想定外事象へのシステム答責性について

木下 佳樹

総合信頼性に求められる性質の一つに，システム答責性 (system accountability) つまり説明責任遂行能力がある．答責遂行には契約遂行が含まれるが，それだけではない．想定外の事象への対処は契約に含まれないが，答責遂行の一部としてステークホルダによって求められることが多い．しかしそれは，契約によって強制されることではありえない．想定外のことは契約に含まれないからである．契約に含まれないことを求める根拠をどこに置くのか．この「想定外事象のシステム答責性問題」を解決するようなシステム答責性の構造を提示するのが本論文の目的である．さらに，この答責性構造をシステムライフサイクル活動として実装し，システム工学以外の分野に見られる幾つかの答責性構造と比較して，我々の構造の妥当性を考察する．我々の構造では，システムの「答責遂行 (説明責任遂行，account)」には，明示された合意を行動によって実施する「契約遂行 (respond)」だけではなく，システムについての客観的な「状況把握 (grasp)」と説明が必要であり，両者を明確に区別する．そして，答責遂行は，これらを相互に関連づける「把握還元 (feedback)」活動，具体的には状況把握を改善のための新たな契約に繋ぐ活動を，両者に加えたものである．想定外事象に対して求められるべきシステム答責活動は，状況把握とそれを新たな契約に繋ぐ活動であり，それらは当初の契約遂行とは独立に行われるものである，というのが，想定外事象のシステム答責性問題への我々の解答である．

1 はじめに

システムの総合信頼性に求められる性質の一つに，答責性がある．説明責任は政治や医療，教育など，様々な分野でとりあげられるが，我々はシステム工学の立場から，システムの振る舞いに関する答責性に関心がある．本論文では,「システム答責性 (system accountability)」という語を用いて，システムに関する答責性に議論を限定することを明確にする．

システム答責性の遂行には契約遂行が含まれるけれども，それだけではない．どんなシステムにでも想定外の事象が発生しうるが，それへの対処は契約には含まれない．想定外の事象はいろいろである．大津波の来襲や，サイバーアタックなど，システムの環境が想定を超えた状況になる場合もある．それに対してなんらかの対処を行うことが説明責任の一部として求められることは多い．しかし，想定外事象への具体的な対処は，契約に含まれるはずがない．事象がまさに想定外だからである．契約書にしばしば設けられる，いわゆる「協議解決条項」は，まさに想定外の事象のための条項であるが，これは通常，契約に定めのない事項一般について，合意が必要になった場合の協議の方法を定めるもので，具体的な合意事項ではない．

しかし，想定外の事象が何であっても，システムが安定して機能し続けるために共通に必要な活動がある．そのような活動は，契約によって強制されることではない．契約によらないとすると，想定外事象の下で，契約にない対処を求める根拠をどこにおくのか？ この問題を「想定外事象のシステム答責性問題」と呼ぶ．本論文では，システム答責性の構造を与え，それを用いてこの問題を解決する．

本論文は以下のように構成される．第 2 節では，答責性活動が「契約遂行」「状況把握」「フィードバック」の三つからなることを説明する．付録 A にはこの活動を国際標準 ISO/IEC/IEEE 15288:2023 [2] のプロセス，アクティビティ，タスクに割り振る，具体的なガイダンスを示す．第 3 節では，システム工学以外の文脈での明示的合意によらない活動の例をいくつか挙げ，それぞれを我々の「状況把握」や「フィードバック」と比較する．

2 答責活動の構造

本論文では，システム答責性 (system accountability) を A. 2. 3 によって定義する．答責性は，単に質問に答えるだけにとどまらず，システムの活動についての最終的な責任を持つこと，つまり結果を受け容れて，障害が生じても当事者意識を持って対処し，是正して必要な補償を提供することが求められる．

On System Accountability for Unanticipated Events (This article has not undergone peer review. Copyrights belong to the Author.)

Yoshiki Kinoshita, 神奈川大学情報学部計算機科学科，同プログラミング科学研究所，同情報学研究所, Dept. of Computer Science, Kanagawa University.

システムの開放性の観点から総合信頼性を規定する国際標準 IEC 62853:2018 [1] には，答責性に関する規定が設けられている．そこでは，答責遂行に求められる活動は契約に基づくものに限定され，それ以外の活動については「暗黙の合意」によるものとして，具体的な内容は言及されない．契約以外の事柄は，一まとめにされて適用範囲の外に置かれ，システムライフサイクルの問題として扱われてはいない．契約外活動には，倫理が関係せざるを得ず，問題が複雑になりがちであるが，本論文ではできるだけ倫理に踏み込まずに，システム工学の立場から，契約外活動の根拠を分析する．

後述するように，政治学などの文脈では，答責遂行を統治者の権力行使を制限するために統治者に課せられる義務とみなす場合もある．しかし，システム答責性に関してはそのような側面を考える必要はない．システムの運営責任者が我利我欲にしたがって，ほしいままに権力を行使する恐れなどはないとしてよいからである．

契約関係は究極のところ，損得勘定に基づく関係である．システム活動には，功利的立場ではない無私の立場から動機づけられたシステム活動も必要なように思われる．そのような活動は本当にあるか，たとえ存在しても必要なものか，などという問題が生じる．本節ではこのような観点から答責活動の構造を考察し，答責を果たすためには,「契約遂行」の他に，契約以外の動機により無私の立場から遂行される「状況把握」と「把握還元」の活動も必要であることを論じる．

2.1 契約遂行

答責 (説明責任) はシステムについての最終的な責任なので，その履行のためには，説明履行および関連する活動が必要である．しかし，その大前提として，システム取得者あるいは利用者と契約した通りにシステムが稼働しなければならないし，システム供給者の内部でそれぞれが定められた通りの活動に携わっていなければならない．この大前提をまとめて「契約遂行」といい，本論文では A. 2. 4 のように定義する．

