セキュアな開発・サービス提供に必須

LANSCOPE
Professional Service

はじめての脆弱性診断
正しい進め方ガイド

-Web・ネットワーク・クラウドのセキュリティ診断-

はじめに

サイバー攻撃が巧妙化する中、脆弱性対策の重要性が高まっています。
脆弱性診断を行いたいという組織が増える一方で、「何から始めれば良いか分からない」「どこを診断すべきか分からない」などといった課題を抱えることがあります。
この資料では、診断の選び方から、診断を行う際の準備やポイントを解説します。

<アジェンダ>

1．脆弱性による脅威と診断の必要性

2．脆弱性診断の進め方　-事前準備から終了後の対応まで-

3．エムオーテックスの脆弱性診断

4．エムオーテックスの診断の特長

脆弱性による脅威と診断の必要性

大半の脅威は「ソフトウェアの脆弱性や設定不備」が攻撃の糸口に利用

企業で運用・開発しているソフトウェアの脆弱性や利用中のネットワーク機器・クラウドサービスの設定不備が攻撃の起点となっています

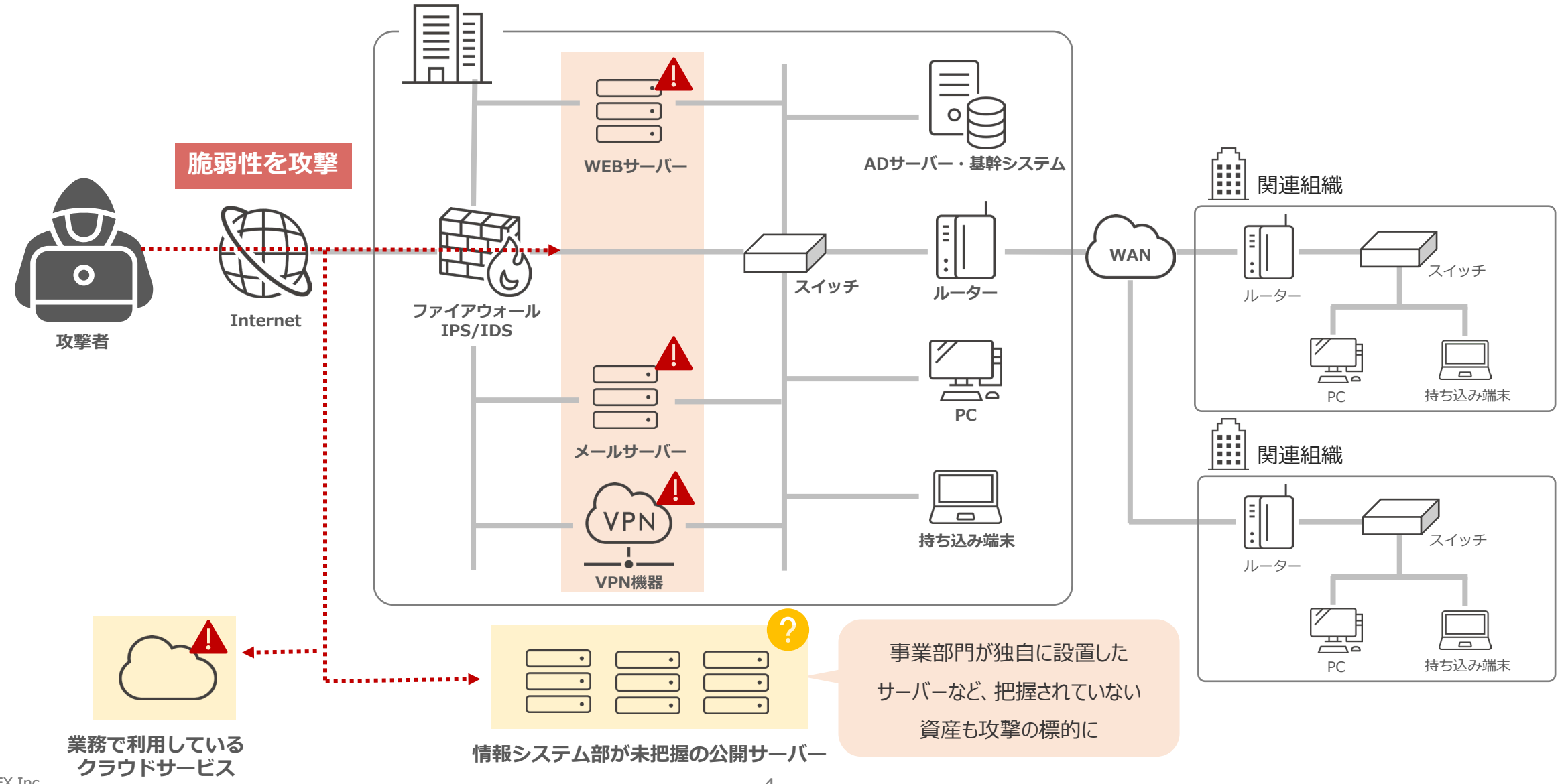
情報セキュリティ10大脅威2024

順位	組織	初選出年	昨年順位
1位	ランサムウェアによる被害	2016年	1位
2位	サプライチェーンの弱点を悪用した攻撃	2019年	2位
3位	内部不正による情報漏えい等の被害	2016年	4位
4位	標的型攻撃による機密情報の窃取	2016年	3位
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	6位
6位	不注意による情報漏えい等の被害	2016年	9位
7位	脆弱性対策情報の公開に伴う悪用増加	2016年	8位
8位	ビジネスメール詐欺による金銭被害	2018年	7位
9位	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	5位
10位	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	10位

※IPA_情報セキュリティ10大脅威 2024を元に作成

脆弱性を狙われる対象

主にインターネットへ公開されている資産が狙われています



システム、ネットワーク、アプリケーション、プロセスにおけるセキュリティの弱点や欠陥を指します

ソフトウェアのバグ

プログラムコードのエラーや不具合が原因で、システムが予期しない動作をする場合があります。これにより、不正なコードの実行や情報漏洩が発生することがあります。

設定のミス

システムやネットワークの設定が不適切な場合、セキュリティホールに繋がります。例えば、デフォルトからパスワードを変更していない・必要以上のアクセス権を付与しているなどがあります。

認証と認可の問題

ユーザー認証やアクセス制御の実装が不適切な場合、未認証のユーザーや権限のないユーザーが機密情報にアクセスすることができます。

古いソフトウェアの使用

サポートが終了したり、アップデートが提供されていない古いソフトウェアを使用している場合、既知の脆弱性が悪用されるリスクが高まります。

ネットワークの弱点

ネットワークの構成や通信プロトコルに脆弱性が存在する場合、不正な侵入やデータの盗聴が行われる可能性があります。

物理的なセキュリティの欠如

サーバールームへのアクセス制御が不十分な場合や、重要なデータが保存されたデバイスが適切に保護されていない場合も、脆弱性となります。

どうしても発生してしまうバグや不備＝脆弱性が攻撃者にとって狙いやすい

パッケージのバグ

EC サイト構築パッケージ（プラグイン等の拡張機能を含む）や SaaS 型サービス を使って簡単にEC サイトやサービスが構築できるようになった。

一方で、パッケージ自体にバグが発生してしまうと、**パッケージを使って構築した全てのサイトやサービスが脆弱性を抱えることになり、狙われやすい。**

提供ベンダーの問題

アプリ開発の不備

人が作業を行うことで、どうしても見落としやコーディングミスが発生。

また進化する技術の実装（対応）のために常に技術的な知見を常に取り込む必要があり、その過程で脆弱性に気づかないケースが発生する。

知識や技術力、人力の限界

運用耐性の問題

自社構築サイトの中には**セキュリティ対策を想定していない、もしくは十分な費用をかけていないサイト**が数多く存在している。そのような EC サイトを狙っ た攻撃が増加している

