セキュリティ対策実行支援プラットフォーム

Secure SketCH

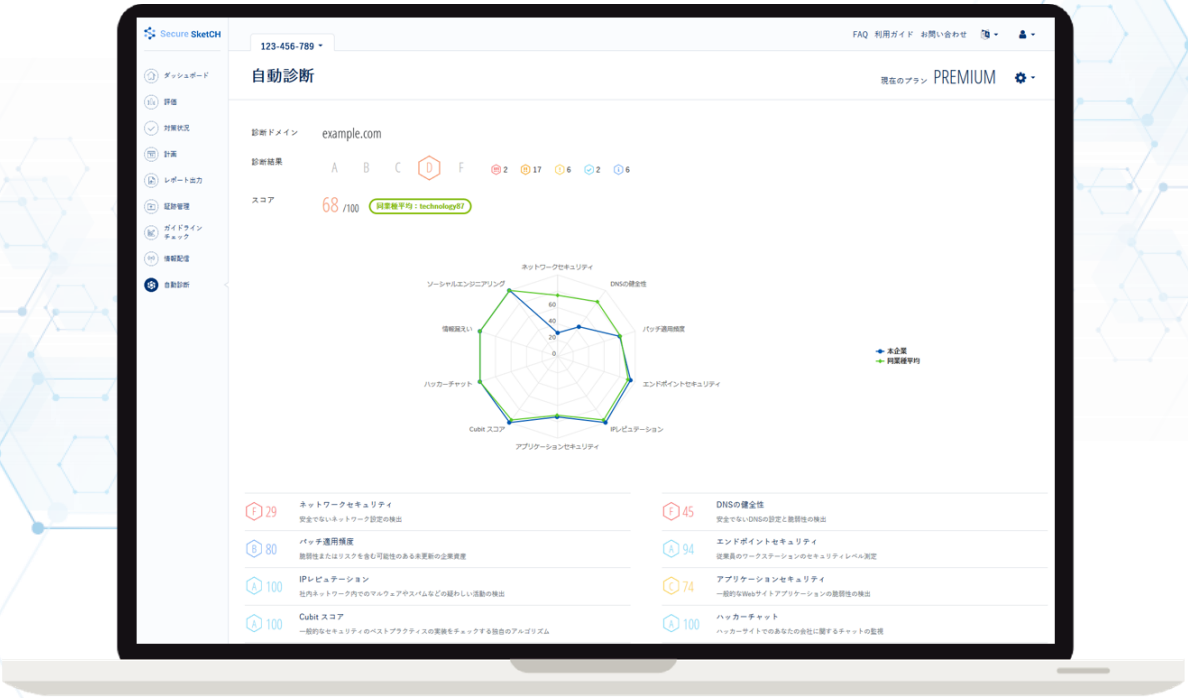
×

セキュリティ格付けサービス

SecurityScorecard

# Secure SketCH 自動診断機能

Ver.3.3　更新日2024/1/10




NRI SECURE

# セキュリティ評価における様々なご要望

## \\ これらのご要望は自動診断機能でご支援できます！ //

### 自社の<br>セルフチェック

- 負荷なく継続的にセキュリティ評価を行いたい
- Secure SketCHによる内部評価に加えて客観性のある評価を行いたい
- 他社と比較した自社の評価を定量的に把握したい

### サプライチェーン<br>マネジメント

- 世界中にあるグループ会社に対して手間をかけずに評価を行いたい
- グループ会社の担当者に負荷をかけずに評価を行いたい
- 業務委託を検討している企業のセキュリティ診断を事前に行いたい

