コンピュータセキュリティ　10−25
(2000. 7. 25)

情報セキュリティ技術への提言

上園　忠弘

城西国際大学　経営情報学部

〒283　千葉県東金市求名1

0475-53-2225(ﾀﾞｲｱﾙｲﾝ)　/　uezono@jiu.ac.jp

最近の情報処理形態は分散処理を前提として一層進行しつつある。この状況ではキーボードとディスプレイのあちら側にはやりたい放題の世界が広がっているように見える。それにつれて内部不正の温床ができてはいないか。情報セキュリティ技術はそれに対処できるであろうか。現在のセキュリティ技術の構造や思考の枠内ではそれが不可能であることを示す。事態を改善するためには、セキュリティに対する想定「敵」を外部者にのみ設定するのではなく、内部者にも視点を移す必要があることを示し、新しいセキュリティ技術の開発への期待を述べる。

情報セキュリティ技術、ISO15408、内部の敵、システムへの脅威

A Suggestion to Information Security Engineering

Tadahiro Uezono

Josai International University

〒283　Gumyou 1, Tougane City, Chiba Prefecture

0475-53-2225　/　uezono@jiu.ac.jp

Modern data processing is mainly based on distributed data procesing. Under this situation, the operation through keyboard and display would produce risky world within an enterprise. Would the information security engineering solve this problem? In this paper, I will show that is not attainable. To improve the situation, I will advise the change in the assumption of the enemy to the security engineering. And state an expectation to the development of new information security engineering.

information security engineering, ISO15408, internal enemy, threats

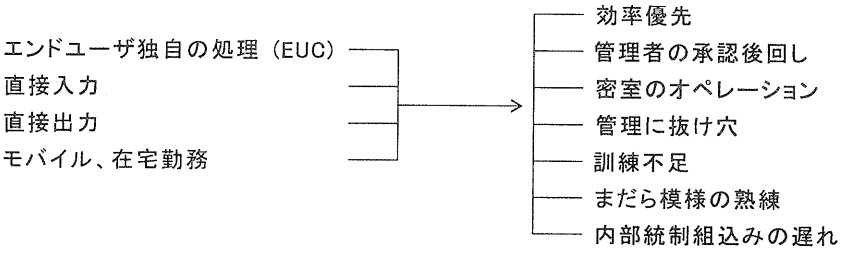
情報セキュリティ技術への提言

1. 最近の情報処理の形態は組織体の組織体の内部管理をまだら模様にしたのではないか。

分散処理方式には多くの利点があるが、どうしても除去できない欠点もある。その欠点とは処理の分散とともに、管理（コントロール）も分散して弱体化することである。この弱点から企業不祥事の発生可能性が生まれる。

企業における最近の情報処理形態とそのもたらす結果は下図のように要約できる。

図表1 最近の情報処理形態とその結果



キーボードとディスプレイのあちら側にはやりたい放題の世界が広がっているように見える。

2. それにつれて内部不正の温床ができているのではないか。

Not all of your security risks come from outside

情報セキュリティを、「情報の権限外の変更、破壊、開示から生じる損失の予防、軽減、分散、復旧の対策」と定義づけるとすれば、情報セキュリティへの敵は外部からのみ来るわけではない。(図2参照)

