慶應義塾大学学術情報リポジトリ
Keio Associated Repository of Academic resouces

Title	クライアントの価値観を可視化するサイバーセキュリティコンサルタントのためのサービスデザイン
Sub Title	Service design for cyber security consultants : visualizing client values and mental models
Author	星野, 新(Hoshino, Arata) 佐藤, 千尋(Satō, Chihiro)
Publisher	慶應義塾大学大学院メディアデザイン研究科
Publication year	2022
Jtitle	
JaLC DOI	
Abstract	
Notes	修士学位論文. 2022年度メディアデザイン学 第971号
Genre	Thesis or Dissertation
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO40001001-00002022-0971

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the KeiO Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

修士論文 2022年度

クライアントの価値観を可視化する
サイバーセキュリティコンサルタントのための
サービスデザイン

慶應義塾大学
大学院メディアデザイン研究科

星野　新

本論文は慶應義塾大学大学院メディアデザイン研究科に
修士 (メディアデザイン学) 授与の要件として提出した修士論文である。

星野　新

研究指導コミッティ：

佐藤 千尋 専任講師　(主指導教員)
大川 恵子 教授　(副指導教員)

論文審査委員会：

佐藤 千尋 専任講師　(主査)
大川 恵子 教授　(副査)
岸 博幸 教授　(副査)

修士論文 2022年度

クライアントの価値観を可視化する サイバーセキュリティコンサルタントのための サービスデザイン

カテゴリ：デザイン

論文要旨

本稿は、サイバーセキュリティコンサルティングの現場で、クライアント組織の価値観を可視化し、コンサルタントがクライアントの要件を汲み取りセキュリティ態勢を強化できるよう支援するサービスデザインの研究である。そこで筆者は、クライアントの代表となるような組織の内部の関係性や価値観・考え方の背景を簡単に理解できるように可視化した、図解中心のパンフレット「組織のセキュリティ態勢・図解ハンドブック」を設計した。この図解ハンドブックは、1）読み手が見ることで組織のセキュリティ態勢やインシデント発生時の対応について一覧で把握することができるケーススタディ型の図解、2）読み手が図表を読み解くための取り扱い説明書、読み方ガイドとして機能するREADME、3）図解を設計する過程で用いた質的調査の手法・分析手順を体系的にフローチャート化した手引き書、の三点から構成された。またデザインの価値を検証するため、クライアント組織の代表とコンサルタントの代表それぞれに質的調査を実施して有効性を検証し、その応用可能性について検討を行なった。

キーワード：

コンサルティング, 暗黙知, 価値観, 可視化, サービスデザイン

慶應義塾大学大学院メディアデザイン研究科

星野　新

Abstract of Master's Thesis of Academic Year 2022

Service Design for Cyber Security Consultants: Visualizing Client Values and Mental Models

Category: Design

Summary

This paper, as a study of service design, aims to visualize the values of client organizations in cyber security consulting and support consultants to capture client requirements and enhance their cyber security measures.

To this end, the author designed an illustrative pamphlet, "Organizational Security Measures: A Pictorial Handbook", which visualizes the internal relationships and background of values and ideas of organizations that represent the client's organization in a way that can be easily understood. This Pictorial Handbook is composed of 1) case study-type diagrams that allow the reader to grasp the organization's security framework and response to cyber security incidents at a glance, 2) README that serves as a reading guide to help the reader understand the diagram, and 3) guide that systematically flowcharts the methods of qualitative research and analysis.

In order to validate the design, this paper conducts a qualitative survey on the representative of the client organization and that of the consultant to examine its validity and applicability.

Keywords:

consulting, tacit knowledge, values, visualization, service design

Keio University Graduate School of Media Design

Arata Hoshino

目　　次

第 1 章　序論 **1**

1.1. サイバーセキュリティコンサルティングの現場 1

1.2. 本研究の課題と対象範囲 3

1.3. 本研究の手法と構成 5

第 2 章　関連研究 **8**

2.1. 関連研究調査における二つのテーマ 8

2.2. 暗黙知の組織知化 9

2.2.1　暗黙知の移転に関する総論 9

2.2.2　組織の構成員間の暗黙知の移転 10

2.2.3　現状の知識移転に関わる制約 11

2.2.4　先行研究から見る本稿の立ち位置 12

2.3. コンサルティングプロジェクトの成功条件 13

2.3.1　クライアント側の知識吸収力 13

2.3.2　組織間の信頼醸成 13

第 3 章　デザイン **16**

3.1. デザインコンセプト 16

3.2. エスノグラフィー 18

3.2.1　調査方法 18

3.2.2　セキュリティメトリクスを設計する工程 19

3.2.3　アクターの背景やアクター間の信頼関係 24

3.2.4　クライアント組織の行動を促すフロー 31

3.2.5　アクターのゴールとメンタルモデル 41

3.2.6 対象者の要件の特定：コンサルタントによる中間評価 . . . 47
3.3. デザインプロセス . . . 52
3.3.1 プロトタイプの作成方法 . . . 52
3.3.2 質的調査：私立大学機関 K セキュリティ専門家 . . . 53
3.3.3 質的調査：私立大学機関 K CSIRT 職員 . . . 55
3.3.4 プロトタイプ v1：私立大学機関 K の文化と制度の可視化図 58
3.3.5 質的調査：CSIRT 研究家 . . . 67
3.4. 最終成果物：図解ハンドブック . . . 68
3.4.1 ケーススタディ型の図解 . . . 68
3.4.2 README . . . 74
3.4.3 図解作成の手引き書 . . . 74

第 4 章 価値検証 **77**
4.1. 検証方法 . . . 77
4.2. クライアント側からの評価：プロトタイプ v1 . . . 78
4.2.1 検証結果 . . . 78
4.2.2 価値検証後の考察 . . . 79
4.3. クライアント側からの評価：図解ハンドブック . . . 82
4.4. コンサルタント側からの評価：図解ハンドブック . . . 83
4.4.1 検証結果 . . . 83
4.4.2 価値検証後の考察 . . . 84

第 5 章 結論 **86**
5.1. 本稿のまとめ . . . 86
5.2. 本稿の制約と今後の展望 . . . 88

謝辞 **90**

参考文献 **91**

付録 **96**
A. 組織のセキュリティ態勢とは . . . 96

B. 組織内のインシデント対応チーム CSIRT 97

図　目　次

1.1　セキュリティメトリクス概略（PwC ウェブサイトより筆者作成）　3
1.2　PwC サイバーセキュリティの業務（PwC ウェブサイトより筆者作成）　5
1.3　研究手法：課題特定〜デザイン　7
1.4　研究手法：価値検証　7

3.1　デザイン概要　16
3.2　想定される行動変容のフロー　17
3.3　エスノグラフィー調査の様子　19
3.4　コンサルタントがセキュリティメトリクスを設計する工程の全体像　20
3.5　コンサルタントのワークフロー　22
3.6　コンサルタントの持つベストプラクティス　23
3.7　クライアント組織の姿勢とコンサルタントの判断　24
3.8　二回目のエスノグラフィーの質問リスト　26
3.9　コンサルタントの文化的背景、同僚やクライアントとの信頼関係の全体像　27
3.10　コンサルタントファーム内部の信頼関係　29
3.11　コンサルタントとクライアント間の信頼関係　30
3.12　三回目のエスノグラフィーの質問リスト　33
3.13　コンサルタントがクライアント組織の行動を促すフローの全体像　33
3.14　セキュリティコンサルティングの現場におけるクライアント組織側の動き　36
3.15　コンサルタントがクライアント組織の価値観を探る上での工夫　37

3.16 クライアントの価値観探りの作業についてのコンサルタントの考え 38
3.17 変更反映後のフロー図：アップデート部分 40
3.18 アクターのゴールとメンタルモデルの全体像 41
3.19 U 氏のゴールとメンタルモデル 44
3.20 T 氏のゴールとメンタルモデル 45
3.21 クライアント側のゴールとメンタルモデル 46
3.22 中間評価を受けて更新したコンサルタントの背景 49
3.23 中間評価を受けて更新した U 氏のゴールとメンタルモデル . . . 50
3.24 中間評価を受けて更新した T 氏のゴールとメンタルモデル . . . 51
3.25 私立大学機関 K セキュリティ専門家への質問リスト 54
3.26 私立大学機関 K CSIRT 職員への質問リスト 56
3.27 プロトタイプ v1：私立大学機関 K の文化と制度の可視化図 . . . 57
3.28 クライアントケース：CSIRT を取り巻くランドスケープ 61
3.29 クライアントケース：背景にある組織文化や信頼関係 62
3.30 クライアントケース：組織の抱える課題 63
3.31 クライアントケース：ゴールとメンタルモデル 66
3.32 ケーススタディ型の図解：私立大学機関 K 1/2 70
3.33 ケーススタディ型の図解：私立大学機関 K 2/2 71
3.34 ケーススタディ型の図解：ベネッセ 72
3.35 ケーススタディ型の図解：セブンペイ 73
3.36 README 75
3.37 図解作成の手引き書 76

4.1 CSIRT 研究家への価値検証の結果指摘された価値 80

B.1 CSIRT 設立経緯 （質的調査の内容より筆者作成） 99

表　目　次

4.1　私立大学機関 K のセキュリティ態勢上の欠かせない存在 . . . . .　81

第 1 章
序　　論

1.1. サイバーセキュリティコンサルティングの現場

近年、サイバー攻撃の脅威が世界的な高まりを見せており、2022 年の世界におけるサイバー攻撃回数は前年比 38 %増であった[1]。日本でも 2019 年から 2022 年の三年間に受けたサイバー攻撃の回数は倍増しており、警察庁が検知した不審なアクセス通信も同期間で倍増している[2]。それに伴い、企業や組織の経営に深刻な影響を及ぼすようなセキュリティインシデントの回数も急増しており、日本国内で発生したセキュリティインシデントの回数は 2020 年からの二年間で二倍以上となっている[3]。そのため、企業や組織ではサイバー攻撃の脅威を自分事として捉え、セキュリティ態勢を強化し、攻撃を未然に防ぐための守りを固める必要がある[2]。

しかしながら現状では、ほとんどの国内企業において組織的なセキュリティインシデント対応の態勢が整備されておらず、全体の約四割程度の国内企業しかインシデント対応を担う専門チームを設置していない[4]。このような状況の中でサイバーセキュリティを専門とするコンサルタントらは、クライアント組織に自分たちのセキュリティ態勢を強化する具体的な行動を促すため、日々コンサルティン

---

1 Check Point Research, https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/, 2023 年 1 月 14 日参照

2 日本経済新聞 サイバー攻撃、日本に矛先　3 年で攻撃数倍増, https://www.nikkei.com/article/DGXZQOUC0971U0Z01C22A2000000/, 2023 年 1 月 14 日参照

3 Digital Arts Security Report 2022 年上半期国内セキュリティインシデント集計, https://www.daj.jp/security_reports/220705_1/, 2023 年 1 月 14 日参照

4 国内企業・団体のセキュリティ対策実態調査, https://www.daj.jp/company/release/common/data/2022/090201_reference.pdf, 2023 年 1 月 14 日参照

グ業務を行っている。

本研究において実施したヒアリング調査によると、サイバーセキュリティコンサルタントらがクライアントとしている組織の中には、自組織の態勢を強化するために、もはやどこから着手をすれば良いか分からないと述べている企業も多い。そこでコンサルタントらの業務の一つには、組織がセキュリティ態勢を強化するために、どの指標を重視すべきであり、指標ごとにそれぞれどれくらいの数値目標を目指し、そのためにどう行動を起こしていくべきか、が一目瞭然に分かりやすいような、指標の一覧表・ダッシュボードの設計サービスが含まれる[5]。この一覧表を、業界ではセキュリティメトリクスという（図1.1：セキュリティメトリクスの概略図）。

ただしこのセキュリティメトリクスはあくまで組織がどう行動するべきかの指針のようなものであり、組織ごとの事情に合わせてテーラーメイドして設計する必要がある。したがって設計のための要件を把握するにはコンサルタントが、クライアント組織ごとの理念や文化、サイバーセキュリティ対策に対する危機意識の度合い、部署間のパワーバランス、各部署の設立経緯、各部署が重視する業務指標、組織内の指揮系統、過去に発生したセキュリティインシデントにおいて組織がどう対応してきたかなど様々な事情を加味し、どの部署の誰を説得すれば組織全体が行動してもらえるか、を知る必要がある。

こうしたセキュリティメトリクスの設計業務を含むサイバーセキュリティコンサルティングの業務は通常、コンサルティングファーム側の担当者とクライアント側の担当者によるコンサルティングプロジェクトの形態をとる。コンサルタントはクライアントと直接向き合う現場においてクライアントの抱える課題や要望を汲み上げ、それに応じた解決策となるような戦略や計画を立案、提案、実行支援し、最終的にクライアントにとって価値のある成果を生むことを目指す。

5 PwC メトリクスの設計, https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/security-management-model4.html, 2023 年 1 月 14 日参照

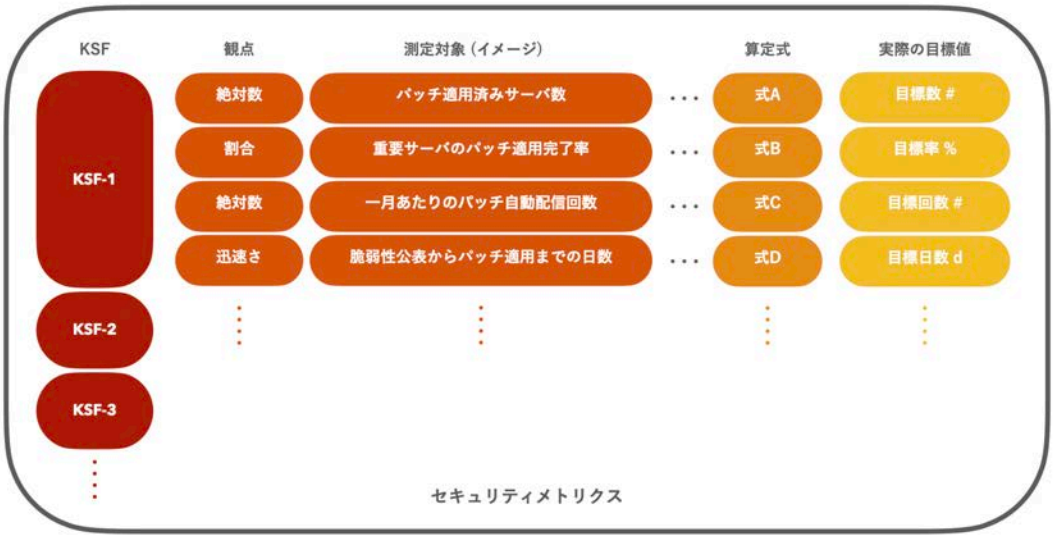

図 1.1 セキュリティメトリクス概略（PwC ウェブサイトより筆者作成）

1.2. 本研究の課題と対象範囲

本研究は、PwC コンサルティング合同会社（以下、PwC）との共同研究であり、サイバーセキュリティの分野を専門とする PwC のコンサルタントに向けたサービスデザインの研究である。PwC において、セキュリティメトリクスのサービスは開始間もない新しいサービスであり、コンサルタントがどのようにしてクライアント組織内部の文化や価値観を把握できるかの方法論が確立していない[6]（図 1.2：PwC サイバーセキュリティの業務概略図）。PwC のコンサルタントらへのヒアリング調査の結果、コンサルタント自身、この価値観を把握するプロセスにかなり難しさを感じているということが分かっている。しかもこれはクライアント側と何回もやり取りを繰り返すことで明らかにするしかないのが現状のため、その非効率さを嫌うクライアントも多く、実践的にも難しい。さらにヒアリング調査からは、どう価値観を汲み取ることができるかのスキルは、個人のコンサルタント

6 PwC サイバーセキュリティ, https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting.html, 2023 年 1 月 14 日参照

が長年の業務経験の中で培ってきた経験や力量に頼ったやり方で行っているのが現状だということが判明している。そのため、どうしても業務上のコツが属人的で暗黙知のようになりやすく、今後コンサルティング側がチームを拡大する際の障壁にもなっていることが明らかになっている。

したがって本研究が解くべき課題は、どのようにしてサイバーセキュリティコンサルティングの現場でクライアント組織の価値観を可視化し、コンサルタントがクライアントの要件を汲み取りセキュリティ態勢を強化できるよう支援できるか、であると定義できる。このリサーチクエスチョンの設定に関しては、エスノグラフィーにおいてPwC側からも支援を希望する声が聞かれ、筆者ら研究チームとの間で合意に至った。詳しくは、第3章にて述べる。

そのため本研究では、PwCのサイバーセキュリティコンサルタントを対象に、いくつかの組織を代表的なケーススタディとして取り上げて、セキュリティ分野を切り口に、組織内部の関係性や価値観・考え方の背景を簡単に理解できるように可視化することを試みる。さらにその過程で用いた質的調査の手法・分析手順自体を、いわば料理のレシピのように体系的にフローチャート化した手引き書も一緒に提供することで、コンサルタントが長期的にクライアント組織の価値観を把握したり、クライアント組織とのより効果的な信頼の構築に役立てられるようにすることを試みる。そうすることで、属人的で暗黙知のようになりがちな価値観探りの手法を体系化・明示化し、コンサルティングチームを拡大する際の新人コンサルタントの教育にも役立てられるようにすることもまた目指す。

また本研究ではこれらのデザインがどのような条件下で有効性を発揮するか、そしてどのような制約があるか、を把握するため価値検証を実施した。本研究はPwCとの長期共同研究のうち初期の範囲を扱うため、本研究における価値検証の範囲は、実際のコンサルティングの現場での導入や使用を含めないProof of Conceptまでを実施対象としている。

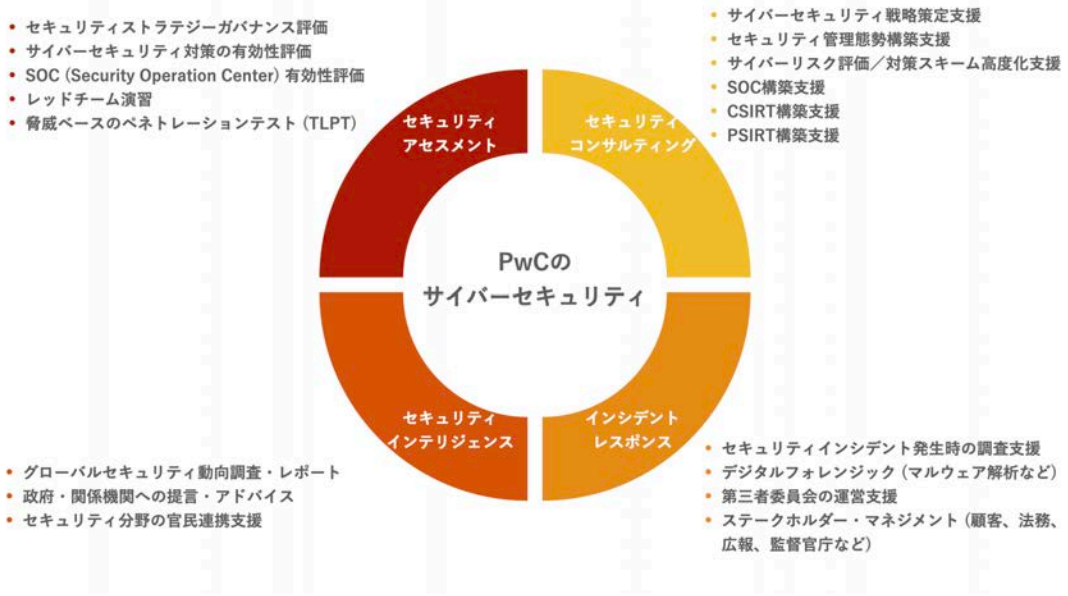

図 1.2 PwC サイバーセキュリティの業務（PwC ウェブサイトより筆者作成）

1.3. 本研究の手法と構成

本研究は、デザインプロセスと価値検証プロセスの二段階から構成される。デザインプロセスは、研究の課題と要件を特定するためのエスノグラフィーと、そこで特定した課題を解決するためのデザインプロトタイプを設計するための質的調査である（図 1.3：デザインプロセスの流れ）。

価値検証プロセスは、設計したプロトタイプに関してコンサルタント側とクライアント側の両方の視点から意見とフィードバックを求め、それに基づいてプロトタイプを修正し、ユースケースを考察するという手法をとっている（図 1.4：価値検証プロセスの流れ）。

デザインプロセスでは計 7 回の質的調査を実施し、そのうち前半の 4 回は PwC のコンサルタントを対象に、コンサルタントの抱える課題や要件を特定することを目的としたエスノグラフィーである。エスノグラフィーは質的インタビュー、いわゆる文脈的質問法 [1] を用いて実施した。これは多くの秘匿事項を扱うコンサルティング業務の特性上、仕事場で対象者と実際に行動を共にする参与観察の実施が難しいという制約があったためである。

この 4 回のエスノグラフィーの内容を元に、1）コンサルタントがセキュリティメトリクスを設計する工程、2）コンサルタントとクライアント間の信頼関係や背景、3）コンサルタントがセキュリティメトリクスを用いてクライアント企業の実際の行動を促すフロー、4）そしてそこから抽出されるコンサルタントのゴールとメンタルモデルの四点を分析し、オンラインプラットフォームの Miro ボード[7]上で図式化した。その後、作成した図表を対象者である PwC のコンサルタントらに見せ、クライアント側が抱える課題や組織内部の価値観や文化、制度を明らかにしてほしいというコンサルタント側の要望を特定するに至った。

したがって後半の 3 回の質的調査は、今度はクライアントの価値観を明らかにするため、クライアントのモデルケースとなるような組織を対象に実施した。調査の対象は、組織ごとに設置された、セキュリティインシデント対応を担うチーム CSIRT で活躍する私立大学機関の職員や、CSIRT に関する研究を行う研究家である。なおこの「CSIRT」というのは、セキュリティインシデント対応版の特殊部隊のようなもので、最近では多くの企業や組織にお抱えの部署として設置されている（CSIRT の詳しい記述に関しては Appendix を参照のこと）。このデザインプロセスについては、第 3 章にて詳述する。

価値検証プロセスでは、計 7 回の質的調査を経て設計した最初のバージョンのプロトタイプから検証を行い、図解ハンドブックが有すると想定した価値がどのような条件下で有効性を発揮するか、またどのような制約があるかを把握するため価値検証を実施した。価値検証は質的インタビューの形式で行い、クライアント側の視点として CSIRT 研究家を対象に 2 回、コンサルタント側の視点として PwC のセキュリティコンサルタントを対象に 1 回実施し、検証の後にプロトタイプの修正とユースケースの考察を加えた。この価値検証プロセスについては、第 4 章にて詳述する。

最後に第 5 章において、想定されるユースケースから見える本研究の制約と展望、拡張可能性について考察し、詳述する。

7 Miro, https://miro.com/, 2023 年 1 月 14 日参照

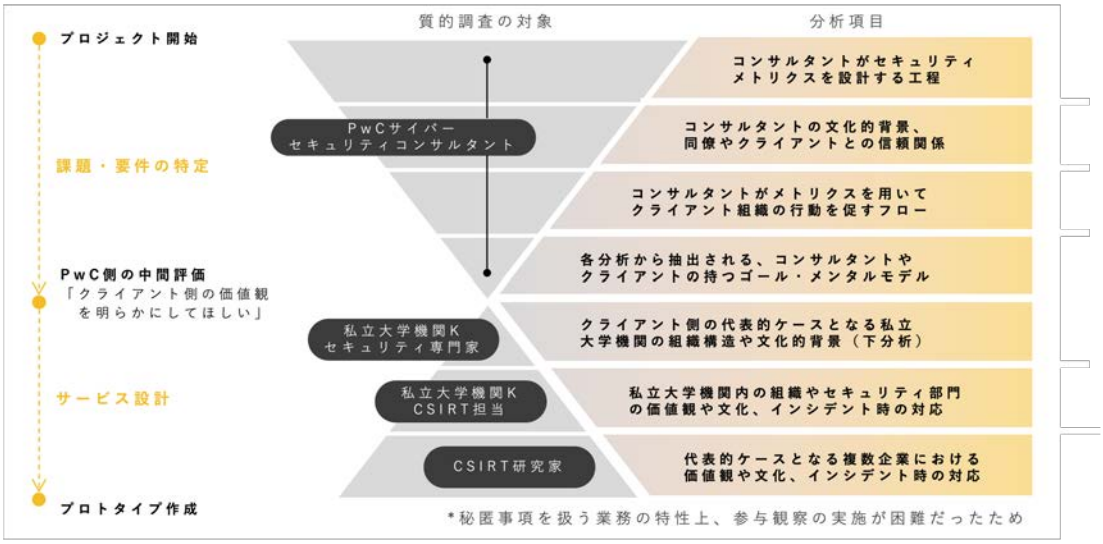

図 1.3 研究手法：課題特定〜デザイン

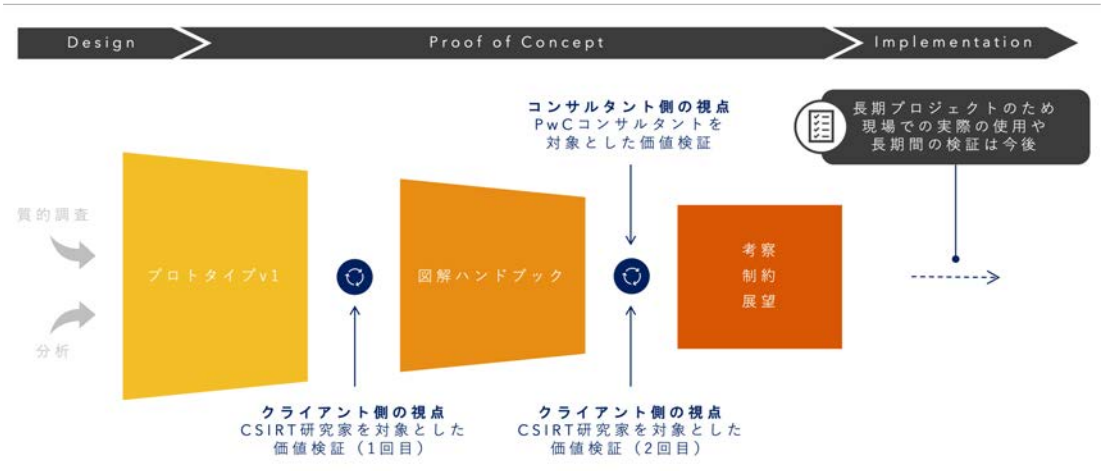

図 1.4 研究手法：価値検証

第 2 章
関 連 研 究

2.1. 関連研究調査における二つのテーマ

本稿では、関連研究を実施する上で重要となる観点として以下の二つのテーマを設定した。

一点目は、関連研究における重要な論点・ポイントは、個人に蓄積されている暗黙知を明示化したり組織知に変換することがそもそも可能なのか、そして前章で述べたメトリクス設計時の価値観を探る作業など、コンサルティングの文脈や外部組織との関係に焦点を当てた研究はあるのか、ということである。前述したようにPwCのコンサルタントらを対象とした質的調査の結果、クライアントが重視する価値観や考え方を探る作業に関して、コンサルティングファームでは現状、個人の経験や力量に頼る場面が多いことが分かっている。そこで本テーマに関する先行研究はまず、このようなコンサルティング業務における個人の知見の共有に関して、一般に現状どのような工夫がなされているかについて示唆をもたらす。

さらに暗黙知の組織知化の中でも、セキュリティメトリクス設計の文脈に関する関連研究調査の有無も確認する。これは、クライアント組織の価値観を可視化する際の手法や、その手法の共有に関する示唆をもたらす。本領域における調査は、このような特定の文脈において現状どのように知見が共有されているかを明らかにした上で、本稿の立場をより一層明確化することに貢献する。

二点目はコンサルティングプロジェクトの成功条件についてである。前述したように、本稿はコンサルタントが長期的にクライアント組織の価値観を把握したり、クライアント組織とのより効果的な信頼の構築に役立てられるようにするこ

とを試みる。そこで本テーマはコンサルタント側あるいはクライアント側におけるどのような条件が、お互いのお互いに対する情報開示を可能にし、コンサルティングプロジェクト全体を成功に導くかについて示唆を与える。本稿では、以上の二点の観点から関連研究調査を展開する。

2.2. 暗黙知の組織知化

2.2.1 暗黙知の移転に関する総論

一般に知識は、前述のような個人の内に培われた暗黙知と明示的な知識である形式知に大別される。この暗黙知と形式知に関する分類的研究は、ポランニーによる 1962 年の論文 *Tacit Knowing: Its Bearing on Some Problems of Philosophy* にまで遡る。ポランニーは、暗黙知は個人の身体と心に深く根ざし、行動、コミットメント、理想、手順を通して表現される知識や経験であると説いた [2]。1990 年代には後続の研究者らがポランニーの定義を理論を発展させ、暗黙知とは文脈依存性が高く直感的・非言語的な形態の知識であるため、その形式化とコミュニケーションには複雑さが生じる [3] [4] と指摘した。一方の形式知は、明示化したり成文化したりすることが可能であるため、少ない手間で知識を伝達することができるとされている [5] [6]。

暗黙知は従来、企業や組織の競争にとって重要な資源であると考えられてきた。グラントは競争優位の観点から、企業における暗黙知は戦略的に重要な資源であり、価値創出の主要な源であると強調した [7]。クインもまた暗黙知はノウハウという形で補完的であるため、戦略的に価値のある資源であり、企業が持つ競争優位の基盤であると主張した [8]。このような状況において企業は暗黙知の形態を保ちながらも、直面する課題の複雑さを乗り越えるために、知識の幅と深さを広げようと試みてきた [9] [10]。

その反面、日本の経営学者である野中と竹内は 1996 年の著書 *The knowledge-creating company: How Japanese companies create the dynamics of innovation*（邦訳『知識創造企業』） [11] の中で、知識マネジメントにおける主な課題はむしろ暗黙知から形式知への変換であると示唆している。野中らは文献において、

1980 年代に攻勢を強めた日本製造業における製品開発プロセスを研究し、企業の製品開発者が暗黙知の保持ではなく、いかに知識を組織知化し企業全体として競争力の源泉となる知識資源を蓄積しているかを明らかにした。そして個人の有する暗黙知を組織全体で形式知化、すなわち組織知化するフレームワーク SECI モデルを発表した。これは、多様な能力や経験を有する人的資本が存在する組織で知識の創造を行うため、個人によって得られた暗黙知とノウハウを、社内の構成員間で１）共同化、２）表出化、３）連結化、４）内面化することで組織知に変換し定着化させるフレームワークを指す。

以上の観点を本研究の文脈に適用すれば、コンサルティングプロジェクトのように知識の一部を外部組織であるクライアントが提供したり、他アクターとの共創を要する場合、個人に蓄積された知識の部分的な組織知化が重要である。またメトリクスの設計のように、クライアントの価値観を質的に測る、という探求され尽くされていない分野に関しては特に、暗黙知の組織知化が待たれている。

2.2.2 組織の構成員間の暗黙知の移転

こうした背景から暗黙知の移転に関する研究は進み、組織の構成員間の暗黙知の移転に関しても研究がなされている。心理学の世界では個人レベルでの知識移転や、ある課題での経験が別の課題での生産性にどのように影響するかの研究が長らくなされてきた [12]。そして個人が他の個人からどのように学ぶかについても研究がなされてきた [13]。また別の研究では、知識移転は組織レベルでも発生し、組織は社内の直接的な経験からのみならず他の組織の経験からも間接的に学ぶことができることが明らかになっている [14]。

