NRI SECURE

金融庁 令和6年10月4日 公表
「金融分野におけるサイバーセキュリティに関するガイドライン」

Secure SketCH の
金融ガイドライン対応評価サービス（簡易・詳細）ご紹介

Secure SketCH

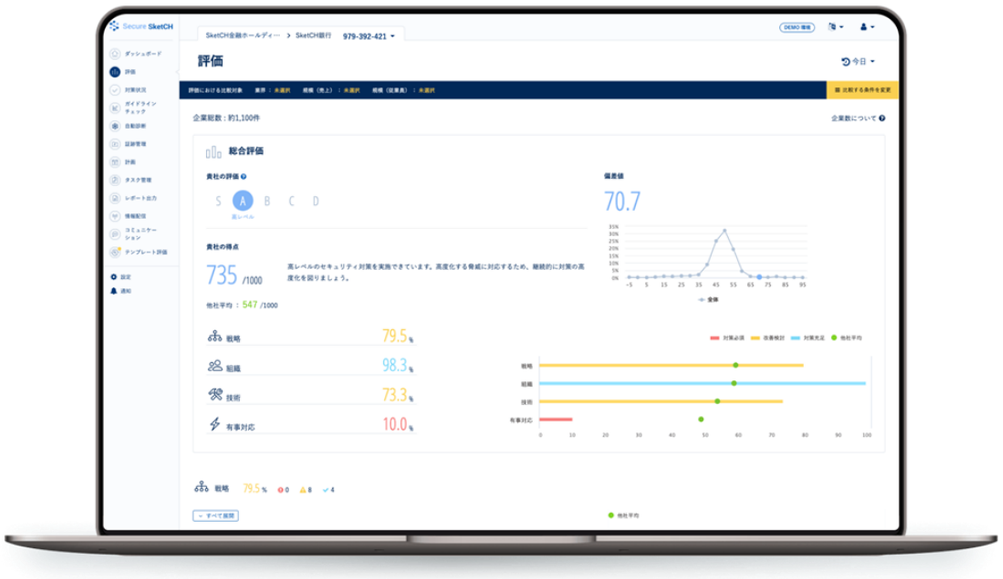
Ver2.1 更新日 2024/12/19

はじめに

金融庁は令和6年10月4日に、金融機関における近年のサイバーリスクの深刻化に対処していくために
「**金融分野におけるサイバーセキュリティに関するガイドライン**」を公表しました。

Secure SketCHでは、金融機関各社が抱える課題を踏まえ、課題の解決および金融ガイドラインのさらなる活用・浸透を促進するべく
金融ガイドラインの対応評価サービス（簡易・詳細）の提供を開始いたしました。
本資料では金融ガイドラインの要点、ならびにSecure SketCHを活用した対応評価アプローチをご紹介いたします。

Secure SketCH | GOOD DESIGN AWARD 2022年度受賞



金融ガイドライン対応
評価サービス（簡易・詳細）の提供開始

❶：簡易評価サービス

ガイドラインチェック機能にて、すばやく・簡単に把握

■ メリット
・標準設問の既存回答の活用
・関係者への迅速な共有

❷：詳細評価サービス

NRIセキュアが作成した専用テンプレートへの回答で詳細に把握（オプション）

■ メリット
・ベストプラクティスの把握
・定量的な評価、ベンチマーク
・サプライチェーン展開への柔軟性

目次

「金融分野におけるサイバーセキュリティに関するガイドライン」を公表

直近3年間、金融機関各社はG7・当局が公開するガイドライン等を踏まえサイバーセキュリティ高度化に取り組んできた。
2024年10月にこれらの集大成として、当局が「金融分野におけるサイバーセキュリティに関するガイドライン」を公表。

