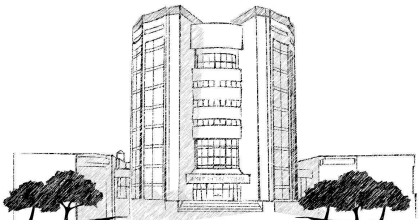
2015년 KISTI 침해사고 대응 분석 보고서
(3/4분기)



2015. 11.

KISTI 한국과학기술정보연구원
Korea Institute of Science and Technology Information
www.kisti.re.kr

목 차

그림 목차

표 목차

Ⅰ 개요

1. 목적 및 필요성

○ 지능화 다양화 되고 있는 사이버 위협 및 APT와 같은 표적 공격으로부터 KISTI의 정보시스템 및 데이터를 안전하게 보호하기 위한 보안 활동 및 대응 방안이 필요함

○ 사이버보안센터에 침해사고 신고 및 처리결과를 분석하여 가시화하고 현장 실사를 통한 보안점검 및 취약점 분석 등을 통하여 향후 사고의 재발방지에 대한 개선 노력이 필요함

2. 분석 내용 및 범위

○ 침해사고 발생 현황 및 침해 위협 유형별 분석
- 월별 침해사고 발생 현황 및 처리결과에 대한 통계 분석
- 침해 위협 유형을 6가지로 분류하고 해당 사고에 대한 조사·분석 및 대응을 통한 위협 사항 도출

○ 부서별 월별 사고 건수 및 처리결과에 대한 분석
- 부서별 월별 사고 건수 및 처리결과에 대한 통계 분석
- 사고 미처리에 대한 원인 분석

3. 분석 활용 계획

○ 침해사고 대응 전략 수립
- 사고 재발 방지 대책 및 사고 대응 프로세스 고도화
- 사고 처리 지원에 대한 환경 및 수준 분석을 통한 시사점 도출

Ⅱ KISTI 침해사고 대응

1. KISTI 침해사고 대응체계

○ KISTI의 침해사고 대응체계는 국가정보원 국가사이버안전센터(NCSC) 및 미래창조과학부 과학기술사이버안전센터(S&Tsec), 원내 전 부서와의 긴밀한 협조체계를 기반으로 대응

[그림 1] KISTI 침해사고 대응 체계

구분	역할
국가사이버안전센터 및 과학기술사이버안전센터	- 중앙집중형 24시간 상시 상황 관제 - 침해사고 발생 시 정보화혁신실 통보 - 침해사고 처리결과 확인
정보화혁신실	- 침해사고(유관기관 통보사항 및 내부탐지) 접수 - 침해사고자 사고내용 통보 및 사고처리 강제 - 침해사고 처리지원 및 사후 조치 확인 - 국가사이버안전센터 및 과학기술사이버안전센터 처리결과 통보
내부 전부서	- 침해사고 처리 - 침해사고 처리결과 정보화혁신실 제출

2. 대응절차

○ KISTI의 침해사고 대응절차는 예방, 탐지, 분석, 대응, 복구 등의 체제를 유지하고 있으며, 세부적으로는 준비단계, 사고탐지단계, 초기대응단계, 사고처리단계, 복구단계, 보고서작성단계, 보고단계 등으로 이루어짐

[그림 2] KISTI 침해사고 대응절차

○ 준비단계 : 침해사고를 예방하기 위하여 시스템을 점검하고 보안장비를 설치하는 것은 물론 사고대응팀을 구성하여 구성원의 역할과 대응절차를 사전에 수립

○ 탐지단계 : 국가정보원 사이버안전센터, 미래창조과학부 과학기술사이버안전센터, 정보화혁신실 등으로부터 이상 징후를 탐지

○ 초기대응 : 침입인지 단순한 장애인지를 결정하는 단계로 사고의 완전한 분석이 아닌 사고의 확산을 방지하고 차단하는 조치를 취하며, 추후 정밀조사를 위한 증거자료 수집

