NET and Human Interface
The best Identity and Access Management solution.

차세대 통합 계정 및 접근 관리

Reporter : ㈜ 넷앤드휴먼인터페이스
D a t e : 2013

서울시 영등포구 여의도동 44-23 하남빌딩 1005호 Tel : 02-2661-1410

CONTANTS

IAM 등장 배경

IAM (Identity & Access Management) 이란?

IAM (통합계정관리 솔루션) 이란 무엇인가?

- EAM (Extranet Access Management) 솔루션의 차등적 접근 제어를 구현하기 위하여, 시스템 관리자가 직원들의 접근 권한 및 계정 관리 작업을 일일이 입력해야 됨으로써, 시스템 관리에 드는 시간/비용 손실이 크다. 이를 해결하기 위하여 기존 EAM 에 자동적 권한 부여 및 계정관리 기능이 추가된 것이 통합 계정 관리 (IAM) 솔루션이다.
- 사용자 계정과 권한 관리를 위한 기술로 유저 프로비저닝 (User Provisioning), 전사적 접근 관리, 분산 관리, 패스워드 관리, 싱글 사인 온 (Single Sign-on) 을 포함한 통합 보안 기술을 지칭한다.

SSO, EAM, IM, IAM 의 비교

구분	SSO	EAM	IM	IAM
Authentication(인증)	지원	지원	미지원	지원
Authorization(권한)	미지원	지원	지원	지원
Administration(관리)	미지원	지원	지원	지원
Provisioning	미지원	미지원	지원	지원

IAM 등장 배경

보안 패러다임의 변화

보안관리 범위와 대상 목표의 변화

- 네트워크 보안(웜 바이러스 또는 외부 공격으로 부터 방어) 에서 컨텐츠 (정보 유출 방지) 로 변화
- 기업 기밀 정보 유출에 따른 기업의 경제적 손실 증가
- 최근 정부 차원의 개인 정보보호와 관련된 각종 규제의 강화

AS-IS

- 방화벽
- 침입 탐지/방지 시스템
- 백신/서버보안
- 기타

IT 시스템 및 네트워크 보안

해커

바이러스

TO-BE

- 문서 보안
- DB 보안
- 데이터유출 방지
- 통합 계정 관리
- 기타

컨텐츠 보안 (정보보호)

산업스파이

개인정보유출

IAM 등장 배경

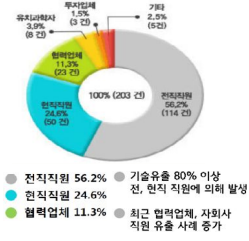
개인 정보 유출 현황

❖ 개인정보 침해건수

〈한국인터넷 진흥원〉

→2010년은 약 5만 5천여 건으로 2009년 대비 36% 증가

❖ 국내 기술 유출에 따른 피해 규모



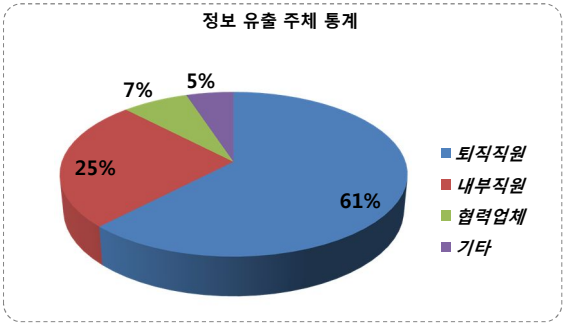
(출처: 산업기밀보호센터)

→ 지난 2004~2010년 국내 산업기술 사건으로 인한 피해는 244건, 피해액 약 435조원 추정

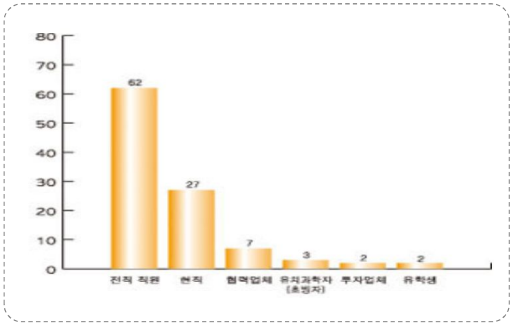
IAM 등장 배경

개인 정보 유출 주체 통계

기업내부 정보 유출 사고의 주체는 ?



출처 : 데이터넷



출처 : 국가정보원

- 조사 결과로 보면 전체 유출 사고의 **86%** 가 내부 및 퇴직자인 것으로 파악되고 있다.
- 해외 자료에서는 **61~70%** 까지 내부자에 의한 데이터 유출 사고로 집계 하고 있다.

