ＢＳＫ第２６－４号

外国においても活用可能な、米国における インサイダー脅威に対する最善の対応策

(Best Practices Against insider Threats in All Nations)

平成２６年２月

公益財団法人　防衛基盤整備協会

はしがき

独立行政法人情報処理推進機構（IPA）セキュリティセンターが毎年出版する「20XX年版10大脅威」は、過去6年間（2008年～2013年）とも、重大脅威のトップテンに必ず「内部犯行」を継続して掲げ、組織によるインサイダー脅威の認識とその対策がいかに重要であるかを示しています。

インサイダー脅威対策に係るこのような重要性は我が国特有のものでなく、グローバルな情報通信技術（ICT）社会における全世界共通の重要課題となっています。例えば、米国における過去2年間（2012年及び2013年）のサイバー犯罪統計値は、インサイダーがアウトサイダーによる犯罪を上回っており、2013年の場合、アウトサイダーが31%であるのに対しインサイダーは34%の犯罪率となっています。

米国のカーネギーメロン大学のCERT（インサイダー脅威センター）は2001年以来、国防総省、国土安全保障省などの政府機関や民間企業とのパートナーシップに基づき、インサイダー脅威に対する包括的な調査・分析を行っており、インサイダー脅威対策に係る多くの成果物を公表しています。

この中で今回ご紹介するのは、2013年に公表された「外国においても活用可能な、米国におけるインサイダー脅威に対する最善の対応策（Best Practices Against Insider Threats in All Nations）」を翻訳したものです。それらには、ソーシャルネットワーキング、クラウドコンピューティング、モバイルワーキングなど、昨今のICTの進化を反映させた19件のインサイダー脅威に対する最善の対応策（以下「ベストプラクティス」）という）が含まれています。なお、本資料をより良く理解して実務にご活用頂けるよう、2012年「インサイダー脅威低減のための常識ガイド第4版（Common Sense Guide to Mitigating Insider Threats,4th Edition）から、各プラクティスに対応する事例を抽出して事例集として併せて翻訳しました。

本小冊子は、これら19件のベストプラクティス及びその適用にあたっての国や組織における規則や文化に対する考慮事項、及び各ベストプラクティスに係る具体的な事例を掲載しており、組織のセキュリティ管理者がインサイダー脅威対策を講ずるにあたって、重要な資料を提供するものと考えられます。

本小冊子が、我が国の情報セキュリティ体制の向上にいささかでも貢献できれば望外の幸せです。

平成26年2月
公益財団法人　防衛基盤整備協会
理事長　宇田川　新一

目　　次

要約

CERT®インサイダー脅威センター（以下「CERT」という）は、700 件以上の事例分析に基づき、インサイダー脅威による被害の防止、検知及び対応のための 19 件のベストプラクティスを推奨する。本技術ノートは、最初に各プラクティスの要約を述べ、次にその重要性を説明するとともに、同プラクティスに係る国際的ポリシー側面からの見方を示す。どの国においても、本報告をインサイダー脅威阻止のための簡潔な教育ガイド、及びインサイダー脅威に係る国際的ポリシー問題を探求したものとして利用することができる。

序論

CERT は、インサイダー脅威を現在の若しくは元の被雇用者、契約者又はビジネス・パートナーであって、組織のネットワーク、システム又はデータに対するアクセス権を持っているか又は持っていた者であり、組織の情報又は情報システムの機密性、可用性又は完全性に対し有害な影響を及ぼす方法で、意図的にアクセス権を利用又はアクセス権を超えた利用を行う者と定義する[Silowash 2012]。CERT は、主に合衆国における 700 件以上のインサイダー脅威事例の分析に基づき、インサイダー脅威の防止、検知及び対応のための近刊「インサイダー脅威低減の常識ガイド（第 4 版）」[Silowash 2012]から採用した 19 件のベストプラクティスを推奨する。本報告書は、これらのプラクティスを、その履行に影響を及ぼす国際的（文化的）問題も調査した。この調査は、どの国においても、インサイダー脅威防止のための教育ガイドとして、及びインサイダー脅威に係る国際的なセキュリティ・ポリシーに係る問題への予備的探求として利用できるものである。我々は、本報告を、インサイダー脅威ベストプラクティスの実施にあたっての国際的（文化的）な領域での効果についての最初の論考として提供する。

ベストプラクティスと国際的ポリシーからの考察

プラクティス 1: 企業全体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せよ

企業全体に及ぶリスクアセスメントは、組織による重要な資産、それら資産に対する脅威、及び攻撃成功によるミッションへのインパクトを明確化するのに役立つ。また、リスクアセスメントによって、重要なリスクの識別とその最小化のために実施する管理策が決まる。

組織は、アウトサイダーから情報システムを保護するための物理的及び技術的対策に努力を傾注することが極めて一般的であるが、信頼するインサイダーによってもたらされる脅威については無視し過ぎている。インサイダーは、高価値情報がどこに保管されているかを知っていると思われる。そしてインサイダーは、組織の IT と物理的システムを知っており、かつ、IT システムに対するアクセスが許可されている。また、インサイダーは同僚からの信頼を得ており、このことはソーシャル・エンジニアリング攻撃の成功をより容易いものとしている。データ・システムに対する物理的アクセスは、インサイダーがキーストローク・ロガーを設定すること、装置を盗み出すこと、及びデータをこっそり盗み出すことを可能にしている。インサイダーは、認可されたアクセス権を利用して企業機密（Intellectual Property: IP）を盗み出すために可搬記憶媒体に電子文書をコピーすること、データ・システムに対して破壊行為を行うこと、又は組織のシステムに保管されている個人識別可能情報（Personally Identifiable Information: PII）を利用して不正行為を行うことができる。組織は、インサイダーから重要資産を保護するため、物理的及び技術的管理策からなる多層防御を利用するべきである。また、組織は、全ての従業員、請負契約者及び信頼されたビジネスパートナーに対して、非開示合意（Nondisclosure Agreement: NDA）に署名すること及び身辺調査を受けることを求めるべきである。そして請負契約者と信頼されたビジネスパートナーに対する身辺調査は、組織内で行うものと同等のものとするべきである。

外国において活用する際の考慮事項

身辺調査の実施、及び非開示合意（NDA）やサービ品質保証制度（SLA）などの約定の有用性は、国によって異なる。国によっては、十分に整備された法律と法の執行システムが存在せず[CIA 2013a]、契約の有効性を担保するには規則があまりにも少ないか又は強制力があまりにも少ない場合がある[CIA 2013b]。汚職で知られている国からの身辺調査（又はリスク評価の全成果）は[Transparency International 2011]、信頼することができない。会社のポリシーに対する違反や過去の有罪判決など、本来、個人のインサイダー脅威リスクを高める特定の指標は、国によってはひょっとしたらインサイダー脅威リスクとは異なった関連付けが行われているかもしれない。

組織がインサイダー脅威プラクティスを導入する際には、文化を考慮すべきである。文化とは、人が社会的及び物理的環境に適応するために求められる全ての属性を合体させたものである。インサイダー脅威指標は、文化や下位文化（サブカルチャー）によって異なり、それらの文化や下位文化は複数の国々に及ぶものもある。例えば、就業遅刻やプロジェクト期限の仕損じなどは、ポリクロニック文化[1]においてインサイダー脅威とは異なる関連付けが行われており、それらの文化において時間は「人々のニーズに合わすために調節されるもの」と見られている。一方のモノクロニック文化においては、スケジュールへの執着に高い価値が置かれている[Hall 1959]。

プラクティス 2：ポリシーと管理策を明確に文書化して、首尾一貫して執行せよ

明確に、かつ、首尾一貫して執行されるポリシーと管理策は、インサイダーが不公平な取扱いを受けていると感じる可能性を減らすことができる。従業員は、明確に文書化（正確で、簡潔で、筋の通った）され、首尾一貫して実施され、参照することができ、ポリシーの背景及びポリシー違反によって生じる結果について記述されているポリシーや管理策に対して、おそらく正確にいつも従うでしょう。従業員は、雇用時及びその後定期的に、ポリシーを理解したことを確証するため及びポリシーを順守することについて確約するために署名するべきである。組織は、組織のシステム及びデータに対する利用の許容範囲、作業成果物の所有権、従業員の実績評価、及び従業員からの不満申告に係るポリシーについて、特に明確にするべきである。

外国において活用する際の考慮事項

ポリシーと管理策についてのコミュニケーションは、その社会が、ローコンテキスト社会（人々がお互いに共有している知識や経験が少ない社会）かハイコンテキスト社会（人々がお互いに共有している知識や経験が多い社会）かといった特性や文化の違いを考慮する必要がある。ローコンテキストの文化においては、明示的な方法でコミュニケートする。ハイコンテキストの文化においては、ギャップを埋める推測された文脈に頼る黙示的な方法でコミュニケートする[Hall 1959]。

ポリシーと管理策の首尾一貫した実施に影響を及ぼす要素には、プラクティス 1 で述べたように、国家の規制、法の執行機関及び腐敗行為が含まれる。従業員の同意に対する要求事項は国によって異なる。例えば、EU の標準は合衆国よりも厳格なように思える[DPWP

[1] 訳注：ポリクロミック（Polychromic）とはモノクロミック（Monochromic）に対応する用語で、モノクロミック文化では時間は有限であり「時は金なり」と感じるが、ポリクロミックな文化では時間の無駄という観念がない。ポリクロミック文化が支配的な国にはサウジアラビア、エジプト、メキシコ、フィリッピンなどがあり、モノクロミック文化が支配的な国にはアメリカ、カナダ、スイスなどがある。

2011]。

プラクティス 3 : 全従業員に対する定期的セキュリティ訓練に、インサイダー脅威意識向上を組み入れよ

従業員に対する定期的なセキュリティ訓練は、組織にとってのリスク、従業員が犯罪加担の標的となる可能性、及び重要資産の保護方法に対する意識を向上させる。組織は、従業員がインサイダー脅威の行動をよく認識できるよう、組織のデータの不正なコピー、パスワード取得・組織の情報の取得又は施設への不正なアクセスを試みるためのソーシャル・エンジニアリング、組織又は従業員にとっての脅威などについて訓練しなければならない。

外国において活用する際の考慮事項

丁寧で効果的な教育と報告の手法は、プラクティス 2 で述べたように、国、文化及びサブカルチャーによって様々である。訓練の方法や内容は、ローコンテキスト又はハイコンテキスト文化におけるコミュニケーションの方法やその他の文化に関連する考察を考慮したものでなければならない。

プラクティス 4 : 雇用プロセスの最初から、不審な又は破壊的な行為に対するモニタと対応を開始せよ

組織は、インサイダーの個人的な、業務上の、及び金銭的なストレス要因を明らかにするため、従業員候補者、契約者及び信頼するビジネスパートナーからの派遣従業員に対し、身辺調査及び定期的な再調査を行うべきである。身辺調査の内容は、地方や法律により異なるが、犯罪歴調査、経歴書の記載内容と雇用状況の確認、信用調査、及び前の雇用者による能力評価を含むものとする。組織は、全ての役職に対するリスク・レベルを明らかにするとともに、より高いリスクの役職にある個人あるいはポストに就くことを希望する個人に対しては、より徹底的な調査を実施するべきである。組織は、規則違反を犯した全てのインサイダー又はリスクを高めるインサイダーのいずれに対しても、首尾一貫して罰則を適用しなければならない。破壊的な行為への対応に含まれるものには、警告、懲罰、又は従業員支援プログラム（Employee Assistance Program: EAP）の紹介がある。EAP は、インサイダーが組織に危害を加えるリスクの削減を可能とするかもしれない。

外国において活用する際の考慮事項

身辺調査[Ben Cohen 2010. EEOC 2012]及び従業員のモニタリング[Lerner 2012]に係る法律は、従業員が進んでインシデント報告を行うかどうかと同様、国や地域によってもかなり異なる。ある国の労働環境は、カースト制度[Human Right Watch, India 2012]、性別[UN

2007]、人種[Wikipedia 2012]及び同性愛[UN 2011]による差別から従業員の保護を行っておらず、また告発者に対する法的保護はたとえそのような保護が少しでもあったとしても無力である[Kaplan 2001, OSHA 2013, Collins 2010]。それらの職場環境では、インサイダーや知人が容易に復讐することができることから、保護を受けていない従業員が不審な又は破壊的行為を報告することは期待できない。

ある国の文化は、極めて集産主義的[2]か又は個人主義的傾向にある[Hofstede 1980]。集産主義者は、グループのためを思ってセキュリティ問題を報告するか、又はグループを傷つけることを恐れて報告をためらうかもしれない。個人主義者は、報告者に何の利益も見出せないことから報告しないかもしれないが、セキュリティ問題を明らかにしたことへの薄謝を稼ぐ目的で報告するかもしれない。

プラクティス５：職場環境における否定的問題を先取りして管理せよ

組織は、職場で許容される行為、経歴管理、紛争解決、勤務時間、服装規定、その他職場の基準が示す期待事項ついて、従業員に明確に伝達するべきである。組織による適切に文書化されたポリシー及びプラクティスの首尾一貫した実施は、公明正大な職場環境を促進するとともに、インサイダーによる不満な気持ちを和らげることにもなる。ボーナス、昇給又は昇任などの期待事項に未だ与っていない従業員は、時には否定的な感覚を心に抱くものである。仮に、組織が一定の期間内に昇給させることもボーナスを付与することもできない場合、管理者からの従業員に対する事前通知により、従業員の期待を収拾することができるかもしれない。また、昇進、昇給及びボーナスに対する明確な必要条件が、期待を抑制することになるかもしれない。セキュリティ要員は、組織の財政的ストレス又はダウンサイジングからの影響を受ける従業員一人一人について、特別な警戒を怠らないようにするべきである。従業員支援プログラム（EAP）は、従業員の職業上のストレスや個人的なストレスの軽減の助けになることから、おそらくインサイダーによる脅威リスクを低めることになると思われる。

外国において活用する際の考慮事項

このプラクティスは、プラクティス 2 で述べたコミュニケーション問題を共有するものである。従業員に対する期待事項は、国、文化及び組織の行動規範の違いにより異なる。したがって、組織は、否定的問題を管理する際に、組織に特化した標準の期待事項を考慮するべきである。

[2] 訳注：集団的な人による所有の社会主義的原理を支持している。

プラクティス 6：汝の資産を知れ

一般に、組織の資産に対する認識は、潜在的なインサイダー危害からの復旧又は危害の低減と同様、情報セキュリティにとって重要である。インサイダーという者は、資産が詳細に記録されていれば、IT 装置を盗むことはほとんどあり得ない。組織がいったん重要な資産の価値を決定すれば、組織はインサイダー及びアウトサイダーの両脅威に対して、効果的な保護策を講じることができる。組織は、全ての物理的資産及び情報資産、それら資産へのアクセス権限が与えられた者、並びにそれら資産の設置場所を管理するべきである。組織は、組織が処理するデータのタイプ、及びそれらデータが処理・保管される場所を把握するべきである。物理的資産に対するインベントリは、資産所有者の職務及びシステム上のデータのタイプを明らかにするべきである。組織は、全ての資産に対するソフトウェア・コンフィギュレーションを文書化するべきである。組織は、サーバー上の各アプリケーション又はデータベースに対する IT サポート連絡先を文書化するべきである。資産とデータに対しては、高価値攻撃目標を決定するための優先順位づけが行われるべきである。資産リストは、時宜を失せず更新されるべきである。

