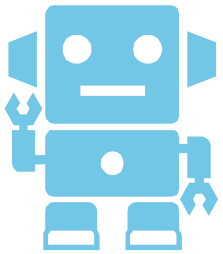
Deloitte.
デロイト トーマツ

これまでとこれから

2016年05月19日

デロイト トーマツ リスクサービス株式会社
代表取締役社長
丸山 満彦



本日のお話は・・・

サイバーセキュリティの問題の本質は何か

サイバーセキュリティ対策を更にしなければならないといわれ続けているが、何が変わっているのか？

20年以上前を振り返りながら、考えてみたいと思います。

私が社会人になったころ

仕事についた1992年当時は
汎用機の時代であったがセキュリティ問題は当然にあった

会社（Client）の状況

IBMの汎用機を用いて会計、販売、生産管理を行っていた。

ハード　System370

OS　MVS（Multiple Virtual Storage）、
　大規模：**VM**（Virtual machine）
　中規模：VSE（Virtual System Environment）

言語　Assembly言語、COBOL

ミドルウェア
　トランザクション処理：**CICS**（Customer Information Control System）

Database
　階層型：**IMS**（Information Management System）
　リレーショナルDB：DB2、Informix

文字コード　**EBCDIC**

端末 3270端末（一部エミュレータ端末）

汎用機用のセキュリティソフト

セキュリティ

RACF（Resource Access Control Facility）

　1976年にリリースされた

ACF2（Access Control Facility）

　“Protect by Default”が基本設計思想

Top Secret

　“Roll based Access Control”

仕事についた1992年当時は
汎用機の時代であったがセキュリティ問題は当然にあった

会社（Client）の状況

IBMのオフコンも会計、販売、生産管理で使われていた。

ハード　AS/400

OS　OS/400

Database　DB2

端末　5250端末（一部エミュレータ端末）

QSECURITY 30で出荷されていた時代だったような気がする

ハード　RS/6000

OS　AIX

X Windows System とX端末

UNIXは様々なFlavorがあり監査では苦労した

BSD系

BSD, SunOS

System V

Solaris, HP-UX, (AIX)

仕事についたころのパソコンの環境

日本語Notebook

ハード　NEC PC-9801 NS/L

CPU i386SX-20MH

HD 30MB

Memory 1.6MB

Display 640*480 VGA 8.9inch 白黒8段階

OS MS-DOS3.3D

文書ソフト　新松　FEP　松茸

スプレッドシート　Lotus1-2-3

Database dBaseIII

http://www.pc-98.jp/htmls/1800000003990-9.html

仕事についたころのパソコンの環境

英語Notebook

ハード　Toshiba T5200

CPU Intel 80386/11MHz

HD 100Mb

Memory　4MB

Display 640*480 VGA 13inch

OS MS-DOS/V 5.0

文書ソフト　WordPerfect, WordStar

スプレッドシート　Lotus 1-2-3, Microsoft Multiplan

http://www.computinghistory.org.uk/det/1342/Toshiba-T5200-100/

セキュリティに関連する日本の基準

電子計算機システム安全対策基準

通商産業省が**1977年**に策定した。

1984年と1991年に改訂され、1995年に情報システム安全対策基準となった。

http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm

当時は、
(1)設備基準（95項目）
(2)技術基準（19項目）
(3)運用基準（48項目）

であった。

システム監査基準

通商産業省が**1980年**に策定した。

1996年に改訂され、2004年にシステム管理基準となった。

http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm

1996年改正当時の構成は次の通り。

(1) 一般基準（９項目）

一般基準は、システム監査において基本となる監査計画及びシステム監査人に求められる要件等の原則を定めている。

(2) 実施基準（191項目）

実施基準は、システム監査の対象である情報システムの企画、開発、運用及び保守業務並びに共通業務に対する監査項目を定めている。

(3) 報告基準（８項目）

報告基準は、システム監査の結果をとりまとめるに当たっての必要事項及び結果に基づく措置を定めている。

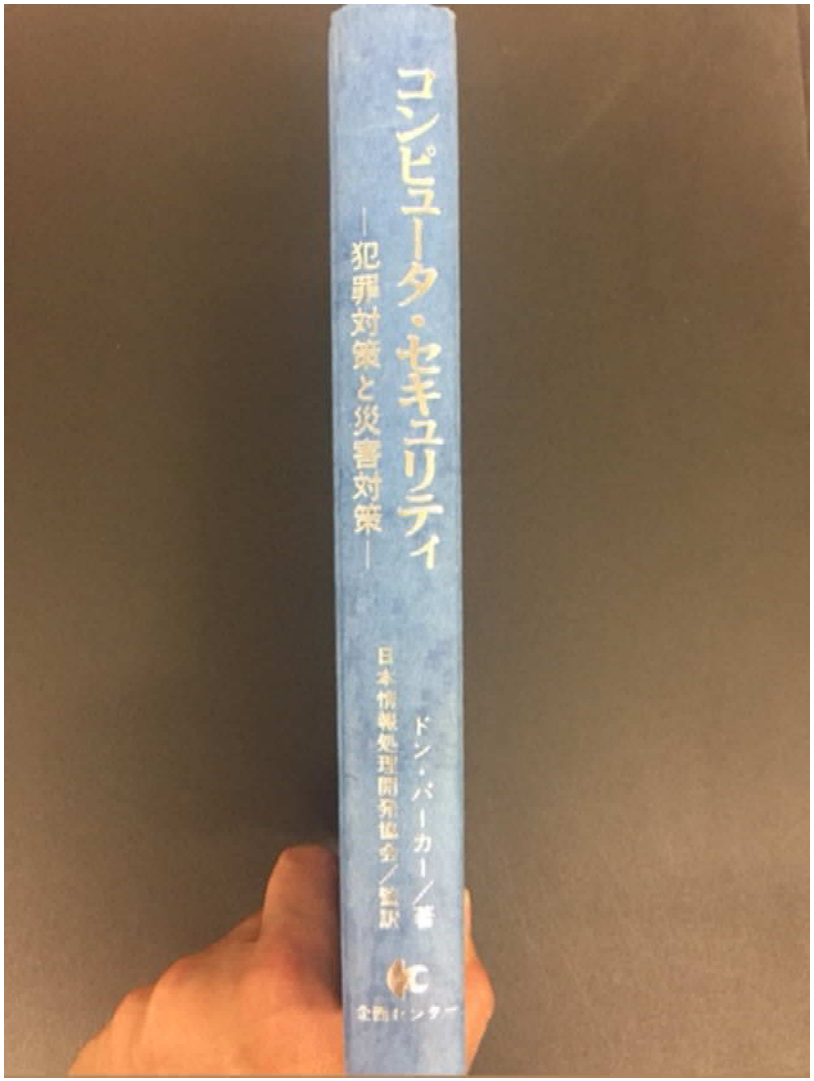
http://www.meti.go.jp/policy/netsecurity/systemauditG.htm

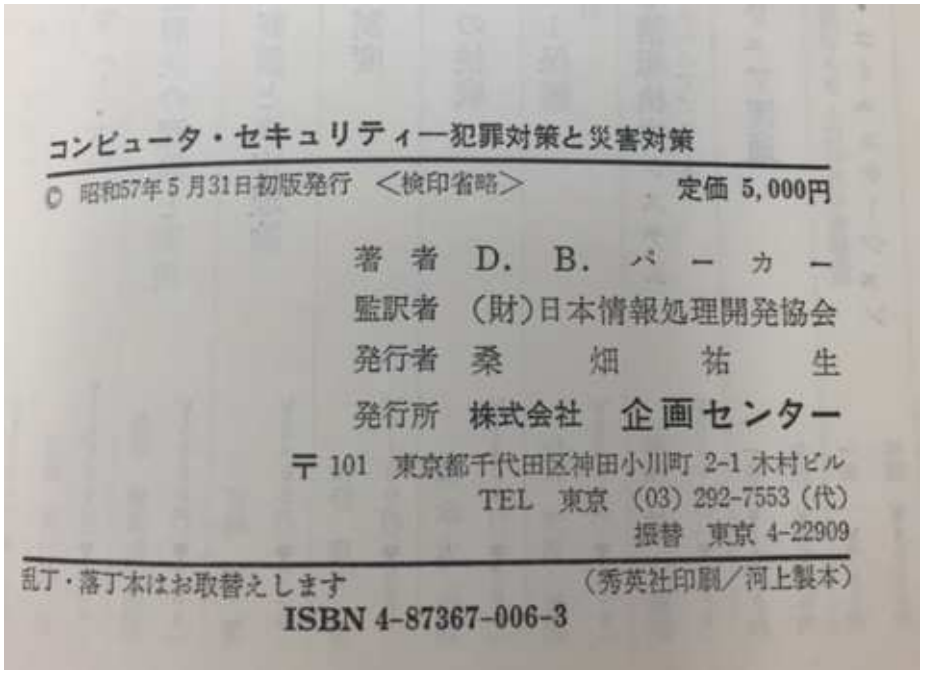
今から35年前の1981年に何が書いているか？

コンピュータ・セキュリティ
犯罪対策と災害対策

コンピュータ・セキュリティ　犯罪対策と災害対策

昭和57年(1982年）発行だが、原著は1981年に出版されている





まず、通商産業省の「推薦の言葉」を読んでみましょう

コンピュータ・システムの導入を中核とする情報化の推進は、経済活動を高度化するとともに、多様で豊かな社会を実現し、「活力とゆとり」のある社会を形成していくために極めて重要である。特に、いわゆる「資源小国」として食料、資源、エネルギーなどの基礎物質に乏しいわが国が、経済・社会の安定的発展を維持していくために情報化は不可欠のものといえる。