EAM 등장

등장 배경

실제 발생 될 수 있는 관리상의 문제

- 내부 직원 한명이 퇴직할 경우 해당 직원이 접속 가능한 서버 또는 네트워크 장비의 접속 권한을 어떻게 일괄적으로 제거할 것인가?
- 특정 직원의 부당한 행위를 발견 했을 경우, 모든 시스템에 해당 직원의 사용 권한 및 현재 세션을 즉각적으로 종료 시키고, 그동한 작업한 내역을 종합적으로 분석할 것인가?
- 계약직 사원 또는 유지보수 업체에게 특정 시간, 특정 IP에만 특정 서비스를 이용하도록 제한해야 할 경우 이것을 어떻게 제한할 것인가?
- 인가된 권한을 가지고, 실제 시스템에 접속 후 악의적인 명령어 사용을 제한하려 할 경우 어떻게 제한할 것인가?
- 계약직 사원 또는 유지보수 업체에게 시스템 접속 시 요구되는 패스워드 정보를 유출하지 않아야 하는데, 어떻게 유출하지 않고 접속 권한을 부여할 것인가?

EAM 등장

Compliance

개인정보의 안전성 확보조치[시행령(안) 제33조)

□ 관리적 보호조치
- 내부관리계획의 수립 및 시행
- 교육계획 수립·시행
- 정기적인 자체 감사 실시

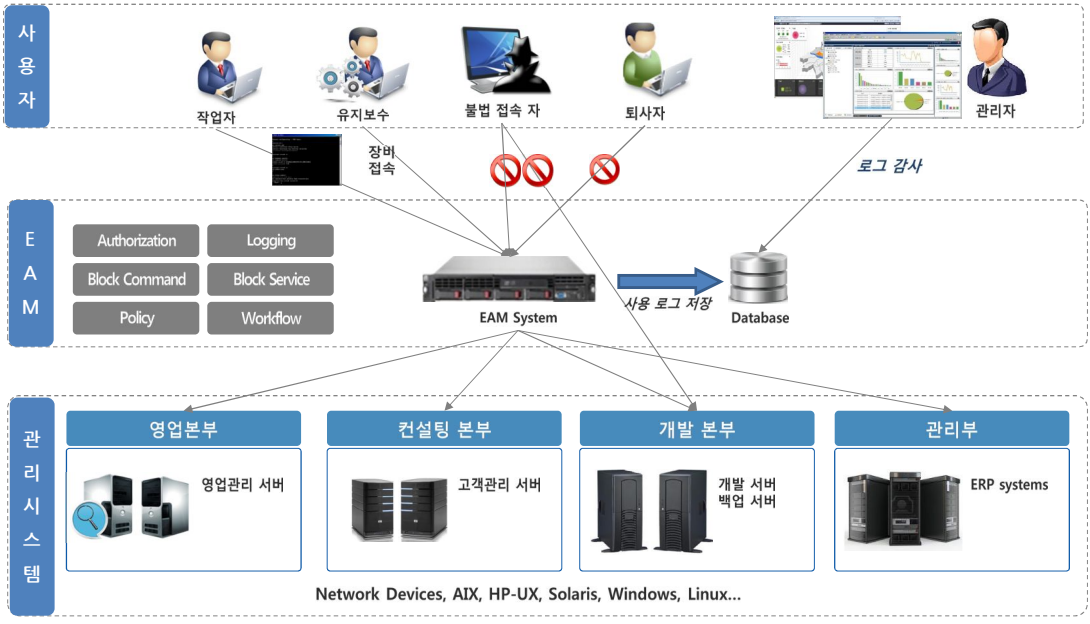
□ 기술적 보호조치
- 접근권한 제한·관리, 접근권한 확인을 위한 식별 및 인증
- 권한 없는 접근을 차단하기 위한 시스템의 설치 등 조치
- 개인정보의 안전한 저장·전송을 위한 암호화 등 조치
- 접속기록의 보관 및 위·변조 방지 조치
- 보안프로그램 설치 및 주기적 갱신·점검 조치

과태료 · 벌칙

- 내부관리계획 수립, 접속기록 보관 등 안전성 확보 미조치
  ☞ 3천만원 이하의 과태료(75조)
- 안전성 확보 미조치로 인한 개인정보 분실 · 도난 · 유출 · 변조 · 훼손
  ☞ 2년 이하 징역 또는 1천만원 이하 벌금(73조)

