IBC セキュリティアセスメントサービス

IBC-SAS Web アプリ脆弱性診断サービス

情報処理推進機構（IPA）が毎年発行している情報セキュリティ 10 大脅威 2025 において、脆弱性にかかわる脅威として「サプライチェーンや委託先を狙った攻撃」、「機密情報等を狙った標的型攻撃」、「システムの脆弱性を突いた攻撃」などがランクインしました。

脆弱性管理の必要性　IPA「情報セキュリティ 10 大脅威　2025」

順位	脅威	昨年順位
1位	ランサム攻撃による被害	1位
2位	サプライチェーンや委託先を狙った攻撃	2位
3位	システムの脆弱性を突いた攻撃	7位
4位	内部不正による情報漏えい等	3位
5位	機密情報等を狙った標的型攻撃	4位
6位	リモートワーク等の環境や仕組みを狙った攻撃	9位
7位	地政学的リスクに起因するサイバー攻撃	-
8位	分散型サービス妨害攻撃（DDoS攻撃）	-
9位	ビジネスメール詐欺	8位
10位	不注意による情報漏えい等	6位

※ 出典：情報処理推進機構（IPA）「情報セキュリティ10 大脅威 2025」

- 第2位「ビジネス上の繋がり」を悪用した攻撃は、自組織の対策のみでは防ぐことが難しいため、関係組織も含めたセキュリティ対策が必要な脅威と言える。また「ソフトウェア開発の繋がり」を悪用した攻撃もまた脅威であり、対策が必要である。
- 第3位 ソフトウェアやハードウェアの脆ぜい弱性対策情報の公開は、脆弱性の脅威や対策の情報を製品の利用者に広 く呼び掛けられるメリットがある。一方で、攻撃者はその情報を悪用し、脆弱性対策を講じていない当該製品を使用したシステムを狙って攻撃を行うおそれがある。近年では脆弱性関連情報が公開されるとすぐに攻撃コー ドが流通し、攻撃が本格化するまでの時間がますます短くなっている。
- 第5位 特定の組織（企業、官公庁、民間団体等）を狙う攻撃のことであり、機密情報等を窃取することや業務妨害を目的としている。攻撃者は社会の変化や働き方の変化に合わせて攻撃手口を変える等、標的とする組織の状況に応じた巧みな攻撃手法で機密情報等を窃取しようとする。

よくある脆弱性診断の課題

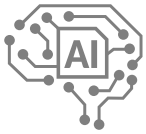
診断開始までの
リードタイムが長く対応が遅れている

報告内容の品質に差があり
提供ベンダーを変更したい

コスト改善を図りたいが
ベンダーの良し悪しが判断できない

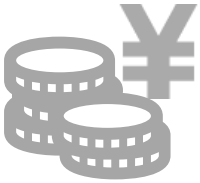
IBCは、AIプラットフォーム（Immuni Web）を利用した脆弱性診断サービスを提供

Web アプリ脆弱性診断（AIプラットフォーム+セキュリティスペシャリストによる診断）



AIがサイト全ページをスピーディーに診断

最新攻撃を自動学習(12h毎)セキュリティ専門家が結果を確認



圧倒的に優れたコストパフォーマンス

Web アプリ診断項目一覧

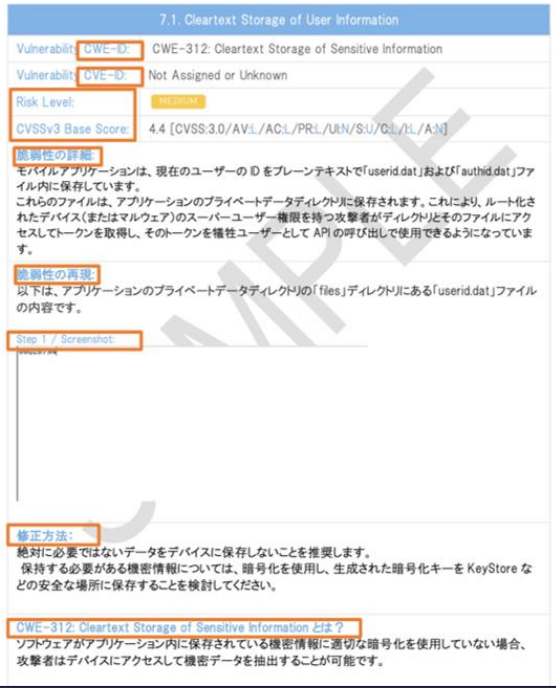
診断項目
OWASP Top10
CWE/SANS Top25
OWASP TestingGuide v4
WEB サーバテスト（PCIDSS/GDPR）
SSLテスト（PCIDSS/GDPR）

