- ☐ Security Consulting
- ☑ Security Assessment
- ☐ Managed Security

三井物産セキュアディレクション株式会社

〒103-0013 東京都中央区日本橋人形町1丁目14番8号 JP水天宮前ビル6階
TEL : 03-5649-1961（代表）
https://www.mbsd.jp/

Part No. TS11-1001-2503

Security Assessment Service

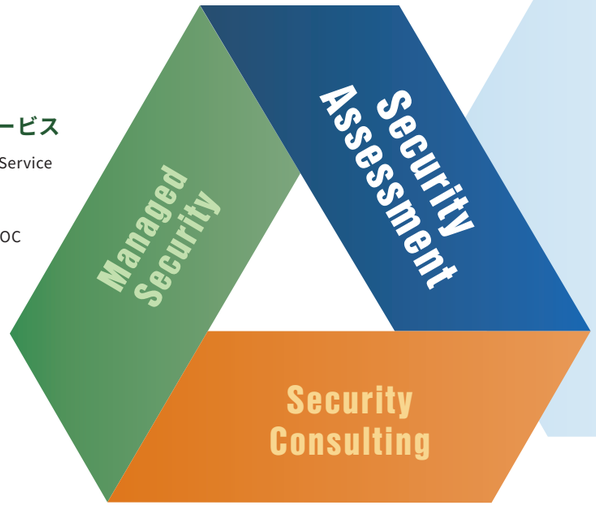
セキュリティ診断サービス

CONTENTS

脅威を可視化する、精密なセキュリティ診断

Services

MBSDの事業は3サービスを軸として提供しています。



セキュリティ監視サービス

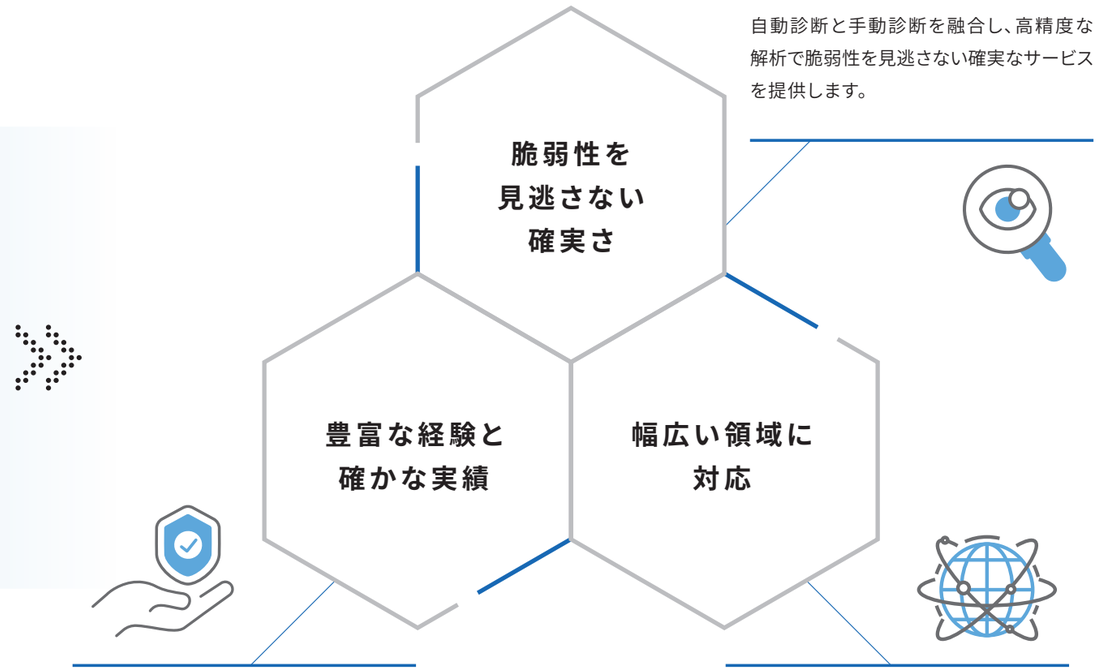
- MBSD Managed Security Service（MBSD-SOC）
- Microsoftセキュリティ監視
- 統合ログ監視・Advanced SOC
- 統合ログ環境構築支援
- Security Force

セキュリティ診断サービス

- Webアプリケーション診断
- ネットワーク診断
- スマホアプリ診断
- ペネトレーションテスト
- TLPT（Threat Led Penetration Test）
- AIシステムに対するセキュリティ診断
- 要塞化支援
- IoT診断
- ゲーム診断
- OT診断

セキュリティコンサルティングサービス

- リスクアセスメント
- セキュリティ組織運用支援
- サイバーBCP/BCM対策構築運用支援
- CSIRT構築・運用支援
- シンクタンクコンサルティング
- AIセキュリティ対策アドバイザリー
- その他のサービス



自動診断と手動診断を融合し、高精度な解析で脆弱性を見逃さない確実なサービスを提供します。

豊富な実績と専門知識に基づき、安心してお任せいただける信頼性の高いサービスを展開しています。

WebからIoTまで幅広い領域に対応し、企業のセキュリティを包括的に強化する診断を実施します。

この小冊子では、当社の具体的なソリューションを通じて、貴社の成長を力強く支えるための セキュリティ診断サービスをご紹介します。

Security Assessment Service セキュリティ診断サービス

国内トップのホワイトハッカー集団が情報資産の脆弱性を網羅的に洗い出します

当社は、2001年に業界に先駆け「Webアプリケーション診断サービス」を開始し、インターネットの進化とともに診断技術を高度化させてきました。20年以上にわたる経験と実績は、多くのお客様から高い信頼を得ており、特に難易度の高い脆弱性の発見において社会に大きく貢献しています[*1]。

一般的な診断サービスでは見逃されがちな脆弱性も、当社の診断により高確率で検出されるケースが多くあります。最新の脅威に対応する専門知識と、高度な診断技術を活用して、単なる診断にとどまらず、継続的なセキュリティ向上を支援することを目指しています。お客様の事業運営を守るため、私たちは常に進化し続けるセキュリティサービスを提供します。

*1: JPCERT CC と IPA が共同で運営する 公的機関JVN（Japan Vulnerability Notes）への脆弱性報告数は 2016年より8年連続 No. 1

