



## 방송통신위원회

수신자 수신자 참조  
(경유)

제목 인터넷전화(VoIP) 침해사고 관련 유의사항 통보

1. 귀 사의 무궁한 발전을 기원합니다.

2. 최근 인터넷전화(VoIP)서비스 사업자의 부주의에 의한 과금 피해사례 발생 등으로 인터넷전화(VoIP)의 보안취약점에 대한 문제점이 제기되고 있는 바, 인터넷전화 사업자는 불임과 같이 자체 보안기능 강화뿐만 아니라 가입자들에게도 안내공문 등을 발송하여 더 이상 동일한 피해사례가 없도록 조치해 주시기 바랍니다.

3. 아울러, 동 사례와 관련하여 긴급 대책회의를 아래와 같이 개최하오니 바쁘시더라도 모두 참석해 주시기 바랍니다.

가. 일 시 : 2009. 12. 15.(화), 10:00 ~

나. 장 소 : 한국인터넷진흥원(KISA) 6층 회의실(송파구 가락동 소재)

다. 연락처 : KISA 보호기술팀(☎ 405-5361)

불임 인터넷전화(VoIP) 장비별 보안설정 방법 1부. 끝.

### 방송통신위원회 위원장



수신자 한국인터넷진흥원장, KT, LG데이콤, SK브로드밴드, 한국과학기술텔레콤, 세종텔레콤, 온세텔레콤, 드림라인, SK텔링크, 큰사람컴퓨터, 삼성네트웍스, 멀티스타텔레콤, 우한넷, 아이투라인, 서브원, KDDI코리아, 에스비인터랙티브, 다이얼커뮤니케이션즈, 엠에스에이커뮤니케이션, 굿텔레콤, 옥션스카이프, 웹투폰, 스프린트텔레콤, 렛츠070 등

방송통신주사보 이재곤

서기관

전결 12/15

박철순

협조자

시행 네트워크 기획 보호과 (2009. 12. 15.)  
-1770

접수

우 110-777 서울 종로구 세종로 20

/ [www.kcc.go.kr](http://www.kcc.go.kr)

전화 02-750-2762

전송 02-750-2769

/ [jglee@kcc.go.kr](mailto:jglee@kcc.go.kr)

/ 비공개(7)

## [붙임] 인터넷전화(VoIP) 장비별 보안설정 방법

### □ 관리용 기본 패스워드 변경

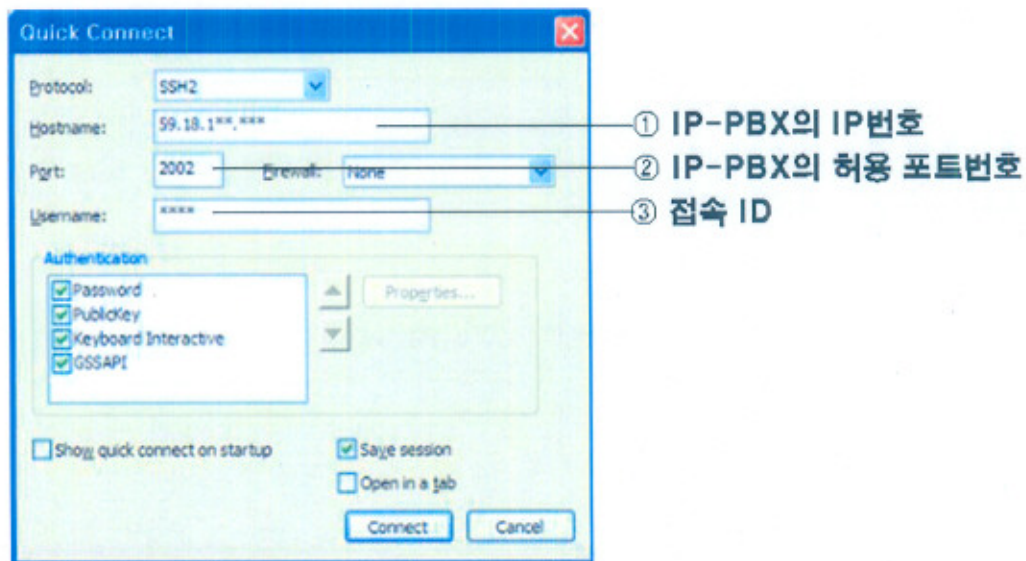
- 각 교환 장비의 출고 시 설정된 기본 패스워드는 반드시 변경
- 문자, 숫자, 특수문자가 조합된 8자리 이상의 패스워드 사용
- 패스워드는 주기적으로 변경

