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)

米国の国家対情報戦略(2008 年)

(THE NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA, 2008)

平成２１年１０月

財団法人 防衛調達基盤整備協会

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)

Dawn Cappelli

Andrew Moore

Randall Trzeciak

Timothy J. Shimeall

2009 年 1 月

本研究は Cylab の資金提供により実施された。

は　し　が　き

本刊行物は、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（以下、 CERT）が作成した「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） 」（２００９年１月）を翻訳したものです。なお、以前のＣＥＲＴの研究によるものは、平成１８年度に情報セキュリティの基本問題の調査研究として､『米国におけるインサイダー脅威の取り組み』(BSK 第 19-4)の中で取り上げており、また、付録に、同様の共通ガイドなどの紹介をしています。本刊行物は、新たな事例を研究することにより内容を更新したものや、新たに項目を設けたものなどを紹介した最新版です。

本刊行物には、インサイダー脅威の範囲を「現若しくは元従業員、契約者、又はビジネス・パートナー」としており、２００３年から２００７年に米国で発生した約１００件のインサイダーの事例の分析結果に基づく､１６件のインサイダー脅威の防止･探知のための優れた実践事例が提示されています。

米国セキュリティ･サービス、CERT、マイクロソフトなどが実施した「２００７年電子犯罪監視調査」によると、コンピュータ犯罪のうち犯人を特定できた事例の３１％がインサイダーによるものだったそうです。インサイダーによる攻撃の脅威は、現実に起こっており、そして経済的な損失は甚大なものになっています。経済的な損失の事例として、この刊行物の実践ガイドにも取り上げていますが、従業員が１億ドルに相当する設計図を盗み、台湾の競争相手にそれを売却した例があります。

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しますが、その一方で、内部からの脅威インサイダーを軽視する傾向にあります。組織の従業員、契約社員、及びビジネス・パートナーの潜在的危機を認識し、その脅威を企業のリスクアセスメントの一部として取り扱うことは組織にとって必須のことであります。

本刊行物が、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望外の幸せです。

平成２１年１０月

財団法人 防衛調達基盤整備協会
理事長　宇 田 川　　新　　一

目　　　次

１．導入

２００５年に、インサーダー脅威の防止と探知のための共通ガイドの第１版がカーネギーメロン大学のCylabから発刊された。この第１版は、コンピュータ緊急対応センター(Computer Emergency Response Team、 以下CERTという。）が実施したインサイダー脅威リサーチ、主として米国シークレットサービスと共同で実施したインサイダー脅威スタディー[1]に基づくものであった。この第１版には、スタディーの一部として１９９６年から２００２年の間に集められた、米国の最重要なインフラストラクチャー部門で生起した１５０件の実例の中から、悪意のあるインサイダー行為を防止・探知するために効果的であると思われる、１２件の実践事例の解説が入っていた。

２００６年７月に出版された第２版には、悪意のあるインサイダー行為のタイプ別の分析という新しい分析方法が取り入れられた。また、異なるタイプのインサイダー脅威（詐欺、機密情報又は専有情報の盗取、及びサボタージュ）のハイレベルの実態を取り上げた新しい項目が加えられた。さらに、カーネギーメロン大学のCylab[2]と国防省人的セキュリティ研究センター[3]の資金協力でCERTが実施した新しいインサイダー脅威リサーチによる新しい実践事例と更新された実践事例が**加えられた。**これらのプロジェクトは、これらの事例に見られる高水準のパターンとトレンドを見出すことを重視したインサイダー脅威問題の新しいタイプの分析方法を取り入れた。具体的には、それらのプロジェクトは、複雑な相互作用、リスクの相対的な度合い、方針、慣行、技術、インサイダーの心理的問題、**及び組織文化が時間を経たことによりもたらした意図しない結果を調査した。**

本版（第３版）は、再度、継続中の CERT の調査で得られた新しい洞察を反映している。Cylab は、継続して最新のインサイダー脅威の事例を収集・分析するために CERT のインサイダー脅威チームに資金を提供した。この継続した努力の目的は、インサイダーの攻撃を誘発する新しい組織的問題はもちろんのこと、インサイダーが攻撃に使用する方法の現状を理解することである。本版には、２００３年から２００７年に米国で発生した約１００件の実例の分析結果に基づく、新しい実践事例と更新された実践事例が

---

[1] インサイダー脅威スタディーの更なる情報は、次のURLを参照されたい。
http://www.cert.org/insider_threat/study.html

[2] Cylabが資金提供したインサイダーITサボタージュのメリットモデルに関する報告書は、次のURLからダウンロードできる。http://www.cert.org/archive/pdf/08tr009.pdf.

[3] 国防省と共同研究したCERTインサーダー脅威リサーチの報告書は、次のURLからダウンロードできる。http://www.cert.org/archive/pdf/06tr026.pdf.

加えられた。

本版には、CERT の研究者達がインサイダー犯罪を新しい方法で分析して得た、新しい調査結果を掲載している。これらの新しい調査結果は、CERT が分析した１１８件の窃盗事例と詐欺事例に基づくものあり、驚くべき発見が示されている。この研究の狙いは、インサイダー窃盗及びインサイダー詐欺の事例を分析し、事例全体から、インサイダーの行動、組織の事象又は状態、及び技術的課題のパターンを特定することであった。確認されたパターンによると、犯罪は、当初予想されていたものとは違い２つの異なる種類に分類された。

・金銭的利益のための情報の窃盗、又は改ざん ― この種類には、インサイダーが、部外者に情報を売却するために、組織のシステムから情報を窃取するか、あるいは自分自身、又はその他の人々の金銭的利益のために、組織のシステムの情報を改ざんする目的でアクセスを使用した事例などがある。

・ビジネス上の利益のための情報の窃盗 ― この種類には、インサイダーが、新しい仕事を得るため、又は自分自身のビジネスを始めるなど個人的なビジネス上の利益のために、組織のシステムから情報を窃取する目的でのアクセス使用した事例などがある。

各種類の犯罪が、時間とともにどのように進化したかを理解するのと同様に、金銭的利益のための窃盗、改ざん、IT サボタージュ、及びその他（上の３つの区分に属さないインシデント）など、各種類の犯罪をはたらく従業員のタイプの違いを理解することは、組織にとって重要なことである。本ガイドは、各種類の悪意のある行為で観察されたパターンとトレンドを掲載している。本ガイドでは、IT サボタージュについても若干の更新がなされたが、窃盗と改ざんについては最も重要な補強がなされている。

本ガイドには、第２版にはなかった幾つかの新しい事例が追加されている。また、第２版から引き継いだ各事例は、CERT のこの１年の研究から得た新しい洞察を反映するために ― あるものは大幅に、その他のものは若干 ― 修正されている。本ガイドには、新しい読者のために、第２版からの事例を再録している。さらに、「最近の調査結果」の項目は、全ての更新された慣行を取り入れているとともに、これまでのガイドでは取り組まれていなかった新しい課題を浮き彫りにする最近の事例が詳述されている。

“インサイダー脅威”とは何かに。

悪意のあるインサイダーについての CERT の定義は、

> **現、若しくは元従業員、契約者、又はビジネス・パートナーで次に該当する者をいう。**
>
> **・組織のネットワーク、システム、又はデータへのアクセスが与えられている者、又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を悪用する者**

ここで留意すべきことは、本ガイドでは、秘密に指定された国家安全保障に関する情報に関連したスパイ事例のインサイダー脅威が除外されていることである。

インサイダー脅威の範囲は、元従業員からもたらされるという伝統的な脅威を越えて拡大している。具体的には、CERT チームは、インサイダー脅威の拡大した範囲の中から、次の重要な新しい課題に注目した。

・部外者との共謀

インサイダー脅威は、組織の境界を超えて拡大した。金銭的利益のために情報を窃取又は改ざんしたインサイダーの半数は、実際に犯罪組織、外国組織、又外国政府を含む部外者によって勧誘されたものである。

本ガイドの“金銭的利益のための窃盗又は改ざん”というタイトルの項に注意を払うことが重要である。この項は、あなたが、勧誘に影響されやすい従業員のタイプを理解するのに役立つであろう。

・ビジネス・パートナー

CERT リサーチチームによって指摘された最近の傾向は、組織の従業員でなく、組織のネットワーク、システム、及びデータへのアクセスを与えられている信頼されたビジネス・パートナーの従業員によって行われたインサイダー犯罪の増加である。この脅威に対応するための提言は事例１に示されている。

・合併と買収（M&A）

企業から CERT チームに寄せられた最近の懸念は、他の組織によって買収された組織の中にインサイダー脅威の高められたリスクである。従業員がストレスと不確

実な組織の雰囲気に耐えている状態にあるので、組織が、買収側や買収される側、双方のインサイダー脅威の増加を認識することが重要である。合併と買収(M&A)に関係する読者は、本ガイドのほとんどの事例に特別な注意を払わなければならない。

・文化的相違

CERT のインサイダー脅威のモデル化において観察された多くの行動パターンは、本ガイドを通して反映されている。しかし、読者は、文化的な問題が従業員の行動に影響を及ぼすことを理解することが重要である。: 米国外で育てられたか、あるいは長い期間を米国外で過ごした人々は、これらと同じ行動パターンを示さないであろう。

・米国外の問題

CERT のインサイダー脅威リサーチは、米国内で生起した事例に基づいている。米国外において支店を運営している米国企業は、従業員の行動に影響する文化的な違いに加えて、本ガイドの一部を他国の法律や政策の違いに合わせる必要があることを理解しなければなりません。

インサイダーは、本当に脅威か。

インサイダーからの攻撃の脅威は、現実でありかつ相当なものである。米国セキュリティ･サービス、CERT、マイクロソフト、及びCSO (Chief Security Officer) マガジンが実施した「２００７年電子犯罪監視調査」[4]では、回答者が電子犯罪の犯人を特定できた事例の３１％がインサイダーであった。さらに、回答者の４９％は、その前年に少なくても１件の悪意のあるかつ意図的なインサイダー・インシデントを経験していた。インサイダー攻撃の影響は壊滅的である。メーカーで働いていたある従業員は、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。

カーネギーメロン大学は、過去数年に亘って、インサイダー脅威に関するいろいろな研究プロジェクトを実施してきた。到達した結論の一つは、インサイダー攻撃は、あらゆる組織で生起し、しばしば、組織に重大な損害をもたらしたということである。これらの実例には、次のものがある。

・個人的利益のために機密、又はセンシティブ情報を改ざんするか、あるいは盗み取るような “ローテク” 攻撃

---

[4] 「２００７年電子犯罪監視調査」は、次のURLを参照にされたい。
http://www.cert.org/archive/pdf/ecrimesummary07.pdf

・ビジネス上の利益に使用するか、あるいは外国の政府若しくは組織に手渡すための企業秘密、又は顧客情報の窃盗
・組織のデータ、システム、又はネットワークを破壊する技術的に高度な犯罪

これらの犯罪がもたらす多くの損害は、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、組織の評判もまた著しく傷つけられる。

インサイダーは、組織に害を加えたいと思っている部外者などよりも、害を引き起こすのに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物理的及び技術的対策を回避することができる。ファイアウオール、IDS（侵入検地システム）、及び電子的建物アクセスシステムのような仕組みは、主として外部の脅威から防御するために実装されている。しかし、インサイダーは、組織が使用している方針、手順、及び技術を知っているだけでなく、しばしば、順守されていない方針や手順、又は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。

CERT のリサーチによると、広範囲で受け入れられている情報セキュリティのための優れた実践事例を使用すれば、調査した多くのインサイダー攻撃を防止できたことを示している。インサイダー脅威事例に関する CERT のリサーチには、各組織が如何にすれば攻撃を防止できたのか、又は少なくても攻撃前に探知することができたのかの調査が当然含まれている。以前の版（１版及び２版）では、悪意のあるインサイダーがもたらすリスクを軽減するため、極めて重要な既存の優れた実践事例を特定した。

本版は、新しい研究方法と最近の事例の背景からの要因による追加的な優れた実践事例を特定した。そして、既に確立した優れた実践事例と結びつかない、調査結果に基づくインサイダー脅威に対処するための幾つかの新しい提案を示した。

今日までの我々の研究に基づき、本報告で概説された実践事例は、インサイダー脅威を軽減するために最も重要なものばかりである。

誰がこの報告書を読むべきか。

このガイドは、様々な読者を対象としている。組織の意思決定者は、これを読むことから利益を得ることができる。インサイダー脅威は、技術的、行動的、及び組織的問題の組合せから影響を受けるので、方針、手順、及び技術的方法で対処されなければならない。従って、管理部門、人事部門、情報技術部門、ソフトウェア・エンジニアリング部門、法律部門、セキュリティ部門、及び重要データの管理部門が、問題の範囲を理解し、組織の全ての従業員にそれを伝え、理解させることが重要である。

本ガイドは、インサイダー脅威を防止するために組織全体で履行すべき実践事例を概説している。本ガイドは、各実践事例を説明し、何故、それが履行されなければならないかを解説している。そして、それが如何に攻撃を防止し、又は早期の発見を容易にするのかと同様に、それが履行されていなければ、何が起こるかを示す複数の実例を提供

している。

これらの実践事例の履行について書かれた多くの参考資料がある。(この話題に関する参考資料のリストは、このガイドの最後に掲載されている。) この報告書は、これらの実践事例の概要を提供するとともに、読者に現行の組織の方針、プロセス、及び技術的管理の見直しが必要であることを認識させることを目的としている。

インサイダーを阻止することできるのか。

インサイダーを阻止することはできるが、それは複雑な問題である。インサイダー攻撃は、方針、手順、及び技術的管理からなる多層防衛戦略を通じてのみ防止することができる。従って、管理者は、業務上の方針と手順、組織文化、及び技術的環境を含む組織の多方面に注意を払わなければならない。即ち、情報技術を超えて、組織全体の業務プロセスと各プロセスに使用されている技術との相互作用まで深く究明しなければならない。

２．謝辞

米国シークレットサービスは、**インサイダー脅威スタディー**を後援するに際し、CERTの研究のために、単に資金提供する以上のものを提供した。CERT の情報セキュリティ専門官及びシークレットサービスの国家脅威評価センター（National Threat Assessment Center）の行動心理学者から構成された共同研究チームは、研究方法を定義するとともに、後に CERT が実施するインサイダー脅威リサーチの基礎となる研究を実施した。シークレットサービスが最初の研究を後援するとともに共同研究を実施し、その研究から得た価値ある事例集を現在実施中の研究に利用することを許可したことに対して、コミュニティを代表してシークレットサービスに深く感謝の意を表する。特に、CERT は、国家脅威評価センターの Marisa Reddy Randazzo 博士、Michelle Keeney 博士、Eileen Kowalski 氏、及び Matt Doherty 氏、並びにこの研究の間、シークレットサービスとの連絡･調整を担当した Cornelius Tate 氏、David Iacovetti 氏、 Wayne Peterson 氏、及び Tom Dover 氏に対し謝意を表する。

また、著者は、事例を調査・集成し、インタビューを実施するとともに、研究報告書の作成を手助けしたインサイダー脅威研究チームの CERT メンバーである Christopher .Bateman 氏、Casey Dunlevy 氏、Tom Longstaff 氏、David Mundie 氏、Stephanie Rogers 氏、Timothy Shimeall 氏、Bradford Willke 氏、及び Mark Zajicek 氏に感謝の意を表する。

インサイダー脅威スタディーの開始以来、CERT チームが心理学者の協力を得られたことは幸運であった。彼らは、広範な経験と新しい考えで我々の仕事に貢献した。: CERT インサイダー研究チームの客員研究員である Eric Shaw 博士は、ほとんどのインサイダー脅威プロジェクトに貢献した。連邦捜査局（FBI）行動科学ユニットの元チーフである Steven Band 博士は、心理的問題に専門的な知識･技能を提供した。そして、国防省の人的セキュリティ研究センターの Lynn Fischer 博士は、CERT の最初のインサイダー脅威リサーチを後援するとともに、現在も様々なインサイダー脅威プロジェクトについて CERT チームとともに働き続けている。

CERT チームは、Cylab による途絶えることのない資金提供に深く感謝する。企業及び政府内、並びに米国内及び海外において、Cylab により後援されたインサイダー脅威リサーチの影響は非常に大きい。Cylab は、CERT チームが政府や企業、経営者や技術スタッフなど、全てに役立つ研究を行うことを可能とする重要な資金を提供した。特に、我々は、インサイダー脅威リサーチの開始から CERT を支持し続けた Pradeep Khosla 氏、Don McGillen 氏、及び Linda Whipkey 氏に感謝の意を表する。同様に、過去１年、一緒に楽しく仕事をした Richard Power 氏、Gene Hambrick 氏、Virgil Gligor 氏、及

び Adrian Perig 氏に感謝の意を表する。

CERT チームは、ここ数年に亘り、様々な Cylab の大学院生からも支援を受けた。Akash Desai 氏、Hannah Benjamin-Joseph 氏、Christopher Nguyen 氏、Adam Cummings 氏、及び Tom Carron 氏の各大学院生は、熱心にチームに加わり、そして彼らの貴重な時間を CERT インサイダー脅威プロジェクトに捧げた。特に、Tom Carron 氏に深く感謝する。彼は、CERT/CyLab インサイダー脅威チームの現メンバーとして、喜んで全てを投げ出し、この報告書をできる限り魅力的なものにするために必要な具体的な例を探すために何度も何度もデータベースを検索した。

シークレットサービスは、CERT インサイダー脅威リサーチに 150 件のオリジナルの事例を提供した。CyLab の研究は、追加された事例に関する資料の特定と収集を必要とした。CERT チームは、カーネギーメロン大学ソフトウェア工学研究所 (Software Engineering Institute : SEI)の図書館長 Sheila Rosenthal 氏の多大なご尽力に対し厚く感謝の意を表する。Sheila 氏は、Cylab が後援した研究チームが使用した 100 件以上の新しい事例関連した豊かな資料源を獲得することに尽力された。

最後に、CERT は、関係した組織、検察官、及び捜査官、並びに研究の質をさらに高めるためにチームに機密文書を提供することに合意・協力したインサイダーの全ての人々に謝意を表する。従業員を幸福にし、問題が拡大する前に解決するためには、“良い人（good guys)”全てが団結し、情報を共有することが重要であるとともに、悪意のあるインサイダー攻撃を防止するため又は破壊的な攻撃の前兆を察知するために、我々の技術的資源とビジネスプロセスを使用することがコミュニティにとって必須である。

３．悪意のあるインサイダー行為の種類別に観察されたパターンと傾向

CERT のインサイダー脅威チームは、約２５０件のインサイダー脅威の実例を収集した。これらの実例の１９０件がこの報告のために詳しく分析された。残りの事例は、使用できる十分な情報がないか、あるいはこのガイドの出版時点で裁判中であるかなどのため、未だ正式な分析がなされていない。

本セクションは、悪意のあるインサイダー行為の種類別に観察されたパターンと傾向を提示している。

- **IT サボタージュ：**現、もしくは元従業員、契約者、又はビジネス・パートナーが、特定の個人、組織、又は組織のデータ、システム及び日常の業務遂行を害するために、ネットワーク、システム、又はデータへの許可されたアクセスレベルを意図的に超えた又は悪用した事例。

- **金銭的利益のための窃盗又は改ざん：**現、もしくは元従業員、契約者、又はビジネス・パートナーが、経済的利益のために、組織の機密又は専有情報（proprietary information : 企業が知的所有権を有する情報）を窃取、又は改ざんする意図をもって、ネットワーク、システム、又はデータへの許可されたアクセスレベルを故意に超えた、又は悪用した事例。

- **ビジネス上の利益のための窃盗又は改ざん：**現、もしくは元従業員、契約社員、又はビジネス・パートナーが、ビジネス上の利益を目的のために、組織の機密又は専有情報を窃取、又は改ざんする意図をもって、ネットワーク、システム、又はデータへの許可されたアクセスレベルを故意に超えた、又は悪用した事例。

- **その他：**現、もしくは元従業員、契約社員、又はビジネス・パートナーが、経済的利益以外、又はビジネス上の利益以外の動機により、組織の機密又は専有情報を窃取する意図をもって、ネットワーク、システム、又はデータへの許可されたアクセスレベルを故意に超えた、又は悪用した事例。

インサーダー事例の４つの種類別内訳は図１[5]のとおり。

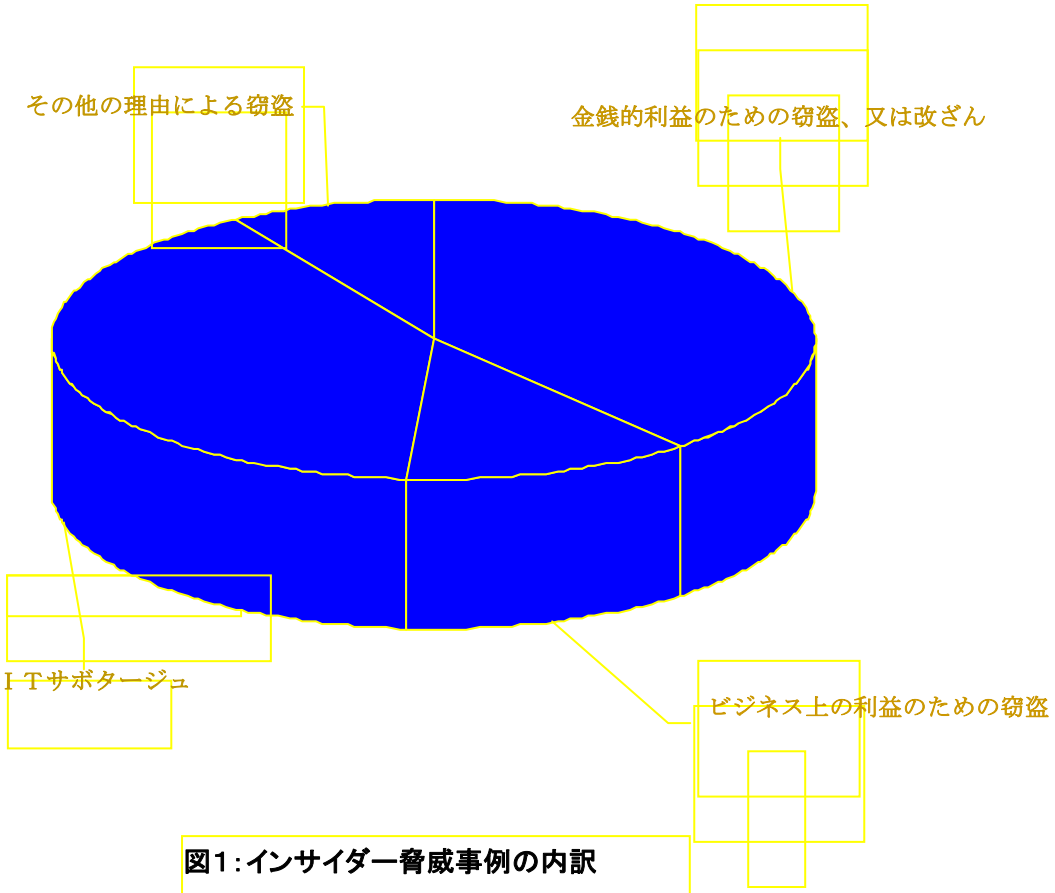


図1：インサイダー脅威事例の内訳

幾つかの事例は、複数の種類に分類される。例えば、一部のインサイダーは、雇用主のシステムに対して IT サボタージュ行為を行い、そして、金銭と引き換えにシステムの回復だけを支援すると申し出て、金銭をゆすり取ろうとした。この様な事例は、「IT サボタージュ」と「金銭的利益のための窃盗又は改ざん」の両方に分類される。１９０件のうち４件が、「金銭的利益のための窃盗又は改ざん」と「IT サボタージュ」に分類された。もう一つの事例には、他の仕事に就く前に、顧客データベースと販売用のパンフレットをコピーされたことに、営業担当副社長が関係していた。この事例は、「ビジネス上の利益のための情報の窃盗」と「IT サボタージュ」に分類された。最後に、三つの事例が「IT サボタージュ」と「その他のための窃盗」に分類された。

[5] １９０件の事例が、この報告書のために分析された。しかし、一部の事例は、複数の犯罪種類に分類された。

種類が重複する事例の数は図２[6]のとおりである。

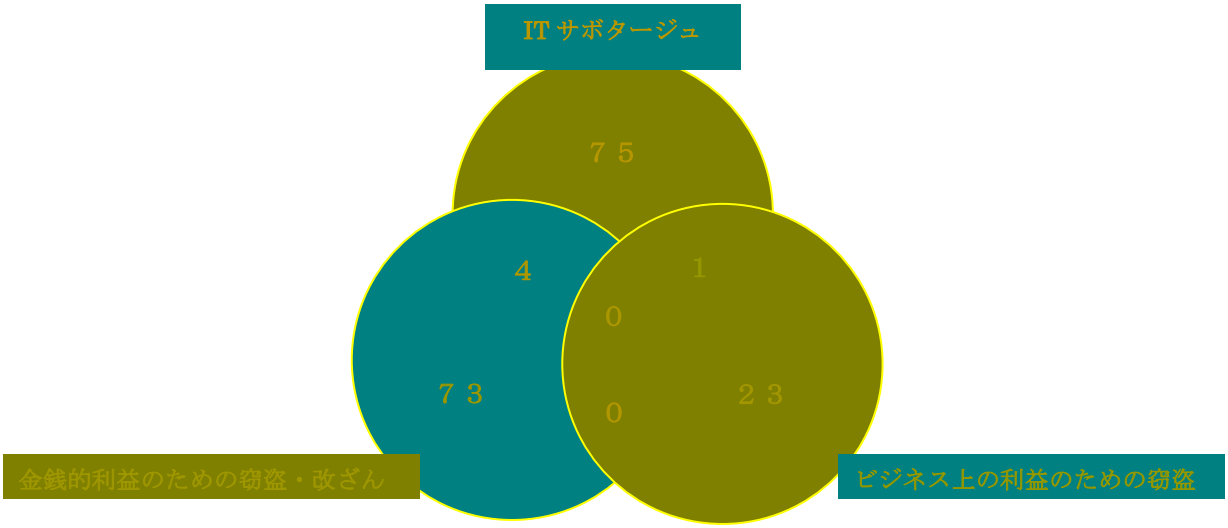


図 2：インサイダー脅威の種類の重複

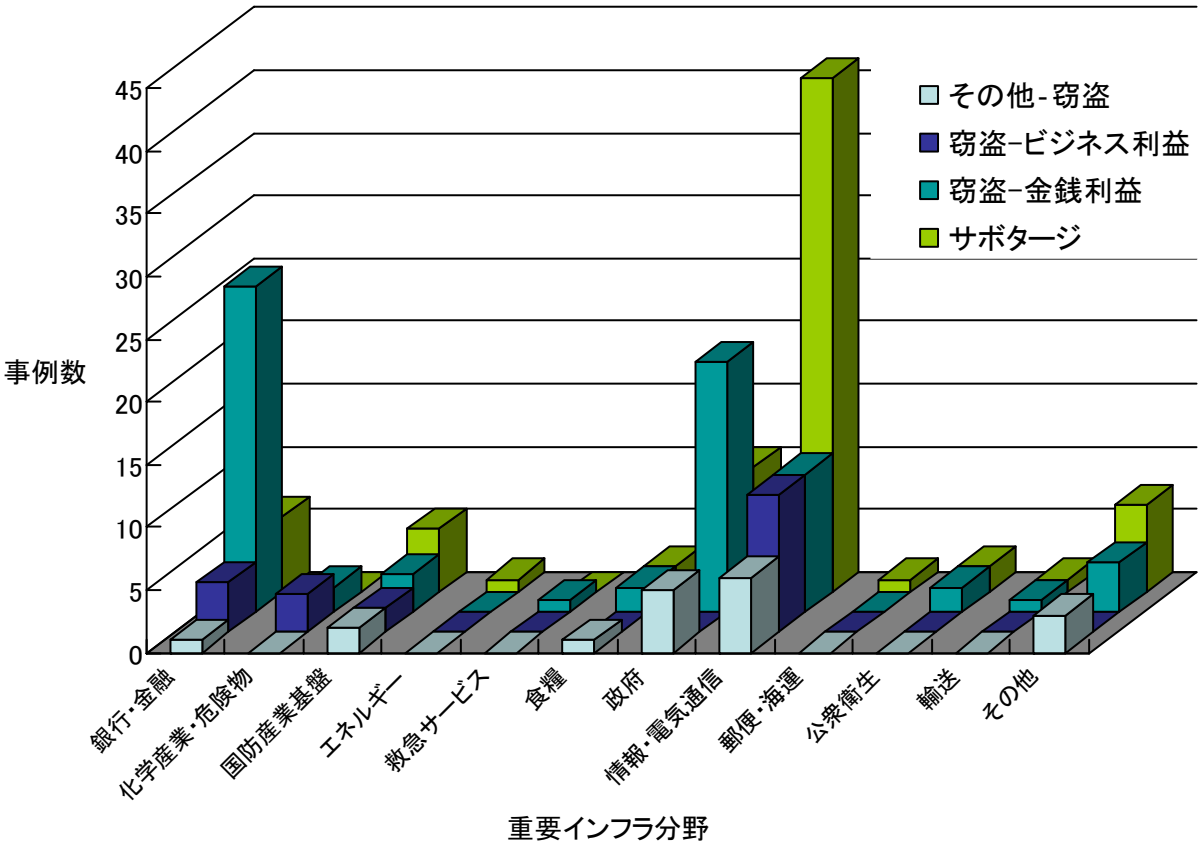
[6] 動機が金銭的利益又はビジネス上の利益でもない１７件の事例は、その他に分類された。この 17 件は、この図 2 には含まれていない。

