脆弱性診断サービス紹介

EGセキュアソリューションズ株式会社

そのウェブサイト、“事業リスク“ かもしれません！

ウェブサイトに脆弱性があると、なぜダメなのか？

理由１：経済的損失の懸念
理由２：個人情報保護法等による法的な要求
理由３：攻撃の加害者となる可能性がある

脆弱性診断により、脆弱性を発見・修正することで
ウェブサイトの安全性を高め、上記リスクを回避する。

事業継続のためのリスク管理として「脆弱性診断」が重要

もくじ

脆弱性診断とは

脆弱性診断とはセキュリティ上の問題となりうるバグ（脆弱性）を発見するサービスの総称のことです。大きく分けて、以下の３種類があります。

1 ウェブアプリケーション脆弱性診断

各サイト固有の機能を構築するためにプログラミングされた箇所に潜む問題を検出する

2 プラットフォーム脆弱性診断

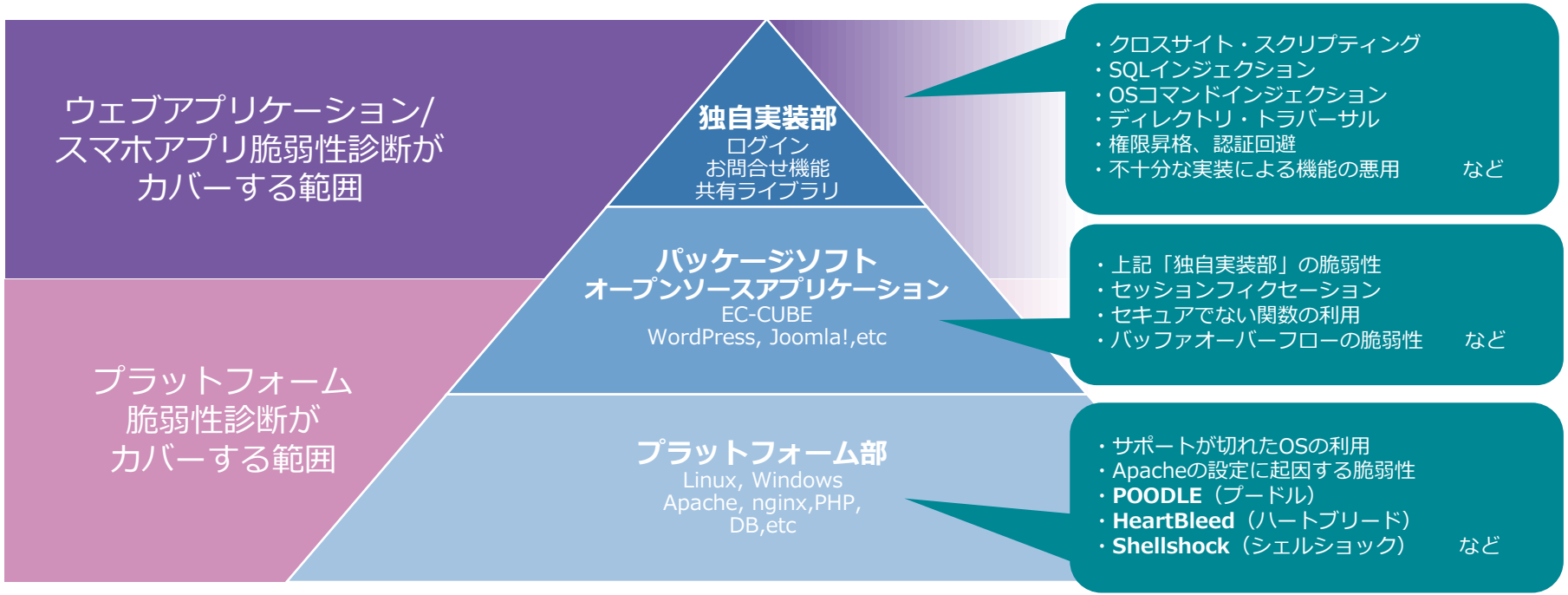
OS（オペレーティングシステム）やミドルウェアなど世界共通で利用されているソフトウェアに潜む問題を検出する

