

～あなたのホームページ、狙われています！～

プラットフォーム・脆弱性診断ツール イージスEWのご紹介

～ ハッカーが攻撃サイトを決定する、レコナイ・ツールのご紹介 ～



2025年2月17日
株式会社 未来研究所

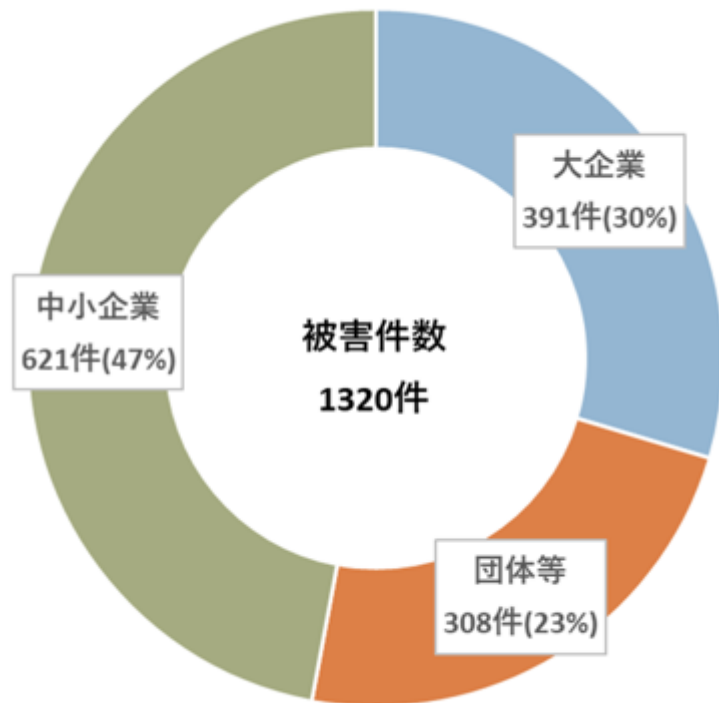
2025年サイバーセキュリティのサイバー事情

※サイバー攻撃での2大感染手口は、

- ・ ホームページからの侵入
- ・ メール添付のクリックからの侵入

サイバー攻撃の危険性は、年々高まっています！

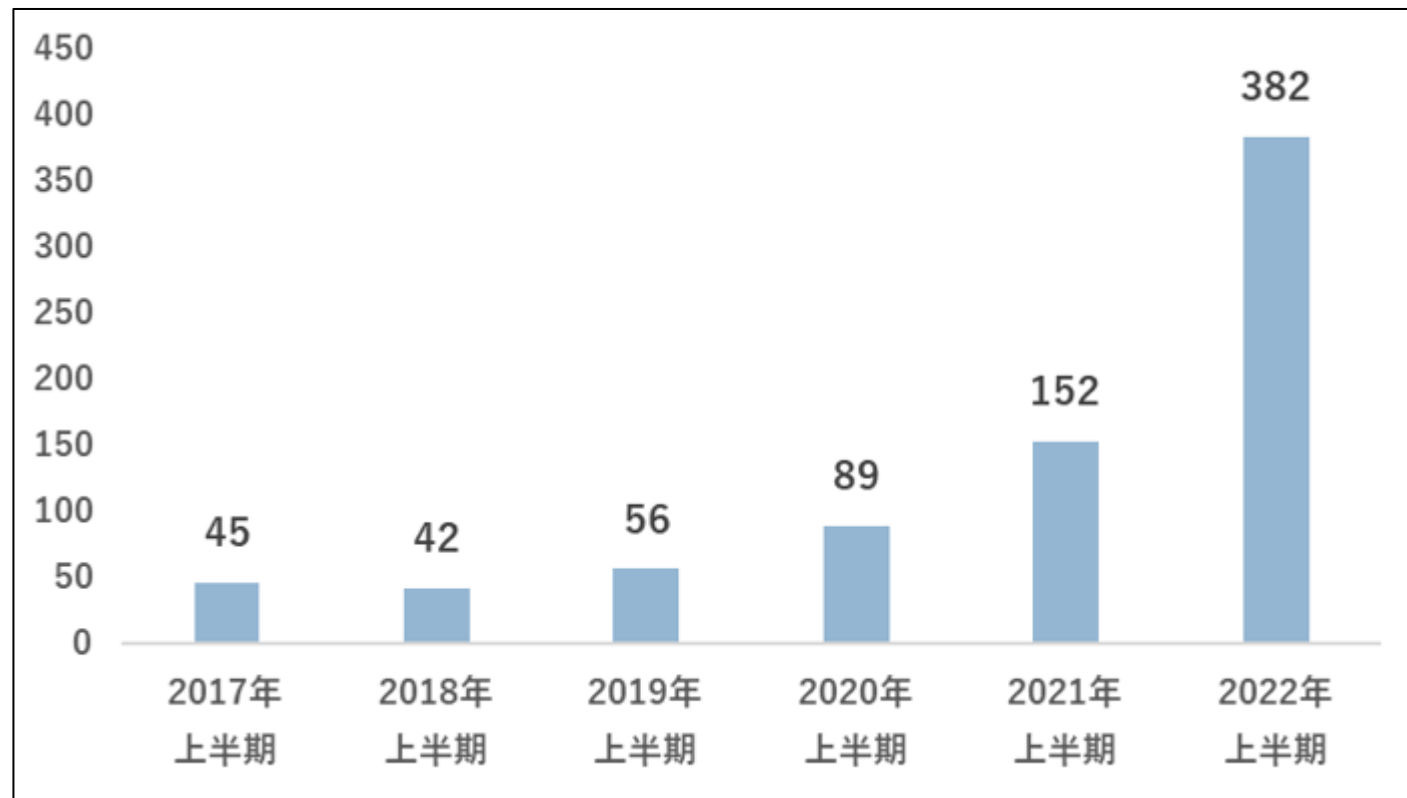
企業規模は関係ありません！



※被害件数を企業規模により分類

報道でよく目にするのは大企業の被害ですが、被害数は中小企業のほうが多いです

年々件数が増えています！

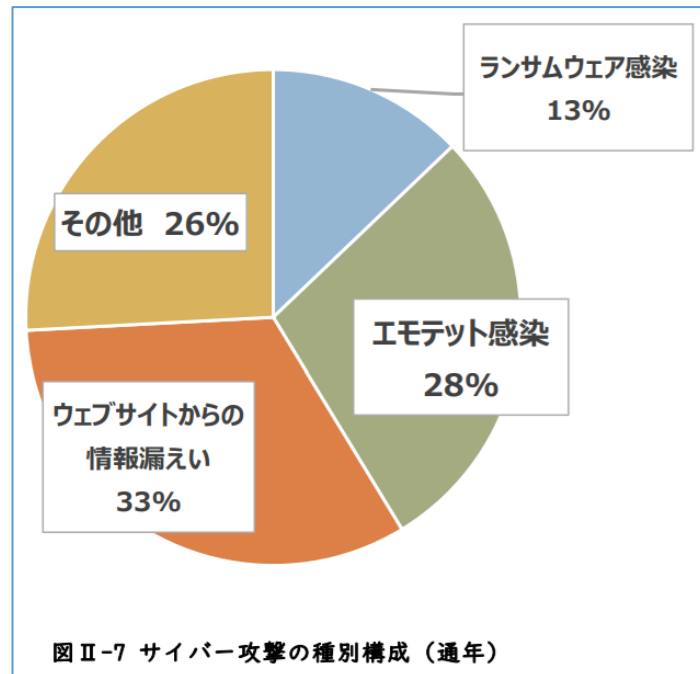


※公表されたサイバー攻撃件数の推移

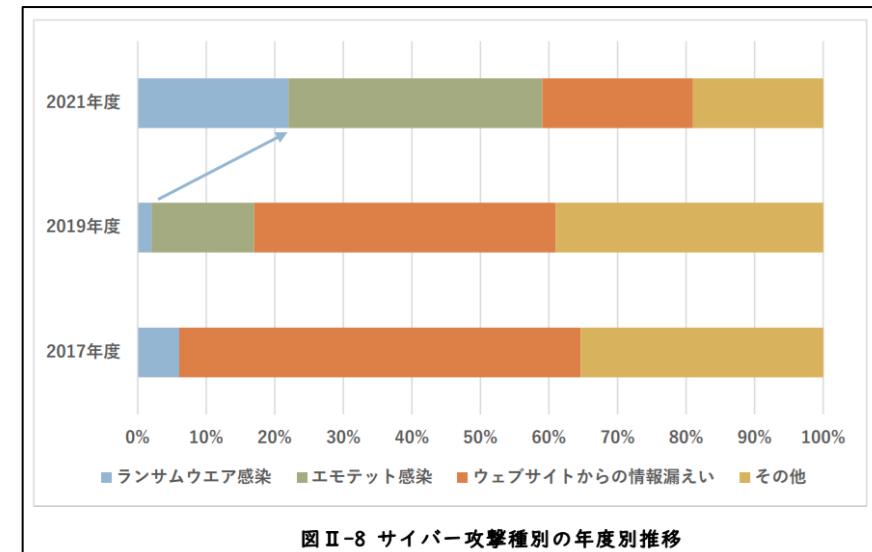
2022年で爆発的に増えた理由としては、攻撃が増加したことも挙げられますが、2022年4月に施行された改正個人情報保護法により、公表が必要になるケースが増え、それまでは隠匿されていた攻撃が明らかにされるようになったことも挙げられます

