

과정명	
08차시	보안 관제

<1> 정보보호의 개념

[1] 정보보호와 정보보안

- 정보보호는 컴퓨터나 네트워크 상의 다양한 범법 행위로부터 정보를 보호하는 것을 뜻함
- 정보보호의 목적은 정보 제공의 주체인 공급자 측면과 정보 사용자 측면에서 물리적이고 논리적인 장치를 통해 사전에 방지하여 정보를 안전하게 보호하는 것임
- 정보가 안전하다는 것은 보호대상이 되는 정보의 기밀성, 무결성, 가용성이 모두 만족되어야 한다는 것을 의미함
- 정보보안은 정보의 수집, 저장, 가공, 검색, 송신, 수신 도중의 정보 유출, 훼손, 변조 등을 방지하기 위한 기술적, 관리적 방법. 즉, 정보보호의 기술, 시스템 보안, 해킹과 정보 보호, 컴퓨터 바이러스, 암호화 기술, 네트워크 보안, 웹과 전자우편 보안, 전자상거래 보안 등 컴퓨터 보안 전반에 관한 것이라고 할 수 있음
- 정보보호가 포괄적인 개념인 것에 비해 정보보안은 기술적인 개념으로 정보보호의 하위 개념이라고 할 수 있음

[2] 보안 관제의 의의

- 보안 관제는 조직의 중요 정보 자원을 보안 공격으로부터 보호하기 위한 일련의 활동으로 좁게는 보안 공격을 탐지하는 모니터링 활동을 의미하지만 넓게는 보안 공격을 분석하여 대응 및 예방까지 수행하는 일련의 통제활동을 포함하기도 함
- 보안 관제 운영은 조직 내의 전문적인 팀으로 직접 운영하거나 외부의 전문적인 업체에 위탁하는 경우로 나눌 수 있음

- 보안 관제 센터를 목적별로 분류하면 IoT 보안 관제, 클라우드 보안 관제, 빅데이터 보안 관제로 분류할 수 있음

(1) IoT 보안 관제

- IoT 보안 발달에 따라 개인의 사생활과 개인정보를 지키기 위해 외부의 공격에 대한 가정의 네트워크 통신망에 대한 관심이 증대되고 새로운 분야의 서비스 창출에 기여할 것으로 보임

(2) 클라우드 보안 관제

- 클라우드는 다양한 IT 기술과 융합된 컴퓨팅 환경으로 여러 취약점이 발견될 수 있음
- 수 많은 데이터가 저장된 상태로 데이터의 관리 및 안전성에 대한 관심이 집중되고 있기 때문에 안정적인 클라우드 서비스의 제공이 요구됨

(3) 빅데이터 보안 관제

- 실시간 사이버 공격을 탐지하는 풀패킷 캡처 시스템으로 네트워크 상에서 일어나는 모든 행위에 대한 확인이 가능한데 이를 위해서는 빅데이터 엔진과 대용량 저장장치가 필요함

- 보안 관제 센터를 기능별로 분류하면 네트워크 공격에 대한 모니터링 관제인 IPS/IDS 관제 서비스, Firewall 관제 서비스, UTM 관제 서비스, DDoS 방어 서비스 웹 공격에 대한 모니터링 관제인 WAF 관제 서비스 서버 및 네트워크 장비에 대한 공격 모니터링 관제인 SMS, NMS 관제 서비스, 사용자 컴퓨터 모니터링인 NAC 관제 서비스로 분류 할 수 있음

