

2021年12月22日
SCSK株式会社

SCSK、NRI、NTT データ 3 社共同で『金融機関向け 「Google Cloud」対応セキュリティリファレンス』を無償で提供

～ FISC の「金融機関等コンピュータシステムの安全対策基準・解説書」
第 9 版令和 2 年 3 月版に対応 ～

SCSK 株式会社(本社:東京都江東区、代表取締役 執行役員 社長 最高執行責任者:谷原 徹、以下「SCSK」)、株式会社野村総合研究所(本社:東京都千代田区、代表取締役会長兼社長:此本 臣吾、以下「NRI」)、株式会社エヌ・ティ・ティ・データ(本社:東京都江東区、代表取締役社長:本間 洋、以下「NTT データ」)、の 3 社は共同、『金融機関向け「Google Cloud」対応セキュリティリファレンス』(以下「本リファレンス」)を 2021 年 12 月 22 日から無償で提供します。本リファレンスは 3 社共同で作成し、公益財団法人 金融情報システムセンター(以下「FISC」)が提供する「金融機関等コンピュータシステムの安全対策基準・解説書」第 9 版令和 2 年 3 月版に対応しています。

1. 背景

金融機関が安全にクラウドサービスを利用するためには、FISC の「金融機関等コンピュータシステムの安全対策基準」(以下「FISC 安全対策基準」)を満たす必要があります^(注 1)。一方、FISC 安全対策基準の項目は多岐にわたっており、金融機関がクラウドサービスに対して行う確認作業が負荷になっています。これまでクラウドサービスの FISC 安全対策基準への対応状況を確認・整理した対応表などの提供が望まれていました。

そこで今回、SCSK、NRI、NTT データの 3 社共同で、Google Cloud の協力のもと、金融機関におけるクラウドサービスの活用促進のために、FISC 安全対策基準第 9 版令和 2 年 3 月版の 309 項目(統制基準、実務基準、設備基準、監査基準)への Google Cloud™ の対応状況を示すセキュリティリファレンスを作成しました。

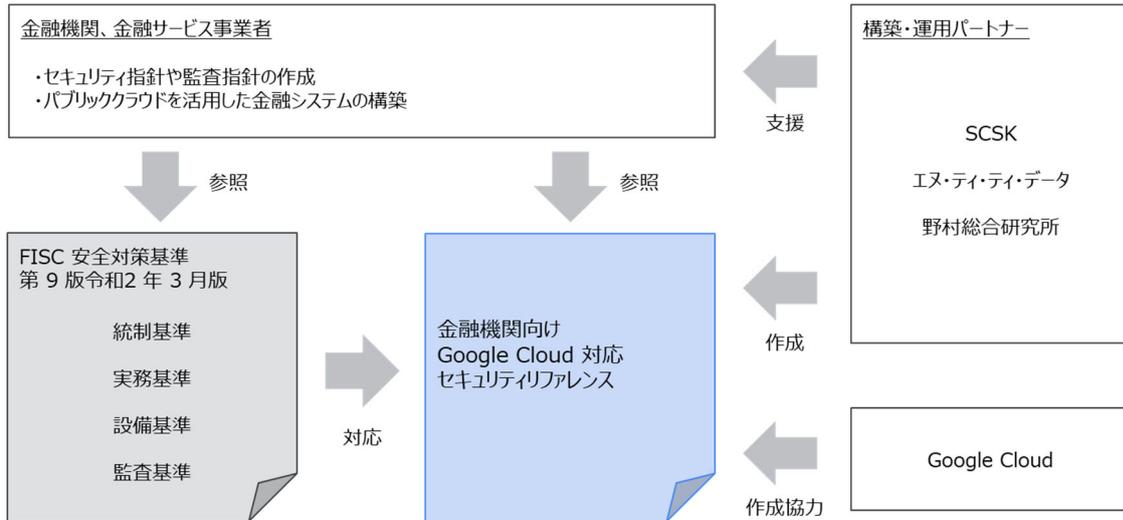
注 1:ほかにも金融庁の監督指針や検査マニュアルなどがあります。

2. 本リファレンスの概要と活用イメージ

本リファレンスの概要と活用イメージは図 1 の通りです。金融機関は本リファレンスを参照することで、セキュリティ指針や監査指針の作成、クラウドサービスを活用した金融システムの構築にかかる負荷を減らすことができます。SCSK、NRI、NTT データの 3 社はリファレンスの提供だけでなく、構築、運用パートナーとしてこれら金融機関を支援します。

図 1 :本リファレンスの概要と活用イメージ

セキュリティ リファレンスの活用イメージ



3. 本リファレンスの構成

リファレンスの構成は図 2 の通りです。「ガイドラインの項目」は、FISC 安全対策基準の基準番号を示しています(注²)。「Google の対応内容」はコントロールマッピング(注³)記載の Google Cloud の対応状況を示しています。「お客様による対応」は、必要となる対応概要とその対応に向けて参考になる対応策や参考 URL を示しています。

