

情報システムに関する内部犯行分析手法の調査研究（抄）

坂 明

email:saka@saka.jp http://saka.jp

mobile phone:090-1114-8663

慶應義塾大学 大学院政策・メディア研究科

〒252-8520 神奈川県藤沢市遠藤 5322

慶應義塾湘南藤沢キャンパス（SFC）

目次

第1章 内部犯行をめぐる状況.....	3
1 内部犯行の発生状況 .....	3
2 人的脅威への対応の動き .....	5
3 内部犯行事案検討の意義 .....	6
第2章 調査研究の目的と分析の手法 .....	7
1 文献調査 .....	7
2 事例分析 .....	8
3 本調査研究報告書の内容と成果についての考え方 .....	9
第3章 文献調査 .....	10
第4章 事例分析による調査項目の検討について .....	11
1 事例分析項目設定についての考え方 .....	11
(1) 調査票各項目へのコード付与 .....	11
(2) 心理的・個人的情報に関する項目 .....	11
(3) 同一要素に対する異なる視点からの見方についての項目 .....	11
(4) モデル作成との関係 .....	11
(5) 犯行誘発要因・犯行抑止要因 .....	12

(6) 人間関係要因 .....	14
(7) 対象及びフェイズ（時期）ごとの対応検討に資する項目.....	15
第5章 対応についての考察 .....	17
1 システム面、人間への対応の両面の対応が必要 .....	17
2 対応検討のトリガー（きっかけ）としてのモデル.....	17
3 システム面の対応の重要性.....	18
4 特定対象に対する対策.....	18
5 情報把握に関連して .....	19
おわりに（略） .....	20
文献 .....	20

## 第1章 内部犯行をめぐる状況

### 1 内部犯行の発生状況

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とっている場合でも、内部に犯行者がいる場合、或いは内部犯行者と外部の犯行者が協力している場合、このような者からの攻撃は脅威となりかねない。

こうした内部犯行者による脅威は、人的な脅威と重なる部分が多いが、我が国は政府レベルですら情報システムに関する十分な人的防護措置がとられていないなど、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とコンピュータ関係事案の対処及びその調整を行うCERT（Computer Emergency Response Team）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、それに基づく一般へのベストプラクティスや教材の提示などが行われている。（これらは、[http://www.cert.org/insider\\_threat/](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評判リスク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。

(例)

○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ーに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）

○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製し、渡していた。（外事事務研究会「戦後の外事事務一 スパイ・拉致・不正輸出」 pp.42-44、東京法令出版 2007年）

○外国人従業員による機密情報の持出

自動車部品メーカーに勤務する外国人従業員が、図面データを貸与パソコンに大量にダウンロードし、繰り返し自宅に持ち帰っていた。同社が従業員に事情聴取を行ったところ、貸与パソコンにデータは残っておらず、私用パソコンは破壊されており、データの使用や外部への持ち出しについて確認することはできなかった。（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.5、文献3）

○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、2007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、2兆2714億円の損失が生じている。このうち、不正な情報持ち出し、内部犯罪・内部不正行為、目的外使用によるものを見ると、件数ベースでみると8.9%、流出した情報について人数ベースでみると30.5%となっている。特に、内部犯罪・内部不正行為だけでも人数ベースでは28.3%を占めており、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「2007年度 情報セキュリティインシデントに関する調査報告書」p.3、p.8、2008年11月28日、<http://www.jnsa.org/result/2007/pol/incident/index.html>）。このことは、今回、事例調査をしてみても実感したところである。

平成20年中の不正アクセス行為にかかる犯行の手口を見ても、「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」が163件（前年比+124件、+318%）、「言葉巧みに利用権者から聞き出した又はのぞき見たもの」が26件（前年比-5件、-16%）に上っている。元従業員や知人等によるものは、「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」の1,368件に次いで多いものとなっている。

## 2 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、内閣としても取組の機運がある。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（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](http://www.cas.go.jp/jp/seisaku/counterintelligence/pdf/basis_members.pdf)）、

