Secure Innovation

沖縄から日本全国、アジア、そして世界へ

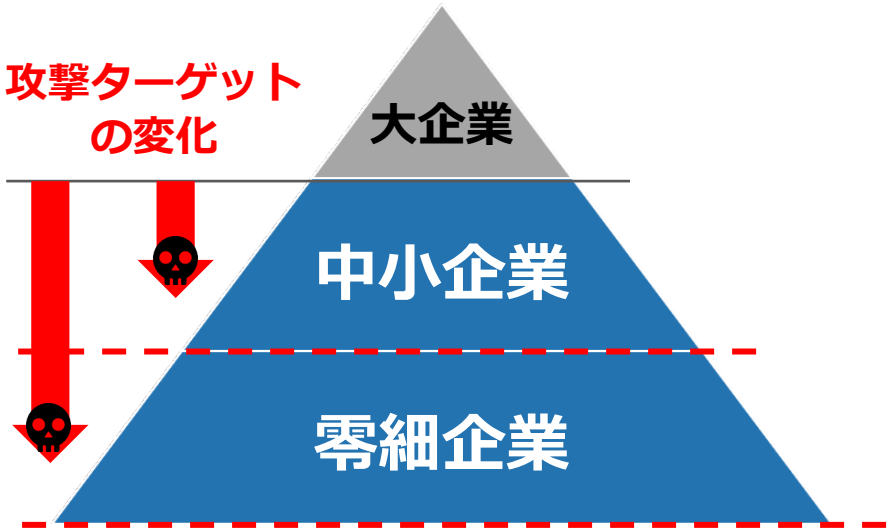
セキュリティ
脆弱性診断サービス

セキュリティインシデントの傾向①

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

サイバー攻撃対象の変化

サイバー攻撃の**ターゲット**が
大企業に留まらず、
中小・零細企業にまで
シフトしてきている



対象変化の理由①　大企業に比べて、対策が充分ではない

攻撃者側から見たときに、リスクや、投下リソースが少ないわりに、
実入り（リターン）が大きい。

対象変化の理由②　大企業へ繋がる情報を持っている

大企業の取引情報や特許に関わる内部データ
担当者情報（標的型攻撃のネタ）
踏み台にされる（オンライン連携・サプライチェーン）

セキュリティインシデントの傾向②

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

2026年　情報セキュリティ１０大脅威（IPA発表）

順位	情報セキュリティ10大脅威　※組織	昨年順位
1 位	ランサム攻撃による被害	1 位
2 位	サプライチェーンや委託先を狙った攻撃	2 位
3 位	AI の利用をめぐるサイバーリスク	初
4 位	システムの脆弱性を悪用した攻撃	3 位
5 位	機密情報を狙った標的型攻撃	5 位
6 位	地政学的リスクに起因するサイバー攻撃（情報戦を含む）	7 位
7 位	内部不正による情報漏えい等	4 位
8 位	リモートワーク等の環境や仕組みを狙った攻撃	6 位
9 位	DDoS 攻撃（分散型サービス妨害攻撃）	8 位
10 位	ビジネスメール詐欺	9 位

独立行政法人 情報処理推進機構 （IPA）「情報セキュリティ10大脅威 2026」より抜粋
https://www.ipa.go.jp/security/10threats/10threats2026.html

外部からの攻撃が複数ランクイン

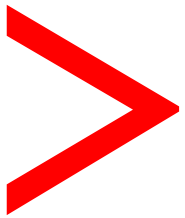
セキュリティインシデントの傾向③

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

サイバー世界の中では、攻撃者が圧倒的に優位

攻撃者

- 世界中からインターネット経由で、攻撃姿も見えず、抑制も効かない
- 攻撃対象が不特定多数で、攻撃手法も様々
- 分業化が進み、様々なツールやサービスが容易に利用できる環境



