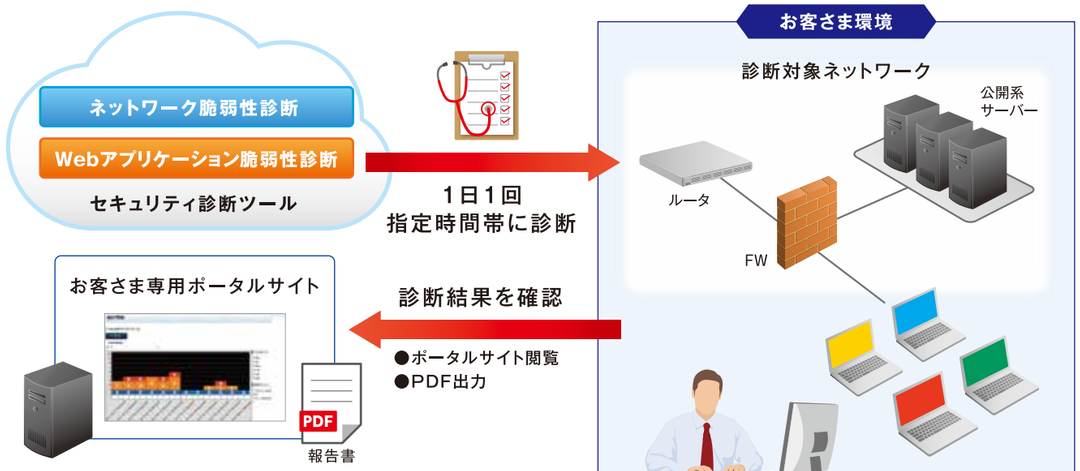
# デイリー自動診断

デイリー自動診断は、独自に開発した診断ツール※を使って1日1回自動で診断を行います。診断結果は、専用ポータル画面でご報告します。毎日、定期的に診断を行うことで、日々増加する脆弱性を即座に発見することができます。

※OWASP Top10／SANS Top20の世界的なセキュリティ基準に準拠




発見された脆弱性は緊急度毎に色分けされたグラフで毎日報告されます。
新しい攻撃手法が発見された時の影響や対策を行った時の効果などが一目で分かります。

## ■サービス内容

| 項目 | 内容 | 対象数（※2） |
|---|---|---|
| 診断対象（※1） | ネットワーク脆弱性診断 | 5 IPまで |
| | Webアプリケーション脆弱性診断 | 1 FQDNまで |
| 診断周期 | 日次・週次・月次より選択可 | ※ネットワークとWebアプリケーションでそれぞれ異なる設定が可能です。 |

※1 インターネットに公開されているシステムとなります。
※2 IP数やFQDN数を追加するオプションもございます。

## ■サービス料金　Webアプリケーション脆弱性診断の内容により、メニューをお選びいただけます。

| 標準メニュー | 内容 | 年間料金（税別） |
|---|---|---|
| ベーシックスキャン | Webアプリケーション診断において、ログイン認証を必要としないページを診断する場合 | 300,000円 |
| フルスキャン | Webアプリケーション診断において、ログイン認証以降のページも診断範囲に含む場合<br>※認証方式によって診断ができない場合がございます。 | 600,000円 |

※ネットワーク脆弱性診断は、ベーシックスキャン及びフルスキャンの差異はございません。


STNet
エスティネット　検索
eigyo@stnet.co.jp
TEL 087-887-2404（ビジネス営業本部）
※お問い合わせの回答は営業時間内（平日9:00～17:00）となります。

本店ビジネス営業部 ／ TEL.087-887-2404　首都圏営業部 ／ TEL.03-4588-4211
香 川 支 店 ／ TEL.087-887-2480　愛 媛 支 店 ／ TEL.089-906-2480
徳 島 支 店 ／ TEL.088-635-2480　高 知 支 店 ／ TEL.088-879-2480


STNetのサービスが、皆さまのビジネスの力に。

データセンター・クラウド　ネットワーク　システム開発

(S)SS2-1



STNet　STNetのサービスが、皆さまのビジネスの力に。

貴社のネットワークやWebサイトは**安全だと言えますか？**

情報セキュリティ対策を考えるには「**現状の可視化**」「**脆弱性を知る**」ことが重要です。

# セキュリティ診断サービス

## 本当に診断をしないといけませんか？

### ソフトウェア等の脆弱性関連情報に関する届出状況

ウェブサイトの脆弱性に関する届出件数の累計は9,628件

**全体の約7割を占めています**

| サービスメニュー | 2017年10月～12月 | 累計 |
|---|---|---|
| ソフトウェア製品 | 37件 | 3,895件 |
| ウェブサイト | 33件 | 9,628件 |
| 合計 | 70件 | 13,523件 |


