

ネットワーク 脆弱性診断報告書

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. エグゼクティブサマリ

1.1 診断概要

項目	内容
案件名	サンプル商事様 ネットワーク脆弱性診断
診断対象	株式会社サンプル商事 本社 外部公開資産（9 台）
対象セグメント	DMZ1 / DMZ2 / ISP 回線
対象環境	本番環境
診断方式	グレーボックス（リモート診断）※1
診断期間	4 営業日（平日 21:00～翌 5:00 の業務時間外に実施）
使用ツール	Nessus Professional、Nmap、curl、nslookup / dig
除外事項	DoS（サービス妨害）試験、認証試行（ブルートフォース等）
診断担当 / 品質レビュー	山田太郎 / 佐藤一郎

※1 グレーボックス診断: 診断対象の IP アドレス・用途・ネットワーク構成等の情報を事前にご提供いただいたうえで、インターネット側からリモートで診断を実施する方式。

1.2 総合評価

総合評価: 緊急 (Critical)

本診断の結果、1 件の**緊急 (Critical)** 所見を含む合計 8 件の脆弱性・設定不備・推奨事項を検出した。

特に xxx.xxx.xxx.43（ロードバランサ）に所見が集中しており、サポート終了済みソフトウェア（Apache 2.2.31 / PHP 5.4.45）の稼働、内部業務アプリケーションの外部公開、TLS 設定の重大な不備など、即時対応が必要な問題が確認された。NW-001（EOL ソフトウェア）と NW-003（旧サービスの残存）は一体の問題であり、NW-003 の旧サービスを停止することで NW-001 の攻撃対象面を直接的に削減できるため、同時に対処する必要がある。

一方、ファイアウォール 3 台はいずれも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 機能の外部露出は確認されなかった。DNS/メールサーバー（xxx.xxx.xxx.12）も堅牢な設定であり、本診断の範囲においてネットワーク境界の防御は適切に機能していると評価する。

1.3 検出脆弱性の統計

深刻度	所見数
緊急 (Critical)	1
高 (High)	2
中 (Medium)	2
低 (Low)	3
情報 (Info)	0
合計	8

上記 8 件は、Nessus のスキャン結果（延べ 74 件）を中心に、同一原因による重複の集約および誤検知の排除を行い、手動検証の結果を加えて整理したものである。

1.4 推奨対応の優先度

優先度は深刻度（技術的な危険度）の順位ではなく、対応の緊急性・影響範囲・実現容易性を総合的に勘案した **対応時期の目安** である。

優先度	該当所見
優先度 1（即時対応）	NW-001、NW-003
優先度 2（1 ヶ月以内）	NW-002、NW-004、NW-005、NW-007（.43:9443/9444 証明書の有効期限まで約 2 週間）
優先度 4（次回改修時）	NW-006、NW-007、NW-008

2. 診断範囲と手法

2.1 診断対象一覧

#	IP アドレス	セグメント	ドメイン	用途
1	xxx.xxx.xxx.11	DMZ1	—	FW (プライマリ)
2	xxx.xxx.xxx.12	DMZ1	—	DNS / MAIL
3	xxx.xxx.xxx.13	DMZ1	—	FW (セカンダリ)
4	xxx.xxx.xxx.41	DMZ2	—	FW
5	xxx.xxx.xxx.42	DMZ2	stg.shop.example.jp	ロードバランサ (スレージング系)
6	xxx.xxx.xxx.43	DMZ2	www.example.ne.jp	ロードバランサ (LB 1 号機)
7	xxx.xxx.xxx.44	DMZ2	—	ロードバランサ (LB 2 号機)
8	xxx.xxx.xxx.45	DMZ2	www.shop.example.jp / stg.shop.example.jp	サンプルオーダー ※2
9	xxx.xxx.xxx.200	ISP 回線	—	サンプルオーダー インターネット

※2 同一 IP アドレス上で本番環境とスレージング環境が稼働している。本ホストは Web アプリケーション診断の対象でもあり、TLS 設定については NW-004 および WebAP-008 で異なる観点から報告している。

2.2 診断手法と使用ツール

フェーズ	手法	内容
Phase 1	ポートスキャン (Nmap 7.95)	全 9 台に対し、TCP 全ポート (1-65535) の SYN スキャン、サービスバージョン検出、OS 検出を実施。UDP は主要ポートに限定
Phase 2	脆弱性スキャン (Nessus Professional 10.9)	全 9 台に対し Advanced Scan を実施。DoS プラグイン無効、全ポート対象
Phase 3	手動検証 (curl、dig 等)	DNS 設定、SSL/TLS 設定、HTTP ヘッダー、HTTP TRACE メソッド、メール送信ドメイン認証 (SPF/DKIM/DMARC) の検証

