情報セキュリティにおける人的脅威対策に関する調査研究報告書

平成 22 年 3 月

財団法人 社会安全研究財団

情報セキュリティにおける人的脅威対策に関する調査研究会

はじめに

情報システムの利用が広がり、また高度化して、社会的な基盤としてその重要度を増すにつれ、情報システムに関する人的脅威が、情報セキュリティ上の大きな問題として認識されるようになった。特に、人的脅威の中でも、故意による内部者の犯行は、発生した場合に大きな被害・影響をもたらすものであり、対策についても、その他の類型の情報セキュリティ上の問題とは異なる対応が必要である。一方で、内部犯行によるものであるため、外部に出ることが少なく、警察やJPCERT/CCなど公的機関に届け出られた事例も限られたものである。特に、内部者による犯行は、特定の組織的な環境や人間関係の中で、システムを熟知した上で行なわれる犯行であるため、組織としての営業秘密を含む非公開情報が公になる可能性があること、関係者に迷惑や被害が生ずるおそれのあること、関係する情報システムの脆弱性が公になることにより更なる情報セキュリティ上の問題につながる可能性があることなどの状況があり、対応に当たった組織、企業、警察を含む公的機関においても、慎重な取り扱いがなされてきた。

近時においては、その問題の重要性から、徐々に関係者間での情報共有が進みつつあるが、前述のような状況から限られた情報についての共有に留まっている。特に、犯行者の内面にまで踏み込んだ分析については、個々の事例を扱った組織や対応機関において一部行われている程度と考えられる。

こうした状況を踏まえ、本調査研究では、内部犯行者の特性や動機について内面に踏み込んだ調査研究の実績のある米国の状況について調査し、これをとりまとめると共に、日本の警察機関の有する事件資料による詳細な事例調査を行い、人的脅威のうち特に問題である内部犯行について、類型化などにより事案発生過程及びその原因を把握し、対策を検討したものである。

本調査研究の実施に当たり、事例の紹介をいただいた警察庁情報技術犯罪対策課、事案の調査にご協力いただいた各警察機関の方々に篤く御礼を申し上げたい。ご協力は、これなくしては本調査研究が成り立たないというものであり、ここにお名前を挙げて御礼を申し上げるのが本来であるが、事案の特定を避ける意味で敢えて担当の警察機関の名称、ご協力いただいた方のお名前を掲げていない。失礼をお詫び申し上げると共に、改めて深甚の謝意を表させていただきたい。

多くの方々のご助力をいただいたとは言え、本調査研究報告書の内容について責を負うべきは、本調査研究委員会である。本報告書に示された内容は、警察庁情報技術犯罪対策課、関係する警察機関、警察大学校政策研究センター、JPCERT コーディネーションセンター、そして実施者である財団法人社会安全研究財団のいずれの正式見解でもなく、当委員会としての見解であることをお断りしておく。

また、本調査研究委員会の委員のうち、2 名が参加して行われた「情報システムに関する内部犯行分析手法の調査研究」(警察大学校学友会情報システムに関する内部犯行分析手法の調査研究グループ(責任者：坂明慶應義塾大学教授)、平成 21 年 3 月)の内容は適宜引用・利用させていただいているが、特に注記していない。ここに表記して警察大学校学友会に謝意を表させていただく。

内部犯行事案の被害・影響の大きさを考えるとき、この分野の調査研究は一層進める必要があると共に、その成果を生かした対策を進めることが重要であると考えている。引き続き、関係の方々のご協力をよろしくお願い申し上げる。

2010 年 3 月

情報セキュリティにおける人的脅威対策に関する調査研究委員会

委員長　辻井　重男

情報セキュリティにおける人的脅威対策に関する調査研究委員会

委員長　辻井　重男	中央大学研究開発機構　教授
委員　江口　有隣	大阪府警察本部警務部参事官（前警察大学校警察政策研究センター主任教授）
委員　坂　　明	警察庁長官官房付（前慶應義塾大学　政策・メディア研究科　教授）
委員　早貸　淳子	JPCERT コーディネーションセンター 常務理事
委員　中川　正浩	警察大学校生活安全教養部長
委員　渡邉　和美	科学警察研究所　捜査支援研究室長
委員　渡辺　昭一	(財)社会安全研究財団　研究主幹

(委員長を除き五十音順)

(オブザーバ)

渡辺　晃	警察庁生活安全局情報技術犯罪対策課課長補佐 (当時、2009 年 6 月～8 月)
内野　雅則	警察庁生活安全局情報技術犯罪対策課課長補佐 (2009 年 8 月～2010 年 3 月)
平川　敏久	警視庁ハイテク犯罪対策総合センター情報班長

実施： 財団法人 社会安全研究財団

事務局： 一般社団法人 JPCERT コーディネーションセンター

目次

本調査研究の意義と概要 7

1-1　人的脅威をめぐる状況 7

1-2　調査研究の概要 10

2 章　米国における内部犯行研究の状況 17

2-1　米国内における内部犯行の実態 17

2-2　米国における人的脅威の研究状況 18

3 章　調査研究の手法 24

3-1　調査事項と手法 24

4 章　人的脅威の実態 30

4-1　人的脅威のモデル 30

4-2　人的脅威の類型別の検討 36

5 章　人的脅威への対策 66

5-1　概要 66

5-2　時期と対象に応じた対策 67

5-3　情報システム面からのポイント 76

5-4　まとめ 79

6 章　付録・補遺 82

6-1　米国の調査票 82

6-2　調査票 90

6-3　内部犯行にかかわる公開文献調査 115

本調査研究の意義と概要

1-1　人的脅威をめぐる状況

情報システムが、社会・経済活動にとって不可欠なものになるにつれ、情報システムに関する問題事案の発生は、企業・組織に対して大きな影響を与えるようになった。特に、外部からの攻撃に対して防御体制をしっかり取っている場合でも、内部犯行者からの攻撃、或いは内部犯行者と外部の犯行者が協力しての攻撃に対しては十分な備えがなされていない場合もある。

こうした内部犯行者による脅威については、我が国は政府レベルですらセキュリティ・クリアランスのような情報に関する人的脅威への防護措置は緒に就いたばかりの段階にあるなど、人的脅威に対する対応について世界に大きく立ち後れている状況にある。

米国においては、国土安全保障省に属する捜査機関であるシークレットサービス(以後シークレットサービス)とコンピュータ関係事案の対処及びその調整を行う CERT/CC[1] が協力して、犯行者のプロファイリング、犯行に至る過程のモデル化、それに基づくベストプラクティスや教材の作成と公開などが行われている。(これらは、http://www.cert.org/insider_threat/にまとめられている。)

日本においては、内部犯行による被害は、被害を受けた組織が風評被害などをおそれることもあり公になる場合は少数であると考えられるが、公になったものを見るだけでも問題の大きさは理解でき、更に潜在的な発生件数を考えると看過できない社会的な問題となっているものと考えられる。

一部公になったものを見ても、銀行システムへの侵入・データ破壊、半導体関連企業からの技術情報漏洩、外国人従業員による機密情報の持出、元従業員による営業秘密侵害

[1] Computer Emergency Response Team Coordination Center の略。米国カーネギーメロン大のソフトウェア工学研究所に設置され、コンピュータセキュリティに対する調査研究や事案対処(コーディネーション)を行っている。

など、当該企業のみならず、国家的な見地からも問題がある状況となっている。以下にその具体例を示す。

〇銀行システムへの侵入・破壊
インド人の元派遣社員(32)が元の勤務場所である銀行のネットワークへの不正アクセス禁止法違反容疑などで逮捕された。同容疑者は、自宅のパソコンから、銀行の内部ネットワークのサーバに 67 回侵入し、約 2600 個のファイルを削除してシステムを破壊するなどした。(読売新聞 2008. 07. 17)

〇半導体関連企業からの技術情報漏洩
半導体関連企業に勤務する会社員が、在日ロシア連邦通商代表部員から謝礼を受け取り、会社の PC から技術情報や企業情報などの社外秘情報をコンパクトフラッシュカードに複写し、渡していた。(外事事件研究会「戦後の外事事件ースパイ・拉致・不正輸出ー」pp.42-44、東京法令出版 2007 年)

〇証券会社システム担当部長代理による顧客データ持ち出し・売却
2009 年 3 月、証券会社のシステム担当であった部長代理が、同社のデータベースに不正に接続して 148 万人の顧客データを持ち出し、うち 5 万人分を名簿業者に売却していたことが判明。元部長代理は窃盗及び不正アクセス禁止法違反で懲役 2 年の実刑判決を受けた。（読売新聞 2009 年 11 月 13 日など）。

〇元従業員による営業秘密侵害
A 社の元従業員 X が、在職当時にアクセス権のあった営業秘密をコピーして保有しており、退職後に海外競合企業 B 社に営業秘密を開示したことが明らかになった。以前、B 社からはライセンス供与の申し出があったが、A 社はこれを断った経緯がある。A 社は、B 社に対して厳重な抗議を行うとともに、元従業員 X の刑事告訴を検討したが、裁判で営業秘密の内容が明らかにされてしまうおそれがあるため、刑事告訴を断念した。(経済産業省「技術情報の適正な管理の在り方に関する研究会報告書 p.6)

近年大きな問題となっている個人情報の流出事案についても、2008 年度において新聞やインターネットで明らかになった事案についての調査によれば、2,3672 億円の損失が生じている。このうち、内部犯罪・内部不正行為、件数ベースでみると 1.40%、流出した情報について人数ベースでみると 4.40%となっており、一旦発生した場合の内部犯

行による被害の大きさが伺える(NPO 日本ネットワークセキュリティ協会「2008 年 情報セキュリティインシデントに関する調査報告書」、http://www.jnsa.org/result/2008/surv/incident/index.html)。

2009 年に警察が認知した不正アクセス行為 2,532 件にかかる犯行の手口を見ると、識別符号をフィッシングサイトにより入手したもの 2,084 件、共犯者等から入手したもの 167 件、他人から購入したもの 92 件に、識別符号を知り得る立場にあった元従業員や知人等によるもの 61 件、利用権者のパスワードの設定・管理の甘さにつけこんだもの 58 件と続いている。2008 年には、識別符号を知り得る立場にあった元従業員や知人等によるもの 163 件であったところ、大きく減少しているしているように思われるが、その被害の大きさを考えると依然としてこのような件数が認知されていることは問題である。

1-1-1　人的脅威への対応の動き

内部的な人的脅威に関する問題については、近時、国全体としても、取組が進んでいる。2006 年 12 月には「カウンターインテリジェンス推進会議」が内閣に設置され[2]、2007 年 8 月には「カウンターインテリジェンス機能の強化に関する基本方針」[3]が公表され、2009 年 4 月からは秘密取扱者適格性確認制度が発足するなど、国の重要な情報保護のための人的な要素に着目した対策の導入が図られている。

米国の調査においても、民間セクターにおいて行った内部犯行事案の調査研究結果と、諜報関係事案における事案の調査研究結果については共通する部分も多いとの指摘が

---

[2] 平成 18 年 12 月 25 日 内閣総理大臣決定「カウンターインテリジェンス推進会議の設置について」
http://www.cas.go.jp/jp/seisaku/counterintelligence/pdf/basis_members.pdf

[3] 「カウンターインテリジェンス機能の強化に関する基本方針」(概要)
http://www.cas.go.jp/jp/seisaku/counterintelligence/pdf/basic_decision_summary.pdf

なされているところであり[4]、民間事案について調査研究を進めることは、国家レベルの情報保護等を考える上でも意義のあるものと考えられる。

また、日本の産業にとって重要な技術情報等の適正な管理の在り方についての検討においても、様々な情報流出ケースの指摘・検討と人的な側面を踏まえた情報の適確な管理について報告書がとりまとめられ[5]、さらに技術やノウハウ等の営業秘密を保護するため、営業秘密侵害罪の用件を見直しを内容とする「不正競争防止法の一部を改正する法律」が 2009 年 4 月 30 日に公布された[6]。

1-1-2　内部犯行事案検討の意義

このように、大きな問題となっている内部犯行事案に関し、取組の機運も高まっているが、内部犯行によるものであるため、外部に出ることが少なく、その詳細を取り上げて分析するということには困難があった。警察など公的機関に届け出があった事例も限られたものではあろうが、警察機関の場合、捜査を行い、その犯行を明らかにするという業務を行っていることから、件数は少ないながら詳細な事実究明を行っている。本調査研究は、この分野で先行している米国の状況について調査を行うとともに、この警察資料を元に、内部犯行の過程や、環境、犯行を行う者の状況などについて調査分析を行い、内部犯行の実態を明らかにするとともに、その対策を示したものである。

1-2　調査研究の概要

1-2-1　概要

本調査研究のうち、米国における内部犯行研究の状況についての分析は、公開文献調査及び実際に調査研究を行った CERT/CC からのヒアリングにより行った。

---

[4] CERT/CC, "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," p.vii, http://www.cert.org/archive/pdf/06tr026.pdf

[5] 経済産業省「技術情報の適正な管理の在り方に関する研究会報告書」2008 年 7 月

[6] 経済産業省　「不正競争防止法の一部を改正する法律」
http://www.meti.go.jp/policy/economy/chizai/chiteki/koufu.htm

日本国内事例の分析については、2007 年から 2009 年 6 月までに検挙したサイバー犯罪(情報技術を悪用した犯罪)[7]であって、内部犯行事案(犯行者が企業等の組織から付与されているコンピュータの利用権限又は付与されていたコンピュータの利用権限を悪用して敢行したもの(派遣社員・アルバイト、元従業員、元社員等による犯行等を想定しており、被害者が第三者であるものを含む。)であるもののうち 30 件について行った。[8]

以下、本調査研究において、「人的脅威」と言うとき、人的脅威のうち内部犯行者によるものを指す。

本調査研究報告書においては、内部犯行事案について、3 つに分類して考察することにする。この 3 分類とは、

1. システム悪用
2. 情報流出・情報アクセス
3. 情報破壊・システム破壊

である。

CERT/CC による研究においては、

1. Employee Fraud
2. Information Theft
3. Sabotage

---

[7] 本報告書では、サイバー犯罪について、警察庁の定義に従い、情報技術を悪用する犯罪とし、不正アクセスの禁止等に関する法律違反、刑法で規定されている電子計算機損壊等業務妨害罪を　はじめとしたコンピュータ又は電磁的記録を対象とした犯罪、ネットワーク利用犯罪(実行に必要不可欠な手段として高度情報通信ネットワークを利用する犯罪)の三分類のものとしている。警察白書平成 20 年版 72 ページなど参照。

[8] 実際の警察資料は、警察職員の身分を持つ委員がこれを閲覧し、個人情報や秘密に当たる情報を除くなどにより法律的・倫理的問題のないものに加工した上で分析を行った。

との分類がなされており[9]、基本的に同様の考え方によっているものと考える。

システム悪用には、情報通信システムを悪用し、例えば自らの銀行口座に不正に入金させ組織の資金を横領するようなケースが含まれる。情報流出・情報アクセスは、電磁化された顧客の情報を電磁媒体に記憶させて持ち出し、これを他者に販売したりする行為や、退職後にかつての職場のシステムにアクセスし、情報を盗み見るようなケースが含まれる。情報破壊・システム破壊は、退職後にかつての職場のシステムにアクセスし、保存されている営業用のデータを消去したり、自らが構築に関与したシステムのデータやプログラムの一部を消去したりしてシステムを破壊する行為が含まれる。

本調査研究においては、この 3 類型についてバランスをとる観点から、

(1) システム悪用　8 件

(2) 情報流出・情報アクセス　13 件

(3) 情報破壊・システム破壊　9 件

を取り上げている。

また、選定にあたっては以下の 3 点を考慮した。

(1) 被害企業の規模及び業種

・大企業、中小企業、家族経営の企業などの各種規模が含まれること

・IT 企業、一般企業、伝統的企業など幅広い業種をカバーすること

(2) 利用システムの規模などについて

・社内システム、外部システムを利用した事案が含まれていること

・大規模システムから小規模システムまで含まれていること

---

[9] Dawn M. Cappelli (CERT) 他,「The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures」, 2008 年 5 月

(3) 犯行動機について

人格的な特性・感情、経済的事情などの理由が含まれていること

これらを考慮し、起こりうる内部犯行の事案を把握し、対策を考える上で必要なデータの収集を図った。

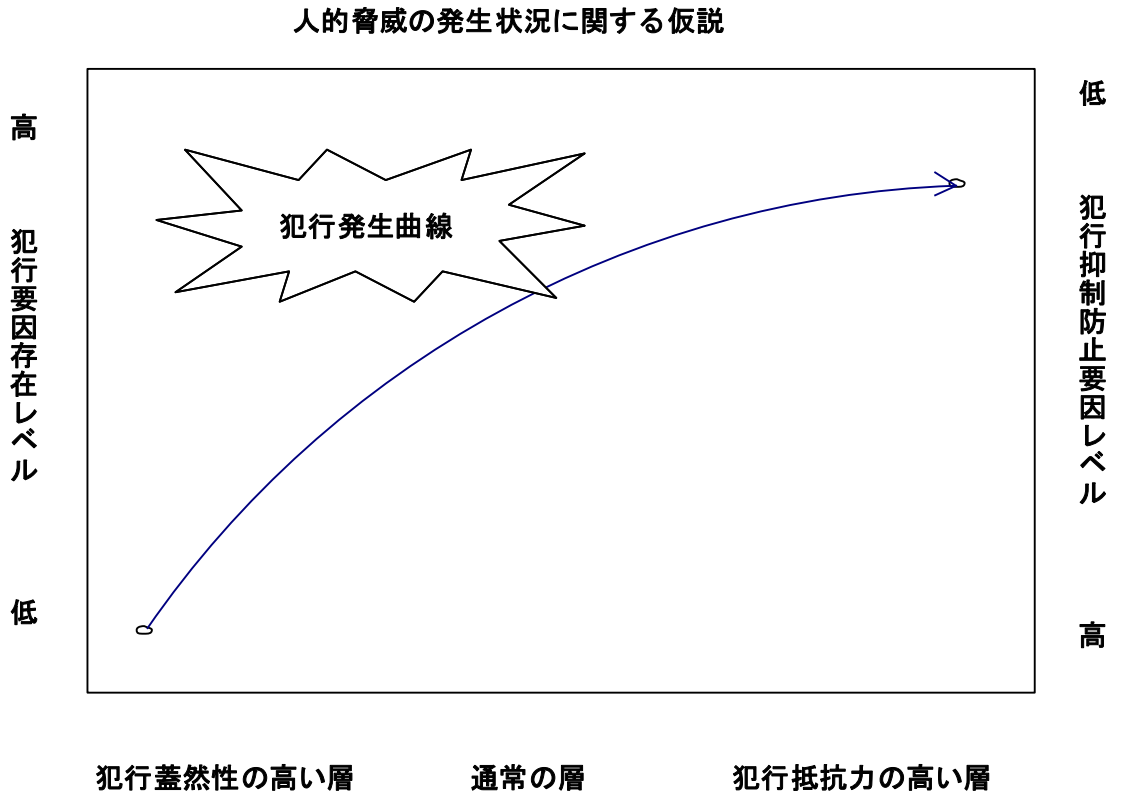
1-2-2　事例調査に当たっての考慮要素

事例調査に当たっては、人的脅威を明らかにするとの観点から、次のような点について考慮しつつ、資料の収集・分析を行った。

犯行誘発要因・犯行抑止要因

図 1 のような仮説を立て、それに対応する調査項目を掲げることとした。

図 1　人的脅威の発生状況に関する仮説



この仮説は、犯行は個人的資質と犯行誘発要因存在レベル(及び犯行抑制防止要因レベル)という要素によって発生の状況が決まってくる、というものである。つまり、犯行蓋然性の高い層(犯行を犯しやすい性質を持つ者)は、犯行を誘発するような要因がそれほど存在していなくても(すなわち犯行要因存在レベルが低くても)、また犯行を抑制し防止するようなシステムが整備されている場合でも(すなわち犯行抑制防止要因レベルが高くても)、犯行を行うことがある。一方、犯行抵抗力の強い層(犯行を犯しにくい性質を持つ者)は、犯行を誘発するような要因がかなり存在していて(すなわち犯行要因存在レベルが高い)、犯行を抑制し防止するようなシステムが欠如しているような場合に(犯行抑制防止要因レベルが低い)、初めて犯行を行うことがあり得る、というものである。そして、その中間層ともいうべき、通常の層(それなりの犯行に対する抵抗力は有しているが、一定レベルの誘発要因があり、抑制防止のための仕組みが不足していれば犯行に及んでしまう場合があるような者)が存在する、と考えるものである。

このようなモデルに従い、項目設定においては、次のような考え方を取った。

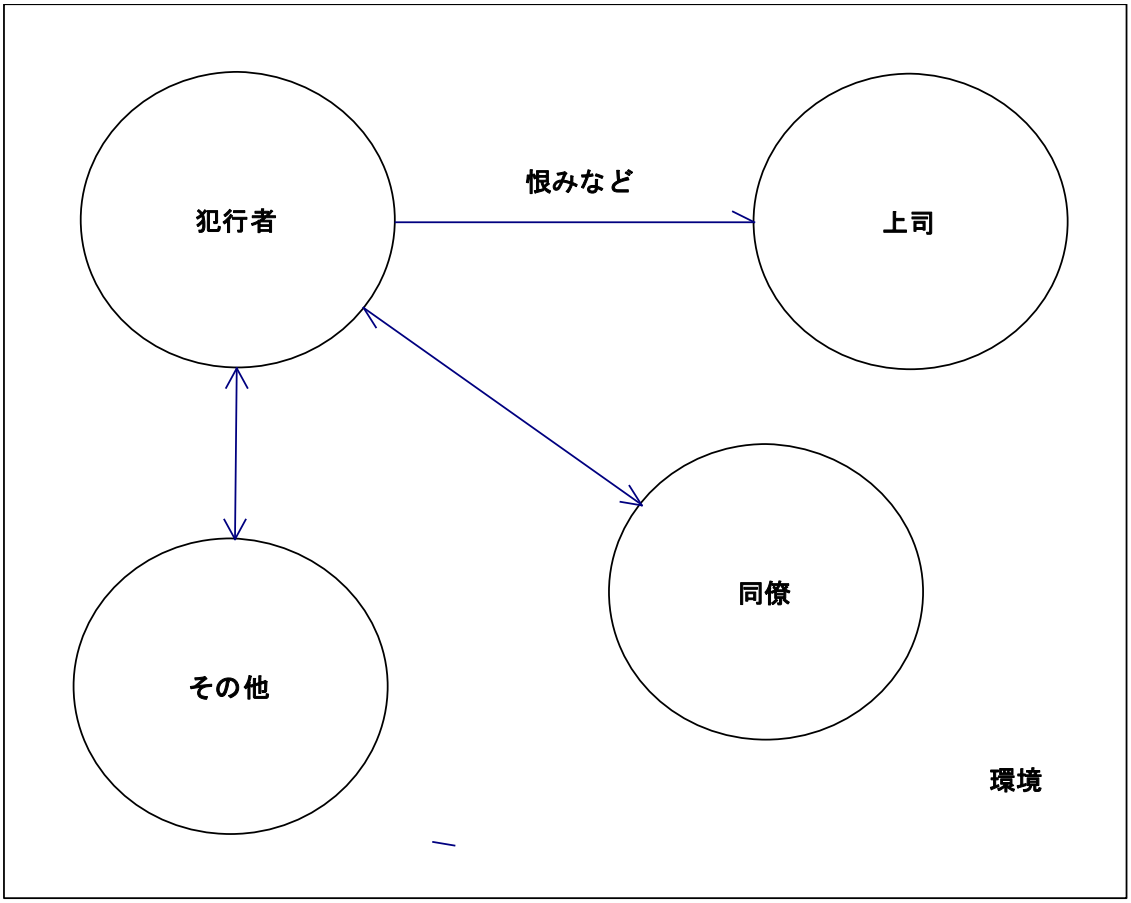
○犯行を行う蓋然性の高い資質を有している者、通常の者、犯行の誘因に対する高い抵抗力を有する者といった分類を想定し、それぞれのレベルがどの程度かについて分析することに資する項目を設定する

○誘因となる要素を抽出できるような項目を設定する

○犯行抑制抑止要因レベルは、犯行誘因の多寡又は強弱に還元できるものとも考えられる(すなわちそちらの見出しの下にまとめることも考えられる)ものであるが、分かりやすく漏れのないようにするため、「犯行抑制防止要因」といった視点からも、項目設定を行うよう努めた。

人間関係要因

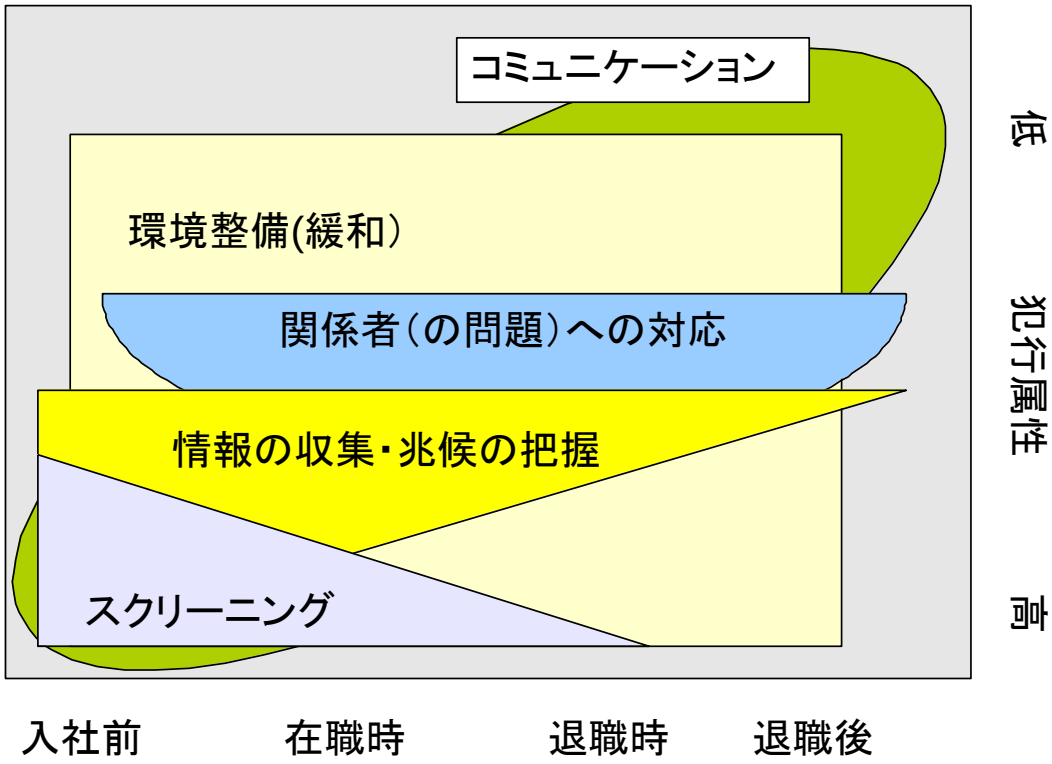
図 2　犯行者を取り巻く環境



犯行の動機としては、上司や会社に対する恨みといった感情が大きな役割を果たしている場合がある。また、逆に、上司や周囲の対応によって犯行が抑止される場合もあると考えられる。従って、今回の調査では、上司や周囲の人々の対応、企業としての対応も項目に含めるよう努めた。(図 2)