2022年

2022.2　金融庁

「金融分野におけるサイバーセキュリティ強化に向けた取組方針」のアップデート

2022.10　G7 基礎的要素（FE）

「金融セクターのランサムウェアに対するレジリエンスに関する**G7の基礎的要素**」公表

2023年

2023.4　日銀・金融庁

「地域金融機関向けサイバーセキュリティ**セルフアセスメント（CSSA）**」の集計結果を公開

2023.5　G7・金融庁

「国際セミナー “G7 Cybersecurity Seminar 2023” 」開催

2024年

2024.6　金融庁

「金融分野における サイバーセキュリティに関する ガイドライン」(案)の公表

2024.10

「金融分野における サイバーセキュリティに関する ガイドライン」の正式公表

サイバーセキュリティの対応事項を網羅

当局のガイドラインは【基本的な対応事項】と【対応が望ましい事項】より計176事項で対応事項が網羅されている。

金融分野におけるサイバーセキュリティに関する
ガイドライン

令和６年 10 月４日
金融庁

本ガイドラインの構成及び事項数

カテゴリ			サブカテゴリ	基本的な対応事項数	対応が望ましい事項数
2.1	サイバーセキュリティ管理態勢の構築	2.1.1	基本方針、規程類の策定等	9	5
		2.1.2	規程等及び業務プロセスの整備	2	0
		2.1.3	経営資源の確保、人材の育成	4	0
		2.1.4	リスク管理部門による牽制	2	1
		2.1.5	内部監査	2	1
2.2	サイバーセキュリティリスクの特定	2.2.1	情報資産管理	6	5
		2.2.2	リスク管理プロセス	12	7
		2.2.3	ハードウェア・ソフトウェア等の脆弱性管理	6	1
		2.2.4	脆弱性診断及びペネトレーションテスト	1	4
		2.2.5	演習・訓練	5	4
2.3	サイバー攻撃の防御			1	0
		2.3.1	認証・アクセス管理	8	0
		2.3.2	教育・研修	5	2
		2.3.3	データ保護	5	2
		2.3.4	システムのセキュリティ対策	19	8
2.4	サイバー攻撃の検知			2	0
		2.4.1	監視	7	3
2.5	サイバーインシデント対応及び復旧	2.5.1	インシデント対応計画及びコンティンジェンシープランの策定	1	1
		2.5.2	インシデントへの対応及び復旧	19	1
2.6	サードパーティリスク管理			10	5
計				126	50

【基本的な対応事項】：126事項

規模や特性によらず、全ての金融機関様が実施すべき対応事項

【対応が望ましい事項】：50事項

どの金融機関も自組織としてどのようなリスクが残存しているか把握しておく必要があるため評価対象とすることを推奨

ただし、サイバー攻撃を受けた際の対外的な影響度等は各金融機関様ごとに異なるため、対策の実施要否・実施時期については、それぞれのリソース状況やコスト等を勘案して判断するのが一般的

経営層や現場とのリスクコミュニケーションが重要

本ガイドラインにおける「基本的な対応事項」の記載項目を踏まえると、金融機関のサイバーセキュリティの責任者にはこれまで以上に経営層や現場担当者の興味・関心を引き付けるようなリスクコミュニケーションが重要となる。

基本的な対応事項
ガイドラインから抜粋

2.1. サイバーセキュリティ管理態勢の構築

2.1.1. 基本方針、規程類の策定等

⑧ 経営陣は、**少なくとも１年に１回、以下の報告**を担当部署等に求めること
- **自組織を取り巻くサイバーセキュリティリスク**の状況
- **サイバーセキュリティに関するリスク評価**の結果
- **取組計画の進捗**状況

