CHAPTER 7

XML の脅威防御

この章では、Cisco ACE Web Application Firewall の XML 検証および脅威防御機能について説明します。内容は次のとおりです。

XML の脅威防御について

ACE Web Application Firewall には、Cisco ACE XML Gateway 製品の高度な XML および Web Service セキュリティならびに統合機能は備わっていませんが、XML の脅威を防御する機能が搭載されています。XML の脅威防御機能では、XML Denial-of-Service（XDoS; XML サービス拒絶）攻撃などの XML ベースの攻撃を識別し、防御します。

脅威の防御設定では、メッセージのサイズ、エレメントの数、属性のサイズなど、XML メッセージのさまざまなプロパティに基づいた制限を適用できます。ACE Web Application Firewall は、ルールに違反しているメッセージを検出すると、イベントを記録してそのメッセージを廃棄します。

XML 固有の脅威の検査に加え、XML メッセージには、メッセージ検査ルールや、仮想 Web アプリケーションによって適用されるプロファイルに設定されたその他の処理が適用されます。

脅威防御の設定の調整

XML の脅威防御の設定には、ほとんどの目的に適する値があらかじめ設定されています。これらの値は、次のとおりに表示し、変更することができます。

ステップ 1 Web コンソールのナビゲーション メニューで、[System Management] リンクをクリックします。

ステップ 2 ACE Web Application Firewall ヘッダーの下にある [I/O process settings] リンクをクリックします。

ステップ 3 設定が [Reactor] という見出しの下に表示されます。必要に応じて、設定を変更します。使用可能な設定には、たとえば、最大ドキュメント サイズ、エレメント レベル、エレメントあたりの属性数などがあります。

設定の詳細については、[I/O process settings] ページからアクセスできるオンライン ヘルプ ページを参照してください。

ステップ 4 [Save Changes] をクリックして、変更内容を作業ポリシーに保存します。

ポリシーが導入された後は、設定した要件を満たしていない着信要求が ACE Web Application Firewall によって遮断されます。