HP IceWall SSO

ここが知りたい！8.0.1(8.0 R1)の新機能特集(2)
ーHP IceWall SSOのWindows統合認証機能 (Windows Kerberos対応)

本トピックでは、HP IceWall SSO 8.0.1(8.0 R1)から新たにオプション機能として提供されたWindows 統合認証機能 (Windows Kerberos 対応)について説明します。
この機能を使用することにより、Windows ドメインにログインしているクライアントから自動的にIceWallサーバへのログインを行い、Windows 環境とのシングルサインオンを実現できます。

本機能を利用するためには、オプション製品「Domain Gateway Option for UNIX」(以下、Domain Gateway Option)の購入が必要です。

1.HP IceWall SSO のWindows統合認証機能

Domain Gateway Option for UNIXを導入せずにWindowsドメイン環境にHP IceWall SSO(以下 IceWall) を構築した場合、Windowsドメイン環境への認証とIceWallへの認証とで、二度の認証オペレーションが必要です。
IceWallのWindows 統合認証機能を利用することによって、IceWallへの認証を自動的に行なうことができます。

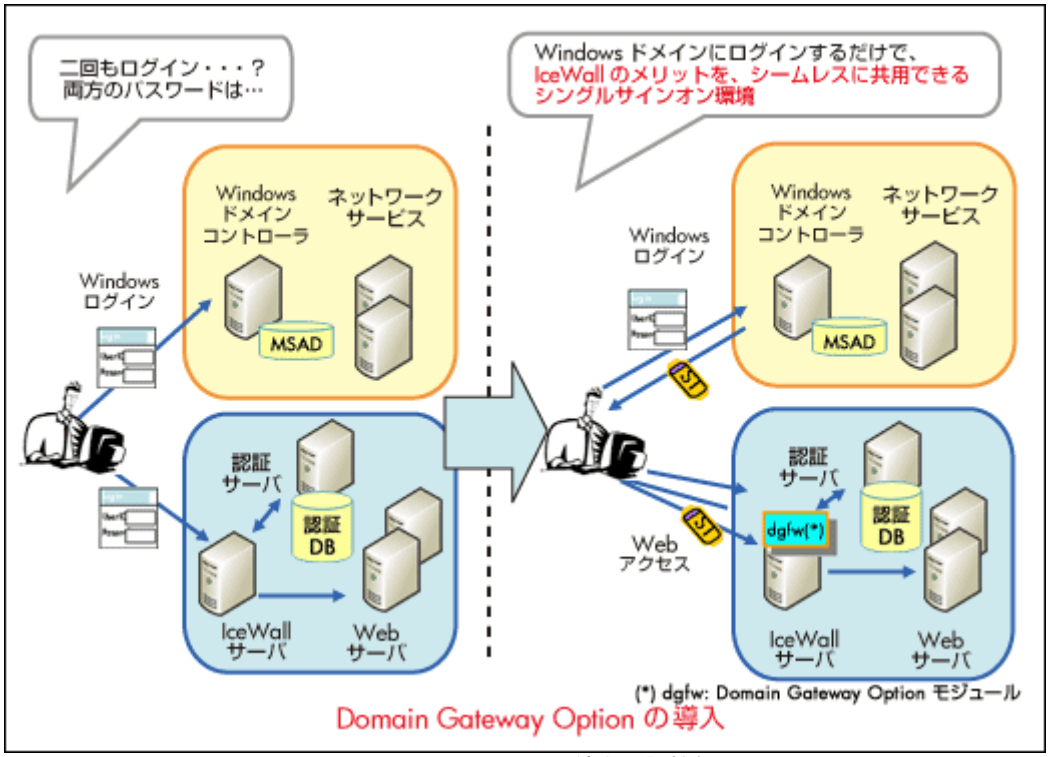

図1. IceWall のWindows統合認証機能

2.Windows Kerberos認証の概要

IceWallのWindows統合認証機能はMicrosoft Windows OSのKerberos認証に対応しています。ここで、Microsoft Windows OSのKerberos認証機能について簡単に説明します。
Microsoft Windows Server 2003にはデフォルトのネットワーク認証プロトコルとしてKerberos バージョン5に基