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」(概要)が公表された

([http://www.cas.go.jp/jp/seisaku/counterintelligence/pdf/basic\\_decision\\_summary.pdf](http://www.cas.go.jp/jp/seisaku/counterintelligence/pdf/basic_decision_summary.pdf))。これは、国の重要な情報や職員等の保護を図るためのものであるが、秘密取扱者適格性確認制度など、人的な要素に着目した対策の導入が図られることとなっている。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なされているところであり (CERT, "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis," p.vii, <http://www.cert.org/archive/pdf/06tr026.pdf>)、こうした面からも内部犯行について調査分析を進めることが重要と考えられる。

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ている(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、文献3)。

### 3 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、まして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になろう。ただ、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、今度の一層に分析や対策立案に当たっての着眼点を明らかにしたものである。

## 第2章 調査研究の目的と分析の手法

今回の調査研究は、

- (1) 米国 CERT とシークレット・サービスが協力して行った調査研究報告書を元に、概ねのチェック項目を把握し、
  - (2) それをベースに日本の事例について詳細調査を行い、
  - (3) 日本版のチェック項目の抽出を行う
- というものである。

これにより、日本でのモデル構築に向けた作業への基礎資料を提供することを目的としている。

### 1 文献調査

米国においては、情報通信システムに関して内部犯行による脅威への関心が高まっており、米国のコンピュータ関係事案対処機関及びその調整機関である CERT と SS（シークレットサービス、国土安全保障省内の捜査機関）の協力によって、詳細なレポートがとりまとめられ、内部犯行に至るモデル作成、対応の好事例集、対応のための訓練コース・資機材の提供などが行われている。これらの資料は、

[http://www.cert.org/insider\\_threat/](http://www.cert.org/insider_threat/)

において公開されている。

ここでは、同サイトで公開されている

CERT, "The "Big Picture" of Insider Threat IT Sabotage Across U.S. Critical Infrastructures" にとりまとめられている事例及びモデルから、調査により抽出している項目についてとりまとめてみる。

## 2 事例分析

詳細調査の対象事例については、日本全国の警察において、平成19年及び20年中に被疑者を検挙（平成18年以前に発生したものも含む。）したサイバー犯罪（情報技術を悪用する犯罪）<sup>1</sup>であって、被疑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。）のうち、6件を取り上げた。本来は10件程度を想定していたが、下記の理由により6件程度でも当初の目的を達成できるとの判断から絞り込むこととした。

（今回対象とした6件選択の理由）

(1) 被害企業について、

○大企業、中小企業、家族経営の企業の各種

○IT企業、一般企業、伝統的企業の各種

が含まれていること、

(2) 犯行形態について

○データ破壊

○情報閲覧

○実質的な財産犯的犯罪

が含まれていること

(3) 利用システムについて

○社内システム、外部システム双方の事例が含まれていること

---

<sup>1</sup> 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p.72など参照。

○規模についても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

(4) 犯行動機として、感情面、経済面などの理由が含まれていること

分析対象とした件数は 6 件と少ないが、米国の研究結果と併せて分析してみた結果、今後の調査分析に当たっての必要な項目・視点のベースとして役立つものであると考えている。

また、少数の事例からではあるものの、対策に向けた若干の知見も得られており、公式の事例による詳細分析によるものとして、活用と今後の調査研究に向けた視点の提供としての意義があるものと考えている。

なお、今回の事例分析に当たっては、事件が特定されることにより関係する方々に影響が及ぶことを避けるため、事件特定に結びつくような情報は本報告書から除いてある。このため、具体的な状況を理解する上で情報が不足しているとの印象を持たれるかもしれないが、この点についてはご寛恕いただきたい。