外国において活用する際の考慮事項

法的保護が欠落している国の従業員は、プラクティス 4 で述べたとおり、文書化プロセスの対象となっていない資産に対する不正行為や窃盗に対する報告をやっかいなことと感じるかもしれない。資産の文書化に対する信頼性と徹底性は、プラクティス 1 で述べたとおり、国家の規則、強制力及び汚職の程度次第である。

プラクティス 7: パスワードとアカウントの厳格な管理のポリシーと厳格なプラクティスを実施せよ

悪意のあるインサイダーは、アカウントを危殆化するため、パスワード・クラッキング、ソーシャル・エンジニアリング、バックドア・アカウントの設定などのテクニック、及びインサイダーが退職した後も利用可能なアカウントを利用している。組織は、悪意のあるインサイダーによる組織のシステムへの不正利用を防止することができる。それは、パスワードを定期的に変更すること及びパスワードの共有を禁止することにより強力なパスワードを確実なものとするため、組織におけるパスワード・ポリシーと手順を策定することである。組織は、請負契約者とベンダーを含む全てのスタッフを、これらポリシーの対象とするべきである。また、法律顧問は、契約の相手方の従業員の離職について、時宜を失せずに報告することを契約条項として要求するべきである。組織は、共有パスワードの利用に制限を設けるとともに、定期的に全てのアカウントの必要性について監査及び再評価を行うべきである。

外国において活用する際の考慮事項

多くの組織は、従業員については社会保障番号など、又はサービスの一部として顧客については銀行口座情報など、いずれにせよ個人データを収集している。合衆国においては、州及び連邦政府の規制により個人情報に対するセキュリティ要求事項を定めている。例えば、定期的に変更される強力なパスワード管理が要求されている[FTC 2006]。多くの国々には、個人データ保護の規制があり、個人データ保護のための適切な情報セキュリティを要求している。例えば、最小限のセキュリティ対策として、パスワードと個人情報の保護を要求している[Italian Data Protection Authority 2003, Annex B]。適切な対策と考えられるのは、国によって異なる。また、組織の文化もこのプラクティスに対して影響を及ぼしている。ある組織では、パスワード・セキュリティについての文書化されたポリシーがあるものの、実際は従業員によるパスワードの共有を容認している。ある組織又はある国の文化における従業員は、厳正な統制に抵抗するかもしれない。例えば、集団的かつ協調的文化の職場環境における従業員は、厳正な管理策が協同を妨げるものと感じるかもしれない[Valdez 2009]。

プラクティス 8：職務の分離と最小特権を強化せよ

組織は、技術的システム及び物理的スペースへのアクセスを制限するための職務の分離と最小特権の仕組みを利用することにより、一人の悪意のあるインサイダーによる可能な犯行の損害を制限することができる。二人ルール（Two-Persons Rule）は、技術的又は非技術的方法で実施することができるものであり、タスク（例：バックアップや復旧機能）を成功裏に完遂させるため、二人の要員の参加を必要とするものである。最小特権ルールは、アクセス権の保有を従業員が与えられた業務の達成に必要な資源に限定することを求めるものである。最小特権ルールの実施は、従業員の経験が雇用ライフサイクルを通じて変化（例：昇任）することから、継続的な（間断のない）プロセスとなる。役割ベースのアクセス制御は、職務権限に応じてアクセスを制限する。

外国において活用する際の考慮事項

企業における要求事項は、このプラクティスに影響を及ぼすかもしれない。例えば、唯一の ID 及びアクセスの必要性を含む強力なアクセス制御対策[PCI Security Standards Council 2010]、又はリスクの管理と対策要求事項に従った職務の分離などの実施を要求することである[FDIC 2012]。また、国家のデータ保護法も、技術的及び物理的アクセス制御を求めるかもしれない[AEPD 1999]。さらに、文化もこのプラクティスに関係しているかもしれない。例えば、従業員は、信頼に高い価値を置いている文化の下での二人ルールに対して、組織が彼らを信用していないと感じるかもしれない。

プラクティス 9 : 全てのクラウド・サービスに対して、明確なセキュリティ合意事項を、特にアクセス制御とモニタリング機能について定めよ

組織は、自身の要求事項につりあった保護とモニタリング要求事項を、クラウド・プロバイダーに確実に求めなければならない。保護には、クラウド・プロバイダー従業員に対する人的資源プラクティスは勿論のこと、物理的及び技術的要求事項が含まれる。クラウド・プロバイダーは、雇用後定期的に更新される従業員の身辺調査を雇用前の従業員に対しても実施すること、従業員に対してポリシーとプラクティスに対する同意を求めるとともに、それらについての訓練を行うこととするべきである。クラウド環境における一つの潜在的なリスクは不正を働く管理者であり、これにはホスティング会社の管理者、ヴァーチャル・イメージ管理者、システム管理者及びアプリケーション管理者が含まれる。これらのインサイダーは、クラウドの脆弱性につけ込むこと、又は攻撃プラットフォームとしてクラウドを利用することができる。組織は、クラウド・プロバイダーのサービス品質保証制度（SLA）と保険をレビューし、リスクと有責義務が適切に取り扱われていることを確実なものとしなければならない。また、組織は、クラウド・プロバイダーのポリシーとプラクティスをレビューし、データの機密性、完全性及び可用性を保護する適切な対策が講じられていることを確かなものとしなければならない。SLA には、クラウド・プロバイダーに対する監査権限、人的資源サプライチェーン管理特有の要求事項、又はセキュリティ違反通知の要求事項を含めてもよい。組織、第三者又はプロバイダー自身が、分散されたインフラをモニタすること、監査ログをレビューすること、診断データを集計すること、及び定期的にクラウド・インフラを監査することにより、仮想マシンやその他のクラウド・システムがセキュリティ・コンフィギュレーション要求事項を満たしていることを継続的にモニタするべきである。

外国において活用する際の考慮事項

このプラクティスには、リスクの決定にあたっての文化的要素が影響を及ぼす。組織は、第三者による組織データへのアクセスに特有のリスクがあることから、そのリスクをどの程度受け入れられるか、並びにそれらを契約、管理策及びプラクティスによってどの程度低減できるかについて決定しなければならない。また、クラウド・サービス・プロバイダーはデータを様々な場所に保管しており、かつ、データ保護やデータ違反に係る法律は企業や国によっても異なる。これらに対する合衆国内の規制は、プラクティス 7 で詳しく述べたように、州によって異なる。組織は、クラウド・サービス・プロバイダーが組織のデータをいかなる裁判管轄権下において保管しようとも、そこで適用されるデータ保護及びデータ違反法にどのように従うかを決めなければならない。組織は、ある裁判管轄区の規則がデータのセキュリティ又はプライバシーを十分に保護しないかもしれないことを念頭に、組織のデータを異なる裁判管轄区に移すプロバイダーの能力を統制することを検討したいと思うかもしれない。さらに、異なる裁判管轄区における法令や判例法が、本プラクティスで概説

したSLA合意事項の執行力に影響を及ぼすかもしれない。

組織は、クラウドに保管されているデータの所有権とプライバシーについて考慮するべきである。従業員は、法的要求事項や文化上の期待にもよるが、彼らのクラウド・データのプライバシーに対してある程度の期待を抱いている。データの所有権に係るルールは、クラウド・プロバイダーが捜査又は訴訟の間にデータを手放すかどうかなど、裁判管轄区によって異なる。同様に、違反が発生した場合、コンピュータ・フォレンジック専門家に対する実施許諾は無論のこと、証拠保存に対する要求事項も国家により異なる。

プラクティス 10：特権ユーザーに対する厳格なアクセス制御とモニタリング・ポリシーを制定せよ

特権を持つユーザーは、組織に対するリスクの増大をもたらすかもしれない。なぜなら、彼らは、システム、ネットワーク及びアプリケーションに対し、一般の従業員に比べ、より一層のアクセス権、技術能力、他のユーザーとしてのログイン能力、並びに監督及び承認の責任事項を持っているからである。悪意のある特権ユーザーは、論理爆弾の仕込み、ウィルスの書き込み、システム・ログの改ざんなどを含め、技術的に巧緻な攻撃と隠蔽工作を行う。組織は、悪意のある特権ユーザーの防止、検知及び対応のため、オンライン上の活動を単一の従業員に帰することを可能にする否認不可性など、いくつかの異なる技術を考慮することができる。組織は、特権ユーザーに対し、ユーザーの合意と行動規範を含め、特権ユーザー特有のポリシーへの署名を要求することができる。特権ユーザーに対しては、職務の分離を実施することが重要である。最後に、組織は離職した特権ユーザーのアクセス権を完全に無効化しなければならない。これは、多くのインサイダー脅威事例に離職した従業員が含まれていることによるものである。

外国において活用する際の考慮事項

組織がどの程度の特権ユーザー・ポリシーを実施できるかは、国の雇用法又は企業の要求事項（例：労組との交渉）によって異なる。また、これらのポリシーの実施は、組織の文化又は特権ユーザーの下位文化（サブカルチャー）によっても異なる。企業又は国際的な規則は、後述のプラクティス12に示すように、文化上の価値と同様、組織が従業員をモニタする能力を妨げることも又は強化することもできる。

プラクティス 11：システム変更管理を制度化せよ

多くの悪意のあるインサイダーは、バックドアの設置など、組織のシステムに対する不正な改ざんを行っている。組織は、変更管理を利用して、変更を文書化すること及び組織のシ

ステムとデータに対する完全性と正確性の保護を行うことができる。組織は、ベースライン・ソフトウェアとハードウェアを識別して文書化するとともに、その内容情報について変更の都度更新しなければならない。また、変更管理プロセスは、変更ログ、バックアップ、ソースコード、その他のアプリケーション・ファイルを保護しなければならない。組織は、変更管理を通じ、異なる従業員に対するそれぞれの役割を明確にして付与することにより、一人の悪意のあるユーザーが検出不能の変更を行うことを困難なものとすることができる。

外国において活用する際の考慮事項

おそらく種々の国際法が、システム変更管理によるデータ保護に影響を及ぼしているかもしれない。国は、個人のデータに対する要求事項を定めているかもしれない。例えば、毎週のバックアップ・コピー及び損失や破壊時に元のデータに復旧する能力を要求すること[AEPD 1999]、又は健康情報が「検出されることなく不適切に改ざんされないこと」を要求することなどである[USG 2007]。

プラクティス 12：従業員の行動のログ、モニタ及び監査のためにログ相関エンジン又は SIEM システムを利用せよ

組織は、単にログ情報によるよりも、絶え間なく増大するデータ収集の中で事象の相関関係を調べることにより、情報に基づくより良い意思決定を行うことができる。組織は、セキュリティ情報・イベント管理（Security Information and Event Management: SIEM）システムを利用して、ベースライン及び不規則な活動の両者を明らかにすることにより、モニタリングのきめ細かさを調整することができる。モニタリング・ポリシーの策定と実行は、法律、人事（Human Resources: HR）及び情報保証（Information Assurance: IA）の各部門を含め、組織を横断するチームによるインプットと共同作業を必要とする。例えば、CERT の調査研究は、悪意のあるインサイダーが辞職するまでの 30 日間以内に攻撃を行うのが一般的であることを示していることから、人事部は情報保証部に対し当該インサイダーが離職待ちの状況にあることを通知するべきである。

外国において活用する際の考慮事項

雇用者が技術的及び非技術的領域において、どのような方法で、何時、そして何をモニタできるかは、組織機構や国により大いに異なる。文化は、従業員のどのような情報を捕えるべきかについて大きな影響を及ぼすかもしれない。従業員の中にはプライベートと考えている情報への立ち入りに憤慨する者がいるもしれないし、一方で他の従業員はそれらのデータがプライベートであるとは少しも思っていないかもしれない。また、国際法や国際的な規則も、それに基づく組織の決定は無論のこと、従業員情報の収集と相関分析に影響を及ぼすかもしれない。国によっては、雇用者が収集できるデータの内容、及び従業員に対する通

知と同意に係る要求事項が規定されているかもしれない。どうであれ、機微データの定義[Spring 2012]やモニタリングの規制など[ECHR 2007, Wugmeister 2008]、国による違いは生じ得る。

プラクティス 13：モバイル装置を含む全エンドポイントからのリモート・アクセスをモニタし制御せよ

また、ますますモバイル社員（モバイル装置を利用する社員）化へと向かう傾向は、モバイル装置に対する悪意のある利用の可能性を高めている。モバイル装置が持つカメラ、マイクロホン、大記憶装置及び通信の機能を利用して、機微データを捕捉したり窃取することが可能となっている。組織は、インサイダーが悪意をもって利用することが可能な、モバイル・アプリケーション機能による潜在的リスクを認識しなければならない。多層防御では、個人的に所有する装置を禁止すること、重要データに対するリモート・アクセスを制限すること、リモート・アクセス特権ユーザー数を制限すること、及び組織外の装置に対するアプリケーション・ゲートウェイを利用することができる。組織は、全てのリモート・トランザクションについてより厳密にログを収集及び監査するとともに、従業員の離職プロセス中におけるリモート・アクセスを確実に無効化するべきである。

外国において活用する際の考慮事項

国の法律は、組織が特定のモバイル機能をどのように利用するかについて、影響を及ぼすことができる。例えば、「正当なビジネス目的のために明らかに必要であり、かつ、あまり立ち入らない方法では同じ目標を達成できない場合」[DPWP 2011]、モバイル装置で利用可能な位置情報確認サービスを雇用者が採用することを推奨することである。また、文化上の規範や法律も、個人的利用と仕事上の利用との両方に利用されている装置にどのようなモニタリングが受け入れ可能かを明らかにすることができるかもしれない[USSC 2010]。国は、リモート・ワーカー（モバイル社員）に対する情報の収集について、特定の要求事項を定めることができる。例えば、雇用者に対して「従業員の個性（*原文のまま*）と道徳的自由を確実に尊敬すること」を要求することである[Italian Data Protection Authority 2003, Section 115]。このような考慮すべき事柄は、システム・アクセス、とりわけモバイル装置からのシステム・アクセスのモニタリングに影響を及ぼす。

プラクティス 14：包括的な従業員退職手順を策定せよ

組織は、従業員の自発的及び非自発的離職を処理するためのポリシーの策定、伝達及び首尾一貫した実践をするべきである。離職した全ての従業員のアカウントは遮断され、組織が貸与した全ての装置は返却され、そして職場の全ての同僚に離職が知らされねばならない。

組織は、離職チェック・リストを策定するとともに、各タスクに個人を割り当て、離職した従業員の物理的及び電子的アクセスを確実に無効化するべきである。最後に、組織は、何らかの不審なネットワーク活動を明らかにするため、離職までの 30 日間、離職する従業員のオンライン活動をレビューするべきである[Hanley 2011]。

外国において活用する際の考慮事項

標準的な組織構造は国によって異なり、離職業務に責任を持つ関連部門も同様である。従業員の離職手続き間のオンライン・モニタリング及び同僚に対する離職通知に適用される法律は、裁判管轄区により異なる。組織は、非競合性、非開示及び知的所有権に係る合意事項の実施に関連する法的問題を考慮しなければならない。

