중소기업 침해사고 현황

- 중소기업 침해사고의 현주소

@이준형 / 책임연구원

PLAINBIT

CONTENTS

중소기업 침해사고 피해지원 서비스 소개

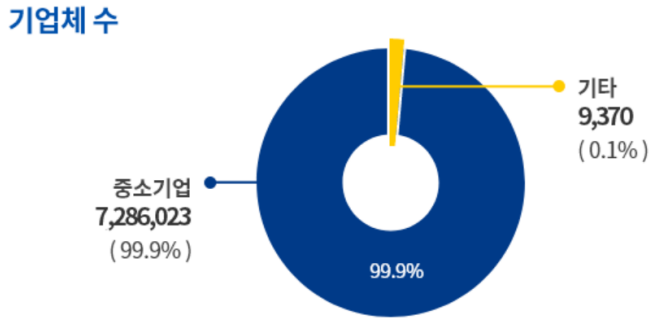
침해사고 피해지원 대국민 서비스

- 한국인터넷진흥원에서 중소기업의 침해사고 피해 최소화를 위해 시작
  - 2019 ~ 현재, 약 5년째 지속적 사업 수행 (약 2,300 건 지원)
  - 약 20명의 분석가 참여
- 지원 범위
  - 전국의 중소기업, 영세 사업자 등 (개인 X)
  - 원격/현장 기술지원, 보안교육, 보안컨설팅
  - 침해사고 사례 세미나
- 국내 중소기업 침해 방어
  - 국내 침해사고 발생 빈도 완화
  - 국민 생활 안정화 기여

