情報セキュリティに関する安全・安心の確保に向けた取り組み

Initiatives Aimed at Ensuring Safety and Security Regarding Information Security

瀧 谷 龍 二

要　約　2022年6月にBIPROGYの協力会社社員によるA市における個人情報を含むUSBメモリー紛失事案が発生した．事業存続が危ぶまれる状況となり，全てを見直す覚悟でおこなった第三者委員会調査では，「コンプライアンス意識の欠如」が指摘される厳しいものであった．BIPROGYは，総合的再発防止策の中で，顧客機密情報を対象とする対応は，セキュリティ専門組織により管理・モニタリングする特例運用管理を実施することに加えて，内部監査人協会の3ラインモデルに準拠し内部監査を適用することとした．特例運用管理と内部監査は，顧客機密情報を対象とする対応を厳格に管理するとともに，コンプライアンスとリスク管理を意識に根付かせていく狙いがある．さらにルールと仕組みを前提とした再発防止策だけでは，今後の事案の風化，意識の希薄化を防げないと考え，意識醸成の施策として，全役職員への意識浸透プログラムや毎年事案発生日を含む週を情報セキュリティ週間と設定し，事案の振り返り，研修やセッションを実施することとした．これらの施策を徹底することにより，一日も早く信頼を取り戻しお客様とともに更なる社会課題の解決に貢献していきたい．

Abstract　In June 2022, an employee of a BIPROGY partner company lost a USB memory stick containing personal information in A City. The situation put BIPROGY's business survival in jeopardy, and the results of the third-party committee investigation, which BIPROGY requested with the determination to review everything, were harsh, pointing to a "lack of compliance awareness". As part of comprehensive measures to prevent recurrence, BIPROGY decided to make operations that handle confidential customer information as exceptional operations, and to have them managed and monitored by a specialized security organization, as well as to conduct internal audits based on the three-line model of the Institute of Internal Auditors. The management and internal auditing as exceptional operations are intended to strictly control operations that handle confidential customer information, as well as to root compliance adherence and risk management in the consciousness of the company. Furthermore, we believe that preventing recurrence based on rules and mechanisms alone will not prevent incidents from fading away and diluting awareness. As awareness-building measures, we will implement an awareness-building program for all officers and employees, and set the week including the day of the incident as Information Security Week every year to review the incident and hold training and sessions. By thoroughly implementing these measures, we hope to regain trust as soon as possible and contribute to solving social issues together with our customers.

1. はじめに

2022年6月21日，BIPROGY株式会社（以降，BIPROGY）の協力会社社員によるA市における個人情報を含むUSBメモリー紛失事案が発生した．顧客の重要な情報を扱う企業として，あってはならない重大な事案であり，事案対応で業務の停滞に加え，取引停止，内定者の

辞退なども発生し事業存続が危ぶまれる状況になった（以降，重大事案または本事案と呼称する）.

BIPROGY はこれまでも情報セキュリティを推進する体制や従業員への教育を常におこなってきたが，そのような中において重大な事案が発生してしまい，全てを見直す覚悟で，外部有識者による第三者委員会を設置し原因の調査をおこなった.

調査では，事案に至った原因として，情報セキュリティ面のリスク管理やモニタリングなどの問題が掲げられる一方，「コンプライアンス意識の欠如」も大きな問題であると厳しく指摘された.

この指摘を受け，BIPROGY は，再発防止策の要として顧客の重要な情報を扱う業務を通常運用ではない特例運用と位置づけ，その管理を特例運用管理とする制度を整備した．特例運用管理は，特例運用としての手続きと情報セキュリティ対策に漏れがないことの確認を現場組織と特例運用管理の専門組織により厳重に実施するものである.

本稿では，再発防止策として実施する特例運用管理の紹介と，二度と重大な情報セキュリティ事案を起こさないために今後取り組むべき方向性について説明する．まず 2 章で第三者委員会により指摘された三つの原因について，3 章で再発防止策について述べ，4 章で特例運用管理の詳細を説明する．5 章では意識醸成等の施策について触れる.

2. 第三者委員会の指摘

第三者委員会より指摘された本事案の原因は以下 1）～ 3）の三つである.

