J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

국방 상용보안제품 도입을 위한 CSfC(Commercial Solutions for Classified Program) 네트워크 보안 아키텍처 분석☆

CSfC Network Security Architecture Analysis for the Assurance of Commercial Security Solutions in Defense Area

이 용 준[1] 박 세 준[2*] 박 연 출[3]
Yong-joon Lee Se-joon Park Yeon-chool Park

요 약

미국은 CSfC(Commercial Solutions for Classified Program) 제도를 통해 진화하는 사이버공격에 대응하기 위해 국가기관이 민간 상용보안제품을 신속히 국가관에 도입할 수 있도록 공인된 안전성 평가 및 인증을 수행하고 있다. CSfC 프로세스에 등록된 상용보안제품은 신속한 승인 프로세스를 거쳐 국방기관에서 사용할 수 있으며 중복된 평가 없이 상용보안제품을 승인한다. 승인된 보안제품은 국방정보시스템 구현에 필요한 시간, 비용, 승인 프로세스로 인한 비용을 절감할 수 있다.

본 연구는 국방에 도입하기 위해 미국 NSA(National Security Agency)에서 제시한 네트워크 보안 아키텍처 MSC(Multi-Site Connectivity), MA(Mobile Access), Campus WLAN, DAR(Data at Rest) 4종에 대한 보안통제 항목을 분석하였다.

☞ 주제어 : CSfC, 다중 망연계, 원격지 접속, 무선 인터넷망, 내부자료 암호화

ABSTRACT

The United States is responding to evolving cyberattacks through the Commercial Solutions for Classified Program (CSfC). Authorized safety evaluation and certification are being carried out so that US government agencies can quickly introduce civilian commercial security products into the national pavilion. Commercial security products registered in the CSfC process can be used by defense agencies through a rapid approval process. Defense agencies approve commercial security products without duplicate evaluation. Approved security products can reduce the time, cost, and cost of the approval process required to implement the defense information system.

In this study, security control for 4 types of network security architecture MSC (Multi-Site Connectivity), MA (Mobile Access), Campus WLAN, and DAR (Data at Rest) proposed by the US National Security Agency (NSA) for introduction to national defense A detailed analysis was performed on the items.

☞ keyword : CSfC(Commercial Solutions for Classified Program), MSC(Multi-Site Connectivity), MA(Mobile Access), Campus WLAN, DAR(Data at Rest)

1. 서 론

세계 각국은 진화하는 사이버공격으로 부터 국가기관의 주요 자산을 보호할 수 있도록 보안제품을 보증하는 제도를 운영하고 있다. 특히 미국은 CSfC(Commercial Solutions for Classified Program) 제도를 통해 급속히 진화하는 사이버공격에 대응하기 위해 국가기관의 주도하에 민간 상용보안제품을 신속히 국가관에 도입할 수 있도록 공인된 안전성 평가 및 인증을 수행하고 있다.

미국의 CSfC 제도는 국가정보시스템에 대한 보안 설계 및 구현 인증 제도로 국가기관에서 상용보안제품을 도입시 평가, 테스트 절차를 거쳐 시스템을 인증하는 데 장시간

1. Far East University, Eumseong-gun, Chungbuk, (27601), Korea.
2. Information Security Group, SK, Seong-Nam City, Gyeonggi-do, (10077), Korea.
3. Advanced Robotics LAB, LG, Seoul, (06763), Korea.
* Corresponding author (sjoon0912@naver.com)
[Received 13 October 2021, Reviewed 20 October 2021(R2 8 November 2021), Accepted 10 November 2021]
☆ This work is the result of commissioned research project supported by the affiliated institute of ETRI[2021-121]. When giving a presentation on this work, the presenter has to clarify that it is the result of the research commissioned by the affiliated institute of ETRI

소요되는 문제를 해결하고 적시적에 도입을 목적으로 제정하였다.

CSfC 프로세스에 등록된 상용보안제품은 신속히 승인 프로세스를 거칠 수 있다. CSfC 프로그램에서는 상용보안제품을 국방기관에 선택하여 사용할 수 있으며 테스트 및 반복적인 평가 없이도 상용보안제품을 승인한다. 승인된 보안제품은 시스템 구현에 필요한 시간, 비용, 승인 절차로 인한 비용을 절감할 수 있다.