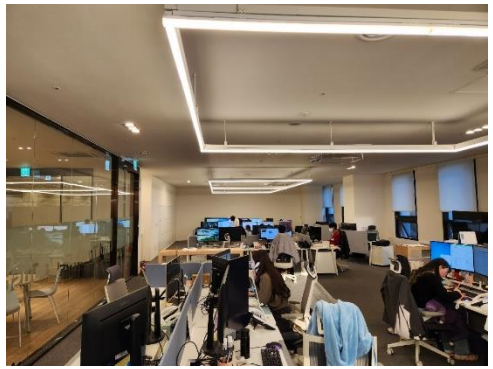
국내 기업의 99.9%는 중소기업...근로자 비중은 81.3%

입력 2022.07.28 06:00 수정 2022.07.28 06:00 가가

▲ 출처: https://www.hankyung.com/economy/article/202207288842Y

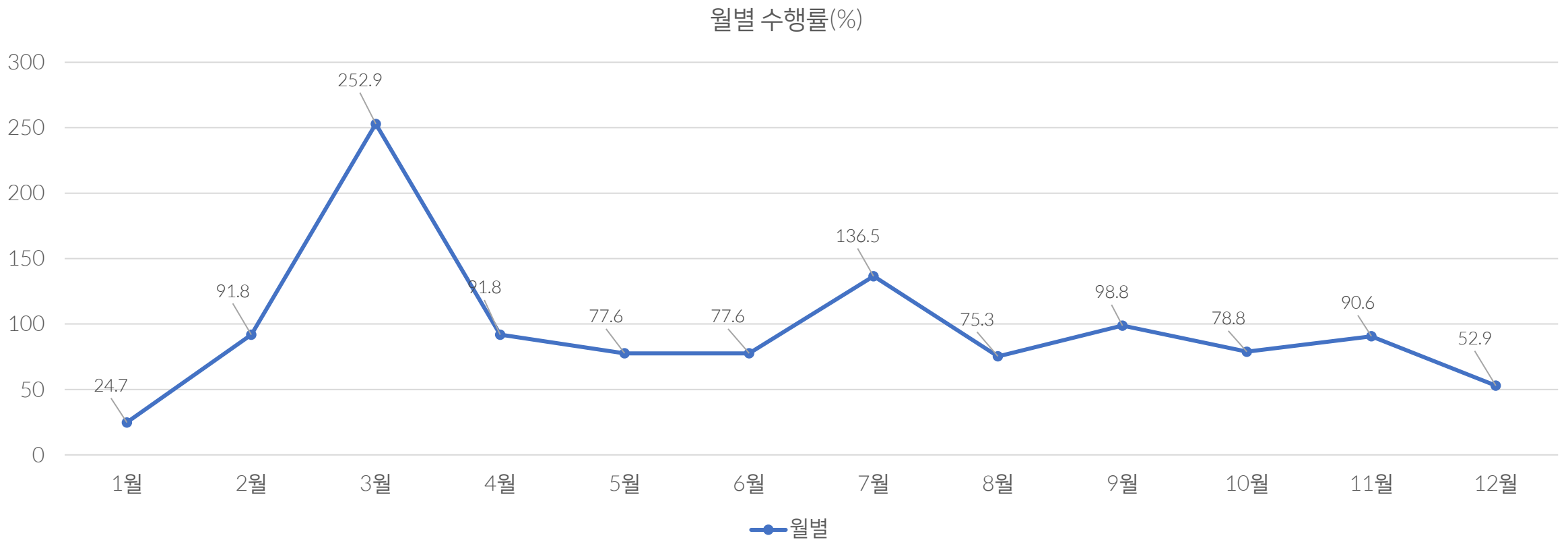


▲ 출처: 중소벤처기업부



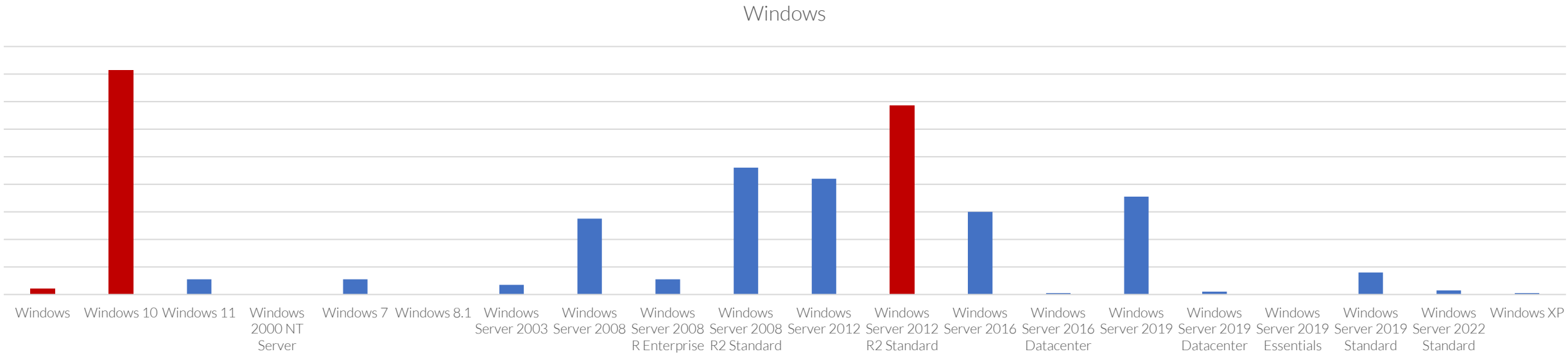
중소기업 침해사고 현황

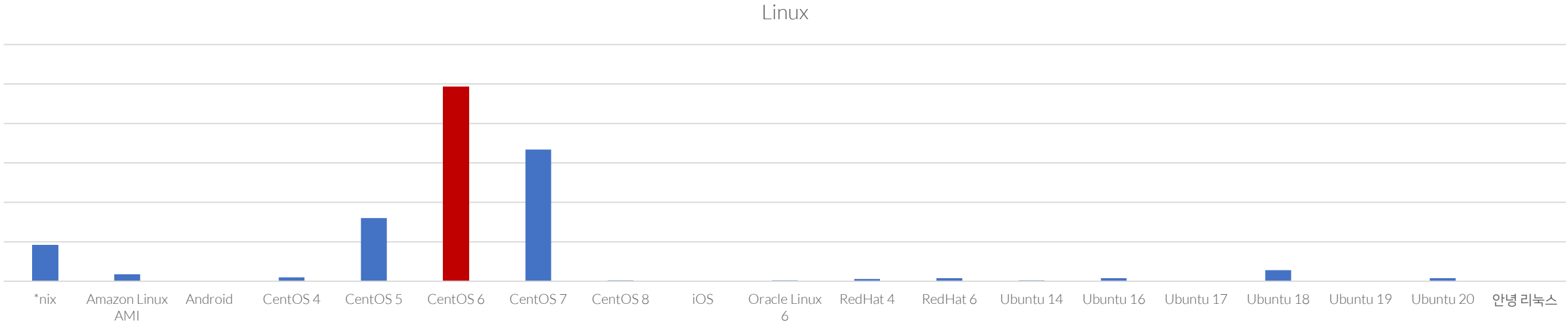
월별 기술지원 수행률



중소기업 침해사고 현황

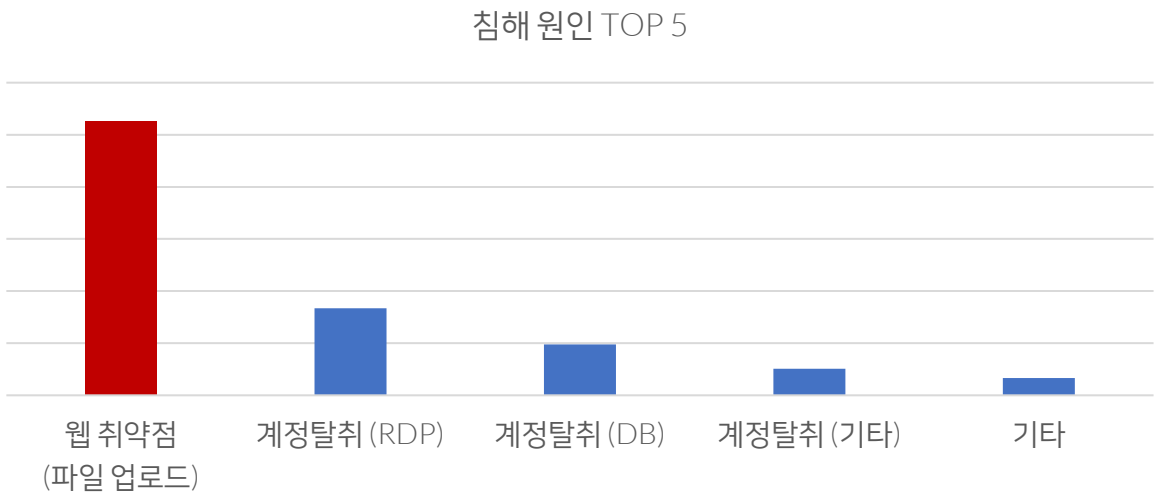
침해 운영체제

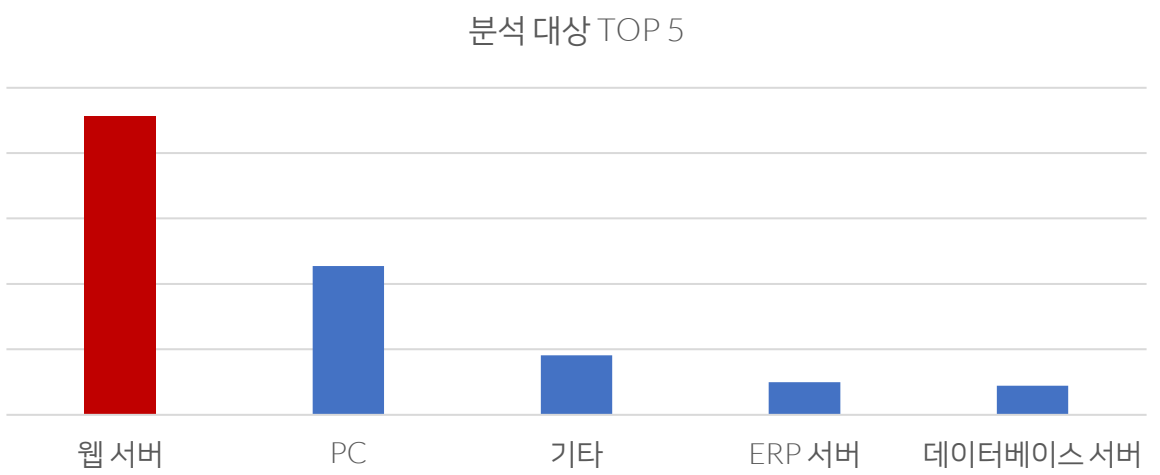


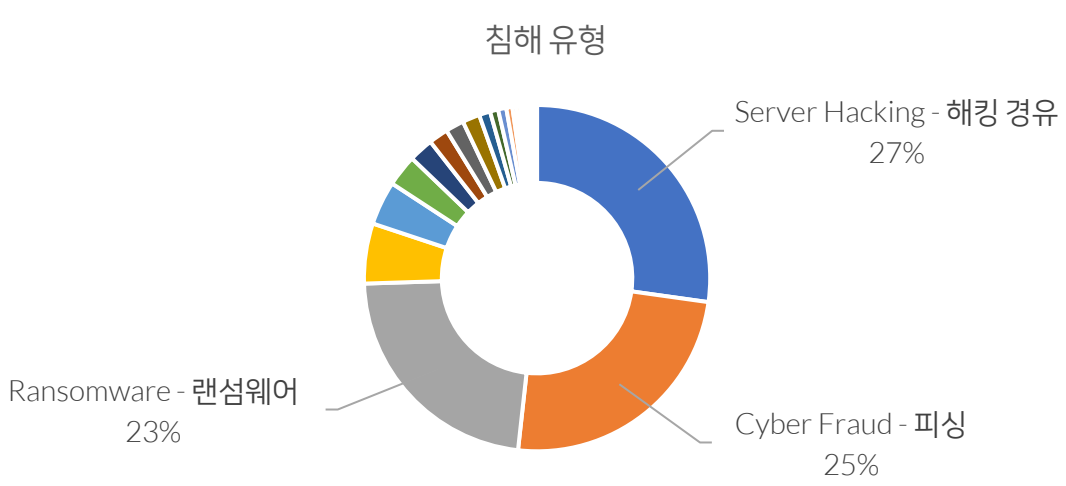


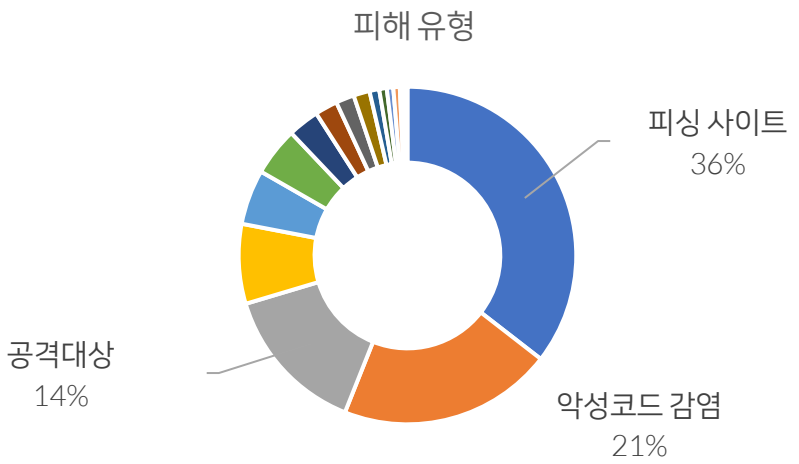
중소기업 침해사고 현황

다양한 통계







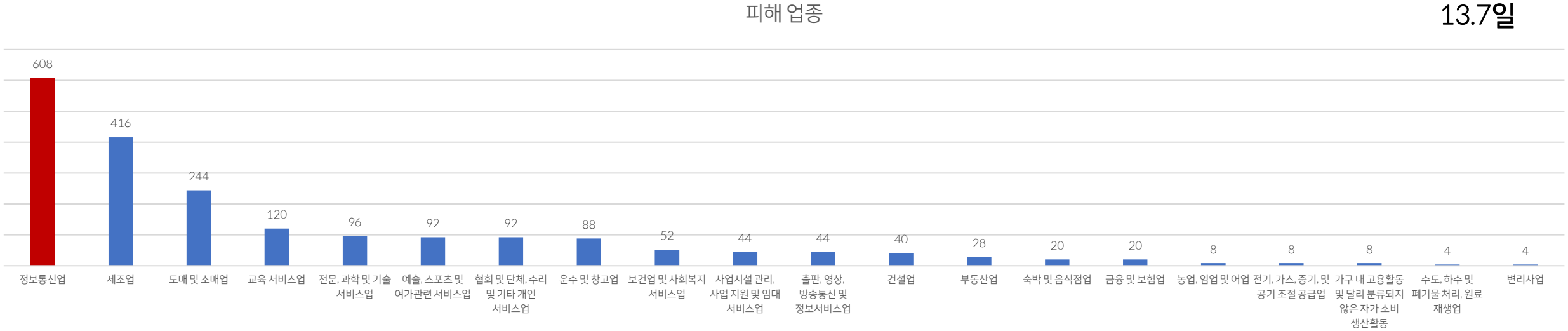