他方、このような社会にあっては、コンピュータ・システムには膨大な情報が集積され、経済・社会の中枢神経としての機能を有してくることとなり、これが何等かの要因によってその機能を停止したり、混乱が生じた場合、その影響は計り知れない広がりと深さを持つことになる。

昭和52年4月に電子計算機システム安全対策基準

昭和56年7月には情報処理サービス事業者を対象とした安全対策実施事業所の認定制度を発足

健全な情報化社会の形成のためには、コンピュータ・システムのセキュリティ確保のため、あらかじめ総合的かつ十分な対策を講じておくことが必要である。通商産業省においては、その一環として、昭和52年4月に電子計算機システム安全対策基準を策定・公表するとともに、昭和56年7月には情報処理サービス事業者を対象とした安全対策実施事業所の認定制度を発足させたところである。

本書は、米国のコンピュータ犯罪の権威であるドン・パーカー氏のまとめられたものであるが、わが国においても今後ますます情報化が進展するにあたって、このようなセキュリティ・ハンドブックをよき参考書として、わが国における電子計算機利用の正しい理解がより深められることを期待する次第である。

1982年4月

通商産業省　機械情報産業局情報処理振興課長

広瀬　勝貞

（おまけ）広瀬勝貞氏のその後　（Wikipediaより）

初代経済産業事務次官に

大分県日田市生まれ。麻布高等学校、東京大学法学部卒業。1966年、通商産業省に入省。石炭局、貿易局、大臣官房秘書課を経て、1976年より外務省に出向し、在スペイン日本大使館に赴任。帰国後は本省勤務の他、中小企業庁や資源エネルギー庁への出向も経験する。1991年、宮澤喜一内閣総理大臣の秘書官に就任。宮澤の退陣後は通産省へ戻り、貿易局長、大臣官房長、機械情報産業局長を経て、1999年9月より通商産業事務次官に就任。2001年の中央省庁再編に伴い、初代経済産業事務次官に就任した。2002年2月に退官。

大分県知事として

2003年、通産省時代の先輩にあたり、1979年から6期24年にわたり大分県知事を務めていた平松守彦から後継指名を受け、大分県知事選挙に無所属（自民・公明・保守3党推薦）で出馬。当初、現職の平松知事の後継指名に加え、地元経済界や業界団体の支援も受けていたため圧勝が予想されていたが、「無党派」を標榜し平松県政からの転換を訴えた吉良州司（のち民主党衆議院議員）の猛追を受けて苦戦を強いられ、3万票弱の僅差で吉良を振り切って初当選した。2007年、2011年の大分県知事選では日本共産党以外の政党は候補者を擁立せず、広瀬自身も表立って政党の支援は受けず、対立候補に大差をつけて再選された。

ドン・パーカーの「まえがき」を読んでみましょう

本書の構想は、私がコンピュータ・セキュリティ研究所のジョン・オマラ氏からセキュリティのハンドブックを書くよう依頼を受ける前から温めていたものである。当初、基本的な問題、概念、理論、最終的な実践までを取り扱った教本を考えていたが、執筆を続けているうちに次第にハウ・ツーもののハンドブックを指向した専門書になった。私がコンピュータの不正使用に関する研究を始めてから既に11年を経ているが、常にその目的とするところは、セキュリティによって解決すべき問題を明らかにしつつ、いかにセキュリティを高めるかにあった。本書は、こうした研究の成果を踏まえて完成したものである。

11年間の研究とコンサルティング活動を通じて１つの結論を出すとすれば、コンピュータ・セキュリティは人間の心理と社会環境に関するものであって、決して技術的な問題ではないということである。私が世界各地で行っている講演で繰り返して述べていることであるが、コンピュータそれ自体は、怠慢でもなければ誤りとか犯罪を犯すものではない。コンピュータが次々と明らかにするこうした事実は、まさに人間だけができることなのである。したがって、問題を解決する糸口は、人間自身、彼らの行動・態度にある。これらの概念については、本書でしばしば強調している。

（略）

ドン・パーカー

コンピュータ・セキュリティは人間の心理と社会環境に関するものであって、決して技術的な問題ではないということである。

→

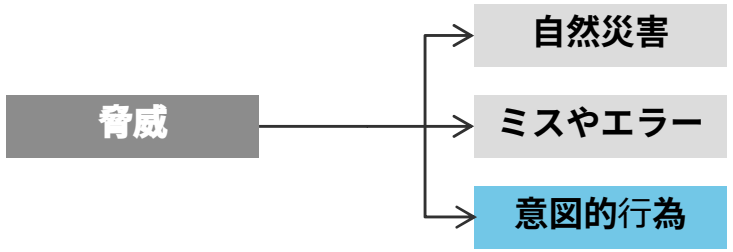
問題を解決する糸口は、人間自身、彼らの行動・態度にある。

「序」を読んでみましょう。

より完成された社会においては、コンピュータ・セキュリティは、本やマニュアルにまとめて掲載されている「なすべきこと」と「してはならないこと」の限界を定めたリストを適用することによって容易に達成できるだろう。しかし、残念ながらコンピュータ・セキュリティは、それほど単純なものではない。コンピュータ・セキュリティは、3種類の基本的脅威から資産を守り、その損害をできるだけ少なくしようと勤めることにある。つまり、自然災害（例えば異常気象）、人が起こすミスとかエラー（例えば、誤ったテープのラベリング）、詐欺やサボタージュなどの意図的行為の3種である。最初の２つの脅威については今までの経験から予測することができる。私達はまた、どうすればこうした脅威を防ぎ、被害の程度を抑えることができるか、さらに損害を最小限に食い止めるにはどうすればよいかを経験から知っている。多くの良識と試行錯誤の繰り返しによって、料理の本にみられる「こうしなさい」「こうしてはいけません」方式のチェック・リストによるアプローチをこうした特定の分野に注意深く適用することも大いに効果があるだろう。しかし、後にも述べるようにコンピュータ・システムそのもののセキュリティについては、この限りではない。

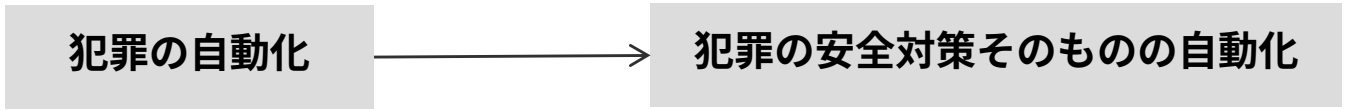
意図的な脅威に対しては、現在使用されている「料理の本」方式のアプローチでは不充分である。犯罪に対する戦いの悲しむべき歴史が、伝統的な方法では不充分であることを証明している。明らかな弱点を強化しようとするあまりに他を無視してしまう、いわゆる「マジノ曲線」現象は、犯罪者に対し、強化した線を避けて防備の不充分な所から攻撃をかけることを容易にさせるのである。犯罪者は、資産を守ろうとする者と同じように安全対策を熟知しており、その裏をかこうとするのである。

意図的な行為によって生じる損害に対しては、別の方法を考えなければならない。チェック・リストだけでは不充分である。IBM社のデータ・セキュリティの専門家のロバート・コートニーは既に800以上のチェック・リストを集め、今なおその収集を続けているが、そのほとんど全てについて欠点があることを指摘している。こうした欠点が極めて数多く発見されることもあって、たとえルーズリーフのバインダー形式であるにせよ、それを出版すること自体大して役に立つとは思えない。



SRIインターナショナルが実施している10年間にわたるコンピュータ犯罪の研究においても、新しい形態の意図的行為が続々と表れているのである。こうした行為は、昔からある詐欺、窃盗、横領、サボタージュ、スパイ、ゆすりなどと同じ犯罪である。しかし、犯罪にコンピュータが関係してくると、昔からの犯罪も新しい性格を持つことになり、その結果、全く新しい形態の犯罪となるのである。資産の保管、処理を自動化したことによって、新しいタイプの犯罪者、新しい犯罪環境と目標を作り出したのである。言い換えれば、データ処理が伝統的に犯罪が起こっていた環境に近づくにしたがって、犯罪も今や自動化されてきたのである。

こうした犯罪の自動化は、伝統的なセキュリティの専門家、法執行者、検察を当惑させるようになった。これと同時に、犯罪の環境とかプロセスの自動化は、犯罪に対する安全対策そのものを自動化する新しい機会を生み出すことにもなった。自動化は、犯罪に対する安全対策そのものを自動化する新しい機会を生み出すことにもなった。自動化は犯罪による猛攻撃を受けても生き残ることができるだろうか。歴史上始まって以来のセキュリティの自動化は、果たして資産とか情報に対する犯罪をコントロールできるだろうか。このようなコントロールを達成するためには、システムとオペレーション分析に対する自動化の方法も矛盾しない新しいセキュリティの方法論が採用されなければならない。