### 3 本調査研究報告書の内容と成果についての考え方

本調査研究は、文献調査と今次の事例分析により、日本における事例分析のための調査票の様式プロトタイプ（原型）を作成することを目的としている。

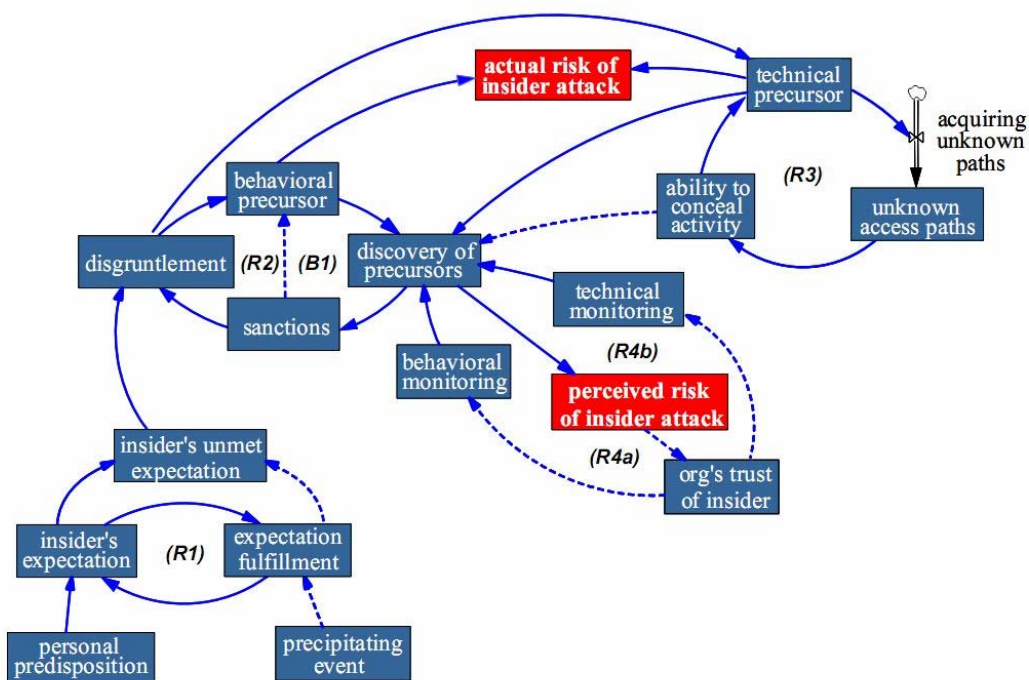
この調査票の様式プロトタイプについては、個々の事件について具体的な日時や関係者名が記載されるものではなく、こうした事件を特定することが可能な情報を削除したものとしている。しかしながら、調査票を全体としてみると、個々の事件としてのまとまりを持った情報であるため、特定の事件と結びつけられることにより、関係者に影響が及ぶ可能性もある。従って、この様式プロトタイプにより作成された個々の調査票の取り扱いについても、慎重な配慮が求められる。

### 第3章 文献調査

先述のように、ここでは、CERTのウェブページ  
[http://www.cert.org/insider\\_threat/](http://www.cert.org/insider_threat/)  
で公開されている

CERT, "The "Big Picture" of Insider Threat IT Sabotage Across U.S. Critical Infrastructures" (文献1) にとりまとめられている事例及びモデルから、調査により抽出している項目についてとりまとめてみる。

図1



Appendix C; CERT, "The "Big Picture" of Insider Threat IT Sabotage Across U.S. Critical Infrastructures," <http://www.cert.org/archive/pdf/08tr009.pdf>

図1は、同報告書に掲載されているモデルである。このモデル作成は、30件の事例の詳細分析に基づいている（同報告書 p.3）。この米国の調査においては、

個人の機微な情報も踏まえて分析が行われており、日本では入手が難しいものや入手できたとしてそれを分析に利用する際に考慮が必要なものなどが見受けられるものの、内部犯行についての"Big Picture"の把握が可能なものになっていると思われる。

