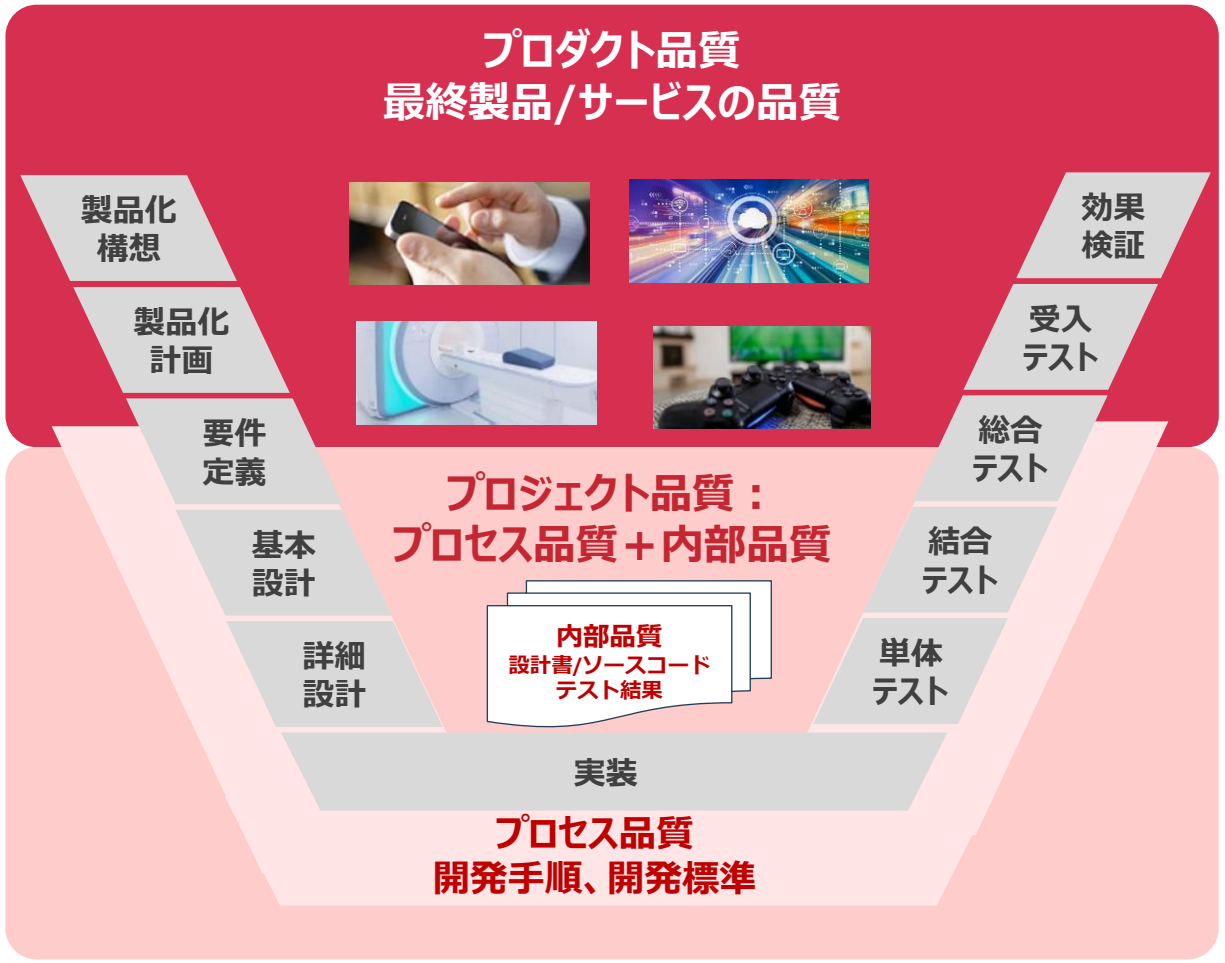
セキュリティー対策サービス
ご紹介資料

株式会社ヴェス
https://www.ves.co.jp

VESのソフトウェア品質支援ソリューション

弊社は、お客様が市場に展開する各種製品やサービスのソフトウェア品質課題を解決する、品質のプロフェッショナルです。
最終製品やサービスの魅力品質に寄与する「プロダクト品質支援サービス」および、ソフトウェア開発プロジェクトを成功に導く「プロジェクト品質支援サービス」にて、お客様ビジネスを成功に導きます。

弊社の考える品質種別



品質種別に対するソリューション例

プロダクト品質支援

ソフトウェア第三者検証

セキュリティ品質

- Webアプリケーション脆弱性診断
- ネットワーク脆弱性診断
- ソースコード診断
- スマホアプリ診断
- IoT脆弱性診断
- クラウドセキュリティ設定診断
- ペネトレーションテスト

プロダクト品質支援サービスは、お客様の製品/サービスが、ソフトウェアの領域において「必要な機能を満たしているか」はもちろんのこと、魅力的で安心安全なソフトウェア品質となっているか、非機能面においても診断/評価支援を実施いたします。

プロジェクト品質支援

ソフトウェア第三者検証

テスト自動化

品質コンサルティング

品質教育

プロジェクト品質支援サービスは、ソフトウェア開発フェーズにおける、内部品質（設計書やソースコードなど）およびプロセス品質（開発手順や開発標準）向上を支援する各種サービスにより、お客様の開発プロジェクトを成功に導く御支援をさせていただきます。

セキュリティ診断サービス一覧

サービスラインナップ

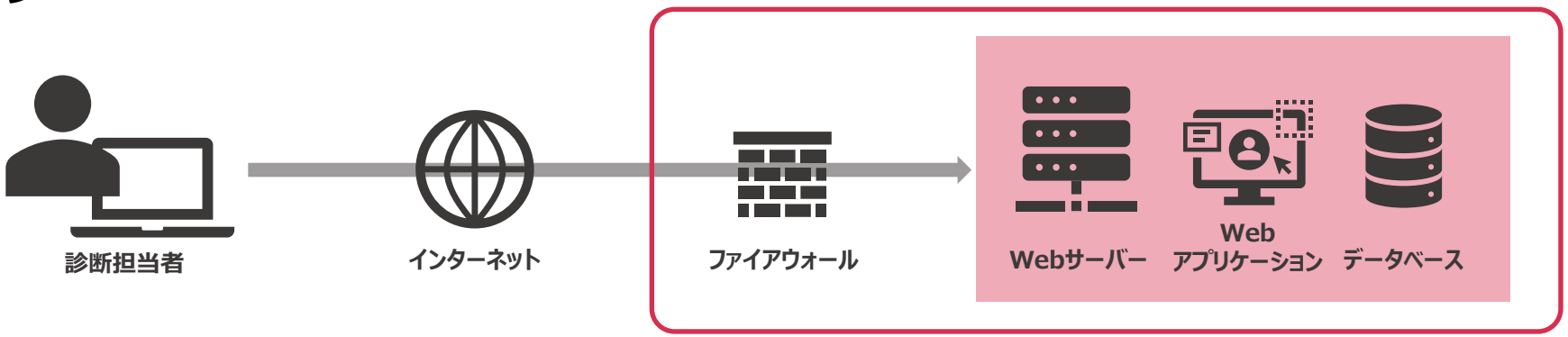
サービス名	サービス概要	目的／効果
Webアプリケーション脆弱性診断	ハッカーの手法を用いて、不正アクセスに対してWebサイトが防御すべき点を検出します	Webアプリケーションに潜む脆弱性の検出
ネットワーク脆弱性診断	ネットワーク、サーバ、OSのほか、ファイアウォールやIPS/IDSといったセキュリティ機器も対象に診断を行います	ネットワーク機器やOS、ミドルウェア等の脆弱性の検出
ソースコード診断	アプリケーションに潜在するセキュリティ上および品質上の問題をソースコードレベルで検査します	開発の上流工程で対策して手戻り対応工数を削減
スマホアプリ診断	特有のリスクを抱えるスマホアプリ自体の脆弱性洗い出しのほか、サーバとの通信を診断するメニューもあります	リリース前スマホアプリの安全性を確認
ペネトレーションテスト	具体的かつ多様なシナリオを用いた疑似攻撃を行い、リスク評価・脅威評価や報告をします	現状のセキュリティ対策の有効性を確認
AI／LLM診断	AIシステムのセキュリティ上のリスクを洗い出します。プロンプトの悪用やユースケースごとのリスクシナリオを洗い出し検証を行います	AIシステムのシステムに潜むリスクを洗い出し、安全・安心な運用を実現するための具体的な対策確認。
IoT脆弱性診断	対象デバイス固有の機能を利用して、攻撃者が攻撃に有益な不正操作、情報窃取、踏み台化が行えるか検査します	様々な種類の製品があるIoT機器に存在する脆弱性の検出
クラウドセキュリティ設定診断	AWS、Microsoft Azure、Google Cloud Platform、Oracle Cloud固有のベンチマーク指標および弊社独自観点で設定内容を確認します	クラウド設定不備によるセキュリティ事故の予防

