보안업무 자동화 및 사용자편의성 강화 방안

2024.10.17





Contents

- 1. 보안솔루션 운영의 어려움
- 2. 보안솔루션 운영의 효율화
- 3. 사용자 편의성
- 4. 사례



1

다양한 보안솔루션 운영



2

복잡한 보안 정책



3

수동적용



4

내부 보안 프로세스



5

감사 대응



6

보안 운영 인력



보안 솔루션 운영시 어려움을 가져오는 요소

복잡한 보안 정책 수작업 정책 적용 보안 운영 인력 유지 어려움





1. 다양한 보안 솔루션 운영

EndPoint 보안 솔루션

만 보안

- 이동식저장장치 예외
- CD/DVD 예외
- 비인가 SW 통제
- 화면보호기
- 파일첨부
- 블루투스 장치 허용
- 기타 장치
- 프로세스 통제

문서 보안

- 복호화 권한
- 문서 복호화
- 문서보안 (워터마크 예외)
- 문서 외부 오픈

보안USB

- USB 사용 허가
- 외부 반출
- USB 등록

출력보안

- 출력물 워터마크 해제
- 개인정보 마스킹 해제
- 화면워터마크 해제

기타

- 개인정보검출
- 화면워터마크 해제
- 악성파일 해시 등록
- 망연계 파일 반출
- PC권한관리

1. 다양한 보안 솔루션 운영

인프라 보안 솔루션

서버접근제어

- 서버 계정 등록
- 서버 접근 권한 등록

BB접근제어

- 매계정 등록
- 매접근 권한 등록

클라우드 서버

- 서버 계정 등록
- 서버 접근 허용
- 서버 접근 권한 변경

파일전송

■ 파일 전송 권한 허용

1. 다양한 보안 솔루션 운영

Network 보안 솔루션

망연계

■ 망간 파일 전송

사이트 차단

■ 사이트 허용 (웹프록시)

NAC

- 신규 네트워크 허용
- 변경 허용

방화벽정책

■ 방화벽 정책 신청

기타

■ 악성 때 등록

1. 다양한 보안 솔루션 운영

기타 솔루션

만반출

■ 띠외부 반출 허용

웹메일

- 메일 발송
- 대용량 메일

데이터변환

■ 테스트 데이터 변환 허가

알림

- 메일/메신저
- 결재 / 기간만료 / 처리완료

기타

■ 화면 캡처 방지

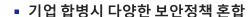
2. 복잡한 보안 정책

컴플라이언스 준수

- 업종에 따른 법령 리스트
- ***법, **시행령, ***규정, **시행세칙 우선순위 확인 (전자금융거래법(시행령), 개인정보보호법(시행령), 정보통신망법 등)



일관된 보안 정책 유지 어려움



- 보안 정책 혼합 운영
- 계열사 별 보안 정책 혼재
- 기존 정책 히스토리 파악 및 솔루션 기능 적용 어려움



- 보안 솔루션 간 연동 필요시 제약사항 발생 가능성
- 정책 연계시 프로세스 통합 기반 어려움 수반



- 수동 정책 적용시 자동화 가능 범위 인지 부족
- 사용자 위주로 편중 가능 (보안 운영 어려움 증가요인)
- 휴먼 에러 발생 가능성 증가

보안 솔루션 정책 연계작업시 제약 사항 발생

복잡한 정책 운영시 수동 작업 비율 상승

3. 수동 적용

보안솔루션 증가 운영방식은 유지

휴먼 에러 발생 확률 증가

만료 정책 회수 어려움

단순 업무 비율증가

신청사용자 정책 반영 시간 증가

4. 내부 보안 프로세스

- ·시스템별 각기 다른 보안 정책 적용 프로세스
- ·보안 프로세스 변경 시 적용 근거 확보 (보안 내규 등)

5. 감사 대응

- ·보안 정책 변경 이력 확보 어려움 (개별 시스템)
- · 번거로운 현황 리포트 (개별 시스템)

6. 보안 운영 인력

- ·보안 운영 인력 유지 어려움
- ·단순 반복 업무 , 정책 변경의 책임 부담

2. 보안솔루션 운영의 효율화

2 보안솔루션 운영의 효율화



3. 사용자 편의성



4. 사례

구축사례 - 제조회사(약2만유저)

보안신청

[SSO 및 그룹사 그룹웨 어 연동]

