

脆弱性診断 総合サマリー報告書

別紙: 診断対象・評価基準・用語集

提出先 株式会社サンプル商事 御中

サンプルレポート

本書は架空の企業・システムを想定したサンプルです。記載の社名・ドメイン・IP アドレス・担当者名・数値は実在しません。

株式会社セキュア DX
セキュリティ事業部

1. 診断対象一覧

1.1 ネットワーク診断対象（9 台）

#	IP アドレス	セグメント	用途	所見数（延べ）
1	xxx.xxx.xxx.11	DMZ1	FW（プライマリ）	0 件
2	xxx.xxx.xxx.12	DMZ1	DNS / MAIL	0 件（DNS レコードの所見 NW-005 は下記に計上）
3	xxx.xxx.xxx.13	DMZ1	FW（セカンダリ）	0 件
4	xxx.xxx.xxx.41	DMZ2	FW	0 件
5	xxx.xxx.xxx.42	DMZ2	ロードバランサ（ステージ ング系）	1 件
6	xxx.xxx.xxx.43	DMZ2	ロードバランサ（LB 1 号 機）	7 件
7	xxx.xxx.xxx.44	DMZ2	ロードバランサ（LB 2 号 機）	0 件
8	xxx.xxx.xxx.45	DMZ2	サンプルオーダー（WebAP 診断の対象と同一ホスト）	1 件
9	xxx.xxx.xxx.200	ISP 回線	サンプルオーダー インター ネット	0 件
-	-	-	DNS レコード （example.co.jp / example.net）	1 件
計	-	-	-	延べ 10 件／実所見数 8 件

※ 所見数は、複数ホストに関係する所見（NW-004、NW-007）をホストごとに重複して計上した「延べ件数」である。

1.2 Web アプリケーション診断対象

#	URL	種別	所見数
1	https://stg.shop.example.jp/	B2B-EC サイト（サンプルオーダー）	11 所見 + 複合所見 1

※ 本番環境（www.shop.example.jp）は診断対象外。ステージング環境が本番同等構成である旨は貴社申告に基づく。

2. CVSS スコアの評価基準

本報告書の深刻度評価は、CVSS v3.1 の基本値（Base Score）に基づく。

深刻度	CVSS スコア目安	説明
緊急 (Critical)	9.0 - 10.0	悪用が容易かつ影響が極めて大きい。直ちに対応が必要
高 (High)	7.0 - 8.9	悪用された場合の影響が大きい。速やかな対応が必要
中 (Medium)	4.0 - 6.9	条件により悪用される可能性がある。計画的な対応を推奨
低 (Low)	0.1 - 3.9	影響は限定的。状況に応じて対応を検討
情報 (Info)	---	直接の脆弱性ではないが、留意すべき情報・推奨事項

※ 本報告書の「優先度」は、上記の深刻度に加え、対応期限・複合リスク・対策の依存関係を勘案して決定している。深刻度が Low であっても対応期限が確定している項目は優先度を引き上げている。

3. 用語集

用語	説明
TLS	通信を暗号化するプロトコル。TLS 1.2 以上の使用が推奨される
Forward Secrecy	暗号鍵が漏洩しても、過去の通信が解読されないようにする仕組み
SPF / DKIM / DMARC	なりすましメールを防ぐための送信ドメイン認証技術。SPF は送信元 IP、DKIM は電子署名を検証し、DMARC は認証失敗時の処理方針を受信側に指示する
MFA (多要素認証)	パスワードに加え、スマートフォン等の別手段でも本人確認を行う認証方式
JWT (JSON Web Token)	ログイン状態をサーバーとやり取りするためのトークン形式。署名により改ざんを検知できる

