日本システム監査人協会支部総会講演

第164回定例会

平成29年1月20日

これまでのシステム監査からこれからのシステム監査を考える

ー事故、犯罪、法制度の歴史的課題からＩＣＴ時代のシステム監査を考察するー

大阪成蹊大学　名誉教授
経済法科大学　客員教授
松田貴典

世界で最初にシステム監査（当時：EDP監査）が始まったのは、米国で1954年（昭和29年）頃である。コンピュータがビジネス活用され、それまでの監査手続きに大きく影響を与え、**新たな監査手法**が求められた。

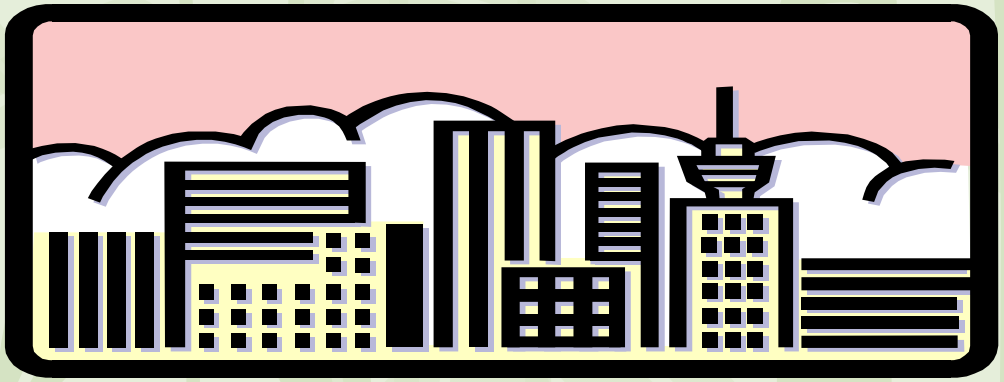
わが国では、昭和49年（1974年）に、日本情報処理開発協会（現：日本情報経済社会推進協会：JIPDEC）が米国にEDP監査の視察団を派遣するとき「システム監査」の用語を使った。そして、日本公認会計士協会は、業務のEDP化で監査証跡が確保できないことを懸念して、昭和42年（1967年）に「EDPシステム内部統制質問書」発表し、経済団体連合会等から意見を求めた。その後、1976年（昭和51年）に日本公認会計士協会が「EDP監査の進め方」を出版し、「**コンピュータ犯罪・不正を防止するために**」を目的として、**本格的なシステム監査**がはじまったといえる。

1987年（昭和62年）3月にシステム監査学会が設立、同年12月に日本システム監査人協会が発足し、実務研究の30年が経過した。求められるシステム監査は、「**情報システムの信頼性、安全性、経済性（有効性）**」への寄与から、「**情報報システムにまつわるリスクに対するコントロールのリスクアセスメントに基づく対応とICTガバナンス実現への寄与**」へと拡大進化した。

しかし、ICT（Information and Communication Technology：情報通信技術）の高度化は**豊かな情報化社会を形成したが、その豊かさに反作用**して「**脆弱な情報社会**」を作ることになる。「**情報システムの脆弱性**」は、ICTの機能の高度活用により、**組織や業務の範囲（適用、内容）、量（データや処理）、質（スピード、ミスや判断・意思決定能力等）を**変化させ、進化させるからである。

そこで、システム監査に関連する事故や犯罪、法制度等の歴史的課題からシステム監査を振り返りながら、これからのシステム監査について考察する。

ＩＣＴの高度化にともなう
ビジネス活用の進化とシステム監査を俯瞰



ビジネス活用とシステム監査の関連

この背景には、わが国でコンピュータの本格的実用が1958年（昭和33年）から、ビジネス活用に普及しはじた1968年（昭和43年）3月の設置台数は**約3560台**と著しく普及した（日本電子計算機株式会社資料より）。

コンピュータを電子計算機と訳し、ビジネス活用された1960年頃は、その活用形態を「**EDPS**（電子計算機を使っての情報処理システム）」と呼んだ。その後、コンピュータを経営や意思決定に活用し、**MIS**（経営情報システム）や**DSS**（意思決定システム）と進化した。コンピュータの活用技術は一層発展し、OA（事務の自動化）やFA（工場の自動化）からネットワークを活用し、企業間競争を優位に展開する**SIS**（戦略情報システム）を構築することになった。

現在の**ICT**（Information and Communication Technology：情報通信技術）による「**U-Japan**（UbiquitousやUniversal）」等の意味を加えて）等）」構想への実現にむけて推進されている。

ICTを活用して構築される情報システムが進化することで、企業等にとってはICTへの投資額も大きくなってくる。そこで、経営者からみれば、構築された情報システムへ投資は適正であり有効に活用されているのか、情報システムは安全に運用され信頼できるのか、**客観的に点検・評価・助言**が得られないか考えることは、至極当然のことである。ここの**システム監査の必要性**の根拠がある。

ＩＣＴの高度化とその活用の進化

年代	1960年～	1970年～	1980年～	1990年～	2000年～	2010年～
形態	EDPS バッチ業務 処理システム	MIS／DSS 経営情報 システム	OA／FA オフィスオート メーション	SIS／EUC 戦略情報 システム	VT バーチャル ユビキタス	クラウドコン ピューティング ビッグデータ
ICT	電子計算機	データベース オンライン	リアル(即時) ネットワーク	高速情報ネット ワーク／分散 自動車・携帯電 話、AI	インターネット CS/S、VR エンベディッド デジタル電話	実装AI・VR IOT スマートフォ ン
活用	手作業をコン ピュータ処理 徹底した計算処 理帳票処理 ・経理業務 ・販売管理	経営判断の情報 提供 部分的なコン ピュータ利用 ・意思決定 ・情報検索	事務や工場の 自動化 コスト削減にIT を活用 ・生産ライン ・自動化	競業企業との 差別化 IT活用が企業 の競争優位に ・CRS(座席予 約)	企業間連携に よる競合 インターネット ビジネス戦略 ・SCM、EC ・電子マネー	自動運転 人工知能と ディープラー ニング ブロックチェー ン(Fintec)
コンピュータ技術	第2～第3世代 IBM360(1964) BurroughsB5000 IC/コアメモリー OS概念の定着	第3．5時代 IBM370、 Burroughs	第4世代 マイクロプロセッサー パーソナルコン ピュータの出現 スーパーコンピュータの出現	汎用コンピュータ ネットワークコン ピュータ	CS/S:Client Server System	SDX SDF DepOpe ベストショア テレワーク

情報システムの進展にともなう監査の進化

年代	1960年～	1970年～	1980年～	1990年～	2000年～	2010年～
監査対象	EDP会計 コンピュータ犯罪	オンラインシステムの信頼性	オンラインリアルタイムシステム	情報システムの戦略活用 2000年問題	経営革新 （SCM、BPR等） SNS	クラウド／Iot ITガバナンス ビッグデータ
研究発表テーマ			・システム監査と内部統制 ・コンピュータ犯罪の傾向 ・システム開発ライフサイクル ・リスクメネジメント ・AIのシステム監査 ・ソフトウェアとめぐる法的問題 ・情報資源管理 ・情報システムの安全対策	・戦略的情報システム監査 ・企画開発業務の監査 ・経営秩序の構築 ・グローバル環境下における情報システムの監査 ・情報システムのセキュリティコントロール ・阪神淡路大震災（震災と安全） ・情報システムの安全対策 ・オープン環境下でのシステム監査	・システム監査とリスクマネジメント ・SNSの情報論理 ・インテーネット社会における監査 ・e社会とシステム監査 ・サイバー社会とシステム監査 ・ユビキタス社会におけるコントルールと文化基盤 ・企業経営と推し進める監査 ・情報システムの脆弱性とリスク対策 ・ITガバナンス	・クラウド時代でのシステム監査 ・東日本大震災でシステム監査 ・想定外の脆弱性時代のシステム監査 ・システム監査の新しいステージ ・多様性が求められるシステム監査 ・ビッグデータ時代のシステム監査 ・個人情報保護／マイナンバ制度のシステム監査 ・レピュテーションリスクマネジメント
課題	情報システムの安全性，信頼性（リカバリーシステムの開発等），	オンラインシステムの信頼性・効率性（ダウン対策。コンピュータ犯罪防止など	ネットワークシステムの開発，システム監査，セキュリティ対策の研究），情報システムの脆弱性問題	経営戦略・業務改革（BPR）手法の開発，ソフトウェア資産評価，情報法（知的財産権法，サイバー法など）	ビジネス問題と情報システムの脆弱性研究（ICT活用とセキュリティ，情報法）， システム監査等	クラウドコンピューティング コンプライアンス問題 情報システムの多様化

銀行が体験したコンピュータ犯罪

取り扱う者によって容易に悪用されることを知る

電子計算機使用詐欺罪（刑法246条の2）

オンライン横領・詐欺事件

■　三和銀行オンライン詐欺事件

1981年（昭和56年）3月25日に三和銀行（現、三菱東京UFJ銀行）茨木支店の女性行員が、同支店の**オンライン端末を不正に操作して巨額の現金他を騙取した横領・詐欺事件**である。女子行員A子は、銀行の開店とほぼ同時に、同支店の端末を操作して大阪の吹田支店、豊中支店、東京の新橋支店、虎ノ門支店の計4支店に開いた架空名義の口座へ、合計1億8千万円を架空入金した後に、伊丹空港から飛行機で東京に向かい、更に東京の新橋支店、虎ノ門支店からも現金を引き出した。現金5千万円と小切手8千万円相当の合計1億3千円を詐取した女性行員は、全額を男性（実業家、既婚者の恋人）に渡し、フィリッピンの首都マニラに逃亡した。

