法とシステム監査研究プロジェクト研究報告

システム監査学会第３６回研究大会

開催日：２０２２年6月１０日（金）

発表：荒木哲郎（弁護士・システム監査技術者）

序　概要

1　研究プロジェクトの概要

■　主査　弁護士　稲垣隆一

■　概要

　国、自治体、企業の遵法経営のために情報システムの企画、開発、運用、保守が抱える課題と、課題解決のためのシステム監査の経営における位置づけ、監査の尺度、監査技法を研究して、コンプライアンス経営のためにシステム監査が果たし得る実務的な役割を明らかにする。

「法とシステム監査研究プロジェクト」メンバー
（原則　五十音順）

氏名	所属等	備考
稲垣　隆一	稲垣隆一法律事務所・弁護士	主査
黒澤　兵夫	TAKE国際技術士研究所	副主査
石島　　隆	法政大学経営大学院イノベーション・マネジメント研究科教授	
多和田　肇	システム監査技術者CIA,CISA	
成田　和弘	システム監査技術者CIA,CISA	
牧野　博文	株式会社東芝、システム監査技術者 情報処理安全確保支援士、CISA	
芳仲　　宏	システム監査技術者、　ISMS認証登録判定委員会委員、ITコーディネータ	
荒木　哲郎	弁護士・システム監査技術者	発表

第１　研究テーマについて

１　テーマ

民法改正に対応した情報システム・モデル取引・契約書のシステム監査的視点からの検討

２　今回のテーマを選択した趣旨

２０２０年１２月にIPAからモデル取引・契約書（第二版）が公表される。

２０２０年４月施行の民法改正を契機に検討されたものであるが、第二版では、民法改正点以外の部分で見直しが望ましい部分にも検討がなされている。

それらの論点はシステム監査においても重要であると思われ、今回、当プロジェクトでは、同論点を素材として、民法改正以外に検討された主要な論点について、システム監査との関係において検討した。

３　検討した論点

モデル契約で検討された民法に直接関係しない論点のうち、

（１）セキュリティ

（２）プロジェクトマネジメント義務及び協力義務

（３）契約における「重大な過失」の明確化

を検討。

（参考）他には（４）システム開発における複数契約の関係、（５）再構築対応

第２　検討内容
１　セキュリティ

- **（１）民法との関係**

  ①　サイバー攻撃等により，情報が漏えいしたことの責任がベンダー側にあるとして，債務不履行に基づく損害賠償義務が認められる場合

  ②　ベンダーは開発当時のセキュリティ水準に沿ったセキュリティ対策を納入物に施していないと，契約不適合責任を問われる可能性あり。

（２）ユーザーの協力義務との関係

ユーザーは，セキュリティ要件に必要な情報の提供と，セキュリティ対策の実装ポリシーの判断において，一定の責任を負う。

（３）モデル契約の見直しの内容

ユーザとベンダとは、それぞれの立場に応じて必要な情報を示しつつ、リスクやコスト等について相互に協議することにより、システムに実装する「セキュリティ仕様」を決めることが必要。

→定義条項、責任者条項、セキュリティ条項の見直し。

- **セキュリティの実装プロセスに関する解説の加筆**
- **セキュリティ検討プロジェクトチーム（以下「セキュリティ 検討PT」という。）による「セキュリティ仕様関連文書」の策定**

（４）セキュリティ条項の見直し。

ア　第２条第２号の「要件定義書」の定義としてセキュリティ要件が非機能要件の一つであることを明記した上で、同条第15号として、「セキュリティ」自体の定義を置いた。

イ　第９条（責任者）の規定で　ユーザ及びベンダの責任者が本件ソフトウェアに具備する具体的機能、すなわちセキュリティ仕様を決定する権限と責任を有することを明記。

ウ　第５０条のセキュリティ条項について，見直し後の条項では、ユーザ及びベンダが求めるセキュリティ仕様についてクリアすべき基準及び開発プロジェクトを進める上での提案や合意についての手順が確立されているかどうかによってA案とB案に分けて規定を置いた。

- 第２条
- ②要件定義書
- 　本件ソフトウェアの機能要件（甲の要求を満足するために、ソフトウェアが実現しなければならない機能に係る要件。システム機能及びデータにより定義される。）及び非機能要件（機能要件以外のすべての要素に係る要件。業務内容及びソフトウェアの機能と直接的な関連性を有さない品質要件、技術要件、移行要件、運用要件、セキュリティ要件及び付帯作業等から成り、それぞれに対する目標値及び具体的事項により定義される。）をとりまとめた文書
- ⑮　セキュリティ
- 本件ソフトウェアにより記録され、又は発信され、伝送され、若しくは受信される情報及び本件ソフトウェア自体（以下「当該情報等」という。）の漏えい、滅失又は毀損（以下「セキュリティインシデント」という。）の防止その他の当該情報等の安全管理のために必要な措置が講じられることをいうものとする。