본 연구는 미국 NSA(National Security Agency)에서 제시한 네트워크 보안 아키텍처 MSC(Multi-Site Connectivity), MA(Mobile Access), Campus WLAN, DAR(Data at Rest) 4종에서 제시한 보안통제 항목에 대해 상세 분석을 하였다.

국방분야 상용보안제품을 신속하고 보증된 절차를 개선할 수 있는 기초자료로 활용할 수 있다.

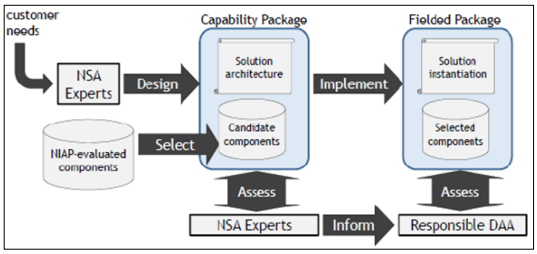
2. 관련 연구

2.1 미국 CSfC 상용보안제품 보증 절차

미국은 국가정보시스템을 보호하고 중요한 데이터를 보호하기 위해 국가 주도로 설계·인증한 보안제품을 우선시하였다. GOTS(Government-Off-The-Shelf) 국가보안제품은 네트워크 보안 아키텍처에서 채택할 때 고수준의 제어 및 보증을 제공한다. GOTS는 장시간에 보안평가와 엄격한 설계 및 구현 프로세스를 거치기 때문에 강화된 보안을 제공한다. 그러나 GOTS 보안제품은 변화하는 환경 및 상호 운용성에 유연하지 않기 때문에 국가정보시스템의 수명주기 비용과 함께 개발기간도 증가한다. 엄격한 개발 및 승인 프로세스로 인해 새로운 보안기술을 도입하는데 수개월에서 수년까지 지연된다. 결과적으로 GOTS 보안제품은 최첨단 기술을 사용하기 어렵다. 반면에, 상용보안제품 COTS (Commercial-Off-The-Shelf)는 국가정보시스템의 보안 및 유연성 요구에 적합한 최신 보안기술을 제공한다. COTS는 제품 출시가 신속하여 시스템의 개발도 신속이 구축할 수 있다. COST는 신속한 개발이 가능하여 수명주기 비용이 GOTS 보안제품에 대비하여 낮다. 상용보안제품은 GOTS보안제품에서 구현하기 어려운 다양한 보안기능을 포함할 수 있는 장점이 있다. 국가정보시스템에 COTS을 선택하는데 중요한 어려움은 상용보안제품에 대한 국가의 통제력이 상실된다는 점이다[1].

국가기관은 상용보안제품의 품질, 안정성, 유연성을 알 수 없으면 보안제품의 보안 및 보증 수준을 확인할 수 없다. 이에 미국의 CSfC 프로그램은 상용보안제품에 대한 신속하면서도 포괄적 승인, 책임, 구현 절차를 도입하여 국가정보시스템이 보안과 안정성을 확보하면서 상용보안제품으로 구축할 수 있다. CSfC 프로세스에 등록된 보안제품은 신속한 승인 절차가 가능하다. 1년에서부터 10년까지 소요될 수 있는 GOTS 절차와 대비하여 CSfC는 국가정보시스템에 상용보안제품을 도입하는데 단기간 소요된다. CSfC 프로그램에서는 테스트를 통해 중복된 평가 없이 상용보안제품을 승인이 가능하다. 결과적으로 승인된 상용보안제품은 국가정보시스템 구축에 필요한 시간, 비용, 승인 절차로 인한 비용을 절감하게 된다.

