Sitecore CMS 6.1

セキュリティ リファレンス

CMS 管理者、アーキテクト、開発者のための概念の概要

目次

Chapter 1

イントロダクション

この文書では、Sitecore Web サイトに関連するセキュリティ インフラストラクチャのデザイン、実装、およびメンテナンスを行う際に CMS 管理者が知っておくべき概念について説明します。特に、ビジネス ニーズへの対応に必要なセキュリティ構造のデザインと実装に欠かせない機能と柔軟性をユーザーに提供するために Sitecore に用意されている、コンストラクトと定義機能を取り上げます。

この文書では、ドメイン、ユーザー、ロール、およびアクセス権という形でセキュリティを制御する方法を構造化する、Sitecore の構成要素について説明します。セキュリティの割り当てと制御を設定するシステム要素の目的と構造について説明します。ドメインや、ドメイン内のロールを設定する方法も紹介します。また、ユーザーとロールを構造化する方法と、セキュリティを個々のアイテムやフィールドに割り当てる方法も説明します。全範囲のセキュリティを一度に管理するセキュリティ プリセットの使用目的を定義します。この文書では、事前にインストールされているセキュリティ モデルのコンポーネント、セキュリティ インフラストラクチャの各部分を構成するデフォルト要素などについても説明します。

この文書には次の章があります:

- **Chapter 1 – イントロダクション**
  この文書の概要と、対象読者について説明します。
- **2.3 – ドメイン**
  Sitecore セキュリティ モデルにおけるドメインの使用方法について説明します。
- **2.5– ユーザー**
  Sitecore セキュリティ モデルにおけるユーザーの使用方法について説明します。
- **2.6 – ロール**
  Sitecore セキュリティ モデルにおけるロールの使用方法について説明します。
- **2.7 – アクセス権**
  Sitecore セキュリティ モデルにおけるアクセス権について説明します。

- **2.8 – セキュリティ プロバイダー**
  ASP.NET サービスと Sitecore データ ソースの間にインターフェースを作成するときに使用される、Microsoft セキュリティ プロバイダーについて説明します。

- **2.9 – セキュリティのプリセット**
  よく使用されるアクセス権をセキュリティ プリセットとしてグループ化する方法を説明します。

- **2.10 – アイテムとフィールド セキュリティ**
  Sitecore におけるアイテムとフィールド セキュリティの動作について説明します。

- **2.11 – ワークフロー セキュリティ**
  各種のワークフロー セキュリティ設定が、ワークフローのアイテムにどう影響するかを説明します。

Chapter 2

Sitecore セキュリティ モデル

この章では、Sitecore セキュリティ モデルを構成するコンポーネントと概念について詳細に説明します。この章では、Sitecore セキュリティ モデルを構成するすべてのコンポーネントと概念について、その機能と目的を詳細に説明します。

この章には次のセクションがあります:

- 機能
- 概要
- ドメイン
- ローカル管理ドメイン
- ユーザー
- ロール
- アクセス権
- セキュリティ プロバイダー
- セキュリティのプリセット
- アイテムとフィールド セキュリティ
- ワークフロー セキュリティ

2.1 機能

ドメインは、共通のルールと手順を持つ単位としてユーザーおよびロールをグループ化する代表的な方法です。ドメイン内には、一連のロールが定義されます。ロールを使用すると、たとえば特定の部署の全ユーザーに同じアクセス権を許可する場合など、構造化された単位にユーザーをグループ化できます。ロールの下にあるのがユーザーで、これは個人ユーザーがブラウザーベースの Sitecore クライアントにログインするとき使用する名前付きのアカウントです。

クライアントにログインしたユーザーまたはロール（合わせて「アカウント」と言う）には、アクセス権のセットをまとめて割り当てることができますが、これにはさまざまなアクションがあって、アイテムごとにアカウントに割り当てることができます。

ロールとユーザーに割り当てられる各種のアクセス権は、セキュリティのプリセットを使用して 1 クリックで割り当てることができます。その方法について説明します。

次に、セキュリティ プロバイダーの概念を紹介し、Sitecore で 3 つの Microsoft セキュリティ プロバイダーを使用して、Sitecore クライアントとセキュリティ データ ソースの間に構造化インターフェースを構築する方法を説明します。