○ 조치단계 : 사고자에게 사고 사실을 통보하고 6하 원칙에 기인하여 언제 누구에 의해 어떤 자료가 유출, 훼손되었는지 조사하고 복구 할 수 있는 방법에 대한 자료 수집

○ 복구단계 : 악성 프로그램을 제거하고 삭제된 프로그램을 복구하는 등의 작업을 통해 침해 시스템과 네트워크를 정상적인 상태로 되돌리는 단계

○ 보고단계 : 사고 내용에 대한 내용을 보고할 수 있도록 문서화

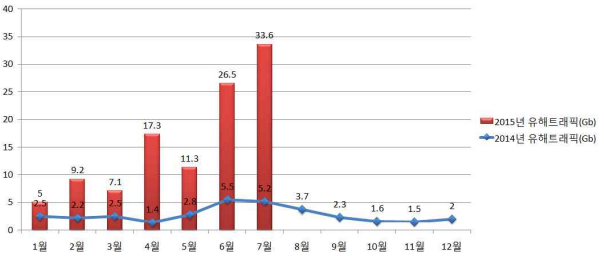
○ 후속조치 : 사고대응 과정에서 발생된 문제들에 대한 검토 회의를 통해 미비점 개선

Ⅲ 현황 분석

1. 7월 종합 분석

○ 7월 침해사고 분석

- 2015년 7월 유해 트래픽은 [그림 3]와 같이 33.6Gb로 전월 대비 6.9Gb 증가하여, 꾸준히 증가하고 있으며, 여전히 높은 수치를 보였다.

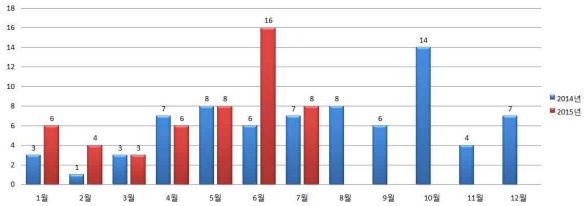


[그림 3] 7월 유해트래픽 추이

- 2015년 7월 침해시도 건수는 [표 1]와 같이 총 8건으로 전월 대비 8건 감소하였다.

구분	2014년						2015년						
	7월	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월	7월
침해 시도 현황	6	7	8	6	14	4	7	6	3	6	8	16	8

[표 1] 7월 침해 시도 현황



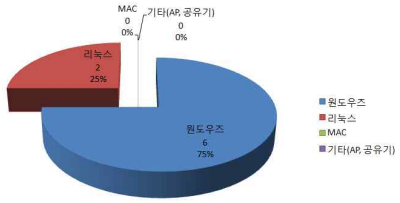
[그림 4] 7월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 2]와 같이 웜·바이러스에 의한 침해시도가 7건으로 가장 많았으며, 대부분 웹서비스(TCP 80) 이용 중 발생한 것으로 파악된다.

구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	7	1	0	0	0	0	8

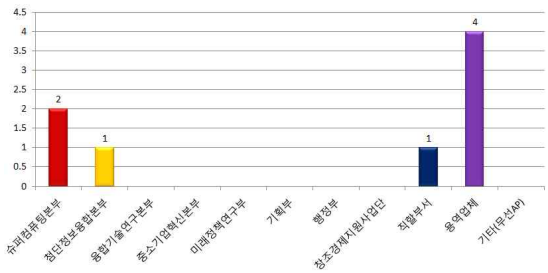
[표 2] 7월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 5]과 같이 윈도우즈 시스템을 통한 사고가 6건으로 가장 많은 비중을 차지했으며, 리눅스를 통한 사고가 2건으로 뒤를 이었다.



[그림 5] 7월 시스템별(OS) 사고 건수

- 부서별로는 [그림 6]과 같이 용역업체가 4건으로 가장 많았고, 그 뒤로 슈퍼컴퓨팅본부가 2건 발생하였으며, 침단정보융합본부, 직할부서가 각각 1건씩 발생하였다.



