未来研究所
Future Research Inc.

ASM vs 脆弱性診断
サイバー攻撃事例と脆弱性診断概要

2025年8月29日
株式会社　未来研究所

2024-2025年、激震が走ったサイバー攻撃例

未来研究所
Future Research Inc.

・具体的なサイバー公的事例集

（１）保険見直し本舗からの501万人の個人情報が漏洩
(NHK2025年4月30日、日本経済新聞2025年5月1日掲載)

（２）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（9万件漏洩）、全国漁業協同組合連合会（1.2万件漏洩）、
スローヴィレッジ（3.2万件漏洩）、なども被害。（4年前からの流出）

（３）管理不足のIoT機器がDDoS攻撃の温床となる事例
IoTボットネット対策としてのJC-STARの必要性

（４）JAXAに対する中国からのサーバー攻撃

保険再販業者からの510万件個人情報・漏洩

未来研究所 Future Research Inc.

- **保険見直し本舗からの501万人の個人情報が漏洩**

(NHK2025年4月30日、日本経済新聞2025年5月1日掲載)

- 2月中旬にランサム感染を認知し、外部調査会社との対策・漏洩データの分析が実施されました（仔細報告書は、保険見直し本舗のHP上での開示無し　→　ランサムの感染要因は、不明）
- 日本の主要生命保険会社、損害保険会社の大手販売店
- 課題

① **主要保険会社は、特定社会基盤事業者である。**この場合、経済安全保障推進法（令和４年法律第43号）の基幹インフラ役務の安定的な提供の確保に関する制度に抵触する可能性がある。
販売階層の間に入る販売店の責務が不明瞭になっている現状がある

②各種ガイドラインは、存在するが、システム・技術的な観点での記載は金融庁「金融機関等コンピュータシステムの安全対策基準」ぐらい

- 「OSやソフトウェア等の脆弱性情報を適時に把握し、脆弱性に対しては適切に対策を講じること。
システムやアプリケーションについて、必要に応じて**脆弱性診断やセキュリティテスト等を実施することが望ましい。**」
- 海外のサイバー先進国（IK、US、EU主要国）では、公共機関と銀行口座を有するため、定期是弱性診断結果の提出が義務付けられている

ECサービス提供者が被害に遭った例

・**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（9万件漏洩）、全国漁業協同組合連合会（1.2万件漏洩）、
スローヴィレッジ（3.2万件漏洩）、なども被害。（4年前からの流出）
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が盗まれました。
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！

原因：ECサイトのシステムに存在した脆弱性
（仔細感染要因は未公表。定期的な、プラットホーム・Webアプリ脆弱性診断を実施していれば、回避可能だった可能性が高い）

※留意点：
流出個人情報に、EU諸国の住人の存在有無が話題になっている。GDPR規制配下の国々では、
流出団体・企業に対し、最悪のケース３２億円相当の罰金が請求される。
悪意ある人の個人情報が漏洩した場合、「１億円支払ったら、GDPR機関への通報をしない」という
様な、強請も発生している

GDPR（EU一般データ保護規則）

・「GDPR（EU一般データ保護規則）」について

GDPRとは、欧州連合（EU）の一般データ保護規則（General Data Protection Regulation）のことです。2018年5月25日に施行され、EU域内における個人データの保護とプライバシー権の確保を目的としています。この規則は、EU域内の個人データの取り扱いだけでなく、EU域外の企業がEUの居住者の個人データを扱う場合にも適用されます。

このため、サイバー攻撃による漏洩した顧客個人情報の中にEU在住者情報が含まれていると、日本国内のみ営業している企業であっても、データ主体が居住する国 の DPA によって、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。

DDoS攻撃：国内のIoT機器の感染端末数は？

未来研究所
Future Research Inc.

- **IoT機器のサイバー攻撃への感染率**
  - 日本中の感染IoT機器群が、年末・年始の金融系DDoS攻撃の犯人？
  - 2024/NICTER観測レポートより
    - 図５：IoT端末がハッカーに乗っ取られる端末数は？　**2,632台/日**
      年換算だと、**96万台/年**。昨年からの残台数を足すと、優に**100万台は超える**
    - 図１０：主にIoT機器からのDRDoS（DDOSの一種）での毎日の日本への攻撃件数：
      467件/日（2023年・2.4万件/日）

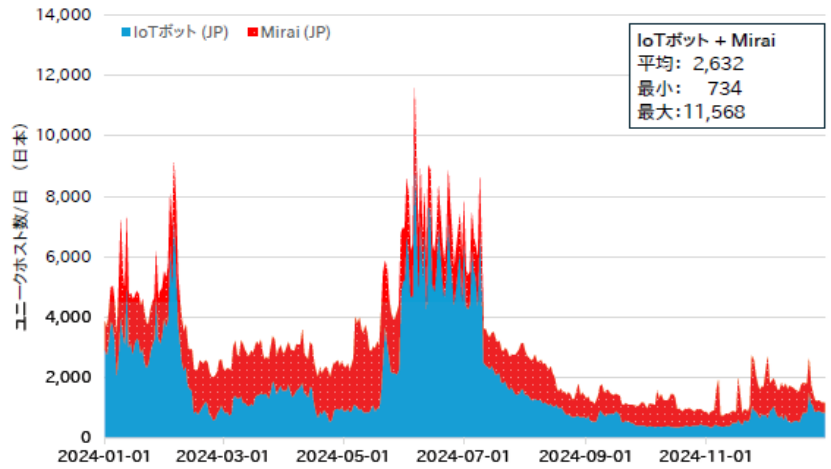


図5: 日本国内における IoT ボット感染ホスト数の推移（積み上げグラフ）

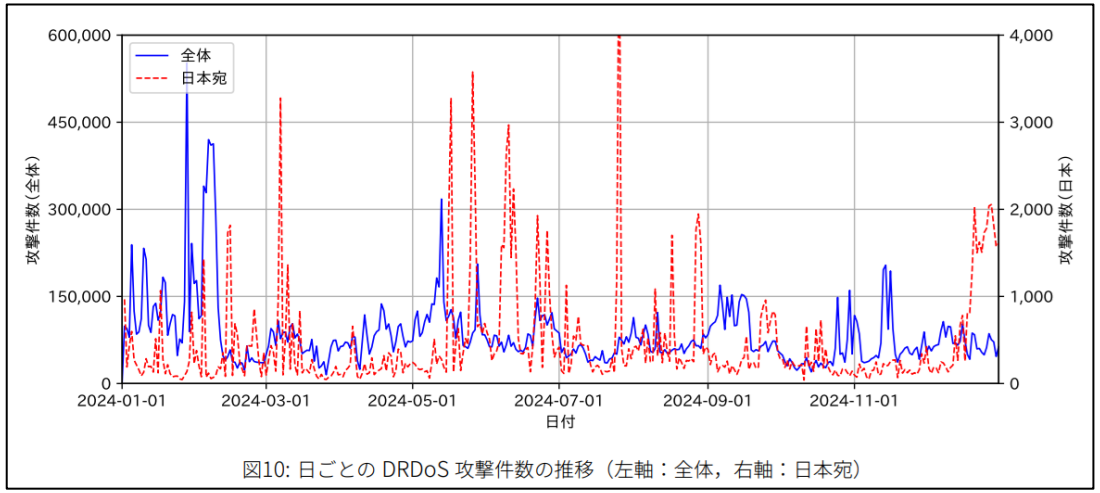


図10: 日ごとの DRDoS 攻撃件数の推移（左軸：全体，右軸：日本宛）

【日本政府】
流石にこの感染端末数は問題！
抜本的な施策が求められた

JC-STAR

感染したIoT機器からのDDOS攻撃

未来研究所
Future Research Inc.

- **年末年始の日本の風物詩となりつつあるDDoS攻撃**

  年末年始の銀行・JR東日本の予約システムのダウン(2024年)

  - １２月末の支払いが全てSTOPし、謝罪電話で忙しい（弊社代表だけ？）
- **DDoS攻撃に対する技術的に完全な回避策はありません**（現時点）

  緩和策はある

  - CDNを用いた高可用性のネットワーク構成で緩和する
  - 中小規模の企業・団体では、予算に制約がある中でもWAFの導入で少し緩和する
- **抜本的対策は、DDoSに利用される感染IoT機器（ボット）を根絶すること**

  総務省：NOTICE、経済産業省・IPA：JC-STAR

  重要社会基盤事業者（重要インフラ１５分野）に求められること

  - ゼロディ攻撃に備えるため、**プラットフォーム脆弱性診断を定期的に実施する**
  - 診断対象：ネットワークに繋がる全機器（社内・社外を問わず、サーバ・ルータ・スイッチ・PC・ディスプレイ・IPカメラ・無線AP・複合コピー機・NAS等）