Webアプリケーション診断サービス

Webアプリケーション脆弱性診断概要

- ✓ 攻撃者の視点からWebアプリケーションに存在する情報漏洩やデータ改ざん、なりすましの原因となる脆弱性を検出します。
- ✓ 診断結果として検出した脆弱性に関する対策の優先度や対策方法をご提示いたします。

サービスイメージ



サービスの流れ

診断前準備・調査			診断実施				診断実施					診断後対応	
予備調査	クローリング	診断対象の確定	脆弱性診断	複数ツールによるスキャン	ホワイトハッカーによる疑似攻撃	エビデンス取得・リスク評価	報告書作成	アナリストによる評価	報告内容レビュー	報告書納品	報告会	結果報告後の対応	再診断

Webアプリケーション脆弱性診断項目

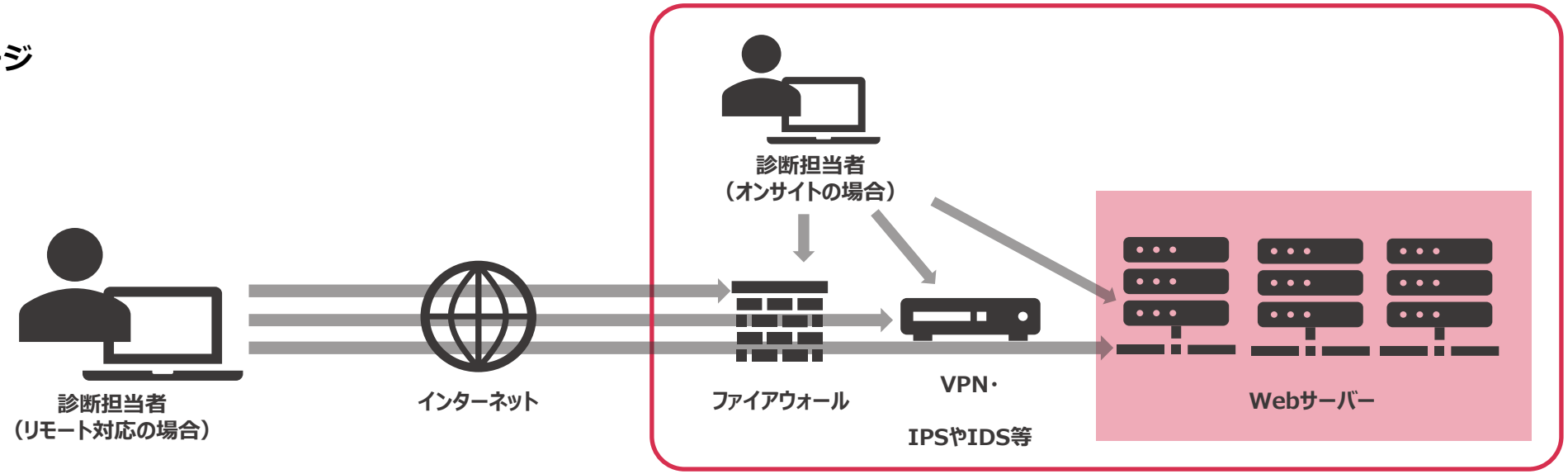
診断項目	主な例 *標準では実施しない項目		
入出力処理	• クロスサイトスクリプティング • HTMLタグインジェクション • SQLインジェクション • コマンドインジェクション	• パスマニピュレーション • ファイルアップロード機能に関する調査 • パラメータ推測 • 例外処理に関する問題	• オープンリダイレクト • CRLFインジェクション • バッファオーバーフロー* • XML外部エンティティ参照
認証	• ログインフォームに関する調査 • ログイン情報の送受信に関する調査	• 復認証回避に関する調査 • パスワードの強度に関する調査	• 認証トークンに関する調査 • 復元可能なパスワード保存
セッション管理	• Cookieに関する調査 • セッションIDに関する調査 • セッションハイジャック	• セッションフィクセーション • クロスサイトリクエストフォージェリ • セッションタイムアウト	• ユーザ権限に関する調査
重要情報の取り扱い	• ユーザ情報の管理に関する調査 • 特定個人情報の管理に関する調査	• クレジットカード情報管理に関する調査 • キャッシュ制御に関する調査	• 強制ブラウジング • GDPR関連に関する調査
システム情報・ポリシー	• システム情報の開示 • エラーメッセージの表示に関する調査	• ディレクトリリスティング • ソフトウェアの既知の脆弱性	• クリックジャッキング • デフォルト設定に関する調査

ネットワーク診断サービス

ネットワーク診断概要

- ✓ 攻撃者がサイバー攻撃の対象を探索する視点を用いて、サーバやVPN等のネットワーク機器に存在する脆弱性を診断します
- ✓ 設定上の問題やパッチ未適用による脆弱性対策にご活用ください

サービスイメージ



サービスの流れ

ネットワーク脆弱性診断項目概要

診断項目	主な例 *標準では実施しない項目		
ホストのスキャン	• TCP、UDP、ICMPでのポートスキャン	• 実行中のサービスの検出	
ネットワークサービスの脆弱性	• DNSに関する調査 • メールサーバに関する調査 • FTPに関する調査	• RPCに関する調査 • ファイル共有に関する調査 • SNMPに関する調査	• SSHサーバに関する調査 • データベースサーバに関する調査 • その他サービスに関する調査
Webサーバの脆弱性	• Webサーバの脆弱性	• Webアプリケーションサーバの脆弱性	• 許可されているHTTPメソッド
各種OSの脆弱性	• Windowsの既知の脆弱性 • Solarisの既知の脆弱性	• 各種Linuxディストリビューションの既知の脆弱性 • その他各種OSの既知の脆弱性	
悪意あるソフトウェア	• バックドアの調査	• P2Pソフトウェアの調査	
ネットワーク機器の脆弱性	• 各種ルータ機器の既知の脆弱性	• 各種ファイアウォール機器の既知の脆弱性	
その他	• その他ホスト全体の調査		