対象及びフェイズ(時期)ごとの対応検討に資する項目

図 3　時期と対象に応じた対策



犯行抑止のためには、時期と対象を考慮した対策を講じることが求められると考え、これを考察するために必要な項目について含めるよう努めた。図 3 は、次のような仮定に基づいている。すなわち、犯行属性の高い者について、入社前―採用時の段階では、コミュニケーション等により、情報の収集・兆候の把握を行い、スクリーニングを行う。在職時においては、(情報の収集・兆候の把握をコミュニケーション等も含めて行い、スクリーニングを行う場合もあろうし、また情報セキュリティ確保のための対策を行うことや関係者の有する財政面の問題や仕事上の悩みについて組織や上司、同僚が共に解決のために対応する、ということもあろう。更に、犯行が行いにくい環境整備を行い、犯行属性を持つ者の傾向を緩和し、一般の職員や犯行属性の低い者にとっても快適な職場環境を整備するということも対応になり得る。その場合でも、コミュニケーションは重要な要素となろう。

2章　米国における内部犯行研究の状況

本調査研究にのぞむにあたって、人的脅威対策の分野に早くから着目し、研究を行っていた米国の各種機関による研究成果について検討を行った。本章ではそれらの調査研究の成果をもとに米国における内部犯行の発生状況などの実態、およびそれらの脅威の認知/発見/対策などに対して如何なる研究が行われているかをまとめる。

2-1　米国内における内部犯行の実態

前章に述べたとおり、内部犯行はその性質上、被害の実態把握が難しい。ここではCERT/CC の報告書で引用されている 2005 年までのケースに加え、E-Crime Watch Survey と呼ばれる大規模組織の CIO へのアンケート調査から被害組織の変遷や被害額の推定を試みる。

E-Crime Watch Survey は毎年、米国の CSO Magazine と CERT/CC などの外部協力研究機関が行っているオンライン犯罪の被害状況調査である。大規模組織の CIO(情報システム責任者)や CSO(情報セキュリティ責任者)あるいは FBI、州警察などに対してアンケートを実施している。

このアンケートでは過去 1 年間に対象組織において確認されたオンライン犯罪の件数及び、それが内部犯行になのか、外部からの攻撃であったか統計をとっている。2004 年から 2007 年について抜粋したのが下表である。

表 1 内部犯行の割合（eCrime watch survery 2004-2007 より）

年	確認されたオンライン犯罪件数	内部犯行の占める割合	それ以外
2004 年	342	**29%**	71%
2005 年	554	**20%**	80%

2006 年	328	**27%**	73%
2007 年	443	**34%**	66%

表 1 からは、大企業や各種組織において発見されるオンライン犯罪の 2 割から 3 割は何らかの形で内部の人間が犯行に関わっていることが読み取れる。またここで「それ以外」と分類されたものの約半数は犯行者を特定できないというケースである。例えば 2007 年に関して言うと内部犯行が 34%、外部の者による犯行が 37%、そして特定不可能であったものが 29%にのぼる。この中には特定に至っていない内部犯行事例がさらに多く含まれることが予想される。

2-2　米国における人的脅威の研究状況

本章では米国における人的脅威の研究状況についてその目的や体制、そして主たる成果を解説する。

2-2-1　人的脅威研究の歴史

米国に於いては人的脅威について早くから専門家が問題意識を持ち調査を開始していた。

初期の米国国防省での研究

国防省では 2000 年より前から主に自組織で発生する様々な内部犯行事例を対象として内部犯行や人的脅威研究を開始していた。この研究に基づいて、内部犯行による被害を抑制・軽減するための調査報告書[10]を 2000 年に発行している。

その後、この研究に国防省の研究機関”The Defense Personnel Security Research Center (以後 PERSEREC)”と CERT/CC とが加わって、軍事に関わるサービス/国防省における IT に関わる内部脅威を協力して分析した。2000 年という早い時期から、内部犯行に目が向けられていたことは注目に値する。前述の国防省のレポートには幾つかの

[10] ”2000 DoD Insider Threat Mitigation report”
(http://cio-nii.defense.gov/org/sio/iptreport4_26dbl.doc 現在参照不可)

内部犯行事例が紹介されているが、それ以外に多くの同様の事例が起きていた可能性は否定できない。また分析や被害軽減を目指す上で技術的・心理的・組織的要因を加味する必要があるため、様々な分野から識者を集めて調査にあたっていた。

ほぼ同時期にシークレットサービスもまた CERT/CC と共同研究を開始した。この時の目標は「物理セキュリティや組織のミッション遂行にインパクトを与えるようなサイバーセキュリティ上の脅威を明確化し、評価し、被害を緩和すること」及び「重要なデータやシステムに脅威を及ぼす人物を明確化し、評価し、被害を緩和すること」であった。

CERT/CC における"The Insider Threat Study"のはじまり

2003 年、CERT/CC は" THE INSIDER THREAT STUDY (以後 ITS)"と銘打った活動を開始する。これはシークレットサービスと CERT/CC が 2003 年度、2004 年度にアメリカ国土安全保障省(Department of Homeland Security)の支援を受けて行った人的脅威に関する調査研究と啓発活動の総称である。その後現在に至るまで、活動は続いている。

ITS においては、システムに正当なアクセス権を持つ者が、それを用いて組織の情報の機密性、完全性、可用性に対して負の影響をもたらした事例について調査を行った。シークレットサービスが持つ心理分析、行動分析に関する知見と CERT/CC が持つネットワークシステムやセキュリティ技術に関する知見を併せ用いて、多元的な分析が行われた。

具体的には内部犯行事例を分析しデータベースに登録した。対象となった事例は 1996 年から 2002 年にかけて米国の重要インフラ事業者(電力、鉄道、通信など)で発生した約 150 事例である。2007 年には 2003 年の活動をほぼ踏襲する形で、新たに 2002 年から 2007 年までの約 100 件の事例について追加で分析とデータベースへの登録を行った。

2003 年以降 ITS からは不定期に研究成果が発表されている。その知見については後の章で解説を試みる。

その後の調査状況

CERT/CC の ITS はその後自らの研究成果を元に内部犯行による被害拡大防止を目的とするセミナーを開催した。また専門家が依頼された組織に赴き、リスク診断を行うコンサルティングサービスを開始した。その後も米国では内部犯行の側面を持つ犯罪が発生

していると考えられるが定量的データに乏しいのは前章で述べた通りである。CSO Magazine 等のメディアや SANS などのセキュリティ研究機関が被害の実態を把握するためのアンケートなどを行っているため、その研究成果が待たれる。

2-2-2　CERT/CC の研究成果

CERT/CC の ITS の中で示された幾つかの重要なポイントについて解説を試みる。言うまでもなくこれは米国における一調査研究に示された考えであり、本研究調査は必ずしも以下に示す定義や類型をそのまま用いてはいない。

内部犯行の定義

まず CERT/CC の研究における内部犯行とは以下の 3 条件を満たす犯罪である。

1. 現在もしくは過去の社員、その他の被雇用者もしくはビジネスパートナー
2. 組織の IT システム(ネットワーク、システム、データ)への正規に認められたアクセス権を持っている、もしくは持っていた者
3. 意図的にそのアクセス権を用い、組織の情報の機密性、完全性、可用性に対して負の影響をもたらした者

負の影響という曖昧な表現を用いているのは、内部犯行によって引き起こされる事象が単純な金銭被害や情報の持ち出しに限らず、企業イメージへの悪影響であったり、企業内部での混乱を引き起こすものであったり、多岐にわたることによる。

内部犯行の調査手法

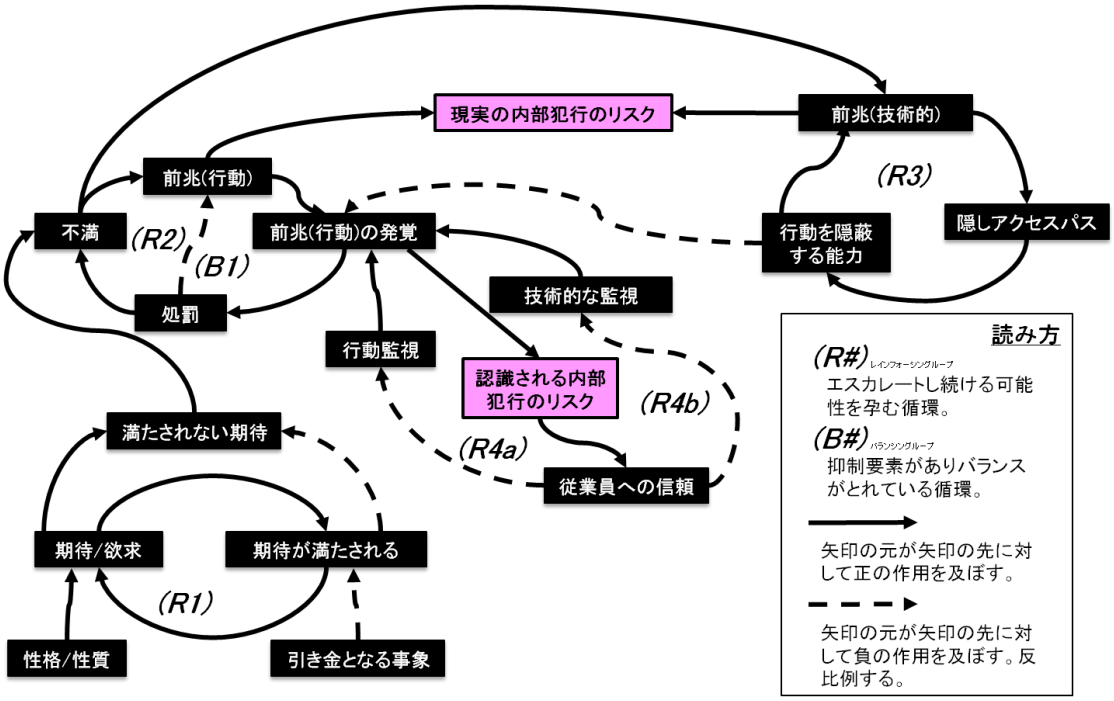
前述の通り、ITS では内部犯行事例を分析しデータベースに登録した。対象となった事例は 1996 年から 2002 年にかけて米国の重要インフラ事業者(電力、鉄道、通信など)で発生した約 150 事例である。2007 年には 2003 年の活動をほぼ踏襲する形で、新たに 2002 年から 2007 年までの約 100 件の事例について追加で分析とデータベースへの登録を行った。

データベースに登録された理由は研究者間でのデータ共有を見越していたことと、ソフトウェアを使ったモデリングを行うことを目的としていたことである。

内部犯行のモデル作成

コーディングの結果を基に、行動や個人の特質が内部犯行に繋がる共通パターンを整理する作業をモデリングと呼ぶ。 CERT/CC が行った調査ではシステムダイナミクスと呼ばれるシミュレーションの手法が用いられた。 システムダイナミクスはビジネスや政策などの全体像を掴むことが難しい、因果関係が絡み合った事象のシミュレーションモデルを作ることに適している。

図 4　内部犯行全体について分析したモデル図



（“Best Practices For Mitigating Insider Threat: Lessons Learned From 250 Cases”を元に作図）

このようにモデルを作成することで、事例への理解が深まることはもちろんのこと、多様な経歴を持つ調査チーム内でのコミュニケーションを円滑にする効果が得られたという。

モデルを使ったシミュレーション

ITS の報告書からは研究チームが幾つかの点についてモデル図に数字をあてはめてシミュレーションを行っていたことも分かる。例えば職場で上司などから与えられる自己裁量の範囲によって、従業員の期待する職場での自由度と満足度はどう変化するかを表したモデル図である。この場合、上司の介入の頻度や従業員の求める自由度を変数として 104 週間のシミュレーションを行っている。内部犯行のモデルにおいては数値パラメータをとれない要素も多く、シミュレーションは補助的に用いられたと考えられる。

内部犯行の類型

作成されたモデルに基づき、犯行の目的や形態に着目し内部犯行の類型を行われた。

1. Employee Fraud
組織の財やサービスをごまかし(deception)やぺてん(trickery)で手に入れる行為

2. Information Theft
機密や知財に関連する情報などを組織から盗み出す行為

3.IT Sabotage
特定個人、組織(含む組織のデータ、システム、日常業務)に損失を与えるという意志に基づいた悪意ある行為

Employee Fraud についてはシステムの破壊や停止を目的とせず、数字を改ざんしたり、不正に金銭を引き出したりという行為が対象となる。それぞれの内部犯行事例はこれらの 3 類型の何れかに属する。また、1 つの事例が 2 つ、あるいは 3 つの類型に属することもある。

明らかになったこと

一連の調査から ITS は幾つかの所見を示している。代表的なポイントを以下に示した。

1. 多くの内部犯行者は悪意ある行動に身を冒す個人的属性を有している
2. 多くの内部犯行者の不満は期待が裏切られたことに端を発する
3. 処罰や(従業員にとって)好ましくない出来事が IT 破壊行為の発生確率を上げる

4. 多くの場合、犯行の兆候を示す振る舞いが確認されている。しかしそれらは看過される

5. 内部犯行者は侵入するため、そして痕跡を隠すために組織の経営層に気づかれぬように裏口を設ける。大半の行為は退職後にその裏口を用いて行われる

6. 組織は技術的な兆候を見落としている

7. 物理的、技術的アクセス制御の欠如が IT 破壊行為を容易にする

これらの原因を特定し、解決していくことがつまり内部犯行の被害軽減の取り組みといえる。

一方で ITS の調査結果が日本の内部犯行事例にそのまま応用できるわけではない。まず調査票には兵役の有無、特定の疾病歴など、日本で調査することの妥当性/倫理性を慎重に検討すべき点も数多く存在する。またさらに ITS では注目されていないが、日本での調査に於いては、プライバシーマーク、JSOX など様々な日本独自の認証や社会制度などを加味することが求められる。

3章　調査研究の手法

3-1　調査事項と手法

本調査研究では、公開されている文書によって主に海外の状況を理解する文献調査と実際の内部犯行事例を分析する事例分析調査を行い、これを元にモデルの作成と分析、対策の検討を行った。

事例分析に当たっては、公開文献から抽出した CERT/CC の内部犯行調査での調査項目をベースに、兵役の有無など日本の社会風土になじまない設問を削除し、また事例分析を行いつつ必要と思われる項目を加えて調査票を作成した。これは、事例分析の精度を、実際の調査を行いつつ上げていくためであると同時に、今後様々な場面で行われるであろう内部犯行事例の分析に当たり、参考となる資料として提供するためである。このため、利用しやすいように、調査票に記入のためのルールや記入例を記載した。さらに回答欄を選択式にするなど、実際の利用に当たっての作業の負荷を軽減する工夫を行った。

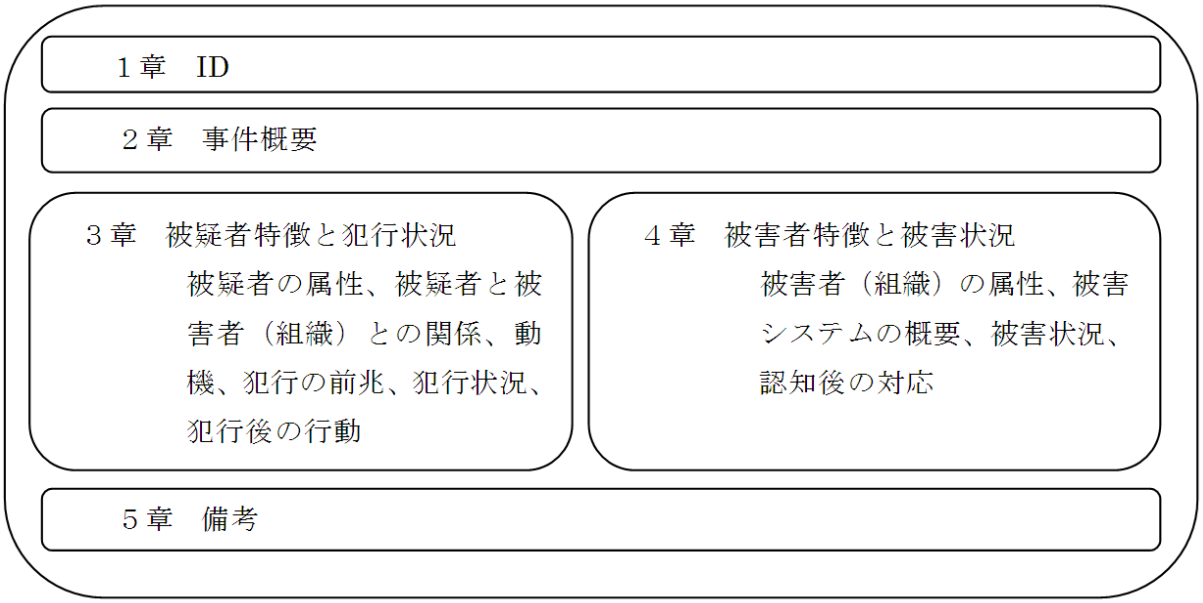
また、モデリングに当たっては、CERT/CC が行った調査においてとられたシステムダイナミクスの手法にこだわらず、日本において実態を理解し対策を検討しやすくするために、犯行者と環境、そしてこれに時間軸を組み入れた視点から、静的なモデルと動的なモデルを設定し、実態を分析するとともに対策の検討を行った。

以下、本章では、こうしたモデル作成、対策検討の基盤となる、事例分析のための調査票の内容について、解説する。

調査票全体の構成

調査票は図 5 の通り構成されている。

図 5　調査票の構成



1 章と 2 章は内部犯行事例の概略を記入する設問が中心である。3 章は主に警察が所有する事例の被疑者調書から、犯行者個人の情報や動機などを書き写すものである。

4 章は主に被害者調書などから、被害者あるいは第三者の視点からの情報を書き写すことを目的としている。特に内部犯行における被害の未然予防や被害の拡大防止を実現するために、技術や使用システムについてより細かく情報収集を行った。

5 章は備考として、1 章から 4 章まででくみ取れなかった事案の特徴や分析時の着眼点及び調査票記入者の所見などを記載することとした。

続く章では調査票中の設問について、特に重要と思われる者について解説を試みる。なお調査票の全文を本報告書 90 ページからの補遺に収録している。

1 章 ID

[1-1 一意番号(ID)]、[1-2. 事件名]及び[1-3 犯行が行われた発生年月日]の 3 点のみを問う。これらはデータベースに登録した際の検索キーとして利用することを想定している。

2 章 事件概要

[2-1. 犯行発覚の経緯]、[2-2. 捜査の端緒]、 [2-3 概要] を筆頭に 2 章では事件の概略を問う設問が中心である。 [2-4 主な適用条文、適用法]で事案に適用された主な法律とその条文について記載することとした。

[2-5 事件類型] は既に述べた CERT/CC による内部犯行の 3 類型のいずれにあたるかを記入する。基準は下記の通りである。複数の類型の特徴を併せ持つ事案も想定されることから複数回答可能としている。

1, システム悪用(Employee Fraud) - システム悪用: 組織の財やサービスをごまかし(deception）やぺてん(trickery）で手に入れる

2, 情報の持ち出し(Theft of Information) - 機密や知財に関連する情報などを組織から盗み出す

3, 破壊行為(IT Sabotage) - 特定個人、組織(含む組織のデータ、システム、日常業務）に損失を与えるという意志に基づいた悪意ある行動"

3 章 犯行者特徴と犯行状況

調査表の 3 章では主に犯行者や犯行の特徴を抽出する。

[3-2 被疑者番号]を設け、被疑者が複数存在する犯行に対応することを試みた。複数犯の場合、犯行者毎に 3 章のシートを埋めることとしている。

[3-2-1 基本事項] この項では[3-2-1-1 性別]、[3-2-1-2 被疑者年齢]、[3-2-1-3. 被疑者国籍]、[3-2-1-4 被疑者住所]、[3-2-1-5. 被疑者職業]、[3-2-1-6 被疑者氏名]などの犯行者に関する個人情報を収集した。これらについては、個人を特定可能な重要機密情報であるため、他の同様の情報とあわせて、モデリングと分析の段階では調査委員会内でも非開示とした。

[3-2-2 生育環境・家庭環境] では犯行者の生育時の家族構成や学歴などを調査した。また度重なる転居や同居人との人間関係からくるストレスによる犯行が考えられることから[3-2-2-3 転居状況]やその他の環境に関する情報を収集した。

[3-2-4 健康状態] 犯行者自身の健康状態を収集した。特に[3-2-4-3 アルコール中毒]、[3-2-4-4 薬物中毒]、[3-2-4-5 パニック障害]、[3-2-4-6 配偶者への暴力]などのトラブルについて状況を調査した。これらは主に米国での結果から心身の健康と内部犯行との連関を考察する価値があると判断したためである。

[3-2-5 経済状況] 経済的な苦境から内部犯行に手を染めることは容易に想像され、ここでは犯行者の経済状況に関する情報を収集した。[3-2-5-1 年収]や[3-2-5-2 借金]などは犯行者の収入、貯蓄及び借金などの金銭的状況を明らかにするための設問であり、ここから犯行が金銭目的であったかを考察可能と考えた。

[3-2-6 被疑者の職務経歴] 犯行者の職務経歴と IT 関連の技術的な能力を把握することを目標とした。内部犯行事例において、企業システムに対する不正にどの程度技術的な知識が必要となるかを把握することは主に技術的対策の検討に資すると考えたからである。

[3-2-7 被害組織の関係] 就業中、退職後を問わず犯行者と被害組織の関係は内部犯行の発生原因を考える重要な点であると考え、この項には多くの設問を用意した。[3-2-7-1 契約上の取り決め]では雇用契約の形態(正社員か否か)や雇用時の不正アクセスや秘密保持契約の有無を確認した。[3-2-7-2 参加していた時期・期間、部署]ではその企業で働いていた期間や部署、職位・職責や給与までを問うた。[3-2-7-3-1. 就職参加時の状況]では犯行者が働く状況という若干曖昧な設問であるが、被害組織の雰囲気を汲むことを目標としている。

[3-2-7-5. 勤務時の状況]では就労の形態、犯行者の組織内での役職や職責、オフィス環境の様子、執務のためのスペースが同僚などからどの程度目の届く場所にあったか、被害組織の情報システム上でどのような権限を持っていたかを確認している。

さらに内部犯行事例は従業員の退職後に犯行に及ぶケースが多い点に着目し、[3-2-7-6 退職関係]では犯行者が退職したのであれば、円満な退職であったのか、犯行者が被害組織に恨みを抱えていないことを確認した。犯行者が被害組織を退職した後の経済的な状況もここでの重要な確認事項である。

[3-2-8 犯行の前兆]では前兆となる行動を大きく[3-2-8-1 行動面の前兆]と[3-2-8-1-2 技術面]とに分けた。ハッキングツールの使用、顧客情報/従業員情報データベースへのア

クセス、バックドアアカウントの作成などが一般的に技術面の前兆と考えられている。[3-2-8-1-1. 行動面の前兆]では職場内でのもめ事、攻撃的・暴力的行動、会社の経費の不適切な使用、気分の揺れが激しい、業務実績がふるわない、怠業、性的いやがらせなどのいわゆる典型的な行動の乱れの有無を確認した。

また、顧客情報・従業員情報への不正アクセスや勤務中の不適切なインターネットアクセスなどの行動がとられていないか、行動がみられる場合はその具体的な内容について確認をおこなった。

[3-2-9 動機] 犯行に及ぼうとした、直接の動機を問うた。会社内の特定の人に対する恨み、不満の発露なのか金銭的利益を得るためのものなのか、はたまたストレスや好奇心によるいたずら気分の犯行だったのかを問うた。

[3-2-10 犯行状況] 犯行状況を問う項である。[3-2-10-1-1 飲酒]、[3-2-10-2-1-2 アクセスの時間] 、[3-2-10-1-3. 関係者による煽り]など、通常であれば犯行に及ぶに至った最後の一押しの要因を探ろうとした。犯行がどの時間帯に行われたか、犯行者が被害を受けた IT システムにどのようにアクセスしたか、犯行に使われたのが犯行者に割り当てられた正当な認証情報だったのか、などの具体的手法についても確認している。

[3-2-11 犯行後の行動] 犯行を隠蔽するために、何が行われたかを理解するために[3-2-11-1-4 システムログの消去]などを設問に含めた。また犯行が組織内で発覚しているか否か、あるいは捜査状況などを確認するための行動の有無を問うた。さらに犯行発覚後の犯行者が自らの犯行をどの段階で認めたか、犯行者が自らの犯行による金銭被害を賠償したかなどを事案の特徴として記録した。

4 章 被害者特徴と被害状況

4 章では被害者となった組織の特徴や犯行による被害の実際を調査することを目的に作成された。[4-1-1 被害者属性] 被害者について尋ねる項目である。企業/団体が被害を届けているケースを想定している。[4-1-1-4. 被害者概要]では被害者となった企業についてその他特筆すべき点、例えば、家族経営のアットホームな雰囲気であるとか、ワンマン経営者で閉鎖的な社風であるなどの比較的主観的な側面が犯行に及ぼす影響についても自由記述で汲み取ることを試みた。