3 スマートフォンアプリケーション脆弱性診断

スマートフォンアプリケーションおよび連携しているサーバとのAPI通信に潜む問題を検出する

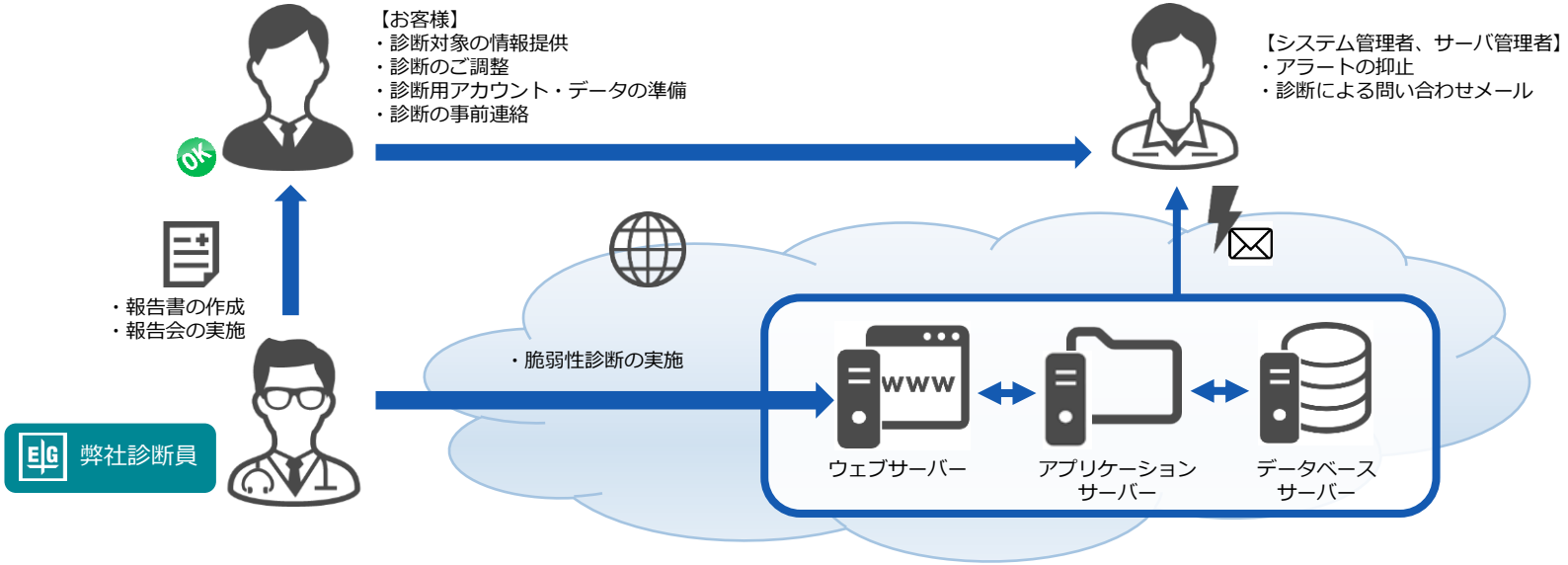
脆弱性診断の種類とカバー範囲

複数の脆弱性診断が存在しますが、各診断によりカバーできる範囲は下記のとおりです。



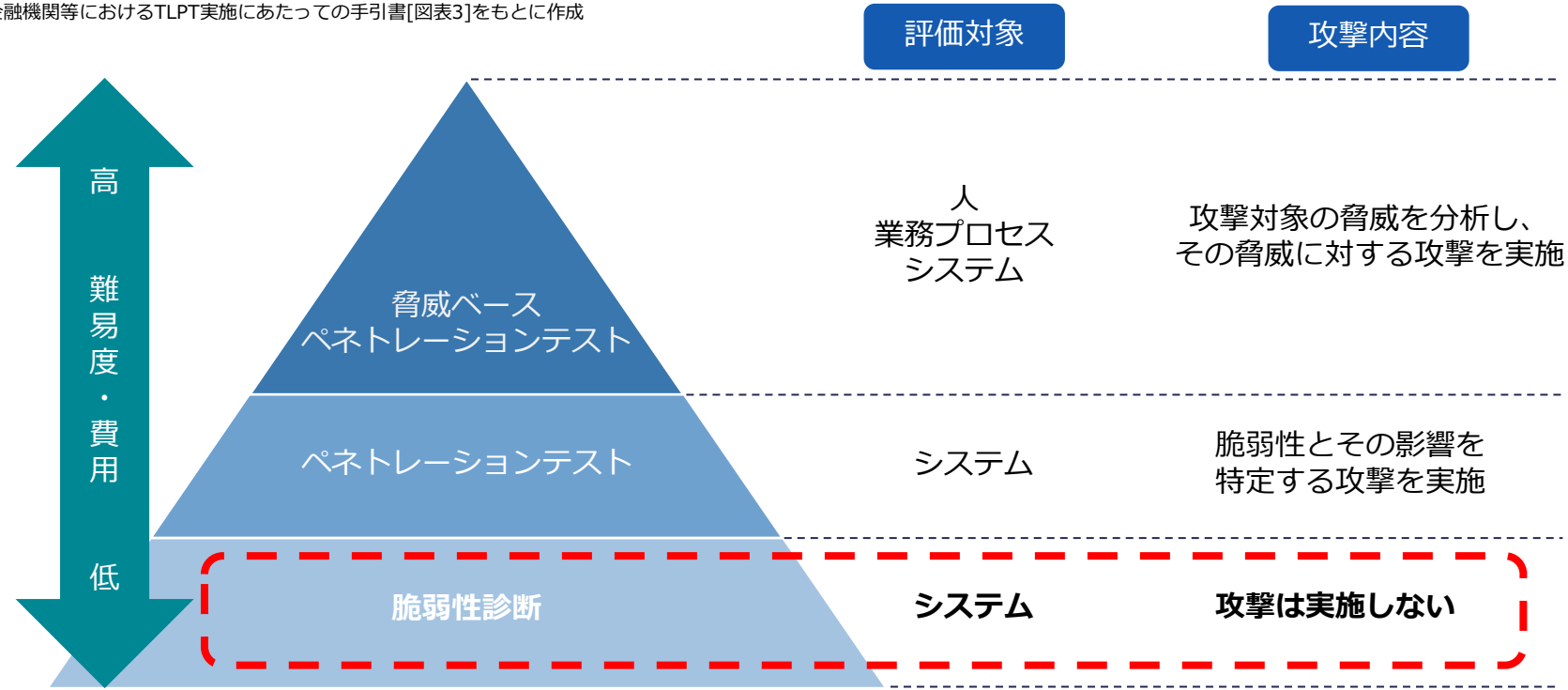
脆弱性診断の実施イメージ

発見された脆弱性は対策方法と共に「報告書」でお客様に報告されます。
脆弱性診断を安全に実施するためには診断前の準備が重要です。



脆弱性診断とペネトレーションテストの違い

金融機関等におけるTLPT実施にあたっての手引書[図表3]をもとに作成



弊社脆弱性診断サービスの実施内容

EGSSの脆弱性診断（アプリ診断）では以下のレベル3までの対応を実施しております。
レベル４～をご希望の際にはペネトレーションテスト、脅威ベースペネトレーションテストをご提案させていただきます。

脆弱性診断サービスのご紹介

ウェブアプリケーション脆弱性診断

ウェブアプリケーション脆弱性診断とは、攻撃者の視点で
疑似攻撃を試行することでアプリケーションに潜む脆弱性を検出する診断です。

診断の対象	ウェブアプリケーション（独自実装部分、パッケージソフトウェア、API等）
確認内容	入力フォーム等動的ページを中心に様々な疑似攻撃を、セキュリティや侵入テストに使用されているツールである「Burp Suite」を用いて実施し、脆弱性や仕様不備を洗い出します

専門のエンジニアが、対象のウェブアプリケーションの特性や取り扱う情報等を考慮したうえで診断を実施します。SQLインジェクションやクロスサイトスクリプティングなどの脆弱性はもちろん、認可制御の不備や認証強度など、仕様上の不備や改善点についても確認いたします。『OWASP TOP10』『安全なウェブサイトの作り方』に準拠する『情報セキュリティサービス基準』適合サービスです。
目的や予算に応じたプラン内容の調整や大量サイトの定期診断などもご相談ください。

留意事項(抜粋)

脆弱性診断作業における留意事項の一部です。
詳しくはサービス約款をご確認ください。

✔診断日程について
