



Forest Book

FOREST SECURITY WHITEPAPER

診断の後が本番

脆弱性を直し切るための是正管理テンプレート（チケット台帳・優先順位・再確認の記録）

発行 株式会社Forest Book（Forest Book Inc.）

株式会社Forest Book Forest Security

2026年10月22日 版 1.0

本資料の複製・社内配布は自由。再配布時は出典を明記のこと。

表紙情報

項目	内容
資料名	診断の後が本番 — 脆弱性を直し切るための是正管理テンプレート
発行	株式会社Forest Book（Forest Book Inc.）Forest Security
版	1.0（2026年10月22日）
想定読者	セキュリティ診断を受けた、または受ける予定の事業会社の情報システム担当者・開発責任者。受託開発会社のPM・テックリード
付属ファイル	是正台帳テンプレート（CSV、UTF-8 BOM付き。Excel・Googleスプレッドシートで開ける）
取扱い	自社内での複製・改変は自由。再配布時は出典を明記

本資料は、診断報告書を受け取った後に「誰が、何を、いつまでに直し、直ったことを誰がどう確かめたか」を記録するための様式と運用手順をまとめたものです。特定の診断事業者の報告書に依存しない形で書かれています。自社の既存の診断結果、ツールのスキャン結果、取引先から届いた指摘のいずれにも使えます。

なぜ診断の後で止まるのか

診断報告書は届く。読まれる。しかし3か月後に台帳を開くと、Highの指摘が「対応中」のまま残っている。多くの現場で起きていることです。原因は技術力の不足ではなく、是正を「仕事」として定義していないことにあります。

まず事実を確認します。IPAの「2024年度 中小企業における情報セキュリティ対策に関する実態調査」（Webアンケート4,191社、2024年10月～2025年1月）によると、不正アクセス被害を受けた企業（n=419）の手口は「脆弱性を悪用」が48.0%で最多でした。被害経験企業（n=975）の過去3期の被害額は平均73万円、平均復旧日数は5.8日。被害企業の約7割が取引先にも影響が及んだと回答しています（サービス停止・遅延36.1%、賠償負担32.4%、調査・復旧費用23.2%）。一方で、セキュリティ専門部署がある企業は9.3%にとどまります。

出典：IPA プレスリリース 2025-02-14 <https://www.ipa.go.jp/pressrelease/2024/press20250214.html>、2025-05-27 <https://www.ipa.go.jp/pressrelease/2025/press20250527.html>（いずれも2026-10-22確認）

同じくIPAの「情報セキュリティ10大脅威 2026」組織編では、「サプライチェーンや委託先を狙った攻撃」が2位で8年連続の選出、「システムの脆弱性を悪用した攻撃」が4位で9回目の選出です。脆弱性の悪用は、新しい脅威ではなく、毎年同じ場所にある脅威です。

出典：IPA 情報セキュリティ10大脅威 2026 <https://www.ipa.go.jp/security/10threats/10threats2026.html>（公開2026-01-29、2026-10-22確認）

法令の側にも期限があります。個人情報保護委員会の案内によれば、不正アクセスなど不正の目的によるおそれがある個人データの漏えい等は、件数にかかわらず委員会への報告対象です。速報は発覚から概ね3～5日以内、確報は30日以内（不正目的のおそれがある場合は60日以内）。また2026年7月に成立した改正個人情報保護法では、重大な違反に対する課徴金制度が導入されます（施行日は公布から2年以内で、本資料作成時点では未定）。

出典：個人情報保護委員会「漏えい等の対応とお役立ち資料」
<https://www.ppc.go.jp/personalinfo/legal/leakAction/>、「令和8年 改正個人情報保護法について」
<https://www.ppc.go.jp/personalinfo/legal/r8kaiseihogohou>（いずれも2026-10-22確認）

数字が示すのは、「診断で見つかった脆弱性を直し切らないこと」の費用が、診断そのものの費用より大きくなりうるという当たり前の事実です。それでも是正が止まるのは、次の4つが決まっていないからです。