防御者

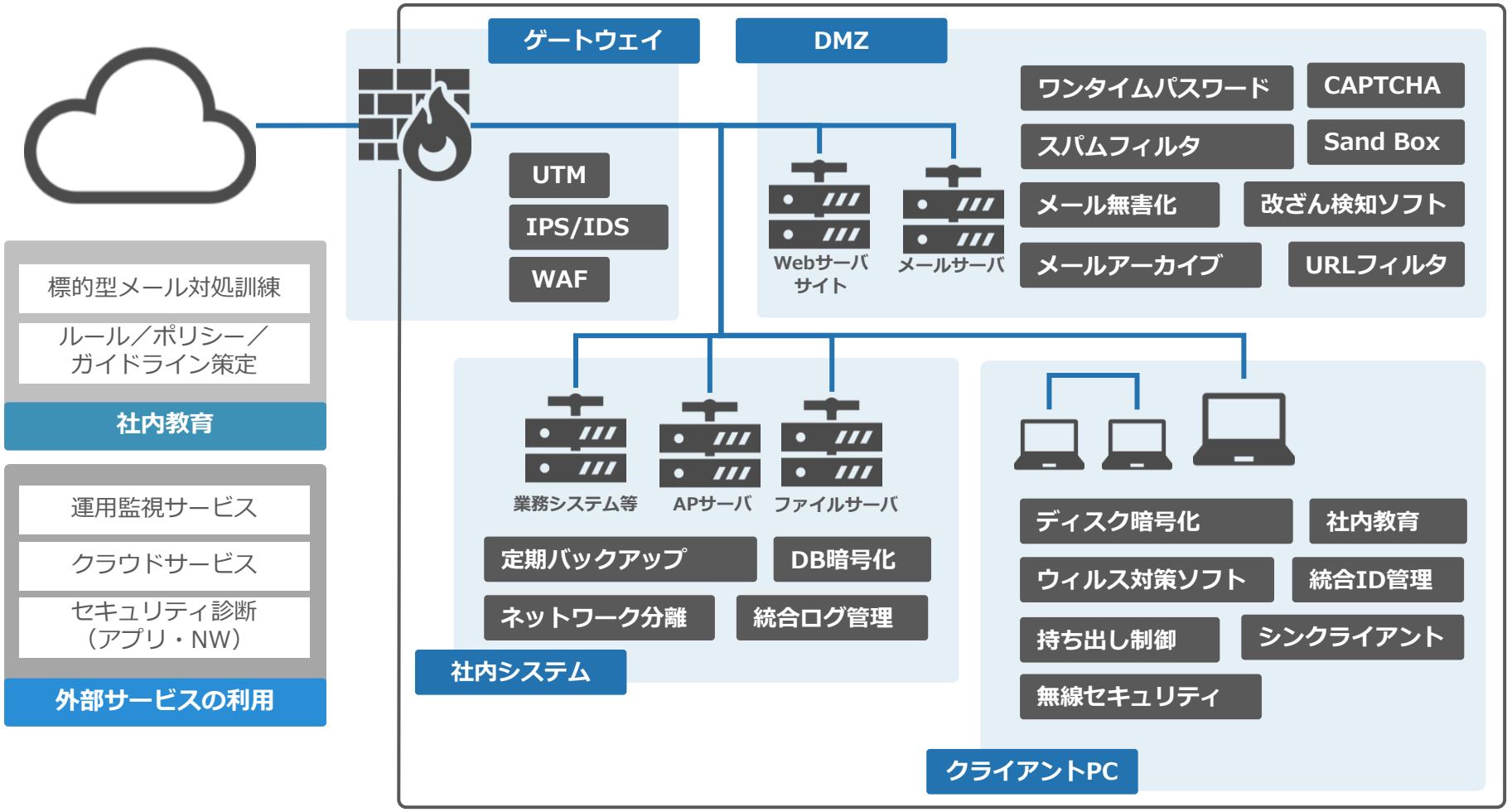
- どこから攻撃されるのか、どういう手口で攻撃されるのか、が不明で、対応コストが膨大
- 防御側での効率化や分業は、まだまだ発展途上である
- 自社への被害の可能性を軽視している

この先も攻撃者の優位性は、揺るがない可能性が高い

多種多様なセキュリティ対策

各レイヤー毎にできる対策は多種多様。
しかし、この対策で**万全(完璧)というものは一つとして存在しない**のが現状・・・

そこで、大事なキーワードは、「多層防御」

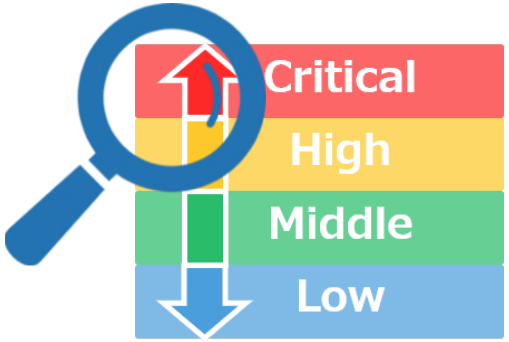


「はじめの一歩」としての セキュリティ診断

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

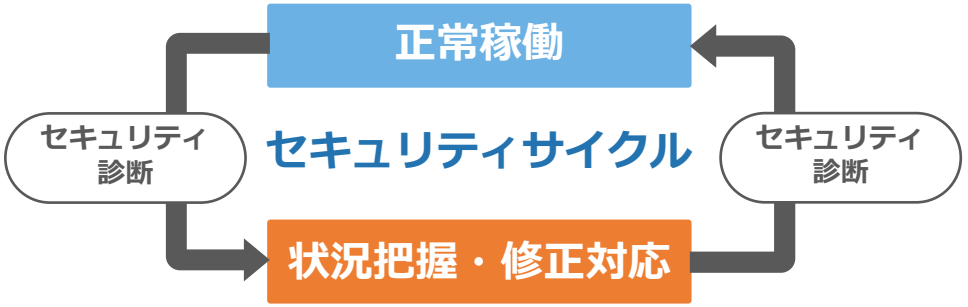
毎日、数十万種類のマルウェアが発見され、新たな脆弱性が生まれており、
企業内のシステムは、日々新たな脅威に晒されている状況です。
多層防御という流れにおいても、**どの対策を優先すべきか？** が永遠のテーマです。
そこで、適切な対策を講じるためにも、**定期的に現在のセキュリティリスクを認識すること**が、**セキュリティ対策の「はじめの一歩」**です。

