情 報 保 護 學 會 誌
第19卷 第3號, 2009. 6

내부정보 유출 징후 분석을 통한 유출방지체계 구축에 관한 연구

이 기 혁*, 이 철 규**

요 약

최근 연이은 정보유출사고로 인해 많은 기업들이 기업 이미지 손실과 같은 무형적 손실을 비롯해 금전적인 배상에 이르는 유형적 손실로 많은 어려움에 처해 있는 상황에서 이런 문제점을 대응하기 위해 기업들은 정보보호를 위한 적절한 주의 의무를 다하면서 체계적으로 보안정책을 기준으로 제한된 리소스를 효과적으로 운영해야 할 필요가 있다. 본 논문에서는 내부정보 유통이 많은 기업 보안환경을 중심으로 다양한 보안인프라를 효과적으로 연계하여 분석하는 검증된 보안정책을 수립하고 적용함으로써 법적 주의 의무를 다하면서도 효과적으로 보안관리업무를 수행할 수 있는 정보유출방지체계를 이행하기 위한 방안을 제시한다.

Ⅰ. 서 론

최근 중대형 기업들의 보안사고가 연이어지면서 사회적인 이슈가 되고 있다. 보안사고가 발생한 기업들은 집단 손해배상 손실, 기업 이미지 손실, 매출 손실, 주가 하락 손실, 기업 경쟁력 손실 등 5중고를 겪고 있으며, 나아가 지속 경영가능성(Sustainability)에 까지 영향을 미치고 있다.

이러한 보안사고로 인한 사회적, 경제적 나아가 국가적 손실을 막기 위해 정부는 각종 정보보호 법률 제·개정을 통해 대책을 강화하고 있다.

최근 제·개정이 추진되고 있는 국내·외 정보보호 규제들은 기업의 능동적이고 책임성 있는 투명한 정보보호 활동을 요구하고 있다.

이는 앞으로의 기업 정보보호는 단순 보안인프라를 마련하는 것이 다가 아니라 기업이 비즈니스를 위해 활용하고 있는 정보를 각종 규제에서 요구하는 합리적 보호수단을 마련하여 사회적, 윤리적 책임성을 가지고 활발하게 정보보호 활동을 수행하고 있음을 스스로 증명해야 되는 것을 말한다. 기업이 정보유출을 보호하기 위해 적절한 조치를 취하지 않거나 해당 직원들에게 그러한 행위가 옳지 않음을 경고하고 지속적으로 관리하지 않는다면 기업은 어떠한 법적 권리도 인정받을 수 없다. 또한 기밀정보를 회사 안과 밖의 경쟁자들로부터 보호하기 위하여 보호 의무(Due Diligence)를 다해야 한다.

이러한 정보유출 등의 보안사고로 유발될 수 있는 기업 비즈니스 위험요인에 대한 경영층들의 관심이 커지면서 기업 정보보호의 중요성이 크게 부각되고 있다. 하지만 지금까지 외부 보안위협을 차단하기 위해 집중된 단위 보안솔루션 기반의 정보보호 대응방법으로는 이러한 변화에 대응하기에 한계가 있다.

실제로 보안인식 부족, 투자비용 및 인력제약 등으로 일부 대기업들을 제외하고는 체계적인 내부정보보호를 할 수 있는 여건이 성숙되어 있지 않은 것이 현실이다. 지금껏 기업은 외부로부터의 보안침해 차단을 위해 방화벽이나 침입차단시스템 등을 도입하는 등 외부 보안위협에 대응하는데 집중했을 뿐 실제 보안사고의 80% 이상을 차지하고 있는 내부 위협은 관용적 태도로 대응하고 있었다.

그러나 최근 발생되는 대규모 정보유출의 원인이 내부의 위협으로부터 기인된다는 인식이 커지면서 이로 인한 피해방지를 위해 내부정보관련 보안솔루션 도입이

* 건국대학교 대학원 벤처전문기술학과
** 건국대학교 대학원 벤처전문기술학과

급격히 늘어나고 있다. 내부정보[1]가 포함된 문서 자체의 보안 강화를 위해 e-DRM을 도입해서 기업 내 생성되는 모든 문서들을 암호화하고 있고, 인터넷을 기반으로 한 업무가 늘어나면서 직원들이 E-mail, 메신저, 인터넷 게시판 등을 통해 내부정보를 외부로 유출할까 두려워 필터링 솔루션을 보강하고 있다. 뿐만 아니라 저장매체를 통한 정보유출이 걱정스러워 DCS(Device Control System)까지 도입해 매체를 통제하고 있다.

그렇다면 이제 정보유출 등 보안사고로부터 안전한가?

나날이 발전하고 있는 기술과 복잡·지능화되고 있는 보안위협을 차단하기 위해 새로운 보안솔루션을 계속 도입한다고 이러한 문제가 해결되는 것은 아니다.

보안 솔루션들이 늘어나고 정보유출에 대한 이슈가 늘어나면서 보안 조직의 역할도 방대해졌다. 오히려 늘어난 보안솔루션들을 운영·관리하기 위해 기업 보안조직의 역할과 보안활동이 의존·편향되고 있고, 보안솔루션들의 증가에 따른 관리 포인트 증대와 복잡성 등으로 기인한 관리 소홀이라는 위협이 또 다른 보안사고를 야기하고 있다.

