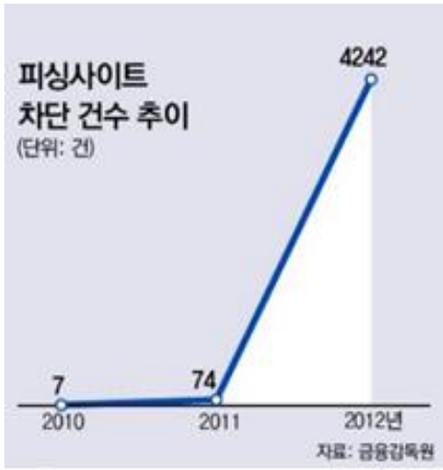
CERT1 인증서 보안관리 솔루션

필요성

인증서 해킹을 통한 피해사례 급증

❖ 악성코드 유포를 통한 인증서 정보 탈취 및 해킹

❖ 피싱사이트 및 파밍 수법을 통한 인증서 해킹 사례 급증

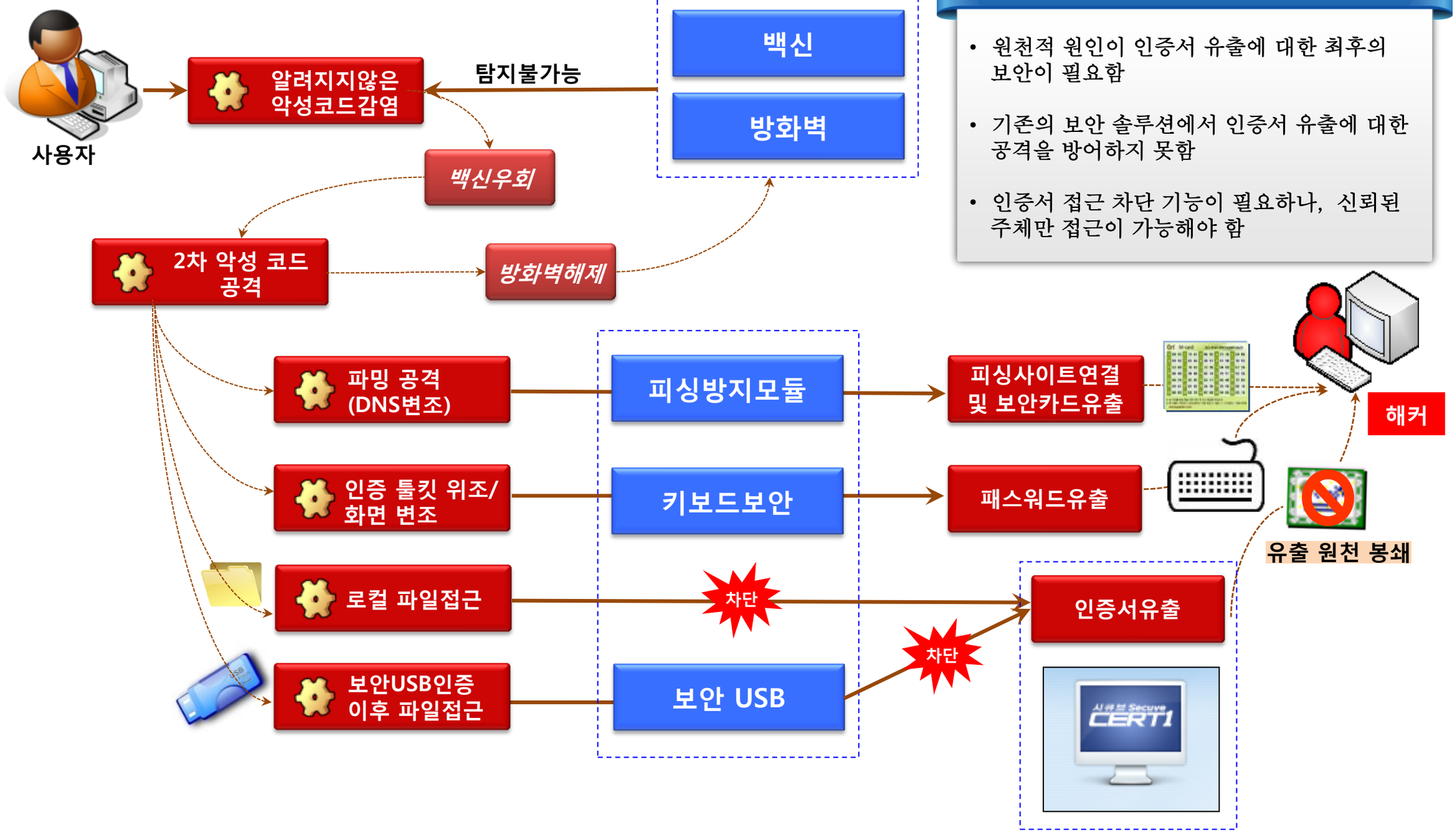


- PC해킹이나 비밀번호 관리 부주의로 인한 피해
- 파밍 등 해킹 기법에 대한 피해 사례 급증
- 변종 된 악성코드 유포를 통한 피해
- 스마트폰 등으로 해킹 확산

전자서명 관련 법규

구분	조	항	준수
전자서명법	제21조 (전자서명 생성정보의 관리)	① 가입자는 자신의 전자서명생성정보를 안전하게 보관·관리하고, 이를 분실·훼손 또는 도난·유출 되거나 훼손될 수 있는 위험을 인지한 때에는 그 사실을 공인인증기관에 통보하여야 한다. 이 경우 가입자는 지체 없이 이용자에게 공인인증기관에 통보한 내용을 고지하여야 한다.	O
	제22조 (인증업무에 관한 기록의 관리)	① 공인인증기관은 가입자의 공인인증서와 인증업무에 관한 기록을 안전하게 보관·관리하여야 한다.	O
	제23조 (전자서명 생성정보의 보호 등)	④ 누구든지 공인인증서를 이용범위 또는 용도에서 벗어나 부정하게 사용하여서는 아니된다.	O
		⑤ 누구든지 행사하게 할 목적으로 다른 사람에게 공인인증서를 양도 또는 대여하거나 행사할 목적으로 다른 사람의 공인인증서를 양도 또는 대여 받아서는 아니된다.	O
전자서명법 시행규칙	제13조의 4 (보호조치)	① 공인인증기관이 법 제18조의3의 규정에 의한 인증업무에 관한 시설의 안전성 확보를 위하여 하여야 할 보호조치는 다음 각호와 같다. 1. 전자적 침해행위로부터 보호조치 4. 그밖에 인증업무에 관한 시설의 안전성 확보를 위한 관리적 조치	O