ヒアリングシートに記載いただくご指定の日時は希望であり、記載日に診断を実施することを確約するものではありません。別途、当社と貴社担当者様との協議のうえ正式な診断日時を取り決めさせていただきます。
当社よりご提示した診断日程は問題が起きないことを想定して設定された日程です。
システムに障害が発生した場合、診断実施に必要な情報が不足している場合、診断対象への疎通ができない場合、リクエストへの応答に時間がかかる場合など、診断が困難な状況下では、診断実施期間が予定した日程を超える可能性があることを予めご了承ください。

✔診断速度について
診断時には 1 秒間に最大 30 リクエストが送信される可能性がございます。診断環境への負荷が懸念される場合は事前にご連絡ください。

✔診断データの準備について
診断前の診断環境のデータ登録、アカウントの準備、また診断後のアカウントの削除、診断中に発生した不要データの削除は貴社にて実施してください。

✔診断による影響について
・脆弱性診断を実施するにあたり、データの変更および削除や大量のメール送信や実際の発注処理の実行など、システムの動作に影響を与える可能性があることがございます。予めご承知おきください。
・診断実施により意図しない障害が発生するおそれがあるため、可能な限り利用者に影響を与えない独立した診断環境を準備願います。また、データをバックアップするなど、事前にデータを保全いただけますようお願いします。

ウェブアプリケーション脆弱性診断　プラン一覧

ウェブアプリケーション脆弱性診断のプランは以下の通りとなります。

プラン概要	Webアプリケーション診断	
	スタンダード	プレミアム
プラン概要	「安全なウェブサイトの作り方」「OWASP TOP10」の項目に沿った網羅的で高精度な診断です。 事前にヒアリングやサイト調査を行うことで、よりサイトにあった診断を実施します。	スタンダードプランの内容に加え、診断対象の洗い出しや選定支援、再診断など脆弱性診断実施前後まで手厚くサポートさせていただきます。 また、スタンダードプランでは対応していないWebSocketやGraphQL、gRPCを利用した通信の診断にも対応しております。 ドキュメントレビューなど、より踏み込んだ形での監査も可能となります。 (別途費用が発生いたします。)
診断方法	ツール+手動	ツール+手動
速報対応	あり(*)	
報告書	通常	
再診断	3か月以内に1度まで無料	
再々診断	個別見積	

