

NACLIPS ENCRYPTER SERVER

MEDIA FILE ENCRYPTING SOLUTION

VERSION 1.0

Published By,
NEXPOLY Technology Inc.
Technology Lab.

1. 시스템 사양	1
2. 시스템 특징	1
3. 시스템 구성 및 주요 기능	1
4. 네트워크 구성도	2
5. 서버 데몬 설정 및 구동	3
6. Nacrips Encrypter Console Commander	5
7. Nacrips Encoder Command Protocol	7



NEXPOLY Technology Inc.
1030, 83, Samwon-ro, Deogyang-gu,
Goyang-si, Gyeonggi-do, Korea.
TEL : 031) 963 - 9035
[HTTPS://www.nexpoly.co.kr](https://www.nexpoly.co.kr)

1.시스템 사양.

솔루션 명칭	나클립스 인크립터 서버
솔루션 분류	멀티미디어 파일 암호화 솔루션
시스템 구성	암호화 서버 엔진 + 콘솔 커맨더
서버 OS 환경	리눅스(x86, x86-64, IA64, SPARC, PPC, Alpha). / 윈도우 시스템(x86, x86-64).
C/S 통신 프로토콜	TCP/IP :: NECP (Nacrips Encoder Command Protocol) / HTTPS (HTTP over SSL) / HTTP
서버 H/W 권장 사양	CPU, 2.0 Ghz Quad Core / Memory, 8.0GByte 이상
프로그램 실행 방식	Server Daemon

2.시스템 특징.

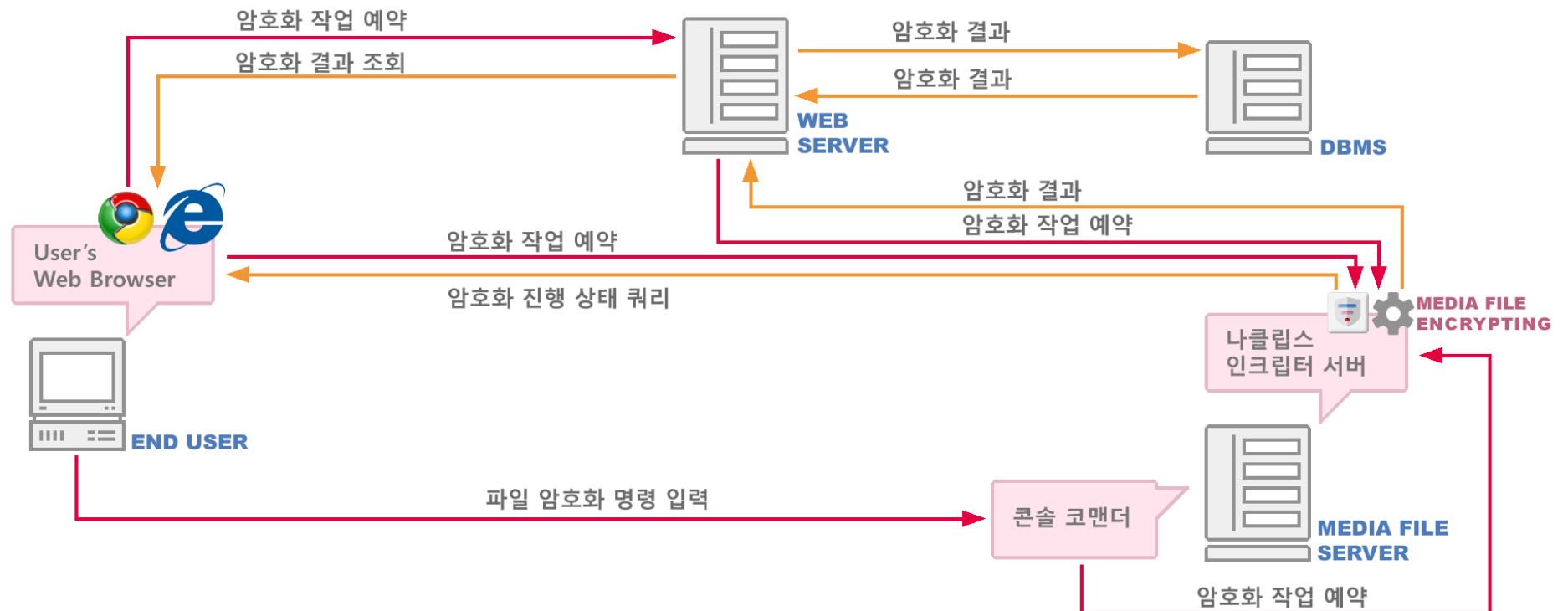
- 동영상 파일 및 오디오 파일의 암호화 변환 서버 엔진.
 - 멀티코어 CPU를 위한 다중 프로세스 작업을 지원하여 부하 분산기능 지원.
 - 서버상에서 하위 디렉토리 포함, 다량의 파일 일괄 암호화 처리기능 지원.
- 작업내역 및 처리결과 DB입력을 위한 인터페이스 제공.
 - 웹 브라우저 또는 네트워크를 통한 암호화 예약 및 상태 조회 인터페이스 제공.
 - 터미널 콘솔에서 암호화 작업 예약 및 조회를 위한 콘솔 명령 프로그램 지원.

