LANSCOPE
Professional Service

3分で分かる！
Webアプリケーション
脆弱性診断のご案内

Webアプリケーションの脆弱性を狙った脅威の増加

- Webアプリケーションの脆弱性を狙った脅威
- 攻撃の半数は脆弱性や設定不備が入口に
- 推奨される「第三者機関による脆弱性チェック」

Webアプリケーションの脆弱性を狙った脅威の増加

クロスサイトスクリプティングによる情報搾取

Webアプリケーションの脆弱性を突いて不正なスクリプトを埋め込み、利用者の入力情報を搾取。クレジットカード情報などの個人情報漏洩が発生

SQLインジェクション攻撃による情報流出

Webサイトの「Q&Aシステム」に対し、SQLインジェクション攻撃が行われ、約2,000件のメールアドレスが流出

OSコマンドインジェクションによるWebサーバー侵害

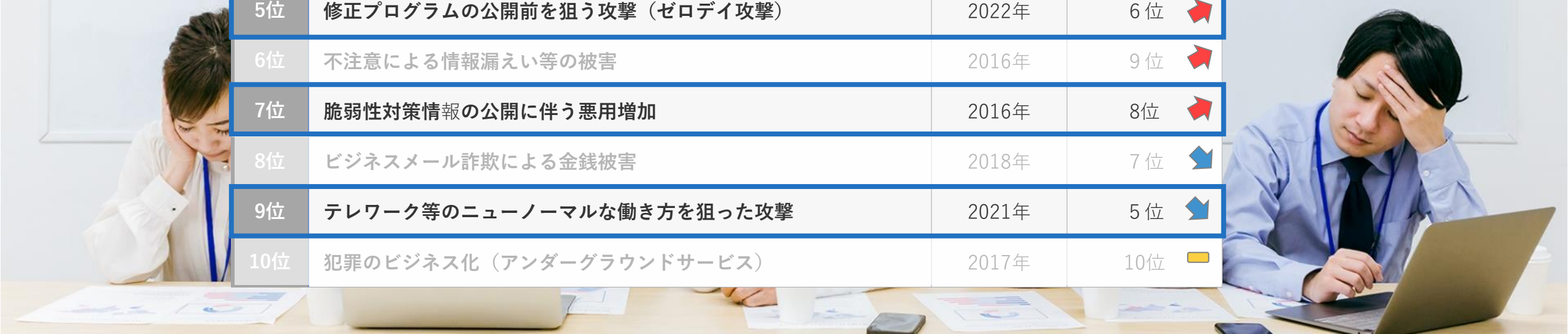
Webアプリケーションの設計上の不備を利用しWebサーバーが攻撃者の制御下に。ファイルの改ざん、削除、流出などの被害

