未来研究所
Future Research Inc.

未知の脅威から守る新たなる盾。次世代ASM【パッシブスキャン】ツール

AEGIS-EW（イージス EW）

御紹介

2023年8月

株式会社　未来研究所

TITANIUM DEFENCE
Ultimate Cyber Security Protection

AEGIS EARLY WARNING SYSTEM

ASM・パッシブスキャン＋ペネトレの決定版
AEGIS-EW

公共施設へのサイバー攻撃事例

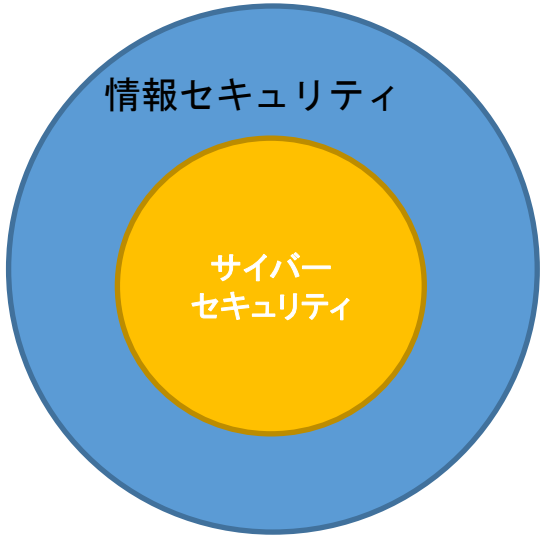
インシデント（Incident)概要

■「インシデント」とは何か？

サイバーセキュリティの用語としての意味は、次のとおりである。

①広義における「インシデント」

「インシデント」とは、情報セキュリティのポリシーや基準に違反することを指す。
インシデントが発生すると、情報資産やシステムに悪影響を及ぼすため、組織や個人は迅速に対応する必要がある。
これにより、被害の拡大を最小限に抑え、システムやデータの保護を確保することが目指す。



②狭義における「インシデント」

サイバーセキュリティ分野における「インシデント」とは、セキュリティ侵害や異常な出来事の発生を指す。
具体的には、システムへの不正アクセス、マルウェア感染、データ漏洩、サービスの停止、サイバー攻撃などがインシデントの一例に該当する。

インシデントによる負担費用

未来研究所
Future Research Inc.

■情報流出における費用負担の一例

情報流出における費用負担には、膨大なコストが必要となる。
以下は、一般的に知られている負担費用例である。

①EU圏が批准しているGDPRにおける例

GDPR（General Data Protection Regulation：一般データ保護規則）によれば、
一般的なデータ保護の規則（第83条）では、最も重大な違反に対しては次のような最低罰金額が設定されている。
(https://gdpr.eu/fines/)

- **一般的義務に違反した場合：**
  最大で2,000,000ユーロ（3億円）または年間売上高の2%のいずれか低い方。
- **個人の権利と自由に関する義務に違反した場合：**
  最大で10,000,000ユーロ（１４．８億円）または年間売上高の4%のいずれか低い方。

②JNSA：2018年情報セキュリティインシデントに関する調査報告書

(https://www.jnsa.org/result/incident/2018.html)

- 2018年では、4万円/1件の費用が必要。

次ページにて、過去発生したインシデント具体例について解説する。

公共施設へのサイバー攻撃事例

未来研究所 Future Research Inc.

- 公共系での個人情報流出・
  住民情報のランサム被害では、個人への賠償金払いも含め、
  然るべき対応求が求められます
  - ー　サイバー先進国でのCISO
    引責辞任は、株主訴訟上、必須となりつつあります
    →　特に公共サイトの被害では、プレス発表の義務化に加え、日本も同様の対応が求められる傾向になるのでは？
  - ー　宇治市・住民基本台帳データ・
    ２２万人（訴訟結果：1.5万円/人
    ＝Total**３３億円**の支払い）
    - https://www.mc-law.jp/kigyohomu/9055/
  - ー　小型のインシデントは散見
- 右表に公共系でのサイバー
  攻撃・事例を示します。
  - ー　公共系の攻撃は、年々増してます

【市町村・県　編】

発生日時	被害者	インシデント概要
2022/10/12	北海道千歳市	標的型サーバ攻撃・メールサーバの乗っ取りにより、81,084件の不審メールを発信したほか、メルマガ購読者の個人情報198件が流出
2022/7/1	全国一般市民	自治体などに提供している電子申請サービスに付随するヘルプデスク業務で、受託会社作業者端末がEmotet(エモテット）に感染、全国使用者とのメールやり取り2,312件が流出した
2015/8/26	長野県上田市	標的型サーバー攻撃：マイナンバーカードDBの流出

【文教・学校　編】

発生日時	被害者	インシデント概要
2023/3/1	静岡県浜松市　浜松開誠館中学・高校	過去5年分以上の生徒の成績データなどが流出し、暗号化された
2023/1/10	つくば市教育委員会	つくば市の小学校＆中学校の学校用WEBサイトが乗っ取られ、更新に必要なIDやパスワードが書き換えられた。これにより、つくば市配下の45校のホームページが使えなくなり、ワーム等の不正プログラムの常駐も確認された。（ただし、原因等は、未公開と予測される（HP上、見つけられなかった））
2022/7/1	千葉県南房総市　小中学校群	VPNルータが乗っ取られての、ランサムウェア被害 小学生1293人、中学生724人の個人情報（住所、氏名、保護者連絡先、成績、出席情報など）流出した後、暗号化された。

【病院　編】

発生日時	被害者	インシデント概要
2022/12/3	金沢西病院	ランサムウェア被害で、診察システムが２か月間に渡りダウン。 システム復旧に２か月間が必要と成り、紙で対応。ただし、医療費はシステム復旧後での請求処理となった。
2021/10/1	つるぎ町立半田病院	VPNルータが乗っ取られての、ランサムウェア被害。３か月間の紙カルテでの対応を余儀なくされた。
		ブラックハッカー集団「LockBit]の声明と病院側の報告の食い違いも、注目を浴びてしまった。（LockBitがお金を取れなかった腹いせ論との見方が多いが、、）

サイバー攻撃パターン例

未来研究所 Future Research Inc.

■サイバー攻撃パターン例

サイバー攻撃には多彩な手法があるが、「通常の保守範囲」で防げるものも多い。下記にその一例を挙げる。

Step1. 多くのケースでは、「VPNルータを**ゼロディ攻撃**(右図：**7位**)で乗っ取る」ことにより攻撃が始まる。これにより、攻撃者は「ネットワーク経由で、自由にルータへアクセス可能」な状態となる。主な原因は、「運用保守がされておらず、ルーターソフトウェアが更新されてない」ためである。

Step2. 攻撃者は、乗っ取ったVPNルータから、内部ネットワークに存在するサーバを探す。多くのVPNルータでは、SSHクライアントをサポートしているため該当サーバのID/PW奪取を行い、標的型攻撃(右図：２位)によりメールサーバの乗っ取り等を行う。

Step3. Step2の実行により、有益な情報の窃盗を完了後、ランサムウェア攻撃(右図：１位)に移行する。このため、ランサムウェア被害に遭うということは、「既に重要データ等が奪取済である可能性」を留意する必要がある。

結論. **「適切な保守運用が行われないＶＰＮルータは、攻撃されるリスクが高い」**

順位	攻撃手法
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報の窃取
3位	サプライチェーンの弱点を悪用した攻撃
4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
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	ビジネスメール詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

独立行政法人情報処理推進機構（IPA）「情報セキュリティ10大脅威 2022」(https://www.ipa.go.jp/security/10threats/10threats2022.html)より抜粋

ゼロディ攻撃とは？

■ゼロディ攻撃とは？

新しく発見されたサイバー攻撃は、仔細な防御方法も含めCVE（共通脆弱性識別子）として採番される。そのCVEは、CWE（共通脆弱性タイプ一覧）として対策防御方法の情報も付加されDB化されます。CWEは、誰もが一律にそのDBへのアクセスが許され、対策防御方法の情報を取得できるサービスです。ハッカーはこの公開サービスを活用し、該当CVEの未対応サイトに対し、対策防御方法の情報から簡単に憶測される攻撃方法により、乗っ取りを実行する。この攻撃の事をゼロディ攻撃と言います。