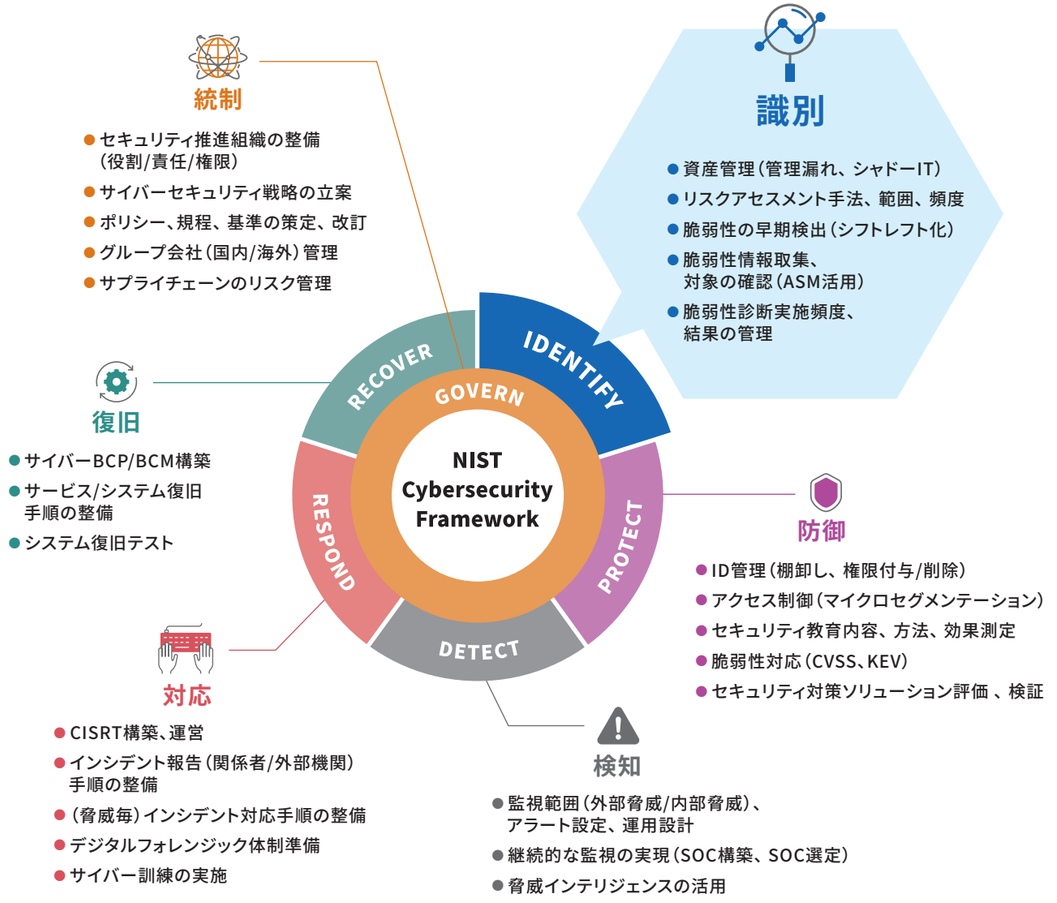
Assessment Service Target

診断サービス対象

- Webアプリケーション診断
- ペネトレーションテスト
- ネットワーク診断
- TLPT（Threat Led Penetration Test）
- スマホアプリ診断
- AIシステムに対するセキュリティ診断
- ゲームセキュリティ診断
- IoT診断
- 要塞化支援（サーバー・クラウド設定検査）
- OT診断（自動車/ビル/工場など）

国際的なフレームワーク NIST CSF (Cybersecurity Framework) 2.0 に対応

NIST Cybersecurity Framework 2.0（CSF 2.0）は、米国国立標準技術研究所（NIST）が策定したサイバーセキュリティ対策の枠組みで、世界中の組織がセキュリティ成熟度を向上させるための指針を提供し、業種や規模を問わず適用可能で、多くの企業に採用されています。「統制」「識別」「保護」「検知」「対応」「復旧」の領域を基盤に、セキュリティの現状把握からリスク軽減の行動計画策定までを包括的に支援します。当社が提供するセキュリティ診断サービスは、CSF 2.0の【識別】領域をカバーします。



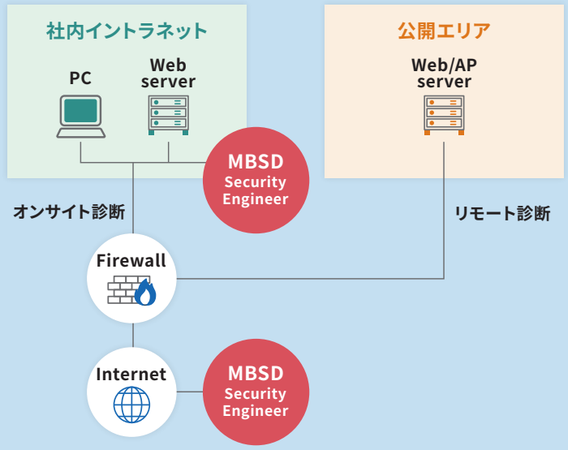
※NIST Cybersecurity Framework2.0より抜粋

Webアプリケーション診断

Webアプリケーション診断では、保有するWebアプリケーションシステムに対して、疑似攻撃を行い、Webアプリケーションシステムに存在する情報漏えいや改ざんといった様々なリスクを調査するサービスです。

手動診断をメインとし、網羅性や機械的なテストを実現するため独自の補助ツールを組み合わせて疑似攻撃を行い、Webアプリケーション上の脆弱性を調査します。

情報セキュリティサービスへの
台帳登録情報はこちら



Webアプリケーション診断の特長

高精度な診断プロセス

- 自動診断ツールのスピードと、熟練エンジニアによる手動診断の精密さを融合。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、見逃されがちな脆弱性も徹底解析します。