3.시스템 구성 및 주요 기능.

구성 모듈	기능 분류	기능 상세	기능 설명
암호화 서버 엔진 Encrypter Server Daemon	미디어 파일 암호화	암호화 예약 관리	멀티미디어 파일을 암호화 예약 / 예약취소 / 진행상태조회 기능.
		멀티미디어 파일 암호화	서버에 저장된 멀티미디어 파일을 암호화 하여 목적 디렉토리로 출력.
		처리내역 인터페이스	암호화 예약 및 작업 처리 내역을 DBMS에 저장하기 위한 인터페이스.
	암호화 서버 보안	암호화 명령 인터페이스	나클립스 암호화 명령 프로토콜(NECP:Nacrips Encoding Command Protocol)을 통해 인증된 사용자가 웹서버를 경유하여 나클립스 암호화 서버에 암호화 명령을 예약 및 조회.
		명령어 IP 필터링	NECP Protocol을 통해 명령을 전송하기 위한 접속 호스트 IP/domain 필터링 기능.
		접속 IP 필터링	접속되는 IP 어드레스의 Allow/Deny 필터링 기능.
	시스템 로그	로그 인터페이스	작업 로그를 텍스트 파일로 저장하거나 웹-인터페이스를 통하여 DB에 기록.

콘솔 커맨더 Nacrips Encrypter Console Commander	암호화 예약	파일 단위 예약/취소	단일 파일에 대한 암호화 예약 및 취소.
		디렉토리 단위 예약	지정 디렉토리의 모든 파일의 암호화 예약. (하위 디렉토리 포함 옵션 가능)
		암호화 설정 지정	파일 암호화 예약시, 암호화 서버 데몬 설정과 다른 암호화 옵션 지정.
	암호화 작업 조회	암호화 상태 조회	단일 파일 / 다중 파일에 대한 암호화 처리 상황 조회.
		암호화 예약큐 조회	암호화 예약 및 처리중인 파일들 조회.

4.네트워크 구성도.