【ハッカーへの必要情報販売サイト：ダークウェブ】

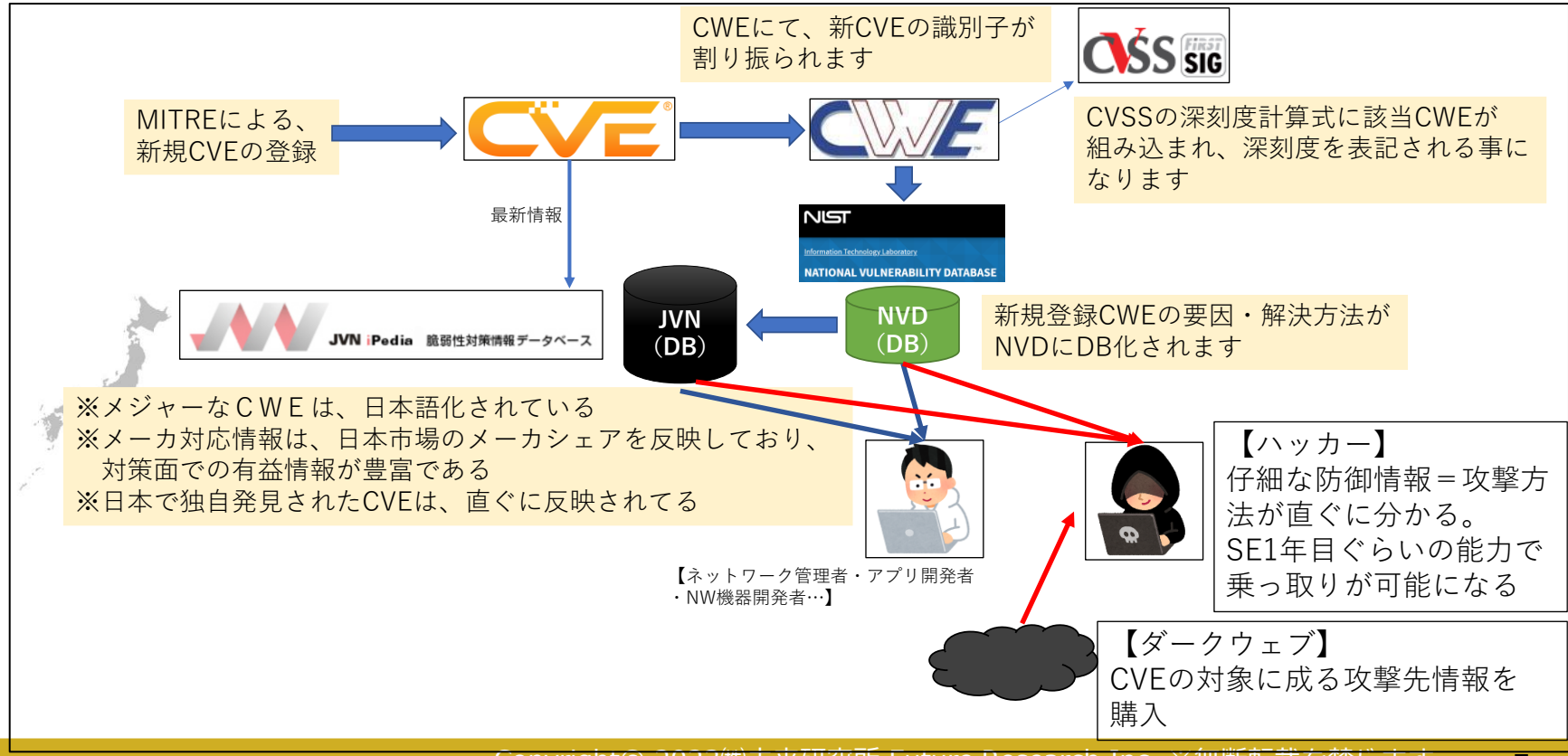
新たなサイバー攻撃が登録されるとダークウェブ上では、

・攻撃ツール
・漏洩しているDBからの対象先情報
・入金時に使用するBitコイン

等々、攻撃に必要な情報が販売されます。脆弱性診断での深刻度が高い場合、SE職1年目レベルの能力で、乗っ取りが可能となります。

■ゼロディ攻撃の真の原因と対策は？

新規に登録されたCVEへの対処をハッカーより先に、システム管理者が終えれば防御できる。
遅ければ、ハッカーの侵入を許すことになる。**（タイムリーな運用保守が必要）**



ゼロディ攻撃への具体的な対策とは？

未来研究所
Future Research Inc.

■インシデントを起こした日本の公共系インシデントの主要因

・VPNルータオプション（自動プログラム更新・フィルター更新・メール通知等）をオーダしておらず、ゼロディ攻撃への対策がなされておらず、脆弱性の放置状態になっていた

落札金額の高騰になるため、逸注を恐れ、SIメーカも真剣にアピールせず

・IT担当者・購入責任者の知識不足

システム検収時の脆弱性診断結果（ASM・ペネトレーション）の提示を義務化していないケースが多い。
また、診断結果への理解不足も否めない

■ゼロディ攻撃への対応を、自動化・定期化する仕組みの実現

・ゼロディ対策を有した、機材・システムを選定すること

UTM/VPNルータ、WAF等のH/W機器メーカおよびインフラアプリ・メーカには、新規サイバー攻撃に対する対応プログラムを早急にリリースし、そのプログラムを対象機器（H/W、サーバ等）に自動インストールする仕組みが必要である

・**定期的な脆弱性診断（ASM・ペネトレーション）が必要**

脆弱性診断の対象範囲は、ネットワーク分野からサーバ・アプリ設定も含むCVE分野まで、広範囲に渡る。
この脆弱性診断を定期的に実施することで、運用にて新たに生じた脆弱性も含め、強固なシステムを維持することができる。

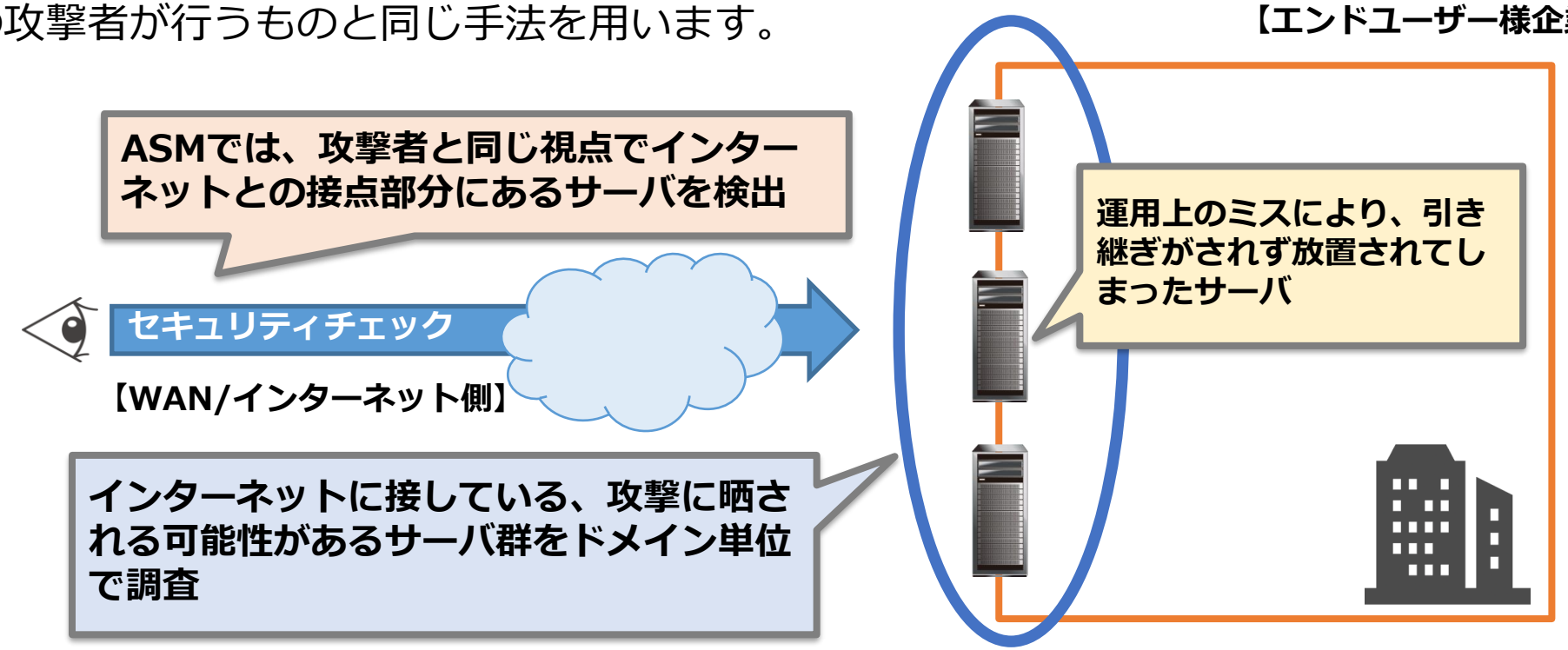
ASM(Attack Surface Management)とは？

機能概要説明

ASM(Attack Surface Management)とは？

■ASM(Attack Surface Management)とはなにか？

組織で管理しているIT資産のうち、攻撃対象として晒される部分に接しているIT資産を洗い出すことによって、
サイバーセキュリティ対策に役立てる取り組みのことです。
日本語では、「攻撃対象領域管理」と呼ばれます。
他のサイバーセキュリティーの分野とは異なり、ASMでは「攻撃者の視点」から行われます。
攻撃ターゲットを特定し、攻撃者からみてチャンスとなり得るリスクを評価します。
これには、実際の攻撃者が行うものと同じ手法を用います。