[4-1-2-1 システム] 被害者となった企業が使用しているシステムについて確認している。[4-1-2-1-1-1]ではメールサーバや社員向けスケジューラーなど一般的な企業において使用されていると思われるシステムの候補を提示し、選択式の回答欄を設けた。

[4-1-2-2 職場環境] 被害者となった企業のセキュリティ対策を確認することを目的としている。セキュリティ対策の中にはバイオメトリクスを用いた入退室管理などに代表される[4-1-2-2-1-1 物理的アクセスコントロール]や定期的な外部監査を受けるなどの[4-1-2-2-1-3 組織的なコントロール]などが含まれると考えた。

[4-1-3 被害状況] の中では大きく内部犯行によってデータが破壊されたのか、外部に流出したのかを確認した。また[4-1-3-2 データの流出]では特にデータの外部流出の実態、すなわち流出したデータの種類、内容、データ量を問うた。また[4-1-3-3 直接的な経済的被害]では直接の被害額を記入することを目的とし、定量化が難しい内部犯行の被害額推定を試みることとした。

[4-1-4 犯行後の対応] 内部犯行については組織内で問題を処理するケースが多いと予想されるため、[4-1-4-3 公的機関への届出]で警察や JPCERT/CC などの公的機関への届出状況を確認した。

5 章 備考

5 章は備考として、1 章から 4 章まででくみ取れなかった事案の特徴や分析時の着眼点及び調査票記入者の所見などを記載することとした。

4章　人的脅威の実態

4-1　人的脅威のモデル

人的脅威のモデルを検討するために、事件特徴からの事件の類型化について検討する。この類型化の目的は、事例の要素をタイプ別に分類し考察することにより内部犯行事案の全体像と内容を把握し、これによって、

- 内部犯行事案の特質(犯行過程含む)の明確化
- 内部犯行事案への対応の検討

を行うことにある。

内部犯行事案の特質の明確化とは、1-2　調査研究の概要で述べたように、

- 犯行誘因・犯行抑止誘因を明らかにする(個人的資質含む)
- 犯行が行われた環境(人間関係を重視)を明らかにする
- 犯行が行われる時間的状況(過程、在職中、退職後など)を明らかにする

ことである。

ここでは、事件の特徴に関する情報を用いて、多次元尺度法(MDS; Multi Dimensional Scaling)による事件の類型化について検討を行った。分析に用いたソフトウェアは SPSS の PROXSCAL である。事例調査により情報を収集した 30 事例について、表 2 に示す事件特徴 6 変数、被害企業のセキュリティの脆弱性 2 変数、犯行者特徴 4 変数、犯行者と被害企業との関係 7 変数、犯行の目的 5 変数についてコーディングを行い、24 変数のバイナリーデータ(該当は 1、非該当は 0)を作成した。表 2 には、各変数についての出現頻度と出現率を示しているが、本調査が警察庁に報告された事例の全数調査ではないこと、ランダムサンプリングに基づく調査ではない事から、表中に示される出現頻度や出現率が日本の内部犯行者による事案の全体特徴を示すものではないことに

注意すべきである。しかし、類型化を行って類型別の特徴を検討する際には有用な情報であり、以降ではこれらの情報とさらに詳細な情報について検討を行う。

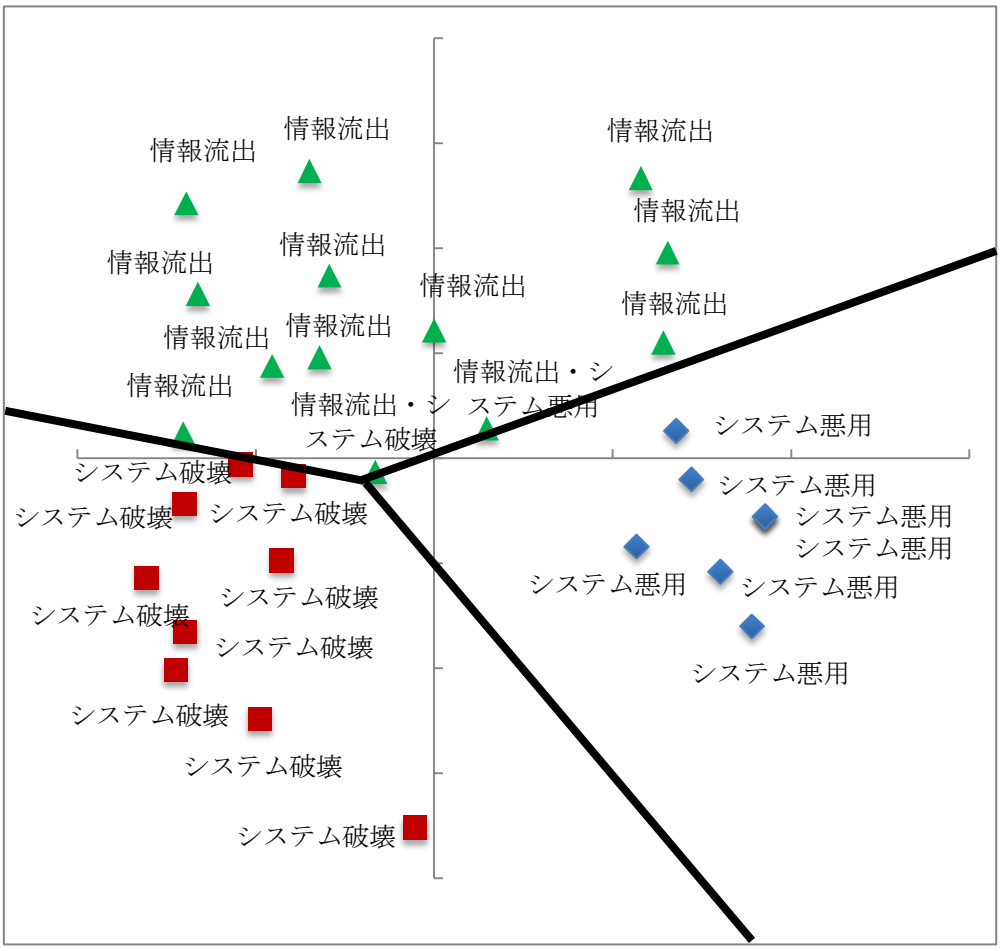
表 2　分析に用いた 24 変数の出現率

大項目	小項目	出現頻度	出現率(%)
１．事件特徴	(1)複数回犯行	25	83.3
	(2)現金被害あり	9	30.0
	(3)業務端末を利用	13	43.3
	(4)外部からアクセス	22	73.3
	(5)証拠隠滅	5	16.7
	(6)在職時の ID 情報利用	17	56.7
2．被害企業のセキュリティの脆弱性	(1)系統だった ID 付与	3	10.0
	(2)監視性低い	19	63.3
3．犯行者特徴	(1)単独犯	27	90.0
	(2)無職	8	26.7
	(3)金銭的困窮	12	40.0
	(4)ストレス：再就職が困難	5	16.7
4．犯行者と被害企業との関係	(1)被害企業の職員	12	40.0
	(2)被害企業の元従業員	18	60.0
	(3)被害企業を解雇	7	23.3

	(4)職場トラブルあり	15	50.0
	(5)システム管理を担当	11	36.7
	(6)HP 管理を担当	7	23.3
	(7)経理を担当	4	13.3
5. 犯行の目的	(1)金銭的利得目的	13	43.3
	(2)情報の換金目的	3	10.0
	(3)データ破壊	9	30.0
	(4)情報活用	11	36.7
	(5)心理的満足	18	60.0

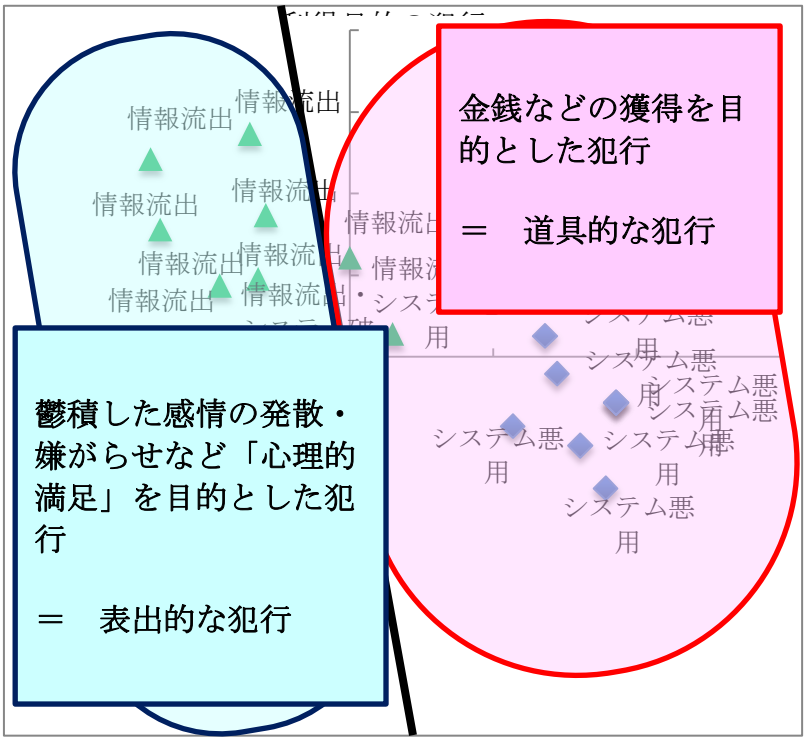
表 2 に示す 24 変数を用いて、事件間の非類似度(Lance and Williams の統計量)を算出し、それに基づいて多次元尺度構成法(SPSS, PROXSCAL)を実施した。その結果を図 6 に示す(*Stress*＝0.2027、*RSQ*＝0.9797)。図 6 に示した布置図は、分析に用いた 30 事例のそれぞれの事件の布置を示すが、パターンの似ている事件は相互に近くに、似ていない事件は相互に遠くに布置される。個々の事件については、事件の態様(システム破壊、システム悪用、情報流出)別で示した。30 事例のうち、2 事例が 2 つの事件態様を犯行で行っており、1 事例は情報流出とシステム悪用、1 事例は情報流出とシステム破壊(リンク先を変更)を行っていた。図 6 からは、事件態様別に事件のパターンが異なっていることが読み取れる。

図 6　30 事件の多次元尺度構成法の結果(*Stress*=0.2027、*RSQ*=0.9797)



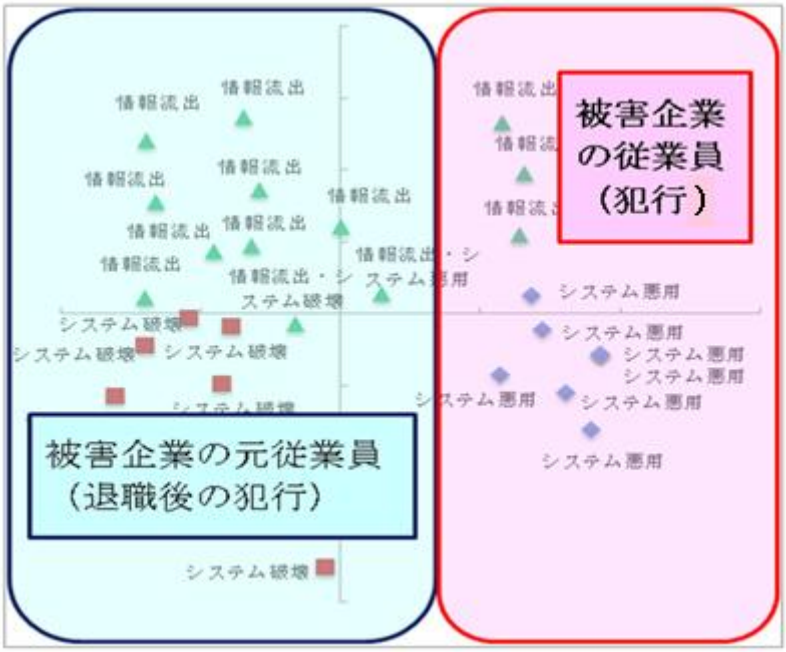
多次元尺度構成法の結果を示す図 7 からは、事件態様別にパターンが異なる傾向がある事が読み取れる。第 1 軸が正の方向では、情報セキュリティの違反行為が金銭的な利得を得る、換金のための情報を獲得するといった目的に沿った合理的な手段となっている。こうした目的を達成するために合理的な手段として犯行が行われる場合を、「道具的な犯行」と呼ぶ。これに対し、第 1 軸の負の方向では、蓄積した不満の発散や嫌がらせ、情報を把握することで心理的な優位性を保つなど、心理的満足のために情報セキュリティ違反行為がなされている。こうした犯行自体から心理的な満足を得る場合を、「表出的な犯行」と呼ぶ。これら犯行のタイプ別の分布を見ると、図 7 に示すとおりであった。道具的な犯行に該当した群では、金銭的に困窮した状態にあった者が多数を占めたが、表出的な犯行に該当した群では、金銭的に困窮した状態にあった者は殆ど居なかった。

図 7　30 事件の多次元尺度構成法の結果における犯行タイプの分布



この犯行のタイプ(道具的な犯行、表出的な犯行)と犯行時の犯行者と被害企業との関係(従業員、元従業員)とは強く関連していた。図 8 には、30 事件の多次元尺度構成法の結果における犯行時の犯行者と被害企業との関係についての分布を示した。図 8 の 30 事件の多次元尺度構成法の結果における犯行タイプの分布と比較して見ても、犯行のタイプ(道具的な犯行、表出的な犯行)は、犯行時の犯行者と被害企業との関係(従業員、元従業員)が強いことが明らかである。道具的な犯行では、被害企業の現職員が金銭的な困窮状態の改善を目的として犯行を行っている場合が多く、表出的な犯行では、被害企業の元従業員が被害企業に対する不満や鬱憤の発散のために外部からアクセスして犯行を行っている場合が多く、同様の理由から退職時に内部で犯行をして被害企業を去ったものもこの群に含まれている。

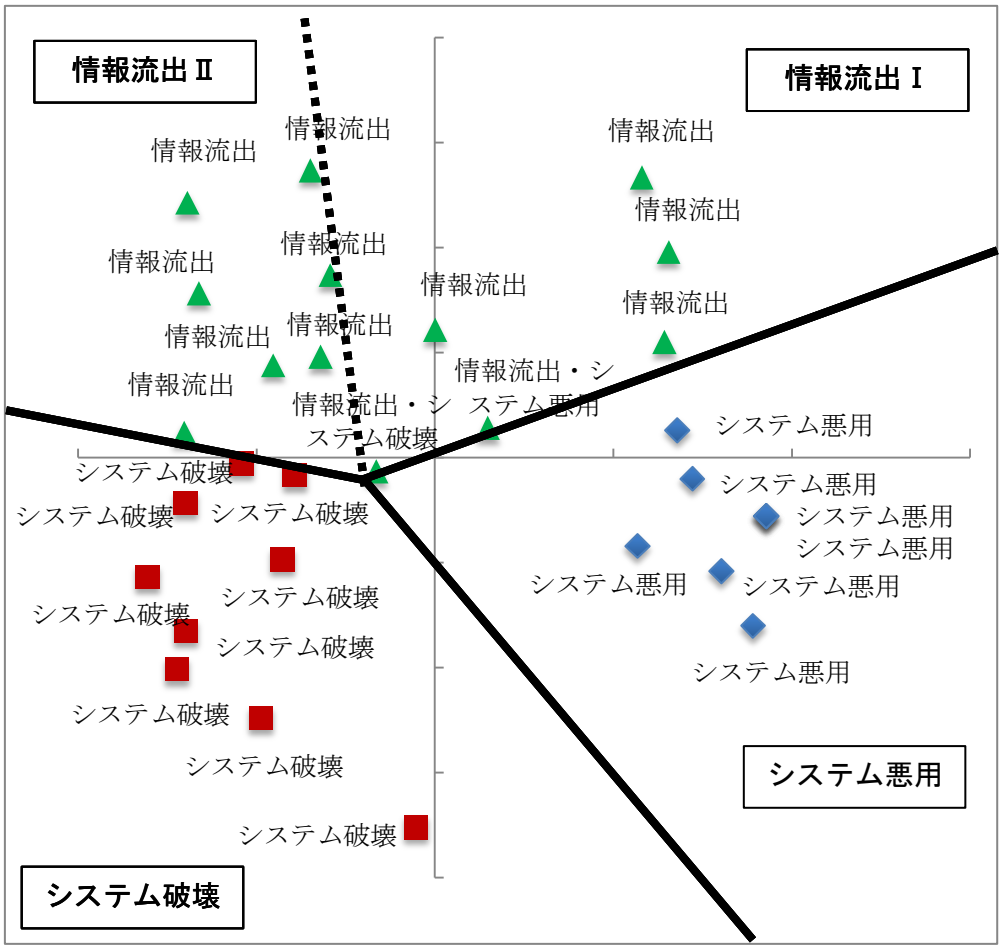
図 8　30 事件の多次元尺度構成法の結果における犯行時の犯行者と被害企業との関係についての分布



この犯行時の犯行者と被害企業との関係(従業員、元従業員)は、犯行者の職場でのトラブルの有無と強く関連していた。犯行時に被害企業に勤務している群では、職場トラブルは殆ど認められなかったが、犯行時には被害企業を退職していた元従業員の群では、殆どの者において退職前に職場でのトラブルが認められ、明らかな職場でのトラブルが認められなかった場合でも、職場や上司に対する強い不満を抱えていた。

こうした顕著な違いが 2 群間には認められたため、事件の態様(システム破壊、システム悪用、情報流出)別の分類に、さらに犯行のタイプ(道具的な犯行、表出的な犯行)を考慮する必要がある。この布置図と事件の態様(システム破壊、システム悪用、情報流出)との関連を見ると、システム悪用は道具的な犯行であり、システム破壊は主に表出的な犯行である。これらに対し情報流出は、換金を目的とした道具的な犯行(情報流出Ⅰ)と、不満の発散や嫌がらせ、情報を得ることで心理的に優位に立とうとする表出的な犯行(情報流出Ⅱ)とに分類できると考えられた。これらのことから、内部犯行者による事案は、①システム悪用、②システム破壊、③情報流出Ⅰ(道具的な犯行)、④情報流出Ⅱ(表出的な犯行)の 4 つに分類することができる(図 9)。

図 9　内部犯行者による情報セキュリティ事案の 4 分類



以降では、これら 4 つのタイプについて、犯行の態様を検討し、対策を検討することとする。

4-2　人的脅威の類型別の検討

4-2-1　類型別による検討

前項で見いだされた①システム悪用、②システム破壊、③情報流出Ⅰ(道具的な犯行)、④情報流出Ⅱ(表出的な犯行)の 4 つのタイプに各事例を分類したところ、①システム悪用に 8 事例、②システム破壊に 9 事例、③情報流出Ⅰ(道具的な犯行)に 8 事例、④情報流出Ⅱ(表出的な犯行)に 8 事例が該当した。3 事例については、道具的な犯行と表出的な犯行の双方が行われていたため、情報流出Ⅰと情報流出Ⅱの双方でカウントすることとした。ここでは、類型別での特徴の違いを把握するため、また各事例の匿名性

を保つため、(1) 個人的・人格的特質、(2) 環境要因、(3) 犯行状況についてのみ 4 分類の簡単な比較を行うこととした。

(1) 個人的・人格的特徴

個人的・人格的特徴として、ここでは、性別、年齢、学歴、職歴、IT 技術、趣味・嗜好、借金、人柄、前科前歴、履歴書について検討を行った。性別については、いずれの類型でも男性が犯行者の主体をしめるが、女性はシステム悪用で多く認められた。

学歴については、いずれの類型も、高卒程度から大卒程度まで幅広く分布している。相対的には、システム破壊と情報流出Ⅰで大卒程度の者が多かった。

職歴をみると、いずれの類型でも転職歴を有する者が多くを占めており、転職回数が 3 回以上となる者が多い。相対的には情報流出Ⅱで転職回数が少ない者が多かった。

IT 技術については、簡単な PC 操作ができる程度の者から、システム開発やシステム管理の能力を持つ者まで幅広い。システム悪用では、それほど高い IT 能力を有さなくとも、業務で使用している端末が使用できる程度の IT 技術の者が多くを占めていた。それに対し、システム破壊や情報流出Ⅰ、情報流出Ⅱでは、システム管理やホームページ管理などの IT 技術やネットワーク構築についての知識を持つ者など相対的に高い IT 技術を有する者が多かった。

趣味･嗜好については､多様なものが挙げられているが､システム悪用と情報流出Ⅰで、高級クラブや競馬、パチンコなど、繰り返し楽しむためには、遊興費として多額を要するものが多く挙げられていた。

借金については､いずれにおいても住宅や車のローンに該当する者がいたが、システム悪用と情報流出Ⅰについては、それ以外の借金を有していた者が含まれていた。システム破壊で、借金のない者が相対的に多かった。

人柄については、きまじめなタイプや、人当たりのいい人もいれば、対人関係が苦手なタイプや虚言などの問題行動が認められる人がいる。システム破壊では、短気や対人関係が苦手なタイプなど職場での円滑なコミュニケーションを阻害するような性格特徴が相対的に多く挙げられていた。・

前科前歴については、ない者が多くを占めるが、ある場合には、窃盗や占有離脱物横領など何かを窃取するものが多くを占めていた。システム悪用には、1名ではあるが、同種の前科を有する者もおり、一部にシステム悪用を繰り返す者がいることがわかる。

履歴書については、入社時の履歴書に虚偽の記載をしていたことが明らかであった者を示した。入社時の履歴書に虚偽の記載をしていた者は数は少ないが一部におり、情報流出Ⅰには該当はなかったが、システム悪用やシステム破壊で、相対的に多かった。

表 3 個人的・人格的特質

分類	システム悪用(9)	システム破壊(10)	情報流出Ⅰ(道具的)（(7)	情報流出Ⅱ(表出的)（(8)
性別	男性(5) 女性(3) 女性複数	男性(9) 女性(1)	男性(7)	男性(8) ※Ⅰと2件重複
学歴	・大卒 ・短大卒 ・高卒(3) ・専門学校卒(4)	・大卒(国内、2) ・大卒(外国、4) ・短大卒 ・高卒(3)	・大卒(5) ・大学中退(1) ・専門学校卒(1)	・大卒(2) ・大学中退(1) ・専門学校卒(1) ・専門学校中退(1) ・高卒(2) ・高校中退(1)
職歴	・ ・アルバイト等を頻回転職 ・転職5回 ・転職3回(2) ・転職1回(前職は解雇) ・転職1回（前職で自営が倒産) ・なし(3)	・転職7回(いずれも会社都合の退職) ・転職4回 ・転職3回(3) ・転職2回(3) ・なし ・不明	・転職3回(3) ・転職2回 ・転職1回(2) ・なし	・転職4回 ・転職3回(2) ・転職2回 ・転職1回(3) ・なし
ＩＴ技	・ＰＣ操作やネッ	・PC操作、HP作	・情報管理やPC	・システムエンジ

術	トバンキングができる(2) ・業務端末を使用できる程度(3) ・ＰＣ操作やファームバンキングができる ･プログラム言語、インターネットを理解 ・サーバーのユーザー管理	成に習熟、 ・英語に高い能力 ・自宅に PC、インターネット接続 ・システム管理、サーバの拡張、設計、保守、運用管理ができる ・ネットワーク設計・製造 ・コンピュータ言語、HTML を勉強、インターネットの知識あり ・インターネットの知識あり ・PC に強い ・DTP(2)	に関する知識あり(それほど高い知識ではない)(2) ・社内の PC 管理、LAN 管理ができる ・システム開発の経験あり ・システム開発、システム管理などができる ・システム管理ができる ･HP 作成、管理ができる	ニア ･初級システムアドミストレイター ・設計 ･Web デザイナー ・ネット販売ができる ・PC 操作ができる ・システム管理ができる
趣味・嗜好	・高級クラブに月 2～3 回通う ・パチンコ ・ネットショッピングと競馬 ・オンラインゲーム ・インターネット ・競馬	・英会話教室に通う ・写真撮影(2) ・映画鑑賞 ・漫画や歴史本の読書 ・コンピュータとつり	・たまにパチンコ ・車いじり ・サーフィン ・つり、ストレス解放の為に夜遊び ・インターネット	・PC とつり ・花の写真 ・PC 組み立て ･インターネット
借金	・過去に自己の経営する会社が倒産、借金あり ・店舗経営で借金がふくれる ・夫が働かず、借金の返済が止まっている	・なし(6) ・車のローン(約 30 万) ・住宅ローン ･親への借金が 50 万円以下 ･借金 200 万円以下	・借金 100 万円以下 ・住宅ローンが 2000 万～3000 万円以下(2) ・借金 200 万円以下 ・住宅ローン	・なし(6) ･住宅と車でローン月 26 万円

	・家の購入代金の借金あり、夫がまともに働かない ・車の購入代金 ・なし(4)		3000 万円弱と消費者金融 600 万円弱	
人柄	・腰が低く、人当たりがよい。面倒見のよい人 ・破れかけのズボンを履くなど疲れたサラリーマン ・我慢強い、おとなしい ・自己顕示欲が強く、何か必ず文句を言うタイプ ・職場ではうざいと、疎まれていた ・幼稚な考え方をする	・要領が悪く、ミスに向き合えない、コミュニケーションが下手 ・機敏に動いて覚えも良くしっかりした人 ・おとなしい ・コミュニケーションが苦手 ・虚言癖あり ・順応性はあるが、短気 ・正義感が強いが、短気	・温厚だが、おっちょこちょい ・基本的には、好青年 ・まじめ、仕事を頼まれると断れない性格 ・幼稚な考え方をする	・気が短く固執的な考え方をするタイプ ・人見知りをしないが、一つの事にこだわりすぎる面がある ・幼稚な考え方をする ・部下から慕われている
前科前歴	・なし(5) ・勤務先での業務上横領と窃盗で刑務所入所歴あり ・窃盗 ・脅迫 ・商標法違反 2 件	・なし(6) ・占有離脱物横領 2 件 ・占有離脱物横領 ・万引き、窃盗 ・万引き	・なし(6) ・脅迫	・なし(6) ・占有離脱物横領 2 件 ・脅迫
履歴書	・虚偽の記載あり(2)	・虚偽の記載あり(3)		・虚偽の記載あり(1)

