その懸念が適切に管理されていることを保証する。

⑤ 容疑を解明する捜査を行い、組織の懲戒手続きを支援するための証拠を提供する。

⑥ リスクに相応した人的セキュリティ対策を適用し、リスクを許容できるレベルまで低減する。

２．インサイダー脅威

歴史的に見て、多くのインサイダー活動の目的は、個人的利益、会社もしくは国家が資金提供するスパイ活動、または過激な動物保護団体などのようなグループの示威活動であった。これらのインサイダー脅威は依然として多くの組織の中心的な脅威であるが、最近注目される多くのテロリスト関連事例によって、テロリスト組織のメンバーからの脅威あるいはそのような組織との接触を有する従業員からの脅威が浮き彫りにされている。テロリストに関連したインサイダー脅威の可能性は、増大しつつある懸念である。従って、この脅威について次に詳細に述べる。これは、組織が直面するその他の脅威が重要でないということではなく、それらの脅威は比較的良く理解され、かつ人的セキュリティ施策の中に反映されているということである。

国際テロリズムからのインサイダー脅威

インサイダー脅威評価の結果は、テロリストグループが、組織内の従業員を利用しようとしていたことを示唆していた。英国における計画的な爆破テロに関連した最近の例をとると、２００７年７月に５人が終身刑に処されたグループのメンバーは、適切な技量とアクセスを有しているインサイダーの潜在的価値を認めていた。男の中の一人は、以前、公益事業会社で働いており、彼が攻撃計画立案に役立つと考えた情報を窃盗した。

これまでに報告されたケースの多くでは、関連する個人は、彼らのアクセス権を悪用しようと思って組織内のポストを得たわけでなく、むしろ、ポストについている間にたまたまアクセス権を悪用したものであった。テロリストに関連したインサイダーが彼らのアクセス権を利用したケースでは、通常、彼らは、仕事関係以外の人物のためやその人物に唆されて行動したか、または自発的にテロリズムに関連した友人もしくは家族に情報を提供した。これらのケースでは、友人や家族に対する個人の忠義心が大きな動機であった。図２はこれらの異なる脅威を要約したものである。

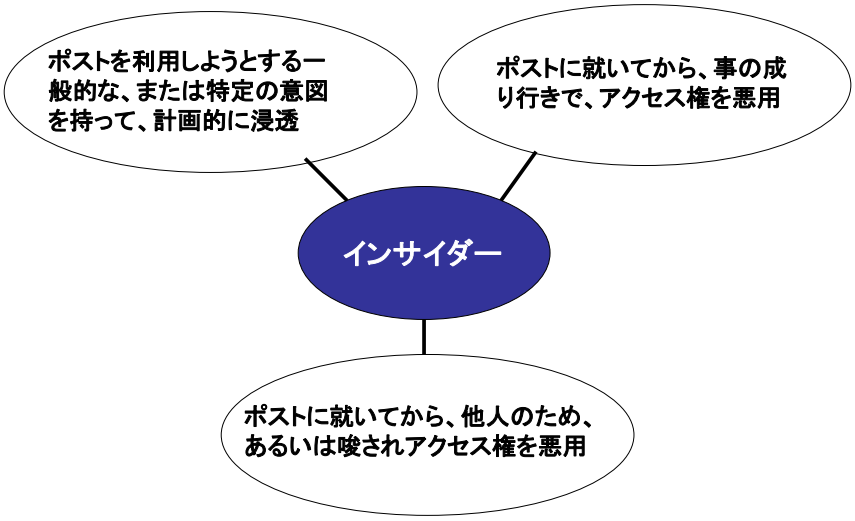


図2：インサイダー脅威の3つのタイプ

今までのところ、テロリズムと関連した多くのインサイダーケースでは、犯罪行為が彼らの雇用の比較的早い段階で起こっているという傾向がある。しかし、インサイダー脅威は雇用のあらゆる段階で起こり得るものであり、元従業員でさえ組織の脅威になるであろう。（例：退職後も誤ってアクセス権が使用できる状態であった場合）

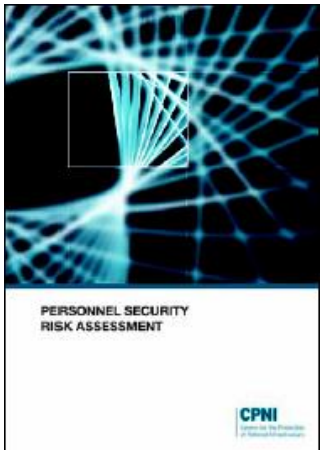
テロリストは次のことを企てるであろう。

- テロ攻撃の実行を直接支援するために、情報またはアクセスを得ること。
- 情報、またはテロ攻撃の実行を容易にする場所、システム、もしくはプロセスへのアクセスを得ること。
- 当局が彼らについて何を知っているか、そして、如何に発見を回避するかを探り当てること。

要約すると、組織は、広範なインサイダー脅威と詐欺、窃盗、産業スパイなどの犯罪行為に対処する経験を有しているが、ますます、テロリズムに関連したインサイダー脅威に晒されている。従って、人的セキュリティ対策が、組織が晒されるかもしれないあらゆるインサイダー脅威に対応していることが重要である。

３．人的セキュリティ・リスクアセスメント

２００６年の CPNI の人的セキュリティ調査によると、組織は、物理的・電子的セキュリティのリスクに取り組んでいるほど積極的には、人的セキュリティのリスクに取り組んでいない傾向にあることを示唆している。特定の人的セキュリティ対策を適用する明確な理論的根拠がしばしば薄弱であり、かつ、資源がバランスよく目標に配分されていない。一般に、セキュリティや人事部門の管理者は、彼らの組織に対するインサイダー・リスクに関する共通の認識を有しておらず、さらに、彼らは、上級管理者の関心を人的セキュリティの課題に向けることが難しいことさえ理解していない。



「人的セキュリティのリスクアセスメント」は CPNI のウェブサイトで入手可能である。

リスクマネージメントとは、組織が直面する人的セキュリティ・リスクを制御するための組織的プロセスである。リスクマネージメントは、全ての人的セキュリティ対策の基盤を提供する。また、それは、リスクアセスメント、実行、評価の継続した循環活動である。

- **リスクアセスメント**：組織に対するインサイダー・リスクは、特定のインサイダー攻撃の可能性と予想される結果の観点から評価される。
- **実行**：セキュリティ対策は、インサイダー攻撃の可能性と影響を受け入れられるレベルまで低減するために選定・実行される。
- **評価**：人的セキュリティ対策は、評価され、かつ、必要な是正処置が講ぜられる.