이러한 이슈와 내부정보유출을 해결하기 위해 최근 다양한 보안 솔루션을 유기적으로 연계하여 관리·차단·통제할 수 있는 정보유출방지솔루션이나 통합보안관리솔루션들이 대두되고 있다. 이들 보안솔루션의 핵심은 분석 룰이며, 결국 얼마나 신뢰성 있는 정보유출탐지 정보를 제공해주고, 기업이 이를 바탕으로 보다 적극적이고 손쉽게 정보보호 활동을 지속·관리하며 강화해 나갈 수 있도록 해줄 수 있느냐에 달려 있다. 이는 바로 탐지·분석 정책의 신뢰성과 효과성이다. 이러한 탐지 정책의 신뢰성과 효과성이 보장되지 않는다면 이 역시 하나의 보안솔루션이 추가되는 것과 크게 다르지 않다.

결국 내부정보보안은 소프트웨어 및 하드웨어 기반의 단위 또는 통합보안솔루션만으로 해결되는 문제가 아니라 합리적 보안정책[Policy]하에, 기업의 최고 자산인 직원[People]이, 중요 정보를 어떻게 취급하고 있는지에 대한 업무내역[Process] 관리를 통해 내부직원의 정책위반과 기밀 유출 시도와 가능성 자체를 제거해야 가능하다.

이를 위해서 본 정책개발에서는 내부정보 유통이 많은 대표적인 통신사업자 보안환경을 중심으로 PPP [Policy, People, Process]를 기반으로 한 내부정보 유출방지 분석 방법론을 수립하고 이를 기반으로 탐지·분석 정책을 개발·적용·검증하여, 기존 내부정보 유출방지 제품군과 차별화된 보다 신뢰성 있고 효과적인 정보유출방지체계를 구축하고자 한다.

Ⅱ. 본 론

2.1 내부정보 유출분석 정책 개발

2.1.1 개발범위 정의

정책개발을 위해서는 기본적으로 사실(Fact)에 근거한 정보를 수집하고 분석해야 한다. 이것을 기반으로 각 정보들 간의 상관관계를 도출하여 신뢰성 있고 효율적인 내부정보 유출 예방/모니터링/탐지/증적추적 등의 보안 관리 활동을 수행할 수 있다.

따라서 신뢰성 있고 효율적인 내부정보 유출 분석을 위해 "회사 구성원들이 어떻게 내부정보 취급하고, 통제되고 있는지"에 대한 세부내역을 파악할 수 있는 분석 정보원의 선정 및 수집 로그정의가 필요하다.

이를 위해 현재 통신사업자에서 설치, 운영되고 있는 시스템들 중 고객정보를 포함한 내부정보 유출분석을 위해 필요한 보안솔루션이 어떤 것들이 있고, 해당 보안솔루션들의 운영은 목적과 주요 보안관리 로그 정보가 무엇인지를 검토하여야 하며 그 결과 [표 1]과 같이 파악되었다.

위 대상 시스템들 중 보안통제 기능이 중복되어 있거나, 연계를 위해 선결되어야 할 기능개선 및 환경적 제약요건 등이 있는 시스템들이 존재하여 본 정책개발에서는 16개 시스템을 연동대상으로 선정하였으며, 선정된 연동대상은 다음과 같다.

NAC[2], AV[3], EDTS[4], e-MMS[5], MMS[6], WMS[7], CDTS[8], BRE[9], e-DRM[10], DCS[11], VPN[12], SPM

1) 조직에서 사용되고 있는 기밀정보, 핵심기술, 개인정보 등과 같이 가장 중요한 무형의 자산을 총칭.

2) 사용자 인증, 내부 보안정책준수 여부를 검사하여 네트워크 접속을 통제하는 기술.

3) 바이러스 및 악성코드로부터 탐지 및 보호기능을 지닌 보안솔루션.

4) 암호화된 문서를 업무상 암호 해제하여 외부자에게 매일 발송하는 시스템.

5) 메일 송수신 정보, 필터링 및 이력관리를 위한 시스템.

6) 메신저 모니터링 및 첨부파일 전송 관리 시스템.

7) 웹사이트 접근 내역 및 차단 정보 모니터링 시스템.

S[13], HRDB[14], ERP/전자결재[15], CILA[16]

〔표 1〕 연동대상 시스템 목적 및 주요 수집 정보

No	시스템	목적	주요 보안관리 로그 정보
1	Network Access Control (이하 NAC)	N/W 접근 통제	• 무결성 점검 관련 정보 • IP 인증 정보
2	Anti Virus (이하 AV)	웜바이러스 예방	• 정보유출 관련 웜바이러스 탐지 및 치료와 관련된 정보
3	Encrypted Documents Transfer System (이하 EDTS)	암호화된 문서를 업무상 암호 해제하여 외부자에게 메일 발송	• 정보 전송 정보 • 전송 시 첨부된 파일 정보
4	e-Mail Monitoring System (이하 e-MMS)	메일 송수신 필터링 및 이력관리	• 정보 전송 정보 • 전송 시 첨부된 파일 정보
5	Messenger Monitoring System (이하 MMS)	메신저 보안	• 대화로그 정보 • 전송 시 첨부된 파일 정보
6	Web Monitoring System (이하 WMS)	웹사이트 접근통제	• 웹사이트 차단목록 정보 • 불법 웹사이트 접근 이력 정보
7	Customer Data Transfer System (이하 CDTS)	고객정보 전송관리 시스템	• 고객정보 업/다운로드/파기/전송 이력 및 승인 정보
8	Business Rule Engine (이하 BRE)	영업전산망 모니터링	• Rule 기반 비정상 영업/고객정보 접근 모니터링 정보
9	Enterprise-Digital Right Management System (이하 e-DRM)	파일 암호화 및 보안 강화	• 암호화 파일 생성/삭제/수정 등 취급내역 정보 • e-DRM 로그인 정보
10	Device Control System (이하 DCS)	매체통제	• 저장매체 사용이력 정보(이동, 복사, 매체 탈부착과 관련된 이력 정보)
11	Virtual Private Network (이하 VPN)	원격 접근 통제	• VPN 접근 이력 정보 • VPN을 활용한 정보 전송 정보
12	Security Policy Management System (이하 SPMS)	정책 변경 요청 및 승인 관리	• 매체활용, 각종 보안 인프라 권한 부여 요청/승인/폐기 정보
13	Human Resource DataBase (이하 HRDB)	인력관리	• 내부 HRDB/조직 정보
14	전자결재/ERP	사내전자 결재시스템	• 퇴직자 정보 • 휴직자 정보
15	Customer Data Leakage Audity system (이하 CILA) (검토요망)	네트워크 보안	• IP변경차단 정책 위반 정보 • 비정상 웹사이트 접근 정보 • 대리점 매체사용 이력 정보
16	Privacy Impact Analysis System (이하 PIAS)	개인정보 영향평가	• 개인정보취급시스템 보유정보 및 현황 정보 • 개인정보취급시스템 개인정보보호 수준 관리 정보
17	Digital Forensics System (이하 DFS)	개인정보 유출감사	• 개인정보취급자 PC Forensic 결과정보
18	Patch Management System (이하 PMS)	패치관리	• 패치자동업데이트 수행 결과 정보
19	출입통제시스템	물리적 출입통제	• 출입 인증 및 사용 이력 정보
20	복사기	문서 복사	• 복사 이력 및 이미지 정보
21	프린터	문서출력	• 출력이력 및 이미지 정보
22	FAX	문서 전송	• 전송 이력 및 이미지 정보

