セキュリティ対策実行支援プラットフォーム

Secure SketCH

自動診断（SecurityScorecard）利用マニュアル
~効果的な運用に向けたステップ~

Ver1.6 更新日 2025/2/19

NRI SECURE

本資料の想定読者

本資料は「SINGLE PREMIUMプラン」「GROUPS PREMIUMプラン・SRSプラン」「3rd PARTY COWORKプラン」ご契約のお客様のうち、Secure SketCHの自動診断（SecurityScorecard連携）を

・これから使い始める方

・効果的な運用の方法を知りたい方

を対象としたマニュアルです。

© NRI SecureTechnologies, Ltd.

目次

1．自動診断（SecurityScorecard連携）の概要 **p３～**

2．効果的な運用に向けたステップ **p７～**

- 推奨する３つのステップ
  - Step. 1　ドメインの登録
  - Step. 2　デジタルフットプリントの精査
  - Step. 3　検知課題の確認・対応

3．参考事例 **P３２～**

4．問合せサポートについて **P３５～**

© NRI SecureTechnologies, Ltd.

1. 自動診断(SecurityScorecard連携)の概要

© NRI SecureTechnologies, Ltd.

サービス概要：

自動診断（SecurityScorecard連携）の建て付け

攻撃者の「偵察」フェーズに着目し、サイバー攻撃者の視点で「自社がどう見えているのか？」の外形を自動で評価する機能です。
得られた評価結果に対し、継続的な確認と改善を繰り返すことで、**“攻撃者（外部）から侵害されにくい環境”**を維持できます。

SecurityScorecard

「偵察」フェーズに着目し
公開情報を自動で収集・分析

外部から侵害されやすさ
を定量的に可視化

■ サイバーキルチェーンの「偵察」フェーズに着目

偵察	武器化	配送	攻撃	インストール	遠隔操作	目的達成
企業に関する情報収集	攻撃コード/マルウェアの作成	メール送信/NW機器へ不正ログイン	攻撃コードの実行	マルウェアを端末にインストール	マルウェアを遠隔操作	データ窃取 改ざん 暗号化など

■ 企業の「外形」をスコア/ランクによる定量評価

スコア	90~100	80~89	70~79	60~69	0~59
ランク	A	B	C	D	F
侵害リスク※	1.0x	2.9x	5.4x	9.2x	13.8x

※FランクはAランクより**13.8倍**も侵害リスクが高い

※米国2024年4月9日よりスコアリングアルゴリズムがアップデートされたことに伴い、Secure SketCHが提供する自動診断機能の評価結果（総合スコアや発見課題等）にも一致部変更が生じております。
詳細については[Scoring 3.0概要説明]をご参照ください。

© NRI SecureTechnologies, Ltd.

サービス概要：

自動診断（SecurityScorecard連携）の評価項目

評価対象の企業ドメインに関連した、ネットワーク・DNS・エンドポイントなど10種類のカテゴリで、約200の項目を自動で評価します。

ネットワークセキュリティ

安全でないネットワーク設定の検出

例：失効した証明書の使用、RDPサービスの一般公開、脆弱なSSHソフトウェアの実行

DNSの健全性

安全でないDNSの設定と脆弱性の検出

例：ドメインにSPFレコードが存在しない、オープンDNSリゾルバの検出

パッチ適用頻度

脆弱性またはリスクを含む可能性のある未更新の企業資産

例：深刻度の脆弱性発見、EOS（サービス終了）製品の利用

エンドポイントセキュリティ

従業員のワークステーションのセキュリティレベル測定

例：古いWebブラウザの使用、古いオペレーティングシステムの使用

IPレピュテーション

社内ネットワーク内でのマルウェアやスパムなどの疑わしい活動の検出

例：マルウェア感染、攻撃するサーバの検出、P2Pの活動

アプリケーションセキュリティ

一般的なWebサイトアプリケーションの脆弱性の検出

例：HTTPSを強制しないサイト、コンテンツ管理システム（CMS）の脆弱性、Cookieの”Secure”属性が存在しない

Cubit スコア

一般的なセキュリティのベストプラクティスの実装をチェックする独自のアルゴリズム

例：管理者用サブドメインの公開、タイポスクワッティングの危険性

ハッカーチャット

ハッカーサイトでのあなたの会社に関するチャットの監視

例：ハッカーサイトでWebサイト改ざん・ブートシェル実行の言及

情報漏えい

会社機密情報の漏洩の可能性

例：機密性の高い情報をGoogle・GitHubへ公開

ソーシャルエンジニアリング

ソーシャルエンジニアリングまたはフィッシング攻撃に対する企業の意識の測定

例：従業員の満足度の低下、マーケティングサイトで会社の電子メールを使用

© NRI SecureTechnologies, Ltd.

サービス概要：

自動診断（SecurityScorecard連携）の評価項目

約200の項目は、過去に攻撃被害を受けた企業が特徴的に保有していた脆弱性やシステム設定などデータに基づき、限定しています。

一般的なASMのアプローチ
＝公開情報を網羅的に洗いざらい見る

大量の検出項目
（網羅的）

量が多く
優先度設定
が難しい

SecurityScorecardのアプローチ
＝敢えてチェック項目フォーカスしている

約200項目
SSCのフォーカス

大量の検出項目
（網羅的）

大量の統計データを持つ強み
を活かし、事件・事故を起こした企
業と同じ悲劇が起きないことを目指
すアプローチ

▼

リスクベースアプローチ

藤本（SecurityScorecard株式会社 代表取締役社長）によれば記者が思った通り SecurityScorecardは、経産省の ASM 導入ガイダンスが求める機能をほぼ全て満たしているという。これが共通点。一方で異なっている点は、約 200 の SecurityScorecardのスキャン項目は、決して公開情報を棚卸的・網羅的に洗いざらい見るのではなく、あくまで過去実際に攻撃被害をこうむった企業が特徴的に持っていた脆弱性や設定などにチェック範囲をあえて限定している（それが約 200 項目）。この仕様が世に言う ASM（Attack Surface Management）と異なるという。