人的セキュリティ・リスクアセスメント

人的セキュリティのリスクアセスメントは、従業員の組織資産へのアクセスおよび従業員が組織や現行のセキュリティ対策へ及ぼすリスクに重点が置かれる。人的セキュリテ・リスクアセスメントのプロセスは、次のことに関して組織を支援する。

- 組織に対するインサイダー・リスクの優先順位の付与
- リスクを軽減する適切な対応策の選定

・　費用対効果およびリスク・レベルに応じた、人的セキュリティ資源の割当
・　インサイダー・リスクに関する上級管理者との意思疎通および対処の適正化

人的リスクアセスメントは組織、グループ、および個人の 3 つのレベルで実施される。組織レベルの評価は、全体として組織にとって懸念されるインサーダー脅威を特定し、優先順位を付与する。(図３) 特定した脅威を可能性と影響 (インパクト) について評価する。その評価により企業へのリスクが判定される。そして、このリスクに従って脅威の優先順位が付与される。

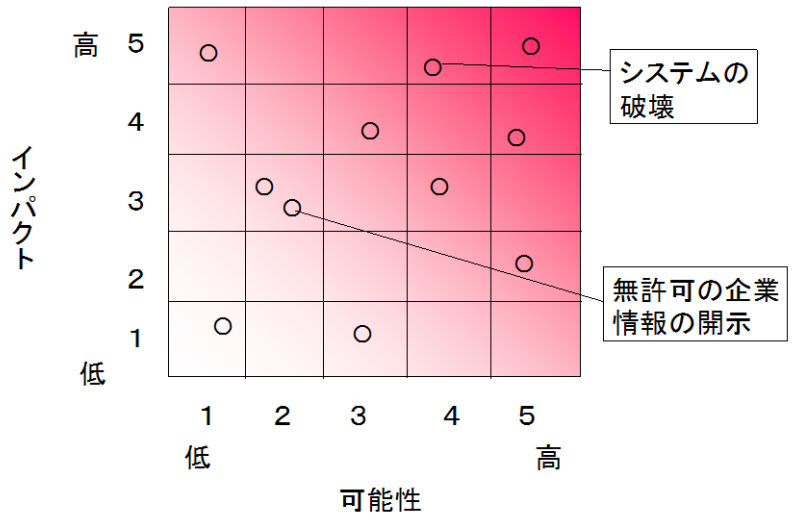


図３　脅威マトリックス（行列）は、無許可の会社情報の開示よりも IT システムの破壊のほうが会社により大きなリスクであることを分かりやすく図示している。

グループレベルの評価は、そのグループのアクセスと環境の脆弱性を考慮し、定義された脅威（犯罪）を犯す確率の高い従業員に焦点を当てる。その結果、リスクに応じたより効果的な対処策の実施と評価が可能となる。

個人レベルの評価は、彼らのインサイダー脅威および脆弱性、ならびに彼らが害を及ぼす可能性を基に、特定の個人によってもたらされる個別のインサイダーリスクを検討する。

人的セキュリティ・リスクアセスメントの方法論に関するより詳しいガイダンスは CPNI のホームページ（http://www.cpni.gov.uk/.）で入手可能である。

人的セキュリティ・リスクアセスメントは、あなたの組織でどの対策を講じるべきかについて助けとなるであろう。以下の各項で、これらの対策を概説するとともに、さらなる情報源を紹介する。

４．人的セキュリティの構造（フレームワーク）

下記に概説したフレームワークは、組織が人的セキュリティ体制を考案または見直しする際に考慮すべき様々な対策を列挙している。これらの対策が組織内で適用かつ実行される方法は、主として、人的セキュリティ・リスクの評価によって決まるであろう。

組織の人的セキュリティへの取り組みは、雇用前の審査からそれ以降の継続的な人的セキュリティ対策まで、従業員の雇用期間を通して、様々な段階での、様々な対策を包含する総合的なものでなければならない。

段階	人的セキュリティ対策		ツール、技術、サービスの例
採用時の人的セキュリティ対策	雇用前の調査	身分証明書	パスポートの調査
		労働権	入国身分の確認
		資格と履歴の調査	証明書の確認
		犯罪記録の調査	基本開示証明書（Basic Disclosure Certificate）
		財務調査	クレジット記録の調査
	国家安全保障審査(注２)		テロリスト審査（CTC）
	採用時のインサイダー脅威と脆弱性の評価		直接および間接の評価技術
雇用期間の人的セキュリティ対策	“操り工作”への対応		従業員啓発プログラム
	セキュリティ文化		セキュリティ問題の報告を促進する奨励策の採用
	アクセス管理	物理的および論理的アクセス権	IT ﾊﾟｽﾜｰﾄﾞ
	保護用監視	物理的アクセスおよび IT システムの監視	コンピュータを介した情報アクセスを監視
	捜査		犯罪に関する有効な証拠集め

表１　人的セキュリティの構造

注２：国家安全保障審査は　所管省庁の承認を得た特定のポストにのみ適用される。このポストは、本書では“ヴェターブル（vettable）”ポストと称される。

これらの対策のいずれを実行する場合も、組織は、本ガイダンスで後述するその他の一般的な原則のみならず、法的要件を考慮しなければならない。対策は、以下の各項でより詳細に述べられている。補足的助言が必要な場合は“追加ガイダンス”と“問合せ先窓口”から得られるであろう。

採用時の人的セキュリティ

採用と契約における人的セキュリティの主たる目的は次のとおりである。

・応募者が彼ら自身について真実かつ正確な情報を提供していることを確認する。
・採用された個人が雇用に必要な要件に合致していることを調査する。(例：就労可能な移住権の保有)
・採用された個人が組織に対してセキュリティ上の脅威をもたらしそうにないという追加的保証を得る。(例：彼は信用できる。)

リスク・アドバイス・グループ（The Risk Advisory Group：以下 TRAG という。）は、金融サービス分野の求職願書に添付された履歴書（CV：curriculum vitae）の２５％には重大な虚偽申告が含まれていると発表した。

“TRAG は２００５年に３，７００人の応募者からの履歴書を調査したところ、破産や群裁判所判決の記入漏れから試験の得点や職歴に関する明らかな虚偽記載に及ぶ虚偽申告を発見した。ガーデアン紙　２００６．１０．１０

挑戦はつまり、上述したようにセキュリティ規準を満たさない少数の個人を特定するために全ての応募者をふるいにかけることである。

雇用前の選別には次の３つのカテゴリーがある。

(1) 雇用前調査

雇用前調査では、応募者の資格を確認し、応募者が雇用条件に適合していることを確かめる。(例えば、その個人が法的に求職に応じることが許可されていること。　)

これらの調査を実行する間に、応募者が重要な情報を隠蔽していないか、さもなければ、自身を偽っていないかが明らかにならなければならない。この点から、雇用前調査は一種の人格テストであると考えられる。更に、誠実さあるいは信頼性の評価は国家安全保障審査や他の雇用選別方法によってより深くカバーされている。(下記参照)

（2）国家安全保障審査（National Security Vetting ：NSV）

国家安全保障審査の目的は、保護指定された資産への長期間、頻繁、無制限なアクセスを必要とするポストに就くためまたはテロリストからのリスクに晒されている人物、建物、もしくは情報へのアクセスに関わるポストに就くための個人の適合性を判定するものである。国家安全保障審査には、基本的な雇用前調査を基礎とし、警察記録の検索を含む追加のセキュリティ調査など様々な選別方法が含まれる。国家安全保障審査は特定のポスト（ヴェターブル・ポスト）にのみ有効であり、決して、適正な雇用前調査や継続した人的セキュリティへの総合的な取り組みの必要性を否定するものではない。

（3）その他の方法：個人のインサイダー脅威と脆弱性の評価

個人のインサイダー脅威と脆弱性の評価は、彼らの誠実さ、信頼性、および性格を評価しようとするものであり、１対１の面談や性格調査アンケートを含む幾つかの方式を取る。

ここで留意すべきことは、全ての組織が適切な基準で雇用前調査を実施すべきことと、国家安全保障審査がヴェターブルポストにのみ適用されることである。

雇用期間における人的セキュリティ

継続的な人的セキュリティに関する詳細なガイダンスは、２００８年に入手可能となるだろう。

過去２、３年に亘る CPNI と利害関係者との作業結果によって、国家インフラストラクチャーの多くで、雇用前審査が定着したにもかかわらず、採用後の人的セキュリティへ投入された時間と努力はかなり減少したことを示している。

