



Powerful Solution for DATABASE & SYSTEM Security
DBSAFER Enterprise V5.0 표준제안서



C O N T E N T S

I. 제안 개요

1. DBSAFER Enterprise 도입의 필요성

II. 솔루션 소개

1. DBSAFER Enterprise 솔루션 개요

2. DB접근제어 기능

3. SYSTEM접근제어 기능

4. 통합계정관리 기능

5. 특징점

III. 회사 소개

1. 일반현황 및 연혁

2. 품질인증

3. 레퍼런스

I. 제안 개요

1. DBSAFER Enterprise 도입의 필요성

DBSAFER Enterprise 솔루션 도입의 필요성

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

- G기업 1천만건 유출
- A기업 1천만건 유출
- 보안 침해 사고의 70~80%가 내부자에 의해서 발생

개인정보유출
사고 급증

보안 시스템
취약성

- DB/OS/Network 보안 만으로는 부족
- 우회경로를 통한 제어의 어려움
- 서버콘솔에 작업 시 보안 취약
- 사용자 계정 관리 기법의 부재



전문적인 DB, 시스템
접근제어 관리체계
필요

- 개인정보보호법 (2011.9.30. 시행)
 - 제9조 (접근권한, 인증 및 계정관리)
 - 제11조(접근제어) 네트워크, DB관련
- 정보통신망법 개정 : 기업의 정보보안관련 책임강화
- 개인정보보호 의무 위반한 업체에 배상명령 (개인정보분쟁위원회)

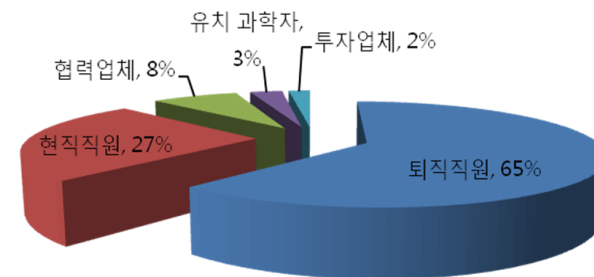
개인정보보호
법률 강화
[공공기관 / 기업]

금융감독원
[금융기관]

- 전자금융감독 시행세칙
 - 제9조(전산자료 보호대책) -3항
 - 제11조(해킹 방지대책) -8항
 - 제13조(홈페이지 등 공개용 서버 관리 대책)-3항



[개인정보 침해 건수 (방통위)]



[유출경로 (국가정보원)]

현황-관련 컴플라이언스 준수

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

■■■ 사업자의 개인정보 보호조치 기준 관련 법령 및 처벌조항 ■■■

정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙	사업자의 개인정보 보호조치 기준	처벌조항
제28조(개인정보의 보호조치) ① 정보통신서비스 제공자 등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정한 기준에 따라서 다음 각 호의 기술적·관리적 조치를 하여야 한다	제9조(개인정보의 보호조치) ① 법 제28조제항 및 제67조제항에 따른 개인정보의 안전성 확보에 필요한 관리적 조치는 다음 각 호와 같다. ② 법 제28조제항 및 제67조제항에 따른 개인정보의 안전성 확보에 필요한 기술적 조치는 다음 각 호와 같다. ③ 행정안전부장관은 업종별 특성을 반영하여 제1항 및 제2항 각 호에 따른 보호조치의 구체적인 기준을 정하여 고시할 수 있다.	제2조(정의) 제2조(정의)	-
1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행	①-1. 개인정보의 안전한 취급을 위한 내부관리계획의 수립 및 시행 ①-2. 개인정보관리책임자의 의무와 책임을 규정한 내부 지침 마련	제3조(내부관리계획의 수립·시행) 제4조(개인정보관리책임자 및 취급자의 의무와 책임)	3천만원 이하의 과태료
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장비의 설치·운영	①-3. 개인정보의 안전한 보관을 위한 잠금장치 등 물리적 접근방지 조치 ②-1. 개인정보에 대한 접근 권한을 확인하기 위한 식별 및 인증 조치	제5조(물리적 접근 제한) 제8조(접근 권한, 인증 및 계정관리)	2년 이하의 징역 또는 1천만원 이하의 벌금
3. 접속기록의 위조·변조 방지를 위한 조치	②-3. 접속기록의 위조·변조 방지를 위한 조치	제11조(접속기록의 위·변조방지)	2년 이하의 징역 또는 1천만원 이하의 벌금
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술 등을 이용한 보안조치	②-2. 개인정보에 대한 권한 없는 접근을 차단하기 위한 암호화와 방화벽 설치 등의 조치	제9조(개인정보의 암호화) 제10조(접근통제)	2년 이하의 징역 또는 1천만원 이하의 벌금
5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치	②-4. 침해사고 방지를 위한 보안프로그램의 설치 및 운영	제12조(보안 프로그램의 설치 및 운영)	2년 이하의 징역 또는 1천만원 이하의 벌금
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호 조치	①-4. 개인정보보호를 위한 정기적인 자체 감사 실시 ①-5. 그 밖에 개인정보의 안전성 확보에 필요한 관리적 보호조치 ②-5. 그 밖에 개인정보의 안전성 확보에 필요한 기술적 보호조치	제6조(정기적 자체 감사) 제7조(출력·복사시 보호조치)	3천만원 이하의 과태료 권고사항

✓ 개인정보보호법

✓ 주식회사 등의 외부감사에 관한 법률

✓ 정보통신망법

✓ 금융감독원 IT감사모범규준

✓ 상장사 IT회계감사

✓ 전자정부 정보보호관리체계 인증지침

✓ ISO 27001 (정보 보안 관리 시스템 인증)

✓ ISMS (정보보호관리체계)

✓ PIPL (개인정보보호 인증제)

✓ PCIDSS (Protect Card Industry Data Security Standard)

컴플라이언스 준수 주요기능

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

관련 기능	관련 법규	제공기능 설명
DB가 아닌 시스템 전체 보안	<p>개인정보보호법 안전성확보조치 기준 제6조 개인정보처리시스템에 대한 접근제어 시스템 설치 및 운영</p> <p>정보통신망 이용촉진 및 정보보호등에 관한 법률 제28조 정보시스템 개인정보의 보호조치</p> <p>방송통신위원회 훈령 제58호 - 방송통신위원회 정보보호 관리지침 제18조 정보시스템 보안관리</p> <p>방송통신위원회 고시 개인정보의 기술적, 관리적 보호조치 기준 제4조 개인정보처리시스템 접근제어</p> <p>신용정보의 이용 및 보호에 관한 법률 제19조 신용정보전산시스템의 안전보호</p> <p>주식회사 등의 외부감사에 관한 법률 제8조(내부회계관리제도의 운영 등) 회계정보를 기록·보관하는 장부를 관리하고 위조·변조·훼손 및 파기를 방지</p>	<p>통합접근제어 및 통합계정관리</p> <ul style="list-style-type: none"> • DB접근제어 • SYSTEM접근제어 • OS접근제어 • 통합계정관리(OS계정, DBMS계정) <p>(동종업계 유일 제공)</p>

컴플라이언스 준수 주요기능

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

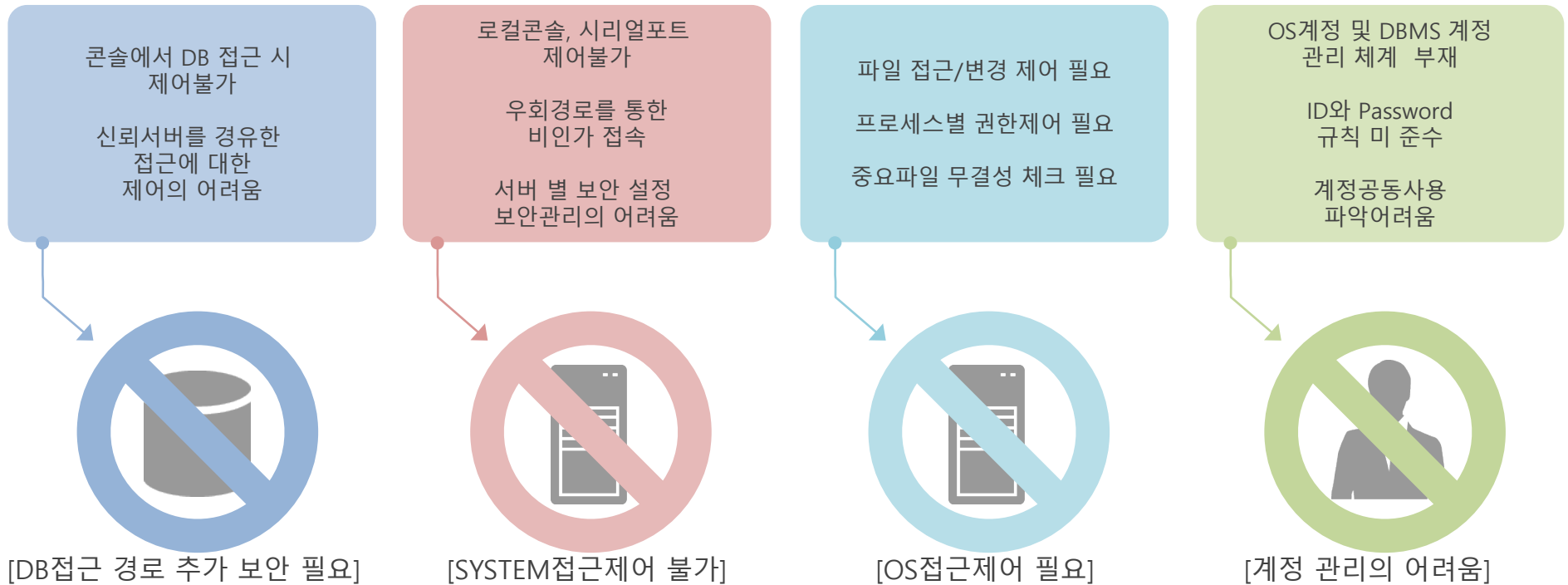
관련 기능	관련 법규	제공기능 설명
전체 통신구간 암호화	개인정보보호법 안전성확보조치 기준 7조 개인 정보의 암호화 (정보통신망으로 송수신시 암호화)	DBSAFER는 사용자 PC와 DBSAFER, DBSAFER와 보안 대상서버의 통신 전구간에 암호화 기능을 제공합니다. (동종업계 중 유일, 전구간 암호화제공)
접속 및 업무 전수기록	개인정보보호법 안전성확보조치 기준 8조 접속기록의 보관 및 위·변조방지 (개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 접속자를 알 수 있는 정보, 수행업무 등을 전자적으로 기록)	모든 DB에 대한 감사 기능은 물론이고, SYBASE IQ, MSSQL의 암호화된 세션정보도 ID,접속AP를 정확하게 로깅 (동종업계 일부 미제공 기능)
개인정보 위치 식별	개인정보보호법 안전성확보조치 기준 제4조 접근권한의 관리 제7조 개인 정보의 암호화 (개인정보 접근권한관리 및 암호화를 위한 식별)	DB를 스캔하여 개인정보의 위치를 식별 제공 및 DB접근제어 시스템과 연동하여 정책적용 기능 제공 (동종업계 일부 미제공 기능)
변경 전후 데이터 기록	전자금융감독규정 제27조 전산원장 제어 (변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용 기록)	DB를 스캔하여 개인정보의 위치를 식별 제공 및 DB접근제어 시스템과 연동하여 정책적용 기능 제공 (동종업계 일부 미제공 기능)
개인정보 표시제한	「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 “개인정보의 기술적, 관리적 보호조치 기준” 제9조(개인정보 표시 제한 보호조치)	개인정보를 마스킹하여 표시제한 조치 기능을 제공
회계정보 접근통제 및 이력관리	주식회사 등의 외부감사에 관한 법률 제8조(내부회계관리제도의 운영 등) 회계정보를 기록·보관하는 장부를 관리하고 위조·변조·훼손 및 파기를 방지	OS접근제어를 통해 회계정보 파일로의 접근통제 및 이력관리 기능을 제공

현황-서버 운용 시 보안 취약점 내재

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

DB에 접근하여 데이터에 접근하는 경로는 다양하다. DB서버의 포트에 직접 접속하여 접근할 수도 있지만 DB서버의 OS영역의 다른 포트를 통해서도 접근이 가능하며, 네트워크를 경유하지 않고 서버실에 직접 들어가서 콘솔에서 로그인하여 가져갈 수도 있다.

DB포트로 직접 접근하는 것은 대부분의 DB접근제어솔루션에서 제공을 하고 있다. 하지만 그 외에 콘솔로 접근하거나 윈도우터미널 서비스 등을 통해 접근하는 다른 다양한 경로에 대해서도 접근제어가 필요하다. 또한 체계적이고 완벽한 접근 제어를 위해서는 접근에 사용되는 OS계정 및 DBMS계정에 대한 관리와 암호규칙 강제화 등 계정에 대한 관리가 필요하다.

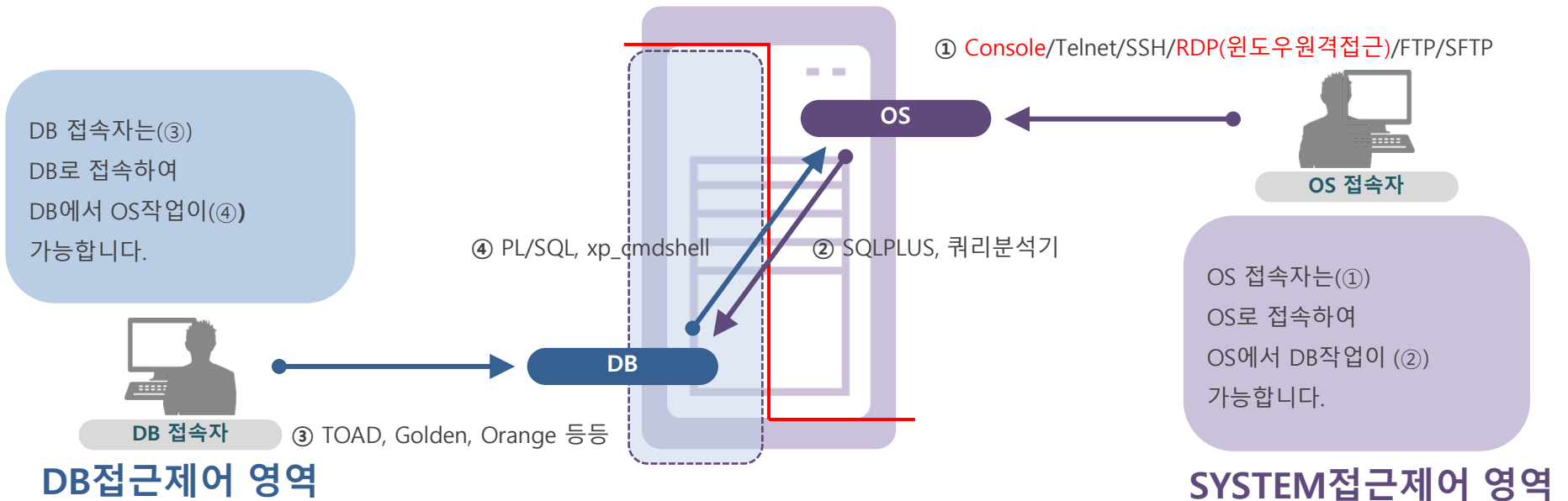


DB와 시스템(OS)은 분리가 불가능

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

DB접근제어 솔루션은 DB 작업을 감사/제어하고 SYSTEM접근제어 솔루션은 OS작업을 감사/제어합니다. 문제는 DB로 접근해서 OS명령어를 실행할 수 있고, OS로 접근하여 DB작업을 할 수 있어 DB작업과 시스템작업을 분리할 수 없는 것 입니다. 하지만 솔루션은 DB접근제어와 시스템접근제어 솔루션으로 분리되어 각자의 영역만 보호하고 있어서 문제가 발생합니다.

DB와 시스템(OS)작업은 분리가 불가능한데 솔루션은 DB접근제어/SYSTEM접근제어 솔루션으로 나뉘어서 각자의 영역만 보호함

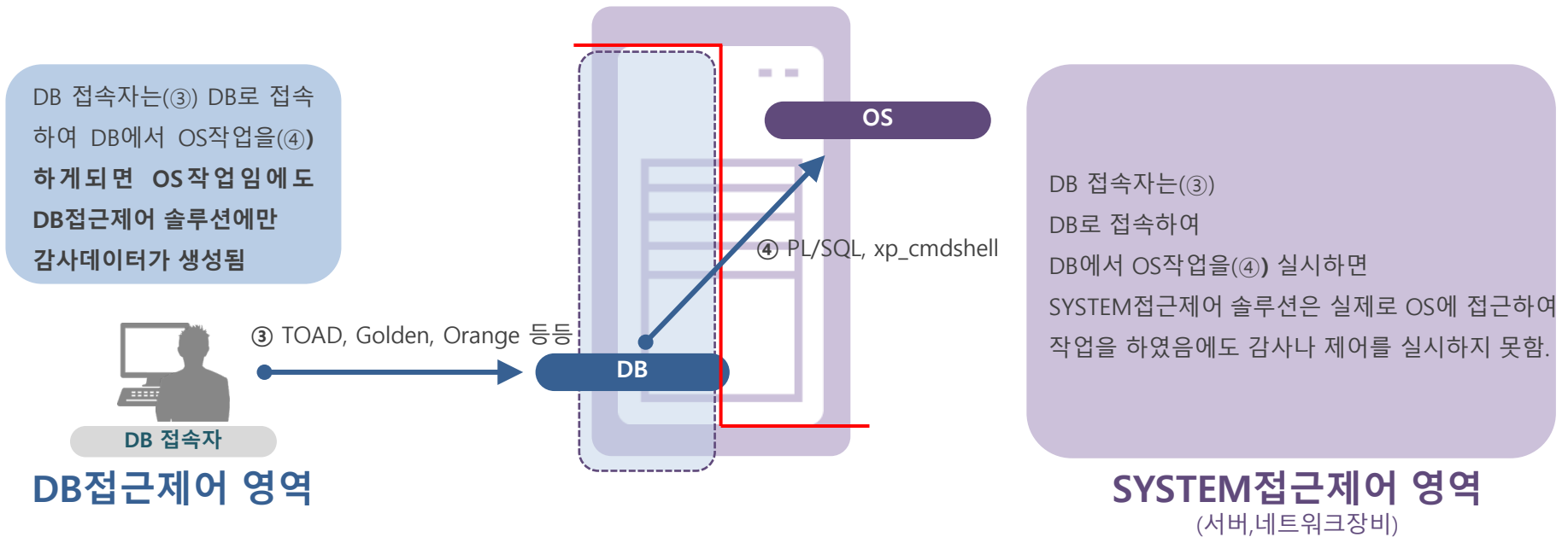


기술적 문제로 DB접근제어와 SYSTEM접근제어로 분산되어 운영

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

OS에서 실행되는 명령들은 SYSTEM접근제어 솔루션에서 감사/통제되는데 DB로 접근하여 OS명령어를 실행하면 SYSTEM접근제어 솔루션이 인지하지 못하여 감사와 제어가 되지 않는 문제가 발생합니다. 이와 반대로 OS에 접근하여 DB로 접근하면 DB접근제어 시스템에서 인지하는 못하는 문제가 발생합니다. 이 같이 하나의 문제점을 기술적인 이유로 2개의 솔루션을 사용하여 풀고 있기 때문에 발생하는 기술적인 문제입니다.

OS작업인데도 불구하고 SYSTEM접근제어 솔루션에서 감사/통제가 되지 않음(OS를 통한 DB작업도 동일한 문제 발생)

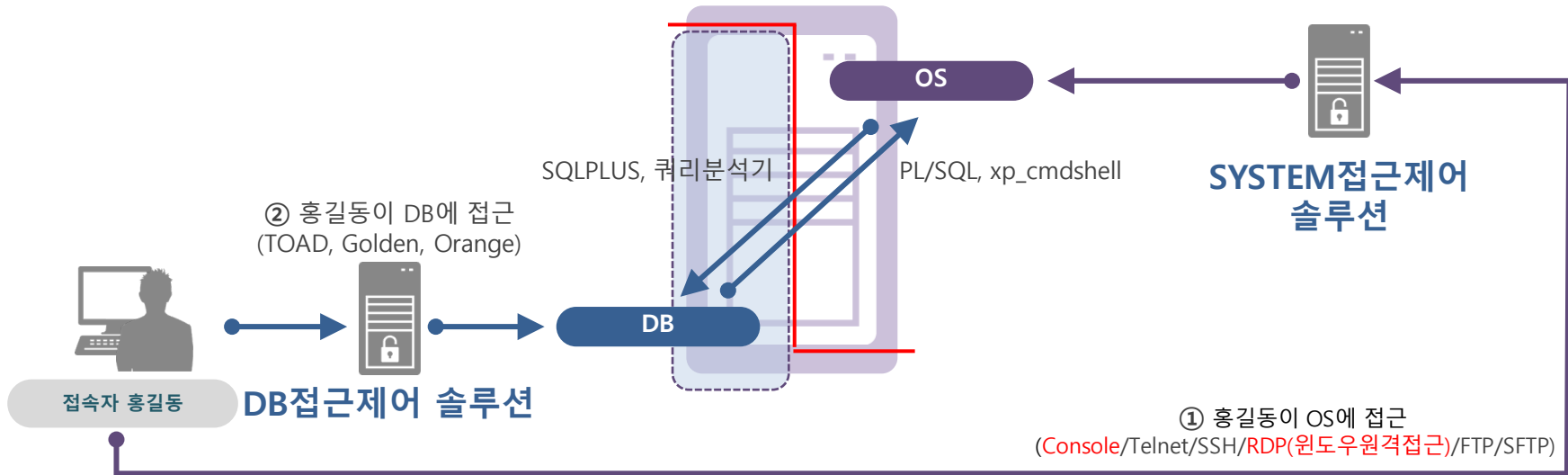


분리 운영으로 "2번 인증/로그분산/보안정책 2중관리"의 문제점 발생

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

DB와 SYSTEM접근제어 솔루션을 각각 운영하기 때문에 발생하는 대표적인 문제는 동일한 사용자가 DB로 접근하면서 인증을 받았어도 OS로 접근하면 또 인증을 받아야 하는 것과 동일한 사용자가 OS작업을 하였어도 DB로 접근했느냐 OS로 접근했느냐에 따라서 로그가 저장된 위치와 실제 적용되는 보안정책이 달라지는 심각한 문제를 가질 수 있습니다.

