防　衛　取　得　研　究　　第五巻　第一号　平成２３年６月

「武器」にまつわる品質管理の話

主　席　研　究　員
浅　見　政　博

1　「武器」に関する品質管理の起源について

最近の調査・研究によれば、約７万５千年前に南アフリカに住んでいた現生人類（ホモ・サピエンス）が使っていた槍の先が、「押圧はく離」(注)と言う石器の製造法で作られていたことが明らかになった。

日本の縄文時代が約１万数千年前であることを考えると、なんと気の遠くなるような古い話である。

ひょっとしたらこの槍は、現生人やその集団の生存をかけた闘争の場で武器として使われ、その「品質」の良否が、勝敗を分けるぐらいの重要な要因になっていたかも知れないのである。

（注）「押圧はく離」: 石などで打撃を与えて石器の原型を作った後、石片をはぎ取り、薄くて鋭利な刃や槍の先端などを作る技術

2　現代の「武器」の品質管理について

わが国の小惑星探査機「はやぶさ」は武器ではないが、今回の偉業を成し得た技術力もさることながら、７年間の長期に亘り宇宙において性能・機能が維持できる「品質」の高さには驚嘆するしかない。

「はやぶさ」と同等以上のレベルが要求されていると言われる「ＢＭＤシステム（弾道ミサイル防衛システム）」が運用されている現代でも、いまだに防衛の現場では、以前の「槍」と機能的に変わらない「銃剣」の類も使われている。

いろんな「武器」の種類があるため、その数だけの品質管理のやり方があると言える。

しかしながら、「槍」から「ＢＭＤシステム」に至る品質管理において全く変わらないことがある。

それは品質管理を行っているが人間（ホモ・サピエンス含む。）であるということであ

る。

3　「武器」の品質管理の極意について

「武器」に造り込まれるべき品質は、使用する目的・環境・規模によって異なり、その違いに応じて数多い品質管理のやり方がある。

しかしながら、それを行うのが「人間」であることに着目すれば、そんなに複雑なものではなく、自ずとその本質的なものにたどり着くものと思う。

長年、防衛装備品の品質管理関係に携わっていた者の一人として、自分なりに「武器」に関する品質管理の成功法を考えた時、いくつかの極意に集約できると確信している。

その極意とは、**「離観の観」「未完の完」「同幹の幹」**の**３つの「カン」**である。

4　「離観の観」について

昔々、世阿弥が、彼の能楽の伝書である「花鏡（かきょう）」のなかで能楽の極意を説いている。

それによると、「常に観客席から自分の姿を観る気持ちで能を演ずることがなによりも大切であり、主観的な観方（みかた）（我観）を離れ、見物人が自分の演技をどう評価するかを自分の観る位置（離観）とすることが、能楽を極めるうえでの極意である。」と伝えている。

武器の製造現場での品質管理は、関係する数多くの会社が、それぞれの特性に応じた品質管理を行っている。

もちろん各会社は、自社の品質管理のやり方やその効果は十分満足できるものと考えているはずである。

でなければ、自分たちが造り上げた武器を自信を持って防衛の現場に送り出せるはずがない。

しかしながら、その満足や自信が自己満足であったり、一人よがりの世界であってはいけないのである。

防衛装備品の調達にも採用されているＪＩＳ９０００シリーズによる品質管理システムでのキーワードは、「顧客重視」の考え方である。

即ち、自社の品質管理システムをいかにすれば、顧客（防衛省）の満足する品質の武器を提供できるかを追求しており、自社自身の満足を求めてはいないのである。

これが世阿弥の言う**「離観の観」**の極意である。

5　「未完の完」について

今流行（はやり）のＪＩＳ９０００$_S$の品質管理要求事項は、防衛省が現在調達している「武器」にも全面的に採用されている。

このＪＩＳ（ＩＳＯ）規格を制定した基本的理念の一つは、「継続的な改善」を行い続けることである。

一昔前にも、多くの会社の品質管理部門において導入されてきた、「計画－実行－チェック－改善」　のＱＣ改善サークルと同様の活動と思われる。

すなわち、品質管理と言うものは、全てが完璧であってこれ以上改善の余地は無いと言う領域には決して到達し得ず、いつも未完の状態にあると言うことである。

そしてこのことは、「永劫の改善活動」を可能とする、システム構築が要求されていることになる。

古来、日本においては完成してしまった万（よろず）の物（もの）は縁起が悪いとされているようである。

日光の陽明門は、誰もが認める超弩級のすばらしい建築物であるが、あまりにも完成度が高いため、縁起を重んじてわざと一本の「逆柱（さかばしら）」を組み入れ、いつまでも未完の状態にしていると言うのは有名な話である。

縁起の話は余計かもしれないが、**「未完の完」**を忘れず、常に改善の情熱を失わないことが、より良い品質管理を行う上の極意の一つと言える。

６　「同幹の幹」について

武器いわゆる防衛装備品も、製造の過程、使用する間には多くの不具合や故障等の不適合事象が発生する。

その都度、再発防止のための対策を考えて、改善を実施しなければならない。

ＪＩＳ（ＩＳＯ）９０００$_S$で規定されている「是正処置」活動がその一つである。

その際、発生した不適合事象は、それぞれが一見異なるものの様に理解され、それぞれ別個の対策がとられる場合がよく見られる。

防衛装備品に係る不適合事象は、時・場所・人・物によって様々な事象として発生するが、その多くが過去において既に発生したことがある不適合事象と同一の原因であったり、他のケースでも発生しているものと根本的には同じ内容であったりするものである。

枝葉末節では異なる事象であるが、幹となる根本的原因は同一の場合が多いのである。

従って、不適合事象の原因については、この同一の幹を追求し、改善の策を考案し、その適用の段階で広範囲に広げることが最も再発防止効果が期待できるものと思う。

これが**「同幹の幹」**の極意である。

昔々、弘法大師空海が、「智者が同一を見るところにおいて、愚者は違いを見る。そしてその違いにとらわれて、様々な迷いを生じ、恐れを生じる。」と説かれたと言われる。

「是正処置」の活動に限らず、各会社が導入している品質管理のシステムそのものも、

対象の製品、会社規模、適用の規格等において千差万別のものである。

品質管理の規格の一つに過ぎないＪＩＳ（ＩＳＯ）９０００$_S$の適用範囲だけでも、武器から食料品、病院、ホテル等のサービス業まで、それこそ多岐に亘る業種に広がっている。

業種やその製品等の違いによって品質管理活動の内容は異なるが、その違いに気を取られることなく、品質管理の同一性を見つけることにより活動の重点を根幹部分に絞ることができるものと考える。

7　最後に

戦後のわが国防衛省（庁）においては、防衛装備品の調達に係る品質管理と言えば、米軍の作成したＭＩＬ　ＳＰＥＣを主体とした品質管理要求がなされていた。

その後、品質管理に関するＭＩＬ　ＳＰＥＣが米軍で廃版となったことに伴い、防衛省は、国際規格（ＩＳＯ）あるいは日本工業規格（ＪＩＳ）を武器の品質管理の分野に導入した。

また２００９年には、ＪＩＳ（ＩＳＯ）９１００の規格の適用範囲が、「航空宇宙分野」から「航空宇宙分野と防衛分野」へ拡大された。

これらの推移を振り返ると、武器に係る品質管理というものが、特異な領域からより共通性・汎用性のある領域へと接近もしくは融合しているように感じられる。

その観点から、ここで述べた武器にまつわる品質管理の３つの極意は、武器独特のものではなく、あらゆる製品等の品質管理の極意であるとも思える。

まさに品質管理の極意である。

＊引用図書等：

①　日本経済新聞（22.10.29　夕）

②　「文章の品格」（林　望　著）

③　「徒然草　解説」（角川書店）

④　「空海の思想」（梅原　猛　著）

イージス艦と情報漏えい

研究員　　吉村　司郎

はじめに

「イージス艦」という言葉は、最近よく耳にすることと思う。例えば、イージス艦「あたご」と漁船との衝突、映画「亡国のイージス」及びイージス艦情報漏えい事件等、イージス艦という言葉を聞いたことがない日本人はだんだん少なくなってきたと思う。

