安全で安心な情報システムを提供する安全・安心チェック

Safety and Security Check Process of Information Systems for Deliver to Customers

鈴 木 龍 生

要　約　2010年代半ば以降，自社製品だけで情報システムを構築する案件は減少し，他社製品を利用した情報システムを構築する案件が増えてきている．他社製品を扱う際，開発プロジェクトに他社製品に対する知見や取引実績が伴わない場合，そこに潜むリスクに気が付かないままプロジェクトを進め，リスクを顕在化させる可能性がある．

このリスクに対し，プロジェクトが認識し，回避・低減を図ることを目的に，2020年に安全・安心チェックプロセスを策定し，運用を開始した．本プロセスでは，外部調達ハードウェア，外部調達サービスシステム，ブロックチェーン技術，AI技術の四つのカテゴリについて，リスクを俯瞰的・網羅的に洗い出したチェックリストを用いることで，多くの開発プロジェクトに適切なリスク対策を施すことができる．

Abstract　Since mid-2010s, fewer information systems are constructed using only in-house products, whereas more information systems are constructed using products manufactured by other companies. When handling products made by other companies, the project will proceed without being aware of the hidden risks, and the risks may increase, if the development project should not involve knowledge or transaction experience regarding other companies' products,

In 2020, we formulated and began operating a safety and security check process with the aim of making projects aware of these risks and working to avoid and reduce them. In this process, by using a comprehensive checklist that provides an overview of risks in the categories of externally procured hardware and service systems, blockchain technology, and AI technology, it is possible to implement appropriate risk countermeasures for many development projects.

1. はじめに

BIPROGY株式会社（以降，BIPROGYまたは当社）は，1958年の設立から1990年代初頭まで汎用機を中心とした自社ハードウェア販売をビジネスの主体としてきた．その売上は7割を占め，保守サービスやソフトウェアといったサービス関連売上は3割であった．1990年代からのコンピュータのダウンサイジングやオープン化により，ビジネスの主体は情報システム開発を中心としたシステムサービスやサポートサービス，アウトソーシングにシフトし，2020年代ではサービス関連売上が7割を占め，BIPROGYとグループ会社（以降，BIPROGYグループ）のビジネスの根幹となっている．

サービス関連売上の中核を成す情報システム開発も，コンピュータ技術の進化とそれに伴う顧客ニーズの高度化・複雑化により，自社製品だけでなく他社製品を利用した情報システムを構築する傾向にある．また，ブロックチェーン技術やAI技術といった新しい技術を使用する情報システムも増えつつある．

本稿では，BIPROGYが顧客へ高品質で安全な情報システムを提供するために構築している

品質保証プロセスについて述べる．まず 2 章で品質保証プロセスの全般的な取り組み，そして 3 章で他社製品や新技術を使用する際に発生するリスクを回避・低減させる安全・安心チェックの概要を述べ，4 章で今後の取り組みについて記す．

2. 品質保証の取り組み

情報システムの社会インフラとしての重要度は増し，求められる品質レベルはより高まっている．BIPROGY では，顧客へ高品質で安全で安心な情報システムを提供するため，図 1 に示すような各種管理プロセスに基づく品質保証の体制・仕組みを構築・整備している．本章の各節で説明する．