包括的なセキュリティ評価

- 発見された脆弱性が業務に与える影響を定量的に評価し、具体的な対策を提案。企業のリスク管理を支援します。

診断後のフォローアップサポート

- 診断後の修正作業をサポートし、再診断で効果を確認。継続的なセキュリティ強化を実現します。

独自の技術とノウハウ

- 自動化技術と専門家の手動診断を融合し、診断精度を向上。最新の脅威に対応し、高度な診断を提供します。

豊富な診断実績

- 数百社以上の大手企業での診断実績が信頼の証。多くの成功事例を基に、企業に最適なセキュリティ対策を提案します。

迅速な対応力

- 最短1週間で診断を実施し、結果を迅速に報告。時間を要さず、速やかにリスクを特定できます。

診断実績

2017年4月〜2022年3月

Performance

Webアプリケーション診断サービス

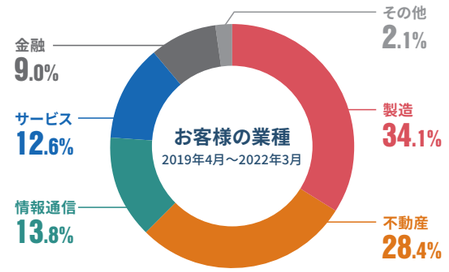
3,000サイト以上

100,000リクエスト以上

ネットワーク診断サービス

2,800案件

5,400IP以上



主な診断項目

通信

HTTPSの適用有無や適用範囲、未使用や適用漏れなどを確認します。

認証/認可

認可処理の有無や方法、適用範囲、不正なパラメータ操作や画面遷移による越権を調査します。

セッション

セッション管理方法、セッションIDの設計・生成・再生成・破棄、Cookieの生成・破棄・用途、画面遷移の管理・監視の有無を確認し、セッションハイジャックやクロスサイトリクエストフォージェリなどのリスクを評価します。

入力/出力

コンテンツの生成方法、値の出力有無・形式・箇所、例外発生時の挙動を確認し、クロスサイトスクリプティングや不要なエラーメッセージの出力などを調査します。

サイトデザイン

設計・仕様上の問題、機能の悪用可否、クロスオリジンのアクセス制御設定、オープンリダイレクト、サーバーサイドリクエストフォージェリ、不正なパラメータ操作、ビジネスロジックに関わる不備、不要な情報の出力、デバッグ機能の残存、JavaScriptハイジャックなどを評価します。

Webサーバー/フレームワーク

製品・ソフトウェアの設定、公開コンテンツ、バージョン情報の出力、ローカルIPアドレスの出力、不要なHTTPメソッドの有効化、コンテンツの公開設定不備、ディレクトリインデックスの設定などを確認します。

Service Delivery Process

サービス提供フロー

事前準備

- お客様ご指定のWebサイトに対して巡回作業を実施
- 巡回の結果をもとに診断対象範囲を決定

脆弱性診断

- 巡回結果をもとに策定したスケジュールにて診断作業を実施
- 診断ツールによる効率の良い診断、およびセキュリティエンジニアによる手動診断を実施

分析評価

- 検出された脆弱性の分析・評価
- 脆弱性が悪用された場合の脅威、影響度などを分析・評価
- 診断結果報告書の作成

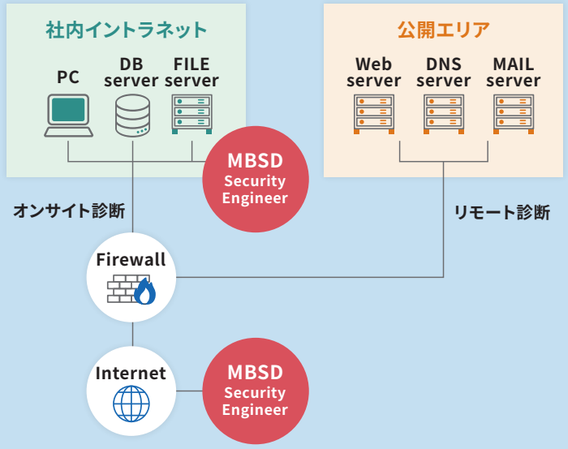
報告

- 診断結果報告書の納品
- お客様への診断結果報告会を実施
- 診断結果（脆弱性、脅威、影響度など）に関する質疑応答

ネットワーク診断

ネットワーク診断（プラットフォーム診断）とは、保有するサーバー/ネットワーク機器/端末などに対して、疑似攻撃を行い、稼働しているOSやミドルウェア、サーバーソフトなどに存在する情報漏えいや改ざん、設定不備、パッチの適用状況など様々なリスクを調査するサービスです。

手動診断と、網羅性や機械的なテストを実現するため独自の補助ツール、商用ツールなどを組み合わせて疑似攻撃を行い、稼働しているOSやミドルウェア、サーバーソフトなどの脆弱性を調査報告いたします。



ネットワーク診断の特長

高いネットワーク診断能力

- 当社のネットワーク診断サービスは2001年から他社に先駆けてスタートし、豊富な手動診断の経験と技術力を保有しています。

豊富な診断実績

- 2,800サイト以上、5,400IP以上の診断実績（2017年4月～2022年3月実績）

脆弱性検証に関する高い技術

- 脆弱性を効率よく検出する手法に関しての研究およびツールの開発を日々行っており、その成果は国内/海外のセキュリティカンファレンスでも発表しています。

多数の脆弱性発見実績

- JPCERT/CCとIPAが共同で運営するJVN（Japan Vulnerability Notes）への脆弱性報告の公表において、新たな脆弱性（0day）を累計200件以上も報告しています。未知の脆弱性を発見する高いスキルを持つセキュリティエンジニアが当社に多数在籍しています。

主な診断項目

ネットワーク調査
TCPおよびUDPスキャン、サービススキャン、OS推測、ホスト名調査を行い、ネットワーク全体の構成と潜在的な脆弱性を把握します。

各種サービスの脆弱性調査
脆弱性スキャンを実施し、稼働中のサービスに存在する既知の脆弱性を検出します。

FTP調査
バナー情報の取得、匿名接続の可否確認、簡易パスワード推測を通じて、FTPサービスのセキュリティ状態を評価します。

SSH調査
バナー情報の取得、認証方法の確認、簡易パスワード推測を行い、SSHサービスの安全性を検証します。

TELNET調査
バナー情報の取得と簡易パスワード推測を実施し、TELNETサービスの脆弱性を評価します。

SMTP調査
バナー情報の取得、不正中継の可否確認、EXPNおよびVRFYコマンドの挙動を調査し、メールサーバーのセキュリティを検証します。

POP調査
バナー情報の取得と簡易パスワード推測を通じて、POPサービスの安全性を評価します。

DNS調査
バナー情報の取得、再帰的問い合わせの可否確認、ゾーン転送の可否を調査し、DNSサーバーの脆弱性を検出します。

HTTP/HTTPS調査
バナー情報の取得、Webスキャン、ファイルおよびディレクトリ調査、簡易パスワード推測、WebDAVやCMS調査、フレームワーク調査、プロキシ調査、SSLの暗号強度とバージョン、証明書の検証を行い、Webサーバーのセキュリティを総合的に評価します。