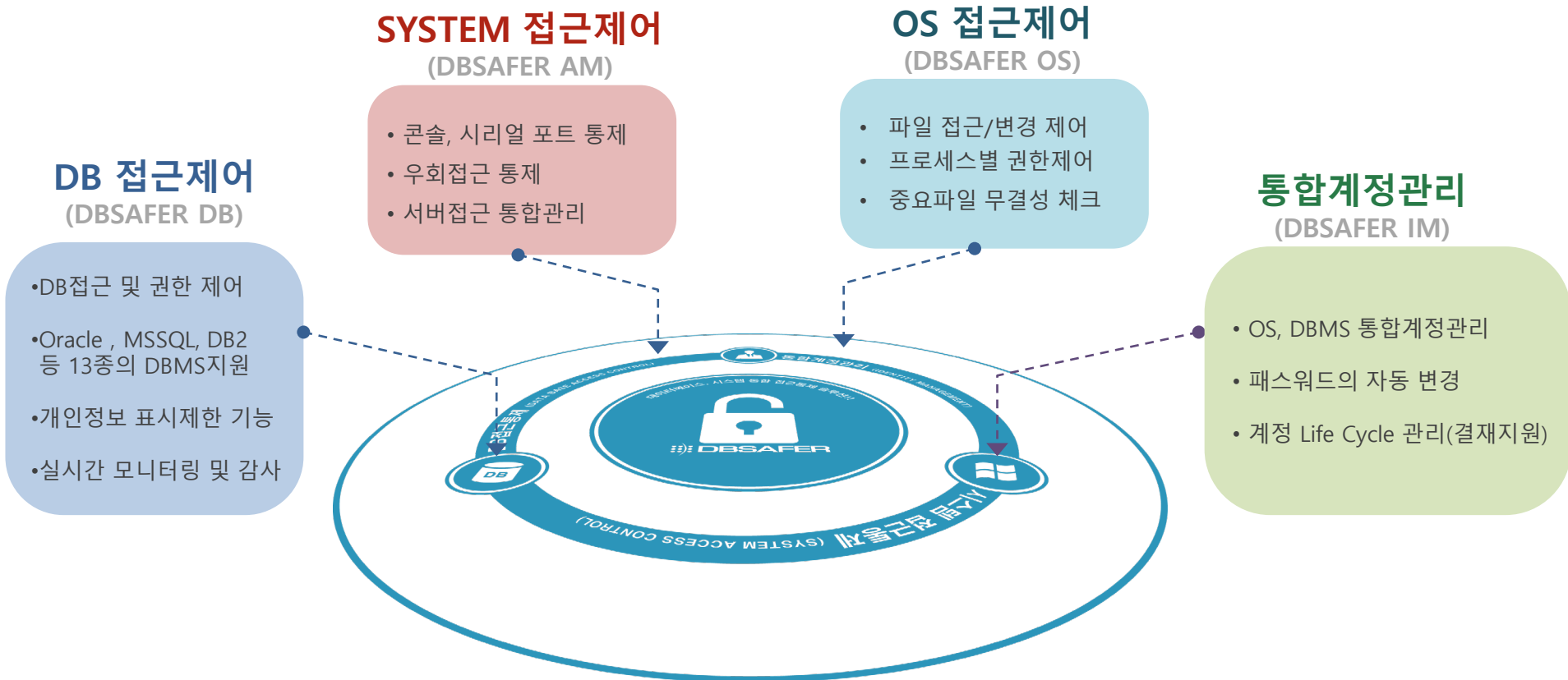
문제점	상세 내용
DB접근제어/SYSTEM접근제어 각각 2번 인증	· 홍길동이 DB(②)에 접근하기 위해서 DB접근제어에서 인증을 받았어도 OS(①)에 접근하기 위해서 또 인증을 받아야 함
2개의 솔루션에 로그가 분리되어 저장	· OS작업 로그임에도 SYSTEM접근제어가 아닌 DB접근제어 솔루션에 로그가 저장되어 있는 경우가 발생 함 (② 번으로 접속) · DB작업 로그임에도 DB접근제어가 아닌 SYSTEM접근제어 솔루션에 로그가 저장되어 있는 경우가 발생 함 (① 번으로 접속)
홍길동 한 명에게 2개의 보안정책 설정 필요	· DB로 접근하는 경우 DB접근제어 솔루션에 보안정책 설정 · 시스템으로 접근하는 경우 SYSTEM접근제어 솔루션에 보안정책 설정



DBSAFER를 이용한 All-in-One 접근제어 [DB, OS작업 감사/제어]

1. DBSAFER Enterprise 도입의 필요성 / I. 제안 개요

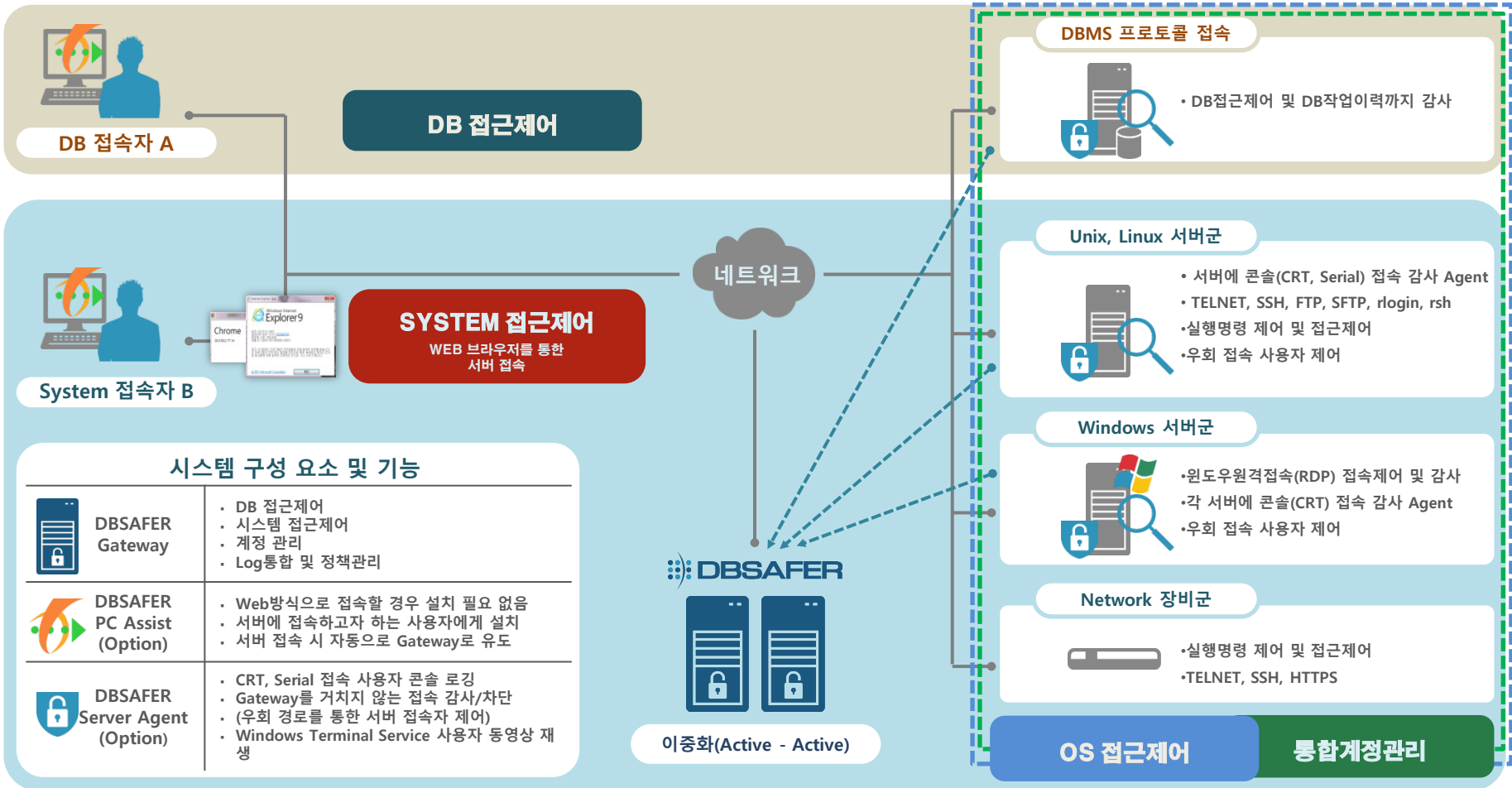
DBSAFER Enterprise는 서버에 대한 다양한 접근경로를 제어 및 감시를 수행하고 사용자 계정을 관리하여 **DB접근제어**, **SYSTEM접근제어**, **OS접근제어**, **통합계정관리**가 통합된 보안환경을 제공한다.



II. 솔루션 소개

1. DBSAFER Enterprise 솔루션 개요
2. DB접근제어 기능
3. SYSTEM접근제어 기능
4. 통합계정관리 기능
5. 특징점

DBSAFER Enterprise 전체 구성도 | 1. DBSAFER Enterprise 솔루션 개요 / II. 솔루션 소개



DBSAFER Enterprise 기능 개요

1. DBSAFER Enterprise 솔루션 개요 / II. 솔루션 소개

DBSAFER Enterprise는 DB접근제어, SYSTEM접근제어, 통합계정관리를 제공하며, 아래와 같이 주요 기능을 제공합니다.

DB접근제어 (DBSAFER DB)

- 다양한 DBMS에 대한 접근을 중앙 관리
- 접근제어 (사번, IP, Application, DB계정, 시간 등)
- 권한제어 (DDL/DML/DCL 구문, Table/Column 등)
- 데이터 마스킹 제공 (개인정보 표시제한 조치 기능)

SYSTEM 접근제어 (DBSAFER AM)

- 다양한 OS에 대한 접근을 중앙 관리
- 원격 접속 제어 및 로깅 (TELNET, SSH, RDP, FTP, SFTP)
- 로컬 콘솔 및 시리얼 관리 포트 보안
- 우회 접속 제어 및 시스템 로그 /자원 관리

OS 접근제어 (DBSAFER OS)

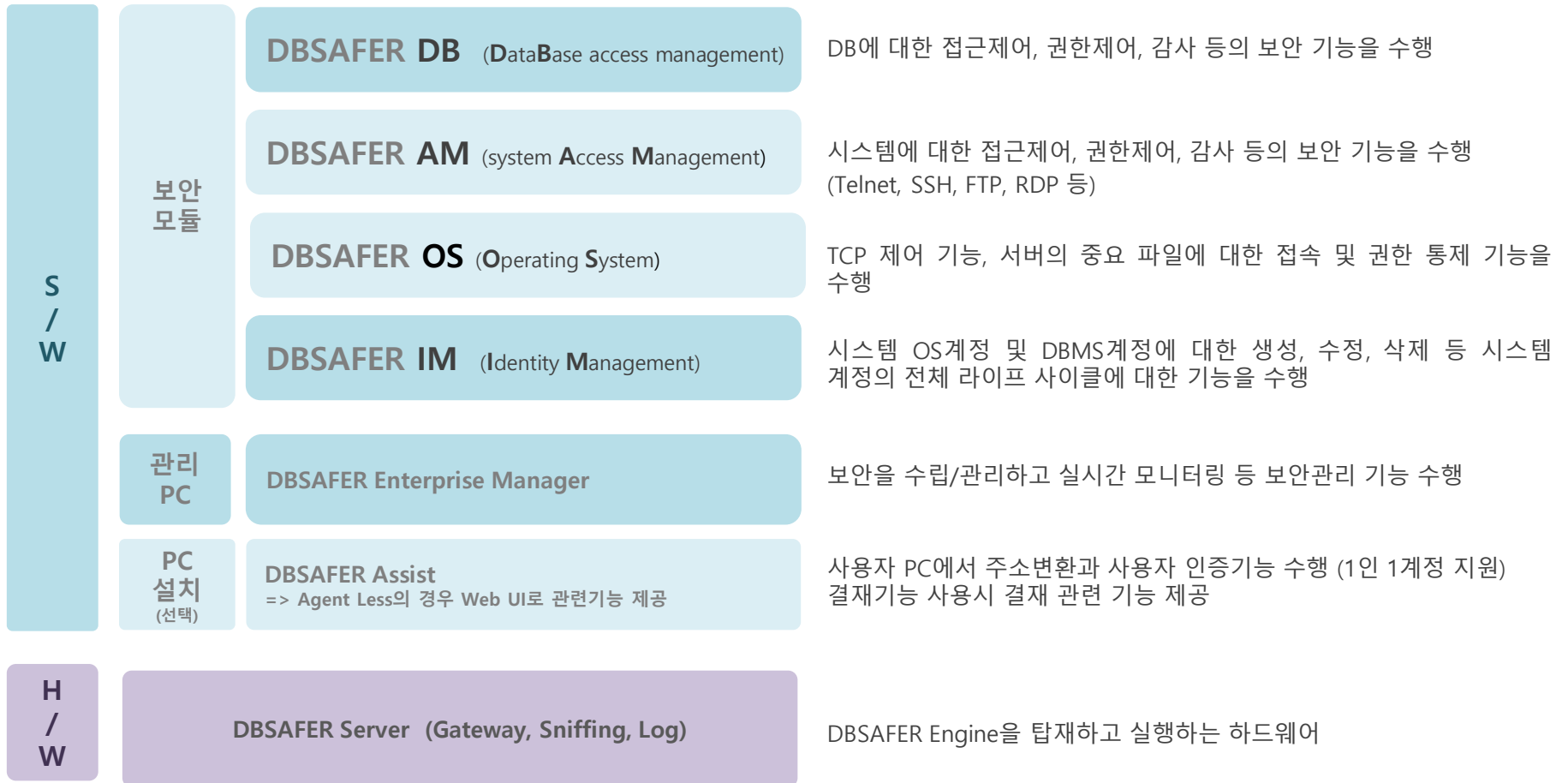
- 특정 디렉토리 또는 파일에 대한 접근을 통제
- 사용자별(IP 주소, 접속계정, 보안계정, 실행권한) 접근통제
- 포트 기반으로 인바운드/아웃바운드 통제
- 프로세스별 접근통제 기능을 제공
- 특정 디렉토리 또는 파일에 접근한 이력에 대해 감사로그 검색

통합 계정관리 (DBSAFER IM)

- 이기종의 OS와 DBMS에 존재하는 계정을 중앙 관리
- 비밀번호 자동 변경 및 계정 자동 수집
- 결재를 통한 계정 Life-Cycle 관리
- 유연한 비밀번호 정책 설정
- 다양한 DBMS 계정권한(Role) 관리

DBSAFER Enterprise 제품구성

1. DBSAFER Enterprise 솔루션 개요 / II. 솔루션 소개



DBSAFER Enterprise 라이선스 체계

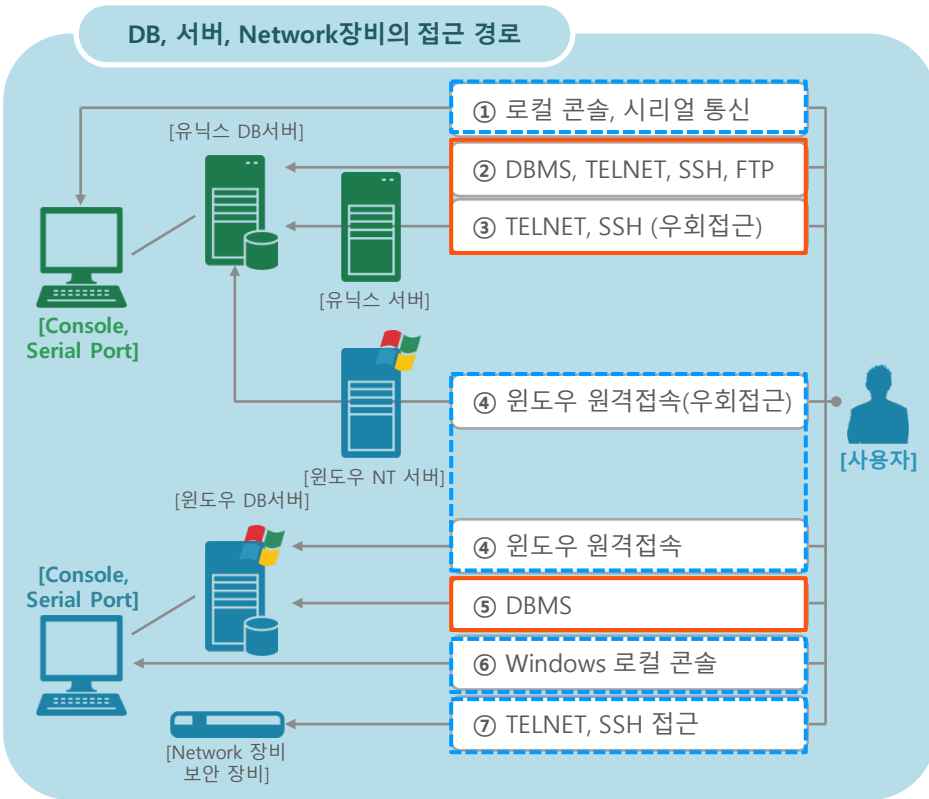
1. DBSAFER Enterprise 솔루션 개요 / II. 솔루션 소개

DBSAFER Enterprise는 DB접근제어, SYSTEM접근제어, 통합계정관리 부분에 대하여 각각 라이선스 정책을 가지고 있으며, 해당 기능을 사용하기 위해서는 각각의 라이선스를 구매하여야 합니다.

라이선스		설명 (라이선스 산정기준)
DBSAFER Enterprise Gateway License		장비에서 사용하는 DB, 시스템 접근제어 모듈에 대한 라이선스 (DBSAFER Enterprise 보안기능 H/W 당 필요)
DBSAFER DB License (DB 접근제어)	DBMS License	DB프로토콜로 DB에 접근할 경우 접근제어/감사/결재 기능 수행 (DB서버당 Core 개수)
	DMS License	DB프로토콜로 DB에 접근하여 DML을 수행할 경우 변경 전,후 데이터 관리 (DB서버당)
DBSAFER AM License (SYSTEM 접근제어)	Network License	DB, 일반서버, Network장비,보안장비 등에 Gateway 방식(PC NAT, Web GUI)으로 접근제어/감사/결재 기능 수행(OS당)
	Server License	DB서버, 일반서버에 설치하여 보안 게이트웨이와 서버 통신구간 암호화 보안 게이트웨이를 통과하지 않는 우회접속 차단 콘솔(모니터)에 직접 접근하는 사용자 접근제어/감사/결재 기능 수행(OS당)
DBSAFER OS License (OS 접근제어)		TCP제어 및 프로세스/파일 접근 및 권한제어 (OS당)
DBSAFER IM License (통합 계정관리)		이기종 서버, DB서버, Network장비에 대한 통합 계정관리 기능제공 (OS계정관리는 OS당, DBMS계정관리 DBMS인스턴스당 라이선스 필요)

서버 접근의 다양한 경로에 대한 감시 및 제어 | 1. DBSAFER Enterprise 솔루션 개요 / II. 솔루션 소개

개인정보보호법에서는 DB로의 접근을 제어 하는 것이 아닌 **개인정보 처리 시스템에 대하여 제어하도록** 되어 있습니다.
 DBSAFER Enterprise는 DB접근제어와 SYSTEM접근제어 기능을 통합한 통합접근제어 제품으로 DB,서버,Network장비로의 모든 접속에 대한 감사/제어 기능을 제공합니다.

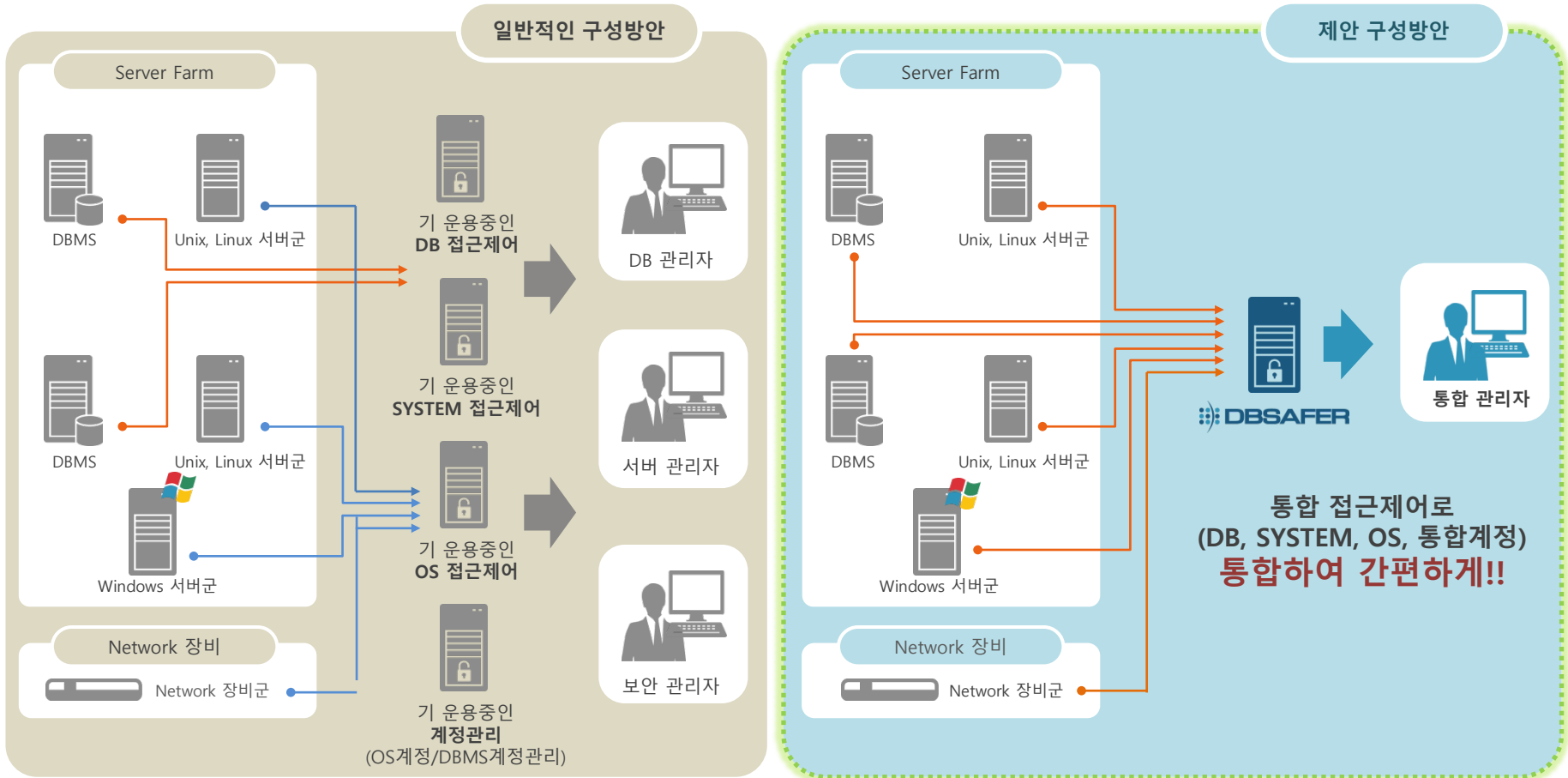


데이터 접근제어 영역		시스템 접근 제어 영역	
접속형태	내용		
① Console, Serial	· 전산(장비)실 내에서 유닉스 DB 서버에 직접 연결하여 접근하는 방식		
② DBMS, TELNET, SSH, FTP, SFTP	· 사용자 PC에 설치 되어 있는 툴을 이용하여 유닉스 DB 서버에 접근하는 방식 (일반적인 방식)		
③ TELNET, SSH, FTP, SFTP	· 사용자 PC에서 타 유닉스 서버를 경유 하여 접근하는 방식		
④ 윈도우 원격접속	· 사용자 PC에서 윈도우 원격접속을 통해서 윈도우서버나 윈도우 DB 서버에 접근하는 방식		
⑤ DBMS, 윈도우 원격접속	· 사용자 PC에 설치 되어 있는 DB툴을 이용하여 윈도우 DB 서버에 접근하는 방식		
⑥ Windows 로컬 콘솔	· 전산(장비)실 내에서 윈도우 NT DB 서버에 직접 연결하여 접근하는 방식		
⑦ TELNET, SSH	· 보안장비나 네트워크장비에 설정변경이나 모니터링을 위하여 접근하는 방식		

통합된 접근제어 보안관리 제공

1. DBSAFER Enterprise 솔루션 개요 / II. 솔루션 소개

DBSAFER는 DB접근제어, SYSTEM접근제어, OS접근제어, 통합계정관리를 하나의 솔루션에서 통합 관리를 제공합니다.



