“てんやわんや”な脆弱性対応から抜け出せ！

AIを活用した効率的な

トリアージ&ASM とは

あらたな答えを、つぎつぎと。

変化の激しいサイバーセキュリティの世界。

私たちは、未知の課題が生まれるたび、培った知見と経験・実績をもとに、
「あらたな答え」を世の中に提供し続けていきます。

世界も驚くような、技術の力で。

そして、サイバーセキュリティの進化を通して、
人は、人にしかできない、創造性を活かした仕事に注力できる、
社会の進化にも貢献していきます。

AeyeSecurityLab

AeyeSecurityLab

誰でも簡単に

プロさながらの高度な

脆弱性診断を

AeyeScan

“てんやわんや”な脆弱性対応から抜け出せ！

AIを活用した効率的な

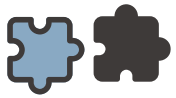
トリアージ&ASM とは

いまや、脆弱性が「山積み」の時代

環境変化に伴い脆弱性が増加する一方、リソース不足で対応しきれなくなっている

攻撃対象の拡大

Webアプリケーション、API、
モバイル、クラウド…
診断対象の範囲が広がり
脆弱性が増加



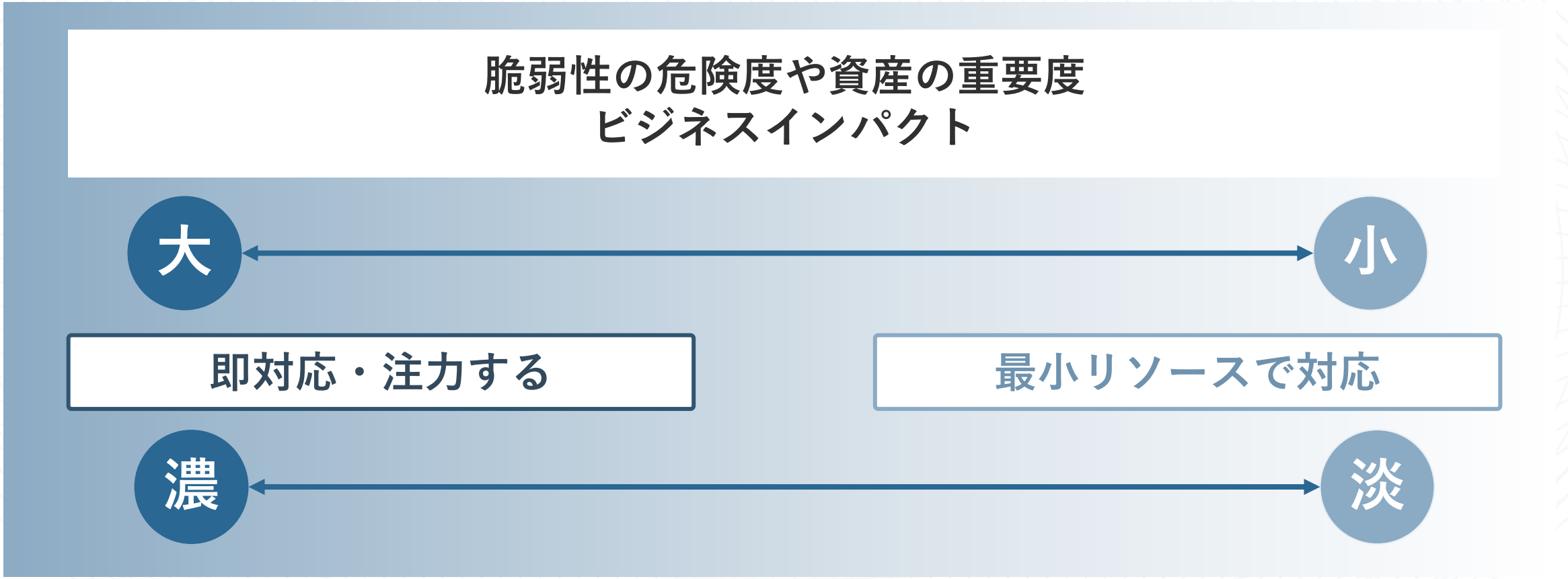
新しい技術の台頭

マイクロサービスや
SaaS連携など、
新しい開発スタイルが
生まれるごとに
新しいリスクも生まれる

既知の脆弱性の放置

修正リソース不足や
診断待ちにより、
既知の脆弱性が
解消されないまま
積み上がっている

濃淡をつけて対応しないと、捌き切ることができない



限られたリソースを最適配分するために「脆弱性トリアージ」が必要

脆弱性トリアージ体制はどのようにつくる？

脆弱性トリアージ体制をつくるには

脆弱性トリアージ体制の作成は、「脆弱性トリアージガイドライン作成の手引き」の「1章 トリアージガイドラインの作成 」を参考にして下さい。

「脆弱性の影響分析」、「リスク判定基準」、「対応の要否と期限を決める」といった
対応基本方針を策定することで、迅速に最低限のトリアージが可能な体制が構築できます。

1. 関係者の役割と責任を明確にする
2. トリアージガイドラインの適用範囲を決める
3. 脆弱性の影響範囲の調査
4. トリアージで決めるべきこと
5. 対応の要否と期限を決める
6. 脆弱性の管理方法

参考： 「脆弱性トリアージガイドライン作成の手引き 」 「1章 トリアージガイドラインの作成 」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

トリアージで決めるべきこと　（1）対象資産の重要度の評価

まず重要度の評価基準の選定から始めましょう。以下は、評価分類の一例です。

資産の種類に基づく分類		影響度の規模(利用者の規模)に基づく分類		利用者層に基づく分類	
高	金融データ、顧客情報、特許性を有する製品や技術情報	高	利用者数1万人以上	高	官公庁利用者(政府調達等)
中	業務データ、従業員の勤怠情報	中	利用者数1000人以上	中	技術者、システム管理者、企業の担当者
