# 脆弱性診断サービスのご案内

**SQAT ® - Software Quality Analysis Team**
**Cracker Probing-Eyes®**
**インシデント対応**

株式会社ブロードバンドセキュリティ

# BBSecとは

## ITセキュリティサービスに特化したトータルセキュリティサービスプロバイダーです

2000年 に 国内ブロードバンド網の相互接続インフラを提供する会社としてスタートし、ネットワークおよびセキュリティの双方に知見を持ち、2006年に現社名に変更、『ITセキュリティサービス』に特化したトータルセキュリティサービスプロバイダーです。

2022年9月現在

| | |
|---|---|
| ■ 会社名 | **株式会社ブロードバンドセキュリティ（略称：BBSec）**<br>**BroadBand Security, Inc.** |
| ■ 本社所在地 | **東京都新宿区西新宿8-5-1 野村不動産西新宿共同ビル4F** |
| ■ URL | **https://www.bbsec.co.jp/** |
| ■ 設立 | **2000年11月30日** |
| ■ 資本金 | **293百万円** |
| ■ 決算期 | **6月** |
| ■ 株式公開情報 | **市場：東京証券取引所　スタンダード市場**<br>**上場日：2018年9月26日　　株式コード：4398** |
| ■ 従業員数 | **222名（2022年6月末現在）** |
| ■ 代表者 | **代表取締役社長　　滝澤 貴志**<br>**代表取締役副社長　森澤 正人** |
| ■ 事業内容 | **1.　セキュリティ監査・コンサルティングサービス**<br>**2.　脆弱性診断サービス**<br>**3.　情報漏えいIT対策サービス** |
| ■ 事業所 | **国内：天王洲オフィス、大阪支店、名古屋支店、東北セキュリティ診断センター**<br>**海外：韓国支店**<br>**セキュリティオペレーションセンター：1拠点（東京都内）** |

# Why BBSec？

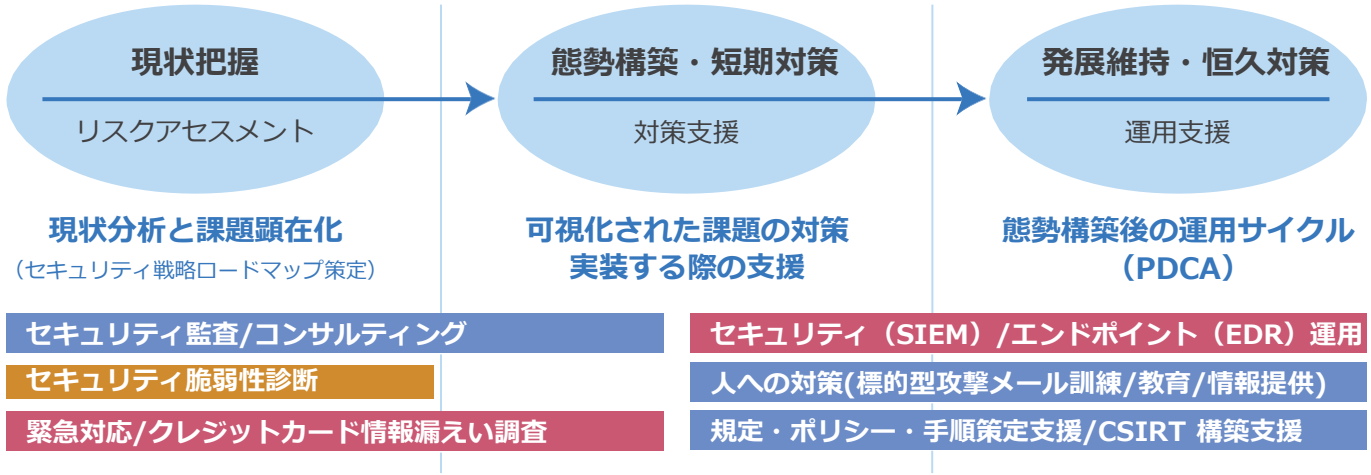
## 多くのお客様から選ばれるのには、理由があります

お客様それぞれの課題に的確な答えを導き出す**セキュリティ監査／コンサルティング**、様々なアプリケーションの脆弱性リスクを発見し対策を提案する**脆弱性診断**、日々の情報システムを情報セキュリティリスクから守る**情報漏えいIT対策**の３つのサービスカテゴリを核にサービスを展開しています。

| | | |
|---|---|---|
| **脆弱性診断実績**<br>延べ **45,500システム**<br>（2022年6月現在） | **SWIFT評価企業数**<br>**30社**<br>（2023年1月現在） | **AWS認定資格取得数**<br>**123名**<br>（2022年5月現在） |
| **PCI DSS準拠認定付与案件数**<br>**678件**<br>（2023年1月現在） | **PCI DSS準拠認定付与企業数**<br>**150社**<br>（2023年1月現在） | **PCI関連資格取得者数**<br>**111名**＜QSA、CISSP等＞<br>（2023年1月現在） |

### 経営課題として、システム・組織の両面からセキュリティ課題を可視化、優先順位付け、セキュリティ対策を実施、運用サイクル（PDCA）をご支援

**BBSecのアプローチ**　例）現状分析からのアプローチの場合



# サービスラインナップ

| | サービス名 | 掲載頁 | サービス概要 | 目的/効果 |
|---|---|---|---|---|
| 手動診断 | Webアプリケーション脆弱性診断 | p. 7 | 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 | p. 9 | 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 | P. 12 | 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 | p. 14 | 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 |
| | IoT脆弱性診断 | p. 17 | 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 | p. 19 | AWS、MicrosoftAzure、GoogleCloudPlatform、OracleCloud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 |
| | ペネトレーションテスト | p. 21 | 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 |
| | ランサムウェア対策総点検 | p. 23 | 標的型攻撃などによりランサムウェアに感染したと想定してその先に起こりうる被害を検証し、リスクを可視化します | 相次ぐランサムウェア攻撃に対する備えとして |
| | ハイブリッド診断 | p. 25 | 外部（攻撃者）の視点と内部（開発者）の視点を組み合わせた包括的な診断メニューにより、精度の高い診断を短期間で実施します | 限られた期間で効果的に問題部位を特定 |
| | 差分診断 | p. 27 | 前回診断時以降に追加更新された脆弱性検査シグネチャを主軸に検査し、診断期間短縮と低コスト化を図ります | 定期的な診断を精度を落とさず効率よく実施 |
| 自動診断 | デイリー自動脆弱性診断 | p. 30 | ネットワークおよびWebサイトの脆弱性を毎日自動診断し、専用のWebページで報告します | 手軽に国産ツールによる診断が可能 |
| | ソースコード自動診断 | p. 33 | ソースコードを専用ポータルにそのまま圧縮/アップロードするだけで自動で静的解析します | ソースコードの安全性を手軽にチェック可能 |
| インシデント対応 | セキュリティ事故調査対応サービス | p. 37 | インシデント発生時に、緊急対応、調査対応、脅威ハンティング、報告・復旧までの統合的な支援を行います | 予期せぬインシデントには専門家による支援が有効 |
| | クレジットカード情報漏えい フォレンジック調査サービス | p. 39 | PCI SSCにPFIの認定を受けたフォレンジック調査機関であるBBSecがクレジットカード情報漏えい事故の調査・報告を行います | クレジットカード情報漏えい事故で必須となるPFIによる調査 |

# 手動診断―SQAT®：Software Quality Analysis Team

SQAT®（Software Quality Analysis Team）サービスは、「システムの弱点をあらゆる視点から網羅する」「正確かつ客観性の高いレポートをする」「お客様にわかりやすく説明する」が特徴です。お客様は、すべての問題部位と脆弱性のポイントの把握、リスクに対する明確な理解、具体的な対策立案のヒントを得ることができます。



## PERFORMANCE

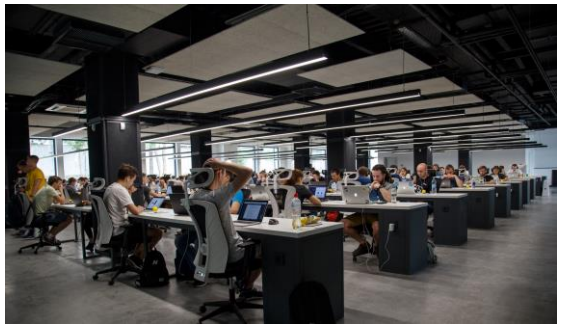
### のべ6,980組織/42,100システムの診断実績

サービス開始以来、民間企業から公共機関まで、業種・システム規模問わず幅広く脆弱性診断を実施してまいりました。

特に厳格なセキュリティレベルが求められる金融機関のようなお客様の診断実績は、継続して多数を占めています。

## QUALITY

### 経験豊富な専門技術者による高精度な診断とリスク評価



OWASP TOP10、ASVS、Testing Guide /NIST SP 800シリーズ、PCI DSS等の標準を踏襲した網羅性の高い診断内容です。

豊富な経験・資格を保有するセキュリティエンジニアおよびセキュリティアナリストにより、複数の手法を組み合わせた高精度な診断とリスク評価を行います。

## SUPPORT

### 診断実施後のお問合せ対応や再診断など各種サポート

診断実施後も診断結果に関するお問い合わせを承ります。診断結果の報告会は、弊社技術者がご訪問またはオンラインにて、ご説明および質疑応答いたします。

また、報告書納品日から３ヶ月の間、リモートでの再診断を無償（サービスによっては有償）でご提供いたします。

# リスクレベル評価基準

検出された脆弱性に対して 「攻撃による影響度」と「攻撃される可能性」について総合的に評価し、危険度を５～１までに分類、問題箇所の事象・リスク・対策方法を解説いたします。

| | リスクレベル | | 解説 |
|---|---|---|---|
| 現象・リスク・対策方法を解説 | 5 | 緊急 | システムの管理者権限でのコマンド実行が可能な場合や、バックドア生成などの攻撃コードが公開されているOS・ミドルウェアが使用されている場合、または脆弱性を利用した攻撃によって、容易に大量の個人情報の取得や改竄が可能な場合などが該当します。 |
| | 4 | 重大 | 「緊急」と同様に個人情報の取得やクライアントへの攻撃などに使用できるが、ある程度の知識が必要であったり有用な情報を得るために複数回の攻撃を実行する必要があったりする場合が該当します。 |
| | 3 | 高 | サービス提供やシステムの可用性に影響を与えるもの、もしくは取得できる情報が限定的な場合に適用されます。また、情報漏洩等の直接的な被害がなくとも、脆弱性が利用される、もしくは公表されることでシステムに対する信用の低下が懸念されるものもここに含まれます。 |
| | 2 | 中 | 設定情報や管理情報といったシステムへの攻撃手段を提供する可能性がある問題、または個人情報等のユーザ情報が漏洩する可能性がある問題のうち比較的実行の難易度の高いものや、他の脆弱性を利用する必要のあるものが対象となります。 |
| | 1 | 低 | システムの一般的な情報やサービスの運用状況等、攻撃者の興味を引く情報の開示の可能性のある問題が該当します。または、ローカルネットワークやクライアントPCへの直接アクセスなど、悪用するための条件が複数必要なものが対象となります。 |
| 現象を解説 | 0 | 情報 | 指摘された項目自体は脆弱性ではありませんが、品質上の問題やセキュリティ向上のための推奨事項等が対象となります。 |

# サイバー保険付帯の脆弱性診断サービス

弊社は、三井住友海上火災保険株式会社との提携により、「サイバー保険を自動付帯した脆弱性診断サービス」を提供しております。

## サービス概要

| | |
|---|---|
| 対象期間 | BBSecによる脆弱性診断の契約日から1年間 |
| 補償対象 | 情報漏えいやサイバー攻撃に起因する賠償損害<br>事故発生時に対策を講じた場合の費用損害 |
| 補償金額 | 最大1,000万円まで |

