일방향 암호화 법규 준수기반의 최고권한계정 패스워드 관리

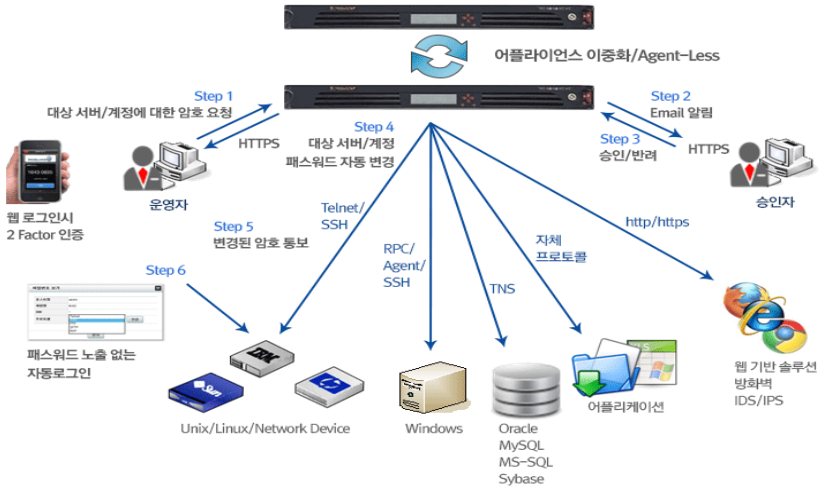
Automated Process Policy Management for Password



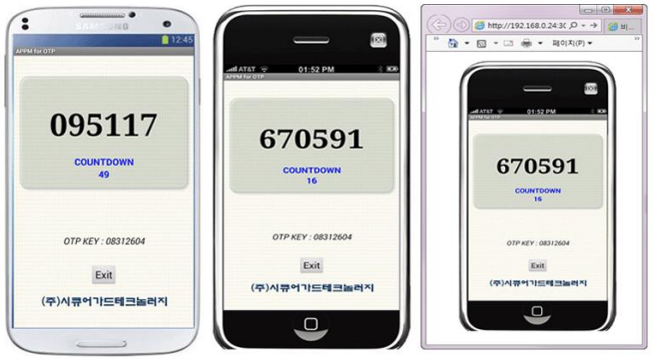
㈜시큐어가드테크놀러지

시큐어가드테크놀러지 소개

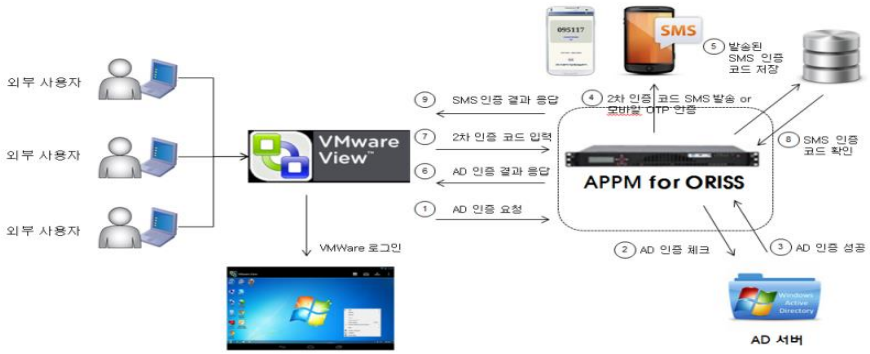
APPM for Password



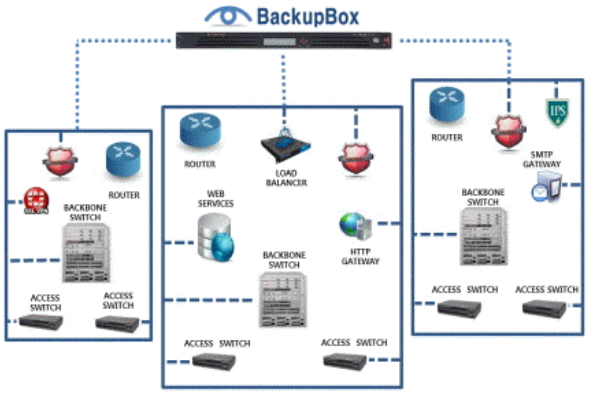
APPM for OTP



APPM for ORISS



APPM for BackupBox



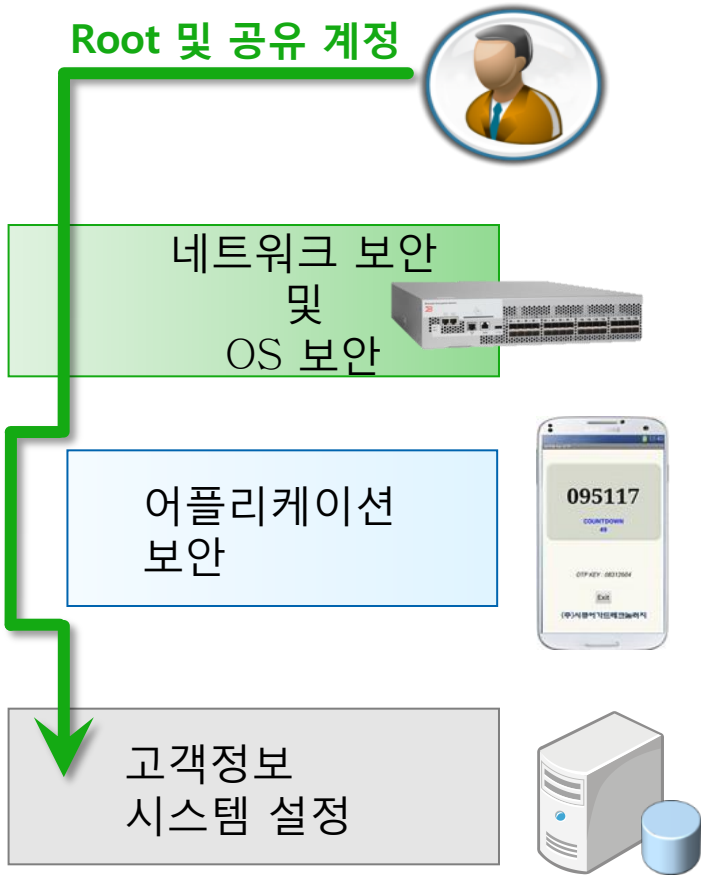
통합패스워드관리
'APPM'
대통령상 수상



"통합패스워드관리 APPM , '글로벌 SW 공모대전' 대통령상 수상"

➢ ‘root’ 및 공유 계정

- 다수의 사용자
- 비밀번호 공유
- 무제한의 시스템 및 데이터베이스 데이터 열람, 수정
- 시스템 파일 수정
- 로그 파일 위변조
- 비밀번호 변경 주체 불확실



```
68 184D4100   PUSH 00414D18
52            PUSH EDX
E8 32230000   CALL 00404AD5
83C4 0C       ADD ESP,0C
8D8424 58010  LEA EAX,[ESP+158]
50            PUSH EAX
68 5C4D4100   PUSH 00414D5C
EB 1B         JMP SHORT 004027D0
68 884D4100   PUSH 00414D88
52            PUSH EDX
E8 15230000   CALL 00404AD5
83C4 0C       ADD ESP,0C
8D8424 58010  LEA EAX,[ESP+158]
50            PUSH EAX
68 BC4D4100   PUSH 00414DBC
8D8C24 70030  LEA ECX,[ESP+370]
51            PUSH ECX
E8 F8220000   CALL 00404AD5
```

```
Format = "%sLocal Settings\Application Data\Felix_Deimel\mRemote\confCons.xml"
Arg1
Dropper.00404AD5

ASCII "%sApplication Data\VanDyke\Config\Sessions"

Format = "%sAppData\Local\Felix_Deimel\mRemote\confCons.xml"
Arg1
Dropper.00404AD5

ASCII "%sAppData\Roaming\VanDyke\Config\Sessions"

Arg1
Dropper.00404AD5
```

[악성 도구의 원격관리 도구 설정 파일 확인 부분 분석]

sitemanager.xml

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<FileZilla3>
    <Servers>
        <Server>
            <Host>192.168.5.129</Host>
            <Port>22</Port>
            <Protocol>1</Protocol>
            <Type>0</Type>
            <User>appm</User>
            <Pass>appmadmin</Pass>
            <TimezoneOffset>0</TimezoneOffset>
            <PasvMode>MODE_DEFAULT</PasvMode>
            <MaximumMultipleConnections>0</MaximumMultipleConnections>
            <EncodingType>Auto</EncodingType>
            <BypassProxy>0</BypassProxy>
            <Name>192.168.5.129</Name>
            <Comments></Comments>
            <LocalDir></LocalDir>
            <RemoteDir></RemoteDir>
            <SyncBrowsing>0</SyncBrowsing>192.168.5.129
```

[FileZilla3 Site Manager 환경 파일]

주목 받는 비밀번호 관리

치명적 보안사고 원인은 기업내부…계정접근관리 솔루션 인기

발췌 Da 디지털데일리

국내 IAM 전문 업체의 한 관계자는 "최근 은행권을 대상으로 계정관리 솔루션 고도화 프로젝트를 진행하고 있다. 은행에서는 전산실 내에서 사용되는 계정, 비밀번호 관리를 보다 엄격하게 하겠다는 취지" 라고 전했다.

