情 報 保 護 學 會 誌
第20卷 第6號, 2010. 12

「위험관리 기반 침해사고 조기 대응 체계」 구축 사례

김 진 섭*

요 약

정신한은행은 '10년 1월부터 6월까지 약 6개월 동안 「위험관리 기반의 침해사고 조기 대응체계 구축」 프로젝트를 수행하여 침해 시도 조기 탐지 및 대응을 위한 「침해사고 조기 경보 시스템」 및 「침해 사고 대응 프로세스 전산화」와 침해사고의 사전 예방 강화를 위한 「정보시스템 상시 취약점 점검 체계」를 모두 하나의 프레임웍으로 묶어 통합 구축하였다.

신한은행은 이를 통해 내부망 및 인터넷 서비스망에 대해서 이미 알려진 네트웍 침입 패턴뿐만 아니라 네트웍 트래픽 전반에 대한 모니터링을 대폭 강화하여 기존 침입탐지 시스템이나 디도스 대응 시스템 등에서 탐지가 불가능했던 신종 침입 유형이나 소규모 디도스 공격 트래픽도 자동화된 탐지가 가능하게 되었다. 그리고 탐지된 침입시도의 유형 및 위험 수준에 따라서 사전 정의된 침해사고 대응 프로세스를 통해, 정보보안 담당자가 관련 부서 및 경영진의 요구사항에 각각 최적화된 전용 상황 모니터링 화면을 공유하며 침해사고를 효과적으로 공동 대응할 수 있게 되었다. 또한 정보시스템 전반에 대하여 상시 취약점 점검을 실시하고 그 점검 결과를 데이터베이스로 구축하고 정보시스템의 위험 수준에 따른 체계화된 대응 방안을 수립할 수 있게 되었다.

신한은행은 금번 구축된 시스템을 정보보안 영역 전반으로 확대하여 동일 프레임웍에서 위험관리 기반의 내부 정보 유출 체계를 구축하고, 향후 그룹사에도 확대 적용하여 전체 그룹사의 보안 수준을 제고하는 데 활용할 계획이다.

※ 금번 구축 사례에서 소개된 침해사고 조기 대응체계는 구축 완료 시점에 사내 명칭 공모를 통해 "Ageis" 로 선정되었으며, 본 사례에서도 전체 시스템을 가리킬 때 Ageis로 지칭한다. Aegis는 그리스 신화에서 Zeus 신이 딸 Athena 신에게 주었다는 방패로써 보호, 후원, 지도 등의 뜻을 가지며, 이지스 또는 아이기스 라고 발음된다.

Ⅰ. 구축배경

1.1 신한은행의 비즈니스와 정보동향

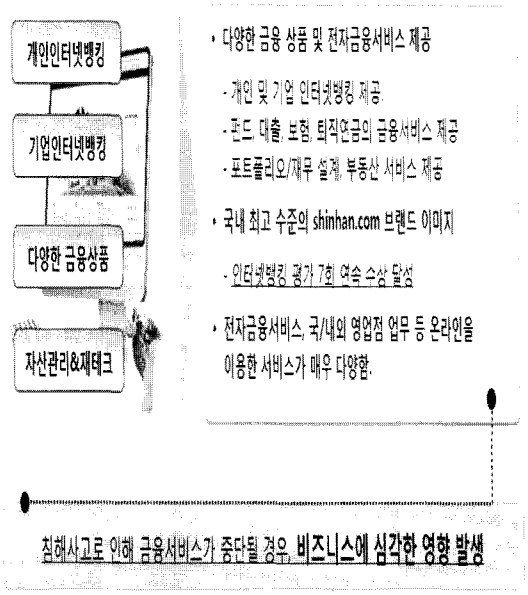
신한은행은 대한민국의 대표적인 우량 은행으로서, 개인 및 기업 뱅킹, 펀드, 대출, 보험, 퇴직연금 등 다양한 금융 서비스에 대하여 국내 최대 규모 수준의 고객을 보유하고 있으며, 이러한 서비스는 대부분 'shinhan.com' 브랜드로 고객에서 인터넷을 통하여서도 제공되고 있다.

이런 활발한 비즈니스를 위한 국/내외 영업점 및 본부부서의 업무는 모두 내부 업무망 및 인터넷과 연동된 다양한 정보시스템을 통해 이루어지고 있으므로 은행 전산 시스템이 일부라로 침해사고로 인하여 중단될 경우, 은행은 전체 비즈니스에 심각한 영향을 받을 뿐만 아니라, 사회적으로 큰 파장을 줄 수 있다. 따라서, 신한은행은 비즈니스의 연속성을 안정적으로 보장하기 위하여 각종 침해사고에 대한 강력한 예방 및 대응 체계의 구축이 필요하다.

1.2 침해사고 조기 대응 체계 구축 배경

신한은행의 정보보안관리 체계는 업무 시스템의 가용성과 내부 정보의 기밀성, 무결성 보장을 목표로 전자금융감독규정, 정보통신기반시설보호법 등 관련 법규와 자체 내규에 따른 정보보안관리 정책 및 통신, 서버, DB, 단말 및 응용프로그램 등 각 부문별로 다양한 보안 시스템으로 구성되어 있으며, 자체 24*365 보안관제체계를 운영하고 있으며 정보시스템 전반에 대하여 매년 1회 이상 보안컨설팅 전문업체와 함께 보안 안전 진단

* 신한은행 IT총괄부 (jskim89@shinhan.com)



〔그림 1〕 신한은행의 금융서비스 현황

업무를 공동 수행하고 있다.

하지만, 이러한 노력에도 불구하고 각종 침해사고로부터 정보시스템을 보호하기 위한 보안 취약점 진단 업무는 매년 또는 분기에 한 번씩 수행하는 1회성 프로젝트로서 신규 서비스의 이행이나 기존 시스템의 증설에 따른 서버 시스템의 신규 구축이나 서버 운영체제 및 웹, WAS, DBMS 등의 응용프로그램의 운영 중 세부적인 환경 설정 변경 시 발생할 수 있는 보안 취약점이나, 최신의 침해 기법에 대해서는 대응이 지연되는 한계가 발생하였다.

또한, 각종 대내외의 침입시도로부터 정보시스템을 보호하기 위해 구축한 침입탐지 시스템이나 디도스 대응 시스템은 침입 시도 패턴이 정형화되지 않은 침입 유형에 대해서는 정확한 탐지가 불가능하거나 조기 탐지가 어려워 그만큼 차단 대응이 늦어질 수 있는 기술적인 한계가 확인 되었으며, 침입 시도가 탐지된 경우에도 기 운영중인 정보보안 시스템에 의한 통제 가능 여부 및 공격 목표가 되는 서버나 응용프로그램 같은 정보자산의 중요도 및 해당 공격에 대한 보안 취약점 유무에 따른 영향도, 즉 각 공격 유형별 실제 위험도에 따른 차별화된 대응을 하기 어려워 침해시도 전반에 대한 차단 대응의 효율성이 저하되는 문제점이 관측 되었다.

기존 운영중인 정보보안관리체계에서 발견된 이러한 문제점들에 대한 해결 및 `09년 발생한 7.7 디도스 대란과 같은 정보보안 침해사고에 대한 좀더 효과적인 대응 체계의 수립을 위해 정보보안관리 체계에 대한 현안 및 문제점 분석을 통한 개선 방안의 추진이 필요하였다.

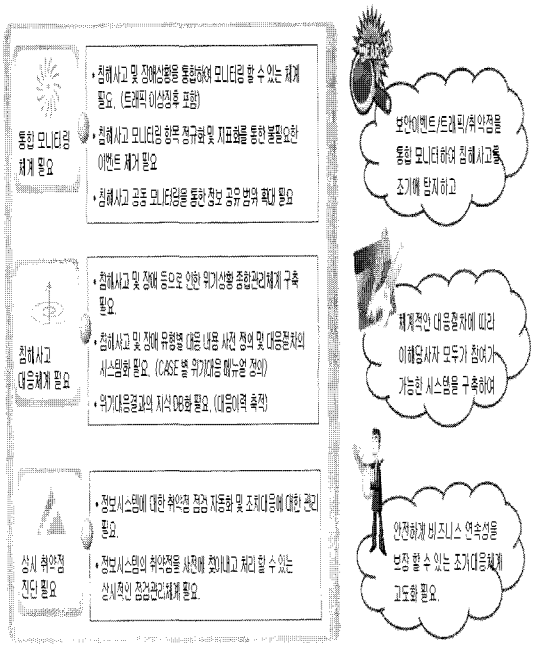
1.3 침해사고 조기 대응 체계 구축 개요

1.3.1 정보보안 관리체계 현안 분석

기존 침해사고 대응 체계를 주 대상으로 전면적인 재검토를 수행한 결과, 다음의 3가지 주요 이슈 사항을 도출하였다.

첫째, 산재되어 있는 개별 모니터링 시스템을 통합하여 관리 할 수 있는 체계와 불필요한 이벤트를 제거할 수 있는 모니터링 항목의 정규화 및 지표화가 부족했다. 이는 침해 사고 대응 업무를 보안담당자만이 아닌, 관련 이해당사자에게까지 확대하는 데 필수 조건이다.