2.1.4. リスク管理部門による牽制

② リスク管理部門は、**サイバーセキュリティ管理の実施状況について、リスク管理担当役員（CRO 等）及び取締役会等に報告**すること。

報告/共有のあるべき姿

経営陣/役員
（企業の代表としての統括責任）

サイバーセキュリティの責任者
（両隣りをつなぐ経営と技術の通訳）

サイバーセキュリティ対策の現場
（事業/グループ/拠点/委託先など）

統一した指標・分かりやすいデータを活用したリスクコミュニケーションを実施することが重要

経営層や現場の疑問に対する、判断材料を用意すべき

リスクコミュニケーションの質を上げるためには、経営層や現場担当者の疑問に対して、有益な判断材料・指示材料の提示が求められる。

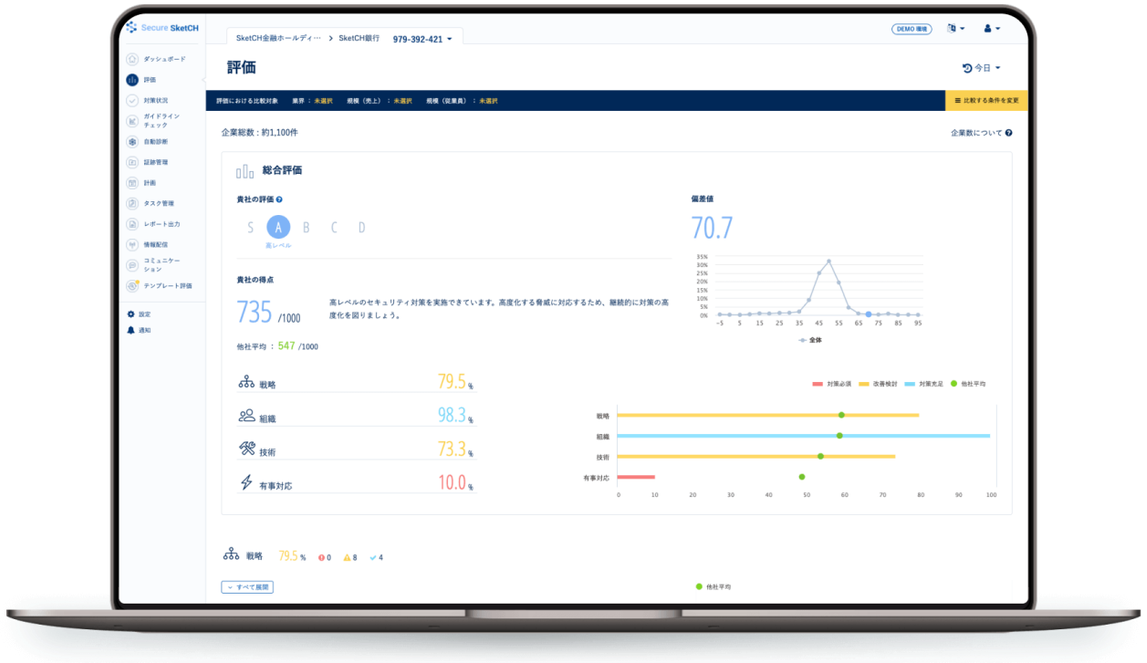
	経営陣/役員 （企業の代表としての統括責任）	サイバーセキュリティの責任者 （両隣りをつなぐ経営と技術の通訳）	サイバーセキュリティ対策の現場 （事業/グループ/拠点/委託先など）
報告/共有のあるべき姿	統一した指標・分かりやすいデータを活用したリスクコミュニケーションを実施することが重要		
	一層 	二層 	三層 
	責任者が示すべき判断/指示材料の例		
疑問と判断材料	責任ある企業として、ガイドラインに最低限の対応ができているか？ 他の金融機関と比較して、自社の対応状況はどうなのか？	対応事項と実態のギャップ分析結果 ベンチマーク情報 （他金融機関の対策状況/平均スコアなど） 具体的に必要な対策/ベストプラクティス 対策を実施しない場合のリスク情報	具体的な改善活動は何をすべきか？ なぜ改善を実施する必要があるのか？ 優先的に対応すべきなのか？

金融ガイドライン対応を、Secure SketCHが支援

Secure SketCHでは「金融分野におけるサイバーセキュリティに関するガイドライン」とのフィット＆ギャップの把握、具体的な対策の理解、他の金融機関とのベンチマークを、低コスト・高品質・スピーディーに実施いただける金融ガイドライン対応評価サービスを提供いたします。

Secure SketCH

GOOD DESIGN AWARD 2022年度受賞



3つの強み・ポイント

- **評価結果が数値でわかる**（全体/カテゴリ別スコア、偏差値）
- **ベンチマークできる**（他金融機関と相対比較が可能）
- **対策やリスクがわかる/更新できる**（継続的セキュリティ強化）