セキュリティの優先度の低さ

多くのガイドラインで脆弱性対策として「第三者機関による脆弱性チェック」が推奨されています

クラウドサービス利用・提供における適切な設定のためのガイドライン（経産省）

Ⅲ．３．１．２ 【基本】設定項目の管理

設定項目の管理の仕組みとして、設定不備のリスクを顕在化させないための措置（予防的措置）と顕在化しても即時に対応できる措置（発見的措置）を実施できる体制を構築すること。

【ベストプラクティス】

i. 管理については、サードパーティやクラウドサービス事業者から提供される設定項目の可視化ツール等を利用する。
ii. 初期の設定だけでなく、設定値の監視の仕組み等を構築する。（予防的措置）
iii. 外部の設定値診断サービス等を活用して定期的に設定値の診断を行う。（予防的措置）
iv. 設定が変更されたことが検知されたら、なるべく早く適正な設定値に戻す、又は自動で復元する仕組みを組み込んでおく。（発見的措置）

IaaS/PaaS を利用している場合

v. 侵害テスト（ペネトレーションテスト）により、リスクのある設定不備を検出する（発見的措置）

※参照：経済産業省「クラウドサービス利用提供における適切な設定のためのガイドライン」
https://www.soumu.go.jp/main_content/000843318.pdf

ECサイト構築・運用セキュリティガイドライン (IPA 独立行政法人 情報処理推進機構)

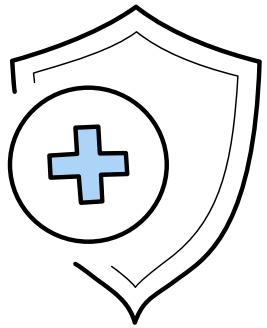
取組 2	自社に人材がおらず、外部委託先の活用により EC サイトを自社構築する場合は、セキュリティ構築および運用に関する対策要件の実施を外部委託先に遵守させる。
要件 3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。
要件 2	EC サイトの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。
要件 3	Web サイトのアプリケーションやコンテンツ、設定等の重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。

※参照：IPA「ECサイト構築・運用セキュリティガイドライン」
https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf

第三者による脆弱性診断の実施が求められています

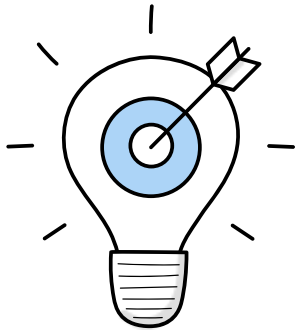
リスクの可視化により顕在・潜在リスクを対策することで、企業の信頼を得ることに繋がります

サイバー攻撃の脅威対策



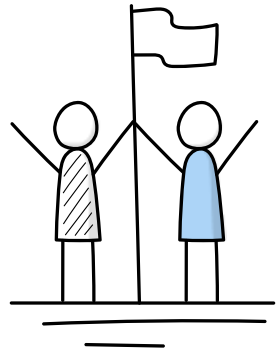
システムやアプリケーションに存在する脆弱性を特定、修正することでセキュリティホールを減らすことに繋がります。

潜在リスクの可視化



システムが直面する具体的なリスクを理解することで、発生しうるリスクを最小限に抑え、予防措置に繋がります。

法令・コンプライアンス遵守



脆弱性を可視化・対策することで国や業界団体や、取引先や親会社などが義務化・推奨するセキュリティ水準に対応することができます。

脆弱性診断の進め方　-事前準備から終了後の対応まで-

1．診断計画を立てましょう
2．診断体制を構築しましょう
3．診断の見積もりを行いましょう
4．環境設定などの準備を行いましょう
5．実施の周知・許可どりを行いましょう
6．診断後の是正対応を行いましょう