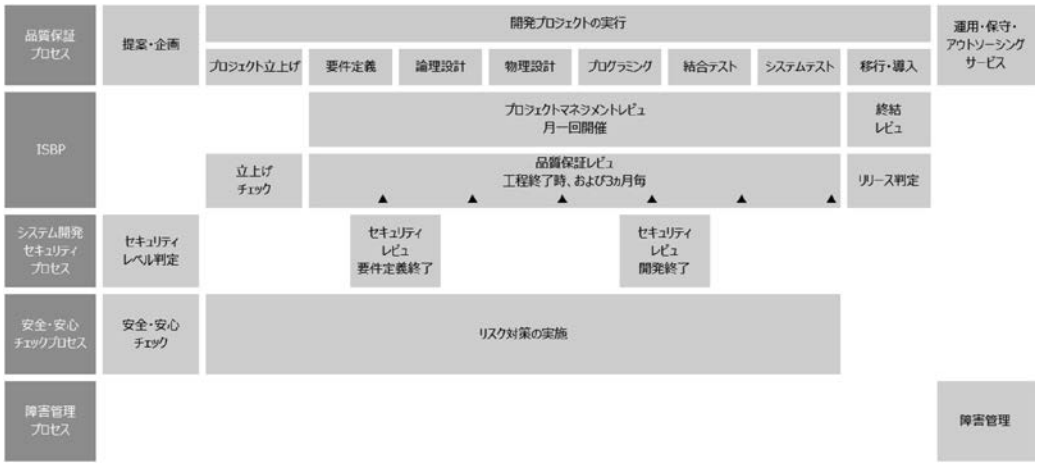


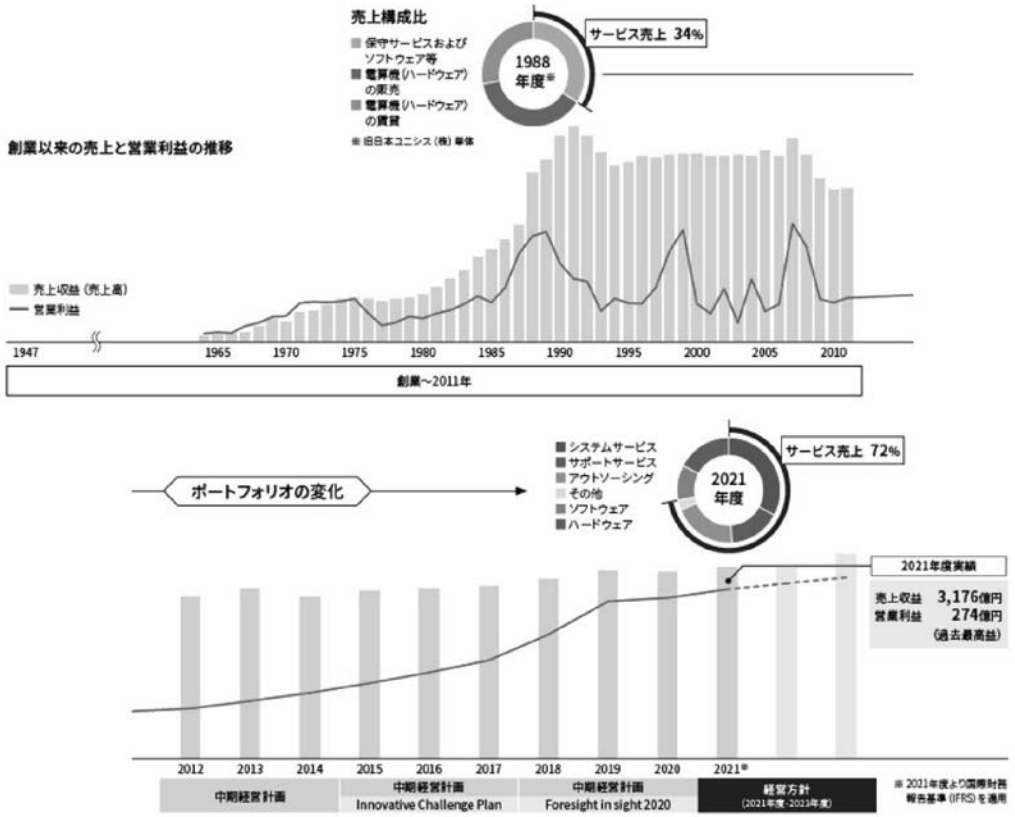
図 1　品証保証の各種プロセス

2. 1　ISBP（Information Service Business Process）

図 2 に示すように，1988 年度と 2021 年度を比べると，BIPROGY のポートフォリオは大きく変化している．すなわち，ビジネスの主流が情報システム開発を中心としたシステムサービスに変化した．そんな中，要求仕様のベースライン化不良や品質問題，納期遅延，本番サービス開始後に影響度の大きな障害を発生させるプロジェクトが一定の割合で存在し，顧客の信頼を損なうと同時に，当社収益にも影響を与える経営課題となっていた．