図３は、重要なインフラストラクチャー分野別の犯罪種類別事例数である。分野別の違いに着目すると興味深い。例えば、「金銭的利益のための情報の窃盗」が銀行・金融分野で最も突出していることは驚くことでない。しかし、政府分野の「金銭的利益のための情報の窃盗」が二番目で、情報技術・電気通信分野が三番目であることは少々予想外であるかもしれない。

他方、「ビジネス上の利益のための情報の窃盗」では、情報技術・電気通信分野に非常に集中し、二番目は銀行･金融分野である。化学･有害物質分野と防衛産業基盤分野は「ビジネス上の利益のための情報の窃盗」を経験したその他のたった２つの分野である。

IT 分野の「IT サボタージュ」の事例数はとても際立っている。「IT サボタージュ」攻撃の数では政府分野が二番目である。　「IT サボタージュ」攻撃を受けなかった２つの分野は化学産業・危険物質分野と救急サービス分野であったことに注目すべきである。：この２つの分野を除いたその他の分野は、少なくとも一回は攻撃を経験している。

図3：重要インフラ分野別の犯罪の内訳



⑴　IT サボタージュ

本報告では、インサイダーの「IT サボタージュ」事例は、次のように定義される。: 現、もしくは元従業員、契約者、又はビジネス・パートナーが、特定の個人、組織、又は組織のデータ、システム若しくは日常の業務遂行を阻害することを意図して、ネットワーク、システム、又はデータへの許可されたアクセスレベルを意図的に超えた、又は悪用した事例。

CERT の研究者は、1996 年から 2007 年の間に米国で発生した 80 件の「IT サボタージュ」を分析した。

誰が、インサイダーであったか。

「ITサボタージュ」をはたらいたインサイダーは、主として男性で、高い技術的配置に就いていた。そして、大多数がシステム・アドミニストレーターとして、又は特権的アクセスが与えられて雇われていた。しかし、米国労働省労働統計局[7]によると、2007 年のコンピュータと数学に関連する職業における全ての従業員の７４％が男性であった。従って、サボタージュが典型的に高度な技術を有する従業員によって行われたことに注目することは有用であるが、男性従業員にだけ注意を集中することはたぶん論理的な結論ではないであろう。さらに、「ITサボタージュ」をはたらいたインサイダーの大多数は元従業員であった。

何故、彼らはそれを犯したのか。

半数以上のインサイダーが不満を抱いていたことが分かっている。そして、彼らのほとんどが、引き金となった事象への復讐から行動した。否定的な事象の例には、解雇、雇用主や監督者との論争、異動、又は降格、並びに昇給又はボーナスへの不満が含まれる。

如何に、彼らは攻撃したか。

「IT サボタージュ」をはたらいたインサイダーの大多数は、攻撃を行った時点でアクセス権を持っていなかった。わずか３０％が、彼ら自身のユーザー名とパスワードを使用し、その４３％がアカウントを侵害した。２４％は、他の従業員のユーザー名とパスワードを使用し、１６％が、彼らが事前に設定した無許可のアカウント（バックドア）を使用した。また、彼らは、退職手続で見落とされたものを含む共有アカウントを使用し、その２３％は、システム・アドミニストレーター又はデータベース・アドミニストレーター（DBA）アカウントを使用し、１１％は、テストアカウント又は訓練アカウントなどのその他の共有アカウントを使用した。

---

[7] 米国労働省労働統計局のＵＲＬはhttp://www.bls.gov/cps/cpsaat9.pdf である。

３５％は、攻撃を実行するために高度な技術的手段を使用した。一般的に使用された技術的方法には、論理爆弾（以下、ロジボム）のようなスクリプト、もしくはプログラムを書き込むこと、又は後で利用するためにバックドア・アカウントを設定することが含まれる。その他の技術的手法には、顧客のコンピュータにウイルスを植え込む、パスワードクラッカーを使用する、遠隔システム管理ツールをインストールするなどが含まれる。

特に、彼ら（インサイダー）が解雇を予想した事例では、約３０％が攻撃前の技術的準備措置を行った。例えば、彼らは、ロジボムを書き込み、テストし、そして仕掛けた。さらに、バックアップを破壊し、バックドア・アカウントを設定した。ほとんどのロジボムは大量のデータを削除するよう設計されていた。しかし、少なくとも一つは、インサイダーが解雇された後６ヶ月後に、密かにビジネスを妨害するよう設計されていた。幾つかのバックドアはかなり露骨であり、アカウント監査で簡単に発見できたが、その他は上手く隠されていた。ほとんどのインサイダーは、リモート・アクセスを使用して通常の勤務時間外に攻撃を行った。

如何に、それらは探知されたのか。

ほとんどの攻撃は、システムの故障、又は異状により手動で探知された。セキュリティ担当者でない者が、しばしば、攻撃を探知した。そのうちのほぼ２５％は顧客が探知した。攻撃の探知に責任を有する従業員には、監督者、同僚、及びセキュリティスタッフが含まれる。

インサイダーが、攻撃を準備・実施する前に、観察可能な懸念される行動が示された。共通の行動上の前兆には、監督者や同僚との争い（時には、とても怒っているか、又は暴力的である）、作業能力の低下、怠慢、又は無断欠勤などがあった。幾つかの事例では、管理者は気がつかなかったか、あるいは問題を無視した。その他の事例では、組織による制裁が問題を解決するより、むしろインサイダーの懸念される行動を増大しただけであった。

如何に、インサイダーは特定されたのか。

ほとんどの事例では、インサイダーを特定するために、リモート・ログ、ファイルアクセス・ログ、データベース・ログ、アプリケーション・ログ、及び電子メール・ログなどのシステム・ログが使用された。ほとんどのインサイダーは、自らの行為を隠蔽するため、ログが犯人特定に使用されることを知り、ログを改ざんすることで隠蔽を企てたり、他のだれかを、彼らの行動に巻き込むためにログを改ざんしたりしていた。

どのような影響があったのか。

事例の６３％で、組織は、システム、又はネットワークの停止によるビジネスの停止、顧客記録の紛失、ソフトウェア、システムの損害、もしくは破壊により製品の製造不能などの幾つかの種類のビジネス上の影響を被った。

その他の否定的な結果は、次のものから生起した。

・消極的なメディアの配慮
・戦略計画、又は間近に迫った一時解雇の計画などの個人的情報が入っている管理電子メールの顧客、競争者、又は従業員への転送
・社会保障番号のような個人情報の暴露
・正当な情報が無効、又は厄介な内容に書き替えられるなどのウェブサイトの改ざん
・公開ウェブサイト上での機密個人情報の公表

事例の２８％で、個人が損害を被った。個人に対する侵害の例には、脅迫、監督者、又は同僚を巻き込むための証拠の改ざん、及び個人情報又はプライベート情報の暴露が含まれる。

IT サボタージュに関する詳細な解説は、「米国最重要インフラストラクチャー全体への IT サボタージュの“全体像”」を参照にされたい。右文献は、次の URL からダウンロードできる。 http://www.cert.org/archive/pdf/08tr009.pdf.

⑵ 金銭的利益のための窃盗又は改ざん

本報告では、インサイダーの「金銭的利益のための窃盗又は改ざん」事例は次のように定義される。: 現もしくは元従業員、契約者、又はビジネス・パートナーが、金銭的利益のために、組織の機密又は専有情報を窃取、又は改ざんすることを意図して、ネットワーク、システム、又はデータへの許可されたアクセスレベルを故意に超えた、又は悪用した事例。

CERT の研究者は 1996 年から 2007 年に亘り、米国で発生した７７件の「金銭的利益のための窃盗又は改ざん」事例を分析した。７３件は、単に「金銭的利益のための窃盗又は改ざん」であったが、4 件は「IT サボタージュ」にも関連していいた。

誰が、インサイダーであったか。

この種類の犯罪を行ったインサイダーのうちのわずか 5 名が元従業員で、その他の者はすべて、違法行為を行った時点で現従業員であった。これらのインサイダーの半数は男性で、半数は女性であった。この種類の犯罪を行ったインサイダーは、どちらかと言

えば、組織の“より低いレベル”の非技術系の仕事に従事していた。彼らの業務には、データ入力及び個人情報（Personally Identifiable Information：PII）、又は顧客情報（Customer Information：CI）の管理で、多くはデータ入力係、又は一般事務員（clerk）に分類された。

何故、彼らはそれを犯したのか。

この種類の全てのインサイダーの主要な動機は、金銭的利益である。インサイダーは、それを売るために盗み、彼ら自身、友人、又は家族の金銭的利益を得るためにデータを改ざんし、又は情報を改ざんすることで部外者から報酬を得た。一部のインサイダーは、彼らの親戚に副収入を提供することが動機付けとなった。少数のインサイダーは、大きなクレジットカードの負債を抱えて、あるいは薬物に関連して財政難に陥っていた。

これらの攻撃の多くは、長い期間継続した企てであり、インシデントのおよそ３分の１は１年以上継続した。攻撃が短かったものの半数は、インサイダーがすぐに捕まったからである。その他の半数は、従業員が退職する時、又は退職直後に犯罪が行われたからである。

これらの事例のインサイダーは、組織外の人物、又は別のインサイダーと共謀していた確率が極めて高い。一部の事例では、インサイダー２名と部外者との共謀が行われていた。
金銭的利益のためのインサイダー窃盗事例では、３分の２の事例でインサイダーは部外者と共謀し、３分の１の事例でインサイダーは組織内の人物と共謀した。これらの窃盗事例では、事例の半数で部外者は、犯罪を行うためにインサイダーを勧誘した。事例の３分の１未満でインサイダーは単独で行動した。

金銭的利益のための情報の窃盗事例における勧誘パターンでは、部外者が、個人情報（PII）又は顧客情報（CI）へのアクセスができる給与の低い非技術系従業員をインサイダーとして勧誘した。インサイダーが情報を窃取し、部外者がインサイダーに報酬を支払うとともに詐欺、又はなりすまし犯罪にその情報を使用した。

一部のインサイダーは、データ、例えば、信用履歴（クレジットカード記録）を改ざんして報酬を得た。信用履歴が良くない人物から報酬を得たインサイダーもいれば、貸付承認の受益者から利益を得る人物（自動車デーラーのような）から報酬を得たインサイダーもいた。別のインサイダーは、医療保険に加入するために運転許可証を偽造し、相当額の偽の請求書を作成した。さらに、別のインサイダーは、身元証明書を偽造し報酬を得た。
最後に、一部のインサイダーは、組織のシステムやビジネスプロセスを熟知していた

ので、改ざんを計画・実行することができた。例えば、給与支払マネージャーは、給料支払簿に毎週夫を加え、夫宛の給与支払小切手を作成し、３０万ドル以上を雇用主からだまし取ったあと、発見されるのを避けるために給与支払システムから夫を直ちに削除した。彼女の犯行は、彼女が退職して約１年後、会計係が無許可の小切手に気がついてようやく発見された。

金銭的利益のための情報の改ざん事例では、半数の事例で、インサイダーは部外者と共謀し、その他のほぼ半数の事例で、組織内部者と共謀していた。そして、３分の１未満の事例で、部外者が犯行のためにインサイダーを勧誘し、３分の１の事例で、インサイダーは単独で犯行に及んだ。

如何、彼らは攻撃したのか。

インサイダーの９５％は、通常の勤務時間内に、情報を窃取又は改ざんし、７５％以上が許可されたアクセス権を使用した。２５％のインサイダーは、犯行に及んだ時点で許可されたアクセス権を有していなかった。**許可されたアクセス権を使用したインサイダーは、すべ**て合法的なユーザーであった。このうちの５人は、システム・アドミニストレーター又はデータベース・アドミニストレーターのアクセス権を、１５％未満は、特権的アクセス権を有していた。ほとんど全てのインサイダーは、データを窃取又は改ざんするのに合法的ユーザーコマンドだけを使用した。犯罪の１６％だけが、スクリプト、もしくはプログラムの使用、バックドアーアカウントの設定、又はアカウントの侵害のような高度な技術的技法を必要とした。

インサイダーの８５％は、犯罪をはたらくために自分のユーザー名及びパスワードを使用した。１０％強は、他の誰かのアカウントを侵害し、２人はログインされたままの無人のコンピュータを使用し、１人は顧客アカウントを使用し、さらにもう１人は社内で使っている訓練アカウントを使用した。９件の事例では、インサイダーは、ソーシャルエンジニアリングの手法でアカウントを侵害することができた。一部のインサイダーは犯罪をはたらくために２つ以上のアカウントを使用した。

２人のインサイダーだけが、違法行為を行う準備のために技術的予備行動を行った。１人は、不正な医療行為提供者がデータベースに追加されるようにした。もう一人は、システムの高度に制限された機能が使用された時に、セキュリティスタッフへ自動通知する機能を無効にした。それから、彼は、彼の不正な企てを実行するためにその機能を使用した。

如何に、それらは探知されたのか。

インサイダーのうちわずか１人が、ネットワーク監視活動により探知された。半数は、請求書、チケット、個人の信用履歴の否定的な徴候などの不審な行為を含むデータ異状

により探知された。大部分の事例は、顧客、法執行官（警官等)、同僚、情報提供者（informant)、監査人、又はその他疑いを持った外部の人物からの通報など、非技術的な手段で探知された。５件の事例では、電子メール又はオンライン上で情報が直接競争業者に売りに出された時にインサイダーが探知された。ほとんどの悪意のある行為は、結果的には複数の人々によって探知された。事例の５０％以上は、非 IT セキュリティ要員によって内部的に探知された。２６％は組織の取引先又は顧客によって、約１０％は顧客によって、そして５％は競争業者によって探知された。

如何に、インサイダーは特定されたのか。

ほとんどの事例で、データ・ログ、システムファイル交換・ログ、ファイルアクセス・ログなどのシステム・ログがインサイダーを特定するために使用された。

どんな影響があったか。

本報告で分析された窃盗、又は改ざんの事例では、インサイダーの組織だけでなく、その他の罪のない犠牲者にも影響があった。例えば、小切手詐欺では、罪のない人の口座に対して切られた偽の小切手のために、罪のない人が督促状を受け取ることになった。その他の事例では、機密の顧客データへ不正アクセスしてクレジットカード詐欺をしたり、法廷記録を改ざんして司法システムを壊した事例がある。一部の事例は、複数のインサイダーが不法入国者又は法的には取得資格のない人々のために、公式の身元確認資料又は運転免許証を偽造した事例や、あるインサイダーが不法入国者が米国に残留できるようにするため、また、亡命を認めない決定を覆すために、データベースを改ざんし、そして報酬を得た事例など非常に重大な結果をもたらした。

インサイダーの組織もこれらの犯罪の結果として、財政的損失のみならず、悪い意味でのメディアの注目を集めるなど損害を被った。あるインサイダーは、州の保険基金に対して合計でおよそ８５万ドルの詐欺をはたらいた。同じ会社で働いていたもう一人のインサイダーは、およそ2,０００万ドルの詐欺又は不審な取引に関連していた。また、別のインサイダーは、連邦機関に対して６０万ドル以上の詐欺をはたらいた。サボタージュと詐欺の双方が関係した事例では、あるインサイダーは、会社のサーバーから１００億個を超えるファイルを削除して会社の突然の株価の下落から彼自身が利益を得るように設定した。組織は回復費用に３００万ドルを要した。

⑶　ビジネス上の利益のための情報の窃盗

本報告では、機密、又は専有情報の窃盗に関連する事例は、次のように定義されている。: 現、もしくは元従業員、契約者、又はビジネス・パートナーが、組織から機密、又は専有情報を窃取し、それをビジネス上の利益のために使用する意図を持って、ネットワーク、システム、又はデータへの許可されたアクセスレベルを意図的に超えた、又はアクセスを悪用した事例。この種類の事例は、最終的目的は、金銭であるという議論が

なされるが、現実はもっと複雑である。これらのインサイダーは、例えば、新しい仕事を得るためにこの情報を使用する、競合ビジネスでの新しい仕事のために使用する、競合ビジネスを開始するために使用するなどより長期間にわたり野心を抱いていた。

CERT の研究者は、1996 年から 2007 年に亘り、米国で発生した２４件の「ビジネス上の利益のための機密又は専有情報の窃盗」事例を分析した。２３件は情報窃盗だけに関連し、１件は IT サボタージュにも関連していた。

誰が、インサイダーであったのか。

分析された全ての事例では、機密、又は専有情報を窃取したインサイダーは、男性で、７１％が技術職、残りの２９％は販売職で、うち２５％は元従業員で、その他の７５％は犯行に及んだ時点で現従業員であった。興味深いことは、インサイダーが犯行に及んだ時点で、既に、約８０％は他の企業からの仕事を引き受けていたか、又は競合会社の設立に取り掛かっていた。

何故、彼らはそれを犯したのか。

定義上、これらのインサイダー全員は、ビジネス上の利益を得るために犯罪に及んだ。一部のインサイダーは、新しい仕事に直ちに役立てるために情報を窃取した。その他のインサイダーは、新しい、競合するビジネスを開始するために情報を使用した。ほとんど全て（９５％）のインサイダーは、犯行（窃盗）の前又は後に退職した。ほとんど（７０％）は退職から３週間以内に犯行に及んだ。

事例の２５％では、インサイダーは情報を外国の企業、又は政府に渡した。非常に大きな経済的影響を及ぼした「ビジネス上の利益のための窃盗」の半数が外国組織に関連があることに注目することは重要なことである。

如何に、彼らは攻撃したのか。

インサイダーの８８％は、犯行に及んだ時点で、情報への許可されたアクセス権を有していた。犯行時点で、窃取した情報への許可されたアクセス権を有していなかったインサイダーだけが元従業員であった。一人の例外を除き、インサイダーは、犯行を可能にするシステム・アドミニストレーター、或いはデータベース・アドミニストレーター（DBA）のような特権的アクセスを有していなかった。一人の元従業員は、付加的仕事をするために特権的アクセスが与えられており、窃盗をはたらくためにそのアクセスを使用した。言い換えれば、システム・アドミニストレーターが情報を窃取するために彼らの優先的アクセスを使用している、という広く知られた懸念は、これらの事例では証明されなかった。

これらの窃盗事例の大部分は、１か月未満の期間に犯行が行われる。これらのインサイダーの３分の１未満は、より長い期間にわたり窃盗を継続し、半数は、サイドビジネスのために、残りの半数は新しい雇用主のために情報を窃取した。これらのインサイダーの３分の１以上は、犠牲となった企業で働いているうちに、新しいビジネスを既に創業したか、又は開始することを計画していた。一部のインサイダーは、退職する時に将来の仕事について嘘をついたり、又は既に他の仕事を引き受けていることを隠したりして、退職後の計画についてごまかしていた。一人のインサイダーは、窃取した情報を外国の国有企業へ移転する媒体としてサイドビジネスを創業した。彼は、企業の基本定款から彼の氏名を除き、そして企業の住所として私書箱を使用することによって、サイドビジネスとの繋がりを隠蔽しようとした。

これら窃盗事例における共謀は、「金銭的利益のための窃盗、又は改ざん」より僅かに少ないが、それでも相当な数である。これらの事例の約半数では、インサイダーは少なくとも一人の他のインサイダーと共謀した。一部の事例では、従業員は、情報を窃取してから退職し、それから追加の情報を窃取するために、元の組織で今もなお働いている従業員を勧誘した。これらの犯罪は通常インサイダー自身のアイディアであった。部外者によって勧誘されたインサイダーは、これらの事例の２５％以下であった。

これらの犯罪の大部分は、勤務時間内に行われたが、少数のインサイダーは勤務時間外に犯行に及んだ。極めて少数（およそ１２％）は、自宅、又は別の組織から組織のネットワークに接続するためにリモート・アクセスを使用した。リモート・アクセスと職場内のアクセスの両方を使用したインサイダーもいれば、通常の勤務時間内と時間外の両方で犯行に及んだインサイダーもいた。

如何に、それらは探知されたのか。

これらのインシデントの多くは、次のような非技術的手段で探知された。

・顧客、又は情報提供者からの通報
・犠牲者の訴えに基づく法執行機関（警察等）の捜査による探知
・同僚からの不審な行動の通報
・突然の新しい競争企業の出現

ある事例では、犠牲となった組織は、展示会での競争企業のブースで、彼らの製品に著しく類似した製品を見て疑いを抱くようになった。もう１つの事例では、インサイダーが、全く同じ製品とサービスを顧客に売却しようとしたので、その顧客は、犠牲となった組織に対して窃盗について警告した。この種類の事例の２５％は、ダウンロードログや電子メールログの監視により、システム・アドミニストレーター、又は IT セキュリ

ティ要員によって探知された。

如何に、インサイダーは特定されたのか。

ほとんどの事例で、ファイルアクセス、データベース、及び電子メールログを含むシステム・ログがインサイダーを特定するために使用された。

どのような影響があったのか。

組織への影響には、経済的損失とその他の損失があった。盗まれた企業秘密がもたらす損失を定量化することは非常に難しい。この種類の事例の３８％では、知的所有権のあるソフトウェア、又はソースコードが窃取された。これと同数の事例では、事業計画、提案、及び他の戦略計画が関係していた。そして、非常に少数の事例では、例えば、製品デザイン、又は製法などの企業秘密に関係していた。

最後に、インサイダー自身が、しばしば、予想しない結果に苦しんだ。一部のインサイダーは、自分の行為が本来犯罪であることに驚いた。何故なら、彼らは、情報はかつて自分が作り、そして、再度作ることができるので、自分が退職する時にそれらを単に入手することは簡単なことであると主張した。一つの事例では、インサイダーは裁判にかけられる前に自殺した。

⑷ 要　　約

本報告のために分析された１７６件の事例の４５％は「ITサボタージュ」に、４４％は「金銭的利益のために情報の窃盗又は改ざん」に、そして、１４％は「ビジネス上の利益のための情報の窃盗又は改ざん」に関係していた[8]。「ITサボタージュ」と「金銭的利益のために情報の窃盗、又は改ざん」が最も一般的な犯罪パターンであるが、これら３つの種類の犯罪の潜在的影響力は、いずれも重大である。従って、組織は、どの犯罪種類が組織にとって、潜在的脅威であるかを考慮すべきである。そして、もし、そうであるならば、これらの犯罪種類に関する本報告の情報を慎重に考慮しなさい。

さらに、本報告の著者は、インサイダーによる「IT サボタージュ」が、組織の規模や複雑さに関係なく、ビジネスを IT インフラストラクチャーに依存しているあらゆる組織にとって脅威であることを強調している。また、多くの組織は、インサイダーによる専有、又は機密情報の窃盗の脅威を無視することはできないであろう。従って、全ての組織が、サボタージュと情報窃盗を防止するために、本報告の後半の部分で詳述される実

[8]幾つかの犯罪が複数の類型に適合したことを思い出しなさい。また、その他の窃盗はこの計算から除外された。

践事例を考慮することを推奨する。

表１は、インサイダー犯罪の３つの種類の概要を提供する。

インサイダー脅威の種類別のハイレベル比較

インサイダーによるサボタージュの潜在的脅威は、否定的な仕事関係の事象の後に、不満を持った技術スタッフによってもたらされる。これらのインサイダーは、単独で行動する傾向がある。否定的な事象の後で、同僚もまた不満を持つかも知れないが、彼らのほとんどは、状況を受け入れ、不満を解消するようになる。実際に犯罪を働くための技術的行為に先行して、観察可能な行動上の前兆が現われた時点で、IT サボタージュの可能性が考慮されなければならない。

「金銭的利益のための情報の窃盗又は改ざん」、及び「ビジネス上の利益のために情報窃盗」に関連するデータは、組織が全ての従業員に対してある程度の注意を働かせる必要があることを示唆している。現従業員は、実際にどんな配置に就いていても、これらのタイプの犯罪をはたらくために合法的なシステムへのアクセス権を使用した。また、「金銭的な利益のための窃盗、又は改ざん」においては、部外者（主として盗んだ情報を市場で売買するか、あるいはその改ざんから利益を得る）、及びインサイダー（主として窃盗又は改ざんを容易にする）両者の高度な共謀があった。「ビジネス上の利益のための窃盗」では、共謀はあまり一般的ではなかったが、それでも相当数あった。「金銭的利益のための犯罪」は、「ビジネス上の犯罪」よりも、部外者によって主導される傾向が強い。

特筆すべきは、ビジネス上の利益のために情報を窃取した従業員の９５％は、窃盗行為の前、又は後で退職しているという事実である。従って、組織がこの種（退職するという）の情報を公式にそれとも噂として知った時は、特別の注意が払われなければならない。信頼と注意のバランスが、組織の方針、行動基準、及び技術的方法の中に考慮されていなければならない。

表１　インサイダー・インシデントの種類別比較の概要

	IT サボタージュ	金銭的利益のための窃盗又は改ざん	ビジネス上の利益のための情報の窃盗
CERT 事例データベースにおける割合（%）	４５％	４４％	１４％
職の種類	技術職（例：システム・アドミニストレーター又はデータベース・アドミニスト	非技術職、機密又はセンシティブ情報へのアクセスができる低レベルの職（例：	技術職(71%)― 科学者、プログラマー、エン

	レーター)	データ入力係、顧客サービス)	ジニアー、営業(29%)
性　　別	男性	半数男性 半数女性	男性
標　　的	ネットワーク、システム、又はデータ	個人情報（PII）又は顧客情報	知的所有権(企業秘密)－71% 顧客情報－33%[9]
使用されたアクセス	無許可のアクセス	許可されたアクセス	許可されたアクセス
何　　時	通常の勤務時間外	通常の勤務時間内	通常の勤務時間内
何　　処	リモート・アクセス	職場	職場
部外者からの勧誘	なし	窃盗事例では半数が勧誘され、改ざん事例では３分の１以下が勧誘された。	4 分の１以下が勧誘された。
共　　謀	なし	改ざん事例ではほぼ半数がもう１人のインサイダーと共謀し、窃盗事例では３分の２が部外者と共謀した。	ほぼ半数が少なくても１人のインサイダーと共謀し、半数は単独であった。

如何に、彼らは止められたのか。

悪意のあるインサイダー行為を実行する方法は、犯罪の種類により様々である。「IT サボタージュ」は、技術的により高度であったが、一方これに比較して「金銭的利益のための情報の窃盗又は改ざん」は技術的に高度ではなかった。

組織が、脅威をもたらすいかなる悪意のある行為からも組織を保護したいならば、この報告の後半の部分で概説されている実践事例を実行することを慎重に考慮することが重要である。犯罪をおこなうための技術的予備行動を防止・探知するために、一定レベルの積極的な技術的対策を実施･維持することが必要である。潜在的なインサイダー脅威の徴候が現れた時に適切に認識・対応するためには、良好な管理基準が実施・維持されていることが必須である。CERT によって調査された事例の法律上、及び契約上の意味合いは、従業員、契約者、及びビジネス・パートナーに理解され、かつ説明されていることが重要である。

組織が、時間とともに従業員の実践の質を低下させることは良くあることである。何故ならば、悪意のあるインサイダー行為が探知できなければ、実践は、競合する優先事項より重要でないと見なされるからである。インサイダーに対する脆弱性の一つは、まさに防御の質に関する従業員の理解である。: 組織の防御力の質が重要である。

[9] 一部のインサイダーは、一つ以上の種類の情報を窃取した。

インサイダー攻撃があった後に何をすべきか。

全ての事例に共通する１つのパターンは、インサイダーを特定するためのシステム・ログの重要性である。システム・ログは、犯罪の種類に係わらず、適切な処置を講ずるために必要な証拠を提供する。多くの技術的能力を有するインサイダーは、システム・ログを改ざんすることにより、しばしば、彼らの行為を隠蔽することを企てるので、組織は、ログの完全性の確保を目的にシステムを設計することが重要である。

インサイダー脅威から組織を保護・防護することに加えて、組織に起こるかもしれないインサイダー・インシデントに対応できる準備ができていることが重要なことである。組織は、インシデント対応計画を準備する際に、しばしば、インサイダー脅威を見落とす傾向がある。インサイダー・インシデントは、注意深く調査（捜査）される必要がある。何故ならば、誰が信用でき、誰ができないかが、必ずしも明らかでないからである。さらに、組織は、フォレンジック（電子捜査）に関する先行的な意思決定をしておくべきである。: 内部的に行うのか、又は外部のフォレンジックの専門家を雇うのか。

本報告の後半の部分は、インサイダー・インシデントを防止するのに効果的があるであろう、又は、少なくても悪意のある行為の早期探知を可能にするであろう１６件の実践事例で構成されている。

4. インサイダー脅威を防止･探知するための最善の実践事例の要約

後述する１６件の実践事例は、CERT が調査し、組織が経験した多くのインサイダー・インシデントの防止と、早期探知が容易にできるだろう防御策を提供している。16 件の中には、第２版の出版以降に収集･分析された約１００件の最近の事例に基づき更新された実践事例もあれば、本版に新たに追加された実践事例もある。各実践事例には更新、又は新規の表示がなされている。

実践事例１：企業レベルのリスクアセスメントにおいて、インサイダー、及びビジネス・パートナーからの脅威を考慮しなさい。（更新）

組織にとって、従業員を信用すること、組織の使命を達成するために従業員にアクセス権を付与すること、及び従業員がもたらす潜在的セキュリティ侵害から資産を保護することなどを均衡させることは困難なことである。組織の技術的脆弱性、及び業務プロセスの欠陥からもたらされる脆弱性を知っているインサイダーのアクセスは、彼らがその気になれば雇用主に対して悪意のある行為を実行する能力と機会を与えている。組織は、契約に基づき共同して働くビジネス・パートナーへの依存を大きくしているので、インサイダー脅威の範囲は拡大し、問題はさらに難しくなっている。組織は、まず、最重要な資産を決定し、インサイダー及び部外者の両者から資産を保護するためのリスクマネージメント戦略を策定するなど、企業レベルの情報セキュリティについての展望を持つことが重要である。