金融機関向け、2つの評価サービス

❶ 簡易評価

ガイドラインチェック機能にて、すばやく・簡単に把握

- 標準設問の既存回答の活用
- 関係者への迅速な共有

❷ 詳細評価：オプション提供

NRIセキュアが作成した専用テンプレートへの回答で詳細に把握

- ベストプラクティスの把握
- 定量的な評価、ベンチマーク
- サプライチェーン展開への柔軟性

❶：簡易評価

金融ガイドラインへの対応状況を、素早く簡単に把握

ガイドラインチェック機能において金融ガイドライン（176項目）への対応状況を、すばやく・簡単に把握できます。

Secure SketCHの利用企業者様は、既存の標準設問の回答を活かしてギャップ分析が可能です。

ガイドラインチェック機能の閲覧画面

10種類以上のガイドラインの準拠状況がわかる

金融ガイドラインの6つのカテゴリー別に実施率がわかる

金融ガイドラインの176項目ごとに回答を更新できる

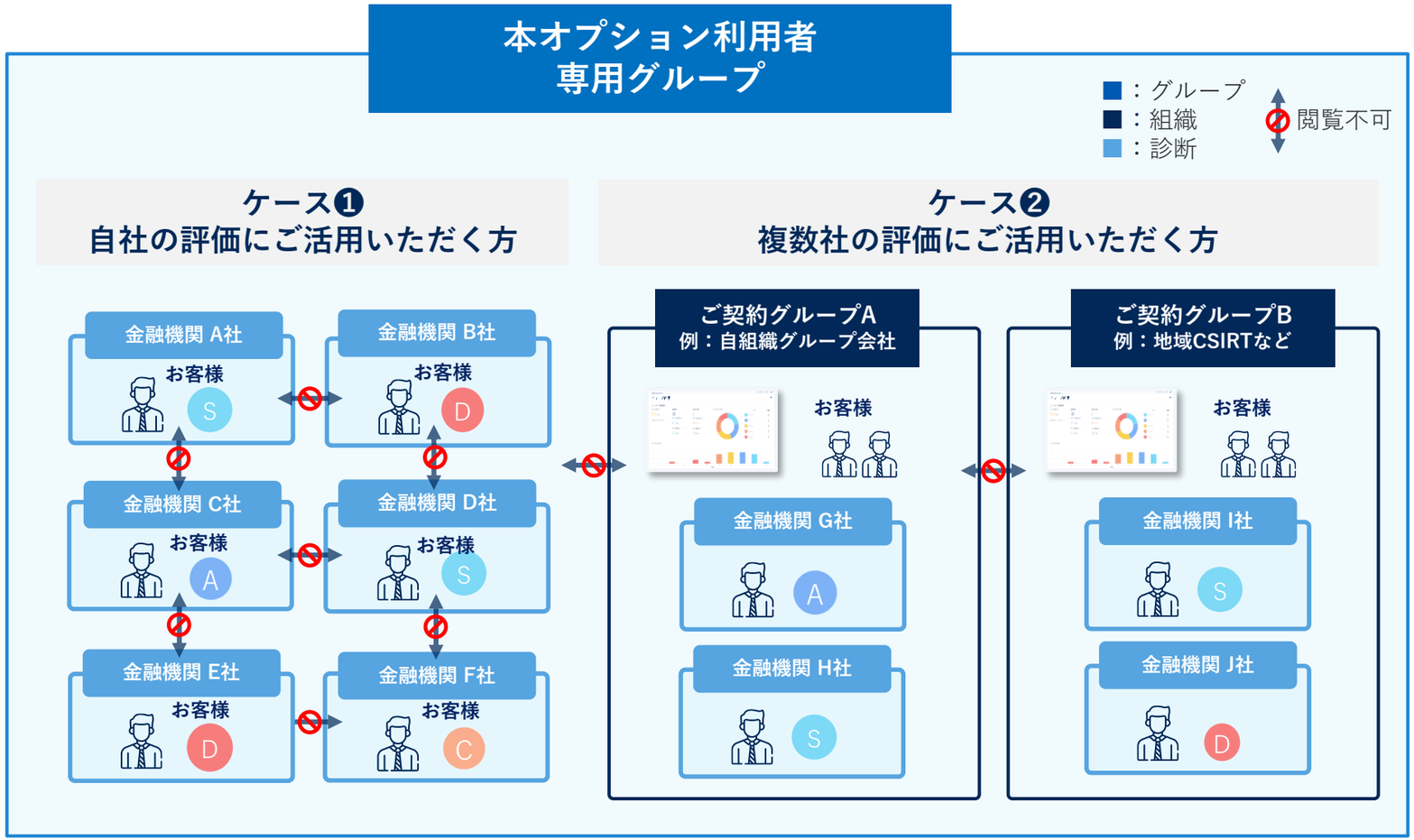
Secure SketCH Point

- Secure SketCH 標準設問に回答するだけで、対応状況が可視化される（既存回答の活用）
- 対応状況がすぐに可視化されるため、ステークホルダーへの迅速な共有が可能（QuickWin）