では、イージス艦とはどんな艦なのか？　イージス艦とは、米国が開発したイージス武器システムを搭載した水上戦闘艦のことである。また、イージスすなわち「ＡＥＧＩＳ」とは、ギリシャ神話の最高神ゼウスがわが娘アテナに贈った盾の名前であり、盾と言っても機動隊が持っているような盾ではなく、山羊の皮で作られた胸当てのようなものである。一切の邪悪な矢を一本も通さないという意味に由来する。したがって、イージス艦とは、あくまでイージスシステム搭載艦の通称であり、正式にはミサイル巡洋艦又はミサイル駆逐艦と言うことになる。

１　イージス艦開発の経緯

冷戦時代、ソ連にとって最も大きな脅威はソ連近海を遊よくし、どこからでもソ連本土を攻撃可能であった米海軍の空母戦闘群であった。この米空母戦闘群を攻撃するためソ連が開発したのが爆撃機搭載のＡＳ－４、ＡＳ―６、艦艇搭載のＳＳ－Ｎ－３等、対艦巡航ミサイルであった。そして単に一方向からの発射ではなく、多方向から多数同時に弾着させる飽和攻撃であった。

一方、当時米国の保有するターターシステムは、回転式レーダーであり、死角の存在、脅威評価及び武器選択が人間の判断であり、また、捜索レーダーから追尾レーダーへの目標情報の移管等、リアクションタイムが長く、ミサイルもセミアクティブ誘導であり、同時対処能力が極めて限定的であったため、ソ連の対艦ミサイルによる飽和攻撃には対処不可能であった。

それに対処するため米国が開発したのが、捜索機能と追尾機能を統合したＳバンドの多機能レーダー及び中間指令誘導付きセミアクティブ型スタンダードミサイルによる短いリアクションタイムで敵の飽和攻撃に対処可能な信頼性の高いシステム、すなわちイージスシステムであった。

２　イージスシステムの構成

イージスシステムは、イージス武器システムとイージス戦闘システムの二つの意味があるが、一般的にはイージスシステムと言えば、イージス武器システムを指す。イージ

ス武器システムの主な要素は、以下のとおりである。

多機能レーダーＳＰＹ－１Ａ

戦闘意思決定システムＣ＆Ｄ　Mk１

武器管制システムＷＣＳ　Mk１

ミサイル発射ランチャー　Mk４１ＶＬＳ

スタンダードミサイル

射撃指揮装置　Mk９９

(1)　多機能レーダーＳＰＹ－１Ａ

イージスシステムの中心的存在であるＳＰＹ－１Ａレーダーは、八角形のパッシブフェーズドアレイレーダーで艦の上部構造物に四方に向けて貼り付けられた４面の固定式平面アンテナから構成されており、外見上はイージス艦の特徴ともなっている。この４面で電波ビームを上下左右に走査させ、全方位３６０度水平線から天頂までをカバーしている。このレーダーは、ＵＹＫ－７というコンピューターで制御されており、探知した目標は自動的に追尾される。探知距離は一般的に約５００Km、追尾可能な目標数は約２００と言われている。

(2)　戦闘意思決定システムＣ＆Ｄ　Mk１及び武器管制システムＷＣＳ　Mk１

戦闘意思決定システムＣ＆Ｄ　Mk１及び武器管制システムＷＣＳ　Mk１は、艦の全てのセンサーやデータリンクからの情報をもとに目標の敵味方識別、脅威評価を行う。数個のＵＹＫ－７コンピューターと数個のコンソールから構成されている。武器管制システムは、交戦する武器の選択を行うものであり、数個のＵＹＫ－７コンピュータと数個のコンソールで構成されており、この二つはイージス艦の中枢とも言える存在である。

3　イージスシステムの交戦手順

ＳＰＹ－１Ａレーダーで探知された対空目標は、自動的に追尾され、目標の針路速力が計測される。戦闘意思決定システムがＳＰＹ－１Ａレーダーの他、艦のあらゆるセンサーやＩＦＦ（敵味方識別装置）からの情報などを元に脅威評価を行い、武器管制システムにより攻撃するための武器が選択される。ミサイルの発射は手動ないしあらかじめ設定した手順(ドクトリン)に基づき、全自動又は半自動に設定できる。目標の位置、針路速力などがドクトリンで設定した一定の基準を満たすと全自動であればミサイルは自動的に発射される。発射されたミサイルと目標はＳＰＹ－１Ａレーダーにより追尾され、ミサイルを目標との会敵位置にＳＰＹ－１Ａのレーダー電波を使って誘導する（中間指令誘導)。ミサイルが目標に接近（命中する数秒前）すると武器管制システムの指示を受

けた射撃指揮装置により、ミサイルの終末誘導用イルミネータがＳＰＧ－６２から目標に連続波が照射され、ミサイルはその反射波をたどって誘導され命中となる。このように終末段階のみＳＰＧ－６２から連続波を照射すればいいため、それ以外の間は、ＳＰＧ－６２は別の目標に向かっているミサイルの終末誘導を行うことができ、これがイージス艦に多目標対処能力を持たせることとなった。ちなみに同時対処能力はＳＰＧ－６２を３基保有の「こんごう」型の場合、概ね１２目標と言われているが、状況によってはもっと多くの目標に対処することも可能である。

4　我が国のイージス艦

「こんごう」型護衛艦は、海上自衛隊が保有する日本初のイージスシステムを搭載したミサイル護衛艦である。昭和56年度中期業務見積もりでターターシステム搭載の「はたかぜ」型ＤＤＧ４隻を建造することとなり、５６年度計画で「はたかぜ」が、５８年度計画で「しまかぜ」が就役した。

一方、米国のイージス艦タイコンデロガ級が就役すると日本にもイージス艦を購入するよう米国から圧力が掛かるようになる。その頃、日本でもシーレーン１０００マイル防衛構想があり、この１０００マイル防衛においても脅威はソ連の爆撃機バックファイアー搭載の対艦ミサイルであり、これに対処するため検討された装備がイージス艦であった。また、米国の対日貿易赤字の是正という政治的要因も加わり、「はたかぜ」型は２隻で中止になり、昭和６３年度計画により、イージス艦が導入されることとなった。このイージス艦は「7200 トン」型と呼ばれ、船体は日本で建造、その艦に米国からＦＭＳ(有償軍事援助)により購入したイージスシステムを搭載することとなった。船体については米国のアーレイバーク級ミサイル駆逐艦をベースに設計された。なお、米国からＦＭＳで購入されたイージスシステムの価格は約 400 億円である。「こんごう」型は４隻建造され、建造費は一隻あたり約 1200 億円であり、通常の汎用型護衛艦の倍の建造費になる。「国民から一人 1000 円を頂戴して建造された。」と言うのはイージス艦艦長の言葉である。また、「たちかぜ」型ＤＤＧが平成１８年度除籍されるための代替艦として１４年度、１５年度に「あたご」型 7700 トン２隻が建造され、現在６隻のイージス艦を保有している。

5　今後のイージス艦の役割

ソ連の爆撃機バックファイアー搭載の対艦ミサイルに対処するため装備したイージス艦であったが、「こんごう」が就役した時には冷戦は終結、ソ連は崩壊し、バックファイアーの脅威は去ったものの、その「こんごう」型に新たな役割を与えることになったのが冷戦後第三国へ拡散した弾道ミサイルであった。平成５年にノドンが、平成１０年にはテポドンが北朝鮮から発射され、「みょうこう」が発射されたテポドン１号の探知、追尾に成功したが日本にも弾道ミサイルの脅威が迫ることとなった。