- 第9条
- 3.　甲の責任者は、次の各号に定める権限及び責任を有するものとする。
- ⑨第50条所定のセキュリティ対策について本件ソフトウェアに具備する具体的機能（以下「セキュリティ仕様」という。）の採否を行う権限及び責任

４【A案　セキュリティ仕様の策定手順が未確立の場合】

- （セキュリティ）　（注）〔〕内はオプション条項
- 第50条　乙が納入する本件ソフトウェアのセキュリティ対策について、甲及び乙は、その具体的な機能、遵守方法、管理体制及び費用負担等を協議の上、ソフトウェア開発業務を開始する前までにセキュリティ仕様を確定させ、書面により定めるものとする。
- 2.　セキュリティ仕様に関する協議に際しては、甲は、乙に対し、本件ソフトウェアが稼働する環境の機器、ソフトウェア及びネットワークの構成等に関する情報その他セキュリティ仕様を確定するために必要な情報を適時に提供しなければならない。
- ○.　〔甲及び乙は、セキュリティ仕様の作成のために参照するガイドラインについて合意した場合、ガイドラインの名称、バージョン及び当該ガイドラインを参照して本件ソフトウェアに適用すべき事項をセキュリティ仕様に盛り込み、第22条（外部設計書の確定）所定の手続により確定するものとする。その際、甲が当該ガイドラインに示された対策の一部を講じない判断をしたときは、その判断（対策を講じないことにより軽微とはいえない影響が生じることが予測できる場合には、その影響を含む。）について、第21条（外部設計検討会）所定の連絡協議会において確認したうえ、第12条第6項の議事録に記載するものとする。〕

- 3.　確定したセキュリティ仕様は、システム仕様書の一部を構成するものとし、その変更が必要となった場合は、第37条（変更管理手続）によってのみこれを行うことができるものとする。
- 4. 甲及び乙は、セキュリティ仕様の確定後から納入物の納入までに、本件ソフトウェアに関して、確定したセキュリティ仕様では対応できないセキュリティ上の脅威又は脆弱性（個別契約の目的を達することができないものに限る。）があることを知ったときは、遅滞なく相手方に書面により通知する。かかる通知書は、第37条第1項に定める変更提案書に該当するものとし、甲及び乙は、第37条第1項各号の事項に加え、セキュリティ上のリスクを検討し、セキュリティ仕様の変更の要否を決定する。
- 5.　乙は、納入物の検収がなされるまでの期間、本件ソフトウェアに関して、確定したセキュリティ仕様では対応できないセキュリティ上の脅威又は脆弱性（個別契約の目的を達することができないものに限る。）があることを知ったときは、甲に通知するものとする。なお、甲乙間において別途契約を締結しない限り、乙は、納入物のセキュリティ上の影響範囲の分析、納入物に対する対策の立案、実施等の義務を負わない。
- 6.　乙は、甲に対し、システム仕様書に記載されたセキュリティ仕様に従って本件ソフトウェアのセキュリティ対策を講じる義務を負うにとどまり、本件ソフトウェアに関してセキュリティインシデントが生じないことを保証するものではない。
- 7. 乙は、本件ソフトウェアに関して、確定したセキュリティ仕様では対応できないセキュリティ上の脅威又は脆弱性に関する情報を収集する義務を負わないものとし、乙の主任担当者又は業務従事者が個別契約の目的を達することができないような脅威又は脆弱性があることを知りながら（重大な過失によって知らなかったときを含む。）、甲に通知をしなかった場合を除き、本契約における義務違反を問われない。

（５）セキュリティ仕様作成のためのガイドライン等について

- 今回の見直しに際して、セキュリティ 検討 PTにおいて、Windows Active Directory 環境を対象に、セキュリティ仕様を作成する際の脅威分析とその対策を検討するための OS、デスクトップアプリ、ブラウザーの セキュリティ設定を検討するためのガイドライン及び当該ガイドラインを前提としたセキュリティ仕様策定プロセスの検討が進められ、

- ①「情報システム開発契約のセキュリティ仕様作成のためのガイドライン～Windows Active Directory編～」
- ②及び「セキュリティ 仕様策定プロセス～「情報システム開発契約のセキュリティ仕様作成のためのガイドライ ン」対応～」