(*)緊急度の高い脆弱性が検出された場合、検出から2営業日以内にご報告いたします。

ウェブアプリケーション脆弱性診断　診断項目（1）

カテゴリ	診断項目	対応状況
パラメータ操作	クロスサイト・スクリプティング（XSS）	◎
	SQLインジェクション	◎
	HTTPヘッダ・インジェクション	◎
	メールヘッダ・インジェクション	◎
	OSコマンド・インジェクション	◎
	ディレクトリ・トラバーサル	◎
	evalインジェクション	△
	ファイルインクルード攻撃	◎
	オープンリダイレクタ	◎
	リファラからの情報漏洩	◎
	XML外部実体参照（XXE）攻撃	◎
	安全でないデシリアライゼーション	○

◎：標準的で網羅的な検査、○：簡易的な検査、△：検査不可の場合有

ウェブアプリケーション脆弱性診断　診断項目（2）

カテゴリ	診断項目	対応状況
コンテンツ	公開ディレクトリチェック	◎
	ディレクトリ・リスティング	◎
	強制ブラウジング・不要なファイルの公開	◎
	キャッシュ制御	◎
ファイルアップロード・ダウンロード	アップロード機能の不備	◎
	ダウンロード機能によるXSS	◎
ユーザの意思に反した機能実行	クロスサイト・リクエストフォージェリ（CSRF）	◎
	クリックジャッキング	◎
通信暗号化	SSL設定不備	◎
	SSL使用状況	◎
	クッキーのセキュア属性不備	◎
セッション管理	セッションID使用状況	◎
	Cookie使用状況	◎
	ログアウト機能	◎
	セッションIDの固定化	◎

◎：標準的で網羅的な検査、○：簡易的な検査、△：検査不可の場合有

ウェブアプリケーション脆弱性診断　診断項目（3）

カテゴリ	診断項目	対応状況
認証	ユーザ認証処理	◎
	アカウントロック機能	◎
	自動ログインの不備	◎
アクセス制御・認可	アクセス制御不備	◎
	認可不備	◎
アカウント管理	パスワードの仕様	◎
	パスワードリマインダの不備	◎
アプリケーション	エラー処理状況	◎
	ロジック流出	○
	バックドア、デバッグオプションの存在	△
仕様の不備	セキュアな実装についての指摘	○

◎：標準的で網羅的な検査、○：簡易的な検査、△：検査不可の場合有

プラットフォーム脆弱性診断

プラットフォーム脆弱性診断とは、ネットワーク機器上で動作する基盤ソフトウェアの脆弱性や設定不備を検出する診断です。

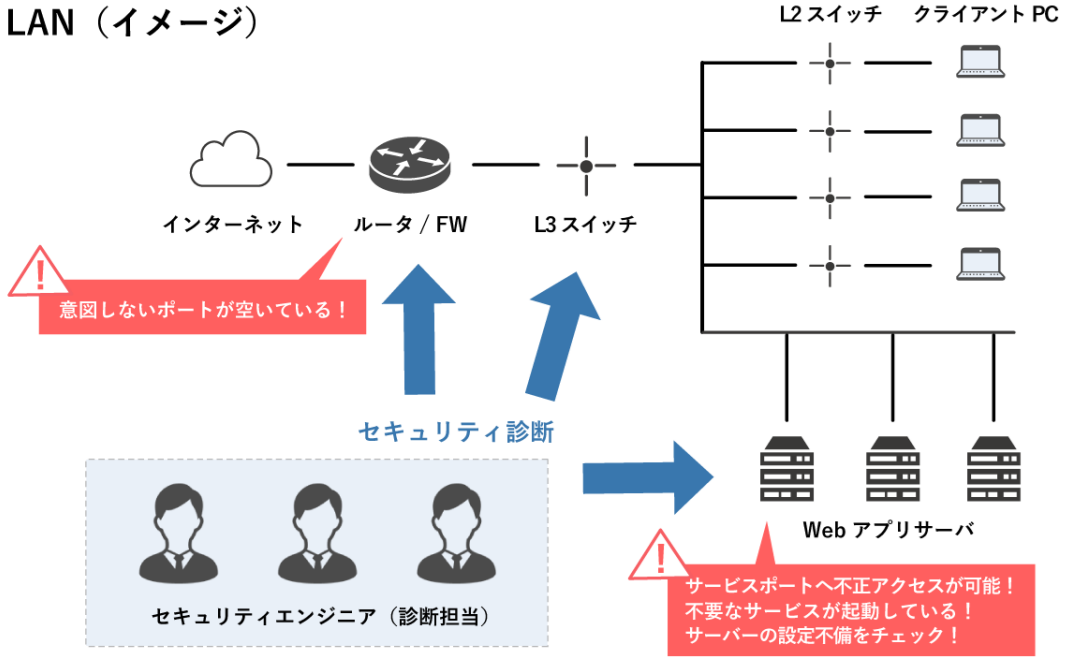
診断の対象	IPアドレスが割り振られた機器全て
確認内容	機器上で動作している基盤ソフトウェアを調査し、それらに脆弱性や設定不備が無いか確認