ソースコード診断サービス

ソースコード診断：概要

- ✓ 独自開発ソフトウェアのソースコードを静的解析し、セキュアなコーディングルールとデータフローをチェックし脆弱性とコーディング品質の検証結果および回避の為の改善案を提示します
- ✓ 開発段階のコードのセキュリティ/品質チェックや、すでに本番環境で稼働しているアプリケーションのセキュリティ診断にご活用ください

脆弱性診断との比較

サービス名	実施工程	診断種別	ソースコード	診断可能な脆弱性の特徴	問題箇所	現象
ソースコード診断	実装フェーズ（製造）	ホワイトボックス	要	• 内部構造を考慮して検査するため、実行が稀な箇所の脆弱性を検出可能 • 即悪用できない潜在的な脆弱性も検出可能	特定可	確認不可
脆弱性診断	テストフェーズ（試験）	ブラックボックス	不要	• 一般に知られている脆弱性 • 特定のパターンを用いた検査で応答を観察することで検出可能な脆弱性	特定不可	確認可

診断の流れ

事前調査 → 自動ツール診断 → 診断結果の確認・精査 → 診断結果分析 → 分析後の結果評価 → 分析結果評価 → 改善推進案検討 → 報告書作成

ソースコード診断：対応言語・検出例

対応言語

- JAVA
- PHP
- C/C++
- C#
- VB.NET
- ASP
- VB6
- Ruby
- Python
- Perl
- JavaScript
- VBScript
- PL/SQL
- Groovy
- Typescript
- GO
- Objective C
- Swift
- 等

検知する脆弱性の例

- SQLインジェクション
- セッション固定
- クロスサイトスクリプティング
- セッションの改ざん
- コードインジェクション
- サービス運用妨害（DoS）攻撃
- バッファオーバーフロー
- パラメータの改ざん
- 未検証の入力
- クロスサイトリクエストフォージェリ(CSRF)
- 安全ではないURLリダイレクト
- HTTPレスポンス分割
- 未検証のファイルのアップロード
- 不適切な例外処理
- 未解放のリソース
- ログの改ざん
- ハードコーディングされたパスワード
- 未使用のコード
- ログファイルによる情報の露出
- エラーメッセージによる情報の露出
- プライバシー違反
- 既知の脆弱性が存在する、または安全性の低い暗号アルゴリズムの使用　等

※ 下線はブラックボックステストでは検出できない脆弱性の例です

検出する品質項目の例

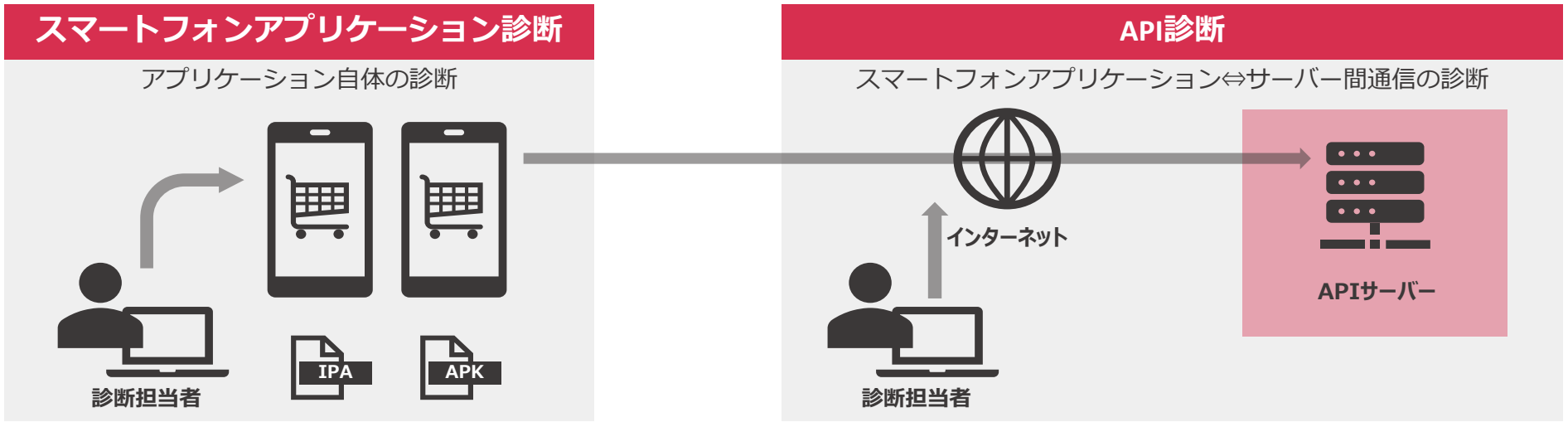
- メソッドにおける未検証の引数
- 不適切な例外処理
- デバッグコードの残存　等

スマートフォンアプリケーション診断

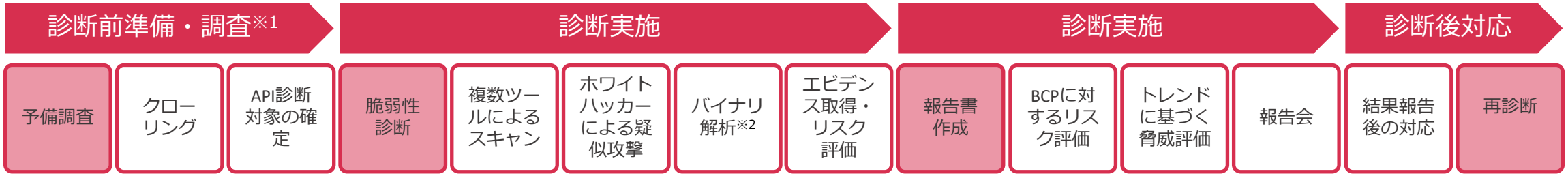
スマートフォンアプリケーション診断概要

- ✓ 実機を使った動的解析とAPK（Android）・IPA（iOS）ファイルの静的解析を実施します
- ✓ サーバ検査・クライアントアプリケーション検査を通じ、利用者情報が適切に取り扱われているか診断します
- ✓ 総務省提言の「関係事業者向け スマートフォン利用者情報取扱指針」で示された基本原則を考慮した診断を行います

サービスイメージ



サービスの流れ



※1　API診断ご依頼時のみ実施いたします
※2「スマホアプリ プラチナ診断」をご依頼の場合に実施いたします。

診断項目

スマホアプリ脆弱性診断（Android、iOS）およびAPI診断の検査項目概要です。

診断項目	主な例	
通信診断	• 不正通信の有無（不要な情報の送信・意図しないサーバとの通信） • 重要情報の送信における不備（個人情報・ID/パスワード・決済情報） • SSL/TLS暗号化通信の検証（証明書・暗号化方式）	
端末内データ診断	• データ保持における不備（File, Database等での平文保持） • データ改竄による不正行為（チート・課金回避） • ログへの重要情報の出力（個人情報・ID/パスワード）	• パーミッションの設定不備* • SDカードへの機密情報の出力*
バイナリ診断 （プラチナプランのみ）	• アプリ間連携・共有機能のアクセス制御不備* • WebView関連の問題点の有無 • 難読化・耐タンパー性の確認	• プロトコルの解析（HTTP以外） • リバースエンジニアリングによる解析（ソースコード・ロジック）

