IBC セキュリティアセスメントサービス

IBC-SAS プラットフォーム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」、「システムの脆弱性を突いた攻撃」、「機密情報等を狙った標的型攻撃」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　2024」

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 では、複数の専門事業者と連携し、お客様のニーズにあった診断サービスを提供しています。**

プラットフォーム脆弱性診断（マニュアル診断）

- パッチ適用状況
- 脆弱な設定
- 不要なサービス
- 容易なパスワード
- 不要なアカウント

プラットフォーム診断項目

No.	診断項目	概要	
		調査・確認事項	主な脅威
1	ホストの存在確認	対象サーバの存在を確認 主にICMPパケットを利用	ICMPレスポンス状況によっては、攻撃者に攻撃の糸口を与える可能性あり
2	ポートスキャン (TCP/UDP全ポート)	対象サーバのオープンポート確認	不正侵入・攻撃を行う前の事前調査として動作しているサービス状況が判明
3	不要と思われるサービス の稼働	サービスの動作状況確認	不要なサービスの動作は、攻撃者に攻撃の糸口を多く与える可能性あり
4	稼働中のサービスからの 情報取得	稼働しているサービスのバナー情報等を取得	動作しているプログラムの特定等により、攻撃に利用される可能性あり
5	OSやアプロケーションソフトウェアの既知の脆弱性	OSのバージョンやセキュリティパッチの適用状況等を確認	既知の脆弱性を利用したコマンドの実行やサービス妨害攻撃を受ける可能性あり
6	脆弱なパスワード設定	認証を伴うサービスに対して容易に推測可能なパスワードが設定されていないか確認	なりすましにより不正にシステムにアクセスされる可能性あり
7	脆弱性の知られている CGIスクリプトの存在	CGIスクリプトの存在確認及びバージョンなどを確認	既知の脆弱性を利用したコマンドの実行やサーバの内部情報を取得される可能性あり
8	アカウントポリシーの調査	アカウントロックアウト値などを取得できた場合設定値の妥当性を評価	設定値に不備がある場合、パスワード推測攻撃が容易になったり、攻撃の成功確率が上がる可能性あり
9	各種サービス(FTPサービス、SSHサービス等)の既知の脆弱性	各種サービスにおいて脆弱性の報告されている古いバージョンのソフトウェアが稼働していないか確認	既知の脆弱性を利用したコマンドの実行やサービス妨害攻撃を受ける可能性あり
10	サービス運用妨害(DoS) の可能性	サービス運用妨害攻撃を実施できる可能性があるか確認	提供しているサービスが停止または、アクセスが困難になる可能性あり
11	サーバ設定上の問題	サーバ設定(書込権限やアクセス制御設定等)がセキュリティ的に妥当であるか確認	セキュリティ的に不備がある設定の場合、不正侵入等の攻撃に利用される可能性あり
12	プライベートアドレス漏洩	対象ホストからの応答にプライベートアドレス等が含まれていないか確認	システムの内部ネットワーク情報が漏えいすることにより、不正侵入等の攻撃に利用される可能性あり
13	DNSゾーン転送の可否	DNS ゾーン転送を不特定のホストに許可しているか確認	ドメイン内に存在すると思われるホストと利用用途を容易に特定することが可能となり攻撃対象が多くなる
14	DNS再帰的問い合わせ の可否	DNS再帰的問い合わせを許可している設定か確認	許可している場合、DNSサーバの不正利用や他のサーバを攻撃する DDoS 攻撃に利用される可能性あり
15	DNS ダイナミックアップデートの可否	DNS レコードをアップデート可能な設定であるか確認	任意のレコード追加により悪意あるサイトに利用者を誘導することが可能
16	メール不正中継の可否	メールサーバのメール中継の設定状況を確認	不正中継が可能な場合、スパムメールの送信などに利用される可能性あり
17	メールサーバによるユーザ情報漏えい問題	メールサーバでユーザに許可しているコマンドやサーバの応答等を確認	コマンドの応答結果により登録されているユーザー情報を特定され、パスワード推測攻撃に利用される可能性あり
18	Web サーバ上のデフォルトコンテンツの存在	システム導入時にインストールされるデフォルトコンテンツが存在するか確認	デフォルトコンテンツに脆弱性があった場合、それを利用した不正侵入や攻撃に利用可能な情報を取得される可能性あり
19	不要なファイルの存在	不要なファイルが公開されていないか確認	ファイルの情報から、攻撃者に攻撃の糸口を多く与えてしまう
20	Proxy 設定の不備	Proxy サーバの設定がセキュリティ的に妥当であるか確認	セキュリティ的に不備がある設定の場合、ほかのシステムを攻撃する際の踏み台として利用される可能性あり
21	不適切な SSL サーバ証明書の利用	SSL サーバ証明書を取得して信頼できる証明書であるか確認	SSL サーバ証明書に不備がある場合、サーバの実在証明ができず、利用者が悪意ある偽のサーバに誘導されても判断がつかず、偽のサーバに情報を送信してしまう可能性あり
22	エラーメッセージによる情報漏えい	エラーメッセージが返るようなリクエストを送りエラーメッセージにサーバ内部情報等が含まれていないか確認	サーバ内部情報等が含まれている場合、取得した情報を不正侵入等の攻撃に利用される可能性あり
23	ワーム感染の有無	既にワームに感染していないかを確認	攻撃や不正侵入、サービス妨害に利用されている可能性あり
24	バックドア検出	バックドアが既に仕組まれていないかなど様々な項目を確認	バックドアがある場合、すでに不正にシステムを利用されている可能性あり

※ 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