「契約遂行」は予め定めた明示的合意に従う活動であることと，法的強制力によって担保されていることが本質的に重要である．契約の不履行には法的不利益が伴うからである．

なお，本論文では「契約」を広い意味にとって，明文化された合意事項を全て含むものとし，契約遂行は，それらの合意を実施することだとする．例えば仕様書は仕様記述担当者との間での契約であり，その遂行は仕様を実装する活動である．また，システムの障害に関しても，事前に想定できるものに対しては，契約の中で対処が具体的に定められる場合が多い．

2.2 状況把握

答責を果たすためには，システム及びその環境の仕組みに加えて，稼働中の現状を刻々と把握することが必要である．このような「状況把握」活動は，答責遂行のために，契約とは独立に，つまり契約条項にあってもなくても必要である．システムとその環境についての状況把握なしに，システムの最終的な説明責任を持てるはずがない．しかし，これが具体的にどんな活動であるのか，は自明ではない．本論文では「状況把握」を A. 2. 5 のように定義する．

システムの情報が自分の過失への責任追及を導くと考えた場合に，その情報を隠蔽しようとするのは，あってはならないことではあるが，自然の成り行きであろう．したがって,「状況把握」の実効的なものにするためには「状況把握」と「契約遂行」の二つの活動を分離して,「状況把握」のための情報が無制限に「契約遂行」に流れないようにする工夫が必要である．例えば，両活動の担当者の重複を避ける，情報のアクセス制限を設けるなどである．

また，正しい理解のためには，無私の立場から利害を考慮しないで分析が行われなければならない．例えばシステム障害発生時に，特定の者の損害だけを軽減する方策を導く分析が行われたり，特定の者の過失を隠蔽するような分析が行われると，状況に対する正しい理解が得られない．

2.3 把握還元

「状況把握」だけでは，状況を理解するだけで，状況改善のための行動にまでは至らない.「ミネルバの梟は夕暮れになって初めて飛翔する」と嘯くばかりでは答責を果たすことはできない．システムの更正・改修は，特に想定外事象による障害の「二の矢を防いで」再発を防止するためには必須の対策である．更正・改修の作業自体は,「契約遂行」に属するが，再発防止にはその根拠となる契約の更改が必要となる場合も多い．これを本論文ではフィードバック契約変更と呼ぶ．把握した状況を基に，システム更正・改修にフィードバックするからである．

契約更改を待たずに状況把握の結果を障害現場に即応させる活動も必要である．それは契約に規定されていないだけでなく，契約と矛盾しそれに違反する場合もあるかもしれない．それでも，無私の立場から得られた状況の正しい理解に基づく活動であれば，事後に関係者の理解が得られるはずなので，契約に拘束されることなく活動を遂行するべきであろう．このような活動を契約外答

責活動と呼ぶ.

フィードバック契約変更や契約外答責活動などの，状況把握からの判断に基づく，契約を超えた活動をまとめて「把握還元」活動とよぶ (A. 2. 5).

3　明示的合意によらない活動の例

契約からの逸脱に対しては，法的あるいは社会的な強制力が働き，逸脱しないようにする動機が生まれる．しかし契約にない活動が必要になった時には，契約関係だけではそれを遂行する動機が生まれない.

本節では，契約によらないに行動についての政治や法律他の分野での考察や実践から，いくつか興味深い事例や考察をとりあげて，システム答責性との比較，応用を論じる.

3. 1　本居宣長の古事記解釈—「うしはく」と「しらす」

本居宣長は，長年顧みられることのなかった古事記の解釈を詳細に行ったことで知られるが，古事記の中で「おさめる」ことを表す語として「うしはく」と「しらす」が明確に使い分けられていることを指摘した．宣長によれば,「うしはく」は領主が私的に領民を支配して力によって支配することであり (B. 1，B. 2).「しらす」は公的つまり無私の立場で国のことを隅々まで知り，また大御心 (世中の惣體の道理) によればどうするべきかを知ることである (B. 3)．そして，宣長は,「うしはく」によらず，専ら「しらす」によるだけで，国土は平穏におさまっていくと論じた (B. 4)．関連する古事記伝のテキストを付録 B に記す.

「国土がおさまる」ことを「システムが安定稼働する」ことに対応させ,「うしはく」を「契約遂行」に,「しらす」を利己を離れた「状況把握」及び「把握還元」に，ある程度対応させることができる.「しらす」と「うしはく」の区別の根本は，動機が私利私欲にあるか大義にあるかだが,「契約遂行」と「状況把握」/「把握還元」の区別は，明文化された合意に基づくか否かである．区別の基準は異なるが，少なくとも表面的には強い関連が認められる.

なお,「うしはく」「しらす」の言葉は，宣長の解釈と他の文脈での解釈では本質的に異なる場合があるので注意が必要である．宣長によると，日本書紀においては両者の区別は明確にはなされていない．また，大日本帝国憲法制定時に井上毅が「しらす」の語を導入しようとしたが叶わず,「統治」の語が採用されたことはよく知られている．内閣官報局から発行された憲法の解説書 (憲法義解) に「統治ノ義ハ古語ノ知(シラ)スニシテ領(ウシハ)クノ義ニ非ズ」と記され，これが判例と同様の扱いを受けていた．しかし一般用語としての「統治」は「うしはく」に近い意味を持つので，注意が必要である.

3. 2　英米法—Common Law と Equity

英国では，中世の時代に，通常の法律 (Common Law) が硬直化して実情に合わなくなり，弥縫策(びほうさく)として「信託 (use)」制度が導入されたが，その欠陥をついて，倫理的でない行為が法の網を掻い潜って横行した．当初はそのような案件は国王に直訴することができ，個別に裁かれたが，すぐに案件の数が増えて手に負えなくなった．そのため，Common Law の不備や硬直性によって救済されない紛争を，国王の「良心と衡平 (Equity)」に基づいて補完する「衡平法裁判所」がつくられた．衡平法裁判所が扱う法律 (衡平法) も，19 世紀までは Common Law とは別に設けられていた.

