전자금융감독규정시행세칙 개정안 관련 Q&A

(IT·핀테크전략국 디지털금융감독팀, '20.11.06.)

목 차

Ⅰ. 적용 범위

1. 외주 직원들도 재택근무가 가능한지? ····· 1

2. 시스템 개발자들도 재택근무가 가능한지? ····· 1

3. 회사 외부에 있는 외주업체에서 전산장비 유지보수를 담당하고 있는데, 이 경우에도 원격 접속하여 유지보수가 가능한지? ····· 1

4. IT직원이 개발·보안·운영 업무가 아닌 이메일, 그룹웨어 등의 업무시스템 사용 목적의 원격접속은 가능한지? ····· 2

5. 중요단말기도 원격접속이 가능한지? ····· 2

Ⅱ. 원격 접속 방식

6. 직접 접속 방식이 무엇인지? ····· 2

7. 간접 접속 방식이 무엇인지? ····· 3

8. 금융회사가 직접 접속, 간접 접속 방식으로 원격접속 방식할 수 있다고 하는데 권고하는 방식이 있는지? ····· 4

9. 시행세칙 제2조의2 제1항 제2호 '규정 제12조의 보안대책을 적용한 단말기'는 회사가 재택근무용으로 PC를 지급하라는 의미인지? ····· 4

10. 시행세칙 제2조의2 제1항 제2호 '전용회선과 동등한 보안 수준을 갖춘 통신망'은 가상사설망(VPN) 사용이 필수인지? ····· 5

Ⅲ. [별표7] 망분리 대체정보보호통제 관련

11. '업무용 단말기' 및 '외부 단말기'의 의미는? ····· 5

12. 개인 PC에도 백신 프로그램 설치 및 검사, 운영체제 버전, 로그인 비밀번호, 화면 보호기 설정 등의 보호대책을 적용해야 하는지? ····· 5

목 차

13. 안전한 운영체제 사용 및 최신 보안패치 적용은 운영체제를 최신버전만 사용해야 한다는 의미인지? ····· 5

14. 외부 단말기로 개인 PC 이용하는 경우 [별표7]의 외부단말기 공통 사항 중 '화면 및 출력물 등으로 인한 정보유출 방지대책 적용'을 위해 화면캡쳐 방지 보안프로그램 등을 적용해야 되는지? ····· 6

15. 평시에 회사에서 사용하는 업무용 단말기를 외부로 반출하여 재택근무시 이용할 수 있는지? ····· 6

16. '원격접속 기록'은 어떤 항목을 남기고 얼마동안 저장하여야 하는지? ····· 6

17. '이중 인증'의 인증수단으로는 어떤 것이 가능한지? ····· 7

18. 가상사설망은 인터넷 연결이 필수인데, '내부망 접속시 인터넷 연결 차단' 및 '인터넷 상시 차단'은 어떻게 구현할 수 있는지? ····· 7

19. 원격 접속 시 외부 단말기에서 업무상 불가피하게 인터넷 등 외부망에 연결해야 하는 경우에는 어떻게 처리해야 하는지? ····· 7

20. '공공장소에서 원격접속 금지'는 어떤 방식으로 준수할 수 있는지? ····· 7

21. 공공장소(커피숍,PC방 등)가 아닌 공유오피스 독립장소, 계열사 및 금융회사 다른 건물, 내부 회의실 등의 장소에서도 원격접속이 가능한지? ····· 8

Ⅳ. 기타

22. 시행세칙이 시행된 이후에도 코로나19로 인한 재택근무관련 비조치의견서('20.2월)가 유효한지? ····· 8

23. 현재 IT직원들은 코로나19 대응을 위해 비상대책에 따라 원격접속을 실시하고 있는데 시행세칙 시행 이후에도 코로나19가 종식되지 않을 경우 IT 직원들의 원격접속은 계속 가능한지? ····· 8

<참고> 망분리 관련 규정 및 시행세칙 ····· 9

Ⅰ. 적용 범위

1. 외주 직원들도 재택근무가 가능한지?