プラクティス 15：安全なバックアップ及び復旧プロセスを実施せよ

組織は、全てのサービス品質保障制度（SLA）を確実に順守するため、安全な試験済みのバックアップと復旧プロセスを備えねばならない。組織は、可能であるならば、職務の分離を実施することにより、単一の特権 IT 管理者がバックアップと復旧プロセスを改ざんし、組織の復旧プロセスを妨害することを確実に不可能とするべきである。トランザクション・ログは、IT 管理者がログを改ざんして悪意のある活動の記録を不明瞭にするか又は削除できないよう保護されるべきである。組織が、秘密が保たれたバックアップ及び復旧プロセスをクラウド・サービス・プロバイダーに依存している場合は、プラクティス 9 を参照するべきである。

外国において活用する際の考慮事項

技術的解決策の利用可用性、多様性及び入手可能性は、発展レベルの違いから国により異なる。ここでは、プラクティス 11 の考慮事項を適用する。

プラクティス 16：正式化したインサイダー脅威プログラムを策定せよ

インサイダー脅威プログラムは、組織全体に適用されるものであり、インサイダー・インシデントの防止、検知及び対応のための明確な役割と責任事項を確立するべきである。インサイダー脅威プログラムの目標は、インサイダー脅威を識別するための明確な基準、悪意のあるインサイダー行為を防止するための技術的及び非技術的管理策の実施に係る首尾一貫した手順、並びにインサイダーが組織に危害を与えた場合の対応計画を策定することである。

法律顧問は、インシデントに係る全ての証拠が集められ、かつ、法的基準に従って保全さ

れることを確実なものとするため、及び必要な場合は迅速な法的対応を行うため、情報の収集プロセス間において極めて重要な存在となる。また、法律顧問は、情報がインサイダー脅威チーム・メンバー全員に適切に共有されることを確実なものとするべきである。これは、例えば従業員の精神的及び肉体的健康情報については、法律が認めるプライバシーを確実なものとするためである。

外国において活用する際の考慮事項

従業員によるオンライン活動のログ収集、モニタ及び調査の量とタイプは、それらが行われる環境と同様に、国によって異なる。外国において活用する際の考慮事項には、どこでインシデントが発生したか、犯罪が起訴されるとしたらどこか、どの法の執行機関が捜査を開始するべきか、及びどの法令に従って被告人の権利を保護するべきかを決定する必要性が含まれる。

プラクティス 17：ネットワーク装置の正常動作のベースラインを確立せよ

組織は、ネットワーク上の正常動作と異常動作を区別する前に、最初にベースライン動作を把握しなければならない。より広範なアプローチには、職場における（行動などの）非技術的動作についても収集することが含まれる。組織は可能な限り、企業、部門、グループ及び個人レベルにおける正常なネットワーク動作を収集するべきである。組織は、データの着眼点、ベースラインに対するそれら着眼点のモニタ時期、及びデータの収集と保管のためのツールを選定しなければならない。組織が選定したデータ・ポイントを長期間モニタすればするほど、ベースラインの信頼性はより高まることになる。

外国において活用する際の考慮事項

組織は、組織全体に及ぶモニタリング戦略の実施に先立ち、法律顧問と相談の上、国際法、連邦法、州法及び地方自治体の法律を順守していることを確実なものとしなければならない。組織はベースライン・データの収集の間、おそらく従業員のプライバシー保護のための課題に気づくであろう。

プラクティス 18：ソーシャル・メディアに対して、特に警戒を怠るな

組織は、ソーシャル・メディア[3]について、ポリシーや手順の確立だけでなく、従業員に対する訓練を行うべきである。従業員によるソーシャル・メディアを利用したこのような情

[3] 訳注：ソーシャル・メディア（social media）とは、インターネット上で展開される情報メディアであり、個人による情報発信や個人間のコミュニケーション、人と人との結びつきを利用した情報の流通などの社会的要素を含んだメディアをいう。

報の出口は、敵対者が攻撃に利用することができる現在又は元の従業員と、彼らが犠牲者又は共謀加担者にせよ、組織の情報を共有することを可能にするおそれがある。例えば、攻撃者は標的型フィッシングの企て又は不正な企みを精緻化するため、組織の情報を利用するかもしれないのである。会社は、潜在的に問題のあるソーシャル・メディアへの投稿について、それが意図的であろうが、そうでなかろうが制限を課すことを検討すべきであるとともに、関連する法規類に従ったソーシャル・メディア・ポリシーを策定するべきである。

外国において活用する際の考慮事項

ソーシャル・メディア・サイトに関連するコミュニケーション問題について、外国において活用する際の考慮事項は、プラクティス 3 で述べたセキュリティ訓練と同様である。組織がソーシャル・メディアに期待することは、国、文化、法律及び組織規範により異なる。したがって、従業員が、職場及び職場外で、ソーシャルネットワーク・キング・サイトを利用することが許される範囲及び従業員が組織についての情報を開示することが許される程度について、管理するとき、組織は地域的な特性を考慮しなければならない。いくつかの国々では、従業員のオンライン上での行動に対して組織が口をはさむ能力を規制している。その一例は、作業環境に関する議論の保護に関するものである[Purcell 2012]。

プラクティス 19：不正なデータ抜き取りに対してドアを閉鎖せよ

組織がインサイダー脅威に対処するための第一のステップは、組織の重要資産（人、情報、技術及び施設）、それらの重要資産にアクセスする権限を持ちアクセスしている人間、及びそれら資産の場所を明らかにすることである。組織は、重要資産に及ぼすリスクを明らかにするため、情報資産がどのような方法で複写又は移動され得るのかを理解しなければならない。データの抜き取りには、多くの技術及びサービスを利用することができる。組織は、組織の情報システムに接続されている全ての装置について、それが物理的又は無線的にせよ、説明できなければならない。取り組むべき問題は、セキュリティと生産性のバランスである。管理策は、認可された情報のやりとりを許可するべきであるが、認可されてない情報の抜き取りを防止しなければならない。

外国において活用する際の考慮事項

技術的解決策の利用可能性、多様性及び入手性は、国による発展レベルの違いにより異なる。モニタリング及び捜査に係る法律は、裁判管轄区により異なる。

今後の活動

今後の活動計画には、本論文で紹介した様々なアイデアをさらに推し進め、国際的にも文化的にも広く適用できるフレームワークを構築することにより、インサイダー脅威と戦うことが含まれています。なぜなら、文化、技術、法律、規制や腐敗行為の環境などの国による違いが、情報セキュリティ全般、とりわけインサイダー脅威に影響を及ぼすことから、それらに違いに対する理解を深め、その特性を明らかにするための活動が実施されねばならないからです。つまり、国によりインサイダー脅威とそのリスクを示す指標との関係が異なることから、それらの関係を意味あるものとするためには、その国に特有のインサイダー脅威の事例を収集し、経験的な方法で分析を行うことが必要となります。CERT は、国際的なインサイダー脅威事例の収集をすでに開始しており、これらを当初合衆国の事例だけで構成されていたデータベースに追加しています。この追加されたデータベースは、様々な国々におけるインサイダー脅威の特性を明らかにする助けとなるものです。

参考文献

URL は、本文書の出版日付（2013 年 8 月）において有効である。

[AEPD 1999]
スペイン・データ保護局勅令994：「個人データを含むコンピュータ・ファイルに対するセキュリティ対策の強制実施に関する規制の承認を行っている」、1999年6月11日、スペイン・データ保護局
Spanish Data Protection Agency (AEPD). Royal Decree 994/1999, of 11 June, which Approves the Regulation on Mandatory Security Measures for the Computer Files which Contain Personal Data.
http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs /reglamento_ingles_pdf.pdf (1999).

[Ben Cohen 2010]
エヤル・ベン・コーヘン：「国際的経歴審査ジャングルを安全かつ合法的に通り抜ける」、2010年4月7日、従業員審査IQ大学
Ben Cohen, Eyal “Navigating the International Background Screening Jungle Safely and Legally.” EmployeeScreenIQ University, April 7, 2010.
http://www.employeescreen.com/university/ navigating-the-international-background-screening-jungle-safely-and-legally/

[Bishop 2008]
M・ビッショップ、C・ゲイツ：「インサイダー脅威を定義する」、サイバーセキュリティ及び情報インテリジェンス研究第4回年次ワークショップ：サイバーセキュリティ及び情報インテリジェンスの将来に向けての挑戦事項を満たすための戦略の開発、テネシー州オークリッジ、2008年5月、米国計算機学会
Bishop, M. & Gates, C. “Defining the Insider Threat,” article 15. Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead. Oak Ridge, TN, May 2008. ACM, 2008.

[CIA 2013a]
合衆国中央情報局（CIA）世界の実情調査：「法律制度」、2013年、中央情報局
Central Intelligence Agency (CIA) of the United States. “Legal System,” The World Factbook.

https://www.cia.gov/library/publications/the-world-factbook/fields/2100.html (2013).

[CIA 2013b]
合衆国中央情報局（CIA）世界の実情調査：「経済 - 概観」、2013年、中央情報局
Central Intelligence Agency (CIA) of the United States. “Economy – Overview,” The World Factbook. https://www.cia.gov/library/publications/the-world-factbook/fields/2116.html (2013).

[Collins 2010]
P・コリンズ、L・スタイン、C・トロンビノ：「情報源を考える：合衆国外での力のない告発者の保護が、いかに外国におけるドット・フランク法謝礼金の影響を脅かし削減させているか」、2010年、海外不正支払防止法に係る第3回年次全国学会
Collins, P.; Stein, L.; & Trombino, C. “Consider the Source: How Weak Whistleblower Protection outside the United States Threatens to Reduce the Impact of the Dodd-Frank Reward Among Foreign Nationals.” The Third Annual National Institute on the Foreign Corrupt Practices Act, 2010. Perkins Coie LLP, 2010.
http://www.perkinscoie.com/files/upload/10_25Article.pdf

[DPWP 2011]
データ保護作業グループ論文29：「スマート・モバイル装置上の位置測位サービスについての意見13/2011」、2011年
Data Protection Working Party. Opinion 13/2011 on Geolocation Services on Smart Mobile Devices, Article 29.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf (2011).

[ECHR 2007]
欧州人権法廷（ECRH）：「コプランド対連合王国（ECRH 253）」、2007年、ECRH
European Court of Human Rights (ECHR). Copland v the United Kingdom (ECHR 253). ECHR, 2007.

[EEOC 2012]
雇用機会均等委員会（EEOC）実施ガイダンス：「公民権法1964のタイトルⅦの下の雇用決定における逮捕と有罪判決の記録について考察」、2012年、EEOC
U.S. Equal Employment Opportunity Commission (EEOC). “Consideration of Arrest and Conviction Records in Employment Decisions under Title VII of the Civil Rights Act of 1964,” EEOC Enforcement Guidance.

http://www.eeoc.gov/laws/guidance/arrest_conviction.cfm (2012).

[FDIC 2012]
連邦預金保険会社（FDIC）審査ポリシーのリスクマネジメント・マニュアル：「第4.2節－内部手順と管理策、職務の分離」、2012年、FDIC
Federal Deposit Insurance Corporation (FDIC). “Section 4.2 – Internal Routine and Controls, Segregation of Duties,” Risk Management Manual of Examination Policies. FDIC, 2012.
http://www.fdic.gov/regulations/safety/manual/section4-2.html

[FTC 2006]
連邦取引委員会：「金融機関と顧客情報：保護ルールを順守する」、2006年、FTC
Federal Trade Commission (FTC). Financial Institutions and Customer Information: Complying with the Safeguards Rule. http://business.ftc.gov/documents /bus54-financial-institutions-and-customer-information-complying-safeguards-rule (2006).

[Hall 1959]
E.T ホール：「沈黙の言語。ダブルデイ」、1959年、
Hall, E. T. The Silent Language. Double Day, 1959.

[Hanley 2011]
マイケル・ヘンリー、ジョジ・モンテリバノ：「CMU/SEI-2011-TN-024、インサイダー脅威管理策：インサイダーの離職間際におけるデータ抜き取り検知のための中央集権化されたロギング」、2011年、カーネギーメロン大学ソフトウェア・エンジニアリング研究所
Hanley, Michael & Montelibano, Joji. Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination (CMU/SEI-2011-TN-024). Software Engineering Institute, Carnegie Mellon University, 2011.
http://www.sei.cmu.edu/library/abstracts/reports/11tn024.cfm

[Hofstede 1980]
Ｇ・ホフステッド：「文化の帰結：労働関連の価値における国際的相違」、1980年、Sage
Hofstede, G. Culture’s Consequences: International Differences in Work-Related Values. Sage, 1980.

[Human Rights Watch, India 2012]

人権監視、インド：「国連メンバーは、カースト制度差別を終了させるための行動をとるべきである。世界中で2億6千万人以上が影響を受けている」、2012年
Human Rights Watch, India. UN Members Should Act to End Caste Discrimination: More Than 260 Million Affected Worldwide. http://www.hrw.org/news/2012/05/14/india-un-members-should-act-end-caste-discrimination (2012).

[Italian Data Protection Authority 2003]
イタリア・データ保護局：「個人データ保護。法律第30条第196項」、2003年6月30日
Italian Data Protection Authority. Personal Data Protection. Legislative Decree No. 196 of 30 June 2003. http://www.garanteprivacy.it/documents/10160/2012405/DataProtectionCode-2003.pdf (2003).

[Kaplan 2001]
エレーヌ・カルパン：「告発者に対す法的保護の国際的な出現」、公開調査ジャーナル（秋／冬　2001年）
Kaplan, Elaine. “The International Emergence of Legal Protections for Whistleblowers.” The Journal of Public Inquiry (Fall/Winter 2001): 37-42.

[Lerner 2012]
キャロライン・ N・ ラーナー：「行政省庁に対する覚書」、2012年6月20日、合衆国特別弁護人局
Lerner, Carolyn N. Memorandum for Executive Departments and Agencies. U.S. Office of Special Counsel, June 20, 2012.

[OSHA 2013]
職業安全衛生管理局：「告発者保護プログラム」、2013年、合衆国労働省
Occupational Safety & Health Administration (OSHA). The Whistleblower Protection Program. United States Department of Labor. http://www.whistleblowers.gov/ (2013).

[PCI Security Standards Council 2010]
支払カード産業セキュリティ標準協議会：「支払カード産業データ・セキュリティ標準：要求事項及びセキュリティ・アセスメント手順第2.0版」、2010年、PCIセキュリティ標準協議会
Payment Card Industry (PCI) Security Standards Council. Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures Version 2.0. PCI Security Standards Council.

https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf (2010).