用語	説明
CSP / HSTS	ブラウザの挙動を制御するセキュリティヘッダー。CSP はスクリプトの読み込み元を制限し、HSTS は HTTPS 接続のみを強制する
WAF (Web Application Firewall)	Web アプリケーションへの攻撃を検知・防御する専用のファイアウォール
CVSS / CVE / CWE	CVSS は脆弱性の深刻度を 0.0 - 10.0 で評価する基準、CVE は公開脆弱性の識別番号、CWE は脆弱性の種類の分類体系
EOL (End of Life)	ソフトウェアのサポート終了。セキュリティパッチが提供されなくなる状態
グレーボックス / ブラックボックス診断	対象の情報 (IP・構成等) を事前に共有して行う診断 / 内部情報を持たず外部からのアクセスのみで行う診断
DMZ (非武装地帯)	インターネットと社内ネットワークの間に設けられた中間ネットワーク領域
Attack Surface	攻撃対象面。攻撃者がアクセスできるポイントの総称

4. 攻撃手法の解説

本報告書で言及される主な攻撃手法について解説する。

4.1 SQL インジェクション

Web アプリケーションの入力欄や URL パラメータに SQL 文の断片を送り込み、データベースに意図しない命令を実行させる攻撃手法。会員情報の一括取得、データの改ざん・削除、認証の迂回などにつながる。

本診断では、商品検索 API の検索キーワードが適切にエスケープされずに SQL 文へ組み込まれていることを確認した (WebAP-001)。対策として、プレースホルダ (バインド変数) を使った SQL 文の組み立てと、アプリケーションが利用する DB アカountの権限最小化を推奨する。

4.2 XSS (クロスサイトスクリプティング)

攻撃者が Web ページに悪意のあるスクリプトを埋め込み、そのページを閲覧したユーザーのブラウザ上で実行させる攻撃手法。セッション情報の窃取、画面の改ざん、フィッシングサイトへの誘導等が可能になる。

本診断では、商品検索画面において検索キーワードがエスケープされずに HTML に出力される反射型 XSS を確認した（WebAP-002）。対策として、出力時の HTML エスケープの徹底と、CSP ヘッダーによる多層防御を推奨する（WebAP-007 参照）。

4.3 パスワードリスト型攻撃（クレデンシャルスタッフィング）

他のサービスから流出した ID とパスワードの組み合わせリストを使い、対象サービスへのログインを自動的に試行する攻撃手法。多くのユーザーが複数のサービスで同じパスワードを使い回しているため、1 つのサービスで漏洩した認証情報が他のサービスでも有効となる可能性がある。

本診断においては、ログイン試行に対するアカウントロックやレート制限が設定されていないこと（WebAP-004）、多要素認証（MFA）が未実装であること（WebAP-005）、ログイン ID が URL から取得可能なこと（WebAP-006）が複合的に作用し、防御が不十分な状態にあると評価した（WebAP-C01）。

4.4 なりすましメール（メールスプーフィング）

送信者を偽装したメールを送信する攻撃手法。メールの送信元アドレスは容易に偽装可能であり、対策を講じていないドメインは、自社名を騙るフィッシングメールに悪用される可能性がある。

対策として、SPF（送信元 IP の検証）、DKIM（電子署名による検証）、DMARC（認証失敗時の処理方針指示）の 3 つのドメイン認証技術を段階的に導入する（NW-005 参照）。

4.5 リモートコード実行（RCE）

攻撃者がネットワーク経由で対象サーバー上の任意のプログラムを不正に実行する攻撃。サポート終了済みのソフトウェアに存在する既知の脆弱性を悪用することで成立する場合が多い。

本診断では、xxx.xxx.xxx.43 上でサポート終了済みのソフトウェアが複数稼働していることを検出している（NW-001）。サーバーの完全な乗っ取り、情報漏洩、他システムへの踏み台利用等の被害が想定される。

4.6 中間者攻撃（Man-in-the-Middle: MITM）

攻撃者が通信経路上に割り込み、通信内容の盗聴や改ざんを行う攻撃手法。公衆 Wi-Fi などの安全でないネットワーク上で特にリスクが高い。

TLS 通信が適切に設定されていない場合（NW-004, WebAP-008）、暗号化が不十分な状態で通信が行われ、盗聴のリスクがある。