実践事例２：方針と規制を明確に文書化するとともに一貫して実行しなさい。（新規）

CERT 事例資料によると、技術的及び組織的な方針及び規制の明確な文書化によって、一部のインサイダー・インシデント、窃盗、改ざん、及び IT サボタージュを減少させることができた。本セクションでは具体的な方針が論じているが、この方針を一貫して実行することが重要である。CERT が調査した事例では、一部の従業員が他の従業員と違って処遇されていると感じた時に、この不公平感に対する報復として雇用主の IT システムを攻撃した。他のインサイダーは、方針が矛盾しているか、あるいは強制されていなかったために、情報を窃取、又は改ざんすることができた。

実践事例３：全ての従業員に対する定期的なセキュリティ認識訓練を実施しなさい（更新）

セキュリティ認識の文化が組織に植え付けられていなければならない。そうすれば、全ての従業員が方針、手順、及び技術的規制の必要性を理解するであろう。組織の全ての従業員は、セキュリティ方針と手順が存在すること、それらが存在する正当な理由があること、それらが実行されなければならないこと、そして、違反は深刻な結果になる

ことを知らなければならない。従業員は、組織の内部者、又は外部者である個人が、組織の使命に反する行動に引き入れようとするかもしれないことを知っている必要がある。従業員たちは、組織のセキュリティ方針と、その方針の違反を報告するプロセスを理解する必要がある。本セクションは、部外者によるインサイダーの勧誘に関連する重要な新しい調査結果に基づき更新がされている。

実践事例４：採用プロセスから、従業員の不審な行動、又は秩序を乱す行動を監視・対応しなさい。（更新）

組織は、従業員を雇用する前に、重大な犯罪行為に拡大する徴候である度重なる方針違反、不審な行動、又は秩序を乱す行動などを厳密に監視しなければならない。また、個人的ストレス､及び職業上のストレスも考慮されなければならない｡本セクションは、１００件の最近の事例の調査結果に基づいて更新された。特に、共謀率と再犯率の高い事例を取り上げている。

実践事例５：否定的な職場問題を予期し、上手く対処しなさい。（新規）

本セクションは、雇用前の問題から始めて、雇用中の問題、そして、退職問題までを通しての組織への提案を記載している。例えば、雇用主は、雇用契約と労働条件をはっきりと公式化する必要がある。従業員の責任及び制約、並びにそれらの違反の結果は、明確に伝えられ、一貫して実施される必要がある。さらに、職場での口論、又は同僚同士の不適切な関係は、健康かつ生産性の高い職場環境を徐々にむしばむであろう。従業員が、報復、又は否定的な結果を心配せずに、仕事関連の問題について管理者、又は人事担当者と話し合うことが奨励されていると感じなければならない。管理者は、問題が制御できないほどに拡大する前に、問題が発見されたか、あるいは報告されたときに直ちにこれらの問題に取り組む必要がある。最後に、大部分のインサイダーの IT サボタージュ攻撃は、退職の直後に発生しているので、敵対的な従業員の退職は、最大限の注意を払って取り扱われなければならない。

実践事例６：物理的環境を追跡し、安全を確保しなさい。（新規）

従業員、及び契約者は、組織の施設と機器へのアクセスができなければならないが、全員が職場の全ての区域へのアクセスが必要というわけではない。各従業員の物理的アクセスを管理することは、インサイダー・リスクマネージメントの基本である。アクセス未遂は、物理的空間、及び機器へのアクセス方針の違反、又は違反未遂を特定するために、ログされ、かつ定期的に監査されなければならない。退職した従業員、契約者、及び信用されたビジネス・パートナーが、組織の非公開区域への物理的アクセスができないことはいうまでもない。本セクションは、物理的アクセスの脆弱性がインサイダー攻撃を許した事例から得た教訓を詳述している。

リモート・アクセスの方針と手順は、慎重に設計され、かつ実装されなければならな

い。最重要なシステムへのリモート・アクセスが必要であるならば、組織は、管理する機器を通してだけの接続、厳密なログ、及び頻繁な監査によって、増加するリスクを相殺することを考慮しなければならない。退職した従業員のリモート・アクセスの無効化と、組織が支給した機器の回収が特に重要である。本セクションは、最近の事例でインサイダーが使用した新しいリモート攻撃方法を盛り込むために更新された。

実践事例 14：退職後に、コンピュータアクセスを無効化しなさい。（更新）

従業員が退職する時に、円満退職であったか否かに関係なく、従業員が許可されていた組織の施設、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ポイントを全て無効化するという厳格な退職手順が実行されていることが重要である。退職した従業員が利用できる全てのアクセスポイントを無効化する素早い行動を行うためには、コンピュータ・システム・アカウント、共有パスワード、及びカード・コントロールシステムを含む、全てのアクセスを継続的かつ厳格に追跡・管理する慣行が必要である。

実践事例 15：安全なバックアップと回復プロセスを履行しなさい。（更新）

組織は、インサイダー攻撃のリスクを完全に排除することができない。リスクは、どんな企業活動にも固有のものである。しかし、組織的弾力性の確保から、リスクは、株主を含む組織関係者にとって容認できるものでなければならない。そして、潜在的インサイダー攻撃の影響を最小限に抑えられなければならない。従って、組織が、インサイダー攻撃の可能性に備えて、単一障害点（致命的欠点）を回避するバックアップと、回復プロセスを履行し、かつ定期的にテストすることにより対応時間を最小限にすることは重要である。本セクションには、組織のインシデント・レスポンスに対する注意不足、及び組織的弾力性の不足が、顧客サービスの深刻な混乱に結びついた最近のインサイダー事例の説明がされている。

実践事例 16：インサイダー・インシデント対応計画を策定しなさい。（新規）

組織は、悪意のあるインサイダーによってもたらされた損害を制御するインサイダー・インシデント対応計画を策定する必要がある。これは、挑戦的なことである。何故ならば、対応チームに割り当てられた人々自身が、組織に対して彼らの技術力を悪用する人々であるかもしれないからである。計画を実行する責任を有する者だけが、計画を理解し、訓練される必要がある。インサイダー攻撃を受けた際に、インサイダーを特定して、後の訴追等に必要な証拠を組織が手元に持つことが重要である。教訓により計画は継続的に改善されなければならない。

５　実践事例

⑴　実践事例１：企業レベルのリスクアセスメントにおいて、インサイダー及びビジネス・パートナーからの脅威を考慮しなさい。（更新）

組織は、許可されたインサイダー・アクセスを有する信頼できるビジネス・パートナーのみならず、内外の脅威から、最重要な資産を保護するために、リスク基盤の包括的なセキュリティ戦略を策定する必要がある。

何をなすべきか。

全ての組織の資源を、全ての脅威から 100%保護するための対策を実施することは、ほとんどの組織にとって現実的ではないであろう。従って、最重要な情報、及びその他の資源を適切に保護し、そして比較的重要でないデータや資源の保護には多くの努力を指向しないことが重要である。組織の使命にとって最重要であると考えられる資産を、内外双方の脅威から保護することが現実的かつ達成可能なセキュリティ目標である。残念なことに、組織は、しばしば、自己組織以外の組織や個人に対して自己組織のネットワーク、システム、又は情報へのアクセスを提供することによってもたらされる脅威の増大を認識することが出来ない。組織の企業レベルの境界線は、組織、情報、及び情報システムに関する特権的な知識やアクセスを有する全ての人々をインサイダーとして包含するよう十分に広範に引かれなければならない。

リスクは脅威、脆弱性、及び使命への影響の組合せである。企業レベルの広範なリスクアセスメントは、最重要な資産とこれらの資産が危険に晒された時の事業への影響を特定するのに有用である。組織は、脅威への対応と組織の事業達成との適切な均衡を維持しながら、組織のネットワークシステムを保護する全体戦略を策定、又は改善するためにアセスメントの結果を活用すべきである[10]。

脅威を正確に評価するためには、システム運用時の脅威環境の理解が必要である。脅威環境の特性化は、脆弱性と影響の評価と同時に進めることが出来る。しかし、脅威環境の特性化は早ければ早いほどよい。本ガイドの目的は、インサイダーの脅威環境、脅威に対する組織的脆弱性、並びにインサイダー・インシデントがもたらす経済面、運用面、及び社会的信用面への影響を含む潜在的な影響を正確に評価することを支援することである。

---

[10] CERTが研究した「企業のセキュリティ管理」は次のURLを参照されたい。
http://www.cert.org/nav/index_green.

残念ながら、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、インサイダーを見落としている。さらに、潜在的インサイダーの脅威を意識せず、かつ脅威を説明せずに設計された情報技術やセキュリティソリューションは、資産保護の役割を潜在的脅威であるインサイダー自身の手に握られる。組織の従業員、契約者、及びビジネス・パートナーの知識やアクセスがもたらす潜在的危機を認識し、その脅威を企業のリスクアセスメントの一部として取り扱うことは組織にとって必須のことである。

また、脅威に対する組織の脆弱性を理解することも重要である。しかし、組織は、しばしば、低レベルの技術的脆弱性に対して余りにも多くの注意を集中しすぎる。例えば、コンピュータ・ネットワーク脆弱性スキャナ（ネットワークを通じてシステムの脆弱性や設定ミスを自動的に検出するツール）への依存など。そのような技術も重要であるが、我々のインサイダー脅威の研究では、組織の業務プロセスが、少なくても技術的脆弱性と同様に重要であることを指摘している。組織は、個別の技術的脆弱性より、むしろ脅威のもたらす影響に取り組む必要がある。さらに、下記の“最近の調査結果”セッションで詳述するように、最近の事例から新しい懸念分野が明らかになってきた。

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、又は機密性に影響を及ぼす。インサイダーは、例えば、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した。また、彼らは、企業秘密又は顧客情報を盗み取ることにより情報の機密性を侵害した。さらに、別のインサイダーは、組織経営者間の電子メールのみならず、顧客の個人情報（PII）を含む機密情報を不適切に流出させた。最後に、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、さらにサービス拒否攻撃（DoS）を行うなど組織の情報の可用性を侵害した。

上述したインサイダー・インシデントでは、現、もしくは元従業員、契約者、又はビジネス・パートナーが、組織の最重要な資産に侵害を与えた。従って、保護対策では、これらの資産（財務データ、機密情報、専有情報、並びにその他事業継続にとって最重要なシステム及びデータ）を保護対象として策定することが重要である。

事例研究：これらが行われなかった場合、何がおこるであろうか。

ある組織は、最重要なシステムとデータを内部の従業員から保護することができなかった。そのシステムは、救急隊（911）へ通報された電話番号から住所を検索するものであった。インサイダーは、契約社員の ID カードを使用して、物理的アクセスを得ることにより、組織のネットワーク運用センター（network operations center：以下、NOC）の 3

つのサーバーから全てのデータベースとソフトウェアを削除した。この無人の NOC は、単に物理的セキュリティにより保護されており、室内の全ての機械は、システム・アドミニストレーターのアクセスでログインされるようになっていた。

NOC のシステム・アドミニストレーターは、自動呼び出し装置により直ちにシステム故障が知らされたが、そこには自動フェイルオーバー（障害迂回）機能がなかった。組織の復旧計画は、単にバックアップ・テープに依存しており、そのバックアップ・テープは、NOC の中に保管されていた。不幸なことに、インサーダーは、システムが容易に復旧されることに気がつき、施設を離れるときに、全てのバックアップ・テープを持ち去った。さらに、その契約者の ID カードは、遠隔地保管施設へのアクセスが許可されていたので、彼は、続いて、５０本以上のバックアップ・テープを盗み出した。

インシデントの前に、このシステムに関して企業レベルのリスクアセスメントが実施されていたならば、組織はこのシステムの致命度を認識し、脅威と脆弱性を評価し、それに応じたリスク軽減戦略を策定していたであろう。

もう１人のインサイダーは、組織のたった１人のシステム・アドミニストレーターであった。ある日、彼は予告無しに退職した。組織が最後の２日間の給与支払いを拒否したので、彼は、そのシステムのアドミストレータ・アカウントのパスワードの返却を拒否した。３日間に亘って、インサイダーは、従業員がアクセスできないようにシステムを変更し、会社のウェブサイトを書き換え、そして、ファイルを削除した。全てのシステムの管理権限を独りの従業員の手に委ねた場合に、組織が被ると思われるリスクを考慮することは極めて重要である。

最近の調査結果

組織は、ますます重要な業務を外注するようになっている。その結果、組織外の人間が、しばしば、組織の方針、プロセス、情報、並びに以前は従業員にのみ提供されたシステム及び情報などへの完全なアクセスを有するようになっている。CERT のインサーダーの定義は、元来、現もしくは元従業員並びに契約者を包含するものであったが、現在は、パートナー、協力者（collaborator）、及び組織と連携する学生をも包含するまでに拡大された。

最近の一つの事例では、大手メーカーの新しい無線ネットワークを設置する契約を結んだ会社の従業員が関係していた。インサイダーは、据え付けチームに属していたので、メーカーのシステムに関して詳細な知識を有していた。彼は、明らかに、**不満を抱いたままで**雇用主によってチームから外された。しかし、彼は製造工場に入り、訪問者ロビーでコンピュータ・キオスクにアクセスすることができた。メーカーのコンピュータ・

システムとセキュリティに精通していることから、キオスクを使って、国内の至る所でメーカーが使用する無線装置のファイルとパスワードを削除した。復旧には、装置を取り外し修理しなければならないため、各施設で広範な操業停止と業務処理上の混乱を引き起こした。

この事例は、いくつかの新しいインサーダー脅威を浮き彫りにしている。まず第１に、企業レベルのリスクアセスメントにおいて、セキュリティを破って、誰にでも利用できるキオスク端末から、セキュリティを破ってメーカーのネットワークへの特権的アクセスを取得するための能力を特定すべきであった。第２に、このインサイダーの所属する会社と大手メーカーとの契約には、プロジェクトに関連する従業員を追加、または排除する場合の厳しい規制を設けるべきであった。具体的には、組織は、契約書に、組織のシステムへの物理的、電子的アクセス権を有するいかなる従業員に対しても、計画された良くない雇用上の活動は、事前通知を必要とするという条項を考慮しなければならない。組織は、自己のネットワーク、システム、又は情報にもたらされる潜在的脅威に対するリスクアセスメントを行うために、雇用処置が行われる前に一定の時間が必要となるであろう。

もう１つの最近のインシデントは、供給協定（supplier agreements）に取引認証、処理確認・処理証明（transaction verification）を組み入れる必要を示している。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軍用電子メールアドレスを作成した。それから、主要な納入業者によっ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、決して現物のリコール部品を返すつもりはなかった。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 回の発送品を受け取った。彼は、この部品をインターネットの eBay（オークションサイト）で売りさばいた。

もう１つの事例は、組織の範囲とインサイダー脅威の範囲を定義することの難しさを示している。ハイテク企業の部外法律顧問は、民事訴訟において企業側代理人となる準備をしていた。その法律顧問は、訴訟事件を準備するために企業秘密を含んだ必要な書類の提供を受けた。その法律事務所は、その訴訟事件の書類をコピーするために、ある製本会社（ドキュメント イメージング会社）と契約した。その製本会社の従業員は、仕事量が多いために、企業秘密文書のコピーを彼の甥に手伝わせた。大学生で従業員でないその甥は、機密文書を叔父の仕事用コンピュータを使って読み取り、そして、それらをハッカーウェブサイトへ送信した。彼の目的は、ハッカーコミュニティがハイテク会社の主要製品をクラックする（セキュリティを侵害する）ことを手助けすることであっ

た。組織は、インサイダーに侵害されるリスクを評価する際に、企業レベルの情報境界線（パートナーや協力者を含めるのか否か）と自己の管理を離れた情報を保護するための法的手段の行使を慎重に検討する必要がある。

⑵　実践事例２:方針と規制を明確に文書化するとともに一貫して実行しなさい。（新規）

組織の方針と規制に関する首尾一貫した明確なメッセージは、従業員が軽率に犯罪を働く可能性、又は不当行為があったとしても組織を激しく非難する可能性を低くするであろう。

何をなすべきか。

誤解されている、周知されていない、又は一貫していない方針、あるいは規制は、従業員の間に不満を醸成し、その結果有害なインサイダー行為を引き起こす可能性がある。例えば、CERT データベースに保存されている事例の複数のインサイダーは、仕事で作り出した知的財産を横領したが、それが彼らの所有物でないことを理解していなかった。彼らは、犯罪を働いたとは思っていなかったので、逮捕された時に非常に驚いた。

組織は、方針と規制に関して、次のことを確実に処置しなければならない。

- 必要ならば、方針の背景にある理由を含む簡潔で首尾一貫した文書化
- 全ての従業員に対して公平
- 一貫した励行
- 方針、必要理由、実施、及び励行に関する定期的な従業員教育

組織は、特に、次に関する方針を明確にしなければならない。

- 使用が許される組織のシステム、情報、及び資源
- 有給の従業員、又は契約者が創造した情報の所有権
- 昇進とボーナス（特別手当）の必要条件を含む従業員の勤務評価
- 従業員の苦情申立ての方法とその処理手順

個人が雇用された場合、違反行為の結果と、期待されているものが何かを説明した組織の方針のコピーを受け取るべきである。さらに、各個人が、組織の方針を読み、かつ合意したという証拠が保存されなければならない。

従業員の不満は、インサイダーによる侵害、特に IT サボタージュ事件で繰り返される要因である。不満は、インサイダーが期待はずれであると感じたときに生じた。インサイダーが感じる期待はずれには次のものがある。

- 不十分な昇給、又はボーナス

・会社資源の使用に関する制限
・縮小された権限と責任
・不公平な仕事条件
・貧弱な同僚関係

方針と規制の明確な文書化は、従業員が期待はずれであると誤解するのを防止することができる。首尾一貫した履行は、従業員が他の従業員とは違う又は悪い処遇を受けていると感じさせない。ある事例では、従業員は長い期間に亘ってずさんな方針の実行に慣れていた。新しい管理者は、即時に厳格な方針の励行を命じた。それは、１人の従業員に敵意を持たせ、組織を攻撃させる原因となった。言い換えると、方針は、長い期間一貫して堅持され、かつ、全従業員によって一貫して履行されなければならない。

もちろん、組織は静的な存在でない：組織の方針と規制の変更は不可避である。従業員の制約、特権、及び責任も同様である。組織は、変化の時機、特に従業員のストレスの大きい時期を認識する必要がある。そして、ストレスポイントとともにやってくるリスクの増大を認識し、従業員との意思疎通をよくしリスクを軽減する必要がある。

事例研究：これらが行われなかった場合、何がおこるであろうか。

昇任したインサイダーは、ある部門のシステム・アドミニストレーターから同じ組織内の他の部門のシステムアナリストへ異動した。新しい配置で、彼は、元の部門と現部門の間の情報共有と協力に関する責任者であった。そして、次の事象が起こった。

・元の部門は彼のシステム・アドミニストレーター・アカウントを停止し、彼に新しい配置に必要なアクセスを与えるために普通のユーザー・アカウントを発行した。
・その後まもなくして、元の部門のシステムセキュリティ管理者は、元従業員の新しいアカウントには無許可のシステム・アドミニストレーターの権限が与えられていることに気が付いた。
・セキュリティ管理者は、そのアカウントを普通のアクセス権に再設定した。しかし、後になって再び、そのアカウントにシステム・アドミニストレーターの権限が与えられていることを発見した。
・セキュリティ管理者はそのアカウントを閉鎖した。しかし、数週間にわたり、他のアカウントが無許可のアクセス、及び使用パターンを示した。

これらの事象を調査した結果、コンピュータ・システムの不正使用の罪でそのアナリストは告訴された。しかし、結局、告訴は取り下げられた。その理由の１つは、アカウントの共有、又はアカウント特権を高めるために脆弱性を悪用することに関する明確な方針がなかったからである。この事例は、組織の部門、グループ、及び子会社全体に首

尾一貫した方針が明確に確立していることの重要性を例証している

従業員が不公平に処遇されていると感じたために、組織の情報又はシステムを侵害した事例が CERT 資料には多数ある。

- インサイダーが組織のシステムにロジボムを仕掛けた。何故ならば、同僚より厳しい労働基準を要求されていると感じたからである。
- ボーナスが期待していたより少なかったため、インサイダーはロジボムを仕掛けた。何故なら、ロジボムによる破壊活動により自社の株価が低下し、そして自分のストックオプションの価値が上昇するであろうと期待したからである。
- 組織の製造サポートシステムを設計し、管理していたネットワーク・アドミニストレーターは、自分が作ったものを破壊するためにロジボムを作動させた。何故ならば、彼は地位と支配権を失ったと感じたからである。
- 雇用主が製品の品質要求基準に十分に取り組んでいないと思った品質管理検査員は、会社にこの問題に対処させようとして、メディアに機密情報を提供した。
- 支払いの遅れた契約者の保険証券をキャンセルするという会社のやり方に憤ったインサイダーは、会社のセンシティブな情報を会社の訴訟に携わっている対立する弁護士に提供した。

これらのインサイダーのしたことは、悪いことであり、違法なことである。そうはいうものの、より明確な方針と苦情手続きが確立していれば、これらの組織が経験した重大なインサイダー攻撃は回避できたかもしれない。

⑶ 実践事例３:全ての従業員に対する定期的なセキュリティ認識訓練を実施しなさい。（更新）

組織の広範な理解と積極的な取り組みがなければ、技術的、又は管理的規制は長続きしないであろう。

何をなすべきか。

全ての従業員は、インサイダー犯罪は必ず起こるものであること、そして重大な結果を引き起こすことを理解する必要がある。さらに、非常に技術的に優れた人物であろうと、わずかな技術的能力を持った人物であろうとも、悪意のあるインサイダーになることを理解することが重要である。犯人の年齢は、10 代後半から定年者まで幅広い。悪意のあるインサイダーには、内気な“一匹狼”、積極的な“俺に任せろ”型の人物、及び外交的な“目立ちたがりや”などの男女が含まれる。職業は、低賃金のデータ入力係、レジ係、プログラマー、芸術家、システム及びネットワーク・アドミニストレーター、販売員、管理者、並びに経営者など広範であった。また、彼らは、新入社員、長期勤続の従業員、最近採用された従業員、最近退職した従業員、契約社員、派遣社員、及び信

頼できるビジネス・パートナーの従業員であった。

セキュリティ認識訓練は、悪意のあるインサイダーを型どおりでなく行動によって特定するよう奨励されなければならない。懸念される行動には次が含まれる。

・組織に対する脅迫、又は組織に損害を与えられることを誇示すること。
・職場外の犯罪者として知られている者、又は不審な人物との交際。
・退職間近の大量のダウンロード。
・副業への組織の資源の使用、又は競合するビジネスを開始することに関する同僚と議論。
・策略を用い、又は信頼関係を悪用して（ソーシャルエンジニアリングと呼ばれる）、従業員のパスワード又はアクセスを得ようとする試み。

インサイダーが、特に、金銭的な利益目的で情報を窃取、又は改ざんを目的に、他の従業員を取り込もうとするソーシャルネットワーキング（インターネットを利用して、友人・知人の輪を広げていくこと）に対する認識を深めるために、管理者と従業員を訓練する必要がある。これらの可能性と結果について、従業員に対して注意喚起することによって、従業員は、これらの働きかけに対して警戒するとともに、それを管理部門に通報するであろう。

ソーシャルエンジニアリングは、しばしば、物理的アクセスを得ようとするか、あるいはアカウントとパスワードを通して電子的アクセスを得ようとするかのどちらかに関連している。１つの最近の事例では、不満を抱いた従業員が、会社の機密情報を入手するためにハードウェア・キーロガー（keystroke logger）を職場のコンピュータに設置した。突然解雇された後、この元従業員は、この装置を回収するために、会社に勤務している非技術系の女性従業員を取り込もうとした。その従業員は、その装置がキーロガーであるとは知らなかったが、彼に手渡すことの危険を察知し、管理部門に通報した。フォレンジック（電子捜査）により、彼は解雇前に少なくても一度は、その装置を取り外し、キーストローク・ファイルを彼のコンピュータに転送していたことが明らかになった。

訓練プログラムにより、組織のセキュリティ文化を創造しなければならない。また、訓練プログラムは、全ての従業員を対象としなければならない。効果的でありかつ永続的であるためには、インサイダー脅威から組織を守る対策が、企業レベルのリスクアセスメントにより決定された組織の使命、価値、及び最重要な資産と結びついていなければならない。例えば、組織が顧客サービスの質に高い価値を置くならば、組織は、顧客情報を最重要な資産とみなし、そのデータの保護対策に最大限の努力をしなければならない。組織は、次に示す多くの幾つかの主要な問題に焦点を当て、悪意のある従業員の

行動に対して、絶えず警戒するよう従業員を訓練しなければならない。

・従業員の秩序を乱す行為の探知と通報（事例４を参照）
・組織の方針と規制の順守の監視（事例２と１１を参照）
・組織システムの変更の監視と管理（例、悪意のあるコードのインストールの防止）（事例９と１１を参照）
・カスタマー・アカウントを修正する従業員と、支払金を修正又は支給する従業員との任務の分離（事例８参照）
・組織の施設、及び物理的資産に対するセキュリティ違反の探知・通報（事例６参照）
・潜在的インシデントに対応するための先行的な計画（事例１６参照）

顧客サービスプロセスに対するリスクを軽減する訓練は、次のことに焦点を合わせなければならない。

・プロセスで使用されるコンピュータ・アカウントの保護（事例７参照）
・顧客記録へのアクセスの監査（事例 12 参照）
・規定された方針と規制の一貫した履行（事例２参照）
・最重要なサーバーへの適切なシステム管理ツールの実装（事例 10、11、12、及び 13 参照）
・顧客サービスデータの有用性を確保するための安全なバックアップ、及び復旧方法の使用（事例１５参照）

訓練内容は、セキュリティ問題を通報するための秘匿された方法を含む、文書化された方針に基づかなければならない。秘匿された通報により、従業員は、影響を心配せず不審な事象を報告することができる。これにより内部告発の文化の壁を克服することができる。従業員は、組織が方針と手順を履行しており、かつ管理者が公平かつ迅速にセキュリティ問題に対処することを理解する必要がある。

システム活動、特にシステム管理と特権的活動が監視されていることが、従業員に知らされていなければならない。全ての従業員は、彼らが自身のパスワードや仕事上の成果物の保護などについて彼らが個人的責任を持つよう訓練されていなければならない。最後に、訓練は、IT 利用規定（acceptable use policy：AUP）と整合されていなければならない。

事例研究：これらが行われなかった場合、何がおこるであろうか。

最重要な製造アプリケーションを主導する開発者は、アプリケーション・ソースコードに対する広範な支配力を有していた。ソースコードの唯一のコピーは、会社から支給された彼のノート型パソコンに保存されていた。しかし、バックアップはなく、管理者

が繰り返し要求しても、ごく僅かな説明書さえも作成しなかった。インサイダーは、ソースコードをいかなる文書にもする気がないと同僚に語った。さらに、作成した文書は分かりにくく、管理者が彼にソースコードのバックアップコピーを作成するよう命じなかったことから、管理者を軽んじていたと語った。

まもなく左遷されることを知ってから１ヵ月後、彼は、彼のノート型パソコンのハードドライブを消去することにより、組織が保有する唯一のソースコードを消し去った。そして、彼は仕事をやめた。法執行機関が、インサイダーの自宅から暗号化された形式のソースコードを発見するのに 2 か月以上を要した。そして、インサーダーが、ソースコードを解読するためのパスワードを提供するまでにさらに 4 ヶ月を要した。この期間、組織は、いかなる修正もできない実行可能なバージョンのアプリケーションに頼らなければならなかった。インサイダーの属していたチームの各メンバーに対して、システムのセキュリティと生存性が彼らの責任であることを周知していたならば、管理者にインサイダーの言動を通報したかもしれない。そうすれば、攻撃を防止できたかもしれない。

もう１つのインサイダー事例は、技術的にはあまり高度ではない攻撃であったが、もし方針と訓練が適切であったならば、回避できるか又はうまく起訴できたかもしれない。４人の役員が競争会社を設立するために会社を辞めた。会社を辞める数日前、そのうちの１人は、データをバックアップしている外部の会社が管理している顧客情報、及びその他のセンシテティブな情報を内蔵した彼の仕事用コンピュータのハードドライブのバックアップコピーを命じた。また、会社は、コンサルトサービス合意文書と価格リストが、インサイダーの仕事用のコンピュータから、彼の名前で登録された外部の電子メール・アカウントへ送信されていると主張した。インサイダーのうちの２人は、元雇用主との間で機密保持契約に署名しているが、彼らが取得した情報は既に公表されているので、それは専有情報に該当しないと主張した。専有情報に関する定義と使用規則に関する明確な方針があれば、攻撃を防止できたか、あるいは起訴のための明白な手段を提供することができたであろう。

最近の調査結果

最近の事例について特筆すべき発見は、金銭的利益のための窃盗３１件の３分の２以上は、インサイダーが組織外の人物によって勧誘されていることである。これらの事例の多くで、インサイダーは、比較的少ない金銭的報酬を受け取る一方で、多くのリスクを背負っている。アウトサイダーは、しばしば、親戚であったり、あるいはインサイダーが有するアクセスを悪用することの価値を認めた知人であったりする。病院の請求書記録部門の女性マネージャーは、患者のクレジットカード情報を兄弟へ提供した。その兄弟は、それを使いオンラインで買い物をして商品を自宅へ発送させた。別の政府機関の人事部門に勤務するインサイダーは、従業員の個人情報（PII）を彼女の彼氏に提供し