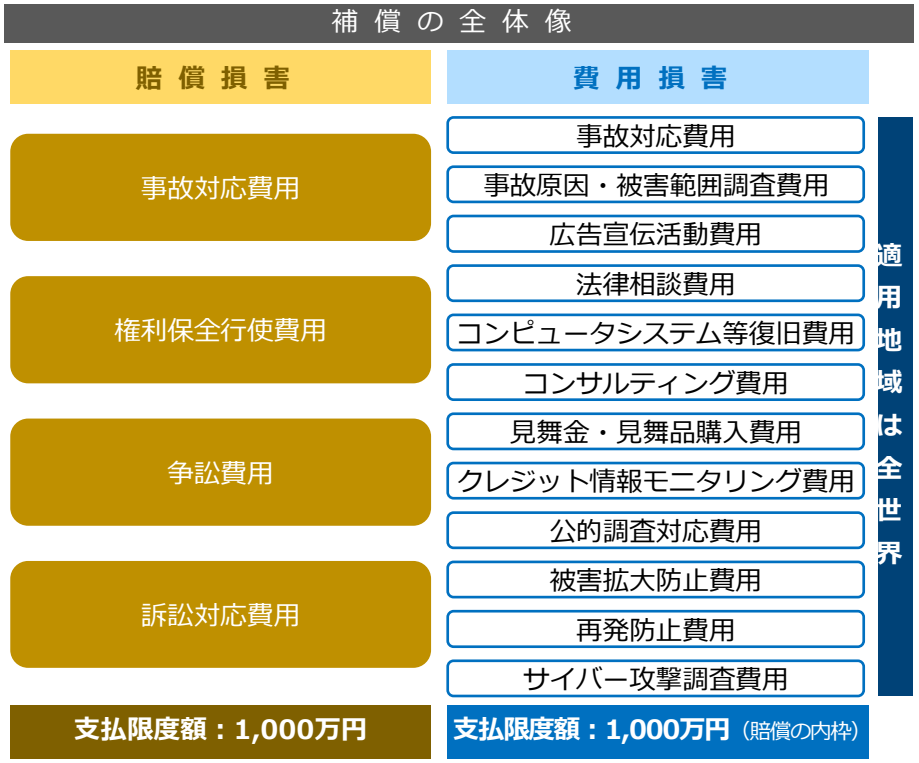
弊社データによると、実際の初動対応には平均して1,000万円程度必要であると想定されます。

## 対象となる脆弱性診断

- **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**
- **スマホアプリ脆弱性診断**
- **クラウドセキュリティ設定診断**
- **ソースコード診断**
- **ペネトレーションテスト**
- **IoTセキュリティ診断**

複数回脆弱性診断を実施した場合、最新の契約日から1年間有効となります。

## 補償概要

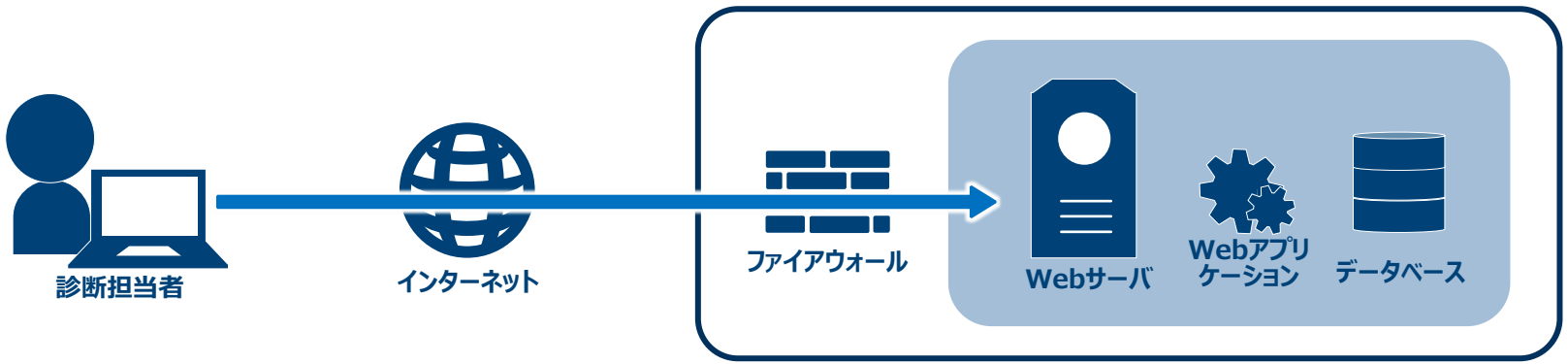


# Webアプリケーション脆弱性診断―SQAT® for Web：概要

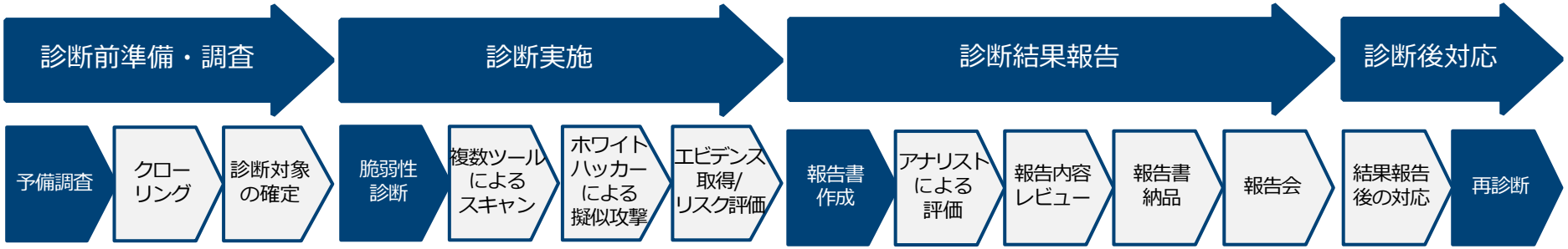
Webサイトを攻撃するハッカーの手法を用いて、外部から動的に脆弱性を診断することで、攻撃の入り口となる可能性のある箇所を検出します。

診断は最新のセキュリティ情報に基づいて実施されますので、システムの新規構築や改修のリリース前だけでなく、定期的な実施等、既存システムの脆弱性確認にも有効です。

## サービスイメージ




## サービスの流れ



# Webアプリケーション脆弱性診断―SQAT® for Web：検査項目

Webアプリケーション脆弱性診断の検査項目概要です。

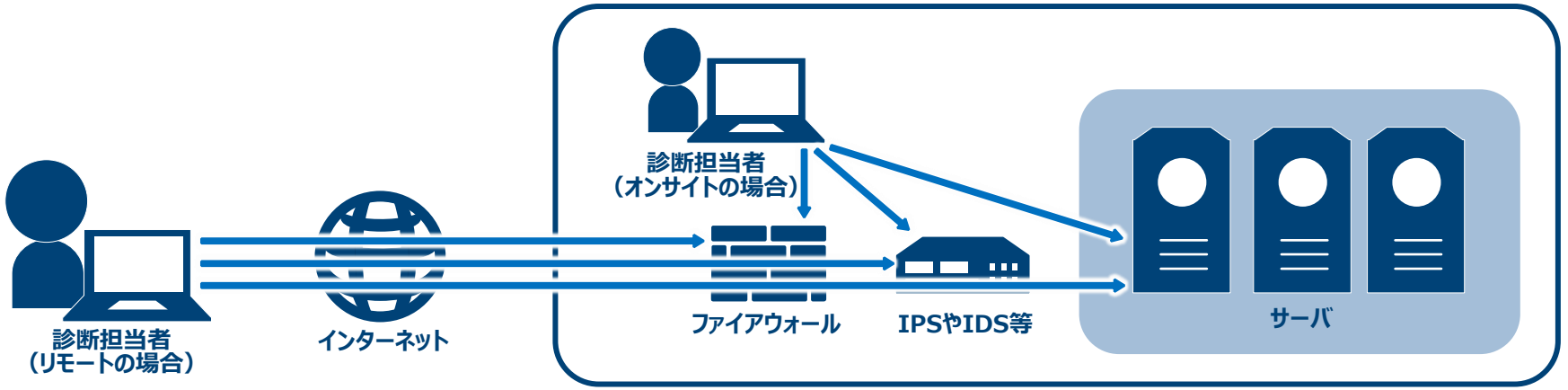
| 診断項目 | 主な例 *標準では実施しない項目 | | |
|---|---|---|---|
| 入出力処理 | クロスサイトスクリプティング | パスマニピュレーション | オープンリダイレクト |
| | HTMLタグインジェクション | ファイルアップロード機能に関する調査 | CRLFインジェクション |
| | SQLインジェクション | パラメータ推測 | バッファオーバーフロー* |
| | コマンドインジェクション | 例外処理に関する問題 | XML外部エンティティ参照 |
| 認証 | ログインフォームに関する調査 | 復認証回避に関する調査 | 認証トークンに関する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

# ネットワーク脆弱性診断―SQAT® for Network：概要

システム全体に影響をおよぼすネットワークをリモートまたはオンサイトで動的診断いたします。

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を対象とした診断も実施し、機器自体の問題やセキュリティパッチ適用漏れを検出することが可能です。脆弱性を徹底的に洗い出し、システムの堅牢化をご支援します。

## 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―SQAT® for Network：検査項目

ネットワーク脆弱性診断の検査項目概要です。

| 診断項目 | 主な例 | | |
|---|---|---|---|
| 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<br>メールサーバに関する調査<br>FTPに関する調査 | RPCに関する調査<br>ファイル共有に関する調査<br>SNMPに関する調査 | SSHサーバに関する調査<br>データベースサーバに関する調査<br>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<br>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<br>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 | | |

# Webアプリケーション/ネットワーク脆弱性診断：診断事例

弊社診断事例の一部をご紹介します。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<br>約15IPアドレス<br>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<br>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 |
| 金融・保険業 | 銀行 | 約300リクエスト<br>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） |
| 金融・保険業 | 外資系保険会社 | 約100リクエスト<br>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 |
| 情報・通信業 | ECサイト運営会社 | 約500リクエスト<br>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<br>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<br>約20IP | 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 |

# ソースコード診断―SQAT® Core：概要

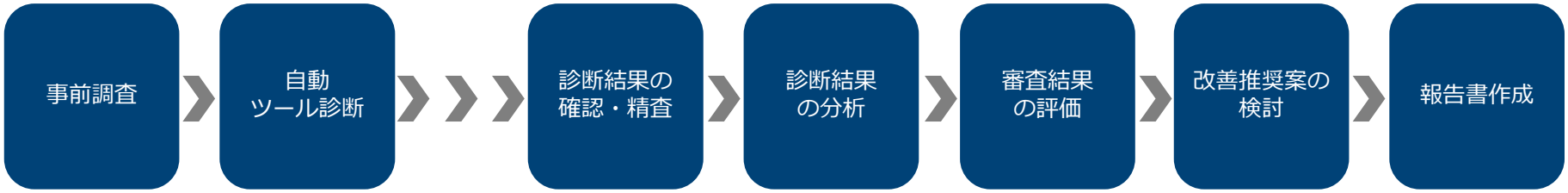
独自開発ソフトウェアのソースコードを静的に分析し、セキュアなコーディングルールと データフローをチェックし、隠された脆弱性とコーディング品質を検証し、結果および回避の為の改善案を提示します。

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利用いただけます。

## 脆弱性診断との比較

| | 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**<br>• **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**<br>• **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