[Purcell 2012]
A・パーセル：「OM12-59、ソーシャル・メディア事例に係る法律顧問代理報告」、2012年、法律顧問局
Purcell, A. Report of the Acting General Counsel Concerning Social Media Cases (OM 12-59). Office of the General Counsel, 2012. http://mynlrb.nlrb.gov/link/document.aspx/09031d4580a375cd

[Silowash 2012]
ジョージ・シロワッシュ、ドウン・カペり、アンドリュー・ムーア、ランドール・トレチャック、ティモシー・シミール、ロリ・フリン：「インサイダー脅威低減のための常識ガイド、第4版」、2012年、カーネギーメロン大学ソフトウェア・エンジニアリング研究所
Silowash, George; Cappelli, Dawn; Moore, Andrew; Trzeciak, Randall; Shimeall, Timothy; & Flynn, Lori. Common Sense Guide to Mitigating Insider Threats, 4th Edition (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University, 2012. http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm

[Spring 2012]
J・スプリング、C・フート：「エンドユーザーのプライバシーに係る受動DNS収集の影響（付録CのC節）」、2012年3月英国のテディントンで開催されたインターネット・ネームの保全と信頼化（SATIN）における発表、2012年、カーネギーメロン大学
Spring, J. & Huth, C. The Impact of Passive DNS Collection on End-User Privacy (Appendix C Section C). Presented at Securing and Trusting Internet Names (SATIN) 2012. Teddington, United Kingdom, March 2012. Carnegie Mellon University, 2012. http://conferences.npl.co.uk/satin/papers/satin2012-Spring.pdf [Transparency International 2011] Transparency International. Corruption Perceptions Index 2011. http://cpi.transparency.org/cpi2011/results/ (2011).

[Transparency International 2011]
トランスペアレンシー・インターナショナル：「不正行為の知覚インデックス2011」、2011年
Transparency International. Corruption Perceptions Index 2011. http://cpi.transparency.org/cpi2011/results/ (2011).

[UN 2011]

国連（UN）人権高等弁務官：「A/HRC/19/41、差別的法律と慣行及び性的指向と性同一性に基づく個人への暴力行為：人権に関する国連高等弁務官年次報告及び高等弁務官事務局と事務総長の報告」、2011年、国連
United Nations (UN) High Commissioner for Human Rights. “Discriminatory Laws and Practices and Acts of Violence Against Individuals Based on Their Sexual Orientation and Gender Identity,” Annual Report of the United Nations High Commissioner for Human Rights and Reports of the Office of the High Commissioner and the Secretary-General, A/HRC/19/41. United Nations, 2011.

[UN 2007]
国連女性進歩局：「女性に対するあらゆる形の排除に係る代表者会議（CEDAW）国家報告」、2007年、国連女性差別撤廃委員会
United Nations (UN) Division for the Advancement of Women. “CEDAW: Country Reports,” Convention on the Elimination of All Forms of Discrimination Against Women, Country Reports. United Nations, 2007.
http://www.un.org/womenwatch/daw/cedaw/reports.htm

[USG 2007]
「合衆国政府（USG）2007年連邦規則（年次出版）タイトル45：公共の福祉。第164部第312節、技術的保護（45 CFR § 164.312(2)）」、2007年、合衆国政府印刷局
United States Government (USG). Code of Federal Regulations (Annual Edition) 2007. Title 45: Public Welfare. Part 164, Section 312, Technical Safeguards (45 CFR § 164.312(2)). U.S. Government Printing Office, 2007.

[USSC 2010]
合衆国最高裁判所（USSC）：「オンタリオ市対Quon」、2010年、合衆国印刷局
U.S. Supreme Court (USSC). The City of Ontario v. Quon, 130 S. Ct. 2619, 2631. Government Printing Office, 2010.

[Valdez 2009]
F・バルデス、P・バトレス、J・モジレンスキー：「プロセス改善における組織文化の役割」、2009年3月、SEPG
Valdez, F.; Buttles, P.; & Mogilensky, J. “The Role of Organizational Culture in Process Improvement.” SEPG North America 2009. San Jose, CA, March 2009.

[Wikipedia 2012]

ウィキペディア：「人種差別」、2012年
Wikipedia. Racism. http://en.wikipedia.org/wiki/Racism (2012).

[Wugmeister 2008]
M・ウグマイスター、A・ベビット：「従業員のプライバシーに対する合衆国とEUのアプローチの比較」、2008年、モリソンとフォスター
Wugmeister, M. & Bevitt, A. Comparing the U.S. and EU Approach to Employee Privacy. Morrison and Foster, 2008
http://www.mofo.com/comparing-the-us-and-eu-approach-to-employee-privacy-02-29-2008/

事　例　集

プラクティス 1 : 企業全体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の考慮を考慮せよ

[事例 1]

「ある抵当証券会社が、外国籍の人物をプログラマーかつ UNIX エンジニアとして雇用契約を結んだ」というある事例がある。しかし、その会社は、このインサイダーがその月初めにスクリプトエラーを起こしたことから、インサイダーに対し契約を解除すると通知したものの、その日の就業時間が終了するまで社内での滞在を許した。その後、インサイダーは就業時間中に、現場で、信頼されたスクリプトにロジック爆弾を仕掛けた。当該スクリプトは、モニタリング・アラートとログインを無効化の上、組織の 4,000 のサーバーに対するルート・パスワードを削除し、それらサーバー上のバックアップ・データを含む全てのデータを削除するものであった。インサイダーは、スクリプトを 3 か月間の活動休止状態に設定し、その後ログイン・メッセージで管理者に挨拶するようデザインした。インサイダーが会社を離れた 5 日後、他のエンジニアがこのマリシャスコードを検出した。インサイダーはその後逮捕された。判決の詳細を入手することはできない。

[事例 1 の考察]

この事例は、契約者に最早サービスが不要であると通知する前に、アカウントを直ちにロックアウトする必要性を例証するものである。組織は、従業員又は請負契約者に雇用条件の変更をいったん通知したら、警戒しなければならない。この事例において、組織は、請負契約者の就業時間終了までの滞在を許すべきではなく、契約者が会社の建物から離れるまでエスコートするべきであった。また、この事例は、システムのバックアップ・プロセスへのアクセス制限の必要性を強調している。組織は、通常の管理者及びバックアップと復旧を実施する責任者との間に、明確な職務の分離を実施するべきである。通常の管理者は、システム・バックアップ媒体又は電子的バックアップ・プロセスへのアクセス権を持つべきではない。組織は、悪意のあるインサイダーによるバックアップ媒体やその他の重要なシステム・ファイルの破壊及びバックアップ・プロセスの破壊を防ぐため、バックアップと復旧プロセスの実施を少数の選定した人物に制限するべきである。

[事例 2]

他の事例では、「政府機関が請負契約者をシステム管理者として雇った」というのがある。契約者は、重要なシステム・サーバーをモニタリングする責任を持っていた。組織は、請負契約者が業務に従事して間もなく、度重なる遅刻、欠勤及び必要時に不在であったかどにより、彼を叱責した。彼の監督者は繰り返し警告したのだが、彼の見下げ果てた実績が免職の理由となった。契約者は、この監督者に対し脅しと侮辱のメッセージを送った。このような事が、職場で就業時間中に 2 週間ほど続いた。請負契約者は、ある一つのサーバーに対する

ルート・アクセス権限を持っていたが、他のサーバーに対するルート・アクセス権限は持っていなかった。彼は特権アカウントを利用し、第 2 のサーバーにアクセスすることが可能な「.rhosts ファイル」[4]を作成した。彼はいったん第 2 のサーバーにアクセスすると、マリシャスコードを挿入した。このコードは、データ量の合計があるポイントに達したとき、組織の全ファイルを削除するものであった。マリシャスコードは、彼の行為を隠ぺいするため、システム・ロギング履歴ファイルを無効化するとともに、マリシャスコードの実行後に全てのトレースを削除するものであった。請負契約者は契約の解除後、システム管理者に対し何度も繰り返しマシンとサーバーが正しく機能しているかどうかを問合せたが、このことが組織を不審がらせることとなった。組織は、マリシャスコードを発見し、システムをシャットダウンするとともに、同コードを除去してシステムのセキュリティと完全性を復旧させた。請負契約者のデータ削除は不成功に終わったのである。彼は逮捕され、10 万 8 千ドルの損賠償金の支払い及び 15 か月の禁錮刑、並びに釈放後 3 年間の保護観察処分が宣告された。彼は、組織への求職申し込みにおいて、前の雇用者がコンピュータ・システムの悪用から彼を解雇したことについて報告することを怠ったっていた。

[事例 2 の考察]

組織は、信頼したビジネスパートナーとの契約において、請負契約者が組織自身のポリシーにつりあったレベルの身辺調査を受けることを契約条項に含めるべきである。この事例において、契約会社が身辺調査を従業員に対して実施していれば、悪意のあるインサイダーが雇用されることはなかったはずである。

プラクティス 2：ポリシーと管理策を明確に文書化して、首尾一貫して執行せよ

[事例 1]

「ある政府機関が、ソフトウエア・エンジニアのリーダーとしてインサイダーを雇った」というのがある。インサイダーは被害組織において、ソフトウェア一式の開発チームを率いた。組織は最初のソフトウェア一式の実行時、大きな問題を発見した。そこで、組織の管理者はインサイダーに対し、すべてのソースコードを文書化するとともに、コンフィギュレーション管理の実施と開発プロセスの中央統制を求めた。インサイダーは、組織が将来ソフトウェア一式の開発をアウトソースするとともに、彼を降格及び給与削減の上、他の部署に配置転換する予定であることを後になって気づいた。彼は、プロジェクトが未だ彼の統制下にある間に、プロジェクトの移行を妨害するため、不明瞭な方法でソースコードを記述した。インサイダーは、不当な扱いに対する不満を提出の上、休暇をとった。組織は、提出された

[4] .rhosts ファイルには、パスワードの利用なしに、コンピュータにリモートからログインすることが許されるユーザーとマシンの組み合わせリストが含まれている。システムの中には、ユーザーがホーム・ディレクトリーに.rhosts ファイルを作成することが許されているものもある。

不満を却下し、インサイダーは辞職した。インサイダーは辞職に先立ち、リムーバル媒体にソースコードをコピーするとともに、パスワード付で暗号化した。それからインサイダーは、彼のラップトップからソースコードを削除し、ラップトップを辞職時に返却した。彼は、ラップトップの返却前にファイルを消去するため、意図的にソースコードを削除したと説明した。とはいえ、彼がコピーを持っていることについては明らかにしなかった。組織は、彼が当該システムの唯一のソースコードのコピーを削除したことに気づいた。そのシステムは、安全関連のシステムであり、当時の生産活動に利用されていた。システムの実行可能ファイルは機能し続けたが、組織はソースコードを紛失したことから、バグを修正することもシステムを強化することもできなかった。最終的には、捜査員が彼の自宅から暗号化されたソフトウェアのコピーを発見した。9 か月後、そのインサイダーはついに彼の罪を認め、暗号鍵を提出した。インサイダーは逮捕されて有罪判決を受け、一年間の禁錮刑及び 1 万 3 千ドルの損害賠償金の支払いを宣告された。

[事例 1 の考察]

この事例において、組織は、ソフトウェア開発に対する明確なポリシー、手順及びプロセスを策定の上、開発を実行するべきであった。組織がすべてのソフトウェア・プロジェクトにこれらの要求事項を順守させていたなら、前述のインシデントの発生を避けることができたと思われる。その理由は、開発者に対する雇用者の期待事項を開発者が知ることができたからである。さらに、組織は、これがミッション・クリティカル・システムであったことから、変更管理プログラムを設けるべきであった。このプログラムは、ソフトウェア・ベースラインを維持するため、ソースコードを変更管理プログラム・マネージャに提出することを要求するものである。これは、当該インサイダー以外の者にソースコードのコピーを確実に保管させるものである。

[事例 2]

他の例では、「ある政府機関の IT 部門がネットワーク管理者としてインサイダーを雇用した」というのがある。インサイダーは、同組織のネットワークを構築した人物であり、ネットワークがどのように機能するかについての正確な知識は無論のこと、ネットワーク・パスワードを持つ唯一の人物であった。インサイダーは、どのようなネットワーク管理者の新たな追加についても、承認することを拒否した。組織は、インサイダーの勤務成績が好ましくないことについて、彼を厳しく叱責した。インサイダーは、困難に直面してその後同僚を脅したことで、他のプロジェクトに配置転換させられた。組織は、インサイダーがネットワーク・パスワードを手放すことを拒否したことから雇用を打ち切り、そして彼は逮捕された。組織は、組織の主コンピュータ・ネットワークから 2 週間近く締め出される結果となった。

インサイダーの同僚は彼の逮捕後、彼が秘密の場所に不正を働くアクセス・ポイントをイ

ンストールしていたことを発見した。これは、誰かが正当なパスワードを利用せずに組織のシステムのリセットを企てた場合、システムを停止させるというものであった。インサイダーは警察に複数のパスワードを提出したが、どのパスワードも無効であった。インサイダーは後になって、インサイダーが信頼していた一人の政府機関職員との面会の場で、本物のパスワードを手放した。インサイダーは、標準セキュリティ慣行に従っていたと主張し、自身の行為を弁護した。インサイダーは有罪判決を受け、4 年間の禁錮刑を宣告されるとともに、損害賠償金支払い額の聴聞会の結論を待ち受けている。組織のインシデント関連の損失は、20 万ドルから 90 万ドルの間に及ぶものである。

[事例 2 の考察]

この事例は、組織が首尾一貫してポリシーと手順を実施する必要性を例証するものである。インサイダーは、手薄な監督下で組織のネットワークをコントロールすることができ、単一の障害発生原因となっていた。組織内従業員の一人以上（少なくとも二人）が、組織のネットワークの知識とアクセス権を持つべきである。このことが、従業員の喪失又は従業員の悪意のある行為によるシステム故障の可能性を削減することになる。また、他の管理者がハードウェアとソフトウェアの変更に伴うネットワークをモニタすることで、システムのチェック・アンド・バランスが可能となる。

プラクティス 3 : 全従業員に対する定期的セキュリティ訓練に、インサイダー脅威意識向上を組み入れよ

[事例 1]

「ある税務署が、マネージャとしてインサイダー（女性）を雇った」というのがある。彼女は、組織のコンピュータ・システムに対する詳しい知識を持ち、組織が新たに導入したコンピュータ・システムの設計を支援した。インサイダーは管理者に対して、彼女の部門の活動はこの新システムによらず処理されるべきであると確信させた。彼女が属する部門の全ての記録は、紙の文書で維持され、小細工するのが容易であった。彼女は 18 年以上にわたり、200 枚以上の不正な小切手を振り出し、総額で数百万ドルに達した。彼女には、この企みに特定の役割を持たないインサイダーとアウトサイダーからなる少なくとも 9 人の共犯者がいた。彼女のアウトサイダー共犯者の一人は姪であり、姪は偽会社の銀行口座に小切手を振込み、そこから金を共犯者に分配していた。銀行の出納係が 40 万ドル以上もの不審な小切手を報告したことから、インシデントが発覚した。彼女は逮捕され、有罪判決を受け、4,800 万ドルの返還、1,200 万ドルの国税及び 320 万ドルの州税の支払いが宣告された。彼女はまた、17 か月半の禁錮刑を宣告された。このインサイダーの動機の一つは、彼女が寄付者として、同僚に私立学校の授業料、葬儀費用、衣料購入などのための金銭をあげることに喜びを感じていたことであった。インサイダーは、同僚に対して相当な遺産を受け取った

と話すことで疑惑を回避していた。また、この気前のよいインサイダーは、それぞれの家の価値が数百万ドルにも及ぶ複数の家、ぜいたくな車、高級な衣料やアクセサリー、宝石、その他のぜいたく品の購入に相当な金を費やした。インサイダーの逮捕時、彼女は銀行口座に8百万ドルの預金を持っていた。インサイダーは、明らかに精神的幼児性外傷を患っており、このことがドラッグとアルコールの乱用及び多額の賭け事の習慣に陥らせた。