た。その彼氏はそれを使用し、不正なクレジットカード・アカウントを開設し、買い物をした。また、CERT の以前の研究によると、アウトサイダー(例えば、自動者のセールスマン)が、ローンを求める個人の信用履歴を更新するようインサイダーを説得し続けたなどがある。組織は、彼らに任された情報を保護する責任と、不心得者がその情報へ彼らのアクセス権を利用しようとする可能性について従業員を教育すべきである。そのような不心得者は、個人のインサイダーかアウトサイダー、また組織かも知れない。インサイダーは、金銭的利益のための情報改ざん事例のほとんど半数で、職務の制限の仕切り越すため、又は同僚に不審な行動を通報されないようにするために、複数の従業員を勧誘した。ある最近の事例では、銀行に勤める数人の用務員が仕事中に顧客情報を盗み、オンラインで顧客住所を変更し、彼らの名前でクレジットカードを作り、カードを使って高価な品物を購入し、顧客の預金口座を使い果たした。従業員は、不審な同僚の行動を匿名で通報する会社の手順、あるいは組織の部内外の個人からの勧誘について、定期的に注意喚起されなければならない。

従業員は、企業情報の機密性と完全性に関することと、それらの侵害は、厳しく処罰されることを教育されなければならない。インサイダーは、しばしば、これを理解しておらず、情報を企業のものより、むしろ彼ら自身の資産であると見なしている。例えば、顧客情報は販売人のもの、ソフトウェアはプログラマーのものと思っている。

また、最近の事例では、賃金に不満をもった技術系従業員が組織の知的財産権を売却した、又は組織の業務に不満の抱いた従業員が情報をレポーターや弁護士に提供したものがある。このような不満の兆候は、しばしば、実際の侵害の前によく現れる。管理者や同僚が、潜在的な攻撃の前兆を認識したら直に通報することを教育されていたならば、このような攻撃は防止できたであろう。

⑷ 実践事例４:採用プロセスから、従業員の不審な行動又は秩序を乱す行動を監視し、対応しなさい。（更新）

悪意のあるインサイダー脅威を減らす１つの方法は、積極的に不審な従業員、又は秩序を乱す従業員に対処することである。

何をなすべきか。

インサイダー脅威を減らすための組織の取り組みは、身元調査の実施や受け取った情報に基づく個人の評価などについて、採用プロセスから開始することである。身元調査は、信用調査を含む刑事上の有罪判決を調査するとともに、各種証明書や過去の仕事を確認しなければならない。さらに、身元調査には、個人の能力や職場問題に取り組む姿勢について、以前の雇用主との話し合いも含まれる。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。内訳は、暴行罪(１８％)、アルコール、又は薬物関連

の罪(１１％)、及び金銭・詐欺に関連しない窃盗罪(１１％)である[11]。この様な比較的高い犯罪率は、身元調査の必要性を裏付けている。これらの積極的方策は、本来、懲罰的であってはならない。むしろ、個人は、適切な指導により、組織人として教化されなければならない。さらに、この(身元調査の)情報は、新しい従業員に対して最重要な機密、もしくは専有情報、又はシステムへのアクセスを付与することが適切かどうかを決定するリスク基盤の意思決定プロセスの一部に使用されるべきである。

身元調査は、契約者と下請者を含む全ての潜在的従業員に要求されなければならない。最近の１つの事例では、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。

組織は、従業員の不適切、又は懸念される行動を発見・対処することができるように管理者を訓練するための時間と資源を投資すべきである。あまり重大でない不適切な行動が、職場では認識されていたが、方針違反のレベルに至らなかったという理由で組織としては対処されなかったという一部の事例がある。しかしながら、幾つかの事例では、セキュリティ方針の定義、又は履行の怠慢が、従業員を大胆にさせ、徐々に重大な違反行為を繰り返させ、その結果、組織に対して重大な危害を及ぼすリスクを増大させた。組織が、一貫して従業員の犯した規則違反に厳しく対処することは重要である。

多くのインサイダーの主たる動機が、金銭的利益のための情報の窃盗、又は改ざんであることを考え合わせると、組織は、従業員の潜在的な金銭的問題、又は説明のできない金銭的利益に関する兆候を監視すべきである。負債の増大、又は高価な買い物を含む従業員の金銭的状況の急激な変化は、潜在的なインサイダー脅威の指標である。従業員が同僚の懸念される、又は秩序を乱す行動を通報するための方針と手順が存在しなければならない。不真面目な通報は選別されなければならないが、全ての通報は調査されるべきである。従業員が不審な行動を示したならば、組織は、しかるべき注意を払って対応しなければならない。秩序を乱す従業員の企業内での配置異動は許されるべきでない。悪意のある行為、又は能力を自慢するなどの脅威(“あなた方は私が如何に容易くこのネットを消去したか信じられないであろう”)や、その他の否定的な感情は、懸念ある行動

11 インサイダー脅威スタディー：『最重要インフラ分野におけるコンピュータ・システム・サボタージュ』は、次ぎのURLを参照されたい。http://www.cert.org/archive/pdf/insidercross01105.pdf

として対処されなければならない。多くの従業員は、時々、心配事や不満を持つであろう。不満を申し出る正式かつ信頼できるプロセスがあれば、彼らを満足させることができ、さもなければ、彼らは、悪意のある行動に訴えるかもしれない。一般に、最重要な資産へのアクセスを有する従業員が困難に直面したならば、この従業員は困難を解決するために援助されなければならない。

懸念のある行動が特定された時に、組織が悪意のある行動のリスクを管理するための幾つかの方策がある。最初に、最重要な情報へのその従業員のアクセスが再評価されなければならない。また、彼、又は彼女のネットワーク・アクセスのレベルも考慮されなければならない。その従業員の最近のオンライン活動を慎重に調査するために、ログを調査すべきである。調査が実施されている間、組織は、機密文書である従業員支援プログラムへのアクセスを含むオプションを調査官に提供すべきである。

事例研究：これらが行われなかった場合、何がおこるであろうか。

あるシステム・アドミニストレーターが、組織のエンジニアリング部門を運営するために雇用された。そして、３か月後に、主要な新しいプロジェクトのリーダーに指名された。彼は、それから同僚を苛め始め、そして苛めが始まった１か月後に、彼はプロジェクトから外された。それから２か月も経たないうちに、彼は能力不足により解雇された。顧客は、彼が無作法であったと言い、同僚は、彼は他の誰より優秀であると思っていたと言った。上司は、彼が最初考えていたほど技術的に優秀でなく、その事実を隠すために同僚を苛めていたと判断した。企業は、彼にカウンセリングを提供したが、それに憤慨した。

彼の解雇からほぼ２ヵ月後、彼(インサイダー)は、彼と関係のあった企業内の女性従業員からシステム・アドミニストレーター・アカウントのパスワードを入手した。このパスワードを使用し、サーバーから、翌日に計画されていた重要な顧客への展示に必要なプロジェクトのホルダーを隠した。企業は、インサイダーに対処するために標準的な勧告を適用したが、それでも、彼は、企業のシステムを妨害することに成功した。この事例は、解雇されたインサイダーと依然として企業内で働いている従業員との社会的関係がもたらす潜在的危険性を浮き彫りにしている。

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別のインサイダーは、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。

最近の調査結果

インサイダーの情報窃盗及び改ざんに関する CERT の分析によると、情報の売却、部外者による改ざん、インサイダー自身の個人的ビジネス上の利益などの犯罪目的の違いにより、犯罪の方法にも重要な違いがあることが分かった。

金銭的な利益が動機の場合、犯罪は、少量のデータ(例：社会保証番号)を繰り返し、長期に亘って窃取、又は改ざんする傾向がある。金銭的利益のための改ざん事例５２件のうちのほぼ半数において犯罪が１年以上継続し、そして、ほぼ９０％が１か月以上継続していた。これは、ほとんどの犯罪において、インサイダーが企業に勤務している間に、インサイダー行為を探知する十分な時間があることを示唆している。一部のインサイダーは、彼らの行動に影響する個人的ストレス要因を持っていた。家族の医療問題、薬物等の濫用、金銭的困難、及び外部からの身体的脅威などである。しかし、事例全体におけるこれらストレス要因の有病率を決定するには更なる分析が必要であろう。

また、インサイダーは、職業的ストレス要因によっても影響される。経済的補償問題、監督者との問題、冷淡な作業環境、及びレイオフなどがこれに含まれる。あるシステム・アドミニストレーターが、組織再編のために計画されているレイオフについて知った後、７０個の企業用サーバーからデータを消去するよう設計されたロジボムを仕掛けた。人員削減を切り抜けた後でさえ、インサイダーはロジボムを改良し、1 年後に作動するよう設定した。幸いにも、システム問題を調査している時に、他のＩＴ要員がロジボムを発見し、破壊的なコードを無効にした。

ビジネス上の利益が動機の場合、犯罪は、非常に大きな量のデータ(例：専有ソースコード)に関係し、しばしば、インサイダーの退職３週間以内に発生する傾向が強い。しかし、ビジネス上の利益のための窃盗、特に、インサイダーが彼の責任範囲外にある情報(例：ソフトウェア・モジュール)に関心を持った場合は、しばしば、窃取する前に相当な計画が必要となる。また、分析された２４件のうちの３分の１以上で、インサイダーは、犠牲となった企業で働いている間に、彼自身のビジネスを既に始めるか、あるいは計画していた。盗んだ情報の移管について競合企業と詳細に詰めている時でも、彼らの

退職理由の多くは虚偽であった。２人の科学者は、企業の企業秘密を盗み、それを中国の国営企業に売却するために競合企業を設立した。彼らは、彼らの企業を情報の移動手段として使用するとともに、企業定款から彼らの名前を除き、企業と彼らとの関係を隠蔽した。

インサイダーと部外者とは、情報の窃盗と改ざんの両方において、高い共謀率を示した。共謀の兆候を探知できれば、組織にとってより高いインサイダー脅威を特定し、かつ適切に対応する機会を提供するであろう。ひそかな従業員間の会合や外部のビジネスとの関係については、組織を騙そうとする明らかな兆候である。匿名で不審な同僚を通報する手段が整備され、かつそれが従業員に周知されていなければならない。ビジネス上の利益のための窃盗事例２４件のうちの３分の２以上がインサイダーの退職から３週間の間に行われていた。組織は、組織の知的所有権に関する個人の法的責任と制約を明らかにし、退職間際の従業員に対処するために、大量のダウンロードに関するログを調査しなければならない。

⑸　実践事例５：険悪な職場問題を予期し、上手く対処しなさい。（新規）

従業員問題に対処する組織の方針を明確に定義・周知することは、規則等の一貫した履行を促すとともに、**険悪な**職場問題が生起した場合のリスク低減に有効である。

何をなすべきか。

雇用の初日から、従業員は、容認される職場行動、服装規定、容認される使用規程、労働時間、キャリア開発、問題解決、及び無数のその他の職場問題に関する組織の慣行と方針を知る必要がある。しかし、その様な方針が存在するだけでは十分でない。新しい従業員とベテランの従業員は、その様な方針の存在と同様にそれらに違反した場合の結果を知っている必要がある。方針の一貫した履行は、組織の調和した環境の維持に不可欠である。従業員が首尾一貫しない方針の履行を目にした時、それは、直ちに職場内の揉め事に至るであろう。分析した事例の多くでは、組織内の一貫しない履行、又は認識された不正は、インサイダーの不満を高める結果に結びついている。同僚は、しばしば、“優れた実行者（star-performer）”が規程の上にあり、特別の処遇を受けている、と感じていた。多くの場合、不満は、インサイダーを IT サボタージュや情報の窃盗に仕向けた。

従業員に問題がある場合、その問題が正当であるか否かにかかわらず、彼らは、組織内の支援を求める手段を必要としている。仕事に関連した問題を報復や険悪な結果を心配せずに、管理者又は人事部門の担当者と気楽に議論できることを従業員は必要としている。従業員が金銭的及び個人的ストレスを含む外部からの問題に直面した場合に、従業員支援プログラムのようなサービスの利用が彼らには有効である。これらのプログラ

ムは、従業員を支援するために信用できるカウンセリングを提供するとともに彼らが、作業能力、健康、又は一般的な幸せを回復するのを手助けする。もし、金銭的利益のために情報の窃盗や改ざんを行ったインサイダーが従業員支援プログラムを利用していたならば、彼（インサイダー）は、犯罪の動機要因となった金銭的及び個人的ストレスに対処する別の方法を見つけていたかもしれない。

従業員が、組織の知的所有権に関する合意書及び競合禁止に関する合意書を正しく認識して、合意書に正式に署名することは必須のことである。彼らが企業を辞めるときに、これらの合意書を思い出させることは重要である。組織の従業員として開発した知的所有権は誰が所有するかについて曖昧さがあってはいけない。情報を窃取したインサーダーの多くは、彼らが企業を辞めるときに、顧客リスト、価格表、及びソースコードを取得したことが企業の規則違反であることを知らなかったと主張した。

最後に、退職プロセスには、退職者から組織の資産を全て回収する処置が含まれていなければならない。コンピュータ及びアクセサリー、ソフトウェア及びハードウェア、組織の機密情報、ソースコード及びコンパイルコード、個人情報端末（PDA）、リムーバブル・メディア、並びに企業に所有権があるセンシティブ、機密、又は知的資産を内蔵するその他の品目を含む全ての資産を返却することが従業員に要求されなければならない。組織は、署名された知的所有権に関する合意書及び競合禁止に関する合意書のコピーを従業員に示すとともに、これらの規則に違反した場合の結果を説明しなければならない。

事例研究：これらが行われなかった場合、何がおこるであろうか。

ある事例では、インサイダーは、州政府職員の健康保険を取り扱う組織で働く下請者であった。疑いを持たない心理学者の医療 ID 番号を使い、インサイダーは、心理学者に関連した氏名と住所を共謀者の氏名と住所に変更した。インサイダーは偽の請求を起こし、支払いを偽の住所に送り始めた。監査人が、心理学者が骨折と開放創の治療のために支払請求をしているのにかかわらず、化学療法も行っていることに疑問を持ったときに、この企ては発見された。また、監査人は、心理学者の氏名が、下請者の氏名になっていることに気が付いた。調査の結果、インサイダーには詐欺の犯罪歴があることと、下請企業が雇用前に身元調査を実施しなかったことが判明した。

２番目の事例は、データベース管理者であると同時にプロジェクト・マネージャーである女性従業員は、同僚の男性従業員が、彼女の専門である技術的決定をないがしろにすることに不満を増大させた。彼女は、敵対的職場環境であると考え、人事部門へ訴えたがなんら処置がなされなかった。彼女が上司に訴えた後、優れていた彼女の実績は下降した。彼女の上司は、彼女からプロジェクト・マネージャーの責任を取り上げ降格さ

せた。彼女は再び訴えたが、逆に、彼女の上司は、彼女が指示に従わなかったとして訴えた。

次に、彼女は、出身国（インド)、人種（アジア人、インド人）及び性別（女性）に基づく差別であると雇用均等委員会（Equal Employment Opportunity Commission：EEOC）に訴えた。結局、彼女は、彼女の訴えに対する組織の無責任さに失望して退職した。退職後、彼女は、彼女の組織に対する（委員会への）苦情が否定されたことを知った。さらに、元の組織が、彼女が現在雇用されている新しい組織に否定的な勤務評定を送ったことを知った時に彼女の我慢は限界に達した。

彼女は、自宅から元の組織のコンピュータに接続した。彼女は、他の従業員のユーザー名とパスワードを使用してシステムにログインした。次に、彼女が退職した後も変更されていなかったデータベース管理者アカウントを使用し、最重要なシステムに侵入し、システムから最重要なデータを削除した。彼女は、昇任、異動、障害者請求に使用される２週間分のデータを削除し、システムの機能停止をもたらした。

⑹ 実践事例６：物理的環境を追跡し、安全を確保しなさい。（新規）

組織は、ビジネスを行うために、電気通信とオンライン取引に一層依存するようになっている。しかし、物理的環境を追跡し、内外の脅威から安全を確保することも未だ重要である。

何をなすべきか。

なりよりもまず、組織は最重要な資産、即ち組織の従業員を保護しなければならない。このプロセスは、職場環境には業務上の危険や部外者からの従業員に対する脅威が存在しないことを確認することから始まる。物理的環境のセキュリティを計画する際に、組織は、ロビー、エレベター、階段、及び駐車場を含む建物周辺部と同様に職場の空間を考慮すべきである。無許可の人物を施設から排除できるならば、セキュリティレベルを高めることができるであろう。

同様に、物理的セキュリティは、攻撃のために再度物理的アクセスをしようとする退職したインサイダーに対するもう１つの防御層になることができる。しかし、元従業員は、電子的セキュリティと同じように、組織の物理的セキュリティを上手く切り抜けることに成功した。一般に使用されているセキュリティ対策には、効果的なものもあれば、不十分なものもある。CERT が調査した事例は次のとおりである。

・施設に、常時、物理的セキュリティの存在を維持すること。
CERT が調査した事例では、一部のインサイダーは、24 時間常駐する警備員のために犯罪をはたらくのに苦労しなければならなかった。例えば、ある退職したイ

ンサイダーは、彼が退職したこと知らされていなかった警備員に、ID カードを忘れたと嘘をついた。しかし、警備員の存在は他のインサイダーに悪意のある行為を思いとどまらせたということも考えられる。

・全ての従業員、契約者、顧客、及びベンダーに対して、施設内では企業が発行した ID カードを携行することを要求しなさい。
CERT 事例資料によると、ある従業員は、元契約者から ID カードを入手し、それを時間外のアクセスが許可されていない施設への物理的アクセスを得るために使用し、ネットワーク運用センターのコンピュータに妨害工作を行った。もう 1 人の元従業員は、共連れ（ピギーバッキング）により、施設に時間外アクセスをすることができた。しかし、繰り返すが、これらの対策は、あまり動機のないインサイダーに対して有効であり、たぶん犯罪を思いとどまらせるであろう。

・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こと。
CERT 事例資料には、インサイダーが警報を巧みに回避した事例は皆無である。

・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こと。
CERT 事例資料によれば、一部のインサイダーは、監視カメラ及び監視ビデオによって特定され、有罪判決を受けた。

一旦、施設周辺の物理的環境が安全になれば、組織は、業務運営の弾力性を確保しながら、最重要な資産の保護に十分な資源を充てることができる。インフラストラクチャーのセキュリティ戦略は、組織の業務運営にとって最も重大な資産は何かを定義することから始まるべきである。これらの資産を、施設への物理的アクセスが制限された中央コンピュータ設備に統合すべきである。当該施設へのアクセス管理は、明確に定義され、そして従業員の採用・解雇のときに変更されるべきである。当該施設へのアクセスは、自動記録方式又は少なくても施設の入退室時の記録用紙への署名によって確認されるべきである。

また、バックアップ媒体の物理的保護も極めて重要である。一部の事例では、悪意のあるインサイダーは、バックアップ媒体を盗むか又は破壊することができた。インサイダー攻撃から復旧するまで間、組織の業務は遅延したり又は活動不能になったりするであろう。

コンピュータ設備に保管された最重要な資産の安全を確保するのに加えて、組織の保護された区域及び保護されていない区域の両方の区域に設置されたコンピュータ、ワークスティション、ラップトップ、プリンター、及び FAX に対する慎重な注意が必要である。コンピュータ・インフラストラクチャーのセキュリティは、組織の周辺部から始まり、ドアや窓を施錠するという事務所の保護にまで至る。CERT データベースの事例によると、ある従業員は、終業時間まで待って、事務室の外側から同僚の名札を外し、彼

自身の名札に交換した。それから、彼は、事務所に忘れ物をしたが鍵を持っていないと守衛に告げた。守衛は、彼の ID カードが事務所の名札と一致したので、ドアの鍵を開けた。従業員は、それから、彼の同僚のコンピュータから専有情報であるソースコードをダウンロードし、それを窃取した。

物理的防御の次のレベルには、コンピュータ資源の安全確保、例えば、パスワードで保護されたスクリーンセーバーの使用、リムーバブル・メディアの暗号化、多元的認証方式を必要とするモバイル機器及びリムーバブル・メディア（例えばラップトップ、メモリースティックと PDA）の安全確保などがある。

できる限り、組織の設備へアクセスする試みは記録されるべきである。アクセス・ログの定期的な監査がアクセス方針の違反又は未遂を特定するために実施されなければならない。これらの違反の自動警報は、組織が大きな損害を受ける前に、セキュリティ違反を探知することを可能とすることができる。

事例研究：これらが行われなかった場合、何がおこるであろうか。

次の例は、契約者に関する重要な物理的セキュリティ及び法律上・契約上の問題を提起している。従業員のセキュリティ・アクセスは、“従業員争議に基づき”、彼の雇用主によって停止された。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。

この種の契約上の問題は、既に事例１の“最近の調査結果”のセクションで議論された。この事例は、組織は、契約業者による従業員に対する差迫った制裁の事前通知を要求するために契約慣行を変更すべきである、というもう一つの例である。さらに、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不満を抱えた従業員がもたらす潜在的損害を例示している。

また、組織は、重要な情報を含んだ文書の追跡及び処分に関する戦略を実行する必要がある。さらに、インサイダー脅威に対する予防策は、全ての従業員に適用されなければならない。たとえ、明らかに組織のコンピュータ資源に対するアクセス権を有していない者であっても。センシティブ、専有、秘密（confidential）、又は極秘（secret）情報の侵害に関連する幾つかの最近の事例は、これらの情報を含んだ資料の処分に関するず

さんな管理が原因である。ある事例では、夜勤の守衛が事務室のごみを漁り、銀行顧客の個人情報を入手し、なりすまし犯罪（identity theft）を働くためにその情報を使用した。他の事例では、ある従業員が破棄するために棄てられた機密資料が入ったホッパー車から企業秘密を含んだ文書を入手することができた。そして、その文書は、外国の競争相手に売却された。

⑺ 実践事例７：パスワードとアカウントの管理方針と行動基準を厳格に実施しなさい。（更新）

組織のコンピュータ・アカウントが漏洩すれば、インサイダーは、手動及び自動の管理対策を回避することができる。

何をなすべきか。

組織がインサイダーからもたらされる脅威を軽減することに如何に注意しても、組織のコンピュータ・アカウントが（インサイダーに）漏洩すれば、インサイダーは、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回避する機会を得るであろう。従って、コンピュータ・アカウントとパスワードの管理方針と行動基準は、違法な目的で組織のシステムを使おうとするインサイダーの能力を妨害するために重要である。適切なコンピュータ・アカウント管理と結びついたきめ細かいアクセス管理は、組織の最重要な電子的資産へのアクセスを次のようにすることができる。

・無許可のアクセスを難しくする。
・不審なアクセスを探知・調査できるよう記録し、かつ監視する。
・そのアカウントから、そのアカウントに関連した個人を追跡できる。

悪意のあるインサイダーがアカウントを侵害するために使用する方法には、パスワードクラック（他人のパスワードを不正に暴くこと）又はソーシャルエンジニアリングで取得する方法、従業員同士で公然と共有するパスワードを使用する方法、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。パスワード作成方針と作成手順によりパスワードの強度を確保するべきである[12]。従業員は誰ともパスワードを共有してはいけない。従業員はパスワードを定期的に変更しなければならない。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。結果として、どのアカウントからであっても、全ての操作がそのアカウントの所有者によって行われるものでなければならない。さらに、匿名の通報システムが運用されていなければならない。通報シス

12 『パスワードの選択と保護』は次のURLを参照されたい。
http://www.us-cert.gov/cas/tips/ST04-002.html.

テムの運用は、従業員に対して無許可のアカウント・アクセスの全ての試みについての従業員からの通報を促進するであろう。

一部のインサイダーは、バックドア・アカウントを設置した。それは、彼にシステム・アドミニストレーター又は優先的アクセスを提供した。その他のインサイダーは、共有アカウントの無効化が退職プロセスで見落とされていたために、それらがまだ利用できることに気づいた。システム・アドミニストレーター・アカウントが一般に使用された。その他の共通アカウントにはデータベース・アドミニストレーター（DBA）アカウントが含まれた。一部のインサイダーは、契約者やベンダーのような外部のパートナーのために設定されたその他のタイプの共有アカウントを使用した。あるインサイダーは、パスワードが変更されずに長い期間繰り返し使用されていた訓練用アカウントを使用した。

技術的管理と結びついた定期的な監査は、次のアカウントの特定を可能とする。

- インサイダーによって悪意のある行為のために使用されたバックドア・アカウント。（インサイダーによって設定されたもの、あるいは以前に従業員によって残されたもの）
- パスワードがインサイダーに知られており、そして退職後も変更されていない共有アカウント。
- 契約者やベンダーのような外部のパートナーのために設定されたアカウント。これらのパスワードは複数の従業員に知られており、そして契約者等が退職した時にも変更されなかった。

全てのアカウントの必要性は、定期的に再評価されるべきである。厳格な手順、技術的管理、及び必要不可欠なものだけにアカウントを制限することは、監査人と調査人が、これらのアカウントから行われた全てのオンライン操作を個人のユーザーにまで追跡するのを可能とし、そしてインサイダーが悪意のある行為を特定されず行う能力を減少させる。全てのユーザーの、全ての特権的アクセスの厳格な文書化含むアカウント管理方針は、退職した従業員による攻撃のリスクを減らす退職プロセスを可能にする。

また、組織のパスワード及びアカウント管理方針は、組織の情報システム又はネットワークへのアクセスを有する全ての契約者、下請者、及びベンダーに適用されることが重要である。これらの方針は契約書に記載されるべきである。それは、あなたの組織のシステムにアクセスした人物を追跡する際に、同じレベルの責任を要求するものでなければならない。契約者、下請者、及びベンダーには、あなたの情報システムにアクセスするためのグループアカウントを与えてはならない。彼らには、パスワードを共有することを許してはならない。そして、それらの従業員が、契約業者など、外部組織から解雇されるときは、あなたの組織がアカウントパスワードを変更できる余裕が得られよう

前もって通知されなければならない。最後に、契約者、下請者、及びベンダーのアカウントを確実に定期的なパスワード変更プロセスに含めなければならない。

事例研究：これらが行われなかった場合、何がおこるであろうか。

不満を持ったソフトウェア開発者は、組織の NUIX サーバーからパスワードファイルを彼のデスクトップへダウンロードした。次に、彼はインターネットからパスワードクラッカーをダウンロードした。そして、ルートパスワードを含む約４０個のパスワードを解読した。幸運にも、損害をもたらさなかった。彼は、アクセスを許可されていない組織のネットワークの一部にアクセスした。彼がシステム･アドミニストレーターにルートパスワードを知っていると自慢した時にやっとこのインサイダーは発見された。その結果、組織は、将来この様な攻撃を防止するための対策を実行するために方針と手順を改正した。システム・アドミニストレーターは、パスワードクラッカーを実行し、弱いパスワードを使用しているユーザーに、それを通知することが認められた。そして、如何、何故、強いパスワードを選ぶかについて従業員を教育するためにセキュリティ訓練が改善された。

また、２番目の事例は、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。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、作業効率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、他の特権的な従業員の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か月後に、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が付き、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。

最近の調査結果

アウトソーシング、サプライチェーン管理、及び市場のグローバリゼーションの普及・拡大は、組織と外部世界との境界を曖昧なものにした。組織のデータと情報へのアクセスの管理について、内部者と外部者の違いを見分けることは益々難しくなっている。契約者、下請者、及びベンダーは、世界市場で競争する組織にとって新しい重要な構成要素となっている。契約者、下請者、及びベンダーとの関係に対処する場合は、インサイダーはもはや組織内の従業員だけではないことを理解しなければならない。ビジネス・

パートナーによって雇用されたインサイダーは、慎重に管理され、契約上の義務を果たすために必要である情報だけへのアクセスを認め、そして、それが必要でなくなったときに、直ちにアクセスが確実に停止されるよう慎重な注意が払われなければならない。

最近の事例では、あるインサイダーは、市場調査会社にシステム・アドミニストレーターとして雇われていた。市場調査会社は、世界最大の消費者データ処理企業の１つである組織と業務を契約していた。契約の結果、彼は、消費者データ処理企業のFTP（ファイル転送プロトコル）サーバーへのアクセスが与えられた。そのため、彼は、銀行、クレジットカード会社、及び電話会社を含む顧客の消費データからサニタイズされた凝集情報を定期的にダウンロードすることができた。システム･アドミニストレーターは、暗号化されたパスワードを含んだ幾つかの無防備なファイルをＦＴＰサーバーに発見した。彼は、消費者データ処理企業の顧客（およそ 200 の大企業）の１０％の顧客データベースのパスワードを簡単に解読した。それから、彼は、何十ものコンパクトディスクに何百万ものアメリカ人の個人データをコピーし始めた。彼からセンシティブな顧客情報を入手したハッカーの捜査中に偶然に窃盗が発見された。その後、彼の住居の捜索でコンパクトディスクが発見された。

この事例は、ひとたび組織の境界を超えた情報の安全を確保するために、組織が適切な法的措置をとることの重要性を強調している。また、組織の情報を管理するどんな第三者に対しても強い規制が必要であることの重要性を示している。

⑻　実践事例８：任務の分離と最少特権を実施しなさい。（更新）

任務の分離と最少特権は、悪意のあるインサイダーがもたらす損害を極限するために、ビジネスプロセスにおいて、及び最重要なシステム又は情報の技術的規制において実行されなければならない。