# ソースコード診断―SQAT® Core ：対応言語・検出例

## 対応言語

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

## 検知する脆弱性の例

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

※ 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

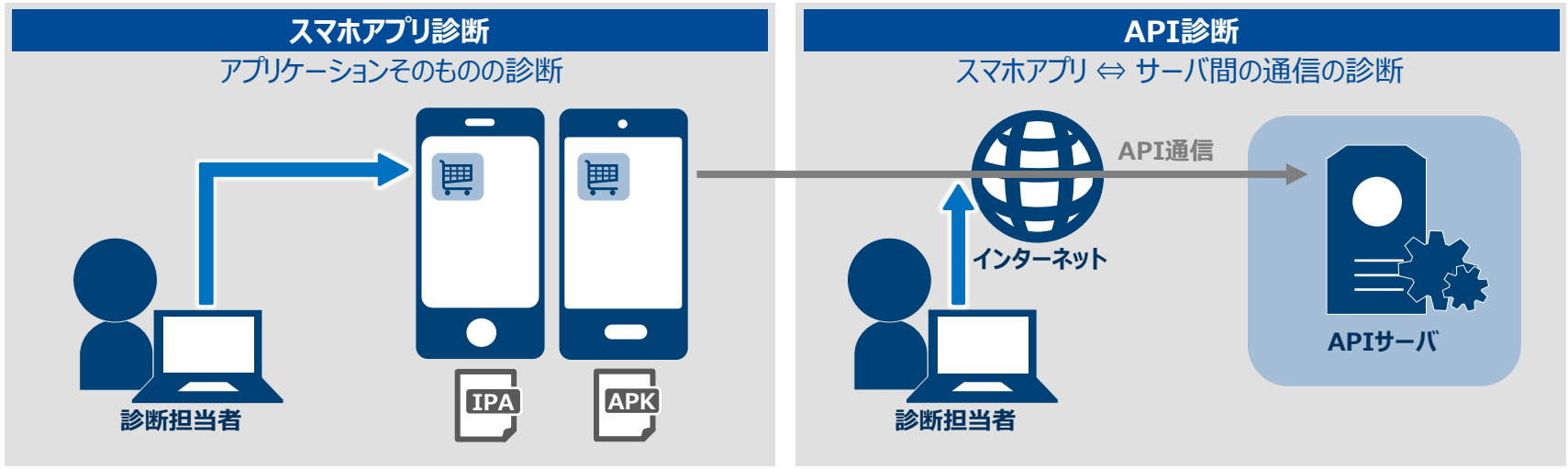
| | | | |
|---|---|---|---|
| メソッドにおける未検証の引数 | 不適切な例外処理 | デバッグコードの残存 | 等 |

# スマホアプリ脆弱性診断―SQAT® for Smartphone：概要

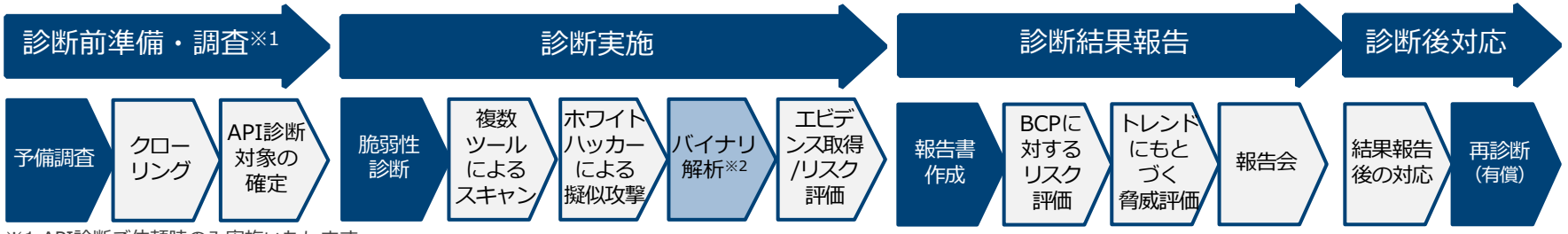
実機を使った動的解析とAPK（Android）・IPA（iOS）ファイルの静的解析を実施します。サーバ検査・クライアントアプリケーション検査を通じ、利用者情報が適切に取り扱われているか診断します。

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（スマホアプリ&API）




※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。

# スマホアプリ脆弱性診断―SQAT® for Smartphone：検査項目

スマホアプリ脆弱性診断（Android、iOS）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）<br>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）<br>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）<br>データ改竄による不正行為（チート・課金回避）<br>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*<br>SDカードへの機密情報の出力* |
| バイナリ診断<br>（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*<br>WebView関連の問題点の有無<br>難読化・耐タンパー性の確認 | プロトコルの解析（HTTP以外）<br>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診断の検査項目概要です。

| 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<br>SQLインジェクション<br>コマンドインジェクション | パスマニピュレーション<br>パラメータ推測<br>例外処理に関する問題 | オープンリダイレクト<br>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<br>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<br>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 |

# スマホアプリ脆弱性診断：診断事例

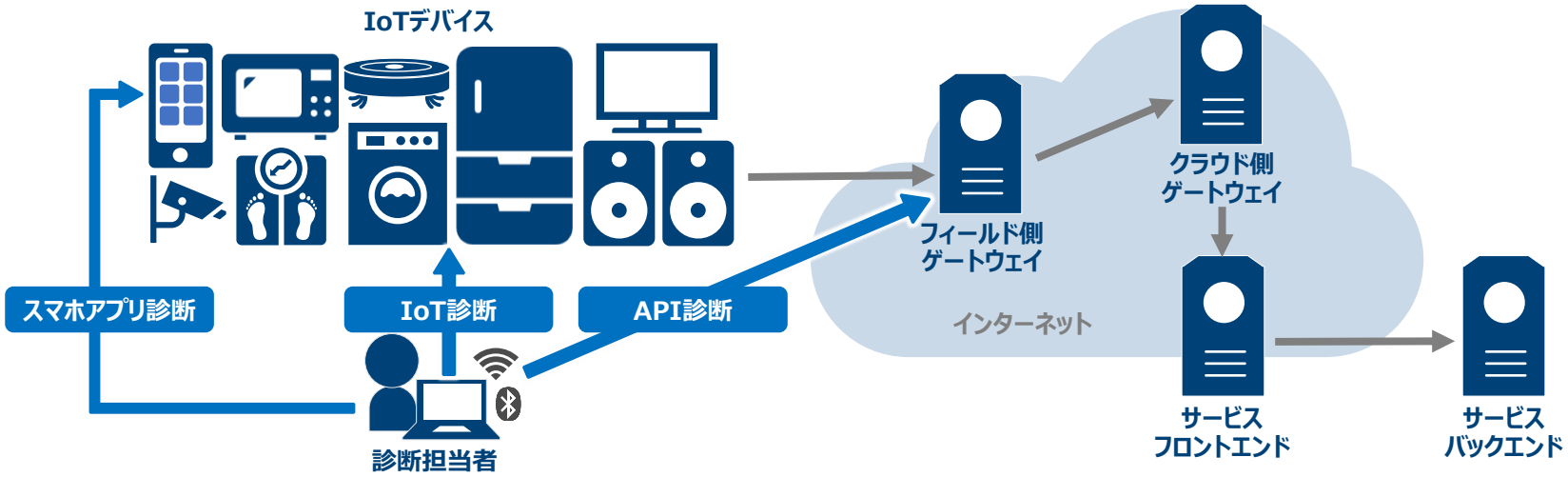
年間50システム以上のスマホアプリ診断を実施しています。以下は弊社診断事例の一部です。

| 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 |

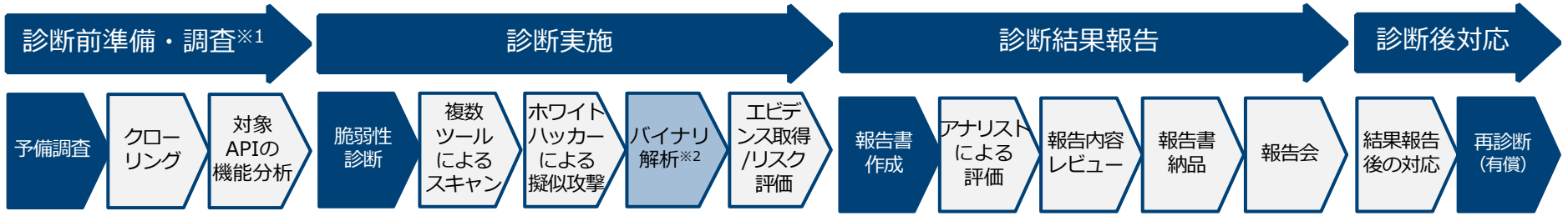
# IoT脆弱性診断―SQAT® for IoT：概要

対象の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、攻撃者にとって有益となる「不正操作」「情報の窃取」「踏み台化」が可能であるかを診断します。 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




※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―SQAT® for IoT：検査項目

IoT脆弱性診断の検査項目概要です。

| 診断項目 | 主な例 | | |
|---|---|---|---|
| インターフェース | Webインタフェース（XSS）<br>Webインタフェース（SQLi）<br>Webインタフェース（CMDi） | Webインタフェース（CSRF）<br>パラメータ推測<br>例外処理に関する問題 | クラウドインタフェースの制御<br>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<br>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<br>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 |

スマホアプリ脆弱性診断（Android、iOS）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）<br>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）<br>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）<br>データ改竄による不正行為（チート・課金回避）<br>ログへの重要情報の出力（個人情報・ID/パスワード）<br>パーミッションの設定不備*<br>SDカードへの機密情報の出力* |
| バイナリ診断<br>※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*<br>WebView関連の問題点の有無<br>難読化・耐タンパー性の確認<br>プロトコルの解析（HTTP以外）<br>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

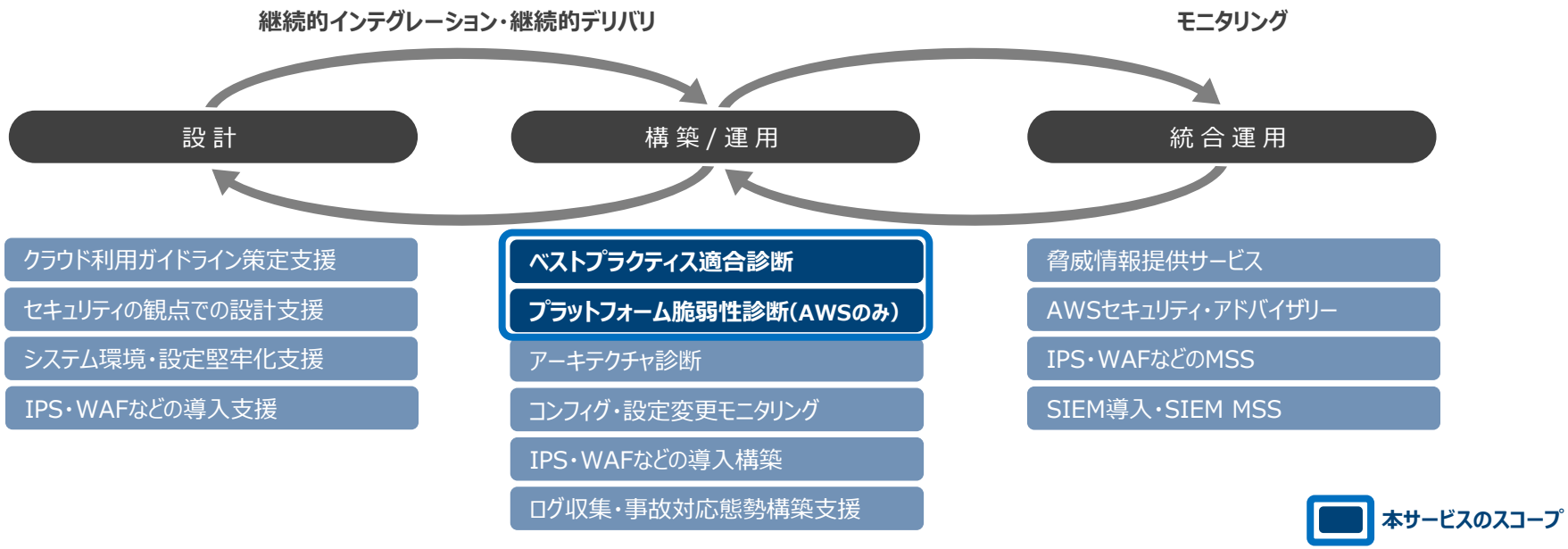
API診断の検査項目概要です。

| 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<br>SQLインジェクション<br>コマンドインジェクション<br>パスマニピュレーション | パラメータ推測<br>例外処理に関する問題<br>オープンリダイレクト<br>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<br>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<br>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<br>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<br>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：概要