ScanNetSecurity　「SecurityScorecard」が自らを ASM と名乗らない理由：https://s.netsecurity.ne.jp/article/2025/02/05/52276.html

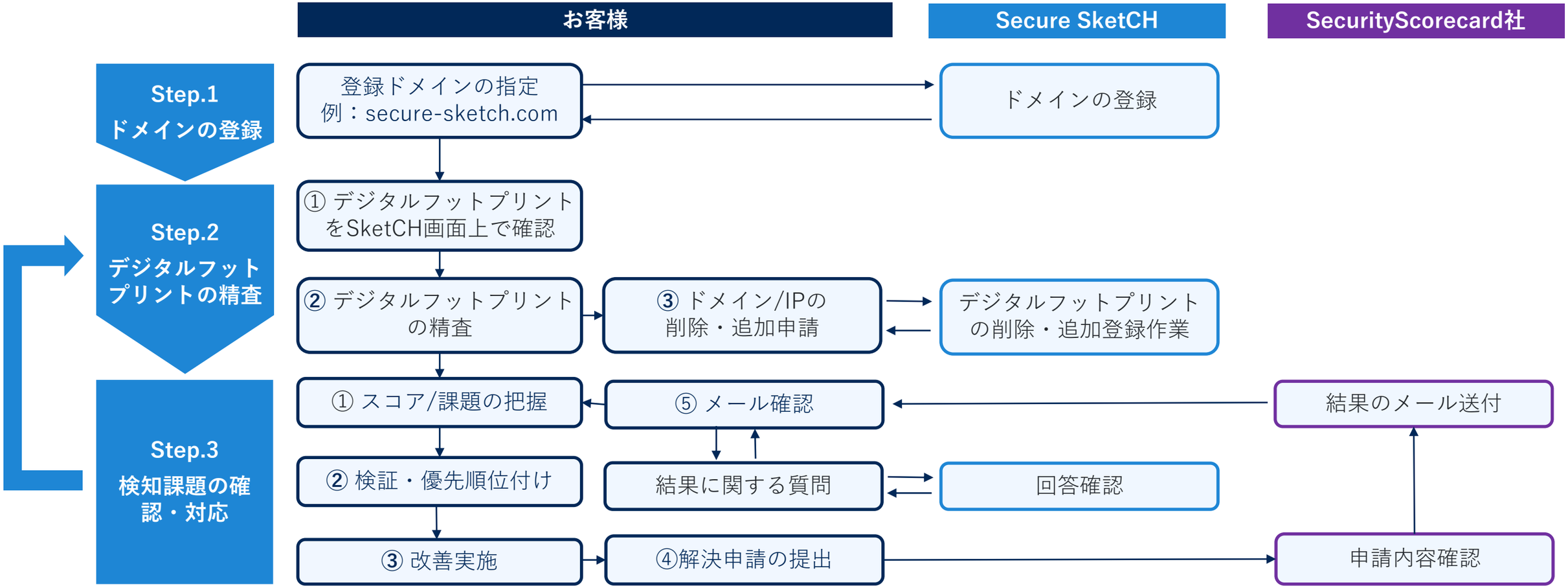
© NRI SecureTechnologies, Ltd.

2. 効果的な運用に向けたステップ

© NRI SecureTechnologies, Ltd.

推奨する３つのStep

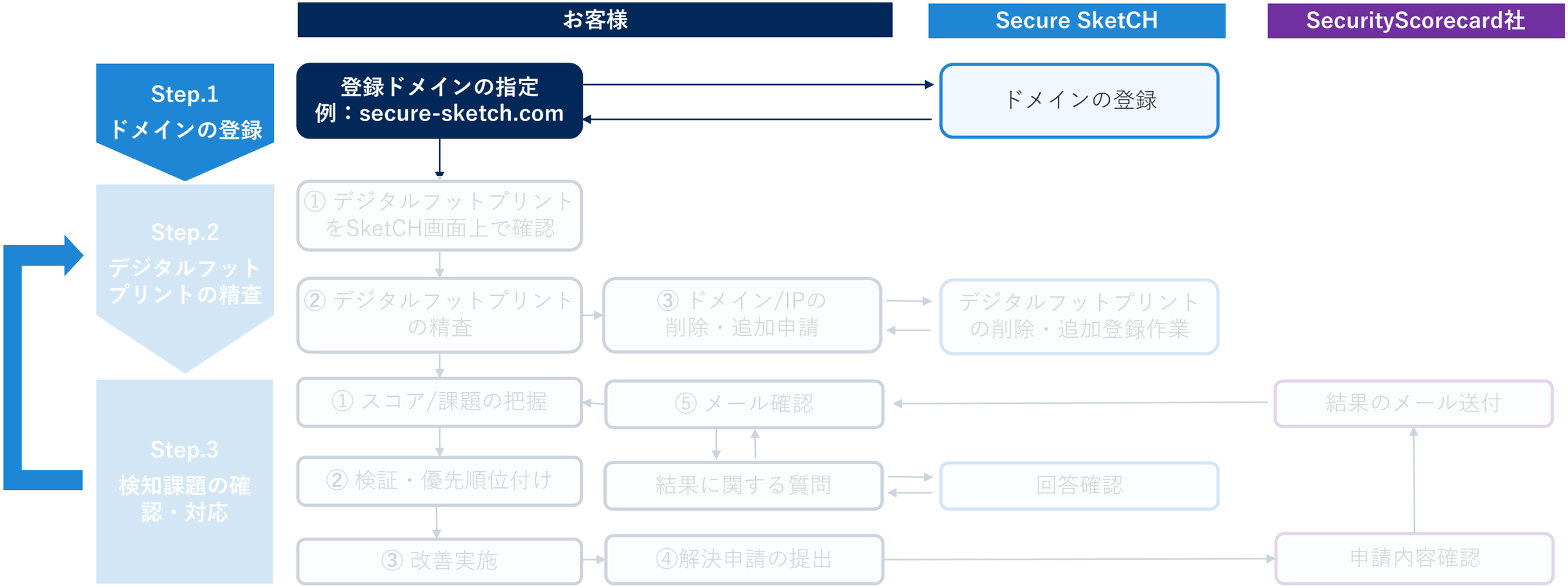
自動診断（SecurityScorecard連携）の効果的な運用に向けた推奨Stepは以下です。



© NRI SecureTechnologies, Ltd.