[事例1の考察]

仮に、組織が不審なインサイダー行為を示す指標についての訓練を従業員に実施していたなら、このインシデントはより早く発見されていたに違いない。このインサイダーの事例は、他の者にとっては近づきがたい彼女の状況に対して、ある手がかりをつかませるものであった。さらに、彼女には、ドラッグやアルコールの乱用及び賭け事の習慣があった。仮に、従業員の誰かが、これらの習慣を不審に思えば、それら不審事象がより早く報告されていたかもしれない。

[事例2]

他の事例では、「不満を抱く従業員が、会社の企業機密の入手を目的として、職場のコンピュータにハードウェア・キーストローク・ロガーを設定した」というのがある。組織が図らずもそのインサイダーを解雇した後、今や元従業員となっているそのインサイダーが、会社で仕事中の非技術職の従業員を強要して、同装置を取り戻させようとした。その従業員はその装置がキーストローク・ロガーであるとは知らなかったが、インサイダーにそれを渡すことにリスクを感じ、管理者に通知した。フォレンジックの結果は、インサイダーが少なくとも一回、解雇される前に同装置を外したこと及び仕事中キーストローク・ファイルを彼のコンピュータに移動させたことが明らかとなった。

[事例2の考察]

この事例において、物理的アクセスを含むネットワーク・システムとアカウントに係る異常な要求に対して、非技術職の従業員は間違いなく用心深かったことから、キーストローク・ロガーが発見されたのである。仮に、組織が従業員に対する訓練において、ソーシャル・エンジニアリングに注意し認識させていれば、組織はこのようなリスクを削減することになる。

プラクティス4: 雇用プロセスの最初から、不審な又は破壊的な行為に対するモニタと対応を開始せよ

[事例1]

最近のある事例において、「組織が請負契約者を雇いシステム管理者の業務を実施させた」

というのがある。その請負契約者の会社は、雇った組織に対して彼の身辺調査が実施済であることを口頭で告げた。請負契約者はその後、組織のシステムを危殆化し、組織の顧客数百万人に及ぶ秘密データを取得した。捜査の結果、その請負契約者には保護されたコンピュータを違法にアクセスした犯罪歴があることが判明した。

[事例 1 の考察]

この事例は、組織が契約する際、契約上で契約の相手方に従業員の身辺調査の実施を求める必要性を例証するものである。

[事例 2]

他の事例では、「大規模な輸送・倉庫会社が、経営陣レベルの責任者としてインサイダーを雇った」というのがある。インサイダーは 11 年の雇用期間の後、会社における最高の信任を得た。しかしながら、彼には被害組織に雇われる以前に、彼が勤めていた他のいくつかの会社から金を盗んだことがあった。そして、このインサイダーは有罪となったが、施設外勤務制度（work release）で刑に服した。彼は、彼の行為に対して身をきれいにしたと主張した後、被害組織に雇われ、経営陣レベルの職に昇進したのであった。メディアは、インサイダーの革新的なマネジメントと運用経験をしきりと称賛した。インサイダーは最後の 2 年間の雇用期間において、彼の雇用者を騙すための仕組みを案出し実行した。インサイダーは彼の部門に請求された送り状の価格をつり上げ、支払いの一部を集めた。さらに、インサイダーは、共犯者が立ち上げた会社に対して、架空のサービスに対する支払を行った。共犯者は、この見返りとして支払いの一部をインサイダーに戻した。被害組織の通常の財務監査において、インサイダーが 50 万ドル以上盗んだ行為が明らかとなった。インサイダーは、6 年の禁錮刑の宣告を受けるとともに、全額賠償を命じられた。

[事例 2 の考察]

この事例は、組織が雇用を決定する前に、採用予定者に対する身辺調査を検討する必要性を例証するものである。経営陣は、候補者に対する完全な身辺調査の結果を見極めなければならないし、候補者に役職を提示する前に、組織がそのリスクを享受したいかどうか判断しなければならない。また、組織は、信頼するビジネスパートナーとの法的合意事項に、組織の身辺調査に対する要求事項を明示することを確実にしなければならない。

[事例 3]

他の興味深い事例として、「映像技術制作プロバイダー組織が、ネットワーク管理者としてインサイダーを雇用した」というのがある。この被害組織は、新監督者を雇用した。新監督者は 12 人～16 人の従業員を解雇したものの、そのインサイダーを昇進させた人物でもあった。インサイダーは、バックドアをインストールして、組織に損害を与える計画がある

ことを同僚に話した。しかし、その同僚は最近の解雇状況から、その計画について新監督者が怖くて話せなかった。インサイダーは、職場で奇妙な行動をとった。彼は自分への電話に対応する際、「王だが」又は「大統領だが」と名乗ったのであった。インサイダーはまた、ビデオカメラを組織のコンピュータ・ルームに設置し、自分が「君達を監視している」と言うために電話を入れたりした。

インサイダーは実に欺瞞的であった。インサイダーは、組織が彼を雇ったとき、資格を持った Cisco Network エンジニアであると偽りの主張をし、そのことでヘッドハンターから推薦されたのである。組織はこの主張の確認を怠った。また、インサイダーは、暴力行為の犯罪歴を隠ぺいしたが、これには凶器による暴行、配偶者に対する肉体的損傷、小火器の所有、2 つの社会保障番号の不正利用が含まれていた。また、このインサイダーは、自宅に突撃用武器を保有しており、それを同僚は以前に見たことがあった。その半自動式の武器は、インサイダーと同居している義兄弟の登録となっていた。

組織は、インサイダーが海外出張を求められた後に、抵抗し、それを回避しようとしたことから、彼に不審を抱き始めた。インサイダーは、飛行が嫌いだと主張したにもかかわらず、パイロットのライセンスを持っていた。また、インサイダーは、彼のアイデンティティ盗難という異様な出来事のせいで、正規の出生証明書がないと主張した。組織は、インサイダーが Cisco Network 認定者でない事実を知り、その後解雇した。インサイダーは離職後も、会社が貸与したラップトップを返却しなかった。組織は、彼がラップトップを返却するまで、退職金の支払いを拒否した。インサイダーは返却要求に従ったものの、ラップトップには物理的な損傷があり、かつ、そのハードディスク・ドライブのデータは消去されていた。

組織はインサイダーの離職後、インサイダーが繰り返し組織のサーバーにリモート・アクセスを行っていることに気づいた。組織はインサイダーに止めるよう求めたが、彼はそのようなことはしていないと否定した。組織はインサイダーからの攻撃を予測し、コンピュータ・セキュリティ・コンサルタントを雇った。コンサルタントは、組織のファイアウォールにおいてそのインサイダーの IP アドレスをブロックするとともに、彼のアカウントの削除、バックドアの有無のチェック、及び不正アクセスの監視を行った。しかしながら、コンサルタントは、インサイダーがアクセスしたサーバーの一つのチェックを怠った。コンサルタントはその後フォレンジック調査を実施し、インサイダーが VPN アカウントを利用してインサイダーの離職とインシデントの間の 2 週間にわたりログインした事実を検出した。組織は、インサイダーが離職する前に設定したこれらアカウントの存在に気づいていなかった。これらのアカウントは、彼の監督者、販売担当副社長、及び組織の最高財務責任者の名前で登録されたものであった。コンサルタントは、理由は分からないが、それらのアカウントが不審なものとは考えなかった。また、コンサルタントは、インサイダーの Citrix アクセスを無効化することを怠ったため、インサイダーによるダイアルイン・アクセスを許す結果と

なった。インサイダーは、彼の自宅のコンピュータからVPNアカウントを利用し、組織のCitrixサーバーに対するリモート・アクセスを行った。インサイダーは、Citrixサーバーにアクセスし、極めて重要なファイルを削除するとともに、同サーバーを操作不能にした。インサイダーは逮捕され、有罪判決を受け、禁錮一年の刑を宣告されるとともに、メンタルヘルス・カウンセリングを受けることを命じられた。

[事例3の考察]

この事例において、組織は次を実施することを無視していた。

- 従業員の雇用前に資格証明書を確認すること。
- 完全な身辺調査を実施すること。
- 適切なアカウント管理手順ポリシーと手順を実施すること。

組織は、個人が主張する企業の認定証又は資格証明書の確認を含め、完全な身辺調査を実施していたなら、このような状況になることを避けることができたに違いない。この事例において、組織は、インサイダーを身辺調査プロセスで決して合格させるべきではなかった。

さらに、組織は、潜在的なインサイダー脅威に対するいくつかの早期警告サインに気付くべきであった。それらは、インサイダーによる次の3件である。

- 同僚に対し、組織のシステムにバックドアを設定したと語ったこと。
- サーバールームに監視カメラを設置し、彼が同僚を監視していると言って、同僚に電話したこと。
- 組織の求めに対して抵抗し、かつ回避しようとしたこと。

同僚と経営陣は、これらの事象に対する懸念を高めるべきであった。他の従業員の行動に懸念を抱く全ての従業員は、報復を恐れることなく、そのような問題を報告できるようにするべきである。第三者がホストとなる密告連絡先（tip line）のような匿名による従業員の報告システムの利用可能性は、情報の提供を恐れる同僚を勇気づけるに違いない。そして、このような情報が、組織によるインサイダーに対するさらに徹底的した調査を推し進めることにつながるのである。

プラクティス5：職場環境における否定的問題を先取りして管理せよ

[事例1]

「ある製造会社が、販売要員としてインサイダーを雇った」というのがある。その組織は、販売要員に対して定期的に会社固有の顧客を更新し、追跡システム（業績評価）を先導することを求めた。インサイダーは、求めに応じて追跡システムを更新しなければ解雇されると

の警告を受けたが、そのようにすることを無視した。そこで組織は、インサイダーを解雇する代わりに、2,500 ドルの減俸による罰則を適用した。インサイダーは、不満を抱き、競合会社への転職を探し求めた。インサイダーは競合会社に対して、彼が解雇された場合は顧客情報を持ち出す計画であることを知らせた。被害組織がインサイダーの行動に不審を抱き始めたことから、インサイダーが競合会社の連絡相手に対し、全ての E メール交信を削除することを求めた。インサイダーは、その競合会社から採用の申し出を受けた。2 週間後、インサイダーは、被害組織のコンピュータ・システムにアクセスし、彼の自宅のコンピュータに顧客記録をダウンロードした。その 2 日後、インサイダーは被害組織に E メールを送り、直ちに辞職する旨を伝えた。次の日、インサイダーは受益組織に再就職した。インサイダーは直ちに被害組織の顧客と接触し、再就職した組織への勧誘を開始した。被害組織は、インサイダーの行動を発見するやいなや、捜査機関に届け出た。捜査機関は、インサイダーのコンピュータを調査し、60MB のデータが削除されていたこと、及びコンピュータのフラグメンテーションが何回か解消されていたことを指摘した。被害組織は、インサイダー及び受益組織に対する民事訴訟を行った。それら訴訟の結果は不明である。

[事例 1 の考察]

この事例において、インサイダーは彼の業績問題に対し警告を受けていたが、組織が減俸処置をとった際、さらに不満を抱いた。被害組織は、インサイダーが警告を受けた時又は彼の俸給が減額された時のいずれかにおいて、彼を監視リストに置くべきであった。組織がこの処置が行っていれば、インサイダーによる顧客データの開示以前に、止めさせることができたかもしれない。また、この事例は、非開示合意、受け入れ可能な利用合意、又は非競合合意でさえも、必要であることを強調するものである。

[事例 2]

他の事例では、「被害組織の銀行が、レイオフに不満を抱いた大量の従業員の辞職のきっかけを作った」というのがある。これらのインサイダーは辞職に先立って、被害組織の顧客データベースから情報をコピーの上、ワード文書にペーストしてディスクに保管した。このようなインサイダーの一人は彼の退職日に、非勧誘合意に署名を行ったのであるが、後にリモート・アクセスを介して顧客情報を盗み出したのである。このインサイダーと元同僚は、これらの事象が発生する 6 か月前、新たな会社を立ち上げ、彼らと打ち合わせ済の同僚を雇うことを計画していた。被害組織は、このインサイダーに対する民事訴訟を行った。

[事例 2 の考察]

この事例は、組織が積極的にデータを保護する必要性を強調している。レイオフは組織の緊張とストレスを高め、このことが否定的な雰囲気に結びつけることから、経営陣はこのような雰囲気がもたらすインサイダー脅威リスクに気づくべきである。組織は、組織のリスク

マネジメント・プロセスの一部として、重要な IP（知的財産）を識別するとともに、不正な改ざん、開示又は削除を防止する適切な対策を講ずるべきである。仮に、この事例における被害組織が、機微ファイルに対する付加的な監査を含む技術的対策を講じていたならば、早期発見と防止が可能であったかもしれない。

プラクティス 6：汝の資産を知れ

[事例 1]

「ある病院施設が、契約による警備員としてインサイダーを雇った」というのがある。インサイダーは、インターネット地下組織に深く係っており、ハッキング・グループのリーダーであった。インサイダーは、被害組織において監督下に置かれることなく、夜間だけ働いていた。インサイダーの不正行為の大部分は、暖房、換気及び空調（HVAC）コンピュータに関連するものであった。HVAC コンピュータは鍵のかかった部屋に置かれていたが、インサイダーは彼のセキュリティ・キーを利用して、同コンピュータへの物理的アクセスを行っていた。インサイダーは、二日間にわたって HVAC コンピュータに計 5 回リモート・アクセスした。さらに、インサイダーは、ナースステーションのコンピュータにアクセスした。このコンピュータは、被害組織の全てのコンピュータに接続されており、また、医療記録及び病棟情報を記憶していた。インサイダーは、組織への攻撃に様々な方法を利用したが、その中にはパスワードクラッキング・プログラムとボットネットが含まれていた。インサイダーの悪意のある行為は、HVAC システムを不安定な状態に陥れ、ついには 1 時間の中断をもたらした。インサイダーとインターネット地下組織の構成員は、分散サービス妨害（DDoS）攻撃を不詳の標的（unknown target）に対して行うため、被害組織のコンピュータ・システムを利用することを計画していたのである。そして、あるセキュリティ調査員が、インサイダーのオンライン活動を発見した。インサイダーは有罪判決を受け、31,000 ドルの損害賠償金の支払い命令、及び 9 年 2 か月の禁錮刑とその後 3 年間の保護観察処分が下された。

[事例 1 の考察]

この事例は、いかに単一のコンピュータ・システムが組織に対し相当な被害を及ぼすかを例証するものである。この事例において、攻撃が病院施設で行われたことから、被害は生命を脅かすことにもなりかねなかったのである。組織の環境を制御及び変更する HVAC システムの改ざんは、温度感受性持つ薬品や供給品及び温度の変化を受けやすい患者に影響を及ぼすことができたのである。インサイダーは、セキュリティをバイパスする追加手段により、患者記録の改ざんや毀損を行い、患者の手当て、診断及び管理に影響を及ぼすことができたのである。組織は、管理者と情報セキュリティ・チームと共同し、組織内の他の部門の重要なシステムを特定することが重要である。この事例において、HVAC コンピュータは施錠された部屋に設置されていたが、データセンターやサーバールームは施錠されていな