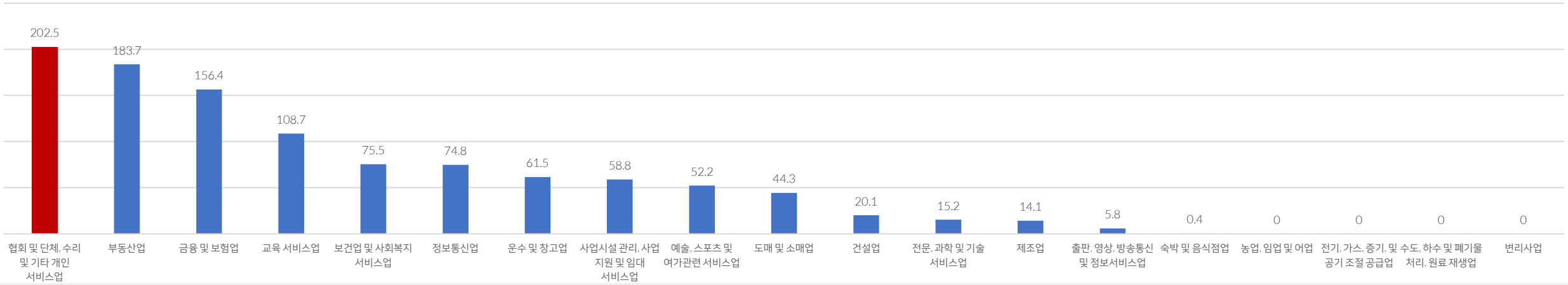
중소기업 침해사고 현황

피해 업종 / DWELL-TIME

평균 신고 기간

13.7일

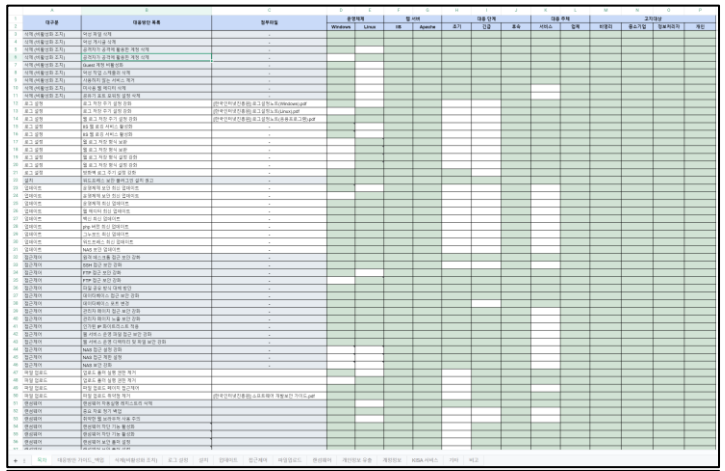


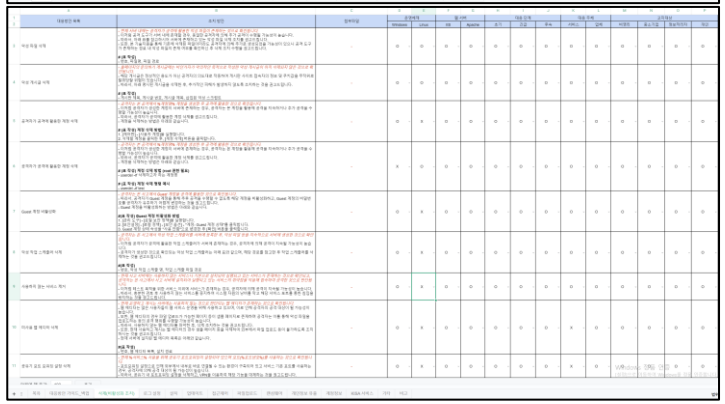


대응방안

- 대응방안 이행률 : 27.5%
- 미이행 사유
  - 외부 업체/고객사 협의 필요
  - 내부 사정으로 인해 추후 조치 예정
  - 보안 장비 구비 예정
  - 운영 시스템 오류 우려로 보류
  - 위험도 평가 진행 후 조치 예정
  - 서버 재설치 예정

총 대응방안 전달	조치 완료	미조치	미응답
567	156	190	221





삭제 (비활성화 조치)	9
로그 설정	10
설치	1
업데이트	9
접근제어	15
파일업로드	4
랜섬웨어	18
개인정보 유출	5
계정정보	7
KISA 서비스	7
기타	23

침해사고 피해지원 사례

자주 발생했던 침해사고

- 민감정보 탈취
  - 신용카드 정보 탈취
  - 개인정보 탈취
- 문자 무단 발송
- 랜섬웨어
- 해킹 경유지
- 네이버 팝업 피싱 사이트

민감정보 탈취 – 신용카드 정보 탈취