EAM 등장

EAM 구성



EAM 등장

EAM 주요 정책

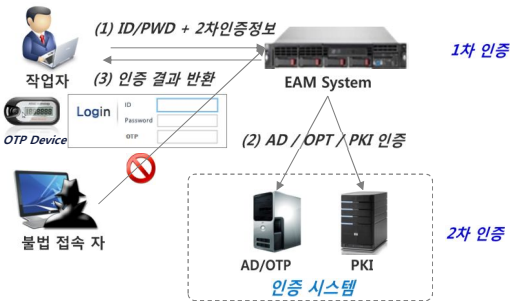
구분	정책	설명
인증 관리	ID/PWD + OTP / PKI, 접근 가능 IP+MAC 인증	• 사용자 계정 인증 관리 • OTP / PKI 등을 이용한 2중 인증 • 접근 가능 IP/MAC 제한 기능
	장비 접속 자동 로그인	• 장비에 접속 시 Password 노출을 막기 위한 자동 로그인 기능
권한 관리	장비 접근 권한 관리	• 사용자별 접근 가능한 시스템 권한 관리
	서비스 사용 권한	• 사용자의 장비별 접근 가능한 프로토콜 권한 관리
	명령어 사용 권한	• 사용자별 시스템에 사용 가능 또는 불가한 명령어 관리
로그 감사	사용 명령어 감사	• 시스템에 접속하여 사용한 명령어 감사
	작업 로그 감사	• 전체 작업 로그 감사 및 분석

EAM 등장

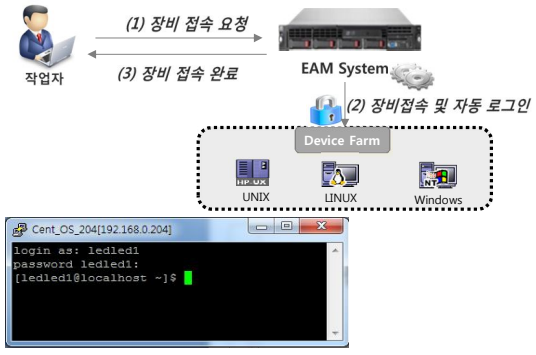
인증 (Authentication) 정책

다양한 인증 방식

- ID/PWD, PKI, OTP, AD 등 인증 방법을 중앙에서 결정 및 관리
- 장비 접속 시 자동 로그인 기능을 이용한 Password 유출 방지



ACL	시스템 로그온 가능 IP/MAC Address 제어
Time	계정 사용 기간/요일 별 로그온 가능 시간 제어
Notify	시스템 로그인 기록 저장 및 알림 기능



➢ *계정 PWD 유출 방지*

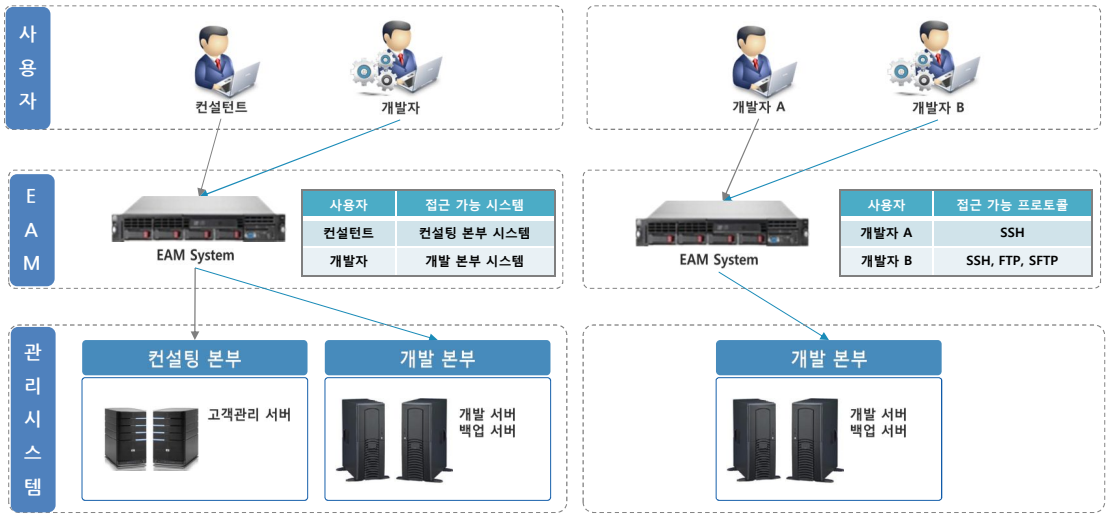
Auto login : All Unix , Linux, Windows

EAM 등장

권한 (Authorization) 정책 (1)

RBAC (Role Base Access Control) 기반 권한 할당

- 사용자별 접근 가능 장비 권한 할당 및 중앙에서 정책 관리
- 사용자별 장비별 사용 가능 프로토콜 권한 할당



EAM 등장

권한 (Authorization) 정책 (2)