その後、国際指名手配され、9月8日にマニラ入国管理局に身柄を拘束され、日本への強制送還となった。

■　この事件を契機として、銀行オンラインシステムの**運用・活用面での脆弱性は非常に拡大し、コンピュータ犯罪や事故のリスクは非常の高い**という、社会認識が高まったと言える。

事件の判決が指摘したこと

■　本事件の判決

1982年（昭和57年）7月27日、大阪地方裁判所にて、被告人A（女性行員）に懲役2年6月、被告人B（男性）に懲役5年の実刑判決

■　判決でのポイント

本件犯行は**コンピューターシステムの弱点を利用したもの**であり、今日、これらのシステムは金融機関は勿論、多方面に普及しており、社会生活上や経済取引上欠くべからざるものである。**システム自体に内在する弱点とはいえ、これを取り扱う者によって容易に悪用されるうるものであることを明らかにし**、その結果、**システムに対する社会の信頼を失わせる**とともに、**同種の事犯を誘発**しかなねないものであり、社会に与える影響は無視できないとした。

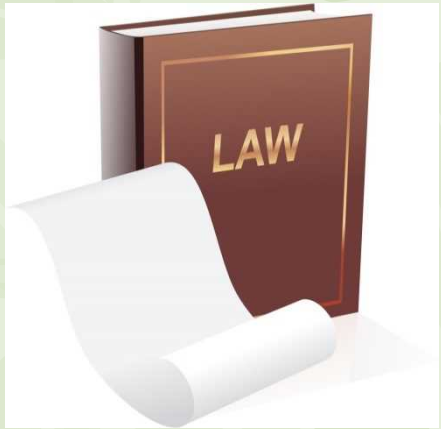
■　この事件を契機に、1987年（昭和62年）の法改正で、**電子計算機使用詐欺罪（刑法246条の2）**が新設された。

個人情報の漏洩と法・制度への影響

個人情報保護法の制定

個人情報保護法の改定

マイナンバー制度と監査



わが国で話題になった個人情報漏洩事件の検証

■1999年5月：京都府U市が住民基本台帳データを利用して乳幼児検診システムを開発企画した際に，住民票データ22万人分が流出しインターネットで販売された。

■2003年6月：ローソンからカード会員情報56万人分が流出。全会員115万人に対して500円の商品券と社長会からの謝罪文を配布

■2003年8月：信販会社アプラスからクレジット顧客情報7万9110人分がダイレクトメール会社に流出。対象者に1000円の商品券とお詫び状を配布

■200311月：ファミリーマートのメールマガジン購読者約18万人の個人情報が流出，委託先企業からの漏洩か。一部がアダルトサイトの架空請求に使われた。

■2004年2月：ヤフーBBの加入者情報約470万人分がDVDに記録され流出，ソフトバンク関連企業に対して数十億円の恐喝。これまでの最大規模の個人情報流出事件。500円の金券とお詫び状の配布

■2004年3月：通販会社ジャパネットたかたの顧客データ約149万人分が流出，内容に住所，氏名，生年月日，電話番号がはいっていた。再発防止対策を最優先のためビジネス業務の中断した。個人情報保護が企業の社会的責任であるとした。

■2005年4月25日の午前9時20分ごろ，兵庫県尼崎市で起きたJR福知山線電車脱線事故は大変痛ましく，負傷者を収容した病院において，負傷者の個人情報の取扱いが大きく分かれた。

■2006年2月頃：ウィニー等による個人情報の漏洩が多発

護衛艦の秘密文書も含む情報がインターネット上に流出（防衛庁海上自衛隊）

宇治市の漏洩事件がもたらす責任と問題

□ 平成１１年５月に京都府宇治市が住民基本台帳を活用してのシステム開発で、住民票**約22万件のデータ流出し**、インターネット販売された事件

① 行政対応：一時ストップ・停滞、回復費・損害賠償費用等々

② 市民感情：不安・不快感

③ **３市民が市と業者及び元請業者に損害賠償請求をおこなった裁判で、**

■ 市に対して：4万5千円（３人×1万5千円）の支払を命ずる判決

・１人当たり1万円5千円の内訳：

（慰謝料1万円、弁護士費用5千円）

■ 業者（システム開発会社）及び元請業者に対しても市と同じ判決

・１人当たり1万円5千円の内訳：

（慰謝料1万円、弁護士費用5千円）

□この事件がもたらした問題は、個人情報の基本情報の漏洩では、少なくとも一万円の慰謝料の支払いが起こることである。その結果、**集団訴訟のリスク（最悪のシナリオ）が発生しうることである。**

■ 市→33億円（22万人×1万5千円）

■ 事件を起こした業者→市に同じく：33億円（22万人×1万5千円）

■ 元請業者→市に同じく：33億円（22万人×1万5千円）

以上を合計すると**総額99億円の訴訟リスクがおこる**

クローズアップされてきた問題点

■アンケートの回答、会員等での個人情報の登録、通信販売での個人情報の記載など、個人情報が社会のなかで、大量に散在しているのではないという懸念

■個人情報は提供することで悪用されると問題になるとして，情報を隠そうとする風潮（**組織の隠蔽体質**）

■個人情報漏洩は現在も発生しており、マスコミが取り上げる主な事件は、
①大量の個人情報を販売目的で不正に複製し持ち出し
②パソコンや電磁的記録（FD，USB等）の紛失、窃盗
③Winny（共有ソフト）等からの漏洩等

■ 個人情報データベース等からの個人情報漏洩による**プライバシー侵害**への危険性、不安が増大

■ しかし、プライバシーが心配だとする一方でソーシャルメディアには、私的な情報を垂れ流しているという**プライバシーパラドックス**の問題が内在する

■ その一方で、利用価値の高い蓄積された膨大な個人情報を**ビッグデータ**として企業の利用が難しい状況になってきている

■ 企業等にとっては、個人情報の漏洩が膨大な経済的損失と**社会的責任**を問われ、対外的な信用の失墜となる

個人情報保護法の改正となった事件

ビッグデータ時代の到来に、個人情報として取り扱うべき範囲の曖昧さ（グレーゾーン）のため、企業が情報の利活用を躊躇しはじめた。

■ 2013年7月1日より、JR東日本が、IC乗車券「Suica」の利用履歴のビッグデータが販売開始された。データを販売した相手は日立製作所で、Suciaのデータを駅エリアのマーケティングに活用していく狙いがあった。

発売直後から「個人情報保護の観点で問題があるのではないか」という指摘があって、同年7月25日には販売中止を決めた。Suciaのデータ販売に関する第一報の段階で「個人情報を含まない形で販売」と報じられていたが、中止の背景に過剰な個人情報保護に敏感な反応があった。

■ 2014年7月9日に、「進研ゼミ」等を運営するベネッセコーポレーションの「**個人情報流出事件**」が、発覚した。顧客情報は最大で3504万件に及んだ。流出した情報は進研ゼミなどの顧客の情報であり、子供や保護者の氏名、住所、電話番号、性別、生年月日等、最大2070万件が流出した。ベネッセは、派遣社員のエンジニアが情報を持ち出し、**名簿業者に売却**したことを認めた。

【参考文献】 個人情報漏洩事件　ウィキペディア　https://ja.wikipedia.org/wiki/

個人情報保護の関連法と主要な制度

■ 1989年（平成元年）10月：行政機関を対象とした「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（旧法）」が施行された。

■ 2002年（平成14年）8月5日**住民基本台帳ネットワークシステム稼働（第1次）**
- 同時に、**11桁の住民票コードを割り当てを通知開始**
- 2003年8月25日住民基本台帳ネットワークシステムの本稼働（第2次）
- **住民基本台帳カード（住基カード）の発行**開始

■ 2003年（平成15年）5月23日に，民間事業者や行政機関から個人データの保護・流出防止を図る**個人情報保護関連5法案**が成立し、2005年（平成17）4月1日に全面施行となった。

■ 2013年（平成25年）5月23日に、「**行政手続きにおける特定の個人を識別するための番号の利用に関する法律（番号法）**」関連4法案が成立し、2015年10月5日から施行され、2016年1月1日に運用開始された。いわゆるマイナンバー制度の実施である。

■ 2015年3月30日　**全自治体が住民基本台帳ネットワークシステムに接続**

■ 2015年9月3日「**個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律**」が**成立**した。個人情報保護法と番号法（マイナンバー法）がセットで改正された。
施行は2017年5月30日

2015年9月3日（2017年5月30日施行）の主な改正点

1．**個人情報の定義**の明確化
- 個人情報の定義の明確化（身体的特徴等が該当）
- **要配慮個人情報**（いわゆる機微情報）に関する規定の整備

2．適切な規律の下で個人情報等の有用性を確保
- **匿名加工情報**に関する加工方法や取扱い等の規定の整備
- 個人情報保護指針の作成や届出、公表等の規定の整備

3．個人情報の保護を強化（**名簿屋対策**）
- **トレーサビリティの確保**（第三者提供に係る確認及び記録の作成義務）
- 不正な利益を図る目的による個人情報データベース提供罪の新設

4．**個人情報保護委員会**の新設及びその権限
- 個人情報保護委員会を新設し、現行の主務大臣の権限を一元化

5．個人情報の取扱いのグローバル化
- 国境を越えた適用と外国執行当局への情報提供に関する規定の整備
- 外国にある第三者への個人データの提供に関する規定の整備

6．その他改正事項
- 本人同意を得ない第三者提供（オプトアウト規定）の届出、公表等厳格化
- 利用目的の変更を可能とする規定の整備
- 取扱う個人情報が**5,000人以下の小規模取扱事業者**への対応