SUNRPC調査
RPC情報の取得を通じて、リモートプロシージャコールサービスの脆弱性を検出します。

SMB調査
アカウント情報、ファイル共有情報、NetBIOS情報の収集、簡易パスワード推測を行い、SMBサービスのセキュリティ状態を評価します。

SNMP調査
簡易コミュニティ名の推測とMIB情報の取得を通じて、SNMPサービスの脆弱性を検出します。

NTP調査
バナー情報の取得を行い、ネットワークタイムプロトコルサービスのセキュリティを評価します。

バックドア調査
ポートスキャンを実施し、システム内に潜在するバックドアの有無を検出します。

Service Delivery Process

サービス提供フロー

事前準備
- 診断対象となるネットワークのヒアリング
- 診断対象IP数、禁止事項の確認 など

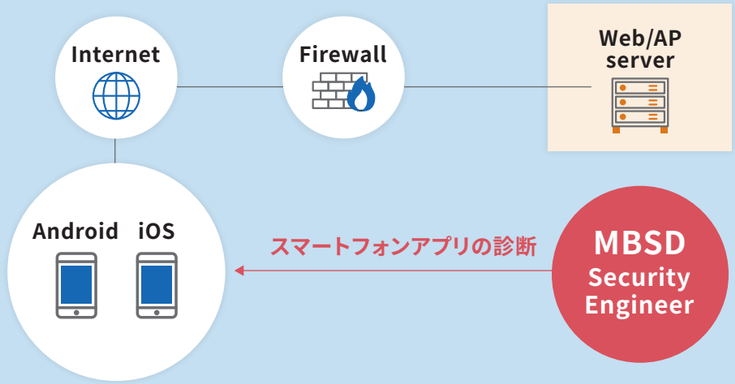
脆弱性診断
- 事前確認に基づき診断作業を実施
- 診断ツールによる効率の良い診断、およびセキュリティエンジニアによる手動診断を実施

分析評価
- 検出された脆弱性の分析・評価
- 脆弱性が悪用された場合の脅威、影響度などを分析・評価
- 診断結果報告書の作成

報告
- 診断結果報告書の納品
- お客様への診断結果報告会を実施
- 診断結果（脆弱性、脅威、影響度など）に関する質疑応答

スマホアプリ診断

スマートフォンアプリケーション診断では、iOSやAndroidなどのスマートフォンアプリケーションに対して疑似攻撃を行い、スマートフォンアプリケーションに存在する情報漏えいやアプリケーションをクラッシュさせるといった様々なリスクを調査するサービスです。
スマートフォンアプリケーション本体に対して疑似攻撃を行い、スマートフォンアプリケーション上の脆弱性を調査報告いたします。スマートフォンアプリケーション本体の診断は、静的解析、動的解析を組み合わせて実施します。



スマートフォンアプリケーションは、Webアプリケーションなどと異なり、ユーザーのAndroid/iOS端末にインストールされ利用されます。そのため、攻撃者はスマートフォンアプリケーションを入手することができ、アプリケーション内の処理は攻撃者自身が手元で容易に解析を行える状況となっています。
スマートフォンアプリケーション診断では、攻撃者と同じ目線で解析することでセキュリティ事故を未然に防止することができます。

スマホアプリ診断の特長

脆弱性検証に関する高い技術

☑ 新たな脆弱性（0day）や脆弱性を検出する手法に関するドキュメントの公開などを行っています。技術ドキュメントは当社Webサイトで公開しています。

多数の脆弱性発見実績

☑ JPCERT/CCとIPAが共同で運営するJVN（Japan Vulnerability Notes）への脆弱性報告の公表において、新たな脆弱性（0day）を累計200件以上も報告しています。未知の脆弱性を発見する高いスキルを持つセキュリティエンジニアが当社に多数在籍しています。

主な診断項目

アプリケーション間連携
- 不正なアプリケーションからのアクセス制限の適切性
- 不正な情報受信による情報漏えいや改ざんの有無
- 重要情報の送信方法の適切性

通信
- 使用プロトコルの確認
- 重要情報送受信時の暗号化通信の有無
- SSL/TLS通信時のサーバー証明書検証の実施
- 個人情報や認証情報などの重要情報の送受信状況
- 適切な許諾を得ずに個人情報などをサーバーに送信していないか

認証
- 認証機能の安全な実装
- アプリケーション連携による認証・認可情報の窃取防止
- ログアウト機能の適切な実装

端末内のデータの取扱
- 共有領域への重要情報保存の有無
- ファイルへのアクセス権限設定の適切性
- 重要情報保存時の暗号化実施
- 適切なタイミングで端末内の情報を削除しているか

アプリケーションファイル・ログ
- 開発環境やテスト環境、開発者に関連する情報の残存
- 重要情報や解析の手がかりとなりうる情報の出力

機能の利用
- アプリケーションが利用しない不要なパーミッションの登録

Service Delivery Process

サービス提供フロー

事前準備
- お客様ご提供の資料やアプリケーションをもとに必要な情報の確認
- 対象アプリのインストールや動作確認、APIの疎通確認など

脆弱性診断
- 事前確認に基づき診断作業を実施
- 静的解析や動的解析を組み合わせながらセキュリティエンジニアによる手動診断を実施

分析評価
- 検出された脆弱性の分析・評価
- 脆弱性が悪用された場合の脅威、影響度などを分析・評価
- 診断結果報告書の作成

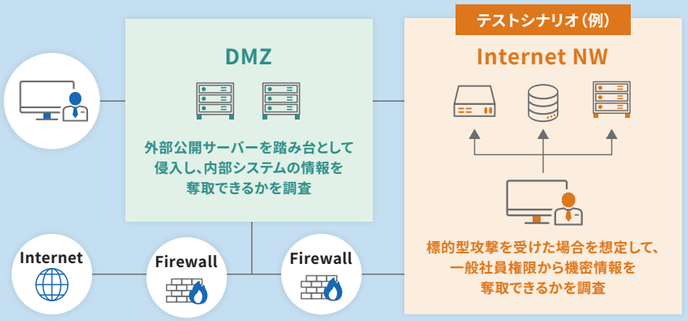
報告
- 診断結果報告書の納品
- お客様への診断結果報告会を実施
- 診断結果（脆弱性、脅威、影響度など）に関する質疑応答