    クラウドサービスにも、プラットホーム脆弱性診断およびＷｅｂアプリ脆弱性診断は、必須です。

中国「ミラーフェイス」から狙われ続ける、JAXA

- 2023年6月～2024年秋迄に4回攻撃され、侵入を許している。
  - 情報ルート
    - JAXAプレス2024年（令和6年）7月5日、朝日新聞デジタル（2024年7月5日）、日経新聞（20251/21)
  - 感染ルート（JAXA公表）
    - 1回・2回目　VPNルータへのゼロディ攻撃およびCVE公表当日
    - 3回・4回目　 VPNルータへのCVE公表前攻撃（マイナスディ攻撃？）
  - 被害
    - MS365上でJAXAが管理していた情報の一部（外部機関と業務を共同で実施するにあたっての情報及び個人情報）が漏洩
- 重要インフラ事業者での対策として
  - ゼロディ攻撃を迂回できる、Daily/Weekly/Monthlyの定期的脆弱性診断は、必須
  - 納品IoT機器の品質保証（SBOM）、IoT機器メーカからの情報漏洩防止強化
  - CVE等、公表作業情報の漏洩防止強化

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】

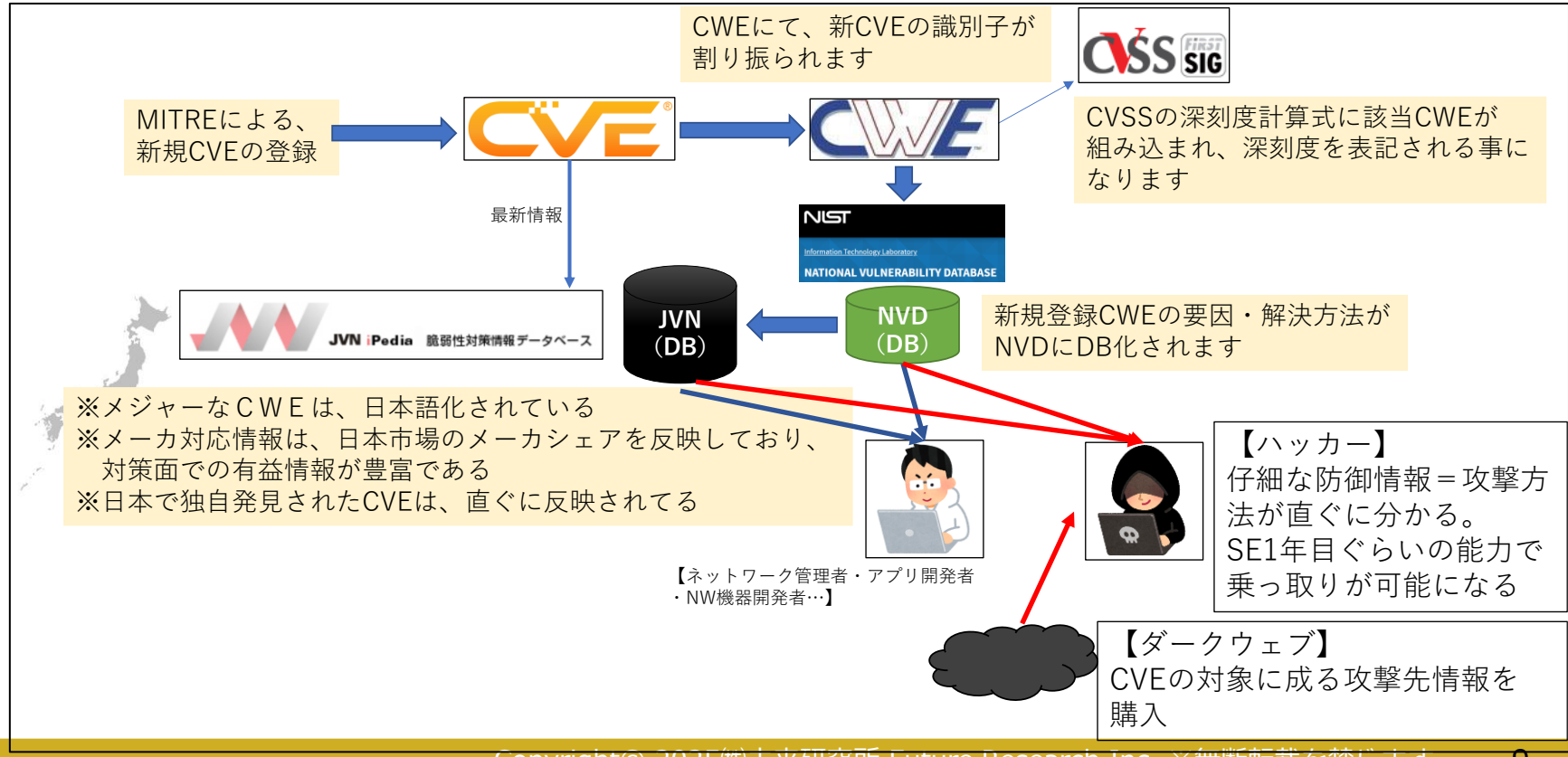
新たなサイバー攻撃が登録されるとダークウェブ上では、

・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）**



脆弱性診断の必要性

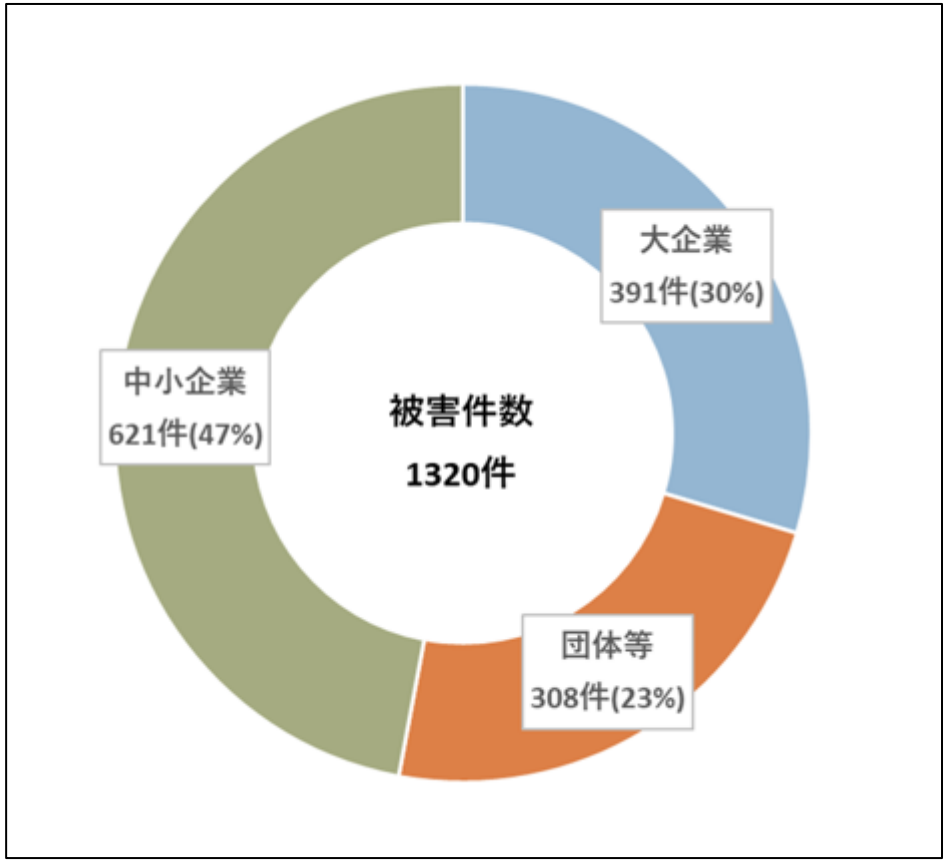
国内Webサービスの約7割は、
① 資産棚卸（ASM）未実施
② 年1回以上の外部脆弱性診断未実施
という調査結果があります。

その状態では OWASP Top 10 相当の脆弱性が残存しやすく、
新人SEレベルの技術でも認証回避や権限昇格が成立するケース
が実際に報告されています。

サイバー攻撃の危険性は、年々高まっています！

未来研究所 Future Research Inc.