何をなすべきか。

任務の分離とは、従業員が情報を窃取できる可能性、又は協力なしで詐欺若しくはサボタージュを行うことができる可能性を極限するために、機能を一人ひとりに分割することである。二人ルール（two-person rule）と呼ばれている任務の分離の１つのタイプがしばしば使われる。それは、仕事の実行に２人の参加を求めるものである。任務の分離は、技術的又は非技術的な規制を通して実施される。例えば、多額な銀行振出小切手の署名には、２人の銀行員を必要とすること、又は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することなどがある。当然、検証と審査は別々の人が実施する。従業員がもう１人の従業員と協力しなければならないならば、従業員が悪意のある行為を働く可能性は小さくなるであろう。

任務の効果的分離には、彼らの仕事をするために必要な資源だけを彼らに許可するという最小特権（least privilege）の実行を必要とする。最少特権は、従業員による機密又は専有情報の窃盗のリスクを削減する。何故なら、従業員のアクセスは、仕事をするために必要なアクセスだけに限られるからである。ビジネス上の利益のための情報の窃盗事例の一部には、販売員が関係していた。その販売員は、開発中の戦略的製品へ不必要なアクセスをした。

特に従業員が昇進、異動、再配置、及び降格などにより、組織内を移動する際に最少の特権の管理が継続して実施されることが重要である。従業員の仕事が替わった時に、組織は、情報及び情報システムへの彼らに必要なアクセスの見直しを怠る傾向がある。そして、前の仕事をするために必要であった情報及びシステムへの彼らのアクセスを取り消すことなく、新しい仕事に必要な新しいシステムや情報へのアクセス権が彼らに与えられることがよくある。従業員が、情報と情報システムへのアクセスを必要とする前の仕事を継続しない限り、彼らの古いアクセス権は無効化しなければならない。

一般的に、組織は、各々の仕事の責任を果たすために必要な組織の資源へのアクセスと同様に、各々の仕事の役割を定義する。鍵となるビジネスプロセス及び機能における責任を有する役割を定義・分離することによってインサイダーリスクを軽減することができる。例えば、

- 最重要なデータ入力業務にはオンライン管理許可を必要とすること。
- ソフトウェア開発とメンテナンスプロセスにはコードチェックを実施すること。
- ソフトウェア配布及びシステム改修を管理するために、環境設定管理プロセス及び技術的規制を使用すること。
- 監査人同士の共謀を防止するための監査手順を設計すること。

物理的規制、管理上の規制、及び技術的規制は、従業員の仕事の達成に必要な資源だけにアクセスを制限するために使用することができる。アクセス管理の隙間は、しばしば、インサイダー犯罪を容易にした。例えば、従業員は、技術的規制より、むしろ方針に基づき行うことになっている任務の分離を回避した。理想的には、組織は、任務の分離をビジネスプロセスの設計に含ませ、そして、技術的及び非技術的手段によってそれらを実行しなければならない。

任務の分離及び最小特権を基礎としたアクセス管理は、インサイダー攻撃のリスクを軽減するために不可欠である。これらの原則には、物理的世界と仮想世界双方との関連がある。物理的世界では、組織は、従業員が仕事・役割に必要でない資源へ物理的アクセスするのを防止する必要がある。研究者は、彼らの研究所空間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への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要とするが、研究所施設へのアクセスを必要としない。仮想世界にも直接の類似性がある。そこでは、組織は、彼らの仕事に必要でない情報又はサービスへの従業員のオンラインアクセスを防止しなければならない。この種の管理は、役割基盤のアクセス管理（role-based access control）と呼称される。従業員の機能的な役割に基づき、組織内の個人のアクセスを禁止することは、彼らが不満により又はさもなければ彼ら自身の目的のために、組織を悪用しようと決心した場合においても、彼らがもたらす損害を制限することができる。

事例研究：これらが行われなかった場合、何がおこるであろうか。

ある事例では、通貨トレーダー（彼は、偶然、大学でコンピューター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、ソフトウェアに不明瞭な機能を実装した。それにより、彼は、５年にわたり総額６億９,１００万ドルの違法な取引を隠蔽することができた。この事例の場合、監査人が彼の活動を探知することはほとんど不可能であった。

インサイダー脅威スタディーのインタビューに同意したインサイダーは、研究者に、“キツネが鶏小屋を守っている”時に問題が起こると語った[13]。具体的に言うと、インサイダーの監督者は、インサイダーと彼の取引が合法的であること又は規則に準拠していることを保証する責任を有する監査部門を監督していた。監査部門の要員がインサイダー活動に対して懸念を持ったとき時、彼らはインサイダーの監督者（その人は、偶然に彼らの監督であった）に懸念を提起した。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、そして、懸念を提起するのを止めるように指示した。

この事例は、任務の分離によって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。

- 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。
- 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。

もう１つの事例では、あるスーパーバイザーは、組織のコンピュータ・システムを使って、不正に、米国移民・亡命者保護決定を変更した。彼は、１件につき数千ドルの報

---

[13] インサイダー脅威スタディー：『銀行及び金融分野の不正なサイバー行為』は次のURLを参照されたい。
http://www.cert.org/archive/pdf/bankfin040820.pdf

酬を得て、２年以上にわたって 5 万ドルを蓄えた。インサイダーは、彼自身で亡命者保護決定を承認するか、部下のうちの 1 人に決定を承認することを頼むか、又は亡命申請書に対する他の誰かの拒否決定を覆した。数人の外国人は、彼らの亡命者申請書に嘘を記載したこと及び彼らの申請を承認するよう公務員を買収したことをインタビューで認めたり、あるいは法廷で罪を認めた。組織は、そのスーパーバイザーのコンピュータ・アカウントから、亡命者保護決定の承認又は修正ができないように、役割基盤に基づくアクセス管理を通して任務の分離を実行していたが、そのスーパーバイザーは、全部のデータベースでどんな決定でも変更することができた。しかし、部下に割り当てられたものだけは変更できなかった。そのスーパーバイザーが亡命者申請を承認するか、又は彼らまたは彼らのチームが関与しなかった亡命者保護判決を覆すのを防止するためには、防御のさらなるレベル、即ち最小特権を実行することができたであろう。

最近の調査結果

最近の事例の分析で、金銭的利益のための情報の窃盗のほぼ３分の 1 と金銭的利益のための情報の改ざんの半分が、少なくとも 1 人の他のインサイダーと共謀していることが分かった。その理由は、任務の分離を管理する規制を回避するために、内部の共謀が必要であったためである。任務の分離だけではインサイダー攻撃を防止できないので、組織は、そのような攻撃の可能性を減少させるための多層防衛を実行することが重要である。

最近の事例では、消費者信用調査会社で働いたインサイダーが関係していた。インサイダーの仕事は、消費者信用データベースに保管される情報を維持することであった。インサイダーは、外部の協力者からの金銭と引替えに、特定の消費者が信用機関及び金融業者とローンを組むことができるように人為的に彼らの信用度を高めるために協力者と共謀した。インサイダーと内部の共謀者は、１７８人の消費者のために信用履歴データを改ざんするか又は削除した。目的は彼らの信用度を強化し、貸手がこれらの消費者に融資することであった。インサイダーは、改ざんの報酬を前払いで受け取り、データベースの変更をするために彼女（インサイダー）の同僚に報酬を渡した。この事例は 4００万ドル以上の危険なローンが生じさせた。

最近の多数の事例から CERT チームが観察した 1 つのパターンでは、顧客のメールアドレスや電子メールアドレスを変更したインサイダーが関係していた。それは、インサイダーが、顧客の個人情報を使用して開いた詐欺的なクレジットカード・アカウントへ自動化した通知、請求、及び他社とやり取りの書簡を顧客が受け取らないようにするためであった。一部の銀行や他の組織では、既に実際に顧客データベースを変更する前に、顧客の住所及び電子メールアドレスの変更を確かめる手順を定めている。任務の分離の原則の上にこの手順を追加することにより情報の保護をより一層強化することができる。

本セクションのこれらの事例は、任務の分離による管理を無効にする共謀の可能性が非常に高いという前提で、従業員の間の潜在的共謀を探知するための監査手順を設計することの重要性を示している。

⑼ 実践事例９：ソフトウェア開発ライフサイクルを通してインサイダー脅威を考慮しなさい。（新規）

技術系従業員は、故意に悪意のある技術的行為をはたらくために、ソフトウェア開発ライフサイクル（以下、SDLC という）の間に挿入された欠陥を悪用した。：非技術系従業員が脆弱性を知って、詐欺的行為を行うためにその脆弱性を悪用したのと同じである。

何をなすべきか。

SDLC の間に挿入された欠陥を使用したインサイダーが、もたらした影響には、次のようなものが含まれる。

・会社の倒産
・詐欺による６億 9,１００万ドル以上の損失
・合法的な運転免許証を得ることができなかった個人のために偽造された運転免許証
・電気通信サービスの混乱
・法廷記録、信用記録、及びその他の重要なデータの改ざん
・顧客システムに植え付けられたウイルス

これらの事例の影響は、明らかに重大であった。組織は、これらの脅威を認識し、内部的にソフトウェアを開発・維持する時及び他から取得したシステムを実装する時に、潜在的脅威と軽減戦略を考慮することが重要である。

調査した事例では、インサイダーは、SDLC の全ての段階で欠陥を悪用した。以下、SDLC の各段階を詳細に分析する。

要求定義（Requirement Definition）

多くのシステムは、ビジネスと作業のプロセスを自動化する。そのようなシステムの要求を定義するときは自動化されるプロセスを慎重に定義しなければならない。調査した事例では、多くのインサイダーは、そこにインサイダー脅威からの保護が考慮されていないという事実を知っていたので、違法な行為を行うことができた。例えば、一部の事例では、自動化されたプロセスに任務の分離が考慮されていなかった。その他の事例では、認証と役割基盤のアクセス管理が、システム・アクセスに要求されていなかった。

システム要求には、データ保全と一貫性チェックの仕様が含まれなければならない。一貫性チェックは、不審な修正、追加、又は削除を探知するために定期的に実行される自動チェックと同様に、システムエンドユーザーによって行われた、製造データの全ての変更をチェックするための自動チェックがされなければならない。言い換えると、要求には、手動監査よりも頻繁に自動的に実行される定期的な監査機能が考慮されていなければならない。

システムの要求定義に詳述される推奨の全てを組織が製造したシステムと取得したシステムの両方に適用されることに留意すべきである。新しいシステムを取得するための評価を実施する場合も、ここで詳述される要求仕様の種類が考慮されなければならない。要求が定義され、そして、潜在的システムが購入のために評価された時に、各々のシステムの能力がこれらの要求に適合することが評価プロセスの重要な一部分である。

システム設計（System Design）

一部の事例では、組織は、彼らのシステム要求定義プロセスにおいて、インサイダーからの保護に取り組んだ。しかし、自動化された業務プロセスの機能の不十分な設計により、一部のインサイダーは、悪意のある行為を行うことができた。例えば、不適切に設計された任務の分離は、インサイダー犯罪を容易にした。場合によっては、任務の分離がシステムに全く設計されていなかった。その他の事例では、任務の分離は実行されたが、「チェッカーをチェックする」設計がなされなかった。インサイダー窃盗又は改ざん事例で観察された共謀は、非常に高度なものであるので、システムデザイナーは、同じ職場の２人の従業員が共謀している事件を探知するために任務の分離の上に、もう１つの防衛の層を実装することを考慮することが必要である。大部分のこの種の犯罪は、長い期間にわたって継続するので、発見はすぐにできないが、不審な行動のパターンは、後で発見するのでなく、むしろより早く捕えることができる。

システム設計の脆弱性に関するもう１つの調査結果は、許可されたシステムオーバーライド（優先処置）に関するものであった。数人のインサイダーは、犯罪を実行するために、例外的な処理に設定された特別なシステム機能を使用した。彼らは、これらの機能が迅速な変更が要求される状況における例外的な処理に設定された機能であり、従って、通常の義務的セキュリティチェックを迂回していることを理解していた。この種の機能は、インサイダーに対して“規則の目をかいくぐる”簡単な方法を提供する。例外的な処理機能を利用して修正、追加、及び削除されたどんなデータでも、特別なデータ保全チェックが行われるよう設計することが重要である。

実装（Implementation）

極めて少数のインサイダーは、初期開発プロセスの間に、実際に、意図的に脆弱性コ

ード又は悪性コードをソースコードに挿入した。この種の行為は、SDLC のメンテナンス段階より一層頻繁に行われた。しかし、１８才のウェブ開発者は、旧会社のネットワークにアクセスするために、システム開発時にソースコードに挿入したバックドアを使って、その会社の顧客にスパム（電子メールによる大量広告）を送ったり、そのアプリケーションを変更したりした。そして、最終的にその会社は倒産に追い込まれた。SOLID（Single responsibility、Open closed、Liskov substitution 、Interface segregation、Dependency inversion）ソフトウェア開発プロセスの一部であるコードレビュー（ソースコードの体系的な検査）と厳格な変更管理は、バックドアを探知することができ、おそらく会社を救うことができたに違いない。

SDLC の間、組織は、システム製造の間に生じるのと同じ種類のインサイダー攻撃に脆弱である。あるソフトウェア開発プロジェクト・マネージャーは、開発環境の中では、（悪意のある）行為をシングルユーザーのものと突き止める方法がないことを理解して、繰り返し彼自身のチームのプロジェクトを妨害した。この事例の動機はユニークであった。彼のチームは、プロジェクト予定表より遅れていた、そして、最終期限に間に合わなかった言い訳としてその妨害活動を行った。組織は、システムの製造過程と同じように、開発プロセスの途上にあるものの復旧機能を検討しておくことが重要である。

設定（Installation）：

開発から製造までのシステムの移行過程における様々な不注意は、インサイダーに攻撃する手段を提供した。いくつかの異なる事例は、次のとおりである。

- システムは、ソースコードのバックアップを作ることなく、大きな政府機関で製造過程にあった。システムが製造に入った後、開発プロジェクト・マネージャーは、プロジェクトのソースコードの唯一のコピーを暗号化した。そして、コードの解読と引替えに金銭をゆすり取ろうとした。
- 開発環境で使われていたものと同じパスワードファイルが、運用システムの製造段階でも使われた。そのため、開発者のうちの 1 人は、運用システムにアクセスし、運用システムにインストールされていた機密データを盗むことができた。
- 全ての顧客システムへの無制限なアクセスは、コンピュータ技術者に、顧客ネットワークに直接ウイルスを植えることを可能とした。
- 組織は、その公的ウェブサイトの全ての変更を管理する Web コンテンツ管理システムを実装した。彼らは、変更を追跡するためにこのシステムを使ったが、ウェブサイトに公開する前に、変更を承認するプロセスを保有していなかった。その結果、大学からの実習生は、夏に実習が終了する前に、組織のウェブサイトに冗談のつもりで資料を公開した。そして、それは世間を騒がせ、その政府機関の信用を落とす結果となった。

組織が、システムを開発段階から製造段階へ移行するときにこれらの問題を慎重に考慮することが重要である。何故ならば、従業員は毎日それらのシステムを使用しているので、たぶん彼らは脆弱性に気が付くからである。

システム維持（System Maintenance）

より多くのインサイダー・インシデントは、初期のシステム実装の間よりも SDLC の維持段階の間に生起した。組織は、初期の開発段階ではより厳しい規制を強要するが、一旦、システムが製造段階に入って最初のリリース後に安定すると、それらの規制はより緩やかになる傾向がある。事例のインサイダーは、様々な方法でそれらの緩やかになった規制を利用した。

多くの組織は、新しいシステムの開発又は既存のシステムのための新しいモジュールの開発において義務的なコードチェックを行うが、それでも、一部のインサイダーは、安定したかなり静的なシステムに、探知されずに悪性コードを挿入することができる。効果のない環境設定（コンフィギュレーション）の変更管理システムがインサイダーの不正行為に寄与した。調査した事例の中の２，３の組織は、悪意のあるインサイダー行為の詳細なログを記録する環境設定管理システムを実装したが、実際には、悪意のある行為を探知するために必要なログを調査するプロセスが準備されていなかった。

また、インサイダーは、攻撃の効果を高めるために、保護されずに設置されたバックアップシステムを破壊することができた。最重要なシステムのリスクマネージメントは、システムそれ自体を超えて、例えば、オペレーテングシステムやバックアップなどの周辺支援システムまで拡大することが必要である。

ユーザー認証は、時間とともにより緩やかになる傾向があるもう１つの領域である。システムが最初にリリースされる時は、システムの認証及びアクセス方式は慎重に実装される傾向があるが、一旦、システムが製造段階になると、ユーザーのアクセス管理は忘れられる傾向がある。システムへのアクセス及びソースコード自体へのアクセスは、時間とともに慎重に管理されなければならない。

事例研究：これらが行われなかった場合、何がおこるであろうか。

電信通信会社のプログラマーは、ボーナスが支給されないと聞き腹を立てた。彼は、プロジェクトリーダーのコンピュータを使用し、会社の第一の製品（インターネットワーク通信インタフェース）を改ざんした。プロジェクトリーダーは個室を使っていたが、しばしば、コンピュータをログインしたまま無人にしていた。彼は、転送ストリーム（抽象データ型）のランダムな場所に符号「i」を挿入した。また、彼は、悪性コードをロジボムとして挿入したが、それは、会社の環境設定管理システムにログ（記録)され、それ

はプロジェクトリーダーが原因であると考えられた。６か月後、インサイダーは新しい仕事に就くために退職した。その６か月後、ロジボムはついに爆発した。そして、顧客に対する会社のサービスに大きな困惑と混乱を引き起こした。この事例は、本セクションで論じた問題の多くを例証している。

もう一つの事例は、SDLC で見逃されたために生起した技術的には低レベルのインシデントである。警察通信オペレーターの主要な責任は、現場の警官に運転免許証に関する情報を伝えることであった。彼女（オペレーター）の知人が彼女に近づき、３人の情報を調べる気があるかどうか尋ねられた時にこの事例は始まった。そして、彼女は同意した。時間とともに、彼女は、報酬のために、人々に関する情報を調べるようになった。ある時点で、彼女は、データベースから情報を読むことができるだけでなく、他のシステムの機能を使用する能力があることを発見した。その時、彼女は、共犯者の要望により、合法的には運転免許証を取得できない人々のために違法な運転免許証を作成した。幸いにも、秘密情報（内報）により、彼女は、１９５件の違法な運転許可証を偽造した罪で逮捕された。この事例は、システム要求を定義する時、システム設計の時、そして実装の間に、役割基盤アクセスの制御条件を見落とすリスクを示している。

⑽　実践事例１０：システム・アドミニストレーター、及び技術的又は特権的ユーザーに対して特別の注意を払いなさい。（更新）

システム・アドミニストレーター及び技術的又は特権的ユーザーは、悪意のある行為を働き、それを隠蔽することができる技術的能力、アクセス、及び監督責任を有している。

何をなすべきか。

サボタージュを行った大部分のインサイダー及び機密又は専有情報を窃取したインサイダーの半数以上が技術者であったことを思い出しなさい。悪意のある行為を行い、かつ隠蔽する技術の中で高度な方法には、スクリプト若しくはプログラム（ロジボムを含む）の書き込み又はダウンロード、バックドア・アカウントの設定、リモートシステム管理ツールのインストール、システム・ログの改ざん、ウイルスの植え付け、及びパスワードの解読が含まれる。

システム・アドミニストレーター及び特権的ユーザー[14]は、システム、ネットワーク、又はアプリケーションへの他のユーザーより高いレベルのアクセス権を持っている。こ

[14]本報告では、特権的ユーザーは、完全なシステム・アドミニストレーター・アクセスには及ばないが、ネットワーク、コンピュータ・システム、又はアプリケーションへの高いレベルのアクセスを有するユーザーを意味する。例えば、データベース管理者（DBA）は特権的ユーザーである。彼らは、新しいユーザー・アカウントを設定する及び彼らのドメインの中でユーザーのアクセス権をコントロールする能力がある。

のより高いアクセスレベルは、次の理由により、より高いリスクをもたらす。

・彼らは、普通のユーザーができない行為を実行する技術的能力とアクセス権を持っている。
・彼らは、通常、彼らの行為を隠蔽することができる。何故なら、特権的なアクセス権は、彼らに、システム・ログファイルを改ざんするためか、あるいは監査ログ及び監視報告を偽造するために他のユーザーとしてログインする能力を提供している。
・たとえ、組織が技術的に任務の分離を実施したとしても、システム・アドミニストレーターは、アプリケーション又はシステムの変更が要請された時に、それを監督及び承認する責任を有する本人である。

行為の否認防止（non-repudiation）を促進する技術により、システム・アドミニストレーターや特権的ユーザーを含むユーザーによって行われたオンライン行為について、確実にその行為を実行したユーザーを特定することができるようになった。従って、悪意のあるインサイダー行為が発生した場合に、否認防止技術により、どんな行為であっても、１人の従業員を特定することができる。システム及びネットワークにおいて、否認防止を容易にするための方針、実施要領、及び技術が存在する。しかし、システム・アドミニストレーターと他の特権的ユーザーは、これらの方針、実施要領、及び技術を設計・作成・実行する責任者であることに留意しなさい。従って、任務の分離もまた、非常に重要である。：ネットワーク、システム、及びアプリケーションのセキュリティ設計は、複数の特権的ユーザーによって作成・実装・実行されなければならない。

たとえ、オンライン行為に係わったユーザーまで追跡できたとしても、全てのユーザーの行為が先行的に監視されていると期待することは不合理である。従って、不審な行動を探知した後、ユーザーの特定を確実にするために、悪意のある行為が生起する前に、組織によって、追加的な防衛処置が取られていなければならない。例えば、システム・アドミニストレーター及び特権的ユーザーは、彼らのドメインの中で全てのコンピュータファイルにアクセスできる。そのようなユーザーが、アクセスすべきでないセンシティブなファイルを読んだり、改ざんしたりするのを防止するために、暗号化のような技術が実装されなければならない。

方針、手順、及び技術的制御において任務の分離が強制されるべきであり、かつ重要なシステム、ネットワーク、アプリケーション、及びデータに関する全ての修正を行う際には複数のユーザーの行動を必要とすべきである。言い換えると、シングルユーザーは、第２のユーザーによるオンライン操作なしでは製造環境の変更を行うことが技術的にできないようにすべきである。あるインサーダーは、たまたま、コンピューターサイエンスの学位を持っていたので、取引システムのソースコードへのアクセスが与えられ

た。彼は、そのアクセスを使い、バックドアを設定した。そして、彼は、それによって、5 年以上にわたり、合計 6 億 9,１００万ドルの取引損失を発見されることなく隠すことができた。

システム制御機能として任務の分離を実施するためには、少なくとも 2 人のシステム・アドミニストレーターが組織によって雇用されなければならないことに注意しなさい。本報告には、たった１人のシステム・アドミニストレーターしか雇用していなかった組織が犠牲となった幾つかの事例がある。多くの小さな組織は、２人以上のシステム・アドミニストレーターを雇うことができないが、組織はその状況に伴うリスクの増加を認識することが重要である。

最後に、調査された多くのインサイダー、特に IT サボタージュに係わったインサイダーは、元従業員であった。組織は、とりわけ、元システム・アドミニストレーター及び技術的又は特権的ユーザーのアクセスを無効化することに慎重でなければならない。アクセスを無効化するための完全に文書化された手順は、散在するアクセスポイントが見落とされないようにするために有効である。さらに、彼らが組織を辞めた後の脅迫のリスクを減らすために、２人のルール（例えば、２人のシステム・アドミニストレーターの雇用）は考慮されなければならない。

事例研究：これらが行われなかった場合、何がおこるであろうか。

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。彼は自宅でロジボムを製造し始めた、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２週間も経たずに、ロジボムは午前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、損失は、同社の１２億４、０００万株にも影響を及ぼした。

もう１つの事例では、あるインサイダーが昇任して同じ組織の別の配置に就いた。両方の配置とも、医学及び高度障害保険請求の記入、承認、支払いに同じアプリケーションを使用していた。アプリケーションは、システム機能ごとに任務の分離を実施するために、役割基盤のアクセスを使用していた。そして、このインサイダーが昇進した時、彼女は新しいアクセスレベルによってアクセスが許可されたが、システム・アドミニストレーターは、彼女の元のアクセスレベルを取り消すことを怠った。（任務の分離の実施が不十分であった。）その結果、彼女は、システムからの支払いについて誰の認可も

なく、アプリケーションへの完全なアクセスを得ることになった。彼女は、婚約者への毎月の支払を、要求し、承認し、許可した。そして、ほぼ２年にわたって、６１万５,０００ドル以上を支払うという結果となった

最近の調査結果

ビジネス上の利益のための情報の窃盗の７１パーセントは、技術的経歴を持った個人によって行われた。多くの場合、プログラマーを含む技術系従業員は、ソースコードやシステムアーキテクチャ(セキュリティ文書)を含む顧客情報と知的所有権を手に入れ、そして、それらと共に組織を去った。それらの従業員は、いくつかの理由のために情報を使った。:新しい仕事を得るため、新しい組織で自分に競争上の有利さを与えるため、及び新しい組織が犠牲となった組織と張り合うのを援助するため。

さらに、最近の事例によると、不満を持ったシステム・アドミニストレーター及びその他の特権的ユーザーの取り扱いの失敗が、依然としてITサボタージュに結びついていることを示している。ある事例では、容疑者は、電子商取引ソフトウェアの開発者であった。彼は、家族を異なる州に移動させることを決めていた。従って、彼はもはや組織のために働くことができなかった。組織は彼をコンサルタントとして雇用した。彼は 1 週間に 2 日働くために州を越えて出勤し、そして１週間に３日在宅勤務をした。彼は不満であった、一旦、契約社員になると、組織は、当然と思っていた利益を提供しなかった。そして、関係は悪化し続けた。ついに、組織は、彼の雇用がおよそ１か月後に終了されると彼に伝えた。

1 週間半後、インサイダーは、家からリモートによりログインし、他の人が開発したソフトウェアとともに自分の開発したソフトウェアを削除し、自分の行為を隠蔽するためにシステム・ログを改ざんし、その直後に、ルートパスワード（サーバー管理者用パスワード）を変更した。それから、彼は、電話会談に参加したが、何をしたかについては決して言及しなかった。電話会談が終了した後、彼は、再び自分の行為を隠蔽するためにログインに問題があると報告した。その日の終わりに、彼は、辞任すると伝えた。この行為は、組織に 230 人時間及び関連経費を含み２万 5,０００ドル以上の犠牲を払わせた。

⑾　実践事例１１：システムの変更管理を実行しなさい。（更新）

システム及びアプリケーションの変更は、バックドア、キーロガー、ロジボム、及びその他の悪意のあるコード又はプログラムの挿入を防止するために管理されなければならない。

何をなすべきか。

管理（controls）とは、情報及び情報サービスを保証し、そして、技術使用に関連したリスクを軽減するのを手助けするプロセスである。変更管理（Change Controls）とは、コンピュータ及びネットワークシステムで行われた全ての変更の正確性、完全性、認証、及びドキュメンテーションを保証するプロセスである[15]。組織のシステムに無許可の改ざんを行う多種多様なインサイダーの侵害行為は、より強力な変更管理の必要性を示唆している。これを支援するために、組織は、ソフトウェアとハードウェアの基準となる環境設定（ベースライン・コンフィギュレーション）を特定しなければならない。異なるユーザー（例：会計係、管理者、プログラマー、受付係）には、異なるコンピュータの使用と情報が必要であることを考え合わせると、組織は幾つかの基準となる環境設定が必要である。従って、環境設定が特定されたならば、組織は、これらの環境設定を構成するようにハードウェアとソフトウェアの特性を定めなければならない。

この特性化（characterization）は、インストールされたソフトウェア、ハードウェア装置、及びディスクの利用バージョンのように情報を追跡する情報の基本的なカタログである。しかし、この様な基本的な特性化は容易に破られるので、より包括的な特性化が必要となる。これらの特性化は次のとおりである。

- 暗号チェックサム（例えば、SHA-1 又は MD5 の使用）
- 界面キャラクタリゼーション（例えば、（メモリマッピング、装置選択、及びシリアルナンバーなど）
- 記録されたコンフィギュレーションファイル

一旦、この情報が捉えられたら、それぞれの環境設定を実行しているコンピュータは、基準となるコピーとそれを比較して認証することができる。それから、それらに不一致があれば、彼らが、良性か、あるいは悪性かを判断するために調査が行われる。これらの技法を使うことにより、システムファイルの変更又は悪性コードの追加は調査の対象となるであろう。

このプロセスを一部自動化し、コンピュータ・システム全体を捜索するファイル整合性システム（file integrity checkers）と呼ばれるツールが存在する[16]。

---

15 内部監査人協会(Institute of Internal Auditors)の情報技術管理(Information Technology Controls)を参照されたい。http://www.theiia.org/download.cfm?file=70284.

16 次ぎのURLを参照されたい。 http://www.sans.org/resources/idfaq/integrity_checker.php for a discussion of file integrity checkers.