推奨する３つのStep

Step.1 ドメインの登録についてご説明いたします。



© NRI SecureTechnologies, Ltd.

登録ドメインの指定

自動診断のご利用開始にあたり、診断対象のドメインの登録が必要です。評価したいドメインを弊社担当者にご連絡ください。
SecurityScorecard社と連携し、ドメイン登録ならびにSecure SketCH上への評価結果の反映を実施いたします。

※連携の設定は当社の担当者にて対応します。

© NRI SecureTechnologies, Ltd.

よくあるご質問

登録ドメインに関するよくあるご質問をご参照ください。

Q **どのようなドメインを登録するケースが多いですか？**

A 企業代表ドメイン（例：nri-secure.co.jp）や製品ドメイン（例：secure-sketch.com）などお客様の目的によって異なります。

Q **自社ではなく、他社のドメインを登録することはできますか？**

A 登録いただけます。競合他社のドメインを評価するユースケースや、委託先のドメインを評価するユースケースもございます。

Q **ドメインを連絡後、即時評価は可能でしょうか？**

A 弊社担当者によるドメイン登録から評価結果の反映まで、1営業日~数営業日かかります。

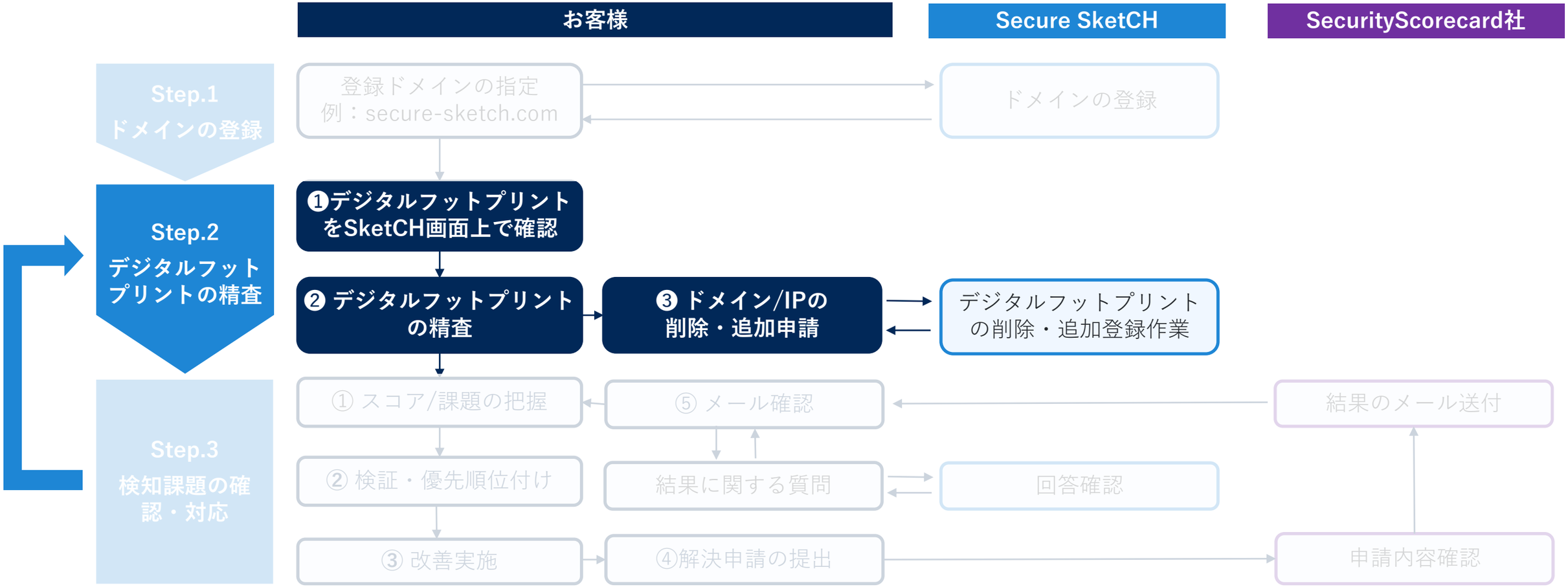
Q **契約期間中に登録ドメインを変更できますか？**

A 一度ご登録いただいたドメインは、ご契約終了まで変更することはできません（ご契約の更新時にて変更を承ります）。

© NRI SecureTechnologies, Ltd.

推奨する３つのStep

Step.2 デジタルフットプリントの精査についてご説明いたします。



© NRI SecureTechnologies, Ltd.

デジタルフットプリントの概要と精査の重要性について

自動診断では、Step1の登録ドメインに紐づいた関連資産（ドメインやIPアドレス）を、デジタルフットプリントとして自動収集・管理いたします。デジタルフットプリントの登録情報は、「課題の検出」や「スコア算出」に影響を与えるため、定期的な確認・精査が必要です。

■ デジタルフットプリントを精査する3つのメリット

1. 自社に関連していない資産を削除することで実態に沿った評価を得られる
2. 未登録のサブドメインを追加登録することで実態に沿った評価を得られる
3. 担当者が認識していなかった評価対象の資産発見につながる

※デジタルフットプリント検出手法の補足については、こちらの資料をご参照ください

© NRI SecureTechnologies, Ltd.

① デジタルフットプリントをSketCH画面上で確認

診断の左側メニューから[自動診断]をクリックします。

画面下部の [デジタルフットプリント] をクリックし、デジタルフットプリントを確認しましょう。

Q **表示されている情報は、最新の情報でしょうか？**

A 表示されている情報（IPアドレスやドメイン）は、リアルタイム情報ではございません。
週に一度（毎週土曜日）に、更新がなされます。

© NRI SecureTechnologies, Ltd.