한편 IAM 솔루션이 시장의 주목을 받고 있는 것과 관련 정광연 한국오라클 상무는 "계정관리는 기업에게 있어 가장 중요한 이슈다. PC, 모바일과 같은 분류는 기업 인프라에 접근하는 채널의 문제에 불과하다" 며 "중요한 것은 기업 데이터 보호를 위해 각 계정의 관리, 계정의 권한을 중앙에서 할 수 있어야한다는 점" 라고 강조했다.

이같은 추세에 맞춰 H 은행은 최근 계정인증체계를 대폭 강화했다. 기존 시스템접근에만 모바일 일회성비밀번호(OTP)를 사용해왔으나, 올해 안 임직원들이 사용하는 모든 PC와 보안시스템, 관리자페이지, 웹서비스 등에도 이를 적용할 계획이다.

또 접근통제를 강화하기 위해 현재 주요시스템 공용계정 200여개에만 적용된 '비밀번호 자동변경시스템' 을 모든 운영시스템, 모든 보안시스템(방화벽, 침입방지시스템 등) 관리계정, 주요 네트워크 관리계정 등에도 적용해 악의적인 접근을 차단할 예정이다.

아울러 시스템 계정관리 솔루션의 수요도 나오고 있다. 기존에는 시스템이나 애플리케이션을 중심으로 사용자의 접근을 제어하거나 관리했으나 사용자별 접근이력이나 시스템 사용 현황을 확인하기에는 제한이 있었다.

특히 최근에는 APT 공격을 통해 일반 사용자 PC를 해킹한 후 다양한 방법으로 시스템 계정을 획득해 추가적인 정보를 탈취하기 때문에 시스템 계정관리는 당위성을 띄는 형국이다.

'H'은행 서비스 적용 이력

1 [2012.11] 공용계정 관리 시스템 도입

- 'D'사 공용계정 관리 시스템 도입
  - UNIX 운영서버 200대 200개
  - 'Root' 계정만 관리

2 [2013.3] 사건 발생 — 3.20 사태발생

- 공용계정 관리 중요성 인식
  - Open계정을 통한 악성코드 감염
  - 공용계정을 통한 악성코드 확산

3 [2013.3] 관리 범위 확산 결정

- 관리 확산 범위
  - 전체 서버 공용계정 대상
  - 주요 네트워크 장비 모든 계정
  - DB를 포함한 전체 서버 모니터링 계정

4 [2013.4] 공용계정 관리시스템 교체 ✓

- APPM 공용계정 관리 시스템 도입
- ※ 교체 사유
  - 국산 네트워크장비, 한글 미지원
  - 워크플로우 커스터마이징 불가

5 [2013.11] 점진적 확산

- [1차] 주요 네트워크 장비(적용완료)
- [2차] DB 및 서버 모니터링 계정(적용中)
- [3차] Application 계정 관리 (예정)

강화되는 비밀번호 컴플라이언스 및 감사 대응

APPM
Automated Process Policy Management

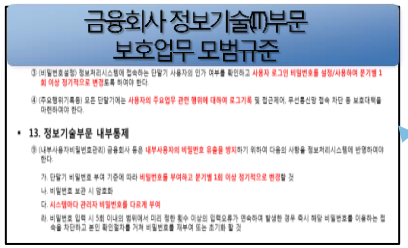
주요 보안사건 사고

- 2008年 2月 옥션 개인정보 대량유출
- 2011年 4月 현대캐피탈 해킹
- 2011年 7月 SK컴즈 개인정보유출
- 2013年 3月 3.20 전산 대란
- 2014年 1月 카드3사 개인정보유출

비밀번호 관리 중요성 대두

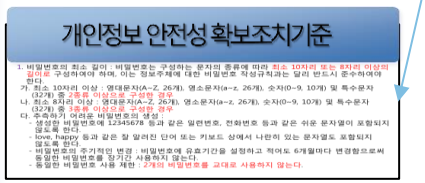
법적 컴플라이언스 강화

금융회사 정보기술(IT)부문 보호업무 모범규준

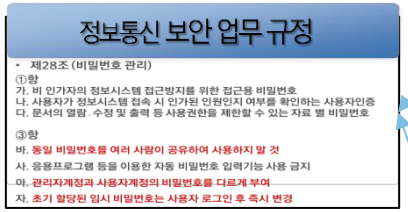


- 13. 정보기술부문 내부통제

개인정보 안전성 확보조치기준



정보통신 보안 업무 규정

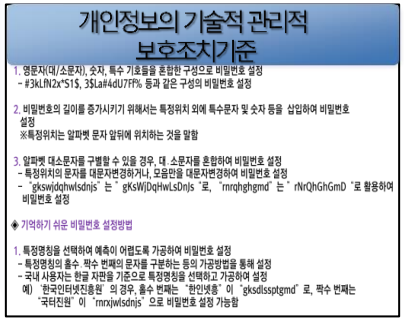


- 제28조 (비밀번호 관리)

①항
가. 비 인가자의 정보시스템 접근방지를 위한 접근용 비밀번호
나. 사용자가 정보시스템 접속 시 인가된 인원인지 여부를 확인하는 사용자인증
다. 문서의 열람. 수정 및 출력 등 사용권한을 제한할 수 있는 자료 별 비밀번호

③항
바. 동일 비밀번호를 여러 사람이 공유하여 사용하지 말 것