以下は、実際の調査票（コードブック）を参照したのではなく、モデルについての説明から抽出した要素であり、実際に米国で使っている調査票ではないことをご理解いただきたい。

#### 第4章 事例分析による調査項目の検討について

本章では、「第2章2事例分析」で述べた警察資料に基づく事例分析に基づき、分析に必要な調査項目について検討を行った。

##### 1 事例分析項目設定についての考え方

###### (1) 調査票各項目へのコード付与

(略)

###### (2) 心理的・個人的情報に関する項目

(略)

###### (3) 同一要素に対する異なる視点からの見方についての項目

同一の項目について、犯行者自身の評価と周囲の評価の双方が出てくる。これは、どちらが正しいというより、そうしたギャップがあることが重要であると考えられる。従って、主体別に調査を行うことになっている。

もちろん、客観的な状況はあるわけで、それらについては項目を統合する、或いは両方残しておいて突き合わせる、といった作業を行う必要がある。

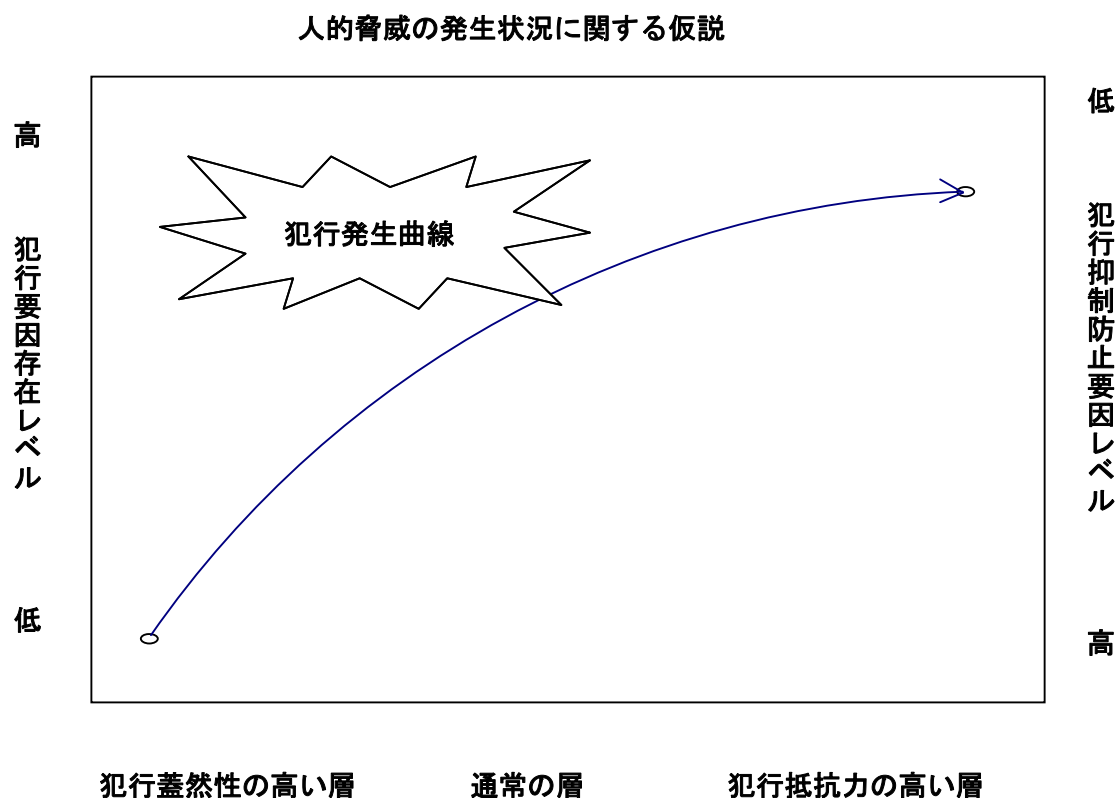
###### (4) モデル作成との関係

(略)

