OO회사 ISMS-P 컨설팅 보고서

금융보안 환경의 Security Compliance Engineering(feat. MCP) 프로젝트

WHS 3기 27반 김서연_0720

출처	결함항목
인터뷰 질문	2.6.6 원격접근 통제
	2.6.1 네트워크 접근
	2.6.2 정보시스템 접근
개인정보처리시스템 현황 A	2.9.4. 로그 및 접속기록 관리
개인정보처리시스템 현황 B	2.7.1. 암호정책 적용
	2.5.1. 사용자 계정 관리
	2.5.5 특수 계정 및 권한 관리

<table>
<tr><td colspan="2">결함항목 개요</td></tr>
<tr><td colspan="2">[인터뷰 질문]
현재는 과도기적인 시기라 사용자는 회사, 집 등 원하는 환경에서 public 인터넷을 통해 시스템에 접속할 수 있도록 임시로 구성한 상태입니다.
언제 어디서든 개인정보처리자가 자율적 판단에 따라 정보시스템에 접속하여 실시간으로 승인된 사용자들의 행동을 모니터링하고, 시스템을 관리할 수 있도록 하고 있습니다</td></tr>
<tr><td>결함항목 제시</td><td>2.6.6 원격접근 통제</td></tr>
<tr><td>결함사항 도출</td><td>보호구역이 아닌 외부(집 등 원하는 환경)에서 원격접근이 제한 없이 허용되고 있음.</td></tr>
<tr><td>결함항목 인증기준</td><td>보호구역 이외 장소에서의 정보시스템 관리 및 개인정보 처리는 원칙적으로 금지하고, 재택근무/장애대응/원격협업 등 불가피한 사유로 원격접근을 허용하는 경우 책임자 승인 접근 단말 지정, 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화, 접속단말 보안(백신, 패치 등)등 보호 대책을 수립/이행하여야 한다.</td></tr>
<tr><td>개선방안 제안</td><td>1.인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하여야 하고, 불가피한 사유로 부득이하게 허용한다면 이에 대한 보완대책을 마련해야 한다.
2. 내부 네트워크를 사용하는 경우에도 시스템에 대한 원격 접근을 원칙적으로 금지하고, 불가피한 경우에는 책임자 승인, 접근 단말 지정, IP 기반의 접근통제를 통하여 승인된 사용자만 접근할 수 있도록 한다.
3. 승인된 사용자의 경우에도 접근 허용범위 및 기간 설정, 강화된 인증, 구간 암호화를 통해 보안을 강화한다.
4. 원격운영관리를 위하여 VPN를 구축하여 운영하고, VPN에 대한 사용 승인 또는 접속 기간 제한을 적용한다.</td></tr>
<tr><td colspan="2">인터뷰 질문</td></tr>
<tr><td colspan="2">1) 원격업무 수행 시 중요정보 유출, 해킹 등 침해사고 예방을 위한 보호대책을 수립/이행하고 있나요?
2) 개인정보처리시스템의 관리, 운영, 개발, 보안 등을 목적으로 원격으로 개인정보처리시스템에 직접 접속하는 단말기는 관리용 단말기로 지정하고 있나요?
3) 2)의 관리용 단말기에 임의조작 및 목적 외 사용 금지 등 안전조치를 적용하고 있나요?</td></tr>
</table>

<table>
<tr><td colspan="2">결함항목 개요</td></tr>
<tr><td colspan="2">[인터뷰 질문]
현재는 과도기적인 시기라 사용자는 회사, 집 등 원하는 환경에서 public 인터넷을 통해 시스템에 접속할 수 있도록 임시로 구성한 상태입니다.</td></tr>
<tr><td>결함항목 제시</td><td>2.6.1 네트워크 접근</td></tr>
<tr><td>결함사항 도출</td><td>중요 서버의 IP주소가 공인 IP로 설정되어 있고, 네트워크 접근 차단이 적용되어 있지 않음.</td></tr>
<tr><td>결함항목 인증기준</td><td>네트워크에 대한 비인가 접근을 통제하기 위하여 IP 관리, 단말 인증 등 관리절차를 수립/이행하고, 업무목적 및 중요도에 따라 네트워크 분리(DMZ, 서버팜, DB존, 개발존 등)와 접근통제를 적용하여야 한다.</td></tr>
<tr><td>개선방안 제안</td><td>1. 공인 IP를 사용하지 않고, 인가된 사용자만이 내부 네트워크에 접근할 수 있도록 통제한다.
2. 중요 서버의 IP주소는 내부 규정에 명시된 사설 IP를 사용하고 방화벽 등 네트워크 접근 차단장치를 사용하여 외부 네트워크 접근 차단을 적용한다.
2. 내부 규정에 명시된 VPN이나 전용망 등을 이용하여 데이터 송수신 및 통신을 처리한다.
3. MAC 주소 인증, 필수 보안 소프트웨어 설치등의 보호대책을 적용한다.</td></tr>
<tr><td colspan="2">인터뷰 질문</td></tr>
<tr><td colspan="2">1) 조직의 네트워크에 접근할 수 있는 모든 경로와 계정을 식별하고 있나요?
2) Public 인터넷으로 접속한 가능한 영역은 서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 접근통제를 적용한 후 Public으로 접근해도 좋다고 판단된 영역인가요?
(->아닐 시 논리적 분리 및 각 영역 간 접근 통제 적용)
3) 네트워크 대역별 IP주소 부여 기준이 마련되어 있나요?
4) 지금 public 인터넷으로 접근 가능한 정보시스템, 응용프로그램, 데이터베이스 현황이 어떻게 되나요?</td></tr>
</table>

