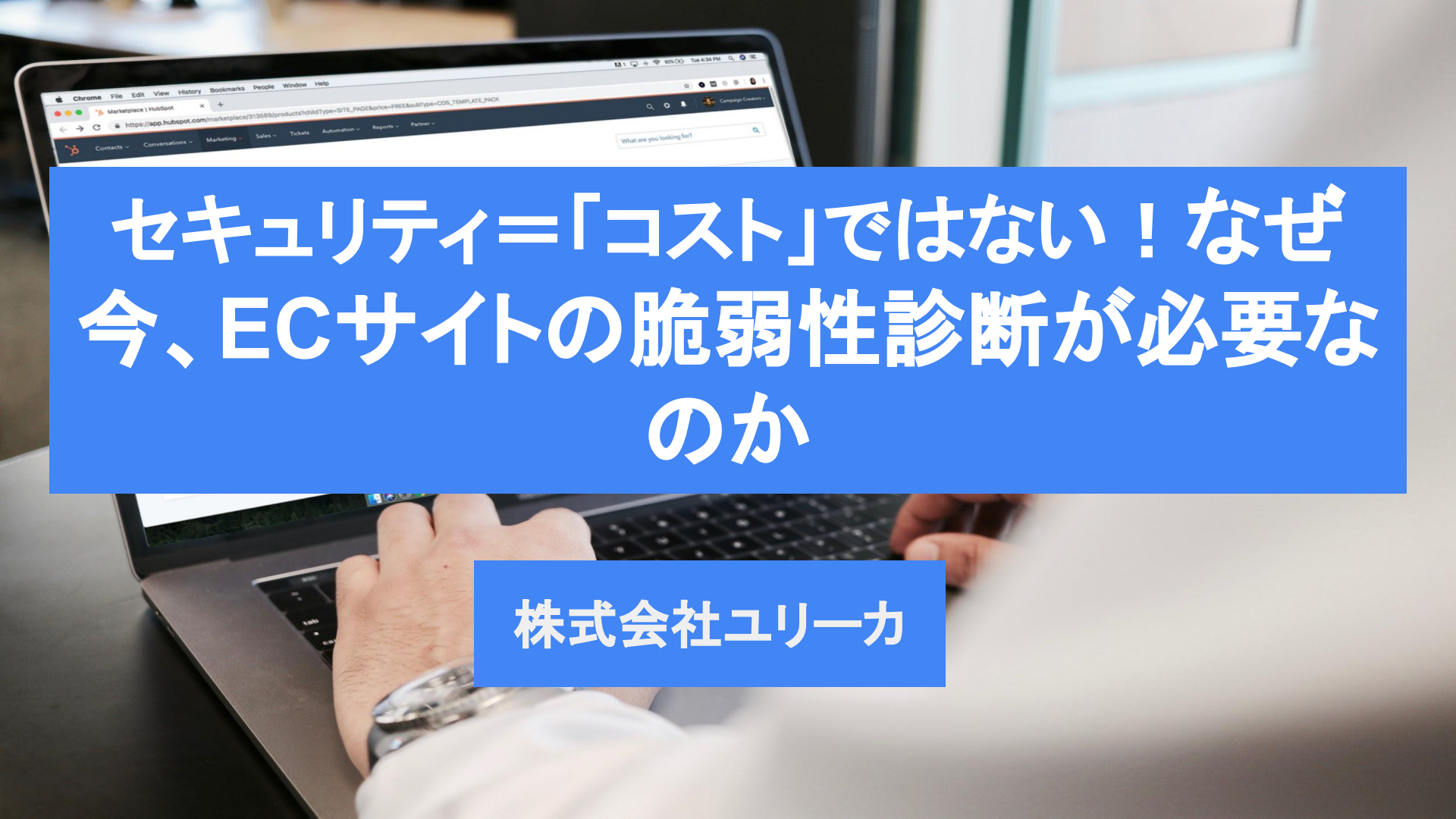


セキュリティ＝「コスト」ではない！なぜ今、ECサイトの脆弱性診断が必要なのか

株式会社ユリーカ

会社概要

株式会社ユリーカ(EUREKA CO. LTD)