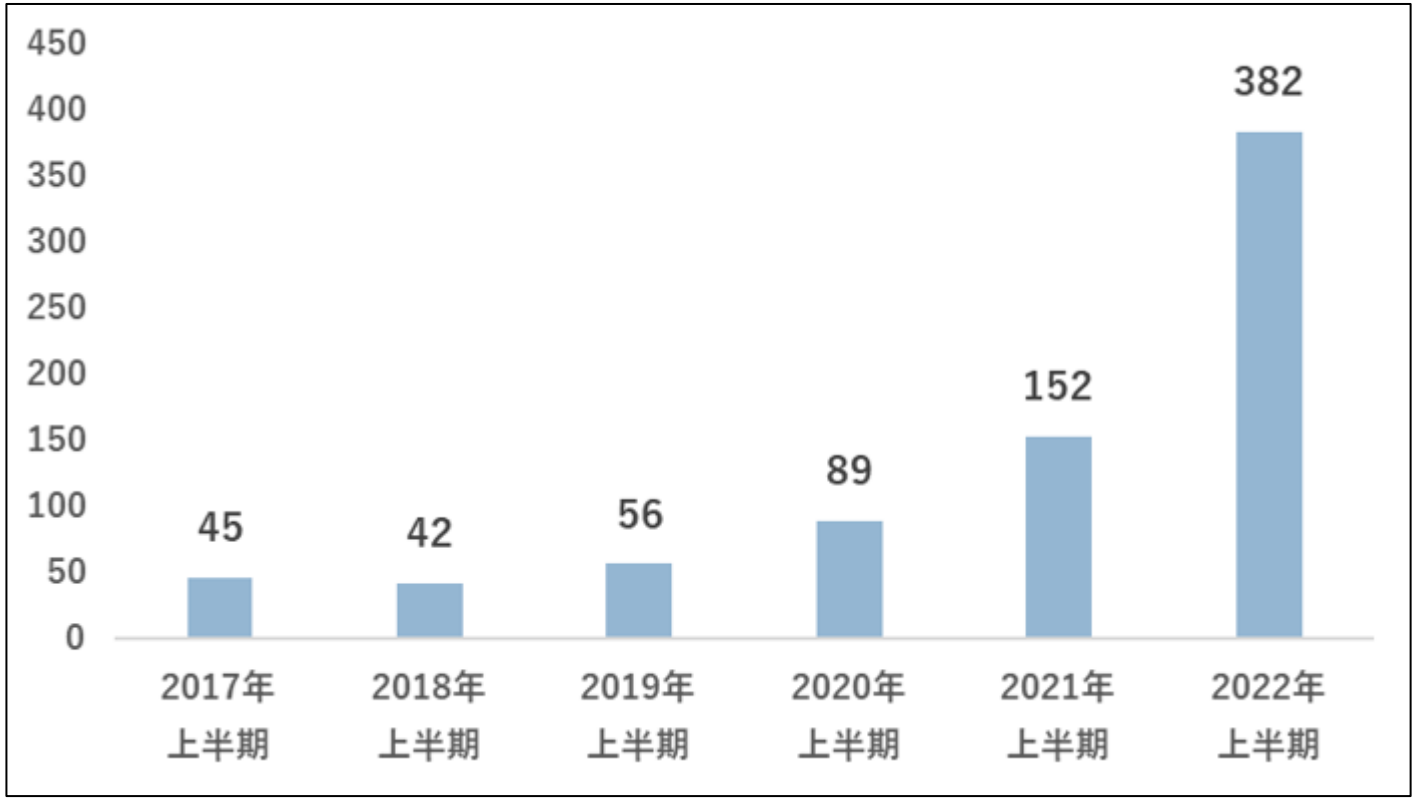
企業規模は関係ありません！



※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、
実は、中小企業の被害件数の方が多いです

JNSA：インシデント損害額調査レポート2024年2月

年々件数が増えています！

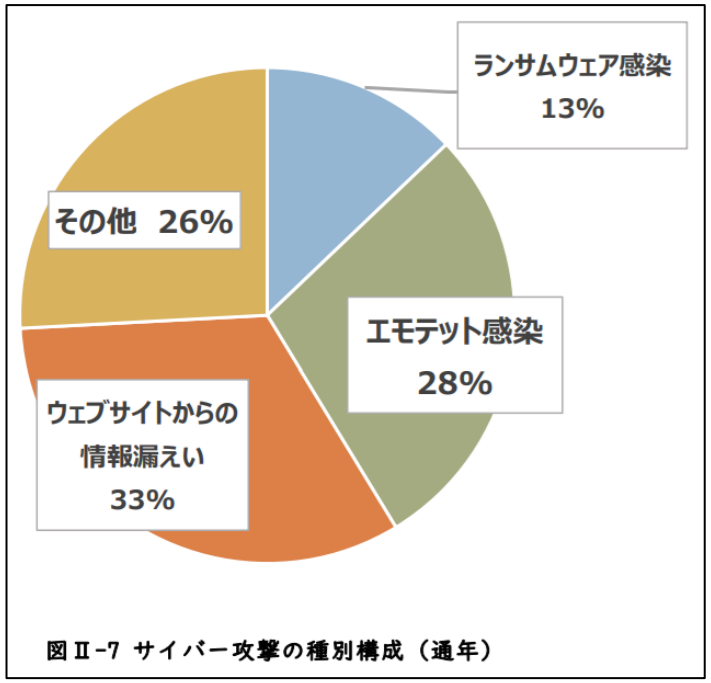


※公表されたサイバー攻撃件数の推移
2022年で爆発的に増えた理由としては、攻撃が増加したことも挙げられますが、
2022年4月に施行された改正個人情報保護法により、公表が必要になるケースが増え、
それまでは隠匿されていた攻撃が明らかにされるようになったことも挙げられます

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

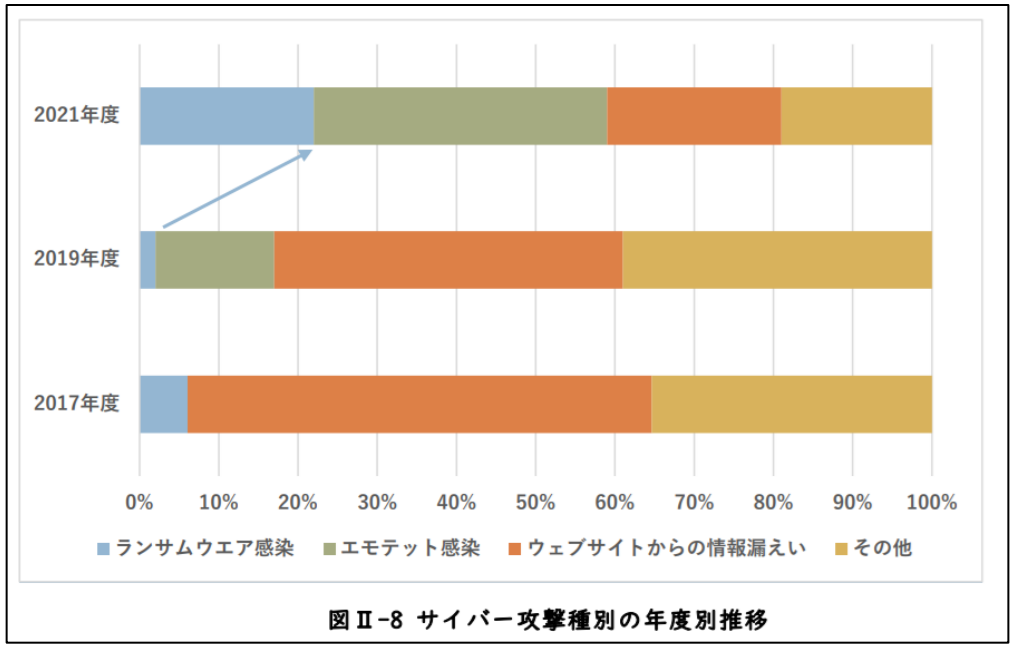
サイバー攻撃の種別（JNSA調べ）

- **サイバー攻撃の種別**
  - 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）



図Ⅱ-7 サイバー攻撃の種別構成（通年）

- **年度別のサイバー攻撃種別推移**
  - エモテット（ランサム）の伸長
    SPF保護範囲外からの「なりすましメール」での乗っ取りも流行中
  - Webサイト経由からの情報漏洩（ランサム）



図Ⅱ-8 サイバー攻撃種別の年度別推移

ランサムウェアに至る、サイバー攻撃手順

■ハッカーによるサイバー攻撃手順

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（レコナイサンス・レコネサンス：RECONNAISSANCE）

IPアドレス・ドメイン総当たりツールを用いて、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・脆弱性試行）

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）の脆弱性があれば、短時間で乗っ取り可能

④データ窃取（情報収集）

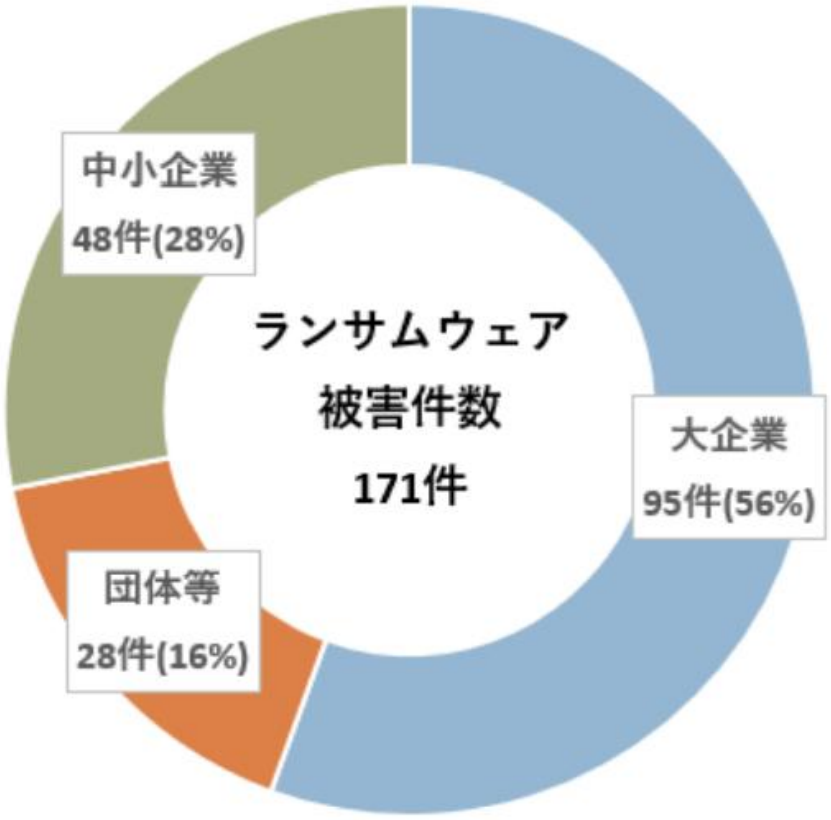
個人情報・機密データの窃取、メールの盗み見を実施
数年間にわたる情報窃取が行われるケースも多い（例：防衛庁、JAL など）