コンピュータの環境設定は長い間不変のままではない。従って、特性化と検証は組織の変更管理プロセスの一部でなければならない。組織内では、誰も他人に気づかれずに変更ができないようにするために、このプロセスでは、異なる役割が定義され、異なる個人によって実行されなければならない。例えば、悪意のある変更（ロジボムを仕掛けることを含む）を探知し、修正する機会ができるように、環境設定の検証は、変更した者以外の人物が実施しなければならない。

変更ログとバックアップは保護される必要がある。そうすれば、無許可の変更は探知され、そして、必要なら、システムを以前の有効な状態に戻すことができる。さらに、CERT のデータベースの事例によると、一部のインサイダーは、自分達の行為を隠すために又は自分達の行為を他人に濡れ衣を着せるために変更ログを改ざんした。

多くの組織は、アンチウイルスソフト及びホストファイアウオール又はネットワークファイアウオールを使用して、悪性コードから防御している。これらの防御は、外部からの侵害に対しては有効であるが、彼らの価値は、次の２つの重要な点で悪意のあるインサイダーの攻撃を防止するのには限界がある。彼らは、新しい又は奇抜な悪性コード（インサイダーによって仕掛けられたロジボムを含む）には効果がなく、さらに、彼らは、機械に直接インストールされたものより、主として、ネットワーク・インターフェース全体に拡がった不具合に関心を持っている。変更管理はこれらの周辺防御の限界への取り組みを支援する。

ちょうど、システム変更を探知･制御するためにツールが実装できるように、ソースコード及びアプリケーションの変更を探知･制御するための環境設定管理ツールが実装されるべきである。実践事例９で記述したように、一部のインサイダーは、彼らの攻撃を実行するためにソースコードを改ざんした。これらの改ざんが、初期実装の間でなく、ソフトウェア開発ライフサイクルの維持段階に行われたことに注意すべきである。一部の組織では、新しいシステムの初期開発段階の間、コードレビューと環境設定管理システムを含む非常に厳しい環境設定管理規制を設けているように見えるが、一旦、システムが製造され、開発が安定すると、組織は、規制を緩めているように見える。そして、強固な動機を持ち、倫理観が欠如した技術的に優れたインサイダーが、悪用することができる脆弱性がそのままになっている。

事例研究：これらが行われなかった場合、何がおこるであろうか。

製造会社のシステム・アドミニストレーターは、機械工として入社した。１０年を経て、インサイダーは重要な製造プロセスをサポートする会社のネットワークを創り、そのネットワークに関するシステム管理に対する唯一の権限を保有していた。結局、彼の会社は拡大し、事務所と工場を全米かつ全世界に開設した。インサイダーは、

・会社における責任の重要性が軽減されるにつれ不満を感じ始めた。
・同僚に口論や暴行を始めた。
・担当していないプロジェクトを妨害した。
・同僚の顔をつぶすために欠陥のあるプログラムをロードした。

彼は、口頭注意と２度の書面による注意を受けて、降格となり、最終的に解雇された。数週間後、ロジボムが会社のネットワークで爆発し、会社のサーバーから最重要な製造プログラムを削除した。損害の見積額は１,０００万ドルを超え、８０人をレイオフするに至った。調査により、インサイダーは退職前の勤務時間外に３回ロジボムを試験していたことが分かった。

悪性コードを探知するための慣行が実施されていたならば、時限式で発動された新しいプログラムを探知していたであろう。システムレベルのプログラムのインストールは２人で実施するというルールを有する変更管理手順と特性化手順は、最初のシステムベースラインと異なる新しいシステムファイルを探知できたであろう。

もう１つの事例では、組織は、ソフトウェアに自動モニター機能を組み入れた。そして、それは、データベースに保管された情報を改ざんするために、高度に使用制限されたスクリーンが使用されたときは何時でも自動通告をセキュリティ担当官へ送ることになっていた。役割基盤のアクセス管理によって、このスクリーンへのアクセスは、少数の特権的ユーザーに制限されていた。自動通告システムは、違法なデータ改ざんに対する防御の第２層を提供した。

しかし、アプリケーションの開発者が偶然アクセスした機能によって、自動通告が送られないようにコードが修正された。それから、彼は、雇用主から多額の金を窃取するためにその機能を使うようになった。

興味深いことに、組織はソフトウェア変更に備え、環境設定管理システムを導入していた。それにより、プログラムがコンパイルされた時、どのファイルが、どのコンピュータ・アカウントからコンパイルされたかを記録したレポートが作成された。また、レポートには、追加された、変更された、又は削除されたモジュールが記載された。しかし、不幸なことに、このレポートは監視されていなかった。そのため、アプリケーションの変更が、詐欺が行われてから１年半以上探知されなかった。それが監視されていたならば、又は環境設定管理システムにより新しい版のソフトウェアをインストールする時に二人ルールが強制されていたならば、セキュリティ通告の除去は探知され、インサイダーは詐欺を犯すことはできなかったであろう。

最近の調査結果

幾つかの最近の事例は、キーロガーを使用した情報の窃盗に関連していた。キーロガーは、コンピュータ・システムへのキーストロークを正確に記録するハードウェア又はソフトウェア装置である。キーロガーは、悪意を持って組織の機密情報、個人のプライベート情報、さらに最悪の場合はパスワード又は暗号鍵を取得するために使用することができる。

ある事例では、支払遅延を理由に契約を無効にする会社の慣行に憤慨した保険会社の苦情・損害賠償担当マネージャーは、最高責任者の秘書のコンピュータにハードウェア・キーロガー装置を設置した。役員の事務所にはアクセスができなかったが、秘書と役員の間で豊富な機密情報がやり取りされていると気が付いていた。さらに、秘書の机は、役員の事務室の様に物理的に安全が確保されていなかった。インサイダーは、秘書のコンピュータから機密情報を収集するためにキーロガーを使用した。そして、その情報を組織に対抗する訴訟を担当している弁護団へ送った。

別の事例では、ソフトウェア・キーロガーが関連していた。その中の１つの事例は、２人のインサイダーは、会社の知的所有権を収集するために外部の人間と共謀し、そして、それを競争者へ渡した。外部の協力者は、インサイダーの１人にウイルスを感染させた添付ファイルの付いた電子メールを送った。インサイダーは故意に感染した添付ファイルをダブルクリックした。それは会社のコンピュータ・ネットワークの装置にキーロガーをインストールし始めた。キーロガーは定期的に機密情報を競争者へ送った。競争者は、犠牲となった組織から顧客を奪うためにそれを使用した。

組織に対する不満を発散させるためのロジックボムの使用は、最近の事例でも続いている。ロジボムは、信用組合の５万以上のアカウントの金銭的記録の削除及び健康管理解決組織の患者と特定薬物の相互作用争議のデータベースを消去するために使用された。別の事例では、単に、インサイダーの後任者の顔をつぶすためにロジボムを爆発させた。

契約社員のシステム・アドミニストレーターは、艦船、潜水艦、及び水中の障害物の位置を追跡して、表示するために用いられるコンピュータ・システムの毎日の活動を監督するという契約を失った。インサイダーは５つのサーバーにロジボムを植え付け、そして、それらが、彼が退職してずっと後に爆発するように設定した。５つのうち３つは爆発し、他の２つは、発見されて無力化された。

一部のインサイダーは、システムを妨害するために、より簡単な方法を選んだ。彼らは、組織が頼みにしていたソフトウェアを簡単に削除した。組織が、システム環境設定又はプログラムの無許可の変更を監査するとともにシステム・ログを保護していれば、

その変更に責任のある個人を特定することができる。しかし、不幸なことに、保護されていないログは、しばしば、高度な技術を持ったインサイダーの標的となっている。

⑿　実践事例１２：従業員のオンライン操作をログ・監視・監査しなさい。（更新）

ログ・監視・監査は、不審なインサイダー活動の早期発見と調査に結びつけることができる。

何をなすべきか。

アカウント及びパスワードの方針及び手順が整備され、かつ実行されているならば、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従業員を明確に結びつけることができる。ログ・監視・監査は、組織により重大な結果が起こる前に、不審なインサイダー行為を発見し、調査する機会を提供する。

金融界における監査は、財務情報の検査と検証を意味する。技術的セキュリティ分野における監査は、様々なネットワーク、システム、及びアプリケーションログ又はデータの検査と検証を意味する。インサイダー脅威を防止又は探知するために、監査には、組織の最重要な資産の調査・検証することが含まれていることが重要である[17]。さらに、監査は、ログされたアクセスの合法性と同様に完全性についても調査し、検証しなければならない。

事前に定義されたビジネスルールを順守しない不審な処理について、手動の調査の必要性を知らせる自動化された完全性チェック機能が考慮されるべきである。インサイダー脅威は、ほとんどの場合、自動ログ、手動の監視、又は監査の組合せによって探知される。例えば、コンピュータ・アカウント設定ログの完全性チェック機能は、アカウントが合法的なシステムユーザーと関連付けられ、かつユーザーがアカウントの存在を認識している手動検証と組み合わさった自動化ログと係わっている。

自動化ツールは、典型的なバックドア・アカウントの設定を探知できる。（システム・アドミニストレーター・アカウントは現従業員とは関連していない。）しかし、残念なことに、バックドア・アカウントの探知は完全には自動化されていない。例えば、１人のインサイダーは、３人の合法的な現従業員の VPN （Virtual Private Network：仮想

17 多くのリスク管理方法論は最重要な資産の保護を基礎としている。例えば、セキュリティのために OCTAVE（Operationally Critical Threat, Asset, and Vulnerability Evaluation：運用上の重大な脅威、資産、及び脆弱性評価） リスク基盤の戦略的評価及び計画立案技法を参照されたい。：http://www.cert.org/octave/.

プライベートネットワーク）アカウントを設定したが、彼らには決してアカウントが設定されたことは話さなかった。解雇された後、彼は２週間の間、夜間にリモート・アクセスを得るために、これらのバックドア・アカウントを使用した。彼は、リモート・アクセスを見張るためにネットワーク監視要員として特別に雇用された契約社員の目の前で、この２週間の間に攻撃のための綿密な準備をした。

同様に、データ監査は、例えば、電子データの改ざん履歴と紙記録を比較するような、又は不審な不一致のある電子記録を調査するような手動プロセスであった。

監査は、継続と無作為の両方で行わなければならない。監視と監査が定期的かつ継続したプロセスであり、それに責任を有する個人の高い優先事項であることを従業員が知っていれば、インサイダー行為の抑止力として機能するであろう。例えば、不満を持ったシステム・アドミニストレーターが、全ての新しいコンピュータ・アカウントが頻繁に調査されていることを知っていれば、彼又は彼女が、後で悪用するためにバックドアアカウントを設定することはありそうもない。

他方、金融機関においてすべての金融取引を毎日監視することは多分実際的でない。毎月及び四半期の監査は、インサイダーに対する防御の一つの層を提供するが、それは、また、インサイダーが詐欺犯罪を長い期間探知されないように計画する基となる予想サイクルを提供する。対象従業員の全ての取引のランダムな監査は、インサイダーが熟慮した攻撃を開始するのを思いとどまらせるためにちょうど十分な予測不能性をプロセスに加えることができる。

最後に、ＣＥＲＴ資料の事例では、２人のインサイダーが、仕事中に彼らのコンピュータから他の外部組織を攻撃した。結果として、組織が実施しなければならなかったフォレンジック（電子捜査）と調査活動は、スタッフと事業運営に非常に悪影響を及ぼした。

事例研究：これらが行われなかった場合、何がおこるであろうか。

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がついた。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リ

モート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。

もう１つのインサイダー攻撃では、監査の不足がインサイダーの攻撃を許した。その攻撃は、技術的には洗練されていなかったが、彼は２年間にわたって約２６万ドルを彼の雇用主から窃取することができた。インサイダーは倉庫のマネージャーであった。攻撃は次のように行われた。

- インサイダーは、監督者に倉庫の全購買システムへの特権的アクセスが必要であることを納得させた。
- 次に、偽のベンダーを倉庫の許可された供給者リストに追加した。
- ２年間にわたり、７８件の購入注文を入力した。供給品はけして受取らなかったが、彼はベンダーへの支払を許可した。

このインサイダーは承認制度を知っていた。そした、全ての彼の詐欺的購入（額）は独自承認の限度額より下であった。ベンダーの銀行口座は、たまたま、インサイダーの妻のものであった。詐欺は、購入注文の１つに関連した文書業務の不規則性に気がついた会計係によって、偶然に発見された。この詐欺は、特権的ユーザーのオンライン操作の綿密な監視によって、より早く探知することができたであろう。何故ならば、この特定のユーザーが異常に広範囲な特権的アクセスを有していたからである。さらに、通常の監査手順でも新しいベンダーを確認することができ、そして自動完全性チェック機能は倉庫目録と購買記録の間の不一致を見つけることができたであろう。

最近の調査結果

ビジネス上の利益のための窃盗の２４件の事例のほぼ全てにおいて、インサイダーは、窃盗の前後に退職した。窃盗のおよそ３分の２は、インサイダーの退職の３週間以内に行われ、半数以上は、すぐに情報を窃取した。ある事例では、インサイダーは、競合組織に勤めることを承諾し、退職を申し出て、退職の最後の日までに、彼は新しい会社に持っていくために専有情報のダウンロードを行った。新しい仕事にいかなる専有情報も持って行ってはいけないという雇用主の警告にもかかわらず、彼は情報を窃取した。窃盗について質問されると、情報をダウンロードしたことを認め新しい仕事を始める時はそれを使いたかったと述べた。

同様な事例では、インサイダーは新しい仕事を承諾した翌日に、企業秘密の入っている文書のダウンロードを開始した。数週間後、何回かの大量のダウンロードの後、インサイダーは会社を去り、競合会社で働き始めた。新しい仕事を始めて丁度２日後、イン

サイダーは盗んだファイルを彼の新しいラップトップにロードした。そして、１か月以内に彼は、電子メールで企業秘密を新しい同僚に送信した。このような窃盗を隠蔽するための技術的努力の欠如は、このタイプの犯罪の他の事例においても明らかであった。これは、オンライン操作、とりわけ、退職の前後の１ヵか月以内のダウンロードの監視が、専有情報の窃盗を防ぐか、あるいは早く探知するために特に有益であったことを示唆している。

窃盗事例では、情報を転送するために、電子メール、電話、ファックス、インターネットからのダウンロード、悪性コードでの収集及び送信、並びに組織のプリンターでの資料の印刷を含む多種多様な技術的手段が使われていた。ある特に復讐心に燃えたインサイダーは、低レベルの従業員が僅かな昇給をもらうか、あるいは解雇される一方で、過大なボーナスをもらう経営陣に対する怒りから行動した。彼は、彼の自宅のパソコンに会社の機密文書をダウンロードし、オフィスからコピーを持ち出し、そして、それらを２人の競争者に電子メールで送り始めた。２人の競争者のどちらも、企業秘密の情報を欲しがっていなかった。そして、両名とも受け取った情報を組織へ送り返した。このインサイダーは、彼の違法な活動を隠そうとも又は否定しようともしなかった。その他の最近のケースでは、同様に、大きなファイルを、彼らの自宅のコンピュータ又は競合企業へ電子メールで送信した現従業員が関係していた。

機密情報の窃盗を監視している組織は、情報が窃取される多種多様な方法を検討して、探知対策をカスタマイズする必要がある。次の機能の実行を可能とする幾つかのデータ漏洩（探知及び防止）ツールが利用できる。

- 異常に大きな添付ファイル付き電子メールをシステム・アドミニストレーターに警告する。
- ネットワークから発信されることが認められない文書にタグを付ける。
- 例えば、個人情報又は新しい製品のコードネームのようなある種の言葉などを含む特定の情報の印刷、コピー、又はダウンロードを追跡又は防止する。
- リムーバブル・メディアへコピーされた全文書の追跡。
- 競争者、米国外、G メール（google のメールサービス）、又はホットメール（MSN のメールサービス）アカウントへの電子メールの発信を防止又は探知する。

多くの窃盗事例では、インサイダーは、彼らの専門外又は責任外の情報をダウンロードしている。組織が、各々の従業員が彼らの仕事を達成するためにどんな情報を必要とするかについて追跡するならば、それは組織に疑わしい行動を探知する手段を提供するかもしれない。役割基盤のアクセス管理は、そのような追跡の基盤を提供するかもしれない。

最後に、組織は、インサイダーが他の組織（多分、以前の雇用主）を、組織のシステムを使って攻撃するという可能性を認識していなければならない。一般的ではないが、その様な犯罪が起こりうる。CERT 資料には２，３のその様な事例が存在する。組織は、その様な事例が引き起こす責任と混乱を考慮する必要がある。

インサイダーによる現雇用主のシステムからの元雇用主に対する攻撃が、現雇用主の転落の大きな要因ともなり得る。インサイダーは、攻撃は、彼への悪行に対する現雇用主と会社への報復であると主張した。現雇用主は、攻撃との関係を否定したが、インサイダーの行為の結果により大きな損害を被った。FBI の捜査官は事務所を取り囲み、従業員に対し、一時仕事を止め、会社のデータやファイルに手を付けるなと命じた。インサイダーは、パニックに陥り、潜在的証拠の大量消去を開始した。インサイダーは、コンピュータへの不正侵入（コンピュータハッキング）の罪で５年及び司法妨害の罪で２０年の刑を受けた。

⑬ 実践事例１３：リモート攻撃に対して多層防衛を構築しなさい。（更新）

リモート・アクセスは、少ないリスクで攻撃できる魅力的な機会をインサイダーに提供する。

インサイダーは、それが、誰かが悪意のある行為を物理的に観察することができる関係を除去するので、ホームからの悪意のある活動を導くほうが簡単であることを認めました。

何をなすべきか。

インサイダーは、しばしば、組織から提供された合法的なアクセスを使用して又は退職後に、組織に対してリモート攻撃を行う。リモート・アクセスは、従業員の生産性を大きく向上させることができるが、最重要なデータ、プロセス、又は情報システムへのリモート・アクセスを提供する際には注意が必要である。インサイダーは、誰からも悪意のある行為を物理的に監視される心配がないので自宅から悪意のある行為を実行するほうがより簡単であることを知っている。

リモート・アクセスを許すこと自体に固有の脆弱性が存在することは、リモート攻撃に対して多層防衛が構築されなければならないことを示唆している。組織は、リモート・アクセスを電子メールと重要でないデータに提供するかもしれないが、最重要なデータと機能へのリモート・アクセスを制限すること、そして、組織によって管理された装置からのアクセスだけに制限することを強く考慮しなければならない。企業に大きな損害を与えるデータ又は機能へのアクセスは、できる限り物理的に職場内に位置する従業員に限定しなければならない。リモート・システム・アドミニストレーター・アクセスは、

完全に禁止できないならば、できるだけ最も小さなグループに限定されなければならない。

最重要なデータ、プロセス、及び情報システムへのリモート・アクセスが必要である場合は、組織は、それにより追加されたリスクを、リモート処理の綿密なログと頻繁な監査によって相殺しなければならない。会社の装置からだけのリモート・アクセスを許可することは、彼らの情報とネットワークへのアクセスを管理し、遠隔地で働く従業員の活動を監視する組織の能力を強化する。ログイン・アカウント、接続日／時間、及び切断日・時間のような情報、並びに、IP アドレスは、すべてのリモートログインを知るためにログされなければならない。また、ログインが失敗した理由を含む失敗したリモートログインを監視することも有効である。最重要なデータへのリモート・アクセスの許可が最低限に保たれるならば、監視はより扱いやすくかつ効果的になるであろう。

リモート・アクセスの無力化は、しばしば見落とされ勝ちであるが、従業員の退職プロセスの重要な部分である。次のことを含む従業員の退職プロセスは極めて重要である。

- 企業所有の機器はどんなものでも回収する。
- リモートアクセス・アカウントを無能力化する。（例：VPN 及びダイアルイン・アカウント）
- ファイアウォール・アクセスを無能力化する。
- 全ての共有アカウントのパスワードを変更する。（システム・アドミニストレーター、データベース・アドミニストレーター（BDA）及びその他の優先的な共有アカウントを含む）
- 全てのオープンコネクションを閉鎖する。

リモートアクセス・ログ、ソース IP アドレス、及び電話記録の組み合わせは、リモート攻撃を行ったインサイダーを特定するのに有効である。侵入者のユーザネームは直接インサイダーを指すので、識別は単純明快である。もちろん、この情報の裏付けは必要である。何故ならば、侵入者が他のユーザーを陥れようとするか、他のユーザーのアカウントを用いて彼ら自身の犯罪から注意を遠ざけようとするか、又はさもなければ監視プロセスを細工したかも知れないからである。

事例研究：これらが行われなかった場合、何がおこるであろうか。

投資銀行の外貨トレーダーは、５年間に亘り、取引損失を銀行の大きな収益の増加のように見せるために、銀行の記録を“改ざん”した。彼の行為は、銀行の花形行員のうちの１人であるように見せさえさせた。そして、認められた業績により高額なボーナスをもらった。実際には、銀行は、数億ドルの損失を出し、さらに彼の行動の結果として、多くの否定的なメディアの注目を引いた。このインサイダーの詐欺行為の大部分は、最

初は仕事中に行われたが、彼は、次第に真夜中に自宅から違法な行為を実行するほうがより簡単であることに気づいた。何故ならば、誰かに肩越しに覗かれている心配がないからである。その結果、他のトレーダーが、詐欺的な行為について知るというリスクはかなり少なくなった。

インサイダー脅威スタディー[18]のインタビューにおいて、このインサイダーは、グループ処理（トレーダーのチームによる処理）のほうが、個々の処理より組織のリスクを軽減するのに有効であると語った。何故ならば、同じ口座で処理している複数のチームメンバーがいるほうが、違法又は疑わしい処理行為を見つけることがより簡単であるからである。この事例においては、孤立した処理は、リモート・アクセスの匿名性とともに、インサイダーが詐欺を継続する要因になった。

もう１つの事例は、政府組織で働く契約プログラマーに関連するものである。政府組織は、契約プログラマーのうちの１人に、開発中のシステムへのアクセスが禁止されること及び責任はテスト活動に限定されることを通知した。彼の抗議が拒否されたあと、プログラマーは退職した。それから、インサイダーは、開発中のシステムからソースコードとパスワードファイルをダウンロードするために、２週間に３回、アドミニストレーター特権（彼はおそらく、それを退職前にインストールした）を持つシステムへバックドアを使用した。異常に大きなリモートのダウンロードは、組織に警告を発した。そして、その事象は、調査（ダウンロードをインサイダーの自宅まで追跡）され、逮捕、起訴、そして懲役刑に終わった。この事例は、リモートアクセス・ログの油断のない監視と不審な行動に対する迅速な対応の価値を示している。

最近の調査結果

遠隔地からの侵害の事例は、CERT の以前の研究と同じように最近の事例でも継続されている。これらの事例の一部には、インサイダーの自宅装置からの侵害が含まれている。しかし、幾つかの最近の侵害は、インサイダーの自宅からでなく、組織の管理下にないリモート装置から、例えば、競合会社の装置から、インサイダーの退職時に無効化されるべきであったアクセスを使用して行われている。これらの事例の１つでは、インサイダーは、組織のシステムに接続するために、PC Anywhere(リモートシステムをコントロールできるツール)を使用した。そして、全てのデータ（電子メール、販売記録、取引文書、秘密保持契約、専有技術情報、及びバックアップのデータ）を削除した。彼は、以前にシステム・アドミニストレーターであったときに、PC Anywhere を準備した。こ

---

18 インサイダー脅威スタディー：『銀行及び金融分野における不法なサイバー活動』
http://www.cert.org/archive/pdf/bankfin040820.pdf

の特殊な攻撃は、組織の転落の大きな要因であった考えられている。リモート・アドミニストレーション・ツールを使用するリモート・アクセスを無効化することは、退職プロセスの一部である。

以前の研究にあるように、リモート・アクセスに関連した幾つかの最近の事例は、退職後に、特定の人に損害を与えることを意図した IT サボタージュ犯罪に関連している。そのような事例の１つでは、解雇された従業員は、元の雇用主のシステムに接続し、従業員の補償に関連した約 1,000 件のファイルを削除した。彼は、彼の求愛を拒否した職場の女性従業員を陥れようと、給料の４万ドルの増加と１０万ドルのボーナスをもたらすよう彼女の記録を改ざんした。さらに女性を陥れるために、彼は、女性従業員の名字を含んだアカウントから、上級マネージャーに電子メールを送信した。電子メールには削除されたファイルの抜粋を含んだ添付ファイルが付けられていた。

⑭　実践事例１４：従業員の退職後に、コンピュータアクセスを無効化しなさい。（更新）

退職した従業員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は重要である。

何をなすべきか。

インサイダーは、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、及びデータへの合法的なアクセスを持っている。しかし、一旦、退職したならば、その退職した従業員（インサイダー）が利用できるすべてのアクセスポイントを無効化する厳しい退職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、違法な無許可のユーザーによるアクセスに対して脆弱となる。一部の組織は、良好な状況での退職であるならば、元従業員に若干の期間、継続的なアクセスを許可することを選択する。：このためには、組織がこれらに関する正式な方針を有していること、かつ潜在的リスクを慎重に考慮することが重要である。さらに、組織内で地位が変更した従業員のアクセスを管理することは重要である。（例えば、従業員から契約社員へ変更、常勤からパートタイムへ変更、又は休暇中であるなど）

正しい退職方針と手順が履行されていないならば、退職プロセスは、その場限りとなり、１つ以上のアクセスポイントが見落とされるなどかなりのリスクをもたらすであろう。インサイダー脅威スタディーによると、インサイダーは、退職プロセスで見逃された不明瞭なアクセス方法を悪用するかなりの才覚があることを示している。正式な退職プロセスが存在するならば、それが厳しく履行されなければならない。組織は新しいインサイダーの脅威を研究し続けるとともに、定期的にこれらのプロセスを見直し、更新することも重要である。退職の時点で、組織が厳格なアカウント管理方針に従っていなければ、退職した従業員のアカウント監査を実行しても間に合わないであろう。バック

ドア・アカウントは退職の数か月前に設定できるので、全ての種類の全てのアカウント（システム・ログイン・アカウント、VPN アカウント、データベースアカウント、アプリケーション・アカウント、電子メール・アカウントなど）の合法性を検証することは、組織の規模によっては、非常に時間のかかるプロセスとなるであろう。従業員が退職する時、組織は自信をもって、その従業員が利用できるすべてのアクセス経路を無効化したと言うことができなければならない。

退職プロセスの幾つかの側面は極めて明白である。例えば、退職した従業員のコンピュータ・アカントを無効化することである。しかし、インサイダー攻撃の犠牲となった組織のアカウント管理手順は、貧弱か、存在しないか、又は包括的でなく脆弱であった。多くの従業員は、複数のアカウントへのアクセスを有している。従業員が退職した時、全てのアクセスを直に無効化できるように、全てのアカウントの設定は追跡され、かつ定期的に調査されなければならない。

構成が各々に対してパスワードを持ち、従業員が終了する場合にそれらのアカウントを変更することを認められた、すべての共有されるアカウントおよびすべてのユーザのレコードを小心に維持することは重要です。

退職プロセスにおいて、時々、見落とされるアカウントは、例えば、システム・アドミニストレーター・アカウント、データベース・アドミニストレーター（DBA）アカウント、テストアカウント、訓練アカウント、及びベンダー・アカウントのような外部組織用アカウントなどの共有アカウントである。さらに、若干のアプリケーションは、複数のユーザーの間でしばしば共有される管理用アカウントを必要とする。組織があらゆる共有アカウントの記録及びパスワードの保有が許可されたあらゆるユーザーの記録を保持すること、そして従業員が退職する時にこれらのアカウントを変更することが重要である。

さらに、退職時に従業員によって開かれたどんなリモート接続も、すぐに閉鎖されなければならない。従業員が敵意を持って退職したならば、組織は、システムへのアクセスを許すかもしれないソフトウェア又はアプリケーションがインストールされていないことを確認するために、従業員の使用していたデスクトップコンピュータとシステム・ログの調査を実施しなければならない。ある事例では、退職した従業員は、彼のデスクトップの中にソフトウェアを残置した。そのソフトウェアは、デスクトップへのアクセスとリモートコントロールができ、そして次の雇用主（next employer）への攻撃のできるものであった。付言すれば、少数のインサイダーは、退職する直前に組織の知的所有権を窃取したが、彼らのデスクトップコンピュータの使用ログが分析され、逮捕された。

要約すると、すべてのアクセス方式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。リモート・アクセスは無効化されなければならないが、不明瞭なリモート・アクセス方式が見落とされたならば、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､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、又はパスワードが変更されていることが重要である。また、退職したインサイダーが、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。

最後に、退職手順には、物理的アクセスを防止するためのステップが含まれなければならない。インサイダーは、元雇用主のシステムにアクセスするために、物理的アクセスを利用した。鍵、ID カード、及び駐車許可証によるアクセス、並びにカード・コントロールシステムのある施設へのアクセスを無効化するために慎重な注意が払われなければならない。従業員が解雇された時に、他の従業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、共連れ（ピギーバッキング）によって組織への物理的アクセスを得ることができ、そして多様なインサイダー攻撃が容易に実行された例がある。

事例研究：これらが行われなかった場合、何がおこるであろうか。

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突然解雇された。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、後任がファイアウオ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、彼女（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。そのサーバーは、以前から問題があり、事実、先週末に機能を停止した。（そして、彼はそれを再び立ち上げるのに週末の全部を使った。）信用組合は、サーバーを正常に戻すのに３日を要した。その期間、顧客は誰も、どんな形であれ彼ら自身のアカウントにアクセスすることができなかった。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。