[그림 6] 7월 부서별 사고 건수

○ 7월 보안 이슈 및 향후 계획

- 이달에는 랜섬웨어가 감염된 사고가 발생하였다. 랜섬웨어는 이메일, 인스턴트 메세지, 웹사이트 등에서 링크를 클릭할 때 설치되며, 설치된 뒤에 문서나 스프레드시트, 그림 파일 등을 암호화해 열지 못하도록 한 뒤, 돈(비트코인 등)을 보내주면 암호화를 해제하여준다고 하며 금품을 요구한다.

- 하지만, 돈을 보낸 뒤에도 데이터가 복구 될수 있는 가능성은 무척 희박하며 일부 랜섬웨어는 파일의 내용도 변경 시킨다.

- 랜섬웨어는 이미 감염된 후에는 데이터를 복구할 수 있는 별다른 방법이 없기 때문에 사용자의 다음과 같은 주의를 요구한다.

1. 취약성 공격 차단 프로그램 사용

- 이번 랜섬웨어의 확산 방법과 같이 웹사이트를 통해 사용자의 취약성을 이용한 악성코드 배포 시에는 취약성을 이용한 공격을 사전에 차단하는 프로그램을 이용하여 안전한 상태를 유지할 수 있다.

2. 스팸 메일 첨부파일 실행 금지

- 출처가 불분명한 메일 삭제, 발신인이 확인되지 않으면 클릭 금지, 지인의 메일도 한번 더 확인해야 한다.

3. 운영체제 및 각종 응용프로그램 보완 업데이트 진행

- MS OS 업데이트를 포함하여 IE, JAVA, Flash, Microsoft Silverlight, XMLDOM, Office, 한글 등 대표적인 어플리케이션은 항상 최신 버전을 유지한다.

4. 백신 프로그램 최신 업데이트 유지

- 백신 프로그램을 필수적으로 설치하고 최신 엔진을 유지한다.

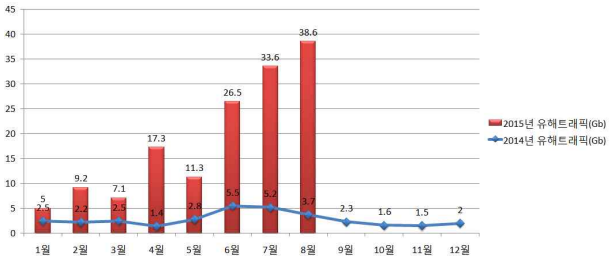
5. 중요 문서 및 파일 백업 필수

- 중요한 파일에 대해서 해당 시스템 이외의 별도 저장공간에 백업하고, 해당 시스템에 저장 시에는 압축 암호화해 별도 보관, 혹시 감염되더라도 피해를 최소화해야 한다.

2. 8월 종합 분석

○ 8월 침해사고 분석

- 2015년 8월의 유해 트래픽은 [그림 7]과 같이 38.6Gb로 전월대비 2Gb 증가하였다.

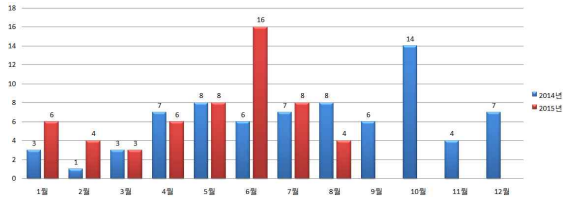


[그림 7] 8월 유해트래픽 추이

- 2015년 8월 침해시도 건수는 [표 3]와 같이 총 4건으로 올해 평균(8건/월)에 비해 4건 적은 수치를 보였다.

구분	2012년					2013년							
	8월	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월	7월	8월
침해 시도 현황	7	8	6	14	4	7	6	3	6	8	16	8	4

[표 3] 8월 침해 시도 현황



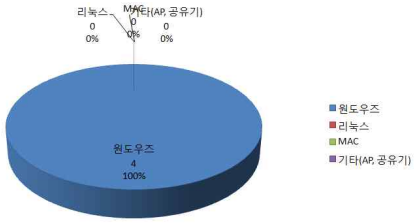
[그림 8] 8월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 4]와 같이 웜·바이러스에 의한 침해시도가 4건으로 모든 사고가 웜·바이러스에 의해 발생 하였다.