雇用前審査は新規採用者に関しては大きな保証となるが、人的セキュリティ脅威に対する完全な解決とはならない。人間性と彼らの態度は、時間と共に、そして人生経験と生活上の出来事によって変わるものである。大部分のインサイダー行為が、組織に参加した時点ではその様な意図を持っていなかったが、採用後に組織への忠誠心と参加意欲が変化した従業員によって実行されたことを示す証拠がある。セキュリティはプロセスである。もし、組織がインサーダー脅威に対する脆弱性を縮小したいと考えるならば、人的セキュリティへの取り組みを本気で継続しなければならない。

５．法的要件

人的セキュリティには広範な法的問題が伴う。したがって、全ての対策が法律に準拠していることを保証するために、常に、法的助言を求めなければならない。

以下の表は、最も関連した法律の概要である。

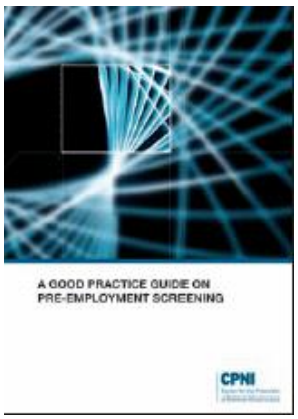
問題点	関連法律	適用	更なる情報
差別：一般	・1998 年イギリス人権法第 14 条 ・1950 年欧州人権条約（ECHR）	組織は差別禁止法律に従って行動しなければならない。	ビジネスリンク http://www.businesslink.gov.uk 欧州人権条約 http://www.echr.info/ 機会均等委員会 http://www.eoc.org.uk/Default.aspx?page=15498 公的セクター情報局 http://www.opsi.gov.uk/acts/acts 1996/1996018.htm
人　種	・1976 年改正人種関連法 ・2003 年人種関係法の修正規則 ・人種・民族による差別禁止に関する EU 指令 2000/43EC	組織は、国籍、出身民族、または皮膚色によって差別してはならない。	人種平等委員会 http://www.cre.gov.uk/legal/rra.html
性	・1975 年改正性差別禁止法 ・1970 年改正賃金平等法	組織は、性によって差別してはならない。	公的セクター情報局 http://www.opsi.gov.uk/si/ si2003/20031657.htm
宗教	・2003 年雇用均等（宗教または信条）規則	組織は、宗教または信条によって差別してはならない。	人種平等委員会 http://www.cre.gov.uk/legal/ rights religion.html
性的指向	・2003 年雇用均等（性的指向）規則	組織は、性的指向を理由に差別してはならない。	
年齢	・2006 年雇用均等（年齢）規則	組織は、年齢によって差別してはならない。	諮問・調停・仲介サービス http://www.acas.org.uk/index.aspx?articleid=350&detailid=1042

障害者	・1995 年改正障害者差別禁止法	組織は、従業員を、通常の日常の活動を妨げない如何なる身体的または精神的障害によって、差別してはならない。	英国政府刊行物発行所（HMSO） http://www.uk-legislation.hmso.gov.uk/acts/acts 1995/1995050.htm
犯罪歴	・1974 年犯罪更正法 ・1974 年犯罪更正法の 1975 年（例外）命令	組織は、“例外”命令が当てはまる組織以外は、個人の犯罪歴によって差別してはならない。	犯罪記録管理局 www.crb.gov.uk スコットランド情報開示機構 www.disclosurescotland.co.uk
移民	・1996 年亡命および移民法第 8 条 ・2006 年移民、亡命、および国籍法	外国籍の者を雇用する際には、その者が適正な労働権を保有していることを確かめなければならない。	移民および国籍局 www.ind.homeof.ce.gov.uk www.ind.homeof.ce.gov.uk/lawandpolicy/preventingillegalworking
個人情報の取扱い	・1998 年データ保護法 ・欧州理事会指令 95/46/EC	データは、 ・安全に保管され、 ・正確で、適量で、適切で、過剰でなく、 ・計画された目的のみに使用され、 ・適当な期間の後、削除され、 ・個人にとってアクセスしやすく、 なければならい。	個人情報保護委員会（ICO） www.ico.gov.uk ・民間セクター情報局 http://www.opsi.gov.uk/ACTS/ acts 1998/19980029.htm
保護用監視と捜査	・1998 年人権法 ・1950 年欧州人権条約	組織は、 ・個人の自由の権利（5 条）、 ・私的生活の権利（第 8 条） を侵害してはならない	民間セクター情報局 http://www.opsi.gov.uk/acts/acts 1998/19980042.htm
	・2000 年合法的な商慣行に関する規則	組織は、 ・個人の自由の権利（5 条）、 ・私的生活の権利（第 8 条） を侵害してはならない。	民間セクター情報局 http://www.opsi.gov.uk/si/si2000/ 20002699.htm

	・1998 年データ保護法(第３部:仕事中の監視　)	従業員の活動の監視（例:コンピュータの使用)は法律に従って実施されなければならない	個人情報委員会（ICO） http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/employment_practices_code/part_3-monitoring_at_work_1.html
	・2000 年捜査権限規制法（RIPA）	本条文の下で通信の傍受を実施する場合は、事前に特定の手順に従わなければならない。 捜査権規制法（RIPA）は、主として、第６条（２)に記載された公的機関に適用される。	民間セクター情報局 http://www.opsi.gov.uk/ACTS/acts2000/20000023.htm

６．雇用前調査

人的セキュリティは就職申込みから開始する。求職者は虚偽の情報を提出すること、または関連情報の開示を怠ることが、解雇の根拠となり、かつ、犯罪になることを知らされていなければならない。また、求職者には　如何なる求人においても雇用前調査の完了が条件となることが知らされていなければならない。もし、違法な活動に関連した不正な申込みがあると判断した場合は、組織は警察に通報しなければならない。



CPNI 発刊物（雇用前の選別ガイド）を参照

雇用前調査は、組織によって直接実施されるかまたは第３者との下請契約となるであろう。いずれにせよ、会社は、雇用を拒否するための敷居（threshold）を明確に理解する必要がある。 例えば、求職者はどの様な場合に前科を理由に申込みを拒絶されるのか、それは何故か？

身元（身分）確認

全ての雇用前調査の中で、身元確認は最も基本的なことである。次の２つのアプローチが使用される。

- 主要な身元証明書の確認およびこれらの文書と個人の照合を含む書類に基づくアプローチ
- その個人の電子的足跡（electronic footprint）を補足・確立するためのデータベース（クレジット契約または電子選挙人名簿のデータベース）の検索を含む電子的アプローチ。そして、その個人は、本人のみが正しく応えられる電子的足跡に関する質問に答えなければならない。

労働権：国籍および滞在資格

次の場合を除いては、１９９６年亡命および移民法（第８条）の下では、１６歳未満または１６歳以上であっても出入国管理の対象となる者を雇用することは犯罪となる。

・ その個人が政府によって英国滞在が認められており、かつ当該の仕事に就くことが許可されている。または、その個人が雇用を許可された分類に入る。

・ （亡命および移民法の）第８条は、もし、雇い主が、従業員が所有する特定の文書を調査・記録しているならば、雇い主に対し法的保護を提供する。法的保護を獲得するためには、これらの調査はその個人が雇用される前に実施されなければならない。