資料：NPO法人 日本ネットワークセキュリティ協会（[JNSA](#)）2024年発表

- サイバー攻撃で感染した原因
 - エモテット（・ランサム）メール添付経由
 - Webサイト経由からの情報漏洩（・ランサム）



- 年度による感染原因推移
 - エモテット（・ランサム）の伸長DMARC、SPMでの送信乗っ取りも流行りである
 - Webサイト経由からの情報漏洩（・ランサム）



■ハッカー攻撃のプロセスと手口

ハッカーは、ASM（アタック・サーフェス・マネジメント）ツールやレコナイ（偵察）ツールを用いて、攻撃可能なターゲットを特定し、リスト化します。
多くの場合、IPアドレス順やドメイン登録順に従って攻撃が実施されます。

①偵察（レコナイツアリング）

ツールを用いて広範なスキャンを実施し、攻撃可能な候補リストを作成
簡単な脆弱性スキャンを行い、セキュリティの弱いターゲットを抽出

②標的選定（ターゲティング）

候補の中から、狙う企業・団体を選定（標的型攻撃）
財務情報、知的財産、個人情報などの価値を考慮して決定

③初期侵入（エクスプロイト・ペネトレーション試行）

サーバ群の管理者権限（ADMIN情報）の取得を試みる
CVSS（共通脆弱性評価システム）深刻度 1（赤）・2（オレンジ）の脆弱性診断結果があれば、短時間で乗っ取り可能

