

認証、認可、およびアカウント管理

エグゼクティブ・サマリ

広域アプリケーション配信分野をリードするブルーコート製品は、WAN およびインターネット内でアプリケーションを加速化し保護します。ブルーコートは、ユーザーおよびネットワーク・リソースをコントロールし、Web 上の脅威から保護して、広範囲に及ぶ WAN ベースのアプリケーションを加速化する、堅牢で柔軟なソリューションを提供します。WAN のいずれかの末端やインターネット・アクセス・ポイント、またはビジネス・クリティカルなサービスの前など、Blue Coat ProxySG アプライアンスは、どこへ導入しても不要なものを止め、必要なものを加速化するコントロール・ポイントになります。このソリューションの一環として、ProxySG アプライアンスは、接続をユーザーレベルでコントロールするための認証、認可、およびアカウント管理をサポートします。

認証、認可、およびアカウント管理とは

AAA (認証、認可、およびアカウント管理)は、ユーザーを識別して付与するアクセス権を決定し、そのユーザーのアクティビティを記録するプロセスです。AAA を使用すれば、ユーザーを識別して所属するグループと属性を特定し、その情報に基づいてアクセス・コントロール・ポリシーを実施することにより、ネットワーク上でユーザーに対して何を許可するかを効率的にコントロールし、すべてのトランザクションを記録することができます。

認証、認可、およびアカウント管理を行うべき理由

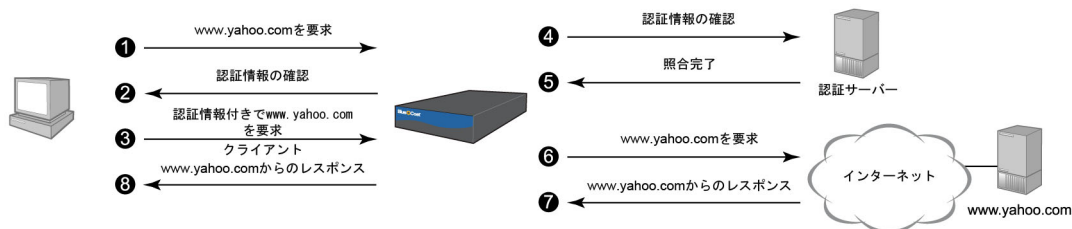
ProxySG アプライアンスの基本機能の 1 つは、ネットワーク接続のコントロールです。ソリューションの一部として、多くの場合で、ユーザーまたはグループに基づいてコントロールを適用することが求められます。たとえば、経営陣だけが利用できるようにする必要があるリソースへのアクセスを制限したり、特定のグループに対してのみインターネット・アクセスを制限したり、ユーザーやグループのメンバーシップに基づいて帯域幅コントロールを実施したりすることがあります。AAA を使用すれば、これらの目的を達成できます。ほとんどの企業は通常、ネットワーク・リソースへのアクセスをコントロールするために、何らかの形式の AAA をネットワークで使用しています。ProxySG アプライアンスを導入すれば、管理者は、ProxySG アプライアンスに既存の認証アーキテクチャを使用させて、ユーザーの識別やグループのメンバーシップおよび属性の特定を行うことができます(既存の認証メカニズムがない状態で導入する場合は、ローカル・パスワード・ファイルを使用してユーザーおよびグループを定義できます)。認証の設定後、ユーザーおよびグループに基づくポリシーを作成することにより、管理者は内部および外部のコンテンツへのアクセスを管理および監視できます。ユーザー、グループ、または属性情報を意思決定プロセスで使用できるため、管理者は接続およびコンテンツに関してよりきめ細かくコントロールすることが可能です。

また、AAA を使用すれば、ProxySG アプライアンスによりユーザーとクライアントからの要求が関連付けられ、それらの要求がアクセス・ログに記録されます。地域法や国際法へのコンプライアンスが求められる企業にとっては、AAA のこのようなアカウント管理コンポーネントが必要になる場合があります。

