Professional Security Services

セキュリティ診断による脆弱性の発見・攻撃の未然防止

多種多様な業種のお客様をご支援してきた経験豊富な富士通のセキュリティ専門家が、組織のリスクマネジメントや、最新の手法を用いて診断・評価・分析し、脆弱性がもたらす危険性と対策方針を提言するなど、お客様の課題解決やお客様自らのセキュリティ成熟度向上に向けた自走もご支援いたします。

情報システムを取り巻く脅威は、日々変化しています。複雑・多様化する様々な脅威からシステムを守るためには、システムに潜む脆弱性を把握することが重要です。富士通のセキュリティ診断サービスは、OSINTベースのレーティングツールであるSecurityScorecardを活用したリスクレイティングサービスと、特定の範囲をより深く調査する診断サービスによりお客様のシステムに存在する脆弱性を最新の手法で調べあげ、問題点と解決策をご提示します。

お困りではありませんか？

- セキュリティを強化したいが、何から手をつけてよいか分からない
- システムにセキュリティ上の問題点がないかどうかを知りたい
- Webサイトや公開サーバ、スマートフォンアプリ等、様々な対象のセキュリティを強化したい

富士通が解決します！

- ✓ システムのセキュリティレベルを正確に把握することができます
- ✓ 優先順位を付けて、計画的に対策していただくことができます
- ✓ 複数の診断手法を組み合わせることで、多層的にシステムを評価しセキュリティを強化することができます

サービスラインナップ

代表的なサービス名を掲載しています。下記以外にもPCI DSS ASVスキャン、スマートフォンアプリ診断、MITRE ATT&CKアセスメント等の複数の診断サービスをご用意しております。

アタックテストサービスエクスプレス

サーバやネットワーク機器に対して、ネットワーク経由で様々な検証を行い、稼働するサービス経由で、OSやアプリケーションの既知の脆弱性を調査します。

主な診断項目
- ポートスキャン
- ネットワーク情報の収集
- バナー情報の調査
- サービス、ソフトウェア、OSの既知の脆弱性
- 暗号化処理
- 設定の不備　等

Webアプリケーションセキュリティ診断

Webアプリケーションに対して、攻撃者の観点で様々な操作を行い、Webアプリケーション特有の脆弱な実装や設定の不備を調査します。

主な診断項目
- SQLインジェクション、コマンドインジェクション
- クロスサイト・スクリプティング
- セッションフィクセーション
- 認証・認可の脆弱性
- ディレクトリトラバーサル
- クロスサイトリクエストフォージェリ　等

