セキュリティ対策実行支援プラットフォーム

Secure SketCH

＼2025年9月実施予定／

Secure SketCH標準設問改定のお知らせ

Ver1.2　更新日 2025/5/7

NRI SECURE

Secure SketCH 標準設問を改定いたします（2025年9月を予定）

Secure SketCHでは、最新のセキュリティガイドラインや脅威に対応した継続的なセキュリティ評価と改善にご利用いただけるように、標準設問やベストプラクティスを定期的にアップデートしてきました。

Secure SketCHが参照するガイドライン・フレームワークの改定や脅威の変化等を踏まえ、 2025年9月に標準設問を改定いたします。

（※ 改定時期や内容は変更する可能性があります）

本資料では、標準設問改定における背景と改定ポイントをご説明いたします。

現在のSecure SketCH標準設問（項目数:75）

カテゴリ	分類	項目数
戦略	セキュリティリスク対応方針	6
	セキュリティ統制	6
組織	情報管理	2
	人材育成・教育	3
	物理アクセス制御	3
有事対応	災害発生時の対応	1
	インシデント対応態勢	3
	インシデント対応訓練	2

カテゴリ	分類	項目数
技術	構成管理・設定管理	6
	ネットワーク管理	6
	無線アクセス管理	2
	データ保護	3
	アカウント管理	5
	メール管理	2
	マルウェア対策	3
	境界防御	6

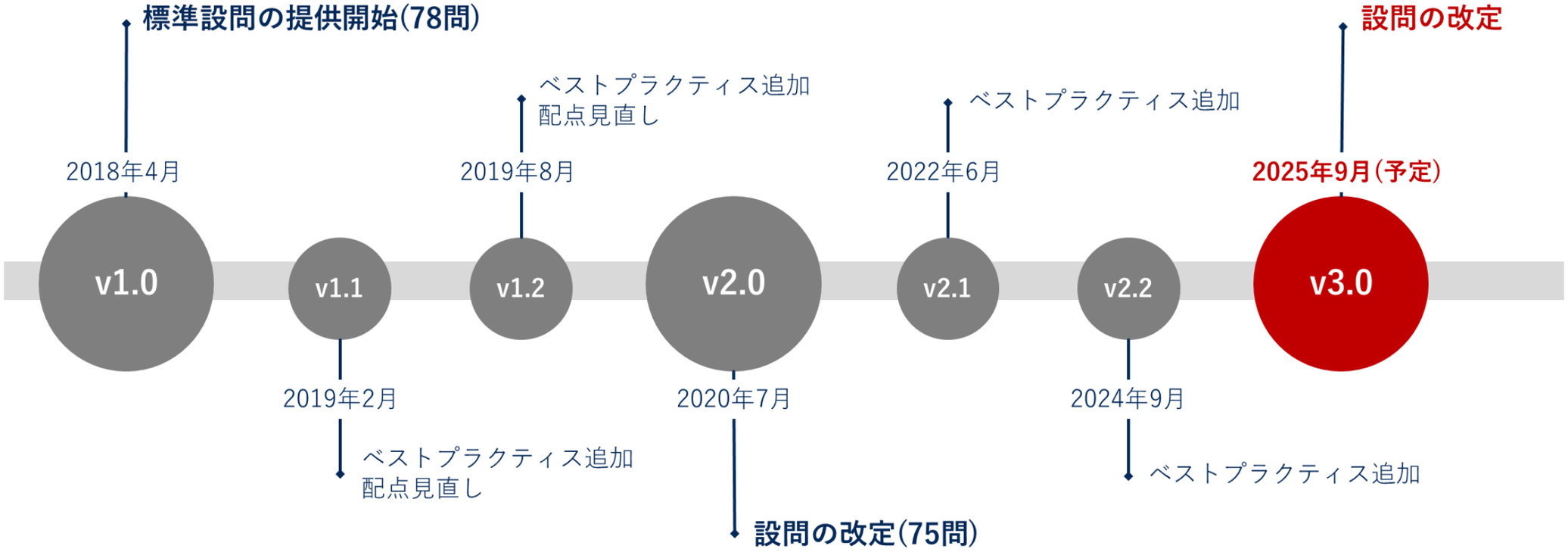
カテゴリ	分類	項目数
技術	クラウドサービス利用管理	4
	セキュリティログの管理・保管	4
	特権アクセス管理	2
	セキュアな開発・運用	6

回答基準：
未実施/一部実施/実施済/定期的に見直し/該当なし

標準設問の改定タイムライン

Secure SketCHでは、これまで定期的に標準設問（設問/回答基準/ベストプラクティス、配点など）をアップデートしてまいりました。2025年9月に、標準設問 v3.0 へと改定を予定いたします。

