



# SAP용 IBM Security Identity Governance 직무 분리

조직에서 SAP 내 직무분리(SoD) 통제 정의가 가능

## 특징

- 교차 플랫폼 솔루션으로 SoD 방침을 중앙에서 정의하여 SAP 및 비 SAP 애플리케이션 전체에 적용
- 활동 기반 SoD 모델이 비즈니스 중심의 활동 관점에서 SoD 방침 정의를 가능하게 함
- 통합 액세스 요청 워크플로로써 모든 유형의 승인 과정, 업무 분배 상향 조정, 하향 조정 등을 처리
- 승인 워크플로의 사실상 모든 지점에서 거의 실시간으로 SoD 스캔
- SoD 도메인으로써 허위 SoD 경고 감소
- SAP 역할 분석으로 SAP 역할 설계에 대한 모범 관행 이행
- “가장” 분석을 통해, 생산 출시 전에 SoD 방침 변경 이 가져올 영향 시험

직무 분리(SoD)는 비즈니스 프로세스의 리스크 관리를 위한 유력한 접근법입니다. 서로 다른 사람이 업무를 수행하도록 함으로써 오류 및 이해 충돌을 방지하며 투명성을 개선시킬 수 있습니다.

## SAP용 직무 분리 (SAP용 SoD)

SAP용 SoD는 ID 및 액세스 관리를 위한 ISIG(IBM® and one space Security Identity Governance) 플랫폼의 일부입니다. SAP용 SoD는 ISIG의 강력한 SoD 기능을 SAP 시스템으로 확대합니다.

## SAP 승인 객체에 대한 기본적인 지원

SAP용 SoD는 SAP 역할 및 낮은 수준의 SAP 권한 객체에 대한 기본적인 검사를 지원합니다. SAP용 SoD는 SAP 권한과 기업 SoD 방침을 상호 연관시켜 SoD 상충이 발생하면 그것을 거의 실시간으로 경고 표시합니다. 또한, “SAP 역할 분석”은 설계 단점 및 보안 리스크에 대한 SAP 역할을 자동으로 점검합니다.

## 액세스 요청 워크플로에서 실시간에 가까운 SoD 점검

SAP용 SoD는 ISIG의 강력한 액세스 요청 워크플로와 긴밀하게 통합하여 액세스가 요청되거나 할당되는 지점에서 거의 실시간으로 SoD 리스크를 점검합니다. 관리자 및 보안 관리자가 액세스 요청에 대한 SoD 위험에 관해 신속한 피드백을 받아 적절하게 행동하거나 요청에 대해 보고할 수 있습니다.



**SoD 완화**

모든 SoD 충돌을 금지할 수는 없습니다. SoD 규정을 신속하게 준수할 수 없거나 프로세스 교정 비용이 SoD 리스크보다 큰 비즈니스 프로세스가 있기 마련입니다. 이런 이유로 SoD 완화 조정 기능은 SoD 솔루션의 필수적인 부분입니다.

SAP용 ISIG 및 SoD는 SoD 리스크 추적 및 관리 도구를 통해 실제 비즈니스 프로세스를 처리합니다. 보안 관리자는 ISIG의 통합 액세스 요청 워크플로를 통해 거래 모니터링과 같은 SoD 보완적 통제를 동원하여 사용자가 따르도록 지원합니다.

**활동 기반 SoD 모델**

SAP의 SoD는 혁신적인 행동 기반 SoD 모델을 활용하여 높은 수준의 비즈니스 중심 행동 관점에서 SoD 상충을 정의합니다. 이 접근법을 통해 비즈니스 전문가들은 IT 전문가들이 관리하는 낮은 수준의 권한과 별도로 SoD 방침을 정의하고 관리할 수 있습니다. 또한 SAP용 SoD는 SoD 도메인을 사용해 모델을 분할하여 허위 교차 도메인 SoD 경고를 줄여줍니다. 마지막으로 “가정” 분석은 생산 출시 전에 방침 변화 효과를 테스트합니다.

아울러, 이런 기능을 통해서 대규모 또는 복합 사업체에 대해 보다 확장 가능한 SoD 관리가 가능하게 됩니다.

**교차 플랫폼 호환성**

SoD의 효과성을 최대화하려면 중요한 모든 기업 거래를 포괄해야 합니다. SAP에 이어 많은 데이터베이스, SOA 서비스 및 사용자 정의 애플리케이션도 역할을 담당합니다. 모든 종류의 권한을 지원하기 위해 상향식으로 고안된 ISIG는 SAP 및 비 SAP 애플리케이션에 걸쳐 비즈니스 프로세스를 보호하는 수단을 제공합니다.