(그림 1)과 같이 NSA의 CSfC는 4종의 네트워크 보안 아키텍처를 제시하고 승인된 상용보안제품 목록을 공개한다. 상용보안제품은 국제적으로 표준화된 암호 및 통신 프로토콜을 준용하기 때문에 국가기관이 요구하는 암호 기능에 부합한다. 결과적으로 규제 부담이 적으면서도 상호 운용성도 향상된다. CSfC 프로그램은 국가기관이 요구하는 보안제품에 대한 강화된 보증을 제공하며 신속하게 국가정보시스템을 구축하도록 한다. CSfC 등록 보안제품은 상세한 보안통제 항목을 충족하기 때문에 국가정보시스템을 보증된지 않은 보안제품의 도입을 방지한다. CSfC 핵심 목표는 민간의 SI(System Integration)기업과 정보보안기업을 통해 국가기관의 시스템 보안을 강화하며 구축 비용 절감하는 것이다. CSfC 등록 보안제품은 보안 대응성을 향상시키면서도 신속하게 도입 기관의 요구를 정확하고 경제적으로 충족할 수 있도록 제도화하였다[2].



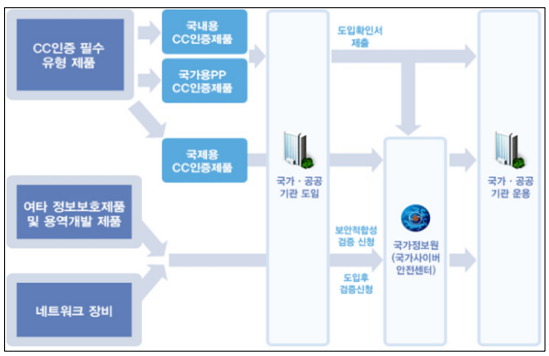
(그림 1) 미국 CSfC 상용보안제품 보증 절차
(Figure 1) US CSfC's Commercial Security Product Assurance Procedure

2.2 한국 보안적합성 상용보안제품 보증 절차

한국은 상용보안제품에 대한 국제적 신뢰성 확보, 국가통신망 정보보호수준 제고와 정보보호제품 경쟁력 강화를 위해 상용보안제품에 대한 평가·인증 제도를 시행하고 있다. 정보보호제품 평가 인증제도는 상용보안제품에 구현된

보안기능의 안전성과 신뢰성을 보증하여 국가기관이 안심하고 이용할 수 있도록 지원하는 제도로 국가정보화기본법 제38조(정보보호시스템에 관한 기준 고시등) 및 시행령 제35조(정보보호시스템의 보완)에 근거하고 있다. 현재 한국의 정보보호제품 도입제도는 정보보호제품 평가, 인증제도(CC 평가인증), 암호모듈 검증 제도, 보안적합성 검증제도를 시행 중에 있다. 특히, 2005년 공통평가기준(CC, Common Criteria) 인증 획득 제품에 대해 CC 인증범위 이외 보안 및 암호기능에 대해 보안성 검토를 실시했다. 이후 2006년 정보보호제품에 대한 보안성 검토를 보안적합성 검증으로 명칭을 변경했고, 2008년 보안적합성 검증제도에서 CC인증제품의 검증절차를 선검증 후도입에서 선도입 후검증으로 전환했다.

보안적합성 검증은 국가 통신망의 보안 수준을 제고하고 외부의 사이버 위협에 대응하기 위해 만들어진 제도이다. (그림 2)와 같이 전자정부법에 기반해 국가·공공기관에서 도입하는 IT 제품의 보안기능에 대해 안정성을 검증한다. 보안기능이 포함된 IT 제품을 도입할 경우 국가, 공공기관은 보안적합성을 검증한 후, 이 과정에서 발견된 취약점을 제거한 다음 운영해야 한다.



(그림 2) 한국 보안적합성 상용보안제품 보증 절차
(Figure 2) Korea Security Conformity's Commercial Security Product Assurance Procedure

2.3 미국, 한국 국가시스템 상용보안제품 보증 비교

미국 NSA가 담당하는 CSfC 제도와 비교하여 한국은 국정원 보안적합성과 유사한 제도이며 공통점은 국가기관이 구축하는 정보시스템의 보안·암호에 대해서 CC인증된 상용보안제품을 채택하고 암호는 KCMVP 인증 여부를 검토하여 개선사항 등을 제시한다. 차이점은 NSA CP (Capability Package)는 국가기관에서 비밀정보 공유에 필요한 상세한 네트워크 보안 아키텍처 4종을 제시하여 보안통제 항목의 준수 여부를 체크하는 방식으로 신속한 평가가 가능하다. 한국의 보안적합성은 표준화된 네트워크 보안 아키텍처를 제시하지 않고 CC인증제품, KCMVP 인증제품을 확인하며 해당 제품이외에 보안기능에 대해 보안성을 평가하는 방식으로 평가기간에 상당한 시간이 소요된다.