づいたKerberos認証機能が実装されています。クライアントシステムがKerberos認証機関であるキー配布センター(以下、KDC)に認証されると、チケットと呼ばれるデータパケットが発行されます。このチケットの中には、ユーザの身元を保証する情報が暗号化されて格納されています。クライアントシステムがネットワークサービスに対してチケットを提出することによって、以下の相互認証が行われます。

- ネットワークサービスに対してユーザが本人であることを証明
- サービスが目的のサービスそのものであることをユーザーに対して証明

Windowsネットワーク環境の場合、ドメインコントローラがKDCの役割を担い、ドメインコントローラの領域内でユーザにチケットを発行します。一度発行したチケットはチケットを提出することで繰り返しネットワークサービスを受けることができます。KDCであるドメインコントローラが認証プロセスにおいて関与するのはチケットの発行時のみです。

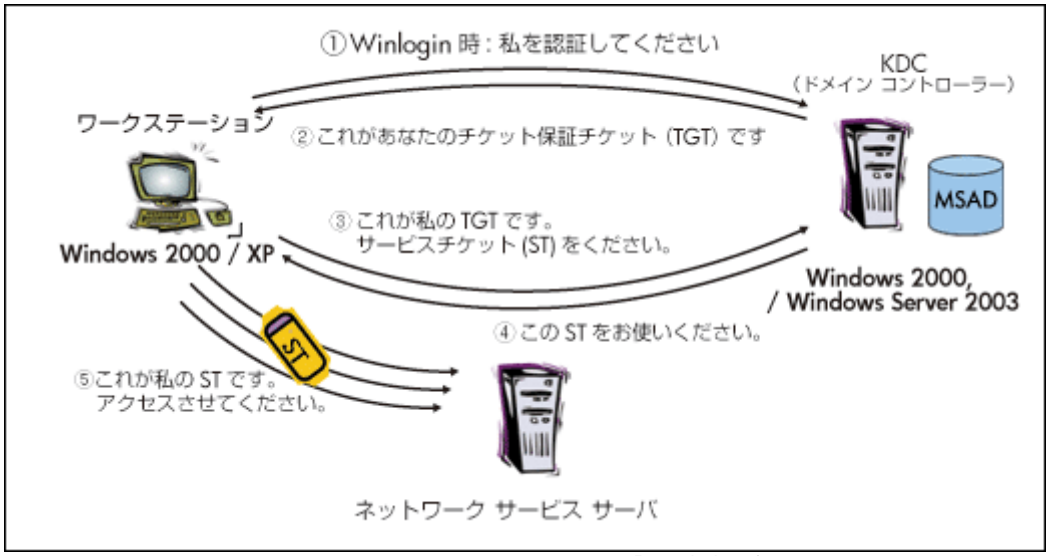

図2. Microsoft Windows OSのKerberos認証の大まかなフロー

3.IceWall Windows統合認証機能の動作フロー

前述のWindows Kerberos認証の基本的な流れを踏まえ、IceWallのWindows統合認証機能においてどのような処理が行われているか説明します。

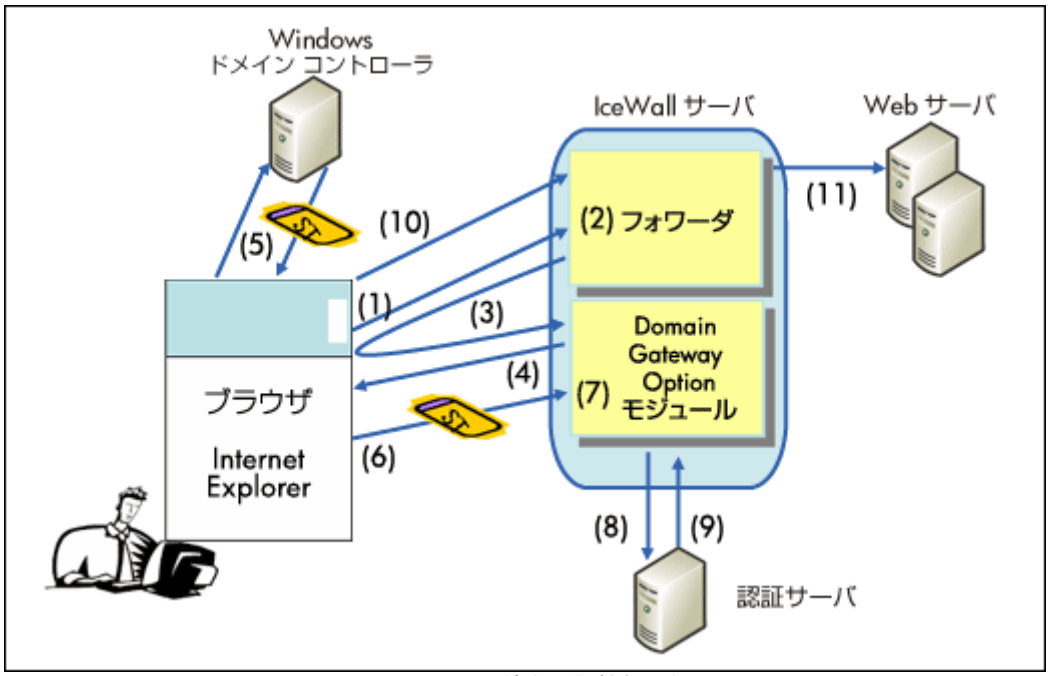

図3. IceWallのWindows統合認証機能の処理フロー

ここではすでにユーザがWindowsドメインにログインしている状況を想定します。

(1) ユーザがアクセスするページのURLを入力し、IceWallサーバを経由してWebサーバへのアクセスを要求します。

(2) ユーザがすでにIceWallサーバにログインしているか確認するために、フォワーダがブラウザからのHTTPリクエストヘッダにIceWallセッションIDが含まれているかを確認します。ここでは、まだユーザはIceWallサーバにログインしておらずHTTPリクエストヘッダにセッションIDは含まれていないと仮定します。
