SHIELDEX

문서방화벽을 통한 APT공격대응방법

Advanced Persistent Threat, 문서방화벽으로 막는다!

The power to do safely

소프트캠프 임성택 부장

SOFTCAMP

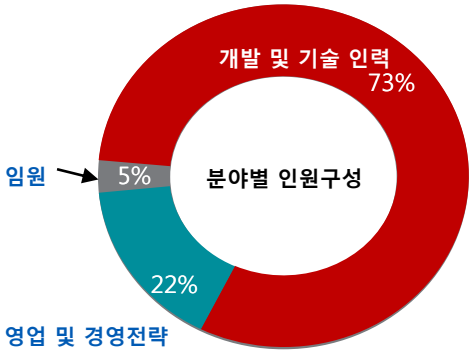
소프트캠프 소개

SHIELDEX

일반현황

회사명	소프트캠프
대표자	배 환 국
설립일자	1999년 7월 15일
사무실	서울 강남구 역삼동
지사	일본 지사(도쿄)

조직 현황



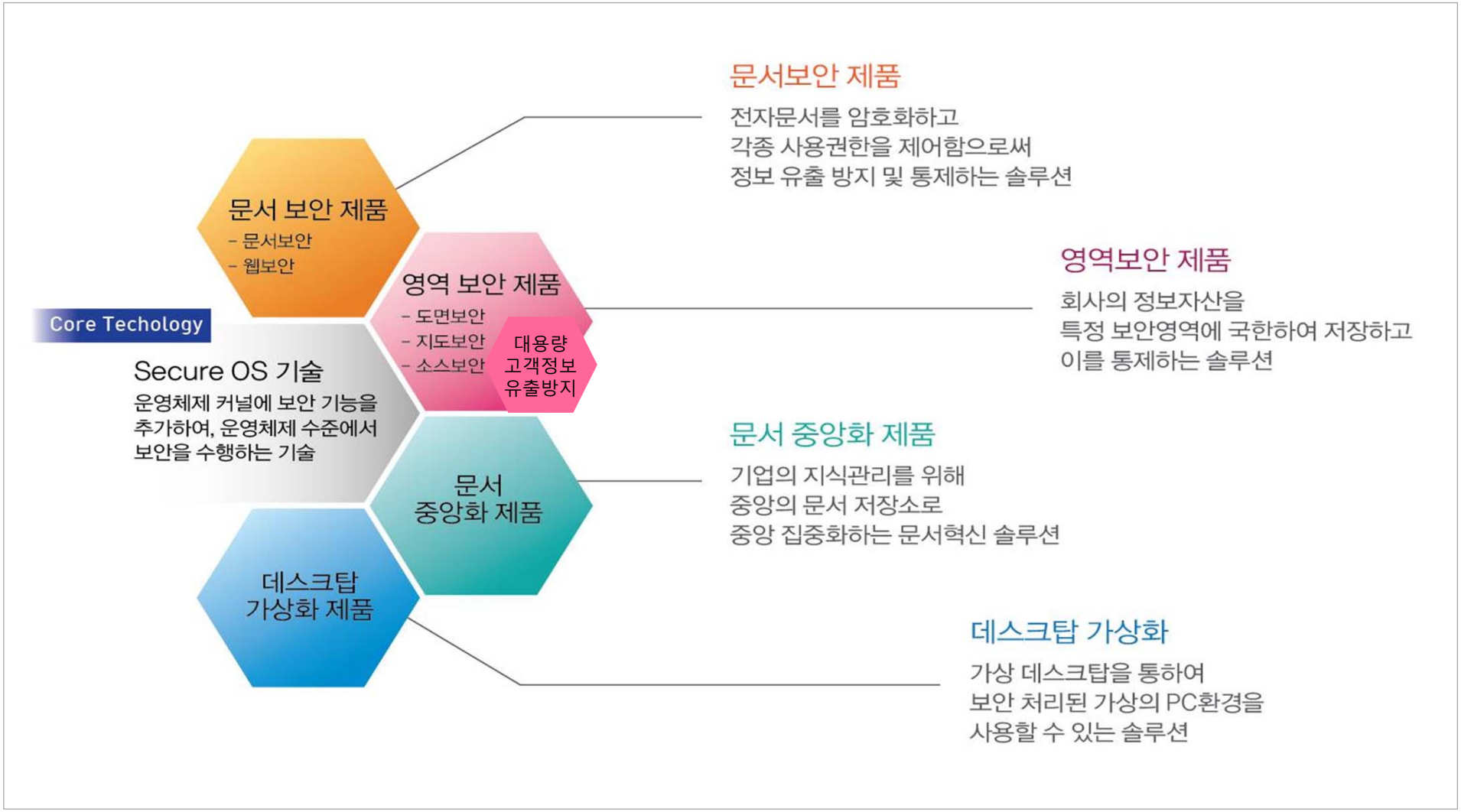
인증 및 수상 현황

- 국가용 암호제품 지정 (국가정보원 IT보안인증사무국)
- 수출유망 중소 기업 선정 (중소기업청)
- 우수제조기술연구센터 지정 (지식경제부)
- 신기술 보유 기업 (한국산업기술진흥협회)
- 기술혁신형 중소기업 인증 (중소기업청)
- ISO-14001 환경 경영 인증 (국제산업인증원)
- 소프트웨어 품질 인증 (한국 정보통신 기술협의회)
- 우량 기술 기업 선정 (기술신용보증기금)
- ISO-9001 품질 경영 인증 (국제산업인증원)

인력분포

전체 인원	임원	경영전략/영업	☑기술 인력
184	9	40	135
100 %	5 %	22 %	73 %

소프트캠프 주요사업분야



<그외: 키보드 보안, PC Keeper>

Contents

You meet the Innovation

- ✓ APT Brief
- ✓ SHIELDEX™ Concept
- ✓ SHIELDEX™ Introduction
- ✓ SHIELDEX™ Main Features
- ✓ SHIELDEX™ Customer Benefits
- ✓ [appendix] 망분리가이드라인에 대한 주요 사항 분석 및 대응

SOFTCAMP

APT (Advanced Persistent Threat) cases

- APT 공격은 치밀한 계획에 따라 장기간에 걸쳐 진행되며, 기업의 내부 시스템을 장악하고 기업의 기밀 정보를 유출합니다.
- 최근 APT 공격은 정보유출에서 그치지 않고, 내부 시스템을 파괴시키는 형태로 나타나며, 국가와 산업에 큰 피해를 입히고 있습니다.

APT 공격 사례

2010

Operation Aurora

- 2010년 1월
- 구글, 다우케미컬 등 30여 개 회사
- 소스코드 등 회사 기밀자료 유출

Stuxnet

- 2010년 9월
- 이란 원전 SCADA
- 원자력발전소 작동중단

2011

Operation Aurora

- 2011년 3월
- 벨기에 브뤼셀 EU 위원회 서버
- 피해 미공개

Knight Dragon

- 2011년 2월
- 오일, 가스, 석유화학 회사 웹사이트
- 피해 미공개

2012

SONY PSN Hacking

- 2011년 4월
- SONY PlayStation Network
- 7,700만 건의 가입자 개인정보 유출, 2개월간 서비스 정지

앱실론 이메일 침해

- 2011년 4월
- 앱실론사 고객 이메일 계정
- 시티은행, 디즈니 등 50개 기업고객 이메일 탈취

2013

국내 N, S사

- 2013년 3월
- 패치관리서버의 특성을 이용하여, 악성코드 내부 유포
- 데이터 삭제 등 서비스 장애

2014

국내 K사

- 2014년 12월
- 사이버 공격에 의한 개인정보 및 내부 중요 자료 유출 의심(현재 진행 중)

APT Characteristics

- APT는 **공격할 대상을 정하고**, PC를 장악하여 관리자 권한 획득을 한 후 공격하는 지능적이고 지속적인 공격방식입니다.
- APT는 내부 PC나 서버에 침투해 **오랜 기간** 모니터링을 실시하고, 첨단 보안 탐지 기법을 **회피**하기 위해 지속적으로 악성코드를 변조시키거나 교체하면서 보안 솔루션의 **패턴 파악을 어렵게 합니다.**