둘째, 침해사고 발생 시 사전에 정의된 매뉴얼에 따라 신속하게 대응 할 수 있는 위기상황 종합관리체계 구축이 필요했다. 지난 7.7 디도스 대란과 같이 실제 일각을 다투는 침해사고가 발생하게 되면 숙련된 정보보안 담당자라도 당황하기 마련이며, 침해사고에 대한 분석 및 대응 못지않게 유관부서 및 경영진, 감독 기관 등



〔그림 2〕 정보보안관리체계 현안 분석 결과

에 보고를 하기 위한 절차도 중요하므로 사전에 세부 내용까지 구비된 매뉴얼의 중요성이 부각되었다.

셋째, 정보시스템의 취약점을 사전에 찾아내고 제거하여 침해사고를 근본적으로 예방하기 위한 보안 안전 진단 업무의 개선이 필수적이며, 이를 위해 상시적인 취약점 점검 및 조치 대응까지 전 과정에 대한 시스템화된 관리가 반드시 필요하다.

1.3.2 침해사고 대응 체계 문제점 및 개선 방향 도출

정보보안관리체계의 주요 현안 분석 결과를 바탕으로 구체적인 개선 방안을 수립하기 위하여 기존 침해사고 대응 체계를 침해사고 예방, 모니터링, 분석 및 대응 등 3개 부문으로 분류하여 세부 운영 현황 분석을 통해 각각 다음과 같은 문제점과 개선 방향을 도출하였다.

〔표 1〕 침해사고 대응 체계의 문제점 및 개선 방향

구 분	문제점	개선 방향
침해사고 예방	■ 정보시스템에 대한 취약점 점검 및 대응을 분기별로 수행하여, 주요 환경 변경 시 취약점 파악 및 조치 불가 ■ 최신 보안 이슈에 대한 관리체계 부재로 인해 신종 보안 이슈에 대한 신속한 확인 및 시스템 영향도 분석 등의 사전 대응 미비	■ 정보시스템에 대한 상시 취약점 점검 체계 구축으로 신규 취약점에 대한 대응 강화 ■ 금보원, 금융ISAC 등 정보보호전문기관의 최신 보안 이슈에 대한 DB 축적 및 체계적인 관리를 통한 신종 침해사고 사전 예방 강화
모니터링	■ 現 보안 이벤트 중심의 모니터링은 신종 보안 위협에 대한 공격 패턴이 보안시스템에 적용되기 전까지 자동 탐지 및 대응 불가 ■ 이상징후에대한 탐지 및 분석이 각 보안시스템별로 수행되어 보안 시스템 간 상호 연관된 이상 징후에 대한 탐지 어려움	■ 트래픽 추이분석, 유해 트래픽 모니터링으로 신종 취약점에 대한 탐지 및 분석 강화 ■ 보안시스템간상관분석으로 보안시스템 상호 연관된 이상징후에 대한 종합 분석 강화
분석 및 대응	■ 이상징후 발생시 관리자가 수동으로 상세 분석을 실시하여 이상징후에 대한 세부 정보 파악 및 분석에 많은 시간이 소요됨 ■ 침해 시도의 위험 수준 및 정보시스템별 위험도에 따른 대응 체계 미비	■ 이상징후 탐지 및 분석 자동화로 침해사고 초기 대응 시간 단축 ■ 정보시스템의 위험도 관리 및 침해시도의 위험 수준에 따른 대응 체계 수립

1.3.3 침해사고 조기 대응 체계 구축 프로젝트 추진

기존 침해사고 대응 체계의 문제점 해결을 위한 개선 방향을 구체화하여 실행하기 위한 방안 검토 결과, 현재 은행의 정보시스템과 정보보안관리체계를 잘 이해하고 있는 기존 정보보안담당자가 주관자가 되어야 하지만 기존 다양한 정보시스템 및 침해시도 유형별 위험 수준 평가 모델 개선이나 침해 트래픽 분석, 상시점검 체계의 시스템화 등은 관련 업무 전문가의 지원과 함께 위협관리시스템(Threat Management System), 시스템 취약점 점검툴 등과 같은 보안 솔루션의 추가 구축이 필요한 것으로 확인되었다.

그러므로 본 업무 수행을 위해 정보보안 담담자가 보안컨설팅 전문 업체 및 보안솔루션 공급사와 함께 공동으로 프로젝트를 추진하게 되었다.

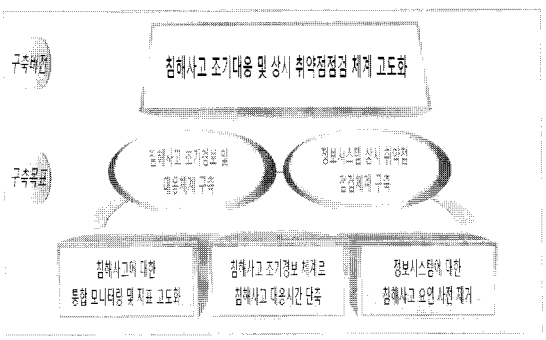
Ⅱ. 구축내용

2.1 구축목표

침해사고 조기 대응 체계 구축 프로젝트를 착수하면서 먼저 침해사고 사전 예방 강화, 침해사고 탐지 및 대응 강화를 위해 각각 다음과 같이 크게 두 가지 구축 목표를 수립하였다.

첫째, 「정보시스템 상시 취약점 점검 체계」를 구축하여 정보시스템에 대하여 이미 알려진 침해사고 요인을 최대한 사전 제거한다.

둘째, 「침해사고 조기 경보 및 대응 체계」를 구축



〔그림 3〕 Aegis시스템의 구축목표

하여 침해사고에 대한 통합 모니터링 및 지표를 고도화하고, 침해사고 조기 경보 체계를 운영하여 침해사고 대응 소요 시간을 최소화한다.

2.2 구축전략

2.2.1 정보시스템 상시 취약점 점검 체계 구축

정보시스템 상시 취약점 점검 체계를 효율적으로 구축하기 위하여 다음과 같이 3단계 추진 절차를 수립하였다.

첫째, 정보시스템의 보안 취약점 진단 및 대응 결과를 체계적으로 관리하기 위한 취약점 관리 데이터베이스(DB)를 구축한다.

둘째, 상시적으로 보안 취약점 점검을 실행하기 위하여, 보안 취약점 점검을 완전 자동화한다. 이를 위해 기 운영중인 시스템 취약점 점검 툴(스캐너)을 새로 구축한 취약점 관리 데이터베이스에 연동한다.

셋째, 취약점에 대한 조치 및 침해시도에 대한 대응 효율화를 위해, 시스템별 자동화된 위험 평가가 가능토록 한다.

2.2.2 침해사고 조기경보 체계 구축

침해사고 조기경보 체계를 효과적으로 구축하기 위해서는 다음과 같이 3단계 추진 절차를 수립하였다.

첫째, 디도스 등 신종 네트워크 침해시도에 대한 탐지 강화를 위해 유해 트래픽 모니터링 전문 솔루션인 위협관리시스템(TMS, Threat Management System)을 신규 도입하여 인터넷 접속 구간에 설치한다.

둘째, 침해사고 통합 모니터링 체계를 구축하여 기 구축된 침입탐지시스템(IDS), 침입방지시스템(IPS), 방화벽(FW), 디도스 대응 시스템과 신규 구축한 위협관리 시스템의 이벤트를 통합 분석하여 침입 시도를 조기 탐지할 수 있도록 한다.

셋째, 탐지된 침입 시도에 대해 자동화된 위험도 평가 체계 및 위험 수준별 대응 프로세스를 수립한다.

2.3 구축절차

2.3.1 추진 방안 수립

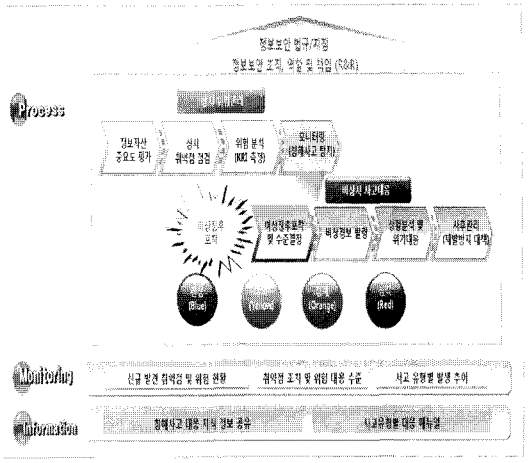
Aegis 시스템을 효율적으로 구축하기 위한 추진 방안으로서, 보안 파트에서 직접 다수의 개별 솔루션 공급사와 함께 시스템 통합 작업을 수행하는 방안(1안)과 보안파트에서 정보보안전문업체를 통해 침해사고 대응 프레임웍을 먼저 구성한 후 개별 솔루션을 연동하는 방안(2안)을 검토하였다.

〔표 2〕 프로젝트 추진 방안 검토

구분	업체별 추진	컨소시엄구성
추진방안	AA → 프레임웍 도입 BA → 침해사고 조기대응 체계 → 종합 관리 체계 CA → 보안 취약점 관리 체계	정보보호전문업체 AA BA → 프레임웍 구축 침해사고 조기대응 체계 → 종합 관리 체계 보안 취약점 관리 체계 CA

그 결과, 1안의 개별 업체들의 솔루션을 직접 연동 구축할 경우, 구축 솔루션 별 연동 및 통합 관리 체계가 미흡할 수 있어, 정보보안 파트에서 정보보호 전문업체로 구성된 컨소시엄을 먼저 구성하고 해당 업체의 프레임웍을 활용하여 개별 보안솔루션 업체의 솔루션을 각각 연동하는 것이 적합한 것으로 판단되어 최종적으로2안으로 결정하였다.