特定個人情報保護評価と監査

1．特定個人情報ファイルを保有しようとする又は保有する行政機関や地方公共団体等は、**事前対応**によるプライバシー等の権利利益の侵害を予測して、リスク分析を実施し、リスクの軽減と**未然防止を講ずるもの**

2．特定個人情報保護評価書に、**個人のプライバシー等の権利利益を侵害するリスク**を自ら分析し、対策を講じて保護に十分であると**「宣言」**

3．諸外国で採用されている**PIA**（Privacy Impact Assessment：プライバシー影響評価）に相当

特定個人情報保護評価では、リスク対策の監査及び自己点検を求めている。

【コンプライアンスの視点での監査も必要】

特定個人情報の取扱いについて**罰則が強化**され、**法人**にも適用される

例えば、◎個人番号事務等に従事する者（していた者）が正当な理由なく、特定個人情報ファイルの不正な提供（第67条）、◎不正な利益を図る盗用した場合（第68条）、◎業務に関する秘密を漏えい又は盗用した場合（第69条）、◎人を欺き、人に暴行を加え人を脅迫し、又は財物の窃盗、施設への侵入、不正アクセス等により個人番号を取得した場合（第70条）等、罰則が強化されるとともに、罰則によっては個人のみならず法人にも適用される

これからの個人情報保護のシステム監査

ネットワークのビジネスの高度化は、個人情報の利用がますます進み多様化する。厳密な個人情報保護の**監査の進化**が求められる。

■社会は厳格な個人情報保護を求めており、自己点検を含めた監査の実施を**義務化**することなる

■個人情報保護には、個人のプライバシー等の権利利益を保護する取組みを「**宣言**」し、適正に実施されていることを保証する**外部監査人**による「**保証型監査**」が求められる

■　個人情報を取り扱う「**ビジネス・プロセス**」**全体で監査**が必要になる

・**個人情報の保護では、個人情報保護マネジメントシステムでの監査**が必須となる。但し、内部監査のみでなく、企業や組織によっては**外部監査**の義務付けが必要となる

■経営の視点での監査が重要となる

- 「ガバナンスと戦略目標の実現」に寄与する監査であること
- 個人情報の漏えいや紛失は、**社会的責任（SR）**を問われることになり、法的な**コンプライアンス側面での監査**が重要となる

■消費者からえた**ビッグデータの活用及び匿名化したデータの販売には、システム監査により匿名性を担保**されることが必要である

個人情報保護マネジメントによる監査

個人情報保護マネジメントシステム（Personal information protection Management Systems：PMS）とは、JIS Q 15001が規定している個人情報を保護の体制を整備し、定められた通り実行、定期的な確認、継続的に改善するための管理の仕組みをいう。管理の原則はISO27001と同様にマネジメントシステムの考え方を取り入れて、**PDCAサイクル**を通じて改善を実施し、**スパイラルアップ**させることを基本としている。

監査はC（点検）に位置づけられ、日常での「運用の確認」と「監査」の実施が求められている。

【ポイント】 PMSの監査は内部監査でおこなうが、監査意見の強化と指摘改善を徹底をはかるために、少なくとも年１回の外部監査が必要である。

【参考】

プライバシーマークは、JIS Q 15001 の要求を満たし、個人情報保護に関して適切な処置を行っていると判断される事業者には、財団法人日本情報経済社会推進協会（JIPDEC）によりマークが使用を許可している。ただ、最近では、**「Pマークの形骸化」の懸念**がでている（読売新聞　2017年1月10日付）。

なお、PDCAサイクルによる実施は、**情報セキュリティマネジメントシステム規格（ISMS）**のほか 、品質マネジメントシステム規格（ISO9001）、環境マネジメントシステム規格（ISO14001）がある。

個人情報保護マネジメント監査の位置づけ

P(計画)
3.2個人情報保護方針
3.3計画
　3.3.1個人情報の特定
　3.3.3リスク分析～
　3.3.7緊急事態への準備

D(実施)
3.4.1運用手順
3.4.2取得、利用及び提供に関する原則
　3.4.2.1利用目的の特定～
　3.4.2.4個人情報の取得～
　　3.4.2.8提供に関する措置
3.4.3適正管理
　3.4.3.1正確性の確保～
　　3.4.3.4委託先の監督
3.4.4個人情報に関する本人の権利
　3.4.4.1個人情報に関する権利～
　　3.4.4.7開示対象個人情報の利用
　　又は提供の拒否権
3.4.5教育
3.5PMS文書
　3.5.1文書の範囲～ 3.5.3記録の管理
3.6苦情及び相談への対応

C(点検)
3.7点検
　3.7.1運用の確認　3.7.2監査
3.8是正処置及び予防処置

A(見直し)
3.9事業者の代表者による見直し

継続的改善

情報資産の保護とコンプライアンス監査

- 著作権法の侵害行為
- インターネット取引の対応
- 不正競争防止法の侵害行為
- コンピュータウイルスを悪用した犯罪

【ポイント】
　情報システムに関連する法的な問題は経営者自身の無知、従業者の無知、考慮不足等による違法行為が多い。コンプライアンスに視点をあてたシステム監査が重要であり、監査での助言・勧告のみならず、緊急改善が求められることが多発している。

【事例】ソフトウェア不正コピーの重大事件

■ 1996年9月，大阪市のソフトウェア会社が，マイクロソフト社，ロータス社，ジャストシステム社の三社に対して**不正複製**で，総額約1億4000万円の損害賠償金で和解が成立
正規ソフトウェア金額を上まわる和解金の支払に同意した。

■ 2001年5月，マイクロソフト社，アップルコンピュータ社，アドビシステム社の三社が，**パソコン用業務ソフトウェアを不正に複製**したとして，東京の司法試験予備校に1億1000万円の損害賠償を求め提訴した。
東京地方裁判所は「正規品の小売価格を同額の約8500万円の支払いを命じた。

■2007年4月に大阪府の財産法人が約7年間、**パソコンソフトを違法に327本分コピーして使用**し、マイクロソフト社、アドビシステム社、オートデスク社の三社から数千万円の損害賠償を求められた。

■2009年11月に北海道庁で職員らが使うパソコン約2万4千台から、マイクロソフト社他の**ソフトウェア約4650本が違法にコピー**していたことが判明した。このうち約4000本がマイクロソフト社で、道庁は今後も使用する3200本分のソフトを1億4千万円で購入することで同社と和解した。

ビジネス情報に関連した著作権侵害行為例

■一般的侵害行為
- 無許可で他人の著書や写真、絵、音楽等をコピーしたりしてHPに掲載（注：自由利用の範囲を超えている場合）
- 海賊版としりながらの「販売・配布・貸与」する行為
- 販売・配布・貸与を目的としての「所持」も侵害行為（１１３条）
- 電子透かしなど権利管理情報を不正に削除・変更など

■企業や組織内での違法行為
- ソフトウェアの許諾（ライセンス）数以上のインストール
- 海賊版のコンピュータ・プログラムを会社のパソコン等で「業務上使用」（使用する権原を得たときに海賊版と知っていたときに限られる）（第１１３条２項）
- 無許可で著書や新聞を複製し配布、広報誌等の掲載
  最近では「DeNA事件」がある（事例参照）

■その他　小説の改ざん、著作者の名誉を害する行為等

【ポイント】
著作権問題は企業や組織ぐるみの犯罪行為を引き起こすことがある。違法性の認識も薄い場合が多い。コンプライアンス監査の実施が求められる。

【事例】DeNA事件

IT大手のディー・エヌ・エー（DeNA）は2016年11月29日、ヘルスケア情報を扱う医療系サイトの「WELQ」に掲載していた全ての記事を、同日21時に非公開にしたと発表した。理由については、「医療情報に関する記事の信憑性について多数の意見が寄せられた」ことである。12月1日には、子育てや旅行、グルメなどに関する8っつのサイトを、**無断転用**の恐れがあるとして、公開をやめると発表した。

同社の調査では、マニュアルや外部ライターへの指示で、他サイトからの無断転用の推奨と読み取れる点が確認されたこと、原稿の正確性などについて「一切負わない」としていたなど、**公開を継続することはできないと判断し、メディア運営の抜本的に見直すとしている**。

東京都は、同社の化粧品や健康食品の原稿に誇大広告とみなせる内容があり、「医療品医療機器法違反（誇大記述広告）」の疑いで調査を始めた。
（参考引用：読売新聞　平成28年12月2日付、12月8日付記事）

【ポイント】 他人の著作物の転用は、著作権法上の問題がおこることもあり、また、誇大広告では、景品表示法等の問題がおこることもある。組織的な「**情報倫理**」「**企業倫理**」の欠如といえよう。

インターネット取引での法的対応

サイバーショッピングをモデルに

ビジネスプロセスの法律

取引のビジネス・プロセスからの法的問題の検討

■ インターネット取引（サイバーショッピング）でのビジネスプロセスでの機能と法的問題となる事項の整理

① Webによる広告・宣伝プロセス

- 消費者に分かりやすい，安全で信頼されるWebサイトであること
  そのためには，消費者が知りたい情報を的確に分かり易く表示すること
- 消費者に法的責任が及ばない電子商取引が実現できる手続であること