サービス・アプリ開発段階から脆弱性診断も含めて同時並行に進めていきましょう

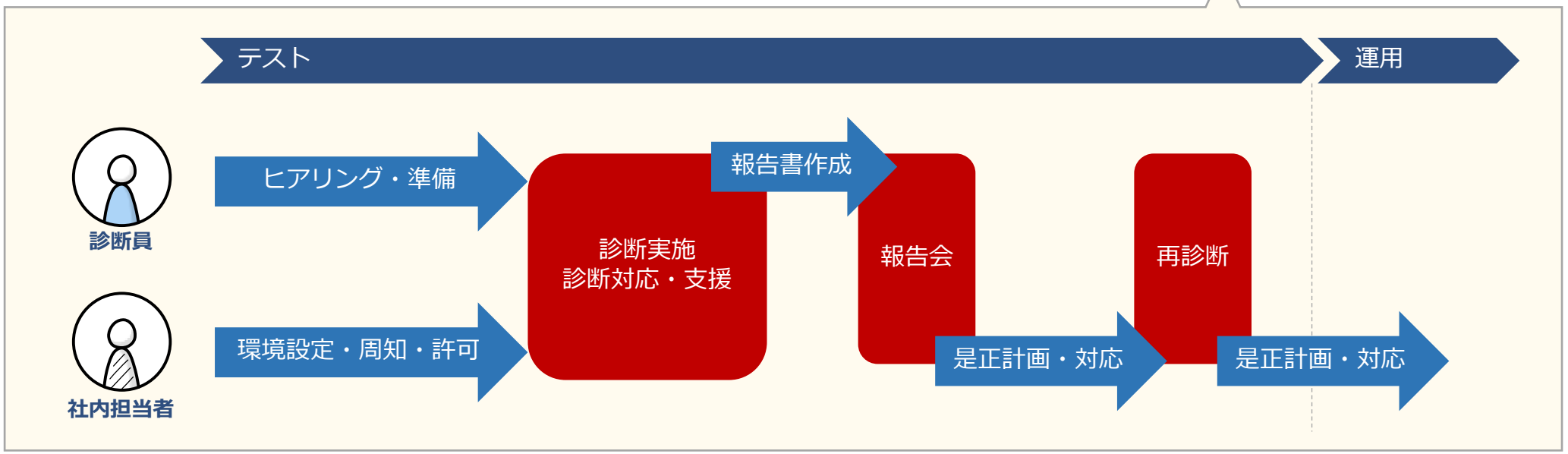
●開発スケジュール

計画 → 要件定義 → 設計 → 開発/実装 → テスト → 運用

●診断準備
- 社内診断担当者アサイン
- 想定対象／規模設定
- 概算診断費用取得
- 診断スケジュール設定

●診断確定
- 見積もり情報の確定
- 対象／規模の確定
- 診断費用の確定
- 診断スケジュール調整

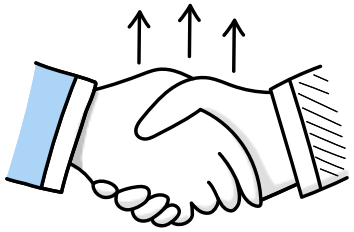
●診断実施
- 診断準備
- 診断実施
- 報告
- 是正対応／再診断



脆弱性診断を実施する前に、計画しておくと推進がスマートです

1

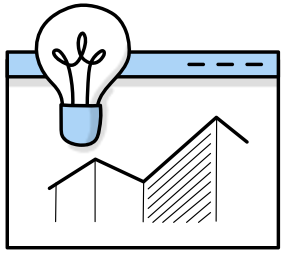
関係部署や担当者にアサイン



担当者を明確にすることで、脆弱性診断をスムーズに推進することに繋がります

2

診断予算の計上



あらかじめ開発・構築費の中に脆弱性診断の費用を組み込んでおくと必要な時に診断実施ができます

3

スケジュールを立てる

設計計画時に「テスト開始後に行う」など明確化すると、希望時期に実施ができます

最適な診断のタイミングで実施できるようにスケジュールを組みましょう

1

定期的・継続的な実施

脆弱性診断は一度行ったら安心ではありません。定期的に実施することが推奨されています。

2

新規システム導入時

自社の環境や利用方法なども踏まえ、自社開発以外のシステム導入時などでも実施を行う必要があります。

3

大規模な変更時

大規模な改修や変更を行った際は思わぬ脆弱性が発生することがあるため、実施を推奨します。

4

システムなどのアップデート時

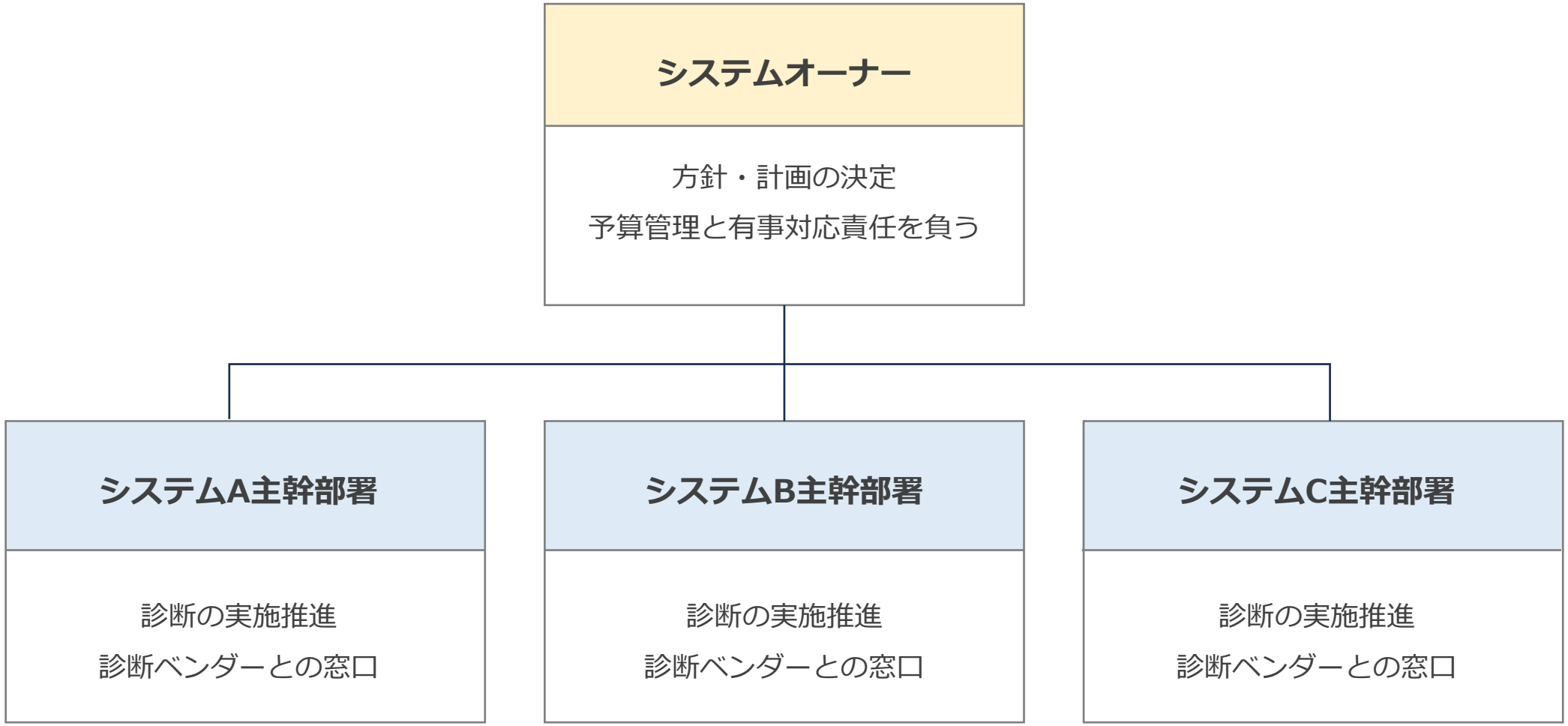
アップデートにより、コードや仕様が変更になることで、新たな脆弱性が発生することが考えられます。