- 쇼핑몰의 결제 페이지를 위장해 신용카드 정보를 탈취한 침해사고
  - 특정 회사의 쇼핑몰 구축 솔루션의 취약점 활용
    - ✓ 로그 생성 함수 취약점
    - ✓ 템플릿 생성 함수 취약점
  - Pay.zip 이란 피싱 페이지 모음을 활용

민감정보 탈취 – 개인정보 탈취

- 공격 유형
  - PhpMyAdmin과 같은 웹 기반 데이터베이스 관리 페이지 침해
  - SQL Injection 공격 활용해 데이터베이스 데이터 탈취
- PhpMyAdmin 활용
  - Brute-force 공격 혹은 CVE-2022-23807(Bypass) 취약점 활용
  - Export 기능 이용해 데이터베이스 다운로드(탈취)
- SQL Injection
  - SQLMAP과 같은 도구로 스캔 후 공격
  - 대부분 성공…

문자 무단 발송

- 문자 발송이 가능한 서버 침해 후 문자 발송
  - 문자 발송 대상
    - ✓ 침해 당한 서버에 저장된 개인 대상
    - ✓ 불특정 다수
  - 문자 발송 방법
    - ✓ 공격자가 문자 발송 스크립트 생성 후 사용
    - ✓ 관리자 페이지에서 제공하는 문자 발송 페이지 사용
  - 피해 추산액
    - ✓ 약 2.4억원