米国の統計によると、業務上詐欺および乱用（Occupational fraud and abuse)は、図表2のツリー図に示すことができる。*1

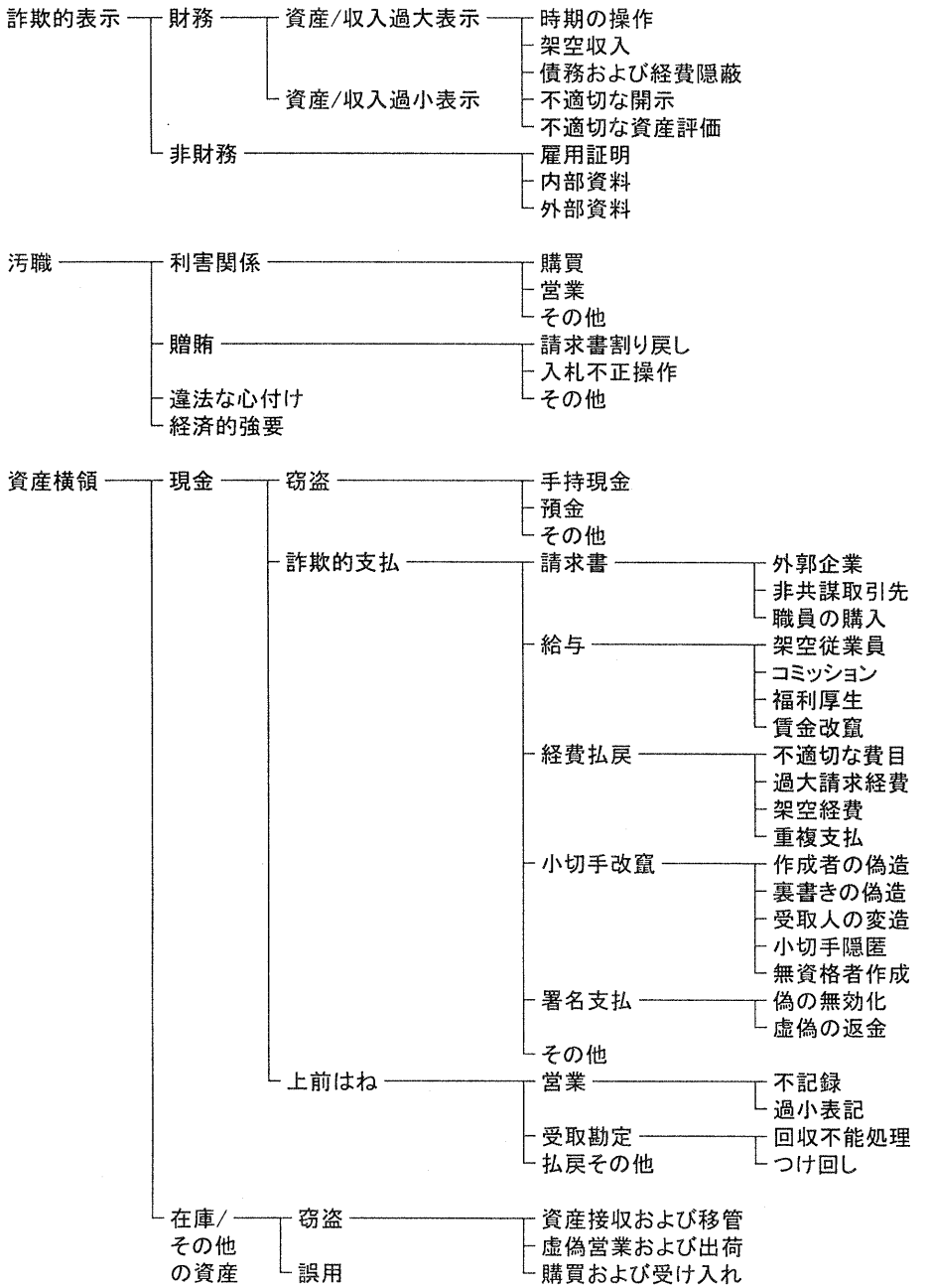
これらの不正は、現代の企業では、よほどの小企業でコンピュータを使用していない場合を除いて、そのほとんど全てがコンピュータ・プログラム内のルーティンの改ざんあるいはテーブル類の変更によってなされるか、あるいは入力データのごまかしによって行われることを指摘しておきたい。ここにコンピュータが明白な形で介在しないケースは、汚職ぐらいであろうか。

---

*1 本統計における「業務上詐欺および乱用」の定義は次の通りである。

「雇用されている組織体の資源または財物を故意に誤用あるいは不正使用することを通して、自己の職業を自己の個人的富のために悪用すること」

図表2　業務上横領および乱用形態の分類



出典："An unholy trinity　The three ways employee embezzle cash.", by Joseph T. Wells, PP.28-33,　Internal Auditor, Vol. LV;11,　Apr.1998

3. 情報セキュリティ技術はそれに対処できるか

現在の情報セキュリティ技術は、あまりにも外部からの「敵」*1に目を奪われていてそれに応えることができないのではないか。情報セキュリティ技術の構造は下図に示すとおりである。