## (5) 犯行誘発要因・犯行抑止要因

今後想定されるモデルについては、図2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 2



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。

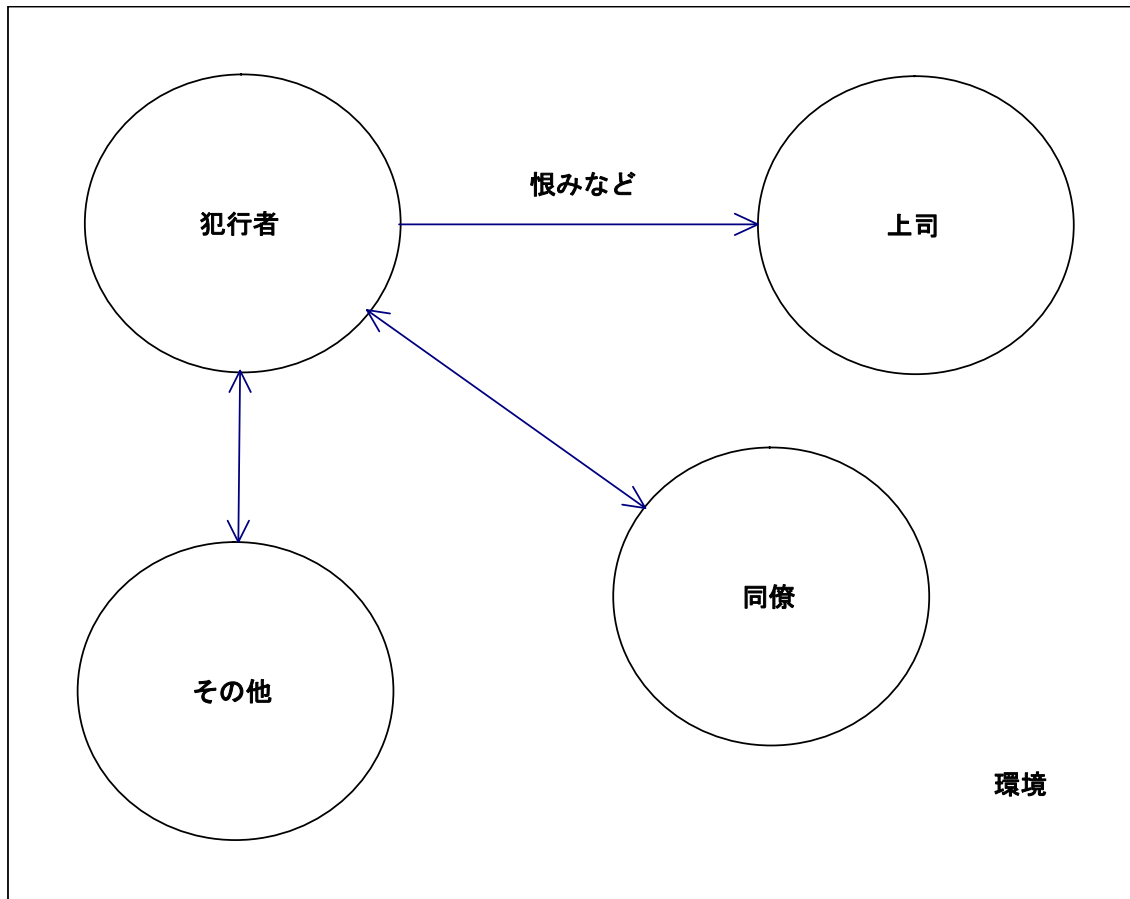
○犯行を行う蓋然性の高い資質を有している者、通常層の者、犯行の誘因に対す  
る高い抵抗力を有する者といった分類を想定し、それぞれのレベルがどの程度  
かについて分析することに資する項目を設定する

○誘因となる要素を抽出できるような項目を設定する

○犯行抑制防止要因レベルは、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。

## (6) 人間関係要因

図3 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3)