□ 외주 직원도 **재택근무 가능**함

○ 「전자금융감독규정시행세칙」(이하 '시행세칙') 제2조의2 제1항 제2호는 **모든 사내 업무용 단말기*에 대해 적용**되므로 단말기 사용자의 **소속에 따라 달리 적용되지 않음**

*「전자금융감독규정」 제15조 제1항 제3호의 내부통신망과 연결된 내부 업무용 시스템

2. 시스템 개발자들도 재택근무가 가능한지?

□ 전산실 내 **정보처리시스템을 직접 접속**하여 개발하는 경우 **원격 접속이 허용되지 않음**

○ 시행세칙 제2조의2 제1항은 「전자금융감독규정」(이하 '규정') 제15조 제1항 제3호의 망분리 적용을 예외로 하는 것으로, 동규정 제15조 제1항 제5호의 **물리적 망분리 적용 대상자는 해당되지 않음**

3. 회사 외부에 있는 외주업체에서 전산장비 유지보수를 담당하고 있는데, 이 경우에도 원격 접속하여 유지보수가 가능한지?

□ 정보처리시스템 **유지보수 목적**의 원격접속은 **불가**

○ 시행세칙 제2조의2 제2항 제3호에 따라 전산실내 정보처리시스템에 대한 원격접속은 장애 등 **비상상황에서만 가능**

4. IT직원이 개발·보안·운영 업무가 아닌 이메일, 그룹웨어 등의 업무시스템 사용 목적의 원격접속은 가능한지?

□ IT직원도 개발·보안·운영 업무가 아닌 이메일, 그룹웨어 등의 업무시스템 사용을 목적으로 원격 접속하는 것은 가능함

5. 중요단말기도 원격접속이 가능한지?

□ 규정 제12조에 따라 중요 단말기는 외부 반출, 인터넷 접속, 그룹웨어 접속을 금지하여야 하므로 **인터넷**을 통해 **외부 기관**과 **연결**하거나, **외부 반출하여 재택근무 할 수 없음**

○ 다만, 중요 단말기는 처리 업무의 종류 및 데이터의 중요도 등 **회사 자체 기준**에 따라 지정할 수 있음

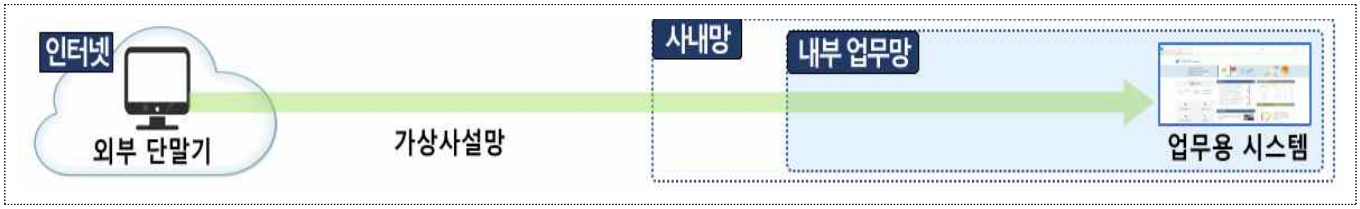
Ⅱ. 접속 방식

6. 직접 접속 방식이 무엇인지?

□ 외부 단말기가 가상사설망을 통해 **내부망의 노드(Node)로 직접 연결**

○ 외부 단말기는 **회사가** 보안 프로그램 설치, 보안 항목을 설정하여 **직접 지급**하여야 하며 **인터넷 연결을 항상 차단**하여야 함

< 직접 방식의 예시 >

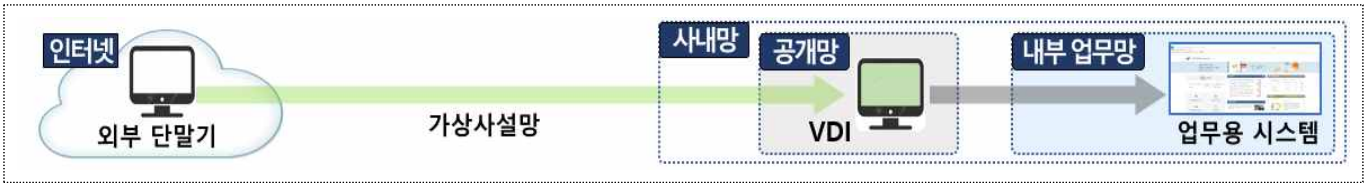


7. 간접 접속 방식이 무엇인지?