ASM(Attack Surface Management)の必要性は？

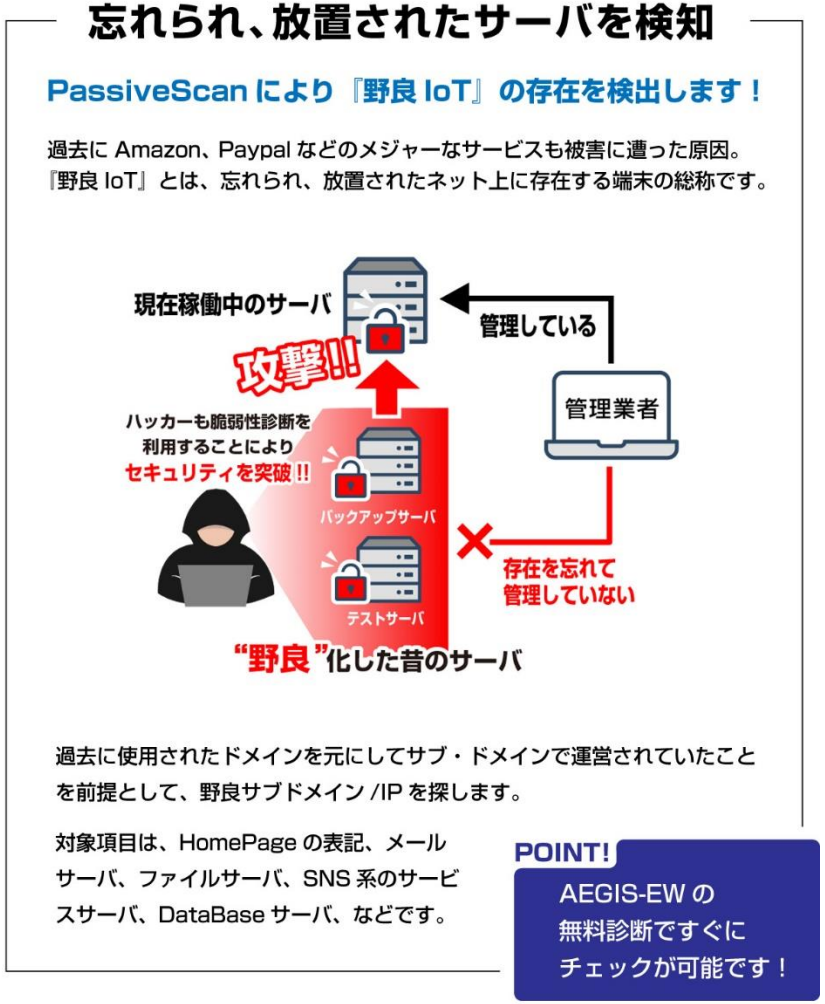
未来研究所 Future Research Inc.

■ASM(Attack Surface Management)の必要性

組織におけるIT資産管理という観点に着目してみると、長期間の運用を通じて「管理しているIT資産」と「実際のIT資産」に乖離が生じます。
これは、「運用組織の変更」「引き継ぎ時での申告漏れ」「管理対象が多岐に及ぶため管理できない」などの実態が存在するためです。

「把握済み稼働システム」のみを監視・制御しても、「放置サーバ（野良サーバ）」が存在すればこれを足がかりにして稼働システムを乗っ取ることが可能です。
なお、私ども未来研究所では、これらの運用管理から外れてしまったサーバを**「放置サーバ（野良サーバ）」**と定義しています。

これらの事象に対しASMを用いることによって、「サイバー攻撃者の視点」から「現在の組織で実際に稼働しているサーバ」という事実を元に、組織内のIT資産を発見するための取り組みを行います。



ASMと脆弱性診断　言葉の定義

未来研究所
Future Research Inc.

■ASMと脆弱性調査の違い

ASMと脆弱性診断の違いは、次のとおりです。
最も大きな違いは、脆弱性診断が「既知のサーバのみ」対象にしているのに対して、
ASMでは動的に「認知外のサーバ」も洗い出して調査対象とします。

ASMとは？
　組織の外部（インターネット）からアクセス可能なIT 資産を発見し、 それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセスをいう
出典；経済産業省ASM (Attack Surface Management）導入ガイダンス

①パッシブスキャン(Passive Scan)
パッシブスキャンでは、ドメイン情報から放置サーバ（野良サーバ）を検出して診断します。
②アクティブスキャン(Active Scan)
アクティブスキャンでは、調査対象診端末に対して、ハッカーと同様の攻撃手法を用いる診断方法（ペネトレーションテスト）を行って診断します。

広義の定義	脆弱性診断	脆弱性診断
狭義の定義（経済産業省・定義）	ASM	脆弱性診断（ペネトレーションテスト）
代表されるスキャン方法	パッシブスキャン(Passive Scan)	アクティブスキャン(Active Scan)
診断対象	インタネット上を検索し、発見した端末を対象とする	対象をあらかじめ指定（IPアドレス等）指定する
脆弱性の確定方法	通常アクセスの範囲で行うため、確度が低い可能性がある	攻撃を模したパケットを送信、その応答を診断するため確度が高い
対象への影響	パケットがセキュリティ監視装置（EDS/EDR）に検出されることは殆どない	セキュリティ監視装置（EDS/EDR）で検出される可能性は高い
AEGIS-EWラインナップ	AEGIS－ASM診断	AEGISペネトレ

参考：経済産業省
「ASM (Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」
https://www.meti.go.jp/press/2023/05/20230529001/20230529001-a.pdf

ASM・パッシブスキャンとペネトレ・アクティブスキャンの役割

未来研究所
Future Research Inc.

■ASMとペネトレーションの３プロセス

システムを診断する場合、次の３つのプロセスにてサーバ脆弱性の評価を行います。
この際に「パッシブスキャン」と「アクティブスキャン」という２つの手法を用いて調査します。

【凡例】
パッシブスキャン・・・・
アクティブスキャン・・・

Step1.調査対象の発見
まず調査対象のドメインに対してDNSによる検索や、パケットトレーサ、独自DBなどを活用して IPアドレス・ホスト名の一覧を取得します。これによって、「調査対象の組織に含まれるインターネットに接しているサーバ群」を特定します。具体的には「グローバルIPアドレス」と「ホスト名」の組み合わせを取得します。これによって、調査対象の保有するインターネットからアクセス可能なサーバ群を発見します。

Step2.調査対象の情報収集
Step1で発見したサーバ群に対して、より詳細な情報を収集します。このプロセスでは、攻撃面を構成する個々の IT 資産における OS、ソフトウェア、ソフトウェアのバージョン、オープンなポート番号などを収集します。なお、この時点では、調査対象に影響を及ぼさないよう「アプリケーションが定義した通常のアクセス方法」を用います。

Step3.調査対象のリスク評価（ペネトレーションテスト）
Step2で収集した情報をもとにサイバー攻撃へのリスクを評価します。
「公開されている既知の脆弱性情報」と「Step2」の情報から脆弱性を判断します。

放置サーバ（野良サーバ）発生の原因は？

■放置サーバ（野良サーバ）発生の多い原因

ネットワーク運用での引継ぎ忘れ、サーバの閉じ忘れが原因です。

①どのような場所で多発するのか？

A. 公共サービス、病院、学校等

②なぜ放置サーバ（野良サーバ）が発生するのか？

B．「インフラ管理者」が年単位で直ぐに変わってしまう
- インフラ保守の主体であるベンダーは、公募により変わってしまう。

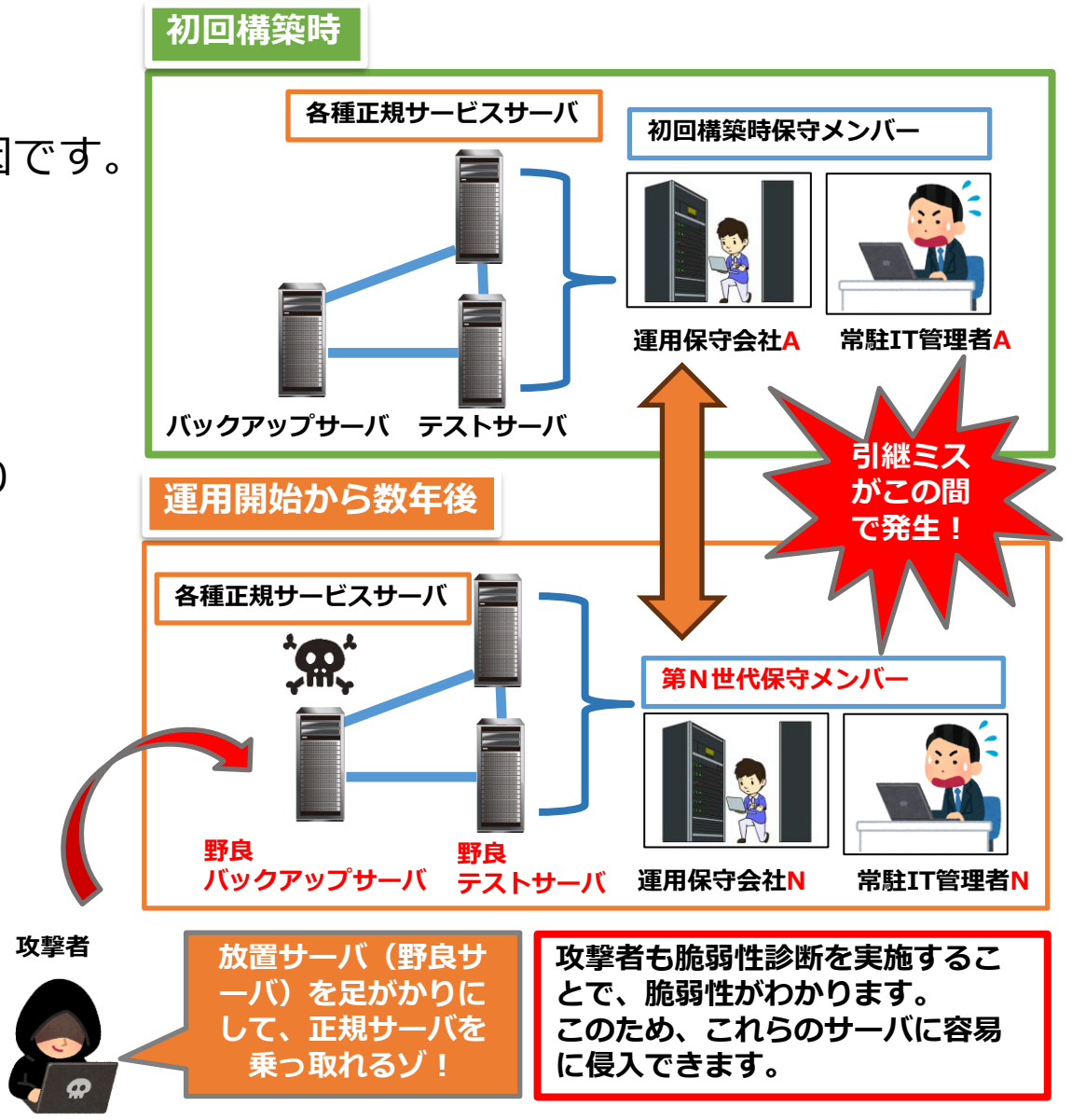
C．「引き継ぎ」が正しくされない
- ネットワーク仕様書に記載の無い「バックアップ・テストサーバ」が忘れられている。