- ツール（Nessus、Nmap）によるポートスキャン/サービススキャンの実施
- 検出したサービス（常駐プログラム）に対する情報取得および挙動確認
  例）不要なサービスを公開していないか
  例）公開しているサービスで不要な設定まで有効化されていないか

インターネットを経由する外部からの診断の他、内部ネットワークのオンサイト診断もご相談ください。

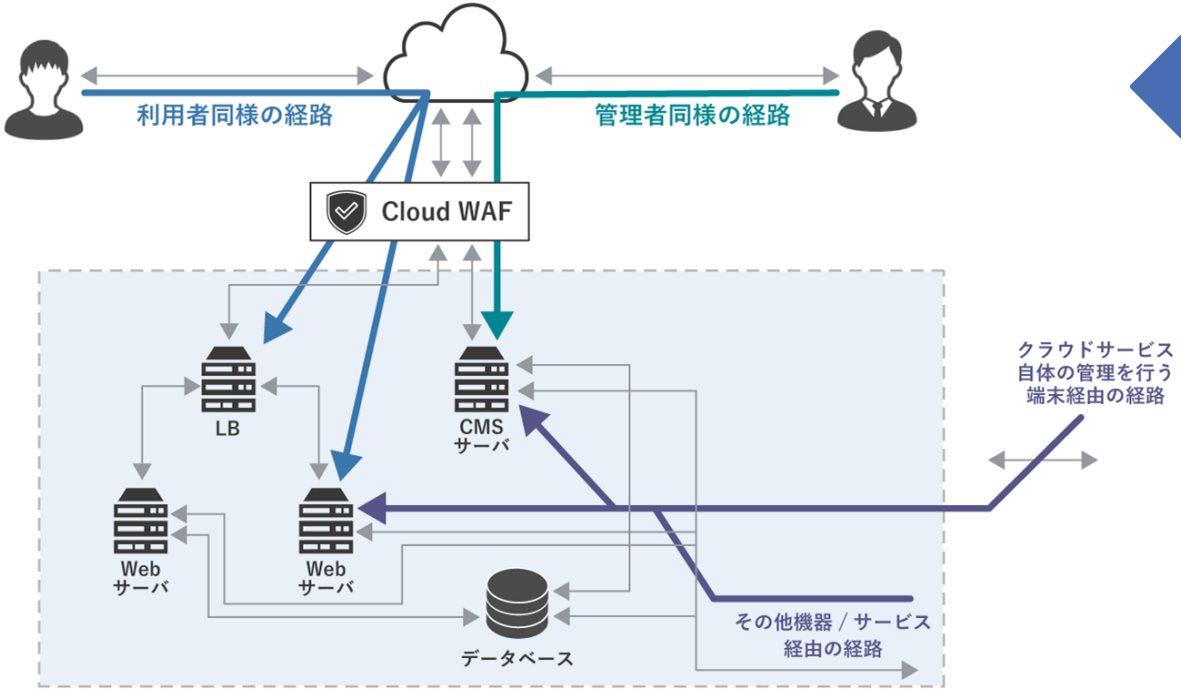
プラットフォーム脆弱性診断

各種ネットワーク機器およびサーバへのネットワーク経由での攻撃に対する脆弱性検査を実施します。



参考：診断対象機器や経路について

診断対象や経路のパターンは多々ございますが、「利用者同様の経路」からの診断が主になります。



クラウド上に構築した
Webアプリケーションの例

診断対象候補機器：
ロードバランサー、Webサーバー、
CMS管理用サーバー
など

診断対象経路：
利用者同様の経路
（WAFあり/なし、LB経由/直接アクセス）
管理者同様の経路
（管理者PC経由/内部機器経由/内部犯）
など

※記載の攻撃経路は一例です

プラットフォーム診断項目の例と、診断により洗い出される脆弱性の例

項目	概要
ポートスキャン	TCP(1～65535)/UDPポート(任意ポート)に対してスキャンを実施
オープンポート(提供サービス)に対するバナー情報取得	診断ツールがバナー情報を収集
	マニュアルによりオープンポートに接続してバナー情報を収集(プレミアムのみ)
オープンポート(提供サービス)に対するポート挙動チェック	診断ツールがオープンポートのサービスを特定し、 セキュリティ上の問題となる動作がされていないかを確認