ペネトレーションテスト

ペネトレーションテストは明確な意図を持った攻撃者がその目的を達成することが可能であるか検証するテストです。「外部から社内に侵入されてしまうか確認したい」、「標的型攻撃のリスクを確認したい」など、お客様の要望に応じて、攻撃者の目的を想定しゴールやテストの対象範囲（スコープ）を設定します。お客様と調整の上、テスト実施時間帯などの条件（レギュレーション）を基にテスト計画を作成します。

以下のようなケースに対して有効なテストとなります

- ☑ 実際に攻撃を受けた場合の影響を把握したい
- ☑ セキュリティ機器の有効性を確認したい
- ☑ 脆弱性診断では顕在化しにくい運用上の問題も含めて確認したい



脆弱性診断との違い Difference

ペネトレーションテストはいわゆる脆弱性診断のようなWebアプリケーション単体やプラットフォーム単体のテストではなく、また網羅的に脆弱性の調査を行うわけではありません。目的や手法も異なります。

	ペネトレーションテスト	脆弱性診断（Webアプリケーション診断/ネットワーク診断）
目的	事前に取り決めた攻撃目標を達成できるか検証します。	評価対象において網羅的に脆弱性を洗い出します。
手法	事前に設計した攻撃手順に沿ってテストを実施します。期間内に攻撃目標を達成するために様々な手法を利用し、必要があれば脆弱性を利用して攻撃を行います。	脆弱性を洗い出すために、あらかじめ取り決められた定型的な手法で調査します。脆弱性の有無を確認するために必要最低限の通信にとどめ、実際に攻撃して影響を確認するような調査までは行いません。
調査対象	その組織が持つすべてのシステム、もしくは指定されたシステム全体が対象になります。	指定されたアプリケーション・サーバーが対象になります。
結果報告	どのような攻撃を行うことで、攻撃目標を達成できたかという報告。テストの過程で判明した脆弱性やセキュリティ上の問題を報告する。	リスクの高いものから低いものまで発見された脆弱性をすべて報告します。

ペネトレーションテストの特長

数千IPに対するテスト実績と豊富なナレッジ

☑ 年間1,000IP以上、累計数千IPに対する多くの案件を通じて得たノウハウを蓄積し、効率良くかつ精密に調査をするスキルを有しています。日々、実用性の高い攻撃コードを収集・実証し、当社独自ツールに組み込むことで独自の手法にてテストを実施します。

侵入リスクを可視化

☑ セキュリティ機器の有効性やどこまで侵入可能であるか、被害が拡大する可能性があるかを分析します。侵入の可否だけではなく、管理者権限の取得や侵入後に得られた情報を活用し、他の対象への侵入を試行することで、想定される影響や被害範囲が可視化可能です。

脆弱性検証に関する高い技術

☑ 実用性の高い攻撃コードを収集・実証し、ツールに依存しないExploitコードの作成を多数の案件を通じて行っています。コードの検証を行うことにより、安全で精度の高いペネトレーションテストをご提供します。

多数の脆弱性発見実績

☑ JPCERT/CCとIPAが共同で運営するJVN（Japan Vulnerability Notes）への脆弱性報告の公表において、新たな脆弱性（0day）を累計200件以上も報告しています。未知の脆弱性を発見する高いスキルを持つセキュリティエンジニアが当社に多数在籍しています。

Service Delivery Process

サービス提供フロー

事前準備

- テストの対象とするゴール・スコープ・攻撃手段を確定するために必要な情報のやりとり

計画策定

- 頂いた情報を元に、ゴール・スコープ・攻撃手段を確定し、テストを実施するスケジュールについて調整

実査

- 事前に取り決めた攻撃手順に沿って、ペネトレーションテストを実施
- テスト結果について報告書を作成

報告

- ペネトレーションテストの結果について報告
- 今後のあるべき姿（To-Be）についても提言

Point 01

一般公開されているセキュリティの問題（脆弱性）だけではなく、公開情報などを収集/分析し、ゴールを達成するために活用します。

Point 02

このテストによりセキュリティ機器の有効性や問題となるサーバー、設定や運用上の問題を特定することができます。

Point 03

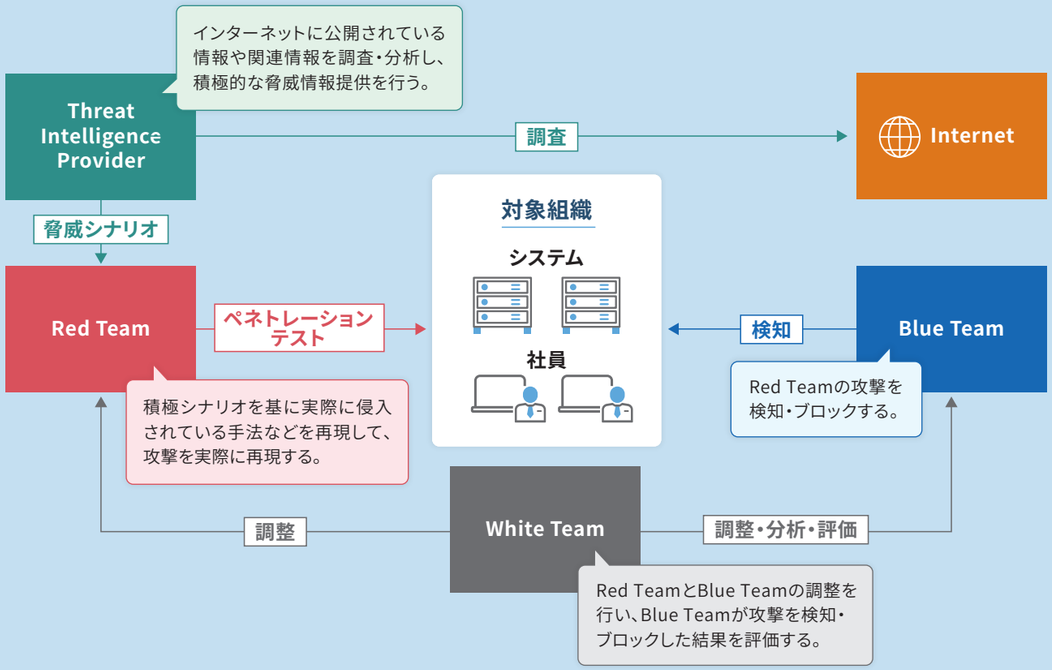
ゴールやスコープを基に攻撃手順を確定し、決定した攻撃手順に基づいてテストを実施します。