かった。これらに対しても付加的な防護対策を講ずることができたはずであり、それによりインサイダーによるシステムの巧みな不正操作を避けることができたかもしれない。

さらに、インサイダーは、組織内の他の重要なシステムにアクセスすることが可能な、ナースステーションのコンピュータにアクセスすることができた。仮に、組織が、危殆化されたワークステーションが組織内の他の部署に対しても影響を及ぼす可能性があることについて完全に理解していたなら、組織はこのようタイプの攻撃を防止するため、追加の防護層を構築することができたと思われる。

プラクティス 7: パスワードとアカウントの厳格な管理ポリシーと厳格なプラクティスを実施せよ

[事例 1]

「請負契約者であるインサイダーがかつて、ソフトウェア開発者及び試験員として被害組織に雇われていた」というのがある。被害組織は、インサイダーの成績不良を理由に契約を解除したが、彼の離職に伴う共有アカウント・パスワードの変更を怠ったのである。インサイダーは、その後の別の雇用者が貸与したラップトップを利用して、被害組織の 24 に及ぶユーザーアカウントに対しリモート・アクセスを行った。インサイダーは、「不正アクセス又はアクセスの企ては犯罪に係る違反行為である。このコンピュータ・システムは監査対象となっている。不正利用に対しては連邦法による罰則が適用される」と表示されたバナー警告を無視した。インサイダーは、彼の行動を隠ぺいするため、*rhost*[5]ファイルを編集した。被害組織のある女性従業員が、彼女のユーザー・ネームが僅か数時間前に、彼女のコンピュータにログオンするために利用されていたことに気づいた。彼女は実際にログオンしていなかったので、インサイダーの現及び以前の雇用者の共同による捜査が進められた。インサイダーの現雇用者のセキュリティ要員が侵入経路を追跡したところ、インサイダーのラップトップにたどり着き、彼と対決した。インサイダーは、次のようないくつかの主張について自信をもって言い張った；「私は被害組織から解雇されたのではなく、契約が更新されていなかっただけである。以前の同僚が、私に問題解決のためログオンすることを依頼したのである。私は、被害組織のネットワークの欠陥を見つけるため、ブレークイン・ゲームを以前の同僚と実施したのである」。インサイダーは逮捕され、有罪判決を受け、未指定の罰金と刑罰だけでなく、2 年間の保護観察処分が下された。インサイダーは、約 130 万ドルの価値がある企業機密が記憶されている 13 のシステムを危殆化した。

---

[5] .rhosts ファイルは、パスワードを利用することなくリモートからコンピュータにログインすることを許すため、ユーザーとマシンの組み合わせリストを内蔵している。あるシステムでは、ユーザーがホーム・ディレクトリーに.rhosts ファイルを作成することを許している。

[事例 2]

別の事例は、「アカウント管理の必要性を例証している」というのがある。インサイダーは、これまで変更されたことがない共有アカウントを利用し、システムにログインすることができた。

[事例 1、2 の考察]

組織は、個人が組織を離れる際、当人がアクセスに利用していたすべてのアカウントに対するパスワードを変更しなければならない。このプロセスには、誰がどのアカウントに対するアクセス権を持っているかを文書化するなどの、注意深いアカウント管理が含まれる。

[事例 3]

他の事例では、「電子商取引会社がチーフ・プロジェクト・エンジニアとしてインサイダーを雇った」というのがある。被害組織は、インサイダーを主要プロジェクトから外し、その後雇用契約を解除した。後になって、伝えられるところによれば、被害組織の従業員であるインサイダーの共犯者が、かつてインサイダーが利用していたプロジェクト情報を記憶しているサーバーに対するパスワードを、インサイダーに与えたとされている。いくつかの情報源によれば、インサイダーは復讐目的でプロジェクトファイルの削除を目論んだとされている。他の情報源では、プレゼンテーションの間にインサイダーがファイルを隠し、彼の共犯者がファイルを復旧することができれば、共犯者はヒーローとなり解雇を免れることをインサイダーが目論んだと主張している。実際、インサイダーはファイルを削除したが、組織は喪失したデータを復旧させることができた。プロジェクトは、260 万ドルの価値があった。インサイダーと彼の共犯者は逮捕されたが、インサイダーに対する有罪宣告はなかった。

[事例 4]

第 4 番目の事例は、「共犯者がアカウント・パスワードを元従業員と共有し、元従業員は会社のデータにアクセスして同データを削除した」というものである。

[事例 3、4 の考察]

組織は、アカウントとパスワードに係る明確なポリシーを持つ必要がある。ポリシーはアカウント情報が組織外のいかなる者とも共有されるべきではないと明言すべきであり、ポリシー違反に対してはそれ相応の取り扱いをしなければならない。このようなポリシーは、インサイダーと彼の共犯者の活動を抑止することができたかもしれない。

プラクティス 8：職務の分離と最小特権を強化せよ

[事例 1]

「インサイダーが、金融・投資機関の副社長兼上級税務システム分析家として、8 年以上に及び勤務した」というのがある。インサイダーは、彼の業務責任事項の一つとして、組織のシステムとネットワークに対するアクセス特権を持っていた。組織がインサイダーの雇用を終結したとき、組織は直ちに彼のアクセス特権を無効化するとともに、組織の信頼されたビジネスパートナーに対し、彼らのシステムに対する彼のアクセス権を同様に無効化するよう通知した。インサイダーは最後に職場を離れた後、未だ無効化されていないアカウントを利用して、ビジネスパートナーのシステムの一つにリモートからログインし、同システム上にある彼の監督者の利用されていないアカウントを危殆化した。そのビジネスパートナーは翌日、インサイダーのアカウントを無効化したが、彼が前日にとった不正な活動に気づいていなかった。インサイダーは、危殆化された監督者のアカウントは無論のこと、その後彼が設定した他のアカウントを利用して、ビジネスパートナーのシステムを次の月内にざっと 50 回ほどアクセスした。彼はこの期間、顧客データへのアクセス、システム内の情報の改ざん、及び彼の雇用中に彼が従事していたデータとコードの一部を破壊した。後に、インサイダーの活動が内部の従業員及び連邦捜査員によって発見されたが、この事例の結果は不明である。このインシデントに関連した被害組織の損害額は、総計で 138,000 ドルと見積もられた。

[事例 2]

他の事例には、「ハイレベルの役員が組織のシステムに対するアクセス特権を持っていた」というのがある。

[事例 1、2 の考察]

一般に、組織内の高い地位にある人物に対して、このようなレベルのアクセス権が必要とされることはない。この人物は、重要なビジネス・データの変更について他の者による確認を求めることなく、それを実施することができた。役員はソーシャル・エンジニアリング攻撃に共通した標的である。組織は、仮にある人物が追加のアクセス権を求めた場合、よりきめ細かい管理と追加のロギング及び監査を施した別途のアカウントを作成することを考慮すべきである。

プラクティス 9 : 全てのクラウド・サービスに対して、明確なセキュリティ合意事項を、特にアクセス制御とモニタリング機能について定めよ

[事例 1]

「リモート・アクセスに USB・VPN トークンを利用しているある小売業の組織が、ネットワーク・エンジニアを解雇した」というのがある。インサイダーは解雇される前に、偽の従業員の氏名でトークンを作成した。インサイダーは解雇の 1 か月後、彼が作成した偽の氏名を使って IT 部門と連絡をとり、VPN トークンを活動化するよう説得した。インサイダーはその数か月後、その VPN トークンを利用して仮想マシンの削除、ストレージ・エリア・ネットワーク（SAN）のシャットダウン、及び E メール・メールボックスの削除を行った。組織は、運用の再開に 24 時間もの IT スタッフの作業を要したとともに、20,000 ドル以上の出費となった。

[事例 2]

他の事例では、「製薬会社の上級管理者が IT 従業員のインサイダーと論争した」というのがある。そのインサイダーは辞職したが、インサイダーの監督者と彼の親しい友達は、彼を契約者として会社に留めるようにと会社を説得した。インサイダーは数か月後、会社から完全に去った。インサイダーは、彼のホーム・ネットワークを利用し、被害組織のサーバーに一つのソフトウェアをインストールした。それからインサイダーは、レストランのインターネット接続と危殆化されたユーザーのパスワードを利用し、サーバーにアクセスした。このサーバーは、組織の E メール、発注追跡及び財務管理システムのホストの役割を果たす仮想マシンを削除するため、彼が前もってソフトウェアをインストールしていたものであった。この攻撃は、組織の業務を数日にわたって停止させた。インサイダーによる攻撃のための接続は、攻撃時間帯のレストランでの彼の注文によって発見された。インサイダーは逮捕され、罪状を認めた。

[事例 1、2 の考察]

これらの事例は、組織が自身のプライベート・クラウドを利用しており、インサイダーは重要なプロセスをホスティングしている仮想マシンに対する管理者用リモート・アクセス権を持っていた、というものである。組織は、組織のシステムにどのようなリモート・アクセス権があり、それらにどのようなリスクが関連するのかについて、注意を払う必要がある。仮想マシンは迅速に展開することができるが、また迅速に破壊することもできるのである。組織は、問題に迅速に対応するため、仮想環境のモニタリングとロギングに注意を払うべきである。また、組織は、仮想サービスの変更が可能なツールのリモート・アクセスについて、統制又は禁止を行わねばならない。

プラクティス 10：特権ユーザーに対する厳格なアクセス制御とモニタリング・ポリシーを制定せよ

[事例 1]

「処方薬給付計画管理に責任を持つ被害会社が、コンピュータ・システム管理者としてインサイダーを雇った」というのがある。被害組織が親会社からの資産の分離独立による新会社の設立後、インサイダーを含む被害組織のスタッフは、組織のコンピュータ・システム管理者がレイオフされるかもしれないことを論じた内容の E メールを回覧した。インサイダーはレイオフされることを恐れ、既存のコンピュータ・コードを改ざんして論理爆弾を作成し、新たなコードを被害組織のサーバーに挿入した。レイオフが行われ、インサイダーは雇用を維持されたが、彼は論理爆弾を除去しなかった。インサイダーは、論理爆弾が指定された日に爆発しなかったことから、論理爆弾のロジックを変更してエラーを修正した。他のコンピュータ・システム管理者がシステム・エラーを調べているときに、この論理爆弾を発見した。その後 IT セキュリティ要員が破壊的なコードを無効化した。この論理爆弾は、70 以上のサーバーの情報を破壊することができ、それには特定患者の薬物相互作用に係る重要なデータベース、顧客の臨床的検討・払い戻し・請求・管理型医療に関する申込書、医者からの新処方の着呼、補填範囲の決定申請書、並びに会社の財務、薬局補修進捗管理、ウェブと薬局の統計報告、及び従業員賃金台帳インプットが含まれていた。このインシデントは、論理爆弾の作成から発見まで 14 か月にも及んだ。発見の遅れは、インサイダーが彼の誕生日に論理爆弾を爆発する決定によるものとされている。インサイダーは、逮捕され、有罪判決が下され、損害賠償金 81,200 ドルの支払いと 30 か月の禁錮刑が宣告された。

[事例 2]

他の事例では、「IT 会社が IT 管理者としてインサイダーを雇った」というのがある。このインサイダーは、解雇されていた他の従業員とデートしていた。インサイダーは、経営陣に対して彼女を再雇用せよと、脅迫メッセージを送った。組織は、この行為に対して彼を解雇した。彼は、組織がインサイダーのアクセス権を無効化する前に、他のユーザーアカウントを設定していた。また、インサイダーはこの間、顧客のファイルを削除した。IT 会社は、インサイダーの解雇後の失業補償請求を拒否した。インサイダーは、彼が前もって設定しておいたバックドア・アカウントを利用し、何度か組織のサーバーにアクセスした。時には、彼のホーム・ネットワーク、またある時は公共ネットワークを利用してアクセスした。インサイダーは、2 人の顧客データを削除し、そのうちの一人の顧客が会社のサーバーにアクセスするのを困難にした。IT 会社は、政府機関に連絡して捜査支援を依頼し、ユーザーアカウントとログからインサイダーを特定した。インサイダーは逮捕され、コンピュータ侵入の罪を認めた。

[事例 1、2 の考察]

これらの両事例とも、インサイダーは確認されることなく、システムを変更することができたのである。最初の事例では、インサイダーが製造システムに論理爆弾を仕掛けた。第 2 の事例では、インサイダーが許可又は確認されることなくアカウントを設定することができた。このようなインサイダーの活動は、適切なモニタリングとアクセス制御管理策が実施されていれば、止めさせられたか又は早期発見につながったと思われる。

このような管理策は、他の事例においても効果的であると思われる。その例として、外国人投資家によるソースコードの不正操作がある。被害組織は、このインサイダーがコンピュータ科学の学位を持っていることから、組織の取引システムのソースコードに対するアクセス権を与えた。彼は、このアクセス権を利用して、発見されることなく取引損失を隠ぺいすることができるバックドアを構築した。この損失額の総計は、数年間で 700 万ドル近くにもなった。

プラクティス 11：システム変更管理を制度化せよ

[事例 1]

「投資銀行である被害組織が、コンピュータ・スペシャリストとしてインサイダーを雇った」というのがある。インサイダーは、債権トレーダーがどの債権の売り買いをするべきか、その決定を支援するリスクアセスメント・プログラムを作成した。このインサイダーは後になって、同じ組織から有価証券トレーダーとして雇われた。理由は不明であるが、インサイダーは経営陣に怒りを覚えるようになった。彼は、年俸 125,000 ドルの収入を得ていたが、ボーナスに不満を抱いていたようである。インサイダーは、復讐心に動機づけされ、彼がコンピュータ・スペシャリスト当時に作成したリスクマネジメント・プログラムに論理爆弾を仕掛けた。その論理爆弾は少しずつ取引のリスクを増加させたことから、トレーダーは彼らの取引がますますリスクを帯びることに気づくことなく、より危険な取引をするようになった。インサイダーは、組織と組織の顧客が年間を通じ 100 万ドル損失するよう企てた。あるプログラマーがプログラムのコードを変更しようとしたとき、誰かがそのプログラムを改ざんしたことに気づいたことから、論理爆弾を発見した。組織は、論理爆弾の爆発に伴う大きな損失の全てを防止することができたが、プログラムの修正に 5 万ドルを費やした。インサイダーは後になって、そのプログラムを個人的な利用のため作成したものであると主張したが、あるトレーダーがインサイダーのそのプログラムを利用して相当額の利益を得たことを彼が明らかにしたことから、この主張は崩れた。インサイダーは解雇され、逮捕され、そして有罪判決が下されたが、刑の宣告内容は不明である。

[事例 2]

他の事例として、「金融サービス会社がシステム管理者としてインサイダーを雇った」というのがある。インサイダーは、ボーナスが通常の半分になると聞いたので、彼の監督者に不平を言った。インサイダーは、組織が従業員のボーナスをカットすると発表したとき、組織の UNIX ベースのネットワーク上に、論理爆弾を構築し仕掛けることで応酬した。その論理爆弾は、本社の約 2,000 のサーバーと国内支社の 370 のサーバーをダウンさせた。インサイダーは、論理爆弾の爆発に先立ち、会社の株式売付選択権を購入した。これは、その後の論理爆弾の爆発が会社の株価を引き下げることを期待してのことである。インサイダーは、組織が彼のことを不審に思い始めたので退職した。会社の株価は下落することはなかったが、論理爆弾は、その修正のため被害組織に 3.1 百万ドルの出費を強いるとともに、会社が完全に回復できないほどの混乱をもたらした。フォレンジック調査は、インサイダーを、VPN アクセスを介したインシデントに結びつけるとともに、彼の自宅のコンピュータ上に論理爆弾ソースコードのコピーを発見した。インサイダーは逮捕され、有罪判決を受け、97 か月の禁錮刑を宣告された。