この課題を解決するため，BIPROGY は品質保証の根幹となるプロセスである ISBP を定めて運用を開始した．ISBP は，顧客の要求に適した開発の手段を定めた「エンジニアリングプロセス」，開発プロジェクトの状況を品質・コスト・進捗の視点で可視化しコントロールする「プロジェクト管理プロセス」，正しい手続きで情報システムが作られていることを各開発工程で確認・保証する「品質保証プロセス」で構成されており，システム開発規模が一定金額以上かつリスクの高い開発プロジェクトを対象に運用する．

開発プロジェクトの立ち上げから本番サービス開始までの間，エンジニアリングプロセスの手順に従い，開発プロジェクトが適切にコントロールされ，品質が確保されていることを各種レビュで確認し，問題を早期に発見・解決することを目的としている．その各種レビュのうち主要なものの概要を表 1 に示す．ISBP の導入前，問題を抱えるプロジェクトは全体の 10%程度存在したが，ISBP が社内に浸透するにつれ減少し，2020 年代には 3%に低下している．



出典：BIPROGY 統合報告書[1]

図 2　BIPROGY グループの売上構成の変化

表 1　ISBP の各種レビュ

レビュ名	実施タイミング	レビュ観点
プロジェクト立ち上げチェック	プロジェクト立ち上げ時	・実行プロジェクトの作業，コスト，リソース，リスクおよび各種管理プロセスの計画とコントロール方法を確認し，プロジェクトの実行開始を承認する．レビュ結果を青・黄・赤で判定する 青：問題がない，もしくは問題があるが適切にコントロールされている 黄：問題はあるが，プロジェクト内で対応が可能 赤：問題があり，プロジェクト内での対応は難しく上位もしくはプロジェクト外部からの支援を要する
プロジェクトマネジメントレビュ	プロジェクト実行時/1 ヵ月毎に実施	・プロジェクト活動計画と対比してプロジェクトの状況（進捗/品質/コスト費消/リスクの遷移/課題対応）を確認し，指摘・改善勧告を行い，レビュ結果を青・黄・赤で判定する
品質保証レビュ	プロジェクト実行時/開発工程終了時もしくは 3 ヵ月毎に実施	・プロジェクト活動計画と対比してプロジェクトの状況（進捗/品質/コスト費消/リスクの遷移/課題対応）を確認し，指摘・改善勧告を行うと共に，現フェーズ継続可否や次フェーズ進行可否を審査し，レビュ結果を青・黄・赤で判定する

リリース判定レビュ	リリース前	・開発フェーズ終了時点までの品質状況，財務状況，進捗状況，および，カットオーバクライテリアの達成を評価し，リリース可否を判定する ・本番サービス開始の準備状況（本番移行時の計画/体制/本番サービス開始後の運用・保守の準備等）を評価し，リリース可否を判定する
終結レビュ	本番サービス開始2～3か月後	・本番運用状況を確認し，開発プロジェクトを総括する ・計画通りとならなかった開発プロジェクトは，その失敗要因等について，計画を達成した開発プロジェクトは，その成功要因等について振り返りと原因分析を行い，ドキュメントを残す

2.2　システム開発セキュリティプロセス

1990年代後半よりインターネットの普及に伴い，それまで社内システムとして利用されていた情報システムは，ネットバンキングやeコマース等インターネットを介して企業間や消費者にサービスを提供するシステムにも利用され始めた．インターネットシステムは，マルウェアの侵入によるコンピュータの乗っ取りや機密情報・個人情報の流出，大量のパケットを送り込みシステム停止に追い込む，システムを暗号化し身代金を要求する，といったサイバー攻撃等，様々な脅威に晒されているため，情報システム構築に際しては十分なセキュリティ対策を施さなければならない．

2002年度，セキュリティ対策が施された情報システムを顧客へ提供することを目的に，表2に示すシステム開発セキュリティプロセスを整備し，開発規模に依らず全開発プロジェクトを