認証、認可、およびアカウント管理の仕組み

名前からわかるとおり、AAA には認証、認可、およびアカウント管理の 3 つのコンポーネントが含まれています。

認証は、ユーザーの身元を確認(特定)するプロセスです。ほとんどの場合、始めに ProxySG アプライアンスがユーザーの最初の要求に応じて認証情報の確認を送信します。ユーザーは、この認証確認に応じて、ProxySG アプライアンスに認証情報を送信します。ProxySG アプライアンスは、その認証情報を照合のために認証サーバーに渡します。認証情報が照合されると、ユーザーの身元が特定され、そのユーザーのグループおよび属性情報も取得できます。ProxySG アプライアンスは、その情報と設定されているポリシーを使用して、ユーザーの要求を認可、つまりそれを処理する方法を決定します。このプロセスの一環として、ユーザー要求が ProxySG アプライアンスのアクセス・ログに記録されるため、アカウント管理も行えます。



認証レルム

ほとんどの認証方式は、ユーザーの身元とグループおよび属性値の特定をサポートしていますが、ユーザーの身元の特定しかサポートしない方式もあります。また、導入方法によっては、ユーザーの特定だけでよい場合もありますが、その他の場合は、2つの認証方式を組み合わせて完全なソリューションを達成します。Blue Coat ProxySG アプライアンスでは、認証レルムにより使用する認証方式を定義できます。以下の認証レルムは、ユーザーとグループ情報の両方の特定をサポートします。

- IWA - Kerberos、NTLM、または Basic 認証情報を使用する統合 Windows 認証。
- LDAP - LDAP サーバーに対する認証。よく知られている LDAP サーバーとしては、Active Directory、Novell eDirectory、および Netscape iPlanet などがあります。
- RADIUS - RADIUS サーバーに対する認証。
- ローカル - ProxySG アプライアンスにローカルでインストールされているパスワード・ファイルを使用する認証。
- Oracle COREid (Oracle Access Manager、および以前は Oblix COREid としても知られる) - Oracle COREid システムとの認証統合。COREid のシングル・サインオン導入をサポートします。
- Netegrity SiteMinder (CA eTrust SiteMinder としても知られる) - Netegrity SiteMinder システムとの認証統合。SiteMinder のシングル・サインオン導入をサポートします。

LDAP および RADIUS 認証の場合、ProxySG アプライアンスが認証サーバーと直接やり取りします。IWA、COREid、および SiteMinder 認証の場合、BCAAA (ブルーコート認証/認可エージェント)を中間エージェントとして使用して、認証サーバーと統合します。

導入方法によっては、認証情報の確認によるユーザーの特定が不要な場合や、不可能な場合があります。そのため、ProxySG アプライアンスは、ユーザーに認証確認を送信する代わりに、クライアントからの要求に含まれる情報に基づいてユーザーを認証する方式もサポートしています。特定プロセスにおいて認証サーバーとのやり取りがないため、グループおよび属性情報は取得されません。ただし、LDAP やローカルなどの認証レルムを個別に設定することで、それらの情報を特定できます。以下の認証レルムは、ユーザーの確認のみを行う認証方式を使用します。

- Certificate - ユーザー証明書を使用する認証。
- Policy Substitution - ユーザー要求のさまざまな情報からユーザーを識別します。
- Windows SSO - クライアントから要求された IP アドレスを Windows ドメイン・ログインにマッピングすることによってユーザーを特定します。

認証モード

Blue Coat ProxySG アプライアンスは、使用する認証確認のタイプや代用認証情報を指定できる、さまざまな認証モードをサポートします。認証確認は、クライアントからユーザー認証情報を取得する際の方式です。以下の認証確認方式を使用できます。

- Origin - 401 認証要求を使用して認証確認します。一般に、リバース・プロキシ導入で使用されます。
- Origin-redirect - オリジン認証確認を発行する前に、ユーザー要求を仮想 URL にリダイレクトします。一般に、透過型の導入で使用されます。
- Proxy - 407 プロキシ認証要求を使用して認証確認します。一般に、明示型プロキシ導入で使用されます。
- Form - 認証フォームを使用して認証確認します。ユーザー認証確認に表示される情報はカスタマイズできます。
- Form-redirect - フォーム認証確認を発行する前に、ユーザー要求を仮想 URL にリダイレクトします。

