SPI Japan 2023

クラウドサービスのセキュリティ品質点検の仕組み構築と運用

～多様なクラウドサービス基盤を活用し、迅速にサービスを立ち上げて安全に価値提供するための要点～

TIS株式会社

品質革新本部 品質監査室

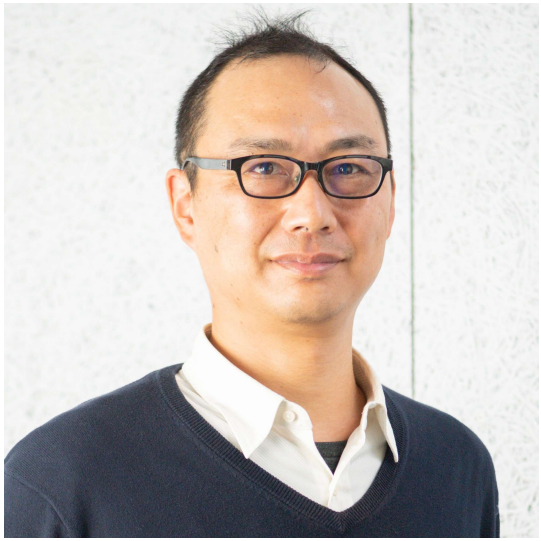
堤智也

E-mail：tsutsumi.tomoya@tis.co.jp

はじめに

自己紹介

TIS株式会社
品質革新本部　品質監査室
セクションチーフ　堤 智也(つつみ ともや)



- 2000年
  TIS(旧東洋情報システム)入社
  Webアプリ開発(旅行・航空業界)・ITアーキテクト業務に従事
- 2009年～
  技術本部生産技術部(当時)に異動し、
  共通開発基盤の構築を担当
- 2011年～
  社内共通クラウド開発環境の
  企画～運営～AWS移築のマネージャ
- 2019年～
  プロフィット部門で勤務
- 2021年～
  品質監査室、クラウドセキュリティ審査業務を担当

TISのご紹介

■ 会社概要

（2023年7月1日現在）

社　　名	TIS株式会社 （TIS Inc.）
創　　業	1971年4月28日
設　　立	2008年4月1日
資 本 金	100億円
代 表 者	代表取締役社長　岡本　安史
本　　店	東京都新宿区西新宿8丁目17番1号
従業員数	連結：21,946名　単体：5,695名 （2023年3月31日現在）
売 上 高	連結：508,400百万円　単体：238,140百万円 （2023年3月期）
営業利益	連結：62,328百万円　単体：29,450百万円 （2023年3月期）

認定資格

- 総務省「届出電気通信事業者登録」
- 経済産業省「情報セキュリティサービス基準適合サービスリスト」
  「情報セキュリティ監査サービス」
- 経済産業省「システム監査企業台帳登録」
- 情報セキュリティマネジメントシステム(ISMS)(ISO/IEC27001)
- ITサービスマネジメントシステム(ITSMS)(ISO/IEC20000)
  [認証対象範囲]
  東京第3センター/東京第4DC/大阪第2DC/大阪第3DC/大阪第4DC
- 品質マネジメントシステム(QMS)(ISO9001)
- プライバシーマーク使用許諾事業者
- 東京都「一般建設業 (電気通信工事)」
- 環境マネジメントシステム(ISO14001:2015)