④データ搾取（情報収集）

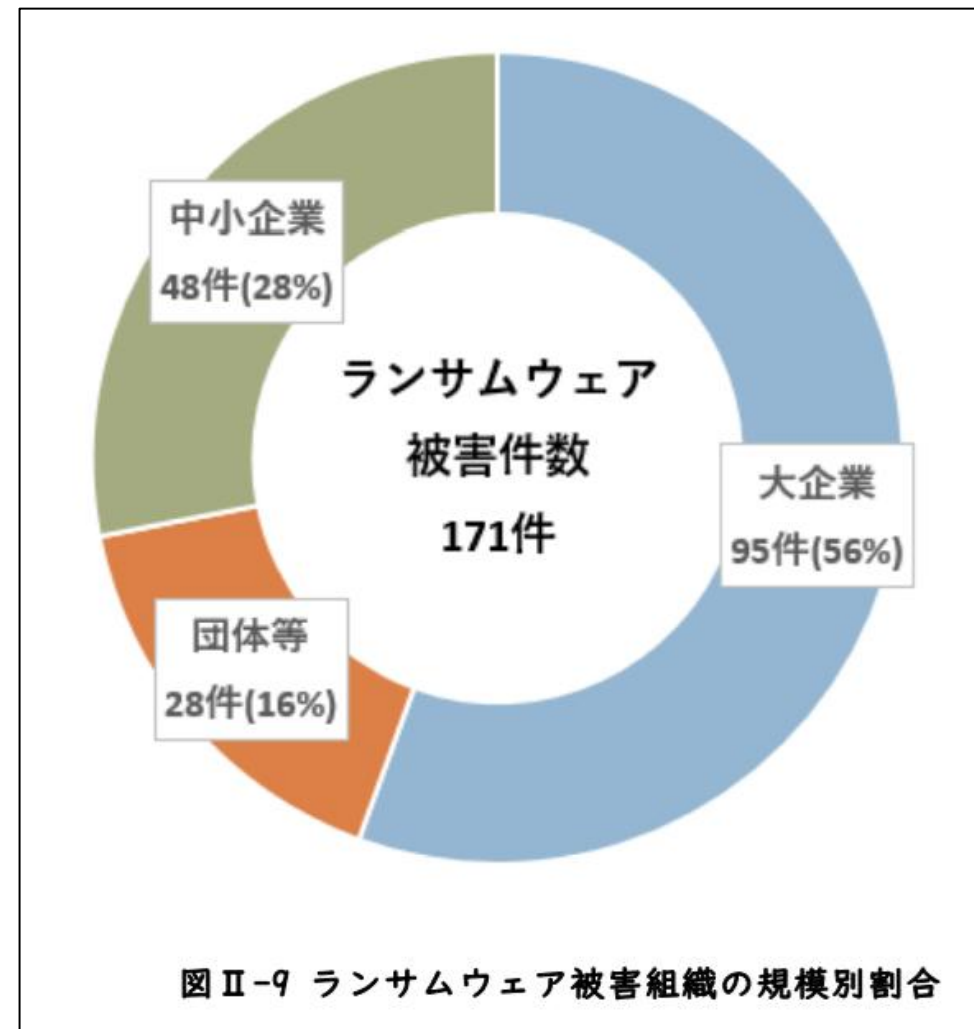
個人情報・機密データの窃取、メールの盗み見を実施
数年間にわたる情報搾取が行われるケースも多い（例：防衛庁、JAL など）

⑤ランサムウェア攻撃（最終段階）

盗む価値のあるデータが尽きた時点で、ランサムウェアを仕掛ける
システムを暗号化し、復旧のための身代金を要求

まとめ：長期的な脅威と対策の重要性

ハッキングは単なる一度きりの攻撃ではなく、長期間にわたる情報搾取が行われることが多いのが特徴。
企業・団体は、定期的なセキュリティ診断や脆弱性対策を実施し、常に、インターネット上および社内資産を効率よく診断および対策を打ちながら、インシデント発生時の訓練（防災訓練）が重要です。



- ・ **ECサイト直接改ざん**・・・日本経済新聞2024年12月4日掲載
タリーズコーヒージャパンなども被害
40企業のサイトに不正なプログラムが組み込まれ、総計30万人分以上のクレジットカード番号などの顧客個人情報盗まれました
対応費用、損害賠償、信頼喪失など、経営に多大な影響を受けます！
- ・ **サイバー攻撃被害企業が制裁金を支払わされる**
「GDPR（EU一般データ保護規則）」というEUの規則があり、サイバー攻撃で漏洩した顧客個人情報の中にEU在住者の情報が含まれていると、日本国内でだけ営業している企業であっても、企業規模に関係なく制裁金が課されます！
**サイバー攻撃への対応をしておらず重大な違反があった場合、
最大2000万ユーロ（約32億円）以上の制裁金を課される可能性があります！**

サイバー攻撃は、経営に深刻な影響を与えます！

• ランサムウェア

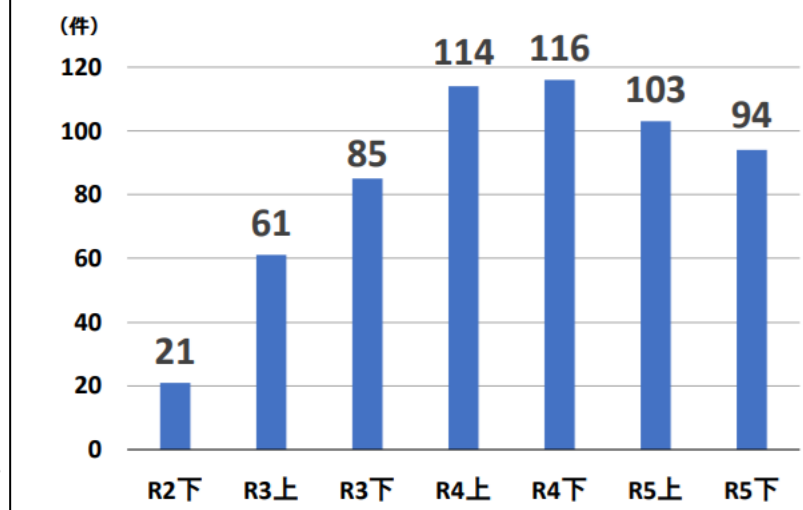
ハッカーがセキュリティの弱点から会社システム内に侵入して、金銭的価値のある情報を盗み取り、情報を吸い尽くした後、最後にシステム内のファイルを使用できなくし、身代金を要求する

ランサムウェアで会社のファイルを使えなくされ、身代金を要求されたときは、すべての情報が漏洩しており、もう手遅れです！

システムを修復するまで、事業中断せざるを得ないなど重大な影響があります！

※令和5年におけるサイバー空間をめぐる脅威の情勢等について by 警察庁

【図表19：企業・団体等におけるランサムウェア被害の報告件数の推移】



• サプライチェーンへの連鎖

大手企業への乗っ取りをおこなうため、サプライチェーン会員で脆弱性が多い関係企業の乗っ取りから、攻撃が開始される。該当会員端末はサイバー攻撃の踏み台に使用され、大企業、並びに他のサプライチェーン会員にもサイバー攻撃が実施される。グループ全体に多大な損害を及ぼしてしまう

