정 보 보 호 학 회 지
제25권 제2호, 2015. 4

# 美軍 암호장비 현황 및 상호운용성 전략

최 준*, 강 성 문*, 최 인 수**

요 약

정보보호 목표를 달성하기 위한 다양한 기술들 중, 암호기술은 정보의 기밀성 보호를 위한 주요 수단으로 활용된다. 각 국가에서는 상업용 암호기술 뿐만 아니라, 국가(국방, 공공)기관 중요 정보 보호를 위한 암호기술을 공개 혹은 비공개 방식에 의해 연구・개발중이다. 본고에서는, 암호 분야에 있어서 세계 최고의 기술력을 보유하고 있다고 알려진 美軍 암호장비의 변천 동향을 알아보고, 이를 토대로, 향후 정보통신환경 변화에 부합된 암호기술 발전방향을 제시하고자 한다.

## Ⅰ. 서 론

암호화(encryption)는 송・수신 되는 정보 혹은 메시지에 대해, 인가받지 못한 이는 판독할 수 없는 글자・숫자・부호 등으로 변환하는 것을 의미한다. 암호기술은 암호화 기능 구현과 관련된 제반 원리・기법으로서 암호알고리즘(암호논리) 및 보안프로토콜 등을 포함하는 용어이고, 암호장비는 암호화 기능을 주요 목적으로 암호기술이 구현 혹은 내장되어 제작된 장치 및 장비 등을 의미한다.

한국을 포함한 세계 각 국에서는 국가용 혹은 상업용 목적으로 다양한 암호기술을 연구 및 개발하고 있다. 암호기술의 활용 범위가 확대됨에 따라 국제적으로 관련 기술들의 표준화도 활발히 추진 중이나, 대부분의 나라들은 비밀 등 중요 정보의 보호를 위한 암호기술은 비공개로 개발, 관리하고 있다. 이에 따라 각 국가별 암호기술의 수준을 정량적으로 차등화 한다는 것은 제한되지만, 미국의 암호 기술력은 세계 최상위 수준으로 인정되고 있다.

미국의 보안기술 관련 연구기관들 중, 1952년 국방부 소속 연방기관으로 창설된 NSA(National Security Agency)는, 비밀(기밀) 정보의 보호를 목적으로 미국 정부기관에 적용되는 암호기술/장비들의 연구개발, 획득 및 운용을 총괄・조정하고 있다. 전통적으로 NSA에서 개발한 암호기술/장비들은 비공개 원칙을 유지하여 왔다. 하지만, 정보통신기술 발전으로 인한 암호기술 적용 범위 확대, 국제 표준 암호기술 분석・평가 참여, 과거 개발된 일부 암호장비의 비밀 해제에 따른 공개 등을 통해, NSA에서 추진하고 있는 암호 정책・전략에 대해 일정부분 공개가 되는 추세이다.

이에 본고에서는, 미군의 암호기술/장비 적용 개념 및 기준을 정리하고 '05년에 NSA에서 공표한 '암호 상호운용성 전략(Cryptographic Interoperability Strategy)'을 중심으로 미군의 최근 암호 발전방향을 제시하고자 한다.

본고의 구성은, Ⅱ장에서 미군의 암호장비 적용 대상 개념 및 NSA가 암호장비를 통해 보호하려는 대상(security factor)을 제시하고, Ⅲ장에서는 미군 암호장비의 Type별 분류 현황 뿐만 아니라, 암호 상호 운용성 전략에 기반한 암호기술 Suite별 분류 현황을 제시하였으며, Ⅳ장에서는 암호 상호운용성 전략(CIS), 끝으로 Ⅴ장에서는 앞에서 제시된 사항들에 대해 시사점 및 결론을 맺는다.

## Ⅱ. 미군 암호장비의 보호 목표

국가 및 국방 분야에서는 비밀로 분류되는 정보보호 목적 달성을 위해, 암호기술과 결합된 암호장비를 특별히 개발・관리하고 있다.