RBAC (Role Base Access Control) 기반 권한 할당

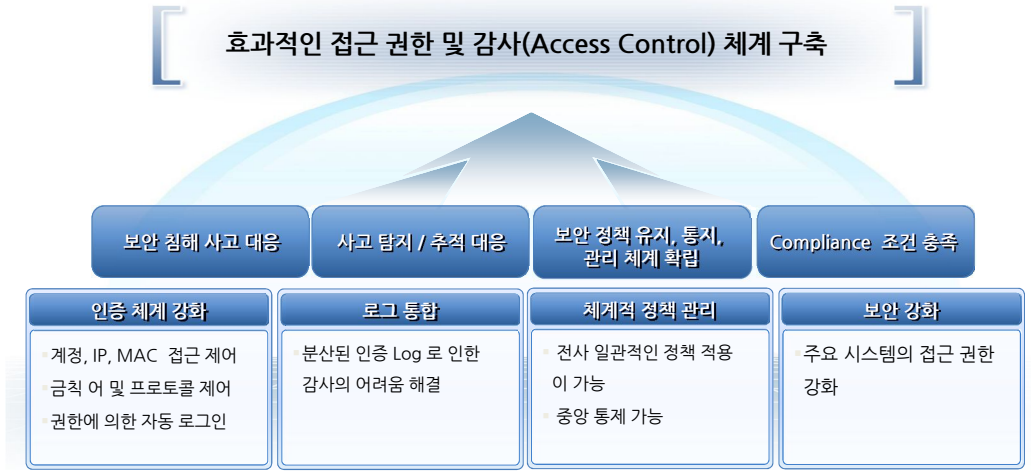
- 사용자별 / 장비별 사용 가능 또는 불가능한 명령어 제어 (정규표현식)

차단	인가되지 않은 명령어 사용 시 EAM 시스템에서 해당 명령어 전송 차단 및 일정 횟수 초과 시 세션 강제 차단
감사	금지 명령어 사용 내역에 대한 감사
Notify	금지 명령어 사용 시 관리자에 즉시 알림

EAM 등장

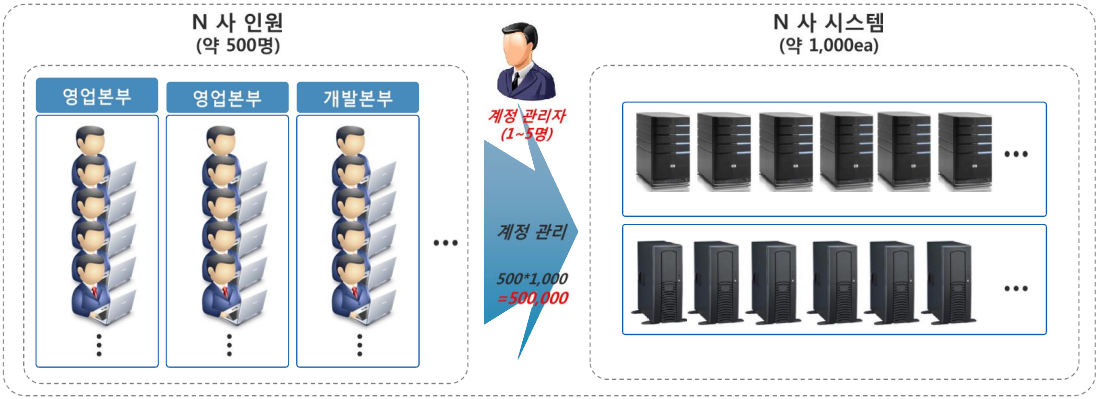
EAM 도입 기대 효과

❖ 중앙 집중식 사용자 인증 및 통합 권한 관리로 인한 생산성 향상 및 보안성과 안정성 획득



IM 등장

IM 의 등장 배경



계정 관리자의 당면 과제

- 관리 시스템의 접속 계정의 1:1 계정 정책 수립은 어떻게 할 것인가?
- 각 계정 또는 계정 그룹별 보안 정책 수립(Password 변경 주기)은 어떻게 할 것인가?
- 퇴사자 또는 입사자 발생 시 많은 시스템에 계정 생성 및 관리 작업은 어떻게 할 것인가?
- 각 시스템별 어떤 계정이 휴면 계정이고, 불법 계정을 어떻게 조사할 수 있을 것인가?
- 전결권자가 아닌데 승인은 어떻게 하지?

퇴근은 할 수 있을까?