本診断では第三者の Web サービス（外部診断サイト等）は使用していない。

3. 検出脆弱性の詳細

本章では主要な所見を深刻度の高い順に記載し、その他の所見は 3.6 に一覧で示す。章番号と所見 ID は一致しないため、以下に対応表を示す。

章番号	所見 ID	所見名	深刻度
3.1	NW-001	サポート終了済みソフトウェアの稼働	緊急 (Critical)
3.2	NW-002	内部業務アプリケーションの外部公開	高 (High)
3.3	NW-004	TLS 設定の重大な不備	高 (High)
3.4	NW-003	旧サービス「レガシーポータル」の残存	中 (Medium)
3.5	NW-005	メール送信ドメイン認証の不備	中 (Medium)
3.6	NW-006~NW-008	その他の所見（一覧）	低 (Low)

3.1 NW-001: サポート終了済みソフトウェアの稼働

項目	内容
深刻度	緊急 (Critical)
CVSS スコア	9.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE	CWE-1104 (Use of Unmaintained Third-Party Components)
検出箇所	xxx.xxx.xxx.43:443 (ロードバランサ配下の Web サーバー)

概要

対象ホストにおいて、サポートが終了して 8 年以上経過したソフトウェアが稼働していることを確認した。xxx.xxx.xxx.43 はロードバランサであり、本所見の Apache/PHP はその背後で稼働する Web サーバーの問題である。

- Apache httpd 2.2.31 (2015 年リリース、2017 年 7 月サポート終了)
- PHP 5.4.45 (2015 年リリース、2015 年 9 月サポート終了)

Nessus 脆弱性スキャンにより、本ホスト単体でこれらのソフトウェアに関連する **緊急 (Critical) 6 件、高 (High) 19 件、中 (Medium) 22 件** の既知脆弱性を確認した。リモートコード実行

(RCE)、メモリ内容の漏洩、サービス停止を含む深刻な脆弱性が含まれる。

主な既知脆弱性

CVE	概要	CVSS スコア
—	Apache HTTP Server 2.2.x サポート終了	10.0 (Nessus 独自評価)
CVE-2017-7679	Apache mod_mime バッファオーバーリード	9.8 (CVSS v3)
CVE-2017-9798	Apache Optionsbleed (メモリ内容の漏洩)	7.5 (CVSS v3)
CVE-2016-3074	PHP libgd 整数符号エラーによるメモリ破壊	9.8 (CVSS v3)

想定リスク

攻撃者がこれらの既知脆弱性を悪用し、サーバー上で任意のコードを実行する、メモリ上の機密情報を窃取する、またはサービスを停止させる可能性がある。本診断ではバージョンバナーからの判定であり、実際に悪用する検証（エクスプロイト）は実施していないが、サポート終了から長期間が経過しており、実際に悪用可能である蓋然性は極めて高い。

推奨対策

- 対象ソフトウェアを現行のサポート対象バージョンへアップデートする
- 当該サーバーで提供しているサービスの棚卸しを行い、不要なサービスは停止する（NW-003 の旧サービス停止により、本所見のリスクを低減できる）
- アップデートが困難な場合は、WAF 等による暫定的な防御策やアクセス元 IP アドレスの制限を検討する

参考情報

- CWE-1104: <https://cwe.mitre.org/data/definitions/1104.html>

3.2 NW-002: 内部業務アプリケーションの外部公開

項目	内容
深刻度	高 (High)
CVSS スコア	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CWE	CWE-923 (Improper Restriction of Communication Channel to Intended Endpoints)
検出箇所	xxx.xxx.xxx.43:9443 (勤怠管理システム)、xxx.xxx.xxx.43:9444 (ファイル共有システム)
備考	CVSS 評価は現状の 503 応答ではなく、メンテナンス解除時の想定に基づく

概要

内部業務用と思われるアプリケーションが、非標準ポートを通じてインターネットから到達可能な状態であることを確認した。現時点では 503 (メンテナンス中) 応答を返しているが、ポート自体は外部からアクセス可能であり、メンテナンス解除時にアプリケーションが直接外部公開される構成となっている。

想定リスク

メンテナンス解除時に、本来は社内限定であるはずの業務システムが外部から直接アクセスできる状態になり、不正ログインや業務情報の漏洩につながるおそれがある。現時点でも、メンテナンスページにシステム名称および部署名 (「情報システム部」) が表示されており、攻撃者にとってシステム構成を推測する手がかりとなる。

再現手順

確認内容	コマンド	結果
勤怠管理	<code>curl -sk https://xxx.xxx.xxx.43:9443/</code>	HTTP 503。「勤怠管理システムはメンテナンス中です。サンプル商事 情報システム部」を表示
ポート状態	<code>nmap -Pn -p 9443,9444 xxx.xxx.xxx.43</code>	いずれも open (対策後は filtered となることが期待される)