代表取締役:代表取締役 青山 雅司(アオヤマ マサシ)

設立:1981年5月6日

資本金:2,400万円

従業員数:65名(2023年3月時点)

事業内容:業務基幹システムの企画から開発、運用保守、新製品やサービスの企画、開発、運用

認証・認定:ユースエール認定、ISMS(ISO 27001)

本社所在地:〒399-0702

長野県塩尻市大字広丘野村1688番地1
広丘ショッピングタウン(GAZA)3階

SIMPLEVOLUTION.
EUREKA

脆弱性・ECサイトの脆弱性診断とは

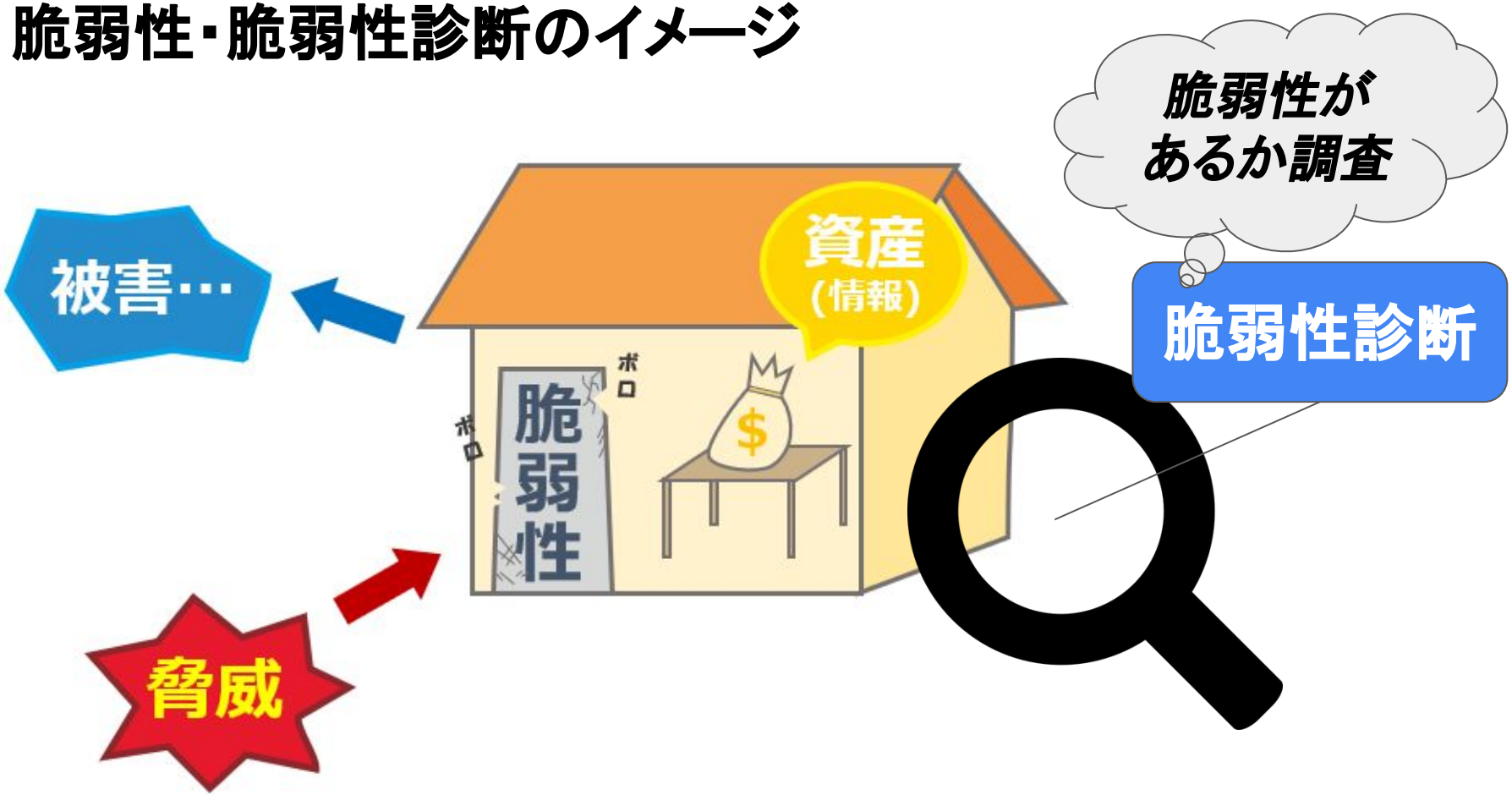
脆弱性とは

システム上の弱点、問題点のことです。脆弱性と似た言葉として「セキュリティホール」があります。悪意のある攻撃者は脆弱性に対して攻撃を仕掛け、機密情報、個人情報などを盗み取ります。