攻撃の半数は脆弱性や設定不備が入口に！

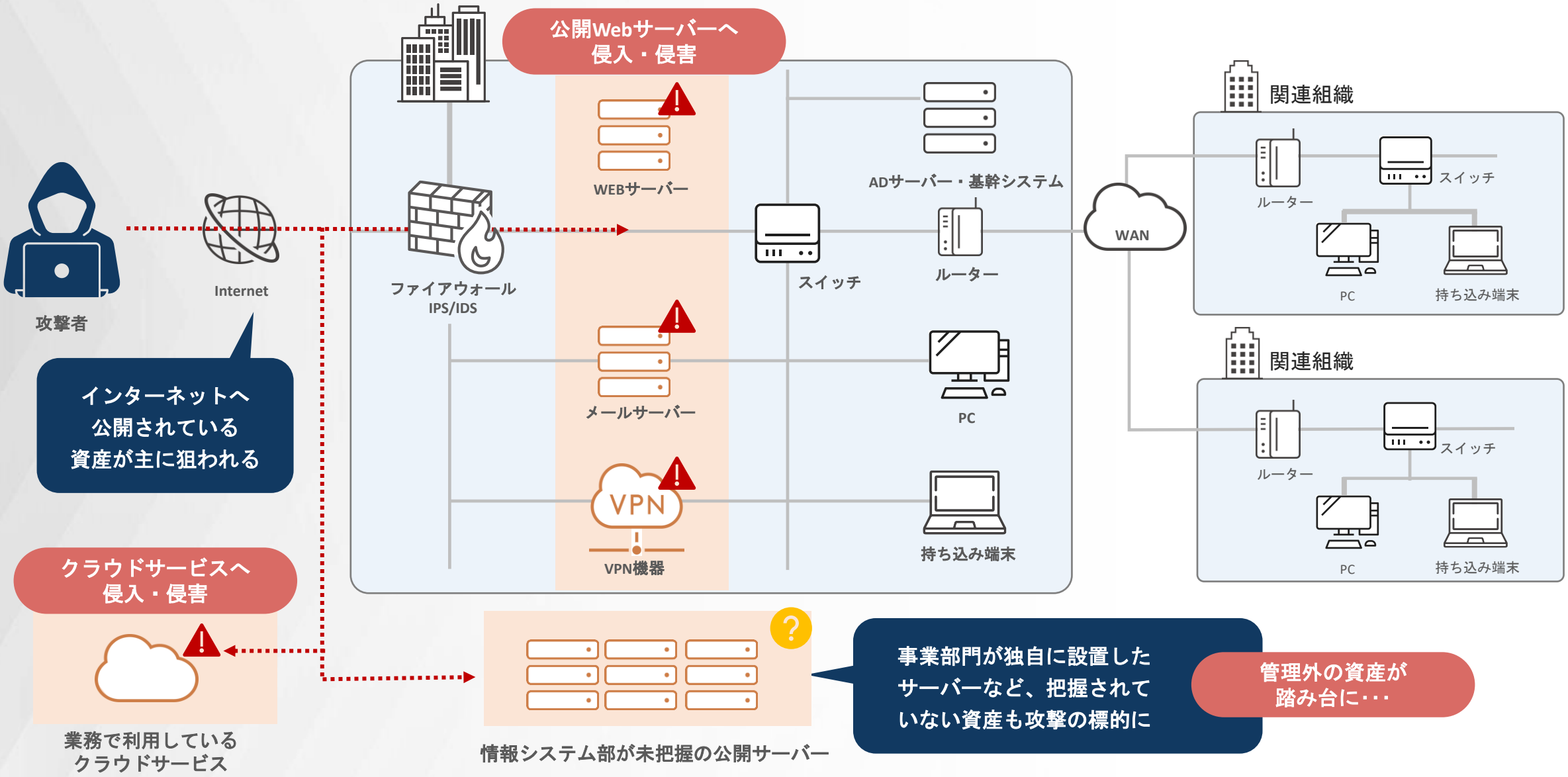
半数が
脆弱性や設定不備
が攻撃の糸口に

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



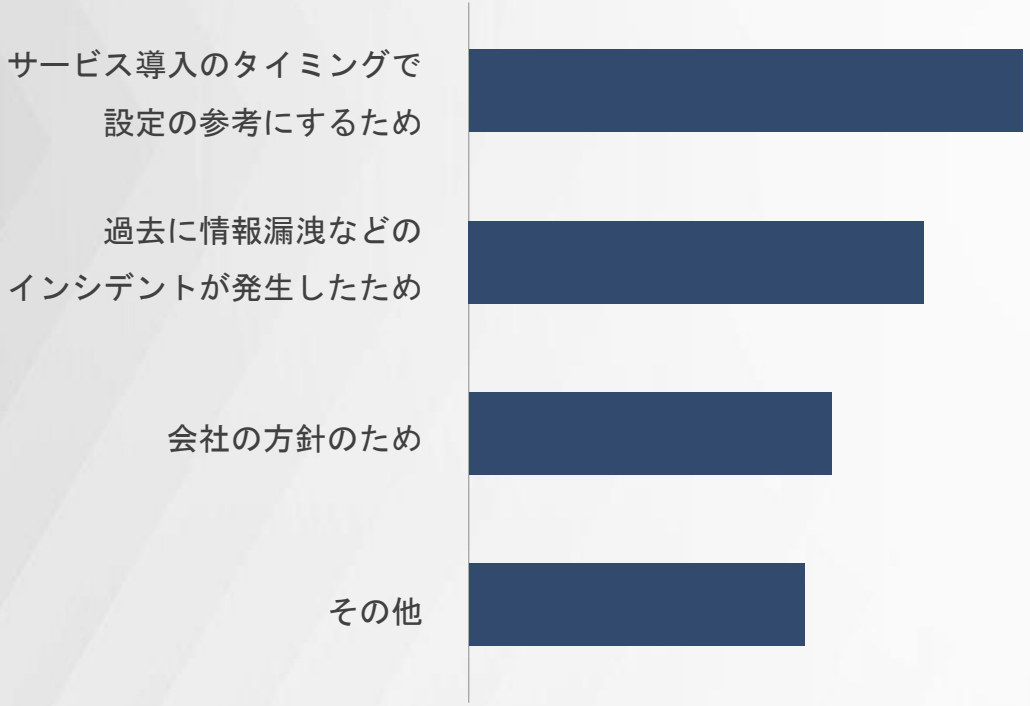