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

長期的な脅威への対策の重要性

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窃取が行われることが多いのが特徴です。
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しながら、インシデント発生に備え訓練（防災訓練）することが重要です。



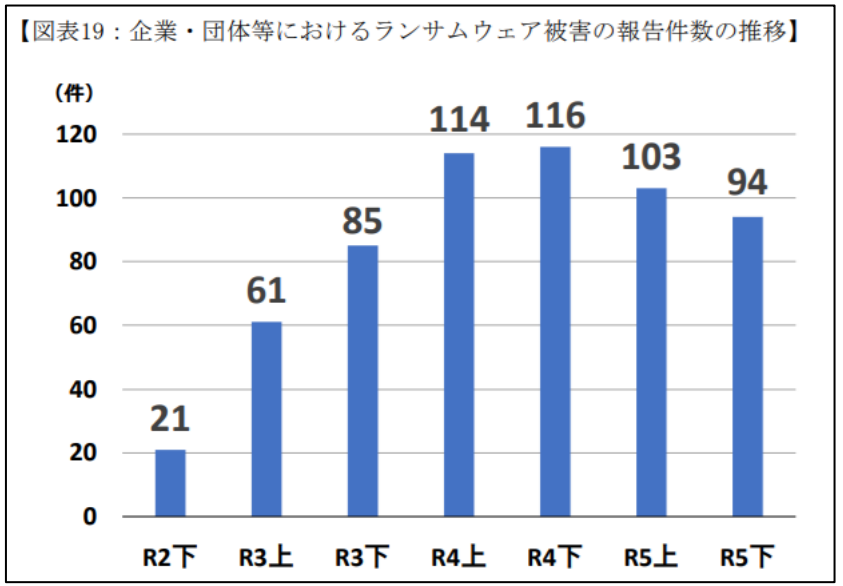
図Ⅱ-9 ランサムウェア被害組織の規模別割合

サイバー攻撃が経営与える影響

・ランサムウェア

ハッカーは、セキュリティの弱点を突いて社内システムに侵入します。
この際、金銭的価値のある情報を徹底的に盗み取ります。
そして、最後にシステム内のファイルを暗号化して使用できなくするのです。
ファイルの暗号化を行ったあと、身代金を要求します。
これが、「ランサムウェア攻撃」です。

身代金要求フェーズでは、
すべての情報が外部に漏洩しているため、もはや手遅れです。
システムを修復するまで間、事業の中断をするしかありません。
このようにランサムウェア攻撃は、
企業活動にとって重大な影響が発生するのです。



※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

サイバー攻撃が経営与える影響

・サプライチェーンへの連鎖

　ハッカーは、大手企業への乗っ取りをおこなう前段階として、サプライチェーン会員で脆弱性が多い関係企業から攻撃を開始します。

攻撃を受けた会員端末は、サイバー攻撃の踏み台に使用されます。

これにより、本来のターゲットである大手企業や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ます。

結果として、グループ全体に多大な損害を及ぼしてしまうのです。

多額の損害賠償に加え、取引が復活するまで約半年かかる場合もあります。

その間、オーダが中断するため、重大な影響を及ぼす可能性があります。

サイバー攻撃対策として、事前の防衛が大事です！

未来研究所 Future Research Inc.

- 「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）

- 空き巣と同様に、ハッカーは侵入しにくいホームページへの攻撃はあきらめることが多いです。
  事前に対策をして、防御を固めておくこと（ハードニング）が必要です。

定期的に、脆弱性診断を行うことで、防御力をUPすることが必要

脆弱性（ぜいじゃくせい）診断は、システムの健康診断

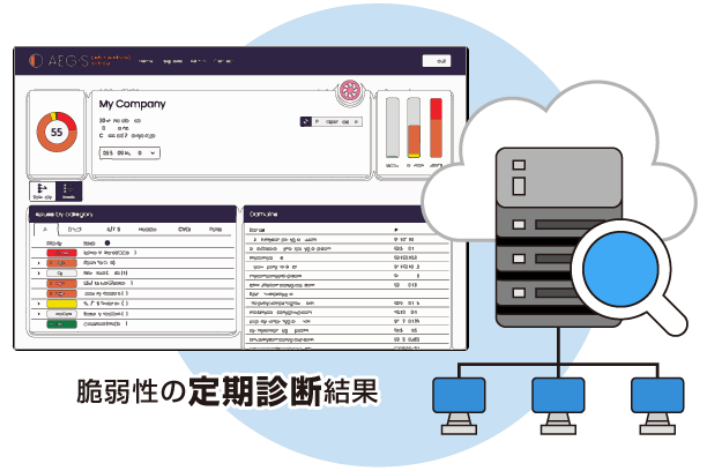
- **人の場合：健康診断**
  システムの場合：脆弱性診断

  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）の深刻度に応じて対策します。

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

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！

システムの健康診断　＝　脆弱性診断

サイバー攻撃対策の順序

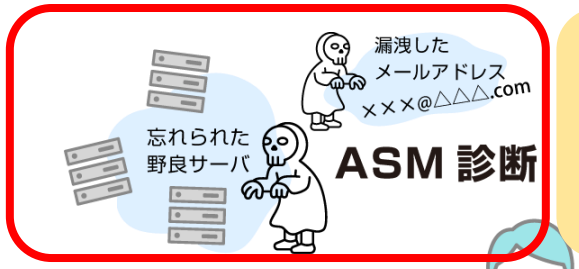
1．まずASM診断を行い、危険な個所（脆弱性）を見つけ出します

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。

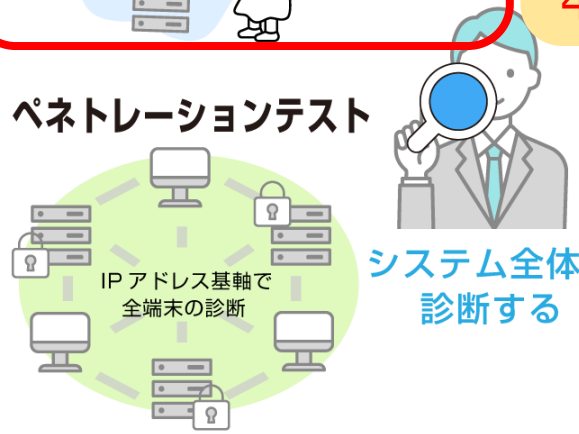
イージスEWのASM診断には、他社製品と違い、ハッカーが攻撃対象を探す方法と同種の「レコナイツール（偵察ツール）」という診断機能が含まれています

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、脆弱性診断で、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。

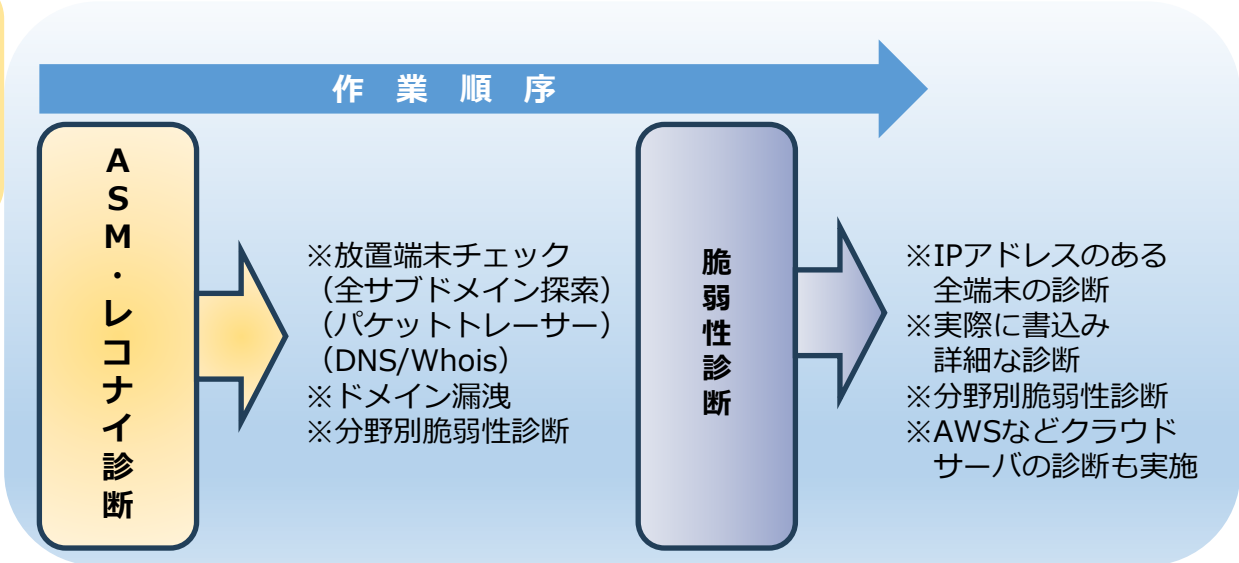


1、ASM・レコナイ診断
2、脆弱性診断
3、作業優先順位の策定
4、改修作業の実施



対策を実行！

対策作業の工程プランを策定し、
一番弱いところから対策を打って行く。
必要なツールがあれば、予算・稟議の対応が必要。



ASM・脆弱性診断・脆弱性診断

未来研究所 Future Research Inc.