決まっていないこと	現場で起きること
指摘ごとの担当者	「開発チーム」宛のまま、個人に割り当てられない
直す順番	報告書の並び順（重大度順）をそのまま着手順にし、簡単に直せるLowの前に設計変更が必要なHighで止まる
「直った」の定義	コードを変えたらクローズ。再現条件で確かめた記録がない
直さない判断の手続き	「今回は見送り」が口頭で決まり、半年後に誰も経緯を知らない

本資料の残りは、この4つを決めるための様式です。

是正管理の全体像

是正管理は、検出から報告までを一本の流れにしたものです。各段階に「入力」「出力」「責任者」を置きます。責任者はチームではなく個人名で書きます。

段階	入力	作業	出力	責任者（例）
検出	診断報告書、スキャン結果、取引先からの指摘、Dependabot等の通知	指摘IDを付けて台帳に登録する。1指摘1行	台帳の新規行（状態：未着手）	情シス担当
トリージ	台帳の新規行	誤検知・対象外・重複を除く。到達可能性（実際に使っている経路か）を確認する	状態：対応要／誤検知／対象外	開発責任者
優先順位	対応要の行	3軸で重大度を確認し、修正規模を加味して着手順を決める	着手順、着手予定月	開発責任者＋情シス担当
担当・期限	着手順	個人名の担当者と期限を決める。期限は重大度ごとの標準日数から始める	担当、期限	開発責任者
修正	担当、期限、推奨修正	チケットに沿って修正し、PRに指摘IDを書く	修正済みのコード・設定、PRのURL	担当者
再確認	PRのURL、再現条件	修正前に成立した再現条件が成立しないことを確かめる。確認した範囲を記録する	再確認記録（確認者、日付、範囲、方法）	修正者以外の人、または診断事業者
記録	再確認記録	台帳の状態を「再確認済み」にし、証拠の所在を書く	更新された台帳	情シス担当
報告	台帳	月次で残件・期限超過・解消件数を1ページにまとめる	月次要約	情シス担当

重要なのは、「修正」と「再確認」を別の人が行うことと、「再確認」が終わるまで状態を「完了」にしないことです。修正者が自分で「直した」と宣言してクローズする運用では、HMAC検証の修正がステージングにだけ入っていた、環境変数は消したがIaCのテンプレートに残っていた、といった取りこぼしが残ります。

優先順位の付け方

CVSSの数値だけで並べると、自社の構成では成立しない指摘が上位に来て、本当に危ない指摘が埋もれます。重大度は「攻撃の成立しやすさ」「影響を受ける資産」「業務影響」の3軸で判定し、各軸の根拠を1行ずつ台帳に書きます。

重大度	攻撃の成立しやすさ	影響を受ける資産	業務影響
Critical	認証なし・外部から容易に成立する	顧客の個人情報、ストアの管理権限、クラウドの管理権限	大量漏えい、他テナント（他ストア・他顧客）への波及
High	認証ありだが一般ユーザー権限で成立する。または認証なしで成立するが条件が限定的	同上	特定テナント・特定顧客のデータ漏えい、または改ざん
Medium	特定条件・内部者・別の脆弱性との組み合わせが必要	業務データ、設定情報	限定的な情報漏えい、改ざん、可用性低下
Low	成立条件が限定的で被害に至りにくい	公開情報、内部構成の一部	防御の多層性の欠如
Info	攻撃として成立しない	なし	推奨事項、将来の要件への準備

判定の手順は次のとおりです。

- 3軸それぞれの水準を決め、最も高い水準を基本の重大度とする
- 「攻撃の成立しやすさ」がLow以下で「影響を受ける資産」がCritical水準の場合、Highに留める（成立しにくいものをCriticalにしない）
- 既に別の防御（WAF、スロットリング、IAM条件）が実害を抑えていることをコードまたは設定で確認できた場合、1段階下げてよい。下げた理由を書く
- 複数の指摘を組み合わせると上位の影響に至る場合、個々の重大度は変えず、台帳の備考に「連鎖」として書く