このような文脈の中でアルゴテとイングラムは 2000 年の論文において、心理学と組織学の研究を基に知識移転のメカニズムを研究し、社会的単位が他の社会的単位の経験から学んだり影響を受けたりするプロセスについて分析した [15]。ここでの社会的単位とはチームや製造施設内のシフト、部門などの組織内の他の単位を意味し、他の研究によっても同様の定義がなされてきた [16] [17] [18] [19] 。これは本稿で言えば、PwC のコンサルティングチームが同様の問題に直面している組織内の他のチームから解決策を学ぶことに該当する。

2.2.3 現状の知識移転に関わる制約

野中の SECI モデルのフレームワークは後に様々な研究者によって検証がなされ、知識の移転には制約が多いこと、特定の条件下でのみ達成されることが分かっている。

ある製造工場におけるシフトの導入と生産性に関する研究では、第一のシフト集団と同様のタスクを行っていた第二のシフト集団が、第一シフトが何ヶ月もかけて達成した生産性のレベルに、数週間で到達したことが明らかにされている [20]。また製薬業界における研究の結果、知識は他社からの移転に比べて、同じ企業内の関連する研究プログラム間において顕著に移転することが示された [21]。さらに知識移転は組織の生産性に大きな正の影響を与えること、また自動的に発生するわけではないことが明らかになっている [22]。実情として、同一企業内での知識移転の試みの 3 分の 1 が失敗し打ち切られたことを明らかにした研究や、知識が組織単位を超えて移転する程度に大きなばらつきがあることを明らかにした研究がある [23] [24] [25]。

そこで知識移転を達成するためのさらなる研究がなされ、知識は組織の三つの基本要素であるメンバー、タスク、ツール、およびそれらを横断して形成されるネットワークに埋め込まれているとするフレームワークが開発された [26] [27]。このフレームワークを用いた実践的研究の結果、知識が埋め込まれている組織の構成要素（メンバー、タスク、ツール）あるいはネットワークを介して、知識は社会的単位から他の社会的単位に転送できることが分かった。例として個人の人材の移動を通じて、とある社会的単位で獲得した知識を別の社会的単位に移すことが挙げられる。

さらに組織の生産性は、ネットワーク内部のメンバー、タスク、ツール間の質が一致し、他のネットワークとの質もまた一致することによって向上することが明らかになっている [28]。例として、最も優秀なメンバーにタスクを割り当てることでタスクの質が向上し、このメンバーが最もタスクに精通した他のメンバーに助言を求める場合、質の一致も同時に発生し生産性が向上する。他の研究者も、効果的なパフォーマンスを実現するために、組織の構成要素の一致が重要であることを強調している [29]。

同様のことは本稿の対象領域と近しい、シンガポールにおける 146 の IT アウトソーシング・パートナーシップについての調査研究からも、明らかになっている。本研究では知識移転の促進には、顧客企業やベンダーとの関係、移転された知識の特性が重要な役割を果たすことが示されている [30]。

これに逆もまた然りで、知識は組織の中のどこに埋め込まれているかに大きく依存し、知識が蓄積されている文脈から別の文脈に移されるとき、組織の構成要素が一致していない場合、適合させることは難しい [15]。アルゴテとイングラムはこの点に関し、人的なネットワークをある文脈から別の文脈に移動することは、メンバーやタスク、ツールを移動するよりも困難であると指摘している [28]。

このような観点から、知識の移転にはいまだに制約があり、その達成にはある特定の条件が満たされる必要があることが過去の研究から明らかになっている。

2.2.4 先行研究から見る本稿の立ち位置

以上の先行研究が行われたフィールドを考慮すると、これまでのところ、コンサルティングの文脈での暗黙知の共有や、外部のクライアントとのコミュニケーションに関する知見の移転、に焦点を当てた研究はほとんどないのが現状である。このことは前述したように、PwC のセキュリティコンサルタントらによっても同様のことが指摘されている。

さらに、現状提案されている知識の移転に関する手法やモデルは、今回の文脈においては適用可能性に疑問がある。例として野中のモデルは、外部への暗黙知の移転の文脈では、外部化と社会化（暗黙知から暗黙知）が重要であり、社会化による暗黙知の共有は、通常「場」の相互作用を基にした共有体験を通じて達成されると指摘している [4]。

しかしながら現状、本稿が対象とするセキュリティコンサルティングの現場では、野中の提唱する「場」の相互作用を基にした共有体験はあまり期待できそうにない。これはコンサルタントらが指摘するように、クライアント側が自身の価値観を語りたがらないという傾向やクライアント自身が各々あまりにも違う価値観を持っており類型化やモデル化が難しいことから、その経験の共有がなされにくいためである。

そこで本研究では、野中の SECI モデルやその他の知識移転モデルによって個人のコンサルタントが持っている既存の暗黙知をそのまま共有するアプローチではなく、より直接的にサービスデザインの質的調査手法によって、クライアントの価値観や判断の背景をわかりやすく可視化・明示化するという手法を取る。そして他のコンサルタントが、その可視化・明示化された内容を見ることで、知識の移転がスムーズに行われるよう支援する。

2.3. コンサルティングプロジェクトの成功条件

2.3.1 クライアント側の知識吸収力

過去の研究によって指摘されているコンサルティングプロジェクトの成功の鍵を握る要素の一つは、クライアント組織側の知識吸収力である。コンサルティングプロジェクトにおける失敗例の多くは、知識を仕事のルーチンや経営慣行に組み込む上での吸収力、すなわちクライアント組織側が外部から提供された知識の重要性を認識し、価値を認め、同化し、適用する能力が大きく影響するとする指摘がある [31]。

このことは、知識を効果的に移転するために、クライアント組織がプロジェクトの開始前に一定の知識吸収力や導入知識を持ち合わせていることが重要であることを示唆している。第 4 章にて詳しく述べるが、本稿では価値検証においてクライアント側からの情報開示の可能性・重要性が指摘されており、それゆえこの文献の存在は価値検証の段階において指摘された価値の正当性を裏付けている。

2.3.2 組織間の信頼醸成

過去の研究によって指摘されている成功要因のもう一つは、クライアント・コンサルタント間の感情・能力両面の信頼関係である。PwC へのヒアリング調査によれば、一般にセキュリティメトリクスの設計は通常数ヶ月程度にわたるため、クライアント側とコンサルタントの間の良好な作業関係の構築が重要な役割を果たすと考えられる。

信頼関係と知識の伝達に関する先行研究によると、コミュニケーションのしやすさと親密さを特徴とする関係は、組織を超えた知識の移転を促進することが示されており、能力と善意の信頼に基づく関係は、 知識移転に正の影響を与えることが判明している [32]。

またポーランドを拠点とする企業を対象に行われた研究では、信頼関係が知識を移転する活動を促進する自発的な交換を促し、より大きな知識交換をもたらすという多くの証拠を提供している。本論文によると信頼が存在するとき、クライアント企業はプロジェクトの成功のために外部コンサルタントに知識の移転を依頼し、相手を信頼することで、プロジェクト目標達成のために協力し合い、互いに知識をより喜んで伝達し合い、信頼の発展を通じて知識の波及効果が生じることが示唆されている [33]。

別の先行研究は、この二つ目の相互信頼関係の内容についてさらに深い示唆を提供している。これは、相互信頼が組織間の知的移転の効果にどう影響を与え、それがプロジェクトの成果にどう影響を与えているかについて検証した論文である。論文の対象領域は企業システムだが、暗黙的で複雑な知識領域ゆえにクライアント側が外部コンサルタントを活用することが多い点、クライアントとコンサルタントの知識が非対称的である点、知識の共有の観点からクライアント側がより重要な役割を担うという点でメトリクス設計の領域と近しいと言える。本論文によると、コンサルタント・顧客企業間の相互の「善意」に対する信頼と「能力」に対する信頼の両方が、知識移転とプロジェクトの成果に正の影響を与え、中でも善意に対する信頼は能力に対する信頼に比べてより大きな影響を与えたことが示唆された。また本論文は両社から最も能力や専門知識の高いメンバーを配置することに加え、企業間の個人的な関係を促進するためのチームビルディングを行なったり、両者の結びつきを管理することが必要であると指摘している [34]。このことは前述の、クライアント企業側の知識吸収力や知識基盤が重要であるとする研究結果と合致する。

さらに、オーストラリアで行われたクライアントとコンサルタントの信頼関係に関する研究は、より信頼関係の成功要因に関してさらに詳細に記述している。15 人のクライアントと 16 人のコンサルタントを対象とした本研究では、１）能

力と誠実さを示すこと、２）善意を示すこと、３）感情的なつながりを確立すること、の三点の社会的実践を伴うプロセスによって信頼が確立されることが示唆されている [35]。

セキュリティ管理の現場でも同様の内容が報告されている。クライアント企業がベンダーにIT アウトソーシングを依頼する際の両者の情報セキュリティ懸念の不一致に関する研究では、アウトソーシング時の情報セキュリティを確保するための三つの主な構成要素を発見した。この研究では、１）情報セキュリティを確保するためのベンダーの能力、２）ベンダーの顧客要件および外部規制への準拠、３）情報が悪用されず、適切な管理が行われているという信頼感が最も重要であると指摘している [36]。

以上より、コンサルティングの現場において知識の効果的な伝達とプロジェクトの成果を左右するのは、能力と相互の善意への信頼であることが明らかになった。このことはサービスデザイン手法における対象者と観察対象者との信頼や安心できる関係の構築、すなわちラポールの形成 [37] が互いの情報を開示する上で有用であることを裏付けている。

本研究ではこのような文脈を踏まえ、セキュリティコンサルティングの現場において、サービスデザインの質的調査手法による価値観の把握を取り入れることを試みる。そして、コンサルタントがクライアント組織の価値観を把握するための手法を確立し、クライアント組織とのより効果的な信頼の構築に役立てられるようにすることを試みる。

第 3 章
デ ザ イ ン

3.1. デザインコンセプト

セキュリティコンサルティングの現場での課題に対するアプローチとして、本研究ではセキュリティ分野を切り口に、組織内部の関係性や価値観・考え方の背景を簡単に理解できるように可視化した、図解中心のパンフレット「組織のセキュリティ態勢・図解ハンドブック」を設計した（図 3.1）。このハンドブックは１）ケーススタディ型の図解、２）図解の読み方ガイドとなる README、３）図解作成の手引き書、の三点から構成される。

図 3.1 デザイン概要

一点目のケーススタディ型の図解は、読み手が見ることでインシデント発生時に組織の部署がどのように対応したのか、何が失策だったのか、得られた教訓を基にどのような事後対策を打ったのかなどを一覧で把握することができる。二点

目の README は、読み手が図表を読み解くための取り扱い説明書、読み方ガイドとして機能する。三点目は、図解を設計する過程で用いた質的調査の手法・分析手順自体を、いわば料理のレシピのように体系的にフローチャート化した手引き書である。読み手がこれを読み実際に質的調査の手法を実施することで、長期的にクライアント組織の価値観を把握することに活用したり、クライアント組織との効果的な信頼を構築することに活用できる。

これらの要素が統合されコンサルタントがクライアント組織の内部の文化や制度、構造を知るためのツールとしての価値を発揮することで、コンサルタントがクライアントの価値観を推し量る仕事上のフローが変わると想定される。

後述のエスノグラフィーの結果明らかになったこととして、従来はコンサルタントは何回もやり取りを重ねてクライアントと調整をする必要があった。しかしながらセキュリティメトリクスを設計するプロジェクトの開始時にこのハンドブックを活用することで、クライアントの価値観のどの領域を探るべきかを他のケースから参考にすることができる。また、手引き書に沿って質的調査手法自体を導入することで、クライアントとのやり取りの工程を短縮させたり、より正確にクライアントの要件を特定することができるようになると想定した（図 3.2）。

本章では、このハンドブックを設計するに至ったプロセスについて述べる。

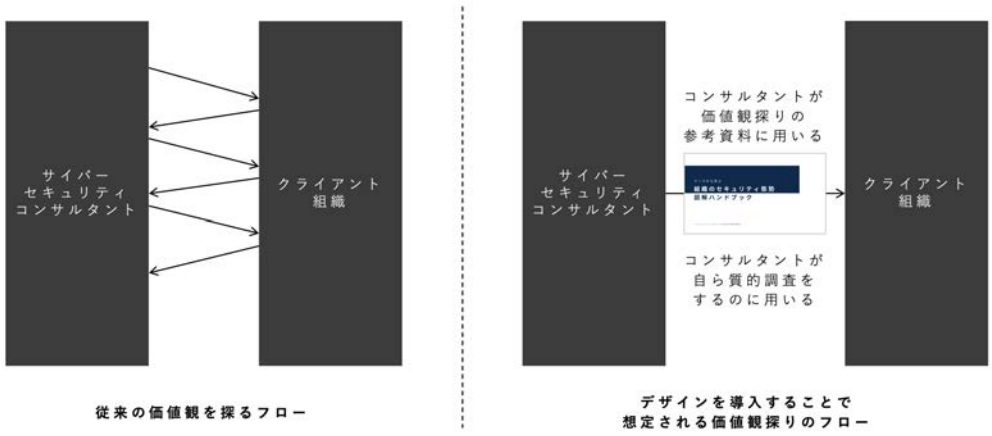

図 3.2 想定される行動変容のフロー

3.2. エスノグラフィー

3.2.1 調査方法

本研究ではまず、価値提供の対象者でもあるPwCのコンサルタントを対象に、コンサルタントの抱える課題や要件を特定することを目的としたエスノグラフィーを計四回実施した。エスノグラフィーでは、サービスデザインにおける文脈的質問法 [1] の手法を用いた。調査の対象は、PwCのサイバーセキュリティ領域を担うU氏とT氏であった。

U氏は30代後半の男性で、中途でPwCのサイバーセキュリティコンサルティング部門に加わり、現在はディレクターの立場からセキュリティメトリクス設計のプロジェクトを含む11のプロジェクトを分野横断的に統率している。大学時代は大電力など発電に関連することを、大学院時代は音声信号処理やノイズリダクションに関連する研究を行い、その後は大手通信会社の企画部門で働くなど、テクノロジーに関わる数多くの経験を積んできた。

T氏は20代後半の男性で、新卒でPwCのテクノロジーコンサルティング部門に入社し、現在はマネージャーとしてU氏と共にセキュリティメトリクス設計のプロジェクトにも携わっている。同氏はセキュリティサービスに関連するプロジェクトへの関与を徐々に減らしつつあり、大学から大学院時代にかけて創薬の研究をしていた背景もあり、むしろ製薬業界やヘルスケア業界に関連するチームで働くことが増えている。

調査では質問事項をあらかじめ箇条書きにし、それを調査前に対象者に事前に共有することでお互いの前提知識の足並みを揃えた。またエスノグラフィー調査の実施中は、事前に用意した質問事項に基本的に沿いながらも、答えの内容に応じて深掘りする部分を柔軟に調整する、半構造化インタビューの形式をとった（図3.3：エスノグラフィー調査の様子）。

なお本節ではエスノグラフィーとして実施したヒアリング調査や質的インタビューの内容を、可能な限り詳しく説明した。これは、本稿におけるエスノグラフィーの手法自体が、アクターの考え方や文化、背景を明示化する方法として価値を持つ可能性があるためである。

図 3.3 エスノグラフィー調査の様子

3.2.2 セキュリティメトリクスを設計する工程

分析手順

2022 年 6 月 28 日、PwC のコンサルティングチームと本研究チームとの打ち合わせ時に、コンサルタントがセキュリティメトリクスを設計する工程についてヒアリング調査を行った。調査ではメトリクス設計の目的や手順、手法に関する PwC 側の資料をあらかじめ共有してもらい、その内容に基づいて業務の具体的な遂行手順、ワークフローについて質問する形式をとった。

質的インタビューの手順は以下の通りである。１）セキュリティメトリクスについての理解を鮮明にするためメトリクスに用いられる指標の例を聞く、２）コンサルタントの指標の実際の立て方や業務の具体的な流れについて明らかにする、３）業務の背景にあるコンサルタントの考え方や判断について焦点を当てる（例：クライアントの反応が鈍かったり腰が重い場合に、コンサルタントが行動を実際に促すために心がけているアプローチについてなど）

調査終了後、内容の文字起こしを基に業務手順を分析し、以下の三つの構成に

分けて分析図を作成した。一つ目はコンサルタントの普段の業務内容であり、コンサルタントの発言記録から業務内容に関するものを抜き出し、Miro ボード上に配置した。その後、業務内容の矢印で繋いでフローチャート化し、それを作業内容ごとにカテゴリー分けした。二つ目は、コンサルタント個人が感覚的に行っている手法や手法上のベストプラクティスである。これも調査中の発言記録から抽出し、フローチャート上の該当箇所に記載した。三つ目は、業務の状況でありがちなクライアント組織の考え方と、それに対するコンサルタントの判断である。これに関しても、この時点までに作成した分析図の上に情報を追記した。

以上の三つの構成を含むことによって、コンサルタントがメトリクスを設計する工程に関する分析図を作成した（図 3.4）。なお図 3.4 はあまりにも精緻なため、これを分割したものを図 3.5、図 3.6、図 3.7 にそれぞれ示した。

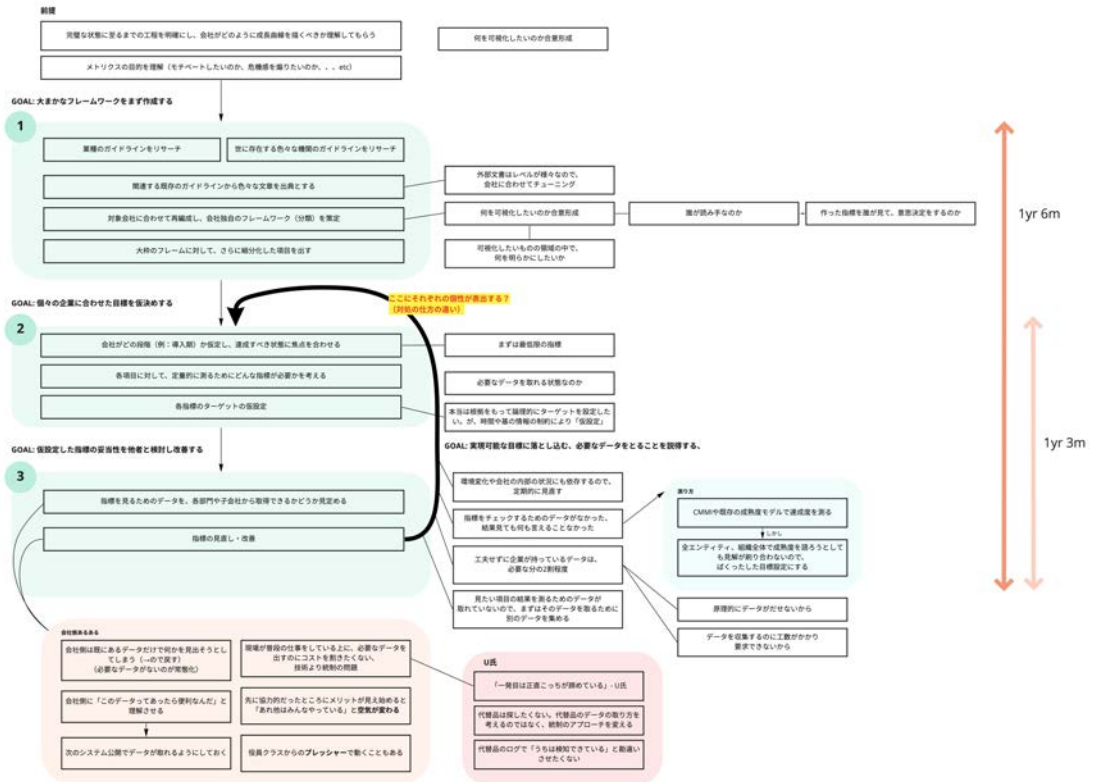

図 3.4 コンサルタントがセキュリティメトリクスを設計する工程の全体像

分析内容

図3.5は、セキュリティメトリクス設計時のコンサルタントのワークフローを示しており、クライアントとの前提知識の共有、大まかなフレームワーク作成、指標ごとの明確な数値目標の仮設定、指標改善のための妥当性評価、の四つの段階に大別される。コンサルタントはまず前提共有時に、クライアントとの期待値の調整を行う。これは組織のあるべきセキュリティ状態を明確化し、どのような成長が必要かを組織側に理解してもらうことを含む。次に、組織が何の指標を重視するべきかに関するフレームワークを策定する。そのために業種ごとの資料や政府機関が発行しているセキュリティガイドラインの調査を行う。その後、対象組織の現状のセキュリティ状態に合わせて指標ごとに数値目標を仮設定し、指標を見るためのデータが取得可能かどうかを調査する。取得可能な場合はクライアント側に行動を働きかけ、不可能な場合は指標の見直しや改善を試みる。

図3.6では、こうした作業においてコンサルタント個人が感覚的に実行しているベストプラクティスを説明した。例としてU氏は、前提共有の段階でクライアント側との合意形成を心がけ、誰がセキュリティメトリクスの読み手なのか、意思決定を行うのかを意識してフレームワークの策定を行なうと述べた。また分析の結果、目標の仮決め時にコンサルタントごとの物事の進め方に違いが表出しており、U氏は実現可能な目標に落とし込むことや必要なデータを取るよう説得することに主眼を置いているとした。多くの場合、組織が既に取得できる状態のデータは二割程度しかないため、まずは周辺のデータを集めるとのことだった。

最後に図3.7に、業務の過程でありがちなクライアント組織の姿勢とコンサルタントの考えを整理した。調査の結果、一部のクライアント組織は既に存在するデータだけで対応しようとしたり、技術的には必要なデータを取得できるにもかかわらず現場側がコストを割きたくないという問題があることが分かっている。それに対しU氏は、経営層からのプレッシャーで現場が動きやすいことや、先んじて協力的だった部署で成果が目に見え始めると空気が変わるとしている。

以上が、現状のセキュリティメトリクス設計時にコンサルタントが実施する工程についてである。本研究では、まずエスノグラフィーを通じて対象の業務遂行プロセスを理解することで、その後の課題や要件の特定に役立てる。

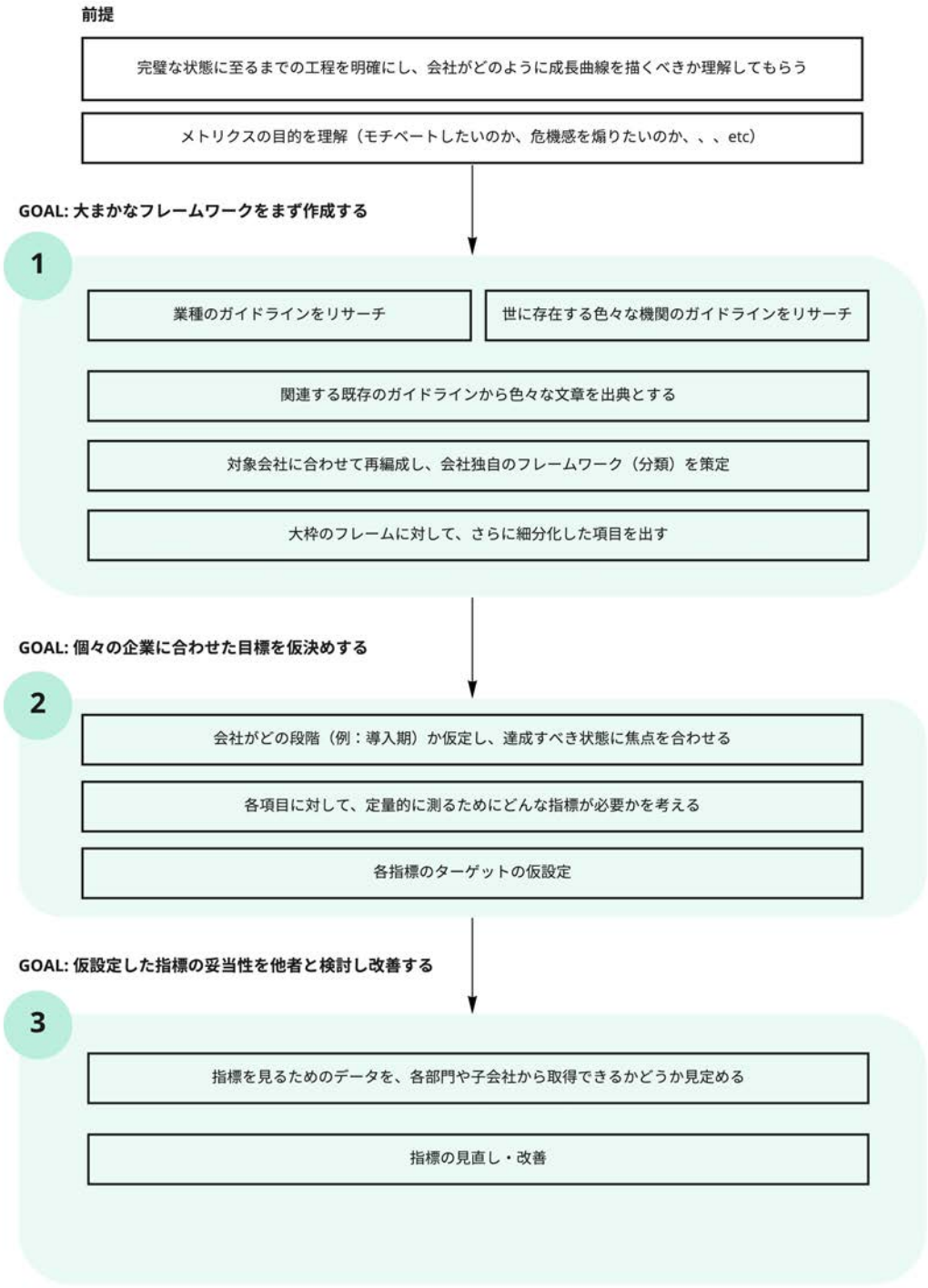

図 3.5 コンサルタントのワークフロー

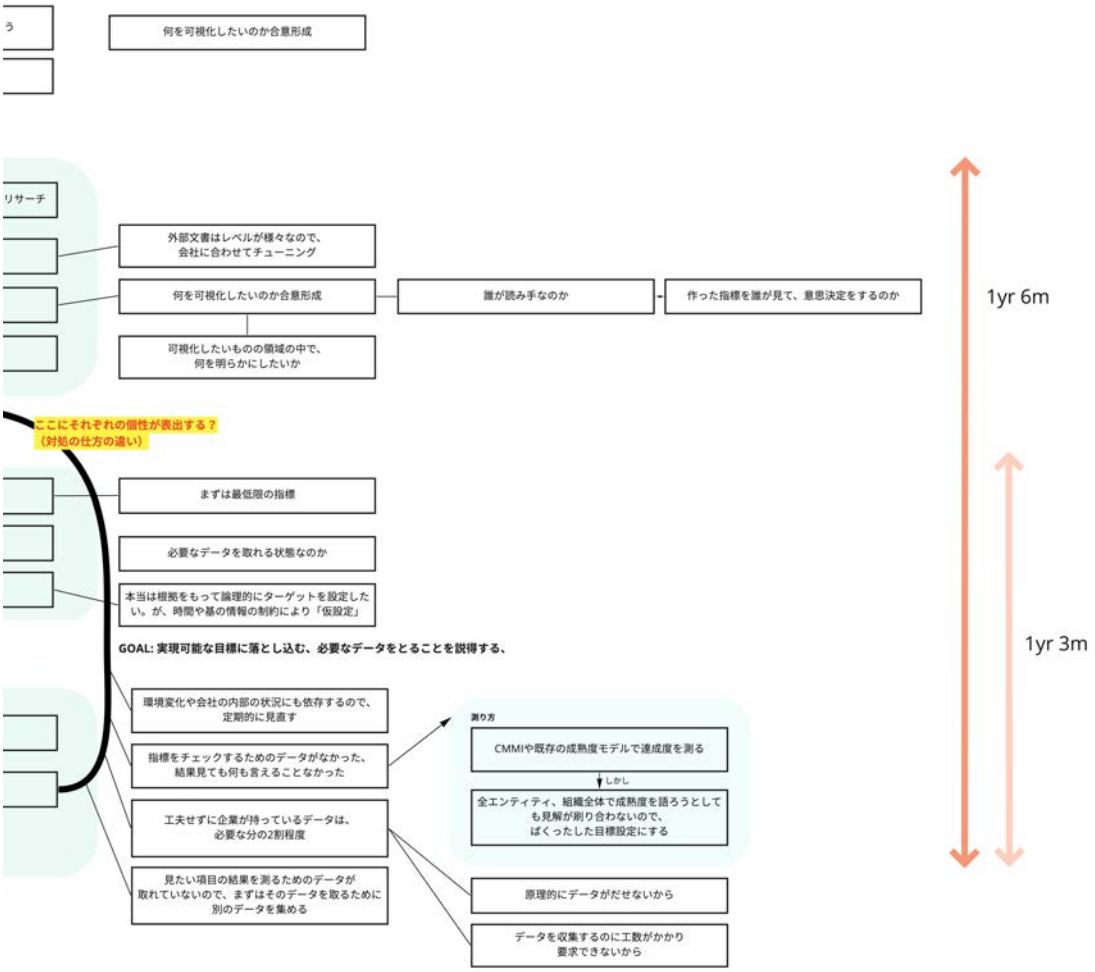

図 3.6 コンサルタントの持つベストプラクティス

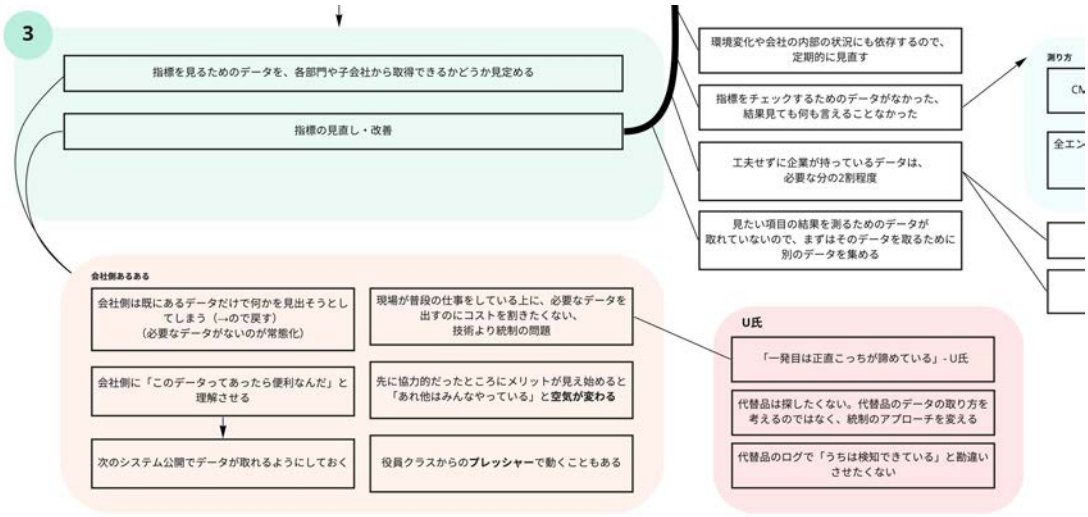

図 3.7 クライアント組織の姿勢とコンサルタントの判断

3.2.3 アクターの背景やアクター間の信頼関係

分析手順

2022 年 8 月 26 日、筆者ら研究チームは PwC の東京オフィスを訪れ、サイバーセキュリティコンサルティングチームに二回目の調査を行った。調査内容は、コンサルタントの方々の出自や経歴、コンサルタント同士やクライアントとの信頼関係についてである。U 氏と T 氏の両名には調査前に事前に用意した質問リスト（図 3.8）の要約を送付し、調査を円滑化することを試みた。

