Computer Software Association of Japan

平成 20 年度
情報システムの信頼性向上のための
取引慣行・契約に関する検討委員会
活動報告

平成 21 年 3 月

社団法人コンピュータソフトウェア協会

目次

情報システムの信頼性向上のための取引慣行・契約に関する検討委員会
委員名簿

（順不同、敬称略）

委員長	板東　直樹	アップデートテクノロジー㈱　代表取締役社長
顧　問	淺田　隆治	フューチャーアーキテクト㈱　顧問
委　員	松木　智	日本 SE㈱　企画本部本部長　専務執行役
〃	水谷　学	ピー・シー・エー㈱　代表取締役社社長
〃	熊崎　克己	ピー・シー・エー㈱　管理本部(法務担当)参事
〃	中根　弓佳	サイボウズ㈱　経営管理本部　知財法務部　部長
〃	小西　理	顧問
〃	高橋　知久	㈱オービックビジネスコンサルタント　管理本部次長
〃	船津　忠	カシオ情報機器㈱
〃	脇坂　隆則	日立ソフトウェアエンジニアリング㈱　ソリューション営業本部　副本部長
〃	黒木　直樹	トレンドマイクロ㈱　戦略企画室　Strategy＆Business Operation　担当ディレクター
〃	宮野　弘幸	日本事務器㈱　経営企画部　部長
〃	瀬戸口　靜美	マイクロソフト㈱　テクニカルソリューション推進統括本部
〃	富田　康義	㈱オービックビジネスコンサルタント　営業本部 ERP ソリューション推進室 ERP ソリューション SE グループ　課長
〃	服部　芳子	㈱内田洋行　アプリケーション 2 課　課長
〃	平野　高志	ブレークモア法律事務所　弁護士
〃	東城　聡	ブレークモア法律事務所　弁護士
オブザーバ	久保寺　良之	IT コーディネータ協会　常務理事　事務局長
〃	松波　道廣	(社)日本コンピュータシステム販売店協会　専務理事
〃	古田　正武	(社)日本コンピュータシステム販売店協会　参与

事務局	鈴木　啓紹	社団法人コンピュータソフトウェア協会

情報システムの信頼性向上のための取引慣行・契約に関する検討委員会
実施概要

○委員会

第１回　日時：平成 20 年 10 月 30 日（木）
場所：平河町 Mercury Room （クオリティ株式会社 8F 会議室）
議題：
・経済産業省「情報システムの信頼性向上に関するガイドライン」第 2 版（案）について
説明：粂野 文洋 氏（三菱総合研究所 情報技術研究センター）
・「情報システム・ソフトウェア取引高度化コンソーシアム」活動進捗状況の説明
・今後の委員会活動について検討

第２回　日時：平成 21 年 2 月 13 日（金）
場所：関東 IT ソフトウェア健保会館「桜華楼」
議題：
・各ワーキング（E-LearningWG、ソフトウェア動作環境ガイドライン策定 WG）の進捗報告
・「情報システム・ソフトウェア取引高度化コンソーシアム」活動進捗状況の説明

○E-Learning WG

主査：松木 智（日本 SE㈱ 企画本部 本部長 専務執行役員）
「情報システム・ソフトウェア取引高度化コンソーシアム」で策定する E-Learning コンテンツ製作協力を実施。

第１回　日時：平成 20 年 12 月 25 日（木）
場所：CSAJ 会議室
議題：
・本ワーキングの活動目的
・契約コンソーシアムでの E ラーニングコンテンツ作成状況
・本ワーキングの今後の活動について

第２回　日時：平成 21 日 2 月 6 日（金）
場所：CSAJ 会議室
議題：
・意見募集の状況
・契約コンソーシアムでの E ラーニングコンテンツ作成状況
・本ワーキングの今後の活動について

成果：「情報システム・ソフトウェア取引高度化コンソーシアム」で策定する E-Learning コンテンツに対する修正意見及び認証制度向け問題作成し、コンソーシアム側へフィードバックした。