일반적으로 미군의 암호장비는 운용 목적 및 환경에 따라, 전송데이터 보호와 저장데이터 보호 용도로 구분된다. 전송데이터 보호 암호장비는 다양한 통신망 환경

* 국방보안연구소 (choijun1014@hotmail.com, smkang111@korea.com)
** 한국국방연구원 (ischoi007@naver.com)

에서 송·수신되는 정보의 보호를 위한 것으로 Link용[1], 전화용, FAX용, VPN용 등의 통신용 암호장비가 해당된다. 저장데이터 보호 암호장비는 PC, 서버, 스마트폰 등에 저장·관리되는 정보의 보호를 위한 것으로, 사용자 컴퓨팅 장치의 활용 확대에 따라 최근 연구개발 소요가 확대되고 있는 분야이다.

통신용 암호장비는 전통적으로 미군이 가장 많이 적용하는 암호장비로서, 암호장비 적용 환경에서 요구되는 통신보안(COMSEC – Communication Security)[2] 기능을 제공한다. COMSEC의 기능은 암호보안, 전송보안, 트래픽보안, 방사보안, 물리적보안 등으로 분류[3]되는데, 암호장비가 적용되는 환경의 기술적 특성 및 운용 개념 등에 기반한 보안요구 수준에 따라, 다양한 COMSEC의 기능들이 적절히 조합되어 구현된다. 각 기능에 대해 알아보면 다음과 같다.

### 2.1. 암호보안(Cryptographic Security)

암호알고리즘 등 암호기술을 기반으로 기밀성(Confidentiality), 인증(Authentication) 등의 보안 기능을 제공하는 것이다. 일반적인 암호장비에는 기본적으로 암호보안 기능이 구현된다.

### 2.2. 전송보안(TRANSEC: Transmission Security)

암호알고리즘을 대상으로 분석·해독 이외의 수단과 방법을 이용하는 전송 데이터 도청, 통신 장애 유발 등을 방지하기 위한 보안기능으로서, 항재밍(Anti-Jamming)·주파수도약(Frequency Hopping)·스펙트럼 확산(Spread Spectrum) 등의 방법이 있다.

### 2.3. 트래픽보안(TFS: Traffic-Flow Security)

암호기술이 적용된 경우 전송 데이터의 기밀성은 유지되지만, 공격자의 트래픽 분석으로 인해 발생 가능한 정보 유통 패턴 및 유통량 변화, 네트워크 주소 등의 누출을 방어하기 위한 보안기능이 요구된다.

대응되는 보안기술로는 정보 유통량에 관계없이 일정한 크기의 트래픽 전송 혹은 트래픽 분석에 이용될 수 있는 정보들의 암호화 방법 등이 사용된다, Link용 암호장비들의 경우 대부분 트래픽보안 기능이 구현된다.

### 2.4. 방사보안(EMSEC: Emission Security)

암호장비 동작시 방출되는 전력 소모량, 신호 및 주파수 등의 정보가 공격자에 의해 암호분석 목적으로 악용되는 것을 방어하기 위한 보안기능으로, 대응방안으로는 암호장비 내부 칩·모듈에서 방사되는 전자파 정보 특성을 조절·통제하는 목적의 TEMPEST 기술이 있다.

### 2.5. 물리적보안(Physical Security)

암호장비 뿐만 아니라 암호장비와 관련된 부품, 문서 등에 대해 비인가자로부터 물리적 보호 및 관리에 관한 업무·기능을 의미한다.

### 2.6. 기타

미군은 2.1~2.5 외에도, 비인가자에 의한 오작동 혹은 암호장비 훼손에 대한 내성 제공(Tamper Resistance 기능)을 요구하고 있으며, 핵폭발에 의한 전자파 방사시 대응 가능한 기능(Electromagnetic Pulse Hardening) 구현까지 고려하고 있다[4].