インタビューでは、対象の人間関係や教育環境、家庭環境など、コンサルタントの人生観や仕事観に影響を与えている要因について踏み込む内容となることが予想された。そのため対象者が筆者を含む調査チームに対して安心して多くの情報を話せる状況を作り出すため、対象者とラポールを形成することを考慮して質的インタビューを設計した。質問は、対象のこれまでの背景に関する質問群（前半）と、セキュリティコンサルティングについての仕事観を中心とした質問群（後半）に大別された。インタビュー時は、考え方に影響していると思われる要因を掘り下げるため、質問を柔軟に追加するよう注意した。

インタビューの前半は、対象者が開示した情報に対して、なぜそのような選択

をしたのか、なぜその局面においてそのような判断をしたのかという質問を通じて経歴の裏にある考えを探ることを試みた。またU氏とT氏に交互に質問することで、同様の状況における異なるケースの回答が得られるよう心がけた。インタビューの後半では業務内容に一層踏み込み、業務の特性やコンサルティングチームにおけるマネジメントや信頼関係について明確にした。最後にU氏は、コンサルタントとクライアント間の信頼こそがプロジェクトを成功させる上で重要だと指摘したため、その深掘りに努めた。

調査後、文字起こしした内容を基に、コンサルタントの仕事観とそれに影響を与えている出自、人生経験などの背景、さらには他のコンサルタントやクライアントとの信頼関係に関する考え方とそれに影響を与えている要因などを分析し、分析図を作成した（図3.9）。分析図の作成にあたっては、大きく二点の要素に分けて情報を抽出し整理した。

一点目は、コンサルタントが所属するPwCの組織について抱いている考えや、コンサルティングチーム内の構成員同士の信頼関係についての要素である。分析図の作成時は、Miroボード上にU氏とT氏を中心とするアクターを配置し、コンサルタントの発言記録から組織に対する考えや信頼関係に関わる内容を抽出して配置した。また、アクター間が抱いている考えの方向性を意識して矢印を置き、その上に考え方に関する情報を配置した（図3.10）。

二点目は、コンサルタントとクライアント組織が互いにどのようなことを期待し、どのような思いを持って接し、信頼関係をどのように捉えているかの要素である。これらの情報も調査の中で出てきた発言記録から抽出し、コンサルタントの箱とクライアント組織の箱を結ぶ矢印上に配置した（図3.11）。

以上の二点の要素を含むことによって、アクターの背景やアクター間の信頼関係の分析図を設計した。図3.9はあまりにも精緻なため、図3.10と図3.11に分割した。なおこの分析図に関しては、後述するメンタルモデルとゴールに関する調査で追加情報を取得し、その内容を反映しアップデートしている。

目的
- Culture Model: 目に見えない要因 (人間関係・教育環境・家庭環境など) が行動に影響している、それを描き出す
  メンタルモデルを取るための作業: 血の通ったモデルを作るために、ラポールを形成しておくことが極めて重要

相手を知る／仲良くなるための質問 - 20分
- 軽く経歴の自己紹介をお願いできますか
- 何年ほどやっていらっしゃるのですか
- 最初はどういうきっかけでセキュリティコンサルティングの仕事を始められたのですか
- 元々入社前から「コンサルティング」をやりたくて仕方がないという感じだったのか、それとも徐々に愛着が芽生えたのか、あるいはその他なのか、どんな感じですか？
- コンサルティングの中でもどんなIndustryに興味があったのですか？それとも最初からSecurityには漠然とした興味があったのですか？
- 今はリモートか否か
- 日々朝出社してから夕方帰るまで、どんな生活を送っていますか？ミーティングが多いのか、一日中PCを眺めている感じなのか、満足度
- 普段接する方々はどんな方が多いですか？Demographicや特性などの人物像 --
  (年齢・バックグラウンド・国籍・性格など)
- チームの仲: ランチタイムはご飯一緒に行くのか

セキュリティコンサルティングについて - 30分
- セキュリティコンサルティングの仕事をどう定義しますか -- 仕事の特性をどう捉えているかを当事者の口から聞きたい
- セキュリティコンサルタントと他のコンサルティング、例えば経営コンサルティングの違いは何だと思われますか？単に対象とするIndustryの違いだと思われますか？働き方にも差があるのか？
- よく言われる「コンサルティングファームは他の企業と違って異質」、これは具体的に何を指しますか？また、どこに起因していると思われますか？
- 自分が気になっている通説として「コンサルティングファームでは自分の成長が著しい」、これはどこに起因していると思われますか？
- 「自己成長を重視する姿勢」は人生のどのタイミングで意識し始めましたか？
- コンサルタントとして、あるいはセキュリティコンサルタントとして一番大事にしていること／メンタリティは何ですか (答えの例：限りあるリソースの中で、何を守り何は守れないのかの意思決定 etc.)

ラップアップ
- 「コンサルティング」という仕事自体、過去15年で様変わりしたと思います。社会からの注目度しかり、働き方しかり、注力領域しかり。これから5年、10年と経っていく中で、コンサルティングの仕事の内容はどう変わっていくと思われますか？あるいはそもそも今後、この仕事の必要性に変化があると思われますか？
- この先、今の仕事を続けたいと思われますか?

こちら側目線で知りたいこと
- 何がデザインされたら嬉しいのか --
- 3年後とかにチームが拡大することを見越し、我々が作るものがどう貢献しうるのか
  (指標・フレームワーク・手順・ガイドライン・タイプ分析ツール・Peer Reviewツールのようなもの)

図 3.8 二回目のエスノグラフィーの質問リスト

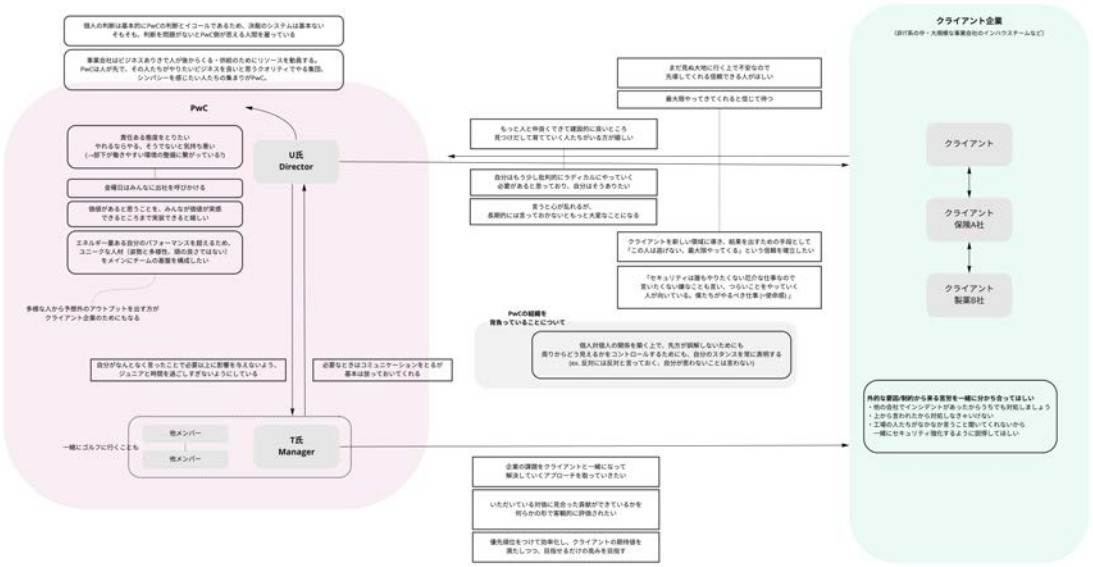

図 3.9 コンサルタントの文化的背景、同僚やクライアントとの信頼関係の全体像

分析内容

まず PwC 内の信頼関係に関して、図 3.10 に示した。前提として U 氏は事業会社とコンサルティングファームの構造的な違いを強調しており、ビジネスありきで後から人を動員する傾向にある事業会社に対して、PwC ではコンサルタントそれぞれが自分の設定した事業を各々の質で提供すると指摘した。また PwC においてコンサルタント個人の判断は、クライアント側から見れば PwC 社全体の判断と同義であると見做されることが多いと指摘した。そのため、決裁のシステムが基本的になく、またそもそも判断に問題がないと PwC 側が思える人材を雇っているとした。

U 氏は PwC のサイバーセキュリティコンサルティングチームでの仕事に対して「価値があると思うことを、みんなが価値を実感できるところまで実装できると嬉しい」と述べており、その価値を与えたいという動機付けの背景として「やれるのならやる、そうでないと気持ち悪い」という考えを挙げている。

そんな PwC のチームにおいて、U 氏は T 氏をはじめとするメンバー（部下）に金曜日には出社を呼びかけるなど職場の環境作りを心掛けており、自分だけでは出せない成果を創出するため、ユニークな人材をメインにチームの基盤を構成す

るようにしている。またU氏は「自分が何気なく言ったことで、必要以上にメンバーに影響を与えないよう時間を共に過ごしすぎないようにしている」とし、一方のチームメンバーもU氏に対して「必要なときはコミュニケーションをとるが基本は放っておいてくれる」と感謝している構図が明らかになった。チームメンバー間は時々一緒にゴルフに行くこともあり、その人間関係の厚さが窺える。

次に、対クライアントの信頼関係に関して、図3.11に示した。クライアント側はセキュリティ態勢の強化に取り組んだ経験すらないことも多く、「まだ見ぬ大地に行く上で不安なので先導してくれる信頼できる人がほしい」「コンサルタントには仲良く建設的に良い部分を育てていってほしい」という姿勢を持っているケースが多い。それに対しU氏はクライアント側との信頼を積極的に確立したいとは考えているものの、その信頼の意味するところは決して意見の迎合ではないとしている。クライアント組織側の長期的なセキュリティ態勢強化のために、批判的に言っておくべきことは、言いたくない場合でもラディカルに言うことが重要だと考えている。また、それこそが「自分たちがやるべき仕事」だと述べている。

さらにU氏は個人対個人の関係を築く上で「クライアント側を誤解させず、かつ長期的に周囲からどう見えるかをコントロールするためにも、自分のスタンスを常に表明する」よう心掛けている（例として反対すべき場面では反対を言っておく、自分が思わないことは言わない、など）。そうすることでPwCの組織を背負っている個人として、後々クライアントに対してなぜ最適解を示せなかったのかを指摘された際、一旦は自分のスタンスを表明したもののそれが実現可能でなかったという防衛が可能になるとしている。この対クライアントの関係に関してT氏は若干異なる姿勢を取っており、「クライアントと一緒になって企業課題を解決していくアプローチを取りたい」「いただいている対価に見合った貢献ができているかを何らかの形で客観的に評価されたい」「優先順位をつけて効率化し、クライアントの期待値を満たしつつ、目指せるだけの高みを目指す」としている。この考え方の違いがどこから生じるのかに関しては、後述のコンサルタントのメンタルモデルとゴールに関する分析においてより掘り下げて分析を行う。

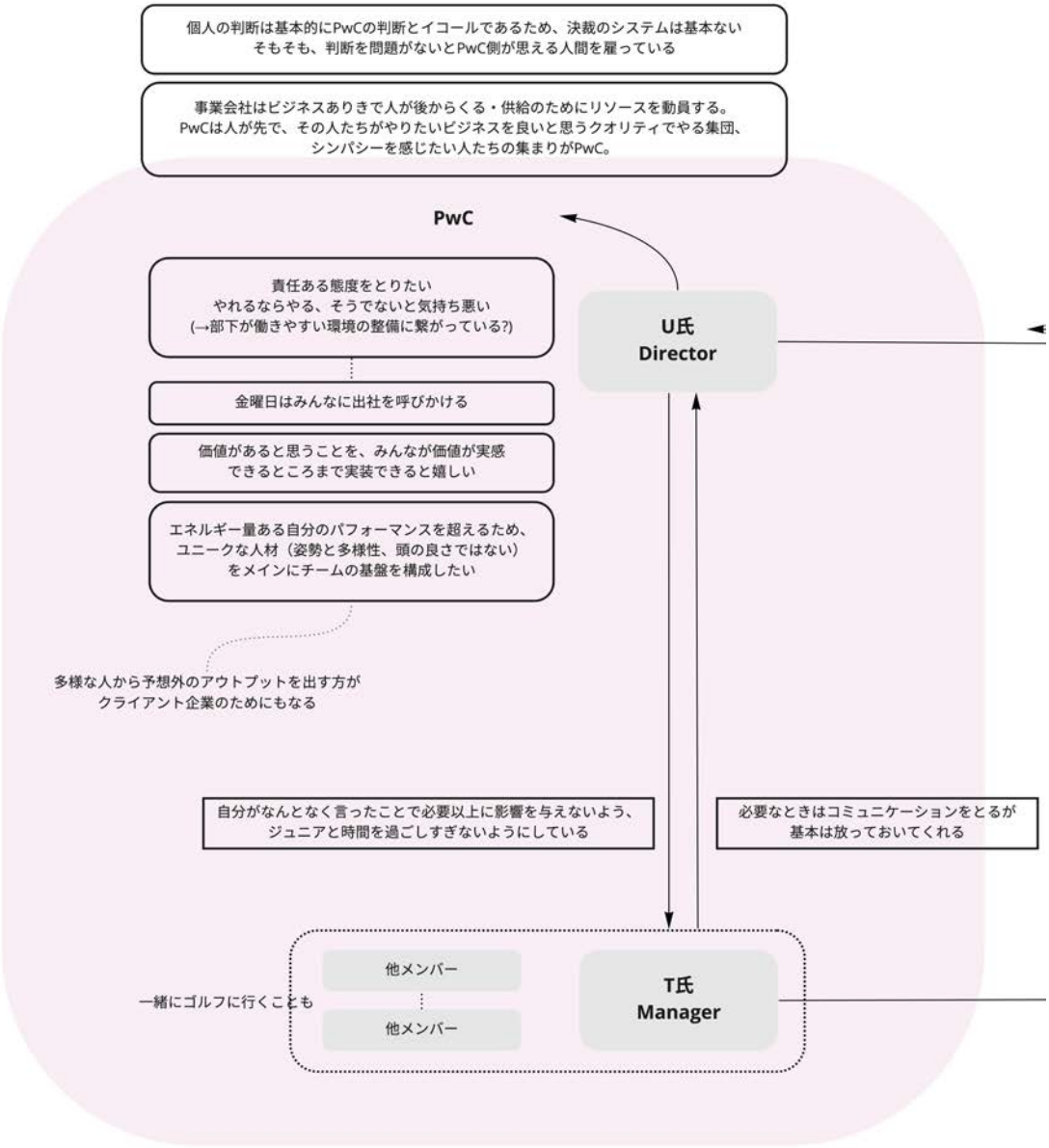

図 3.10 コンサルタントファーム内部の信頼関係

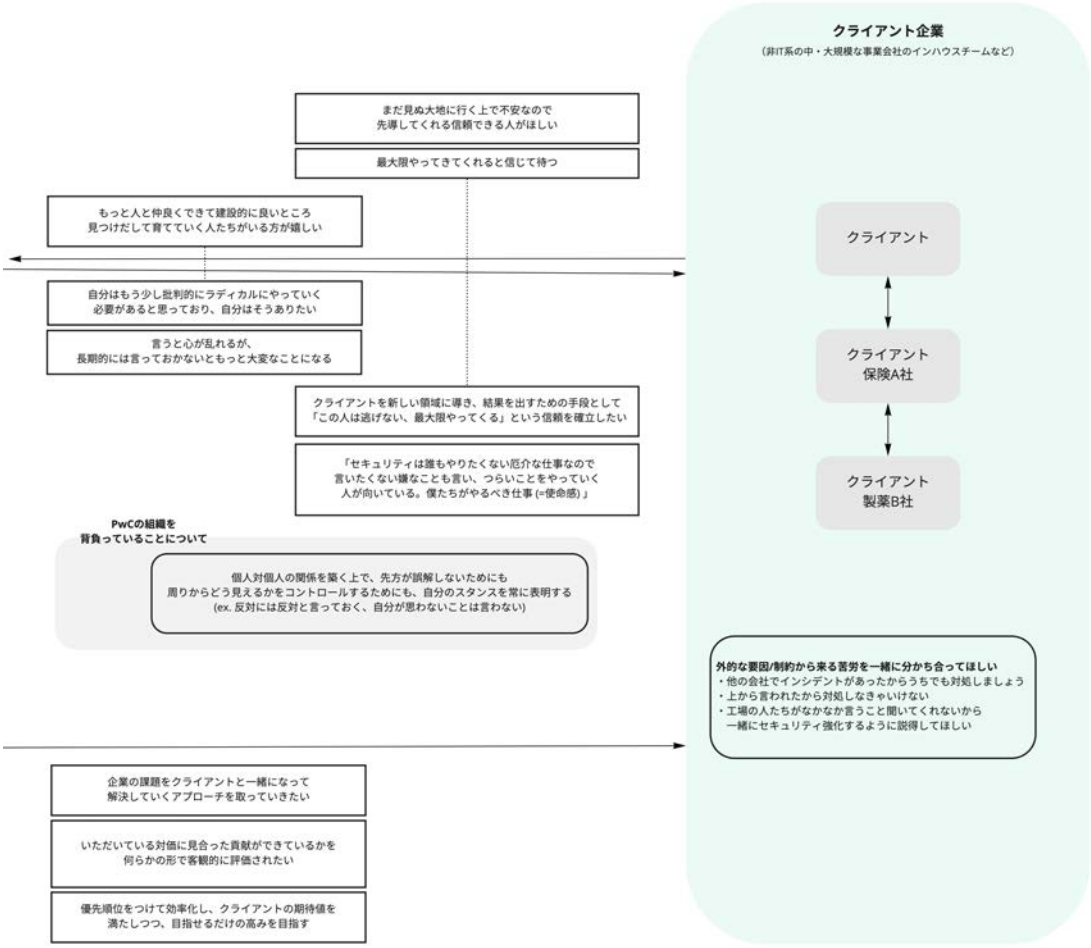

図 3.11 コンサルタントとクライアント間の信頼関係

3.2.4 クライアント組織の行動を促すフロー

分析手順

2022 年 8 月 31 日、三回目のエスノグラフィー調査に先立ち、PwC の U 氏と T 氏を対象に、作成したコンサルタントの文化的背景、同僚やクライアントとの信頼関係に関する分析結果（図 3.9）を持参の上、フィードバックを依頼した。

その結果、クライアント側に実際的な行動を取ってもらうため、組織内のどこに作用するべきかが重要だとの指摘があった。これは例えば、企業の取締役会に作用すれば組織全体が比較的すぐに動きやすいなどといった、組織行動における影響力の掛けどころと解釈される。U 氏はこのクライアント組織の行動変容を促すために作用すべき側面を探ったり、そのために伝え方を工夫するプロセスこそが、コンサルティングチーム内で体系化されておらず、個々人の暗黙知が堆積している箇所であると指摘した。

それを踏まえ、2022 年 9 月 6 日、U 氏と T 氏を対象に三回目のエスノグラフィー調査を実施し、コンサルタントがクライアント組織の行動変容を促すため、作用すべき側面をどのように探っているのかを明らかにすることを試みた。この調査も用意した質問リスト（図 3.12）を対象者に事前に送付した。インタビューは１）コンサルタントがクライアント組織を動かす際に、働きかけるべき点をどのように探っているのか、２）クライアント組織の腰が重いときはどんな場合があり得るのか、３）クライアント組織の腰が重いと判断される場合に、コンサルタントはどのような行動変容のための工夫を行っているのか、の三点から構成された。

一つ目の作用点の探り方に関しては、クライアント組織に働きかける際にどのようなスタンスで組織と向き合い、どのようなメッセージを発することを意識してコミュニケーションを行っているかを深掘りした。また個人のコンサルタントが暗黙的、経験的に有する手法があるかを把握するため、コンサルタントがどのような定石的に用いている手法についても質問した。

二つ目のクライアント組織の腰が重いときに関しては、対象者が過去に担当した経験のあるプロジェクトの中から、組織の考え方や発言の傾向の具体的な例を、可能な範囲で共有するよう依頼した。また、組織単位で腰が重い場合と個人単位で腰が重い場合に関して、何が違いを生んでいるのかについても掘り下げた。

三つ目のクライアント組織の行動変容を促すための工夫については、コンサルタントがどのように腰が重いクライアントにセキュリティ態勢を強化することの重要性を認識してもらうよう工夫しているかについて質問した。さらに、PwC の組織を背負いつつも個人のコンサルタントに裁量が任されやすい傾向にあるコンサルティングの現場において、その組織形態が対クライアントの業務においてどのように影響しているのかについても探った。

調査後、文字起こしした内容を基に分析を行い、図表を作成した（図 3.13）。分析図の作成にあたっては、大きく三つの構成に分けて情報を抽出し整理した。

一つ目は、クライアント側の組織構造がどのように、コンサルタントがクライアント側の作用すべき側面を把握することを可能にしているか、という点である。特にコンサルタントと接する場面において、クライアント側の考え方がどのように現場に表出するかという点を図表上に可視化した。そのため、図上ではコンサルタント側とクライアント側を別の大枠に分け、双方の内部的な考え方を枠内に、その考えの表出するところは枠の淵に、枠を超えて相互的にやり取りをするコミュニケーションの部分は枠と枠の間の矢印上に配置した（図 3.14）。

二つ目は、上述のようなクライアント側の特性や表出する考え方を、コンサルタントがどのような工夫や手法上のコツを駆使して汲み取っているかという点である。これはコンサルタント個人がこれまでクライアントと現場で接してきた自身の経験の中で、クライアントの言動やそれにどう対応したかの過去のケースを話してもらうことで実施した。そのような調査の中で共有された内容を矢印上に配置し、図表を作成した（図 3.15）。

三点目は、作用点を探るプロセスに対して、コンサルタントが現状感じていることについてである。調査の中で、どの作業部分が特に感覚的で、それが明示化されるとどのような影響を与えるのかに関しての発言を収集した。それに関連する内容を抜粋し、箱状に配置した（図 3.16）。

以上の三つの構成を統合することによって、メトリクスを用いてクライアント組織の行動を促すフローを分析し、図 3.13 の分析図を作成した。図 3.13 は精緻なため、図 3.14、図 3.15、図 3.16 に分割した。

前提
- コンサルタントの立場として、クライアント側に具体的にどんなアクションを取ってほしいのか
- 現状、メトリクスはボトムアップと表現していたが、現状は (逆算型でないとすれば)
  何を心がけてメトリクスを作っているのか

クライアント企業を動かすときの作用点について
- クライアント企業における、アクションを取る (作用点となる) 個人とは具体的に誰なのか
  (職位によって表されないかも知れない)
- 他のケースだと違う人が作用点になり得たりしますか？
- コンサルタントは感覚的に作用点を探るとあったが、現状、具体的にどう作用点を探り、働きかけているのか
- 現状、作用点を探る際に、アクションを取る個人の関心事をどう探っているのか

クライアントの腰が重いとき
- どういう時にクライアント側の腰が重そうだと感じたか
- クライアントの腰が重い状態を動かすのはどんな要素がありそうか。プロジェクトのDeadlineの存在なのか、外圧なのか

腰が重いときに動かすプロセス
- クライアント側がメトリクスだけでは腰が重く動けない際、行動を促すために、どのようなメッセージの伝え方・見せ方を心がけているか

追加質問
- 組織P社のインターフェースとして立つときに、コンサルタント個人は組織をどれくらい意識しているのか
- 最後に：対個人・対組織の信用はどう測れると思うか、アクター間のTransactionの回数や濃さなのか

図 3.12 三回目のエスノグラフィーの質問リスト

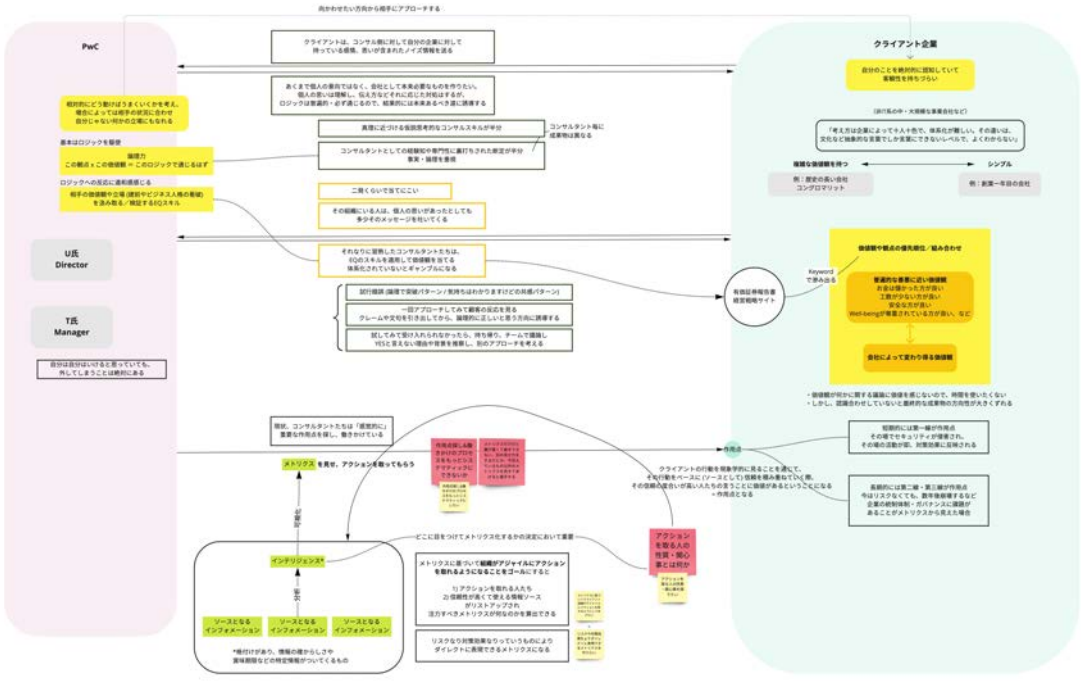

図 3.13 コンサルタントがクライアント組織の行動を促すフローの全体像

分析内容

まず図 3.14 に、セキュリティコンサルティングプロジェクトにおけるクライアント組織側の動きについて示した。

前提として PwC のコンサルタントは「創業間もない中小企業よりも現在 PwC がクライアントとしているような歴史の長い大組織の方が顕著だ」とした上で、組織内のパワーバランスや価値観が複雑で、組織の考え方の傾向を類型化・モデル化することは難しいと認識している。特に組織が重視する指標に関しては、短期的な利益が優先される組織もあれば、安全性や社会的責任が第一の組織、従業員やユーザーの幸福が優先される組織など、組織ごとに千差万別だとしている。

U 氏はこれまでの経験上、（特に有事の場合に顕著だが）クライアント組織の中にはそういった重視する指標や価値についての議論に重きを置かない組織が多くあり、「できることなら一回のやり取りで当ててほしい」とやり取りの工数を割こうとしない傾向があると指摘した。そこでコンサルタントは、経営戦略サイトや有価証券報告書などにキーワードとして表出するクライアント組織の理念などを頼りに、組織の価値観や重視する指標を把握する作業を行なっている。

なおコンサルタントはクライアント組織内の構造に、第一線、第二線、第三線からなる三つのセキュリティ防衛ライン、「Three Lines of Defense」があると言及した。また、組織内の防衛ラインや部門ごとにセキュリティ態勢に対する向き合い方や考え方の違いがあることも指摘した。これについてはこの回の調査内では十分な情報が得られなかったため、後日行ったヒアリングや追加調査において補足情報を取得し、図をアップデートした（詳しくは後述）。

次に図 3.15 に、コンサルタントがどのように作用点を探る工夫をしているかを示した。前述したようにクライアント組織の価値観はある程度、組織側が開示している資料などに表出するため、コンサルタントはそれらを手がかりにまずは価値観を推し測ろうとする。さらにプロジェクトが始まると、クライアント組織側はコンサルタント側に向けて、自分の企業に対して抱いている感情や思いが含まれたノイズ情報を送ろうとする。その上で、コンサルタント側に「二発程度で当ててこい」という姿勢を示すこともあるという。

これに対しコンサルタント側は、この観点とこの価値観であればこういうロジックで通じるだろうという論理力を駆使した手法と、相手の価値観や立場を汲み取り検証するための EQ スキルを用いた手法の、両方を駆使していることが分かった。多くの場合、このようなケースにおいてコンサルタントは論理力を駆使する。コンサルタントが指摘するに、本来クライアント組織のセキュリティ態勢を強化することが目的なので、そこに介在するのは個人の意向ではなく、あくまでその組織に本来必要なものという真理のみである。それゆえ企業の状態を診断した上で、普遍的な論理的正しさを武器に、組織が本来あるべき道に誘導することをコンサルタントはまず試みる。

これはある意味、クライアント組織の特質とコンサルティングファームが有する能力の補完性を示唆している。これまで複数の企業ケースを見てきた経験からコンサルタント曰く、クライアント組織は一般的な傾向として、自分の業績や立場を絶対的に認知しているがゆえ客観性を持ちにくいとしている。それに対しコンサルティングファームの場合、相対的にどう動けばうまくいくかを考え、場合によっては相手の状況に立場を合わせることができるとしている。そのため、論理を武器にした正しさを打ち出しやすい。

しかしながら実際的には、前述のようにクライアント組織ごとにどの指標を重視するかの KPI は異なっており、それゆえ、その背後にある価値観を当てにいく作業が必要がある。場合によってそれが経営者の属人的な判断であるケースや現場の人間の思いに隠されたケースがあり、習熟したコンサルタントはクライアントと接しながら EQ スキルを適用して価値観を当てにいく。そこにはコンサルタントの様々な暗黙的なコツが蓄積しており、例として一旦共感を示した上で論理的正しさを伝える工夫や、あるいは一回アプローチして文句を引き出した上で説得にかかる方法、あるいは持ち帰ってチーム内で議論するなどである。

コンサルタントはこういった作用点を探りに行く過程に対して、「極めて感覚的な作業」と捉えている。したがってこの手法を可視化することで、セキュリティメトリクスに基づいて組織が行動を取る実際のアクターは誰なのか、あるいはその際に信頼性が高く有用な情報ソースは何なのかがリストアップされ、注力すべきメトリクスが何なのかを算出できると考えている。これを図 3.16 に示した。