これを受けて平成１１年から当時のＴＭＤ（戦域ミサイル防衛）のひとつであるＮＴＷＤ(海軍戦域広域防衛)の共同研究が開始され、一方で平成１５年度には「こんごう」型へのＢＭＤ能力の付与が決まり、現在までに４隻の「こんごう」型イージス艦にＢＭＤ能力が付与されている。２３中期防で更に「あたご」型にもＢＭＤ能力付与が計画されている。ちなみにＢＭＤ（弾道ミサイル防衛）能力付与のための改修費、スタンダードミサイルＳＭ３ブロック１Ａの取得（１発約２０億円×９発）及び発射試験のための経費は１隻あたり約３４０億円である。

このように巨額の予算がかけられたイージス艦であるが、今後も艦隊防空に加えＢＭＤにおいて我が国を弾道ミサイルから防衛するという新たな役割を担うことになる。したがって、同じ護衛艦であってもその掛かる経費もさることながらイージス艦は、他の護衛艦に比べ、格段の差の能力を有する世界最強の護衛艦なのである。

6　イージス情報漏えい事件

イージスシステムは、極めて高価である上に機密のレベルが高く、開発国である米国の提供認可査定が極めて厳しいことから、その保有は、相応の経済力と米国の信頼を持った国家に限られ、当初は日本にだけリリースされたシステムであった。

２００７年１月、海上自衛官の妻(中国籍)を出入国管理法違反の容疑で調べた際、押収した外付けハードディスク内にイージス艦の情報が発見された。２００７年１２月１３日、事案の発端となった海上自衛隊開発隊群プログラム業務隊所属(当時)の３等海佐がイージス艦情報を漏えいしたとして逮捕された。当該３等海佐は、日米相互防衛援助協定に伴う秘密保護法違反容疑で起訴(２００８年１２月、懲戒免職)されたほか、流出の舞台となった海上自衛隊第１術科学校では、当該３等海佐にイージス艦情報を要求してその情報を受け取った元学校教官ら４名が書類送検され、一連の事案に係わった自衛官も多数が懲戒処分を受けた。平成２３年３月１日、当該３等海佐は、懲役２年６月執行猶予４年で結審された。

この問題は、確かに３等海佐の保全意識の希薄が主因であるが、これだけではないもっと大きな問題が隠されていると思われる。すなわち、海上自衛隊の組織が招いた漏えい事件でもあると考えられる。なぜ、第１術科学校の教官が、起訴された３等海佐に「学生の教材用に適当なイージス艦に関する資料」を要求したのか。海上自衛隊第１術科学校では、幹部中級課程（１等海尉クラスに対する専門教育）教育を実施している。専門が「射撃」の中級射撃課程では、艦砲射撃に関する教育を１年間かけて実施しており、課程修了後、全員が護衛艦の砲術長として補職され、艦砲の射撃指揮官となる。その中にはイージス艦の砲術長を命ぜられる者もおり、着任後直ちに出港し、射撃を実施する場合もある。

イージスシステムの教育は、その基幹要員である砲雷長に対し、米国留学又は横須賀で実施されているが、砲術長まで教育する余裕がなく、そのため、イージス艦に補職さ

れる学生には、砲術科のイージス艦乗艦経験教官が修業前に補習により、イージスシステムに関するおおまかな知識を付与して修業させているのが現状である。なぜならば、イージスシステムは全ての武器をシステムの中に割り当てているため、イージス艦の砲術長は、イージスシステムを理解していなければ艦砲射撃を指揮することは極めて困難であり、コンソール操作も出来ない。それゆえ、補職される学生が困らないようにイージスシステムに関する補習教育のため、砲術科の教官が元米国留学した同僚にイージスシステムに関する資料の提供を依頼したのが事件の発端である。

資料を要求した学校教官も資料を提供した３等海佐も金儲けあるいは我が国の安全を害する目的でのスパイ活動等ではなく、学生のため、海上自衛隊のためにと思い、起こした事件である。したがって、この事件は、３等海佐だけの問題ではなく、海上自衛隊の教育体系及び補職の問題でもある。また、これまでの海上自衛隊の旧態依然の体質である「海上自衛隊は、装備の導入が先であり、教育はその後」というこれまでの体制が招いた事件とも言える。

おわりに

イージス艦とは、その能力において世界最強の戦艦であるがゆえにイージス艦情報漏えいは、日米関係に大きな影響を及ぼした。当時、「こんごう」のＢＭＤ能力付与のための改修が進められていたが、米国側はイージス艦の情報漏えい問題を受けて、２００７年７月に改修に必要なソフトウェアや文書の供給を停止した。日本側が新たな情報保全体制の取り組みを説明（当時、小池防衛大臣が米国との秘密軍事情報保護協定（ＧＳＯＭＩＡ）を締結(2007.8.10)）したのを受け、８月３日に供給が再開された等の経緯もあった。また、航空自衛隊の次期主力戦闘機（Ｆ－Ｘ）選定作業にも大きな影響を及ぼした。こうした情報の漏えいが日米関係だけでなく、その他の同盟諸国にも大きな影響を及ぼすことを保全講習を通じてその関係者に今後とも伝えていかねばならない。

インサイダー脅威への対策

客員主任研究員　横山恭三

目次

はじめに

昨年（2010 年）は、インサイダーによると見られる２つの大きな世界的な事件が発生した。

一つはウィキリークスの「ケーブルゲート」事件[1]である。2010 年 11 月 28 日、ウィキリークスは、米国の外交文書（「大使館機密公電」）220 点をウェブサイトで公開した。ウィキリークスは 1966 年から 2010 年までの、米国の大使館機密公電 25 万点を入手したと発表し、その後さみだれ式に公開を続けている。ガーディアン紙によると機密資料の容量

[1]ウォーターゲート事件をもじった言葉

は 1.6 ギガバイトで、小さなメモリーカードに保存されていたようである。米軍は、2010 年 6 月に機密情報漏洩の容疑で陸軍の情報アナリストであったブラッドリー・マニング上等兵を逮捕した。米検察当局はスパイ罪での立件を狙っていると見られる。

もう一つは、日本の警視庁公安部資料の流出事件である。2010 年 10 月 28 日、警視庁公安部資料 114 件がルクセンブルグからインターネット上に流出した。流出した文書は、国際テロ捜査を担当する警視庁外事３課のほか、警察庁や愛知県警などが作成したとされる。内部犯行と見られていることから、警視庁は、地方公務員法（守秘義務）違反などで被疑者の検挙を目指すものと見られる。

インサイダー脅威そのものは目新しいものではないが、上記の事例は、情報のデジタル化、ネットワークでの情報の共有管理、大容量の保存機能などの近年の情報通信技術の進歩により、膨大なデータが瞬時のうちにインターネットのウェブサイトに公開されてしまうデジタル時代におけるインサイダー脅威を浮き彫りにしている。しかし、インサイダー脅威は情報漏洩だけではない、情報の窃盗又は改ざん、システムとネットワークに対する妨害（サボタージュ）などがある。そしてこれらのインサイダーがもたらす損害は、財政的なものだけでなく、事件が広く報道されることにより組織の評判も著しく傷つけられる。

多くの組織は、外部からのアクセス又は妨害から情報を保護することに注意を集中するが、その一方で、インサイダー脅威を軽視する傾向にある。特に我が国ではその傾向が強く見られる。その背景には、日本人が元来「性善説」を好む傾向にあることが考えられる。しかし、「性善説」では、狡猾なインサイダーに立ち向かえない。組織は、「人を見たらドロボーと思え」という諺を肝に銘じてインサイダー対策に取り組まなければならない。