■ 特長

TISは3,000社以上のビジネスパートナーとして「成長戦略を支えるためのIT」を提供

TISの50年の実績が裏付ける、高度な実現力と先進性

TISの提案力と課題解決力を支えるのは200を超えるサービスメニュー

“攻める” “やり切る” 現場力、人材力

背景

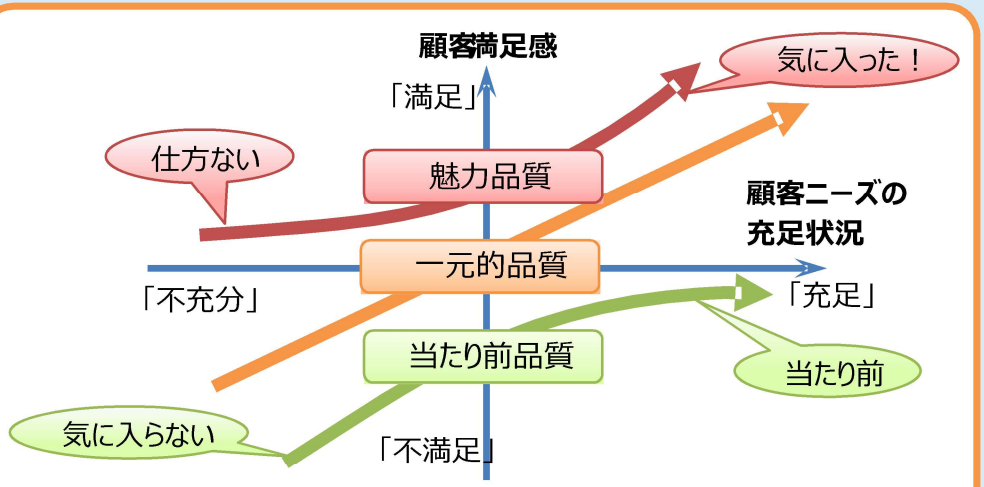
当たり前品質から魅力品質へ

OUR PHILOSOPHY
ターゲット：質で語られる信頼のトップブランド
スタイル：オネスト、オープン

コーポレート・サステナビリティ基本方針　マテリアル
高品質なサービスを通じ、社会に安全を

当たり前品質から魅力品質へ

利用者の期待は、機能だけにとどまらず、利用目的や利用場面に応じて、安全性・セキュリティはもとより、快適さや楽しさ、また、ビジネスへの高度の貢献といった内容まで含まれるようになってきており、非常に多様化している。



この図は、顧客視点で品質を分類で表現した狩野モデル』で、
『顧客ニーズの充足状況』と、『顧客満足感の関係をモデル化したものです。
TISは顧客を虜にする事を目標に、「魅力品質」を追及し継続的改善を推進

必要な機能を使えるというだけではよいサービスであるとはいえず、利用者が必要とする機能を「高い満足度」で使えることが強く求められるようになっている。

TISの実態は、想定している機能が動作しない危惧のみを考え、機能を正しく動くようにすることが主要な品質であるという考えるケースが多いように感じる。

クラウドセキュリティ基準未達のままサービスイン

- **クラウドセキュリティ基準**が認知されていない
  - × ISO/IEC 27017に準拠したクラウドセキュリティ基準はあるが認知されていない。
  - × お客様からクラウドサービスに関する取り組みの照会があった際、特にないと回答してしまうケースも。
- **現場で実装・確認**がなされていない
  - × 一般的なセキュリティ脆弱性対策などは実装・確認されているが、クラウドサービスならではの観点での実装・確認はされていない。
- **全社的な状態把握の仕組み**もなかった
  - × 一般的な工程毎のExit/Entryクライテリア運用されていたが、クラウドサービスならではの観点による組織的な点検の仕組みはなかった。

セキュリティ品質に関する当時の社内体制

- 品質革新本部
  - ISO9001及びISO20000に基づく**マネジメント品質・プロセス品質**が中心
  - セキュリティ品質についてはセキュリティ脆弱性検査程度
    ⇒**クラウドサービスならではの品質点検**はやっていない
- 管理本部コンプライアンス統括部
  - ISO27001に基づくISMS運営
  - ISO27017に基づくクラウドセキュリティ基準制定
    ⇒**サービス個々の品質点検**はやっていない