標準設問のタイムライン



Secure SketCHのヘルプセンターにて、過去実施した標準設問やベストプラクティスの改定履歴をご確認いただけます

Secure SketCH 標準設問とは（現在：v2.2）

企業のセキュリティ対策状況を網羅的に評価・可視化するための、NRIセキュアが独自に策定した設問です。
現在の設問は 2020年7月より提供しており、「4カテゴリ」「20分類」「75設問」で構成されています。

戦略	1	セキュリティリスク対応方針	01-1	セキュリティリスクの特定・評価
			01-2	セキュリティリスクへの対応計画策定・実施管理
			01-3	セキュリティリスク管理体制の構築
			01-4	脅威インテリジェンスの活用
			01-5	セキュリティリスクへの取り組みの開示
			01-6	サイバー保険への加入検討
	2	セキュリティリスク統制	02-1	法令・ガイドラインの把握・対応
			02-2	セキュリティポリシーの策定・周知
			02-3	人事サイクルへのセキュリティ対策の組み込み
			02-4	グループ会社のセキュリティ統制
			02-5	顧客・取引先等との責任分界点の明確化
			02-6	サプライチェーンのセキュリティ統制
組織	3	情報管理	03-1	情報資産の管理方針の策定
			03-2	情報資産の管理
	4	人材育成・教育	04-1	セキュリティ人材の育成
			04-2	従業員へのセキュリティ教育
			04-3	メールを使ったサイバー攻撃への対応能力向上
	5	物理アクセス制御	05-1	重要度に応じた物理ゾーニング
			05-2	施設入退室時の認証実施
			05-3	端末の物理的な管理
技術	6	構成管理・設定管理	06-1	ハードウェア資産の管理
			06-2	ソフトウェア資産の管理
			06-3	サーバなどのシステムの構成管理
			06-4	脆弱性管理プロセスの整備
			06-5	端末のセキュアな設定の標準化
			06-6	未許可ソフトウェアの利用制限
	7	ネットワーク管理	07-1	ネットワーク機器の構成管理
			07-2	ネットワーク構成の把握
			07-3	ネットワーク分離
			07-4	リモートアクセスの利用ポリシーの策定・周知
			07-5	リモートアクセスの制御
			07-6	外部からの不正な通信の検知（IDS、IPSの導入など）

技術	8	無線アクセス管理	08-1	無線通信の管理
			08-2	無線アクセスポイントの管理
	9	データ保護	09-1	通信データの暗号化
			09-2	保存データの暗号化
			09-3	データバックアップの取得・保護
	10	アカウント管理	10-1	アカウントの作成・棚卸
			10-2	アカウントの認証
			10-3	アクセス権の管理
			10-4	パスワードポリシーの策定・周知
			10-5	通常と異なるアカウント挙動の監視・是正
	11	メール管理	11-1	受信メールのセキュリティチェック
			11-2	送信メールのセキュリティチェック
	12	マルウェア対策	12-1	パターンファイルマッチングによるマルウェア対策
			12-2	振る舞い検知によるマルウェア対策
			12-3	マルウェア感染を想定した端末ログ取得・即時対応（EDRの導入など）
	13	境界防御	13-1	許可しない通信の拒否（FWの導入など）
			13-2	インターネットアクセスのログ取得（プロキシサーバの導入など）
			13-3	Webアクセスの制限（コンテンツフィルタリングの導入など）
			13-4	Webアプリケーションへの攻撃検知・対応（WAFの導入など）
			13-5	異常な通信量の増加への対応
			13-6	アプリケーション単位での不正な挙動の検知・制御
	14	クラウドサービス利用管理	14-1	クラウドサービス利用ポリシーの策定・周知
			14-2	クラウドサービス利用プロセスの整備
			14-3	クラウドサービスのセキュリティ設定
			14-4	クラウドサービス利用の可視化・制御

技術	15	セキュリティログの管理・保管	15-1	ログの取得
			15-2	ログの保管・保護
			15-3	ログの分析
			15-4	ログの相関分析
	16	特権アクセス管理	16-1	特権アカウントの利用プロセスの整備
			16-2	特権アカウント作業の事前申請と操作記録の突合
	17	セキュアな開発・運用	17-1	システム開発ライフサイクルのポリシー策定・適用
			17-2	セキュリティを考慮したシステム設計
			17-4	セキュリティを考慮したシステム運用
			17-6	侵入テストの実施
有事対応	18	災害発生時の対応	18-1	IT-BCPの整備
	19	インシデント対応態勢	19-1	インシデント対応方針の策定・周知
			19-2	インシデント対応マニュアルの策定・周知
			19-3	インシデント対応チームの組成
	20	インシデント対応訓練	20-1	インシデント対応チームの訓練
			20-2	組織横断的なインシデント対応訓練

