第 10 章　セキュリティ

この章では、Jira のセキュリティ設定に関する以下の内容について学びます。

- Jira の権限の階層について
- Jira の一般的なアクセス制御について
- 権限設定をきめ細かく管理する方法

第 8 章「ユーザー」にも関連する部分があります。必要に応じて第 8 章の内容も確認してください。

10. 1　Jira 権限の階層

Jira は階層で権限を管理します。各階層は、その 1 つ上の階層よりきめ細かく詳細に設定することができます。ユーザーがリソースへアクセスする場合、たとえば課題の閲覧では、（課題にすべて設定されている場合は）ユーザーは 3 つの権限の階層をすべて満たす必要があります。

表 10-1 権限の階層

権限の種類	説明	主な権限割り当て対象
グローバル権限	「誰がJiraにアクセスできるか」といったJira の全体的なアクセス権の制御を行います。	グループのみ
プロジェクト権限	プロジェクトレベルで権限の制御を行います。主に課題に対する操作を設定します。	アプリケーションロール プロジェクトロール
課題セキュリティ	各課題を閲覧できるユーザーを制御します。デフォルトの権限スキームでは利用できません。	プロジェクトロール 現在の担当者 課題の報告者 プロジェクトリーダー

権限の種類により主な割り当て対象が異なります。Jira グローバル権限はグループ以外に割り当てることはできません。これは Jira の仕様上の要求と制限によるものです。プロジェクトレベル権限はさまざまな対象に割り当てることができますが、主にアプリケーションロールまたはプロジェクトロールに対して割り当てることになるでしょう。課題レベルセキュリティは、ケースによって権限を割り当てる対象はまちまちです。

なお、Jira では課題に含まれるフィールドレベルでのセキュリティ制御（表示・非表示の設定など）はできませんのでご注意ください。