Common Law は，まさに明示的な契約であり，衡平法裁判所設立の経緯は，明示的な契約だけではうまくおさめられないことが，英国において認知されたことを示している．しかし，法 (Common Law) で足りないことを，別の法 (衡平法) で補完しようとした．この点において，我々の「状況把握」「把握還元」が契約と独立して遂行されることとは異なる.

なお，19 世紀になって「Common Law と衡平法はどちらが上位なのか」という問題が議論されるようになり，結局は二つの法体系が統一されることとなってしまった．Equity の考えは法理としては現在にも残っているし，大陸法や日本の法律にも取り入れられている．それをもとに契約関係とは別の信認関係 (信任関係) の概念が生まれて，直感的で漠然とした信頼関係の少なくとも一部分が法的に取り扱われるに至っている．[4].

Common Law は究極においては支配者の力による強制を根拠とするので，これを「うしはく」に対応させ，良心と衡平に基づく衡平法を「しらす」に対応させることができる．衡平を法の枠内におさめてしまったところは宣長の意味での「しらす」や我々の「状況把握」「把握還元」とは異なる.

3. 3　A. Schedler による答責性の概念

A. Schedler は，政治的答責性 (political accountability) の概念を考察し，これは応答責任 (answerability) と制裁義務 (enforcement) の二次元的な構造を持っていると主張した [3].

Schedler の応答責任と制裁義務は，我々の「状況把握」および「契約遂行」の両活動によっておおむね遂行される．他にも，“Who is Accountable for What?” や “Accountable for Whom?” など，システム答責性 (system accountability) にも通じる論点が見られるが，Schedler

が考察する policical accountability は，権力行使を制限する道具としての側面が強い．政治的権力の濫用を防止し是正する三つの側面が指摘されている．(1) 権力に対する制裁という脅威．(2) 透明な権力行使の義務付け．(3) 活動の弁明の強制の三つである．しかし，システムライフサイクルにおいては，政治とは異なって，権力の濫用が問題になることはない．システム答責性が求められる目的は，契約にないことまで遂行させて，適切にシステムの力を発揮させることであって，権力者が恣に権力を振るうことを制限するのとは目的が逆である．

また，Schedler のこの論文では，常に権力の行使と制限に注目する結果，宣長の「しらす」や英米法の Equity の背景となっている大御心や良心のような倫理的問題には触れられておらず，その点では我々のシステム答責性と共通している．

3.4 国際民間航空条約—調査情報の保護

国際民間航空条約 (いわゆるシカゴ条約) は第 26 条で事故の調査を国に義務付けている．そして同条約附属書 13 で事故調査について詳しく定めているが，特に，データの保護条項に注目したい．コックピット音声記録や供述，通信記録などのクリティカルな情報を，事故調査以外の目的に使用することを禁じている．

「状況把握」活動の一環として行われる，システム障害の調査においても，重要な情報を状況把握以外の目的に利用することを禁じる必要がある．これは，障害調査の実践上で以下の効果を持つ．

情報隠蔽の防止 真実を語ることにより自らが逮捕あるいは解雇される可能性があると，真実を語らなくなるので，提供情報の目的外使用禁止などの一定の保護を加えて，極端な不利の可能性を減殺し，真実を語ることを促進する．

積極的情報提供 質問されたことに単に回答するだけでなく，心理的側面からの経緯，自らの状態 (疲労の度合いなど)，組織の問題点などについての積極的な情報提供を奨励する．

4 おわりに

第 1 章に示した「想定外事象のシステム答責性問題」つまり「想定外事象の下で，契約にない対処を求める根拠をどこにおくのか？ 」という問題への我々の解答は

> 答責達成に求められる功利的でない無私の立場
> の「状況把握」の結果が根拠になる

というものである．答責を分析した結果，答責達成には「契約遂行」の他に「状況把握」と「把握還元」が必要であると考えられる．システムには答責性が当然求められるので，答責活動の必要要素の一つである「状況把握」が契約にない対処の根拠を与えるのである．

本論文では，システム工学の立場から「想定外事象のシステム答責性問題」に対処するための枠組を提示した．それは，明示的合意に基づく「契約遂行」のみならず，契約と完全に独立し無私の立場から遂行される「状況把握」および「把握還元」の三つのアクティビティによってシステム答責性 (System Accountability) を果たすことができる，というものである．さらに，国際標準 ISO/IEC/IEEE 15288:2023 のどのタスクによって遂行されるべきかを与えて，これらのアクティビティを具体化した．

第 3 節の事例が示すように，契約関係を結ぶ「契約遂行」だけでは活動がうまく進まないことは，古くから知られている．契約関係以外の関係として第一に思い浮かぶのは信頼関係である．しかしこれは直感的で漠然としている上に，根拠が倫理や宗教に求められることも多く，それは究極的には正しい方向だとも思われるものの，多数の共通理解を得ることが難しい．そのため，倫理や宗教ではなく，システム工学の概念に基いて，本研究では「状況把握」と「把握還元」の二つの活動によって，契約関係でない信頼関係を深める可能性を示した．そして，これらを含む答責活動を，国際標準 [2] の概念に沿ったガイダンスとして実装し，モデルの有効性を示した．

謝辞 森田直，武山誠，木下修司の各氏は，本論文の草稿に対して有益なコメントを寄せられた．記して感謝する．

参 考 文 献

[1] IEC: Open systems dependability, Ed.1, IEC 62853:2018.
[2] ISO, IEC, and IEEE: Systems and software engineering — System life cycle processes, ISO/IEC/IEEE 15288:2023.
[3] Schedler, A.: Conceptualizing Accountability, *The Self-Restraining State: Power and Accountability in New Democracies*, Schedler, A., Diamond, L., and Plattner, M. F.(eds.), Lynne Rienner Publishers, Boulder, CO, 1999, pp. 13–28.
[4] 岩井克人: 信任関係の統一理論に向けて—–倫理と法が重なる領域として—, 経済研究, (2016).

