EC SECURITY / STORE OPERATIONS

CHEAT SHEET / 2026.10.25

futureshopのWeb担当者・経営者へ

不正アクセス・情報漏洩を防ぐ ECサイト対策チェックリスト

24 CHECKS

確認できたら✓ ／ 不明は空欄のまま確認する ／ 対象外は「—」　　点検日 _____　担当 _____

店舗で点検： 管理者ID・端末・顧客情報・独自コード。 **提供元に確認：** 基盤・決済の仕様、復旧範囲・条件。

01 管理者・権限を整理する　ADMIN

- ☐ 01 **管理者IDは一人ひとつにする**
  共用せず、本人の名前・メールで登録。制作会社にも専用アカウントを発行する。
- ☐ 02 **2段階認証を無効にしない**
  メール認証の一時無効設定を点検。SSO利用時は認証元の多要素認証を確認する。
- ☐ 03 **担当業務に必要な権限だけ渡す**
  管理者設定・顧客情報・CSV出力の権限を限定。制作担当に全権限を渡さない。
- ☐ 04 **退職・契約終了時にアクセスを止める**
  管理画面・メール・外部ツールの権限を解除。共有した接続情報も変更する。

02 管理画面への入口を守る　ACCESS

- ☐ 05 **パスワードと認証メールを守る**
  長い固有のパスワードを使い、メールにも多要素認証。認証コードは他人に渡さない。
- ☐ 06 **作業PCを更新し、偽メールに備える**
  OS・ブラウザーを更新し、保護機能を有効に。管理画面は保存済みのURLから開く。
- ☐ 07 **固定IP環境では接続元を制限する**
  接続許可IPアドレスを設定。在宅・委託先の接続と、締め出し時の対応も確認する。
- ☐ 08 **ログイン・管理者の操作履歴を見る**
  前回ログイン日時と管理者ログを点検。未知のIP・設定変更・CSV出力は調べる。

03 会員・顧客情報を守る　CUSTOMER DATA

- ☐ 09 **会員登録の認証・パスワードを確認**
  メールアドレス認証を有効に。会員パスワードは12桁以上・英数大小混在を推奨。
- ☐ 10 **顧客CSVの出力・保存を制限する**
  業務に必要な項目・期間だけ出力。会社管理の保存先に置き、閲覧者と削除日を決める。
- ☐ 11 **公開領域に顧客情報を置かない**
  FTP・サイトの公開領域に、受注CSV・顧客名簿・バックアップ等の非公開資料を置かない。
- ☐ 12 **顧客情報の共有先・範囲を限定する**
  委託先へ渡す情報は必要最小限に。宛先・添付を確認し、共有リンクは相手を限定する。

04 改ざん・外部連携を点検する　CODE & TOOLS

- ☐ 13 **測定タグは必要なページだけに**
  広告・解析・接客タグの提供元と用途を確認。不要なタグを停止し、編集権限も絞る。
- ☐ 14 **購入・会員画面の独自コードを点検**
  Webスキミング防止機能の対象を確認。不要なJavaScript・iframeを除き、動作確認する。
- ☐ 15 **API・FTPの接続情報を管理する**
  接続情報の共有先を記録し、不要な連携を停止。ファイル転送には暗号化されたFTPSを使う。
- ☐ 16 **WordPress・独自フォームも更新**
  別サーバーのCMS・プラグインも保守対象に。独自コードの修正・更新担当を決める。

05 決済・不正注文に備える　PAYMENT

- ☐ 17 **EMV 3Dセキュアの利用を確認する**
  SBPSは利用設定をONに。F-REGIは標準仕様。対象外となる取引も提供元へ確認する。
- ☐ 18 **不正検知の対象・判定を確認する**
  AI不正検知はSBPSのカード決済向け。対象外の取引を把握し、判定を見る担当を決める。
- ☐ 19 **疑わしい注文は出荷前に照会する**
  「照会推奨」や不自然な注文・配送先変更は、出荷を保留して決済会社の手順で確認。
- ☐ 20 **カード情報の受け取り・表示を点検**
  カード番号をメール等で集めない。3Dセキュアでの情報提供は「個人情報の取扱い」に反映。

06 経営者が運用・復旧を決める　MANAGEMENT

- ☐ 21 **責任者・点検日・対応期限を決める**
  社内・制作会社・提供元の担当範囲を明確に。未対応項目には担当者と期限を付ける。
- ☐ 22 **復旧用データと戻し方を確認する**
  デザイン・独自コードの変更前の版を安全に保管。提供元の復旧範囲・条件も確認する。
- ☐ 23 **公式通知を受け取り、対応する**
  futureshop・決済会社・連携先の案内を確認。担当交代時は通知先・受注メール先も更新。
- ☐ 24 **事故時の連絡先・判断者を決める**
  社内責任者・futureshop・制作会社・決済会社の窓口と、販売停止を判断する人を決める。

異変が起きたら、証拠を残して連絡する　FIRST RESPONSE

不正ログイン・改ざんの疑い　時刻・画面・ログを保全し、責任者・futureshopへ連絡。販売・決済の停止を判断。

端末感染・認証情報の流出　感染端末は通信を切る。安全な端末からパスワード変更・接続情報の失効を進める。

初期化・履歴削除をしない。制作会社・決済会社とも連携し、漏洩の影響と必要な報告・連絡を確認する。

参考：futureshop公式 対策ガイド・管理者設定・決済・セキュリティマニュアル／IPA

情報確認：2026.10.25 ｜ 契約・利用方式による違いは公式の最新案内を確認。

株式会社レイズ 制作
AI & CYBERSECURITY ｜ security.raise-co.net