구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	4	0	0	0	0	0	4

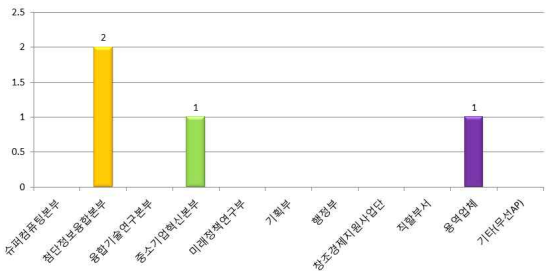
[표 4] 8월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 9]과 같이 윈도우즈 시스템을 통한 사고가 4건으로 모든 사고가 윈도우 시스템을 통해 발생하였다.



[그림 9] 8월 시스템별(OS) 사고 건수

- 부서별로는 [그림 10]과 같이 첨단정보융합본부가 2건으로 가장 많았으며, 그 뒤로 중소기업혁신본부, 용역업체에서 각각 1건씩 발생하였다.



[그림 10] 8월 부서별 사고 건수

○ 8월 보안 이슈 및 향후 계획

- 웹서비스(TCP 80)를 통한 침해시도는 올 초부터 꾸준히 발생하고 있는 것으로 나타났다. 주로 웜·바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 시스템 정보를 전송하는 행위가 많이 발생하였다.

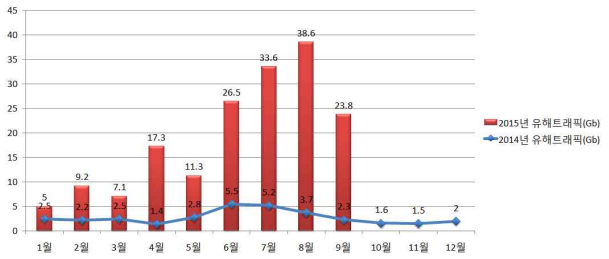
- 웹사이트 방문 시 의심스러운 프로그램(ActiveX)의 설치를 금하며, 출처 및 의심스러운 이메일은 열람하지 않도록 주의가 요구된다. 또한 업무용 PC가 DDoS 공격 및 해킹 공격을 유발하는 좀비 PC가 되지 않도록 윈도우 및 백신을 최신 버전으로 업데이트 하는 등 신규 취약점에 대한 대비가 요구된다.

- 이달에는 BIND DNS신규 취약점 발견으로 인해 BIND 보안업데이트가 진행되었다. 신규 취약점은 BIND DNS에 조작된 특정패킷을 보내면 서비스장애가 발생하는 취약점(CVE-2015-5477)으로 BIND 9.9.7-P1 및 이전의 9.x 버전과 BIND 9.10.2-P2 및 이전의 9.10.x 버전에서 발생하였다. 이에 기관 DNS 서버 총 4대에 대한 BIND S/W 업그레이드 작업이 진행되었다.

3. 9월 종합 분석

○ 9월 분석

- 2015년 6월 유해 트래픽은 [그림 11]와 같이 23.8Gb로 전월 대비 14.8Gb 감소하였다.

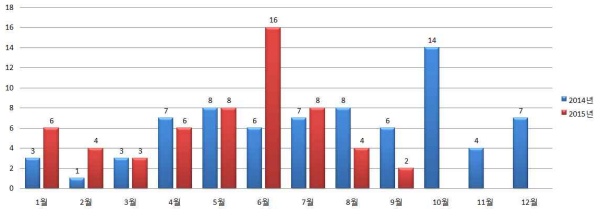


[그림 11] 9월 유해트래픽 추이

- 2015년 9월 침해시도 건수는 [표 15]와 같이 총 2건으로 전월 대비 2건 적은 수치를 보였고 6월 이후 꾸준히 감소하고 있다.

