IBM WebSphere Commerce

보안 안내서

버전 5.4

IBM WebSphere Commerce

보안 안내서

버전 5.4

주!

이 책과 이 책이 지원하는 제품을 사용하기 전에 117 페이지의 『주의사항』에 있는 일반 정보를 읽으십시오.

초판(2002년 3월).

이 개정판은 새 개정판에 별도로 명시하지 않는 한, IBM® WebSphere Commerce의 버전 5.4 및 모든 후속 릴리스와 수정에 적용됩니다. 제품 레벨에 대한 올바른 개정판을 사용 중인지 확인하십시오.

책에 대한 주문은 한국 IBM 담당자 또는 해당 지역의 IBM 지방 사무소로 문의하십시오. 다음 주소에서는 책을 구비하고 있지 않습니다.

IBM은 여러분의 의견을 환영합니다. 다음 중 한 가지 방법으로 사용자 의견을 보내실 수 있습니다.

1. 아래로 전자 우편을 보내십시오.

   `ibmkspoe@kr.ibm.com`
2. 팩스로 보내실 경우에는 아래 번호를 사용하십시오.

   `02-3781-5200`
3. 우편으로 보내실 경우에는 아래 주소로 우송해 주십시오.

   135-270
   서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
   한국 아이.비.엠 주식회사
   고객만족센터

IBM에 정보를 보내는 경우, IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

목차

서문

이 문서에서는 WebSphere Commerce 5.4의 보안 특징과 이들 특징 구성 방법에 대해 설명합니다.

WebSphere Commerce와 관련된 인증, 권한 및 액세스 제어 정책 같은 보안 문제를 자세히 설명합니다. 이 문서의 목표는 사이트의 보안을 담당하는 사람(시스템 운영자나 WebSphere Commerce 사이트 운영자를 포함할 수 있음)에게 WebSphere Commerce 프로덕션 사이트를 신뢰할 수 있는 방법으로 보안할 수 있게 하는 포괄적인 문서를 제공하는 것입니다.

이 문서는 WebSphere Commerce 사이트에 대한 보안 책임자 또는 보안 관리자를 대상으로 합니다.

중요

이 문서에서는 전자상거래 사이트 전개와 관련된 WebSphere Commerce 보안 문제만을 다룹니다. 운영체제의 보안 취약점과 관련된 문제는 다루지 않습니다. 운영체제를 보안하기 위해 취해야 하는 적절한 수단을 판별하려면 운영체제 공급업체에 문의해야 합니다.

이 문서에서의 이동

이 문서는 다음과 같은 부분으로 구성되어 있습니다.

- 1 페이지의 제 1 부 『WebSphere Commerce 보안 모델』에서는 WebSphere Commerce 보안 모델에 대해 설명하고 WebSphere Commerce 보안의 개념적 개요를 제공합니다. 이 부분은 WebSphere Commerce 보안의 일반적인 개요를 원하거나 WebSphere Commerce 사이트에서 보안을 계획하는 사람에게 유용합니다.
- 37 페이지의 제 2 부 『WebSphere Commerce 사이트 운영자 보안 태스크』에서는 사이트 보안과 관련된 WebSphere Commerce 사이트 관리 태스크에 대해 설명합니다. 이 부분은 사이트 보안과 관련된 사이트 관리 태스크를 수행하는 사람에게 유용합니다.
- 69 페이지의 제 3 부 『시스템 운영자 보안 태스크』에서는 시스템 보안과 관련된 WebSphere Commerce 시스템 관리 태스크에 대해 설명합니다. 이 부분은 시스템 관리 태스크를 수행하는 사람과 시스템 보안에 관심이 있는 사람에게 유용합니다.

- 89 페이지의 제 4 부『WebSphere Commerce 개발자 보안 태스크』에서는 개발자의 관점에서 WebSphere Commerce 액세스 제어에 대해 설명합니다. 이 부분은 코드에 액세스 제어 정책을 구현하는 액세스 제어 개념을 이해하려는 사람에게 유용합니다.

진행 중인 보안 평가

WebSphere Commerce 상품군은 지속적으로 IBM 보안 전문가의 독립된 그룹으로부터 보안 분석을 받습니다. 이 전문가들은 브라우저를 통한 WebSphere Commerce에 대한 액세스만을 갖는 사용자의 관점에서부터 WebSphere Commerce 서버가 실행 중인 동일한 시스템에 계정을 갖고 있는 특권이 더 많은 사용자에 이르기까지 보안 분석을 수행합니다. 보안 전문가 분석의 피드백이 WebSphere Commerce의 보안을 지속적으로 개선하는 데 사용됩니다.

WebSphere Commerce 5.4에서의 보안 개선

다음 절에서는 WebSphere Commerce Suite 5.1과 상대적인 WebSphere Commerce 5.4에서의 보안 개선사항을 나열합니다. 이들 개선사항의 대부분은 WebSphere Commerce Business Edition 5.1 릴리스에서 이루어졌습니다. 이들 개선사항은 일반적으로 다음에 적용할 수 있습니다.

- WebSphere Commerce 사이트 운영자
- 시스템 운영자
- WebSphere Commerce 개발자

때로는 이들 역할이 교환 가능함에 유의하십시오.

사이트 운영자에 대한 개선사항

다음은 일반적으로 사이트 운영자를 대상으로 하는 WebSphere Commerce 5.4 보안 개선사항입니다.

액세스 제어

- **액세스 제어 프레임워크** -- 핵심 개선사항은 새 액세스 제어 프레임워크가 WebSphere Commerce 5.4에서 구현되었다는 점입니다. 이러한 새 프레임워크는 액세스 제어 정책을 사용하여 주어진 사용자가 주어진 자원에 대해 주어진 조치를 수행하도록 허용되는지를 판별합니다. 새 액세스 제어 프레임워크는 객체 단위 액세스 제어를 제공합니다. WebSphere Application Server가 제공하는 액세스 제어와 함께 작업하지만 이를 대체하지는 않습니다. 새 액세스 제어 프레임워크는 91 페이지의 제 11 장『액세스 제어』에서 자세히 설명됩니다.

  새 액세스 제어 프레임워크는 다음 방법으로 이전 액세스 제어를 개선합니다.

빠릅니다.

광범위한 액세스 정책의 의도를 캡쳐합니다. 프레임워크는 일반적이어서 사용자 그룹, 자원 그룹, 조치 그룹 및 관계 그룹의 광범위한 배열을 처리할 수 있습니다.

계층적입니다.

조직이 소유하는 액세스 제어 정책이 하위 조직에도 적용됩니다.

사용자 정의가 가능합니다.

액세스 제어 정책이 응용프로그램 코드와 분리되므로 코드를 재컴파일하지 않고 정책을 변경할 수 있습니다.

컴팩트합니다.

새 프레임워크는 확장성이 큽니다. 액세스 제어 정책의 수는 오브젝트 수가 아니라 비즈니스 프로세스의 수와 함께 성장합니다. 대부분의 그룹화 프레임워크가 암시적 조건을 바탕으로 하므로, 조건이 충족되는 동안은 정책이 적용됩니다.

- **사이트간 스크립** -- WebSphere Commerce 구성 관리자의 사이트간 스크립트 보호 노드를 사용하여 허용되지 않는 것으로 지정되는 속성이나 문자를 포함하는 모든 사용자 요청을 거부합니다. 이것은 39 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.

인증

- **암호 저장** -- WebSphere Commerce 5.4는 암호 자체를 저장하는 대신 WebSphere Commerce 데이터베이스의 SHA-1 해시 설계를 사용하여 암호의 단방향 해시를 암호화하고 저장합니다. 이것은 사이트 또는 시스템 운영자를 포함하여 누구도 사용자 암호를 해독할 수 없게 합니다.
- **암호 무효화** -- WebSphere Commerce 구성 관리자의 암호 무효화 노드를 사용하여 사용자가 처음으로 시스템에 로그인할 때 암호를 변경하도록 요구합니다. 이것은 39 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.
- **계정 정책** -- WebSphere Commerce 관리 콘솔의 계정 정책 페이지를 사용하여 사이트에 대한 계정 정책을 설정함으로써 사용 중인 계정 관련 정책을 정의하십시오. 이것은 39 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.
- **암호 정책** -- WebSphere Commerce 관리 콘솔의 암호 정책 페이지를 사용하여 사이트에 대한 암호 정책을 설정함으로써 사용자의 암호 선택 특성을 제어하십시오. 이것은 39 페이지의 제 4 장 『사이트 보안 개선』에서 자세히 설명됩니다.

- **계정 잠금 정책** -- WebSphere Commerce 관리 콘솔의 계정 잠금 정책 페이지를 사용하여 사이트에 대한 계정 잠금 정책을 설정함으로써 사용자 계정이 손상되는 기회를 줄이십시오. 이것은 39 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

권한부여

암호로 보호된 명령 -- WebSphere Commerce 구성 관리자의 암호로 보호된 명령 노드를 사용하여 사용자가 지정된 명령을 실행 중인 요청을 실행하려는 경우 암호를 입력해야 하도록 설정하십시오. 이것은 39 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

암호화된 데이터

데이터베이스 갱신 도구 -- WebSphere Commerce 구성 관리자의 데이터베이스 갱신 도구 노드를 사용하여 암호 및 신용 카드 정보뿐 아니라 WebSphere Commerce 데이터베이스의 판매자 키 같은 암호화된 데이터를 갱신하십시오. 이것은 39 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

세션 관리

로그인 시간 종료 -- 로그인 시간 종료 노드를 사용하여 장시간 동안 활동하지 않는 사용자를 로그오프하고 시스템에 다시 로그온하도록 요청하십시오. 이러한 개선 기능은 WebSphere Commerce 구성 관리자를 통해 호출되며 39 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

감사 추적

액세스 로그 작성 -- 액세스 로그 작성을 사용하여 WebSphere Commerce에 대한 모든 보안 위협을 빨리 식별하십시오. 이러한 개선 기능은 WebSphere Commerce 구성 관리자를 통해 호출되며 39 페이지의 제 4 장『사이트 보안 개선』에서 자세히 설명됩니다.

시스템 운영자에 대한 개선사항

다음은 일반적으로 사이트 운영자를 대상으로 하는 WebSphere Commerce 5.4 보안 개선사항입니다.

- 중요한 보안 개선사항은 표준이 아닌 포트 번호(예: 포트 443과 반대인 포트 8000)에서 실행하도록 WebSphere Commerce 관리 도구를 구성하는 능력입니다. 이 포트에 대한 액세스를 제한하여 관리 도구에 대한 액세스를 로컬 네트워크나 인트라넷으로 제한할 수 있습니다.
- WebSphere Commerce 관리 콘솔에서 보안 확인 실행 페이지를 사용하여 가능한 보안 노출을 포함할 수 있는 임시 WebSphere Commerce 파일을 확인하고 삭제하는 보안 프로그램을 실행하십시오.

WebSphere Commerce 프로그래머에 대한 개선사항

핵심 개선사항은 새 액세스 제어 프레임워크가 WebSphere Commerce 5.4에서 구현되었다는 점입니다. 이러한 새 프레임워크는 액세스 제어 정책을 사용하여 주어진 사용자가 주어진 자원에 대해 주어진 조치를 수행하도록 허용되는지를 판별합니다. 새 액세스 제어 프레임워크는 객체 단위 액세스 제어를 제공합니다. WebSphere Application Server가 제공하는 액세스 제어와 함께 작업하지만 이를 대체하지는 않습니다. 새 액세스 제어 프레임워크는 91 페이지의 제 11 장『액세스 제어』에서 자세히 설명됩니다.

새 액세스 제어 프레임워크는 다음 방법으로 이전 액세스 제어를 개선합니다.

빠릅니다.

광범위한 액세스 정책의 의도를 캡쳐합니다. 프레임워크는 일반적이어서 사용자 그룹, 자원 그룹, 조치 그룹 및 관계 그룹의 광범위한 배열을 처리할 수 있습니다.

계층적입니다.

조직이 소유하는 액세스 제어 정책이 하위 조직에도 적용됩니다.

사용자 정의가 가능합니다.

액세스 제어 정책이 응용프로그램 코드와 분리되므로 코드를 재컴파일하지 않고 정책을 변경할 수 있습니다.

컴팩트합니다.

새 프레임워크는 확장성이 큽니다. 액세스 제어 정책의 수는 오브젝트 수가 아니라 비즈니스 프로세스의 수와 함께 커집니다. 대부분의 그룹화 프레임워크가 암시적 조건을 바탕으로 하므로, 조건이 충족되는 동안은 정책이 적용됩니다.

WebSphere Commerce Suite 5.1 Pro Edition에서의 보안 개선

Commerce Suite 5.1이 새 전자상거래 아키텍처를 보여주었고 C++ 기반의 Commerce Suite 4.1을 완전하게 재작성하였지만, 이전 WebSphere Commerce Suite 버전의 모든 보안 특징 및 새 보안 개선사항을 추가했습니다. 이들 개선사항이 WebSphere Commerce 5.4에서 계승되었습니다.

Commerce Suite 5.1은 이전 릴리스에서 제공되었던 WebSphere Commerce Suite 운영자 및 구매자 자원에 대한 권한없는 액세스에 대해 계속 보호했습니다.

- WebSphere Commerce Suite 사용자가 중요한 정보에 대한 액세스를 얻기, 제출하기 전에 인증 또는 SSL 모드에 있음을 보장하는 액세스 제어 기능에 대한 지원을 계속합니다.
- Commerce Suite 4.1과 동일한 모델처럼 WebSphere Commerce Suite 명령을 그룹에 지정하여 사이트 운영자나 상점 레벨 운영자만이 특정 명령을 실행할 수 있도록 합니다.

일반 보안 개선사항

Java™로 Commerce Suite 5.1을 재작성함으로써, C++로 작성된 소프트웨어에 발생하는 많은 고유의 보안 문제점이 제거되었습니다. Java는 포인터를 사용하지 않으므로, 대부분의 C++ 기반 소프트웨어의 보안 취약점인 버퍼 오버플로우 문제점을 제거했습니다. 업계 표준인 J2EE 스펙을 준수하여 WebSphere Commerce Suite는 강력한 유형 확인을 사용하여 서버가 크래커나 해커가 지정한 불법 명령문을 실행하지 않도록 합니다.

업계 표준인 Triple DES(데이터 암호화 표준) 알고리즘이 WebSphere Commerce Suite 시스템의 중요한 정보를 보호하는 데 사용되었습니다. Triple DES 알고리즘을 포함하는 패키지는 디지털로 서명되어 패키지가 불법 변경된 경우, WebSphere Commerce Suite 서버가 시작하지 않습니다.

세션 관리

쿠키가 도난되지 않았음을 보장하기 위한 고유한 기술을 사용하여 WebSphere Commerce Suite 세션 관리가 최대 보안을 위해 완전히 재작성되었습니다. SSL을 통해서만 이동하고 암호화된 시간소인으로 구성되는 인증 쿠키를 사용하여, 재작성된 세션 관리 설계가 세션 도난에 대해 보호됩니다.

인증

실행 중에 WebSphere Commerce Suite 서버에 필요한 시스템 및 응용프로그램 암호가 판매자가 지정하는 12비트 키를 사용하여 안전하게 암호화되었고 WebSphere Commerce Suite 구성 파일에 저장되었습니다. 사용자 URL 항목 상자에 나타나는 중요한 정보가 권한이 없는 노출로부터 구매자를 보호하기 위해 암호화됩니다.

로그 작성

WebSphere Commerce Suite 로그 시스템은 보안을 핵심 고려사항으로 갖고 설계되어 구매자의 암호와 신용 카드 정보 같은 중요한 정보가 기본적으로 WebSphere Commerce Suite 로그 파일에 기록되지 않았습니다.

이 책에서 사용된 규칙

이 책에서는 다음 강조표시 규칙을 사용합니다.

- **굵은체**는 필드, 아이콘 또는 메뉴 선택사항의 이름과 같은 GUI(Graphical User Interface) 제어 또는 명령을 표시합니다.
- 모노체는 파일 이름, 디렉토리 경로 및 이름과 같이 정확하게 입력해야 하는 텍스트의 예를 표시합니다.
- *기울임꼴*은 단어를 강조하는 데 사용합니다. 기울임꼴은 시스템의 적절한 값으로 대체해야 하는 이름을 표시합니다. 다음과 같은 이름이 표시되면 설명한 대로 사용자의 시스템 값을 대체하십시오.

host_name

WebSphere Commerce Studio 시스템의 완전한 호스트 이름(예를 들어, ibm.com은 완전한 이름입니다).

Windows

drive 논의되는 제품 또는 구성요소를 설치한 드라이브를 표시하는 문자(예: C:).

이 아이콘은 태스크를 완료하는 데 도움이 되는 추가정보를 표시합니다.

추가 정보

WebSphere Commerce 5.4와 관련된 정보는 다음 웹 사이트를 참조하십시오.

http://ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html

WebSphere Commerce Suite와 관련된 정보는 다음 웹 사이트를 참조하십시오.

http://www.ibm.com/software/webservers/commerce/wcs_pro/lit-tech-general.html

Commerce Studio, Professional Developer Edition 5.1 또는 WebSphere Commerce Studio의 이전 버전과 관련된 정보는 다음 웹 사이트를 참조하십시오.

http://www.ibm.com/software/webservers/commerce/commercestudio/lit-tech-general.html

제 1 부 WebSphere Commerce 보안 모델

이 부분에서는 WebSphere Commerce 보안의 개념적 개요를 제공합니다.

제 1 장 WebSphere Commerce 보안 모델에 대한 소개

이 장에서는 다양한 WebSphere Commerce 보안 개념뿐 아니라 WebSphere Commerce 보안 모델에 대해 설명합니다.

개요

이 문서의 정보는 인증, 권한, 정책 및 기밀성의 일반 개념에 대해 설명합니다.

인증의 개념

인증은 사용자나 응용프로그램이 주장하는 정체성이 맞는지를 검증하는 처리입니다. WebSphere Commerce 시스템에서 인증은 시스템에 액세스하는 모든 사용자 및 응용프로그램에 대해 필요합니다. 사용자 인증 처리는 항상 SSL하에서 수행됩니다. 이것은 네트워크를 기웃거리는 프로그램을 사용하는 제삼자가 사용자가 암호를 제출할 때 네트워크에서 *염탐*하지 못하도록 합니다. 암호는 일반적인 보안 실례와 같이 인증 처리 중에 절대로 암호 해독되지 않습니다. 모든 사용자 암호는 *판매자 키*라고 알려진 128 비트 키를 사용하여 해시되고 암호화됩니다. 판매자 키는 WebSphere Commerce 시스템의 설치 및 구성 중에 지정됩니다.

WebSphere Commerce 시스템은 관리 목적을 위해 자체 암호를 갖습니다. 이들 암호는 WebSphere Commerce 사이트측 보안 정책의 일부로서 주기적으로 변경되어야 합니다. WebSphere Commerce 5.4 시스템 암호 변경 방법에 대한 자세한 내용은 71 페이지의 제 7 장 『암호 설정 및 변경』을 참조하십시오.

권한의 개념

권한부여는 사용자가 자원에 대해 특정 조작을 수행할 수 있는지 여부를 판별하는 처리입니다. 권한은 WebSphere Commerce 자원에 대한 액세스 제어 정책으로부터 판별됩니다. WebSphere Commerce 시스템의 다음 두 영역에서 액세스 제어가 필요합니다.

- 권한이 없는 액세스로부터 WebSphere Commerce Enterprise JavaBeans™(EJB beans) 보호. 이 처리는 55 페이지의 제 5 장 『WebSphere™ Application Server 보안 사용』에서 설명됩니다.
- 권한 부여된 당사자만이 WebSphere Commerce 명령의 서로 다른 그룹을 실행할 수 있도록 보장. 이 처리는 91 페이지의 제 11 장 『액세스 제어』에서 설명됩니다.

액세스 제어 정책의 개념

전자상거래 사이트에 참여할 조직과 사용자들의 정의를 완료했다고 가정할 때 일련의 정책을 통해 해당 활동을 관리할 수 있는데, 이 처리를 *액세스 제어*라고 합니다.

액세스 제어 정책은 어떤 사용자 또는 사용자 그룹이 사이트에서 특정 활동을 수행하도록 권한 부여되는지를 설명하는 규칙입니다. 이러한 활동에는 전자상거래 사이트를 운영하고 유지보수하는 데 필요한 수많은 다른 활동뿐 아니라 등록에서부터 경매 관리, 상품 카탈로그 갱신 및 주문에 승인 부여까지를 포함할 수 있습니다.

정책은 사용자에게 사이트에 대한 액세스를 부여하는 것입니다. 하나 이상의 액세스 제어 정책을 통해 자신의 책임을 수행하도록 권한부여되지 않으면 사용자는 사이트의 어떤 기능에도 액세스할 수 없습니다.

WebSphere Commerce 5.4에 대한 액세스 제어 모델은 액세스 제어 정책의 강제 시행을 바탕으로 합니다. 액세스 제어 정책은 액세스 제어 정책 관리자에 의해 강제 시행됩니다. 일반적으로 사용자가 보호 가능한 자원에 액세스하려 시도할 때 액세스 제어 정책 관리자는 먼저 해당 사용자에게 어떤 액세스 제어 정책이 적용될 수 있는지를 판별한 후 적용 가능한 액세스 제어 정책을 바탕으로 사용자가 주어진 자원에 대해 요청한 조작을 수행하도록 허용되는지 여부를 판별합니다.

감사 추적의 개념

컴퓨팅에서 *감사 추적*은 컴퓨터 활동을 추적하는 데 사용되는 전자적 또는 종이 로그를 의미하는 데 사용됩니다. 예를 들어 직원은 미수금 계정 같은 기업 네트워크의 한 부분에 액세스할 수 있지만 급여 같은 시스템의 다른 부분에 액세스하도록 권한 부여되지 않을 것입니다. 해당 직원이 암호를 입력하여 권한이 없는 섹션에 액세스하려 시도하는 경우, 이러한 부적절한 활동이 감사 추적에 기록됩니다.

전자상거래 시스템에서 감사 추적은 고객 활동으로 기록하는 데 사용됩니다. 감사 추적은 고객과 시스템과의 초기 접속뿐 아니라 상품 또는 서비스의 지불 및 운송 같은 후속 조치를 기록합니다. 회사는 감사 추적을 사용하여 모든 조회나 불만사항에 응답할 수 있습니다. 또한 감사 추적을 사용하여 계정을 조정하고 앞으로의 사업계획과 예산수립을 위한 분석 및 이력 정보를 제공하고 세무 감사의 경우에 판매 기록을 제공할 수 있습니다.

감사 추적은 또한 사이버 공간과 인터넷을 통한 컴퓨터 범죄를 조사하는 데 사용할 수도 있습니다. 시스템에 대해 개별적으로 수행되는 악의적 공격을 밝히기 위해 조사자는 범인이 남긴 감사 추적을 따라갈 수 있습니다. 때로는 사이버 범죄의 범인이 모르고 인터넷 서비스 제공업체의 활동 로그나 대화방 로그에 감사 추적을 남길 수 있습니다.

기밀성의 정의

기밀성은 중요한 정보를 의도하지 않은 받는 사람이 읽지 못하도록 보호하는 처리입니다. WebSphere Commerce 시스템에서 기밀성은 중요한 정보가 사용자의 브라우저에서 WebSphere Commerce 서버로 및 WebSphere Commerce 서버에서 사용자의 브라우저로 이동할 때 필요합니다. 79 페이지의 제 8 장『IBM HTTP Server를 사용한

프로덕션을 위한 SSL 사용』에 설명된 대로, SSL(Secure Sockets Layer)을 사용하는 것이 이 시나리오에 대한 기밀성을 제공합니다.

기밀성은 또한 세션 관리 영역에서 강력한 요구사항입니다. HTTP(Hypertext Transfer Protocol) 프로토콜이 stateless이기 때문에 *쿠키*가 사용자를 WebSphere Commerce 서버에 지속적으로 식별하는 데 널리 사용됩니다. 이 쿠키가 도난되는 경우, 사용자 계정이 손상될 수 있습니다. 이것을 일반적으로 *세션 도난*이라고 합니다. WebSphere Commerce는 63 페이지의 제 6 장 『세션 관리』에 설명된 대로 쿠키 스펙의 고유한 특징을 사용하여 세션 도난을 방지합니다.

제 2 장 인증

WebSphere Commerce는 인증을 사용자 또는 응용프로그램이 주장하는 정체성이 맞는지를 검증하는 처리로 봅니다. 이 절에서는 WebSphere Commerce 인증의 여러 측면을 자세히 설명합니다.

WebSphere Application Server 인증 모델

WebSphere 인증은 인증 데이터의 유형과, 사용자 인증 데이터가 들어 있는 사용자 레지스트리를 바탕으로 합니다. 인증을 위해 사용자 ID와 암호가 제공되는 경우, 인증은 사용자 레지스트리에 위임됩니다. 인증을 위해 디지털 인증이 사용되는 경우, 인증 신임장이 연관된 사용자 레지스트리 항목에 맵핑됩니다.

	Unix	**Windows**	**LDAP 사용자 레지스트리**	**사용자 정의 사용자 레지스트리**
운영체제 (사용자 ID와 암호)	인증은 시스템 호출이 사용자 ID 및 암호의 유효성을 검증하게 하여 시스템에 위임됩니다.	인증은 시스템 호출이 사용자 ID 및 암호의 유효성을 검증하게 하여 Windows Security Access Manager에 위임됩니다.	없음	없음
운영체제 (디지털 인증)	없음	없음	없음	없음
LPTA (사용자 ID와 암호)	없음	없음	주어진 사용자 ID와 암호에 대한 DN(인식 이름)을 사용하여 LDAP 바인드가 수행됩니다.	checkPassword 호출이 사용자 정의 레지스트리에 대해 수행됩니다.
LPTA (디지털 인증)	없음	없음	웹 서버의 신뢰도를 바탕으로 인증 컨텐츠가 LDAP 항목에 신임 맵핑됩니다.	웹 서버의 신뢰도를 바탕으로 인증 컨텐츠가 mapCertificate 메소드 호출을 사용하여 신임 맵핑됩니다.

인증 메커니즘이 LTPA(Lightweight Third Party Authentication)인 경우, 인증은 제삼자 서버에 위임됩니다. 사용자 ID와 암호가 사용 가능한 경우, LDAP 디렉토리 중 하나에 대해 검증됩니다. 이것은 `checkPassword` 메소드를 호출하여 레지스트리 또는 사용자 정의 사용자 레지스트리에 대해 LDAP 바인드를 수행하여 완료됩니다. LTPA 토큰이 사용 가능한 경우, 클라이언트 동일성을 설정하기 위해 해당 토큰이 제삼자 서버에 의해 검증됩니다.

디지털 인증이 인증 데이터인 경우, 사용자는 웹 클라이언트와 웹 서버 사이에 상호 SSL 연결을 설정해야 합니다. 이 경우, WebSphere는 웹 서버에 있는 자신의 신뢰도를 바탕으로 인증이 사용자에게 속한다고 믿습니다. 그런 다음 인증에 존재하는 사용자 정보(예: DN)가 일치하는 사용자 항목을 찾기 위해 사용자 레지스트리(LDAP 또는 사용자 정의 사용자 레지스트리)에 맵핑됩니다.

WebSphere Application Server는 여러 가지 인증 메커니즘 중 하나를 사용하여 사용자를 인증합니다. J2EE는 엔터프라이즈 bean 컨테이너를 인증하는 방법을 지정하지 않습니다. 그러나 WebSphere는 SAS(Secure Association Service)를 사용하여 Java 클라이언트를 엔터프라이즈 bean에 인증합니다. 웹 자원에 대한 인증 메커니즘은 웹 응용프로그램에 대한 `web.xml` 배치 설명자의 `login-config` 요소를 사용하여 지정됩니다. 엔터프라이즈 응용프로그램에 있는 각 웹 응용프로그램은 서로 다른 `login-config` 값을 지정할 수 있습니다. 다음은 `formlogin`이 지정되는 `login-config` 요소의 예입니다.

```
<login-config>
  <auth-method>FORM</auth-method>
  <realm-name>Example Form-Based Authentication</realm-name>
  <form-login-config>
    <form-login-page>/login.html</form-login-page>
    <form-error-page>/error.jsp</form-error-page>
  </form-login-config>
</login-config>
```

인증 데이터

이 절에서는 WebSphere Commerce가 사용하는 인증 데이터의 유형에 대해 설명합니다.

챌린지 메커니즘

챌린지 메커니즘은 서버가 인증 데이터를 요구하고 사용자로부터 검색하는 방법을 지정합니다. WebSphere Application Server Servlet 스펙이 다음 인증 방법이나 챌린지 메커니즘을 식별합니다.

기본 인증(사용자 ID와 암호)

이것은 사용자가 보호 웹 자원에 액세스하려 시도할 때 웹 브라우저가 사용자에게 사용자 ID와 암호를 입력하도록 요청하는 대화 창을 표시하는 친숙한 인증 스타일입니다.

사용자가 식별자와 암호를 제공한 후 보안 서비스가 알려진 사용자의 데이터베이스인 사용자 레지스트리에 대해 입력된 정보의 유효성 검증합니다. 사용자가 제공한 정보가 올바른 경우, 보안 시스템은 사용자가 인증된 것으로 간주합니다. 이 버전에서는 레지스트리가 로컬 운영체제 레지스트리여야 합니다.

챌린지는 대개 다음 방법으로 발생합니다.

1. 웹 서버가 HTTP 권한이 없는 클라이언트 오류(401) 코드와 WWW_Authenticate 머리글을 발행합니다.
2. 웹 브라우저가 대화 상자 창을 팝업합니다.
3. 사용자가 이 대화 상자 창에 사용자 ID와 암호를 입력합니다.
4. 정보가 웹 서버로 보내집니다.
5. 웹 서버에 첨부된 플러그인이 정보를 추출하고 인증합니다.

기본 챌린지 유형은 LPTA 또는 원시 운영체제 인증 메커니즘 중 하나를 사용할 때 올바른 선택입니다.

다이제스트 인증

이 인증 메커니즘은 WebSphere에서 지원되지 않습니다. 다른 인증 메커니즘 중 하나를 지정해야 합니다.

양식 기반 또는 사용자 정의 인증

이 인증 메커니즘은 HTML 페이지나 JSP 양식을 통한 사이트 고유의 로그인을 허용합니다.

이 유형의 챌린지 메커니즘은 기본 챌린지 유형에서와 같이 401 오류 코드를 보내는 것과는 반대로 HTML 양식을 사용하여 사용자 ID와 암호를 검색하도록 서버를 구성하려는 경우에 유용합니다. 시스템 운영자가 자원을 요청하는 사용자가 인증되기 위해 경로 재지정되는 URL을 지정합니다. 이 챌린지 유형은 인증 메커니즘이 LPTA일 때와 단일 사인온이 사용될 때만 지원됩니다.

인증 기반 인증(X.509 인증)

인증 챌린지 메커니즘은 웹 서버가 SSL을 통해 상호 인증을 수행하도록 구성됨을 의미합니다. 클라이언트는 연결을 설정하기 위해 인증을 제시해야 합니다. 그런 다음 이 인증이 사용자 레지스트리에 신임 맵핑됩니다.

WebSphere Application Server에서 LDAP 디렉토리는 인증 기반 인증을 지원하도록 구성할 수 있는 유일한 레지스트리입니다. 그러므로 인증 기반 챌린지를 사용하려면 LTPA를 인증 메커니즘으로 사용해야 합니다.

사용자 레지스트리

사용자 레지스트리는 사용자와 그룹 정보 및 사용자의 인증 정보(예: 암호)가 들어 있는 사용자 저장소의 캡슐화입니다. 프린시펄(즉, 사용자 레지스트리에 있는 인간 사용자 또는 시스템 엔티티의 표현)에 의해 제공되는 인증 정보는 사용자 레지스트리에 의해 검증 또는 유효성 검증될 수 있습니다. 사용자 레지스트리는 또한 권한을 구성할 때 사용자 및 그룹 정보를 얻기 위해 참조됩니다.

각 WebSphere 관리 도메인은 하나의 사용자 레지스트리를 사용하여 사용자 인증 및 특권 데이터를 제공합니다. 관리 도메인은 관리 저장소를 공유하는 하나 이상의 WebSphere 관리 서버의 세트입니다. 관리 저장소는 시스템 구성 데이터를 보유하는 데이터베이스입니다.

사용자 레지스트리에는 프린시펄의 인증 정보(예: 암호)와 특권 속성(예: 그룹)이 들어 있습니다. 모든 운영체제가 이러한 사용자 레지스트리를 지원합니다. 대부분의 시스템에서 사용자 레지스트리는 원시 운영체제 사용자 도메인(예: UNIX의 `/etc/password`) 또는 네트워크 사용자 도메인(예: NT SAM 또는 LDAP 사용자 레지스트리)에 맵핑됩니다.

WebSphere는 LDAP 사용자 레지스트리와 원시 운영체제의 두 사용자 도메인을 바탕으로 하는 사용자 레지스트리를 지원합니다. Windows NT 운영체제의 경우, NT Domain 및 NT WorkGroup 레지스트리가 지원됩니다.

WebSphere Application Server Advanced Edition 4.0은 다음 LDAP 제공자를 지원합니다.

- IBM SecureWay Directory
- Domino 4.6 및 5.0 디렉토리
- Netscape Directory Server
- Windows2000 Active Directory

프린시펄

프린시펄은 액세스 동일성, 그룹 동일성 및 기타를 포함하여 그와 연관된 특권 속성 세트가 있습니다. 프린시펄은 다음과 같은 액세스 제어를 위한 다양한 특권 속성이 있습니다.