クラウド利用の不安を払拭するため、ベストプラクティスに基づく適切な設定になっているか、各パブリッククラウド環境に特化したベンチマークは指標に基づき、専門家の知見を活かした独自の観点で評価を行い、対策方法をご提供します。

## サービスのスコープ




## 診断の流れ

# クラウドセキュリティ設定診断：検査項目

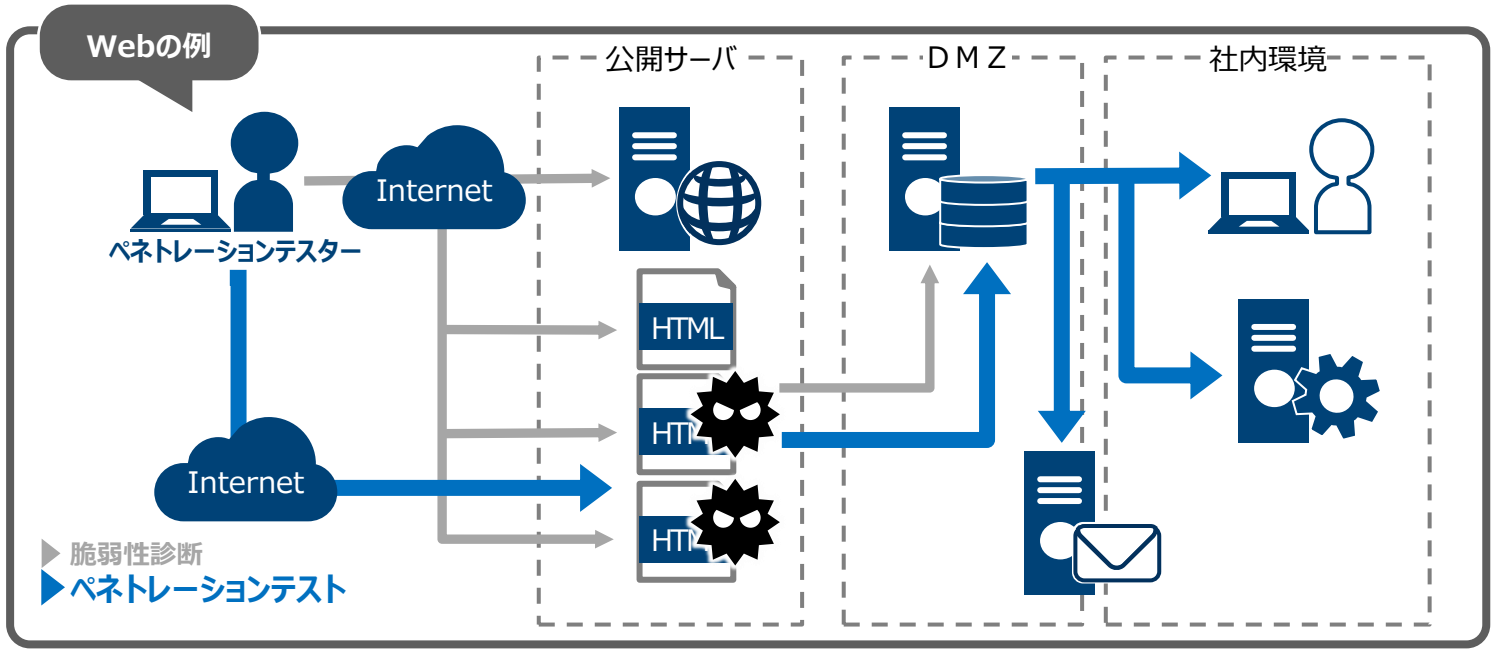
各パブリッククラウドにおける診断項目概要です。

| 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<br>• ロギング<br>• モニタリング | • ネットワーキング<br>• 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<br>• ID/アクセス管理<br>• 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<br>• 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<br>• 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<br>• 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<br>• ロギング<br>• モニタリング<br>• ネットワーキング | • 仮想マシン<br>• ストレージ<br>• データベース<br>• 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<br>• ロギング<br>• モニタリング<br>• ネットワーキング | • 仮想マシン<br>• ストレージ<br>• データベース<br>• 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<br>• ロギング<br>• モニタリング | • ネットワーキング<br>• ストレージ<br>• 資産管理 |

# ペネトレーションテスト：概要

事前の綿密な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仕掛け、システムの堅牢性を確認する検査です。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・深刻度の把握等に役立ちます。

## サービスイメージ



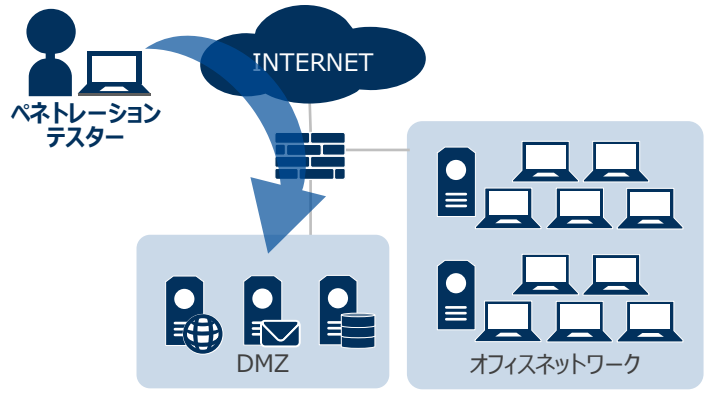

## ペネトレーションテストの流れ

| 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 |

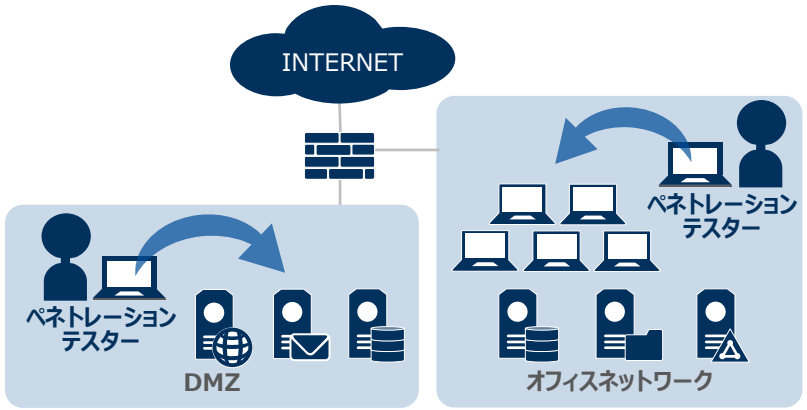
# ペネトレーションテスト：シナリオ設計

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。

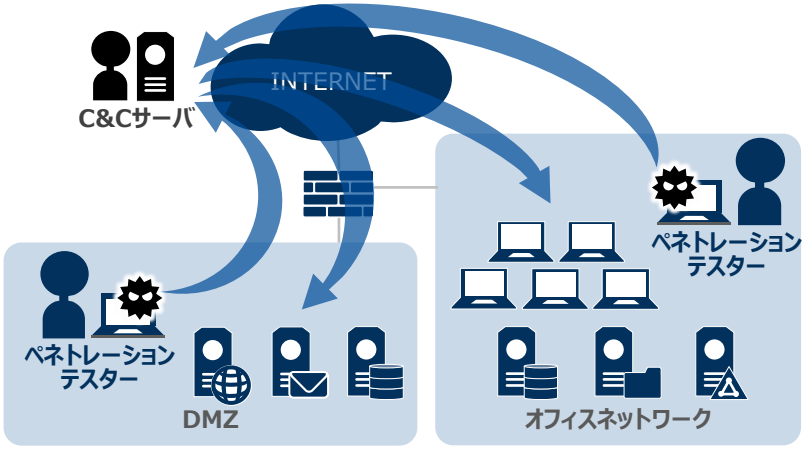
## 例1：リモートによるDMZ環境への侵入



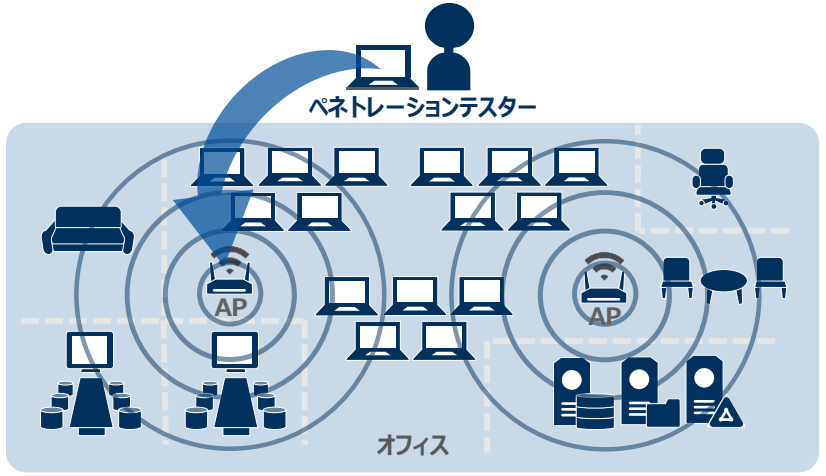

## 例2：オンサイトでの侵入




## 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



# ランサムウェア対策総点検：概要

規模の大小問わず、日本のあらゆる業種が被害を受けているランサムウェア攻撃に対し、3つのサービスを組み合わせることにより、「今、そこにあるリスク」を明確にして、攻撃耐性および攻撃を受けた場合の被害範囲を把握します。

## サービスメニュー

ランサムウェアに感染したら
内部ネットワークへの影響は
実際どうなるの？

### ランサムウェア感染リスク可視化サービス

お客様のPCで弊社がご用意した擬似ランサムウェアを実行していただき、感染した状態をシミュレート。
擬似感染したPCからどのような情報が抜き取られるのか、また、接続されている社内ネットワークのリスクはどれほどか、影響度合いを可視化するサービスです。

サブドメイン乗っ取りの
被害が多発しているって
聞いたけど…

### サブドメイン乗っ取り対策サービス

一時的に使用するために取得したサブドメインがすでに使用されていないのにそのまま放置されていると、攻撃者に乗っ取られて罠サイト等に悪用される危険があります。
Webサイト全体をスキャンすることで、サブドメインテイクオーバーの危険をいち早く察知します。