❷ 詳細評価：オプション提供

本オプションご契約者様に、専用の環境を用意いたします

本オプションを利用する各金融機関様は、NRIセキュアが用意した専用のグループ環境に所属いただきます。
当局ガイドラインのギャップ分析と定量評価の自動化、各金融機関の評価結果を統計データとして確認が可能になります。



専用グループ所属で得られるメリット

ケース❶ 自社の評価にご活用いただく方

- 当局ガイドラインに対するフィット＆ギャップ分析と定量評価を、NRIセキュアが定義した評価ロジックにより自動化できる
- 専用グループに所属する、他の金融機関の評価結果を統計データとして参照できる
- NRIセキュアが用意した、当局ガイドラインの各項目における対策/ベストプラクティや、未対策リスクなど参考情報がわかる

ケース❷ 複数社の評価にご活用いただく方

- 上記に加え、ご契約をいただいた複数社のグループ単位で評価結果を一元的に管理し横比較ができる

NRIセキュア独自の評価項目：271項目に回答

ケース❶
自社の評価

本ガイドラインの要求事項を踏まえてNRIセキュアが独自に作成した評価項目：271項目に対し、具体的な対策の実施例やリスクなど、専門家のナレッジを確認しながらフィット＆ギャップを把握いただけます。

ガイドライン原文

2.1. サイバーセキュリティ管理態勢の構築

2.1.1. 基本方針、規程類の策定等

【基本的な対応事項】

① 取締役会等は、サイバーセキュリティリスクを組織全体のリスク管理の一部としてとらえ、サイバーセキュリティ管理の基本方針を策定すること。サイバーセキュリティ管理の基本方針には、例えば、以下の事項を記載すること。
- セキュリティ対策の目的や方向性
- 関係主体等（顧客、地域社会、株主、当局等）からの要求事項への対応及び法規制等への対応
- 経営陣によるコミットメント

金融ガイドラインに対応した専門テンプレートの回答画面

2.1【基本的な対応事項】サイバーセキュリティ管理態勢の構築　全43問

2.1.1.基本方針、規程類の策定等

2.1.1.1-1 必須　　コメント (0)

【2.1.1.①-1】サイバーセキュリティ管理の基本方針を文書化しており、以下の項目の内容をすべて含んでいること。

1.セキュリティ対策の目的や方向性
2.関係主体等（顧客、地域社会、株主、当局等）からの要求事項への対応及び法規制等への対応
3.経営陣によるコミットメント

■ガイドライン原文
2.1.1①基本的な対応事項
取締役会等は、サイバーセキュリティリスクを組織全体のリスク管理の一部としてとらえ、サイバーセキュリティ管理の基本方針を策定すること。サイバーセキュリティ管理の基本方針には、例えば、以下の事項を記載すること。
・セキュリティ対策の目的や方向性
・関係主体等（顧客、地域社会、株主、当局等）からの要求事項への対応及び法規制等への対応
・経営陣によるコミットメント

■NRIセキュアによる参考情報:補足・実施例
・【補足】情報セキュリティの基本方針等の中に、サイバーセキュリティに関する項目が含まれているなど、サイバーセキュリティの基本方針が独立していることは必須ではないものの、サイバーセキュリティが重要なリスクとして取り扱われていることがわかるよう、明確にサイバーセキュリティの基本方針が定められている必要がある。

・【例】サイバーセキュリティ管理の基本方針が整備され、目的と方針、および参考にしている国内外の基準やガイドラインが記載されている。

■NRIセキュアによる参考情報:未遵の場合のリスク
サイバーセキュリティに関する対策の目的や方向性が示されないため、一貫性のある対策が推進できず、結果として想定外のリスクが残存するおそれがある。