5

セキュリティインシデント発生時

インシデントが発生した際、脆弱性が原因になるケースが想定されます。脆弱性診断をフォレンジックに活かせます。

関係者によるチーム化を実施、システムによって主幹が異なることがある場合、それぞれに体制を用意する



計画時に診断に必要なコストも確保することが重要！必要経費として前もって準備しておきましょう

☑ 「規模」や「対象機能数」などの把握

脆弱性診断は、実施するサービスやアプリケーションなどの規模や機能数、ページ数などにより数十万～数百万程度と幅が広いものになるため、範囲を把握しておきましょう。

☑ 「ツール診断」か「人による診断」か

「ツール診断」か「手動診断」かによっても費用感は大きく異なります。コストだけでなく、それぞれの違いや特徴を把握し、自社に合せた診断を選びましょう。

実施すべき主な診断メニュー

●Webアプリケーション診断

ECサイト、SNS などインターネットに公開するWeb アプリケーションの脆弱性を診断

●ネットワーク診断

ポート開放状況やOSS、ミドルウェアに既知の脆弱性がないか診断

●スマートフォンアプリケーション

スマートフォン用のアプリケーションに対し、セキュリティ上の脆弱性を診断

●クラウドセキュリティ診断

AWSやAzureなどのクラウドサービスに対し、CISベンチマークやベストプラクティスに基づいて診断

●ソースコード診断

開発されたソースコードに対し、静的な解析・診断

●ペネトレーションテスト

攻撃者の目線で疑似攻撃を実施、攻撃耐性をチェック

●ゲームセキュリティ診断サービス

急速に拡大する、ゲーム内のチート行為に対するセキュリティ対策を支援

●IoTセキュリティ診断サービス

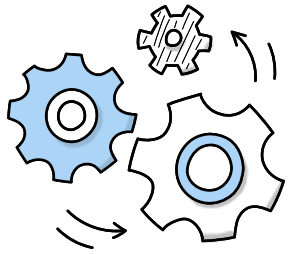
IoTシステムを構成するアプリケーションやプラットフォームなどのリスクを診断

権限付与や監視設定など、外部からのアクセスに備えた環境設定を行います

NO	内容	概要	ポイント・注意点
1	アクセス制限を許可する	診断元IPアドレスの許可など、疎通可能な状態にする	診断後は許可設定を戻すことを忘れないようにしましょう
2	監視設定から除外する	WAFやIPS/IDSなどの監視設定から、診断元IPアドレスを除外する	診断後は除外設定を解除することを忘れないようにしましょう
3	テストアカウントの用意	権限ごとに複数のアカウントの準備やアクセスに必要な証明書などの準備を行う	
4	テストデータの準備	テストデータを複数登録し、必要に応じて追加できるように準備する	
5	診断実施場所の確保（オンサイトの場合）	オンサイト診断時の診断作業スペースの確保や入館の許可などを手配する	
6	診断端末の準備（オンサイトの場合）	オンサイト診断時の端末の持込やネットワー接続などができない場合に備えた専用端末を用意しておく	
7	システムを稼働させるための機器準備	Web診断などでシステムを正常稼働させるためのシュミレーターなどを準備する	

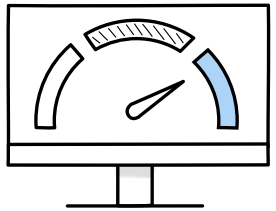
いざ実施が決まれば、トラブルにならないように関係部署に連絡・許可取りを行いましょう

システム主幹部署から診断員のアクセス許可を取得する



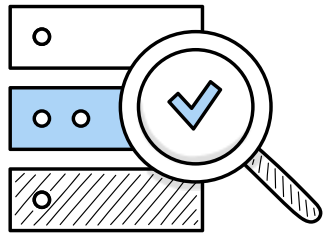
外部の人間がアクセスすることになるため、アクセス許可などの接続設定の変更を依頼する必要があります。

システム稼働関係者へ診断作業実施の連絡をおこなう



診断作業中に既存システムに影響するようなケースもあるため、調整が必要になる場合があります。

CSIRT・SOCへ診断作業実施の連絡を行う

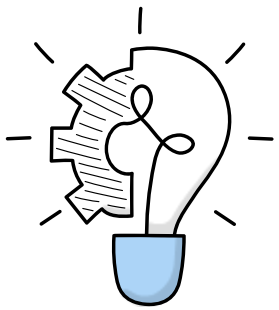


外部の人間がアクセスすることになるため、セキュリティの観点から、作業状況の記録などが発生する可能性があります。

診断のために許可した設定を元に戻し、診断結果を受けて是正計画を立てましょう

1

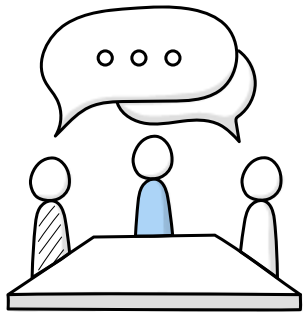
診断後の環境復元



診断担当は、監視除外設定やIPアドレス制限などの変更、診断ツールやデータの削除などを実施

2

是正計画の立案



診断結果を受け、関係者と対策方針を策定する。是正後は、診断員に再診断を再度依頼する

<是正のポイント>

多くの脆弱性が発生することがあります。診断ベンダーと相談し、脆弱性レベルに合わせて優先順位をつけて対応することをおススメします。

<MOTEXの診断例>

High：直ちに是正対策を実施
Medium：　1か月以内に改善
Low：半年以内の改善
Information：必要に応じて実施

参考：よくあるご質問と対応例

フェーズ	ご質問	対応例
計画/見積	まだ画面設計の段階でサイトができていないのですが、お見積り可能でしょうか？	画面イメージや遷移図をいただくことでお見積り可能です。また、診断リソースが豊富ですので、診断期間については開発スケジュールに合わせて柔軟に変更いたします。
	キックオフにて診断対象の認識を合わせたいのですが、対象の妥当性に自信がもてないです。他に診断した方がよい画面はないですか？	追加発注が難しい場合や、スケジュール的に対象の追加が難しい場合には、診断員の判断で対象画面の入れ替えを行い、見積もり範囲内でサービス提供できるように調整することも可能です。
	アクセス制限されてるシステムは、診断する必要はありますか？	診断を想定しているシステムの構成図やユースケース図を拝見させていただくことで、簡単な脅威分析も可能です。その結果を基に、診断実施の有無をお客様にてご判断いただければと思います。
診断結果確認	検出された脆弱性に対して、プロジェクト側に対策を渋られて困っておりまして、対策の必要性などを補足いただくことは可能ですか？	事前にご相談いただければ、環境を考慮した上での攻撃経路の推測や、当該脆弱性による悪用の事例紹介等、プロジェクト側に危機感を持っていただくような報告を行うことも可能です。また、対策しない理由の妥当性を確認することも可能です。
	指摘を改修する意思はあるが、指摘が大量にありすぎてどこから手を付けるべきか、良いアイディアはありますか？	基本的には「危険度が高く」「アクセスが多い箇所」、つまりリスクが高い箇所から優先的に対処すべきだと考えております。背景や経緯を考慮したアドバイスが必要であれば、サポートすることもできる可能性があるので、別途ご相談ください。
脆弱性の改修	脆弱性への対策方針を決めたいのですが、再診断にて指摘を受けないか不安です。	脆弱性の改修方法について不安な点や不明な点がありましたらご相談ください。詳細な実装までは回答できない場合もございますが、可能な限り対応させていただきます。なお、対策によっては指摘自体は修正されるものの、新たな指摘の原因となるケースもあります。特に、報告書に記載されていないようなイレギュラーな対策をされる場合に新たな脆弱性が埋め込まれる傾向にありますので、不安な場合にはお気軽にご相談ください。
	システムの都合上、報告書記載の対策が実施できないのですが、どうすればよいでしょうか？	代替策をご提案することも可能ですので、お気軽にお問合せください。また、根本的な対策が実施できない場合でも脆弱性が悪用されるリスクを可能な限り低くするための代替コントロールをご提案させていただきます。