重大度は「どれだけ危ないか」であり、「どの順で直すか」ではありません。着手順は重大度に修正規模を掛け合わせて決めます。目安は次のとおりです。

	修正規模 小 （数時間）	修正規模 中（数日）	修正規模 大（設計変更）
Critical	即日着手	即日着手。暫定対策（機能停止、WAFルール、権限剥奪）を先に入れる	暫定対策を即日。恒久対策は計画化
High	今週中	今月中	暫定対策を今週中。恒久対策は四半期内
Medium	今月中	四半期内	次の改修に同梱
Low	次の改修に同梱	次の改修に同梱	リスク受容を検討

判定例を6件示します。いずれも架空の構成です。

例	指摘の概要	成立しやすさ	影響資産	業務影響	判定	根拠の要点
1	Webhook受信エンドポイントがHMACを検証せず、任意のJSONを注文通知として保存する	認証なし・外部から容易 (Critical)	注文・顧客データ (Critical)	不正データの大量登録、全テナントに波及 (Critical)	Critical	URLが推測可能で、ペイロード内のストア識別子を信用して書き込む
2	HMAC検証をJSON.stringify(req.body)で行い、比較が===。検証自体は動いている	署名偽造には秘密が必要 (Low〜Medium)	注文・顧客データ (Critical)	検証が無効化された場合に例1と同じ (High)	High	現時点で偽造は成立しないが、正規通知の拒否が発生し、運用者が検証を外す誘因がある
3	セッショントークンの署名とexpは検証するがaudとdestを照合せず、リクエストのshopパラメータでデータを絞る	アプリを導入した別テナントの一般ユーザーで成立 (High)	他テナントの顧客データ (Critical)	他テナントへの波及 (Critical)	Critical	攻撃者は正規に導入するだけでよく、追加条件がない
4	Lambda実行ロールにdynamodb:*とResource: "*"。関数は1テーブルの読み書きのみ	単独では成立しない。コード実行やSSRFとの組み合わせで成立 (Medium)	全テーブル (Critical水準だが成立しにくい)	連鎖時に全データ (High)	Medium	「成立しにくいものをCriticalにしない」調整を適用。外部入力起点の別の脆弱性があればHighに上げる
5	Lambda環境変数に外部サービスのアクセストークンが平文。保存時暗号化はAWSマネージドキー	設定参照権限を持つ内部者またはCI (Medium)	管理権限相当のトークン (Critical水準)	当該テナントの全データ (High)	High	内部者・CI侵害時に即座にトークンが取れる
6	CloudWatch Logsに顧客のメールアドレスが出力され、保持期間が無期限	ログ閲覧権限を持つ内部者 (Medium)	氏名・メール等の個人情報 (High水準)	限定的な漏えい、アクセスログ・アクセス制限の根拠を損なう (Medium)	Medium	外部から到達できないためHigh以上にはしない。保持期間とマスクポリシーで対処

是正台帳テンプレート

台帳は1指摘1行です。スプレッドシートでもGitHub Projectsでも構いませんが、列は固定します。列を増やすのは自由、減らすのは不可です。付属のCSVがそのまま使えます。

列	定義	記入例
指摘ID	発見元を含む一意のID。診断事業者のIDがあればそれを使う	FB-SMPL-003
件名	観測した事実を1文で。「脆弱性がある」ではなく何がどうなっているか	注文作成Webhookの署名検証がJSON再シリアライズ後のボディで行われている
発見元	診断、スキャンツール名、取引先指摘、自社発見	第三者診断 (2026-11)
重大度	Critical/High/Medium/Low/Info	High