- *보안 이름*은 프린시펄 이름의 독자에게 친숙한 버전입니다. 프린시펄은 그와 연관된 보안 이름을 가질 수 있습니다. 보안 이름은 해당 액세스 동일성을 변경하지 않고 변경될 수 있습니다. 일반적으로 일반 사용자만이 해당 보안 이름을 다룹니다. 보안 이름과 연관된 다양한 동일성이 존재하는 경우, 보안 시스템에서 다루는 범위 안에서 사용됩니다. 예를 들어, 프린시펄이 보안 이름 `bobs`가 있습니다.
- 액세스 ID는 프린시펄의 액세스 동일성입니다. 일반적으로 레지스트리에 따라 달라지며 읽을 수 없는 문자열입니다. 프린시펄의 액세스 ID는 고유하며 사용자 레지스트리에 고유한 동일성을 나타냅니다. AIX 또는 Solaris 레지스트리의 경우에는 uid이며, NT 레지스트리의 경우 SID이고 LDAP 사용자 레지스트리의 경우 DN입니다. WebSphere는 액세스 제어 정보(역할이라고도 함)를 이들 특권 속성과 연관시킵니다. 따라서 이들을 *액세스* 동일성이라고 합니다. 예를 들어, 프린시펄 Bob Smith와 연관된 액세스 ID가 `ldapserver.mycompany.com/cn=Bob Smith, ou=Employee, o=MyCompany`일 수 있습니다.

인증 메커니즘

*인증 메커니즘*은 연관된 사용자 레지스트리에 대해 인증 데이터를 검증하여 사용자를 인증하고 실행 스레드에서 사용자 동일성과 연관될 수 있는 신임장을 발행합니다. 예를 들어 인증 메커니즘이 LTPA인 경우, 사용자에 관한 정보가 들어 있는 LDAP 디렉토리가 인증이 수행되는 사용자 레지스트리로 간주됩니다. 일단 사용자 ID와 암호가 검증되면 LTPA 인증 메커니즘이 다운스트림 호출에서 안전하게 위임될 수 있는 LTPA 토큰을 포함하는 신임장을 발행합니다.

다음은 지원되는 인증 메커니즘입니다.

- LTPA(LDAP 사용자 레지스트리 또는 사용자 정의 사용자 레지스트리)
- 로컬 운영체제 인증 메커니즘(사용자 레지스트리: NT, AIX 또는 Solaris)

LTPA를 인증 메커니즘으로 사용할 때 신뢰되는 제삼자 서버가 사용자를 인증하는 데 사용됩니다. 이런 경우, LDAP 디렉토리 또는 사용자 정의 사용자 레지스트리가 구성되어야 합니다. 인증은 다음과 같이 진행됩니다.

1. LTPA 서버가 다음 중 하나를 수행합니다.
   - 주어진 사용자 ID를 바탕으로 사용자 항목에 대한 LDAP 디렉토리에 대해 검색을 수행한 후 검색된 DN(인식 이름)과 암호를 사용하여 LDAP 바인드를 수행합니다.
   - `CustomRegistry` 구현에서 `checkPassword` 메소드를 호출합니다.
2. LDAP 바인드 또는 `checkPassword` 호출이 완료되면 LTPA 토큰이 사용자에게 발행됩니다. 해당 사용자의 다운스트림 요청은 이 토큰의 유효성 검증을 바탕으로 합니다.
3. 단일 사인온이 사용되는 경우에는 LTPA 토큰이 사용자의 브라우저에 LTPA 쿠키로서 저장됩니다. 그 결과, 동일한 사용자의 후속 요청은 쿠키에 들어 있는 토큰의 유효성을 검증하여 인증됩니다.

원시 운영체제를 인증 메커니즘으로 사용할 때 인증은 주어진 데이터를 인증하기 위해 원시 루틴을 호출하는 기본 운영체제의 사용자 레지스트리를 바탕으로 합니다. 이 인증 메커니즘에 의해 발행되는 신임장은 안전하게 위임할 수 있는 신임장이 아닙니다. 그러므로 이 인증 메커니즘 모드는 단일 서버 단일 노드 시나리오에서만 지원됩니다. WebSphere 도메인에 둘 이상의 응용프로그램 서버(또는 노드)가 있는 경우, 유일하게 지원되는 인증 메커니즘은 LTPA입니다.

Unix 운영체제(AIX 및 Solaris)의 경우에는 사용자가 제공하는 암호가 암호화되고 암호 파일(예: `/etc/passwd`)에 저장된 암호와 비교됩니다. Windows NT 운영체제의 경우에는 주어진 사용자에 대한 암호를 검증하기 위해 NT 보안 시스템에 대한 시스템 호출이 이루어집니다.

어느 경우에나 인증은 특권이 부여된 동일성 아래에서 실행되어야 합니다. AIX 또는 Solaris의 경우에는 일반적으로 root 사용자입니다. Windows NT의 경우에는 시스템 운영자가 WebSphere AdminServer 서비스와 연관된 사용자 ID에 Act as operating system 특권을 지정해야 합니다.

인증 유효성 검증

이것은 서버가 X.509 클라이언트 인증을 신뢰하는지 검증하는 처리이며 또한 WebSphere Commerce 데이터베이스에 정의되는 인증 정책을 따릅니다.

LDAP 바인드

이것은 사용자를 인증하기 위해 LDAP 바인드 조작을 수행하여 제공된 챌린지 정보가 올바른지 검증하는 처리입니다.

데이터베이스 바인드

이것은 인증 처리 중에 제공되는 사용자 ID와 암호가 WebSphere Commerce 데이터베이스에 저장된 인증 정보와 비교할 때 올바른지 검증하는 처리입니다.

신임장

WebSphere 서버는 인증서, 토큰 또는 사용자 ID와 암호 쌍 같은 신임장 유효성 검증을 바탕으로 하는 인증 메커니즘을 지원합니다. 신임장은 이러한 설계를 지원하는 사용자 레지스트리에 대해 검증됩니다. 예를 들어, 사용자 ID와 암호 기반 인증은 인증이 LDAP 바인드를 사용하여 수행되는 LDAP 사용자 레지스트리에 대해 수행될 수 있습니다.

LTPA 토큰

LTPA 토큰은 사용자가 요청하는 자원에 대한 액세스 권한을 판별하는 데 필요한 사용자 정보가 들어 있는 데이터입니다. 여기에는 LTPA 서버의 디지털 서명과 함께 인증 데이터가 들어 있습니다.

LTPA 설계의 경우에는 사용자에 관한 정보가 들어 있는 LDAP 디렉토리가 인증이 수행되는 사용자 레지스트리입니다. 자원 서버는 보안 서버에 접속하여 LTPA가 인증 메커니즘이 되도록 지정합니다. 또한 요청과 연관된 인증 데이터를 제공합니다. 그러면 보안 서버는 LTPA 서버에 대해 인증 데이터의 유효성을 검증하고 LTPA 토큰을 리턴합니다. 사용자의 후속 요청은 이 LTPA 토큰의 유효성을 검증하여 인증됩니다.

WebSphere Commerce 토큰(쿠키 기반 세션 관리)

쿠키 기반 세션 관리가 사용될 때 사용자의 정보가 들어 있는 메시지(쿠키)가 웹 서버에 의해 브라우저로 보내집니다. 이 쿠키는 사용자가 특정 페이지에 액세스하려 시도할 때 다시 서버로 보내집니다. 쿠키를 다시 보내면 서버는 사용자를 식별하고 세션 데이

터베이스에서 사용자의 세션을 검색할 수 있으므로 사용자의 세션을 관리합니다. 쿠키 기반 세션은 사용자가 로그오프하거나 브라우저를 닫을 때 종료합니다. 쿠키 기반 세션 관리는 안전하며 성능상의 이점을 갖습니다. 쿠키 기반 세션 관리가 구매자 세션에 권장됩니다. URL 재작성을 사용하지 않고 사용자가 자신의 브라우저에서 쿠키를 사용하게 하려는 경우, 구성 관리자의 세션 관리 페이지에서 **쿠키 수용 테스트**를 선택하십시오.

보안상의 이유로 쿠키 기반 세션 관리는 다음 두 유형의 쿠키를 사용합니다.

- 비보안 세션 쿠키

  세션 데이터를 관리하는 데 사용됩니다. 세션 ID, 협상된 언어, 현재 상점 및 쿠키가 구성될 때의 구매자 선호 통화가 들어 있습니다. 이 쿠키는 SSL 또는 non-SSL 연결을 통해 브라우저와 서버 사이에 이동할 수 있습니다. 비보안 세션 쿠키에는 다음 두 유형이 있습니다.

  – WebSphere Application Server 세션 쿠키는 Servlet HTTP 세션 표준을 바탕으로 하며 WebSphere Application Server의 모든 문서에서 발견할 수 있습니다. WebSphere Application Server 쿠키는 메모리 또는 다중 노드 배치의 데이터베이스로 지속됩니다.

  – WebSphere Commerce 세션 쿠키는 WebSphere Commerce에 내부적이며 데이터베이스로 지속되지 않습니다.

  사용할 쿠키 유형을 선택하려면 구성 관리자의 세션 관리 페이지에 있는 **쿠키 세션 관리자** 매개변수에 대해 `WCS` 또는 `WAS`를 선택하십시오.

- 보안 인증 쿠키

  인증 데이터를 관리하는 데 사용됩니다. 인증 쿠키는 SSL을 통해 이동하며 최대 보안을 위해 시간소인이 붙습니다. 이것은 사용자를 인증하는 데 사용되는 쿠키이지만, 중요한 명령, 예를 들어, 사용자에게 신용 카드 번호를 묻는 `DoPaymentCmd`가 실행됩니다. 이 쿠키가 도난되어 권한이 없는 사용자에 의해 사용될 수 있는 아주 작은 위험이 있습니다. 쿠키 기반 세션 관리가 사용될 때마다 인증 코드 쿠키가 WebSphere Commerce에 의해 항상 생성됩니다.

세션 및 인증 코드 쿠키가 모두 보안 페이지를 보기 위해 필요합니다.

쿠키 오류에 대해 `CookieErrorView`가 다음 경우에 호출됩니다.

- 사용자가 동일한 로그온 ID를 갖고 다른 위치에서 로그인했습니다.
- 쿠키가 손상되었거나 부당하게 변경되었습니다.
- 쿠키 수용이 `true`로 설정되고 사용자의 브라우저가 쿠키를 지원하지 않습니다.

단일 사인온 지원

HTTP 단일 사인온 이면의 철학은 복수 HTTP 요청 사이에서 사용자 인증을 보존하는 것입니다. 목적은 다음과 같습니다.

- 다음을 포함한 주어진 신뢰 도메인 안에서 보안 신임장에 대해 사용자에게 여러 번 프롬프트하는 것을 피하기 위해:
  - 협동하지만 본질적으로 다른 웹 서버
  - Domino 서버 같은 협동 응용프로그램
- 사인온 만기를 지원하기 위해

단일 사인온(SSO) 시나리오에서 HTTP 쿠키가 모든 새 클라이언트-서버 세션(기본 인증 가정)에 대해 사용자가 인증 정보를 입력하는 부담을 덜기 위해 사용자의 인증 정보를 이종의 웹 서버에 전달하는 데 사용됩니다. 단일 사인온은 LTPA가 선택된 인증 메커니즘인 경우 구성 가능한 옵션입니다. WebSphere 운영자는 SSO가 적용되는 네트워크 도메인을 지정해야 합니다.

예를 들어 도메인이 mycompany.com으로 지정되는 경우, SSO는 a.mycompany.com 및 b.mycompany.com 같이 mycompany.com 도메인을 제공하는 모든 웹 서버에 적용됩니다. 사용자의 첫 번째 요청을 처리하는 웹 서버가 SSO를 수행할 쿠키를 작성합니다. 이 경우, 로그인 URL도 지정된 도메인에 들어가야 합니다(예: http://www.mycompany.com/finance/login.html).

HTTP 쿠키를 지원하는 HTTP 클라이언트(웹 브라우저)에 있는 사용자가 자원을 요청할 때 웹 서버가 HTTP 쿠키의 양식으로 사용자의 토큰 신임장(LTPA 토큰)을 작성합니다. 쿠키의 domain 부분이 쿠키가 유효해야 하는 네트워크 도메인입니다. 예를 들어 도메인 값이 WebSphere 구성에서 mycompany.com으로 설정되는 경우, 브라우저는 해당 도메인에 상주하는 모든 웹 서버에 이 쿠키를 제시합니다. 도메인의 웹 서버가 인증을 수행할 때 LTPA 쿠키를 찾습니다. LTPA 쿠키가 있는 경우, 웹 서버는 쿠키에서 LTPA 토큰을 추출하고 유효성을 검증합니다.

WebSphere 운영자는 LTPA 토큰에 대한 만기 시간을 지정할 수 있습니다. 기본적으로 30분으로 설정되며, 그 후에는 사용자가 재인증해야 합니다. 쿠키가 지속적이지 않도록 하기 위해 쿠키에 대한 만기 시간은 브라우저의 활동 시간으로 설정됩니다.

SSO가 보안 세션에서만 사용되도록 구성되는 경우, 쿠키의 secure 필드가 on으로 설정됩니다. 이것은 쿠키가 SSL 연결을 통해서만 이동하도록 보장합니다.

단일 사인온은 또한 WebSphere(3.5 이상)와 LTPA 토큰 메커니즘을 사용하는 Domino(5.05 이상) 서버 사이에서도 지원됩니다.

WebSphere 4.0에서 LTPA 메커니즘을 사용하는 단일 사인온은 Advanced Edition에서만 지원되며 Advanced Edition Single Server에서는 지원되지 않습니다. Advanced

Edition Single Server의 경우에는 사용자 동일성이 HTTP 세션의 일부로 보유되며, 따라서 해당 개정판에서 사용자는 웹 응용프로그램 액세스당(컨텍스트 루트를 바탕으로) 한 번만 프롬프트됩니다. 다시 말하면, 사용자는 해당 브라우저 세션 안에서 사용자가 액세스하는 웹 응용프로그램의 수만큼 사용자 ID와 암호(예를 들어, 양식 기반 로그인을 사용할 때)를 입력하도록 프롬프트될 수 있습니다.

WebSphere Commerce에서의 단일 사인온을 구현하는 단계는 87 페이지의 제 10 장 『단일 사인온』을 참조하십시오.

인증 정책

인증은 사용자가 자신에 대해 주장하는 사람인지를 검증하는 처리입니다. 인증은 일반적으로 두 단계로 수행됩니다.

1. 프린시펄의 인증 데이터 획득
2. 사용자 레지스트리에 대한 인증 데이터 검증

WebSphere 보안은 프린시펄이 요청한 자원과 연관된 인증 정책을 바탕으로 프린시펄을 인증합니다. 사용자가 웹 서버나 WebSphere Application Server로부터 보호 자원을 요청할 때 서버가 사용자를 인증합니다.

WebSphere 서버는 인증서, 토큰 또는 사용자 ID와 암호 쌍 같은 신임장의 유효성 검증을 바탕으로 하는 인증 메커니즘을 지원합니다. 신임장은 이러한 설계를 지원하는 사용자 레지스트리에 대해 검증됩니다. 예를 들어, 사용자 ID와 암호 기반 인증은 인증이 LDAP 바인드를 사용하여 수행되는 LDAP 사용자 레지스트리에 대해 수행될 수 있습니다.

WebSphere 서버는 또한 제삼자 인증 설계를 지원합니다. 클라이언트와 서버 프린시펄은 상호 신뢰하는 제삼자인 LTPA 서버에 인증됩니다. 모든 인증 설계는 클라이언트가 서버를 신뢰하지 않으며 서버가 클라이언트를 신뢰하지 않는다고 가정해야 합니다(서버가 다른 서버에 클라이언트로서 작용할 때 이와 동일한 프린시펄이 서버에 적용됩니다). 제삼자 인증 메커니즘의 주된 장점은 사용자 레지스트리가 중앙집중적으로 관리된다는 점입니다.

사용자와 웹 서버 및 WAS 사이의 인증을 수행하기 위한 인증 정책은 웹 응용프로그램의 배치 설명자의 일부로서 J2EE 로그인 구성 태그의 형식으로 지정될 수 있습니다.

- `auth-method` 설명자를 사용한 인증 방법
- 보안 채널에 대한 요구사항을 지정하는 데이터 제한자
- 양식 기반 인증을 위한 양식 구성

세션 정책

WebSphere Commerce 5.4에서 세션 정책은 로그인 시간 종료 정책에 포함됩니다.

로그인 시간 종료 정책을 사용할 때 WebSphere Commerce는 장시간 동안 활동하지 않는 사용자를 로그오프하고 해당 사용자에게 로그인 시간 종료 노드를 사용하여 시스템에 다시 로그온할 것을 요청합니다. 이러한 개선사항을 WebSphere Commerce 구성 관리자를 통해 호출되며 43 페이지의 『구성 관리자 - 로그인 시간 종료』에서 자세히 설명됩니다.

계정 정책

다음 절에서는 WebSphere Commerce에서 사용 가능한 계정 정책에 대해 설명합니다.

계정 정책

WebSphere Commerce 운영자의 계정 정책 페이지를 사용하여 계정 정책을 설정할 수 있습니다. 계정 정책은 암호 및 계정 잠금 정책 같은 계정 관련 정책을 정의합니다.

계정 정책을 작성한 후에는 사용자에게 해당 정책을 지정할 수 있습니다. 계정 정책이 사용 중인 경우(즉, 사용자에게 계정 정책이 지정된 경우) 계정 정책을 삭제할 수 없음에 유의하십시오.

계정 정책 작성에 대한 자세한 내용은 50 페이지의 『운영자 - 계정 정책』을 참조하십시오.

또한 WebSphere Commerce 온라인 도움말의 참조 주제 "기본 인증 정책"도 참조하십시오.

계정 잠금 정책

WebSphere Commerce 운영자의 계정 잠금 정책 페이지를 사용하여 WebSphere Commerce 내의 여러 사용자 역할에 대한 계정 잠금 정책을 설정할 수 있습니다. 계정 잠금 정책은 사용자 계정에 대해 나쁜 의도의 조치가 실행되는 경우 조치가 계정을 손상시키는 기회를 줄이기 위해 해당 계정을 사용 불가능하게 만듭니다.

계정 잠금 정책은 다음 항목을 강제 시행합니다.

- 계정 잠금 임계값. 이것은 계정이 사용되기 전의 올바르지 않은 로그온 시도 횟수입니다.
- 연속 실패 로그인 지연. 이것은 두 번의 로그인 시도 실패 후에 사용자가 로그인할 수 없는 기간입니다. 연속으로 로그인에 실패할 때마다 지연이 구성된 시간 지연 값(예: 10초)만큼 증가됩니다.

계정 잠금 정책 작성에 대한 자세한 내용은 52 페이지의 『운영자 - 계정 잠금 정책』을 참조하십시오.

암호 정책

다음 절에서는 WebSphere Commerce에서 사용 가능한 암호 정책에 대해 설명합니다.

암호 정책

WebSphere Commerce 운영자의 암호 정책 페이지를 사용하면 암호의 특성을 정의하여 암호가 사이트의 보안 정책을 따르도록 보장하기 위해 사용자의 암호 선택을 제어할 수 있습니다.

이 기능은 암호가 따라야 하는 속성을 정의합니다. 암호 정책은 다음 조건을 강제 시행합니다.

- 사용자 ID와 암호가 일치할 수 있는지 여부
- 연속 문자의 최대 발생
- 모든 문자의 최대 인스턴스 수
- 암호의 최대 수명
- 최소 영문자 수
- 최소 숫자 수
- 최대 암호 길이
- 사용자의 이전 암호의 재사용 가능 여부

암호 정책 작성에 대한 자세한 내용은 51 페이지의 『운영자 - 암호 정책』을 참조하십시오.

또한 WebSphere Commerce 온라인 도움말의 참조 주제 "기본 인증 정책"도 참조하십시오.

암호 무효화

암호 무효화 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 암호 무효화 노드를 사용하십시오. 이 기능이 사용될 때 WebSphere Commerce 사용자는 사용자의 암호가 만기되면 암호를 변경해야 합니다. 그 경우, 사용자에게 암호를 변경해야 하는 페이지가 경로 재지정됩니다. 사용자는 암호를 변경할 때까지 사이트의 어떤 보안 페이지에도 액세스할 수 없습니다.

암호 무효화 노드 사용에 대한 자세한 내용은 44 페이지의 『구성 관리자 - 암호 무효화』를 참조하십시오.

암호로 보호된 명령

암호로 보호된 명령 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 암호로 보호된 명령 노드를 사용하십시오. 이 기능이 사용될 때 WebSphere Commerce는 WebSphere Commerce에 로그온된 등록 사용자가 지정된 WebSphere Commerce 명령을 실행하는 요청을 계속하기 전에 암호를 입력하도록 요구합니다.

주의: 암호로 보호된 명령을 구성할 때 명령 선택사항 목록에 표시된 명령의 일부는 일반 또는 게스트 사용자에 의해 실행될 수 있습니다. 이러한 명령을 암호로 보호된 명령

으로 구성하면 일반 및 게스트 사용자가 해당 명령을 실행하는 데 제한을 받습니다. 그러므로 암호로 보호될 명령을 구성할 때 주의해야 합니다.

주: WebSphere Commerce는 `authenticated`로 지정되거나 사용 가능한 명령 목록의 `URLREG` 테이블에서 `https` 플래그가 설정된 명령만을 표시합니다.

암호로 보호된 명령 노드 사용에 대한 자세한 내용은 44 페이지의 『구성 관리자 - 암호로 보호된 명령』을 참조하십시오.

제 3 장 인증(액세스 제어)

WebSphere Commerce는 사용자 또는 응용프로그램이 자원에 액세스하기 위한 충분한 권한이 있는지 검증하는 처리로 인증을 봅니다. 이 절에서는 WebSphere Commerce 권한 또는 액세스 제어의 여러 측면을 자세히 설명합니다.

WebSphere Commerce에서 권한 또는 액세스 제어는 액세스 제어 정책을 사용하여 수행됩니다. 액세스 제어 정책은 어떤 그룹의 사용자가 자원 세트에 대해 조치 세트를 수행할 수 있는지를 설명하는 규칙입니다. WebSphere Commerce는 기본 액세스 제어 정책 세트를 제공합니다. 이들 기본 액세스 제어 정책은 XML 형식으로 지정되며 전자상거래 사이트에 필요한 여러 일반 액세스 제어 요구사항을 해결하도록 설계됩니다. WebSphere Commerce의 액세스 제어 구성요소를 이해하려면 먼저 전자상거래 사이트의 일반적인 조직 계층을 이해해야 합니다.

조직 계층

WebSphere Commerce 구성원 서브시스템 안에서 사용자와 조직 엔티티는 하나의 계층으로 구성됩니다. 일반적으로 이 계층은 조직 및 조직 단위에 대한 항목과, 리프 노드에 있는 사용자에 대한 항목이 있는 일반적인 조직 계층을 에뮬레이트합니다. 계층은 맨 위에 *루트 조직*이라는 부르는 인공적인 조직 엔티티를 포함합니다. 기타 모든 조직 엔티티와 사용자는 이 루트 조직의 하위입니다. 루트 조직 아래에 하나의 판매자 조직과 여러 구매자 조직이 있을 수 있는데, 이 모든 조직은 그 아래에 하나 이상의 하위 조직이 있습니다. 조직 운영자는 조직의 수장이며 조직 유지보수를 담당합니다. 판매자 조직측에서 각 판매자 조직은 그 안에 하나 이상의 상점이 있습니다. 상점 운영자는 상점 유지보수를 담당합니다. 아래 도표에서는 B2B 전자상거래 사이트의 조직 계층을 보여줍니다.

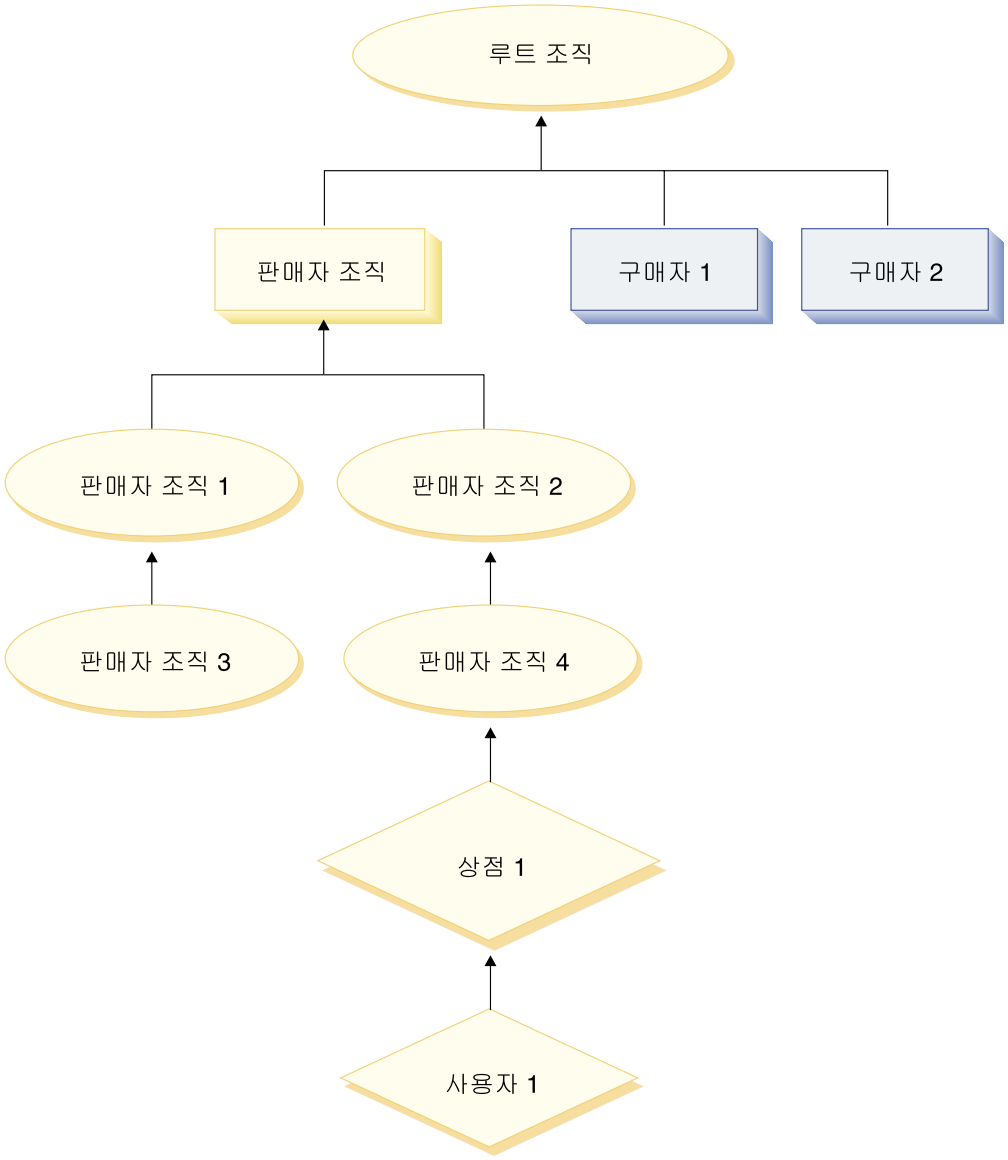

그림 1. B2B 사이트의 조직 계층

루트 조직

루트 조직은 조직 계층의 맨 위에 있습니다. *사이트 운영자* 역할을 갖는 사용자가 루트 조직 관리를 담당합니다. 사이트 운영자는 WebSphere Commerce 및 연관된 소프트웨어와 하드웨어를 설치, 구성 및 유지보수합니다. 이 역할은 일반적으로 액세스 및 권한(즉, 구성원 작성 및 적당한 역할에 구성원 지정)을 제어하고 웹 사이트를 관리합니다. 사이트 운영자는 상점 운영자와 기타 모든 운영자뿐 아니라 운영자가 액세스하는 조직을 지정할 수 있습니다. 사이트 운영자는 권한 부여된 당사자만이 기밀 정보에 액세스할 수 있도록 각 운영자에게 암호를 지정해야 합니다. 이것은 카탈로그 갱신 또는 RFQ 승인 같은 핵심 책임을 제어하는 수단을 제공합니다.

WebSphere Commerce 사이트에는 하나의 판매자 조직이 있습니다. B2B 사이트에는 하나 이상의 구매자 조직도 있습니다. 사이트 운영자는 판매자 조직(상점을 소유하는 조직)의 액세스 제어 정책과, 해당 상점에서 구매하는 각 조직의 액세스 제어 정책을 둘 다 정의할 수 있습니다. B2C 사이트에는 구매자 조직이 없습니다. B2C 고객은 기본 조직의 구성원으로 모델링됩니다.

조직(구매자)

B2B 사이트에서 사이트 운영자는 비즈니스 수요에 따라서 하나 이상의 구매자 조직을 작성합니다. 그런 다음 사이트 운영자는 구매자 조직에 대한 모든 특별 액세스 제어 정책을 정의하고 구매자 조직을 관리할 구매자 관리자를 지정합니다. 구매자 관리자는 사용자를 등록하고 해당 조직과 관련된 액세스 제어 정책에 따라서 사용자에게 조직의 비즈니스 수요에 맞는 여러 가지 역할을 지정합니다.

사이트 운영자가 적당한 경우 구매자 조직의 액세스 제어 정책을 수정 및 관리할 수 있음에 유의하십시오.

조직(판매자)

B2B 및 B2C 사이트 모두에서 사이트 운영자는 하나의 최상위 레벨 판매자를 작성합니다. 이 판매자 조직 아래에 다른 하위 조직 또는 조직 단위가 작성될 수 있습니다. 이러한 모든 판매측 조직 엔티티는 하나 이상의 상점을 소유할 수 있습니다. 그런 다음 사이트 운영자는 판매자 조직에 대한 모든 특별 액세스 제어 정책을 정의하고 해당 조직을 관리할 판매자 관리자를 지정합니다. 판매자 관리자는 사용자를 등록하고 해당 조직과 관련된 액세스 제어 정책에 따라서 사용자에게 조직의 비즈니스 수요에 맞는 여러 가지 역할을 지정합니다.

판매자 관리자의 책임은 다음과 같이 요약됩니다.

- 상점을 소유할 조직을 작성합니다. 선택적으로 조직 내에서 승인이 필요한 처리를 정의합니다. 이 단계는 B2B 사이트에만 필요합니다.
- 조직에 역할을 지정합니다.
- 사용자를 작성합니다.
- 사용자에게 역할을 지정합니다.

구성원 그룹: 사용자 그룹과 액세스 그룹

WebSphere Commerce의 구성원 서브시스템을 사용하여 구성원 그룹을 작성할 수 있는데, 이 그룹은 여러 비즈니스 이유 때문에 범주화되는 사용자의 그룹입니다. 그룹화는 여러 목적을 위해 사용될 수 있는데, 액세스 제어 목적, 승인 목적, 할인과 가격 계산 및 상품 전시 같은 마케팅 목적이 포함됩니다. `user group` 유형의 구성원 그룹은 일반적인 사용을 위한 반면, `access group` 유형의 구성원 그룹은 액세스 제어가 목적입니다.

user group 유형의 구성원 그룹은 공통적인 관심을 공유하는 판매자로 정의되는 사용자의 콜렉션입니다. 사용자 그룹은 큰 상점이 단골 고객이나 우수 고객을 위해 제공하는 클럽과 유사합니다. 사용자 그룹의 일부가 되면 고객은 상품 구매시 할인이나 기타 보너스를 얻을 자격이 생길 수 있습니다. 예를 들어 시장 조사에서 장년층 고객이 반복적으로 여행 가이드와 여행 가방을 구매하는 것으로 나타나는 경우, 해당 고객들을 Seniors' Travel Club이라는 구성원 그룹에 지정할 수 있습니다. 비슷하게 단골 고객에게 비즈니스에 대해 보상하는 사용자 그룹을 작성할 수 있습니다.

access group 유형의 구성원 그룹은 액세스 제어를 목적으로 사용자를 그룹화하기 위한 것입니다. 액세스 그룹은 액세스 제어 정책의 한 요소입니다. 액세스 그룹의 멤버쉽은 대개 암시적으로 정의됩니다. 구성원 그룹의 멤버쉽을 정의하는 암시적 조건은 MBRGRP 테이블의 CONDITIONS 열에 있습니다. 또한 사용자를 명시적으로 구성원 그룹에 추가할 수 있습니다. 마찬가지로, 명시적으로 사용자를 구성원 그룹에서 제거할 수 있습니다. 이러한 명시적 스펙은 모두 MBRGRPMBR 테이블을 사용하여 완료될 수 있습니다. 액세스 그룹의 멤버쉽에 대한 기준은 대개 역할, 사용자가 속해 있는 조직 또는 사용자 등록 상태를 바탕으로 합니다. 예를 들어, 판매자 관리자라는 액세스 그룹은 해당 사용자가 판매자 관리자의 역할을 수행하는 그룹입니다.

WebSphere Commerce는 여러 기본 역할을 포함하며 각 역할에 기본 구성원 그룹이 대응합니다. 예를 들어, 기본적으로 판매자 관리자라는 역할이 있고 대응하는 판매자 관리자라는 구성원 그룹이 있습니다.

역할

위에서 언급한 대로 WebSphere Commerce는 기본 역할 세트를 제공합니다. 사이트 운영자는 역할에 사용자를 지정하기 전에 모든 조직에 특정 역할을 지정해야 합니다. 역할은 절대적이거나 범위를 지정할 수 있습니다. 절대 역할에서 사용자에게 역할이 지정되지만 사용자가 속해 있는 조직에 대해 해당 역할을 반드시 수행할 필요는 없습니다. ″공인 회계사(CPA)″가 절대 역할의 한 예입니다. 사용자가 CPA일 수 있지만, 그 사람이 속해 있는 조직에 대한 회계사가 아닐 수 있으며 다른 조직의 회계사일 수 있습니다. CPA는 절대 역할이지만 회계사는 범위가 지정된 또는 상대 조직 역할입니다. WebSphere Commerce의 대부분의 역할은 범위가 지정됩니다. 예를 들어, 한 사용자가 조직 X에 대한 상품 관리자입니다. 그런 다음 이 사용자가 조직 X와 해당 하위 조직의 컨텍스트 안에서만 상품 관리 조작을 수행하도록 액세스 제어 정책이 설정될 수 있습니다.