標準設問の改定を実施する3つの背景

2025年9月に予定している標準設問：v3.0への改定において、世間のセキュリティガイドラインや脅威動向の変化、
7,000社が利用するSecure SketCHに寄せられたご意見・ご要望に対応します。

背景① 新しいガイドライン	参照するガイドライン・フレームワークの最新化
背景② サイバー攻撃のトレンド	世の中のセキュリティ脅威動向の変化
背景③ Secure SketCH 利用企業 （7,000社突破）	お客様からいただいたご意見・ご要望の増加

背景①：参照するガイドライン・フレームワークの最新化

Secure SketCHが参照するガイドライン・フレームワークの改定ポイントや要素を、標準設問：v3.0に反映します。

2020年7月 v2.0 → 2025年9月（予定） v3.0

参照するガイドライン・フレームワークの最新化

2021年5月	CIS Controls	v7.1 ➔ v8.0
2022年2月	ISO IEC 27002	2013 ➔ 2022
2023年5月	サイバーセキュリティ経営ガイドライン	v2.0 ➔ v3.0
2024年2月	NIST Cybersecurity Framework	v1.1 ➔ v2.0
2024年5月	NIST SP800-171	v2.0 ➔ v3.0

標準設問：v3.0 に反映・強化する観点（例）

戦略	セキュリティガバナンス（統治）の重要性強調 委託先・サードパーティリスク管理に関する項目追加 脅威インテリジェンスの活用促進、など
組織	セキュリティ人材拡充に関する対応方針の見直し 物理セキュリティの監視強化、など
技術	ゼロトラストセキュリティモデルの浸透 データ保護（マスキング/漏洩防止等）の強化、など
有事対応	サイバーレジリエンスの強化 インシデント発生時の情報共有・開示の促進、など