2안에 의해 정보보안전문업체는 다수의 정보보호 전



〔그림 4〕 Aegis 구축 방법론

※ (주1) Aegis: 금번 구축 사례에서 소개된 침해사고 조기대응체계는 구축 완료 시점에 사내 명칭 공모를 통해 "Ageis" 로 선정되었다. 본 사례에서도 전체 시스템을 가리킬 때 Ageis로 지칭한다. Aegis는 그리스 신화에서 Zeus 신이 딸 Athena 신에게 주었다는 방패로써 보호, 후원, 지도 등의 뜻을 가지며, 이지스 또는 아이기스 라고 발음된다.

문업체를 대상으로 제안평가를 통해, 에이쓰리시큐리티를 선정하였으며, Aegis 시스템의 기본 프레임웍으로는 동사의 전사적보안관리(ESP, Enterprise Security Platform) 을 채택했다. 그리고 유해 트래픽 모니터링 전용 시스템으로는 나우콤의 위협관리시스템(TMS, Threat Management System)을 선정하였다.

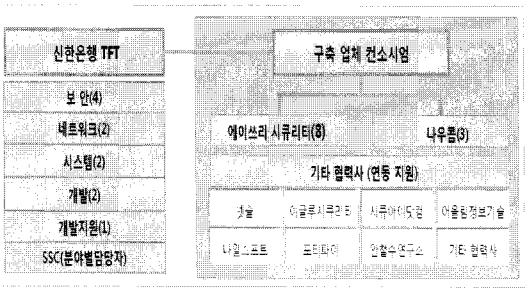
2.3.2 구축 방법론 선정

Aegis(1) 시스템의 효과적인 구축을 위한 방법론으로 기존 은행의 정보보안 정책 및 침해사고 대응 절차에 에이쓰리시큐리티의 위험관리 방법론(RCMM, Risk and Crisis Management Method)을 접목하여, 정보보안 위험에 대한 예방(상시위험관리), 침해사고대응(비상시 사고대응), 정보제공(침해사고 유형별 대응 매뉴얼 등) 및 보안정책관리(정보보안 법규/지침), 통합 모니터링(핵심위험지표 이용) 절차 등을 수립하였다. [1]

2.3.3 구축 조직 구성

Aegis 시스템 구축을 위해 정보보안파트에서 유관부서로 구성된 은행TFT 및 구축 업체 컨소시엄을 공동으로 묶어 추진 조직을 구성하였다.

공동추진 조직은 은행 TFT가 주축이 되어 전체 프로젝트를 총괄하고 구축 업체 컨소시엄에서는 에이쓰리시큐리티가 주축이 되어 나우콤 및 기타 협력사 간 협업을 조율했다. 신한은행 TFT는 보안팀(4명), 네트워팀(2명), 시스템팀(2명), 응용시스템 개발팀(2명), 시스템 개발 지원팀(1명) 및 시스템 운영 전담 조직인 신한 데이터시스템즈의IT-SSC(분야별 담당자)로 구성 됐고, 구축 업체 컨소시엄은 에이쓰리시큐리티(8명), 나우콤(3명) 외에 기타 신한은행의 협력 보안 업체들로 구성됐다.

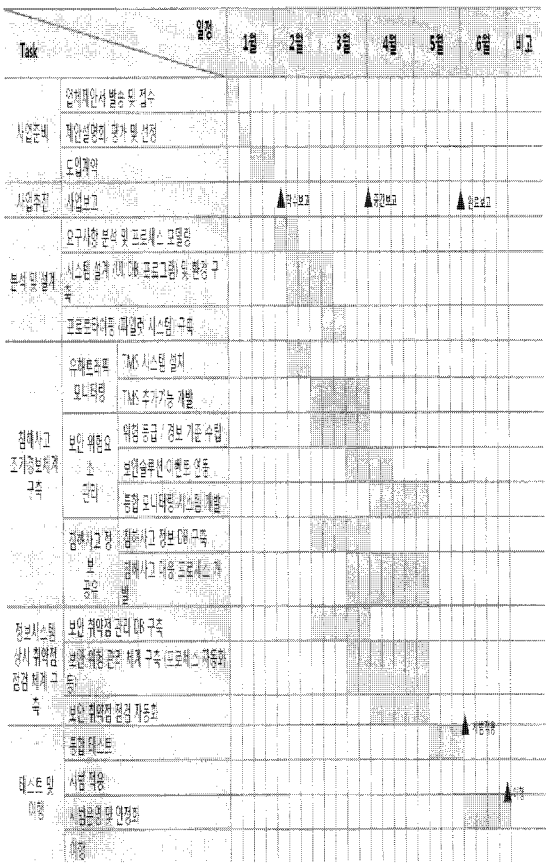


〔그림 5〕 조직 구성

2.3.4 구축 일정

Aegis 시스템의 구축은 최초 사업준비에서 테스트 및 이행까지 총 6개월에 걸쳐 진행 되었으며, 순수 시스템 구축 기간은 2010. 1. 15 ~ 5. 15까지 총 4개월이 소요 됐다. 세부 구축 경과는 다음과 같다.

- 사업 준비 기간: 제안 설명회를 통하여 구축 업체 평가 및 선정, 사업 착수 보고 실시
- 분석 및 설계 기간: 프로젝트의 요구사항 분석 및 프로세스 모델링, 시스템 구축을 위한 개발 환경 구축 및 현황 및 요구사항 분석한 내용을 토대로 시스템 설계를 수행하고 파일럿 시스템 구축
- 구축 기간: 침해사고 조기경보체계, 정보시스템 상시 취약점 점검 체계 구축
- 테스트 및 이행 기간: 통합 테스트를 실시 및 시범 운영 기간을 거쳐 본이행 실시



〔그림 6〕 Aegis의 구축 일정

2.4 시스템 구성

Aegis 시스템은 개념적으로 데이터 수집, 데이터 처리, 사용자 인터페이스, 내부 인프라 연동 등 크게 4 가지 부문으로 구성된다.

첫째, 데이터 수집 부분은 위협관리시스템(TMS), 보안관제시스템(ESM), 자동 취약점 점검 툴 등으로부터 정상/유해/ 실시간 트래픽, 침해(공격) 이벤트, 장애/자원 이벤트, 취약점 점검결과 데이터를 가져온다. 수집된 데이터는 Aegis 시스템의 하위 모듈들에서 입력 정보로 사용된다.

둘째, 데이터 처리 부분은 Aegis 시스템의 코어로서 「침해사고 통합 모니터링 모듈」, 「침해사고 대응 모듈」, 「취약점점검 대응 모듈」 등 3 가지 모듈로 구성되며, 각 모듈들은 보안관제시스템(ESM), 위협관리시스템(TMS), 시스템 취약점 점검툴, 사내 그룹웨어(전자결재시스템), 사내 문자 메시지 전송시스템(UMS) 등과 연동된다.

셋째, 사용자 인터페이스는 Aegis 시스템의 사용자별 역할(Role)과 책임(Responsibility)에 따라 접근 가능한 데이터 및 화면을 정의한다. Aegis 시스템에서 사용자 역할은 경영자/임원, 보안관리자/보안관제센터, IT상황반/위기대응조직/서버운영자/통신담당자 등으로 구분되며 역할에 따라 최적화된 화면 구성 제공 및 접근 권한이 제한된다.

마지막으로 내부 인프라 연동 부분은 Aegis 시스템 사용자들에게 필요한 알림(Alert)이나 전자결재 프로세스를 연동하기 위해 사내 전자메일 시스템, 메신저 및 문자메시지(SMS) 전송시스템(UMS)와 연계한 것으로 Aegis 사용자들 간 커뮤니케이션 강화 및 편의성 증대를 목표로 한다.

2.5 시스템 주요 기능

Aegis 시스템의 주요 기능은 침해사고 조기 경보, 침해사고 위기 대응, 정보 시스템 상시 취약점 점검 등 크게 세 가지로 구분할 수 있다.

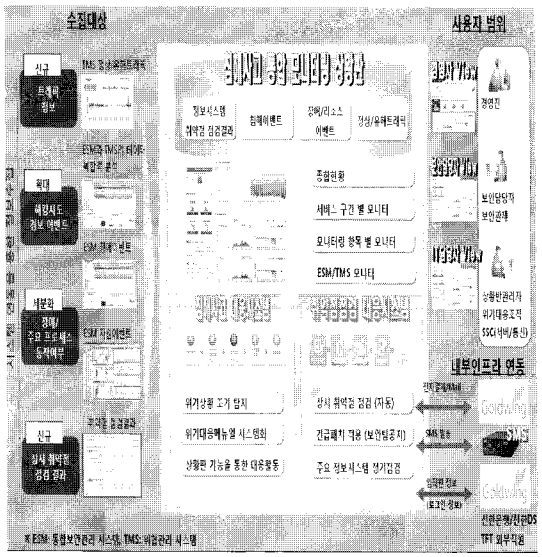
2.5.1 침해사고 조기경보

침해사고 조기 경보 기능은 침해사고 통합모니터링, 개별 모니터링 항목 관리, 통합 모니터링 항목 관리, 경보 심각도 관리 기능 등으로 분류된다.