② デジタルフットプリントの精査

Secure SketCHに表示されているデジタルフットプリントを確認しましょう。

一番左側に表示されている項目がドメイン・IPアドレスです。

ドメイン

ドメイン	ドメインの種類	状態	発見項目	発見課題	スコア影響	IPアドレス数
example.co.jp	親ドメイン	評価中	0	0	0	1
www.example.co.jp	サブドメイン	評価中	0	0	0	1
mail.example.co.jp	サブドメイン	評価中	0	0	0	1

IPアドレス

IPアドレス	状態	検出場所	発見項目	発見課題	スコア影響	ドメイン	検出	ソース
192.0.2.0	評価中	Japan	0	0	0	example.co.jp	WHOIS	A Record
192.0.2.1	評価中	Japan	0	0	0	example.co.jp	DNS Lookup	A Record
192.0.2.2	評価中	Japan	0	0	0	example.co.jp	SSL Certificate	ThreatMarket SSL

© NRI SecureTechnologies, Ltd.

② デジタルフットプリントの精査（資産：ドメインの場合）

デジタルフットプリント確認画面で表示されているドメインについて、以下４つの観点で、確認・精査しましょう。

	４つの観点		対応方針
1	自社に関連している資産 （例：example.com example1.com）	➡	そのまま登録を続けましょう。
2	自社に関連していない資産 （例：example.co.jp www.example.co.jp）	➡	弊社サポート宛にご連絡（P18参照）いただくことで デジタルフットプリントから削除が可能です。
3	自社に関連性があるが、評価対象外にしたい資産 **対象外にできるケース** ■ クラウド事業者として顧客に払い出された、サービス提供者の責任範囲外であるドメイン ■ 購入したドメインだが、利用していないドメイン（パークドメイン※）	➡	デジタルフットプリントから削除できませんが 検知された課題が、スコアに反映されないように 個別に評価対象外として申請できる場合がございます。 詳しくは、弊社サポート宛にご連絡（P18参照）ください。
4	自社に関連しているのにも関わらず、登録されていない資産 （例：www.example.com）	➡	弊社サポート宛にご連絡（P18参照）いただくことで デジタルフットプリントに追加登録が可能です。

※ SecurityScorecard社が定義する条件を満たす場合、パークドメインとして自動で登録なされます。
パークドメインの登録条件はヘルプセンターをご確認ください。

© NRI SecureTechnologies, Ltd.

② デジタルフットプリントの精査（資産：IPアドレスの場合）

デジタルフットプリント確認画面で表示されているIPアドレスについて、以下４つの観点で、確認・精査しましょう。

	４つの観点		対応方針
1	自社に関連している資産 （例： 192.0.2.20 198.51.100.8 ）	➡	そのまま登録を続けましょう。
2	自社に関連していない資産 （例： 203.0.113.1 ）	➡	弊社サポート宛にご連絡（P18参照）いただくことで デジタルフットプリントから削除が可能です。
3	自社に関連性があるが、評価対象外にしたい資産 **対象外にできるケース** ■ クラウド事業者として顧客に払い出された、サービス提供者の責任範囲外であるIPアドレス ■ ゲストデバイスのIPアドレス	➡	デジタルフットプリントから削除できませんが 検知された課題が、スコアに反映されないように 個別に評価対象外として申請できる場合がございます。 詳しくは、弊社サポート宛にご連絡（P18参照）ください。
4	自社に関連しているのにも関わらず、登録されていない資産 （例： www.example.com ）	➡	弊社サポート宛にご連絡（P18参照）いただくことで デジタルフットプリントに追加登録が可能です。

© NRI SecureTechnologies, Ltd.

② デジタルフットプリントの精査（削除時の注意点）

デジタルフットプリントの削除に関して、注意点があります。

注意①

親ドメインが登録されている場合
特定のサブドメインのみを削除することはできません。

【例】親ドメイン(example.com)とサブドメインが登録されている場合

対応不可

example.com
├ www.example.com
└ mail.example.com

特定のサブドメイン（例：www）のみを削除することはできない※

対応可

example.com
├ www.example.com
└ mail.example.com

親ドメインを削除することで全サブドメインが削除される

注意②

IPアドレスと紐づくドメインが両方登録されている場合
IPアドレスのみを削除することは原則できません。

【例】203.0.113.1 = example.com の両方が登録されている場合

対応不可

203.0.113.1 のみを削除することはできない

対応可

example.com
203.0.113.1
を削除した後であれば
を削除することができる

※ 当該サブドメインのDNSレコードを削除することで、デジタルフットプリントから自動で削除なされます。詳しくはヘルプセンターをご確認ください。

© NRI SecureTechnologies, Ltd.

③ デジタルフットプリントの削除・追加申請

Step2-2のデジタルフットプリント精査後、削除対象の資産（ドメイン/IPアドレス）や、追加対象の資産がある場合には
お問い合わせフォームより、弊社サポート宛にご連絡ください。申請内容を確認後、デジタルフットプリントの変更作業を実施します。

デジタルフットプリントに関するご相談があれば、お気軽にサポート宛にご連絡ください。
また、いずれの申請においても最終的な判断は、弊社ではなくSecurityScorecard社が行うため、
ご要望にお応えできない可能性がございます。予めご了承ください。

© NRI SecureTechnologies, Ltd.

③ デジタルフットプリントの削除・追加申請

お問い合わせフォーム画面に入力する、「お問い合わせ内容」のテキストの例として、ご利用ください。

P 16-17 観点２：削除依頼の例

診断ドメイン：（例：example.com）

以下は、自社に関連していないドメインであるため
デジタルフットプリントから削除をお願いします。
・(例：example.co.jp)

P 16-17 観点３：登録変更依頼の例

診断ドメイン：（例：example.com）

クラウド事業者として顧客に払い出された以下のドメインが、
デジタルフットプリントに登録されています。当該ドメインへ
の課題が検出されないように、変更をお願いします。
・（例：example.co.jp）