列	定義	記入例
攻撃の成立しやすさ	高／中／低と根拠	低（署名偽造には秘密が必要）
影響資産	何が影響を受けるか	注文・顧客データ
業務影響	放置した場合に起きること	検証無効化時に不正注文の登録
対象資産	エンドポイント、関数名、ロール名、ファイルパス	POST /webhooks/orders/create (src/webhooks/verify.ts)
環境	本番／ステージング／両方	両方（同一コード）
発見日	YYYY-MM-DD	2026-11-10
状態	未着手／対応中／修正済み（再確認待ち）／再確認済み／リスク受容／誤検知／対象外	修正済み（再確認待ち）
修正規模	小／中／大	小
修正担当	個人名	山田（開発）
期限	YYYY-MM-DD。重大度の標準日数から始め、合意で変える	2026-11-28
暫定対策	恒久対策前に入れた対策と日付。なければ「なし」	なし
修正PR／変更記録	PRのURL、変更セットID	github.com/org/app/pull/412
再確認日	YYYY-MM-DD	
再確認者	修正者以外の個人名、または診断事業者	
再確認範囲	何を、どの環境で、どう確かめたか	
関連要件	公式ドキュメント名、基準の要件番号	Shopify Webhooks HTTPS delivery、ASVS 5.0.0 9.1.1
備考	連鎖、調整理由、範囲の注記	他のWebhookルートも同じ関数を使用。個別確認は未実施

CSV形式（ヘッダー行と記入例2行。付属ファイル `remediation-register-template.csv` と同じ内容）：

指摘ID,件名,発見元,重大度,攻撃の成立しやすさ,影響資産,業務影響,対象資産,環境,発見日,状態,修正規模,修正担当,期限,暫定対策,修正PR/変更記録,再確認日,再確認者,再確認範囲,関連要件,備考
 FB-SMPL-001,注文作成Webhookの署名検証がJSON再シリアル化後のボディで行われ比較がタイミング安全でない,第三者診断（2026-11）,High,低（署名偽造には秘密が必要）,注文・顧客データ,検証無効化時に不正注文の登録,POST /webhooks/orders/create (src/webhooks/verify.ts),両方（同一コード）,2026-11-10,修正済み（再確認待ち）,小,山田（開発）,2026-11-28,なし,https://github.com/example/app/pull/412,,,,Shopify Webhooks HTTPS delivery; ASVS 5.0.0 9.1.1,他のWebhookルートも同じ関数を使用。個別確認は未実施
 FB-SMPL-004,Lambda実行ロールにdynamodb:*とResource:*が付与されている,第三者診断（2026-11）,Medium,低（単独では成立しない）,DynamoDB全テーブル,連鎖時に全データへ到達,arn:aws:iam::xxxx:role/app-api-role,本番,2026-11-11,対応中,中,佐藤（インフラ）,2026-12-15,なし,,,,Security Hub IAM.21,「成立しにくいものをCriticalにしない」調整を適用

運用の約束事は3つです。状態を「再確認済み」にできるのは再確認者だけ。期限を変えるときは備考に旧期限と理由を残す。「誤検知」「対象外」にするときは判断者名を備考に書く。

修正チケットの書き方

台帳は一覧用、チケットは作業用です。指摘1件につき1チケットを、開発チームが日常的に見ている場所（GitHub Issues、Jira等）に置きます。チケットに個人情報・秘密情報の値を書いてはいけません。リポジトリがパブリックなら公開Issueには貼らず、プライベートな手段で渡します。