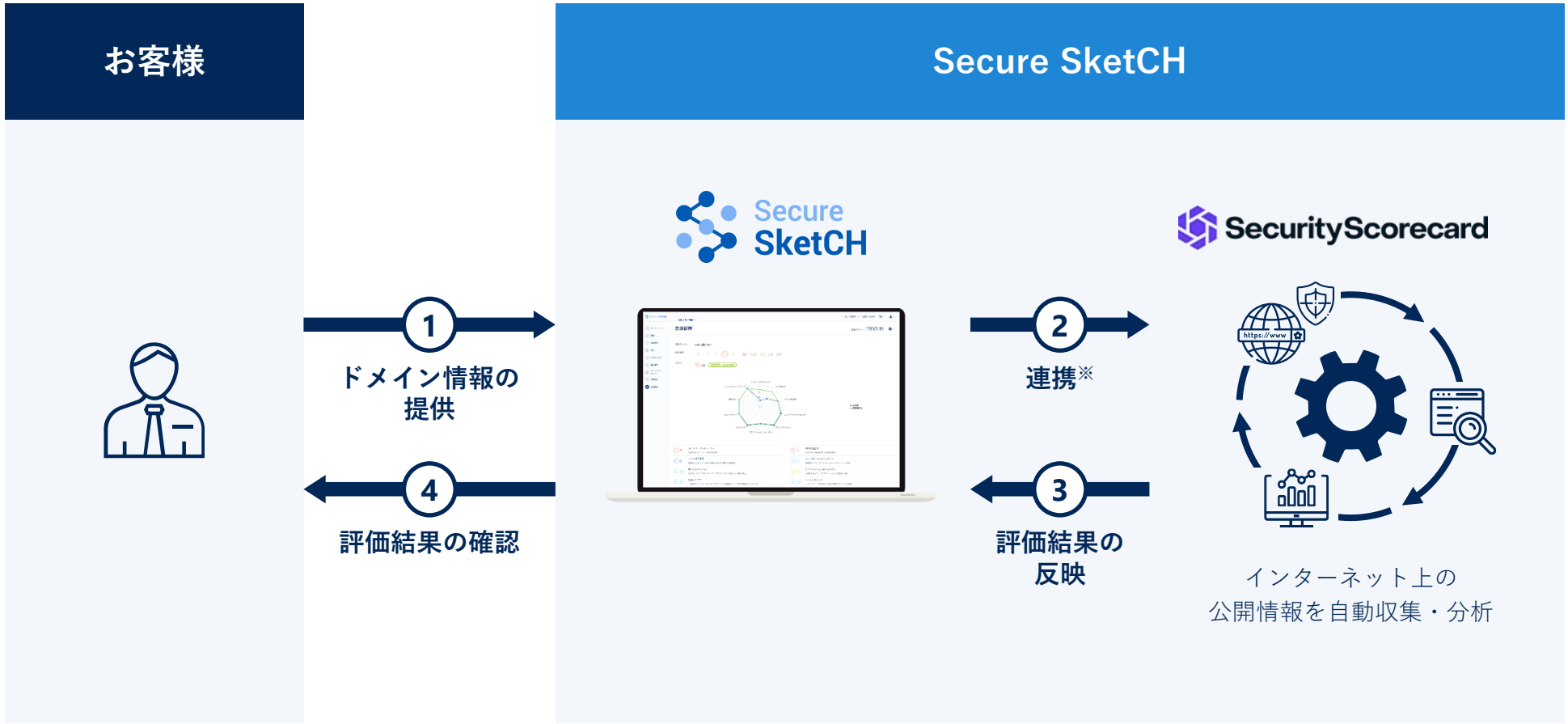
### サイバーセキュリティ<br>デューデリジェンス

- 買収対象会社のシステムに、情報漏洩や情報セキュリティ違反などのリスクがないか事前に調べたい

# 自動診断機能とは



ドメイン情報を元に、インターネット上の公開情報を収集・分析してセキュリティの弱点を評価する機能です。
外部視点の評価を自動で実施でき、作業負荷ゼロで自社や関連企業の客観的なセキュリティ評価を行うことができます。