5.서버 데몬 설정 및 구동

나클립스 인크립터 서버 설정.

```
[admin@media admin]$ ls /usr/local/nencrypter/conf/
bookinghosts.allow      ..... 암호화 예약 명령이 가능한 호스트 IP 주소들 지정
daemon.conf             ..... 나클립스 인크립터 서버 설정파일.
hosts.allow             ..... 접속 허용 IP 주소들 지정 (선택 옵션)
hosts.deny              ..... 접속 거부 IP 주소들 지정 (선택 옵션)
httpaccess.allow        ..... 명령어 허용 웹페이지 도메인 주소들 지정 (선택 옵션)
mediafiles.ext          ..... 암호화 가능한 원본 동영상/오디오 파일 확장자 지정.
ssl.conf                ..... 암호화 명령통신 프로토콜을 HTTPS로 사용할 경우 설정옵션.

[admin@media admin]$ cat /usr/local/nencrypter/conf/daemon.conf
; 1.NECP 명령어 포트 ..... def : 5667
C2S_PORT = 5667
; 2.나클립스 인크립터 서버 이름 지정
server_name = Nacrips Encrypter Server V1
; 3.원본 미디어 파일 최상위 디렉토리 지정 ..... def : media
MEDIA_ROOT = /media_files
; 4. 암호화 출력 파일 최상위 디렉토리 지정 ..... def : export
EXPORT_ROOT = /media_files/export
; 5.로그 파일 디렉토리 ..... def : logs
LOG_ROOT = logs
; 6.원격 접속 IP 필터링 기능 여부 ..... def : false (ref- hosts.allow/hosts.deny)
ip_filter = true
; 7.암호화 출력 파일 생성시 동일 파일, Overwrite 여부 지정 .... def : true
overite_same_file = false
; 8.암호호 출력 파일 생성시 서브 디렉토리 생성 여부 ..... def : true
create_sub_directory = true
; 9.최대 암호화 작업 프로세스 갯수 ..... def : 2
enc_process_count = 10
;10.최대 암호화 작업 예약 대기열 수 ..... def : 1024
enc_queue_size = 2048
; -.encrypt anything files ..... def : no (multimedia file only)
encrypt_all_files = no
; -.미완료된 암호화 출력 파일 자동 삭제 여부 ..... def : false
```

```
clear_incompleted_export = no
; -.암호화 결과 DB 인터페이스 URL
web_interface_url = http://192.168.1.101/nencrypter_ifce/webface.php
; -.원격접속 최대 동시 접속수 ..... def : 0 (maximum)
max_connection = 0
; -.enable ssl(https) protocol ..... def : false
enable_ssl = yes
```

나클립스 인크립터 서버 데몬 실행.

```
[admin@media admin]$ /usr/local/nencrypter/daemonctrl start
NACLIPS.encrypter Daemon Controler for Linux Intel 64-Bit Machine. Ver:1.1.200.
Copyright(C) 2010-2017 NEXPOLY Technology Inc, All Rights Reserved.
NACLIPS.encrypter Daemon for Linux Intel 64-Bit Machine. Ver:1.0.0.00.
Copyright(C) 2020 NEXPOLY Technology Inc, All Rights Reserved.

        Host Server Name : cent58
        Server IP Address : 192.168.1.100

.. Reading Main Configuration ....
    16 Configuration(s) fixed up.
.. Reading Encrypting Reservation Host List ....
    3 allowd host(s) registered.

        User Connection Port : 5667
        Encoder Server Name : Nacrips Encrypter Server V1
            Product Code : 1181
        Maximum Connection : 100
        Source Media Directory : /media_files
        Media Export Directory : /media_files/export

        User Connection Log : /usr/local/nencrypter/logs/con.log
        Daemon Process Log : /usr/local/nencrypter/logs/pro.log
        Encrypting Job EnQueue Log : /usr/local/nencrypter/logs/cmd.log
        Encrypting-Stat Query Log : /usr/local/nencrypter/logs/stt.log
        Media Encrypting Log : /usr/local/nencrypter/logs/enc.log
        Job EnQue Web-Interface Log : /usr/local/nencrypter/logs/web.log
```

```

        Error Log : /usr/local/nencrypter/logs/err.log
        Remoted-IP Filtering? : Yes
        3 allowd host(s) registered.
        0 denied host(s) registered.

        Overwrite Same Output ? : No
        Create sub-directory ? : Yes
        Encrypting Thread Count : 3
        Encryption List-Queue Size : 2048
        Interface URL for Encryption : https://192.168.1.101/nencrypter_ifce/webface.php
        Check CORS option? : No
        Clear incompleated exported media fi : No

## Starting up NACLIPS.encrypter Daemon .....
## Starting up EncrypterEngine          ..... OK(pid:18998).
## Starting up ServerEngine             ..... OK(pid:18997).
    
```

6. NACLIPS Encrypter Console Commander.

나클립스 인크립터 콘솔 커맨더(nencryptcmd)는 나클립스 인크립터 서버로 로컬 접속 또는 원격으로 접속하여 파일 암호화 예약을 하거나 암호화 상태 조회를 하는 커맨드 라인 프로그램 (Command Line Program) 입니다. 나클립스 인크립터 콘솔 커맨더는 리눅스 버전과 윈도우 버전을 지원합니다.