ランサムウェアに感染したら
外部に対して影響が出る
可能性がある？

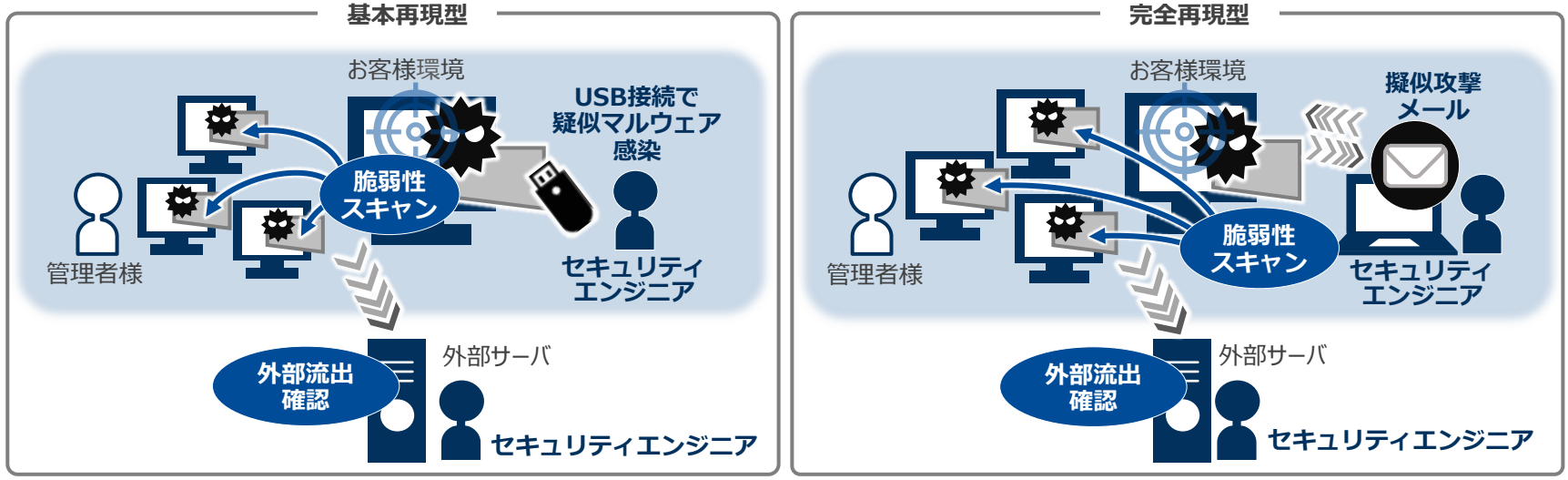
### ネットワークスキャンサービス

指定されたネットワーク全体を漏れなくスキャンし、オープンポートやIPアドレスをすべてチェック。
ネットワーク内のデータが外部に出やすい状態になっていないか、管理者が把握していない抜け穴や裏口、シャドーITが存在していないか、確認します。

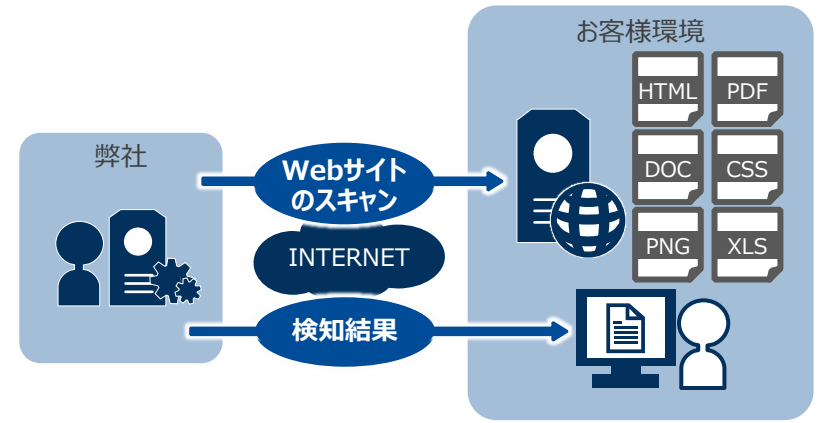
# ランサムウェア対策総点検：サービスイメージ

ランサムウェア対策総点検の各サービスのイメージです。

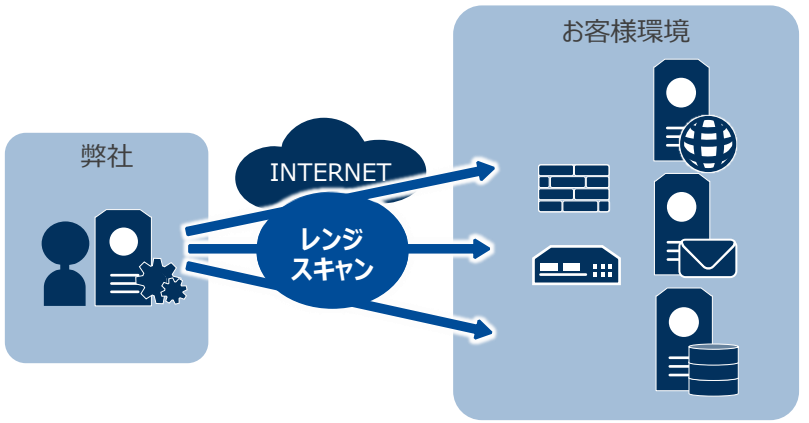
## ランサムウェア感染リスク可視化サービス




## サブドメイン乗っ取り対策サービス




## ネットワークスキャンサービス



# ハイブリッド診断―SQAT® GlassBox：概要

「ソースコード診断」と「Webアプリケーション脆弱性診断」をワンストップでご提供します。前者ではシステムの内部構造に着目し、ソースコードレベルでセキュリティ上の問題点を検出し、後者ではシステムの外部から攻撃者視点でセキュリティ上の問題点を検出します。

## サービスイメージ

### ホワイトボックステスト

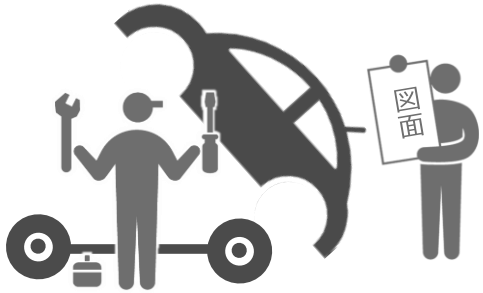
**システムの内部構造に着目して機能や動作を検証**

**開発工程で例えると、プログラム・詳細設計書レベルで評価を行う「単体テスト」**

**Webアプリケーションの診断を車の検査に例えると…**

**ソースコード診断**

解体したり、設計図を見たりして、車を構成する個々の部品や部品同士の連携、仕組み等を検査




### ブラックボックステスト

**システムの内部構造とは無関係に外部から見た機能や動画を検証**

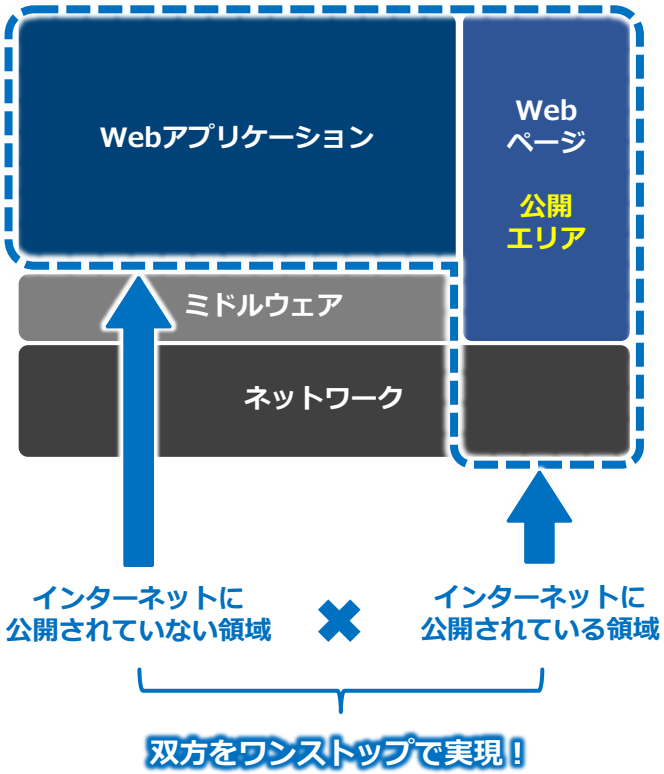
**開発工程で例えると、仕様・機能設計書レベルで評価を行う「総合テスト」**

**システム脆弱性診断**

解体せずに、車内外の見えている部分や想定される動作等に関する検査

# ハイブリッド診断―SQAT® GlassBox：診断イメージと効果

## 診断イメージ




## 実施による効果

### 「プロアクティブ」なセキュリティ対策

導入・変更・アップグレード時ほか継続的な診断実施により、システム内で見逃されてきた脆弱性や、開発で使用されるテクノロジーにおける新たに脆弱性等を、問題が顕在化する前に把握・対処可能になります

### 「コンプライアンス」実現の一助

企業のセキュリティポリシーや業界のセキュリティ基準を遵守していないシステムを特定できるため、コンプライアンス向上の一助となります

### 意思決定スピード向上

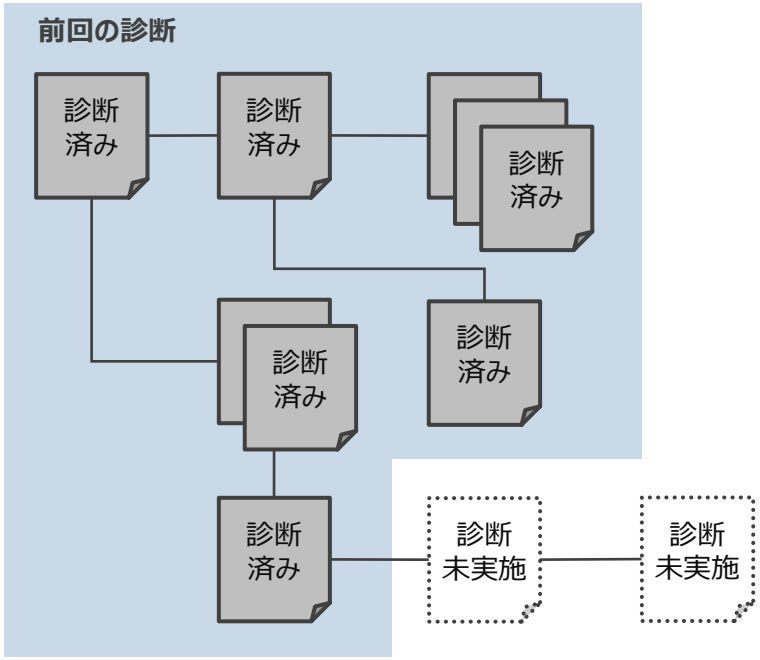
外部からの脆弱性診断とソースコード診断の併用により、限られた期間で効果的に問題部位を特定できるため、サービスの継続・改修に関する意思決定のスピードを高められます