ユーザーに対して発行される認証確認の数と、ProxySG アプライアンスおよびバックエンド認証サーバー間で発生するトラフィック量を減らすために、ProxySG アプライアンスは代用認証情報の使用をサポートしています。代用認証情報は、ユーザーの実際の認証情報の代わりとして受け取られる認証情報です。以下の代用認証情報がサポートされています。

- 接続 - ユーザーが1回の接続につき1回だけ認証されます。
- クッキー - 認証後に認証クッキーが設定され、その後の要求で使用されます。
- IP アドレス - 認証ユーザーへのマッピングにユーザーの IP アドレスが使用されます。固有の IP アドレスを使

用する認証方式(Windows SSO など)を実装する場合や、ユーザー・エージェントがクッキーをサポートしない場合は、代用 IP が便利です。

認証方式でクッキーや代用 IP の使用が指定されていても、ユーザーは 1 回の接続につき 1 回しか認証されないことに注意してください。

ProxySG アプライアンスでは、前述の認証確認方式と代用認証情報をさまざまに組み合わせて使用できます。要求ごとに最適な認証モードを判断して使用する自動モードもあります。

ブルーコート認証/認可エージェント(BCAAA)

BCAAA は、SGOS とは別にインストールして設定する必要があるソフトウェア・エージェントです。BCAAA は、ProxySG アプライアンスと特定の認証方式の間を仲介するサービスです。

IWA の場合、BCAAA をドメイン・メンバー・サーバーにインストールし、Windows API を使用して、ユーザーの認証とグループ情報の取得を行います。Oracle COREid の場合、COREid Access System へのアクセスが BCAA を介してルーティングされ、BCAAA は COREid Access System 内のカスタム・アクセス・ゲートとして機能します。BCAAA は COREid Access Server と通信してユーザーを認証し、COREid セッション・トークン、認可アクション、およびグループのメンバーシップ情報を取得します。

認可アクションとして指定されている HTTP ヘッダ変数とクッキーが BCAA に返され、ProxySG アプライアンスに転送されます。BCAAA は、Netegrity SiteMinder 認証にも必要であり、Windows と Solaris の両方でサポートされています。SiteMinder システム内では、BCAAA がカスタム Web エージェントとして機能します。SiteMinder ポリシー・サーバーと通信してユーザーを認証し、SiteMinder セッション・トークン、レスポンス属性情報、およびグループのメンバーシップ情報を取得します。OnAuthAccept および OnAccessAccept 属性に関連付けられたカスタム・ヘッダおよびクッキーのレスポンス属性は、ポリシー・サーバーから取得され、ProxySG アプライアンスに転送されます。

BCAAA は、Windows SSO 方式の一部としても使用され、ドメイン・コントローラでユーザーのログインを監視したり、クライアント・マシンにユーザーのログイン情報を照会したりするように設定できます。

シーケンスレルム

Blue Coat ProxySG アプライアンスは、認証におけるシーケンスレルムの使用をサポートしています。シーケンスレルムは、さまざまな認証レルムを組み合わせるために使用されます。ProxySG アプライアンスは、認証が問題なく完了するまで、シーケンス内の各レルムに対してユーザーの認証を試みます。組織で複数の認証レルムをサポートしたいが、ユーザー要求を特定のレルムに簡単にマッピングできない場合などに、シーケンスレルムを使用すると特に便利です。シーケンスレルムは、認証チェックの優先順位を指定する場合にもよく使用されます。たとえば、シーケンスレルムを使用して、プライマリ認証方式として IWA や LDAP を最初に試行し、それが失敗したら、Windows SSO やポリシー代用などの SSO 方式を試行するよう指定できます。

ポリシーによる認可

ProxySG でポリシーを実装することで、ユーザー要求の認可が行えるようになります。管理者は、ユーザーまたはグループ・ベースの強力なポリシーを定義し、内部および外部のコンテンツへのアクセスを管理および監視できます。そのために、ProxySG アプライアンスは、認証ごといくつかのポリシー条件やプロパティをサポートしています。