IM 등장

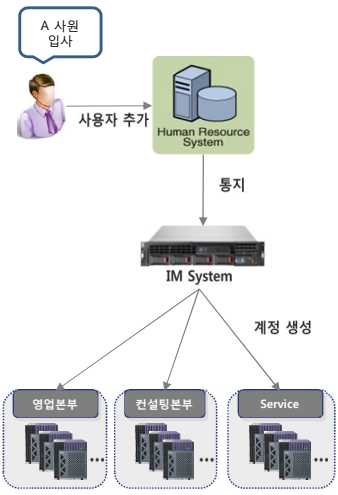
Compliance

		조항	내용
제3장. 전자금융거래의 안전성 확보 및 이용자 보호	제4절 정보기술 부문	제12조. 단말기 보호대책	제3항. 비밀번호는 **생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상**으로 설정하고 **분기별 1회 이상 변경**할 것
		제13조. 전산자료 보호대책	제1항.제1호. **사용자계정과 비밀번호를 개인별로 부여**하고 **등록·변경·폐기를 체계적으로 관리**할 것
			제1항.제2호. **외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당**하고 적절한 통제장치를 갖출 것
			제1항.제14호. 사용자가 전출·퇴직 등 **인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제**할 것
			제2항. 제1항 제1호의 **사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리**하여야 한다.
		제32조. 내부사용자 비밀번호 관리	제1항. 담당업무 외에는 열람 및 출력을 제한할 수 있는 **접근자의 비밀번호를 설정**하여 운영할 것
			제2항.가호. 제12조제3호에 따라 비밀번호 부여 및 변경
			제2항.다호. **시스템마다 관리자 비밀번호를 다르게 부여**

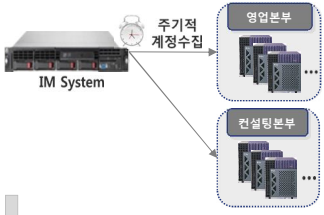
IM 등장

관리자의 문제 해결

Provisioning



Reconsilation



➢ *전체 시스템의 등록된 계정 수집*

비 정상 계정 탐지

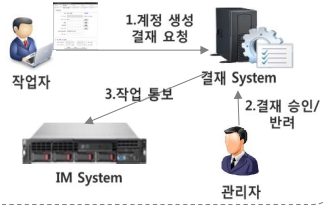
- Lock 계정
- Password 사용 만료 계정
- Ghost 계정 (System 에만 존재)
- Broken 계정 (IM 에만 존재)
- 휴면 계정

Policies & Workflow

➢ *주요 정책*

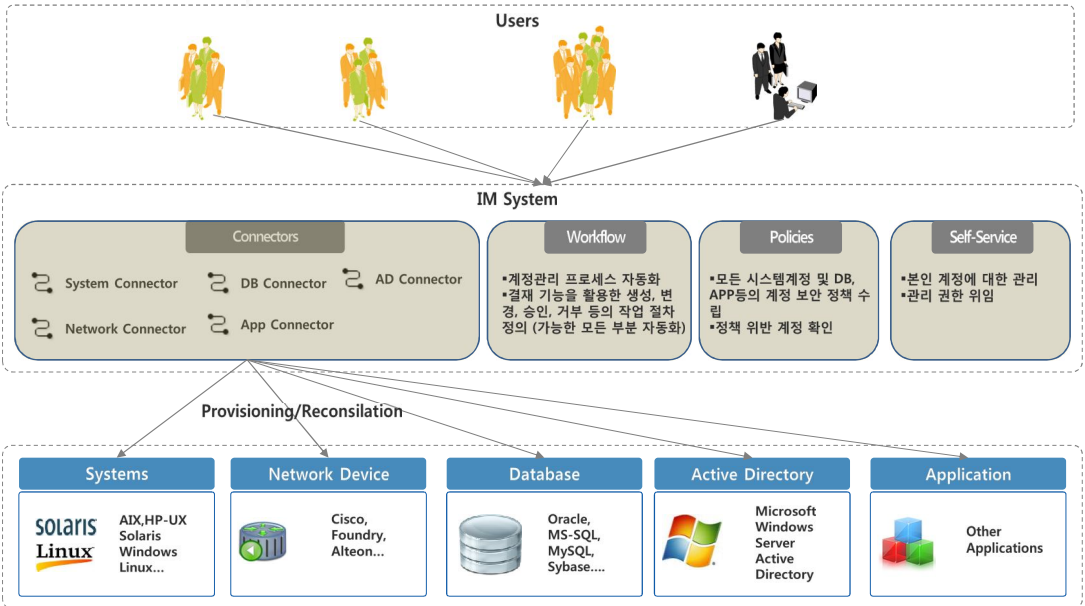
구분	정책
ID 관리	ID 최소/최대 길이
	영/숫자 혼합 여부
Password	최소/최대 길이
	대/소문자/숫자/특수문자 혼합
	딕셔너리 설정
보안 정책	계정 및 PWD 사용 기간
	휴면 및 퇴사자 계정 처리정책