○ソフトウェア動作環境ガイドライン策定 WG
主査：脇坂 隆則（日立ソフトウェアエンジニアリング㈱ ソリューション開発本部
セキュリティソリューション部 部長）
モデル契約・取引＜追補版＞の指摘事項にあるシステム性能、ライフサイクルを担保する情報開示をどうしていくべきか という点について検討し、1)ソフトウェアの応答性能・処理速度などの適正な動作基準とそのハードウェア要件、2）ユーザの償却期間中に想定しない保守の打ち切りが無いようなサポート・保守に関する情報開示についての参考となる資料を策定。
第 1 回　日時：平成 20 年 12 月 15 日（木）
場所：CSAJ 会議室
議題：
・本ワーキングの活動目的
・動作環境表示の法的な問題点（消費者契約法等）について解説
・本ワーキングの今後の活動について

第 2 回　日時：平成 21 年 1 月 15 日（木）
場所：CSAJ 会議室
議題：
・動作環境要因についての論議
・本ワーキングの今後のスケジュールについて

第 3 回　日時：平成 21 年 1 月 27 日（火）
場所：日本事務器社－会議室
議題：
・動作環境要因についての論議
・本ワーキングの今後のスケジュールについて

第 4 回　日時：平成 21 年 2 月 13 日（金）
場所：マイクロソフト社－会議室
議題：
・動作環境要因についての論議
・本ワーキングの今後のスケジュールについて

成果：モデル契約・取引＜追補版＞への追加参考資料としてソフトウェア動作環境ガイドラインを策定し、「情報システム・ソフトウェア取引高度化コンソーシアム」へ提出した。

○意見提出
・「情報システムの信頼性向上に関するガイドライン第 2 版」に対する意見
日　時：平成 20 年 10 月 31 日（金）
提出先：経済産業省 商務情報政策局 情報処理振興課 提出

情報システムの信頼性向上のための取引慣行・契約に関する検討委員会
提出意見書

経済産業省商務情報政策局情報処理振興課　パブリックコメント担当　宛

「情報システムの信頼性向上に関するガイドライン第2版(案)」に対する意見

[氏名]	社団法人コンピュータソフトウェア協会 「情報システムの信頼性向上ための 取引慣行・契約に関する検討委員会」 担当：鈴木啓紹
[住所]	〒100-00144 東京都千代田区永田町 2-4-2　秀和溜池ビル 4F
[電話番号]	03-5157-0780
[ＦＡＸ番号]	03-5157-0781
[電子メールアドレス]	hsuzuki@csaj.jp

【意見 1】

・該当箇所(どの部分についての意見か、該当箇所が分かるように明記して下さい。)

ガイドライン第2版（案）全体に対して

・意見内容

1)ガイドライン第 2 版（案）は、＜実施例＞が追記されているが、記述内容は実施例になっておらず具体的になにを実施すればよいのかが不明である。最低限、対象別に実施方法や参考すべき指針、資料を示さなければ、利用者にとって負担が大きく活用は見込まれない。ガイドラインであるならば、実施例にもとづき利用者の気づきを促すものであるべきである。PCI DSS 等に匹敵する水準にすべきではないか。

※PCI DSS（Payment Card Industry Data Security Standard の略称。加盟店・決済代行事業者が取り扱うカード会員のクレジットカード情報・取引情報を安全に守るために、JCB、アメリカンエキスプレス、Discover、マスターカード、VISA の国際ペイメントブランド 5 社が共同で策定した、クレジット業界のグローバルセキュリティ基準。情報セキュリティに対する具体的な実装を要求している基準であることから米国企業では業界を超えて採用されている。）

2)昨今の情報システムのトラブルは、開発したアプリケーションというよりは、そのアプリケーションを稼動するためのミドルソフトや運用ソフト、OS との連携部分やパッケージソフトとの連携部分の問題が多い。しかし、第 2 版（案）では、「パッケージソフトウェア」に関連する具体的な指摘事項がまだまだ少ない。