回答（単一回答）
○: 実施できている
△: 概ね実施できている
▲: 一部のみ実施できている
×: 実施できていない
－: 該当なし（想定リスクなし）

専門家のナレッジ

ガイドラインの要求事項を踏まえた評価項目（独自271設問）

ガイドライン原文

NRIセキュアが作成した参考情報
・補足/対策の実施例
・未対応の場合のリスク

お客様によるセルフ回答
・5段階基準

金融ガイドライン対応を促進を可能にするSecure SketCHのその他の特徴

☑ 複数メンバで共同回答ができる
☑ いつでも回答を更新/修正できる
☑ 各設問ごとに証跡を管理できる

回答内容に基づいた成熟度やスコアに加えベンチマーク情報がわかる

ケース❶
自社の評価

回答結果に基づきスコアリングレポートが即時で表示されます。5段階のランク、スコア、カテゴリごとの遵守率に加え、他金融機関の平均スコアや全体順位、偏差値などベンチマーク情報が得られます。　（※2024年12月時点、約120社との比較可能）

スコアリング

評価ランク

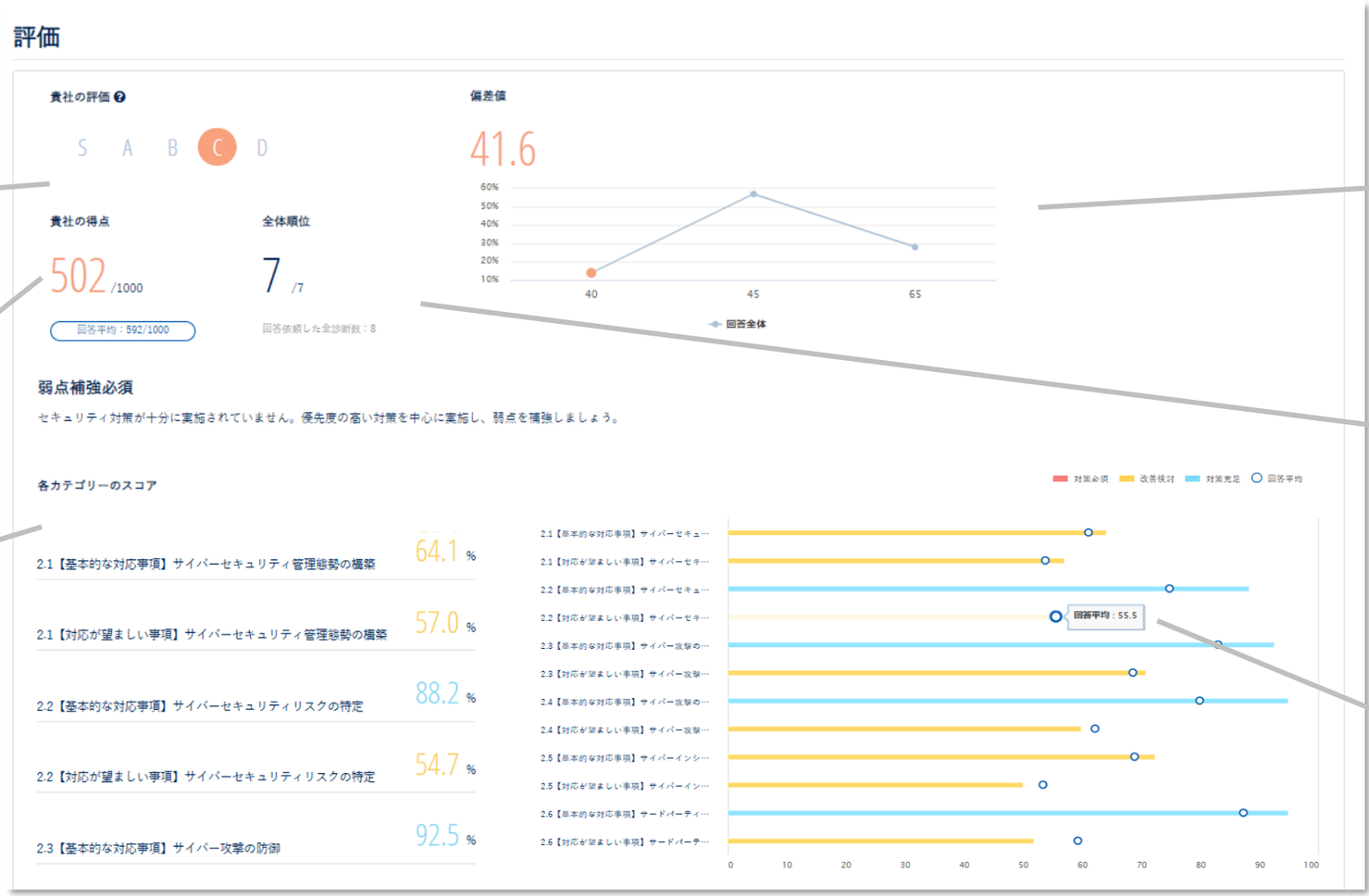
ランクはS・A～Dの５段階で表示

評価スコア

1000点満点のスコアで表示

各カテゴリーの遵守率

・基本的な対応事項
・対応が必要な事項
　ごとに、遵守率を表示



ベンチマーク

偏差値

総合スコアを点数で表示

平均スコア

同設問に回答した
他金融機関の平均スコア

全体順位

同設問に回答した
金融機関内における順位

平均遵守率

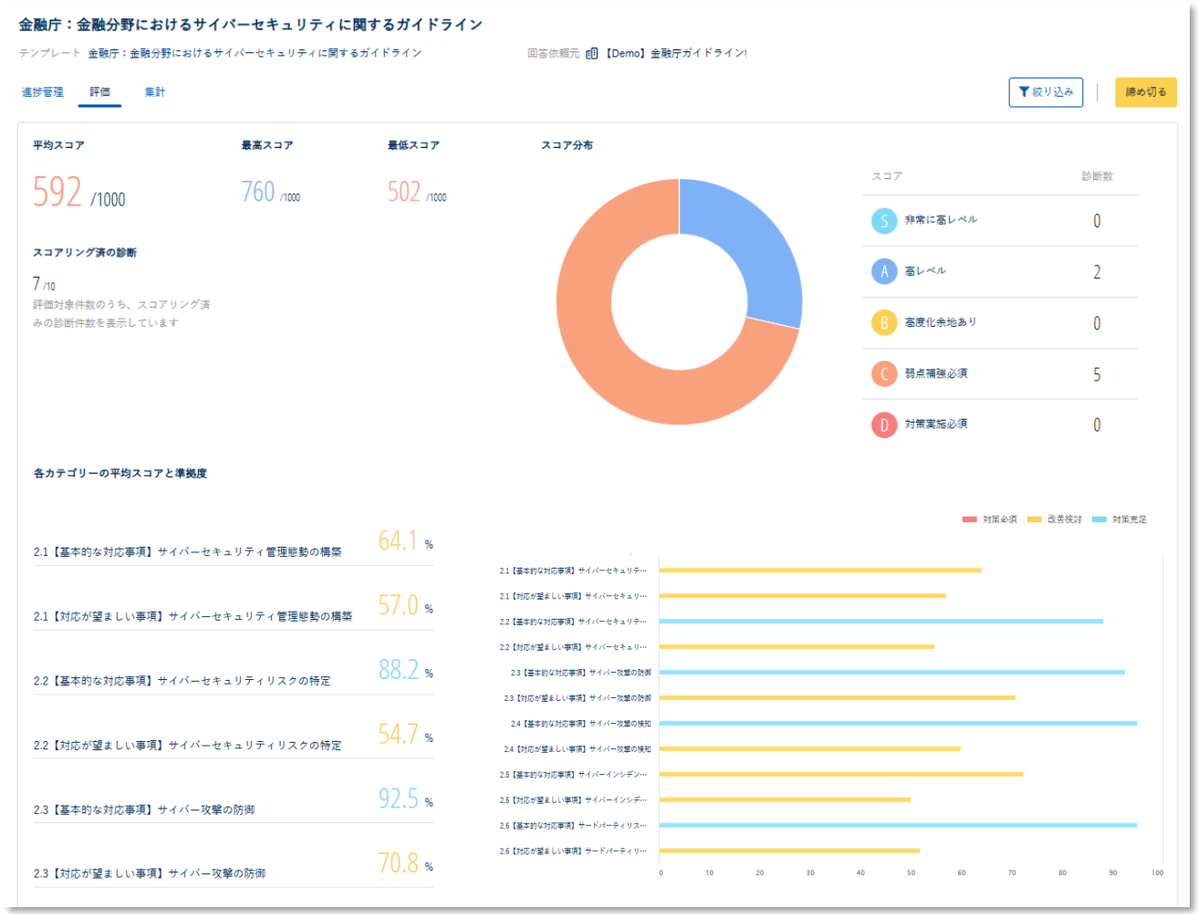
同設問に回答した
金融機関内の、各カテゴリーにおける平均遵守率

グループ管理機能で共助の取組みを実現（複数社の同時契約の場合に限る）

ケース❷
複数社の評価

グループ管理機能でグループ会社やコミュニティ/業界団体など、複数の企業の評価結果を一覧で管理いただけます。
複数社での共助の取組みに加え、金融ガイドラインが要請するサプライチェーン全体への展開や統制も行えます。

