

脆弱性診断

総合サマリー報告書

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. 診断全体概要

1.1 診断の目的

本診断は、株式会社サンプル商事（以下、貴社）が運営する Web アプリケーション（サンプルオーダー）および外部公開資産に対して、外部からの攻撃者の視点でセキュリティ上の弱点を調査し、具体的な改善策を提示することを目的とする。

1.2 診断範囲

項目	Web アプリケーション診断（WebAP 診断）	ネットワーク診断（NW 診断）
対象	サンプルオーダー（B2B-EC サイト）	外部公開資産 9 台
対象 URL/IP	https://stg.shop.example.jp/ （本番環境は診断対象外）	DMZ1 / DMZ2 / ISP 回線 3 セグメント
環境	ステージング環境（本番同等構成）	本番環境
診断方式	ブラックボックス（リモート）	グレイボックス（リモート）
診断期間	7 営業日	4 営業日
診断担当 / 品質レビュー	山田太郎 / 佐藤一郎	山田太郎 / 佐藤一郎

2. 総合評価

総合評価: 緊急（Critical）

本診断の結果、NW 診断と WebAP 診断を合わせて **合計 20 所見**（NW 診断 8 所見、WebAP 診断 11 所見 + 複合所見 1 件）の脆弱性・設定不備・推奨事項を検出した。

最も深刻な所見は、NW 診断で検出された **ロードバランサ（xxx.xxx.xxx.43）上のサポート終了済みソフトウェア**（Apache 2.2.31 / PHP 5.4.45、いずれもサポート終了から 8 年以上経過）である。リモートコード実行を含む多数の既知脆弱性が該当し、即時対応が必要である。この EOL ソフトウェア上では旧サービス「レガシーポータル」の移行案内ページ（NW-003）が現に稼働しており、NW-001 と NW-003 は不可分の一体問題として、当該ページの停止または基盤ソフトウェアの緊急更新を推奨する。

WebAP 診断では、商品検索 API に **SQL インジェクション**（WebAP-001、**高（High）**）を検出した。認証済みユーザーであればデータベース内の会員情報・注文情報を取得できる可能性があり、個人情報漏洩に直結するため即時の修正を推奨する。また、反射型クロスサイトスクリプティング（WebAP-002）など、入力値の検証・出力エスケープに関する所見が確認された。

さらに、アカウントロック・レート制限の欠如（WebAP-004）、多要素認証の未実装（WebAP-005）、ログイン ID の URL 露出（WebAP-006）が組み合わせることで、流出した ID・パスワードによる不正ログインを阻止する手段がない状態にある。この複合リスクを**高（High）**相当（WebAP-C01）として優先的な対応を推奨する。

一方、JWT の署名検証や価格改ざん防止など EC サイトにおいて重要な機能は適切に実装されており、ファイアウォール 3 台は全ポートが外部から遮断されていた。ただし、これらは本診断の範囲・手法・実施時点において確認できた事項であり、脆弱性が存在しないことを保証するものではない。

2.1 検出脆弱性の統計

深刻度	NW 診断	WebAP 診断	合計
緊急（Critical）	1	0	1
高（High）	2	2（うち複合所見 1）	4
中（Medium）	2	5	7
低（Low）	3	2	5
情報（Info）	0	3	3
合計	8	12	20

※ 深刻度の区分は CVSS v3.1 の基本値に基づく（別紙参照）。複合所見（WebAP-C01）は個別所見の重複カウントではなく、組み合わせにより生じる追加リスクの評価である。

3. クロス診断分析（横断的所見）

WebAP 診断と NW 診断の結果を横断的に分析し、単独の診断では把握しにくい複合的なリスクを特定した。

3.1 ソーシャルエンジニアリングの複合リスク（WebAP-003 + NW-005）

ソーシャルエンジニアリングとは、システムの弱点を直接攻撃するのではなく、「人」を騙して情報を得たり、不正な行動を起こさせたりする攻撃手法の総称である。今回のケースでは「なりすましメール」がこれに該当する。