インサイダー対策は、まず、情報セキュリティ対策が確実に実施されていることが前提である。今日、情報セキュリティ製品・システム評価基準（ISO/IEC15408）や情報セキュリティマネジメントシステムの認証基準（ISO/IEC27001）が、国際標準として規格化されている。各組織はこれらの国際基準を採用すべきである。これらの情報セキュリティ対策が完全であるならば、インサイダー対策のための特別な施策は必要ないと言っても過言でない。本稿で取り上げる対策も、上記の情報セキュリティ対策に含まれているものであるが、日本においては未だ十分に対策が徹底されていないと思われるので、数多くのインサイダー事例から効果的であると思われる対策を筆者なりに抽出・強調した次第である。

以下、米国と英国の情報セキュリティ機関が発表した調査研究[2]に基づき、多くの事例を交えながら、インサイダー脅威の実態と組織が取り組むべき具体的なインサイダー対策を紹介する。

１．インサイダーの定義

インサイダーの世界共通の定義は存在しない。米国のカーネギーメロン大学のコンピュータ緊急対応センター（Computer Emergency Response Team : CERT）（以下、CERT

[2]「参考文献一覧」に記載

という）は、「現もしくは元従業員、契約社員、派遣社員、又はビジネス・パートナーで、組織のネットワーク、システム、又はデータへのアクセス権が与えられている者若しくは与えられていた者で、組織の情報若しくは情報システムの機密性、完全性、又は有用性に悪影響を与えるような方法で、このアクセスレベルを故意に越えて使用する者又はこのアクセス権を悪用する者」をインサイダーと定義している。一方、英国の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：CPNI）（以下、CPNI という）は、「合法的なアクセス権を悪用する者」と簡潔に定義している。本稿では、CERT の定義を準用する。

２．インサイダー脅威

インサイダー脅威は、組織の事業にとって最重要な情報の完全性、可用性、又は機密性に悪影響を及ぼす。例えば、インサイダーは、顧客財務情報を操作したり、雇用主のウェブサイトを書き換えたりするなど様々な方法で組織の完全性を侵害する。また、彼らは、組織の機密情報、専有情報（proprietary information：企業が知的所有権を有する情報）、又は顧客情報を盗み取ったり、組織経営者間の電子メールのみならず、顧客の個人情報を含む機密情報を不適切に流出させ、組織の情報の機密性を侵害する。さらにインサイダーは、データを削除し、システムとネットワーク全体を妨害し、バックアップを破壊し、あるいは DoS（Denial of Service：サービス拒否）攻撃を行うなど組織の情報の可用性を侵害する。

インサイダーは、組織を攻撃したいと思っている部外者よりもかなり好都合な立場にある。例えば、無許可のアクセスを防止するためのファイアウォールや IDS（Intrusion Detection System ： 侵入検知システム)、電子的な建物へのアクセスシステムなどの物理的及び技術的対策を回避することができる。さらに、インサイダーは、組織が使用しているセキュリティポリシーや手順、技術などを知っているだけでなく、しばしば、順守されていないポリシーや手順、さらに悪用できるネットワークやシステム上の欠点など組織の脆弱点を知っている。このようなインサイダーが引き起こすインサイダー事件は、次の事例１、２、３のように、しばしば、組織に壊滅的な影響を及ぼす。

▲事例１

あるメーカーで働いていた１人の従業員は、新しい仕事に就くことを願って、１億ドルに相当する企業秘密を含んだ設計図を盗み、台湾の競合者にそれを売却した。[3]

▲事例２

浄水化を担当していたあるコンサルタントは、地方政府によって仕事を拒否された。彼は、インターネット、無線通信機、盗んだ管制ソフトを用いて、工場のコントロールシステムをハックし、結果として、オーストラリアのクイーンズランド州のマルー

[3]「インサイダー脅威の防止・探知のための共通ガイド第３版」P4

チドールの川と海岸線沿いに百万リットルの汚水を流出させた。[4]

▲事例３

三菱 UFJ 証券会社システム部の部長代理の男性が不正に顧客情報データベースから約 148 万人の顧客情報を持ち出し、このうち 4 万 9,159 人分の個人情報を 3 社の名簿業者に売り込んだ。公判では、情報漏洩による三菱 UFJ 証券の損失額が、70 億円以上になることが明らかになった。[5]

３．インサイダーのタイプとタイプ別の行動様式

インサイダーは、様々な目的・動機により本人が保有するアクセス権を悪用する。これらのインサイダーのタイプは次の 3 つに分類できる。

・意図的に就職したインサイダー
最初からポストを利用しようとする意図を持って、計画的に組織に就職したインサイダー

・雇用中に忠誠心が失われたインサイダー
入社時には悪意を持っていなかったが、雇用中に何らかの要因により忠誠心が失われたインサイダー

・退職前後に組織に復讐するインサイダー
職場に対する不満から、退職前後に、組織に復讐しようとするインサイダー

（1）意図的に就職したインサイダー

このタイプのインサイダーには、国家又は企業から資金提供を受けたスパイ（経済スパイ[6]や産業スパイ[7]など）、競合ビジネスを起業するもくろみを持って就職する者が含まれる。このタイプのインサイダーは、組織の機密情報、専有情報、又は財務情報などを窃盗する。また、まれにサボタージュを目的に組織に潜入し、時限式のウイルスを仕掛けるスパイがいると言われている。次の事例４は、典型的な経済スパイの例である。

▲事例４[8]

「米国で 20 年以上活動し続けて 2007 年に有罪判決を受けた中国系米国人のエージェントは、1978 年に香港経由で米国に入国した後、米国の主要な情報・防衛企業に勤務し、着実に地位を向上しながら機密情報へのアクセスを拡大した。彼は、1985 年に帰化し米国市民となり、1996 年に保全適格証を付与された。彼は、中国のためにスパイ活動を継続し、約２年に一度、妻を同行して中国に旅行し人民解放軍の運営者

---

[4]「雇用中の人的セキュリティ：優れた実践事例ガイド」P69

[5] http://itpro.nikkeibp.co.jp/article/NEWS/20090909/336929/

[6]外国政府、外国政府の影響下にある組織、または外国政府の職員の利益になることを承知または意図して、企業秘密を意識的かつ意図的に横領すること。経済スパイ法（Economic Espionage Act of 1996）

[7]その企業秘密の所有者に損害を与えることを承知または意図して、所有者以外の誰かの経済的利益のために、州間通商または外国貿易のために製造された製品に関連した企業秘密を意識的かつ意図的に横領すること。経済スパイ法（Economic Espionage Act of 1996）

[8]「外国の経済情報収集および産業スパイ活動に関する議会への年次報告(２００７年)」

（handler）に情報を届けるとともに新たな任務を受領した。この事例が示す重要なことは、人民解放軍のスパイ工作における忍耐強いかつ断固とした取り組みを示していることである。つまり、エージェントには、企業に浸透してから機密情報にアクセスできる地位に就くまで十分な時間が許容されていることである。」これは、典型的な経済スパイ事件である。

（2）雇用中に忠誠心が失われたインサイダー

忠誠心が失われる要因には、「私生活・職場環境の変化」と「第三者による勧誘」がある。この両者は相互に影響し合う部分もある。本人の病気や家族の死・病気などは、精神的ストレスとなり、「第三者の勧誘に」に対して脆弱となる。逆に、第三者の勧誘に応えて報酬を得たインサイダーは、金銭的支出が急増するなど私生活が変化する。このタイプのインサイダーは、本人又は第三者の金銭的利益のためにデータや情報などを改ざんしたり、第三者に情報を売却するために組織の機密情報、専有情報、又は財務情報などを窃盗する。

勧誘する第三者がスパイの場合、インサイダーはスパイの協力者（エージェント）となり、（米国などのようにスパイ防止法が制定されている場合は）スパイ罪が適用される。他方、第三者が、親族、知人等の場合は、窃盗罪や詐欺罪が適用されるであろう。いずれにしても、このタイプのインサイダーの主要な動機は、金銭的利益である。次の事例５は、たまたま自分のアクセス件を悪用することの価値を認め、金銭的利益のために忠誠心を失った事例である。