*印付きはAndroidのみの検査項目です

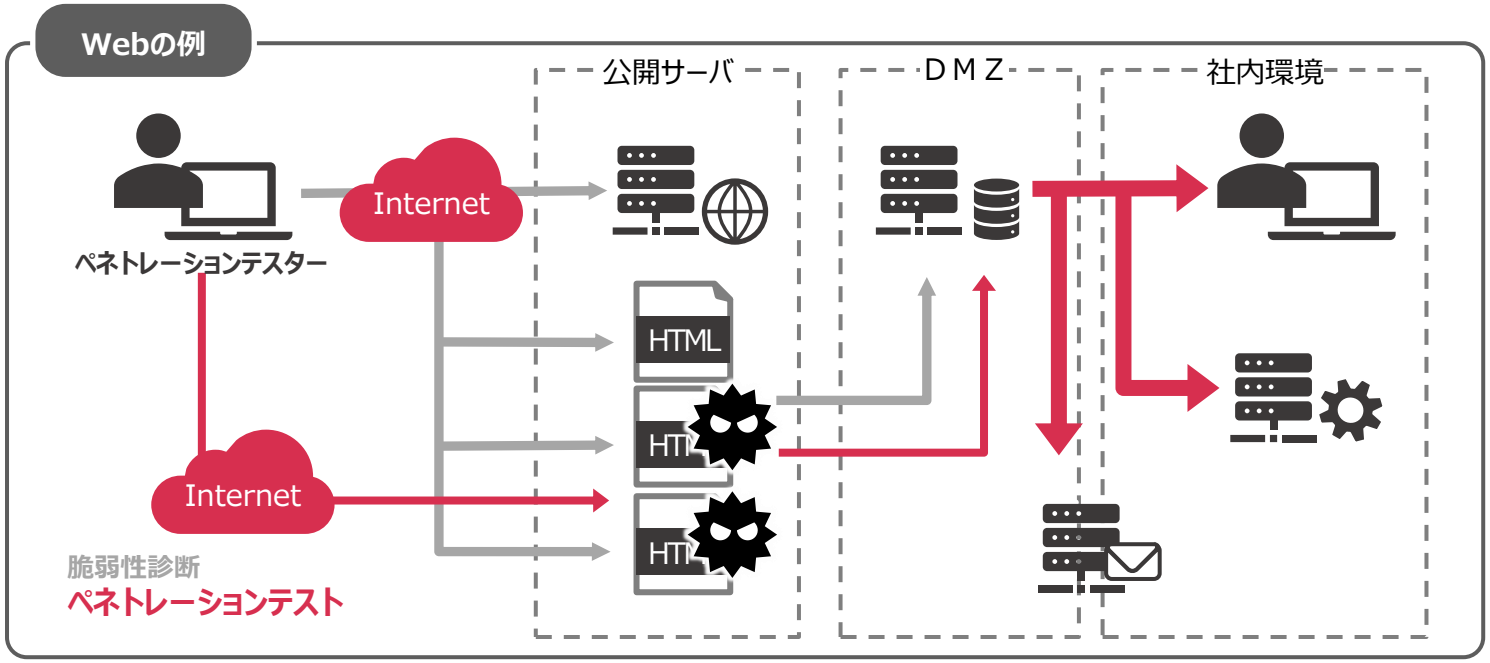
API診断項目	主な例		
入出力処理	• クロスサイトスクリプティング • SQLインジェクション • コマンドインジェクション	• パスマニピュレーション • パラメータ推測 • 例外処理に関する問題	• オープンリダイレクト • CRLFインジェクション
認証	• ログイン・認証処理に関する調査	• パスワードの強度に関する調査	
セッション管理	• セッションID・トークンに関する調査 • セッションハイジャック・固定化	• クロスサイトリクエストフォージェリ • アカウントの権限に関する調査	
重要情報の取り扱い	• 個人情報・決済情報などの管理に関する調査	• キャッシュ制御に関する調査	• 強制ブラウジング
システム情報・ポリシー	• システム情報の開示・エラーメッセージの表示	• ディレクトリリスティング	• ソフトウェアの既知の脆弱性

ペネトレーションテスト

ペネトレーションテスト：概要

- ✓ 事前調査により特定した「システムのより脆弱な箇所」を起点としてシナリオベースの疑似攻撃を行うことでシステムの堅牢性を確認します
- ✓ システム特性に応じた効果的な防御方法の構築、現在のセキュリティ対策の有効性の確認、万が一攻撃を受けた場合の被害範囲・深刻度の把握が可能です。

サービスイメージ



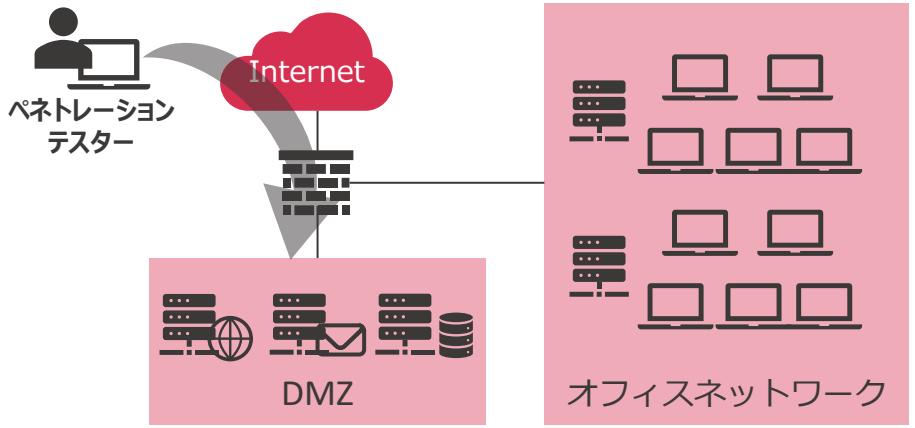
サービスの流れ

ヒアリング・シナリオ作成	事前準備	テスト実施	テスト結果分析・報告
システム環境、データ保管、ログ取得・監視状況等を確認し、テスト内容/範囲、シナリオ等を決定	決定した内容に基づいた、ツール、エクスプロイトコード、C&Cサーバ等、攻撃の準備	合意した期間・範囲で、権限奪取、認証突破、機密情報奪取等、侵入可否の検証	テスト結果を分析し、実施した攻撃内容と結果、侵入に関するリスクについて報告書を作成・提出