선정 · 정의된 연동대상 및 수집 정보를 바탕으로 법적 보호의무에 충실하면서도 효율적인 Resource 활용을 통한 내부정보 보호를 위해 보안 정책 위반자 적발 · 관리, 내부정보 유출징후 사전 탐지 · 대응, 정보유출행위 추적 · 조치가 가능한 관점에서 내부정보 유출분석 정책을 수립하는 것을 개발 범위로 한다.

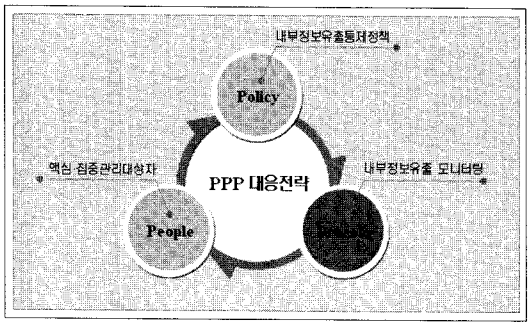
8) 고객정보 전송관리 시스템.
9) 고객정보 조회 및 유통되는 영업전산망의 Rule 기반 접근 모니터링 시스템.
10) 암호화 파일 생성/삭제/수정.
11) 저장매체의 사용이력과 탈착여부를 감시하는 시스템.
12) 가상 사설망으로써 사용자가 기업내부의 네트워크를 사용할 수 시스템.
13) 매체활용, 각종 보안 인프라 권한 부여 요청/승인/폐기 정보 관리.
14) 인력관리를 위한 내부 조직정보 시스템.
15) 사내 인사, 재무, 경영 정보의 효율성을 위해 구축된 전자결재 시스템.
16) 시스템내 IP변경 차단, 비정산 웹사이트 접근 정보, 매체사용과 같은 네트워크 보안 프로그램.

2.1.2 정책 개발 방법론

최근 발생되고 있는 정보유출은 외부로부터의 악의적인 공격이라기보다 전·현직 내부직원의 고의적이거나 부주의한 행동과 내부정보 취급 프로세스 위반으로 인해 발생한다.

외부공격으로부터 내부정보를 보호하기 위해 각종 시스템을 도입하고, 단위 솔루션을 기반으로 이에 대응하는 것에 중점을 두는 기존 보안책만으로는 정보유출의 문제를 해결할 수 없다.

이런 이유로 보다 근본적인 문제 해결을 위해 기업은 PPP[Policy, People, Process] 관점의 대응전략 변화가 필요하다.



〔그림 1〕 PPP[Policy, People, Process] 대응전략

■ Policy

해당 기업의 비즈니스 환경에 따라 국·내외 Compliance 준거 요건들을 기반으로 구성된 기업 내부정보유출통제정책을 말한다. 본 통제정책을 통하여 구성원들이 내부정보를 취급할 때 준수해야 할 업무절차 및 기준과 이를 위해 운영되고 있는 각 보안통제 시스템의 연계운영 정책 및 모니터링·대응 기준을 제시한다.

■ People

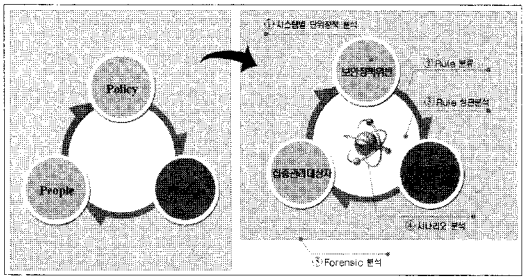
기업 내부정보유출통제정책 기반 하에 집중관리가 필요한 인력을 중심으로 내부정보유출통제를 수행하는 것을 의미한다. 집중관리대상자는 기업 내 주요 시스템 운영·개발자를 포함한 핵심 내부정보취급자와 퇴직자, 휴직자 및 내부정보 통제시스템 연계를 통해 탐지된 보안정책 위반자 등 내부정보유출통제를 위해 집중 모니터링 추적관리가 필요한 인력을 의미한다.