インターネット上の公開資産には、さまざまなリスクが潜んでいます



実際の診断現場でも危険度の高い脅威が多く検出！

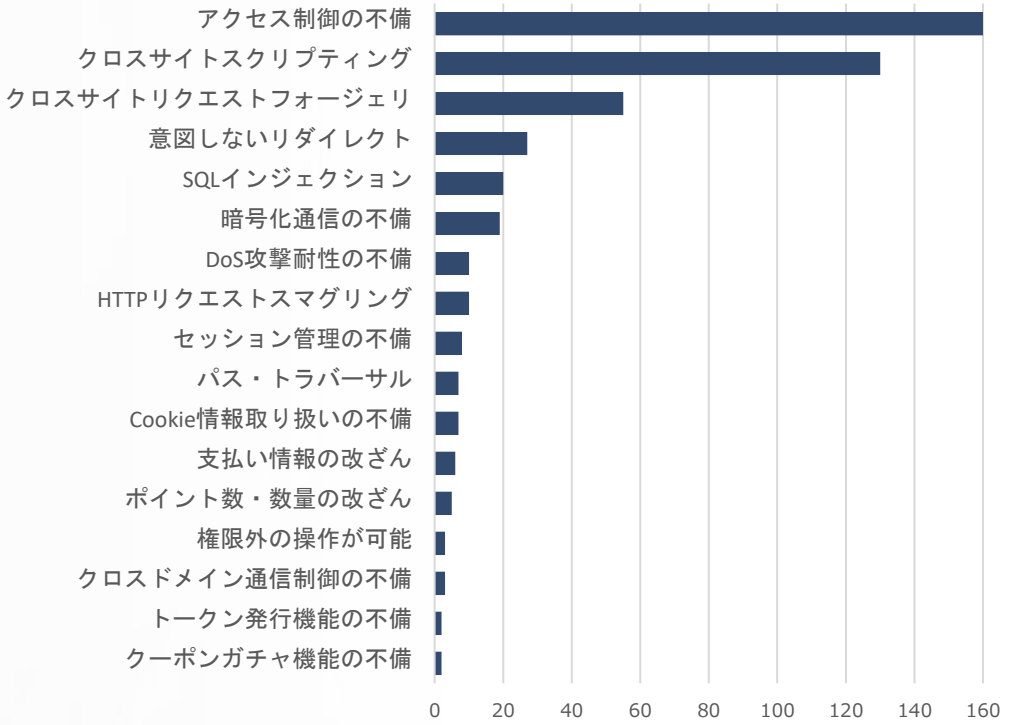
サービス導入時やインシデント発生を受けて、脆弱性診断サービス等を受けるケースが増えています。

