Web セキュリティに対する Wagby の対応

2019年12月

株式会社ジャスミンソフト

よく知られているセキュリティの課題

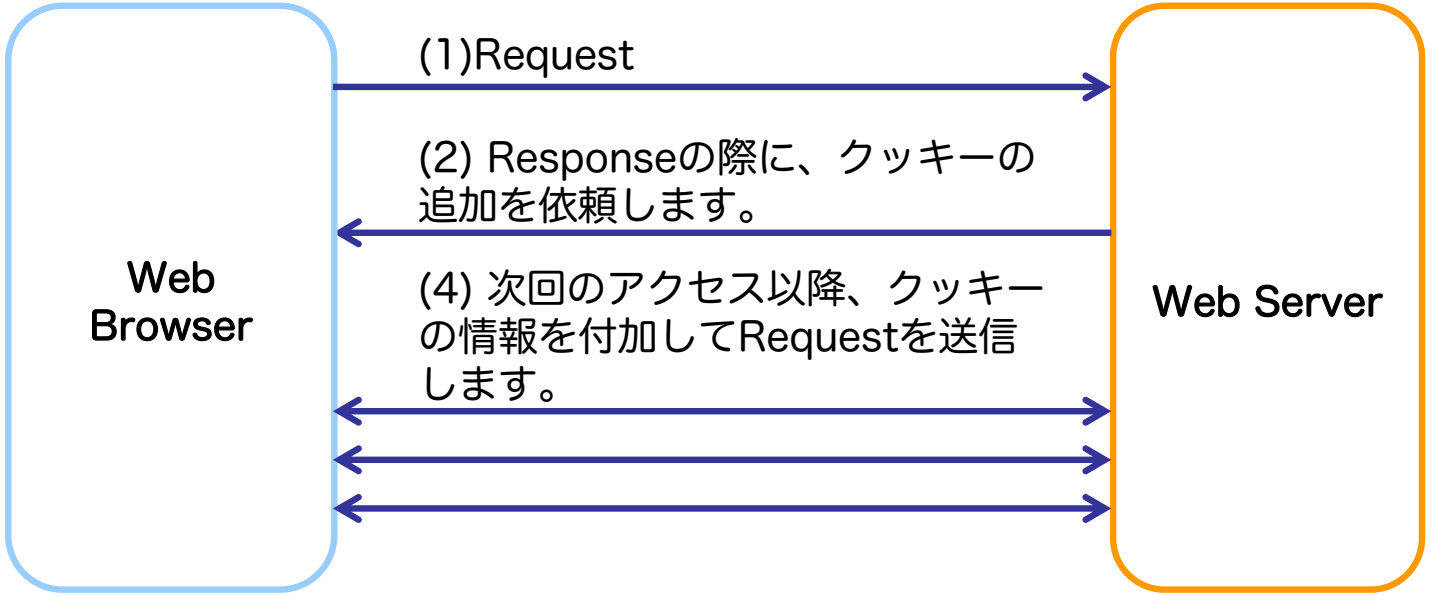
Wagby は次に示す既知の課題に対応しています。（新しい攻撃が発見された場合、その対応も行ってまいります。）

SQLインジェクション	クロスサイト・スクリプティング (XSS)	クロスサイト・リクエスト・フォージェリ (CSRF)	OSコマンド・インジェクション
ディレクトリ・リスティング	メールヘッダインジェクション	パストラバーサル	意図しないリダイレクト
HTTPヘッダ・インジェクション	認証	セッション管理の不備	アクセス制御の不備・欠落
クローラへの耐性			