P 16-17 観点４：追加依頼の例

診断ドメイン：（例：example.com）

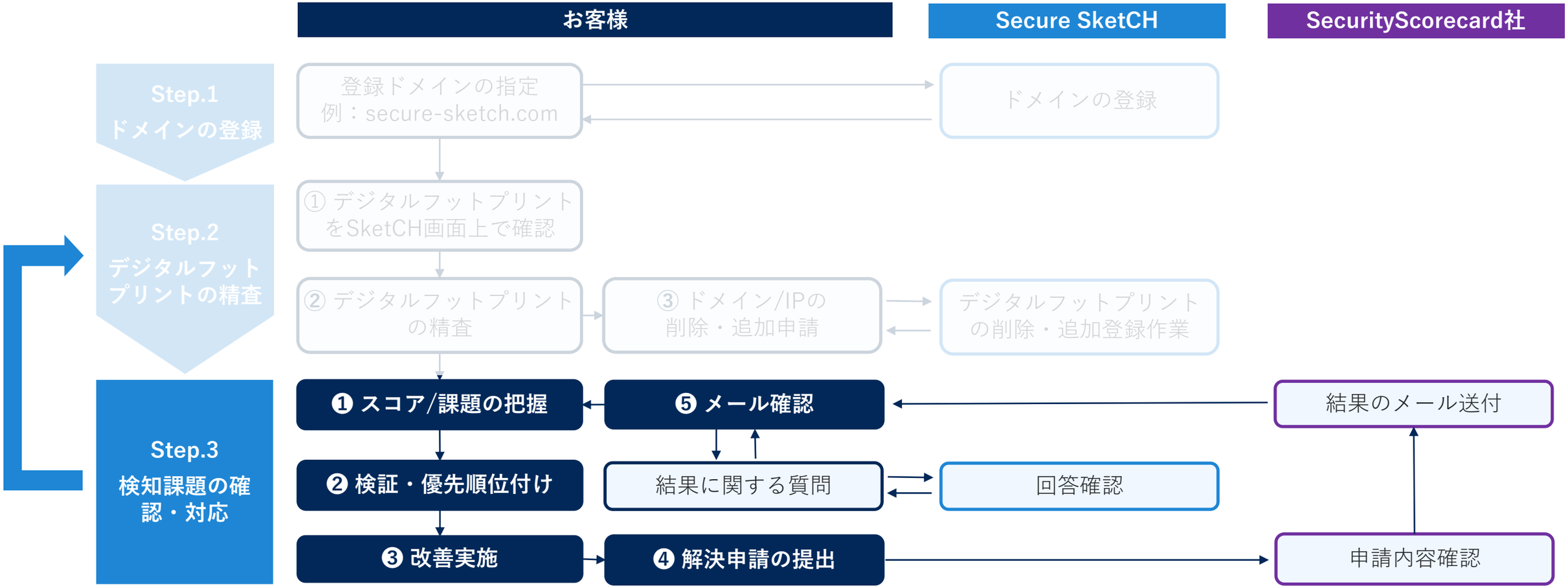
以下は、自社に関連しているサブドメインですが、デジタル
フットプリントに登録がないため、登録をお願いします。
・(例：www.example.com)

削除や追加の依頼ドメイン・IPアドレスの数が
10個以上ある場合には、お問い合わせフォームより
その旨をサポート宛にご連絡ください。
本資料に記載以外の、別の申請方法をご提案いたします。

© NRI SecureTechnologies, Ltd.

推奨する３つのStep

Step.3 自動診断で検知された課題の確認方法や、対応後の運用手順についてご紹介します。



© NRI SecureTechnologies, Ltd.

発見課題の解消に向けた流れ

スコアや発見課題の確認から、課題の改善対応完了までの一般的な対応の流れと実施項目の例です。

	❶ スコア/課題の把握	❷ 検証・優先度付け	❸ 改善実施	❹ 解決申請	❺ メール確認
対応の流れ	**評価スコアやランク、発見課題を把握する。**	**課題の検証や改善是非を判断する。また対応の優先度を付ける。**	**発見課題の推奨事項や解説記事を参考に、改善を実施する。**	**改善実施後に解決申請を提出する。**	**解決申請に対する結果メールを確認する。**
実施項目例	✔ 評価スコアやランクを確認する ✔ 同業種平均と比較し、自社の立ち位置を測る ✔ 10種類のカテゴリのスコアや各発見課題を把握する	✔ 課題の詳細と対象を確認する ✔ 誤検知の可能性を検証する ✔ 改善是非を判断し、対応の優先度を付ける	✔ 発見課題の推奨事項や解説記事を参考に、改善を実施する ✔ 関係者に改善対応を指示する	✔ 解決申請を提出する※	✔ 解決申請に対する承認結果をメールで受け取る ✔ メールを確認し、必要に応じて改善内容を見直す

※：改善を実施した場合、一定期間後（課題によって日数は異なる）に当該課題が自然消滅されますが、解決申請を提出することで、自然消滅を待たずにSecurityScorecard社が改善内容を確認し、課題を削除いたします。

© NRI SecureTechnologies, Ltd.

① スコア/課題の把握

Step2で精緻化したデジタルフットプリントに対する評価結果を確認します。

評価スコアやランク、同業種平均や10種類の評価項目の内容を把握いただけます。より詳しい画面の説明はこちらをご確認ください。

評価ランク表示

ランクはA～D・Fの５段階で表示

評価スコア表示

総合スコアを点数で表示

10種類の評価項目の表示（10のリスク分析）

総合スコアを点数で表示

同業種平均

同業種のスコアと比較した自社の立ち位置をグラフで表示

※SecurityScorecard社が保有する統計データの平均数値となります。

業種は以下から選択いただけます
変更ご希望の場合には弊社サポートにご連絡ください

- construction 建設
- education 教育
- energy エネルギー
- entertainment エンターテイメント
- financial_services 金融サービス
- food 食品
- government 政府
- healthcare ヘルスケア
- hospitality サービス業
- information_services 情報サービス
- legal 法律
- manufacturing 製造
- non_profit 非営利団体
- pharmaceutical 医薬品
- retail 小売
- technology テクノロジー
- telecommunications 電気通信
- transportation 運送

© NRI SecureTechnologies, Ltd.