WebSphere Commerce와 함께 제공되는 기본 역할을 다음 카테고리로 그룹화할 수 있습니다.

- 사이트 작업
- 사이트 및 컨텐츠 개발
- 기술 작업

- 마케팅 관리
- 상품 관리
- 비즈니스 관계 관리
- 물류 및 작업 관리
- 조직 관리

사이트 작업

다음 기술 작업 역할이 WebSphere Commerce에서 지원됩니다.

- 사이트 운영자
- 상점 운영자

사이트 운영자

사이트 운영자는 WebSphere Commerce 및 연관된 소프트웨어와 하드웨어를 설치, 구성 및 유지보수합니다. 운영자는 시스템 경고, 경보 및 오류에 대해 응답하고 시스템 문제점을 진단 및 해결합니다. 이 역할은 일반적으로 액세스 및 권한(구성원 작성 및 적당한 역할에 구성원 지정)을 제어하고, 웹 사이트를 관리하고, 성능을 모니터하고, 로드 밸런싱 태스크를 관리합니다. 사이트 운영자는 또한 테스트, 스테이징 및 프로덕션 같은 개발의 여러 단계에 대한 여러 서버 구성의 설정 및 유지보수를 담당할 수 있습니다. 이 역할은 또한 중요한 시스템 백업을 처리하고 성능상의 문제점을 해결합니다.

상점 운영자

상점 운영자는 상점 자원을 관리하고 세금, 운송 및 상점 정보에 대한 변경사항을 갱신 및 공개합니다. 상점 운영자는 또한 조직에 대한 액세스 제어 정책을 관리할 수 있습니다. 대개 상점 개발팀을 이끄는 상점 운영자는 상점 아카이브를 공개하는 권한을 갖는 팀에 대한 유일한 역할입니다(사이트 운영자도 상점 아카이브를 공개할 수 있습니다). 상점 운영자는 대개 웹에 대해 많이 알고 상점의 비즈니스 프로시저에 대해 철저한 지식을 갖고 있습니다.

사이트 및 컨텐츠 작성

WebSphere Commerce는 상점 개발자 사이트와 컨텐트 개발 역할을 지원합니다.

상점 개발자

상점 개발자는 Java Server Pages 파일과 모든 필요한 사용자 정의된 코드를 작성하고 WebSphere Commerce에 포함되는 모든 표준 기능을 수정할 수 있습니다. 일단 상점 아카이브가 작성되면 상점 개발자는 수동으로 또는 상점 프로파일 노트북과 세금 및 운송 노트북을 사용하여 상점 아카이브를 변경하는 권한을 갖습니다. 상점 개발자에는 상점 아카이브를 WebSphere Commerce 서버에 공개할 권한이 없습니다.

물류 및 작업

WebSphere Commerce는 다음 물류 및 작업 관리 역할을 지원합니다.

- 물류 관리자
- 운영 관리자
- 수령인
- 반품 관리자
- 포장업자

B2C -- 물류 관리자

때로는 운송 관리자라고도 하는 물류 관리자는 운송 회사에서 창고까지 그리고 개별 고객까지의 대량 수송이나 운송을 관리하고 협상합니다. 이 역할은 회사가 최상의 비용으로 최상의 운송업체를 사용하여 회사 전략을 만족시킬 책임을 갖습니다. 운송은 고객 서비스의 중요한 측면이며 온라인 비즈니스의 중요한 성공 요소일 수 있습니다.

B2B -- 운영 관리자

이 역할은 주문 처리를 관리하여 주문이 적절하게 이행되는지, 지불이 수령되는지 및 주문이 운송되는지 확인합니다. 운영 관리자는 고객 주문을 검색하고, 정보를 보고, 주문 정보를 관리하고, 반품 정보를 작성 및 편집할 수 있습니다.

포장업자

포장업자는 서비스 센터로부터 상품을 오더피킹하고 고객에게 운송하기 위해 상품을 포장합니다. 포장업자는 또한 출고 요청서와 출고 전표를 관리하는데, 이것들은 주문 이행 중에 상품의 운송을 확인하는데 사용됩니다.

수령인

수령인은 서비스 센터에 있는 재고를 받고, 주문한 상품에 대한 예상 재고 레코드와 임시 수령을 추적하고, 고객 반품의 결과로서 반품된 상품을 수령합니다.

반품 관리자

반품 관리자는 반품된 상품의 처리를 관리합니다.

- 반품 목록 작성
- 반품된 상품 목록 작성
- 반품된 상품 처리

상품 관리

다음 상품 관리 역할이 WebSphere Commerce에서 지원됩니다.

- 구매자(판매자측)
- 카테고리 관리자
- 상품 관리자 또는 판매 계획 관리자

구매자(판매자측)

구매자는 판매할 상품을 구매합니다. 구매자는 공급업체 또는 제조업체와의 관계를 처리하고 운송과 지불 옵션 같은 유리한 조건을 갖는 원하는 상품을 얻기 위해 협상합니다. 구매자는 가격을 설정할 수 있습니다. 구매할 수량을 판별하고 재고가 적절하게 보충되도록 보장하기 위해 구매자가 재고량을 관리합니다.

카테고리 관리자

카테고리 관리자는 카테고리를 작성, 수정 및 삭제하여 카테고리 계층을 관리합니다. 카테고리 계층은 상점에서 판매 설정되는 상품이나 서비스를 구성합니다. 카테고리 관리자는 또한 상품, 예상 재고 레코드, 공급업체 정보, 재고량 및 반품 이유를 관리합니다.

상품 관리자

판매 계획 또는 상품 관리자는 고객 구매를 추적하고, 할인을 제안하고, 온라인 상점에서 상품을 전시, 가격 책정 및 판매하는 최상의 방법을 판별합니다.

- 모든 카테고리 관리자 태스크를 수행합니다.
- 모든 마케팅 관리자 태스크를 수행합니다.

판매 관리

다음 비즈니스 관계 관리 역할이 WebSphere Commerce에서 지원됩니다.

- 판매 관리자
- 회계 담당
- 고객 서비스 대표
- 고객 서비스 영업대표

판매 관리자

판매 관리자는 고객을 확보하고 유지하며, 판매 예측을 만족시키고, 고객 비즈니스 증가에 대한 인센티브를 제공하고, 장기 구매 계약을 관리하고, 가격 책정 조건을 설정하고, 재고량 예측을 설정하기 위해 상품 관리자와 함께 작업하고, 특별 판매를 위해 마케팅 관리자와 함께 작업합니다.

회계 담당

회계 담당은 관계를 빌드하기 위해 개별 계정에 대해 작업하고 고객 서비스 문제를 관리합니다. 이들은 장기 구매 계약 가격 책정을 변경하고, 장기 구매 계약 및 프로파일을 협상하고, 계정 카테고리별로 수익성을 분석하는 권한을 부여 받을 수 있습니다.

고객 서비스 대표

이 역할은 모든 고객 서비스 태스크에 액세스할 수 있습니다. 고객 서비스 대표는 고객 조회(예: 고객 등록, 주문, 반품 및 경매)를 관리하며 시스템이 거부하는 반품 레코드 승인 및 지불 예외(신용 카드 인증 실패 같은)에 관하여 고객과 접촉하는 것과 같은 고객 서비스 영업대표가 액세스할 수 없는 태스크를 완료하는 권한이 있습니다.

고객 서비스 영업대표

온라인 비즈니스가 얼마나 잘 고객에게 셀프 서비스 기능을 제공하도록 설계되는지와 상관없이, 웹에 대해 가장 잘 아는 고객조차도 개인 담당자가 필요할 때나 고객 유형이 있습니다. 대부분의 온라인 비즈니스는 고객이 직접 서비스를 얻기 위한 전자 우편, 팩스 또는 연락처를 제공합니다. 고객 서비스 영업대표가 고객의 모든 조회 처리를 담당합니다.

마케팅 관리

WebSphere Commerce는 마케팅 관리자의 마케팅 관리 역할을 지원합니다.

마케팅 관리자

마케팅 관리자는 고객에게 마켓 전략과 브랜드 메시지를 전달합니다. 이 역할은 고객 예상 행위를 모니터, 분석 및 이해합니다. 또한 마케팅 관리자는 대상 판매를 위한 고객 프로파일을 작성 또는 수정하고 캠페인 및 특별 판매를 작성 및 관리합니다. 캠페인 이벤트 계획 수립은 판매자, 마케팅 관리자 및 판매 계획 관리자로 구성되는 팀에 의해 처리될 수 있습니다.

조직 관리

WebSphere Commerce는 다음 조직 관리 역할을 지원합니다.

- 판매자 관리자
- 구매자 관리자
- 구매자 승인자
- 구매자(구매측)

판매자 관리자

판매자 관리자는 판매 조직에 대한 정보를 관리합니다. 판매자 관리자는 적당한 비즈니스 역할의 지정을 포함하여 판매 조직 내의 하위 조직과 판매 조직의 여러 사용자를 작성하고 관리합니다.

구매자 관리자

구매자 관리자는 구매 조직에 대한 정보를 관리합니다. 이들은 구매 조직 내의 하위 조직을 작성 및 관리하고 사용자를 구매자로 승인하는 것을 포함하여 여러 사용자를 관리합니다. 구매자 승인자 및 구매자 조직 운영자 같은 다른 구매측 역할이 작성되고 관리될 수 있습니다.

구매자 승인자

구매자 승인자는 주문이 판매자와의 구매를 위해 제출되기 전에 구매자가 작성한 주문을 승인하는 구매 조직의 개인입니다.

구매자(구매측)

구매자는 구매자 또는 구매자 조직 대신 판매자로부터 구매하는 개인입니다. 대개 구매는 판매자와 협상된 하나 이상의 계약하에 이루어집니다. 구매자는 판매자의 웹 사이트와 상호작용하여 구매합니다.

자원 카테고리

자원 카테고리는 자원의 클래스를 의미합니다. 자원 카테고리는 주문, RFQ 및 경매 같은 Java 클래스입니다. 자원은 이들 클래스의 인스턴스입니다. 예를 들어, 경매 운영자 A가 작성한 Auction1이 하나의 자원이며 경매 운영자 B가 작성 Auction2가 또다른 자원입니다. 이들 두 자원은 자원 카테고리인 경매에 속합니다.

자원 카테고리는 ACRESCGRY 테이블에 정의되어 있습니다.

자원 그룹

자원 그룹은 관련된 자원의 세트를 식별합니다. 자원 그룹은 장기 구매 계약 또는 관련 명령 세트 같은 비즈니스 오브젝트를 포함할 수 있습니다. 액세스 제어에서 자원 그룹은 액세스 제어 정책이 액세스를 권한 부여하는 자원을 지정합니다.

자원 그룹은 ACRESGRP 테이블에 정의되어 있습니다.

암시적 자원 그룹

암시적 자원 그룹은 특정 속성 세트와 일치하는 자원을 정의합니다. 실례로 자원의 Java 클래스 이름이 자원 그룹일 수 있습니다. 속성을 지정하여 그룹에 암시적으로 자원을 추가하면 각 자원을 지정할 필요없이 수많은 자원에 대한 액세스를 권한 부여하기가 쉬워집니다. 또한 자원 변경이 발생할 때 자원을 추가 또는 삭제해야 할 필요가 없습니다.

암시적 자원 그룹은 ACRESGRP 테이블의 CONDITIONS 컬럼을 사용하여 정의됩니다.

명시적 자원 그룹

명시적 자원 그룹은 하나 이상의 자원 카테고리를 자원 그룹과 연관시켜 지정됩니다. 이 연관은 ACRESGPRES 테이블에서 수행됩니다. 클래스 이름을 나열하여 자원 카테고리를 그룹에 명시적으로 추가하면 일반 속성을 반드시 공유하지 않을 수 있는 개별 자원을 그룹화할 수 있습니다.

자원 관계

각 자원은 그와 연관된 몇 가지 종류의 관계와 각 관계를 이행하는 구성원 세트가 있습니다. 예를 들어 모든 자원은 *소유자*의 관계를 갖는데, 이것은 자원의 소유자에 의해 이행됩니다. 기타 관계에는 문서를 받는 사람과 카탈로그 항목에 대한 공급업체가 포함될 수 있습니다. 이들 자원 관계는 자원의 특정 인스턴스에 대해 특정 조치를 수행할 수 있는 사람을 판별하는 데 있어서 중요합니다. 예를 들어, 문서 작성자는 문서를 삭제할 수 없을 수 있지만 감사역은 삭제할 수 있습니다. 마찬가지로, 검토자는 단지 문서를 읽고 승인할 수는 있지만 문서를 전달하거나 다른 작업을 수행할 수는 없습니다.

관계는 ACRELATION 테이블에 저장되며, ACPOLICY 테이블의 ACRELATION_ID 컬럼을 사용하여 액세스 제어 정책에 선택적으로 지정됩니다.

액세스 제어 정책

액세스 제어 정책은 WebSphere Commerce의 자원에 대해 특정 조치를 수행하도록 사용자 또는 사용자 그룹에 권한 부여합니다. 하나 이상의 액세스 제어 정책을 통해 권한 부여되지 않으면 사용자는 시스템의 어떤 기능에도 액세스할 수 없습니다. 액세스 제어 정책을 이해하려면 사용자, 조치 및 자원의 개념을 이해해야 합니다. 사용자는 시스템을 사용하는 사람입니다. 자원은 시스템에서 보호해야 하는 오브젝트입니다. 조치는 사용자가 자원에 대해 수행할 수 있는 활동입니다.

액세스 제어 정책의 요소

액세스 제어 정책은 다음 네 요소로 구성됩니다.

액세스 그룹
정책이 적용되는 사용자의 그룹

조치 그룹
조치의 그룹

자원 그룹
정책에 의해 제어되는 자원. 자원 그룹은 사용자가 수행할 수 있는 모든 경매 관련 명령뿐 아니라 "장기 구매 계약" 또는 "주문" 같은 비즈니스 오브젝트나 관련 명령 세트를 포함할 수 있습니다.

자원 관계(선택적)
각 자원 유형은 그와 연관된 관계 세트가 있습니다. 각 자원은 각 관계를 이행하는 사용자 세트가 있습니다. 특정 액세스 그룹에 속하는 사용자는 사용자가 자원에 관한 특정 관계를 만족하는 동안은 지정된 자원 그룹에 속하는 자원에 대해 지정된 조치 그룹의 조치를 수행하도록 허용됩니다. 예를 들어, 주문에 대한 "소유자" 관계가 있는 상점을 위해 작업하는 상점 운영자가 주문을 삭제할 수 있는 정책을 만들 수 있습니다.

액세스 제어 정책 개념

액세스 제어 정책은 사용자에게 사이트에 대한 액세스를 부여합니다. 하나 이상의 액세스 제어 정책을 통해 자신의 책임을 수행하도록 권한 부여되지 않으면 사용자는 사이트의 어떤 기능에도 액세스할 수 없습니다.

각 액세스 제어 정책의 양식은 다음과 같습니다.

```
AccessControlPolicy [AccessGroup,ActionGroup,ResourceGroup,Relationship]
```

액세스 제어 정책의 요소는 사용자가 자원과 관련되어 특정 관계를 만족하는 경우에 한하여 특정 액세스 그룹에 속하는 사용자가 지정된 자원 그룹에 속하는 자원에 대해 지정된 조치 그룹의 조치를 수행할 수 있도록 지정합니다. 예를 들어, [AllUsers, UpdateDoc, doc, creator]는 사용자가 문서의 작성자인 경우 모든 사용자가 문서를 갱신할 수 있다고 지정합니다.

다음 절에서는 액세스 제어와 연관된 개념적 정보와 전문 용어에 대해 설명합니다.

액세스 그룹

액세스 그룹은 액세스 제어 목적을 위해 특별히 정의되는 사용자의 그룹입니다. 사이트 운영자는 관리 콘솔을 사용하여 사이트에 대한 액세스 그룹을 작성, 유지보수 및 삭제합니다. 구매자 관리자나 판매자 관리자는 WebSphere Commerce 조직 관리 콘솔을 사용하여 사용자에게 역할을 지정하거나 명시적으로 사용자를 액세스 그룹에 지정합니다. 액세스 그룹을 사용할 때 사용자는 대개 그들의 역할, 조직 및 등록 상태를 바탕으로 그룹화됩니다.

사용자가 사이트에서 수행하는 활동 유형을 바탕으로 액세스 그룹에 사용자를 추가하기 위해 역할을 속성으로 사용할 수 있습니다.

액세스 그룹은 암시적, 명시적 또는 둘다일 수 있습니다.

암시적 액세스 그룹: 암시적 액세스 그룹은 기준 세트에 의해 정의됩니다. 기준을 충족시키는 모든 사람이 해당 그룹의 구성원입니다. 속성을 지정하여 액세스 그룹을 암시적으로 추가하면 각각의 이름을 지정할 필요 없이 수많은 사용자에게 액세스를 권한 부여하기가 쉬워집니다. 또한 사용자의 속성이 변경될 때 그룹의 구성원을 갱신할 필요가 없게 합니다. 액세스 그룹의 단순한 기준은 사용자가 역할을 수행하는 조직에 관계 없이, 특정 역할을 지정한 모든 사람을 포함하는 것입니다. 더 복잡한 기준은 특정 조직의 가능한 역할 세트 중 하나를 수행하는 사용자만이 액세스 그룹에 속함을 지정하는 것입니다.

명시적 액세스 그룹: 명시적 액세스 그룹에는 일반 속성을 공유하거나 공유하지 않을 수 있는 명시적으로 지정된 사용자가 포함됩니다. 액세스 그룹을 명시적으로 추가하면 일반 속성을 반드시 공유하지 않을 수 있는 개별 사용자를 그룹화합니다. 또한 암시적으로 정의된 그룹에 포함되기 위한 조건을 충족시키지만 사용자가 제외되기 원하는 개인을 제외할 수 있습니다.

조치

일반적으로 조치는 자원에 대해 수행되는 조작입니다. 제어기 명령에 대한 역할 기반 정책에서, 조치는 Execute이며 자원은 실행 중인 명령입니다. 보기에 대한 역할 기반 정책에서, 조치는 보기의 이름이며, 자원은 com.ibm.commerce.commands.ViewCommand 입니다. 자원 레벨 액세스 제어의 경우, 조치는 보통 WebSphere Commerce 명령으로 맵핑되며 자원은 보통 보호된 EJB의 원격 인터페이스입니다. 예를 들어, 제어기 명령 com.ibm.commerce.order.commands.OrderCancelCmd는 com.ibm.commerce.order.objects.Order 자원에서 작동합니다. 마지막으로 Display 조치는 데이터 bean 자원을 활성화하기 위해 사용됩니다. 조치는 ACACTION 테이블에 저장됩니다.

조치 그룹

조치 그룹은 관련된 조치의 그룹입니다. 다음 명령을 포함하는 AccountManage 그룹이 조치 그룹의 한 예입니다.

- com.ibm.commerce.account.commands.AccountDeleteCmd
- com.ibm.commerce.account.commands.AccountSaveCmd

사이트 운영자만이 조치 그룹을 작성, 갱신 및 삭제할 수 있습니다. 이것은 관리 콘솔에서 수행됩니다. 조치 그룹은 ACACTGRP 테이블에 저장됩니다.

자원

자원은 시스템에서 보호될 필요가 있는 오브젝트입니다. 예를 들어 RFQ, 경매, 사용자 및 주문이 보호되어야 하는 WebSphere Commerce에 있는 몇 가지 자원입니다. 각 자원은 소유자를 갖습니다. 자원의 소유권을 사용하여 어떤 액세스 제어 정책이 자원에 적용되는지를 판별할 수 있습니다. 액세스 제어 정책은 조직 엔티티인 소유자를 갖습니다. 정책은 정책을 소유하는 동일한 조직 엔티티에 의해 소유되는 자원에만 적용됩니다. 상위 조직 엔티티가 소유하는 정책도 자원에 적용됩니다.

제어기 명령 자원: 제어기 명령에 대한 역할 기반 액세스 제어의 경우, Execute 조치가 제어기 명령 자원에서 수행되도록 구조화됩니다. 이 정책은 지정된 역할로 사용자에 대한 제어기 명령의 실행을 제한하기 위한 것입니다. 이 정책에 대한 액세스 그룹은 보통 단일 역할에 대한 것으로, 예를 들어 상품 관리자(상품 관리자 역할을 가짐)가 있습니다. 여기에서 자원 그룹은 상품 관리자가 실행할 수 있는 제어기 명령 세트입니다.

데이터 bean 자원: 모든 데이터 bean에 보호가 필요하지는 않습니다. 기존 WebSphere Commerce 응용프로그램 안에서 보호가 필요한 데이터 bean은 이미 필수 액세스 제어를 구현합니다. 보호할 것에 대한 질문은 새 데이터 bean을 작성할 때 발생합니다. 보호할 자원을 결정하는 것은 응용프로그램에 따라 다릅니다.

데이터 bean 오브젝트가 그 자신에 존재할 수 있는 경우, 직접 보호되어야 합니다. 데이터 bean의 존재가 다른 데이터 bean의 존재에 의존하는 경우, 다른 데이터 bean에 보호를 위임해야 합니다. 직접 보호되는 데이터 bean의 예로는 Order 데이터 bean이 있습니다. 간접적으로 보호되는 데이터 bean의 예로는 OrderItem 데이터 bean이 있

는데, Order 데이터 bean이 없으면 존재할 수 없기 때문입니다. 데이터 bean 자원을 보호하는 방법에 대해서는 *WebSphere Commerce 5.4 프로그래머 안내서*를 참조하십시오.

데이터 자원: 데이터 자원은 경매, 주문, RFQ 및 사용자 같이 조작될 수 있는 비즈니스 오브젝트를 의미합니다. 이들 자원은 보호됩니다.

자원 및 정책 소유권

조직 엔티티가 모든 정책을 소유합니다. 모든 액세스 제어 자원은 보통 조직 엔티티인 소유자를 가지며(예: 주문은 상점을 소유하는 조직에 의해 소유) 사용자는 자원을 소유합니다(예: 등록된 사용자는 자신의 사용자 등록 정보 소유). 자원 및 액세스 제어 정책의 소유권은 어떤 정책을 특정 자원에 적용해야 하는지 결정할 때 중요합니다. 주어진 자원의 경우, 소유하는 조직의 엔티티와 소유자의 상위 조직 엔티티에 속하는 정책이 적용됩니다.

액세스 제어 정책의 유형

액세스 제어 정책의 두 가지 유형이 있습니다.

- 정상 정책
- 템플리트 정책

정상 정책

정상 정책은 고정된 소유자를 갖습니다. 예를 들어, 판매자 조직이 정상 정책을 소유하는 경우, 판매자 조직에서 소유하는 자원과 하위 조직 엔티티가 소유하는 자원이 있는 경우 적용됩니다. 루트 조직은 WebSphere Commerce에서 다른 모든 조직의 상위 조직이므로, 루트 조직(구성원 ID = -2001)에서 소유하는 정책은 정의에 의해 사이트의 모든 자원에 적용됩니다. 그러므로 루트 조직에서 소유하는 정상 정책은 때로 사이트 레벨 정책이라 언급됩니다.

루트 조직에서 소유하지 않는 정상 정책은 사이트별로 적용되지 않고, 정책 소유자나 하위 조직 엔티티에서 소유하는 자원에만 적용되므로 조직 레벨 정책이라 언급됩니다. 상점 운영자는 자체 조직 엔티티와 하위 조직 엔티티에 대한 정책을 관리할 수 있습니다. 사이트 운영자는 모든 정책을 수정할 수 있습니다.

템플리트 정책

템플리트 정책은 동적 소유자를 갖습니다. 템플리트 정책은 자원 소유 조직 엔티티와 상위 조직 엔티티를 소유하는 자원에 동적으로 적용합니다. 예를 들어 루트 조직 아래에 10개의 조직이 있는 경우, 상점 운영자는 조직 역할을 위해 조직에서 소유하는 자원만을 수정할 수 있게 하려고 합니다. 이를 설정하는 방법은 두 가지입니다.

1. 액세스 중인 자원에 따라 동적으로 10개의 조직에 적용할 한 개의 템플리트 정책을 갖습니다. 템플리트 정책에서 액세스 그룹에 대한 기준은 동적일 수 있습니다. 예를 들어, 사용자가 조직 X3에서 소유하는 자원을 액세스하도록 시도 중인 경우, 템플

리트 정책의 소유자는 동적으로 조직 X3으로 변경하며, 액세스 그룹은 동적으로 자체 범위가 조직 X3이 되므로, 사용자는 조직 X3에 대한 상점 운영자의 역할을 수행해야 합니다.

2. 10개의 정책을 가지며, 각각은 10개의 조직 중 하나가 소유합니다. 조직 X1에 대한 액세스 그룹은 사용자가 조직 X1에 대한 상점 운영자 역할을 수행해야 함을 지정합니다. 조직 X2에 대한 액세스 그룹은 사용자가 조직 X2에 대한 상점 운영자 역할을 수행해야 함을 지정합니다.

처음 솔루션의 이점은 오직 하나의 실제 정책 사본이 있지만, 논리 사본은 10개라는 것입니다. 사이트 운영자가 템플리트 정책을 관리할 수 있습니다.

템플리트 정책 대체: 템플리트 정책의 다른 특징은 지정된 조직 엔티티의 템플리트 정책을 대체할 수 있다는 것입니다. 위의 예로 다시 돌아가서, 11번째 조직 엔티티를 WebSphere Commerce에 추가하여 이러한 가장 새로운 조직 엔티티에서 위의 템플리트 정책을 적용하게 하려는 경우, 이를 지정하는 방식이 있습니다. 템플리트 정책의 정책 id와, 11번째 조직의 조직 엔티티 ID를 지정하여 ACORGPOL 테이블에 항목을 추가해야 합니다. 또한 이것은 상점 운영자가 특정 조직의 컨텍스트에서 템플리트 정책을 삭제하거나 갱신할 때 관리 콘솔을 통해 수행될 수 있습니다.

액세스 제어의 레벨

WebSphere Commerce에는 두 가지의 광범위한 액세스 제어 레벨인 명령 레벨(역할 기반이라고도 함)과 자원 레벨(인스턴스 기반이라고도 함)이 있습니다.

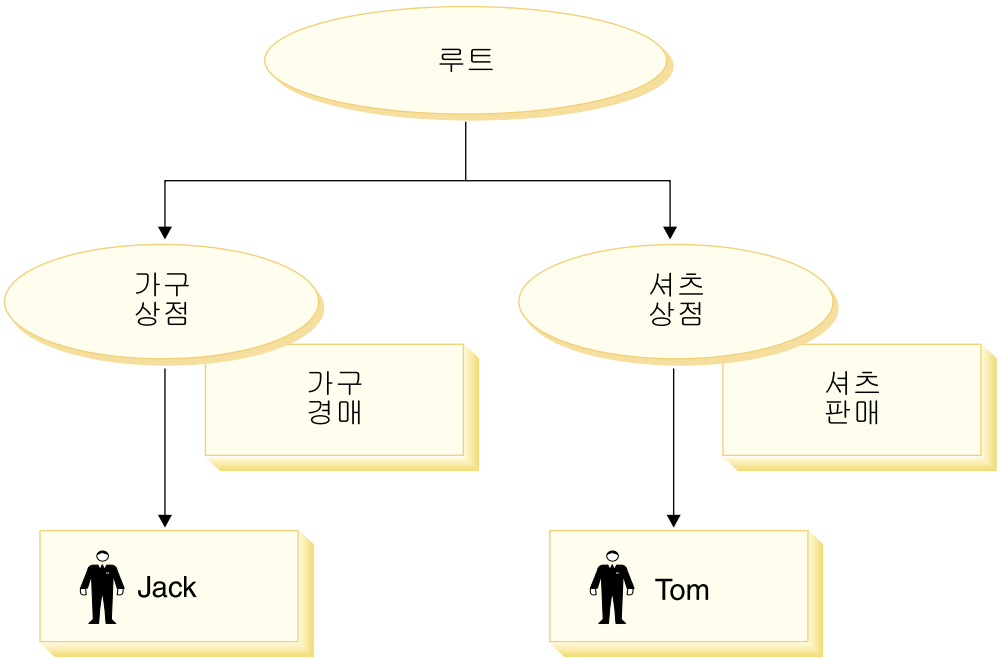

그림 2. 정책 레벨

명령 레벨 또는 역할 기반 액세스 제어

명령 레벨 또는 역할 기반 액세스 제어는 굵은 액세스 제어입니다. 이것은 "누가 무엇을 할 수 있는가"를 판별합니다. 역할 기반 액세스 제어를 사용할 때 특정 역할의 모든 사용자가 특정 유형의 명령을 실행할 수 있도록 지정할 수 있습니다. 액세스 제어 정책 판매자가 경매를 수정할 수 있음을 고려하십시오. 32 페이지의 그림 2에서 Jack과 Tom은 둘 다 판매자이므로 둘 모두 경매를 작성할 수 있습니다.

명령 레벨 또는 역할 기반 액세스 제어는 제어기 및 보기 명령에 사용될 수 있습니다. 이 유형의 액세스 제어는 명령이 실행될 자원을 고려하지 않습니다. 단지 사용자가 특정 명령을 실행하도록 허용되는지를 판별합니다.

이 액세스 제어 레벨은 필수이며 런타임에 의해 강제 실시됩니다. 모든 제어기 명령은 명령 레벨 액세스 제어에 의해 보호되어야 합니다. 또한 직접 호출할 수 있거나 다른 명령으로부터의 경로 재지정에 의해 실행(보기로 전달하여 실행되는 것과 대조적으로)될 수 있는 모든 보기는 명령 레벨 액세스 제어에 의해 보호되어야 합니다.

제어기 명령에 대한 명령 레벨 액세스 제어: 제어기 명령을 실행할 때마다, 액세스 제어 정책은 명령 자원에서 "실행" 조치를 수행하도록 사용자에게 부여하는 액세스 제어 정책이 존재해야 합니다. 자원은 제어기 명령의 인터페이스 이름입니다. 액세스 그룹의 범위는 보통 단일 역할입니다. 예를 들어 회계 담당 역할을 갖는 사용자가 `AccountRepresentativesCmdResourceGroup` 자원 그룹에서 모든 명령을 실행하도록 지정할 수 있습니다.

보기에 대한 명령 레벨 액세스 제어: 보기가 URL에서 직접 호출되거나 명령의 경로 재지정 결과인 경우, 액세스 제어 정책을 가져야 합니다. 그러한 정책은 `ACACTION` 테이블에서 조치로 지정된 보기 이름을 가져야 합니다. 이 조치는 `ACACTACTGP` 테이블을 사용하여 조치 그룹과 연관되어야 합니다. 이 조치 그룹은 `ACPOLICY` 테이블의 해당 명령 레벨 정책에서 참조되어야 합니다.

인스턴스 기반 또는 자원 레벨 액세스 제어

인스턴스 레벨 또는 자원 레벨 액세스 제어 정책은 객체 단위 액세스 제어를 제공하여 누가 어떤 자원에 대해 어떤 명령을 수행할 수 있는지를 판별합니다. 역할 기반 액세스 제어 예인 판매자가 경매를 수정할 수 있음은 자원 레벨 액세스 제어를 위해 판매자는 자신이 작성한 경매를 수정할 수 있음으로 미세 조정될 수 있습니다. 32 페이지의 그림 2에서 Jack은 가구 상점 판매자입니다. Tom은 셔츠 상점 판매자입니다. Jack은 가구 상점에 가구 경매를 작성합니다. Tom은 셔츠 상점에 셔츠 경매를 작성합니다. Jack은 가구 경매를 수정할 수 있지만 셔츠 경매는 수정할 수 *없습니다*. Tom은 셔츠 경매를 수정할 수 있지만 가구 경매는 수정할 수 *없습니다*.

요약하면, 먼저 시스템이 명령 레벨 액세스 확인을 수행합니다. 사용자가 명령을 실행하도록 허용되는 경우, 후속 자원 레벨 액세스 제어 정책이 수행되어 사용자가 의심이 가는 자원에 액세스할 수 있는지를 판별합니다.

자원 레벨 액세스 제어는 명령 및 데이터 bean에 적용됩니다.

명령에 대한 자원 레벨 액세스 제어: 명령 레벨 액세스 제어 점검이 완료된 후에, 액세스 권한이 부여되면 자원 레벨 점검이 다음 두 가지 경우 중 하나로 수행됩니다.

- 명령에서 `getResources()`를 구현합니다. 이 방법은 현재 조치에 대해 점검될 필요가 있는 자원의 인스턴스를 지정하며, 여기에서 명령은 조치입니다. WebSphere Commerce 런타임은 `getResources()`로 지정된 모든 자원에 대한 액세스를 현재 사용자가 가지도록 강제 실시합니다. 기본값으로, `getResources()`는 널(Null) 값을 리턴하며, 자원 레벨 점검을 수행하지 않습니다.
- 명령은 `checkIsAllowed(Object Resource, String Action)`를 호출합니다. 여기에서 명령 작성자는 런타임이 getResources()를 호출하는 시간에 어떤 자원을 확인해야 하는지 알지 못하며, 필요하면 명령에서 이 `checkIsAllowed()` 메소드를 호출하여 현재 조치와 자원 쌍이 권한 부여되는지 여부를 판별할 수 있습니다. 조치 기본값은 현재 명령의 interfacename입니다. 이 메소드가 호출되면, 액세스가 거부된 경우 다음 예외가 발생합니다.
  `ECApplicationException(ECMessage._ERR_USER_AUTHORITY, ..)`

데이터 bean에 대한 자원 레벨 액세스 제어: 위에서 설명한 대로, 보기는 보통 역할에 근거하여 명령 레벨 정책으로 보호됩니다. 예를 들어, 명령 레벨 정책은 판매자 관리자가 특정 보기에 대한 액세스를 가짐을 지정할 수 있습니다. JSP의 데이터 bean은 사용자가 판매자 관리자 역할을 수행하는 조직과 모두 관련됨을 확인하는 것이 종종 필요합니다. 이것은 보호 가능한 자원으로 기본(독립) 데이터 bean을 지정하여 수행됩니다. 그런 다음 Databean Manager의 `activate()` 메소드를 사용하여 데이터 bean이 호출될 때마다, WebSphere Commerce 런타임은 데이터 bean 자원에서 ″표시″ 조치를 수행하기 위해 현재 사용자 권한을 부여하는 정책이 있는지 확인합니다.