詳細な説明

1. クッキーの取り扱い

クッキーはWebブラウザに一時的に少量の情報を保存する仕組みです。重要な情報（例：パスワード）を保存しないような運用ルールが求められています。

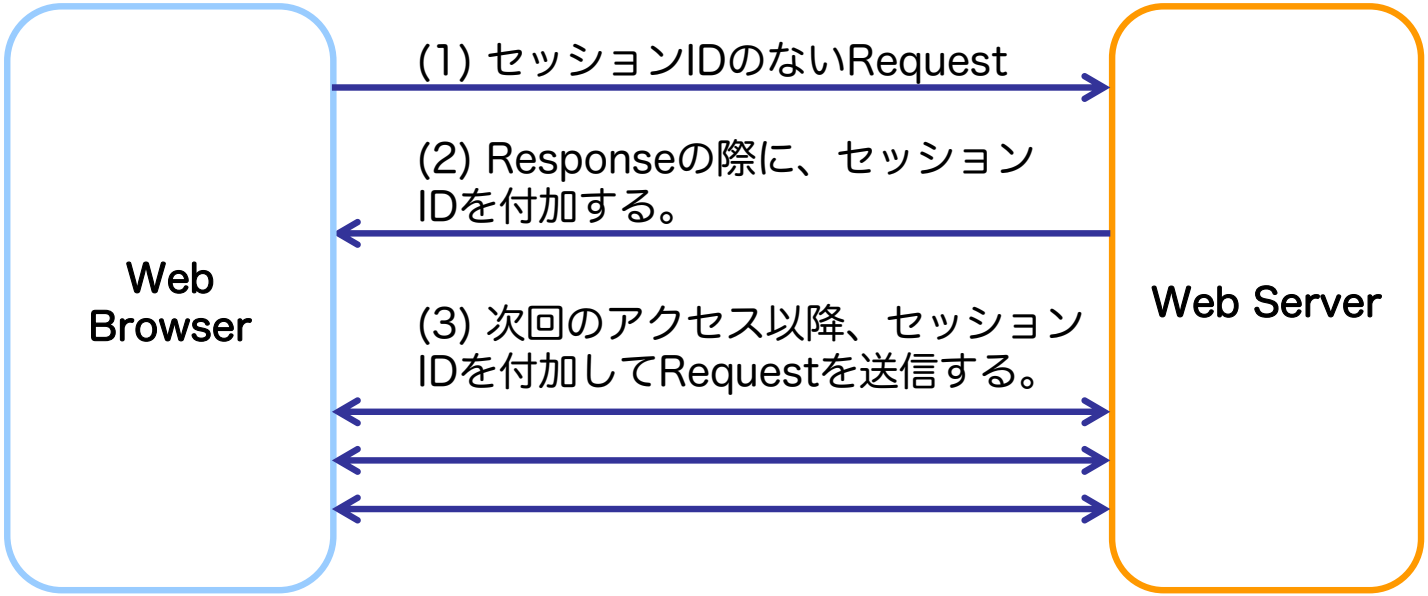


(3) ブラウザのクッキー領域に格納されます。

Wagby の対応：
(1)　クッキーは（後述する）セッションIDの管理に用いています。重要な情報は扱いません。
(2)　クッキーの有効期間を変更できます。業務要件にあった設定が行えます。

