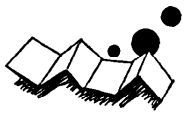
解　説



コンピュータ犯罪†

鳥　居　壮　行††

1. はじめに

わが国で最初のコンピュータ犯罪が発覚したのは，1971年2月である．日経マグロウヒル社の日経ビジネス誌の顧客ファイルがコピーされ，競争相手である日本リーダーズ・ダイジェスト社に売却されていたことが発覚した．それから11年後の1981年には，三和銀行事件が発生し，もはやコンピュータ犯罪を放置しておけなくなり，各方面でコンピュータ犯罪防止対策へ取組むようになった．ここでは，コンピュータ犯罪の位置づけと，ケースの分類・整理を中心にとりまとめる．

2. コンピュータ犯罪とは何か

われわれがコンピュータ犯罪を研究する目的は，事例からコンピュータ・システムの弱点を学び，それを克服する方法を考え出すことといってもよい．コンピュータ犯罪研究の目的は，その人の立場により，あるいは考え方により異なることは当然であろう．しかし，コンピュータ関連の組織に身を置く者にとっては，セキュリティ対策のためのコンピュータ犯罪研究であってしかるべきであろう．

2.1 コンピュータ犯罪の定義

コンピュータ犯罪を定義することにさほど重要な意義を見い出せないが，定義しないことには研究の領域が明確にならない．そこで，情報化の推進をはかる通産省と，コンピュータ犯罪の捜査に直面している警察庁の考え方をとりあげてみたい．

通産省の考え方としては，同省が1982年6月に設置したコンピュータ・セキュリティ研究会が，「コンピュータ犯罪とは，コンピュータが直接的あるいは間接的に何らかの形で介在した社会悪行為である」[1]と定義している．この定義から，コンピュータが直接的に介在するケースとは，ハードウェア，ソフトウェア，データなどのコンピュータ関連資産が犯罪の対象として位置づけられている場合であるし，コンピュータが間接的に介在するケースとは，犯罪の対象は金銭や物品であるが，それらを入手するためにコンピュータを悪用する場合といえる．

一方，昨年版の警察白書によれば，コンピュータ犯罪とは，「コンピュータ・システムに向けられた犯罪またはこれを悪用した犯罪」[2]と定義している．コンピュータ・システムに向けられた犯罪とは，コンピュータ・システム自体が狙われていることを意味していると思われるし，コンピュータ・システムを悪用した犯罪とは，犯罪のために手段としてコンピュータ・システムを悪用したケースと理解することができる．

この二つの定義は，それぞれ異なる立場からのものであるが，基本的には同じことを表現していると解釈してよいと思われる．そして，セキュリティ対策のためにコンピュータ犯罪を研究する場合は，これらの定義のようになるべく広く解釈して対象領域とすべきである．この事件はコンピュータ犯罪か否か，というような議論は，セキュリティ対策にとって意味はなく，その事件にとってコンピュータ・システムの脆弱性はどこにあったのかが重要なことである．

2.2 コンピュータ犯罪の分類

コンピュータ犯罪には，つぎつぎと新しい手口あるいは傾向が出てきている．たとえば，IBM産業スパイ事件であるが，米国のある著名なコンピュータ犯罪研究家は，この事件をビジネスプランの窃取として「情報の窃取」の中に位置づけている．コンピュータ犯罪を分類することは，ケースを整理するうえにおいて，またセキュリティ対策を立てるうえにおいて非常に役に立つ．

前述の通産省のコンピュータ・セキュリティ研究会では，コンピュータ犯罪を大きく次の4つのタイプに分類している[3]．

① 金銭の不法領得

② コンピュータ・システムおよびデータ等の破壊

† Computer Crime by Moriyuki TORII (Japan Information Processing Development Center).