グループ管理機能で、各社の平均スコアや分布がわかる



本ガイドラインでも、複数社での共助の取組みを推奨

1.3. 業界団体や中央機関等の役割

サイバー空間における脅威情報や、最新の攻撃手法の動向の把握等について、個別金融機関等による対応のみでは必ずしも効率的・効果的ではない場合がある。特に、規模が小さい又は取引範囲が限定的な金融機関等においては、十分な情報や対応のノウハウの蓄積が困難なことも考えられる。

我が国金融セクター全体の底上げの観点からは、業界団体や中央機関等が、必要に応じて当局と連携しながら、金融機関等にとって参考とすべき情報や対応事例の共有、態勢構築に関する支援その他業態全体のサイバーセキュリティ強化のための活動（演習、シナリオ分析[6]、人材育成など）等の共助の取組みを推進することにより、金融機関等による対応の向上に中心的・指導的な役割を果たすことが望ましい。

各社のスコアや準拠率を一覧で管理できる

金融ガイドライン対応評価サービスの提供概要

1)提供方法・期間：

Secure SketCHでの提供（年間ライセンス、個別見積り）となります

2)利用可能企業：

金融ガイドライン対応評価サービス（簡易・詳細）は、

・規模や地域を問わず、あらゆる金融機関にご利用いただけるサービスです

・Secure SketCHの既存利用状況を問わず、新規利用要望にも対応いたします

・自社（1社だけ）の評価でも、複数社（グループ/コミュニティ等）の評価でもご利用いただけます

3)前提条件（必要となるSecure SketCHプラン）

❶ 簡易評価サービス、❷ 詳細評価サービス：オプション提供の、どちらの場合においても

SINGLE PREMIUM、GROUPS PLUS/PREMIUMのご契約が必要でございます

重要インフラから小規模事業者までどんな企業様にもマッチ

導入企業7000社、グローバル98ヵ国、重要インフラから小規模事業者まで、幅広い企業様のご利用実績がございます。