エムオーテックスの脆弱性診断

LANSCOPEプロフェッショナルサービス

巧妙化するサイバー攻撃や脆弱性などの最新脅威に対しセキュリティプロフェッショナルの知見で対抗

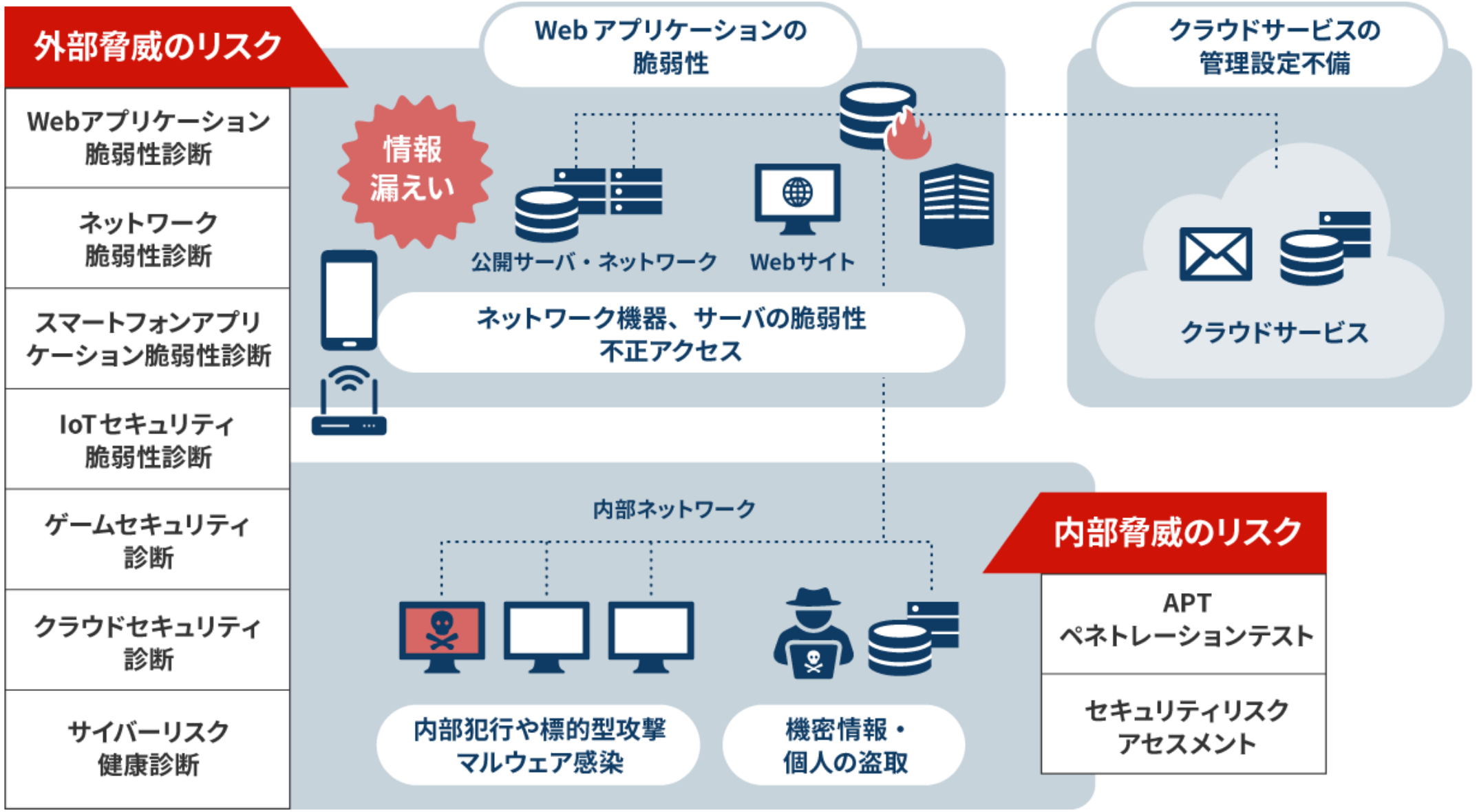
LANSCOPE
Professional Service

最新の攻撃手法と最適な対応策を探求したセキュリティエンジニアが、Web・ネットワーク・クラウドなどを診断。脆弱性の有無をチェックし、オリジナルレポートを提出します。検出されたリスクの解説や、具体的な対策案もご提案します。

- 人による柔軟で細やかな診断で12,000件以上の実績
- 全3カテゴリ13種類の脆弱性診断
- リピート率90%以上！柔軟性と技術力に高い評価

https://www.lanscope.jp/professional-service/

MOTEXのセキュリティ診断の領域とは



サービス一覧

Webシステム・アプリ提供者/開発者様向け

<Web>

- Webアプリケーション脆弱性診断サービス
- Webペネトレーションテストサービス
- ソースコード診断サービス

<ネットワーク>

- ネットワーク脆弱性診断サービス
- ネットワークペネトレーションテストサービス

<IaaS>

- クラウドセキュリティ診断サービス (IaaS 系)

<スマホ>

- スマートフォンアプリケーション脆弱性診断サービス

情報システム担当者様向け

- APTペネトレーションテストサービス
- クラウドセキュリティ診断サービス(SaaS 系)
- サイバーリスク健康診断サービス

その他のサービス

- ゲームセキュリティ診断サービス
- IoTセキュリティ診断サービス

貴方に最適な「MOTEX脆弱性診断」が分かるフローチャート

START

インターネットに
公開しているものは？

Webサイト

ECサイトなど
顧客情報を取り扱うサイトだ

NO

サイトやサーバに対する脅威があるか傾向を把握したい！

Webアプリケーション健康診断
ネットワーク健康診断

YES

サイトの構成は？

1. Webアプリケーションのみ
2. Webアプリケーション＋サーバー
3. Webアプリケーション
   サーバー（Windows、Linux）
   インフラ系クラウド（AWS・Azure）

1

サイトの改ざん・顧客データの漏洩対策をしたい！

Webアプリケーション脆弱性診断

2

サイト改ざん・情報漏洩・サーバダウン・踏み台リスクを把握したい！

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

3

アプリから基盤までシステム全体のセキュリティチェックしたい！

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
クラウドセキュリティ診断

リモートアクセス
（VPN機器、RDPサーバ）

システムのセキュリティアップデートができているか心配！

ネットワーク脆弱性診断

オフィスツール系の
クラウドサービス
（Microsoft 365など）

外部への公開設定ミスなど、情報漏洩リスクが気になる！

クラウドセキュリティ診断

部門運営のシステム
グループ会社のシステムなど

攻撃を受けやすい度合いは？未把握の資産を洗い出し！

サイバーリスク健康診断

サービス詳細

サービス	診断カテゴリ	診断対象	見つかるリスク
Webアプリケーション脆弱性診断サービス ホームページや ECサイト、SNS などインターネットに公開する Web アプリケーションの脆弱性を診断します	Web アプリケーション	Web サーバー / Web アプリケーション	Web アプリケーションの脆弱性 （XSS, SQLインジェクション、認証周りの脆弱性等）
Webペネトレーションテストサービス ※詳細はお問い合わせください Webアプリケーションに対し、脆弱性を悪用したサーバへの侵入や個人情報などの重要情報窃取ができないか調査します	Webアプリケーション/ネットワーク	Web サーバー / Web アプリケーション	Webアプリケーションの脆弱性を突いた侵入リスク
ソースコード診断サービス ※詳細はお問い合わせください Webアプリケーションやスマートフォンアプリケーションのソースコードを静的解析し、脆弱な実装がないかを診断します	ソースコード	アプリケーションのソースコード	アプリケーションの内在するソースコードレベルの脆弱性
ネットワーク脆弱性診断サービス 診断対象のサーバーやネットワーク機器がもつ IP アドレスに対して、稼働するOSやミドルウェアの脆弱性等を診断します	ネットワーク	Web サーバー/ ルーター / DNS サーバー Mail サーバー / FireWall 等	ミドルウェアの脆弱性　（Apache、IIS / sendmail / bind 等） サーバー OS の脆弱性　（Windows / Linux 等）
ネットワークペネトレーションテストサービス 診断対象のサーバーやネットワーク機器がもつ IP アドレスに対して、稼働するOSやミドルウェアの脆弱性を利用した侵入のリスクを診断します	ネットワーク	Web サーバー/ ルーター / DNS サーバ Mail サーバー / FireWall 等	対象サーバーやネットワーク機器の脆弱性を突いた侵入リスク
クラウドセキュリティ診断サービス 対象クラウドサービスの管理画面上の設定に対して、問題のある設定や脆弱な設定の有無をヒアリング及び診断します	クラウドサービス	AWS / Azure / Google Cloud Platform / Microsoft 365 / Box / Zoom /Slack /　Salesforce /Google WorkSpace	管理設定ミスによるリスク （基本認証・多要素認証・ユーザー権限の設定等）
スマートフォンアプリケーション脆弱性診断サービス スマートフォン用のアプリケーションに対し、セキュリティ上の脆弱性を診断します	スマートフォン	スマートフォンアプリ / Webview・API	スマートフォンアプリ（クライアントアプリ）側 およびWebview・API側の脆弱性（認証の脆弱性等）