② 通信による契約プロセス

- 間違いなく発注でき，間違いが気付いたら訂正と取り消しができること
- 消費者を対象としたビジネスでは，入力情報を確認してから契約となること

③ 受注商品の発送（引渡）プロセス

- 商品の速やかな発送。コンテンツ商品は迅速な送付（送信）であること

④ 決済プロセス

- 商品の発送とともに請求（原則，未払リスクは事業者のリスク）がくること
- 商品の破損，瑕疵，返品等は事業者の責任で実施されること

⑤ その他，Webサイトの安全性確保

- 情報システムのダウン，プログラムバグのないシステムであること
- 個人情報保護対策，不正アクセス対策などの万全のセキュリティ対策があること

取引のビジネス・プロセスからの主な法律・制度等（一例）

ビジネス・プロセス	内　　容	主な法律・制度等
①Web広告・宣伝	適法ホームページの作成 商品の掲載（申込の誘引） 著作物の再利用 取扱い不能商品の販売 個人情報利用の目的等	著作権法／景品表示法 特定商取引法／金融商品販売法， 古物営業法，刑法（猥褻物，富くじ罪）， 不正競争防止法、薬事法ほか 「販売業者」に係るガイドラインほか
②通信による契約	発注手続きの正確化 （契約の成立，取り消し等） 暗号による個人情報保護	民法特例法／消費者契約法 電子署名・認証法 ほか
③商品発送	コンテンツのダウンロード 配送，郵送等	著作権法，電気通信事業法ほか 瑕疵による返品，ライセンス商品
④決済	電子決済，振込み， クレジット，代引き他	不正アクセス禁止法／刑法 預金者保護法／エスクロー制度他
その他	情報管理，クレーム受付， プイラバシー保護等	プロバイダ責任制限法，個人情報保護法など

広告・宣伝にける法的問題と論点（１）

Webページやメールでの広告・宣伝

（１） 特定商取引（旧訪問販売法）による規制

訪問販売，通信販売等，消費者トラブルを生じやすい特定の取引類型を対象に，事業者の行為を規制する行政上のルールを定め，消費者取引の公正を確保

（改正法13年6月1日，平成14年7月1日，平成16年11月11日施行）

- ☞インターネットビジネスは通信販売（法2条2項）となる
- ☞「！連絡方法無！」は認められない。受取後の再送禁止
- ☞誇大広告の禁止，不実勧誘の禁止，規制逃れの防止等
- ☞ファクシミリ広告への規制

  ファクシミリ広告を請求等していない消費者へのファクシミリ広告の禁止（オプトイン規制）

  ☞ 個人は300万円以下の罰金か2年以下の懲役，法人は3億円以下の罰金

（２） 景品表示法による規制

- ☞インターネットビジネス事業者が，消費者が優良誤認するような商品の掲示（法第4条第1号）
- ☞「医学理論に基づき，楽々5～6kg減量，食事制限なし」など学問的根拠のない表示
- ☞ブロードバンド通信で「通信速度10Mbps」と表示，実際には場所，設備状況で変わることを表示していないことなど
- ☞Web上の懸賞企画（オープン懸賞）は景品表示上の規制対象とならないが，商品がサービスを購入しなければ懸賞に応募できない企画は，取引付随性があり，規制の対象

2. 広告・宣伝にける法的問題と論点（２）

（３） **著作権法による規制**

☞他人の絵や写真，音楽の著作物が広告・宣伝に不法使用

☞雑誌や新聞の記事，写真，絵をHPに不法使用

（４） **消費者契約法等による規制**

☞事業者の責任を制限する条項に対する規制

・債務不履行責任，不法行為責任，瑕疵担保責任等の責任を全面的に免責する条項は無効

（５） **不正競争防止法による規制**

☞ 企業等の**営業秘密（企業秘密等）**に関する不正に取得・開示するなど

☞ コンテンツ（映像・音等）にかけられている技術的保護を無効にする装置の譲渡等

☞ **ブランド企業と間違えるドメイン名の不正登録等**

☞ 商品の表示において品質・内容等の誤認させるような記載等

（６） **その他個別の法（薬事法、児童買春・児童ポルノ法、刑法等）による規制**

☞ 売ってはいけない商品がある：

ポルノ，鉄砲，ニセモノ（偽情報），劇薬，宝くじ，賍物品（盗品）の販売など

☞ 有名タレントの写真を掲載：**パブリシティ権の侵害**

❒ ウェブサイトの利用規定の有効性

☞利用者がサイト利用規定に同意の上での申し込みは有効といえる

☞消費者契約法等，**消費者の利益を一方的に害する条項は無効**

電子メール広告規制の内容

【平成20年改正：オプトアウト規制からオプトイン規制へ】

■ ネット販売事業者（ネットショップ）及び電子メール広告受託事業者等の「電子メール広告」に関して、「オプトアウト規制」から「オプトイン規制」に平成20年6月改正、同年12月1日施行。

1. 規制対象の「電子メール広告」

「通信販売」、「連鎖販売取引」、「業務提携誘引販売取引」の商品や役務などの「電子メール広告」が対象となる。

2. 規制の対象者

消費者と直接契約するネット通販事業者はもちろんのこと、ネット通販事業者から電子メール広告に関する業務を「一括して受託」している「電子メール広告受託事業者」も対象となった。

【注】 一括受託とは：

- 消費者から電子メール広告送付について「請求や承諾」を得る業務
- 消費者からの請求や承諾の「記録を作成し保存」する業務
- 送信する電子メール広告に、消費者が「受信拒否の意思を表示するための方法や連絡先を表示」する業務

3. 規制内容

① 請求や承諾を得ていない電子メール広告の原則禁止（オプトイン規制）
② 電子メール広告の送信を拒否する方法の表示義務と、拒否した消費者への送信禁止
③ 消費者からの請求や承諾の記録の保存義務（広告を行った日から3年間）
④ 罰則強化（刑事罰と行政処分がなされる）

民法特例法による契約の成立と錯誤

❒**電子消費者契約民法特例法**（平成13年12月25日施行）

（正式名「電子消費者契約及び電子承諾通知に関する民法特例に関する法律」）

■　電子商取引における消費者の操作ミスの救済

☞BtoCの電子契約では消費者の申込み確認措置が必要

☞民法95条「要素の錯誤」に該当。但書の「重大な過失があるときは無効の主張ができない」が原則適用されない

■電子商取引等における契約の成立時期の転換

☞承諾通知が申込者に到着した時点で成立（到達主義）

到達：通知情報が相手方のいわゆる支配圏内に置かれた時点

①電子メールの場合：

承諾通知がメールサーバの中に読取可能な状態で記録された時点

②Web画面の場合：

Web画面に承諾通知が表示された時点

■留意事項

☞ CtoC（オークション），電子メール申込み等は適用外

インターネット取引での法的対応

インターネット「ドメイン名」事件

不正競争防止法関連事件

【事例】インターネット「ドメイン名」事件

■インターネット上の実質的な住所にあたる「ドメイン名」に自社の登録商標を使われるなどとして、営業上の利益が侵害される恐れがあるとして、大手信販会社「ジャックス」（本社：北海道函館市）が簡易組み立てトイレ販売会社「日本海パクト」（本社：富山市）を相手取り、不正競争防止法に基づき、**ドメイン名使用の差し止め**などを求めた民事訴訟判決が、平成12年12月6日に富山地裁で言い渡された。裁判長は、「ドメイン名の使用が不正競争行為にあたり、原告の営業上の利益が侵害される恐れもある」とした。

■　大手スーパーのイトーヨーカ堂の社名を使ったインターネットのドメイン名を同社と無関係の会社が不当に登録、使用したとして、仲裁センターは、この会社にドメイン名登録をイトーヨーカ堂に移転するよう命ずる裁定を下した。
　問題のドメイン名は「itoyokado. co. jp」で、神奈川県内の不動産会社が1999年に登録し、ホームページを開設した。その後、ホームページ上にドメイン名を「お譲りします」などと掲示したほか、2000年11月には「最低落札価格十億円」としてネットオークションに出品した。

■　ソニーがドメイン名「sonybannk. co. jp」を無断で取得を無断で取得されたとして、その明け渡しを求めていた問題で、仲裁センターは、ドメイン名を取得していた新潟県長岡市の投資コンサルタント会社に対し、名義の移転を命じる裁定を下した。

【事例】不正競争防止法での話題事件と判決

紛争事件	内容	判決
動くかに看板事件	有名かに料理屋の名物「動くかに看板」と類似したかに看板を使用した同業者に対し，看板の使用禁止及び損害賠償が認められた（１号）	大阪地裁判決 昭和62年5月27日
iMac事件	米アップルコンピュータの日本法人等が同社のヒット商品のパソコン「iMac」のデザインを違法に模倣されたとして、日本法人のソーテックを相手に同社のパソコン「e-One」の製造販売等の差止を求めて認められた（１号）	東京地裁判決 平成11年9月20日
男性用かつら顧客名簿事件（４号）	勤めた者が，退職後大阪市内で男性用かつらの製造・販売業を退職する際，顧客名簿をコピーし不正に取得。自己の営業後，理髪，かつらの受注した。不正取得し名簿の廃棄及び損害賠償を命じた。	大阪地裁判決 平成8年4月16日
「ジャックス」ドメイン名不正登録事件	大手信販会社「ジャックス」が簡易組み立てトイレ販売会社「日本海パクト」を相手取り、不正競争防止法に基づき、ドメイン名の使用差し止めされた。	富山地裁判決 平成1年12月6日
その他	本みりんタイプ調味料事件（１３号） ミートホープ事件，船場吉兆事件，うなぎ虚偽表示事件（以上１３号）	昭和４９年 平成１９年～現在