推奨対策

- 内部業務アプリケーションへのアクセスを VPN 経由に限定し、インターネットからの直接アクセスを遮断する
- ファイアウォールで当該ポート (9443, 9444) へのインバウンド通信を拒否する

- メンテナンスページからシステム名称・部署名を削除し、汎用的なメッセージに変更する

3.3 NW-004: TLS 設定の重大な不備

項目	内容
深刻度	高 (High)
CVSS スコア	7.4 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)
CWE	CWE-327 (Use of a Broken or Risky Cryptographic Algorithm)
検出箇所	xxx.xxx.xxx.43:443、:9443、:9444、xxx.xxx.xxx.45:443

概要

対象ホストの TLS 設定において、以下の重大な不備を確認した。

- TLS 1.0 / 1.1 が有効 (RFC 8996 により 2021 年に正式廃止、PCI DSS 不適合)
- RC4 暗号 (RFC 7465 で使用禁止)、3DES 暗号 (SWEET32 攻撃に脆弱) を使用する暗号スイートが有効
- Forward Secrecy 未対応、TLS 1.3 未対応
- 総合暗号強度: C (不合格)

.43 と .45 は同一のロードバランサ配下で同一の SSL 設定を共有していると推定される。なお .45 は、IP アドレス直接接続時 (本診断) とドメイン名接続時 (WebAP 診断: WebAP-008) で TLS ネゴシエーション結果が異なる。ロードバランサ側のバーチャルサーバー設定により TLS プロファイルが異なっている可能性がある。

想定リスク

中間者攻撃による HTTPS 通信の盗聴・改ざんのリスクがある。RC4 や SWEET32 等の既知攻撃手法により暗号化された通信が解読される可能性がある。

推奨対策

- TLS 1.0 / 1.1 を無効化し、TLS 1.2 以上のみを許可する (無効化前に古い端末・ブラウザからの接続有無を確認する)
- RC4、3DES を使用する暗号スイートを無効化し、ECDHE 等の Forward Secrecy 対応暗号スイートを優先する
- ロードバランサの全バーチャルサーバーの TLS プロファイルを確認のうえ変更する

参考情報

- IPA TLS 暗号設定ガイドライン: https://www.ipa.go.jp/security/crypto/guideline/ssl_crypto_config.html

3.4 NW-003: 旧サービス「レガシーポータル」の残存

項目	内容
深刻度	中 (Medium)
CVSS スコア	5.3 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CWE	CWE-459 (Incomplete Cleanup)
検出箇所	xxx.xxx.xxx.43:80, :443

概要

本所見は NW-001 (EOL ソフトウェア) と不可分の一体問題である。移行案内ページは静的コンテンツであるが、基盤となる Apache 2.2 (EOL) にはリモートコード実行を含む Critical 級の既知脆弱性が存在するため、コンテンツの内容にかかわらずサーバー侵害のリスクは同一である。

- ポート 80: 503 応答 (「レガシーポータルはメンテナンス中です」)
- ポート 443: <https://www.example.net/portal/> へリダイレクトされ、サンプルオーダー (後継サービス) への移行案内ページが表示される。SSL 証明書のドメイン不一致により、ブラウザに警告が表示される (NW-007 参照)

想定リスク

利用していないシステムを稼働させたままにしておくと、攻撃者が侵入を試みる入口が不必要に増える。特に古いソフトウェア (NW-001) と組み合わせることで、侵入のリスクが一段と高まる。旧サービスの停止は NW-001 の攻撃対象面を直接的に削減する対策となる。

推奨対策

- サービス終了済みのアプリケーションを停止し、関連するポート (80, 443) を閉鎖する
- example.net および www.example.net の今後の運用方針を確認する (不要であれば DNS レコードの削除・ドメインの整理、または DMARC p=reject の設定)
- www.example.net を停止する場合は、適切なリダイレクト先への 301 リダイレクト設定を検討する

3.5 NW-005: メール送信ドメイン認証の不備

注記: 本所見は、Web アプリケーション診断とのクロス分析により検出されたものである。DNS/MAIL サーバー（xxx.xxx.xxx.12）の設定検証の延長として、対象ドメインのメール送信ドメイン認証を調査した結果を報告する。

項目	内容
深刻度	中 (Medium)
CVSS スコア	4.7 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N)
CWE	CWE-290 (Authentication Bypass by Spoofing)
検出箇所	example.co.jp (主要ドメイン)、example.net (旧サービスドメイン)

概要

WebAP 診断での API レスポンスに含まれるメールアドレス情報の検出 (WebAP-003) を端緒として、DNS レコードを詳細調査した結果、メール送信ドメイン認証に以下の不備を確認した。