1）BIPROGY 役職員のコンプライアンス意識の欠如

秘匿性，機密性の高い要配慮個人情報を含む膨大な量の個人情報データを取り扱う業務に従事しながら，それが漏えい等した場合のリスクに思い至らず，十分に対応策を検討せずに，安易な方法で USB メモリーを運搬し，データを削除しないまま飲酒行為に及ぶといった点は，コンプライアンス意識が決定的に欠如していた表れであることは言うまでもなく，さらに，その上位者においても，個人データの安全性を図る観点から定められた社内でのルールを遵守するよう指導監督していない点においてコンプライアンス意識に欠けたものと言わざるを得ない．また，アンケート調査で，USB メモリーを使用する際のルールを認識しながら守らなかったことがある社員が一定数存在し，過去に USB メモリーを紛失する事案が発生していたにもかかわらず，再発防止に向けた適切な措置が実施されたとは言い難く，セキュリティ内部監査も十分に実施されたとも考え難い．よって関係者固有の問題でなく，BIPROGY の情報セキュリティの深刻な問題である.

2）制度の運用におけるリスク管理意識の欠如

BIPROGY では，情報セキュリティの保全及び個人情報の保護を目的として，組織体制を整え，各種規程を整備する等の措置を講じているが，少なくとも A 市を顧客とする 2022 年度業務では，業務責任者や業務担当者に当たる当社従業員及び協力会社の従業員は，定められた各種規範の大半を遵守していなかった.

3）業務執行におけるモニタリング機能の不全

監査等により定期的にモニタリングをおこない，違反状態を適切に捕捉し，改善することは，不祥事の発生防止のために重要であるが，A 市を顧客とする業務について，第三者委員会の調査で多くの問題点が発見されたのに対し，過去の BIPROGY のセキュリティ内部監査では，問題点が指摘されていなかった.

3. 再発防止策

BIPROGY は，本事案発生直後より直接的原因に対する是正策として，全案件の顧客機密情報を含む本番アクセス及び可搬メディア利用状況とその安全管理対策，そして協力会社との全契約に対する委託管理の適正を緊急点検し，そこで検出された問題への恒久対策と第三者委員会の調査結果を踏まえた対策を合わせて，総合的再発防止策を以下のとおりとした.

1）組織的安全管理措置について

ⅰ）機密性が高い顧客情報資産へアクセスするプロジェクトへの安全管理措置

機密性が高い顧客機密情報資産へアクセスするプロジェクトは，プロジェクトを担当する組織内で組織長が週次でその運用に対する安全管理措置を点検することに加えて，新たに設置したセキュリティ専門組織がその安全管理措置の妥当性を外側から客観的に審査・承認し網羅的に管理・モニタリングする仕組み・体制とする．これによって日常的に顧客情報資産にアクセスすることによる慣れや意識の低下に対処し，あらためてそれが特別な行為であることを繰り返し認識し浸透させる.

ⅱ）社内規程及びビジネスプロセスの改定

本事案を受け適用した再発防止策のうち，恒久対応に相当する対策の継続性を担保し，正式なルールとして BIPROGY グループ全体へ展開し徹底するために，可搬メディアの取り扱いルール強化，顧客機密情報と顧客本番環境アクセスのルール強化，サービスビジネスにおいて顧客本番環境にアクセスする際のルール新設等を内容とする社内規程の改定，その他稟議決裁規程，情報サービス・アウトソーシングサービスなどのビジネスプロセス関連規程の改定を実施する.

ⅲ）教育及び指導

情報セキュリティ・リスクの理解と個人情報を含む顧客機密情報の取り扱いルール再徹底のための教育に加えて，セキュリティや法令・契約遵守を常に意識させることを目的に週次で理解度を測るテストを全役職員に実施する.

情報セキュリティ遵守事項に係るプロジェクトチーム内への周知や協力会社向け教育の実施状況確認を実施する.

2）物理的・技術的安全管理措置について

受託業務における可搬メディア利用状況の責任者による確認，受託業務以外で利用している可搬メディアの必要性の定期的な見直しと，継続利用する場合は社内規程どおり管理されていることを管理簿などの証跡ベースで報告することを徹底する.