ECサイトの脆弱性診断とは

ECサイトの脆弱性診断とは、ECサイトのアプリケーションや、ミドルウェア、サーバーOS、ネットワークなどに脆弱性がないか診断することです。

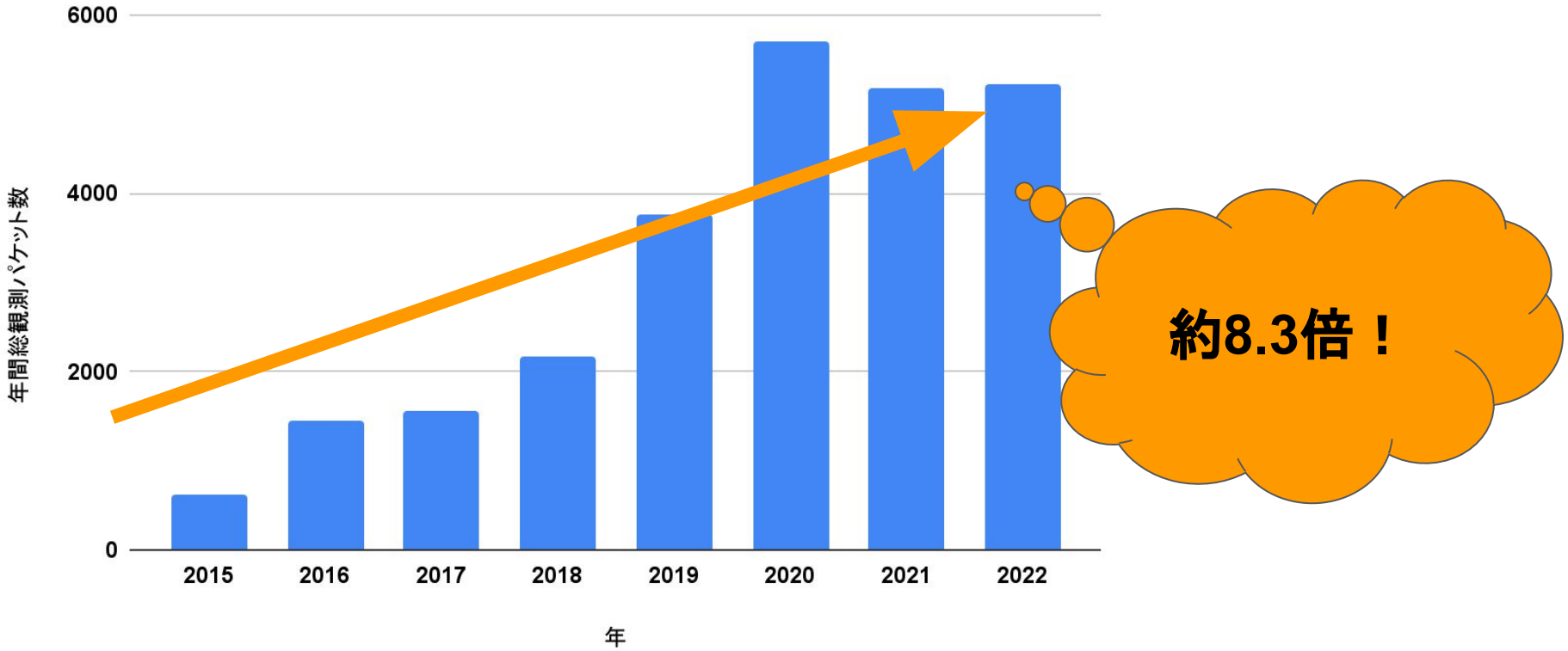
脆弱性・脆弱性診断のイメージ



ではなぜ今、ECサイトの
脆弱性診断をする必要があるのか？

サイバー攻撃の発生件数は国内外共に年々増加している

サイバー攻撃に関する通信の推移(年/パケット数(億))



出典：国立研究開発法人情報通信研究機構「 NICTER観測レポート2022」
https://www.nict.go.jp/press/2023/02/14-1.html