不正競争行為とされる行為の類型（ICT関連）

1．周知表示混同惹起行為（2条1項1号）

他人の氏名、商号、商標など（商品等表示）として需要者に広く認識されているものと同一、または類似の表示をしたり、そのように表示した商品を譲渡などして、他人の商品または営業と混同させる行為

2．著名表示冒用行為（2条1項2号）

他人の著名な商品等表示と同一または類似のものを自己の**商品名等表示**として使用したり、そのように表示した商品を譲渡などする行為

3．商品形態模倣行為（2条1項3号）

他人の商品の形態を模倣した商品を譲渡などする行為

4．営業秘密に関する不正行為（2条1項4号～9号）

営業秘密を不正に取得したり、不正に取得した営業秘密を使用・開示したり、正当に取得した営業秘密を不正な利益を図る目的または営業秘密の保有者に損害を与える目的で使用・開示する行為など

5．コンテンツ（映像・音等）にかけられている技術的保護を無効にする装置の譲渡等（2条1項10号～11号）

映像・音・プログラムにかけられたアクセス制限やスクランブル（暗号化）、コピーガードを無効化する機能のみを有する装置等を譲渡などする行為

6．ドメイン名の不正登録等（2条1項12号）

不正な利益を受ける目的または他人に損害を与える目的で、他人の氏名、商号、商標などと同一・類似のドメイン名を使用する権利を取得、保有する行為、またはドメイン名を使用する行為

以下、省略

コンピュータウイルス関連事件

コンピュータウイルス作成罪

パソコン遠隔操作事件

コンピュータウイルス作成の犯罪

■ コンピュータウイルス作成者を「著作権法違反」で逮捕

2008年1月24日、京都府警はアニメ画像に無断で**コンピュータウイルス（原田ウイルス）**を埋め込み、インターネットで流出させたとして、大阪府の20歳の大学院生Nを逮捕した。Nは2007年の10月～11月に、他人の著作物である人気アニメーション「LANNAD-クラナド」の画像にコンピュータウイルスを組み込んで、ファイル交換ソフト**「ウイニー（Winny）」**のネットワーク上で配信し、**著作権法に違反（公衆送信権侵害等）**した。

■ コンピュータウイルス作成者を「**器物損壊罪**」で逮捕

2010年8月4日、警視庁は、音楽ファイル等を装ったコンピュータウイルス（イカタコウイルス）を作成し、感染したパソコンファイルを破壊したとして、大阪府のNを、**器物損壊容疑**で再逮捕した。Nは、上記事件で執行猶予中であった。

■ これらの事件を背景に、コンピュータウイルスを作成したり、配布する行為を犯罪とする**刑法の改正**となった。

コンピュータウイルス作成罪の成立

■ **不正指令電磁的記録に関する罪（コンピュータウイルス作成罪）**は、コンピュータに不正な指令を与える電磁的記録の作成する行為等を内容とする犯罪（刑法168条の2及び168条の3）。2011年6月17日（同年7月施行）の刑法改正で新設された犯罪類型である。いわゆるコンピューターウイルス（以下、ウイルス）を悪用した犯罪などを取り締まるための刑法改正。

■ 正当な理由がないのに、無断で他人のコンピューターにおいて実行させる目的で、**ウイルスを「作成」したり「提供」したりした場合**には、3年以下の懲役または50万円以下の罰金となる。

■ また、正当な理由がないのに、**無断で他人のコンピューターにおいて実行させる目的で、ウイルスを「取得」または「保管」した場合**には、2年以下の懲役または30万円以下の罰金となる。

■ **ウイルス作成・提供罪**は（１）正当な理由がないのに、（２）無断で他人のコンピュータにおいて実行させる目的で、ウイルスを作成・提供した場合に成立する。ウイルス対策ソフト開発などの目的でウイルス的プログラムを作成する場合などは該当しないとしている。また同罪は故意犯であり、プログラミングの過程で**誤ってバグを発生**させても犯罪にはならない。

情報資産の保護とコンプライアンスのシステム監査

ICTの高度活用は、情報に関連して知的財産の侵害の恐れがでてくる。**コンプライアンス監査**が求められる

■ ソフトウェアライセンス契約は、ソフトウェアの使用許諾の契約である。**ライセンス契約本数以上のソフトウェアのダウンロードや不正コピー**は、違法行為であり、発覚すると企業や組織の名誉(レピュテーション)と信頼の低下を招くことなる。
ソフトウェア資産台帳による、徹底管理と不正使用のチェックの仕組みとその**適正な運用のシステム監査**が求められる。

■ 企業・組織等での広報活動は、ホームページの作成が必須である。作成にあたっては、**他人の著作物の無断転用や無断掲載**は、違法行為となる。

■ インターネット・ドメインの不正登録、営業秘密となる情報等(例えば、顧客情報)に不正は持ち出し、商品形態の模倣など、**不正競争防止法**に違反する行為となる。

■ 企業や組織のなかでコンピュータウイルスを作成し、配布するような行為が起こっている。他人の**スマートフォンの内容を覗き見る行為**等も違法行為となる。徹底した**コンプライアンスの社員教育と監査**が重要になる。

コンピュータウイルス対策の実施状況監査

■ **コンピュータウイルス対策基準**は、平成7年7月7制定。平成9年9月24日、平成12年12月28日に最終改定されている。

本基準は、コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたものである。システムユーザ基準、システム管理者基準、ソフトウェア供給者基準、ネットワーク事業者基準及びシステムサービス事業者基準から成る。

記載項目は、コンピュータ管理、ネットワーク管理、運用管理、事後対応、教育・啓蒙、**監査**である。監査は現在ともに、これからもますます重要となる。

出典：経済産業省：http://www.ipa.go.jp/security/antivirus/7kajonew.html

■ **ウイルス対策7か条**：独立行政法人 情報処理推進機構

- メールの添付ファイルは、開く前にウイルス検査を行うこと
- ダウンロードしたファイルは、使用する前にウイルス検査を行うこと
- アプリケーションのセキュリティ機能を活用すること
- セキュリティパッチをあてること
- ウイルス感染の兆候を見逃さないこと
- ウイルス感染被害からの復旧のためデータのバックアップを行うこと
- 最新のウイルス定義ファイルに更新しワクチンソフトを活用すること

【ポイント】

ウイルス対策の実施状況の監査は、これからも必須となる。

パソコン遠隔操作事件

大手IT企業のAは、2012年(平成24年)の7月から8月にかけて、他者のパソコン(PC)を**遠隔操作**し、これを踏み台として襲撃や殺人などの犯罪予告を行ったサイバー犯罪事件である。事件で使用されたコンピューターウイルスの**トロイの木馬**の一種「iesys.exe」をPCに感染させ2ちゃんねるや大阪市HPなどに犯罪予告の書き込みを行った事件。神奈川県警、大阪府警、警視庁、三重県警が遠隔操作を見抜けず、それぞれPCの持ち主だった**男性4人を誤認逮捕**した。

Aは**威力業務妨害**や**ハイジャック防止法違反**などの罪に問われた。東京地裁裁判長は、「見ず知らずの第三者を犯人に仕立て上げるなど、サイバー犯罪の中でも悪質な犯行だ」として、懲役8年(求刑懲役10年)を言い渡した。

参考文献:パソコン遠隔操作事件　ウィキペディア
https://ja.wikipedia.org/wiki　アクセス　2016. 12. 20

スマホ遠隔操作の一斉摘発

2016年11月に無断で交際相手のスマホに遠隔操作ソフト「アンドロイドアナライザー」を仕込んだ男が「**不正指令電磁的記録供用罪**」で起訴されるとともに、作成販売した横浜市の「インターナル」の会社社長も「**不正指令電磁的記録作成罪**」で起訴された。

のぞき見するためには、スマホ所有者の目を盗んでインストールする必要がある。同社は、ホームページでインストールするとスマホに通知されるとうたい、不正防止を施しているとしていたが、実際には通知されないように設定できたという。被害者はインストールされたことに気付いていない。

（出典：読売新聞　2016年11月26日付記事）

ウイルスの作成やバラマキ防止の法改正は後追いとなる。また、「**情報倫理**」の問題でもあり、**幼い頃からの教育**が必須なる。

ストーカー行為等の規制等に関する法律

2016年5月に発生した小金井市女子大生ストーカー刺傷事件を受けて、「ストーカー行為等の規制等に関する法律」の改正案が2016年12月6日に可決、成立し、一部は2017年1月3日に施行された（その他は、成立から6ヶ月以内に施行予定）。

ストーカー行為等の規制等に関する法律は、2000年（平成12年）11月24日に施行された。当初、規制対象となる行為を、公権力介入の限定の観点から、恋愛感情などの好意の感情に基づくものに限定されていた。しかし、その後、SNS（ Social Networking Service）への執拗な書き込みやスマートフォンの中身をのぞき見できる遠隔操作ソフトウェアやアプリケーションによる被害が多発していた。 TwitterやLINE等のSNS等でのメッセージの連続送信や、個人のブログへの執拗な書き込みを、つきまとい行為に追加、罰則の強化とともに「非親告罪」等とした。