#### 예시 1) 제너시스템즈의 IP-PBX의 패스워드 변경 방법

- 시스템 관리용 계정과 사용자 관리용 계정으로 구분됨
- 시스템 관리용 계정은 명령어 입력창(콘솔:Consol)을 통해 접속, 사용자 관리용 계정은 웹을 통해 접속함

#### ○ 시스템 관리용 계정의 패스워드 변경방법(SSH이용)

##### ① SSH(Secure Shell)방식으로 IP-PBX시스템에 접속함



[SecureCRT프로그램을 이용한 SSH 접속방법]



② IP-PBX시스템에 접속하여 관리자 패스워드를 변경함

```
[root@EDU2 Backup]# passwd root
```

Changing password for user root.  
New UNIX password: \_\_\_\_\_  
Retype new UNIX password: \_\_\_\_\_

① 패스워드 변경 명령 실행

② 변경할 패스워드 입력

③ 변경된 패스워드 확인을 위한 재입력

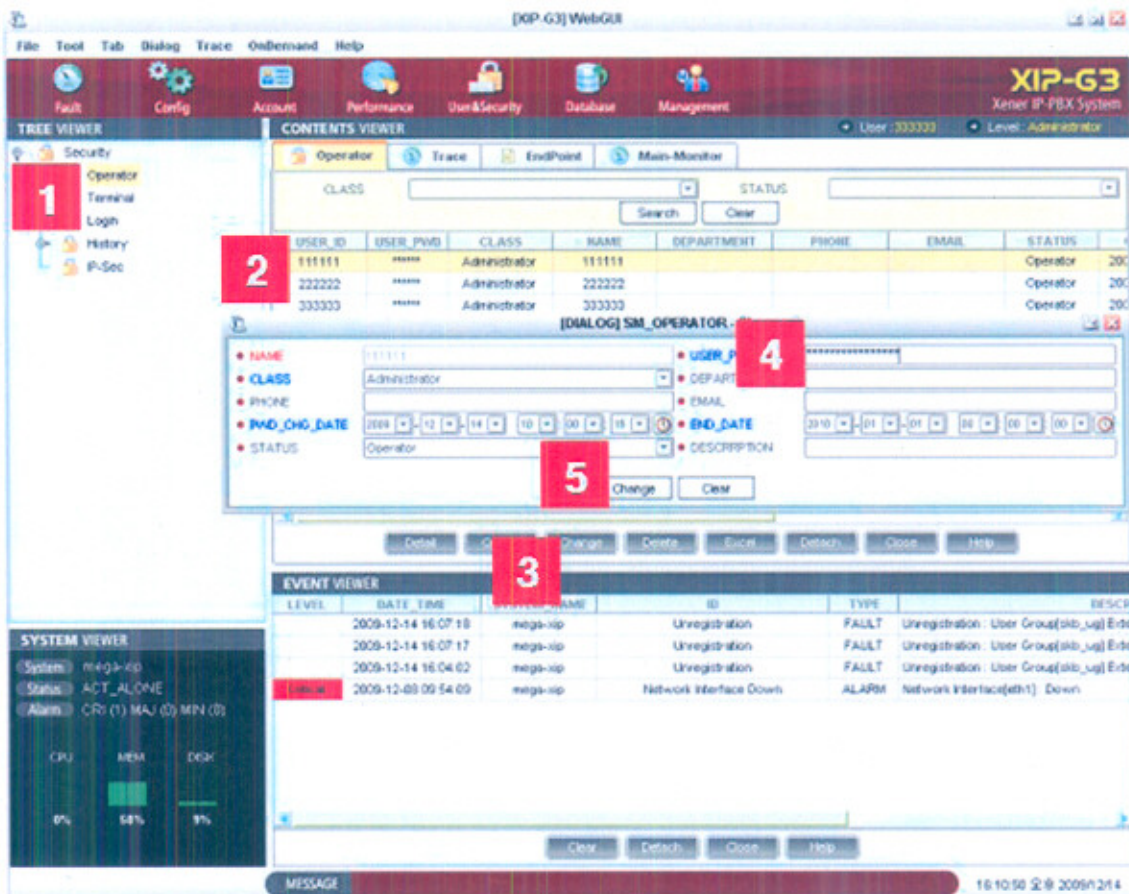
[SSH 접속 후 패스워드 변경 화면]