**IBM Security 솔루션 소개**

IBM Security는 최고급 및 통합 엔터프라이즈 보안 제품 및 서비스 포트폴리오를 제공합니다. 전 세계적으로 이름 높은 IBM이 지원하는 포트폴리오는 IBM® X-Force® 연구 및 개발의 지원을 받는 포트폴리오는 보안 정보를 제공해 조직이 총체적으로 사람, 인프라, 데이터 및 애플리케이션, ID 및 액세스 관리용 오픈링 솔루션, 데이터베이스 보안, 애플리케이션 개발, 리스크 관리, 엔드포인트 관리, 네트워크 보안 등을 보호하도록 지원합니다. 이러한 솔루션은 조직이 효과적으로 리스크를 관리하고 모바일, 클라우드, 소셜 미디어 및 기타 엔터프라이즈 비즈니스 아키텍처에 대한 통합 보안을 구현하도록 지원합니다. IBM은 세계에서 가장 광범위한 보안 연구, 개발 및 제공 조직을 운영하며, 130개가 넘는 국가에서 150억 개의 보안 이벤트를 모니터링하고, 3,000개가 넘는 보안 특허를 보유하고 있습니다. 또한, IBM Global Financing은

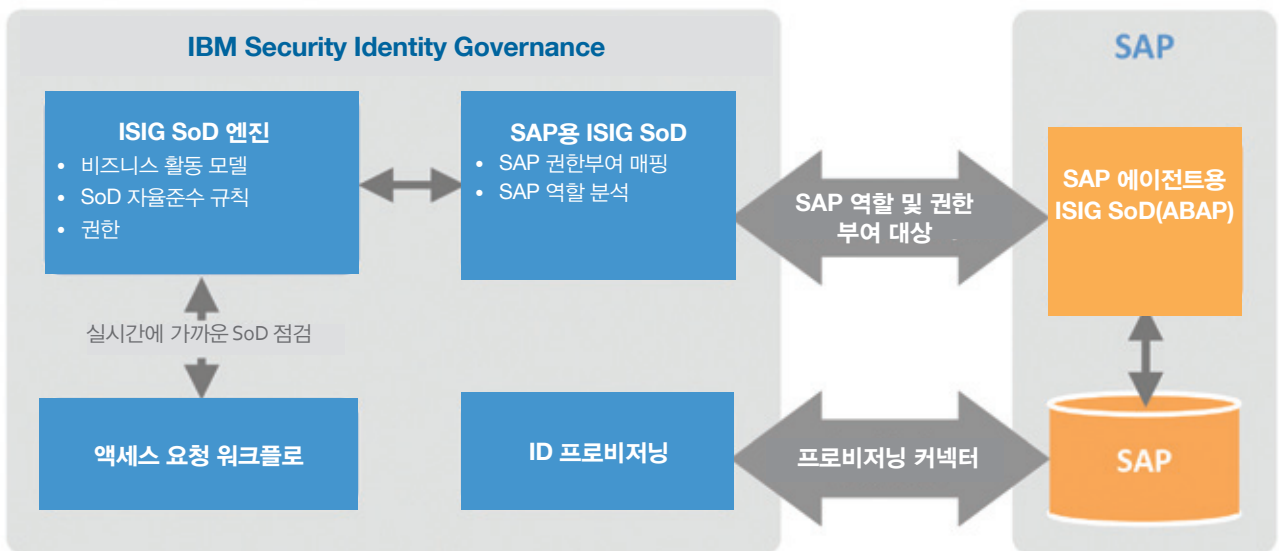


그림 1: SAP용 직무 분리(SoD)

가장 비용 효율적이고 전략적인 방법으로 비즈니스에서 필요로 하는 소프트웨어 기능을 취득할 수 있도록 지원합니다. IBM은 신용 있는 고객과 협력하여 귀사의 비즈니스 및 개발 목표에 적합하고 효과적인 현금 관리를 가능하게 하며 귀사의 총소유비용을 개선하는 맞춤형 재무 솔루션을 제공합니다. IBM Global Financing으로 중대한 IT 투자에 자본을 투입하고 귀사의 비즈니스를 발전시키십시오. 자세한 정보는 다음 웹사이트를 참조하십시오: [ibm.com/financing](http://ibm.com/financing)