랜섬웨어

- 랜섬웨어의 침해 경로는 다양함
  - Remote Desktop Protocol
  - 웹 파일 업로드
  - SSH / FTP
  - 사용자 부주의
  - MSSQL
  - …
- 사용자 입장에서 피해가 제일 눈에 띄는 공격

랜섬웨어 – BitLocker

- Windows 운영체제의 BitLocker 기능을 사용해 랜섬 행위 유발
  - 2016년부터 발생한 침해사고
  - Windows 기본 보안 기능을 활용하다 보니 탐지나 대응이 쉽지 않음
  - 공격자는 복구 키를 네트워크 다른 컴퓨터에

    저장하거나 본인 컴퓨터로 저장함

랜섬웨어 – NAS 대상

- 사내에서 사용하던 NAS 데이터가 모두 암호화되어 사용 불가
  - Synology NAS 사용
- 일반적으로 NAS가 암호화되었다면 아래 내용 확인 필요
  - SSH/FTP 포트가 열려 있는가?
  - 웹 관리 패널이 외부에서 접근 가능한가?
  - NAS와 연결 상태가 온라인인 PC가 있는가?

해킹 경유지 – RRAS

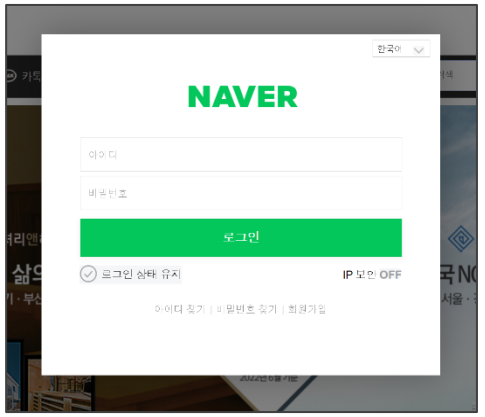
- Windows RRAS 구축 후 사용
  - RRAS(Routing and Remote Access Service) 서비스를 구축 해 VPN 서버처럼 활용
  - 공격자는 RRAS 서비스를 설치하기 위해 침투
    - ✓ 사용자는 서버 악용 여부를 확인할 수 없음
    - ✓ 공격자는 개인 VPN 서버를 구축

해킹 경유지 – 공격 거점

- 공격을 준비하거나 감행하기 위한 주요 서버
  - 공격자는 침투 후 본인의 계정을 생성해 본인의 시스템처럼 사용
    - ✓ king, default(User), … 생성
  - 보통 북한 관련 공격자가 이와 같은 서버를 많이 구축하려 함

민감정보 탈취 – 피싱 사이트

- 네이버 로그인 팝업 창을 띄워 사용자 계정 정보 탈취하는 침해사고
  - 공격은 2021.10 ~ 현재까지 진행 중
  - 2022년 가장 공격이 성행했고 현재(2023년)는 소강 상태