2. セッションの管理

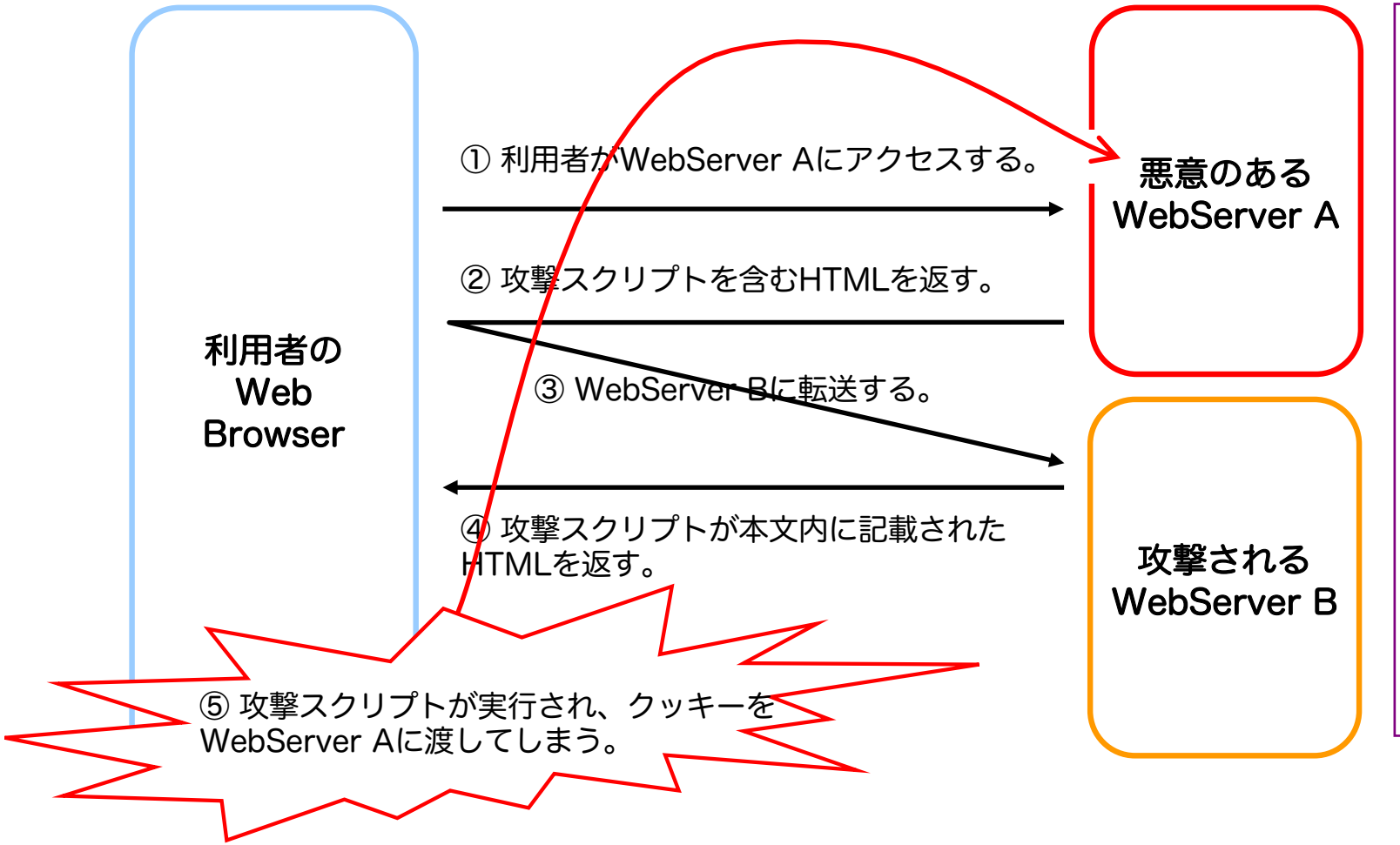
同一ユーザからのアクセスを判定させるために「セッション管理」を行います。
セッションIDの漏洩は、「なりすまし」攻撃につながります。



Wagby の対応：
(1) セッションIDはランダムな文字列とし、解析を困難としています。
(2) サーバ側での強制ログオフ機能（セッション無効化）を提供しています。（漏洩対策）。

3. クロスサイトスクリプティング脆弱性

クッキーを漏洩させる手段です。入力データ内に含まれるスクリプトを除去しない場合に発生します。これは作成したプログラムの欠陥となります。



Wagby では、自動生成されるすべてのファイルで、スクリプトの無効化（サニタイジング）を行っています。

ヒューマンエラーを除去できるため、高い信頼性を確保することができます。

4. SQLインジェクション脆弱性

開発者が意図しないSQLを生成させることで、データへの不正アクセスを行います。これも作成したプログラムの欠陥となります。

- 以下のようなSQL文を実行するWebシステムを設計しました。
  - SELECT * FROM CUSTOMER WHERE TYPE="public" AND BIKOU="{SEARCH_STR}"
  - {SEARCH_STR}はWebフォームから指定できる。
  - このSQL文を実行するページはTYPE列が”public”となっているデータしか見せないことが重要です。
- しかしSQLインジェクション脆弱性があった場合、Webフォームから以下のように入力することで、すべてのデータを閲覧できてしまいます！
  - 「" OR "A"="A」

Wagby の対応：
(1) 入力文字列を適切な型（数値、日付型）に変換したのちに使用するようになっています。
(2) 適切なサニタイジング処理を通し、機能制約なしでセキュリティを高めています。
(3) Prepared Statement 方式を併用し、JDBC レベルでもサニタイジングを行います。