ペネトレーションテスト

システムに対して、実際の攻撃コードを用いて、侵入できるかどうかという観点でテストを行い、安全性と耐性を評価します。

主なテスト項目
- ログイン試行
- システム情報の収集
- 既知の脆弱性の調査
- 脆弱性の利用、Exploit実行
- 侵入・重要情報の収集　等

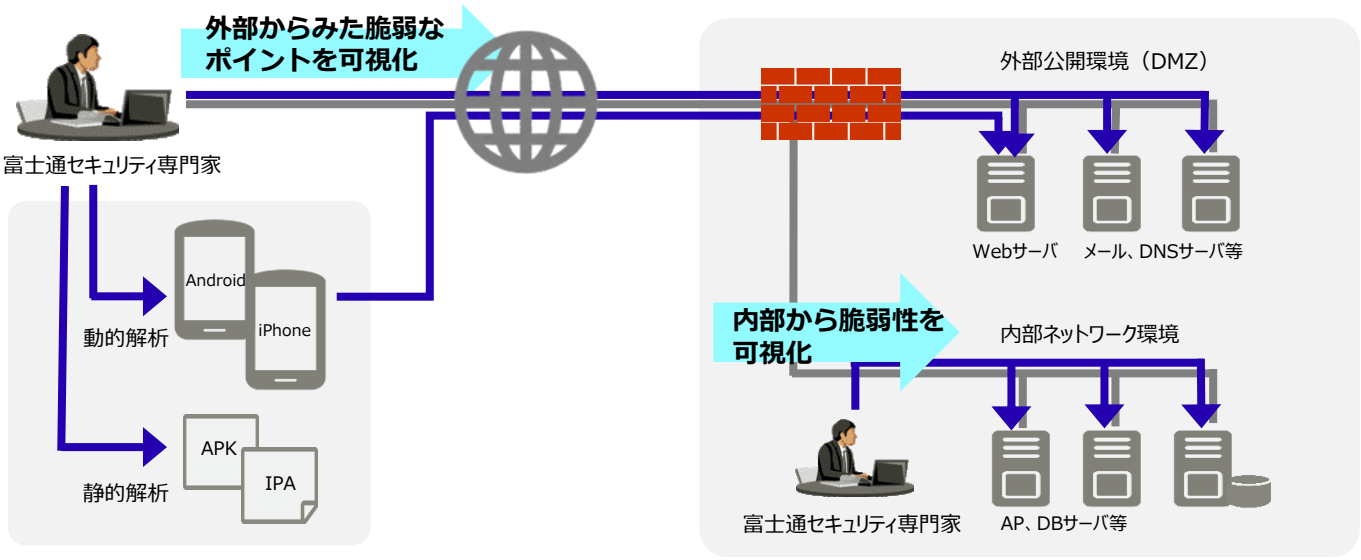
セキュリティリスクレイティングサービス

貴社ドメインに対して、攻撃者視点で公開情報分析を行い、貴社のセキュリティリスクを可視化し、サプライチェーン全体の脆弱性対策をご支援します。

主な調査項目
- OSINTベースで把握するセキュリティリスクの可視化
- サプライチェーン全体のセキュリティリスクと脆弱性の評価
- 不審な通信やマルウェア感染の早期検知と迅速な対応
- 公開された脆弱性情報と不要なネットワークポートの特定
- 漏洩した認証情報による不正アクセスのリスク軽減
- サイバー攻撃の予兆検知とプロアクティブな対策の実施

セキュリティ診断サービスご提供イメージ

富士通のセキュリティ専門家が、インターネット経由またはお客様環境にお伺いして診断を行います



セキュリティ診断サービス提供の流れ

ヒアリング・計画
システム概要をお聞きしお客様に適した診断計画を立案します。

診断実施
経験豊富なセキュリティ専門家が対象システムの脆弱性を調査します

結果解析・報告
結果を解析し、対処が必要な脆弱性を対処方法とあわせて報告書にまとめ、ご提示します

アフタサポート
診断結果に関する不明点が生じた場合のQAサポートや、対処完了後の再診断をご提供します

セキュリティリスクレイティングサービスの「利用ライセンス」モデルをご利用の場合は、別途ご案内します。

セキュリティ診断サービスの特長

国の認定を受けたサービスをご提供します

「情報セキュリティサービス基準」として経済産業省が求める技術要件や品質管理要件を定めております。弊社の脆弱性診断サービスはこの基準に適合するサービスとして登録されております。（サービス登録番号：018-0016-20）

018-0016-20

情報セキュリティサービス基準登録サービス
- Web アプリケーションセキュリティ診断サービス スタンダード
- Web アプリケーションセキュリティ診断サービス アドバンスト
- アタックテストサービス エクスプレス スポット診断サービス

高度なセキュリティ知見を持つ専門家がご提供します

各種セキュリティ関連資格を有する経験豊富な専門家が診断作業を実施します。
例）PCI DSS ASV, CISSP, CISA, OSCP, CEH, 情報処理安全確保支援士等

豊富な実績により安心してご利用いただけます

2,000社以上のお客様や社内実績から培ったノウハウをベースに診断をし、脆弱性の対策をアドバイスします。またクレジットカード業界におけるPCI DSSや、自動車業界におけるWP29などのセキュリティ基準への準拠に向けたレギュレーション対応における診断実績も多数あります。

複数の手法を用い脆弱性を多角的に調査します

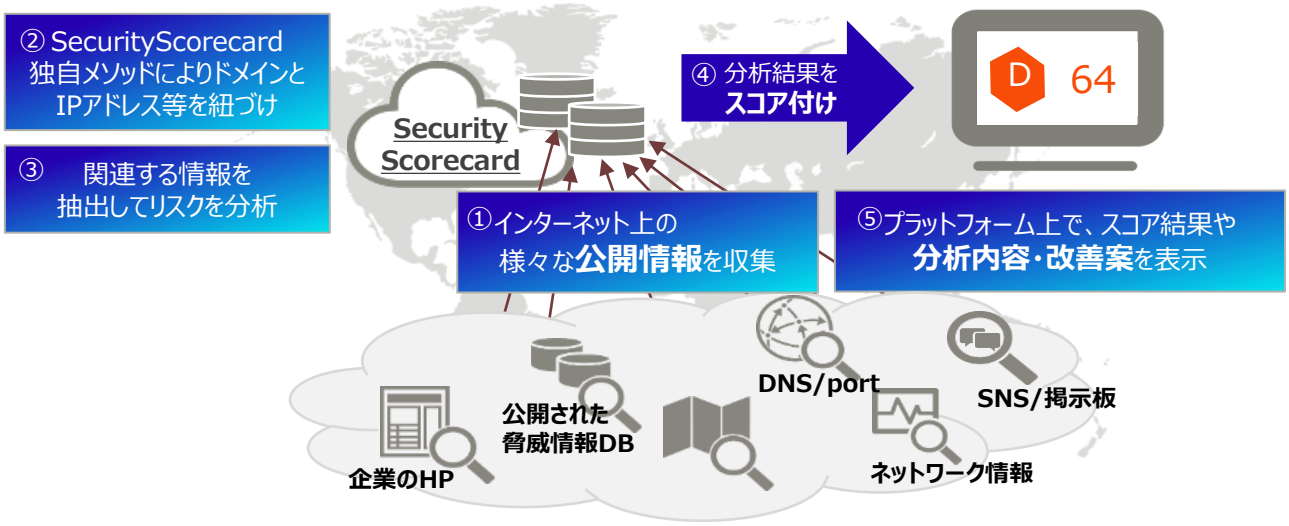
ICTシステムの多様化に伴い、診断手法や診断範囲も拡大しています。脆弱性検出においては、業界で評価の高い商用ツールに加えて、独自開発ツール、専門家による手動診断等、さまざまな手法を組み合わせて、総合的に診断します。常に最新の脆弱性情報を収集し、診断手法に反映しています。