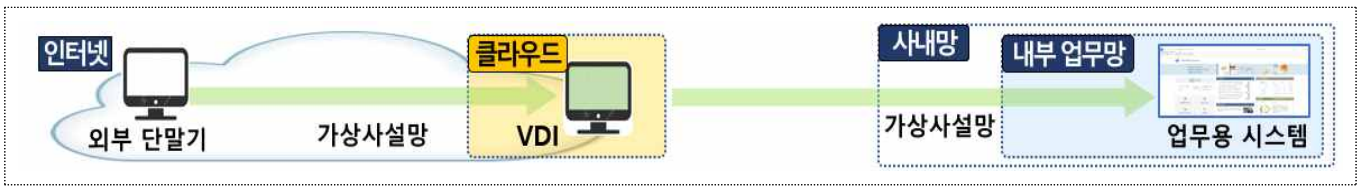
□ 외부 단말기가 **업무용 단말기를 경유**하여 내부망에 접속하는 것으로 외부 단말기는 **업무용 단말기의 입력 및 화면 출력만 처리**하고 업무용 단말기와 **파일 송수신이 차단**되어야 하며, **내부망 연결시 인터넷 연결을 차단**하여야 함

< 간접 방식의 예시 >

❶ 내부망과 분리된 원격접속 전용 VDI를 경유하여 내부망에 접속

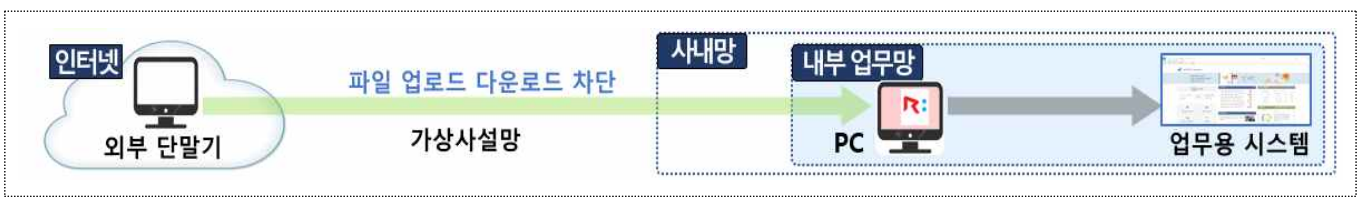


❷ 클라우드에 있는 원격접속 전용 VDI를 경유하여 내부망에 접속



❸ 내부망에 위치한 업무용 VDI로 접속

❹ 원격접속 프로그램을 통해 내부망 업무용 단말기로 접속



☞ ❹방식은 ❶~❸ 방식보다 보안상 취약할 수 있으므로 **원격접속 프로그램에 대한 보안성 점검, 기본 접속 포트 변경, 업무용 단말기의 미인가 조작을 차단하는 등 보안통제를 철저히 할 필요**

8. 금융회사가 직접 접속, 간접 접속 방식으로 원격접속 방식할 수 있다고 하는데 권고하는 방식이 있는지?

□ 회사 **시스템 환경에 따라** 관련 기반기술과 방식을 **자율적으로 선택**하여 이용할 수 있음

○ 원격접속 기술 및 구현 방식은 제한하지 않으나, **[별표7]의 망분리 대체 정보보호 통제**를 준수하여야 하여야 함

9. 시행세칙 제2조의2 제1항 제2호 '규정 제12조의 보안대책을 적용한 단말기'는 회사가 재택근무용으로 PC를 지급하라는 의미인지?