セキュリティリスクの把握



セキュリティリスクの有無、脆弱性レベルを把握し、
適切な対処だけでなく、効果的な予算配分に繋げる

セキュリティサイクルの実現



日々、新しい脆弱性に晒されている状況では、
診断→状況把握・対処のサイクルは必要不可欠。
リリース前だけでなく、リリース後の継続も推奨。

セキュリティリスクの把握を継続的に行うことが重要

診断メニュー

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

Webアプリケーション診断

・ハイブリッド診断<ツール+手動>
・リモート（オンサイトも可能）

経験豊かなセキュリティ技術者がWebサーバ上で稼動するアプリケーションに対し、 外部から擬似攻撃を行い、Web アプリケーションに潜む脆弱性や潜在要因を診断します。
これによりWebサイトの機密情報漏洩、なりすまし、ネットショップサイトの価格改ざん、フィッシング等々の被害の危険性を洗い出すことができます。

特 徴

診断ツールは純国産のもので日本語(マルチバイト文字）への完全対応はもちろんのこと、日本国内におけるセキュリティの最新トレンドをも組み込んだ診断が可能。

プラットフォーム診断

・リモート（オンサイトも可能）

お客様のシステムを構成するサーバやファイヤーウォール等のネットワーク機器に対して、OSやアプリケーションに潜むセキュリティホール（弱点・脆弱性）が存在しないかどうかをネットワーク経由にて診断し、対応策を提示します。これにより不正アクセスやセキュリティ事故を拡大させる踏み台になってしまう等の危険性を洗い出すことができます。

特 徴

日々SOCを運営しているノウハウをベースにした高度なスキルを持つセキュリティエンジニアが診断を行うことでツール診断に散見する誤検知を省きながら、網羅性と正確性の高い診断を行います。

**ネイティブアプリ診断、およびIoT診断（欧州のRE指令・CRA、国内のJC-STARに基づいたテスト等）、車載セキュリティの脆弱性テストも別途メニューを用意しております。
担当までご相談ください。**

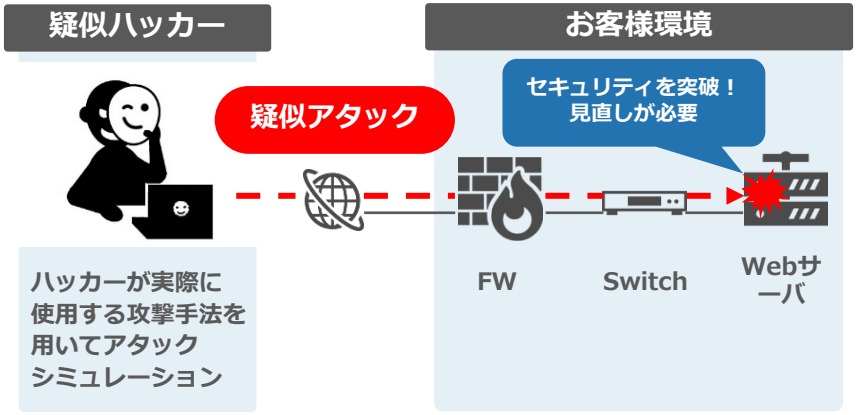
診断内容①

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

診断方法

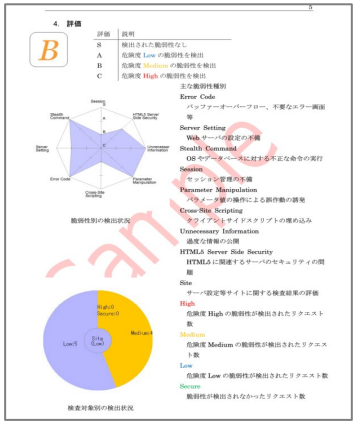
お客様環境に対してリモート接続をして疑似アタックを実施し、脆弱性の有無とその危険性レベルをチェック！
（オプションでオンサイト診断も可能ですので、ご相談ください。）