Point 04

テスト実施後は、ゴールの達成可否などのテスト結果及びセキュリティ改善策についてご報告します。

TLPT（Threat Led Penetration Test）

TLPT（脅威ベースペネトレーションテスト）は、組織やシステムの脅威を分析し、脅威シナリオを作成した上で、実際の攻撃者と同様の手法を用いた攻撃に対する組織の検知・防御能力（サイバーレジリエンス力）を評価します。通常のペネトレーションテストが汎用的な脅威を想定するのに対し、TLPTはThreat Intelligence Providerによる脅威調査・分析に基づいて現実的な脅威を想定し、Red Teamが攻撃トラフィックを発生させるペネトレーションテストを実施します。この間、Blue Team（SOCやCSIRTなど）が攻撃を検知・防御し、White Teamが対応状況を観察して組織のセキュリティ対応力を評価します。



ペネトレーションテストとの違い Difference

TLPTサービスの実施範囲

脅威の調査・分析	ペネトレーションテスト	組織の評価

一般的なペネトレーションテストの実施範囲

一般的なペネトレーションテストサービスの場合、汎用的な脅威を想定しテストを行うのに対して、TLPT支援で行う、脅威ベースのペネトレーションテストは事前に脅威を調査・分析し、その結果に基づき現実的な脅威を想定した上で、ペネトレーションテストを行い、攻撃トラフィックを発生させます。
また、同時に、ペネトレーションテストを行うことで貴社Blue Teamによる検知・対応状況を観察し、組織におけるセキュリティを評価します。

TLPTの特長

現実で脅威となるシナリオを用いたテスト

- Threat　Intelligenceにより実際の攻撃者と同様にインターネットに公開されている脅威情報や対象情報を基に、個々の組織に合わせて攻撃シナリオを作成
- 現実で起こりえる脅威に対する対応状況やサイバーレジリエンス能力を評価することが可能

脅威となるリスクを可視化

- セキュリティ対策機器の有効性やどこまで侵入可能であるか、侵入された場合に被害が拡大する問題を分析
- 侵入の可否だけではなく、管理者権限の取得や侵入後に得られた情報を活用し、他の対象への侵入を試行することで、想定される影響や被害範囲を可視化

サイバーレジリエンス能力を評価

- 攻撃によるシステム上の問題点の調査だけでなく、組織におけるサイバー攻撃に対するサイバーレジリエンス力（攻撃を検知・ブロックし被害を最小化し、システムを復旧する能力）を評価

To-Beギャップ分析による組織の成熟度を評価

- 社内規定など組織におけるインシデントなどへのアクションプランを評価し、本来求められる理想像とのギャップ分析を行い、組織におけるセキュリティの成熟度を評価

Service Delivery Process

サービス提供フロー

1カ月程度	2~3カ月程度	2週間～1カ月程度	1~2カ月程度
事前準備 ● ヒアリング ● ネットワーク構成、設計書のご提供	**脅威情報の調査・シナリオ作成** ● 脅威シナリオを作成 ● 実地での調査	**ペネトレーションテストの実施** ● 模擬攻撃を実施 ● 利用した攻撃方法をWhite Teamと共有	**報告** ● Red Teamの攻撃に対するBlue Teamの検知・ブロックの有効性を評価・報告 ● 今後のあるべき姿（To-Be）についても提言

AIシステムに対するセキュリティ診断

当社は2015年からAIセキュリティを調査・研究し、豊富なナレッジと情報発信を重ねてきました。AIシステムには特有のセキュリティリスクが存在し、AIを組み込んだアプリケーションでは攻撃の幅が拡大します。AIセキュリティ診断は、擬似的な攻撃や評価でこうしたリスクを洗い出すサービスです。

AI特有のリスクは従来対策では防ぎきれず、特に生成系AI（GPT/GeminiやDALL・E/Stable Diffusionなど）の活用増加により、新たな攻撃手法や被害事例が日々公表されています。このため、AI特化型の診断が求められます。

主な診断項目

学習データ汚染
- Convex Polytope Attack
- Feature Collision Attack
- Bullseye Polytope Attack

モデル汚染
- BadNets
- 機械学習フレームワークを悪用したバックドア

回避攻撃
- Adversarial Example
- Adversarial Patch

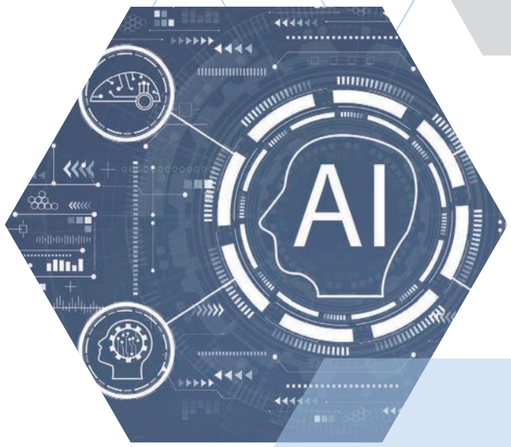
学習データ窃取
- メンバーシップ推論攻撃
- Model Inversion Attacks

モデル窃取
- Copycat CNN

防御機構回避
- Prompt Injection
- Jailbreaking
- Macaronic Prompting
- Evocative Prompting