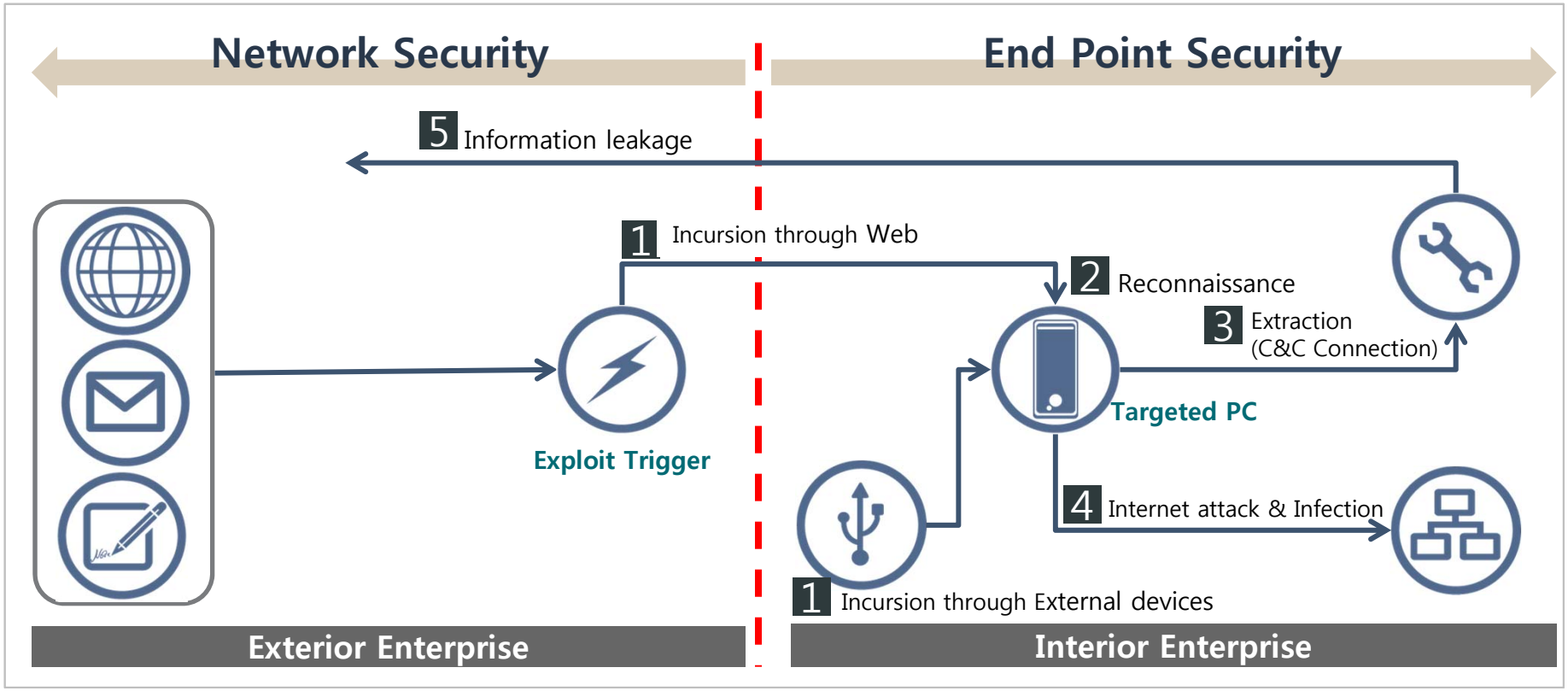
APT Characteristics

	Targeted	Persistent	Evasive	Complex
Characteristics	특정 조직을 대상으로 뚜렷한 목적 달성을 위해 데이터를 훔치거나 피해를 주기 위해 설계	장기간 잠복하며 다양한 단계에 걸쳐 공격	기존 보안제품들의 탐지방법을 피할 수 있도록 체계적으로 설계	공격대상의 허점을 공략하기 위해 다양한 공격방법을 조합하여 공격
Example(Google)	• 특정타깃기업: Google • 공격자: Elderwood Group (중국인민해방군과 관련 있는 해커그룹) • 발생 년도: 2009년 • 공격목표: 소스코드 공격	Aurora 공격은 2009년 말 처음 발견되기 몇 달 전부터 감행되었으며 2010년 2월까지 지속되었음	Aurora 공격은 인터넷 익스플로러의 알려지지 않은 취약점을 착취하도록 특별 제작되었기 때문에 제로데이 공격을 감지하던 전통적인 보안제품들을 회피	Aurora 공격은 인터넷 익스플로러의 알려지지 않은 취약점을 바이너리 악성코드 (Malware binaries)와 SSL 커넥션으로 가장한 비밀 커넥션을 사용하여 공격

APT Process

- APT 공격은 침투, 정찰, 데이터의 발견 및 수집, 정보 유출의 단계로 진행됩니다.
- 이 모든 프로세스는 치밀한 계획에 따라 장기간에 걸쳐 진행되며, 진행하는 동안 악성코드를 끊임없이 변조시켜 탐지가 어렵습니다.

APT Process



기존 방식의 한계

- 기존 APT 대응 솔루션의 보안 방식으로는 APT 공격에 대해 효과적인 대응 및 사전 예방이 불가능합니다.

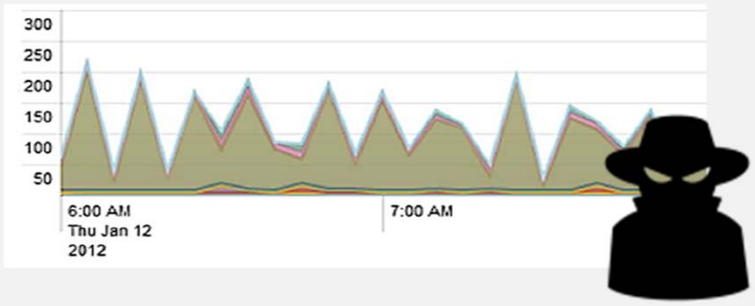
패턴 분석의 한계

- APT공격/신종악성코드에 대하여 무방비
  → **악성코드의 경우 기존 패턴이 20%인 반면, 새로운 유형의 악성 코드가 80%를 차지**
- 바이러스나 APT 악성코드 제작자는 기존 바이러스 백신으로 검사하여 검출되는지 확인하여 개발 배포
  → **사전적 대응이 아닌 사후적 대책**
- **표적형 공격, 지능형 지속 해킹 등에 대하여 사전 대응 불가**

<다양화 되고 지능화되는 공격 패턴>

모니터링/포렌직 솔루션의 한계

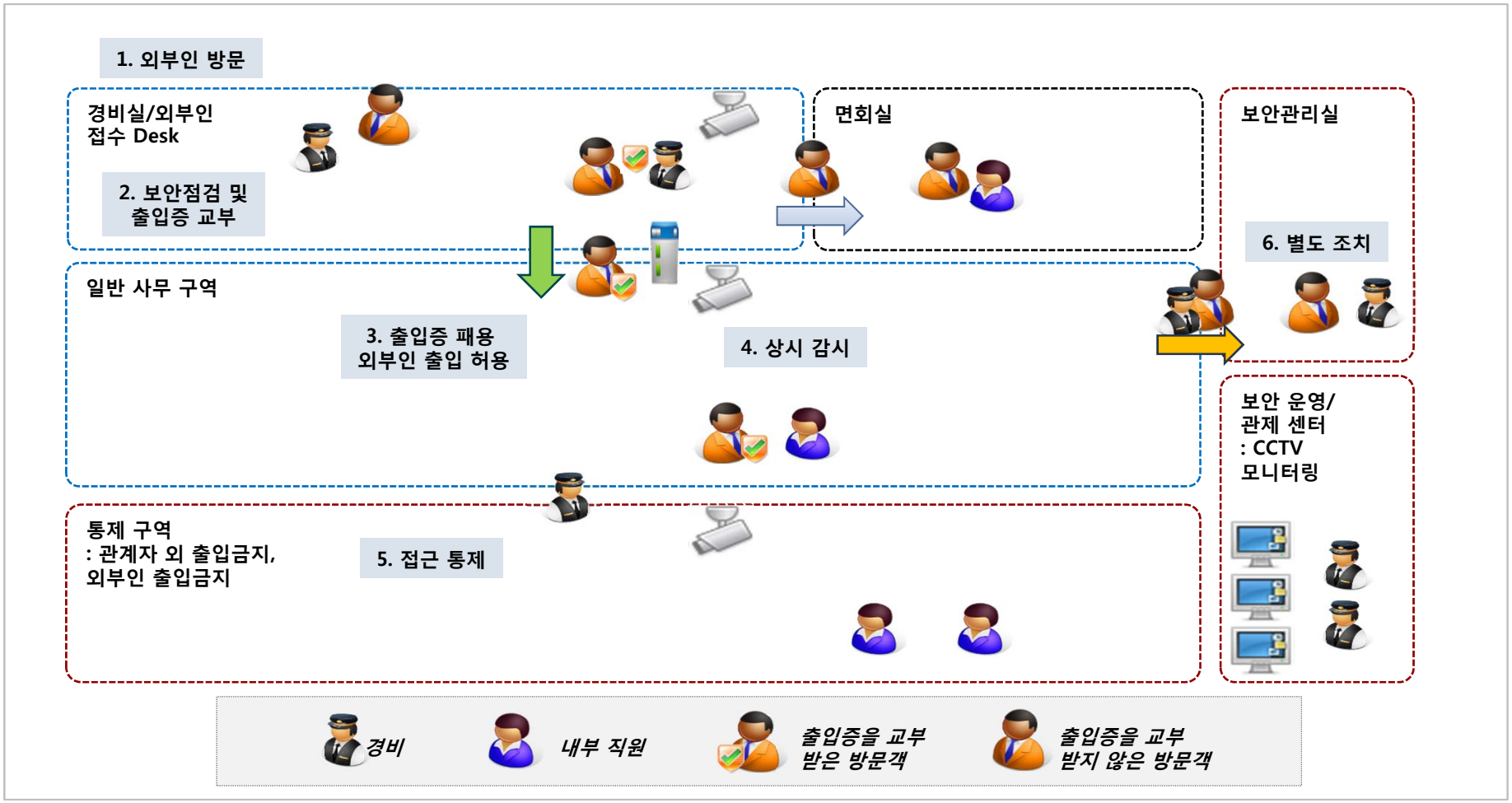
- PC 상에서 동작하는 모든 프로그램의 모든 행위에 대해서 감시
  → **과도하게 많은 로그로 인해 분석이 불가 또는 용이하지 않음**
- APT공격은 평상시에 잠복해 있다가 특정시각에 일시적으로 공격활동을 시작 → **사전 검출 또는 대응할 방법 부재**
- 악성코드는 공격을 마친 후 최종적으로 자신의 흔적을 모두 삭제하므로 **원인과 유입경로 추적이 어려움**



<악성코드에 대한 추적 감시의 어려움>

제품 컨셉 Motive – 외부인 출입보안체계

✓ 최근 기업들은 외부인 출입 보안 체계를 확립하여 내부 자산을 보호하고 있습니다.



제품 컨셉 도출

- 외부인 출입관리를 위해 출입 보안 체계를 갖춘 것과 마찬가지로, IT 환경에서도 외부 유입파일을 관리하기 위한 보안 체계가 필요합니다.
- 외부에서 유입되는 파일에 대한 격리, 검역, 감시, 통제, 차단 등의 조치를 취할 수 있도록 솔루션을 설계하였습니다.