○ 사용자 관리용 계정의 패스워드 변경방법(웹 이용)

① 웹 기반의 사용자 관리시스템에 접속하여 로그인함

<http://xx.xx.xxx.xxx/oam/ippbx.jnlp>

※ xx.xx.xxx.xxx는 IP-PBX에 부여된 IP주소임



[웹 기반의 사용자 관리시스템 패스워드 변경 화면]

- ② [1]Security Operator 메뉴 -> [2]변경할 USER\_ID 선택 -> [3]Change 버튼 클릭 -> [4]팝업창 정보 중 USER\_PWD

변경 -> [5]Change 버튼 클릭

## 예시 2) Addpac 게이트웨이 시스템 관리자 패스워드 변경방법

① 게이트웨이 시스템에 접속하여 관리자 패스워드를 변경함

[관련명령어]

단계	명령어	설명
1	# config	APOS 명령어 설정 모드로 전환한다.
2	(config)# user change <login-name> <old password> <new password>	Password를 변경하고자 하는 ID를 입력 후, password를 변경한다.

```
root# user change root old-password new-password
root#
```

[시스템 관리자 화면]

## □ 장비 접근제어 설정

ACL(Access Control List)은 게이트웨이 및 IP-PBX 등 인터넷전화 장비에 접근을 허용하는 대상을 관리하는 기능으로 인가된 사용자 및 장비만 호를 연결할 수 있도록 제한할 수 있음. 따라서 비인가 장비들의 접근으로 인한 인터넷전화 서비스의 불법사용을 차단하기 위해서는 반드시 설정해야 함