## Ⅲ. 미군 암호장비 / 암호기술 분류

NSA 창설 이후 현재까지, 미군의 암호장비/암호기술은 1950~1960년대 전자 기계장치(Electromechanical) 기반 1세대, 1970년대 진공 튜브(Vacuum tube) 기반 2세대, 1980년대 집적회로(Integrated Circuit) 기반 3세대, 1990년대 전자식 키 분배(Electronic Key Distribution) 기반 4세대, 21세기 이후 네트워크 중심전(Network - Centric Systems)에 활용을 목표로 하는 5세대 등, 총 다섯 세대(Five generations)로 변화·발전되어 왔다[5].

다음의 3.1. / 3.2.절에서는 상기 언급된 다섯 세대와 연관되어 적용된, 암호장비 및 암호기술에 대한 특성과 현황을 제시하고자 한다.

1) Link encryption is an approach to communications security that encrypts and decrypts all traffic at each end of a communications line (e.g. the line between two network switches)[1].

### 3.1. 암호장비 분류(Type 1 ~ Type 4)

보안 목적에 따라 암호장비의 기능 및 특성은 다양한데, 미군 및 미국 정부기관에서 사용하는 암호장비는 정보의 가치등급(예: 비밀여부, 민감성 등 고려)과, 사용되는 암호기술 등의 특성에 따라 4가지 유형(Type 1~Type 4)으로 구분된다[6].

Type 1 – 미국 국가안보(National Security Information)와 관련된 정보들 중 비밀(classified)과 민감한(sensitive) 자료의 보호를 위해 적용되는 암호장비 유형이다. 사용되는 암호기술은 NSA가 평가・인증・승인・관리・통제를 담당한다[3]. Type 1의 암호장비는 암호학적 측면, 기능적 측면, Tamper Registance, 방사보안(EMSEC) 기능, 암호장비 제조 및 배포에 대한 제조과정 등 제반사항에 대해 정형화된 분석(Formal Analysis)을 요구하며, 이에 따라 평가・인증받게 된다[7].

Type 2 – 미국 국가안보와 관련된 정보들 중 SBU(sensitive but unclassified) 정보. 즉, 비밀은 아니지만(unclassified) 민감한 자료의 보호를 위해 적용되는 암호장비 유형이다. 사용되는 암호기술은 NSA가 평가・인증・승인・관리・통제를 담당한다.

Type 3 – 국가 안보정보가 아닌 미국 정부 업무와 관련된 정보들 중 SBU(sensitive but unclassified) 정보에 대해 적용되는 암호장비 유형이다. 사용되는 암호기술은 민간에서 개발되어 미국 연방정부 표준인 FIPS[2]에 공표된 기술로서, 미국 NIAP[3]에서 평가・인증을 담당하며, 미국 표준기술국 NIST(National Institute of Standards and Technology)가 승인한다.

Type 4 – Type 1~Type 3와 상이하게, 특정 기관(NSA, NIST)의 평가・인증・승인을 받지 못한 유형이다.

2) Federal Information Processing Standards

3) NIAP : National Information Assurance Partnership의 약자로서, 상용 정보보호 제품의 신뢰성, 안전성 등을 평가・인증하기 위한 국가 차원의 조직. NSA와 NIST가 공동 참여하여 운영된다.

### 3.2. 암호기술 분류(Suite A & Suite B)

암호보안은 미군 암호장비의 핵심적, 기본적인 보안기능으로, 이는 다양한 암호기술을 통해 구현된다.

앞서 설명하였듯이 미군이 활용하는 다양한 암호장비들 중, 국가안보 관련 비밀 등 중요 정보의 보호를 위한 암호장비는 Type 1 암호장비이며, 여기에는 NSA에서 인가한 암호기술이 적용된다. 과거 NSA는 Type 1 암호장비 대상 비공개 암호기술을 적용하였으나, Ⅳ장에서 세부적으로 설명할 암호 상호운용성 전략의 일환으로 암호기술 적용 정책이 변화하였으며, 이를 기반으로 비밀 보호 관련 미군 암호장비에 적용되는 암호기술은 표 1에서 보는 바와 같이, Suite A와 Suite B의 범주로 구분된다[8].