多額の損害賠償に加え、取引復活まで約半年かかり、その間のオーダー受理作業が中断します。事業継続が危ぶまれます！

「自分の会社は大丈夫」「狙われるはずはない」と考えている方は多いです。
しかし、ハッカーの考えは違います。

ハッカーは「空き巣」と同じで、油断している狙いやすいホームページやシステムを狙います！

サイバー攻撃を受けてしまうと、**対応費用・顧客への賠償・事業停止による利益喪失・データ回復のための身代金支払・ブランドイメージなどの損害を被ります！**
中小企業であっても数千万円単位の損害が発生すると想定されています。

(NPO法人 日本ネットワークセキュリティ協会調べ)

空き巣と同様、ハッカーは侵入しにくいホームページの攻撃はあきらめることが多いです。

事前に対策をして、防衛を固めておくこと（ハードニング）が必要です

脆弱性診断（ぜいじゃくせい）とは？ プラットフォーム脆弱性診断ツール・イージスEWの特徴は？

※ハッカーが攻撃サイトを選定するツールが、
ASM（Attack Surface Management）と
レコナイツール！ これらの機能がない脆弱性診断
ツールは、意味がありません。

※ペネトレーションテストは、どこのメーカーも、**ほぼ
同じ結果**（基は、OpenVAS@フリーウェアなので）
⇒ 高額支払不要！

ハッカーは、狙いやすい弱点があるホームページや企業のシステムを攻撃します！

不用心だな！
隙だらけだぞ！

~@xx.jp ~@xx.com
ダークウェブに流出した
メールアドレスやパスワード

情報の悪用

ハッカーは、特定の大企業だけを狙うのではなく、事前にASM・レコナイ（偵察）ツールで無差別な偵察を行い、セキュリティ対策をしていない企業を見つけ出します。

ペネトレーション（侵入）テストはサーバに侵入するときに見つかる可能性が高いため、ハッカーはASM・レコナイツールをはじめに使用します！

開かれたポート

侵入と漏洩

放置された古いサーバ

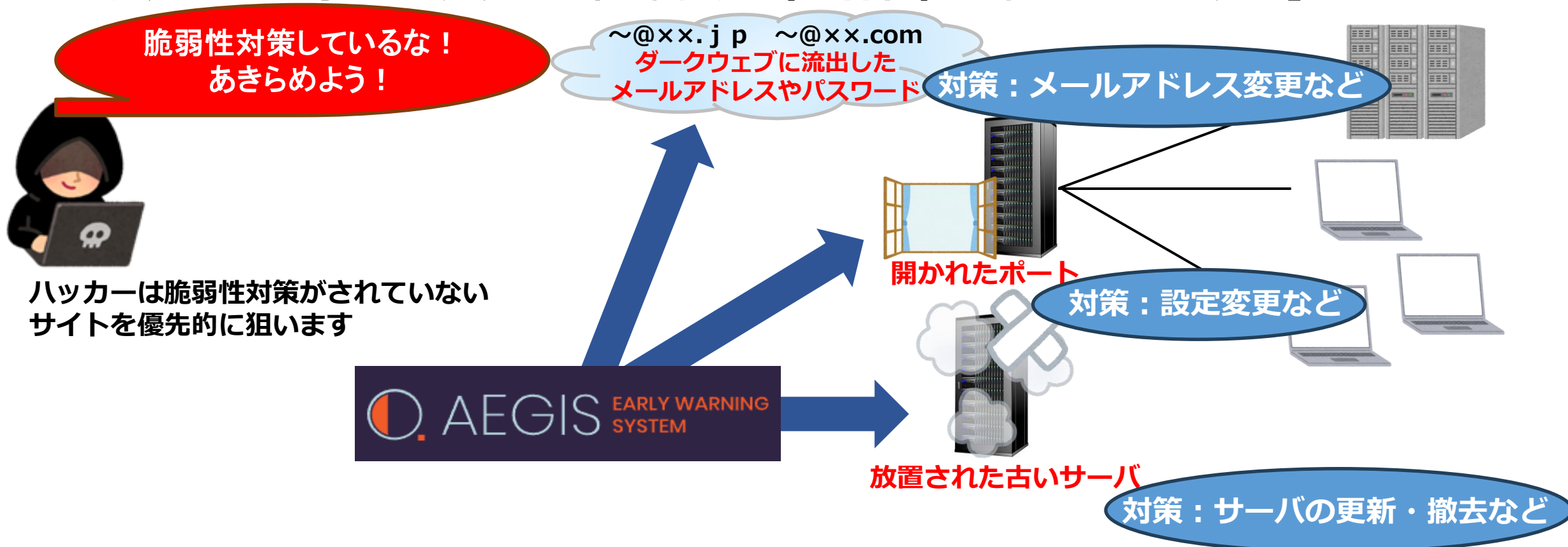
侵入や踏み台

ハッカーが狙う弱点を「脆弱性（ぜいじゃくせい）」といいます。

「脆弱性」は目に見えないため、普通にPCを使っているだけでは気づけません！
ほとんどの脆弱性は、自動で直らないため、自力で対策することが必要です！

脆弱性診断ツールは危険な個所を検出・診断します！

イージスEWは、インターネット上のホームページや社内システムを守るため、「ハッカーに攻撃されやすい危険な個所（脆弱性）を検出・診断する」ツールです



イージスEWがお客様の目に見えない危険な個所を見つけ、**見つけた危険な個所は、専門のスタッフが対応策を説明、または、「伴走サービス」で修正します**

- **人の場合：健康診断**
システムの場合：脆弱性診断

人間の場合は、いきなり細胞診をしたり治療を始めたりしません
まず、健康診断を受け、病気を見つけます

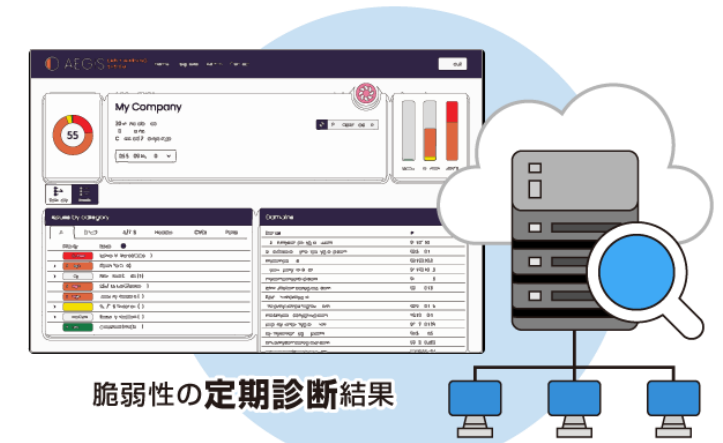
システムも同じで、インターネット上の資産、およびイントラネットの端末に対して診断を行い、検出された脆弱性（ぜいじゃくせい）の緊急度に応じて対策します