나클립스 인크립터 콘솔 커맨더(nencryptcmd) 명령 형식.

nencryptcmd **COMMAND** [*server*=SERVER_IP[:PORT]] [*source_media*=SOURCE-MEDIA-FILE-PATH] [*export_path*=EXPORT-MEDIA-PATH] [OPTIONS]

commands:

enqueue = 미디어 파일 및 디렉토리 단위의 암호화 예약.

dequeue = 암호화 예약 또는 진행중인 암호화 작업의 취소.

current = 현재 진행중인 암호화 상태 조회.

clean = 완료된 암호화 상태를 깨끗이 초기화 한다. (모든 암호화 작업이 완료된 후에 명령 가능)

options :

-o = *overwrite* - 이미 존재하는 파일이면 덮어쓰기.

-r = *recursive* - 하위 디렉토리 포함.

-c = *clone directory* - 원본소스 디렉토리 지정시, 원본 디렉토리 구조를 그대로 복제하여 출력디렉토리를 생성한다.

-s = *use https protocol* - 나클립스 인크립터 서버가 HTTPS 통신 프로토콜로 실행중일때 사용한다.

ext = *extensions* : 원본 소스 미디어 파일의 확장자를 설정한다. (이때 나클립스 인크립터 서버에서 설정된 미디어 확장자는 무시한다. - mediafiles.ext 설정파일 참고.)

usage :

```
nencryptcmd enqueue source_media=/work/sample.mp4 export_path=/mp4_files/ -o -s
```

```
nencryptcmd enqueue server=192.168.1.100 source_media=/work/ export_path=/mp4_files/ ext=mp4 -o -c -r
```

```
nencryptcmd dequeue server=127.0.0.1:8087 encoding_sequence=3245 encoding_passkey=32034034
```

```
nencryptcmd current -s
```

나클립스 인크립터 콘솔 커맨더(nencryptcmd) 사용예.

```
#nencryptcmd enqueue 8087 source_media=/mp4/orig.mp4
```

```
1 encrypting job was enqueued.
```

; 로컬 서버에 있는 /mp4/orig.mp4 단일파일을 /mp4 디렉토리로 암호화 출력되도록 암호화 예약한다. 이때 인크립터 서버의 접속포트는 8087로 지정한다.

```
#nencryptcmd enqueue server=192.168.1.1:8087 source_media=/mp4/ export_path=/enc_mp4/ -o
```

```
/mp4 -> 28 media files found. Enqueued.
```

```
1 encrypting jobs (28 files) were enqueued.!!
```

; 192.168.1.1서버에서 나클립스 인크립터 서버가 가동중일때, /mp4/ 디렉토리의 모든 파일을 /enc_mp4/ 디렉토리에 암호화 출력되도록 암호화 예약한다.

; 이때 암호화 출력되는 파일이 이미 존재할 경우, 해당 파일을 Overwrite 한다.

```
#nencryptcmd enqueue source_media=/media/ export_path=/enc/ -c -r -s ext=avi,mp4
```

```
/media/server/test -> 16 media files found. Enqueued.
```

```
/media/server -> 10 media files found. Enqueued.
```

```
/media -> Not found media files. Skipped.
```

```
2 encrypting jobs (26 files) were enqueued.!!
```

; /media 디렉토리 및 하위 디렉토리내의 확장자가 avi,mp4인 파일만 /enc 디렉토리에 출력되도록 암호화 예약한다.

; 이때, 출력 디렉토리의 구조는 원본 디렉토리 구조를 그대로 복제하여 생성하며, 로컬서버에서 실행중인 인크립터 서버로

; 명령어 전송 프로토콜은 https 프로토콜을 사용한다.

```
#nencryptcmd current server=192.168.1.1 -s
```

```
Query result : 1005 OK_RETURN_CURRENT
```

```
Current encrypting source : /media_files/OK/12/AA/data/00/0F/_xfiupx_20151210002158326.mp4
```

```
Remained source files count : 33
```

```
Remained source files bytes : 158.59MB
```

```
Failed encrypting count : 0
```

; 192.168.1.1 서버에서 구동중인 나클립스 인크립터 서버의 현재 암호화 진행 상태를 조회한다. 이때 통신 프로토콜은 HTTPS를 사용한다.

```
#nencryptcmd dequeue encrypting_sequence=3245 encrypting_passkey=32034034
5th encrypting job was dequeued.
; 예약번호 3245번의 암호화 작업을 취소한다.
```