	マニュアルによりオープンポートに接続してサービスを特定し、 セキュリティ上の問題となる動作がされていないかを確認
自動化ツールによるセキュリティ診断	各種サーバーに対し、1万以上の項目の既知の脆弱性を診断
各種サーバーFTP、SSH、SMTP、POP、DNS、TELNET、SMB、NTP、SNMP	各種サーバーの設定不備調査 SPAMメールの送信に利用される恐れのある、 第三者によるメールの不正中継が可能かどうかを診断
HTTPサービス診断ツールによるセキュリティ診断	既知のセキュリティホールを持ったサンプルファイル(サンプルCGI等)のチェックおよび設定内容等を診断、暗号強度・証明書・SSL/TLSバージョンの調査

スマートフォンアプリケーション脆弱性診断

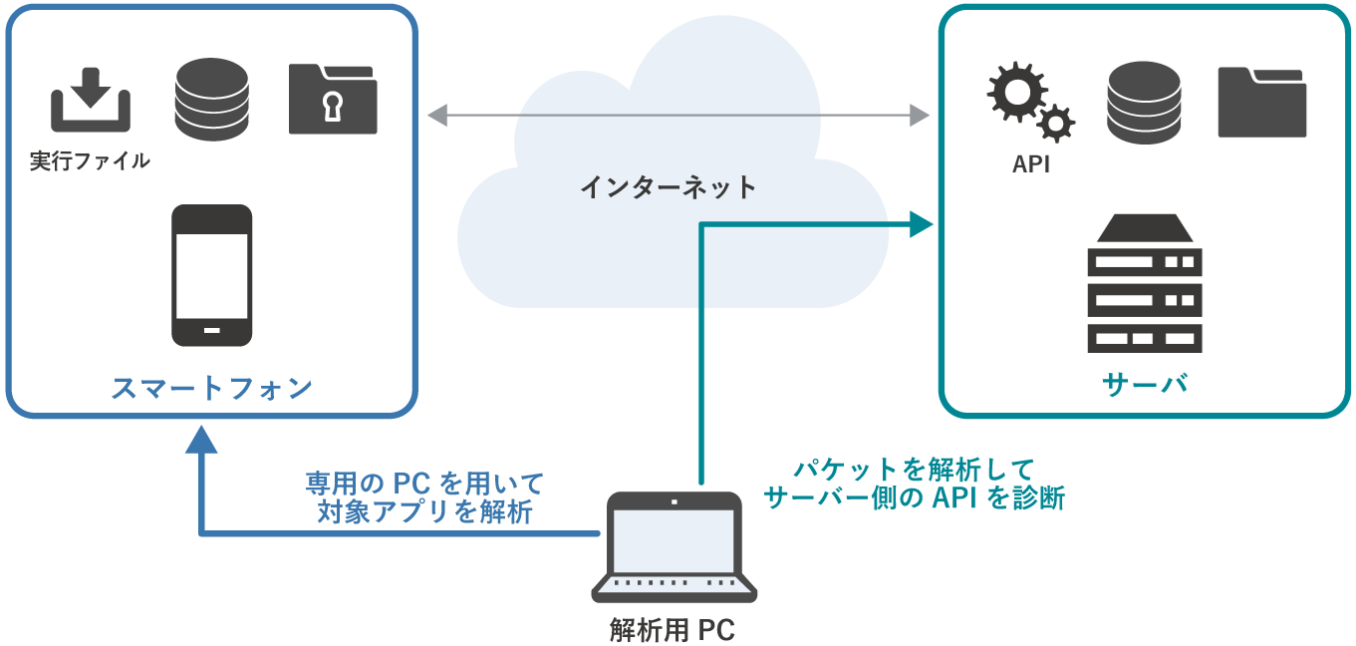
**スマホアプリ脆弱性診断では、通信における脆弱性の診断と
スマホアプリそのものに不正行為ができる脆弱性がないか解析します。**

診断の対象	サーバへの通信（API）脆弱性診断
確認内容	スマートフォンアプリの静的解析、動的解析

- APIの診断
  スマートフォンからサーバにアクセスしてサーバのAPIを診断（診断項目はウェブアプリと同様）
- スマホアプリ静的解析
  開発経験のあるエンジニアが目視でソースコードを診断
- スマホアプリ動的解析
  専用のPCで実行プログラムを動作し、不正な動作を調査
  デバッガーを用いてプロセスアタッチを行い、アプリケーションのリソースを解析
  逆アセンブルを行いソースコードを解析