※連携の設定は当社の担当者にて対応します。

# 10種類の評価項目



自動診断機能では10種類のカテゴリを約200の診断項目から判定し、A～D・Fの５段階で評価します。

### 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、RDPサービスの発見、脆弱なプロトコルをサポートしているSSL/TLSサービス


### DNSの健全性

安全でないDNSの設定と脆弱性の検出

例：SPFレコードなし、DMARCの設定がないSoftfailを含むSPFレコード

### 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：深刻度高の脆弱性を最近発見、深刻度高のCVEのパッチ適用頻度、EOS（サービス終了）製品

### 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ブラウザの発見、古いオペレーティングシステムの発見

### 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、攻撃の検知、悪意のあるスキャンが検出されました

### 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、HTTPを含むリダイレクトチェーン、Cookieに”Secure”属性がありません

### 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：ランサムウェアの影響を受けやすいリモートアクセスサービスの公開

### 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：不正侵入の疑い、ランサムウェアの被害者として宣伝されているドメイン

### 情報漏えい

会社機密情報の漏洩の可能性

例：リスクのある資格情報、情報漏洩の試み、資格情報が最大２年間危険にさらされています

### 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：公開された個人情報、タイポスクワットの可能性のあるドメインが検出されました

# 自動診断機能で実現できること



ドメイン情報だけで診断ができるので、負担なく効率的に客観的な評価を行うことができます。

## 客観的な視点での評価

データ・ファクトに基づき客観的に評価するため、内部評価では見落とされていたリスクに気づくことができます。

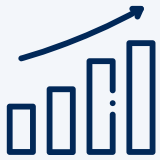
## 担当者の負荷ゼロ

評価シートへの回答やファイルの受け渡しはなく、システム担当者との調整が不要でシステム担当者にも負荷がかかりません。

## 地域に縛られず評価が可能

現地に行く必要もなく、ドメインさえ分かれば世界中どこの企業でも地域を超えて評価を行うことができます。

## 定量的に可視化



同業他社との比較や自分の弱点が点数として定量的にわかるため、報告がしやすく変化も視覚的に理解することができます。

# 1 診断結果の表示



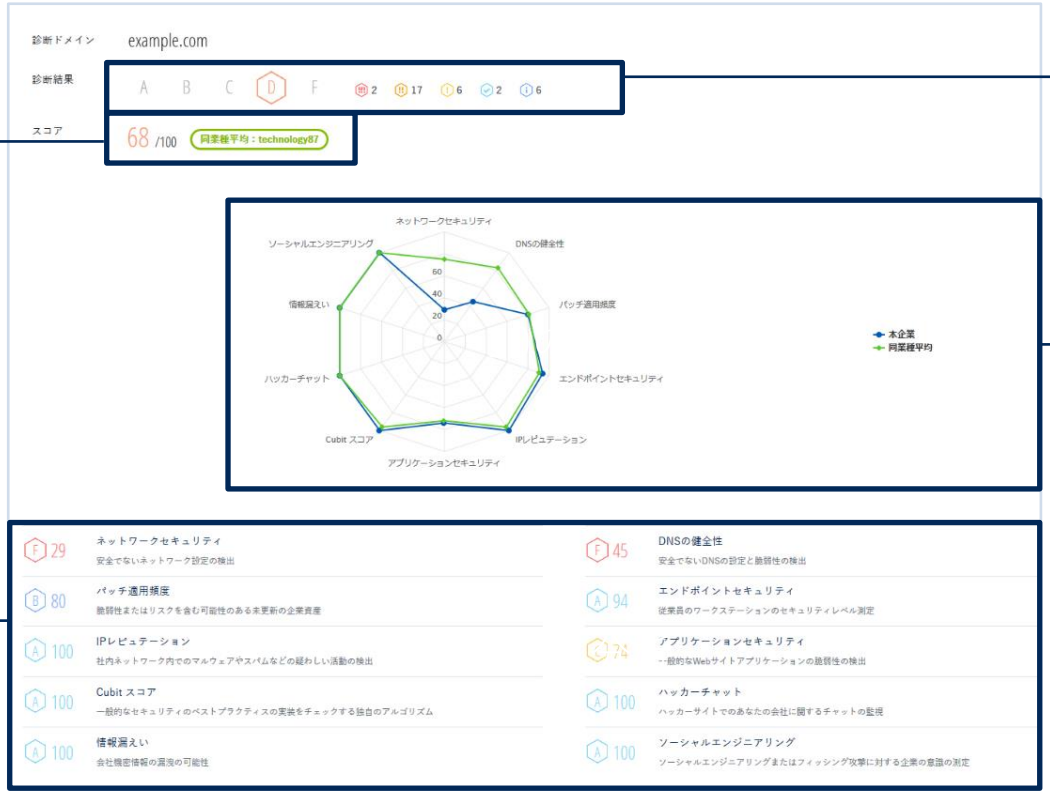
自動診断の評価結果を定量的に可視化します。
同業種と比較した結果や発見事項の深刻度合いも分かるので、何から対応するべきか簡単に判別ができます。