- 보안 솔루션

보안 관제 서비스	<ul style="list-style-type: none"> 고객의 정보 기술 자원 및 보안 시스템에 대한 운영 및 관리를 전문적으로 아웃소싱하여 각종 침입에 대하여 관제 센터에서 실시간으로 중앙 감시, 분석, 대응하는 서비스
통합 보안 관리	<ul style="list-style-type: none"> 방화벽, 침입차단시스템, 침입탐지시스템, 가상 사설망 등의 보안솔루션들의 로그, 이벤트를 하나로 모으는 통합 보안관리 시스템 서로 다른 기종의 보안 장비를 통합 관리하는 기능과 네트워크 자원 현황을 모니터링하는 보안 모니터링 기능을 제공
보안정보 및 이벤트 관리	<ul style="list-style-type: none"> 보안 정보관리와 보안 이벤트 관리를 통합한 시스템 2015년 가트너에 의해 처음 도입 빅데이터 수준의 장시간 심층 분석 인덱싱 기반
위협 관리 시스템	<ul style="list-style-type: none"> 2003년 1.25 인터넷 대란을 기점으로 각 기관에서 외부 위협으로 부터 내부 정보자산을 보호하기 위해 위협을 조기에 감지하고 발생한 위협을 감소 또는 제거하는 것을 목표로 만들어진 관리 시스템
위협 관리 시스템	<ul style="list-style-type: none"> 방화벽, 가상 전용 네트워크, 침입 차단 시스템, 웹 콘텐츠 필터링, 안티 스팸 소프트웨어 등을 포함하는 여러 개의 보안 도구를 이용한 관리 시스템

- 보안 관제는 관련 정보를 수집하기 위한 보안 관제 시스템과 이러한 시스템을 운영 및 관리하는 보안 관제 조직으로 이루어져 있음

(1) 보안 관제 시스템

- 침입을 탐지하고 대응하기 위한 시스템 필요
- 침입탐지 시스템, 침입방지 시스템, 침입차단 시스템과 같은 정보보호 시스템 활용
- 지능화된 공격을 탐지하고 대응하기 위해 다양한 시스템에서 발생하는 로그와 이벤트를 활용한 통합 보안 관제 전용 시스템을 이용하는 방향으로 발전
- 보안 관제 시스템의 구성

구분	역할	예
정보 시스템	보안 관제의 대상, 보안 공격자의 침해 대상	윈도우, 서버, DBMS, 네트워크 장비 등
정보 보호 시스템	침입 탐지 및 대응을 위한 정보 제공	IDS/IPS, 방화벽, NAC, DLP 등
통합 보안 관제 시스템	침입 탐지 정보의 수집 및 처리	SIEM/ESM 등

(2) 보안 관제 조직

- 탐지 및 예방의 역할을 수행하는 보안 관제 모니터링 팀, 대응 및 예방의 역할을 수행하는 침해 사고 대응 팀, 공유 및 개선의 역할을 수행하는 정보 공유 분석 센터로 구성

1) 보안 관제 모니터링 팀

- 365일 24시간 동안 보안 관제 시스템에서 발생하는 이벤트에 대해 모니터링
- 침해 사고 발생 전 보안 취약점에 대해 사전 조사
- 평상시와 다른 이상 트래픽 등의 이벤트가 발생한 경우, 정해진 절차에 따라 보고하고 이벤트에 대한 대응 조치가 시작되도록 함

2) 침해 사고 대응 팀

- 이상 트래픽이나 이벤트에 대해 상세 분석을 통해 여부를 판단하고 이에 대한 대응 조치 수행
- 조직에 따라 보안 취약점 사전 조사 업무 수행

3) 정보 공유 분석 센터

- 각 산업 분야별로 보안 침해 사고에 효과적으로 공동 대응하기 위한 조직

- 국내에서는 금융감독원 주도의 금융 정보 공유 분석 센터, 통신 사업자를 중심으로 사이버테러 취약점과 침해 요인, 대응 방안에 관한 정보를 가입 기관에 제공
 - 침해 사고가 발생하면 실시간 정보와 분석 업무 수행
- 보안 관제 센터의 운영은 탐지/분석, 대응/조치, 보안대책/보고의 세 단계로 이루어짐
- (1) 탐지/분석
 - 관제 센터의 담당자가 분석을 요청하면 분석담당자가 특정 자원 모니터링을 하거나 연관성 분석, 정책에 따른 경보 및 전파나 로그 분석을 이용해 의뢰된 분석 요청에 대해 분석하고 분석 결과를 통해 1차 대응 방안을 지시함
 - (2) 대응/조치
 - 담당자가 총괄 담당자에게 보고를 하고 2차 대응 지시를 받아 공격 IP를 차단하거나 블랙리스트를 관리하는 등의 대응과 조치를 취함
 - (3) 보안대책/보고
 - 1, 2차에 걸친 조치 이후 다음을 위해 보안 대책 방안을 작성하여 공유
 - 보고서를 작성하여 이후 유사한 문제가 발생하는 것을 미연에 방지