■ Process

내부정보 취급 업무 시 내부정보취급자의 악의적 또는 부주의 등으로 인해 유발될 수 있는 프로세스상의 내부정보유출 위험을 보안통제 관리 포인트로 정의하고, 각 보안통제시스템 연계를 통해 지속적으로 모니터링·탐지·대응 관리하는 것을 말한다.

결국, PPP[Policy, People, Process] 관점의 대응전략의 변화는 기업 내부정보유출통제정책 체계하에서, 내부정보를 취급하는 핵심인력 및 보안통제 위반자 등 집중 관리 대상자를 중심으로, 내부정보 취급업무 시 야기될 수 있는 내부 정보유출 위험을 탐지·모니터링·예방하고 지속적으로 관리해 나가는 것을 말한다.

이러한 PPP 관점의 대응전략하에서 내부정보 유출을 지속적으로 통제·관리하기 위해서는 단위 솔루션 기반이 아닌, 각 내부정보 통제시스템 연계를 통한 내부정보 유출 시나리오 기반의 유출분석 정책이 필요하다.

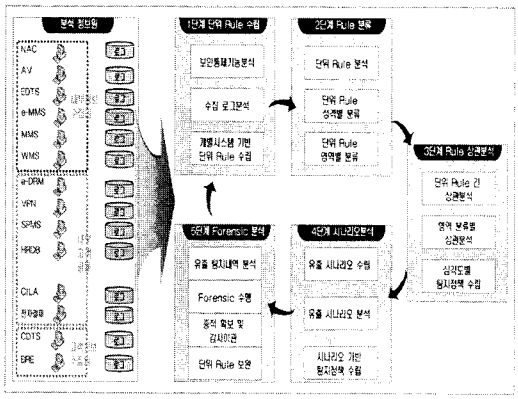


〔그림 2〕 PPP관점의 내부정보 유출분석 정책

위와 같이 PPP를 기반으로 보다 신뢰성 있고 효율적인 내부정보 유출분석 정책개발을 위해 수립·적용된 "5단계 정책 개발 방법론"및 각 단계별 정책 개발 내용은 다음과 같다.

· 1단계 : 단위 Rule 수립

선정·정의된 연동대상 및 수집 로그를 기준으로 해당 보안 시스템의 고유 통제 기능을 활용하여 내부정보유출과 관련된 보안통제 누락, 우회, 유출 징후, 유출 적발 등의 탐지가 가능하거나, 해당 시스템의 효과적인 보안통제 및 강화를 위해 필요한 추가 보안기능 등을 고려하여 개별 시스템의 단위 Rule을 수립한다.



〔그림 3〕 5단계 정책 개발 방법론

▪2단계 : 단위 Rule 분류

1단계에서 수립된 개별 시스템의 단위 Rule을 성격별, 영역별로 분류한다.

〔표 2〕 Rule 성격별 분류

성격별	분류 내용
정보유출 예방조치	▪룰에서 탐지된 정보를 이용해서 사적으로 정보유출을 예방할 수 있는 조치를 취하도록 유도하는 룰이 속한 그룹 ▪룰의 결과에 따라 예방조치를 취할 수 있는 근거 제공
정보유출 징후모니터링	▪룰에서 탐지된 정보를 분석했을 경우 정보유출 징후로 판단하여 집중적으로 관리 및 모니터링 해야 할 사람을 도출하는 룰이 속한 그룹 ▪룰의 결과에 따라 집중 모니터링 해야 할 근거 제공
정보유출 탐지	▪룰에서 탐지된 정보를 분석했을 경우 정보유출 가능성이 높은 정보를 도출하는 룰이 속한 그룹 ▪룰의 결과에 따라 감사 등 실증 자료를 획득해야 할 근거 제공

▪3단계 : Rule 상관분석

보다 신뢰성 있는 내부정보유출 탐지를 위해 PPP[보안정책, 정보유출, 사람] 관점으로 분류된 단위 Rule을 기준으로 Rule간 상관분석을 수행한다. 상관분석 시 추가 보안통제 우회탐지, 보안정책 적용 누락탐지, 보안통제 기능강화, 내부정보 유출탐지 및 Rule 연계를 통해 탐지결과의 신뢰성을 강화할 수 있는지 여부를 분석한다.

분석을 통해 개발된 Rule을 1~3단계 심각도로 그룹핑하여 보다 효과적으로 모니터링 · 대응할 수 있도록 구현하고, 연동대상 시스템간 정책 연계를 통해 보안통제 시너지를 증대한다.

〔표 3〕 Rule 영역별 분류

성격별	분류 내용
보안정책 영역	▪내부정보유출통제정책에 명시되어 있는 기본 보안정책을 준수하지 않고 내부정보취급업무를 수행하고 있는 정책 위반 또는 누락을 탐지해내는 Rule이 속한 그룹
정보유출 영역	▪내부정보취급자가 메일, 메신저, 기타 저장매체 등을 통해 외부로 정보를 비정상적으로 전송, 반출한 경우를 탐지해내는 Rule이 속한 그룹
사람영역	▪정보유출방지를 위해 집중 모니터링이 필요한 퇴직자, 휴직자, 핵심 내부정보 취급자, 보안정책 위반자 및 기타 집중관리대상자가 내부정보유출통제정책에 명시된 보안정책을 위반하였거나, 비정상적으로 내부정보를 취급한 경우를 탐지하는 Rule이 속한 그룹룰의 결과에 따라 감사 등 실증 자료를 획득해야 할 근거 제공