DBSAFER Enterprise 시스템 구성방식 | 1. DBSAFER Enterprise 솔루션 개요 / II. 솔루션 소개

접근 제어 및 감사 제품				
구분	•Sniffing 방식	•Server Agent 방식	•Gateway 방식 •(In-line, Proxy 구성 가능)	•TTP Gateway 방식 •(Trusted Transparent Proxy로 In-Line, Proxy 구성가능)
보안기능	<ul style="list-style-type: none"> 우회접속차단 가능 	<ul style="list-style-type: none"> 강력한 보안 기능 우회접속차단 가능 	<ul style="list-style-type: none"> 강력한 보안 기능 제공 (단, 우회접속차단 필요) 	<ul style="list-style-type: none"> 강력한 보안 기능 제공 (단, 우회접속차단 필요)
안정성	<ul style="list-style-type: none"> Agent 가 설치되지 않는 방식, 서버에 영향 없이 안정적 운영 가능 	<ul style="list-style-type: none"> 서비스 재 시작 없음 서버 재 시작 없음 Software TAP방식 장애 없음 	<ul style="list-style-type: none"> Agent 가 설치되지 않는 방식, DB서버 서버에 영향 없이 안정적 운영 가능 Gateway 구성에 따른 장애 대응 방안 필요 (이중화 or Bypass) SSH 제어 및 모니터링 가능 암호화 대체 기능제공 (데이터마스킹) 	<ul style="list-style-type: none"> Agent 가 설치되지 않는 방식, DB서버 서버에 영향 없이 안정적 운영 가능 SSH 제어 및 모니터링 가능 암호화 대체 기능제공 (데이터마스킹)
확장성	<ul style="list-style-type: none"> 확장시 각각의 세그먼트 마다 H/W 연결 필요 	<ul style="list-style-type: none"> 서버마다 Agent 설치 필요 	<ul style="list-style-type: none"> 별도의 H/W 나 Agent 추가 없이 확장 가능 	<ul style="list-style-type: none"> 별도의 H/W 나 Agent 추가 없이 확장 가능
제품특징	<ul style="list-style-type: none"> 모니터링만 할 경우 권장 	<ul style="list-style-type: none"> Gateway방식에서 우회경로차단 및 서버 접근제어 용으로 활용 	<ul style="list-style-type: none"> 보안성 및 확장성이 뛰어나며, 이중화 구성 시 가장 좋은 구성 제안이 가능 	<ul style="list-style-type: none"> 안정성 : Sniffing방식과 동일 보안성 : Gateway방식과 동일 성능 : Gateway방식과 동일 최적의 구성 방식

✓Server Agent 방식 설계 원칙

고려사항	적용 기술	비고
서비스의 연속성을 위한 설계원칙	<ul style="list-style-type: none"> 후킹 기술 사용 절대 불가 네트워크 트래픽을 driver level에 처리하지 않고 application level에서 Raw socket을 sniffing 함 (프로그램이 오동작하거나 강제 종료 시켜도 네트워크에는 전혀 영향이 없음) DB보안 서버 장애 시 Fail-open 모드로 자동 전환 기 접속된 세션 보호 사용자의 고의적인 프로세스 종료 및 각종 비정상 동작에 대한 자동 복구 기능 수행 	
성능	<ul style="list-style-type: none"> 최소한의 자원 사용으로 최대의 성능 목표 (Memory 5M bytes 이하, 평상시 0.1% 미만 점유, 과부하 시 3% 미만 점유) 	
설치 및 이식성	<ul style="list-style-type: none"> ANSI-C로 작성하여 다수의 OS 플랫폼에 바로 이식 가능 특정 라이브러리 설치 없이 서버에이전트 동작 (프로그램만 서버에 복사하여 동작) 	

DB접근제어 구성 개요

2. DB접근제어 기능 / II. 솔루션 소개

DB 접근제어 및 감사 솔루션은 DB에 대한 접근/권한 제어, SQL 감사/로깅 등을 통하여 DB를 통한 대량의 내부정보유출의 위험을 최소화함.

DB접근제어시스템 (Gateway + Sniffing + Server Agent 방식)



✓구성 방식

Gateway 방식	<ul style="list-style-type: none"> • Proxy(Gateway)를 통하여 접근 제어 • 보안성 및 확장성이 뛰어남
Sniffing 방식	<ul style="list-style-type: none"> • 단순 모니터링 구성 • 물리적으로 구성이 복잡해질 수 있음 • DB에 영향 없음, 제어가 제한적임
Server Agent 방식	<ul style="list-style-type: none"> • 서버마다 Agent 설치 • 우회접속 차단지원, 서버 리소스사용 • 콘솔로깅 지원

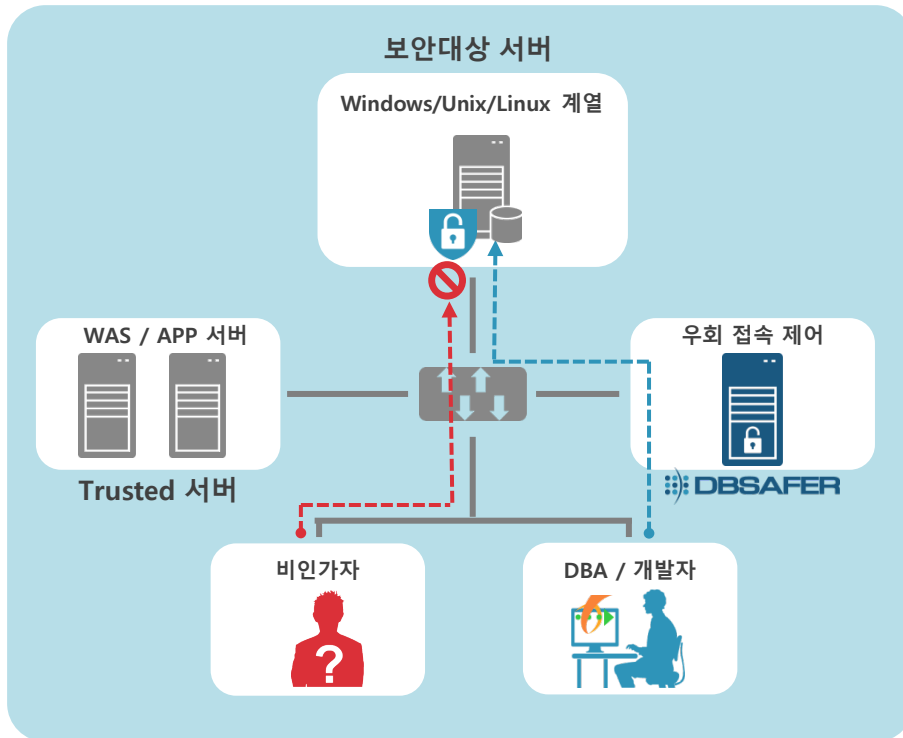
✓주요 기능

접근제어	• 가상계정, IP, APP등으로 접근제어
권한제어	• 명령어, Table, Colum 단위로 가능
SQL 감사/로깅	• 모든 SQL 내역 감사, 로깅, 검색
분석 및 보고서	• 다양한 통계 분석 및 보고서 제공

직접접근(보안 우회접근)에 대한 제어 방안

2. DB접근제어 기능 / II. 솔루션 소개

Proxy Gateway 방식으로 구축한 경우, 보안장비(DBSAFER)를 경유하지 않고 보안대상서버로 직접 접근이 되면 제어/로깅 등의 보안기능을 제공 할 수 없게 된다. 그러므로 직접접근(보안 우회접근)에 대한 제어기능이 필요하며, 아래와 같이 다양한 방식으로 직접접근(보안 우회접근)에 대한 제어를 제공한다. 보안 우회 접근에 대한 차단은 **접근제어 솔루션 중 DBSAFER만 유일하게 제공한다**.



[우회/직접 접속 불가]

제공	방안	설명
고객사 환경	네트워크방화벽	장점: 설정 간단함 단점: 유사시 수동 설정 변경
	서버방화벽	장점: 설정 비교적 간단함 단점: 유사시 수동 설정 변경
	스위치 ACL	장점: 방화벽이 없는 경우 적용가능 단점: 유사시 수동 설정 변경
벤더 솔루션	스니핑 이용 차단	IPS와 유사하게 패킷을 보고 차단 시 리셋 패킷을 전송, 100%는 차단불가
	시스템 접근제어	유사시 자동 설정 변경 지원됨 동일 제품군중 DBSAFER 유일 제공

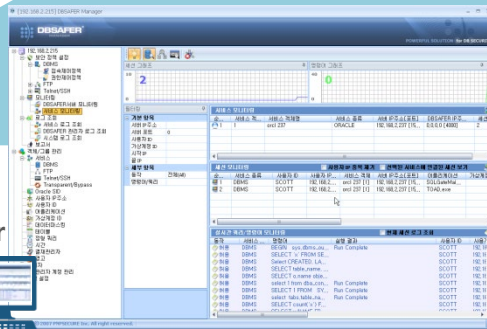
이기종 DBMS 지원 및 통합 관리 | 2. DB접근제어 기능 / II. 솔루션 소개

DBSAFER는 다수의 이기종 DBMS를 하나의 사용자 인터페이스를 통해 통합관리 할 수 있다. 현재 DBSAFER Enterprise V5.0이 지원하는 상용 DBMS는 총 15가지 유형으로 Oracle(모든 버전 지원), MSSQL, Sybase ASE/IQ, Informix, DB2/UDB, Altibase, Teradata, MySQL, Cubrid, Tiberio, PostgreSQL(Netezza, GreenPlum, Vertica) 에 대해서 지원한다.

모든 유형의 DBMS 통합 관리



DBSAFER
Enterprise Manager



SSL 통신

Service

- 서비스 설정
- 접속 및 권한 제어 정책 설정
- 통합 및 선택적 모니터링
- 감사 로깅
- 보고서
- 사전/사후 결재 처리

이기종 PC Agent 지원(Windows 계열, MaOS 계열)

2. DB접근제어 기능 / II. 솔루션 소개

DBSAFER는 사용자의 다양한 PC환경에서 기능을 제공합니다. OS는 Windows 계열과 MacOS 계열을 지원합니다. (기능은 동일)
 PC Agent 의 기능은 크게 2가지로서 사용자에 대한 인증과 보안대상 서버로의 트래픽을 보안장비로 유도하는 주소변환(NAT)기능입니다.
 PC Agent 하나로 DB접근제어 시스템접근제어에 대해 동일하게 기능을 제공합니다.
 MacOS는 업계에서 유일하게 지원하며 관련 화면은 아래와 같습니다.

[User Login]

DB보안 사용자 인증

PNP SECURE DB보안 사용자인증

Login

USERNAME

PASSWORD

Remember Me

OK Cancel

[User Screen]

PCAgent 사용자

DB보안 사용자 인증

PNP SECURE DB보안 사용자인증

USERNAME

PASSWORD

Remember Me

OK Cancel

[NAT Service List]

NAT 서비스 (wdkim)

동기화

No ▲	서비스	서버명	서버 IP
1	TERMINAL	SSH_3.119	192.168.3.119
2	DBMS	ORA_192.168.6.10	192.168.6.10
3	TERMINAL	RDP_2.193	192.168.2.193
4	FTP	FTP_3.22	192.168.3.22
5	TERMINAL	TELNET_3.22	192.168.3.22
6	TERMINAL	SSH_3.22	192.168.3.22

연결서버 : 192.168.3.45
서비스 개수 : 6

닫기

[Dock Icons]

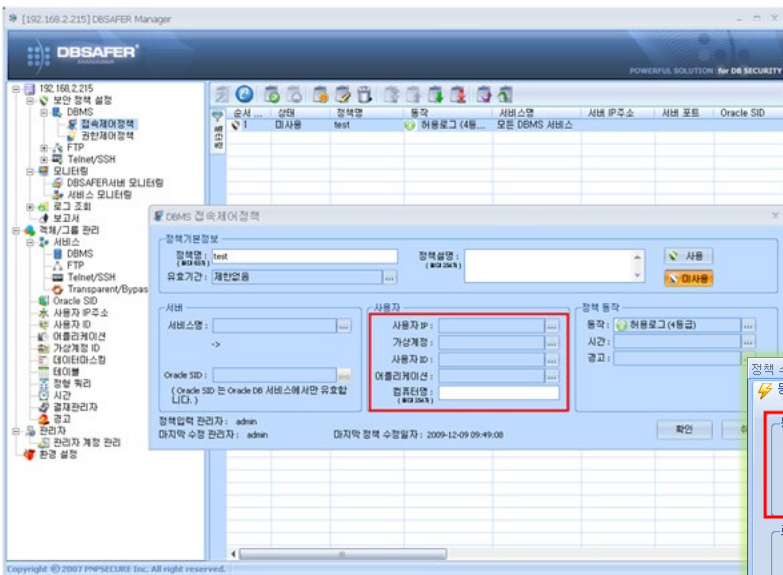
NAT 서비스 내역

- 암호변경
- 로그아웃
- 공지사항
- 쪽지
- 옵션 ▶
- 모든 윈도우 보기
- 가리기
- 종료

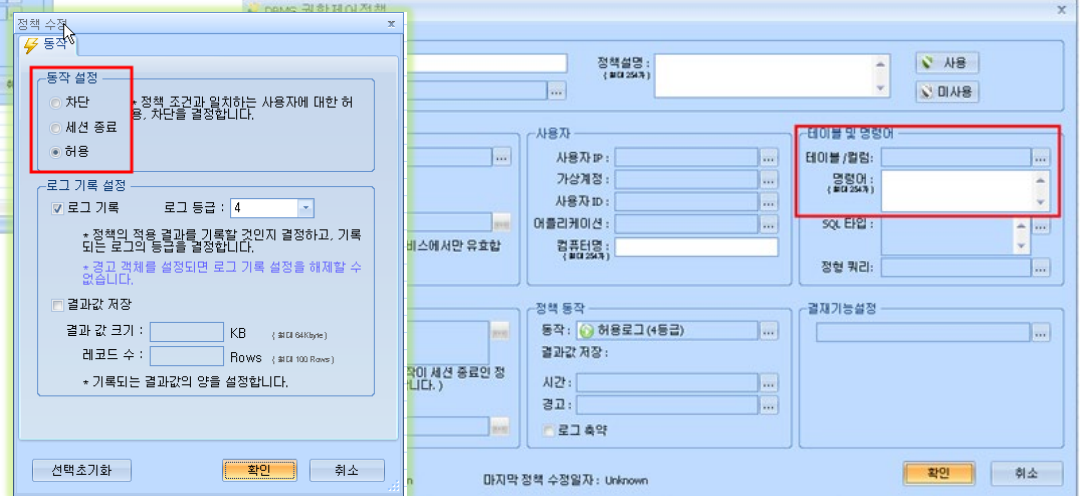
접근제어

2. DB접근제어 기능 / II. 솔루션 소개

보안대상 서버로의 접근에 대하여 다양한 Object를 AND 조합으로 접근제어 정책을 제공한다.
Object종류는 가상계정, 사용자 IP(IP대역 포함), Application(TOAD/Orange/Golden/SQL-PLUS/기타), DB계정, 날짜/시간 등이 있다.



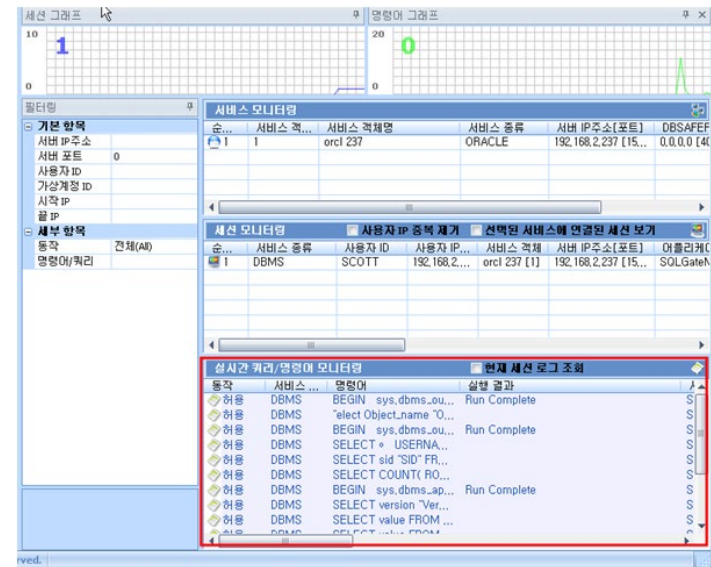
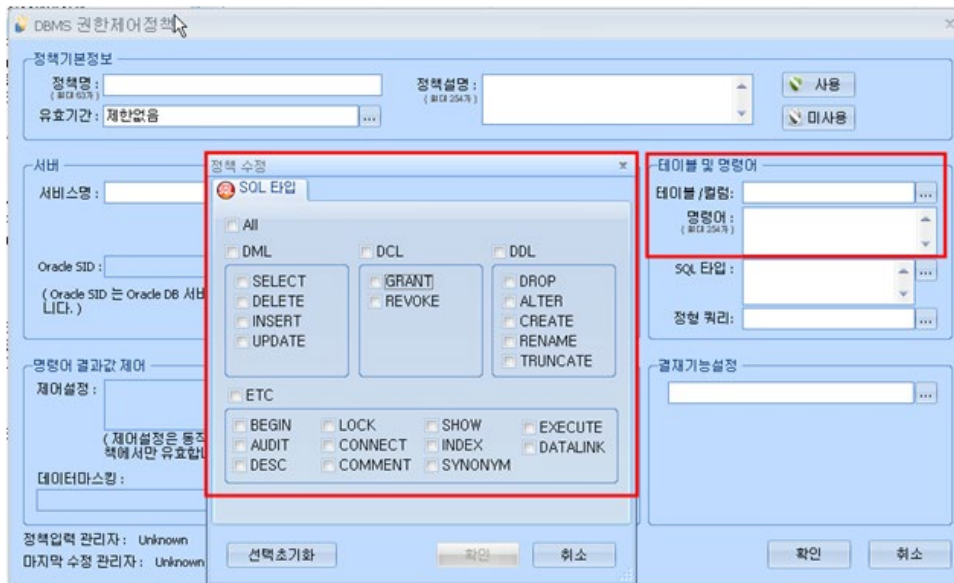
- ✓ 사용자 IP 별 제어
 - 차단하고자 하는 사용자의 IP를 Single 또는 Range로 지정하여 차단/허용
- ✓ DBMS 접속 계정 차단
 - DBMS에 접속하는 계정에 따라 접속을 차단/허용
- ✓ Application 별 차단
 - DBMS에 접속하는 Application에 따라 접속을 차단 허용
- ✓ 특정 명령어와 Table 및 Column 명 까지 조합 하여 명령어에 대한 사전 차단



권한제어

2. DB접근제어 기능 / II. 솔루션 소개

DBSAFER는 DDL/DML/DCL 구문과 Table, Column에 대한 권한제어를 제공하며, 제어 시에도 연결된 세션을 유지한다. DB의 부하를 증가시키는 명령의 제어와 특정 사이즈 이상의 결과값(Return data)에 대한 제어 기능 등을 제공합니다.