注)不明であったものについては、記載していない

(2)環境要因

環境要因として、ここでは、業務の専門性、業務の監視性、職場への不満をとりあげた。

業務の専門性については、それぞれ分業化され、専門化された業務に就いている者が多かった。システム悪用では、経理を担当する者の他、通常業務で個人情報を扱う端末を使用する者などがいた。システム破壊では、システム管理やホームページ管理、翻訳業務、秘書業務、広告業務など多様な業務の者が該当していた。情報流出Ⅰでは、システム管理やホームページ管理などの業務の他、事業部を統括する立場にある者が含まれていた。情報流出Ⅱでは、コンピュータの管理やWebデザイナーの他、営業、設計業務、事故調査業務、本社幹部などであり、システム破壊と同様に多様な業務の者が該当していた。

業務の監視性については、全体的に低い状況が伺われた。システム悪用では、その業務の専門性から当該業務を全面的に任されており、他に理解できる人がいないことから、実質的には監視性は全くない状況にある者もあった。また、同様業務の担当が多い場合でも、上司が全ての担当者について監視性の高い状態を維持する事は難しく、個別の監視性が低くなる場合があった。システム破壊では、上司による監視が主であったが、信頼して任せているために、逸脱行為がなかなか明らかにならない場合が多かった。情報流出Ⅰでは、実質的な責任者である場合や、逸脱行為がなかなか明らかにならない場合があった。情報流出Ⅱでは、職場での相互間の監視性が低い場合が多かった。

職場への不満については、何らかの不満を抱えている者が多かったが、システム悪用と情報流出Ⅰにおいては、特に何ら不満を感じていなかった者が相対的に多かった。職場への不満の内容を検討すると、システム悪用では、経営支援のシステム自体に不信感を抱いていた者や、経営者や上司の態度に強い不満を抱いているものがいた。システム破壊では、能力が認められず解雇されたり、慣れない業務を担当させられて低い評価を受けたり、努力や能力が評価されないといったことが不満の内容として多くを占めていた。情報流出Ⅰでは、上司とそりが合わないことや、経営者との対立、多忙や責任の重圧によるストレスの他、業績が上がらない為に収入減少へのストレスを感じていた者などがいた。情報流出Ⅱでは、経営者や上司からの屈辱的な扱いや、対立場面での上司との喧嘩など具体的な出来事を恨みに思っていた者や、能力の評価や報酬が期待より低いことを不満に思う者の他、経営方針や経営者の生活態度への疑問などが挙げられていた。

表 4 環境要因

分類	システム悪用(8)	システム破壊(9)	情報流出Ⅰ(道具的)(8)	情報流出Ⅱ(表出的)(8)
業務の専門性	・経理は、他にアルバイトが 1 人 ・親族で経営している ・他に経理の知識のある人がいない ・振り込み関係の担当は 2 人 ・振り込み作業は全面的に任されていた ・オペレータ ・全面的に任され、実質上司はいない状態	・翻訳業務 ・ホームページ更新業務 ・秘書業務 ・システム管理、サーバの拡張、設計、保守、運用管理(これらの能力は平均以下と評価されている) ・HP の作成管理(2) ・広告関係の実質的責任者 ・営業 ・システム管理	・インターネット導入に伴うプロバイダ契約からメールシステム導入までを担当 ・もともとはエラー時対応のため担当現場のメールを自宅 PC でも受信できる設定にしていた ・システム管理(2) ・HP の作成管理 ・営業関係事業部のマネージャー	・システム開発業務から営業に変更 ・コンピュータの構築、管理 ・設計業務 ・Web デザイナー ・事故調査等を担当・本社幹部
業務の監視性	・帳簿の帳尻さえあえば、振り込み手続きの内容についてチェックする人はいない(4) ・使用者側の人間なので、口出しをする人はいない ・上司に経理の知識はなくノーチェック ・原則として 1 人 1 人が異なるスケ	・上司による監視あり。ミスが多く、得意先からもクレームが入る ・ホームページ更新作業は任されており、自宅からも作業できる環境にしていた ・上司による管理(3) ・取締役なので、口出しをする人は	・業務が細分化されており、実質的な責任者で、他の人からチェックされることはない ・他に詳しい人はいない(3) ・社内では監視性が高いので、ネットカフェからアクセス	・監視性は低い(2) ・同僚も同様のことをしており、相互監視の力は弱い

	ジュールで動くため、監視の継続は困難 ・多数のオペレータが同時に勤務しており、個別の監視性は低い ・口出しをする人はおらず、1人の勤務もあり	いない ・ホームページ更新作業は任されていた ・システム管理は任されていた		
職場への不満	・店舗経営について借金が増えていくばかりで経営支援のシステムのあり方に不満があった ・経営者の横柄な態度に強い不満・無理してこなしている業務を認めてもらえない ・上司の態度に強い不満 ・特になし(4)	・理由も聞かされず突然の解雇 ・慣れない業務を任せられ、家庭との両立が難しくなり、ストレスを感じていた ・転職先で解雇の対象となり、前勤務先に職を求めたが断られた ・当初説明を受けた業務とは異なる業務を担当させられ不満に思っており、退職金のトラブルへの上司の対応には強い不満を抱いていた ・待遇が期待はずれであり、経営者の経営態度に疑問を感じていた(最終的にケンカ別れ)	・経営者の親族が直属の上司となり、その上司と折りがあわず、ストレスに感じていた ・仕事量が増えた事と、責任ある地位に就いたことから、強いストレスを感じていた ・報酬や会社の経営方針をめぐって経営者と意見が対立したが、経営者の対応に強い不満を抱いていた ・特になし(業績が上がらず、職場での評価が下がることや収入の減少を心配し、精神的に追	・営業の実績が上がらず経営者から屈辱的な扱いを受け、経営者の生活態度にも強い不満を抱いていた ・上司や同僚と意見の食い違いがあり嫌気がさしていたところ、上司と大喧嘩して逃げ出すように退職 ・自分がリストラで辞めさせられたのに、能力が高くない上司が解雇されないことに対して強い不満や恨みを感じていた ・転職の際に提示されたものと給料や労働条件が

		・給料をもらえず生活に窮していたのに、経営者の対応に強い不満を抱いていた ・半ば強制的な解雇に対する腹いせ ・努力が評価されない、重要なプロジェクトを立ち上げたが十分な支援がえられない、会社のためを思った発言を非難される	い詰められた) ・特になし	異なっていたので、経営者に裏切られた気持ちでいた ・時間外の手当が一切なく、ボーナスなし、仕事の進め方がワンマンだったことに不満があったが、経営者から人前でうだつが上がらないと指導を受けたことを屈辱に感じていた ・経営者の態度に不満を感じ、経営者から嫌がらせをされているように感じていた ・会社の経営方針に強い疑問を感じていた

注)不明であったものについては、記載していない

(3)犯行状況

犯行状況として、ここでは、犯行手段、動機、破壊・流出データ、犯行後の行動をとりあげる。

犯行手段は、類型別で大きく異なっていた。システム悪用では、日常業務で従事している作業や端末を利用していた。思いつきで行った者から、人や新聞記事から学んだ知識を実行してみた者まで様々である。システム破壊では、日常業務で使用していたシステムに、組織の内部または外部からアクセスして犯行を行っていた。この場合、自分が使

用していたIDとパスワード使用する他、組織内で共有していたIDとパスワードを使用したり、同僚のIDとパスワードを使用したりしていた。情報流出Ⅰでは、業務として使用していたシステムを使用した者の他、情報収集のためにキーロガーを仕掛けたり、退職前に職場の人間のメールを自宅で自動受信設定をしていたものを利用していた者がいた。情報流出Ⅱでは、退職前に職場の人間のメールを自宅で自動受信設定をしていたり、システムにアクセスできる環境を設定していた者が多数を占めていた。

動機については、類型別で大きく異なっていた。システム悪用では、借金返済や経済的な余裕のなさなど、経済的な逼迫感から動機が形成されている者が多かった。また、数は少ないが、もったいないからという軽い気持ちで動機が形成されている者もいた。システム破壊では、経営者や上司への嫌がらせや鬱積した感情の発散のために犯行を行っている者が多く、中には、その後自分を頼って来る事を期待しての犯行もあった。情報流出Ⅰでは、経済的な逼迫感から生活費を捻出するために個人情報を換金することを目的とした者が多かったが、個人が関わる事態に活用する為の情報が欲しいという動機もあった。情報流出Ⅱでは、嫌がらせのためや、中傷のネタを探すことを目的としたものの他、被害組織や幹部の情報を自分が把握することによって、心理的に優位な立場に立とうとすることを目的としたものがあった。

破壊・流出データについては、システム悪用に該当はないため、システム破壊、情報流出Ⅰ、情報流出Ⅱについてみていく。システム破壊の場合、自分が業務で開発したり管理していたシステムの情報を対象とした場合が多く、それらの情報を削除することで、被害組織の業務に多大な障害を与えるものが多かった。情報流出Ⅰでは、個人情報、特に顧客情報を対象としていた。情報流出Ⅱでは、被害組織の幹部や組織の情報が対象となっていた。

犯行後の状況については、システム悪用では、犯行後に逃走したり、犯行の直前直後に退職してしまった者が多かった。これに対して、システム破壊や情報流出Ⅰ、情報流出Ⅱではそのまま勤務していた者やそのままの生活を続けていた者が多くを占めていた。

表 5 犯行状況

分類	システム悪用(8)	システム破壊(9)	情報流出Ⅰ(道具的)(8)	情報流出Ⅱ(表出的)(8)

犯行手段	・業務で行っている作業(4) ・人から教わった手段 ・業務上横領の事件に関する新聞記事を参考にした ・試しにやってみたらできたので、実行 ・人に教わって、キーロガーを仕掛ける	・業務で使用していたHP管理システムへ、前任者のIDとパスワードを使って ・業務で使用していたHP管理システムに管理者IDとパスワードを使って(2) ・業務で使用していたシステムに、管理者IDとパスワードを使って ・業務で使用していたPCに自分のIDとパスワードで入って ・業務で使用していたサーバに同僚のIDとパスワードを推測して入って ・外部から業務で使用していたサーバに業務のＩＤとパスワードで入って ・元同僚のＩＤ，パスワードを使って	・メールシステムのメンテナンス業務を通じ換金可能性のある情報が組織内でメールでやりとりされていることを察知し、退職後もメール受信可能な状態を維持 ・業務として管理していたサーバに個人情報があった(2) ・社内的な対立があり、相手方の動向を把握するため他の従業員のPC使用監視のためキーロガーを仕掛けた ・HPの連絡先を変更し、そこへの連絡内容を盗み見し、そこで得られた売却して利益を得た情報を売却して	・退職前には、業務のために自宅からサーバに接続できる設定にしており、管理者用のIDとパスワードを使って ・退職前から、会社幹部のメールを自宅で受信する設定にして見て楽しんでいたが、退職後も幹部や同僚のメールを自動受信して見ていた ・自宅から自分のIDがまだ残っていたので、メールをみたり、恨みに思っていた上司のID、パスワードを推測して ・勤務先から、元勤務先のシステムに管理者IDとパスワードを使って ・退職前に自宅から会社のサーバにアクセスできる環境にしており、元勤務先の社員のIDとパスワードを推測して

				・退職前にシステム管理のIDとパスワード情報を入手しておいた ・直属上司のIDとパスワードを知っていたのでそれを利用して
動機	・借金の返済に充てるため(2) ・経営不振で追い詰められて ・過酷な労働の欲求不満解消と仕返し ・配偶者がまともに働かないことによる生活不安 ・借金の返済と経済的な逼迫感から ・ポイントが捨てられるのはもったいないから ・経済的に余裕がなかったことから	・職が見つからずいらいらしており、これは解雇されたせいだと思いついて、衝動的に ・すぐに正社員として雇ってもらえると期待したのに、期待を裏切られたから ・対応に強い不満を抱いていた上司を困らせようと思って ・嫌がらせ ・経営者に対する嫌がらせ ・自分では実績も上げ経営者の意向にも沿って仕事をしていたつもりなのに一方的に解雇されたため ・経営者や役員たちの対応に腹が	・職が見つからず、生活費もままならなくなり、少しでもお金を稼ぎたい ・個人情報を換金して借金をできるだけ減らしたい(2) ・上司に報告する為の情報が欲しい ・元勤務先経営者への恨みと生活費を捻出するため	・飲酒時に、ふと嫌がらせをしてやろうと思いついて ・会社が訴訟に巻き込まれ、いい気味だと思い、あわてている様子が見たくなって ・引き継いだ業務の状況が知りたくて ・元の会社と係争中であり、他者ともトラブルがないかの情報を得るため ・社内情報を把握して、中傷ネタを探し、公開されている掲示板に書き込むため ・転職後のモチベーションを高めるため

		立っていたため ・自分を頼って連絡してくると思って		
破壊・流出データ		・受注業務管理情報 ・HP に自分が作成して掲載したデータ ・ポータルサイトのデータ ・過去に自分が作成管理していた Web サイトの顧客データ及び商品データ ・自分が管理を担当していたホームページの更新管理に必要なデータ ・ホームページ上の記事 ・自分が管理していた Web サーバ上のインデックスファイル ・メールアカウントの削除 ・サイトのトップページデータ	・競合企業への経営情報提供 ・業務で管理していたサーバ上の個人情報(2) ・業務で管理していた HP への登録情報	・元勤務先の経営者と愛人のメールの内容 ・元勤務先の会社幹部のメールの内容 ・元勤務先の上司のメールの内容 ・採用情報 ・会社の機密情報
犯行後	・逃走 ・逃走 ・逃走 ・発覚前に退職	・解雇後の犯行、就職活動中 ・退職直前の犯行、その後退職	・退職後の犯行(表向きは円満な退社) ・退職後の犯行	・勧誘されての転職後の犯行 ・大喧嘩して退職後の犯行

	(2) ・発覚前に休業 ・そのまま勤務(2)	(3) ・退職後、就職活動中の犯行、そのまま ・退職後の犯行(3)	(方針が合わず退職) ・そのまま勤務(2)	・会社を見限って自主的に退職、求職中の犯行(2)

注)不明であったものについては、記載していない

4-2-2　人的脅威の類型の特徴

以下では、前項でまとめた表の内容について、補足的に特徴点などについて説明する。

(1)　個人的特性・状況

1　犯行関係者

1.1　単独、複数

今回の調査対象では、ほとんどが単独での犯行である。

ただし、形式的に単独犯であっても、例えばリストラのために解雇されたような場合、解雇された者は犯行者だけではないし、企業が生き残りのために合併したような場合には、出身企業別のグループのようなものが形成される場合がある。犯行者は、それらの集団内での情報共有やグループへの対抗者への何らかの行動の準備といった目的で情報へのアクセスを行うようなケースはみられる。

また、犯行目的が経済的な利益の場合、他の犯罪形態と同様、複数人が意図を共有して犯行に及ぶことはあり得る。

更に、個人情報その他の情報を販売することにより利益を得ようとしるようなケースについては、これが売買されるマーケットの存在といった環境が存在していることが前提となっている。

2　個人的特性

2.1　犯行者には継続勤務が困難で頻繁に転職を繰り返す者が見られる

2.2　逃避的行動・安易な行動

結果について十分考察せずに、行動を行うような性格的傾向を有する者がいる。

2.3　自己本位の認識

自ら構築に深く関わったシステムなどを攻撃し、破壊するケースも見られる。このようなケースの場合、愛着や関心を有しており、破壊に至る前に何らかのアクセスを行っているケースもある。こうした愛着や関心、さらにはこうしたシステムを構築したとの自負心が、自らを評価しなかった関係者に対する恨みにつながり、犯行に及ぶというケースが見られる。このような場合、アクセス方法についても犯行者は知っておりさほど困難なくアクセスできること、また自ら作成したものであるためこれを改変・破壊することや利用して利益を得ることに躊躇がないことなどから、犯行に当たり、深く意識することなく、一時の感情にかられて犯行に及ぶことがある。こうしたことが、退職後一定期間を経過したような場合であっても犯行がなされることの背景になっている。すなわち、一定期間が経過し、ある程度犯行者の身辺も退職時のような慌ただしさがなくなり、ふっと時間が空いたようなときに犯行が行われることがある。このようなケースは、退職後の生活の確保も含めた多忙さのようなものがなくなり、その意味で犯行の抑止要因も失われている状況であるとも言える。

その他のものも含め、自己本位の認識の例を挙げれば次の通りである。

2.3.1 自らが作成したシステムのケア、自らの担当業務の経緯の確認

2.3.2 過剰な「正義感」(グループの場合含む)

2.3.3 相手の「非」への対応

3　直接的な犯罪誘因

直接的な犯罪を引き起こす状況として、飲酒や時間的余裕といった環境と、関係する組織への感情の高まりがある。

(2)　組織・企業

- 組織・企業規模
  - 小規模の組織・企業の場合の問題点
    - 事業規模の小さい組織の場合、特に上位の者が抑圧的な行動をとっているような場合、そのはけ口として情報・システム破壊が発生することもある。
    - 情報・システム破壊は、事業に深刻な影響を及ぼす可能性もあるが、犯行自体は、既に入手しているID・パスワードを使用してのデータ編集など、犯行者にとって手慣れた手法で行うことが可能である。
    - 従って、これを行うに当たって大きな心理的・物理的な障害はない。
    - 一見「暇だからやった」ように見える事案もある。或いは、それに飲酒という状態が加わっていることもある。しかしながら、このような場合であっても、犯行者の性向によるものばかりではなく、犯行者の心理的な状態からやむにやまれぬ思いで行為に及んでいるケースもある。そして、そのような心理的な状態に陥る理由として職場環境が影響を及ぼしている場合がある。
- 組織・企業スタイル
  - 経営者のスタイル
  - 社員の待遇
  - 職場の雰囲気、コミュニケーションスタイル

これらの要素は、客観的な考察に加え、犯行者の主観的なとらえ方がどのようなものかが重要である。

経営者がワンマンであったり、組織の資金を私的に利用している、愛人を持っているといった噂、自分や他の社員の待遇についての情報等は、自らに対する仕打ちとそれに対する自己の感情に加え、これを明らかにしたり、経営

者に「警鐘を鳴らし」「制裁を加える」ことは正しいことであるとの一方的な思い込みを持ち、これが犯行に駆り立てる一つの要因となることもある。今回の調査では、問題事例のみを見ているわけだが、問題が発生していないような企業、ないしは兆候の段階で対応ができている企業は、上下間・職員間のコミュニケーションが確保されているのではないかと思われる。

– 企業の経営状況・環境
  統合・合併企業の場合、善意であるかどうかに関わりなく双方のコミュニケーションがうまくいかないことがあり、また経営拠点が複数である場合にも同様にコミュニケーションの問題が生じ、これが犯行者の「理解してもらえない」といった感情につながり、行動に結びついていくことがあり得る。

– コンプライアンスのための体制・実際
  ほとんどの企業では、契約書で情報の保護について定めており、また、退職後についても情報漏洩について禁じる文書を用意している。これの定着のための努力については今回の調査対象とした資料からは判然としない。

(4) 情報システム

1 攻撃の状況

1.1 情報システムアクセス手法

1.1.1 内部から

1.1.1.1 システムの悪用

被害が発生しているケースについては、犯行者が上司・経営者の信頼を得ているケースがほとんどであり、特に小規模な組織においては、発覚するまで特に日常的な管理体制は整備されていなかったものが多い。

1.1.1.2 人間関係の悪用

情報セキュリティのためのシステムがしっかりと構築されている

場合には、情報(システム)へのアクセスに際し、手続きのいずれかの段階で人間が関与してくることになる。例えば、特定のデータにアクセスする場合には、必ず複数でアクセスするとか、常に物理的なアクセス管理がなされ人の監視のある場でアクセスするなどの条件が付されている。内部犯行者は、このような場合に、人間関係を利用して手続を簡略化したり、虚偽の申し立てによってアクセスを確保したりしているときがある。特に、犯行者が十分な経験・知見・地位・アクセスを管理している者との人間関係等を持ち、アクセスを管理している者がこれらの点で劣っている場合(地位が低い,経験が浅い又は派遣社員である、どのような場合に当該情報にアクセスできるかについての十分な知識がないなど)には、本来拒否されるべきアクセスが許容されてしまうことがある。また、本来、人間は他の者に親切にしたい、との気持ちもある。こうした点を突いて犯行者は本来許されないアクセスを行う場合がある。

1.1.2 外部から

今回調査分では、外部からの攻撃は一般のインターネットを介しての攻撃で、VPN や専用線を利用したものはなかったが、可能性としては当然あり得る。また、バックドアやクラッキングの例も含まれていないが、脆弱性を突いた外部からの攻撃による被害は、内部犯行によらなくても参考文献に挙げている日本ネットワークセキュリティ協会の資料にもあるとおりかなりの件数に上っている。内部者が行おうとした場合にはより容易に行うことができるのは当然であろう。

1.1.2.1 利用回線

1.1.2.1.1 インターネット

1.1.2.1.1.1 一般(※件数)

1.1.2.1.1.2 VPN

1.1.2.1.2 専用線

1.1.2.2 ID・パスワードの利用

1.1.2.2.1　　自己の ID、パスワード使用

1.1.2.2.2　　他の職員の ID、パスワード使用

1.1.2.2.2.1 現職の他の職員の ID、パスワード使用

1.1.2.2.2.2 退職した他の職員の ID、パスワード使用

1.1.2.2.2.3 他の職員の ID、パスワードの推測

1.1.2.2.3　　特異な例として、フィッシングによる入手がある。

1.1.2.3 バックドア、クラッキング等

1.2　システム悪用

これは、汎用システムの利用がほとんどである。

犯行者の行動のチェックのための体制の有無が課題になる。

1.3　情報・システム破壊

次のような類型が見られる。

1.3.1 データ破壊

1.3.1.1 情報提供ホームページの削除

1.3.1.2 イントラネットのデータ削除

1.3.2 データ利用不可

1.3.2.1 ファイルにパスワードをかけるなど

1.3.3 システム破壊

1.3.4 システム利用不可

1.3.5 システム利用不可につながる行為

1.3.5.1 スパムメール、DOS を誘引する行為

1.3.5.1.1　　他の者のメールアドレスを迷惑メール業者に登録

1.4　情報流出

情報システムへのアクセスが前提となる。
大量のデータの入手については、現職中に行われることになる。
入手した情報は、情報自体の販売、情報を利用しての事業、恨みのような感情の発散などに利用される。

1.5　証拠隠滅

1.5.1 アクセスログの消去を行っているケースがある。

2　情報システム構築体制

2.1　単独、少人数など

かなり大きな組織でも、全体を見て管理しているような層は少ないことが見て取れる。構築・運用時に、複数の主体が実質的に関与するような体制が構築されているか、業務についてチェック体制がととのっているかがポイントになる。

3　情報システム管理体制

3.1　情報システム構築後のシステム運用体制

2.1 参照

4　情報システム保護体制

4.1　物理的保護体制

4.2　情報システムへの、入退室管理を含む物理的な保護体制に付いては、必ずしも十分でない。

特に、業務に利用するシステムについては、組織外からのアクセスも含めて業務効率との対立がある。どのようなシステムを構築するかは、組織としてのトップマネージメントの判断が重要になる。

4.3　システム的な体制

4.3.1 当該企業・組織としての体制

4.3.1.1 アカウント情報の保護

4.3.1.2 パスワード及びそのメンテナンス体制の課題

かならずしも ID/パスワード方式にアクセス管理の方法に限られているわけではなく、重要情報の操作に入室管理などの物理的な保護措置を高じている企業もある。

また、同僚の ID・パスワードを知っている、同一の ID・パスワードを共有しているなどのケースも見られた。

4.3.1.3 退職時のアカウント無効化

4.3.1.4 退職決定後のアカウント無効化

退職後のアカウントの無効化は当然であるが、それでも手続きミスを含めてなされていない例が見られる。また、同僚など他の内部者の ID/パスワードを用いた例もある。更に、退職決定後実際の退職までの間に犯行に及んだ例もある。

(5)　被害・影響の大きさ

1　システム悪用

システム悪用は 8 件あるが、いずれも経済的な利益を目的としたものである。

被害額としては、様々であり、舞台となった企業からするとかなり大きな額であるものもあるが、今回調査対象の企業にはそれによって倒産や事業縮小に追い込まれるなどの状況に至ったものはなかった。

2　情報・システム破壊

情報や情報システムの破壊については、バックアップのないところもあり、特に中小企業の場合 100%の復旧は難しいケースもある。

3　情報流出

情報流出に関しては、組織・企業、一般の方々とも意識が高まっている。それだけに内部犯行のような形で情報が流出した場合、企業は、一般の顧客やユーザとの関

係で直接的に情報が流出した関係者に経済的補償を行うようなケースもある。さらに、取引先から損害賠償を求められることもあり、企業の「評判」が大きな価値になっていることを考えると、被害は甚大である。

特に、中小企業の場合、情報が流出したことにより業務の縮小をせざると得なくなっているようなケースもある。

なお、被害・影響の大きさは、犯行者がある程度認識している場合もあるが、そうでない場合もある。その意味で、被害組織・企業においては、犯行者の意図と関わりなく、被害の実態を把握し、これに対応する必要がある。

4-2-3　ダイナミック・モデル

以下では、前項までで検討したシステム悪用、システム破壊、情報流出Ⅰ、情報流出Ⅱについて、犯行者の心理的な力動過程(ダイナミクス)をふまえた上で、抽象化した形で事案が発生する流れ・動きをまとめておく。ここで紹介する典型例については、事案が特定できないように主要でない情報を修正した上で、個々の犯行者が犯行に至るダイナミクスを提示することによって、事案の特徴を把握することを可能とするためのモデルである。