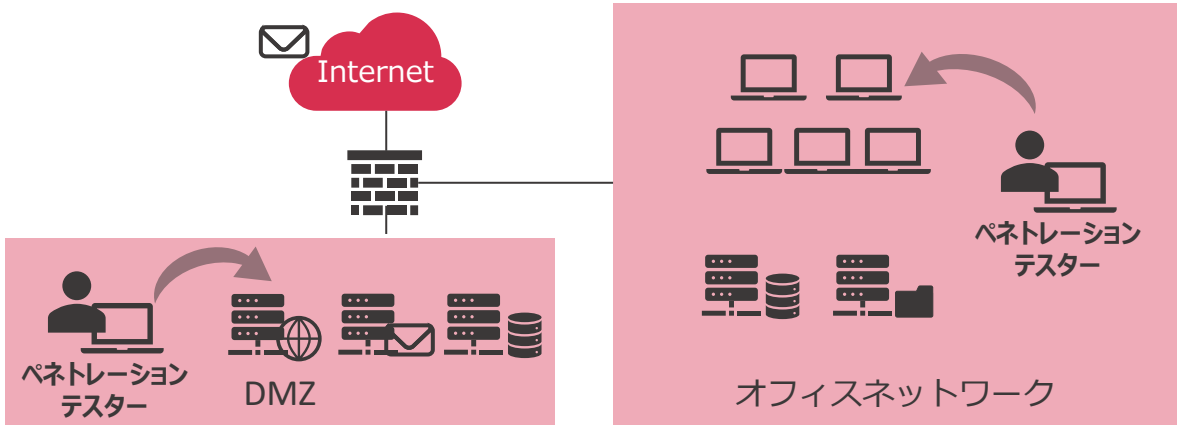
ペネトレーションテスト：シナリオ設計

ペネトレーションテストにおけるシナリオのイメージ例です。

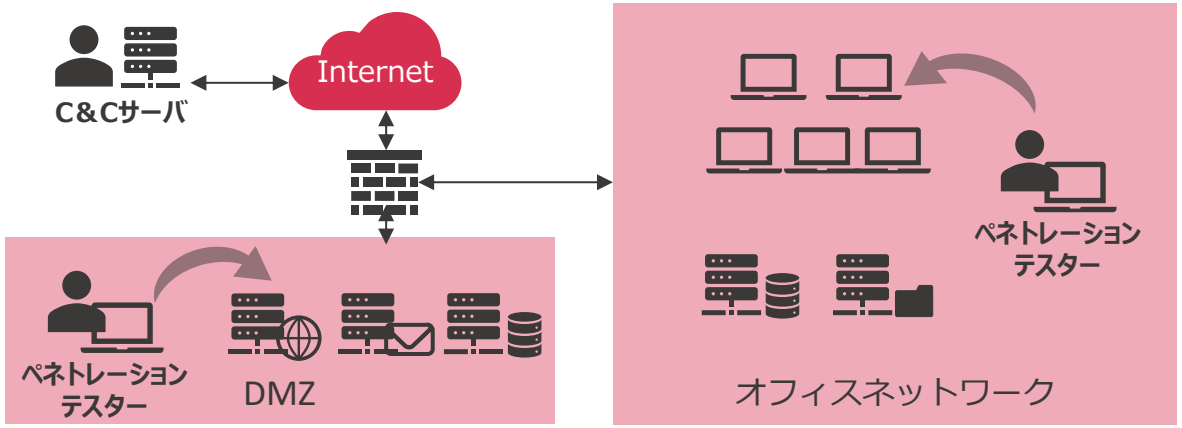
例1：リモートによるDMZ環境への侵入



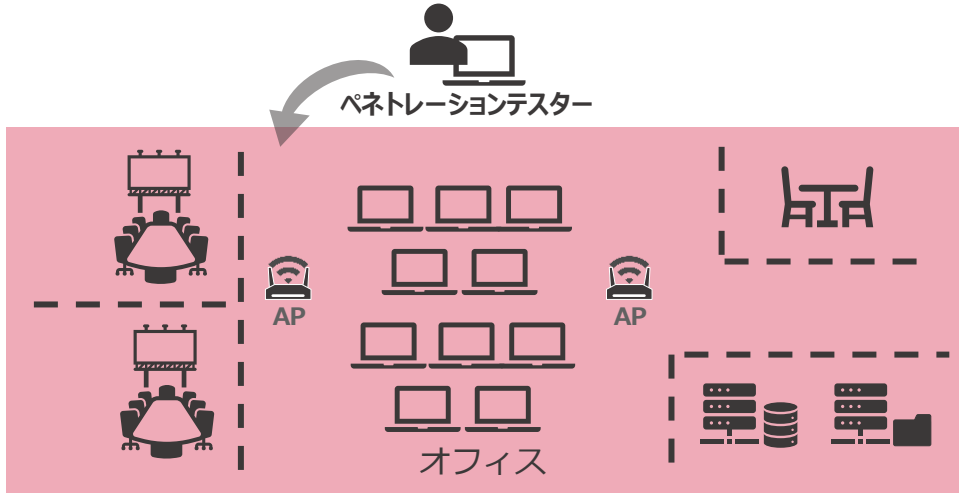
例２：オンサイトでの侵入



例３：疑似マルウェアによる侵入



例4：Wi-Fiアクセスポイントへの侵入

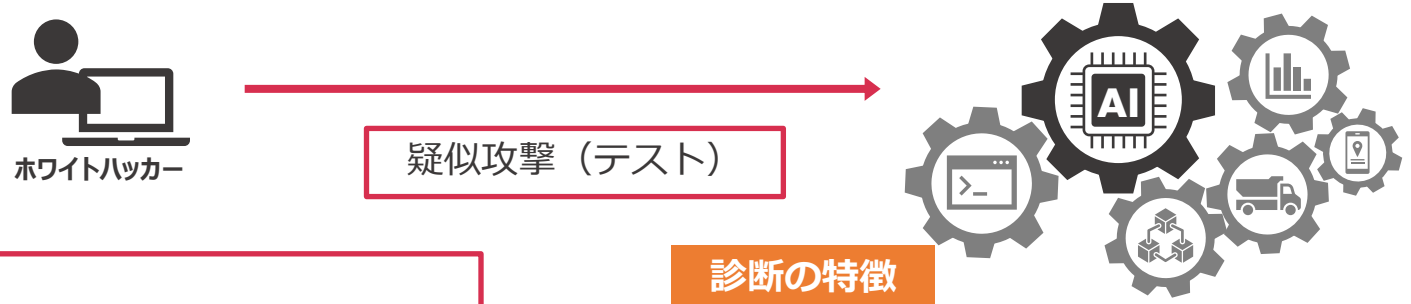


AI/LLMセキュリティ診断

AIレッドチーミング（ライト）：概要

- ✓ プロンプトインジェクション、プロンプトリーキングなどの手法を用いて、AIシステムに対する疑似攻撃を実施
- ✓ システムに潜むリスクを洗い出し、安全・安心な運用を実現するための具体的な対策をご提案します。

サービスイメージ



テスト内容

①プロンプトインジェクション
LLMに与える指示文（プロンプト）を悪用し、本来の設計や意図を無視させた処理を誘発する攻撃手法です。
チャットのようにLLMへ直接指示分を入力をする方法と、外部のWebサイトの参照やファイル読み込み等を通した間接的に指示分を入力する方法があります。

②プロンプトリーキング
LLMに与える指示文（プロンプト）を悪用し、本来公開すべきでない内部情報を出力させる攻撃です。内部情報として、システムプロンプトや本来権限のない内部情報の閲覧などがあります。
プロンプトインジェクションの一部です。

診断の特徴

①ユースケースに基づくテスト
生成AIは利用目的や方法に応じてリスクが異なります。当社はユースケースから導出したリスクシナリオに対して、重点的にテストし、重要なリスクを的確に把握します。