出典:独立行政法人 情報処理推進機構（IPA）ソフトウェア等の脆弱性関連情報に関する届出状況［2017年第4四半期（10月～12月）］

- ⚠ ますます洗練化・巧妙化する攻撃手法、日々増加する脆弱性
- ⚠ 個人情報だけでなく、会社の機密情報もターゲットに
- ⚠ サーバーの乗っ取りで、被害者だけでなく加害者になる可能性も

## » お困りではありませんか？

- 何から手をつければよいか分からない… → 解決 調査結果から診断範囲を決められます
- 費用はできるだけ抑えたいが… → 解決 安価で簡単な自動診断もあります
- 診断を受けてもその後の対処が不安だ… → 解決 報告会でしっかりサポートします

## STNetがその解決策をご提案します！

※本サービスは、株式会社ブロードバンドセキュリティと協業してご提供いたします。

# 手動型セキュリティ診断

オンライントレードやショッピング、情報公開など、Webを活用したビジネスは今や組織にとって必要不可欠な存在になりました。
その一方で、情報システムへの侵入経路として悪意ある攻撃を受ける対象にもなっており、組織にとって、その脆弱性を排除することはコーポレートガバナンス上、必要不可欠な事項となっています。手動型セキュリティ診断は、ツール診断と手動診断を組み合わせて実施し、このような悪意ある攻撃を受ける前に、自らリスクを発見し、防御するための問題特定ツールです。

## サービス種類

| | |
|---|---|
| ネットワーク脆弱性診断 | システム全体に影響を及ぼすネットワークを外部から診断します。 |
| Webアプリケーション脆弱性診断 | インターネットを介して外部からWebアプリケーションの脆弱性を診断します。 |

※このほか、オンサイト診断もございます。詳しくは当社営業担当までお問い合わせください。

## サービス利用の流れ

**STEP 1**　診断前準備・調査 → クローリング → POINT 対象画面の機能分析

- クローリング※を実施し、診断対象機能・リクエストの選定と検査手法を設定いたします。
  ※機能・画面・URL・パラメータ・値・アクセス時の留意事項をリクエスト単位で調査します。
- 手動での詳細な確認では、機械的な判断では見落としてしまう画面遷移・分岐にも対応いたします。

**STEP 2**　診断実施　POINT 複数ツールによるスキャン → ホワイトハッカーによる擬似攻撃 → エビデンス取得リスク評価

緊急度が高い脆弱性は速報で通知

- 商用/自社開発ツールを用いて、システム全体の脆弱性・問題部位を洗い出します。
- 数年以上の経験を持ったエンジニアが、業界標準および当社独自の手法を用いて擬似攻撃を行います。
- 専門部門が、対象システムの特性に応じたリスクを評価いたします。

**STEP 3**　報告書作成～報告会 → リスク評価 → POINT トレンドにもとづく脅威評価 → 報告会

- レビュー専門部門が、対象システムの利用範囲や環境を考慮し、リスクの評価を行います。
- 昨今のセキュリティ事象や傾向を加味したリスク分析結果にもとづき、脅威を評価します。
- 診断・解析を担当したエンジニアが報告を行い、質疑応答にも対応いたします。

**STEP 4**　診断保守 → POINT 結果報告後の対応 → 再診断

- 報告書提出後3ヶ月間は指摘内容・対策についての質問をお受けいたします。
- ご報告後1ヶ月以内を目途に、修正いただいた箇所の再診断を実施いたします。

## サービス特長

- ツール診断と手動診断を組み合わせ、**複数の手法で精度の高い診断**結果を導き出します
- 診断結果を技術員が分かりやすく解説するほか、**3ヶ月間のお問い合わせに対応**します
- **再診断まで標準提供**しておりますので、脆弱性発見後の対処結果も再確認が可能です

## 診断内容について

**診断項目の網羅性**　手動診断は、ツール診断より多くの問題箇所の特定が可能です。

ネットワーク脆弱性診断

| | |
|---|---|
| ホストスキャン | TCP、UDP、ICMP でのポートスキャン、実行中のサービスの検出 |
| 脆弱性 | ネットワークサービス、Webサーバー、各種OS、ネットワーク機器 等の調査 |