▪4단계 : 시나리오 분석

시나리오 분석은 심각도 1에 준하는 조건들로 탐지

〔표 4〕 상관분석 개발 Rule의 심각도 분류

심각도 분류	위험도	분류 내용
심각도 1	높음	▪동일한 사람이 보안정책 및 환경 위반 영역과, 정보 유출 영역, 사람영역 모두에서 비정상 행위자로 탐지된 경우 ▪모든 영역을 위반한 사항으로 정보유출이 시도 되었다고 매우 신뢰할 수 있는 정도의 수준을 나타내는 것으로, Forensics 등을 통한 정밀 업무 분석 등을 실시할 수 있는 근거 제공
심각도 2	보통	▪동일한 사람이 보안정책 및 환경위반 영역에 속하는 룰과 정보유출영역에 속하는 룰에 비정상행위자로 탐지된 경우 ▪이러한 사용자는 집중 관리 대상자로 선정하여야 하고, 실제로 유출된 정보가 고객 또는 내부정보가 포함되어 있는지 검증 하는 절차를 수행하여야 함.
심각도 3	낮음	▪동일한 사람이 보안정책 및 환경위반 영역과, 정보 유출 영역, 사람 영역에 관계없이 2개 이상의 비정상 행위자로 탐지된 경우 ▪이러한 사용자는 집중 관리 대상자로 선정하여 지속적으로 모니터링 되어야 함

된 내역 중 실제 내부정보취급환경에서 악의적 행위를 통해 내부정보를 외부로 유출 가능하거나, 유출에 준하는 비정상 행위를 수행한 내역을 Case별 시나리오로 만든다. 이렇게 만들어진 유출 시나리오를 기반으로 시나리오 Rule을 개발한다.

• 5단계 : Forensics 분석

탐지 결과 중 시나리오 및 심각도 1의 탐지 내역을 집중적으로 모니터링 · 분석하고, 분석결과에 따라 유출 징후 정밀조사 및 증적 확보를 위한 Forensic을 요청 · 수행할 수 있도록 구현 시 이에 대한 프로세스를 수립하고 이를 반영 · 고려하여 정책 개발을 수행한다.

2.1.3 정책 개발

"2.1.2 정책 개발 방법론"에서 살펴본 방법론에 따라 내부정보 유출분석 정책을 개발하였으며, 각 단계별 정책 개발 결과는 다음과 같다.

■ 1단계 단위 Rule 수립

개별 시스템을 기반으로 총 46개의 단위 Rule이 수립되었으며, 각 단위 Rule들은 16개의 대상시스템에서 상호 연관이 있는 정보들을 조합하여 만들었다. 각 단위 Rule별 내용 및 목적은 [표 6]과 같다.

〔표 5〕 개별 시스템 기반 단위 Rule 수립 결과

대상 시스템	구분	Rule 명	중요도	관련시스템
e-DRM	1-1	# e-DRM솔루션 미설치자	중	e-DRM, HRDB, SPMS
외 10개				
CILA	2-1	# IP 변경 시도	상	CILA, 예외정책 적용대상 IP목록
외 3개				
NAC	3-1	# 보안솔루션 미설치자	중	NAC, IP별 필수 솔루션목록, SPMS 예외자 목록
외 4개				
Anti Virus	4-1	# 정보유출 유관 및 기타 특정 바이러스 감염자	하	AV, 정보유출과 유관한 Virus/ Warm 목록
SPMS	5-1	# 집중관리대상자 정책변경 신청/승인/사용 이력이 있는 경우	중	e-DRM, SPMS, HRDB, ERP
VPN	6-2	# VPN 접근권한 위반(IP, 계정, 접근 시스템 등)	상	VPN, HRDB, ERP
VPN	6-7	# VPN e-DRM 파일 리딩	중	VPN, e-DRM, 특정 키워드 목록
e-MMS	7-2	# 퇴직예정자, 집중관리 대상자가 발신자인 메일 중 특정 키워드가 존재하는 메일	중	e-MMS, HRDB, ERP, 키워드 목록
외 5개				
WMS	9-2	# 비정상 Site 접근(구직 Site, 웹하드, 웹메일 및 기타 차단 사이트)	중	WMS
WMS	9-3	# 집중관리 대상자(예외자 포함) 등 특정대상자, 특정 시간대특정 Web Site 접근 이력(대상자 목록)	중	WMS, HRDB, ERP
EDTS	10-1	# 집중관리대상자(퇴사자, 퇴사예정자, 휴직자 등) 송수신	중	EDTS, HRDB, ERP
외 5개				
CDTS	11-1	# 등록자, 요청자, 추출자 및 송수신자가 집중관리대상자인 경우	중	CDTS, HRDB, ERP
외 4개				
HRDB	12-3	# 퇴직자/휴직자 계정을 통한 특정시스템, 메일 로그인 및 사용 이력	중	HRDB
BRE	14-1	# 심각도 2이하 수집 데이터 중 집중관리 대상(퇴직, 휴직, 정책예외자 등)과 관련된 건	중	BRE, HRDB, ERP
BRE	14-2	# 심각도 2이하 Data 중 타 시스템 탐지 Rule중 복자(IP, 사번…)	중	BER, NAC, AV, e-DRM, DCS, SPMS

■2단계 Rule 분류

▪ 단위 Rule 성격별 분류

1단계 단위 Rule 수립을 통해서 개발된 46개의 단위 Rule 분석을 수행하였으며, 46개 단위 Rule을 내부정보 유출 사전예방, 내부정보 유출 모니터링, 내부정보 유출 탐지 3가지 성격별로 다음과 같이 분류하여 운영자가 3가지 관점에서 지속적으로 탐지결과를 관리하고 문제 발생 시 신속하게 대응을 수행할 수 있도록 하였다.