リスクレベル: 高（High）（複合評価）

診断種別	所見	単独での評価
WebAP	WebAP-003: API レスポンスからの組織内部情報漏洩（営業担当者メール、営業所情報、権限構造）	中（Medium）
NW	NW-005: メール送信ドメイン認証の不備（example.net: DMARC 未設定、example.co.jp: p=none）	中（Medium）

複合的なリスク:

Web アプリケーションの API レスポンスには営業担当者のメールアドレス用フィールド（repEmail）や営業所メールアドレス（officeEmail）が含まれており、これらのドメイン（@example.net、@example.co.jp）を偽装したフィッシングメールが、送信ドメイン認証の不備により受信者に到達する可能性が高い。

想定される攻撃シナリオ:

- 攻撃者がサンプルオーダーに一般ユーザーとしてアカウントを作成、または既存の取引先アカウントの認証情報を入手してログイン
- ユーザー情報 API から営業担当者のメールアドレス・営業所情報を取得
- example.net ドメインは DMARC 未設定・SPF ソフトフェイルのため、偽装メールが受信サーバーに到達
- 営業所の実在する住所・電話番号を含むため、受信者が真正のメールと誤認する確率が高い

単独では Medium の 2 つの所見が組み合わさることで、ソーシャルエンジニアリングの実行可能性が「理論上」から「技術的に実行可能」に引き上げられる。

なお、本リスクの被害を受けるのは貴社のシステムではなく、貴社の取引先・顧客であると想定される。B2B 事業においては、取引先に貴社を騙った詐欺メールが届くことによる信用上の損害は、自社システムの停止に匹敵し得る。

対策の優先度: 両所見を同時に対策することで複合リスクを解消できる。

- API レスポンスから営業担当者情報を除外（WebAP 側）。営業担当者名・営業所連絡先を画面に表示している場合は、画面要件をご確認のうえ実施をお願いする
- メール送信ドメイン認証の強化（NW 側: DKIM 署名の導入、DMARC ポリシーの段階的強化）

DMARC の強化手順（NW 診断報告書 NW-005 に準拠）：

1. p=none のまま DMARC レポートの受信設定（rua）を行い、正規の送信元をすべて把握する
2. p=quarantine（隔離）へ移行し影響を監視する
3. p=reject（拒否）へ移行する

旧サービスドメイン example.net については、正規のメール送信がないことを確認のうえ p=reject を設定する（またはドメイン自体の廃止を検討する）。

3.2 TLS 設定の全社的な課題（NW-004 / WebAP-008）

TLS は、ブラウザとサーバーの間の通信を第三者に読まれないようにする仕組みである。今回の指摘は暗号がないということではなく、現在では安全と見なされない古い方式が「選べる状態のまま残っている」という事象である。

所見	対象	問題
NW-004	xxx.xxx.xxx.43, xxx.xxx.xxx.45（IP アドレス直接接続時）	TLS 1.0 / 1.1 有効、RC4・3DES 使用、Forward Secrecy 未対応（暗号強度 C）
WebAP-008	stg.shop.example.jp（= xxx.xxx.xxx.45。SNI 接続時）	Forward Secrecy 未対応、TLS 1.3 未有効化

複数のホスト・サービスにまたがって TLS 設定の不備が確認された。個別対応ではなく、全社的な TLS 設定ポリシーを策定し、一括で適用することを推奨する。

推奨 TLS ポリシー:

- TLS 1.2 以上のみ有効（TLS 1.0 / 1.1 を無効化）、TLS 1.3 を可能な限り有効化
- ECDHE 系暗号スイートを優先（Forward Secrecy 確保）
- RC4、3DES、および MD5/SHA-1 を用いる暗号スイートを無効化
- 適用は ①新しい暗号スイートを先に有効化 → ②接続性を確認 → ③旧プロトコル・旧暗号スイートを無効化、の順序で実施する（順序を誤ると通信断が発生する）

3.3 旧サービス「レガシーポータル」の残存（横断的課題）

旧サービス「レガシーポータル」に関連する構成要素が、2 つの診断・5 つの所見にまたがって確認された。当該サービスの現在の利用状況・残存理由は当社では把握できていないため、貴社にてご確認のうえ、対応方針のご検討をお願いする。