▲事例５

「軍事産業に雇用されたコンピュータヘルプデスク係は、彼が担当する軍事システムに偽りの電子メールアドレスを作成した。それから、主要な納入業者に対して、リコールされた軍事装備品の交換部品を要求するために、これらの電子メールアドレスを使用した。納入業者は、交換部品が受領された後、現物のリコール部品が送り返されるものと思い、交換部品を電子メールで指定された住所に送った。インサイダーは、発送先に自宅住所を記載していた。このインサーダーは、小売価格で５００万ドルに相当するほぼ 100 回の発送品を受取り、インターネットのオークションサイトで売りさばいた。」[9]

（3）退職前後に組織に復讐するインサイダー

このタイプのインサイダーのほとんどが、解雇、雇用主や監督者との反目、異動、降格、減給、又はボーナスの減額などに不満を抱いていた。彼らは、組織の業務遂行を妨害する目的で、情報（データ、ファイル、プログラムなど）の破壊、削除、劣化、改ざん、又は隠ぺい、即ち「情報システムに関連したサボタージュ」（以下、IT サボタージュと言う）を行なっている。

次の事例６は、典型的な IT サボタージュの例である。この事例のように、IT サボター

[9] 同上実践事例 1、P31

ジュを働くインサイダーの多くは、システム・アドミニストレーターなど特権的アクセスが与えられていた元従業員が多い。

▲事例６

「国際的金融組織のシステムアドミニストレーターは、年１回のボーナスが予想より低くなるだろうという噂を聞いた。彼は自宅でロジックボム[10]を製造し始めた、そして、２か月半にわたって、典型的なサーバーアップグレード手順の一部としてロジックボムを会社のサーバーに移すために許可されたリモートアクセスを使用した。彼は、上司からボーナスが予想したよりかなり低いことを知ったとき、すぐに退職した。それから約２週間後、ロジックボムは午前９時３０分に爆発した。そして、米国全体でおよそ 1,000 台のサーバーの中の 100 億件のファイルを削除した。犠牲となった組織は、そのネットワークの修復費用を 300 万ドル以上と見積もった。そして、その損失は、同社の 12 億 4,000 万株の株価にも影響を及ぼした。」[11]

４．インサイダー脅威への対策

インサイダーは、無許可のアクセスを防止するためのファイアウォールや IDS（侵入検知システム)、電子的な建物へのアクセスシステムなどの物理的及び技術的対策を回避することができる。そもそも、インサイダーは、組織のネットワークやシステム上の欠点などの組織の脆弱点を知っている。このために、インサイダー行為を事前に探知することは極めて難しい。従って、次の４つのプロセスで対処すべきである。

第１プロセス：入れない

インサイダー脅威となる人物（スパイ）や将来インサイダーになりやすい人物を採用しない。

第２プロセス：取り除く

組織の中のインサイダー脅威を軽減する又は取り除く。

第３プロセス：近づけない

アクセスを許可した者以外を、保護すべき組織の IT 資産に近づけない。

第４プロセス：捕まえる

インサイダー行為を行ったものを捕まえる。

以下、具体的な対策とその対策に関連した事例を紹介する。

（１）第１プロセス：入れない

●対策１：厳格な雇用前調査の実施

雇用前調査の目的は、組織に対してインサイダー脅威となる人物（スパイ）や将来インサイダーになりやすい人物を特定し、採用しないことである。すべての組織は適切な

[10] 論理爆弾：特定の日付や時刻など、何らかの条件が満たされた際にデータを破壊するプログラムの総称

[11]「インサイダー脅威の防止・探知のための共通ガイド第３版」実践事例 10、P60

基準に基づき雇用前調査を実施しなければならない。雇用前調査には、身元調査、職歴調査、犯罪歴調査、財務調査などがある。調査の手段は、応募者が提出する書類の真正性の確認と面接による応募者の性格や誠実性、信頼性などの評価である。最近では性格調査アンケートの使用も考慮されている。

これらの雇用前調査により、応募者が重要な情報を隠ぺいしていないか、さもなければ、応募者が身元や本心を偽っていないかが明らかにならなければならない。応募者の健全性と信頼性に関して懸念を惹起するものには次のものがある。

・違法活動への関与
・職務に関連する時効のない有罪判決、特に、応募者が自発的に申し出たものでなく他の調査で明らかになった場合
・履歴書又は申込書における虚偽又は実証できない記載事項
・職歴における説明のつかない空白
・疑わしい提出書類。例えば、補強説明の不足又は文書が本物でないという疑念
・応募者が自分の情報の提供を回避する又は嫌がるなど

スパイを雇用することが絶対にあってはならないが、圧力に弱いなどの性格特徴、懸念国に居住する家族、好ましくない経歴などからインサイダーになりやすい人物を見逃さないことが重要である。

CERT の研究によると､IT サボタージュを犯したインサイダーの 30%には逮捕歴がある。この様な比較的高い犯罪率は、雇用前調査の必要性を裏付けている。次の事例 7 は、雇用前調査が適切であったならば、インサイダー行為を防止できた例である。

▲事例 7

「ある組織がシステム管理業務のために 1 人の契約社員を雇った際に、その契約社員の身元調査が行われている旨、契約業者から伝えられた。その契約社員は、後に、組織のシステムを侵害し、雇用者の何百万人分の機密データを窃取した。調査によって、その契約社員には、過去に保護されたコンピュータに不正アクセスした犯罪歴があることが分かった。」[12]

（2）第 2 プロセス：取り除く

このプロセスには、兆候を探知する、通報する、そして適切に対処する、という 3 つのステップが含まれている。

●対策 2 ：従業員の態度や行動の変化の継続的な監視

人間は弱いものである。昨日まで忠実だった従業員が、翌日にはインサイダーとなる場合もある。従業員は、環境の変化に影響されやすく、それが態度や行動の変化として現われる。従って、管理者は、潜在的なインサイダー脅威であることを示すあらゆる変化又は疑わしい行動を察知するために、採用後も部下の態度と行動を観察し続けなければ

12 「インサイダー脅威の防止・探知のための共通ガイド第 3 版」実践事例 4 、P３９

ならない。また、すべての従業員にインサイダー脅威への自覚を促して、従業員が同僚の無許可のアクセスなどの不審な行動を直接管理者又は通報ホットラインを通じて報告させなくてはならない。そして、管理者は、従業員が個人的判断能力を弱めるような、あるいは第三者に対する脆弱性を高めるような環境にある時に、相談相手になるなど適切に対処し、インサイダー脅威を軽減あるいは取り除かなければならない。

潜在的なインサイダー脅威であることを示すリスク徴候には次のものがある。

・麻薬又はアルコールの不正使用
・特に暴力を提唱する過激派の見解や行動、事件に対する支持の表明
・自身の職務遂行又はセキュリティ姿勢に悪影響を及ぼす宗教的、政治的若しくは社会的な主張・団体への親和など行動の突然若しくは顕著な変化
・ライフスタイルの重大かつ不可解な変化
・金銭的支出の突然の変化
・仕事への関心の突然の喪失又は職務の変更若しくは期待はずれに対する過剰反応
・極端な感情的行動などのストレスの兆候
・勤務パターンの変化、例えば、単独での作業、普段と違う時間帯の作業、休暇をとりたがらないなど
・セキュリティ対策又は権限外の職場区域への異常な関心
・頻繁かつ不可解な欠勤
・定められたセキュリティ手順の度重なる不履行

しかし、従業員の不審な行動はしばしば見落とされるので、出来るならば、従業員に対する定期的なセキュリティ評価（面接や評価フォームによる調査）を実施すべきである。特に、ある従業員を機密情報へアクセスする機会のある配置へ異動させる場合には、かならずセキュリティ評価が実施されなければならない。諸外国では、政府機関の職員の適格性（信頼性）を確認するために適格性確認制度[13]が導入されている。