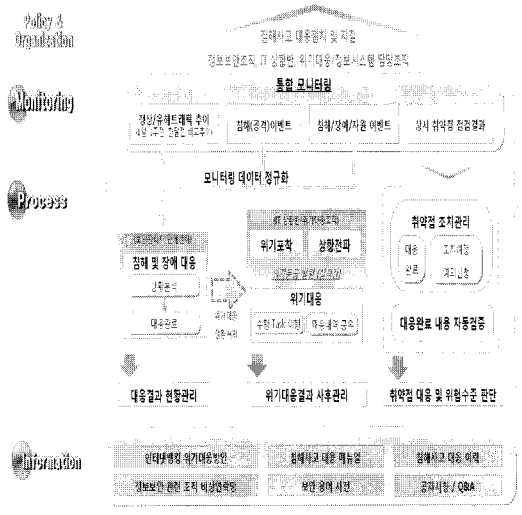
2.5.1.1 침해사고 통합모니터링

침해사고 통합모니터링 기능은 「종합현황 화면」과 「상세 현황 화면」으로 구분된다.

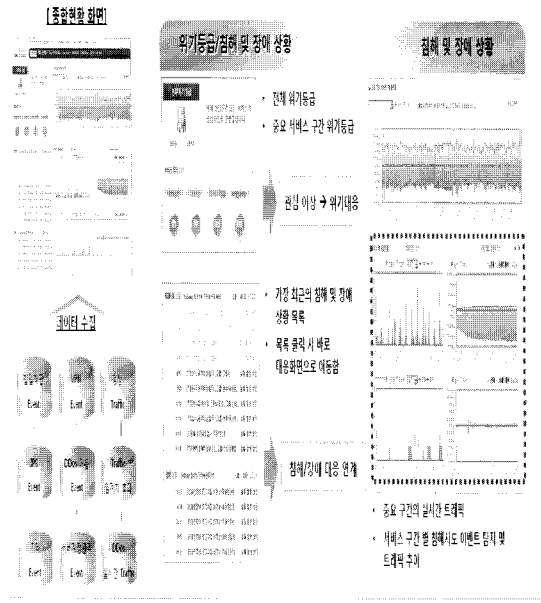
종합 현황 화면」은 은행 전체의 위기등급 및 서비스 위기상황을 '심각-경계-주의-관심-정상'으로 구분하여 보여준다. 위험수준에 따라 발생된 상황들은 글자색 및



〔그림 7〕 Aegis 시스템 개념 구성도



〔그림 8〕 Aegis 시스템의 주요 기능 구성



〔그림 9〕 침해사고 및 장애 상황 통합모니터링 체계

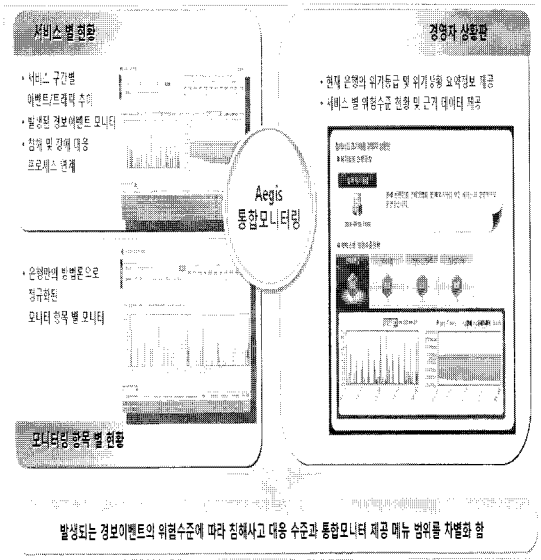
전용 아이콘으로 구분되어 표시되고, 마우스로 선택 시 바로 대응이 가능한 화면으로 이동된다. 또, 인터넷뱅킹 구간의 실시간 트래픽현황 및 주요 서비스구간에 대한 이벤트 발생건수 추이, 유해 트래픽 현황을 보여주어 트래픽 추이의 이상 변동에 대해 모니터링을 가능케 한다.

통합모니터링 상세현황」은 다시 「서비스별 현황」, 「모니터링 항목 현황」, 「경영자 상황판」으로 세분화 된다.

「서비스별 현황」은 은행의 주요 서비스 구간별로 이벤트/트래픽 추이 및 현재 발생된 경보 이벤트를 보여주며, 「모니터링 항목 현황」은 정규화된 모니터링 항목을 기준으로 침해시도 내역을 표시한다. 「경영자 상황판」은 은행의 경영진 및 임원에게 제공되는 화면으로 은행 전체의 현재 위기등급 및 서비스 위기상황, 주요 서비스에 대한 실시간 이벤트 발생 추이와 유해 트래픽 발생 여부를 경영자가 신속하고 효과적으로 파악할 수 있도록 핵심정보 위주로 제공한다. 만약 은행에 위기가 발생할 경우에는 위기상황 현황정보에 해당 내용이 표시되고, 위기대응 상황판으로 이동하여 보다 상세한 정보를 알 수 있다.

2.5.1.2 개별 모니터링 항목 관리

개별 모니터링 항목 관리 기능은 ESM, TMS 시스템의 개별 모니터링 항목 및 경보를 수집하는 기능으로



〔그림 10〕 이상징후 발생시 상세 모니터링 화면

Aegis 시스템 내부에서 작동한다. 이 기능을 이용하여 Aegis 시스템에서는 ESM, TMS의 침해, 장애, 공격 이벤트, 유해/정상 트래픽 초과 경보를 수집, 처리 할 수 있게 된다. 개별적으로 수집, 처리되던 경보들을 Aegis 시스템에서 통합하여 더욱 효율적인 침해사고 이상 징후 탐지 및 대응이 가능하게 된다.

2.5.1.3 통합 모니터링 항목 관리

통합 모니터링 항목 관리 기능은 ESM, TMS 의 경보들을 수집하여 개별 보안 시스템의 이상 징후들의 연관 분석을 실시하여 경보를 발생 시키는 기능으로 개별 모니터 항목 관리 기능과 마찬가지로 시스템 내부적으로 수행되는 기능이다. TMS 및 ESM에서 각각 발생 하는 경보를 조합하여 분석함으로 더욱 복합적인 상황에서 침해사고 징후에 대한 모니터링이 가능하게 해준다.

2.5.1.4 경보 심각도 관리

경보 심각도 관리 기능은 침입 시도 탐지에 따른 경보 발령 시 해당 서비스 구간의 중요도와 보안시스템에 대한 영향도에 따른 심각도를 먼저 산출하여 위험 기반의 탐지 및 대응이 가능하게 한다.

2.5.2 침해사고 위기 대응

침해사고 위기 대응 기능은 위기 자동탐지, 위기 대

응 프로세스 전산화, 위기 대응 상황판, 위기 상황과 수행 Task 매핑 등으로 분류할 수 있다.

2.5.2.1 위기 자동 탐지

위기 자동 탐지 기능은 시스템에서 내부적으로 위기 상황과 모니터링 항목을 매핑시켜, 모니터링 된 내용이 사전 정의된 조건을 충족하면 자동으로 위험 경보가 발생토록 한다.

2.5.2.2 위기 대응 프로세스 전산화

위기 대응 프로세스 전산화는 오프라인에서 수행되던 위기 대응 프로세스를 전산화 한 것이다. 위기발견 > 위기대응 > 사후관리에 이르는 일련의 절차를 시스템에서 직접 등록하고, 대응 이력을 조회할 수 있다. 이를 통해 모든 위기대응 이력은 데이터베이스로 구축되어 사후검토 및 개선점 도출 시에 유용하게 사용 가능하다.

2.5.2.3 위기대응 상황판

위기대응 상황판 기능은 위기대응 처리 내용을 실시간으로 상황판을 통해 조회하는 것이다. 이 기능을 활용하여 위기대응 상황 전파 및 대응내역을 공유 할 수 있다. 위기대응 담당자가 입력한 처리 내용은 위기대응 상황판에 바로 업데이트 되고 위기대응 담당자들은 위기대응 상황을 위기대응 상황판을 이용해 실시간 공유 가능하게 된다.

2.5.2.4 위기 상황과 수행 태스크(Task) 매핑

금번 프로젝트에서 새로 정의한 위기 상황 50여종을 위기 상황별 수행 태스크(Task)와 매핑하는 기능이다. 이 기능을 이용하여 위기 발생 시 미리 정의된 수행 절차에 따라 위기 대응을 하게 된다. 새로운 위기상황 발견 시 위기상황을 새로이 등록하거나 수행 태스크 및 위기대응 담당자의 역할이 변경 될 경우, 위기상황의 세부 설정 조정을 지원하여 위기대응 절차를 지속적이고 유연하게 운영토록 지원한다.

2.5.3 정보시스템 상시 취약점 점검

정보시스템 상시 취약점 점검 기능은 정보자산 관리 기능, 상시 자동 취약점 점검 기능, 위험 관리 기능 등으로 구성된다.