当局ガイドラインの対応評価サービスに関して、ご興味のある企業様は、お気軽にお申し付けください。

利用実績（2024/12月時点）

会員数	日経225企業の利用率	グローバル利用実績
7,000 社	39 %	98 ケ国

Z HOLDINGS / 日テレ / brother / MUFG 三菱UFJフィナンシャル・グループ / au カブコム証券 A member of MUFG / NTN / hulu / フジ・メディア・ホールディングス / 乾汽船 / 丸三証券
SEVEN HOLDINGS / GREE / Daiichi-Sankyo / YAMAHA Revs Your Heart / 日産証券 / Sonic Garden / TimeTree / AVANT GROUP / Anritsu / RELO GROUP
SEVEN BANK セブン銀行 / MACROMILL / 明治安田生命 / KURASHICOM / SBS リコーロジスティクス / Kyash / ZOJIRUSHI / ARTERIA アルテリア・ネットワークス株式会社 / アディーレ法律事務所 / MARVELOUS
NIKKO CHEMICALS / YANMAR / PERSOL パーソル キャリア / 京都銀行 / LIFULL / J's Communication / one visa / TTK / プラスアルファコンサルティング / AUCNET

セキュアスケッチ

詳しく見る

お問合せ先：support@secure-sketch.com

詳細な説明やデモのご要望も承ります。

お気軽にお問い合わせください。

support@secure-sketch.com

サービスサイト　https://www.nri-secure.co.jp/service/solution/secure-sketch

NRIセキュア ブログ　https://www.nri-secure.co.jp/blog

NRI SECURE