<table>
<tr><td colspan="2">결함항목 개요</td></tr>
<tr><td colspan="2">[인터뷰 질문]
현재는 과도기적인 시기라 사용자는 회사, 집 등 원하는 환경에서 public 인터넷을 통해 시스템에 접속할 수 있도록 임시로 구성한 상태입니다.
언제 어디서든 개인정보처리자가 자율적 판단에 따라 정보시스템에 접속하여 실시간으로 승인된 사용자들의 행동을 모니터링하고, 시스템을 관리할 수 있도록 하고 있습니다</td></tr>
<tr><td>결함항목 제시</td><td>2.6.2 정보시스템 접근</td></tr>
<tr><td>결함사항 도출</td><td>시스템에 접속할 수 있는 사용자가 명확히 정의되어 있지 않음.
개인정보처리자가 실시간 승인 사용자 모니터링 시스템 등 주요 시스템에 접근할 때 통제 수단이 없음.</td></tr>
<tr><td>결함항목 인증기준</td><td>서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.</td></tr>
<tr><td>개선방안 제안</td><td>1.서버, 네트워크시스템, 모니터링시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
2. 서버 간 접속을 제한하여 인가된 사용자가 서버를 경유하여 다른 인가받지 않은 서버에 접속할 수 있는 경우를 제한하고, 모니터링한다.
3. 정보시스템에 접속 후 일정시간 업무처리를 하지 않는 경우 자동으로 시스템 접속을 차단한다.
4. 서버접근제어 시스템을 운영하고, 모든 서버로의 접근은 서버접근제어 시스템을 통하도록 한다.</td></tr>
<tr><td colspan="2">인터뷰 질문</td></tr>
<tr><td colspan="2">1) 정보시스템별 운영체제에 접근이 허용되는 사용자, 접근 가능 위치, 접근 수단 등이 정의되어 있고 통제되고 있나요?
2) 시스템에 접속하는 사용자와 개인정보처리자는 어떤 조건을 통해 정의하였나요? 이 조건이 내부 규정에 지정되어 있고 충족되고 있나요?
3) 개인정보처리자가 승인된 사용자들을 모니터링하기 위해 접속하는 정보시스템은 독립 서버로 운영되고 있나요?
4) 모든 서버로의 접근에 서버접근제어 시스템을 통하도록 접근통제 정책을 가져가고 있나요? 혹시 우회 경로는 없나요?</td></tr>
</table>

결함항목 개요	
[OO회사 개인정보처리시스템 현황 A] 접속로그관리	
결함항목 제시	2.9.4. 로그 및 접속기록 관리
결함사항 도출	모든 접속IP가 동일하게(192.168.1.3) 기록되어 실질적 사용자 단말, 실제 접속 위치/환경 식별이 불가. 개인정보처리시스템에 접속한 기록을 확인한 결과, 처리한 정보주체 정보에 관련된 정보를 남기고 있지 않음.
결함항목 인증기준	서버, 네트워크시스템 등 정보시스템에 접근을 허용하는 사용자, 접근제한 방식, 안전한 접근수단 등을 정의하여 통제하여야 한다.
개선방안 제안	1. 내부망에서 NAT, 프록시 등으로 인해 IP가 동일하게 보일 경우, MAC 주소, Hostname, OS 정보 등을 추가로 로그에 기록한다. 2.로그를 임의로 삭제 및 편집이 불가능하게 관리하고, 위변조 방지 기술을 적용한다. 3.로그 저장 위치와 운영시스템을 분리한다. 4. 개인정보처리시스템에 접속한 기록은 접속자의 계정, 접속 일시, 접속자 IP주소, 처리한 정보주체 정보 및 상세한 수행업무를 기록하여 책임추적성을 강화한다
인터뷰 질문	
1) 정보시스템의 로그기록은 별도 저장장치를 통해 백업하고 로그기록에 대한 접근권한은 최소화하여 부여하고 있나요? 관리자 말고 또 접근할 수 있는 사람이 있나요? 2) 로그를 임의로 삭제되거나 편집할 수 있나요? 3) 로그 기록 대상, 방법, 보존기간, 검토 주기, 담당자 등에 대한 세부 기준 및 절차가 수립되어 있나요? 4) 중요 로그에 대한 최대 크기를 충분하게 설정하고 있나요?	