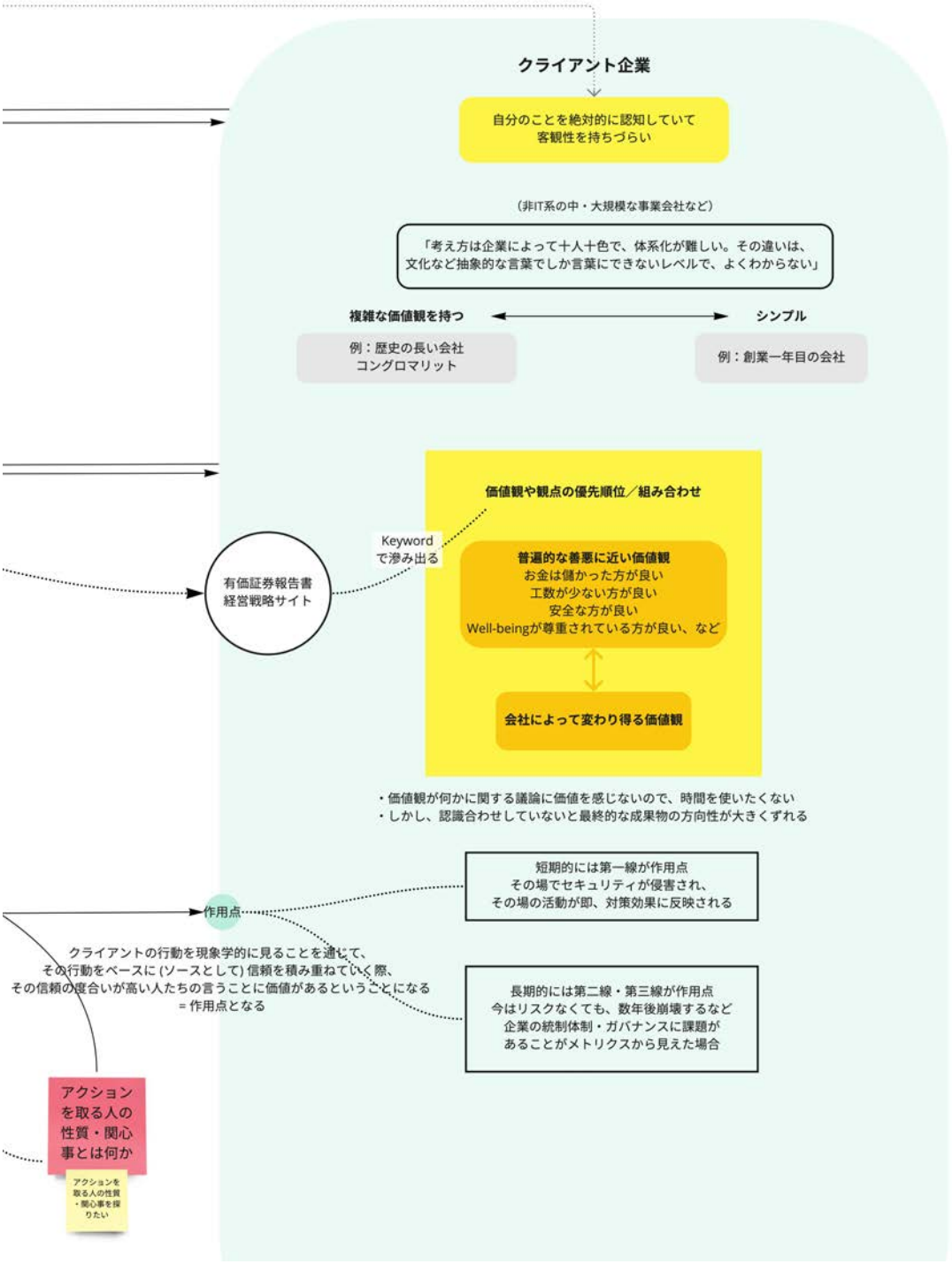

図 3.14 セキュリティコンサルティングの現場におけるクライアント組織側の動き

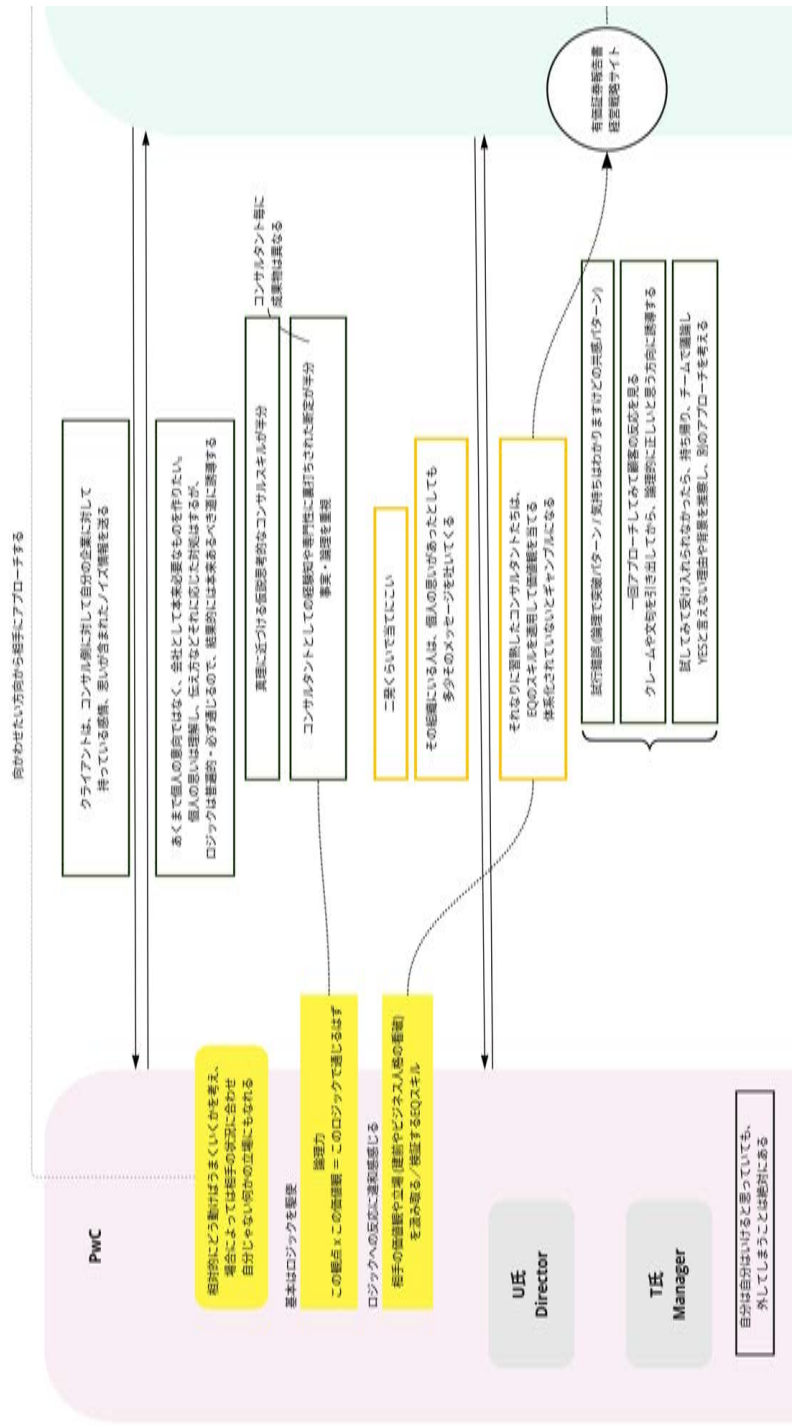

図 3.15 コンサルタントがクライアント組織の価値観を探る上での工夫

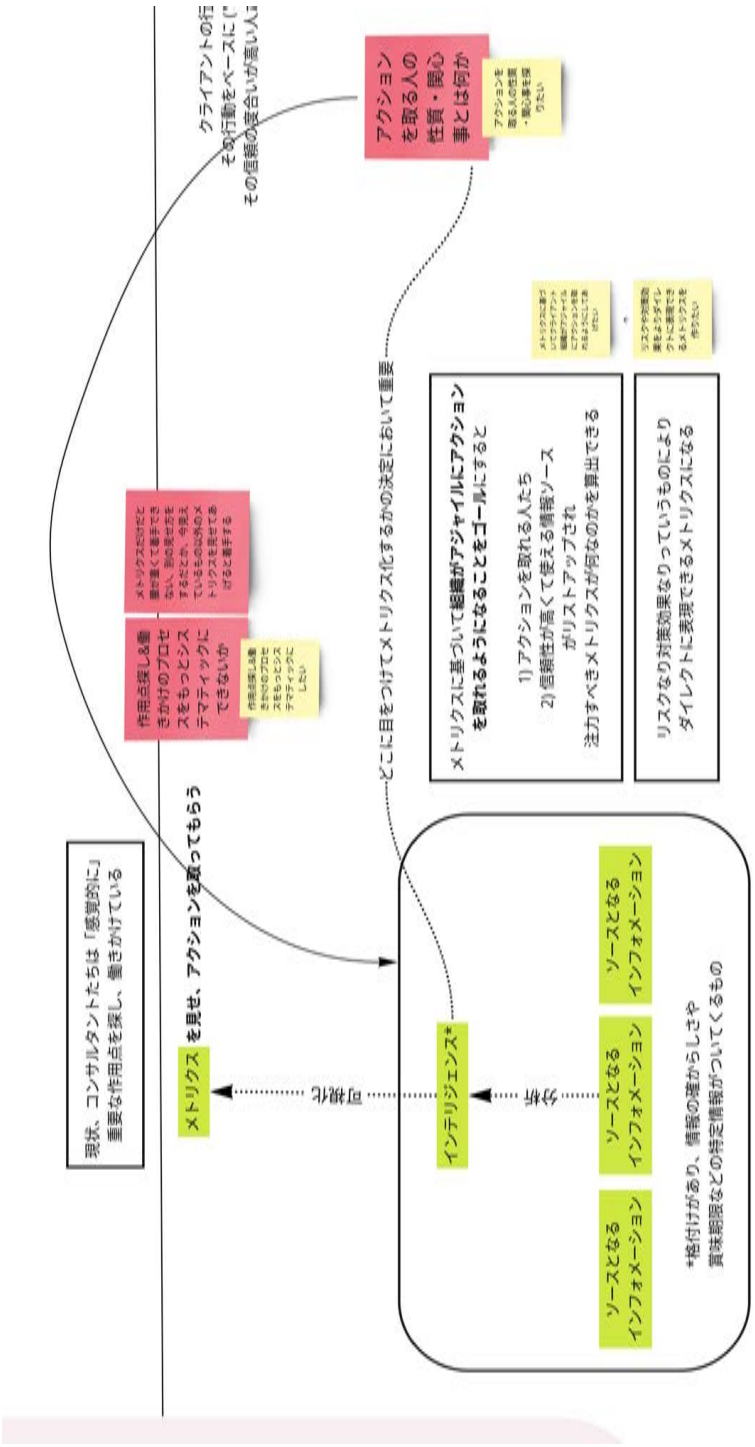

図 3.16 クライアントの価値観探りの作業についてのコンサルタントの考え

その後の分析のアップデート

2022 年 9 月 6 日の調査において、対象の両氏はクライアント組織側にありがちなセキュリティ態勢や組織構造についても言及したが、精緻な分析を行う上で、この回の調査のみでは不十分な内容だった。そのため後日、作成・分析したフロー図 3.12 を持参の上、再度対象の両氏や私立大学機関 K 大学院のセキュリティ専門家に対してヒアリングを行ってクライアント側の組織体制についての情報を取得し、フロー図に反映しアップデートした。時系列が前後するが、ここでは便宜上、変更反映後のフロー図におけるアップデート部分を以下の図 3.17 に示す。

アップデート部分の部分の大半は、既にコンサルタントから指摘のあった「Three lines of defense」に関してである。組織における Three lines of defense は、セキュリティ侵害への対応やそれに備えた態勢強化を行う組織内の三つの機能を指す。第一線は基本的には現場のビジネス部門や業務執行部門を指し、部門ごとに個別のビジネス目標や KPI がある。例として銀行のローン部門などが挙げられ、この場合の KPI は貸し付け額などである。多くの場合、セキュリティの強化や管理のために労力を割くことは業務の邪魔になりやすく、それをコストと捉える向きもある。コンサルタントの短期的な作用点は、この第一線である（例：セキュリティを意識した行動を普段の業務に取り入れるためのガイドラインの策定）。

それに対し、第二線は、リスク管理部門・コンプライアンス部門など間接管理部門である。第二線は、第一線の統制を構築したり、生じ得るリスクに対する監視を行い、第一線に助言を行う立場にある。そして高い独立性と客観性を持つ立場から、第一線と第二線の活動が適切に統制されていることを経営層や取締役会に保証する内部監査部門、すなわち第三線がある。この第二線と第三線は、将来的なインシデントの発生などを見据えて企業の統制体制・ガバナンスを強化すべき立場にあるため、コンサルタントの長期的な作用点となる。

なお、上記の記述や図中の 3 lines of defense の定義に関する説明は、調査と一部は PwC のサイバーセキュリティコンサルティングサービスのウェブサイト[1]から引用したものである。

1 PwC「3 lines of defense」, https://www.pwc.com/jp/ja/knowledge/column/viewpoint/grc-column001.html, 2023 年 1 月 14 日参照

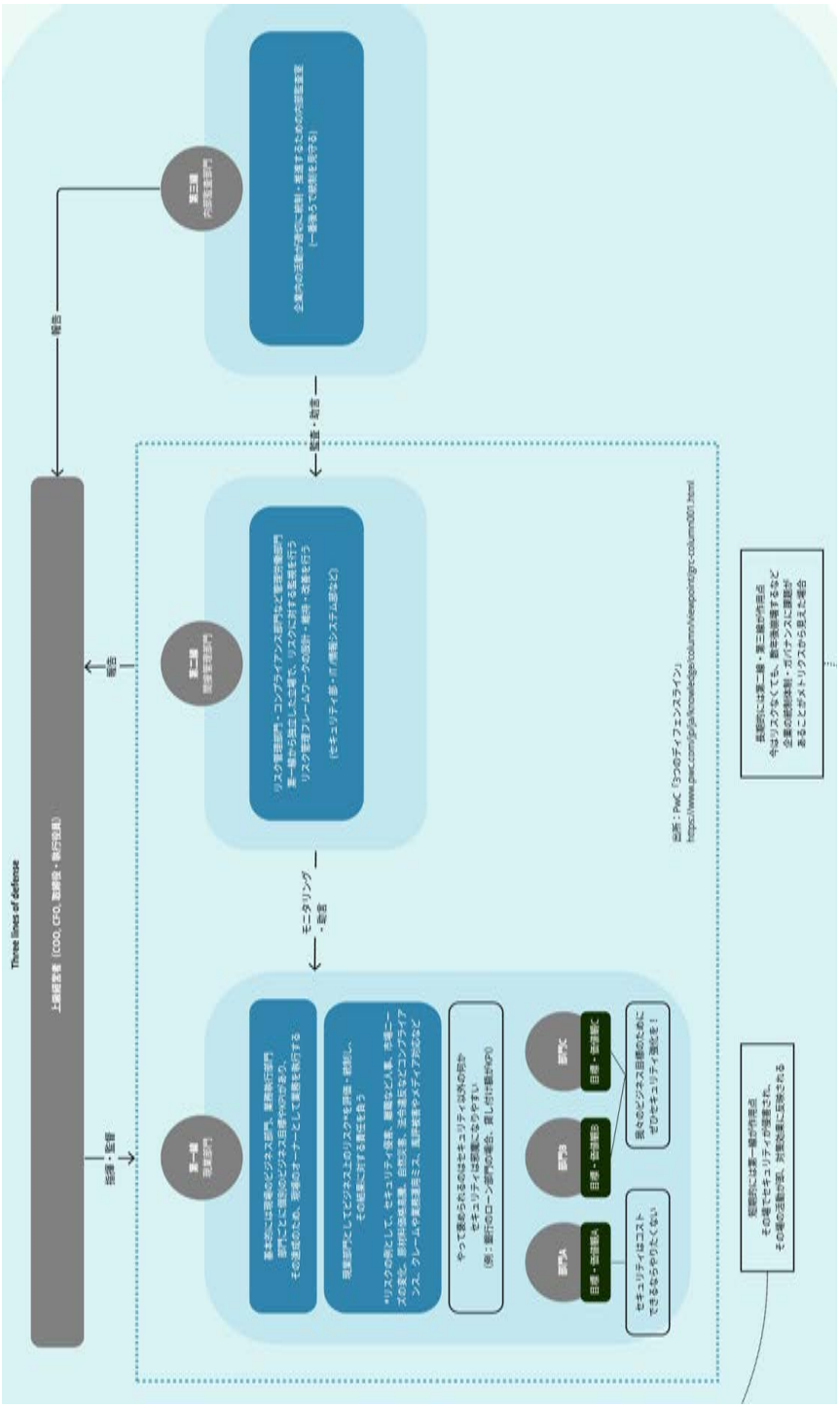

図 3.17 変更反映後のフロー図：アップデート部分

3.2.5 アクターのゴールとメンタルモデル

分析手順

ここまで三回のエスノグラフィーを経て作成した分析図群を基に、U 氏と T 氏、そしてクライアント組織が持っていると想定されるゴールとメンタルモデルをサービスデザインの手法を用いてそれぞれ抽出した。

一般にサービスデザインの手法では、アクターの行動から「なぜその行為をしているのか」を人の関係性や背景を想起しながら観察し、ゴールとメンタルモデルを解釈する。アクターはあるゴールを達成するため現場で様々な行動をとっており、ゴールを達成するための「認知」と「行動」のセットがメンタルモデルと定義される。例として運転の練習をする際、「交差点を右折したい」というゴールに対する「交差点に差し掛かると、方向指示器を点滅させる」というメンタルモデルなどがその例である [38]。

しかしながら本研究ではコンサルティング業務の特性上、身体的な動作を伴わないため、ゴールはアクターが職務上ミッションとしていること、メンタルモデルは「こういう判断に迫られると、こういう行動をとる」と定義した。そこで三回のエスノグラフィーを経て作成した分析図群から「〜したい」というゴールを含む情報と、それを達成する判断と行動を組となるように抽出、文脈に応じて解釈し、Miro ボード上の付箋に記載した。それを U 氏、T 氏、クライアント組織ごと、特性ごとに分類分けした後、上位のゴール、大ゴール・中ゴール・小ゴールなどゴールの抽象度ごとに並べ替えた。このような方法で作成したアクターのメンタルモデルとゴールの分析図を、後述の三つの図に示した。

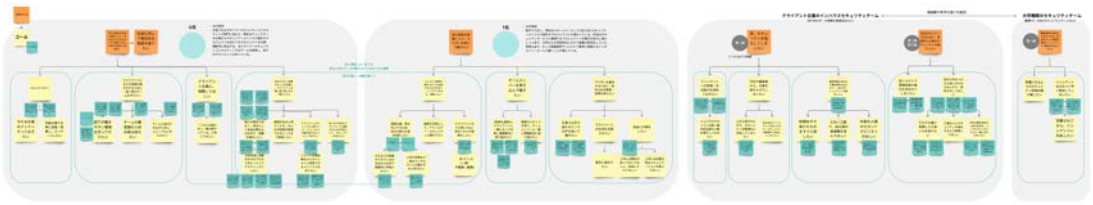

図 3.18 アクターのゴールとメンタルモデルの全体像

分析内容

まず図 3.19 に、U 氏のゴールとメンタルモデルを示した。上位のゴールに関しては、既に分析を終えている分析図上の発言を解釈し、「社会に対して責任ある態度を取りたい」「持てる能力は社会に還元したい」とした。分析では、これらが以下の四つの中ゴールを作り出している。

一つ目は、仕事には全力で挑みたいというゴールである。これは積極的にやりたがる人の少ないセキュリティ業務において、率先して課題を解決しようとする姿勢と、より貢献しようとするメンタルモデルに繋がっている。そして、可能な限り仕事に没頭したいという下位ゴールに繋がっていると思われる。

二つ目は、高い質のチームを作りたいというゴールである。これはあくまで、クライアントに与える価値を最大化するための手段であると解釈した。このゴールは、部下が働きやすい環境整備やチームの最低限の質を保ちたいというゴール、またユニークな人を入れたいという下位ゴールに繋がっている。これらのゴールが観測されたメンタルモデルには、次チームメンバーと接すると最低限のコミュニケーションは心がけるが、あまり時間を一緒に過ごして影響を与えることのないようにする、などが挙げられる。

三つ目は、クライアント組織に信頼してほしいというものである。特に業務遂行のためにも、目の前にいるコンサルタントは逃げないと思ってほしい、などが下位ゴールとして挙げられる。これは、反対意見を持つクライアントに対して伝え方を工夫するというメンタルモデルから観測された。

四つ目は、企業の意思決定者と直接接し社会に大きな影響を与え得るという立場から、クライアント組織に真に貢献したい、動かしたいというゴールである。これには、個人の意向でなく組織が本来必要としているものを作りたい、そのための作用点探しのプロセスを体系的に行いたい、などの複数の下位ゴールが付随している。これは、プロジェクトが始まると行動を取る人の考え方を推察したり、必要があれば批判的な態度を取るという行動から観測された。

次に図 3.20 に、T 氏のゴールとメンタルモデルを示した。T 氏は U 氏とは少し異なるゴールを有し、上位のゴールは「自己成長を実感したりやりがいを感じて働きたい」であると解釈した。これは、仕事の効率を上げてプライベートの時間

を確保したい、自由に仕事をしたいといった下位ゴールから観察された。また、効率的に仕事をするというメンタルモデルも観測に影響している。他にもチームメンバーを巻き込んで働きたいというゴールもあり、これはクライアントと一緒に共創的に課題解決に取り組みたいという下位ゴールを伴う。

これらを踏まえ、T 氏の定義するヘルスケア業界を動かすような仕組み作りを通じた貢献や社会的インパクトというのは、T 氏の大学時代の創薬の研究経緯を考慮すれば、自分の得意や興味を活かしてやりがいを感じて働きたいということの表れではないかと分析した。したがって下位ゴールは、その文脈での上位ゴールに寄与するものであって、例として自分の能力を高め成長したいのは与える貢献の絶対量を最大化するためであり、そのために貢献ができているかを客観的に評価されたいという小ゴールが誘引されるものと解釈した。

まとめとしてこの時点の分析では、同じ社会への貢献やインパクトがゴールであっても、U 氏と T 氏ではその上位ゴールが異なるものと考えられる。これは仮説としては、世代や役職の違いが影響しているのではないかと推察した。

最後に図 3.21 に、クライアント側のゴールとメンタルモデルを示した。クライアント組織は、前述したように第一線と、第二線・第三線でその性格が異なる。第一線は、有事の際の現場の担当者としてインシデントへの防御・対応能力を高めておきたいというゴールや、顧客情報の機会損失が出るため一刻も早くインシデントを解決したいといったゴールが見られた。特に後者は、少ない工数で自分達の価値観を汲んでほしい、価値観や理念に関する議論に時間や手間をかけたくないといった姿勢が表出しているものと分析した。これはプロジェクト進行時に、価値観を問われると意義を感じず次の話題に行こうとするといったメンタルモデルから分析したものである。さらに、第二線・第三線は、場合によっては安いコストで対策強化を済ませてしまいたいというものや、そもそも何から手をつけたら良いのか分からないので指針を示してほしいといったゴールがあるとの指摘を解釈した。

以上を踏まえ作成したアクターのゴールとメンタルモデルに関する図表を、対象であるコンサルタントに見せ、フィードバックをもらうと同時に、どの領域に注力したいか、支援してほしいかの意向を確認した。

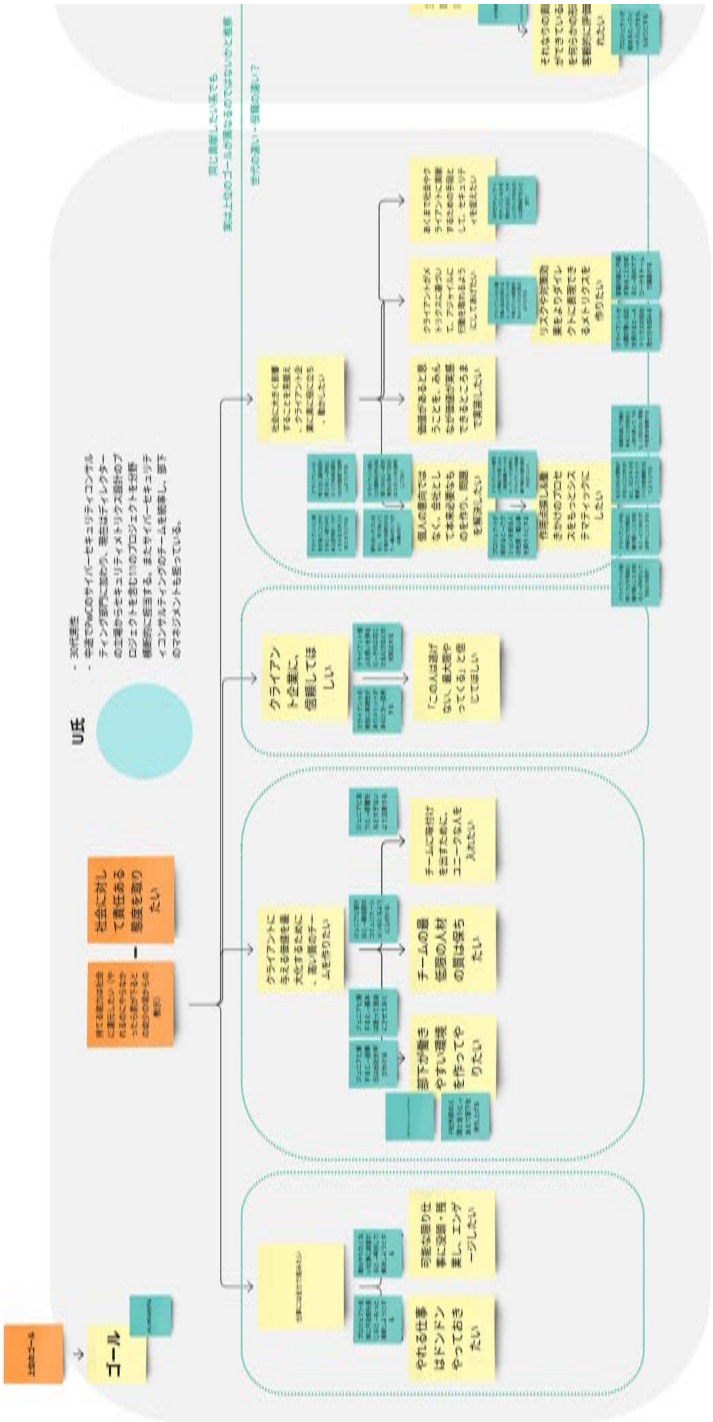

図 3.19 U 氏のゴールとメンタルモデル

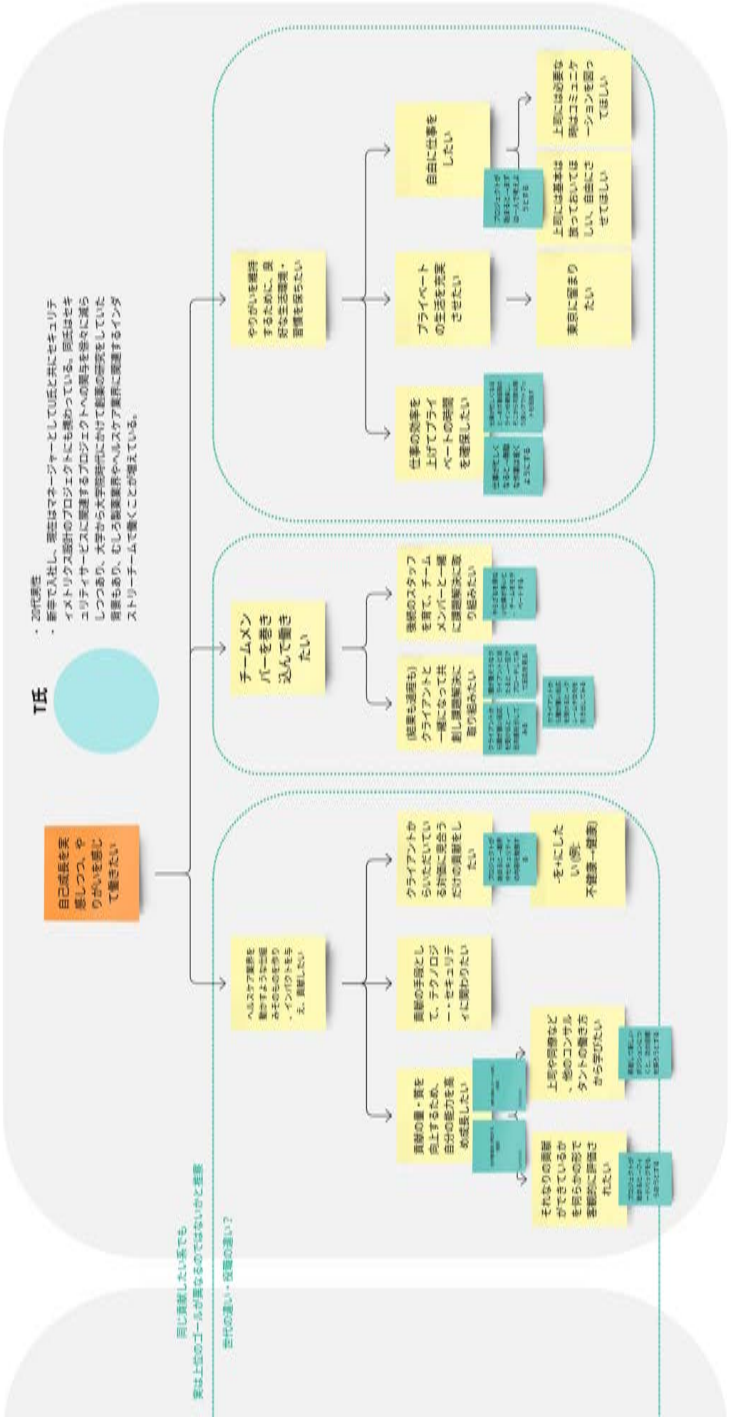

図 3.20 T 氏のゴールとメンタルモデル

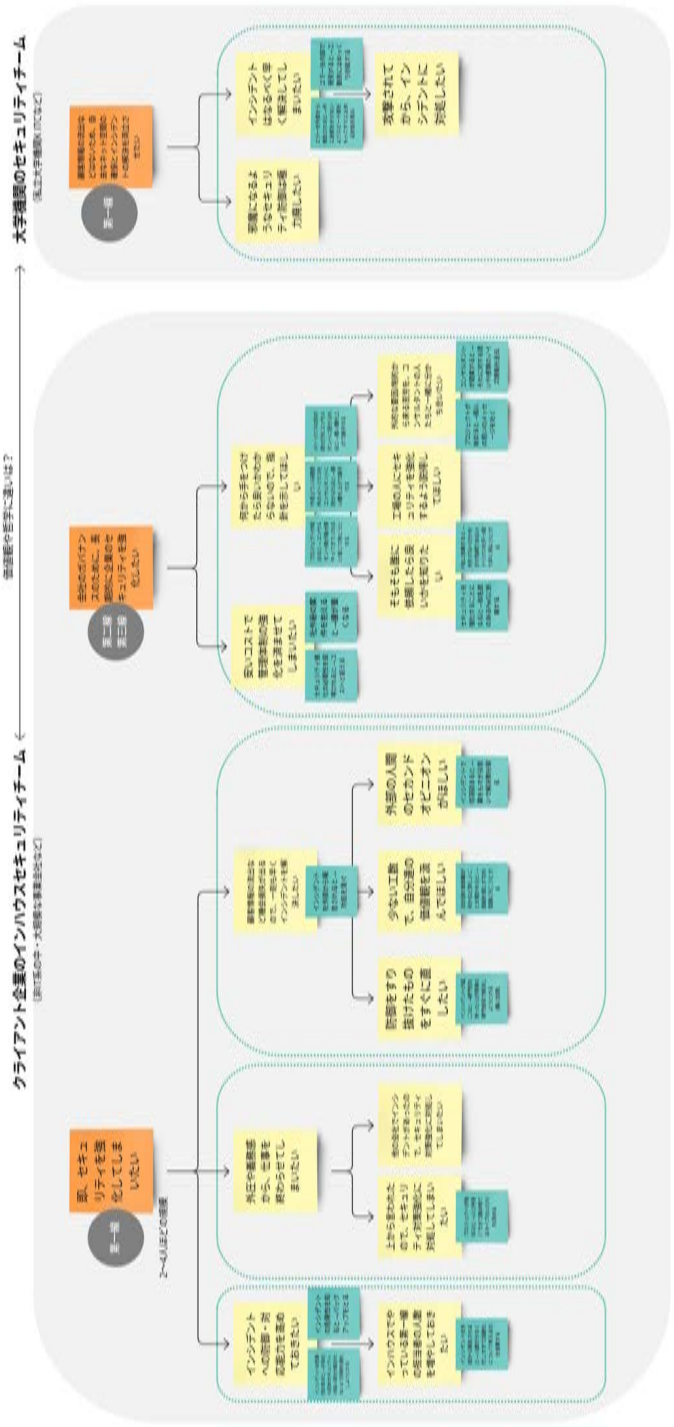

図 3.21 クライアント側のゴールとメンタルモデル

3.2.6 対象者の要件の特定：コンサルタントによる中間評価

2022 年 10 月 18 日、この時点までの計四回のエスノグラフィーを通じて実施した分析、特に最初三回のエスノグラフィー内容を抽出、整理した結果であるアクターのゴールとメンタルモデルに関する分析図をコンサルタントに見せ、分析結果の中間評価を行った。目的はこれまでの分析の整合性を確認すると共に、対象者である PwC のコンサルタントがどの領域のゴールを達成したいか、筆者ら研究チーム側に支援されたいかの意向を確認し、研究が今後提供し得る価値の方向性・応用可能性について特定することである。

