창립 1주년 성과보고서

2018. 5.

서울교통공사 Seoul Metro

정보보안단

목 차

Ⅰ 사이버 보안사고 ZERO화 추진

1. 24시간 365일 실시간 사이버 위협 대응체계 구축

○ 중대피해를 동반한 사이버 보안사고 ZERO화 달성

○ 사이버 공격에 대한 신속한 대응수준 향상

- 보안서비스 대응수준 향상 : 3등급(2~4시간 대응) → 1등급(1시간 이내 대응)

3등급	➡	1등급
'14년 PC/서버 악성코드 감염 및 권한 탈취		'17년(2회) 웹서버 악성코드(웹쉘) 설치 시도
약 5개월 후 발견		1시간 이내 탐지·차단

2. 정보시스템 계정·권한 관리체계 확립

○ 서울시 정보시스템 사용자계정 점검관리 평가 결과 1위

- 전체 66개 서울시(본청 및 구청 등) 및 산하기관 중 1위(90.65점)달성
- 전체평균 76.54점, 투자출연기관 평균 80.99점

○ 인적오류로 인한 사고예방 관리 강화로 보안수준 향상 및 사고위험 축소

- 관리 현행화 및 권한부여 최소화로 적정성 확인과 오·남용 방지 기여

1 24시간 365일 실시간 사이버위협 대응체계 구축

안전우선

☐ 추진목적

○ 불법침입 및 해킹의 전문적 대응을 위한 실시간 보안관제 구축으로 증가하는 사이버 위협속에서 공사 정보화 서비스의 안전성 및 신뢰성 제고

☐ 추진내용

○ 24시간 365일 실시간 사이버 보안관제 운영

– 전문인력에 의한 사이버 보안관제 체계 도입

○ 기존 1~4호선 주간 보안관제에서 1~8호선 주야간 보안관제로 확대

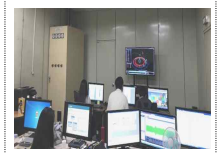
○ 타산업군 네트워킹을 통한 추가 정보수집 및 예방활동 강화

○ 침해대응 라이프 사이클(Life-Cycle) 수립에 따른 단위요소별(예방, 탐지, 대응, 보고, 공유) 관리

☐ 추진성과

○ 중대피해를 동반한 사이버 보안사고 ZERO화 달성

○ 주·야간 전담 모니터링을 통한 보안서비스 대응수준 3등급 → 1등급 향상

통합 전		통합 후(개선점)	
· PC/서버 악성코드 감염 및 권한 탈취 발생('14년 12월) - 약 5개월 후 발견 및 신고 · 대응 수준 : 3등급 이하	⇨	· 아파치 웹 서버 악성코드 설치 시도('17년 9월) - 1시간 미만 탐지 및 차단 · 대응 수준 : 1등급	

※ KISA 보안서비스 지표 기준 : 1등급 1~60분, 2등급 1~2시간, 3등급 2~4시간

☐ 향후계획

○ 일부 노후화된 보안장비의 교체 및 고도화 추진(인터넷망 분리사업 연계)

○ 전문 분야별 통합보안관제센터 구축

– 분야별 전문인력(관제, 분석, 운영, 진단 등) 확보로 긴밀한 대응 가능

기 획 처	처장 : 이재명 ☎6311-9390	팀장 : 안병윤 ☎9391	담당 : 임하연 ☎9394

2 정보시스템 계정·권한 관리체계 확립

안전우선

☐ 추진목적

○ 대·내외적으로 정보시스템 계정·권한관리 소홀에 따른 정보유출사고발생

○ 계정·권한 관리체계 및 기준수립으로 보안사고 위험 발생 가능성 축소

☐ 추진내용

○ 정보시스템 계정 및 권한관리 정책 및 상세기준 마련 시행

– 정보시스템 관리자들의 계정·권한관리 실천력 향상

○ 체크리스트 기반 계정 및 권한 관리실태 점검 체계화

– 체크리스트 기반 자체점검 및 점검결과 점수화 산출을 통해 현 관리수준 진단과 함께 계정 및 관한 관리의 중요성 인지력 향상

☐ 추진성과

○ 인적오류로 인한 사고예방 관리노력 강화로 보안수준 향상 및 사고위험 축소

– 관리 현행화 및 권한부여 최소화로 적정성 확인과 오·남용 방지 기여

○ 서울시 정보시스템 사용자계정 점검관리 평가 결과 1위

– 전체 66개 서울시(본청 및 구청 등) 및 산하기관 중 1위(90.65점)달성

– 전체평균 76.54점, 투자출연기관 평균 80.99점

통합 전	통합 후(개선점)
· 정보시스템의 계정·권한 관리체계 및 기준 부재 · 정보시스템 관리자들의 계정·권한 관리 중요성에 대한 낮은 인지력	· 정보시스템에 대한 계정·권한 관리체계 수립 및 점검실시 - 평가: 체크리스트(40)+증빙자료(60) · 서울사산하기관 우수기관 선정 

☐ 향후계획

○ 주기적 점검 실시(분기 1회)로 보안 취약틈새 최소화 및 관리노력 확대

○ 정보시스템 계정·권한관리 자동화 도입 검토

– 취약성·생산력 저하 극복위한 자동화된 계정관리 솔루션 도입

정보보안처	처장 : 이재명 ☎6311-9390	팀장 : 안병윤 ☎9391	담당 : 고혜진 ☎9398