컴플라이언스 소개서

국가 핵심기술 보호를 위한 클라우드 보안 컴플라이언스 프레임워크

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

디지털 전환이 가속화됨에 따라 국가핵심기술을 보유한 공공기관들이 운영 효율성 향상을 위해 클라우드 도입을 확대하고 있습니다. 이러한 변화에 대응하여 산업통상자원부와 국가정보원은 2023년 국가핵심기술 클라우드 협의회를 설립하고, 보안 전문가, 산업계 관계자, 클라우드 서비스 제공업체(CSP)와의 다자간 협의를 통해 위험 기반 보안 프레임워크를 구축했습니다. 그 결과 2025년 4월 국가전략자산 보호를 위한 클라우드 보안관리지침이 공식 제정되었습니다.

국가핵심기술 클라우드 컴퓨팅 서비스 보안관리지침 개요

한국의 국가핵심기술을 다루는 클라우드 컴퓨팅 서비스 보안관리지침은 다음의 내용을 통해 한국의 국가핵심기술을 다루는 클라우드 컴퓨팅 서비스에 대한 보안 표준을 제시합니다:

- 클라우드 환경에서 민감한 산업 데이터 저장/처리를 위한 보안 통제 정의
- 클라우드 환경을 통한 기술 유출 방지
- 조직 및 연구기관의 안전한 클라우드 도입 보장

보안관리지침은 다음과 같은 3개 장으로 구성됩니다.

- **1장:** 국가핵심기술 클라우드 컴퓨팅 서비스 이용을 위한 보안관리 가이드의 전반적 개요
- **2장:** 국가핵심기술 조직과 클라우드 컴퓨팅 서비스 제공업체가 클라우드 컴퓨팅 서비스 환경에서 국가핵심기술 **관련 정보를 저장하고 처**리할 때 준수해야 하는 **보안관리 항목**
- **3장: 국**가핵심기술 보유 조직과 클라우드 컴퓨팅 서비스 제공업체가 클라우드 컴퓨팅 서비스에 저장된 국가핵심기술 관련 정보에 대한 **접근, 조회 및 이용 권한을 해외 기업에 허용**할 때 준수해야 하는 **보안관리 항목**

요구사항

- 국가핵심기술 보유기관이 클라우드 컴퓨팅 서비스를 이용하고자 할 경우 「산업기술보호법」, 「산업기술보호지침」 상 국가핵심기술의 보호조치를 준수하여야 함.
- 이 안내서의 내용과 관련 법규가 서로 일치하지 않는 경우에는 「산업기술보호법」, 「산업기술보호지침」에 규정된 내용이 안내서보다 우선임.
- 국가핵심기술 보유기관 및 클라우드 컴퓨팅 서비스 사업자는 「산업기술보호법」, 「산업기술보호지침」, 본 안내서 외 클라우드 컴퓨팅 서비스 관련 법령을 준수하여야 함.

적용 대상 및 범위

1. 국가핵심기술을 다루는 조직

- **해당 산업:**
  - 반도체 및 디스플레이
  - 이차전지 (예: 전기차 배터리)
  - 첨단소재, 생명공학, 항공우주
  - AI, 양자 기술 및 기타 국가전략기술 (산업기술 보호법 적용 대상)

2. 클라우드 서비스 제공업체 (CSP)

1) 국내 CSP: 네이버 클라우드, KT 클라우드, NHN 클라우드, 등.

2) 해외 CSP: AWS, Microsoft Azure, Google Cloud (한국 기업이 민감한 데이터 처리에 사용하는 경우).

3. 연구기관 및 대학: 정부 지원 R&D에 참여하는 기관 (예: KAIST, ETRI) 중 클라우드 인프라를 활용하는 기관

4. 정부기관 및 계약업체: 클라우드에 산업/국방 관련 데이터를 저장하는 공공부문 기관.