†† (財)日本情報処理開発協会

③ マシンタイムの盗用
④ コンピュータ関連資産の窃取
ⓐ 有形資産（ハードウェア等）
ⓑ 無形資産（プログラム，情報等）

この分類については，①の「金銭の不法領得」を「金銭および物品の不法領得」にした方がよいと思われる．コンピュータの利用がますます進展していく中においては，何も常に金銭が狙われるとは限らず，物品を狙い，入手して売りとばせば金銭を手に入れることができる．したがって，物品の不法領得もあるということを明確にしておく必要があろう．

警察側の分類としては，前述の昨年版警察白書によれば，コンピュータ犯罪をその手口から次の6つに分類している．

① 不正データの入力
② データ，プログラム等の不正入手
③ コンピュータの破壊
④ コンピュータの不正使用
⑤ プログラムの改ざん
⑥ 磁気テープ等の電磁的記録物の損壊

わが国のコンピュータ犯罪は，通産省の分類によれば「金銭の不法領得」が圧倒的に多く，警察の分類によれば「不正データの入力」が圧倒的に多い．つまり，このことは，金銭を狙い，不正データを入力するという手口が多いことを物語っている．

3. コンピュータ犯罪の分析

3.1 コンピュータ犯罪の歴史

コンピュータ犯罪を通産省の類型別に，最初の事件が発生した順にあげてみると，まず，コンピュータ関連資産の窃取であるリーダーズ・ダイジェスト事件が，1971年2月に発覚している．これは，すでに述べたように，わが国最初のコンピュータ犯罪である．具体的には，コンピュータ関連資産の中でも，無形資産である情報（顧客情報）が磁気テープから磁気テープへコピーされ，売却（8万2,000人で82万円）された事件であるが，ダイレクトメールに使用されたのがきっかけで発覚した．

つぎに，金銭の不法領得については，1973年4月の岡村製作所事件が最初である．この事件は，販売事務係長が売掛金等の入金に際し，架空口座に振り込み横領したものである．事務上の処理は，伝票を偽造してコンピュータに入力し，つじつまを合わせていた．

コンピュータ・システムおよびデータ等の破壊については，1975年2月に間組事件が発生した．間組のコンピュータ室が，過激派により爆弾を仕掛けられ，爆破された．この種の事件は，過去において欧米では多発したが，わが国では間組事件のみである．

マシンタイムの盗用は，1981年10月に岡山大学事件が表面化した．これは，岡山市内のマイコン・ショップが，店でマイコンを岡山大学のコンピュータに接続して客に実演して見せていたもので，マシンタイムの盗用は延べ45時間に及んだ．岡山大学の先生が同店をおとずれた際に，IDナンバとパスワードを書き込んだリストを忘れていったため，それを使用したものとされている．

以上のように，タイプ別の最初のコンピュータ犯罪が出現してきたが，年別の発生件数[4]を見ると次の通りである．

1971年	1件	1978年	6件
1972年	0件	1979年	4件
1973年	2件	1980年	0件
1974年	4件	1981年	15件
1975年	4件	1982年	8件
1976年	1件	1983年	1件
1977年	1件		

3.2 コンピュータ犯罪の傾向

コンピュータ犯罪は，バッチ・システムが主体の頃にはさほど多発せず，また難問をかかえたような事件も少なかった．しかし，オンライン・システムの普及とともに，発生件数も増え，難しい問題をかかえた事件も発生するようになってきた．そして，今後は，ネットワークの拡大化にともなって，さらに新しい手口が出現する可能性すら見せ始めている．

コンピュータの普及はめざましく，とくに小規模コンピュータの能力アップとともに，将来，一家に一台パソコン時代も夢ではなくなってきている．一方では，ネットワークがますます拡大しており，環境からしてコンピュータ犯罪が減少する要素は何もない．

米国では，1983年夏，ミルウォーキーの414（電話の局番からつけたもの）グループと称するマイコンマニアの青少年グループが摘発された．彼らは，ニューヨークのスローン・ケタリングがんセンター，核兵器の研究で知られるロスアラモス国立研究所，セキュリティ・パシフィック銀行，ダラスのコンサルティング会社，カナダのセメント会社等に不当にアクセスしていたずらしていた．

主犯のジェラルド・ウォンドラは，アップルⅡを使

い，自宅からテレネットに介入し，全米ならびにカナダのコンピュータ・システムにアクセスしていた．おりしも，マイコン少年が NORAD（コロラド州の北米宇宙防空司令部）のシミュレーション・プログラムに自宅からアクセスし，ゲームと思い込んで核戦争のシミュレーションを行い，あわや米ソの核戦争勃発というストーリの映画「ウォーゲーム」がヒットしていたこともあって，この事件はコンピュータ関係者のみならず衝撃を与えた．

今後，コンピュータ犯罪で心配されることは，1つは被害額が巨大化することであり，もう1つは不正アクセスの増加であろう．とくに後者は，プログラムやデータの窃取ならびに変更，そして破壊など，多種多様になる可能性が強い．その場合，データを故意に変更して，結果的に人を殺してしまうことすら有り得る．したがって，不正アクセス防止対策がきわめて重要になりつつあるといえる．