結論：

長く使用されているドメインほど、危険度が高い

攻撃者は、攻撃の足がかりとするための「放置サーバ（野良サーバ）」をいつも探しています。

AEGIS-EW（イージス EW）によるパッシブスキャンで「放置サーバ（野良サーバ）」洗い出しをオススメします。



AEGIS-EW ASM（パッシブスキャン）の脆弱性検出手法

■ASM・Passive Scan(パッシブスキャン)について

日本において「サイバーセキュリティ脆弱性診断」を指すとき、その定義は「非常に曖昧なもの」となっています。一般的は、次スライドにて説明する「Active Scan（ペネトレーションテスト)」を指す場合が殆どです。
しかし、「Active Scan（ペネトレーションテスト)」だけでは「診断漏れ」が発生します。
これは、**「管理者さえも認知していない放置サーバ（野良サーバ）」**が存在するためです。

この「放置サーバ（野良サーバ）」を発見するための技術が「Passive Scan(パッシブスキャン)」です。
パッシブスキャンでは、ドメイン情報から関連するサーバを自動で検出します。
また、該当のサーバに対して「アプリが規定する標準の通信」を用いて、脆弱性を診断します。
なお、サイバー先進国（米国・英国・オセアニア等）では、Passive ScanとActive Scanの両モードを実施しています。

AEGIS-EW
ペネトレーションテスト（アクティブスキャン）の脆弱性検出手法

■ペネトレーションテスト（Active Scan）について

Active Scan（**ペネトレーションテスト**）の特徴
攻撃者が行うサイバー攻撃と同様の手法を用いて、脆弱性レベルを診断します。

これにより対応方法も明確となる（サイバーセキュリティ防御能力アップ：ハードニング）
ただし、**「端末のIPアドレスが事前に分かっていることが前提」**です。
開発案件の納品時に、サイバー攻撃に対するハードニング（堅牢性の施策を施すこと）証明としてActive Scanの結果を添付します。
サイバー先進国での公共機関では、契約の条件として審査時の要件となっています。

AEGIS-EW(イージス EW）のご紹介

サイバー健康診断（ASM診断）のおすすめ

AEGIS-EW特徴：メリット

未来研究所
Future Research Inc.

【必要な情報は、メインドメインのみ】
例：　XXX.co.jp, YYY.jp, ZZZ.com

①エンドにとって使いやすく、提案が容易！
「サブドメイン自動検出機能つき」
②脆弱性診断結果が一目で解り、説得しやすい！
「視覚的なサーバ安全度スコアリング」
③他社製品と比較して、安い！
「明瞭かつ低価格な導入コスト」

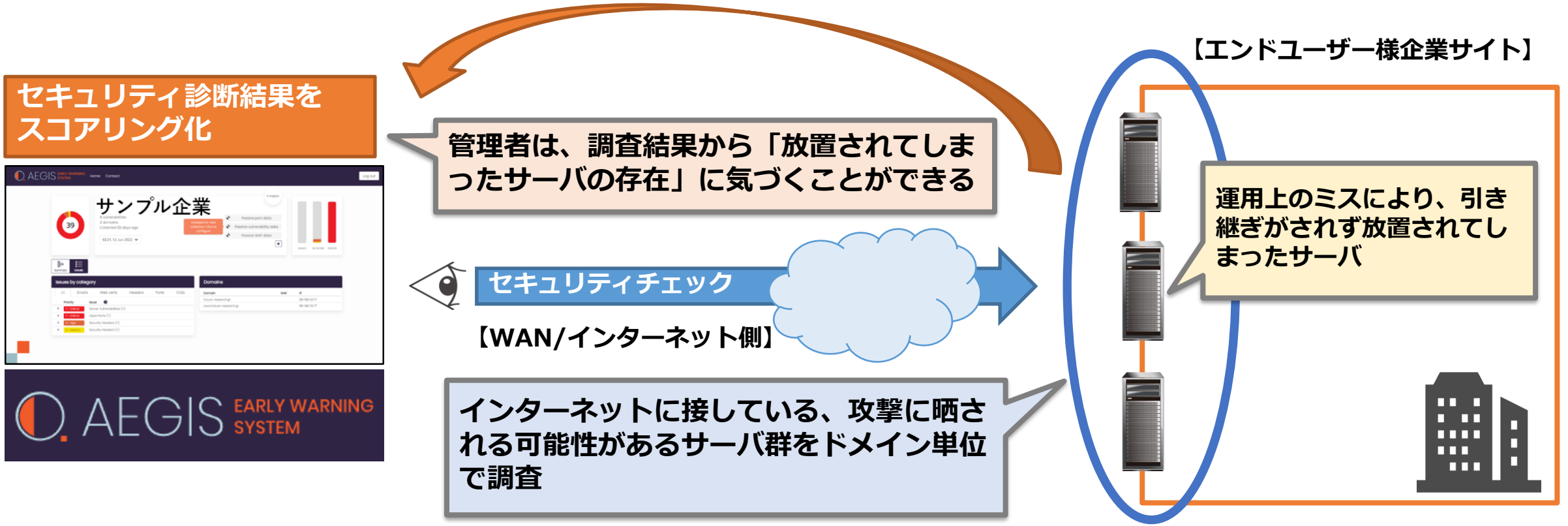
AEGIS-EWは、ドメイン情報を元にインターネット上に存在するサーバ群を、
自動検索し、脆弱性を診断します
（社内ネットワーク端末を診断する場合は、別商材（Edge-BOX）を使用します）

ASMツールAIGES-EW(イージス EW)とは？

未来研究所 Future Research Inc.

■AIGES-EW(イージス EW)におけるASM

AIGES-EWは、このASMを実現するためのツールであり、
ASMのうち「EASM(External Attack Management:外部攻撃対象領域管理)」を担当します。
EASMでは、インターネットなどの「組織の外部に公開しているIT資産」を対象とした脆弱性とリスクに焦点を置いています。



AEGIS-EW特徴：放置サーバの発見

■サブドメイン自動検出機能

AEGIS-EW(イージス・EW)の最大の特徴は、
メインドメイン名からサブドメインも自動検出して脆弱性診断を行うことができる点です。
Nessusにも、OpenVASにも無いオリジナル機能です。

サブドメインを自動検出して、
脆弱性診断対象としてデータベース化

【エンドユーザー様所有ドメイン】
お客様ドメイン名.co.jp

ドメイン名.co.jp	IPアドレス
サブ・ドメイン名A.co.jp	xxx.yyy.xxx.zzz
サブ・ドメイン名B.co.jp	xxx.yyy.xxx.zzz
サブ・ドメイン名C.co.jp	xxx.yyy.xxx.zzz
サブ・ドメイン名D.co.jp	xxx.yyy.xxx.zzz

AEGIS EARLY WARNING SYSTEM

サブドメイン自動検出

【WAN/インターネット側】

【エンドユーザー様企業サイト】

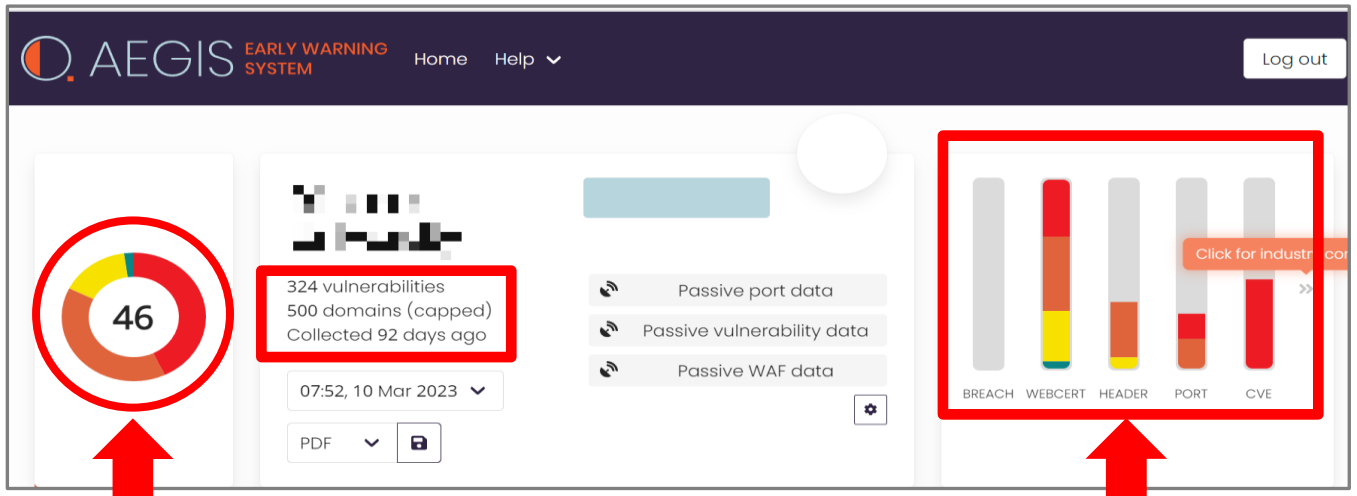
脆弱性診断に必要な情報は、
「メインドメイン名」だけでOK！

AEGIS-EW特徴：見やすいダッシュボード

未来研究所 Future Research Inc.