タイトルは命令形にします。「HMAC検証に問題がある」ではなく「何をどう変えるか」を書くと、担当者が最初に読む1行で作業が分かります。

タイトル：**[Security][High]** 注文作成Webhookの署名検証を生ボディで行いタイミング安全な比較に変更する

指摘ID

FB-SMPL-001（技術報告書 版1.0、2026-11-14）

重大度

High（攻撃の成立しやすさ：低／影響資産：注文・顧客データ／業務影響：検証無効化時に不正注文の登録）

現状

`src/webhooks/verify.ts` 42行目で `JSON.stringify(req.body)` をHMACの入力にして

いる。比較は `===`。キーの順序や空白が異なる正規通知を拒否するため、再試行が繰り返されている。

影響

正規通知の取りこぼしが続き、運用者が検証を無効化する誘因になる。無効化されれば、任意のJSONが注文として登録される。

修正方針

- [] Webhookルートにのみ `express.raw({ type: 'application/json' })` を適用し、生ボディ（Buffer）を保持する
- [] `crypto.timingSafeEqual` でbase64デコード後のバッファを比較する。長さ不一致時はfalseを返す
- [] `X-Shopify-Webhook-Id` をDynamoDBに条件付き書き込みし、重複配信を無視する
- [] 空白位置を変えた同一JSON、改変ボディ、ヘッダーなしの3ケースで単体テストを追加する

参考

- Shopify「Subscribe to webhooks (HTTPS delivery)」 <https://shopify.dev/docs/apps/build/webhooks/subscribe/https>
- OWASP ASVS 5.0.0 9.1.1

完了条件

- [] 上記の作業がmainに取り込まれ、ステージングにデプロイされている
- [] ステージングで改変ボディのWebhookが401になることを確認した（確認者：修正者以外）
- [] 台帳の状態が「再確認済み」になっている

範囲の注記

本指摘は `/webhooks/orders/create` について確認した。同じ `verifyWebhook` を使う他のルートも同時に修正されるが、個別の動作確認は行っていない。

ラベルは `security`、`severity:high` のように重大度別に付けると、月次レビューで絞り込めます。PRの本文にも指摘IDを書く習慣をつけると、台帳とコードが双方向にたどれます。

再確認の記録様式

「直った」と言えるのは、修正前に成立していた再現条件が成立しなくなったことを、修正者以外の人が確かめたときです。コードレビューの承認は再確認ではありません。記録は次の様式で、台帳の「再確認範囲」列か、チケットのコメントに残します。

項目	記入内容	例
指摘ID		FB-SMPL-001
再確認日		2026-12-02
再確認者	修正者以外の個人名	鈴木（QA）
確認した環境	本番／ステージング、コミットハッシュまたはデプロイID	ステージング、コミット 3f9a2c1
確認方法	再現手順の再実行、コードの該当行の確認、設定のCLI出力のいずれか。複数可	改変ボディ・空白変更・ヘッダーなしの3ケースを送信し、改変とヘッダーなしが401、空白変更が200になることを確認
証拠の所在	HTTPログ、CLI出力、スクリーンショットの保存先	evidence/FB-SMPL-001/2026-12-02/
確認した範囲	何を確認し、何を確認していないか	<code>/webhooks/orders/create</code> のみ。他の3ルートは同一関数だが未確認
判定	再確認済み／未解消（差し戻し）／部分解消	再確認済み

「部分解消」は、たとえば本番とステージングで片方だけ修正が入っている場合に使います。状態は「修正済み（再確認待ち）」のままにし、残りの範囲を備考に書きます。

設定変更（IAMポリシー、ログ保持期間など）の再確認は、変更後のCLI出力を保存するだけで足ります。ただし、IaC（CDK、SAM、Terraform）で管理している環境では、手で直した設定が次のデプロイで戻ることがあります。IaCのテンプレート側も直っていることを、ファイルパスと行番号で確認してください。

月次レビューの進め方

月に1回、30分で台帳を見直します。参加者は開発責任者、情シス担当、必要なら経営者。議題は固定し、資料は台帳と1ページ要約だけにします。

時間	議題	決めること
0～5分	先月からの変化	新規検出の件数、解消件数、重大度別の残件数と前月比を読み上げる。議論はしない
5～15分	期限超過の指摘	1件ずつ、修正を続ける（新期限を決める）／リスク受容に回す／暫定対策を入れる、のいずれかを決める。保留にしない

時間	議題	決めること
15～22分	今月着手する指摘	担当者本人が着手月を宣言する。他の作業との優先順位の衝突はここで経営者が裁く
22～27分	判断待ち事項	「リスク受容してよいか」「追加予算が要るか」など、現場で決められないことを決裁者に問う。答えが出ないものは誰がいつまでに答えるかを決める
27～30分	次回までの宿題	台帳の更新担当と、次回日程を確認する