最新の機器であっても、日々脆弱性は発見され増えていきます。

1回の診断では不十分です。システムも定期診断が必要です！



人の健康診断



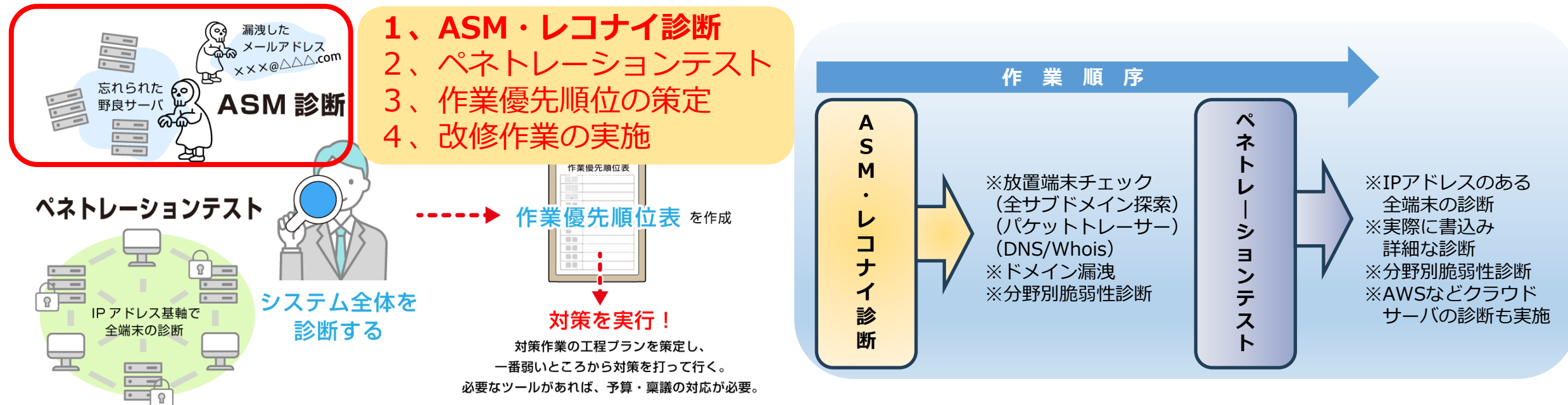
システムの健康診断
||
サイバーセキュリティの脆弱性診断

システムの健康診断 = 脆弱性診断

1. まずASM診断を行い、危険な個所（脆弱性）を見つけ出します

…ASM診断は、申し込むだけでホームページに負担をかけずにできる、お手軽な診断です
イージスEWのASM診断には、他社製品と違い、ハッカーが攻撃対象を探す方法と同種の
「レコナイツール（偵察ツール）」という診断機能が含まれています
イージスEWで診断すれば、ハッカーに狙われやすい個所を先に検出できます！

2. ペネトレーションテストで、検出した脆弱性をより詳しく調べ、効果的な直し方を見つけます



イージスEWで、ホームページの危険性を検出！

脆弱性診断ツール イージスEW (AEGIS-EW)

AEGIS EARLY WARNING SYSTEM

見やすい
GUI

深程度の割合が
円グラフによって
一目で認識できる



分析しやすい
分類分野

グラフは
色で判断可能で、
専門知識は不要です

※専門知識不要！※

赤色

オレンジ色

は危険！

危険な脆弱性を放置すると、ハッカーに乗っ取られ、多大な金銭的被害を受け、社会的信用に傷がつきます！

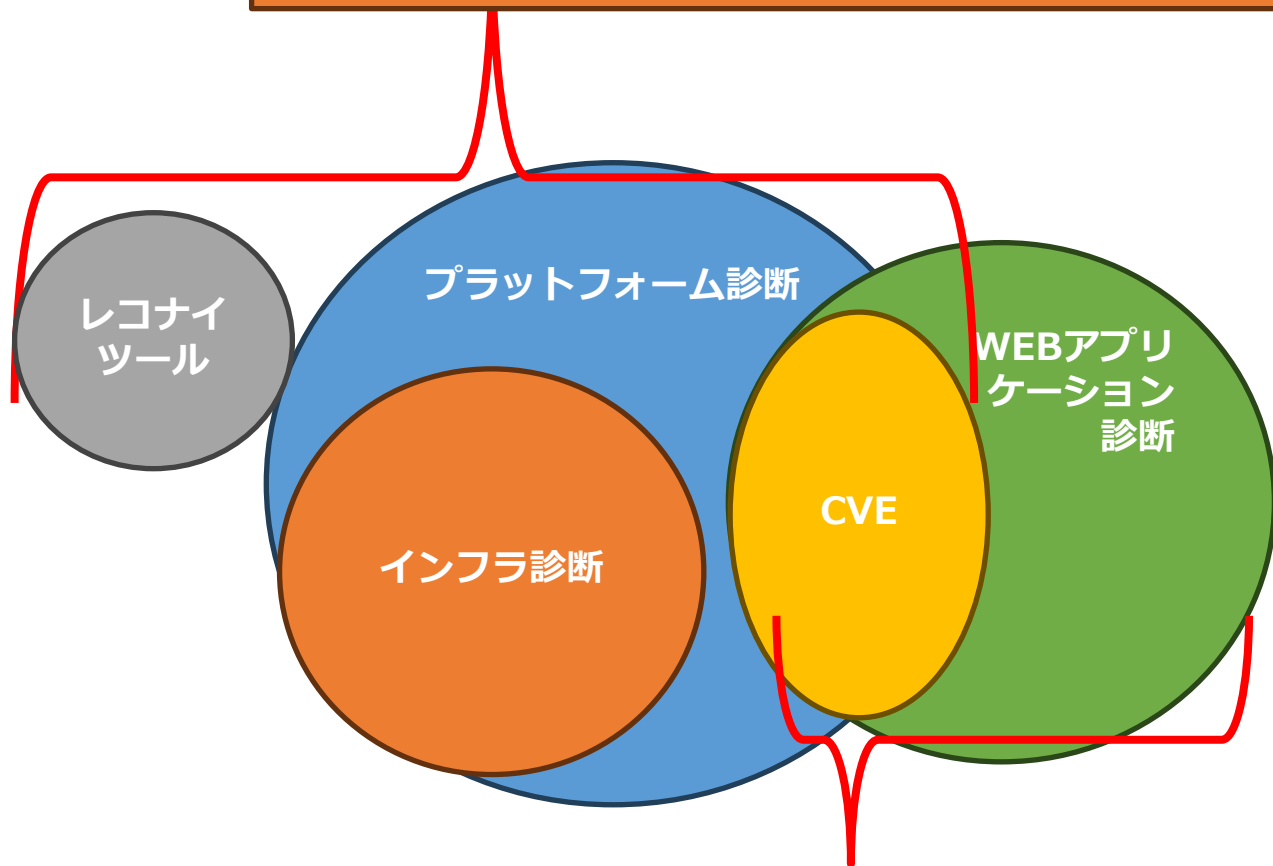
赤色やオレンジ色の危険な個所（脆弱性）が検出されたホームページは
1年目～3年目の初心者SEでも簡単に乗っ取ることができます！