3)現実の情報システムトラブルを鑑みた場合、セキュリティの重要性は一般にも周知されているにもかかわらず、セキュリティに関連する記述がまだまだ不足しているといわざるを得ない。例えば、Web 通信販売などは国民生活にとって極めて身近な企業基幹系といえるが、これらシステムの脆弱性、欠陥は個人情報漏洩やクレジットカード情報の漏洩など、広範囲に 2 次的被害を招く恐れがあり、国民の関心も高いところである。さらに、大量の個人情報を取り扱う事業者におけるシステムの信頼性向上は、事業継続の観点からも最も重要なポイントとなるべきだが、これらの言及がない。さらに、全般に、情報システムを有する側の視点でのガイドラインとなっており、システムの便益を直接・間接に享受する側の視点で、「本来のあるべき姿」が描かれていない。

4)ガイドライン全体を通じて記述されている内容は、情報処理試験で出題されるようなレベルに見受けられるため、現職の情報システム部門担当者が読みこなして、自らのシステムの改善、改良に資するものとは言い難い。第 1 版は本邦初出であり、公表後の業界団体、利用者にとっての取り組みの嚆矢となったが、第 2 版（案）が単に構成を踏襲し、補強するだけでは意義を果たしているとは言えないのではないか。利用者にとって、新たな示唆に富むガイドラインとして機能する内容であることが切望される。

5) 多々ある規格、基準、指針、資格をガイドライン巻末で掲示しているだけのため、利用に際する有効性、実効性に欠ける。資料の利活用方法を具体的に提示すべきである。

6)第 2 版（案）の前提となる A.調達ソフトウェアの不具合、B.ネットワーク連携などによるオープン化の影響、C.移行時の事故対応　等の単語が追加されているが、これ等に対する具体的な対策の記述がない。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

1)本当に、＜実施例＞を例示するならば、
A.大規模クリティカルシステムの場合、B.中規模基幹業務、C.小規模基幹業務、D.その他 OA 業務、などに分けて、やるべきことを具体的に明記すべきと思われる。さらに言えば、例え企業規模が小さくても、巨大企業の重要な業務やサプライチェーンを担う企業もあることから、「単純な企業規模」ではなく、「業務の重要性に応じた視点」での記述をすべきである。本来の「信頼性ガイドライン」のあるべき姿について、所轄、事務局の考え方を明示して頂きたい。

2)パッケージの信頼性はソフトウェア単独ではなく、OS、ドライバ、ミドルウェア、パッケージソフトウェアの組み合わせと、それらの運用および保守で問題が発生している。先般発生したANAの事例はこの第2版（案）の指摘事項では防げないと思われる。また、これらソフトウェアのバージョンアップを第三者が担うことから、「信頼性」＝「可用性」については、運用・保守・テスト・リリースについて具体的に記述するべきである。

3)第2版（案）であるならば、第1版の指摘を受けて、より具体的に現実の情報システムに沿った記述内容が多く記述されるべきである。
昨今、インターネットやイントラネットなどでの業務が拡大しており、また、データの受け渡しも媒体、電子メールでの添付、Webシステムを介した形態（宅ファイル便）など、多様化されている。インターネットが介在するシステムは、攻撃に遭うとシステムが停止する、パフォーマンスが落ちる、多方面に悪影響を及ぼす（マルウェアの踏み台など）恐れがあり、これらを回避し信頼性を確保することは、もはや社会的責務であるため。

4)「ガイドライン」であるならば、内容に具体的な実効性を担保する回答や事例を示し、読み手が信頼性確保のための気づきや、新たな行動をとる内容、構成すべき。

5）巻末資料を一つ一つ紐解き、ガイドラインの当該箇所と資料の当該箇所を突き合わせ、具体的対策に行動をとるような利用者があるとは思えないため。

6)具体的な事例に基づく対策内容の例示が「第2版（案）」の本来のあるべき姿であるため。

【意見2】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P2　「（3）調達ソフトウェアの不具合」に対して