① スコア/課題の把握

発見された課題の詳細を確認することが可能です。発見事項をクリックすると、発見事項の解説や推奨事項、リスクなど各種情報に加え接続IPアドレスやドメイン・ポートなど対象資産を確認いただける画面に遷移します。詳しい手順や画面の説明はこちらをご確認ください。

発見事項一覧表示

発見事項ごとの深刻度を表示

深刻度	スコア影響	発見事項	件数	分野
高	0.7	深刻度高の脆弱性を最近発見	265293	パッチ適用頻度
高	0.9	深刻度高のCVEのパッチ適用頻度	348784	パッチ適用頻度
高	0.4	未認証Elasticsearch Serviceの発見	105	ネットワークセキュリティ
高	0.1	産業用制御システムデバイスにアクセス可能	98	ネットワークセキュリティ
中	0.1	PostgreSQLサービスの発見	686	ネットワークセキュリティ
中	0.4	弱い暗号スイートをサポートしているTLSサービス	53699	ネットワークセキュリティ
中	0.4	弱い署名を使用するSSL証明書	8324	ネットワークセキュリティ
中	0.1	VNCサービスの発見	1979	ネットワークセキュリティ
低	0.1	X-Frame-Options未実装のWebサイト	509	アプリケーションセキュリティ
低	0.1	Cookieに'Secure'属性がありません	42	アプリケーションセキュリティ
ポジティブ	0	TLS証明書ステータス要求（"OCSPステープル"）の検出	7171	ネットワークセキュリティ
参考	0	公開された個人情報（履歴）	241	ソーシャルエンジニアリング
参考	0	分析された中程度の重大度のCVEパッチ	1	パッチ適用頻度

発見課題詳細

推奨対応やリスク、発見課題の対象を表示

ネットワークセキュリティ

弱い暗号スイートをサポートしているTLSサービス

深刻度 中　件数 53699

解説

SSL（Secure Socket Layer）の後継であるTLS（Transport Layer Security）は、TLSサーバー（ウェブサイトなど）とTLSクライアント（ウェブブラウザなど）間の通信を暗号化するネットワークプロトコルです。
すべての通信は、暗号スイート：いくつかのアルゴリズムの組み合わせによって保護されます。
暗号化アルゴリズムに寿命はありませんが、学者や研究者、国家は常に弱点がないか評価を行っています。
アルゴリズムの信頼性は時間とともに変化し、弱い暗号スイートで保護されている通信は、改ざんまたは解読される可能性があります。

推奨事項

「詳細」列の「evidence」に記載されているプロトコルを無効化してください

リスク

弱い暗号スイートをサポートしているTLSサービスが発見されています

発見課題

CSV出力　解決申請

接続	ポート	詳細	最終検出日時
216.[redacted]	443	{"last_seen_at"=>"2023-07-17T14:37:07.000Z", "evidence"=> ["TLS v1.0", "TLS v1.1"], "ip"=>"2[redacted] }	2023-07-17

© NRI SecureTechnologies, Ltd.

② 検証・優先度付け

発見課題の対象となる資産（IPアドレス・ポートなど）を確認し、誤検知の有無を検証しましょう。

誤検知ではない場合、発見課題の深刻度やリスク発生時の業務への影響・攻撃者の有用性などを考慮して、改善是非を判断しましょう。

発見課題詳細

推奨対応やリスク、対象を表示

ネットワークセキュリティ

弱い暗号スイートをサポートしているTLSサービス

深刻度 中　件数 53699

解説	SSL（Secure Socket Layer）の後継であるTLS（Transport Layer Security）は、TLSサーバー（ウェブサイトなど）とTLSクライアント（ウェブブラウザなど）間の通信を暗号化するネットワークプロトコルです。 すべての通信は、暗号スイート：いくつかのアルゴリズムの組み合わせによって保護されます。 暗号化アルゴリズムに寿命はありませんが、学者や研究者、国家は常に弱点がないか評価を行っています。 アルゴリズムの信頼性は時間とともに変化し、弱い暗号スイートで保護されている通信は、改ざんまたは解読される可能性があります。
推奨事項	「詳細」列の「evidence」に記載されているプロトコルを無効化してください
リスク	弱い暗号スイートをサポートしているTLSサービスが発見されています

発見課題　CSV出力　解決申請

接続	ポート	詳細	最終検出日時
216.[redacted]	443	{"last_seen_at"=>"2023-07-17T14:37:07.000Z", "evidence"=>["TLS v1.0", "TLS v1.1"], "ip"=>"2[redacted]}	2023-07-17

検出課題に対する改善判断のフロー（例）

IP/ドメインが自社に関連あるものか確認
- No → デジタルフットプリントの精査 P11~ 参照
- Yes ↓

誤検知ではないかを検証※
- No（誤検知である） → 誤検知として解決申請 P28 参照
- Yes ↓（誤検知でない）

（※よく発生する課題の解説記事は P27参照）

改善是非を判断

対応の評価観点の例

- ○ 発見課題の深刻度（高/中/低）
- ○ 攻撃コードの有無
- ○ 攻撃の実行のしやすさ
- ○ 対象サービスが扱う情報価値
- ○ リスク発生時のビジネス影響
- ○ 対応できる社内リソース
- ・
- ・

改善是非の判断例	優先度
可能な限り迅速に改善対応を行う	高
定期的なメンテナンスの際に対応する	中
リスクを許容し対応しない	低

© NRI SecureTechnologies, Ltd.

（参考）タスク管理※

「タスク管理」を用いることで、自動診断で検出された課題に対する一連の改善対応を、タスクとして管理できます。

作成タスクに対し担当者・優先度など設定いただけ、Secure SketCH上で進捗を管理いただけます。詳しくはこちらをご確認ください。

タスク管理画面

タスク作成・登録画面

※「タスク管理」はPREMIUM・PLUSご契約者様にご利用いただける機能です。

© NRI SecureTechnologies, Ltd.