スマートフォンアプリケーション脆弱性診断

専用の解析用PCを用いて、スマートフォンアプリケーション並びに連携しているサーバーのAPIに対して
インターネット経由で脆弱性診断を実施します。



スマートフォンアプリケーション脆弱性診断　診断項目（1）

カテゴリ	診断項目	iOS	Android
データ保護	アカウント情報の保護	○	○
	アプリケーションログ	△	○
	キーボードキャッシュの無効化	○	○
	クリップボードの許可状況	○	○
	パスワードやPINの画面表示	○	○
	OSバックアップファイルへの機密データ出力	△	ー
	共有ファイルの利用状況	○	○
	キャッシュファイルの利用状況	○	○
	最低限のパーミッション設定	○	○
	機密データ利用目的への説明	○	○
	機密データのメモリロードと破棄状況	△	○
暗号化	暗号化キーのハードコーディング	△	○
	脆弱な暗号化方式の採用	△	○
	脆弱な暗号化アルゴリズムの利用	△	△
	暗号化キーの使いまわし	△	△
	乱数ジェネレーターの強度	△	△

○：動的解析で診断できる項目
△：静的解析で診断すると精度よく検出できる項目（動的診断でも可）
ー：機能がないため診断対象外の項目

スマートフォンアプリケーション脆弱性診断　診断項目（2）

カテゴリ	診断項目	iOS	Android
認証とセッション管理	認証処理の不備	△	△
	セッションIDの生成方法	○	○
	ログアウト	○	○
	パスワードポリシー	○	○
	不適切なバイオメトリクス認証の実装	△	ー
	ログイン通知機能の不備	○	○
ネットワーク通信	TLSの利用	△	△
	SSL証明書の検証不備	△	△
	証明書ストアの利用方法	△	○
プラットフォームAPI	不要なAPIの使用	※1	○
	データ入力値へのチェック処理	○	○
	カスタムスキームの利用状況	○	○
	危険なスキームの利用	○	○
	WebViewのJavascriptアクセス	ー	○
	危険なIMEIやUUIDの利用方法	△	△
	危険なシリアル化APIの使用	△	△

○：動的解析で診断できる項目
△：静的解析で診断すると精度よく検出できる項目（動的診断でも可）
ー：機能がないため診断対象外の項目

スマートフォンアプリケーション脆弱性診断　診断項目（3）

カテゴリ	診断項目	iOS	Android
プログラムコードとビルド設定	不適切なプロビジョニング	○	ー
	デバッグモードの有効化	△	△
	デバッグシンボルの削除状況	△	○
	利用コンポーネントの既知の脆弱性	△	△
	エラーハンドリング状況	○	○
	セキュリティコントロールのエラー設定状況	○	ー
	メモリリークやメモリ保護の状況	△	△
	スタック保護やPIEサポートの設定状況	△	△
リバースエンジニアリング	不適切なRootチェック	○	○
	不適切なエミュレータチェック	○	○
	機密データのメモリへの直接ロード	△	△
	データ改ざん検知機能の有無	○	○
	リバースエンジニアリングツールの検知	○	○
	デバッグプロトコルの許可状況	△	△
	プログラムコードの難読化	○	○
サーバーAPI	※ Webアプリケーション脆弱性診断の診断項目を参照のこと	ー	ー

○：動的解析で診断できる項目
△：静的解析で診断すると精度よく検出できる項目（動的診断でも可）
ー：機能がないため診断対象外の項目

弊社の脆弱性診断が選ばれる理由

具体的な検証例と対策方法の提示

EGセキュアソリューションズの脆弱性診断はウェブアプリケーション開発にも精通した熟練技術者による診断が中心です。そのため、単なる脆弱性の指摘や一般的な対策方法にとどまらず、脆弱性の検証例のご提示や診断対象サイトの特性に合わせた対策方法のご提案ができるのです。

高いお客様満足度

EGセキュアソリューションズの脆弱性診断における最大の価値は、報告書と報告会にあります。
報告書の読み上げや脆弱性の説明にとどまらない、セキュリティコンサルティングの知見や最新のセキュリティトレンドを踏まえた一歩踏み込んだ解説が、お客様からご好評いただいています。

ウェブセキュリティの第一人者・徳丸浩監修

『体系的に学ぶ　安全なWebアプリケーションの作り方』（ソフトバンククリエイティブ）の著者であり、セキュリティ関連資格試験の監修や様々なメディアでの解説も豊富な徳丸浩による長年の経験と最新の調査・分析に裏打ちされたノウハウにより生まれた脆弱性診断サービスです。

脆弱性診断への弊社のこだわり

主軸はセキュリティエンジニアの手動による診断

弊社の脆弱性診断サービスはツール診断が補助という位置付けで実施しています。
その理由は、手動診断はツールでの自動診断に比べてきめ細かい診断ができるためです。

週に一度の社内勉強会でメンバー全員と情報を共有する

手動診断はエンジニアのスキルに依存する診断方法であるため、個人のスキルによって品質に差が出やすい方法でもあります。このような問題に対処すべく、弊社では品質管理責任者である徳丸をはじめ、常に最新の脆弱性情報を収集しながら検証を繰り返しています。また、その結果を全員で共有することで脆弱性診断の診断項目や手法に反映しています。このような取り組みは、エンジニア全員のスキルアップによるサービス品質向上に繋がります。また、この取り組みを継続することで日々繰り返される最新の攻撃方法に対抗することができるのです。