사. 응용프로그램 등을 이용한 자동 비밀번호 입력기능 사용 금지
아. 관리자계정과 사용자계정의 비밀번호를 다르게 부여
자. 초기 할당된 임시 비밀번호는 사용자 로그인 후 즉시 변경

개인정보의 기술적 관리적 보호조치기준



1. 영문자(대/소문자), 숫자, 특수 기호들을 혼합한 구성으로 비밀번호 설정
 - #3kLfN2x*S1$, 3$La#4dU7f%% 등과 같은 구성의 비밀번호 설정

2. 비밀번호의 길이를 증가시키기 위해서는 특정위치 외에 특수문자 및 숫자 등을 삽입하여 비밀번호 설정
 ※특정위치는 알파벳 문자 앞뒤에 위치하는 것을 말함

3. 알파벳 대소문자를 구별할 수 있을 경우, 대. 소문자를 혼합하여 비밀번호 설정
 - 특정위치의 문자를 대문자변경하거나, 모음만을 대문자변경하여 비밀번호 설정
 - 'gkswjdqhwlsdnjs' 는 ' gKsWjDqHwLsDnjs '로, 'rnrqhghgmd' 는 ' rNrQhGhGmD '로 활용하여 비밀번호 설정

◆ 기억하기 쉬운 비밀번호 설정방법

1. 특정명칭을 선택하여 예측이 어렵도록 가공하여 비밀번호 설정
 - 특정명칭의 홀수 짝수 번째의 문자를 구분하는 등의 가공방법을 통해 설정
 - 국내 사용자는 한글 자판을 기준으로 특정명칭을 선택하고 가공하여 설정
 예) '한국인터넷진흥원' 의 경우, 홀수 번째는 '한인넷흥' 이 'gksdlssptgmd' 로, 짝수 번째는 '국터진원' 이 'rnrxjwlsdnjs' 으로 비밀번호 설정 가능함

- 비밀번호 복잡도 설정
- 비밀번호 변경주기
- 비밀번호 보관 암호화
- 관리자 비밀번호 개별 설정
- 비밀번호 오류 횟수차단
- 비밀번호 공유금지
- 일방향 암호화

전자금융감독규정

제14조

9. 정보처리시스템의 운영체제(Operating System) 계정으로 **로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것**

제32조

1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
2. 비밀번호는 다음 각 목의 사항을 준수할 것
 가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 **8자리 이상으로 설정하고 분기별 1회 이상 변경**
 비밀번호 보관 시 암호화
 시스템마다 관리자 비밀번호를 다르게 부여
3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 **비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것**

정보통신망 이용촉진 및 정보보호 등에 관한 법률

제15조

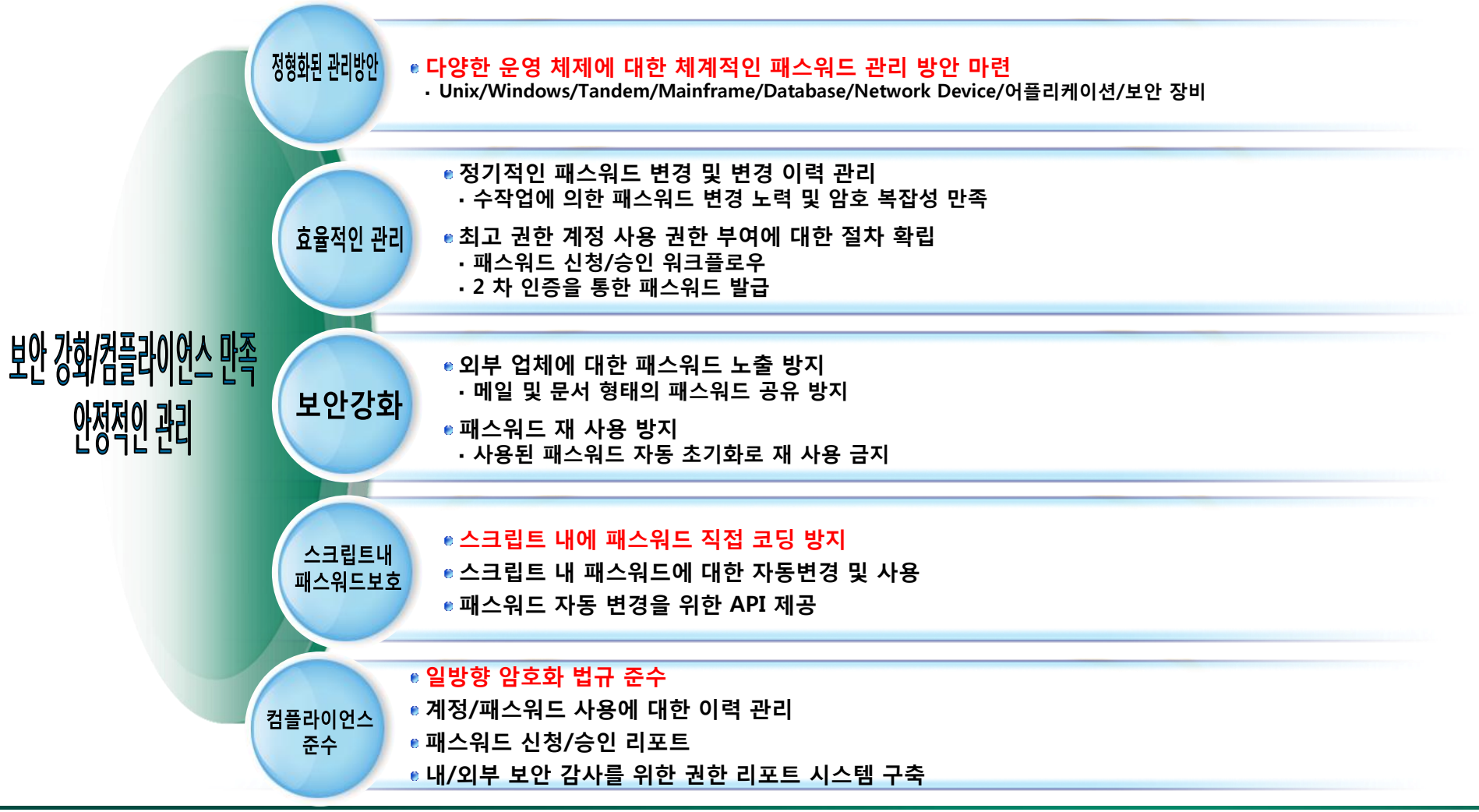
4. 비밀번호 및 바이오정보(지문, 홍채, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보를 말한다)의 **일방향 암호화 저장**

O 은행 보안감사 지적사항

최고 권한 계정에 대한 효율적인 관리 방안

APPM
Automated Process Policy Management

- 최고 권한 계정의 패스워드에 대한 별도의 관리 프로세스, 일회용 비밀번호 사용 및 사용 이력 관리
- 신청/승인에 의한 패스워드 발급 및 리포트 시스템을 통한 컴플라이언스 구축



Automated Process Policy Management for Password

(Appliance Server !)

일회용 비밀번호 발급 솔루션 소개

- 일회용 비밀번호 발급 솔루션 개요
- 비밀번호 발급 솔루션 아키텍처 : 일방향 암호화 정책 준수

APPM
Automated Process Policy Management

일회용 비밀번호 발급!