결함항목 개요	
[OO회사 개인정보처리시스템 현황 B] Amazon RDS Custom	
결함항목 제시	2.7.1. 암호정책 적용
결함사항 도출	DES는 매우 오래된 알고리즘으로 안전하지 않음.
결함항목 인증기준	개인정보 및 주요 정보보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호강도, 암호사용 정책을 수립하고 개인정보 및 주요정보의 저장/전송/전달 시 암호화를 적용하여야 한다.
개선방안 제안	1. DES는 매우 짧은 56비트 키 길이를 사용하는 알고리즘으로 보안에 취약하다. 따라서 AES 등의 최신 강력한 암호화 알고리즘 사용이 권장된다.
인터뷰 질문	
1) DES가 법적 요구사항을 반영한 암호 알고리즘이 맞나요? 2) 암호키는 어떻게 관리하고 있나요? 3) 내부 정책/지침에 암호통제 관련 법적 요구사항을 고려한 암호화 대상, 암호강도, 저장 및 전송 시 암호화 방법, 암호화 관련 담당자의 역할 및 책임 등에 관한 사상이 적절히 명시되어 있나요? 4) 어떤 컬럼에 암호화를 적용하고 있나요?	

<table>
<tr><td colspan="2">결함항목 개요</td></tr>
<tr><td colspan="2">[OO회사 개인정보처리시스템 현황 B]
개인정보처리시스템에 접근할 수 있는 사용자 계정 목록에 일률적으로 권한 부여 및 관리</td></tr>
<tr><td rowspan="2">결함항목 제시</td><td>2.5.1. 사용자 계정 관리</td></tr>
<tr><td>2.5.5 특수 계정 및 권한 관리</td></tr>
<tr><td rowspan="2">결함사항 도출</td><td>개인정보처리시스템에 접근할 수 있는 사용자 계정에 일률적으로 모든 리소스에 모든 권한을 부여하여, 개인정보처리시스템 사용자에게 필요 이상의 과도한 권한을 부여하여 업무상 불필요한 정보 또는 개인정보에 접근이 가능함.</td></tr>
<tr><td>개인정보처리시스템의 관리자 및 특수권한 등의 승인 이력이 시스템 상으로 확인되지 않음.</td></tr>
<tr><td rowspan="2">결함항목 인증기준</td><td>정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록/해지 및 접근권한 부여/변경/말소 절차를 수립/이행하고, 사용자 등록 및 권한 부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.</td></tr>
<tr><td>정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.</td></tr>
<tr><td>개선방안 제안</td><td>1.최소 권한 원칙을 적용하여 모든 사용자 계정에 대해 업무상 필요한 최소한의 리소스/권한만 부여한다. IAM 정책에서 "Action": "*" 및 "Resource": "*"와 같은 광범위 권한 사용을 금지하고, 관리자/특수계정도 등록이 필요하되 역할별·업무별로 필요한 권한만 분리해 부여한다.
2. 계정의 등록, 권한 부여·변경·말소 등 일련의 절차는 책임자 승인 하에 이루어지도록 하고, 모든 처리 내역을 시스템에 자동으로 기록 및 보관하여 책임 추적성을 확보한다.
정기적으로 계정 및 권한 현황을 점검하여 불필요한 권한이나 장기 미사용 계정은 즉시 해지 또는 말소하며, 사용자 등록 시 보안 책임과 의무를 충분히 인식할 수 있도록 안내 및 서약을 실시한다.</td></tr>
<tr><td colspan="2">인터뷰 질문</td></tr>
<tr><td colspan="2">1) 개인정보처리시스템에 대한 사용자 계정 권한을 부여할 때, 어떤 기준과 절차에 따라 권한을 설정하나요?</td></tr>
</table>

2) 관리자/특수계정 운영이 필요할 것 같은데, 운영한다면 어떤 방식으로 식별 및 통제할 것인가요?
3) 사용자 계정, 권한 부여·변경·말소 이력은 시스템상에서 자동으로 기록/관리되고 있나요?
   관련 이력을 조회하는 방법을 보여줄 수 있나요?
4) 신규 계정 등록 시 사용자가 보안책임 및 의무를 인식하고 서약하도록 안내하는 절차가 있나요?
5) 정기적으로 불필요한 권한, 미사용 계정, 퇴직자 계정 등 계정 및 권한을 점검/정비하는 주기와 방법은 어떻게 되나요?