資格および職歴

資格と職歴の確認は、禁固刑または解雇などの否定的な情報を隠そうとする応募者を特定するのを手助けする。説明のできない相違は調査されなければならない。

資格

ある会計係が国家インフラストラクチャー組織から金銭を詐取していることが発覚した。この事件の捜査で、この人物は全く資格がなく、さらに面接で教育資格について嘘をついていたことが判明した。

資格について詳細を確認する際に、次のことはいつも重要なことである
・そのポストが資格調査を必要としているかを考慮する。
・いつも、証明書の原本を要求し、それをコピーする。
・証明書などの詳細と応募者が提出したものと比較する。
・個人から提供された詳細を確認するために、独自に、（証明書に記載された）学校、会社などが存在するかを確認し、それらと接触する。

職歴調査

法的理由により、人物証明書（character reference）を入手することは益々難しくなっている。しかし、雇用期間を確認するために過去の雇い主に尋ねるべきである。職歴調査を実施する際は、次のことが重要である。

・5 年間が望ましいが、最低 3 年間の職歴を調査する。
・独自に、雇い主の存在を確認し、（ライン管理者を含む）詳細を知る人物と接触する。
・人事部門に詳細（日付、配置、給料）を確認する

・可能ならば、ライン管理者から雇い主としての意見・評価を求める。

有罪判決（前科）

有罪判決は、執行の終了または未了であっても、必ずしも、雇用の障害とはならない。（犯罪者更正法参照）しかし、犯罪歴の種類によっては、受け入れられない特定のポストがある。前科情報を入手するため、会社は応募者に次の何れかを要求することができる。

① 前科自己申告用紙への記入。
② 基本開示証明書（Basic Disclosure certificate）をスコットランド情報開示機構に要求する。

財務調査

幾つかのポスト、例えば、従業員のポストが金銭を扱うことが必要な場合は財務調査を行うことが正当と認められている。セキュリティと財務歴との相関を解釈することは容易ではない。各組織は、それぞれの組織の敷居（例えば、受け入れられる借金のレベル）を決定することが求められる。

財務調査を実施することができる幾つかの方法がある。一般申込み用紙に自己申告の項目を入れることができる。（例えば、郡裁判所の判決に関するもの。）あるいは第３者の情報提供サービス機関に信用調査を委託する。

契約社員の採用

組織は、IT スタッフ、清掃作業員、管理コンサルタントなどの多種多様な契約社員を雇用している。契約社員に対して、会社資産（建物、システム、情報、または職員）へのアクセス権を付与する場合は、同等レベルのアクセス権を有する正社員と同等レベルの雇用前調査が確実に実施されることが重要である。

契約社員にはそれぞれのポストに必要な調査の種類が説明されなければならない。また、その調査はどんな下請契約にも適用されなければならない。契約社員または調査機関が調

査を実施した場合は、会計監査を受けなければならない。(契約社員に関する追加のガイダンスについては“安全な契約”の項を参照)

海外調査

外注のレベルが高くなり、また、国家インフラストラクチャーで働く外国人の急増に伴い、海外で生活し、働いていたことのある応募者の選別がますます重要となった。組織は、可能な限り、海外からの応募者に関しても、長年英国に在住している応募者と同じ情報（例：居住証明、雇用照会、犯罪歴）を収集しなければならない。しかし、他国には、人的セキュリティを管理するための必要情報の収集について、英国とは異なる法律や規制上の要求事項があることに留意しなければならない。従って、このステップは難しいものとなるだろう。

海外調査の実施を望む組織にはいくつかの可能な選択肢がある。

① 応募者に書類を要求する。
② 専門的/外部の調査サービスを雇う。
③ 組織自ら海外調査を実施する。

状況によっては、十分な海外調査が出来ないかもしれない。(例：他国から入手できる情報が少ない。）この場合、雇用しないか、または、確信の不足を補うために別のリスクマネージメントを実行することを決心することになるだろう。

７．国家安全保障審査（National Security Vetting：NSV）

国家安全保障審査プロセスは特定のヴェターブル・ポストに適用される。そのポストには、秘密に指定された政府情報へのアクセス権、テロリスト攻撃の潜在的目標、および/またはテロリストに役に立つ情報へのアクセス権が付与される。首相の“英国政府の審査政策声明”（１９９４）は、国家安全保障審査の政策と手順を定めている。

国家安全保障審査の対象者は、セキュリティアンケート（Security Questionnaire ：SQ）を終了していることが前提である。審査の種類とレベルは必要なクリアランス（秘密情報取扱資格）のレベルにより異なる。審査には、秘密に指定された国家情報へのアクセスのための審査（例えば、高度審査（Developed Vetting：DV）やセキュリティ調査（Security Check：SC）など）とテロリストに役立つ情報へのアクセスのためのテロリスト対策調査（Counter Terrorist Check：CTC）がある。全ての国家安全保障審査（NSV）は、それが正社員または契約社員のものであっても、政府の省もしくは庁、またはセキュリティ取締機関によって支援されなければならない。　彼らはどのポストが高度審査（DV）、セキュリティ調査（SC）、および/またはテロリスト対策調査（CTC）の対象になるかの基準を決定する

審査対象者が警察または英国情報局保安部の記録に現われないという事実は、彼らが必ずしも信頼できるということを意味しない。彼らの身元が最初に確認されない限り、如何なる審査も意味を持たない。

国家安全保障審査（NSV）は、総体的な人的セキュリティ体制の代替ではない。従業員が国家安全保障審査（NSV）のクリアランスを保持しているという脈絡において、継続的な人的セキュリティの管理が不可欠である。

８・インサイダー脅威と脆弱性の評価

人的セキュリティの最も挑戦的な側面は、組織に対しインサイダー脅威となる人物、および将来インサイダーになりやすい人物を特定することである。これは非常に難しい問題である。この種の評価あるいは“選別（screening）”を実行するための実用的かつ信頼できる技術が不足している。CPNI は、この分野の研究に関する重要なプログラムを有しているが、現時点では、組織が考慮できる取り組み方法および適正な実践を支える原則に関する一般的な説明しか出来ない。

原則

選別は、技術的に複雑で、資源集約的で、そして重大な影響をもたらす可能性のある威圧的活動である。従って、いかなる選別法であっても以下の原則を順守すべきことが肝要である。

- 適法性：いかなる選別法であっても、雇用と差別に関する法律に定められた基準に適合しなければならない。

- 倫理：選別は英国心理学会の心理テスト適性実施基準（Code of Good Practice：CGP）の様な広くよく知られた基準に従って、専門的に実施されなければならない。

- 科学的根拠：いかなる選別技術の使用でも、その有効性を根拠としなければならない。選別プロセスで使用されるどんな指標も、その指標とセキュリティ懸念の関連についての厳格な分析に基づいたものでなければならない。

- 均衡：そのプロセスは、その手段・処置が、仕事により与えられる機会および/または従業員に対する懸念のレベルと均衡していることを保証しなければならない。

- 有用性：選別プロセスには目的に適合したプロセスとツールが含まれなければならない。

- 費用対効果：活動は投資の価値に見合うものでなければならない。

- 実用性：プロセスとツールは、時間と資源の制約の中でも実行できるものでなければならない。

・　透明性：どの選別プロセスも、プロセスの実行またはプロセスに基づく意志決定に関連する者全てに、眼に見えかつ理解されているものでなければならない。

2 段階アプローチ

インサイダー脅威と脆弱性の選別は、セキュリティ脅威の懸念を示す個人を特定し、そして、次にその懸念が実際に根拠のあるものかどうかを判断するという 2 段階のプロセスと見ることができる。第 1 段階で使用される技術は、全ての求職者または全ての従業員に適用されるものなので、多数の者に適したものでなければならない。第 2 段階で使用される技術は、懸念の持たれる少数の個人を対象としたものとなるであろう。