액세스 제어가 권한 없는 조치를 막는 방법

이 절에서는 정책 기반 액세스 제어가 사용자들이 권한 부여된 조치만을 수행할 수 있음을 보장하기 위해 작업하는 방법에 대해 설명합니다.

사용자 시작 조치를 수행하기 전에 권한 확인

*정책 관리자*는 현재 사용자가 지정된 자원에 대해 지정된 조치를 실행하도록 허용되는지 여부를 판별하는 액세스 제어 구성요소입니다. 액세스 제어 정책은 XML 형식으로 지정됩니다. 설치시에 기본 정책이 자동으로 적당한 데이터베이스 테이블에 로드됩니다. 런타임시 정책 관리자는 SQL 조회를 사용하여 데이터베이스 테이블의 정보를 읽습니다. 액세스 제어 정보가 캐시되므로 정책 관리자가 수행하기 위해 호출될 때 사용자의

권한을 빨리 확인할 수 있습니다. 액세스 제어 정책은 또한 UI 사용자들이 액세스하도록 권한 부여된 조치와 정보만을 보도록 보장하기 위해 사용됩니다.

사용자가 특정 조치를 수행하려 시도할 때 생성된 이벤트가 액세스 확인을 트리거하여 사용자가 권한 부여되는지 확인합니다. 정책 관리자는 시스템에서 사용자가 대상 자원에 대해 조치를 수행하도록 허용하는 액세스 제어 정책을 찾습니다. 이러한 정책이 최소한 하나가 있으면 정책 관리자는 액세스를 부여하고 그렇지 않으면 액세스를 거부합니다.

제 2 부 WebSphere Commerce 사이트 운영자 보안 태스크

이 부분에서는 WebSphere Commerce 사이트 운영자가 일반적으로 수행할 수 있는 보안 태스크에 대해 설명합니다.

제 4 장 사이트 보안 개선

WebSphere Commerce 사이트의 보안을 개선시키기 위해 WebSphere Commerce 구성 관리자에 있는 다음 기능을 사용할 수 있습니다.

- 로그인 시간 종료 노드를 사용하여 장시간 동안 활동하지 않는 사용자를 로그오프하고 시스템에 다시 로그온하도록 요청하십시오. 자세한 내용은 43 페이지의 『구성 관리자 - 로그인 시간 종료』를 참조하십시오.
- 암호 무효화 노드를 사용하여 사용자가 처음으로 시스템에 로그인할 때 암호를 변경하도록 요구하십시오. 자세한 내용은 44 페이지의 『구성 관리자 - 암호 무효화』를 참조하십시오.
- 암호로 보호된 명령 노드를 사용하여 사용자가 지정된 명령을 실행하는 요청을 실행 중인 경우 암호를 입력하도록 설정하십시오. 자세한 내용은 44 페이지의 『구성 관리자 - 암호로 보호된 명령』을 참조하십시오.
- 데이터베이스 갱신 도구 노드를 사용하여 암호 및 신용 카드 정보뿐 아니라 WebSphere Commerce 데이터베이스의 판매자 키 같은 암호화된 데이터를 갱신하십시오. 자세한 내용은 45 페이지의 『구성 관리자 - 데이터베이스 갱신 도구』를 참조하십시오.
- 사이트간 스크립트 보호 노드를 사용하여 허용되지 않는 것으로 지정되는 속성이나 문자를 포함하는 모든 사용자 요청을 거부하십시오. 자세한 내용은 46 페이지의 『구성 관리자 - 사이트간 스크립트 보호』를 참조하십시오.
- 액세스 로그 작성을 사용하여 WebSphere Commerce에 대한 모든 보안 위협을 빨리 식별하십시오. 자세한 내용은 49 페이지의 『구성 관리자 - 액세스 로그 작성 사용』을 참조하십시오.

또한 WebSphere Commerce 관리 콘솔의 보안 드롭 다운에서 다음 기능을 사용할 수 있습니다.

- 계정 정책 페이지를 사용하여 사이트에 대한 계정 정책을 설정함으로써 사용 중인 계정 관련 정책을 정의하십시오. 자세한 내용은 50 페이지의 『운영자 - 계정 정책』을 참조하십시오.
- 암호 정책 페이지를 사용하여 사이트에 대한 암호 정책을 설정함으로써 사용자의 암호 선택 특성을 제어하십시오(사용자가 WebSphere Commerce 데이터베이스에 대해 인증되는 경우에만). 자세한 내용은 51 페이지의 『운영자 - 암호 정책』을 참조하십시오.

- 계정 잠금 정책 페이지를 사용하여 사이트에 대한 계정 잠금 정책을 설정함으로써 사용자 계정이 손상되는 기회를 줄이십시오(사용자가 WebSphere Commerce 데이터베이스에 대해 인증되는 경우에만). 자세한 내용은 52 페이지의 『운영자 - 계정 잠금 정책』을 참조하십시오.
- 보안 확인 실행 페이지를 사용하여 가능한 보안 노출을 포함할 수 있는 임시 WebSphere Commerce 파일을 검사하고 삭제하는 보안 프로그램을 실행하십시오. 자세한 내용은 53 페이지의 『운영자 - 보안 확인 실행』을 참조하십시오.

관련 개념에 대한 정보는 WebSphere Commerce 온라인 도움말의 다음 주제를 참조하십시오.

- 구성 관리자
- WebSphere Commerce 구성 파일
- 관리 콘솔
- 보안

관련 태스크에 대한 자세한 내용은 WebSphere Commerce 온라인 도움말의 다음 주제를 참조하십시오.

- 구성 관리자 실행
- 관리 콘솔 열기

보안에 대한 보기

WebSphere Commerce의 특정 보안 기능을 사용하기 전에 해당 기능을 사용하려면 먼저 상점에 대한 연관된 보기를 정의해야 합니다. 아래 정보는 다음에 대한 보기를 정의하는 방법에 대해 설명합니다.

- 로그인 시간 종료(『로그인 시간 종료』)
- 암호 무효화(41 페이지의 『암호 무효화』)
- 암호로 보호된 명령(42 페이지의 『암호로 보호된 명령』)
- 사이트간 스크립트 보호(42 페이지의 『사이트간 스크립트 보호』)

보기 작성 및 상점 입구 개발에 대한 일반 정보는 *상점 개발자 안내서*를 참조하십시오.

로그인 시간 종료

로그인 시간 종료 기능을 사용하려면 상점에 대한 LoginTimeoutErrorView 및 ReLogonFormView 보기를 정의해야 합니다.

LoginTimeoutErrorView

로그인 시간 종료 정보가 올바르지 않는 경우, WebSphere Commerce는 사용자의 브라우저를 이 보기로 경로 재지정합니다. 이것이 발생하는 경우 누군가가 쿠키를 무단 변경했기 때문일 수 있습니다.

표 1. LoginTimeoutErrorView 속성

ECConstants.EC_LOGIN_TIMEOUT_ERROR_MSGCODE	**1** : 만기 시간이 잘못된 값으로 설정됨 **2** : 로그온 시간이 잘못된 값으로 설정됨 **3** : 만기 또는 로그온 시간이 잘못된 값으로 설정됨

ReLogonFormView

이 보기는 사용자의 세션이 만기된 후 사용자에게 표시됩니다. 사용자에게 사용자의 로그온 ID와 암호를 입력하는 양식을 제공해야 합니다. 제출 버튼이 로그온 명령을 호출합니다. 또한 사용자를 다른 페이지, 대부분 상점 입구 페이지로 경로 재지정하는 취소 버튼도 있어야 합니다.

ReLogonFormView에 대한 속성은 없습니다.

표 2. ReLogonFormView 양식 속성

ECUserConstants.EC_UREG_LOGONID	사용자의 로그온 ID.
ECUserConstants.EC_UREG_LOGONPASSWORD	사용자의 로그온 암호.
ECUserConstants.EC_RELOGIN_URL	제공된 신임장이 올바르지 않은 경우에 표시되는 URL. 대부분의 경우, 이 보기의 이름입니다.
ECConstants.EC_STORE_ID	상점 식별자.
ECConstants.EC_URL	입력되는 신임장이 다른 사용자에게 속할 때 표시되는 URL. 대부분의 경우, 이것은 상점 홈페이지 또는 상점 로그온 페이지에서 사용되는 것과 동일한 URL입니다.

암호 무효화

암호 무효화 보안 기능을 사용하려면 상점에 대한 ChangePassword 보기를 정의해야 합니다.

ChangePassword

이 보기는 사용자의 암호가 만기된 경우에 표시됩니다. 사용자에게 현재(만기된) 암호와 새 암호를 입력하는 양식을 제공해야 합니다. 제출 버튼은 ResetPassword 명령을 호출합니다. 또한 사용자를 다른 페이지, 대부분 상점 입구 페이지로 경로 재지정하는 취소 버튼도 있어야 합니다.

표 3. ChangePassword 속성

ECConstants.EC_PASSWORD_EXPIRED_FLAG	**1**: 사용자의 암호가 만기되었습니다. 이 속성은 이 보기를 암호가 동일할 때 암호 변경 기능에 사용되는 보기를 구별하기 위해 필요합니다. 사용자가 암호 변경에 대한 보기를 호출할 수 있으며, 이 보기에 지정된 JSP가 두 경우 모두에 동일해야 합니다. JSP는 표시할 것을 결정하기 위해 이 속성을 찾습니다. **널(Null)값**: 속성이 URL에 있지 않습니다. 이것은 정상적인 암호 변경 행위입니다.
ECUserConstants.EC_UREG_LOGONID	현재 사용자 로그온 ID.
ECConstants.EC_LOGIN_RETURN_URL	암호 변경이 완료된 후 브라우저가 경로 재지정되는 URL. 이 URL이 이름 ECConstants.EC_URL의 조치 명령으로 전달됩니다.

표 4. ChangePassword 양식 속성

ECUserConstants.EC_UREG_LOGONID	사용자의 로그온 ID id. 현재 로그온 ID가 보기에 전달되었습니다.
ECUserConstants.EC_UREG_LOGONPASSWORDOLD	기존 암호.
ECUserConstants.EC_UREG_LOGONPASSWORD	새 암호.
ECUserConstants.EC_UREG_LOGONPASSWORDVERIFY	새 암호 확인.
ECConstants.EC_URL	암호 변경이 완료된 후 사용자가 경로 재지정되는 URL. 이 값이 보기에 전달되었습니다.
ECUserConstants.EC_RELOGIN_URL	암호 변경에 실패하는 경우 브라우저가 경로 재지정되는 URL.

암호로 보호된 명령

암호로 보호된 명령 보안 기능을 사용하려면 상점에 대한 PasswordReEnterErrorView 및 PasswordReEnterFormView 보기를 정의해야 합니다.

PasswordReEnterErrorView

이 보기는 다음 시나리오에서 사용됩니다.

- 사용자가 올바른 암호를 제공하지 못하고 로그오프됩니다.
- 인증에 실패했습니다.

두 경우 모두 사용자에게는 현재 페이지의 링크를 통해 다른 페이지로 계속하는 방법이 있어야 합니다.

표 5. PasswordReEnterErrorView 속성

ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	**>0**: 사용자를 인증하려 시도할 때 문제점이 발생했습니다. **널(Null)값** : 속성이 URL에 없습니다. 암호를 제공하지 못한 사용자가 로그오프됩니다.

PasswordReEnterFormView

이 보기는 사용자가 암호로 보호된 명령을 실행하려고 시도할 때 표시됩니다. 사용자에게 암호를 입력하는 양식을 제공해야 합니다. 암호에 대한 두 개의 입력 필드가 있어야 합니다.

표 6. PasswordReEnterFormView 속성

ECConstants.EC_PASSWORD_REREQUEST_URL	URL이 양식의 제출 버튼을 사용하여 실행됩니다.
ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	사용자에게 표시되는 메시지를 지정하는 메시지 코드: **1**: 입력된 암호가 일치하지 않습니다. **2**: 암호를 입력하지 않았습니다. **3**: 잘못된 암호를 입력했습니다.

조치: URL이 다음 매개변수로서 전달됩니다.

표 7. PasswordReEnterFormView 양식 속성

ECConstants.EC_PASSWORD_REREQUEST_PASSWORD1	첫 번째 암호.
ECConstants.EC_PASSWORD_REREQUEST_PASSWORD2	두 번째 암호.

사이트간 스크립트 보호

사이트간 스크립트 보호 보안 기능을 사용하려면 상점에 대한 ProhibitedAttrsErrorView, ProhibitedCharacterErrorView 및 ProhibCharEncodingErrorView 보기를 정의해야 합니다.

ProhibitedAttrsErrorView

이 보기는 사용할 수 없는 속성을 포함했기 때문에 요청이 처리되지 않을 때 사용자에게 표시됩니다.

ProhibitedCharacterErrorView

이 보기는 사용할 수 없는 문자를 포함했기 때문에 요청이 처리되지 않을 때 사용자에게 표시됩니다.

ProhibCharEncodingErrorView

이것은 위의 ProhibitedCharacterErrorView와 동일합니다.

구성 관리자 - 로그인 시간 종료

주: 상점에 대한 로그인 시간 종료 보안 기능을 사용하려면 40 페이지의 『로그인 시간 종료』에 설명된 대로 상점에 대한 LoginTimeoutErrorView 및 ReLogonFormView 보기를 정의해야 합니다.

로그인 시간 종료 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 로그인 시간 종료 노드를 사용하십시오. 이 기능이 사용될 때 장시간 동안 활동하지 않는 WebSphere Commerce 사용자는 시스템에서 로그오프되고 다시 로그온하도록 요청됩니다. 사용자가 다음에 성공적으로 로그온하는 경우, WebSphere Commerce는 사용자가 작성한 원래 요청을 실행합니다. 사용자가 로그온에 실패한 경우, 원래 요청이 무시되고 사용자는 시스템에서 로그오프 상태로 있게 됩니다.

WebSphere Commerce 도구(예: 관리 콘솔, WebSphere Commerce 액셀러레이터, 상점 서비스 등)의 경우, 로그인 시간 종료 기능이 사용자에게 재로그인 페이지를 표시하지 않음에 유의하십시오. 대신 브라우저 창을 닫고 도구에 다시 로그온하는 것은 사용자에게 달려 있습니다. 따라서 도구의 경우, 사용자가 제출한 원래 요청이 처리되지 않습니다.

이 기능을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 호출하고 다음과 같이 인스턴스에 대한 로그인 시간 종료 노드로 이동하십시오.

   WebSphere Commerce → *host_name* → **인스턴스 목록** → *instance_name* → **인스턴스 등록 정보** → **로그인 시간 종료**
2. 로그인 시간 종료 기능을 활성화하려면 **사용** 선택란을 누르십시오.
3. 로그인 시간 종료 값 필드에 로그인 시간 종료 값을 초 단위로 입력하십시오.
4. 변경사항을 구성 관리자에 적용하려면 **적용**을 누르십시오.
5. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

로그인 시간 종료 값이 *instance*.xml 파일에 밀리초 단위로 저장되는 반면, 구성 관리자의 값은 초 단위로 입력됨에 유의하십시오.

구성 관리자 - 암호 무효화

주: 암호 무효화 보안 기능을 사용하려면 41 페이지의 『암호 무효화』에 설명된 대로 상점에 대한 ChangePassword 보기를 정의하십시오.

암호 무효화 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 암호 무효화 노드를 사용하십시오. 이 기능이 사용될 때 WebSphere Commerce 사용자는 사용자의 암호가 만기되면 암호를 변경해야 합니다. 이 경우, 사용자에게 암호를 변경해야 하는 페이지가 경로 재지정됩니다. 사용자는 암호를 변경할 때까지 사이트의 어떤 보안 페이지에도 액세스할 수 없습니다. 이 기능을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 호출하고 다음과 같이 인스턴스에 대한 암호 무효화 노드로 이동하십시오.
   WebSphere Commerce → *host_name* → **인스턴스 목록** → *instance_name* → **인스턴스 등록 정보** → **암호 무효화**
2. 암호 무효화 기능을 활성화하려면 **사용** 선택란을 누르십시오.
3. 변경사항을 구성 관리자에 적용하려면 **적용**을 누르십시오.
4. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
5. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

구성 관리자 - 암호로 보호된 명령

주: 암호로 보호된 명령 보안 기능을 사용하려면 42 페이지의 『암호로 보호된 명령』에 설명된 대로 상점에 대한 PasswordReEnterErrorView 및 PasswordReEnterFormView 보기를 정의해야 합니다.

암호로 보호된 명령 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 암호로 보호된 명령 노드를 사용하십시오. 이 기능이 사용될 때 WebSphere Commerce는 WebSphere Commerce에 로그온된 등록 사용자가 지정된 WebSphere Commerce 명령을 실행하는 요청을 계속하기 전에 암호를 입력하도록 요구합니다.

주의: 암호로 보호된 명령을 구성할 때 명령 선택사항 목록에 표시된 명령의 일부는 일반 또는 게스트 사용자에 의해 실행될 수 있습니다. 이러한 명령을 암호로 보호된 명령으로 구성하면 일반 및 게스트 사용자가 해당 명령을 실행하는 데 제한을 받습니다. 그러므로 암호로 보호될 명령을 구성할 때 주의해야 합니다.

이 기능을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 호출하고 다음과 같이 인스턴스에 대한 암호로 보호된 명령 노드로 이동하십시오.

   WebSphere Commerce → *host_name* → **인스턴스 목록** → *instance_name* → **인스턴스 등록 정보** → **암호로 보호된 명령**

2. 일반 탭에서
   a. 암호로 보호된 명령 기능을 활성화하려면 **사용**을 누르십시오.
   b. 재시도 필드에 재시도 횟수를 입력하십시오(기본 재시도 횟수는 3입니다).
3. 고급 탭에서
   a. 암호로 보호된 명령 목록 창에서 목록에서 보호하려는 WebSphere Commerce 명령을 선택하고 **추가**를 누르십시오. 사용자가 선택한 명령이 현재 암호로 보호되는 목록 창에 나열됩니다.
   b. 임의의 WebSphere Commerce 명령에 대한 암호 보호를 사용하지 않으려는 경우, 현재 암호로 보호되는 명령 목록 창에서 명령을 선택한 후 **제거**를 누르십시오.
4. 변경사항을 구성 관리자에 적용하려면 **적용**을 누르십시오.
5. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

주: WebSphere Commerce는 `authenticated`로 지정되거나 사용 가능한 명령 목록의 `URLREG` 테이블에서 `https` 플래그가 설정된 명령만을 표시합니다.

구성 관리자 - 데이터베이스 갱신 도구

구성 관리자의 데이터베이스 노드에서 사용 가능한 데이터베이스 갱신 도구를 사용하여 주어진 인스턴스에 대한 WebSphere Commerce 데이터베이스에 있는 판매자 키뿐 아니라 암호화된 모든 데이터(예: 암호 또는 신용 카드 번호)를 갱신하십시오. 도구를 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 호출하고 다음과 같이 특정 데이터베이스 항목으로 이동하십시오.

   WebSphere Commerce → *host_name* → **인스턴스 목록** → *instance_name* → **인스턴스 등록 정보** → **데이터베이스** → *database_name*

2. *database_name*을 오른쪽 마우스 버튼으로 누르고 **데이터베이스 갱신 도구 실행**을 선택하십시오.
   - 선택한 인스턴스에 대한 모든 데이터베이스의 암호화된 데이터를 이주하려면 **이 인스턴스에 대한 모든 데이터베이스 갱신**을 선택하십시오.
   - 드롭 다운 목록(기본값)에서 데이터베이스를 선택하여 특정 데이터베이스의 암호화된 데이터를 이주하려면 **선택한 데이터베이스 갱신**을 선택하십시오.

3. 조치 항목 상자에서 실행하려는 조치를 선택하고 매개변수 필드에 필수 정보를 기입하십시오.

조치	매개변수	필수 조치
판매자 키 변경	기존 판매자 키	현재 WebSphere Commerce 인스턴스를 작성할 때 사용한 기존 판매자 키를 입력하십시오.
	새 판매자 키	새 판매자 키를 입력하십시오. 이것은 구성 관리자가 현재 암호화된 데이터를 다시 암호화하기 위한 16자리 16진수입니다. 판매자 키에는 최소 하나의 영숫자(a - F)와 최소 하나의 숫자(0 - 9)가 포함되어야 합니다. 모든 영숫자는 소문자로 입력해야 하고 한 행에 같은 문자를 다섯 번 이상 입력할 수 없습니다.

4. 선택한 WebSphere Commerce 데이터베이스 또는 사용자의 모든 WebSphere Commerce 데이터베이스에 대해 데이터베이스 갱신 도구를 실행하려면 **확인**을 누르십시오.
5. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

구성 관리자 - 사이트간 스크립트 보호

주: 상점에 대한 로그인 시간 종료 보안 기능을 사용하려면 42 페이지의 『사이트간 스크립트 보호』에 설명된 대로 상점에 대한 `ProhibitedAttrsErrorView`, `ProhibitedCharacterErrorView` 및 `ProhibCharEncodingErrorView` 보기를 정의해야 합니다.

사이트간 스크립트 보호 기능을 사용 또는 사용 불가능하게 하려면 구성 관리자의 사이트간 스크립트 보호 노드를 사용하십시오. 이 기능은 사용될 때 허용되지 않는 것으로 지정되는 속성이나 문자열을 포함하는 모든 사용자 요청을 거부합니다. 구성 관리자의 이 노드에 허용되지 않는 속성과 문자열을 지정할 수 있습니다. 또한 해당 특정 명령에 대한 지정된 속성의 값이 사용할 수 없는 문자열을 포함할 수 있도록 하여 사이트간 스크립트 보호로부터 명령을 제외할 수 있습니다. 사이트간 스크립트 보호 가능은 기본적으로 사용되지 않습니다.

경고: 사이트간 스크립트 보호는 구성을 바탕으로 명령의 실행을 제한한다는 점에서 제한적 기능입니다. 이 기능은 어떤 속성이나 문자열이 사용할 수 없는 것으로 정의되었는지를 확인하지 않으므로, 이 기능을 구성할 때 사용할 수 없는 속성이 명령에 의해 사용되지 않는 것인지 확인하십시오. 또한 사용할 수 없는 문자열이 일반적으로 명령에 전달되는 값이 아닌지 확인하십시오. 이 기능을 구성할 때 매우 주의하십시오.

이 기능을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 호출하고 다음과 같이 인스턴스에 대한 사이트간 스크립트 보호 노드로 이동하십시오.

   WebSphere Commerce → *host_name* → **인스턴스 목록** → *instance_name* → **인스턴스 등록 정보** → **사이트간 스크립트 보호**

2. 사이트간 스크립트 보호 기능을 활성화하려면 다음과 같이 일반 탭을 사용하십시오.

   a. **사용**을 누르십시오.

   b. WebSphere Commerce 명령에 대해 허용하지 않으려는 속성을 추가하려면 사용할 수 없는 속성 테이블을 오른쪽 마우스 버튼으로 누르고 **행 추가**를 선택하십시오. 허용하지 않으려는 속성을 입력하십시오. 행당 하나의 속성만을 지정할 수 있습니다.

   c. 사용할 수 없는 속성 테이블에서 속성을 제거하려면 테이블에서 해당 속성을 포함하는 행을 강조표시하고 오른쪽 마우스 버튼으로 누른 후 **행 삭제**를 선택하십시오.

   d. WebSphere Commerce 명령에 대해 허용하지 않으려는 문자열을 추가하려면 사용할 수 없는 문자 테이블을 오른쪽 마우스 버튼으로 누르고 **행 추가**를 선택하십시오. 허용하지 않으려는 문자열을 추가하십시오. 행당 하나의 문자열만을 지정할 수 있습니다.

   e. 사용할 수 없는 문자 테이블에서 문자를 제거하려면 사용할 수 없는 문자 테이블에서 해당 문자를 포함하는 행을 강조표시하고 오른쪽 마우스 버튼으로 누른 후 **행 삭제**를 선택하십시오.

   주: 다음 문자열은 사용할 수 없는 문자 필드에 기본적으로 지정됩니다. 이들 문자열은 대부분 나쁜 의도의 사이트간 스크립트 공격에서 스크립트 태그로 공통적으로 사용됩니다.

   - `<SCRIPT`
   - `<SCRIPT`
   - `<%` 및 `<%`

3. 특정 명령에 대한 지정된 속성의 값이 사용할 수 없는 문자열을 포함할 수 있도록 하여 사이트간 스크립트 보호에서 WebSphere Commerce 명령을 제외하려면 다음과 같이 고급 탭을 사용하십시오.

   a. 명령 목록 상자에서 명령을 선택하십시오.

   b. 사용할 수 없는 문자가 예외 속성 목록 창에서 허용되는 속성 목록을 쉼표로 구분하여 입력하고 **추가**를 누르십시오.

   c. 속성과 함께 명령을 제거하려면 예외 명령 목록 창에서 명령을 선택하고 **제거**를 누르십시오.

   또한 속성을 선택하고 **제거**를 눌러 명령에서 특정 속성을 제거할 수도 있습니다.

4. 변경사항을 구성 관리자에 적용하려면 **적용**을 누르십시오.
5. 인스턴스에 대한 구성을 성공적으로 갱신할 때 갱신 성공을 표시하는 메시지가 수신됩니다.
6. WebSphere Application Server 관리 콘솔에서 WebSphere Commerce 서버 인스턴스를 중지한 후 다시 시작하십시오.

주:

1. 명령이 사이트간 스크립트 보호에서 제외될 때 지정된 속성의 값이 기호의 HTML 인코딩을 사용하여 인코드됩니다. 예를 들어, 명령 cmd1?user=<Thomas>는 ascmd1?user=<Thomas>로 인코드됩니다.
2. 사용할 수 없는 문자 필드에 문자열을 지정할 때 다음에 주의하십시오.
   - 일련의 특정 문자는 문자열이 URL 인코딩 표준에 따라서 단일 문자로 변환될 수 있습니다. 예를 들어, 문자열 <%bb는 문자열 <*X*로 변환되는데 *X*는 HEX 'bb'(10진수 187)의 16진 표시 값을 갖는 단일 문자입니다. 이 경우, 문자열 <%bb는 URL에서 전달되는 경우 사이트간 스크립트 보호에 의해 포착되지 않습니다.
   - 일련의 특정 문자는 URL 인코딩 표준을 따르지 않는 경우 문자열 변환에 실패하게 만들 수 있습니다. 예를 들어, 문자열 <%gg는 HEX 'gg'가 올바른 16진 값 표시가 아니므로 변환에 실패하게 만듭니다. 이 경우, 문자열 <%gg는 예외를 유발하여 사이트간 스크립트 보호가 사용되는지 여부와 상관없이 이러한 문자열을 포함하는 URL 요청에 대한 응답이 없게 됩니다.

예: 다음 예를 고려하십시오.

- 사용할 수 없는 문자열: <SCRIPT, <%

  사용할 수 없는 속성: mycomment, description

명령	상태
cmd1?description=Available...	거부됨
cmd2?userid=Thomas...	승인됨
cmd3?mycomment=<SCRIPT>...	거부됨
cmd4?password=<%...%>...	거부됨

- cmd1 명령의 text 속성이 사용할 수 없는 문자열(<SCRIPT, <%)을 포함할 수 있게 하고 다른 속성(예: txt 속성)은 허용하지 않으려는 경우, cmd1을 제외하고 예상 속성으로 text를 지정할 수 있습니다.

명령	상태
cmd1?text=<SCRIPT>...	승인됨
cmd1?text=<%...%>...	승인됨
cmd1?txt=<SCRIPT>...	거부됨
cmd1?txt=<%..%>...	거부됨

구성 관리자 - 액세스 로그 작성 사용

액세스 로그 작성 기능은 사용될 때 WebSphere Commerce 서버로 들어오는 모든 요청 또는 액세스 위반의 결과인 요청만을 기록합니다. 액세스 위반 예로는 인증 실패, 충분하지 않은 명령 실행 권한 또는 암호 규칙을 위반하는 암호를 사이트에 재설정하는 것 등이 있습니다. 이 기능이 사용될 때 WebSphere Commerce 운영자가 WebSphere Commerce 시스템에 대한 보안 위협을 빨리 식별할 수 있습니다.

인증 실패 또는 권한 부여 실패 이벤트가 발생할 때 다음 정보가 액세스 로그 파일 데이터베이스 테이블인 ACCLOGMAIN 및 ACCLOGSUB에 기록됩니다.

- 클라이언트의 호스트 이름
- 명령을 실행하는 스레드의 ID
- 클라이언트의 사용자 ID
- 이벤트가 발생한 시간
- 실행된 명령
- 명령이 실행된 상점
- 조작이 수행된 자원
- 액세스 제어 확인 결과

액세스 로그 작성을 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 실행하십시오.
2. **호스트 이름 → 인스턴스**를 선택한 후 **구성요소** 폴더를 여십시오.
3. **AccessLoggingEventListener**를 선택하십시오.
4. 일반 패널에서 **구성요소 사용** 선택란을 활성화하십시오.
5. 고급 패널을 선택하고 **시작**을 사용하십시오.
6. **적용**을 누르십시오
7. 구성 관리자를 종료하십시오.
8. WebSphere Application Server를 다시 시작하십시오.

로그 파일의 크기를 변경하거나 모든 요청이 기록되는지 여부를 지정하려면 WebSphere Commerce 인스턴스 서브디렉토리에 있는 WebSphere Commerce 인스턴스에 대한 *instance*.xml 파일을 수동으로 편집해야 합니다.

1. 편집기에 인스턴스에 대한 *instance*.xml 파일을 여십시오.
2. <LogSystem>/<activitylog> 노드에 있는 다음 노드를 찾으십시오.

   ```
   <accessLogging cacheSize="aa" logAllRequests="bbbbb" />
   ```

   여기서,

- *aa*는 항목이 데이터베이스에 기록되기 전에 메모리에 기록되는 최대 항목 수를 지정하는 정수 값입니다. 일반적으로 숫자가 높을수록 액세스 로그 작성에 관한 성능이 향상됩니다. 기본값은 32입니다.
- *bbbbb*는 `true` 또는 `false`입니다. 값 `true`는 모든 들어오는 요청이 기록됨을 의미합니다. 값 `false`는 액세스 위반만이 기록됨을 의미합니다. 과다하거나 불필요한 로그 작성을 방지하기 위해 값 `false`가 권장됩니다. 사이트에서의 인증 문제점이나 보안 위반을 의심할 때만 `true`를 사용하십시오. 기본값은 `false`입니다.

3. 갱신을 완료했을 때 WebSphere Commerce 인스턴스에 대한 *instance*`.xml` 파일을 저장하십시오.
4. WebSphere Application Server를 다시 시작하십시오.

다음 예에서 액세스 로그 작성은 데이터베이스 테이블에 항목을 로그 작성하기 전에 메모리에 3 항목을 보관합니다. 또한 WebSphere Commerce 서버에 대한 모든 들어오는 요청을 기록합니다.

```
<accessLogging cacheSize="3" logAllRequests="true" />
```

운영자 - 계정 정책

WebSphere Commerce 운영자의 이 페이지를 사용하여 계정 정책을 설정할 수 있습니다. 계정 정책은 암호 및 계정 잠금 정책 같은 계정 관련 정책을 정의합니다. 이 페이지에서

- **새로 만들기**를 눌러 새 정책을 작성할 수 있습니다.
- 목록에서 정책을 선택하고 **변경**을 눌러 기존 정책의 특성을 변경할 수 있습니다.
- 목록에서 정책을 선택하고 **삭제**를 눌러 기존 정책을 삭제할 수 있습니다.

새 계정 정책을 작성하려면 다음을 수행하십시오.

1. 관리 콘솔을 여십시오.
2. 관리 콘솔의 보안 드롭 다운 메뉴에서 **계정 정책**을 누르십시오.
3. 이름 필드에 계정 정책에 대한 이름을 입력하십시오(예: `my_account_policy`).
4. 암호 정책 메뉴에서 이미 존재하는 암호 정책을 선택하십시오.
5. 계정 잠금 정책 메뉴에서 이미 존재하는 계정 잠금 정책을 선택하십시오.
6. **확인**을 누르십시오.

계정 정책을 작성한 후에는 사용자에게 해당 정책을 지정할 수 있습니다. 계정 정책을 사용 중인 경우(즉, 사용자에게 계정 정책이 지정된 경우)에는 해당 계정 정책을 삭제할 수 없음에 유의하십시오.

또한 WebSphere Commerce 온라인 도움말의 참조 주제 ″기본 인증 정책″도 참조하십시오.

운영자 - 암호 정책

WebSphere Commerce 운영자의 이 페이지를 사용하면 암호의 특성을 정의하여 암호가 사이트의 보안 정책을 따르도록 보장하기 위해 사용자의 암호 선택을 제어할 수 있습니다.

- **새로 만들기**를 눌러 새 정책을 작성할 수 있습니다.
- 목록에서 정책을 선택하고 **변경**을 눌러 기존 정책의 특성을 변경할 수 있습니다.
- 목록에서 정책을 선택하고 **삭제**를 눌러 기존 정책을 삭제할 수 있습니다.