(표 1)과 같이, 한국 국방에서 실시하는 보안측정과 CSfC를 비교하면 공통점은 국방정보체계의 보안·암호에 대해서 CC인증제품 채택, KCMVP 인증 여부를 시스템 도입, 운영 중에 검토하여 개선사항을 제시한다. 차이점은 국방부 보안측정도 표준화된 네트워크 보안 아키텍처를 제시하지 않기 때문에 국방기관의 표준화되지 않은 국방정보체계에 대해 검토를 실시한다. 이로 인해 보안측정에 시간이 소요된다.

(표 1) CSfC, 보안적합성, 보안측정 비교 분석
(Table 1) Comparative analysis of CSfC, Security Conformity, and Security Measurement

구분	미국	한국	
	CSfC	보안적합성	보안측정
평가기관	NSA	국정원	군사안보지원사
평가시기	구축, 운영, 개선	구축, 개선	구축, 운영, 개선
소요기간	1~2개월	3개월	3개월
평가방식	• NSA가 제시한 네트워크 보안 아키텍처의 보안통제 수용 여부 확인 • CSfC 등록 상용보안제품 여부 확인 • 현장실사	• 국가기관이 제출한 시스템 구성도, 네트워크 등 산출물 보안성 검토 • 정보보안제품, 암호모듈 제품 검토 • 현장실사	• 군기관이 제출한 국방정보체계 구성도, 네트워크 등 구축 산출물 보안성 검토 • 정보보안제품, 암호모듈 제품 검토 • 현장실사
상용보안제품보증	• CC인증 후 CSfC 등록된 상용보안제품 도입	• CC인증 상용보안제품 도입 • PP가 없는 보안제품은 보안적합성 검토 및 시험을 통해 도입	• CC인증 상용보안제품 도입 • PP가 없는 보안제품은 취약점 시험을 통해 도입
암호모듈보증	• CMVP 인증 암호모듈 도입	• KCMVP 인증 암호모듈 도입	• KCMVP 인증 암호모듈 도입

현재 국방정보체계에 대한 표준화된 보안기능은 국방정보기술 아키텍처에 따르고 있으며 NSA에서 제시한 4종의 CP와 유사한 보안통제항목을 근거로 하고 있다. 다만 NSA는 표준화된 네트워크 보안 아키텍처와 승인된 상용보안제품을 게시하고 있으나 현재 한국의 국방 아키텍처는 단위 아키텍처에 대한 보안기능에 대한 이력관리를 하고 있다. 추가적으로 국방분야 암호모듈 적용에 있어 군사안보

지원사는 국방-CMVP 평가를 준비하고 있으나 현재 시행은 되지 않아 국가기관에서 인증된 KCMVP 모듈을 사용하도록 하고 있다.

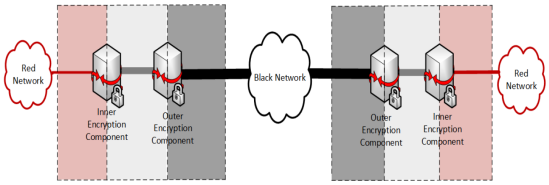
3. CSfC 네트워크 보안 아키텍처 현황

3.1 MSC(Multi-Site Connectivity)

MSC 네트워크 보안 아키텍처는 공개된 네트워크 또는 다른 보안 수준의 네트워크를 통해 전송할 때 기밀정보 보호를 목적으로 제안되었다. MSC 솔루션은 암호화 터널을 통해 동일한 보안 수준에서 두 개 이상의 네트워크를 상호 연결하는 것을 지원한다. MSC 네트워크 보안 아키텍처는 다양한 네트워크 유형에 적용할 수 있도록 확장성을 제공한다[1].