サイバー攻撃被害の事例

某男性ダンスグループのECサイト

発生時期：2020年

攻撃者が脆弱性を利用し、決済処理プログラムを改ざん

4万件以上のクレジットカード情報が流出

サイトの運営停止を決定

某大手食品加工メーカーのECサイト

発生時期：2021年

入力したカード情報が外部に流出するように変更されるように決済フォームを改ざん

100名以上のカード情報180件以上が流出

サイトの運営停止を決定

もし被害にあってしまったら、、

経済産業省とIPAが最近サイバー被害を受けた20社のECサイト運営事業者を対象に行った2022年度の調査

顧客情報の平均漏えい件数/1社

約3,800件

19社の事故対応の費用の平均額

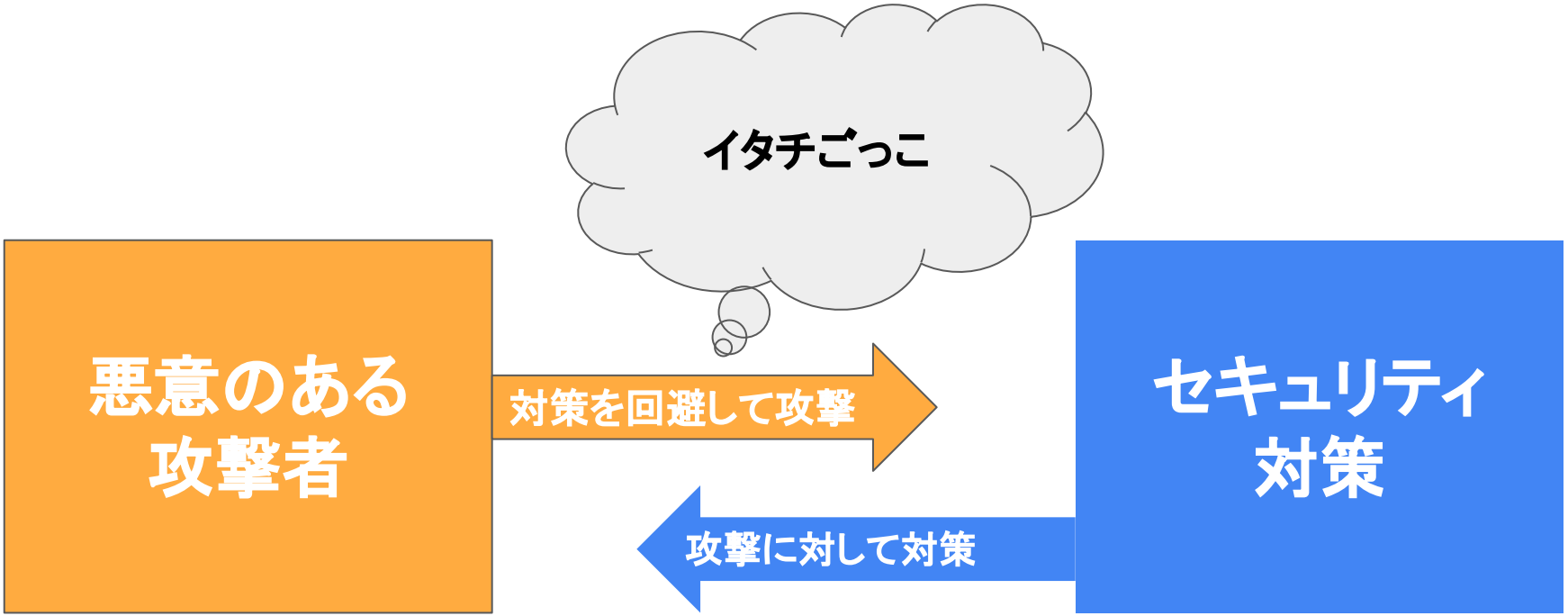
約2,400万円

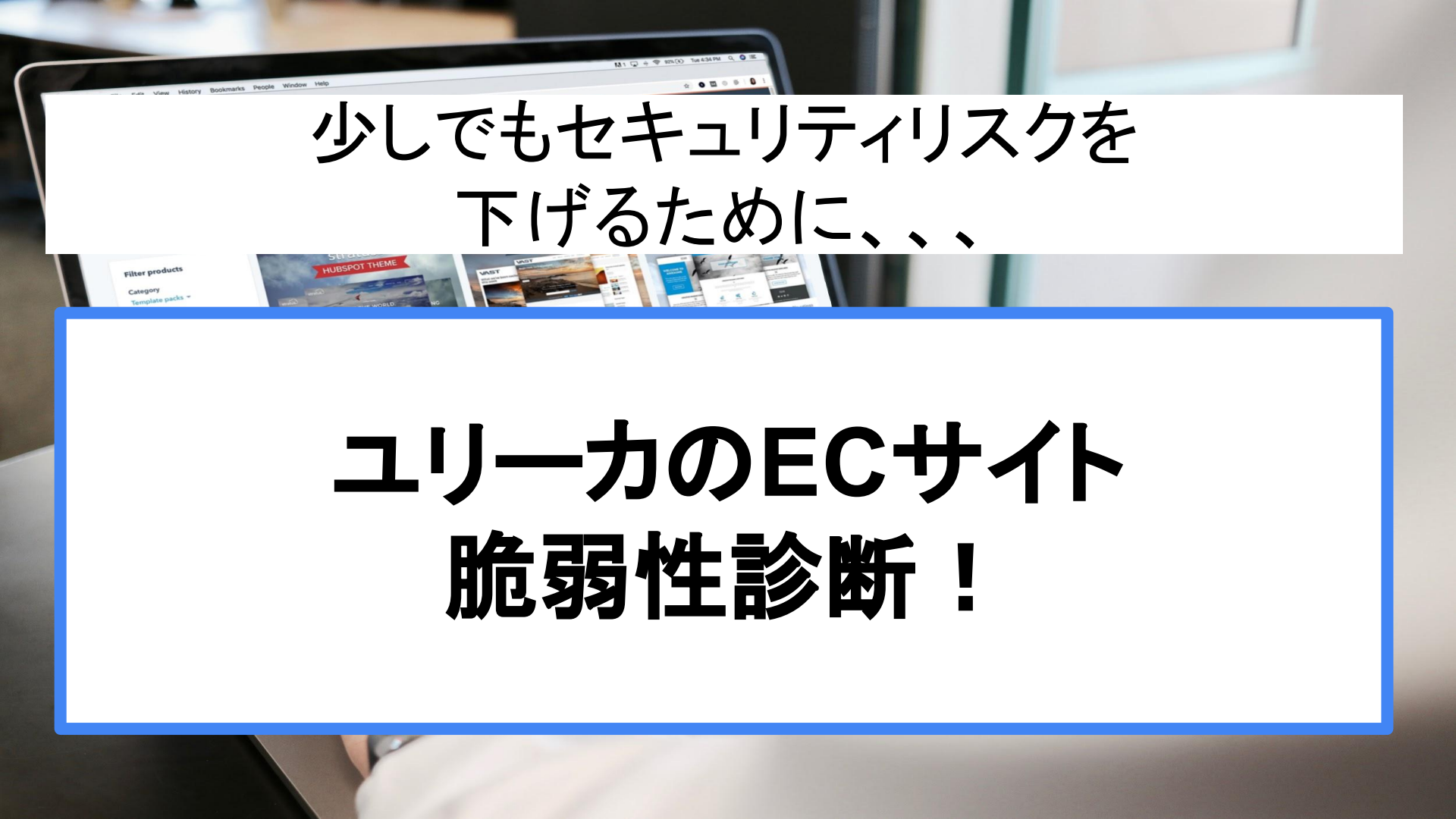
75%
CMS等の脆弱性を放置または最新版へのアップデートを怠っていた

90%
運用時のセキュリティ対策を実施していなかった

出典：独立行政法人情報処理推進機構PA「プレス発表 「ECサイト構築・運用セキュリティガイドライン」を公開」

”万全な”セキュリティ状態を”常に維持”することは困難！