第三者による脆弱性診断サービスを受けたきっかけは？



※エムオーテックスアンケート（N：339）

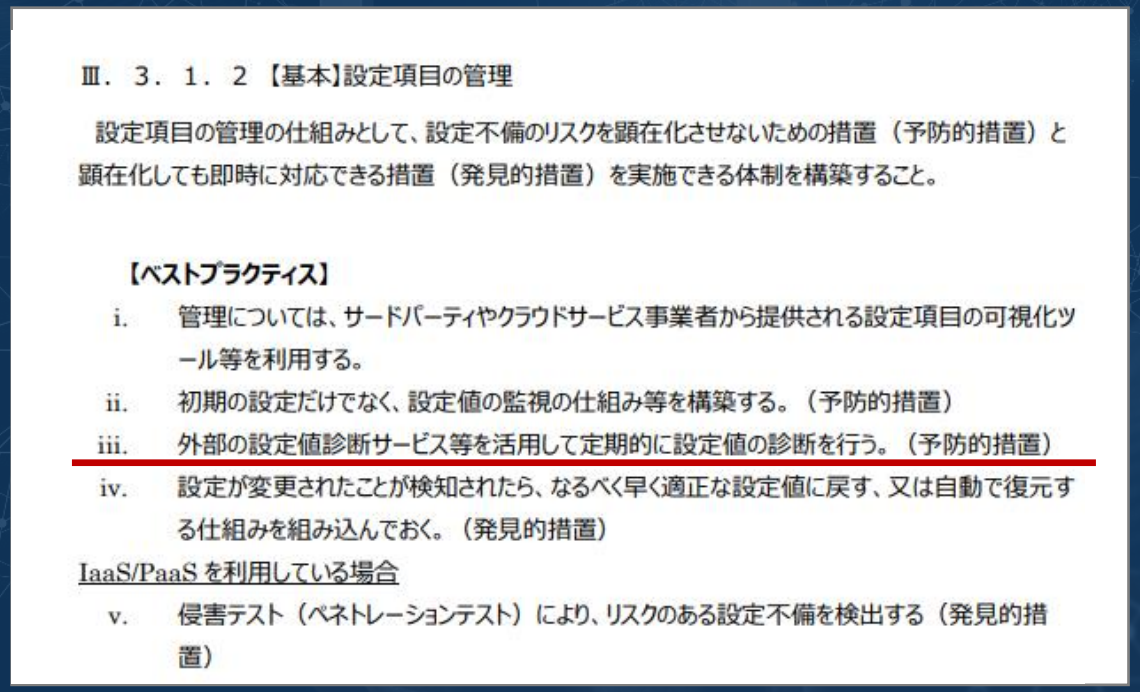
MOTEXが脆弱性診断を実施した際によく検出される脆弱性は？



※MOTEX Professional Service Webアプリケーション脆弱性診断実績より算出

推奨される「第三者機関による脆弱性チェック」

官庁や各業界のセキュリティガイドラインで「第三者機関による脆弱性チェック」が推奨されています



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）

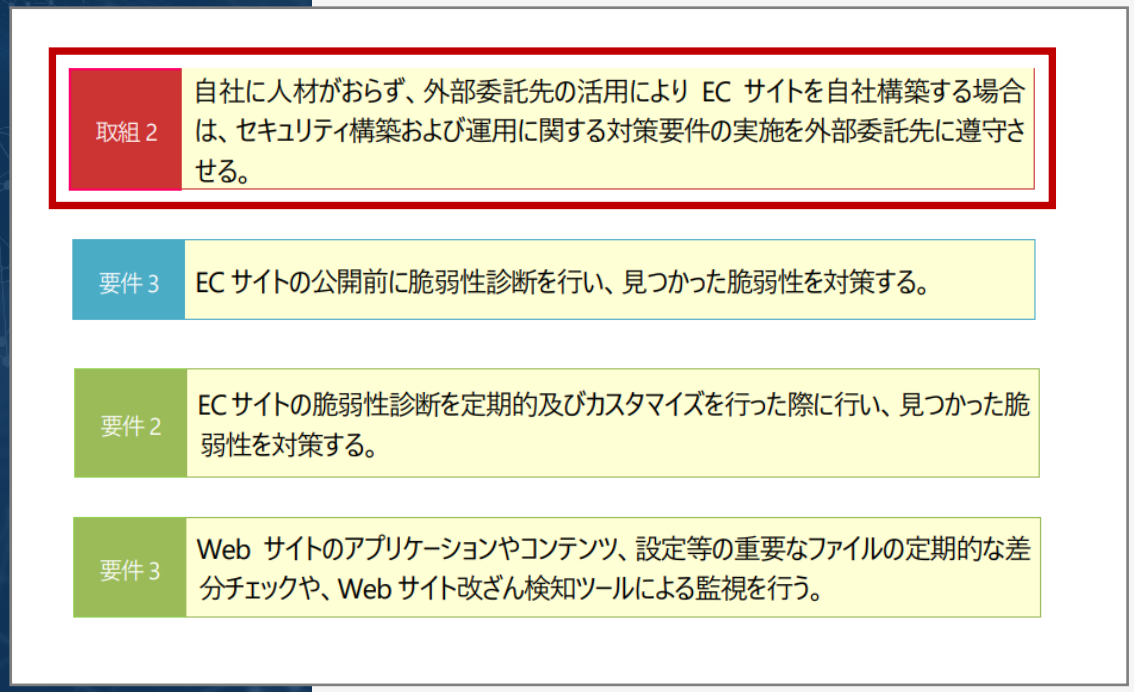
iii. 外部の設定値診断サービス等を活用して定期的に設定値の診断を行う。（予防的措置）

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



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://v 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

