

**{{프로젝트명}}**

**전자금융기반시설 보안 취약점 종합 평가결과**

**{{출력일}}**

[붙임]

**차 례**

[I. 개 요 1](#_Toc48832794)

[1. 평가 목적 1](#_Toc48832795)

[2. 평가 일정 2](#_Toc48832796)

[3. 평가 인력 3](#_Toc48832797)

[II. 대상 및 방법 4](#_Toc48832798)

[1. 평가 대상 4](#_Toc48832799)

[2. 평가 방법 9](#_Toc48832800)

[3. 평가 기준 10](#_Toc48832801)

[4. 중점 점검사항 12](#_Toc48832802)

[III. 평가 결과 13](#_Toc48832803)

[1. 결과 총평 13](#_Toc48832804)

[2. 분야별 평가 결과 17](#_Toc48832805)

[IV. 평가 지수 22](#_Toc48832806)

[1. 분야별 평가 지수 22](#_Toc48832807)

[V. 보호대책 27](#_Toc48832808)

[1. 관리적 부문 27](#_Toc48832809)

[2. 물리적 부문 27](#_Toc48832810)

[3. 기술적 부문 28](#_Toc48832811)

[[참고] 보안 취약점 평가 지수 산출 기준 29](#_Toc48832812)

**[ 첨 부 ]**

{%p for li in 첨부파일%}

{{loop.index}}. {{li}}

{%p if loop.last %}

{%p if 모의해킹\_실시여부 == ‘실시’ %}

{{loop.index+1 }}. 모의해킹

{%p endif %}

{{loop.index+2}}. 전자금융기반시설 보안 취약점 목록

{{loop.index+3}}. 전자금융기반시설 보안 취약점 평가기준

{{loop.index+4}}. 전자금융기반시설 보안 취약점 평가 시작회의

{{loop.index+5}}. 전자금융기반시설 보안 취약점 평가 결과설명회

{%p endif %}

{%p endfor %}

|  |
| --- |
| **본 취약점 평가는 『금융보안원 보안 취약점 평가 방법론』에 의거하여 실시하였고, 금융보안원은 관계법령에 따라 비밀유지 의무를 준수하고 있습니다. 아울러 동 취약점 평가결과에 관한 활용은 취약점 신청기관에 있음을 알려드립니다.** |

개 요

평가 목적

○ 전자금융기반시설(이하 ‘기반시설’)에 대한 보안 취약점 분석·평가는 「전자금융거래법」 제21조의3에 근거하여 해킹, 악성코드 유포 등 전자금융거래의 안전성을 위협하는 사이버 침해 시도로부터 기반시설을 보호하기 위한 목적으로 실시함

|  |  |
| --- | --- |
| **관계 법령** |  |
| **【 전자금융거래법 】**  ▪제21조의3 (전자금융기반시설의 취약점 분석·평가)  ① 금융회사 및 전자금융업자는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자금융기반시설에 대한 다음 각 호의 사항을 분석·평가하고 그 결과(「정보통신기반 보호법」 제9조에 따른 취약점 분석·평가를 한 경우에는 그 결과를 말한다)를 금융위원회에 보고하여야 한다.  1. 정보기술부문의 조직, 시설 및 내부통제에 관한 사항  2. 정보기술부문의 전자적 장치 및 접근매체에 관한 사항  3. 전자금융거래의 유지를 위한 침해사고 대응조치에 관한 사항  4. 그 밖에 대통령령으로 정하는 사항  **【 전자금융거래법 시행령 】**  ▪ 제11조의4 (전자금융기반시설 취약점 분석·평가의 내용)  법 제21조의3제1항 제4호에서 "대통령령으로 정하는 사항"이란 다음 각 호의 사항을 말한다.  1. 정보기술부문과 연계된 전자금융보조업자의 정보처리시스템 등에 관한 사항  2. 그 밖에 전자금융거래의 안정성과 신뢰성을 확보하기 위하여 필요한 사항으로서 금융위원회가 정하여 고시하는 사항 | |

평가 일정

○ 일정 : {{시작일}} ∼ {{종료일}} ({{영업일}}영업일)

○ 인원수 : {{평가\_인력|length }}명

○ 공수 : {{적수}}적수(Man/Day)

|  |  |  |  |
| --- | --- | --- | --- |
| 기간  단계 | 1주차 | 2주차 | 3주차 |
| 00.00. ~ 00.00. | 00.00. ~ 00.00. | 00.00. ~ 00.00. |
| Ⅰ. 사전 분석 |  |  |  |
| **1. 계획 수립** |  |  |  |
| **2. 현황 파악** |  |  |  |
| Ⅱ. 취약점 분석 |  |  |  |
| **1. 정보보호 관리체계** |  |  |  |
| **2. 서버/데이터베이스** |  |  |  |
| **3. 네트워크 인프라,**  **네트워크/정보보호시스템 장비** |  |  |  |
| **4. 웹 애플리케이션** |  |  |  |
| **5. 모바일 애플리케이션** |  |  |  |
| **6. HTS 애플리케이션** |  |  |  |
| **7. 모의해킹** |  |  |  |
| Ⅲ. 취약점 평가 |  |  |  |
| **1. 취약점 평가** |  |  |  |
| **2. 보안대책 수립 및 협의** |  |  |  |
| **3. 보안 취약점 분석·평가 지수 산출** |  |  |  |
| Ⅳ. 결과서 작성 및 전달 |  |  |  |
| 1. **결과서 작성** |  |  |  |
| **2. 결과 설명회** |  |  |  |