MSC 솔루션은 두 개의 독립된 암호화 터널을 사용하여 공개된 네트워크를 전송할 때 데이터의 기밀성과 무결성을 보호한다. 데이터를 보호하기 위한 암호화 터널방식인 VPN(Virtual Private Network)은 게이트웨이에서 생성된 IPsec(Internet Protocol Security) 또는 MACsec(Media Access Control Security) 사용할 수 있다. MSC 네트워크 보안 아키텍처의 암호화 구성은 VPN 게이트웨이 또는 MACsec 장치이며 내부 암호화 계층과 외부 외부 암호화 계층으로 구분한다.

(그림 3)에서 MSC 네트워크 보안 아키텍처는 비밀 데이터가 공개 네트워크를 통해 전송하기 전에 내부 암호화 구성요소와 외부 암호화 구성요소에 통해 2회 암호화된다. 반대로 수신된 통신 데이터는 외부 암호화 구성요소와 내부 암호화 구성요소에 의해 2회 복호화 된다.

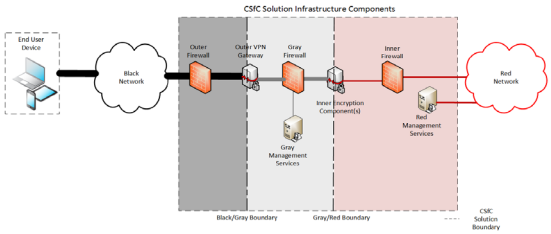


(그림 3) MSC 네트워크 보안 아키텍처
(Figure 3) MSC Network Security Architecture

3.2 MA(Mobile Access)

(그림 4)와 같이, MA 네트워크 보안 아키텍처는 신뢰할 수 없는 네트워크 또는 다양한 네트워크를 통해 전송되는 기밀정보를 보호하기 위한 MA 솔루션을 제시한다. MA 솔루션은 최종 사용자 단말기 EUD(End User Device)가 공개망에서 동일한 보안등급에서 통신할 수 있도록 EUD에서 이중화 암호화를 통해 내부망에 연결한다[2].

MA 솔루션은 인터넷 프로토콜 보안을 사용하는데 외부망에서는 IPsec을 사용하고 내부망에서는 IPsec 또는 TLS (Transport Layer Security)을 사용한다. MA 네트워크 보안 아키텍처에서 내부 암호화 구성요소는 VPN 또는 EUD의 TLS로 구성된다. VPN 구성요소는 VPN 게이트웨이와 VPN 클라이언트로 정의하고 TLS 구성요소는 TLS 서버 또는 SRTP(Secure Real-Transport Protocol)와 EUD(TLS Client, SRTP Client) 간에 TLS를 구축한다.

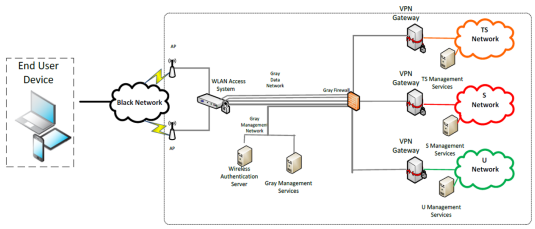


(그림 4) MA 네트워크 보안 아키텍처
(Figure 4) MA Network Security Architecture

3.3 Campus WLAN(Wireless Local Area Network)

(그림 5)은 Campus WLAN 네트워크 보안 아키텍처를 보여준다. Campus WLAN 네트워크 보안 아키텍처는 무선 장치를 통해 기존 엔터프라이즈 네트워크에 연결할 때의 위험을 최소하기 위한 목적이다. 국가기관에서 무선 네트워크는 모바일 사용자와 국가정보시스템에 대한 통제된 연결을 제공해야 한다. Campus 용어는 다양한 무선환경으로 국가정보시스템에 접속할 수 있는 영역으로 정의한다. Campus WLAN 솔루션은 무선 네트워크를 통신할 때 데이터의 기밀성과 무결성을 보호하기 위해 AES 256을 사용하는 IPsec과 WPA3(Wi-Fi Protected Access3)으로 이중 암호화 계층을 사용한다. 데이터 흐름을 보호하는 두 계층은 VPN Client와 EUD에서 WLAN Client에 의해 연결한다[3].