SHIELDEX Concept 도출 과정

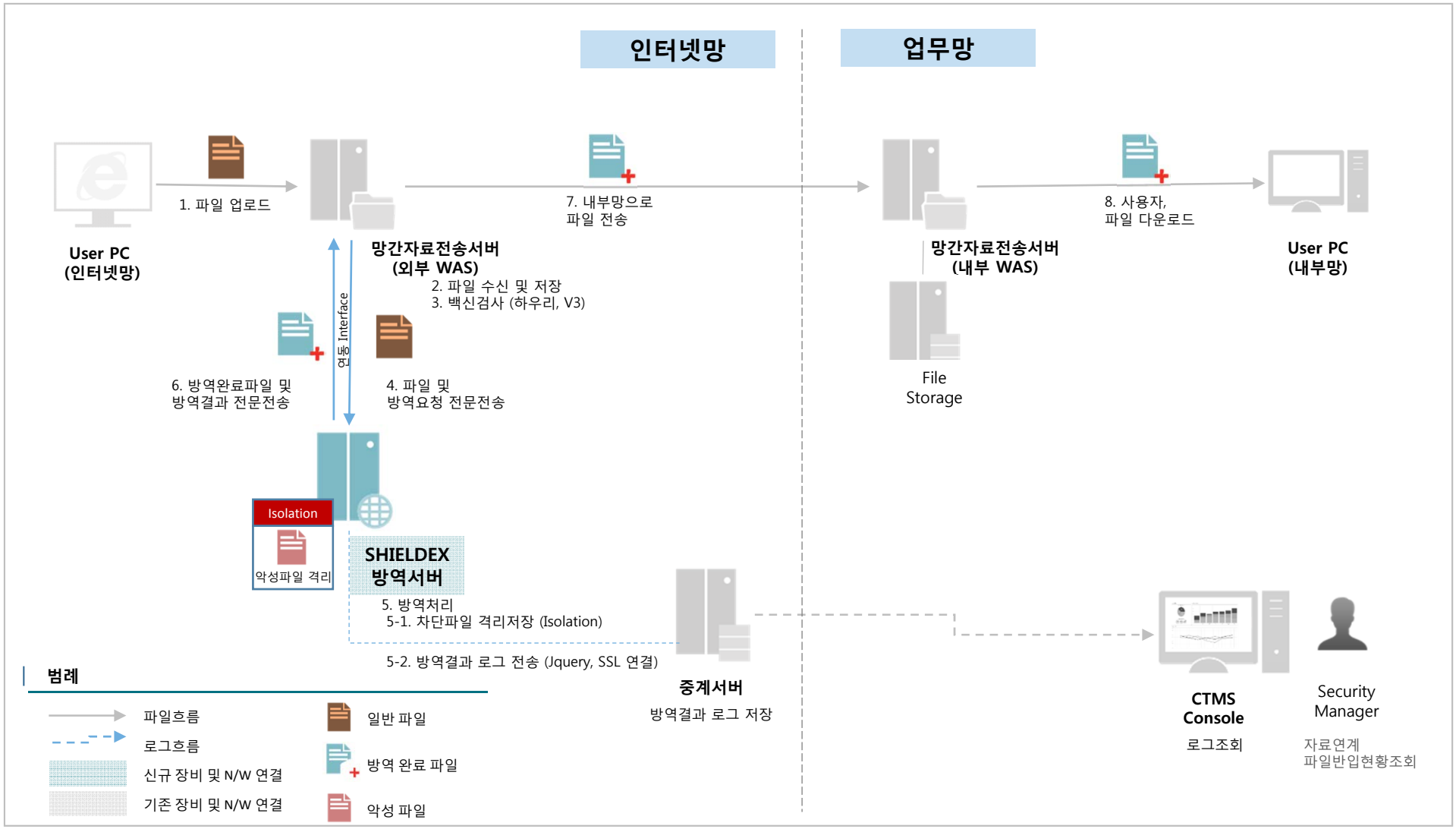
외부인 출입 보안 체계

면회실	• 내부와 격리된 별도의 업무미팅 공간 • 별도 출입증 발급 필요 없음
외부인 출입 절차	• 경비실 or 방문접수 Desk에서 방문 승인절차 후 출입증 교부
상주 내방자 관리	• CCTV, 출입증을 통한 통제, 위치 추적 등의 방법을 통해 출입 허가 받은 구역에 대해서만 통행 허용
통제 구역	• 중요 시설에 대한 관계자 외 출입금지, 외부인 출입금지 구역 설정
보안 사고 조치	• 경보 발생, 경비 출동하여 이상 행동을 실시한 자에 대한 색출/적발 후 퇴출

외부 유입 파일 관리 체계

V-Room	• 격리된 환경 제공으로, 외부유입파일 실행에 따른 Local System 변화를 최소화함
파일 유입 절차	• 문서/실행파일에 대한 1차적 방역 • 외부 유입파일에 대한 식별
유입 파일 관리	• 동작 모니터링, 권한에 따른 기능 동작 허용 • 외부 유입 파일에 아이콘 표시 및 추적
R-Area	• 시스템 변조/파괴가 가능한 영역에 대한 통제, 악의적인 시도 시 프로세스 차단
보안 사고 조치	• 전사적 위험 프로그램에 대해 실행차단/삭제, 유입경로 파악

SaniTrans 구성도

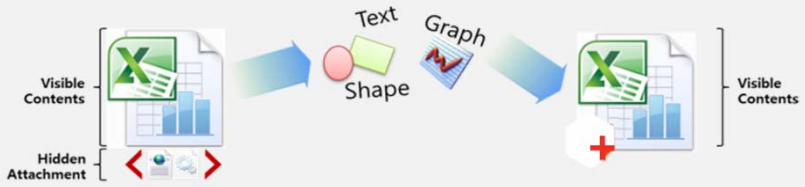


SHIELDEX™ SaniTrans 방역기능

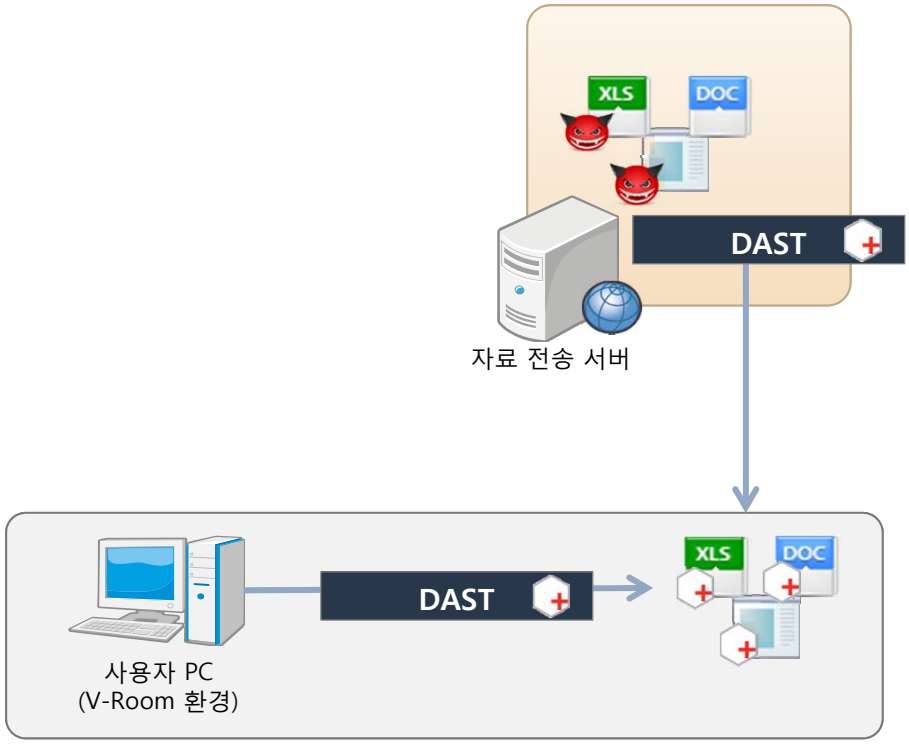
- MS Office, PDF, HWP 등의 주요 확장자 문서에 대하여 방역처리 후 자료전송시스템으로 전달
  - ① 문서파일 진위여부 판단
  - ② Visible Contents 추출
  - ③ 컨텐츠 재구성 및 사용자 전달
- 압축파일은 압축파일 내 지원포맷을 확인하여 방역처리 후, 다시 압축하여 자료전송시스템으로 전달

DAST
(Document Attachment Sanitization Technology)

- **Visible Contents(텍스트, 이미지 등) 만 추출하여 안전한 문서로 재작성하는 기술**
- **문서에 포함된 Hidden Attachment를 제거**



- 일반문서 : 정상적으로 변환되며, 매크로/VB 코드 등이 포함 시 제거되어 변환
- 악성코드 문서 : 악성코드 문서의 특성 상 정상적으로 변환되지 않음