구분	2014년										2015년		
	9월	10월	11월	12월	1월	2월	3월	4월	5월	6월	7월	8월	9월
침해 시도 현황	8	6	14	4	7	6	3	6	8	16	8	4	2

[표 5] 9월 침해 시도 현황



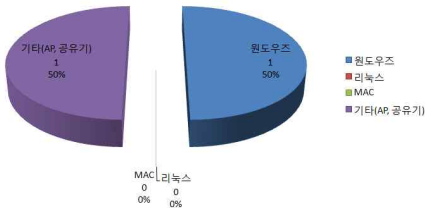
[그림 12] 9월 침해시도 건수 추이

- 침해유형별로 살펴보면 [표 6]와 같이 웜·바이러스에 의한 침해시도가 2건으로 모든 사고가 웜·바이러스에 의해 발생 하였다.

구분	웜·바이러스	자료훼손 및 유출	홈페이지 위·변조	경유지 악용	서비스 거부	단순 침입시도	합계
건수	2	0	0	0	0	0	2

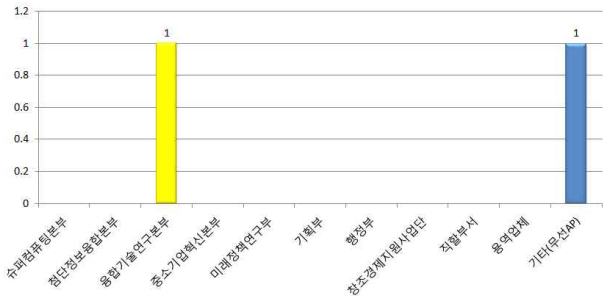
[표 6] 9월 침해 위협 유형별 분석

- 시스템별(OS)로는 [그림 13]과 같이 윈도우즈 시스템을 통한 사고가 1건, 무선 AP를 통한 사고가 1건 발생하였다.



[그림 13] 9월 시스템별(OS) 사고 건수

- 부서별로는 [그림 14]과 같이 융합기술연구본부가 1건으로 무선 AP를 통한사고가 1건 발생하였다..



[그림 14] 9월 부서별 사고 건수

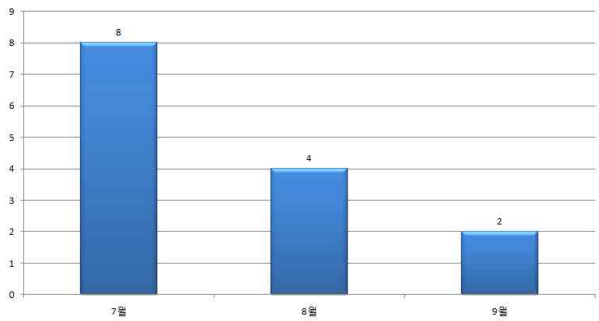
○ 9월 보안 이슈 및 향후 계획

- 9월의 보안사고 중 주목할 만한 사항은 기관 무선 AP를 통한 사고이다. 점차적으로 태블릿PC 및 스마트폰 등 모바일 기기를 업무에 활용하는 사례가 증가하고 있으며, 더불어 기관 무선 AP를 통한 침해시도도 증가 추세를 보이고 있다.

- 현재 기관 무선 AP를 통한 사고발생 시 사용자 및 사용 Device에 대한 정확한 추적 및 조사가 어려운 실정이다. 따라서 위 문제를 해결하기 위한 대책으로 소속 직원이 사용하는 무선 Device에 대한 식별 및 접속 로그에 대한 분석이 가능하도록 시스템을 개선할 필요가 있으며, 사용자별로 접속 가능한 Device를 제한하는 등의 보안 강화가 요구된다.

Ⅳ 종합분석 및 개선방안

○ 2015년 7월부터 9월까지의 침해시도 건수는 [그림 15]와 같이 총 14건으로 7월이 8건으로 가장 많이 발생하였으며, 그 뒤로 8월이 4건 9월이 2건으로 꾸준히 감소하고 있다.