A システム答責活動ガイダンス

A.1 目的

システム答責活動の目的は，形成された合意内容を遂行することが第一である．しかしそれだけではなく，合意とは独立に，状況を把握して説明すること，さらに把握した結果をフィードバックして必要に応じて合意を形成しなおして，システムの改善に繋げることも答責活動の目的である．

A.2 用語と定義

A.2.1 答責

決定や行動の結果について，関係者からの質問に答えるとともに，その結果に対処し，必要に応じて是正や補償を行う最終的な責任

注記 1　答責は最終的な責任を負う責務であるから，これを分割したり，他者に委譲することはできない.

注記 2　政治的答責など，類似の概念と明確に区別する必要がある場合にはシステム答責とよぶ．システム答責要素，システム答責性などについても同様である.

A.2.2 答責要素

答責を果たすために遂行される，一連の責務

注記 1　具体的には質問応答，対処，是正，補償の四つが答責要素である.

A.2.3 答責性

答責を負っているという性質

注記 1　文脈によっては，答責性が，このような責務を負う状態や立場を指す場合もある.

A.2.4 契約遂行

明示的合意に基づいたシステム運用，障害発生時の規定手順の実施，および契約不履行あるいは損害発生時の補償等の責任履行

注記 1　利害関係者 (システム取得者 / システム供給者 / 利用者等) の権利・義務の精算を扱う．該当する明示的合意は，合意の範囲内における責任の根拠となる.

注記 2　明示的合意は，法的契約，サービス水準合意 (Service Level Agreement, SLA)，規約，仕様書等，あらゆる形のものであり，広義の契約である.

A.2.5 状況把握

システムおよびその環境の状況を正確に観測し，論理的かつ客観的な観点から正しく分析し，開示する活動，およびその知見に基づいて判断した結果の活動

注記 1　観測と分析は以下の意味で能動的な活動を含む. 決められた観測項目と方法を適用するだけではなく，項目と方法を常にみなおし，より正確な観測と分析をを期す.

注記 2　システムの環境には，システムが置かれている物理的な状況だけではなく，関連する取り決めや基準，標準，法令をはじめとする規則を含む.

注記 3　正確な観測と正しい分析は，内部監査を含む.

注記 4　これらの活動は，システム障害発生時の活動だけでなく，障害が特に認められない平時における準備活動も含む.

注記 5　「状況把握」活動は,「契約遂行」活動から完全に独立して実施されるものである.

注記 6　「状況把握」活動は，状況を正確に知り，それを理解し，さらにシステムについての情報を積極的に獲得しにいく活動を含む.

注記 7　客観的説明とは自らの利益の保護の意図も拡大の意図も持たないで行う説明である.

注記 8　想定外事象下では，契約に明示されていない活動もなされ得る．そのような活動に関する状況把握も本活動の対象である.

A.2.6 把握還元

状況把握からの判断に基づく，契約を超えた活動

注記 1　還元活動は，契約によらず遂行する契約外答責活動と，新たな契約を促すフィードバック契約変更の二つからなる.

注記 2　契約外答責活動の遂行に際しては，その根拠となる判断を明確にし，ステークホルダ及び社会一般に説明可能にしておくことが，特に重要である.

A.2.7 答責遂行

契約遂行，状況把握，および把握還元の三つを合わせた活動

注記 1　答責遂行は，説明責任遂行といいかえることもできる.

注記 2　答責遂行は，答責性を果たす活動である.

注記 3　想定外の故障に関して，答責遂行は復旧および改修，改善を返答および応答することに加えて，中長期的なシステム改善の必要の有無の判断を含む.

注記 4　「フィードバック」は,「状況把握」の結果に基づいてシステムの修正が必要であるかどうかを判断し，必要だと判断した場合には契約を更改することである.

注記 5　答責は，契約が想定していない活動の実施を含み得る．したがって答責活動を契約のなかで要求することはできない.

A.3 答責活動の関心事

システムの障害に際しては，契約に基づく対処だけでなく，システムとその環境をよく知り理解し，求めに応じていくらでも説明する「状況把握」活動，および把握事項を活動に還元する「把握還元」が必要である.,「状況把握」活動と「把握還元」活動は，契約に含まれない活動事項を指すものである．契約に含まれる活動事項は「契約遂行」によって進められる.

「契約遂行」が契約関係を確実にするのに対し,「状況把握」と「把握還元」は，信頼関係を深める作用をもつ.