시장점유 1위

Ⅰ
√ 패스워드 기록/기억 불필요
√ 패스워드 주기적 변경 불필요

Ⅱ
√ 관리자 퇴사시 패스워드 변경 불필요
√ 유지보수인력 작업 시 요청/승인 발급

Ⅲ
√ 패스워드의 안전한 발급
√ 패스워드 노출 없는 자동 로그인

비밀번호 발급 아키텍처

1. 관리자 콘솔을 통한 패스워드 변경 정
   책 정의
2. 초기 설
   자동 수집, 일
3. 워크플로
   일회용 비밀
4. 직접 접
5. 감사 리



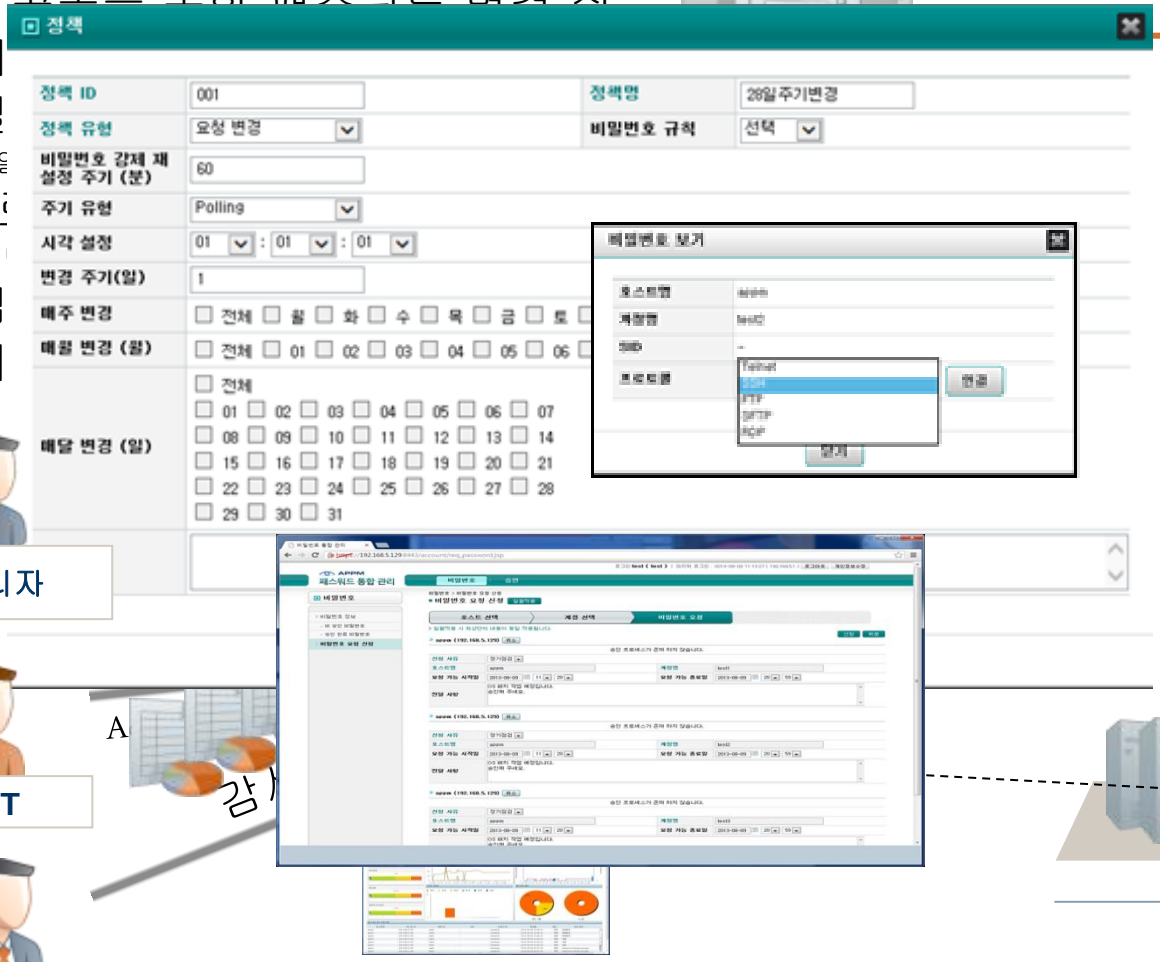
보안 관리자



IT



감사자





비밀번호변경 어댑터

시스템	계정	비밀번호
Unix	root	tops3cr3t
Oracle	SYS	tops3cr3t
Windows	Administrator	tops3cr3t
Firewall	admin	tops3cr3t
Cisco	enable	tops3cr3t



비밀번호 관리 대상 시스템

시큐어가드테크놀로지, 일방향 암호화 특허 출원

발췌 : 대한민국 ICT의 새로운 창 IT DAILY

[아이티데일리] IT 보안 솔루션 전문 기업 시큐어가드테크놀러지(대표 방학재)는 통합 패스워드 관리 솔루션 'AAPM'의 일방향 암호화 기술을 특허 출원했다고 25일 밝혔다.

이번에 출원한 특허는 '정보통신망법 시행령 제15조 4항 1호'의 법규를 준수하는 일방향 암호화 기술이다.

일방향 암호화 기술이란 여타 패스워드 관리 솔루션이 간과하고 있는 두 가지 상황, ▲시스템 접근을 위해 접속 계정의 비밀번호를 관리 서버 내부에 저장하고 ▲비밀번호 발급을 위해 서버 계정의 비밀번호를 데이터베이스 내부에 저장하는 상황에서 비밀번호를 남기지 않는 기술이다.

한편, 해당 기술이 적용된 시큐어가드테크놀러지의 APPM은 ▲최고 권한 계정의 비밀번호를 주기적, 일괄적으로 변경, 관리하고 ▲승인관리를 통해 권한이 부여된 사용자에게 비밀번호를 자동으로 생성, 발급하는 통합 패스워드 관리 솔루션이다.

APPM의 특징은 ▲비밀번호 변경 실패 작업에 대한 검증 프로세스 및 ▲논리적, 물리적 장애 시에도 비밀번호를 빠르고 안전하게 복원해 사용할 수 있는 백업 기능이다. 특히 APPM의 백업 기능은 '3차 이동식 저장매체 백업' 방식으로 해당 기술 역시 특허 출원돼 있다.

최고 권한 계정 패스워드 관리

(No Agent install !)

비밀번호 관리 솔루션 기능

- 다양한 관리 대상 시스템
- 갖추어야 할 자체 보안 기능
- 장애 대응 방안 – 3차 백업

다양한 관리 대상 시스템

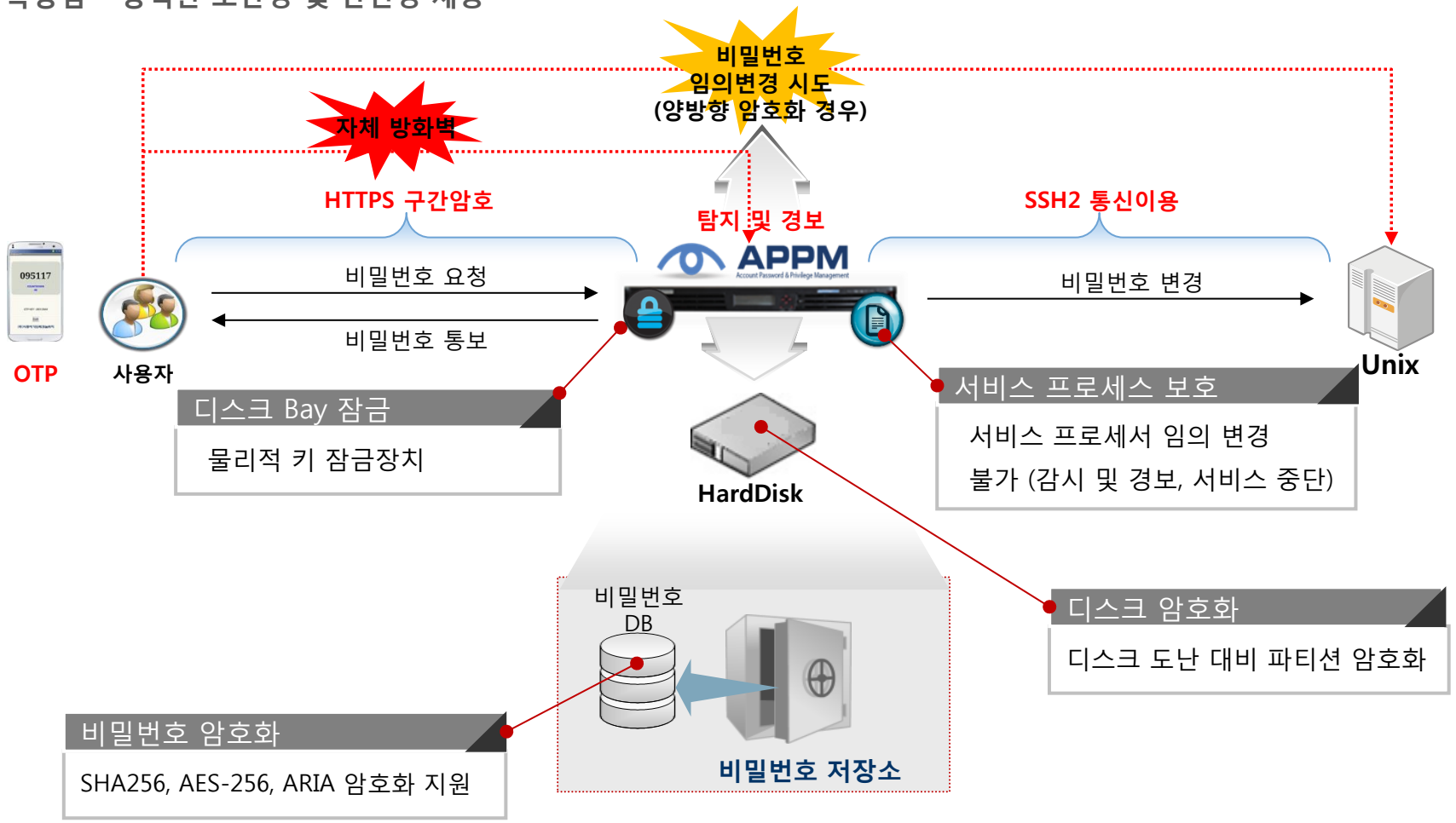
APPM
Automated Process Policy Management

일회용 비밀번호 관리는 에이전트 설치 없이 Agent-Less 기반으로 다양한 서버 및 데이터베이스, In-House 어플리케이션에 대한 패스워드 변경 기능을 제공 합니다.



