



SecurityScorecard



セキュリティ リスク レーティング サービス

総合評価

C 72

脅威指標

- B 86** ネットワーク・セキュリティ
セキュアでないネットワーク設定の検出
- D 60** DNSの正常性
セキュアでないDNS設定と脆弱性のある検出
- B 82** パッチ適用程度
脆弱性リスクを含む可能性のある古い脆弱性
- D 61** エンドポイント・セキュリティ
従業員がアンチウイルスソフトウェアをインストールしていない脆弱性
- C 75** IPレピュテーション
企業ネットワーク内のIPアドレスがスパム送信元として悪名高い脆弱性
- B 82** アプリケーション・セキュリティ
脆弱なウェブアプリケーションの脆弱性
- A 90** キュービット・スコア
一般的なウェブアプリケーションの脆弱性をチェックする脆弱なアルゴリズム
- A 100** ハッカーチャッター
脆弱なウェブアプリケーションの脆弱性をチェックする脆弱なアルゴリズム
- A 90** 運送された情報
脆弱なウェブアプリケーションの脆弱性をチェックする脆弱なアルゴリズム
- C 70** ソーシャル・エンジニアリング
脆弱なウェブアプリケーションの脆弱性をチェックする脆弱なアルゴリズム

項目毎の評価 (10項目)

業界内比較: 業種名

業種平均との比較

検知された脆弱性

脆弱性	検出数
高いリスクポート	7
サイトの脆弱性	6,693
検出されたマルウェア	0
運送された情報	0

ソリューション概要:

サプライチェーン攻撃へのリスクを瞬時に点数化し、改善すべきポイントを可視化するスコアリング・サービス。

経済産業省がオブザーバーとして参加しているサプライチェーン・サイバーセキュリティ・コンソーシアム (SC3) でも、「大企業と中小企業がともにサイバー・セキュリティ対策を推進する」と謳っているとおり、企業の大小を問わず産業界を挙げたサプライチェーン全体のサイバー・セキュリティ強化が急務です。

「SecurityScorecard」は、そのようなサプライチェーン攻撃へのリスクを、総合評価、10項目のリスクファクターについて5段階/100点満点でスコアリングし、改善すべきポイントを可視化するレーティング サービスです。自社だけでなく、サプライチェーン全体のセキュリティ・リスク耐性を把握することができます。

特長:

1. 攻撃者目線で、インターネットなどからドメインに紐づくセキュリティ・リスクを常時収集し、今後サイバー攻撃を受ける可能性を示唆する詳細なリスク分析結果を提供
2. セキュリティ・リスクを総合評価/10項目のリスクファクターについて、5段階 (A ~ D/F) および 100点満点で評価し、社内 (グループ会社 / 経営陣など) や取引先との目標設定や対応策を明確化
3. 対象システムの運用に侵入することなく分析可能

参照リンク:

公式ページ: <https://securityscorecard.com/jp>

インテルのパートナー企業による、すぐに導入可能なソリューションは、インテル® ソリューション・コネクトをご覧ください。
<https://www.intel.co.jp/SolutionConnect>