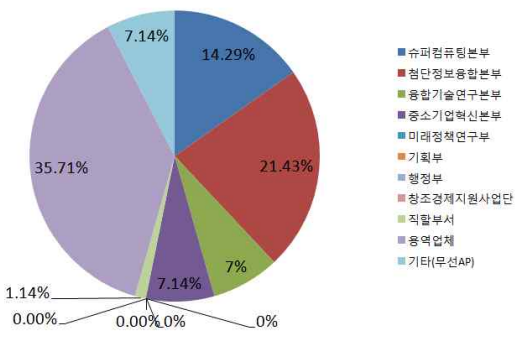
[그림 15] 3분기 월별 침해시도 건수

○ 침해 유형별로는 [표 7]과 같이 웜·바이러스에 의한 사고가 13건으로 가장 많은 비율을 차지하였으며, 그 뒤로 자료유출 및 회손사고가 1건 발생되었다.

	7월	8월	9월
웜·바이러스	7	4	2
자료훼손 및 유출	1	0	0
홈페이지 위·변조	0	0	0
경유지 악용	0	0	0
서비스 거부	0	0	0
단순침입시도	0	0	0
합계	8	4	2

[표 7] 침해 위협 유형별 분석

○ 부서별로는 [그림 16]과 같이 용역업체가 5건(35.71%)으로 가장 많은 비중을 차지하였으며, 그 뒤로 첨단정보융합본주가 3건(21.43%), 슈퍼컴퓨팅본부에서 2건(14.29%)의 사고가 발생하였다.



[그림 16] 3분기 부서별 사고 건수 비율

• **외주용역사 직원(방문객 포함)**

- 외주용역(방문)사를 통한 사고가 총 5건으로 전체의 35.71%를 차지할 정도로 높은 사고율을 보였다. 외주용역 직원 및 방문객의 PC에도 소속직원과 동일한 수준의 보안 에이전트 설치 후 기관 네트워크에 접속 할 수 있도록 사업부서의 철저한 보안 관리가 요구된다.
- 또한 사업부서 방문객의 개인 노트북 및 휴대형 저장매체를 활용할 경우에는 사업담당자의 승인 하에 반입·반출하며, 최신 백신프로그램으로 악성코드 감염여부를 점검하고 자료 무단 반출 여부를 지속적으로 점검하여야 할 것이다.

• 보안사고 대응

- 현재 국정원 및 과학기술사이버안전센터를 통한 침해사고 접수 시 개인이 1차적으로 SysCheck 점검 및 백신 검사를 실시하고 있다. (단, 지원 요청 시 유지보수 업체에 의해 점검)
- 하지만 사고 발생 직후 즉각적인 대응이 어려워 정확한 사고 조사가 이루어지지 못하는 경우가 많으며, 서울 분원 및 각 지원에서 발생하는 사고에 대해서는 정보보안 담당 직원을 통한 점검 없이 백신 점검 및 포맷 등의 조치만 지원하고 있다. 향후 사고 대응 및 악성코드 분석을 위한 보안솔루션(포렌식 도구, 이벤트 수집 및 분석 도구 등) 도입 및 사고 조사에 필요한 전문 인력 확보가 요구된다.

• IP 주소 관리 강화

- 3분기에는 부서별 IP주소 현황조사 및 사용자PC이름 현행화를 통해 보안사고 발생시 신속한 사고자 파악이 이루어져 사고조사가 빠르게 이루어 졌다.

- 기존에는 부서 단위로 C클래스를 할당하여 부서에서 자율적으로 IP를 관리하도록 하고 있으나, 신규 직원 및 퇴직 직원 발생, 혹은 소속 직원의 부서 변경 시 정확한 IP 관리가 이루어지지 않기에 정보화혁신실에서는 부서별 IP할당에 따른 관리 미흡으로 증가된 미사용 IP 관리와 보안사고 시 사고 PC의 IP확인 지연으로 인한 보안 위험을 최소화 하기 위해 IP 현황조사 및 사용자 PC이름 변경을 추진하였다.

- 마지막으로 사이버보안센터를 활용하여 침해사고의 프로세스를 체계화 하고 자료 증적을 통한 사후 점검 등 소속직원들의 자발적인 재발방지를 위한 노력이 요구된다.