SRIでは、コンピュータの不正使用による新しい事件と自動化された分野での犯罪の研究を通じて、コンピュータに関連するあらゆる種類の損害の問題に対処する新しい方法を開発した。コンピュータ・セキュリティに関した多くの本に記されているチェック・リストの中から、安全対策を選び出すという伝統的な方法は、人によるエラーやミスに対しては効果的である。しかし、チェック・リストによる方法は、故意に犯罪を犯そうとする知能犯に対しては効果がない。つまり、私達の敵となる犯罪者は、私達と違ったチェック・リストを使っているのである。換言すれば、コンピュータ犯罪を犯そうとする者は、公開されたチェック・リストには出ていないシステムの弱点に気づいているのである。したがって、コンピュータ・セキュリティの専門家は、犯罪を犯そうとする者と同程度の創造性を持っていなければならない。犯罪を犯そうとする者とコンピュータ・セキュリティの専門家との間でゲームをしていると考えるのも良いだろう。しかも、このゲームのルールは、セキュリティの専門家ではなく犯罪者によって作られるのである。この方法では、経験と敵の役割を演じることによって脅威のシナリオを開発し、使用することが必要である。

コンピュータ・セキュリティの専門家は、犯罪を犯そうとする者と同程度の創造性を持っていなければならない。

こうしたアプローチには、多くの利点がある。つまり、多くの面で極めて柔軟性に富んでいることから、非現実的で効果の少ない「料理の本」式の方法を使わなくてもすむわけである。この方法は、いかなる規模とかタイプのコンピュータ・システム（ここでは、要員、設備、ハードウェア、ソフトウェアを含めて大規模なものを指す）にも適用が可能である。コンピュータ・セキュリティについての議論の多くは、大規模システムに適した安全対策の推奨について行われているが、一般的にはこれを小規模システムにスケール・ダウンすることはできない。例えば、役割ごとに責任を明確に分担することは小規模システムにおいては困難である。また他の方法においては、セキュリティ計画のための無制限の資源と、推薦された安全対策の使用の義務付けを前提としているが、私がここで提案している方法を用いれば、いかなる予算でもその希望に応じて実行することができる。したがって、以前はほとんど何の安全対策も施されていなかった領域においてさえ、この方法をセキュリティの計画と実施のために使用することできる。また、監査のために使うこともできれば、これによって保護の度合いを高めることもできる。

経験と敵の役割を演じることによって脅威のシナリオを開発し、使用することが必要である。

しかし、いくつかの欠点と問題点があることも認識しておく必要がある。

最初に言っておかねばならないが、ここで提案された方法は決して広い範囲にわたってテストされたわけではない。この方法は、３種類のアプリケーションを用いて2年以上かけて開発されたものであり、この本の中で示しているような理想的な形で実施されてはいないものの、結果的には満足のいくものであった。開発においては、セキュリティ計画及びセキュリティの調査に多くの経験を持つSRIのコンピュータ・セキュリティ担当者がテストを行った。最も重要なことは、この方法が被害者、犯人、実際の損害に関連した種々の問題などに関する豊富な経験と知識に基づいていることである。こうした情報は、現実的、実際的な脅威におかれた情況を予想するのに大きな助けとなる。このことはまた、経験を持たないコンピュータ・セキュリティの専門家にとっては、シナリオ作りをすることが困難であることを示している。事実、この方法の成功は、多くの実際の経験に基づいているのである。

これに対して批判する人の中には、潜在的脅威を全て考慮したシナリオは膨大なものになり過ぎると言うかもしれない。しかし、シナリオは一般化することによって必要とされる数を減らすことができるうえ、たとえそうしても「料理の本」方法よりもより包括的に脅威を取り扱うことできる。この脅威のシナリオによる方法は、経験を積んだEDP監査人が、コントロールや安全対策を評価する際に１人でシナリオを考えている場合とそれほど違うものではない。この本で述べていることは、このプロセスを形式化しただけであって、それによってシナリオによる方法を分り易くしたものである。

読者の中には偶発的事故に比較すると、意図的行為に損害が必要以上に強調されていると考え方があるかもしれない。いずれにしろ、意図的行為によるより、偶発的事故による損害の方がはるかに大きいのは衆目の一致するところである。また、著者の研究の中心がコンピュータ犯罪であるところから、今回の議論が読者をそれほど重大ではない問題の方に導いてるかもしれない。一方、コンピュータ・セキュリティに関する本を書く場合に悩む共通の点は、この問題があまりにも広範囲であるため、著者がセキュリティの全ての分野について十分な判断を下せる専門家たり得ないことである。ある本は、データベース・マネジメントのセキュリティについて、また別の本では物理的なセキュリティについて入念な記述をしたという具体になるのである。また、著者が包括的にこの問題を扱うよう要求されても、ある種のトピックスはやむを得ず背景の中に取り残されてしまうかもしれない。

**コンピュータ・セキュリティの問題が
あまりにも広範囲であるため、
セキュリティの全ての分野について
十分な判断を下せる専門家たり得ない**

　このような点を考慮すると、私は読者にこの本が自然災害、保険、オペレーティング・システムのセキュリティ、その他について、表面的にしか触れていないことを断っておかねばならない、なお、この本では、いくつかの新しいコンピュータ・セキュリティ概念について、かなり広範囲に取り上げており、また偶発的事故と意図的な行為を別々のもの（論争の的になっている考え方であるが）として取り扱っている。脅威とリスク分析の方法及びコンピュータ・セキュリティの職能の構成方法については、充分な検討が加えられている。このほか、セキュリティの調査検討の実施方法、包括的と言うより選択的な計量的リスク・アセスメント、安全対策の原則について詳細な検討を行った。

**偶発的事故と意図的な行為を別々のものとして
取り扱っている**

この本は、エラーやミスというより、むしろ意図的な行為に対するセキュリティに焦点を当てている。この理由については、この本の中でも充分な説明を行った。これらの問題のうち、どれが主流となるかは誰にもわからないが、意図的行為によって生じる損害の対策を扱うことの方が挑戦のしがいがあろう。さらに、偶発的事故に備えただけでは、意図的行為による損害の備えにはならないが、意図的行為の対策にわずかな費用を加えるだけで偶発的事故に対する備えになると私は確信している。この関係は、一方向のみで双方向というわけには行かない。

この本を読む際には、私の偏見、限界について考慮してもらいたい。読者にとっては、かならずしも私の概念、結論、強調したい点に合意できないかもしれないが、私はこの本が読みがいのある刺激的案ものであることを保証したい。

**偶発的事故に備えただけでは、
意図的行為による損害の備えにはならないが、
意図的行為の対策にわずかな費用を加えるだけで
偶発的事故に対する備えになる**

目次を見てみましょう

第Ⅰ編 コンピュータ・セキュリティと組織

第1章 セキュリティに係わる問題

- 1.1 変遷するセキュリティのニーズ
- 1.2 コンピュータ・セキュリティの問題
- 1.3 自動化を指向する犯罪

第2章 組織に対して重要な力を発揮するEDP

- 2.1 情報は力なり
- 2.2 情報システムの形態

第3章 コンピュータ・セキュリティと組織構造

- 3.1 EDP活動
- 3.2 その他の部門
- 3.3 セキュリティ政策

EDP = Electronic Data Processing

目次を見てみましょう

第Ⅱ編 コンピュータ・セキュリティの性質

第4章 概念と定義

- 4.1 セキュリティの定義
- 4.2 リスク回避
- 4.3 資産
- 4.4 脅威
- 4.5 偶発的事故と意図的行為の特徴
- 4.6 損害の確率への理論的アプローチ
- 4.7 セキュリティ戦略
- 4.8 偶発的事故と意図的行為の防止例
- 4.9 保護のレベル

第5章 セキュリティの機能

- 5.1 セキュリティの次元
- 5.2 セキュリティの優先順位
- 5.3 セキュリティ機能に対する資源の割付
- 5.4 抑制機能
- 5.5 防止機能
- 5.6 検知機能
- 5.7 回復と訂正

第6章 コンピュータ・セキュリティの組織

- 6.1 組織の機能
- 6.2 代替できる報告関係
- 6.3 EDP監査の組織
- 6.4 コンピュータ・セキュリティ機能の組織化
- 6.5 セキュリティ情報ファイル

第7章 コンピュータ・セキュリティと法律

- 7.1 プライバシー
- 7.2 海外不正取引防止法
- 7.3 州コンピュータ犯罪法
- 7.4 連邦犯罪法
- 7.5 コンピュータ・セキュリティ法のインパクト

第III編 コンピュータ・セキュリティ・プログラム

第8章 開始
- 8.1 方法論
- 8.2 対策本部の組織
- 8.3 セキュリティ評価の範囲
- 8.4 プロジェクト計画

第9章 資産の識別と査定
- 9.1 資産の移動によるリスクの回避
- 9.2 資産の識別
- 9.3 もっとも重要な資産
- 9.4 資産の査定
- 9.5 デルファイ法
- 9.6 その他の資産に関する問題

第10章 脅威の識別
- 10.1 脅威の除去によるリスクの回避
- 10.2 組織内で発生した損害
- 10.3 組織外で発生した損害
- 10.4 脅威のモデル

第11章 リスク・アセスメント
- 11.1 コートニーのリスク・アセスメント
- 11.2 危険度分析
- 11.3 危険度分析のケース・スタディ
- 11.4 シナリオ分析
- 11.5 シナリオのケース・スタディ
- 11.6 アンケート調査法
- 11.7 実際的なリスク・アセスメント

第12章 安全対策の識別、選択、実施
- 12.1 安全対策の識別
- 12.2 安全対策の選択原則
- 12.3 監査用ツールとテクニック
- 12.4 EDPコントロール
- 12.5 勧告
- 12.6 勧告の幹部への売込み
- 12.7 実施及び進行中のプログラム
- 12.8 コンピュータ・セキュリティの特質