### **ISIG (IBM Security Identity Governance) 소개**

ISIG는 기존의 Identity Management에서 Identity & Access Governance로의 진화를 나타냅니다. ID 관리가 일반적으로 사용자 프로비저닝과 같은 IT 프로비저닝에 집중하여 사용자 관리를 보다 효율적이고 경제적으로 한 반면, ISIG는 규정 준수, 감사 및 리스크 관리 요건을 처리하도록 설계되었으며 기존 ID 관리는 이것의 일부에 불과합니다. 통합된 ISIG 접근법은 IT 인프라에서 규정 준수 방침 및 리스크 관리를 구분하고, “ID 인텔리전스” 기능을 통해 액세스 통제 방침을 구현합니다.

### **왜 IBM인가?**

IBM Security 솔루션은 사기 예방 및 식별, 액세스 관리 분야에서 전 세계 조직들의 신뢰를 받고 있습니다. 이 입증된 기술은 조직이 최신 보안 위협으로부터 고객, 직원 및 업무 핵심 자원을 보호할 수 있도록 지원합니다. 새로운 위협이 등장하면서 IBM은 조직이 전체 제품, 서비스, 비즈니스 파트너 솔루션 포트폴리오를 갖춘 핵심 보안 인프라를 구축하도록 지원할 수 있습니다. IBM은 조직에 보안 취약성을 줄이고 전략적 이니셔티브의 성공에 집중할 수 있는 권한을 부여합니다.

### **자세한 정보**

자세한 정보는 다음 웹사이트를 참조하십시오:  
[ibm.com/security.com](http://ibm.com/security.com)



© Copyright IBM Corporation 2015

IBM Corporation  
Software Group  
Route 100  
Somers, NY 10589

2015년 3월

IBM, IBM 로고, [ibm.com](http://ibm.com) 및 CrossIdeas는 전 세계 많은 관할지에 등록된 International Business Machines Corp.의 상표입니다. 그 밖의 제품 및 서비스 이름은 IBM 또는 해당 회사의 상표입니다. 현재 IBM 상표 목록은 다음 웹사이트의 “저작권 및 상표 정보”에서 확인할 수 있습니다:  
[ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)

Adobe, Adobe 로고, PostScript 및 PostScript 로고는 미국 또는 기타 국가에서 사용되는 Adobe Systems Incorporated의 상표 또는 등록 상표입니다.

Linux는 미국 또는 기타 국가에서 사용되는 Linus Torvalds의 등록 상표입니다.

Microsoft, Windows, Windows NT 및 Windows 로고는 미국 또는 기타 국가에서 사용되는 Microsoft Corporation의 상표입니다.

본 문서는 출판 시점에 유효한 문서로서, IBM에서 언제든지 변경할 수 있습니다. IBM이 사업을 운영하는 모든 국가에서 모든 제안이 제공되는 것은 아닙니다.

이 문서의 정보는 상품성, 특정 목적에의 적합성에 대한 보증 및 비침해에 대한 보증이나 조건을 포함하여 명시적 또는 묵시적으로 어떠한 보증 없이 “있는 그대로” 제공됩니다.

IBM 제품은 제품과 함께 제공되는 계약서의 이용 약관에 따라 보상을 받으실 수 있습니다.

올바른 보안 관행 기술: IT 시스템 보안은 기업 내외에서의 부적절한 접속에 대한 예방, 탐지 및 대응을 통하여 시스템 및 정보를 보호하는 일을 담당합니다. 부적절한 접속으로써 정보를 변경, 파괴 또는 악용하거나 다른 정보를 공격하는 등 시스템 손상 또는 시스템 오용으로 이어질 수 있습니다. 어떠한 IT 시스템 또는 제품도 완전히 안전하다고 고려되지 않으며, 어떠한 단일 제품 또는 보안 조치도 부적절한 접속 방지에 완전히 효과적일 수 없습니다. IBM 시스템 및 제품은 포괄적인 보안 접근법의 일환으로 설계되었고, 추가 운영 절차에 필연적으로 관여하고, 최대한 효과적으로 되기 위해 기타 시스템, 제품 또는 서비스를 요구할 수도 있습니다. IBM은 시스템 및 제품이 제3자의 악성 또는 불법적인 행위로부터 면제된다고 보증하지 않습니다.

CrossIdeas는 2014년 7월에 IBM에 인수되었습니다.



재활용 하십시오