## 評価スコア表示

総合スコアを点数で表示

## 評価ランク表示

ランクはA～D・Fの５段階で表示




## 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
※SSC内の平均数値となります。

## 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

# 2 発見課題の確認



発見された項目の解説や、対策の推奨事項、同規模組織の対策状況を表示します。
具体的な指摘事項もわかるので、対応箇所がひと目で確認できます。

## 発見事項一覧表示

発見事項ごとの深刻度を表示

| 深刻度 | 減点 | 発見事項 | 件数 | 分野 |
|---|---|---|---|---|
| 高 | 0.2 | HTTPSを強制しないサイト | 3 | アプリケーションセキュリティ |
| 高 | 3.2 | オープンDNSリゾルバの検出 | 1 | DNSの健全性 |
| 中 | 0.8 | 弱い署名を使用するSSL証明書 | 1 | ネットワークセキュリティ |
| 中 | 0.8 | 深刻度中のCVEのパッチ適用頻度 | 133 | パッチ適用頻度 |
| 中 | 0.1 | 古いWebブラウザの発見 | 1 | エンドポイントセキュリティ |
| 低 | 0.7 | 失効制御のないTLS証明書 | 80 | ネットワークセキュリティ |
| 低 | 0 | マルウェアイベント, 1年以内 | 21 | IPレピュテーション |
| 参考 | 0 | タイポスクワットとみられるドメインを検出 | 17 | Cubit スコア |
| 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 | 1560 | ネットワークセキュリティ |

## 発見課題詳細

推奨対応やリスクを解説

評価結果と国内外の各種ガイドラインを関連付けてセキュリティ対策の実施状況を確認・管理することができます。

## ガイドラインごとのマッピング

各ガイドラインの項目に関連する自動診断関連課題を表示


### 対応ガイドライン（2024年5月現在）

- 経済産業省：サイバーセキュリティ経営ガイドライン Ver 2.0
  サイバーセキュリティ経営ガイドライン Ver 3.0
- NIST：Cyber Security Framework ver.1.1
- ISO 27001
  ISO/IEC 27002:2022
- CIS：CIS Controls V7.1
  CIS Controls V8
- NIST：SP800-171 Rev2
- 米国防総省：CMMC 1.0