〔표 6〕 단위 Rule 성격별 분류

내부정보 유출 사전예방	내부정보 유출 모니터링	내부정보 유출 탐지
e-DRM솔루션 미설치자	승인되지 않은 저장매체 사용자	CDTS 파기 파일 R/W
e-DRM 장기 미인증자	보안문서 출력 건수(업무 시간 내/외)	퇴직자, 휴직자 계정을 통해 퇴직 후 및 휴직기간에 메일이 발송된 경우
e-DRM 비정상 사용자	승인되지 않은 FTP 사용자	메일 송신자가 특정 사람인 메일 발송 이력(경쟁사, 특정인 등)
외 20개		

▪ 단위 Rule 영역별 분류

46개 단위 Rule을 PPP[Policy, People, Process] 관점의 보안정책, 사람, 정보유출 3가지 영역으로 분류하여 내부정보 유출방지정책 체계하에, 집중관리대상자를 중심으로, 내부정보 유출 위험을 지속적으로 모니터링 · 탐지 · 대응할 수 있도록 하였다.

〔표 7〕 단위 Rule 영역별 분류

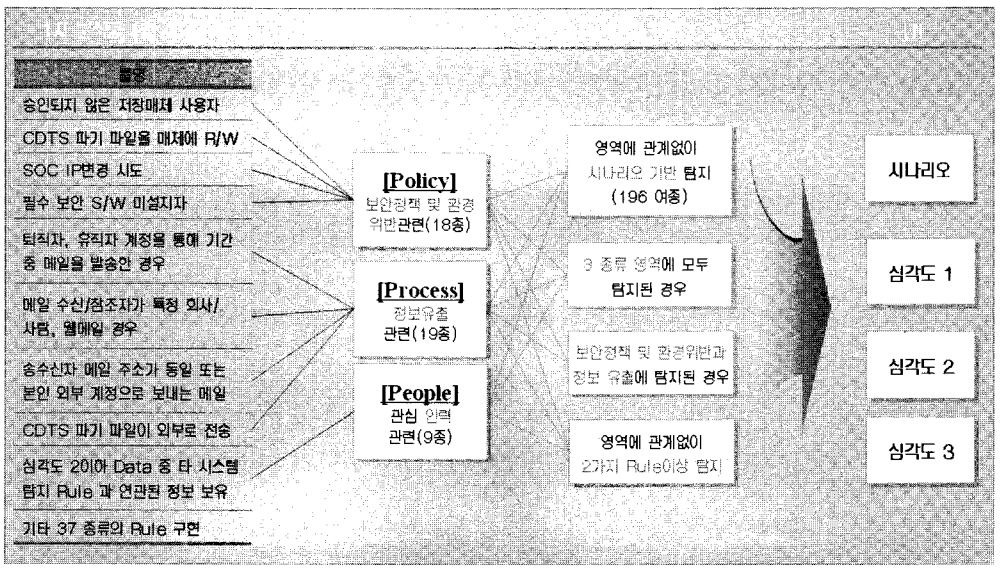
보안정책 및 위반	정보유출 탐지 모니터링	집중관리 대상자
e-DRM솔루션 미설치자	보안문서 출력 건수 (업무시간 내/외)	보안 해제권자가 집중관리 대상자(퇴직예정자)인 경우
e-DRM 장기 미인증자	승인되지 않은 ftp 사용자	집중관리대상자 정책변경 신청/승인/사용 이력이 있는 경우
외 17개		

■3단계 Rule 상관분석

▪ 상관 분석 기준

단위 Rule 간 및 영역 분류별 상관 분석 시 다음과 같은 사항을 기준으로 연계 필요성 여부를 분석하였다.

- Rule 연계를 통해 도출된 탐지 결과가 보다 신뢰성이 강화될 수 있는지 여부
- 내부정보유출통제정책 우회 행위 탐지 가능 여부
- 내부정보유출통제정책 적용 누락 탐지 가능 여부



〔그림 4〕 심각도 Level별 Rule 분류

- 내부정보유출 징후 탐지 가능 여부
- 내부정보유출 적발 가능 여부
- 기타 보안통제 기능강화 가능 여부

▪상관분석을 통한 심각도 Level별 Rule 분류

단위 Rule 간 및 영역 분류별 상관 분석 결과를 기준으로 다음과 같이 1~3 Level의 심각도 분류가 정의되었다.

- 심각도 1 Level

내부정보유출 분석을 통해 PPP[Policy, People, Process] 관점 즉, 내부정보유출 통제정책을 위반한 집중관리대상자의 내부정보유출 행위가 탐지된 경우로, 위험도가 높은 수준의 심각도를 가지고 있은 Level을 말한다.

심각도 1 Level로 상관분석 분류된 Rule은 총 3,078개이며, 내부정보유출 통제정책 위반 영역 18개 Rule과 집중관리대상자 영역 9개 Rule 및 내부정보유출 행위 관련 19개 Rule 간 조합을 통해 개발되었다.

- 심각도 2 Level

내부정보유출 분석을 통해 PP[Policy, Process] 관점 즉, 내부정보유출 통제정책을 위반한 자의 내부정보유출 행위가 탐지된 경우로, 해당 탐지 내역 분석을 통해 실제 정보 유출이 있었는지 확인하고 조치가 필요한 수준의 심각도를 가지고 있은 Level을 말한다.