위험지수 = 발견위험도 / 전체위험도 X 100

※발견위험도 = Σ 발견된 취약점 X 취약점의 위험도
전체위험도 = Σ 전체 취약점 X 취약점의 위험도

〔그림 11〕 위험지수 산출식

2.5.3.1 정보자산 관리

정보자산 관리 기능은 서버, 응용프로그램, 네트웍, 보안시스템 등의 정보시스템에 대한 구성 정보를 관리하는 기능으로 자산의 등록, 수정, 폐기 등을 수행 할 수 있다.

2.5.3.2 상시 자동 취약점 점검

상시 자동 취약점 점검 기능은 정보시스템의 취약점 점검을 사전 정의된 스케줄에 의해 자동으로 실행되게 하는 기능으로 시스템 취약점 점검툴과 연동되어 작동한다. 시스템 취약점 점검툴의 점검 결과는 데이터베이스에 축적되어 취약점 발견 내역, 조치 내역 등을 지속적으로 관리할 수 있게 해 준다.

2.5.3.3 위험관리 기능

위험관리 기능은 시스템에서 발견된 취약점을 기반으로 산출된 위험지수를 활용하여 정보 시스템의 위험 수준 현황을 관리하는 기능으로서, 위험 기반의 취약점 대응 업무를 지원한다.

위험지수는 각 정보시스템에서 발견된 실제 위험도의 합계를 최대 가능 위험도로 나눈 백분율로 계산하며, 이 때 발견된 실제 위험도는 시스템별 취약점과 해당 취약점의 위험도를 가중하여 합산한다.

2.6 운영 프로세스

Aegis 시스템의 효율적인 운영을 위하여, 기존의 침해사고 조기 경보 및 대응 프로세스와 정보시스템의 취약점 점검 프로세스를 개선하였다.

2.6.1 침해사고 조기 경보 및 대응

침해사고 조기 경보 및 대응 프로세스는 모니터링, 탐지 및 전파, 위기대응, 피드백 등의 네 가지 단계로 구성된다.

〔그림 12〕 위기 대응 프로세스 및 분야별 역할

2.6.1.1 모니터링

모니터링 단계에서는 보안 이벤트 및 트래픽 추이를 실시간으로 모니터링하는 업무를 수행한다. 보안팀, IT 상황반/IT기획, 시스템/통신/개발 팀에서는 Aegis 시스템을 이용하여 주요 보안 이벤트 및 트래픽 추이를 모니터링 한다.

2.6.1.2 탐지 및 전파

탐지 및 전파 단계에서는 해킹, 디도스, 비정상 트래픽 추이 증가 등을 탐지하고 SMS, 유선 메일 등으로 상황을 전파하는 활동을 수행한다. 탐지 업무는 시스템에서 자동 수행되며, Aegis시스템을 통하여 Aegis시스템 및 ESM, TMS에서 발생되는 경보를 통합하여 탐지한다.

먼저 ESM 에서는 발생되는 자원, 장애, 이벤트 경보를 Aegis 시스템으로 자동 송신 하는데, 기존 ESM의 개별 모니터 항목 중에는 모니터 항목으로서 유용성이 부족한 항목들이 있어 본 프로젝트를 진행하며 ESM 개별 모니터 항목을 최적화 하였다.

TMS에서는 트래픽, 이벤트 경보를 Aegis 시스템으로 자동 송신 한다. TMS 개별 모니터 항목에는 이벤트 및 트래픽 임계치 초과 항목만 있었는데 디도스에 대한 모니터링을 강화 하기 위해 본 프로젝트를 통해 디도스 항목을 추가 하였다.

Aegis 시스템에서는 ESM과 TMS에서 발생된 경보를 상관분석하여 경보를 발생 시키므로 개별 보안 시스템에서는 탐지 할 수 없는 종합적인 상황에서 발생하는 경보를 탐지하게 되어 모니터링의 범위를 확대하게 되었다.

탐지 된 경보는 정보보안팀에서 분석하여 위기 상황 발생 여부를 판단 하게 되는데 위기 상황으로 판단되면 위기를 발령하게 되고 위기 상황이 아니면 자체 처리를 하게 된다. 자체 처리 경보도 심각도에 따라 내부적으로 정의한 긴급, 주의, 보통의 세 가지 등급에 따라 처리된다. 경보 심각도는 서비스 구간의 중요도(상,중,하), ESM 에이전트 영향도, TMS 객체/그룹/센서의 영향도(3,2,1,), ESM/TMS 개별 경보의 위험도(H,M,L) 등을 가중하여 산출하며 1~27점 사이의 값을 갖는다.

2.6.1.3 위기 대응

위기 대응 단계는 침해사고 내용 및 대응 방안을 분석하여 피해 및 영향도를 정의하고 상황 별 수행 업무에 따라 위기 대응을 업무를 실행하게 한다. 이를 위해 신규 정의한 50여 종의 위기상황에 따라 위기를 분류하여 처리하며 위기상황 별로 역할과 책임(R&R) 및 수행 업무가 매핑되어 있어 각 파트별 담당자들은 미리 정의된 자신의 임무에 따라 위기 대응을 하게 된다.

각 파트별 담당자들은 위기대응 상황판을 통해 위기 등급(Red-2, Red-1, Orange-2, Orange-1, Yellow-1, Blue-2, Blue-1, Green, 미확정)의 변화 추이를 모니터링 할 수 있고 위기등급이 Green으로 설정되면 위기 대응이 종료 된다.

2.6.1.4 피드백

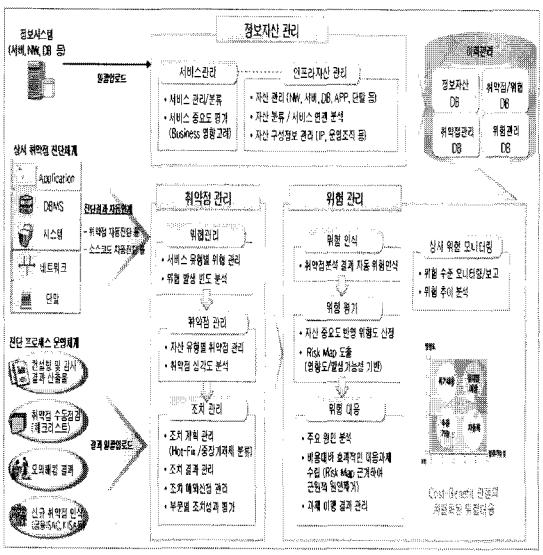
피드백 단계는 위기대응에 대한 최종 단계로서 대응 이력을 검토하는 업무를 수행한다. 상황 종료 공지를 하고 완료 보고 및 내용에 대한 검토를 실시한다. 위기가 재발 하지 않도록 위기대응 내역에 대한 적정성 및 효율성 등을 판단하고 평가한다.

2.6.2 정보시스템 상시 취약점 점검

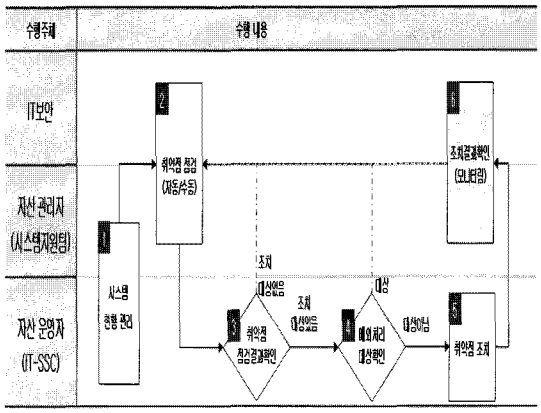
정보시스템에 대한 취약점 점검 프로세스는 상시화

등급	등급코드	시나리오	판단근거
Grey	미확정	위기등급을 확정하기 어려울 경우 선택	위기등급을 확정하기 어려울 경우 선택
Green	G1	사이버 테러등 징후가 없고, 인터넷이 정상적으로 운영	사이버테러 징후가 없는 정상적인 상황(보안)
Blue-1	B1	국내외 기관등에서 사이버테러징후가 있다는 보고	금융위, 금감원, 금융ISAC, KISA 등 정보보호 관련 기관에서 사이버테러 징후에 대한 정보 수신시(보안)
Blue-2	B2	타기관에서 사이버 테러가 발생하나, 당행 공격 없음	금융위, 금감원, 금융ISAC, KISA 등으로부터 특정기관에 사이버테러가 발생했다는 정보 수신시(보안)
Orange-1	Y1	DDoS차단시스템을 통하여 효과적으로 방어가 되는 경우	-Ddos 공격이 탐지 및 차단확인(보안) -콜센터 인터넷 지연 문의업무(상황반)
Orange-2	O1	행내 DDoS차단시스템을 통하여 차단하였으나, 인터넷뱅킹 지연이 발생하는 경우 - 일부 공격PC가 내부시스템으로 접속 - L4 스위치/웹서버 동시접속제수 초과 - reset - DDoS장비 용량에 근접하여 거래지연	콜센터 인터넷 지연 문의로 콜대기 건수 10건 이상이 5분 이상 지속(상황반) 통신장비/보안장비의 접속건수가 평시대비 2배 이상(통신/보안)
Orange-3	O2	-행내 DDoS차단시스템을 통하여 차단하였으나, 일부 고객이 접속이 불가능한 경우 -DDoS 차단시스템에서 일부만 대응이 가능한 경우	-콜센터 인터넷 접속장애 문의로 콜대기 건수 10건 이상이 5분이상 지속(상황반) -홈페이지 일부고객 접속 불가(개발파트) -접속불가 IP의 차단 목록 확인(보안)
Red-1	R1	-행내 DDoS 차단시스템을 통하여 차단하였으나, 외부 유입트래픽이 시스템 용량을 초과하는 경우 (1) 외부 유입 트래픽이 DDos	-콜센터 인터넷 접속장애 문의로 콜대기 건수 30건 이상이 20분이상 지속, (IT 상황반) -인터넷 회선 사용률 90 % 초과, (통신) -Ddos장비 임계치 90% 초과, (보안)
Red-2	R2	-인터넷뱅킹 서비스가 전면 마비되는 경우 -행내 DDoS차단시스템 및 외부DDoS차단 시스템을 통하여 공격차단이 불가능한 경우 (1) Domain을 이용하여 공격하는 경우 (2) IP Address를 이용하여 공격하는 경우	-콜센터 인터넷 접속장애 문의로 콜대기 건수 30건 이상이 20분이상 지속, (IT 상황반) -DDos 공격 보안시스템에서 차단 불가, (보안) -통신/보안 장비 임계치 초과, (통신/보안) -웹서버 세션 임계치 초과, (시스템)