アイテムとフィールド セキュリティを使用してアクセス権を個々のアイテムやフィールドに割り当てる方法も説明し、最後にワークフロー セキュリティを使用するときセキュリティがどのようにワークフローに影響するかを考えます。

2.2 概要

Sitecore セキュリティ モデルでは、コンテンツから機能まで Web サイトのほぼあらゆる要素について、管理者がアクセスを許可または拒否することができます。

2.2.1 .NET モデル

Sitecore で .NET セキュリティ エンジンを使用すると、いくつか直接的なメリットがあります。

.NET セキュリティ エンジンを使用するメリットは、次のとおりです:

- Sitecore CMS は標準的な ASP.NET のセキュリティ処理方法を採用しているため、Sitecore を Windows テクノロジと同調させることが可能
- Sitecore は直接 Microsoft のさまざまなプラグ アンド プレイ機能を利用可能
- 実際のデータ ソースからの抽象化
- デフォルトの設定をカスタム プロバイダーによって簡単に置換し、拡張できるオプション
- 純粋 ASP.NET ソリューションのパフォーマンス速度
- 同時に複数のプロバイダーを使用でき、アカウントを識別可能なストレージ領域に保持可能

2.2.2 アカウントとは何か

Sitecore では、ユーザーとロールをまとめて "アカウント" と呼びます。したがって、"アカウント" とはユーザーまたはロールのことです。

一般的な用語としても、システムを通じてセキュリティはユーザーやロールではなくアカウントに対して設定されるのが普通です。つまり、セキュリティを設定する際、システムはユーザーとロールを特に区別せず、すべてをアカウントとして扱うということです。

2.3 ドメイン

Sitecore のドメインは、共通のルールと手順を持つ単位として管理されるアカウントのグループです。

ドメインは、複数の論理関係を持つアカウントをまとめる際に使用されます。たとえば、Sitecore クライアントの使用権を持つアカウントをすべて Sitecore ドメインに格納することができ、公開された Web サイトへのアクセス権を持つアカウントはすべて Extranet ドメインに格納することができます。

2.3.1 デフォルト ドメイン

Sitecore には、次の 3 つのドメインがあらかじめ用意されています:

- **Built-in** – メモリーにのみ存在する仮想のドメイン。Sitecore CMS では、Extranet をデフォルト ドメインとして設定します。その場合 Web サイトにアクセスするときほとんどのアカウントは **extranet¥anonymous** になります。ただし、Web サイトでデフォルト ドメインが指定されていない場合、アカウントは **built-in¥anonymous** として登録されます。

- **Extranet** – Web サイト セキュリティのドメイン。イントラネット、エクストラネット、インターネットの Web サイトに公開された情報にアクセスできるユーザーを定義します。Sitecore の文書では、構築されるアプリケーションの内容にかかわらず、エクストラネット セキュリティと呼ばれるのが一般的です。

- **Sitecore** – 内部セキュリティのドメイン。Sitecore クライアントのセキュリティを処理します。サイトの構築と保持を行うコンテンツ エディター、管理者、デベロッパー、その他のメンバーに関する情報が格納されます。

2.4 ローカル管理ドメイン

ローカル管理ドメインとは、特定ドメインのユーザーがそのドメインしか参照できず、システム内の他のドメインは参照できないというドメインです。ローカル管理ドメインは通常ローカル管理者が管理し、ローカル管理者自身もシステム内の他のドメインを参照することができません。また、ローカル管理ドメインで定義されているユーザーは、そのユーザー自身のドメイン内で定義されているアカウントしか参照できません。こうすると、各ローカル管理ドメインは他のドメインを参照できないアカウントによって管理および使用されるため、1 つのインストール環境内から複数のサイトをサポートするプロセスが単純になります。

ローカル管理ドメインの概念は、Sitecore の "委任モデル" の一部です。委任モデルには、"グローバル表示ロール" や "管理ドメイン" などの追加機能があります。

2.4.1 グローバル表示ロール

どのドメインのユーザーも参照できるロールのリストです。

2.4.2 管理ドメイン

ユーザーに関連付けられるドメインのリストです。ユーザーは複数のドメインを参照できます。

ローカル管理ドメインのユーザーの場合、関連付けられた他のドメインを参照する権限を追加されます。

通常ドメイン (ローカル管理ではないドメイン) のユーザーは、デフォルトですべてのドメインを操作できます。このタイプのユーザーに 1 つまたは複数の管理ドメインを追加すると、ローカル管理ドメインか通常ドメインにかかわらず、その管理ドメインしか参照できないように制限されます。