赤色やオレンジ色の脆弱性があるホームページはハッカーの格好のターゲットです！

イージスEWは「ASM診断+レコナイ」「ペネトレーションテスト」が可能です
イージスEWで診断し、赤色やオレンジ色の危険な個所を修正しましょう！！

■ 未来研究所が提供する、脆弱性診断ツール

【イージスEW】プラットフォーム脆弱性診断



OWASP ZAPでのWebアプリ脆弱性診断

【イージスEW】

①プラットフォーム

- ・メールなりすまし対策
- ・ダークウェブ流出・情報漏洩
- ・サーバ証明書の診断

②インフラ 純粋なL4（トランスポート層）

- ・ポート

③CVE 共通脆弱性識別子

④レコナイ（偵察ツール）

- 野良端末検出
- ドメイン情報の漏洩履歴

【OWASP ZAP】

④Webアプリケーション

（OSの脆弱性は、チェックしません。OS部分はプラットフォーム診断がチェックします）

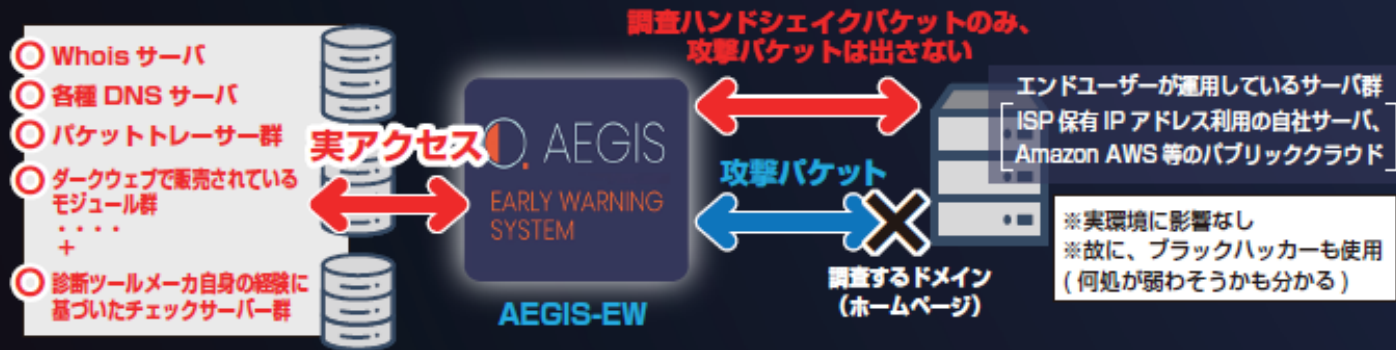
- ・MS系 IIS上のアプリケーション
- ・OSS系 Apache, Nginx, Tomcatなどで動作するWebアプリケーション
- ・クラウド環境系 各種・クラウド上のアプリケーション など

■ 8つの分野別診断項目

脆弱性が8つの分野別に表示されるため、各分野ごとに分析・対策が可能です

CVE 共通脆弱性識別子	CLOUD Cloudプラットフォーム診断	MAIL 送信ドメイン認証	BREACH データ侵害 (情報漏洩)	WEBCERT Web 認証関連	HEADER HTTP ヘッダー 関連	PORT ポートスキャン 攻撃	SUBDOMAIN 野良端末検出
個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番している識別子です。脆弱性検査ツールや脆弱性対策情報提供サービスの多くがCVEを利用しています。	Amazon AWS・Microsoft Azureにおけるセキュリティポリシーを診断します。VPC (Virtual Private Cloud) のデフォルトセキュリティグループが不要な通信を制限しているかを確認します。また、重要なセキュリティイベントに対するアラーム設定やルートアカウントに対するハードウェアMFA (Multi-Factor Authentication) の有効化について確認することも可能です。	「受信したメールが正規の送信元から送られてきたかどうか」を確認できる仕組み。メール送信が行われるサーバ(SMTP)に対して、「IPアドレス認証」や「電子署名」を用いて、「メールのなりすまし」が行われているかどうかを判断します。(SPF,DKIM,DMARCチェックもサポート)	攻撃者が、Webサービス等に攻撃を仕掛けて得た個人情報やデータをダークウェブ等に拡散する行為のこと。特にメール情報の漏洩から発生が多く、メールアドレスを基軸にした診断を実施します。	WEBサーバ証明書に関する認証プロトコル全般の脆弱性チェックを診断します。例えば、TLS、SSLのバージョン情報、等。	WEBアプリケーションとのHTTPプロトコルをセキュアにするための各種ヘッダーのサポート状況を診断します。これにより、サポートOSの正しいチェックモジュールが搭載されているか、攻撃防御を実施するための設定が成されているか、等をチェックします。	ポートスキャンからの外部侵入に対する脆弱性の診断を行います。必要最低限のポートのみを使用し、不要なポートは常に閉めておく対策が求められます。	サブドメインの管理は、セキュリティにおいて非常に重要な要素です。管理されていない野良端末（特に開発環境やテスト環境）が存在する場合、攻撃者にその隙間を突かれるリスクが高まります。野良端末検出機能は、これらの放置されたサーバを自動的に探し出して、リスト化します。
			レコナイ ツール				レコナイ ツール