• 서버 보안

- 관제현황 보고서에 따르면 3분기 공격 대상 포트와 스캐닝 대상포트 중 가장 많은 비율을 차지한 포트가 각각 TCP/22 (ssh),TCP/23 (Telnet)으로 원격접속에 대한 침해시도가 많이 탐지 되었다. 따라서 시스템 운영자는 비인가된 접속에 대한 로그관리와 ssh와 같은 서비스의 포트설정 변경, 원격에서 루트계정 로그인 금지, 패스워드 정책강화와 주기적인 패스워드 변경 등 서버보안을 위한 보안정책을 강화하여야 한다.

V 결론

○ 2014년 3분기 총 21건의 침해시도에 비해 2015년 2분기의 총 침해시도건수는 14건으로 7건의 감소를 보였다. 3분기에는 유해 트래픽이 평균 32Gb로 올해 최고치를 보였다. 이와 관련해서 새로운 바이러스와 악성코드들에 의해 발생할 수 있는 침해와 공격시도들을 대비하여 더욱 세심한 주의가 요구된다.

○ 3분기에는 2분기에 이어 복합 취약점을 이용한 악성코드 유포가 지속 되고 있다. MS IE, MS XML, Adobe Flash Player, Java 애플릿 취약점 등을 복합적으로 악용하여 악성코드를 유포시키는 사례가 올해들어 지속적으로 나타나고 있으며 주의를 요구한다.

○ 이러한 악성코드를 이용한 사고는 꾸준히 발생하고 있으며 대부분 TCP/80를 이용하여 발생하기 때문에 이용자는 MS 윈도우의 보안 업데이트를 항상 최신 상태로 유지할 것을 권장하고 백신프로그램을 이용하여 주기적으로 점검하여야 하며, Adobe Flash Player 및 Java 관련 취약점에 의한 악성코드에 감염되지 않도록 주의하여야 하며 웹사이트 방문시 의심스러운 프로그램 설치 금지 및 출처가 의심스러운 메일 열람 금지등 사용자 교육이 요구 된다.

- 향후 침해사고 발생 시 해당 직원에 대한 책임 추적성을 강화하고 사이버 보안진단의 날 행사를 활성화하는 등 전사적으로 보안문화가 형성될 수 있도록 해야 할 것이다.

- 향후 급증하는 사이버 침해와 정보 유출 사고에 대한 대응능력 배양 및 중요 정보자원의 위협 요인에 대한 사전 예방활동 강화를 위하여 지속적인 정보보안 모니터링 체제 강화를 통한 통합 위협 분석 및 위협 요인에 대한 개선 활동 수행이 요구된다. 또한 업무환경 변화 및 유관기관의 정책 변화에 대응하기 위한 내부규정 정비, 자체 보안감사 수행 및 예방활동 강화 등 정보보호 수준 신뢰도 제고를 위한 정보보안 전략 수립 등 종합적인 전주기적 보안관리 활동을 수행해야 할 것이다.

[별첨 1] 월별 침해위협 발생 현황

○ 7월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
1	2015-07-29 18:51	용역업체	웜・ 바이러스 감염(추정)으로 인한 악성 도메인 접속 시도 탐지	2015-07-30
2	2015-07-28 13:16	용역업체	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-07-28
3	2015-07-23 10:32	기술인텔리전스 연구실 윤혜성	웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-07-23
4	2015-07-22 18:40	슈퍼컴퓨팅 인프라실 이영주	웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-07-23
5	2015-07-22 10:31	용역업체	웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-07-22
6	2015-07-17 02:10	첨단연구망 서비스실 조현훈	OpenSSL의 취약점을 이용하여 시스템 정보유출 탐지	2015-07-18
7	2015-07-16 11:38	정보화혁신실 김재경	웜・바이러스 및 악성 프로그램 감염(추정)으로 인하여 경유지로 감염신호 전송	2015-07-16
8	2015-07-14 10:39	용역업체	웜・바이러스 감염(추정)으로 인한 악성 도메인 접속시도 탐지	2015-07-14