[事例 1、2 の考察]

両社の事例とも、インサイダーは、マリシャスコードを重要な製造システムに埋め込むことにより、不正な操作をすることができた。インサイダーは、被害組織とその顧客又は株主に損害を負わせた。職務の分離を伴った変更管理プロセスが、これら攻撃の成功の可能性を削減することができたと思われる。さらに、仮に、組織がシステム・ベースライン又はファイル・ハッシュを比較するツールを定期的に利用していれば、システムへの変更が検出され、相当な損害を被る前に、攻撃を低減するか又は無効化できたと思われる。

プラクティス 12：従業員の行動のログ、モニタ及び監査のためにログ相関エンジン又は SIEM システムを利用せよ

[事例 1]

ある事例において、「大規模な電気通信会社のヘルプデスク技能者が、会社が貸与した彼のコンピュータにハッキング・ツールをインストールして他の従業員の信用証明書を盗み、それらを外部の共犯者に手渡した」というのがある。共犯者は、それら信用証明書を利用して会社のウェブサイトに不正なアクセスを行い、同サイトを台無しにした。このことが、組織の評判に相当な損害をもたらし、結果として顧客数と市場占有率が減少した。組織は、インサイダーのコンピュータに彼がハッキング・ツールをインストールした事実を発見したことから、彼を降格し、彼に対し彼のオフィスからのインターネット・アクセスを禁止するというポリシー上の制限を課した。しかしながら、会社は、技術レベルでこれらの制限を実施していなかったので、彼に引き続きインターネット・アクセスへの接続、及び期限切れの

顧客アカウントを利用した E メールを許す結果となった。インサイダーは、インスタント・メッセージを利用して、捜査に協力した同僚を脅迫した。これだけではない、会社にはログ相関又はセキュリティ情報・イベント管理（Security Information and Event Management: SIEM）機能が欠落していたため、多くの事象を彼の不正行為に関連付けることを怠る結果となった。アクセス・ログは最終的に、インサイダーとアウトサイダーをインシデントに結びつけた。

[事例 2]

他の事例として、「インサイダーが、組織のシステムのウィルス対策アプリケーションを無効化し、マルウェアをインストールした上、そのマルウェアを利用して彼の監督者のシステムに不正なアクセスを行い、重要なサーバーに論理爆弾を仕掛けた」というのがある。

[事例 1、2 の考察]

これらの事例において、仮に、組織が適切な監査を実施するとともに IDS/IPS を利用していれば、様々なセキュリティ事象がアラートを発したに違いない。それらの事象とは、ウィルス対策アプリケーションを無効化したこと、変則的なトラフィックが IDS センサーを通過したこと、及び論理爆弾をインストールしたことである。これらの事象を相関することにより、このインサイダーについてのより一層の悪意のある実態を明らかにすることができたはずであり、そして SIEM システムは緊急な対応を求める高優先順位のアラートを発生することができたとおもわれる。

プラクティス 13：モバイル装置を含む全エンドポイントからのリモート・アクセスをモニタし制御せよ

[事例 1]

ある事例において、「他の製造会社に機材を供給しているある国際的なタイヤ製造会社で、2 人のエンジニアが働いていた」というのがある。この 2 人のエンジニアはそれまで、海外の会社に雇われて特殊な機材部品の設計に従事していた。これらインサイダーは、タイヤ製造会社の以前の顧客であった他の会社が企業機密版機材を持っていることを知っていた。しかも、その 2 人のエンジニアは、以前その設計のため雇われていたのである。彼らは、タイヤ製造会社が以前に納入した機材の検査を装って、以前の顧客の工場を訪問した。被害組織の工場は、いくつかの保全ドアの内側にある施設へのアクセスを制限するとともに、写真撮影禁止の掲示を行っていた。訪問者は、署名して入出すること、及び常にエスコートされることが求められていた。また、被害組織は、訪問者に対して非開示合意（NDA）に署名することを求めていたが、2 人のインサイダーは前年に署名済であると偽った。一人のインサイダーが見張っている間に、他のインサイダーが自分の携帯電話のカメラで企業機密機

材の写真を何枚か撮った。2 人のインサイダーが被害組織の施設を出た後、1 人のインサイダーは、彼のカメラから映像をダウンロードし、彼の個人アカウントから彼の職場 E メール宛にメールした。彼はその後、他社の企業機密版の機材を製造するため、この映像を彼の職場アカウントからタイヤ製造工場に送った。

[事例 1 の考察]でた

この事例による攻撃のタイプは、多くの組織に問題を提供している。組織のセキュリティ・ポリシーとスタッフは、モバイル装置のカメラをしばしば看過することがあり、このようなことが、攻撃者による会社の機微情報に対する技術的保護策を巧みに回避させる結果となっている。しかしながら、この事例は物理的領域を超えている。インサイダーが写真撮影を行った装置は企業機密であった。ドアや警告サインが写真装置による撮影を阻止するため設置されていたが、訪問者が確実にポリシーに従っていることはほとんど確認されていなかった。機微な企業機密がおかれている区域は、不正な写真撮影を防止するため、付加的な管理策の設置が必要である。例えば、組織は、金属検知装置や警備員をこれら機微区域に配置し、誰にもモバイル装置を制限区域に持ち込ませないことを確実なものとすることができる。さらに、非開示合意やその他の法的文書については、訪問者が会社の建物に到着するかなり前に確認するべきである。この事例において、訪問者は過去に NDA に署名したと明言した。組織は、従業員に対して規則に従い再確認することを要求するべきである。仮に、被害組織がファイルに NDA があるか否かを確認の上、常時訪問者に随伴し、すべてのモバイル装置の保全区域内への持ち込みを禁止すれば、このインシデントは発生することがなかったと思われる。

[事例 2]

伝えられるところによれば、未だ判決が下されていない事例に、「あるチャリティーでの作業員（女性）が、寄贈者の小切手やクレジット・カードの写真を彼女のスマートフォンで大量に撮影した後、彼女のスマートフォン携帯電話サービス接続を介して、オフサイトに伝送した」というのがある。

[事例 2 の考察]

伝えられるところによれば、チャリティーの寄贈者は、この密かに抜き取られたデータに伴う被害者となった。この人物が罪を認めるか否かにかかわらず、最新のモバイル装置には、組織の IT セキュリティ・システムに検知されることなく、密かに個人識別可能情報（Personal Identification Information: PII）を抜き取る能力があることは明らかである。金属検知装置とモバイル装置の機微な区域への持ち込みに対するルールが、この経済的な損失に係る事例を防止したに違いない。

プラクティス 14：包括的な従業員退職手順を策定せよ

[事例 1]

ある事例において、「被害組織が、情報技術指導者としての職務を付与したインサイダーを解雇した」というのがある。インサイダーは約 1 か月後、彼の以前の管理者アカウントとパスワードを利用して、他の州で第三者がホスティングしている会社のウェブ・サーバーにリモート・アクセスした。このアカウントとパスワードは、会社が除去していなかったものである。彼は、解雇に対する復讐のため、ウェブ・サーバーから約 1,000 のファイルを削除した。

[事例 2]

他の事例では、「ユニファイド・メッセージング[6]・サービス会社のシステム管理者が、組織の E メール・サーバーにセキュリティ脆弱性を発見した」というのがある。インサイダーはこの脆弱性を管理者に報告したが、組織は何らの是正処置もとらなかった。インサイダーはその後、同会社を辞職し他の会社に就職した。インサイダーが被害組織を離れてから 6 か月後、彼は被害組織が無効化していなかった有効な E メール・アカウントを利用し、被害組織の顧客 5,600 人に E メールした。その E メールは、被害組織の E メール・セキュリティの欠陥を開示するとともに、顧客に対し顧客の E メール・アカウントを安全にするための方法について、インサイダーの個人用ウェブサイトにアクセスすることを指示したものであった。E メールは、被害組織のサーバーを突然停止させ、被害組織の評判を修復不能に陥れ、その後ほどなくして被害組織はビジネスからの撤退を余儀なくされた。

[事例 1、2 の考察]

CERT インサイダー脅威データベースには、組織が元の従業員に関連する全てのアカウントの削除又は遮断を怠った事例が沢山ある。組織は、規定内容が明瞭な退職手続と堅実なアカウント管理プロセスを組み合わせることにより、元の従業員による組織のシステムへのアクセスは最早あり得ないという信頼性を高めるべきである。

プラクティス 15：安全なバックアップ及び復旧プロセスを実施せよ

[事例 1]

「ある情報技術支援ビジネス会社が、コンピュータ・サポート技術者としてインサイダーを雇った」というのがある。インサイダーは、彼の職務の一部として、組織のネットワークに対する管理者レベルのパスワードで制御されたアクセス権を持っていた。インサイダーが組織を退職したとき、彼は組織のコンピュータへのアクセス権限を失った。インサイダー

[6] 複数の異なる手段でやりとりされるメッセージを統括的に管理するシステムの総称をいう。

は組織から退職 3 か月後のある週末の夜、彼の管理者レベルのアカウントとパスワードを利用して、組織のネットワークに対しリモート・アクセスした。インサイダーは、組織の IT システム管理者のパスワード全てを変更するとともに、組織のサーバーのほとんど全てをシャットダウンした。インサイダーは、侵入から迅速に復旧させることができるファイルを、バックアップ・テープから削除した。組織と組織の顧客は数日間、システム中断の憂き目にあった。このインシデント追跡の結果は、彼のホーム・ネットワークにたどり着いた。インサイダーは逮捕され、有罪判決を受け、31,000 ドルの損害賠償金の支払い及び 12 か月と 1 日の禁錮刑が宣告された。また、インサイダーは、不法なハッキングの帰結について、若者を対象に 100 時間の講義を行うコミュニティ・サービスも命じられた。

[事例 1 の考察]

この事例において、インサイダーは、リモート・アクセス及びバックアップ媒体からのファイルの削除ができた。仮に、組織が、バックアップ媒体へのアクセス制御に注意を払うとともに、悪意のあるインサイダーによるリモート・アクセスを可能にしたアカウントを除去していれば、インサイダーは組織のシステムに侵入することはできなかったと思われる。また、この事例は、複数のバックアップとオフサイトでの保管の必要性についても例証している。仮に、組織がバックアップ媒体に対するオフサイトでの保管を実施していれば、組織は別の復旧用媒体を利用してビジネスを立ち上げ、妥当な時間内に運用を再開できたと思われる。

プラクティス 16：正式化したインサイダー脅威プログラムを策定せよ

[事例 1]

サボタージュ（妨害行為）[7]の事例として、「情報技術支援ビジネス会社が、コンピュータ・サポート技術者としてインサイダーを雇った」というのがある。インサイダーは、彼の職務の一部として、組織のネットワークに対する管理者レベルのパスワードで制御されたアクセス権を持っていた。インサイダーは組織からの退職 3 か月後のある週末の夜、彼の管理者レベルのアカウントとパスワードを利用して、組織のネットワークに対しリモート・アクセスした。インサイダーは、組織の IT システム管理者全員のパスワードを変更するとともに、組織のほとんど全てのサーバーをシャットダウンした。インサイダーは、侵入から迅速に復旧させることができるファイルを、バックアップ・テープから削除した。組織と組織の顧客は数日間、システム中断の憂き目にあった。インサイダーは、逮捕されて有罪判決を受け、損害賠償金 30,000 ドルの支払いと 1 年乃至 2 年間の禁錮刑を宣告されるとともに、引き続く数年間の保護観察処分となった。また、インサイダーは、不法なハッキングの帰結について、若者を対象に 100 時間のコミュニティ・サービス講義を行うことも命じられた。

---

[7] 我が国における「サボタージュ（怠業）」の意味とは異なるので注意されたい。

[事例 1 の考察]

この事例は、インサイダー脅威プログラムの必要性を強調するものである。インサイダーは、組織のシステムにリモート・アクセスし、組織から離れた後に悪意のある行動を犯すことができた。仮に、被害組織の人事（HR）部門がインサイダーの退職を組織の情報保証（IA）チームに伝達していたとすれば、インサイダーのアカウントを利用禁止又は削除することができ、インシデントを防げたのではないかと思われる。被害組織は、「プラクティス 14：包括的な従業員退職手順を策定せよ」で述べたように、包括的な退職プロセスを持つべきであった。CERT インサイダー脅威データベースは、インシデントがサボタージュに関連した状況下でも発生することを示している：就業時間後の管理者用アカウントへのアクセスとリモートでの利用。SIEM 解決策のカスタマイズされたルールは、このような状況を検知し IA チームに不審な活動についてレビューするよう注意喚起することで、組織が潜在的な攻撃を検知するのを支援するものと思われる。SIEM システムについてのさらなる議論は、「プラクティス 12：従業員の行動のログ、モニタ及び監査のためにログ相関エンジン又は SIEM システムを利用せよ」を参照されたい。さらに、組織は、「プラクティス 13：モバイル装置を含む全エンドポイントからのリモート・アクセスをモニタし制御せよ」で述べたように、リモート・アクセスを注意深くモニタするべきである。

[事例 2]

同様に、次に示す不正行為の事例は、「インサイダー脅威プログラムがどのようにインサイダー脅威を防止、検知及び対応することができたか」を示すものである。あるインサイダーが、被害組織に簿記係として雇われた。インサイダーは約 2 年間、70 枚以上の小切手を組織の口座から振り出して彼女の個人的支払に充てるとともに、組織のコンピュータ口座記録を異なる受取人名に変更した。インサイダーは、組織から約 200,000 ドル横領した。インサイダーの行為は、管理者が電子小切手元帳に不審な点を見つけたときに検知された。インサイダーは有罪判決を受け、1 年乃至 2 年間の禁錮刑を宣告された。しかしながら、裁判所の損害賠償金支払い命令はたったの 20,000 ドルであり、会社は横領された金額の大部分を永久に失った。

[事例 2 の考察]

インサイダーはこのインシデントの発生以前に、同様の不正行為により有罪判決を受けていた。インサイダー脅威チームが身辺調査を要求するポリシーと手順を作成していれば、これにより彼女の過去の有罪判決が審査プロセス間に確実に発見され、従業員としては不適任と判定されたことから、インシデントを全面的に防止することができたと思われる。インサイダー脅威チームが、通常とは異なる不審な事象を検知するためのプロセスを確立していれば、電子小切手元帳に対する通常とは異なる一連の変更を検知することができたと

思われる。それによりインサイダー脅威チームは、より密着してインサイダーの活動をモニタすることで、不正行為をより早期に発見できたと思われる。早期の不正行為検知が、損失を少なくしたであろう。

[事例 3]