3.3 コンピュータ犯罪の特色

わが国のコンピュータ犯罪で重要な意味をもつ事件をあげると次の通りである．

1971 年　リーダーズ・ダイジェスト事件（わが国初のコンピュータ犯罪）．

1974 年　真由子ちゃん事件（身代金を架空預金口座に振り込ませ，キャッシュカードで引き出そうとした事件）．

伏見信用金庫事件（キャッシュカード偽造事件）．

キャッシュカード盗用事件（暗証番号に生年月日を使用していることが見破られた）．

1975 年　間組事件（コンピュータ室爆破事件）．

1979 年　山口銀行事件（被害額がわが国史上最大）．

1981 年　三和銀行事件（内部・外部の共謀によるオンラインを悪用した詐欺事件）．

北浜クレジット事件（社内の幹部を頂点とする多人数によるグループ犯行）．

近畿相互銀行事件（キャッシュカードの磁気ストライプへの書き込みが判決で文書偽造にあたるとされた）．

岡山大学事件（マシンタイムを盗用した）．

北海道銀行事件（通信回線からデータを盗聴した）．

1983 年　新潟鉄工事件（ソフトウェアをコピーして持ち出した）．

わが国のコンピュータ犯罪で最も多いのは，キャッシュカードをめぐる犯罪である．1974 年は，今日のキャッシュカード犯罪の原型が出現した年と位置づけることができる．とくに，その後のキャッシュカード盗用事件の増加ぶりには，目を見はるものがある．これらのキャッシュカード犯罪の多発は，欧米に比べてわが国の特徴であり，銀行オンライン・システムの普及にともなう現象であるともいえる．

つぎに，1975 年には，間組コンピュータ室の爆破事件が発生したが，その後この種の事件は発生していない．米国では，1970 年代の初頭に，学生運動のあおりで多数の爆破事件が発生したし，ヨーロッパでは，多数の大企業のコンピュータ・センターが，コングロマリットの心臓部だとして極左に爆破された．コンピュータ爆破事件が少ないのも，わが国コンピュータ犯罪の特徴である．

さらに，1981 年になると，三和銀行事件や北浜クレジット事件などに見られるように，複数犯が増える傾向にあり，被害額も大きくなってきている．ただし，それでも現段階では，米国の金融機関等で発生している大規模コンピュータ犯罪と比較すると，10 分の1程度にも満たない．今後は被害額にも注目する必要があろう．

この 1981 年には，不正アクセスによるマシンタイム盗用事件や盗聴事件という，新しい手口も現われた．とくに，不正アクセスについては，ネットワークの拡大とともに，最も心配される事柄である．

4. ケーススタディ

4.1 情報をめぐる犯罪

情報を窃取する手口としては，まずコピーがある．このコピーも，磁気テープから磁気テープへコピーする場合もあれば，ドキュメント類のハードコピーの場合もある．つぎに，盗聴がある．盗聴についても，直接通信回線に接続して録音する場合もあれば，衛星通信等においては傍受することになる．現在，盗聴事件は世界中で二例といわれているが，その1つは日本の北海道銀行事件であり，もう1つは米国で発生した事件で，コンピュータに発信器を取り付けて，数キロ離れた場所で傍受したものといわれている．さらに，磁気テープ，ドキュメント等をそのまま持ち去ることもできる．また，情報は見読してメモしたり頭の中に入れて利用することも可能である．

すでに述べたように，わが国最初のコンピュータ犯罪であるリーダーズ・ダイジェスト事件は，顧客ファイルのコピー事件である．同様の事件としては，1978 年に，チャリティ・プレート協会事件が発生している．これは，福祉団体の日本チャリティ・プレート協会

の協力者ファイル(銀行の貸し金庫に保管)を総務課長がコピーし,他の福祉団体へ横流しをしたものである.

4.2 ソフトウェアをめぐる犯罪

わが国におけるこの種の事件としては,1983年に発生した新潟鉄工事件が記憶に新しい.この事件は,同社の企画管理部長代理とその部下ら四人による仕業で,同社が約20億円をかけて開発したCADソフトウェアをコピー(約3万枚)して持ち出し業務上横領罪に問われた.