標準設問の改定背景：

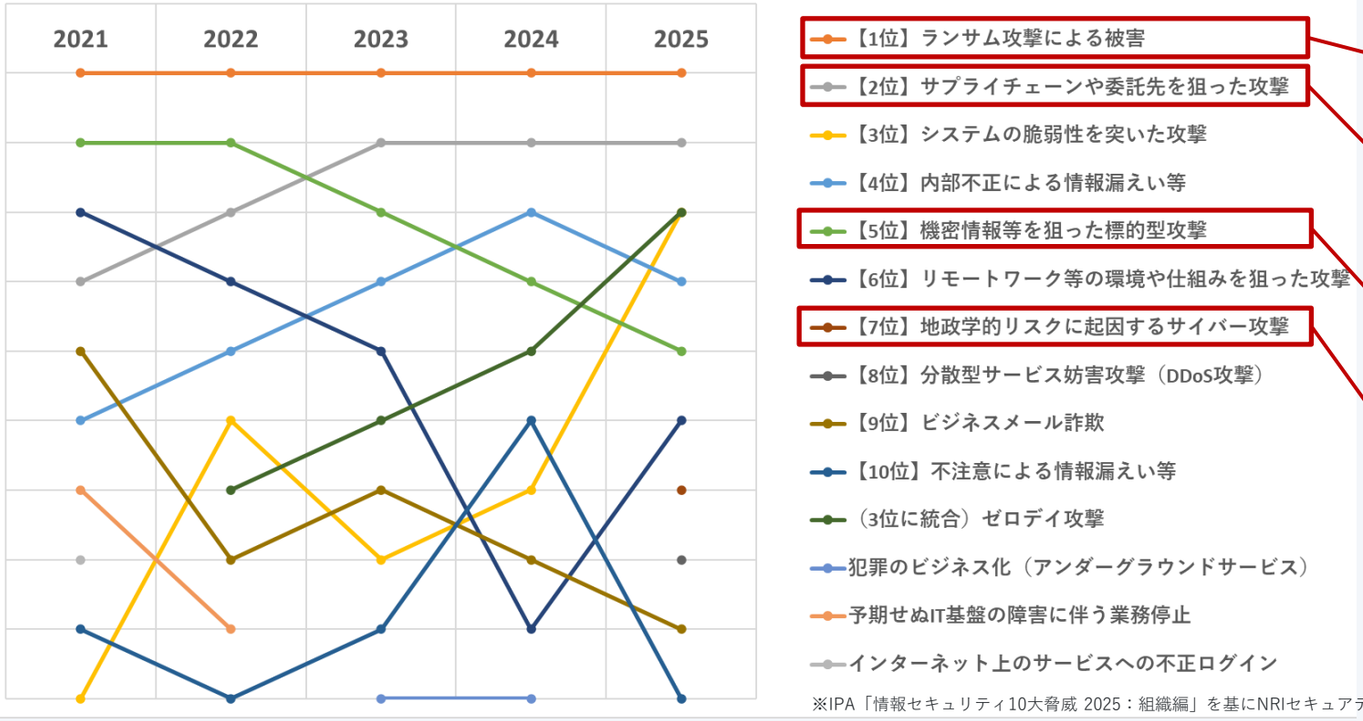
背景②：世の中のセキュリティ脅威動向の変化

変化し続けるサイバー脅威に備えるべく、新しい対策分野や見直しポイントを、標準設問：v3.0に反映します。

2020年7月 v2.0

2025年9月（予定） v3.0

脅威動向の変化（IPA10大脅威［組編］）



※IPA「情報セキュリティ10大脅威 2025：組織編」を基にNRIセキュアテクノロジーズが作成

標準設問：v3.0 に反映・強化する観点（例）

- ネットワークセグメンテーションの最小化
  機器・システムの構成管理の強化
- サードパーティリスク管理の仕組み化・体制構築
  契約時に考慮すべきセキュリティ要件の追加
- 従業員一人ひとりのセキュリティリテラシーの向上
  不審なメールを簡単に報告できる仕組みの整備
- 脅威インテリジェンスの活用
  インシデント対応能力の向上、レジリエンス強化

標準設問の改定背景：

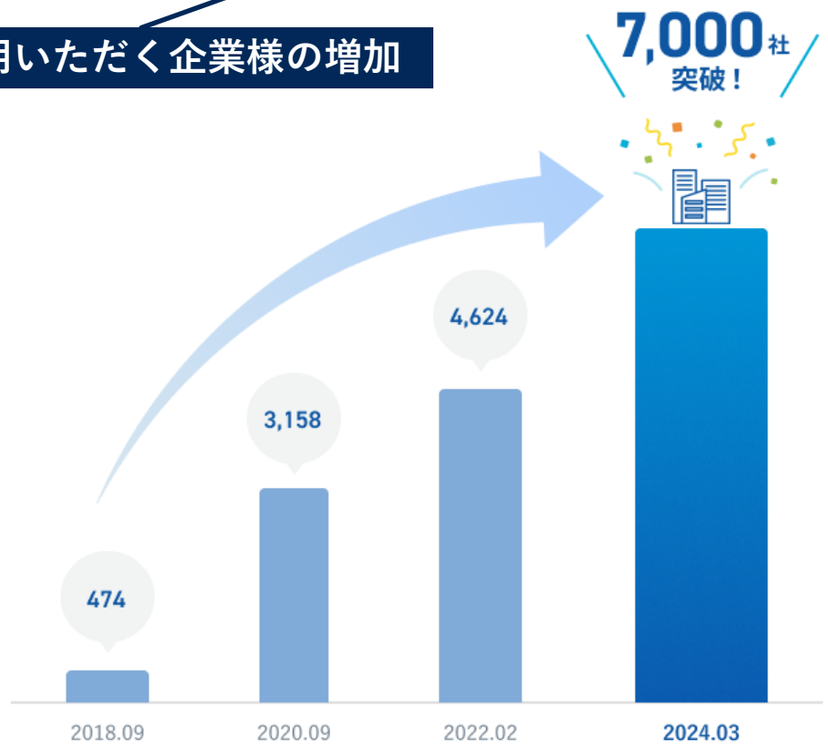
背景③：お客様からいただいたご意見・ご要望の増加

Secure SketCHをご活用いただくユースケースが増加する中、標準設問（設問/回答基準/ベストプラクティス）の理解のしやすさ、回答のしやすさに関するご意見・ご要望をいただく機会が増えています。いただいた内容を標準設問：v3.0に反映いたします。