Thales의 지원 방법

Thales의 솔루션은 국가핵심기술 기관과 CSP가 클라우드 컴퓨팅 서비스 보안관리 가이드라인을 준수할 수 있도록 보안을 간소화하고 자동화하여 보안 및 컴플라이언스 팀의 부담을 경감시킵니다.

- **데이터 중심**
  - 데이터를 사용하는 애플리케이션, 데이터가 위치한 환경, 데이터가 통과하는 네트워크에 관계없이 기관의 가장 가치 있는 자산인 데이터 자체를 보호하는 데이터 중심 보안을 제공합니다.

- **높은 신뢰성**
  - 암호화 및 키 관리 시스템은 최고 수준의 가용성과 성능, 그리고 인증된 검증된 보안을 제공합니다. **HYOK(Hold Your Own Key)** 등의 키 관리는 암호화 키에 대한 강력한 직무 분리를 제공하며, 조직은 CSP에 키를 위탁하는 대신 자체적으로 키를 통제할 수 있습니다. HYOK를 통해 조직은 CSP와 클라우드 서비스의 모든 활동에 대한 명확하고 명시적인 책임 구분/경계 설정을 달성할 수 있습니다.

- HSM과 HSE를 사용한 **양자 내성 솔루션**을 채택하여 데이터를 "HNDL(Harvest Now, Decrypt Later)" 공격으로부터 보호함으로써 기관이 민감한 정보를 보호하고, 컴플라이언스를 보장하며, 양자 컴퓨팅 시대에서도 신뢰를 유지할 수 있습니다.

- **접근 관리**는 모든 접근 지점에서 접근 통제를 시행하여 확인된 관리자만 특권 계정에 접근할 수 있도록 하고, 덜 민감한 애플리케이션과 일반 사용자에게는 덜 엄격한 접근 통제를 시행해야 합니다.

지침	Thales 지원 방안	솔루션 영역
제 1 장		
1. 기본 원칙		
이용자 의무사항 클라우드 컴퓨팅 서비스 종료 또는 이전으로 인해 국가핵심기술 관련 정보를 처리해야 할 때, 제공업체에 모든 **관련 정보의 폐기**를 요청하고, 제공업체의 협조를 통해 폐기된 정보가 복구 불가능하게 삭제되었음을 확인해야 합니다.	• CipherTrust Manager에서 키 제거는 안전한 삭제를 보장하여 데이터의 모든 인스턴스를 디지털 방식으로 완전 소거	**데이터 보안** Cloud Key Manager Transparent Encryption
공통 의무사항 이용자는 클라우드 컴퓨팅 서비스와 **분리된 별도의 안전한 장소**에 저장·관리되는 **고유 키**를 활용하여 **데이터를 암호화하고 관리**해야 하며, 제공업체의 고유 키를 활용하여 데이터를 추가 암호화(이중 암호화)하여 저장해야 합니다. 제공업체는 이용자가 별도로 보유한 키를 활용하여 암호화된 데이터에 대해 추가 암호화(이중 암호화)를 수행할 수 있는 필요한 환경을 제공해야 합니다.	• 온프레미스, 클라우드 간, 빅데이터 또는 컨테이너 환경에서 저장 데이터 암호화. • 온프레미스 FIPS 140-2 Level 3 환경에서 암호화 키 보호 • 하이브리드, 단일 및 멀티 클라우드 환경 전반의 키 관리 중앙화 (키 검색, 네이티브 클라우드 키 관리, 자동 키 순환 포함) • 클라우드 제공업체의 암호화 키 요청 관리 및 Microsoft DKE, Google EKM, AWS XKS 등 다양한 신규 HYOK(Hold Your Own Key) 서비스 지원 • 클라우드 네이티브, BYOK 및 HYOK 키에 대한 지역별 단일 창 보기와 모든 클라우드 키 관리 서비스를 관리하는 단일의 직관적인 UI로 시간과 데이터를 모두 보호	**데이터 보안** Cloud Key Manager Hardware Security Modules(HSM) Transparent Encryption
2. 관리적보안		
정책		
공통 의무사항 이용자는 제공업체 또는 전문기관이 수행하는 클라우드 컴퓨팅 서비스 전반 운영 관리의 **보안 취약점 개선 결과**를 확인해야 하며, 제공업체는 전반 운영 관리에 대한 **보안 취약점 점검**을 정기적으로 실시하고 점검 결과 및 개선 사항을 이용자에게 제공해야 합니다.	• 데이터 저장소에 대한 평가 테스트를 실행하여 알려진 취약점을 스캔	**데이터 보안** Data Activity Monitoring