▲로그인 팝업 피싱 창

출력지

- 피싱 페이지 팝업 출력

경유지

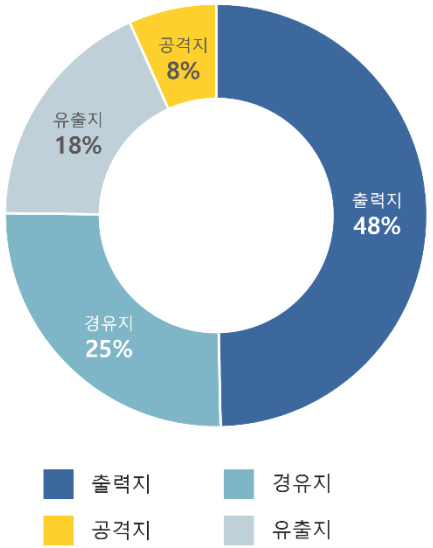
- 정보 유출지 내 저장된 로그인 페이지 연결

정보유출지

- 피싱 로그인 페이지 파일
- 계정정보 수집 파일 저장

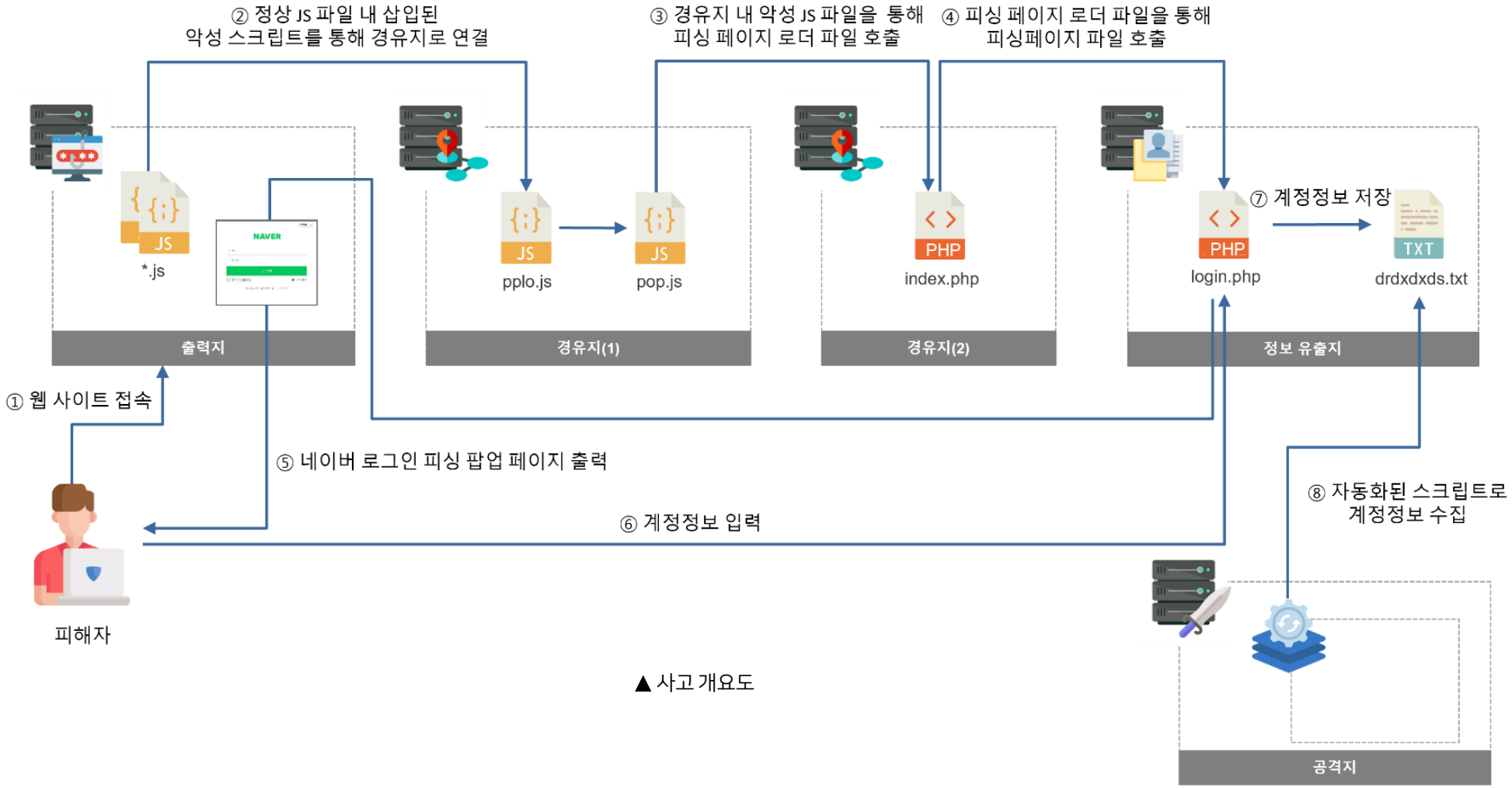
공격지

- 계정정보 수집 파일 수집
- 추가 공격 대상 파악
- 웹셸 업로드 및 접근
- 공격 인프라 구축 거점



상세 보고서 : https://kisa-irteam.notion.site/bb4b19a9bfe44da599ace4ab4897eff1

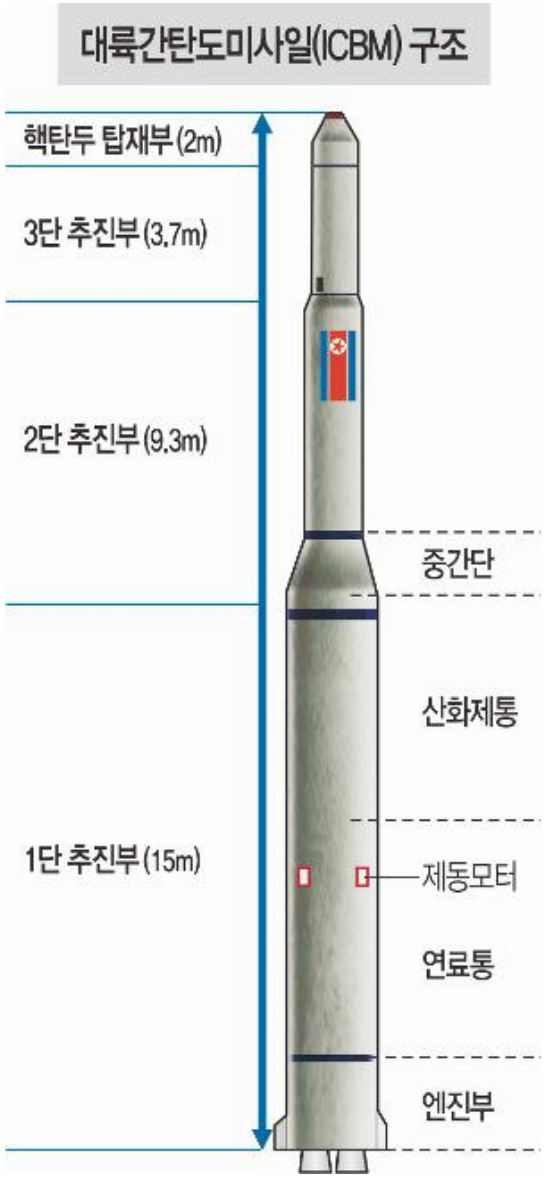
민감정보 탈취 – 피싱 사이트



▲사고 개요도

보안 인식 개선

- 미사일 = 침해사고
  - 목적 달성을 위한 전개 과정은 대부분 비슷하지만 탄두(영향)에 따라 사고의 파급력과 양상이 달라짐
  - 침해사고가 발생했다면, 결론이 어떻게 지어지는지는 공격자 판단에 따라 달라짐
    - ✓ 생화학탄두 ➔ 랜섬웨어
    - ✓ 핵탄두 ➔ 파괴형 악성코드
    - ✓ …
  - 침해 결과에 집중하는 것 보다 침해 발생 원인에 대해 집중!!