附録

A. 業務活動の原則

B. データ処理組織の行動基準

C. 連邦コンピュータ犯罪法

D. コンピュータ犯罪の方法

E. 危険度分析のためのEDP職務の内容

F. EDP監査ツール及びテクニック

G. EDPコントロール

H. シナリオの例

第 I 編 コンピュータ・セキュリティと組織

第1章 セキュリティに係る問題

1.1 変遷するセキュリティのニーズ

有名な銀行強盗ウィリー・サットンに、なぜ銀行に押し入ったかを尋ねれば、「そこに金があったからだ」と答えたはずである。今後は、不当な利益を得るためにコンピュータ、電気通信システムに焦点を合わせたアマチュアのホワイト・カラーやプロによる犯罪が増加するだろう。コンピュータに関するセキュリティ、監査、管理機構も大幅にかわりつつある。

　初期のコンピュータ技術者は、コンピュータは比較的安全な環境の下にあると考えていた。彼らが考えなければならなかったのは、エラーやミス、そして自然災害から生じる偶然的事故による損害であった。EDPをとりまく環境において、偶発的事故や意図的行為による損害を受ける可能性が大きくなるにしたがって、EDP部門の管理者は、今まで以上に保護対策に対する責任が大きくなってきている。この分野で先進的な組織は、既にデータ処理部門でEDPセキュリティの専門家を養成しており、同様にEDP監査の専門家を養成しているところもある（これらの専門家はデータ処理部門の最も高いレベルの管理者として報告されてはいるが、通常は監査部門に入れられる。）

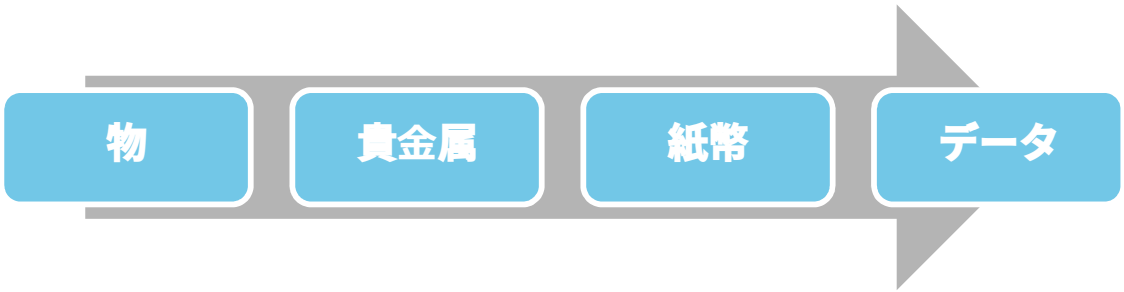
初期のコンピュータ技術者は、
コンピュータは比較的安全な環境の下にあると
考えていた。

データ処理部門で
EDPセキュリティの専門家を養成しており、同様に
EDP監査の専門家を養成しているところもある。

1.2 コンピュータ・セキュリティの問題

技術が進むにつれて、その技術を行為のよる損害から守るために必要とされる機能の開発は次第に困難となってきた。この理由の１つは、今日の複雑なシステムを管理する人間の能力が限界に近づきつつあるからである。

意図的行為による損害の基本的問題は、流通性のある資産をどのように保護するかにある。



流通性のある資産の変遷

1.3 自動化を指向する犯罪

ビジネスにおける犯罪が金があるところを狙うとするなら、現在では、間違いなくコンピュータ及び電気通信システムということになるだろう。

1960年前半になって、企業の経営者達もコンピュータ・プログラムも貴重な企業の資産として保護し、コスト評価を行う必要があることを認め始めた。

1960年前半になって、
企業の経営者達も
コンピュータ・プログラムも
貴重な企業の資産として
保護し、コスト評価を行う必要がある
ことを認め始めた。

犯人が十分な技術的能力、知識、手段、才能を持っている場合には、ユーザの組織を意図的行為による損害から防ぐ有効な技術的手段を備えているとはいえない。犯人となるのに充分な能力を備えた人の数は急激に増加し続けている。さらに、今日の多くのコンピュータは、公衆電話網によって接続されており、このためシステムには新しい技術が付加される一方、弱点も付け加えることになった。このような状況の下では、私達はシステムの完全性を証明しそれを維持することはほとんど不可能である。今まで述べてきたことがこの本が書かれた背景である。私はこの本が、EDPセキュリティ及び監査の発展の一助となり、こうした分野に関係する方々が急速な進歩を見せる技術に対応し、高度で複雑なシステムの利用に充分フォローしていけることを念願してやまない。

システムの完全性を
証明しそれを維持することは
ほとんど不可能である

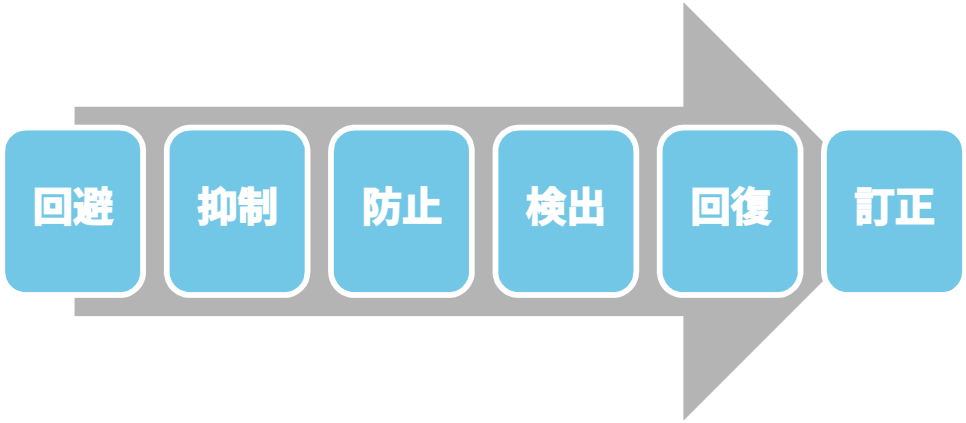
第II編 コンピュータ・セキュリティの性質

第4章 概念と定義

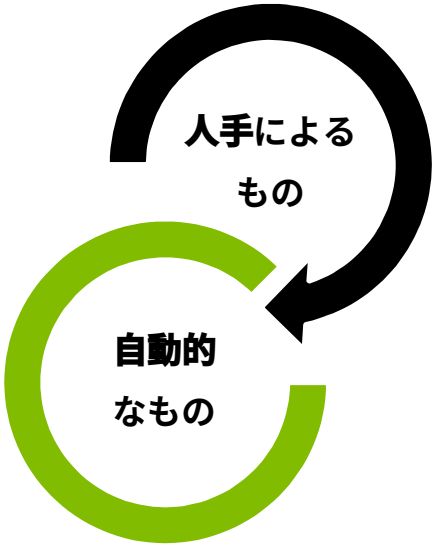
4.1 セキュリティの定義

辞書によるセキュリティの標準的な定義では、“危険、恐怖、不安、不確実性、経済的不安定などからの解放”となる。

セキュリティは、 回避、 抑制、 防止、 検出、 回復、 訂正の６つの機能からなっている。



安全対策には、自動的なものと、人手によるものがある。マニュアルによる安全対策は、1人もしくはそれ以上の権限を与えられた人によって常に正しい状態を保つことが要求される。一方自動的安全対策は、開始、停止、監視、検査、補給を除けば人の介在なしに機能する。



第4章 概念と定義

4.3 資産

守るべきものが何かを識別することが、組織を損害から守るためのステップである。

資産の例

- **データ処理要員**
- **コンピュータ・システム・サービス**
- **コンピュータ関連施設**
- **アプリケーション・プログラム及びドキュメンテーション**
- **データ**

・・・・

第4章 概念と定義

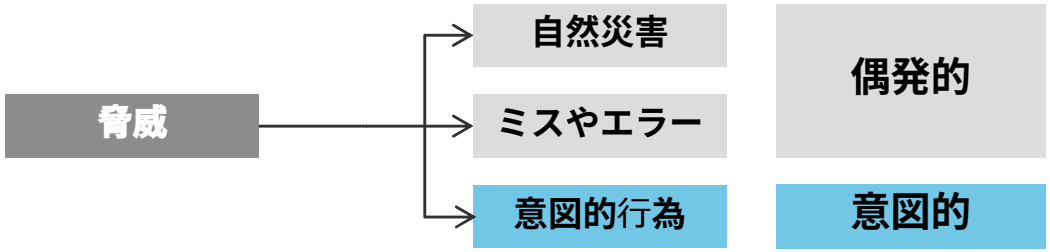
4.4 脅威

脅威とは、差し迫った望ましくない出来事の兆候である。

脅威は行為の類別に分類することもできる。自然災害、エラーとかミス、意図的行為の３つである。

保護が目的であれば、行為の類型は簡単に偶発的と意図的の２つに分けることができる。

セキュリティを改善するためのアプローチは、セキュリティの主要な２つの型、つまり偶発的事故と意図的行為の区別、そしてそれを別々の問題として扱うことについては、この章であきらかにしたい。個別の対応は、危険防止と保護には大きな効果をもつものの、損害を受けた後の回復にはほとんど役立たない。・・・２つの問題は平行して取り扱わなければならない。



２つの問題は平行して取り扱わなければならない

4.5 偶発的事故と意図的行為の特徴

(1)頻度

コンピュータ・サービスを行う組織におけるエラーとミスの発生は、損害事件の統計的分析が充分可能なほど頻度が高い。・・・エラーとミスの主な場所とソースを明らかにするための分析を行うことができる。また事故発生の統計データからは、確率とそれから予想される損害を計算することができる。