- 지원확장자: doc(x)/ppt(x)/xls(x)/csv/pdf/hwp/txt/지원 (한셀, 한쇼 추가예정)
- 압축파일: zip/lzh

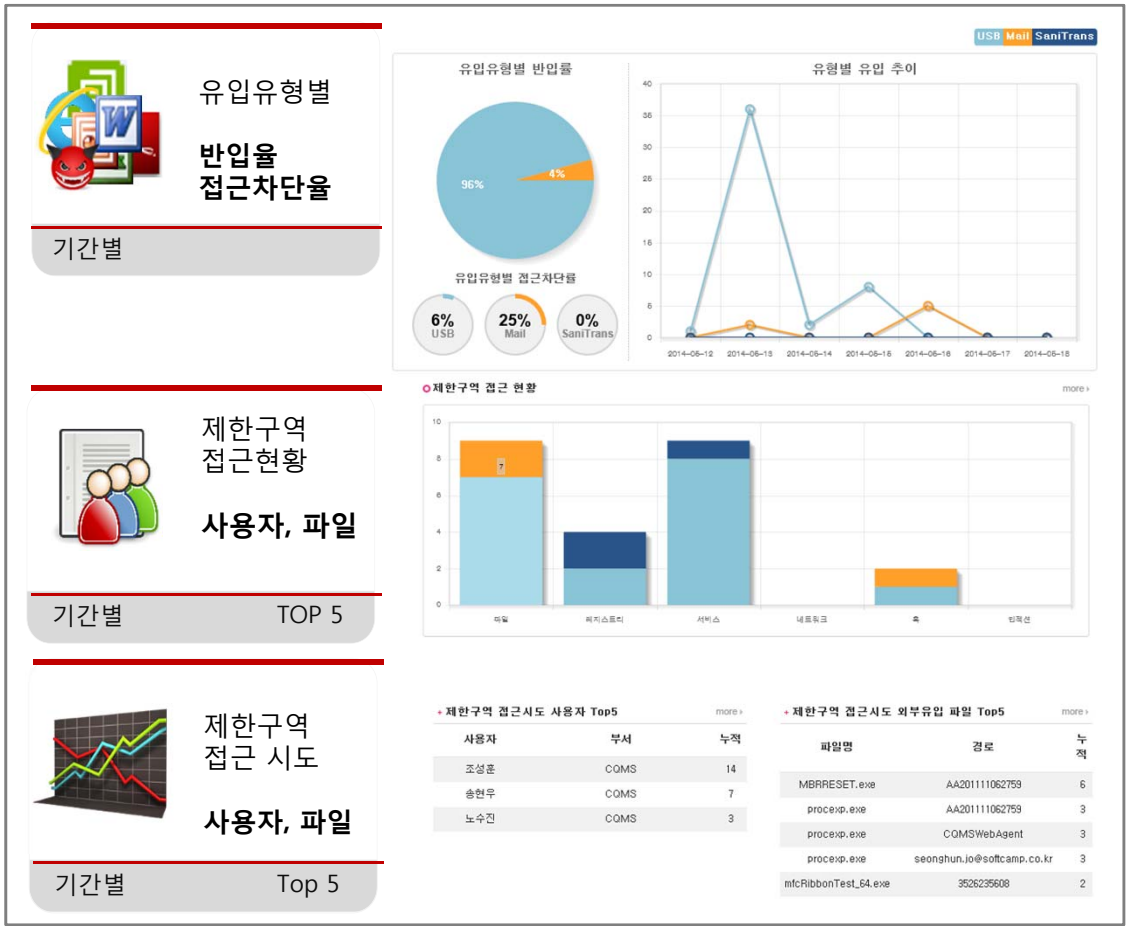
외부유입파일 관리 (현황 관제)

✓ 관리자 콘솔에서 유입유형별 반입율, 제한구역 접근현황, 사용자/파일 누적건수 등의 통계를 제공합니다.

SHIELDEX™ Console

접근 시도에 대한 현황 파악 및 추적 기능

- 외부유입파일의 유입경로별 현황
- 외부유입파일의 제한구역 접근 시도 현황
- 기간별 파일/사용자별 현황 데이터 제공
- 외부유입파일/유입경로 별 추적 기능 제공

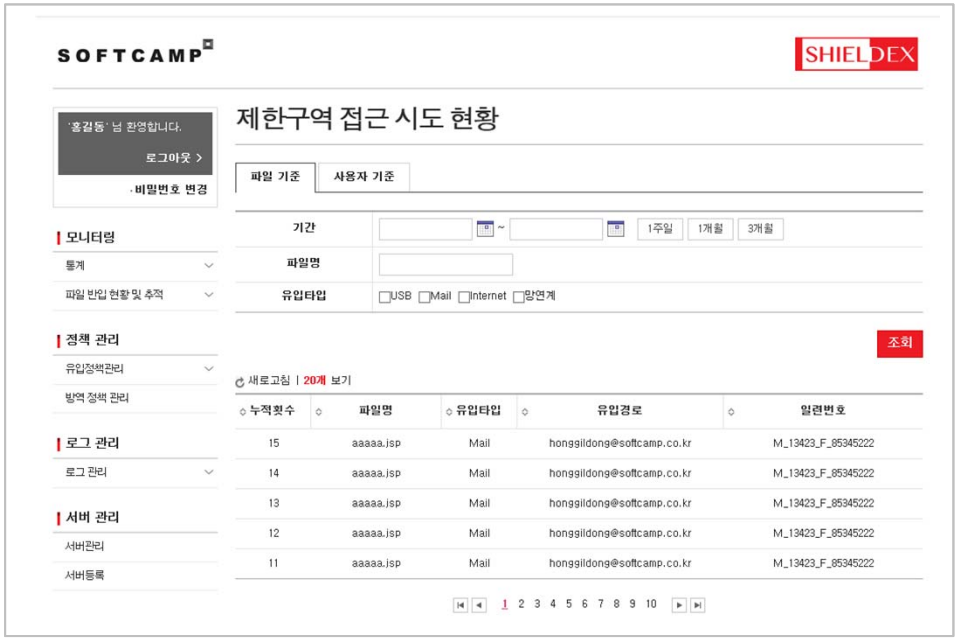


외부유입파일 관리 (로그 추적)

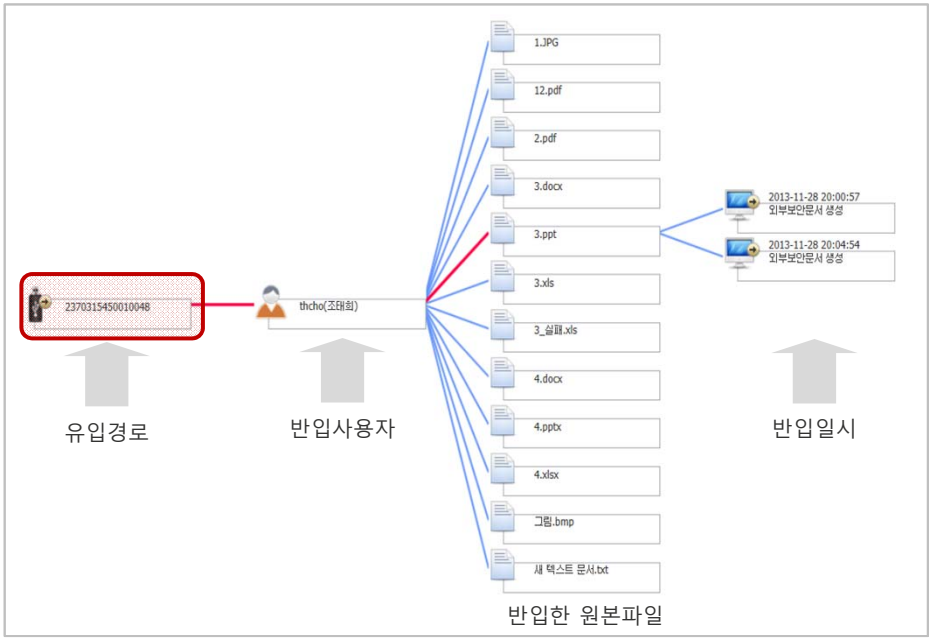
✓ 외부유입파일에 대한 이력은 ① 유입 경로별 사용 로그, ② V-Room 사용 로그, ③ 내부 반입 로그, ④ 반입파일 추적 로그에 대한 로그를 남기고 있습니다.

- 망연계를 통한 파일 유입 이력, 내부 반입 시도 시 실패 로그에 대한 이력 등

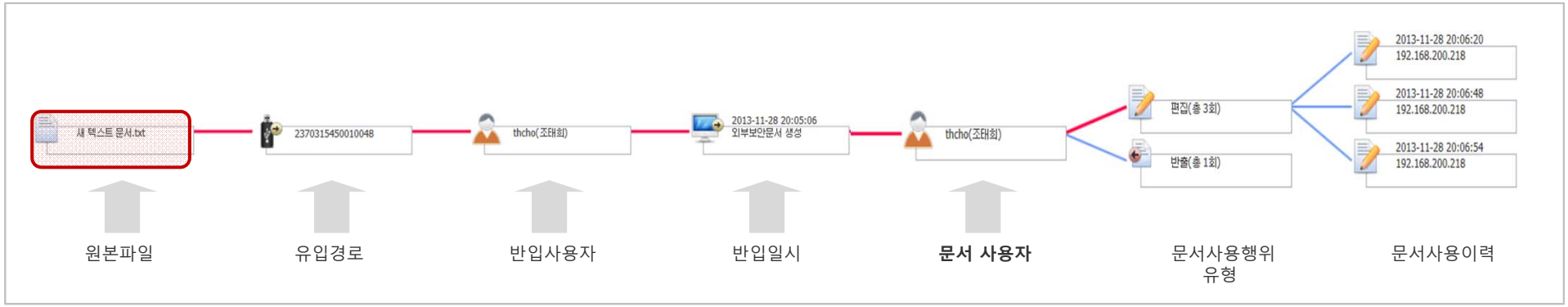
제한구역 접근시도 현황



유입경로 기준 검색 및 차단



파일명 또는 파일일련번호 기준 검색 및 차단



SHIELDEX™ Trace Server UI

✓ 관리자 콘솔에서 직관적인 UI 를 제공하여, 관리자의 실시간 모니터링 및 정책관리를 용이하게 합니다.

요약 통계

서버현황 관리

SHIELDEX™는 기존 보안 방식의 한계를 보완하고, 단계별 위험 제거를 통해 보안 위협을 최소화합니다.