②手動・自動を組み合わせた診断
ユースケースに応じた手動テストに加えて、自動ツールによる疑似攻撃を行うことで、短時間で幅広くリスクを洗い出します。

③AIセーフティ・セキュリティガイドライン準拠
AIセーフティ・セキュリティガイドラインに沿ったテストで安全・安心なシステム構築・運用を支援します。

サービスの流れ

AIシステムのヒアリング → テスト環境準備 → 攻撃実行 → 報告書作成 → 修正箇所に対する攻撃実行（再診断）

AIレッドチーミング（スタンダード）：スケジュール

- ✓ **標準スケジュールは、計画策定、テスト準備から報告まで2か月間**

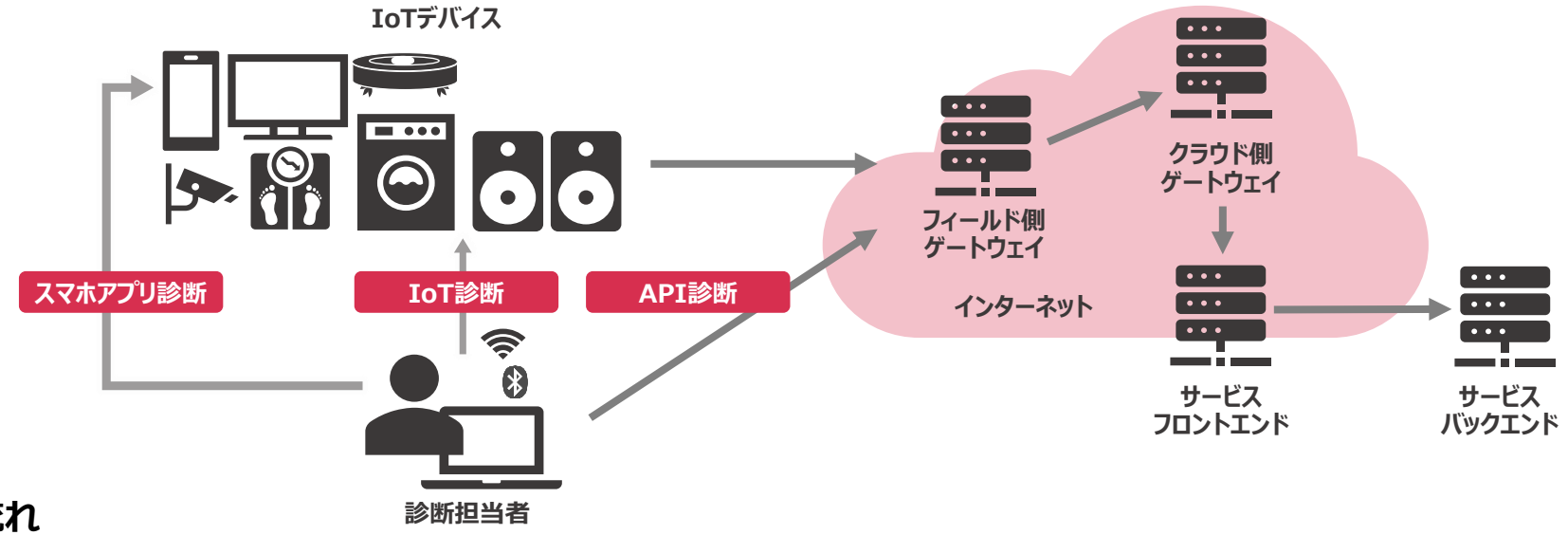
実施事項	N月				N+1月			
	第1週	第2週	第3週	第4週	第1週	第2週	第3週	第4週
計画策定	AIシステム詳細ヒアリング							
		リスクシナリオ作成						
		攻撃シナリオ作成						
テスト準備・テスト			テスト環境準備					
				攻撃シナリオ実行				
結果報告・再テスト						結果分析		
							報告書作成	
							別途再テストを実施(問題個所1か所につき1回まで)	

IoTセキュリティ診断サービス

IoT脆弱性診断：概要

- ✓ 診断対象デバイス固有の機能（各種プロトコル・インタフェース接続）を利用し、攻撃者による「不正操作」「情報の窃取」「踏み台化」等に悪用可能な脆弱性有無の診断をおこないします
- ✓ 利用されているOS/ミドルウェアの既知の脆弱性の有無も確認します。

サービスイメージ



サービスの流れ

診断前準備・調査※1			診断実施					診断実施				診断後対応	
予備調査	クローリング	対象APIの機能分析	脆弱性診断	複数ツールによるスキャン	ホワイトハッカーによる疑似攻撃	バイナリ解析※2	エビデンス取得・リスク評価	報告書作成	アナリストによる評価	報告書内容レビュー	報告会	結果報告後の対応	再診断

※1　API診断ご依頼時のみ実施いたします
※2「スマホアプリ プラチナ診断」をご依頼の場合に実施いたします。

IoT脆弱性診断：検査項目

✓ IoT脆弱性脆弱性診断査項目概要

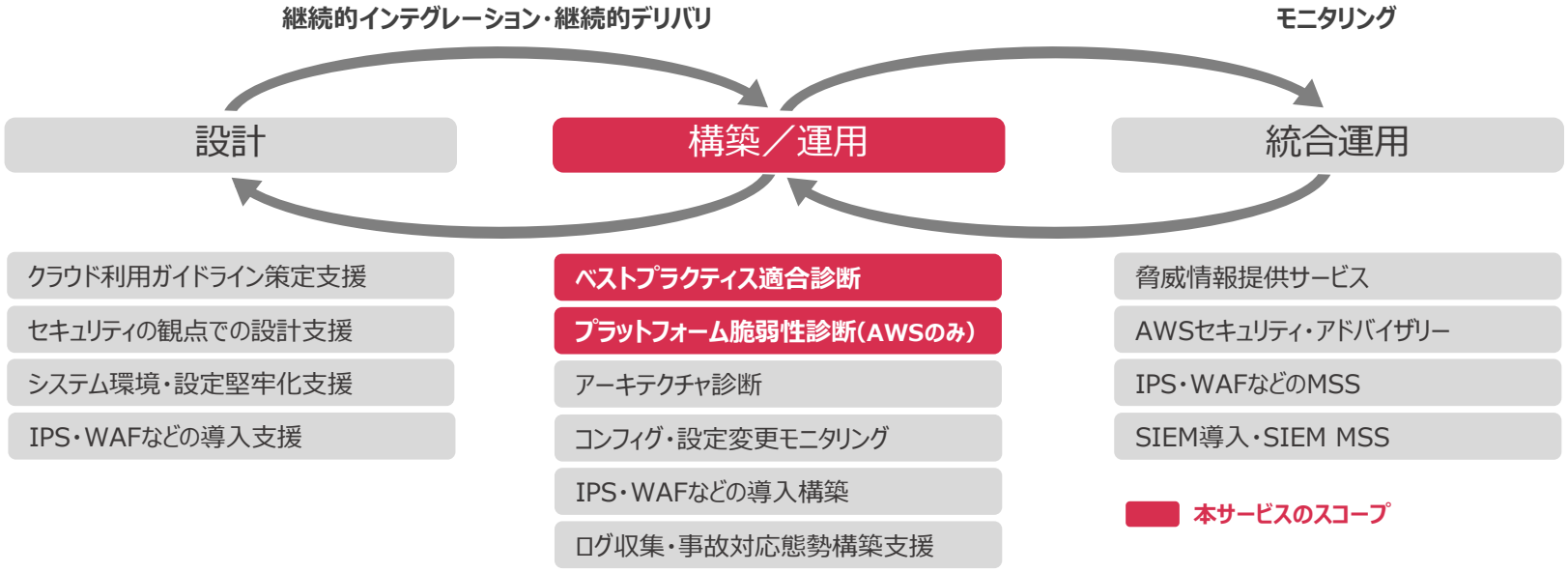
API診断項目	主な例		
インターフェース	• Webインタフェース（XSS） • Webインタフェース（SQLi） • Webインタフェース（CMDi）	• Webインタフェース（CSRF） • パラメータ推測 • 例外処理に関する問題	• クラウドインタフェースの制御 • 物理インタフェースの制御
認証/認可	• ログイン・認証処理に関する調査 • パスワードの強度に関する調査	• セッションID・トークンに関する調査 • 不適正な権限管理	
ネットワークサービス	• オープンポートの状態	• NWレイヤの既知の脆弱性	
暗号化・難読化	• 個人情報・決済情報などの管理	• 暗号化のロジック	• 耐タンパー性
システム情報・ポリシー	• システム情報の開示・エラーメッセージの表示	• プライバシーの取り扱い	• ファーム/ソフトウェアの既知の脆弱性