(3) リクエストはフォワーダからブラウザを経由してDomain Gateway Optionモジュールにログイン要求としてリダイレクトされます。
(4) Domain Gateway OptionモジュールはHTTPリクエストヘッダにKerberosのサービスチケットが含まれているかを確認し、もし含まれていなかったらブラウザにサービスチケットの提示を要求します。
(5) もしブラウザがサービスチケットを持っていない場合、ブラウザはWindowsドメインコントローラからサービスチケットを取得します。
(6) ブラウザがDomain Gateway Optionモジュールにサービスチケットを送信します。
(7) Domain Gateway Optionモジュールがサービスチケットを検証し、サービスチケットからユーザIDを抽出します。
(8) Domain Gateway Optionモジュールが認証サーバに、取得したユーザIDによるログイン要求を送信します。
(9) 認証サーバはログインを認可するとセッションIDを生成し、Domain Gateway Optionモジュールに返します。
(10)Domain Gateway OptionモジュールがHTTPリクエストヘッダにIceWallセッションIDを追加し、ユーザが(1)で指定したURLをフォワーダへリダイレクトします。
(11)フォワーダでは(2)と同様にHTTPリクエストヘッダにセッションIDが含まれているかを確認し、正当なセッションIDが含まれている場合、後段のWebサーバにリクエストを転送します。
(12)以降同一のWebサーバへのアクセスがあるごとに(11)が行われます。

4.まとめ

IceWallのWindows統合認証機能を導入することにより、以下のメリットが得られます。

- Windowsドメインへの認証オペレーションのみでIceWallのシングルサインオン環境を利用できます。
- Windows環境においてもIceWallのさまざまなメリットを利用できます。
  - 後段のWebアプリケーションの稼動OSを意識する必要がありません。
  - ファイアウォールとしての役割によってセキュリティが強化されます。

2006.06.29　日本ヒューレット・パッカード コンサルティング・インテグレーション統括本部　チーフコンサルタント
望月恒男