평가 인력

|  |  |  |  |
| --- | --- | --- | --- |
| **소속기관** | **담당분야** | **직위** | **성명** |
| {%tr for x in 평가\_인력 %} | | | |
| {% vm %}금융보안원 | {{x.담당분야}} | {{x.직위}} | {{x.성명}} |
| {%tr endfor %} | | | |

대상 및 방법

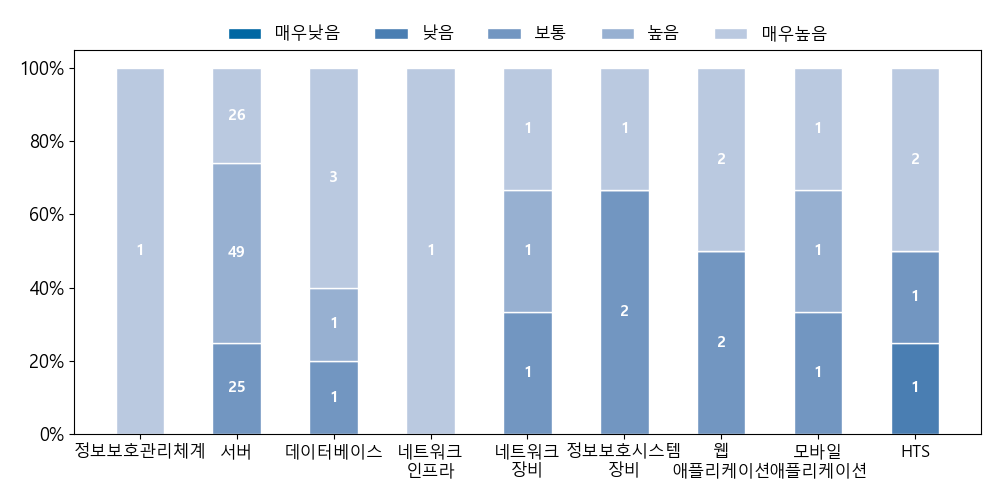
* 1. 평가 대상
     1. **분야별 평가 대상**

| 분야 | | 용도 | 수량 | 자산번호 | 평가  실시여부 |
| --- | --- | --- | --- | --- | --- |
| {%tr for x in 인프라\_영역 %} | | | | | |
| {% vm %}인프라 영역 | {{x.분야R}} | {{x.용도}} | {{x.수량}} | {{x.자산번호 }} | {{x.실시여부}} |
| {%tr endfor %} | | | | | |
| {%tr for x in 서비스\_영역 %} | | | | | |
| {% vm %}서비스 영역 | {{x.분야R}} | {{x.용도}} | {{x.수량}} | {{x.자산번호 }} | {{x.실시여부}} |
| {%tr endfor %} | | | | | |
| 기타 | 모의해킹 | | | | {{모의해킹\_실시여부}} |

* + 1. **분야별 자산 분석**

| 분야 | | **매우**  **높음(5)** | **높음(4)** | **보통(3)** | **낮음(2)** | **매우**  **낮음(1)** | 수량 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| {%tr for x in 인프라\_영역 %} | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | |
| {%vm%}인프라 영역 | {{x.분야}} | {{x.자산.5}} | {{x.자산.4}} | {{x.자산.3}} | {{x.자산.2}} | {{x.자산.1}} | {{x.자산합}} |
| {%tr endif %} | | | | | | | |
| {%tr endfor %} | | | | | | | |
| {%tr for x in 서비스\_영역 %} | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | |
| {%vm%}서비스 영역 | {{x.분야}} | {{x.자산.5}} | {{x.자산.4}} | {{x.자산.3}} | {{x.자산.2}} | {{x.자산.1}} | {{x.자산합}} |
| {%tr endif %} | | | | | | | |
| {%tr endfor %} | | | | | | | |
| **합계\*** | | {{통계.\_5}} | {{통계.\_4}} | {{통계.\_3}} | {{통계.\_2}} | {{통계.\_1}} | {{통계.\_total}} |