この 2 段階アプローチは、採用時と継続的な人的セキュリティの両方に適用される。両方の場合とも、測定可能な指標と評価方法が必要である。指標とは、（インサイダー脅威または脆弱性のような）特定のセキュリティ懸念と明確な関連のある行動と特性である。評価方法には、指標を測定するツールまたは報告するツールが含まれる。例えば、偽りを見つけるための効果的な個人との面接技術、性格アンケート、または内部告発システムなどである。

指　標

活発なインサイダーを確実に暴露する指標を特定することは難しい。さらに、将来のインサイダーを判別する指標を見つけることは一層難しい。これまでの研究によると、インサイダーの人格、動機、および行動は様々である。特定のインサイダーの行動（例えば、機微な情報の開示）は、生活経験、労働環境、および人格などの多くの要素の複雑な混合によって成り立っていることを示している。

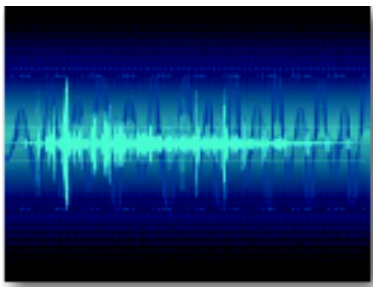
インサイダーに関する信頼できる統計データはなく、さらに、指標に関する継続中の研究も近い将来に正確で信頼できる測定ツールをもたらしそうにない。しかし、疑惑を特定・解明することができる指標のリストを提供することは出来そうである。雇い主は、採用時および継続した人的セキュリティ履行の過程で、従業員の行動と性格を判断するためにチェックリストを使用する。換言すれば、指標のいずれか一つをもってインサイダー行動を予測することはできない。チェックリスト、即ち複数の指標によって、雇い主は潜在的に重要な行動と特性を感知することができる。

インサイダーに対する脆弱性の指標と、インサイダー脅威の指標とは違うものであろう。

しかし、インサイダー脅威か脆弱性かどちらかだけの指標は一つもない。また、孤立した指標はどれ一つとして意味をなさないであろう。特定の対象者または従業員が見せる指標が多ければ多いほど、疑惑はますます正当化されるであろう。

評価技術

個々のインサイダー脅威を評価するために使用される技術の種類は様々である。幾つかの技術は、疑惑を特定する初期のプロセスに適している。例えば、性格アンケートは比較的簡単に多数に実施することができるし、採点と分析を自動化することができる。対照的に、他の方式（面談は一つの明白な例であるが、嘘発見器はもう一つの例であろう。）は、対面のやりとりが必要であり、そのため、一人ずつ、特定の個人に適用される。



現在使用可能なツールはすべて、信頼性と有効性の欠落、対抗策に対する脆弱性（個人が偽って前向きな姿勢で自己紹介するなど)、および実用性の問題によって限定されている。懸念を特定するための最初のフィルターとして使用される応用技術がより遠隔で、より大量であればあるほど、さらなる調査とこれらの懸念を解決するために、ますますより多くの標的化技術（targeted techniques）が必要となる。このために効果的な選別には複数の方式の混合が用いられるであろう。

９．セキュリティ文化

組織の文化は、セキュリティにとって重要な意味合いを持っている。優れた人的セキュリティのツールと技術をもってしても、もし、セキュリティ文化が貧弱であるならば、組織はインサイダー脅威に対し脆弱である。

セキュリティ文化とは、組織のセキュリティに強い影響を与える態度と行動、特に、組織全体に広く、深く根付いた態度と行動である。例えば、

・セキュリティが重要であり従業員の責任の中で最も重要な要素であるという心の持ち方が従業員に浸透しているならば、その様な心の持ち方が確立していない組織より、より安全な組織であろう。

・セキュリティ違反報告が当然視されている組織は、セキュリティ違反の報告が確実におこなわれない組織やセキュリティ違反の報告が従業員の間に大きな緊張を引き起こす組織より、より安全な組織であろう。

優れたセキュリティ文化の特性

事例報告は、効果的なセキュリティ文化が次のような特質を有していることを示唆している。

- **認識**：組織のセキュリティ・リスクが広く理解され、かつ従業員に受け入れられている。リスクに対する理解はバランスしており、パラノイア（被害妄想）を回避している。

- **オーナーシップ（帰属意識）**：セキュリティは組織の業務の重な一部であると見られており、かつ、従業員は、組織の一員である自分にとって、セキュリティは重要な責任であると考えている。

- **報告**：セキュリティ違反は確実に報告され、そして報告することは当然のことと受け入れられ、かつ組織における業務の一面であると受け入れられている。

- **コンプライアンス（遵法精神）：**組織全体に、セキュリティ施策・手順に対する高いレベルのコンプライアンスが存在する。（例えば、常に、パスワードの変更と身分証明書の提示がなされている。）

- **規律：**機微な情報またはアクセスは、明確な必要性がない限り提供されない。

- **警戒心：**ある従業員がセキュリティ慣行（例：身分証の提示）に従わない場合は、他の従業員から尋問される。

効果的なセキュリティ文化を持っている組織は､次を強調する傾向があるように見える。

- **コミュニケーション（意思疎通）：**組織のセキュリティ手順の正当性が、入社研修時および入社後も定期的に明確に伝えられる。また、セキュリティ問題に関する議論が奨励され、かつ積極的な討議がなされる。

- **上級者の支援：**上級管理者が組織のセキュリティ対策に高い価値を置いていることが組織全体で理解されている。

- **厳格な懲戒手順　：**セキュリティ違反が既定の指針に基づき一貫して、かつ厳格に処理される。

- **インセンティブ（褒賞）の提供**：セキュリティ懸念の報告と同様に、セキュリティ改善アイデアの創出も報いられる。

１０．操り工作（マニピュレーション）への対応

ソーシャルエンジニアリング(social engineering)は、組織の部内者もしくは部外者が、情報を取得するため、またはアクセス資格がないものにアクセスするために、従業員を操ろうとするプロセスの一般的な呼称である。全ての従業員は、彼ら自身と組織を守るために、ソーシャルエンジニアリングを理解し、警戒するよう訓練されていなければならない。

ソーシャルエンジニアリングとはどの様な活動か。

熟練したソーシャルエンジニア（social engineer）は、組織の専門用語と編成について事前にたくさん勉強するなど周到に準備する。ソーシャルエンジニアリング工作では、一瞬たりとも、たった一人の従業員に対しても直接の質問もせずに、情報を引き出す巧妙な手段が使用されるであろう。その技術は、例えば、好意から恩返しをしたいまたは困っている同僚を手助けしたいというような人間の基本的な性向を利用するなど、しばしば、非常に単純である。しかし、熟練したコミュニケーター（communicator）は、それらの技術を使用することにより、組織に大きな損害を与えるであろう。

例えば、同僚、新入社員、配達人、もしくは作業員に成り済まし、またはパスワードを紛失したと偽ったりしながら、ソーシャルエンジニアは次のことを行う。

・断片的な情報を入手しようとする。

・長期間に亘り、異なる複数の従業員を標的とする。

・僅かな親切や好意を求める。

・一見無害な会話から情報を入手する。

断片情報は、バラバラでは役に立たず、かつ機微なものでもないが、集まると非常に価値あるものとなる。ソーシャルエンジニアは、公然か、より巧妙かどちらかの幾つかの異なる方法を採用するであろう。次は協力を得るために使用される良く知られた技術である。

.