지침	Thales 지원 방안	솔루션 영역
3. 기술적 보안		
1) 데이터		
공통 의무사항 제공업체와 협의하여 **이용자**는 클라우드 컴퓨팅 서비스에 저장되거나 전송되는 국가핵심기술 관련 정보를 보호하기 위한 **암호화 대상, 암호화 강도(복잡성), 키 관리, 패스워드 사용**에 대한 정책을 수립·시행해야 합니다. 제공업체와 협의하여 **이용자**는 암호화 키의 생성, 사용, 저장, 배포, 폐기를 포함한 **암호화 키 관리 절차**를 수립해야 하며, 이용자의 암호화 키는 이용자가 통제할 수 있는 별도의 물리적으로 분리된 서버에 저장·백업되어야 하고, 이용자에게는 최소한의 접근 권한이 부여되어야 합니다.	• 온프레미스, 클라우드 간, 빅데이터 또는 컨테이너 환경에서 저장 데이터 암호화 • 데이터베이스의 민감한 정보를 가명화 • 온프레미스 FIPS 140-2 Level 3 환경에서 암호화 키 보호 • 클라우드 및 온프레미스 환경에서 키 라이프사이클 관리로 키 관리 간소화 • 직무 분리 원칙을 위해 암호화된 데이터와 암호화 키를 다른 장소에 저장 • 양자 컴퓨팅의 위협에 대응하기 위한 포스트 양자 민첩성 도입 • 역할과 컨텍스트를 기반으로 정책으로 내부 및 외부 사용자의 시스템과 데이터 접근 제한 • 위험 점수를 기반으로 상황별 보안 조치 적용 • 조건부 접근이 포함된 스마트 싱글 사인온으로 패스워드 피로 방지	**데이터 보안** Cloud Key Management Hardware Security Modules Tokenization Transparent Encryption **신원 및 접근 관리** Workforce Access Management Adaptive access
이용자 의무사항 **국가핵심기술 관련 정보**의 유형, 법적 요구사항, 민감도 및 중요도에 따라 정보를 분류하고 관리해야 합니다. 국가핵심기술 관련 정보의 소유권은 제공업체와의 계약 단계에서 명확히 규정되어야 합니다. 국가핵심기술 관련 정보의 **암호화 수준**에 대한 보안 요구사항을 도출하여 계약에 반영해야 하며, 생성된 국가핵심기술 관련 정보를 저장, 처리, 수신하기 위한 기술적 조치를 제공업체에 제공해야 합니다.	• 모든 데이터 저장소를 검색하고 분류하여 민감도와 가치를 기준으로 분류 • 파일 콘텐츠를 분류하여 보안 또는 개인정보보호 관점에서 조직에 어떤 의미를 갖는지 파악	**데이터 보안** Data Discovery & Classification