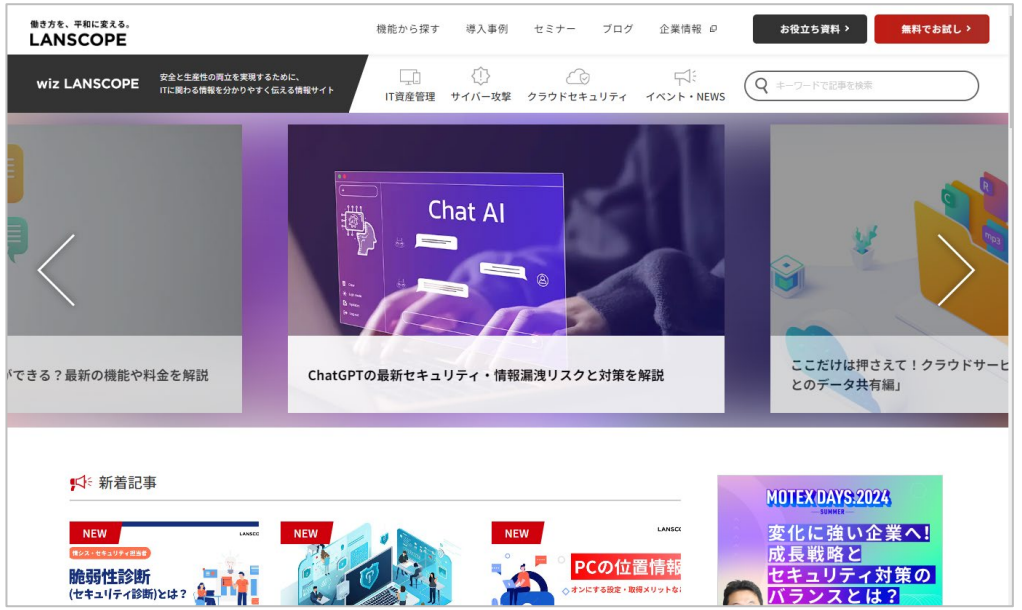
気になる診断があったら･･･

セキュリティ診断ソリューションサイト

エムオーテックスのセキュリティ診断をご紹介したソリューションサイトです。
診断の概要や、お見積り、お役立ち資料などを掲載しています。

https://www.lanscope.jp/professional-service/

WizLANSCOPE（ブログ）



安全と生産性の両立を実現するためにITに関わる情報を分かりやすく伝える情報サイトです。診断員による脆弱性やセキュリティ診断に関する記事も掲載されています。

https://www.lanscope.jp/blogs/

エムオーテックスの診断の特長

安心のサービス提供実績

充実の提供実績

実績**12,000**件以上

サービス提供開始から20年、
蓄積されたナレッジ・ノウハウにより
お客様の様々なニーズに合わせた
確かなサービスを提供します。

サイバーセキュリティ国家資格取得

60名以上

サイバーセキュリティの難関国家資格
である「情報処理安全確保支援士」が
多数在籍しています。
幅広い知見を生かし、質の高い診断を
提供いたします。

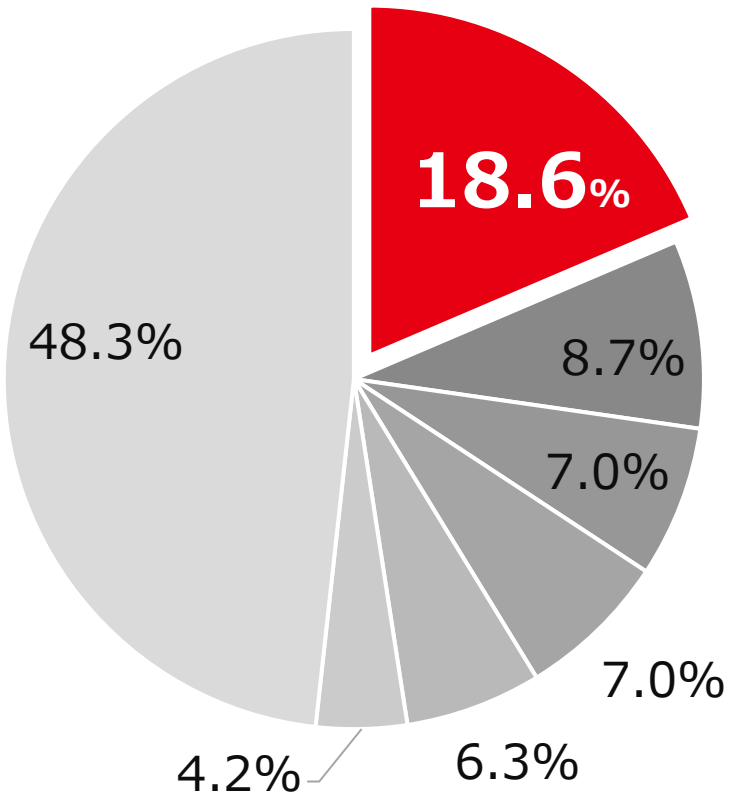
高いリピート率

90%

診断の丁寧さや提示する報告書に
ご満足いただき、毎年多くのお客様から
リピートの診断のご相談があります。

パブリッククラウド向け脆弱性診断サービスにおいてシェアNO.1獲得※

パブリッククラウド向け脆弱性診断サービス／CSPMサービス市場
通信業：ベンダー別売上金額シェア（2023年度予測）



LANSCOPE
Professional Service

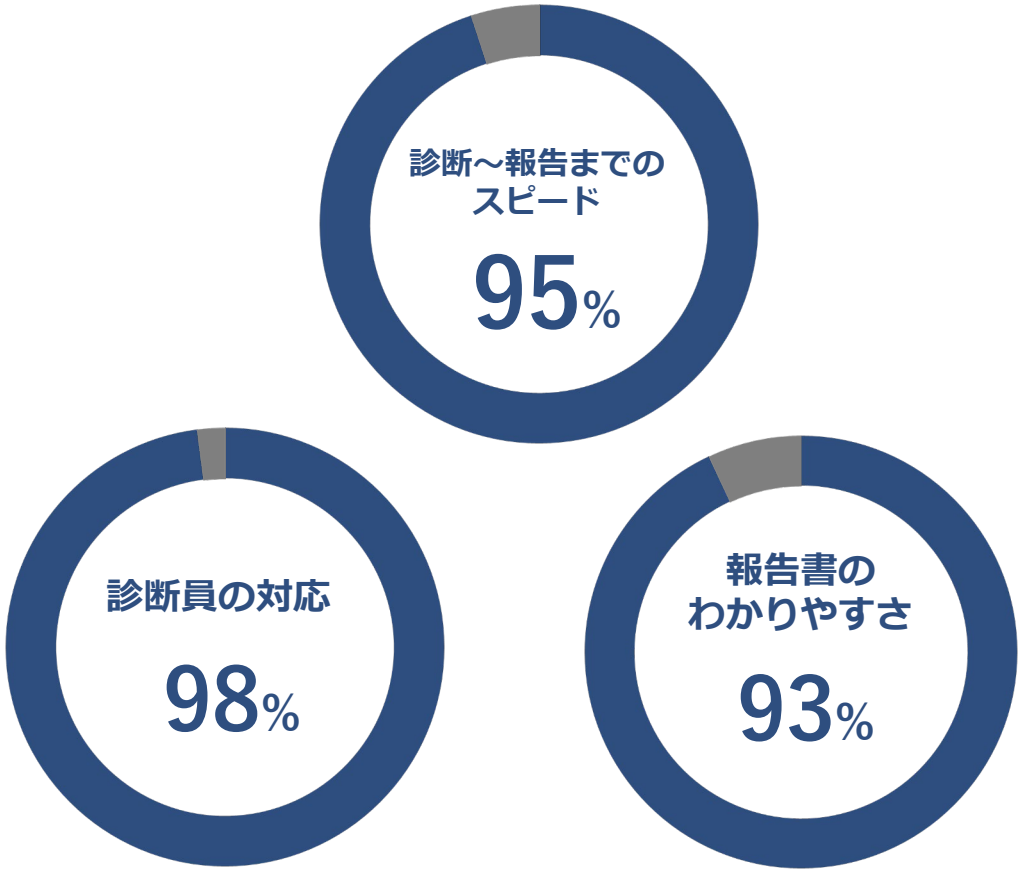
クラウドセキュリティ診断パッケージ

IaaS
AWS / Microsoft Azure / GCP

SaaS
Microsoft 365 / Box / Zoom
Salesforce / Slack
GoogleWorkspace

※ITR「ITR Market View：サイバー・セキュリティ・コンサルティング・サービス市場2023」パブリッククラウド向け脆弱性診断サービス／CSPMサービス市場－通信業：ベンダー別売上金額シェア（2023年度予測）

「最適で柔軟なサービス提供」「スピーディーな診断」「対話重視のサポート」
MOTEX の診断サービスは高い満足度を頂いています



※ 診断サービスを受けたお客様のアンケート結果より

IT会社
開発部門様

危険度の高い脆弱性(アクセス制御、権限昇格、なりすまし等)が診断によって複数検出された。

報告書の内容も分かりやすく、スムーズに改修対応ができた。