低	ホームページ等で既に公開されている情報	低	利用者数1000人未満	低	一般の利用者(BtoCのサービス等)

参考：「脆弱性トリアージガイドライン作成の手引き」「1章 トリアージガイドラインの作成」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

トリアージで決めるべきこと　（2）脆弱性の危険度の評価

次に脆弱性の危険度を確認し、対応の緊急性を評価する基準を設けます。

評価方針の設定

CVSS基本値や、脆弱性診断事業者が提供する危険度評価を参考に分類

CVSSでは「攻撃元区分」「攻撃条件の複雑さ」「攻撃前の認証要否」など、複数の要素を元に最終的な値が算出されますが、特に重視する項目があれば基準の一つとしてもOK

危険度評価の定義例（3段階の場合）	
高	CVSSが7.0 - 10.0
中	CVSSが4.0 - 6.9
低	CVSSが0.0 - 3.9

危険度評価の定義例（4段階の場合）
Critical
High
Medium
Low

※3段階の場合と同様、それぞれの段階で定義を記載

参考：「脆弱性トリアージガイドライン作成の手引き」「1章 トリアージガイドラインの作成」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

対応の優先度の決め方

対象の重要度評価と脆弱性の危険度評価から、マトリックスを作成して対応の優先度を決めます。

CVSS				
	高	中 (30日以内)	高 (10日以内)	緊急 (5日以内)
	中	低 (90日以内)	中 (30日以内)	高 (10日以内)
	低	低 (90日以内)	低 (90日以内)	中 (30日以内)
		低	中	高
		資産重要度		

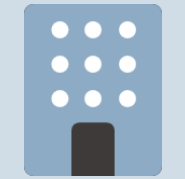
参考：「脆弱性トリアージガイドライン作成の手引き」「1章 トリアージガイドラインの作成」https://wg1.isog-j.org/TriageGuidelines/docs/chapter1/

ビジネスインパクトを考慮した結果優先度が下がった事例

トリアージ対象の脆弱性：CVE-2022-3080(CVSSスコアは7.5)

BIND 9と呼ばれるDNSサーバーの実装に発見された脆弱性。クライアントからフルサービスリゾルバとして動作するBIND 9のDNSサーバーに対し、細工された問い合わせを送信することにより、特定の条件下でサービス不能（DoS）にさせることができる。

トリアージを実施するA社の状況



A社

- 複数のブログやWebメディアを運営する企業
- ページ上に掲載される広告を主な収益源

2種類の用途でそれぞれ独立したDNSサーバーを運用

権威DNSサーバー
ブログやWebメディアのドメインの問い合わせに応答する

フルサービスリゾルバ
社内業務に利用するオフィス端末のインターネットアクセスに利用する。

参考：「脆弱性トリアージガイドライン作成の手引き 」「5章 事例」https://wg1.isog-j.org/TriageGuidelines/docs/chapter5/section2/