求められるコンプライアンスの監査の重要性

ICTの高度化すると、情報システムの多様化がおこり、**コンプライアンス監査が**より求められることになる。

企業や組織のなかで、コンプライアンス問題の対策として、コンプライアンスの監査に期待されるが、対策としては難しい問題である。その理由として以下のことがあげられる。

- 情報は**無形の財産**（知的財産）であり、無形であることで価値の認識や使用・移転等の手続き忘れ等により、知的財産の侵害の恐れがでてくる。
- ICTの高度活用は、情報システムを戦略的に活用することになり、法的な問題に気がつかないことや法的な問題を分析せずに開発をすることが多くなる。
- 企業等でのコンプライアンスへの侵害行為は、**個人でも起こしやすい**。個人が起こした問題であっても、その被害や責任は計り知れないものとなる。そして、**責任は企業等で負うことになる**。
- コンプライアンの問題は、決してICTに関連したことのみではない。企業法務全体に関連することであるが、ICTに関連した監査は「**法とICT**」の両面からアプローチする必要があり、**システム監査人**が実施することになる。

これから求められる監査技術の進化への対応

■ デジタルフォレンジック技術

PCデータの復元・解析

■ 精査⇒試査⇒AIよる精査と分析

データ改竄事件

大阪地検特捜部主任検事証拠改ざん事件

2010年(平成22年)9月21日に、大阪地方検察庁特別捜査部のM主任検事が、障害者郵便制度悪用事件で証拠物件のフロッピーディスクを改竄したとして証拠隠滅の容疑で逮捕された。同年10月1日には、当時の上司であった大阪地検元特捜部長O及び元副部長Sが、主任検事による故意の証拠の改竄を知りながら、これを隠したとして犯人隠避の容疑で、それぞれ逮捕された事件である。

この事件がきっかけとなって、**デジタルデータの証拠調査し消されたデータを復元するデジタルフォレンジック技術により、証拠データを抽出**した。

【参考文献】 AOS フォレンジック調査 https://fss.jp/ 2016.12.18

デジタルフォレンジックスと監査

デジタルフォレンジクス（Digital Forensics）は、コンピュータ自身のハードディスクや、CD-ROM、フロッピーディスク等の電子機器に残る記録媒体のデータを収集・分析し、その法的な証拠性を明らかにする技術である。コンピュータやデジタル記録媒体の中に残された法的証拠に関わるデジタル的な法科学（Forensic Science）の一分野である。

デジタルフォレンジクスの目的は、コンピュータ・システム自身やハードディスクドライブまたはCD-ROMのような記録媒体、電子文書中のメッセージやJPEG画像のような、デジタル製品の最新の状態を明らかにすることである。

デジタルフォレンジクスは、不正アクセスや機密情報漏洩など、コンピュータや通信ネットワークに直接関係する犯罪における捜査手法として注目されているが、企業や組織になかでも、ICTの高度利用にともなって、外部からの新入やデータの改竄がないか、システム監査の証拠集め、情報セキュリティ監査や安全対策の面からも、今後重要な技術となってくる。

【参考文献】

「デジタルフォレンジックス」「e-Words」 http://e-words.jp/ 2016.12.18

不正会計事件：オリンパス／東芝

■　オリンパス事件

2011年（平成23年）7月、雑誌FACTAの調査報道によるスクープした「オリンパスの巨額の損失事件である。オリンパスは、「飛ばし」という手法で、損益を10年以上の長期にわたって隠し続けた末に、**負債を粉飾決算で処理した事件**である。実は、オリンパスは、バブル崩壊時に多額の損失を出したが、歴代の会社首脳はそれを知りつつ、公表していなかった。例を見な非常に長期にわたる「損失隠し」だった。同社はこれを会計処理するために、2008年に実態とかけ離れた高額による企業買収を行い、それを投資失敗による特別損失として計上して減損処理し、本当の損失原因を**粉飾**しようとした。

■　東芝事件

2015年（平成27年）で最大の経済事件といえば、東芝の**不正会計問題**である。5月に突然、第三者委員会を設置すると発表して以降、ズルズルと決算発表を遅らせ、7月に調査報告書が発表されると会長、社長ほか取締役8人が即日辞任。最終的に過去7年間の決算で税引き前利益を合わせて2248億円もかさ上げしていたことが明らかになった。12月には金融庁が過去最高となる73億円の課徴金命令を下した。

出典：オリンパス事件　ウィキペディア　https://ja.wikipedia.org/wiki　アクセス：2017.1.10
出典：東芝不正会計　ハーバービジネスオンライン　https://hbol.jp/74656　アクセス：2017.1.10

会計監査手法の進化（AIによる精査）

■ EDP監査時代（監査初期）：**精査**

会計データの全件をリストアップして、母集団を**精査**

■ 近年から現在：**試査から精査へ**

CAAT（Computer Assisted Audit Techniques）はコンピュータ利用監査技法を活用して監査を実施する。企業や組織内のデータは、大部分が電子データとして管理されており、IT技術を活用することにより短時間で、データの分析や不正の兆候を発見できる。監査を実施する際の手法に監査データを**サンプリング（試査）**によって実施する。

母集団を試査するが、ITを利用して母集団全体を**精査的手法**により検証になってきている。

■ 今後（将来）：**AIによる精査と分析**

AI（人工知能）による**精査的手法に進化**する。異常な取引の特性の要件定義を行い、その要件に該当する取引の識別をおこなって見えないリスクまで識別する。また、期末や期中の監査を待たず、AIにより常時監視される「継続的監査」（Continuous Auditing）が実施される。

これからのIoT時代に備えて
IoTセキュリティの監査
をどのように考えるのか

ーIoT開発におけるセキュリティ設計の手引きを参考にしてー

IoTのセキュリティの現状と課題

IoTを情報の流れと構成からみると、「モノ」(Things:デバイス(機器)やシステム等)がネットワークと接続し、それを介して情報のやり取りをし、「モノ」に対しては情報やサービスが提供される。「モノ」をPCに置き換えてみれば、一般的なインターネットシステムと構造的には何ら変わらない。従って、これまで情報セキュリティで培われてきた技術を活用して対策することになる。ただ、IoTの描く世界では、以下のような固有の様々な課題が存在しており、それらが対応を困難にしている。

(1) ネットに繋がる脅威をこれまで考慮してなかった分野の機器の接続が想定される
(2) 生命に関わる機器やシステムが繋がることが想定される
(3)「モノ」同士が、無線等で自律的に繋がることが想定される
(4)「モノ」のコストの観点から、セキュリティ対策が省かれることが想定される
(5) ネットを介して収集される情報の用途は、「モノ」側では制御が困難であり、バックエンドにあるシステムやクラウドサービス側での管理範囲となる
(6) つながる世界を拡げていくためには、「モノ」同士の技術的(通信プロトコル、暗号、認証等)、およびビジネス的な約束事が不可欠となってくる

この内、課題(1)(2)(3)(4)については、「モノ」におけるセキュリティ対策を「モノ」の開発者が考えることになるが、
課題(5)(6)に対しては、様々な分野の事業者の連携や業界基準、あるいは個人情報やプライバシー情報の取り扱いなどにおいては制度や規制が必要になってくる

引用文献:独立行政法人情報処理推進機構 「IoT開発におけるセキュリティ設計の手引き」 2016年5月

ガイドラインは、IoT機器やシステム、サービスの提供にあたってのライフサイクル（方針、分析、設計、構築・接続、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの。
各指針等において、具体的な対策を要点としてまとめている。

工程	指針	主な要点
方針	IoTの性質を考慮した基本方針を定める	・経営者がIoTセキュリティにコミットする ・内部不正やミスに備える
分析	IoTのリスクを認識する	・守るべきものを特定する ・つながることによるリスクを想定する
設計	守るべきものを守る設計を考える	・つながる相手に迷惑をかけない設計をする ・不特定の相手とつなげられても安全安心を確保できる設計をする ・安全安心を実現する設計の評価・検証を行う
構築・接続	ネットワーク上での対策を考える	・機能及び用途に応じて適切にネットワーク接続する ・初期設定に留意する ・認証機能を導入する
運用・保守	安全安心な状態を維持し、情報発信・共有を行う	・出荷・リリース後も安全安心な状態を維持する ・出荷・リリース後もIoTリスクを把握し、関係者に守ってもらいたいことを伝える ・IoTシステム・サービスにおける関係者の役割を認識する ・脆弱な機器を把握し、適切に注意喚起を行う
一般利用者のためのルール		・問合せ窓口やサポートがない機器やサービスの購入・利用を控える ・初期設定に気をつける ・使用しなくなった機器については電源を切る ・機器を手放す時はデータを消す

引用文献：IOT推進コンソーシアム　総務省　経済産業省　「IoTセキュリティガイドライン１．０概要」 平成２８年７月

「セキュリティ品質」の定義化と工程監査

■ IoTには現状と課題から品質管理に「**セキュリティ品質**」を定義化し導入する

■ ライフサイクル（方針、分析、設計、構築・接続、運用・保守）のけるセキュリティ管理基準を策定し、ライフサイクルでの工程ごとに「**工程監査**」を実施する

・工程監査：方針、分析、設計、構築・接続、運用・保守の各工程で監査を実施することと定義する

・品質マネジメントでは、監査はPDCAでのC（Check）に位置づけられているが、IoTの監査ではライフサイクルでの各工程（方針、分析、設計、構築・接続、運用・保守）での問題点等洗い出しや分析をおこなう。そして、A（Action）において**管理基準の改訂**をおこなう

■ セキュリティ管理基準は、**企業内と業界で統一的**に作成する

これからの監査の課題

- 視野の狭い「脆弱性」
- 監査基準の改訂と
  時代のサブコントロール基準

これからの監査の課題（１）

高度情報化時代に視野が狭い「脆弱性」

- ICTの脆弱性のみが「脆弱性」ではない
- ICTの脆弱性から多様化した脆弱性へ

一般的な定義の脆弱性
視野が狭い脆弱性の定義

■ 脆弱性(vulnerability)とは、コンピュータのOSやソフトウェアにおいて、**プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥**のことをいう。脆弱性は、セキュリティホールとも呼ばれている。脆弱性が残された状態でコンピュータを利用していると、不正アクセスに利用されたり、ウイルスに感染したりする危険性がある。