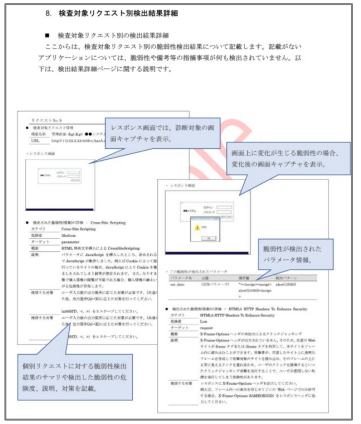
誤検知・過剰検出の多いツール診断のみのサービスとは違い、当社セキュリティエンジニアによって検出結果の確認・検証を実施することで 検知漏れや誤検出を最小化し、**信頼性の高い診断結果を提供**します。

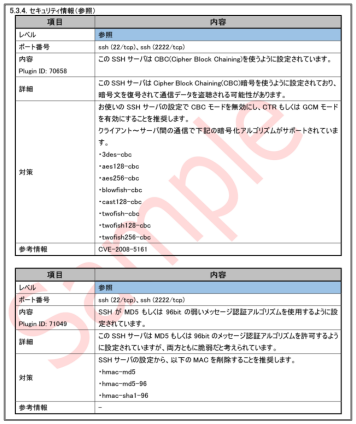


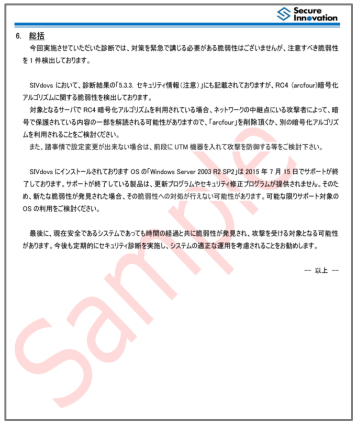
診断レポート

脆弱性の有無やレベルだけではなく、具体的な対処方法までも含め、実際に技術者の方が改善対応に繋げやすい内容をご報告します。









診断内容②

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

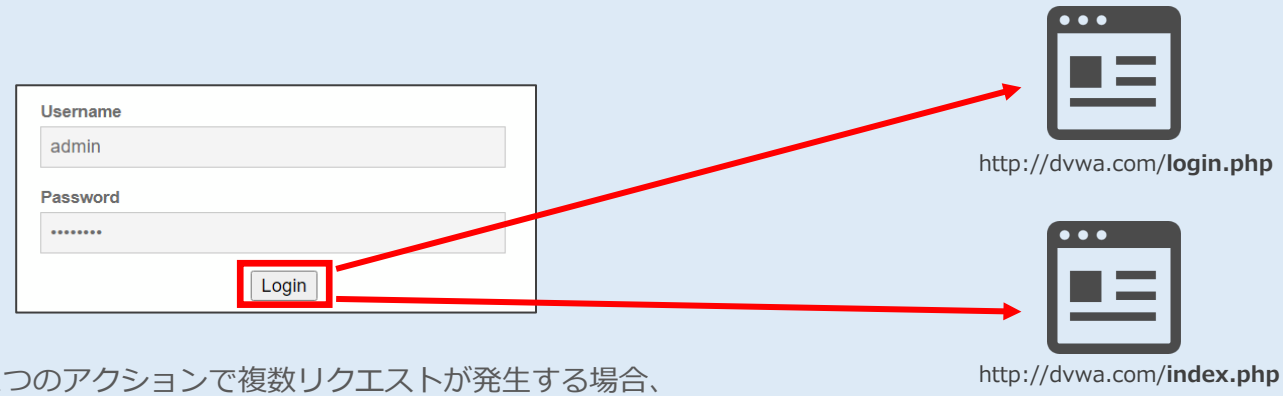
Webアプリケーション診断の対象カウント単位

Webアプリケーション診断における対象の単位として、実際にWebブラウザから対象のWebアプリケーションに対して発生するHTTPリクエスト数にてカウントしております。

リクエスト数によるカウントの特徴

実際に発生するHTTPリクエストをカウントすることで、診断対象の漏れが発生しにくくなります。非同期通信やシングルページアプリケーションなど、画面が変わらないようなWebアプリケーションで、診断対象から漏れてしまうようなことや対象が曖昧になることを防ぐことができます

例：ログインボタン押下時のアクション



※1つのアクションで複数リクエストが発生する場合、
2リクエストとしてカウント。

診断内容③

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

主な診断項目

Webアプリケーション診断

SQLインジェクション
OSコマンドインジェクション
パラメータ操作による脆弱性
クロスサイトスクリプティング
セキュア属性の無いCookie
不要なエラーコードの表示
バッファーオーバーフロー
クロスサイトリクエストフォージェリ
セッション管理に関する問題
プロトコルの不適切な適用
不要なエラーメッセージの表示
HTML5のクロスオリジン設定に関する問題
HTML5のレスポンスヘッダに関する問題
SandBox属性の無いインラインフレーム
Webサーバ設定ミスによるサーバ情報、アプリ情報の漏えい
Webサーバのディレクトリやファイルの不適切な公開設定
Webサーバの既知の脆弱性