7. NACLIPS Encoder Command Protocol(NECP : Rovecat)

나클립스 인코더 명령 프로토콜(NACLIPS Encoder Command Protocol. 이하, NECP)은 변형된 HTTP 프로토콜 형태로서, 웹브라우저나 기타 네트워크 프로그램을 통하여 원격지에서 미디어 서버의 동영상 파일을 암호화 예약 및 조회를 할 수 있는 명령어 프로토콜 입니다. NECP 프로토콜은 아래와 같은 형식을 따릅니다.

프로토콜 형식.

1. Post 형식 (Client to Server)

```
Command/Server_Code Server_IP_Addr:Server_Port/Client_IP_Addr Protocol_Name/Version
Content-Length: Content_Length

Content_Body (Options)
```

2. Return 형식 (Server to Client)

```
Protocol_Name/Version Return_Code
Date: Date_Time_String
Server: Server_Engine_Description
Content-Length: Content_Length

Content_Body (Result)
```

NACLIPS Encoder Command Protocol 사용예.

1. 암호화 예약 명령 예

> Client To Server Post

```
ENQUEUE/NENCRYPTER 192.168.1.100:5667/192.168.1.201 ROVECAT/1.0
Content-Length: 55

source_media: mp4/40sec.mp4
export_path: /export/enc
```



```
overwrite: 1
```

mp4/40sec.mp4 파일을 export/enc/ 디렉토리에 출력 하도록 암호화 예약 등록. 이때, 출력 디렉토리에 같은 이름의 파일이 있을 경우 Overwrite 하도록 한다.

> Server to Client Return

```
ROVECAT/1.0 200 OK
Date: Thu, 27 Sep 2016 08:31:51 GMT
Server: NACLIPS.encrypter/1.1.0.00 (NEXPOLY Technology Inc.)
Content-Length: 110

Result: 1000 OK_ENC_ACCEPTED
Connection-Sequence: 6554
Encrypting-Sequence: 4879
Encrypting-Passkey: 392030
```

암호화 예약이 성공적으로 등록되었음. 이때, 접속 순번은 6554번이며, 암호화 예약 번호는 4879번이다.

2. 인코딩 작업 상태 조회 명령 예

> Client To Server Post

```
GETSTATUS/NENCRYPTER 192.168.1.100:5667/192.168.1.201 ROVECAT/1.0
Content-Length: 25

encrypting_sequence: 4879
```

인코딩 예약번호 4879번 인코딩 작업의 상황 조회.

> Server to Client Return

```
ROVECAT/1.0 200 OK
Date: Thu, 27 Sep 2012 09:35:36 GMT
Server: NACLIPS.encrypter/1.1.0.00 (NEXPOLY Technology Inc.)
Content-Length: 223

Result: 1002 OK_RETURN_STATUS
Connection-Sequence: 6554
```

```
Encrypting-Sequence: 4879
Encrypting-Source: mp4/40sec.mp4
Encrypting-Target: export/enc/40sec_mp4.nnc
Encrypting-Status: 1
Encrypting-Percent: 82
Elapsed-Seconds: 25
Remainging-Seconds: 10
```

조회한 예약번호의 현재 암호화 작업 상황을 성공적으로 리턴함.

3. 암호화 작업 취소 명령 예

> Client To Server Post

```
DEQUE/NENCRYPTER 192.168.1.100:5667/192.168.1.201 ROVECAT/1.0
Content-Length: 32

encrypting_sequence: 4880
encrypting_passkey: 3134330
```

인코딩 예약번호가 4880번인 암호화 작업을 취소합니다.

> Server to Client Return

```
ROVECAT/1.0 200 OK
Date: Thu, 27 Sep 2012 09:35:36 GMT
Server: NACLIPS.encrypter/1.1.0.00 (NEXPOLY Technology Inc.)
Content-Length: 71

Result: 1004 OK_ENC_DEQUE
Encrypting-Sequence: 4880
Dequeuing-Return: 1
```

대기중이던 4880번 암호화 작업 성공적으로 취소함.