\* 정보보호관리체계, 네트워크 인프라, 모의해킹 분야는 합계에 포함되지 않음



* + 1. **분야별 환경분석 (기존 보호대책 중심)**

|  |  |  |
| --- | --- | --- |
| **분야** | | **내용** |
| {%tr for x in 인프라\_영역 %} | | |
| {%tr if x.실시여부==”실시” %} | | |
| {%vm%}인프라 영역 | {{x.분야R}} | {%p if x.분야!=”네트워크 인프라” and x.분야!=”정보보호시스템 장비”%}  {%p for z in x.환경분석 %}   * {{z.0}} - {{z.1}}   {%p endfor %}  {%p else %}  {%p for line in x.환경분석 %}   * {{line.0}}   {%p for idx in range(1, line | length) %}   * {{line[idx]}}   {%p endfor %}  {%p endfor %}  {%p endif %} |
| {%tr endif %} | | |
| {%tr endfor %} | | |
| {%tr for x in 서비스\_영역 %} | | |
| {%tr if x.실시여부==”실시” %} | | |
| {%vm%}서비스 영역 | {{x.분야R}} | {%p for z in x.환경분석 %}   * {{z.0}} - {{z.1}}   {%p endfor %} |
| {%tr endif %} | | |
| {%tr endfor %} | | |
| {%tr if 모의해킹\_여부==”실시” %} | | |
| 기타 | 모의해킹 | * 상기 내용 참고 |
| {%tr endif %} | | |

* 1. 평가 방법

**가. 평가 방법**

○ 「전자금융기반시설 보안 취약점 평가기준(2022-1호, 2021.12.)」 적용

**나. 평가 절차**

|  |  |  |
| --- | --- | --- |
| **평가 순서** | **평가 단계** | **주요 업무** |
|  |  |  |
| ① | 사전 분석 단계 | 평가계획 수립 및 업무현황 파악 등 |
|  | ▼ |  |
| ② | 취약점 분석 단계 | 자산분석, 취약점 분석 등 |
|  | ▼ |  |
| ③ | 취약점 평가 단계 | 정보보호 수준평가 등의 종합평가 |
|  | ▼ |  |
| ④ | 대책 수립 단계 | 발견된 취약점에 대한 보안대책 수립 등 |
|  | ▼ |  |
| ⑤ | 사후 관리 단계 | 발견된 취약점에 대한 조치계획 수립 등 |

* 1. 평가 기준

○ 전자금융기반시설 보안 취약점 평가기준 (2022-1호, 2021.12.) 적용

○ 총 {{수행분야}} 개 분야, {{통계.평가항목}}개 평가항목 적용

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **분야** | | **평가내용** | **평가항목** | | **구분** | | | | |
| **관리** | | **물리** | | **기술** |
| {%tr for x in 인프라\_영역 %} | | | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | | | |
| {%vm%}인프라 영역 | {{x.분야R}} | {%p for z in x.평가기준 %}   * {{z}}   {%p endfor %} | {{x.평가항목}} | {{x.관리}} | | {{x.물리}} | | {{x.기술}} | |
| {%tr endif %} | | | | | | | | | |
| {%tr endfor %} | | | | | | | | | |
| {%tr for x in 서비스\_영역 %} | | | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | | | |
| {%vm%} 서비스 영역 | {{x.분야R}} | {%p for z in x.평가기준 %}   * {{z}}   {%p endfor %} | {{x.평가항목}} | {{x.관리}} | | {{x.물리}} | | {{x.기술}} | |
| {%tr endif %} | | | | | | | | | |
| {%tr endfor %} | | | | | | | | | |
| {%tr if 모의해킹\_여부==”실시” %} | | | | | | | | | |
| 기타 | 모의해킹 | * 내·외부자에 의한 해킹 가능성 * 개인정보 절취 가능성 * 웹쉘 존재 여부 등 | - | - | | - | | - | |
| {%tr endif %} | | | | | | | | | |
| **합계** | | | {{통계.평가항목}} | {{통계.관리}} | | {{통계.물리}} | | {{통계.기술}} | |

* 1. 중점 점검사항
     1. **모의해킹으로 개인정보 유출가능성 점검**

○ 정보보호시스템 운용 실태 파악

- 탐지/차단 정책 적정성 점검

- 실시간 모니터링 여부 및 로그 분석

○ 개인정보 유출 가능성 점검

- 침해사고 사례를 반영한 시나리오 적용

- 개별 취약점을 조합해 DB접근 시도

- 데이터베이스 내 개인정보 암호화 여부 확인

* + 1. **금융회사 자체 취약점 체계 점검**

○ 내부 취약점 체계 점검

- 사내 정보보호 규정∙지침 검토

- 취약점 분석 인력 확보 확인

○ 금융보안원과 금융회사의 역할 분담 인식

- 금보원은 매년 1~2회 취약점 분석(최신 기법)