▲ 출처: http://news.kmib.co.kr/article/print.asp?arcid=0923463186

보안 인식 개선

- 침해대응 단위의 변화 (개인 ➔ 조직)
  - 1명이 사고를 대응하던 체계 ➔ 조직이 사고를 대응하는 체계
    - ✓ 대표적 예 : (FSB) Effective Practices for Cyber Incident Response and Recovery (2020)

- 전반적인 인식 개선 필요 ➔ 빠르고 정확한 침해대응 가능

분류	현재	개선
일반 사용자	• 우리는 피해 없으니까 괜찮다. • 사고 관련 내용은 아무도 몰라야 한다. • 악성파일만 삭제하면 될 것 같다. • 피해 복구가 되었으니 더 이상의 조치는 필요 없다.	• 다른 곳에 피해를 주고 있을 수 있다. • 사고 관련 내용은 적극적으로 공개해야 해결하는데 도움이 된다. • 악성파일은 언제든 다시 생성될 수 있다. • 침해 결과 해결보다 원인해결이 더 중요하다.
보안업무 관련 사용자	• 우리가 알아서 조치하겠다. • 보안 솔루션 설치되어 있다. (혹은 설치하겠다.) • 대응방안 적용보다 중요한 일이 많다. • 서버 재구축하면 된다.	• 침해대응은 생각보다 복잡하다. • 보안솔루션은 완벽하지 않다. • 공격자는 사람 1명과 무한에 가까운 공격 기계가 존재한다. • 대응방안이 마련되지 않으면 서버 재구축은 불필요하다.

중소기업 침해대응 제안

자원 관리

- 정보보호의 기본
- 관리 대상 자원들
  - 인프라 장비(보안 장비 포함) 로그
    - ✓ 방화벽 로그
    - ✓ 웹 로그
    - ✓ 서비스 로그
  - PC / 서버 / 기타 장비
  - IP 할당 정보
  - 접속 정보
  - 개발/유지보수 협력 업체(개인)
- 현황 파악 & 모니터링은 필수
  - 발생했거나, 발생하고 있거나, 발생할 예정이거나 ➔ 모두 확인 가능

- 로그 보존 방법은?
- 로그 보존에 따른 스토리지 비용은?

분류	자원 관리 실패 사례	실패에 따른 대응 영향
로그	• 로그 옵션 OFF • 로그 3일 분량 저장 • 로그 저장 경로 파악 불가 • 시스템에 로그가 너무 많이 쌓여 로그 다운로드 불가	정확한 원인 파악 불가
자원 현황	• 유휴 서버 / PC 존재 • 웹 서버는 존재하지만 어디에 있는지는 모름(?) • 자원의 사용자 파악 불가 • 클라우드 자원의 생성/삭제 현황 파악 불가 • 네트워크 구성도 부재 혹은 예전 버전	침해 확산 범위 및 영향도 파악 불가
자원 상태	• 접속 계정 정보 모름 • n년전 마지막 운영체제 업데이트	초동 대응 불가
기타	• 인터넷 노출 방치 (중요 정보/페이지 등)	대응 범위의 급진적 확대

중소기업 침해대응 제안

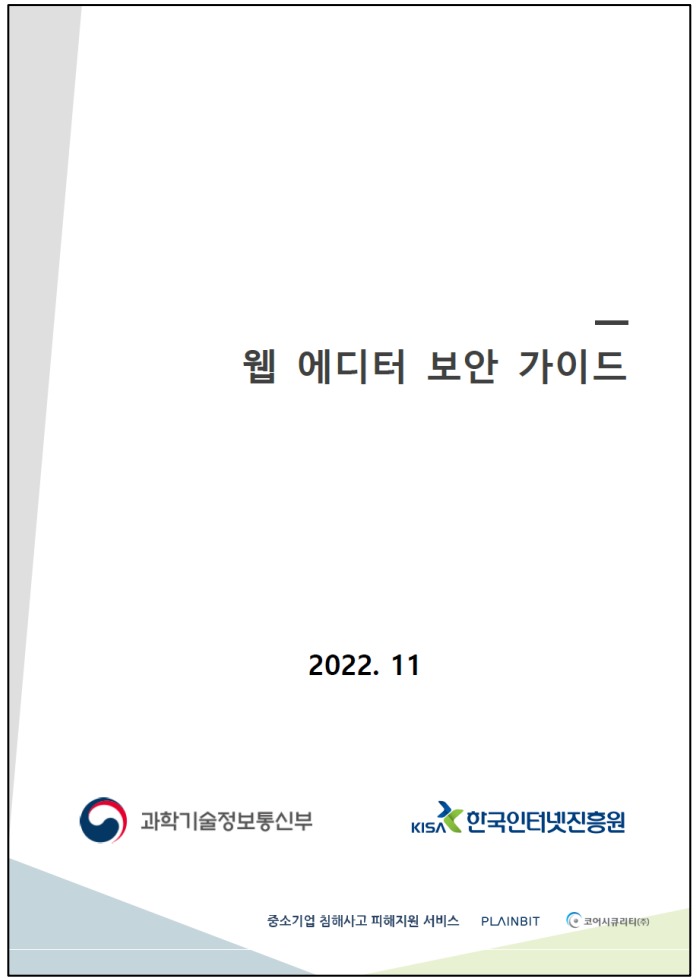
오픈 소스 점검

- 현재 웹 서버 침해사고에서 가장 많이 활용되는 취약점 ➔ 파일 업로드 취약점
  - 보통 오픈소스 웹 에디터에 존재하는 파일 업로드 취약점 공격
  - 공개된 오픈소스 웹 에디터는 CKEditor 제외하고 모두 개발 종료 ➔ 취약점 패치 X

- 오픈 소스는 제3자 입장의 어플리케이션이어서 웹 사이트 전체의 권한 등에 적용을 받지 않음
  - 관리자 페이지 내에서 동작하는 웹 에디터도 외부에서 호출 가능

- 현재 사용하고 있는 웹 에디터가 있다면 점검 필요
  - 보안 점검 가이드(웹 에디터 보안 가이드) :

    https://www.boho.or.kr/kr/bbs/view.do?searchCnd=1&bbsId=B0000127&searchWrd=&menuNo=205021&pageIndex=2&categoryCode=&nttId=67020