지침	Thales 지원 방안	솔루션 영역
2) 인증 및 권한 관리		
공통 의무사항 **이용자**는 클라우드 컴퓨팅 서비스와 **별도의 개별 인증 및 접근통제** 방법을 적용하고 안전하게 관리해야 하며, 정기적인 접근 기록 및 최소 권한 관리 검토를 포함해야 합니다. 제공업체는 필요한 모든 환경을 제공해야 합니다. **이용자**는 클라우드 컴퓨팅 서비스에 대해 OTP, 지문 등 **인증서(PKI) 기반의 다중 인증**을 사용해야 하며, 제공업체는 이러한 인증을 제공하기 위한 조치를 취해야 합니다. **접근 기록**의 범위를 정의하고, 사고 발생 시 서비스 통제·관리 및 책임 추적이 가능한 형태로 **저장**하여 유지해야 합니다(최소 1년간).	• 가장 광범위한 하드웨어 및 소프트웨어 방법으로 다중 인증(MFA) 활성화 • 데이터/애플리케이션의 민감도를 기반으로 적응형 인증 정책 구축 및 배포 • 피싱 및 중간자 공격으로부터 보호. • 단일 창에서 여러 하이브리드 환경에 대한 접근 정책 및 적용 중앙화 • 모든 시스템에 대한 모든 접근 이벤트의 감사 추적 및 보고서 생성, 외부 SIEM 시스템으로 로그 스트리밍	**신원 및 접근관리** Multi-Factor Authentication Risk-Based Authentication PKI and FIDO Authenticators
이용자 의무사항 클라우드 컴퓨팅 서비스에 대한 접근은 사용자 인증, 접근 주체별 권한 부여, 로그인 횟수 제한, 비정상 로그인 시도 경고 등을 포함한 **안전한 사용자 인증 절차**로 통제되어야 합니다.		
3) 네트워크 보안		
클라우드 컴퓨팅 서비스에서 국가핵심기술 관련 정보가 이동하는 구간에는 **암호화된 통신 채널**을 사용해야 합니다.	• 고속 암호화로 전송 중 데이터를 보호	**데이터 보안** High Speed Encryption
제 2 장		
1) 보안관리: 자원 - 데이터		
이용자 의무사항 외국 기업 등이 접근하는 장치에 국가핵심기술 관련 정보를 직접 저장하는 것을 제한해야 하며, 이에 대한 접근 권한을 부여받은 기타 인원도 마찬가지입니다. 국가핵심기술 관련 정보를 접근 장치에 직접 저장해야 하는 경우, 클라우드 컴퓨팅 서비스와 분리되어 이용자가 통제할 수 있는 별도의 안전한 장소에 저장·관리되는 고유 키를 사용하여 암호화된 형태로 저장해야 합니다.	• 온프레미스, 클라우드 간, 빅데이터 또는 컨테이너 환경에서 저장 데이터 암호화 • 클라우드 및 온프레미스 환경에서 키 관리 간소화 • FIPS 140-2 Level 3 환경에서 암호화 키 보호	**데이터 보안** Cloud Key Manager Hardware Security Modules Transparent Encryption
제공자 의무사항 이용자는 외국 기업 등에 의해 권한이 부여된 접근에 대해 다중 인증을 통한 강화된 인증 방법을 사용해야 합니다. 제공업체는 이를 위한 필요한 환경을 제공해야 합니다.	• 가장 광범위한 하드웨어 및 소프트웨어 방법과 폼 팩터로 다중 인증(MFA) 활성화 • 데이터/애플리케이션의 민감도를 기반으로 적응형 인증 정책 구축 및 배포 • 위험 점수를 기반으로 상황별 보안 조치 적용 • 조건부 접근이 포함된 스마트 싱글 사인온으로 패스워드 피로 방지	**신원 및 접근관리** Multi-Factor Authentication Risk-based authentication PKI and FIDO Authenticators

지침	Thales 지원 방안	솔루션 영역
2) 보안관리: 네트워크		
이용자 의무사항 외국 기업 등에 접근 권한을 허용하는 기간 동안 비상적인 계정, 접근, 또는 로그(부여, 열람, 사용 등) 등의 행위에 대한 실시간 모니터링을 수행해야 하며, 이상 징후가 발견되면 조치를 취해야 합니다.	• API 활동 모니터링, 사용량 추적, 이상 징후 탐지, 잠재적 무단 접근 시도 식별 • 데이터베이스 공격 및 비정상적 접근 요청을 실시간으로 경고하거나 차단 • 시간 경과에 따른 파일 활동을 모니터링하여 금융기관을 위험에 빠뜨릴 수 있는 활동에 대한 경고 설정 • 비정상적인 I/O 활동에 대한 프로세스를 지속적으로 모니터링하고 악의적 활동을 경고하거나 차단	**애플리케이션 보안** API Security **데이터 보안** Data Activity Monitoring Transparent Encryption Ransomware Protection

애플리케이션 보안, 데이터 보안, 신원 및 접근 관리 : Thales는 사이버보안의 세 가지 핵심 영역에서 포괄적인 사이버보안 솔루션을 제공합니다.