トリアージする脆弱性はどうやって見つける？

トリアージする脆弱性の発見は、まず「ASM」から始めるべき

DXの推進に伴い、未把握のWeb資産が増加している。
脆弱性対策の抜け漏れを防ぐためにも、ASM（Attack Surface Management）と
脆弱性診断は合わせて行うのが望ましい。

未把握のWeb資産の一例

事業部門がアジャイル開発で
構築・運用するWebサイト

PoCで作ってみた
SaaS/IaaS/PaaS上のアプリ

スクラップ＆ビルドの連続で
誰も管理できていないAPI

ASM・脆弱性診断・トリアージは内製でできる

外部委託する方法以外に、内製で行うこともできる。

Web資産の発見（ASM）	脆弱性診断	トリアージ
ASMツールを活用し未把握のWeb資産を発見する	脆弱性診断ツールを活用し脆弱性を発見する	「脆弱性トリアージガイドライン作成の手引き」を参照しながら行う

参考：「脆弱性トリアージガイドライン作成の手引き」 https://wg1.isog-j.org/TriageGuidelines/

内製する上での課題

ASM・脆弱性診断・トリアージを内製する上では、それぞれ以下のような課題がある。

Web資産の発見（ASM）	脆弱性診断	トリアージ
探索に必要な 手がかりがわからない	専門知識のないメンバーで 対応できない	リソース不足 人によって認識が異なる
誤検知の精査に 手間や時間がかかる	ツールを導入しても 使いこなせず工数がかかる	ビジネス上の優先度や 修正容易性を加味しづらい
発見経路や 検出理由まではわからない	診断の精度やカバー範囲など 品質に不安がある	CVSSだけでは 自社環境まで考慮できない

内製でのASM・脆弱性診断・トリアージの課題を解決するAeyeScan

AI・RPA活用により、脆弱性診断を自動化するクラウド型Webアプリケーション診断ツール

1

最短10分で診断開始

専門知識は不要！
SaaS環境なので24時間放置しておけます。

お客様

1 スキャン登録

3 結果レポート

AeyeScan

2 自動診断

Webサイト

3

診断結果レポートも自動生成

開発担当にすぐ渡せるレポートが簡単に出力できます。

2

画面遷移図を自動作成

AeyeScanがサイトを自動巡回、診断すべき画面を抽出して画面遷移図を生成します！

さまざまな企業さまに導入いただいております

ユーザー企業

人材・教育

OHSAWA DRIVING SCHOOL
河合塾
Junion
JINSOKEN
ZENKIGEN
Direct Sourcing
PERSOL
Leverages
workport

インフラ

EPARK
AIRE
HIS
H.O RETAILING
NTT EAST
odakyu
近鉄情報システム株式会社
SymEnergy
水ing Swing Corporation
Suzuyo
NANKAI 南海システムソリューションズ
日本調剤
HITOWA GROUP
ベルーナ
grow up together MEDIA
Looop
Loyalty Marketing, Inc.

金融

アイフル
MS&AD MS&ADインターリスク総研
JOBPAY
SOMPOひまわり生命
DMM FinTech
Tokyo Century
Net Protections

メディア

集英社
中日新聞
NIKKEI
Media Do

製造

AICA
AISIN
KITZ 株式会社キッツ
KOSÉ
SAKI
TIGER
TEIJIN
Denkei
House
Mizuno
ユーグレナ

エンタメ

e+ イープラス
CAPCOM
GungHo Online Entertainment, Inc.
とらラボ! TORANOANA LABORATORY
BookLive

SaaS

Advanced Media, Inc. 株式会社アドバンスト・メディア
Lexica E-Retailing Platform
estie
エアアンドエムマット株式会社
M-aid
エムティーアイ
OZ INTERNATIONAL
Classi
COACH A Co.,Ltd.
cybozu
Speee
SecureNavi
Diamond head
DMM Boost
TAL
Digital Garage
TEMONA
NAVITIME
KNOCK ON THE DOOR
BATONZ
VALUE HR
freee
vector
porters
hokan
Money Forward
RUN.EDGE
RVSTA 株式会社リバスタ
Rescuenow