図表3　情報セキュリティ技術の構造:

- 資格を与えられた者の無謬性の仮定
  - 資格を与えられた者はその資格を悪用しないという仮定
- 資格を与えられていない者＝敵　という仮定
  - 外部者は敵であるという仮定

図表4　情報セキュリティ技術の対象

情報セキュリティ技術	目　　的	対象者	対象
－アクセス制御	有資格者のみのアクセス	外部の敵	機密情報
－暗号技術	情報の秘匿	外部の敵	機密情報
－推論制御	統計からの機密抽出の防御	内外の敵	データベース
－データフロー制御	情報横流しの防止	内外の敵	機密情報
－セキュリティ・ホールの閉鎖	不正侵入の防止	外部の敵	情報システム
－不正プログラムの検知・修正技術	ウィルス防御	外部の敵	情報システム
－許諾なしのコピー	コピー防止機能	内外の敵	ソフトウェア
	電子透かし技術	内外の敵	同　上
－ログ分析	アクセス者の行動トレースを通じて「敵」を割り出す		

最近流行の ISO15408 が主眼とする点も、やはりネットワークにおける外なる敵への防御にあるように思われる。コモンクライテリア(現行のISO15408)では、情報システムに対する脅威とセキュリティ機能は、図表5の如くであるとされる。ここに挙げられた脅威は、無資格者によって引き起こされるものと、故障あるいは生涯によるものとが大部分を占めていて、有資格者によって行われる可能性があると明白に示される脅威は、＊印をつけた僅か2例に過ぎない。

すなわち、有資格者が行う不正はほとんど想定されていない。いっぽう、同図において「無資格者」による行為としている部分を「有資格者」が行った場合、表の右側に示されたセキュリティ機能が有効に働くであろうか。それは働かない。それらのバリアは有資格者にとっては内に等し

＊1　ここに言う「敵」とは、情報セキュリティの論者が慣用的に使う用語で、「やってほしくないことをたくらむ悪者たち」のことであり、彼らの言葉は慣用的に「攻撃」と呼ばれている。D.W. デヴィーズ、W.L. プライス、上園忠弘監訳、「ネットワーク・セキュリティ」、P.17、日経マグローヒル、1985

図表5　情報システムに対する脅威とセキュリティ機能要件

対象	脅威	機能要件
記憶媒体上のデータ	記憶媒体の不正持ちだし	記憶媒体上のデータの暗号化
	無資格者が業務アプリケーションの参照、変更、削除、追加	データに対するアクセス管理
	無資格者が操作コマンドで参照、変更、削除、追加	操作コマンドに対するアクセス管理
	無資格者が記憶媒体をダンプ	ダンプ機能の使用制限、データの暗号化
	記憶媒体上の残存データを参照	データ削除時にデータ領域をクリヤ
	不正コピー	コピー機能（操作コマンド）の使用制限、コピー時のアクセス管理、コピー対象データの暗号化、電子透し
	無資格者がデータの属性変更（不正利用妨害）	データ管理者の資格の管理
	ファイルの偽造	ファイルに対するアクセス管理
	記憶媒体の破壊	記憶媒体保管場所の管理、記憶媒体の2重化
	記憶媒体用ハードウェア障害	記憶媒体の2重化
	暗号化データの秘密鍵紛失	秘密鍵の復旧管理
	*有資格者の操作ミスによる削除	操作ミス防止対策(再確認、削除資格の追加指定)
通信回線のデータ	通信回線上でデータを傍受	回線上のデータの暗号化
	中継システム上でデータの傍受、改竄、削除、追加	同上
	同上　データ宛先、発信者、利用属性等の変更	通信制御データの暗号化
	通信回線の障害	通信回線の2重化
	データの不正な再送	不正再送の防止(一連番号確認、時刻確認等)
業務ソフト	無資格者による実行	プログラムに対するアクセス管理、有資格者離席時の対策設定
	同上　ライブラリ内容の参照、変更、削除	プログラム・ライブラリに対するアクセス管理 プログラム管理者の資格管理
	同上　プログラム利用属性の変更	
	コンピュータのハードウェア障害	情報システムの2重化
業務処理	不当な事務処理（Telnet, FTP 等）	監視（トラフィックやプログラム実行状況の監視）
	データ送受信、データ内容の否定	拒否の防止（TTP, 暗号機能利用の証拠保管）
	データ原本の否定	原本の保証（TTP）
	サービス提供の拒否	監査
	プライバシー侵害	匿名やペンネームを許す、追跡不可能性の保証
表示	無資格者ののぞき見	物理的対応策
	不正コピー、印刷	有資格者の離席時対策、コピー、印刷機能使用制限
印刷	無資格者の参照、持ち出し	印刷物の物理的管理
	不正コピー	コピー防止対策