Webアプリケーション脆弱性診断

| | |
|---|---|
| 認証 | ログインフォームに関する調査、ログイン情報の送受信に関する調査 |
| セッション管理 | Cookieの取り扱いに関する調査、セッションIDに関する調査、クロスサイトリクエストフォージェリ |
| 入出力処理 | クロスサイトスクリプティング、SQLインジェクション、コマンドインジェクション、ディレクトリトラバーサル、ファイルアップロード、パラメータ推測 |
| 一般的な脆弱性 | 既知のソフトウェア脆弱性、強制ブラウジング、ディレクトリリスティング |
| Webサーバー設定 | システム情報の開示、サーバーエラーメッセージ　など |

## 診断提供条件について

| | |
|---|---|
| 診断対象 | サーバー、ネットワーク機器に対する脆弱性診断・Webアプリケーションに対する脆弱性診断 |
| 診断内容 | 外部脆弱性診断 |
| 診断調査時間 | 平日日中時間帯（基本10:00-18:00）※1 |
| 診断方法 | ツールによるスキャンの実施・手作業による検査、分析 |
| 成果物・報告会 | 診断報告書（電子データにて提出）※2 |
| 速報通知 | 緊急度の高い脆弱性が発見された場合、翌日までにサマリーをメールにて提出 |
| サポート | 報告書提出後、3ヶ月間メール・電話にて問い合わせ可能・ご報告後1ヶ月以内を目途に再診断を実施※3 |

※1 平日夜間帯、休日での診断対応の場合は別途有償対応となります。　※2 別途有償にて、英語での報告書提出も可能です。　※3 再診断実施後は、簡易報告書を電子メールにて提出いたします。

## 脆弱性の評価基準について

**危険度による対処優先順位付け**

◎CVSS、OWASP Top10等、国際的な脆弱性評価基準をもとに、独自の基準を適用し脆弱性のランク付けを行っております。
◎危険度5（緊急）～1（低危険度）までの脆弱性項目に対して詳細に解説をいたします。

詳細解説対象項目

| | | |
|---|---|---|
| 5 | 緊　急 | 容易に悪用可能であり、インターネットワームや、自動攻撃ツールによる無差別攻撃によっても損害が発生する可能性があるもの等、特に迅速な対応が必要なもの。 |
| 4 | 重　大 | 緊急レベルの脆弱性に匹敵する損害が予想されますが、緊急レベルと比較して悪用が難しいもの。<br>クロスサイトスクリプティング、SQLインジェクションなどが該当。 |
| 3 | 高危険度 | システムの停止や、ユーザー情報の間接的な悪用等、悪用された場合の損害もしくは悪用手法が限定的なもの。 |
| 2 | 中危険度 | 直接損害が発生する可能性は高くないが、内部関係者向け情報から、システムの弱点が露呈する可能性があるもの。 |
| 1 | 低危険度 | システムの一般的な情報や、サービスの運用状況等、システムに対する攻撃者の興味を引く可能性があるもの。 |
| 0 | 情　報 | 品質やセキュリティのさらなる向上のため、当社が推奨する項目など。 |

CVSS（共通脆弱性評価システム）…ソフトウェアや情報システムに存在する保安上の弱点や不具合の深刻度を評価する手法の一つ。
OWASP Top10…最も重大なウェブアプリケーションセキュリティリスクのトップ10

## サービス料金

診断対象規模や範囲によって異なりますので、個別にお問い合わせください。

## セキュリティ対策は継続的な取り組みが重要です。

◎セキュリティ対策は常に見直しを行い、安全な業務遂行環境を継続して保持する必要があります。

| | 重点点検項目 | 確認頻度 |
|---|---|---|
| 1 | 利用製品のバージョンが最新であることの確認 | 数週間～1ヶ月に1回程度 |
| 2 | Webサーバー上のファイルの確認 | 1週間に1回程度 |
| 3 | Webアプリケーションのセキュリティ診断 | **1年に1回程度、機能追加などの変更時** |
| 4 | ログインID／パスワードの確認 | 1年に1回程度 |

※出典:一般財団法人JPCERTコーディネーションセンター「注意喚起「サイバー攻撃に備えてWebサイトの定期的な点検を」」


検査にブランクがあることによるリスクは想定以上！

STNetは、お客さまの継続的なセキュリティの改善をご支援いたします