기존 보안 방식의 한계 보완

- 기존 패턴 분석을 통한 사후 대처는 새롭게 발생하는 악성코드에 효과적으로 대처하지 못함
- 망분리 환경에서도 외부에서 유입되는 파일에 대한 관리 필요

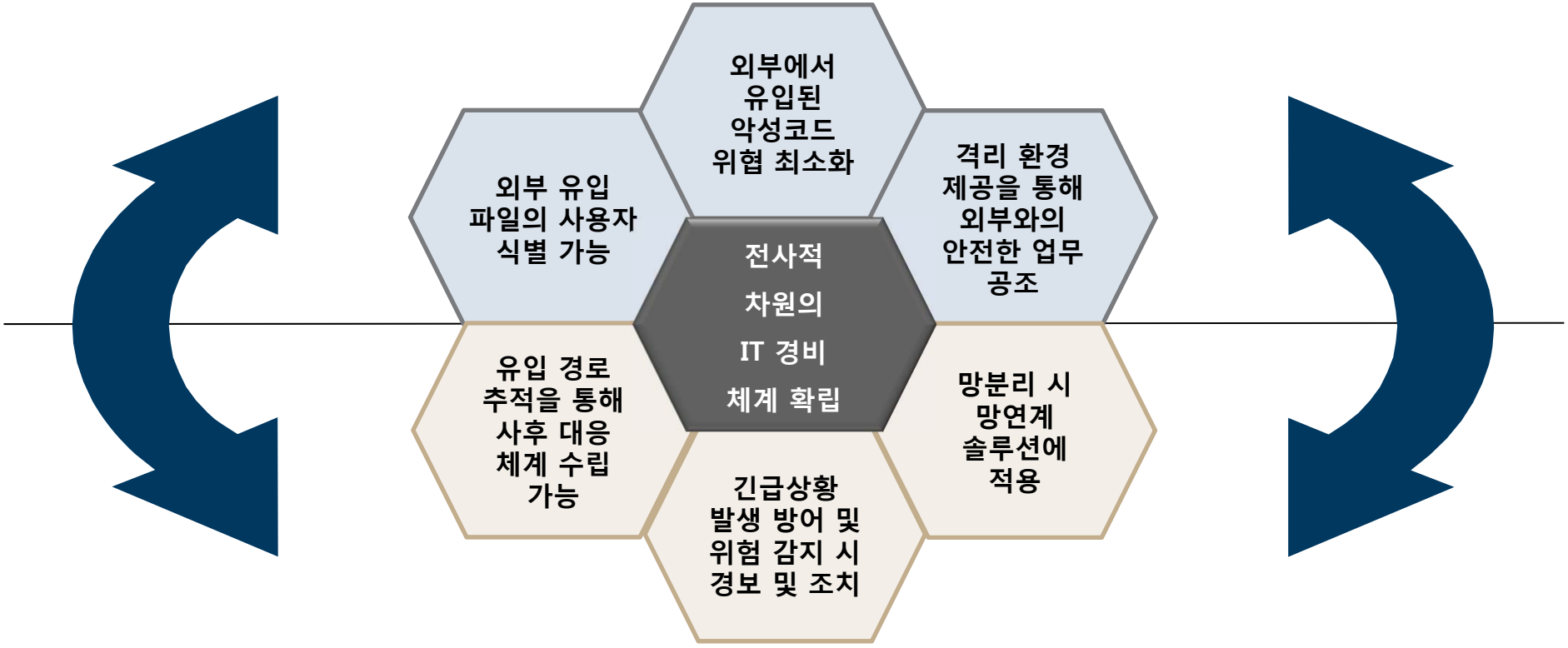
단계별 위협 제거를 통한 보안 위협 최소화

- 다양한 경로의 외부 유입파일에 대한 위협을 단계적으로 제거/감시하는 상시 방역 시스템 구축
- 위기 발생에 대한 위험을 사전에 차단하고, 위험 감지 시 능동적 대응 체계 확립

	Step 1	Step 2	Step 3	Step 4	Step 5
	면회실	방역	감시	접근통제	위기대응 및 추적
위협 제거	내부와 격리된 영역 제어	방역을 통해 위협 요소 제거	외부 유입 파일의 지속적 동작 감시	통제 구역에 대한 접근 차단	악성코드 소거/불능 처리
	다중 보안 체계를 통해 사용자가 느끼는 PC환경에서의 보안 지수 상승				

기업 내부에서 관리되는 정보 자산에 대한 안전성을 확보함으로써, 기존 IT 보안 솔루션들이 갖고 있던 문제점을 보완합니다. 전사적 차원의 IT 보안 체계 확립을 통해 1차적으로는 업무의 연속성을 보장하며, 2차적으로는 근본적 문제에 대한 대응 체계 확립을 가능하게 합니다.

➢ *1차적: 외부 유입 파일에 대한 식별과 차단을 통해, 안전한 환경에서 업무 공조 가능*



➢ *2차적: 긴급상황에 대한 대응 및 사후 대응 체계 구축, 각종 솔루션에 적용하여 업무 활용 극대화*

APT 대응 솔루션과의 비교

SHIELDEX

APT 대응 솔루션 VS. SHIELDEX

	APT 대응 솔루션	SHIELDEX
주요 기능	▪ 네트워크로 유입되는 트래픽 분석/탐지 ▪ 시그니처 분석/ 가상환경 분석/탐지 ▪ 블랙리스트/ 화이트리스트 분류 및 정책 업데이트 ▪ 악성코드 탐지 및 치료 ▪ 악성코드 탐지현황 분석자료 제공	▪ 분석/탐지 방식이 아닌 외부유입파일의 위협행위에 대한 원천 방어 ▪ 파일 내부반입 시 방역 - 실행파일 추적, 문서파일의 위협 컨텐츠 제거 ▪ PC 핵심영역 보호 - 악성코드의 실환경 변경/접근 차단 ▪ 외부유입파일 통제 - 반입차단/ 실행차단/ 폐기 등 정책적용 가능, 블랙리스트/화이트리스트 등록 가능 ▪ 외부유입파일 추적 및 관리 - 외부유입파일 사용현황 및 통계 (Log Trace)
관리 범위	▪ N/W Traffic (Web, Mail 등) 을 통한 파일, 웹페이지 ▪ Win XP/Win 7 의 주문형 샌드박스	▪ USB, Mail, 망간자료전송시스템, 인터넷(IE) 등 외부에서 내부로 들어오는 경로의 유입파일
특징	▪ N/W Traffic 분석/탐지 ▪ Appliance 장비 형태 (Client 치료 시 Agent 필요)	▪ 외부유입파일이 실환경에 접근하기 전, Micro VM 에서 실행하여 실환경 보호 ▪ 실제 사용자 환경의 중요영역 접근을 원천적으로 차단 ▪ 실행파일, 문서파일(DS 연동)의 모든 Life-Cycle 추적 가능

Anti-spam System 과의 비교

SHIELDEX

Anti-spam System VS SHIELDEX

✓ 스팸메일 차단 솔루션은 차단을 목적으로 하고, 실덱스는 유입되는 첨부파일을 격리/방역/관리/추적 하는 솔루션입니다.

	스팸메일 차단 솔루션	SHIELDEX
목적	▪ 광고, 음란, 악성코드 등을 내재한 원하지 않는 메일의 수신을 차단하는 솔루션	▪ 유입되는 파일을 격리/방역/관리/추적하는 솔루션 ▪ 메일을 통해 유입되는 악성코드를 원천적으로 차단
주요 기능	▪ 제목, 헤더, 본문 등에 포함된 문자열 검사 ▪ 첨부파일명이나 첨부파일에 포함된 문자열 검사 ▪ 첨부파일의 확장자 형식 검사 ▪ 패턴에 의한 스팸유형 검사 ▪ 백신 연동을 통한 첨부파일 검사	▪ 제목, 본문등에 포함된 URL 실행 차단 ▪ 본문의 스크립트 실행방지 ▪ 첨부파일 가상화 (샌드박싱) ▪ 첨부파일 반입 후 지속적인 감시 및 유해행위 차단 ▪ 패턴에 의한 메일수신 원천 차단
특징	▪ 광고, 음란성 등 스팸메일을 차단하는 것에 효과적 ▪ 악성코드는 백신에 의존함. 백신은 알려진 악성코드에 대해서만 대응이 가능하므로 제로데이 공격에 무방비	▪ 첨부파일을 가상화함으로써 악성코드가 실행되어도 실환경에 영향을 주지 않는 신기술 방식 ▪ 가상환경에서 실환경으로 첨부파일 반입 후에도 지속적인 감시 및 주요영역 보호 수행 ▪ 제로데이 공격 및 알려지지 않은 새로운 유형의 악성코드에 대한 대응환경 제공 ▪ 가상화된 파일 실행을 위한 응용프로그램은 실환경 프로그램과 연동되므로 별도의 응용프로그램 실행 불필요 ▪ 본문등에 포함된 URL 및 스크립트에 대한 가상환경 지원으로 본문을 통한 공격 대응 ▪ 스팸메일차단솔루션과 연계시 더욱 효과적