- 금융회사는 정기적/수시 취약점 분석

- 신규 서비스, 신규 인프라 장비 중점 점검

* + 1. **대고객용 전자금융거래 서비스 중점 점검**

○ 전년도 취약점 분석∙평가 결과 참조

- 전자금융 웹 애플리케이션 취약점 다수

- 개인정보 유출 위험 확인

○ 전자금융거래 서비스 중점 점검

- 불법 자금이체 가능성 점검

- 본인 인증 우회 테스트

1. 평가 결과
   1. 결과 총평

○ 전체 평가항목 {{통계.평가항목}}개 중, {{통계.취약점\_전체}}개({{통계.취약점\_종류}}개 종류)의 취약점이 발견

- 전자금융기반시설에 대한 취약률은 {{통계.취약률}}%

- {{통계.조치\_전체}}개 취약점은 평가기간 중 조치되어 잔여 취약점은 총 {{통계.잔여\_취약점}}개

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **분야** | | **대상** | **평가항목** | **취약점 통계 \*** | | | | | | | | |
| **취약점 (수)** | | | | | **취약점**  **(종류)** | **취약률** | **평가지수** | **평가등급** |
| **전체** | | **관리** | **물리** | **기술** |
| {%tr for x in 인프라\_영역 %} | | | | | | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | | | | | | |
| {%vm%}인프라영역 | {{x.분야R}} | {{x.수량}} | {{x.평가항목}} | {{x.취약점\_전체}} | {{x.취약점\_관리}} | | {{x.취약점\_물리}} | {{x.취약점\_기술}} | {{x.취약점\_종류}} | {{x.취약률}}% | {{x.평가지수}} | {{x.평가등급}} |
| {%tr endif %} | | | | | | | | | | | | |
| {%tr endfor %} | | | | | | | | | | | | |
| {%tr for x in 서비스\_영역 %} | | | | | | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | | | | | | |
| {%vm%}서비스영역 | {{x.분야R}} | {{x.수량}} | {{x.평가항목}} | {{x.취약점\_전체}} | {{x.취약점\_관리}} | | {{x.취약점\_물리}} | {{x.취약점\_기술}} | {{x.취약점\_종류}} | {{x.취약률}}% | {{x.평가지수}} | {{x.평가등급}} |
| {%tr endif %} | | | | | | | | | | | | |
| {%tr endfor %} | | | | | | | | | | | | |
| {%tr if 모의해킹\_여부==”실시” %} | | | | | | | | | | | | |
| 기타 | 모의해킹 | - | - | - | - | | - | - | - | - | - | - |
| {%tr endif %} | | | | | | | | | | | | |
| **합계** | | {{통계.\_total}} | {{통계.평가항목}} | {{통계.취약점\_전체}} | {{통계.취약점\_관리}} | | {{통계.취약점\_물리}} | {{통계.취약점\_기술}} | {{통계.취약점\_종류}} | {{통계.취약률}}% | - | - |

\* 평가지수 및 등급 산정시 정보보호관리체계, 네트워크 인프라, 모의해킹 분야는 포함되지 않음

○ 우선 조치가 필요한 취약점(위험도 4이상) : {{통계.핫픽스}}건 중 {{통계.조치\_핫픽스}}건 조치

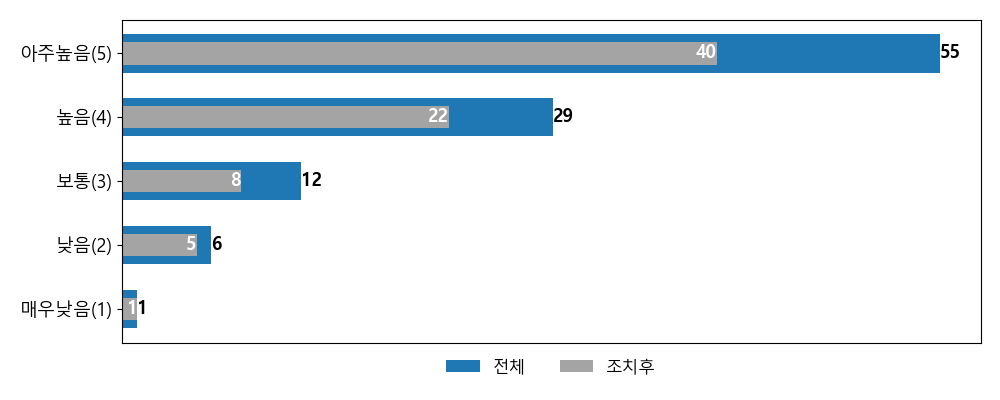
- 아주높음(5) : 중요 정보 노출, 웹/시스템 관리자 권한 획득 가능