애플리케이션 보안: 클라우드, 온프레미스 또는 하이브리드 모델에서 대규모로 애플리케이션과 API를 보호합니다. 당사의 시장 선도 제품군에는 분산 서비스 거부(DDoS) 및 악성 봇 공격에 대한 웹 애플리케이션 방화벽(WAF) 보호, API 보안 및 보안 콘텐츠 전송 네트워크(CDN)가 포함됩니다.

데이터 보안: 하이브리드 IT 전반에서 민감한 데이터를 검색하고 분류하며, 암호화, 토큰화 및 키 관리를 사용하여 저장, 전송 또는 사용 중인 데이터를 어디서든 자동으로 보호합니다. Thales 솔루션은 또한 정확한 위험 평가를 위해 잠재적 위험을 식별, 평가 및 우선순위를 매깁니다. 또한 이상 행동을 식별하고 활동을 모니터링하여 잠재적 위협을 식별하고 컴플라이언스를 확인함으로써 조직이 노력을 집중할 곳의 우선순위를 정할 수 있도록 지원합니다.

신원 및 접근 관리: 고객, 직원 및 파트너를 위한 애플리케이션 및 디지털 서비스에 대한 원활하고 안전하며 신뢰할 수 있는 접근을 제공합니다. 당사의 솔루션은 적절한 사용자가 적절한 시점에 적절한 리소스에 대한 접근 권한을 부여받도록 보장하는 세분화된 접근 정책과 다중 인증을 통해 역할과 컨텍스트를 기반으로 내부 및 외부 사용자의 접근을 제한합니다.

기업 및 조직은 단일 통합 플랫폼에서 제공되는 Thales의 신원 및 접근제어, 애플리케이션 및 데이터 보안 솔루션 제품군을 활용하여 규정을 준수하고 향후에도 지속적으로 규정 준수를 유지할 수 있습니다. 지금 바로 문의하십시오!

Thales 소개

Thales는 데이터 보안 분야의 글로벌 리더로, 전 세계 정부와 가장 유명한 기업들이 가장 민감한 데이터를 보호하는 데 신뢰하고 있습니다. 개인정보 보호를 위해 의존하는 사람들이 자신들의 데이터를 보호하기 위해 Thales에 의존합니다. 데이터 보안과 관련하여 조직들은 점점 더 많은 결정적 순간에 직면하고 있습니다. 암호화 전략 구축, 클라우드로의 이전, 컴플라이언스 요구사항 충족 등 어떤 순간이든 디지털 전환을 보호하기 위해 Thales에 의존할 수 있습니다.

법적 고지사항: 본 문서에 포함된 정보는 발행일 현재 기준으로 작성되었습니다. Thales는 본 자료를 정보 제공 목적으로만 제공하며, 그 내용은 법적 자문에 해당하지 않고 관련 법률의 준수 여부에 대한 보증이나 보장을 의미하지 않습니다. 관련 법률의 해석에 대해서는 각 당사자가 전적으로 책임을 집니다. 본 정보는 특정 업그레이드, 기능 또는 성능의 제공을 보장하는 것으로 해석되어서는 안 됩니다. 제품 구매 결정 시 본 자료에 기술된 예상 일정이나 잠재적 업그레이드, 기능 또는 성능에 의존해서는 안 됩니다. Thales는 본 자료의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임을 지지 않습니다.

cpl.thalesgroup.com

연락처 - 모든 사무소 위치 및 연락처 정보는 cpl.thalesgroup.com/ko/contact-us를 방문하시기 바랍니다.

© Thales - July 2025•GHv7