OWASP Top 10 の診断項目詳細	
1	アクセス制御の不備
2	暗号化の失敗
3	インジェクション
4	安全が確認されない不安な設計
5	セキュリティの設定ミス
6	脆弱で古くなったコンポーネント
7	識別と認証の失敗
8	ソフトウェアとデータの整合性の不具合
9	セキュリティログとモニタリングの失敗
10	サーバーサイド・リクエスト・フォージェリ

以下のガイドラインに準拠し、脆弱性診断を実施

国際セキュリティガイドライン
NIST SP 800-115 Technical Guide to Information Security Testing and Assessment
PCI DSS Information Supplement: Penetration Testing Guidance
FedRAMP Penetration Test Guidance
ISACA’s How to Audit GDPR

報告書イメージ


7.1. Cleartext Storage of User Information

Vulnerability CWE-ID: CWE-312: Cleartext Storage of Sensitive Information

Vulnerability CVE-ID: Not Assigned or Unknown

Risk Level: MEDIUM

CVSSv3 Base Score: 4.4 [CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N]

脆弱性の詳細:
モバイルアプリケーションは、現在のユーザーの ID をプレーンテキストで「userid.dat」および「authid.dat」ファイル内に保存しています。
これらのファイルは、アプリケーションのプライベートデータディレクトリに保存されます。これにより、ルート化されたデバイス（またはマルウェア）のスーパーユーザー権限を持つ攻撃者がディレクトリとそのファイルにアクセスしてトークンを取得し、そのトークンを犠牲ユーザーとして API の呼び出しで使用できるようになっています。

脆弱性の再現:
以下は、アプリケーションのプライベートデータディレクトリの「files」ディレクトリにある「userid.dat」ファイルの内容です。

Step 1 / Screenshot:

修正方法:
絶対に必要ではないデータをデバイスに保存しないことを推奨します。
保持する必要がある機密情報については、暗号化を使用し、生成された暗号化キーを KeyStore などの安全な場所に保存することを検討してください。

CWE-312: Cleartext Storage of Sensitive Information とは？
ソフトウェアがアプリケーション内に保存されている機密情報に適切な暗号化を使用していない場合、攻撃者はデバイスにアクセスして機密データを抽出することが可能です。

SAMPLE

CWE（Common Weakness Enumeration）共通脆弱性タイプ一覧
発見された脆弱性がどのような攻撃手法により活用されるのかを示します。脆弱性の修正方法を知る際に役立ちます。

CVE(Common Vulnerabilities and Exposures)共通脆弱性識別子
発見された脆弱性の共通番号を表示します。脆弱性の修正方法を知る際に役立ちます。

CVSS（Common Vulnerability Scoring System）共通脆弱性評価システム
発見された脆弱性がどの程度危険であるかをCritical,High,Middle,Lowの4種類で評価します。

脆弱性の詳細
発見された脆弱性がどのようなものであるか説明します。

脆弱性の再現
発見された脆弱性が誤検出でないことを確認するため、再現方法を示します。

スクリーンショット
発見された脆弱性の再現方法をキャプチャします。

修正方法
発見された脆弱性の修正方法を示します。

脆弱性によるリスクの説明
発見された脆弱性によるリスクに関して記述します。

※ Immuni Web以外のWebアプリ脆弱性診断サービスも提供しております。
複数の専門業者と連携し、お客様のニーズにあった診断サービスを提供しておりますので、是非ご相談ください。

IBC
アイビーシー株式会社

本社
〒104-0033
東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780 fax.03-5117-2781

西日本事業所
〒532-0003
大阪府大阪市淀川区宮原4-1-14 住友生命新大阪北ビル3F
tel.06-7653-1014 fax. 06-7177-0542