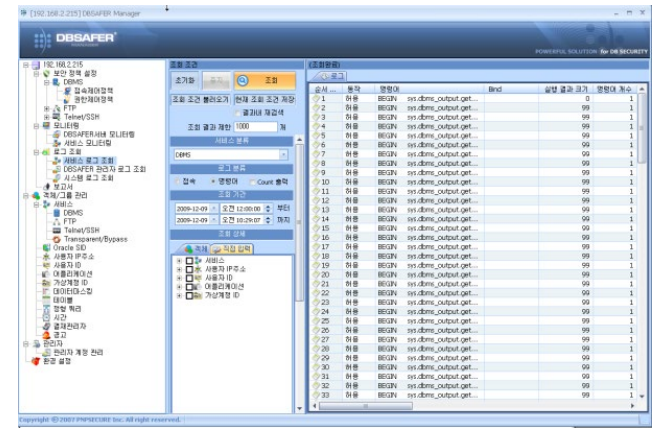
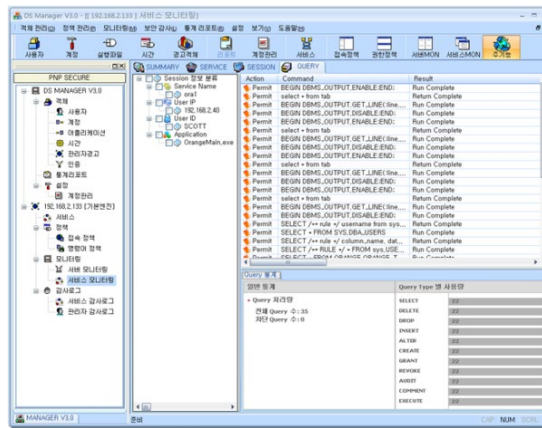
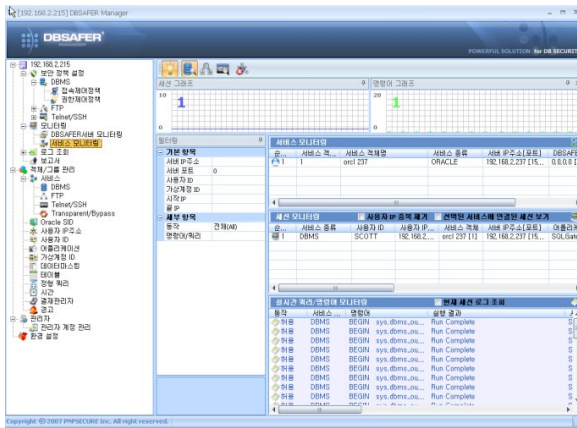


- ✓ DBSAFER는 DCL 구문뿐 아니라 테이블단위 접근제어 설정, DML, DDL 등에 대한 명령을 차단할 경우에도 접속된 세션을 유지하며 SQL 명령어, DB Table 등의 모든 조건을 이용하여 권한을 제어한다.
- ✓ 특정 명령어와 Table 및 Column 명까지 조합하여 명령어에 대한 사전 차단을 하고 주석이나 힌트 절에 대한 차단도 지원한다.
- ✓ DB 서버가 사용자에게 특정 시간이 지나도록 결과값을 주지 않은 경우 해당 세션을 강제로 종료시키는 기능을 제공한다.

감사 및 로깅

2. DB접근제어 기능 / II. 솔루션 소개

DBSAFER는 감사데이터에 대하여 실시간 모니터링을 제공하며, 특정 사건에 대한 로그 분석 시에 다양한 관점에서 신속하게 해당 시점의 로그에 접근하여 정확한 자료를 확인 할 수 있도록 사용성, 효율성을 제공한다.

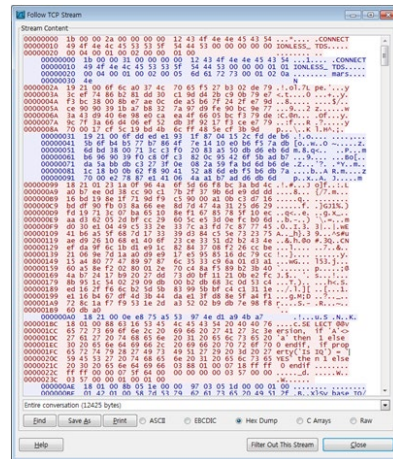


- ✓ SYBASE IQ나 MSSQL 등과 같이 암호화 통신(또는 로그인 정보만 암호화)에 대해서도 감사 및 로깅 기능을 제공한다.
- ✓ 사용자별, 접속 세션별 접속 이력 및 쿼리에 대한 실시간 모니터링하며, 보안관리자의 접근 내역은 별도로 관리 한다
- ✓ 통합 Dashboard 및 통합관리 화면을 통하여 감시 대상서버, DB에 대한 세션, SQL 변화 추이 및 상태 정보를 그래프로 제공
- ✓ 로그에서 특정 로그를 검색하는 기능
- ✓ 모든 DB 접속 SQL 및 BIND 값 로깅 및 결과값(OPTION)로깅
- ✓ 사용자별, 접속세션별 접속 이력을 실시간으로 모니터링기능을 제공한다.
- ✓ 감시대상 DB로 요청되는 초당 SQL 요청 수, 초당 평균 응답시간, 데이터 조회 건수, 네트워크 사용량(패킷량의 변화), 경보 전달 건수를 실시간으로 볼 수 있는 기능 제공을 제공한다.

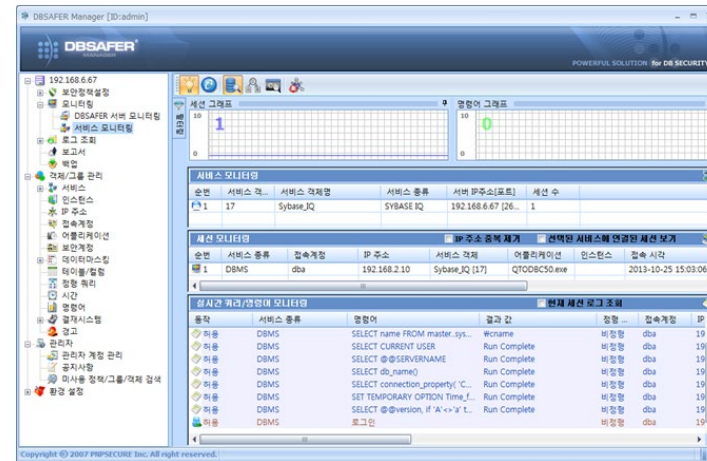
감사 및 로깅 (암호화 통신에 대해서도 지원)

2. DB접근제어 기능 / II. 솔루션 소개

지원하는 모든 DB접속에 대하여 감사 및 로깅 기능을 제공하고, SYBASE IQ나 MSSQL과 같이 암호화된 통신에 대해서도 아이디를 포함한 세션 정보는 물론 모든 송수신데이터에 대하여 타 DBMS에 제공되는 보안기능과 동일하게 제공한다.



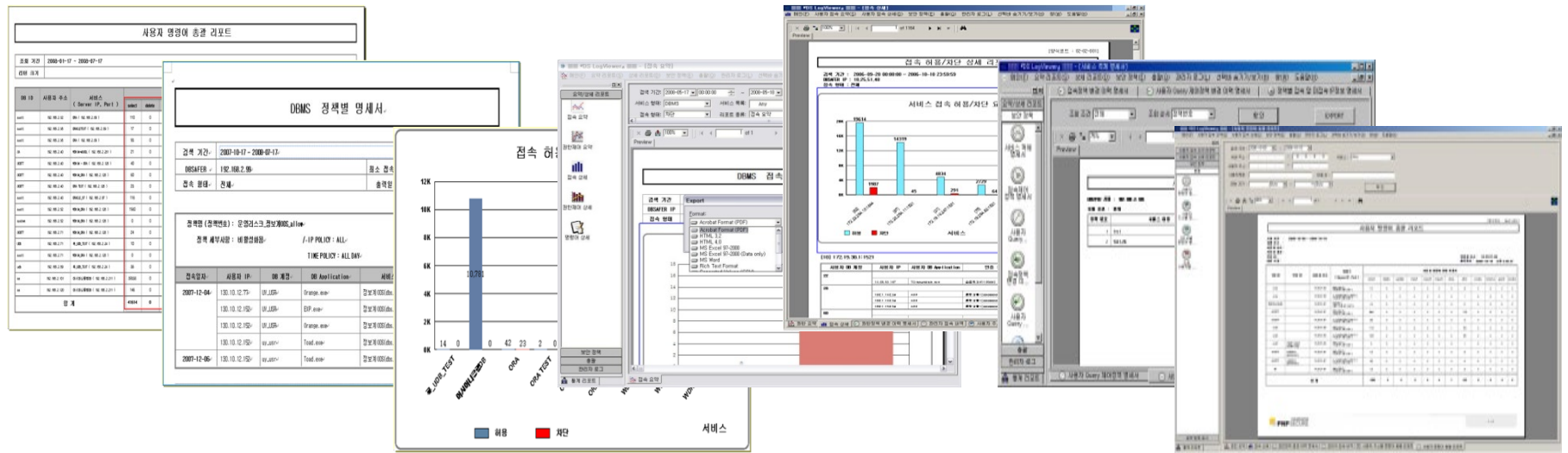
[암호화 되어 있는 패킷상태]



[암호화 되어 있는 세션을 실시간 모니터링 중인 화면]

보고서 기능 | 2. DB접근제어 기능 / II. 솔루션 소개

DBSAFER는 보안대상 DB에 대하여 접근 추이를 그래프 뿐만 아니라 그래프로 표현 및 출력 기능을 제공하며, SQL 구문별 명령어 별로 검색 및 통계 보고서 기능을 제공한다. 생성된 보고서는 외부 데이터로 (PDF, HTML, HWP, DOC, XML, XLS, TXT, 등..) Export 하는 기능을 제공한다.



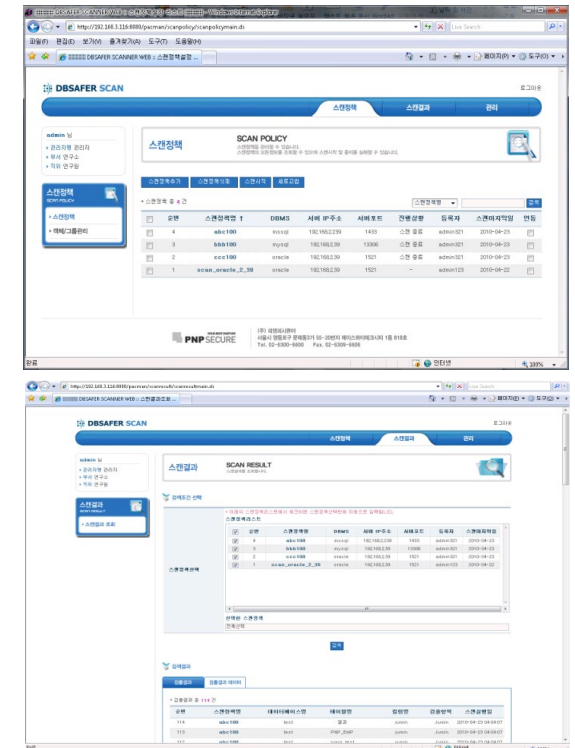
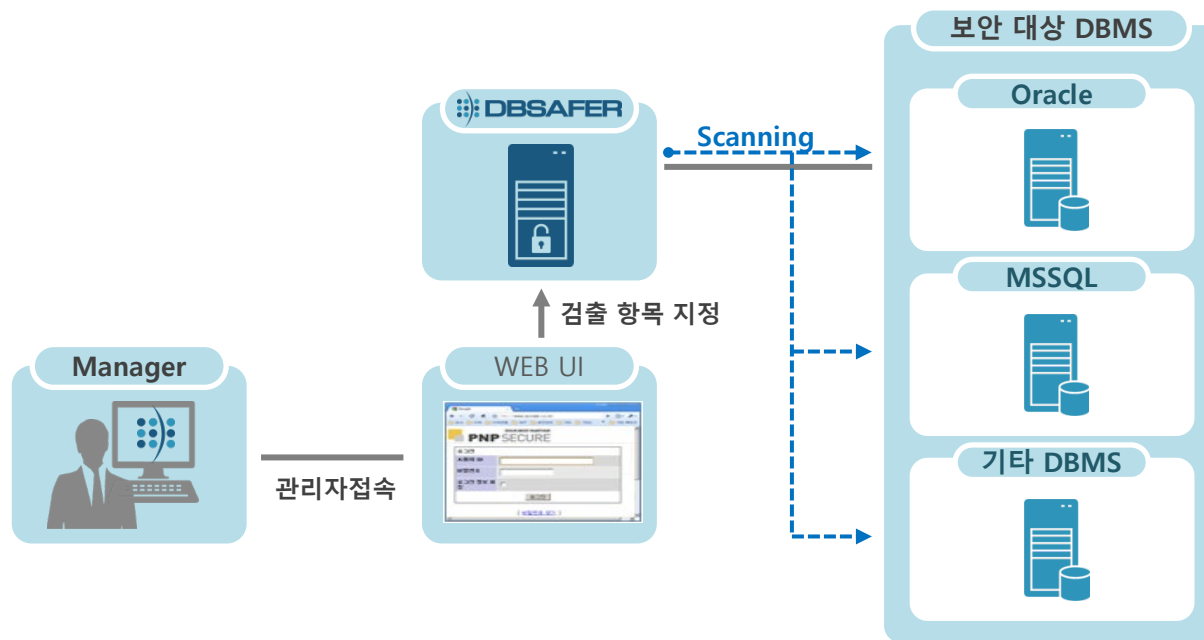
- ✓ DB 접근 추이를 그래프로 표현 및 출력 기능을 제공하며, SQL 구문별 명령어 별로 검색 및 통계 보고서 기능을 제공한다. 그리고, 생성된 보고서를 PDF, HTML, DOC, XML, XLS, TXT, HWP 등 다양한 형태로 변환한다.
- ✓ 사용자 정보, 서비스 객체명세서, 접속제어 정책 명세서, 사용자 Query 제어정책 명세서, 접속 정책 변경 이력 명세서, 사용자 Query 제어정책 변경 이력 명세서, 정책 별 접속 및 미 접속 IP 정보 명세서, 정책 별 접근 명세서 등 이외에 일,주간,월간 요약/상세 보고서, 총괄로그, 관리자 로그 등에 대한 보고서도 생성, 저장 기능 제공.

DBSCANNER 기능을 통한 개인정보의 위치를 식별 (옵션)

2. DB접근제어 기능 / II. 솔루션 소개

개인정보 관리책임자는 DB내 개인정보의 위치를 식별하여 관리하여야 합니다. 대부분은 관리자가 인지하고 있는 이상의 개인정보가 있으며, 또한 새로 생성되고 제거되는 개인정보에 대해 관리하기란 쉽지 않습니다.

개인정보스캐너는 시스템적으로 개인정보의 위치를 식별하여 관리자에게 제공하며, DB접근제어 모듈과 연동되어 자동 또는 관리자의 확인만으로 개인정보 보안정책을 적용하는 기능을 제공하여 체계적인 관리를 제공합니다.



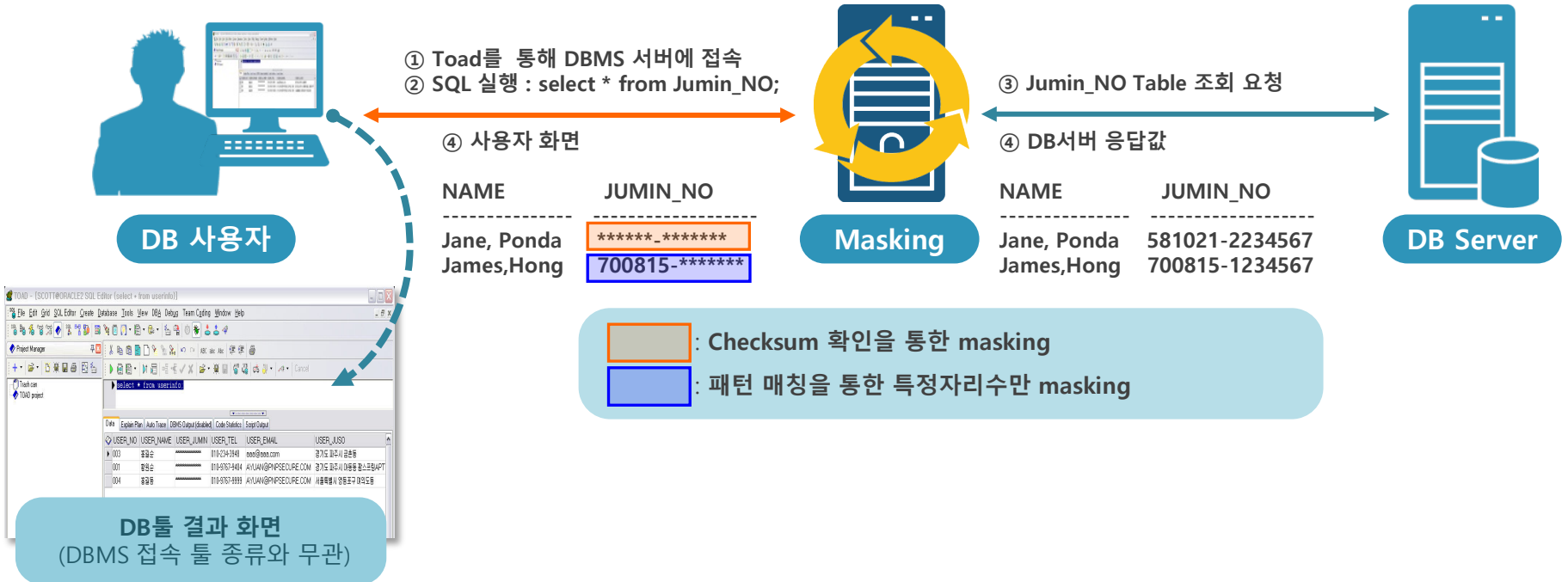
- 개인정보 관련 Table/Column 정보를 추출하여 DBSAFER의 데이터마스킹 정책에 자동으로 등록
- Stored procedure의 경우 Procedure 정보를 추출하고 DBSAFER 서비스와의 연계를 통해 사용자가 실행 하는 Stored procedure의 동작을 확인

조회 결과 값 제어 [데이터마스킹] | 2. DB접근제어 기능 / II. 솔루션 소개

데이터마스킹 기능은 제안사가 특허를 보유한 암호화 대체 기술로서 주민등록번호 등 개인정보의 전체 또는 일부를 별표로 치환한다.
 「정보통신망 이용촉진 및 정보보호 등에 관한 법률의 "개인정보 표시 제한조치"를 제공하는 기능(기술적·관리적 보호조치 기준-제9조)이다

- 주민번호의 경우 Masking의 오류를 최소화하기 위해 "13"번째 Checksum을 인식하여 동작하는 기능제공
- 정책에 따라 주민 번호의 전체 또는 일부분만 Masking(예:"701125-*****")기능 제공

⑤ 서버 응답 값에 대해 체크 및 응답 값 변경(Masking)



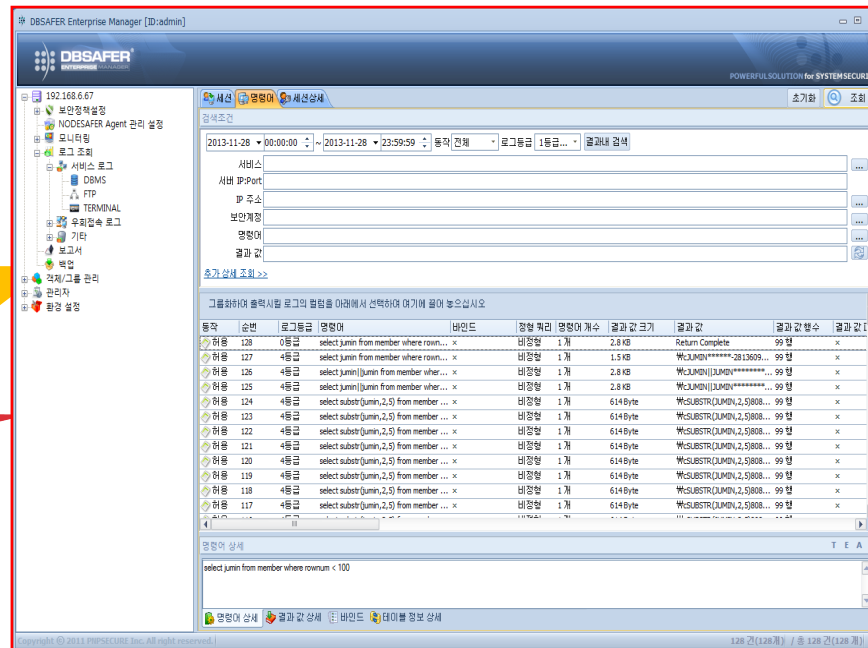
중복 쿼리 축약

WAS의 정형 및 비정형 쿼리의 중복으로 인한 로그데이터 유실 및 속도 저하는 중복 쿼리 축약 기능으로 중복 쿼리를 최소화시켜 Sniff 및 로그 장비의 부하를 감소 시키며, 로그 데이터의 경량화로 하드웨어에 투자되는 비용을 최소화 한다.

S(대형유통사)사의 WAS에서 발생된 로그로 인하여 30,000여 개의 버퍼 파일이 발생하였으며, DB에 저장되는 로그는 계속 밀려서 1일전의 로그가 저장되고 있음

중복로그 데이터

로그 데이터 유실 및 CPU부하로 인한 속도 저하 현상 발생

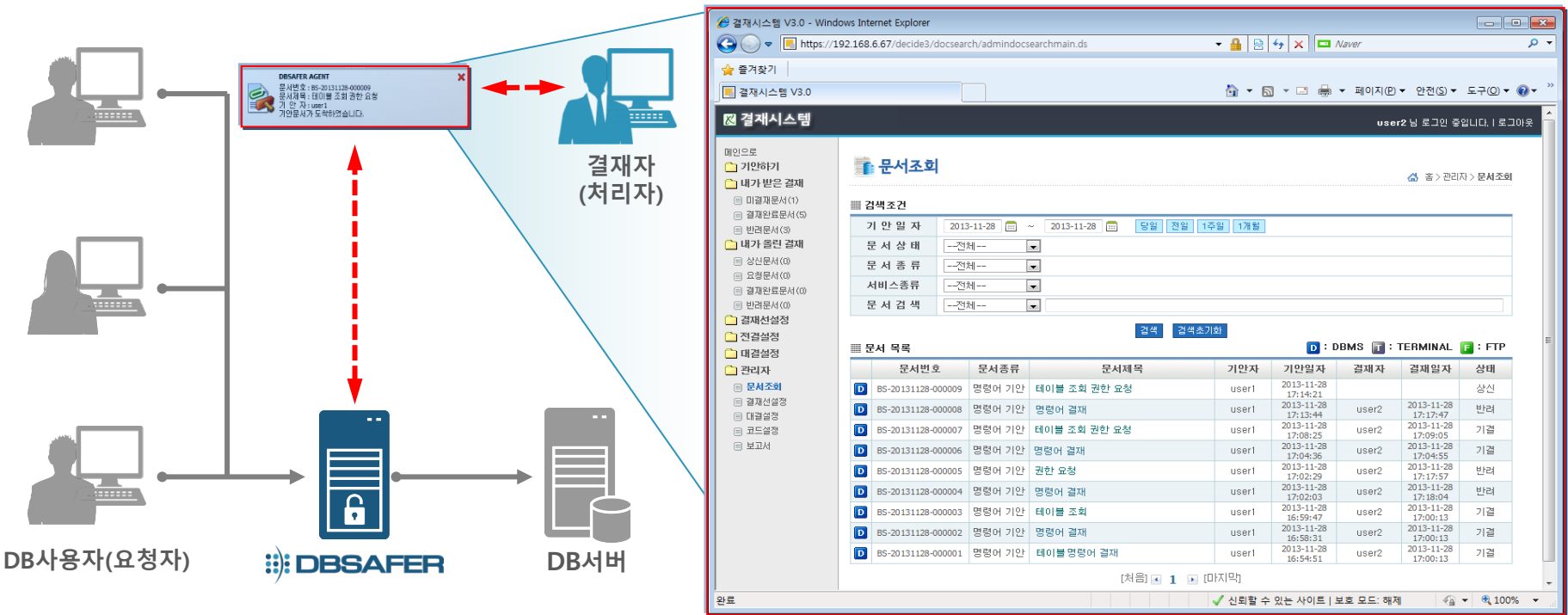


- ### 구성원리 및 특징
- 로그 발생시 최초 로그는 바로 DB에 저장
 - 중복 로그는 10초에 1번씩 count 값만 갱신
 - 중복 로그라도 2분에 1번씩은 새로운 로그를 기록
 - 초당 10,000쿼리 발생시에도 임시 버퍼 파일이 발생하지 않으면서 100% 모두 처리
 - CPU 부하를 줄여서 Sniff 서버의 로그 유실을 최소화 함
 - DBSAFER Manager 에서 중복 count를 기준으로 로그를 정렬할 경우 판독 가능

명령어 결재 기능

2. DB접근제어 기능 / II. 솔루션 소개

DBSAFER의 결재시스템은 User ID/User IP 및 Table 단위의 조건을 조합하여 쿼리를 결재하는 기능을 제공하며, 사용자가 요구하는 내역에 대한 이력보고서를 생성할 수 있다.