5. OSコマンドインジェクション脆弱性

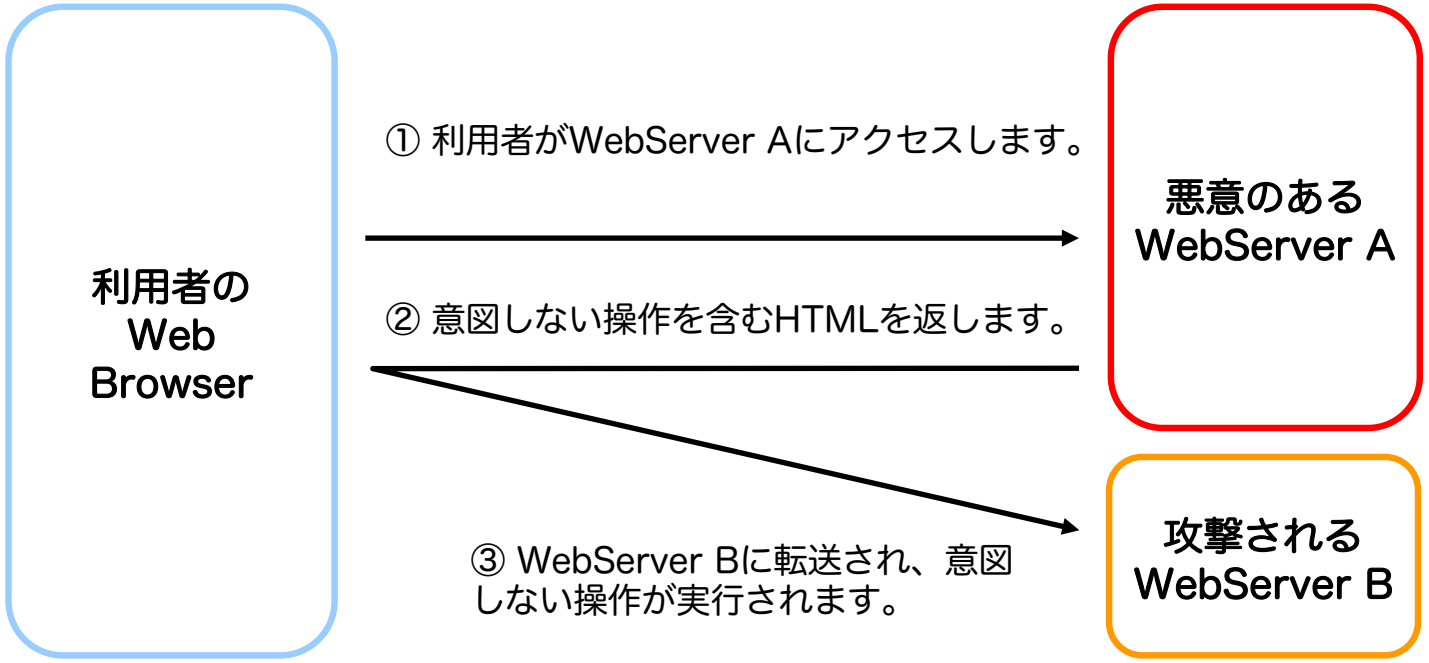
開発者が意図しないOSコマンドを実行させたり、非公開のファイルを閲覧できる脆弱性です。入力データへのチェックが甘いという欠陥になります。

- Webフォームでの入力をファイル名として扱い、オープンする場合、入力値をチェックしないと意図しないファイルをオープンされてしまいます。

Wagby の対応：
(1) ファイルアクセス時（ファイルのダウンロードや画像ファイルへのアクセスなど）において、不正なファイル名となっていないかどうかを常にチェックします。

6. クロスサイトリクエストフォージェリ脆弱性

悪意のあるWebサイトにより、利用者に別のWebサイトに対して意図しない操作を行わせる攻撃方法です。「CSRF」とも呼ばれています。



WebServer Bに利用者がログオンしている状態を狙って行われることが多いです。
例えば、ショッピングサイトにログオンしながら、別のサイトを閲覧している際に高額な商品の購入を決定するようなリンクを意図せずにクリックしてしまうといった攻撃が想定されます。