(7) 対象及びフェイズ（時期）ごとの対応検討に資する項目

図4 時期と対象に応じた対策

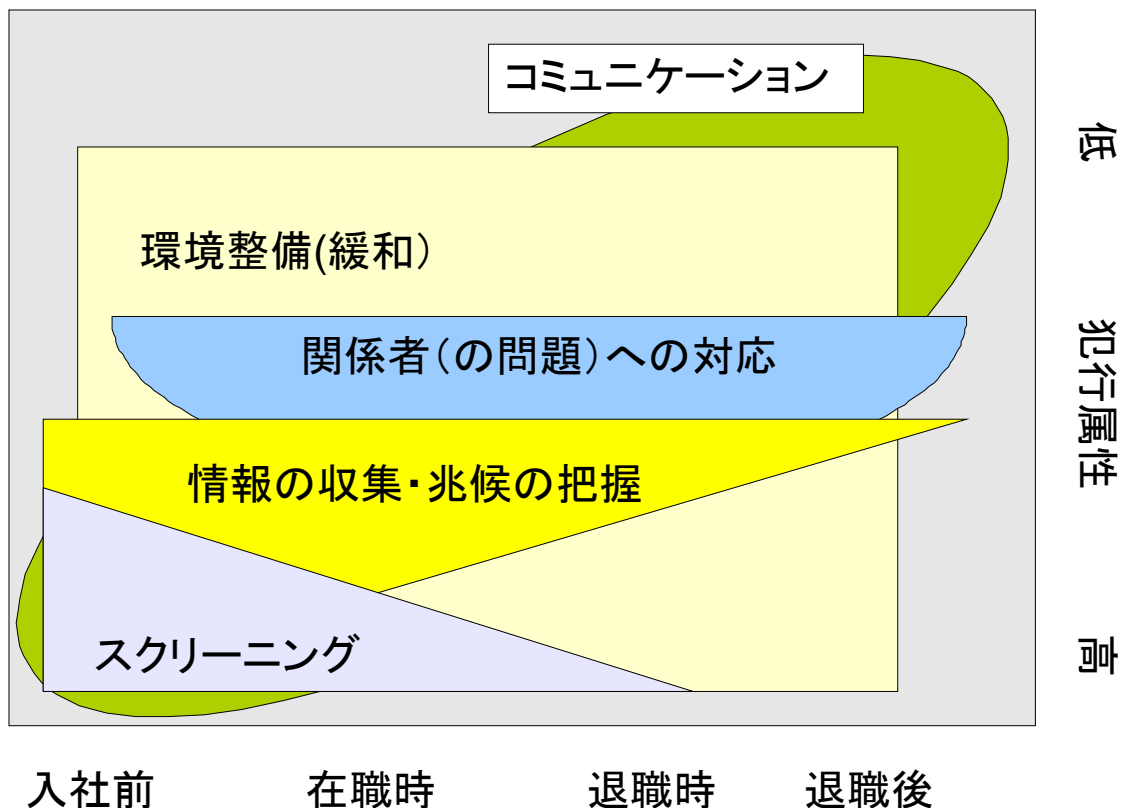


図4のように、犯行抑止のためには、時期と対象を考慮した対策を講じることが求められると考え、これを考察するために必要な項目について含めるよう努めた。図4においては、次のような仮定に基づいて作成したものである。すなわち、犯行属性の高い者について、入社前～採用時の段階では、コミュニケーション等により、情報の収集・兆候の把握を行い、スクリーニングを行う。在職時においては、犯行属性のある者については（或いは本来は情報システムに関係する全職員が対象になるのかもしれないが）、情報の収集・兆候の把握をコミュニケーション等も含めて行い、スクリーニングを行う場合もあろうし、また情報セキュリティ確保のための対策を行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、さらには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。