이 기능은 암호가 따라야 하는 속성을 정의합니다. 암호 정책은 다음 조건을 강제 시행합니다.

- 사용자 ID와 암호가 일치할 수 있는지 여부
- 연속 문자의 최대 발생
- 모든 문자의 최대 인스턴스 수
- 암호의 최대 수명
- 최소 영문자 수
- 최소 숫자 수
- 최대 암호 길이
- 사용자의 이전 암호의 재사용 가능 여부

새 암호 정책을 작성하려면 다음을 수행하십시오.

1. 관리 콘솔을 여십시오.
2. 관리 콘솔의 보안 드롭 다운 메뉴에서 **암호 정책**을 누르십시오.
3. 이름 필드에 암호 정책에 대한 이름을 입력하십시오(예: `my_password_policy`).
4. 필요한 대로 다음을 갱신하여 구매자에 대한 기본값에서 임의의 값을 수정하십시오.
   - **사용자 ID와 암호가 일치할 수 있습니까?** 사용자 ID와 암호가 동일할 수 있는지 여부를 정의합니다. 목록에서 예 또는 아니오를 선택하십시오.
   - **최대 연속 문자 유형**. 암호에서 연속 문자의 최대 발생을 정의합니다. 최소값은 두 개의 연속 문자입니다. 예를 들어, 값 2를 사용할 때 `aaabc` 같은 암호를 입력할 수 없습니다.
   - 모든 문자의 **최대 인스턴스 수.** 동일한 문자가 한 암호에 나타날 수 있는 최대 횟수를 정의합니다. 최소값은 한 문자의 1 인스턴스입니다. 예를 들어, 값 2를 사용하면 `abcaabc` 같은 암호를 입력할 수 없습니다.

- **암호의 최대 수명.** 암호가 존재할 수 있는 최대 시간을 일 단위로 정의합니다. 최소값은 1일입니다. 이 기간 후에는 사용자에게 암호를 변경하라는 프롬프트가 표시됩니다.
- **최소 영문자 수**. 암호에 사용되는 최소 영문자 수를 정의합니다. 최소값은 0개의 영문자입니다.
- **최소 숫자 수**. 암호에 사용되는 최소 숫자 수를 정의합니다. 최소값은 0개의 숫자입니다.
- **최소 암호 길이**. 암호의 가장 작은 길이를 문자 단위로 정의합니다. 최소값은 1 문자입니다.
- **암호 재사용 여부?** 사용자의 이전 암호를 재사용할 수 있는지 여부를 정의합니다. 목록에서 예 또는 아니오를 선택하십시오.

5. **확인**을 누르십시오.

주:

1. 암호 정책을 사용 중인 경우(즉, 사용자에게 해당 암호 정책이 지정된 경우)에는 암호 정책을 삭제할 수 없습니다.
2. 암호 정책은 사용자가 WebSphere Commerce 데이터베이스에 대해 인증되는 경우에만 강제 시행됩니다.

또한 WebSphere Commerce 온라인 도움말의 참조 주제 ″기본 인증 정책″도 참조하십시오.

운영자 - 계정 잠금 정책

WebSphere Commerce 운영자의 이 페이지를 사용하여 WebSphere Commerce 내의 여러 사용자 역할에 대한 계정 잠금 정책을 설정할 수 있습니다. 계정 잠금 정책은 사용자 계정에 대해 나쁜 의도의 조치가 실행되는 경우, 조치가 계정을 손상시키는 기회를 줄이기 위해 해당 계정을 사용 불가능하게 만듭니다.

계정 잠금 정책은 다음 항목을 강제 시행합니다.

- 계정 잠금 임계값. 이것은 계정이 사용되기 전의 올바르지 않은 로그온 시도 횟수입니다.
- 연속 실패 로그인 지연. 이것은 두 번의 로그인 시도 실패 후에 사용자가 로그인할 수 없는 기간입니다. 연속으로 로그인에 실패할 때마다 지연이 구성된 시간 지연 값(예: 10초)만큼 증가됩니다.

계정 잠금 정책을 설정하려면 다음을 수행하십시오.

1. 관리 콘솔을 여십시오.
2. 관리 콘솔의 보안 드롭 다운 메뉴에서 **계정 잠금 정책**을 누르십시오.
3. 계정 잠금 정책 페이지가 모든 기존 계정 잠금 정책을 나열합니다. 이 페이지에서

- **새로 만들기**를 눌러 새 정책을 작성할 수 있습니다.
- 목록에서 정책을 선택하고 **변경**을 눌러 기존 정책의 특성을 변경할 수 있습니다.
- 목록에서 정책을 선택하고 **삭제**를 눌러 기존 정책을 삭제할 수 있습니다.

새 계정 잠금 정책의 경우, 계정 잠금 정책 페이지에서

1. 이름 필드에 계정 잠금 정책에 대한 이름을 입력하십시오(예: `my_policy`).
2. 계정 잠금 임계값 필드에 계정 잠금 임계값을 입력하십시오. 예를 들어, 6(여섯 번의 시도의 경우)을 입력하십시오.
3. 대기 시간 필드에 연속 실패 로그인 지연을 초 단위로 입력하십시오. 예를 들어, 10(10초의 경우)을 입력하십시오.
4. **확인**을 누르십시오.

주:

1. 계정 잠금 정책을 사용 중인 경우(즉, 사용자에게 계정 잠금 정책이 지정된 경우)에는 해당 계정 잠금 정책을 삭제할 수 없습니다.
2. 계정 잠금 정책은 사용자가 WebSphere Commerce 데이터베이스에 대해 인증되는 경우에만 강제 시행됩니다.

운영자 - 보안 확인 실행

400 이 기능은 iSeries용 WebSphere Commerce에 적용되지 않습니다.

이 페이지를 사용하여 가능한 보안 노출을 포함할 수 있는 임시 WebSphere Commerce 파일을 검사하고 삭제하는 보안 프로그램을 수동으로 실행할 수 있습니다. 일반적으로 보안 실행 프로그램은 계획된 작업으로 실행하며 기본적으로 한 달에 한 번 실행하도록 설정됩니다.

보안 확인 프로그램을 호출하려면 다음을 수행하십시오.

1. 관리 콘솔을 여십시오.
2. 관리 콘솔의 보안 드롭 다운 메뉴에서 **보안 확인**을 누르십시오.
3. 보안 확인 실행 페이지에서 **실행**을 누르십시오.

프로그램에서 취한 모든 조치를 포함한 보안 확인의 결과는 보안 확인 로그 창과 로그 서브디렉토리의 `sec_check.log` 파일에 기록됩니다.

NT *drive*:\WebSphere\Commerce\instances*instance_name*\log

2000 *drive*:\Program Files\WebSphere\Commerce\instances*instance_name*\log

AIX /usr/lpp/Commerce/instances/*instance_name*/log

Solaris /opt/WebSphere/Commerce/instances/*instance_name*/log

Windows Windows 이외의 플랫폼에서는 중요한 파일을 권한이 없는 사용자가 액세스할 수 없도록 하기 위해 파일 권한이 WebSphere Commerce에서 자동으로 설정됩니다. Windows 플랫폼에서는 사용자가 다음과 같이 수동으로 권한을 설정해야 합니다. 이 프로시저는 운영자 그룹만이 중요한 파일에 대한 read/write/execute 권한을 갖도록 합니다.

1. Windows 탐색기에서 *drive*:\WebSphere 폴더를 오른쪽 마우스 버튼으로 누르십시오.
2. **특성**을 누르고 **보안**을 누르십시오. 기본적으로 "Everyone" 그룹은 이 폴더에 대해 **모든** 권한을 갖습니다.
3. **추가**를 누르십시오
4. 창이 표시됩니다(사용자, 컴퓨터 선택...). 이 창에서 **운영자** 그룹을 선택하십시오.

   주: 운영자를 사용자로 볼 수 있으므로 여기에서는 약간 애매모호할 수 있지만 운영자 사용자가 아닌 운영자 그룹을 추가해야 합니다.

   추가를 누른 후 **확인**을 누르십시오.
5. 보안 탭에 운영자 그룹이 추가되었습니다. "Everyone"을 제거해야 합니다. **Everyone**을 선택하고 "계승 가능한 권한 허용...."이라는 상자를 선택 취소하십시오.
6. 표시되는 보안 창의 **제거**를 누르십시오.

제 5 장 WebSphere™ Application Server 보안 사용

이 장에서는 WebSphere Application Server에 대한 보안 기능을 사용하는 방법에 대해 설명합니다. WebSphere Application Server 보안을 사용하면 모든 엔터프라이즈 JavaBean 구성요소가 다른 사람의 원격 호출에 노출되지 않게 합니다.

Windows UNIX

주: WebSphere Application Server 보안 사용시, 시스템이 다음 요구사항을 충족시키는 것이 가장 바람직합니다.

- 최소 1GB 시스템 메모리
- WebSphere Commerce 응용프로그램을 위한 최소 384MB의 힙 크기

시작하기 전에

보안 사용을 시작하기 전에 보안을 사용하려는 WebSphere Application Server가 사용자 ID의 유효성을 검증하는 방법을 알아야 합니다. WebSphere Application Server는 LDAP 또는 운영체제의 사용자 레지스트리를 WebSphere Application Server 사용자 레지스트리로 사용할 수 있습니다.

LDAP 사용자 레지스트리를 사용한 보안 사용

Windows LDAP를 WebSphere Application Server 사용자 레지스트리로 사용 중일 때 WebSphere Application Server 보안을 사용하려면 관리 권한을 갖는 사용자로서 시스템에 로그인하고 다음 단계를 수행하십시오.

UNIX LDAP를 WebSphere Application Server 사용자 레지스트리로 사용 중일 때 WebSphere Application Server 보안을 사용하려면 `wasuser`로서 시스템에 로그인하고 다음 단계를 수행하십시오.

1. WebSphere Application Server 관리 서버를 시작하고 WebSphere Application Server 운영자의 콘솔을 여십시오.
2. 콘솔에서 글로벌 보안 설정을 다음과 같이 수정하십시오.
   a. 콘솔 메뉴에서 **보안 센터**를 선택하십시오.
   b. 일반 탭에서 **보안 사용**을 선택하십시오.
   c. **인증** 탭에서 LTPA(Lightweight Third Party Authentication)를 선택하십시오. LTPA 설정을 채우고, 기능을 사용하지 않으려는 경우에는 **단일 사인온 사용** 선택란을 선택 취소하십시오. 사용 중인 디렉토리 서버의 유형에 따라 다음과 같이 **LDAP 설정** 탭을 채우십시오.

표 8. *SecureWay 사용자*

필드 이름	정의	견본 값	주
보안 서버 ID	사용자 ID	*user_ID*	• 이것은 LDAP 운영자가 아니어야 합니다. • cn=xxx로 지정된 사용자를 사용하지 마십시오. • 이 사용자의 오브젝트 클래스가 LDAP 고급 특성 창의 사용자 필터 필드에 지정된 오브젝트 클래스와 호환되는지 확인하십시오.
보안 서버 암호	사용자 암호	*password*	
디렉토리 유형	LDAP 서버의 유형	SecureWay	
호스트	LDAP 서버의 호스트 이름	*hostname.domain.com*	
포트	LDAP 서버가 사용 중인 포트		이 필드는 필수가 아닙니다.
기본 인식 이름	검색이 발생하는 인식 이름	o=ibm, c=us	
바인드 인식 이름	검색할 때 디렉토리에 바인드하기 위한 인식 이름		이 필드는 필수가 아닙니다.
바인드 암호	바인드 인식 이름에 대한 암호		이 필드는 필수가 아닙니다.

Windows

표 9. *Netscape 사용자*

필드 이름	정의	견본 값	주
보안 서버 ID	사용자 ID	*user_ID*	• 이것은 LDAP 운영자가 아니어야 합니다. • cn=xxx로 지정된 사용자를 사용하지 마십시오. • 이 사용자의 오브젝트 클래스가 LDAP 고급 특성 창의 사용자 필터 필드에 지정된 오브젝트 클래스와 호환되는지 확인하십시오.
보안 서버 암호	사용자 암호	*password*	
디렉토리 유형	LDAP 서버의 유형	Netscape	

표 9. Netscape 사용자 (계속)

필드 이름	정의	견본 값	주
호스트	LDAP 서버의 호스트 이름	*hostname.domain.com*	
포트	LDAP 서버가 사용 중인 포트		이 필드는 필수가 아닙니다.
기본 인식 이름	검색이 발생하는 인식 이름	o=ibm	
바인드 인식 이름	검색할 때 디렉토리에 바인드하기 위한 인식 이름		이 필드는 필수가 아닙니다.
바인드 암호	바인드 인식 이름에 대한 암호		이 필드는 필수가 아닙니다.

Windows

표 10. Domino 사용자

필드 이름	정의	견본 값	주
보안 서버 ID	짧은 이름/사용자 ID	*user_ID*	이 사용자의 오브젝트 클래스가 LDAP 고급 특성 창의 사용자 필터 필드에 지정된 오브젝트 클래스와 호환되는지 확인하십시오.
보안 서버 암호	사용자 암호	*password*	
디렉토리 유형	LDAP 서버의 유형	Domino 5.0	
호스트	LDAP 서버의 호스트 이름	*hostname.domain.com*	
포트	LDAP 서버가 사용 중인 포트		이 필드는 필수가 아닙니다.
기본 인식 이름	검색이 발생하는 인식 이름		이 필드는 필수가 아닙니다.
바인드 인식 이름	검색할 때 디렉토리에 바인드하기 위한 인식 이름		이 필드는 필수가 아닙니다.
바인드 암호	바인드 인식 이름에 대한 암호		이 필드는 필수가 아닙니다.

Windows

표 11. 활성화 디렉토리 사용자

필드 이름	정의	견본 값	주
보안 서버 ID	sAMAccountName	*user_ID*	• 모든 일반 사용자의 사용자 로그온 이름. • cn=xxx로 지정된 사용자를 사용하지 마십시오. • 이 사용자의 오브젝트 클래스가 LDAP 고급 특성 창의 사용자 필터 필드에 지정된 오브젝트 클래스와 호환되는지 확인하십시오.
보안 서버 암호	사용자 암호	*password*	
디렉토리 유형	LDAP 서버의 유형	활성화 디렉토리	
호스트	LDAP 서버의 호스트 이름	*hostname.domain.com*	
포트	LDAP 서버가 사용 중인 포트		이 필드는 필수가 아닙니다.
기본 인식 이름	검색이 발생하는 인식 이름	CN=users, DC=domain1, DC=domain2, DC=com	
바인드 인식 이름	검색할 때 디렉토리에 바인드하기 위한 인식 이름	CN=*user_ID*, CN=users, DC=domain1, DC=domain2, DC=com	*user_ID* 값은 표시 이름입니다. 이것이 사용자 로그온 이름과 반드시 같지는 않습니다.
바인드 암호	바인드 인식 이름에 대한 암호	*bind_password*	이것은 보안 서버 암호와 동일해야 합니다.

d. **역할 맵핑** 탭에서 WCS appserver를 선택하고 **맵핑 편집...** 버튼을 누르십시오.
   1) WCSSecurity 역할을 선택하고 **선택...** 버튼을 누르십시오.
   2) 사용자/그룹 선택 선택란을 선택하고 55 페이지의 2c단계에서 입력된 사용자 ID를 추가하십시오.

e. **완료**를 누르십시오.

3. 관리 콘솔을 닫고 WebSphere Application Server 관리 서버를 중지한 후 다시 시작하십시오. 이제부터 WebSphere Application Server 운영자의 콘솔을 열 때 보안 서버 ID와 암호를 입력하도록 프롬프트가 표시됩니다.

4. WebSphere Commerce 구성 관리자를 열고 **인스턴스** → *instance_name* → **인스턴스 등록 정보** → **보안**을 선택한 후 **사용** 선택란을 누르십시오. 55 페이지의 2c단계에서 입력한 사용자 이름과 암호를 입력하도록 프롬프트가 표시됩니다. **적용**을 누른 후 구성 관리자를 종료하십시오.
5. WebSphere Application Server 관리 서버를 중지한 후 다시 시작하십시오.

운영체제 사용자 레지스트리를 사용한 보안 사용

운영체제 사용자 유효성 검증을 WebSphere Application Server 사용자 레지스트리로 사용할 때 WebSphere Application Server 보안을 사용하려면 관리 권한을 갖는 사용자로서 로그인한 후 다음 단계를 수행하십시오.

1. WebSphere Application Server 관리 콘솔에서 다음과 같이 글로벌 보안 설정을 수정하십시오.
   a. 콘솔 메뉴에서 **보안 센터**를 선택하십시오.
   b. 일반 탭에서 **보안 사용** 선택란을 선택하십시오.
2. **인증** 탭을 선택하고 **로컬 운영체제** 라디오 버튼을 선택하십시오.
3. **보안 서버 ID** 필드에 보안 서버 ID를 입력하십시오. 다음과 같이 사용자 이름을 입력하십시오.

표 12.

필드 이름	견본 값	주
사용자 ID	*user_ID*	Windows 사용자가 로그인시 사용한 운영체제 관리 특권을 갖는 사용자 ID. 시스템이 도메인에 속하는 경우, 완전한 사용자 ID를 사용하십시오(예를 들면, DomainXYZ\user_id). 이 계정이 도메인 서버에 존재하고 운영자 그룹의 구성원인지 확인하십시오. UNIX 루트 또는 루트 권한을 갖는 사용자 ID.
보안 서버 암호	*password*	이것은 사용자가 로그인시 사용한 운영체제 관리 특권을 갖는 사용자에 속하는 암호입니다.

4. **역할 맵핑** 탭에서 WC 엔터프라이즈 응용프로그램을 선택하고 **맵핑 편집...** 버튼을 누르십시오.
   a. WCSecurityRole을 선택하고 **선택...** 버튼을 누르십시오.
   b. 사용자/그룹 선택 선택란을 선택하고, 3단계에서 사용된 사용자 ID를 검색 필드에 입력한 후 **검색**을 누르십시오. 사용 가능한 사용자/그룹 목록에서 해당 사용자를 선택하고 **추가**를 눌러 선택된 사용자/그룹 목록에 추가하십시오. 그런 다음 보안 센터를 종료할 때까지 각 패널의 **확인**을 누르십시오.

5. WebSphere Commerce 구성 관리자를 열고 **인스턴스 목록** → *instance_name* → **인스턴스 등록 정보** → **보안**을 선택하고 **보안 사용** 선택란을 선택하십시오. 인증 모드에 대한 **운영체제 사용자 레지스트리**를 선택하고 59 페이지의 3단계에서 입력한 사용자 이름과 암호를 입력하십시오. **적용**을 누른 후 구성 관리자를 종료하십시오.
6. WebSphere Application Server 관리 서버를 중지한 후 다시 시작하십시오. 이제부터 WebSphere Application Server 관리 콘솔을 열 때 보안 서버 ID와 암호를 입력하도록 프롬프트가 표시됩니다

WebSphere Commerce EJB 보안 사용 안함

WebSphere Commerce Business Edition에서 EJB 보안을 사용하지 않을 수 있습니다. WebSphere Commerce EJB 보안을 사용하지 않으려면 다음을 수행하십시오.

1. WebSphere Application Server 관리 콘솔을 시작하십시오
2. **콘솔** → **보안 센터...**를 누르고 **일반** 탭의 **보안 사용** 선택란을 선택 취소하십시오.
3. WebSphere Commerce 구성 관리자를 열고 **인스턴스 목록** → *instance_name* → **인스턴스 등록 정보** → **보안**을 선택한 후 **보안 사용** 선택란을 지우십시오.
4. WebSphere Application Server 관리 콘솔을 종료하십시오.
5. WebSphere Application Server 관리 서버를 중지한 후 다시 시작하십시오.

WebSphere Commerce 보안 배치 옵션

WebSphere Commerce는 다양한 보안 배치 구성을 지원합니다. 다음 표에서는 사용자가 사용할 수 있는 보안 배치 옵션에 대해 설명합니다.

표 13. 단일 시스템 보안 시나리오

WebSphere Application Server 보안이 사용됩니다.	• 운영체제를 WebSphere Application Server 레지스트리로 사용하십시오. • 데이터베이스를 WebSphere Commerce 레지스트리로 사용하십시오.
	• LDAP를 WebSphere Application Server 레지스트리로 사용하십시오. • LDAP를 WebSphere Commerce 레지스트리로 사용하십시오
	• LDAP를 WebSphere Application Server 레지스트리로 사용하십시오.

표 13. 단일 시스템 보안 시나리오 (계속)

WebSphere Application Server 보안이 사용되지 않고 WebSphere Commerce 사이트가 방화벽 뒤에 있습니다.	• WebSphere Application Server 레지스트리가 필수가 아닙니다. • 데이터베이스를 WebSphere Commerce 레지스트리로 사용하십시오.
	• WebSphere Application Server 레지스트리가 필수가 아닙니다. • LDAP를 WebSphere Commerce 레지스트리로 사용하십시오.

표 14. 복수 시스템 보안 시나리오

WebSphere Application Server 보안이 사용됩니다. LDAP가 항상 전개됩니다.	• LDAP를 WebSphere Application Server 레지스트리로 사용하십시오. • LDAP를 WebSphere Commerce 레지스트리로 사용하십시오
	• LDAP를 WebSphere Application Server 레지스트리로 사용하십시오. • 데이터베이스를 WebSphere Commerce 레지스트리로 사용하십시오. • LDAP를 설정하고 LDAP 레지스트리에 하나의 관리 항목을 배치해야 합니다.
WebSphere Application Server 보안이 사용되지 않고 WebSphere Commerce 사이트가 방화벽 뒤에 있습니다.	• 데이터베이스를 WebSphere Commerce 레지스트리로 사용하십시오. • WebSphere Application Server 레지스트리가 필수가 아닙니다. • 단일 사인온이 지원되지 않습니다.
	• LDAP를 WebSphere Application Server 레지스트리로 사용하십시오. • WebSphere Application Server 레지스트리가 필수가 아닙니다.

주: WebSphere Commerce 사이트를 방화벽 뒤에서 운영하는 경우, WebSphere Application Server 보안을 사용하지 않을 수 있습니다. 방화벽 뒤에서 악성 응용프로그램이 실행 중이 아니라고 확신하는 경우에만 WebSphere Application Server 보안을 사용하지 않아야 합니다.

제 6 장 세션 관리

웹 브라우저와 전자상거래 사이트는 HTTP를 사용하여 통신합니다. HTTP가 stateless 프로토콜이기 때문에(각 명령이 이전의 명령에 대해 어떤 지식도 없이 독립적으로 실행됨을 의미) 브라우저측과 서버측 사이에 세션을 관리할 방법이 있어야 합니다.

WebSphere Commerce는 두 유형의 세션 관리(*쿠키* 기반과 URL 재작성)를 지원합니다. 운영자는 *쿠키* 기반 세션 관리만을 지원하거나 *쿠키* 기반 및 URL 재작성 세션 관리를 모두 지원하도록 선택할 수 있습니다. WebSphere Commerce가 *쿠키* 기반만을 지원하는 경우, 구매자의 브라우저가 *쿠키*를 승인할 수 있어야 합니다. *쿠키* 기반 및 URL 재작성이 모두 선택되는 경우에는 WebSphere Commerce가 먼저 *쿠키*를 사용하여 세션을 관리하려고 시도하고, 구매자의 브라우저가 *쿠키*를 승인하지 않도록 설정된 경우에는 URL 재작성이 사용됩니다.

쿠키 기반 세션 관리

쿠키 기반 세션 관리가 사용될 때 사용자의 정보가 들어 있는 메시지(*쿠키*)가 웹 서버에 의해 브라우저로 보내집니다. 이 *쿠키*는 사용자가 특정 페이지에 액세스하려고 시도할 때 다시 서버로 보내집니다. *쿠키*를 다시 보내면 서버는 사용자를 식별하고 세션 데이터베이스에서 사용자의 세션을 검색할 수 있으므로 사용자의 세션을 관리합니다. *쿠키* 기반 세션은 사용자가 로그오프하거나 브라우저를 닫을 때 종료합니다. *쿠키* 기반 세션 관리는 안전하며 성능상의 이점을 갖습니다. *쿠키* 기반 세션 관리가 구매자 세션에 권장됩니다. URL 재작성을 사용하지 않고 사용자가 자신의 브라우저에서 *쿠키*를 사용하게 하려는 경우, 구성 관리자의 세션 관리 페이지에서 **쿠키 수용 테스트**를 선택하십시오.

보안상의 이유로 *쿠키* 기반 세션 관리는 다음 두 유형의 *쿠키*를 사용합니다.

- 비보안 세션 *쿠키*

  세션 데이터를 관리하는 데 사용됩니다. 세션 ID, 협상된 언어, 현재 상점 및 *쿠키*가 구성될 때의 구매자 선호 통화가 들어 있습니다. 이 *쿠키*는 SSL 또는 non-SSL 연결을 통해 브라우저와 서버 사이에 이동할 수 있습니다. 비보안 세션 *쿠키*에는 다음 두 유형이 있습니다.

  – WebSphere Application Server 세션 *쿠키*는 Servlet HTTP 세션 표준을 바탕으로 합니다. WebSphere Application Server *쿠키*는 메모리 또는 다중 노드 배치의 데이터베이스로 지속됩니다. 자세한 내용은 `http://www.ibm.com/software/webservers/appserv/infocenter.html`에 있는 WebSphere Application Server InfoCenter에서 "세션 관리"를 검색하십시오.

– WebSphere Commerce 세션 쿠키는 WebSphere Commerce에 내부적이며 데이터베이스로 지속되지 않습니다.

사용할 쿠키 유형을 선택하려면 구성 관리자의 세션 관리 페이지에 있는 **쿠키 세션 관리자** 매개변수에 대해 WCS 또는 WAS를 선택하십시오.

- 보안 인증 쿠키

  인증 데이터를 관리하는 데 사용됩니다. 인증 쿠키는 SSL을 통해 이동하며 최대 보안을 위해 시간소인이 붙습니다. 이것은 사용자를 인증하는 데 사용되는 쿠키이지만, 중요한 명령, 예를 들어, 사용자에게 신용 카드 번호를 묻는 DoPaymentCmd가 실행됩니다. 이 쿠키가 도난되어 권한이 없는 사용자에 의해 사용될 수 있는 아주 작은 위험이 있습니다. 쿠키 기반 세션 관리가 사용될 때마다 인증 코드 쿠키가 WebSphere Commerce에 의해 항상 생성됩니다.

세션 및 인증 코드 쿠키가 모두 보안 페이지를 보기 위해 필요합니다.

쿠키 오류에 대해 CookieErrorView가 다음 경우에 호출됩니다.

- 사용자가 동일한 로그온 ID를 갖고 다른 위치에서 로그인했습니다.
- 쿠키가 손상되었거나 부당하게 변경되었습니다.
- 쿠키 수용이 "true"로 설정되고 사용자의 브라우저가 쿠키를 지원하지 않습니다.

세션 관리를 위한 쿠키 사용

WebSphere Commerce에서 쿠키를 사용하려면 다음을 수행하십시오.

1. 구성 관리자를 여십시오.
2. **인스턴스**를 선택한 후 **세션 관리** 폴더를 여십시오.
3. 적절한 세션 값을 선택하십시오.
   - 쿠키 수용 테스트

     쿠키만을 지원하는 사이트의 경우 고객의 브라우저가 쿠키를 수용하는지 확인하려면 이 선택란을 선택하십시오.
   - 쿠키 세션 관리자

     쿠키를 관리할 WebSphere Commerce 또는 WebSphere Application Server를 선택하십시오. 기본값은 WebSphere Commerce입니다.
     – WebSphere Application Server 세션 쿠키는 Servlet HTTP 세션 표준을 바탕으로 합니다. WebSphere Application Server 쿠키는 메모리 또는 다중 노드 배치의 데이터베이스로 지속됩니다. 자세한 내용은 http://www.ibm.com/software/webservers/appserv/infocenter.html에 있는 WebSphere Application Server InfoCenter에서 "세션 관리"를 검색하십시오.
     – WebSphere Commerce 세션 쿠키는 WebSphere Commerce에 내부적이며 데이터베이스로 지속되지 않습니다.

4. **고급** 탭을 누르십시오. 적절한 세션 값을 선택하십시오.
   - *쿠키 경로*

     대개 이 필드는 수정하지 않아야 합니다. *쿠키*가 보내질 URL의 서브세트인 *쿠키*에 대한 *경로*를 지정합니다.
   - *쿠키 연령*

     이 필드는 수정하지 않아야 합니다. 기본값은 브라우저가 닫힐 때 *쿠키*가 만기되는 것입니다.
   - *쿠키 도메인*

     대개 이 필드는 수정하지 않아야 합니다. 도메인 제한 패턴을 지정합니다. 도메인은 *쿠키*를 볼 서버를 지정합니다. 기본적으로 *쿠키*는 *쿠키*를 발행한 WebSphere Commerce 서버로만 다시 보내집니다. 기본적으로 *쿠키*는 *쿠키*를 저장한 *호스트*에만 리턴됩니다. 도메인 이름 패턴을 지정하면 이것이 대체됩니다. 패턴은 점으로 시작하고 최소한 두 개의 점을 포함해야 합니다. 패턴은 *초기* 점 이후의 한 항목만을 일치시킵니다. 예를 들어 ".ibm.com"은 올바르며 a.ibm.com 및 b.ibm.com과는 일치하지만 www.a.ibm.com과는 일치하지 않습니다. 도메인 패턴에 대한 자세한 내용은 Netscape의 *쿠키* 스펙 및 RFC 2109를 참조하십시오.
5. **적용**을 누르십시오.
6. 구성 관리자를 닫으십시오.
7. WebSphere Application Server 관리 콘솔에서 인스턴스를 중지한 후 다시 시작하십시오.

URL 재작성

URL 재작성을 사용할 때 브라우저로 리턴되거나 경로 재지정된 모든 링크에 세션 ID가 추가됩니다. 사용자가 이들 링크를 누를 때 URL의 재작성된 양식이 클라이언트 요청의 일부로 서버에 보내집니다. Servlet 엔진이 URL에 있는 세션 ID를 인식하고 이 사용자에 대한 적합한 오브젝트를 얻기 위해 세션 ID를 저장합니다. URL 재작성을 사용하려면 링크에 HTML 파일 확장자(.html 또는 .htm인 파일)를 사용할 수 없습니다. URL 재작성을 사용하려면 표시 목적을 위해 JSP 파일을 사용해야 합니다. URL 재작성을 갖는 세션은 구매자가 로그오프할 때 만기됩니다.

URL 재작성 세션 관리 사용

세션이 관리되는 방법을 지정하려면 다음을 수행하십시오.

1. 구성 관리자를 여십시오.
2. **인스턴스**를 선택한 후 **세션 관리** 폴더를 여십시오.
3. 적절한 세션 값을 선택하십시오.

   URL 재작성 사용. 세션 관리에 URL 재작성을 사용하려면 이 선택란을 선택하십시오.

쿠키 세션 관리자. WebSphere Application Server를 선택하십시오.

4. **적용**을 누르십시오.
5. 구성 관리자를 닫으십시오.
6. WebSphere Application Server 관리 콘솔에서 인스턴스를 중지한 후 다시 시작하십시오.

URL 재작성을 위한 JSP 템플리트 작성

URL 재작성을 사용하여 세션 상태를 유지보수하려는 경우, 일반 HTML 파일에 웹 응용프로그램의 일부에 대한 링크를 포함하지 마십시오. 이러한 제한은 URL 인코딩이 일반 HTML 파일에서 사용될 수 없기 때문에 필요합니다. URL 재작성을 사용하여 상태를 유지보수하려면 사용자가 세션 중에 요청하는 모든 페이지에는 Java 해석기가 이해할 수 있는 코드가 있어야 합니다. 사용자가 세션 중에 액세스할 수 있는 사이트 일부와 웹 응용프로그램에 일반 HTML 파일이 있는 경우, JSP 파일로 변환하십시오. 이것은 쿠키를 사용하여 세션을 유지보수하는 것과는 달리 URL 재작성을 사용한 세션 유지보수에서는 응용프로그램의 각 JSP 템플리트가 `<A>` 태그의 모든 `HREF` 속성에 대해 URL 인코딩을 사용해야 하기 때문에 응용프로그램 작성자에게 영향을 주게 됩니다. 응용프로그램에 있는 하나 이상의 JSP 템플리트가 `encodeURL(String url)`을 호출하지 않거나 `RedirectURL(String url)` 메소드를 인코드하지 않는 경우에는 세션이 유실됩니다.

링크 작성

URL 재작성을 사용할 때 사용자가 브라우저로 리턴하거나 경로 재지정하는 모든 링크에 세션 ID가 추가되어야 합니다. 예를 들어, 웹 페이지에 있는 다음 링크는

```
<a href="store/catalog">
```

아래와 같이 재작성됩니다.

```
<a href="store/catalog;$jsessionid$DA32242SSGE2">
```

사용자가 이 링크를 누를 때 재작성된 URL 양식이 클라이언트 요청의 일부로 서버에 보내집니다. Servlet 엔진은 `;$jsessionid$DA32242SSGE2`를 세션 ID로 인식하고 이 사용자에 대한 적합한 `HttpSession` 오브젝트를 얻기 위해 저장합니다.