③ 改善実施

発見課題に記載の「推奨事項」の内容を参考に、改善を実施しましょう。改善を実施した課題は、一定期間後※に自然消滅なされます。

※ 課題によって日数が異なります

発見課題詳細

推奨対応やリスク、対象を表示

ネットワークセキュリティ

弱い暗号スイートをサポートしているTLSサービス

深刻度 中　件数 53699

解説　SSL（Secure Socket Layer）の後継であるTLS（Transport Layer Security）は、TLSサーバー（ウェブサイトなど）とTLSクライアント（ウェブブラウザなど）間の通信を暗号化するネットワークプロトコルです。
すべての通信は、暗号スイート：いくつかのアルゴリズムの組み合わせによって保護されます。
暗号化アルゴリズムに寿命はありませんが、学者や研究者、国家は常に弱点がないか評価を行っています。
アルゴリズムの信頼性は時間とともに変化し、弱い暗号スイートで保護されている通信は、改ざんまたは解読される可能性があります。

推奨事項　「詳細」列の「evidence」に記載されているプロトコルを無効化してください

リスク　弱い暗号スイートをサポートしているTLSサービスが発見されています

発見課題　CSV出力　解決申請

接続	ポート	詳細	最終検出日時
216.[redacted]	443	{"last_seen_at"=>"2023-07-17T14:37:07.000Z", "evidence"=> ["TLS v1.0", "TLS v1.1"], "ip"=>"2[redacted]}	2023-07-17

アプリケーションセキュリティ

Content Security Policy（CSP）がありません

深刻度 中　件数 19842

解説　Content Security Policy（CSP, コンテンツセキュリティポリシー）は、悪意のあるクロスサイトスクリプティング（XSS）攻撃からWebサイトを保護する、価値ある安全策を提供します。
適切に設定されたポリシーは、攻撃者がWebサイトにコードや他の悪質なコンテンツ参照を埋め込むことを阻止します。
Content Security Policyがないと、Webサイトの開発者が「攻撃者によるWebサイトの動作を変更するコンテンツの埋め込み」されうる間違いを起こしやすくなります。

推奨事項　Webサーバー設定でCSPヘッダーを有効にします。

リスク　Content Security Policy（CSP）ディレクティブは、Webページをレンダリングするときにリソースをロードできる場所をWebブラウザに指示します。

発見課題　CSV出力　解決申請

ドメイン	スキーム	詳細	最終検出日時
[redacted]2.com	https	{"last_seen_at"=>"2023-08-10T15:59:39.577Z", "evidence"=> ["No content security policy directives found."], "initial_url"=>"", "final_url"=>"https:/[redacted]}	2023-08-11 00:59:39 +0900

© NRI SecureTechnologies, Ltd.

③ 改善実施

Secure SketCHヘルプセンターでは、発生件数が特に多い課題に関する解説記事（課題の説明や改善方法など）を公開しています。

公開している解説記事

- 弱い暗号スイートをサポートしているTLSサービス
- 古いWebブラウザの発見
- 古いオペレーションシステムの発見
- SPFレコード無し
- DMARCの設定がないSoftfailを含むSPFレコード
- Content Security Policy (CSP) がありません
- HTSTベストプラクティスが未実装のウェブサイト
- 安全でないHTTPSリダイレクトパターン

※ その他の課題に関しては、SecurityScorecard社が公開するWebページよりご確認ください。

© NRI SecureTechnologies, Ltd.

④ 解決申請の提出

「解決申請」を提出することで、SecurityScorecard社が改善内容を確認します。申請が承認されることで、自然消滅を待つことなく課題を削除いただけます。詳しい実施手順についてはこちらをご確認ください。

1

2

3 提出

※ 提出された解決申請は、弊社を介さず直接SecurityScorecard社に通知されます。
申請結果は、通常72時間以内にメールにて送付がなされます(次ページ参照)。

© NRI SecureTechnologies, Ltd.

⑤ 結果のメール確認

④で提出した「解決申請」はSecurityScorecard社が確認いたします。結果の通知メールが、ご登録アドレス宛に送付がなされます。
メール本文において Result：Approval の場合は「承認」、 Result： Rejected の場合は「却下」なされています。

メール件名	【Secure SketCH】Automatic Diagnosis, issue findings you applied to resolve have been updated. -example.com
送信元	noreply@secure-sketch.com

メール本文（一部）

[Result notification]

Issue name:
Medium-Severity Vulnerability in Last Observation

Target:
210.[redacted]

Result:
Approval

⇒解決申請が「承認」

Application date:
2023/02/28 19:47(+0900)

Select a resolution:
I cannot reproduce this issue and I think it's incorrect

[Result notification]

Issue name:
SSL/TLS Service Supports Weak Protocol

Target:
210.[redacted]

Result:
Rejected

⇒解決申請が「却下」※

Application date:
2023/03/06 16:12(+0900)

Select a resolution:
I cannot reproduce this issue and I think it's incorrect

※ 解決申請結果のメール内容には「却下」理由は記載されていません。「却下」されるよくあるケースを、次ページに公開しております。

© NRI SecureTechnologies, Ltd.

⑤ 結果のメール確認

解決申請が「却下」される、よくあるケースは以下の通りです。

Q **検知課題の「深刻度 高/中/低のCVEのパッチ適用頻度」に対する解決申請が却下されました。**

A 本課題は、他の課題と解決の仕組みが異なるためです。
一定期間内にCVEのパッチ適用していない場合は、その後に改善を行った場合でも、発見課題として一定期間残り続けます。
詳しくはこちらをご参照ください。

Q **発見課題のリスクを受容すると判断したのにも関わらず、解決申請が却下されました。**

A 攻撃者視点ではリスクが残っている状態とみなせるためです。詳しくはこちらをご参照ください。

Q **自社に関連のないIPアドレス/ドメインに対する課題であるのに、解決申請が却下されました。**

A 自社に関連のない資産に対する課題である場合でも、提出された解決申請は却下なされます。
デジタルフットプリントの精査が必要であるため、P11~P19をご参照の上、資産の削除をご依頼ください。

※ 上記以外のケースで「却下」理由を把握されたい場合には、弊社サポート宛にご連絡ください

© NRI SecureTechnologies, Ltd.

3. 参考事例

© NRI SecureTechnologies, Ltd.