- 높 음(4) : 웹/시스템 사용자 권한 획득 가능

- 보 통(3) : 다른 취약점과 연계될 경우 사용자권한 획득 가능

- 낮 음(2) : 2차 공격에 활용 가능한 중요 정보 노출

- 아주낮음(1) : 공격과 직접적인 연관은 없으나 단순 정보 노출



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **분야** | | **대상** | **평가**  **항목** | **취약점 통계** | | | | | |  | **조치\* 통계** | | | | | |
| **취약점(수)** | | | | **취약점(종류)** | **취약률** |  | **조치(수)** | | | | **조치**  **(종류)** | **조치율** |
| **전체** | **관리** | **물리** | **기술** |  | **전체** | **관리** | **물리** | **기술** |
| {%tr for x in 인프라\_영역 %} | | | | | | | | | | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | | | | | | | | | | |
| {%vm%}인프라 영역 | {{x.분야R}} | {{x.수량}} | {{x.평가항목}} | {{x.취약점\_전체}} | {{x.취약점\_관리}} | {{x.취약점\_물리}} | {{x.취약점\_기술}} | {{x.취약점\_종류}} | {{x.취약률}}% |  | {{x.조치\_전체}} | {{x.조치\_관리}} | {{x.조치\_물리}} | {{x.조치\_기술}} | {{x.조치\_종류}} | {{x.조치율}}% |
| {%tr endif %} | | | | | | | | | | | | | | | | |
| {%tr endfor %} | | | | | | | | | | | | | | | | |
| {%tr for x in 서비스\_영역 %} | | | | | | | | | | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | | | | | | | | | | |
| {%vm%}서비스 영역 | {{x.분야R}} | {{x.수량}} | {{x.평가항목}} | {{x.취약점\_전체}} | {{x.취약점\_관리}} | {{x.취약점\_물리}} | {{x.취약점\_기술}} | {{x.취약점\_종류}} | {{x.취약률}}% |  | {{x.조치\_전체}} | {{x.조치\_관리}} | {{x.조치\_물리}} | {{x.조치\_기술}} | {{x.조치\_종류}} | {{x.조치율}}% |
| {%tr endif %} | | | | | | | | | | | | | | | | |
| {%tr endfor %} | | | | | | | | | | | | | | | | |
| **합계** | | {{통계.\_total}} | {{통계.평가항목}} | {{통계.취약점\_전체}} | {{통계.취약점\_관리}} | {{통계.취약점\_물리}} | {{통계.취약점\_기술}} | {{통계.취약점\_종류}} | {{통계.취약률}}% |  | {{통계.조치\_전체}} | {{통계.조치\_관리}} | {{통계.조치\_물리}} | {{통계.조치\_기술}} | {{통계.조치\_종류}} | {{통계.조치율}}% |

\* 평가기간 중 현장에서 즉시 조치된 취약점을 의미

* 1. 분야별 평가 결과

{%p for x in 인프라\_영역 %}

{%p if x.분야 == “정보보호관리체계” and x.실시여부 ==”실시” %}

* + 1. **정보보호관리체계**

{%p for li in x.결과\_총평 %}

○ {{li}}

{%p endfor %}

○ 평가 결과

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **평가항목 수** | | **취약점 수** | **취약점 종류** | **취약률** |
| {%tr if x.조치 == ‘Y’ %} | | | | |
| **{{x.평가항목}}** | 분석시 | {{x.취약점\_전체}} | {{x.취약점\_종류}} | {{x.취약률}}% |
| 조치후 | {{x.AP\_취약점\_수}} | {{x.AP\_취약점\_종류}} | {{x.AP\_취약률}}% |
| {%tr else %} | | | | |
| **{{x.평가항목}}** | | {{x.취약점\_전체}} | {{x.취약점\_종류}} | {{x.취약률}}% |
| {%tr endif %} | | |

○ 주요 취약점

|  |  |  |  |
| --- | --- | --- | --- |
| **취약점ID** | **세부구분** | **평가항목** | **문제점** |
| {%tr for li in x.주요\_취약점 %} | | | |
| {{li. vulnerability\_item\_\_code}} | {{li. vulnerability\_item\_\_category}} | {{li. vulnerability\_item\_\_name}} | **((직접 입력))** |
| {%tr endfor %} | | | |

{%p endif %}

{%p endfor%}

{%p for x in 인프라\_영역 %}

{%p if x.실시여부 ==”실시” and x.분야 != “정보보호관리체계” %}

* + 1. **{{x.분야}}**

{%p for li in x.결과\_총평 %}

○ {{li}}

{%p endfor %}

○ 평가 결과

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **평가항목 수** | | **취약점 수** | **취약점 종류** | **취약률** |
| {%tr if x.조치 == ‘Y’ %} | | | | |
| **{{x.평가항목}}** | 분석시 | {{x.취약점\_전체}} | {{x.취약점\_종류}} | {{x.취약률}}% |
| 조치후 | {{x.AP\_취약점\_수}} | {{x.AP\_취약점\_종류}} | {{x.AP\_취약률}}% |
| {%tr else %} | | | | |
| **{{x.평가항목}}** | | {{x.취약점\_전체}} | {{x.취약점\_종류}} | {{x.취약률}}% |
| {%tr endif %} | | |