システム悪用のダイナミクス

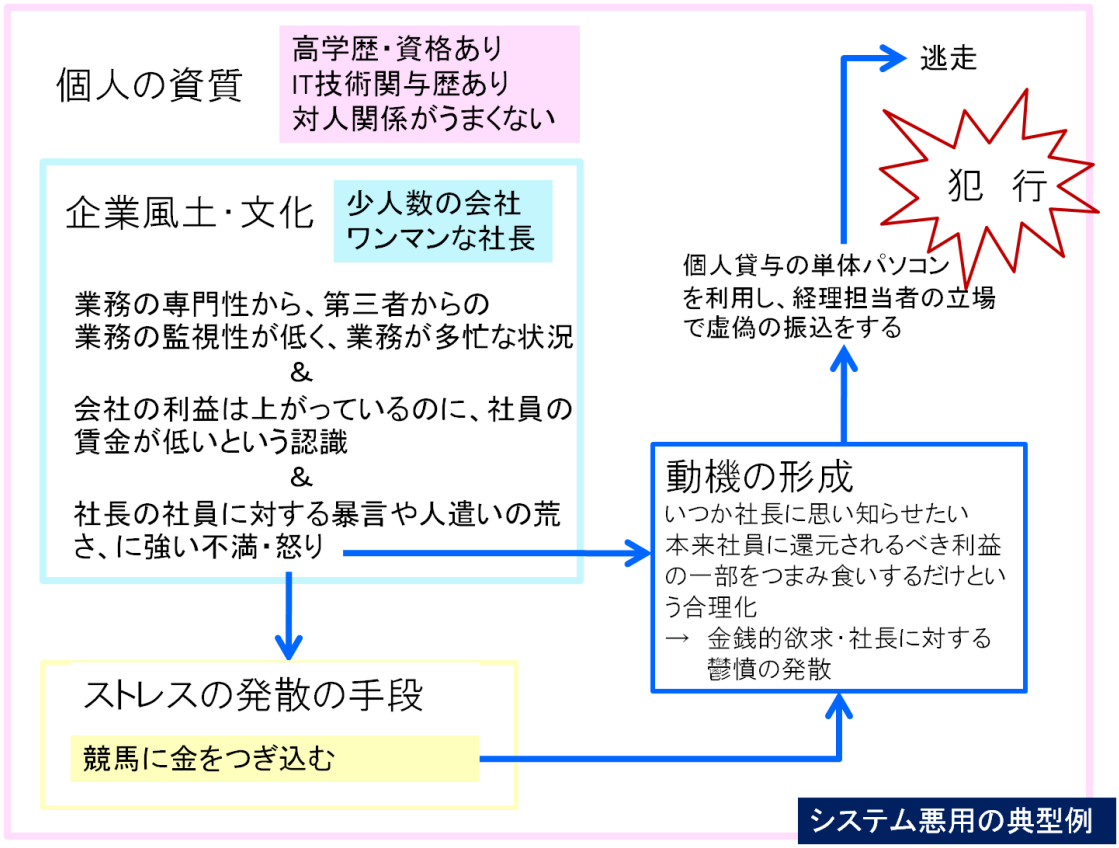
システム悪用の典型例におけるダイナミクスを図 10 に示した。

システム悪用の場合、経理担当など通常業務で現金や電子マネーなどを扱う立場にある者が、経済的に逼迫した状況において、監視性の低い状況を利用しての犯行を行っている。犯行に至るダイナミクスを検討するために、個人的な資質、環境要因となる企業の風土・文化、犯行までの動機形成の過程、犯行に至るまでの過程について示す。

システム悪用の典型例の場合、個人的な資質としては学歴が高く資格を有するなど高い技術力が見込まれるが、対人関係があまり上手ではないタイプが多い。そして重要な情報として、犯行者は何らかの借金を抱えるなど、経済的な不安を抱えている場合が多い。

犯行者が勤務する企業の風土や文化としては、少人数の組織であったり、ワンマンな経営者がいたりするなど、独特な文化を有している。少人数の組織であるために、細分化された業務を監督指導する立場の人がおらず、監視性が低い環境で経理業務などに従事している。業務は比較的多忙である場合が多い。また、ワンマンな経営者ゆえに、社員の意見や考え方に関する情報は上がっていかず、社員は多かれ少なかれ組織や上司に対する不満を抱えており、場合によっては、経営者の社員に対する態度などに強い不満や怒りを抱いている場合がある。

図 10　システム悪用のダイナミクス



犯行者は、こうした状況の中で自らの力で変える事のできないストレス源から受けるストレスを発散するために、趣味に取り組むが、その趣味として、高級クラブ通いや競馬、オンラインゲームなど、犯行者が継続して楽しむにはある程度の経費を必要とするものが選択される場合が多い。犯行者が趣味に多額のお金を消費すると、借金返済に窮する事態になるなど、経済的な逼迫感はさらに増大していくことになる。組織や経営者に対する不満を抱える中、組織での業務で行う監視性の低い状況での作業を利用して、金銭的な利得を得たい、借金を返済しながら楽に生活できるお金を得たいという動機が形成される。その場合、憎い経営者や組織に損害を与えても構わない、多忙な勤務に相当する評価や収入が得られていないのだから、それを補償する分と考えれば構わないだろうといった形で、思いついた犯行を合理化、正当化しようとする。犯行者は機会をみて試すが、その後帳簿の帳尻をつければ発覚しない、誰にも気づかれないという状況を経験し、お金を得る為の犯行が強化され、犯行が繰り返される。ある程度多額といえる金額を搾取した後には、発覚を恐れて、あるいは帳簿の帳尻をつける作業が面倒になって、行方をくらませたり、退職したりする。

典型例の場合には少人数の組織であったが、大規模な組織であったとしても、犯行者は派遣社員の一人であるなど、企業の風土や文化に必ずしも馴染んでいない。上司にとっては監視すべき対象が多数存在するために、一人一人への監視性は低い状況にあり、犯行者は必ずしも監視性が高いとは言えない状況で個人情報を扱う業務に取り組んでいる。大規模な組織の場合には、犯行者が経営者や上司に対する強い不満を抱えている場合は少なく、どちらかというと、組織への帰属意識が弱いために、勤務先の組織から金銭的な利得を得ても、それほど悪いことをしているわけではないという考えを持ち、犯行の合理化を行っている。

システム破壊のダイナミクス

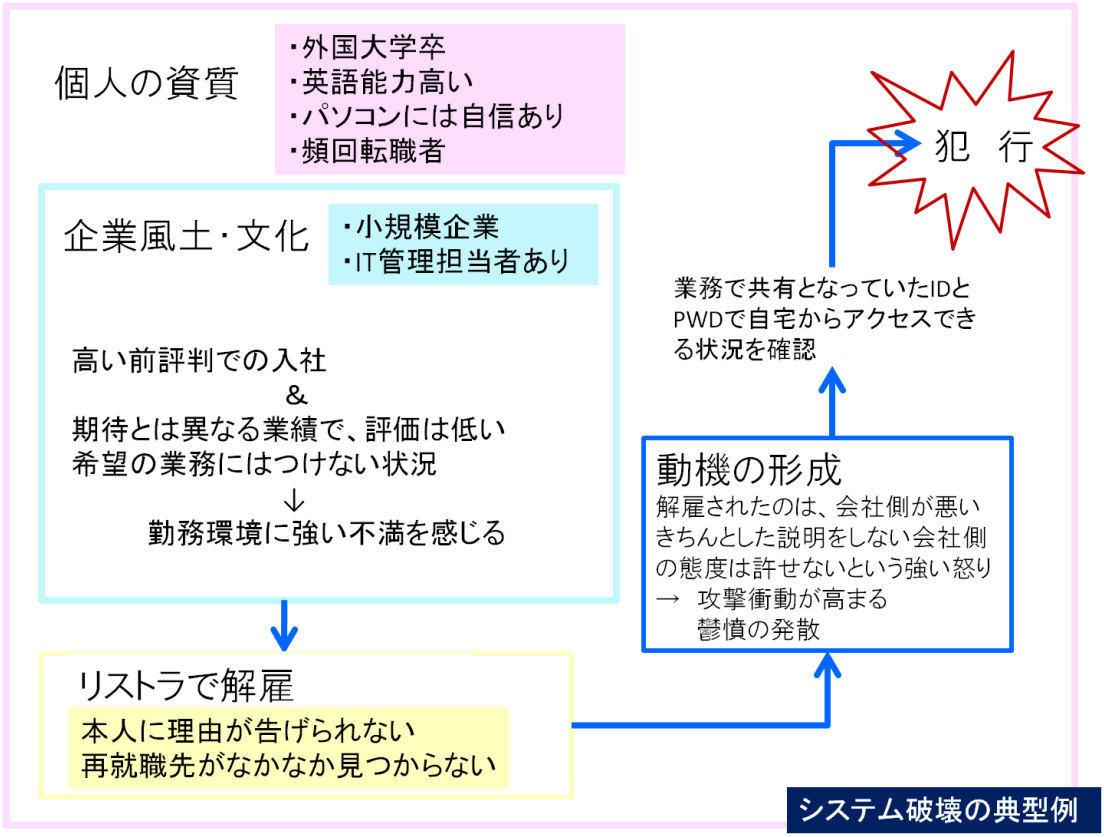
システム破壊の典型例におけるダイナミクスを図 11 に示した。

システム破壊の場合、業務上システム管理者としてシステムを作成したり管理したりする立場にあった者が、職場でトラブルを起こして退職した後、以前勤めていた勤務先の業務に必要な情報を破壊してダメージを与えることによって、心理的な満足を得ようとする場合が多い。

個人の資質として、IT 技術については裏打ちされたものはないが、ある程度の業務ができる自身を有しており、その他にも外国語の能力が高いなどの技能を有している。しかし、頻回転職者であり、職場適応の悪い者が多い。

犯行者が勤務する企業は、小規模の組織である場合が多いが、ある程度の分業がなされており、システム管理者がおかれている場合もある。IT 技術に対する自信と高い技能から、入社前の評判が高いが、実際に業務に当たらせると、能力が高いわけではなく、ミスが多かったりするなど、勤務状況に問題がある場合が多い。リストラで解雇されるが、本人に具体的な理由は告げられない場合もあり、解雇された者が納得していない場合もある。そうした場合、新たな勤務先が見つけられないと、自分の評価の基準となる集団(準拠集団)がいつまでも解雇された組織となってしまい、経済的な不安や生活上の不安、うまくいかない事のイライラや鬱憤の原因は自己の能力ではなく、以前の勤務先に帰属される。そもそも解雇した組織が悪いという思いに加え、きちんと説明しない組織側の態度は、まさに自分が不当に扱われたことを示すものだと感じ、以前に勤めていた組織に対する強い怒りや恨みを抱くようになる。攻撃的な衝動が高まるが、正面から交渉したり、非難したりすることはせず、自分が以前に関与していた業務で必要とする情報を破壊することによって、以前勤めていた組織を困らせたいという動機を形成する。犯行者自身が行った行為によって、相手が困った事態に陥ったり、確実なダメージを受けたりすることは、犯行者が持っている状況をコントロールする力を自覚させ、あまり状況がコントロールできない状況にある現実の自分を満足させる事ができる。

図 11　システム破壊のダイナミクス



多くの場合、退職直前のトラブルや退職時のトラブルが犯行者に動機を形成させる主要な要因となっているが、場合によっては、円満に退職したにもかかわらず、こうしたシステム破壊を行う者もいる。そうした者の場合には、自ら選択した離職にもかかわらず、新しい環境に適応できなかったり、新しい職場で評価が低いなどの事態に直面したりすることによって、準拠集団が以前勤めていた組織に戻ってしまい、そこに固執することから、攻撃の対象を以前勤めていた組織とした犯行が行われている。

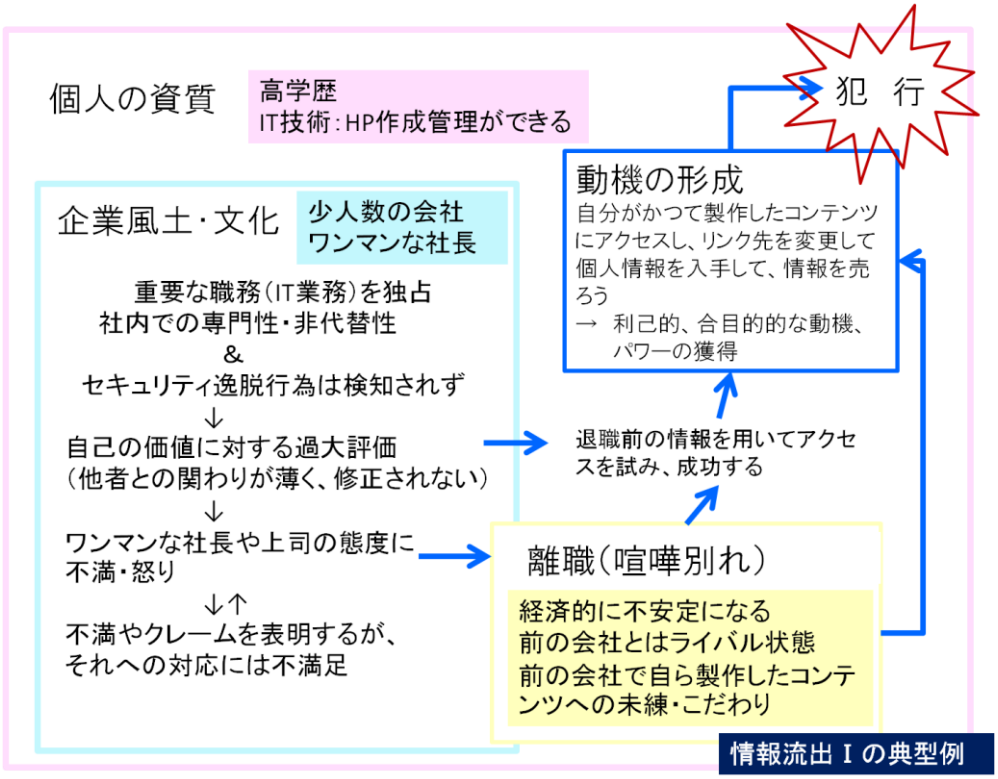
情報流出 I のダイナミクス

情報流出 I の例として、退職者による犯行のダイナミクスを図 12 に示す。

情報流出 I の場合、経済的に逼迫した状況にある犯行者が、勤務先あるいは以前勤めていた企業で、自分が管理あるいは作成したシステムやコンテンツにアクセスして、そのシステムを経由して換金したり何かに利用できる個人情報を入手したりするものである。

個人的な資質としては、比較的高い学歴を有し、IT 技術についても、システム管理や HP 管理などある程度の技術力を有している。企業の文化や風土としては、少人数な組織で、ワンマンな経営者という独特の文化を有している。こうした環境の中、組織の経営にとって重要な業務に位置づけられる IT 業務を犯行者が独占して取り組んでいる。他に IT 業務に詳しい者がいないために、犯行者の専門性、非代替性は高いものとなっている。犯行者は、他に詳しい者がいないことを利用して、悪意の有無にかかわらず、許可なしで自宅などの職場外部からのアクセス環境を整え、アクセスを行っている。しかし、こうしたセキュリティ違反行為は他者に検知されず、そのまま放置されることになる。犯行者が取り組む業務の重要性や専門的な業務を代替して行う者の不在から、犯行者は次第に自己の価値を高く評価するようになる。勤務する中で、経営者や上司の態度に対する不満を感じた場合に、それをダイレクトに表明したり、ぶつけたりするが、それは高い価値を持つ自分の意見は受け入れられるべきだという感覚に裏打ちされていると考えられる。多くの場合、経営者は上司からの犯行者の評価は、犯行者自身が思っているほど高くはない。こうしたギャップに怒りを感じて、犯行者は離職する。場合によっては、業務能力の低さから解雇される場合もある。

図 12　情報流出Ｉのダイナミクス



離職したものの、犯行者の生活は不安定な状況に陥る。再就職が困難な場合もあり、そうしたストレス状況にある原因は、個人の能力ではなく、以前に勤めていた企業に帰属される。また、再就職した場合でも、同様の業務に取り組む企業であるために、以前に勤めていた企業が自分にとって近い存在に感じている場合もある。特に、自らが作成したシステムやコンテンツについては強い愛着を感じており、犯行者がそれにアクセスすることは、システムやコンテンツに全く関係のない部外者からのアクセスと同様のものだという認識は薄い。以前の組織を退職する前に業務上で知り得た情報を使って、アクセスを試みるが、それは成功する。うまくアクセスできたことによって、自らが作成したシステムを利用して、換金できる情報を盗み出し、金銭的な利得を得て、現在の経済状況を改善したいという利己的な動機が形成される。これが以前勤めていた企業に損害を与えることになったとしても、自分を評価してくれなかった組織が損害を受けても構わないと考える。自分が作成したシステムを利用して自分が利することで、自己効能感を高めることにもつながっている。

情報流出Ⅰの多くは退職者による犯行であるが、中には現職者による犯行もある。その場合には、経済的に逼迫した状況は同様であるが、換金するなど利用価値のある情報を管理する立場にある者が行っており、職場内で意見の対立等のトラブルは見られない場合が多い。

情報流出Ⅱのダイナミクス

情報流出Ⅱの例として、退職者による犯行のダイナミクスを図 13 に示す。

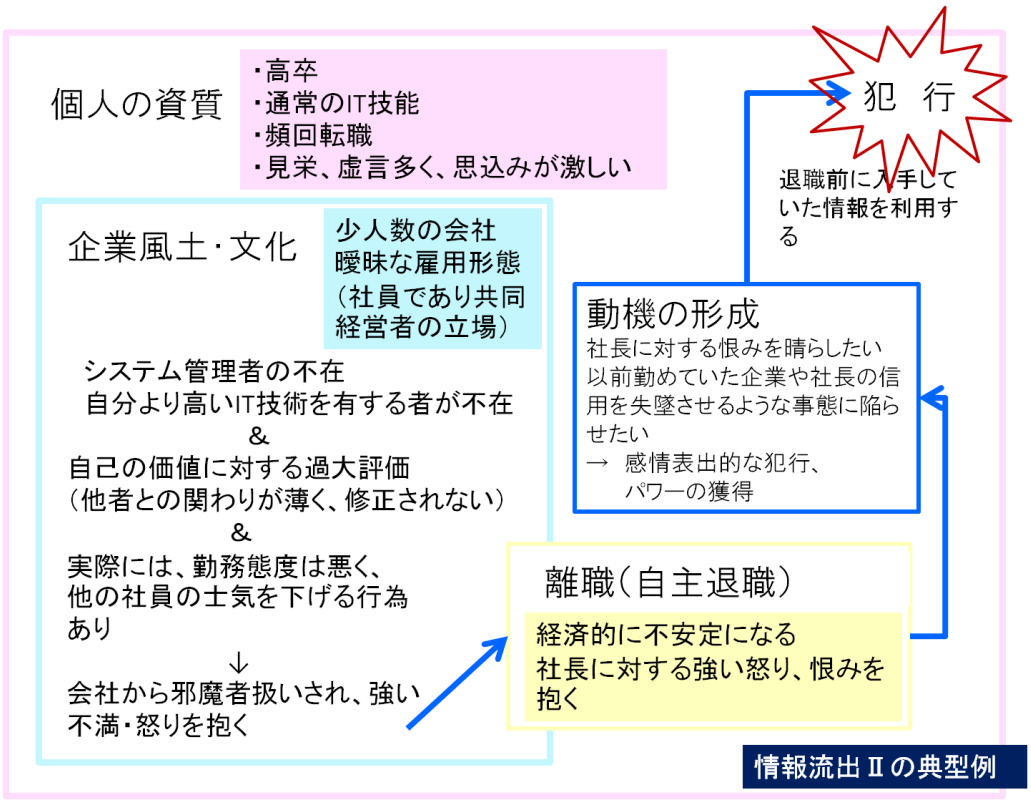
情報流出Ⅱの場合、以前勤めていた企業で強い不満を抱いていた相手である経営者や上司に対して嫌がらせをする為に、自分が管理あるいは作成したシステムやコンテンツにアクセスして、情報を入手し、掲示板などに避難中傷する文章として掲載したり、他者にその情報を流すことによって、鬱憤を晴らしたり、心理的な満足を得ようとするものである。

個人の資質としては、高卒程度あるいは専門学校程度の学歴を有し、特に高い技術ではないがIT業務がこなせる程度のIT技術を有している。ただし、頻回転職者であるなど、社会への適応状況はよくない場合が多い。経済的には逼迫した状況にはないが、勤務していた組織を解雇されたり、組織を見限って円満に退職したりしていることで、就職活動や転職のためのストレスを感じている。見栄っ張りであったり、虚言癖があったり、思いこみが激しいなど、勤務先などの対人関係で信頼できる関係を築けない場合もある。

企業の文化や風土としては、少人数な組織で、ワンマンな経営者という独特の文化を有している。ワンマンな経営者との契約で入社するが、雇用状態が曖昧なまま勤務しており、経営者側と犯行者側とで、雇用条件や報酬について異なった見解を持っている場合もある。同様にIT業務を行う者もいるが、システム管理者のいない状態で、自分より上のIT技術を有する者もいない。相対的に、自分の価値を高く見積もるが、他者との関わりが表面的で、思いこみも激しいため、自己価値の過大評価は修正されない。また、実際には勤務態度が悪かったり、業績が悪かったりするが、これについて内省することはない。経営者や上司、社員からの評価が、自分が期待するよりも低く、彼らの態度が気に入らず、強い不満を抱くようになる。表面的には、何らクレームをつけることなく、

円満に退社するが、経営者や上司に対する強い怒りや恨みはおさまることなく抱き続けている。退職により経済的に不安定な状況になるため、就職活動をしたり、再就職先を見つけて勤務したりしているが、以前の勤務先で抱いた怒りや不満の内容にこだわりを持っており、何らかの形で経営者や上司に対する恨みを晴らしたいという動機が形成される。信用を失墜させる行為や嫌がらせを行うことによって、経営者や上司を困った状態に陥れたいという考えを持ち、それによって心理的な満足感を得ようとする。

図 13　情報流出Ⅱのダイナミクス



退職前に入手していた管理者情報を用いて、システムにアクセスし、そこで得た情報を掲示板などに避難中傷する文章として掲載したり、第三者にその情報を流すことによって、信用を失墜する事態に陥らせることによって、自分の鬱憤を晴らしたり、心理的な満足を得る。

5章　人的脅威への対策

5-1　概要

ここでは、調査実施に当たり検討した 3 つのモデルをベースに、事例分析、モデルでの検討、類型化、力同過程分析で得た知見をとり入れて対策を検討する。3 つのモデルとは、以下のものである。

（1）犯行者の特性と犯行の動機、犯行の誘発要因と抑制要因(p.13 図 1 参照)
（2）人間関係を含む環境要因(p.14 図 2 参照)
（3）時期と対象に応じた対応の検討(p.15 図 3 参照)

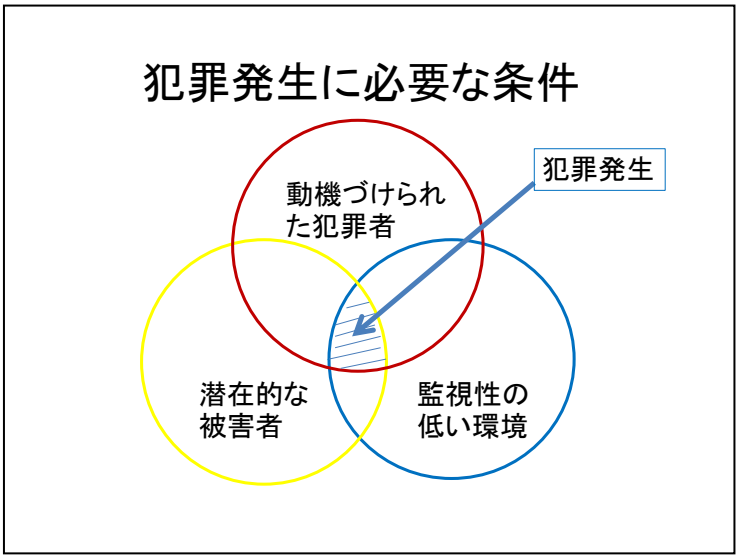
ルーチンアクティビティ理論によれば、犯罪は、「潜在的犯罪者」、「標的ないしは潜在的被害者(ターゲット)」、「環境(場所)」の 3 つの要素が時間的・空間的に収束したところで発生すると言われている(図 14)。犯罪発生にはこの 3 つの要素が不可欠である。したがって、犯罪の発生を未然に防ぐためには、この 3 つの要素が重ならないようにすること、つまり、犯罪者となるリスクを持つ人、潜在的な被害者(物)、環境のそれぞれの要素に関する対策を実施することが必要となる。

（1）　犯罪者となるリスクを持つ人については、犯罪者が犯罪に至る原因を取り除き、犯罪者となるリスクを持つ人を減少させるための対策や、犯罪者になることを抑制する力を強化するための対策が考えられる。たとえば、劣悪な社会環境が犯罪の原因になっているのであれば、そのような社会環境を改善することや、社会的な規範を遵守する価値観を持つよう教育する、などが挙げられる。
（2）　潜在的な被害者(物)については､潜在的な被害者(物)が持つ犯罪被害への抵抗性を高めるための対策が考えられる。たとえば、侵入窃盗の被害に遭いにくい家屋作りのために、「戸締りを完全にする」、「窓のガラスを割れにくいものにし、面格子や雨戸をつける」といった対策をとることが挙げられる。

（3）　環境については、犯罪を誘発する「環境」を作らない、あるいは減らすための対策が考えられる。具体的には、潜在的な犯罪者に、「犯行を行いにくい」と思わせる環境を設計することが環境についての対策となる。

（4）　情報セキュリティ事案における内部犯行者による犯行を未然に防ぐための対策も、他の犯罪と同様に、犯罪者となるリスクを持つ人、潜在的な被害者(物)、環境のそれぞれについて対策を講ずる必要がある。

図 14　犯罪発生に必要な条件



以降の章においては、情報セキュリティ事案における内部犯行者による事件の事例調査の結果から、犯罪者となるリスクを持つ人、潜在的な被害者(物)、環境のそれぞれについて、実施可能な対策を考察する。