물리적 / 논리적 강력한 보안성 및 안전성 제공

■ 특장점 – 강력한 보안성 및 안전성 제공



[특허출원] 3차 백업을 통한 안전한 비밀번호 관리 및 복구 방안 제공



3 장애 발생

Active & Standby
비밀번호 관리 시스템
장애

4 USB 회수





5 복호화키 USB 회수

NH농협은행 금고에 저장되어 있는 복호화키 USB 회수



6 지정 PC 복호화

별도의 지정된 관리PC에서 어플리케이션을 통해 접근 후 복호화키 및 저장된 비밀번호 복호화

7 시스템 접속

비밀번호 관리 시스템 복구 전까지 관리 대상 시스템에 접속이 필요한 경우 복호화 된 비밀번호를 이용하여 접속

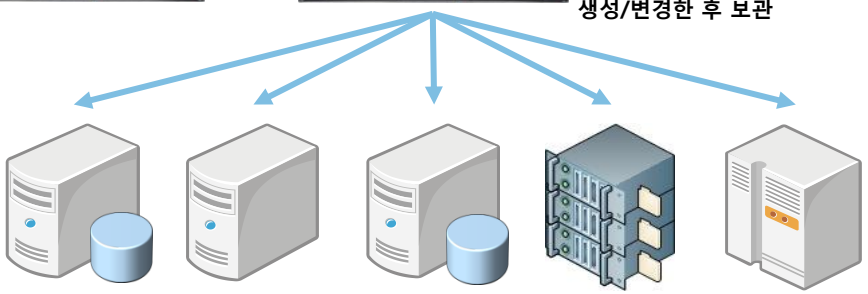
2 비밀번호 실시간 백업

비밀번호 관리 시스템에 USB 이동 저장 매체를 설치하여 실시간으로 비밀번호를 3차 백업

1 비밀번호 관리 시스템

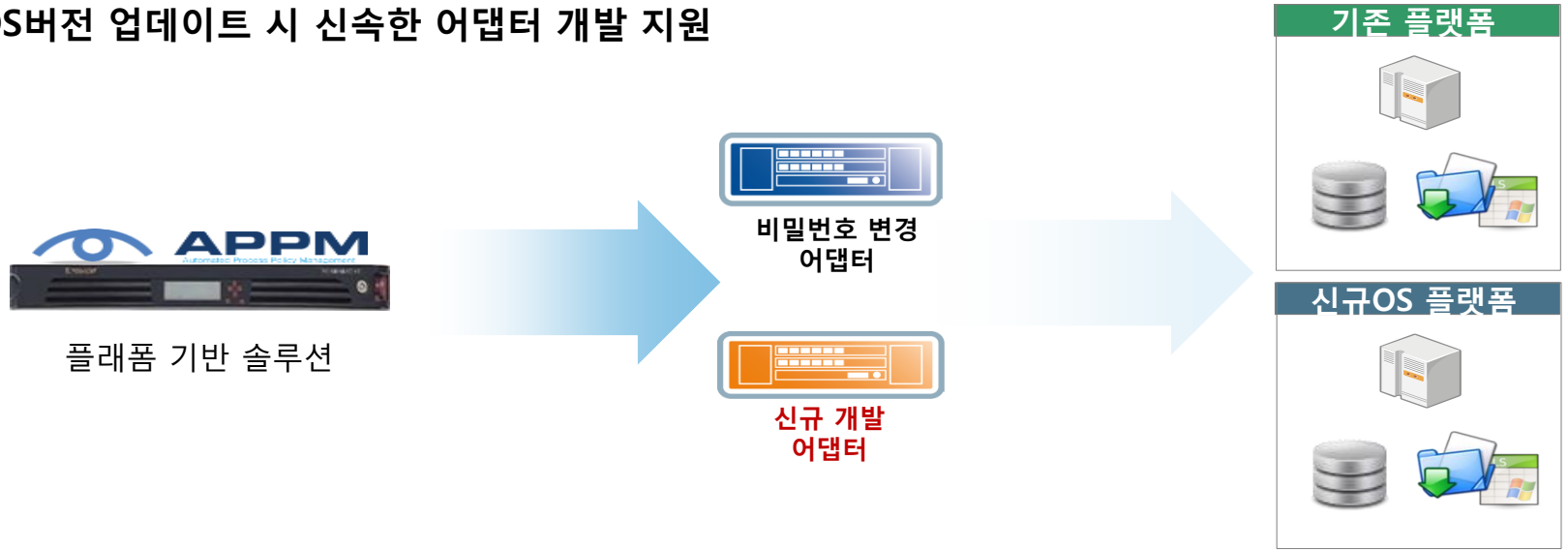
비밀번호 관리 시스템은 관리 대상 시스템의 주요 계정에 대한 비밀번호를 생성/변경한 후 보관

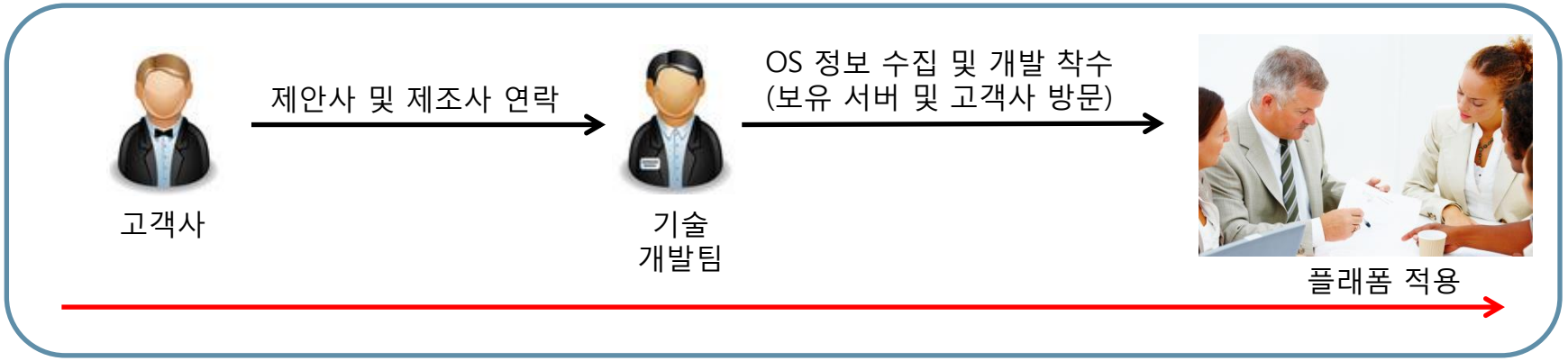




비밀번호 관리 대상 시스템

신규 OS버전 업데이트 시 신속한 어댑터 개발 지원





최고 권한 계정 패스워드 관리

(No Agent install !)