所見	残存箇所	深刻度
NW-003	xxx.xxx.xxx.43 上で example.net の移行案内ページが稼働中	中 (Medium)
NW-005	example.net ドメインの送信ドメイン認証が未整備 (DMARC 未設定)	中 (Medium)
NW-006	Cookie 名に旧サービスドメインが含まれる (LB-example.net)	低 (Low)
NW-007	xxx.xxx.xxx.43:443 の SSL 証明書 CN が www.example.net	低 (Low)
WebAP-003	API レスポンスに @example.net が格納されている	中 (Medium)

推奨対応: 旧サービスに関連する資産（稼働中サーバー、DNS レコード、SSL 証明書、Cookie 名、API レスポンス内のデータ、ドメイン契約）を棚卸しのうえ、不要と判断されたものは停止・整理されることを推奨する。

4. 推奨対応の全体優先度

NW 診断・WebAP 診断の全所見を統合し、対応の優先度を整理する。「優先度」は危険度の順位ではなく、いつまでに対応するかを目安である。深刻度（CVSS）に加えて、①対応期限の有無、②他所見との複合リスク、③対策の依存関係を勘案して決定している。

優先度 1: 即時対応（直ちに）

#	所見	診断種別	深刻度	対象
1	NW-001: EOL ソフトウェアの稼働	NW	緊急 (Critical)	xxx.xxx.xxx.43
1-2	NW-003: 旧サービス「レガシーポータル」の残存 (NW-001 と同時対応)	NW	中 (Medium)	xxx.xxx.xxx.43
2	WebAP-001: SQL インジェクション	WebAP	高 (High)	商品検索 API

優先度 2: 1 ヶ月以内（速やかに）

#	所見	診断種別	深刻度	対象
3	NW-002: 内部業務アプリの外部公開	NW	高 (High)	xxx.xxx.xxx.43
4	NW-004: TLS 設定の重大な不備	NW	高 (High)	xxx.xxx.xxx.43, .45
5	WebAP-002: クロスサイトスクリプティング (反射型)	WebAP	中 (Medium)	商品検索画面
6	WebAP-003: API レスポンスへの過剰なデータ公開	WebAP	中 (Medium)	ユーザー情報 API
6-2	NW-005: メール送信ドメイン認証の不備 (WebAP-003 と同時対応)	NW	中 (Medium)	example.net, example.co.jp
7	WebAP-004: アカウントロック・レート制限の欠如 (複合条件下では高 (High) 相当)	WebAP	中 (Medium)	ログイン API
7-2	WebAP-005: 多要素認証 (MFA) の未実装 (WebAP-004 と同時対応)	WebAP	情報 (Info)	ログイン認証
7-3	WebAP-006: URL パラメータへのユーザーID 含有 (WebAP-004 と同時対応)	WebAP	情報 (Info)	クーポン API
8	NW-007 のうち xxx.xxx.xxx.43:9443/:9444 の SSL 証明書更新 (有効期限まで約 2 週間)	NW	低 (Low) (期限あり)	xxx.xxx.xxx.43

優先度 3・4: 計画的に対応

優先度	該当所見
優先度 3 (3 ヶ月以内)	WebAP-007 (セキュリティヘッダー未設定)、WebAP-008 (TLS Forward Secrecy、NW-004 と同時対応)
優先度 4 (次回改修時)	NW-006 (サーバー情報の露出)、NW-007 (SSL 証明書の構成)、NW-008 (HTTP TRACE)、WebAP-009 (X-Powered-By 露出)、WebAP-010 (パスワードポリシー)
推奨事項 (参考情報)	WebAP-011 (security.txt の未設置)

5. 対策ロードマップ（推奨）

優先度テーブル（第 4 章）の順序に加え、対策の技術的依存関係を考慮して編成している。実際の実施スケジュールは貴社の開発・運用計画に合わせてご調整をお願いする。

Phase 1: 緊急対応（報告書受領後 2 週間以内）

- SQL インジェクションの修正（WebAP-001: プレースホルダ化と DB 権限の最小化）
- .43 ホスト上のサービスの利用状況確認と対応（NW-003 の移行案内ページ停止、NW-002 の外部公開遮断）
- EOL ソフトウェアの更新計画策定（NW-001）
- xxx.xxx.xxx.43:9443/:9444 の SSL 証明書更新