- として策定された。

（６）　システム監査との関係

- **システム監査において，情報セキュリティに関しては，情報セキュリティ管理基準を使用する場合が多いと思われる。**

- **セキュリティ仕様策定のプロセスのチェックポイントの作成に利用できないか。**
- **∵ガイドラインは，開発者（ベンダー向け）？**

・　**ただし，セキュリティ仕様作成プロセスの，〔参考４：ユーザー・ベンダー間のリスクコミュニケーションにおいて参照することが望ましい資料等〕には，情報セキュリテイ管理基準は載っていない。**

本来、載せるべきではないか。

2　プロジェクトマネジメント義務及び協力義務

（1）見直しの視点

- 　近年特に問題となっている、ベンダのプロジェクトマネジメント義務及びユーザの協力義務について、モデル契約上の手当てによって、紛争の予防に資することはできないか。また、それぞれの義務について裁判例を踏まえて一定の整理ができないか。

- 　しかし，

-

- 　裁判例で示されたプロジェクトマネジメントや協力義務は、それぞれ個別事案における判断であり、汎用性の高いモデル契約の中にこれらの義務を規定することは難しいことから、条項の形で追記することは見送られた。

（２）具体的見直し点

ア　新たな裁判例を当該事案に関連する箇所における紹介

イ　ユーザ及びベンダの役割分担・プロジェクトマネジメントに関する記述の見直し

（ウ　マルチベンダ形式における用語法の修正）

エ　ベンダの中止提言を踏まえた解約権のオプション条項としての追加

- イ　ユーザ及びベンダの役割分担

- （協働と役割分担）
- 第8条　甲及び乙は、本件業務の円滑かつ適切な遂行のためには、乙の有するソフトウェア開発に関する技術及び知識の提供と甲によるシステム仕様書の早期かつ明確な確定が重要であり、甲乙双方による共同作業及び各自の分担作業が必要とされることを認識し、甲乙双方による共同作業及び各自の分担作業を誠実に実施するとともに、相手方の分担作業の実施に対して誠意をもって協力するものとする。
- 2.　甲乙双方による共同作業及び各自の分担作業は、別添〇のとおりとし、各個別契約においてその詳細を定めるものとする。
- 3.　甲及び乙は、共同作業及び各自の実施すべき分担作業を遅延し又は実施しない場合、それにより相手方に生じた損害の賠償も含め、かかる遅延又は不実施について相手方に対して責任を負うものとする。

エ　ベンダの中止提言を踏まえた解約権のオプション条項としての追加

- 当初，３７条の協議（変更の協議）の結果、個別契約の続行をしても当該個別契約の目的を達成できないと客観的に認められる場合には、ベンダがユーザに中止を提言するものとし、それでもユーザが合理的な理由なく応じない場合にはベンダが個別契約の解約ができるという条項が提案されたが、この条項の追加についてはユーザ側から異論が出される等したため，最終的にオプション条項となった。

- 反対の理由

∵①中止の提言は常に求められるものではない。

②プロジェクトを続行することは最終的にはユーザの責任で判断できるようにしておくべき。

③個別契約の目的を達成できるかは究極的にはユーザの主観を考慮せざるを得ず、ベンダが客観的な観点から判断することは実務的には困難。

【A案：ベンダによる解約条項を定めない場合】

- **（変更の協議不調に伴う契約終了）**

第38条　前条の協議の結果、変更の内容が作業期間又は納期、委託料及びその他の契約条件に影響を及ぼす等の理由により、甲が個別契約の続行を中止しようとするときは、甲は個別業務の未了部分について個別契約を解約することができる。

2. **甲は、前項により個別業務の未了部分について解約しようとする場合、中止時点まで乙が遂行した個別業務についての委託料を支払うとともに、解約により乙が出捐すべきこととなる費用その他乙に生じた損害を賠償しなければならない。趣旨・・ベンダの保護**

- **契約が請負か準委任かは関係なし**
- **ユーザが、ベンダの債務不履行その他の事由に基づき、損害賠償請求をすることを妨げない。**

【B案：ベンダによる解約条項を定める場合】

- （変更の協議不調に伴う契約終了）
- 第38条　前条の協議の結果、変更の内容が作業期間又は納期、委託料及びその他の契約
- 条件に影響を及ぼす等の理由により、甲が個別契約の続行を中止しようとするときは、甲は個別業務の未了部分について個別契約を解約することができる。
- 2. 甲は、前項により個別業務の未了部分について解約しようとする場合、中止時点まで乙が遂行した個別業務についての委託料を支払うとともに、解約により乙が出捐すべきこととなる費用その他乙に生じた損害を賠償しなければならない。
- 3. 前条の協議の結果、作業期間又は納期、委託料及びその他の契約の条件に重大な影響を及ぼす等の理由により、個別契約を続行することが困難となる事情が客観的に認められる場合は、乙が当該事情及びその理由を明示したうえで書面により中止を提言することができるものとする。
- 4. 乙による前項の提言にもかかわらず、甲が合理的な期間内に合理的な理由を提示することなくこれに応じない場合、乙は、個別業務の未了部分について個別契約を解約することができるものとする。