サイトオーナー様からのヒアリング結果をナレッジとして蓄積

ウェブサイトの機能は多岐にわたるため、エンジニア視点の手法だけではカバーできないケースもあります。そのため、サイトオーナー様から運用状況や懸念点等をヒアリングし、その結果を社内のナレッジとして蓄積しながら診断項目に加えています。

このような取り組みを通して品質を維持しながら
お客様にとって最適な診断サービスとなることを常に目指しています。

脆弱性診断導入の流れ

脆弱性診断導入の流れ

①ヒアリングシートご提出/御見積・スケジュール調整

診断対象サイトに関する情報をヒアリングシートにご記入いただきます。
ヒアリングシートを基に、御見積書・スケジュール(仮)をご提示します。

目安期限：
診断開始1～2か月前

↓

②ご発注/スケジュール確定

正式にご発注いただくことで、初回の診断スケジュールを確定いたします。

目安期限：
診断開始3～4週間前

↓

③診断準備/アクセス確認

診断に必要なアカウントのご準備等実施いただきます。
アカウントいただき次第、アクセス確認を行います。

目安期限：
～診断開始1週間前

↓

④診断実施/報告書納品

決定したスケジュールで診断を実施し、報告書を納品します。
オプションとして報告会の開催を行います。

診断期間：
対象リクエスト数による

↓

⑤アフターフォロー

再診断の実施及び報告書の内容に関するお問い合わせをお受けします。

アフターフォロー期間：
報告書納品から3か月

お見積に必要な情報

概算のお見積にはご希望のプランと対象サイトのページ数、API数、IPアドレス数などをご提示ください。
ご希望の予算や納期もお伝えください。
別途弊社にてご用意するヒアリングシートにご記入をお願いいたします。

目的に合わせたプラン、対象範囲のご提案や精緻なお見積りを希望される場合には、
弊社にて診断対象サイトを調査いたしますので以下をご準備ください。

1．設計書などの当該サイトの構成が分かる資料

2．対象としたいWebページのURL情報

3．テストアカウント情報（会員制サイトの場合）

4．注意してほしい操作などの有無

会社概要

名　称	EGセキュアソリューションズ株式会社
所在地	〒105-0001　東京都港区虎ノ門1-2-8　虎ノ門琴平タワー 8F
設　立	2008年4月2日
代　表	齊藤 和男
株　主	イー･ガーディアン株式会社 (東証プライム/証券コード：6050)　100%
事業内容	1．情報セキュリティ、情報システムに関する監査、コンサルティング 2．情報セキュリティに関する調査、研究、執筆、教育 3．情報セキュリティ関連の教育及びコンテンツ制作

IS575950 / ISO27001:2013

情報セキュリティサービス基準適合（脆弱性診断サービス）
2020年9月23日登録
https://sss-erc.org/iss_books/020-0012-20/

020-0012-20

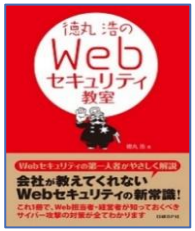
取締役CTO　徳丸 浩（とくまる ひろし）について

略　歴

1985年京セラ株式会社に入社後、ソフトウェアの開発、企画に従事。1999年に携帯電話向け認証課金基盤の方式設計を担当したことをきっかけにWebアプリケーションのセキュリティに興味を持つ。2004年同分野を事業化。
2008年独立、Webアプリケーションセキュリティを専門分野とするHASHコンサルティング株式会社（現EGセキュアソリューションズ株式会社）を設立。
2015年イー・ガーディアングループに参画。2019年よりイー・ガーディアン子会社のグレスアベイル株式会社取締役、2020年より同子会社株式会社ジェイピー・セキュア取締役を兼任。2021年より取締役CTO就任。

独立行政法人情報処理推進機構（IPA）非常勤研究員
(株)パイプドビッツ社外技術顧問　他多数

著　書



実　績　等

相次ぎ発生する預貯金の不正引き出しについて、テレビ東京ワールドビジネスサテライト等メディアでの解説や東洋経済、産経新聞他、Itmedia等IT系メディアの取材実績多数。
その他、セキュリティイベントでの基調講演やゲスト講演も多数。

著書『体系的に学ぶ 安全なWebアプリケーションの作り方　第2版』を教材、出題範囲とする民間試験「ウェブ・セキュリティ基礎試験」（徳丸基礎試験）が2019年より開始。

本サービスに関するお問合せ・お見積のご依頼