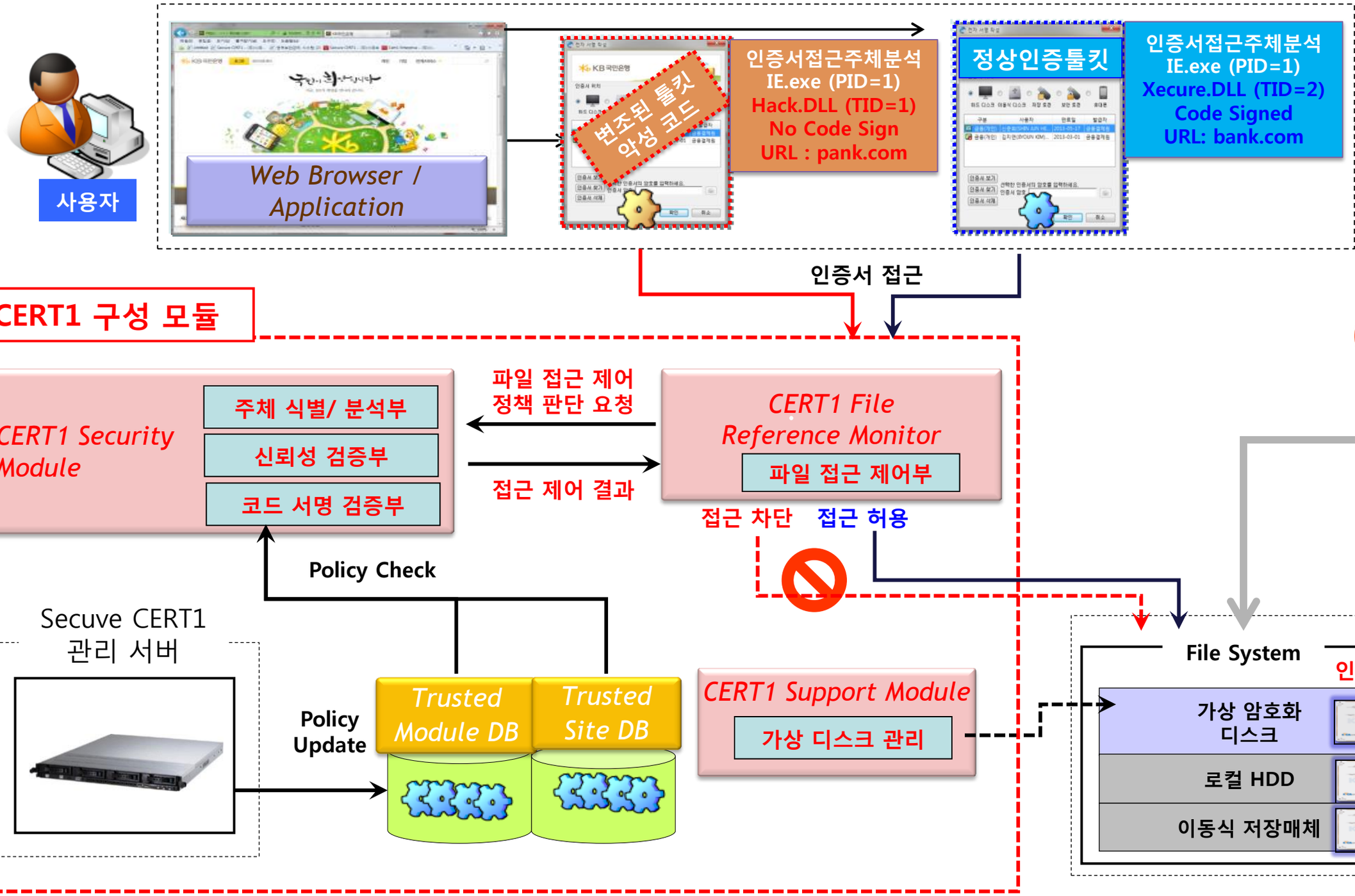
인증서 유출과정 분석 및 대응



요구되는 보안기능

- 원천적 원인이 인증서 유출에 대한 최후의 보안이 필요함
- 기존의 보안 솔루션에서 인증서 유출에 대한 공격을 방어하지 못함
- 인증서 접근 차단 기능이 필요하나, 신뢰된 주체만 접근이 가능해야 함

핵심기술


사용자
Web Browser / Application
변조된 툴킷
악성 코드
인증서접근주체분석
IE.exe (PID=1)
Hack.DLL (TID=1)
No Code Sign
URL : pank.com
정상인증툴킷
인증서접근주체분석
IE.exe (PID=1)
Xecure.DLL (TID=2)
Code Signed
URL: bank.com
인증서 접근
CERT1 구성 모듈
CERT1 Security Module
주체 식별/ 분석부
신뢰성 검증부
코드 서명 검증부
파일 접근 제어
정책 판단 요청
접근 제어 결과
CERT1 File Reference Monitor
파일 접근 제어부
접근 차단
접근 허용
Policy Check
Secuve CERT1
관리 서버
Policy Update
Trusted Module DB
Trusted Site DB
CERT1 Support Module
가상 디스크 관리
File System
인증서
가상 암호화 디스크
로컬 HDD
이동식 저장매체

제품군

Secuve CERT1

● 법인용 공인인증서

- 제품명 : Secuve CERT1 Enterprise
- 특징
  기업의 사업자 법인인증서를 중앙관리하며, 인증서의 사용 내역을 추적하여 기업 내 인증서 사용의 투명성 제공하고, 외부 반출/유출을 방지합니다.

Secuve CERT1 개인용(USB)

- 제품명 : Secuve CERT1 USB
- 특징
  개인의 USB에 저장된 공인인증서를 불법복제 및 유출 등 위협에서 강력히 보호하며, 안전한 공인인증서 사용 환경을 보장합니다.