심각도 2 Level로 상관분석 분류된 Rule은 총 342개이며, 내부정보유출 통제정책 위반 영역 18개 Rule과 내부정보유출 행위 관련 19개 Rule 간 조합을 통해 개발되었다

- 심각도 3 Level

내부정보유출 분석을 통해 PPP[Policy, People, Process] 관점 즉, 내부정보유출 통제정책을 위반, 핵심관리되어야 할 집중관리대상자의 위반행위 탐지, 내부정보유출 행위 탐지 중 2개 이상 비정상 행위자로 탐지된 경우로, 해당 탐지 대상자를 집중관리대상자로 선정하고 지속적인 모니터링 · 관리 및 조치가 필요한 수준의 심각도를 가지고 있은 Level을 말한다.

심각도 3 Level로 상관분석 분류된 Rule은 총 1,036개이며, 내부정보유출 통제정책 위반 영역 18개 Rule과 집중관리대상자 영역 9개 Rule 및 내부정보유출 행위 관련 19개 Rule 영역에 상관없이 2개 Rule의 조합을 통해 개발되었다.

■4단계 시나리오 분석

기업 내부정보취급업무 환경에서 실제 내부정보유출 통제정책을 위반 및 우회한 정보유출 행위가 발생 할 수 있는 시나리오를 수립하고, 연동대상 시스템 단위 Rule과 상관분석을 통해 수립된 심각도별 탐지정책을 활용하여 Case화된 시나리오 탐지정책을 수립한다.

이렇게 수립된 시나리오 기반 탐지정책은 다음과 같다.

〔표 8〕 시나리오 기반 탐지정책

No	SN	시나리오
1	S1	e-DRM솔루션 미설치자(1-1)가 고객정보관련 특정 키워드(고객, 주민번호, 전화번호 등)가 포함된 정보를 EDTS, Mail, 메신저를 통해 전송(10-5, 7-5, 7-8)한 경우
2	S2	e-DRM솔루션 미설치자(1-1)가 내부정보관련 특정 키워드(경영, 회계, 인사, 판매, 연구 등)가 포함된 정보를 EDTS, Mail, 메신저를 통해 전송(10-5, 7-5, 7-8)한 경우
3	S3	"S1"에 탐지된 사람이 집중관리 대상자인(7-2)이거나 수신자가 특정 경쟁회사/사람인 경우(7-7)
4	S4	"S2"에 탐지된 사람이 집중관리대상자인(7-2)이거나 수신자가 특정 경쟁회사/사람인 경우(7-7)
5	S5	e-DRM솔루션 미설치자(1-1)가 고객정보관련 특정 키워드(고객, 주민번호, 전화번호 등)가 포함된 일정 용량 이상, 갯수 이상의 파일을 저장매체에 저장(1-8, 1-9, 2-5)한 경우
등 99개		

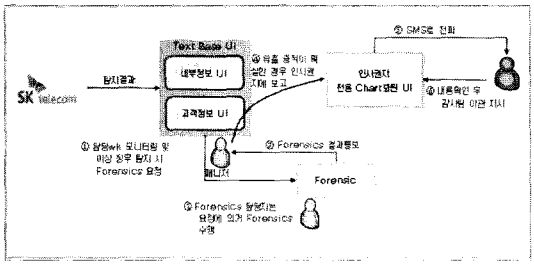
■5단계 Forensic 분석

1단계 단위 Rule 수립에서부터 4단계 시나리오 분석까지 4단계를 통해 수립된 탐지 정책을 적용하여 내부정보유출 탐지를 수행하고, 심각도 1 Level 및 시나리오 Rule을 중심으로 탐지된 내역이 실제 정보유출 여부인지 확인하는 분석 활동을 수행한다.

추가적으로 유출 · 위반 행위에 대한 정밀분석 및 증적 확보가 필요할 경우 다음과 같은 프로세스로 Forensics 분석 업무를 수행한다.

위 Forensics[17] 요청 및 수행 절차와 연계된 유출 탐

17) 컴퓨터를 매개로 이루어지는 행위에 대한 법적 증거 자료 확보를 위하여 컴퓨터 저장 매체 등의 컴퓨터 시스템과 네트워크로부터 자료(정보)를 수집, 분석 및 보존하여 법적 증거물로서 제출할 수 있도록 하는 일련의 행위를 말함.



〔그림 5〕 Forensics 요청 및 수행 절차

지내역 분석활동을 통해 탐지결과의 신뢰성 확보를 위한 지속적인 단위 Rule 추가·보완 작업이 필요하다.

이를 위해 단위 Rule 개선 및 유지·관리 시 1~4단계 개발 방법론에 근거하여 해당 정책을 변경 및 적용하는 것이 용이하도록 기 개발된 정책의 관리성 및 확장성이 보장되도록 구현되었다.

3.1 개발 정책 적용 결과분석

3.1.1 정책 적용 결과 분석

지금까지 개발된 46개 단위 Rule에 대한 모의 테스트 시나리오 및 실 환경 Rule 적용 결과 검증 수행을 통해 정보유출방지를 위한 다양한 운영환경개선 요소들이 도출되었다.

〔표 9〕 46개 단위 Rule 검증 결과

[NAC]NAC 미적용 네트워크 사용자	▪ NAC, e-DRM 시스템 기능 제약 및 비정상 업무 행위, IP 관리 누락 등으로 NAC 미적용 사용자 중 정상 사용자가 존재함
[e-DRM] e-DRM 솔루션 미설치자	▪ HRDB에 등록된 정보가 타 시스템 연계 등을 통해 자동으로 업데이트되어 최신정보로 관리되고 있지 않아 비정상 사용자 탐지가 과도하게 발생되고 있음
[e-DRM]동시 다중인증사용자	▪ 다수 PC 사용자 또는 이동 근무자가 비정상 사용자로 탐지되고 있음
외 27건	

이러한 운영환경 개선요소들을 정리해보면 다음과 같다.