図 2:本リファレンスの構成

ガイドラインの項目	Google の対応内容 (コントロールマッピング抜粋)	お客様による対応 (クラウド視点でお客様が対応すべき内容を記載)
基準番号 実31	Google の対応状況 Google は ISO27001 認証を受けています。この基準では、「情報セキュリティの意識向上、教育および訓練」(ISO 27001 2013、附属書 A.7.2.2) が規定されています。セキュリティに対する意識向上や研修をはじめとする、情報セキュリティの監督管理体制は、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google の全社員および委託業者は、初期研修に組み込まれたセキュリティ研修に加え、在籍期間中も継続的にセキュリティ研修を受けています。新規の社員および委託業者は初期研修で Google が行動規範に同意します。この行動規範では、Google が顧客データを安全に保護する義務を負うことが定められています。職務に応じて、専門的なセキュリティ研修が追加で義務付けられている場合もあります。たとえば、情報セキュリティ チームに配属されたエンジニアは、安全なコーディング方法、プロダクト設計、脆弱性自動テストツールなどについて指導を受けます。エンジニアはこの他にも、セキュリティ関連の技術プレゼンテーションへの出席や、新規の脅威、攻撃パターン、防御技術などを紹介するセキュリティ関連ニュースレターの購読などを職務の一環として行っています。	お客様による対応 【概要・説明】 ・ Google Cloud コンソールの画面はレイアウトが予告無く変更される。そのため、オペレーション習熟のための教育・訓練の頻度については従来よりも向上させる必要がある。 【対応策例】 【参考文献、参照 URL】
実32	Google は ISO27001 認証を受けています。この基準では、「マルウェアからの保護」(附属書 A.12.2) が規定されています。脆弱性管理に関する統制についても、第三者機関によるレビューと検証を受け、SOC 2、Type II の報告書を取得しています。 Google はセキュリティ上の脅威を積極的に探索する脆弱性管理プロセスを実施しています。この管理プロセスは、一般に流通しているツールと独自の社内ツール、自動および手動による集中的な侵入試行、品質保証プロセス、ソフトウェアセキュリティ審査、外部監査などで構成されています。脆弱性の追跡と対処は脆弱性管理チームが担当しています。改善が必要な脆弱性が見つかったと、その内容が記録され、重大度に応じて優先順位が設定され、オーナーが割り当てられます。脆弱性管理チームはこのような問題を追跡して、問題が解決したことが確認されるまで対応作業を続けます。また、Google はセキュリティ研究コミュニティのメンバーと連携して、Google のサービスやオープンソース ツールについて報告されている問題を追跡しています。セキュリティ問題の報告について詳しくは、 https://www.google.com/about/appsecurity/ をご覧ください。 Google Cloud のお客様は、適切なウイルス対策の設定など、お使いの環境を設定、管理するすべての権利と責任を保有します。	【概要・説明】 ・本項目はコンピュータウイルス感染時に備え、防御・検知・復旧の手順を整えておく、というものである。 ・各手順について、防御は【実20】、検知は【実21】、復旧は【実22】で整理しているので、それらを統合した手順を用意すること。 【対応策例】 【参考文献、参照 URL】 ・ Google Cloud security foundations guide https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

注2:要求事項については、FISC 安全対策基準の本紙を参照ください。

注3:「コントロールマッピング」とは、FISC 安全対策基準の各項目に対して、Google Cloud による対策の状況を整理したものです。詳細については、次の Web サイトをご参照ください。

<https://cloud.google.com/security/compliance/fisc-japan>

4. 本リファレンスの入手方法

下記の URL から、ダウンロードできます。

<https://form.scsk.jp/public/application/add/19342>

5. グーグル・クラウド・ジャパン合同会社 上級執行役員 パートナー事業本部 石積 尚幸様からのコメント

「金融業界に知見のある SCSK 株式会社、株式会社野村総合研究所、株式会社エヌ・ティ・ティ・データ 作成の本リファレンスの公開が、金融システムに携わる企業にとって最適な形で Google Cloud を導入いただき、デジタルトランスフォーメーション(DX)のさらなる推進に貢献できることを歓迎いたします。」

本件に関するお問い合わせ先

【本リファレンスに関するお問い合わせ先】

SCSK 株式会社

ソリューション事業グループ

基盤サービス事業本部 サービス開発推進部

E-mail:gcp-sales@ml.scsk.jp

【報道関係お問い合わせ先】

SCSK 株式会社

企画本部 広報部 高野

TEL:03-5166-1740

※Google Cloud は Google LLC の商標です。

※記載された内容は発表日現在の情報です。また、文中に記載された会社名および製品名などは該当する各社の登録商標または商標です。