SI・IT企業

Rworks
アクモス 株式会社
AVANT GROUP
Insight Edge
Infcurion
80&Co.
SBWorks
NTT Integration
NTT DATA
NTT ビジネスソリューションズ
OMRON
Globalway
KDDI Agile Development Center
circlace
さくら情報システム
SUNDAY SYSTEMS
CEC
GA TECHNOLOGIES
tdi 情報技術開発株式会社
Simplex Inc.
777WORKS 株式会社スリーセブンワークス
SOFT CREATE
SOLTEC
高千穂交易株式会社
電通総研
TOPPAN
JOPS
JAST
PCNET 株式会社パシフィックネット
Human Interactive Technology inc.
FUJISOFT
FUJITSU
MACROMILL
三菱電機デジタルイノベーション株式会社
YONA
リピスト

セキュリティ企業

NEC NECセキュリティ
NTT DATA 株式会社NTTデータ先端技術
GSX GLOBAL SECURITY EXPERTS
cybertrust
LAC

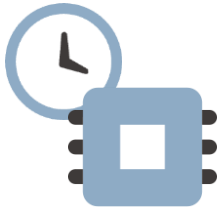
社名五十音順（導入いただいた企業様の一部です）会社名及びロゴは各社の商標または登録商標です

高度な生成AI活用により、効率的かつ信頼性の高い探索が可能

生成AIをASMに活用することで…！

会社名だけで攻撃面を探索

検索結果に上がってきた
組織名(文字列)を解読



発見経路/理由が分かる

生成AIが攻撃面を見つけるまでに
辿ったルートを説明

膨大な情報源から総合的に判定

- SSL証明書の情報
- IR情報(Web公開済み)など

重要度を自動でランク付け

Webサイトの属性を自動判定し
ビジネス上の重要度をもとにランク付け

生成AIが、Webサイトの属性を自動判定＆重要度をランク付け

サイト用途

Medium

- ECサイト
- VPN管理サイト

Low

- 外部SaaSサイト
- テストサイト

保持データ

High

- 個人情報
- クレジットカード情報

利用技術

Low

- WordPress
- EC-CUBE
- 旧式技術
  （JSP/PHP/CGIなど）

技術スタックだけでなく「ビジネス上の重要度」をもとに判定

トリアージ対応を圧倒的に効率化できる

生成AIが、リスクの深刻度を自動で可視化し、わかりやすく解説

既に悪用されている脆弱性		CVSSスコア／深刻度	悪用可能性(EPSS)	悪用観測(KEV)
実際の攻撃で使われている脆弱性	＋	脆弱性の技術的な深刻度・影響範囲	近い将来悪用される可能性	公的機関などが悪用を確認済みと公開している情報

検出したWebサイトで使用されているミドルウェアやライブラリにおける
”既知の脆弱性”とその”悪用情報” を自動で可視化

トリアージに基づく戦略的セキュリティ対策を実現

AeyeScanの導入を検討してみませんか？

操作性の確認、実際に利用してみたい方へ

AeyeScanの無料トライアル

トライアルにかかる費用は不要。実際の操作性はどうなの？
またどのように脆弱性が発見されるのか？
などの疑問は無料トライアルで解消しましょう。

無料トライアルの申し込み

お見積りの希望・導入をご検討している方へ

AeyeScanへのお問い合わせ

お見積りの希望・導入をご検討してくださっている方は
お問い合わせフォームよりご連絡ください。
当日もしくは遅くとも翌営業日にはご連絡を差し上げます。

お問い合わせフォーム

定期開催中！ AeyeScanがよく分かるデモ動画・セミナー

AeyeScanを検討してみたい方へ

AeyeScanがどんなものか知りたい方向けに、
デモを交えてわかりやすくご紹介。
まずは気軽に使い勝手をチェック！

AeyeScanデモ動画を視聴

AeyeScanの操作を体験してみたい方へ

実際の操作を通して、一連の機能を体感。
導入前の不安や疑問をまるごと解消。
“わからないまま”をなくすセミナーです。

ハンズオンセミナーの日程を確認

セキュリティ対策にお悩みの方へ

最新の事例や対策ノウハウをテーマ別に紹介。
月替わりで学べる無料ウェビナーを開催中。
お気軽にご視聴いただけます！

ウェビナーの日程を確認

セキュリティに、確かな答えを。