「状況把握」遂行にあたっては，内部情報提供者が，その提供行為のために自身に不利な責任追及を受けることがないよう,「契約遂行」活動，特にその内の責任履行活動

との間で，情報のアクセス制御を適切に行なう必要がある．さもないと,「状況把握」活動の実効性が損なわれる．

A.4　契約遂行

「契約遂行」は，明示的合意（法的契約，サービス水準合意書 (Service Level Agreement, SLA)，規約，仕様書等）に基づき，事前に定められた権利・義務を体系的に遂行し，精算する活動である．本活動は，システムライフサイクルにおける契約関係の確実性を担保し，不履行に伴う法的・経済的不利益を回避する役割を果たす．

契約遂行における具体的内容は，ISO/IEC/IEEE 15288:2023 に規定されたシステムライフサイクルプロセスにおいて，主に合意プロセス（Acquisition Process / Supply Process）および各種運用・維持・品質保証等のプロセス（Operation Process / Maintenance Process / Quality Assurance Process 等）のアクティビティ・タスクとして割り振られる．表 1 に，契約遂行の活動項目と 15288 プロセス体系とのマッピングを示す．

A.4.1　活動項目の選定理由（Rationale）

本ガイダンスにおいて選定した契約遂行の各活動項目と，その選定理由は以下の通りである．

A.4.1.1　法令・契約遵守

明示的な合意および関連法令に基づきシステムを稼働・維持・管理することは，契約履行の最も基礎的かつ直接的な義務である．ここでの契約には，契約に基づいて適用される付属規程（各種ポリシー等）が含まれ，その遵守には契約に基づく日々の運用の実施自体が含まれる．仕様書やサービスレベルに記載された機能および制約条件を日常的に正しく提供・遵守することは，システム取得者および供給者間の権利義務関係の前提であり，合意された効用を提供する最低限の責務となる．

本活動は，単なる機能不全の防止にとどまらず，不法行為責任や社会的信用の失墜，さらには法的な罰則を防ぎ，平時においてシステムが正常に効用を発揮していることを担保する．これが欠けるとそもそも契約の目的が達成されないため，契約遂行の出発点となる最も根幹的なアクティビティとして選定した．

A.4.1.2　SLA/KPI 監視

契約に基づいた運用が客観的に履行されているか否かを追跡・証明するためには,「事実データの蓄積」が不可欠である．定量的指標である SLA および主要業績指標 (Key Performance Indicator, KPI) の定常的な監視 (monitoring) を行い，指標データの取得にとどまらず，その記録および適切な管理・保管を確実に行うことが重要となる．これにより，合意違反の有無を客観的に判定する根拠が確保され，ステークホルダ間の不必要な対立が防がれる．

主観や感情的な主張に依存せず，記録・管理されたデータに基づいて契約の履行状況を改ざんなく立証・評価できる状態を維持することは，契約関係の健全性を保つ上で不可欠な要素である．

A.4.1.3　規定手順に基づく復旧

想定内の故障や過失による障害発生時において，契約で事前に取り決めた範囲の手続き（手順書や SLA 規定）に従って一次対応および復旧作業を実施することが義務付けられている．

事前に合意された枠組み内での復旧手順の遵守は，障害による損害の拡大を防ぐと同時に，供給者側の責任範囲をあらかじめ定められた限度内に収め，二次的なトラブルを回避するために必須となる．

A.4.1.4　規定範囲内の通知・報告

障害や事故が発生した際，契約上の義務として定められた期限・手段・内容に基づきステークホルダへ事象を通知することが求められる．

タイムリーで形式を満たした通知は，取得者側の二次被害防止や代替措置の決定を可能にする．また，通知義務を適切に果たすこと自体が，報告遅延による追加的な契約違反リスクを未然に防ぐ重要な要素となる．

A.4.1.5　損害発生時の補償履行

契約不履行や SLA 未達によって損失が生じた際，事前に定めた損害賠償，ペナルティ支払い，返金等の補償手続きを遅滞なく履行することが，法律上および契約上の権利義務の精算において必須である．

金銭的・法的な補償の迅速な履行は，発生した不利益に対する実質的な責任追及を完結させ，契約関係における経済的不均衡を解消するための最終的な責務である．

A.4.1.6　責任範囲の確定と精算

契約関係の終了時や障害対応完了時において，各ステークホルダが負担すべき責任やコストの範囲を明確に確定・精算するプロセスが必要である．

責任の所在と負担範囲を確定させてクローズアウト（清算）を行うことで，過去の事象に対する果たすべき責任の完了が公的に客観化され，将来にわたる無制限・無期限の責任追及を防止する効果を持つ．

A.4.2　契約遂行チェックリスト

[C1]　明示的合意の同定と可視化

- □ 運用対象のシステムに関して，適用される法的契約，SLA，規約，仕様書等の明示的合意事項および付属規程（ポリシー）が網羅的に特定され，関係者間で共有されているか．
- □ 各合意事項における権利・義務および免責範囲が明確に区別・定義されているか．

表 1　契約遂行の活動項目と ISO/IEC/IEEE 15288:2023 とのマッピング

契約遂行の活動項目	15288 プロセス	15288 アクティビティ	15288 タスク
法令・契約遵守	Operation process (6.4.12)	Operational use (6.4.12.3 b)	Perform system operation (6.4.12.3 b) 1))
	Supply process (6.1.2)	Execute agreement (6.1.2.3 c)	Execute the agreement according to established terms and conditions (6.1.2.3 c) 1))
SLA/KPI 監視	Operation process (6.4.12)	Perform operation (6.4.12.3 b)	Track system operational service performance against agreements (6.4.12.3 b) 2))
	Quality assurance process (6.3.8)	Perform product or service evaluations (6.3.8.3 c)	Measure quality characteristics against contractual requirements (6.3.8.3 c) 1))
規定手順に基づく復旧	Maintenance process (6.4.13)	Perform maintenance (6.4.13.3 b)	Execute corrective maintenance and restoration per procedures (6.4.13.3 b) 2))
	Operation process (6.4.12)	Support operation (6.4.12.3 c)	Respond to operational incidents and requests according to procedures (6.4.12.3 c) 1))
規定範囲内の通知・報告	Supply process (6.1.2)	Execute agreement (6.1.2.3 c)	Provide required status reports to agreement parties (6.1.2.3 c) 3))
損害発生時の補償履行	Supply process (6.1.2)	Execute agreement (6.1.2.3 c)	Fulfill financial and legal obligations upon default (6.1.2.3 c) 4))
	Acquisition process (6.1.1)	Manage agreements (6.1.1.3 c)	Process claims and remedies per contractual terms (6.1.1.3 c) 2))
責任範囲の確定と精算	Supply process (6.1.2)	Agreement closure (6.1.2.3 e)	Settle liabilities and close out agreement obligations (6.1.2.3 e) 1))

[C2] 定常運用の履行と記録

- □ 合意された仕様，SLA，および付属規程を満たすようにシステムが適切に運用・保守されているか.
- □ SLA や KPI の達成状況を客観的に証明するためのログおよび指標データが取得され，合意された手順に従って安全に記録・管理されているか.