- **権限**：権力を有する人からの要求には応じるという性向を利用するために、先任であることまたは専門家であることを強調する。

- **慣習への服従（Conformity）：**他の同僚が以前、情報を提供したことまたはアクセスが認められたことを述べることにより今回の（情報）要求を正当化する。

- **趣味：**友好関係を築くために共通の趣味に焦点をあてることにより、友人を支援しようとする性向を利用する。

- **互恵主義：**標的に与えた援助を強調する。そして、恩義に報いようとする義務感を利用する

- **一貫性：**過去に標的が（要求に）応じたことを指摘し、過去の行動と一致した行動でなくてはならないことを強調する。

これらの方法は､必要な情報を入手するために､公然とまたは暗黙のうちに用いられる。一般に､次のような異なる方法を使うことにより､(標的に対し）いかなる直接の質問をせず標的が情報を提供するように仕向ける。

- **報告された事実の引用：**もし、情報の特定の部分が既に公知されているならば、他を議論することは有害でないという見解を利用する。

- **誤った声明（発言）：**手助けであろうと、個人の地位または自尊心を高めるものであろうと、話し手の間違いを正すという自然の性向を利用する。

- **偽りの懐疑心：**話し手が話したことまたは彼らが関連していることの有効性や真実を証明したいという性向を利用する。

- **偽りの無知：**知識の不足している人々を教えたい、または知識を与えたいという自然の性向を利用する。

その他の技術には、繰り返し有名人が自分の知人であるように見せかけたり、急いでいるように見せかけるなどが含まれる。単純なお世辞が、標的がそれと知っていたとしても、いまだに人々から話を引き出す有効なツールであることを再認識することは重要である。特に、これは人を助けることを訓練された職員に当てはまることであろう。（例：受付係や IT 支援スタッフ）

セキュリティ対策

ソーシャルエンジニアリングに対する脆弱性を縮小させるために、組織が導入できるいくつかのセキュリティ対策がある。

- 効果的なセキュリティ文化は、操り工作（マニピュレーション）に対抗するための主要な要素である。とりわけ、情報を提供する前に質問者の信用（例えば、身分証明書、雇用資格、またはアクセス権）をチェックするという手順を従業員に徹底させたり、訪問者が詳細な身元情報を提供することを拒否するなどの兆候に対して注意を喚起させたりするのがセキュリティ文化である。

- 自己主張の訓練は大きな効果をもたらすことが出来る。具体的には、他人に“ノー”と言える個人の能力を開発することである。

- 従業員を保護する最良の方法は、主として、脆弱であると考えられるポストに配置される従業員を重点に、異なる種類のソーシャルエンジニアリングについて教育することである。

１１．アクセス管理

“アクセス管理”とは、妨害から組織の物理的資産と IT 資産を保護するために組織によって実行される方策とプロセス—手動または自動化—の総称である。

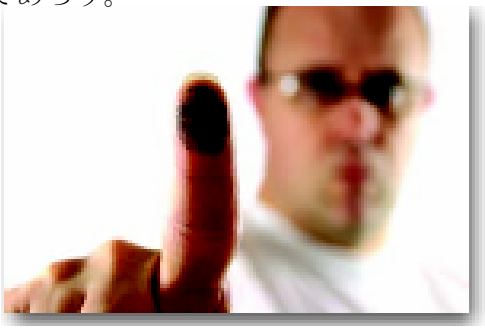
組織資産へのアクセスは“最小特権の原則”（時には“Need to Know 原則”と呼ばれる。）によって管理・運営されなければならない。“最小特権の原則”では、従業員には仕事を効果的に遂行するために必要なレベルの、決してそれ以上のものでないアクセス権が付与されることが厳しく求められている。物理的セキュリティおよび IT セキュリティ双方のアクセス許可範囲は、仕事の役割のレベルに応じ使いやすく定義され、「人的セキュリティ・リスクマネージメント計画」によって通知される。

IT 資源と建物双方への従業員のアクセス権は、役割と責任の変更の都度見直されなければならない。新しい役割に伴って新しい許可を付与すると同時に、もはや必要でなくなれば、現在付与されているアクセス権は縮小されるかまたは取り消されなければならない。組織を去ると同時に、従業員の組織へのアクセス権は直ちに無効とされなければならない。

これを達成するために、組織のアクセス管理施策において、人事、セキュリティ、および IT システム管理などの主要な部門へ通知する責任と報告時期が明確に定められていなければならない。

物理的アクセス

立入許可証（セキュリティパス）は適切な許可を有する個人のみが組織の建物にアクセスできることを保証するために使用されるべきである。各々の仕事の役割の必要に応じてアクセスを制限するために、立入許可証は、組織のサイズまたはその業務の秘匿レベルに応じて、プログラムされるかまたは色分けされなければならない。例えば、上級管理者はあらゆる事務所へのアクセスが必要であるが IT サービスルームへのアクセスは必要ないであろう。



立入許可証は、全ての従業員から目に見えるように身に付けられ、そして、理想的にはせいぜい５年以内の正面を向いた顔写真が貼付されていなければならない。また、立入許可証には、その着用者がその建物またはその部門に立入ることが適切であるかどうかを他の従業員が判断

するのを助けるため、秘密取扱資格（クリアランス）のレベルまたは組織のセキュリティに関連する他の情報が表示される。立入許可証を着用していないものは誰でも尋問されるかまたは関連する管理部門へ通報されなければならない。

立入許可証には、アクセスが許可された建物または組織を、部外者に察知されるいかなる情報も記載してはならない。組織は、紛失した時に戻ってくる可能性を高めるために、立入許可証に印刷できる私書箱を設置することを検討しなければならない

アクセスレベルの変更と同じように、立入許可証の発行は、二重発行または混乱の可能性を低減するために唯一の場所または部門で統制されなければならない。従業員のアクセス権の変更は､組織のアクセス管理規則に規定された時間内に処理されなければならない。従業員の組織内の地域または建物全部へのアクセス権が取消された場合は、破壊活動を含むセキュリティ違反の可能性を局限するために直ちに変更が実行なされなければならない。

よりセンシティブな地区では、立入許可証の所持者だけが知っている PIN 番号（暗証番号）の入力を義務付けることが必要であろう。更に、その様な地域への出入りに関する無作為検査が必要である。しかし、その様な威圧的な措置の必要性については全ての関係者に明確に説明されていなければならない。この場合もまた、強固なセキュリティ文化が理解と協力を促進するのを手助けするであろう。

IT システムアクセス

物理的アクセス管理と同じように、組織の IT 資源へのアクセス権も、唯一、仕事が必要とするレベルに基づき付与されなければならない。

システム利用者に付与したアクセス権の変更と同じように、パスワード（暗証番号）は、注意深く統制されなければならない。そして、理想的には唯一の場所または唯一の部門で取り扱われるべきであろう。IT アクセスのレベルの変更は、組織のアクセス管理規則に定められた時間内に処理されなければならない。また、従業員の特定システムまたは IT 資源全体へのアクセス権が取消された場合は、セキュリティ違反の可能性を局限するために変更は迅速に実行されなければならない。

たった一つのソフトウエア・パッケージまたはパッケージ・ソフト（マイクロソフト・オフィスなど）へのアクセスによって、他の従業員が作成した文書を閲覧することが可能であるので、より機微な文書を保護するためにパスワードの使用が考慮されなければならない。