情報システムに対する脅威とセキュリティ機能要件 続き

対象	脅　　威	機　　能　　要　　件
監査・監視	監査ログ、データの改竄	監査人の管理、監査ログ、データのアクセス管理
	無資格者の監査ログ、データの参照、改竄、削除	監査ログ、データのアクセス管理
	監査ログ記録不良（媒体、記録用バッファの障害）	記録媒体の2重化化、バッファの管理
	異常検出時の対応不良	オンライン監視、オンライン警告、定期監査
	監査ログの情報不足に基づく監査不能	監査管理（ログ収集タイミング、ログ・データ内容の再検討）
利用主体	利用主体（個人、システム）識別不能	ユニークな識別（個人、システムごとに ID 割り当て）
	利用主体の確認不確実	認証（暗号秘密鍵、パスワード、持ち物、身体的特徴）
	認証情報の不正な開示	認証情報の保護(一方向性暗号、秘密鍵管理、持ち物所有者確認)、被害者による早期発見（認証処理情報の通知）
	認証情報の不正な推測	推測防止（試行回数制限、長い秘密鍵)、被害者による早期発見
	無効な認証情報の使用	失効の管理
	認証情報の偽造	偽造防止（信頼できる認証機関、持ち物物理的保護)、被害者による早期発見
システム	*有資格者による不正、ミス	利用者資格管理(最小特権)、監査、規定検討、教育・訓練
	コンピュータ・ウィルス	ウィルス・チェック、アクセス管理(妥当な 利用者資格設定、ファイルの保護)、監視と処置（システム停止、外部システムの切断）
	セキュリティ機構破壊、バイパス、停 止、起動せず	セキュリティ機構の強度検証
	システムへの不正侵入	利用主体の識別、認証と資格確認
	システムの不正動作	操作コマンドの使用資格確認

TTP: Trusted Third Party

出典：田淵治樹、「セキュリティ・ポリシーに基づき安全なシステムを設計」、日経コミュニケーションズ、P.159、1998.5.4

注.　1. 出典で使われている用語を若干変更させていただいた。
2. 脅威欄の ＊ 印は、内部の資格権限があるものによる不正が行われる可能性のある項目として、筆者が付け加えた。

いからである。

4. セキュリティ技術だけにその責任を負わせられるか／負わせるべきか

情報セキュリティ対策を受け持つのはもちろん技術だけではない。法律、規制、情報倫理、組織内規程等がありうる。しかし、セキュリティの内部的崩壊に対する対策は、これらの非技術的対策にだけ任せておけばよいだろうか。もしその問いに対する答えがイエスであるとすれば、それはあまりにも技術を限定的役割に押し込めるものではないか。

5. 新しいセキュリティ技術への期待

コンピュータの内部者による悪用は、すなわち有資格者による不正であると考えて良い。それに対する対策を、セキュリティ技術は今までおろそかにしてきた観がある。

このギャップを充たすものは、おそらく広い意味でのモニター技術であろう。キーボードとディスプレイのあちら側に広がる密室の世界にはモニターの機能が必要である。それはあるいはプライバシーの問題をクリアしなければならないかも知れない。しかし、それは克服できる障害であろう。モニター機能に関連して進歩を期待するもう一つの昨日はログ解析技術である。膨大なログを適切に解析する技術、おそらくソート・マージ技法の飛躍的発展なども必要であろう。

若く、有能で積極的な研究者の出現を期待したい。

以上。