- 5.前項に基づき、乙が個別契約を解約した場合、甲は乙に対し、当該解約時点まで乙が遂行した個別業務についての委託料を支払うものとする。

- 6.第4項に基づいて個別業務の未了部分について個別契約が解約される場合であっても、甲及び乙は、債務不履行その他の事由に基づき、相手方に対して損害賠償を求めることは妨げられない。

- システム開発のプロセスにおいて、当初の想定から著しく外れたような事態が発生しており、開発の続行のために個別契約に変更が必要である状況であるにもかかわらず、変更協議が不調となった結果ユーザ・ベンダ双方が被ることになる損失が大きくなることが当初から想定される場合等（大規模なプロジェクト等）に、ユーザ・ベンダのコミュニケーションを促進する観点から、A案のユーザからの解約権に加え、一定の場合におけるベンダからの解約権を規定

（３）　システム監査との関係

- 契約は原則、開発前のものに対し、監査は事後的。

- ただ、役割分担が上手くできていたかは、監査でも当然問題になる。
  →（裁判例等は当然参考になる。）

- 契約で定めがあったとしても、分担がうまくできていたかは別問題。

- 契約で定めていたか否かは、一応ポイントになるものの、もし、それが崩れていたのであれば、その過程（原因）をきちんと調査すべき。

３　契約における「重大な過失」の明確化

- （１）見直しの視点
- 　従前のモデル契約においては、「重大な過失」の有無が損害賠償の責任制限条項の適用の分水嶺となっており、また、ソフトウェア開発業務等の請負型の業務における契約不適合責任においても、「重大な過失」の有無が客観的起算点による期間制限の適用の分水嶺となった。この「重大な過失」について、ベンダ側の予測可能性の担保の観点からより明確化することはできないか。

2　具体的見直し

- 契約条項として重過失については特段の定義をすることはせず、重過失概念に関する一般的な理解とシステム開発に関する裁判例のうち重過失についての判例を逐条解説に追記することで、重過失を考える上での手がかりを提供する。

（モデル契約）第５３条

- （損害賠償）
- 第53条　甲及び乙は、本契約及び個別契約の履行に関し、相手方の責めに帰すべき事由により損害を被った場合、相手方に対して、（〇〇〇の損害に限り）損害賠償を請求することができる。但し、この請求は、当該損害賠償の請求原因となる当該個別契約に定める納品物の検収完了日又は業務の終了確認日から〇ヶ月間が経過した後は行うことができない。
- 2.本契約及び個別契約の履行に関する損害賠償の累計総額は、債務不履行（契約不適合責任を含む、）不当利得、不法行為その他請求原因の如何にかかわらず、帰責事由の原因となった個別契約に定める〇〇〇の金額を限度とする。
- 3.前項は、損害賠償義務者の故意又は重大な過失に基づく場合には適用しないものとする。

（目的物の種類又は品質に関する担保責任の期間の制限）
民法第五百六十六条

- 売主が種類又は品質に関して契約の内容に適合しない目的物を買主に引き渡した場合において、買主がその不適合を知った時から一年以内にその旨を売主に通知しないときは、買主は、その不適合を理由として、履行の追完の請求、代金の減額の請求、損害賠償の請求及び契約の解除をすることができない。**ただし、売主が引渡しの時にその不適合を知り、又は重大な過失によって知らなかったときは、この限りでない。**

（モデル契約）第○条（契約不適合責任）

5. 乙が本条に定める責任その他の契約不適合責任を負うのは、前条の確定後〇ヶ月／〇年以内【であって、かつ甲が当該契約不適合を知った時から〇ヶ月以内】に甲から当該契約不適合を通知された場合に限るものとする。但し、前条の確定時において乙が当該契約不適合を知り若しくは重過失により知らなかった場合、又は当該契約不適合が乙の故意若しくは重過失に起因する場合にはこの限りでない。

3　重過失の概念

- **近時の裁判例では、「注意義務違反の程度が著しい場合」**
- **（ア）義務違反の結果**
- **（イ）違反した義務自体が重要（それすら怠っている）。**
- **・・・（ア）と（イ）の両方を含む。**