これとは逆に、意図的に引き起こされた損害は、発生率が低く統計分析が難しい。統計分析に足るほどの発生率を持つのは、クレジット・カードなどの支払業務における詐欺のような一部のケースに限られている。意図的行為の大半、特に重大な損害を伴うものはほとんど発見できないため、確率や損害の予想、性質、場所のパターン、ソースなどを明らかにすることは困難である。したがって、現時点で満足できる定量的なリスク分析はほとんど存在しない。

偶発的事故	意図的行為
頻度が高く、 統計的分析が可能な場合がある	発生確率が低く 統計分析が難しい

(3) 行為の複雑性

偶発的に生じる損害は、単一の孤立した行為から生じるもので、それぞれの事件は一般に他の損害事件とは関係ない。一方、意図的に引き起こされた損害は通常、連続した行為から生じたものである。また、エラーやミスに気付き、それに意図的につけ込んで損害を起こすこともありえる。多くの犯人は、発見や逮捕をさけるために、故意に意図的行為を複雑化しようとする。

偶発的事故	意図的行為
損害は独立した行為から生じる場合が多い	連続した行為から生じる

(4) 加害者の行動の複雑性

エラーとかミスを起こす行動は比較的単純である。行為の瞬間に係わるものであることから、行為の後その本人がせいぜいエラーの原因となった弱点を防護する必要性を感じる位である。一方意図的行為を行った人達の大半は、極めて複雑な行為をとる。意図的にコンピュータ犯罪を行った23人の者にインタビューを行った結果、特定のコンピュータ・システムや作業環境の脆弱な点を探すことよりも、まず個人の問題とか目標が先であると語った。システムの脆弱性を探したり調べたりすることは、意図的加害者が起こす複雑な行動パターンの一面にすぎない。システムに介入し、それを利用する目的さえ確認できれば、加害者は計画を立て、情報を集め、組織し、共謀し、そして最後に彼の全ての意図的行為を正当化するために都合のよい理由づけを行うことになる。効果的セキュリティを行うためには、これらの全ての点に注意を向けなければならない。

エラーやミス	意図的行為
比較的単純 行為の瞬間に係わる	複雑な行動をとる 計画的に行動をする

うけい

(8) セキュリティ・チェック・リスト

文献の多くは、チェック・リストを用いるか、あるいは料理のテキストのようなアプローチでコンピュータ・セキュリティを論じている。その戦略は、チェック・リストの中で、良く知られた安全対策とそれに対して用意されたコントロールを実施するという概念に基づいている。この方法は、特にエラーやミスを扱う場合には役立つが、意図的に引き起こされた損害に対しては充分ではないし、また有効でもない。犯人はチェック・リストを見て、容易に安全対策と立証されているコントロールを知り、それを回避するためにシステムに何らかの変更を加えるよう工夫する。したがって、単にチェック・リストの中で取り上げられた安全対策を導入するだけでは、意図的行為に対して充分な保護が達成されたことにはならない。こうしたチェック・リストが、安全対策自体を攻撃や破壊から守ることに必要なものや、そのための手段に関する情報を備えていることは稀である。

エラーやミス	意図的行為
チェック・リスト方式でもある程度対応できる。	チェック・リスト方式では不充分で有効ではない チェック・リストをみてそれを回避する。 安全対策自体を攻撃や破壊から守ることが必要。

(11) 保護のレベル

偶発的事故に対して安全対策が提供する保護のレベルは、行為と安全対策の1対１の関係から容易に決定できる。事故の発生率が高くなれば、損害の確率計算が容易になることは疑問の余地がない。一方意図的な行為においては、保護のレベルは発生する行為と保護すべき資産に関した安全対策の組合せを基に決定される。統計の不足が、有効性を決定するのを困難にしている。

偶発的事故	意図的行為
安全対策が提供する保護のレベルは、行為と安全対策の1対１の関係から容易に決定できる。	発生する行為と保護すべき資産に関した安全対策の組合せを基に決定される。 統計の不足が有効性を決定するのを困難にしている。

(12) 達成可能な保護レベル

偶発的事故の大半は防ぐことが可能である。・・・その理由の１つは、保護対策が効果的であったかどうかは、発生した事故統計をとることで測定できるし、得られたニーズに応じて適切なセキュリティを設定することができるからである。

意図的な行為による損害を高いレベルで保護するのは、損害が発生する可能性に関する私達の知見が充分でないため非常に困難である。

個々の損害に関する評価は、保護の完全性を決定するのが困難であることなども含め、多くの要素によって影響を受ける。出し抜き行為がどんどんエスカレートし、犯人のやり口が巧妙になってくるため、信頼できる測定を行うことが不可能となる。

偶発的事故	意図的行為
大半は防ぐことができる。 保護対策が効果的であったかどうかは、発生した事故統計で測定できるため。	非常に困難である。 損害が発生する可能性に関する知見が充分でないため。

(13) 潜在的加害者

　偶発的損害の場合、潜在的加害者は容易に確認できる。つまり、そうした損害に関連する行為の権限とか手段をもっている人達のことである。反対に、意図的におこされる損害に関しては、潜在的加害者の確認は難しい。・・・権限を与えられていないにもかかわらずこうした行為に関する技能や知識、機会をもつ多数のものも含まれるからである。例えば、リモート・ターミナルがしようされている場よでは、どこでもコンピュータ・システムに損害を与えることのできる多くの人達が存在しているのである。

偶発的事故	意図的行為
潜在的加害者は容易に確認できる。	潜在的加害者の確認は難しい。

(15) 損害の限界

偶発的に生じる損害の規模には限度がある。損害の規模には限度がある。損害の規模が様々であっても、その発見の確率と損害がやむまでの時間は、損害規模に比例して大きくなる。被害者は通常、自己の損害を目にし、評価することによって、タイムリーに損害を食い止めることができる。ところが、意図的行為によって生じた損害をタイムリーに発見することは必ずしも損害の規模とは関係しない。加害者が損害を隠すために大きな努力を払っている場合は、異常に大きな損害であっても発見することができない。さらに、犯罪方式がますます自動化する傾向にあることから、1000分の1秒単位で大損害が起こる可能性も出てくるだろう。人々がこのような状況に充分迅速に対応することは不可能となろう。

偶発的事故	意図的行為
損害の規模には限度がある。 発見の確率と損害がやむまでの時間は、損害規模に比例して大きくなる。 損害を目にし、評価することによって、タイムリーに損害を食い止めることができる。	潜在的加害者の確認は難しい。 損害を隠すために努力を払っている場合、大きな損害であっても発見することができない。 瞬間に大損害を与える可能性もある。

(16) 発見

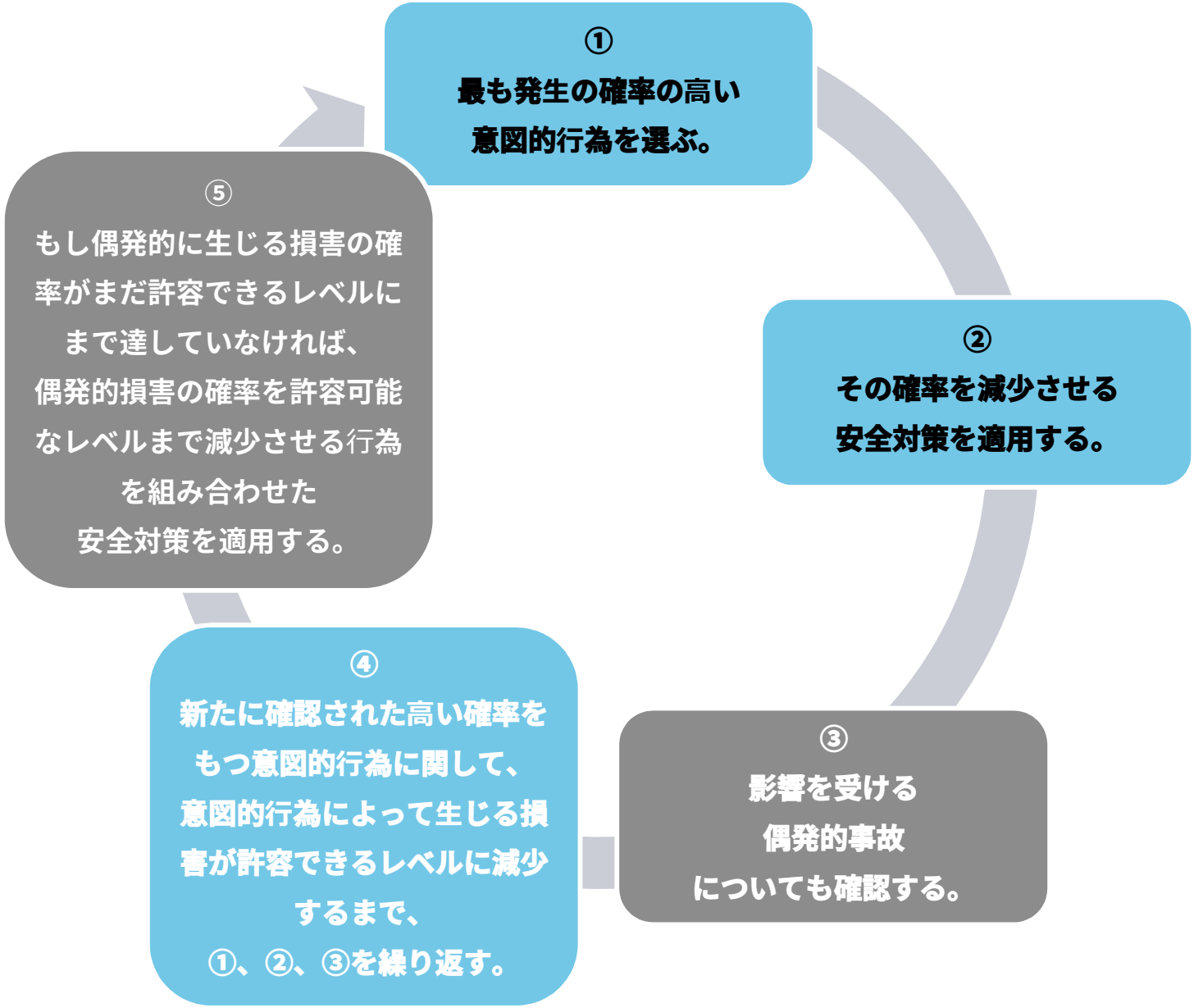
偶発的に生じる損害の加害者は、行為前、行為中にかかわらず過ちの自覚がない。したがって、もし発覚を避けるための試みがなされるとすれば、それは損害発生後である。発覚の恐れが少ないこと、損害報告にためらいが少ないこと、回復のために被害者に協力する度合いが大きいことなどが、偶発的な損害の証拠と言える。一方犯罪者へのインタビューによれば、犯人は行為前、行為中、行為後を通じて予期せぬ発覚を非常に怖れ、このため彼らの努力と彼らの持つ才知の多くは発覚防止に払われていることが明らかにされている。このように、意図的行為によって生じた損害の発見は、自己の場合に比較するとより大きな挑戦であり、セキュリティ専門家の注意はもっとこれに多く向けられるべきである。