다음 예에서는 Java 코드가 JSP 파일 안에 임베드되는 방법을 보여줍니다.

```
<%
 response.encodeURL ("/store/catalog");
%>
```

브라우저로 리턴할 URL을 재작성하려면 출력 스트림에 URL을 보내기 전에 JSP 템플리트에서 `encodeURL()` 메소드를 호출하십시오. 예를 들어, URL 재작성을 사용하지 않는 JSP 템플리트가 다음을 갖는 경우,

```
out.println("<a href=\"/store/catalog\">catalog</a>")"
```

아래 코드로 바꾸십시오.

```
out.println("<a href=\"");
out.println(response.encodeURL ("/store/catalog"));
out.println("\">catalog</a>");
```

경로 재지정할 URL을 재작성하려면 encodeRedirctURL() 메소드를 호출하십시오. 예를 들어, JSP 템플리트가 다음을 갖는 경우,

```
response.sendRedirect (response.encodeRedirectURL ("http://myhost/store/catalog"));
```

encodeURL() 및 encodeRedirectURL() 메소드는 HttpServletResponse 오브젝트의 일부입니다. 두 경우 모두에서 이들 호출은 URL을 인코딩하기 전에 URL 재작성이 구성되었는지 확인합니다. 구성되지 않은 경우, 원래 URL을 리턴합니다.

양식 작성: 제출을 위한 양식을 작성하려면 양식 템플리트의 ACTION 태그에서 response.encodeURL("Logon");을 호출하십시오. 예를 들면, 다음과 같습니다.

```
String strLoginPost = response.encodeURL("Logon");
<FORM NAME="Logon" METHOD="post" ACTION= <%= strLoginPost %> >
...
</FORM>
```

첫 번째 페이지 작성: 대개 홈페이지인 진입 페이지는 프레임을 포함할 수 없습니다. 상점에서 프레임을 사용하려는 경우, 상점에 대한 링크를 갖는 비프레임 페이지가 상점의 진입 페이지로 작용하도록 할 수 있습니다. 그러나 상점이 프레임을 사용하고 고객이 먼저 진입 페이지를 통하지 않고 프레임을 갖는 페이지에 액세스하려는 경우, 고객의 세션이 유실될 수 있습니다. 고객들은 또한 **이전** 버튼을 사용하여(프레임을 갖는 경우에만) 진입 페이지로 리턴하고 진입 페이지를 최신 정보로 고치는 경우에는 세션을 유실할 수 있습니다. 진입 페이지를 최신 정보로 고치면 고객에게 새 세션 ID가 부여됩니다. **이전** 버튼의 대안으로 진입 페이지로의 역 링크가 이런 유형의 세션 유실을 막기 위해 필요합니다.

제 3 부 시스템 운영자 보안 태스크

이 부분에서는 반드시 WebSphere Commerce 사이트 운영자는 아니더라도 사이트에 있는 시스템 운영자가 일반적으로 수행할 수 있는 보안 태스크에 대해 설명합니다.

제 7 장 암호 설정 및 변경

대부분의 WebSphere Commerce 구성요소는 운영체제에 의해 유효성이 검증된 사용자 ID 및 암호를 이용합니다. 암호 변경에 대한 자세한 내용은 운영체제 문서를 참조하십시오. 이 장에서는 운영체제를 통해 사용자 ID 및 암호의 유효성을 검증하지 않는 WebSphere Commerce 구성요소를 위해 암호를 설정 및 변경하는 방법을 다룹니다.

사용자 ID, 암호 및 웹 주소에 대한 빠른 참조

WebSphere Commerce 환경 관리에는 다양한 사용자 ID가 필요합니다. 이들 사용자 ID가 필수 권한과 함께 아래 목록에 설명되어 있습니다. WebSphere Commerce 사용자 ID인 경우에는 기본 암호가 식별됩니다.

Windows® 사용자 ID

Windows 사용자 ID는 운영자 권한을 갖고 *있어야* 합니다. DB2®를 사용 중인 경우, 사용자 ID와 암호가 다음 규칙을 따라야 합니다.

- 8자를 초과할 수 없습니다.
- A - Z, a - z, 0 - 9, @, #, $ 및 _ 문자만 포함할 수 있습니다.
- 밑줄(_)로 시작할 수 없습니다.
- 사용자 ID는 대문자, 소문자 또는 대소문자 혼합의 USERS, ADMINS, GUESTS, PUBLIC, LOCAL을 사용할 수 없습니다.
- 사용자 ID는 대문자, 소문자 또는 대소문자 혼합의 IBM, SQL, SYS로 시작할 수 없습니다.
- 사용자 ID는 Windows 서비스 이름과 같을 수 없습니다.
- 사용자 ID는 로컬 시스템에서 정의되어야 하며 로컬 운영자 그룹에 속해 있어야 합니다.
- 사용자 ID는 *운영체제의 일부로서 작용*하는 고급 사용자 권한을 갖고 있어야 합니다.

*운영체제의 일부로서 작용*하는 고급 사용자 권한이 없이 설치를 수행할 수 있지만 DB2 설치 프로그램이 사용자가 관리 서버에 대해 지정하는 계정의 유효성을 검증할 수 없습니다. DB2를 설치하는 데 사용되는 모든 사용자 계정에 이 고급 사용자 권한이 있는 것이 바람직합니다.

중요

Windows 사용자 ID가 운영자 권한을 갖지 *않거나* 8자를 초과하거나 로컬 시스템에 정의되지 않는 경우, 해당 문제점이 사용자에게 통지되며 사용자는 설치를 계속할 수 없습니다.

DB2를 사용 중인 경우, 이 사용자 ID를 DB2 데이터베이스 사용자 이름(데이터베이스 사용자 로그온 ID)으로 사용합니다.

위의 기준에 맞는 사용자 ID를 작성해야 하는 경우, Windows 온라인 도움말에서 Windows 사용자 ID 작성에 대한 정보를 찾을 수 있습니다.

400 **iSeries 사용자 프로파일**

두 개의 iSeries 사용자 프로파일이 WebSphere Commerce를 설치 및 구성할 때 자주 사용되고 참조됩니다.

- WebSphere Commerce를 설치하고 구성 관리자에 액세스하기 위해 작성하고 사용하는 사용자 프로파일. WebSphere Commerce를 설치 및 구성하려면 USRCLS(*SECOFR)의 iSeries 사용자 프로파일이나 QSECOFR 사용자 프로파일을 사용해야 합니다. 사용자 프로파일을 작성해야 하는 경우, iSeries용 *WebSphere Commerce 5.4 설치 안내서*를 참조하십시오.
- WebSphere Commerce 인스턴스를 작성할 때 구성 관리자가 작성하는 사용자 프로파일. 이 사용자 프로파일을 "인스턴스 사용자 프로파일"이라고도 합니다. USRCLS(*USER)의 사용자 프로파일이 WebSphere Commerce 인스턴스를 작성할 때마다 구성 관리자에 의해 작성됩니다. 사용자 프로파일을 작성해야 하는 경우, iSeries용 *WebSphere Commerce 5.4 설치 안내서*를 참조하십시오.

구성 관리자 사용자 ID

구성 관리자 도구의 그래픽 인터페이스를 사용하여 WebSphere Commerce 구성 방법을 수정할 수 있습니다. 기본 구성 관리자 사용자 ID 및 암호는 `webadmin`과 `webibm`입니다.

Windows UNIX WebSphere Commerce 시스템이나 WebSphere Commerce와 동일한 네트워크에 있는 모든 시스템에서 구성 관리자에 액세스할 수 있습니다.

400 Microsoft Internet Explorer 5.5를 지원하고 WebSphere Commerce 시스템과 동일한 네트워크에 있는 모든 시스템에서 구성 관리자에 액세스할 수 있습니다.

Windows UNIX IBM HTTP Server 사용자 ID

IBM HTTP Server를 사용 중인 경우, 웹 브라우저를 열고 다음 웹 주소를 입력하여 웹 서버 홈페이지에 액세스할 수 있습니다.

`http://host_name`

웹 서버를 사용자 정의한 경우, 호스트 이름 뒤에 웹 서버의 첫 페이지 이름을 입력할 수도 있습니다.

WebSphere Commerce 인스턴스 운영자

인스턴스 운영자 사용자 ID와 암호가 다음 WebSphere Commerce 도구에 적용됩니다.

- WebSphere Commerce 액셀러레이터. Windows 운영체제를 실행하는 원격 시스템으로부터 WebSphere Commerce 액셀러레이터에 액세스하려면 Internet Explorer 웹 브라우저를 열고 다음 웹 주소를 입력하십시오.

  `https://host_name:8000/accelerator`

- WebSphere Commerce 관리 콘솔. Windows 운영 체제를 실행하는 원격 시스템으로부터 WebSphere Commerce 관리 콘솔에 액세스하려면 Internet Explorer 웹 브라우저를 열고 다음 웹 주소를 입력하십시오.

  `https://host_name:8000/adminconsole`

- 상점 서비스. 웹 브라우저를 열고 다음의 웹 주소를 입력하면 상점 서비스 페이지에 액세스할 수 있습니다.

  `https://host_name:8000/storeservices`

기본 인스턴스 운영자 사용자 ID는 `wcsadmin`이고 기본 암호는 `wcsadmin`입니다.

주: `wcsadmin` 사용자 ID는 절대 제거해서는 안 되며 항상 인스턴스 운영자 권한을 갖고 있어야 합니다.

WebSphere Commerce는 사용자 ID와 암호가 다음 규칙을 따를 것을 요구합니다.

- 암호의 길이가 최소한 8자여야 합니다.
- 암호가 최소한 하나의 숫자를 포함해야 합니다.
- 암호에서 한 문자가 다섯 번 이상 포함되지 않습니다.
- 암호가 동일한 문자를 네 번 이상 연속해서 반복하지 않습니다.

Payment Manager 관리자

Payment Manager 를 설치할 때 WebSphere Commerce 운영자 ID `wcsadmin`에 자동으로 Payment Manager 관리자 역할이 지정됩니다. 아직 수행하지 않은 경우, Payment Manager 범주 클래스를 WCSRealm으로 전환하려면 *WebSphere Commerce 5.4 설치 안내서*의 지시사항을 수행하십시오.

Payment Manager 관리자 역할은 사용자 ID가 Payment Manager 를 제어하고 관리할 수 있도록 합니다.

400

주:

1. Payment Manager 통합과 관련된 WebSphere Commerce 기능이 작동하지 않기 때문에 로그온 사용자 ID `wcsadmin`을 삭제하거나 이름을 바꾸지 마십시오. `wcsadmin`의 사전 지정된 Payment Manager 역할을 변경하지 마십시오.
2. Payment Manager 역할을 WebSphere Commerce 운영자에게 지정하고 나중에 이 운영자의 로그온 사용자 ID를 삭제하거나 이름을 변경할 경우, 사용자 ID를 삭제하거나 이름을 바꾸기 전에 먼저 운영자의 Payment Manager 역할을 제거해야 합니다.

중요

400 Payment Manager 는 두 개의 다른 관리 ID에 Payment Manager 관리자 역할을 사전 지정했습니다.

- `ncadmin`
- `admin`

사용자에게 부주의로 Payment Manager 관리자 역할이 지정되는 것을 방지하려면 다음을 수행하십시오.

1. WebSphere Commerce 관리 콘솔을 사용하여 WebSphere Commerce 에 위의 관리 ID를 작성하십시오.
2. Payment Manager 사용자 인터페이스에서 **사용자**를 선택하십시오.
3. 이들 두 관리 ID에서 Payment Manager 관리자 역할을 제거하십시오.

또한 Payment Manager 인스턴스 암호를 알아야 하는데, 이 암호는 Payment Manager 인스턴스를 시작, 중지 또는 삭제하는 데 필요합니다. 또한 Payment Manager 인스턴스에 카세트를 추가하는 데 필요합니다. Payment Manager 인스턴스가 WebSphere Commerce 구성 관리자에 의해 작성되는 경우, Payment Manager 인스턴스 암호가 WebSphere Commerce 인스턴스 로그온 암호와 동일하며 이를 인스턴스 사용자 프로파일 암호라고도 합니다. Payment Manager 인스턴스가 **CRTPYMMGR** 명령을 사용하여 iSeries 세션으로부터 또는 iSeries 태스크 페이지로부터 작성되는 경우, 암호를 제공하도록 프롬프트됩니다.

구성 관리자 암호 변경

구성 관리자를 실행할 때 사용자 ID와 암호를 입력하는 창에서 **수정**을 눌러 구성 관리자 암호를 변경할 수 있습니다.

다른 방법으로는 구성 관리자 사용자 ID 또는 암호를 변경하여 WebSphere Commerce 설치 경로 아래의 bin 서브디렉토리로 전환한 후 명령창에 다음을 입력하십시오.

```
config_env
java com.ibm.commerce.config.server.PasswordChecker -action [action type]
   -pwfile [password file] -userid [user ID]
   -password [userid password] [-newpassword [new userid password]]
```

여기서 조치 유형은 Add, Check, Delete 또는 Modify입니다. 매개변수가 아래에 설명됩니다.

pwfile

파일이 저장될 파일에 대한 경로. 기본 경로는 WebSphere Commerce 설치 경로 아래의 bin 서브디렉토리입니다. 이 매개변수는 항상 필수입니다.

userid

작성, 확인, 삭제 또는 수정하려는 사용자 ID를 입력하십시오. 이 매개변수는 항상 필수입니다.

password

추가, 확인, 삭제 또는 수정하려는 암호를 입력하십시오. 이 매개변수는 userid 매개변수와 함께 사용해야 합니다. 매개변수는 항상 필수입니다.

newpassword

특정 사용자 ID에 대한 암호를 변경하려면 이 매개변수를 사용하십시오. 매개변수는 userid 및 password 매개변수와 함께 사용해야 합니다. 이 매개변수는 조치 유형 Modify를 지정할 때 필수입니다.

IBM HTTP Server 운영자 암호 설정

IBM HTTP Server 운영자 암호를 설정하려면 다음을 수행하십시오.

1. 시스템의 IBM HTTP Server 설치 디렉토리로 전환하십시오.
2. 다음 명령을 입력하십시오.

   Windows `htpasswd -b conf\admin.passwd user password`

   UNIX `htpasswd -b conf/admin.passwd user password`. 여기서 *user* 및 *password*는 IBM HTTP Server에 대한 관리 권한을 갖기 원하는 사용자 ID와 암호입니다.

이제 IBM HTTP Server 관리 암호가 설정되었습니다.

SSL 키 파일 암호 변경

IBM HTTP Server를 사용 중인 경우, SSL 키 파일 암호를 변경하려면 아래 단계를 따르십시오.

1. Windows **시작 메뉴 → 프로그램 → IBM HTTP Server → 키 관리 유틸리티**를 누르십시오.
2. **키 데이터베이스 파일** 메뉴에서 **열기**를 선택하십시오.
3. 시스템의 IBM HTTP Server 설치 경로에 있는 ssl 서브디렉토리로 전환하십시오. 키 파일(파일 확장자 .kdb)이 이 폴더에 있어야 합니다. 그렇지 않으면 79 페이지의 제 8 장 『IBM HTTP Server를 사용한 프로덕션을 위한 SSL 사용』에 설명된 지시사항에 따라서 새 키 파일을 작성하십시오.
4. **키 데이터베이스 파일** 메뉴에서 **암호 변경**을 선택하십시오. 암호 변경 창이 나타납니다.
5. 새 암호를 입력하고 **파일에 암호 저장**을 사용하십시오.
6. **확인**을 누르십시오. 암호가 변경되었습니다.

이제 SSL 키 파일 관리 암호가 성공적으로 변경되었습니다.

WebSphere Commerce 암호화된 암호 생성

WebSphere Commerce에서는 암호화된 암호를 생성할 수 있습니다. 암호화된 암호를 생성하려면 다음을 수행하십시오.

1. WebSphere Commerce 설치 디렉토리의 bin 서브디렉토리로 이동하십시오.
2. 명령행에서 다음 스크립트를 실행하십시오.

   Windows `wcs_password.bat` *`password SALT merchant_key`*

   UNIX `/wcs_password.sh` *`password SALT merchant_key`*

   여기서

   - *password*는 일반 텍스트 암호입니다.
   - *SALT*는 암호와 함께 사용되는 SALT입니다. 이것은 해당 암호가 갱신될 특정 사용자에 대한 USERREG 데이터베이스 테이블의 SALT 열에 있습니다.
   - *merchant_key*는 인스턴스 작성 중에 입력된 판매자 키입니다.

Payment Manager 암호화된 암호 생성

WebSphere Commerce에서는 Payment Manager를 위한 암호화된 암호를 생성할 수 있습니다. 암호화된 암호를 생성하려면 다음을 수행하십시오.

1. WebSphere Commerce 설치 디렉토리의 bin 서브디렉토리로 이동하십시오.
2. 명령행에서 다음 스크립트를 실행하십시오.

Windows `wcs_pmpassword.bat` *`password SALT`*

UNIX `/wcs_pmpassword.sh` *`password SALT`*

여기서

- *password*는 일반 텍스트 암호입니다.
- *SALT*는 암호와 함께 사용되는 SALT입니다. 이것은 USERREG 데이터베이스 테이블의 SALT 열에 있습니다.

제 8 장 IBM HTTP Server를 사용한 프로덕션을 위한 SSL 사용

IBM HTTP Server를 사용한 WebSphere Commerce 인스턴스를 작성한 후 SSL이 테스트 목적을 위해 사용됩니다. 사이트를 구매자에게 열기 전에 이 장의 단계를 수행하여 프로덕션에 SSL을 사용해야 합니다.

보안 정보

IBM HTTP Server는 암호화 기술을 사용하여 비즈니스 트랜잭션을 위한 보안 환경을 제공합니다. 암호화는 정보를 수령인이 암호화를 해제할 때까지 읽을 수 없도록 인터넷에서 정보 트랜잭션을 암호화하는 것입니다. 보낸 사람은 알고리즘 패턴이나 키를 사용하여 트랜잭션을 암호화하고 수령인은 암호 해독 키를 사용합니다. 이들 키는 SSL(Secure Sockets Layer) 프로토콜에 의해 사용됩니다.

웹 서버는 인증 처리를 사용하여 비즈니스를 수행하려는 사람의 동일성을 검증(즉, 그들이 자신에 대해 주장하는 사람이 맞는지 확인)합니다. 여기에는 인증 기관(CA)이라는 신뢰되는 제삼자가 서명한 인증 확보가 포함됩니다. IBM HTTP Server 사용자의 경우, CA는 Equifax® 또는 VeriSign® Inc.일 수 있습니다. 다른 CA도 사용할 수 있습니다.

프로덕션 키 파일을 작성하려면 다음 단계를 완료하십시오.

1. 프로덕션용 보안 키 파일을 작성하십시오.
2. 인증 기관으로부터 보안 인증을 요청하십시오.
3. 프로덕션 키 파일을 현재 키 파일로 설정하십시오.
4. 인증을 받고 프로덕션 키 파일을 테스트하십시오.

이들 단계가 아래에 자세하게 설명됩니다.

주:

1. 이미 인증 기관이 서명한 프로덕션 키 파일을 사용 중인 경우, 이들 단계를 건너뛸 수 있습니다. 사용 여부를 판별하려면 이 장을 읽으십시오.
2. 이들 단계를 수행하면 브라우저가 보안 메시지를 표시할 수 있습니다. 각 메시지의 정보를 주의깊게 읽고 진행 방법을 결정하십시오.

프로덕션용 보안 키 파일 작성

프로덕션용 보안 키 파일을 작성하려면 웹 서버 시스템에서 다음을 수행하십시오.

1. IBM HTTP Server를 중지하십시오.

2. 시스템의 IBM HTTP Server 설치 서브디렉토리의 conf 서브디렉토리로 디렉토리를 이동하십시오.
3. httpd.conf의 백업 사본을 작성하십시오.
4. 텍스트 편집기에서 httpd.conf를 여십시오.
5. 다음 행에서 포트 443에 대한 주석 처리가 제거되었는지 확인하십시오.
   - Windows

     ```
     #LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
     #Listen 443#Listen 443#<VirtualHost host.some_domain.com:443>
     #SSLEnable
     #</VirtualHost>
     #SSLDisableKeyfile "drive:/WebSphere/HTTPServer/ssl/keyfile.kdb"
     #SSLV2Timeout 100
     #</VirtualHost>
     #SSLDisable
     ```

   - UNIX

     ```
     #LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
     #AddModule mod_ibm_ssl.c
     #Listen 443#<VirtualHost host.some_domain.com:443>
     #SSLEnable
     #</VirtualHost>
     #SSLDisableKeyfile "keyfile"
     #SSLV2Timeout 100
     #</VirtualHost>
     #SSLDisable
     ```

     여기서 *keyfile*은 다음 중 하나입니다.

     AIX `/usr/HTTPServer/ssl/keyfile.kdb`

     Solaris `/opt/IBMHTTPD/ssl/keyfile.kdb`

     Linux `/opt/IBMHTTPServer/ssl/keyfile.kdb`
6. 다음 행에서 포트 8000에 대한 주석 처리가 제거되었는지 확인하십시오.
   a. #Listen 8000
   b. #<VirtualHost host.some_domain.com:8000>. 또한 이 행에 완전한 호스트 이름을 대체해야 합니다.
   c. #SSLEnable
   d. #</VirtualHost>

   주: 방화벽 소프트웨어가 WebSphere Commerce Tools에 구성한 포트(기본적으로 포트 8000)에 대한 외부 액세스를 차단하는 것이 바람직합니다. 작업 방법에 대한 자세한 내용은 사이트에서 사용 중인 방화벽 소프트웨어의 문서를 참조하십시오.
7. 변경사항을 저장하십시오.

8. `httpd.conf` 파일에 구문 오류가 없음을 확인하려면 시스템의 IBM HTTP Server 설치 서브디렉토리의 `bin` 서브디렉토리로 이동하고 다음 명령을 실행하십시오.

   UNIX `./apachectl configtest`

   Windows `apachectl configtest`

9. IBM HTTP Server를 시작하십시오.

인증 기관으로부터 보안 인증 요청

이전 단계에서 방금 작성한 보안 키 파일의 유효성을 검증하려면 Equifax 또는 VeriSign 같은 인증 기관(CA)의 인증이 필요합니다. 인증에는 서버의 공용 키, 서버의 인증과 연관된 인식 이름 및 인증의 일련 번호와 만기 날짜가 들어 있습니다.

다른 CA를 사용하려는 경우, 수행할 프로시저에 대한 정보를 직접 문의하십시오.

Equifax 사용자

Equifax로부터 보안 서버 인증을 요청하려면 다음 웹 주소를 참조하여 제공되는 지시사항을 수행하십시오.

`http://www.equifax.com`

2 - 4 영업일 안에 Equifax로부터 전자 우편을 통해 보안 서버 인증을 받아야 합니다.

VeriSign 사용자

VeriSign으로부터 보안 서버 인증을 요청하려면 다음 URL을 참조하여 제공되는 지시사항을 수행하십시오.

`http://www.verisign.com`

AIX IBM HTTP Server에 대한 프로시저를 사용 중인 경우에도 **인터넷 접속 보안 서버**(ICSS)에 대한 링크를 따르십시오. 제공되는 지시사항을 수행하십시오. 아직 수행하지 않은 경우, 인증을 받을 때 이전 절에 설명된 대로 프로덕션 키 파일을 작성하십시오.

Solaris IBM HTTP Server에 대한 프로시저를 사용 중인 경우에도 **인터넷 접속 보안 서버**(ICSS)에 대한 링크를 따르십시오. 후속 페이지에 프로시저가 OS/2® 및 AIX® 플랫폼에 적용된다고 표시됩니다. 이들 지시사항은 Solaris software에도 적용됩니다.

제공되는 지시사항을 수행하십시오. 요청을 제출한 후에 3 - 5 영업일 안에 인증이 도착해야 합니다. 아직 수행하지 않은 경우, 인증을 받을 때 이전 절에 설명된 대로 프로덕션 키 파일을 작성하십시오.

프로덕션 키 파일을 현재 키 파일로 수신 및 설정

CA로부터 인증이 도착한 후 웹 서버가 프로덕션 키 파일을 사용하도록 해야 합니다. 다음 단계를 수행하십시오.

1. 인증 기관에서 받은 *certificatename*.kdb, *certificatename*.rdb 및 *certificatename*.sth 파일을 시스템의 IBM HTTP Server 설치 경로 아래의 ssl 서브디렉토리에 복사하십시오. 여기서 *certificatename*은 인증 요청과 함께 제공된 인증 이름입니다.
2. 키 관리 유틸리티를 여십시오.
3. *certificatename*.kdb 파일을 열고 프롬프트가 표시될 때 암호를 입력하십시오.
4. **개인 인증서**를 선택하고 **받기**를 누르십시오.
5. **찾아보기**를 누르십시오.
6. 인증 기관에서 받은 파일을 저장한 폴더를 선택하십시오. *certificatename*.txt 파일을 선택한 후 **확인**을 누르십시오.
7. **개인 인증서** 목록 상자에 이제 VeriSign *certificatename* 인증이나 Equifax *certificatename* 인증이 나열됩니다.
8. 키 관리 유틸리티를 종료하십시오.
9. 시스템의 IBM HTTP Server 설치 경로 아래의 conf 서브디렉토리로 디렉토리를 이동하십시오.
10. httpd.conf의 백업 사본을 작성하십시오.
11. 텍스트 편집기에서 httpd.conf를 여십시오.
12. 80 페이지의 5단계에 나열된 행에서 주석 처리가 제거되었는지 확인하십시오.
13. Keyfile "*keyfile path name*" 지시문을 검색하고 위의 단계에서 작성한 파일을 가리키도록 경로 이름을 변경하십시오.
14. IBM HTTP Server를 중지한 후 다시 시작하십시오.

프로덕션 키 파일 테스트

프로덕션 키를 테스트하려면 다음을 수행하십시오.

1. 브라우저를 사용하여 다음 URL로 이동하십시오.

   https://*host_name*

   주:

   a. 웹 서버를 사용자 정의한 경우, 호스트 이름 뒤에 웹 서버의 앞 페이지 이름을 입력해야 할 수 있습니다.

   b. http가 *아닌* https를 입력하십시오.

   키가 올바르게 정의된 경우, 새 인증에 대한 여러 메시지가 표시됩니다.

2. **새 사이트 인증** 패널에서 이 인증을 승인하는 경우, **이 인증을 영원히(만기할 때까지) 승인** 라디오 버튼를 선택하십시오.
3. 웹 브라우저에서 캐시와 프록시(또는 소켓) 서버 설정을 원래 상태로 복원하십시오.

이제 서버에서 SSL이 사용되었습니다.

제 9 장 IBM SecureWay Directory LDAP Server에 대한 SSL 사용

다음은 IBM SecureWay Directory LDAP Server 및 WebSphere Commerce에 대해 SSL 보안을 구성하는 단계입니다.

SecureWay 설치

IBM SecureWay Directory LDAP Server를 설치하려면 다음을 수행하십시오.

1. Secureway 설치 지시사항에 따라서 IBM SecureWay Directory LDAP Server를 설치하십시오. GSKit 구성요소를 설치되었는지 확인하십시오.
2. 설치가 완료된 후 IBM Key Manager(Windows의 *drive*:\Program Files\IBM\GSK4\bin\gsk4ikm.exe)를 호출하십시오.
3. 새 CMS 키 데이터베이스 파일을 작성하십시오. **파일에 암호 저장**이 선택되었는지 확인하십시오(예: ldap_key.kdb).
4. 자체 서명 인증을 작성하십시오.
5. Base64-encode data 데이터 유형으로 인증을 발췌하십시오.
6. 새 SSLight 키 데이터베이스 클래스(예: keyring.class)를 작성하십시오.
7. **서명자 인증서** 섹션에서 5단계에서 작성한 인증 파일을 추가하십시오.
8. 브라우저로 주소 http://hostname/ldap를 여십시오.
9. **보안 → SSL → 설정**을 누르고 다음 변경을 수행하십시오.
   - SSL 상태: SSL 설정 또는 SSL만
   - 인증 방법: 서버 인증
   - 보안 포트: 636
   - 키 데이터베이스 경로 및 파일 이름: drive::/Keys/ldap_key.kdb
   - 키 레이블: *your_label*(인증 레이블)
10. **갱신**을 누르고 SecureWay를 다시 시작하십시오.

WebSphere Commerce

Secureway에 대해 작업하도록 WebSphere Commerce를 설정하려면 다음과 같이 *instance*.xml 파일을 수정해야 합니다.

```
java.naming.security.ssl.keyring = keyring
'keyring' is the name of the SSLight key database class (keyring.class)
This class file should put in the class path in WAS.
```

```
java.naming.security.ssl.authentication = ibm
'ibm' is the password specified when create the SSLight key database class.

java.naming.security.protocol = ssl
LdapPort = 636

<MemberSubSystem name="Member SubSystem"
                     ProfileDataStorage="LDAP"
                     AuthenticationMode="LDAP">
  <Directory LdapAdminDN="cn=root"
                 LdapAuthenticationMode="SIMPLE"
                 LdapTimeOut="0"
                 LdapVersion="3"
                 EntryFileName="drive:/WCS/xml/ldap/ldapentry.xml"
                 LdapPort="636"
                 SingleSignOn="0"
                 LdapAdminPW="EaDPFd9VAf0="
                 LdapHost="yazhuang.torolab.ibm.com"
                 MigrateUsersFromWCSdb="ON"
                 JNDIEnvPropName1="java.naming.security.ssl.keyring"
                 JNDIEnvPropValue1="keyring"
                 JNDIEnvPropName2="java.naming.security.ssl.authentication"
                 JNDIEnvPropValue2="ibm"
                 JNDIEnvPropName3="java.naming.security.protocol"
                 JNDIEnvPropValue3="ssl"
                 display="false"
                 LdapType="SECUREWAY" />
</Membersubsystem>
```

WebSphere Commerce를 다시 시작하십시오.

제 10 장 단일 사인온

이 장에서는 WebSphere Commerce의 단일 사인온 설정 방법을 설명합니다.

전제 조건

단일 사인온을 사용하려면, 다음 요구사항을 만족시켜야 합니다.

- 기존 LDAP 서버를 설치하고 구성해야 합니다. LDAP 서버를 구성하려면 *IBM WebSphere Commerce Version 5.4 추가 소프트웨어 안내서*를 참조하십시오.
- WebSphere Commerce가 설치 및 구성되어야 합니다.
- WebSphere Application Server 보안이 사용되어야 합니다. WebSphere Application Server 보안을 사용하려면 55 페이지의 제 5 장 『WebSphere™ Application Server 보안 사용』을 참조하십시오.

단일 사인온 사용

제한사항

단일 사인온이 WebSphere Commerce에서 사용될 때 몇 가지 핵심 제한사항이 있습니다. 제한사항은 다음과 같습니다.

- LPTA 쿠키는 다른 웹 서버 포트에서 플로우할 수 있습니다.
- `ldapentry.xml` 파일을 수정하고 오브젝트 클래스 `ePerson`을 추가할 필요가 있을 수 있습니다. 이것은 `ldapocs` 요소의 속성입니다.
- `instance.xml`을 수정하고 LDAP 구성요소에서 사용자에 대한 이주가 "on" 상태인지 확인해야 합니다.
- 단일 사인온 구성에 참여하는 시스템은 동기화된 시스템 시계를 가져야 합니다.
- WebSphere Application Server LPTA 토큰을 읽고 발행할 수 있는 응용프로그램 간에만 단일 사인온이 지원됩니다.

단일 사인온을 사용하려면 다음을 수행하십시오.

1. WebSphere Application Server 내에서 단일 사인온을 사용하십시오. 자세한 정보는 다음 사이트에서 사용 가능한 WebSphere Application Server InfoCenter의 "단일 사인온"을 검색하십시오.

   ```
   http://www.ibm.com/software/webservers/appserv/doc/v40/ae
   /infocenter/index.html
   ```

단일 사인온: **WebSphere Application Server**를 선택하고 다음 절을 완료하십시오.

- **WebSphere Application Server에 대한 SSO 구성**.
  - **WebSphere Application Server 보안 설정 수정**.

    주: LDAP 필드를 채우는 방법을 설명하는 단계는 무시할 수 있습니다.
  - **LTPA 키를 파일로 반출**.

2. WebSphere Commerce 시스템에서, WebSphere Commerce 구성 관리자를 시작하십시오.
3. **구성원 서브시스템** 노드를 구성하려면, 다음을 수행하십시오.
   a. **WebSphere Commerce** → *host_name* → **인스턴스 목록** → *instance_name* → **인스턴스 등록 정보** → **구성원 서브시스템**을 펼치십시오.
   b. **인증 모드** 드롭 다운 메뉴에서, **LDAP**를 선택하십시오.
   c. **단일 사인온** 선택란을 사용하십시오.
   d. **호스트** 필드에 LDAP 서버의 완전한 호스트 이름을 입력하십시오.
   e. **운영자 인식 이름** 필드에 운영자의 인식 이름을 입력하십시오. 이것은 LDAP 서버에서 사용된 것과 같은 이름이어야 합니다.
   f. **운영자 암호** 필드에, 운영자 암호를 입력하십시오. 이것은 LDAP 서버에서 사용된 것과 같은 암호이어야 합니다. **암호 확인** 필드에서 암호를 확인하십시오.
   g. 나머지 각 필드를 완료하십시오.
   h. **적용**을 누른 다음, **확인**을 누르십시오.
4. WebSphere Application Server를 다시 시작하십시오.

제 4 부 WebSphere Commerce 개발자 보안 태스크

이 부분에서는 WebSphere Commerce 프로그램과 함께 수행해야 할 보안 태스크에 대해 설명합니다. 일반적으로 WebSphere Commerce 프로그래머가 이들 태스크를 수행합니다.

제 11 장 액세스 제어

액세스 제어 이해

WebSphere Commerce 응용프로그램의 액세스 제어 모델은 사용자, 조치 및 자원의 세 가지 기본 개념을 갖습니다. 사용자는 시스템을 사용하는 사람입니다. 자원은 응용프로그램에서 또는 응용프로그램에 의해 유지보수되는 엔티티입니다. 예를 들어, 자원은 상품, 문서 또는 주문일 수 있습니다. 사람을 표시하는 사용자 프로파일도 자원입니다. 조치는 사용자가 자원에 대해 수행할 수 있는 활동입니다. 액세스 제어는 주어진 사용자가 주어진 자원에 대해 주어진 조치를 수행할 수 있는지를 판별하는 전자상거래 응용프로그램의 구성요소입니다.