表2　システム開発セキュリティプロセスの概要

サブプロセス	サブプロセスの概要
セキュリティレベル判定	・構築する情報システムが取り扱うデータの機密度[*1]およびシステム形態により，セキュリティレベルを設定する セキュリティレベル 高：データの機密度が高，もしくはインターネットシステム 中：データの機密度が中，かつインターネットシステム以外 低：データの機密度が低，かつインターネットシステム以外
セキュリティレビュ	・構築する情報システムのシステム基盤，アプリケーションシステムを対象にシステム特性に応じたセキュリティ対策を，チェックチートを基に論理的に机上確認し，指摘・改善勧告を行う セキュリティレベル高：セキュリティ技術主管による第三者レビュ セキュリティレベル中・低：プロジェクトもしくは組織内有識者によるレビュ ・要件定義フェーズ終了時，プログラム開発フェーズ終了時の2回実施を基本とし，要件定義フェーズ終了時の指摘・改善指示への対応をプログラム開発フェーズ終了時に確認する
脆弱性診断	・結合テストフェーズ以降，構築された情報システムに対し，脆弱性の有無をテストツールによって物理的に実機確認し，指摘・改善勧告を行う ・診断対象は，システム基盤，Webアプリケーション，スマホアプリケーションである

対象に適用を開始した．構築する情報システムの特性に応じてセキュリティレベルを判定し，チェックシートに基づくレビュと実機を用いた脆弱性診断でセキュリティ対策を確認し，改善勧告を行い是正させるプロセスである．

セキュリティレビュで使用するチェックシートは，日々変化する脅威に対し適宜見直し，構築する情報システムに対し最新のセキュリティ対策を施している．また，2022 年度よりセキュリティレベルが高となる開発プロジェクトに対し，セキュリティ技術者研修の受講者をアサインすることを義務付け，開発する情報システムの特性に応じたセキュリティ対策が開発段階で漏れなく実施されることを目指している．

2. 3　障害管理

本番サービス開始後も，顧客が安心して情報システムを利用するために，運用管理を委託されたプロジェクトやアウトソーシングサービス等において，情報システムの品質が保たれていることを継続的に確認している．しかしながら，顧客の情報システムに万が一障害が発生した場合，障害対応だけでなく，発生時点での社内関連部署への迅速な情報伝達・エスカレーションを行い，顧客への的確な初動対応と報告，その後の状況フォローといった対応も同時並行で実施するべきである．

BIPROGY グループでは，障害が与える影響度に応じたエスカレーションルートを定めた障害管理体制を整備し，障害管理システムで障害を早期に捉え，的確な指示の下，顧客フォローを含めた障害対応を図っている．発生した障害に対し，その対応だけで完了とするのではなく，根本原因を分析し再発防止策も定め，BIPROGY グループ内で共有し未然防止へ繋げている．

2. 4　安全・安心チェックプロセス

2010 年代半ばから，情報システムを取り巻く環境は大きな変化を遂げている．IoT やセンサーの技術は著しく向上し，家電製品等今まで情報システムと切り離されていた機器（以下，ハードウェア）とも連動するようになった．また，情報システムの稼働環境は，Azure[*2] や AWS[*3] といったクラウドシステムに移行し，その構築も一から行うのではなく，ベンチャー企業を含めた様々な企業から提供されるサービスシステムを採用し組み合わせて開発することが増えてきている．また，ブロックチェーン技術や AI 技術といった新しい技術が出現し，これらを利用した情報システムのニーズも高まっている．そのような情報システムを開発する際，開発プロジェクトに知見や取引実績が伴わないと，顧客へ損害を与え，当社収益へ悪影響を与えるリスクを顕在化させることがある．これらのリスクをプロジェクトが認識し，回避・低減を図ることを目的に，2020 年に安全・安心チェックプロセスを策定し，運用を開始した．次章では，安全・安心チェックプロセスの概要を述べる．

3.　安全・安心チェックプロセスの概要

他社が製造したハードウェアやサービスシステム，新技術を利用する情報システムを開発する際，機能面の品質不良による開発期間の延伸，本番サービス開始後の障害の頻発，障害対応の長期化，といった問題を引き起こすことがある．その原因の多くは，開発プロジェクトに他社が製造したハードウェアやサービスシステム，新技術に対する知見や取引実績が不足していたため，事前にリスクや留意すべき事項を認識できず，適切なリスク対策を講じないまま開発