30分で終わらないときは、議題を増やすのではなく、台帳の状態列が最新でないことを疑ってください。会議の前に台帳が更新されていれば、議論は期限超過と判断待ちに集中できます。

「リスク受容」を決める基準と記録

すべての指摘を直す必要はありません。しかし「直さない」は、「誰も手をつけなかった」とは違います。リスク受容は、権限を持つ人が、根拠を書いて、期限付きで決めるものです。

受容を検討してよい条件は、次のすべてを満たす場合です。

- 重大度がMedium以下である。High以上は暫定対策なしに受容しない
- 攻撃の成立に、外部から到達できない条件（内部者、特定の権限、別の脆弱性）が必要である
- 修正の費用または副作用が、想定される影響に見合わない理由を具体的に書ける
- 代替の防御（監視、アクセス制限、保持期間の短縮）を入れているか、入れない理由を書ける

記録は次の様式です。台帳の状態を「リスク受容」にし、備考に記録の所在を書きます。

項目	記入内容
指摘ID・件名	
重大度と3軸の根拠	
受容する理由	修正しない技術的・業務的理由。「工数がない」だけでは不可
代替の防御	入れた対策、または入れない理由
受容の条件	この前提が崩れたら再評価する、という条件。例：当該機能を外部公開した場合、同じロールを別の関数を使い始めた場合
判断者	対象資産の責任を持つ役職者の個人名
判断日	
再評価日	判断日から6か月以内を推奨

再評価日が来たら、月次レビューの「判断待ち事項」に自動的に載せます。前提が変わっていなければ、同じ様式で再受容します。期限なしの受容は、「忘れた」と区別がつきません。

経営者・取引先への報告の仕方

経営者と取引先が知りたいのは、指摘の技術的な詳細ではなく、「今どれだけ残っていて、いつ片付くのか」「決めてほしいことは何か」です。月次の1ページ要約を次の様式で作ります。台帳から機械的に作れる内容

にしておく、毎月の作業が30分で済みます。

区画	内容	書き方
今月の要点	3行以内	「High 2件を解消。Critical 残0件。期限超過1件は12月のリリースで対応予定」のように、件数と時期だけを書く
重大度別の残件数	表。Critical／High／Medium／Low、前月比、期限超過	増減の理由は1行で
当月の解消	指摘ID、件名、再確認日、再確認者	「修正した」ではなく「再確認済み」の件数を書く
新たな検出	発見元、件数、重大度、着手予定	新しい診断・スキャン・依存パッケージの通知を含む
判断待ち事項	決裁者に求める判断と期限	「FB-SMPL-004 のリスク受容可否。12月15日までに回答を」
来月の予定	着手する指摘と担当	個人名
検査の範囲	この要約に基づく台帳の対象と、含まれていない資産	「対象はアプリAとAWSアカウント末尾1234。社内ツールBは含まない」

取引先に提出する場合は、指摘の件名と証拠（ファイルパス、コード断片）を外し、重大度別の件数、解消の推移、再確認の方法（誰が、どの環境で）、検査の範囲だけを渡します。取引先が本当に確認したいのは「是正の仕組みが回っているか」であり、個々の脆弱性の中身ではありません。中身を求められた場合は、NDAの範囲で技術報告書を別途開示します。

「指摘0件」を目標にしないでください。台帳が空になるのは、検出をやめたときです。健全な台帳は、新規検出が毎月少し入り、同じくらい解消され、High以上の滞留がない状態です。

Forest Securityについて

Forest Securityは、株式会社Forest Bookが提供する、Webサービス／ECの外部連携・カスタムアプリをAWSで運用する中小企業・開発会社向けのセキュリティ診断と是正管理のサービスです。Shopifyアプリ（公開・カスタム）とAWSサーバーレス（Lambda、API Gateway、DynamoDB、SQS、EventBridge、S3、Step Functions）の開発経験をもとに、ソースコードとクラウド設定の両方を確認し、直す順番を決め、直るまでの進捗を管理します。