■ASM(Attack Surface Management＝攻撃対象領域管理)

ASMと脆弱性診断の違いは、次の通りです。
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は「認知外（忘れられている）サーバ」も見つけ出して対象にすることです。

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)
パッシブスキャンは、ドメイン情報から放置サーバ（野良サーバ）を検出して、ハンドシェイクパケットのみで診断します。

②アクティブスキャン(Active Scan)
アクティブスキャンは、調査対象診端末に対して、ハッカーが実際にアクセスする手法に近い診断方法（脆弱性診断）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 （経済産業省の定義）	ASM	脆弱性診断
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	あらかじめ指定したIPアドレスを対象とする
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し、その応答で診断するため確度が高い
対象への影響	セキュリティ監視装置（EDS/EDR）に検出される可能性は殆どない	セキュリティ監視装置でアラームを検出することがある　多くの帯域を使用する
レコナイ・ツール （ハッカーが使用する偵察ツール）	ASMの領域に含まれる	対象外

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

脆弱性診断は、ASM＋脆弱性診断

- 脆弱性診断だけでは、**砂上の城**です
  - **ハッカーが最初に攻撃先を探すツールがASM（レコナイ）です！**

何も対策をしていない状態

建物（システム環境）は無防備。
何も対策をしていないため
ハッカー攻撃に遭う危険な状態！

ペネトレーションテストを実施

建物は改築（ペネトレーションテスト）を
実施して立派な『お城』に変わったが
砂の地面（インターネット環境）が
不安定なため、まだまだ危険な状態！

ペネトレーションテストを実施
＋ ASM を実施

地面を強固（ASM を実施）にしたので
完全なハードニング基礎が完成して

完全防備となった!!

脆弱性診断ツールでの使用されるCVSS

※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！

CVSS（共通脆弱性評価システム）とは、ソフトウェアやシステムの脆弱性の重大性（深刻度）を定量的に評価し、**スコア（0.0～10.0）**として表す仕組みです。元は、米国NISTにて発案され、今は日本始め多くの国の指標として活用されています。

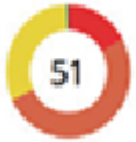
CVSS（共通脆弱性評価システム）v3.1

■CSVSS3.1基準について

・運営母体が、NISTからFIRSTに移転して運営されている
・NIST SPシリーズでも共通指標として活用されており、日本でも標準指標として使用されている
・深刻度を示す色・評価基本値は世界共通。どの脆弱性診断ツールでも同じ診断結果で表記される（同一FEED（診断項目）の場合）
・サイバー先進国では、赤・オレンジの申告が発生している場合、受け入れが却下される場合が多い（米国・英国では、赤・オレンジがあると公共機関との銀行口座が維持できない）

深刻度	CVSS v3.1基本値
緊急(Critical)	9.0～10.0
重要(High)	7.0～8.9
警告(Middle)	4.0～6.9
注意(Low)	0.1～3.9
なし(None)	0

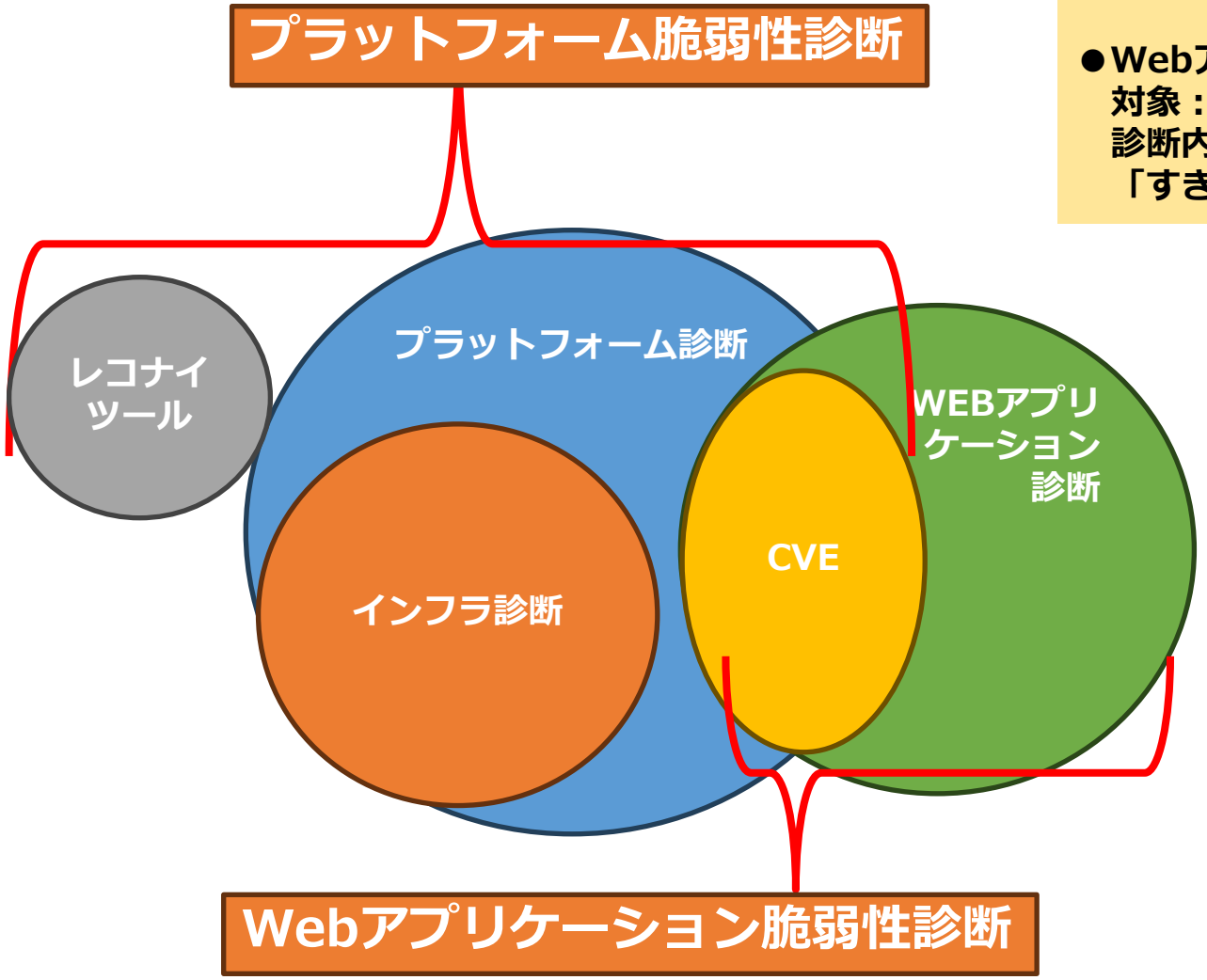
※注意事項
　脆弱性診断の結果を基にした総合評価点（この場合51点）については、
国際的に標準化された配点基準は存在せず、ツールメーカが独自で採点しているので、留意すること。



脆弱性診断ツールの種類

未来研究所
Future Research Inc.

■脆弱性診断ツール群



●プラットホーム脆弱性診断
対象：ネットワーク上に存在する全ての端末群（可能性も含む）
診断内容：OSやミドルウェアに「穴」が空いてないかを調べる診断

●Webアプリケーション脆弱性診断
対象：必ず存在するサーバ等の端末
診断内容：Webサイトの操作画面（ログイン・入力フォーム）などに「すき間」がないか調べる診断

【プラットホーム診断】OpenVAS,イージスEW, Nessus等
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
世界共通で、規格化されいる番号CVE番号が使用されている

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

【Webアプリケーション診断】OWASPZAP、Burp Suite等

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

ASMに組み込まれるレコナイツール

■ハッカーが最初に行う、攻撃サイトの抽出ツール（自動検出）

経済産業省の定義したASM機能
（Whois, DNSサーバ調査のみでは、役に立ちません）
＋
レコナイ機能（Reconnaissance＝偵察）…イージスEW独自機能

レコナイサンス (偵察)ツールは、ハッカーが攻撃対象を決めるために用います。イージスEWは、ハッカーと同等のツールを使用し、攻撃対象領域（Attack surface）や漏洩した情報を見つけ出します。

レコナイ（偵察）にて、野良端末（管理表には記載がないサブドメイン通信履歴）、過去の漏洩情報の履歴確認等を行います。　少なくとも、これらの脆弱性がある場合、該当ドメインの乗っ取りはSE1年目で可能です。（CVSSは、赤の深刻度１となります）

脆弱性診断分野　例

未来研究所
Future Research Inc.