# その他便利な機能

その他にも様々な便利な機能を有しております。

## レポート出力画面

自動診断の評価結果をレポート出力でき、社内での共有や報告に活用できます。


## 得点タイムライン表示

各カテゴリーごとのスコアを時間軸で表示できます。


## イベントログ

変更された評価の詳細を過去に遡って確認できます。


## 評価変動の週次連絡

評価結果に変動があった場合の、お知らせのメールを週次配信を設定できます。

## 発見課題のCSV出力

発見課題の一覧をCSVで出力することもできます。

## 解決申請

Security Scorecard社への課題解決申請が可能です。

## 多言語対応

英語と中国語（簡体字）にも対応していて、海外拠点の評価もできます。

# 設問回答による診断との相乗効果

設問回答による内部評価と自動診断機能による外部評価を組み合わせることで、
社内視点と攻撃者視点の両面からの多面的な評価を行うことができます。

## 社内視点の内部評価

### 設問回答による診断

約80問の設問に回答するだけで、
自社のセキュリティ対策状況を可視化

## 攻撃者視点の外部評価

### SecurityScorecard

ドメイン情報をもとに自動でインターネット上の
公開情報を収集・分析し、セキュリティレベルを評価

### 360度からの多面的な評価

# 様々な活用シーン

自動診断機能は自社のセルフチェックからサプライチェーン全体まで
様々なセキュリティ評価のシーンでご活用いただけます。

ユースケース 1

## 自社のセルフチェック

＜自社＞

自社のセキュリティ担当者が多忙でも客観的な評価を継続的に実施できます。

ユースケース 2

## グループガバナンス

＜子会社・関連会社＞

担当者との調整なしでグループ全体の対策状況を客観的に評価でき、各社のデータを一元管理できます。

ユースケース 3

## グローバルガバナンス

＜海外拠点＞

現地への渡航や担当者との調整なしで海外拠点の対策状況を客観的に評価でき、各拠点のデータを一元管理できます。

ユースケース 4

## サプライチェーンマネジメント

＜取引先・委託先＞

関係各社との調整なしでサプライチェーン全体の対策状況を客観的に評価でき、各社のデータを一元管理できます。

ユースケース 5

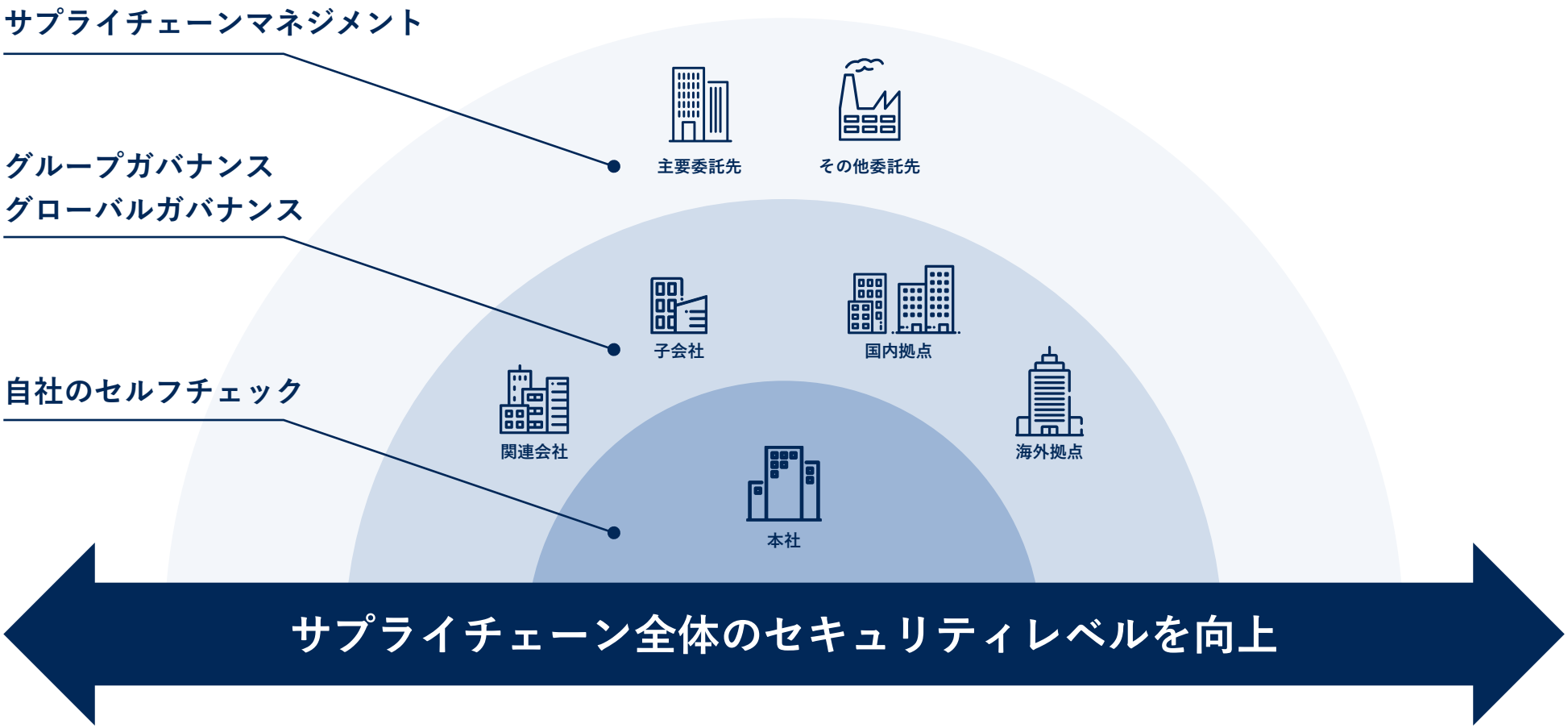
## サイバーセキュリティDD

＜買収対象会社のシステム＞

買収対象会社のシステムに、情報漏洩や情報セキュリティ違反などのリスクがないか、セキュリティ評価に活用できます。

# サプライチェーン全体への展開

Secure SketCHを活用いただくことで、自社のセルフチェックだけでなくサプライチェーン全体で
セキュリティ対策状況を可視化して、攻撃リスクに備えることができます。