クラウドセキュリティ設定診断

クラウドセキュリティ設定診断：概要

- ✓ クラウド環境の設定上の問題による情報漏えいや不正アクセスを未然に防ぐための検証サービス
- ✓ 各パブリッククラウド環境に特化したベンチマーク指標に基づき、専門家の知見を活かした独自の観点で評価を行い、対策方法をご提供

サービスイメージ



サービスの流れ

アクセス確認	診断実施	診断結果分析	報告書提出
診断用に準備いただいたアカウントでのログイン確認	手動＋対象クラウドネイティブまたは弊社独自ツールで診断	診断結果の分析と評価を行い、推奨策も含む報告書を作成	診断結果に関する質疑応答

クラウドセキュリティ設定診断：検査項目

診断メニュー	診断概要		主な検出項目例	
AWS				
セキュリティベンチマークのチェック	アーキテクチャに依存しない、クラウドにおける基本的なセキュリティ設定が正しく行われているかを診断		• ID/アクセス管理 • ロギング • モニタリング	• ネットワーキング • その他（CISベンチマーク外）
セキュリティに関するAWSベストプラクティス適合診断	VPC/EIP/EC2/EBS/ELBのセキュリティ設定がベストプラクティスに適合しているか診断		• セキュリティグループ • ID/アクセス管理 • S3バケットのアクセス許可	• Route53 MX、SPFリソースレコードセット • CloudFront SSL証明書
プラットフォーム診断	ネットワーク診断	ネットワーク設定を分析してEC2インスタンスのセキュリティ上の脆弱性を診断	ネットワーク到達可能性	
	ホスト診断	各種設定がポリシーに準拠しているか診断	• 共通脆弱性識別子 • CISセキュリティ設定ベンチマーク	• セキュリティのベストプラクティス • 実行時の動作分析
Microsoft Azure				
セキュリティベンチマークのチェック	アーキテクチャに依存しない、クラウドにおける基本的なセキュリティ設定が正しく行われているかを診断		• ID/アクセス管理 • ロギング • モニタリング • ネットワーキング	• 仮想マシン • ストレージ • データベース • その他（CISベンチマーク外）
Google Cloud Platform				
セキュリティベンチマークのチェック	アーキテクチャに依存しない、クラウドにおける基本的なセキュリティ設定が正しく行われているかを診断		• ID/アクセス管理 • ロギング • モニタリング • ネットワーキング	• 仮想マシン • ストレージ • データベース • その他（CISベンチマーク外）
Oracle Cloud Infrastructure				
セキュリティベンチマークのチェック	アーキテクチャに依存しない、クラウドにおける基本的なセキュリティ設定が正しく行われているかを診断		• ID/アクセス管理 • ロギング • モニタリング	• ネットワーキング • ストレージ • 資産管理

Appendix

診断報告書サンプル（1/3）

報告書のサンプルとなります。

診断結果>総合評価

2−1　総合評価

今回実施した診断の診断結果に基づき、弊社の評価基準に照合した総合評価を脆弱性診断に対して行いました。以下に評価クラスと評価の根拠となった診断結果を示します。

クラウドシステム

B	危険性の高い脆弱性は確認されておらず、セキュリティ上問題の少ない状態です

- Web サーバの設定不備に起因する軽微な問題が複数確認されております

また、表 2-1-1 は総合評価を改善するために必要な対策の一覧です。一般に公開される Web アプリケーションについては、A もしくは B の総合評価となるよう対策を実施することを推奨します。

表 2-1-1　総合評価を改善するために必要な対策

対策内容	対策が行われた場合の総合評価
危険度 Low を含む、全ての脆弱性の対策を実施	A

評価基準につきましては「5−3　評価基準」として添付しておりますので、必要に応じてご参照下さい。

診断結果>概要

2−2　概要

本診断の診断対象範囲において検出された脆弱性を危険度別に集計したものを図 2-2-1　危険度別脆弱性検出数に、診断項目別に集計したものを図 2-2-2　診断項目別脆弱性検出数、表 2-2-1　診断項目別脆弱性検出数一覧に示します。

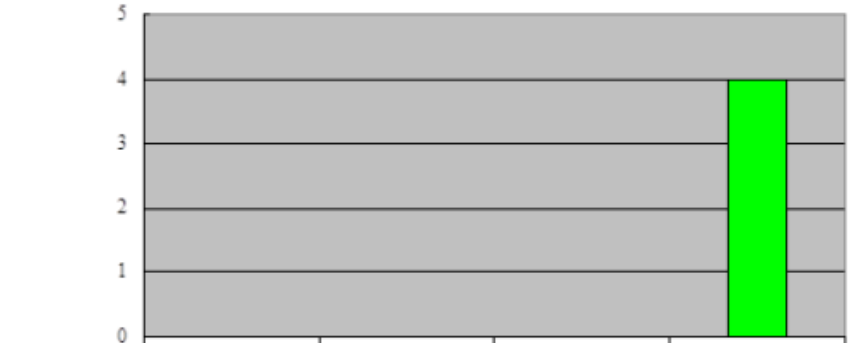


図 2-2-1　危険度別脆弱性検出数

診断報告書サンプル（2/3）

報告書のサンプルとなります。

診断結果>脆弱性検出数一覧

表 2-2-1　診断項目別脆弱性検出数一覧

診断項目	脆弱性名称	危険度	クラウドシステム
クロスサイトスクリプティング	-	-	-
ステルスコマンド	-	-	-
SQL インジェクション	-	-	-
バッファオーバーフロー	-	-	-
既知の脆弱性	-	-	-
強制ブラウジング	-	-	-
hidden フィールドの操作	-	-	-
サードパーティ製品の設定ミス	アプリケーション標準エラーページの使用	Low	1
	アプリケーションバージョンの出力	Low	1
	X-Frame-Options ヘッダの未使用	Low	1
	X-Content-Type-Options ヘッダの未使用	Low	1
バックアップファイルの検出	-	-	-
バックドア、デバッグオプション	-	-	-
HTML 中のコメント	-	-	-
ディレクトリトラバーサル	-	-	-
不適切なエラーハンドリング	-	-	-
パラメータの改竄	-	-	-
Web サービスの脆弱性	-	-	-
クロスサイトリクエストフォージェリ	-	-	-
セッション管理の脆弱性	-	-	-
合　計		Critical	0
		High	0
		Medium	0
		Low	4

診断結果詳細

3　診断結果詳細

本章では、検出された脆弱性について解説を行います。

脆弱性の確認では Web ブラウザとして Google Chrome 127.0.6533.100 を使用しているため、それ以外のアプリケーションでは再現しない場合があります。
また、本章に記載されている URL や HTML、検出根拠の内容は診断時において有効だったものを記載しており、アクセスの度に変化するパラメータ等により、そのままの形では再現できない場合がございますので、あらかじめご了承下さい。