■AIGES-EW(イージス EW)におけるダッシュボード

「AIGES-EW(イージス EW)」では該当ドメインの診断結果を、総合評価点で示します。
なお、納品方法はについては**「ダッシュボードでの診断結果表示」**となります。
（ダッシュボード内にレポート出力機能もあります）。



総合評価（**46点/100満点**）
脆弱性危険度分類：
「非常に重要度の高い脆弱性リスク」あり

本来、あってはならないはずの
「深刻度１（図内赤グラフ）の脆弱性」
がサブドメイン内に存在

視覚的なサーバ安全度スコアリング

ドメインの脆弱性リスクをグラフ化！
サーバ安全度スコアリングを
（100点満点中 XX点）で表示します。

POINT!
専門知識は不要。
色分けで理解できる！

AEGIS-EW は、サーバ脆弱性診断に詳しくないエンドユーザ様でも見やすく、わかり易いものとなっています。
スコアリングは一般的な脆弱性診断に用いられるリソース群だけでなく、開発元である Titanium-Defence Ltd. チームが保有する 30 年以上のサイバーセキュリティ・コンサルティングで得たチェック項目によって評価されます。

サイバーセキュリティ環境のレベル

総合点が円グラフによって
分かりやすく示されます。

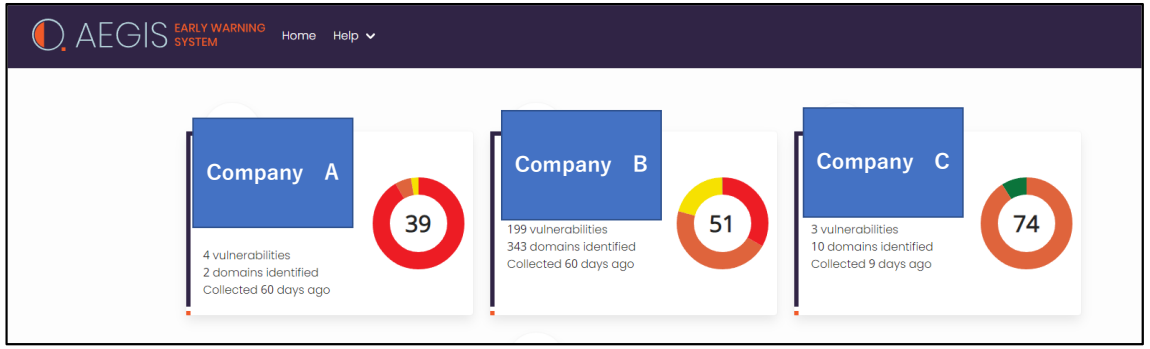
100 ～ 80 = 最小限のリスクで非常に安全度が高い
79 ～ 60 = 比較的安全度が高い … 部分的に「脆弱性リスク」あり
59 ～ 40 = 脆弱性リスクがある … 「重要度の高い脆弱性リスク」あり
39 ～ 20 = 安全度が低い … 「非常に重要度の高い脆弱性リスク」あり
19 ～ 0 = 深刻な状態にある … 「極端に危険な脆弱性リスク」あり

AEGIS-EW特徴：視覚的スコアリング

未来研究所
Future Research Inc.

■視覚的なサーバ安全度スコアリング

AEGIS-EW(イージス・EW)では、ドメインの脆弱性リスクをグラフ化した
「サーバ安全度スコアリング（100点満点中／xxx点）」で表示されます。
これにより、サーバ脆弱性診断に詳しくないエンドユーザ様でも見やすくわかりやすいものとなっています。
なお、スコアリングは一般的な脆弱性診断に用いられる下記リソース群だけでなく、開発元であるTitanium Defence Ltd.チームが保有する30年以上のサイバーセキュリティ・コンサルティングで得たチェック項目によって評価されます。



39, 51, 74 は、サイバーセキュリティ・ヘルスチェック値であり、技術的に診た総合的な脆弱性強度を示しています。値が低いほど、脆弱性が弱く至急の対応が必要です

●脆弱性リスクチェックの結果は100点満点でスコア化され、値が小さいほど危険度が高くなります。

＊100 – 80 = 最小限のリスクで非常に安全度が高いサイバーセキュリティ環境
＊ 79 – 60 = 比較的安全度が高いサイバーセキュリティ環境　…部分的に「脆弱性リスク」が存在
＊ 59 – 40 = 脆弱性リスクがあるサイバーセキュリティ環境　…「重要度の高い脆弱性リスク」が存在
＊ 39 – 20 = 安全度が低いサイバーセキュリティ環境　…「非常に重要度の高い脆弱性リスク」が存在
＊ 19 – 0 = 深刻な状態にあるサイバーセキュリティ環境　…「極端に危険な脆弱性リスク」が存在

AEGIS-EW特徴：システム堅牢性の確認

■ペネトレーションテスト・Active Scan実施の必要性

「AIGES-EW」におけるアクティブスキャン(Active Scan：**ペネトレーションテスト**)は次のとおりです。

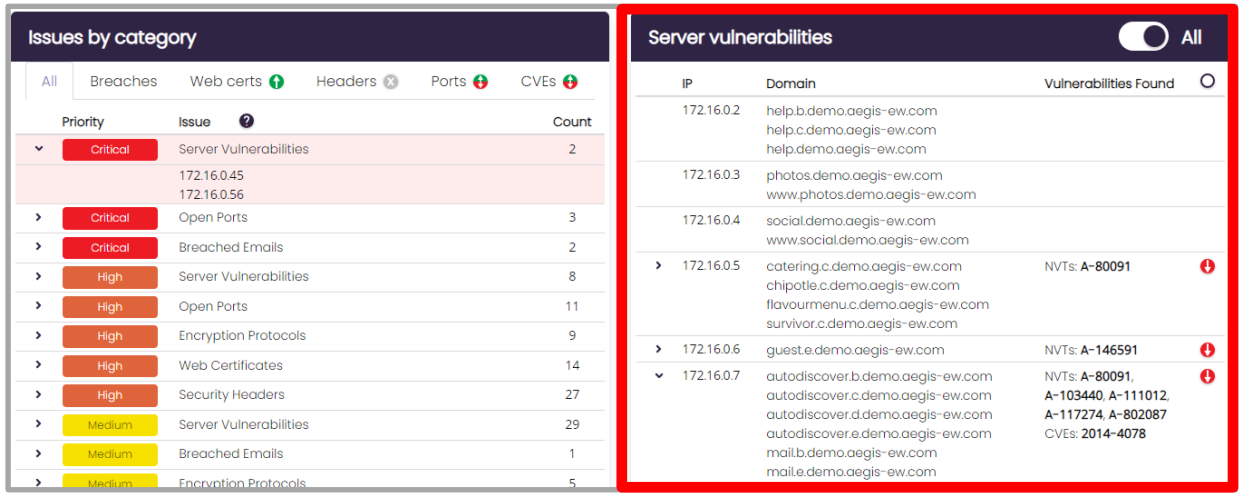
目的：

攻撃者が行うサイバー攻撃と同様の手法を用いて、脆弱性レベルを診断します。

スキャン技術：

調査対象サーバに対して、「実際の脆弱性に基づく攻撃パターン」を仕掛けて、侵入を試みます。
AEGIS-EWでは、45,000パターン以上の攻撃を実施することが可能です。

【Active Scanの一例】



Active Scanの実施結果では、より詳細な脆弱性の情報を得ることができ、システム堅牢性向上に役立てることが可能です。

AEGIS-EW特徴：低価格な導入コスト

未来研究所 Future Research Inc.

■明瞭かつ低価格な導入コスト

AEGIS-EW(イージス・EW)の利用料金は、ドメインやサブドメイン名に含まれるサーバ数に依存します。
このため、明瞭で誰にでも分かりやすい料金体系となっています。
価格は全て「オープンプライス」です。一例として下記のような価格を設定した場合でも、利益を出すことが可能です。

都度ごとの診断（ワンショット価格）

【サイバー健康診断費用】

※１回の実施費用

商材名	プロフェッショナル	エクスパート
チェック名	パッシュブ・スキャン脆弱性チェック	ペンテスト・脆弱性チェック
スキャン方法	Passive	ACTVE
ドメイン数（サブドメイン数含む）	推奨価格（税抜）	推奨価格（税抜）
1 to 9	¥85,000	¥150,000
10 to 24	¥95,000	¥175,000
25 to 49	¥104,400	¥200,000
50 to 99	¥111,000	¥225,000
100 to 199	¥118,400	¥250,000
200 to 499	¥132,000	¥275,000
500 to 999	¥146,000	¥300,000
1000 - 2000	¥160,000	¥325,000

定期ごとの診断（リピート価格）

【定期サイバー健康診断（１年・３年）費用】

※マンスリー（１回/月）の脆弱性チェックサービス・１年・３年コース
※ウィークリー（１回/週）の脆弱性チェックサービス・１年・３年コース
※ディリー（１回/日）の脆弱性チェックサービス・１年・３年コース