▲事例８

「エンジニアリング担当の副社長であり同時に企業のソフトウェア開発の責任者であったインサイダーは、長い期間、上級の経営陣と反目していた。この反目は、インサイダーによる口頭による非難によって特徴付けられた。インサイダーは週に１、２度個人攻撃を行っていたが、ある時、レストランで企業の代表執行役員(CEO)に向かって大声で個人攻撃をした。この激しい意見の対立は、インサイダーを退職に向かわせた。退職手当が支払われなかったので、彼は開発中の成果物の一部をリムーバブルメディアにコピーし、それを企業のサーバーから削除し、さらに、最新のバックアップ・テープを持ち出した。それから、彼は５万ドルと交換にソフトウェアを復元すると申し出た。彼は起訴され、恐喝罪、企業秘密の横領罪、及び重窃盗罪で有罪判決を受けた。しかし、ソフ

[13] 特定の秘密の取扱いについては、その秘密を取扱うことについての適格性（信頼性）を確認した者に行わせる制度。

トウェアの最新版は決して復元することはなかった。組織が、初期の破壊的行動の警告を認識した時点で彼のアクセスから資産を保護したならば、相当な損失が回避できたであろう。」[14]

（3）第 3 プロセス：近づけない

組織は、IT 資産を防護するために、従業員の IT 資産への立ち入りと電子的アクセスを「アクセス管理」により制御する。アクセス管理には、重要建物等への立ち入りをテンキーシステムのコードを知っている者や磁気ストライプカードを保有している者を、アクセス権を付与した者と見なす物理的な方法と、各システムへのアクセスを従業員のアカウント情報とアクセス権情報で管理する電子的な方法がある。

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。特に、従業員が退職したならば、彼の全てのアクセス経路が無効にされなければならない。

●対策３：アクセス管理原則の順守

アクセス管理には、「最小特権（least privilege）の原則」、「役割（任務）を基本としたアクセス管理（role - based access control）」、「任務分担（separation of duties）の原則」、及び「Need to Know の原則」の 4 つの原則がある。この 4 つの原則は相互に関連しており、ときには、混同して使用される場合があるので注意が必要である。

・「最小特権（least privilege）の原則」

「最小特権の原則」とは、すべてのプログラムおよびユーザーは、目的のジョブを達成するために必要な最小限の権限において処理を実行することである。この原則に従うことで、セキュリティホールによる被害を最小限に抑えることが可能となる。

システムに大きな影響を及ぼす変更操作は一般にシステム管理者のみに許されるようになっており、こうした操作を行う特別な権限は「特権」と呼ばれる。機密情報やハードウェアを直接扱う重要なプログラムは管理者権限など特別な特権で動作する。万一このようなプログラムにセキュリティホールがあると、プログラムは悪用されシステム管理権限が奪われる。このようなプログラムでは特権が与えられなければ達成できない処理を局所化し、またその他の処理では特権を放棄することで、セキュリティホールによる被害を最小限に抑える設計を行なう。

「最小特権の原則」により、セキュリティが突破された場合でも、システムへの悪影響を局限化することができる。

・「役割（任務）基盤のアクセス管理（role - based access control）」

「役割基盤のアクセス管理」とは、役割（任務）を基本とするアクセス管理のことで、従業員の機能的な役割に応じて、従業員にアクセス権を付与することである。例えば、研究者は、かれらの研究施設にアクセスする必要があるが、人事ファイルキャビネットにアクセスを必要としない。同様に人事担当者は人事記録へのアクセスを必

[14]「インサイダー脅威の防止・探知のための共通ガイド第 3 版」実践事例 4 、P40

要とするが、研究施設へのアクセスを必要としない。これを電子的なアクセス管理の観点から言えば、例えば、これを人事部のファイルへのアクセス制御では、ファイルへのアクセス権を人事部に限定することであり、ネットワークによるアクセス制御で言えば、同様に、サーバーへのアクセス権を人事ネットワークセグメントからのものに限定することである。

「役割基盤のアクセス管理」により、従業員が組織に復讐しようとするとき、あるいは彼ら自身の目的のために、組織の IT 資産を侵害しようとするときにおいても、彼らがもたらす被害を局限することができる。

・**「任務分担（separation of duties）の原則」**（二人のルール （two-person rule）とも言われる。）

「任務分担の原則」とは、ある重要な任務の実行に２人の参加を求めることである。例えば、多額な銀行振出小切手の署名には、２人の銀行員の署名を必要とすること、又はソースコードが運用される前には、ソースコードの検証と審査を必要とし、検証と審査を別々の行員が実施することである。

「任務分担の原則」により、従業員が悪意のある行為を働く可能性を小さくすることができる。

・**「Need to Know の原則」**

「Need to Know の原則」とは、特定の IT 資産へアクセスできる人数を最小限にするということである。例えば、役職の高い管理者が、高いレベルのクリアランス（秘密情報取扱い資格）を保有しているからと言って、その管理者に、仕事の遂行に関係ない IT 資産へのアクセス権を付与しないことが重要である。

「Need to Know の原則」により、情報漏洩のリスクを大きく削減することができる。

次の事例９は、以上の原則が守られなかったために生起したインサイダー活動である。

▲事例９[15]

「通貨トレーダー（彼は、偶然、大学でコンピュータサイエンスを副専攻していた）は、組織で使用されるソフトウェア（取引を記録、管理、確認そして監査する）の多くを開発した。彼は、ソフトウェアに不正な機能を実装し、５年にわたり総額６億９，１００万ドルの違法な取引を隠ぺいすることができた。監査部門の要員がインサイダー活動に対して懸念を持ち、監査部門の監督者（その人は、インサイダーの監督者であった）に懸念を提起しが、監督者は、インサイダーが欲求不満になり退職するのを恐れて、監査部門の要員にインサイダーの活動について心配せず、懸念を提起するのを止めるように指示した。」

この事例は、インサイダー攻撃を防止できる又は早期に探知できる２つの方法を示している。

15「 インサイダー脅威の防止・探知のための共通ガイド第３版」実践事例８、P52

・組織の最重要なシステムのエンドユーザーには、システムを機能的に修正する許可又は直接基礎的データにアクセスする許可を与えてはいけない。（役割基盤の原則、最小特権の原則）
・最重要なデータを維持する責任とその同じデータを監査する責任を、同じ人に決して割り当ててはいけない。（任務分担の原則）

●対策４：厳格な物理的アクセス管理

セキュリティパスやドア管理システムなどによるアクセス管理は、無許可の人物の IT 資産への物理的アクセスを阻止することができるが、アクセス許可を有するインサイダーの IT 資産へのアクセスを阻止することはできない。しかし、一般に用いられている物理的なセキュリティ対策の中にもインサイダー対策として効果的なものがある。次の対策は、動機の強くないインサイダーに悪意のある行為を思い止まらせるという抑止効果がある。

・重要施設に、24 時間常駐する警備員を配置する。
・無許可の個人が組織の施設に入った時に、阻止・警告する警報を使用する
・施設への出入と重大な業務運営を記録するために、監視カメラを使用する。
・一人での勤務時間外の作業を禁止する。

また、昨年（2010 年 9 月）、イランの各地で産業用のコンピュータシステムが、数週間にわたりサイバー攻撃を受け、約３万台のパソコンが「スタックスネット」と呼ばれるコンピュータウイルスに感染した。この事案はイランの核施設を標的としていたため世界的に注目を集めた。この事案では、スパイがイランの原子力発電所の職員の自宅に忍び込み、USB メモリーに感染させたことも考えられる。この事案のように、職員が知らず知らず感染した USB メモリーを職場の持ち込みシステムに接続すれば、ほとんどのインサイダー対策が無効となる。唯一有効な対策は、不正デバイス（USB、PC カード、CD-R）を持ち込ませない手荷物検査である。リスクが高い場合は、身体検査が必要になるかもしれない。