組織の性格あるいは取扱う情報に応じて､非常に機微な情報または異なる部門が所有する文書を保護するために、ソフトウエア・プライバシー・ウォール（個人用ファィアウォール）または別々のサーバーが必要となるであろう。組織の IT 資源にアクセスするための PIN 番号またはパスワードと同じように､（磁気カードのような）トークン（token）を使用する認証システムのような追加的措置がシステムまたは情報の保護に役立つであろう。

全ての組織は、組織の IT 資源に対するリモートアクセスを減少するために、機微な情報をインターネットから分離すべきである。これらの対策は、ソフトウエアの監視やファィアウォールのような保護デバイスの使用から、インターネットや組織自身の情報資産に接続しない独立したサーバーの使用に及ぶであろう。

１２．保護用監視

保護用監視活動は、防御を透過しようとする試みを特定することを目的とする。
保護用監視活動は通常、IT 資源の保護と関係しているが、その原則は同様に、物理的アクセスの制限のためにも適用できる。

物理的アクセス

立入許可証（セキュリティパス）が発行されたならば、従業員による立入許可証の使用は監視されなければならない。最も基本的なレベルでは、全ての従業員は、特に管理職にあるものには同僚の無許可のアクセスの試みに注意することが要求される。

建物全体で電子セキュリティ・ロックを使用する組織では、それぞれの保護された出入口での立入許可証の使用と使用の試みを記録するために、通常自動化された監査報告が作成される。捜査が必要なセキュリティ違反が発生した場合は、これら（監査報告）が過去に遡って調査されるであろう。しかしながら、組織の資産の秘匿度によっては、リアルタイム警報を発するようプログラムするかまたは許可レベルを超えてアクセスしようとする試みを発見するために少なくとも定期的に監査報告を調査すべきであろう。

さらに、監視カメラシステム（CCTV）のような保護用監視手段を、監視レベルを高めるために必要に応じて使用すべきである。いずれの追加的対策も従業員の異常な行為を特定する可能性を高めることができる。

IT システムへのアクセス

組織の IT 資源は、無許可のアクセスを探知する仕組み（メカニズム）によって保護されなければならない。無許可のアクセスには、例えば、無許可のハードウエアの取付け、USB ポートもしくは CDROM ドライブによる無許可のソフトウエアの挿入、または従業員による彼らの権限を越えた文書もしくはシステムへのアクセスの企てのような直接的な侵入が含まれる。

規模とアーキテクチャ(基本設計概念)にもよるが、IT ネットワークに挿入された新しいハードウエア装置またはソフトウエアを発見することは非常に難しいが、独立型コンピュータでこれを達成することは非常に容易である。しかし、これは当然リモート・アクセスでなくローカル・アクセスの発見である。物理的アクセスの監視と同じように、全ての従業員、特に管理職にあるものは同僚による無許可の行動が特定でき、そして、直ちに尋問が出来なければならない。

独立型コンピュータやネットワークに悪質なソフトウエアが挿入される可能性を低減するために、幾つかの緊急の処置を取ることができる。例えば、USB または CD ROM の機能を無効にするような処置である。多くのセキュリティ対策と同じように、この種の制約ソフトが実装される場合は、組織が直面しているリスクと正当な使用者が被る不便さがバランスされていなければならない。

ソフトウエア・アプリケーションによって、従業員による組織のシステムの使用を詳細に監視することが可能である。この様なソフトがインストールされた場合には、承認されたレベルを超える文書またはシステムへの度重なるアクセスの試みなどの使用者の異常な行動を発見するために自動監査記録が定期的に点検されなければならない。

いくつかのケースでは、特定の仕事のためのシステムへのアクセスのプロファイル（図表）を時間をかけて作成するのと同じソフトウエア・ソリューション（解決法）を使用することが出来る。即ち、このプロファイルを逸脱した行動を探知することが出来る。可能ならば、リアルタイムの警報を IT システム管理者に提供できる探知システムがプログラムされるべきである。そうすることにより、セキュリティ・リスクを軽減するための処置を迅速に講ずることができる。

従業員に関する情報のどのような記録でも、データ保護法パート３に基づき実施されなければならないことを覚えておくことは重要である。法律は、仕事中の監視を禁止していない。しかし、法律は、（監視するという）威圧的行為を、雇い主が、雇い主の利益または他の利益の観点から正当化することを求めている。さらに、法律は公開性を求めている。非公然の監視が例外的に正当化された場合を除き、どんな監視であっても労働者にはその性格・範囲・理由が知らされなければならない。

１３．捜　査

セキュリティ違反疑惑または不正行為に関する報告は、従業員通報ホットライン、管理者による観察、自動警報システムなどの幾つかの情報源から寄せられる。悪意のある報告または偽りの報告は常識で判断できるが、万一、報告が事実であるようであれば、組織は、従業員の健全性と監視手順の有用性を確認するために、迅速に行動を取らなければならない。

セキュリティ違反疑惑または不正行為は直ちに既定の手続きに従って適切な部門へ通知されなければならない。多くの組織においては、それは人事またはセキュリティ部門であろう。そして、事件の性質および入手した情報もしくは証拠を踏まえて如何に捜査するか、または捜査するか否かが決定される。

原則

どのケースも状況は異なるので、如何に捜査を進められるかを詳しく述べることは難しい。しかし、常に適用できる幾つかの一般的原則が存在する。

- もし、関係する従業員が存在する場合は、違反の性格によっては、当該従業員に捜査のことを知らせるべきか否かを考慮しなければならない。

- 違反事案の多くは単純な原因によって引き起こされていることを忘れてはならない。可能ならば、従業員に彼らの行動を説明する機会を与えなければならない。

- 問題を迅速に取り組まなければならない。

- 出来るだけ沢山証拠を集めるとともに、必要なら、目撃者が名乗り出るよう奨励しなければならない。

- 刑事犯罪の証拠は、できるだけ早い機会に、警察に通報されなければならない。

- 証拠の収集を含む全ての捜査活動は、後に起訴することを想定し、法廷での証拠能力に関する法的要件に基づき実施されなければならない。

- 捜査が職場に及ぼす悪影響に注意しなければならない。

１４．安全な契約

契約社員は、特殊な人的セキュリティ上の挑戦となっている。例えば、契約社員の雇用期間は比較的短いので、セキュリティ契約が曖昧だったり、いい加減だったりする大きな可能性がある。（例えば、更なる下請け業務）

契約社員に関連したインサイダー・リスクを管理するために次のことは重要である。

- 正規従業員と同じ基準の雇用前調査を実施すること。厳格な締切りまたは背景調査のための有効情報の欠如によって、雇用前調査が実施できず、結果として生じたリスクは効果的に管理されなければならない。どんな追加的セキュリティ対策の実行であっても、人的セキュリティ・リスクアセスメントに基づくものが好ましい。

- 雇用前調査または他の人的セキュリティ対策が、雇用側機関よりむしろ契約代理店で実施される場合は、両者で作成する契約書には、調査に関する詳細な説明が記載されなければならない。さらに、契約代理店によって実施される雇用前調査は定期的に監査されなければならない。

- 仕事に来ている人物が、契約業者から派遣された人物であることを確認する。（例えば文書による確認または電子的身元調査サービス（electronic identity checking service）の利用）