결재 업무 흐름도

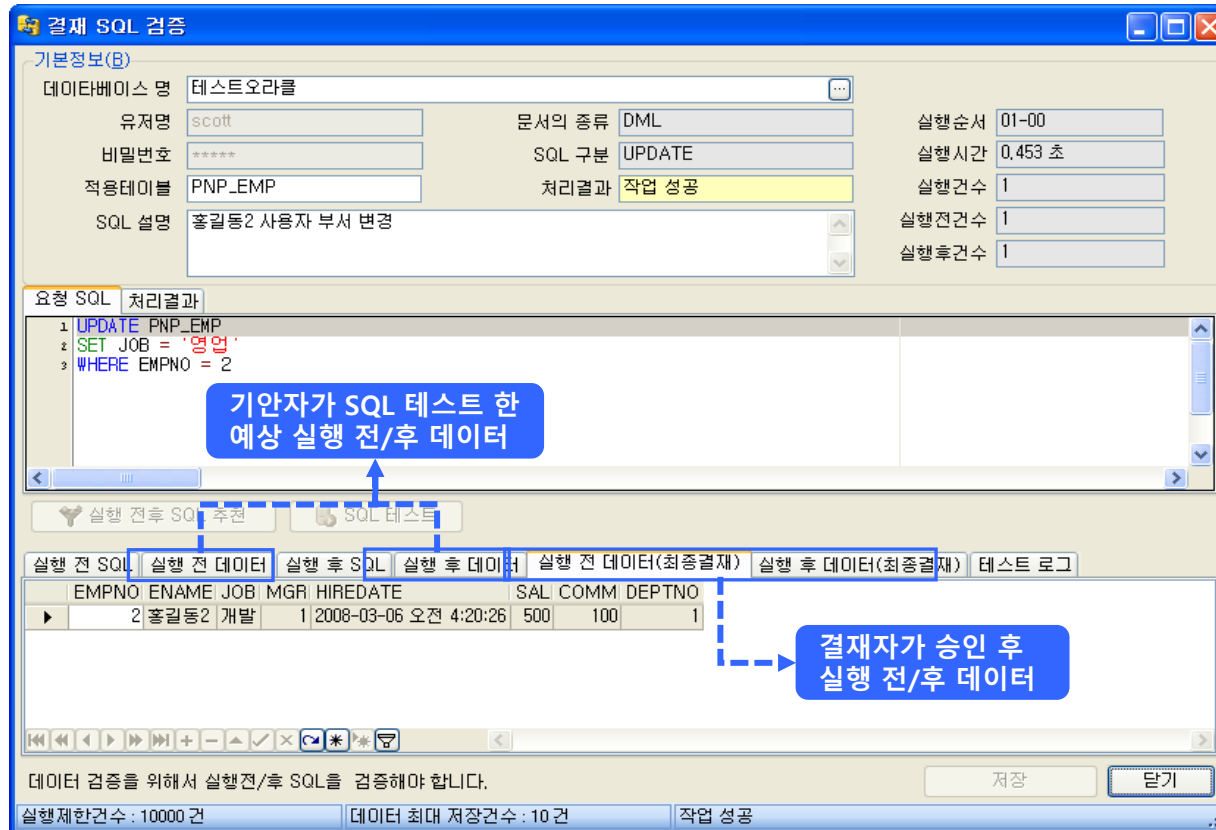
결재 문서 조회

사전/사후 데이터를 포함한 결재 기능 (옵션)

2. DB접근제어 기능 / II. 솔루션 소개

DBSAFER는 금융감독원의 권고사항인 결재 전/후 데이터 보관, 작업요청 및 결재 이력을 보관한다.

DMS Client 사용 시 DBMS의 종류에 무관하게 처리가 가능하며 기존의 전자결재 결재라인을 이용할 수 있어 결재라인을 별도로 관리할 필요가 없다.



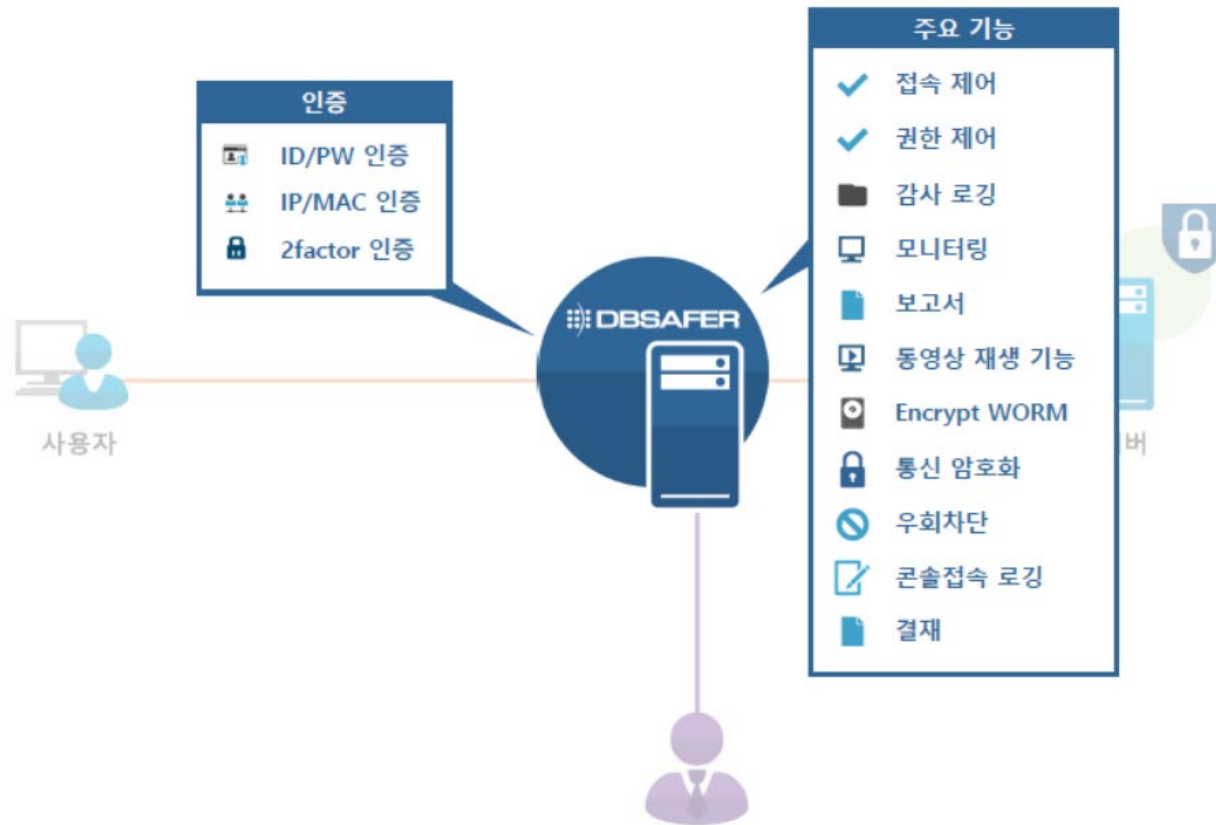
•DBSAFER는 각 DB 서버를 그룹별로 나누고 그룹에 대한 권한을 부여 받은 관리자가 사용자가 요청한 SQL문에 대하여 검색과 결재기능을 지원함.

•결재가 필요한 SQL문은 결재가 승인될 때까지 기다리게 되며, 설정을 통하여 승인 받지 않고 미리 처리하는 사후 결재기능도 지원함.

SYSTEM 접근제어 주요기능

2. SYSTEM 접근제어 기능/ II. 솔루션 소개

SYSTEM 접근제어(DBSAFER AM)은 중요 개인정보에 접근하는 모든 행위에 대하여 강력한 접근제어 기능을 제공합니다.

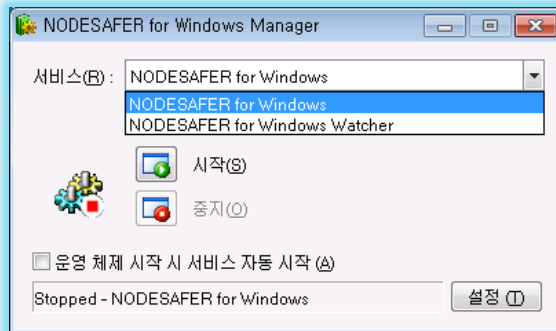


SYSTEM 접근제어 지원 OS

3. SYSTEM 접근제어 기능 / II. 솔루션 소개

DBSAFER Enterprise가 지원하는 OS는 AIX, HP Unix, Linux, SUN, Window와 같이 현재 운영 중인 모든 OS에 대해 지원을 하며 각 OS별 동작 화면의 예는 아래와 같습니다.

Windows



IBM AIX

```
[root@localhost /root]# uname -a
AIX localhost 3 5 00C893EB4C00 powerpc unknown AIX
[root@localhost /root]# ps -ef|grep dbsafer
root      5161      1  0 19:42 pts/0    00:00:00 ./dbsafer_policy_manager start
root      5349      1  0 19:43 pts/0    00:00:00 ./dbsafer_server_agent start
root      5355    3980  0 19:43 pts/0    00:00:00 grep dbsafer
[root@localhost /root]#
[root@localhost /root]#
[root@localhost /root]#
[root@localhost /root]#
```

LINUX

```
[root@choiDB dbsafer2]# uname -a
Linux choiDB 2.6.9-67.ELsmp #1 SMP Wed Nov 7 13:58:04 EST 2007 i686 i686 i386 GNU/Linux
[root@choiDB dbsafer2]# ps -ef|grep dbsafer
root      4309      1  0 18:12 pts/0    00:00:00 ./dbsafer_policy_manager start
root      4358      1  0 18:12 pts/0    00:00:00 ./dbsafer_server_agent start
root      4810    3980  0 18:46 pts/0    00:00:00 grep dbsafer
[root@choiDB dbsafer2]# █
```

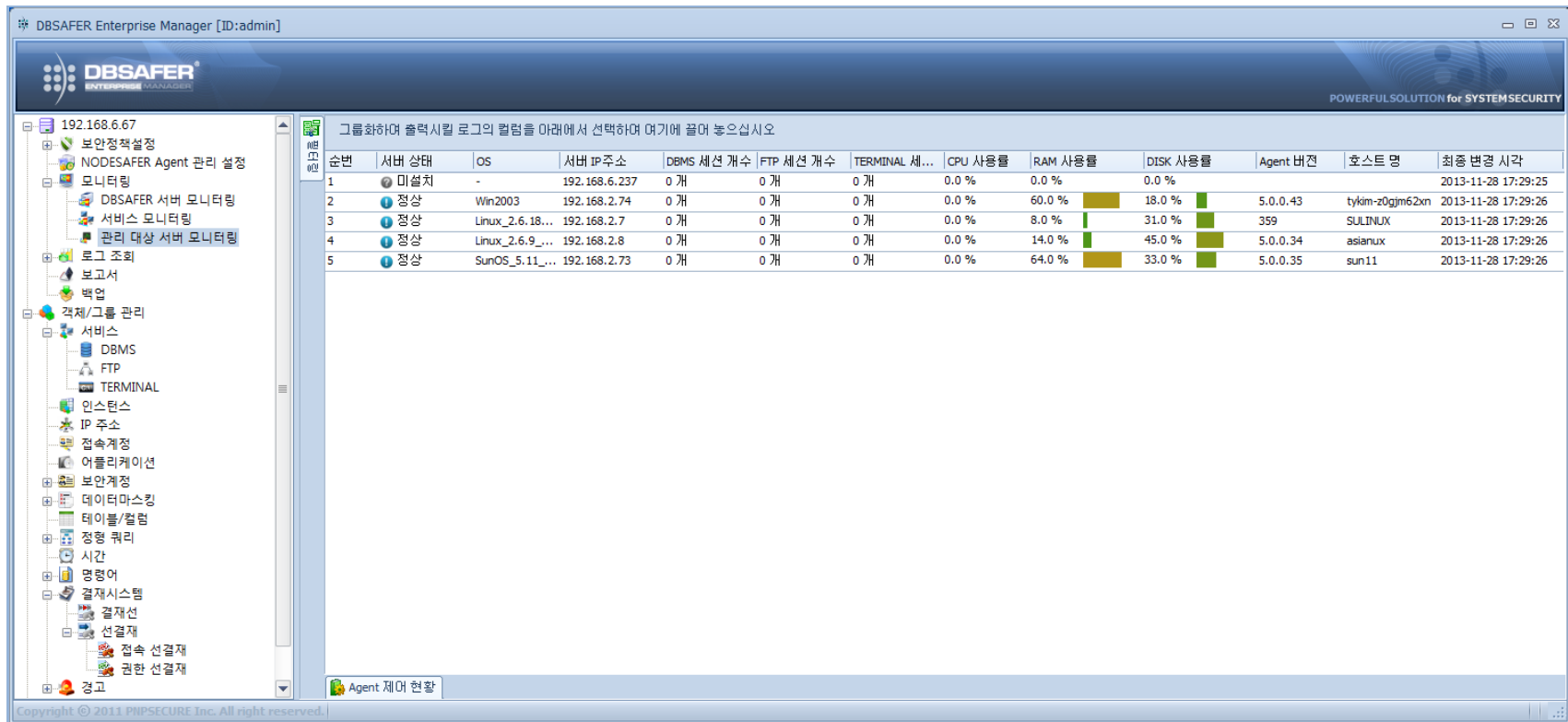
SUN Solaris

```
# uname -a
SunOS lisa 5.10 Generic_127127-11 sun4u sparc SUNW,Sun-Fire-V210
# ps -ef|grep dbsafer_
root      915    889   0 19:53:57 pts/4      0:00 grep dbsafer_
root      903      1  0 19:53:21 pts/4      0:00 ./dbsafer_policy_manager start
root      911      1  0 19:53:44 pts/4      0:00 dbsafer_server_agent start
#
#
```


서버 자원 및 세션 실시간 모니터링

3. SYSTEM접근제어 기능 / II. 솔루션 소개

- ✓서버의 자원 정보(CPU/Memory/Disk) 및 세션 정보 그래프 제공
- ✓보안대상 서버의 보안기능 동작여부와 주요 통계정보를 제공



[서버 리소스 모니터링]

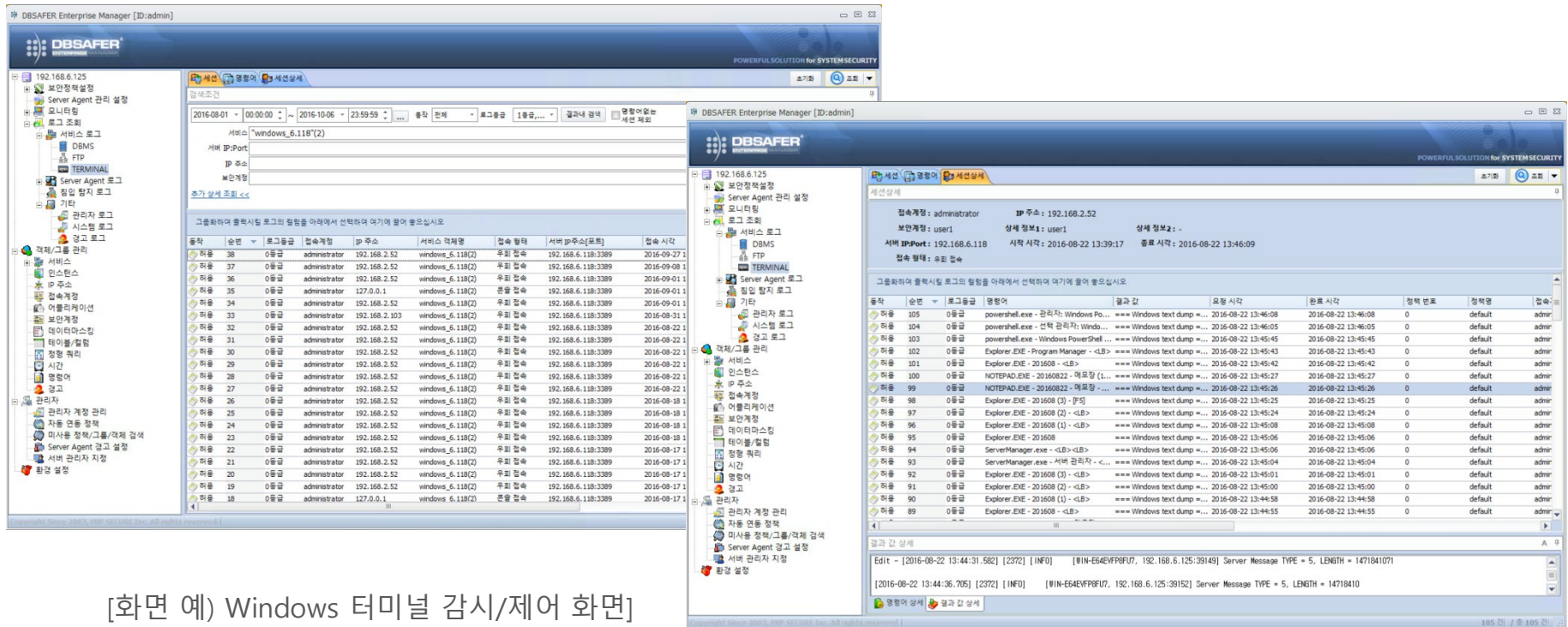
서비스 감시/제어

3. SYSTEM 접근제어 기능 / II. 솔루션 소개

다음의 프로토콜에 대하여 서비스를 관리하고 제어 및 로그를 수행한다.

- ✓ Windows 터미널 (RDP/윈도우원격접속)
- ✓ Unix/Linux 터미널 (TELNET/SSH/시리얼포트/로컬 콘솔 등)
- ✓ 파일 전송 서비스 감시/제어 (FTP/SFTP 등)

- ✓ 메인 프레임 TN-3270, TN-5250
- ✓ 보안장비 HTTPS



[화면 예) Windows 터미널 감시/제어 화면]

다양한 사용자 접속 환경 지원 [C/S, Web] | 3. SYSTEM접근제어 기능 / II. 솔루션 소개

DBSAFER Enterprise는 기존의 접속 프로그램이나 환경을 변경하지 않는 C/S(PC NAT)방식과 Web을 통한 사용자 접속 방식 모두를 제공하여 사용자의 편의성과 보안성을 동시에 만족합니다.

사용자 접속방식	그림	설명	장점	단점
C/S 방식 (PC NAT)		<ul style="list-style-type: none"> · 사용자기 기존에 접속하던 방식 그대로 "TELNET 192.168.1.100"으로 접속하면 자동으로 보안서버 (192.168.2.2)를 경유하여 192.168.1.100에 접속됨 	<ul style="list-style-type: none"> · 기존의 접속 방법을 전혀 변경할 필요가 없음 · 자체 개발한 TELNET, FTP 프로그램까지 보안 가능 	<ul style="list-style-type: none"> · 사용자가 OS의 계정을 알고 있어야 함
Web 방식		<ul style="list-style-type: none"> · 사용자에게 접속 가능한 서버 리스트만을 리스트 형태로 나타내며, 가능한 서비스를 선택 후 자동 접속합니다. · 이 때 사용자는 자신의 비밀번호를 노출시키지 않아, 계정 도용의 위험으로부터 최소화함 	<ul style="list-style-type: none"> · 사용자의 PC 환경에 관계 없이 Web으로 접속이 가능 · 사용자에게 OS계정을 노출하지 않아도 접속할 수 있음 	<ul style="list-style-type: none"> · 자체 개발한 TELNET, FTP 프로그램사용할 경우 프로그램 실행 시 실행 옵션 기능 필요

OS 자동로그온

3. SYSTEM접근제어 기능 / II. 솔루션 소개

사용자는 클릭만으로 원하는 서버에 다양한 프로토콜로 자동로그온 기능을 제공합니다. 웹 페이지에서 초기에 한번의 인증은 필요합니다. 자동로그온 지원되는 프로토콜은 TELNET / SSH / FTP / SFTP / RDP(윈도우 원격접속) 등이 있습니다.



OS 자동로그온

웹에서 사용자 인증을 통하여
접속 가능한 서버와 프로토콜 목록으로 이동

DBSAFER User jhryu [192.168.3.89] | 환경설정 | 로그아웃

서버 < DBSAFER 사용자 >

검색

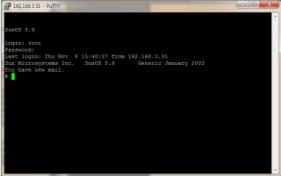
서버명: IP: 운영체제: **전체**

새로고침

Index	서버명	IP	운영체제	용도	SSH	Telnet	FTP	RDP
1	NEW_192.168.2.135	192.168.2.135	Linux	개발	SSH	TELNET	FTP	RDP
2	AIX 5.1 x64	192.168.3.144	AIX	개발	SSH	TELNET	FTP	RDP
3	HP-LUX 11.23 PA	192.168.3.143	HP-LUX	개발	SSH	TELNET	FTP	RDP
4	HP-LUX 11.23 IA	192.168.3.140	HP-LUX	개발	SSH	TELNET	FTP	RDP
5	Linux_192.168.3.132	192.168.3.132	Linux	개발	SSH	TELNET	FTP	RDP
6	NEW_192.168.3.135	192.168.3.135	Linux	개발	SSH	TELNET	FTP	RDP

**클릭을 통하여
자동로그온**

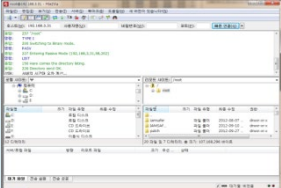
OS로그온 결과 화면



[TELNET / SSH 접속]



[윈도우터미널 접속]



[FTP / SFTP 접속]

WEB 브라우저를 통한 자동 접속 관리

3. SYSTEM 접근제어 기능 / II. 솔루션 소개

사용자에게 접속 가능한 서버 리스트만을 리스트 형태로 나타내며, 가능한 서비스를 선택 후 자동 접속합니다. 이 때 사용자는 자신의 비밀번호를 노출시키지 않게 되어, 계정 도용의 위험으로부터 최소화합니다. 접속 선택 시 사용할 접속 어플리케이션의 설정 변경을 제공한다.