・意見内容

「調達ソフトウェアの不具合」という原因の追加で挙げられているが、これに対する信頼性を確保すための対策記述がどこにあるか不明である。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

【意見 3】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P2「（8）運用方法・手順等の誤り」

・意見内容

「運用・保守方法・手順書の誤り」とするか「保守方法・手順等の誤り」を追加すべきである。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

完全化保守では、保守実施にあたって結果として、システム障害が発生する可能性があるため。

【意見 4】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P3（Ｂ）企業基幹システムの文章内に記述のある「外部利用者」について

・意見内容

取引先、顧客等を示す単語に変更すべきである。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

基幹系システムの利用対象が必ずしも企業社内に限られていないため。

【意見 5】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P10　（１０）誤操作等防止への配慮

「画面設計において、選択式の入力方式や確認を求めるダイアログ表示等、操作の防止に配慮した部品配置及び画面遷移等を行う。」の記述に対して

・意見内容

画面設計だけの指摘であり、記述内容が不足している。証券誤発注のような、異常値の対応について、具体的な記述を追加すべきである。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

証券企業の誤発注事件の教訓が「第 2 版（案）」に反映されていないため。

【意見 6】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P14　（２）問題の診断と根本原因の究明

「さらに根本原因の究明を行い、情報システム利用者及び情報システム供給者間で共有し再発防止を図る。」の記述に対して

・意見内容

個別不具合の特定はできても、文書化、教育、周知、などの環境構造から発生する不具合の示唆がない。マニュアルの不備による操作ミスと、オペレータのキーの押し間違いでは本質が異なる。障害の種別においては、これら原因と結果が混在する用語の明確な区別にあたり、障害の本質的な原因と責任の所在が明らかになるようにすべきである。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

ベンダ、ユーザでの責任の押し付け合いを回避し、構造的な原因についての解明がなされるよう、高所大所から、過去の社会インフラ障害の具体的事例をもって、提言をすべきである。

【意見 7】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P15（５）関連・類似システムの障害情報の活用と情報公開

・文末「広く情報共有することが望ましい」の記述に対して
・実施例がカットされている点について

・意見内容

・文章を「広く報道を含めた形で社会的に情報共有されることが望ましい。」に変更すべきである。
・実施例として以下を追加すべきである「利用者、顧客への代替措置の周知、2 次被害や再発の防止などを目的とした、障害の事実、経過、原因、措置を含めた広報体制を確立する。」

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

広く国民生活を脅かす事態を招く企業の責任であることは極めて一般的な社会常識であり当然のことである。また、かかる広報体制の確立は、リスクマネジメントの観点からも障害発生時の対応、対策手順が整っている証左である。

【意見 8】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P18（２）インターネット経由のアクセスへの対処

・文章全体について

・＜実施例＞文末-「情報セキュリティ対策を実施する」のコメントに対して

・意見内容

・文章内に以下のセンテンスを盛り込むべきである。「通信販売サイトなどは、個人情報、クレジットカード情報など、情報漏洩によって 2 次被害が拡大する可能性がある。他方、脆弱性を利用するマルウェアの進化は秒進分歩であり、継続的な監視と監査、さらにはアーキテクチャの改善が必須の状況にあることの注意喚起を求められたい。」

・「情報セキュリティ対策を定期的、継続的に実施する。」に変更すべきである。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

・現状に即した具体例が必要であると思われる。

・取り扱う情報の性質（個人情報、クレジットカード情報等）を鑑み、必要に応じてシステム監査を実施し、対策、体制、アーキテクチャの見直しを図る必要があるため。

【意見 9】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P20（３）契約の妥当性・遵守状況のチェック体制の構築

＜実施例＞にある「社内法務部門による契約書のレビュー体制」の記述に対して

・意見内容

実態を鑑みた場合、「社内法務部門及び必要に応じて弁護士と、契約対象となる情報システムの関係者による契約書レビュー体制」と変更すべきである。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