WebSphere Commerce 응용프로그램에는 두 가지 기본 레벨의 액세스 제어가 있습니다. 액세스 제어의 첫 번째 레벨은 WebSphere Application Server에 의해 수행됩니다. 이 점에서 WebSphere Commerce는 WebSphere Application Server를 사용하여 엔터프라이즈 bean과 Servlet을 보호합니다. 액세스 제어의 두 번째 레벨은 WebSphere Commerce의객체 단위 액세스 제어 시스템입니다.

WebSphere Commerce 액세스 제어 프레임워크는 액세스 제어 정책을 사용하여 주어진 사용자가 주어진 자원에 대해 주어진 조치를 수행하도록 허용되는지를 판별합니다. 이 액세스 제어 프레임워크는 객체 단위 액세스 제어를 제공합니다. WebSphere Application Server가 제공하는 액세스 제어와 함께 작업하지만 이를 대체하지는 않습니다.

WebSphere Application Server에서의 자원 보호 개요

다음 WebSphere Commerce 자원은 WebSphere Application Server에 의한 액세스 제어로 보호됩니다.

- 엔티티 beans
  이들 bean은 전자상거래 응용프로그램의 오브젝트를 모델링합니다. 이들은 원격 클라이언트가 액세스할 수 있는 분산 오브젝트입니다.
- JSP 템플리트
  WebSphere Commerce는 표시 페이지를 위해 JSP 템플리트를 사용합니다. 각 JSP 템플리트는 엔티티 bean에서 데이터를 검색하는 하나 이상의 데이터 bean을 포함할 수 있습니다. 클라이언트는 URL 요청을 작성하여 JSP 페이지를 요청할 수 있습니다.
- 제어기 및 보기 명령
  클라이언트는 URL 요청을 작성하여 제어기 및 보기 명령을 요청할 수 있습니다. 또

한 VIEWREG 테이블에 등록된 JSP 파일 이름 또는 보기 이름을 사용하여 하나의 표시 페이지에 다른 페이지에 대한 링크가 포함될 수 있습니다.

WebSphere Commerce 서버는 일반적으로 다음 웹 경로를 사용하도록 구성됩니다.

- `/webapp/wcs/stores/servlet/*`
  이것은 요청 Servlet에 대한 요청에 사용됩니다.
- `/webapp/wcs/stores/*.jsp`
  이것은 JSP Servlet에 대한 요청에 사용됩니다.

다음 도표에서는 앞의 웹 경로 구성에 대해 WebSphere Commerce 자원에 액세스하기 위해 요청이 잠재적으로 따를 수 있는 라우트를 보여줍니다.

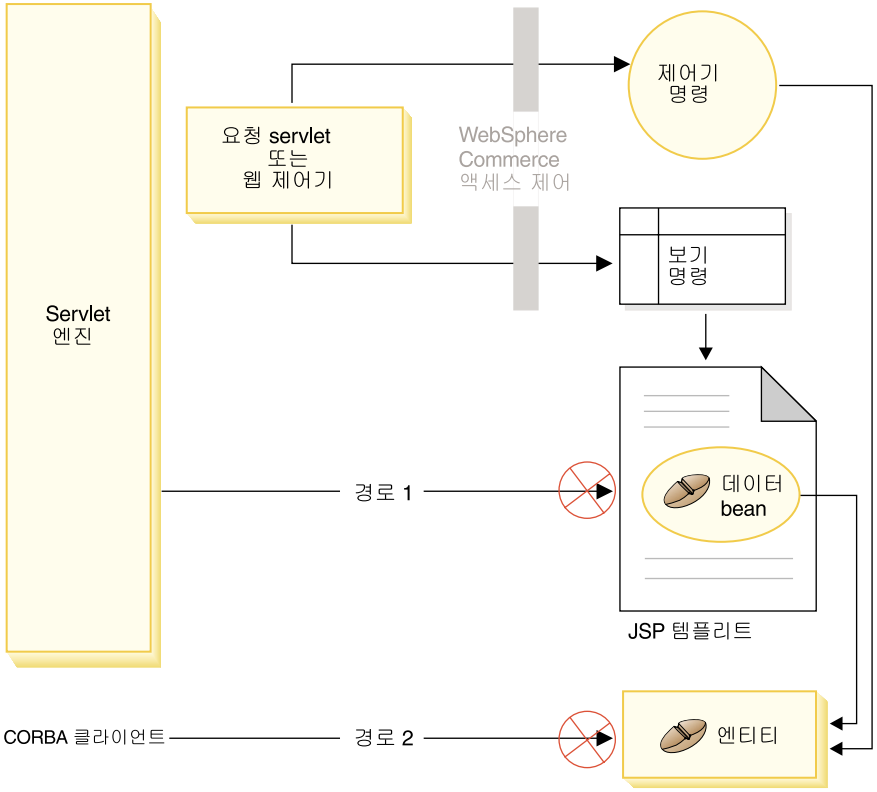

그림 3. WebSphere Commerce 자원에 액세스하기 위한 요청의 라우팅

모든 정규 요청은 요청 Servlet으로 경로 재지정된 후 요청 Servlet이 웹 제어기로 경로 재지정되어야 합니다. 웹 제어기는 제어기 명령과 보기에 대한 액세스 제어를 구현합니다. 그러나 위에 표시된 웹 경로는 나쁜 의도를 가진 사용자가 JSP 템플리트(경로 1) 및 엔티티 bean(경로 2)에 직접 액세스하는 것을 가능하게 합니다. 이러한 나쁜 의도의 공격이 성공하지 못하게 하기 위해 해당 경로는 런타임시 거부되어야 합니다.

JSP 템플리트 및 엔티티 bean에 대한 직접 액세스는 다음 접근 방식 중 하나를 사용하여 막을 수 있습니다.

WebSphere Application Server 보안

WebSphere Application Server는 보안 기능을 제공합니다. 이 접근 방식을 사용할 때 모든 엔터프라이즈 bean 메소드와 JSP 템플리트는 시스템 동일성에 의해서만 호출되도록 구성됩니다. 이들 WebSphere Commerce 자원에 액세스하려면 URL 요청이 웹 제어기로 전달되기 전에 시스템 동일성을 현재 스레드로 설정하는 요청 Servlet으로 라우트되어야 합니다. 그런 다음 웹 제어기가 요청을 대응하는 제어기 명령이나 보기에 전달하기 전에 호출자가 필수 권한을 갖는지 확인합니다. JSP 템플리트 및 엔티티 bean에 직접 액세스하려는(즉, 웹 제어기를 사용하지 않고) 모든 시도는 WebSphere Application Server 보안 구성요소에 의해 거부됩니다.

WebSphere Commerce 자원을 보호하기 위한 WebSphere Application Server 구성에 대한 자세한 내용은 *WebSphere Commerce 설치 안내서*를 참조하십시오. WebSphere Application Server 내에서의 보안에 대한 자세한 내용은 WebSphere Application Server 문서의 시스템 관리 주제를 참조하십시오.

사용자 정의된 엔터프라이즈 bean에 있는 메소드에 대한 WebSphere Application Server 보안 구성에 대한 자세한 내용은 *WebSphere Commerce 5.4 프로그래머 안내서*의 "새 엔터프라이즈 bean을 엔터프라이즈 응용프로그램으로 어셈블링" 및 "수정된 엔터프라이즈 bean을 엔터프라이즈 응용프로그램으로 어셈블링" 절을 참조하십시오.

방화벽 보호

WebSphere Commerce 서버가 방화벽 뒤에서 실행할 때 인터넷 클라이언트는 엔티티 bean에 직접 액세스할 수 없습니다. 이 접근 방식을 사용할 때 JSP 템플리트에 대한 보호는 페이지에 포함되는 데이터 bean에 의해 제공됩니다. 데이터 bean은 데이터 bean 관리자에 의해 활성화됩니다. 데이터 bean 관리자는 JSP 템플리트가 보기 명령에 의해 전달되었는지 여부를 검출합니다. 보기 명령에 의해 전달되지 않은 경우, 예외가 발생하고 JSP 템플리트에 대한 요청이 거부됩니다.

WebSphere Commerce 액세스 제어 정책 소개

WebSphere Commerce 액세스 제어 모델은 액세스 제어 정책의 강제 시행을 기반으로 합니다. 액세스 제어 정책은 액세스 제어 규칙이 비즈니스 로직 코드와 분리될 수 있게 하여 액세스 제어 명령문을 코드로 하드코드해야 하는 필요성을 제거합니다. 예를 들어, 다음과 유사한 코드를 포함시킬 필요가 없습니다.

```
if (user.isAdministrator())
   then {}
```

액세스 제어 정책은 액세스 제어 정책 관리자에 의해 강제 시행됩니다. 일반적으로 사용자가 보호 자원에 액세스하려 시도할 때 액세스 제어 정책 관리자는 먼저 어떤 액세

스 제어 정책이 보호 자원에 대해 적용될 수 있는지를 판별한 후 적용 가능한 액세스 제어 정책을 바탕으로 사용자가 요청한 자원에 액세스하도록 허용되는지 여부를 판별합니다.

액세스 제어 정책은 ACPOLICY 테이블에 저장되는 4-튜플 정책입니다. 각 액세스 제어 정책의 양식은 다음과 같습니다.

```
AccessControlPolicy [AccessGroup, ActionGroup, ResourceGroup, Relationship]
```

4-튜플 액세스 제어 정책의 요소는 사용자가 의심이 가는 자원과 관련되어 관계 또는 관계 그룹에 지정된 조건을 충족시키는 경우에 한하여 특정 액세스 그룹에 속하는 사용자가 지정된 자원 그룹에 속하는 자원에 대해 지정된 조치 그룹의 조치를 수행할 수 있도록 지정합니다. 예를 들어, `[AllUsers, UpdateDoc, doc, creator]`는 사용자가 문서의 작성자인 경우에 모든 사용자가 문서를 갱신할 수 있도록 지정합니다.

액세스 그룹은 MBRGRP 데이터베이스 테이블에 정의되는 특정 유형의 구성원 그룹입니다. 액세스 그룹은 유형 `-2`의 구성원 그룹 유형과 연관되어야 합니다. 값 `-2`는 `AccessGroup` 구성원 그룹 유형을 표시하는데, 이것은 MBRGRPTYPE 테이블에 정의됩니다. 액세스 그룹과 구성원 그룹 유형 사이의 연관이 MBRGRPUSG 테이블에 저장됩니다.

특정 액세스 그룹에 대한 사용자의 멤버쉽은 명시적으로 또는 암시적으로 지정될 수 있습니다. MBRGRPMBR 테이블이 해당 사용자가 특정 구성원 그룹에 속한다고 표시하는 경우에 명시적 스펙이 발생합니다. 암시적 스펙은 사용자가 MBRGRPCOND 테이블에 지정된 조건(예: 상품 관리자의 역할을 수행하는 모든 사용자)을 만족하는 경우에 발생합니다. 또한 결합된 조건(예: 상품 관리자의 역할을 이행하고 최소 6개월 동안 해당 역할에 있었던 모든 사용자) 또는 명시적 제외도 있을 수 있습니다.

사용자를 액세스 그룹에 포함시키는 대부분의 조건은 특정 역할을 이행하는 사용자를 바탕으로 합니다. 예를 들어 상품 관리자 역할을 이행하는 모든 사용자가 카탈로그 관리 조작을 수행할 수 있게 하는 액세스 제어 정책이 있을 수 있습니다. 이 경우, MBRROLE 테이블에서 상품 관리자 역할이 지정된 모든 사용자가 암시적으로 해당 액세스 그룹에 포함됩니다.

구성원 그룹 서브시스템에 대한 자세한 내용은 WebSphere Commerce 온라인 도움말을 참조하십시오.

ActionGroup 요소는 ACACTGRP 테이블에서 옵니다. 조치 그룹은 명시적으로 지정된 조치의 그룹을 의미합니다. 조치 목록이 ACACTION 테이블에 저장되고 해당 조치 그룹에 대한 각 조치의 관계가 ACACTACTGP 테이블에 저장됩니다. 조치 그룹의 한 예로는 ″OrderWriteCommands″ 조치 그룹이 있습니다. 이 조치 그룹은 주문을 갱신하는 데 사용되는 다음 조치를 포함합니다.

- com.ibm.commerce.order.commands.OrderDeleteCmd

- com.ibm.commerce.order.commands.OrderCancelCmd
- com.ibm.commerce.order.commands.OrderProfileUpateCmd
- com.ibm.commerce.order.commands.OrderUnlockCmd
- com.ibm.commerce.order.commands.OrderScheduleCmd
- com.ibm.commerce.order.commands.ScheduledOrderCancelCmd
- com.ibm.commerce.order.commands.ScheduledOrderProcessCmd
- com.ibm.commerce.order.commands.OrderItemAddCmd
- com.ibm.commerce.order.commands.OrderItemDeleteCmd
- com.ibm.commerce.order.commands.OrderItemUpdateCmd
- com.ibm.commerce.order.commands.PayResetPMCmd

자원 그룹은 특정 유형의 자원을 함께 그룹화하는 메커니즘입니다. 자원 그룹에 있는 자원의 멤버쉽은 다음 두 방법 중 하나로 지정할 수 있습니다.

- ACRESGRP 테이블에 조건 열 사용
- ACRESGPRES 테이블 사용

대부분의 경우, 자원을 자원 그룹에 연관시키기 위해 ACRESGPRES 테이블을 사용하는 것으로 충분합니다. 이 방법을 사용할 때 자원은 Java 클래스 이름을 사용하여 ACRESCGRY 테이블에 정의됩니다. 그런 다음 이들 자원이 ACRESGPRES 연관 테이블을 사용하여 적합한 자원 그룹(ACRESGRP 테이블)과 연관됩니다. Java 클래스 이름만으로는 자원 그룹의 구성원을 정의하기에 부족한 경우(예를 들어, 자원의 속성을 바탕으로 이 클래스의 오브젝트를 추가 제한해야 하는 경우), 전적으로 ACRESGRP 테이블의 조건 열을 사용하여 자원 그룹을 정의할 수 있습니다. 속성을 바탕으로 이 자원 그룹화를 수행하려면 자원이 Groupable 인터페이스도 구현해야 함에 유의하십시오.

다음 도표에서는 자원 그룹화 스펙의 예를 보여줍니다. 이 예에서 자원 그룹 10023에는 ACRESGPRES 테이블에 있는 것과 연관된 모든 자원이 포함됩니다. 자원 그룹 10070은 ACRESGRP 테이블의 조건 필드 열을 사용하여 정의됩니다. 이 자원 그룹에는 주문 원격 인터페이스의 인스턴스가 포함되며, 또한 status = "Z"(공유 요청 목록 지정)도 있습니다.

주: ACRESGRP 테이블의 조건 열에 대한 XML 정보의 세부사항이 *WebSphere Commerce 액세스 제어 안내서*에 있습니다.

ACRESGRP

AcResGrp_Id	GrpName	조건
10023	AccountRepresentatives CmdResourceGroup	null
10070	SharedRequisitionList ResourceGroup	<profile> <andListCondition> <simpleCondition> <variable name="Status"/> <operator name="="/> <value data="Z"/> </simpleCondition> <simpleCondition> <variable name="classname"/> <operator name="="/> <value data="com.ibm.commerce.order.objects.Order"/> </simpleCondition> </andListCondition> </profile>

ACRESGRPES

AcResGrp_Id	AcResCgry_Id
10023	10246
10023	10247
10023	10248
10023	10249
10023	10250

ACRESCGRY

AcResCgry_Id	ResClassname
10246	com.ibm.commerce.contract.commands.ContractCreateCmd
10247	com.ibm.commerce.contract.commands.ContractCreateCmd
10248	com.ibm.commerce.contract.commands.ContractCreateCmd
10249	com.ibm.commerce.contract.commands.ContractCreateCmd
10250	com.ibm.commerce.contract.commands.ContractCreateCmd

그림 4. 자원 그룹화 스펙

ACACTGRP, ACRESGRP 및 ACRELGRP 테이블의 MEMBER_ID 열은 값 -2001(루트 조직)을 가져야 합니다.

액세스 제어 정책은 선택적으로 네 번째 요소로서 Relationship 또는 RelationshipGroup 요소를 포함할 수 있습니다.

액세스 제어 정책이 Relationship 요소를 사용하는 경우, 이것은 ACRELATION 테이블에서 옵니다. 한편 RelationshipGroup 요소를 포함하는 경우, ACRELGRP 테이블에서 옵니다. 어느 것도 포함되어서는 안 되지만 하나를 포함시키면 다른 것은 포함시킬 수 없음에 유의하십시오. ACRELGRP 테이블의 RelationshipGroup 스펙이 ACRELATION 테이블의 Relationship 정보에 우선합니다.

ACRELATION 테이블은 사용자와 자원 사이에 존재하는 관계의 유형을 지정합니다. 관계 유형의 몇 가지 예로는 작성자, 제출자 및 소유자가 있습니다. 관계 요소의 사용 예는 주문의 작성자가 항상 주문을 갱신할 수 있음을 보장하기 위해 관계 요소를 사용하는 것입니다.

ACRELGRP 테이블은 특정 자원과 연관될 수 있는 관계 그룹의 유형을 지정합니다. 관계 그룹은 하나 이상의 관계 체인의 그룹화입니다. 관계 체인은 하나 이상의 일련의 관계입니다. 관계 그룹의 예는 사용자가 자원의 작성자여야 하며 또한 자원에서 참조되는 구매 조직 엔티티에 속하도록 지정하는 것입니다.

관계 그룹(또는 관계) 스펙은 액세스 제어 정책의 선택 부분입니다. 사용자 고유의 명령을 작성했으며 이들 명령이 특정 역할에 제한되지 않는 경우에는 공통적으로 사용됩니다. 이 경우, 사용자와 자원 사이에 관계를 강제하기 원할 수 있습니다. 일반적으로 명령이 특정 역할로 제한되는 경우, Relationship 요소를 사용하기보다는 액세스 제어 정책의 AccessGroup 요소를 통해 수행됩니다.

액세스 제어 정책과 관련된 또다른 중요한 개념은 액세스 제어 정책 *소유자*의 개념입니다. 액세스 제어 정책 소유자는 액세스 제어 정책을 소유하는 조직 엔티티입니다. 액세스 제어 정책이 액세스 제어 정책 소유자가 소유하는 자원에만 적용될 수 있기 때문에 액세스 제어 정책의 소유자를 아는 것은 중요합니다.

의심이 가는 각 자원에 대해 액세스 제어 정책 관리자는 권한을 부여하는 정책이 발견될 때까지 또는 모든 정책이 확인되었고 권한을 부여하는 정책이 없을 때까지 소유하는 조직 엔티티나 구성원 계층에서 해당 상위 조직 엔티티에 의해 소유되는 액세스 제어 정책을 적용합니다.

구성원 계층을 표시하는 다음 도표를 고려하십시오.

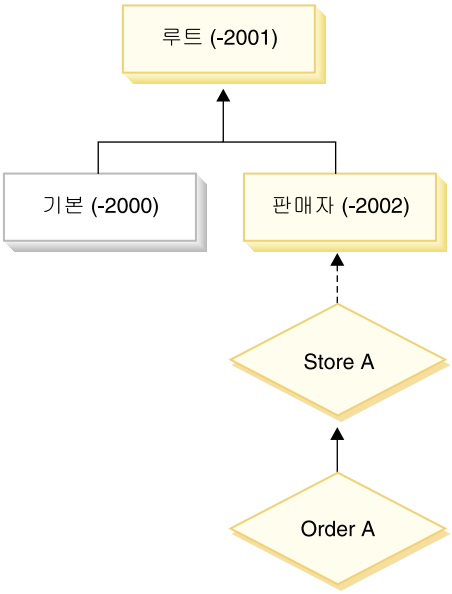

그림 5. 구성원 계층

자원 "OrderA"의 경우, 판매자 또는 루트 조직이 소유하는 모든 액세스 제어 정책이 적용될 수 있습니다. 액세스 제어 정책 관리자가 사용자에게(액세스 제어 정책에 있는 4개 요소를 바탕으로) 허용을 부여하는 하나의 정책을 이들 조직 중 하나가 소유하는 정책 중에서 찾는 경우 즉시 액세스 제어 정책 검색을 중지합니다. 그러나 해당 조직이 소유하고 사용자에게 보호 자원에 대한 조치를 수행할 허용을 부여하는 어떤 액세스 제어 정책도 찾지 못하는 경우 액세스가 거부됩니다.

관계 그룹

관계 그룹을 사용하면 복수 관계를 지정할 수 있습니다. 관계는 사용자와 의심이 가는 자원 사이에 직접적일 수 있거나 사용자를 자원에 간접적으로 관련시키는 관계의 체인일 수 있습니다.

주: 관계 그룹과 관련된 다음 절의 경우 WebSpher Commerce Professional Edition에서 사용 가능한 유일한 조직은 RootOrganization, DefaultOrganization 및 SellerOrganization임을 인식하는 것이 중요합니다. 다른 조직을 참조하는 예는 WebSpher Commerce Business Edition에만 적용됩니다.

관계와 관계 그룹 비교: 액세스 제어 정책은 사용자가 액세스하려는 자원에 대한 특정 관계를 이행하도록 지정하거나 사용자가 관계 그룹에 지정된 조건을 이행하도록 지정할 수 있습니다.

대부분의 경우, 관계 지정이 응용프로그램에 대한 액세스 제어 요구사항을 충족시킵니다. 그러나 정책이 사용자가 사용자와 자원을 소유하는 조직 사이에 직접적이 아닌 관계를 지정해야 하는 경우, 자원 그룹을 사용해야 합니다.

예를 들어 사용자가 해당 조직에 대한 특정 역할을 수행 중이거나 구매 조직의 구성원일 것을 요구하는 구매 조직과 사용자 사이의 연관을 지정해야 하는 경우, 관계 그룹과 관계 체인을 사용해야 합니다.

사용자와 의심이 가는 자원 사이에 직접적인 연관을 강제 시행할 필요가 거의 없는 경우 간단한 관계를 사용할 수 있습니다. 예를 들어 사용자가 자원의 작성자이도록 강제 시행해야 하는 경우일 수 있습니다.

여러 개의 간단한 관계를 결합하는 경우(예: 사용자가 작성자 또는 제출자), 이것이 관계 체인이 되고 관계 그룹을 사용해야 합니다. 간단한 관계의 조합은 WebSpher Commerce Professional Edition 또는 WebSpher Commerce Business Edition을 사용할 때 발생할 수 있습니다.

관계 그룹에 대한 일반 정보: 관계 체인은 하나 이상의 일련의 관계입니다. 관계 체인의 길이는 포함되는 관계의 수에 의해 결정됩니다. 이것은 관계 체인의 XML 표현에 있는 `<parameter name="aName" value="aValue">` 항목의 수를 검사하여 판별할 수 있습니다.

마지막 `<parameter name="Relationship" value="aValue">` 속성만이 자원의 fulfills() 메소드에 의해 처리되어야 합니다. 나머지는 액세스 제어 정책 관리자에 의해 내부적으로 처리됩니다.

관계 체인의 길이가 2 이상인 경우, 첫 번째 `<parameter name="aName" value="aValue">` 항목은 사용자와 조직 엔티티 사이에 있습니다. 마지막 `<parameter name="aName" value="aValue">` 항목은 조직 엔티티와 자원 사이에 있습니다. 체인의 중간 `<parameter name="aName" value="aValue">` 항목은 조직들 사이에 있습니다.

관계 그룹을 정의해야 하는 경우, XML 파일에 관계 그룹 정의를 정의하여 수행해야 합니다. `defaultAccessControlPolicies.xml` 파일을 수정하거나 사용자 고유의 XML 파일을 작성할 수 있습니다. 이러한 XML 기반 정보 작성에 대한 자세한 내용은 *WebSphere Commerce 액세스 제어 안내서*를 참조하십시오.

다음 절에서는 여러 가지 유형의 관계 그룹 예를 보여줍니다.

하나의 관계 체인으로 구성되는 관계 그룹: Business 액세스 제어 정책의 일부로서 사용자가 자원의 BuyingOrganizationalEntity인 조직 엔티티에 속하도록 강제 시행할 필요가 있을 수 있습니다. 이것은 길이가 2인 하나의 관계 체인으로 구성되는 관계 그룹의 작성이 필요합니다. 관계 체인은 두 개의 개별 관계로 구성되기 때문에 길이가 ″2″라고 합니다. 첫 번째 관계는 사용자와 해당 상위 조직 엔티티 사이에 있습니다. 사용자는 해당 관계에서 ″하위″입니다. 두 번째 관계의 경우, 액세스 제어 정책 관리자가 상위 조직 엔티티가 자원과의 BuyingOrganizationalEntity 관계를 이행하는지를 확인합니다. 다시 말하면, 자원의 구매 조직 엔티티인 경우에는 ″true″를 리턴합니다.

다음 XML 조각은 defaultAccessControlPolicies.xml 파일에서 가져온 것이며 이 유형의 관계 그룹을 정의하는 방법을 보여줍니다.

```
<RelationGroup Name="MemberOf->BuyerOrganizationalEntity"
      OwnerID="RootOrganization">
   <RelationCondition><![CDATA[
      <profile>
         <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="HIERARCHY" value="child"/>
            <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
         </openCondition>
      </profile>
   ]]></RelationCondition>
</RelationGroup>
```

Business 또다른 예는 사용자가 의심이 가는 자원의 구매 조직 엔티티인 조직 엔티티에 대한 회계 담당의 역할을 갖도록 강제 시행하는 것일 수 있습니다. 다시, 이것은 길이가 2인 하나의 관계 체인으로 구성되는 관계 그룹을 사용합니다. 체인의 첫 번째 부분은 사용자가 회계 담당 역할을 갖는 모든 조직 엔티티를 찾습니다. 그런 다음 이 조직 엔티티 세트에 대해 액세스 제어 정책 관리자가 이 중 최소한 하나가 자원과의 BuyingOrganizationalEntity 관계를 이행하는지 확인합니다. 다시 말하면, 이 중 하나가 자원의 구매 조직 엔티티인 경우에는 true를 리턴합니다.

다음 XML 조각은 defaultAccessControlPolicies.xml 파일에서 취한 것이며 이 유형의 관계 그룹을 정의하는 방법을 보여줍니다.

```
<RelationGroup Name="AccountRep->BuyerOrganizationalEntity"
      OwnerID="RootOrganization">
   <RelationCondition><![CDATA[
      <profile>
         <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="ROLE" value="Account Representative"/>
            <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
         </openCondition>
      </profile>
   ]]></RelationCondition>
</RelationGroup>
```

복수 관계 체인으로 구성되는 관계 그룹: 복수 관계 체인을 포함하도록 관계 그룹을 구성하는 것이 가능합니다. 이렇게 할 때 사용자가 모든 관계 체인을 만족해야 하는지 (*AND* 시나리오) 아니면 사용자가 관계 체인 중 최소한 하나를 만족해야 하는지(*OR* 시나리오) 여부를 지정해야 합니다.

Business 이 유형의 관계를 설명하기 위해 다음 XML 조각이 사용자가 자원의 작성자여야 하고 또한 자원에 지정된 BuyingOrganizationalEntity에 속하도록 하는 데 사용됩니다. 사용자가 자원의 작성자이도록 지정하는 첫 번째 체인의 길이는 1입니다. 사용자가 자원에 지정된 BuyingOrganizationalEntity에 속하도록 지정하는 두 번째 체인의 길이는 2입니다.

```
<RelationGroup Name="Creator_And_MemberOf->BuyerOrganizationalEntity"
      OwnerID="RootOrganization">
 <RelationCondition><![CDATA[
```

```
  <profile>
   <andListCondition>
    <openCondition name="RELATIONSHIP_CHAIN">
     <parameter name="RELATIONSHIP" value="creator" />
    </openCondition>
    <openCondition name="RELATIONSHIP_CHAIN">
     <parameter name="HIERARCHY" value="child"/>
     <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
    </openCondition>
   </andListCondition>
  </profile>
 ]]></RelationCondition>
</RelationGroup>
```

AND 시나리오 대신 사용자가 두 관계 체인 중 하나를 만족하도록 요구하는 경우, <andListCondition> 태그가 <orListCondition> 태그로 변경되어야 합니다.

Professional Business WebSpher Commerce Professional Edition(WebSpher Commerce Business Edition뿐 아니라)에서 사용할 수 있는 관계 그룹을 설명하기 위해 사용자가 자원의 작성자 또는 제출자이도록 강제 시행하는 데 사용되는 관계 그룹을 고려하십시오. 이것은 다음 XML 조각에 표시됩니다.

```
<RelationGroup Name="Creator_Or_Submitter"
     OwnerID="RootOrganization">
   <RelationCondition><![CDATA [
   <profile>
      <orListCondition>
         <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="RELATIONSHIP"value="creator"/>
         </openCondition>
         <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="RELATIONSHIP"value="submitter"/>
         </openCondition>
      </orListCondition>
   </profile>
   ]]></RelationCondition>
</RelationGroup>
```

액세스 제어의 유형

명령 레벨 액세스 제어와 자원 레벨 액세스 제어의 두 유형의 액세스 제어가 있는데, 둘다 정책 기반입니다.

명령 레벨(“역할 기반”이라고도 함) 액세스 제어는 광범위한 정책 유형을 사용합니다. 특정 역할의 모든 사용자가 특정 유형의 명령을 실행하도록 지정할 수 있습니다. 예를 들어, 회계 담당 역할을 갖는 사용자가 AccountRepresentativesCmdResourceGroup 자원 그룹에서 모든 명령을 실행하도록 지정할 수 있습니다. 또는 아래 도표에 묘사된 대로 모든 상점 운영자가 StoreAdminCmdResourceGrp에 의해 지정되는 모든 자원에 대해 ExecuteCommandActionGroup에 지정된 모든 조치를 수행할 수 있도록 지정하는 정책의 예가 있습니다.

주: MBRGRPCOND 테이블의 조건 열에 대한 XML 정보는 관리 콘솔을 사용하여 액세스 그룹을 설정할 때 생성됩니다. 관리 콘솔을 사용한 액세스 그룹 설정에 대한 자세한 내용은 WebSphere Commerce 온라인 도움말을 참조하십시오.

ACPOLICY

PolicyName	Member_Id	MbrGrp_Id	AcActGrp_id	AcResGrp_Id	AcRelGrp_Id
StoreAdministrators ExecuteStoreAdmin CmdResourceGroup	-2001	-8	10052	10018	null

MBRGRP

MbrGrp_Id	MbrGrpName
-8	StoreAdministrators

MBRGRPCOND

MbrGrp_Id	조건
-8	<profile> <simpleCondition> <variable name="role"/> <operator name="="/> <value data="Store Administrator"/> </simpleCondition> </profile>

ACACTGRP

AcActGrp_Id	GroupName
10052	ExecuteCommandActionGroup

ACRESGRP

AcResGrp_Id	GrpName
10018	StoreAdminCmdResourceGroup

명령 레벨 액세스 제어 정책은 항상 제어기 명령에 대한 조치 그룹으로서 `ExecuteCommandActionGroup`을 갖습니다. 보기의 경우, 자원 그룹은 항상 `ViewCommandResourceGroup`입니다.

모든 제어기 명령은 명령 레벨 액세스 제어에 의해 보호되어야 합니다. 또한 직접 호출할 수 있거나 다른 명령으로부터의 경로 재지정에 의해 실행(보기로 전달하여 실행되는 것과 대조적으로)될 수 있는 모든 보기는 명령 레벨 액세스 제어에 의해 보호되어야 합니다.

명령 레벨 액세스 제어는 명령이 실행될 자원을 고려하지 않습니다. 단지 사용자가 특정 명령을 실행하도록 허용되는지 여부를 판별합니다. 사용자가 명령을 실행하도록 허용되는 경우, 후속 자원 레벨 액세스 제어 정책이 적용되어 사용자가 의심이 가는 자원에 액세스할 수 있는지를 판별할 수 있습니다.

상점 운영자가 관리 태스크를 수행하려 시도할 때를 고려하십시오. 액세스 제어 확인의 첫 번째 레벨은 이 사용자가 특정 상점 관리 명령을 실행하도록 허용되는지 여부를 판별하는 것입니다. 일단 사용자가 사실상 허용되는지 판별한 후(상점 운영자는 storeAdminCmds 그룹의 명령을 실행하도록 허용되기 때문에) 자원 레벨 액세스 제어 정책이 호출될 수 있습니다. 이 정책은 상점 운영자에게 사용자가 상점 운영자인 조직이 소유하는 상점에 대해서만 관리 태스크를 수행하도록 허용된다고 명시할 수 있습니다.

요약하면, 명령 레벨 액세스 제어에서 “자원”은 명령 자체이며 “조치”는 단순히 명령을 실행(다시 말하면, 명령 오브젝트를 구체화하는 것)하는 것입니다. 액세스 제어 확인은 사용자가 명령을 실행하도록 허용되는지를 판별합니다. 대조적으로 자원 레벨 액세스 제어에서 “자원”은 명령이나 bean이 액세스하는 보호 가능한 자원이고 “조치”는 명령 자체입니다.

액세스 제어 상호작용

이 절에서는 WebSphere Commerce 액세스 제어 정책 프레임워크에서 액세스 제어가 작업하는 방법을 보여주는 상호작용 도표를 제공합니다.