The screenshot displays the DBSAFER User interface. At the top, it shows the user 'dbsafer [192.168.3.116]' and navigation options like '환경설정' and '로그아웃'. Below this is a table of servers with columns for '서버' (Server), '계정' (Account), and '용도' (Usage). The table lists two servers: 'NEW_192.168.6.157' and another server with IP '192.168.6.157' and OS 'Linux'. A red dashed box highlights the '용도' column, and a red arrow points to a terminal window showing a successful login for the selected server.

Below the table, there are sections for '내 정보 수정' (Edit My Info) and '어플리케이션 경로설정' (Application Path Setting). The '어플리케이션 경로설정' section includes fields for SSH, TELNET, and FTP protocols, each with a dropdown menu and a file path. The SSH and TELNET paths are set to 'C:\Users\iamlove7\Desktop\putty.exe', and the FTP path is set to 'FileZilla'. There are '적용' (Apply) and '초기화' (Reset) buttons. To the right, there is a section for '어플리케이션 다운로드' (Application Download) with icons for 'iPutty v0.60h' and 'FileZilla v3.5.3'.

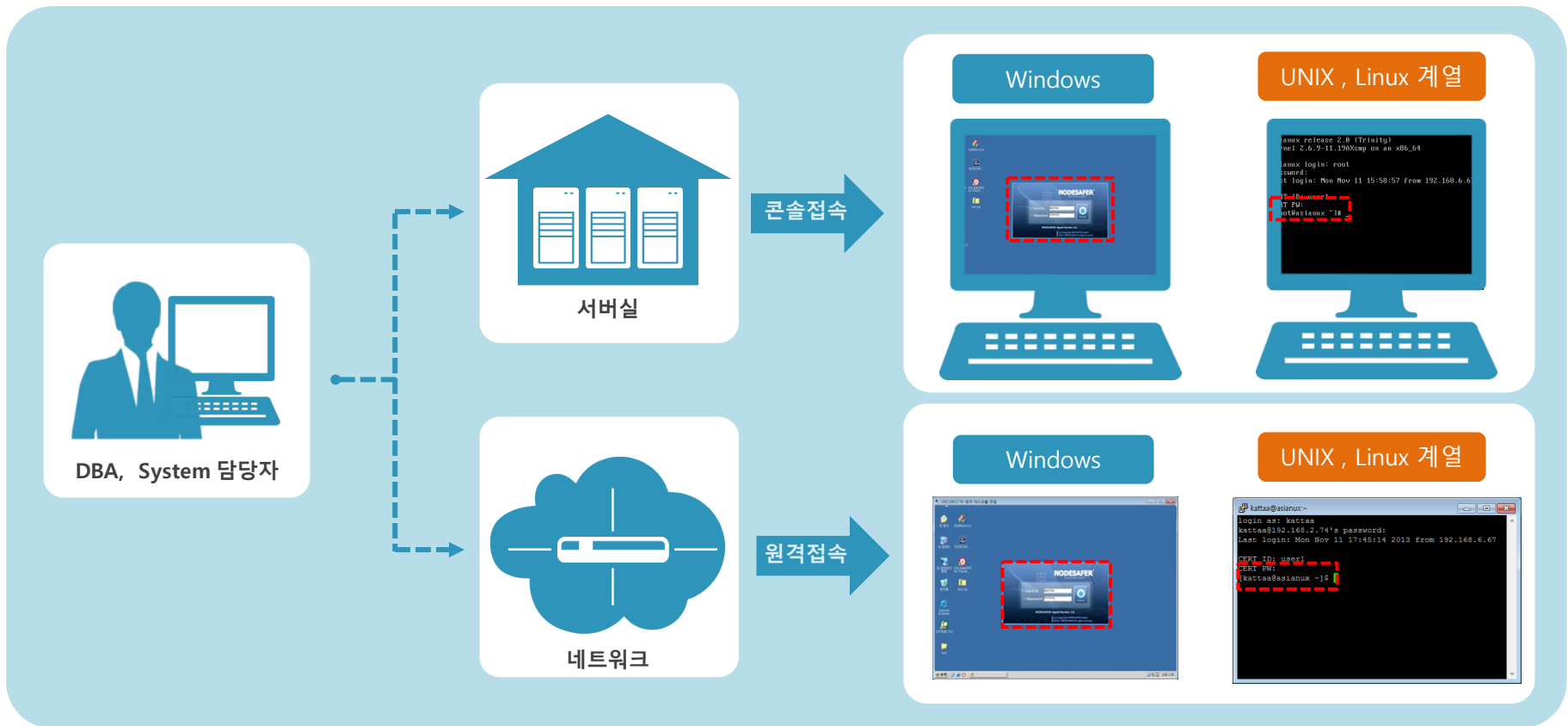
[접근 가능한 서버 선택 후 로그인 한 화면]

[접근 어플리케이션 관리 화면]

서버실내 콘솔접근에 대한 제어

3. SYSTEM접근제어 기능 / II. 솔루션 소개

원격 접속 및 서버실 내에서의 보안대상 시스템에 접근할 경우에 보안계정 로그인을 통한 제어기능을 제공합니다.
보안대상시스템에 접근하기 위해서 우선 OS에 대한 인증이 되어야 하며, 다시 한번 콘솔접근을 위한 DBSAFER 사용자 인증이 필요합니다.



스크립트 파일 제어 | 3. SYSTEM접근제어 기능 / II. 솔루션 소개

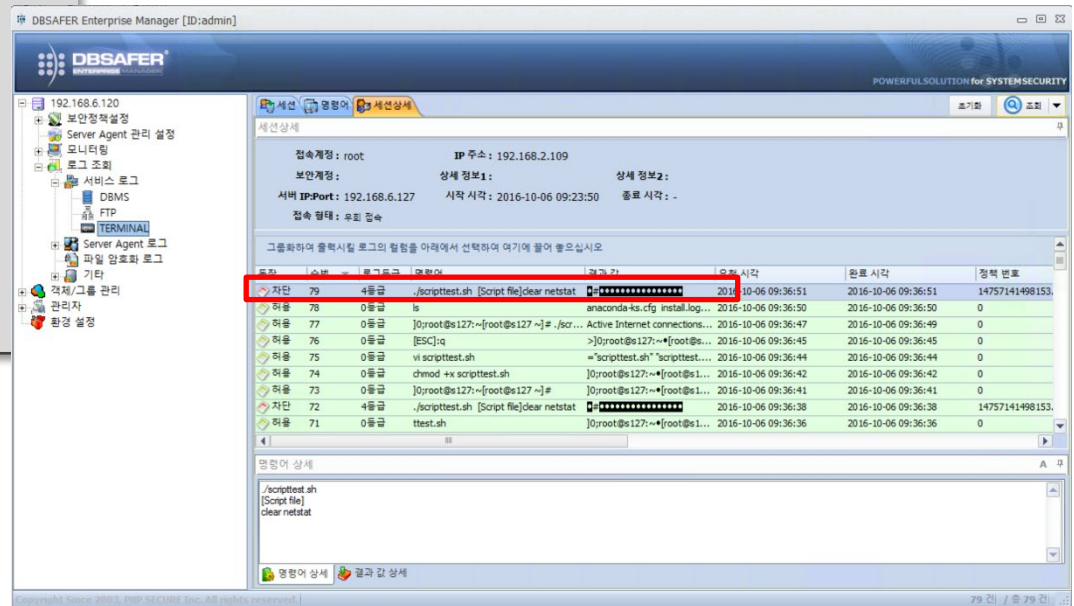
사용자가 실행한 스크립트 파일의 내용을 분석하여 정책을 적용하는 기능을 제공
 (예, 차단대상 명령어가 실행하는 스크립트에 포함되어 있을 경우 스크립트를 실행하지 못하도록 차단함)

```
[root@DBSAFER ~]# cat scripttest.sh
clear
netstat
[root@DBSAFER ~]# ./scripttest.sh

TELNET SERVICE DENY (Command)
Please check your permission.....

[root@DBSAFER ~]# _
```

[스크립트 파일 제어 결과 화면]

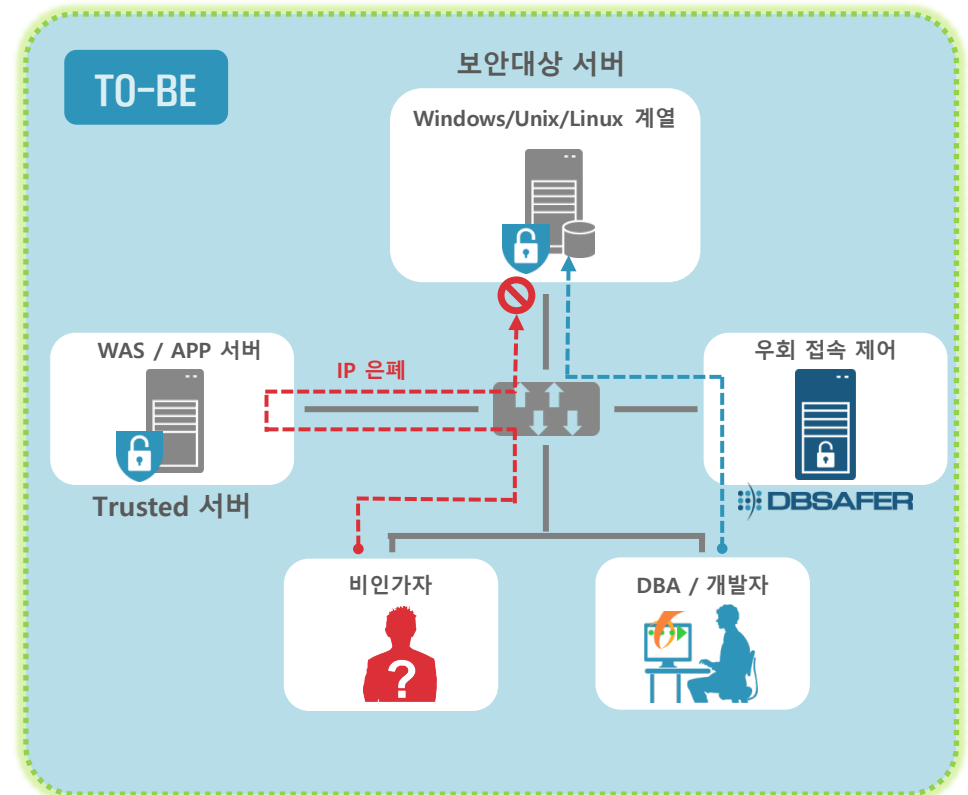
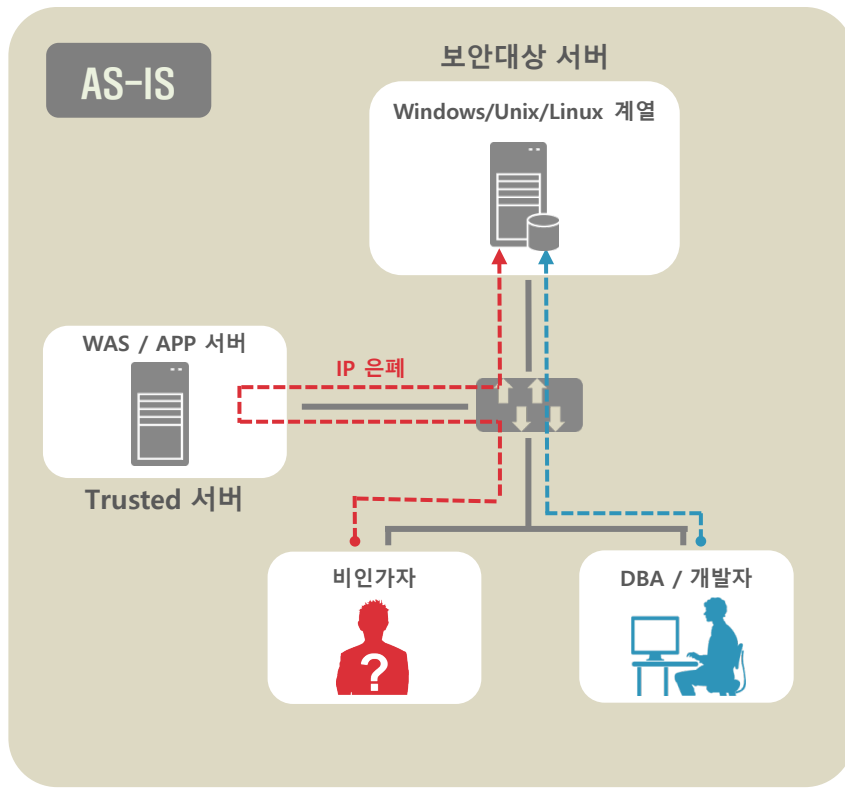


[스크립트 파일 제어 로그 화면]

우회 접속(서버 경유한 IP은폐) 제어

3. SYSTEM접근제어 기능 / II. 솔루션 소개

보안을 우회하기 위한 목적으로 서버를 경유하며 IP를 은폐한 접근에 대하여 DBSAFER Enterprise는 출발지 IP를 인식하여 제어 및 로깅 기능을 제공합니다.



우회 접속(서버 경유한 IP은폐) 경로 추적 | 3. SYSTEM접근제어 기능 / II. 솔루션 소개

사용자가 여러 대의 서버를 거쳐 접속을 한 경우, 접속한 경로와 실제 최초 접속 정보를 제공함.

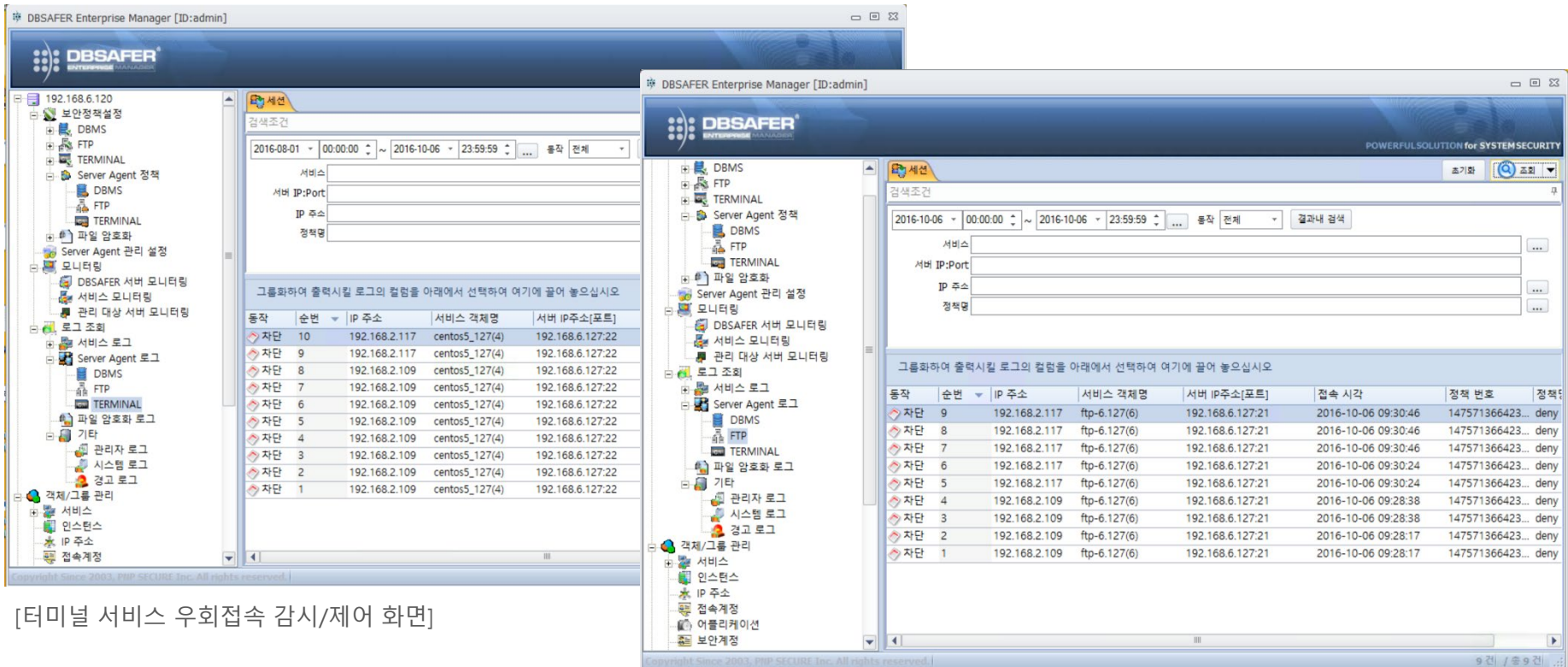
The diagram 'ShellTracer v1.0' illustrates the network path for a shell session. It shows a Client (192.168.3.79) connecting to a target R&D server (192.168.3.130) through a central Network cloud. The path involves a DBSAFER device in the Network segment (labeled '1') and another DBSAFER device in the R&D segment (labeled '2'). The connection methods shown are 'Inline', 'Proxy', and 'Port mirroring'. The Client IP is 192.168.3.79 and the Target IP is 192.168.3.130. The Network segment also contains WAS and DBMS servers, with the DBMS server IP being 192.168.2.134.

[우회 접속 경로 추적 화면]

[우회 접속 경로 추적 화면(자동생성됨)]

우회접속 감시/제어 | 3. SYSTEM접근제어 기능 / II. 솔루션 소개

보안서버를 우회하여 이루어진 접속을 제어하는 기능으로 세션 기반의 접근제어를 제공하며, 스니핑 방식과 프로세스 방식을 모두 제공함.



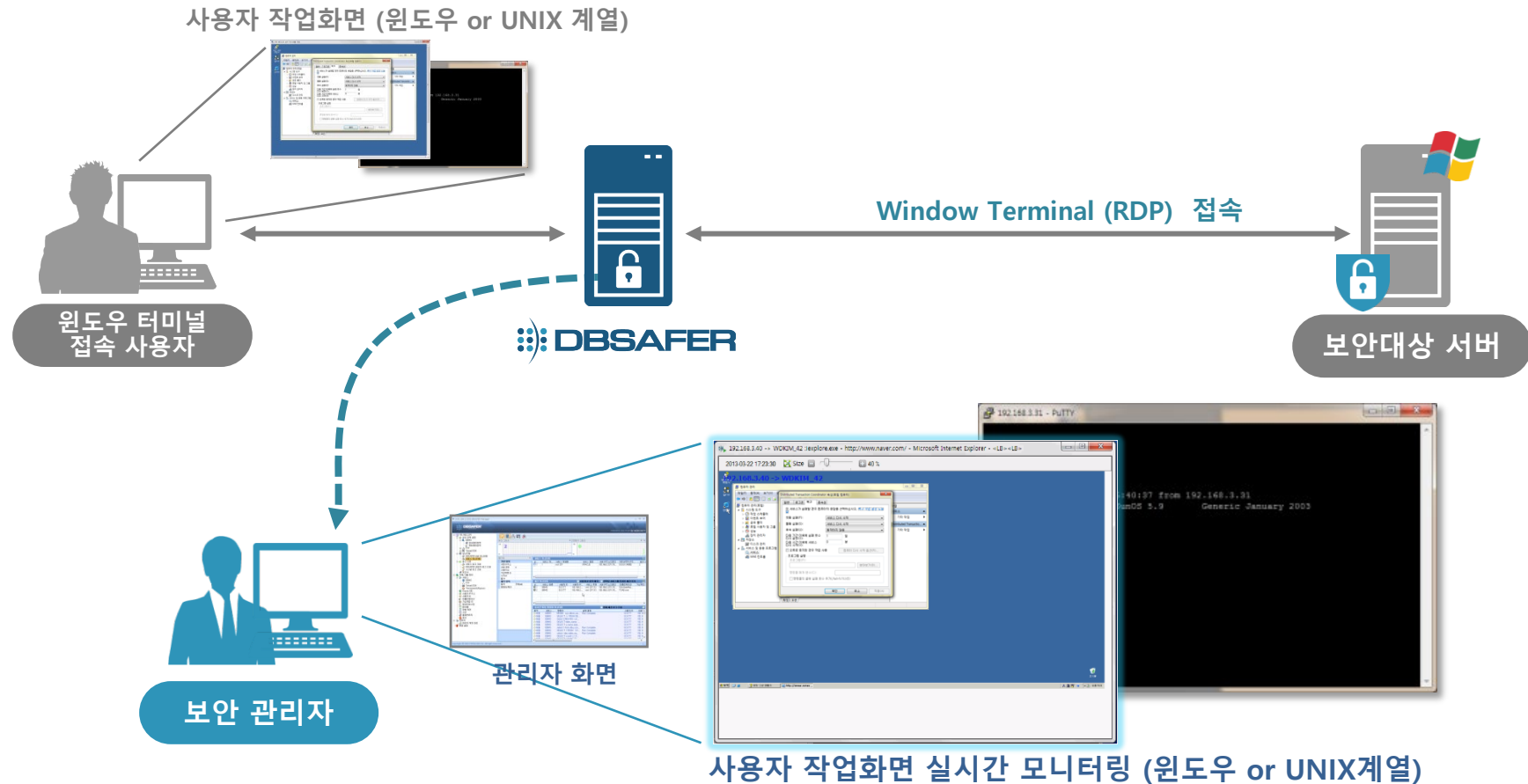
[터미널 서비스 우회접속 감시/제어 화면]

[파일전송 서비스 우회접속 감시/제어 화면]

원격접근 실시간 모니터링

3. SYSTEM접근제어 기능 / II. 솔루션 소개

보안대상 서버에 윈도우 터미널 서비스(RDP)로 접속하여 수행하는 업무에 대하여 관리자는 로그조회 뿐만 아니라 사용자와 동일한 보는 화면과 동일한 화면을 실시간 모니터링을 할 수 있도록 기능을 제공합니다.