同様に、次に示す知的財産（IP）窃盗による損失の事例は、「インサイダー脅威プログラムが設定されていれば防止することができたか又は削減することができたに違いない」ことを例証するものである。インサイダーは、被害組織に研究化学者として雇われ、電子技術を含む様々な研究開発プロジェクトに従事した。インサイダーは、異なる会社からの求人申し出を受けた。インサイダーは被害組織を退職する 4 か月前に、被害組織のサーバーから、15,000 以上の PDF ファイル及び 20,000 以上の抄録を含む高価値の企業機密をダウンロードした。インサイダーがダウンロードした量は、彼の次に大量にダウンロードした者の 15 倍以上に上るものであった。かつ、それらデータは、彼の研究とは無関係のものであった。被害組織は彼の退職後、インサイダーによる大量のダウンロードを検知した。インサイダーは競合組織における仕事の開始後、ダウンロード情報の大部分を競合会社が貸与したラップトップに転送した。被害組織は、競合組織に対して同組織がダウンロードされた高価値情報を持っていることを通知した。競合組織は、インサイダーのラップトップを押収し、被害組織に引き渡した。インサイダーはその後有罪判決を受け、1 年乃至 2 年間の禁錮刑及び 14,000 ドルの損害賠償金と 30,000 ドルの罰金の支払いを宣告された。

[事例 3 の考察]

インサイダー脅威チームは、コンピュータ・システム上における通常とは異なる動作をモニタし、インサイダーの異常なダウンロードを検知することより、インサイダーからの危害の防止、早期検知又は削減ができたに違いない。そこで、インサイダー脅威チームは会社の優先順位に基づき、会社がインサイダーの雇用契約を即座に解除の上、捜査機関に依頼するか、又はモニタリングを強め、インサイダーの活動範囲に係る情報をより収集するために以前のログを調べるかを決定することができたであろう。組織は、価値ある IP の移転を阻止できたに違いない（訴訟では、その IP を競合会社又はその他が取得又は利用したかについて確認しなかった）。IP が極めて高いリスクにあり、かつ、被害組織の管理外にしばらくの間置かれていたことは確かであった。インサイダー脅威チームが活動していれば、このような脅威の防止、検知及び対応ができたと思われる。

プラクティス 17：ネットワーク装置の正常動作ベースラインを確立せよ

[事例 1]

「金融機関である被害組織が、上級金融分析家としてインサイダーを雇った」というのが

ある。インサイダーは、毎日曜日に組織のオフィスにやって来て、USB メモリに 20,000 以上の抵当権申込書をダウンロードした。インサイダーは、このダウンロードを 2 年間にわたり実施し、個人識別可能情報（PII）を含む 2 百万以上の記録を売却した。組織は、インサイダーが通常の就業時間以外に働きに来ていたことに気づいたが、組織は単にインサイダーが精励しているのだと信じていた。インサイダーは時々、通常勤務時間内でも記録をダウンロードした。組織は、USB メモリ又はその他の記憶装置を組織のコンピュータ上で利用することを禁止するポリシーを持っていた。また、組織は、組織のほぼ全部のコンピュータ上での USB メモリのアクセスを無効化していたが、インサイダーのコンピュータにはこのセキュリティ機能が欠落していた。インサイダーは、彼の不正行為を隠ぺいするため、記録の大部分を公共のコンピュータから E メールしていたが、時たま彼のパソコンから E メールした。長期の犯罪歴を持つアウトサイダーの共犯者とインサイダーは、20,000 の記録を一束にして 500 ドルで売却した。インサイダーは、50,000 ドル～70,000 ドルを儲け、その売上を彼の名義で開いた架空のコンサル会社の銀行口座に預金した。少なくとも 19,000 人の抵当権申込者が、アイデンティティ窃取の犠牲となった。多数の集団民事訴訟が被害組織を相手として提出された。この集団訴訟は、被害組織を経営難に陥らせるものであり、インシデント発生後 1 年を経て持ち出された。

[事例 2]

他の事例に、「化学製品の開発を専門としているある組織が、合衆国に帰化した市民のインサイダーを化学研究者として雇った」というのがある。インサイダーは、電子技術を含む様々な研究開発プロジェクトに責任を持っていた。被害組織は、インサイダーに対して海外勤務を申し出たが、インサイダーの家族は海外勤務を望まなかった。その結果としてインサイダーは、競合組織に雇用を求めた。競合組織は、インサイダーに 3 か月後に設けられるある役職を提案した。インサイダーは競合組織での新たな業務の開始 2 週間前まで、被害組織に対して彼の辞職計画を知らせなかった。インサイダーは、競合組織からの求人申し出を受け、かつ、彼が被害組織を辞職するまでの 4 か月の間に、被害組織のサーバーから約 17,000 の PDF ファイルと 22,000 の抄録を含む高価値企業機密をダウンロードした。ダウンロードはオンサイトで就業時間中に、15 時間～20 時間行われた。インサイダーがダウンロードしたデータの量は、彼の次に大量にダウンロードした者の 15 倍に及んだ。また、ダウンロードしたデータは、彼の研究とは関係がないものであった。盗まれた知的財産は、おおよそ 4 億ドルの価値があった。

[事例 1、2 の考察]

これら両事例において、インサイダーは、平均的なユーザーによる通常の利用をはるかに超えた大量の情報にアクセスし、ダウンロードすることができた。組織は、通常活動のベースラインを確立し、そのベースラインを超える全ての活動について警戒する必要がある。組

織は、いかなる不利益な取り扱いや悪事の出現をも避けるため、全ての従業員の活動をモニタリングするポリシーと手順を慎重に文書化の上、固守しなければならない。また、組織はポリシー及び手順の策定、完成及び実施に際して、法的助言を得るべきである。

プラクティス 18：ソーシャル・メディアに対して、特に警戒を怠るな

[事例 1

「あるセキュリティ研究者が、連邦政府の国防機関に勤務する実在しない若い女性を念頭に、サイバー脅威分析家というふれ込みで、仮想のソーシャル・メディア・プロファイルを作成した」というのがある。伝えられるところによれば、彼女の情報セキュリティ分野における卓越した経験、及び彼女の有力な知人や友達のリストにより、彼女は政府及び国防機関の高官とのコネを確立した。彼女は、単に彼女のオンライン・プロファイルに基づくだけで、求人の申し出を受けたり、談話の約束をしたり、また夕食の約束までもしたのである。一人の人物は、写真を取り交わしもした。この写真は、彼が海外でパトロール中に撮影したものであり、位置情報が組み込まれていたものであった。他の人物は、彼のプロファイルの中で、機微なパスワード復旧情報を明らかにした。また、その他の人物も、機微な個人情報を明らかにした。架空の人物は、300 にも及ぶ近い間柄となった個人とのネットワークを確立した。それらのうちの幾人かは、国家の機密に係る職務に従事しており、ソーシャル・メディアのリスクを知るべきであった[Waterman 2010]。

[事例 1 の考察]

この事例は、多くの人物がオンライン上に見つけた情報をあまりにも信頼しすぎていたことを例証するものである。この架空の人物の信憑性は、あるセキュリティ研究者が自称セキュリティ専門家に対する信用証明書（述べられている事実が真実であることを証明する文書）を求めたことから、秘密が明らかにされ始めた。仮に、架空のセキュリティ専門家と連絡した他の人々が、彼女の信用証明書を確認していたとすれば、この実験の犠牲者とはならなかったに違いない。

[事例 2]

他の事例として、「ある攻撃者が元合衆国副大統領候補の E メール・アカウントを危殆化した」というのがある。この攻撃者は、単に検索エンジンを利用して、パスワード復旧のための質問事項に答えることでパスワードを見つけただけであり、その質問事項には、誕生日、ZIP コード、及び彼女がどこで配偶者と会ったかが含まれていた。そして、彼はパスワードをリセットした。それから、攻撃者は彼女の E メールを通読後、住民討論の場にそれらを掲示した[Zetter 2008]。

[事例 2 の考察]

組織は、オンラインへの情報開示、とりわけ個人情報開示のリスクについて、従業員への訓練を行うべきである。一見何ら害を及ぼさないと思われる断片的な情報の開示が、潜在能力のある攻撃者による大量な情報の引きずり出しへと導き、個人のアカウント又は会社のアカウントやインフラさえも、攻撃者よる危殆化を可能にしてしまうのである。

プラクティス 19：不正なデータ抜き取りに対してドアを閉鎖せよ

[事例 1]

ある一つの事例として、「飲料製造会社の経営陣トップが、役員の経営管理アシスタントとしてインサイダーを雇った」というのがある。インサイダーは、役員のそばで勤務するアシスタントの立場から、組織の企業機密情報にアクセスすることを許されていた。それらの情報には、未だ一般公開されていない製品サンプルは無論のこと、秘密文書や著作権文書が含まれていた。ビデオ監視カメラは、インサイダーが企業機密や製品サンプルを彼女のバッグにしまい込むのを捉えた。インサイダーは、いくつかの文書をコピーするとともに、他の物も盗んだ。また、インサイダーは、被害組織の秘密のプロジェクトの一つに関連する役員の E メールのコピーを印字した。犯罪歴のある 2 人の共犯者が、インサイダーを手助けした。主たる共犯者は、手紙を介して競合組織と連絡し、被害組織の企業機密の売却を申し出た。主たる共犯者は、追加の情報を競合組織にファックスした。これには、被害組織の秘密のプロジェクトに係る機微な E メールのコピー、及び共犯者が所有する受益組織の銀行口座情報が含まれていた。幸いにも、競合組織が当局に知らせたことから、FBI が秘密捜査を実施した後、彼らは逮捕された。

[事例 1 の考察]

この事例は、インサイダーによるデータの盗み出しに利用可能ないくつかの方法を例証している。組織は、組織内におけるデータ盗み出しポイントのすべてを認識するとともに、それらを企業全体のリスクアセスメントに含めるべきである。これにより、組織は、明らかにされたリスクを削減するための低減戦略を実施することができるのである。

[事例 2]

他の事例としては、「化学製品製造会社が上級研究科学者として、専属の外国人インサイダーを雇った」というのがある。そのインサイダーは、新電子技術製品に利用する化学物質に関連した数百万ドルのプロジェクトに従事していた。インサイダーは会社に辞職を申し出た翌月、化学的な手順に関し詳細を記述したマイクロソフト・ワード文書を、受益組織にある彼の E メール・アカウントに E メールした。インサイダーは被害組織において、彼の会社貸与のラップトップから被害組織の国外支社へデータを伝送することについて、繰り

返し尋ねた。組織は一貫して、伝送には承認が必要であると回答した。インサイダーは、IT部門に対し承認が下りていると偽って伝送方法を尋ねることにより、伝送を強引に実施することを企てた。被害組織はインサイダーが退社する前に、インサイダーのコンピュータのフォレンジック調査を実施した。この調査は、従業員の転勤の際に実施される標準的な手続きであった。組織がインサイダーにラップトップを返却した。翌日、インサイダーは、職場で、しかも早朝時間帯に、ラップトップから外部記憶装置に 500 以上の文書をダウンロードした。数日後、被害組織は、インサイダーが秘密の文書をダウンロードしたこと、及び彼と受益組織との関係について問い詰めた。インサイダーは最初、彼が文書を外部ドライブにダウンロードしたことについては自白したが、それ以外の活動や受益組織とのつながりについては否定した。インサイダーは、文書は参考資料であるとみなした。その後の調査で、インサイダーが文書を彼の私用パソコンにコピーしていたこと、及びインサイダーが彼の個人的なオンライン E メール・アカウントに情報を伝送していた証拠があることが明らかとなった。インシデントは、情報が受益組織と共有される以前に、検知された。

[事例 3]

第三の事例は、「納税書類作成サービス会社が、納税書類作成者としてインサイダーを雇った」というものである。インサイダーは、職場での勤務時間帯に、少なくとも 30 人の顧客の個人識別可能情報（PII）をプリントアウトした。インサイダーはこの情報を利用し、偽の確定申告を偽の外国人名義と正確な社会保障番号（SSN）により提出した。還付金の合計 290,000 ドルは、17 の銀行口座に振り込まれた。

[事例 2、3 の考察]

これらの事例は、インサイダーがシステムからデータを移すいくつかの方法があることを強調している。組織は、データの不正な除去及び転送を防ぐための対策を講じなければならない。組織がデータのリムーバル・デバイスへの移転方法及び資料の印字方法をコントロールするためのポリシーを定義することが可能となるような技術が既に存在している。組織は、この事例集に述べられているシナリオを含め、企業全体に及ぶリスクアセスメントを注意深く実施した後、これらの選択肢について検討するべきである。

参考文献

[Waterman 2010]

ショーン・ウォーターマン：「架空の Femme Fatale がサイバーセキュリティを馬鹿にした」、2010 年 7 月 18 日、ワシントン・タイムズ

Waterman, Shaun. “Fictitious Femme Fatale Fooled Cybersecurity.” *Washington Times*, July 18, 2010. http://www.washingtontimes.com/news/2010/jul/18/fictitious-femme-fatale-fooled-cybersecurity/?page=1

[Zetter 2008]

キム・ゼッター：「ペイリン E メール・ハッカーは容易かったと言う」、2008 年 9 月 18 日、ワイヤード

Zetter, Kim. *Palin E-Mail Hacker Says It Was Easy. Wired*, September 18, 2008. http://www.wired.com/threatlevel/2008/09/palin-e-mail-ha/

平成２４～２５年度発刊資料

ＢＳＫ 第２５－　１号『情報優位の獲得：ｺﾝﾋﾟｭｰﾀ･ﾈｯﾄﾜｰｸ作戦及びｻｲﾊﾞｰｽﾊﾟｲ活動のための中国の能力』
ＢＳＫ 第２５－　２号『防　衛　産　業　基　盤　セ　ク　タ　ー　計　画』
ＢＳＫ 第２５－　３号『情 報 セ キ ュ リ テ ィ の 現 状 と 動 向 に つ い て』
ＢＳＫ 第２５－　４号『諸外国による兵器技術・情報の収集活動等と我が国の対策について』
ＢＳＫ 第２５－　５号『重要インフラ防護におけるレジリエンス・マネジメントについて』
ＢＳＫ 第２５－　６号『防　衛　調　達　の　制　度　改　革　を　考　え　る』
ＢＳＫ 第２５－　７号『防衛施設の建設工事に従事する技術者の育成に関する調査研究』
ＢＳＫ 第２５－　８号『中国の電気通信機器会社であるファーウェイ（華為）とＺＴＥ（中興通訊股份有限公司）によりもたらされる米国の国家安全保障問題に関する調査報告書』
ＢＳＫ 第２６－　１号『防衛関連企業等のレジリエンス基盤確保のための情報共有について（平成 25 年度）』
ＢＳＫ 第２６－　２号『我が国の産業競争力の低下及び安全保障上の脅威につながる技術情報流出の実態と対応策について』
ＢＳＫ 第２６－　３号『情報セキュリティの現状と動向について（平成２５年度）』

本報告書の中で意見にわたるものは、委託研究先の見解であることをお断りしておきます。

外国においても活用可能な、米国におけるインサイダー脅威に対する最善の対応策

平成２６年２月　発行
非 売 品　　禁 無 断 転 載・複 製
発　　行　：　公益財団法人　防衛基盤整備協会
編　　集　：　防衛基盤研究センター刊行物等編集委員会
〒160-0003　東京都新宿区本塩町２１番３－２
電　　話　：　０３－３３５８－８７５４
ＦＡＸ　：　０３－３３５８－８７３５
メール　：　koueki@bsk-z.or.jp
ＢＳＫホームページ：　http://www.bsk-z.or.jp