[C3] 規定手順に従った障害一次対応

- □ 想定内の障害発生時において，事前に合意された規定手順（障害対応マニュアル等）に則った一次対応および復旧作業が遅滞なく実施されているか.
- □ 契約上の条件を満たすタイムラインおよび手段で，障害の発生ならびに状況がステークホルダへ通知されているか.

[C4] 精算および補償手続きの実行

- □ 契約不履行や SLA 未達が発生した場合，合意された条件および範囲に基づいて，速やかに補償（損害賠償・ペナルティ等の精算）が履行されているか.
- □ 実施された責任履行手続きが，該当する明示的合意の範囲内において正当な根拠を持っているか.

A.5　状況把握

「状況把握」は，システムおよびその環境の状況を正確に観測し，論理的かつ客観的な観点から正しく分析し，開示する活動である．本活動は,「契約遂行」活動から完全に独立して実施されるものであり，自らの利益の保護や拡大の意図を持たない客観的な説明を可能にするとともに，ステークホルダや社会との深い信頼関係を構築する役割を果たす.

状況把握における具体的内容は，ISO/IEC/IEEE 15288:2023 に規定されたシステムライフサイクルプロセスにおいて，主にシステム評価，データ監視，測定・評価（Project Assessment and Control Process / Measurement Process），検証，妥当性確認（Verification Process / Validation Process），および品質保証，情報管理等のプロセス（Quality Assurance Process / Information Management Process 等）のアクティビティ・タスクとして割り振られる．表 2 に，状況把握の活動項目と 15288 プロセス体系とのマッピングを示す.

A.5.1　活動項目の選定理由（Rationale）

本ガイダンスにおいて選定した状況把握の各活動項目と，その選定理由は以下の通りである.

A.5.1.1　能動的観測と環境状況の把握

システムおよびその環境（物理的環境，関連する規約や標準，法令等）の状況を正確に観測・把握することは，客観的な説明責任を果たすための基盤となる事実（ファ

表 2　状況把握の活動項目と ISO/IEC/IEEE 15288:2023 とのマッピング

状況把握の活動項目	15288 プロセス	15288 アクティビティ	15288 タスク
能動的観測と環境状況の把握	Project assessment and control process (6.3.2)	Assess the project (6.3.2.3 b)	Assess project and technical status against plans (6.3.2.3 b) 1))
	Verification process (6.4.9)	Perform verification (6.4.9.3 b)	Observe and capture system behavior under actual conditions (6.4.9.3 b) 2))
観測手法・項目の不断の見直し	Measurement process (6.3.7)	Prepare for measurement (6.3.7.3 a)	Select and specify measures / Define procedures (6.3.7.3 a) 2))
	Quality assurance process (6.3.8)	Perform process evaluations (6.3.8.3 b)	Re-evaluate adequacy of monitoring items and tools (6.3.8.3 b) 1))
無私・客観的な分析と内部監査	Project assessment and control process (6.3.2)	Assess the project (6.3.2.3 b)	Conduct required management and technical reviews, audits (6.3.2.3 b) 3))
	Quality assurance process (6.3.8)	Perform product or service evaluations (6.3.8.3 c)	Evaluate products for conformance without bias (6.3.8.3 c) 1))
想定外事象・契約外活動の事実解明	Validation process (6.4.11)	Perform validation (6.4.11.3 b)	Analyze system behavior under unforeseen operational conditions (6.4.11.3 b) 2))
事実に基づく透明な情報開示	Information management process (6.3.6)	Perform information management (6.3.6.3 b)	Publish, distribute, or provide access to information to stakeholders (6.3.6.3 b) 2))
	Project assessment and control process (6.3.2)	Assess the project (6.3.2.3 b)	Record and provide status and findings from assessment tasks (6.3.2.3 b) 4))
情報提供者保護とアクセス制御	Information management process (6.3.6)	Prepare for information management (6.3.6.3 a)	Designate authorities/ responsibilities for access control (6.3.6.3 a) 3))

クト）を獲得する上で不可欠である．これは障害発生時のみならず，平時における準備活動としても定常的に実施される必要がある．

あらかじめ決められたデータのみを機械的に収集する受動的な対応にとどまらず，システムとその環境について積極的に情報を獲得しにいく能動的な姿勢を確保することが，正確な状況把握を達成する上で重要となる．

A. 5. 1. 2　観測手法・項目の不断の見直し

システムの複雑化や環境の変化に伴い，従来の観測項目や分析方法だけでは予兆や異常を捉えきれなくなるリスクが常に存在する．そのため，観測手法や項目自体を常に見直し，より正確な観測・分析を期すための再評価手続きを維持することが必要である．

過去の枠組みに固定化されず，観測精度を継続的に向上させる姿勢を明示的な活動として定義することで，未知の事象や潜在的リスクに対する感度を高めることができる．

A. 5. 1. 3　無私・客観的な分析と内部監査

収集されたデータに基づき，自社や特定のステークホルダの利益保護・拡大の意図を完全に排除した主観を交えない客観的な分析（内部監査を含む）を実施することは，分析結果の正当性と論理性を保証するために必須である．

特定の責任回避や不都合な事実の隠蔽を許さず，無私の立場から事象の真因や論理的帰結を分析・整理するプロセスを確立することが，システムの健全な把握と真の信頼関係構築に直接寄与する．