■8つの主な分野別診断項目

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ものかどうか」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。 レコナイツール	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

ASMと脆弱性診断

【ASM】
ハッカーが初期偵察に使用します
何が分かるのか？
↓
・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**

【脆弱性診断】
IPアドレスを基軸に、深い部分まで侵入を試み、結果をもとに診断します

イージスEWは、OpenVAS（Github/Freeware）の診断項目を網羅したGreenBorn社のAPIを使用し、7万にも渡る項目の診断を実施します

脆弱性診断の必要性

■ASMと脆弱性診断の比較

なぜ、脆弱性診断を行う必要があるのか？
理由は、「ASMだけではわからないことがある」ためである
【ASMと脆弱性診断の違い】

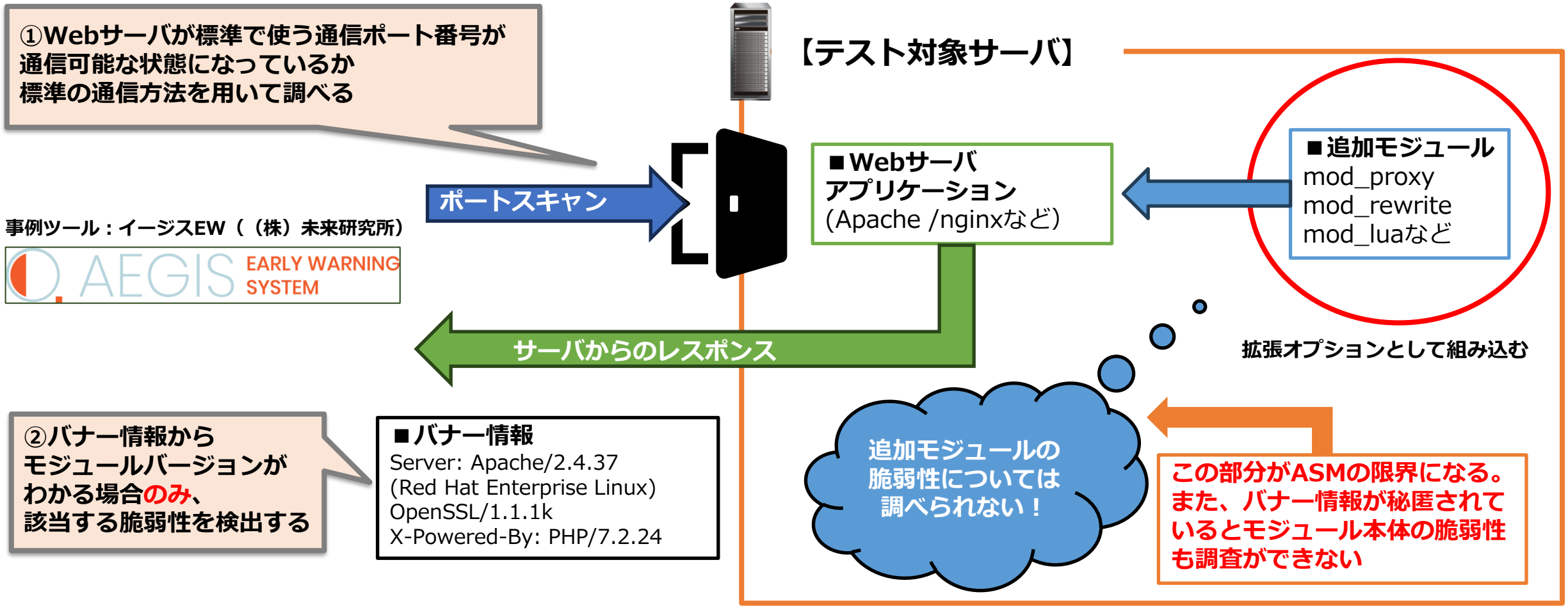
項目	ASM (Attack Surface Management)	脆弱性診断
診断の目的	・外部攻撃に対する表面的な脆弱性を可視化し、早期に対応可能な問題をリスト化する ・リスク評価の補助	・内部・外部攻撃を含めた本番環境での攻撃リスクを詳細に調査し、実際に悪用されるシナリオを想定
対象とするシステム	本番、ステージングいずれでも実施可能（影響が極めて少ない）	**出来ればステージング環境で実施。無ければ本番ステージングで実施**
診断の深度	「浅い」 ・そのポートが空いているか ・バナー読み取りは正常通信の範囲のみ	「深い」 ・侵入攻撃を実際に仕掛けている ・エラー時の戻り値や攻撃成功時の挙動から脆弱性を調査する
読み取れる情報の範囲	「狭い」 ・バージョン情報からわかる脆弱性のみ ・オプションモジュールについては、バナーでわかる場合だけ ・モジュールのバージョン検出ができる場合のみ、CVEを列挙	「広い」 ・パスワードの強度がわかる（FTP／SSH） ・オプションのモジュールに由来する脆弱性もわかる ・挙動からバージョンを推測 ・モジュールバージョンが検出できない場合でも、ハッキングアルゴリズムを実施してCVEを洗い出す ・本当に脆弱性を検出できた場合のみCVEを表示
実施のリスク	・軽微：通常、システムのパフォーマンスにほとんど影響を与えない ・本番環境でも安全に実施可能	**・中～高：本番環境での負荷や、一部サービスの停止リスクを伴う可能性** **・攻撃シミュレーションが原因でシステムの動作が不安定になる場合がある** ・事前のバックアップが必要である
コスト・時間	・低：自動化ツールでの定期実施が可能 ・短時間で完了	・高：専門スキルを持つテスターによる評価が必要 ・時間がかかるケースが多い

ASMと脆弱性診断の違い

未来研究所
Future Research Inc.

■ASMでは、具体的に何を見ているのか？

ASMでは、標準の通信方法でのみ調査をしている。このため、調査できる内容に限界がある



ASMと脆弱性診断の違い

■脆弱性診断では、具体的に何を見ているのか？(1)

脆弱性診断は、実際のサイバー攻撃を安全な範囲で行う。
このため、ASMより深い範囲で脆弱性診断を行う。

【テスト対象サーバ】

①Webサーバが標準で使う通信ポート番号が通信可能な状態になっているかだけでなく、本当のサイバー攻撃と同様に
オーバーフロー値や変形データを用いて調査する

■攻撃の例（セッションハイジャック）
GET /?redirect=/userpage%0d%0aSet-Cookie:%20sessionid=98３ー66
HOST: sample.com
（加工済GETパラメータを用いて任意のSessionIDを挿入）

サイバー攻撃を実施

■Webサーバ
アプリケーション
(Apache /nginxなど)

■追加モジュール
mod_proxy
mod_rewrite
mod_luaなど

サーバからのレスポンス

②バナー情報からサーバの詳細情報がわからない場合でも、攻撃を通じてサーバの脆弱性を調査する

■バナー情報
HTTP/1.1 200 OK
< Server: nginx

④複数の攻撃シナリオを実施した結果、追加モジュールの脆弱性も判明する

③複数の攻撃シナリオを実施することにより、追加モジュールの組み込み状況と脆弱性をあぶり出そうと試みる

サーバに対して、複数の攻撃シナリオを実施

事例ツール：イージスEW（（株）未来研究所）

AEGIS EARLY WARNING SYSTEM

ASMと脆弱性診断の違い

未来研究所 Future Research Inc.