サービス提供後もお客様を強力にサポート

セキュリティ対策は、継続的に実施していく必要があります。富士通はシステムインテグレーターの強みを生かし、診断後もお客様のよりセキュアなシステム構築と運用をご支援します。

セキュリティリスクレイティングサービス

サイバー攻撃は、公開情報を悪用し、サプライチェーンの脆弱性を突いて巧妙化の一途を辿っています。自社の対策だけでは不十分であり、サプライチェーン全体のセキュリティ状況を把握することが不可欠です。
当社は、SecurityScorecardを活用し、攻撃者視点での公開情報分析を通じて、貴社のセキュリティリスクを可視化します。そして、その可視化されたリスクに基づき、サプライチェーン全体の脆弱性対策を、当社の専門知識と経験をもってご支援し、「攻撃されにくい環境」の実現をサポートいたします。



サイバーセキュリティリスク評価の特長

- 対象のセキュリティ状態を、5段階で格付け(A/B/C/D/F)
- 組織全体と10の評価カテゴリーで格付け（**224以上※の調査リスク項目**）
- SaaS型のセキュリティ格付けサービス
- ダークウェブや漏えいした情報も調査
- 調査対象に対して**侵入的なスキャン等は行わない**
- 業界トップの**約1,200万社**※のスコア実績
- 収集や分析などをすべて**自動化し公平な評価**
- **攻撃者が収集可能な外部情報**を収集して分析
- 検知リスクの収集手段が根拠が公開されている
- 市場調査会社Forresterの、2024Q2のレポートで **最高の評価**（Leader）
- **ASM**(Attack Surface Management)の観点でも活用可能

※ 2024年5月現在

おもなユースケース

サプライチェーン管理	・契約先や業務委託先のセキュリティレベルの管理および向上 ・委託先だけではなく、再委託先等も同時に管理
委託先やサプライヤーの選定評価	・契約予定の企業のセキュリティリスクを事前の確認 ・与信調査だけではなく、セキュリティ対策レベルを調査し、構築したサプライチェーンのセキュリティレベルを維持
グループ統制	・海外子会社を含めたグループ全体のセキュリティレベルの強化 ・時差や言語、文化の違い等に悩まされない一元管理
自己監視	・自社のセキュリティリスクの改善や経営層への報告・方針説明 ・部署単位や事業所単位の評価

ご提供モデル

ご検討にあわせて大きく2つのモデルをご提供

	コンサルティングサービス （1回 / 定期評価）	利用ライセンス
概要	富士通のコンサルタントによる分析・評価結果報告書の作成、改善策ご提示	お客様にライセンスを購入頂き、SecurityScorecardをご利用いただく
ライセンス	当社が保有（1ドメイン評価あたりの課金制）	お客様が保有（自組織＋10ドメイン～）
コンサルタントのサポート	あり	活用トレーニングや稼働支援、運用代行など個別対応メニューあり
メリット	• SecurityScorecardの操作知識が不要 • 要点を押さえたレポートでのご報告が可能	• 登録したドメインの脆弱性を常時監視可能 • アラート通知、各種レポート等の機能の有効活用
注意点	• 評価対象が増えた場合、調査毎に費用が発生	• 部門のリソース、運用にあたっての知識についてフォローが必要
おもなご利用ケース	各基準等で内部的なリスクの洗い出しは実施しているが、実際に外からどう見えているかについては把握できていない	グループ各社のセキュリティ対策は任せっきりになっており、どこまで対策ができているのか把握できていない