○ 주요 취약점 {% if x.TOP10 == ‘Y’ %}TOP10 {% endif %}

|  |  |  |  |
| --- | --- | --- | --- |
| **취약점ID** | **평가항목** | **위험도** | **발생빈도** |
| {%tr for li in x.주요\_취약점 %} | | | |
| {{li. vulnerability\_item\_\_code}} | {{li. vulnerability\_item\_\_name}} | {{li. vulnerability\_item\_\_risk}} | {{li. vulnerable\_asset\_count}} |
| {%tr endfor %} | | | |

{%p endif %}

{%p endfor%}

{%p for x in 서비스\_영역 %}

{%p if x.실시여부 ==”실시” and x.분야 != “정보보호 관리체계” %}

* + 1. **{{x.분야}}**

{%p for li in x.결과\_총평 %}

○ {{li}}

{%p endfor %}

○ 평가 결과

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **평가항목 수** | | **취약점 수** | **취약점 종류** | **취약률** |
| {%tr if x.조치 == ‘Y’ %} | | | | |
| **{{x.평가항목}}** | 분석시 | {{x.취약점\_전체}} | {{x.취약점\_종류}} | {{x.취약률}}% |
| 조치후 | {{x.AP\_취약점\_수}} | {{x.AP\_취약점\_종류}} | {{x.AP\_취약률}}% |
| {%tr else %} | | | | |
| **{{x.평가항목}}** | | {{x.취약점\_전체}} | {{x.취약점\_종류}} | {{x.취약률}}% |
| {%tr endif %} | | |

○ 주요 취약점 {% if x.TOP10 == ‘Y’ %}TOP10 {% endif %}

|  |  |  |  |
| --- | --- | --- | --- |
| **취약점ID** | **평가항목** | **위험도** | **발생빈도** |
| {%tr for li in x.주요\_취약점 %} | | | |
| {{li. vulnerability\_item\_\_code}} | {{li. vulnerability\_item\_\_name}} | {{li. vulnerability\_item\_\_risk}} | {{li. vulnerable\_asset\_count}} |
| {%tr endfor %} | | | |

{%p endif %}

{%p endfor%}

{%p if 모의해킹\_실시여부==”실시” %}

* + 1. **모의해킹 (예시)**

○ 외부 모의해킹 점검결과, 업무 관련 정보 및 시스템 사용자/웹 관리자 권한 획득 가능

○ 내부 모의해킹 점검결과, 개발 중인 웹 서비스 권한 및 프린터 관리자 권한 획득 가능

○ 모의해킹 결과, 3가지 시나리오로 공격이 가능함

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구분** | **시나리오** | | **취약점명** | **조치여부** |
| 외부모의해킹 | 시나리오 A | 메일 홈페이지에 악성코드 설치를 통한 시스템 사용자 권한 획득 | PT1-WCE-003 : 파일 업로드를 통한 시스템 명령 실행 | 미조치 |
| 시나리오 B | 메일 관리자 페이지 웹 관리자 권한 획득 및 업무정보 유출 | PT1-WCE-003 : 파일 업로드를 통한 시스템 명령 실행 | 미조치 |
| PT1-WCE-003 : 파일 업로드를 통한 시스템 명령 실행 | 미조치 |
| PT1-WCE-003 : 파일 업로드를 통한 시스템 명령 실행 | 미조치 |
| 내부모의해킹 | 시나리오 C | 메일 관리자 페이지 웹 관리자 권한 획득 및 업무정보 유출 | PT1-WCE-003 : 파일 업로드를 통한 시스템 명령 실행 | 미조치 |
| PT1-WCE-003 : 파일 업로드를 통한 시스템 명령 실행 | 미조치 |
| PT1-WCE-003 : 파일 업로드를 통한 시스템 명령 실행 | 미조치 |

○ WEB/WAS서버 내 웹쉘(악성코드) 존재 여부 점검

- 점검결과, 발견된 웹쉘(악성코드) 없음

|  |  |  |  |
| --- | --- | --- | --- |
| **자산번호** | **용도** | **IP주소** | **점검 결과\*** |
| **디렉터리 경로** | **대상 URL** |
| S46 | 인터넷뱅킹1 | 192.168.254.148 | ○ |
| /wwwroot/opencompany\_war/ | https://moa.banking.company.or.kr |
| S47 | 인터넷뱅킹2 | 192.168.254.149 | ○ |
| /wwwroot/opencompany\_war/ | https://moa.banking.company.or.kr |
| S48 | 홈페이지 | 222.231.31.80 | ○ |
| d:\wwwroot\company | http://www.company.or.kr/ |