첫째, 단위 보안솔루션 운영 중 발생되고 있는 보안통제 누락 사항들이 식별되었다.

둘째, 단위 보안솔루션 보안기능 강화 및 보안솔루션 연계를 통한 내부통제 시너지가 증대되었다.

셋째, 단위 보안솔루션들의 운영 시 지속적으로 관리·개선되어야 할 보안요건이 식별되었다.

넷째, 법적 대응 및 Due Diligence가 가능한 활발한 내부정보보호 활동 수행의 근거가 제공되었다.

다섯째, Forensics 연계를 통해 보다 전문화·체계적인 정보유출 추적·분석 및 대응이 가능하다.

Ⅲ. 결 론

본 정책개발을 통해 최근 내부정보유출 사고 대응과 국·내외 정보보호관련 규제 강화에 보다 신뢰성 있고 효과적으로 대응할 수 있는 정보유출방지체계가 구축되었다.

본 정보유출방지체계는 기업 내부정보 Life Cycle 상에 유발되는 비정상적인 활동을 통합 모니터링하고 모니터링 결과에 근거한 정보유출 사고 징후 판단 및 사전 조치활동 수행을 통해 정보유출을 보안사고를 예방할 수 있다.

또한 6하 원칙에 의거 보안사고 유발자 및 유발 원인, 유출경로를 분석하여 동일 사고의 재발 방지를 위한 사후 조치활동이 가능하며, 보안상 관리 허점이 될 수 있는 보안업무 수행인력 및 핵심 내부정보취급자의 업무를 패턴화하여 집중 모니터링하고, 탐지 및 정책위반 보안통계를 기반을 둔 다양한 보안활동 등을 통해 구성원의 인식제고를 유도할 수 있는 근거자료로도 활용 가능하다.

최근 DLP 등의 정보유출방지솔루션과 통합보안관리 시스템과 차별화되어 기업 내부정보보호정책 기반 하에 내부정보를 취급하는 사람을 중심으로 한 정보유출대응과 내부정보취급 업무 프로세스 단계에서 유발될 수 있는 내부정보유출 행위에 대한 신뢰성 있는 정보제공뿐만 아니라 이를 기반으로 한 기업의 효과적인 Due Diligence 및 법적 대응에 이르기까지 PPP 기반의 완전한 내부정보유출분석 방법론이 적용·구현된 것이다.

하지만 이러한 정보유출방지체계의 신뢰성 및 효과성이 보장되기 위해서는 탐지된 정보유출행위에 대한 보안조직의 활발한 예방 및 추적대응 활동도 중요하지만 무엇보다도 탐지·분석 Rule에 대한 지속적인 개선·관리가 반드시 수반되어야 한다.

향후 보다 다양한 보안솔루션들로 대상 범위를 확장

하고, 본 정책개발 시 제한되었던 단위 솔루션들의 보안 기능 고도화 등을 통해 탐지·분석 Rule을 개선하는 작업을 수행하여 보다 더 신뢰성 있고, 효과적인 정보유출 방지체계를 통한 포렉식 검증이 필요하다.

참고문헌

[1] SK텔레콤(주) http://www.sktelecom.com.

[2] 한국정보보호진흥원 홈페이지 http://www.kisa.or.kr.

[3] 국회 홈페이지, http://www.assembly.go.kr.

[4] 안철수 연구소, http://www.ahnlab.com.

[5] 국제해킹동향 및 정보제공홈페이지 http://www.zone-h.org.

[6] 국가사이버안전센터 홈페이지 http://www.ncsc.go.kr.

[7] 전사적 위험관리 : 개념과 사례, LG경제연구원, 2004. 1.

[8] 유비쿼터스 기술과 서비스, 진한엔엠비, 2005, 이기혁.

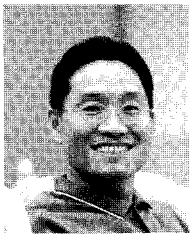
[9] 유비쿼터스 IT혁명과 제3공간, 전자신문사, 2004.

[10] 송성근 외 3명 "정보기술 유출에방을 위한 기업내 컴퓨팅 환경 최적화 방안연구", 한국정보보호학회지, 2008. 12.

[11] 이기혁 외 1명 "민간기업의 개인정보유출 위험에 대한 측정방법과 그 사례에 대한 연구", 정보보호학회지, 2008. 6.

[12] 최 승, "불확실성을 고려한 위험분석 방법론 연구", KIPS 논문집 제11권 제2호, 2004. 11.

〈著者紹介〉



이 기 혁 (Lee Gi Hyouk)

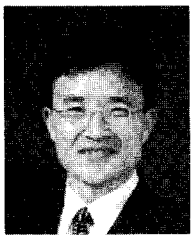
정회원

2008년 3월~현재: 건국대학교 대학원 벤처전문기술학과 공학박사 과정중

1994년 5월~현재: SK Telecom (주)정보기술연구원 재직중

<관심분야> 정보통신공학, 정보통신정책분야, 정보보호학, 개인정보보호공학등

<저서> 유비쿼터스 사회를 향한 기술과 서비스(2005, 진한엠엔비) 유비쿼터스 컨버전스(2004, 진한엠엔비), 차세대무선인터넷기술(2003, 진한엠엔비)등 다수



이 철 규 (Lee Cheol Gyu)

1991년 3월: 일본 게이오대학교 공학석사

1997년 3월: 일본 게이오대학교 공학박사

2004년 8월~현재: 건국대학교 대학원 벤처전문기술학과 교수,

2008년 9월~현재: 건국대학교 벤처창업지원센터 소장, 한국창업학회이사

<관심분야> 벤처기술경영, 정보보호학, 경영컨설팅학, 경영공학 등