〔표 1〕 Suite A / Suite B 범주

| Suite 유형 | 범 주 |
|---|---|
| A | NSA developed for highly sensitive communication, critical authentication systems |
| B | Commercially available and published algorithms for unclassified and classified use |

표 1에서 보는 바와 같이, Suite A는 민감도가 높거나 중대한 정보(외부 누출시 치명적 악영향을 줄 수 있는 정보)에 대해 적용되는 기술로서, NSA가 개발을 담당하며, 비공개를 원칙으로 한다.

Suite A에 포함되는 기술들은 Type 1에서 요구되는 국가안보 관련 정보(classified & sensitive informations)에 적용 가능하며, 일부는 Type 2에서 요구되는 정보 등급에도 적용이 가능하다.

Suite A 암호기술은 과거와 같이 NSA에서 개발한 비공개 암호기술들을 통칭하는 범주로 볼 수 있으며, 표 2의 암호기술들이 해당된다(암호알고리즘 명칭 등은 일부 공개되어 있으나 세부 구조는 비공개)[9].

반면, Suite B에 포함되는 공개 암호기술들은, 미국 정부 및 국제 표준 암호기술을 기반으로 규정되어 있으며, 필요시 Type 1과 Type 2가 요구되는 국가안보 관련 정보 등급(classified, SBU)에 적용 가능하다.

즉, 공개된 Suite B 범주의 암호기술들이, 비밀이 아닌 정보에도 적용될 수 있다는 것은, 기존 GOTS(Government off-the-shelf) 중심의 암호기술만

〔표 2〕 Suite A Cryptography

| Algorithm |
|---|
| ACCORDIAN, BATON, BAYLESS, CARDIGAN, CARDHOLDER, CARIBOU, CRAYON, FASTHASH, FIREFLY, GOODSPEED, HAVEQUICK, JACKNIFE, JOSEKI, JUNIPER, KESSE, MAYFLY, MEDLEY, PEGASUS, PHALANX, SAVILLE, WALBURN, WEASEL 등 |

적용되었던 정보들에 대해, COTS(Commercial off-the-shelf) 암호기술까지 병행 사용할 수 있도록 정책 변경을 함으로써, 다양한 정보통신 환경에서 국제 표준 암호기술을 토대로 하는 정보 유통을 보장하고, 상호운용성의 목적을 달성한다는 것이다.

암호알고리즘 명칭을 제외한 세부사항이 비공개로 관리되는 Suite A(예: 표 2 참조)와 달리, Suite B에 대해서는 암호알고리즘・키교환・전자서명・해쉬함수 등을 대상으로 표 3과 같이 비밀 등급(Top Secret, Secret) 별 활용 가능한 기술들이 국제 표준 기술들을 토대로 제시되어 있다[10].

〔표 3〕 Suite B Cryptography

| Function | Algorithm | Spec. | Parameters |
|---|---|---|---|
| Encryption | AES (Advanced Encryption Standard) | FIPS Pub 197 | 128 bit key for SECRET |
| | | | 256 bit key for TOP SECRET |
| Key Exchange | ECDH (Elliptic Curve Diffie – Hellman) | NIST SP 800-56 A | Curve P-256 for SECRET |
| | | | Curve P-384 for TOP SECRET |
| Digital Signature | ECDSA (Elliptic Curve Digital Signautre Algorithm) | FIPS Pub 186-4 | Curve P-256 for SECRET |
| | | | Curve P-384 for TOP SECRET |
| Hashing | SHA (Secure Hash Algorithm) | FIPS Pub 180-4 | SHA-256 for SECRET |
| | | | SHA-384 for TOP SECRET |

## Ⅳ. Cryptographic Interoperability Strategy

이 장에서는 앞에서 일부 언급이 되었지만, 통신간 사용되는 객체들의 상호운용성 및 유기적 정보공유를 통해 네트워크 중심전 환경을 지향하는 5세대 암호기술/장비 개발 추진을 목표로, NSA 주도하에 ’05년부터 추진된 ‘암호 상호운용성 전략(이하 CIS)’에 대해 구체적으로 알아보고자 한다.