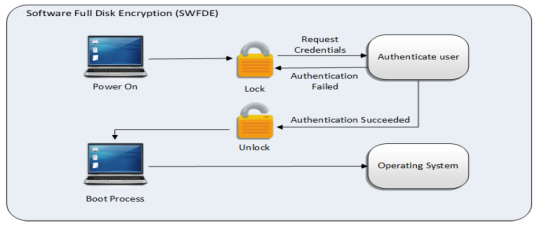
Campus WLAN 솔루션은 두 계층의 IPsec 암호화를 사용하는 Campus WLAN을 구축하면 도입하는 국가기관은 Mobile Access 네트워크 보안 아키텍처를 준수하여 등록할 수 있다. Campus WLAN 솔루션은 CSfC 구성요소 목록의 제품을 사용하여 구성, 계층화, 구축된다. 도입기관과 SI 기업은 Campus WLAN CP에서 선택된 구성요소를 보장하기 위해 상호운용성 테스트를 수행하여 최종적으로 기밀정보 통신의 안전성을 보증한다.



(그림 5) Campus WLAN 네트워크 보안 아키텍처
(Figure 5) Campus WLAN Network Security Architecture

3.4 DAR(Data at Rest)

(그림 6)은 DAR 네트워크 보안 아키텍처에서 EUD에서 DAR 보호의 두 계층을 포함하는 솔루션으로 정의한다. DAR 솔루션의 목표는 EUD 전원이 꺼지거나 인증되지 않은 요청으로 부터 기밀 데이터를 보호하는 것이다. 비밀정보를 요청하는 사용자에게 DAR 솔루션의 두 계층에서 인증정보(암호, 토큰)를 제시하여 검증하도록 한다. DAR 솔루션은 외부•내부 계층인 이중 암호화 계층으로 구성된다. 외부 계층은 첫 번째 단계에서 인증되며 내부 계층은 두 번째 단계로 인증된다. 데이터 소유자는 보호되어야 하는 비밀정보에 대한 권한을 설정할 수 있다[4].



(그림 6) DAR 네트워크 보안 아키텍처
(Figure 6) DAR Network Security Architecture

4. CSfC 네트워크 보안 아키텍처 보안통제 항목 분석

4.1 CSfC 네트워크 보안 아키텍처 특징분석

(표 2)와 같이, 미국 NSA에서 제시한 4종의 네트워크 보안 아키텍처는 국가기관에 필요한 MSC(Multi-Site Connectivity) 460개 보안통제항목, MA(Mobile Access), 473개 보안통제항목, Campus WLAN, 415개 보안통제항목 DAR(Data at Rest) 151개 보안통제항목을 제시하였으며 개별 네트워크 보안 아키텍처에는 구축 가능한 다양한 유형의 모델을 제시하고 있다. 국방기관은 구축할 네트워크 보안 아키텍처를 선택하고 보안과 보증에 필요한 상세한 보안통제항목을 준수여부를 확인하여 보증절차를 신속히 완료할 수 있다.

(표 2) NSA CSfC 네트워크 보안 아키텍처 특징
(Table 2) NSA CSfC Network Security Architecture Features

아키텍처	버전	네트워크 유형	보안통제
MSC	Ver 1.1.8 (2021.5)	다중 망연계 (국가기관 상호간의 원격통신에 이중 암호화)	460개
MA	Ver 2.1 (2021.6)	원격지 접속 (단말기를 통해 국가기관망에 원격 접속시 이중 암호화)	473개
Campus WLAN	Ver 2.2 (2021.6)	무선 인터넷망 (국가기관 업무환경에서 무선 인터넷망을 통한 국가기간망 접속시 암호화)	415개
DAR	Ver 5.0 (2020.11)	내부자료 암호화 (국가기관 정보시스템 내부의 정보 암호화)	151개

4.2 CSfC 네트워크 보안 아키텍처의 보안통제 항목 분석

(표 3)과 같이 4종의 네트워크 보안 아키텍처의 평균 보안통제항목은 375개 요구사항을 제시하고 있으며 전체적으로 보안통제항목의 순위는 MA(473개), MSC(460개), Campus WLAN(415개), DAR(151개) 순이다.