Passive Scan (受動スキャン) ASM (Attack Surface Management)



※ASMは、ハッカーが最初に使用するツール
使用することで何がわかるのか？

- ・ 野良端末の存在が分かります
(多くは、**完全放置状態**。モジュールが古く、
乗っ取り可能な場合が多い)

- ・ 機器のファームバージョンが分かります
(バナー表示がONの場合)

→ **VPNルータの簡単乗っ取り**

- ・ 外部サービス経由で漏洩したドメイン由来
の個人情報も分かります

→ **例：社員のメールアドレスが
PW付きで漏洩している**

Active Scan (ペネトレーションテスト)



※ペネトレーションテスト

IPアドレスを基軸に、深い部分まで侵入を
試みた結果を表記する。

イージスEWでは、OpenVAS
(Github/Freeware) を網羅した
GreenBorn社のAPIを使用し、7万件にも渡る
診断項目で対応

イージスEW 無料ASM脆弱性診断&結果説明会

■ 無料ASM脆弱性診断の実施後に報告書を作成し、説明会を実施いたします

イージスEWの無料ASM脆弱性診断結果の説明会を無料で実施いたします。
(個別の脆弱性の詳細を分析するためには、有料診断が必要です)

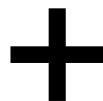
無料説明会

検出された脆弱性診断結果の
簡易的な対処方法をお伝えします

【イージスEWにより自動生成される評価レポート】

※サマリー版

※有料版：CVSS、CVE 等、過去の漏洩情報も記載



Cyber Security Board Report

Date: 2020-07-03
Demo

Data breaches^{1,2}
There are 6 email breaches, of which 2 are critical. You have accepted no email breaches.
The most recent breach was December 2021.

Web certificates and encryption^{1,2}
There are 14 web certificates that pose a non-critical security threat. You have accepted no security threats.
No data from the previous month.
In the past three months there were 14 domains that have only been seen with issues.

Open ports^{1,2}
There are 14 server addresses with open ports, totaling to 57 open ports. There are 3 server addresses with critical open ports, totaling to 3 critical ports. You have accepted no open ports.
No data from the previous month.
In the past three months there were 14 server addresses that have only been seen with open ports.

Server vulnerabilities^{1,2}
There are 39 server addresses with vulnerabilities, totaling to 263 vulnerabilities. There are 2 server addresses with critical vulnerabilities, totaling to 92 critical vulnerabilities. You have accepted no vulnerabilities.
No data from the previous month.
In the past three months there were 39 server addresses with vulnerabilities.

Notes:
1. The counts in each section are of non-accepted as audited and deemed secure or otherwise not a concern.
2. Active port data. Only including prior collections via active port data. Only including prior collections via active port data.

Demo

C (51/100)
Collected 1125 days ago
15:28, 03 Jul 2020

Domains (98 identified)

Domain	IP	Grade	Protocol
ablink.nz.demo.aegis-ew.com	172.16.0.61	A	TLS 1.2, TLS 1.3
ablink.nz.c.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
ablink.nz.demo.aegis-ew.com	172.16.0.81	A	TLS 1.2, TLS 1.3
ablink.nz.f.demo.aegis-ew.com	172.16.0.91	A	TLS 1.2, TLS 1.3
ablink.online.c.demo.aegis-ew.com	172.16.0.121	A	TLS 1.2, TLS 1.3
ablink.yourorder.b.demo.aegis-ew.com	172.16.0.131	A	TLS 1.2, TLS 1.3
abmail.nz.b.demo.aegis-ew.com	172.16.0.551	A	TLS 1.2, TLS 1.3
abmail.nz.c.demo.aegis-ew.com	172.16.0.741	A	TLS 1.2, TLS 1.3
abmail.nz.demo.aegis-ew.com	172.16.0.21	A	TLS 1.2, TLS 1.3
abmail.nz.f.demo.aegis-ew.com	172.16.0.31	A	TLS 1.2, TLS 1.3
abmail.online.c.demo.aegis-ew.com	172.16.0.41	A	TLS 1.2, TLS 1.3
abmail.yourorder.b.demo.aegis-ew.com	172.16.0.81	A	TLS 1.2, TLS 1.3
access.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
adverts.c.demo.aegis-ew.com	172.16.0.131	A	TLS 1.2, TLS 1.3
api.b.demo.aegis-ew.com	172.16.0.211	A	TLS 1.2, TLS 1.3
api.demo.aegis-ew.com	172.16.0.521	A	TLS 1.2, TLS 1.3
autodiscover.b.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
autodiscover.c.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
autodiscover.d.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
autodiscover.f.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
beta.c.demo.aegis-ew.com	172.16.0.31	A	TLS 1.2, TLS 1.3
bringtrack.b.demo.aegis-ew.com	172.16.0.63	A	TLS 1.2, TLS 1.3
catalog.c.demo.aegis-ew.com	172.16.0.51	A	TLS 1.2, TLS 1.3
c.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
chipotle.c.demo.aegis-ew.com	172.16.0.51	A	TLS 1.2, TLS 1.3
d.demo.aegis-ew.com	172.16.0.751	A	TLS 1.2, TLS 1.3
delivery.b.demo.aegis-ew.com	172.16.0.741	A	TLS 1.2, TLS 1.3
demo.aegis-ew.com	172.16.0.721	A	TLS 1.2, TLS 1.3
dev.b.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
dev.c.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
e.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3
exchange5.demo.aegis-ew.com	172.16.0.71	A	TLS 1.2, TLS 1.3

Issues by category (139 vulnerabilities)

Priority	Issue	Count
CRITICAL	Server Vulnerabilities	2
CRITICAL	Open Ports	3
CRITICAL	Breached Email	3
HIGH	Server Vulnerabilities	1
HIGH	Open Ports	1