その際、まず、犯罪者となるリスクを持つ人について、時期と対象に応じた対策を記述しつつ、その中で犯行者の特性と犯行の動機、犯行の誘発要因と抑制要因、人間関係を含む環境要因にふれ、その後更に潜在的な被害者(物)、環境についても、検討していきたい。

5-2　時期と対象に応じた対策

5-2-1　入社前

入社前には、能力のみならず採用しようとする人物が担当することとなる職務を遂行するために必要な適格性についても十分チェックしておく必要がある。例えば、経済的問題を抱えている者を経理担当とすることは、犯行への誘惑が多い環境に当該者を置くことになり、当人にとっても採用しようとする企業にとっても問題が多い。

また、情報システムがそれぞれの組織において業務の基盤となっていることを考えると、情報システムを担当することが予定される者については、その重責を担い、組織の基幹業務を遂行する、誠実さを含む人格的適性を有しているかをチェックすることが望ましい。その際には、

（1）短期間で転職を繰り返している
（2）履歴書に嘘がある場合
（3）経済的な問題を抱えているケース
（4）一見輝かしい経歴にまどわされない

といった点がチェックポイントになる。履歴書の精査は重要なポイントであり、内容自体もさることながら、その内容の検証により相手が信頼に足るか、嘘をつくような者であるかどうかがわかる。従って、個々の要件について、当該職種に必要な適性を有しているかを判断することに加え、全体としてその人物が求める職務に適性を有しているかを判断することが必要である。[11]

さらに、既に多くの組織・企業において実践されていることであるが、情報及び情報システムの取り扱い・利用について、契約に盛り込み、違反した場合の措置についても書き込んでおくことは、犯行抑止に寄与するものと考えられる。

---

[11] CERT/CC においては、国家的な情報流出事案について国防省と共同で研究を行っているが、米国において国家的秘密情報を取り扱うためには、適格性について審査を受け、それに合格する必要がある。その審査に当たっては、経済的状況や薬物の使用状況などのチェックポイントがあるが、最終的な判断はそれらのチェックポイント個々についての該当性よりも全体として秘密情報を取り扱うに足る人格的適格性を有しているかをチェックすることとなる。

また、内部犯行事案が組織に対する恨みの感情から引き起こされていることを考えると、こうした恨みの原因になりやすい労働条件・処遇条件の認識の違いがないように、これらの事項について採用時に明確化しておくことにより、後々のトラブルを避け、関係者の恨みを買うような事態に陥ることを防ぐことができる。

5-2-2　在職中

内部犯行の態様としては、記述のように、在職中に行われるものと退職後に行われるものがあり、在職中に行われる犯行は経済的な利益や対立する者に対する攻撃などを目的とする道具的なものが中心である。対策としてはこうした犯行に至る過程のいずれかの段階で、当該犯行に関係する状況を把握し、防止・抑止措置を執ることが重要である。そのためには、関係する状況についての情報を入手できるような態勢を有している必要がある。また、そもそもそうした犯行を行いにくい環境を構築しておくことが有効である。

また、退職後に犯行に及ぶケースについても、犯行者の個人的な特性が大きく寄与しているような事案であっても何らかの在職中の状況が原因となっている。犯行者に一次的な責任があることは当然としても、様々な勤務に関係する状況が退職後の犯行に結びついている。そして、これも記述のように、退職後に行われる犯行としては表出的なものが多くなっている。つまり、恨みその他様々な感情が、在職中から積み重なり、退職後にそれが爆発することになる。この場合には、そのような感情を生み出す状況と、退職後に犯行が可能になるような「道具」「環境」を潜在的犯行者が入手するような環境が生まれないように配慮することが求められる。

このような観点から在職中の対策としては、以下のようなものが考えられる。

(1)　職場全体のコミュニケーションをよくしておく

これは、それ自体として恨みの感情を醸成しないなどにより内部犯行の抑制効果がある。また、経済的状況による犯行についても、良好なコミュニケーションにより他の職員か

らの情報の入手がなされ、早期に組織としてこれに対応することが可能になることが考えられる。[12]

また、表出的な犯行を防ぐという観点からは、早い段階で、問題のない或いは問題の少ない(場合によっては建設的な)「表出」を促す、という面でもコミュニケーションは有効である。さらに、退職後の犯行につながる、個人的特性以外の様々な要因について把握するという観点からも重要なツールとなり得る。

(2) 抑止システムの整備

犯行を抑止する制度・仕組み・システムの整備も重要である。

情報漏洩や情報システムへのアクセスについて、組織としての規則を設け、それを実効性確保のためのサンクション等と合わせて文書化し、契約に盛り込みなどすることにより、更に規範としての認識が共有されるようにすることのほか、情報システム利用・管理体制、情報システム保護体制、情報システム構築体制などの各フェイズにおいて犯行を抑止するような仕組みとしておく。また、情報システムの管理体制について、情報システムのモニタリングや利用権限がなくなったときの措置などについては、これについて契約に盛り込むとともに、その存在を広く知らしめ、事前の抑制を検討することが適当である。

(3) 兆候の把握

内部犯行につながる要因は様々であり、米国での研究成果を見ても、必ずしも潜在的犯行者にとって不利益なイベントばかりではなく昇任や賞揚措置などでも不満を感じ、それらが犯行に結びつくことがある。

従って、兆候の把握に当たっては、解雇・転勤・降格(システムへのアクセス権限の喪失含む)・昇任・賞揚、様々な要因や環境変化について、精神的な動揺や犯行動機を形成する心的要因になっていないかを観る必要がある。

---

[12] ある意味では、密告の奨励のように見える表現であるが、実際にはそうした「監視的雰囲気」ではこのような情報の流通は期待できない。コミュニケーションや単なる雰囲気だけに留まらず、実際に当該組織・企業や、職場の(人間)関係が、潜在的犯行者の環境を理解し、それに対応する体制と熱意を持っている環境であることが必要である。

また、金銭的な問題についても、例えば消費者金融業者との連絡ではないかと思われるような動きなど様々な兆候があり得る。

外面的な兆候としては、

- 服装や身だしなみの乱れ
- 態度の変化(職場で、他のことを考えているような様子など)
- 上司や同僚、取引先とコミュニケーションがとれなくなる

などがある。

これらの情報が対応担当者及び組織の上位者に把握され、これに対応する体制が整っていることが望ましい。

5-2-3　退職期

(1)　コミュニケーションの重要性

ここでは、「退職の前後の時期」を指して「退職期」という。

在職中においても、コミュニケーションの重要性について指摘したが、ある意味では、退職期にはよりコミュニケーションが重要になってくる。

業務面において引き継ぎなどをしっかりと行う、ということの中にはそれに伴うコミュニケーションが当然含まれる。退職に際しても、必ずしも良好な関係のまま退職を迎えているケースばかりではなく、むしろ今回取り上げるようなケースの場合には、解雇、喧嘩別れによる退職、職場の環境に耐えられずに退職といった状況が多い。これらの状況では、組織と潜在的犯行者とが相互の意思を通わせることは容易ではない。しかし、それであっても、業務の引き継ぎやアカウントの無効化、退職後の情報不正利用の禁止の文書化などを確実に行う必要がある。また、労働法制・福利厚生面で対象者が不必要に不利益を被ることのないように手続きを行うとともに、その内容を対象者に確実に伝え趣旨も説明しておくことが望ましい。

(2)「退職期」の意味

「退職期」と言った場合、退職者側から見た「退職期」と組織・企業側から見た「退職期」が存在しており、これは必ずしも一致するものではなく、むしろ時期的には異なることが一般的である。

潜在的な犯行者である退職者の場合、退職期にはいくつかの意味がある。

ア　道具的犯行に及ぶ可能性のある場合

この場合には、

・退職後も組織のシステムにアクセスするための情報の入手

・退職後に活用し利益を得るための情報入手のための仕組み作り

などが行われることになる。従って、こうしたことがなされないように、潜在的犯行者がその職務を通して有していた様々なシステムへのアクセス手段、情報について、無効化や回収を確実に行う必要がある。

これは、大きな組織においては、しっかりとした規則と体制も構築されるようになってきているが、一方で書類上は無効化などが行われたことになっていても、実際には行われていないなどの状況も起こりうる。大きな組織の場合、多人数分の処理を集中的に行う場合には退職者一人一人にきめ細かい対応ができているかについて問題意識を持つ必要があるし、分散的に行う場合には、それぞれの部署で確実に手続がなされているかを確認することが求められる。特に、情報システムに関する内部犯行は、情報システムをよく知っている者により行われる場合が多いわけであり、そのような者が、何か抜け道を確保していないか、或いは確保できるような抜け穴が管理体制にないか、常にチェックを怠らないことが重要である。システム的なモニタリングも有効である。

イ　表出的な犯行に及ぶ可能性のある場合

退職前後は、まさに潜在的犯行者にとって感情の昂ぶる時期である。喧嘩別れのような形で退職する場合はもちろんであるが、一見穏やかに見えても本人や周囲もよい感情を持っていないこともある。このような状況で、退職前に休暇といった時間的な余裕が潜在的犯行者にあると、退職後と同様に感情が高ぶり、攻撃に及ぶこともある。また、自ら構築し又構築したと自負しているようなシステムの場合、退職を決定してから実際の退職までの間に、破壊したり、アクセスや管理に必要なデータを持ち出したり、或いは

返却しなかったり、データやシステムへのアクセス方法について引き継がなかったり、といった行動に出ることがある。一見感情を抑えて退職に向かっているように見える者もいるため、この時期に対応をとることは難しい面もあるが、まだ正式に退職になっていなくても、早期に(退職前の休暇に入る前に)情報システムからのアクセスはできないようにし、引き継ぎはその前に済ませるよう、管理的立場にある者が監督しておくことが適当であろう。正式な退職前にアカウントを無効化することには組織全体で、安全と円滑な業務の移行のために必要なものであるとの認識を共有しておくことが望ましい。

これは、表出的な犯行の可能性がある場合だけの問題ではないが、まだ組織に潜在的犯行者が所属している段階で、アカウントの無効化や利用していた端末を回収することで組織側としては当該者の業務の内容を把握して円滑な業務継続に役立てることと併せて、不適切な行動がないかもチェックすることができる。なお、こうしたことを行うことについては、犯行が疑われるような状況に至る前に、広く一般の者も含めてあらかじめ文書で同意を得ておくとスムーズに行うことができるであろう。

(3)　退職期の対応

退職が決まった場合には、潜在的犯行者のアカウント無効化など、情報システムに関する業務の確実な引き継ぎと業務チェックを行うことになる。

アカウントの無効化等の確実な措置

関連デバイスの回収、ID やパスワードの変更・削除を含むアカウントの無効化、物理的なアクセス不許可など、システム・環境的に、退職(予定)者がかつての業務システム及び関連する業務システムにアクセスできないような措置を確実に取る。

これは当然のことであり、また大きな組織であれば当然行われている、と思われがちであるが、必ずしもそうではない。文書の上では削除されていることになっているのに当該アカウントが有効であったり、組織が大きく退職者が多い場合に対応が遅れるような場合、退職した場合にはアカウント無効化がなされることになっているが退職が決まった段階などに柔軟な対応がとれない又はそのようなアドホックな場合には対応が遅れることなどは、情報セキュリティ関係の制度が整っている組織・企業でも起こりうることである。むしろ、大きく官僚的な組織の場合、起こりうるとも言える。

また、業務引継についての問題であるが、犯行者自身がシステム管理を担当していた場合には、アカウント初期化を含むアカウント管理のための資料を有している場合もあり得る。特に、比較的小規模の組織・企業で、外部システムを利用しているような場合、実際のアカウント無効化や初期化の措置は外部システム運用者に依頼することになる。従って、外部システム運用者との人間関係を含むアカウント管理「依頼」のためのデータ・環境さえ有していれば、引き続き企業のアカウントを実質的に有し続けることが可能な場合もあり得る。更に、こうしたデータ・環境を利用して、当該組織のアカウント初期化のような攻撃を行うことも可能になる。従って、外部システムを利用している場合には、退職(予定)者及び犯行を行う可能性の高い者から、関連するデータを回収し無効化するほか、外務システム運用者にも担当者の変更等、必要な連絡を行っておくなど、環境面の配慮も必要である。

このような、システム担当者と外部システム運用者との関係は、本来であればプラスのものとして重要である。すなわち、一般的なインシデント発生時には、システム管理者と外部システム運者とは迅速に協力体制を構築して事案に対処することになる。従って、普段から良好な関係を持つとともに、事案発生時にはそれを活用して迅速な対応を行うことが求められる。すなわち、ある意味では、正式な手続きがなくても、迅速に事案対処のための措置を協力して取る、ということになる。例えば、組織が外部から攻撃を受けた場合、システム担当者は外部システム運用者に対して「とりあえず職員のアカウントを初期化して欲しい。」という要請を出すこともあり得る。そして、このような要請に応える、という体制をとっている外部システム運用者もある。内部犯行の問題は、内部者が攻撃側に回った場合、こうしたリソースも攻撃に使われると言うことである。つまり、攻撃側に回った内部者は、このような関係、いわば迅速な業務復旧のためのサービスを悪用して、当該組織の重要アカウントを初期化し、業務不全に陥らせることもできる、と言うことである。

このような事態を防ぐためにも、複数のシステム管理者、又は少なくともシステム管理を更に監督する者の存在が重要になってくる。組織の大小にかかわらず、これは不可欠と言える。

契約関係の確認

退職後において、秘密漏洩の禁止、アカウント使用・アクセスの禁止などについて、文書を取り交わしておくことは一般的に行われているが、一定の抑止効果を期待できる。

5-2-4　退職後

今回の事例調査でみても、30 件中 18 件が退職後に発生しており、退職後にも「内部犯行ではないか」との視点から対策を考えていくことが必要となっている。また、犯行は必ずしも退職後すぐ行われるわけではなく、退職後新たな勤務先も決まりそこで働き出した後のような、いわば一段落ついた段階で攻撃に及ぶ例も多い。すなわち、退職後すぐは潜在的犯行者も新たな生活基盤を整えることに忙しく、さまざまな感情についてもその発現が抑えられている状況にあるケースも多いが、新たな勤務先が決まり働き出したり、その他新たな生活に入ったところで、いわば「暇」ができ、こうした状況(環境)によってこれまで押さえられてきた思いが吹き出し、犯行に及ぶことがある。

退職後における対策の留意点としては、組織・企業として、特に潜在的犯行者に対するものということではなく、退職者全般についてもケアをする、ないしはフォローする態勢を持つ、ということが大切であると思われる。これは、人事を担当する部門が担当するといったような一部の問題ではなく、組織・企業全体として考えるべき問題であり、さらにそのためには、潜在的犯行者にとって当該組織・企業を退職したことの意味が関係者にある程度共有されていることが望ましい。[13]

犯行者は、必ずしも 1 回で組織・企業が大きな被害を被るような攻撃を行うわけではなく、不正アクセスや情報盗み見といった「小さな」行動から、徐々にエスカレートして情報やシステムの破壊に及ぶことがあるので、早期に退職した潜在的犯行者の行動が把握され対策をとることができれば、実質的な被害を防ぐことができる。例えば、潜在的犯行者がとる行動として、現職の者への(不自然な)連絡[14]が見られるが、これらをきっ

---

[13] これは、どのような事情で潜在的犯行者が退職したかをある程度周囲の人々が知っているということを意味する。現実にはプライバシーや個人情報の保護といった観点から難しい問題もあると思われるが、立ち入った状況についての情報でなくても、事案に関連する「雰囲気」だけでも共有され、事案に組織のマネージメント層も関心を持っている、ということが共有されているだけでも、対応が異なってくるものと考える。

[14] 具体的にアクセスに必要な情報を聞いてくるということではないが、以前の職場に執着していることが伺えたり、組織の特定の者に恨みを持っているような発言があった

かけ(トリガー)として、不審なシステムへのアクセスのチェック、潜在的犯行者の心情などへの理解と対応がなされることにより被害を防止できる可能性がある。ただし、情報システムへの(不審な)アクセスも含めて、非常に微細なものであることが多く、よほど意識していないと見落としがちのものである。そもそも、記述のように、犯行者の認識として、実際に行うことは自らの目の前からの比較的簡単なコンピュータの操作なので、軽い気持ち、勢いでやってしまうこともあり、前兆事案自体も軽微で把握しにくものであることも少なくない。

情報システムへの不審なアクセスについては、システム的なチェックも一方法であろう。

記述のように、犯行者は、小さい行動から大きな行動に進んでいくことも多く、小さい行動の段階で「これなら気付かれない」との認識を持ち、行動がエスカレートすることがあるため、こうした前兆の把握は重要である。また、企業に恨みをもって退職していった、とか情報持ち出しなどの不正な行為が原因で退職をしたというような職員については、こうした現職への接触も含め、情報を入手できるような態勢があると好ましい。

5-3　情報システム面からのポイント

5-3-1　システム運用

今回、調査した事例の中でもシステム開発・運用に携わった者による犯行もかなり見られた。このような者による犯行を防ぐためには、これまで述べたような対策と併せて、次のような対策を講じることが有効と考えられる。

（1）　システムの開発・運用は複数の者で担当する。
（2）　システムへのアクセス権限を適切に管理する。
（3）　実際の業務に当たっても一人に任せきりにしない。
（4）　チェックシステムを導入しておく。

り、組織内の情報について強い関心を示していたり、情報システムに異常があるかなど自らの犯行を組織が気づいているか探りを入れたりといったものが考えられる。

これは、いずれも当然のことと見られるかもしれないが、実際にはかなり大きな組織においても実現が難しい状況になっている。事故による情報漏洩事案からも伺えるように、システム開発は内部だけで行われるのではなく、外注先を含む多くの企業・開発者が関係してなされる。その過程で、管理のための情報が関与者に共有され、最終的にシステムを改変することのできる権限がいずれかの部署・人に残ってしまうことがあり得る。事例を見ても、小規模の企業で少人数(多くは実質的には一人)による開発運営がなされていることは理解されやすいと思うが、大規模な組織であってもシステムは細分化され、それぞれのサブシステムについての実質的な担当者はごく少ない数になる。さらに、全体のシステムを統合的に動かすためには、各サブシステムについて責任者的な地位にある者は、他のシステムについても一定程度アクセスできる資格を持つことになることがある。このような場合、これらのサブシステムの責任ある者が内部犯行に及んだ場合、組織全体のシステムに大きな影響を及ぼすことになる。また、開発が終了し、システムができあがった後にはユーザに対してはアクセス権限をしっかり管理することが通常である。ただ、システム構築後も、そのメンテナンスに当たるようなグループに所属する者については、システム保全業務に当たる際に別の特権的アカウントを利用し、さらにこの特権アカウントをメンテナンスグループで共有するようなケースも考えられる。システムの構築やメンテナンスにはさまざまなフェイズが考えられるが、それぞれのフェイズにおいて、アクセス権限をそれぞれの個人について適切に管理し、かつ実際の運用も複数で行う、ということは状況をしっかり把握し、意識的に行って初めて実現されるものであることを認識する必要がある。

複数で業務を行うという場合でも、職位の差、正社員・派遣社員の差、経験・知見の差から、実質的に潜在的犯行者と共に業務を行っているとは言えないような状況になっている場合もある。このような場合は、潜在的犯行者がどのようなことを行っているかについて十分理解できなかったり潜在的犯行者のセキュリティ関係規則の例外的措置について必要の有無の判断ができなかったりするような状況が生じ得る。また、内部犯行事案が、様々な感情により引き起こされ得ることを考えると、業務について実質的に相談したり協力したりできる者が身近に存在しているということは、犯行につながる「恨み」「感情のもつれ」を防ぐという意味でも、また組織・企業として業務効率を上げるという意味でも効果があるものと考えられる。

チェックシステムとは、ログを記録しこれを他の利用手続きによるデータと照合することや、異常なデータのダウンロードやアクセスについて抑止や警告を出すような、いわばシステム的なものに加えて、監督者(上司を含む)が、何らかの形でチェックをするような仕組についても含む。システムを悪用して組織・企業の資金を自らの口座に送金していたような事例について見ると、管理者・経営者が経理関係の事務を犯行者に任せきりにしているような例があり、システム的に管理者アカウントの設定が可能になっていても、その設定を行っていないようなケースも見られる。システムとして抑止が可能になっている場合でも、これを運用する人間側で活用することがなければ実効性を担保することは難しい。現実には、いずれの組織も少ない人員で業務を進めていることから、多くの時間を裂くことは難しいとしても、機器・システムと人間の役割分担を工夫することにより、潜在的犯行者に抑止システムが有効に機能していることを認識してもらい、また業務面でも犯行抑止面でも実際に効果を上げていくことが求められる。

5-3-2　事案発生時における情報システム面からの対応のポイント

必要な資料・データの確保

組織としては、多くの場合、まず業務の継続性確保が重要になる。

社内の業務プロセスを通じた調査に加え、デジタルフォレンジック(電子鑑識)の技術も活用する。犯行者は、バックアップを破壊することもあり、そのような場合には、組織を挙げた事業継続のための措置が必要になる。

併せて、原因追及のための資料・データの確保も重要である。特に、内部犯行の場合、システムを復旧しても、さらにそれを犯行者により破壊される場合がある。内部犯行の可能性もあるとの認識を持ち、それに対応した措置をとらないと結果的に事業継続においても大きな問題が生じることになる。

関係企業との協力関係の構築

現代の情報システムは、一つの組織・企業だけで構築されていることはまれである。特に、規模の大きくない組織の場合、イントラネットでの業務システム、外部との情報交換を行うための電子メールシステムや決済のためのシステム、潜在的な層も含んだ顧客への情報発信や顧客との関係構築・契約関係の締結と実現といった、さまざまな段階において、外部企業からのサービス提供を受けていることがある。

内部犯行者がこうしたシステムを利用して情報を取り出したり、提供されているシステムを利用して構築した環境を破壊したり、提供されているシステムを利用して構築されているデータベースやネットワークを破壊した場合には、こうしたシステムを提供している企業と協力して事案に対応する必要がある。特に、迅速なシステム復旧のためには、夜間・休日を問わない支援態勢・対応態勢があるかが重要になる。また、犯行者の行動を把握するためには、これを分析・追及するためのデータが保管されており、かつこのシステムの提供を受けている企業が分析・追及のためのデータにアクセス可能であることが必要である。さらに、システム提供を受けている企業は、当該システムについての専門家を有していないことが通常であると考えられ、対応に当たって支援を受けることが可能であることが求められる。もちろん、このような態勢を確保することにはコストもかかるわけで、提供を受けるシステムの、当該組織・企業における重要度に応じて要求水準は変わってくるであろうが、外部委託先の企業含め、関係企業とは、事案発生時に、迅速に、かつ人的な要因も視野に入れた現状把握と対応が可能な体制を構築しておき、例えば、夜間・休日であっても、システムの使用記録などのチェックが可能であるかなどを確認しておくことが適当である。

5-4　まとめ

5-4-1　人的脅威対策における考え方

人的な脅威について分析をしてみると、実は情報セキュリティというものは人により支えられているものであることに改めて気づかされる。

今回の調査研究では、問題事例を取り上げたわけであるが、実際には多くの人々の努力により情報システムが守られている。そして、当然ながら、こうした情報システムはそれぞれの組織の目的に応じた社会的な価値を生み出すために構築され、利用されている。

これまで、内部犯行事案の対策として挙げてきた

・コミュニケーションや組織の融合

・職員や関係者の待遇の明確化

・職員の抱える問題の把握とその解決への助力

・合併した企業における融和の促進

・分散拠点間の良好な連絡協調

・職場におけるさまざまなハラスメントの防止

・不満を持って辞めていった人々を含む退職者との関係のフォロー

などは、組織としてプラスの価値を生み出すための対策とも重なるものである。すなわち、人的脅威を防止するということは、多くの人々が既に行っている「セキュリティ対策」「プラス価値の産出」を促進することによって実現される部分が大きい、ということである。そして、それは、一人一人の職員の心情や環境の把握を通じてなされる、ということである。

人的脅威への対応を人的側面から行うということは、人的な面からの着眼の対策により、システム側に過度の負担をかけず、情報セキュリティを確保する、という意味でもある。完璧なセキュリティ確保のために本来共有されるべき情報を死蔵したり、活動を消極的なものにしたりすることは本末転倒とも言える。対策において、人的側面からのもの、すなわち行動関連情報や背景事情の、その時々の状況・段階と相手方の特性に合わせた把握やチェックを含めて考えることで、対策の幅が大きく広がるものと考える。言い換えれば、技術的なシステム、ネットワークモニタリングだけでなく、職員への助力も考えた人的(心理的)な暖かいモニタリング、職場の雰囲気への留意も重要ということになろう。政府においては、特別に秘匿すべき情報の保護のために 2009 年 4 月より秘密取扱者適格性確認制度が導入されている[内閣官房カウンターインテリジェンス推進会議, 2007]が、重要な情報やそのためのシステムの取扱いに際しては、政府以外の組織・企業においても実質的にこうした人的な特性に配意したスクリーニングも検討の余地がある。

5-4-2　実効性のある対策

これまでも、「セキュリティを組織文化として根付かせる」ということが言われてきた。セキュリティの確保を、上記のようにプラスの効果をもたらすものと考えるとき、これを実効性のあるものとし、組織の目指す価値の実現と一体となった「文化」とすることは大切なことである。

そのためには、情報(システム)の重要性とそれを支える上での人間の貢献の重要性の認識の共有と、それに伴う責任や措置について周知されていることが大切である。

また、これは、内部犯行だけではなくあらゆるインシデントに共通することであるが、インシデント対応の方針と手順を作成し、必要な人々、部署に周知し、訓練を繰り返し、さらに対応を充実したものにしていく、ということが重要である。特に、内部犯行者による攻撃の場合、いつ何時発生するかわからないばかりでなく、対策を講じても、さらにそれを破る方法を知っている場合もあり、事業の継続性をしっかりと確保するとともに、インシデントの原因を把握するための体制構築と実際の措置についても、その重要性を認識し、訓練を含む備えをしておくことが望まれる。