プラットフォーム診断

バックドアが仕掛けられているかどうかのチェック
危険なCGIの検出、クロスサイトスクリプティングの可能性
DNS、メールサーバに関する脆弱性チェック
データベースに関する脆弱性チェック
Unixデフォルトアカウントのチェック
Dosを受け付けてしまう弱点の検査
FTPに関する脆弱性チェック
FireWallに関する脆弱性チェック
リモートからシェルが奪取できる可能性をチェック
他のカテゴリには含まれない脆弱性をチェック
一般的には利用されないソフトや機器のチェック
P2Pのファイル共有に関する脆弱性チェック
RPCに関する脆弱性チェック
特定のポートで稼働しているソフトのタイプを識別
ウェブサーバに関する脆弱性チェック
Windowsに関する脆弱性チェック
Windowsのユーザー管理に関する脆弱性チェック

代表的なセキュリティ団体・組織が掲げる診断項目や
最新の技術動向を加味した診断内容

診断内容④

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

PCIDSSに関する主な診断項目（オプション）

Webアプリケーション診断

- ユーザセッションが15分以上アイドルの場合、再認証を要求することを確認
- 無効な認証の試行が制限されていることを確認
- 無効なログオン試行回数20回以下でユーザアカウントをロックアウトするよう設定されていることを確認
- パスワード／パスフレーズが、最小レベルの複雑さを満たしていることを確認

プラットフォーム診断

- 内部IPアドレスやルーティング情報の開示を確認
- すべての既知のセキュリティ脆弱性を確認
- ベンダのデフォルトアカウントの使用有無を確認
- 不要なサービス、プロトコル、デーモンの存在を確認
- 安全でないサービス、プロトコル、デーモンの存在を確認
- すべての管理者アクセスに強力な暗号使用を確認
- 安全でない暗号の存在を確認
- 適用可能なセキュリティパッチが定期用されていることを確認
- すべての認証要素の読み取りができないことを確認
- 無効な認証の試行が制限されていることを確認
- すべてのリモートアクセスに対して多要素認証の有無を確認
- CDE内のシステムがスコープ外システムおよびネットワークから隔離されていることを確認（境界ペネトレーションテストの場合のみ実施）

標準の診断にプラスして
PCIDSS セキュリティガイドラインに準拠した診断項目を実施

診断内容⑤

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

主な診断項目

WordPress診断

- WordPressの脆弱性を確認
- プラグインの脆弱性を確認 ※
- テーマの脆弱性を確認 ※
- ユーザ情報を確認
- 不要な情報公開を確認
- XML-RPCのステータスを確認
- WP-Cronのステータスを確認

※プラグイン、テーマの総数が最大24項目まで診断可能

AWS設定診断

- IAMを確認
- ストレージを確認
- ロギングを確認
- モニタリングを確認
- ネットワーキングを確認

CISベンチマークが定めるAWSセキュリティベストプラクティスを準拠した診断内容

代表的なセキュリティ団体・組織が掲げる診断項目や
最新の技術動向を加味した診断内容

診断メニュー（ペネトレーションテスト）

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

ペネトレーションテスト

診断対象となるシステムの脆弱性を突かれた場合にどの程度の被害に繋がるかを確認・検証するための安全評価を行うサービスです。
検証シナリオ（ゴール設定）に対し、あらゆる経路から侵入を検討、疑似攻撃を実施し、弱点を発見していきます。

特徴

ペネトレーションテストは脆弱性スキャンに加えて実施され、スキャンで見つけた脆弱性や、設定ミス等の情報を利用するなど、攻撃者が実行する攻撃を試して結果を診断します。

当社のペネトレーションテストは、CEH（認定ホワイトハッカー)やCHFI（コンピュータ ハッキング フォレンジック調査員)等の高度なセキュリティ資格保持者により実施いたします。

テスト手法

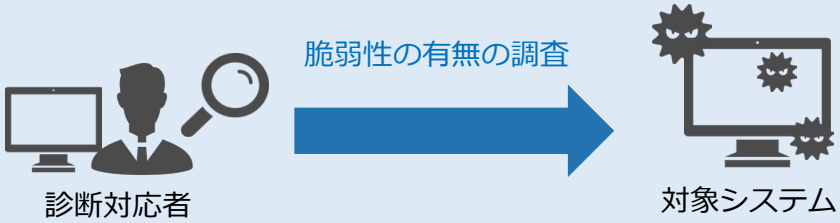
ペネトレーションテストでは、現実に行なわれる可能性のある悪意の攻撃を具体的に想定し、テストいたします。