3）委託先管理について

ⅰ）情報セキュリティ

安全管理措置及び個人情報の取り扱いに責任を持つ役職者による教育及び指導等により，委託先監督に関する法令・BIPROGY 規程の遵守を徹底する．委託先管理，特例運用管理に関する教育を全役職員に対して実施し．部長相当職の従業員に対しては当該教育を個別に実施する．

顧客機密情報（個人情報を含む）の取り扱いを協力会社に委託する場合も，新たに設置したセキュリティ専門組織にて安全管理措置を審査・承認し，その実施状況をモニタリングするとともに，形骸化を防止するため，セキュリティ内部監査において運用状況を監査する．

ⅱ）管理プロセス見直し

委託先管理の責任者を新たに設置，委託先管理プロセスを見直し，BIPROGY と顧客との契約条件に従って BIPROGY から協力会社への委託がなされていることを確認できるエビデンス管理や運用が適切におこなわれていることの週次レベルでのモニタリングを実施，委託先管理プロセスが適切に運用されていることを確認するため，セキュリティ内部監査において運用状況を監査する．

4. 特例運用管理

本事案を受けて，BIPROGY グループの情報セキュリティポリシーに次の記載を追加した．「BIPROGY グループの事業活動において取り扱う重要な情報資産を情報セキュリティによる保護の対象とし，お客様サービスにおける重大なセキュリティインシデントの防止のため①顧客情報資産にアクセスしない，②可搬メディアは使用しない，③情報は限定した場所から持ち出さないことを当社グループの情報セキュリティ対策の三大原則とする．当該原則に準拠しない対応をする場合は，顧客の合意のもとそのリスクと必要性について関連する役職員が正しく認識したうえで厳密な管理のもとで実施する．顧客機密情報を対象とする場合は，特例運用として総合セキュリティ運営会議の承認を得る．」

総合セキュリティ運営会議は，総合的再発防止策で設置するとしたセキュリティ専門組織である．総合セキュリティ運営会議は，三大原則に準拠しない顧客機密情報を対象とする対応の管理・モニタリングをおこなう．そしてこの制度を特例運用管理とした．

三大原則に準拠しない対応は，図 1 に示すように，担当組織の組織長が確認と承認をおこな

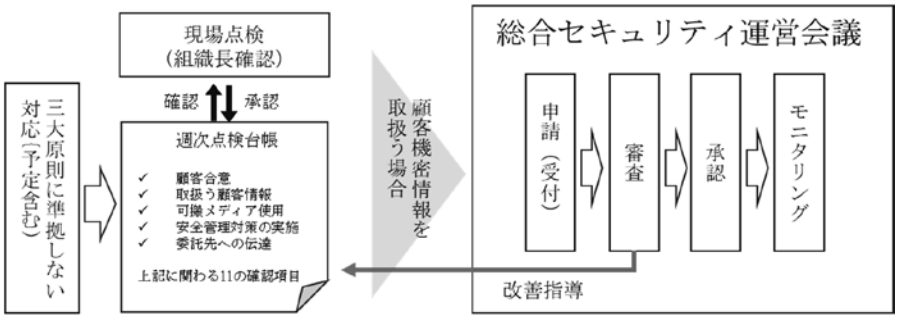

図 1　三大原則に準拠しない対応の管理

う現場点検と顧客機密情報を取り扱う場合の総合セキュリティ運営会議がおこなう審査，承認，モニタリングの二段階で管理する．本章では，特例運用管理における現場点検と総合セキュリティ運営会議について述べ，従来から準拠している 3 ラインモデルについても触れる．

4.1　現場点検

三大原則に準拠しない対応の発生が見込まれ，回避できない場合には，プロジェクトの責任者は組織責任者に報告する．組織責任者は，再度，回避可否の確認をおこない，対応の実施止む無しと判断すると，安全管理対策が取られていることを確認の上，更に上位の決裁を受けることで実施が可能となる．これを現場点検と位置づけている．

現場点検で確認する項目と内容例を図 2 に示す．2 段に分かれているが合わせて一つの報告である．

	お客様名	プロジェクト名	システム名	実施予定内容 （アクセスする顧客本番環境や個人情報の記載、作業内容を含む）	作業実施期間	顧客合意	個人情報の取り扱い	顧客機密情報の使用環境	可搬メディア使用
例	A社	販売管理システム運用保守	販売管理システム	運用保守業務として、顧客からの問い合わせによるデータ調査作業及び作業依頼対応	2023/09/04～ 2023/09/08	文書で合意有り	個人情報の取り扱い有り（ただし、使用時はマスクされた状態）	個人情報をマスクしたデータを保守環境で使用	データを保守環境に導入する際に使用