4종의 CSfC 네트워크 보안 아키텍처의 보안통제항목을 분야별로 분석하면 DAR 경우는 내부 데이터에 대한 S/W, H/W를 통한 이중 암호만을 담당하기 때문에 보안관제, 보안담당자 역할별 통제항목이 없기 때문에 요구사항이 적다. 보안제품 기능이 핵심기능으로 분류가 되는데 Campus WLAN(175개), MA(171개), DAR(80개), MSC(47)개 순으로 차이가 있다. Campus WLAN은 다양한 무선환경에 대한 보안기능을 포함하고 있으며 MA도 무선환경에서 TLS 중계기에 대한 다양한 보안기능이 요구되기 때문에 보안제품 기능이 상세하게 필요하다. MSC 보안 네트워크 아키텍처는 유선환경만 제공하기 때문에 보안제품 기능이 상대적으로 적다.

(표 3) CSfC 네트워크 보안 아키텍처의 보안통제 항목
(Table 3) CSfC Security Control Items of Network Security Architecture

구분		MSC	MA	Campus WLAN	DAR
버전		V1.1.8	V2.1	V2.2	V5.0
발표일		2021.5	2018.6	2018.7	2020.11
보안통제 분류	보안제품 선정	37	42	22	18
	운영관리	85	71	56	28
	시험	1	1	1	1
	키관리	88	88	88	7
	보안관제	191	89	62	17
	역할	11	11	11	-
	보안제품 기능	47	171	175	80
	총계	460	473	415	151

4.3 CSfC 네트워크 보안 아키텍처 상용보안제품 선정 분석

4종의 CSfC 네트워크 보안 아키텍처 분석을 통해서 선택 가능한 상용보안제품은 총 10종(VPN, MACsec, TLS, WPA3, 인증(IA/AA), 암호(SW/HW), FW, IDS, IPS, SEIM)을 채택할 수 있는 것으로 분석되었다. VPN, MACsec, TLS, [5]-[8].

(표 4)와 같이, 4종의 네트워크 보안 아키텍처는 VPN, MACsec, TLS, WPA3, 암호(SW, HW) 상용보안제품은 이중 암호화를 위해 사용되며, 인증(IA/AA) 상용보안제품은 사용자 인증을 위한 목적이며 FW, IDS, IPS, SIEM은 보안관제를 위해 채택한다. 암호통신을 위해 기본적으로 PKI 인증을 위한 CA(Certification Authority) 보안제품을 사용해야 하는데 기존에 국가기관이 도입한 기업형(Enterprise) CA 사용하도록 하여 상용보안제품 10종에는 추가하지 않았다[9]-[11].

(표 4) CSfC 네트워크 보안 아키텍처의 상용보안제품(10종)
(Table 4) CSfC Commercial Security Solutions(10) of Network Security Architecture

CP	상용보안제품(10종)									
	VPN	MACsec	TLS	WPA3	암호(SW/HW)	인증(IA/AA)	FW	IDS	IPS	SEIM
MSC	○	○					○	○	○	○
MA	○		○				○	○	○	○
Campus WLAN				○		○	○	○	○	○
DAR					○					

5. 결 론

본 연구는 미국의 NSA에서 주관하는 CSfC 제도의 분석을 통해 미국 연방정부, 연방기관, 국가 주요기반시설 운영기관에 신뢰성이 있고 안정성이 보장된 상용 정보보호제품을 도입하기위한 절차, 기준 및 요구사항에 대해 분석하였다.

주요 연구내용으로는 미국은 CSfC(Commercial Solutions for Classified Program) 제도를 마련하여 급속히 빨라지고 다양해지는 사이버공격에 대응하기 위해 국가기관의 주도로 민간 상용보안제품을 신속히 국가관에 도입할 수 있도록 공인된 안전성 평가 및 인증을 수행하고 있다.