プロジェクトを進めたことにある．本章では，外部調達ハードウェアと外部調達サービスシステム，ブロックチェーン技術，AI 技術を利用する際に潜むリスクと留意すべき事項を例示し，安全・安心チェックプロセスの概要を述べる．

3. 1　潜むリスクと留意点

本節では，外部調達や新技術利用に潜むリスクとそれが顕在化した際に起こり得る事象を整理する．

3. 1. 1　外部調達ハードウェア

コンピュータは年々小型化が進み，2023 年現在は家電製品，自動車，検査機器といったハードウェアにも組み込まれている．またネットワークの無線化も進んだことにより，ハードウェアと連動した情報システムが提供されている．

特に可動式のハードウェアや発火機能のあるハードウェアの場合，不具合があると人体や資産に損害を与える可能性があり，製造物責任法（PL 法）[2]への対処等，製品安全に係る法令や基準の遵守が求められる．ハードウェアを利用した情報システムを構築する際，ハードウェアの機能面を評価するだけではなく，ハードウェア自体の安全性や，アフターサービスを始めとする顧客支援の体制，万が一の事態に備えた保険の加入等，供給元企業自体に対する評価も行う．ハードウェアの外部調達に潜むリスクと，そのリスクが顕在化した場合の事象を表 3 に例示する．

表 3　外部調達ハードウェアのリスクと顕在化した際の事象

リスク	顕在化した際の事象
供給元企業および製品が法令や規格，基準に準拠していない	・安全な製品が供給されず，人の生命や人体，または財産へ係る被害を生じる
問合せや不具合・インシデントに対する体制が整備されていない	・問合せ対応や不具合調査に時間を要し，利用者の利便性を損ない，利用者が本来得られる利益を享受できない ・他の利用者への対応も遅れ，損害を大きくする
顧客・供給元企業との役割分担が不明確	・責任分界点が明確でなく，障害等の対応に時間を要する ・障害対応のコスト負担が適切に配分されない
保険に未加入	・事故が発生した場合，損害賠償を負担できない

3. 1. 2　外部調達サービスシステム

顧客ニーズが多様化・複雑化し，スピード開発も求められる中，クラウド上に提供されているサービスシステムを利用した情報システム開発が主流となりつつある．

他社が製造したサービスシステムを初めて利用する際，そのサービスシステムに対する知見が少ないため，十分な品質が伴わず開発期間が延伸する，本番サービス開始後に障害が頻発する，といった不利益を顧客へ与え，当社収益にも影響を及ぼす可能性がある．それを回避するためには，供給元企業と情報セキュリティ・役割分担等をサービス開始前に取り決め，協力関係を築いておくことが得策である．サービスシステムの外部調達に潜むリスクと，そのリスクが顕在化した場合の事象を表 4 に例示する．

表 4　外部調達サービスシステムのリスクと顕在化した際の事象

リスク	顕在化した際の事象
企業ポリシー（情報セキュリティ指針，個人情報保護方針等）が確立されていない	・事故対応の連絡ルート，体制も整備されておらず，顧客へ適格な初動対応や報告，フォローが実施できない ・情報管理に対して社員教育が行き届かず，機密情報や個人情報が流出する
認証（ISMS，P マーク，PCIDSS 等）を取得していない	
顧客・供給元ベンダとの役割分担が不明確	・責任分界点が明確でなく，障害等の対応に時間を要する ・障害対応のコスト負担が適切に配分されない
供給元ベンダの企業体力	・企業体力が脆弱なため，開発要求や問合せ，障害への対応が遅くなる ・デリバリを優先し品質の伴わないサービスを提供する

3. 1. 3　ブロックチェーン技術

ブロックチェーンには，不特定多数のユーザが分散してデータを保持するため，データの改ざん耐性が強く透明性が高い，不特定多数のユーザがお互いの情報を記録するため，システムダウンが起きにくいという特徴がある．高信頼性，透明性が求められる金融業界や医療業界の他，製造業や流通業等のグローバルサプライチェーンでも利用されており，様々な用途での調査・研究も進められている新技術である．

しかしながら，メリットに対してデメリットも合わせ持っている．ブロックチェーン技術を利用するには，これらを理解しておくことが望ましい．ブロックチェーン技術を利用した情報システムを提供する際の留意すべき事項を表 5 に例示する．