認証および認可ポリシーの例

ブルーコートシステムズ社の管理者は、ユーザーがインターネットにアクセスする場合にのみユーザー認証を行い、イントラネットへのアクセスでは認証は必要ないと考えています。インターネットへのアクセスについて、一般の従業員には特定のタイプの Web サイトへのアクセスを禁止し、社内特定の組織には、業務上その必要があるため、アクセスを可能にします。経営陣に制約は設けません。

```
<PROXY>
url.domain=intranet.bluecoat.com ALLOW
authenticate(NTLMRealm)
<PROXY>
group=cf-cal%executives ALLOW
group=cf-cal%hr category=("Travel", "Job Search/Careers") ALLOW
category=("Travel", "Job Search/Careers", "Gambling", "Nudity") exception (content_filter_denied)
```

*ALLOW がデフォルトのポリシーです。

アクセス・ログによるアカウント管理

ブルーコートのアプライアンスは、すべてのクライアントからの要求の記録をアクセス・ログの形式で保持するよう設定できます。いくつかの定義済みのアクセス・ログ形式を使用して、カスタム形式を作成できます。AAA においてアクセス・ログに記録する必要がある最も重要な情報は、ユーザーとそれに関連する要求です。一般的なアクセス・ログのエントリは以下のとおりです。

以下のエントリでは、アクセス・ログ・フィールドの「cs-username」を使用してユーザー名のみを記録します。

```
2007-03-22 23:05:39 64 10.167.10.100 304 TCP_HIT 256 497 GET http www.google.ca 80 /images/nav_logo2.png - user1 - DIRECT 72.14.203.99 image/png http://www.google.ca/ "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" PROXIED "none" - 10.167.42.28
```

以下のエントリでは、アクセス・ログ・フィールドの「cs-userdn」を使用してユーザーの FQDN (Fully Qualified Domain Name 完全修飾ドメイン名)を記録します。

```
2007-03-22 23:07:32 55 10.167.10.100 304 TCP_HIT 256 497 GET http www.google.ca 80 /images/nav_logo2.png - CN=user1,CN=Users,DC=authteam,DC=waterloo,DC=bluecoat,DC=com - DIRECT 72.14.203.99 image/png http://www.google.ca/ "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" PROXIED "none" - 10.167.42.28
```

ブルーコートのアプライアンスの特長

認証と認可を超えるもの

認証と認可の一般的な役割は、ユーザーを特定し、身元情報や認可情報を使用して、ネットワーク・リソースへのアクセスをコントロールすることです。Blue Coat ProxySG アプライアンスでは、認証と認可がそれよりもはるかに強力な力を発揮します。管理者は、認証と認可を通して取得した情報から、帯域幅、コンテンツ・フィルタリング、内部/外部コンテンツ、ウィルス・スキャン、その他について、ユーザーやグループのメンバーシップに基づいて意思決定を行うことができます。

幅広いソリューション

ブルーコートは、総合的な認証、認可、およびアカウント管理ソリューションを提供します。ProxySG アプライアンスは、多数の認証方式、認証確認タイプ、および代用認証情報がサポートされているため、ほとんどすべての環境に導入できます。



ブルーコートシステムズ合同会社

〒105-0021 東京都港区東新橋 1-9-2 汐留住友ビル16階

Tel 03-6251-9111 (代表) Fax 03-6251-9112

Mail japan.info@bluecoat.com URL http://www.bluecoat.co.jp/

Copyright ©2009 Blue Coat Systems, Inc. All rights reserved worldwide. 本ドキュメントのいかなる部分も、Blue Coat Systems, Inc.の書面による許可なく、いかなる手段でも複製または電子媒体に変換することを禁じます。仕様は予告なく変更される可能性があります。本ドキュメントに記載されている情報は正確で信頼できる内容ですが、Blue Coat Systems, Inc.はそれを使用することに対して一切の責任を負わないものとします。ブルーコート、ProxySG、PacketShaper、および IntelligenceCenter は Blue Coat Systems, Inc.の米国および世界各国での登録商標です。本ドキュメントで使用されているその他のすべての商標は、それぞれの所有者の所有物です。
v.TP-AAA-v1-1007