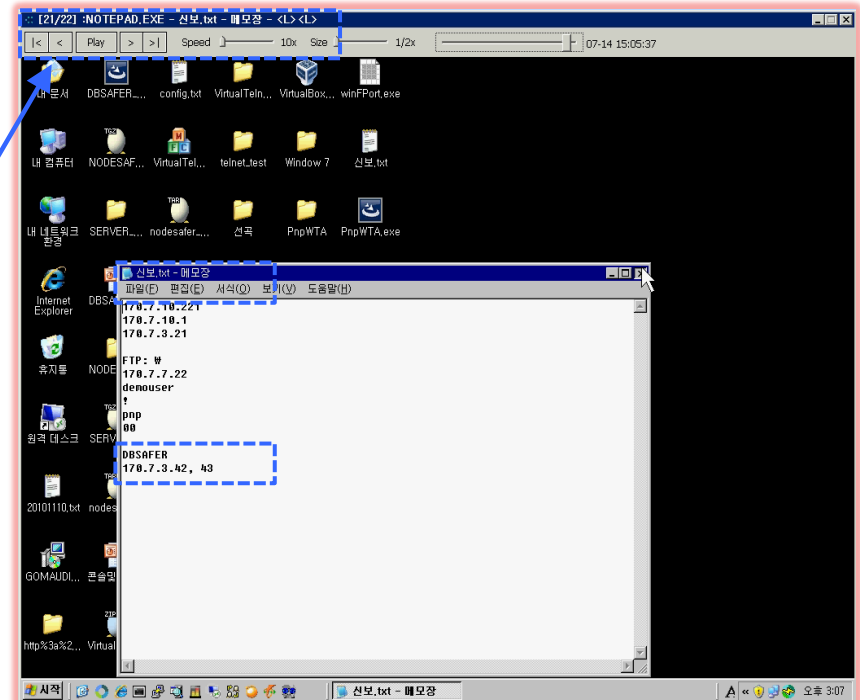
원격접근 이력 재현 및 메타 검색 3. SYSTEM접근제어 기능 / II. 솔루션 소개

Windows Terminal(RDP), TELNET/SSH, Console등의 접속 로그에 대해

- ✓ 사용자 화면과 동일한 화면을 재현하는 기능을 제공.
- ✓ 보안사고시 검색이 가능하도록 메타 검색 기능을 제공.
- ✓ 저장 시에 로그양을 최소화 하기 위한 이미지 압축 알고리즘 적용.



[Windows 감사 로그를 메타데이터로 조회하여 바로 원하는 화면을 검색하여 조회기능 제공]



[Windows 원격 접속 Replay 위치 추적]

타 인증 시스템[스마트 카드, 전화인증, OTP]과의 2-factor 인증 지원 | 3. SYSTEM접근제어 기능 / II. 솔루션 소개

스마트 카드, 전화 인증, OTP와 같은 타 인증 매체와의 2-factor 인증을 제공 함으로써 시스템 접근에 대한 보안을 강화할 수 있습니다. 현재 2-factor 인증은 전화인증, OTP 인증 기능을 타사에 적용되어 운영되고 있습니다.

The image displays the DBSAFFER configuration interface for terminal access control. The main window, titled 'TERMINAL 권한제어정책', shows the configuration for a policy named 'TELNET_AUTH_REQUEST_DECIDE_#2'. Under the '정책 동작' (Policy Action) section, the '2-factor 인증 대기시간(초)' (2-factor authentication wait time in seconds) is set to 180 seconds, which is highlighted with a red box. Other settings include '동작' (Action) set to '결재 결과에 따름로그 (4등급)' and '결재 대기 시간' (Queue wait time) set to 5 seconds. An inset dialog box titled '사용자 승인' (User Approval) is shown, indicating the target server is 'Oracle10g' with IP '192.168.2.237'. The user ID is 'dwpark' and the OTP generation number is blank. The dialog also shows a remaining authentication time of 113 seconds and buttons for '확인' (Confirm) and '취소' (Cancel).

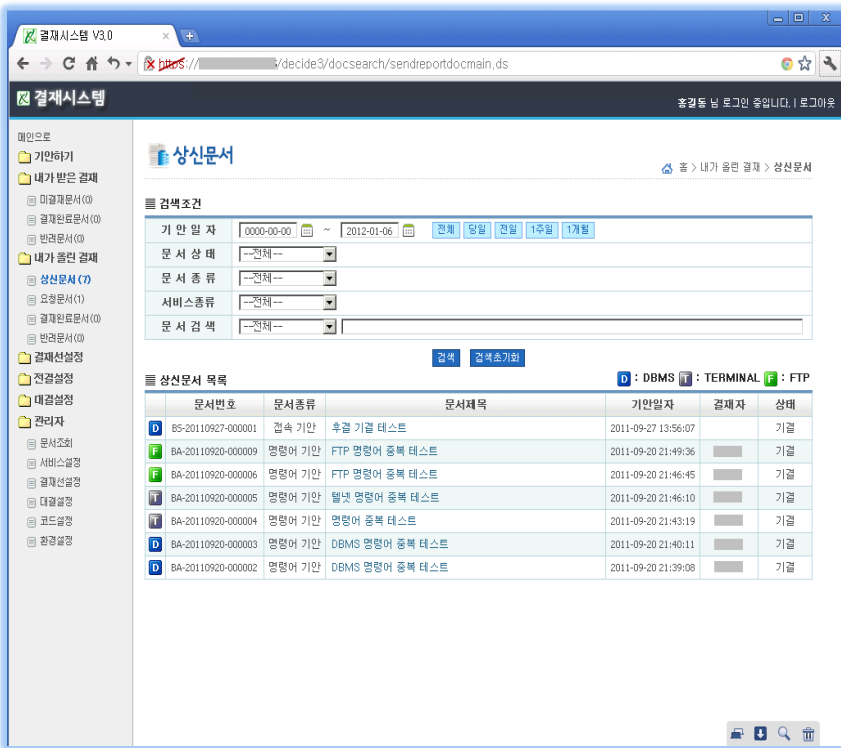
[2-factor 인증 정책 설정 및 로그인 시도 시 2-factor 인증 요청 화면]

명령어 결재 기능

3. SYSTEM접근제어 기능 / II. 솔루션 소개

사용자가 승인이 필요한 명령어를 실행한 경우 (TELNET, SSH, FTP, SFTP)

- > 사용하는 툴에 관계없이 자동으로 사용요청 화면이 나타나며
- > 명령어 실행이 필요한 경우 요건을 입력하여 승인을 요청하며
- > 결재에 의해서 실행 권한을 획득 후 명령 실행.



[명령어 사용을 요청하는 기안 문서 작성 화면]



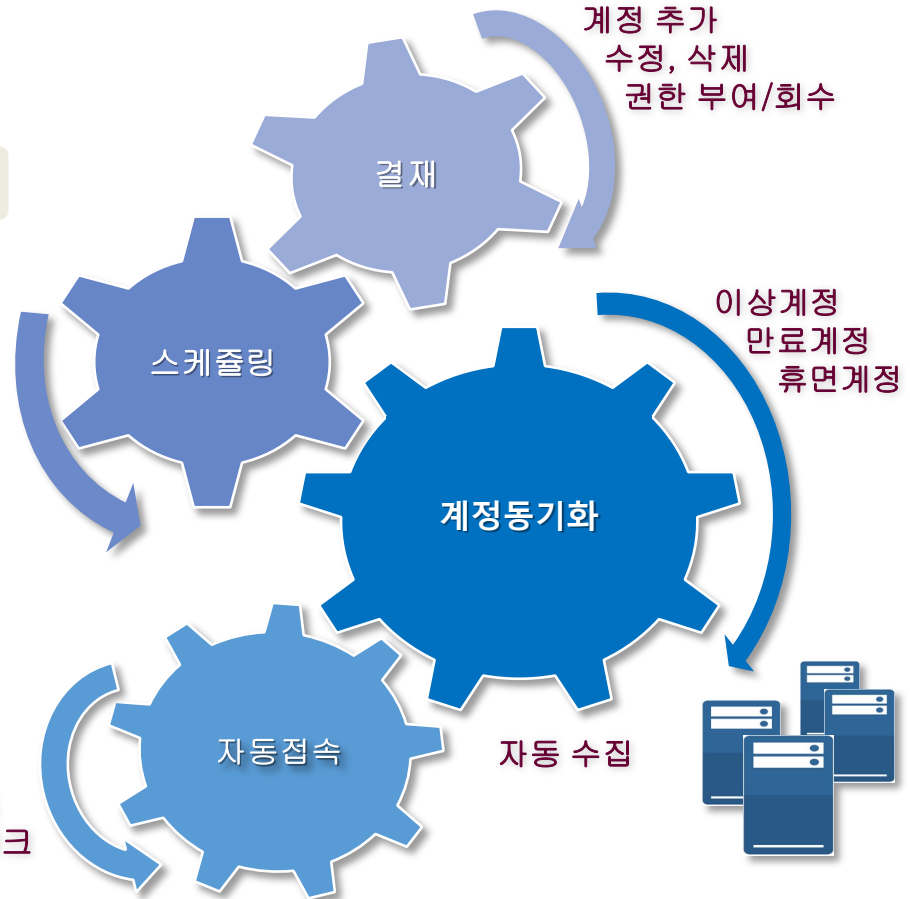
[명령어 사용을 요청한 상신 목록 화면]

통합 계정 관리 주요 기능

4. 통합 계정 관리 기능 / II. 솔루션 소개

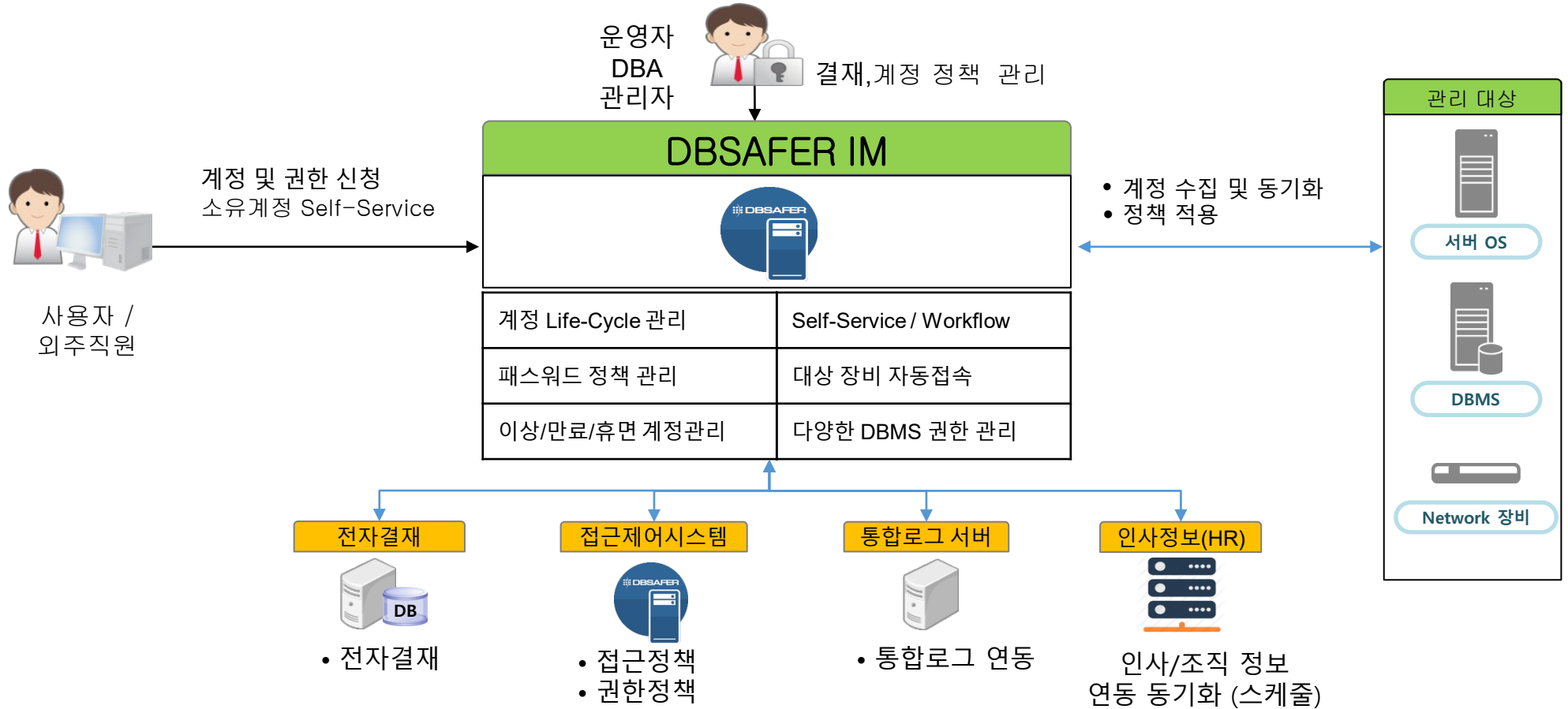
다수의 서버에 산재하는 시스템 OS 계정 및 DBMS 계정에 대한 Life-Cycle을 중앙에서 통합 관리한다. (상세자료: **별도 제품소개서 참조**)

- 1 여러 이 기종 장비의 계정 통합 관리
- 2 비밀번호 자동 변경 및 계정 자동 수집
- 3 결재를 통한 계정 Life-Cycle 관리
- 4 유연한 비밀번호 정책 설정
- 5 이상/만료/휴면계정 관리
- 6 비밀번호 노출 없는 자동 접속
- 7 다양한 DBMS 계정권한 관리



통합 계정 관리 주요 기능 | 4. 통합 계정 관리 기능 / II. 솔루션 소개

다수의 서버에 산재하는 시스템 OS 계정 및 DBMS 계정에 대한 Life-Cycle을 중앙에서 통합 관리한다. (상세자료: **별도 제품소개서 참조**)

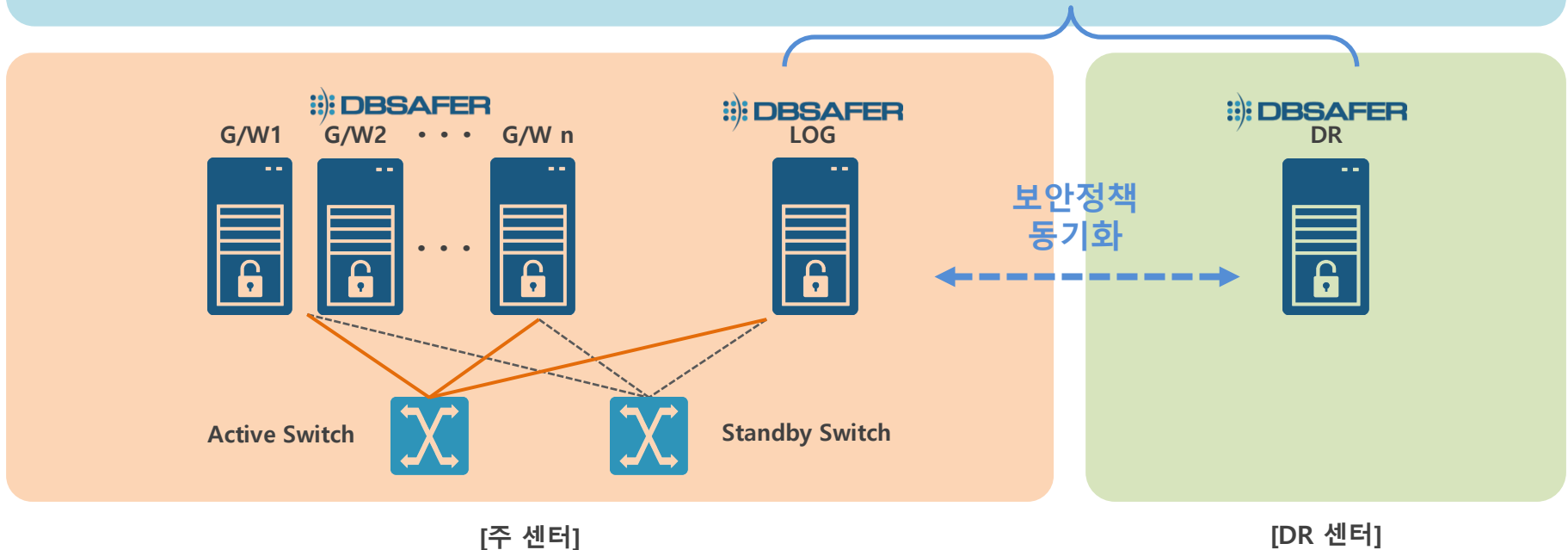


분산 환경 및 이중화 지원

5. 특징점 / II. 솔루션 소개

보안 **서비스의 연속성 제공을 위한 이중화**(Active-Active) 지원 및 DR 센터의 DBSAFER에 대해서 통합기능을 제공한다.
통합기능이란 정책/모니터링/로그에 대하여 Active된 다수의 DBSAFER를 한대의 DBSAFER 처럼 인식하는 기능으로 한번의 정책수정으로 모든 DBSAFER가 동기화되며 통합된 실시간 모니터링과 로그검색을 제공한다.

Active-Active 그룹구성지원과 DBSAFER를 그룹으로 지정한 경우 한번의 정책설정으로 **모든 DBSAFER에 정책이 적용되며 모니터링 및 로그 검색도 한 대의 DBSAFER처럼 동작한다.** 특히 **DR쪽의 DBSAFER가 이와 동일하게 동작하여 주센터 장애 시에도 DR DBSAFER에 의해서 모든 DB 접속이 보안장비를 통해서 운영이 가능하다.**



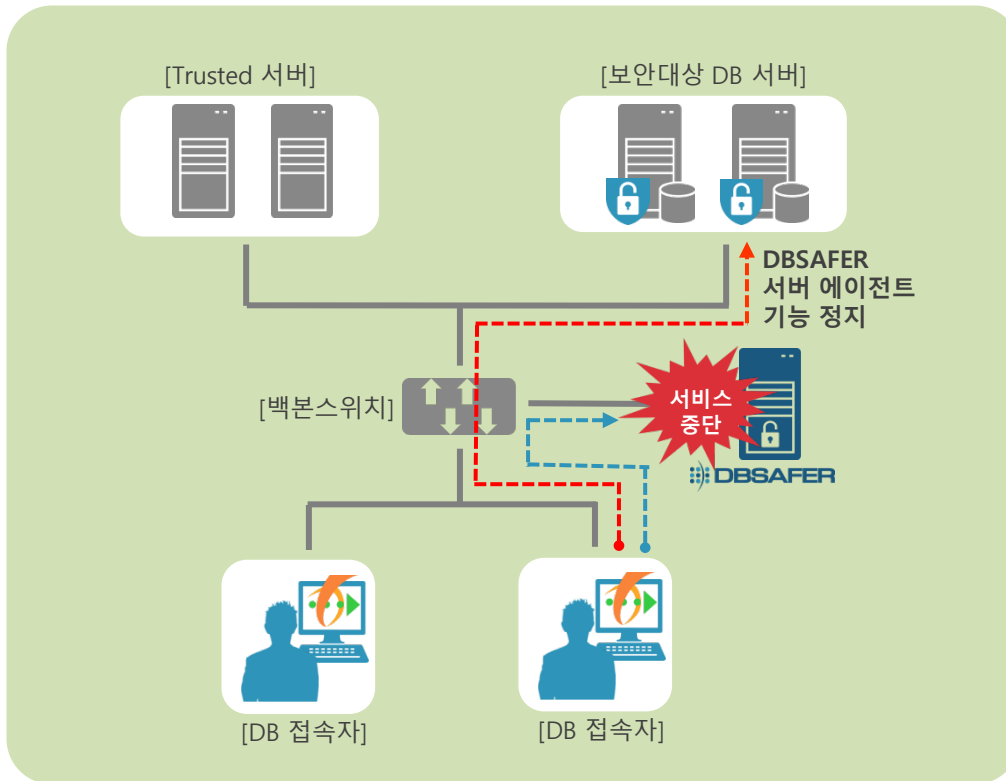
전수 로깅을 위한 사후감사 기능

5. 특징점 / II. 솔루션 소개

보안장비의 패치 또는 전원작업 및 만일에 있을 수 있는 서비스 중단 순간에는 제어를 못하게 됩니다.

그 순간에도 서버 또는 사용자 PC에 이력을 보관하여 보안장비 복구 시에 해당 순간의 로그를 기록하여 사후감사기능을 통하여 100% 전수 로깅합니다.

DBSAFER Enterprise 서버 장애 시 서비스 및 사용자에게 영향을 주지 않도록 Fail Open 기능도 지원합니다.