- **という考え方によっているものが多い。**

４　裁判例

ジェイコム株式誤発注事件（東京高裁平成25年7月24日）

- 事案
- 2005年12月8日、新規上場したジェイコム（現・ライク）の株式の取引をめぐり、みずほ証券（旧法人）が誤注文をした事件。
- みずほ証券の担当者が「61万円1株売り」とすべき注文を「1円61万株売り」と誤ってコンピュータに入力した→株価急落

- 担当者は、売り注文を出してから誤りに気付き、1分25秒後の9時29分21秒に取消し注文を送ったが、東京証券取引所のコンピュータプログラムに潜んでいたバグのため、この取り消し注文を受け付けなかった。

- みずほ証券は、システムが正しく動作して取り消し手続きが受け入れられれば、損失は5億円前後で済んだはずであるとして、2006年10月27日、東証に対して訴訟費用を含む414億円の賠償を求めて東京地方裁判所に提訴した。

  →東京地方裁判所は、東証に約１０７億円の支払を命じる判決

- （１）重過失について

- 「今日において過失は主観的要件である故意とは異なり，主観的な心理状態ではなく，客観的な注意義務違反と捉えることが裁判実務上一般的になっている。そして，注意義務違反は，結果の予見可能性及び回避可能性が前提になるところ，**著しい注意義務違反（重過失）というためには，結果の予見が可能であり，かつ，容易であること，結果の回避が可能であり，かつ，容易であることが要件となるものと解される。**このように重過失を著しい注意義務違反と解する立場は，結果の予見が可能であり，かつ，容易であることを要件とする限りにおいて，判例における重過失の理解とも整合するものと考えられる。そうすると，重過失については，以上のような要件を前提にした著しい注意義務違反と解するのが相当である。」

- ・取引参加者規程１５条「当取引所は，取引参加者（証券会社）が業務上当取引所の市場の施設の利用に関して損害を受けることがあっても，当取引所に故意又は重過失が認められる場合を除き，これを賠償する責めに任じない。」と定められている。

- 「本件バグの作込みを回避することが容易であったとは認めることができず，また，本件バグの発見・修正が容易であったとも認めることができない。（中略）また，本件不具合が複数の条件が重なることにより発生する性質のものであったことも，被控訴人において，結果の予見が可能であり，かつ，容易であったとの認定を阻むものである。
- 以上によると，本件においては，被控訴人の重過失（著しい注意義務違反）の要件である結果の予見が可能であり，かつ，容易であること，結果の回避が可能であり，かつ，容易であることが充足されていないことになる。したがって，被控訴人は，取消注文に対応することのできない売買システムを提供するという債務不履行があったが，重過失があったものと評価することはできない。（中略）
- 以上で検討してきたとおり，被控訴人には，適切に取消処理ができるコンピュータ・システム提供義務の不履行が認められるが，被控訴人に重過失があるとはいえない。したがって，被控訴人は，本件免責規定によってその債務不履行責任を免れることになる。」

→債務不履行責任は否定。

- **本件免責規定の不法行為への適用の有無**

「契約上の免責規定は，当該契約当事者間における不法行為責任にも適用されると解するのが当事者の合理的な意思に合致すると解される（最高裁平成１０年４月３０日判決・裁判集民事１８８号３８５頁参照）。したがって，本件では不法行為の場面においても，本件免責規定によって，被控訴人に軽過失がある場合は免責されるが，被控訴人に故意・重過失がある場合においては，その責任を免れないものと解される。

- そして，売買停止措置は，取引参加者が「市場の施設」たる本件売買システムを利用して取引をしている間にされるものであり，本件免責規定による免責範囲に含まれると解される。」

・ 約定株式数が発行済み株式の３倍を超えた時点以後の売買の不停止は、重過失。

→地裁の結論維持。

４　システム監査との関係

- 事後的であるシステム監査でも、開発行為の監査等において契約内容が適切であったかは問題になる。

  →免責条項の有無、また、その内容はチェックすべき。

- 実際の免責条項の内容のチェックにおいては、請求原因の種類、また、帰責事由の範囲（個別契約等）を意識してすべき（ex.モデル契約５３条）　。

- ただし、最近の野村VS日本IBM事件の第１審においては、重過失の場合に免責条項の適用が制限される旨の明文規定はなかったにもかかわらず、争点となった

  （ただし、控訴審では、そもそもベンダー側の責任が否定されたので、免責条項の適用はなかった。）。

- ご清聴ありがとうございました。