▲事例 10[16]

「ある従業員は、雇用主によって、エネルギー管理施設の IT コンサルタントとして下請契約されていた。契約の停止が伝えられた後、彼は、日曜日の夜遅く、エネルギー生産設備へアクセスした。そして、彼は“緊急電源オフ”ボタンを押した。それにより、送電網間の交換を制御していたコンピュータシステムが停止した。彼は、緊急電源ボタンを囲んでいるガラスケースを壊すためにハンマーを使用した。２時間の間、コンピュータシステムの停止により、組織はエネルギー取引市場へのアクセスができなかったが、幸いにも、送電系統への直接の影響はなかった。この事例は、組織の事業にとって、最重要なシステムに打撃を与えるために、物理的管理体制の不備を悪用するインサイダーがもたらすリスクを例示している。」

16 「インサイダー脅威の防止・探知のための共通ガイド第 3 版」実践事例 6、P46

●対策５：厳格な電子的アクセス管理

ハッカーがリモートアクセスにより、大量のデータを書換えあるいは持ち出すことができる今日の環境において、ファイアウォールとアンチウイルスソフトの必要性は明らかである。しかし、その様な対策も、合法的なアクセス権を有する従業員が電子的なアクセス権を悪用することは防止できない。

従業員は、アカウントとパスワードによりネットワークにログインし、そのアカウントに認められたアクセス権を行使する。組織のアカウントが漏洩し、インサイダーがそのアカウントを使用すれば、彼はインサイダー攻撃を防止するために準備された管理対策を容易に回避するであろう。

インサイダーがアカウント（ID やパスワード）を盗み取るために使用する方法には、「アカウントクラック」又は「ソーシャルエンジニアリング」[17]で取得する方法、従業員同士で公然と共有するアカウントを使用する方法、及びコンピュータのテキストファイル又は電子メールに保管したパスワードを無人でログインしたままのコンピュータから取得する方法等がある。従って、パスワードは同僚からさえも保護されなければならない。そのためには、強いパスワードが使用され、パスワードは誰とも共有されず、パスワードは定期的に変更されなければならない。そして、全てのコンピュータは、指定時間内に入力がなければパスワードで保護されたスクリーンセーバーを自動的に始動するよう設定されていなければならない。

次の事例 11 は､パスワードセキュリティに対する従業員の認識の重要性を示している。

▲事例 11

「２人の臨時のデータ入力員と１人の正社員は、他の従業員のコンピュータアカウントを使用することによって、会社から約７万ドルを横領した。彼らのグループ内では、生産性を向上するために公然とパスワードを共有していた。システムの役割基盤に基づくアクセス付与により、他の従業員のアカウントには特権的システム機能へのアクセスが提供されていた。データ入力員は、ベンダーへの支払いを管理しているビジネスプロセスを破壊するために、これらのアカウントを許可なく使用した。最初に、彼らのアカウントを使い、有効なデータをデータベースに入力した。それから、彼らは、他の従業員の特権アカウントを使用してベンダーの名前と住所を彼らの友人や親戚のそれに改ざんし、システムから小切手を振り出した。それから、データ及びベンダーの情報をオリジナルなものへ戻した。約５ヵ月後に、総勘定元帳（General Ledger）部門の会計係が、発行された小切手の数が通常より多いことに気付き、さらに、調査によって小切手の不規則性が明らかになったことにより詐欺が発見された。」

●対策６：厳格な退職手順の履行

[17] 人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する方法のこと。

雇用されている間、組織のネットワーク、システム、アプリケーション、及びデータへのアクセス権を持っていた元従業員が退職したならば、彼の組織のネットワークとシステムへの全てのアクセス経路を無効化する厳格な手順を履行することが重要である。さもなければ、組織のネットワークは、インサイダーの無許可のアクセスに対して脆弱となる。

元従業員のすべてのアクセスを無効化する多層防衛が実行されていなければならない。まず、リモートアクセスは無効化されなければならないが、防衛の次の層は、アカウントである。元従業員によるすべてのアカウントの使用を無効化しなければならない。そうすれば、たとえリモートアクセスが設定されていても、従業員（インサイダー）がそれ以上侵入することを防止できる。従って、イントラネット・アカウント、特定用途向けアカウント、及びユーザーが許可された他の全てのアカウントが無効化されていること、パスワードが変更されていることが重要である。また、元従業員（インサイダー）が、他の人々、例えば従業員、顧客又は外部のウェブサイトユーザーのためのアカウントを設定する業務に就いていたならば、退職したインサイダーは、それらのアカウントにアクセス可能であることを肝に銘じるべきである。

退職手順には、物理的アクセスを防止するために、鍵、身分証明書、セキュリティパス、及び駐車許可証を確実に回収すること、必要に応じてコンビネーション鍵を変更するなどが含まれていなければならない。また、ある従業員が解雇された時に、他の従業員、特に警備員がその人物が解雇されたことを知っていることは重要である。退職した従業員が ID カードを忘れたと嘘を言い、組織への物理的アクセスを得て、インサイダー攻撃が容易に実行した例がある。

▲事例 12

「信用組合のシステムアドミニストレーターは、彼の仕事振りに不満だった雇用主によって予告なしに解雇された。その夜、彼は、技術的に劣った後任が自分のアクセスを無効化していないだろうと考えた。彼は、自宅からシステムにアクセスを試み、そして、後任がファイアウォールを通しての彼のアクセスを無効化していないことが分かった。彼のアカウントは無効化されていたが、後任者は、システムアドミニストレーター･アカウントのパスワードを変更していなかった。インサイダーは､組織の主サーバーを停止するためにそのアカウントを使用した。信用組合は、サーバーを正常に戻すのに３日を要した。この事例は、組織が１人のシステムアドミニストレーターの代わりとなる有能な人材を確保していない場合にもたらされる結果の重大さと完全にアクセスを無効化する必要性を示している。」[18]

（4）第 4 プロセス：捕まえる

18 「インサイダー脅威の防止・探知のための共通ガイド第 3 版」実践事例 14、P75

このプロセスには、従業員のセキュリティパスの使用とオンライン操作を記録（ログ）・監視・監査（以下、アクセス監視という）する、従業員の健全性を調査する、そして警察の捜査に協力する、という 3 つのステップが含まれている。

通常、建物のセキュリティロックでは、セキュリティパスの使用状況が記録され、情報システムではコンピュータ上で行われた処理や操作の動作記録（ログ）が記録される。そして、それぞれの記録やログを監視することにより、インサイダー活動の早期発見と調査・捜査に結びつけることができる。

●対策７：厳格な物理的アクセス監視

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、保護されたすべての出入口でのセキュリティパスの使用と使用の試みを記録し、通常、監査報告が自動作成される。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。しかし、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にプログラムするか又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定期的に監査報告を調査すべきである。

さらに、監視カメラシステム（CCTV）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。監視カメラシステムは、セキュリティ警報が本当であるかを判定するのに役立つとともに事件後の調査・捜査にとっても重要なものである。

●対策８：厳格な電子的アクセス監視

情報システムではコンピュータ上で行われた処理や操作の動作記録（ログ）が記録される。ファイルを開こうとしたが不成功の試みなどの失敗した操作もログが記録される。（図１「情報システム利用監視システムの概要」参照）アカウントが適切に管理されている組織は、高い可能性で、オンライン操作とそれらを実行したインサイダーを明確に結びつけることができる。従って、従業員のオンライン操作をログ・監視・監査することはインサイダー行為の早期発見と調査・捜査に必須である。