# よくある質問(1/2)

**Q** **評価結果はどのくらいの頻度で更新されますか？**

**A** 発見事項の種別に応じ、日次／週次／月次の頻度で結果が更新されます。

**Q** **評価に利用するデータは何ヶ月前のものですか？**

**A** 基本的に常に最新のデータを評価に用いていますが、一部評価項目では異なる場合があります。

**Q** **サブドメインは評価できますか？**

**A** 登録できるのはメインドメインのみです。ドメイン情報から関連するIPアドレス検出し、評価します。
そのため、サブドメインも評価対象に含まれます。

**Q** **評価項目は変わりますか？**

**A** 近年のサイバーセキュリティ脅威やトレンドの進化を踏まえて、評価項目は定期的に見直しされます。
また、発見事項の深刻度、スコアリングロジックについても定期的に見直されますので、最新の脅威に対応できます。

**Q** **Webアプリケーション/プラットフォーム診断との違いは何ですか？**

**A** 自動診断はインターネット上に公開されている情報を用いて企業のセキュリティリスクの評価を行うため、
Webアプリケーション診断とは異なり、評価対象のシステムに負荷をかけません。
そのため、評価対象は自社システムに限らず、グループ会社や取引先企業などのあらゆるサプライチェーン全体の
セキュリティリスクの継続的な評価に活用できる点が特徴です。

これらの質問以外でお困りの場合、ヘルプセンターもぜひご活用ください。
https://www.secure-sketch.com/knowledge

# よくある質問(2/2)

**Q** **コーポレートHPのドメインとサービス（ネットスーパー等）ドメインを保有している場合、どちらを登録するのがよいですか？**

**A** コーポレートHPのドメインを登録する企業様を多くお見受けします。
背景としては、自動診断ではエンドポイント等含む10項目の評価カテゴリがあり、
コーポレートHPのドメインを登録する方がより広範囲で情報収集が可能なためです。
ただし、BtoC向けサービスやECサイトが主要事業の場合は、サービスドメインを登録する企業もいらっしゃいます。
なお、双方を登録することも可能です。（この場合、登録ドメイン数分のご契約が必要です。）

**Q** **コーポレートHPのドメインと、メールドメインが異なる、どちらを登録する方が有効ですか？**

**A** コーポレートドメインを推奨します。
メールドメインのみで利用している（Aレコードが存在しないドメイン等）場合は評価ができかねます。

**Q** **子会社の評価を行いたいのですが、メールドメインは親会社のドメインを使っているかつ、
HPは親会社のサブドメインを利用している場合、子会社としての評価はできないのでしょうか？**

**A** 上記ケースの場合、評価を実施する場合は、親会社のドメインを登録する必要があります。
その場合、親会社の資産や課題も評価対象に含まれるので、子会社単体としてのスコア結果は算出されません。
大量の資産が発見される中で、子会社に関連する資産を特定し、改善対応を行う必要があります。

**Q** **委託先管理用途で、クラウドサービスの評価に自動診断を利用したいです。
クラウドサービスのドメインがサブドメインとなっている場合は、当該サービスのメインドメインを登録するのがよいでしょうか？
その場合、評価したいクラウドサービス以外の情報も含まれてしまうと思いますが、どうすればいいでしょうか？**