U 氏はまず、現時点版の分析の整合性について言及し、コンサルタントとして働く上での考え方や、コンサルタント側のゴールとメンタルモデルの分析について評価を行った。結果として、社内におけるコンサルタント同士の信頼関係や対クライアントの信頼関係の考え方が、コンサルタントとして経験を積む上で変化してきたことを挙げた。特に、長年コンサルタントして働く上でより効率的に仕事ができるようになり、その結果としてクライアント組織を本来あるべき状態にするために、求められる役割を引き受けることができるようになったとした。この詳細については、以下の図 3.22 に示した。

またそのような文脈の中で U 氏の上位ゴールはただコンサルタントとしてクライアント組織に貢献することで社会に貢献したいという動機づけではなく、体力や精神力などエネルギーを使い果たす上で「どうせエネルギーを使うなら、価値ある活動に長くエンゲージしたい」「どうせエネルギーを使うなら、やれるのにやらないと気持ち悪い」ということである。そしてそのゴールの下に、社会に大きく影響することを見据え、クライアント企業が価値を実感できるように実装したいという中位ゴールがある。その下に付属する信頼に関しても、従来分析したようにただ信頼を確立したいということではなく、結果を作るための手段として信頼関係を構築したいということが判明した。

さらに部下を含めコンサルティングチームのマネジメントについても、従来分析したように単に質の高いチームを組成したいということではなく、U 氏自身からは出せないような突飛な発想やそれに基づく成果を創出することが理由であり、したがってあえて「ユニークな人材をメインにチームの基盤を構成したい」との

指摘があった。これらの評価内容を基に更新した分析を、U 氏に関しては図 3.23 に、T 氏に関しては図 3.24 に示した。

またU 氏は、今後研究上の要件として注力、支援すべき領域について言及した。これまでの分析図の制約としてコンサルタント側の分析については比較的普遍性のある分析内容になる可能性があるため、セキュリティメトリクスという特定サービスに対象を限定するべきだと指摘した。これはセキュリティメトリクスのサービス対象となる企業は価値観の類型化が難しく、クライアントがどこに価値を感じるか、特にあるクライアントの場合はここに価値を感じるというケースが見えることが重要であるためである。

さらにU 氏は、セキュリティメトリクスというサービスが現時点ではまだ新しいサービスであり、現状では意欲的なリーディングカンパニーしか取り組んでいないと述べた。特にセキュリティメトリクスに用いられているテクノロジーや手法は従来からセキュリティ分野では用いられているものではなく、形式的にやっている企業には手が出ない領域だとした。一方将来的にはその限りでなく、今後サービスの提供対象の裾野が広がっていく可能性を指摘した。そのため、数年先を見据えたアウトプット研究として、例え一ケースであったとしてもクライアント側のケースから学ぶ必要があると述べた。応用可能性については、セキュリティメトリクスの価値を明示化できれば、現状ではコンサルタント自身が気づいていない、他分野への応用可能性に気づくことができるかもしれないとした。

以上をまとめると、計四回のエスノグラフィーを通じて本研究の対象者であるコンサルタントの働き方やその背景についての分析を行い、対象が抱える課題と要件の特定を行った。その結果、コンサルタントの要望として、クライアント側が抱える課題や組織内部の価値観や文化、制度を明らかにしてほしいということが特定でき、これに関してコンサルタント側と合意することができた。またこれを踏まえ、本研究が解くべき課題は、どのようにしてサイバーセキュリティコンサルティングの現場でクライアント組織の価値観を可視化し、コンサルタントがクライアントの要件を汲み取りセキュリティ態勢を強化できるよう支援できるか、であると設定するに至った。

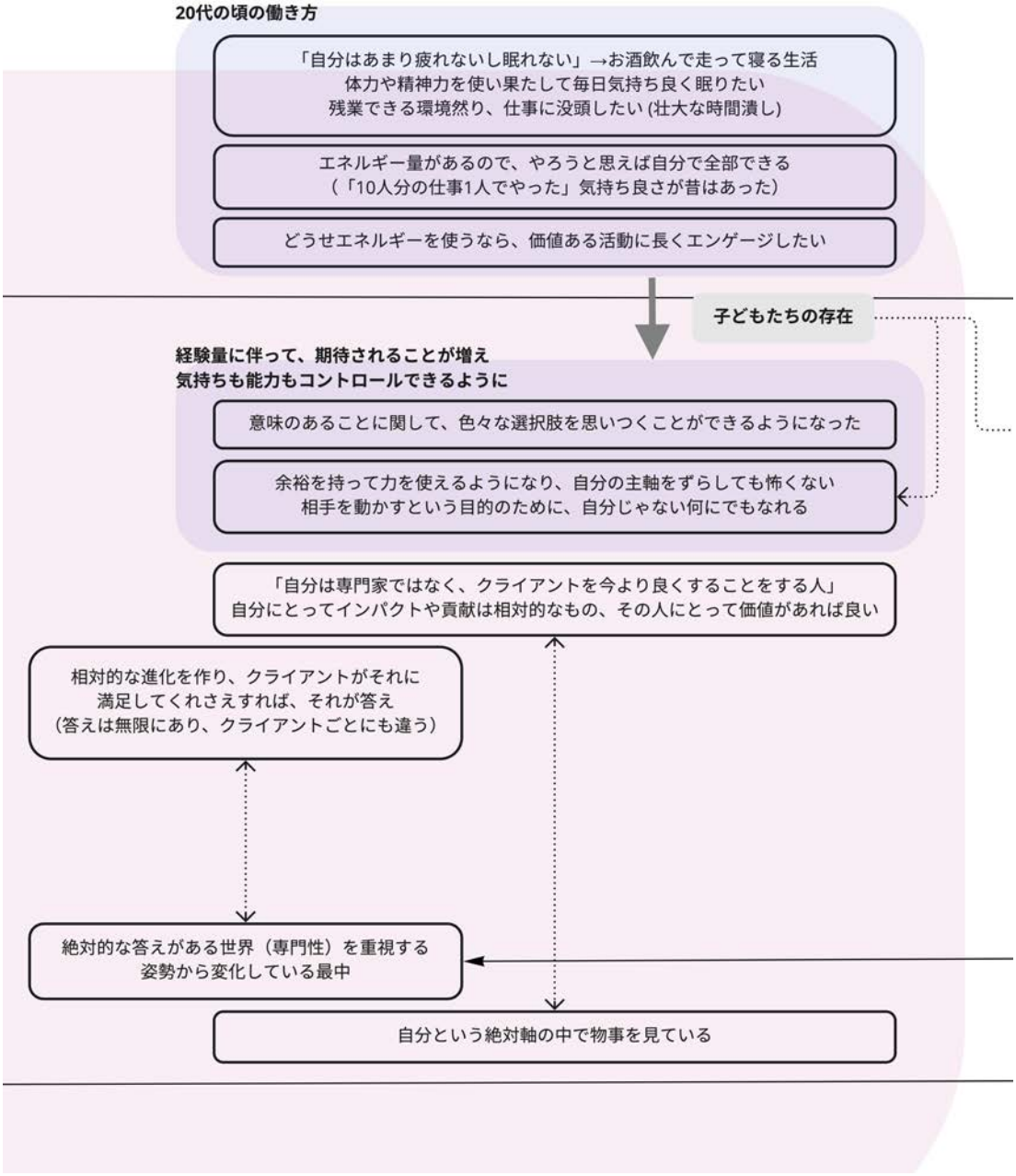

図 3.22 中間評価を受けて更新したコンサルタントの背景

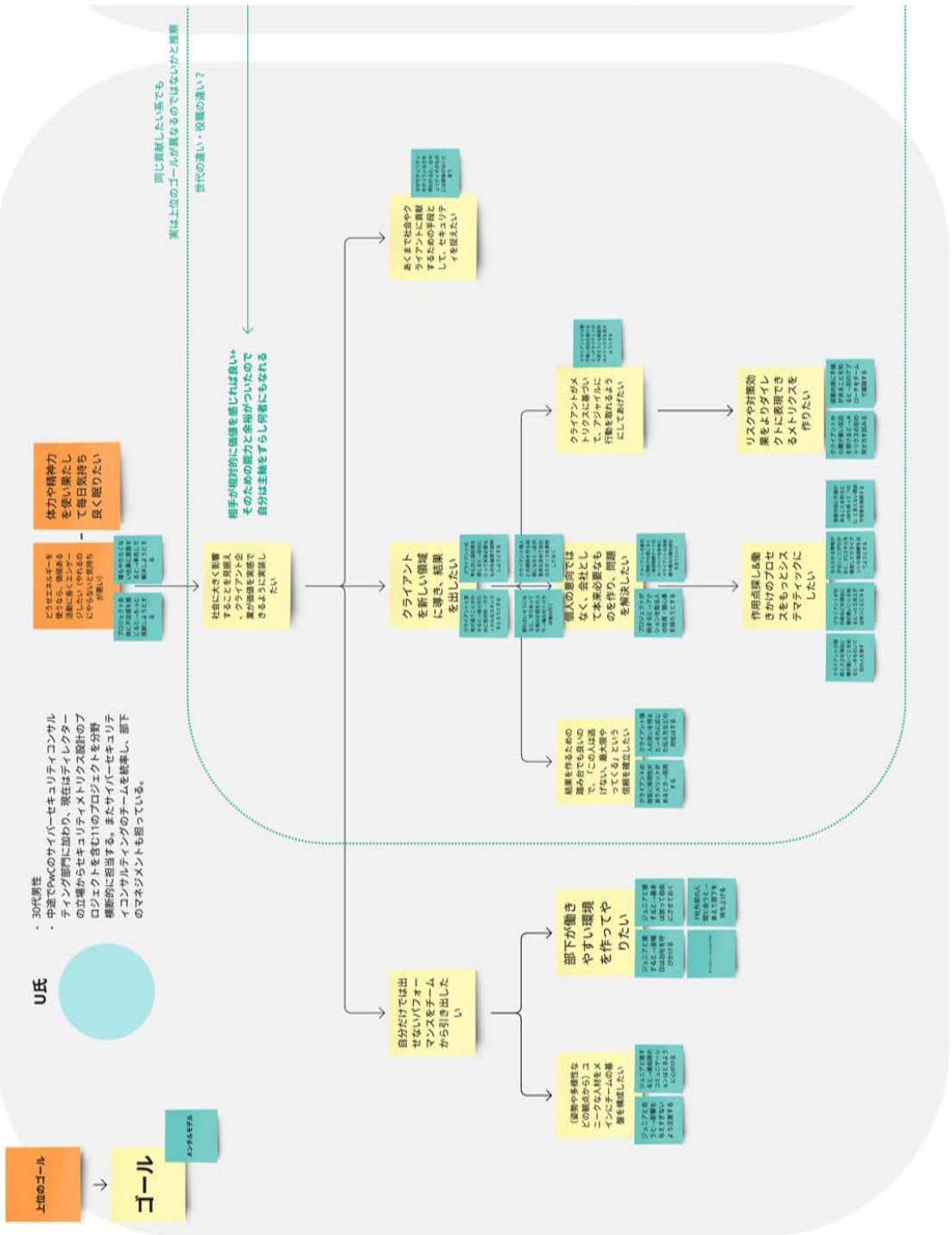

図 3.23 中間評価を受けて更新したU氏のゴールとメンタルモデル

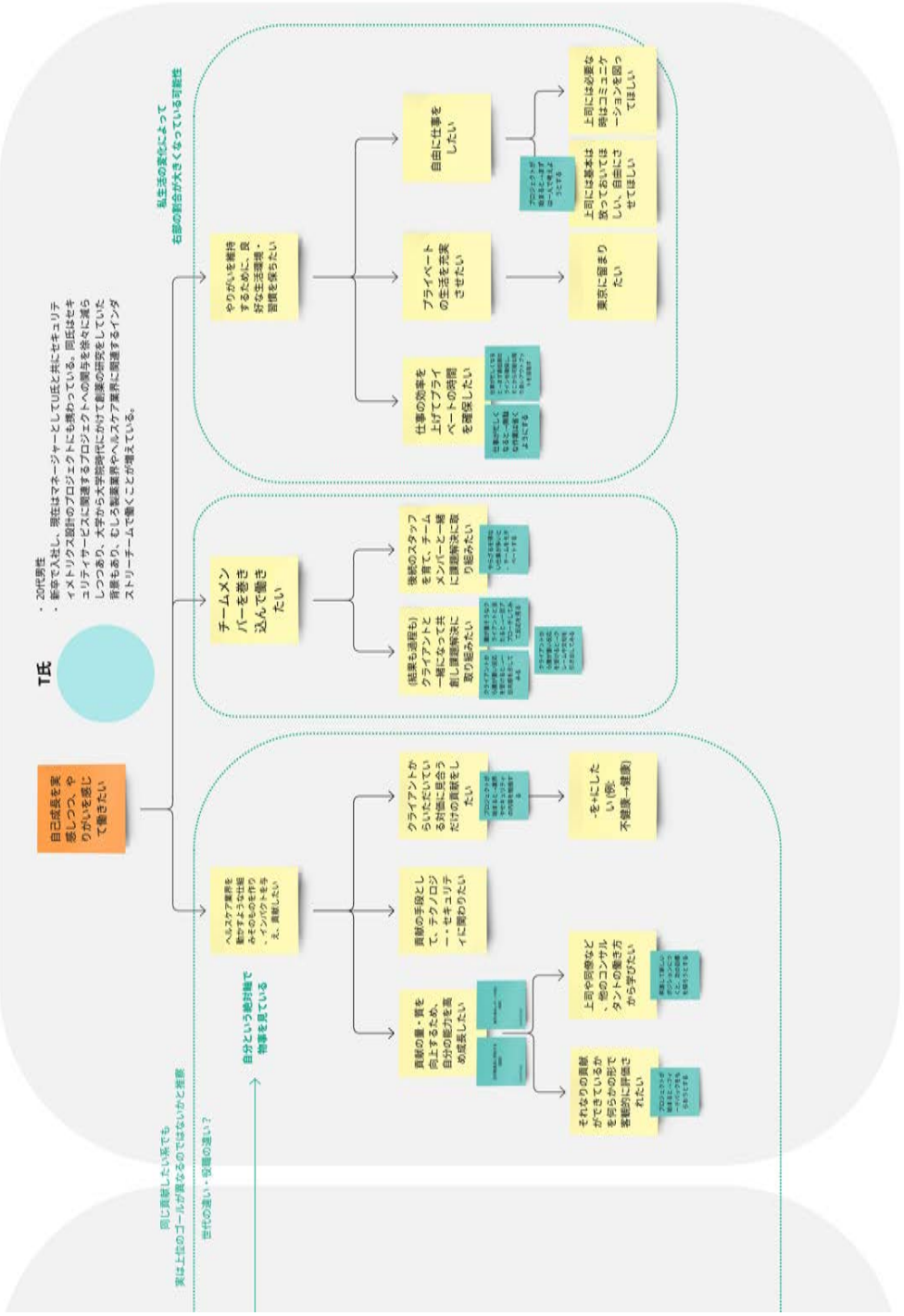

図 3.24 中間評価を受けて更新したT氏のゴールとメンタルモデル

3.3. デザインプロセス

3.3.1 プロトタイプの作成方法

エスノグラフィーを通じて特定されたコンサルタントの要件に基づき、本研究ではクライアントのモデルケースとなるような組織への質的調査を通じて、クライアント側が抱える課題や組織内部の価値観や文化、制度を明らかにすることを試みた。そして質的調査の結果明らかにしたクライアント組織の分析内容を、コンサルタントが見て理解しやすい形で可視化するため「組織のセキュリティ態勢・図解ハンドブック」を設計した。この図解ハンドブックのプロトタイプを作成するために実施した質的調査の対象は、インシデント対応を担うチーム CSIRT で活躍する私立大学機関の職員と、CSIRT に関する研究を行う研究家である。

最初の質的調査の対象は、私立大学機関 K におけるセキュリティ専門家の S 氏と、私立大学機関 K CSIRT におけるセキュリティ専門家の H 氏である。私立大学機関 K CSIRT は、基は私立大学機関 K インフォメーションテクノロジーセンター（ITC）が長年担ってきた学内のサイバーセキュリティ態勢の強化を近年引き継ぎ、学内のネットワーク環境やデータの流れを監視することでセキュリティインシデントの検知・対処を行っている。S 氏は私立大学機関 K において CSIRT 設立の経緯を知る人物として、H 氏への質的調査の事前分析に協力を依頼した。また H 氏は私立大学機関 K ITC の時代からサイバーセキュリティの専門家として長年セキュリティ業務を牽引し、私立大学機関 K CSIRT の設立とその役割の発展に大きく貢献してきた人物として分析に協力を依頼した。

三人目の質的調査の対象者は、CSIRT 研究家の Y 氏である。Y 氏は、日本シーサート協議会に加盟する企業や組織のセキュリティ態勢について深い知見を有し、CSIRT の創設のみに留まらない本質的なサイバーセキュリティ態勢の強化を訴えてきた。日本シーサート協議会は、日本における CSIRT の普及と発展、インシデントに関わる情報共有を担う連盟であり、PwC CSIRT や私立大学機関 K CSIRT を含む国内の企業や組織に設立された CSIRT の多くが加盟している[2]。

2 日本シーサート協議会, https://www.nca.gr.jp/, 2023 年 1 月 14 日参照

これら、組織内部において専門家として実務的な経験を豊富に有する私立大学機関 K 側の S 氏および H 氏と、多くの企業や組織のセキュリティ態勢を俯瞰的に見られる立場にある Y 氏の二種類アクターをクライアント側の代表的な対象として質的調査を実施した。それによって、クライアント組織におけるセキュリティの考え方や価値観のケースを抽出することを試みた。

質的調査を経て抽出された情報を、エスノグラフィー後に作成した分析図とほぼ同じ要領で図表化し、組織のセキュリティ態勢・図解ハンドブックの構成要素となる個別の図解のプロトタイプを作成した。最終的にそれらの図表をまとめ、図解ハンドブックの形になるように整理した。デザインプロセスの節では、クライアント組織側の価値観を明らかにするために行った質的調査の内容と、その結果作成したプロトタイプの詳細について時系列順に述べる。

3.3.2 質的調査：私立大学機関 K セキュリティ専門家

2022 年 10 月 28 日、クライアント組織側の組織構造や文化的背景についての理解を鮮明にするため、クライアント側の代表的ケースとなる私立大学機関 K のセキュリティ専門家 S 氏に質的調査を行い、その内容を基に事前分析を行なった。質問リストは以下の図 3.25 に示した。

この質的調査の目的は、後述の私立大学機関 K の CSIRT 職員を対象に質的調査を行う前に、大学機関におけるセキュリティの現状や業界での立ち位置について把握し、事前分析することであった。そのため質的調査は、組織におけるセキュリティを取り巻く現状や CSIRT やセキュリティ対策が始まった歴史的な経緯についてのテーマを中心に掘り下げた。

その後、企業と大学機関における考え方や判断の仕方の傾向にどのような違いがあるかを質問し、私立大学機関のケースが持つ特殊性や他の組織に事例を適用する際の制約を探った。この際、私立大学機関 K における具体的な組織構造や、内部の部署間のパワーバランス、部署ごとにどのような考え方の違いがあるかについて重点的に質問し、それが組織全体のインシデント対応にどのような影響を与えているかを明らかにした。

前提

- U氏、T氏への過去のインタビューを通じてゴール群を整理し、それを基に、U氏がどのゴールに特にご関心があるかを伺いました。その結果、クライアントがP社の提供するもののどこにバリューを感じるのかが分かるとありがたいという話をいただきました。
- そこで、私立大学機関KのITCはリーディングカンパニーではないですが、リーディング私学のセキュリティチームとしてお話を伺い、参考にすることができるのではないかという話になりました。P社の現時点でのクライアント企業には、リーディングカンパニーにおけるリスクマネジメントやセキュリティ管理を担う方々が多いので、同じリーディング組織の関連領域のチーム同士の比較を行うということを前提としたものです。その上で質問なのですが・・・

質問

- 私立大学機関KのITCに限らず一般的な話として、大学機関で働くセキュリティチームの方々は、セキュリティ業界の中でどういう立ち位置の方が多いでしょうか？（どういう経緯でどういうモチベーションで働いていらっしゃる方が多いのか、そもそも私立大学機関K ITCの人数や規模はどのくらいなのか）
- リスクマネジメントが対象とするリスクには様々なものがあると思います。例えば大学機関がリスクを認識する中で、セキュリティに関してはどのような認識でいるのが一般的だと思われますか？セキュリティを重視したり優先したりなど、リスク全般に占めるセキュリティのウェイトは重いと思われますか？
- ここまで私立大学機関KのITCについて伺ってきましたが、殊これをP社側の領域に話を広げようとする場合、P社の現時点でのクライアント企業と私立大学機関K ITCの、リスクに対する考え方、セキュリティに対する考え方にはどのような違いがありそうですか？
- 時間があれば：過去に発生したインシデント然り私立大学機関KのITCのセキュリティチームの対応はしっかりしている印象なのですが、他の単科大学とかになると事情はまた異なってくるものなのでしょうか？

図 3.25 私立大学機関 K セキュリティ専門家への質問リスト

3.3.3 質的調査：私立大学機関 K CSIRT 職員

2022 年 12 月 6 日、S 氏への質的調査を基に実施した事前分析を携え、私立大学機関 K CSIRT 職員 H 氏を対象に質的調査を行い、その内容を基に分析を行なった。質問リストは以下の図 3.26 に示した。この質的調査の目的は、クライアント側のケースとした私立大学機関 K が抱える課題や組織内部の価値観や文化、制度を明らかにし、コンサルタントが理解しやすい図表を作成することであった。

半構造化インタビューの形で実施した質的調査は、S 氏への質的調査の結果作成した組織構造や部署ごとのより詳細な人数などの整合性について確認することから始まった。また、CSIRT の設立経緯や H 氏自身がその中でどのような役割を担ってきたか、そして部署ごとに生じる価値観の違いの傾向やその背景について深掘りした。さらに、セキュリティインシデント対応とその予防に関わる機能を CSIRT として組織化する以前と以後で、インシデント対応やセキュリティ態勢の強化にどのような変化が生じたのかを質問し、CSIRT がもたらす役割について鮮明化することを試みた。

質的調査の終盤では、過去に私立大学機関 K の SF 地区で発生したセキュリティインシデントを具体的なケースとして例示し、インシデント発生時にどの時点でどの部署が問題を発見し、各部署がどのように対応したのか、どの時点で経営層に報告したのか、そして得られた教訓を基にどのような事後対策を打ったのか、などを深掘りした。

以上の私立大学機関 K を代表ケースとした二回にわたる質的調査の内容を文字起こしし、S 氏と H 氏の両名の発言記録から、組織内部の部門構造、その考え方の違い、所属するアクターの経歴や背景に関わる詳細、インシデント発生時の具体的な動き、態勢強化に向けた変化、そしてそれを踏まえた H 氏の組織に関する考察などについての情報を抽出した。今度は抽出した情報を Miro ボード上に枠や矢印を用いて配置し、私立大学機関 K の文化や制度を可視化する図表を作成した。これを図 3.27 に示す。なお、この図 3.27 を、本研究における最初のバージョンの初期プロトタイプ「プロトタイプ v1」とし、後に価値検証で用いた。

導入的な質問

- 軽く経歴の自己紹介をお願いできますでしょうか
- 最初、セキュリティ領域にご関心を持ち始めたそもそものきっかけは何でしたか？現職に就かれたきっかけは何でしたか？
- 今回のインタビューにあたって、CSIRTと私立大学機関KのITCに関する前提情報はいくらか私立大学機関K大学院のセキュリティ専門家の方にお伺いしました。その上で長年私立大学機関KのITC・CSIRTを率いて来られたHさんに質問なのですが、まずCSIRTが存在する組織とない組織の違いはどんなところに現れてくると思われますか？
- 逆に、思いきってCSIRTの組織を作ってはみたは良いものの、実態を伴わなかったりする例もあるのでしょうか？
- CSIRTの連合であるNCAに加盟することは、どんな意味を持つのでしょうか？どんな違いやメリットを生み出すのでしょうか？組織内にCSIRTは存在しているものの、NCAに加盟していない状態というのはどんな状態なのでしょうか？
- NCAは情報共有を目的の一つとしていると伺いました。NCA加盟組織間で行われる情報共有の内容とは、何でしょうか？

大学機関全般のセキュリティ業務上の理念や行動原理に関わる質問

- 組織としてのミッション・達成すべきゴールと、Hさん個人として現在与えられている役割上のミッションをそれぞれ教えていただいてもよろしいでしょうか？
- その目標を達成するために、現状で何かしらのKPIを立てていらっしゃいますか？
- 私立大学機関KにCSIRTがなかった時代とある時代で、Hさんのインシデントの対処の仕方に何か変化は生じましたか？

ケース別

- ここからはより具体的に、何かインシデントやイベントが起こった際に、私立大学機関KのITCの組織やHさん個人がどんな風に考え行動したかの「判断」の部分について理解するための質問をお伺いします。インシデントを取り上げて喋れる範囲で、公開されているもので構いませんので、教えていただけると幸いです。例として、SFC地区の学生情報、顔写真、教員情報など数千件が漏洩したインシデントがあったかと思います。
- どんな判断がございましたか？

私立大学機関KのITCに関する外形的な質問

- 私立大学機関KのITCの各キャンパスの組織ごとに考え方の違いはありますか?
- 私立大学機関KのITCが普段リスクマネジメント業務を行う中で、どのようなリスクを主に対象としていらっしゃいますか?それらのリスク群の中で、セキュリティ対策はどのような位置付けですか?