公判において,予想された通り弁護人は,被告らが開発したソフトウェアであり,著作権法による権利に基づく正当な行為であることを主張している.今後のなりゆきが注目される.

米国では,すでに1964年に,この種の事件としては最初の判決が出ている.テキサス州で発生したハンコック事件である.プログラマであるハンコックが,会社のプログラム(500万ドル相当価値)を窃取し,取引先に売却しようとしたものである.公判において,プログラム(無体物)は,窃盗罪の対象となる財産には当らないとの主張がなされたが却下され,懲役5年の判決が下された.

4.3 キャッシュカードをめぐる犯罪

キャッシュカード犯罪は多種多様である.身代金誘拐事件で身代金をキャッシュカードで引き出す手口から,キャッシュカードの偽造,キャッシュカードの盗用などがある.そして,気になることは,強盗に押入り,金品とともにキャッシュカードも奪い,暗証番号を聞き出し,口封じのために殺人に至るという事件がすでに発生している.

キャッシュカードの偽造事件である近畿相互銀行事件と北海道銀行事件では,2つの大きな相違点がある.1つは,近相事件が内部のキャッシュカード作成担当者の犯行であるのに対して,北銀事件は,外部の電電公社職員であった.もう1つは,キャッシュカード偽造のために必要な磁気ストライプ部分の,口座番号や暗証番号等の情報の入手方法が異なる.近相事件の場合は,実際にキャッシュカードを作成する過程で,高額預金者を選び,必要情報を自分の住所録にメモしている.北銀事件の場合は,電電公社職員として通信回線の保守にたずさわっている立場を利用して盗聴したものである.

近相事件は,オンライン・センターのデータ処理部門で,オペレータとしてキャッシュカードの発行にあたっていた行員が,サラ金から1500万円もの借金をかかえ,利息すら支払えない状態になり犯行に及んだものである.まず,上司の机の中から鍵を持ち出してコピーを作成した.つぎに,キャッシュカード発行依頼書から,残高の多い口座を選び,口座番号,氏名,暗証番号等を自分の住所録にメモした.そして,自分が発行を受けているキャッシュカード4枚に,メモしたデータを記録して偽造した.これが,1981年10月9日に,いろいろな相互銀行の14カ所で989万9,000円を引き出した第1回目の犯行である.

この直後,犯人は近相のオンライン・センターに入り込み,未使用のキャッシュカード250枚を盗み,うち12枚を偽造し,10月12日に,相互銀行8カ所で行使し,1,016万6,000円を引き出した.これが2回目の犯行である.

犯人は,有印私文書偽造,同行使,窃盗などの罪に問われた.公判で弁護人は,「キャッシュカードの磁気ストライプ部分は,それ自体視覚可能なものではなく,文書ではない」と主張した.これは,「刑法上,文書とは物体の上に文字その他の符号によって意思または観念を表明したもので,視覚可能なもの」という点を突いたものである.しかし,判決公判においては,「視覚に訴える際に文字や符号で表示されればよい」と,電磁的記録物が再生できる点をもって視覚可能との判断を示し,キャッシュカードの磁気ストライプ部分の記録についての文書性が認められた.

4.4 銀行オンライン・システムを悪用した犯罪

銀行オンライン・システムの悪用にもいろいろある.キャッシュカード犯罪もこの範疇に入るが,ここではそれ以外についてのべてみたい.この種の典型的な事件としては,三和銀行事件がある.

三和銀行事件は,1981年に発生した事件で,同行茨木支店のオンライン端末機のオペレータである女子行員が,外部の愛人と共謀して犯したものである.この女子行員と愛人は,あらかじめ大阪と東京の同行支店に架空名義の口座を開設した.

3月25日,午前10時頃,女子行員は,架空口座につぎのとおり合計1億8,000万円のニセ入金を操作した.

- 吹田支店(大阪) 鈴木啓一名義口座, 3,000万円
- 豊中支店(大阪) 佐々木健一名義口座 3,000万円
- 新橋支店(東京) 鈴木吉男名義口座 6,000万円
- 虎ノ門支店(東京) 佐々木武雄名義口座 6,000万円

10時半頃,女子行員は,上司に歯医者に行くといって外出し,その足で預金引き出しに向っている.引き出したのはつぎの通り.