<2> 보안 관제의 수행 원칙과 업무 유형

[1] 보안 관제의 수행 원칙

- 보안 관제는 무중단의 원칙, 전문성의 원칙, 정보 공유의 원칙에 따라 운영되어야 함
- (1) 무중단의 원칙
 - 보안 공격을 신속히 탐지/차단하기 위해서는 24시간 365일 중단 없이 서비스 제공
 - 기관의 업무 네트워크를 마비시키는 DDoS 보안 공격들이 발생할 수 있기 때문에 보안 공격에 대한 신속한 탐지 및 대응 필요
 - 보안 관제 운영 조직에서 항상 적정수의 보안 관제 인력 유지 체계 필요
 - (2) 처리량의 최대화
 - 정보 보호 시스템 및 통합 관제 시스템 등에 대한 지식과 네트워크 등의 이론에 대한 전문 지식 및 노하우 등 필요
 - 침해 대응 팀의 인력이라면 프로그램 분석 및 포렌식 기술 등에 대한 지식, 경험 및 노하우 중요
 - 전문성에 따라 탐지할 수 있는 보안 공격의 범위가 달라질 수 있음
 - (3) 응답 시간의 최소화
 - 보안 공격은 동일하거나 유사한 공격이 여러 조직이나 기관을 걸쳐 동시 다발적으로 발생
 - 한 보안 관제 조직에서 보안 공격을 사전에 미리 탐지했다면 다른 보안 관제 조직에 공유
 - 관계 법령이 위배되지 않는 범위 내에서 보안 관제 관련 정보 신속히 공유

[2] 보안 관제의 업무 유형

- 보안 관제 업무는 고객의 특성을 고려하여 직접 관제, 파견 관제, 원격 관제의 3가지 유형의 서비스 제공 형태를 보이며, 최근에는 클라우드 관제 분야까지 확대되고 있음
 - 보안 관제 업무는 보안 관제가 운영되는 조직에 따라 직접 관제, 파견 관제, 원격 관제, 클라우드 관제, 하이브리드 관제로 분류할 수 있음
- (1) 직접 관제
 - 내부에 직접 관제 시스템 구축 및 구축에 투입되는 인력이 내부의 자체 인력
 - 보안 관제 시스템의 구축 및 운영에 필요한 보안 관제 인력을 자체적으로 양성하고 관리
 - 보안 관제 관련 업무의 연속성이 보장되나 조직의 특성 및 규모에 따라 보안 관제 인력의 전문성이 다소 떨어질 수 있음
 - (2) 파견 관제

- 관제 대상 기관이 자체적으로 보안 관제 시스템을 구축하고 보안 관제 전문업체로부터 전문 인력을 파견 받아 침해/장애 발생 시 즉각적인 관제 업무를 수행
- 파견 관제의 대상은 공공분야 및 금융권
- 고객사에 특화된 관제서비스 제공이 가능하며, 침해/장애 발생 시 즉각적인 조치가 가능하고 업무 연속성 및 효율성 증대라는 장점이 있으나 인력 관리가 필요하고 단가가 높음