可搬メディアの管理	委託先体制 （再委託含む）	委託先へのセキュリティ教育実施	実施する安全管理対策	証跡	二段組織管理者確認日	二段組織管理者	一段組織長承認日	一段組織長名
A社所有のUSBメモリであり、A社管理基準に則り使用	1次：B社（3名） 2次：C社（4名）	情報セキュリティ管理計画書を委託先メンバ全員に説明済	・顧客管理端末にて作業を実施 ・機器の持ち込み、情報を含めた外部への持出は禁止 ・他、取り扱う顧客機密情報、アクセス制御、等の安全管理に関わる内容は、情報セキュリティ管理計画書で記載し、顧客の了解を得て、プロジェクトメンバ全員に周知徹底している	・作業報告書 日ごとに作業の目的、作業者、手順、結果を記載し、週次で作業報告書を作成し社内確認ののち、顧客へ提出	2023/8/25	部長	2023/8/31	本部長

図 2　現場点検台帳

点検はチェックリストでなく証跡の確認までおこなう．確認は，現場責任者である部長とその上司である本部長の二段階でおこなうよう定めている．

4.2　総合セキュリティ運営会議

BIPROGY グループの情報セキュリティ推進体制は，CISO（Chief Information Security Officer）が委員長を務める総合セキュリティ委員会とその下部組織，及び各組織の情報セキュリティ責任者，担当者で構成されている（図 3）．総合セキュリティ委員会は，BIPROGY グループのサイバーセキュリティ戦略の策定と個人情報保護を推進する．また，リスク管理委員会と連携し，重大事案の原因究明と再発防止策のグループ全体への徹底を図っている．

総合セキュリティ運営会議は，総合セキュリティ委員会の直下の組織で，議長は CISO である．総合セキュリティ運営会議への特例運用申請は，現場組織のトップである本部長がおこなう．

申請では，総合セキュリティ運営会議が指定する様式に必要事項の記載と記載内容が証明できる証跡の提出が必須である．記入項目は，「プロジェクト基本属性」，「本番環境アクセス・顧客機密情報属性」，「安全管理措置内容」に大分され，記入項目の合計数は 64 項目ある．特に重要な申請内容について表 1 に紹介する．