Wagby では、セッション IDを「ワンタイムトークン」として活用する仕組みを備えています。これによって、この攻撃を防いでいます。

7. ユーザ認証の扱い

Wagby は認証の基本となる「ユーザとパスワード」の扱いが充実しています。

Wagby の対応：

(1) ログオン認証に成功しなかった場合、すべての操作を認めません。
(2) 指定した回数、連続して認証を誤った場合、ユーザアカウントをロックします。
(3) パスワードの有効期限を個別に設定することができます。
(4) 過去と同じパスワードを設定することはできないような指定も行えます。
(5) パスワードは暗号化することもできます。システム管理者であっても、パスワードを読み取ることはできません。

8. すべての操作を記録する

Wagby は「誰が、いつ、どのデータを操作したか」という監査記録をすべて保存します。さかのぼってチェックすることもできます。

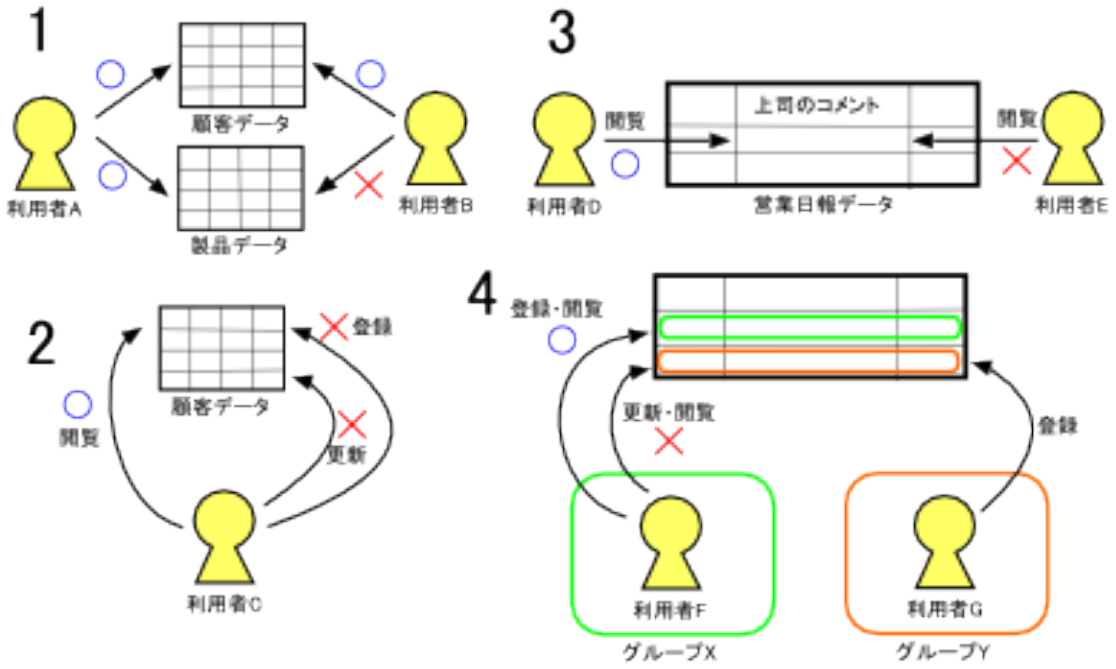
Wagby が記録する情報：

(1) 日付と時間
(2) メッセージタイプ（通常、エラー、警告）
(3) メッセージを発したクラス名
(4) メッセージを発したメソッド名
(5) ログオンアカウント
(6) IPアドレス
(7) 画面名
(8) イベント名
(9) 対象データの主キー

Wagby は操作ログに「どの項目の値が、何から、何に変わったか」まで記録することができます。

9. 充実した権限管理

Wagby はモデル単位、機能単位、項目単位、グループ単位といった、さまざまな視点での権限管理を設定できます。



(1) 利用者Aは顧客データと製品データを操作できるが、利用者Bは顧客データにアクセスできない。[データ種別毎の設定]