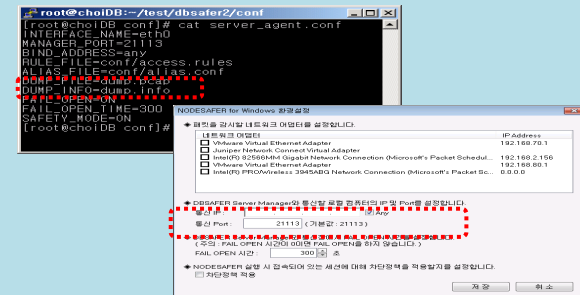


구성 설명

✓ 서비스 중단 시 동작 방식

- **보안중요시** : 서비스 재가동까지 비정형쿼리 사용자(개발자, DBA)는 접속이 불가함
- **업무중요시** : 제어는 되지 않지만 업무를 위해 Fail-Open 후 사후감사 기능사용

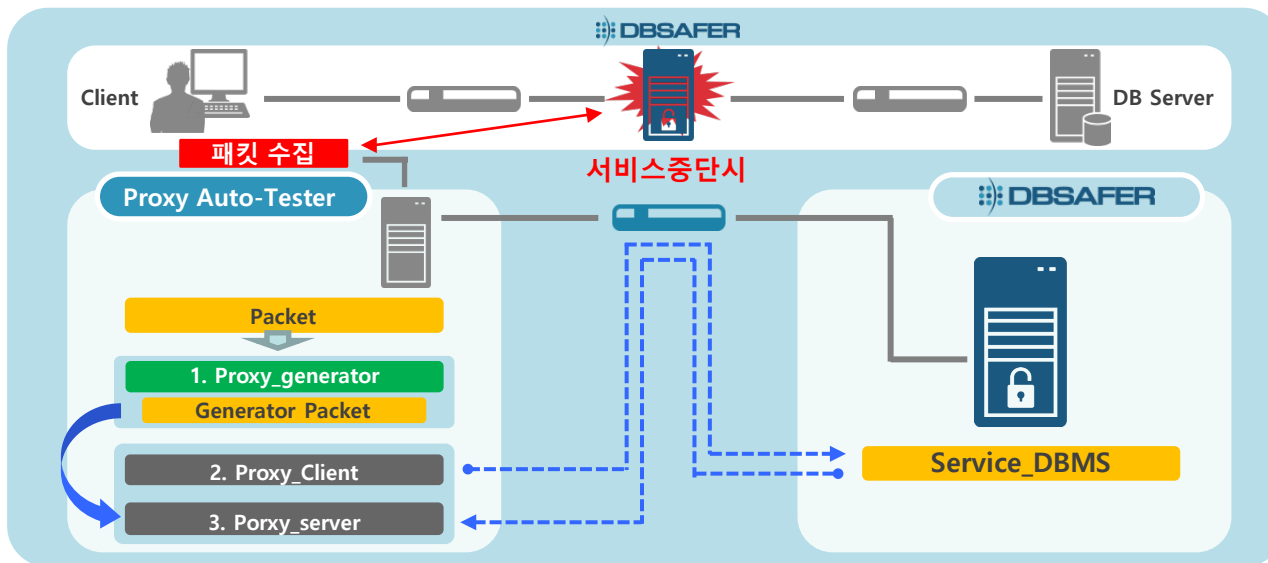
✓ 설정 화면



장애 예방 및 재발방지

5. 특징점 / II. 솔루션 소개

Gateway(Proxy)모듈에 대한 자동화된 장애 예방 및 재발방지 프로그램을 개발(Proxy Auto-Tester)하여 중요시스템에 대한 사전 장애 감지 및 장애 발생시 동일한 장애 발생을 원천적으로 봉쇄할 수 있어 대형 고객사의 Gateway(Proxy)방식 선정의 기준입니다. 장애상황을 패킷 기반으로 기록 후 시뮬레이션 함으로써 구조적인 해결책을 제시합니다.



- 서비스 장애 발생시 관련 패킷을 수집
- 수집된 패킷을 Proxy Auto-Tester 프로그램을 통해 장애 재현을 통한 빠른 장애 대응
- Proxy_Client에서 generator Packet을 전송하여, DBSAFER에 장애 상황을 재현 및 테스트

장애사전예방

1. 고객사의 현장 패킷을 현장에서 수집하여 실제 Gateway(Proxy)에서 실행하는 것과 동일하게 시뮬레이션을 실시할 수 있어 사전에 장애발생 여부를 확인 할 수 있다.
2. 수집한 패킷에 대해서 세션을 증폭 및 배속등을 설정할 수 있어 빠른 시간 내에 확인 가능

동일장애 재발방지

1. 장애 발생시 보안장비 내부의 Log나 Core파일로 Debugging 하는 방식이 아니라 장애가 발생한 패킷을 기반으로 모든 Bug를 테스트 할 수 있는 구조적인 해결책 제시가 가능

C O N T E N T S

III. 회사 소개

1. 일반현황 및 연혁
2. 품질인증
3. 레퍼런스

III. 회사 소개

1. 일반현황 및 연혁
2. 품질인증
3. 레퍼런스

일반현황 및 기업신용도

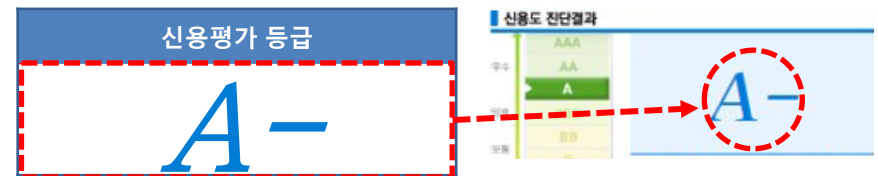
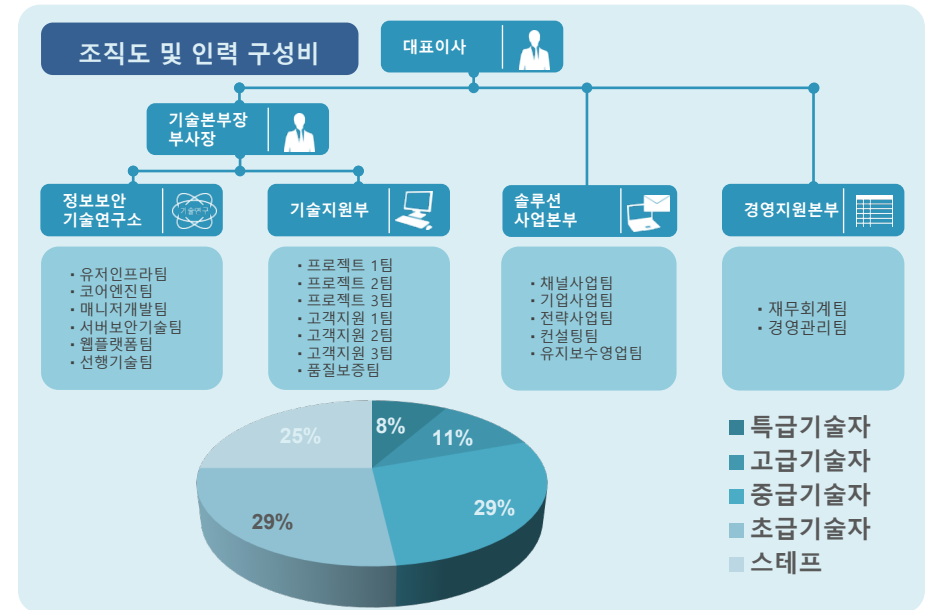
1. 일반현황 및 연혁 / III. 회사소개

(주)피앤피시큐어는 국내 DB, 시스템 보안을 선도하는 No1. 통합접근제어 전문기업으로서 신용평가등급은 "A-"로 동종업계 최상위 수준이며, 2018년에는 접근제어 제품만의 매출이 278억을 돌파하였습니다.

법인명	(주) 피앤피시큐어		대표자	박 천 오
주소	경기도 성남시 분당구 대왕판교로 645번길 16 플레이뮤지엄 5층 www.pnpsecure.com			
전화번호	1670-9295			
사업분야	데이터베이스 보안 솔루션 사업 클라우드 통합 보안 솔루션 사업			
설립연도	2003년 12월			
해당부문 사업기간	2003년 12월 ~ 2020년 2월 현재 (16년 2개월)			
보유인력 현황	기술	개발인력 : 39명 기술지원인력 : 59명	총원 : 124명	
	관리	영업인력 : 18명 관리 및 지원 : 8명		
신용등급	A-		2018년 매출	약 278억

✓ 접근제어 제품만의 매출액[최근 3년]

구 분	2016년	2017년	2018년
총자산	313억	317억	543억
당기순이익	62억	86억	116억
매출액	220억	253억	278억



1. 회사 일반 현황

회사연혁

(주)피앤피시큐어는 정보보안 전문가와 개발자들이 모여 세계 최고의 정보보안 솔루션을 개발·공급하고자 설립되었습니다. 오늘날 세계시장은 네트워크 환경을 기반으로 한 E-Business를 경쟁적으로 확대함으로써 새로운 정보보안 시장을 형성해가고 있습니다. 이에 (주)피앤피시큐어는 전 세계의 정보보안 표준으로 신뢰할 수 있는 솔루션을 개발·공급하는 기업으로 나아가고 있습니다.

주요연혁	
2001년	• [제품개발 착수] DBSAFER개발
2003년	• [법인설립] (주)피앤피시큐어 설립
	• [제품출시] 국내 최초의 <게이트웨이 방식의 DB보안프로그램> DBSAFER V1.0
2004년	• [연구개발사업] 게이트웨이 방식의 데이터베이스보안 프로그램 개발
	• [정보통신우수신기술 선정] 정보통신부 지정
	• [프로그램 등록] <DBSAFER v1.2>
	• [소프트웨어사업자 등록] 한국 소프트웨어산업협회
2005년	• [제품출시] DBSAFER V1.5
	• [기업부설연구소 설립] 등록완료
	• [IT마크 획득] 정보통신 우수신기술
	• [히트상품 선정] 전자신문 2005년 상반기
	• [신 소프트웨어 대상] 7월 3주 추천작 선정
	• [신제품인증(NEP)] <게이트웨이 방식의 데이터베이스 보안 소프트웨어> 신제품인증서 획득
2006년	• [보안적 합성검증] <DBSAFER V2.0> 국가정보원 국가용 정보보호시스템 보안적합성 검증필 획득
	• [GS인증획득] <DBSAFER V2.0> 소프트웨어 품질인증 획득
	• [특허등록] <데이터베이스 감시 및 보안방법 및 장치>
	• [연구개발사업] SQL Query 결재 프로그램 개발

주요연혁	
2007년	• [인증획득] 벤처기업인증, 이노비즈기업 선정
	• [중소기업 선정 및 협약] 산업보안기술개발사업업체
	• [특허등록] <TCP/IP 기반의 주소변경 방법 및 장치>
	• [프로그램등록] <DBSAFER v2.0>
	• [프로그램등록] <DECIDE v2.0>
	• [연구개발사업] Client단에서의 Protocol Redirection을 통한 중앙제어시스템 개발
2008년	• [연구개발사업] 중소기업을 위한 일체형 DB보안 어플라이언스 개발
	• [사옥이전] 문래동 사옥으로 이전
	• [특허등록] <데이터 마스킹을 이용한 보안 시스템과 이를 이용한 데이터보안 방법>
2009년	• [연구개발사업] 데이터 마스킹 처리 DB보안 어플라이언스 개발
	• [인증획득] ISO9001, ISO14001 인증획득
	• [신기술인증(NET)] <네트워크보안시스템의 가용성보장을 위한 패킷제어 모듈 및 장치 기술>
	• [GS인증획득] <DBSAFER V3.0> 소프트웨어 품질인증 획득
	• [CC인증획득] <DBSAFER, v3.0(보증등급: EAL2)> 국제공통평가기준(CC) 인증 획득
• [특허등록] <보안장치 장애로부터 네트워크의 안정된 통신상태를 보장하는 통신 시스템>	

1. 회사 일반 현황

회사연혁

(주)피앤피시큐어는 정보보안 전문가와 개발자들이 모여 세계 최고의 정보보안 솔루션을 개발·공급하고자 설립되었습니다. 오늘날 세계시장은 네트워크 환경을 기반으로 한 E-Business를 경쟁적으로 확대함으로써 새로운 정보보안 시장을 형성해가고 있습니다. 이에 (주)피앤피시큐어는 전 세계의 정보보안 표준으로 신뢰할 수 있는 솔루션을 개발·공급하는 기업으로 나아가고 있습니다.

주요연혁	
2009년	• [프로그램등록] <DBSAFER v3.0>
	• [프로그램등록] <DBSAFER DMS v2.0>
	• [프로그램등록] <NODESAFER v2.0>
	• [프로그램등록] <WASSAFER v4.0>
	• [자본금 증자] 5억 증자
2010년	• [제품출시] <NODESAFER> V3.0출시
	• [위탁과제] 중소기업용 고객정보 DB대량유출방지 기술연구
	• [연구개발사업] TTP 기술을 이용한 고가용성 보안 Proxy 기술개발
	• [연구개발사업] 중소기업 내 중요 데이터의 보안을 위한 지능형 보안분석기술 개발
	• [GS인증획득] <WASSAFER V4.0> 소프트웨어 품질 인증 획득
	• [CC인증획득] <WASSAFER V4.0(보증등급: EAL2)> 국제공통평가기준(CC) 인증 획득
• [자본금 증자] 10억 증자	
2011년	• [제품출시] <NODESAFER> V4.0출시
	• [병역특례 업체지정] 병역 특례업체
	• [특허등록] <가용성보장을 위한 프록시 기반의 보안시스템>
	• [해외특허등록] <Method and apparatus for redirecting based on TCP/IP> 일본 특허 등록

주요연혁	
2011년	• [특허등록] <SSH 통신환경의 암호화된 데이터 탐지시스템과 탐지 방법>
	• [특허등록] <질의어 변경을 통한 중요정보 보안 시스템 및 방법>
	• [특허등록] <데이터베이스 검출시스템과 이를 이용한 검출방법>
	• [프로그램등록] <NODESAFER v3.0>
	• [산업기술보호의 날] 지식경제부장관상 수상(백순용 연구소장)
2012년	• [신기술실용화 표창] 지식경제부장관상 수상(박천오 대표이사)
	• [발명의 날 포상] 발명진흥회장상 수상(박천오 대표이사)
	• [특허등록] <데이터베이스로의 우회접근을 방지하는 데이터베이스 보안 시스템>
2012년	• [특허등록] <네트워크 보안을 위한 접속경로 추적시스템과 추적방법>
	• [특허등록] <접속자의 식별 신뢰도를 높은 프록시 기반의 서버보안방법과 보안 시스템>
	• [면허취득] <정보통신공사업>
	• [모범중소기업인표창] 산업통상자원부장관상 수상(박천오 대표이사)
2013년	• [장영실상 수상] 박천오 대표이사, 정보보안기술연구소 백순용 연구소장 진선태 수석, 박대원 수석
	• [모범중소기업인표창] 산업통상자원부장관상 수상(박천오 대표이사)

1. 회사 일반 현황

회사연혁

(주)피앤피시큐어는 정보보안 전문가와 개발자들이 모여 세계 최고의 정보보안 솔루션을 개발·공급하고자 설립되었습니다. 오늘날 세계시장은 네트워크 환경을 기반으로 한 E-Business를 경쟁적으로 확대함으로써 새로운 정보보안 시장을 형성해가고 있습니다. 이에 (주)피앤피시큐어는 전 세계의 정보보안 표준으로 신뢰할 수 있는 솔루션을 개발·공급하는 기업으로 나아가고 있습니다.

주요연혁	
2014년	· [업체지정] 서울시우수기업브랜드
	· [국제청장 표창] <모범납세자> 수상
	· [GS인증] <DBSAFER Enterprise V5.0> 소프트웨어 품질인증 획득
	· [CC인증] <DBSAFER Enterprise V5.0(보증등급: EAL4)> 국제공통평가기준(CC) 인증 획득
	· [특허등록] <프록시를 경유한 접속 세션정보 확인시스템과 이를 기반으로 한 세션 정보 확인방법>
	· [특허등록] <스크립트에 의한 서버작업 식별시스템과 이를 이용한 식별방법>
	· [인수합병] 2014년 7월 NHN엔터테인먼트의 자회사 편입
2015년	· [특허등록] <통신 암호화를 통한 보안시스템 및 보안방법>
	· [사옥이전] 경기도 성남시 분당구 삼평동 플레이뮤지엄 입주
	· [특허등록] <리눅스 커널 기반의 파일 접근 제어시스템과 제어방법>
	· [기업등록] 중견기업등록
2016년	· [특허등록] <암호문의 편집을 통한 원문 해독 방지방법과 방지시스템>
	· [수상] 적십자회원 유공장 은장수여
	· [인증] 2016년 청년 친화 강소기업 선정
2016년	· [프로그램등록] <INFOSAFER v1.1>

주요연혁	
2016년	· [프로그램등록] <QueryBox V2.0>
	· [프로그램등록] <QueryBox-S V2.0>
	· [프로그램등록] <DATACrypto V1.0>
	· [GS인증] <INFOSAFER V1.1> 소프트웨어 품질인증 1등급 획득
	· [소프트웨어 무료 배포] DB 성능관리 및 개발 도구 <QueryBox> 무료배포
	· [미래창조과학부 장관표창] 2016 S/W산업발전 유공자 표창 (박천오 대표이사)
	· [수상] 적십자회원 유공장 금장수여
2017년	· [상표등록] QueryBox-SAFER
	· [상표등록] QueryBox
	· [저작권등록] DATACrypto V3.0
	· [특허등록] <프로세스 동작 추적을 통한 AP서버의 보안 게이트웨이 자동 전환 시스템과 전환방법>
	· [GS인증] <DATACrypto V3.0> 소프트웨어 품질인증 1등급 획득
2018년	· [인증] 2018년 청년 친화 강소기업 선정
	· [상표등록] DATACrypto

1. 회사 일반 현황

회사연혁

(주)피앤피시큐어는 정보보안 전문가와 개발자들이 모여 세계 최고의 정보보안 솔루션을 개발·공급하고자 설립되었습니다. 오늘날 세계시장은 네트워크 환경을 기반으로 한 E-Business를 경쟁적으로 확대함으로써 새로운 정보보안 시장을 형성해가고 있습니다. 이에 (주)피앤피시큐어는 전 세계의 정보보안 표준으로 신뢰할 수 있는 솔루션을 개발·공급하는 기업으로 나아가고 있습니다.

주요연혁	
2018년	· [특허등록] <원격서버작업 식별을 통한 서버 보안시스템과 이를 이용한 보안 방법>
	· [대통령 표창] 2018년 과학·정보통신의 날(박천오 대표이사)
	· [수상] 2018년 과학기술진흥유공자 장관표창 (진선태 부사장)
	· [인증] 국가정보원 암호모듈 검증필 DATACrypto V3.0
	· [국무총리 표창] 2018년 신기술, 신제품 실용화 유공기업
	· [수상] 2018 ICT대상 ICT 혁신 / 복지 부분 장관 표창
	· [수상] 서울시 정보보호체계 공로상 시장 표창
2019년	· [CC인증] <INFOSAFER V1.1(보증등급: EAL3)> 국제공통평가기준(CC) 인증 획득
	· [특허등록] <네트워크 보안 상황에 대한 시각화 모니터링 시스템과 이를 이용한 모니터링 방법>
	· [특허등록] <접근 제어 제어를 위한 Role_Rule 기반 정책의 혼용 방법과 시스템>
	· [특허등록] <프록시를 경유한 접속 세션 확인시스템과 방법>

2. 주요 원천기술 보유현황 주요 보유기술

(주)피엔피시큐어는 보안관련 원천기술에 대하여 다양한 국·내외 특허를 보유하고 있습니다.



특허내역	구분	등록	특허등록
데이터베이스 감시 및 보안방법 및 장치	국내특허등록	2006-06-20	제10-0593661호
데이터베이스 관리시스템의 결재방법 및 장치	국내특허출원	2006-12-20	제10-2006-130963호
TCP/IP 기반의 주소변경 방법 및 장치	국내특허등록	2007-12-27	제10-0791718호
데이터 마스킹을 이용한 보안 시스템과 이를 이용한 데이터보안 방법	국내특허등록	2008-04-01	제10-0820306호
가용성 보장을 위한 프록시 기반의 보안 시스템	국내특허등록	2011-03-31	제10-1027725호
SSH 통신환경의 암호화된 데이터 탐지시스템과 탐지 방법	국내특허등록	2011-06-03	제10-1040543호
질의어 변경을 통한 중요정보 보안 시스템 및 방법	국내특허등록	2011-09-26	제10-1069367호
데이터베이스 검출시스템과 이를 이용한 검출방법	국내특허등록	2011-11-08	제10-1083425호
Method and apparatus for redirecting based on TCP/IP	국제특허등록	2011-04-08	제4718638호
데이터베이스로의 우회접근을 방지하는 데이터베이스 보안시스템	국내특허등록	2012-03-30	제10-1134091호
네트워크 보안을 위한 접속경로 추적시스템과 추적방법	국내특허등록	2012-06-20	제10-1160219호
접속자의 식별 신뢰도를 높인 프록시 기반의 서버보안방법과 보안시스템	국내특허등록	2012-12-14	제10-1214613호
프록시를 경유한 접속 세션정보 확인시스템과 이를 기반으로 한 세션정보 확인방법	국내특허등록	2014-05-09	제10-1395830호
스크립트에 의한 서버작업 식별시스템과 이를 이용한 식별방법	국내특허등록	2014-06-16	제10-1410445호
통신 암호화를 통한 보안시스템 및 보안방법	국내특허등록	2014-10-01	제10-1448711호

2. 주요 원천기술 보유현황

주요 보유기술

(주)피앤피시큐어는 보안관련 원천기술에 대하여 다양한 국·내외 특허를 보유하고 있습니다.



특허내역	구분	등록	특허등록
리눅스 커널 기반의 파일 접근제어 시스템과 제어 방법	국내특허등록	2015-02-24	제10-1497629호
암호문의 편집을 통한 원문 해독 방지방법과 방지시스템	국내특허등록	2015-04-22	제10-1516751호
프로세스 동작 추적을 통한 AP서버의 보안 게이트웨이 자동 전환 시스템과 전환방법	국내특허등록	2017-07-28	제10-1764678호
원격서버작업 식별을 통한 서버 보안시스템과 이를 이용한 보안방법	국내특허등록	2018-03-22	제10-1843161호
네트워크 보안 상황에 대한 시각화 모니터링 시스템과 이를 이용한 모니터링 방법	국내특허등록	2019-04-29	제10-1975385호
접근 제어 제어를 위한 Role/Rule 기반 정책의 혼용 방법과 시스템	국내특허등록	2019-05-13	제10-1979915호
프록시를 경유한 접속 세션 확인시스템과 방법	국내특허등록	2019-05-15	제10-1980843호

2. 인증 획득 현황 | 주요 인증 현황

(주)피앤피시큐어는 CC인증, NET(신기술인증), NEP(신기술제품), IT우수제품 및 ISO 9001인증, ISO 14001 등의 다양한 인증을 보유하고 있습니다.



2. 인증 획득 현황 주요 인증 현황

(주)피엠피시큐어는 CC인증, NET(신기술인증), NEP(신기술제품), IT우수제품 및 ISO 9001인증, ISO 14001 등의 다양한 인증을 보유하고 있습니다.



3. 주요 고객사 현황

레퍼런스

은행권						
정부기관						
금융권						
통신/제조						
공사/공단						
인터넷기업						
유통						
병원/의료						
대학						
지방자치단체						
교육기관						

- ㈜피앤피시큐어의 주력 제품 DBSAFER는 국내 전체 시장의 60%를 점유함으로써 업계 1위의 위상을 이어가고 있습니다.
- 공공, 금융, 통신/제조, 유통, 의료 등 다양한 분야의 4,000여 고객사에서 안정적으로 운영 중입니다.

감사합니다.



총 판 : (주) 삼에스소프트

대표전화 : 031 - 212 - 3390 | 팩스 : 031 - 212 - 3345

(주)삼에스소프트 기술영업팀 | sales@3es.co.kr

<http://www.3es.co.kr>