偶発的事故	意図的行為
回復のために被害者に協力する度合いが大きい。	行為前、行為中、こう以後を通じて発見を非常に恐れ、発覚防止に多くの努力が払われている。

4.7 セキュリティ戦略

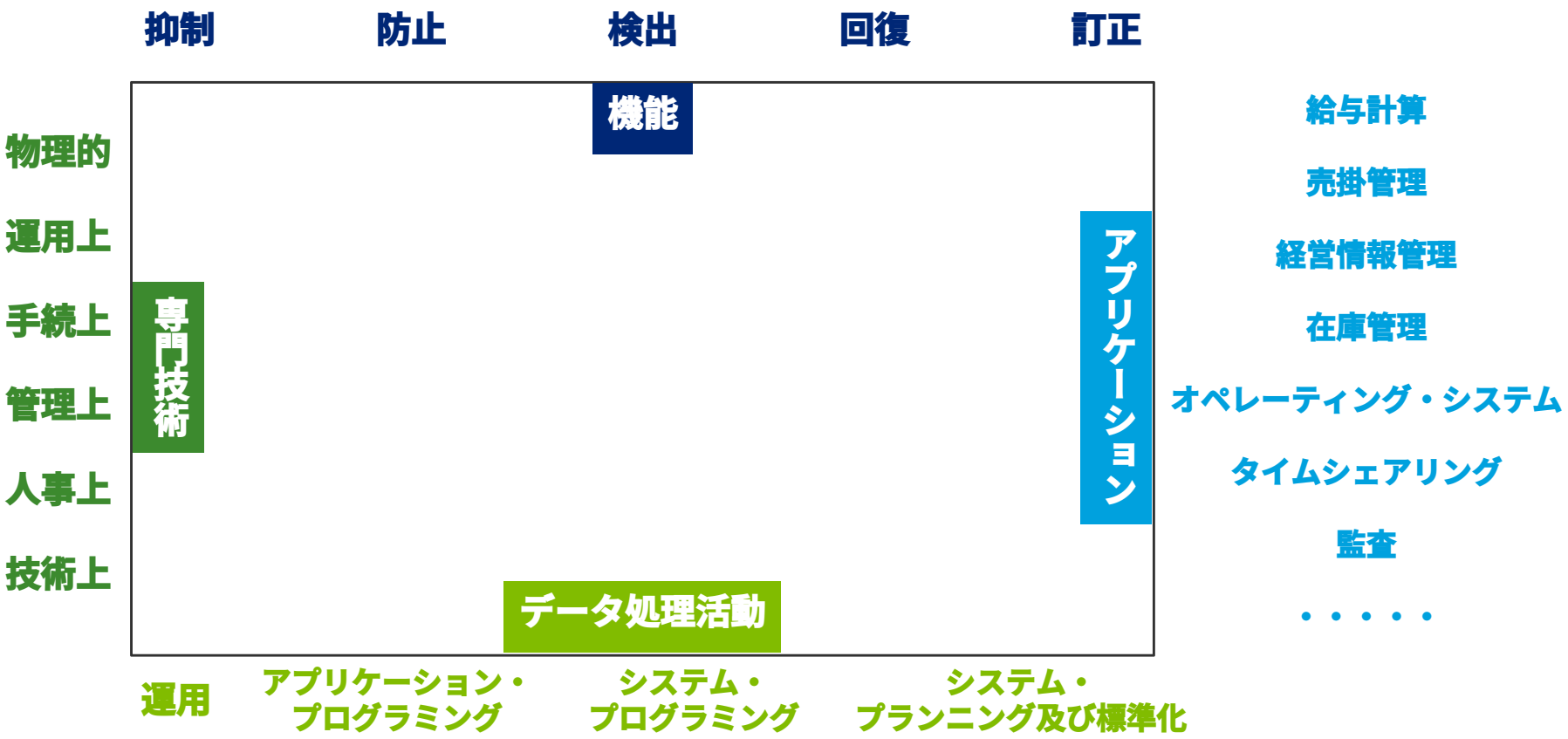
偶発的事故の確率を減少させる安全対策を採用した場合は、それがどの事故を想定したものであっても、セキュリティは着実に高められる。ところが、意図的行為の確率を減少させる安全対策の場合には、発生に対して最大の確率を持つ行為の確率を減少させない限りセキュリティを高めることはできない。したがって、意図的行為に対するセキュリティは、一連の対策の中での最も弱い部分でそのレベルでとまってしまうのである。

・・・この結合された戦略の適用に必要なステップは次に示すとおりである。



第５章 セキュリティの機能

5.1 セキュリティの次元



5.2 セキュリティの機能における優先順位

	一般的なセキュリティ対策の場合	不正への対応
1	基本回復機能	抑制
2	主な脆弱性に関する防止機能	防止
3	明白でない事故の検出	検出
4	後の訂正のための機能	回復
5	長期的な抑制機能	訂正

一般的には、回復機能が最も高い優先順位を持つ、他のセキュリティ機能が無い場合でも、組織は少なくとも回復機能を持ち、事故によるビジネス活動の停止を未然に防がなければならないからである。・・・組織にとって2番目の優先順位を持つものは、明白な犯罪の防止を防ぐという意味での防止機能である。その次は検出機能である。これは、明らかな形をとらない事故を、最適の回復が行えるようタイムリーに発見するためのものである。訂正機能は、回復後の防止機能及び検出機能の再配置、修正を意味する。最終的に新しいプログラムでは、抑制の手法についても検討しなければならない。

抑制機能は、損害の防止を直接的には保証してくれない。また、訂正は明らかにプログラム開始に関しては副次的な機能であり、損害に対する検出、防止、回復が適切に行われなかったため特定の脆弱性が見つかった場合にのみ役立つものである。検出は、直ぐには明らかにならないような損害に関して、それも事前にのみ必要とされる機能である。・・・また、検出機能は、損害の発見だけでなく、防止手段や防止のための装置が正常に働いているかどうかを判断する上でも不可欠な要素である。・・・初めてセキュリティを実践する組織は、検出機能以前に主要な損害を防止することに注意を向ける必要がある。また一般的には、セキュリティ資源の大部分をこの機能に注ぎ込むべきである。回復機能は、最初は一時しのぎにしからなないが、後には重要なバックアップ機能となる。

5.4 抑制機能

「抑制 (deterrence)」という名詞は、動詞「思い止まらせる (deter)」から派生しており、危険、困難または不愉快な付帯状況、もしくはその結果を考えさせるか、あるいはそれに対して恐れを抱かせることによって行為を起こそうという気持ちそのものを無くせることを意味する。ここで特に重要なのは、恐れという言葉の意味である。・・・権威に対する尊厳が大事なのである。・・・コンピュータ・セキュリティの体制固めを行う際には、考えられる範囲で恐れの源となる要因を検討することが重要になる。

抑制機能の価値

犯罪を犯す人は、それが悪いことだとわかっていながら実行することから、抑制機能は余り意味がないと指摘する人もいる。このことは、確かに本職の犯罪者に対しては事実かもしれないが、コンピュータ犯罪の主役は、これまでの経験からみても素人のホワイト・カラー犯罪者であり、こうした人々に対しては必ずしも当てはまらない。犯罪を指向する意志が完全に熟してしまってからでは、抑制機能は効力を失うのは事実である。抑制機能の進化は、その意思がある臨界点を越えないように抑える働きをすることにある。