契約社員が組織内で仕事を開始したら、直ちに彼らはセキュリティ上、管理されなければならない。次の処置が手助けとなる。

- ポストで悪意を持って行動している契約社員に関連する脅威とリスクのレベルを判断するためにリスクアセスメントを実施する。

- 雇用側機関と契約社員との契約書または雇用側機関と契約代理店との契約書のどちらかに、順守すべき業務実施規則および基準が定められていることを確認する。

- 顔写真付入門証（photo pass）を契約社員と代理店のスタッフに提供する。そして常時着用を義務付ける。理想的には、契約社員の訪問と訪問の間、彼らの入門証は雇用側機関で保管する。そして、契約社員が再び訪問する際は、当該契約社員の身元確認がなされた後でのみ毎回再発行される。

・　雇用側機関と契約代理店（もし、代理店が関与していない場合は、契約社員）は、当該契約社員が働けない場合に一時的な交代要員を提供する手続きに合意すべきである。これらの協定は契約書に組み入れられるべきである。そして、雇用側機関は如何なる追加的人的セキュリティ対策（例えば、交代者が現場にいる場合のアクセスの制限または監視）を実施すべきかを決定する必要がある。

・　契約社員の必要な雇用前調査が実施されていないかまたは調査の結果が完全には肯定的でない場合であっても、契約社員の専門的知識・技能が必要であるために雇用された場合は、当該契約社員に対する追加的人的セキュリティ対策が考慮されなければならない。（例：監視の継続）

１５．有用な問合せ窓口

一般情報

・ www.cpni.gov.uk　国家インフラストクチャー保護センター：人的・物理的・電子的セキュリティの様々な側面に関する助言を提供する。

・ www.berr.gov.uk　商務企業規制改革省（旧貿易通産省）

・ www.cipd.co.uk　人材能力開発研究所(CIPD)は、人間の管理と開発に関する専門家協会であり、雇用法、裁判、経歴管理、内部告発を含む人事と人的資源の広範な問題に関する有用なガイダンスを提供する。

・ www.bsi-global.com　英国規格協会（BSI）は、セキュリティ幹部の雇用前選抜の実施基準である BS７８５８：２００４を開発した。

安全な採用

次のウェブサイトは労働権、身元調査、ならびになりすまし犯罪および身分詐称の防止に関する情報とガイダンスを提供する。

身元（身分）確認

・ www.idfraudpreventiontraining.com　クレジット（信用販売）不正使用防止組織（CIFAS）と連携し、「身分詐称防止訓練」は身分詐称について助言する。―（英国マニュアル）

・ www.apacs.org.uk　銀行共同支払決済機構（APACS）は顧客に支払サービスを提供する機関の為の英国同業者組合である。サイトには支払い詐偽（クレジットカード、小切手、オンライン、身分詐称を含む）およびそれを如何に防止するかに関する情報が含まれる。

・ Employers' Helpline - 0845 010 6677：身元確認のために提出された文書の有効性に

懸念があるならば、雇い主支援ラインは更なる支援を提供することができる。

労働権

・ www.ind.homeof.ce.gov.uk　内務省・移民国籍局（NID）、国境移民局（BIA）の別名でも知られる。不当な差別を回避するための、「1996 年亡命および移民法」セクション８に関する政府の実施基準のコピーは次の URL からダウンロードできる。
www.ind.homeof.ce.gov.uk/lawandpolicypreventingillegalworking

・ www.workingintheuk.gov.uk　本ウェブサイト（Working in the UK）の目的は、英国で働くことを望む外国人に開かれている様々なルートに関する情報を提供することである。

・ www.employingmigrantworkers.org.uk　出稼ぎ労働者の雇用に関するオンラインガイド

・ The HM Revenue and Customs website (www.hmrc.gov.uk)　英国歳入税関庁ウェッブサイトは労働権に関する更なる情報を提供する。

職歴

・ www.businesslink.gov.uk　ビジネスリンクは雇い主に　雇用前調査を含む雇用の助言ならびに信用照会先および資格調査に関する助言を提供する。

・ www.companieshouse.gov.uk　貿易産業省・企業設立関係局ウェブサイトは、会社の経営状態の調査および雇用に関する特定の側面（資格剥奪等）を確認するのを手助けする。

・ www.holdthefrontpage.co.uk/peoplesearch　ウェブサイト「ホールド・ザ・フロントページ」では、ジャーナリストとカメラマンについて検索できる。

有罪判決（前科）

・ www.crb.gov.uk　内務省・犯罪記録管理局（CRB）はイングランドとウェールズに亘る犯罪記録調査の問合せに応じる。

- www.disclosurescotland.co.uk　スコットランド犯罪記録管理局の一部であるスコットランド情報開示（官民提携）機構（Disclosure Scotland）は犯罪記録調査の問合せに応じる。

- 適用除外ポストの全リストは犯罪記録管理局のウェブサイト、www.crb.gov.uk or の“アクセスカテゴリーコード開示”の下の図書資源（Resource Library）から、または犯罪記録管理局の問合せライン 0870909811 に連絡することにより入手できる。

- 犯罪記録の取得費用は開示レベルによって異なる。雇い主は、費用がもし必要ならば、その費用はすぐに支払が必要か、または採用後応募者が自ら支払うかについて、事前に応募者に忠告しなければならない。更なる詳細情報は、www.crb.gov.uk と www.disclosurescotland.co.uk から入手できる。基本開示証明書（Basic Disclosure Certificate）はオンライン
- www.disclosurescotland.co.uk で利用できる。

- www.the-sia.org.uk　民間警備業機構（SIA）ウェブサイトは、とりわけ海外犯罪記録調査に関する助言とガイダンスを提供する。(“海外居住者”に関連した資料を発見するために検索機能を使用する。)

信用調査

次は信用調査の問合せ機関である。

- www.experian.co.uk　Experian
- www.equifax.co.uk　Equifax
- www.callcredit.co.uk　Call Credit

法的要件

- www.ico.gov.uk　情報コミッショナー委員会（ICO）はデータ保護法の管理・取締りを担当している。このサイトには中小企業向けの“Quick Guide”を含む雇用実施基準のガイドを掲載されている。データ保護法に関連した実施基準は次の URL で参照できる。

http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/codes_of_practiceAspx

・ www.businesslink.gov.uk　ビジネスリンク（また、“雇用履歴リンク”でも参照できる。）は、差別の回避を含む雇用の様々な側面に関する情報を提供する。

金融サービス

・ www.fsa.gov.uk　金融サービス機構（FAS）（民間金融サービス業界の団体）（FAS）ウェブサイト

・ www.cifas.org.uk　クレジット不正使用防止組織（CIFAS）は英国の身分詐称防止サービス（非営利の会員組合）のウェブサイトである。このサイトは従業員の身分詐称などの詐欺問題に関するガイダンス、報告および研究を提供。

・ www.bba.org.uk　英国銀行協会（BBA）ウェブサイトは、金融サービス業界における詐偽防止に関する一般的な助言および情報を提供する。

その他

・ www.soca.gov.uk　重大組織犯罪庁（Serious Organised Crime Agency：SOCA）は、犯罪収益疑惑に関連する情報に対処することを任務とする。また、何時、疑わしい活動を提訴するかに関する情報を提供している。

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・ガイド(Security 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に対する技術収集動向(2006 年)』

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』
― 英国における人的セキュリティお取り組み ―
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)』

人的セキュリティ：脅威、挑戦、および対策

(PERSONNEL SECURITY : THREATS, CHALLENGES AND MEASURES(2007 年 12 月))

― 英国における人的セキュリティへの取り組み ―

平成２０年３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

如何なる人セキュリティ策が使用できるか？