表 5　ブロックチェーン技術の留意点

観点	留意点
信頼性	・ブロックチェーンの障害許容性，回復性はネットワークを構成するサーバ台数によるため，十分な数のサーバを確保しなければならない
効率性	・ブロックチェーンのレスポンスタイム，スループットは採用するブロックチェーン技術に依存するため，一般的に RDB と同等の性能の実現は困難である
機密性	・ブロックチェーンに記録したデータは修正・削除ができず，利用者からの削除依頼に対応できないため，個人情報の管理には適さない ・コンソーシアム型の場合，ブロックチェーンに記録したデータはネットワーク全体に共有されるため，複数企業でネットワークを構成する際，参加企業全体に公開されることに合意せざるを得ない
保守性	・コンソーシアム型の場合，ネットワークを構成するすべてのサーバを停止しない限りシステム全体を停止することができないため，複数企業でネットワークを構成する際，参加企業全体で停止および開始の承認プロセスを整備しなければならない

3. 1. 4　AI 技術

AI 技術は，多種多様なデータを機械学習させて最適解を導く技術である．とりわけ生成 AI は ChatGPT[*4] の出現により，人々にとってより身近な存在となっており，今後も様々な場面で AI 技術が利用される社会になっていくと予想される．

しかしながら，2023年においては，フェイク動画による社会扇動や，顔認証AIによる人種差別，自動運転車による人身事故，人材採用AIシステムによる性差別等，社会問題となる事例も発生している．AI技術を利用した情報システムを提供する際の留意点を表6に例示する．

尚，BIPROGYグループでは，2020年2月に「BIPROGYグループのAI倫理指針[3]」を策定し遵守することを社外に公表している．

表6　AI技術の留意点

観　点	留意点
AI倫理	・「BIPROGYグループのAI倫理指針」を遵守していること
フェールセーフ機能	・AIモデル部分の誤判定や，精度劣化によるリスクを認識した上で，AIシステム全体または人的に対処するフェールセーフ機能を備え，顧客と合意すること
生成AI	・入力情報に機密情報や個人情報を登録する場合，その情報が結果に含まれることを認識した上で，情報漏洩リスクへの対策を行い顧客と合意すること ・自動生成された結果には，誤った情報や他人の権利の侵害や，不適切・有害な内容が含まれる恐れがあると認識した上で．結果を必ず精査すること

3.2　安全・安心チェックプロセスとは

本節では，安全・安心チェックプロセスの概要について述べる．

3.2.1　安全・安心チェックリスト

安全・安心チェックリストは，外部調達ハードウェア，外部調達サービスシステム，ブロックチェーン技術，AI技術の四つのカテゴリに対し，リスクを俯瞰的・網羅的に洗い出したものであり，どの開発プロジェクトでも適切なリスク対策を施すことができる．

外部調達ハードウェア，外部調達サービスシステムに対しては「供給元企業の信頼」「製品の安全性」「顧客および供給元企業との役割分担」の視点でリスクを整理し（表7），ブロックチェーン技術，AI技術に対しては，前節で述べた留意すべき事項をリスクとして整理している．

表7　外部調達ハードウェア/サービスシステムのチェックリスト例

リスク項目	確認事項
供給元企業の信頼性	・反社会勢力でない/財務状況が健全 ・相応の法令や規律の準拠および相応の外部認証資格を取得 ・個人情報保護等情報システム管理システムを構築 ・問合せやインシデント対応の体制を整備
製品（ハードウェア，サービスシステム）の安全性	・製品が満たすべき法令や規格，基準に準拠し，表示すべき認証マークの表示 ・安全を確保するために，未然防止の機能や誤使用を防ぐための情報を提供 ・サイバー攻撃等に備えたセキュリティ対策
顧客および供給元企業との役割分担	・サービスレベルアグリメントの存在と明文化 ・事故発生時の責任範囲（責任分界点，事故調査時の情報提供等）を取り決め，明文化している ・製品の開発やアフターサービスに対応する十分な要員を確保
その他	・当該製品に関係する保険（PL保険，リコール保険等）を付与