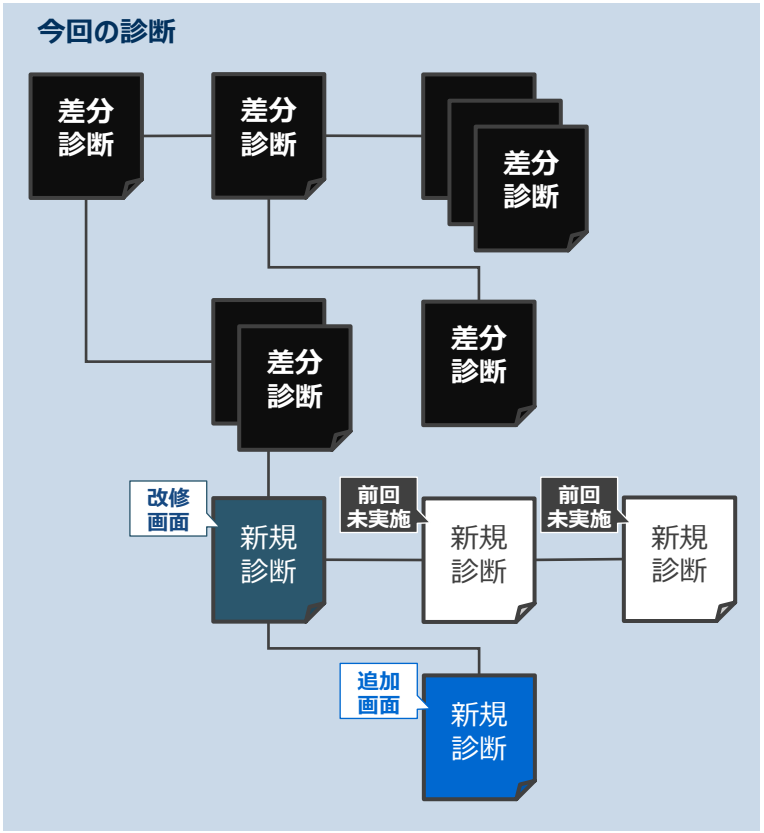
# 差分診断：概要

前回受診時以降に追加/更新された脆弱性検査シグネチャを主軸とした検査を実施することにより、診断期間の短縮と低コスト化実現するサービスです。

前回検出された脆弱性は再診断でリスクを再評価 します。

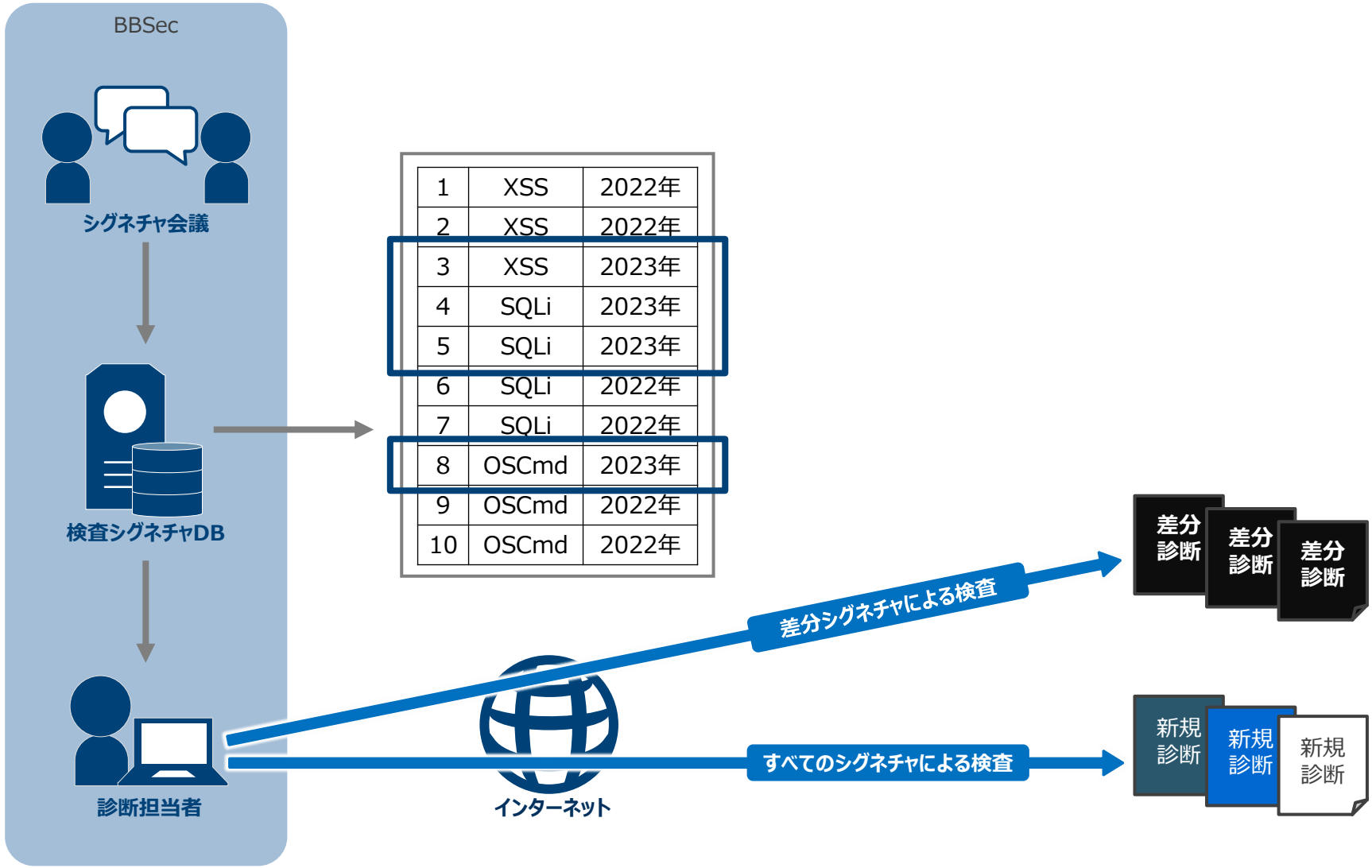
## 差分診断対象の考え方



# 差分診断：検査方法

定期的に実施しております検査シグネチャの更新を受けて、差分診断を実施します。検査方法は以下のとおりとなります。




| | | |
|---|---|---|
| 1 | XSS | 2022年 |
| 2 | XSS | 2022年 |
| 3 | XSS | 2023年 |
| 4 | SQLi | 2023年 |
| 5 | SQLi | 2023年 |
| 6 | SQLi | 2022年 |
| 7 | SQLi | 2022年 |
| 8 | OSCmd | 2023年 |
| 9 | OSCmd | 2022年 |
| 10 | OSCmd | 2022年 |

# 自動診断—Cracker Probing-Eyes®

定期的な脆弱性診断により、その時点でのリスクを最小化することは極めて重要です。次の脆弱性診断実施までの間に発生する外的変化にできるだけ早く気づき、いち早く対応できるよう、インターネットを介して高頻度で気軽に実施可能な自動診断ツールを提供しております。



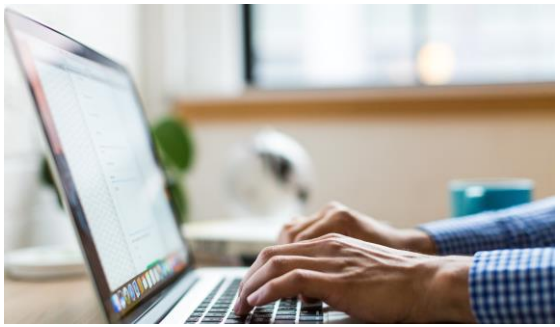
## QUALITY

### 最新のセキュリティ情報に基づく脆弱性診断

手動診断サービスと同様、米国国家安全保障局（NSA）、米コンピュータセキュリティ研究所（CSI）、米連邦捜査局（FBI）、SANS等世界的なセキュリティ基準をベースに弊社独自基準を設けた、信頼性が高く、最新動向を反映した診断内容です。

## REPORT

### 定点観測にも活用可能なわかりやすいレポート



発見された脆弱性を緊急度毎に色分けし、グラフで毎日報告します。新しい攻撃パターンが発見された時の影響や対策実施後の効果などが一目でわかります。

また、緊急性の高いもの（緊急および重大以上）については、診断終了時にメールでご連絡いたします。

## CONVENIENCE

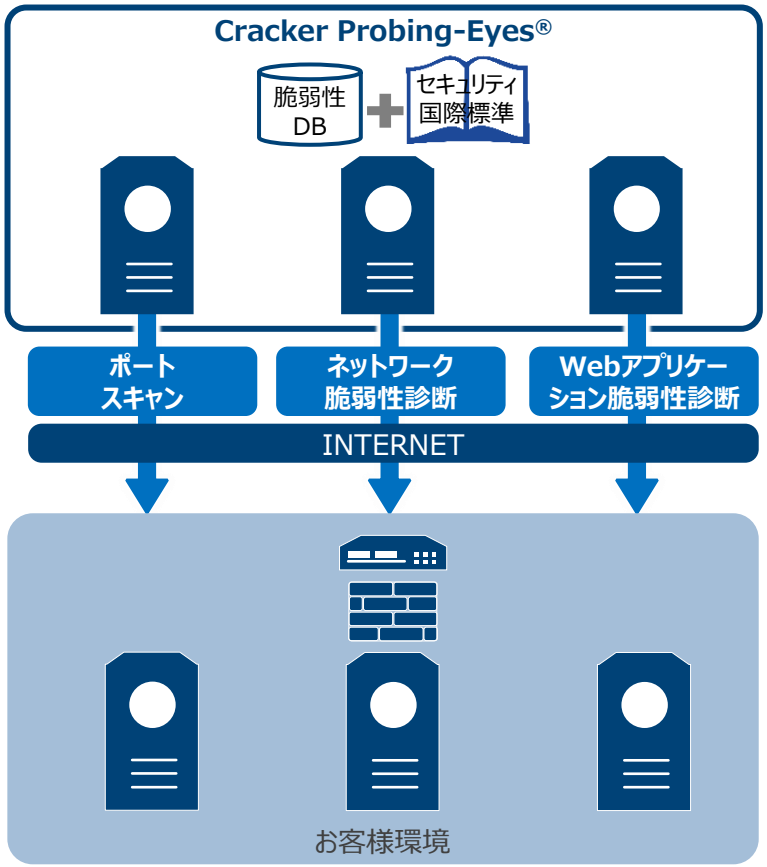
### 導入・設定・操作が簡単ですぐに使用可能

長年の経験をもとに利用者の利便性を考慮したツールです。インターネット越しに指定の頻度で診断や検査を実施するだけで済み、お客様のシステムの設定変更や新たな設備投資は不要です。ツール開発チームによるサポートも提供しております。

# デイリー自動脆弱性診断―Cracker Probing-Eyes®：概要

1日1回、インターネット越しにお客様サイトの脆弱性をチェックする自動診断サービスです。米国国家安全保障局（NSA）、米コンピュータセキュリティ研究所（CSI）、米連邦捜査局（FBI）、SANS等、世界トップクラスのセキュリティ組織により策定された規格や基準に準じた信頼性の高い診断プログラムは、お客様のシステムを健全に保つ上で、大きな効果を発揮します。

## サービスイメージ




## お客様側でのご準備

■ **診断可否確認作業（ご発注前）**

Web診断ご希望の場合、対象のHTML構成やリクエスト内容によっては診断不可となる場合がございますため、弊社エンジニアが事前に可否確認を実施させていただきます。

（1URLあたり2～3営業日程度要します）

■ **アクセス準備（ご発注後）**

- CPE診断元IPアドレスへのアクセス許可
- 認証情報・アカウントのご準備（フルスキャンをご希望の場合）

■ **申込書のご記入とご送付（ご発注後）**

- 診断希望時間の選択
- 以下はご契約が年間の場合のみ
- 診断完了、休止、障害、メンテナンスメールの通知先メールアドレスの確認
- CPEポータルへログインするためのアカウント用メールアドレス確認（メーリングリスト不可）
- ご希望診断周期の確認

# デイリー自動脆弱性診断―Cracker Probing-Eyes® ：検査項目

ネットワーク脆弱性診断の検査項目概要です。

| 診断項目 | 主な例 | |
|---|---|---|
| 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<br>メールサーバに関する調査<br>FTPに関する調査<br>RPCに関する調査<br>ファイル共有に関する調査 | SNMPに関する調査<br>SSHサーバに関する調査<br>データベースサーバに関する調査<br>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<br>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<br>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<br>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<br>各種ファイアウォール機器の既知の脆弱性 | その他各府ネットワーク機器の既知の脆弱性 |
| その他 | その他ホスト全体の調査 | |

WordPressに関する以下のような脆弱性のチェックが可能です。

| 診断項目 | 主な例 |
|---|---|
| WordPressの脆弱性検査 | 脆弱性が存在するバージョンのWordPressを使用していないかを検査します |
| WordPressのプラグインの脆弱性検査 | インストールされているプラグインに脆弱性がないか検査します※ |
| WordPressのテーマの脆弱性検査 | インストールされているテーマに脆弱性がないか検査します※ |