미국의 CSfC 제도는 국가보안시스템에 대한 보안 설계 및 구현 인증 제도로 국가기관에서 상용보안제품을 도입시 평가, 테스트 절차를 거쳐 시스템을 인증하는 데 장시간 소요되는 문제를 해결하고 적시적으로 도입을 목적으로 제정하였다.

본 연구는 국방분야 민간 상용보안제품 도입을 위해 미국 NSA(National Security Agency)에서 제시한 네트워크 보안 아키텍처 MSC(Multi-Site Connectivity), MA(Mobile Access), Campus WLAN, DAR(Data at Rest) 4종에 대한 보안통제 항목에 대해 상세 분석을 하였다.

CSfC 프로세스에 등록된 상용보안제품은 신속한 승인 프로세스를 거칠 수 있다. CSfC 프로그램에서는 상용보안제품을 국방기관에 선택하여 사용할 수 있으며 테스트를 통해 중복된 평가 없이 상용보안제품을 승인한다. 승인된 보안제품은 국방정보체계 구축에 필요한 시간, 비용, 승인 절차로 인한 비용을 절감할 수 있다.

국방분야 상용보안제품을 신속하고 보증된 절차를 개선할 수 있는 기초자료로 활용할 수 있다.

참고문헌(Reference)

[1] NSA, MSC(Multi-Site Connectivity) Capability Package Ver 1.1.8, 2021.5.

[2] NSA, MA(Mobile Access) Capability Package Ver 2.1, 2021.6.

[3] NSA, Campus WLAN(Wireless Local Area Network) Capability Package Ver 2.2, 2021.6.

[4] NSA, DAR(Data at Rest) Capability Package Ver 5.0, 2020.11.

[5] collaborative Protection Profile for Network Devices, Version: 2.1, 2018-09-24

[6] Network Device Collaborative Protection Profile (NDcPP)/Stateful Traffic Filter Firewall Collaborative Protection Profile (FWcPP) Extended Package VPN Gateway, Version: 2.1, National Information Assurance Partnership, 2017-03-08. https://www.commoncriteriaportal.org/files/ppfiles/ep_vpn_gw_v2.1.pdf

[7] PP-Module for Virtual Private Network (VPN) Clients, Version: 2.2, National Information Assurance Partnership, 2021-01-05. https://commoncriteria.github.io/pp/vpnclient/vpnclient-release.pdf

[8] PP-Module for Virtual Private Network (VPN) Gateways, Version: 1.1, National Information Assurance Partnership, 2020-06-18. https://www.commoncriteriaportal.org/files/ppfiles/mod_vpngw_v1.1.pdf

[9] collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0, 2018-03-14. https://www.commoncriteriaportal.org/files/ppfiles/CPP_FW_V2.0E.pdf

[10] collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Intrusion Prevention Systems (IPS), Version 2.11, 2017-06-15.

[11] Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption, Version 1.2, 2016-05-10.

◐ 저 자 소 개 ◑

이 용 준(Yong-joon Lee)
1999년 강남대학교 전자계산학과 학사
2001년 숭실대학교 컴퓨터학과 석사
2005년 숭실대학교 컴퓨터학과 박사
2020년~현재 : 극동대학교 해킹보안학과 교수
관심분야 : 해킹보안, 국방보안, 인공지능보안
E-mail : 2020032@kdu.ac.kr

박 세 준 (Se-joon Park)
1996년 숭실대학교 수학과 (이학사)
1998년 숭실대학교 컴퓨터공학과 (공학석사)
2004년 숭실대학교 컴퓨터공학과 (공학박사)
2006년~현재 SK 정보보호담당 수석연구원
관심분야 : 인공지능보안, 개인정보보호, 정보보호
E-mail : sjoon0912@naver.com

박 연 출 (Yeon-chool Park)
2004년 숭실대학교 컴퓨터학과 박사
2005년~2009년 성균관대학교 ISRI 연구교수
2009년~2010년 스웨덴 Umeå Univ. Post-Doc.
2011년~2013년 프랑스 Pascal Institute Post-Doc.
2013년~현재 LG전자 CTO 책임연구원
관심분야 : 로봇비전, 인공지능, 딥러닝
E-mail : fearhope@gmail.com