- 吹田支店　2,500 万円
- 新橋支店　500 万円　　保証小切手 4,800 万円
- 虎ノ門支店　2,000 万円

保証小切手　3,200 万円

そして，その後，マニラへと逃亡した．この事件で注目すべき点は，入金操作の 1 億 8,000 万円という金額である．おそらく，エラーに見せかけようとした可能性が強いし，銀行側はエラーと思い込んでいたため手配が遅れたと見られている．つまり，2,000 万円入力するのに，ゼロを 1 つ多く間違えると，2 億円になり，実際の数字 2,000 万円との差である 1 億 8,000 万円が宙に浮くことになる．したがって，食い違いの数字が 9 の倍数で出てくると，発見した人もエラーではないかと思いがちである．エラーだと思い込んでくれると，犯人としては時間かせぎが出来ることになる．この女子行員は，エラーと見せかけるために，目標が 1 億円であれば 9,000 万円を，2 億円なら 1 億 8,000 万円を，3 億円なら 2 億 7,000 万円をというように，9 の倍数でニセ入金操作をしたものと思われる．

4.5 マシンタイムをめぐる犯罪

わが国におけるマシンタイムの盗用事件は，1981 年の岡山大学事件のみである．

この事件では，マイコン・ショップに対して刑事責任は問われていない．当事者間において解決がはかられている．これが，米国であればかなり異なってくる．米国は，コンピュータ犯罪防止法への取り組みが進んでいる．連邦法は成立していないものの，州レベルではコンピュータ犯罪防止法を成立させているのがすでに 20 州を超えている．内容的には，州によって多少異なるが，一般的には，「財産」と「サービス」を明確に定義して，これらを不法領得・破壊・侵害する者を処罰するのがコンピュータ犯罪防止法といってもよい．そしてサービスには，「コンピュータ・タイム」が明記される例が多く，わが国の岡山大学事件もこれに該当している．

たとえば，アリゾナ州刑法典第 13-2310 条[5] では，サービスをつぎのように，「サービスには，コンピュータ・タイム，データ処理および記憶機能を包含する」と定義している．カリフォルニア州刑法典第 502 条[6] では，財産をつぎのように，「財産には，人間ならびにコンピュータ・システム双方が読むことのできるデータおよび伝送中のデータを含め，有体であると無体であるとを問わず，商業証券，データ，コンピュータ・プログラム，コンピュータ・システムおよびコンピュータ・プログラムに関連する資料，またはそれらのコピーを包含するが，それらに限定されない」と定義している．

5. コンピュータリスク・マネジメントの概念

コンピュータリスクには，エラー，コンピュータ犯罪，事故，災害，プライバシ侵害等々がある．これらのコンピュータリスクをいかにマネージするかが重要な課題となる．しかも，コンピュータ・システムには莫大な資金がかかり，あらゆる業務を処理するようになり，ネットワークは広がり，実際にエラーや事故などが発生すると，その影響力は実に大きくなってきている．

コンピュータリスク・マネジメントを構成するのは，まず，コンピュータ部門自体の安全対策を充実させ，つぎに，それらに対する客観的な立場でのシステム監査人によるチェック・評価，つまりセキュリティ監査，そして，不幸にしてエラー・事故・コンピュータ犯罪等が発生して損害を蒙った場合のコスト面の補塡という面からの保険の付保ということができよう．また，これらをうまく行うためには，事前のアセスメント，つまりリスク・アナリシスを実施する必要がある．

5.1 リスク・アナリシス

まず，どのようなリスクが想定されるか，その影響

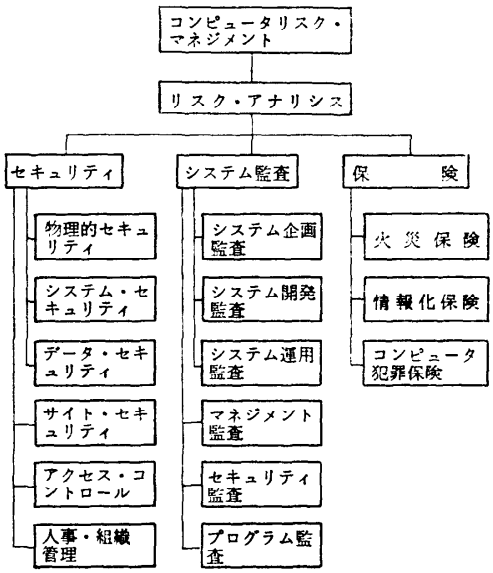


図-1　コンピュータリスク・マネジメントの概念

度はどの程度か，リスクからコンピュータ・システムを保護するためにはどうしたらよいのか等を検討し，つぎに，どの程度の保護策を講じるべきかを決めなければならない．

そして，検討すべき基本的な事項をあげるとすれば，つぎの4点ということになろう．

①潜在的なリスクとしては，どのようなものがあるか．
②それらのリスクが顕在化した場合，どの程度のダメージを蒙るか．
③コストとの関連でどの程度の保護策を講じるべきか．
④保護策でカバーできない部分についてはどうするか．