➢ *Workflow*



IAM 등장

IM 주요 구성 요소



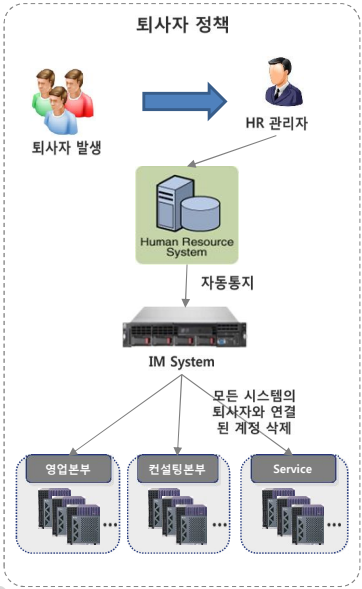
IAM 등장

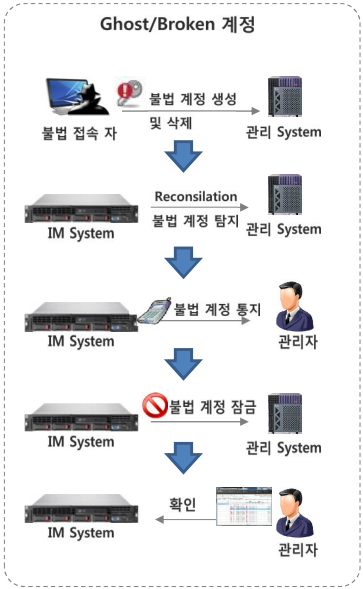
주요 정책

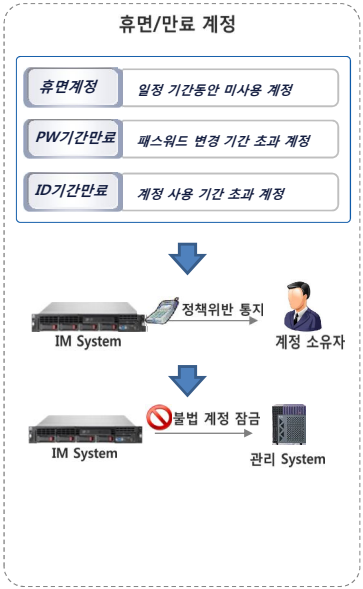
구분	정책	설명
계정 관리	Reconsilation	• Linux, Unix, Windows, Active Directory, Database, Network Device 계정 수집
	Provisioning	• 계정 추가, 수정, 삭제
기본 정책	퇴사 및 부서 이동자 정책	• 퇴사자 발생 시 즉시 관련 계정 삭제 또는 Lock • 부서 이동 시 관련 계정 정책 자동 반영
	패스워드 보안 정책	• 패스워드 보안 규칙 준수 • 주기적 패스워드 자동 변경
불법 계정	Ghost / Broken	• 불법으로 서버에 생성한 계정 탐지 (Ghost) • 불법으로 삭제한 서버의 계정 탐지 (Broken)
	정책 위반 계정	• 휴면 계정 • 패스워드 정책 미 준수 계정 • 사용 기간 초과 계정
계정 권한	공용 계정	• Naming Rule • 공용 계정 소유자 설정 • 공용 계정 권한 신청/승인
	개인 계정	• 1:1 계정 정책

IM 등장

주요 계정 관리 정책



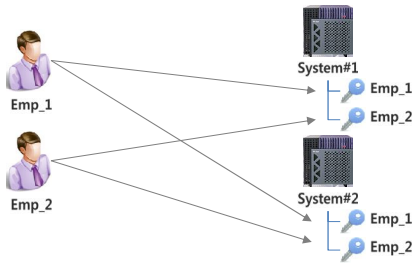




IM 등장

주요 정책 설명 - 공용 계정 정책

1:1 개인 계정 정책



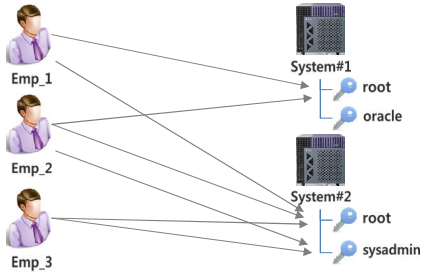
➢ 장점

- 시스템 계정별 소유자가 1명이라 해당 계정에 대한 명확한 소유자가 존재한다.
- 개인 계정에 대해서, 개인이 관리할 수 있다. (PWD 변경)

➢ 단점

- 사용자 수가 많을 경우 시스템별 계정수가 많아진다.
- 각 사용자별 UID, GID 등과 같은 유일 속성에 대한 매핑 작업에 대한 관리 업무가 늘어난다.