商材名	プロフェッショナル	プロフェッショナル	プロフェッショナル	エクスパート	エクスパート	エクスパート	エクスパート	エクスパート	エクスパート
チェック名	パッシュブ・スキャン脆弱性チェック	パッシュブ・スキャン脆弱性チェック	パッシュブ・スキャン脆弱性チェック	ペンテスト・脆弱性チェック	ペンテスト・脆弱性チェック	ペンテスト・脆弱性チェック	ペンテスト・脆弱性チェック	ペンテスト・脆弱性チェック	ペンテスト・脆弱性チェック
スキャン方法	Passive	Passive	Passive	Active	Active	Active	Active	Active	Active
スキャン周期	マンスリー	ウィークリー	ディリー	マンスリー	ウィークリー	ディリー	マンスリー	ウィークリー	ディリー
サービス適用期間	1 Year	1 Year	1 Year	1 Year	1 Year	1 Year	3 Year	3 Year	3 Year
ドメイン数（サブドメイン数含む）	推奨価格（税抜）	推奨価格（税抜）	推奨価格（税抜）	推奨価格（税抜）	推奨価格（税抜）	推奨価格（税抜）	推奨価格（税抜）	推奨価格（税抜）	推奨価格（税抜）
1 to 9	¥235,000	¥290,000	¥400,000	¥555,000	¥665,000	¥800,000	¥1,310,000	¥1,640,000	¥2,050,000
10 to 24	¥260,000	¥315,000	¥425,000	¥615,000	¥775,000	¥880,000	¥1,475,000	¥1,800,000	¥2,205,000
25 to 49	¥290,000	¥345,000	¥450,000	¥670,000	¥880,000	¥1,015,000	¥1,640,000	¥1,960,000	¥2,370,000
50 to 99	¥315,000	¥370,000	¥480,000	¥720,000	¥990,000	¥1,125,000	¥1,800,000	¥2,130,000	¥2,530,000
100 to 199	¥340,000	¥400,000	¥510,000	¥775,000	¥1,100,000	¥1,235,000	¥1,960,000	¥2,285,000	¥2,700,000
200 to 499	¥398,000	¥450,000	¥560,000	¥830,000	¥1,200,000	¥1,340,000	¥2,125,000	¥2,450,000	¥2,850,000
500 to 999	¥450,000	¥500,000	¥620,000	¥880,000	¥1,320,000	¥1,450,000	¥2,285,000	¥2,610,000	¥3,020,000
1000 - 2000	¥500,000	¥560,000	¥680,000	¥940,000	¥1,420,000	¥1,555,000	¥2,450,000	¥2,770,000	¥3,180,000

※最新の推奨販売価格は、こちらから

AEGIS-EW 診断結果・有料セミナー	商品名	商品番号	推奨販売価格（税抜　¥）
診断結果概要説明S（２時間想定編）	AEGIS-EW診断結果説明2	AGS-SMR-2	150,000
診断結果概要説明L（４時間想定編）	AEGIS-EW診断結果説明4	AGS-SMR-4	250,000

ご購入およびオプションサービスについてのご案内

AEGIS-EW 実際の活用事例

■AEGIS-EWの実際の活用事例

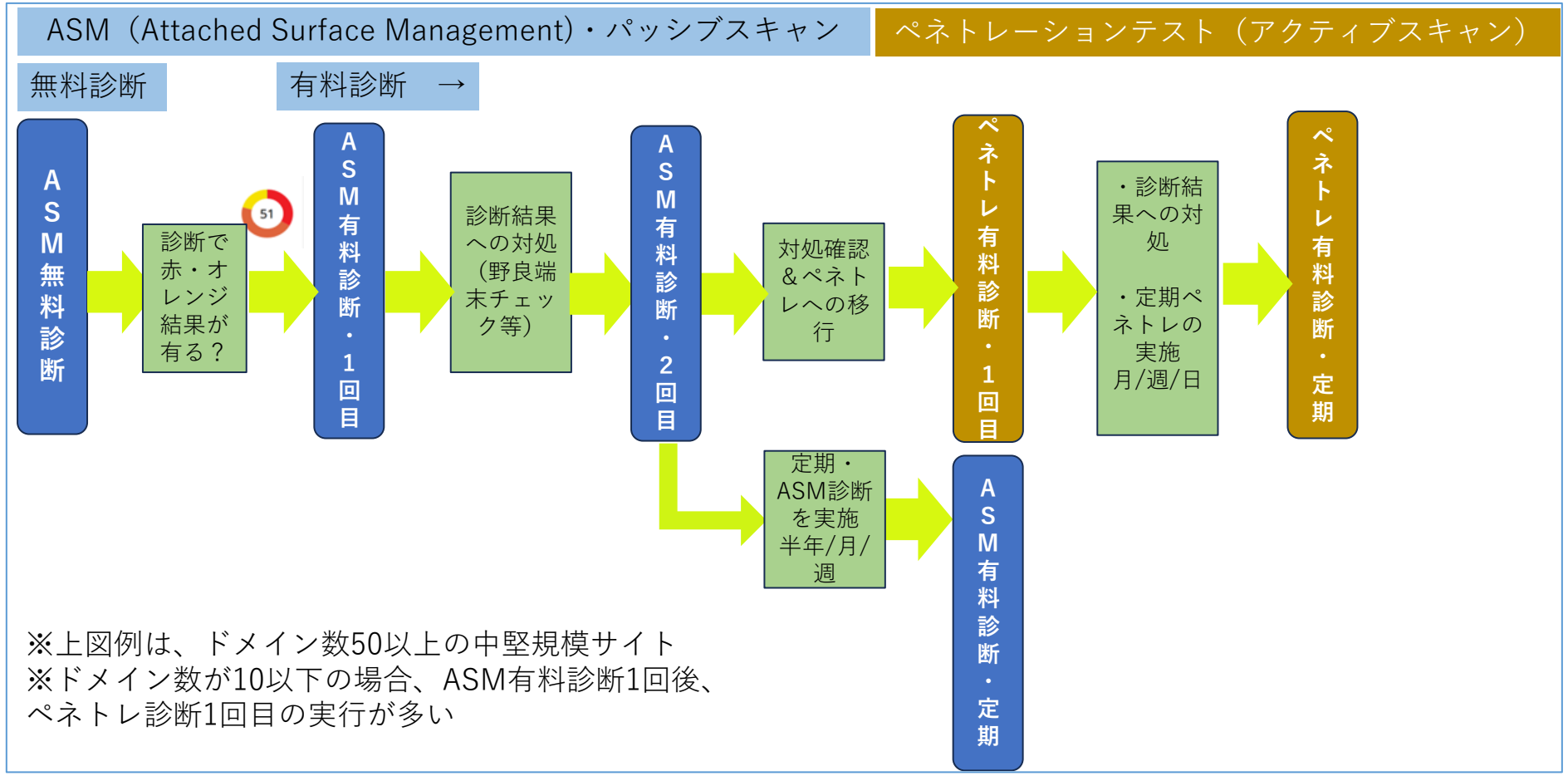
ASM（パッシブスキャン）の無料診断診断から、ペネトレーション（アクティブスキャン）の定期活用まで、どの様な工程で、お客様の対応が実施されていくのかを示します。下図は、ドメイン数が50以上あり深刻度の高い脆弱性が観られたお客様の例です。

ドメイン数が少なく深刻度も低いケースは、1回のASM有料診断後、ペネトレの実施が多く観られます

【費用感例】

※ドメイン50以上
2回のASM診断
＋
1回のペネトレ診断
＋
ASM/ペネトレの定期実施

※ドメイン10以下
１回のASM診断
＋
1回のペネトレ診断
＋
ASM/ペネトレの定期実施



AEGIS-EW：購入・サポートの流れ

未来研究所 Future Research Inc.

①脆弱性診断対象ドメインをお教えください

脆弱性診断を実施したいドメインを弊社/販売店までお伝えください。

②簡易・無料診断結果のご報告

受付から、１週間以内に脆弱性リスクをスコアリングした「簡易・無料脆弱性診断スナップショットビュー」をご提供します。
必要であれば、検出ドメイン総数（サブドメインも含みます）に基づいた見積書をご提出いたします　※1

③発注書の処理・ダッシュボードで使用するメールアドレスの御通知

オーダー時には、販社様ルールの下、発注を実施していただくか、弊社ECサイト（近日オープン予定）でのご発注でも構いません。
ご指定メールアドレスにて、脆弱性診断結果をお客様にて確認して頂くためのAEGIES-EWアカウントを制作していただきます　※2

④AEGIS-EW診断結果アップの御通知

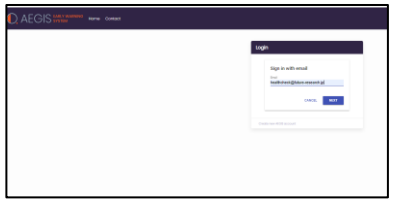
診断結果の終了をお伝え致します。これによりお客様ご自身で「AEGIS-EW(イージス・EW)」の脆弱性診断結果の仔細情報を、観て頂く事ができ、対応策を考えていただけます

⑤AEGIS-EWサイト診断結果・有料セミナーの御検討

御客様は、脆弱性診断結果の内容を、弊社認定講師による個別説明会（Web会議）を受ける事ができます。受講者の制限はございません。
基本的に、脆弱性診断の深刻度の深い事象について、発生要因の原因記載ページの探し方と、発生原因要素の説明をさせていただきます。　※3