A. 5. 1. 4　想定外事象・契約外活動の事実解明

大津波やサイバー攻撃といった事前に明示的合意（契約）で想定されていない事象下においては，契約に含まれない臨機応変な対処や現場判断が避けられない．そのような契約外の活動や想定外の挙動に関しても，事実関係を正確に特定・分析対象とすることが求められる．

契約の範囲外で起きた出来事であっても，何が起き，どのような判断と行動がなされたのかを客観的に解明する活動項目を設けることで，想定外事象に対する状況把握の空白を防ぐことができる．

A. 5. 1. 5　事実に基づく透明な情報開示

得られた知見や分析結果を，自己の利益防衛や自己弁護の手段とすることなく，求めに応じてステークホルダおよび社会へ誠実に開示・説明することは，状況把握の最終的なアウトプットとして不可欠である．

過不足なく客観的事実を提示し，隠蔽なく説明し尽くす行動自体が，契約の履行関係を超えた高い信頼関係を築く原動力となる．

A. 5. 1. 6　情報提供者保護とアクセス制御

状況把握の実効性を担保するためには，内部情報提供者や調査対象者が自身への不利益をもたらす責任追求（解雇や賠償等）を恐れて事実を隠蔽・歪曲することを防ぐため，「免責的保護」に関する一定の考慮を，ジャスト・カルチャーの観点から導入することが必要である．

「状況把握」で得られた調査データや分析結果が,「契約遂行」における責任追及や損害賠償履行の根拠として転用されることは不当なので，適切な情報アクセス制御が実施されなければならない.

A. 5. 2　状況把握チェックリスト

[S1]　能動的観測体制の確立と見直し

- □ 平時および緊急時において，システム内部の状態のみならず周辺環境（物理環境，法令，標準等）のデータを正確に収集する観測体制が構築されているか.
- □ 既定の観測項目や手法に固執せず，システムの状況変化に応じて観測項目や分析方法を継続的に見直しているか.

[S2]　客観的分析および内部監査の実施

- □ 障害時および想定外事象の発生時において，自社の保身や特定ステークホルダの利益保護を排した，客観的・無私な立場からの事実分析および内部監査が実施されているか.
- □ 事実解明の分析プロセスにおいて，主観的解釈や偏見を排除し，ログや計測データに基づく論理的な原因追及がなされているか.

[S3]　情報開示と客観的説明の遂行

- □ 把握した事実および分析結果が，利益の保護・拡大を意図せず，ステークホルダに対して正確かつ論理的に開示・説明されているか.
- □ 契約に定めがない想定外事象下の活動に関しても，実施された事実関係が客観的に整理され，説明可能な状態となっているか.

[S4]　アクセス制御と内部情報提供者の保護

- □ 状況把握によって得られた情報や調査ログが,「契約遂行」担当者による不当な個人責任追及や損害賠償請求に転用されないよう，適切なアクセス制限措置が講じられているか.
- □ 内部関係者が事実を躊躇なく提供できるよう，調査目的以外の情報利用を制限する保護・情報運用のルールが徹底されているか.

A. 6　把握還元

「把握還元」は契約外答責活動と，フィードバック契約変更の二つからなる.

契約外答責活動は，緊急事態におけるシステム運用に際して遂行される活動で，契約にない，あるいは契約に矛盾さえし得るが「状況把握」活動による知見に基づくものである．いわゆる fit-for-purpose な活動がこれにあたる.

フィードバック契約変更は,「状況把握」活動による知見を組織の知識資産として定着させ，既存システムの改善や将来のシステム設計・運用，組織プロセスの高度化へフィードバック（還元）する活動である．これは,「状況把握」から得られた学びを一時的なものに終わらせず,再発防止や持続的な価値創出につなげる役割を果たす.

「把握還元」における具体的内容は，ISO/IEC/IEEE 15288:2023 に規定されたシステムライフサイクルプロセスにおいて，主に組織の事業イネーブリングプロセス（Knowledge Management Process / Quality Management Process / Infrastructure Management Process）およびテクニカルマネジメントプロセス（Decision Management Process / Risk Management Process 等）のアクティビティ・タスクとして割り振られる．表 3 に，把握還元の活動項目と 15288 プロセス体系とのマッピングを示す.

A. 6. 1　活動項目の選定理由（Rationale）

本ガイダンスにおいて選定した把握還元の各活動項目と，その選定理由は以下の通りである.

A. 6. 1. 1　観測・分析結果の知識体系化

「状況把握」において収集・分析されたデータや事故・障害の原因究明結果は，単なるログとして保存するだけでなく，再利用可能な知識資産として構造化・体系化する必要がある.

個人や単一プロジェクトの記憶に留めず，組織的に管理可能な形に変換（Transform）することで，同様の事象に対する対応コストを削減し，組織全体の知見として蓄積することが可能となる.

A. 6. 1. 2　システム設計・仕様への再発防止策フィードバック

分析によって得られた真因や改善点を，既存システムの改修や次世代システムのアーキテクチャ定義・要求仕様へ確実に反映させることは，同種障害の再発を防ぐための直接的な手立てである.

事実の把握だけに留まらず，システムアーキテクチャや設計基準の再定義（Refine）にまで踏み込むことで，システムのレジリエンス（回復力・強靭性）を本質的に向上させることができる.

A. 6. 1. 3　組織プロセス・基盤の持続的改善

技術的なシステム改修にとどまらず，システムの運用手順，開発標準，教育体制，さらには開発基盤・インフラに潜む課題に対しても是正処置・予防処置（Corrective and Preventive Actions）を講じることが不可欠である.

品質マネジメントプロセスを通じて組織全体のプロセス改善へ還元することで，個別の不具合対応を超えた組織能力（Organizational Capability）全体の向上を達成できる.