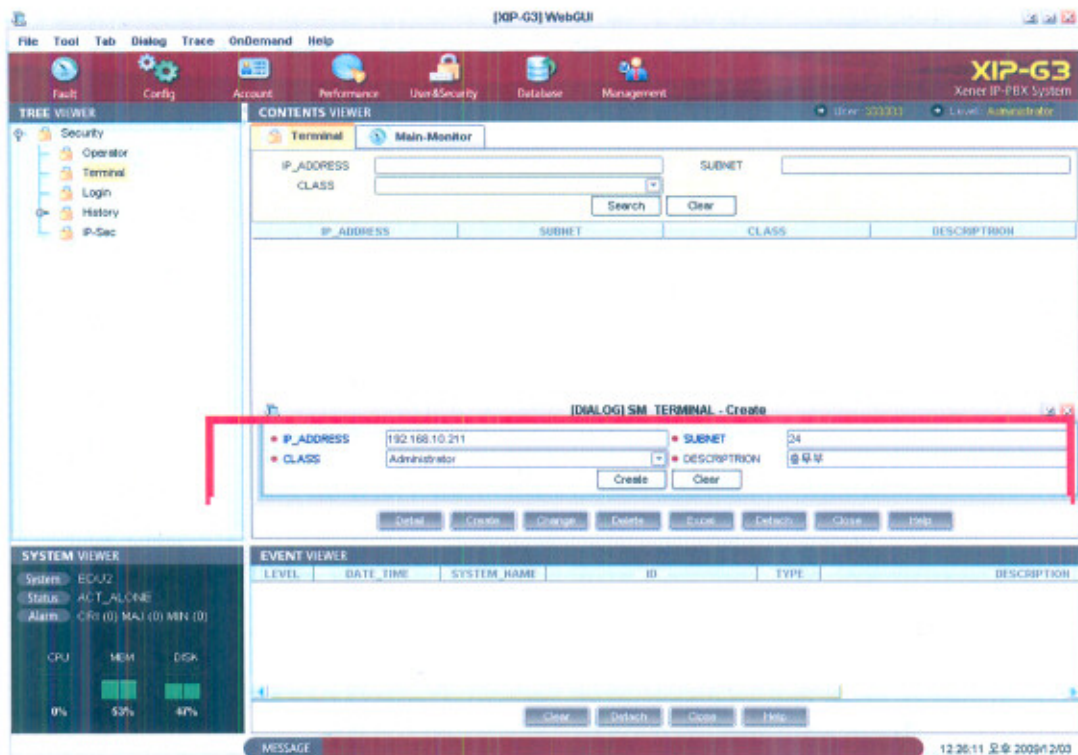
## 예시 1) 제너시스템즈의 IP-PBX시스템 접근제어 설정방법

① 웹 기반의 사용자 관리시스템에 접속하여 로그인함

<http://xx.xx.xxx.xxx/oam/ippbx.jnlp>

※ xx.xx.xxx.xxx는 IP-PBX에 부여된 IP주소임

② User & Security Terminal 메뉴에서 접근을 허용할 IP주소 입력 후, Create 버튼을 클릭함



[사용자 관리시스템 ACL 설정 화면]

- ※ IP-ADDRESS: IP-PBX로 트래픽 전송을 허용하는 장비의 IP주소를 입력해야 함
- ※ SUBNET: 트래픽 전송이 허용된 장비의 서브넷 마스크를 입력해야 함

## 예시 2) Addpac사의 게이트웨이 접근제어 설정방법

게이트웨이에 등록된 SSW(Proxy, G/K) 및 본-지사 간 구성을 위한 Routing-table의 Static IP-주소가 아닌 다른 IP-주소로부터 수신되는 메시지 차단 기능

### [관련명령어]

call-barring unconfigured-ip-address 기능 활성화

단계	명령어	설명
1	(config)# voice service voip	voice service voip 명령어 설정 모드로 전환한다.
2	(config-vservice-voip)# call-barring unconfigured-ip-address	해당 기능을 활성화 한다



## call-barring unconfigured-ip-address 기능 비활성화

단계	명령어	설명
1	(config-vservice-voip)# no call-barring unconfigured-ip-address	해당 기능을 비활성화 한다

### [IP접근제어 설정화면]

call-barring unconfigured-ip-address 설정 예	
AP2620#	
AP2620#	
AP2620# conf t	
Enter configuration commands, one per line. End with CNTL/Z	
AP2620(config)# voice service voip	
AP2620(config-vservice-voip)# call-barring unconfigured-ip-address	
AP2620(config)#	
AP2620(config)# exit	
AP2620#	
AP2620#	

## □ 상세 보안 설정 사항은 제조사 제공 매뉴얼 및 조치사항 참고

- o 제너시스시스템즈: <http://www.xener.com>
- o addpac: <http://www.addpac.com>
- o LG노텔: <http://www.lg-nortel.com>
- o 시스코: <http://www.cisco.com>
- o 네이블커뮤니케이션즈: <http://www.nablecomm.com>
- o Audio codes: <http://www.audiocodes.com>