凡例：
- お客様アクション
- 弊社アクション

例：簡易・無料脆弱性診断スナップショットビュー
※フォーマットの方は、逐次変更されていきます。
※深刻度１（赤）、深刻度２（オレンジ）の事象がある場合、早急の対処をおすすめします。



https://aegis-ew.com/login/

発注する際に、お客様が「AIGES-EW」公式サイトで登録したメールアドレスをお伝えください。

※1　DNS応答のあった全ドメイン／サブドメインから、エンドユーザ様の稼働中ドメイン合計数を御社にご報告します。（ドメイン数は「スナップショットビュー」内の合計ドメイン数となり、価格表から御見積金額が決定されます）お客様は、販社様より御見積を取得していただくか、弊社ECサイトサイトからの発注となります
※2　本アカウントは、お客様自身で、自社の診断結果を何時でも確認できるAEGIS-EWのアカウントとなります。Eメールアドレスとお客様にて設定していただくパスワードで、アカウントを新設していただけます
※3　本セミナーは、あくまでも一般論となります。お客様システム内部の環境には言及いたしません。お客様システムの改修依頼は、別途、個別相談となりますので、ご連絡の方、宜しくお願い致します

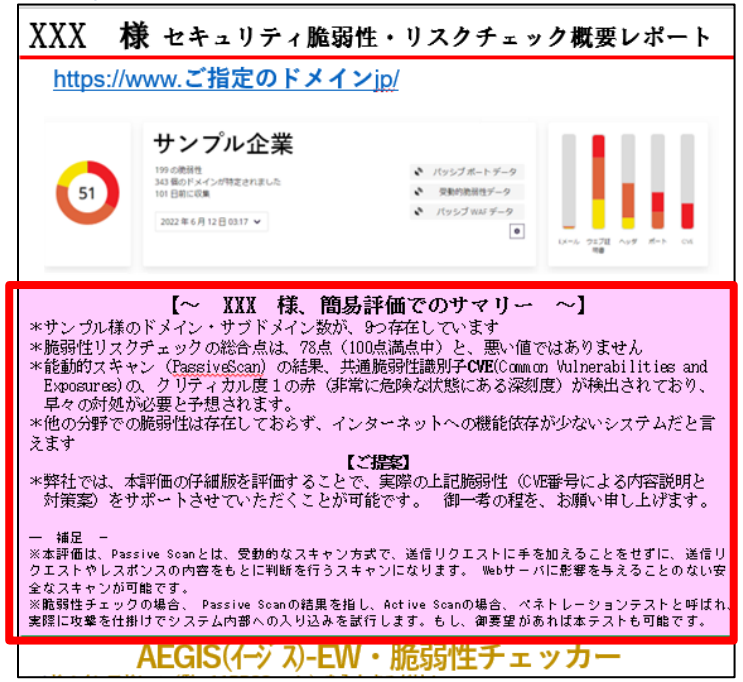
限定特別キャンペーン(サイバー健康診断）のご案内

未来研究所 Future Research Inc.

■AEGIS-EW(イージス・EW)日本初上陸記念キャンペーン

(株)未来研究所では、「AEGIS-EW(イージス・EW)」のASM簡易脆弱性診断を、無料にて実施させていただいてます。

「サーバ安全度スコアリング」と
簡易診断結果サマリーをお届けします。


XXX　様 セキュリティ脆弱性・リスクチェック概要レポート

https://www.ご指定のドメインjp/

サンプル企業

51

【～　XXX　様、簡易評価でのサマリー　～】

＊サンプル様のドメイン・サブドメイン数が、9つ存在しています
＊脆弱性リスクチェックの総合点は、78点（100点満点中）と、悪い値ではありません
＊能動的スキャン（PassiveScan）の結果、共通脆弱性識別子CVE(Common Vulnerabilities and Exposures)の、クリティカル度１の赤（非常に危険な状態にある深刻度）が検出されており、早々の対処が必要と予想されます。
＊他の分野での脆弱性は存在しておらず、インターネットへの機能依存が少ないシステムだと言えます

【ご提案】

＊弊社では、本評価の仔細版を評価することで、実際の上記脆弱性（CVE番号による内容説明と対策案）をサポートさせていただくことが可能です。　御一考の程を、お願い申し上げます。

－　補足　－

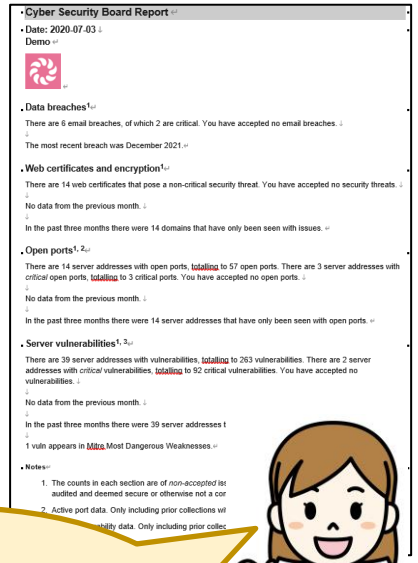
※本評価は、Passive Scanとは、受動的なスキャン方式で、送信リクエストに手を加えることをせずに、送信リクエストやレスポンスの内容をもとに判断を行うスキャンになります。　Webサーバに影響を与えることのない安全なスキャンが可能です。
※脆弱性チェックの場合、 Passive Scanの結果を指し、Active Scanの場合、ペネトレーションテストと呼ばれ、実際に攻撃を仕掛けでシステム内部への入り込みを試行します。もし、御要望があれば本テストも可能です。

AEGIS(イージス)-EW・脆弱性チェッカー

＋

【自動生成・評価レポート】

※サマリー版


Cyber Security Board Report

Date: 2020-07-03

Demo

Data breaches[1]

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]

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, totalling to 57 open ports. There are 3 server addresses with critical open ports, totalling 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, 3]

There are 39 server addresses with vulnerabilities, totalling to 263 vulnerabilities. There are 2 server addresses with critical vulnerabilities, totalling to 92 critical vulnerabilities. You have accepted no vulnerabilities.

No data from the previous month.

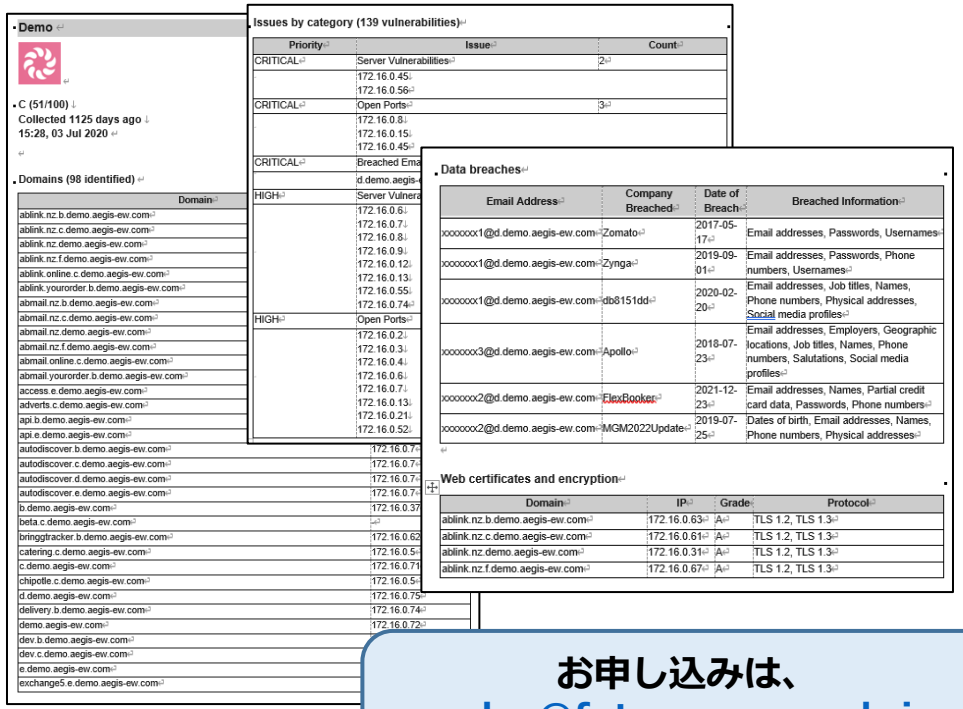
In the past three months there were 39 server addresses t

1 vuln appears in Mitre Most Dangerous Weaknesses.