セキュリティ品質を所管する2組織には
クラウドサービス個々の品質点検をやる体力なし

セキュリティ品質に関する当時の社内体制

セキュリティ品質を所管する2組織には
クラウドサービス個々の品質点検をやる体力なし

❑ 対処方針

■ 品質革新本部内に専門部隊構築

- ▶ 現場にやりなさいというためには
  完全アウトソーシングではうまくいかない

■ セキュリティコンサル外販部隊との協力体制構築

- ▶ 早期に運用を立ち上げ・定着させるためには
  品質革新本部だけでは能力不足

実施事項

チェックリストの整備

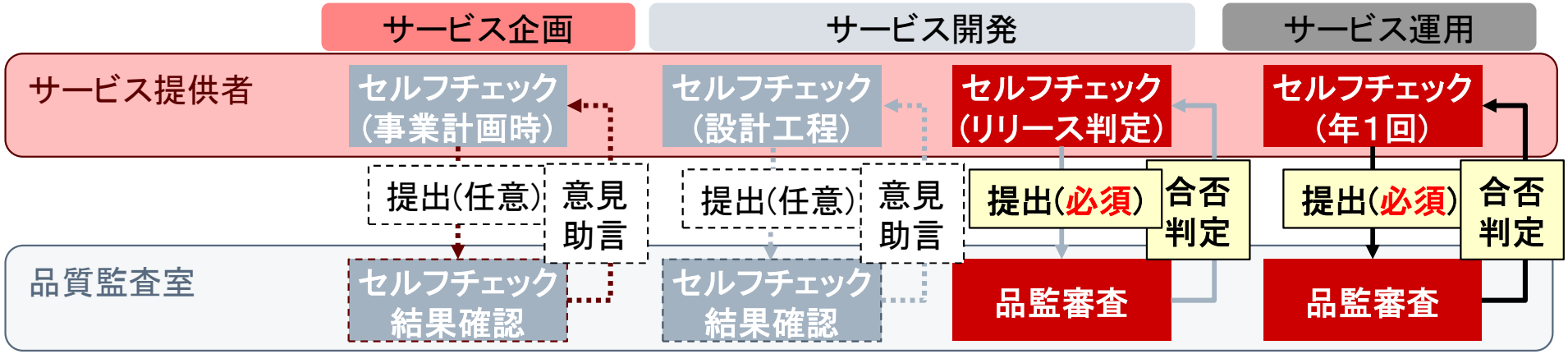
- クラウドセキュリティ基準をベースにクラウド情報セキュリティ監査制度の内容を加味したチェックリストを作成。
  - 基準の条文をわかりやすく表現を変えて記載。
    場合によっては複数の確認項目に分けて記載。
  - 確認項目の文中で説明を要する用語等に関連する
    例示や補足を記載。
  - 「対応不要」、「対応見送り」の選択肢を設け、
    セルフチェックのハードルを下げた。
  - 提供中サービスから複数選定して試行を依頼。

- チェックリストの構造

審査を実施する第三者組織の立ち上げ

- 審査を実施する第三者組織を立ち上げ(「品質監査室」立ち上げ)
  - セキュリティに関する有識者を他組織から招聘
    - 当社にISMSを導入した際の中心人物
    - セキュリティの知見がある人物(現場有識者)
  - セキュリティコンサル外販部隊との協業体制構築
    - セキュリティコンサル外販で培った知見・ノウハウを社内向けに注入
    - 社内向け点検で経験を蓄積し、外販ビジネスのレベルアップに寄与

セルフチェックと第三者組織による審査



サービス企画

事業計画のインプットとしてチェックリストを確認し、対応する事項、対応しない事項を選定する。
対応する事項について、事業計画や以降の各種計画に織り込んで、対応してください。
品監への提出は任意です。

サービス開発

設計工程で対応する事項について設計に織り込まれているか確認してください。
品監への提出は任意です。
リリース判定として対応する事項が実装できているかを確認してください。
品監への提出は必須です。

サービス運用

年に一度、対応する事項が想定通りに実装されているか確認してください。
品監への提出は必須です。

セルフチェックと第三者組織による審査

- クラウドセキュリティチェックリストによるセルフチェックと第三者組織による審査の運用定着
  - 組織長をその気にさせる　…トップダウンの力を借りる
    - 経営層が参加する会議で趣旨説明して賛同を得る…経営の意思化
    - 組織長に趣旨を理解してもらい、配下部門に指示してもらう…組織の施策化
    - 各組織の品質マネジメントシステム責任者に趣旨を理解してもらう…展開力増幅
  - 支援活動を充実
    …ダメというだけでなく、じゃあどうすればいいの？に応える活動
    - セルフチェック結果の確認後、即審査ではなく、改善ポイントを伝え、改善を促すことに注力
    - ローンチ前の点検だけでなく、企画・設計段階でも相談に乗ることを表明
    - ISO27017認証取得支援活動開始
  - 雰囲気つくり　…取り組んだ方がいいかなと思わせる
    - 認証サービスの一覧公開
    - 認証ロゴの制定