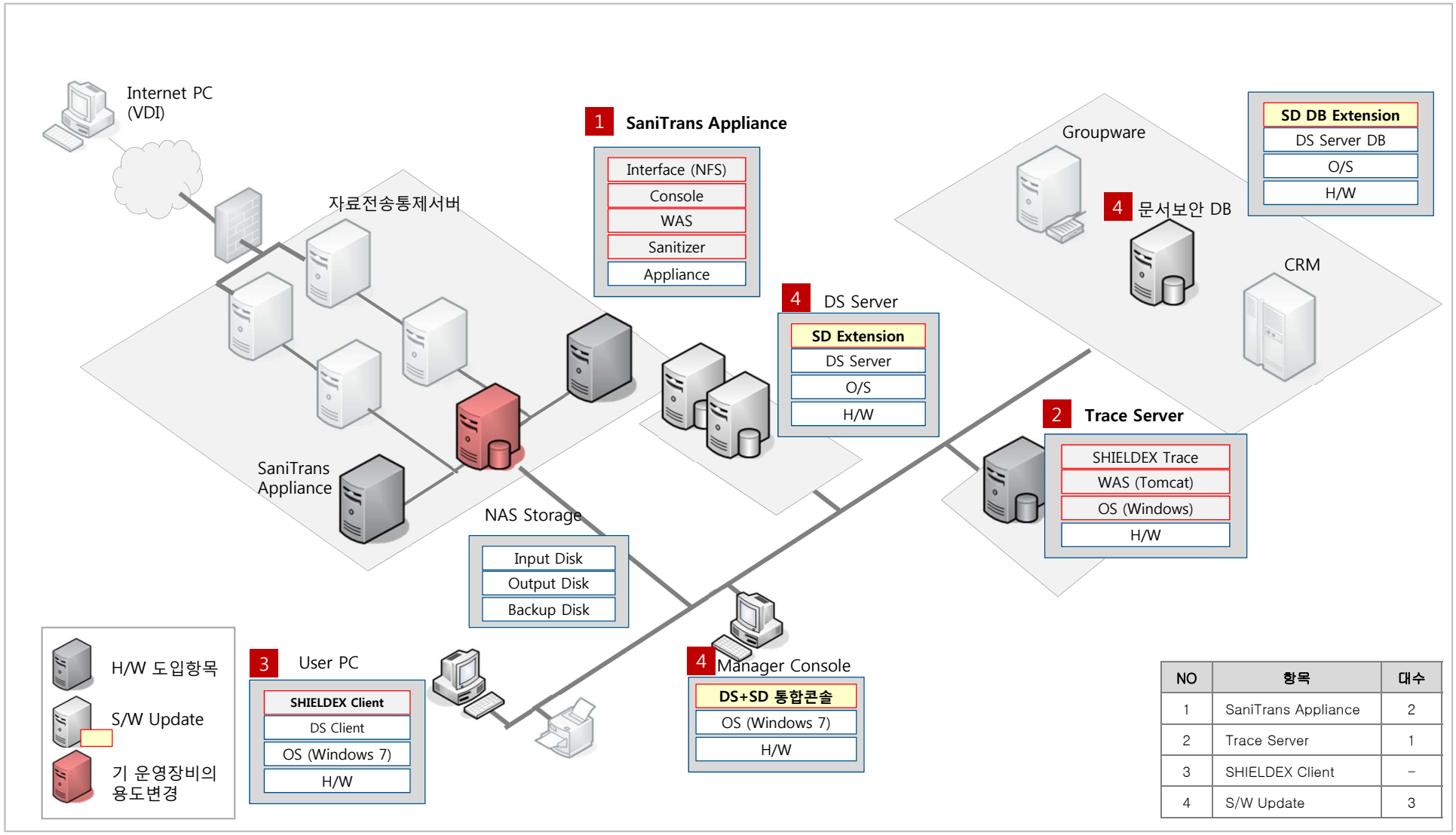
SHIELDEX™ Reference (1/2)

| OO 은행 SHIELDEX 도입 배경

✓ 외부유입파일 및 유입경로(자료연계, 이동식저장매체) 를 중앙통제하고, 외부유입파일의 사용현황을 추적하여 망분리된 환경에서도 알려지지 않은 위협에 빠르게 대응할 수 있는 체제를 구축하고자 하였습니다.

목표	도입 전	해결방안	SHIELDEX 기능
외부 유입 파일 통제	• 망분리 환경에서도 외부에서 파일이 유입가능한 경로(망연계, USB) 에 통제체계 미흡	• 외부 유입 원천 차단 → 사전대응 –망연계, USB 유입경로에 대한 통제 –유해파일 방역 실패 시 유입 차단	• SHIELDEX V-Room Client - USB 등 이동식저장매체 통제 • SHIELDEX SaniTrans - 망간자료전송시스템 유입파일 통제
외부 유입 파일 방역	• 유해 파일 유입 원천 방지 체계 부재 • 식별된 패턴에 의한 유해 파일 격리/폐기 (백신) → 사후 대응	• 파일 내 악성코드 제거 후, 컨텐츠 재구성 및 암호화 → 사전 대응 • PC 내 시스템 중요 영역 침해 방지 –PE Type의 실행 파일	• SHIELDEX V-Room Client, SaniTrans - 파일 방역처리 및 컨텐츠 재구성 (DS 4.0 연동하여 암호화) • SHIELDEX WatchMon Client - 시스템 중요영역 접근 감시
외부 유입 파일 이력 관리	• 유입 파일 현황 관리체계 부재 • 시스템 중요 영역 접근 현황 파악 불가 • 사용 이력 및 유통 현황 관리체계 부재	• 실시간 외부 유입파일 유입 현황 파악 및 모니터링 • PC내 시스템 중요 영역 접근 현황 관제 • 사용 이력 및 유통 현황 관제 및 추적	• Trace Server - 외부유입파일 검색 및 모니터링 - 유입경로, 사용자, 사용행위 추적 (외부문서 추적기능은 DS 4.0 연동)

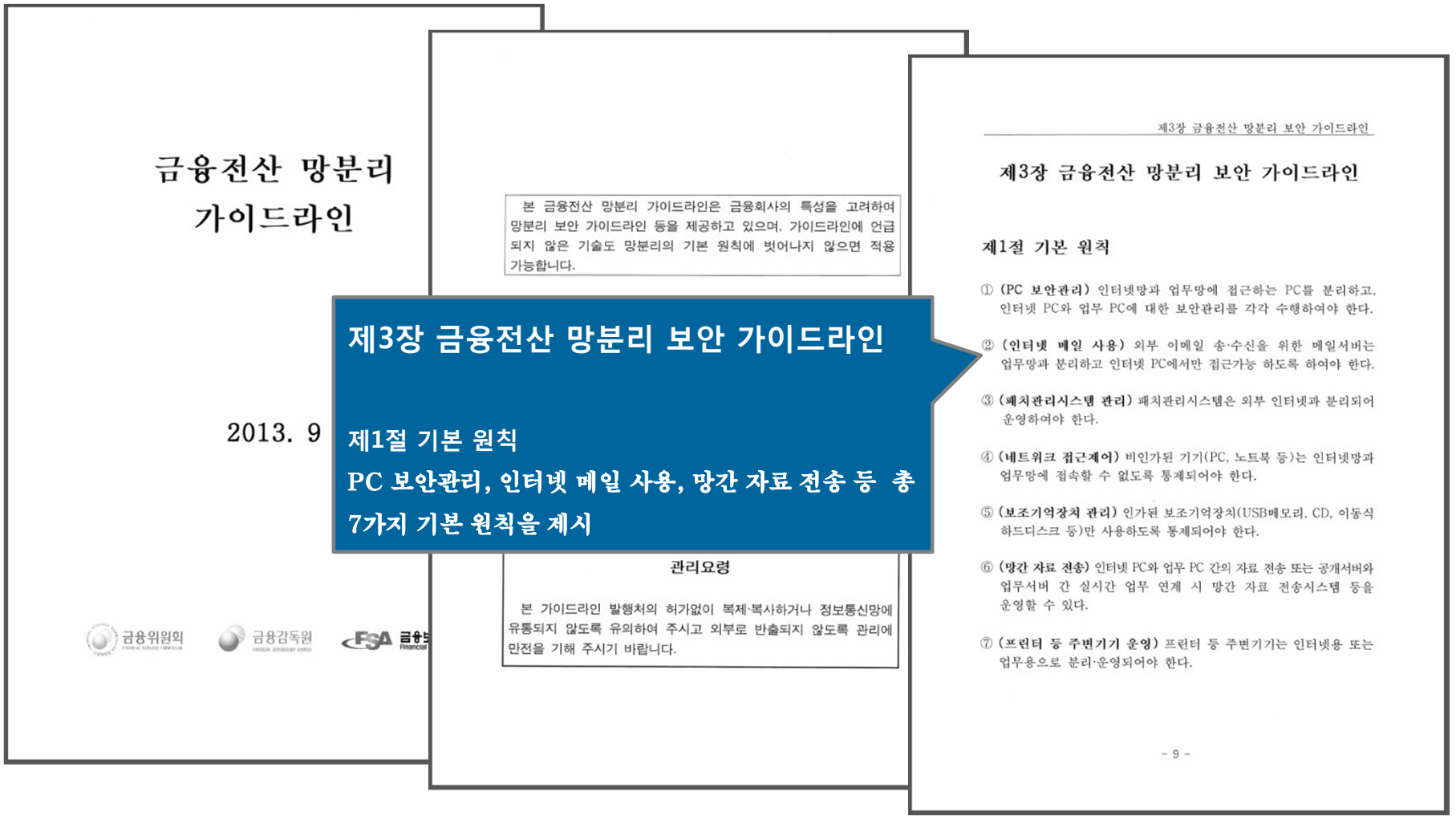
SHIELDEX™ Reference (2/2)



NO	항목	대수
1	SaniTrans Appliance	2
2	Trace Server	1
3	SHIELDEX Client	-
4	S/W Update	3

망 분리 가이드라인

1. “금융전산 망분리 가이드라인” 2013.09



망 분리 가이드라인 – PC 보안관리

제2절 PC 보안관리

1. 인터넷 PC 보안관리

인터넷 PC에서는 업무와 관련된 정보를 생성·저장할 수 없으며, 외부 이메일 및 웹서버 접속 등은 인터넷 PC를 통해서만 수행하여야 한다.

- 업무관련 문서 작업은 원칙적으로 금지하고 업무특성상 필요한 경우에는 제한적 승인·관리
- 금융회사에서 사용하는 웹하드, 인터넷 메신저 등의 사용은 원칙적으로 금지하되 업무특성상 필요한 경우에는 제한적 승인·관리
- 업무와 무관한 인터넷사이트 접속은 보안시스템 등을 활용하여 원천 접근 제한하도록 조치

2. 업무 PC 보안관리

업무 PC에서는 업무 관련 정보를 생성·저장할 수 있으며, 외부 이메일, 웹서버 접속 등 인터넷 접속이 차단되도록 하여야 한다.