■脆弱性診断では、具体的に何を見ているのか？(2)

脆弱性診断では、「データ部分とヘッダ部の両方を用いて攻撃シナリオを実施」します。
これにより、ASMでは検出することができない脆弱性を調査可能です

事例ツール：イージスEW（（株）未来研究所）

AEGIS EARLY WARNING SYSTEM

サイバー攻撃を実施

【テスト対象サーバ】

■Webサーバ
アプリケーション
(Apache /nginxなど)

■追加モジュール
mod_proxy
mod_rewrite
mod_luaなど

アプリケーション側が想定していないデータが挿入されることによって、脆弱性が洗い出される

追加モジュールに由来する脆弱性も
過去に攻撃が成功したデータパターンを用いることにより、検出ができる

脆弱性診断では、次のような攻撃シナリオを実施して脆弱性を洗い出す。
一例として、HTTPの脆弱性調査を下記に示す。

例1：
「①リクエスト行」に本来禁止されているDELETE（ファイル削除）、PUT（ファイル置換）などを挿入

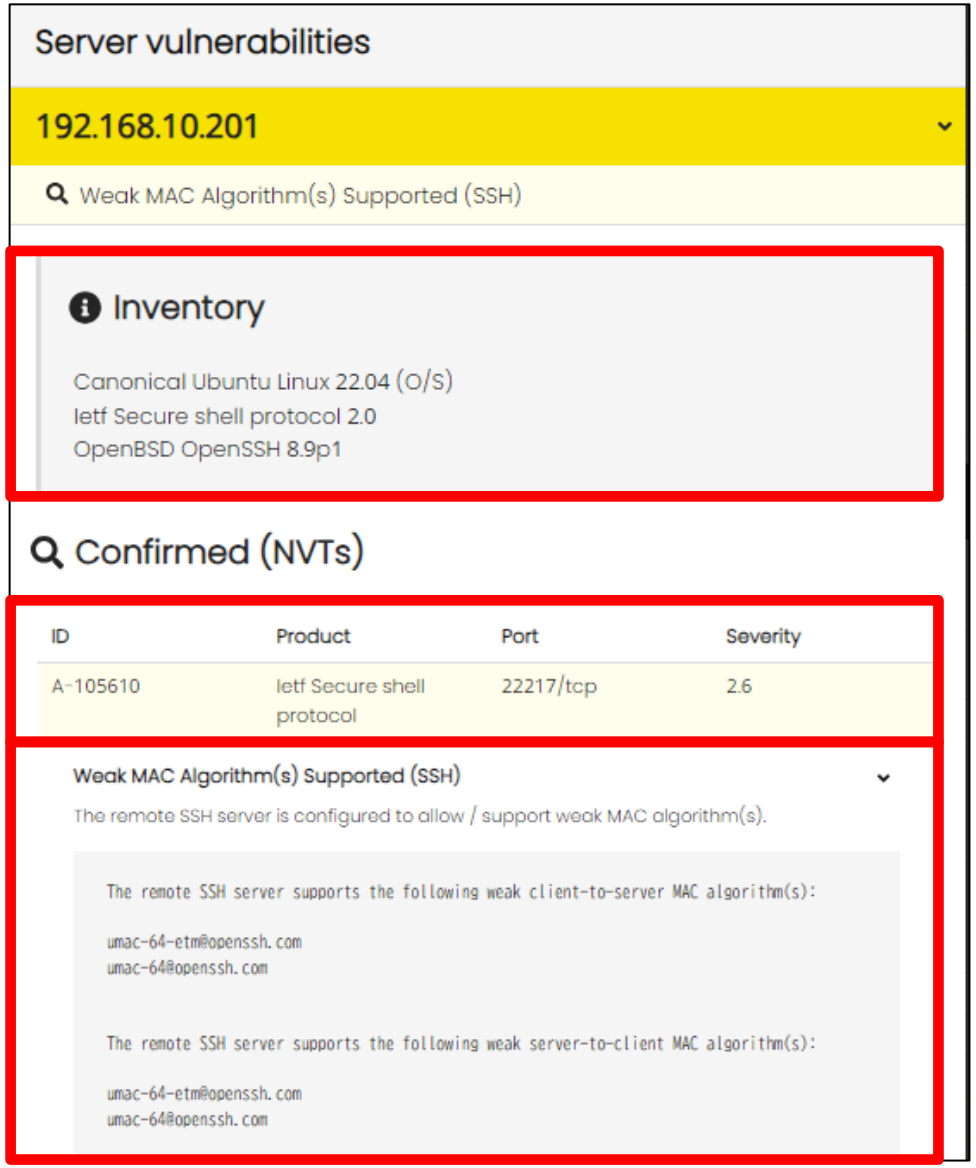
例2：
「②HTTPヘッダー」に極端に大きな値（オーバーフロー値）やサーバ側のHTTPヘッダーを書き換える値を用いた攻撃

例3：
「④データ部分」を解析して、脆弱性を調査する（例：jQueryなどのバージョンを検出する）

①リクエスト行 GET /XXX/index.html HTTP/1.1
②HTTPヘッダー Date: Tue, 15 Nov 1994 08:12:31 GMT Host: future-research.jp User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) Content-Length: 352
③(空白)
④データ部分 実際のデータ（HTMLなど）

脆弱性診断実施時の結果表示例

事例ツール：イージスEW（（株）未来研究所）



脆弱性診断では、全て「稼働しているサービスに対して、実際の侵入を試みている」このため、ASMよりも深い範囲で脆弱性の検出が可能である

■OS情報・モジュール情報
実際に、モジュールに対してアクセスをして、バナー情報から取得する。

■検出された脆弱性
例のように、ウェルノウンポート番号から変更した場合（SSH:22/tcp → 22217/tcp）であっても、実データから使用モジュールを判別して脆弱性の調査を行う

■脆弱性の詳細
例では、「実際に弱いMAC認証アルゴリズムで接続を試みた結果」を表示している。これにより、弱い暗号強度のMAC認証アルゴリズムを有効化する設定が/etc/ssh.conf内に残っていることが洗い出されている

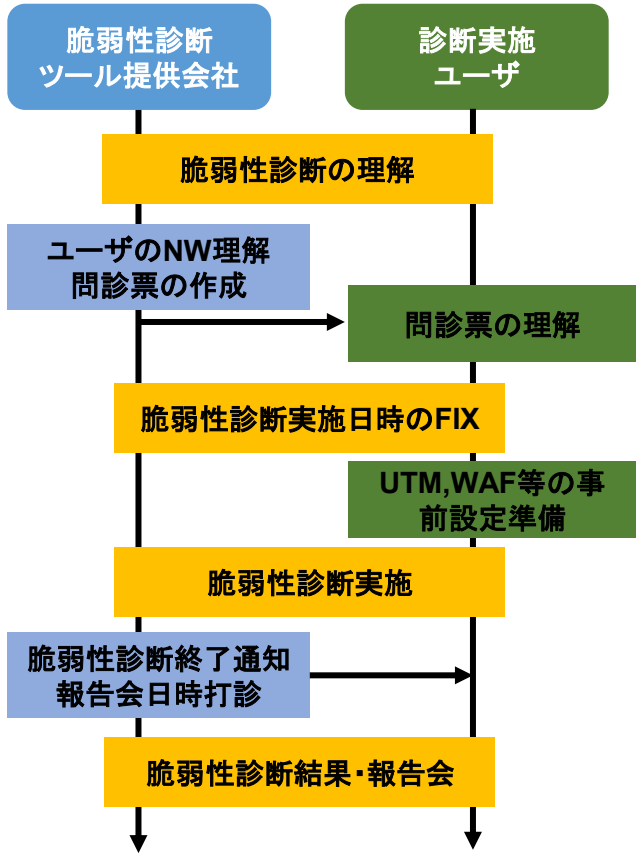
ASMと脆弱性診断の実施について

■ASMの実施タイミング

診断のためのアクセス時間も少ないため、通常、実施のタイミングの制限はない。　24/365いつでも実施可能

■脆弱性診断の実施タイミング

脆弱性診断では、FEED（診断登録されているDBフィールドの呼び名）に登録されている、典型的な侵入パタンも実施する。
診断端末数にも依存はするが、膨大な診断パケットが発生する。
このため、診断のための通信帯域が急増するため、通常業務への影響が心配される。
故に、脆弱性診断の実施日は、深夜・休日に集中的に実施するケースが多い。
また、インターネット経由のSaaSで診断を行う場合には、診断用IPアドレスが各種・セキュリティツール（IPS/IDS・UTM VPNルータ、WAF、EDR等）に検知されないための設定を、事前に行う必要がある。



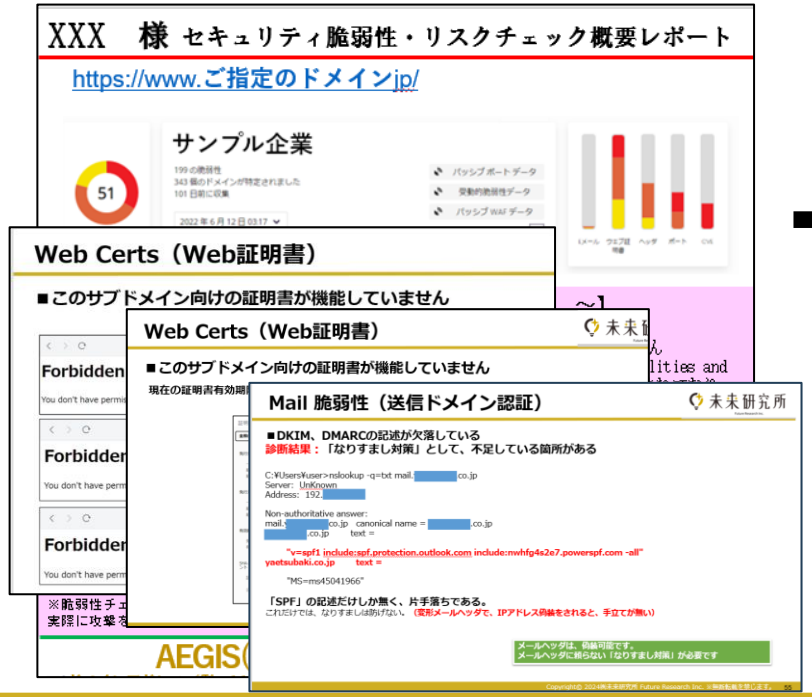
脆弱性診断結果説明会

未来研究所
Future Research Inc.