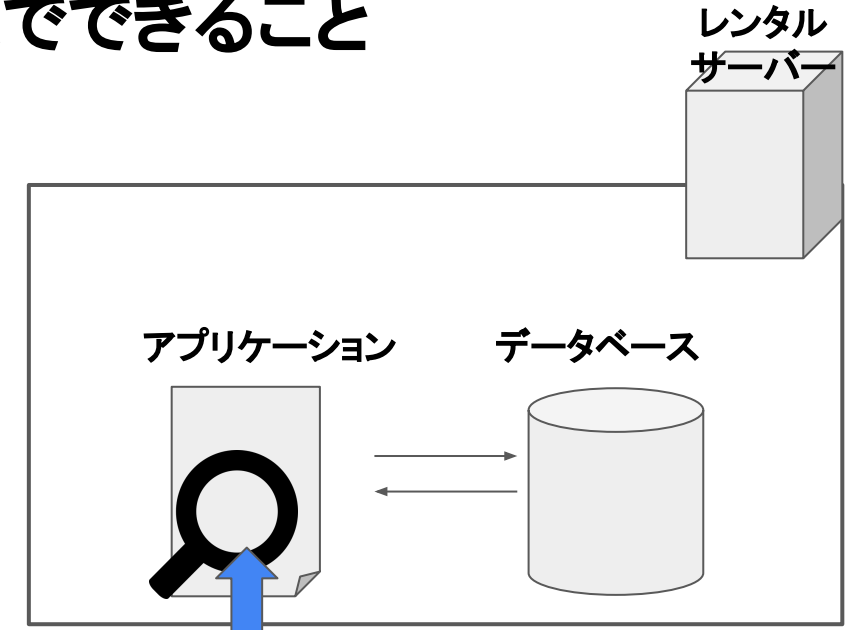




少しでもセキュリティリスクを
下げるために、、、

ユリーカのECサイト
脆弱性診断！

ECサイト脆弱性診断サービスでできること



※AWS、GCP、Azureなどのクラウドサービス上で構築されている Webサイトは診断の際にクラウドサービス側で攻撃されていると判断される可能性があるため、診断の対象外となります。
※ミドルウェア、サーバー OS、ネットワークの診断は対象外となります。
※診断するには対象サイトのテスト環境をご用意していただく必要があります。