■ セキュリティホール は、脆弱性についての俗表現である。**最も多い脆弱性はソフトウェアのバグや仕様上の欠陥によるもの**で、脆弱性が発見されると開発者により修正プログラムが提供されることが多い。システムを安全に保つにはこまめにこうした修正プログラムを適用することが重要となる。

■ 情報セキュリティに対する脆弱性となるのはシステム上の問題点だけでなく、機密情報の管理体制が整っていないなどといった人間の振る舞いに関する問題点も脆弱性となりうる。こうした**脆弱性をシステム的なものと区別して「人為的脆弱性」**と呼ぶこともある。

出典:
① 総務省ホームページ:脆弱性とは
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/11.html
② e-words:脆弱性 http://e-words.jp/w

新たな情報システムの脆弱性の定義とその分析

「情報資産や人員の管理方法に由来する弱点」(ISMS)
ISMS:Information Security Management System (JIPDEC)

「情報資産の中や周辺環境，管理体制，制度のなどに内在し，損失を発生しやすくさせたり，拡大化させる要因」(上原孝之)

■ 情報システムの脆弱性とは、情報システムの構築に伴い、その「効用」に比して不可避的に発生し、潜在化する「欠陥」である。

■ 無限に拡大化と進化する情報化により、「脆弱性」は変化と拡大化を繰り返し、予期できない脅威の実現の要因となる。

■ 「脆弱性」はシステム固有に存在し、脅威の実現の可能性(リスク)に繋がる

■ 「システム監査」や「リスク・マネジメント」では脆弱性分析からはじめなければならない。狭い脆弱性の視点では、監査は不適切になる。

(出典:松田貴典著「情報システムの脆弱性」白桃書房 1999)

ITの脆弱性に起因して4つの側面の脆弱性

情報技術／経営管理・組織管理／国際・社会的／法・倫理

■情報システムの脆弱性は，ITの本質的な特性に起因して，無知，無法，無規制，無対策等の**コントロール（統制）**欠如とマネジメント（管理）の失敗で**「脆弱性」**が発生する

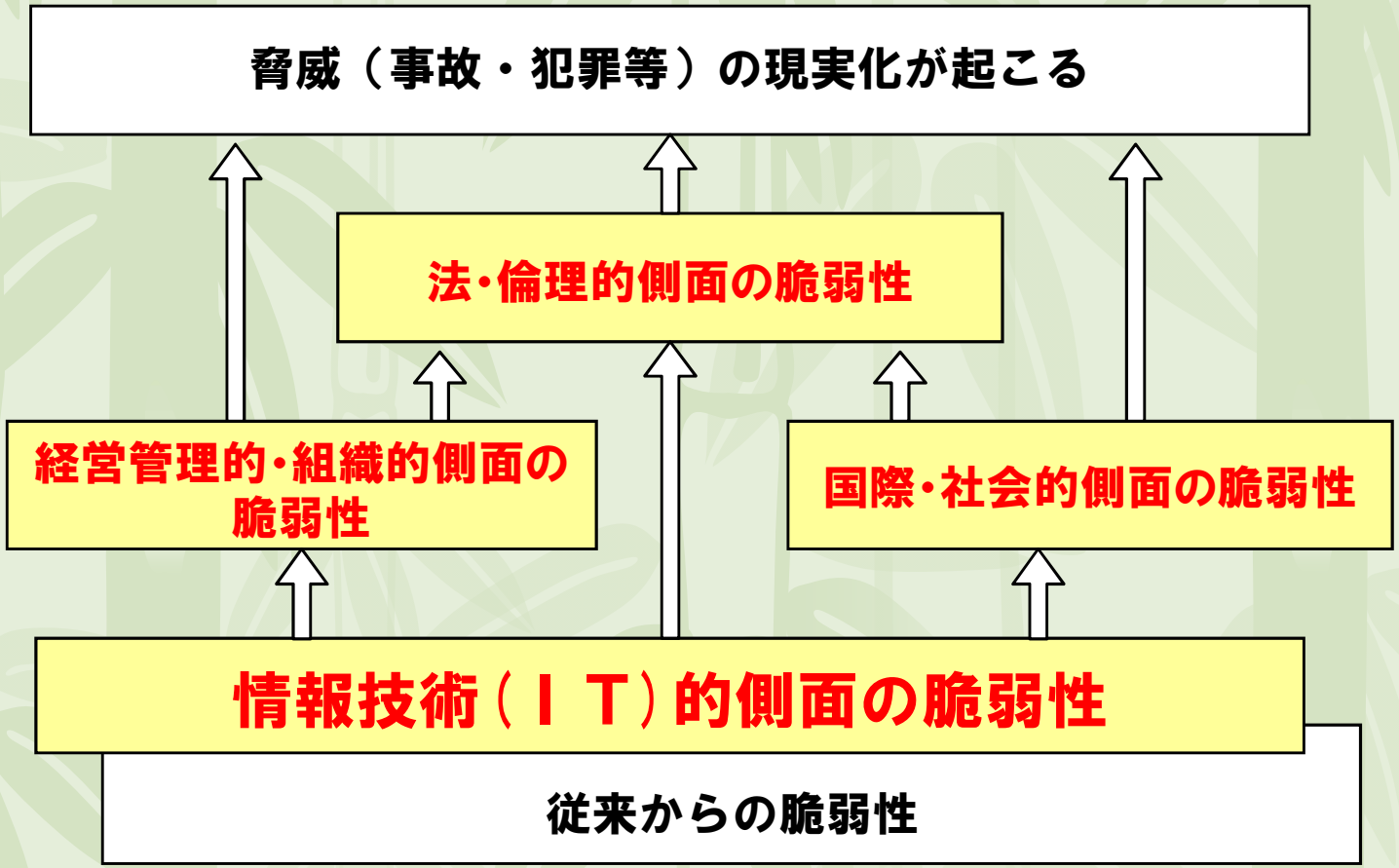
■脆弱性は，**脅威の現実化（顕在化）の誘因**となる。

■脆弱性には，**①情報技術（IT）的側面，②経営管理・組織的側面，③国際・社会的側面，④法・倫理的側面**があり、潜在化する。

■脆弱性は，通常にコントロールされているが，このコントロールの強弱で脅威の現実化（顕在化）する**「リスク」**が発生し，高くも低くもなる。

■脆弱性のントロールが弱い間隙（例えば，ネットワークの弱い個所）をついて**「脅威の現実化の誘引」**となり，**「被害」**が発生する。この被害の大きさが問題となる。すなわち，脆弱性のコントロールは，被害の発生を**抑制・防止し，その大きさを極小化**することにある。