□ **개인PC도 이용할 수 있으나**, 원격접속 하는 외부 단말기는 규정 **제12조의 단말기 보호 대책 및 [별표7]을 준수**하여야 함

○ 다만 내부망에 자료를 전송할 수 없도록 통제장치가 되어 있는 경우(간접접속방식), 규정 제12조의 '보조기억매체 및 휴대용 전산장비 접근통제'는 외부 단말기에 적용하지 아니할 수 있음

10. 시행세칙 제2조의2 제1항 제2호 '전용회선과 동등한 보안 수준을 갖춘 통신망'은 가상사설망(VPN) 사용이 필수인지?

□ VPN 사용을 권고하나, ①전송 데이터의 기밀성 및 무결성 보장 ②클라이언트 및 서버 인증 처리 ③중간자 공격, 재생 공격을 예방할 수 있는 다른 방식의 암호 통신도 이용 가능

Ⅲ. [별표7] 망분리 대체 정보보호 통제 관련

11. '업무용 단말기' 및 '외부 단말기'의 의미는?

□ **'업무용 단말기'**란 회사 **내부통신망*에 위치한** Desktop, Laptop, Thin Client, VDI, 태블릿 등의 단말기 (규정 제15조제1항제3호 적용 대상)

* (**내부망**) 방화벽 등으로 외부망과 구분되어 회사 외부에서는 접근할 수 없고 회사가 통제할 수 있는 범위의 사설 네트워크으로 전산센터, 본사, 백업센터, 재해복구센터, 지점 등 전용선이나 전용 사설망으로 연결된 구간

□ **'외부 단말기'**란 회사 내부통신망으로 **원격 접속 시 이용**하는 **외부망에 위치한** Desktop, Laptop, Thin Client, VDI 태블릿 등의 단말기

12. 개인 PC에도 백신 프로그램 설치 및 검사, 운영체제 버전, 로그인 비밀번호, 화면 보호기 설정 등의 보호대책을 적용해야 하는지?

□ 적용해야 함, 망분리 예외적용으로 인한 각종 보안사고를 예방하기 위해서는 **개인 단말기**에 대해 **최소한의 보안 통제 적용**은 **필요**

○ 백신 설치·업데이트 및 안전한 운영체제 이용은 일반 인터넷 뱅킹 이용자에도 적용되는 사항으로 원격접속 하는 임직원 개인PC에서도 **충분히 적용 가능**하다고 판단됨

13. 안전한 운영체제 사용 및 최신 보안패치 적용은 운영체제를 최신버전만 사용해야 한다는 의미인지?

□ 최신 운영체제를 이용하여야 한다는 의미는 아니며, **기술지원이 종료된 운영체제**는 사용하지 말아야 하고 알려진 보안 취약점에 대한 **보안 패치**는 적용되어야 함

14. 외부 단말기로 개인 PC 이용하는 경우 [별표7]의 외부단말기 공통 사항 중 '화면 및 출력물 등으로 인한 정보유출 방지대책 적용'을 위해 화면캡쳐 방지 보안프로그램 등을 적용해야 되는지?

□ '화면 및 출력물 등으로 인한 정보유출 방지대책 적용'은 화면 캡쳐 방지 보안프로그램 이외에도 **다양한 방식을 이용할 수 있음**

○ 보안프로그램 설치 외 내부 업무용 시스템 및 업무용 단말기 등에 **마스킹 처리, 워터마크** 적용 등 기타 방법으로 화면 및 출력물 등으로 인한 정보유출 방지대책 적용이 가능함

15. 평시에 회사에서 사용하는 업무용 단말기를 외부로 반출하여 재택근무시 이용할 수 있는지?

□ **가능함,** 회사에서 사용하는 업무용 단말기를 **외부로 반출**하여 재택근무용으로 **이용할 수 있으나,**

○ [별표7] '외부 단말기' 통제와 '업무용 단말기' 통제 사항을 모두 적용하여야 하며

○ 반출한 단말기는 **인터넷 연결을 항상 차단**하고 재택근무 후 **회사로 재반입 시** 내부망 연결 전 **악성코드 진단 및 치료**를 실시하여야 함

16. '원격접속 기록'은 어떤 항목을 기록하여야 하고, 얼마동안 저장하여야 하는지?