	侵入糸口の調査	侵入糸口の見極め	侵入調査
概要	侵入糸口を探索するとともに、侵入に必要な情報を収集	侵入糸口に存在する脆弱性を判断し、複数の糸口から突破口を見極め	収集した情報を用いて、最も効率的な方法で突破口から侵入を試み、ターゲットへ接近
具体的内容	・スキャニングによる重点箇所の絞り込み ・情報収集（システムの既知脆弱性、パッチの適用状況、設定不備） など	・機微レベルや想定される被害レベルに応じた糸口の優先順位付け ・攻撃コードによる侵入可否の判断 など	・権限昇格 ・フィルタリング回避 ・パスワード解析 ・辞書攻撃 など

脆弱性診断と ペネトレーションテストの違い

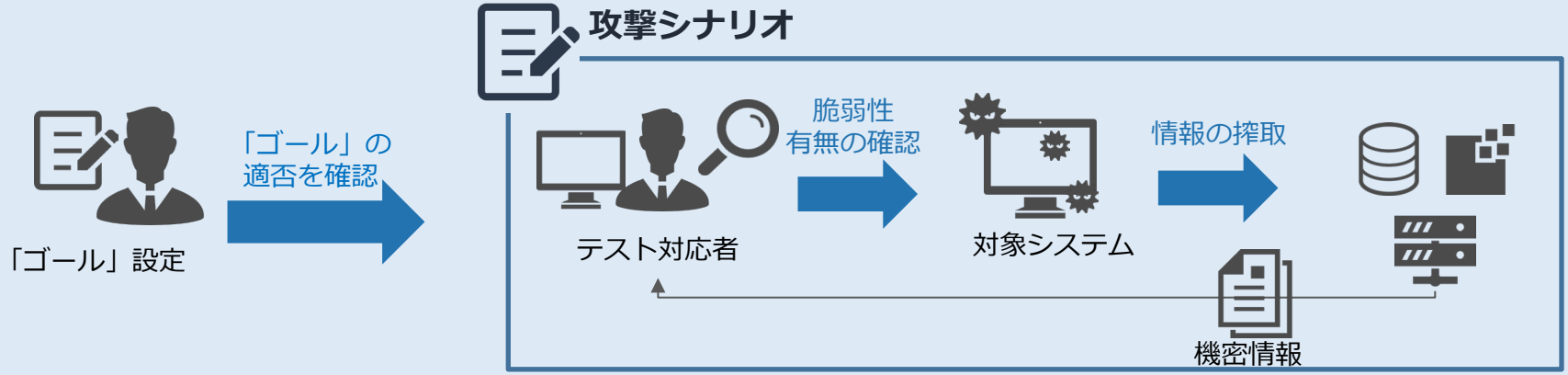
脆弱性診断
(Webアプリケーション診断
プラットフォーム診断等)

Webアプリケーションやネットワーク機器、OS、ミドルウェア等について不正にアクセスされるような脆弱性はないかどうか、
システム全体を網羅的に確認し、**脆弱性の有無**の調査が目的。



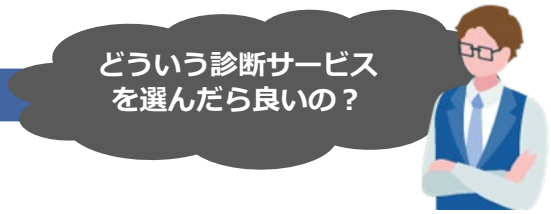
ペネトレーションテスト

機密情報窃取等の「ゴール」を設定し、現実的な攻撃シナリオを用いて、
「ゴール」を**満たせるか否か**(攻撃された際の実影響)の確認が目的。



当社のセキュリティ診断の特徴

Secure Innovation
沖縄から日本全国、アジア、そして世界へ



①経産省「情報セキュリティサービス基準」登録事業

経産省では、**「情報セキュリティサービス基準」**を策定しております。
この「情報セキュリティサービス基準」には、一定の技術要件及び品質管理要件を満たし、
品質の維持・向上に努めているかを審査されますが、**当社サービスはその審査をパスして登録されており**、
安心してご利用いただけるコストパフォーマンスに優れた診断サービスとなっております。

②Webアプリケーション診断の再診断が1回無料

是正対応の効果を確認していただくためにWebアプリケーション診断は**初回診断後の再診断を1回無料**でご提供いたします。

③良いとこ取りのハイブリッド診断　※Webアプリケーション診断のみ

診断にはツール診断と手動診断という区別がありますが、それぞれに長所短所が存在しています。
それぞれの長所の良いとこ取りのハイブリットな手法を採用しています。
使用する診断ツールも実績の豊富な高品質なものを使用し、**最新の技術動向・攻撃手法を加味**した形でWASCやOWASPといった
代表的なセキュリティ団体が掲げる脆弱性項目もカバーしています。

④高品質な診断レポート

脆弱性の有無やリスクレベルといった結果だけでなく、**対処方法までもがきちんと記載**され、
具体的な改善対応に繋げることが可能となるレポートを提供します。

⑤充実したアフターフォロー

診断後の質疑応答への対応もちろん、自社で**SOCを運営**しており、修正方法のコンサルティングや
セキュリティ製品の導入支援等、セキュリティ診断に留まらないその後の**脆弱性への対応支援**も可能です。