3−1　アプリケーション標準エラーページの使用

診断項目	サードパーティ製品の設定ミス
危険度	Low
対象サイト／検出件数	クラウドシステム／1 件

対象サイトにおいて、アプリケーションの標準エラーページが使用されていることを確認しております。

アプリケーションの標準エラーページは、その出力内容から使用しているアプリケーションの種類やバージョンを推測される可能性があります。また、アプリケーションによっては標準エラーページ自体が動的ページとなっており、過去には標準エラーページに脆弱性が確認されたこともあるため、注意が必要です。

図 3-1-1 は、https://stg.ship-viewer.tokyokeiki-marine.com/xxx にアクセスした際に確認されたアプリケーションの標準エラーページの出力結果です。
Microsoft IIS (Internet Information Services)の標準エラーページが出力されていることを確認できます。

診断報告書サンプル（3/3）

報告書のサンプルとなります。

総括

4　総括

本診断の結果、「サードパーティ製品の設定ミス」に分類される危険性の低い脆弱性が複数確認されております。緊急に対策を要するものではありませんが、サイトの安全性をより高めるため対策を実施することを推奨します。

今後の Web アプリケーションセキュリティへの対策としては、脆弱性が発生することを予防することも念頭に置き、以下のような対応の検討をお奨めします。

✓　開発当初からセキュリティを考慮した Web アプリケーションの実装の実施
開発時からセキュリティを考慮した実装を行うことにより、よりセキュリティ的に安全な Web アプリケーションを構築することが可能となります。通常の開発では開発者・開発会社によってセキュリティレベルが大きく変化することが予想されますが、開発指針・チェックリストを作成しておくことで最低限のセキュリティレベルを維持することが可能になると考えます。

✓　Web アプリケーションファイアウォールの導入による防衛
リリース前の脆弱性診断が難しいケースや、頻繁に Web サイトの更新を行うようなサイトでは、Web アプリケーションファイアウォールの導入が効果的です。
クロスサイトスクリプティングや SQL インジェクション等多くの Web アプリケーション脆弱性に対して防衛することが可能です。

以上で本報告を総括させて頂きますが、本診断報告書について指摘された脆弱性を修正するのみではなく、今後のセキュリティ対策に活用して頂ければ幸いです。

補足情報

5−3　評価基準

本診断結果報告書における総合評価は、表 5-3-1 に規定される絶対評価と、診断対象の環境を考慮して評価される相対評価によるものです。
絶対評価は、A、B、C、D のいずれかのアルファベット 1 文字で表記され、診断結果を絶対評価の評価基準に照合し適合するクラスが評価として与えられます。

表 5-3-1　絶対評価の評価基準

クラス	評価基準
A	脆弱性が検出されていない、もしくは診断環境に依存し実際に影響を受ける可能性は無いと考えられる軽微な脆弱性のみが検出されている。
B	システム情報の漏洩を始めとした、単体では被害を受ける可能性が低いと考えられる脆弱性のみ検出されている。
C	危険性の高い脆弱性が検出されており、被害を受ける可能性がある。
D	個人情報の漏洩に繋がる深刻な脆弱性が検出されている。または、検出されている複数の脆弱性を組み合わせることで個人情報の漏洩に繋がることが懸念される状態である。

相対評価は、絶対評価では表すことができない診断対象の環境やリスト対象等、外的要因について考慮されて評価されるものであり、＋（プラス；より安全）、－（マイナス；より安全でない）を絶対評価に付与することで表されます。

なお、上記評価基準は、弊社の診断実績を基に、診断結果を簡潔に表現するために作成された、弊社独自基準になります。上記評価基準による評価は、あくまでも診断結果を簡潔に表現するためのものであり、弊社は評価に対しての保証や責任は負いかねますのでご了承下さい。

スマートフォンアプリケーション脆弱性診断：診断事例

年間50システム以上のスマホアプリ診断を実施しています。以下は弊社診断事例の一部です。

業種	対象組織	規模	利用ケース
卸売業、小売業	食品会社	2アプリ	社内業務管理をスマートフォンから利用できるシステム基盤構築にともなうセキュリティチェック
サービス業	広告会社	2アプリ	一般消費者向け販促ツールであるスマホアプリの新規構築にかかるセキュリティチェック
ソフトウェア業	ITソリューション会社	2アプリ	一般向けナビゲーションシステムの機能改修におけるセキュリティチェック
ソフトウェア業	ITソリューション会社	1アプリ	地方自治体で採用された健康促進・チェック用スマホアプリのリリース前のセキュリティ診断
金融業	銀行	1アプリ	口座照会など銀行利用のためのスマホアプリの新規リリースにともなうセキュリティチェック
金融業	金融会社	2アプリ	振り込み・契約管理等のためのスマホアプリの多要素認証実装に伴うセキュリティチェック
金融業	金融会社	2アプリ	信用取引等オンライントレードのためのスマホアプリ更改におけるセキュリティチェック
金融業	金融会社	2アプリ	口座開設やオンライントレードのためのスマホアプリ新規リリースにおけるセキュリティチェック

Webアプリケーション／ネットワーク脆弱性診断：診断事例

Webアプリケーション／ネットワーク脆弱性診断の事例をご紹介します。ここ数年は年間7,000システム以上の診断を実施しております。

業種	対象組織	規模	利用ケース
官公庁	海上保安庁	約40リクエスト	一般利用者向け電子計算機システムに対して、外部脆弱性診断を定期的（年2回）に実施
公益・特殊・独立行政法人	一般財団法人	約20リクエスト 約15IPアドレス 約５API	試験受験申込サイトに対して、外部脆弱性診断を定期的（年2回～3回）およびシステム更改時に実施
金融・保険業	メガバンク（大手銀行）	約1000リクエスト 約100IPアドレス	メガバンクおよび傘下のグループ銀行のシステムについて「Webサイトシステム」および「外部サービス」のセキュリティに関する検査として脆弱性診断を定期的（毎年）に実施
	銀行	約300リクエスト 約20IPアドレス	PCI DSS準拠のための脆弱性スキャン・ペネトレーションテストを実施（Web：年1回、NW：年4回）
	外資系保険会社	約100リクエスト 約60IPアドレス	米国親会社のセキュリティポリシーで要求される基準を満たすために外部脆弱性診断を定期的（年1回）に実施
情報・通信業	ITソリューション会社	約300リクエスト	ソリューション開発したWebサイトに対してサービス提供前のセキュリティチェックに活用
	ECサイト運営会社	約500リクエスト 約30IPアドレス	オンラインショッピングサイトと周辺システムに対して、外部/内部からの脆弱性診断を定期的（年１回）に実施
電気・ガス業	ガス会社	約2000リクエスト 約150IPアドレス	グループ全体で保有するWebサイト/インフラに対して、定期的な脆弱性診断を実施。また、対象システムの重要度に応じたペネトレーションテストを実施
製造業	鉄鋼会社	約1000リクエスト	社内業務システムに対して、機能拡充前に現状のセキュリティリスク可視化に脆弱性診断を活用
小売業	自動車部品販売会社	約30リクエスト 約20IPアドレス	公開業務Webアプリおよび各拠点サーバに対する脆弱性診断の実施
娯楽業	ゲーム会社	約300リクエスト	ゲーム関連のコミュニティサイトに対して、新規構築～機能追加の都度、外部脆弱性診断を実施


VES
validation engineering service