■脆弱性診断の報告書（報告会）に関する注意点

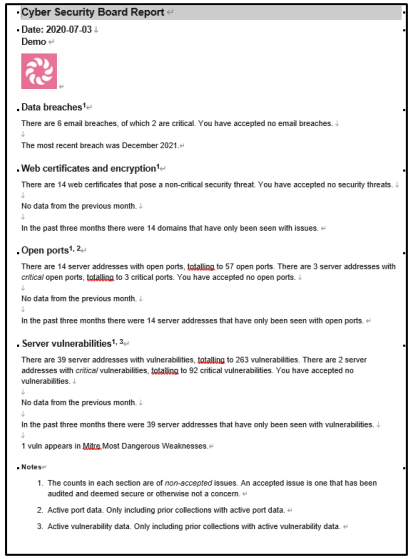
① 脆弱性診断の報告書には、診断結果の内容に加えて、それに対する具体的な改修方法が
　説明されるかどうかが重要です
② 中には、診断のみを行い、改修のアドバイスや支援を行わない業者も存在します
③ 診断を依頼する際は、報告会でどこまで対応してもらえるのかを事前に確認しておくことが大切です

【評価レポートの事例（イージスEW）】

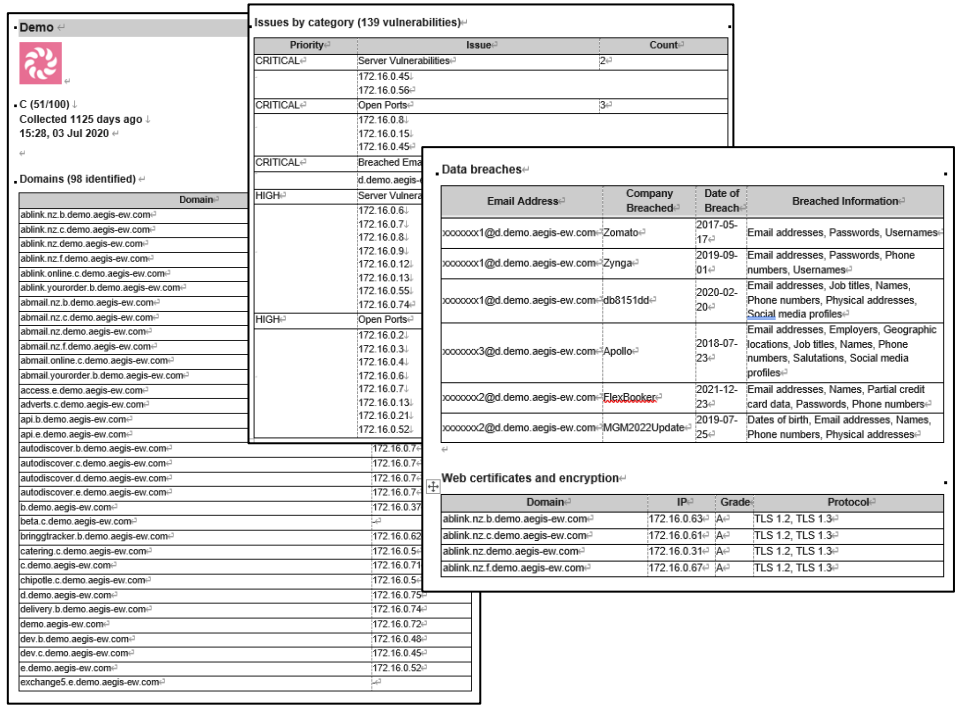


＋

※サマリー



※詳細：CVSS、CVE　等、過去の漏洩情報も記載



事例ツール：イージスEW（（株）未来研究所）

AEGIS EARLY WARNING SYSTEM

脆弱性診断ツールの定義を明確に！

■最近では、日本の市場でも、UTM（統合脅威管理）やEDR（エンドポイント検知と対応）といったセキュリティ製品も含めて、「脆弱性診断ツール」という言い方が広まりつつあります。
まず最初に必要なのは、システム全体をチェックする「システムの人間ドック」だという認識を持つことです。

①「システムの人間ドック」であるプラットホーム・Webアプリケーション脆弱性診断を実施する

② 診断結果から、深刻度が高い（CVSSv3.1 赤・オレンジ）事象から改修する。
そのために必要な予算を算出し、経営層からの予算を取得する

③ 初めて、UTM・WAF・EDR等のセキュリティツールの設置も考慮したハードニング作業を開始

④ 脆弱性診断管理ツールにて、定期的な診断を行い、ゼロディ攻撃への対処も実施する

脆弱性診断ツールを選ぶ際に、押さえるべき選定基準

未来研究所
Future Research Inc.

■脆弱性診断ツールの重要なポイント

① ユーザが求める脆弱性診断の対象領域は？
- ASM / ASM（レコナイ含む）診断
  プラットホーム脆弱性診断ツール
- 脆弱性診断
  プラットホーム脆弱性診断ツール or Webアプリケーション脆弱性診断ツール
  もしくは、両方

②ユーザの脆弱性診断管理方法について
- 1台毎の脆弱性診断（脆弱性診断）
  → OpenVAS、Nessus等で対応
- 対象端末台数（対象ドメイン、IPアドレス数）が数十台から数千台数
  → 自動で定期的に全端末を脆弱性診断してくれる総合管理ツールが必要
  → イージスEW、Tanabel、SSC,,等々

③対象端末が、インターネット・イントラネット（社内端末群）・納品前診断（特定社会基盤）の場合
- 全セグメントの管理が可能であること（次ページ、参照）

④診断結果の改修方法は？工数・予算的な課題は？

脆弱性診断の義務化で見た、日本と世界

未来研究所
Future Research Inc.

【脆弱性診断の義務化で診た日本と世界】

区分	日本	アメリカ US	イギリス GB	EU諸国 EU
公共機関における脆弱性診断の義務	明確な義務規定なし（※安全対策基準で「望ましい」） ただし、公共機関が特定社会基盤事業者に含まれる場合、役務に関するシステムの脆弱性診断実施は、義務化されている	**FISMA法により義務化**。NIST SP 800-53準拠でCDM含む。	NCSCガイドライン準拠。**Cyber Essentials Plus取得時に第三者診断が必須**。	**NIS2指令**により義務化。各国の国家当局に報告義務あり。
金融機関における脆弱性診断の義務	金融庁ガイドラインで強く推奨されており、特定社会基盤枠にも脆弱性診断は義務化されており、**役務システムに関しては、インターネット・社内ネット・納品前システムに置いて、実施が義務化**されている。金融庁は金融庁は、内部監査部門とのコミュニケーションを重視し、モニタリングの効率化を図っている	GLBA法・FFIECガイドラインにより**年次評価・報告が事実上義務**	FCA監督のもと、**脆弱性対応は業務継続性の一部として義務化**	**DORA規則（2025施行予定）により脆弱性診断・ペネトレーションテストの定期実施と報告が義務化**
行政への提出義務	**原則なし**（個人情報保護委員会・金融庁への報告はインシデント時） 1年に1回ほどの脆弱性診断を推奨しているが、その評価システム・合否指針・対策義務等は、策定されておらず**深刻度の高い脆弱性は放置されているケースが多い**	連邦政府部門はDHSへ報告。**年次監査に診断レポート提出**。	一部行政契約にて提出を義務化（Cyber Essentials準拠）。	NIS2では**重要事業者に診断報告・リスク評価の提出義務**
保険会社（生命、損保）における脆弱診断の義務	金融庁が定義している特定社会基盤には、主要保険会社も含まれており、銀行と同様のハードニングを課している。**役務システムに関しては、インターネット・社内ネット・納品前システムに置いて、実施が義務化。**	**年次評価・報告が事実上義務化**。保険会社のサイバーセキュリティ対策は、州毎で規制。ニューヨーク州・23NYCRR Part500(サイバーセキュリティ規制）、他州・全米保険監督官協会（NAIC）の「サイバーセキュリティモデル法」に準拠	保険会社へのサイバーセキュリティ規制：UK-GDPR（一般データ保護規則、インシデント発生時72時間以内でのICOへの報告義務）、NIS2（セキュリティ管理業務の定期評価レポート提出）、サイバーセキュリティ・レジリエンス法（2025年～：技術系評価も含む：**定期セキュリティの脆弱性診断結果報告、IT-BCP訓練報告**、等）	・DORA（デジタル運用レジリエンス法）規則（2025施行予定）により**脆弱性診断・ペネトレーションテストの定期実施と報告が義務化** ・NIS2指令　重要事業者に診断報告・リスク評価の提出義務
法的強制力	基本は**行政指導レベル**（特定社会基盤事業者に対しては、法的拘束力あり）	明確な**連邦法**	法的拘束力あり（公共契約との連動）	**EU規則または各国法で義務化**（違反時罰則あり）

Thanks