本調査研究では、内部犯行を取り上げ情報セキュリティにおける人的な脅威について検討してきたが、対策においても、人的な側面を中心にとりまとめることとなった。これを通じ、情報セキュリティ対策としても、システム側、「情報」側からの検討だけでなく、人的な側面も含めた諸要素の全体的なガバナンスという視点が非常に重要であることが明らかになり、このような観点は、組織のリソースの効果的な配分にも資するものと考えている、今後の課題として、これらのバランスも考慮したより具体的な対策の提示を含めたガバナンスに関する施策の可視化が望まれる。

6章　付録・補遺

6-1　米国の調査票

下表は CERT/CC のモデルから作成した米国で用いられた調査項目の一覧である。あくまで公開の報告書から読み取れる調査項目についてまとめたものであり、記載していない項目も調査の対象となっている可能性がある点に留意いただきたい。

表 6　米国の調査票

1._人的要素			
	1.1._固有情報		
		1.1.1._性別	
		1.1.2._国籍	
		1.1.3._年齢	
		1.1.4._住所	
		1.1.5._学歴	
		1.1.6._職歴	
	1.2._能力		
		1.2.1._技術的能力	
		1.2.2._その他	
	1.3._企業内での地位		
		1.3.1._システムに対す	

		るアクセス権限の内容	
		1.3.2._その他	
	1.4._性格		
		1.4.1._mental health disorder	
			1.4.1.1._アルコール中毒
			1.4.1.2._薬物中毒
			1.4.1.3._パニック障害
			1.4.1.4._配偶者への暴力癖
			1.4.1.5._その他
		1.4.2._social skills and decision making bias	
			1.4.2.1._ルールに従わない
			1.4.2.2._職場で他の従業員をいじめる
			1.4.2.3._衛生上の問題がある
			1.4.2.4._その他
	1.5._ルール違反の前歴		
		1.5.1._逮捕	
		1.5.2._ハッキング	

		1.5.3._セキュリティ規則の違反	
		1.5.4._ハラスメントの苦情対象	
		1.5.5._経費・勤務時間・出張等についての不正	
2._動機			
	2.1._金銭的問題		
	2.2._金銭的欲求(greed)		
	2.3._復讐		
		2.3.1._復讐の要因	
	2.4._利益		
		2.4.1._経済的	
		2.4.2._職業的	
		2.4.3._職場内	
3._環境			
	3.1._業種		
	3.2._セキュリティ措置		
	3.3._勤務環境		
	3.4._アクセスコ		

	ントロールの存在の有無		
		3.4.1._物理的アクセスコントロール	
			3.4.1.1._構内への物理的アクセスを管理するためのルール
			3.4.1.2._構内への物理的アクセスを管理するためのメカニズム
		3.4.2._電気的アクセスコントロール	
			3.4.2.1._情報システムへの電気的なアクセスを管理するためのルール
			3.4.2.2._情報システムへの電気的なアクセスを管理するためのメカニズム
		3.4.3._事例	
			3.4.3.1._他の従業員がアクセスしたままで不在
			3.4.3.2._組織に知られずにアカウントを作成できる
			3.4.3.3._確認や組織に知られることなしにコードを作成しシステムに組み込む

			3.4.3.4._退職後のアクセスを不可能にする措置が十分でない
4._先行事案			
	4.1._満たされない期待		
		4.1.1._昇進	
		4.1.2._異動	
		4.1.3._昇給	
		4.1.4._賞与	
		4.1.5._権限	
		4.1.6._勤務環境	
			4.1.6.1._インターネットへのアクセス制限
			4.1.6.2._その他
	4.2._ストレス事案		
		4.2.1._制裁	
		4.2.2._解雇	
		4.2.3._休職	
		4.2.4._事例	
			4.2.4.1._よくない勤務評価

			4.2.4.2._不適切な行動に対する叱責
			4.2.4.3._職務懈怠による休職措置
			4.2.4.4._業績不振による降格
			4.2.4.5._権限の制約･インターネットアクセス制限
			4.2.4.6._給与・賞与に対する不満
			4.2.4.7._退職に際して手当などがない
			4.2.4.8._新たな上司
			4.2.4.9._離婚
			4.2.4.10._家族の死去
	4.3._行動面の前兆		
		4.3.1._薬物利用	
		4.3.2._職場内でのもめ事	
		4.3.3._攻撃的・暴力的行動	
		4.3.4._会社の経費の不適切な使用	
		4.3.5._気分の揺れが激しい	

		4.3.6._業務実績がふるわない	
		4.3.7._怠業	
		4.3.8._性的いやがらせ	
		4.3.9._資格についてのごまかし	
		4.3.10._服装規定の不遵守	
		4.3.11._不潔	
		4.3.12._その他、社内ルールやポリシーの(明確な)違反	
	4.4._技術面での前兆		
		4.4.1._ハッキングツールのダウンロード・利用	
		4.4.2._文書管理・ソフトウェアの欠陥	
		4.4.3._顧客情報・従業員情報への不正アクセス	
		4.4.4._勤務中の不適切なインターネットアクセス	
		4.4.5._アクセスパスの	

		作成	
			4.4.5.1._バックドアの仕込み及び利用
			4.4.5.2._パスワードクラッカーのインストールと起動
			4.4.5.3._遠隔操作ツールのインストール
			4.4.5.4._組織のシステムにアクセスするためのモデムのインストール
			4.4.5.5._退職時のシステムセキュリティ措置の不備の利用
5._行為			
	5.1._窃盗		
		5.1.1._企業対象	
		5.1.2._同僚対象	
		5.1.3._知的財産	
		5.1.4._企業秘密	
		5.1.5._その他秘密情報	
	5.2._破壊		
		5.2.1._情報	
		5.2.2._システム	

		5.2.3._ネットワーク	
		5.2.4._企業評価・声望	

6-2　調査票

本調査においては個々の事例を元となる資料(被疑者調書など)をもとに、調査票に詳細を描き写す作業を行った。(この作業をコーディングと呼ぶ。) 調査票は CERT/CC の内部犯行調査の成果物である報告書を参考に作成した。この調査票が内部犯行を理解する上での参考となることを期待し、付録として本報告書に加筆し掲載した。

1 章と 2 章は内部犯行事例の概略を記入する設問が中心である。3 章と 4 章は一部設問が重複しているものがあるが、これは原資料が違う点に注意されたい。3 章は主に警察が所有する事例の被疑者調書から、犯行者個人の情報や動機などを書き写すものである。つづく 4 章は主に被害者調書などから、被害者あるいは第三者の視点からの情報を書き写すことを目的としている。詳細については報告書本編を参照されたい。

1-1. 一意番号(ID)
記入例　00001
回答の書式　　半角数字 5 桁
入力すべき内容　ユニークなケース ID。

1-2. 事件名
記入例　大手都銀 A のシステム監査部員が顧客名簿を持ち出した事例。
回答の書式　　自由記述 50 文字程度
入力すべき内容　ケースを特定する呼称。

1-3. 犯行が行われた発生年月日
記入例　2008/07/14
回答の書式　　日付を YYYY/MM/DD 形式

入力すべき内容　ケースにおける主たる犯行が行われた日時。

2. 事件関係項目

2-1. 犯行発覚の経緯

記入例　不審に思った同僚が上長に報告した。

回答の書式　　自由記述 50 文字程度

入力すべき内容　犯行が第三者によって以下に発見されたか。

2-2. 捜査の端緒

記入例　部下からの報告を受けた上長と総務が相談。顧問弁護士を通じて警察に捜査依頼した。

回答の書式　　自由記述 50 文字程度

入力すべき内容　警察による捜査が行われるに至ったきっかけ。

2-3. 概要

記入例　大手都銀 A のシステム監査部員が顧客名簿を持ち出した。

回答の書式　　自由記述

入力すべき内容　事件の概要。

2-4. 主な適用条文、適用法

記入例　不正競争防止法の X 条 Y 項。

回答の書式　　自由記述

入力すべき内容　調書から事案に適用された主な条文を記載する。

2-5. 事件類型

記入例　4

回答の書式　　"選択式(複数回答可)

1, システム悪用(Employee Fraud)

2, 情報の持ち出し(Theft of Information)

3, 破壊行為(IT Sabotage)"

入力すべき内容　"事件を CERT/CC 類型にあてはめるとどのタイプとなるか。類型の基準は下記の通り。

1, システム悪用(Employee Fraud) - システム悪用: 組織の財やサービスをごまかし(deception)やぺてん(trickery)で手に入れる。

2, 情報の持ち出し(Theft of Information) - 機密や知財に関連する情報などを組織から盗み出す。
3, 破壊行為(IT Sabotage) - 特定個人、組織(含む組織のデータ、システム、日常業務)に損失を与えるという意志に基づいた悪意ある行動"。

2-6. 犯行目的
記入例　ギャンブルにはまり悪化した家計を支えるために、名簿を持ち出し業者に転売することで金銭を得ようとした。
回答の書式　　自由記述
入力すべき内容　犯行の目的を自由記述。

3. 関係
3-1. 被疑者構成
記入例　単独の犯行
回答の書式　　自由記述
入力すべき内容　単独犯か。複数による組織だった犯行か?

3-2. 被疑者 1
記入例　被疑者 1。
回答の書式　　被疑者 1,被疑者 2 など
入力すべき内容　被疑者の番号を記載する。

3-2-1. 基本事項
3-2-1-1. 被疑者性別
記入例　男性
回答の書式　　二者択一 (男性/女性)
入力すべき内容　被疑者の性別を記載。

3-2-1-2. 被疑者年齢
記入例　34
回答の書式　　数字二桁 XX
入力すべき内容　被疑者の犯行時の年齢を記載。

3-2-1-3. 被疑者国籍
記入例　日本

回答の書式　　自由記述
入力すべき内容　被疑者の国籍を記載する。

3-2-1-4. 被疑者住所
記入例　東京都板橋区板橋 1-33-xx 建物名 309 号室
回答の書式　　自由記述
入力すべき内容　被疑者の犯行時の現住所を記載。

3-2-1-5. 被疑者職業
記入例　会社員
回答の書式　　自由記述
入力すべき内容　被疑者の犯行時の主たる職業を記載。

3-2-1-6. 被疑者氏名
記入例　鈴木 正男
回答の書式　　苗字(半角スペース)名前
入力すべき内容　被疑者の氏名を記載。

3-2-1-7. 被疑者前歴
記入例　無し
回答の書式　　自由記述
入力すべき内容　被疑者の前科などを記載。

3-2-1-8. 被疑者に関する特記事項
記入例　1
回答の書式　　選択式
1,虚言癖がある、誠実さに欠ける
2,見方が一面的、一方的
入力すべき内容　「虚言癖がある、誠実さに欠ける 」「見方が一面的、一方的」などの選択肢を選択。(複数回答可能)

3-2-2. 生育環境・家庭環境
3-2-2-1. 家族構成
記入例　父、母、祖母、妹
回答の書式　　自由記述

入力すべき内容　犯行時の被疑者の家族構成などを記載する。調書の記載に従う。

3-2-2-2. 学歴
記入例　1870 年 第一中学校卒業
1880 年 第二高校卒業
1900 年 第三大学 経済学部卒業
回答の書式　　自由記述
入力すべき内容　被疑者の学歴を中学校から記載する調書に記載がない場合、省略可能だが最終学歴は必須。

3-2-2-3. 転居状況
記入例
"1970 年 広島県広島市に生まれる
1880 年 東京都板橋区に転居
"
回答の書式　　自由記述
入力すべき内容　被疑者が転居している場合に転居した年と場所を記載。

3-2-3. 現在の同居人
3-2-3-1. 同居人
記入例　配偶者と子供 1 人(10 歳、男児)
回答の書式　　自由記述
入力すべき内容　犯行時の同居人を自由記述する。(家族以外のルームメイトや友人などを含む)

3-2-4. 健康状態

3-2-4-1. 通院状況
記入例 特になし(歯医者に年に数回程度)
回答の書式　　自由記述
入力すべき内容　被疑者が犯行時の通院状況。

3-2-4-2. 既往歴
記入例 高血圧・C 型肝炎
回答の書式　　自由記述

入力すべき内容　被疑者の既往歴。

3-2-4-3. アルコール中毒
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　左記の症状が認められる場合に Y。

3-2-4-4. 薬物中毒
記入例　Y
回答の書式　　二者択一 (Y/N)
入力すべき内容　左記の症状が認められる場合に Y。

3-2-4-5. パニック障害
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　左記の症状が認められる場合に Y。

3-2-4-6. 配偶者への暴力癖
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　左記の症状が認められる場合に Y。

3-2-4-7. その他
記入例　とくになし
回答の書式　　自由記述
入力すべき内容　その他記載すべき事項。

3-2-5. 経済状況
3-2-5-1. 年収
記入例　1000 万円
回答の書式　　自由記述
入力すべき内容　被疑者の年収を記載。

3-2-5-2. 借金
記入例　25 年払いの住宅ローン(借入総額 2000 万)

回答の書式　　自由記述
入力すべき内容　被疑者の借金状況について記載。

3-2-5-3. 貯蓄
記入例　XX 銀行に定期預金 200 万と普通預金 300 万円
回答の書式　　自由記述
入力すべき内容　被疑者の預金額を記載。

3-2-5-4. 特記事項
記入例　特になし
回答の書式　　自由記述
入力すべき内容　被疑者の経済的状況について特記事項を記載。

3-2-6. 被疑者の職務経歴
3-2-6-1. 被疑者の職務経歴
記入例
1978 年　XX システム開発　入社
1988 年　XX システム開発　制御システム課長
1994 年　XX 銀行　入社
1998 年　XX 銀行　IT 推進課
2000 年　XX 銀行　IT 推進課長
回答の書式　　自由記述
入力すべき内容　被疑者の主な職歴を記載。

3-2-6-2. 被疑者の技術的能力
記入例　自宅にパソコンを 3 台持ち、インターネットバンキングやオークションなどに利用。XXX という情報技術の資格をもつことからも技術的能力は高い。
回答の書式　　自由記述
入力すべき内容　被疑者の IT に関する技術的な能力を記載。自宅でのパソコン保有の有無など。

3-2-7. 被害組織との関係
3-2-7-1. 契約上の取り決め
3-2-7-1-1. 雇用形態
記入例

契約社員
回答の書式　　選択式
1,社員 2,契約社員 3,派遣社員 4,業務委託を受けて 5,アルバイト/インターン 6,その他()"
入力すべき内容 被疑者の雇用形態について最も適切なものを選択。

3-2-7-1-2. 特に不正アクセスや秘密保持等に関する取り決め
記入例
1,顧客情報守秘の宣誓書を入社時に提出
2,雇用契約書内に自社特許に関する守秘義務を定めた条項あり
回答の書式　　自由記述
入力すべき内容 被害組織との間で結ばれた守秘義務契約や誓約書、覚書のうち関連が強いと思われるものについて記載。

3-2-7-2. 参加していた時期・期間、部署
3-2-7-2-1. 被害組織に参加していた時期、期間
記入例 2000/4/1 から 2007/8/15
回答の書式　　自由記述
入力すべき内容 被疑者が被害組織に在籍していた期間を記載する。

3-2-7-2-2. IT 部門に属していた期間
記入例 2004/9/1 から 2007/4/30
回答の書式　　自由記述
入力すべき内容 被疑者が被害組織における IT 部門に在籍していた期間を記載する。

3-2-7-3. 就職・参加時の状況
3-2-7-3-1. 就職参加時の状況
記入例　3 年連続最高益を記録し、社員は年に 20%のペースで増加していた。
回答の書式　　自由記述
入力すべき内容 被疑者参加時の被害組織の雰囲気。特に業績などについて記載する。

3-2-7-4. 処遇
3-2-7-4-1. 給与の水準
記入例　年収 500 万程度
回答の書式　　自由記述

入力すべき内容　被疑者の給与水準を具体的に記載。

3-2-7-4-2. 給与額推移
記入例
回答の書式　　自由記述
入力すべき内容　被疑者の給与の増減を具体的に記載。

3-2-7-4-3. 組織内の地位
記入例　IT 推進課長、社内横断情報化プロジェクトのメンバー
回答の書式　　自由記述
入力すべき内容　被疑者の組織内での役職、職責を記載。

3-2-7-5. 勤務時の状況
3-2-7-5-1. 就労形態
3-2-7-5-1-1. 単独
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　執務のためのスペースが個室あるいは第三者の目の届きにくい場所に合った場合 Y。

3-2-7-5-1-2. 周囲の関心度
記入例　ほぼ 1 人
回答の書式　　自由記述
入力すべき内容　執務のためのスペースが周囲の同僚などからどの程度目の届く場所にあったかを自由記述。

3-2-7-5-2. 権限
記入例　情報システム部と総務部が管理する全てのサーバの管理者権限を所有。
回答の書式　　自由記述
入力すべき内容　被害組織の情報システム上でどのような権限を持っていたか。

3-2-7-6. 退職関係
3-2-7-6-1. 退職の理由
記入例　4
回答の書式　　"選択式

1, 会社都合による退職(リストラ含む)
2, 自己都合による退職(金銭面のトラブル)
3, 自己都合による退職(人間関係のトラブル)
4, 自己都合による退職(円満退職)
5, 解雇、懲戒免職"
入力すべき内容　被疑者が被害組織を退職した際の理由。在職中の犯行であった場合は本設問に回答しない。退職時に目立ったトラブルが内場合、円満退職として扱う。

3-2-7-6-2. 退職の理由(解雇、懲戒免職の場合)
記入例　40 万円の交際費の私的流用が発覚し、自己都合退職
回答の書式　　自由記述
入力すべき内容　特に退職の理由が解雇や懲戒で有った場合にその理由について記載する。

3-2-7-6-3. 退職後の金銭面の状況
記入例　退職後 1 年間で消費者金融などから 500 万円の借り入れを行った。
回答の書式　　自由記述
入力すべき内容　被疑者が被害組織を退職した後の経済的な状況について。特に問題が認められない場合「良好」と回答する。それ以外の場合は状況について記載する。

3-2-7-6-4. 退職後の職業関係の状況
記入例　良好
回答の書式　　自由記述
入力すべき内容　被疑者が被害組織を退職した後の職業関係の状況について。特に問題が認められない場合「良好」と回答する。それ以外の場合は状況について記載する。

3-2-7-6-5. 退職後の人間関係の状況
記入例　良好
回答の書式　　自由記述
入力すべき内容　被疑者が被害組織を退職した後の被害組織関係者以外との人間関係の状況について。特に問題が認められない場合「良好」と回答する。それ以外の場合は状況について記載する。

3-2-7-6-6. 退職後の被害組織関係者との関係
記入例　3

回答の書式　　自由記述
入力すべき内容　退職後に被害組織内部の人間との接触の有無

3-2-7-6-7. 退職後の被害組織との関係
記入例　2,4
回答の書式　　自由記述
入力すべき内容"被疑者が退職後に被害組織と接触した場合について、その内容を記載。接触が無かった場合には 5 を選択"。

3-2-7-6-8. 退職後のシステムアクセスに関係する状況
記入例　1
回答の書式　　自由記述
入力すべき内容　被疑者が退職後に被害組織システムに対してアクセスした状況について記載。

3-2-8. 犯行の前兆
3-2-8-1. 就職期間中
3-2-8-1-1. 行動面の前兆
記入例　2,4,5
回答の書式　　選択式(複数回答)
1, 職場内でのもめ事 2,攻撃的・暴力的行動 3, 会社の経費の不適切な使用 4,気分の揺れが激しい 5,業務実績がふるわない 6,怠業 7,性的いやがらせ 8,資格についてのごまかし 9,虚言 10,服装規定の不遵守 11,不潔 12,その他、社内ルールやポリシーの(明確な)違反
入力すべき内容　犯行前、被疑者に見られた犯行の前兆となりうる特徴について調書から確認できるものを選択。

3-2-8-1-2. 技術面での前兆
3-2-8-1-2-1. ハッキングツールのダウンロード・利用
記入例　Y
回答の書式　　Y/N の二択
入力すべき内容　犯行前、被疑者に上記の行動が見られた場合 Y。そうでない場合は N。

3-2-8-1-2-2. 文書管理・ソフトウェアの欠陥の利用

記入例　Y
回答の書式　　Y/N の二択
入力すべき内容　犯行前､被疑者に上記の行動が見られた場合 Y｡そうでない場合は N｡

3-2-8-1-2-3. 顧客情報・従業員情報への不正アクセス
記入例　Y
回答の書式　　Y/N の二択
入力すべき内容　犯行前､被疑者に上記の行動が見られた場合 Y｡そうでない場合は N｡

3-2-8-1-2-4. 勤務中の不適切なインターネットアクセス
記入例　Y
回答の書式　　Y/N の二択
入力すべき内容　犯行前､被疑者に上記の行動が見られた場合 Y｡そうでない場合は N｡

3-2-8-1-2-5. アクセスパスの作成
記入例　なし
回答の書式　　選択式(複数回答)
1,バックドアの仕込み及び利用 2,パスワードクラッカーのインストールと起動 3,遠隔操作ツールのインストール 4,組織のシステムにアクセスするためのモデムのインストール
5,退職時のシステムセキュリティ措置の不備の利用　6, アクセス制御(パスワード等)の修正
入力すべき内容　犯行前、被疑者に左記のように、組織外から内部へアクセスするための抜け穴を作成したかについて。選択肢に当てはまらない抜け穴を用意した場合には、その他として具体的に記載する。
6 は事前にパスワードを変更する、あるいはパスワードを変更できる環境を用意するなどが相当する。

3-2-8-1-3. その他
記入例　なし
回答の書式　　自由記述
入力すべき内容　モデル作成のために、前兆行動と会社の対応との因果関係が認められる場合にそれを記載する。

3-2-8-2. 退職後

3-2-8-2-1. 外部からの不審なアクセス
記入例　犯行の約 3 週間前に Web サーバに大量のアクセスが集中し閲覧が困難になった。システム管理部門が調査し、原因不明となっていた。
回答の書式　　自由記述
入力すべき内容　犯行が退職後に行われた場合、犯行前に外部からの不審なアクセスの有無、内容について記載。
犯行が退職前で有った場合空欄のままでよい。

3-2-8-2-2. 情報漏れを伺わせる事案
記入例　顧客名簿が P2P ファイル共有ネットワークに漏えいしているという情報が匿名掲示板などに書き込まれた。
回答の書式　　自由記述
入力すべき内容　犯行が退職後に行われた場合、犯行前に外部からの不審なアクセスの有無、内容について記載。
犯行が退職前で有った場合空欄のままでよい。

3-2-9. 動機
3-2-9-1. 背景
3-2-9-1-1. 会社に対する恨み、不満
3-2-9-1-1-1. 給与
記入例　特になし
回答の書式　　自由記述
入力すべき内容　上記の点について被疑者が恨み、不満を持っていた場合にその内容を記載。特に不満を伺わせるコメントがない場合には「特になし」と記載する。

3-2-9-1-1-2. 待遇
記入例　同期と比較して昇進が遅れていた
回答の書式　　自由記述
入力すべき内容　上記の点について被疑者が恨み、不満を持っていた場合にその内容を記載。特に不満を伺わせるコメントがない場合には「特になし」と記載する。

3-2-9-1-1-3. 仕事内容
記入例　特になし
回答の書式　　自由記述

入力すべき内容　上記の点について被疑者が恨み、不満を持っていた場合にその内容を記載。特に不満を伺わせるコメントがない場合には「特になし」と記載する

3-2-9-1-1-4. リストラ
記入例　特になし、リストラされていない
回答の書式　　自由記述
入力すべき内容　上記の点について被疑者が恨み、不満を持っていた場合にその内容を記載。特に不満を伺わせるコメントがない場合には「特になし」と記載する。

3-2-9-1-2. 会社内の特定の人に対する恨み、不満
3-2-9-1-2-1. 仕事上の問題
3-2-9-1-2-1-1. 給与面、人事面の評価の問題
記入例　同期と比較して昇進が遅れていたことの原因を直属上司である田中係長の「えこひいき」と考え私怨をいだいていた
回答の書式　　自由記述
入力すべき内容　上記の点について被疑者が恨み、不満を持っていた場合にその内容を記載。特に不満を伺わせるコメントがない場合には「特になし」と記載する。

3-2-9-1-2-1-2. 業務上のやり方の問題
記入例
回答の書式　　自由記述
入力すべき内容　上記の点について被疑者が恨み、不満を持っており、なおかつその恨み不満の矛先が組織内の特定個人に向けられていた場合にその内容を記載。

3-2-9-1-2-2. 個人的な問題
記入例　特になし
回答の書式　　自由記述
入力すべき内容　被疑者がなんらかの個人的な問題による恨み、不満を持っていた場合にその内容を記載。

3-2-9-1-3. 個人生活上の問題
3-2-9-1-3-1. ストレス
記入例　特になし
回答の書式　　自由記述

入力すべき内容 被疑者が強いストレスを抱えていた場合にその内容を記載。特に不満を伺わせるコメントがない場合には「特になし」と記載する。

3-2-9-1-3-2. 経済的問題
記入例 実父が 3 年前からガンで入院したことに伴い、医療費が年に 200 万円程度かかる状況であった。
回答の書式 自由記述
入力すべき内容 被疑者が経済的な問題を抱えていた場合にその内容を記載。特に不満を伺わせるコメントがない場合には「特になし」と記載する。

3-2-9-2. 直接的な動機
3-2-9-2-1. 経済的利益
記入例 Y
回答の書式 二者択一 (Y/N)
入力すべき内容 犯行の直接の動機として経済的利益を得ることが含まれる場合に Y。

3-2-9-2-2. 会社を困らせる
記入例 Y
回答の書式 二者択一 (Y/N)
入力すべき内容 犯行の直接の動機として会社全体を困らせることが含まれる場合に Y。

3-2-9-2-3. 会社内の特定の人を困らせる
記入例 直属の上司田中氏を困らせてやろうと考えた
回答の書式 自由記述
入力すべき内容 犯行の直接の動機として会社内の特定個人を困らせることが含まれる場合に、その対象を含めて記載。

3-2-9-2-4. 好奇心
記入例 N
回答の書式 二者択一 (Y/N)
入力すべき内容 犯行の直接の動機として好奇心を満たすことが含まれる場合に Y。

3-2-9-2-5. その他
記入例 特になし
回答の書式 自由記述

入力すべき内容　その他犯行の直接的な動機について記載。

3-2-10. 犯行状況
3-2-10-1. 犯行時の状況
3-2-10-1-1. 飲酒
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　被疑者が犯行時に飲酒をおこなっていたか?