契約の妥当性チェックは法務部門のみならず、関係者全員が知るべきところ、本記述では、IT に詳しい法務部門担当者がいない場合は、そもそも意味をなさず、また、情報システム担当者は民法上の契約類型に基づく、瑕疵担保責任、損害賠償、債務不履行を関知しなくてもよいように受け止められる。また、第 1 版の指摘を担保するためにモデル契約書の策定事業を業界団体として取り組んできたが、これらとの整合性がない。既出のモデル契約書＜追補版＞（『意見 11-理由を参照』）との整合性を確保するための精査が必要である。

【意見 10】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P22（１）複数システム供給者間での責任明確化

＜実施例＞文末にある「契約書に明記する」の記述に対して

・意見内容

「民法の契約類型を契約書に明記する。」に変更すべきである。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

情報システム取引においては売買、準委任、請負の 3 類型が適用されるところ、請負（完成義務あり、瑕疵担保）、準委任（完成義務なし、善管注意義務の債務不履行）のどちらともつかない契約が紛争の元となっており、かつ、責任所在を曖昧にさせる原因となっている。

【意見 11】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

P22（３）下請発注時のシステム供給者間の責任明確化

＜実施例＞の記述に対して

・意見内容

モデル契約＜追補版＞の課題指摘事項との整合性を図る必要がある。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

第 2 版（案）は、第 1 版指摘事項の活動について、踏襲をしておらず、先祖帰りとも思える構成となっているため。『経済産業省 情報システムの信頼性向上のためのモデル取引・契約に関する研究会 報告書～情報システム・モデル取引・契約書～（パッケージ、SaaS/ASP 活用、保守・運用）＜追補版＞』を参照。

【意見 12】

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

表1：「情報システム障害に係る原因と種別」の記述に対して

・意見内容

ガイドライン全体に IT セキュリティに関する記述が少なく、表 1 に IT セキュリティ項目を追加する必要がある。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

然るべき対策を講じていないばかりに、マルウェアの攻撃に遭い、その結果、情報システムに重大な障害を与え、復旧までに多くの時間・費用・労力を要し、またサービスを受ける側（顧客）及び、取引会社に多大な迷惑・損害を与えることになる。

特に最近のマルウェアは、Web を経由して感染することが多く、一度感染するとマルウェアが他のマルウェアを Web 経由でダウンロードし、多重感染するケースが圧倒的多数報告されている。「Web のマルウェア対策」を行っていない企業の一例では、従業員が不正なマルウェアを配布する Web にアクセスしてしまった為に、複数のマルウェアに感染し、そのマルウェアが社内ネットワークを介し 1,000 台超のコンピュータに蔓延し、その結果、39 種のマルウェアに多重感染したことが確認され、「情報システム」の復旧（マルウェアの完全除去）までに、延べ 100 名のエンジニアを使い、2 ヶ月の期間を要した実例がある。このような例もまさに、「情報システムの信頼性向上に関するガイドライン」に必要な要件であると考える。

企業情報システムに対するマルウェアの攻撃は、大きく外部からの攻撃に因る場合と、内部に持ち込まれたマルウェアに因る場合、その複合に分けられるが、企業ネットワークに既に潜むマルウェアが、感染・破壊活動を行う際の、マルウェア自身の挙動をモニタリング・分析し、対処するソリューションや、実施体制の監査、定期的な見直しは、特に大規模ネットワーク、海外拠点の多い行、ミッションクリティカルなネットワークを有する企業には必要とである。IPA で報告されている「ウイルスの見えない化」に対抗する、可視化ソリューションについて言及すべきである。

平成 20 年度 情報システムの信頼性向上のための
取引慣行・契約に関する検討委員会 活動報告書

平成 21 年 3 月 発行

発行　社団法人コンピュータソフトウェア協会（CSAJ）
〒107-0052　東京都港区赤坂 1-9-15 日本自転車会館 1 号館 5 階
TEL：03-3560-8440　FAX：03-3560-8441
URL：http://www.csaj.jp/