抑制機能の安全対策としての価値

(1) 履歴調査（診断）

自分の情報に詳しい相手に対して犯罪行為を行うことには躊躇するものである。

(2) 従業員に対するカウンセリング

各人が、個人的な問題を専門のカウンセラーと相談できるようにすれば、合法的な解決策を見つけることも可能であし、また潜在的な犯罪行為を避けることも可能である。

(3) セキュリティに関する概況説明

損害はそう頻繁に発生するものではないし、またセキュリティ自体が生産性や能力を改善する手段ではないため、従業員はともすると損害に対する備えの必要性を忘れ、責任を忘れてしまいがちである。・・・損害が組織や従業員にどのような結果をもたらすかを説得することによって高めることができる。

(4) 行為規範

管理者を通じて周知を図るとともに、強く支持推進されなければならない。

(5) 法律と規制

人々が法律の存在を認識し、その範囲を意味を理解していなければ、これらの法律による抑制効果を発揮することはできない。

(6) 監査

監査が持つ最大の価値は抑制機能にある。これまでのコンピュータ犯罪において経理上の不正や窃盗を働いた人によると、犯罪の第一歩は監査人を欺くことだと指摘している。・・・監査人による抑制効果は、監査人の活動を予測できないようにすることによって発揮される。

(7) 任務の分担

2人以上の担当者に役割分担をさせる方法も安全対策の１つとして広く活用されている。

(8) 物理的なアクセス・コントロール

(9) 論理的なアクセス・コントロール

(10) 論理機構と記憶装置の区分

あまりにも複雑であることが、不正行為をあきらめされることにもなる。

5.5 防止機能

防止機能は、以前から最も効果的なセキュリティ機能とされているが、その価値には費用対効果による条件がつく。つまり、防止機能に必要なコストは、予想される損害を越えてはならないということである。完全な防止機能は机上の概念にすぎない。

**防止機能に必要なコストは、
予想される損害を越えてはならない**

防止機能のもっと現実的な目標は、潜在的犯罪者が目標を達成するための手段として、別の手段を求めざるを得ないようにすることである。・・・犯罪者が注ぎ込むことができる資源を枯渇させることによる抑制効果を持たせるのである。

**犯罪者が注ぎ込むことができる
資源を枯渇させることによる抑制効果を持たせる**

防止機能の３つのレベル

積極的防止	最も高度で、執拗な犯罪者の不正行為を防止することを目的とするレベル。
直面防止	犯罪者に犯していることが不正行為であることを意識させるのに必要かつ充分な安全対策を設けるレベル。
消極的防止	資産を目につかないようにし、誘惑に駆られるのを防ぐレベル。

5.6 検知機能

ほとんどの防止手段は、セキュリティ・システムに検知機能が組み込まれていない場合は効果がない。しかし、通常検知機能だけでも充分とはいえない。

通常、検知機能は防止機能と共に使われる。・・・一般に、技術的または自動化された検知機能は、人間による検知機能より優れている。

検知機能においては、混乱させることなく適切な情報を人々に伝える必要がある。タイムリーに通知し、その意味するところを人にわかるようにしなければならない。

検知機能は防止機能と共に使われる

**自動化された検知機能は、
人間による検知機能より優れている。**

5.7 回復と訂正

抑制機能、防止機能、タイムリーな検出機能が実現できないとか、全体的にみてセキュリティの問題を扱う上であまり効果的でない場合は、欠陥を回復したり訂正したりする機能が不可欠となる

第III編 コンピュータ・セキュリティ・プログラム

第12章 安全対策の識別、選択、実施

12.1 安全対策の選択原則

(1) 費用対効果

また、安全対策の多くは、性能や生産性を引き上げエラー率を低下させるので、最終的に費用の削減に結がることも忘れてはならない。

(2) リアルタイムによる人的介入の削減

人間による操作とか操作中の人的介入を必要としない安全対策は、同等の保護能力を発揮する人間による安全対策より優れているのが普通である。

(3) 補助装置及び2重安全装置の省略

安全対策やそれが保護する資産に対して侵害・攻撃があった場合でも、人命が危険にさらされないならば、安全対策自身が人命を損なうようなものであってはならない。

(4) 設計機密の欠如

安全対策の機構を秘匿することに重点を置くのではなく、それをはきしようとする努力やその複雑さを重視すべき原則は、コンピュータ・セキュリティの安全対策にも適用されるべきだろう。

(5) 最小特権（知らせる必要性の圧縮）

特権や知識に対する必要性を最低限度に抑える原則

(6) エントラップメント（罠）

システムの持つ脆弱性の１つまたはいくつかを、潜在的侵害者に魅力あるものと映じるように罠をしかけるわけである。さらに、この特定の脆弱性には、何らかの不正を試みようとする行為をタイミング良く検知するする機構を与えておく。違法行為を行おうとする者が攻撃をかけようとする場合、これらの弱点のどれかを対象とする可能性が強く、彼は検査されストップをかけられることになる。

この戦略にもいくつかの欠点がある。まず第一に、これが合理的な犯罪者を想定している点である。・・・犯罪者がセキュリティ設計者と同じセンス、技量、知識、手段をもっていると考えることでそうしないと全く裏をかかれてしまう結果となる。

第２の問題点は、ある個人を不正行為におびき寄せる不公正さを内包している点である。

(7) コントロールとその対象者の独立性

安全対策によってコントロールまたは制約を受ける人々は通常、対象者と呼ばれ、安全対策を効果的に機能させる人々は、コントローラと呼ばれる。・・・尾コントローラとその対象者が互いに独立したものであり、しかも違った層から出た人々で構成されるべき・・・

(8) 包括的適用

規則や手順に例外が存在すれば、問題が生じるよりむしろ安全対策に支障が生じるだろう。安全対策を設定するならば、必ずそれは均等に化されるべきである。・・・この原則が生み出すメリットは簡便さと整合性である。

(9) 区画化及び深層防御法

区画化という用語は船舶設計に由来する。

一方深層防御とは、特定の目標に働きかけようとする反抗者が次々と出くわさなければならないよういくつもの安全対策を重ねる概念である。

この原則を真剣に考慮すれば、・・・よりシンプルでコストも割安な一組の連続的な安全対策に置き換えることができる。

(10) 隔離、経済性及び最少の共通機構

安全対策は、他の安全対策との組合せを観点として考察されなければならないが、同時に他の安全対策と分離し、できるだけ共通の機構に依存していないことも重要である。

(11) 完全性及び一貫性

安全対策には、機能面の完全さと導入利用以前の仕様書との一致が求められる。これは完全で一貫した一組の仕様書及び操作手順書が必要となる。・・・仕様書では安全対策者がなすべきことを正確に記載するとともに、その安全対策が行ってはならないことを指示する、・・・

(12) 計装

どのような安全対策であっても、その適切な機能、故障、加えられる障害などを適時モニタする計装（計測管理用装置の装備）がなければ完全とはいえない。

(13) 職員の受容と寛容

安全対策は、合理的な許容限度を越えて要員に束縛を与えるものであってはならない。

(14) 持続性

安全対策が自動化されるにしたがって、ますます長時間効果的に機能するようになってきた。一方、人間の行動に対する依存度が高い安全対策は、時間の経過とともに機能が低下する傾向にある。

(15) 監査能力

安全対策は、その使用との一致及び性能を監査するためにテストできるようになっていなければならない。

(16) 責任能力

各安全対策には、それに責任を持つ要員が少なくとも1人は容易されていなければならない。

(17) 反応及び回復

安全対策は、それが実際に働いている場合にどのように反応するかによって評価されなければならない。安全対策は、ほごされている資産を破壊するかもしれない・・・

安全対策の反応は、コンピュータ・システムに対し、より以上のあるいは別の攻撃のために利用できる情報を開示するようなものであってはならない。

(18) 残留効果及びリセット

安全対策が活動した後の、残留状態やデータにも当然注意が払われなければならない。また、安全対策をリセットしたり、再稼動するのにひつような環境やニーズにも注意を向けるべきである。安全対策がその機能を果たした後は、保護されていた資産は少なくとも以前と同じように安全な状態にしなければならない。

(19) メーカ、サプライヤ、サービス提供者の信用度

安全対策が信用するに足るものであるためには、その信頼性、完全性、仕様との一致、持続性などが立証されなければならない。これら全ての条件の立証が不可能ないし非現実的である場合は、メーカ、サプライヤ、保守サービス業者が信頼に足る存在でなければならない。