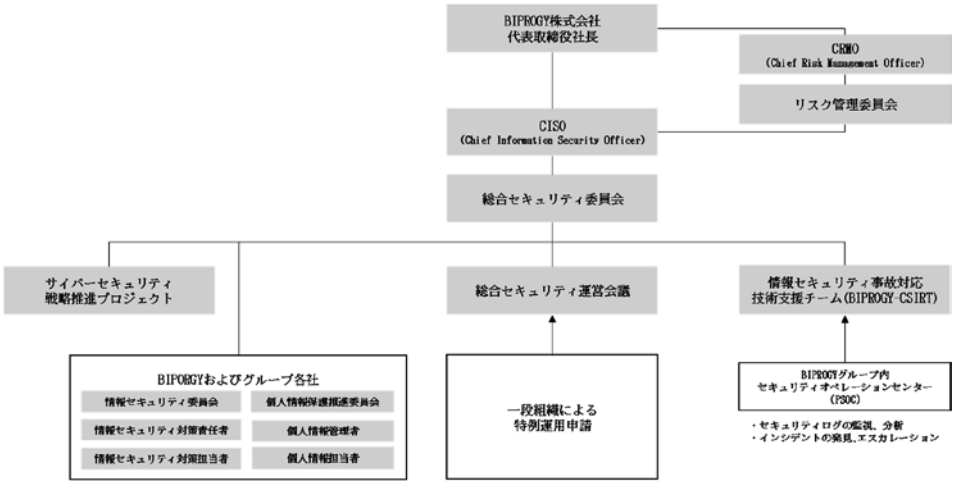

図 3　BIPROGY グループ情報セキュリティ推進体制

表 1　申請内容一覧

申請大項目	申請内容
プロジェクト基本属性	情報セキュリティ対策の三大原則に準拠できない理由
	特例運用実施によるセキュリティリスクと対策
	特例運用実施体制メンバ全員（委託先を含む）へのセキュリティ教育実施
本番環境アクセス・顧客機密情報属性	顧客機密情報の格納場所に対するセキュリティ要件
	顧客機密情報へのアクセス場所とアクセス方法に対するセキュリティ要件
	顧客機密情報へアクセスする端末に対するセキュリティ要件
	本番環境アクセスおよび顧客機密情報取り扱いについての顧客合意
安全管理措置内容	顧客機密情報の格納場所に対するセキュリティ対策
	顧客機密情報へのアクセス場所とアクセス方法におけるセキュリティ対策
	顧客機密情報へアクセスする端末におけるセキュリティ対策
	個人情報を取り扱う場合の個人情報管理規程に則った管理計画
	可搬メディアを使用する場合の可搬メディア管理規程に則った管理計画
	特例運用の作業計画，作業手順
	顧客機密情報の受渡，保管，利用，廃棄の運用手順
	顧客機密情報取り扱い体制と安全管理措置についての顧客合意

申請内容は，顧客機密情報を取り扱う上において，情報セキュリティ関連規程で定められているものであるが，第三者となる総合セキュリティ運営会議への報告のため，プロジェクト内で周知済のことも改めて詳細に記入しなければならず，証跡の提出も必須であり，本事案の発生前にはなかった手続きであることから現場の負荷は少なくない．突発的な作業や短い期間の作業では申請手続きが間に合わない場合もあり，問い合わせが多数発生した．そのような中でも特例運用を厳格に管理することで，コンプライアンスとリスク管理を意識に根付かせていく

狙いがある．表2に示す審査承認基準を満たした申請が承認となる．

承認された特例運用は，モニタリングに移行する．モニタリングでは，申請部門から特例運用の発生状況，安全管理対策実施状況，問題が発生した場合の原因と対策の報告を受け，総合セキュリティ運営会議に報告をする．モニタリング対象となった複数の特例運用の実行においては，2023年7月末時点ですべて承認された安全管理対策どおりであったことをモニタリングしている．

総合セキュリティ運営会議への申請は，顧客機密情報を取り扱う場合としているが，今後，三大原則に準拠しない対応全てと，開発資材など，漏洩の影響が大きいと考えられる情報及びそれを取り扱う行為の全てを対象とする方針である．

表2　審査承認基準一覧

審査項目	承認基準
顧客機密情報の取り扱い	顧客機密情報を取り扱うことについて顧客の合意を得ていること
	取り扱う顧客機密情報の「種類」と「件数」が明確であること
	個人情報を含む場合，個人情報管理ができていること
	マイナンバーを含む場合，準拠すべきガイドラインに従っていること
本番環境アクセス	本番環境アクセスについて顧客の合意を得ていること
	本番環境アクセスにおける安全管理対策が取られていること
可搬メディア	可搬メディア使用について顧客の合意を得ていること
	可搬メディア管理規約に準拠していること
機密情報の借用/持ち出し	機密情報の借用/持ち出しについて顧客の合意を得ていること
	機密情報の借用/持ち出し規約に準拠できていること
委託先管理	委託先体制が明確であること
	委託先管理に情報セキュリティ管理計画を示していること
	委託先メンバへのセキュリティ教育を実施できていること
情報セキュリティ対策の文書化	情報セキュリティ対策が文書化され，顧客の合意を得ていること

4.3　3ラインモデル準拠

BIPROGYグループにおいて，重要な業務は内部監査人協会（IIA）の3ラインモデルに準拠することで確実に実施してきた．特例運用管理は，重大事案の反省と第三者委員会の調査結果を受けた再発防止策の要であることから，従来の3ラインモデルを提供する重要な業務と同等に3ラインモデルを適用することとした（図4）．

お客様サービスを担当する第1線が顧客から受託する業務や提供するサービス等における情報セキュリティに関するリスク管理を自律的かつ組織的に実施し，第2線である総合セキュリティ運営会議が客観的に審査・承認・改善指示・モニタリングを実施，さらにそれらの実施状況を第3線の内部監査部門が的確に監査・モニタリングすることで形骸化を防止し継続的に改善することとしている．これによって，3ライン全体で抜け漏れなく組織的に，かつ継続的にリスクを管理し安全管理措置を徹底する．