別の場合(ある午前ログインされたシステム管理者)に、また彼女の最後のログインが 1

時間前に元あった彼女の業務に書かれたログイン・ソフトウェアによって通知されました。

彼女は、以前は標準シェル履歴ファイルではなくユニークなファイルへの彼女のアカウントによるアクションのロギングを転送するステップを取りました。

もう１つの事例では、システム・アドミニストレーターは、ある朝ログインしたところ、彼女の特注したログインソフトウェアによって、彼女の最後のログインが 1 時間前にあったと通告された。彼女は、数日間、実際にログインしていなかったので、即座に警報を作動させた。彼女は、標準的なシェル（ユーザーからのコマンド入力を受け付け、解釈するプログラム）履歴ファイルよりむしろユニークなファイルによって彼女のアカウントの操作履歴を記録するよう処置をとっていた。従って、彼女は、侵入者のステップを追跡することができ、そして侵入者が彼女のアカウントを使って、もう１人の従業員の電子メールを読んでいるのを発見した。そして、侵入者は、操作履歴が残らないよう、アカウントの標準的な履歴ファイルを削除していた。ログインは、子会社のコンピュータまで追跡された。さらなる調査で、同じコンピュータは、前月も会社のシステムに定期的にログインしていることが明らかになった。調査により、元従業員が勤務時間内に毎日、元雇用主のシステムに最高１６回にアクセスしたことが明らかになった。このインサイダーは、

・少なくとも２４個のユーザー・アカウントにアクセスしていた。
・電子メールを読んでいた。
・彼の以前のプロジェクトのソースコードを調査した。
・そのプロジェクトの２つのソフトウェア改修通告（modification notices）を削除した。

この元従業員は、業績不良のために解雇された後、子会社で働いていた。この事例は、元従業員のアクセスを完全に無効化すること、退職後のアクセスを慎重に監視することや、退職した技術系従業員には、特別の注意を払うことの重要性を示している。

最近の調査結果

最近の事例によると、組織は、退職した従業員のアクセスを完全に無効化することが困難であると感じていることが明らかになった。次の事例で示されるように、多くの一般に認められた、最善の実践事例（ベスト・プラクティス）は、未だ実行されていない。IT サボタージュに加えて、雇用主は、その情報を使用するか、売却するか、又は単純に好奇心から、組織の知的所有権へアクセスしようとする元従業員に対して関心を持つ必要がある。

ある最近の事例では、金融市場情報出版業者の技術担当の副社長は、５年間に亘る組織との意見の不一致の後、解雇された。彼は、会社のコンピュータ・ネットワークと内部の電子メールシステムを監督していた。解雇の３年後に、彼は、従業員の仕事状況に関する役員の電子メールを盗み見るために、旧会社の電子メールシステムにアクセスした。

このインサイダーは５か月にわたり、自宅から電子メールのやり取りをスパイした。彼は、どの従業員が解雇されるかに関心があった。人事部長と役員との間で従業員の解雇についてやり取りした電子メールを傍受した。インサイダーは、それらの従業員に解雇の可能性を知らせた。電子メールを受け取った従業員は、監督者に通知した。監督者は、調査を開始した。調査によって、組織のユーザー名やパスワードが実質的に３年間変更されていないことが判明した。

⑮　実践事例１５：安全なバックアップと回復プロセスを履行しなさい。（更新）

組織が講じた予防措置にもかかわらず、インサイダーは、攻撃を成功させる可能性がある。従って、組織がその可能性に備えて、定期的にテストされた安全なバックアップと回復プロセスを履行することによって組織の弾力性を強化することは重要である。

何をなすべきか。

インサイダー攻撃の防止は、防御の第一線である。しかし、経験は、決意の固いインサイダーには成功裏にシステムを侵害する手段が常にあることを教えている。効果的なバックアップと回復プロセスが準備され、かつ運用されている必要がある。そうすれば、侵害が発生した場合でも、最少の中断で事業活動を継続することができる。我々の研究によれば、効果的バックアップと回復の仕組みで次のような差が生じることが明らかである。

- バックアップにより、システムを正常運用に戻すための数時間の運用中断
- 現行のバックアップが利用できない場合、何週間にも及ぶ手動データ入力
- バックアップコピーが存在しなかった場合、数ヶ月又は数年に及ぶ情報の再構築

バックアップ及び回復戦略では、次を考慮しなければならない。

- バックアップが保管されている施設への管理されたアクセス
- 物理的メディア（例えば、誰も、オンラインデータ及び物理的バックアップメディア双方にアクセスすべきでない）への管理されたアクセス
- バックアッププロセスを変更する際の“任務の分離”及び“二人ルール”の実行

さらに、バックアップメディアの遠隔保管を含むバックアップのサービスを提供する

責任を有するどんな第三者のベンダーにも、法的・契約上の説明責任と完全な開示が要求されなければならない。そして、要求された回復期間、誰が保管中のメディアにアクセスするのか、物理的メディアが遠隔地に輸送中は誰がアクセスするのかが、サービスレベルの協定に明確に記載されていなければならない。また、本報告の幾つかの事例は、信頼されたパートナー組織の従業員によってもたらされる脅威を示している。それらの脅威のための軽減戦略は、バックアップサービスプロバイダにも適用されなければならない。

可能であるならば、遠隔地の安全な施設に保管された余剰のコピーとともに、バックアップの複数のコピーが存在しなければならない。様々な人々が各々のコピーの保管に対して責任を持たなければならない。そうすれば、バックアップ手段を侵害するためには複数の個人の協力が必要となる。特に、余剰のコピーが、第三者のベンダーによって遠隔地の安全な施設で保管されている場合、バックアップ保護のレベルを上げるためには、暗号化が必要である。暗号化は保護のさらなるレベルを提供するが、それは更なるリスクを伴う。暗号化キーを管理するときは、“２人ルール”を常に守られなければならない。そうすれば、情報のバックアップに責任を有する従業員が組織を去る場合でも、あなたは解読プロセスを常に管理することができる。システム・アドミニストレーターは、バックアップが保存されている物理的メディアをインサイダーの不正行為または破壊から保護するために適切な処置を講じなければならない。我々の研究によるインサイダー事例では、次の攻撃が行われた。

- バックアップを削除した。
- バックアップメディアを盗んだ。（ある事例では遠隔地のバックアップを）
- バックアップシステムの欠点によりシステムを回復することのできない行動を実行した。

サボタージュ攻撃を受けた組織はバックアップ対策を策定したが、一部のシステム・アドミニストレーターは、まず初めの段階でバックアップの機能確認を怠った。このような行動は、回復の唯一の手段を失うことになり攻撃による組織への否定的な影響を拡大させた。インサイダー攻撃から防護するために、組織は次のことを実行しなければならない。

- バックアップの機能確認を行い、かつ定期的にテストする。
- メディアとコンテンツを改ざん、窃盗、又は破壊から保護する。
- “任務の分離”と環境設定（コンフィギュレーション）管理手順をバックアップシステムに適用する。
- バックアップのプロセス及び物理的メディアを保護するために“2 人ルール”を適用する。そうすれば、他のもう一人の知識と承認がなければ、一人では行動が起こせない。

残念なことに、一部のネットワークへの攻撃は、通信方式に干渉するかもしれない。そして、それは、攻撃からの回復を含む組織的活動に不確実性や混乱を増大させる。これがインサイダー攻撃の真実である。何故なら、インサイダーは組織の通信方式を熟知しており、そして、攻撃の間、組織のデータ回復プロセスにとって必須の通信を妨害するからである。ネットワーク機能停止の場合に、最重要な業務を遂行するのに十分な容量を持った信頼できる通信経路を、ネッワークの外に維持することによって、組織は、この影響を軽減することができる。この種の保護対策には、２つの利点がある。ネットワークに対する攻撃の被害を軽減することができる。そして、インサイダーは、効果が少ないためにネットワークの結合性（connectivity）への攻撃を行わないであろう。

事例研究：これらが行われなかった場合、何がおこるであろうか。

最重要な資産の集中化とバックアップに対するサボタージュは、一部のインサイダーに、余剰コピーと回復の手段を排除することによって、攻撃の影響を拡大することを可能にさせた。あるインサイダー（たった１人のシステム・アドミニストレーター）は、管理者を説得し、１つのサーバーに会社の重大な製造プログラム全ての唯一のコピーを集中した。そのサーバーは、後で、同じインサイダーが作成したロジボムの標的であった。攻撃から回復するために、他のソフトウェアのコピーは役に立たなかった。何故ならば、彼は、会社の方針に違反して、唯一のバックアップ・テープを、脅して手に入れていたからである。ロジボムは、会社のプログラムの全てを削除し、会社に数百万ドルの被害を与え、そして、全社的なレイオフを引き起こした。集中化は組織の効率に貢献するが、集中化したデータの損害又は損失した場合でも、ビジネスの継続が確保できるよう、バックアップ・テープが定期的に作成され、かつ保護されるよう十分に注意しなければならない。

もう１つの事例では、インサイダーは、リストラにより解雇された。会社は、適切な手順に従い、彼が事務所で所有物を片付ける間、それから建物を出るまで付き添った。IT スタッフも、インサイダーのリモート・アクセスを無効にして、パスワードを変更など会社のセキュリティ方針に従った。しかし、組織内の３人で共有していた 1 つのパスワードを見落とした。解雇されたインサイダーは、退職したその夜、システムへアクセスし､アカウントを使用して､そこで勤務している時に作成したプログラムを削除した。これらのプログラムの幾つかは、会社の重要なアプリケーションをサポートしていた。

削除されたファイルを、バックアップ・テープによって回復することに失敗した。インサイダーがバックアップ・テープに対して管理責任を持っていたが、会社の人々はバックアップ・テープが不当に破壊されているとは思わなかったので、バックアップ・テープは、重要なデータがきちんと記録されているかどうかをテストされていなかった。

その結果、北米と南米の組織の活動は２日間停止された。そして、8 万ドル以上の損失をもたらした。この事例は、バックアップ・テープが定期的にテストされていない場合、インサイダー攻撃の後の回復が遅延することを示している。

最近の調査結果

バックアップ及び回復プログラムを保有していないか、あるいはそれが不完全な組織は、インサイダー攻撃による破壊的な損害を被っている。ある最近の事例では、インサイダーは、突然に、そして、説明がなかったが明らかに財政的補償に関する意見の相違から、会社（インターネットサービスプロバイダ、以下、ISP）を辞めた。退職直後に、インサイダーは未払い賃金を要求したが、同社は支払いを拒否した。会社を訴えている間、インサイダーは、顧客インターネットサービスをサポートしている重要なソフトウェアをリモートで削除した。同社には回復のために利用できるバックアップがなかったため、削除されたソフトウェアを書き直す間、システムは３日間、機能停止した。会社の損失は合計およそ 12 万ドルになった。

他の最近の事例では、インサイダーは、個人及び法人顧客に有線及び無線でインターネットを提供する ISP で働いていた。そのサービスの一部として、組織は、州と州の間及び外国との商業・通信（コマース・コミュニケーション）サービスを提供していた。ISP は、無線タワーと顧客の無線アクセスポイントとの間に無線ラジオ(Wi-Fi)信号を使用していた。無線タワーとアクセスポイントは、組織の設備であるコンピュータによって運用されていた。

ビジネスと財政的問題で ISP を辞めたインサイダーは、直接的な競争業者のところに就職した。元雇用主のネットワークを攻撃するのに、アドミニストレーター・アカウントを使用し ISP のネットワーを支配した。インターネットサービスを切断するために、ISP の顧客のワイヤレスアクセスポイントのうちの 110 件を再プログラムした。彼は、無線タワーコンピュータで彼が書いたプログラム・コマンドを実行した。無線タワーコンピュータは、顧客のアクセスポイントにコマンドを送信した。そして、それは顧客がインターネットにアクセスするのを妨害した。切断されたサービスには、臓器提供者の知らせを電子メールに頼っていた 1 人の顧客のサービスが含まれていた。

残念なことに、ISP は、顧客設定へのリモート・アクセスの回復計画は考えていなかった。そのため、リモートによってネットワークを修復することができないため、ISP は、インターネットアクセスができなくなった加入者の下に技術者を送った。全ての顧客にサービスを提供するのに ISP には 3 週間を要した。そして、一部の顧客は、その期間インターネットにアクセスできなかった。インサイダー行為により、ISP のアクセスポイントは繰り返し無線信号を放送した。その信号は、他の ISP の信号と干渉した。

全体で、170 人以上の顧客（個人、家族、及び企業を含む）が、インターネットサービスを受けられなくなり、そのうちの一部は 3 週間の間、サービスを受けられなかった。そして、合計で、6 万 5,０００ドル以上の損害をもたらした。

⑯ 実践事例１６：インサイダー・インシデント対応計画を策定しなさい。（新規）

調査手順及び悪意のあるインサイダーへの対応は独特の挑戦である。；対応は、計画され、明確に文書化され、そして組織マネージャーと弁護士によって合意されていなければならない。

何をなすべきか。

インサイダー・インシデントに対する対応は、部外の攻撃者によるインシデントへの対応計画と異なる。組織は、インサイダーである犯人が、対応チームに割り当てられる、又はその対応計画の進み具合を知っているという可能性を最小にする必要がある。これは、挑戦的である。何故ならば、対応チームに割り当てられる技術者が、組織に対して技術力を悪用することができる最も多くの知識と能力をもっているからである。もう 1 つのインサイダー・インシデント対応の挑戦は、調査に参加するマネージャーが感じるかもしれない躊躇又は抵抗である。この躊躇には、いくつかの原因がある。ビジネスに不可欠なチームの資源を（対応チームへ）転用すること、対応チームメンバーをさらけだしてしまうこと、管理の欠陥又はシステムセキュリティ上のミスを暴露すること、そして、当惑と損失に対する責任を受け入れることである。

組織は、関係する人々の権利を念頭に入れながらインサイダー・インシデント対応計画を策定する必要がある。インサイダーによる損害を局限する具体的な活動は、状況に適合した適切な努力とともに特定されなければならない。計画には、一般的なプロセスと対応チームのメンバーの責任が記載されなければならない。組織の各部門間の意思疎通のために調停者が指名され、かつその調停者は、各部門の長から信用されていなければならない。部門の長は、計画とインシデントの調査でどんな情報が共有されるのか、あるいは共有されないのかを理解する必要がある。

インサイダー・インシデント対応計画の詳細が、多分、全ての従業員で共有されるというわけではない。計画を実行する責任者だけが理解して、その内容と遂行について訓練されていなければならない。従業員は、その（計画の）存在を知って、そして、報告すべき不審な行動の種類と同様に、報告する（匿名で）方法が訓練されていなければならない。マネージャーは、如何に個人的問題や仕事上の問題を取り扱うべきか、そして、いつそれらがインサイダー侵害のリスクになるかを理解しなければならない。組織が悪意のあるインサイダー攻撃からの損害を経験したり、新しい形の内部又は外部からの攻

撃のような、その他のリスクが出現したならば、従業員の訓練は見直されなければならない。インサイダー・インシデントから学んだ教訓は、インサイダー・インシデント対応計画にフィードバックし、計画を継続的に改善しなければならない。

事例研究：これらが行われなかった場合、何がおこるであろうか。

宝くじ代理店のあるインサイダーは、１年半に亘ってはずれ券を当り券に変更し、ほぼ６万３,０００千ドルを詐取していた。そのために、彼は通常通りチケットを購入し、当り券にするために宝くじ代理店のデータベースを改ざんした。宝くじ代理店は、不正なチケットを発見した時点で調査を開始した。幸運にも、インサイダーは休暇であった。さもなければ、インシデントを調査する調査員に選ばれていたかもしれない。休暇から戻り、不正なチケットに直面した時、インサイダーは挙動不審であった。そのため、彼は休職となり、物理的アクセスも無効となった。

組織が、容疑者を排除するための正式な手続きを取る間、同僚にインシデントを知らせることを怠ったため、インサイダーは、まだ組織の人員を管理・統制することができた。休職に入る前に、インサイダーは、犯罪行為を証明したかもしれない履歴ログを削除した。さらに、彼は、ある同僚に 4 週間分のバックアップ・テープを、それらは現在使われている新しいバックアップデータフォーマットの下で役に立たないと嘘を言って、削除するよう頼んだ。同僚は、この要請に応じた、そして、組織は、インサイダーがシステムセキュリティ制御を勝手に書き換えた証拠の多くを失った。また、インサイダーも、他の同僚に、無実を証明するであろう、幾つかの追加的バックアップ・テープを探すよう依頼した。同僚はこれに従った。そして、組織は、それらのテープを決して取り戻すことはできなかった。組織に首尾一貫したインサイダー・インシデント対応計画が整備され、従業員がインサイダーの要請に応じることに対する責任について教育を受けていれば、組織はインサイダーの詐欺行為に対して上手く対応できたかもしれない。

もう１つの事例では、製造工場の組立て検査官は、品質に関係なく承認するよう圧力をかけられていること及び検査官に対する支援が不足していることについて管理側に不満を言った。独立評価員が、主張に根拠がないと判断したにもかかわらず、インサイダーは会社を訴えると脅迫し、沈黙の換わりに現金による和解を提案した。この恐喝の試みは、会社によって拒否された。そして、会社は、数年後に、新聞が会社の専有情報を暴露するまでなんの処置も取らなかった。インサイダーが情報漏洩に責任があるという匿名の非公式の情報を受けた後に、組織は調査を開始した。

法執行機関の調査で、組織は、インサイダーが 2 年以上に亘り、責任外の組織の機密情報をダウンロードしていたという証拠を発見した。インサイダーは、取り外し可能な記憶装置（USB）を使って、大量の情報をダウンロードし、自宅にそれを保存していた。

また、調査によって、インサイダーと新聞記者との電子メールのやり取りの証拠を発見した。彼らは、電子メールで専有情報、記事、会合などを打ち合わせていた。後からだから言えることだが、組織が、脅迫未遂の時点で、インシデント対応計画を発動していたならば、インサイダーのその後の行動を防止したかもしれない又は新聞への機密情報の流失を防止できたかもしれない。

６　実践事例の参考文献／出典

１．Alberts Christopher、Dorofee Audrey、Killcrece Georgia、Ruefle Robin、Zajicek Mark 共著『CSIRT（コンピュータ セキュリティ インシデント レスポンス チーム）のためのインシデント管理プロセスの定義：.進展中の作業（CMU/SEI-2004-TR-015)』ソフトウェアエンジニアリング研究所、カーネギーメロン大学、ピッバーグ、ペンシツベニア州、２００４年、: http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html.

２．英国規格協会：http://www.bsigroup.com/.

３．CERT「生存性と情報保障のカリキュラム（SIA)」: http://www.cert.org/sia.

４．CERT「仮想訓練環境(VTE)」： https://www.vte.cert.org/.

５. 統合情報セキュリティ作業グループ（Corporate Information Security Working Group : CISWG）議長Adam H. Putnam「ベスト・プラクティスとメトリックスチームに関する報告」技術・情報政策小委員会、政府間関係及び政府改革調査委員会、米国下院、２００５年：http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661.

６．国家サイバーセキュリティ局　国土安全保障省「セキュリティの構築」：https://buildsecurityin.us-cert.gov/daisy/bsi/home.html.

７．米国連邦金融機関検査協議会（Federal Financial Institutions Examination Council : FFIEC ）『情報技術検査ハンドブック』：http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html.

８．情報セキュリティフォーラム（ISF)「グッド・プラクティスの標準」：http://www.isfsecuritystandard.com/.

９．情報システム監査・コントロール協会(ISACA-Information Systems Audit and Control Association). : http://www.isaca.org.

10．国際標準化機構　『情報技術 - - セキュリティ技術 - - 情報セキュリティ実施基準』(ISO/IEC 17799:2005/Cor 1:2007)　２００７年：http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46381 .

11．国際標準化機構『情報技術 - - - セキュリティ技術 - - - 情報セキュリティ実施基準』(ISO/IEC 27001:2005)　２００５年：http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=4210.

12. マスターカードワールドワイド　「マスターカードSDP *(Site Data Protection).*プログラム」：https://sdp.mastercardintl.com/pdf/pcd_manual.pdf.

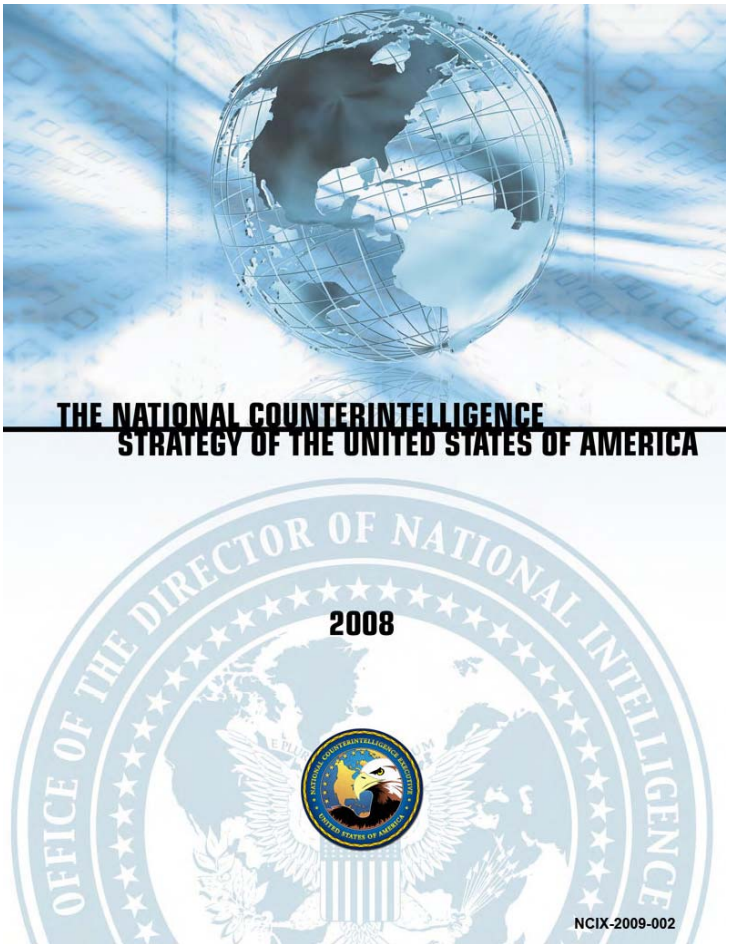
13．米国標準技術局（NIST)「特別出版（800 シリーズ)」; http://csrc.nist.gov/publications/PubsSPs.html.

14．英国商務庁　情報技術インフラストラクチャー図書館：http://www.ogc.gov.uk/index.asp?docid=1000368.

15．ビザ　「カード保有者情報セキュリティプログラム」：http://usa.visa.com/merchants/risk_management/cisp_tools_faq.html.

米国の国家対情報戦略(2008 年)

(THE NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA, 2008)



国家対情報戦略(２００８)は、国家対情報政策会議との協力により改訂されたものである。国家対情報局長が主宰する国家対情報政策会議は、以下の関連各省庁の長に指名された上級の対情報担当官で構成される。

国務省
国防省（統合参謀本部を含む）
司法省（連邦捜査局を含む）
エネルギー省
国土安全保障省
中央情報局

はしがき

本刊行物は、2002 年対情報強化法（合衆国法典第５０篇４０１条）に基づき国家対情報局長が作成した「米国の国家対情報戦略 2008(National Counterintelligence Strategy of the United of states of America 2008)」を翻訳したものです。本出版物は、一昨年 6 月に出版した「BSK第 19-6 号、米国の国家対情報戦略(2007)」の改訂版となります。

本報告は、①外国の情報活動と電子的侵入からの国家の保護、②米国情報組織の完全性の保護、③国家政策と意思決定に対する支援、④米国の経済的優位、企業秘密、およびノウハウの保護、⑤軍に対する支援など、米国の対情報組織の課題と対処法が説明されています。我国は対情報戦略を具備していませんが、現実には外国の経済スパイ、産業スパイ、又は企業機密窃盗などの脅威に直面しています。したがって、対情報に関する米国の考え方を知ることは大いに参考になるものと思われます。

米国では、昨年１月、大統領令により「包括的国家サイバーセキュリティ・イニシアチブ(Comprehensive National Cybersecurity Initiative)」が発表されました。この大統領令は、機密文書であり内容は公表されていませんが、マスコミの報道等をとおして、このイニシアチブの 12 件のプログラムのうちの一つがサイバー対情報(cyber counterintelligence)であることが知られています。また、昨年 7 月 30 日に出された行政命令 13470 において対情報の定義が改訂されました。この改訂によりサイバー脅威への対応が対情報活動分野に追加された模様です。その理由は、今日の諜報活動や破壊工作の多くがコンピュータネットを利用して行われるようになったことにあるようです。

以上のような背景を受けて、本報告では、以前の報告にはなかったサイバー対情報という用語が“前書き”の最初のパラグラフに記載されています。しかし、ごく簡単に触れられているだけで具体的な内容についての言及はありません。サイバー対情報が、対情報コミュニティの活動に及ぼす影響については、次回の報告が俟たれるところです。

本出版物が､我が国における情報セキュリティの向上にいささかでも貢献できれば望外の幸せです。

平成２１年１０月

財団法人 防衛調達基盤整備協会
理事長　宇 田 川　　新　　一

目　　次

序

本国家対情報戦略は、本土へのテロ攻撃を警告・防止するのに役立ち、その他の非対称脅威に対処し、そして伝統的かつ永続的な戦略的課題に関する信頼できる情報を提供するという米国情報の基本的な責任について詳述している。また、本戦略は、外国の勢力およびグループの情報活動によってもたらされる脅威から国家機密を保護するために、米国政府の対情報組織が、公共部門や民間部門の課題に対処する方法、および外国勢力等に関する秘密情報を入手する方法を説明している。

本戦略は、国家対情報局長により起草され、米国政府の対情報組織全体との調整がされ、国家対情報政策会議に承認された。

本戦略は、米国法典第５０篇第４０２a条の規程に基づき大統領の承認を得ることにより、米国政府の対情報プログラムおよび活動の実行に関する指針となる。本戦略が適切に履行されるならば、「２００２年国家対情報強化法」において米連邦議会が意図した米国の対情報機能の統合と有効性は一層強化されるものと、私は確信する。

J.M. McConnell
国家情報長官

まえがき

昨年、対情報局は、国家対情報政策会議の支援を得て、国家対情報戦略の大幅な改正案を起草し、大統領に承認された。議会の要求に基づき、今年も再び国家対情報戦略を見直した。そして、我々の掲げる目標が来年度も有効であり続けることを確信した。掲げる目標、特にサイバー対情報(cyber counterintelligence)の議論の主眼点について軽微な修正を行い、大統領は、その提案を承認した。急激ではないが年々絶えず進化している永続的な脅威に直面している我々にとって、戦略の策定・実行の継続は重要である。従って、対情報コミュニティは、２００７年に達成した進歩を基礎とし、これらの目標の履行を継続する。

昨年、大統領は、対情報のあらゆる能力を反映させるために、行政命令１２３３３の対情報の定義を改訂し、対情報の戦略的重要性を認めた。２００７年と２００８年の前半に、、コミュニティとして仕事をする中で大きく進歩した。例えば、対情報局は、法令に基づく統合機能をより効果的に実行するために、サプライ・チェーン・リスク ― 即ち、重要な調達に、安全性が低下するように不法に手を加えられているかもしれないリスク ― に対する、より洗練された対策を開発した。

これらの対策、さらに対情報局と情報コミュニティ全体の仲間とのより活発な連繋を基礎に、コミュニティ全体としてこのリスクに対処する上で、より大きな均一性を達成し始めた。一方で、大統領の包括的国家サイバーセキュリティ・イニシアチブ(Comprehensive National Cybersecurity Initiative)の対情報に関する条項を作成する際に連邦捜査局とともに主導権を握った。また、情報漏洩が発生した際に損害評価（damage assessment）を実施するプロセスを再設計した。これらの措置は、戦略的目標を活動として実現するという具体的な進歩を意味するものである。来年度も、これらの措置を実行するとともに、強化された国防省（訳者注：Defense Counterintelligence and Human Intelligence Centerが国防省に新設された）の対情報との戦略的一貫性をもたらすために国防長官のイニシアチブに特別の注意を払うであろう。

米国は、安全保障、自由、および繁栄に対する大きな挑戦に直面している。従って、戦略の策定と実行の継続は重要である。国際テロリズム、大量破壊兵器(WMD)の継続した拡散、非対称戦、過激主義運動、および破綻国家は、公正で安定した国際秩序に対し激しい挑戦状を突きつけている。これらの挑戦に対応する我々の能力は、伝統的および非伝統的な敵対者によって脅かされている。我々の敵対者 ― 外国の情報機関、テロリスト、外国の犯罪組織、およびハッカーは、米国の安全保障の利益を損なうために、公然(overt)の活動、非公然（covert）の活動、および地下活動（clandestine）を行っている。

対情報(注1)は、このような活動を防止することのできる国力の幾つかのツールの一つである。しかし、その有効性は、多くの分野における他の政府機関や民間部門との協力に頼っている。

冷戦の期間中、米国の敵対者は、米国の極めて厳重に保護された国家安全保障機関の保有する最重要な機密へのアクセスに成功するとともに、実質的に米国の情報と防衛コミュニティの全組織に浸透した。その結果、秘密漏洩、情報源の衰退、および人命の損失という観点から国家安全保障に重大な損害をもたらした。さらに、その結果は、戦場において我々に壊滅的な結果をもたらす恐れもあった。今日、我々は、新しい形の戦争(conflict)を戦っている。それは、

既に米国に侵入し、世界中の米国市民と我々の同盟国を脅かしているテロリストとの戦いである。この戦い ― 軍事のみならず文化、経済、外交、および政治の次元の戦い ― において、対情報活動の失敗がもたらす結果は、国家の最重要な情報、インフラストラクチャー、軍事力、ならびに世界中の米国の国益、技術、および市民を危険にさらすなど直接的かつ壊滅的なものとなるであろう。また、我々は、米国政府の情報ネットワーク、電子的に制御されたインフラストラクチャー、および最重要な技術に対する増大するサイバー脅威に直面している。この脅威は、組織的に阻止できない限り、我々の国家安全保障と経済を徐々に衰退させるであろう。