(3) 원격 관제

- 관제서비스업체에서 보안 관제에 필요한 관제시스템을 구비하고 대상 기관의 침입차단시스템 등 보안장비 중심으로 보안 이벤트를 상시 모니터링하여 침해사고 발생 시 긴급 출동하여 대응 조치하는 서비스 형태
- 파견 관제에 비해 저렴한 단가의 인력과 별도의 회선 구축 없이 인터넷망을 통한 관제가 가능하다는 장점이 있으나, 한정된 서비스 제공과 사이트에 특화된 관제 서비스에 어려움이 발생하고, 침해/장애 발생 시 즉각적인 조치가 어려우며 통보는 즉시 가능해도 조치를 위한 인력 수급이 필요함

(4) 클라우드 관제

- IT자원을 인터넷 접속을 통해 사용하는 클라우드 환경에 대한 관제
- 기업은 클라우드 내에서 일어나는 보안 위협을 모니터링하여 오프라인 환경과 동일한 보안관제 서비스를 받음
- 클라우드 서비스를 제공하는 업체가 대상
- 보안관리 영역에 대한 직접 관리 부담이 감소하고 관제전문인력이 제공하는 보안관제 서비스를 제공 받을 수 있으며, 로컬에 장비 설치 및 유지보수가 필요하지 않다는 장점이 있으나 관제 대상 및 업무를 이해하기 어렵고 리스크가 매우 크며 고객의 비즈니스를 이해해야 하는 어려움이 존재함

(5) 하이브리드 관제

- 보안 기업의 통합보안관제센터에서 확보한 위협 정보를 원격으로 제공하여 파견 관제의 한계점을 보완하는 방식
- 필요한 시간에만 원격 관제 형태로 관제 업무를 수행
- 원격 관제의 장점과 파견 관제의 장점을 골고루 융합시킨 서비스
- 침해/장애 시 파견 인력을 통한 선 조치 후 원격 관제 팀의 공조 가능하다는 장점이 있으나 파견 인력의 등급에 따른 서비스의 퀄리티 편차가 발생할 수 있으며 파견 인력에 대한 관리가 필요함

<3> 보안 침해 대응

[1] 탐지 규칙

- 보안 공격을 대응하는 방법으로 탐지 규칙을 이용하여 IDS/IPS 등에서 보안 공격을 사전에 탐지하는 방법이 있음
- 탐지 규칙은 특성 악성코드 또는 보안 공격이 네트워크로 유입되는 것을 탐지하기 위해 개발된 시그니처를 말하며, 탐지 패턴 또는 탐지 룰이라고도 부름
- 보안에서 시그니처는 특정 악성코드 혹은 취약점 등을 식별할 수 있는 문자열을 뜻함
- 새로운 공격이 시도될 때마다 그 공격에 대응하는 탐지 규칙 또한 같이 개발됨
- 탐지 규칙은 탐지 조건을 설정하는 옵션과 대응 동작과 탐지 조건을 적용할 정보를 설정하고 시그니처에 해당되는 문자열을 정의하는 헤더로 이루어져 있음
- 탐지 헤더는 대응 동작, 프로토콜 종류, 출발지 및 도착지의 IP 주소, 출발지 및 도착지 포트, 방향으로 구성되어 있음
- 보안 공격에 대해 만들어지는 탐지규칙이 경우에 따라서는 정상적인 네트워크 트래픽을 보안

