2025년 금융 시스템 리스크 분석: '디지털 블랙스완' 시나리오 심층 보고서

목차

서론: 보이지 않는 위협, 디지털 블랙스완의 도래

디지털 전환(Digital Transformation)은 금융 산업의 효율성을 전례 없는 수준으로 끌어올렸습니다. 실시간 결제, 알고리즘 트레이딩, 클라우드 기반 핵심 뱅킹 시스템은 이제 거스를 수 없는 흐름이 되었습니다. 그러나 이 빛나는 혁신의 이면에는, 과거에는 상상조차 할 수 없었던 새로운 형태의 시스템 리스크가 그림자처럼 도사리고 있습니다. 우리는 고도로 연결되고 상호 의존적인 디지털 금융 생태계 속에서, 단 하나의 균열이 전체 시스템의 붕괴를 초래할 수 있는 취약성에 노출되어 있습니다.

본 보고서는 이러한 보이지 않는 위협 중 가장 치명적인 시나리오, 즉 '디지털 블랙스완(Digital Black Swan)'의 위험을 심층적으로 분석하고, 이에 대비하기 위한 실질적인 데이터 기반 리스크 관리 프레임워크를 제시하는 것을 목표로 합니다. 여기서 ';디지털 블랙스완'이란, 참고 자료에서 정의된 바와 같이, 발생 확률은 극히 낮지만 일단 발생하면 금융 시스템 전체를 마비시킬 수 있는 '핵심 금융 인프라에 대한 시스템적 사이버 공격'을 의미합니다. 이는 단순한 데이터 유출이나 일시적인 서비스 장애를 넘어, 거래 기록의 위변조를 통해 금융 시스템의 근간인 '신뢰(Trust)' 자체를 파괴하는, 예측 불가능하고 극단적인 파급효과를 낳는 사건입니다.

본 보고서의 목적은 단순한 이론적 논의에 그치지 않습니다. 은행의 리스크 관리자가 현업에서 즉시 활용할 수 있도록, 제공된 참고 자료(`stress_test_scenarios_4`, `Indicators.xlsx` 등)를 기반으로 구체적인 모니터링 지표, 조기 경보를 위한 뉴스 키워드, 그리고 위기 발생 시 실행 가능한 대응 방안을 체계적으로 제시하고자 합니다. 2025년, 인플레이션이나 지정학적 리스크와 같은 전통적인 위협 요인만큼이나, 혹은 그 이상으로 은행의 생존을 위협할 수 있는 이 디지털 특이점(Singularity)에 대한 철저한 분석과 대비가 왜 필수적인지, 본 보고서를 통해 명확히 이해하게 될 것입니다.

핵심 분석: '디지털 블랙스완' 시나리오 해부 및 모니터링 체계 구축

이 섹션은 본 보고서의 핵심으로, '디지털 블랙스완' 시나리오가 어떤 논리적 경로를 통해 현실화될 수 있는지, 그리고 그 파괴적인 연쇄 반응을 조기에 감지하기 위해 우리는 무엇을 어떻게 관찰해야 하는지에 대해 심층적으로 분석합니다. 이는 정량적 데이터와 정성적 정보를 결합한 다차원적 접근을 통해, 보이지 않는 위협을 가시적인 관리 대상으로 전환하는 과정입니다.

시나리오의 논리적 근거와 전개 과정 심층 분석

본 시나리오는 우연한 사고가 아닌, 명확한 의도를 가진 공격 주체에 의해 촉발됩니다. 참고 자료 '시나리오 3'에서 언급된 바와 같이, 특정 국가의 지원을 받는 고도로 정교한 해킹 그룹(Advanced Persistent Threat, APT)이 공격의 배후로 상정됩니다. 이들의 목표는 금전적 이득이나 단순한 혼란 야기를 넘어, 경쟁국의 금융 시스템을 마비시키고 글로벌 금융 패권에 도전하는 지정학적 목적을 가질 수 있습니다.

충격의 원인: 왜 핵심 금융 인프라(CFI)인가?

공격자들은 최대의 파급효과를 위해 금융 시스템의 가장 취약한 '단일 실패점(Single Point of Failure)'을 노립니다. 이들이 주목하는 핵심 금융 인프라(Critical Financial Infrastructure, CFI)는 다음과 같은 기관들입니다.

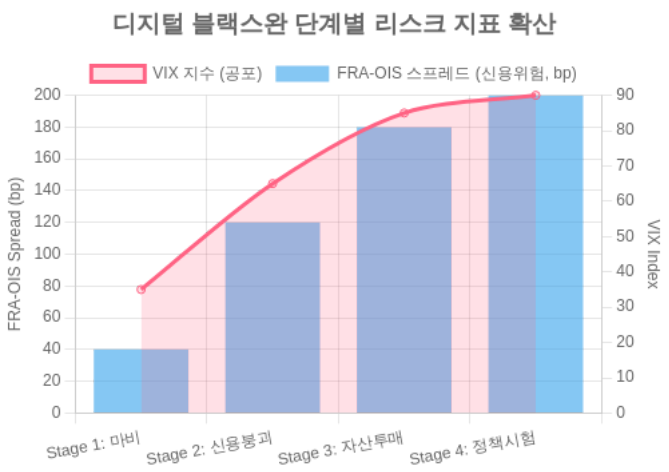
- **중앙예탁청산기관 (CCP: Central Counterparty Clearing House):** 미국의 DTCC, 유럽의 Euroclear와 같이 수많은 증권 및 파생상품 거래의 중심에서 거래 상대방 리스크를 흡수하고 최종 결제를 보증하는 기관입니다. CCP의 기능 마비는 곧 시장 전체의 거래 불능을 의미합니다.
- **글로벌 은행간 결제망 (SWIFT):** 전 세계 은행들이 국경 간 자금 이체를 위해 사용하는 메시징 네트워크입니다. SWIFT의 중단이나 데이터 위변조는 국제 무역과 금융 거래의 혈맥을 끊는 것과 같습니다.
- **핵심 클라우드 서비스 제공자 (CSP):** Amazon Web Services (AWS), Microsoft Azure, Google Cloud 등 다수의 대형 은행들이 핵심 뱅킹 시스템과 데이터를 위탁 운영하는 클라우드 플랫폼입니다. 특정 CSP의 광범위한 장애는 해당 서비스를 이용하는 모든 금융기관의 동시 다발적인 운영 마비를 초래할 수 있습니다.