図 3.26 私立大学機関 K CSIRT 職員への質問リスト

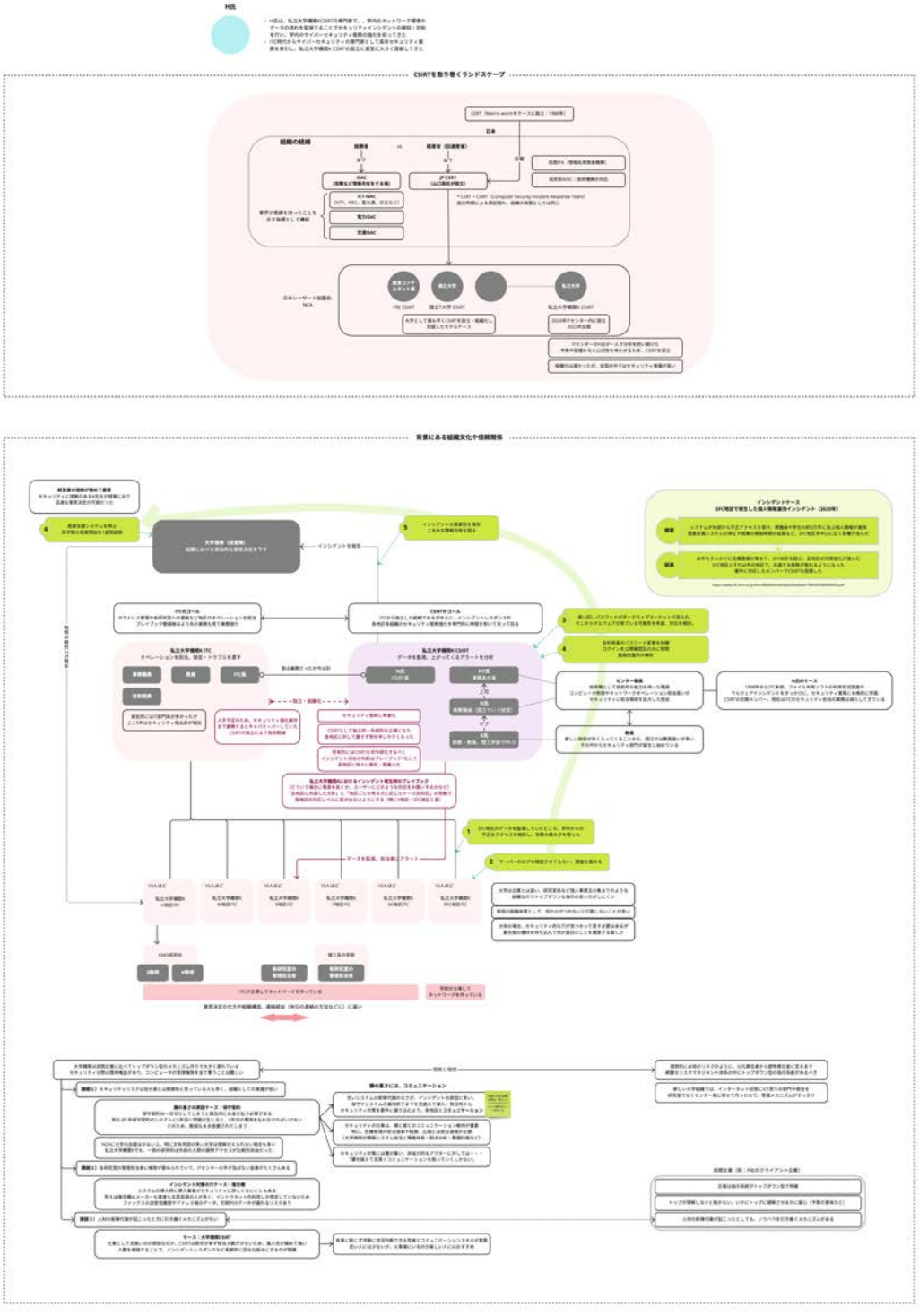

図 3.27 プロトタイプ v1：私立大学機関 K の文化と制度の可視化図

3.3.4 プロトタイプ v1：私立大学機関 K の文化と制度の可視化図

私立大学機関 K の組織構造や考え方を示す図表

図 3.27 は、私立大学機関 K の CSIRT を取り巻くランドスケープ、私立大学機関 K 内部の組織の考え方や関係性およびその背景にある組織の文化や歴史的経緯、そして私立大学機関 K が抱える課題の三点から構成されている。

一つ目の CSIRT を取り巻くランドスケープの歴史的経緯は、図 3.28 に示した。日本で急速に広まった CSIRT 組織を束ねる存在として日本シーサート協議会が設立され、コンサルティングファームや大学機関など自前の CSIRT を持つ組織が次々に加盟した。私立大学機関 K は CSIRT の設立は 2020 年と若干遅れたが、全国の中ではセキュリティ意識が高い組織であり続けたきた。

二つ目の私立大学機関 K 内部の文化と歴史的経緯に関しては、図 3.29 に示した。元々、私立大学機関 K における情報関連の業務全般は長年 ICT が担ってきており、業務の一部として六つある各地区のデータを監視したり、セキュリティ上の危険性に関してアラートを発出する役割を担ってきた。私立大学機関 K では地区ごとに考え方の違いがあり、これは学部主導でネットワークを構築した SF 地区と ITC が主導したその他の五地区では、意思決定の仕方や組織構造、あるいは連絡の手段や系統に違いが出てくるということである。

また、私立大学機関 K の各地区は元々企業とは異なり、研究室長などはある種の個人事業主のような風土を持ってきたためにトップダウン型の指示が言いにくい気風があった。それゆえ組織内にどんな機材があり誰が管理しているのかを把握、指摘しにくいといった課題があった。ところが近年、CSIRT が設立され ITC から独立すると、ITC と CSIRT のゴールにそれぞれ明確な違いが見られるようになった。ITC は従来の情報関連の業務全般のオペレーションを遂行し、各地区の各研究室への連絡などを担うものの、セキュリティ態勢強化の案件は減らしつつある。その反面、CSIRT はデータの監視やアラート、インシデントレスポンスなどの業務に専業化するようになり、独立的・外部的な立場から各地区に話を通しやすくなった。

さらに私立大学機関 K の CSIRT は将来を見据え、インシデントが実際に発生した際の判断や初動の NG 例をプレイブック化することに取り組んでいる。ここで

言うプレイブックとは、例としてインシデント発生時にどのような場合にシステムの電源を抜くか、あるいはどういう場合に抜いてはいけないのかなど、ケース別にユーザーにお願いするべき対応を明記したマニュアルである。こうしたプレイブックには、全地区に共通した方針と、地区ごとの考え方に応じたケース別対応の両面が含まれている。こうすることで、CSIRT 内部の限られた専門家が担っている業務の属人性を排し、各地区の対応レベルに差が出ないようにすることが可能となる。特に理工系の Y 地区と SF 地区は意識向上や対策が進んでいるものの、その他の地区は出遅れたため、足並みを揃えることに取り組んでいる。

またもう一つ重要な観点は、私立大学機関 K においてセキュリティ上の問題が生じた際に意思決定を行うのは、大学の経営層すなわち理事だということである。実際には大学理事が ITC や CSIRT から上がってくるインシデントの報告に基づいて休講やシステム停止などの措置を決定し、各員に通達する仕組みになっている。

以上を踏まえ、この図 3.29 には、SF 地区で発生した個人情報漏洩インシデントのケースを具体例として、私立大学機関 K 内の各部署がどのように対応を行なったかの事例を可視化した。このインシデントは 2020 年に SF 地区のシステムが外部から不正アクセスを受け、教職員や学生の約 3 万件に及ぶ個人情報が漏洩した事件である。

当時セキュリティ対策業務を担っていた ITC が、SF 地区のデータを監視していたところ、学外からの不正なアクセスを検知した。その後、サーバーのログを精査し調査を進める中で、攻撃と情報漏洩の規模の重大さを認識した。ITC は、特に使い回されたパスワードがダークウェブマーケットで売られ、その脆弱性を踏んでマルウェアが学内のシステムに侵入している可能性を考慮し、対応を急遽検討した。その結果、全利用者のパスワード変更を依頼し、学内システムへのログインを公開鍵認証のみに制限し、脆弱性箇所の解析を行なった。

この時、ITC が特に腐心していたのは大学経営層との密な情報連携である。インシデントの重要性を報告したあと、結果的に大学理事は授業支援システムの停止を決定し、秋学期の授業開始は一週間延期することを各員に通達した。ここで迅速な意思決定が可能だったのは当時の大学理事に、セキュリティに関する一定の理解があったからだと考えられる。この件をきっかけに被害地区を超え他地区

でも対策強化に進展が見られ、SF 地区とそれ以外の地区で共通した態勢が取れるようになり、事件に対応したメンバーによって CSIRT が設立された。

図 3.30 には、こうしたインシデントのケースに浮き彫りになった私立大学機関 K の課題を示した。質的調査の内容を元に、整理した現状の課題は三点である。

一点目は、セキュリティリスクは自分達とは無関係と思っている人も多く、組織としての意識が低いという点である。2020 年のインシデントを経ても部分的にはまだ意識改革が進んでおらず、セキュリティ対策強化に乗り出す上で腰が重いケースがある。その原因の一つとして、保守契約が挙げられる。保守契約は一旦切らしてしまうと遡及的にお金を払う必要があるため、例えば 1 年保守契約のシステムに 5 年目に問題が生じると、5 年分の費用を払わなければいけない。そのため、脆弱なまま放置されてしまうのである。こうした例では、保守やシステムの運用終了までを見据えて導入・発注時からセキュリティ対策を要件に盛り込むよう、各地区とコミュニケーションを取る必要がある。腰の重いアクターを動かすにはコミュニケーションが鍵だと考えている私立大学機関 K の CSIRT では、泥臭く周知を図っていく努力を続けている。

二点目は、各研究室の管理者に装置の権限が委ねられており、IT センターの手が及ばない装置が多くあるという点である。その例の一つに複合機があり、システムの導入業者がセキュリティに疎く、現場の管理者が脆弱なシステムを導入してしまう問題がある。具体的には、複合機メーカーにおける文房具業界出身の業者がイントラネット内利用の想定で複合機を導入し、ファックスの送受信履歴や印刷 PDF データが漏洩する、などのケースがある。

三点目は、人材の新陳代謝が起こったときに引き継ぐメカニズムがない点である。セキュリティ業務は仕事として泥臭いのが原因なのか、CSIRT は若手が来ず担当人数が少ないため、属人性が極めて強い。人数を補強することで、インシデントレスポンスなど長期的に回る仕組みにするのが課題である。

以上、私立大学機関 K の CSIRT を取り巻くランドスケープ、私立大学機関 K 内部の組織の考え方や関係性およびその背景にある組織の文化や歴史的経緯、そして私立大学機関 K が抱える課題の三つの要素が統合され構成されることで、クライアント組織の文化と制度を可視化する図表を作成した。

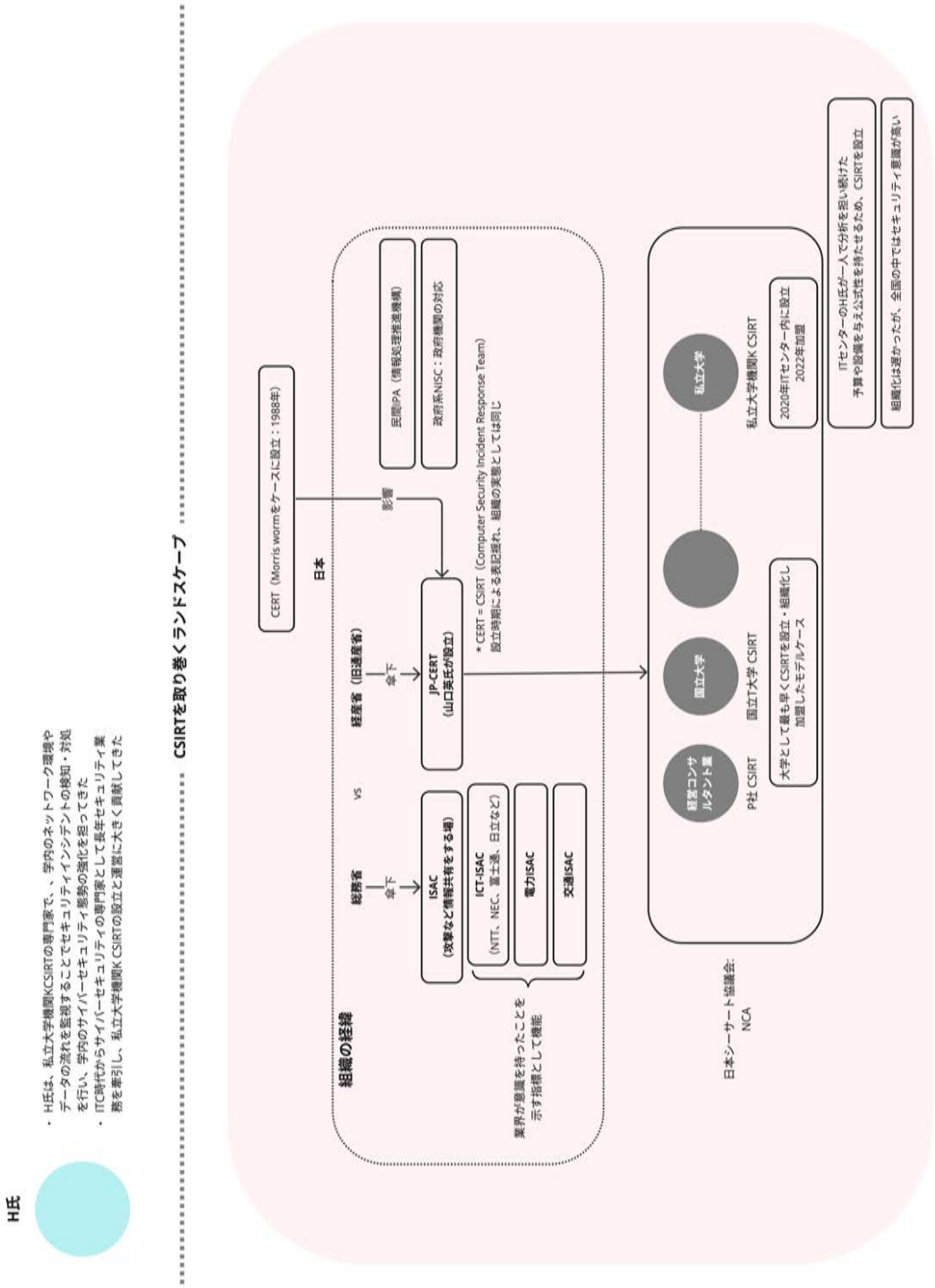

図 3.28 クライアントケース：CSIRT を取り巻くランドスケープ

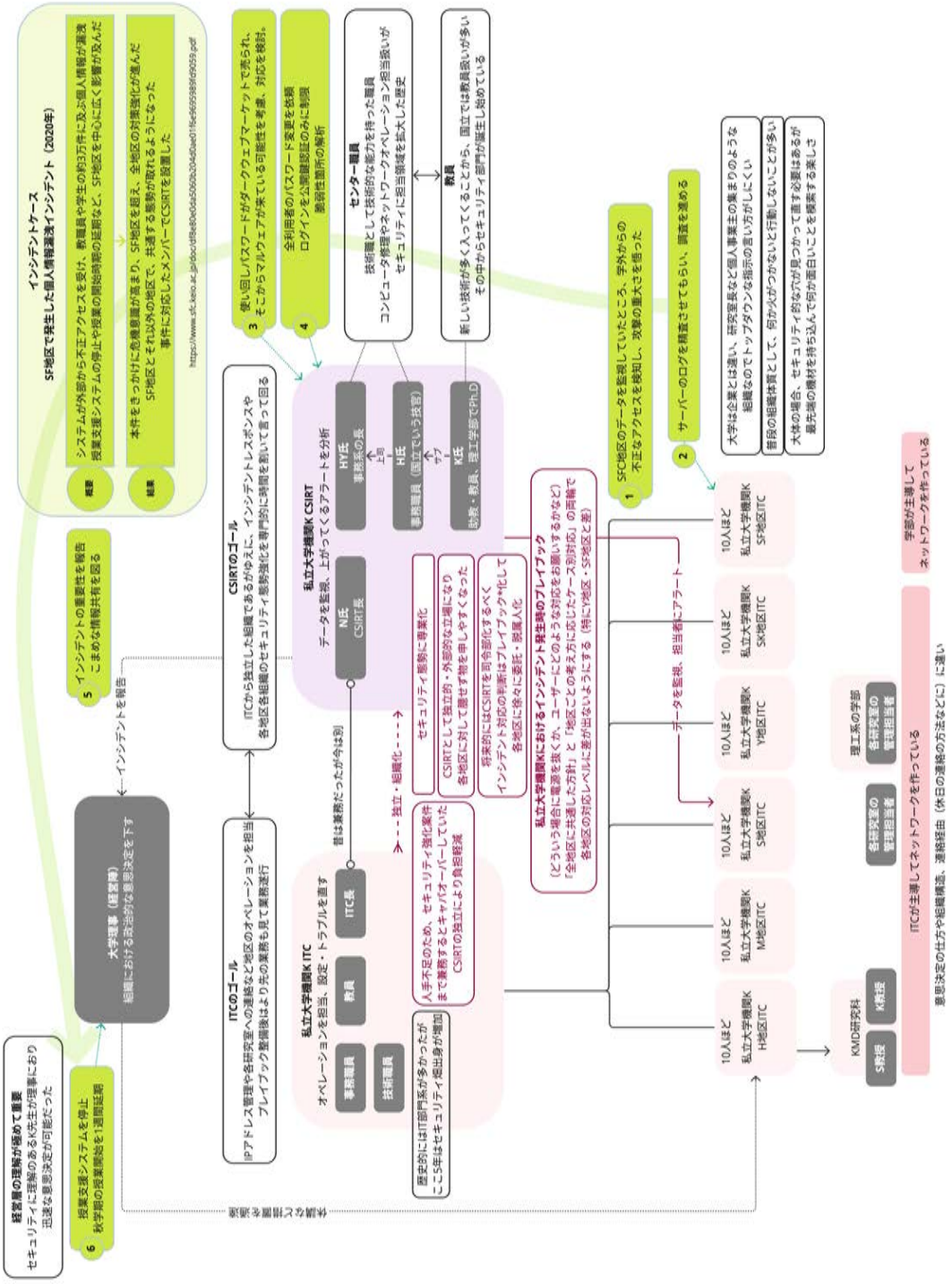

図 3.29 クライアントケース：背景にある組織文化や信頼関係

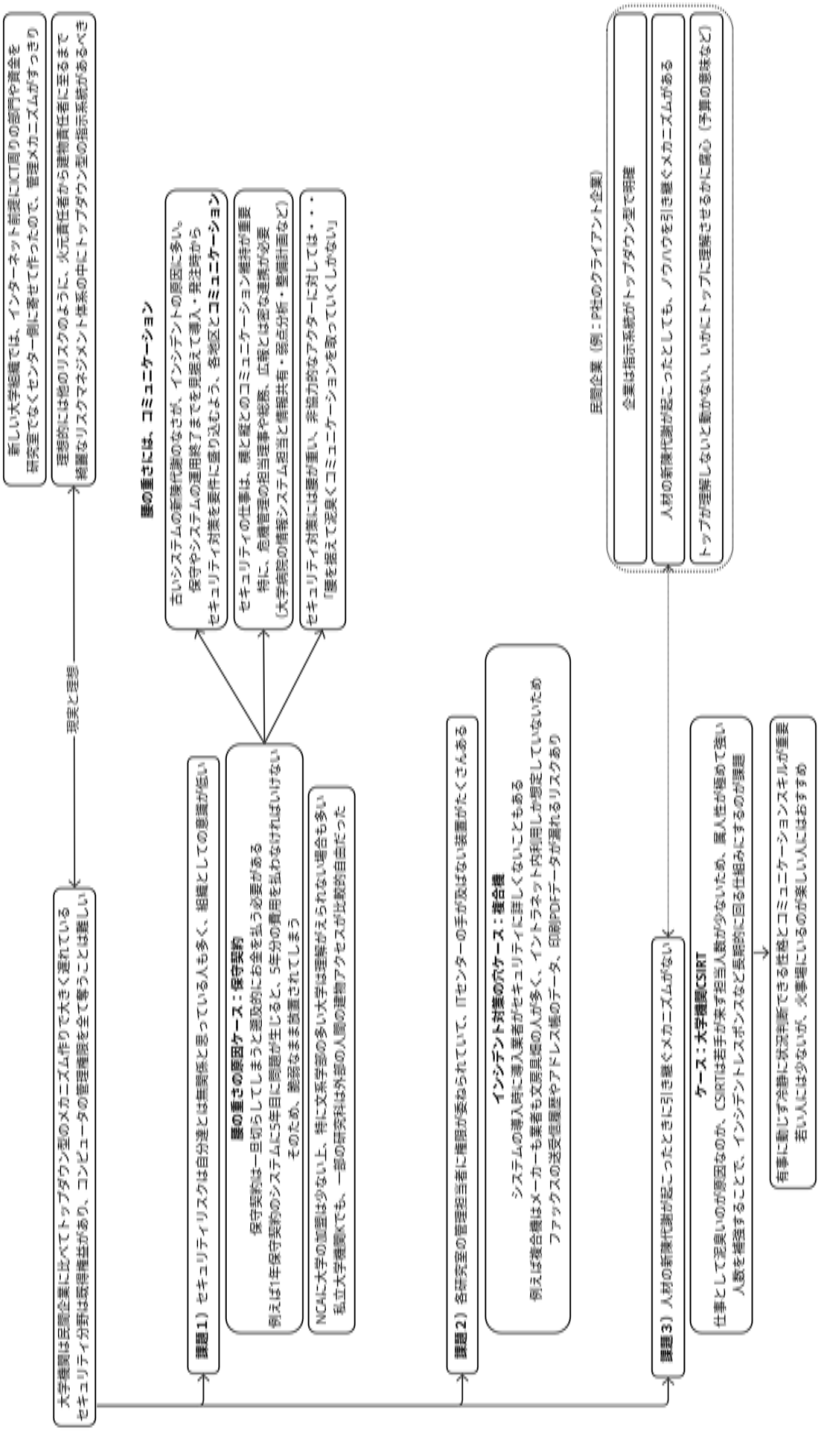

図 3.30 クライアントケース：組織の抱える課題

私立大学機関 K におけるゴールとメンタルモデル

図 3.31 には、ここまでの分析を通じて抽出、解釈されたクライアント組織のゴールとメンタルモデルについて示した。私立大学機関 K では、第一線である現業部門と、第二線・第三線である間接管理部門・内部監査部門はそれぞれ異なるゴールを持っており、CSIRT はその両方に働きかけを行う立場にある。

第一線では、「現場で発生する、業務に支障をきたすような様々な問題を解決してしまいたい」という上位ゴールがある。その下に複数の中位ゴールがあり、うち一つは他組織で起きたインシデントに危機感を募らせて対応能力を高めたい、上層部がガバナンスの観点から態勢強化を指示してきたので対処したいといった、外圧に対応したいというゴールである。もう一つはインシデント発生時に対応を急ぐ現場における「情報の流出など機会損失が出るので一刻も早く解決したい」というゴールで、それには極力少ない工数で手短に自分達の考え方・価値観を汲んでほしい、外部の意見がほしいといった下位ゴールが付随する。

それに対し地区や部署によっては異なる反応を示す場合もあり、例として外圧があっても優先事項に見えないので普段のことを超えた仕事は極力したくないといったものである。この場合、他の組織がインシデント攻撃を受けても関心を抱かない、普段の業務に集中するといった行動に繋がり得る。あるいは、インシデントで問題が発生すると人事評価に関わるかもしれないので、報告せずにことなきを得たいといった消極的なゴールも挙げられる。

次に、第二線・第三線に関しては上位のゴールに、「組織のガバナンスのため、長期的に組織のセキュリティ態勢を強化したい」というものが挙げられる。エスノグラフィーの段階で PwC 側のコンサルタントが経験したケースとして「極力安いコストで済ませてしまいたい」というゴールを持つアクターもいると指摘したが、私立大学機関 K の場合、H 氏に把握されている範囲ではこれは該当しない。また平時のセキュリティ態勢を強化することで、インシデントが発生する可能性を下げたい、といった中位ゴールには、いくつかの下位ゴールが付随する。

一つは予防的なセキュリティ態勢の強化について、どこから手をつけたら良いかわからないので第三者に指針を示してほしいというものである。私立大学機関 K の場合、CSIRT と密に連携している部門はどの機材をどう管理し、どのように

セキュリティレベルを上げるかということについて道筋がついている。しかしながら部署によっては、何から手をつけたら良いかわからない、場合によってはそもそも誰に依頼したら良いかすらわからないといった下位ゴールを持っている場合がある。(なお、こういったゴールを持つアクターに対し、サイバーセキュリティコンサルティングは行動指針を示す余地がある)。それに加えて、様々な部門が色々な機材を持ち込み保守の契約もできていないため、問題を解決したいといったゴールも質的調査の内容から観測された。

さらに有事の際に現実的に動くレベルのセキュリティレベルを整えておきたい、そのためにインシデントレスポンス能力を高めておきたいといったゴールも挙げられる。これは一方で組織内部の自由を束縛しすぎることなく、適度にセキュリティを強化したいという大学機関ならではのゴールと相反する場合もある。これには隠された意図もあり、組織内部の自由を束縛しすぎた結果、ユーザーが抜け道を探して問題が裏に潜ってしまうのを防ぎたいということが挙げられる。こうした考えが色濃く表出する部署に関しては、部署それぞれの価値観を尊重した上でセキュリティ担当者によるセキュリティ強化のための説得が欠かせない。

以上が、私立大学機関 K のセキュリティ専門家と CSIRT 職員に質的調査を実施した結果、得られたクライアント側の価値観のケースである。本研究ではここまでの時点の図表「プロトタイプ v1」を用いて、CSIRT 研究家に対し価値検証を行った。これを後述の第 4 章、価値検証の項目で詳しく論じる。価値検証では、本プロトタイプが発揮すると想定した価値の実際や予期しなかった価値の有無を検証するに留まらず、このプロトタイプの抱える制約や改善のためのフィードバックも取得した。そのフィードバックに基づいて作成した第二バージョンの図解が「図解ハンドブック」であり、これが本研究における最終的な成果物であり、本章次節の最終成果物の項目で詳述する。したがって本来のデザインと検証の工程に則れば、時系列はデザインプロセス→価値検証→最終成果物であるが、本稿の構成上、最終成果物について先に述べる。

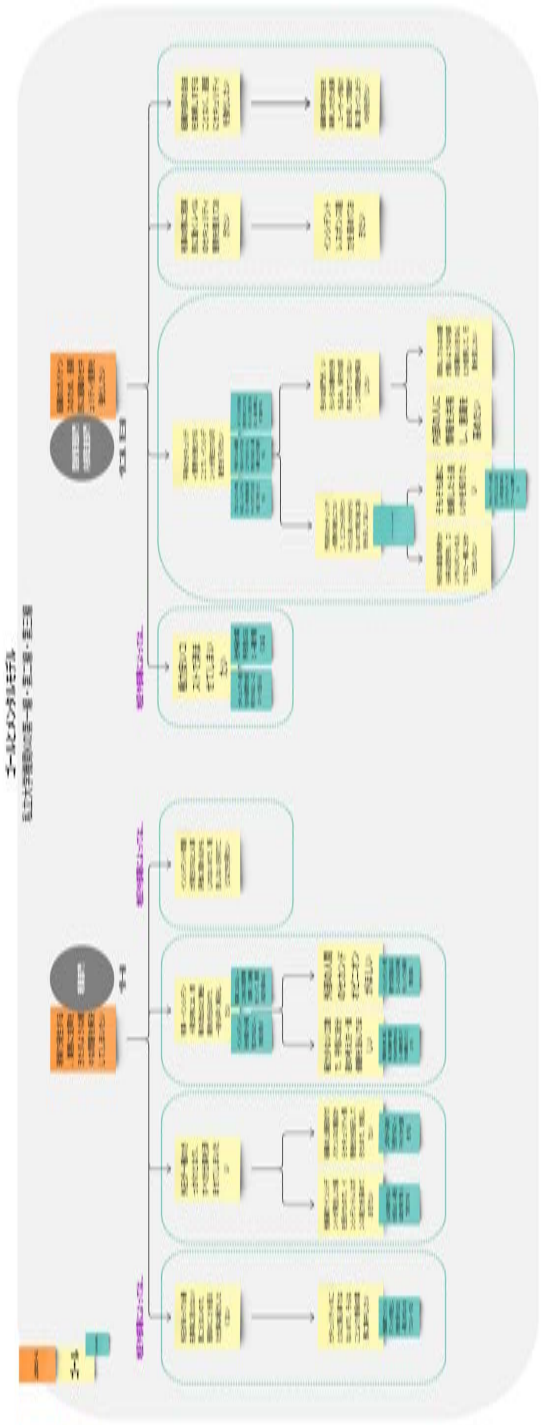

図 3.31 クライアントケース：ゴールとメンタルモデル

3.3.5 質的調査：CSIRT 研究家

2022 年 12 月 6 日、CSIRT 研究家の Y 氏を対象に質的調査を行い、その内容を基にクライアントの代表的なケースについての分析を行なった。この質的調査の目的は、多くの企業のセキュリティ態勢を俯瞰的に見てきた Y 氏を対象に調査することによって、私立大学機関 K に留まらず他の様々な組織における課題や組織内部の価値観や文化、制度を明らかにすることである。

質的調査は半構造化インタビューの形で実施し、組織ごとのセキュリティに対する考え方には具体的にどんな違いがあるか、何がその考え方の違いを生むか（日本の慣習的な文化由来なのか、業種や組織特有の文化由来なのか、個人の考え方由来なのか）などについて掘り下げた。

Y 氏はまた過去に発生したインシデントの事例や企業におけるセキュリティ態勢上よくあること（例：歴史的に品質保証部門の発言権が強いなど）について多く例示した。特に例として指摘したインシデントは、2014 年にベネッセグループで発生した個人情報流出事件[3]と 2019 年にセブンペイ QR コード決済サービスで発生した不正アクセス事案[4]である。Y 氏はそれぞれの企業におけるインシデント発生の原因や、どの側面を教訓として見るべきなのか、今後同じようなインシデントを予防するために重要となるセキュリティ対策は何か、などについて指摘した。

そこで質的調査後、更新版である図解ハンドブックの一部として、ベネッセグループとセブンペイにおけるインシデントケースを扱うこととし、図解作成にあたっては Y 氏が指摘したポイントを主に盛り込んだ。また、インシデント発生時および発生後の組織の構造や対応など一般に公開されている範囲については、インシデントに関連するプレスリリースなどを参照した。そのようにして抽出した情報を Miro ボード上に枠や矢印を用いて配置し、クライアントの代表ケースの文化や制度を可視化する図表を作成した。これを図解ハンドブックとして価値検証に用い、最終的に完成したもののを最終成果物の節にて詳述した。

---

3 ベネッセ個人情報流出事件, https://www.benesse.co.jp/customer/bcinfo/01.html, 2023 年 1 月 14 日参照

4 セブンペイ不正アクセス事件, https://www.7andi.com/company/news/release/201908011500.html, 2023 年 1 月 14 日参照

3.4. 最終成果物：図解ハンドブック

3.4.1 ケーススタディ型の図解

「組織のセキュリティ態勢・図解ハンドブック」を構成する最初の要素は、ケーススタディ型の図解である。これは、S 氏と H 氏への質的調査を通じて作成した私立大学機関 K に関する図解（図 3.32 と 3.33）、Y 氏への質的調査を通じて作成したベネッセに関する図解（図 3.34）、そしてセブンペイに関する図解（図 3.35）の四つのページから構成される。読み手はこれらの図解を見ることで、インシデント発生時に組織の部署がどのように対応したのか、インシデント対応において何が失敗だったのか、得られた教訓を基にどのような事後対策を打ったのか、を一覧で把握することができる。

読み手はまず、図 3.32 に示した私立大学機関 K に関する図解の一ページ目のヘッドラインを見ることで、私立大学機関 K が業界においてどのような立ち位置にあり、組織における重要人物がセキュリティ部署を CSIRT や牽引してきた経緯を把握することができる。またヘッドラインからは過去に発生した個人情報漏洩インシデントの概要について知ることができる。次に図解を見ると、組織内の部署など全体の組織構造とアクターの顔ぶれを俯瞰することができる。次に図表上の箱を繋ぐ矢印から部署やアクター間の関係性を把握し、吹き出しを見て、それが指し示す部署やアクターの考え方や補足事項の詳細を知る。その後、紫の導線に沿って過去のインシデントケースをたどり、各部署がどのように判断でどう行動したかを把握し、インシデント対応から得られる教訓について学ぶ。最後に、青色の箱・外枠・矢印・線に視線を移すと、これらはインシデント発生の経験を経て組織が行った組織変革やセキュリティ態勢強化のための施策の内容について把握する。

その後、図 3.33 に示した私立大学機関 K に関する図解の二ページ目を開くと、特集ページのように記載された CSIRT 担当者の視点で見る私立大学機関 K の課題というタイトルを目にする。そしてヘッドラインから、このページがクライアント組織における「腰の重さ」の正体や原因を私立大学機関 K をケースから紐解くのだということが見て取れる。その後、下に記載されている図解に目をやると、

腰の重さの原因となっている三つの課題がすぐに把握でき、過去に発生したケースの解説とともに具体的に知ることができる。以上の要素が私立大学機関 K に関する図表である。

図 3.34 に示したベネッセや図 3.35 に関するケーススタディ型の図解も、同じ要領で読むことができる。図 3.34 のベネッセの例では、紺色の左枠に記載されたヘッドラインを確認し、何がポイントになっているのかの要約と解釈について一覧で把握できる。この例では、外部委託の業者選定の際に、有事の行動や責任の分担までを見据えた契約や法務手続きができていなかった点や、記者会見の質疑応答時に謙虚な姿勢を示せなかったことで批判を浴びた点について知り、教訓を得ることができる。またベネッセはインシデント後に組織を再編し、全従業員への研修やオフィスの入退室管理を徹底するなどセキュリティ態勢を大幅に強化したことから、教訓を糧にどのような事後対策を取ったかを把握することができる。さらにヘッドライン下のハイパーリンクからは、組織のセキュリティ態勢に関わるより詳細な情報を入手できる。そして図解に目をやると、紫色の枠からはインシデントへの各部署の対応や失策について、青色の枠からはインシデント後に、情報漏洩を起こした組織内部署がいかに解体され、顧客データベースの保守・運用事業がセキュリティを強化された別会社に移管され、本社で組織化した CSIRT がどう活動しているかなど時間的な変化を伴う組織構造の動きについて、図表から一覧して知ることができる。

図 3.35 についても内容は異なるものの図表の表記ルールは統一されているため、全く同じ要領で読むことができる。左枠のヘッドラインや図解からは、子会社側のセブンペイが親会社側にすぐに報告を上げずコミュニケーションの不足が失敗を招いてしまった点や CSIRT を有する親会社セブン＆アイ・ホールディンスがグループ全体を管理するガバナンスに欠陥があった点などのポイント、そしてその後の事後対策として日頃のリスク対応訓練を強化した点を知ることができる。

最終成果物となった図解ハンドブックでは、三つの組織に関するケースを扱ったが、これを同じ表記ルールで他の組織にも拡張することで、クライアント側が抱える課題や組織内部の価値観や文化、制度に関する複数のケースをわかりやすく把握するという経験を読み手に提供する。