メーカー会社
情報システム部門様

各部門との窓口や診断結果の取りまとめ、報告までを一括で対応してもらえたのが助かった。
診断にかかる各種QA対応まで迅速に対応してもらえ、大幅な工数削減になった。

IT会社
開発部門様

最新の脆弱性についても即時に情報を収集・診断項目に反映されていた。脆弱性の公表からわずか2週間で、該当の脆弱性についても検査してもらい、問題ないことが分かり安心した。

診断項目の策定について

定期的にインシデント情報や脆弱性などを収集、解析し、適宜、診断ルールに反映しております。

JPCERT , NISC , IPA	OWASP	PCIDSS , JNSA , WASF	海外セキュリティメーカー
インシデントに関する 技術情報の収集 ※IPA10大脅威選定委員	安全なWebサイトを 構築するための情報共有	セキュリティ協議会に 参画による情報収集	新たな脅威・脆弱性ルールの共有 日本特有の脆弱性ルールの フィードバック

各種協会・団体からの情報収集

<セキュリティイベント>

最先端の攻撃情報の収集

<診断チーム>

診断ルールの検討
自社ツール開発

<研究機関>

最新のセキュリティ動向を踏まえた診断

定期的に診断項目を見直し、常に最新のセキュリティ基準での診断を実施致します

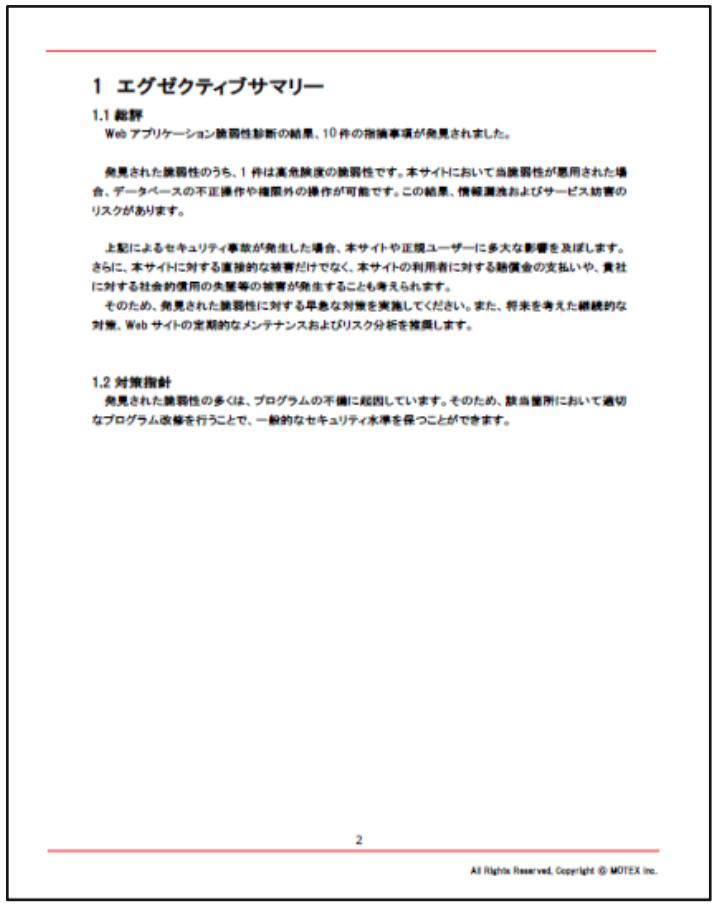
※緊急性の高い脆弱性については随時、診断全体については半期に一度見直しております

下記のセキュリティ基準を満たす診断項目にて、高品質の診断サービスを提供しています。

基準名	概要
OWASP	セキュアなアプリケーションの開発・購入・運用を推進するために作られた、オープンコミュニティ。 世界各国のセキュリティ専門家が参加し、先進的な研究を行っており、世界的なセキュリティ基準として参考とされております。
IPA **安全なWebサイトの作り方**	IPAへの届出件数の多い脆弱性や危険度が高い脆弱性を引用した、開発者が安全なウェブサイトを作成するためのガイド文書。 アプリケーションを開発する上で、基本的なセキュリティ基準とされています。
PCIDSS	クレジットカードブランド5社が、セキュリティリスクの効果的な低減を目的として共同策定した、 カード情報保護のための統一的な国際セキュリティ基準。
Androidアプリのセキュア設計・ **セキュアコーディングガイド**	日本スマートフォンセキュリティ協会が立ち上げたセキュアコーディングのワーキンググループが作成した、 Android アプリケーションのセキュア設計、セキュアコーディングのガイド文書。
CISベンチマーク	セキュリティの促進を目的とした米国の非営利団体が随時公開している、 ソフトウェアやクラウドサービスに対するセキュリティ基準