공격으로 판단하거나 반대로 악의적인 보안 공격 트래픽을 정상 접근으로 잘못 판단하기도 함

(1) 긍정 오류

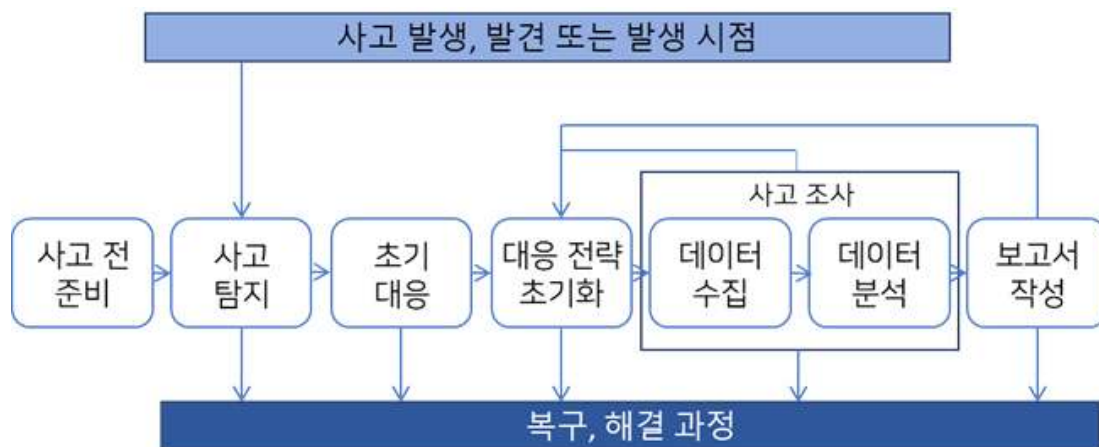
- 정상적인 접근을 공격 시도로 오해
- 정상적인 요청의 차단으로 가용성 침해

(2) 부정 오류

- 공격 시도를 정상적인 접근으로 인식하여 통과시킴
- 실제 보안 공격이 차단되지 못해 보안사고가 발생할 수 있기 때문에, 보안성의 관점에서는 부정 오류가 더 위험함

[2] 침해 대응

- 최근 발생한 보안 침해 사고는 복잡하고 다양한 기술을 이용하기 때문에 검증된 보안 기술을 지속적으로 적용하여 사고 발생을 억제해야 하며 침해 사고가 발생한 경우에는 이를 철저히 조사 및 대응하여 향후 동일한 사고가 발생하지 않도록 조치해야 함



(1) 사고 전 준비

- 사고 발생 전 침해 대응 팀이 미리 조직적인 대응 준비를 하는 단계
- 침해 대응 팀은 조직적인 침해 대응 체계의 핵심이며, 보안 전문가뿐 아니라 각 분야의 전문가로들로 구성함

(2) 사고 탐지

- 이상 징후를 확인하고 침해사고 발생을 발견하는 단계
- 보안 침해 사고는 통합 보안 관제 시스템 등에 의해 실시간으로 발견
- 침해 사고 발생 이후 사고 징후에 대해 추가 조사 중 발견하는 경우도 존재

(3) 초기 대응

- 초기에 사고를 조사하여 사고 정황에 대한 사항을 기록하고 관련 부서에 통지
- 해당 시스템의 네트워크 단절 및 방화벽 설정 등 변경
- 초기 대응을 마무리 하면 실제 사고 여부, 침해된 시스템에 대한 적절한 대응책의 유무, 사건의 유형, 사고로 인한 잠재적인 업무 영향 등에 대해서 알 수 있음

(4) 대응 전략 수립

- 현재 상황에서 최적의 대응 전략을 결정하고 관리자 승인을 획득하는 단계
- 초기 조사 결과를 참고하여 소송이 필요한 사항인지 결정
- 사고 조사 과정에 수사기관 공조 여부를 판단

(5) 사고 조사

- 포렌식 등을 통하여 데이터를 수집하고 분석하는 단계
- 자료 수집은 사건 분석을 하는 동안 깊이 살펴보아야 할 범행들과 단서들의 수집 과정으로 법적 소송을 염두에 둔다면 증거가 무결성과 적법성을 유지하도록 디지털 데이터 수집

(6) 보고서 작성

- 의사 결정자가 쉽게 이해할 수 있는 형태로 사고에 대한 정확한 보고서 작성

(7) 복구 및 해결

- 향후 유사 공격을 식별 및 예방하기 위한 보안 정책을 수립하고 현재 문제가 되는 조직의 프로세스를 수정하는 단계
- 시스템에 설치된 백도어 등의 악성코드를 제거하고 시스템의 서비스가 가능하도록 네트워크 연결
- 계정 정보의 탈취가 발생했을 수 있기 때문에 관리자 및 시스템의 비밀번호 재설정
- 운영체제 및 백신 등의 보안 패치 적용