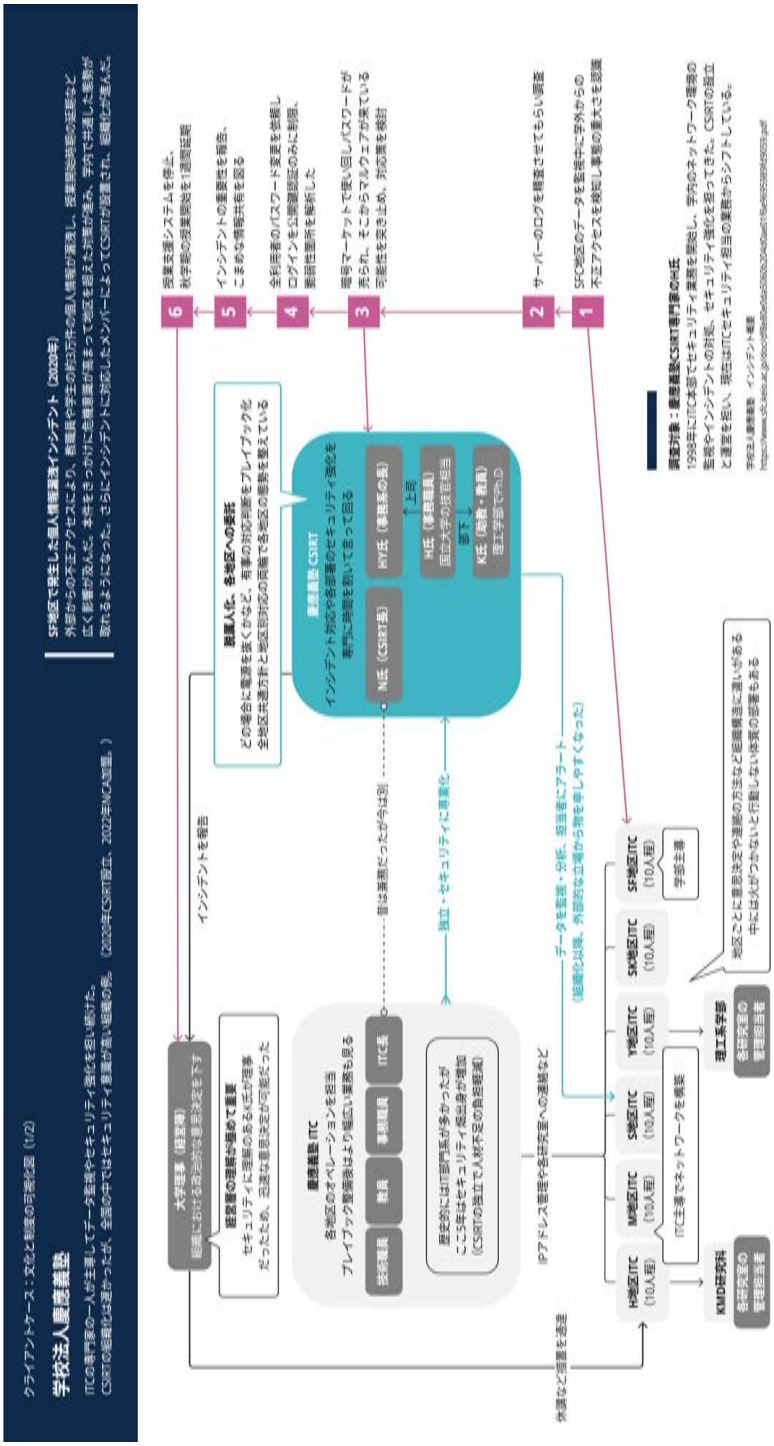

図 3.32 ケーススタディ型の図解：私立大学機関 K 1/2

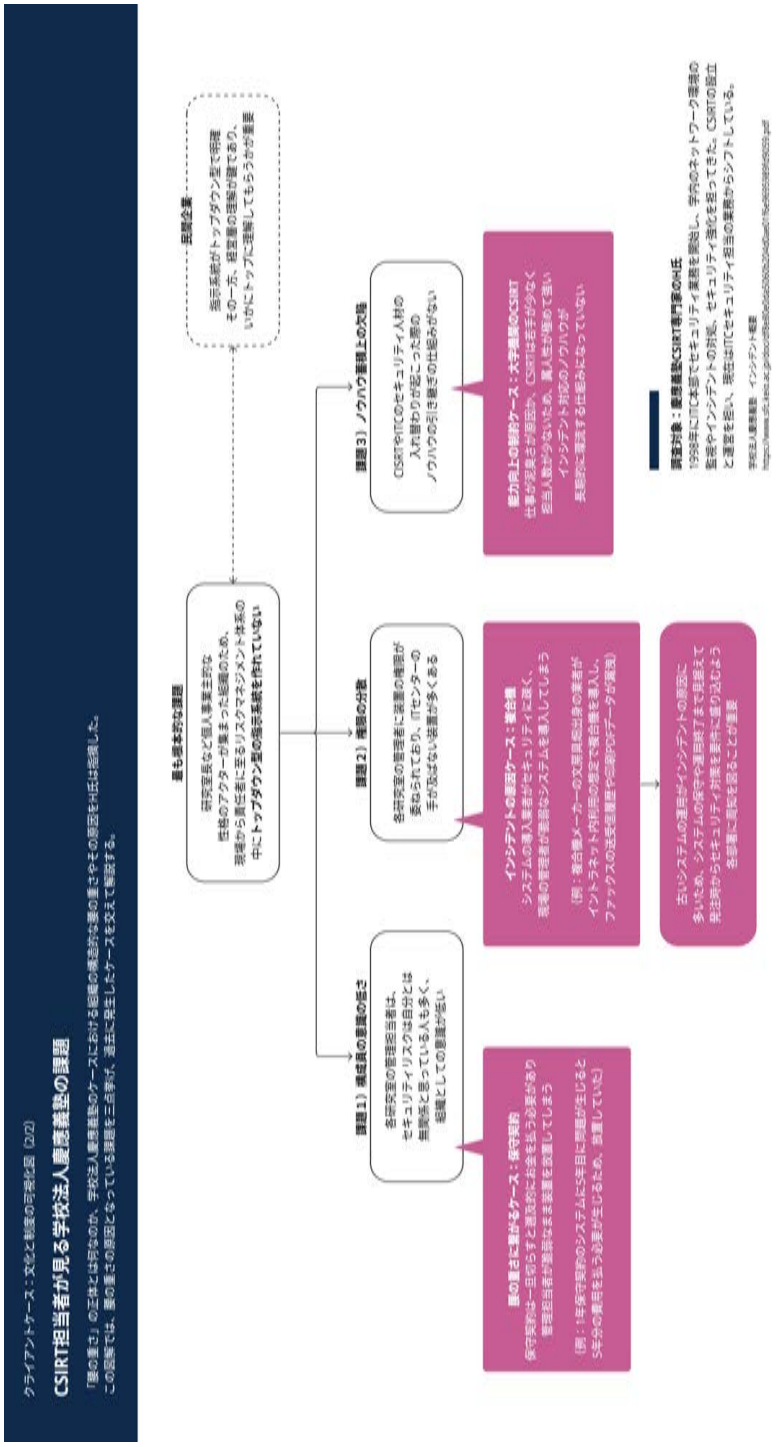

図 3.33 ケーススタディ型の図解：私立大学機関 K 2/2

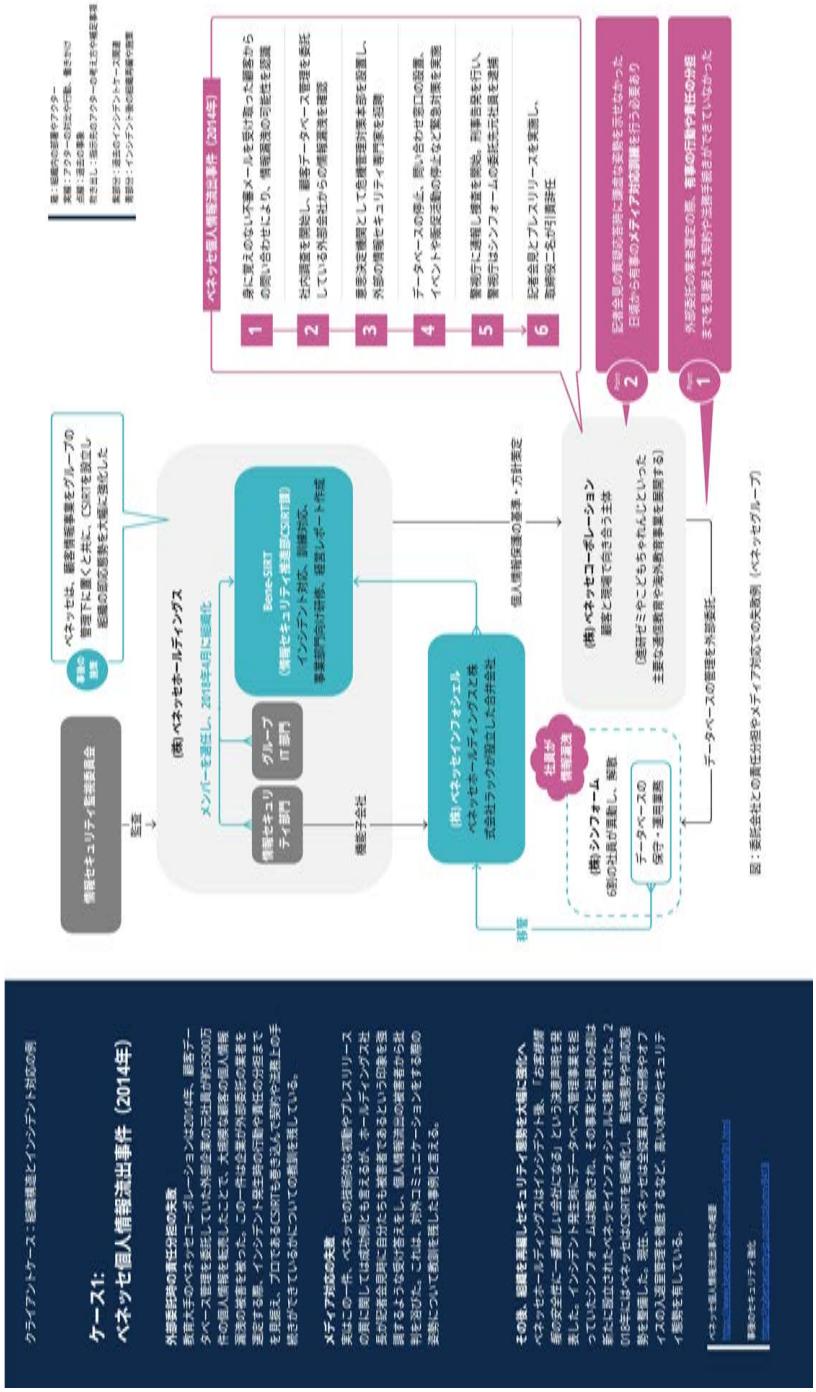

図 3.34　ケーススタディ型の図解：ベネッセ

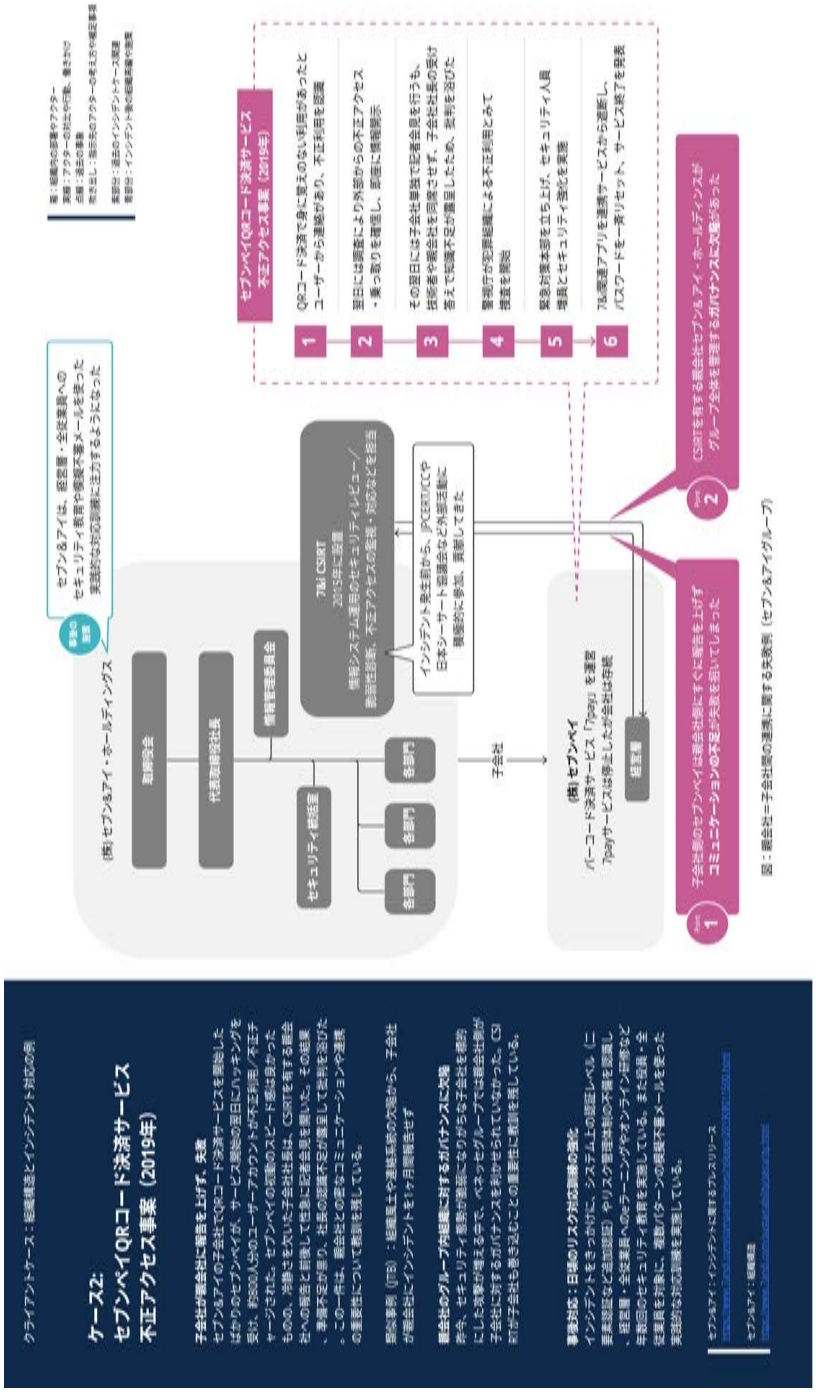

図 3.35 ケーススタディ型の図解：セブンペイ

3.4.2 README

「組織のセキュリティ態勢・図解ハンドブック」を構成する二つ目の要素は、図3.36 に示した README である。これは、読み手が図表を読み解くための取り扱い説明書、表記ルールについての読み方ガイドとして機能する。

README では、図解を簡略化した図から虫眼鏡のように指示された矢印を辿り、どのような順序で図表を読み解くべきか番号が振ってある。読み手は番号に沿って上から順に見ることで、図表の読み方を知ることができる。複数のケースに関して表記ルールを統一してあるため、読み手はこの README を図解ハンドブックの最初に読むことで読み方をまず把握し、その上でケーススタディ型の図解を読み解くことできる。

3.4.3 図解作成の手引き書

「組織のセキュリティ態勢・図解ハンドブック」を構成する二つ目の要素は、図3.37 に示した図解作成の手引き書である。この図表は、組織内部の文化や制度を明らかにするための質的調査手法・分析手順自体を、料理レシピのように体系的にフローチャート化した手引き書である。この図解ハンドブックのフローチャートには 20 の工程があり、読み手はどのようにして質的調査を行い、分析を行い、それを基に図解を作成するかの手順を簡単に学ぶことができる。

手引き書の 20 ステップは、A) 質的調査前の事前調査、B) 対象への質的調査、C）図解の作成の三つの構成に分かれている。質的調査に関わる箇所には、クライアント組織の背景を理解するために行うべき質問例を用意してあり、すぐに現場で使用できる。また図解を作成するための統一された表記ルールと作成方法を詳細に順を追って示してあるので、読み手は図表の作成を再現することができる。さらに質的調査の対象組織の CSIRT 設置有無で場合分けをしており、読み手は対象の事情に応じて調査すべき事項を柔軟に変更できる。読み手はこの手引き書を参考に、自分自身で質的調査を行い、長期的にクライアント組織の価値観を把握するのに役立てることができる。

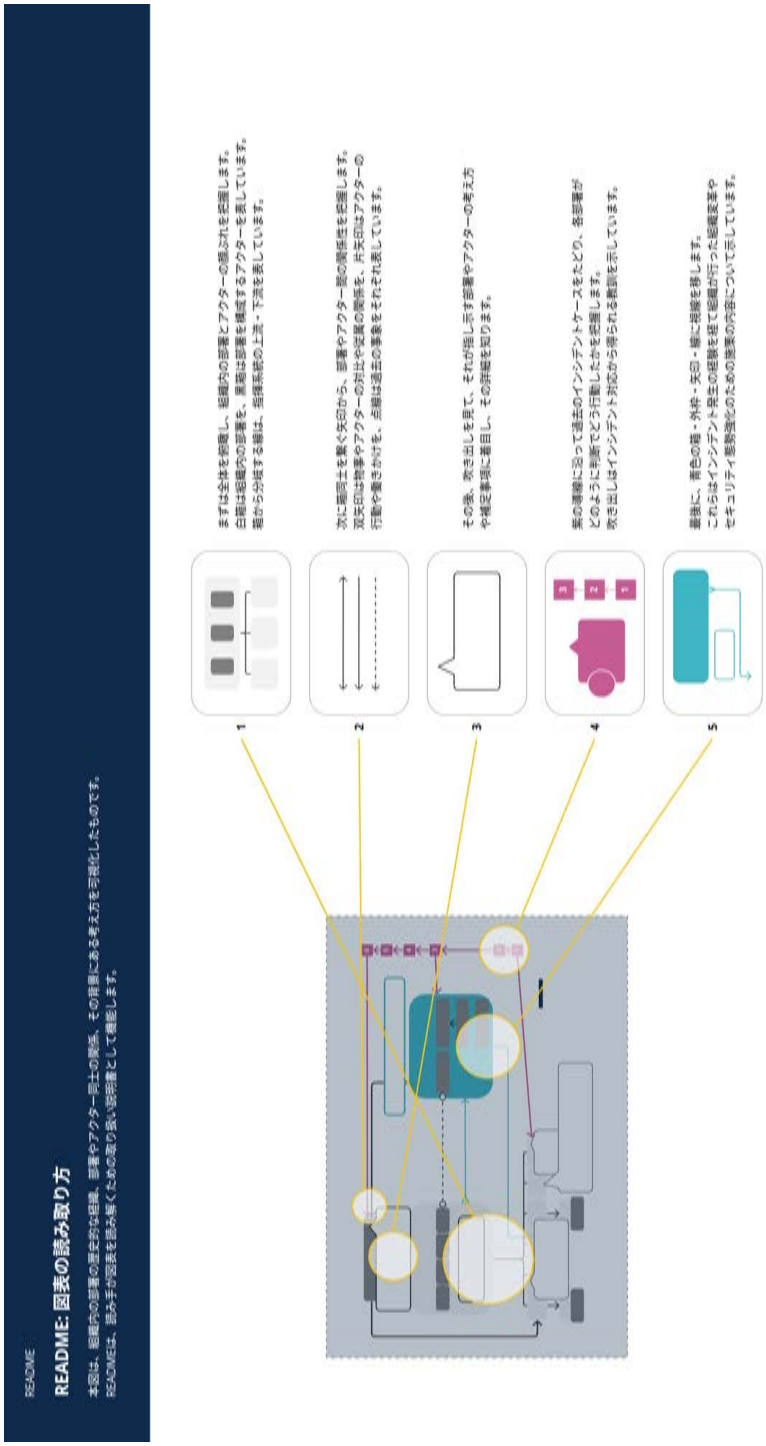
README
README: 図表の読み取り方
本図は、組織内の部署の歴史的な経緯、部署やアクター同士の関係、その背景にある考え方を可視化したものです。
READMEは、読み手が図表を読み解くための取り扱い説明書として機能します。
1
2
3
4
5

図 3.36　README

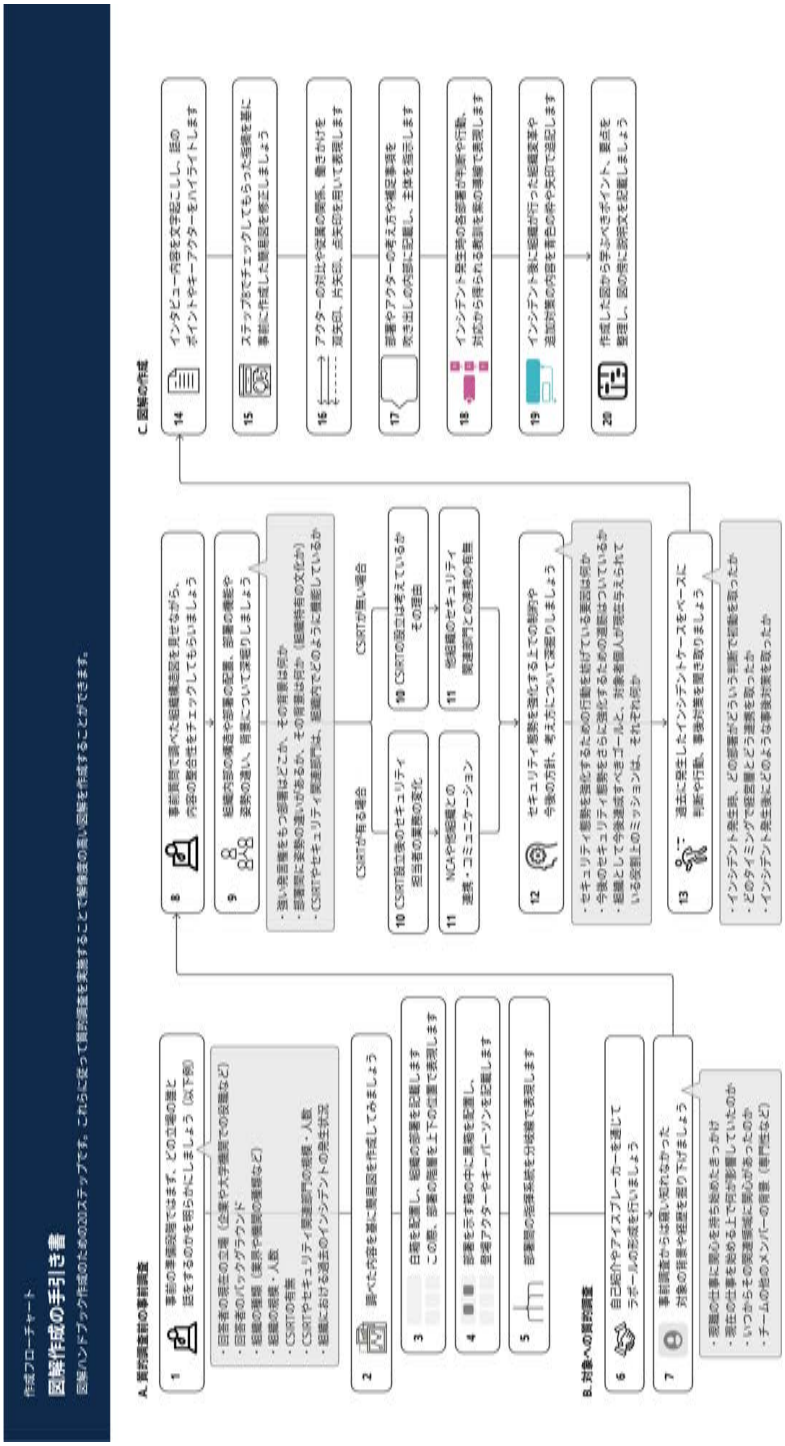

図 3.37　図解作成の手引き書

第 4 章
価 値 検 証

4.1. 検証方法

価値検証ではまず、最初のバージョンのプロトタイプ v1 から検証を行い、図解ハンドブックが有すると想定した価値がどのような条件下で有効性を発揮するか、またどのような制約があるかを把握するため価値検証を実施した。価値検証はオンライン会議ツール Zoom 上での質的インタビューの形式で行い、クライアント側の視点として CSIRT 研究家を対象に 2 回、コンサルタント側の視点として PwC のセキュリティコンサルタントを対象に 1 回実施した。

検証では 7 回にわたる質的調査と分析の結果として、社内の人間関係や各部署の歴史的経緯、部署間のパワーバランスやどの部署の誰を説得するとセキュリティ強化をする上で効果的なのかなど、クライアント組織ごとに価値観や文化、制度があまりにも異なることが明らかになった旨、そのために図解プロトタイプを作成した旨を説明した。さらに、どのような対象を基に図表を作ったかの手順も共有した。

以上の前提のインプットを行ったのち、プロトタイプへのコメントをもらい、また図を見せながらこのプロトタイプがどのような貢献をもたらすか、図解を使って対象の価値観を探ることをすると今よりも手間が増えるか否かを聞いた。また逆に現状の図解プロトタイプが抱える制約や、図解を利用する上で他にどのようなユースケースが考えられるかを質問した。

これらの内容を基にユースケースに関する考察と、必要に応じてプロトタイプの修正を加えた。

4.2. クライアント側からの評価：プロトタイプ v1

4.2.1 検証結果

2022 年 12 月 6 日、プロトタイプ v1（図 3.27）について価値検証を行うため、CSIRT 研究家の Y 氏を対象に、半構造化インタビューを実施した。まず Y 氏は前提として、過去に行なった CSIRT 組織に関するモデル化の共同研究の結果として、社内の人間関係や歴史的背景、会社内部のパワーバランスなど「組織文化をモデル化することはできないという結論に至った」と述べた。その背景として、一つとして同じ CSIRT が存在しないという事実を指摘した。

その上で、本デザインがどのような貢献するかについて、「汎用的なモデルにはなれなくとも、あくまで事例として、こういう事例があるということを示すことにはとても意味がある（共通的な教科書というよりは、参考用の資料集）」と指摘した。例として、外から一見すると組織の文化や制度は同じように見えるのに中から見ると組織ごとに全く違って見えることがあると指摘した上で、「そういった組織ごとの著しい文化や背景の違いを認識してもらうことを目的にこの図表を使うのならば、それはすごく意義があると思う」と述べた。

また様々な企業におけるセキュリティ対策環境や CSIRT を俯瞰して見てきた立場から、「自分が見る限り、多くの企業や大学など組織はモデルが多いと思っていることがまだ多い」と述べ、コンサルタントにお願いする際もモデルを示してほしいと言うケースが多いと指摘した。それゆえこの図表を通じて、そもそもモデル化や共通化はできないのだ、一つとして同じ CSIRT や組織文化はないのだということが示せればとても意味があるとした。

Y 氏はそのケース例となる大学機関についても示唆を与えた。

> 大学は複雑な構造であり、学部ごとにパワーバランスが違っていたり中小企業の社長のような複雑な組織構造を持つきらいがある。例えば千葉大学は元々教育大学と医学大学が起源のため、医学部と教育学部の発言が強い。そういった、こういう歴史的経緯がありこういう学部のパワーバランスになっている、ゆえに CSIRT のありようもこういう風になっている、ということが図解で示せればとても意味がある。

Y 氏は、将来的にはこういうケースを一つではなく複数持つことが重要だと思うかという質問に対し、「一つのケースであっても組織の価値観は文化や歴史的背景に強く結びついているものなのだということが示せるだけでも、とても価値はあると思う」と指摘した。

さらに Y 氏は、最初のバージョンのプロトタイプ v1 の制約と今後の改善点について指摘した。特にこのデザインが改善ができるとすれば大きく二点あり、1）組織内部の権限の所在や権限移譲がどうなっているのか、そして 2）社内で人望が厚く発言力の強いキーパーソンはどういうところにいるのか、を盛り込むべきだという点である。特にキーパーソンに関しては、現状の私立大学機関 K に関して質的調査を行なった H 氏の例があるが、それがどのように組織にとって重要であるかについて強調の余地があったため、それを図解ハンドブックに反映した。

最後に応用可能性について、この図表をどういうシナリオでより活用され得ると思うかとの質問には、セキュリティ強化未達の企業にはまだ CSIRT が何かすら分かっていない人も多いと指摘した上で、まずは CSIRT が何たるかを知ってもらう上での基礎資料にはなると思うとした。

さらに CSIRT を既に構築済みの組織については、「名ばかりの CSIRT を作って日本シーサート協議会に加盟しているものの、実態が伴わないような組織も多い。そういった組織が、CSIRT の改善を考えるときの参考資料になり得る」と述べた。Y 氏はこういった状況で本デザインを利用しそうなアクターとして、CSIRT の担当者や部門のディレクターなど責任者がありえると指摘した。

4.2.2 価値検証後の考察

本デザインのユースケース

一回目の価値検証のポイントは、コンサルタント側が参考資料として用いるのみならず、クライアントが自組織のセキュリティ態勢の不備を認識し、より正確な解像度の高い要件をコンサルタントに伝えるという価値が発揮される可能性が指摘された、ということである。そこで考察として、想定される図解ハンドブックの利用シナリオは二点あると考えられる。これを図 4.1 に示した。

一つ目のシナリオは、セキュリティ態勢の強化が未達成な企業や組織が、自分たちがどうやってセキュリティを強化するべきか／できるかを知る参考資料としての使い方である。クライアント組織は図解ハンドブックを参考にすることで、セキュリティ態勢を強化するために必要となるリソースが何なのか（姿勢やメンタリティなのか、CSIRT のような部署や組織体制なのか）を把握することができる。

二つ目のシナリオは、セキュリティ態勢強化への意識がある程度あり CSIRT は既に構築済みなものの、実態が追いついていないような組織を対象にした、組織改善のための指南書としての使い方である。例えばデザインで取り扱ったケースは、失敗例も示してはいるが、全国の中ではセキュリティ意識が高い事例と言える。したがってそういった組織がどのように CSIRT を継続的に運用し、コミュニケーションを通じて組織内にセキュリティ態勢強化のための機運を醸成しているかをケースとして参考にすることで、自組織のセキュリティ態勢の強化につなげることができる。

また、これを PwC のサイバーセキュリティコンサルティングチームにも提供することで、彼らがクライアント組織に接する場面で、もしかしたらセキュリティメトリクスと併せて使用し、クライアント組織の行動を変容させるツールとして活用するといった用途が想定できる。

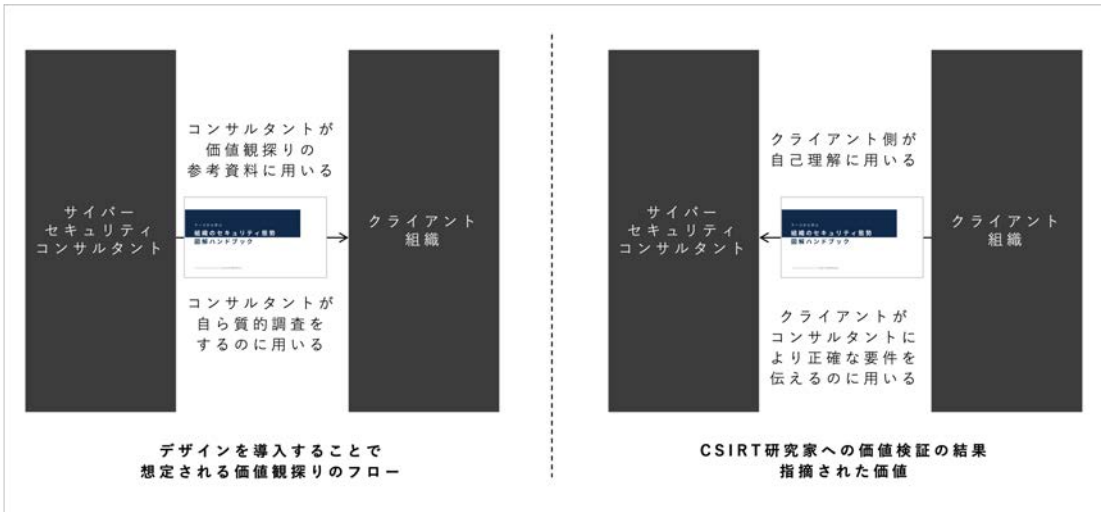

図 4.1 CSIRT 研究家への価値検証の結果指摘された価値

コンサルタントが本サービスを持続的に利用できるようにする仕組み

コンサルタントが持続的に本サービスを利用できるようにする上で重要な観点は、本サービスが明らかにするクライアント組織のケースがどこまで汎用的で、逆にどこまで属組織的かということである。