報告書サンプル

エグゼクティブサマリー
(総評、対策指針)



1 エグゼクティブサマリー

1.1 総評

Web アプリケーション脆弱性診断の結果、10 件の指摘事項が発見されました。

発見された脆弱性のうち、1 件は高危険度の脆弱性です。本サイトにおいて当脆弱性が悪用された場合、データベースの不正操作や権限外の操作が可能です。この結果、情報漏洩およびサービス妨害のリスクがあります。

上記によるセキュリティ事故が発生した場合、本サイトや正規ユーザーに多大な影響を及ぼします。さらに、本サイトに対する直接的な被害だけでなく、本サイトの利用者に対する賠償金の支払いや、貴社に対する社会的信用の失墜等の被害が発生することも考えられます。

そのため、発見された脆弱性に対する早急な対策を実施してください。また、将来を考えた継続的な対策、Web サイトの定期的なメンテナンスおよびリスク分析を推奨します。

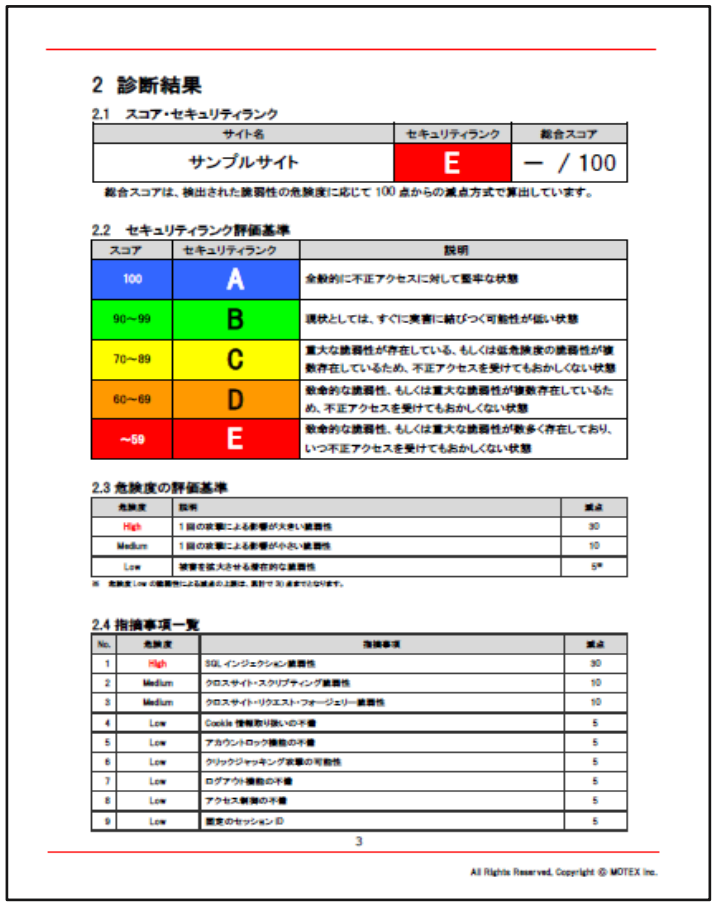
1.2 対策指針

発見された脆弱性の多くは、プログラムの不備に起因しています。そのため、該当箇所において適切なプログラム改修を行うことで、一般的なセキュリティ水準を保つことができます。

2

All Rights Reserved, Copyright © MOTEX Inc.

診断結果
(スコア・セキュリティランク)



2 診断結果

2.1 スコア・セキュリティランク

サイト名	セキュリティランク	総合スコア
サンプルサイト	E	ー / 100

総合スコアは、検出された脆弱性の危険度に応じて 100 点からの減点方式で算出しています。

2.2 セキュリティランク評価基準

スコア	セキュリティランク	説明
100	A	全般的に不正アクセスに対して堅牢な状態
90～99	B	現状としては、すぐに実害に結びつく可能性が低い状態
70～89	C	重大な脆弱性が存在している、もしくは低危険度の脆弱性が複数存在しているため、不正アクセスを受けてもおかしくない状態
60～69	D	致命的な脆弱性、もしくは重大な脆弱性が複数存在しているため、不正アクセスを受けてもおかしくない状態
～59	E	致命的な脆弱性、もしくは重大な脆弱性が数多く存在しており、いつ不正アクセスを受けてもおかしくない状態

2.3 危険度の評価基準

危険度	説明	減点
High	1 回の攻撃による影響が大きい脆弱性	30
Medium	1 回の攻撃による影響が小さい脆弱性	10
Low	被害を拡大させる潜在的な脆弱性	5※

※ 危険度 Low の脆弱性による減点の上限は、合計で 30 までとなります。

2.4 指摘事項一覧

No.	危険度	指摘事項	減点
1	High	SQL インジェクション脆弱性	30
2	Medium	クロスサイト・スクリプティング脆弱性	10
3	Medium	クロスサイト・リクエスト・フォージェリー脆弱性	10
4	Low	Cookie 情報取り扱いの不備	5
5	Low	アカウントロック機能の不備	5
6	Low	クリックジャッキング攻撃の可能性	5
7	Low	ログアウト機能の不備	5
8	Low	アクセス制御の不備	5
9	Low	固定のセッション ID	5

3

All Rights Reserved, Copyright © MOTEX Inc.

指摘事項詳細
(説明・リスク・対処方法)

3 指摘事項詳細

凡例

No 指摘事項	
検査区分	検査区分名
検査項目	検査項目名
検出手法	指摘事項を検出した診断方法(マニュアル診断、もしくはツール診断)
危険度	指摘事項の危険度(High、Medium、Low)
攻撃難易度	発見された指摘事項を利用する攻撃の難易度(易、難)
説明	
指摘事項の説明。	
検証例	
指摘事項の攻撃方法、もしくは検証方法の解説と例。	
対策	
指摘事項への対策方法。	
該当箇所	
脆弱性が検出されたプログラムやファイル。 No.は 4.3 診断対象一覧の No.に対応。	

【例】

No.	画面名※1	アクション(通信の送信先 URL)※2	パラメータ※3
1	トップ	http://sample.motex.co.jp/cgi-bin/search.cgi	keyword
2	ログイン	http://sample.motex.co.jp/cgi-bin/login.cgi	login
		http://sample.motex.co.jp/cgi-bin/login2.cgi	Pass

※対象画面の URL は 4.3 診断対象一覧に記載しています。

～該当箇所のイメージ～

【画面名※1】

6

All Rights Reserved, Copyright © MOTEX Inc.

本資料に関するお問い合わせ

■ マーケティング本部
プロダクトマーケティング部
E-mail　product@motex.co.jp

ご導入後の製品利用に関するお問い合わせ

サポートセンター　0120-968995 （携帯・PHSからは06-6308-8981）
お電話受付時間　9:30～12:00/13:00～17:30（平日、祝祭日除く）
Email お問い合わせ　support@motex.co.jp