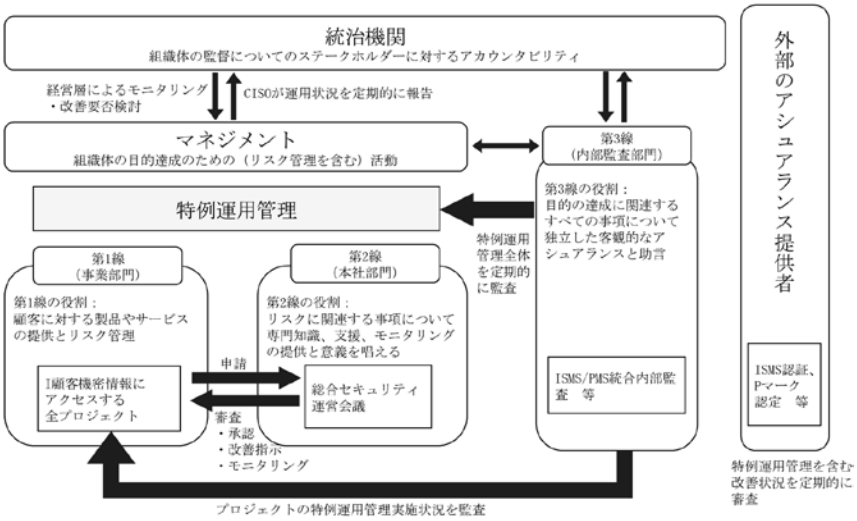

図 4　IIA の 3 ラインモデルにおける特例運用管理の位置づけ

5.　意識醸成等の更なる施策について

2022 年 6 月の重大事案以前にもセキュリティ事案が発生し，原因分析に基づく対策を進める中で，規程とプロセスの改定・追加を実施してきた．また，ルールだけでは機能しないため，プロセスや技術的対応の仕組みも構築したので，ルールと仕組みが膨大になった．

BIPROGY グループでは，情報セキュリティのルール，仕組みを図 5 に示す情報セキュリティポリシー＆プロシージャとして定めた．基本方針とポリシーが 7 文書，プロシージャが 13 文書あり，それ以外にも様々な関連ガイドがある．

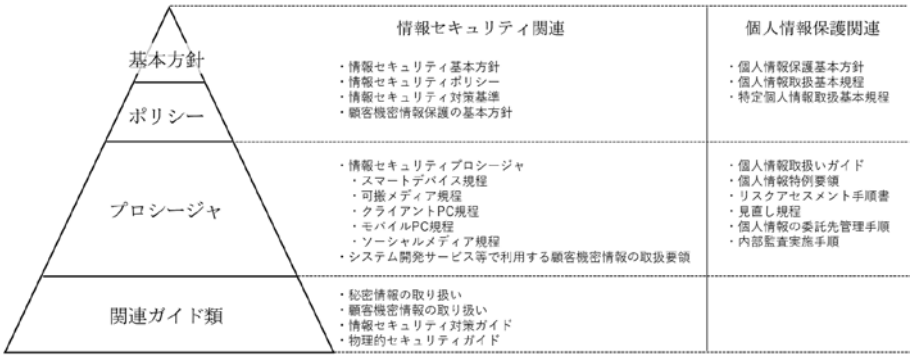

図 5　情報セキュリティポリシー＆プロシージャ文書体系

ルールと仕組みを前提とした再発防止策は，発生した事象の原因に対するものであり，ルールと仕組みに依存しすぎてしまうと，規定がなかったり，環境の変化により合わなくなったりしているセキュリティインシデントへの対応は困難である．ルールと仕組みがなくても個人と組織が，セキュリティインシデントの発生を防ぐ行動を自らとれるようになることが理想であり，そのためにはルールと仕組み以外の施策も用意すべきと考えている．

第三者委員会の指摘に「BIPROGY 役職員のコンプライアンス意識の欠如」と「制度の運用

におけるリスク管理意識の欠如」があった．足りなかった部分を意識で補うことが重要と考え，意識の醸成につながる施策を実施している．本章で説明する．

5.1　意識醸成等の施策

BIPROGY グループでは，事案の風化，意識の希薄化，再発防止策の形骸化を防止し，二度と同様の事案を発生させないことをグループ役職員全員の意識と自覚に刻み込むために，「信頼される BIPROGY グループに必要な意識の浸透プログラム」を定期的に実施している．セキュリティ，個人情報保護などの領域から毎週テーマを設定し，顧客の重要情報を取り扱う場面で，情報セキュリティ対策を軽視したり，対策の実行を怠ったりすると取り返しのつかないセキュリティ事案につながることへの理解を質問形式で深めていく内容である．また，毎年 6 月の重大事案発生日を含む週を情報セキュリティ週間とすることを総合セキュリティ委員会で決定した．2023 年度の情報セキュリティ週間（6 月 19 日の週）には，CISO から BIPROGY グループ役職員へのメッセージを展開するとともに，各種の情報セキュリティ並びに個人情報保護関連の研修やセッション等を実施した．