하드 코딩된 비밀번호 관리 방안

- 다중 PUSH 방식을 이용한 비밀번호 관리
- PULL 방식을 이용한 비밀번호 관리

하드코딩 된 비밀번호 관리방안

APPM
Automated Process Policy Management

- **PUSH 기능**
  - Agent-Less 기반으로 동작
  - 파일 형태로 존재하는 환경 파일 내의 패스워드 제거 기능 제공
  - 하나 혹은 하나 이상의 다중 서버에 대한 패스워드 Sync 기능 제공
  - Push 성공/실패에 대한 모니터링 및 경보 기능 제공

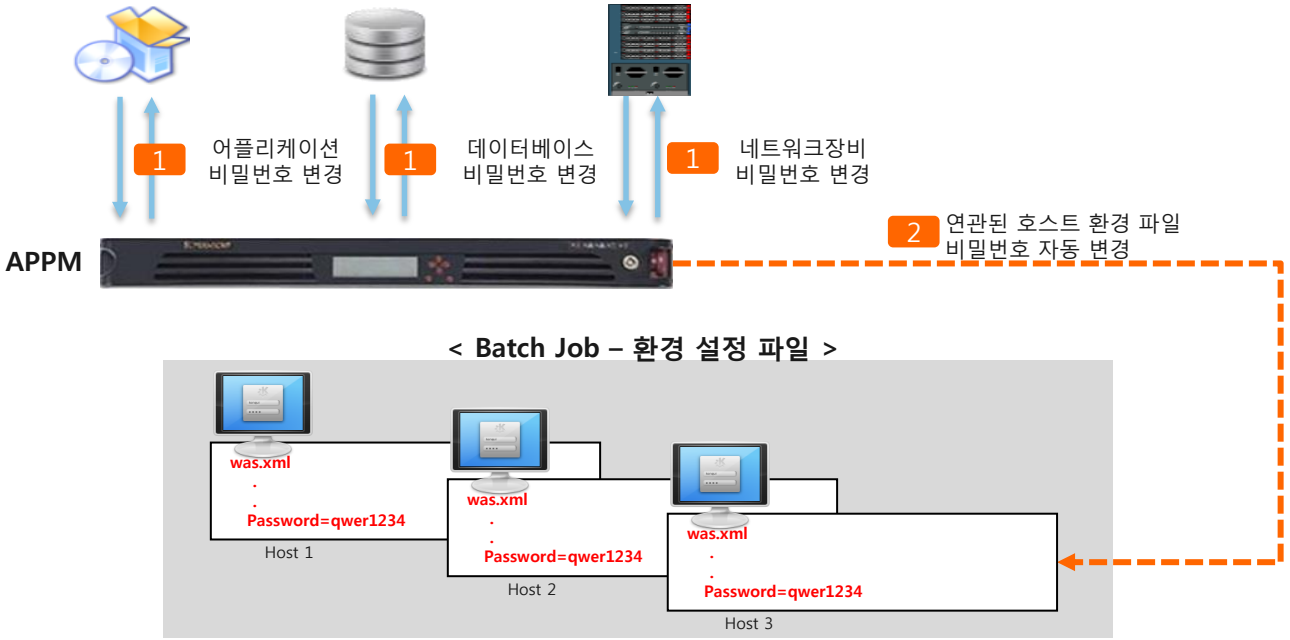
- **PULL 기능**
  - 호스트에서 APPM에게 패스워드를 요청 방식
  - 스크립트 내에 패스워드 직접 코딩 방지 - 제거 및 사용 후 자동 Reset
  - 요청 스크립트에 대한 무결성 체크
  - 패스워드 자동 변경을 위한 다양한 API 제공
    - Unix/Linux/Windows CLI
    - C Sheared Library, VC++ DLL
    - JAVA API

하드코딩 된 비밀번호 관리방안 - 다중 PUSH 제공

❖ **목적 : Agent 설치 없이 원본 계정의 패스워드 변경 시 APPM 서버가 자동으로 대상 환경 파일의 패스워드를 Update해 줍니다.**

❖ **특징**

- 변경 대상은 하나 혹은 하나 이상의 다중 서버 지원
- 환경 파일(.inf, .xml, .conf 등) 형태 지원 뿐만 아니라 명령어 형태(Web Logic 등)로 실행되는 형태도 지원
- 모든 PUSH 처리 현황을 실시간으로 모니터링 하고 문제 발생시 경보 처리 함



PUSH 기능

- Agent-Less 기반으로 동작
- 파일 형태로 존재하는 환경 파일 내의 비밀번호 제거 기능 제공
- 하나 혹은 하나 이상의 다중 서버에 대한 비밀번호 Sync 기능 제공
- Push 성공/실패에 대한 모니터링 및 경보 기능 제공

※ 신규장비 연동 시 수 시간 (약 3시간) 이내 연동 적용 가능

하드코딩 된 비밀번호 관리방안 - API 혹은 CLI 기반의 PULL 방식 제공

❖ **목적 : 배치 스크립트 및 소스 코드 내부에 사용중인 하드코딩 된 패스워드를 제거**

❖ **API 지원 방식**

- Unix/Linux CLI 제공 / Unix/Linux Shared Library 제공
- Windows dll Library 제공 / Java Class Library 제공

❖ **특징**

- API(혹은 CLI)에서 요청한 패스워드는 지정된 시간 후 자동으로 다른 패스워드로 초기화 됨(옵션)
- API(혹은 CLI)를 요청한 부모 스크립트의 무결성 체크 기능 제공



PULL 기능

- 호스트에서 APPM에게 비밀번호를 요청 방식
- 스크립트 내에 비밀번호 직접 코딩 방지 - 제거 및 사용 후 자동 Reset
- 스크립트에 대한 무결성 체크
- 비밀번호 자동 변경을 위한 다양한 API 제공

※ 신규장비 연동 시 수 시간 (약 3시간) 이내 연동 적용 가능

최고 권한 계정 패스워드 관리

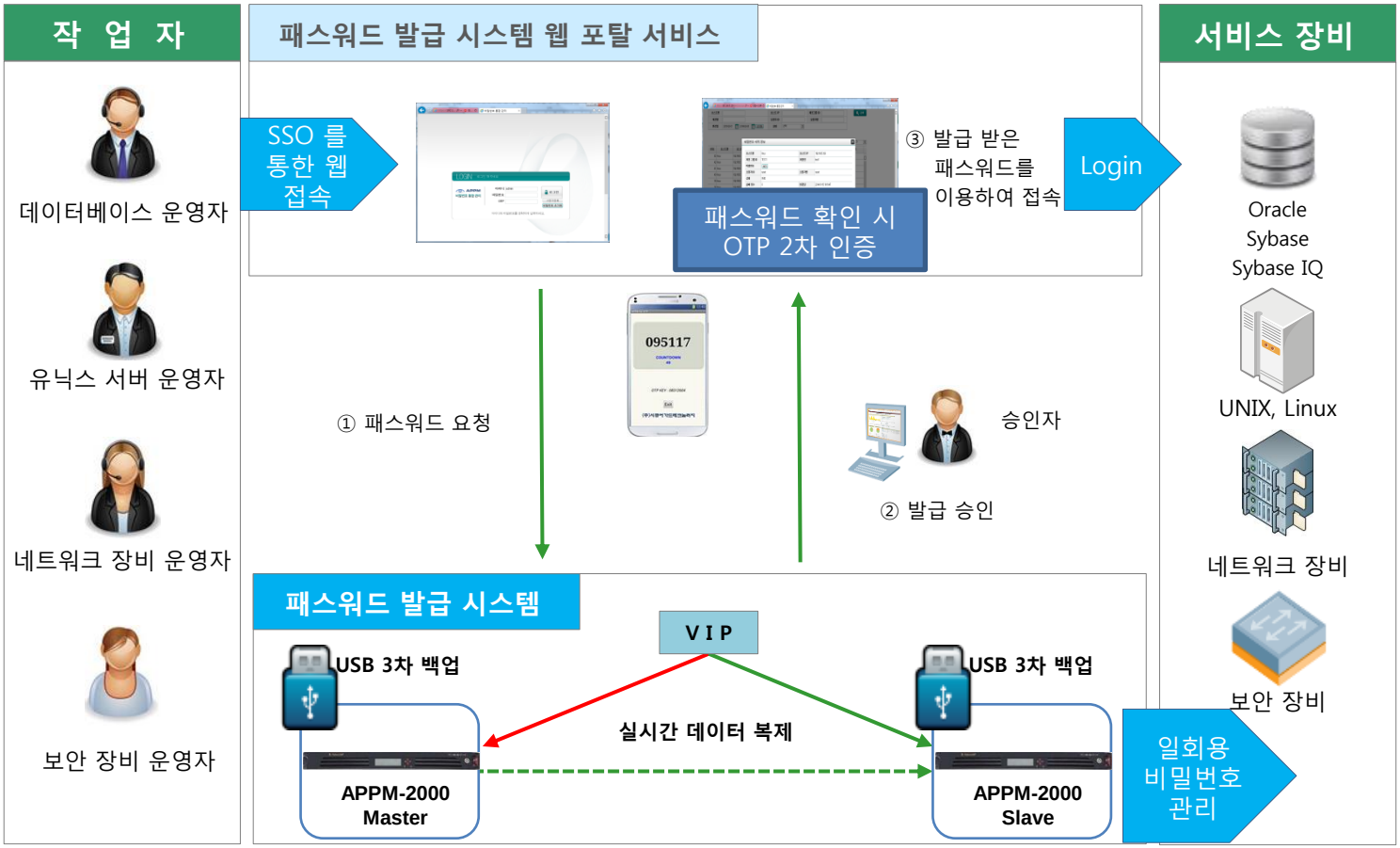
(No Agent install !)