MOTEX Professional Service

Webアプリケーション脆弱性診断

- MOTEXのWebアプリケーション脆弱性診断とは
- 診断の流れ
- MOTEXの脆弱性診断選ばれる理由
- ユーザー事例

こんな課題はありませんか？

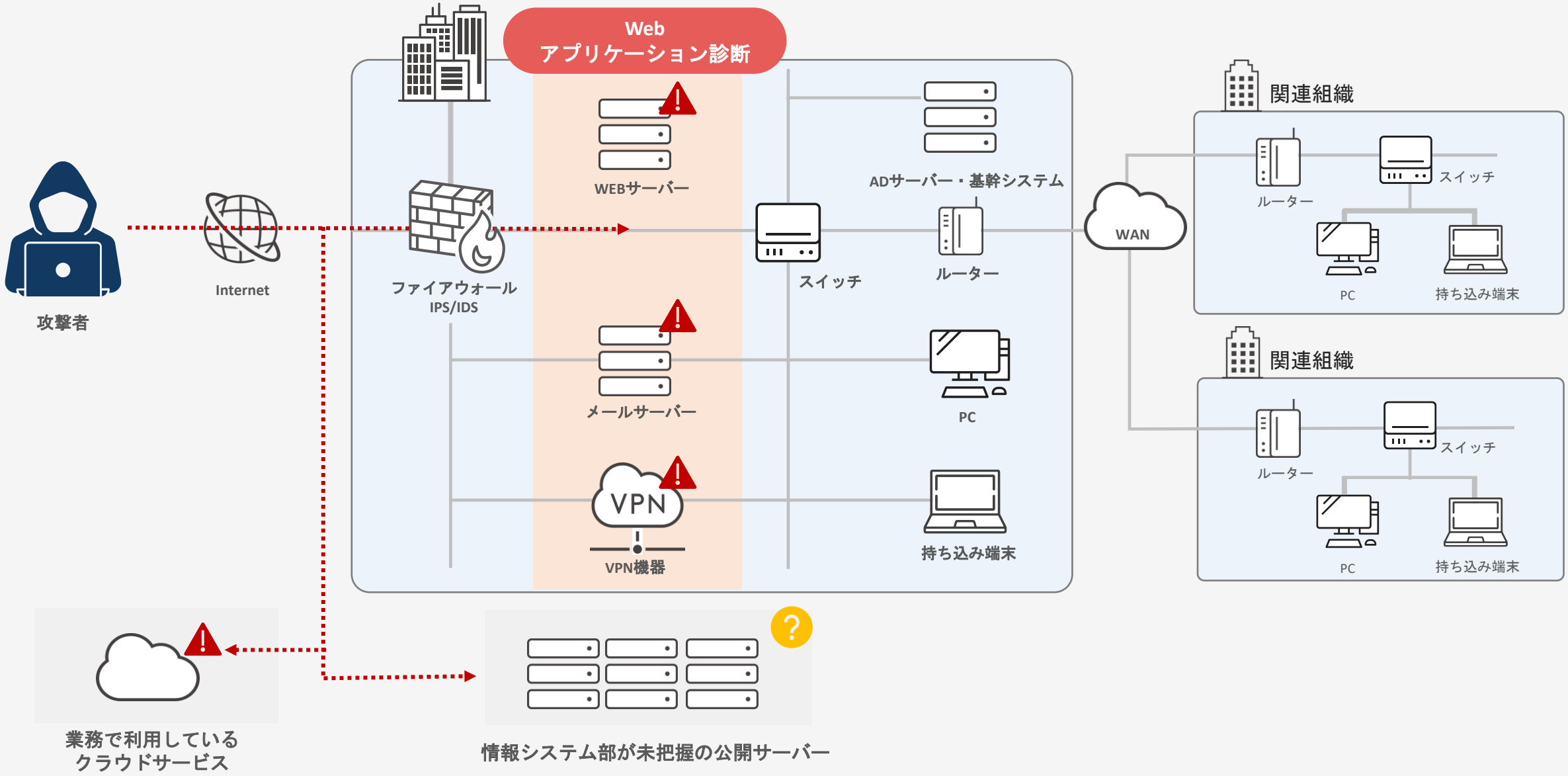
公開資産であるWebアプリケーションやサーバーに対してサイバー攻撃が増加しています

開発中のWebサービスが遅れそう！
リリース日までに診断をする
時間が取れるか心配

他社のサイトが改ざんされる
事故を受けて
自社は大丈夫か心配

新規取引先から
脆弱性診断の要件仕様が届いたが
自社のノウハウがない

公開されているWebサーバに対して脆弱性診断が可能です



MOTEX Professional Service Webアプリケーション脆弱性診断とは

難関国家資格である情報処理安全確保支援士を取得したセキュリティエンジニアが、セキュリティリスクの有無をチェックします。診断後はオリジナルレポートを提出。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。

できること 1

セキュリティリスクに繋がる
脆弱性や設定ミスを調査

できること 2

診断結果を解説する
報告会を実施※

できること 3

診断結果を踏まえた
対策を助言

できること 4

短納期や定期診断※にも
効率的に対応できる診断体制

※メニューやプランにより異なります

Webアプリケーションのセキュリティリスクを効果的に把握できます

Web アプリケーション脆弱性診断

概 要

企業の**Webサイト**や**ECサイト**は、世界中からのアクセスが可能であるため、攻撃の標的になりやすく、セキュリティ上の弱点があると、**顧客情報の流出や不正サイトへの誘導**などの**改ざんリスク**が生じます。この診断では、**Webアプリケーション**の脆弱性を調査し、対策方法をレポートで提案します。