- 노트북 등 휴대형 장비는 업무 PC로 사용을 제한하고 업무망 접속을 차단하되 업무특성상 필요한 경우에는 제한적 승인·사용 및 반출·입 시 보안관리 조치
- 와이브로, 무선랜 등 비인가 무선인터넷 연결을 차단하도록 조치
- 스마트폰, USB메모리 등을 이용한 정보유출 방지를 위해 비인가 보조기억장치 연결을 차단하도록 조치
- 업무 PC에서 특정 인터넷 접속이 필요한 경우, 관리자의 승인·관리 하에 망간 자료 전송시스템 활용 등 보안 대책 강구
- 업무 PC에서 외부 이메일 수신은 전면 금지하되 망간 자료 전송시스템 등을 통한 열람 기능*만은 예외적 허용 가능

※ 이미지 등으로 변환하여 악성코드 유입 방지

망간 자료 전송시스템을 통한 열람 기능만 예외적으로 허용
-> 사용자 편의성을 위해 악성코드 유입 방지 및 보안 적용 필요

망 분리 가이드라인 – 인터넷 메일

금융전산 망분리 가이드라인

제3절 주요시스템 보안

1. 인터넷 메일 사용

인터넷 메일을 송·수신하는 메일 서버는 악성코드 감염에 의한 업무망 피해를 방지하기 위해 인터넷망 구간에 구축하고 인터넷 PC에서만 접근 가능하도록 하여야 한다.

사내 전용 메일이 필요한 경우에는 업무망에 사내 메일 서버를 별도로 구축·운영하고 인터넷 PC의 접근을 차단하여야 한다.

1.1. 구성요소

- 인터넷 메일 서버(인터넷망)
- 사내 메일 서버(업무망에 선택적으로 구축 가능

<그림 2> 인터넷 메일 사용

인터넷 메일과
사내 전용 메일 서버 분리

- 12 -

제3장 금융전산 망분리

1.2 보안관리

- 메일 서버는 메일을 이용하여 전파되는 악성코드 또는 스팸메일 등을 차단하기 위한 보안 시스템 적용
- 인터넷에서 송·수신되는 메일(그룹사, 지주사 등 인터넷 메일 포함)을 위해 구축되는 메일 서버는 업무망과 분리되어 업무 PC에서 접근할 수 없도록 차단
- 필요 시 사내 메일 사용을 위한 별도 메일 서버를 업무망에 구축하고 인터넷 PC에서 접속할 수 없도록 차단
- 그룹사, 지주사 등의 그룹웨어와 연동된 업무메일은 악성코드 탐지 등 보안을 강화한 경우에 한하여, 제한적으로 업무 PC로 접속 이용 가능

메일 서버에 보안
시스템 적용 필요

그룹사/지주사 등 광의로
통합 조직이더라도
업무메일은 악성코드 등
보안 강화 필수

- 13 -

망 분리 가이드라인 – 자료 전송

5. 망간 자료 전송

인터넷망과 업무망이 분리된 환경에서 인터넷 PC와 업무 PC 간 자료 전송 또는 공개서버와 업무서버 간 실시간 업무 연계를 위하여 망간 자료 전송시스템을 구축·운영할 수 있다.

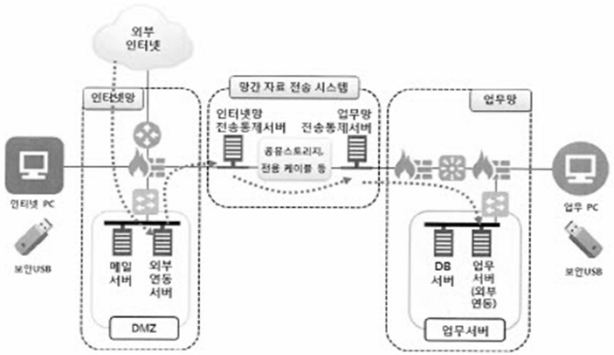
특히, 외부 인터넷의 웹 서비스로부터 내부 업무를 위한 자료수집 등은 망간 자료 전송시스템을 활용할 수 있다.

※ 인터넷뱅킹, HTS 등 성능이 중요시 되는 실시간 서비스는 추후 장기적으로 안정성 등 확보 후 적용 검토

또한 인터넷 PC와 업무 PC 간 자료 전송 시에는 보안USB를 이용하여 망간 자료 전송을 할 수 있다.

5.1 구성요소

- 망간 자료 전송시스템



<그림 6> 망간 자료 전송

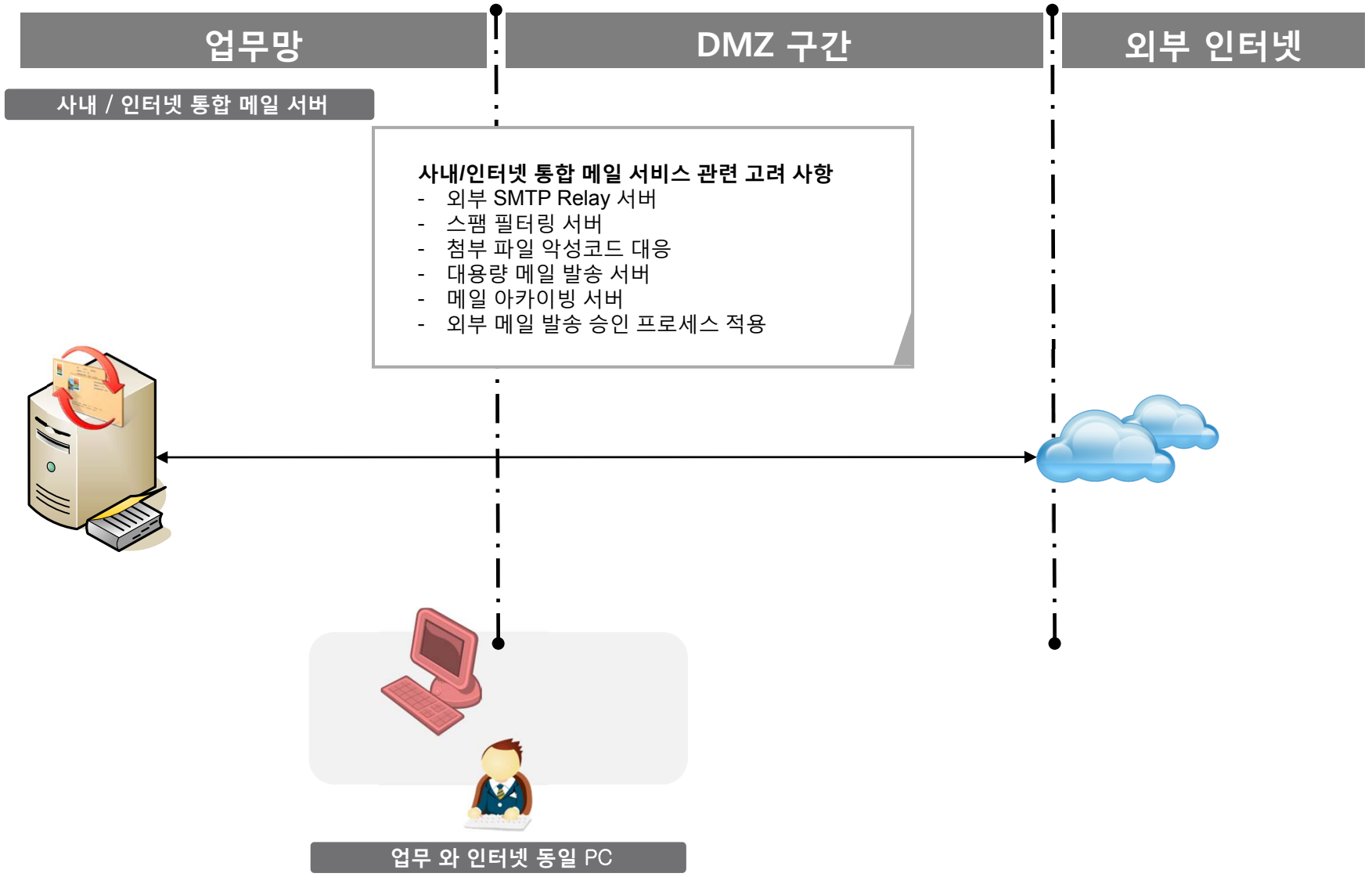
5.2 보안관리

- 전송통제서버는 인터넷망과 업무용으로 각각 구축하고 자료 전송은 전송통제서버를 통해서만 수행
- 전송통제서버는 인가된 관리자만 접속 가능 하도록 식별 및 인증을 수행하고 용역업체 등 외부로부터 원격 접속 금지
- 전송통제서버는 인가된 관리자 PC에서만 접속할 수 있도록 네트워크 접근통제
- 인터넷망과 업무망 전송통제서버 간 통신은 일반적인 형태의 사용하고 일방향성 유지
- 개서버와 업무서버 간 전송통제시스템을 각각
- 시 악성코드 검사를
- 등을 관리서버에 등록
- 삽입하면 사용자에 대한 식별 및 인증을 수행하고 자동으로 악성코드 감염여부를 검사하도록 백신 프로그램 설정
- 보안USB 분실 시, 중요 데이터가 유출되는 것을 방지하기 위해 저장된 데이터를 완전 삭제 하거나, 저장되는 자료를 일정기간 이후 삭제하는 등의 보안 조치
- 보안USB 및 인터넷 PC와 업무 PC 간 자료 전송 내역에 대한 로그 기록은 3년 이상 보존하도록 조치