□ 원격접속 **사용자의 정보, 접속 일시, 접속한 내부 시스템** 등을 포함하고 **1년 이상 보존** (전자금융감독규정 제13조 전산자료 보호대책)

17. '이중 인증'의 인증수단으로는 어떤 것이 가능한지?

□ 인증수단을 특정하지는 않고 있으나, 지식기반·소유기반·특징기반 인증수단 중 **서로 다른 방식**에 속하는 인증수단 **2개를 조합**

18. 가상사설망은 인터넷 연결이 필수인데, '내부망 접속시 인터넷 연결 차단' 및 '인터넷 상시 차단'은 어떻게 구현할 수 있는지?

□ VPN 터널링을 위한 인터넷 연결은 가능하나 **터널링 목적 이외의 인터넷은 차단**하여야 함

○ 인터넷 차단 방법은 보안 프로그램 등을 이용하여 회사가 자율적으로 선택할 수 있음

19. 원격 접속 시 외부 단말기에서 업무상 외부망에 연결해야 하는 경우에는 어떻게 처리해야 하는지?

□ 외부단말기에서 회사 내부 업무망에 접속 후 동 **내부망을 경유**하여 인터넷에 접속(**외부 단말기에서 직접 인터넷 접속 금지**)함으로써

○ 외부단말기에 회사의 기존 인터넷 보안 통제사항(유해 사이트 차단, 악성코드 방지대책 등) 등이 적용되도록 하여야 함

20. '공공장소에서 원격접속 금지'는 어떤 방식으로 준수할 수 있는지?

□ 기술적으로 강제할 수 없는 통제방안의 경우, 직원교육 등을 통해 보안의식 함양 및 책임감 부여

21. 공공장소(커피숍,PC방 등)가 아닌 공유오피스 독립장소, 계열사 및 금융회사 다른 건물, 내부 회의실 등의 장소에서도 원격접속이 가능한지?

□ 가능함, 재택근무 장소를 집으로 한정하는 것은 아니나 **단말기의 분실, 도난 및 모니터 노출에 의한 정보 유출, 유무선 공유기 취약점**등에 의한 **보안 사고 위험을 통제할 수 있는 장소**를 이용하여야 함

Ⅳ. 기타

22. 시행세칙이 시행된 이후에도 코로나19로 인한 재택근무관련 비조치의견서('20.2월)가 유효한지?

□ 시행세칙 개정안의 시행 시기인 **'21년 1월 1일 전까지 유효**함.

23. 현재 IT직원들은 코로나19 대응을 위해 비상대책에 따라 원격접속을 실시하고 있는데 시행세칙 시행 이후에도 코로나19가 종식되지 않을 경우 IT직원들의 원격접속은 계속 가능한지?

□ IT직원들은 장애·재해·파업·테러 등 긴급 상황 발생시 업무 연속성을 위하여 **회사 자체 비상계획**에 따라 원격접속 가능하며, 이는 이번 시행세칙 제2조의2 제1항 개정 이후에도 변동 없음

○ 다만, **'21년 1월 1일부터는 [별표7]의 개정된 사항을 반영**하여 원격접속을 실시하여야 함

<참고>

망분리 관련 규정 및 시행세칙

전자금융감독규정 제15조

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

3. 내부통신망과 연결된 내부 업무용 시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다) <개정2013.12.3.>

5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.) <신설 2013.12.3., 개정 2015.2.3.>

전자금융감독규정 시행세칙 제2조의2

제2조의2 (망분리 적용 예외) ① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 다음 각 호의 어느 하나와 같다

1. 내부 통신망에 연결된 단말기가 업무상 필수적으로 외부기관과 연결해야 하는 경우(다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다).

2. 규정 제12조의 보안대책을 적용한 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 외부망으로부터 내부 업무용시스템으로 원격접속 하는 경우

② 규정 제15조제1항제5호에서 금융감독원장이 인정하는 경우란 다음 각 호와 같다.