〔그림 13〕 위기 상황 시나리오별 위기등급 및 판단기준 수립 예



〔그림 14〕 정보시스템 상시 취약점 관리 체계



〔그림 15〕 정보시스템 상시 취약점 관리 시스템 운영 프로세스

된 자동 점검 방식이 추가되었다. 기존의 매년 또는 분기에 한 번씩 수작업으로 수행하던 취약점 점검 업무를 일, 주 단위로 자동으로 수행토록 취약점 점검 및 대응 프로세스를 강화하였다.

강화된 취약점 점검 프로세스는 각 시스템에 설치된 취약점 점검 Agent로부터 주기적으로 수집된 취약점 점검 결과를 데이터베이스에 구축하고, 시스템 운영자들이 취약점 조회 화면을 통해 확인 및 조치토록 하고 조치 결과가 자동으로 재점검되도록 취약점 점검 Agent가 재 동작하는 방식이다.

정보시스템 상시 취약점 점검 프로세스는 시스템 현황관리, 취약점점검, 취약점점검결과 확인, 예외처리 대상확인, 취약점 조치, 조치결과 확인 등 전체 6개 단계로 구성된다.

2.6.2.1 시스템 현황 관리

시스템 현황 관리 단계에서는 신규 시스템을 등록, 변경하고 관리하는 업무를 수행한다. 자산 운영자는 신규 시스템이 도입되거나 기존 운영 시스템의의 주요 정보가 변경될 경우 Aegis 시스템에 등록하여 정보시스템 데이터베이스를 구축한다.

2.6.2.2 취약점 점검

취약점 점검 단계에서는 자동 또는 수동 취약점 점검을 수행하고, 점검 이력을 관리한다. 수동 취약점 점검 업무는 모의해킹 등을 통해 수작업으로 수행되며, 자동 취약점 점검 업무는 자동화된 시스템 취약점 점검툴을 이용한다. 자동 또는 수동 취약점 점검이 끝난 후 취약점이 발견되면 전자메일 시스템을 통하여 해당 정보시

〔표 3〕 정보시스템 상시 취약점 관리 절차

번호	업무명	세부 내용	수행주체	비고
1	시스템 현황관리	신규 시스템 등록, 변경 관리 등	시스템 지원팀 (IT-SSC)	
2	취약점 점검	취약점 점검 실시(자동, 수동) 취약점 점검/조치 결과 모니터링, 이력 관리 등	IT보안 (시스템 지원팀)	자동화된 상시 취약점 점검 실시 수동 점검(모의 해킹) 실시
3	취약점 점검결과 확인	발견된 취약점들을 확인하고, 세부 내용 및 조치 방법 확인	IT-SSC	
4	예외처리 대상확인	점검 결과 중 조치가 불필요한 예외 처리 대상 제외	IT-SSC (시스템지원팀)	예외 처리는 전자 결재 연동
5	취약점 조치	취약점별 조치 계획 수립 및 취약점 제거 활동 수행	IT-SSC	상시 취약점 점검 시스템에서 제공하는 조치방법 활용
6	조치 결과 확인	수동 또는 자동(재점검 실시)으로 취약점 조치 결과 확인	IT보안 (시스템 지원팀)	

스템의 담당자에게 자동으로 취약점 점검 결과 확인 요청 메일이 발송된다. 모든 취약점 점검 결과는 취약점 관리 DB에 저장되어 이력으로 관리되며 Aegis 시스템을 이용하여 취약점 점검 현황을 지속적으로 모니터링 하게 된다.

2.6.2.3 취약점 점검 결과 확인

취약점 점검 결과 확인 단계에서는 발견된 취약점들을 확인하고, 세부 내용 및 조치 방법을 확인하는 업무를 수행한다. 자산 운영자는 발견된 취약점에 대해 확인을 하고 조치 대상으로 판단 될 경우 세부 취약점 내용 및 조치 방법을 확인한다.

2.6.2.4 예외처리 대상확인

예외처리 대상확인 단계에서는 점검 결과 중 조치가 불필요한 예외 처리 대상을 제외하는 업무를 수행한다. 자산 운영자는 조치대상 취약점의 내용을 확인하여 실효성이 없거나 해당 취약점에 대한 다른 보완 수단이 있는 경우에는 내부 결재를 통해 예외 처리를 신청하게 된다. 예외처리가 승인되면 해당 취약점은 조치 대상에서 제외 된다.

2.6.2.5 취약점 조치

취약점 조치 단계에서는 취약점 별 조치 계획을 수립하고 취약점을 제거하는 업무를 수행한다. 자산운영자는 취약점에 대한 조치 계획을 세우고 취약점에 대한 조치를 수행하고 조치결과를 승인 받는다.

2.6.2.6 조치 결과 확인

조치결과확인 단계에서는 수동 또는 자동으로 취약점 조치 결과를 확인 하는 업무를 수행한다. IT 보안 관리자는 조치결과에 대해 직접 확인을 하거나, 자동 취약점 점검 스캐너를 이용하여 재점검을 실시하여 자동으로 취약점 점검 결과를 확인한다.

Ⅲ. 시스템 특징 및 구축 효과

3.1 시스템 주요 특징

Aegis 시스템 및 관련 운영프로세스의 주요 특징은 다음과 같다.

첫째, 시스템 취약점의 상시 점검과 체계적인 대응이 가능하다. 기존 독립 운영되던 시스템 취약점 점검툴을 Aegis 시스템에 연동시키고 스케줄링을 설정하여 취약점 상시 점검이 가능하게 되었으며, 취약점 점검 결과를 데이터베이스화하고 사내 전자결재 시스템과 연동시켜 체계적인 취약점 조치 결과 관리가 가능해졌다. 특히, 각 정보시스템별로 탐지된 취약점 별 위험수준, 발생 빈도를 측정하여 지표화 함으로써 취약점 발생의 근원을 찾아 제거하고, 기 발생된 취약점의 대응 우선순위를 감안한 조치 계획을 수립 할 수 있게 하였다.

둘째, 정보보안 침해사고 대응 체계가 업무 서비스 및 정보시스템의 위험관리에 기반하여 자동화 구축되었다. 정보보안시스템에서 발생한 모든 이벤트의 업무시스템에 대한 영향도가 사전 정의된 위험 평가 모델에 따라 자동 분석 되도록 하였으며, 각 위험 수준에 따라 최적화된 대응이 될 수 있는 기반이 마련되었다.

셋째, 그 동안 종이 문서로만 존재하여 실제 침해 사

고 발생 시 적용이 쉽지 않았던 침해사고 대응 절차가 전산화되었다. 디도스 공격, 시스템 비인가 접속(해킹 시도), 시스템 장애 등의 각종 이벤트들을 관련 업무 서비스의 중요도와 침해사고 영향도에 따른 다단계의 심각도로 구분하여 각 이벤트별로 탐지 즉시 긴급 대응 필요성 여부가 쉽게 인지될 수 있게 하였다. 특히, 침해사고 발생 시 각 분야별 담당자가 조치할 사항을 쉽게 확인하고 대응 할 수 있도록 50여 가지의 침해사고 유형별 대응 프로세스를 자체 개발하고 매트릭스 형태로 정의하여 그 활용도를 높였다.

넷째, 침해사고 발생 시 각 업무 분야별 담당자 간 공동 모니터링과 공동 대응이 가능해졌다. 경영진 및 정보보안 담당자, 서버/통신 관리자, 개발 담당자 등에게 각각 최적화된 침해사고 모니터링 화면을 제공하고, 모든 침해사고 대응 사항을 침해사고 대응 시스템에 등록하도록 하여, 관련팀 전체가 실시간으로 침해사고 대응 현황을 공유하고, 침해 공격 및 대응의 상황 변화에도 신속히 대응 할 수 있게 되었다.