○全体構成の概略は以下の通り。

#### 1.\_事件・調査実施関係項目

#### 2.\_事件関係項目

#### 3.\_被疑者関係

##### 3.1.\_被疑者構成

##### 3.2.\_被疑者 1

###### 3.2.1.\_基本事項

###### 3.2.2.\_生育環境・家庭環境

###### 3.2.3.\_健康状態

###### 3.2.4.\_経済状況

###### 3.2.5.\_被疑者の職務経歴

###### 3.2.6.\_被害組織との関係

###### 3.2.7.\_犯行の前兆

###### 3.2.8.\_動機

###### 3.2.9.\_犯行状況

###### 3.2.10.\_犯行後の行動

#### 4.\_被害者関係

##### 4.1.\_被害者

###### 4.1.1.\_被害者属性

###### 4.1.2.\_犯行に関する環境

###### 4.1.3.\_被害状況

###### 4.1.5.\_被害回復状況

#### 5.\_備考

## 第5章 対応についての考察

対応の検討は、今後の課題としたいが、今回の調査に基づいて若干のコメントを行いたい。

### 1 システム面、人間への対応の両面の対応が必要

これはある意味で当然のことであり、米国では、従来システム面の対応に力点が置かれていたので、人的脅威への対応について人間の側面からの対応について近年強調されているところがあるようにも考えられる。また、これはそれぞれ独立しているものではなく、人間の振る舞いがシステム上にどのように立ち現れるのかを分析することも重要と考える。

また、対策の分類として、

○特定対象に対する対策

○一般的予防・防御対策

といった形も考えられる。

### 2 対応検討のトリガー（きっかけ）としてのモデル

米国のモデルは、日本から見ると機微な個人的情報もベースにして作成されているところがある。そうした機微な情報も含め、モデルの適合性についての程度のものと考え、活用するかという課題がある。

例えば、どのような属性を持つ個人が人的脅威をもたらすか、という点についても、特定の属性群を有する者が全て犯行に及ぶわけではなく、おそらく及ばない者の方が多いのではないかと思われる。従って、モデルは該当人物や該当するケースについて直ちにラベルを貼り、強い対策を講ずるためのものというよりは、観察ないし対策検討のためのきっかけとして活用することになる。

逆に言えば、モデルの精度もある程度余裕のあるものとして考えても、その

利用方法が適切である限り差し支えないと思われる。

### 3 システム面の対応の重要性

また、システム面では、軽微な攻撃についても、障害の原因の究明の際、人的脅威の可能性、すなわち攻撃の可能性も含めて検討することが重要であると思われる。人間の振る舞いがシステム上にどのように立ち現れるのかを分析することも重要であるが、そのためにはデータの集積とその分析が必要であり、一種のデータマイニングのような方策も検討に値する。

### 4 特定対象に対する対策

分析により高度の犯行蓋然性が見られた者に対しては、段階に応じた対応が取られることになる。

例えば採用時について考えてみると、採用時にこれまでの職務履歴を大きく故意に自らに有利になるように偽っているような場合、それが採用担当者に分かった場合には、対象者の誠実性に問題ありとして採用されない場合が多いと思われる。(ただし、米国で項目に挙げられている、**mental disorder** の部分は疑問の点も多い。)このような形でのスクリーニングは、人的脅威の発生の防止に寄与している。

既に組織内に、蓋然性が高いとされている者がいる場合には、実質的には通常者を内部犯行に走らせないようにする対策と同様の方策をとることになると思われる。そもそも、図2の仮説にもあるように、犯行に対する通常の抵抗力を有する者でも、人的脅威をもたらす犯行者になり得る。

従って、「積極的対策導入」「衝突回避的対策導入」とも言うべき、ネガティブな刺激を与えるような対策ではなく、私生活も含めた問題解決に向けたアプローチをとることが一般的には適当と考えられる。