※ アクセス許可等によりコンテンツ/プラグインディレククトリにCracker Probing-Eyes®の診断元IPアドレスからアクセスできない場合、詳細な検査ができないため、あらかじめ許可設定をいただく必要があります。

# デイリー自動脆弱性診断：導入事例

Webアプリケーション開発・提供、自社製品・サービス紹介サイト、EC/コミュニティサイト等での定期診断でご利用いただいています。定期診断のほか、手軽にいち早くWebアプリケーションやネットワークの脆弱性を網羅的に発見できる診断ツールとして、都度利用でもご活用いただいています。

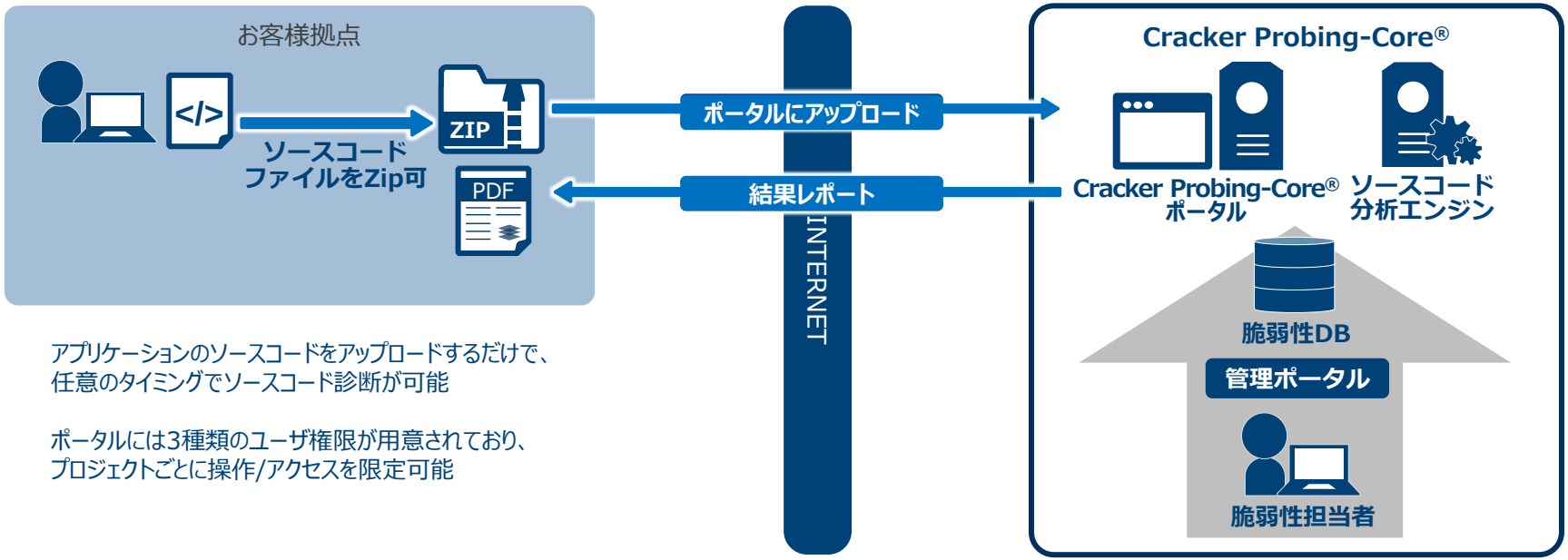
以下はご利用例の一部です。

| 業種 | 対象組織 | 規模 | 利用ケース |
|---|---|---|---|
| 卸売業、小売業 | ECサイト運営会社 | 約20サイト | オンラインショッピングサイトに対して、マニュアル診断後の定期的なスキャンに活用されています。 |
| 専門・技術サービス業 | ITソリューション会社 | 約10サイト | 開発したWEBサイトに対して、本サービス提供前の事前確認に活用されています。 |
| 製造業 | 鉄鋼会社 | 約30サイト | 鉄鋼関連の製品・商品情報を紹介するコーポレートサイトに対して、簡易的なスキャンに活用されています。 |
| 娯楽業 | ゲーム会社 | 約30サイト | ゲーム関連コンテンツのコミュニティサイトに対して、プラットフォームの定期的なスキャンに活用されています。 |
| 保険業 | 保険会社 | 約5サイト | 保険関連情報の会員向けサイトに対して、定期的なスキャンに活用されています。 |
| 不動産業 | 不動産会社 | 約20サイト | 不動産関連情報のコーポレートサイトに対して、簡易的なスキャンに活用されています。 |
| 娯楽業 | エンタテインメント会社 | 約20サイト | エンタテインメント情報を配信するコミュニティサイトに対して、定期的なスキャンに活用されています。 |

# ソースコード自動診断―Cracker Probing-Eyes® Core：概要

アプリケーションのソースコードを専用のポータルにその ままま圧縮/アップロードするだけで、ソースコードの脆弱性と品質の診断を行える自動分析ツールです。新たな設備投資不要でご利用いただけます。開発のあらゆるタイミングで品質分析が行えるため、開発の上流工程で、セキュリティに関する課題への対応が可能となり、手戻りによるコストや労力の削減を実現できます。

## サービスイメージ




アプリケーションのソースコードをアップロードするだけで、
任意のタイミングでソースコード診断が可能

ポータルには3種類のユーザ権限が用意されており、
プロジェクトごとに操作/アクセスを限定可能

## 診断の流れ

# ソースコード自動診断―Cracker Probing-Eyes® Core：対応言語・検出例

| 対応言語 | | | | |
|---|---|---|---|---|
| JAVA | VB.NET | Python | PL/SQL | Kotlin |
| PHP | ASP | Perl | Groovy | 等 |
| C/C++ | VB6 | JavaScript | Typescript | |
| C# | Ruby | VBScript | GO | |

| 検知する脆弱性の例 | | |
|---|---|---|
| SQL Injection | Unvalidated input | Hardcoded password |
| Session fixation | Cross-site request forgery | Dead Code |
| Cross-site scripting | URL redirection attack | Information exposure through log files |
| Session poisoning | HTTP splitting | Information exposure through an error message |
| Code injection | Dangerous files upload | Privacy Violation |
| Denial of Service (DoS) | Unhandled exceptions | Use of a Broken or Risky Cryptographic Algorithm |
| Buffer overflow | Unreleased resources | |
| Parameter tampering | Log forgery | |

※ 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

# PCI DSS準拠向けスキャン / ペネトレーションテスト対応

## サービス概要

| | PCI DSS v3.2対応 | PCI DSS v4.0対応 |
|---|---|---|
| 内部脆弱性スキャン | ○ | ○ |
| 外部脆弱性スキャン | ○* | ○* |
| 内部ペネトレーションテスト | ○ | ○ |
| 外部ペネトレーションテスト | ○ | ○ |
| セグメンテーションテスト | ○ | ○ |

* ASVスキャンについては応相談。

## PCI DSS v4.0対応

PCI DSS v4.0へのアップグレードに伴い、脆弱性診断に関して変更された主な要件は以下のとおりです。

| | |
|---|---|
| 脆弱性スキャンの頻度 | 脆弱性スキャンの頻度の記述が「四半期に一度」から「3ヵ月に1回」と変更されました。 |
| 認証スキャンの実施 | 脆弱性スキャンに関して、「認証スキャン」が必要となりました。 |
| ペネトレーションテストの内容 | ペネトレーションテストに関してのガイダンスが追加、修正され、ペネトレーションテストに求められる内容がより具体的になりました。 |

# インシデント対応

情報漏えいやサイバー攻撃などの重大インシデント発生時に、トップクラスのセキュリティコンサルタントを中心にセキュリティ事故調査対応チームを形成し、お客様をサポート。事故調査・現場対応・解析・報告・復旧支援・再構築支援まで、安全かつ的確にワンストップで対応いたします。

## ANYTIME

### セキュリティ事故緊急レスキュー隊が常時スタンバイ

いつ何時訪れるか想定できないITセキュリティインシデントに対応するため、24時間365日体制の受付窓口を準備しています。

状況を正確に把握して的確な対策を行うため、ハイスキルのセキュリティ技術者が初期対応の陣頭指揮にあたります。

## QUALITY

### サイバー攻撃復旧のスペシャリスト集団が対応

セキュリティ環境構築について豊富な実績と知識をもつ専門スタッフが在籍。

激しいサイバー攻撃にを受けてどう対策してよいかわからない、といった緊急事態にも様々な緊急の状況に対応してきた経験豊富な技術者が、丁寧に対応いたします。

## SUPPORT

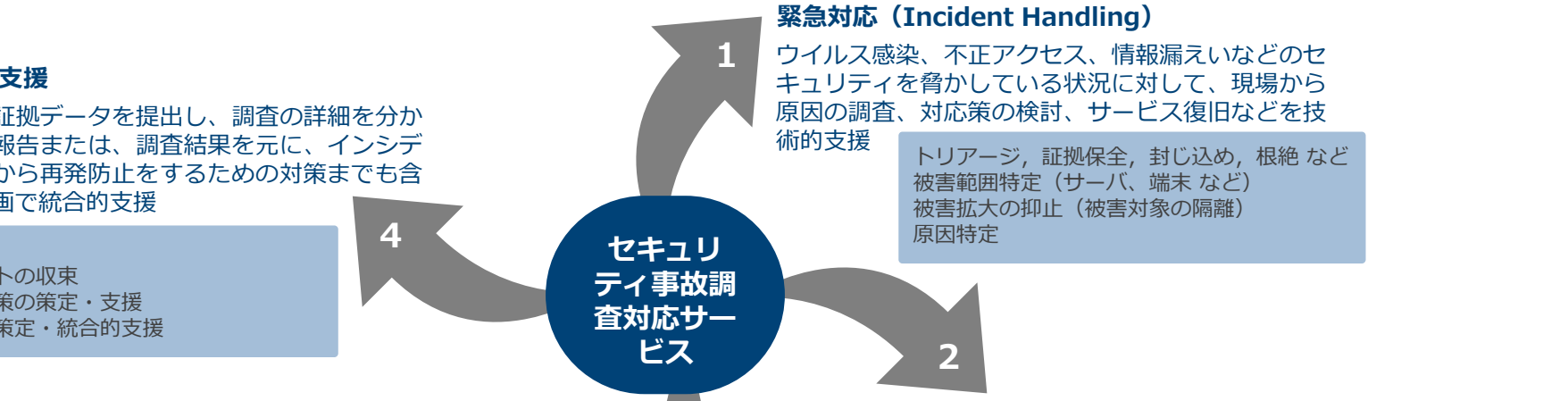
### 幅広い業界におけるシステムセキュリティ管理運営の実施

金融業、保険業、情報通信業などミッションクリティカルなシステムを運用する幅広い業界をサポート。

インシデント対応やデータ保全と並行して、お客様業務の停止期間を最小限に抑えるための施策を共に考え、ビジネス平常回復に向けたご協力をいたします。

# セキュリティ事故調査対応サービス：概要

セキュリティ事故調査対応サービスは、セキュリティ事故に対応する各種支援・調査をワンストップでご提供するサービスです。お客様からのご相談に基づき、初期のヒアリングを行った後、NDA締結後にヒアリングとデータ保全・収集を行い、解析・分析などの調査を行った後に、報告、復旧支援などを行います。




**緊急対応（Incident Handling）**

ウイルス感染、不正アクセス、情報漏えいなどのセキュリティを脅かしている状況に対して、現場から原因の調査、対応策の検討、サービス復旧などを技術的支援

トリアージ，証拠保全，封じ込め，根絶 など
被害範囲特定（サーバ、端末 など）
被害拡大の抑止（被害対象の隔離）
原因特定

**調査対応（Digital Forensics Investigation）**

不正アクセスや機密情報漏洩などのサイバーセキュリティインシデントにおける原因究明手段として、PCやサーバなどの記録媒体やネットワーク機器のログファイルなどを分析し、その証拠を見つけ出す技術的支援