2020年7月 v2.0

2025年9月（予定） v3.0

ご利用いただく企業様の増加



お客様からいただくご悩み/ご要望と
標準設問：v3.0での解決策（例）

Why

・評価対象間の評価項目の目線を合わせたい　（GROUPS）
・IT知見が乏しい委託先の回答負荷を下げたい（3rdPARTY）

など理由から、シンプルな表現・分かりやすさを追求したい

What How

例示を付与することや文言を訂正するなどして、
設問/回答基準/ベストプラクティスをより分かりやすく表記する

企業ごとに回答基準の解釈に差異が生じないように
回答基準の具体化や設問ごとの整合性を図る、等

想定Q＆A（自社向け評価機能の利用時）

自社向けの評価利用時

SINGLE GROUPS 3rd PARTY

自社向け評価に標準設問をご活用いただく企業様に向けたQ＆Aです。

Q1 **標準設問 v3.0 改定後でも、従来の標準設問 v2.2 を引き続き利用することはできますか？**

A1 **標準設問 v3.0への改定後は、従来の標準設問 v2.2を利用することはできなくなります。**
標準設問 v3.0へのご回答をいただくことで、最新のガイドラインや脅威に対応した定量評価（スコア・偏差値など）やガイドラインチェック機能の活用に加え対策優先度情報や最新のベストプラクティスの確認など改善活動に役立つ最新の各種コンテンツを利用いただけますので、何卒ご理解の程お願いいたします。

Q2 **標準設問 v3.0 改定後でも、過去回答した標準設問 v2.2 の評価結果や回答内容を参照することはできますか？**

A2 標準設問 v3.0 改定後でも、対策状況画面にて標準設問 v2.2 の過去の回答結果を参照することや、過去タイムライン機能でスコアをご確認いただけます。

Q3 **標準設問 v3.0 改定後では、従来より登録している設問詳細画面のメモ、コメント、証跡、計画、タスク内容は引き継がれますか？**

A3 設問改定前にご登録いただく設問詳細画面のメモ、コメント、証跡、計画、タスクは、**設問改定後に関連する設問がある場合、自動で引継ぎがなされます。**
（削除を予定する一部の設問に登録いただいたメモ、コメント、計画は引き継がれません）

想定Q＆A（自社向け評価機能の利用時）

自社向けの評価利用時

SINGLE GROUPS 3rd PARTY

自社向け評価に標準設問をご活用いただく企業様に向けたQ＆Aです。

Q4 標準設問 v3.0 の回答をする際、全て未回答の状態から回答を始める必要がありますか？

A4

一からすべての設問にお答えいただく必要はありませんので、ご安心ください。
標準設問 v3.0 にご回答いただく際、以下の様に設問を３つのタイプに区分いたします。
- ①：新しい設問、②：従来の標準設問 v2.2より回答基準の変更がある設問、③従来の標準設問 v2.2より回答基準の変更が無い設問

②と③に関して、従来の標準設問 v2.2の一部回答内容が、あらかじめプリセットされた状態でご回答いただきます。

Q5 標準設問 v3.0 への回答後は、従来の標準設問 v2.2の評価結果（スコアや他社平均、偏差値など）と比べて変化は生じますか？

A5

標準設問 v3.0は、設問構成（設問の増減やカテゴリ、回答基準）の見直しに加え、設問の重み（各設問、各回答基準）の見直しを実施いたします。
そのため定量的な評価結果（スコアやランク、他社平均や偏差値など）は、**改定前後で大幅に変動する可能性があること、予めご了承ください。**

Q6 従来の標準設問 v2.2 と標準設問 v3.0との設問構成の変更点を教えていただくことは可能でしょうか。

A6

標準設問 v3.0 改定の1か月前を目安に、標準設問 v2.2 と標準設問 v3.0との設問構成の変更点などを記載した、設問改定方針を別途ご案内いたします。

想定Q＆A（テンプレート評価機能の利用時）

テンプレート評価利用時

SINGLE GROUPS 3rd PARTY

標準設問のテンプレート評価機能をご活用いただく企業様に向けたQ＆Aです。

Q1 **標準設問 v3.0 改定後でも、テンプレートとして従来の標準設問 v2.2 を引き続き利用し、各拠点に回答を依頼することはできますか？**

A1 **標準設問 v3.0への改定後は、テンプレートとして従来の標準設問 v2.2を利用することはできなくなります。**
テンプレートとして標準設問 v3.0をご利用いただくと、最新ガイドラインや脅威に対応した評価活動を実施いただけますので、何卒ご理解の程お願いいたします。

Q2 **2025年9月時点において、テンプレートとして従来の標準設問 v2.2 を利用し、各拠点に回答を依頼する計画があります。**
既に回答を依頼しているテンプレートを、標準設問 v3.0に切り替えることはできますか？

A2 既に回答を依頼しているテンプレートを、途中で切り替えることはできません。
当該回答依頼を締め切るか、削除していただいた後、改めてテンプレートとして標準設問 v3.0を選択した回答依頼を作成いただく必要がございます。
（参考）回答依頼を編集・削除、リマインドする

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