### 4.1. 추진 배경 / 목적

2000년 이후 미군은, 과거 플랫폼 중심에서 네트워크 중심전을 위한 군사력 발전을 추진해왔으며, 네트워크 중심전에서는 유기적인 네트워킹을 기반으로 한 정보공유 및 상호운용성이 요구되었다.

하지만, 전통적으로 미국에서 사용되어 오던 암호기술/장비들은 응용 및 확장 측면에서 많은 제한점을 갖고 있으며, 또한 보안기술의 정책적 측면에서도 이러한 제한점을 해소할 수 있도록 수립되어 있지 않았다. 이로 인해, 군인 혹은 군 관계자, 정부기관, 협력국가 간에 기밀성이 보장되는 안전한 통신이 용이하지 않았다. 이에 따라 암호기술/장비 측면에서도 유기적인 정보공유와 상호운용성을 지원할 수 있는 추가적 능력 발전이 요구되었으며, 이를 해결하기 위한 방안으로 ’05년 이후 NSA 주도로 CIS가 추진되었다.

앞서 설명한 Suite A와 Suite B 암호기술의 구분은 대표적인 CIS 전략 추진의 결과이다. 全 미군 차원의 효율적인 상호운용성 지원을 위해서는 공통의 암호기술을 사용하는 것이 가장 직관적인 해결책이였으며, Suite B가 여기에 해당하는 것이다.

즉, CIS 추진을 통해, COMSEC 기능을 위한 별도 처리 과정을 최소화 하면서 보안관련 각종 표준기술, 프로토콜, 운용모드들의 상호운용성을 증대시키는 것이다.

### 4.2. CIS 운영개념

CIS의 운영개념은 그림 1[8]에서 보는 바와 같이 GOTS(Government off-the-shelf)와 COTS(Commercial off-the-shelf)가 적용될 수 있는 영역으로 구분할 수 있다[4].

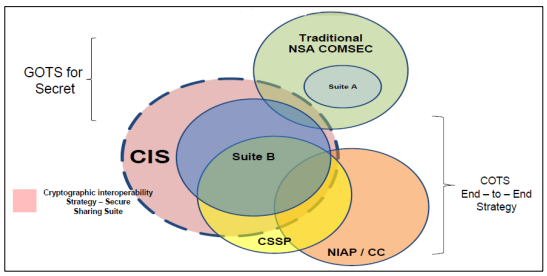
4) 그림 1의 CSPP는 The Commercial Solutions Partnership Program, CC는 Common Criteria 의미

국가안보 관련 비밀로 분류된 정보들에 대해서는 Suite A 계열 기술을 토대로 NSA가 통제하되, 그 외 정보들의 영역에 대해서는 국제표준 기술 및 Suite B 계열 기술 등 COTS 기반의 기술을 통해, 암호 통신에 관여하는 최종 말단 객체간(End-to-End) 원활한 정보공유 및 상호운용성을 향상 시키는 개념이다.

### 4.3. CIS에 의한 정책/기술 변화 방향

미군에서 CIS가 추진되기 전에는, 국가안보와 관련하여 비밀이면서 민감한 정보에 대해서는, NSA 주도하에 개발된 비공개 전용 암호기술을 적용한다는 원칙을 고수해왔다.

하지만, 4.1.에서 제시한 바와 같이 CIS의 필요성이 증대됨에 따라, 공개된 표준 기술 기반의 공통으로 활용 가능한 암호기술을 수용하였으며, 이러한 정책/기술 변화에 따라 이기종간 COMSEC 통신시 발생 가능한 제한사항을 해소하고, 정보공유 및 상호운용성을 보장하려고 노력 중이다. 이러한 노력을 통해, 21세기에 들어 지향하고자 하는 네트워크 중심전 하에서 요구되는 보안 통신 목적을 달성하고자 하는 것이다.