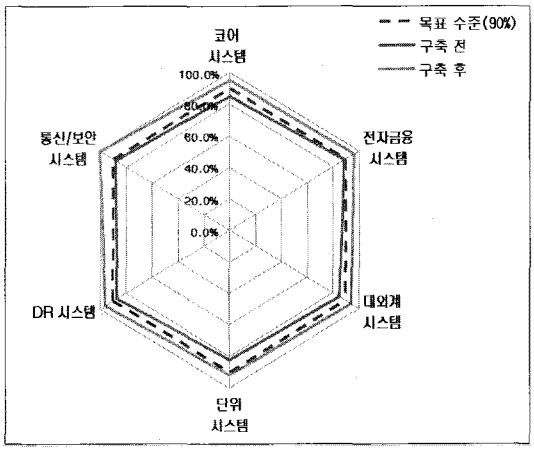
3.2 구축 효과 분석

`10년 1월부터 약 6개월간의 프로젝트 수행을 통해 '정보시스템 상시 취약점 점검 체계', '침해사고 조기 경보 시스템', '침해사고 대응 프로세스 전산화'등을 하나의 단일화된 Aegis 시스템으로 구축 완료하였으며, `10년 6월부터 7월말까지 2개월 동안의 운영을 통한 성과 분석 결과는 다음과 같다.

3.2.1 침해사고 사전 예방 강화

서버 시스템 및 사내에서 자체 개발한 응용프로그램 등에 대하여 매주 또는 매월 단위로 자동화된 보안 취약점 진단을 실시하여 관련팀 간 취약점 정보를 공유하고, 이를 기반으로 한 위험 평가와 체계적이고 신속한 취약점 제거 등 조치 대응이 가능해졌다. 이를 통해 정보시스템의 안전도 수준이 지속적으로 상향 안정화되고 있어, 정보시스템의 취약점을 이용한 해킹, 바이러스 등의 침해사고나 장애 유발이 사전에 예방 되는 효과가 클 것으로 예상된다.

Aegis 시스템의 구축 전/후, 자체적으로 실시한 정보시스템의 보안 안전도 수준 평가 결과, 구축 전 85.9%



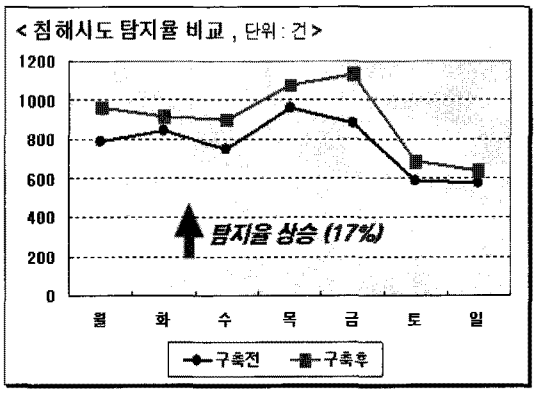
〔그림 16〕 Aegis 구축 전/후 정보시스템 보안 수준 비교

에서 95.5%로 평균 9.6%의 보안 수준이 향상되었으며, 전 부문에서 자체 목표 수준인 90% 가 넘는 보안 수준을 지속적으로 유지할 수 있었다.

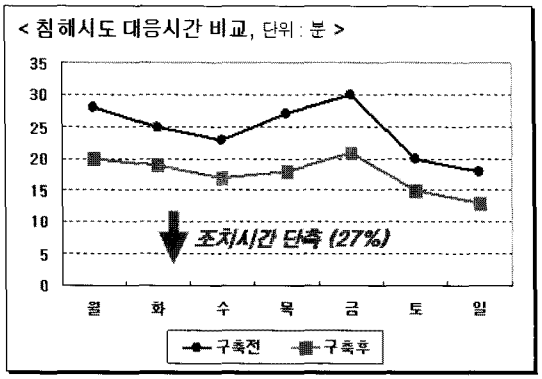
3.2.2 침해시도 탐지 강화

기존 보안관제시스템(ESM)과 새로 구축한 위험관리 시스템(TMS)의 트래픽 분석 데이터를 통합 모니터링하고 연관 분석을 통하여 그 동안 탐지하지 못하였거나 조기 탐지가 불가능했던 미세한 침해시도도 신속히 탐지가 가능해졌다.

Aegis 시스템의 구축 전/후 각 2개월간, 일별 전체 침해시도 탐지 건수에 대한 분석 결과, 전체적으로 약 17%의 추가적인 침해시도 탐지가 가능했음을 확인할 수 있었다. (분석 기간: `10년 4월 1일 ~`10년 7월 31)



〔그림 17〕 Aegis 구축 전/후 침해시도 탐지율 비교



〔그림 18〕 Aegis 구축 전/후 침해시도 대응시간 비교

3.2.3 침해시도 분석 및 대응 시간 단축

전체 보안 이벤트에 대해 업무 서비스 구간별 중요도와 침해사고 영향도가 지표화되어 정보보안 관제 담당자는 이상 징후 발생 즉시 위험 수준을 인지하여 불필요한 이벤트에 대한 대응을 최소화 할 수 있게 되었다. 또한, 침해사고 유형별 대응 프로세스를 사전에 정의하여 침해사고 발생 시 각 분야별 업무 담당자가 조치할 사항을 쉽게 확인하고 대응 할 수 있게 되었다.

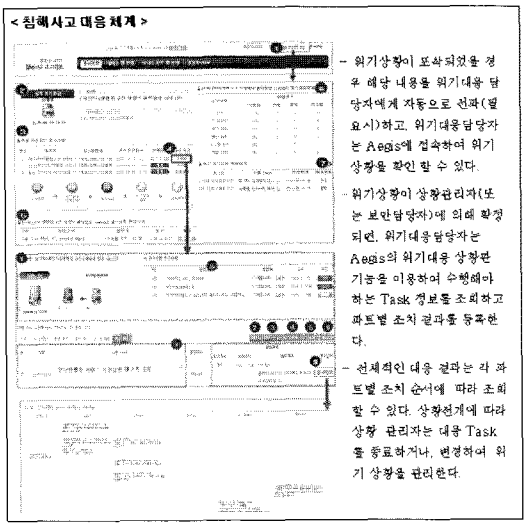
Aegis 시스템의 구축 전/후 각 2개월간, 보안 담당자의 직접 대응이 필요했던 주요 이벤트에 대해 최초 해당 이벤트의 발생에서부터 이벤트 내용 분석 및 필요 사항 조치, 조치 내용 등록 등 각 단계별 소요 시간 분석 결과, 약 27%의 총소요 시간 단축 효과가 발생한 것으로 분석되었다. (분석 기간: `10년 4월 1일 ~`10년 7월 31)

3.2.4 침해사고 대응 체계 개선

침해사고 대응에 유관 부서 간 협업이 필요하거나 장시간이 소요되는 경우, 전체 상황관리자 또는 보안담당자는 몇 번의 화면 조작으로 발생한 침해사고에 대해 관련팀별 조치사항을 전파 할 수 있게 되었다.

정보보안, 서버/통신 시스템 담당자, 응용 프로그램 개발자 등 각 분야별 업무 담당자는 침해사고 대응 조치 결과를 모두 침해사고 대응 시스템에 등록하고, 상황관리자는 이를 통하여 전체적인 대응 상황을 파악하여 상황을 종료하거나 추가적인 대응이 필요한 경우 변경된 조치사항을 다시 전파할 수 있게 되었다. 이러한 일련의 대응 내용은 시스템에 기록되어 대응 이력 조회 또는 사후관리에 사용된다. 즉, 침해사고 대응 프로세스와 매뉴얼을 세부적으로 수립하고, 전산화 함으로써 침해사고 발생 시 즉각적인 대응이 가능하게 되었다.

Aegis 시스템에서 침해사고 발생 시 주요 업무 처리 흐름은 다음과 같다.



〔그림 19〕 침해시도 대응 시스템 업무 흐름도

Ⅳ. 개선할 사항 및 향후 발전 방향

4.1 미진사항 및 개선 사항 검토

금번 프로젝트의 구축 효과를 측정해 본 결과, 침해사고에 대한 관련 부서 간 공동 참여 기반 마련과 정보시스템 전반에 대한 안전도의 개선이라는 명확한 효과도 있었지만, 몇 가지 시스템 운영상의 부족한 부분도 함께 확인되었다.

4.1.1 외부 보안 이슈 대응 체계화

금융보안연구원 및 한국인터넷진흥원(KISA), 국가사이버안전센터(NCSC) 등 외부 보안전문 기관으로부터 접수되는 최신 보안이슈나 침해사고 정보가 조직 내 정보시스템에 끼치는 영향도를 즉시 확인 할 수 있는 대응 체계 구축을 미리 준비하지 못하였다.

대내외에서 발생하는 최신 보안이슈에 대한 대응 수

준은 내부 시스템 관리자의 역량에 따라 크게 달라 질 수 있다. 따라서 최신 보안 이슈에 대해 일관되고 효과적인 대응 수준을 유지하기 위해서는 이에 대한 대응 체계가 프로세스화되어 관련 보안 이슈가 해당 정보시스템에서 반드시 대응되도록 해주어야 한다. 이 부분은 향후 개선 과제로서 효과적인 구현 방안에 대해 앞으로 더 많은 검토가 필요한 것으로 판단된다.

4.1.2 IT 인프라 시스템 연동 강화

침해사고의 효과적인 예방과 침해사고 발생 시 신속한 대응을 위해서는 조직 내 부서간의 유기적인 협력과 더불어 각종 IT 인프라 시스템들 또한 상호 유기적으로 연동되어야 한다는 것이 재확인되었다.