3-2-10-1-2. 関係者と共同
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容

3-2-10-1-3. 関係者による煽り
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　被疑者の性別を記載。

3-2-10-2. 犯行手口
3-2-10-2-1. システムへのアクセス方法
3-2-10-2-1-1. 犯行に及んだ場所
記入例　2
回答の書式　　選択式
0, 物理的なアクセス
1, 社内のネットワークから
3, 社外からインターネットを利用して
4, 社外から社員のみにゆるされた接続方式を利用して
入力すべき内容　被疑者が被害を受けた IT システムにどのようにアクセスしたかを選択する。

3-2-10-2-1-2. アクセスの時間帯
記入例　業務時間中に行われた
回答の書式　　自由記述
入力すべき内容　犯行がどの時間帯に行われたかを記載する。

3-2-10-2-1-3. 認証情報(自分に発行されたもの)の悪用
記入例　1
回答の書式　　選択式
1, 被疑者に対して発行された個人アカウントが悪用された
2, 被疑者に対して発行された共有のアカウントが悪用された
3, 被疑者に対して発行され、すでに無効にされているはずのアカウントが悪用された
4, その他
入力すべき内容　犯行に被疑者に対して与えられた/与えられていたパスワードなどが利用された場合。

3-2-10-2-1-4. 認証情報(不正に取得したもの)の悪用
記入例　3
回答の書式　　"選択式
1,システム管理者の地位を利用して入手した他人のアカウントが悪用された
2,引き継ぎや手伝いと言った作業の為に教わった他人のアカウントが悪用された
3,他の従業員が机の周囲などに貼っていたアカウントが悪用された
4, システム管理者の特権を利用して本来ダミーのアカウントを作成した
5,その他"
入力すべき内容　犯行に被疑者に対して与えられた/与えられていたパスワード以外が利用された場合。

3-2-10-2-1-5. システムに関する知識
記入例　2
回答の書式　　選択式
1,そのような地位にいた、業務上必要なため知っていた
2,職場の同僚などから教えてもらった
3,本人の技術的能力から推察、解明した
4,その他
入力すべき内容　犯行に必要となるシステムに関する予備知識(ID,パスワードはこれに含まない)を被疑者がいかに手に入れたか。

3-2-10-2-2. 犯行手口
記入例
回答の書式　　自由記述

入力すべき内容　犯行手口について詳細に記述。

3-2-10-2-3. 犯行行為
記入例
回答の書式　　自由記述
入力すべき内容　犯行行為について詳細に記述する。回数、被疑者が得た利益などもポイント。

3-2-11. 犯行後の行動
3-2-11-1. 犯行を隠蔽するための行動
3-2-11-1-1. 会社からの調査に対する虚偽の申告
記入例　Y
回答の書式　　二者択一 (Y/N)
入力すべき内容　犯行を隠蔽するために上記の行動が見られた場合に Y。

3-2-11-1-2. 使用した PC の処分や記録の消去
記入例　Y
回答の書式　　二者択一 (Y/N)
入力すべき内容　犯行を隠蔽するために上記の行動が見られた場合に Y。

3-2-11-1-3. 利用していたプロバイダとの契約解除
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　犯行を隠蔽するために上記の行動が見られた場合に Y。

3-2-11-1-4. システムログの消去
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　犯行を隠蔽するために上記の行動が見られた場合に Y。

3-2-11-1-5. その他
記入例　特になし
回答の書式　　自由記述
入力すべき内容　その他犯行を隠蔽するための行動が認められた場合その内容を記載する。

3-2-11-2. 会社側が了知しているかを確認するための行動
3-2-11-2-1. 会社側が了知しているかを確認するための行動
記入例　かつての同僚に対してメールや電話などで「最近変わったことはないか」などと頻繁に尋ねた
回答の書式　　自由記述
入力すべき内容　犯行が組織内で発覚しているか否か、あるいは捜査状況などを確認するための行動が見られた場合その内容について記載。

3-2-11-3. 補償措置
3-2-11-3-1. 犯行を認めたか
記入例　2
回答の書式　　選択式
0,自首　1,(発覚後に)自発的に申告　2,企業・組織からの追及により認める　3,捜査機関による捜査の段階で認める　4,裁判で認める　5,認めない
入力すべき内容　被疑者が自らの犯行をどの段階で認めたかを選択する。

3-2-11-3-2. 金銭的賠償を行う
記入例　N
回答の書式　　二者択一 (Y/N)
入力すべき内容　被疑者が自らの犯行による金銭被害を賠償した場合に Y。

3-2-11-3-3. その他
記入例　特になし
回答の書式　　自由記述
入力すべき内容　その他犯行後の被疑者の行動について特筆すべき点を記載する。

4. 被害者関係
4-1. 被害者
4-1-1. 被害者属性
4-1-1-1. 被害者所在地
記入例　特になし
回答の書式　　自由記述
入力すべき内容　被害企業の所在地。

4-1-1-2. 被害者名
記入例　特になし
回答の書式　　自由記述
入力すべき内容　被害企業の法人名。

4-1-1-3. 被害者代表者
記入例　特になし
回答の書式　　自由記述
入力すべき内容　被害企業の代表者の氏名。

4-1-1-4. 被害者概要
4-1-1-5. 被害者規模
4-1-1-5-1. 従業員数
記入例　特になし
回答の書式　　自由記述
入力すべき内容　被害企業の従業員数。

4-1-1-5-1-1. その他
記入例　閉鎖的な雰囲気を感じていた
回答の書式　　自由記述
入力すべき内容　被害者となった企業についてその他特筆すべき点。例えば、家族経営のアットホームな雰囲気であるとか、ワンマン経営者で閉鎖的な社風であるとか。

4-1-2. 犯行に関係する環境
4-1-2-1. システム
4-1-2-1-1. システム構成
4-1-2-1-1-1. 汎用性のあるシステム
記入例　1,2,3,4,5
回答の書式　　選択式
1, メールサーバ 2, 顧客情報管理システム 3, 社員向けスケジューラー 4, 社内情報共有システム 5, 社内 Web サーバ 6, 会計システム 7, 在庫管理システム 8, 生産管理システム 9, 内線通話システム 10, その他
入力すべき内容　組織で利用されている、汎用的なシステムについて使われているもの全てを選択。

4-1-2-1-1-2. 当該企業・組織固有のシステム
記入例　広告代理店 B 社との間に専用の広告出稿システムを構築運用している。
回答の書式　　自由記述
入力すべき内容　その他組織で利用されている汎用性のないシステムについて自由記述する。

4-1-2-1-2. システム構築運用の形態
記入例　2
回答の書式　　選択式
1,被害組織自体が構築・運用している場合
2,実質的に他組織が構築・運用している場合
3,両者の組み合わせ
入力すべき内容

4-1-2-1-3. 組織外のシステムの利用
記入例　3
回答の書式　　選択式
1,ネット取引　2,ファームバンキング　3,その他
入力すべき内容

4-1-2-1-4. その他
記入例　特になし
回答の書式　　自由記述
入力すべき内容　その他組織で利用されているシステムについて特筆すべき事項。

4-1-2-2. 職場環境
4-1-2-2-1. 犯行のチェックに関係する仕組み
4-1-2-2-1-1. 物理的アクセスコントロール
記入例　顧客情報を扱うシステムがあるフロアには最低2回の虹彩による認証をパスする必要がある
回答の書式　　自由記述
入力すべき内容　犯行を防ぐために取られていた物理的なアクセスコントロール手段について記載。

4-1-2-2-1-2. システム的アクセスコントロール

記入例　特になし
回答の書式　　自由記述
入力すべき内容　犯行を防ぐために取られていた技術的なアクセスコントロール手段について記載。

4-1-2-2-1-3. 組織的なコントロール
記入例　2
回答の書式　　選択式
1, マンダトリーバケーション 2, 2 年ごとの配置換え 3, 定期的な内部監査の実施 4, 定期的な外部監査の実施 5, 認証の取得
入力すべき内容　犯行を防ぐために取られていた組織的なコントロール手段について記載。

4-1-2-2-2. 一般的なセキュリティ対策
記入例　2
回答の書式　　"選択式
1, 定期的なシステムパスワード変更 2, ウイルス対策ソフトの利用 3,セキュリティポリシーの策定 4, アクセスログモニタリング 5, 時刻合わせ 6,その他"
入力すべき内容　一般的なセキュリティ対策として被害組織において実施されていた項目を追加。

4-1-2-2-3. その他
記入例　特になし
回答の書式　　自由記述
入力すべき内容　その他組織環境について特筆すべき事項。

4-1-3. 被害状況
4-1-3-1. データの破壊
4-1-3-1-1. 影響を受けた内部システム
記入例　2,3
回答の書式　　選択式
1, メールサーバ 2, 顧客情報管理システム 3, 社員向けスケジューラー 4, 社内情報共有システム　5, 社内 Web サーバ 6, 会計システム 7, 在庫管理システム 8, 生産管理システム 9, 内線通話システム 10, その他

入力すべき内容　犯行により使用不能になった、データの損壊が発生したシステムを選択。

4-1-3-1-2. 影響を受けた外部システム
記入例　3,4
回答の書式　　選択式
1,Web サーバ 2,EC サイト(広告収入なし) 3,EC サイト(広告収入あり) 4,電子受発注システム 5, その他
入力すべき内容　犯行により使用不能になった、データの損壊が発生したシステムの中で、社外にも利用者がいるものを選択。

4-1-3-2. データの流出
4-1-3-2-1. 流出したデータの種類
記入例　1,2
回答の書式　　選択式
1, 顧客データ 2, 社員のデータ 3, それ以外の業務データ
入力すべき内容　犯行により流出した情報について選択肢の中から回答。

4-1-3-2-2. その他流出したデータの内容
記入例　住所、電話番号、家族構成、収入などが記載された東京支社従業員名簿(50 名)が流出した。
回答の書式　　自由記述
入力すべき内容　犯行により流出した情報についてより詳細な内容を回答。

4-1-3-3. 直接的な経済的被害
4-1-3-3-1. 取引システムの不正使用
記入例　特になし
回答の書式　　自由記述
入力すべき内容　企業が犯行に関わって被った直接の金銭被害額を記載。金銭被害が発生していない場合には特になしと記載。

4-1-3-3-2. 会計システムの不正使用
記入例　会計システムの不正使用により、500 万円の営業損失が 2 年間隠蔽されていた。
回答の書式　　自由記述

入力すべき内容　企業が犯行に関わって被った直接の金銭被害額を記載。金銭被害が発生していない場合には特になしと記載。

4-1-3-4. 企業価値についての被害
記入例　特になし
回答の書式　　自由記述
入力すべき内容　企業価値に関する被害で具体的なものがあれば記載する。

4-1-3-5. 企業関係者の被害
記入例　特になし
回答の書式　　自由記述
入力すべき内容　企業関係者が本件をきっかけに被った被害で具体的なものがあれば記載する。

4-1-4. 犯行後の対応
4-1-4-1. 障害(犯行)発生の把握
4-1-4-1-1. 障害把握体制
4-1-4-1-2. 障害の原因の対応把握体制
4-1-4-1-2-1. 外部・内部からの攻撃の可能性についての考慮
記入例
回答の書式　　自由記述
入力すべき内容

4-1-4-1-3. 退職者に対する調査
4-1-4-1-3-1. 電話、面談等での照会
記入例
回答の書式　　自由記述
入力すべき内容

4-1-4-2. 対応
4-1-4-3. 公的機関への届出
4-1-4-3-1. 警察への届出
記入例
回答の書式　　自由記述
入力すべき内容　警察への届け出がおこなわれたか?そしてその時期と理由を記載。

4-1-5. 被害回復状況
4-1-5-1. 復旧の度合
記入例
回答の書式　　"選択式
1, ほぼ完全に復旧 2, 部分的に復旧 3, ほぼ復旧できず "
入力すべき内容 犯行による IT システムへの被害をどの程度復旧することができたか?
永久にデータが失われたなどの場合は 3 を選択する。

4-1-5-2. 顧客への補償
記入例
回答の書式　　自由記述
入力すべき内容 犯行によって組織が顧客へ行った補償の内容。

4-1-5-3. 加害者からの補償
記入例
回答の書式　　自由記述
入力すべき内容 加害者から被害組織への補償の内容。

4-1-5-4. その他
記入例
回答の書式　　自由記述
入力すべき内容 その他被害の回復状況について特記事項があれば記載する。

5. 備考
5-1. 備考
記入例
回答の書式　　自由記述
入力すべき内容 その他上記設問では反映されていない、事案の特徴や調査においての着眼点、調査票記入者の所見などを自由に記載。

6-3　内部犯行にかかわる公開文献調査

本調査においては、CERT/CC で行われた”Insider Threat Research”などの先行研究の成果となる文献を検討した。ここではその際に対象となった文献の中から、特に必要と思われるものの概略を紹介する。

Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem

著者:　Anderson, D.F., Cappelli, D.M., Gonzalez, J.J., Mojtahedzadeh, M., Moore, A.P., Rich, E., Sarriegui, J.M., Shimeall, T.J., Stanton, J.M., Weaver, E., and Zagonel, A.

公開時期:　2004 年 6 月

内容:

・"CERT を中心に 25 人の学術関係者が会し、内部犯行に関する分析の手法を検討したワークショップの成果物。
・内部犯行の分類の手法として、「用いられた技術の洗練度」と「金銭を目的としたものか否か」をそれぞれ X 軸と Y 軸にとってマップする手法が試行された(P10)
・Tim Loyd/Omega 事件を題材に実際の分析が行われた。
・内部犯行に関する俯瞰的なダイナミクス図が収録されている。"

URL:　http://www.cert.org/archive/pdf/InsiderThreatSystemDynamics.pdf

ページ数:　36

Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector

著者: Marisa Reddy Randazzo, Ph.D. (USSS)., Michelle Keeney, J.D., Ph.D. (USSS)., Eileen Kowalski (USSS)., Dawn M. Cappelli (CERT)., Andrew P. Moore (CERT)., Timothy Shimeall (CERT)., and Stephanie Rogers (CERT)

内容: 特に金融セクターにおける内部犯行の事例(23 例、計 26 人の内部犯)を分析したレポートである。対象となったのは 1996～2002 年の事例のみ。8 つの Findings がある。

URL: http://www.cert.org/archive/pdf/bankfin040820.pdf

ページ数: 25

E-Crime Watch Survey 2004

著者: CSO Magazine

公開時期: 2004 年 9 月

内容: CSO Magazine による調査の 2004 年度版である。

URL: http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf

ページ数: -

Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors

著者: Michelle Keeney, J.D., Ph.D. (USSS)., Eileen Kowalski (USSS)., Dawn M. Cappelli (CERT)., Andrew P. Moore (CERT)., Timothy Shimeall (CERT)., and Stephanie Rogers (CERT)

公開時期: 2005 年 5 月

内容:

・内部犯行調査の歴史を概説。 2001 年に USSS と CERT の協力がはじまった。FY2003-2004 にかけては DHS の資金提供を受けていたことなど。

・P11 以降は 1996-20002 までの重要インフラでの内部犯行を数字の単純集計で紐解いている。その後の章では考察や予防法を紹介している。

・付録には実際のケースのより詳細な紹介や各種データが収録されている。

URL: http://www.cert.org/archive/pdf/insidercross051105.pdf

ページ数: 45

E-Crime Watch Survey 2005

著者: CSO Magazine

公開時期: 2005 年 9 月

内容: CSO Magazine による調査の 2005 年度版である。

URL: http://www.cert.org/archive/pdf/ecrimesummary05.pdf

ページ数: -

Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders Analysis and Observations

著者: Eric D. Shaw (Consulting & Clinical Psychology, Ltd.)., Lynn F. Fischer (Defense Personnel Security Research Center)

公開時期: 2005 年 9 月

内容: 米国防総省内での 10 の内部犯行の事例からの知見をまとめた報告書である。

URL: http://www.dhra.mil/perserec/reports/tr05-13.pdf

ページ数: 67

Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System Sabotage

著者: Dawn M. Cappelli (CERT)., Akash G. Desai (CMU)., Andrew P. Moore (CERT)., Timothy J. Shimeall(CERT)., Elise A. Weaver (wpi.edu)., and Bradford J. Willke (CERT)

公開時期: 2006 年 8 月

内容:

・MERIT による内部犯行のモデリングとそのモデルを利用したシミュレーションの結果をまとめた論文。

・モデルを使って主張されているのは 1)継続的に自由度を制限し続けた方が社員の不満は少ない 2)ルール違反に対して早期発見、早期処罰が結果として社員の不満が少ない

3)退職時に監査を行い、攻撃に使われる未知のアクセスパスを 50%あるいは 80%塞ぐことができれば、ダメージを大幅に軽減できる の 3 点である。

・付録として収録されている iAssemble という仮想の企業を使った内部犯行に関するケーススタディを行うことを組織のマネジメントに対して推奨している。

URL: http://www.cert.org/archive/pdf/merit.pdf

ページ数: 34

E-Crime Watch Survey 2006

著者: CSO Magazine

公開時期: 2006 年 9 月

内容: CSO Magazine による調査の 2006 年度版である。

URL: http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

ページ数: 15

Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis

著者: Stephen R. Band, Ph.D. (Counterintelligence Field Activity - Behavioral Science Directorate)., Dawn M. Cappelli (CERT)., Lynn F. Fischer, Ph.D. (DoD Personnel Security Research Center)., Andrew P. Moore (CERT)., Eric D. Shaw, Ph.D. (Consulting & Clinical Psychology, Ltd.)., and Randall F. Trzeciak (CERT).,

公開時期: 2006 年 12 月

内容: 内部犯行調査におけるモデルとそれを用いた分析についての説明。P59 から P63 に渡って、実際に作成された"Abstract Common Model", "Insider IT Sabotage Model", "Espionage Model"の三種類が収録されている。

要旨: 1)様々な個人が元から備える資質に加えてストレス因子が積み重なることが内部犯行のリスクをおしあげる。2)内部犯行に至るまで、あるいはその最中には技術面/行動面における前兆とよべる現象が確認される。3)組織の問題点は前兆の検知や適切な対

応が行われない点にある。 4)内部犯行が発生した組織の多くに物理的、電子的なアクセスコントロールが充分でないという問題が確認されている。

これらの考察に基づき、後半では推奨される対応やポリシーのひな形が提示されている。

URL: http://www.cert.org/archive/pdf/06tr026.pdf

ページ数: 90

Protecting Against Insider Threat

著者: Dawn Cappelli (CERT)., Andrew P. Moore., and Timothy J. Shimeall

公開時期: 2007 年 2 月

内容: 内部犯行の現状を紹介し、その後 13 のベストプラクティスを紹介している短いレポートである。

URL:
http://www.sei.cmu.edu/library/abstracts/news-at-sei/securitymatters200702.cfm

ページ数:

Insider Threats in the SDLC: Lessons Learned From Actual Incidents of Fraud, Theft of Sensitive Information, and IT Sabotage

著者: Dawn M. Cappelli (CERT)., Randall F. Trzeciak (CERT)., and Andrew P. Moore (CERT)

公開時期: 2007 年 3 月

内容: SEPG Conference in Austin, TX - March 27, 2007 での発表資料。

Secure Development Life Cycle(セキュアな製品開発サイクル)に関するカンファレンスであるため、コードレビューの重要性を内部犯行の事例を交えて強調するという内容になっている。

Cylab Common Sense Guide - Best Practices の遵守を開発者に対して求めている。(P27)

URL: http://www.cert.org/archive/pdf/sepg500.pdf

ページ数: 28

E-Crime Watch Survey 2007

著者: CSO Magazine

公開時期: 2007 年 9 月

内容: July 26, 2007 – August 13, 2007 に米国のセキュリティ専門家や警察関係者に対して E-Crime の現状をアンケート形式で問い、寄せられた合計 671 の有効回答を分析したもの。

URL: http://www.cert.org/archive/pdf/ecrimesummary07.pdf

ページ数: 23

Combating the Insider Cyber Threat

著者: Frank L. Greitzer (Pacific Northwest National Laboratory)., Andrew P. Moore (CERT)., Dawn M. Cappelli (CERT)., Dee H. Andrews (Air Force Research Laboratry)., Lynn A. Carroll (Karta Technologies)., and Thomas D. Hull (Oak Ridge Institute for Science and Education)

公開時期: 2008 年 1 月

内容: CERT が Insider Threat Workshop という有料セミナーにおいて実施している MERIT という体験ゲームを奨める内容。要旨とよべるものはない。

URL: http://www.cert.org/archive/pdf/combatthreat0408.pdf

ページ数: 4

Risk Mitigation Strategies: Lessons Learned from Actual Attacks

著者: Dawn M. Cappelli (CERT)., Andrew P. Moore (CERT)

公開時期: 2008 年 4 月

内容: PPT 形式の発表資料で、過去の調査結果からの抜粋が中心である。

要旨: 1)内部犯行の問題は情報セキュリティ担当だけでなく、企業の人事や法務や総務も関心をもつべきである。 2)内部犯行に対するインシデントレスポンスプランを考慮すべきである。 3) セキュリティ文化を組織に根付かせよう。組織のメンバーは全てその組織の情報資産を守る責任があるということを訴えるべきである。

URL: http://www.cert.org/archive/pdf/defcappellimoore0804.pdf

ページ数: 47

The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures

著者: Andrew P. Moore (CERT)., Dawn M. Cappelli (CERT)., and Randall F. Trzeciak (CERT)

公開時期: 2008 年 5 月

内容: 150 例に及び米国の重要インフラでの内部犯行の事例のなかで特に 30 例の IT Sabotage の事例についてモデリングや詳細な解析を行った結果に基づく報告書。

解析から生まれた 7 つの考察が紹介されている。また作成されたダイナミクスに基づき、問題となりやすいポイント、改善の要となるポイントが示されている。P18 以降は MERIT プロジェクトの成果を流用したワークショップの内容が紹介されている。

要旨: 内部犯行では様々な要素が絡み合って犯行に繋がるため、モデリング分析することは有用である。その他の手法をいくつか試したが最終的にシステムダイナミクスが最適という結論に至ったことを主張。

URL: http://www.cert.org/archive/pdf/08tr009.pdf

ページ数: 47

Spotlight On: Programming Techniques Used as an Insider Attack Tool

著者: Dawn M. Cappelli (CERT)., Tom Caron., Randall F. Trzeciak (CERT)., and Andrew P. Moore (CERT)

公開時期: 2008 年 12 月

内容: CERT の内部犯行データベースの中でコンピュータプログラミングの技法が使われたものは 15 例のみである。その 15 例を分析した結果をまとめたのが本資料である。

15 例で行われたプログラムが詳細にわたって記載されている。またそれらのケースから企業がとるべき 15 の対策が紹介されている。

URL: http://www.cert.org/archive/pdf/insiderthreat_programmers_1208.pdf

ページ数: 11

Common Sense Guide to Prevention and Detection of Insider Threats, Version 3.1

著者: Dawn M. Cappelli (CERT)., Andrew P. Moore (CERT)., Randall F. Trzeciak (CERT)., and Timothy J. Shimeall

公開時期: 2009 年 1 月

内容:

・CERT が調べた 1996～2007 の IT Sabotage のケース、合計 80 例に関して言うと、金銭的な利益を得ようとしたものはわずか 5 例にとどまる。残りは復讐などが動機となっている。

・内部犯行を防ぐために重要な 16 の対策が掲載されている。

要旨: 主な論点は過去の調査を踏襲。加えて、以下のような新たなテーマが示された。「外部の第三者と結託して行われる内部犯行」「ビジネスパートナーが関与する事例の増加」「企業合併による内部犯行増加」「文化の違いがもたらす影響。たとえば米国企業で世界各地に支社を持つ場合、内部犯行には各国の文化や法制度の違いが色濃く反映される」などである。

URL: http://www.cert.org/archive/pdf/CSG-V3.pdf

ページ数: 88

Spotlight On: Malicious Insiders with Ties to the Internet Underground Community

著者: Michael Hanley., Dawn M. Cappelli (CERT)., Andrew P. Moore (CERT)., and Randall F. Trzeciak (CERT)

公開時期: 2009 年 3 月

内容: 内部犯行者が第三者と結託して行われる内部犯行にテーマを絞ったレポート。

要旨: 1) いくつかのデータからその脅威は現実のものであり、攻撃は社外から、従業員が退職後に在職中に得た情報を用いて行われる。 2) 攻撃に使われるアカウントは犯行に及ぶ者のものではなく、別の誰かのアカウント、もしくは犯行のために事前に作成された裏アカウントである。 3)犯行者はほとんど全てが高度な技術的能力を持ち、システム管理などを専門とする部署で働いていた。

URL:
http://www.cert.org/archive/pdf/CyLab%20Insider%20Threat%20Quarterly%20on%20Internet%20Underground%20-%20March%202009P.pdf

ページ数: 14

Insider Risk Evaluation and Audit

著者: Eric D. Shaw (Consulting & Clinical Psychology, Ltd.)., Lynn F. Fischer (Defense Personnel Security Research Center)., and Andrée E. Rose (Northrop Grumman Technical Services)

公開時期: 2009 年 8 月

内容: 米国防省に付属する研究所の内部犯行に関する調査報告書である。対策として、入社時に行うスクリーニングの監査シートのサンプルなどを示し、より対策に具体性を持たせようという試みが見られる。

URL: http://www.dhra.mil/perserec/reports/tr09-02.pdf

ページ数: 79

SANS Institute InfoSec Reading Room: Mitigating Insider Sabotage

著者: Joseph Garcia (所属不明)

公開時期: 2009 年 9 月

内容: 各種公開文献から内部犯行の事例について紹介する前半部と、対策を紹介する後半部にわかれている。対策編ですすめられているのは、物理セキュリティの確保、パスワード管理の徹底、システム上での権限の管理、退職時の手順や従業員教育/定期監査などの運用面での対策などである。

特に物理セキュリティ対策について、ソフトウェアの紹介など現実的な方策を示している点が特徴的か。

結論では多重防御の必要性を強調している。

URL:

http://www.sans.org/reading_room/whitepapers/casestudies/rss/mitigating_insider_sabotage_33189

ページ数: 31