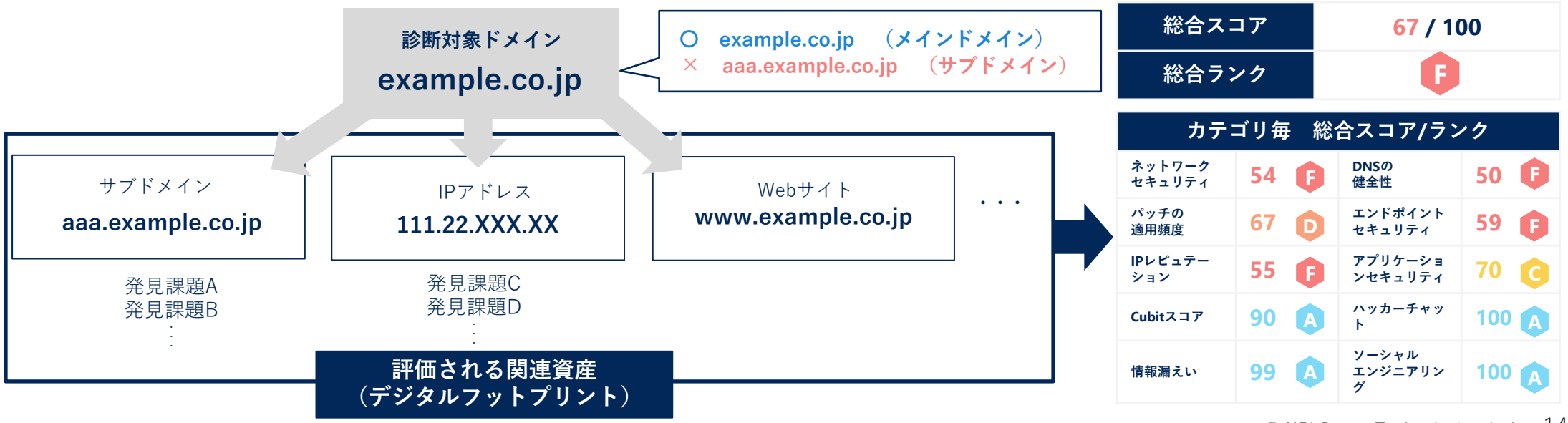
**A** 前提として、自動診断は企業全体のセキュリティ対策状況を包括的に評価することを目的としたとした評価サービスです。
評価実施する場合は、いずれもメインドメインを登録いただく必要があるため、当該サービスのメインドメインを登録する必要がございます。
特定クラウドサービス（サブドメイン等）を評価対象として指定することはできませんので、ご了承ください。
なお、セキュリティの観点から、メインドメインのDNSやSSL設定に被害・侵害があった場合、
配下のサブドメイン（サービスドメインなど）も影響を受ける可能性があるため、そういった全体のリスク管理視点でご活用いただけます。

これらの質問以外でお困りの場合、ヘルプセンターもぜひご活用ください。
https://www.secure-sketch.com/knowledge

# ご利用時の注意点

## 評価対象ドメインの選定時の注意事項

- 診断対象として設定可能なドメインは「**メインドメイン**」のみです。
  自動診断機能では、設定したドメイン情報を元に関連資産（サブドメインやIPアドレス、等）をデジタルフットプリントとして収集し、
  組織全体が持つ脆弱なポイントを包括的に発見し、総合的な評価やランク付けを行います。
  そのため、サブドメインやIPアドレスなどの特定の資産のみを診断・スコア算出することはできません。
- 以下は診断対象として、設定できません。
  ・サブドメイン
  ・リダイレクト元のドメイン（例：example.com➔example.co.jpにリダイレクトされている場合の前者ドメイン）
  ・Aレコードが存在しないドメイン（メールのみで利用など）



# ご利用時の注意点

## 契約周りの注意事項

- ドメイン設定後、評価結果が表示されるまで3営業日ほどかかる場合があります。
- ドメイン設定後、ご契約期間中の診断ドメインの変更はできません。
- ドメイン変更については、ご契約更新のタイミングで可能です。
  変更をご希望の場合は、ご更新可否と併せて、ご連絡ください。

※上記条件を満たしていないにも関わらず、登録時にエラーが発生する際には 、
Secure SketCHサポートチーム（support@secure-sketch.com）までご連絡ください。

# お申し込み方法

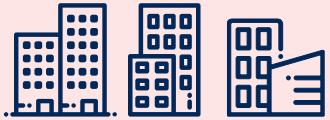
1社でご利用の場合はPREMIUMプラン、複数社でご利用の場合はGROUPSプランへの加入が必要ですので、
まずは下記「お問い合わせフォーム」よりお問い合わせください。
プラン加入後にドメイン情報をご提供いただき、当社の担当者にて機能の連携を行います。

1社でご利用の場合

**SINGLEプラン**

複数社でご利用の場合

**GROUPSプラン**
**3rd PARTYプラン**



**お問い合わせフォーム**

**https://app.secure-sketch.com/inquiry/new**

NRI SECURE