- 침해 사고 발생 시 사고의 징후

- (1) IDS/IPS에서 탐지한 원격 접속
- (2) 여러번 로그인을 실패한 로그
- (3) 관리자가 생성하지 않은 계정 발견
- (4) 출처 불명의 파일 또는 프로그램 발견
- (5) 로그 파일의 삭제
- (6) 시스템 성능 저하 및 충돌 발생
- (7) 업무 외 시간대에서의 시스템 활동 기록

- 침해 사고별 대응 전략

- (1) DoS 공격
 - 수사 기관과의 공조를 통해 라우터 등의 네트워크 장비 재설정
- (2) 비인가 접근 및 사용
 - 가능성 있는 IP 주소 식별, 증거물 포렌식 이미지 확보
 - 침입에 사용된 취약점 확인 및 이에 대한 패치 시행으로 시스템의 보안 재설정 및 복구
- (3) 홈페이지 공격
 - 수사 기관에 의뢰하여 범인 검거를 요청하고 웹 사이트 복구
- (4) 중요 정보 훼손 및 유출
 - 관련된 시스템의 이미지를 확보하고 도난 신고 및 법적 대응 준비
 - 수사 기관의 참여로 상세한 조사가 시작될 수 있으니 일정 기간 동안 시스템은 오프라인 유지

[3] 보안 관제 센터의 관리와 연동

- 보안 관제센터 관리 방안에는 조직변화 관리 방안, 모니터링 인력 운영 방안, 사고 유형별/상황별 사전, 사후 대응 기술과 프로세스에 따른 처리 기술, 정보 보호 국제 표준 인증 등이 있음
- (1) 조직변화 관리 방안
 - 조직의 연속성이라는 경영의 주요 목표 달성을 위해 변화는 필연적
 - 변화의 원리에 대한 이해와 저항의 종류 및 변화 관리 방안을 숙지하여 변화에 적극 대응
- (2) 사고 유형별/상황별 사전, 사후 대응 기술과 프로세스에 따른 처리 기술
 - 1) 대용량 로그 처리 기술
 - 빅데이터, 빠른 검색 시간 제공, 분석 처리 기반의 확장성
 - 2) 정보와 로그의 융합기술
 - 관제 결과의 정보와 로그와의 융합된 연관성 정보를 획득하기 위한 방법과 절차의 자동화
 - 3) 악성코드 분석 기술
 - 전문가 분석 시간 감소를 위한 자동화된 분석 기술, 분석 패턴 DB 공유화 방법
 - 4) 네트워크 패킷 분석 기술
 - 원본 패킷 저장 기술, 자동화된 난독화 패킷 해석 기술, 자동화된 데이터 추출 및 검색 기능

5) 모바일 환경 보안 기술

- 스마트기기의 보안 적용 기술, 모바일과 클라우드 환경에서의 보안위협 탐지 기술

(3) 정보 보호 국제 표준 인증(ISO27001)

- 물리적, 기술적, 관리적 보호 조치 수준에 대한 객관적인 평가를 통해 인증서를 발급하는 것
- 적합한 정보보호 관리 수준을 평가하는 제도

- 보안 관제 센터 운영의 개선 방안은 보안관제 업무 관리 부분과 침해 사고 관리 부분으로 나눌 수 있음

(1) 보안 관제 업무 관리 부분

- 보안관제 업무 수행을 위한 정책, 조직, 시스템 및 인력 관리 부분

1) 보안관제 수행 조직을 하나의 독립 조직으로 간주

2) 정보 보호 관리 체계라는 표준을 바탕

3) 보안 관제에 필요한 정책, 조직, 시스템에 대한 수준 관리 등의 항목을 통해 개선점 도출

(2) 침해 사고 관리 부분

- 침해사고 관리 방법을 통해 취약점 분석과 평가, 침해사고 탐지와 대응, 보안관제 서비스 품질 관리 등의 개선 항목 도출