診断実績①

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

主な診断実績 （24年11月時点）

業種	実施内容
某国立大学（複数）	受験・入学手続きシステム
某私立大学（複数）	受験・入学手続きシステム
大手総合専門学校	資料請求受付＆応募者管理システム イベント申込＆申込者管理システム
大手出版社 （上場企業）	Webマガジン購入＆レンタルサイト
大手出版社 （上場企業）	日本語eラーニングサービスサイト
大手流通企業 （上場企業）	コーポレートサイト
大手流通企業 （上場企業）	ケータリング受付サイト
クレジットカード 会社（複数） ※PCI DSS準拠診断	社内システムおよび公開サイト （会員サイト含む）、社内ネットワーク
社会インフラ会社 （上場企業）	コーポレートサイトおよび公開 Webサイト（会員サイト含む）
通信回線会社 グループ	工事施工管理業務システム

業種	実施内容
大手不動産管理会社 （上場企業）	アセットマネジメントシステム
スポーツ系公益財団法人	某プロスポーツリーグWebサイト
人材情報サービス会社	学生向けリクルーティングサービス
大手コンサルティング ファーム	人事クラウドシステム
大手機器製造会社 （上場企業）	レシート自動データ化システム （ネイティブアプリ含む）
社会インフラ会社 （上場企業）	IoT機器管理システム
大手ディベロッパー （上場企業）	テナント管理システム
大手ディベロッパー （上場企業）	注文住宅受付Webサイト
大手旅行会社子会社 （複数）	商品紹介Webサイト
大手地図情報会社	社内及び公開NW

診断実績②

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

主な診断実績 （24年11月時点）

業種	実施内容
大手システムインテグレータ（上場企業）	ID決済プラットフォームシステム
某官公庁	補助制度電子申請システム
某航空会社	顧客向けECサイト
某公共交通会社	コーポレートサイト
大手食品会社（上場企業）	パートナー企業向け会員サイト
社会インフラ会社	Webサイトおよび取引先向けwebサイト
ソフトウェア開発会社	データ解析プラットフォーム
某自治体	自治体公式webサイト
大手住宅設備機器メーカー（上場企業）	WebAPI
社会インフラ会社（上場企業）	Webアプリケーション
Webマーケティング会社	会員制動画プラットフォーム

業種	実施内容
大手教育サービス会社（上場企業）	学習システム
ビジネスマッチングサービス会社	WebAPI
ディベロッパー	期間イベントwebサイト
ソフトウェア開発会社	予約システムプラットフォーム
大手小売業（上場企業）	ECサイト
アパレル会社	ECサイト
動画コンテンツ制作会社	動画配信プラットフォーム
リクルーティングサービス会社	WebAPI
公益財団法人	内部向け管理システム
社会インフラ会社	サービス紹介サイト
地方信販会社	会員顧客向けサービスサイト

【参考】診断実施に際しての留意点・依頼事項①

診断対象環境

診断対象環境がAWSやAzure等のクラウドサービスの環境である場合、
診断可能なサービスや申請が必要なケースがあるため、クラウドサービス側にご確認ください。

接続環境

当社オフィスからの対象アプリケーションへリモート接続する形での診断を想定しているため、
接続元IPによる許可設定やドメイン登録等の接続許可設定のご対応を宜しくお願いします。

対象ページへのアクセス

接続を許可されたページおよび発行いただいた会員IDでアクセス可能なページのみ診断を
行うことが出来ますので、診断対象ページへアクセスが可能となるような
ご対応（権限付与、会員ID作成等）を宜しくお願いします。

診断時の影響

メール送信をする画面の診断の際に大量のメールが送信されたり、バッファオーバーフロー等
の負荷の掛かる診断をする際には、対象アプリケーションに高負荷が掛かることがあります。
そのため、診断用環境をご用意いただくことが理想的ではございますが、難しい場合は、
診断期間中の利用については使用をお控えいただいたり、関係者に対して診断中である旨を
事前にお伝えする等のご配慮をよろしくお願いします。

バックアップ

細心の注意を払い診断を行いますが、疑似的なアタックを行う形になりますので、
念のため、診断実施前には事前バックアップの取得を推奨いたします。

【参考】診断実施に際しての留意点・依頼事項②

診断時間

お客様のご指定の時間帯で診断ツールを稼働させますが、対象アプリケーションの作りや
アプリケーションが稼働している環境(サーバ・NW等）により処理時間が変動するため、
確定的な所要時間をお伝えすることが出来ません。
そのため、ご指定の時間外になってしまうと思われる際は、ツールの稼働を停止し、
別日程・時間帯での対応をご相談させていただきます。