○ 8월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
9	2015-08-27 14:18:	산업정보분석실 김상국	웜・바이러스 감염(추정)으로 인한 악성 도메인 접속 시도 탐지	2015-08-27
10	2015-08-27 13:04	정보융합연구실 아르바이트	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 감염신호 송수신 행위 탐지	2015-08-27
11	2015-08-20 17:03	용역업체	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 중국 악성도메인 접근 시도 탐지	2015-08-20
12	2015-08-19 20:09	정보융합연구실 아르바이트	정보유출형 악성코드 감염(추정)에 의한 경유지로 감염신호 전송 탐지	2015-08-20

○ 9월 침해 위협 발생 현황

사고 번호	발생시간	사고부서	사고내용	처리시간
13	2015-09-08 15:52	생명의료 예측기술연구실 학생연구원	웜・바이러스 감염(추정)으로 인한 악성 도메인 접속 시도 탐지	2015-09-08
14	2015-09-04 00:20	무선 AP	웜・바이러스 및 악성 프로그램 감염(추정)으로 인한 감염신호 송수신 행위 탐지	2015-09-05

[별첨 2] 부서별 사고 건수

부서명	7월	8월	9월
슈퍼컴퓨팅본부	2	0	0
첨단정보융합본부	1	2	0
융합기술연구본부	0	0	1
중소기업혁신본부	0	1	0
미래정책연구부	0	0	0
기획부	0	0	0
행정부	0	0	0
창조경제지원사업단	0	0	0
직할부서	1	0	0
용역업체	4	1	0
기타(무선AP)	0	0	1
합계	8	4	2

[별첨 3] 침해시도 유형별 내용

침해시도	내용
웜・바이러스	· 웜·바이러스 감염 시도 및 전파 시도
자료훼손 및 유출	· FTP, 서버 및 PC 등의 권한이나 공유 설정의 취약으로 자료가 변조, 삭제되거나 유출, 열람 시도
홈페이지 위・변조	· 취약점 등을 이용하여 홈페이지의 메인 페이지 변조 시도나 사용하지 않는 페이지 삽입 시도 및 피싱을 목적으로 한 홈페이지의 변조
경유지 악용	· 해킹 피해 이후 다른 사이트를 공격하는 경유지로 활용하려는 시도
서비스 거부	·정보시스템의 데이터나 자원을 적절한 대기 시간 내에 사용하는 것을 방해하거나 과도한 부하를 일으켜 사용을 방해하려는 시도
단순침입시도	· 스캐닝 기법 등으로 시스템이나 네트워크의 취약점 점검 및 계정 추측 등의 침입 시도

[별첨 4] 사이버위기 상황 발생 시 대상별 협조 사항

대상	협조 사항
직원	1. OS, 백신, 업무용 프로그램 최신 업데이트 수행 2. 백신 소프트웨어 실시간 감시기능 사용 3. 출처, 첨부파일이 의심스러운 이메일은 열람하지 말고 삭제 4. 개인컴퓨터의 부팅, 로그인, 화면보호기의 패스워드를 설정하고 반드시 사용 5. 공유폴더 사용의 최소화하고 사용 시 반드시 최소 권한만을 부여하여 사용 6. 웹사이트 방문 시 설치하는 프로그램은 인증서 및 디지털서명을 참고하여 신뢰성을 확인 후 설치 7. 메신저를 이용한 파일 다운로드 시 최신 백신소프트웨어로 점검 후 사용 8. 중요한 자료는 패스워드를 설정하여 저장
시스템 운영 담당자	1. 웜·바이러스, 해킹 등에 의한 피해발생 가능성이 증가함에 따라 각종 시스템의 모니터링 강화 2. 해외 사이버 공격 피해가 확산되어 국내 유입이 우려되므로 이에대한 대비 필요 3. 네트워크 이상트래픽 과다 탐지 또는 부분 장애 등 사이버위협 징후 탐지활동 강화 필요