プロンプトテンプレート窃取
- Prompt Leaking

P2SQLインジェクション
- P2SQL Injection



主な特長

自社開発、SaaS利用など幅広い利用方法をカバー

☑ AIシステムは、企業の利用方法などにより様々な使われ方が存在しており、ツールベースの評価では対応することができません。

- 自社でモデルを作成するケース
- GPT/Geminiなど外部の大規模言語モデル（LLM）を組み込むケース
- Langchainなど連携用のライブラリを組み合わせ内部のリソースを参照させるケースなど

当社の診断サービスでは豊富なナレッジを有しているため、現状のシステムを考慮した確認手法やセキュリティリスクの洗い出し、評価を実施することが可能です。

豊富なナレッジ、最新の攻撃/防御手法をカバー

☑ AIに対する攻撃手法/防御手法の研究は盛んに行われており、日々新しい攻撃手法/防御手法が提案されています。当社はこれまで多くの情報発信を行っており、豊富なナレッジを有しております。

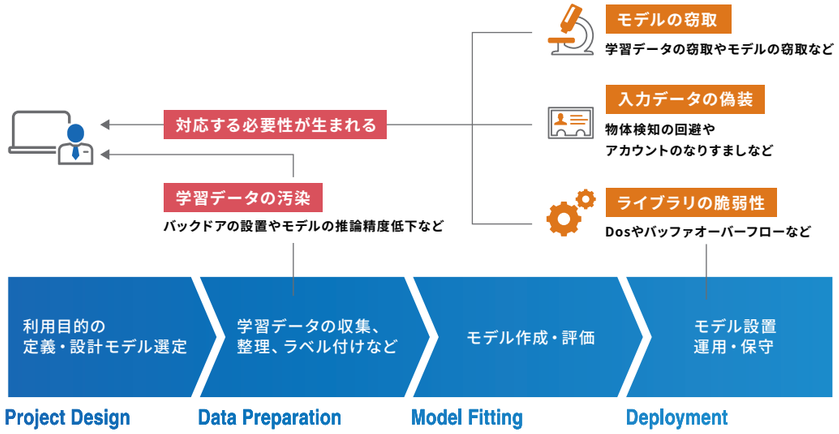
以下サイトでご覧いただけます

AIディフェンス研究所	MBSD技術者ブログ	AIセキュリティ情報発信ポータル

新しい攻撃手法やそれに対する防御手法の提示など、豊富なナレッジで評価や対策をご支援いたします。

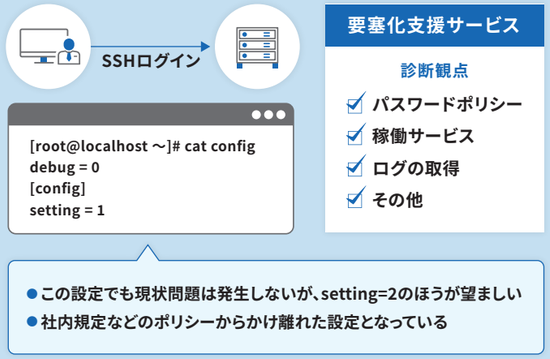
AI Development & Threats

AI開発の各工程と想定される脅威



要塞化支援

要塞化支援サービス（サーバー構成診断）は実際のサーバーへログインし内側から潜在的なリスクを洗い出すアセスメントです。パスワードポリシーやサーバーの設定不備といった外部からの脆弱性診断では露見しないような問題を洗い出すことが可能です。サーバーをより堅牢に運用したい場合に有効です。実際のサーバーやクラウド環境へログインし、CIS認定のスキャナをベースに内側から潜在的なリスクを洗い出します。サーバーの設定不備、潜在リスク、ログ取得の正確性、パスワードポリシーなど約200項目にもおよぶ監査項目をチェック、分析し、ご報告いたします。

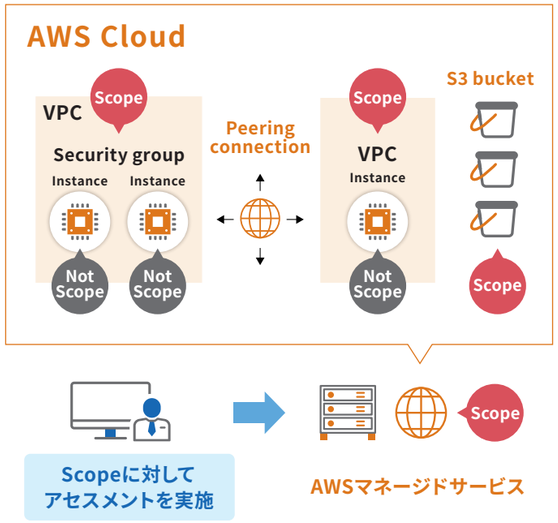


サーバー環境における設定検査

01 サーバー構成診断（Redhat Linux）	02 サーバー構成診断（CentOS）	03 サーバー構成診断（Windows Server）	04 サーバー構成診断（AIX）

など

AWS/Azure対応



AWSマネージドサービス

- AWS Identity and Access Management（IAM）
- AWS Config
- AWS CloudTrail
- AWS CloudWatch
- AWS Simple Notification Service（SNS）
- AWS Simple Storage Service（S3）
- AWS VPC

監査項目をチェック/分析/ご報告

- ☑ サーバー設定不備
- ☑ パスワードポリシー
- ☑ 潜在リスク
- ☑ 監視設定
- ☑ ログ取得の正確性
- ☑ S3バケット

要塞化支援の特長

サーバーのセキュリティを客観的に評価

☑ ベースラインに基づいて設定値を確認していくため、サーバーのセキュリティレベルを客観的に判断することが可能です。

外部からのリスク評価で露見しない問題を指摘

☑ 脆弱性診断は外部からの調査となるため、社内からの不正アクセスリスクや潜在的なリスクについては検証や対処が困難となっています。一方、要塞化支援サービスでは、サーバー内部から状況を評価するため、正確に評価/分析することが可能です。