調査対象データ保全
調査対象データ抽出
調査対象データ解析
解析したデータに対する詳細分析

**脅威ハンティング（Threat Hunting）**

調査対象の範囲を詰めたうえで、ネットワーク環境に侵入の兆候または痕跡があるかを調査し、攻撃の封じ込めと根絶を実施、サイバー攻撃を受ける時間や影響を最小限に抑える

特定した範囲内（数百/千台）の侵入・攻撃有無特定
定期的な検査（シナリオ利用）・侵入・攻撃検知
短期間で証拠収集
リモートで悪性ファイル・プロセスを操作（中止、削除など）

**報告・復旧支援**

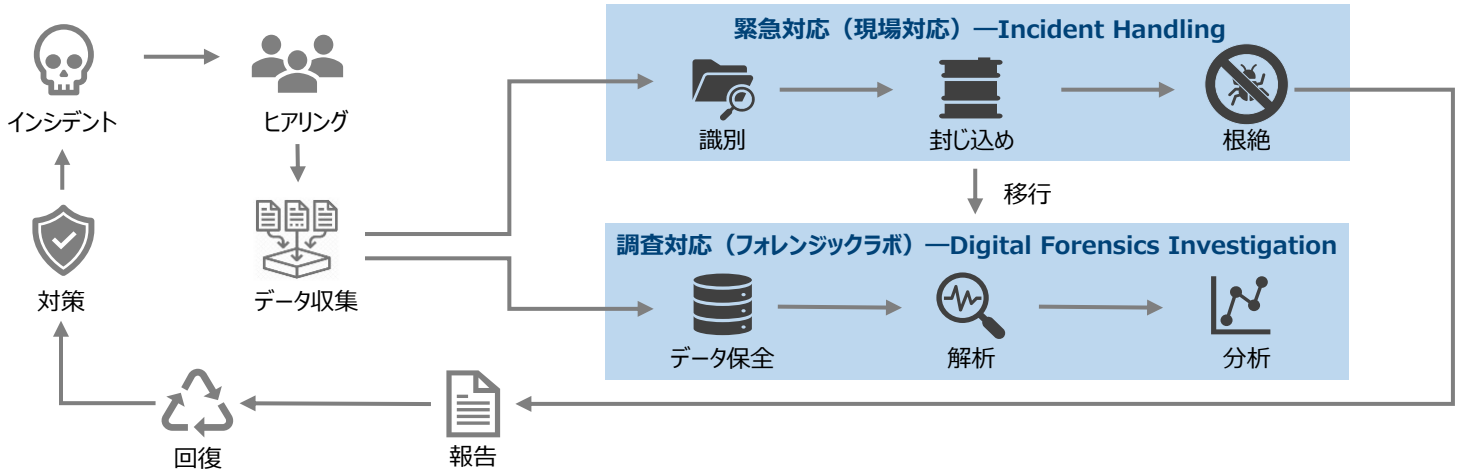
結果報告、証拠データを提出し、調査の詳細を分かりやすくご報告または、調査結果を元に、インシデントの収束から再発防止をするための対策までも含めた復旧計画で統合的支援

結果報告
インシデントの収束
再発防止対策の策定・支援
復旧計画の策定・統合的支援

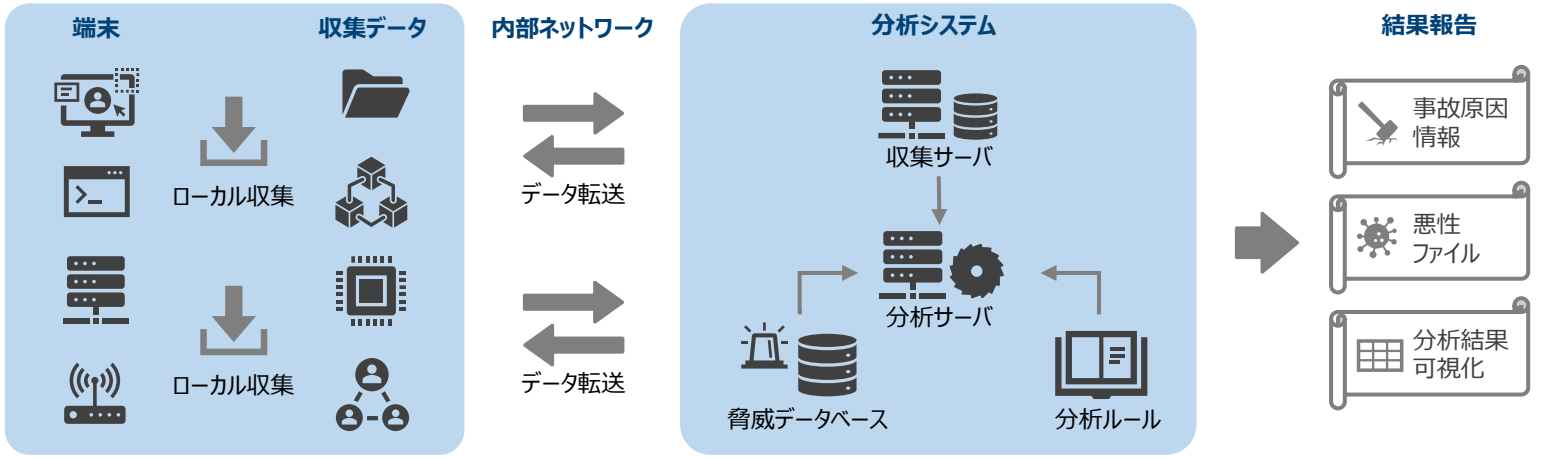
**デジタルフォレンジックチーム**
**セキュリティコンサルタント**
**セキュリティオペレーションセンター**
**セキュリティエンジニア**

# セキュリティ事故調査対応サービス：サービスの流れ

## 緊急対応サービス × 調査対応サービス




## 脅威ハンティングサービス



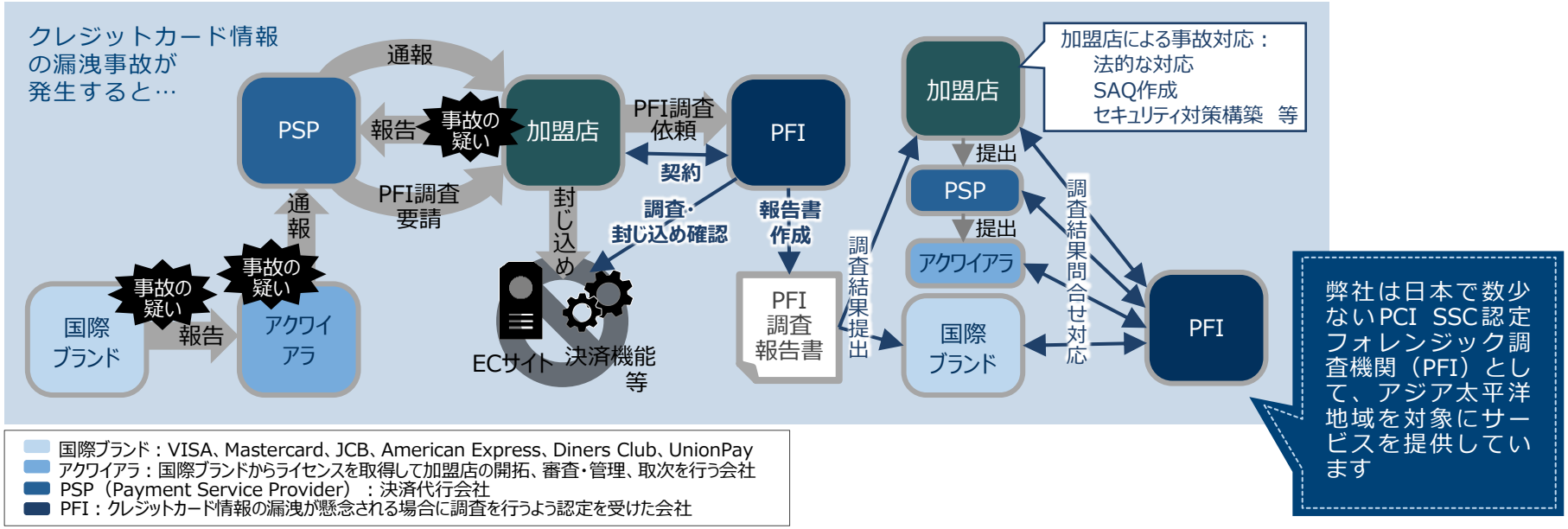

- 専用エージェント設置
- 収集ルール設定
- スポット/恒久
- 動的なデータ収集

- 大規模データ収集および保全
- 分析・フィルタールール設定
- APT、未知攻撃検知
- セキュリティ監視サービス

- 監視コンソール
- 分析結果報告
- リモート管理

# クレジットカード情報漏えいフォレンジック調査サービス：概要

クレジットカード情報の漏えい事故が発生した場合、その調査はPCI SSC が認定したPFI によって行われることが必須となっています。BBSecはPFIの認定を受けたフォレンジック調査機関として、クレジットカード情報漏えい事故の調査サービスを提供しています。




## PFI調査の目的

- **クレジットカード情報漏洩事故の調査**
  **原因・侵入経路・被害範囲を突き止める**
- **危険の封じ込め**
  **対象ECサイトの安全性を確認する**

## PFI調査に要する期間

**約５週間（調査開始から報告書の提出まで）**

※ 証拠入手状況や調査対象の変更等により大幅に延長となるケースもあります

# クレジットカード情報漏えいフォレンジック調査サービス：流れと特長

## サービスの流れ

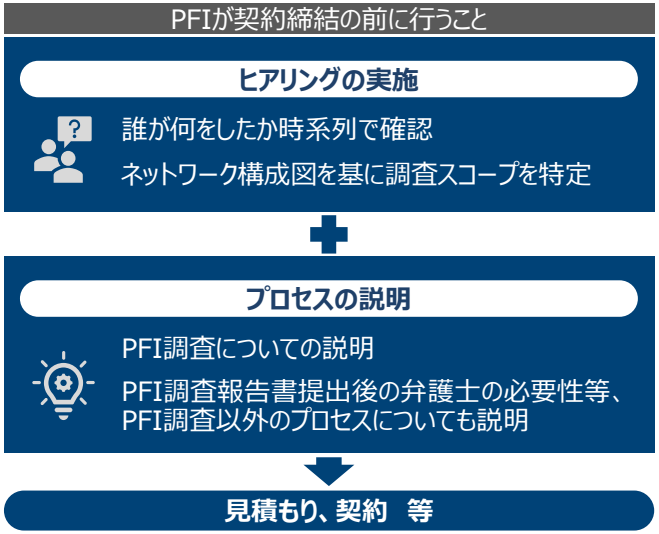
**01** 調査依頼（緊急コンタクトセンターにて24時間365日受付）

**02** 被害状況確認

**03** 原因調査・特定

**04** 報告

**05** 再発防止支援（別途有償）




## サービスの特長

デジタルフォレンジック関連のサービスで培った経験を持つスペシャリストが、PCI SSCの基準に則った調査・報告を行うことで、お客様のインシデント対応を支援いたします。

また、クレジットカード情報漏えいフォレンジック調査サービスの調査・報告完了後に以下のような再発防止策を支援することが可能です。

- PCI DSSの要件を踏まえた再発防止策や改善策などのコンサルティング
- インシデントの改善策などを踏まえた上でのPCI DSSの準拠支援
- 暗号化決済ソリューションのセキュリティ基準・PCI P2PEのコンサルティング、準拠支援
- クレジットカードの不正利用を防止する3Dセキュアのセキュリティ基準・PCI 3DSのコンサルティング、準拠支援