Notes

1. The counts in each section are of non-accepted iss audited and deemed secure or otherwise not a cor
2. Active port data. Only including prior collections wi

※仔細版：CVSS、CVE　等、過去の漏洩情報も記載


Demo

C (51/100)

Collected 1125 days ago

15:28, 03 Jul 2020

Domains (98 identified)

Domain
ablink.nz.b.demo.aegis-ew.com
ablink.nz.c.demo.aegis-ew.com
ablink.nz.demo.aegis-ew.com
ablink.nz.f.demo.aegis-ew.com
ablink.online.c.demo.aegis-ew.com
ablink.yourorder.b.demo.aegis-ew.com
abmail.nz.b.demo.aegis-ew.com
abmail.nz.c.demo.aegis-ew.com
abmail.nz.demo.aegis-ew.com
abmail.nz.f.demo.aegis-ew.com
abmail.online.c.demo.aegis-ew.com
abmail.yourorder.b.demo.aegis-ew.com
access.e.demo.aegis-ew.com
adverts.c.demo.aegis-ew.com
api.b.demo.aegis-ew.com
api.e.demo.aegis-ew.com
autodiscover.b.demo.aegis-ew.com
autodiscover.c.demo.aegis-ew.com
autodiscover.d.demo.aegis-ew.com
autodiscover.e.demo.aegis-ew.com
b.demo.aegis-ew.com
beta.c.demo.aegis-ew.com
bringgtracker.b.demo.aegis-ew.com
catering.c.demo.aegis-ew.com
c.demo.aegis-ew.com
chipotle.c.demo.aegis-ew.com
d.demo.aegis-ew.com
delivery.b.demo.aegis-ew.com
demo.aegis-ew.com
dev.b.demo.aegis-ew.com
dev.c.demo.aegis-ew.com
e.demo.aegis-ew.com
exchange5.e.demo.aegis-ew.com

Issues by category (139 vulnerabilities)

Priority	Issue	Count
CRITICAL	Server Vulnerabilities	2
	172.16.0.45	
	172.16.0.56	
CRITICAL	Open Ports	3
	172.16.0.8	
	172.16.0.15	
	172.16.0.45	
CRITICAL	Breached Ema	
	d.demo.aegis-	
HIGH	Server Vulnera	
	172.16.0.6	
	172.16.0.7	
	172.16.0.8	
	172.16.0.9	
	172.16.0.12	
	172.16.0.13	
	172.16.0.55	
	172.16.0.74	
HIGH	Open Ports	
	172.16.0.2	
	172.16.0.3	
	172.16.0.4	
	172.16.0.6	
	172.16.0.7	
	172.16.0.13	
	172.16.0.21	
	172.16.0.52	
	172.16.0.7	
	172.16.0.7	
	172.16.0.7	
	172.16.0.7	
	172.16.0.37	
	172.16.0.62	
	172.16.0.5	
	172.16.0.71	
	172.16.0.5	
	172.16.0.75	
	172.16.0.74	
	172.16.0.72	

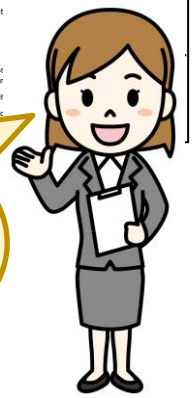
Data breaches

Email Address	Company Breached	Date of Breach	Breached Information
xxxxxxx1@d.demo.aegis-ew.com	Zomato	2017-05-17	Email addresses, Passwords, Usernames
xxxxxxx1@d.demo.aegis-ew.com	Zynga	2019-09-01	Email addresses, Passwords, Phone numbers, Usernames
xxxxxxx1@d.demo.aegis-ew.com	db8151dd	2020-02-20	Email addresses, Job titles, Names, Phone numbers, Physical addresses, Social media profiles
xxxxxxx3@d.demo.aegis-ew.com	Apollo	2018-07-23	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles
xxxxxxx2@d.demo.aegis-ew.com	FlexBooker	2021-12-23	Email addresses, Names, Partial credit card data, Passwords, Phone numbers
xxxxxxx2@d.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。
おまちしております。



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

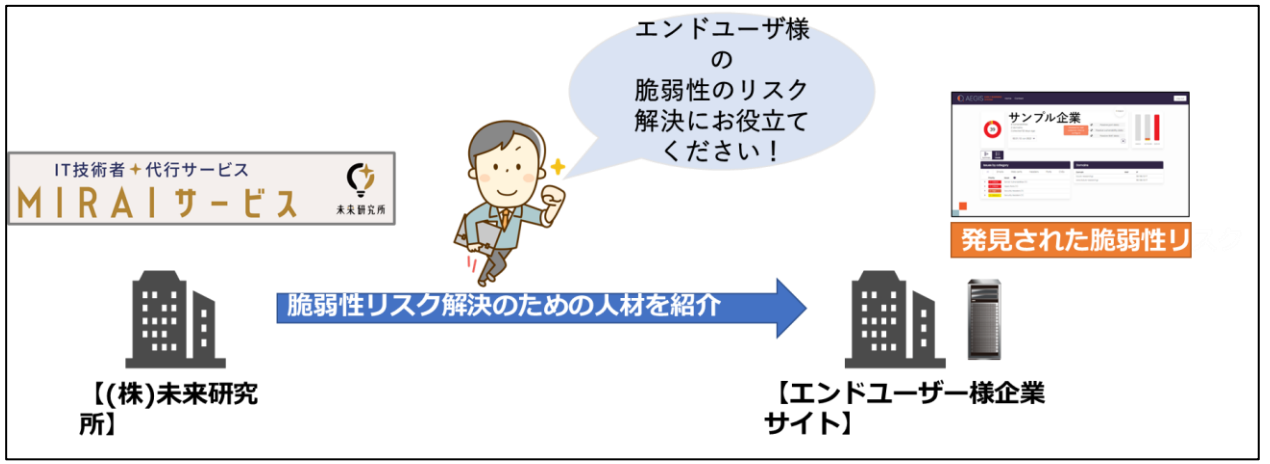
脆弱性診断の付加サービス・ご案内

■ AEGIS-EW診断結果・有料セミナー

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、および実際の結果に基づいた対策でのセミナーを実施させていただきます。

ご要望があれば、対策エンジニアの支援も可能です。

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。



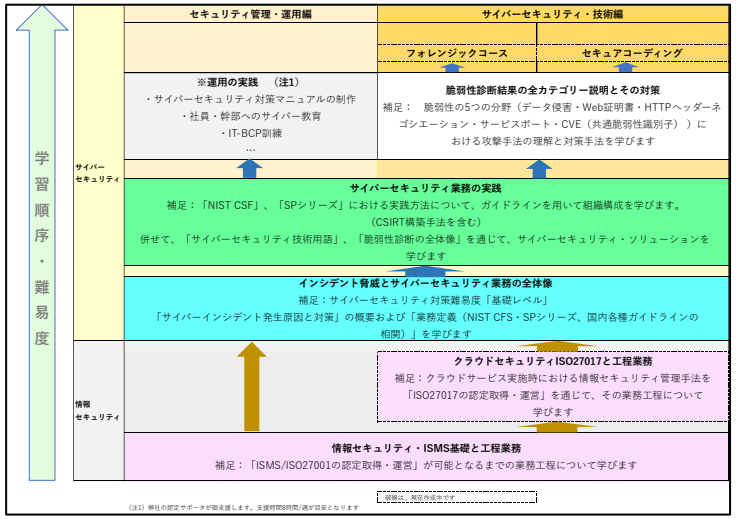
■ 未来の学舎・セキュリティ編の研修コース

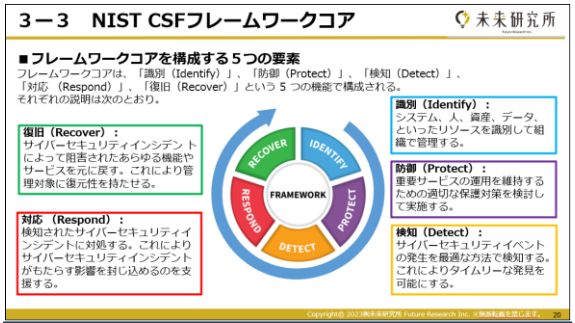
対象者：

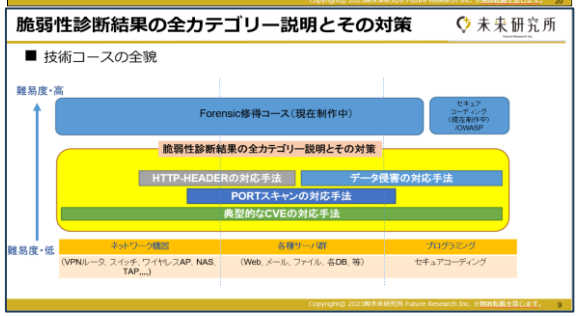
①セキュリティ業務を実行しなくてはならないが、何処から始めて良いかが、分からない

②公共組織でIT分野の受発注を担当するが、サイバーセキュリティ商材の全般、およびポイントが良くわからない

③脆弱性診断の結果に基づいて、対処を行う必要がある担当システム者







Thanks

ASMにおける脆弱性検出手法

未来研究所
Future Research Inc.

■ASMにおける脆弱性検出手法一覧

まず、「脆弱性」とは情報セキュリティ・サイバーセキュリティ用語で、
「IT機器全般のコンピュータに存在する情報セキュリティ上の欠陥」を指します。
別名「セキュリティホール」とも呼ばれます。
「AIGES-EW(イージス EW)」では、次の２つの手法を用いて調査対象サーバの洗い出しと脆弱性診断を行います。なお、このツールで行われる診断方法は、次の大きく２つに分類されます。

①パッシブスキャン(Passive Scan)
パッシブスキャンでは、ドメイン情報から放置サーバ（野良サーバ）を検出して診断します。

②アクティブスキャン(Active Scan)
アクティブスキャンでは、調査対象診端末に対して、ハッカーと同様の攻撃手法を用いる診断方法（ペネトレーションテスト）を行って診断します。

広義の定義	脆弱性診断	脆弱性診断
狭義の定義	ASM・脆弱性診断	ペネトレーション・テスト
スキャン方法	パッシブスキャン (Passive Scan)	アクティブスキャン (Active Scan)
現存する商材名 (Web/カタログより推測)	AEGIS-EW(PS) Security Scorecard BitSight	AEGIS-EW(AS) OpenVAS Nessus

※弊社では、サイバーセキュリティ・マネージメント評価は、IPA等の多くの機関から各種ガイドラインが既にリリースされており、評価ツールも多数あるため、こちらを使用した方が、日本語での対応もあり、有効であるとコンサルティングしています