参考事例１：

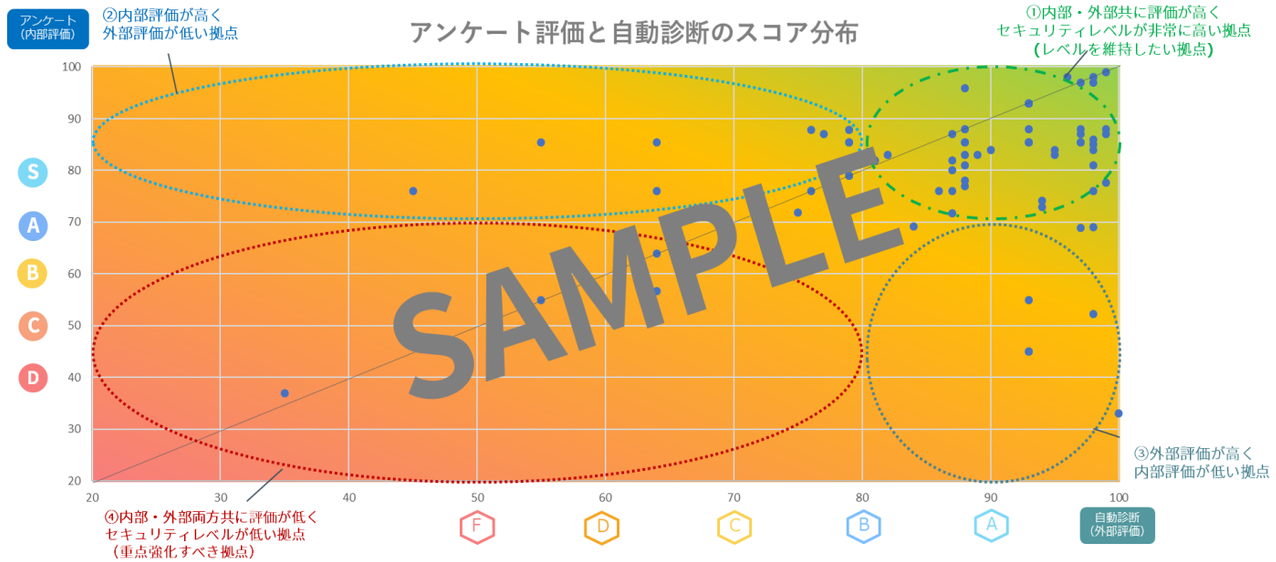
【内部】Attack Surfaceの継続的なセキュリティ統制⇒グローバルの弱点把握

ブラザー工業株式会社様は、Secure SketCHのアンケート機能と自動診断（SecurityScorecard）の両方を利用して
グローバル72拠点をセキュリティ対策状況を評価し、両スコア分布をグラフ化することで改善すべき拠点を可視化されました。

brother

グローバル72拠点の「セキュリティ対策状況の可視化」と「多面的評価」を実現し、監査コストは4分の1に削減

ブラザー工業株式会社



グローバル各拠点のセキュリティ対策において、**何ができていて、どこを改善すべきなのかが一目瞭然**でした。アンケート回答による自己評価と自動診断を組み合わせた結果をまとめていただいたのも、**社内外の複眼的な視点で、どの拠点のセキュリティレベルが高いのか、あるいは低いのかが非常にわかりやすかった**ので、経営層への説明もしやすくなりました。(ブラザー工業様)

ブラザー工業株式会社 様｜導入事例｜NRIセキュア
https://www.nri-secure.co.jp/service/case/secureskeetch_brother

© NRI SecureTechnologies, Ltd.

参考事例２：

【外部】定量的かつ客観的なセキュリティ開示⇒社外ステークホルダーへの説明

株式会社京都銀行様は、Secure SketCHの自動診断（SecurityScorecard）の診断結果とスコアを統合報告書に掲載し、ステークホルダーに対し客観的なセキュリティ開示を実施されました。

京都銀行

サイバーセキュリティの評価に客観性を持たせ、統合報告書でステークホルダーへの開示を実現

株式会社京都銀行

【事例】 外部評価を活用した取り組み

サイバーセキュリティへの取り組みにおいて、これまでの金融庁から還元される資料を基にした自己評価に加え、NRIセキュアテクノロジーズ株式会社が提供するSecure SketCHの自動診断機能(SecurityScorecard社のリスクレーティング連携)を採用し、客観的かつ俯瞰的な評価を活用した取り組みを行っております。

現時点では5段階評価の最上位評価かつ同業種平均を上回る評価を得ておりますが、発見された課題解決に取り組むとともに、リスク状況の変化に応じた将来的な情報セキュリティの高度化を図ってまいります。

【Secure SketCHによる評価結果(一部抜粋)】

診断ドメイン	kyotobank.co.jp
診断結果	A B C D F
スコア	91 /100 同業種平均：financial_services87

当行が2022年7月に発行したステークホルダーに向けの統合報告書に、サイバーセキュリティ向上の取り組みとして、評価結果を掲載することができました。セキュリティ対策状況の客観的なエビデンスを社外に開示することで、**当行に対する評価の視線の水準がワンステージあがった**ように感じています。（京都銀行様）

株式会社京都銀行 様｜導入事例｜NRIセキュア
https://www.nri-secure.co.jp/service/case/secureskeetch_kyotobank

© NRI SecureTechnologies, Ltd.

4．問合せサポートについて

© NRI SecureTechnologies, Ltd.

弊社サポート宛のお問い合わせについて

自動診断（SecurityScorecard連携）に関する基本サポート内容は、以下４つです。

基本サポート

１：自動診断で提供する機能の使い方の教示

２：自動診断の評価内容やスコアの算出ロジックの提供

３：弊社ヘルプセンター等で公開する情報提供

４：「解決申請」に対する却下理由の提示や解決に向けたフォロー

留意事項

※貴社固有の環境に対する課題の改善方法や対策の是非などについては、
基本サポート内でお答えすることはできません。

・各社固有のOSやシステムに対する脆弱性の対応方法、影響の調査
・各社のネットワーク構成に対する評価
・各社の環境に依存したSPFレコードやCSPの記載方法など

※ Secure SketCHヘルプセンターには、自動診断のよくあるご質問を掲載しております。
弊社サポート宛にお問い合わせいただく前に、ぜひ一度ご確認ください。

© NRI SecureTechnologies, Ltd.

Secure SketCH

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