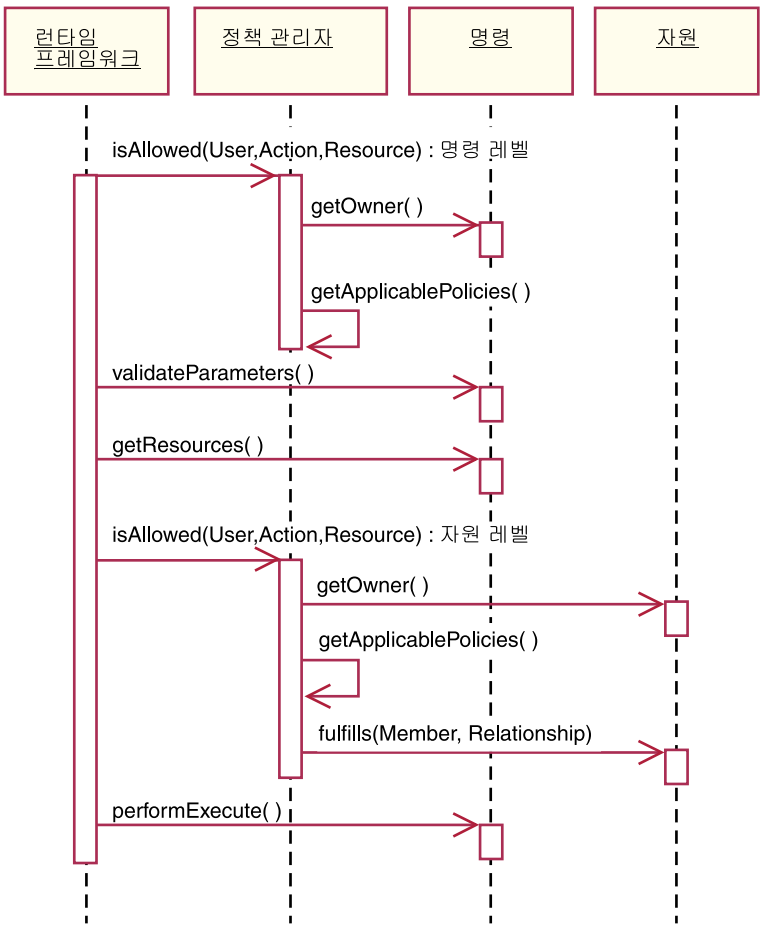

그림 6. 정책 상호작용

앞의 도표에서는 액세스 제어 *정책 관리자*가 수행하는 조치를 보여줍니다. 액세스 제어 정책 관리자는 현재 사용자가 지정된 자원에 대해 지정된 조치를 실행하도록 허용되는지 여부를 판별하는 액세스 제어 구성요소입니다. 액세스 제어 정책 관리자는 자원의 소유자와 해당 상위 조직이 소유하는 정책을 검색하여 이것을 판별합니다. 최소한 하나의 정책이 액세스를 부여하는 경우, 권한이 부여됩니다.

다음 목록에서는 앞의 상호작용 도표에 있는 조치에 대해 설명합니다. 조치는 도표의 맨 위에서 맨 아래쪽으로 정렬됩니다.

1. `isAllowed()`
   런타임 구성요소는 사용자가 제어기 명령이나 보기에 대한 명령 레벨 액세스를 갖는지 여부를 판별합니다.
2. `getOwner()`
   액세스 제어 정책 관리자가 명령 레벨 자원의 소유자를 판별합니다. 기본 구현이 명령 컨텍스트에 있는 상점 소유자(`storeId`)의 구성원 식별자(`memberId`)를 리턴합니다. 명령 컨텍스트에 상점 식별자가 없는 경우, 루트 조직(`-2001`)이 리턴됩니다.

3. getApplicablePolicies()
   액세스 제어 정책 관리자가 지정된 사용자, 조치 및 자원을 바탕으로 적용 가능한 정책을 찾고 처리합니다.
4. validateParameters()
   초기 매개변수 확인 및 해석.
5. getResources()
   자원-조치 쌍의 벡터인 액세스 벡터를 리턴합니다.

   아무것도 리턴되지 않는 경우, 자원 레벨 액세스 제어 확인이 수행되지 않습니다. 보호되어야 하는 자원이 있는 경우, 액세스 벡터(자원-조치 쌍으로 구성됨)가 리턴되어야 합니다.

   각 *자원*은 보호 가능한 오브젝트(com.ibm.commerce.security.Protectable 인터페이스를 구현하는 오브젝트)의 인스턴스입니다. 대부분의 경우, 자원은 액세스 bean입니다.

   액세스 bean이 com.ibm.commerce.security.Protectable 인터페이스를 구현하지 않을 수 있지만, 107 페이지의 『엔터프라이즈 bean에서 액세스 제어 정책 구현』에 포함된 정보에 따라서 해당하는 엔터프라이즈 bean이 보호되는 한 액세스 제어 확인이 계속 발생할 수 있습니다.

   *조치*는 자원에 대해 수행될 조작을 표시하는 문자열입니다. 대부분의 경우, 조치는 명령의 인터페이스 이름입니다.
6. isAllowed()
   런타임 구성요소는 사용자가 getResources()에 의해 지정되는 모든 자원-조치 쌍에 대한 자원 레벨 액세스를 갖는지를 판별합니다.
7. getOwner()
   자원이 소유자의 memberId를 리턴합니다. 이것이 어떤 정책이 적용되는지 판별합니다. 자원 소유자와 해당 상위 조직이 소유하는 정책만이 적용됩니다.
8. getApplicablePolicies()
   액세스 제어 정책 관리자가 적용 가능한 정책을 검색한 후 적용합니다. 사용자에게 자원에 액세스하는 권한을 부여하는 자원-조치 쌍당 최소한 하나의 정책이 발견되는 경우에는 액세스가 부여되고, 그렇지 않으면 거부됩니다.
9. fulfills()
   적용 가능한 정책에 관계 그룹이 지정된 경우, 구성원이 자원에 대해 지정된 관계(들)를 만족하는지 확인하기 위해 자원에 대한 확인이 수행됩니다.
10. performExecute()
    명령의 비즈니스 로직.

Protectable 인터페이스

자원이 WebSphere Commerce 액세스 제어 정책에 의해 보호되기 위한 핵심 요소는, 자원이 com.ibm.commerce.security.Protectable 인터페이스를 구현해야 한다는 점

입니다. 이 인터페이스는 엔터프라이즈 bean 및 데이터 bean과 함께 가장 일반적으로 사용되지만 보호가 필요한 특정 bean만이 인터페이스를 구현해야 합니다.

Protectable 인터페이스를 사용할 때 자원은 `getOwner()`와 `fulfills(Long member, String relationship)`라는 두 개의 핵심 메소드를 제공해야 합니다.

조직 또는 조직 엔티티가 액세스 제어 정책을 소유합니다. `getOwner` 메소드는 보호 가능한 자원 소유자의 memberId를 리턴합니다. 액세스 제어 정책 관리자가 자원의 소유자를 판별한 후 구성원 계층에 있는 소유자에 대한 각 상위의 memberId도 가져옵니다. 그런 다음 원래 getOwner 요청뿐 아니라 소유자의 상위 중 하나에 속하는 모든 액세스 제어 정책의 소유자에 속하는 모든 액세스 제어 정책이 적용됩니다.

지정된 소유자에 적용되는 액세스 제어 정책과 멤버쉽 계층에서 소유자의 상위 레벨 상위 중 하나에 적용되는 액세스 제어 정책이 적용됩니다.

`fulfills` 메소드는 주어진 구성원이 자원에 대해 필수 관계를 만족하는 경우에만 true를 리턴합니다. 일반적으로 구성원은 단일 사용자이지만 조직일 수도 있습니다. 액세스 제어 정책에서 관계 그룹을 사용 중인 경우에는 조직입니다.

Groupable 인터페이스

액세스 제어 정책의 응용프로그램은 자원 그룹에 고유합니다. 자원 그룹화는 클래스 이름, 주문의 상태 또는 storeId 값 같은 속성을 바탕으로 수행될 수 있습니다.

자원이 액세스 제어 정책을 적용할 목적으로 해당 클래스 이름이 아닌 속성에 의해 그룹화될 경우, `com.ibm.commerce.grouping.Groupable` 인터페이스를 구현해야 합니다.

다음 코드 단편은 Groupable 인터페이스를 표시합니다.

```
Groupable interface {
Object getGroupingAttributeValue (String attributeName, GroupContext context)
}
```

예를 들어, 보류 중 상태(`status = P(Pending)`)에 있는 주문에만 적용되는 정책을 구현하기 위해 주문 엔티티 bean의 원격 인터페이스가 Groupable 인터페이스를 구현하고 attributeName의 값이 `"status"`로 설정됩니다.

Groupable 인터페이스의 사용은 보기 드뭅니다.

액세스 제어에 대한 추가 정보 찾기

WebSphere Commerce 액세스 제어 모델에 대한 자세한 내용은 *WebSphere Commerce 액세스 제어 안내서*를 참조하십시오. 이 안내서에서는 액세스 제어의 상세한 개요를 제공하며, 관리 콘솔을 사용하여 정책, 조치 그룹 및 자원 그룹을 작성 또는 수정하는 방법에 대해 설명합니다.

액세스 제어 정책 구현

이 절에서는 사용자 정의된 코드에서 액세스 제어 정책을 구현하는 방법에 대해 설명합니다.

보호 가능한 자원 식별

일반적으로 엔터프라이즈 bean과 데이터 bean이 사용자가 보호하려는 자원입니다. 그러나 모든 엔터프라이즈 bean과 데이터 bean이 보호되지는 않습니다. 기존 WebSphere Commerce 응용프로그램 내에서 보호가 필요한 자원은 이미 Protectable 인터페이스를 구현합니다. 새 엔터프라이즈 bean과 데이터 bean을 작성할 때 보호해야 하는 것에 대한 질문이 떠오릅니다. 보호할 자원을 결정하는 것은 응용프로그램에 따라 다릅니다.

명령이 `getResources` 메소드에서 엔터프라이즈 bean을 리턴하는 경우, 엔터프라이즈 bean은 액세스 제어 정책 관리자가 엔터프라이즈 bean에서 getOwner 메소드를 호출하기 때문에 보호되어야 합니다. 해당하는 자원 레벨 액세스 제어 정책에 관계가 지정되는 경우, `fulfills` 메소드도 호출됩니다.

사용자 고유의 모든 엔터프라이즈 bean과 데이터 bean에 대해 Protectable 인터페이스를 구현(및 따라서 자원을 보호하에 둠)하려는 경우, 응용프로그램에는 많은 정책이 필요할 수 있습니다. 정책의 수가 증가하면 성능이 저하될 수 있고 정책 관리가 더 힘들게 됩니다.

기본 자원과 종속 자원 사이에 이론적 구별이 이루어집니다. *기본 자원*은 스스로 존재할 수 있습니다. *종속 자원*은 관련 기본 자원이 존재할 때만 존재합니다. 예를 들어, 상자 밖에 있는 WebSphere Commerce 응용프로그램 코드에서 Order 엔티티 bean은 보호 가능한 자원이지만 OrderItem 엔티티는 아닙니다. 이유는 OrderItem의 존재가 Order에 종속되기 때문입니다. 즉, Order는 기본 자원이고 OrderItem은 종속 자원입니다. 사용자가 Order에 액세스해야 하는 경우, 주문에 있는 항목에도 액세스해야 합니다.

마찬가지로, User 엔티티 bean은 보호 가능한 자원이지만 Address 엔티티 bean은 아닙니다. 이 경우, 주소의 존재는 사용자에 종속되므로 사용자에 액세스하는 모든 것이 주소에도 액세스해야 합니다.

기본 자원은 보호되어야 하지만 종속 자원은 종종 보호가 필요하지 않습니다. 사용자가 기본 자원에 액세스하도록 허용되는 경우, 기본적으로 해당 종속 자원에도 액세스하도록 허용되어야 함을 의미합니다.

엔터프라이즈 bean에서 액세스 제어 정책 구현

액세스 제어 정책에 의한 보호가 필요한 새 엔터프라이즈 bean을 작성하는 경우, 다음을 수행해야 합니다.

1. 새 엔터프라이즈 bean을 작성하여 `com.ibm.commerce.base.objects.ECEntityBean`에서 확장하십시오.

2. bean의 원격 인터페이스가 com.ibm.commerce.security.Protectable 인터페이스를 확장하는지 확인하십시오.
3. bean이 상호작용하는 자원이 자원의 Java 클래스 이름이 아닌 속성에 의해 그룹화되는 경우, bean의 원격 인터페이스도 com.ibm.commerce.grouping.Groupable 인터페이스를 확장해야 합니다.
4. 엔터프라이즈 bean 클래스에는 다음 메소드에 대한 기본 구현이 들어 있습니다.
   - getOwner
   - fulfills
   - getGroupingAttributeValue

   필요한 모든 메소드를 대체하십시오. 최소한 getOwner 메소드를 대체해야 합니다. 이들 메소드의 기본 구현이 다음 코드 단편에 표시됩니다.

```
*****************************************************************************
public Long getOwner() throws Exception, java.rmi.RemoteException
{
   return null;
}
*****************************************************************************
*****************************************************************************
public boolean fulfills(Long member, String relationship)
   throws Exception, java.rmi.RemoteException
{
      return false;
}
*****************************************************************************
*****************************************************************************
public Object getGroupingAttributeValue(String attributeName,
   GroupingContext context) throws Exception, java.rmi.RemoteException
{
      return null;
}
*****************************************************************************
```

   다음은 OrderBean bean을 바탕으로 하는 이들 메소드의 간단한 구현입니다.

```
*****************************************************************************
public Long getOwner() throws Exception, java.rmi.RemoteException
{
   com.ibm.commerce.common.objects.StoreEntityAccessBean storeEntAB = new
   com.ibm.commerce.common.objects.StoreEntityAccessBean();
   storeEntAB.setInitKey_storeEntityId(getStoreEntityId().toString());
   return storeEntAB.getMemberIdInEJBType();
}
*****************************************************************************
*****************************************************************************
public boolean fulfills(Long member, String relationship)
   throws Exception, java.rmi.RemoteException
   {
      if (relationship.equalsIgnoreCase("creator"))
      {
         return member.equals(getMemberId());
      }
      else if (relationship.equalsIgnoreCase (
```

```
            com.ibm.commerce.base.helpers.EJBConstants.
            SAME_ORGANIZATIONAL_ENTITY_AS_CREATOR_RELATION)) {
               com.ibm.commerce.user.objects.UserAccessBean creator = new
                  com.ibm.commerce.user.objects.UserAccessBean();
               creator.setInitKey_MemberId(getMemberId().toString());
               com.ibm.commerce.user.objects.UserAccessBean ab = new
                  com.ibm.commerce.user.objects.UserAccessBean();
               ab.setInitKey_MemberId(member.toString());
               if (ab.getParentMemberId().equals(creator.getParentMemberId()))
                  return true;
             }
         return false;
   }
   ********************************************************************************
   ********************************************************************************
   public Object getGroupingAttributeValue(String attributeName,
      GroupingContext context) throws Exception
      {
         if (attributeName.equalsIgnoreCase("Status"))
            return getStatus();
      return null;
      }
   ********************************************************************************
```

5. 엔터프라이즈 bean의 액세스 bean과 생성된 코드를 작성(또는 재작성)하십시오.

데이터 bean에서 액세스 제어 정책 구현

데이터 bean이 보호되어야 하는 경우, 액세스 제어 정책에 의해 직접 또는 간접적으로 보호될 수 있습니다. 데이터 bean이 직접 보호되는 경우, 해당 특정 데이터 bean에 적용되는 액세스 제어 정책이 존재합니다. 데이터 bean이 간접적으로 보호되는 경우, 액세스 제어 정책이 존재하는 다른 데이터 bean에 보호를 위임합니다.

액세스 제어 정책에 의해 직접 보호되어야 하는 새 데이터 bean을 작성하는 경우, 데이터 bean이 다음을 수행해야 합니다.

1. `com.ibm.commerce.security.Protectable` 인터페이스를 구현하십시오. bean은 `getOwner()` 및 `fulfills(Long member, String relationship)` 메소드의 구현을 제공해야 합니다. 이들은 bean의 원격 인터페이스에 구현되어야 합니다.

   데이터 bean이 Protectable 인터페이스를 구현할 때 데이터 bean 관리자는 `isAllowed` 메소드를 호출하여 현재 액세스 제어 정책에 따라서 사용자에게 적당한 액세스 제어 특권이 있는지 판별합니다. `isAllowed` 메소드가 다음 코드 단편에 의해 설명됩니다.

   ```
   IsAllowed(Context, "Display", protectable_databean);
   ```

2. bean이 상호작용하는 자원이 자원의 Java 클래스 이름이 아닌 속성에 의해 그룹화되는 경우, bean은 `com.ibm.commerce.grouping.Groupable` 인터페이스를 구현해야 합니다.

3. `com.ibm.commerce.security.Delegator` 인터페이스를 구현하십시오. 이 인터페이스는 다음 코드 단편에 의해 설명됩니다.

```
Interface Delegator {
Protectable getDelegate();
}
```

주: 직접적으로 보호되기 위해서는 getDelegate 메소드가 데이터 bean 자체를 리턴해야 합니다(즉, 데이터 bean이 액세스 제어를 목적으로 그 자신을 위임합니다).

직접 보호되어야 하는 데이터 bean과 간접적으로 보호되어야 하는 데이터 bean 사이의 구별은 기본 자원과 종속 자원 사이의 구별과 유사합니다. 데이터 bean 오브젝트가 그 자신에 존재할 수 있는 경우, 직접 보호되어야 합니다. 데이터 bean의 존재가 다른 데이터 bean의 존재에 종속되는 경우, 다른 데이터 bean에 보호를 위임해야 합니다.

직접 보호되는 데이터 bean의 예로는 Order 데이터 bean가 있습니다. 간접적으로 보호되는 데이터 bean의 예는 OrderItem 데이터 bean입니다.

액세스 제어 정책에 의해 직접 보호되어야 하는 새 데이터 bean을 작성하는 경우, 데이터 bean이 다음을 수행해야 합니다.

1. com.ibm.commerce.security.Delegator 인터페이스를 구현하십시오. 이 인터페이스는 다음 코드 단편에 의해 설명됩니다.

   ```
   Interface Delegator {
   Protectable getDelegate();
   }
   ```

   주: getDelegate에 의해 리턴되는 데이터 bean이 Protectable 인터페이스를 구현해야 합니다.

데이터 bean이 Delegator 인터페이스를 구현하지 않는 경우, 액세스 제어 정책의 보호 없이 대량 자료 반입됩니다.

제어기 명령에서 액세스 제어 정책 구현

새 제어기 명령을 작성할 때 새 명령은 com.ibm.commerce.commands.ControllerCommandImpl 클래스를 확장하고 com.ibm.commerce.command.ControllerCommand 인터페이스를 구현해야 합니다.

명령이 보호되어야 하는 자원에 액세스하는 경우, 자원을 보유할 AccessVector 유형의 개인용 인스턴스 변수를 작성하십시오. 그런 다음 이 메소드의 기본 구현이 널(Null) 값을 리턴하는 것이어서 자원 확인이 발생하지 않으므로 getResources 메소드를 대체하십시오.

새 getResources 메소드에서 명령이 작용될 수 있는 자원 또는 자원-조치 쌍의 배열을 리턴해야 합니다. 조치가 명시적으로 지정되지 않으면 조치는 실행될 명령의 인터페이스 이름으로 기본 설정됩니다.

또한 메소드가 자원을 구체화해야 하는지 또는 자원에 대한 참조를 보유하는 기존 인스턴스 변수를 사용할 수 있는지를 판별하는 것이 바람직합니다. 자원 오브젝트가 이미 존재하는지 확인하는 것이 시스템 성능을 향상시키는 데 도움이 될 수 있습니다. 그런 다음 필요한 경우 새 제어기 명령의 performExecute 메소드에 동일한 getResources 메소드를 사용할 수 있습니다.

다음은 getResources 메소드의 한 예입니다.

```
private AccessVector resources = null;

public AccessVector getResources() throws ECException {

   if (resources == null) {
      OrderAccessBean orderAB = new OrderAccessBean();
      orderAB.setInitKey_orderId(getOrderId().toString());
      resouces = new AccessVector(orderAB);
      }
   return resources;
}
```

예를 들어 OrderItemUpdate 명령을 고려하십시오. 이 명령의 getResources 메소드는 Order 및 User 보호 가능한 오브젝트를 리턴합니다. 조치가 지정되지 않으므로 OrderItemUpdate 명령에 대한 인터페이스로 기본 설정됩니다.

getResources 메소드에 의해 복수 자원이 리턴될 수 있습니다. 이것이 발생할 때 조치가 수행되어야 하는 경우 사용자에게 지정된 모든 자원에 대한 액세스를 제공하는 정책이 발견되어야 합니다. 사용자가 세 자원 중 두 개에 대해 액세스하는 경우, 조치가 계속되지 않을 수 있습니다(세 개 중 세 개가 필요합니다).

추가 매개변수 확인 또는 제어기 명령에 있는 매개변수의 해석을 수행해야 하는 경우, validateParameters() 메소드를 사용할 수 있습니다. 이것은 선택적입니다

추가 자원 레벨 확인

제어기 명령의 getResources 메소드가 호출될 때 보호되어야 하는 모든 자원을 판별하는 것이 항상 가능하지는 않습니다.

필요한 경우, 태스크 명령이 getResources 메소드를 구현하여 명령이 작용할 수 있는 자원 목록을 리턴할 수 있습니다.

자원 레벨 확인을 호출하는 또다른 방법은 checkIsAllowed(Object resource, String action) 메소드를 사용하여 액세스 제어 정책 관리자를 직접 호출하는 것입니다. 이 방법은 com.ibm.commerce.command.ECTargetableCommandImpl 클래스로부터 확장하는 모든 클래스에 사용 가능합니다. 예를 들어 다음 클래스는 ECTargetableCommandImpl 클래스로부터 확장합니다.

- com.ibm.commerce.command.ControllerCommandImpl
- com.ibm.commerce.command.DataBeanCommandImpl

checkIsAllowed 메소드도 com.ibm.commerce.command.ECCommandImpl 클래스를 확장하는 클래스에 사용 가능합니다. 예를 들어, 다음 클래스가 ECCommandImpl 클래스로부터 확장합니다.

- com.ibm.commerce.command.TaskCommandImpl

"create" 명령에 대한 액세스 제어

getResources 메소드가 명령에서 performExecute 메소드 전에 호출되므로 아직 작성되지 않은 자원에 대한 액세스 제어에 대해 다른 접근 방식을 취해야 합니다. 예를 들어 WidgetAddCmd가 있는 경우, getResources 메소드가 작성될 자원을 리턴할 수 없습니다. 이 경우, getResources 메소드가 자원의 작성자를 리턴해야 합니다. 예를 들어, 명령이 명령 팩토리에 의해 작성, 주문이 상점 안에서 작성, 사용자가 조직 안에서 작성됩니다.

명령 레벨 액세스 제어에 대한 기본 구현

명령 레벨 액세스 제어의 경우, getOwner() 메소드의 기본 구현은 storeId가 지정되면 상점 소유자의 memberId를 리턴합니다. storeId가 지정되지 않으면 루트 조직의 memberId가 리턴됩니다(memberId = -2001).

getResources() 메소드의 기본 구현은 null을 리턴합니다.

validateParameters()의 기본 구현은 아무것도 수행하지 않습니다.

보기에서 액세스 제어 정책 구현

보기에 대한 자원 레벨 액세스 제어는 데이터 bean 관리자에 의해 수행됩니다. 데이터 bean 관리자는 다음 경우에 호출됩니다.

1. JSP 템플리트가 <useBean> 태그를 포함하고 데이터 bean이 속성 목록에 없을 때.
2. JSP 템플리트가 다음 활성화 메소드를 포함할 때.

   ```
   DataBeanManager.activate(xyzDatabean, request);
   ```

주: 보호되어야 하는(직접 또는 간접적으로) 모든 데이터 bean은 Delegator 인터페이스를 구현해야 합니다. 직접 보호되어야 하는 데이터 bean은 그 자신에게 위임하며, 따라서 Protectable 인터페이스도 구현해야 합니다. 간접적으로 보호되는 데이터 bean은 Protectable 인터페이스를 구현하는 데이터 bean에 위임해야 합니다.

권장되지는 않지만, 액세스 제어 확인의 생략이 다음 경우에 발생합니다.

1. JSP 템플리트가 데이터 bean을 사용하는 것이 아니라 액세스 bean을 직접 호출하는 경우.
2. JSP 템플리트가 데이터 bean의 populate() 메소드를 직접 호출하는 경우.

제어기 명령의 결과가 보기로 전달될 경우(ForwardViewCommand를 사용하여), 명령 레벨 액세스 제어가 보기에 대해 수행되지 않습니다. 또한 제어기 명령이 응답 특성의

속성 목록에 대량 자료 반입된 데이터 bean(보기에서 사용됨)을 넣은 후 보기로 전달하는 경우, JSP 템플리트가 데이터 bean 관리자를 통하지 않고 데이터에 액세스할 수 있습니다. <useBean> 태그가 JSP 템플리트에 사용되어야 합니다. 사용자에게 이미 제어기 명령을 통해 액세스가 부여된 자원(데이터 bean)에 대한 모든 중복 자원 레벨 액세스 제어 확인을 생략할 수 있으므로 이 방법은 JSP 템플리트를 더 효율적으로 만드는 방법일 수 있습니다.

제 5 부 부록

주의사항

이 정보는 미국에서 제공되는 제품 및 서비스용으로 작성된 것입니다.

IBM은 다른 국가에서 이 책에 기술된 제품, 서비스 또는 기능을 제공하지 않을 수도 있습니다. 현재 사용할 수 있는 제품 및 서비스에 대한 정보는 한국 IBM 담당자에게 문의하십시오. 이 책에서 IBM 제품, 프로그램 또는 서비스를 언급했다고 해서 해당 IBM 제품, 프로그램 또는 서비스만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 대신 사용할 수도 있습니다. 그러나 비IBM 제품, 프로그램 또는 서비스의 운영에 대한 평가 및 검증은 사용자의 책임입니다.

이 책에서 IBM 사용권 프로그램을 언급했다고 해서 해당 IBM 사용권 프로그램만을 사용할 수 있다는 것을 의미하지는 않습니다. IBM의 지적 재산권을 침해하지 않는 한, 기능상으로 동등한 제품, 프로그램 또는 서비스를 IBM 제품, 프로그램 또는 서비스 대신 사용할 수도 있습니다. IBM이 명시적으로 지정한 경우를 제외하고 다른 제품과 결합된 운영에 대한 평가 및 검증은 사용자의 책임입니다.

IBM은 이 책에서 다루고 있는 특정 내용에 대해 특허를 보유하고 있거나 현재 특허 출원 중일 수 있습니다. 이 책을 제공한다고 해서 특허에 대한 사용권까지 부여하는 것은 아닙니다. 사용권에 대한 의문사항은 다음으로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터
전화번호: 080-023-8080

2바이트(DBCS) 정보에 관한 사용권 문의는 한국 IBM 고객만족센터에 문의하거나 다음 주소로 서면 문의하시기 바랍니다.

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

다음 단락은 현지법과 상충하는 영국이나 기타 국가에서는 적용되지 않습니다.

IBM은 타인의 권리 비침해, 상품성 및 특정 목적에의 적합성에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 어떠한 종류의 보증없이 이 책을

현상태대로 제공합니다. 일부 국가에서는 특정 거래에서 명시적 또는 묵시적 보증의 면책사항을 허용하지 않으므로, 이 사항이 적용되지 않을 수도 있습니다.

이 정보에는 기술적으로 부정확한 내용이나 인쇄상의 오류가 있을 수 있습니다. 이 정보는 주기적으로 변경되며, 이 변경사항은 최신판에 통합됩니다. IBM은 이 책에서 설명한 제품 및/또는 프로그램을 사전 통고없이 언제든지 개선 및/또는 변경할 수 있습니다.

이 정보에서 비IBM의 웹 사이트는 단지 편의상 제공된 것으로, 어떤 방식으로든 이들 웹 사이트를 옹호하고자 하는 것은 아닙니다. 해당 웹 사이트의 자료는 본 IBM 제품 자료의 일부가 아니므로 해당 웹 사이트 사용으로 인한 위험은 사용자 본인이 감수해야 합니다.

IBM은 귀하의 권리를 침해하지 않는 범위 내에서 적절하다고 생각하는 방식으로 귀하가 제공한 정보를 사용하거나 배포할 수 있습니다.

(i)독립적으로 작성된 프로그램 및 기타 프로그램(이 프로그램 포함) 간의 정보 교환 및 (ii)교환된 정보의 상호 이용을 목적으로 정보를 원하는 프로그램 사용권자는 다음 주소로 문의하십시오.

135-270
서울특별시 강남구 도곡동 467-12, 군인공제회관빌딩
한국 아이.비.엠 주식회사
고객만족센터

이러한 정보는 해당 조항 및 조건에 따라(예를 들면, 사용권 지불 포함) 사용할 수 있습니다.

이 정보에 기술된 사용권 프로그램 및 사용 가능한 모든 사용권 자료는 IBM이 IBM 기본 계약, IBM 프로그램 사용권 계약(IPLA) 또는 이와 동등한 계약에 따라 제공한 것입니다.

이 책에 있는 모든 성능 데이터는 제한된 환경에서 산출된 것입니다. 그러므로 다른 운영 환경에서의 결과와는 상당히 다를 수도 있습니다. 일부 측정은 개발 단계의 시스템에 대해 수행되었을 수 있으며 이러한 측정이 일반적으로 사용 가능한 시스템에서 동일하다고 보장할 수 없습니다. 또한 일부 측정치는 보외법을 통해 이루어졌으므로 실제 결과는 다를 수 있습니다. 이 책의 사용자는 본인의 고유 환경에 적용할 수 있는 데이터를 확인해야 합니다.

비IBM 제품에 관한 정보는 해당 제품의 공급업체, 공개 자료 또는 기타 범용 소스로부터 얻은 것입니다. IBM에서는 이러한 제품들을 테스트하지 않았으므로, 비IBM 제품과 관련된 성능의 정확성, 호환성 또는 배상 청구에 대해서는 확신할 수 없습니다. 비IBM 제품의 성능에 대한 의문사항은 해당 제품의 공급업체에 문의하십시오.

IBM의 향후 방향이나 의도에 관한 모든 내용은 사전 통지 없이 변경되거나 취소될 수 있으며 목적과 목표만을 표현합니다.

이 정보는 계획 목적만을 위한 것입니다. 여기에 있는 정보는 설명된 제품이 사용 가능하게 되기 전에 변경될 수 있습니다.

이 정보에는 일상적인 비즈니스 작업에서 사용되는 데이터와 보고서의 예가 들어 있습니다. 가능한 완벽하게 설명하기 위해 예에는 개인, 회사, 브랜드 및 제품의 이름이 포함되어 있습니다. 이러한 모든 이름은 가상의 것이며 실제 비즈니스 기업에 의해 사용되는 이름 및 주소에 대한 유사성은 전적으로 우연한 것입니다.

이 제품에서 제공되는 신용 카드 이미지, 상표 및 거래 이름은 신용 카드 표시의 소유자가 해당 신용 카드를 통해 지불을 승인하도록 권한을 부여한 판매자만이 사용해야 합니다.

상표

다음 용어는 미국 또는 기타 국가에서 사용되는 IBM Corporation의 상표 또는 등록상표입니다.

AIX	IBM	Net.Data
SecureWay	WebSphere	

Solaris, Solaris Operating Environment, Java, JavaBeans 및 또는 Java 기반 상표와 로고는 Sun Microsystems, Inc의 상표 및 등록상표입니다.

VeriSign 및 VeriSign 로고는 VeriSign, Inc.의 상표 및 서비스표 또는 등록상표 및 서비스표입니다.

UNIX는 미국 또는 기타 국가에서 사용되는 The Open Group의 등록상표입니다.

Windows, Windows NT 또는 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표 또는 등록상표입니다.

기타 회사, 제품 또는 서비스 이름은 다른 회사의 상표 또는 서비스표일 수 있습니다.

IBM 한글 지원에 관한 설문

FAX : (02) 3787-0123

보내 주시는 의견은 더 나은 고객 지원 체제를 위한 귀중한 자료가 됩니다.
독자 여러분의 좋은 의견을 기다립니다.

책 제목: IBM WebSphere Commerce
보안 안내서
버전 5.4

성 명		직위/담당업무	
회 사 명		부 서 명	
주 소			
전화번호		팩스번호	
전자우편 주소			
사용중인 시스템	o 중대형 서버 o UNIX 서버 o PC 및 PC 서버		

1. IBM에서 제공하는 한글 책자와 영문 책자 중 어느 것을 더 좋아하십니까? 그 이유는 무엇입니까?
   ☐ 한글 책자 ☐ 영문 책자
   (이유:)

2. 본 책자와 해당 소프트웨어에서 사용된 한글 용어에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

3. 본 책자와 해당 소프트웨어에서 번역 품질에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

4. 본 책자의 인쇄 상태에 대한 귀하의 평가 점수는?
   ☐ 수 ☐ 우 ☐ 미 ☐ 양 ☐ 가

5. 한글 소프트웨어 및 책자가 지원되는 분야에 대해 귀하는 어떻게 생각하십니까?
   ☐ 한글 책자를 늘려야 함 ☐ 현재 수준으로 만족
   ☐ 그다지 필요성을 느끼지 않음

6. IBM은 인쇄물 형식(hardcopy)과 화면 형식(softcopy)의 두 종류로 책자를 제공합니다. 어느 형식을 더 좋아하십니까?
   ☐ 인쇄물 형식(hardcopy) ☐ 화면 형식(softcopy) ☐ 둘 다

IBM 한글 지원 서비스에 대해 기타 제안사항이 있으시면 적어주십시오.

_____

_____

_____

☺ 설문에 답해 주셔서 감사합니다.
귀하의 의견은 저희에게 매우 소중한 것이며, 고객 여러분들께 보다 좋은 제품을 제공해 드리기 위해 최선을 다하겠습니다.