2.4.3 ローカル管理者

ローカル管理者とは、ローカル管理ドメインか 1 つまたは複数の管理ドメインのアカウントのみを操作できるユーザーです。ローカル管理者は、Sitecore Local Administrators ロールのメンバーになり、ローカル管理ドメインのメンバーになる (あるいは 1 つまたは複数の管理ドメインを割り当てる) ことで定義します。

メモ
Sitecore のローカル管理者は、Sitecore にログインし、そのドメイン内のセキュリティ アプリケーション (セキュリティの割り当ても含む) を管理することができます。ローカル管理者が、ドメインを作成したり、管理ドメインをユーザーに割り当てたりすることはできません。

2.5 ユーザー

ユーザーは、個人が Sitecore クライアントにログインするとき使用する名前付きのアカウントです。Sitecore 6 には多くのデフォルト ユーザーが用意されており、それらのユーザーは変更しないようにしてください。

重要
この唯一の例外は "Admin" ユーザーです。システムのセキュリティを保護するために、"Admin" ユーザーのパスワードは必ず変更してください。パスワード変更は、システムで行うセキュリティ上の最初の変更です。

デフォルト ユーザーと同様の権限を持つユーザーが必要な場合には、デフォルト ユーザーのいずれかを編集するのではなく、新しいユーザーを作成することをお勧めします。デフォルト ユーザーを編集すると、セキュリティ モデルの他の部分に影響する可能性があるためです。

2.5.1 事前定義されているユーザー

事前定義されているデフォルト ユーザーは次のとおりです:

- **Built-in¥anonymous – built-in** ドメインを通じて Web サイトのアクセス自由な部分を表示するユーザーに割り当てられる仮想ユーザー。
- **built-in¥owner** – アイテムの現在の作成者 / 所有者のフィールドで参照されるユーザーを指す仮想ユーザー。
- **extranet¥anonymous** – Web サイトのアクセス自由な部分を表示するユーザー。
- **sitecore¥anonymous** – Web サイトのログイン画面にのみアクセスできるユーザー。これは、Web サイトのアプリケーション フレームワーク セクションへのアクセスを続行するユーザーに使用されます。
- **sitecore¥Admin** – 事前定義された "Administrator" CMS ユーザー。

2.5.2 ユーザー テンプレート

ユーザーの定義は、ユーザー テンプレートで作成されるアイテムから取得され、このテンプレートには次のフィールドがあります:

- **Administrator** – このフィールドを選択すると、ユーザーはセキュリティ設定にかかわらず、すべてにアクセスできます。
- **CanBoost** – 将来的に使用するために予約されています。
- **ClientLanguage** – Sitecore クライアントのユーザー インターフェースで使用される言語。
- **ContentLanguage** – Sitecore コンテンツのユーザー インターフェースで使用される言語。

- **DefaultItem** – デフォルトでコンテンツ エディターに表示されるアイテムを定義します。
- **Email** – ユーザーの電子メール アドレス。
- **Fullname** – ユーザーの氏名。
- **Password** – ユーザーのパスワード。"password" フィールド タイプとして格納されます。
- **Portrait** – Desktop の Sitecore メニューでユーザーを表すアイコンまたはイメージ。
- **RegionalIsoCode** – ユーザーが使用する地域の ISO コード。この設定で数字、通貨、日付と時刻の形式に影響を与えます。
- **Roles** – このユーザーに割り当てられるロール。
- **Start Url** – ユーザーがログインしたときのホーム ページで使用される URL。
- **Wallpaper** – Sitecore クライアントの壁紙。

2.6 ロール

ロールは、Web サイトの認証を管理するためにシステムで定義されます。ロールを使用すると、マネージャー、営業員、匿名ユーザーなどのような構造化された単位でユーザーをグループ化することができます。同じアクセス権を個々のユーザーにそれぞれ割り当てるのではなく、ロールを通じて複数のユーザーにセキュリティ アクセス権を割り当てることができるため、セキュリティ アクセスの編成が容易になります。ロールを使用すると、権限の変更やユーザーの追加と削除にも柔軟に対応でき、サイト全体を変更する必要はありません。