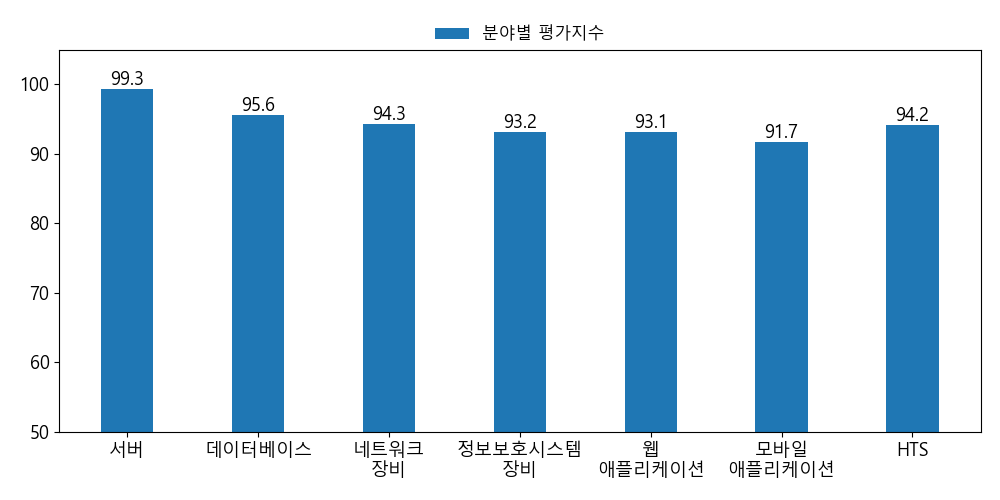
※ ○ : 웹쉘 미발견, X : 웹쉘 발견, N/A : 점검불가

{%p endif %}

1. 평가 지수
   1. **분야별 평가 지수**

○ 분야별 평가지수 및 등급

|  |  |  |  |
| --- | --- | --- | --- |
| 평가분야 | | **평가 지수** | 평가 등급 |
| {%tr for x in 인프라\_영역 %} | | | |
| {%tr if x.실시여부==”실시” %} | | | |
| {%vm%}인프라 영역 | {{x.분야}} | {{x.평가지수}} | {{x.평가등급}} |
| {%tr endif %} | | | |
| {%tr endfor %} | | | |
| {%tr for x in 서비스\_영역 %} | | | |
| {%tr if x.실시여부==”실시” %} | | | |
| {%vm%}서비스 영역 | {{x.분야}} | {{x.평가지수}} | {{x.평가등급}} |
| {%tr endif %} | | | |
| {%tr endfor %} | | | |
| **합 계** | | **{{통계.평가지수}}** | **{{통계.평가등급}}** |



{%p if 통계.기존 == “Y” %}

○ 분야별 기존/신규 평가 지수 비교

- 평가분야 평균 지수의 합은 기존 {{통계.기존\_평가지수}}, 신규 {{통계.신규\_평가지수}}로 나타남

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **분야** | | **기존 평가 대상\*** | | | **신규 평가 대상\*** | | |
| **자산수** | **평가**  **항목** | **평가**  **지수** | **자산수** | **평가**  **항목** | **평가**  **지수** |
| {%tr for x in 인프라\_영역 %} | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | |
| {%vm%}인프라 영역 | {{x.분야R}} | {{x.기존\_자산}} | {{x.기존\_평가항목}} | {{x.기존\_평가지수}} | {{x.신규\_자산}} | {{x.신규\_평가항목}} | {{x.신규\_평가지수}} |
| {%tr endif %} | | | | | | | |
| {%tr endfor %} | | | | | | | |
| {%tr for x in 서비스\_영역 %} | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | |
| {%vm%}서비스 영역 | {{x.분야R}} | {{x.기존\_자산}} | {{x.기존\_평가항목}} | {{x.기존\_평가지수}} | {{x.신규\_자산}} | {{x.신규\_평가항목}} | {{x.신규\_평가지수}} |
| {%tr endif %} | | | | | | | |
| {%tr endfor %} | | | | | | | |
| **합계**  **(분야별 평가지수의 평균값)** | | {{통계.기존\_자산}} | {{통계.기존\_평가항목}} | {{통계.기존\_평가지수}} | {{통계.신규\_자산}} | {{통계.신규\_평가항목}} | {{통계.신규\_평가지수}} |