사내에는 일반 고객용 서비스를 제공하는 업무 시스템 외에도 그룹웨어시스템, 메신저시스템, 전산업무 관리시스템, 패치관리시스템, IP관리시스템 등 다양한 서비스를 지원하는 IT인프라들이 존재한다. 침해사고의 효과적인 대응을 위해서는 보안시스템의 확충을 통한 침해사고 차단 기능 강화도 중요하지만 이러한 IT 인프라가 함께 연동되지 않으면 정보보안 시스템의 활용도가 상당히 제한된다.

금번 프로젝트에서도 그룹웨어, 메신저, UMS(Unified Messaging System) 시스템 등의 연동 작업은 효과적으로 잘 진행된 것으로 평가되지만, 단말 패치관리시스템이나 IP관리시스템과의 연동은 해당 패키지의 수정이 제한 되어 처음 계획한 만큼 추진되지 못하여 사내 PC나 자동화기기 등 단말에서 발생한 이벤트에 대해서는 자동화된 사용 현황 확인이 어려운 한계가 발생하였다.

향후 내부 단말에 대한 패치 관리시스템과 IP관리시스템도 추가 연동하고 단말기 운영 현황과 패치 상태 등도 침해사고 통합 모니터링 및 위험 수준 평가 및 대응 절차에 함께 반영하는 모델의 정립이 필요한 것으로 판단된다.

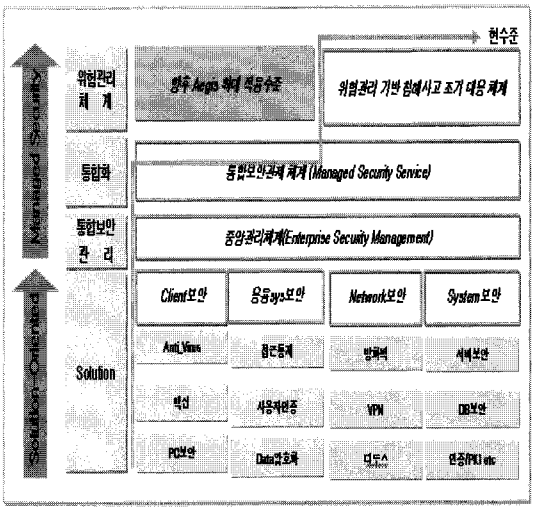
4.2 향후 발전 방향

금번 프로젝트의 추진 경과와 현재 정보보안시스템 전반의 수준 평가를 통해, Aegis의 향후 발전 방향을 검토해 본 결과는 다음과 같다.

4.2.1 Aegis 적용 범위 확대

유관 부서와의 협업 체계를 확대하고 Aegis의 적용 범위를 내부정보 유출방지 등 보안 체계 전 부문으로 확대 적용하여야 한다.

현재 보안관리체계 수준과Aegis 시스템의 확대 적용 시 보안 수준 정도의 개념도는 다음과 같다.



〔그림 20〕 Aegis 발전 방향

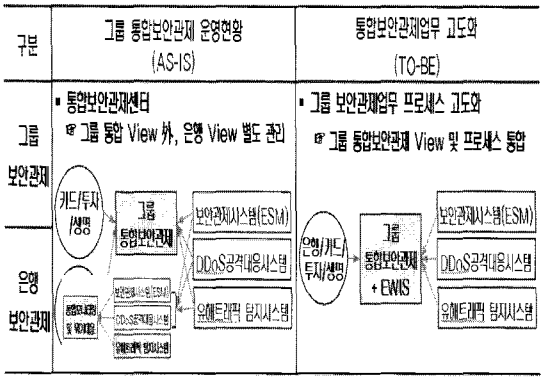
정보보안시스템을 구축할 때 최우선 추진 목표는 항상 침해사고 예방과 내부 정보 유출 방지인데, 현재 Aegis는 디도스 공격, 비인가 접속 시도 등 외부에서 인터넷을 통한 침해 접속 시도와 내부망 내 유해 트래픽에 대한 조기 대응 등 네트워과 시스템 부문의 침해사고 대응 강화를 주요 기능으로 구성되어 있다.

그러므로 단말 운영팀, 응용프로그램 개발팀과 협업을 통해 PC보안, 문서보안관리체계(DRM) 등 단말 환경과 응용 시스템 영역에 대한 보안 체계도 Aegis의 기존 통합 모니터링 및 위험 관리 모델에 추가하면 내부 정보 유출 방지를 위한 모니터링과 대응도 좀더 체계화가 가능한 것으로 예상 된다.

4.2.2 그룹사 통합보안관제시스템 고도화

Aegis 시스템을 그룹사 전체의 통합보안관제체계로 확대 적용하여야 한다.

신한금융 그룹은 내부적으로 지주사망으로 모두 연



〔그림 21〕 그룹사 통합보안관제시스템 고도화 방안

결되어 있으며, 그룹사의 공통 업무를 위해 통합 TFT를 수행하는 경우가 많으므로 일부 그룹사라도 보안 수준이 낮아 침해사고가 발생할 경우 전체 그룹사에 영향을 끼칠 수 있으므로 공동 대응이 필요하다.

신한금융그룹은 최근 기존 은행에서 운영하던 보안관제센터를 그룹 차원으로 확대 통합하여, 보안관제업무의 고도화 기반을 마련하였다. 여기에 신한은행에서 안정성과 효과성이 기검증된Aegis와 같은 위험관리 기반의 침해사고 대응 체계와 공동 대응 프로세스를 적용하여, 그룹사 전체적으로 고도화된 침해사고 대응 체계를 구축함으로서 각 그룹사의 보안 수준이 함께 상향 평준화가 가능할 것으로 예상된다.

4.3 결언

최근 몇 년 전부터 정보보호관리체계(ISMS)의 국제 표준인 ISO27001이나 국내 표준인KISA ISMS인증을 취득하는 기업이 급격히 늘어나고 있다. 이러한 ISMS 인증을 받기 위한 기본 요건에는 인증 범위에 해당하는 정보시스템에 대한 위험평가와 이를 기반으로 한 위험처리 계획 수립 및 조치 결과 관리가 포함되어 있다.

하지만, 금번 프로젝트 추진을 위해 국내 유명한 다수의 정보보호 전문업체로부터 추진 방안을 제안 받아 검토해본 결과, 다양한 침해시도 및 그 공격 목표가 되는 정보시스템에 대한 위험 수준의 평가 방법이 명확히 정립되어 있지 않거나 너무 이론에만 치우쳐 실제 구축 경험이 있는지 의심되는 경우도 있었다.

바꾸어 말하면, 이러한 정보보호 전문업체의 컨설팅을 통해 ISMS 인증을 받은 기업들은 정보시스템에 대한 위험 관리를 최초 인증 심사를 받을 때만 제대로 하고, 그 후에는 즉시에 수행을 못하거나 계속 수작업으로 관리할 수 밖에 없어 많은 어려움을 겪을 것으로 추정이 된다.

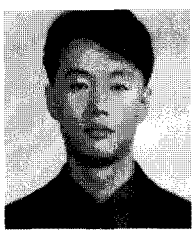
당행 또는 2003년도에 당시 BS7799 인증을 받을 때부터 정보시스템에 대한 자동화된 위험관리체계를 구축하기 위해 많은 노력과 시행착오를 겪어왔으며, 본 프로젝트를 실행할 때도 가장 중점을 둔 것은 업체의 보안 컨설턴트가 제시한 이론보다는 그 동안의 경험을 바탕으로 한 소속사의 정보시스템과 보안시스템의 운영 현실을 감안한 실제 구축 및 지속적으로 운영 가능성 이었다. 본 구축 사례가 부족하지만, 학계와 정보보호 전문업체가 더 많은 기업에서 좀더 실효성이 높은 정보보호관리체계 자동화 시스템 및 침해사고 대응 체계를 구축하기 위한 이론과 시스템을 만드는 데 도움이 되었으면 한다.

끝으로, 금번 프로젝트를 통해 당행은 침해사고의 예방, 탐지, 대응 체계를 전반적으로 강화 할 수 있게 되었다. 이러한 성과의 주요 요인은 사내 유관 부서 담당자가 모두 담당 시스템에 대한 정보보안 업무가 모두 자신의 책임이라는 주인정신과, 전체 업무 담당자와 정보보안 업체 간 상호 신뢰를 바탕으로 한 협업과 위험관리 관점의 침해사고 대응 체계 구축이라는 명확한 목표가 있었기 때문에 가능했던 것으로 판단된다. 비슷한 고민을 하고 있는 타금융회사나 민간 기업에서도 당사의 사례가 적절한 참고 사례가 되었으면 한다.

참고문헌

[1] 에이쓰리시큐리티(주), 위험관리 방법론(RCMM, Risk and Crisis Management Method)

〈著者紹介〉



김 진 섭 (Kim Jin Seob)

1989년 4월 : 조흥은행 입사
1996년 1월 ~ 1999년 5월 : 조흥은행 전산실 운영
2000년 2월 국민대학교 정보관리학과 졸업
1999년 5월 ~ 현재 : 신한은행 IT보안팀 차장
<관심분야> 정보보호, 정보시스템 감사