表 3　把握還元の活動項目と ISO/IEC/IEEE 15288:2023 とのマッピング

把握還元の活動項目	15288 プロセス	15288 アクティビティ	15288 タスク
観測・分析結果の知識体系化	Knowledge management process (6.2.6)	Maintain domain knowledge (6.2.6.3 b)	Maintain knowledge, skills, and assets for reuse (6.2.6.3 b) 1))
	Information management process (6.3.6)	Transform information into knowledge (6.3.6.3 c)	Maintain information assets for historical reference and learning (6.3.6.3 c) 1))
システム設計・仕様への再発防止策フィードバック	Decision management process (6.3.3)	Analyze decision information (6.3.3.3 b)	Evaluate lessons learned to support decision-making (6.3.3.3 b) 2))
	System architecture definition process (6.4.4)	Relate system to architecture (6.4.4.3 e)	Refine architectural elements based on operational feedback (6.4.4.3 e) 1))
組織プロセス・基盤の持続的改善	Quality management process (6.2.5)	Perform quality management evaluation (6.2.5.3 c)	Implement corrective and preventive actions based on assessment findings (6.2.5.3 c) 2))
	Infrastructure management process (6.2.2)	Maintain infrastructure (6.2.2.3 c)	Improve organization infrastructure using operational experience (6.2.2.3 c) 1))
教訓の組織横断的共有	Knowledge management process (6.2.6)	Share knowledge (6.2.6.3 c)	Share lessons learned and best practices across projects (6.2.6.3 c) 1))
契約外答責活動	Operation process (6.4.12)	Perform operation (6.4.12 a)	Use the system in its intended operational environment (6.4.12 a) 1))
		Manage results of operation (6.4.12 c)	Record results of operation and any anomalies encountered (6.4.12 c) 1))
			Record operational incidents and problems and track their resolution (6.4.12 c) 2))
			Maintain traceability for operations (6.4.12 c) 3))

A. 6. 1. 4　教訓（Lessons Learned）の組織横断的共有

特定のプロジェクトで得られた成功要因や失敗の教訓（Lessons Learned）を，組織内の他部門や将来の新規プロジェクトへ迅速かつ効果的に共有・流布（Share）する仕組みを維持することが重要である．

部門間のサイロ化を防ぎ，組織全体で教訓を共有・活用することで，同一の過ちの繰り返しを防止し，イノベーションと効率化を加速させることができる．

A. 6. 1. 5　契約外答責活動

想定外事象が発生した時に，契約の範囲外の活動や，契約に矛盾する活動であっても，「状況把握」の結果から，必要だと判断されれば，その活動を遂行する．

契約にない，あるいは契約と矛盾する活動なので，その妥当性のステークホルダによる事後承認が求められる．そのために必要な記録を残しておくことが必要である．

A. 6. 2　把握還元チェックリスト

[K1]　事実と知見の知識化

- □ 「状況把握」で解明された事実，原因，得られた知見が，客観的なデータとして知識ベースやアーカイブに構造化されて登録されているか．
- □ 単なる事実の記録にとどまらず，他プロジェクトでも参照可能な一般的な教訓として整理されているか．

[K2]　システムおよび設計へのフィードバック

- □ 明らかになった課題や再発防止策が，システム要求仕様，アーキテクチャ設計，運用マニュアル等へ確実に反映・更新されているか．
- □ 意思決定プロセスにおいて，過去の分析結果や知識が客観的な判断材料として活用されているか．

[K3]　組織プロセスおよび基盤の改善

- □ 根本原因分析の結果に基づき，開発標準，品質保証ガイドライン，インフラ構築基準などの組織的プロセスに対する是正・予防処置が取られているか．
- □ プロセス改善の実施結果が評価され，継続的な品質向上サイクルが機能しているか．

[K4]　組織横断的な知識共有と活用

- □ 得られた教訓（Lessons Learned）やベストプラクティスが，プロジェクトや部署の壁を越

えて共有される仕組み（研修，レビュー，知識共有会議等）が存在するか.

□ 新規プロジェクトの立ち上げ時や要件定義時に，過去の還元事例を参照・活用する規律が定着しているか.

B　古事記伝抜粋

B.1　古事記伝一ノ巻より

ウシハクは，大人佩（うしはく）にて，我私の物として，己が心のままに領き支配（まつりご）つ意にて，異国の君たちの，国を己が物にして，己が心のままに政をする，是即ちウシハクなり.

B.2　古事記伝四十四ノ巻より

凡（すべ）て強威（強き勢ひ）を振ひて，自ら領有（ウシハ）き居るをば，うしはくと云ふ

B.3　古事記伝一ノ巻より

シラスは，知らすにて，其国の万の事を，あまねく知り給ふの意なり．されば下に在る万の民，物をも，我が私の所有（もの）とは見給はず，皆天つ神の御国の御民御物なるを，其天つ神の御代として，あまねく知らしめ給ふを，シラスとは云ふなり．皇国の御代々の天つ日嗣は，此天つ神の御霊をうけ給ひて，ただ大御神の御心を御心として，天下を照らしシラシ給ふのみにして，一毫（いちごう）も我が私の御心は交り給はず.

B.4　古事記伝一ノ巻より

大御神の，あまねく天下を照し給ふがごとく，御代々のすめらみことも，其大御心をおのれが心と意識（おひ）給ひて，ただ大公無私（オホオホヤケ）に，天下の万の事を，あまねく照らし知り給ふを，シラスとは云ふなり.

かるがゆゑに，下にある民（たみ）も，皆大御神の御民（みたみ）として，愛（めぐ）み養ひ給ふによりて，天下おのづから平らけく安らけく，御治（ミシラ）すこと，神ながらの道にして，さらに人の智巧（サトシキタクミ）を加へ給はず.