ユーザーは複数のロールに所属できるため、サイトの領域ごとに異なるアクセス権を付与できます。

複数のロールを割り当てられたユーザーは、割り当てられたすべてのロールのアクセス権を取得します。

ロールを他のロールに割り当てることも可能です。この機能を "ロール イン ロール" と言います。このトピックの詳細については、「2.6.3 ロール イン ロール」のセクションを参照してください。

2.6.1 事前定義されているロール

Sitecore には、一連のロールが事前定義されています。

Everyone ロール

Everyone ロールは、物理的なロールではなく仮想ロールです。Windows の "Everyone" コンストラクトを反映します。ロール データベースの一部としては存在せず、セキュリティの割り当てと解決のときにのみ使用されます。Everyone ロールを使用すると、ユーザー全員または特定ドメインのユーザー全員にアクセス権を割り当てることができます。Everyone ロールは、グローバル ロールとしても、ドメインごとのローカル ロールとしても使用することができます。

Sitecore¥Author

これは、"コンテンツ ロール" に該当します。コンテンツ ツリーのコンテンツにアクセスできるロールです (そのために "コンテンツ ロール" と呼ばれます)。このロールには、2 つの Sitecore Client ロールも割り当てられているため、ユーザーにこのロールを割り当てると、Sitecore Client Authoring ロールと Sitecore Client Users ロールが自動的に割り当てられることになります。

このロールで、メディア ライブラリーやコンテンツ エディターなどの基本的なアイテム編集機能を使用できますが、リボン上のタブ セットが一部制限されます。

Sitecore¥Designer

このロールでは、テンプレートの標準値を通じて個々のアイテムおよびアイテム グループのレイアウト詳細を変更するときに必要なコンテンツ ツリーの領域、あるいはページ エディターのデザイン ペインを設定するときに必要なアイテムに対して、読み取りと書き込みのアクセス権があります。このロールには、2 つの Sitecore Client ロールも割り当てられているため、ユーザーにこのロールを割り当

てると、Sitecore Client Designing ロールと Sitecore Client Users ロールが自動的に割り当てられることになります。sitecore¥Designer ロールは Author ロールおよび Authoring ロールのメンバーではない点にも注意してください。

このロールで、ページ エディターのデザイン ペインの機能と、コンテンツ エディターの [**プレゼンテーション**] タブにあるデザイナー オプションを使用し、各種のページ デザインを編集することができます。このロールでアイテムを実際に操作することはできません。

Sitecore¥Developer

このロールを割り当てられたユーザーはコンテンツ ツリー内のアイテムを操作できるため、このロールも "コンテンツ ロール" の 1 つです。このロールには、sitecore¥Author ロールと sitecore¥Designer ロールの両方のアクセス権があります。また、sitecore¥Sitecore Client Developing、sitecore¥Sitecore Client Maintaining、sitecore¥Sitecore Client Configuring の各ロールも追加されるため、通常の Sitecore デベロッパーが必要とするシステム領域のすべてにアクセスできることになります。

このロールでは、コンテンツ エディターのコンテンツ操作機能を使用できるほか、クライアント オーサーとクライアント デザイナーが通常使用するデザインおよびオーサリングのロールも付与されます。コンテンツ エディター上のリボンにあるその他の機能も使用でき、このロールを割り当てられたユーザーは開発の機能をすべて使用できます。このロールで、Sitecore メニュー上の [開発ツール] メニューにもアクセスできるため、パッケージ デザイナーなど他の開発ツールも使用できます。

Sitecore Client Authoring

これは、ユーザーが基本的なアイテム編集機能を使用できる "ユーザー インターフェース" ロールです。基本的なオーサリング機能を利用するためには、ほとんどのクライアント ユーザーにこのロールへのアクセス権が必要です。

Sitecore Client Designing

このロールで、ページ エディターのデザイン ペインの機能を使用でき、ユーザーは Sitecore クライアントのアイテムに関連付けられているレイアウト詳細を設定することができます。