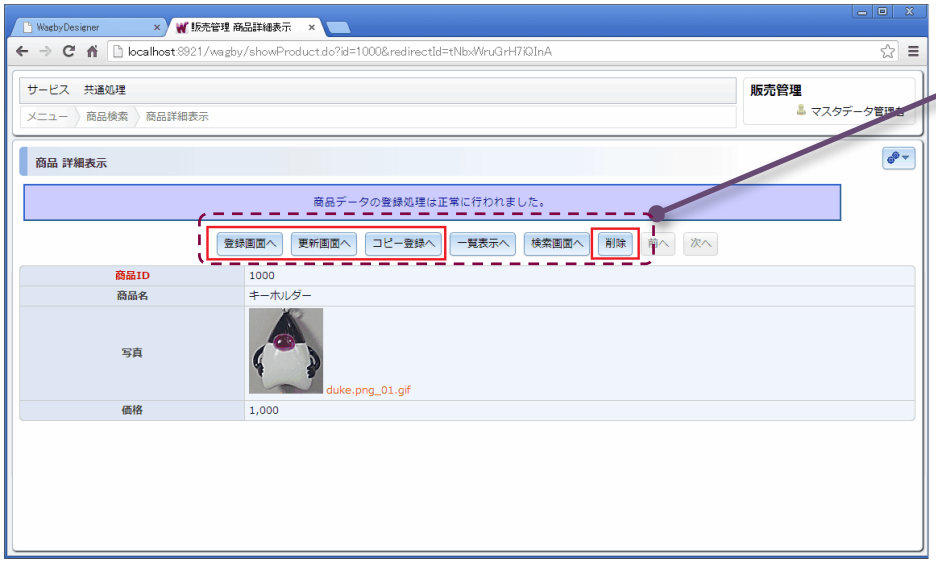
(2) 利用者Cは顧客データを閲覧できるが、登録と更新ができない。[機能毎の設定]

(3) 利用者Dは営業日報データをすべて閲覧できるが、利用者Eは同データの中の「上司のコメント」という欄を閲覧できない。[データ項目毎の設定]

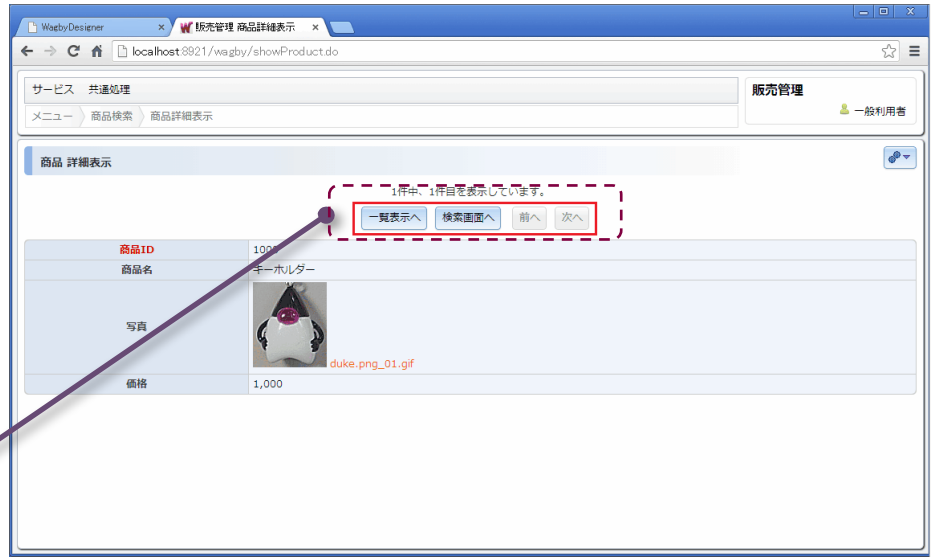
(4) 利用者Fはグループ X に所属しており、同グループが登録したデータは閲覧できる。他のグループが登録したデータは閲覧できない。[グループ毎の設定]

10. 「できることしか見せない」ポリシー

Wagby ではユーザアカウント毎にメニューや表示ボタンが変わります。
「できることしか見せない」ことで、操作エラーを事前に防止します。



このデータに関する更新権限と削除権限をもっているユーザの場合、操作ボタンが表示されます。



権限がないユーザでは、ボタンそのものが最初から表示されません。

不正な URL を入力して無理矢理、画面を開こうとした場合は「権限エラー」画面に遷移します。よって、不正アクセスを行うことはできません。

「Web セキュリティに対する Wagby の対応」
2019年12月 第1.0.3版
株式会社ジャスミンソフト