運用改善

チェックリストの「例示・補足」改善

❑ 改善例: セキュリティインシデントの報告手順

✓ より具体的な説明を「例示・補足」欄に追記

条文	確認項目	**例示・補足**
（セキュリティ事象の報告手順） 第11条　クラウドサービス提供責任者は、クラウドサービス利用者およびクラウドサービス提供者が検知した情報セキュリティ事象を報告する仕組み、および報告された情報セキュリティ事象をクラウドサービス利用者が追跡できる仕組みを提供するものとする。	CLD提供責任者は、「CLD利用者」が検知した情報セキュリティ事象★を「CLD提供者」に報告するための仕組みを、CLD利用者に提供している。	★インシデント、不具合の可能性，関連するシステム、サービスやネットワークの状態に関連する事象 ※報告の方法・手段を備えていること。報告ページ、メール、電話、ヘルプデスク等妥当なものならなんでもよい 【証跡】 顧客提示文書「利用者が検知した際の報告方法・手順」の記載箇所
	CLD提供責任者は、「CLD提供者」が検知した情報セキュリティ事象を「CLD利用者」に報告するための仕組み★を、CLD利用者に提供している。	★セキュリティ事象の告知ページ、メール配信等による報告する仕組み 【証跡】 顧客提示文書「当該クラウドサービスが受理／検知したセキュリティ事象を利用者に開示する方法・仕組等」の記載箇所
	CLD提供責任者は、CLD利用者およびCLD提供者により報告された情報セキュリティ事象の状況をCLD利用者が追跡するための仕組み★を、CLD利用者に提供している。	★セキュリティ事象の採番等により、追跡を容易とする仕組み 【証跡】 顧客提示文書「当該クラウドサービスが受理／検知したセキュリティ事象の状況を利用者が追跡できる仕組み」の記載箇所

指摘の多い事項に関する事例蓄積・展開

- リスクコミュニケーションとは

  「情報を共有、対話や意見交換を通じて意思の疎通をすることにより、リスクに関する相互理解を深めたり、信頼関係を醸成するためにリスクコミュニケーションを実施するもの」