見つかるリスクの一例

セキュリティ設定の不備
によるサイトの改ざん

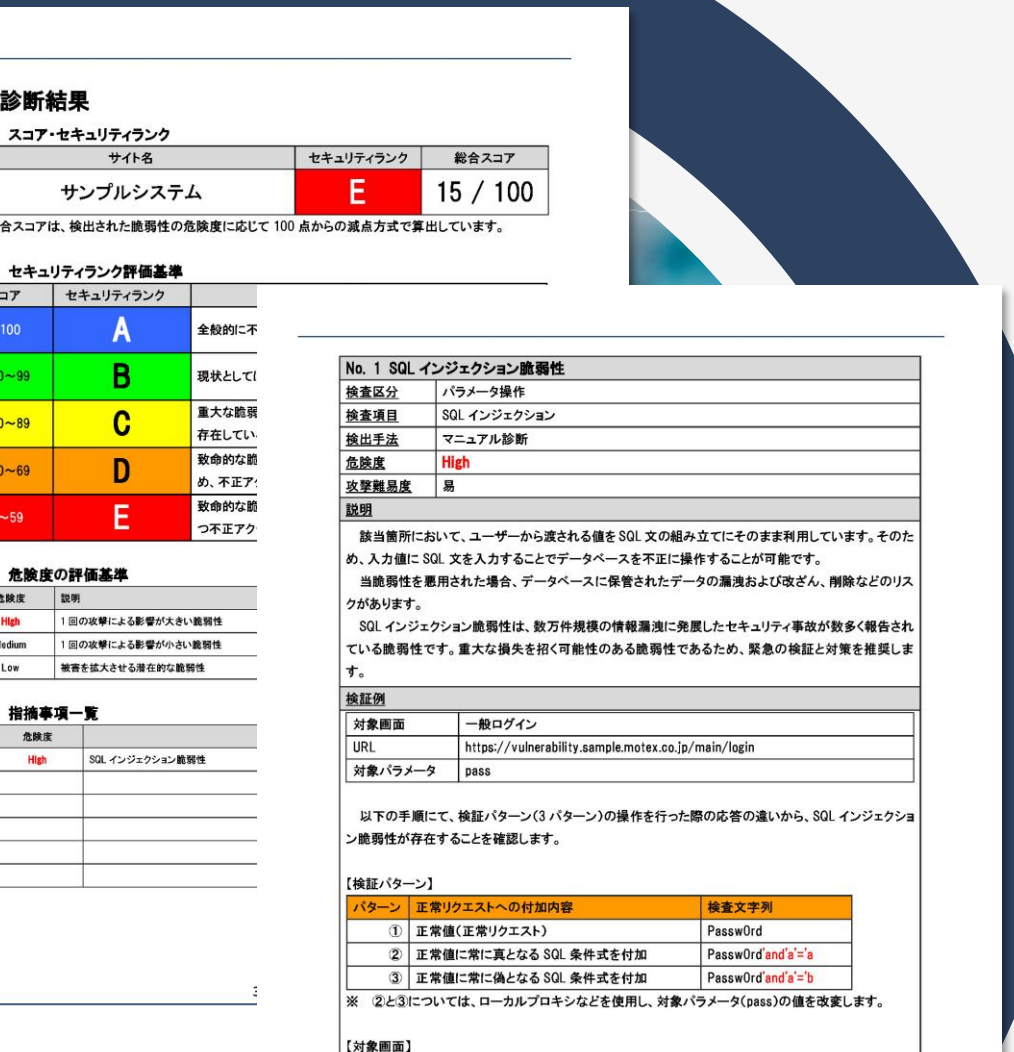
不適切な認証・認可による
機密情報の漏洩

Webアプリケーション健康診断	Webアプリケーション脆弱性診断
まずは脆弱性の傾向を チェックしたい企業様向け	サイトの特性に合わせて 網羅的に対策したい企業様向け
診断項目数　20	診断項目数　31
弊社選定の5画面	10画面～
￥300,000（税抜）	￥650,000～（税抜）

Webアプリケーション脆弱性診断 ― 診断項目

検査区分	診断項目	検査区分	診断項目
サーバー設定	ディレクトリ・リスティング	アカウント管理	権限昇格
	強制ブラウジング		情報管理
アプリケーション	エラー処理状況		パスワード使用状況
	ロジック流出	パラメータ操作	HTTPヘッダ・インジェクション
	バックドア、デバックオプションの存在		メールヘッダ・インジェクション
	ファイル機能 （アップロード、ダウンロード）		クロスサイト・スクリプティング
	クロスサイト・リクエスト・フォージェリ―		SQLインジェクション
通信	通信の暗号化強度		OSコマンド・インジェクション
	リファラ情報		パス・トラバーサル
セッション管理	セッションID使用状況		バッファオーバーフロー
	Cookie使用状況		LDAPコマンド・インジェクション
	ログアウト機能		その他パラメータ操作
認証	ユーザー認証処理	クライアント側スクリプト	クライアント側コメント
	アカウントロック機能	その他	クライアント・アプリケーションに関する問題
	ブルートフォース攻撃（辞書攻撃）耐性		その他、HTTPプロトコルに依存する問題
	アクセス権限		

※診断を実施する環境やプランによって、診断項目が異なる場合もございます。



診断結果

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
サンプルシステム	E	15 / 100

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。

セキュリティランク評価基準

コア	セキュリティランク	
100	A	全般的に不
0~99	B	現状として
0~89	C	重大な脆弱 存在してい
0~69	D	致命的な脆 め、不正ア
~59	E	致命的な脆 つ不正アク