(20) 多重機能

１つのセキュリティ機能を実行するためには１つの安全対策が選定されるのが通例である。

これから・・・

Internet of Things
つながるものはすべてが攻撃対象となる

考えられるリスク

システム停止

誤作動

情報搾取

どこからでも

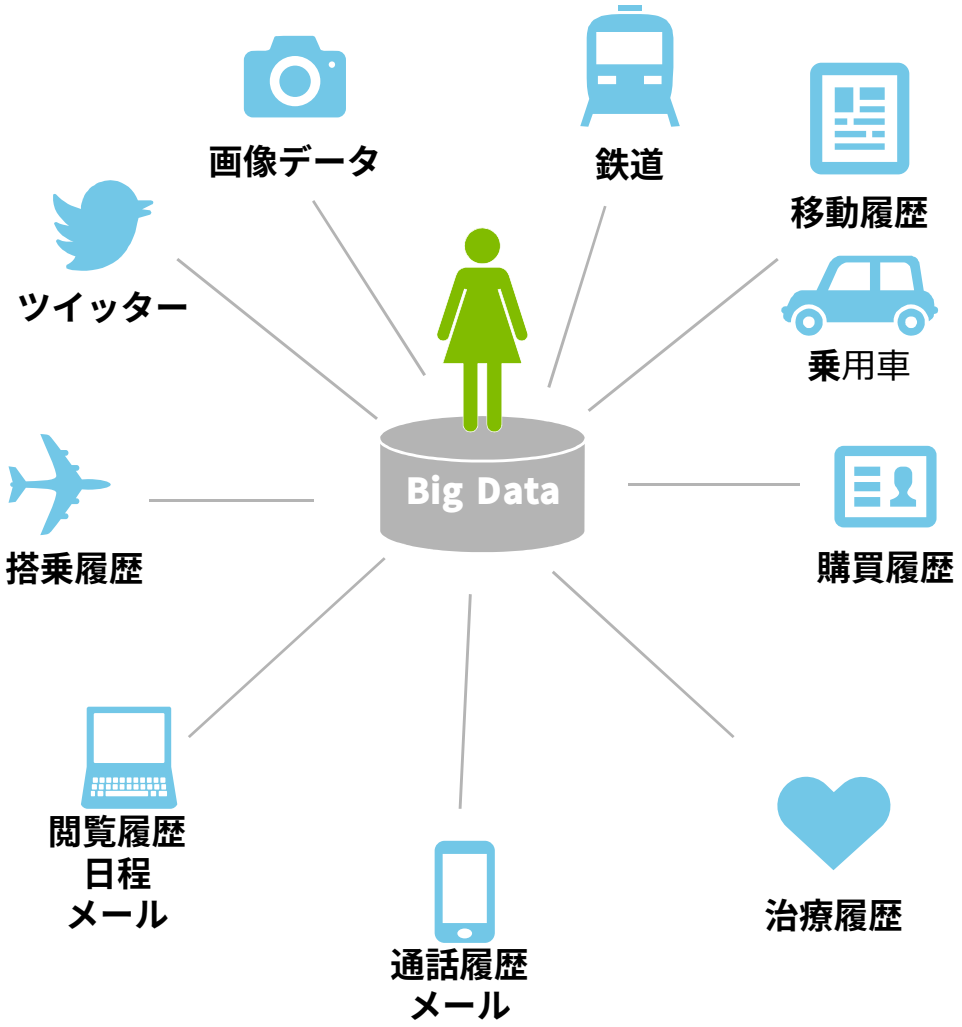
インターネットにつながっている「もの」に

攻撃ができる

それが直接狙われなくても

踏み台として利用されることもある

Big Data
インターネット上で自らのプライバシーをどのように守るべきか？



技術進歩

センサー技術の進歩

ストレージの容量の拡大

情報処理技術の進歩

新たな付加価値が見出されるかもしれない。

プライバシー上の懸念

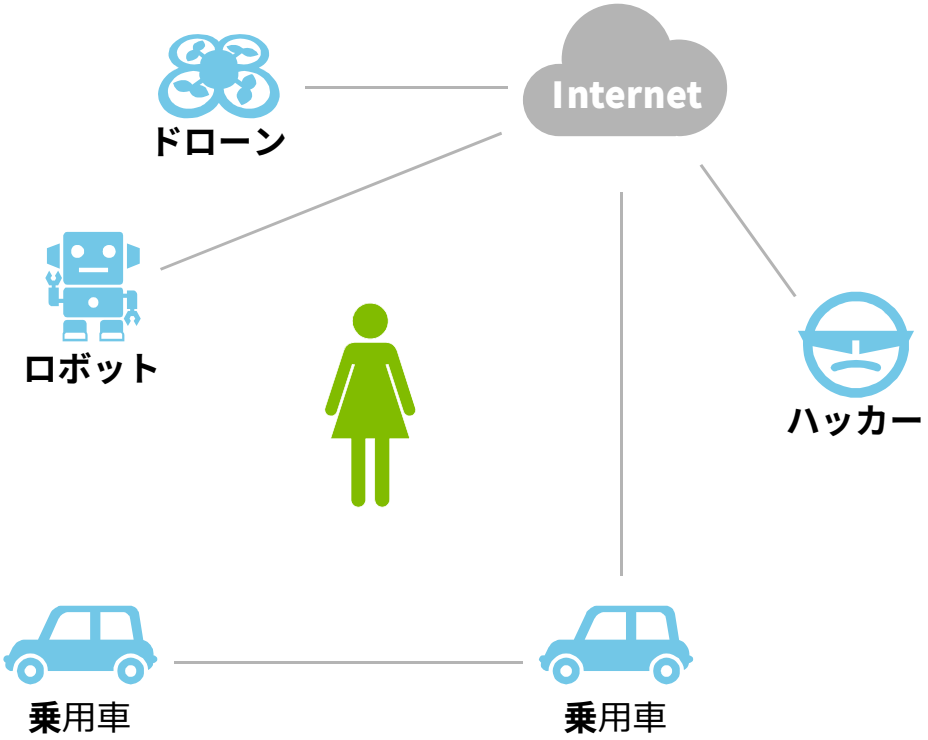
自分についての情報が蓄えられ、紐付けられ

想定もしていない人に

想定もしていない目的で

利用されているかも知れない

Autonomous control
自律移動する機械と人間が物理的な空間を共有する



従来の産業ロボットの安全管理

稼動部分への人の立ち入り制限

自立移動する機械の安全管理

？？？

自律移動する機械と人間が物理的な空間を共有する

何をするかは変わらないだろう。どのようにすべきかは変わるだろう

What

かわらないだろう

How, How much

技術や状況によってかわるだろう

山口英先生を偲んで

2016年5月9日11時38分 山口英先生 永眠

http://iplab.aist-nara.ac.jp/member/suguru/index-j.html

出会いと別れ

出会い

UNIXセキュリティ 1995年ごろ？

経済産業省　情報セキュリティ監査委員会（2002-2003年 ）
（ただし先生は一度も出席せず）

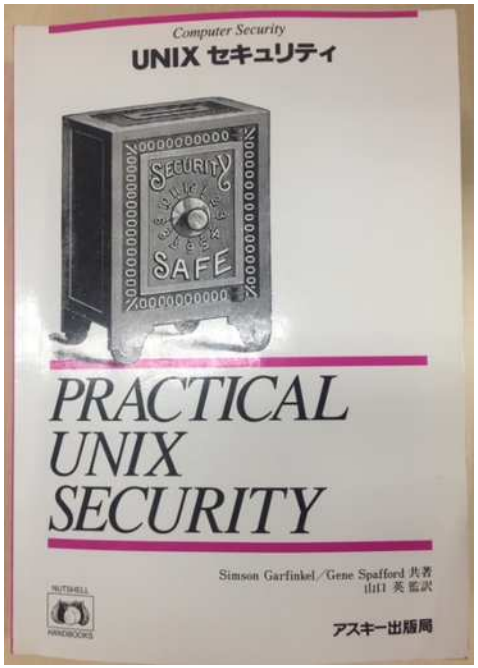
経済産業省 情報セキュリティ総合戦略策定委員会（2003年-2004年）

2004年4月から内閣官房 情報セキュリティセンター
情報セキュリティ補佐官

私はNISCで統一基準の策定に係わる

2006年くらいから？

JPCERT/CC　監事として参画



別れ

2016年1月20日 奈良先端大学でお話をしたのがお会いした最後

2016年4月21日 JPCERT/CCの理事会で声を聞いたのが最後

http://itpro.nikkeibp.co.jp/atcl/interview/14/262522/090700192/?rt=nocnt

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド（英国の法令に基づく保証有限責任会社）のメンバーファームおよびそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ コンサルティング合同会社、デロイト トーマツ ファイナンシャルアドバイザリー合同会社、デロイト トーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査、税務、法務、コンサルティング、ファイナンシャルアドバイザリー等を提供しています。また、国内約40都市に約8,700名の専門家（公認会計士、税理士、弁護士、コンサルタントなど）を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト（www.deloitte.com/jp）をご覧ください。

Deloitte（デロイト）は、監査、コンサルティング、ファイナンシャルアドバイザリーサービス、リスクマネジメント、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスを提供しています。デロイトの約225,000名を超える人材は、“making an impact that matters”を自らの使命としています。

Deloitte（デロイト）とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド（“DTTL”）ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を指します。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL（または“Deloitte Global”）はクライアントへのサービス提供を行いません。DTTLおよびそのメンバーファームについての詳細は www.deloitte.com/jp/about をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、その性質上、特定の個人や事業体に具体的に適用される個別の事情に対応するものではありません。また、本資料の作成または発行後に、関連する制度その他の適用の前提となる状況について、変動を生じる可能性もあります。個別の事案に適用するためには、当該時点で有効とされる内容により結論等を異にする可能性があることをご留意いただき、本資料の記載のみに依拠して意思決定・行動をされることなく、適用に関する具体的事案をもとに適切な専門家にご相談ください。

有限責任監査法人トーマツ 東京事務所エンタープライズ リスク サービスは、2006年2月8日、監査法人として初めて情報セキュリティマネジメントの国際規格であるISO/IEC27001の認証を取得しました。
2009年4月1日には、デロイト トーマツ リスク サービス株式会社をこの認証範囲に含めております。

IS 501214 / ISO (JIS Q) 27001

有限責任監査法人トーマツ 東京事務所におけるBCP/BCMサービス提供部門およびデロイト トーマツ リスクサービス株式会社は、2011年3月11日に事業継続マネジメントシステムの規格であるBS25999-2:2007の認証を取得し、2013年2月19日に国際規格であるISO22301:2012の認証を取得しました。

BCMS 568132 / ISO 22301

Member of
Deloitte Touche Tohmatsu Limited