Data breaches

Email Address	Company Breached	Date of Breach	Breached Information
xxxxxxx1@demo.aegis-ew.com	Zomato	2017-05-17	Email addresses, Passwords, Usernames
xxxxxxx1@demo.aegis-ew.com	Zynga	2019-09-01	Email addresses, Passwords, Phone numbers, Physical addresses, Social media profiles
xxxxxxx1@demo.aegis-ew.com	db8151dd	2020-02-20	Email addresses, Job titles, Names, Phone numbers, Physical addresses, Social media profiles
xxxxxxx3@demo.aegis-ew.com	Apollo	2018-07-23	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles
xxxxxxx2@demo.aegis-ew.com	FlexBooks	2021-12-23	Email addresses, Names, Partial credit card data, Passwords, Phone numbers
xxxxxxx2@demo.aegis-ew.com	MGM2022Update	2019-07-25	Dates of birth, Email addresses, Names, Phone numbers, Physical addresses

Web certificates and encryption

Domain	IP	Grade	Protocol
ablink.nz.b.demo.aegis-ew.com	172.16.0.63	A	TLS 1.2, TLS 1.3
ablink.nz.c.demo.aegis-ew.com	172.16.0.61	A	TLS 1.2, TLS 1.3
ablink.nz.demo.aegis-ew.com	172.16.0.31	A	TLS 1.2, TLS 1.3
ablink.nz.f.demo.aegis-ew.com	172.16.0.67	A	TLS 1.2, TLS 1.3

ぜひこの機会に
ご検討ください。
お待ちしております。

お申し込みは、
sales@future-research.jp
までお気軽にどうぞ！

	価格（税抜）	主な機能
ASM診断	総ドメイン数：1～9 1回：85,000円 年間月1回：235,000円 年間週1回：290,000円	サブドメイン探索 CVE（共通脆弱性識別子）検出 オープンポート調査 Webサーバ証明書調査 HTTPヘッダー調査 メールなりすまし対策状況調査 データ侵害・情報漏洩調査
ペネトレーション テスト	総ドメイン数：1～9 1回：150,000円 年間月1回：555,000円 年間週1回：665,000円	Cloud（Amazon AWS・Microsoft Azure）調査 各端末の詳細な診断

※ASM診断には、レコナイツール（偵察ツール）診断機能が含まれています

※「総ドメイン数」とは、お客様のホームページドメイン「www.ooo.jp」から派生した、全ての関連ドメインの数です。

■ イージスEW診断結果・有料セミナー

有料診断結果全般の説明と、各脆弱性分野の対策方法レクチャ、および実際の対策セミナーを実施させていただきます。

ご要望があれば、エンジニアによる改修支援も可能です。（伴走サービス）



■ 脆弱性診断結果の改修サービス「伴走サービス」

CVSS緊急・重要脆弱性の改修支援を、週1日就業（35h/月）～から提供します。
遠隔地の場合、Edge-BOX（VPN BOX）をお送りし、お客様と一緒に改修します。
脆弱性リスクを解決する人材をお探しの際は、是非ご相談ください。

■ MIRAIサービス

脆弱性診断結果の改修サービス「伴走サービス」以外にも、IT技術者が不足して「一人IS」「IS不在」を余儀なくされている SME・中堅企業様への、IS代行サービスを行います。専門知識と技術を持った弊社スタッフがサポートします。

- 「サイバーセキュリティ対策を、エンドユーザの状況・要望に合わせた、長期的な伴走サービス（ハードニング）」
 - － 例：
 - CSIRT、PSIRT、JC-STAR、SBOM等への対応を実施したいが、ISMSの認証取得をしていない
 - － 新たな1年プロジェクトで、ISMS取得(必要時ISO27017も)を新規スタートさせて、並行してサイバー業務も遂行
 - 上司がサイバーの知見がなく「サイバー予算の承認が出ない」
 - － 社内で、「サイバー事業でのDX新規事業（3年後の外販開始）」を立ち上げ、外販の前に社内での知見を積み上げることで、承認。（近い将来、お金を生むなら承認する by 役員）
 - － 役員会議でのCIO/CISOの新設を打診、現状上司の範疇外で承認させ遂行
 - 部下の「担当者がいない」を言い訳に、サイバー業務がすすまない
 - － 社内で、組織を横断した新プロジェクトメンバーを募集し、役員直下のハンドリングで実施
 - 大学群では、2千を超すIPサブドメイン数が存在し、多数の深刻度が高いぜ弱性結果が存在する
 - － 新たに、「大学メインドメイン使用におけるセキュリティポリシー」を、策定（原案あり）し、1年間をかけてインターネット上で検索されるドメイン数を、数百以下に抑えハードニング化を実現

- よくある、「サイバー対策の誤認・間違い例」
 - ISMSは取得してないが、CSIRT・PSIRTを設置・運用したい
 - 結局、ISMSの取得も必要になる。
 - メーカー営業マンから勧められたUTMだけ入れて満足しており、他のセキュリティ対策は行わず、放置されている
 - 社内のイントラ側の防御のためにUTM+ルータにて対応を実施。ただし、エンドユーザは、本ルータでインターネット上のHP等の資産も守られると主張……
(エンドユーザの学習不足)
 - ペネトレーションテストを実施しているので、完全だと思っている
 - ASM・レコナイの存在を知らない（野良端末からの乗っ取り発生）
 - 最初からペネトレーションを掛ける、バカなハッカーは居ない（ことを知らない、）
 - 病院・県市町村の担当者に多い
 - 大手SIが、ASM・レコナイの必要性を担当者に説いていない
 - » 大手SIでは、現行システムでの深刻度がひどく、無料改修/大変な減額改修を強要されてるので、ASM/レコナイを、極力行わない指針
 - ホームページサービスプロバイダーが、責任を被ると思っている
 - ポートの脆弱性を治せないプロバイダーを使用し、該当ポートからの乗っ取りは、プロバイダーが責任を取ってくれると勘違いをしている（要、読破・使用権許諾書）
 - 他社セキュアHPプロバイダーへの、引っ越しを推奨・運用支援を実施
 - AWS,AZURUの仮想OS使用者も同様の認識を持った担当者も存在

Thanks