Sitecore Client Securing

このロールでは、コンテンツ エディターなどの適切なアプリケーションを使用するアクセス権を、ユーザーが割り当てることができます。

Sitecore Client Account Managing

このロールでは、アクセス マネージャー、ドメイン マネージャー、ロール マネージャー、ユーザー マネージャーを使用してユーザーがドメイン、ロール、ユーザーを保持できます。

Sitecore Minimal Page Editor

このロールでは、Sitecore Client Authoring ロール (このロールを付与されるユーザーにも引き続き必要) で使用できる機能が制限されます。ページ エディターで使用できる機能も必要最小限に制限され、このロールを割り当てられたユーザーは [ページ エディター] リボンにアクセスできなくなります。

Sitecore Limited Page Editor

このロールでは、Sitecore Client Authoring ロール (このロールを付与されるユーザーにも引き続き必要) で使用できる機能が制限されますが、Sitecore Minimal Page Editor ロールよりはアクセス権が高くなります。このロールでは、エディターで使用できる機能が制限されます。ただし、Minimal Page Editor ロールとは異なり、このロールを割り当てられたユーザーには標準の [ページ エディター] リボンの簡略版が表示されます。

Sitecore Limited Content Editor

このロールでは、Sitecore Client Authoring ロール (このロールを付与されるユーザーにも引き続き必要) で使用できるコンテンツ エディター機能が制限されます。

このロールを割り当てられたコンテンツ オーサーは、[コンテンツ エディター] リボンの [**ホーム**]、[**レビュー**] および [**パブリッシュ**] の各タブしか使用できず、アイテムの右クリック メニューで表示されるコピー、移動、並べ替えの機能を使用できません。

2.6.2 ロール テンプレート

ロールの定義は、“ロール“ テンプレートで作成されるアイテムから取得され、このテンプレートには次のフィールドがあります。

- **Roles** – 定義されているロールのリスト。

2.6.3 ロール イン ロール

ロールは、他のロールのメンバーになる場合があります。ロールのメンバーであるユーザーは、そのロールがメンバーとして所属する他のロールのメンバーシップを自動的に継承します。ロール イン ロールは、Sitecore Author ロールや Designer ロールのように、複数のロールをユーザーに追加する必要がないため、よく使用されるロールをグループ化して管理する場合に便利です。

2.7 アクセス権

アクセス権は、使用可能なアクションのセットで、アカウントに対して、またはアイテムごとに割り当てることができます。アクセス権は、明示的に許可または拒否することもでき、親アイテムから継承される場合もあります。セキュリティ アクセス権は、個々のユーザーまたはロールに対して付与と拒否が可能です。

重要
管理を簡素化するために、アイテムは親からアクセス権を継承する場合があります。あるアイテムがアカウントまたはそのロールに対するアクセス権を指定していない場合に、親アイテムで定義されているアクセス権をそのアイテムに適用するかどうかは、アイテムのセキュリティ継承フラグによって制御されます。Sitecore では、アカウントまたはそのロールに対して定義されている権利が見つかるまで、または継承フラグが無効なことを確認するかデータ レポジトリのルートに達するまで、継承されたアクセス権が再帰的に評価されます。

重要
セキュリティ継承は、デフォルトで有効です。アイテムに対してセキュリティ継承を明示的に無効にしない限り、継承が許可されます。

重要
Sitecore では、最小許容のアプローチでアクセス権を決定します。あるアイテムがアカウントやそのロールに対するアクセス権を指定していない場合、デフォルトでそのアクセス権を拒否します。アクセス権のデフォルト値は拒否です。

重要
ユーザーのアクセス権がロールのアクセス権より優先されます。あるアイテムがユーザーに対して明示的にアクセス権を許可または拒否している場合、そのユーザーのロールのアクセス権は適用されません。ユーザーにアクセス権を明示的に付与すると、そのユーザーのロールでそのアクセス権が拒否されていても無視されます。

重要
2 つのロールでアクセス権が競合する場合は、常に拒否が許可より優先されます。ユーザーのいずれかのロールに対してアクセス権を拒否すると、他方のロールに対して許可されているアクセス権は無効になります。あるアイテムがユーザーに対してはアクセス権を指定していないが、そのアクセス権をユーザーのいずれかのロールに対して許可している場合に、他方のロールに対するアクセス権を拒否すると、このユーザーに対するアクセス権が拒否されます。