1:N 공용 계정 정책



➢ 장점

- 시스템에 존재하는 계정을 여러 사용자가 공유해서 사용하므로, 시스템별 계정수가 적다.
- 개인계정 보다 상대적으로 계정수가 적으므로 관리가 용의함.

➢ 단점

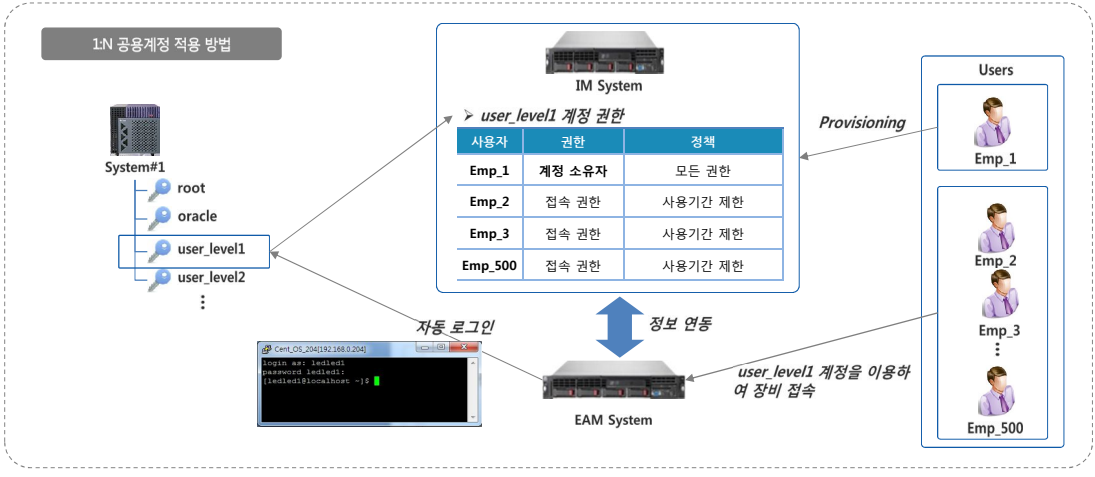
- 패스워드가 노출 또는 변경될 경우 같이 사용하는 모든 사용자에 영향을 미친다.
- 여러 시스템에 동일 ID 에 동일 PWD 를 쓸 경우 계정 정보 노출 시 보안 이슈.

IM 등장

공용 계정 관리 정책

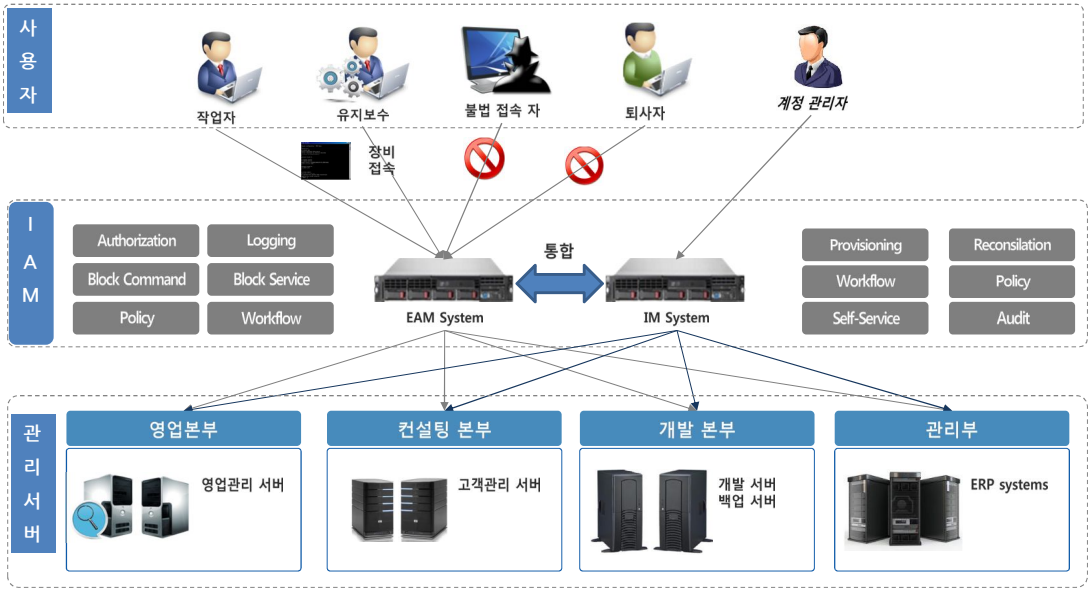
➢ 계정 관리 방법의 변화

- 사용자가 500 명이라고 가정할 경우 1:1 계정 정책을 사용할 경우 실제 시스템에 500 개 이상의 계정이 생성되어 IM 시스템을 도입하더라도 관리의 어려움이 발생한다.
- 시스템의 계정을 권한 레벨별로 생성하고, 해당 계정을 사용할 수 있는 권한 사용자를 IM 에서 관리 (1:N)하도록 한 후 EAM 시스템과 연계하여, 장비 접속 시 할당받은 계정으로 자동로그인 시켜 패스워드 노출을 방지할 수 있다.