安全・安心チェックリストは2019年度までの事例を基に作成し，2023年に生成AIに対するチェック項目を追加した．また，ローコード・ノーコード開発に対しても顧客の期待が高まっており，今後継続的に改善を図っていく．

3.2.2　安全・安心チェックプロセスの流れ

提案・企画フェーズで，安全・安心チェックリストを基にリスクを認識し，リスクの回避・低減に向けて対策を検討する．BIPROGY内で解決できないリスクは，供給元企業や顧客とリスク対策（回避・低減・移転・保有）を協議し決定する．特に，責任分界点は，顧客・供給元企業との3者間において合意形成を行う．

提案・企画フェーズで対策が定まらないリスクがある場合，開発フェーズにおいても検討を継続実施する，本番サービス開始までに全リスクに対して対策を講じ，3者間での合意形成を図る（図3）．

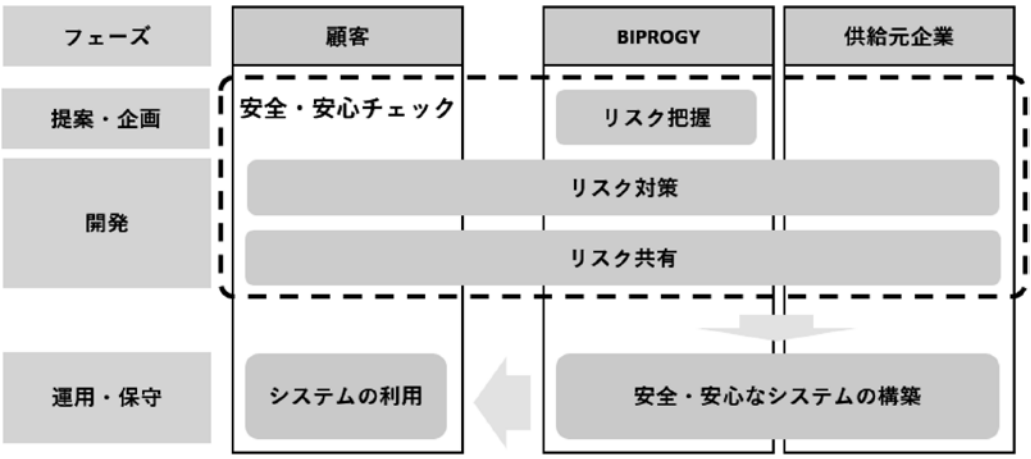


図3　安全・安心チェックプロセスの概念図

開発フェーズや保守・運用フェーズにおいて，新たに外部調達するハードウェアやサービスシステム，新技術を利用することになった場合，あらためて安全・安心チェックを実施する．情報システムのライフサイクル全般を通じ，安全で安心な情報システムの提供を保証するプロセスである．

4.　今後の取り組み

安全・安心チェックプロセスは，2020年度から運用を開始しており，今後も改善を継続する．

4.1　安全・安心チェックプロセスの定着に向けて

2020年からの年度別の実施件数を図4に示す．尚，2023年度は4月から8月までの集計値である．

外部調達サービスシステムの実施件数が最も多い．2020年度実績に対し，2021年度，2022年度の実績は低調であったが，本プロセスの浸透が進んでおり，2023年度は2020年度実績を上回る見込みで，今後も増加が予想される．