CISとは ABOUT CIS

- CIS（Center for Internet Security）はアメリカ合衆国ニューヨーク州に拠点を置く非営利団体で、全世界のITコミュニティの力を使い、サイバーの脅威から保護することを目的として活動しています。
- CIS Benchmarksは、脅威にさらされる可能性があるOS/ソフトウェア/ネットワークを保護するためのガイドラインとして作成され、40種類以上のプラットフォームに対応しています。
- 本サービスでは、CIS認定のスキャナであるNessus Professionalをベースにセキュリティ上の問題となる可能性のある設定を調査いたします。

Service Delivery Process

サービス提供フロー

準備

- 対象の選定
- 監査に必要な情報について確認
  - ・対象サーバーの構成（OS、ソフトウェア、管理者権限のID/パスワード）
  - ・接続方法
  - ・パスワードポリシー など

作業

- ツールでのチェックのほか、追加で情報収集を行い、監査の補助となる情報を収集

評価

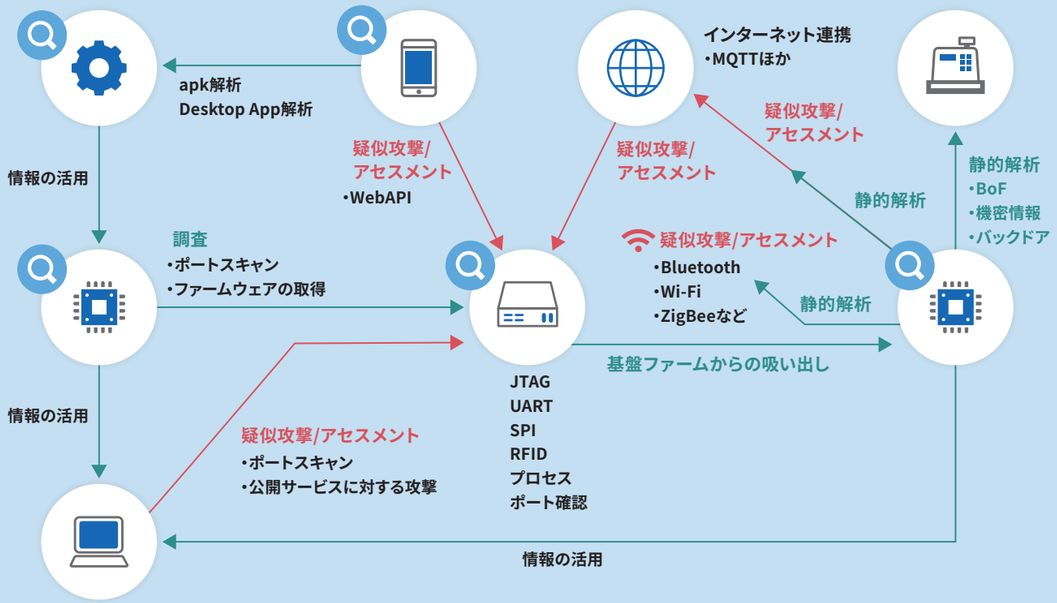
- ツールの実行結果と事前の確認事項の結果を合わせて評価

報告

- 評価の結果を報告書にて報告

IoT診断

IoTセキュリティ診断（組み込み機器診断）は、悪意ある攻撃者の視点で疑似攻撃を行うアセスメントです。サーバー等と異なり、組み込み機器は攻撃者の手元にあるため、ソフトウェアだけでなくハードウェアからも攻撃を受ける可能性があります。IoT機器では、市場投入前のセキュリティ対策が重要です。本診断では、攻撃による被害を事前に調査し、リリース前の対策計画や製品ロードマップに活用できます。
当社の診断では、機器管理用Webアプリケーションやサービス提供ポートの脆弱性診断/ペネトレーションテストに加え、独自仕様を持つ組み込み機器の通信やハードウェアを対象に、経験豊富なエンジニアが脆弱性を手動で調査します。



IoT診断の特長

機種の機能、特性等を考慮

- 組み込み機器は、機器ごと様々なサービスが提供されます。機種の機能、特性等を考慮して実際の脅威や攻撃のシナリオを組み立て評価します。

深い知見と、高い解析技術

- 独自のプロトコル（通信規格）によって制御されているケースが多いIoT機器の通信に対して、問題点を見つけることができる高い解析技術を有しています。

多数の脆弱性発見実績

- 未知の脆弱性を発見する高いスキルを持つセキュリティエンジニアが当社に多数在籍しており、組み込み機器に関する脆弱性報告の公表を多数行っています。

ゲームセキュリティ診断

ゲーム業界は高度な技術革新に伴い、サイバー攻撃の脅威が増大しています。当社のゲームセキュリティ診断サービスはオンラインやモバイルゲームを対象に、独自の脆弱性診断を通じて不正アクセス、データ改ざん、チート行為を未然に防ぎ、ユーザーの信頼を確保します。当社の専門家チームは最新の攻撃手法や脆弱性情報を追跡し、ゲームサーバー、クライアント、通信プロトコル、APIなどを包括的に評価します。診断結果に基づき、改善策と強化策を提示し、開発チームと連携して迅速な対応をサポートします。

さらに、リリース前後の診断を推奨し、継続的なセキュリティ強化により品質向上とユーザー体験の最適化を実現します。業界最高水準のセキュリティで、ゲームビジネスの成功を力強く支援します。

- **最新の攻撃手法や脆弱性情報を追跡**
- **不正アクセス、データ改ざん、チート行為を未然に防止**
- **継続的なセキュリティ強化**

OT診断

- **ネットワーク構成、アクセス制御など多角的に診断**
- **最新規制や業界標準に沿ったコンプライアンス確保をサポート**
- **定期的な診断と改善**

現代の産業環境では、デジタル化したOT（Operational Technology）システムがサイバー攻撃の標的となっています。当社のOTセキュリティ診断サービスは、自動車、工場などの産業制御システムを対象に脆弱性評価を実施し、システムの可用性・信頼性・安全性を確保、事業継続性を支援します。

当社エキスパートは特有のプロトコルや機器に精通し、ネットワーク構成、アクセス制御などを多角的に診断します。結果に基づく優先度付けと具体策でセキュリティを強化し、最新規制や業界標準に沿ったコンプライアンス確保もサポート。定期的な診断と改善を通じて、OTシステムの防御力を維持・向上し、産業デジタル化を安全に推進します。