退職時については、先述のように、特に企業にとって重要な情報を知っている退職者について、適切なフォローを行い、企業・組織が良好な関係を継続し

ていくことが大切と考えられるが、一般的にも、退職時に冷酷に亘らないことは大切と考えられる。解雇通告の方法の配慮、解雇予告又は解雇予告手当の支給、退職時に所要の手続きをとること、社会保険関係の配慮、退職時の支払いの適正な計算と時期を誤らない支出などが考えられる。また、ここでも人間の感情が関係することから、実際に上記のような措置をとると共に、これをきちんと退職者に伝え、無用の反感を持たれないようにする必要がある。すなわち、ここでもコミュニケーションが重要である。また、コミュニケーション能力の欠如は、問題発生の要因となり得る。

## 5 情報把握に関連して

重大事案の防止のためには、早期に、前兆事案（実際の不正アクセスや軽微なデータ改ざん・破壊を含む）を把握し、これに対処する必要がある。

人的脅威への対応という観点からは、犯行を行う者についてのそれぞれの状況を踏まえて早期対応を行うということになるが、動機の部分で対応するとう場合、常に当該犯行を行う者についての私生活も含めた情報を把握し、これも踏まえて対応を行う、ということになる。米国の例を見ても、例えば、「衛生上の問題」すなわち不潔や服装の乱れ、態度の変化などは外部から観察できるものではあるが、こうした兆候を把握するためには、普段から当該者に対して周囲が気を配り、それに対応する体勢が職場にあることが必要となる。更に、こうした兆候から、当該者が犯行に及ぶことを防止するためのシステム面・人事面などの対応（システムへのアクセス制限、配置部署の変更など）は、逆に問題を深刻化させることもあり得る。すなわち、当該者が、そのような兆候を示すに至った根本的な問題に対して、企業・組織として対応する体勢があるか、ということが問われていることになる。

更に、こうした外面的な兆候について適切な判断を行う場合には、先述のように私生活に関わる情報についても関係者が把握する必要があるが、こうした情報は従来よりも組織において共有されにくくなっている。特に、こうした情

報が、当該者の排除のために使われる場合には、当該者はむしろこうした情報を秘匿する行動を取るであろう。従って、企業・組織は、当該者と常日頃からコミュニケーションをとり、その状況の改善にも協力するという姿勢があることがこうした犯行の未然防止にもつながることになる。

米国の場合、個人の経済的信用能力について、一般的に情報を入手することが可能であるほか、裁判記録の閲覧も一般的に可能である。日本のように、過去の裁判の新聞記事の公開も名誉毀損に当たるといようなことはなく、基本的には公開である裁判の記録については、オープンなものとの位置付けである。紙ベースでの公開（つまり記録が保存してある公官署に出向いて閲覧する必要がある）ばかりでなく、現在はインターネットでアクセスできるところも増えているとのことである。さらに、一部の重大犯罪については、その犯人の居住地も公開されている。こうした状況が米国のモデル作成及び対応に影響を与えていると思われ、日本で同様のモデルに基づく対応を取ることができる環境があるかは検討する必要がある。（文献資料 4、5）

おわりに（略）

## 文献

- 1 CERT, "The "Big Picture" of Insider Threat IT Sabotage Across U.S. Critical Infrastructures, " <http://www.cert.org/archive/pdf/08tr009.pdf>, 2009/01/10 閲覧
- 2 酒巻久、椅子とパソコンをなくせば会社は伸びる！、祥伝社、2005年7月
- 3 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28日、<http://www.meti.go.jp/press/20080728006/20080728006.html>
- 4 DAVID C. LANE, BACKGROUND CHECKS, 2008年12月, 慶應義塾湘南藤沢キャンパスでの講義資料（非公開）

松井茂記、性犯罪者から子どもを守る メーガン法の可能性, 2007, 中央公論社

米国CERTのモデルから作成した調査項目

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. 電氣的アクセスコントロール						
			3.4.2.1. 情報システムへの電氣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氣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無い					
			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. 職場内でのめめ事						
		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						

















			4.1.5.2. 自ら復旧										
			4.1.5.3. 顧客への補償										
			4.1.5.4. 加害者からの補償										
			4.1.5.5. その他										
5. 備考													