新たな四つの脆弱性側面の提言とその階層関連



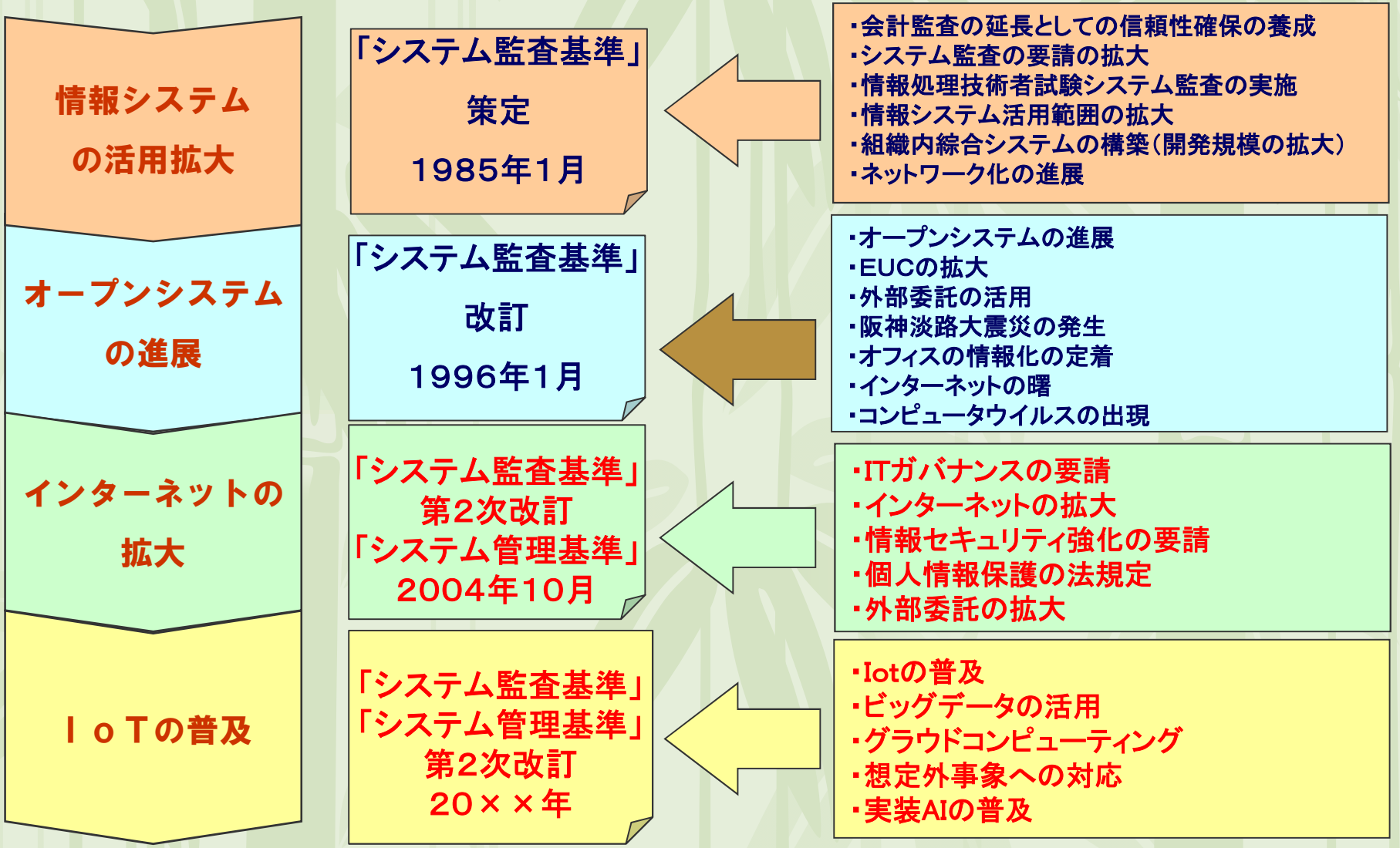
これからの監査の課題（２）

これからの時代にもシステム監査基準・管理基準はさらに重要となる

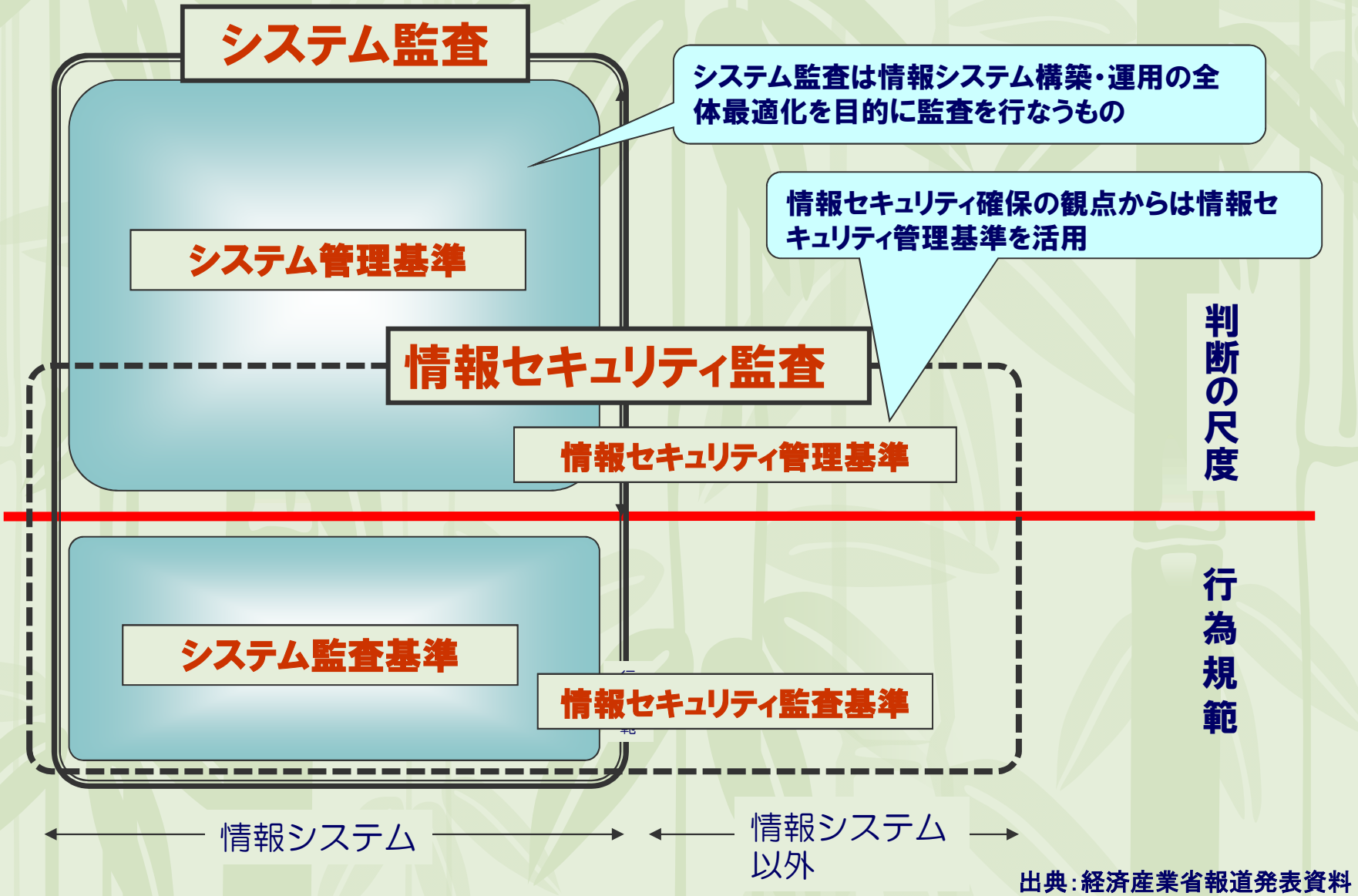
- システム管理基準の改訂
  サブコントルールの作成が重要
- 経営者の寄り添ったシステム監査

システム監査基準・管理基準の改訂の歴史と今後

社会の変化、情報技術の進展、情報システムの普及に伴い、システム監査基準・管理基準が改訂されてきた



システム監査と情報セキュリティ監査での基準の関係



出典：経済産業省報道発表資料

システム監査基準とシステム管理基準

情報システムにまつわるリスクに対するコントロールを適切に整備・運用する目的は

- ・情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため
- ・情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため
- ・情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため
- ・情報システムが、関連法令、契約又は内部規程等に準拠するようにするため

システム監査基準

システム監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範

システム管理基準

組織体が主体的に経営戦略に沿って効果的な情報システム戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範

【出典】 喜入博　著 「情報セキュリティリ監査基準制度」(FISC)2003

システム管理基準の改訂
サブコントロールの作成

システム管理基準は、＜一部省略＞、組織体が属する業界又は事業活動の特性等を考慮して、必要ある場合には、本管理基準の主旨及び体系に則って、該当する関係機関などにおいて、**独自の管理基準**を策定し活用することが望ましい。また、時々の関連技術動向、関連法令、及び社会規範などを考慮し、それらを反映した詳細な**サブコントロール項目**を策定することが望ましい。

高度・複雑化・多様化する情報化の時代の監査は、監査対象に特化し専門監査人が必要となり、監査にあたっての監査基準及びサブコントロールの作成が重要となる。まず、時代に即した監査基準の改訂が急務である。

求められるシステム監査

経済産業省は「システム監査」及び「ITガバナンス」

■ システム監査は、組織体の情報システムにまつわるリスクに対するコントロールが適切に整備・運用されていることを担保するための有効な手段となる。

■ システム監査の実施は、組織体のITガバナンスの実現に寄与することができ、利害関係者に対する説明責任を果たすことにつながる。

■ ITガバンナンスは「企業が競争優位性の構築を目的としてIT戦略の策定及び実行をコントロールし、あるべき方向へと導く組織能力」と定義

システム監査は今なおこの実現に寄与していない。
経営者に寄り添ったシステム監査の実施には、進化と多様化する「情報システムの脆弱性」を俯瞰し、求められるシステム監査の追い求めることが重要である。
これまで述べてきたことは、その一端にすぎない。

進化と多様化する情報システムを俯瞰する視点
多様化する情報システム脆弱性への対応ー

ICTの経営活用の視点

- 経営戦略の策定、情報システムの戦略的活用
- 業務改革、企業間供給連鎖(SCM)への情報化
- ITガバナンス、企業の社会的責任(CSR)問題
- 進展するICT(Iot、Fintec等)への対応

拡大化する情報システムの脆弱性

情報システムの法的視点

- 知的財産権の活用と保護
- ネットワーク取引の法的問題
- 事業者のコンプライアンス
- 個人情報保護とプライバシー

情報セキュリティ・安全性の視点

- 事故・災害における危機管理
- 想定外リスクへの対応
- 多様化する情報システムへの人材育成
- システム監査・セキュリティ監査への知見

参考・引用文献

（１）青山監査法人システム監査部編「システム監査の方法」
　　中央経済社　昭和59年　1984
（２）日本公認会計士協会編「EDP監査の進め方」（財）大蔵財務協会
　　昭和51年　1976
（３）宇佐美博著「システム監査の歴史について」愛知大学情報処理センター　2001
（４）日本生産性本部経営指導部編「電子計算機活用の基礎知識」昭和43年
（５）喜入　博　著「情報セキュリティリ監査基準制度」（FISC）2003
（６）松田貴典著「情報システムの脆弱性」白桃書房　1999
（７）ウィキペディア「個人情報漏洩事件」https://ja.wikipedia.org/wiki/
（８）松田貴典著「情報システムの法とセキュリティ」白桃書房　2005
（９）独立行政法人情報処理推進機構「IoT開発におけるセキュリティ設計の手引き」
　　2016年5月
（１０）IoT推進コンソーシアム　総務省　経済産業省
　　「IoTセキュリティガイドライン１．０概要」平成28年7月
（１１）「システム監査基準」「システム管理基準」経済産業省ホームページ
　　http://www.meti.go.jp/policy/netsecurity/new_systemauditG.html