本資料で示した台帳・チケット・再確認・月次レビューの運用は、Forest Security Careとして提供しています。Careは、ReviewまたはAssessment（診断）を完了した顧客に対し、最低6か月契約で次を行います。

運用項目	Care Lite	Care Standard
AWS設定の差分点検	月1回	月1回
依存パッケージ・既知脆弱性のレビュー	月1回	週1回の集計（リポジトリ2つまで）
GuardDuty等の検出結果レビュー	月1回	営業日ベースで週1回
確認済み高優先度事項の連絡	確認後2営業日以内	確認後1営業日以内
是正チケットの進捗管理	月1回更新	月1回更新＋優先案件は都度
月次報告書（本資料の1ページ要約に相当）	あり	あり
定例会議	四半期30分	月30分

運用項目	Care Lite	Care Standard
技術相談	なし	月60分まで

「確認済み」の起点は、ツールが検出した時刻ではなく、Forest Bookが内容を確認した時刻です。連絡期限は努力目標であり、契約上の扱いは個別に定めます。

Forest Securityがやらないこと：

- 24時間365日の監視、SOC、MDR、リアルタイム検知
- インシデント発生時の復旧作業、フォレンジック、監督官庁への届出代行
- 網羅的なペネトレーションテスト、負荷試験、ソーシャルエンジニアリング、物理セキュリティ
- Shopifyのプラットフォーム本体、決済代行会社、CDN、その他第三者が運営する資産への検査
- 脆弱性が存在しないことの保証、法令・認証への適合の保証、App Store審査の可否の保証
- 自社（Forest Book）が開発・修正した資産に対する、独立した第三者としての監査意見
- 無制限の修正実装（修正はスポット支援として時間単位で別途提供）

料金は対象資産の規模により個別に見積もります。相談は無料（30分）です。

問い合わせ先：株式会社Forest Book info@forest-book.jp

サービスサイト（予定）：<https://security.forest-book.jp>

〒220-0004 神奈川県横浜市西区北幸二丁目10番48号 むつみビル3階

出典

文書	URL	確認日
IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」速報（2025-02-14）	https://www.ipa.go.jp/pressrelease/2024/press20250214.html	2026-10-22
同 報告書プレスリリース（2025-05-27）	https://www.ipa.go.jp/pressrelease/2025/press20250527.html	2026-10-22
IPA「情報セキュリティ10大脅威 2026」	https://www.ipa.go.jp/security/10threats/10threats2026.html	2026-10-22
個人情報保護委員会「漏えい等の対応とお役立ち資料」	https://www.ppc.go.jp/personalinfo/legal/leakAction/	2026-10-22
個人情報保護委員会「令和8年 改正個人情報保護法について」	https://www.ppc.go.jp/personalinfo/legal/r8kaiseihogohou	2026-10-22
Shopify「Subscribe to webhooks (HTTPS delivery)」	https://shopify.dev/docs/apps/build/webhooks/subscribe/https	2026-10-22
Shopify「Set up session tokens」	https://shopify.dev/docs/apps/build/authentication-authorization/session-tokens/set-up-session-tokens	2026-10-22
AWS「Security best practices in IAM」	https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html	2026-10-22
AWS「Lambda environment variable encryption」	https://docs.aws.amazon.com/lambda/latest/dg/configuration-envvars-encryption.html	2026-10-22

文書	URL	確認日
AWS「CloudWatch Logs data protection」	https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/mask-sensitive-log-data.html	2026-10-22
OWASP ASVS 5.0.0（2025年5月）	https://github.com/OWASP/ASVS	2026-10-22

本資料の重大度基準は、Forest Securityの診断で用いている3軸基準と同じものです。CVSS v3.1／v4.0のベクトルは、顧客が求めた場合にのみ併記します。本資料の記載は2026年10月22日時点の公開情報に基づきます。