- 具体的に何をすればよいか現場で理解しづらい

- リスクコミュニケーション計画書のサンプルを策定し現場に展開
- 同様に、現場の好事例を蓄積し展開

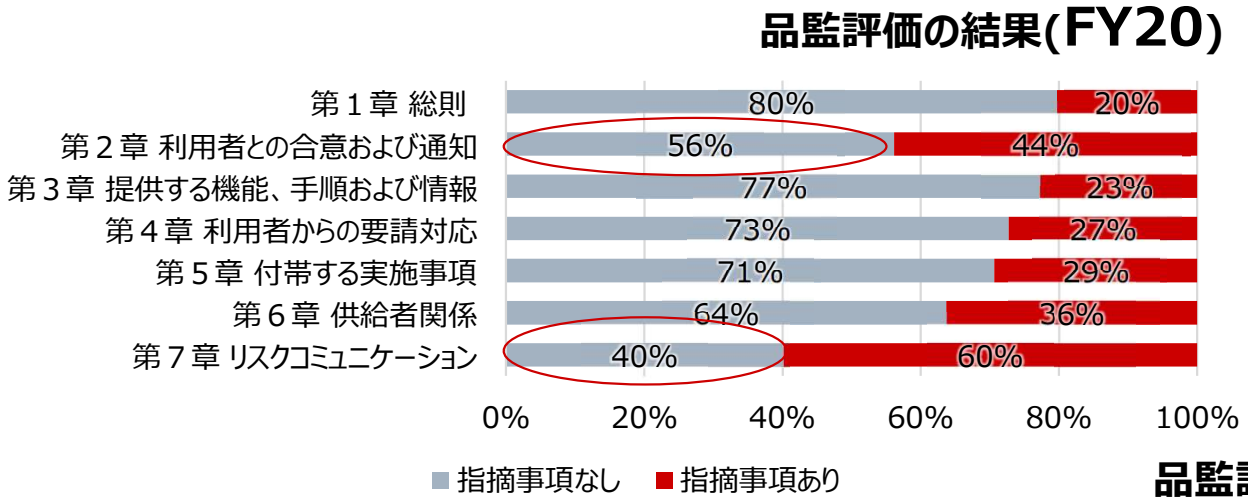
実施結果

遵守率の向上

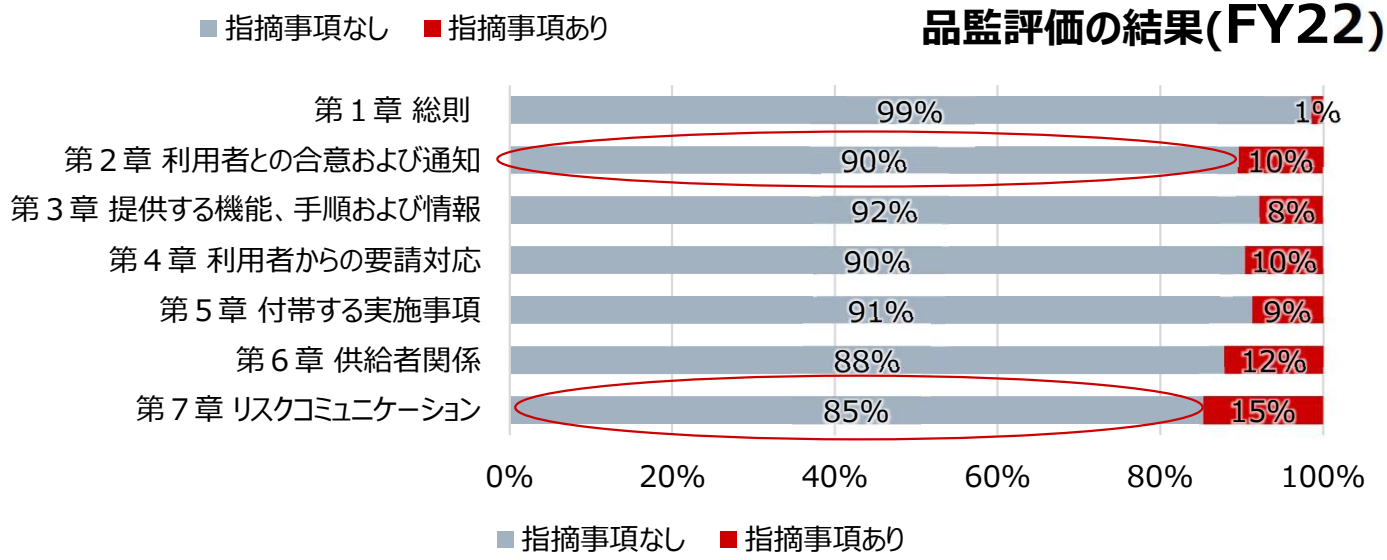
FY20からFY22の改善点

平均遵守率が68.6%→90.9%に改善

特に、第2章(セキュリティインシデントの報告手順を含む) ならびに
第7章(リスクコミュニケーション)において大幅な遵守率向上が見られる。



平均遵守率
68.6%



平均遵守率
90.9%

その他の改善

- 新規サービスの自発的な提出
  - 新規サービス審査実施数 2件(FY20) → 4件(FY22)
  - 企画・設計段階でも相談を受ける事例が増加
- フォローアップ率※の減少

  ※フォローアップ率: 審査において指摘事項が残り、フォローアップ審査に回った率

  77%(FY20) → 36%(FY22)
- ISO27017新規認証取得
  - TIS社内: 毎年1サービスずつ増加
  - TIG※: 1社(2サービス)に対して支援実施中

    ※TIG: TISインテックグループ
- TIG各社の審査が浸透
  - グループ会社新規事業開発部門から審査要請あり

結論

問題解決の度合い

- クラウドセキュリティ基準を遵守するという文化が根付いてきている
  - ✓ チェックリストでセルフチェックして、品質監査室に提出して指摘・助言をもらうということが当たり前になりつつある。
  - ✓ 企画・設計段階でも品質監査室による確認を必須化する組織が出てきた。
- クラウドセキュリティ点検がサービスの価値を上げることにつながるという共通認識が芽生えた
  - ✓ ローンチ前のセルフチェック・提出だけでなく、企画や設計段階でチェックリストを確認して、品質監査室に相談する事例が増えてきている。
  - ✓ 「当たり前品質から魅力品質へ」の意識が根付き始めた。
- 提出されたチェックリストに対し遅滞なく、適切な指摘・助言ができる体制は確立できた

今後の課題

- 形骸化防止
  - 認証ロゴの有効活用

    - ✓ 社内外にロゴを通じてアピールすることでセキュリティ意識を向上
  - 審査結果や成果の可視化
    - ✓ 社内ポータルサイトで審査済サービス一覧を公開
  - 弱点克服に注力した指摘・助言
    - ✓ 前年度のチェックリストを出して終わり、ではなく、成長を促す指摘
- 認知度向上
  - クラウドサービスのセキュリティ品質向上が競争優位性をもたらすことを営業に着信
    - ✓ 営業部門向け説明会実施。提案書差し込み資料作成。
  - グループ会社に対してさらに展開拡大
  - 対外発信にも注力して当社のプレゼンス向上に寄与

    本日の発表も認知度向上活動の一環です