ドメイン	DMARC	DKIM	SPF
example.net (旧サービス)	未設定	未検出	~all (ソフトフェイル) のみ
example.co.jp (主要)	p=none (監視のみ)	未検出	設定あり

想定リスク

悪意ある第三者が貴社のドメインを騙ったメールを送信しても、受信側で偽物と判定されにくい状態になっている。取引先や顧客が、貴社を装ったフィッシングメールの被害に遭うおそれがある。WebAP-003 で検出された営業担当者情報と組み合わせることで、標的型フィッシングの実行可能性が高まる (総合サマリー報告書 3.1 参照)。

再現手順

確認内容	コマンド	結果
DMARC	<code>dig TXT _dmarc.example.co.jp / dig TXT _dmarc.example.net</code>	example.co.jp は p=none、example.net はレコードなし
DKIM	<code>dig TXT default._domainkey.example.co.jp</code>	既定セレクトアでは未検出

推奨対策

- example.co.jp: DMARC レポート (rua) を受信して正規の送信元を把握したうえで、p=none → p=quarantine → p=reject と段階的に移行する。DKIM 署名の導入を推奨する
- example.net: DMARC p=reject を設定し、ドメインの不正利用を防止する。NW-003 の旧サービスの運用方針と合わせて検討する

参考情報

- IPA なりすましメール対策: <https://www.ipa.go.jp/security/anshin/measures/mail.html>

3.6 その他の所見（一覧）

所見 ID	所見名	深刻度	検出箇所	概要と推奨対策
NW-006	サーバー・インフラ情報の露出	低 (Low)	xxx.xxx.xxx.43:443	Server / X-Powered-By ヘッダーでバージョンが露出、Cookie に Secure / HttpOnly なし。ServerTokens Prod、expose_php = Off、Cookie 属性の付与を推奨
NW-007	SSL 証明書のドメイン不一致・構成の問題	低 (Low)	xxx.xxx.xxx.43、.42	.43:443 の証明書 CN が旧サービス名義、.43:9443/9444 の証明書は約 2 週間後に期限切れ。証明書の棚卸しと期限までの更新、有効期限の自動監視を推奨
NW-008	HTTP TRACE メソッドの有効化	低 (Low)	xxx.xxx.xxx.43:443	TRACE メソッドが有効。現代のブラウザでは実害はほぼないが、TraceEnable Off の設定を推奨

4. ホスト別サマリ

ホスト	用途	緊急	高	中	低	所見 ID
xxx.xxx.xxx.43	ロードバランサ (LB 1 号機)	1	2	1	3	NW-001, 002, 003, 004, 006, 007, 008
xxx.xxx.xxx.45	サンプルオーダー	0	1	0	0	NW-004
xxx.xxx.xxx.42	ロードバランサ (STG)	0	0	0	1	NW-007
xxx.xxx.xxx.12	DNS/MAIL (DNS レコード)	0	0	1	0	NW-005

件数は各ホストに該当する所見の延べ数であり、合計は 1.3 の報告件数（8 件）と一致しない。

xxx.xxx.xxx.43 はロードバランサであり、外部からのアクセスはすべてこの機器を経由して背後のサーバー群に到達する。そのため本ホストの所見には、ロードバランサ自体の設定に起因するもの（NW-004、NW-007、NW-008）と、背後のサーバーに起因するもの（NW-001、NW-002、NW-003）の両方が含まれる。対策にあたっては両方の層での対応が必要となる。

5. 補足情報

5.1 診断の限界事項

- 本診断は外部（インターネット側）からのリモート診断であり、内部ネットワークからの診断は含まない
- 脆弱性の検出はバージョンバナーや設定情報に基づく判定であり、実際に悪用する検証（エクスプロイト）は実施していない
- 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おり、ファームウェアバージョンの特定は外部診断から不可能であった。ファームウェアの確認と既知脆弱性の評価は、管理者へのヒアリングまたは内部診断で実施することを推奨する
- 本報告書は診断期間・手法・アクセス権限の範囲内で検出された事項を報告するものであり、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い
- DoS 試験およびアプリケーション層の認証テストは、事前合意に基づき実施していない

5.2 今後の推奨事項

- 検出された脆弱性の修正後、再診断の実施を推奨する（優先度 1・2 の所見は対策完了後 3 ヶ月以内）
- xxx.xxx.xxx.43 で稼働しているサービスと旧サービス関連資産（ドメイン、DNS 設定、SSL 証明書）の棚卸しと、不要なものの停止・整理を推奨する
- 定期的な脆弱性診断（年 1 回以上）と、内部ネットワーク側からの診断の実施を推奨する

6. 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/

※ 用語集・CVSS スコアの評価基準は「別紙: 診断対象・評価基準・用語集」を参照。