外部共有版　2026年11月

Webシステム
セキュリティ対策実施報告書

既存Webシステムで見つかったアクセス制御と認証の問題に対応し、検証を経て本番環境へ反映した。対象は、データ取得、メッセージ・添付、管理機能、検索、パスワードの保護、ログイン時の追加認証。

アクセス制御と入力処理

公開データの取得	公開データ取得機能で扱うデータと返却項目を許可リストに限定した。必要な選択肢の取得は引き続き利用できる。
メッセージと添付	閲覧、返信、削除、添付取得の前に、操作する利用者が対象のやり取りに関与していることを確認する。添付の保存領域への直接アクセスを遮断した。
管理機能とデータ出力	管理画面、データ出力、取込などで、利用者の役割と対象データの閲覧範囲をサーバー側で確認する。
検索と絞り込み	検索条件をSQLの命令文と分けて渡す方式に変更した。ページ番号や取得件数を検証し、利用者に許可された検索範囲を適用する。
更新操作と画面表示	対象の更新操作にCSRF対策を追加し、一部の変更処理をPOSTに統一した。メッセージの件名や添付名は、ブラウザーがHTMLとして解釈しない形式で表示する。

実施範囲

初期調査で優先したアクセス制御・検索の改修に加え、ログインとアカウント復旧を強化した。本報告書は、改修箇所と反映時の検証記録をまとめたもの。継続確認の範囲は3ページ目に記載する。

認証とアカウント保護

パスワードの保管・再設定を見直し、管理者と機関アカウントにメールによる二段階認証を追加した。

パスワードの保存	新規登録・変更・取込時のパスワードをbcryptでハッシュ化して保存する。旧方式の保存データは、既存のパスワードでのログイン成功時に順次移行する。
パスワードの再設定	利用者と機関向けの再設定に、メールで届く有効期限付き・一度限りのリンクを使用する。リンクの確認に使うトークンはハッシュ化して保存する。新しいパスワードの確定までは現在のパスワードが有効。
試行回数の制限	連続したログイン失敗が一定回数に達すると、該当アカウントへの新規ログインを一時停止する。再設定の申請や認証コードの入力・再送にも回数制限を適用する。
セッションの保護	認証の進行に合わせてセッションIDを更新する。資格情報の変更を検知して以前のセッションを失効させ、代理操作では元の管理者の認証状態を確認する。

二段階認証の流れ

1. **IDとパスワードを確認**
   照合に成功すると認証待ちとなり、利用者の権限はコード確認後に付与する。
2. **メールで受け取った認証コードを入力**
   認証コードは有効期限付きで一度限り使用でき、保存時はハッシュ化する。機関アカウントにメールが未登録の場合は、入力した宛先の確認後に保存する。
3. **ログインを完了**
   新たに初期パスワードを発行した管理者は、メール認証後の初回ログインでパスワードを変更する。

管理者は個別アカウントで運用する。適用前からログインしていた利用者には再ログインが必要となる。

本番反映と検証結果

テスト環境と本番環境のデータベースを分離し、事前検証後に本番へ反映した。

検証段階	主な確認内容	記録上の結果
テスト環境	本番用の改修コードで、認証、メール登録、権限制御、既存機能への影響を確認。	200項目以上で成功
本番環境	試験用アカウントで、認証・再設定、権限外操作の拒否、既存機能を確認。	200項目以上で成功
公開画面	トップページ、各ログイン画面、認証画面の表示に必要なファイルのHTTPS応答を確認。	確認対象は正常応答
反映内容と後処理	配置ファイルとデータベースの定義を照合。メンテナンス解除と試験データの削除を確認。	照合・後処理完了

反映時の記録

本番データベースと対象ファイルのバックアップを取得した。適用中にデータベース更新処理が一時停止したため、処理を修正して再開した。反映後に配置内容とデータベースを照合し、メンテナンスを解除した。

検証の範囲と継続確認

認証メールの到達

試験用アカウントでメールの生成とコード認証を確認した。実際の利用者の受信箱への到達は、利用者の初回ログイン時に確認する。

対象外の経路と運用

今回の改修範囲外では、画面出力と更新操作の保護、添付アップロード、診断ファイル・エラー情報の公開範囲、CSVの安全性、実行環境・依存ライブラリの保守が継続確認事項となる。

作成根拠は、内部の初期診断、改修記録、本番反映記録、自動検証結果。試験結果は本番反映時点の対象範囲を示す。