脆弱性があるか診断！

サービスの機能と特徴

ログインが必要なサイトも診断可能

無料で公開されているツールの中には、ログインが必要なページは診断ができないものがあります。

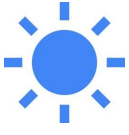
診断結果のレポートを発行

セキュリティ対策のきっかけ作りや安全性を顧客に示す際の証拠として活用できます。

OWASPの基準を採用

Webアプリケーションのセキュリティに関する研究活動をしているアメリカ合衆国の非営利組織「OWASP」の基準を参考にしています。

公開中の稼働サイトに影響なし



テスト環境対して診断するため、稼働サイトには影響がなく、診断の為に公開を一時停止や夜間に対応する必要もありません。

検出された脆弱性を一覧化

検出された脆弱性

各脆弱性の内容や脆弱性レベル（深刻度）をご確認いただけます。

検出された脆弱性

	検出された脆弱性	内容	脆弱性レベル
1.	CSP: script-src unsafe-inline	script-srcで指定したディレクティブにunsafe-inlineを使用している（Javascriptやインラインでのscriptタグの許可している）ため攻撃に対して脆弱になっている可能性がある。	中
2.	Absence of Anti-CSRF Tokens	クロスサイトリクエストフォージェリ（CSRF）攻撃を防ぐトークンの設定がされていない可能性がある。	中
3.	CSP: style-src unsafe-inline	style-srcにunsafe-inlineを設定している。	中
4.	CSP: Wildcard Directive	CSPを設定するディレクティブの設定がされていない。	中
5.	Content Security Policy (CSP) Header Not Set	Webサーバ側でブラウザに対してContent Security Policyを利用するようにレスポンスをする設定がされていない。	中
6.	CSP: Notices	Content-Security-Policyヘッダを利用していない	低
7.	X-Debug-Token Information Leak	X-Debug-Tokenもしくは、X-Debug-Token-Linkヘッダを含んでいる。	低
8.	Strict-Transport-Security Header Not Set	Webサーバーがウェブブラウザーにhttpsを使用するように指示していないため、情報が平文でやり取りされる可能性がある。	低
9.	Cookie Without Secure Flag	Cookieの内容が暗号化されない通信で利用することができ、内容が取得され、情報漏洩などのセキュリティ侵害が発生する可能性がある。	低
10.	Server Leaks Version Information via "Server" HTTP Response Header Field	Webアプリケーション サーバーは、HTTP 応答ヘッダを介してバージョン情報を公開しているため、Webアプリケーション サーバーが対象とする他の脆弱性を特定されることがある。	低
11.	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Webアプリケーション サーバーが、HTTP 応答ヘッダのX-Powered-Byを介して情報を漏洩しているため、Webアプリケーションが依存している他のフレームワーク/コンポーネントの脆弱性を特定しやすくなる可能性がある。	低
12.	Private IP Disclosure	プライベートIPまたはAmazon EC2プライベートホスト名がWebSocketメッセージで発見されたため、内部システムを標的とする攻撃に役立つ可能性がある。	低
13.	Cookie without SameSite Attribute	サイトをまたがるアクセス時にクライアントからCookieを送信するか否かを制御するSameSite属性の設定をしていない状態でCookieを利用している。	低
14.	Modern Web Application	対象のサイトはモダンウェブアプリケーションの可能性がある。	情報
15.	User Controllable HTML Element Attribute (Potential XSS)	ユーザが入力したクエリー用のパラメータとPOSTデータがHTMLをコントロールしている。	情報
16.	Re-examine Cache-control Directives	ブラウザーのキャッシュ動作を管理するcache-controlが正しく設定されていないか、欠落しているため、ブラウザーとプロキシーがコンテンツをキャッシュできる可能性がある。	情報
17.	Information Disclosure - Suspicious Comments	レスポンスされたデータにコメントなどセキュリティを突く情報が入っている。	情報

診断結果

検出された脆弱性の種類の数などを基に[ECサイトがどのくらい安全/危険なのかを確認]できます。

安全度

検出された脆弱性を基に算出された[ECサイトの安全度]です。数字が高いほど安全性が高いECサイトとなります。

脅威となる攻撃の種類

検出された脆弱性の傾向から[脅威となる主な攻撃の種類を確認]できます。

サービスの料金

今回セミナーに
ご参加いただいた
企業様限定

ECサイト脆弱性診断
基本料金

~~¥50,000~~

¥20,000

（税別）/1サイト

＋

テスト環境構築
テストユーザー作成

別途お見積り

※オプションサービスのため任意

簡単4ステップ！サービスの流れ

事前申し込み書を記入し発注するだけ！

事前申し込み書記入

診断事前申し込み書にご要件をご記入いただきます。

発注

弊社から見積書が送付され、発注書をご送付いただければサービス開始となります。

診断実施

診断実施後、最短3営業日でレポートの提出が可能です。

診断結果受け取り

レポート内容は貴社の機密情報になるため、ご指定いただいた特定の担当者の方のみに送付いたします。


【株式会社ユリーカ】脆弱性診断サービス事前申請フォーム

Webサイト脆弱性診断サービスの事前申請フォームになります。こちらにご記入いただいた内容で弊社から見積書が送付されますので、ご検討いただければ幸いです。
こちらに記入いただきました内容は個人情報保護方針に基づきセキュリティの厳重な環境で管理されます。