\* (기존 평가 대상) 전년도에 점검한 대상, / (신규 평가 대상) 금년도에 처음 점검한 대상

○ 취약점 재발견율

- 전체 취약점 재발견율\*은 {{통계.재발견율}}%로 나타남

\* 재발견율 : 기존 평가대상의 취약점(A) 중 전년도와 동일하게 발견된 취약점(B)의 비율

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **평가분야** | | **기존 평가대상** | | | | | |
| **자산수** | **평가**  **항목** | **취약점(A)** | **재발견취약점(B)** | **재발견율(B/A)** | **평가**  **지수**  **(재발견율 반영)** |
| {%tr for x in 인프라\_영역 %} | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | |
| {%vm%}인프라 영역 | {{x.분야R}} | {{x.기존\_자산}} | {{x.기존\_평가항목}} | {{x.기존\_자산\_취약점\_수}} | {{x.재발견\_취약점}} | {{x.재발견율}} | {{x.재발견\_평가지수}} |
| {%tr endif %} | | | | | | | |
| {%tr endfor %} | | | | | | | |
| {%tr for x in 서비스\_영역 %} | | | | | | | |
| {%tr if x.실시여부==”실시” %} | | | | | | | |
| {%vm%}서비스 영역 | {{x.분야R}} | {{x.기존\_자산}} | {{x.기존\_평가항목}} | {{x.기존\_자산\_취약점\_수}} | {{x.재발견\_취약점}} | {{x.재발견율}} | {{x.재발견\_평가지수}} |
| {%tr endif %} | | | | | | | |
| {%tr endfor %} | | | | | | | |

○ 재발견 취약점 {% if 통계.재발견\_TOP10 == ‘Y’ %}TOP10 {% endif %}

|  |  |  |  |
| --- | --- | --- | --- |
| **취약점ID** | **평가항목** | **위험도** | **발생빈도** |
| {%tr for li in 통계.재발견\_취약점 %} | | | |
| {{li. vulnerability\_item\_\_code}} | {{li. vulnerability\_item\_\_name}} | {{li. vulnerability\_item\_\_risk}} | {{li. vulnerable\_asset\_count}} |
| {%tr endfor %} | | | |

{%p endif %}

1. 보호대책
   1. 관리적 부문

|  |  |  |
| --- | --- | --- |
| **구분** | **문제점** | **보호대책** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |

* 1. 물리적 부문

|  |  |  |
| --- | --- | --- |
| **구분** | **문제점** | **보호대책** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |

* 1. 기술적 부문

|  |  |  |
| --- | --- | --- |
| **구분** | **문제점** | **보호대책** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |
| **((직접 입력))** | **((직접 입력))** | **((직접 입력))** |

**[참고] 보안 취약점 평가 지수 산출 기준**

**1. 자산가치 평가항목**

○ 자산가치 산출방법

|  |
| --- |
| 자산가치 = 자산 중요도 ＋ 정보 성격 ＋ 가용성 수준 |

|  |
| --- |
| ▪ 자산 중요도 = 자산의 상대적 중요도를 기준으로 구분  ▪ 정보 성격 = 어떤 한 곳에 집적되어 있을 때 위험성이 커지는 정보의 특성과 정보 자체가 가지고 있는 민감성을 동시에 고려하여 정보 성격을 구분  ▪가용성 수준 = 해당 시스템이 업무연속성 유지차원에서 제공하는 가용성의 정도를 산정 자산가치 |

2. 평가분야별 지수 산출기준

○ 취약도 및 취약도율

|  |
| --- |
|  |

|  |
| --- |
| ▪ 취약도  ▪ 취약도율  ▪ 자산가치  ▪ 취약점 위험도  ▪ 취약점 보유여부 또는 취약률 |

○ 기존 및 신규 대상의 평가분야별 지수 산출식

|  |
| --- |
|  |

|  |
| --- |
| ▪ 기존 및 신규 대상의 평가분야별 지수  ▪ 자산가치  ▪ 취약점 위험도  ▪ 취약점 보유여부 또는 취약비율  ▪ 자산 개수  ▪ 취약점 개수 |

○ 재발견율 산출식

|  |
| --- |
|  |

|  |
| --- |
| 평가분야에 대한 재발견율  평가분야에 대한 재발견 취약점 개수  평가분야에 대한 취약점 개수 |

○ 기존 대상 평가분야별 지수의 재발견율을 반영한 산출식

|  |
| --- |
| → (재발견율 미반영)      → |

|  |
| --- |
| ▪ 기존 대상의 평가분야별 지수  ▪ 신규 대상의 평가분야별 지수  ▪ 평가분야에 대한 재발견율 |

○ 평가분야별 지수 산출식

|  |
| --- |
|  |

|  |
| --- |
| ▪ 평가분야의 지수  ▪ 평가분야별 기존 대상의 지수  ▪ 평가분야별 신규 대상의 지수  ▪ 평가분야별 기존 대상의 자산 개수  ▪ 평가분야별 신규 대상의 자산 개수 |

○ 보안 취약점 분석·평가 지수 및 등급 환산 기준

|  |  |
| --- | --- |
| **취약점 분석‧평가 지수** | 평가 등급 |
| 90 ～ 100 | 1등급 |
| 80 ～ 90 미만 | 2등급 |
| 70 ～ 80 미만 | 3등급 |
| 60 ～ 70 미만 | 4등급 |
| 60 미만 | 5등급 |