2.7.1 アクセス権

Sitecore には、次のように一連のアクセス権が事前定義されています:

- **読み取り** – アカウントのコンテンツ ツリーや公開された Web サイトにアイテムが表示されるかどうかを制御します。そのプロパティおよびフィールド値も含みます。

- **書き込み** – アカウントがフィールド値を更新できるかどうかを制御します。書き込みアクセス権には、読み取りアクセス権と、フィールドごとにフィールド読み取り/フィールド書き込みのアクセス権が必要です (フィールド読み取り/書き込みはデフォルトで許可されます)。

- **作成** – アカウントが子アイテムを作成できるかどうかを制御します。作成アクセス権には、読み取りアクセス権が必要です。
- **名前の変更** – アカウントがアイテムの名前を変更できるかどうかを制御します。名前の変更アクセス権には、読み取りアクセス権が必要です。
- **削除** – アカウントがアイテムを削除できるかどうかを制御します。削除アクセス権には、読み取りアクセス権が必要です。

  重要
  アカウントで 1 つまたは複数の子アイテムに対して削除アクセス権が拒否されている場合でも、[削除] コマンドを使用するとすべての子アイテムが削除されます。

- **管理** – アカウントがアイテムに対するアクセス権を設定できるかどうかを制御します。管理アクセス権には、読み取りアクセス権および書き込みアクセス権が必要です。
- **フィールド読み取り** – アカウントがアイテム上の特定のフィールドを読み取れるかどうかを制御します。
- **フィールド書き込み** – アカウントがアイテム上の特定のフィールドを更新できるかどうかを制御します。
- **言語読み取り** – ユーザーが特定言語バージョンのアイテムを読み取れるかどうかを制御します。
- **言語書き込み** – ユーザーが特定言語バージョンのアイテムを更新できるかどうかを制御します。
- **サイト アクセス** – ユーザーが特定のサイトにアクセスできるかどうかを制御します。
- **ワークフロー状態削除** – 特定のワークフロー状態に現在関連付けられているアイテムをユーザーが削除できるかどうかを制御します。
- **ワークフロー状態書き込み** – 特定のワークフロー状態に現在関連付けられているアイテムをユーザーが更新できるかどうかを制御します。
- **ワークフロー コマンド実行** – 特定のワークフロー コマンドがユーザーに表示されるかどうかを制御します。
- *— すべてのアクセス権を同時に制御します。特定のアイテムに割り当てられているアクセス権を、すべて一度に許可または拒否することができます。
- **継承** – セキュリティ権限を親アイテムから子アイテムに渡せるかどうかを制御します。セキュリティ モデルでは、アカウント単位で継承を選択できます (すべてのアクセス権に適用されます)。選択した継承設定は、選択したアカウントのみに適用されます。

2.7.2 アクセス権の設定

アクセス権ごとに、次の 3 つの設定が可能です:

- [**許可**] – 選択したアカウントに関連したアクセス権を明示的に許可します。
- [**拒否**] – 選択したアカウントに対して関連したアクセス権を明示的に拒否します。アクセス権の拒否は許可より優先されます。したがって、ユーザーやそのいずれかのロールが拒否された場合、あるいはユーザーやそのいずれかのロールにアクセス権がまったく許可されていない場合、ユーザーはアクセス権を拒否されます。
- [**継承**] – アクセス権を許可または拒否します。あるユーザーのアクセス権のステータスは、ユーザーに設定されている明示的なアクセス権の全体、当該のアイテムとコンテンツ ツリーで上位にあるアイテムについて割り当てられているロールなど、多くの要因に基づいて決定されます。

2.7.3 セキュリティ コンストラクト

セキュリティ モデルには、次の 3 つのセキュリティ コンストラクトもあります:

- [**セキュリティ継承**] – セキュリティ継承が無効な場合、ユーザーに付与される実効アクセス権は、ユーザーとそのユーザーに割り当てられたロールに指定されている設定によって決まります。セキュリティ継承が有効な場合、ユーザーに付与される実効アクセス権は、コンテンツ ツリーで上位にあるアイテムに指定されている設定によって決まります。
- [**実効アクセス権**] – ユーザーと、割り当てられているすべてのロール、セキュリティ継承、ワークフロー状態のセキュリティ、ロック、保護、アクセス権に動的に影響するその他の要因について設定を考慮してユーザーに割り当てられたアクセス権のセットです。
- [**フィールド セキュリティ**] – フィールド セキュリティを使用すると、インフォメーション アーキテクトは特定のフィールドに対するアクセス権を特定のアカウントに制限することができます。デフォルトでは、アイテムのどのフィールドもアイテムに適用されたセキュリティを反映します。つまり、ユーザーがアイテムに書き込み可能であれば、そのアイテムのフィールドはすべて書き込み可能です。フィールド セキュリティでは、アイテムに対して読み取り / 書き込みアクセス権を持つ特定のユーザーについて、そのアイテムの一部のフィールドへのアクセス権も制限できます。

2.8 セキュリティ プロバイダー

セキュリティ プロバイダーは、サービスとデータ ソースの間に構造化されたインターフェースを提供するセキュリティ指向のソフトウェア モジュールです。デバイス ドライバーが物理的なハードウェア デバイスを抽象化するのと同様に、セキュリティ プロバイダーは物理的なストレージ メディアを抽象化します。

ASP.NET の設定によって、情報は仮想的にどこにでも格納できます。必要なのは、その情報を読み出すカスタム プロバイダーだけです。

2.8.1 Sitecore のセキュリティ プロバイダー

Sitecore CMS 6 は、3 つの Microsoft セキュリティ プロバイダーを使用します。

- **メンバーシップ プロバイダー** – ASP.NET のメンバーシップ サービスと、Sitecore のメンバーシップ データ ソースの間にインターフェースを提供します。メンバーシップ プロバイダーには、登録されたユーザーに関するデータを含む Sitecore Security データ ソースとの間のインターフェース、ユーザーを作成および削除するメソッドの提供、ログイン資格情報の検証、パスワードの変更、メンバーシップ情報の格納と読み出しなどの機能があります。

- **ロール プロバイダー** – ASP.NET のロール管理サービスと、Sitecore のロール データ ソースの間にインターフェースを提供します。ロール プロバイダーには、ユーザーをロールにマッピングするロール データなどのデータ ソースとのインターフェース、ロールを作成するメソッドの提供、ロールの削除、ユーザーのロールへの追加などの機能があります。ユーザー名を指定すると、ロール マネージャーはロール プロバイダーを利用して、そのユーザーが所属するロール (1 つまたは複数) を特定します。

- **プロファイル プロバイダー** – ASP.NET のプロファイル サービスと、Sitecore のプロファイル データ ソースの間にインターフェースを提供します。プロファイル プロバイダーには、ASP.NET で提供されるプロファイル プロパティ値を Sitecore のプロファイル データ ソースに書き込む機能と、ASP.NET から要求されたときデータ ソースからプロパティ値を読み戻す機能があります。また、プロファイル データ ソースの管理をコンシューマーに許可する (たとえば特定の日付以降アクセスされていないプロファイルを削除する) 方法も実装します。

2.9 セキュリティのプリセット

セキュリティのプリセットは、よく使用されるセキュリティ アクセス権を 1 クリックでまとめて設定できる機能です。セキュリティのプリセットは、`sitecore/System/Settings/Security/Presets` で作成および格納することができます。

プリセットを設定すると、1 つのプリセットにアカウントをまとめ、それぞれに独自の設定が可能です。プリセットは、コンテンツ エディターの [**セキュリティ**] タブ、[**プリセット**] グループから適用することができます。

2.9.1 事前定義されているセキュリティのプリセット

Sitecore クライアントには、2 つのセキュリティのプリセットが事前定義されています:

- [**継承の削除**] – このプリセットは、'*' (Everyone) ロールに対して継承アクセス権を [拒否] に設定します。したがって、アイテムは親アイテムからセキュリティ権限を継承しなくなります。
- [**ログインが必要**] – このプリセットは、extranet/Anonymous ユーザーに対して読み取りアクセス権を [拒否] に設定します。したがって、エクストラネット ログインではアイテムとその子へのアクセス権が必要になります。

2.9.2 セキュリティ プリセット テンプレート

セキュリティのプリセット定義は、"セキュリティのプリセット" テンプレートで作成されるアイテムから取得され、このテンプレートには次のフィールドがあります:

- **Users** – プリセットを割り当てられるユーザーのリスト。
- **Domain** – プリセット / ユーザーの組み合わせが適用されるドメイン。
- **Security Preset** – セキュリティのプリセット。
- **Overwrite** – プリセットが、アイテムに対する以前の割り当てを完全に上書きするかどうかを制御します。

2.10 アイテムとフィールド セキュリティ

Sitecore セキュリティ モデルでは、各アイテムに個別の割り当てが可能です。アクセス権は、許可されている場合には再帰的に継承されます。フィールド セキュリティを使用すると、インフォメーション アーキテクトは特定のフィールドに対するアクセス権を特定のユーザーおよびロールに制限することができます。

デフォルトでは、アイテムのどのフィールドもアイテムに適用されたセキュリティを反映します。つまり、ユーザーがアイテムに書き込み可能であれば、そのアイテムのフィールドはすべて書き込み可能です。ただし、フィールド セキュリティでは、アイテムに対して読み取り/書き込みアクセス権を持つ特定のユーザーについて、そのアイテムの一部のフィールドへのアクセス権も制限できます。

セキュリティ設定をフィールド レベルで割り当てることもできます。たとえばデベロッパーは、特定のフィールドに対する読み取り / 書き込みアクセス権を持つように 1 つのロールを設定し、別のロールには読み取りアクセス権のみを設定し、3 つ目のロールにはどちらのアクセス権も設定しない、などが可能です。

個々のフィールドに対するセキュリティ設定は、各フィールドの [セキュリティ] セクションにある [フィールド セキュリティ] コントロールで行います。

2.10.1 標準テンプレートのフィールド セキュリティ

デフォルトでは、すべてのアイテムが Sitecore 標準テンプレートからセキュリティ設定を継承します。

標準テンプレートの特定のフィールドに対するセキュリティ設定を変更すると、標準テンプレートのフィールドに対する読み取り / 書き込みアクセス権を、ロールやユーザーごとに付与または拒否できます。

メモ
Everyone ロールでは、標準テンプレートのほとんどのフィールドに対するアクセスが拒否されています。つまり、これらのフィールドは管理者ユーザーしか参照できないということです。保護されているフィールドを管理者以外のユーザーにも表示する場合には、まず読み取りアクセス権が Everyone ロールにも継承されるように設定する必要があります。特定のフィールドを表示できるようにしたいロールやユーザーに、読み取りアクセス権が許可されるように設定します。フィールドを変更可能にするロールとユーザーには、書き込みアクセス権を許可してください。

重要
標準テンプレートは変更しないことを強くお勧めします。標準テンプレートはシステム間で継承されるため、変更するとアップグレード時のプロセスが複雑になり、その他の問題の原因にもなるからです。

2.11 ワークフロー セキュリティ

ワークフロー状態に関するセキュリティ設定は、ワークフローのアイテムについてユーザーが実行できるアクションに影響します。また、ワークボックスでユーザーに表示されるワークフロー コマンドもこの設定によって制御されます。

2.11.1 ワークフロー アイテムとコマンドのアクセス権

ワークフロー アイテムには、次のアクセス権を割り当てることができます:

- **ワークフロー状態削除** – 特定のワークフロー状態に現在関連付けられているアイテムをユーザーが削除できるかどうかを制御します。
- **ワークフロー状態書き込み** – 特定のワークフロー状態に現在関連付けられているアイテムをユーザーが更新できるかどうかを制御します。

ワークフロー コマンドには、次のアクセス権を割り当てることができます:

- **ワークフロー コマンド実行** – 特定のワークフロー コマンドがユーザーに表示されるかどうかを制御します。

2.11.2 解決済みワークフローのアクセス権

解決済みワークフローのアクセス権を、個々のアイテムに設定できます。解決済みアイテムには、次のアクセス権があります:

- **読み取り** – コンテンツ エディター、公開された Web サイト、その他でのアイテム表示には、そのアイテムに対する読み取りアクセス権が必要です。
- **書き込み** – ワークボックスでのアイテム表示には、そのアイテムに対する書き込みアクセス権が必要です。アイテムが他のユーザーによって現在チェック アウト (ロック) されている場合には、そのアイテムに対する書き込みアクセス権がないことがあります。