危険度の評価基準

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

指摘事項一覧

危険度	
High	SQL インジェクション脆弱性

No. 1 SQL インジェクション脆弱性	
検査区分	パラメータ操作
検査項目	SQL インジェクション
検出手法	マニュアル診断
危険度	High
攻撃難易度	易

説明

該当箇所において、ユーザーから渡される値を SQL 文の組み立てにそのまま利用しています。そのため、入力値に SQL 文を入力することでデータベースを不正に操作することが可能です。

当脆弱性を悪用された場合、データベースに保管されたデータの漏洩および改ざん、削除などのリスクがあります。

SQL インジェクション脆弱性は、数万件規模の情報漏洩に発展したセキュリティ事故が数多く報告されている脆弱性です。重大な損失を招く可能性のある脆弱性であるため、緊急の検証と対策を推奨します。

検証例

対象画面	一般ログイン
URL	https://vulnerability.sample.motex.co.jp/main/login
対象パラメータ	pass

以下の手順にて、検証パターン(3 パターン)の操作を行った際の応答の違いから、SQL インジェクション脆弱性が存在することを確認します。

【検証パターン】

パターン	正常リクエストへの付加内容	検査文字列
①	正常値(正常リクエスト)	Passw0rd
②	正常値に常に真となる SQL 条件式を付加	Passw0rd'and'a'='a
③	正常値に常に偽となる SQL 条件式を付加	Passw0rd'and'a'='b

※ ②と③については、ローカルプロキシなどを使用し、対象パラメータ(pass)の値を改変します。

【対象画面】

誰が見ても理解ができる！

顧客満足度99%※の詳細な報告書

一目でわかるスコアリング

セキュリティレベルを数値化

誰が見ても同じ指標でセキュリティレベルが判断できます

経営層への報告書用サマリー

報告のために別途資料作成をする必要はなし！

そのまま報告書として使えます

脆弱性の内容・検証例・対策までを解説

実際の検証経緯を詳細に記載することで、再現性が高まり

効率的に脆弱性対策ができます

実施の流れ

報告書のご提出後も3ケ月間の

アフターケア期間を用意

診断後もご相談が可能です

01

ヒアリングシートの記載

お客様

ヒアリングシートを記入していただきます。記載内容を元にサービス内容に齟齬がないか認識合わせを実施します。

02

環境とバックアップの準備

お客様

診断環境の準備をしていただきます。診断が攻撃と判定されないように関係各所に事前の連絡をお願いします。

事前準備（1～4週間）

03

診断の実施

MOEX

万が一危険度が高い脆弱性が発見された場合は、報告書提出前に、速報としてご連絡します。

04

報告書作成

MOTEX

診断結果をもとに不適合項目を抽出し、報告書にまとめ納品します（報告会のオプション有）

診断作業（3週間）

MOTEXの診断
選ばれる理由

MOTEXの脆弱性診断は

人が実施する柔軟で細やかな

診断が強みです。

脆弱性診断のリーディングカンパニー

業界に先駆けて企業の「脆弱性診断」をスタート。
積み上げてきたノウハウと技術力で12,000件以上の実績を誇ります。

人だから対応できる細やかで柔軟な診断

専門のエンジニアが常に最新の状態で診断。ツールによる診断で課題になりがちな
「診断できない項目」や「システムに対する影響」も解決します。

診断項目数は業界トップクラス

OWASP TOP１０やセキュリティ動向やベンダー提供情報から診断が
必要と判断した独自項目も加えて診断。常に見直し、強化しています。

お客様に合わせた最適な提案

お客様のアプリケーションの仕様を把握したうえで、、最適な対策をご提案。
お客様特有の環境や条件を踏まえたうえで、対策を提案します。

株式会社サイバーエージェント 様

https://www.lanscope.jp/case/20241011_2959/

高い技術・柔軟なリソース調整・円滑なコミュニケーションで年間数百件の脆弱性診断を安定して運用

ユーザーが安全してサービス利用できるように、リリース前や機能追加前に加え、サービスリリース後も定期的に自社で脆弱性診断を実施。自社診断リソース不足の解消だけでなく、技術の進歩にも対応が必要で、新しい技術が登場した際には外部からも知見を入れて対応するために、外部のベンダーという第三者による診断を検討

ー　高い技術力・リソース調整力・円滑なコミュニケーション力を備えた信頼できるパートナー

エムオーテックスの診断員は、自社でも10年以上診断を行っているサイバーエージェントがセキュリティベンダーに求める基準を満たした**「技術力」に加えて、サービス担当部署と連携し円滑に診断を進めるために必要な「柔軟なリソース調整力」と「コミュニケーション力」といった総合力を保有**しています。
診断員はチームとコミュニケーションを頻繁にとりながら、柔軟にテストを実行しています。発注や報告書の提出といったフローにおいても、**ベンダー側が用意したテンプレートやツール利用が多い中、弊社側のフローや普段使っているツールを活用**してもらっており、負荷なく進められています。