IAM

EAM + IM = IAM 구성

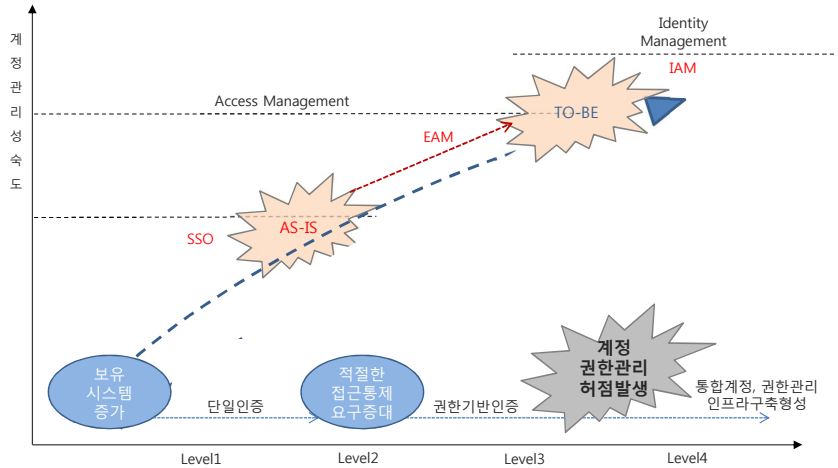


IAM

통합 계정 관리 트랜드 분석

- 계정관리가 단일사용자 인증인 SSO(Single Sign On), 권한 및 접근 제어가 가능한 EAM(Extranet Access Management) 형태에서 현재는 계정관리, 프로비져닝, 접근제어, 모니터/감사등 정책기반의 통합 계정관리 형태인 IAM(Identity Access Management)으로 변모하고 있습니다.

IT보안 트렌드 변화



IAM

ROI

- 정량적인 기대 효과 치
  - > 50,000 User
  - > 5 개 기존 업무 적용
  - > 3 년 내에 5 개 신규 업무개발 예정이며 현재 10 개의 서버 도입 중

IAM Solution 도입은 1 년에 300% ROI 효과를 볼 수 있으며 관리 대상 사용자와 관리대상 시스템이 많을 수록 ROI 효과를 볼 수 있는 기간이 짧아 진다.
– Gartner

Consulting

계정 관리 측면		User Self Service 측면		Provisioning 측면		Password 관리 측면	
Without IAM	With IAM	Without IAM	With IAM	Without IAM	With IAM	Without IAM	With IAM
$6.00/user (1 year)	$0.80/user (1year)	$7.40/user (event 발생)	$1.30/user (event 발생)	$50.60/user (1 year)	$22.40/user (1 year)	$19.30/user	$2.60/user
1 년에 $5.20/user 절감		1개의 업무당 $6.10/user 절감		1 년에 $28.20/user 절감		$16.70/user 절감	
절감 이유	관리자의 workload와 교육 비용 절감	**절감 이유**	등록과 패스워드 reset 의 자동화로 관리자의 workload 감소	**절감 이유**	자동화된 사용자 등록을 통한 계정 관리 비용 감소	**절감 이유**	Help desk staff 비용 절감

- 국내 EAM 및 IM 시장은 2000년을 시작으로 지속적으로 활성화 되고 있는 상황이고, 최근 개인 정보 유출 사건으로 인하여, 도입 필요성이 증대 되고 있음.

- 다양한 인증 및 중앙 집중식 권한 관리로 확고한 보안 정책 수립이 가능

- EAM 이나 IM 솔루션을 각각 보유하고 있으나, 두개 솔루션이 통합(Integration) 되었을 경우 가장 좋은 ROI 가 기대됨

- 자동화된 계정관리 및 접근권한관리를 통합적으로 수행할 수 있도록 해 전사 시스템에 대한 사용 편의성 증가, 보안성 강화, 운영 및 개발비용 감소등의 효과를 얻을 수 있음

NET and Human Interface

The best Identity and Access Management solution.

감사합니다.