その他，情報セキュリティ事案の影響を認識できるビデオ教材の作成や情報漏洩事案を対象とした現場対応訓練など，意識醸成につながる新たな施策を実施する予定である．

5.2　意識の醸成によるルール・仕組みとの関係

意識醸成等の施策は，事案の風化，意識の希薄化を防ぐとともに，ルールと仕組みの意図の理解に向かわせていくもので，理解が進み意識と自覚に刻むことができたルールと仕組みは見直していく．図 6 に示すように，ルールと仕組みをシンプルにし，セキュリティインシデントに対しては意識醸成で培われる類推力と想像力により，シンプルになる前のルールと仕組みがカバーしてきたところはもちろんのこと，新たに発生するセキュリティインシデントへも広く対応できるようになることを目指す．

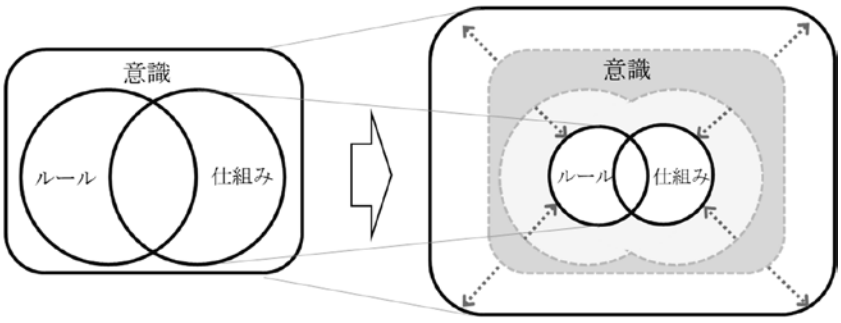

図 6　意識の醸成によるルール・仕組みとの関係

BIPROGY は毎年 100 名を超える新人を採用している．新人研修で最初におこなう講義は，「情報セキュリティ・個人情報保護」と「コンプライアンス基礎」である．これから BIPROGY グループを担う新しい世代が，ルールと仕組みのみに頼らず類推力と想像力で顧客の重要な情報を守っていける人材に育っていくことで，既存の役職員の意識醸成を後押していくことを期待している．

6. お わ り に

特例運用管理は，顧客の重要な情報を扱う企業として当然の対応について確認をおこなうものである．しかし，「コンプライアンス意識の欠如」や「モニタリング機能の不全」の指摘のとおり，当然の対応ができていなかったことから，まずは取り組みの第一歩として，特例運用管理を通じ，当然の対応ができていることの確認を第一とすることで，BIPROGY グループの文化，風土として浸透させていきたい．また，現場任せにせず，第 2 線・第 3 線で監視すること，定期的に全役職員に教育の機会を与えることで，取り組みが形骸化しないように務めていく．

BIPROGY グループは，お客様と連携して社会課題を解決してくことを基本方針としており，これらの対策を徹底することにより，一日も早く信頼を取り戻して．お客様と共に更なる社会課題の解決に貢献していきたい．

参考文献　［1］ IIA の 3 ラインモデル：3 つのディフェンスラインの改定，内部監査人協会（IIA），2020 年 7 月　https://www.iiajapan.com/leg/pdf/data/iia/2020.07_1_Three-Lines-Model-Updated-Japanese.pdf

［2］ 第 25 回事務局参考資料（監査の信頼性の確保/内部統制・リスクマネジメントについて），金融庁，2021 年 3 月 9 日
https://www.fsa.go.jp/singi/follow-up/siryou/20210309/03.pdf

※　上記参考文献に含まれる URL のリンク先は，2023 年 10 月 19 日時点での存在を確認．

執筆者紹介　瀧　谷　龍　二（Ryuji Takiya）
1990 年日本ユニシス(株)入社．通信業界，行政向けシステム開発に従事したのち，2023 年 2 月より特例運用管理の企画・運営を担当．