구축 사례

- oo 은행
- oo 은행
- oo 감독원
- oo 전자 글로벌

구축사례 – oo 은행

oo은행은 유닉스 운영 서버, 네트워크 장비, 보안 장비, 데이터베이스를 포함한 모든 주요 장비의 비밀 번호 관리 서비스를 APPM을 통해 운영하고 있습니다.

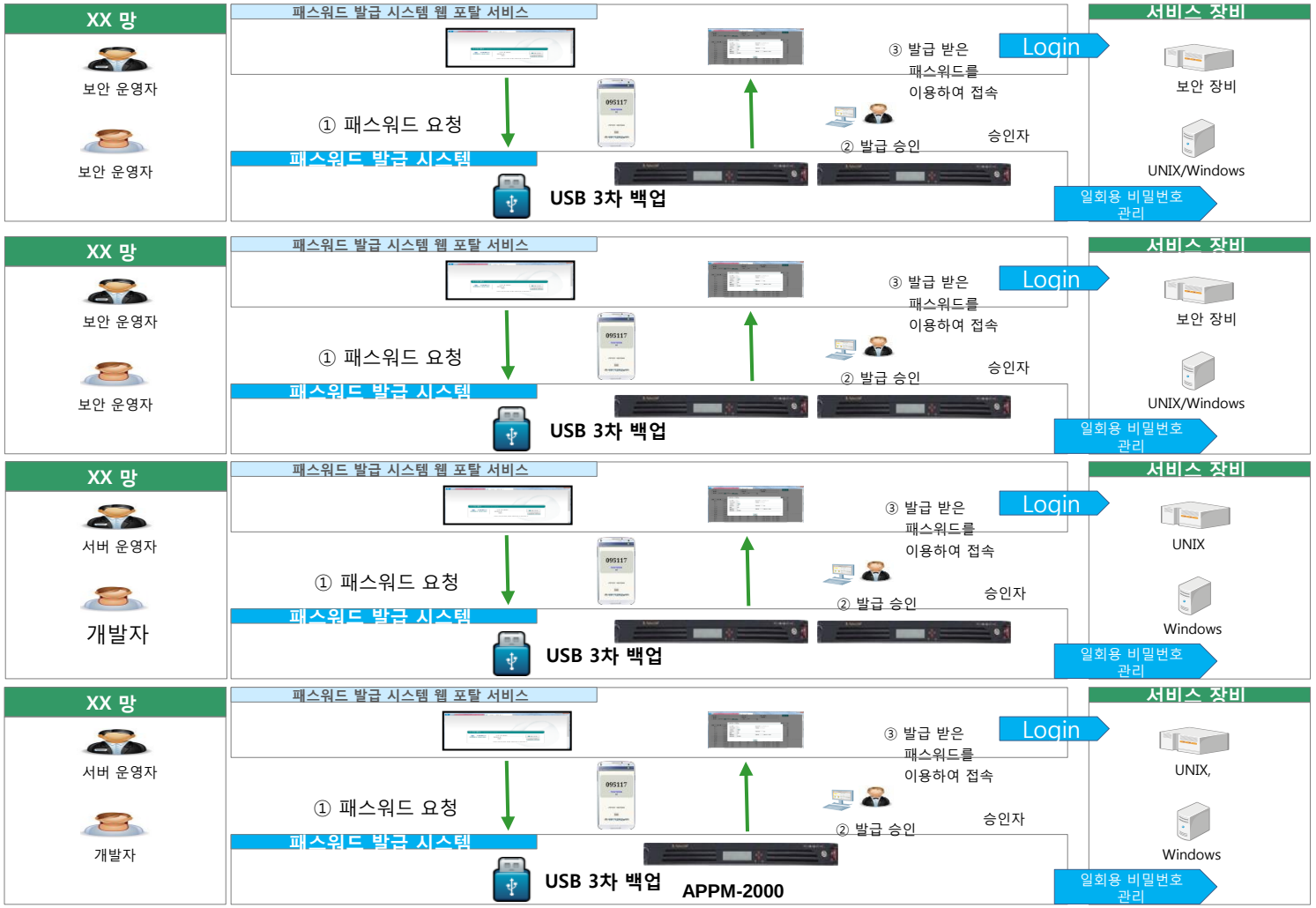


- 대상 주요 장비 OOO 여대-RDBMS 포함
- 대상 계정 수 OOOO 여개
- 1일 패스워드 발급 건수 약 OOOO~OOOO 여건 발급
- SSO를 통한 APPM 웹 자동 로그인
- 패스워드 불출 시 OTP 2차 인증
- 비 승인(직원), 승인(외주), 사후 승인 워크플로우 정책 혼합 사용
- 요청 변경, 정책 사용

구분	운영 플랫폼
서버	Solaris, HP-UX, AIX, Linux
데이터 베이스	Oracle, Sybase, Sybase IQ
네트워크 장비 및 보안 장비	Cisco, AVAYA , BROCADE, ERS5200, ERS8600, MF2-2000,SNIPER-DDX, SNXG400, NXG100V

구축사례 – OO 은행

OO 은행은 유닉스 운영 서버, 보안 장비를 포함한 주요 장비의 비밀 번호 관리 서비스를 APPM을 통해 운영하고 있습니다.
보안팀의 경우 보안 장비에 대한 일회용 비밀번호 관리를 위해 별도로 APPM 서버를 운영하고 있습니다.



국내 유일 '정보통신망 법 15조' 일방향 암호화 정책 준수 Reference



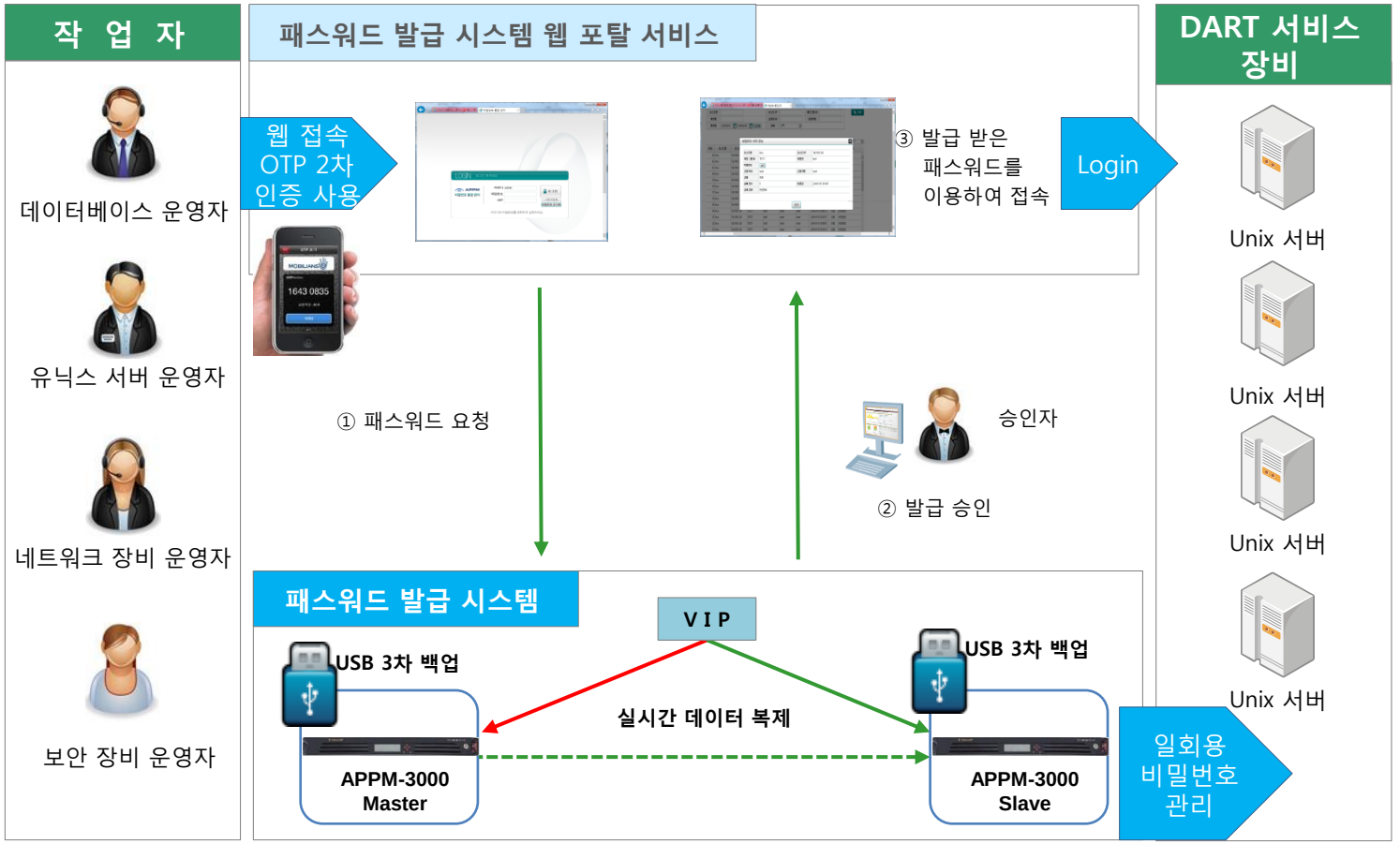
※ 비밀번호 미저장

- APPM 2000 7대 운영
- 대상 주요 장비 000 여대
  - 유닉스, 서버
  - 윈도우 서버
  - 방화벽
  - 보안 장비
- 시큐어가드테크놀러지 OTP 사용

구분	운영 플랫폼
서버	Solaris, HP-UX, AIX, Linux, Windows
보안 장비	방화벽 PC 보안, 무선보안, IPS, IDS,

구축사례 – oo 감독원

oo 감독원은 DART 서비스의 운영 장비에 대하여 비밀 번호 관리 서비스를 APPM을 통해 운영하고 있습니다.