ー　並行した複数の診断案件を安定的に実施できるクオリティを評価

診断の期間は、短い案件では2日程度、長い案件では1～2カ月程度かかります。**サービスや業務に影響が出ないように診断を実施するための細やかなスケジュール調整**など、柔軟な対応で効率よく運用し、定常的に脆弱性診断を実施してます。細かやかなコミュニケーションの元、プロジェクトの状態や納期など様々な要因がある中でも多くの案件を進行しながら、**診断を計画通りに進められています。**

サービス業	
利用サービス	Webアプリケーション診断
会社規模	5,000名以上

他にもネットワーク・クラウド・サイバーリスクなど多彩なメニューをご用意

LANSCOPE Professional Serviceのさまざまな脆弱性診断メニュー

ネットワーク脆弱性診断

対象のサーバおよびネットワーク機器のセキュリティリスクを効果的に把握できます

インターネットに公開されている**ネットワーク機器やサーバー**は、不要な通信ポートの開放やOSの更新漏れなどの脆弱性が存在することで、攻撃を受ける危険性があります。
この診断では、**ネットワーク機器やサーバーの脆弱性を調査し、最適なセキュリティ対策**をレポートで提案します。

クラウドセキュリティ診断

ご利用のクラウドサービスのセキュリティリスクを効果的に把握できます

クラウドサービスはインターネット上で誰でもアクセスできるため、定期的な管理設定の見直しを行わないと、セキュリティ上の問題が発生する可能性があります。
この診断では、**クラウドサービスのセキュリティリスクを調査し、適切な設定方法**をレポートで提案します。

サイバーリスク健康診断

自社およびグループ企業の外部公開資産を洗い出し、セキュリティリスクを把握できます

外部に公開されているVPN機器やサーバーの管理が不十分な場合、適切な対策が取れず攻撃者に狙われやすくなります。
この診断では、**外部に公開されている資産を洗い出し、サイバー上の危険性を調べ**、適切な対策をレポートで提案します。

お気軽にお問い合わせください

お問い合わせ

その脆弱性診断のお悩み
私達にお気軽にご相談ください

https://go.motex.co.jp/l/320351/2022-09-05/7zggwn

12,000社以上のお客様を診断してきた経験豊富なセキュリティのプロフェッショナルが、脆弱性のお悩みにお答えします。お気軽にお問い合わせください。

＜ よくあるご相談 ＞

・脆弱性診断を検討しているけど気軽に相談できるところがない･･･
・取引先からセキュリティ要件がきたので対応したい
・外部からの不正なアクセスができない状態か診断したいがどんな診断がいいか分からない

サイバーセキュリティの情報を発信しています

サイバーセキュリティに関連したイベントやセミナー、情報発信を行っています。皆様のサイバーセキュリティの一助となれば幸いです。

お役立ち情報を定期発信「ブログ」

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

セキュリティ診断セミナー

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

スマホアプリ診断を解説！項目や種類、対策できる脆弱性とは

ワンタイムパスワードとは？確認方法などわかりやすく解説

HTTPヘッダインジェクションとは？例や対策を解説

クラッキングとは？ハッキングとの違いや有効な対策を解説

パスワードスプレー攻撃とは？原因や今すぐ行うべき対策も解説

ルートキットとは？有効な対策や感染時の対処法を解説

なりすましとは？手口や対策、事例をわかりやすく解説

PSIRTとは？役割やCSIRTとの違いをわかりやすく解説

ビッシングとは？手口や被害事例、今すぐやるべき対策を解説

COMPANY PROFILE

会社紹介

会社概要

会社名	エムオーテックス株式会社
代表取締役社長	宮崎 吉朗
設立	1990年7月
従業員数	463名（2024年4月現在）
株主	京セラコミュニケーションシステム株式会社 （2012年から資本参加）
事業内容	自社製品の開発・販売、サイバーセキュリティのコンサルティング・ソリューション導入・運用監視サービス

拠点

本社	大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル
東京本部	東京都港区三田3-5-19 住友不動産東京三田ガーデンタワー22F
名古屋支店	名古屋市中区錦1-11-11 名古屋インターシティ 3F
九州営業所	福岡市博多区博多駅前1-15-20 NMF博多駅前ビル2F
長崎 Innovation Lab	長崎県長崎市出島町1-41 クレインハーバー長崎ビル3F

製品・サービスに関するお問い合わせ

■ プロフェッショナルサービス営業部
E-mail　security-sales@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）
E-mail お問い合わせ　support@motex.co.jp