Phase 2: 短期対応（報告書受領後 1 ヶ月以内）

- 出力エスケープの徹底（WebAP-002）と API レスポンスの過剰データ除外（WebAP-003）
- ログイン API のレート制限実装（WebAP-004） + 多要素認証の導入検討（WebAP-005） + ログイン ID の URL からの除外（WebAP-006）
- TLS 設定の全社統一（NW-004, WebAP-008）とメール送信ドメイン認証の強化（NW-005）

Phase 3: 中期対応（報告書受領後 3 ヶ月以内）

- セキュリティヘッダーの一括設定（WebAP-007）
- .43 ホストのマイグレーション計画（NW-001）
- サーバー情報の露出対策・パスワードポリシーの見直し（NW-006, WebAP-009, WebAP-010）

Phase 4: 継続的改善

- 定期的な脆弱性診断の実施（年 1 回以上）と、対策完了後の再診断（優先度 1・2 の所見は対策完了後 3 ヶ月以内を推奨）
- 開発プロセスへのセキュリティテスト組み込み（SAST/DAST）、依存パッケージの脆弱性監視
- 旧サービス関連資産の棚卸しと整理、SSL 証明書・ドメインの有効期限監視の仕組み導入

6. 良好な点（ポジティブ所見）

本診断の範囲内において、以下のセキュリティ対策が適切に機能していることを確認した。これは「実際に攻撃を試みて防がれることを確認した項目」である。

ネットワーク

- ファイアウォール 3 台: 全ポートが外部から遮断されており、管理インターフェースや VPN 機能の外部露出なし
- DNS/メールサーバー: ゾーン転送拒否、BIND バージョン非公開、再帰問い合わせ拒否

Web アプリケーション

- JWT 署名検証: 署名アルゴリズムの厳密な検証。alg:none 攻撃・アルゴリズム混同攻撃をいずれも拒否
- 価格改ざん防止: サーバー側で商品マスタから正規価格を取得。クライアント側の金額パラメータは無視
- 認可制御: 他ユーザーの注文・カート情報へのアクセス (IDOR)、権限昇格はいずれも成立せず

※ 上記は本診断の範囲・手法・実施時点において確認できた事項であり、将来にわたる安全性を保証するものではない。

7. 報告書体系

本サマリー報告書は全体像の把握を目的とする。各所見の詳細（再現手順、技術的根拠、具体的な推奨対策）は個別報告書に記載している。

文書	内容	所見数
本書（総合サマリー報告書）	全体評価、クロス診断分析、優先度マトリクス	—
別紙: 診断対象・評価基準・用語集	診断対象一覧、CVSS スコア評価基準、用語集	—
NW 診断報告書	NW-001～NW-008 の詳細	8 所見
WebAP 診断報告書	WebAP-001～WebAP-011 + WebAP-C01 の詳細	12 所見

8. 免責事項

- 本診断は診断実施時点における評価であり、提供されたアクセス権限の範囲内で実施したものである。本報告書に記載のない脆弱性が存在しないことを保証するものではなく、誤検知・未検知の可能性を排除できない
- 本診断は一時点における評価であり、継続的なセキュリティ監視・保証を提供するものではない。定期的な再診断の実施を推奨する

- 推奨対策は一般的な技術的対処の方向性を示すものであり、採否・実施方法・実施時期の判断および実施に伴うシステムへの影響については、貴社の責任のもとで検証・判断をお願いする
- 本報告書は脆弱性情報を含むため、共有範囲を限定のうえ保管をお願いする。第三者に提供する場合は守秘義務を課したうえで必要最小限の範囲にとどめていただきたい

9. お問い合わせ窓口

本報告書の内容に関するご質問、対策実施に関するご相談は、以下までお問い合わせください。

項目	内容
会社名	株式会社セキュア DX
部門	セキュリティ事業部
担当者	山田太郎
メール	sample@example.com
Web サイト	https://www.secure-dx.co.jp/