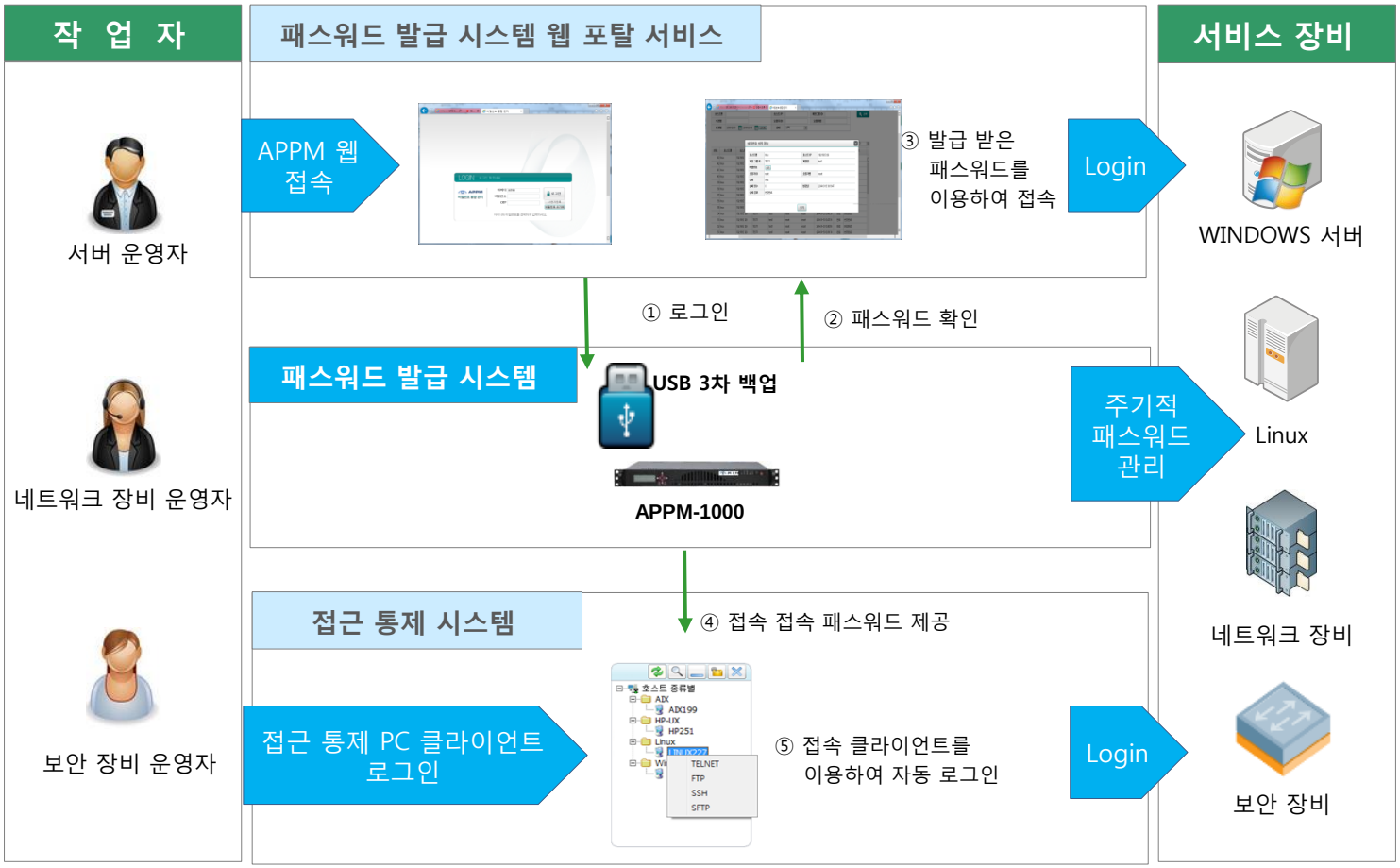


- 대상 장비 OO 대
- 대상 계정 수 OO 개
- 모든 계정에 대해 워크플로우 정책을 통해 패스워드 발급
- APPM 웹 콘솔 로그인 시 OTP 2차 로그인
- 워크플로우와 SMS(외주직원), 메신저(내부직원) 연동
- USB 3차 백업
- 요청 변경 정책 사용

구분	운영 플랫폼
서버	AIX

구축사례 – oo 전자 글로벌

oo 전자 글로벌은 대규모 네트워크 장비에 대한 패스워드 관리를 APPM을 통해 운영하고 있습니다.



- 윈도우, 리눅스 OOO여대
- 네트워크 장비 OOO 여대
- USB 3 차 백업
- 주기적 변경 정책 사용
- 접근 통제 클라이언트를 통한 자동 로그인 기능 사용

구분	운영 플랫폼
서버	Windows 2000, 2003, 2008, Linux
네트워크 장비 및 보안 장비	Cisco, Alteon, AVAYA , BROCADE, Astro, Motorola, Optowiz, Secui, Handreamnet, Snxg400, Subgate, via scope, Windows

레퍼런스

▶ 금융권 레퍼런스

하나은행 | NH농협 | Sh 수협은행 | SMART BANK KEB 외환은행

KED 한국기업데이터 Korea Enterprise Data | 금융감독원 | 신영증권 | 하나캐피탈

현대해상화재보험 | 여신금융협회 THE CREDIT FINANCE ASSOCIATION | AXA 다이렉트 redefining / standards | 수호천사동양생명

HF 한국주택금융공사 | HanaSKCard | IBK기업은행 금융그룹 IBK캐피탈 | KB 국민카드

▶ 기타

SAMSUNG | 공무원연금공단 | 한국소비자원 Korea Consumer Agency | 국민건강보험 일산병원 National Health Insurance Service Ilsan Hospital

LG U+ | NFRI 국가핵융합연구소 National Fusion Research Institute

감사합니다..

GiT 굿모닝아이텍(주) joinusbiz 조인어스비즈

굿모닝아이텍[주]
연락처 : 02-3775-2349
E-mail : gitsales@goodmit.co.kr, www.goodmit.co.kr