- 보안 예외 정책 선택 및 파일 첨부
- 32가지 보안 신청 업무

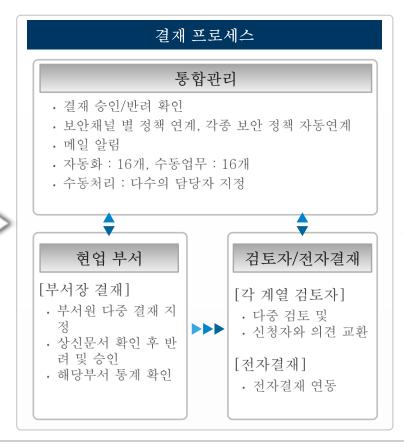
결재

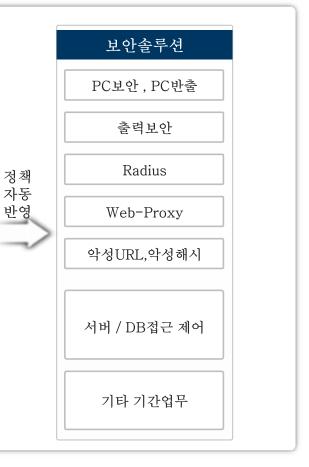
상신

- 검토 및 전자결재 연동
- 기존 신청 위치에서 링 [계열사 관리 및 다국어 지원]
- 계열사 보안 검토자
- 다국어 지원

[DRM 다중 연동]

- 소캠
- MS AIP





구축 사례 - 증권사 (약 1,000 유저)

보안신청

[SSO 로그인]

- 보안 예외 정책 선택 및 파일 첨부
- 15여가지 보안 신청 업 무

[라그륟에서스템크실차상 신]

• 결재가 필요한 타 보안 시스템에서 솔루션 API 를 통해 결재 상신

결재 상신

결재 프로세스 통합관리 • 결재 승인/반려 확인 • 보안채널 별 정책 연계, 각종 보안 정책 자동연계 • 메신저 알림 • 자동화 : 10개, 수동업무 : 8개 현업 부서 정보보호그룹 [부서장 결재] [보안 운영 결재 또는 • 부서원 다중 결재 지 합의] 정 • 상신문서 확인 후 반 • 각 채널별 주요 사항 합의 려 및 승인 • 임계치 이상시 합의 • 해당부서 통계 확인 . 중요 항목 결재

보안채널

PC보안, PC권한

문서보안, 보안usb

DLP. 망연계(2개망)

정책

자동

반영

NAC, 출력보안

비업무사이트

소명관리 타 보안 시스템 결재 연동

신청기간, 파일크기, 결재 가이드

구축사례 - 은행(약 10,000 유저)

보안신청

[SSO 로그인]

- 알림 Agent (결재, 작 업완료, 공지사항 등)
- 보안 예외 정책 선택 및 파일 첨부
- 40여가지 보안 신청 업 무

결재 상신

결재 프로세스

문서반출 통합관리

- 결재 승인/반려 확인
- 보안채널 별 정책 연계, 각종 보안 정책 자동연계
- 알림 에이전트를 통해 실시간 작업 안내 및 공지사 항 안내
- · RPA 를 통한 수작업 최소화

현업 부서

[부서장 결재]

- 부서원 다중 결재 지
- 상신문서 확인 후 반 려 및 승인
- 해당부서 통계 확인

정보보호그룹

[보안 운영 결재 또는 합의]

- 각 채널별 주요 사항 합의
- 임계치 이상시 합의
- 중요 항목 결재

보안채널

망연계

문서보안

DLP

정책

자동

반영

RPA

적용

NAC, 출력보안

PC보안

정보보안통합 서비스, SSO 신청 (정보 변경, 신규, 삭제)

신청기간, 파일크기, 결재 가이드

구축사례 - 서비스(약 11,000 유저)

보안신청 결재 프로세스 보안채널 직무별 PC보안 보안 통합승인관리 [SSO 로그인] • 그룹웨어 메뉴 통해 접 • 결재 승인/반려 확인 문서 보안 속보안 예외정책 선택 • 보안채널 별 정책 연계 출력물 보안 및 파일첨부 · 외부파일 생성 정책 • 3방향 그룹웨어 통합 자동 • 파일반출 수행 결재 IP 관리 반영 상신 연계 (고정IP, DHCP) 현업 부서 정보보호그룹 사이트 예외 [부서장 결재] [정보보호그룹 합의] 보안 서비스 • 부서원 다중 결재 지 • 각 채널별 주요 사 (계정신규, 변경, 각종 일반사항) 정 항 합의 . 상신문서 확인 후 반 • 임계치 이상시 합의 신청기간, 파일크기, 려 및 승인 결재가이드 . 해당부서 통계 확인