takei.kosuke@viva-eureka.co.jp アカウントを切り替える

このフォームを送信すると、メールアドレスが記録されます

*必須

貴社名 *

回答を入力

ご担当者の氏名 *

経済産業省とIPAも推奨

ECサイトのセキュリティ対策と実践方法をまとめた「ECサイト構築・運用セキュリティガイドライン」にて脆弱性診断は必須とされている。定期的な診断をおすすめします。

出典：独立行政法人情報処理推進機構IPA「プレス発表 「ECサイト構築・運用セキュリティガイドライン」を公開」

ECサイトを定期的に脆弱性診断し、
その都度セキュリティ対策をするのは大変....

クラウド型ECで自動アップデート！脆弱性の発生を未然に防ぐ！

ECサイトを常に最新状態に！

	最新性	拡張性	安全性	トラフィック負荷耐性	費用感	構築期間
GMOクラウドEC	◎	◎	◎	○	高	中～長期
オープンソース型EC	△	○	×	○	低	短～中期

クラウドECプランでは標準機能が常に最新状態で
ご利用でき、脆弱性への対策は自動で更新されます。

オフィシャルパートナー

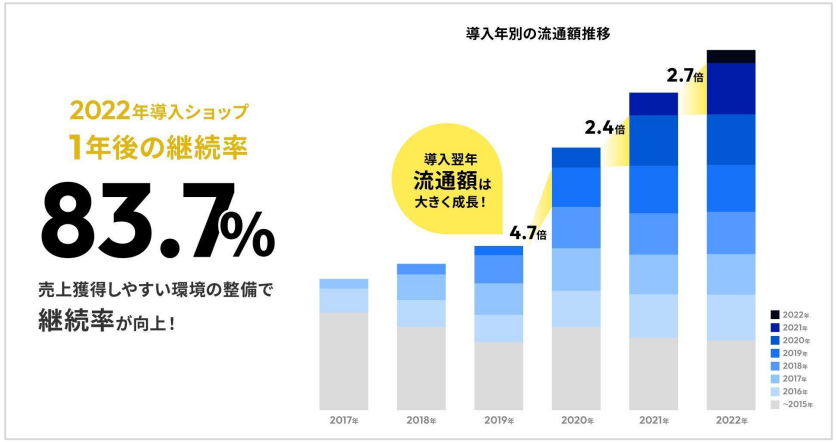
makeshop by GMO

GMOクラウドEC

makeshop by GMO の実績

2022年 流通額
3,055億円※1
No.1

導入実績
10,000
社以上※2



makeshop は **11年連続で年間総流通額SaaS業界 No.1** を獲得しています。
ショップ運営者の売上の総和である流通額を最重要指標としてサービス強化をしています。

makeshop は業種業界問わずご利用いただけるサービスのため、中規模・大型の法人ショップ向けプランの**導入店舗数1万店舗以上**のショップ様にご利用いただいています。

GMOクラウドEC

カスタマイズ可能なコマースのプラットフォーム
あらゆるコマースビジネスの課題を解決

サブスク

オークション

BtoB受発注サイト

メーカー直送

ショッピングモール型

オムニチャネル・OMO

お問い合わせ

makeshop、GMOクラウドECに関してのご相談はこちらから！

https://viva-eureka.com/service/ec-site/

ECサイトの脆弱性診断に関してのご相談はこちらから！

https://viva-eureka.com/service/%e8%84%86%e5%bc%b1%e6%80%a7%e8%a8%ba%e6%96%ad%e3%82%b5%e3%83%bc%e3%83%93%e3%82%b9/