診断時の登録データ

何かしらのデータを登録する画面の診断をする際には、診断者側でもテストデータを
登録（DB格納）する必要があります。アプリケーションによっては、診断であっても
登録不可とするケースや特定の文字列（必ずtestを付ける等）でなければならない、
といったようなご指定・制限が存在するケースもあるため、その場合は事前にお伝えください。

納品後の質疑応答

報告書納品後の質疑応答に関しては、納品日より2週間を想定しております（原則メール対応のみ）。
診断結果および再現確認等に関する質疑を受け付けますが、
改修方法等のアプリケーション固有のご質問については回答できない場合がございます。

診断結果の責任

今回の診断サービスは、OWASP TOP10に適合した診断ではございますが、
特定の資格・認証等の取得ならびに維持、またはサービス対象システムにおける全ての脆弱性の
発見を保証するものではございませんので、その点は予めご理解のほど宜しくお願いいたします。

再診断について

再診断は初回の診断で検出された脆弱性に対して修正を施された部分が対象範囲となります。
再診断をご要望の際は報告書の納品から3ヵ月以内にご依頼をお願いいたします。

Apendex

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

まずお手軽に実施するなら

セキュリティ脆弱性診断ライトパック

脆弱性診断の重要性は理解しながらも、限られたIT予算や専門人材の不足により
「ハードルが高い」という声も多く聞かれます。
そこで、当社セキュリティ脆弱性診断の品質は保ちながら、
低コストでリスクを可視化できるパッケージをご用意しました。

安価でも高品質保持

経験豊富な診断員による優先度の高い診断対象の選定します。
ツール診断＋手動診断で難しい診断項目もチェックします。

迅速な対応で安心

最小限のスコープで迅速に診断し、短納期を目指します。
診断完了から5営業日以内に診断報告書を納品します。

再診断無料

検出された脆弱性に対して再診断を実施します。（報告書提出日から3カ月以内の申し出に限る）

通常の診断との違い	お客様から対象サイト（システム）のトップURLをご教示いただいた後、当社診断員が確認し、**優先度が高い**と考えられる診断対象リクエストを任意で選定します。

選べる３つのパックプラン

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

プラン	プラットフォーム診断	Webアプリケーション診断	再診断※
ブロンズ	1 IP（FQDN）	なし	有り
シルバー	1 IP（FQDN）	5リクエスト(画面遷移)	有り
ゴールド	**3 IP（FQDN）**	**10リクエスト(画面遷移)**	**有り**

※再診断は初回診断の報告書ご提出日から3カ月以内のお申出に限り、検出された脆弱性に対して実施します。

オプション

- オンサイト対応：リモートによる診断を基本としていますが、ご希望に応じてオンサイトでの対応も可能です（別途お見積り）
- 報告会：検出した脆弱性の分析結果の報告と対策方法など、提出した報告書の内容を「報告会」としてご説明も可能です。
- 2回目以降の再診断：初回再診断後、改めて再診断を要する場合はご相談を承ります。

価格：130,000円～　詳細は営業担当までお問い合わせください。

ライトパック、よくあるご質問

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

Q.ライトパックはどんなサービスですか？

「ライトパック」は、**限られたご予算や短納期での脆弱性診断をご希望の企業様向けに設計された、コストパフォーマンスに優れたサービス**です。自動診断ツールと専門技術者による手動チェックを組み合わせ、特に重要なリスクを効率的に抽出いたします。

Q.通常の診断と比較して、精度が劣ることはありますか？

本サービスは、**自動診断ツールと診断員による手動チェックを行うという点では精度の違いはございません**。
診断対象を絞って実施する形になるため、精度というよりも診断範囲が限定的となりますが、診断優先度の高い部分を選定して実施するため、コストと成果のバランスに優れた診断内容となっております。

Q.診断対象はどのように決まりますか？

事前ヒアリングにて、お客様のシステム構成やご希望等をお伺いした上で、当社診断員が実際にサイト接続をして対象を確認させていただき診断対象（IPやアプリケーション等）を決定いたします。
ライトパックでは、**経験豊富な診断員が優先順位の高いリスク領域を選定**いたします。

Q.オンサイトでの診断は可能ですか？

ライトパックではオンサイト診断はお受けしておりませんが、ご希望の場合は事前にご相談ください。（オプション対応・別途お見積りとなります）

ご不明な点がございましたら、随時オンライン会議でのご説明も可能です。
お気軽にお問い合わせください。

お問い合わせ

Secure Innovation
沖縄から日本全国、アジア、そして世界へ

資料請求やお見積依頼など、お気軽にお問い合わせください。
担当からすぐにご連絡いたします。

お問い合わせフォーム

https://www.secure-iv.co.jp/contact

pr@secure-iv.com

098-943-2718

受付時間 9:00～18:00（土日祝祭日を除く）