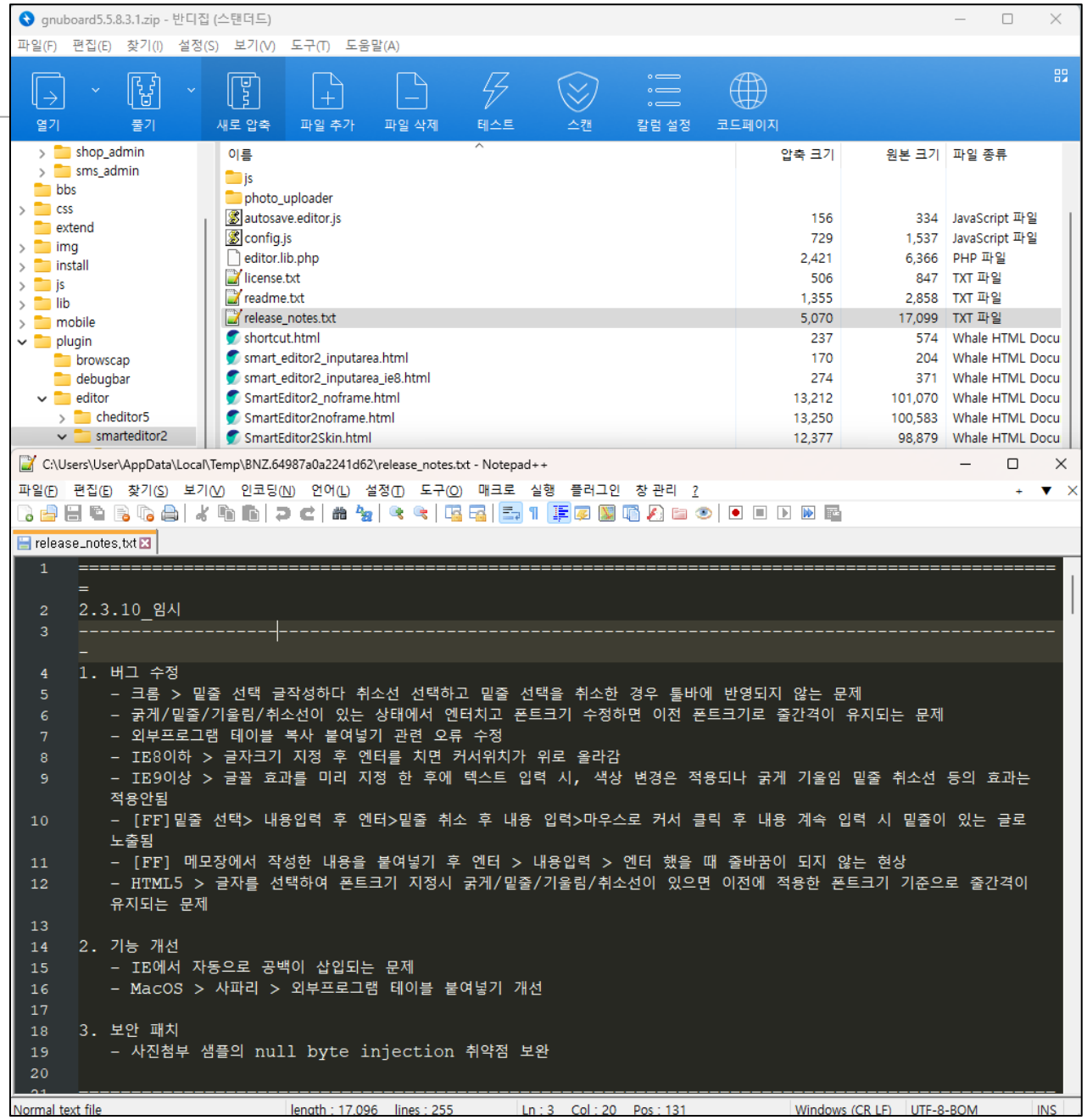


중소기업 침해대응 제안

오픈 소스 점검

- 공개된 웹 에디터

웹 에디터 종류	최신 버전	최신 버전 등록 일자
Alditor	-	2006-09-20
cheditor	5.1.9.4	2021-11-09
cheditor5	5.1.9.4	2021-11-09
Ckeditor	38.0.1	2023-05-23
Dreamweaver	21.3	2022-06-30
EZEditor	0.2.5	2015-12-23
FCKeditor	2.6.11	2014-06-02
Froala Editor	3	2019-05-16
G-Editor	1.0.0	2007-11-13
namoeditor	4	2022-07-01
Quill Editor	1.3	2014-08-12
RainEditor	10	2008-03-26
SmartEditor2	2.10.0	2019-08-10
Summernote Editor	0.8.20	2021-10-15
TinyMCE Editor	5.10.7	2022-12-06



▲ 출처: 그누보드 23.06.19 일자 보안 업데이트 버전

대국민 서비스 적극 활용

- 기업을 대상으로 진행되는 무료 보안 서비스 활용
  - 정기 서비스

한국인터넷진흥원	한국정보보호산업협회
• 내 서버 돌보미 • 보안 취약점 점검 • SW 보안약점 진단 • 중소기업 홈페이지 보안강화 • 중소기업 침해사고 피해지원 서비스 • 사이버 위협정보 분석공유 (C-TAS) • 사이버 위기대응 모의훈련 • 사이버 시큐리티 훈련 플랫폼 • DNS 싱크홀	• 정보보호 컨설팅/제품 공급기업 모집 • 랜섬웨어 대응지원 • 한국제로트러스트위원회

  - 비정기 서비스
    - ✓ 개인정보보호 무료교육 등

중소기업 침해대응 제안

PLAINBIT

결론

- 기본에 충실하자!
- 기술에만 의존하지 말자!
- 확장하는 것은 좋다, 최소한 3단계 확장 시 1단계 정도의 보안 확대를 고려하자!
- 복잡해진 IT 환경처럼 보안도 상당히 복잡해졌다!
- 공격자는 최고 수준의 보안을 뚫으려 노력하지만 결국 느슨해진 사용자의 허점을 이용한다!
  - 평균적인 보안 수준을 고민해보자!