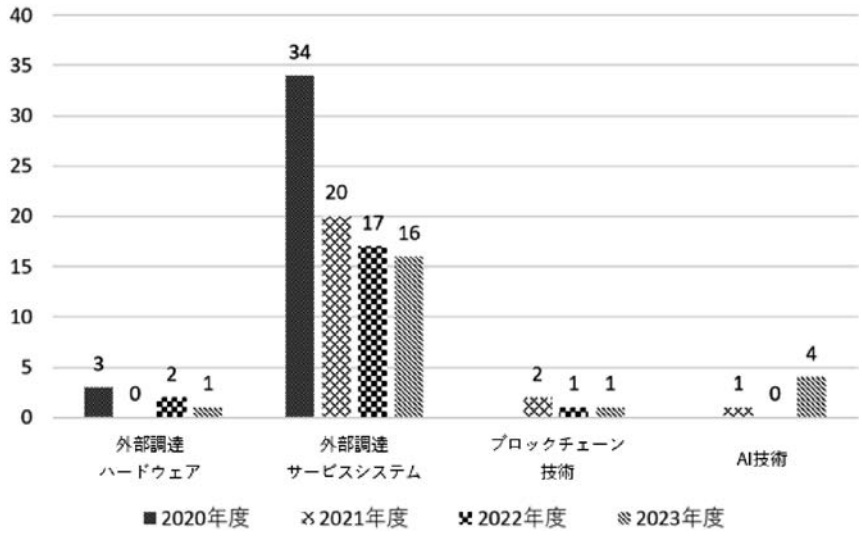


図 4　安全・安心チェックの実施件数

外部調達ハードウェア，ブロックチェーン技術，AI 技術の実績は各年度とも数件に留まっているが，AI 技術は 2023 年の ChatGPT の出現により世間の注目度が高まっており，多くの情報システムで利用されることが見込まれる．

今後，対象となる情報システム開発案件が発生した際，どの開発プロジェクトでも本プロセスを漏れなく実施できるよう，社内ホームページでの情報発信による啓発活動を引き続き実施すると共に，e ラーニングによる教育環境を整備し，社内への浸透・定着に向けて取り組んでいく．

4. 2　安全・安心チェックプロセスのグループ会社適用

安全・安心チェックプロセスは BIPROGY を対象としたプロセスである．今後，BIPROGY グループ各社に共有を図り，各社で実施している安全で安心な情報システムを提供するプロセスへ，業態やビジネス内容に応じた全面的・部分的な組み込みを促進する．そして，BIPROGY グループ全体として「情報システムの提案・企画から開発，保守・運用まで安心して任せられるグループ企業」を目指していく．

5. お　わ　り　に

BIPROGY では，ISBP，システム開発セキュリティプロセス，障害管理に本稿で述べた安全・安心チェックプロセスを加えた品質保証プロセスを構築・整備しており，2022 年 6 月の情報流出につながりかねなかった USB メモリー紛失事故の再発防止にも取り組んでいる．しかし 2023 年 11 月，セキュリティ設定不備によるお客様情報等の漏えいが確認される事案が発生した．このような事態を重く受け止め，ルール（仕組み）ベースと，業務で取り扱う情報リスクについて当事者意識をもって考え行動するプリンシプル（意識醸成）ベースの両面における再発防止対策を強化し，継続的に改善していく．

最後に，安全・安心チェックプロセスの構築・推進に携わった BIPROGY 関連部署諸氏に感謝の意を表す．

＊ 1　データの機密度は以下の 3 段階を定義している.
高：国家機密情報・生命やプライバシーに係る個人情報・機密度が高と顧客が判断する情報等
中：機密度高に分類されない個人情報・機密度が中と顧客が判断する情報等
低：不特定多数に公表できる情報・一般的な Web 情報等
＊ 2　Microsoft 社が提供するクラウドサービス.
＊ 3　Amazon Web Services, Inc. が提供するクラウトサービス.
＊ 4　OpenAI 社が提供する生成 AI システム.

参考文献

［1］ 統合報告書 2022，BIPROGY，2022 年 3 月，P12 ～ 13
https://pr.BIPROGY.com/invest-j/ir/pdf/ir2022.pdf
［2］ 製造物責任法（平成六年法律第八十五号），デジタル庁
https://elaws.e-gov.go.jp/document?lawid=406AC0000000085
［3］ BIPROGY グループの AI 倫理指針，BIPROGY，2022 年 5 月 16 日
https://www.biprogy.com/com/ai_ethics_principles_BIPROGY_group.pdf

※　上記参考文献に含まれる URL のリンク先は，2023 年 10 月 25 日時点での存在を確認.

執筆者紹介

鈴　木　龍　生（Ryusei Suzuki）
1991 年日本ユニシス(株)入社．以来流通小売および通信販売を中心にフィールド SE としてユーザへの開発業務に従事．2018 年より品質マネジメント部にて，システム開発セキュリティプロセスの主管業務に従事し，2022 年より安全・安心チェックプロセスの主管業務を兼務.