5.2 セキュリティ

コンピュータ・セキュリティは，コンピュータ部門自体の仕事である．建物や設備，コンピュータ・システム，データなどを安全に保つことが必要である．見方をかえれば，コンピュータ・システムの設置場所を安全に保護し，建物やコンピュータ・システムやデータ等への接近をコントロールし，要員の管理を適正に行って安全性のレベルを高める努力が必要である．

5.3 システム監査

コンピュータ部門自身で進めているセキュリティ対策が，安全性を確保するのに十分であるかどうかを，独立かつ客観的な立場のシステム監査人が検討・評価する必要がある．重要なことは，システム監査人がセキュリティ対策をつくるのではなく，あくまでもセキュリティ対策の状態を監査し，問題点があれば改善勧告を出すなどして，セキュリティ対策の改善に寄与することである．

5.4 保 険

保険としては，最も基本的には火災保険があり，コンピュータ関連の保険としては情報化保険とコンピュータ犯罪保険がある．情報化保険は，コンピュータ関連機器類や情報メディア等に発生した事故による損失を補塡するコンピュータ総合保険と，情報処理業者が顧客に与えた損失を補塡する情報処理業者賠償責任保険とがある．コンピュータ犯罪保険は，財産保険，信用保険とともに，金融機関包括補償保険を構成している．

6. おわりに

今日，情報技術（処理技術，伝達技術，利用技術，管理技術等）の発達はめざましく，現時点では限界に達する徴候を見せてはいない．今後とも，新しい情報技術を導入した方式が出現すると，必ずといってよいほど新しいリスクが伴っているということになるであろう．したがって，コンピュータ犯罪は，これまでよりも，これからの方が問題である．

わが国の情報処理をとりまく環境で，今後コンピュータ犯罪をめぐって大きな脅威になる可能性を秘めた事柄は，つぎのような点であろう．

- ネットワークの拡大
- データベースの発達
- OA 化の進展
- 個人データ蓄積の量的拡大
- パソコン少年の社会への流入

これらは，いずれも豊かな生活を求める高度情報化社会へのステップとして欠くことのできないことであろう．必要なことは，十分な事前のアセスメントを実施すること，技術的・管理的な安全対策の充実をはかることである．一方では，“人”の問題，“心”の問題としての処方箋が大切であることを忘れてはならない．

とくに，学校教育においては，コンピュータの使い方だけを教えて情報化教育だといわれたのでは問題が多く，情報化社会に対応した人間教育とでもいうのが，“情報化倫理”なども重要になろう．いずれにしても，“社会に出る前”の教育についても考えてみる必要がある．また，別の観点からは，大学において情報処理教育が相当に進んでいるのに，“コンピュータ・セキュリティ論”，“システム監査論”という講座が開設されたという話を聞いたことがない．根本的には，ここらから手をつける時期にさしかかっているように思われる．

参 考 文 献

1) 健全なる情報化社会の構築に向けて，通産省，コンピュータ・セキュリティ研究会，p. 51 (1982)．
2) 昭和58年版警察白書，警察庁編，p. 7 (1983)．
3) 1)に同じ，p. 60.
4) 1)に同じ，pp. 53-57.
5) 世界コンピュータ年鑑，日本情報処理開発協会編，p. 137 (1982)．
6) 5)に同じ，p. 138.
7) Parker, D. B.: Crime by Computer, Charles Scribner's Sons, 1976 (邦訳：コンピュータ犯罪，羽田三郎訳，秀潤社 (1977))．
8) Whiteside, T.: Computer Capers-Tales of Electronic Thievery, Embegglement, and Fraud, Harper & Row, Publishers, Inc., 1978 (邦訳：コンピュータ犯罪—恐るべきアメリカ，湯沢章伍訳，講談社 (1982))．

(昭和59年1月27日受付)