1. 「금융회사의 정보처리 업무 위탁에 관한 규정」에 따라 정보처리 업무를 국외 소재 전산센터에 위탁하여 처리하는 경우(다만, 해당 국외 소재 전산센터에 대해서는 물리적 방식 외의 방법으로 망을 분리하여야 하며, 이 경우에도 국내 소재 전산센터 및 정보처리시스템 등은 물리적으로 망을 분리하여야 한다)

2. 업무상 외부통신망과 연결이 불가피한 다음의 정보처리시스템(다만, 필요한 서비스번호(port)에 한하여 연결할 수 있다)

   가. 전자금융업무의 처리를 위하여 특정 외부기관과 데이터를 송수신하는 정보처리시스템

   나. DMZ구간 내 정보처리시스템과 실시간으로 데이터를 송수신하는 내부통신망의 정보처리시스템

   다. 다른 계열사(「금융회사의 정보처리 업무 위탁에 관한 규정」 제2조 제3항의 "계열사"를 말한다)와 공동으로 사용하는 정보처리시스템

3. 규정 제23조의 비상대책에 따라 원격 접속이 필요한 경우

4. 전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기와 외부통신망과의 연결 구간, 규정 제15조제1항제3호의 내부 업무용 시스템과의 연결 구간을 각각 차단한 경우

③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 <별표7>에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

<별표 7> 망분리 대체 정보보호통제

<table>
<tr><th>구분</th><th colspan="3">통제 사항</th></tr>
<tr><td>공통</td><td colspan="3">○ 외부망에서 내부망으로 전송되는 전산자료를 대상으로 악성코드 감염여부 진단·치료
○ 지능형 해킹(APT)차단 대책 수립·적용
○ 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링</td></tr>
<tr><td>메일 시스템</td><td colspan="3">○ 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립·적용
○ 메일을 통한 정보유출 탐지·차단·사후 모니터링 대책 수립·적용</td></tr>
<tr><td>업무용 단말기</td><td colspan="3">○ 사용자의 관리자 권한 제거
○ 승인된 프로그램만 설치·실행토록 대책 수립·적용
○ 전산자료 저장 시 암호화</td></tr>
<tr><td rowspan="6">원격 접속</td><td rowspan="3">외부 단말기</td><td>공통</td><td>○ 백신 프로그램 설치, 실시간 업데이트 및 검사 수행
○ 안전한 운영체제 사용 및 최신 보안패치 적용
○ 로그인 비밀번호 및 화면 보호기 설정
○ 화면 및 출력물 등으로 으로 인한 정보유출 방지대책 적용</td></tr>
<tr><td>업무용 단말기를 경유하여 내부망에 접속하는 경우 (간접접속)</td><td>○ 외부 단말기와 업무용 단말기의 파일 송·수신 차단</td></tr>
<tr><td>외부 단말기에서 내부망에 직접 접속하는 경우 (직접접속)</td><td>○ 인가되지 않은 S/W 설치 차단
○ 보안 설정 임의 변경 차단
○ USB 등 외부 저장장치 읽기/쓰기 차단
○ 전산자료 (파일, 문서) 암호화 저장
○ 단말기 분실 시 정보 유출 방지 대책적용 (하드디스크 암호화, CMOS비밀번호 적용 등)</td></tr>
<tr><td>내부망 접근통제</td><td colspan="2">○ 업무상 필수적인 IP, Port에 한하여 연결 허용
○ 원격접속 기록 및 저장(예: 접속자 ID, 접속일자, 접속 시스템 등)</td></tr>
<tr><td>인증</td><td colspan="2">○ 이중 인증 적용(예: ID/PW + OTP)
○ 일정 횟수(예 : 5회) 이상 인증 실패 시 접속 차단</td></tr>
<tr><td>통신 회선</td><td colspan="2">○ 안전한 알고리즘으로 네트워크 구간 암호화
○ 내부망 접속시 인터넷 연결 차단 (단, 직접 내부망으로 접속하는 원격 접속 단말기는 인터넷 연결 상시 차단)
○ 원격 접속 후 일정 유휴시간 경과 시 네트워크 연결 차단</td></tr>
<tr><td>기타</td><td colspan="2">○ 원격접속자에 대한 보안서약서 징구
○ 공공장소에서 원격 접속 금지</td></tr>
</table>