CERT1 소개


administrator
관리자PC
파일서버
법인인증서
업로드
인증서
권한설정
인증서 사용
내역 조회
인증서관리자
시큐브 Secuve
CERT1
인증서사용
승인신청
인증서다운로드
허용정책
인증서사용
사용내역전송
CERT1 서버
가상디스크
가상디스크
인증서 사용자
차단
인증서 허용 정책
승인 사이트
허용 기간
12
저장매체
사용횟수
3..2...1...0
사용 장소
사내(내부망)
사외(외부망)
인증서 유출 / 오·남용
미 승인 사이트
인증서 오남용
악성 코드 및
위/변조 프로그램
인증서유출
내부직원
불법유출
퇴사자
불법유출

개인용 USB

CERT1 실행 / 인증서보호

인증서 보안 저장소

T:\

USB장착

시큐브 Secuve CERT1

허용

신뢰된 인증툴킷

차단

인증서 유출

악성코드 / 위변조 코드

Secuve CERT1 USB

사용자 PC

OTP생성

Secuve CERT1 OTP

Secuve CERT1 관리서버

Secuve CERT1 관리서버

- 신뢰 인증 모듈 정책 업데이트
- CERT1 프로그램 자동 업데이트
- CERT1 라이선스 검증
- CERT1 OTP 서버

주요기능

항목	구분	주요기능
인증서 보안 저장소 제공	공통	암호화된 공간인 인증서 보안 저장소(T Drive)에 인증서를 안전하게 관리 암호화 되어 있어 USB 분실 시에도 안전함 신뢰모듈의 인증서 접근 시, T 드라이브 동적 마운트 & 자동 언마운트 (최소노출)
인증서 사용 로그 제공	공통	공인인증서 사용에 대한 실시간 로그 제공 (접근 시간, 접근 사이트, 접근 모듈 등 상세한 로그 기록)
멀티브라우저 지원	공통	모든 종류의 인터넷 브라우저 (인터넷 익스플로러, 크롬, 파이어 폭스, 사파리)의 악성코드로부터 인증서 유출 방지
동작 환경 설정 및 자동 업데이트 제공	공통	사용자 알림 설정, 사용자 정의 정책 설정 기능 제공 시스템 부팅시 항상 자동 업데이트 기능이 수행되어 최신 버전으로 유지됨 (수동 업데이트 및 주기적 업데이트도 가능)
검증된 암호 모듈 사용	공통	자사 cGriffin 암호 모듈 (CC인증) 사용 가상 암호화 디스크 : SEED-256, 네트웍 암호 : SSL, 해시 : HMAC-SHA-256 데이터 완전 삭제 모듈 : Gutmann Method 기타 : 메모리 난독화, 코드 난독화, 자체 보호 사용

주요기능

항목	구분	주요기능
공인증서 암호 유출 방지 (인증 화면 도용 방지)	개인용 (USB)	악성코드가 정상 인증 툴킷 화면 위로 패스워드창을 겹쳐 사용자를 속이는 공격 방어 인증 화면 도용 방지를 통한 패스워드 유출 방지 [특허 출원]
파밍 / 스미싱 / 악성 코드 차단 (동적 모듈별 접근 통제 및 소프트웨어 코드 서명 정보 검증)	개인용 (USB)	동적 라이브러리 및 코드 사인 기반의 파일 접근 제어 [특허 등록] 동적 모듈별 접근 통제 가능 (브라우저 자체가 아닌 사용하는 Active X 수준까지 분석, JAVA 지원) 인가된 소프트웨어의 코드 서명값 검증을 통한 배포자 검증 및 무결성 확인 호스트 파일 위·변조 탐지 알림 (피싱 방지) 인가된 동적 모듈/프로그램의 해쉬값 검증 (본사에서 자동 모니터링 서비스를 통한 상시적인 신뢰 정책 관리)
Secuve CERT1 OTP 인증	개인용 (USB)	사용자 스마트폰을 이용하여 Secuve CERT1 OTP 앱을 통한 모바일 OTP 인증 패스워드 인증 이외의 이중 인증 수단 제공 (옵션)
법인인증서 중앙관리	기업법인용	법인인증서를 등록, 폐지, 허용 사이트 및 사용 권한에 대한 중앙 일괄 관리 1회용 패스워드 발급으로 원본 인증서 패스워드 보호
법인인증서 사용통제	기업법인용	법인인증서 사용 신청 및 승인 관리를 위한 결재프로세스 적용 허용정책(승인사이트, 허용기간, 저장매체, 사용횟수, 사용장소)에 의한 인증서 사용 통제
사용내역 감사 및 통계 정보 제공	기업법인용	사용자의 인증서 사용내역에 대한 관리자 감사 데이터 제공 인증서 사용에 대한 통계 및 인증서 신청 / 관리를 위한 통계 정보 제공
법인인증서 신청서 알림 기능	기업법인용	법인 인증서 사용 신청 및 승인에 관련되니 모든 결재 진행 과정을 이메일 / 팝업 을 통해 알림 제공