組織のネットワーク全体の操作を監視することが、複雑なインサイダー活動を探知するのに有効であるが、インターネットや電子メールを分離して監視することも有益である。インターネットの使用は、不適切なウェブサイトにアクセスしようとする従業員の試みを探知するために監視される。この文脈で言えば、政府転覆又は過激派を支援しているサイトが不適切なサイトに含まれる。また、電子メールサービスを監視・制限することによって、インサイダー行為のリスクを軽減することができる。例えば、①秘、極秘、及びその他の用語（例えば、政策の漏洩、商業的なデータを意味する用語）などのセンシティブな内容を意味する言葉によって、発信メールや添付ファイルをフィルタリングする、②悪意のあるソフトを組織のネットワークに持ち込むリスクを軽減するために、従業員がメールの添付ファイルを開くオプションをブロックする、などがある。

▲事例 13

「大きな国際企業は、リモートアクセスを監視しているときに、元コンサルタントが

そのネットワークへ無許可アクセスを行い、アドミニストレーター・アカウントを設定していたことに気付いた。直ちにインサイダーの以前のオンライン操作の調査が行われた。そして、その調査により、彼が 10 か月の間に 5 回にわたり、会社のネットワーク上でいくつかの異なるパスワードクラッキングプログラムを実行したことが分かった。最初は、彼は解読されたパスワードを会社のサーバーのファイルに格納した。後で、彼はより高度なパスワードクラッキングプログラムを会社のシステムにインストールした。このプログラムにより、彼は自動的に、すべてのアカウントとパスワードを定期的に組織外のコンピュータに転送することができた。会社従業員 5,000 人分のパスワードが首尾よく転送された。この事例はログと先行的な監視の重要性を示している。これらが実行されていれば、アカウントとパスワード又はバックドアアカウントを使用して悪意のある行動を犯す前に、このインサイダーの行為は探知されたであろう。」[19]

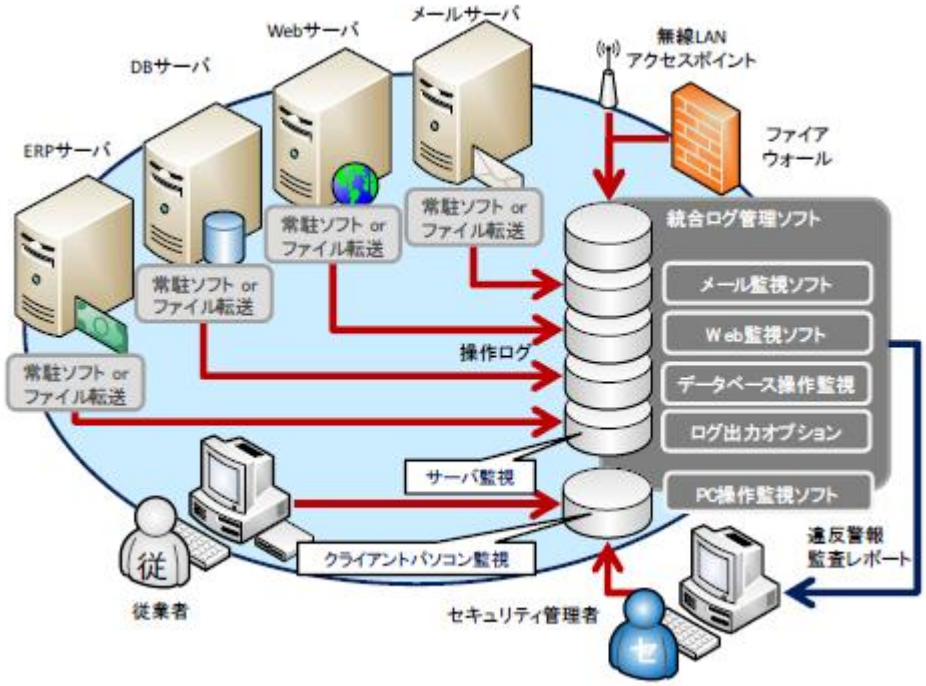

図１　情報システム利用監視システムの概要[20]

おわりに

インサイダー対策の要訣は、先ず、適切な情報セキュリティ対策を講じた上で、インサイダー脅威が現実であることを組織全体で理解・認識し、情報技術を越えて、組織のあらゆる機能を動員し、特に人事管理機能（雇用前調査、セキュリティ評価など）を活用して、インサイダー脅威に適切に対処することである。しかし、いかに優れたセキュリティ対策

19　「インサイダー脅威の防止・探知のための共通ガイド第 3 版」実践事例 12、P67

20　ＢＳＫ第２０－６号「インサイダー犯罪防止のための監視･監査体制のあり方」(平成１９年度)

のツールと技術を以ってしても、「組織のセキュリティ文化」が貧弱であったならば、組織はインサイダー脅威に対し脆弱となる。「組織のセキュリティ文化」とは、セキュリティに関して、組織全体に広く、深く根付いた態度と行動である。例えば、セキュリティは重要であり、それは各個人の責任であるという心の持ち方が従業員に浸透している。あるいはセキュリティ違反を発見したら通報するということが当然視されている、などである。組織はすべての従業員を対象とした教育・訓練を通して、次の事項を重視しつつ「組織のセキュリティ文化」を積極的に創造しなければならない。

・役割と責任を自覚させる。

従業員に対し、順守が求められる対策の理論的根拠を効果的に伝えることが不可欠である。もし、従業員が、なぜ、それぞれの対策が実施されているのか、彼らの責任が何かを理解したならば、彼らはより一層セキュリティ対策に取り組むであろう。

・通報ホットラインを提供する。

匿名あるいはその他の方法で、セキュリティ上の懸念又は疑惑を通報することができる信頼できるツールを社員に提供することは、セキュリティ文化の育成を手助けする積極的な方法である。しかし、意思疎通のよい組織では、通常、従業員が同僚等のセキュリティ違反行為を通報したいと思うときは、ライン管理者が最初の接点となるであろう。通報ホットラインは、この人間関係に変わるものではない。

・厳格な懲戒手順を定め、手順に従い厳格に処分する。

セキュリティ違反したことが明白な場合には、懲戒手続きに従うことが重要である。これにより、他の従業員に対し、このような行動が許されないことを示すとともに、セキュリティ規則を順守することを促すであろう。

最後に、インサイダー対策におけるライン管理者の重要性を指摘しておく。部下を直接監督・管理する役割を有するライン管理者は、部下の懸念ある行動を探知する責任と、従業員が個人的判断能力を弱めるような、あるいは第三者に対する脆弱性を高めるような環境（例えば、離婚または金銭的困難）にある時に適切に対処する責任を有している。万一、この様な時に、従業員に対して十分な支援を与えることができなければ、従業員は第三者の工作（ソーシャルエンジニアリング[21]）に取り込まれやすくなったり、または組織内でアクセス権を悪用しようとするかもしれない。しかるに、ライン管理者の「部下の異常な行動を探知する能力」や「部下の個人的な問題を適切に処理する能力」は様々である。そのような問題を解決する能力を示すことができないライン管理者に対しては、満足する技量に達するまで教育を継続しなければならない。（了）

---

[21] ソーシャルエンジニアリング（social engineering）とは、組織の部内者もしくは部外者が、情報を取得するため、またはアクセス権がない情報資産等へ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。

参考文献一覧

１．BSK 第 21－７号「インサイダー脅威の防止･探知のための共通ガイド第３版（Common Sense Guide to Prevention and Detection of Insider Threats 3rd Edition – Version 3.1)、米国カーネギーメロン大学のコンピュータ緊急対応センター、2009 年 1 月」

２．BSK 第 20－11 号「雇用中の人的セキュリティ：優れた実践事例ガイド（(ONGOING PERSONNEL SECURITY：A GOOD PRACTICE GUIDE)）、英国国家インフラストラクチャー保護センター、2008 年 10 月」

３．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)、英国国家インフラストラクチャー保護センター、2007 年 12 月」

４．ＢＳＫ第 20－６号「インサイダー犯罪防止のための監視･監査体制のあり方」

以下余白