価値検証からも明らかなように、本デザインが示した私立大学機関 K のケースは他の組織の価値観を探る際の資料集として参考にできる要素を含んでいるものの、やはり制度やリソースの面で他の組織と異なる。実際、他の対象組織には稼働可能な CSIRT や H 氏のようなセキュリティ担当者が存在しない可能性も考慮しなければならない。あるいは、仮に H 氏のようなキーパーソンがいたとしても、その思想を実行するだけの ITC のような組織が整備されていないかもしれない。

したがって PwC のコンサルタントが組織の価値観を把握するための資料集としてプロトタイプ v1 を活用する場合、私立大学機関 K のケースでは少なくとも表 4.1 に挙げたような人材面、制度面、資金面、経営面のアクターやエコシステムが揃っていたという前提に留意する必要がある。そして他の組織にそれらのリソースがなければ、それは本サービスがもたらす価値の限界・制約である。

その制約を突破するために究極的には、コンサルタント自身が異なるクライアント組織と当たるたび、価値観を明らかにするサービスデザインの手法を用いて図表を作成できる状態が望ましいと想定した。そのため、図解ハンドブックでは手法を習得するための手引き書の要素を足し、一連の図解ハンドブックとしてデザインを拡充するに至った。

表 4.1 私立大学機関 K のセキュリティ態勢上の欠かせない存在

人材面	H 氏のようなキーパーソンが存在しなかったら組織はどうなっていたか
制度面	H 氏が主導することができたとしても、それを実行する ITC のような オペレーション組織が存在しなかったらどうなっていたか
資金面	H 氏や ITC が存在しても、セキュリティ体制を持続可能に回すだけの 資金的リソースが存在しなかったらどうなっていたか
経営面	インシデントの報告をした際に、セキュリティに理解を示し迅速に 意思決定を下せる経営層が存在しなかったら、どうなっていたか

4.3. クライアント側からの評価：図解ハンドブック

2023 年 1 月 6 日、修正版の図解ハンドブックについての価値検証を行うため、もう一度 CSIRT 研究家の Y 氏に対し、半構造化インタビューを実施した。

Y 氏は、これまで多くの組織はメールの開封率など量的なデータを見ることはしてきたものの、例えば担当者がどれくらいルールに則って上層部に報告を上げたかや、そもそも上げなかった人がいる場合はなぜ、どういう背景で上げなかったのか、といった質的な調査手法は行ってこなかったと述べた。そのためクライアント組織自身が、質的な調査手法を持っていることが今後重要となると指摘した。さらにクライアント組織側が自己理解のために使うことができるのであれば、セキュリティコンサルティングの現場にとっても意義深いとし、ユースケースとしては CSIRT の担当者が、経営層に対してセキュリティ対策が効果があることを説得する際の材料にもできると指摘した。

ここまでのクライアント側からの評価を踏まえて整理、考察する。本研究では元々の課題設定として、コンサルタント側がクライアントの要件を把握することを前提とした。この本来の意図は、最終的な目標はあくまでもクライアントの満足いくものを提供し、コンサルティング・クライアントのコンサルティングプロジェクトの結果、生まれた成果物が互いに合意できることである。したがって、PwC 側がクライアント側の要件を把握し、そのためにクライアントの価値観を汲み取ることが課題であると定義し、現状のプロトタイプを設計した。

しかしながら CSIRT 研究家への価値検証を通じて明らかになったのは、むしろ本デザインは、クライアント側が課題を自己把握しコンサルタント側に高い解像度で要件を開示することに使えるのではないか、という価値である。したがって図 4.1 に示した通り、想定価値とは図解ハンドブックの使用先が逆方向と別の形の価値が指摘されたものの、プロセスとしてはクライアント組織の情報をどれだけ可視化できるかが全体の流れのポイントであり、その可視化に対して本デザインは一定の効果を発揮しそうであることが価値検証から明らかになった。

4.4. コンサルタント側からの評価：図解ハンドブック

4.4.1 検証結果

2023 年 1 月 13 日、図解ハンドブックについての価値検証を行うため、PwC のコンサルタントの U 氏を対象に半構造化インタビューを実施した。

価値検証ではまず図解ハンドブックへのコメントを聴取し、その後 CSIRT 研究家への価値検証の結果を開示した上で、指摘された価値についてコンサルタントはどう考えるかを聞いた。結果としてコンサルタントは、セキュリティ態勢を強化するために推し量るクライアントの価値観といっても、業務の特徴によってこのデザインはそれぞれ異なる価値を発揮する、と指摘した。その上でセキュリティコンサルティングには、組織の枠を超えて標準化されるべき業務と組織ごとに最適化されるべき業務の二つの類型の業務があるとし、以下のことを指摘した。

> インシデントが実際に発生してしまった場合の対応や、組織のリスク評価などは組織の枠を超えて標準化されるべき業務であり、「インシデントを解決すること」「組織のセキュリティリスクを下げること」が絶対的な解となり得る。したがって、こういった業務においては組織ごとの事情や価値観は、二の次となるべきである。
>
> 一方で、長期的なセキュリティガバナンス態勢の強化などは、企業ごとに異なる事情に合わせて解が調律される必要があり、標準化のための絶対的な解がないため、組織ごとに最適化されるべき業務である。

その上で、企業や組織の枠を超えて対応ガイドラインを標準化できるような業務では、CSIRT 研究家の Y 氏が指摘したようにクライアントが自社の特徴を自己把握する上で本デザインが有効だとし、コンサルタント・クライアント間のやり取りの工数や手間が減るとした。

また、クライアント組織にとっては業界で標準化されているインシデント対応計画通りに行動できなかった原因を振り返る資料として使ったり、あるいは今後自社がどういう状態を目指すべきなのかを自己把握する上で、効果的で価値があ

るだろうと述べた。しかしながら、こうした図解を作ることに手間やコストがかかるようであれば現実的ではないといった制約も聞かれた。

コンサルタントは図解作成の手引き書に記載したフローチャートの再現性についても言及し、コンサルタントが同じプロセスをこなすことは十分可能であるとした。その上で例えば手引き書の質問群などは企業の背景理解に活用できるため、組織のリスク評価のプロジェクト冒頭に行っているヒアリングですぐにでも使えるだろうと述べた。またそれによって図表が作成でき、社内でのパワーバランスや、セキュリティ統括部門の出自、実際にセキュリティリスクが高まっている部門との関係性などの前提理解が図解で示されれば、チーム間で共通理解が持ちやすくなって業務が効率化するため、生み出される成果の質は上がるだろうとした。ただこの用途においても制約があるとし、コンサルタントがヒアリング調査時に本格的に使用するためには、より標準化させた状態、すなわちフローチャート上でより多くの解答パターンの想定が必要だとした。

それに対して、クライアント組織ごとの長期的なセキュリティガバナンスの話など、標準化が難しい業務では、別の価値が指摘された。こうした業務ではクライアント組織ごとに最適化させた計画を作る際、コンサルタントが自分の担当する組織がどうユニークであるかを把握するため、担当組織の特徴が他の組織の中央値とどうズレているのかを参考にし、事例データベースとして使う上で有効だと指摘した。しかしながらこれも、参考とするにはより多くの事例が必要で、現状の図解ハンドブックが提供するケース数では足りないという制約がある。

またこうした組織ごとに最適化する必要があるような業務では、長期的に必要とするセキュリティ態勢は企業ごとに千差万別なので、この図解ハンドブックはクライアント側の役にはあまり立たないという指摘があった。

4.4.2 価値検証後の考察

本デザインのユースケース

ここまで数回の価値検証にて指摘された価値と制約を踏まえ、本デザインの最終的なユースケースは大きく三点想定できる。

一点目は、インシデント対応など今後標準化していくべき目標が定まっているような業務に関して、手引き書を用いて、クライアント組織に業務の内製化を促すという使い方である。将来的に手引き書を使い手の組織がより理解しやすいものに改良し、業務の型をさらに標準化させることができれば、クライアント組織はコンサルタントに頼らずとも、業務上の問題を自前で解決できる。これはセキュリティ強化のコスト削減に繋がるため、クライアント組織にとって有益である。

また、そういったコモディティ化したサービスを標準化することは、コンサルタント側にとっても実は意義があるとU氏は指摘している。その背景としてU氏は、現状のセキュリティ業界はコンサルタントにとって仕事の機会が多い反面、人手が足りていないと指摘した。そのため手引き書を用いて業務を標準化し、単価の低い業務をクライアント側で内製化させることで、コンサルタント側はより組織ごとに最適化すべき付加価値の高い業務に集中できるとのことである。

二点目は、入社間もないコンサルタントがこれまで感覚に頼って覚えてきた仕事を、体系的に実践できる教材としての使い方である。そのためには標準化すべき業務に関しては、インシデント対応や組織のリスク評価に留まらず他の様々な領域で手引き書化することが求められる。例としてU氏は、PwCのサイバーセキュリティが対象とする50近くある他の業務機能（第1章の図1.2で示したような業務）にもこの手引き書が適用できれば、教材として素晴らしいと述べている。特に現状の手引き書は、専門用語を使わず特定の表記ルールに沿って書かれているため、多くの人が使用する教育コンテンツ用手引きとして有用だと指摘した。ただしこれが教育コンテンツとして適用可能なのは、一般的に正しい解が存在するような業務に限定されるというのが制約である。

三点目は、コンサルタントが組織ごとに最適化させていくべき業務において、担当する組織の特徴を把握することに活用するといった使い方である。これは前述したように図解ケースが、コンサルタントが担当する組織と中央値の差を把握するために価値を発揮するためである。

今後、本デザインが以上のユースケースに特化していくことで価値を最大化し、将来的にはセキュリティコンサルティングの文脈を超えて、他の領域にも適用可能な価値を発揮すると筆者は期待する。

第 5 章
結　　論

5.1. 本稿のまとめ

本研究は、サイバーセキュリティの分野を専門とするPwCのコンサルタントに向けたサービスデザインの研究である。本稿ではまず、コンサルタントの抱える課題や要件を特定することを目的に、PwCのコンサルタントを対象に計4回のエスノグラフィーを実施した。その結果、現状のセキュリティコンサルティングのプロジェクトにおいてクライアント組織内部の文化や価値観を把握する方法論が確立していないことや、コンサルタント自身が価値観を把握するプロセスに難しさを感じていることが明らかになった。そしてクライアント側が抱える課題や組織内部の価値観や文化、制度を明らかにしてほしいというコンサルタント側の要望を特定するに至った。

そこで今度クライアントの価値観を明らかにするため、CSIRT職員やCSIRT研究家などクライアントのモデルケースとなるような組織について知見を有するアクターを対象に、計3回の質的調査を実施した。質的調査による情報抽出の結果、筆者はPwCのサイバーセキュリティコンサルタントを対象に、クライアントの代表となるような組織の内部の関係性や価値観・考え方の背景を簡単に理解できるように可視化した、図解中心のパンフレット「組織のセキュリティ態勢・図解ハンドブック」を設計した。この図解ハンドブックは、1）読み手が見ることで組織のセキュリティ態勢やインシデント発生時の対応について一覧で把握することができるケーススタディ型の図解、2）読み手が図表を読み解くための取り扱い説明書、読み方ガイドとして機能するREADME、3）図解を設計する過程で用いた質的調査の手法・分析手順自体を、いわば料理のレシピのように体系的

にフローチャート化した手引き書、の三点から構成された。

最初のプロトタイプの段階では、コンサルタントがクライアントの価値観のどの領域を探るべきかをケーススタディ型の図解を参考することで、手引き書に沿って質的調査を行うことでクライアントとのやり取りの工程を短縮させ、より正確にクライアントの要件を特定することができるようになると想定した。そこでその想定について検証するため、クライアント側の代表としてCSIRT研究家に価値検証を実施した。その結果、コンサルタントがクライアント組織の価値観探りに直接用いるのではなく、むしろクライアント側が課題を自己把握しコンサルタント側に高い解像度で要件を開示することに使えるのではないか、という価値が指摘された。

そこで本研究における最終成果物となる修正後のプロトタイプに関して、PwCのコンサルタントを対象に価値検証を実施し、本デザインの制約と価値について分析した。その結果、組織の枠を超えて標準化されるべき業務と、組織ごとに最適化されるべき業務の二つの類型の業務によって、本デザインはそれぞれ異なる価値を発揮する、との指摘を得た。特に組織の枠を超えて標準化されるべき業務では、クライアント組織側の理解が進むことに貢献する反面、フローチャート上でより多くの解答パターンの想定が必要だという現状のデザインの制約も聞かれた。組織ごとに最適化されるべき業務では、コンサルタントが自分の担当組織の特異な点を把握するための事例データベースとして有効な反面、現状の図解ハンドブックが提供するケース数では足りないという制約が指摘された。

筆者はそれを基に本デザインの将来的なユースケースとして、1）インシデント対応など今後標準化していくべき目標が定まっているような業務に関して、手引き書を用いて、クライアント組織に業務の内製化を促すツールとしての使い方、2）入社間もないコンサルタントがこれまで感覚に頼って覚えてきた仕事を、体系的に実践できる教材としての使い方、3）コンサルタントが組織ごとに最適化させていくべき業務において、担当する組織の特徴を把握することに活用するといった使い方、の三つの貢献の方向性について考察した。

5.2. 本稿の制約と今後の展望

本研究は、現状の図解ケースが提供する組織のケース数が少ないということ、そして手引き書がもたらす価値が組織のリスク評価などまだ極一部の業務に相当する部分の手順化・標準化にしか対応していないということ、の大きく二つの制約を抱えている。

前者のケース数が少ないという制約は PwC への価値検証からも指摘されており、特にコンサルタントが担当組織の特性を把握する際の事例データベースとして活用する場合は、扱うケースの数がデータベースとしての価値を左右すると指摘を受けている。したがって本研究が将来的に、日本シーサート協議会や組織を俯瞰的に見られる立場にある協会や団体と研究上の連携をし、より多くの組織に対して質的調査を実施し、扱うケースの数を増やすことは重要であると考えられる。こうすることで、コンサルタントが企業に最適化させた計画を作ることを支援すると同時に、業務の標準化の精度を上げることにも貢献する。

また後者の、一部業務の標準化にしか対応できていないという制約も、価値検証から指摘されている。例として、PwC のコンサルタントからは組織のリスク評価プロジェクト冒頭の背景理解ではすぐに使えると指摘があったものの、クライアント組織のセキュリティ態勢強化を目的とするその他の業務にはいまだに対応できていない。そこで、今後手引き書が対応可能な機能や業務の幅を広げていくために、「組織の価値観を可視化するための手引き書」そのものの作り方ガイドを、一段階一般化して作ることを目指す展望が考えられる。そうすることで、コンサルタントは組織のリスクの評価やインシデント対応の枠を超えて、組織のセキュリティ態勢を強化するための他のさまざまな業務においても、同じように手引き書を作ることができるようになる。その結果として、より多くの仕事を標準化して効率化し、手引き書自体をクライアント側に販売するなどして内製化を促すことも可能である。また手引き書を業務ごとに作成することで、新人コンサルタントの教育に役立て、コンサルティングファーム内での知識の集約につながると期待する。

これはある意味、これまで答えの雛形を提供することも多かったコンサルティング業界が、答えの解き方を作ることに終始する形態にシフトすることに貢献す

るかもしれない。PwC の U 氏の言葉を借りれば、「業務における答えのガイドラインを出すのではなく、答えの出し方のガイドラインを出す」ということである。そうすることでコンサルタント自身も、標準化しコモディティ化した仕事から離れて付加価値の高い仕事にシフトでき、長期的な視点で見れば、より多くの業務が標準化されることに繋がる。また標準化が達成されれば、これは PwC のセキュリティコンサルティングの現場に留まらず、現在世界中の多くのセキュリティ態勢強化を必要とする組織の業務内製化に貢献し、業界の裾野を広げるものと筆者は期待している。

そして最後に、本研究は現場での適用のない範囲での価値検証となってしまったが、本研究のデザインやそれがさらに進化した形のデザインが、多くの実際の企業や組織と向き合う現場で長期的に検証・実証されることで、この研究の真の価値が発揮されるものと筆者は期待している。

謝　　辞

本稿は 2022 年から 2023 年にかけて、筆者が慶應義塾大学大学院メディアデザイン研究科に在籍中の研究成果をまとめたものです。

まず私の大学院における指導教員であり、本研究に先立ち、コロナ禍の吹き荒れた 2020 年以降、幅広い知見から的確なご指導をいただきました佐藤千尋先生には感謝の念に堪えません。厚くお礼申し上げます。

加えて、研究内容や研究の手法について底抜けに温かくご指導いただきました大川恵子教授、研究フィールドをご提供いただいたばかりか、常に最適なタイミングで現れ研究内容に的確なご助言を賜りました砂原秀樹教授、そしてプレゼンテーションのたびに温和な質問をいただきました Dunya Donna Chen 先生に厚くお礼申し上げます。

そして本研究は、共同研究のパートナーである PwC コンサルタントの上村様、展様の多大なるご協力なしには実現し得ませんでした。筆者による執拗で深淵な質的インタビューの数々にもめげず、大変親身にお付き合いいただきましたこと心より感謝申し上げます。

また年末年始の忙しい時期にも関わらず、質的調査にご協力いただきました CSIRT 研究家の Y 様、慶應義塾 CSIRT の H 様に心より感謝申し上げます。

最後になりましたが、画面越しにお世話になりました同期の皆さん、サービス学会での論文提出に伴い深夜まで執筆にご協力いただいた有馬さんと山内さん、世界各地から温かいエールを送ってくれた CEMS の友人たち、私の学生生活を経済的かつ精神的に支えてくれた家族、そして北イタリアで論文執筆のための山小屋と素晴らしい時間を提供してくれた Filippo Perini 君と彼のご家族に心から感謝の意を示し、以上を持って謝辞といたします。

参 考 文 献

[1] Hugh Beyer and Karen Holtzblatt. Contextual design. *interactions*, Vol. 6, No. 1, pp. 32–42, 1999.

[2] Michael Polanyi. Tacit knowing: Its bearing on some problems of philosophy. *Reviews of modern physics*, Vol. 34, No. 4, p. 601, 1962.

[3] Ikujiro Nonaka and Georg Von Krogh. Perspective—tacit knowledge and knowledge conversion: Controversy and advancement in organizational knowledge creation theory. *Organization science*, Vol. 20, No. 3, pp. 635–652, 2009.

[4] Ikujiro Nonaka. A dynamic theory of organizational knowledge creation. *Organization science*, Vol. 5, No. 1, pp. 14–37, 1994.

[5] Ikujiro Nonaka and Hirotaka Takeuchi. The knowledge-creating company. *Harvard business review*, Vol. 85, No. 7/8, p. 162, 2007.

[6] Andrew C Inkpen and Adva Dinur. Knowledge management processes and international joint ventures. *Organization science*, Vol. 9, No. 4, pp. 454–468, 1998.

[7] Robert M Grant. Prospering in dynamically-competitive environments: Organizational capability as knowledge integration. *Organization science*, Vol. 7, No. 4, pp. 375–387, 1996.

[8] James Brian Quinn. The intelligent enterprise a new paradigm. *Academy of Management Perspectives*, Vol. 6, No. 4, pp. 48–63, 1992.

[9] Andrea Prencipe. Breadth and depth of technological capabilities in cops: the case of the aircraft engine control system. *Research policy*, Vol. 29, No. 7-8, pp. 895–911, 2000.

[10] Dovev Lavie. The competitive advantage of interconnected firms: An extension of the resource-based view. *Academy of management review*, Vol. 31, No. 3, pp. 638–658, 2006.

[11] Ikujiro Nonaka. The knowledge-creating company. In *The economic impact of knowledge*, pp. 175–187. Routledge, 2009.

[12] Mark K Singley and John Robert Anderson. *The transfer of cognitive skill*. No. 9. Harvard University Press, 1989.

[13] Albert Bandura. Social learning theory. morristown, 1971.

[14] Barbara Levitt and James G March. Organizational learning. *Annual review of sociology*, pp. 319–340, 1988.

[15] Linda Argote and Paul Ingram. Knowledge transfer: A basis for competitive advantage in firms. *Organizational behavior and human decision processes*, Vol. 82, No. 1, pp. 150–169, 2000.

[16] Henrik Bresman. External learning activities and team performance: A multimethod field study. *Organization science*, Vol. 21, No. 1, pp. 81–96, 2010.

[17] Dennis Epple, Linda Argote, and Rukmini Devadas. Organizational learning curves: A method for investigating intra-plant transfer of knowledge acquired through learning by doing. *Organization science*, Vol. 2, No. 1, pp. 58–70, 1991.

[18] Douglas A Irwin and Peter J Klenow. Learning-by-doing spillovers in the semiconductor industry. *Journal of political Economy*, Vol. 102, No. 6, pp. 1200–1227, 1994.

[19] Anne S Miner and Philip Anderson. Industry and population-level learning: Organizational, interorganizational, and collective learning processes. *Advances in strategic management*, Vol. 16, pp. 1–30, 1999.

[20] Dennis Epple, Linda Argote, and Kenneth Murphy. An empirical investigation of the microstructure of knowledge acquisition and transfer through learning by doing. *Operations research*, Vol. 44, No. 1, pp. 77–86, 1996.

[21] Rebecca Henderson and Iain Cockburn. Scale, scope and spillovers: the determinants of research productivity in ethical drug discovery. 1994.

[22] Linda Argote and Ella Miron-Spektor. Organizational learning: From experience to knowledge. *Organization science*, Vol. 22, No. 5, pp. 1123–1137, 2011.

[23] Craig S Galbraith. Transferring core manufacturing technologies in high-technology firms. *California management review*, Vol. 32, No. 4, pp. 56–70, 1990.

[24] Eric D Darr, Linda Argote, and Dennis Epple. The acquisition, transfer, and depreciation of knowledge in service organizations: Productivity in franchises. *Management science*, Vol. 41, No. 11, pp. 1750–1762, 1995.

[25] Gabriel Szulanski. Exploring internal stickiness: Impediments to the transfer of best practice within the firm. *Strategic management journal*, Vol. 17, No. S2, pp. 27–43, 1996.

[26] Joseph E McGrath and Linda Argote. Group processes in organizational contexts. *Blackwell handbook of social psychology: Group processes*, pp. 603–627, 2001.

[27] Holly Arrow, Joseph E McGrath, and Jennifer L Berdahl. *Small groups as complex systems: Formation, coordination, development, and adaptation.* Sage Publications, 2000.

[28] Linda Argote and Erin Fahrenkopf. Knowledge transfer in organizations: The roles of members, tasks, tools, and networks. *Organizational Behavior and Human Decision Processes*, Vol. 136, pp. 146–159, 2016.

[29] Michael L Tushman and David A Nadler. Communication and technical roles in r&d laboratories: An information processing approach. *TIMS Studies in the Management Sciences*, Vol. 15, No. 1, pp. 91–112, 1980.

[30] Thompson SH Teo and Anol Bhattacherjee. Knowledge transfer and utilization in it outsourcing partnerships: A preliminary model of antecedents and outcomes. *Information & Management*, Vol. 51, No. 2, pp. 177–186, 2014.

[31] Wesley M Cohen and Daniel A Levinthal. Absorptive capacity: A new perspective on learning and innovation. *Administrative science quarterly*, pp. 128–152, 1990.

[32] Daniel Z Levin and Rob Cross. The strength of weak ties you can trust: The mediating role of trust in effective knowledge transfer. *Management science*, Vol. 50, No. 11, pp. 1477–1490, 2004.

[33] Anna Sankowska. Relationships between organizational trust, knowledge transfer, knowledge creation, and firm's innovativeness. *The Learning Organization*, 2013.

[34] Dong-Gil Ko. The mediating role of knowledge transfer and the effects of client-consultant mutual trust on the performance of enterprise implementation projects. *Information & Management*, Vol. 51, No. 5, pp. 541–550, 2014.

[35] Natalia Nikolova, Guido Möllering, and Markus Reihlen. Trusting as a 'leap of faith': Trust-building practices in client–consultant relationships. *Scandinavian Journal of Management*, Vol. 31, No. 2, pp. 232–245, 2015.

[36] Gurpreet Dhillon, Romilla Syed, and Filipe de Sá-Soares. Information security concerns in it outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management*, Vol. 54, No. 4, pp. 452–464, 2017.

[37] Karen O'Reilly. *Key concepts in ethnography*. Sage, 2009.

[38] Hugh Beyer and Karen Holtzblatt. *Contextual Design: Defining Customer-Centered Systems*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1997.

[39] Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, et al. Computer security incident handling guide. *NIST Special Publication*, Vol. 800, No. 61, pp. 1–147, 2012.

付　　録

A．組織のセキュリティ態勢とは

一般に、組織の「セキュリティ態勢」「セキュリティ管理態勢」という言葉が指し示す領域は広範である。P 社が公表している業務範囲や後述する大学の情報セキュリティ関係者への質的調査から、組織におけるセキュリティ管理態勢はおよそ、セキュリティ上の問題発生前の予防、異常の検知、問題発生後の対応の三つの段階に大別される[1]。

まず一つ目の問題発生前の予防の段階では、組織が必要なインシデント予防策を講じているか否かを評価し、不足部分があればそれを強化することが肝要である[2]。一般に P 社が組織の態勢強化の支援対象とする範囲はこの予防の段階であることが多く、これはサイバーリスクの評価や分析、脆弱性やパッチ管理の構築、侵入検知システムの導入、インシデントの種類に対応した対応マニュアルの作成、組織の従業員に対するセキュリティ意識向上トレーニングなどを含む。

二つ目はインシデントや何らかの異常の検知の段階であり、そのための態勢構築が組織にとって欠かせない。カーネギーメロン大学のインシデント対応の専門家によれば、これは通常運転時と比較した際に、ネットワークやシステムの動作に何らかの異常な挙動が発生していないかを継続的に監視することで実現する。そして組織のネットワークに通常と異なるデバイスが接続されてされていたり不自然なアプリケーションが介入しているなど、ネットワーク上に生じる異常の兆

1　PwC サイバーセキュリティ，https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting.html

2　PwC サイバーセキュリティ，https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting.html

候を把握することで問題の検出を行うことができる[3]。

三つ目は、問題発生後の対応段階である。自社でセキュリティ・インシデントを発見する、あるいは他者からの報告を受けてインシデントが検出されると、組織はその詳細を分析して事態を把握し、制御機能を復旧させ、さらなる二次被害の発生を食い止めるための計画を作成することが求められる。その後、可能な限り速やかに通常の業務に戻れるよう計画を実行に移す[4]。米国における事例では問題発生後の対応について、米国標準技術研究所（NIST）が独自のインシデント対応モデルを開発している [39]。NIST はハンドブック *NIST Special Publication Computer Security Incident Handling Guide* の中で、「contain, eradicate and recover」という用語を使ってインシデント対応の手順を説明し、主に米国連邦行政府のインシデント対応担当者への普及を図っている。

以上のようなセキュリティ管理態勢を実行されていることが、組織にとっては本来望ましい。しかしながら実際的にこれらの対策を実現できている組織は現状では少なく、それゆえ組織を支援する P 社のサイバーセキュリティコンサルティングの価値が発揮されている。

B. 組織内のインシデント対応チーム CSIRT

質的調査の結果判明している事実として、P 社の現状のクライアント組織の多くは資金的余力のある大企業であることが多く、中には独自のセキュリティ管理部門を有する企業もある。一方でその一部は部門を有するだけであって、前述の予防・検知・対応のプロセスを踏襲できていない場合も多い。このような組織のセキュリティに対する準備の進捗や捉え方を測る指標の一つとして、コンピュータ・セキュリティ・インシデント対応チーム（CSIRT）の有無が挙げられる。

CSIRT は、サイバーセキュリティインシデントの検出や対応、そのための予防

3 Computer Emergency Response Team（CERT）, `https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team`

4 Computer Emergency Response Team （CERT）, `https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team`

的な対策を実行するインシデント対応の専門家集団である。前出のインシデント対応の研究家によれば、CSIRT は 1988 年に米国のカーネギーメロン大学で結成されたコンピュータ緊急対応チーム（CERT）が基となっている。発足当初、普及初期のインターネットにインターネットワームによる被害が生じ、サイバーセキュリティ上の脆弱性となるシステムの欠陥や対策の不備といった問題が浮き彫りになった。結果的にこうしたシステムを運用する組織においてインシデントに対する危機意識が高まり、その後、他の組織にも飛び火する形で数多くの CSIRT が設立された[5]。

本稿で行ったサイバーセキュリティを担当する大学関係者らへの質的調査によると、日本でもこの潮流に刺激を受ける形で旧通商産業省の傘下で最初の JPCERT/CC が設立された。その後総務省の傘下に攻撃情報の共有を行うことを目的に設立された ISAC や、民間の IPA、政府機関を対象とする NISC など、多種多様なサイバーセキュリティ対策に関する組織が設立された（日本におけるこれら組織の広がりに関する詳細は図 B.1 に示した）。CSIRT は現在、P 社がクライアントとするような企業を含む一部の組織に設立されるようになってきている。

5 Computer Emergency Response Team （CERT）, https://www.techtarget.com/whatis/definition/CERT-Computer-Emergency-Readiness-Team

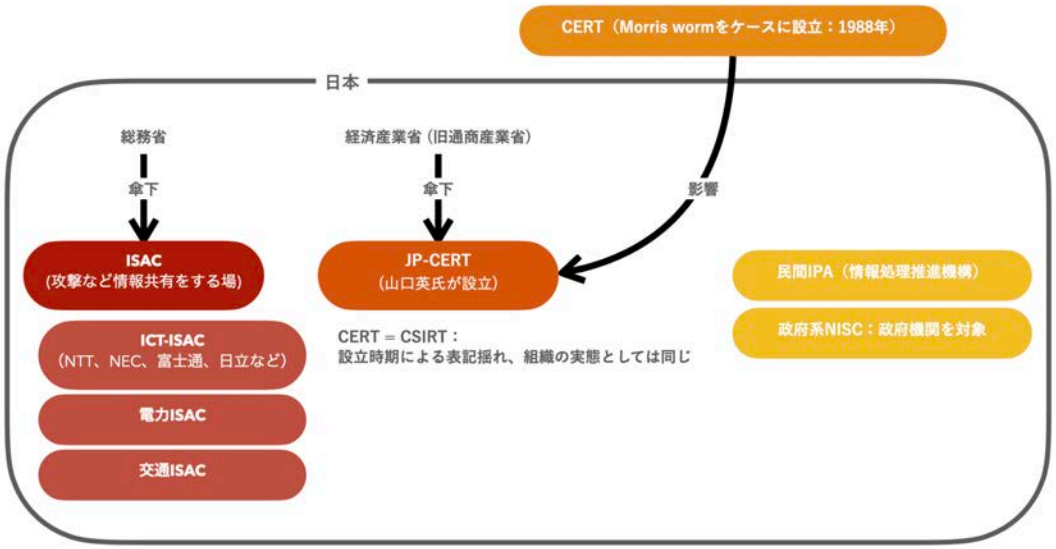

図 B.1 CSIRT 設立経緯 （質的調査の内容より筆者作成）