망간 자료 전송시스템 및 보안 USB를 통한 자료 전송 허용
-> 자료 전송 시 악성코드 유입 방지 및 보안 적용 필요

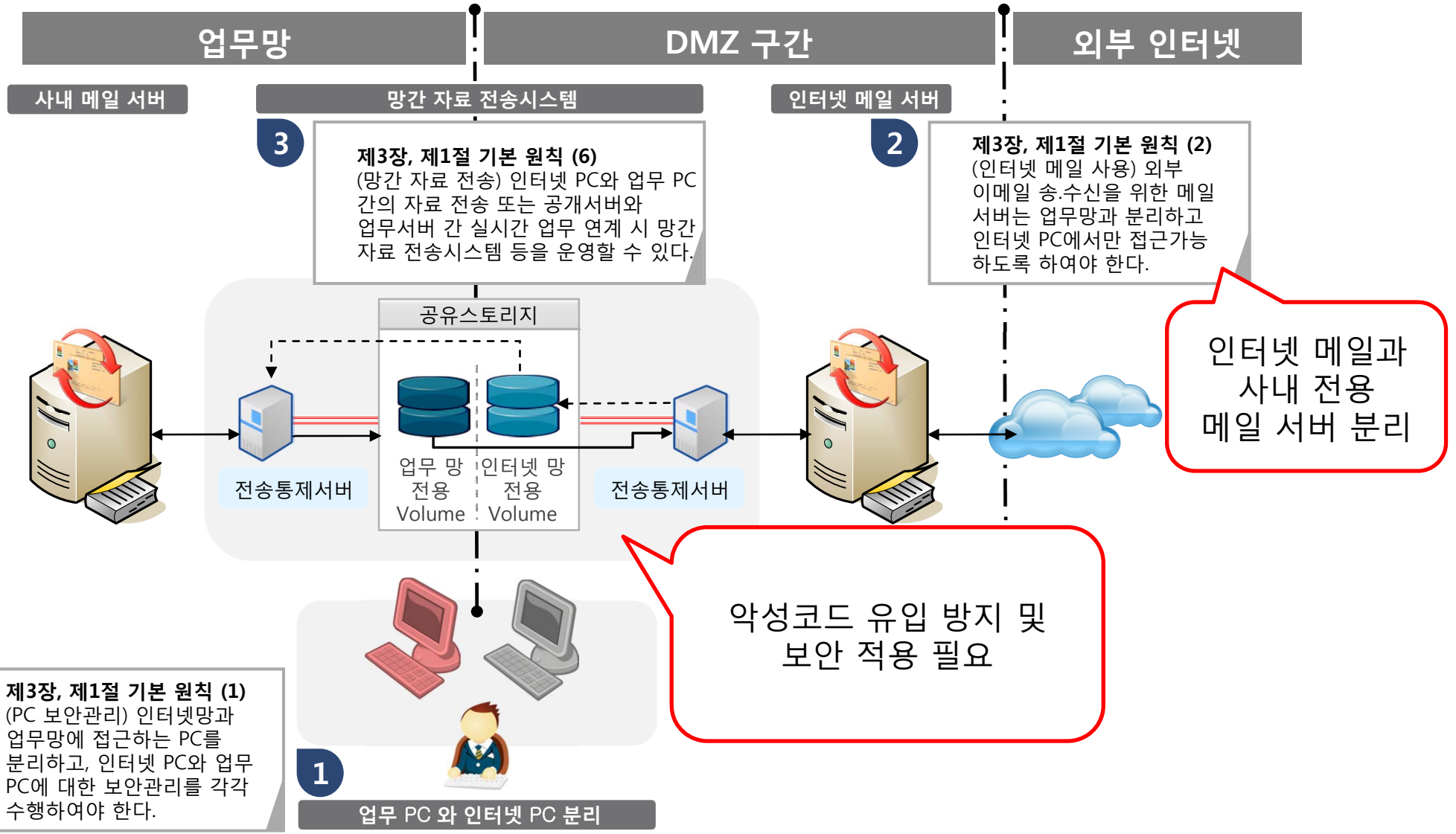
망 분리 가이드라인

“금융전산 망분리 가이드라인”에 따른 인터넷 메일 서버 분리 : As-Is



망 분리 가이드라인

“금융전산 망분리 가이드라인”에 따른 인터넷 메일 서버 분리 : To-Be



네트워크 망 분리 및 망 연계

SHIELDEX

망분리의 보안성 강화 효과 유지 & 망간 자료 전송

차단, 방어 개념에서 격리, 분리로 정보 자산의 안전성 확보

- 내부 업무망(정보 자산 시스템)과 외부 접속 시스템의 물리적인 네트워크 분리
- 금융기관, 정부기관 및 주요 산업 시설의 IT인프라 보안 권고 방안
- 악의적인 침해 시에도 기업 및 기관의 정보자산의 보호 목적
- 불법적이거나 실수에 의한 정보자산의 유출 방지
- 반드시 필요한 서비스만 한정적으로 분리된 망간 연동

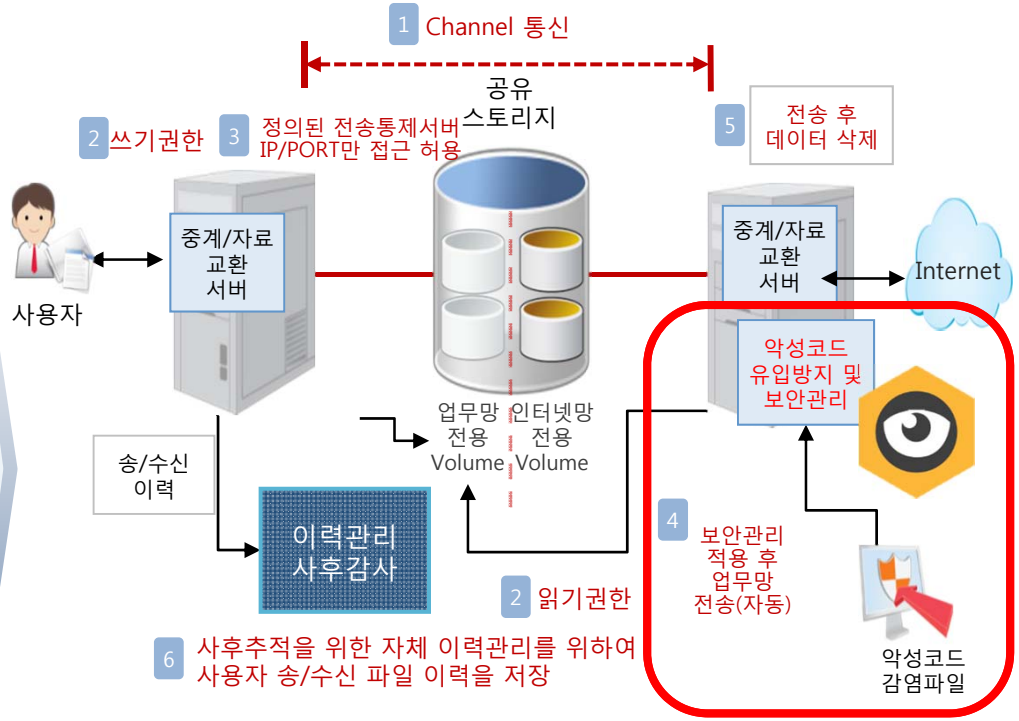
망간 자료 전송의 관리 중점사항 및 보안대책

SHIELDEX

망간 자료전송 관리 중점사항

보안 대책	관리중점사항
1 정보 접근통제 및 관리	공유 스토리지와 자료교환서버 간에 고속 광케이블을 사용 또는 TCP/IP 프로토콜이 아닌 전용 프로토콜 적용
2 공유스토리지 접근권한 설정	저장공간에 자료 전송 측은 쓰기만 가능 자료 수신 측은 읽기만 가능하도록 접근권한 설정
3 공유스토리지 접근인증 절차	다단계 인증방식을 통해 공유 스토리지에 접근하여 자료를 전송할 수 있는 외부서버(혹은 업무서버)를 엄격히 제한
4 내부망으로의 악성코드 유입 방지	자료교환서버는 내부망으로의 악성코드 유입을 방지
5 내부망에서 자료전송시 중요자료 유출방지	내부망 자료교환서버는 반출이 허용된 유형의 자료파일에 대해서만 제한적으로 전송을 허용
6 파일이력(로그) 유지	자료교환서버는 사후추적을 위해 파일 이력을 유지

공유스토리지를 이용한 자료전송 보안대책 적용



안전한 자료전송 시스템 구축

- 자료교환시스템 보안위협 및 대책 적용
- 업무담당자가 고려해야 할 자료전송 체크리스트 준수

자료교환시스템 보안성 강화

※ 출처 : 국가,공공기관 내부망과 인터넷간 안전한 자료전송 보안가이드라인, 국가정보원, 2012.2

SOFTCAMP

SHIELDEX

The power to do safely

ⓒ 1999-2015 Softcamp Co., Ltd

All rights reserved. No part of this work covered by the copyright hereon may be reproduced or used in any form or by any means -- graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems -- without written permission of SoftCamp Co., Ltd, Inc.,

SoftCamp, the traditional SoftCamp Logo, "SoftCamp Co., Ltd, Inc.," "Document Security," "S-Work," "MaxeOn," "S-Work for Storage," "SHIELDEX," "Secure Workplace," and "Secure Keystroke" are trademarks of SoftCamp Co., Ltd. All other trademarks mentioned herein are the property of their owners.

Printed in the Republic of Korea

The information herein is for informational purposes only and represents the current view of SOFTCAMP Co,. Ltd. as of the date of this presentation. Because SOFTCAMP must respond to changing market conditions, it should not be interpreted to be a commitment on the part of SOFTCAMP, and SOFTCAMP cannot guarantee the accuracy of any information provided after the date of this presentation.