対情報コミュニティ(注2)は、相互支援組織から、９．１１後の世界の国家的課題へ全ての対情報能力を集中させることができる統一機構へと進化した。「改正２００２年対情報強化法」と「２００４年情報改革・テロリズム防止法」は、この変革を促進するとともに、国家対情報局(NCIX)に対し、この「国家対情報戦略」の作成とその履行状況について大統領に報告することを命じた。２００７年の努力にかかわらず、多くはいまだ未達成である。

お互いにまったく異なる、軍と各省庁の情報機関の対情報活動(注1)を統合するプロセスの継続は、喫緊の国家的要求である。従って、対情報コミュニティは、より一層厳密な政策、ドクトリン、基準、および技術を通して、政策と実行を国家情報長官(DNI)の定める予算と優先事項に一致させ、この統合プロセスを推進しなければならない。国家安全保障の意思決定者に対し、的を射た情報を提供するとともに、米国の機密と最重要な資産を保護するために、対情報活動は、周到に準備され、かつ統合されていなければならない。各省庁と軍の情報機関相互の人事交流を促進する国家情報長官(DNI)の統合任務イニシアチブ(joint duty initiative)は、重要で期待できる統合努力の一部分である。

米国の対情報能力は、対情報活動に責任を有する、様々な機関の権限と任務に適するよう時間をかけて進化してきた。しかし、個々を見れば、現有の対情報能力では、国家の直面する脅威の大きさに匹敵する対処能力を提供できず、また、重要な国家優先事項に取り組む際も各機関が必ずしも結束して対処できたわけではなかった。さらに、法令や行政命令は、対情報コミュニティの活動と資源が、国の統合対情報政策と一致していないことを繰り返し注意喚起している。連邦議会は２００２年に、米国政府の対情報の長として対情報局長（NCIX）の職を創設した。それから３年後、「大量破壊兵器に関する米国の情報能力委員会」は、活動と資源が統合対情報政策と一致していないことについて強く注意を促すとともに、対情報のための“任務管理者（ミッション・マネージャー）”の創設を求めた。そして、２００６年に国家情報長官（DNI）は、対情報局長(NCIX) を任務管理者に指名した。法令に規定された権限に基づき、対情報局長（NCIX）と対情報局（ONCIX）は、対情報コミュニティの統合を主導するとともに、米国に対する情報脅威を特定・評価・優先順位を付与し、そして対処する責任を果している。対情報局長（NCIX）は、国家対情報政策会議(注4)との協議に基づき、国家の対情報活動の実行を指導する統合国家対情報プログラムの優先事項を策定する。さらに、対情報局長（NCIX）は、米国に対する情報脅威を阻止するために、情報コミュニティ、広範な政府機関、法執行コミュニティ、民間部門、および学界との連携を促進する。連邦政府の各対情報機関は、統一された取り組みによってのみ、我国の経済的・軍事的・政治的安全保障、情報システムの完全性、経済競争力の優位性、軍、および政府の意思決定プロセスを強化するという我々の職

務を成功裡に遂行することができる。

対情報コミュニティはかなり進歩した。そして、大統領、議会、および国家情報長官（DNI）は、我々の進歩が継続することを期待している。我々は、測定可能な方法で、努力の成果を確実に手にしなければならない。さらに、資源は有限であり、かつ近い将来増加することは望めないであろう。従って、対情報局長（NCIX）は、国家の対情報機関の能力を改善するために厳しい決断をしなければならない。同時に、浸透事件や無許可の情報開示事件後に実施される対情報評価（counterintelligence assessment）に基づく勧告に沿った適切な脅威軽減対策を確実に履行しなければならない。戦略目標を成功裡に達成するためにはかなりの進歩が不可欠である。

本戦略は、情報コミュニティ全体の徹底した協議プロセスの成果物である。本戦略は、対情報コミュニティの戦略目標を説明している。そして、それは法令の要求に一致するものである。また、本戦略は、連邦政府の全ての対情報機関の組織上、事業上、および予算上の優先事項を明らかにしている。この優先事項は、大統領の「国家安全保障戦略」、国家情報長官（DNI）の「国家情報戦略」、およびその他の関連する指針と指導に一致するものである。基本的な戦略的目標は毎年変更されるものではないし、また変更すべきものでもない。しかし、リスクマネージメントプロセスは、対情報コミュニティに対し、課題、好機、および脆弱性を継続して評価することを要求している。例えば、本戦略の年次改訂において、米国に対するサイバー脅威への対応とサプライ・チェーン・リスクへのより効果的な対応が、我々の課題としてひときわ目立つ要素となった。従って、対情報局は、国家対情報政策会議の支援を得て、本戦略を毎年見直し、状況の要求に沿って改訂するであろう。

Joel F. Brenner
国家対情報局長（NCIX）

注１ 対情報とは、“外国の勢力、外国の組織、外国人、または国際テロリスト運動によってか、あるいはそれらに代わって実施されるスパイ活動(espionage)、その他の情報活動、破壊工作(サボタージ)、または暗殺を特定し、欺き、逆用し、攪乱し、または防止するために実施される活動およびそれにより収集された情報である。”（改正行政命令１２３３）(訳者注：行政命令１２３３３は行政命令１３４７０(2008 年 7 月 30 日)により改正された)

注２ 対情報コミュニティを構成する各省庁の権限は、「１９４７年国家保障法」「改正行政命令１２３３」、「２００２年対情報強化法」、および「２００４年情報改革とテロリズム防止法」に由来する。

注３ 対情報活動には、これに限定されるものではないが、収集、分析、捜査、およびオペレーションが含まれる。

注４ 国家対情報政策会議の権能は、「２００２年対情報強化法」により付与されている。国家対情報政策会議は、対情報活動の実行を管理するために、大統領の承認を必要とする政策と手順を開発する主要なメカニズムとして機能する。

１　導　入

米国の対情報の各機関は、統一かつ団結したコミュニティとして行動する。また、各機関は、其々の機関の能力と権限に基づき、かつ国家対情報局長（NCIX）によって設定された優先事項に従い彼らの目標を達成する。

２．外国のスパイ活動と電子的侵入からの国家の保護

米国は、米国の国内外の軍事的、外交的、および経済的利益に対して有利な立場を獲得しようとする外国の情報活動、テロリストのテロ活動、およびその他の非伝統的な敵対者からの多種多様な安全保障上の脅威に直面している。これらの脅威は、単一の機関では能力的または資源的に対処不可能である。従って、対情報コミュニティは、これらの脅威を理解し、攪乱し、逆用し、そして阻止するために共同して対処しなければならない。必要に応じて、逮捕や国外追放によってこれらの活動を阻止する。

このため、対情報コミュニティは、米国の利益を標的とした敵対的情報活動を特定し、優先順位を付与し、そして、これらの活動を打破するために、収集、分析、捜査、およびオペレーションの資源を活用する。また、我々はサイバースペースに関する能力を拡大する。サイバー環境は、前例のない機会を敵対者に提供するとともに、情報システムに大きく依存した国家に脆弱性をもたらしている。強固かつ十分に保護された情報インフラストラクチャーは、国家安全保障の維持のあらゆる側面において実質的に極めて重要である。外部の敵対者と同様に部内で信頼されているインサイダーは､米国の情報インフラストラクチャーを標的として､利用し、妨害し、そして潜在的な破壊を行っている。従って、対情報コミュニティは、あらゆる情報技術を駆使して敵対者の情報活動を逆用・打破しなければならない。

各対情報機関は、対情報コミュニティより広範な情報コミュニティの同僚と協力し、戦略的脅威指針(注５)に従って、外国勢力とテロリストを含む非国家グループの情報能力と活動を評価するとともに、彼らの資源、計画、作戦、および世界的影響力を解明する。
外国の情報機関とテロリストグループは、資金等を調達し、要員を訓練・展開し、地下活動と非合法活動双方の情報作戦を我々に対し仕掛けている。対情報コミュニティは、彼らは誰か、彼らの情報協力者は誰か、彼らは何をするのか、彼らは何故それをするのか、彼らは何ができるのか、を理解しなければならない。そして、各対情報機関は、敵対的情報活動に対抗し、逆用し、そして打破するために―特に、米国の中枢に浸透したスパイを根絶するために―これらの知識を活用する。

従って、対情報コミュニティは、世界中の優先される外国勢力あるいは非国家グループに対しあらゆる手段を使用し、積極的かつ戦略的な作戦を実行する。外国勢力の情報活動は、我々に、彼らの作戦を逆用し、彼らの情報にアクセスする機会となり、延いては彼らの組織の完全性を崩壊させる好機となる。我々は、米国に対する敵対的情報活動を防止または打破するために世界規模の作戦を実行する。各対情報機関は、それぞれが保有する固有の能力、権限、および資源をもって、情報コミュニティの統一努力に貢献する。

注５ 国家対情報局長（NCIX）は、「国家情報優先事項フレームワーク（NIPF)」、「国家脅威識別と優先順位評価（NTIPA)」、およびその他の指示等から戦略的脅威指針を選定する。

３．米国の情報システムの完全性の保護

米国の情報システムは、米国政府と同盟国に信頼できる情報を提供しなければならない。このシステム―人々、施設、情報システム、および保有するインフォメーション―の完全性と信頼性は、敵対者等の浸透（訳者注：浸透（Penetration）は、米軍では「対象組織の情報の獲得もしくはその活動に影響を及ぼすために対象組織内からスパイ（agent）をリクルートすること､またはスパイもしくは技術的監視装置を対象組織内へ潜入させること」と定義されている。「米軍統合用語集」）または影響から組織を保護する我々の能力に依存している。この目標を達成するために、対情報コミュニティは、政府全体の保全（security）、調達、情報保証（information assurance）、およびその他の関連専門分野の同僚と緊密に連携・協力する。浸透を防止する保全対策の有効性は、敵対的情報脅威の性質と範囲に関する最新の情報によって強化される。１つの機関だけでは、米国情報組織と最重要な国家資産の完全性を確保することは出来ない。

脅威と脆弱性は、我々の文化、慣行、基準、ノウハウ、方式、および資源における人的および技術的側面に固有なものである。これらの脅威と脆弱性を評価することは、リスクマネージメントの基本的かつ継続的な任務に不可欠なものである。このリスクに対応するには、対策および厳格な基準・慣行の制定ならびに相手の弱点を活用する機会を特定するなど脅威および脆弱性を低減する措置が必要である。

米国の情報システムの完全性を脅かす外国勢力や敵対的グループの能力は、我々の情報能力と対情報能力のみならず、彼らが有する我々の保全措置に関する知識の多寡に依存する。彼らは、開放的、民主的、かつ非常に透明性の高い我々の社会の活発な諸活動の中から、知識の一部を入手している。さらに、我々のインフォメーションシステムおよびネットワーク、サプライチェーンおよび調達手続、ならびに外国と共同開発プロジェクトへのアクセスによって、敵対者は知識を高めることができる。その知識は、既に米国政府への浸透と米国市民の裏切り行為によって非常に高められている。外国の情報工作員（Intelligence Operative）がもたらす脅威を低減できるか否かは、彼らが我々について何を知らないのかを確認するのと同様に、彼らが何を知っているのかを知り得る我々のスキルと、知り得た知識を活用する我々のスキル次第である。そして、このスキルは、敵対者のあらゆる作戦的および分析的手段を理解するために、我々が、彼らの組織への浸透に成功するか否かに大きく依存している。我々が敵対者の組織へ浸透できる限り、我々は、敵に関する優れた情報報告を作成することができると同時に、機密情報と意思決定プロセスをより良く保護することができる。

意思決定者は､敵対者にコントロールや操作されていない情報を要求する｡あらゆる情報は、敵対者の操作を受けやすいので、如何なる手段によって収集された情報であっても信頼性を審査することは極めて重要である。従って、いかなる対情報機関も、共通の基準に従い、対情報任務に関連した情報源と収集方法の信頼性を審査しなければならない。その他の任務分野につ

いても、我々は、収集、分析、配布要領、および他の情報活動を調査し、改善策や最優良事例を勧告・実施する。

情報は、外部だけでなく内部の脅威に対しても脆弱である。転覆活動（subversion）、反逆行為（treason）、および情報漏洩（leak）は、我々の脆弱性、政府や企業の機密、および情報源や方法などを露呈してしまう。このインサイダーの脅威は、米国の安全保障に対する途方もないダメージの源泉である。この脅威に対抗するには、国家の積極的な努力が必要である。対情報コミュニティは、保全、情報保証、情報、および法執行、ならびに科学および技術分野に責任を有する機関と協力しながら、インサイダーの脅威を抑止し、探知し、そして無効にする新しい施策、ツール、および方法を開発しなければならない。例えば、不可解な行動パターンや異常な事象を発見する、より精密な監査および分析ツールが導入されなければならない。そして、それらは常に監視されていなければならない。これらの新しいツールや技術を既存の手段に追加し、外国のスパイを巧みに騙し、積極的な捜査を実施し、逮捕することに対情報コミュニティは努力する。そして、外国の政府職員が関係している場合は、外交官の地位にふさわしくない行為に関与したことにより国外退去させる。

「２００４年情報改革とテロリズム防止法」は国家情報長官（DNI）に対して“国家安全保障上の開示要件に一致する範囲で、情報コミュニティが保有する情報の開示とアクセスを最大限にするための措置を講じる”ことを命じている。この指令に沿って、「国家情報戦略」は、情報コミュニティに対し、コミュニティのメンバーと顧客が“彼らが必要とするときに、必要とする情報にアクセスできる”よう措置することを要求している。より具体的に言えば、情報の「所有者」という考え―共有するより死蔵することを良いとする考え―を放棄し、情報共有による業務の効率化が我々に求められている。 この要求は、対情報コミュニティから完全な支持を受けている。同時に、我々は、アクセス基準を満たすものだけが利用できる非常にセンシティブな一部の情報を、最新の注意を払って保護しなければならない。制約の少ない情報の共有は、直接の対情報リスクとなる。即ち、機密文書の利用が容易になればなるほど、情報漏洩が起きやすくなり、また、盗まれやすくなる。

幾つかのスパイ事件が、既にこの脆弱性を浮きぼりにしている。そして、その事件は米国の国家安全保障に莫大な損害を及ぼした。対情報当局としては、米国が今後も決して反逆行為あるいはスパイ行為から損害を被らないということは保証できない。しかし、我々は、国家情報に関する我々のシステムをより厳しいものへと転換し、外国からの浸透を阻止し、かつその探知を容易にする組織、施策、および実施手順を既に運用していることを、大統領、連邦議会、および米国民へ確信を持って言うことができる。このため、我々は、米国に対する情報活動にサイバースペースを使用する外国の情報機関に対応するために、サイバースペース分野での我々の努力を拡大しなければならない。我々は、スパイに対応するため他のコミュニティと共同して行動しなければならない。;保全機能や法執行機能を包含していない対情報コミュニティは、保全機関および法執行機関と緊密に連携しなければならない。

４　国家の政策立案と意思決定に対する支援

外国勢力と敵対的グループは、自国の国家安全保障目標を支援するために情報活動を実施し、重要な利益のある地域にパワーを投入し、時には米国と同盟国の安全を脅かす。これらの情報活動を解明することにより、彼らの戦略的能力、限界、および計画に関する兆候を獲得することができ、さらに、受け入れがたい被害をもたらすだろう彼らの意図についての警告を得ることができる。これらの情報は、作戦計画者や運用者のみならず上級の政策立案者や意志決定者にとっても不可欠なものである。

切迫した脅威、脆弱性、および好機に関する助言を国家意思決定者に与える対情報コミュニティの能力を強化することが喫緊の課題である。各対情報機関は、統一した戦略的分析、ならびに共同した情報捜査および作戦によってこの課題を解決するであろう。対テロリズムおよび拡散防止作戦などを含む国家安全保障計画ならびに国家情報システムにおける兆候・警告（I&W）機能は、外国の情報活動の標的になりやすい。敵対者の情報能力は進化している。従って、敵対者を打破するための我々の有効性は、収集と分析双方の分野における致命的な欠落部分を特定し、これを補強する我々の能力に依存している。この目標を達成するため、我々は、オープンソース情報を含む利用可能な全ての情報源を積極的に使用するとともに、新しい技術と他組織との協力関係を活用する。

また、対情報の考慮事項は、作戦計画に盛り込まれなければならない。そうすることにより、作戦コミュニティは、情報操作や欺瞞により彼らの任務を妨害しようとする敵対者の企図を事前に認識することができる。作戦プランナーは作戦中も、対情報的展望を継続して保持しなければならない。そうすれば情報収集の機会を捉えることができ、さもなければこの機会を逃すであろう。この対情報的展望は、我々が敵対者の情報活動とテロリストグループとの関係を解明する際にも必須なものである。

「国家情報戦略」は、対情報局長（NCIX）に対して、テロ・ネットワークの解明を支援するよう命じている。対情報コミュニティは、国家テロ対策センター（NCC）と協力し、テロリストの作戦の阻止および米国の情報能力の保護に直ちに役立つ分析結果を提供する。対情報コミュニティは、テロ対策をさらに支援するため、作戦報告や情報報告を調査しテロリストの浸透または情報操作に関する企てを探知する。また、我々は、鍵となる外国の情報機関が如何に進歩しているのか、テロリズムと戦い敵対的な活動に対抗する米国の努力を如何に妨害するのかを評価する。

外国の情報機関の能力を評価するということは、彼らの情報収集手段、開発プログラム、および活動について理解することを意味する。彼らの組織は、如何に構築されているのか、彼らの意思決定プロセスが如何に機能するのか、彼らは米国の利益を標的として何処に展開されているのかについて我々は理解しなければならない。これは、対情報コミュニティが支援しなければならない収集面の挑戦であり、かつ我々が取り組まなければならない分析面の挑戦でもある。我々は、外国情報機関に関する知識のギャップを解消するために協力するとともに、このギャップを踏まえて国家情報長官官房（ODNI）の統合収集戦略に貢献する。

また、我々は、国家安全保障会議（NSC）、大統領直属情報諮問会議（PIAB）、および国家情報長官（DNI）に対し、戦略分析、対情報見積、および政策オプションを提供し、国家安全保障に関する協議を支援する。我々は、定期的に我々の情報環境アセスメントを報告し、また、必要に応じ直ちに使用できる代替案を提案する。

最も厳格な保全と対情報態勢をもってしても、秘密に指定された情報および作戦の漏洩は起こり得るであろう。従って、万一漏洩が発生した場合は、被害を軽減し、更なる損失を防止するための行動を開始すると同時に、国家安全保障に対するリスクの戦略的評価を行う被害見積（damage assessments）を迅速かつ適切に実施しなければならない。犯罪行為に関わりがある場合は司法省と協議し、必要に応じて、被害見積プロセス（damage assessment process）を直ちに開始し、結果を迅速に作成する。単に我々の損失を報告するだけでは十分でない。対情報局長（NCIX）は、適切な監察官および予算当局と協議し、直ちに実行可能な勧告を提案するためのフォロー・アップメカニズムを設置する。

５　米国の経済的優位、企業秘密、およびノウハウの保護

対情報コミュニティは、政府全体の同僚と協力して、最重要な国家資産、最重要なインフラストラクチャー、センシティブな技術、鍵となる資源、ネットワーク、および知識を外国の情報機関等の攻撃から保護する。米国の水道および下水道システム、電気配電網、金融システム、給与支払いシステム、ならびに航空および地上管制システムー代表的なものだけを列挙したがーは電子制御されており、外国から資金提供を受けたハッカーおよび特定の組織に属さない所謂フリーランスのハッカー双方の巧妙な攻撃の対象となり易い。
また、情報コミュニティのサプライチェーンもグローバル化した市場の中で付け入られるリスクがある。海外協力事業に携わっている外国企業および米国企業は、米国システムおよび技術への無許可または意図的でないアクセスを求める敵対者の標的になるかもしれない。これらの活動は、我々の知的財産を盗むこと、あるいは金融混乱もしくは物流混乱を引き起こすために情報を操作することを目的としている。国の物理的インフラストラクチャーの保護は政府の他の部門の責任であるが、対情報は、誰が計画・実行しようとしているのかを理解すること、あるいは攻撃をかわし、場合によっては、攻撃を逆用するための準備をすることにおいて重要な役割を有している。

我々は、連邦政府、民間部門、学界、および資産を管理しているがその重要性を認識していない組織などの無数の団体に存在する国家の最重要な資産とインフラストラクチャーを特定し、それを保護することを手助けしなければならない。これらの組織と、対情報機関、法執行機関、および保全機関との間の協力は、我が国の敵対者が関心を有する標的を特定するために極めて重要である。また、もし敵対者に知られた場合、たぶん標的にされであろうし、その上その損失が国家安全保障に損害をもたらすであろう情報を特定することは極めて重要である。各対情報機関は、敵対者の戦略、収集優先事項、意図、および技術的要求に関する知識を解明・利用するために、法執行機関および保全機関と連携する。そして、我々はこの知識を収集要求事項に転換する。また、我々は、米国政府以外の所有者を含む最重要な国家資産およびインフラス

トラクチャーの所有者に対して、脅威情報と警報を提供する。

６　米国軍隊に対する支援

対情報活動は、米国を防護するもの、とりわけ、米国軍隊を保護する。国家権力の手段である軍隊の作戦遂行能力を維持するために、対情報コミュニティは敵対者の米国軍隊を標的にした情報活動を無力化する。

軍隊は、長い間、テロ攻撃とテロリストを支援する敵対的情報活動の標的であった。ここ数十年間に、我々は、ベイルートの海兵隊兵舎、サウジアラビアのホバル・タワー（Khobar Towers）、およびアデン湾の米艦船コールの爆破を目にしてきた。この様なテロ活動は、通常、標的の偵察や攻撃を計画するための情報オペレーション（intelligence operations）の後で行われている。我々が察知し、そして阻止しなければならないのはこれらの情報オペレーションである。改正された行政命令１２３３３号は、国家の対情報部門に対しスパイ活動からの保護を命じている。更に、「国家情報戦略」は、対情報コミュニティに対し、“軍隊の防護を強化するための対情報措置を実施せよ”命じている。これらの命令に基づき、移動中もしくは兵舎内の軍隊または作戦区域内の軍隊を標的とするあらゆる敵対的情報活動を無力化するために、対情報コミュニティは攻勢および防勢能力を運用する。

対情報コミュニティは、軍事計画、作戦、能力、意図、および配備等を含む全世界的軍事態勢に対する敵対的情報脅威に対処する。対情報部門は、軍の戦術行動から戦略的イニシアチブまでのあらゆる分野を支援する。軍の有効性は、事前情報を入手した敵に妨害されずに軍事作戦を遂行できるか否かによって決まる。軍事作戦を支援する義務は、国防総省を超えて対情報コミュニティ全体に拡大している。対情報コミュニティは、軍に指向された敵対的情報活動、とりわけ、テロ攻撃に先んじて実施される情報活動を無力化するために軍と協同しなければならない。

７　効果的な調整を達成するための対情報コミュニティの管理

各行政官庁の実施する対情報プログラムの統合と効果的な管理は、対情報局長（NCIX）の最優先事項である。国家情報長官官房の上級予算担当官（Chief Financial Officer：CFO）の協力を得て、国家対情報局（ONCIX）は、進行中のプログラムの進捗と成果を評価し、かつ不要な冗長性を特定するために計画を作成するとともに、上級予算担当官（CFO）に対し資源投入の効果的な方法について助言する。各対情報機関は、法令に定められた機能を実行するために必要な資源データと業務見積を対情報局長（NICX）へ提出する。付言すれば、緊急事態およびその他の不測事態においても対情報プログラムは継続されなければならない。

８　対情報コミュニティの教育・訓練の改善

ますます複雑さを増す対情報環境の中で、我々は、絶えず拡大する脅威に取り組まなければならない。新しい脅威に適合するには順応性があり、革新的で、かつ広い教養を有する様々な分野の人材が必須である。

「改正２００２年対情報強化法」に定められたところに基づき、かつ対情報コミュニティとの協議を通じて、国家対情報局（ONCIX）は、対情報活動に携わる個人を教育し、専門家として育成するための施策と基準を策定する。我々は、「情報コミュニティの戦略的人材育成５カ年計画」および他の連邦政府の取り組みとの整合を図りながら、ベスト・プラクティス（最優良事例）と対情報コミュニティに必要な資格基準を制定し、中核となる訓練コースを創設し、専門職としての能力基準を定め、そして研究イニシアチブを支援するためにコミュニティとして一体として取り組む。我々は、可能な範囲で、訓練目標と基準を国立情報大学（National Intelligence University）のものと整合させる。

我々は、新しい情報脅威に適合するために、順応性のある熟練した対情報要員を育成する。特に、次の３つの領域に努力を集中する。第１に、対情報コミュニティ以外から様々な技能と経験を有する人材を採用する。具体的には、他の文化圏での生活経験があるか、英語以外の言葉を話すか、または情報技術に関する専門技能を有するものを対象とする。 第２に、これらの選抜された要員に対し、コミュニティのベスト・プラクテスに基づいた対情報活動に必要なノウハウに関する基本的な知識を付与する。第３に、リーダーシップ能力を養成するための主要な補職を特定するとともに昇進ゴールと評価基準を明確にすることにより、専門家としての育成を目的とした経歴管理基準を作成する。このライスサイクル方式には、所要人員数の正確な見積と情報コミュニティ全体のより広範な人材育成努力との統合が不可欠である。

９　公共部門のみならず民間部門における対情報リスクに関する国家的認識の向上

国家に対する情報脅威を特定・評価・対応するという任務をよりよく達成するために、我々は、他の政府機関、民間部門、および一般市民への働きかけを重視する。民間部門および学界との意義ある対話によって、我々は多くのことを学ぶことができるとともに、国家が直面する情報脅威に関する情報の公表・周知を調整するためのメカニズムを提供することができる。

外国の情報活動は、情報コミュニティやその他の国家安全保障機関のような伝統的な標的以外にも拡大している。民間部門と学界は、先進の科学的発見、最先端の技術、および先進の研究開発の肥沃な土壌であるため、外国の情報収集家にとっては垂涎の“ソフトターゲット”である。企業、大学、および一般市民が毎日使用しているサイバーネットワークは敵対的情報組織による組織的敵対活動の対象であること、そして、その敵対的活動は国家のインフラストラクチャーと電子ネットワークの完全性と安全を脅かすものであることを、米国市民は絶対理解しなければならない。対情報コミュニティは、現在我々が直面している脅威とその対応を改善するために民間部門、学界、および一般市民との対話に積極的に取り組んでいる。

各対情報機関は、研究開発を通じて、将来の脅威を予想・特定するための対情報技術の向上を図るため、意欲的な民間部門や学界のパートナーと協力する。対情報コミュニティが意欲的なパートナーとの間にリエゾン関係（本格的かつ正式な連携）が構築できるならば、外国の情報活動を標的とするとともに米国の国家安全保障を防護するために不可欠な技術等を入手することができるであろう。

１０　結論

以上述べた戦略目標は、対情報コミュニティの施策、計画立案、収集優先順位、分析、作戦、プログラム策定、予算編成、および実行の指針となるものである。国家対情報局（ONCIX）は、国家対情報政策会議と協議しつつ、対情報コミュニティを構成する各機関の相対的な優位性を生かした対情報コミュニティの統一努力による戦略目標の履行状況を監督する。また、国家対情報局（ONCIX）は、対情報コミュニティのこれらの戦略目標における進歩を監視し続け、我々の指導者に率直で正確な評価を提供し続ける。

平成２０・２１年の発刊・平成２１年度発刊予定資料

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の取り組み ―
ＢＳＫ 第２０－　３号『我が国をめぐる兵器技術情報管理の諸問題(平成 19 年度)』
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)』
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)』
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)』
ＢＳＫ 第２０－　７号『新しい防衛調達モデルの探索的調査研究(総論)』
ＢＳＫ 第２０－　８号『国の安全保障に係わる装備品等を生産している企業に対する外国資本による買収に関する各国の法規制の状況 』
ＢＳＫ 第２０－　９号『管理者用情報セキュリティ・ハンドブック』(保全講習受講用)
ＢＳＫ 第２０－１０号『効果的な意識向上促進の取組み方』『携帯電話、携帯用パソコン、携帯情報端末(PDA)、その他電子装置を携帯する海外旅行』
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』

ＢＳＫ 第２１－　１号『我が国をめぐる兵器技術情報管理の諸問題(平成２０年度)』
ＢＳＫ 第２１－　２号『米国における情報システムの不測事態対応計画について(平成 20 年度)』
ＢＳＫ 第２１－　３号『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 年度) 』
ＢＳＫ 第２１－　４号『新しい防衛調達モデルの探索的調査研究(その２)』
ＢＳＫ 第２１－　５号『中央政府における究極の省庁別財務責任者である会計官、主席財務官等の役割に関する国際比較研究』
ＢＳＫ 第２１－　６号『多層防衛：セキュアで弾力性のあるＩＴ組織の礎』(保全講習受講用)
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』『米国の国家対情報戦略(2008 年) 』

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　の　国　家　対　情　報　戦　略(2008 年)
(THE NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA, 2008)

平成２１年１０月　発行
非 売 品　　禁 無 断 転 載・複 製
発　　行　：　財団法人　防衛調達基盤整備協会
編　　集　：　防衛調達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　：　hozen@bsk-z.or.jp
ＢＳＫホームページ：　http://www.bsk-z.or.jp