〔그림 1〕 '美 암호 상호운용성 전략' 체계도

## Ⅴ. 결 론

본고에서는 미군이 암호기술을 통해 달성하고자 하는 보호 목표와 이를 달성하기 위한 수단으로서 사용중인 다양한 암호장비 현황을 고찰해 보았으며, CIS 전략에 대해 제시하였다.

주목할 사항은, 미군의 경우 비밀보호를 위한 암호기술/장비에 대해 비공개된 전용 기술을 사용하여 왔지만, 통신에 관여되는 모든 객체들이 네트워크화 되는 현대의 정보통신 환경에 적합한 암호기술 운용을 위해, 일정 부분 국제표준 암호 기술들의 수용 및 정보 공유의 필요성 등을 인정하였다는 것이다, 이에 따라, 표준화된 공개 암호기술까지 병행 사용할 수 있도록 정책 변경을 함으로써, 다양한 정보통신 환경에서 원활한 정보공유 및 상호운용성의 목적을 달성한다는 것이다.

미군의 암호기술이 세계적으로 인정받고 있다고 해서, 반드시 우리나라 또한 미군과 동일하게 암호기술을 연구・개발하고 운용해야 된다는 것은 아니다. 하지만, 급변하는 정보통신환경에 부합된 암호기술 패러다임의 변화 필요성을 인식하고, 체계적인 전략 수립을 모색해 보는 것은 우리나라에게도 요구된다고 볼 수 있으며, 본고에서 제시된 사항이 이러한 요구사항 발생시, 국가적 차원에서 공감대를 형성하는데 도움이 될 수 있기를 기대해본다.

## 참 고 문 헌

[1] http://en.wikipedia.org/wiki/Link_encryption
[2] http://en.wikipedia.org/wiki/COMSEC
[3] 한국국방연구원, All-IP 정보통신 환경 대비 국방 암호장비 및 기술 발전방향 연구, KIDA 출판, pp. 30-32, Aug. 2014.
[4] http://en.wikipedia.org/wiki/NSA_encryption_systems
[5] Wikipedians, Cryptography, Pedia press, pp. 444-448, Nov. 2011.
[6] Committee on National Security Systems, CNSS Instruction No. 400 - National Information Assurance (IA) Glossary, CNSS, pp. 78-79, Apr. 2010.
[7] http://en.wikipedia.org/wiki/Type_1_encryption
[8] Anne Gugel, NSA Cryptographic Interop erability Strategy, Oct. 2010.
[9] http://en.wikipedia.org/wiki/NSA_cryptography
[10] https://www.nsa.gov/ia/programs/suiteb_cryptography/

## 〈저 자 소 개〉


**최 준 (Jun, Choi)**
정회원

2001년 2월 : 경희대학교 이학부 (수학) 졸업
2003년 2월 : 고려대학교 정보보호 대학원 공학석사
2008년 2월 : 고려대학교 정보보호 대학원 공학박사
2014년 11월~현재 : 국방보안연구소
관심분야 : 암호논리, 암호키관리, 정보보호프로토콜

**강 성 문 (Sung-Moon, Kang)**
비회원

1985년 2월 : 한남대학교 전자계산학과 졸업
1990년 8월 : 성균관대학교 컴퓨터감사학과 석사
2008년 8월 : 고려대학교 정보보호 대학원 공학박사
2015년 1월~현재 : 국방보안연구소
관심분야 : 정보보호정책, 사이버보안, 위험관리

**최 인 수 (In-Soo, Choi)**
비회원

1993년 2월 : 고려대학교 수학과 졸업
1995년 2월 : 고려대학교 수학과 석사
2007년 2월 : 고려대학교 정보경영공학 박사수료
2002년 2월~현재 : 한국국방연구원 연구위원
관심분야 : 정보보호, 컴퓨터공학, C4ISR