コンサルティングサービス

コンサルティングサービスご提供の流れ

1準備
調査対象の選定
対象ドメインを決定します

2 調査
SecurityScorecardによる結果を出力
ドメイン情報からリスクを評価

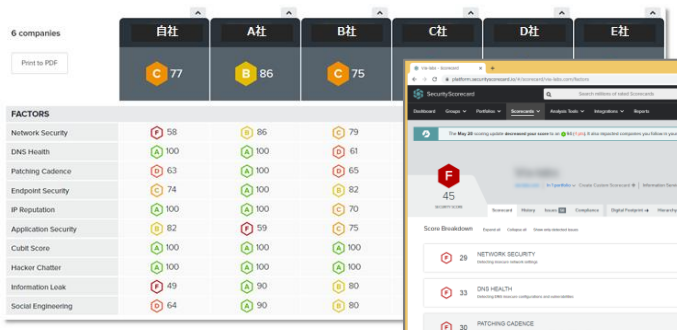
3 解析
当社コンサルタントによる分析
評価結果の精査、業界平均との比較、リスクの優先度

4 報告
リスク評価と対策のご提案

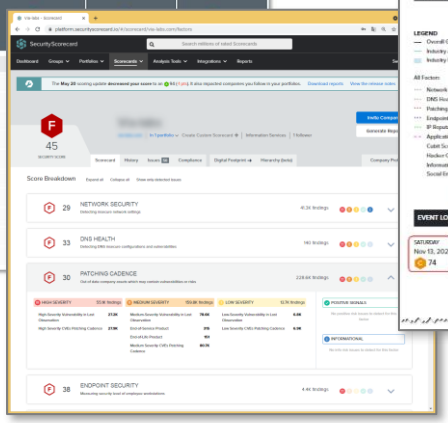
コンサルティングサービスでは、SecurityScorecardで出力されるサマリーレポート、詳細レポートに加え、富士通独自の提言書を取りまとめ、リスクに対する改善案含め分かりやすくご報告します

ライセンスご利用サービス

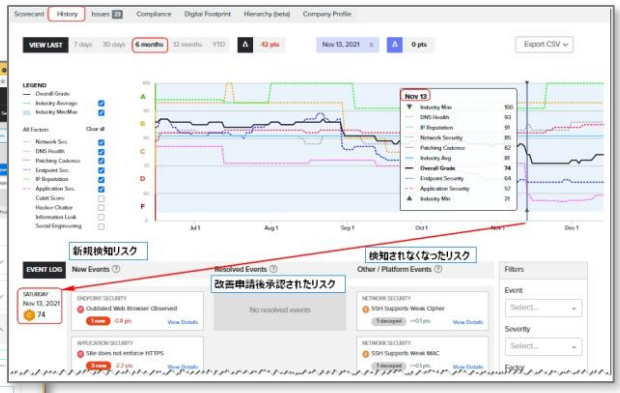
ライセンスを購入いただき、お客様ご自身でSecurityScorecardを操作・運用いただけます。
SecurityScorecardのフル機能を活用し、グループ企業・サプライチェーン統制に活用できます



■ 診断画面イメージ：総合評価



■ 診断画面イメージ：詳細評価、問題点など



■ 診断画面イメージ：スコア変動

ライセンスご導入時のサポート

① **利用開始時のセットアップ支援**
② **利用に関するメールベースでの日本語QA対応**
③ **四か月に一度、オンライン打合せの実施**
- 利用状況のヒアリングやそれに伴う不明点を解決

④ **製品アップデート情報の提供**
⑤ **検知された問題点解決のための当社ソリューションのご案内**

ご導入事例

コンサルティング　ご導入事例　某大学様
支援機関１カ月、目的：自組織の外部評価

課題
- 大学の情報セキュリティに対する意識が低かった。
- 情シス管理外のシステムのセキュリティ対策が放置されていた。

支援のポイント **大学の情報セキュリティレベルの見える化を実現**
- 大学自体の情報セキュリティレベルの向上を目的として、利用者や管理者、経営層向けに研修の実施や内部監査も同時に支援を実施。
- 評価だけでなく、問題検知の際に、影響範囲の調査や、対処後の脆弱性確認もワンストップで提供。

効果
- 認識できていなかった不正アクセスを検知できるようになり、教員に対する、情報セキュリティ意識を啓蒙。
- セキュリティリスクの可視化（スコア化）により、全学セキュリティ活動の効果を定量的に報告できる。

今後の活動
- 中高や後援会等、大学の関連組織全体のセキュリティリスクの管理。
- ライセンスを購入してもらい、業務委託先などを大学で管理。

当社 ご支援内容

教育や内部監査も支援 全学での情報セキュリティレベル向上を目的として、利用者や管理者、経営層向けの研修や、内部監査も同時に支援を実施。※別メニューとの組合せにてご採用	**検知だけでなく影響範囲や再構築も支援** SecurityScorecardでの結果報告だけでなく、不審な通信の影響範囲の調査や、再構築したサーバの脆弱性確認も追加で支援。

お問い合わせ先

富士通株式会社
富士通コンタクトライン（総合窓口）0120-933-200
受付時間：9:00～12:00および13:00～17:30（土・日・祝日・当社指定の休業日を除く）
お問い合わせフォーム