이러한 CFI에 대한 공격은 단순한 서비스 거부(DDoS) 공격을 넘어, 시스템 내부에 침투하여 거래 기록을 대규모로 위변조하거나, 백업 시스템까지 파괴하여 복구를 불가능하게 만드는 파괴적인(destructive) 형태를 띨 것입니다. 이는 금융 시스템의 근간인 '거래의 무결성(Integrity)'과 '신뢰'를 근본적으로 파괴하는 행위입니다.

4단계 파급 경로(Contagion Path) 분석

공격이 성공했을 때, 위기는 다음과 같은 4단계의 연쇄 반응을 통해 시스템 전체로 확산됩니다.

1. **1단계: 운영 마비 및 극도의 불확실성 (Operational Paralysis & Extreme Uncertainty)**
   특정 CCP의 청산 및 결제 기능이 중단되면서, 수많은 증권 및 파생상품 거래가 미결제(fail) 상태에 빠집니다. 시장 참가자들은 자신이 보유한 자산의 소유권을 증명할 수도, 거래 상대방이 누구인지, 그들의 재무 상태가 안전한지 전혀 확인할 수 없는 극도의 정보 비대칭 상황, 즉 '정보의 안개(Fog of War)'에 놓입니다. 공격의 배후, 피해 범위, 데이터 위변조 여부가 즉각적으로 파악되지 않으면서 시장은 걷잡을 수 없는 공포에 휩싸입니다.
2. **2단계: 유동성 증발 및 신용 시스템 붕괴 (Liquidity Evaporation & Credit System Collapse)**
   거래 상대방 리스크(Counterparty Risk)가 사실상 무한대로 치솟습니다. 어제의 거래 상대가 오늘 존재하지 않을 수도 있다는 공포는 은행 간 대출(Interbank Lending) 시장을 완전히 동결시킵니다. 모든 금융기관은 오직 생존을 위해 현금 확보에만 나서면서, 단기자금시장의 핵심인 레포(Repo) 시장마저 마비됩니다. 이는 시장 전체의 유동성이 순식간에 증발하는 '유동성 블랙홀' 현상을 야기하며, 신용 창출 시스템 자체가 붕괴됩니다. 미연준(Federal Reserve)이 경고한 시스템적 취약점이 현실화되는 순간입니다.
3. **3단계: 자산 투매 및 시장 붕괴 (Fire Sale &; Cascading Failure)**
   유동성 확보가 절실해진 금융기관들은 보유 자산을 종류와 등급을 가리지 않고 투매(Fire Sale)에 나섭니다. 한 기관의 매도는 자산 가격 하락을 유발하고, 이는 다른 기관의 담보 가치 하락과 마진콜로 이어져 또 다른 매도를 촉발하는 악순환의 고리, 즉 연쇄 붕괴(Cascading Failure)가 발생합니다. 주식, 채권, 부동산 등 모든 자산 클래스에서 패닉 셀링이 동시다발적으로 일어나며, 자산 가격 발견 기능 자체가 마비됩니다.
4. **4단계: 중앙은행의 최종 대부자 역할 시험 (Test of Central Bank as Lender of Last Resort)**
   이 상황에서 금리 인하와 같은 전통적인 통화정책은 아무런 의미가 없습니다. 시장의 신뢰와 거래 메커니즘 자체가 파괴되었기 때문입니다. 중앙은행은 작동 불능에 빠진 시장에 직접 유동성을 공급하고, 심지어는 거래를 보증하거나 결제 시스템을 직접 복구해야 하는 전례 없는 조치를 취해야 하는 압박에 직면합니다. 이는 기존 통화정책의 틀을 완전히 벗어나는 미지의 영역이며, 중앙은행의 신뢰도마저 시험대에 오르게 되는 궁극의 위기 상황입니다.



디지털 블랙스완 시나리오의 4단계 파급 경로에 따른 핵심 리스크 지표(VIX, FRA-OIS Spread)의 폭발적 증가 예상 경로

실용적 모니터링 시스템 구축 방법론

이처럼 파괴적인 시나리오에 대응하기 위해서는 위기의 징후를 조기에 포착하는 정교한 모니터링 시스템이 필수적입니다. 이는 단순히 몇 개의 지표를 추적하는 것을 넘어, 데이터의 구조화, 정량·정성 정보의 결합, 그리고 지표 간의 상호 연관성 분석을 포함하는 통합적인 접근을 요구합니다.

데이터 구조화의 중요성

사용자가 제공한 `Indicators.xlsx`, `News_Keywords.xlsx`, `Scenario_Indicator_Link.xlsx` 등의 파일 구조는 효과적인 조기 경보 시스템의 청사진을 제시합니다. 각 지표에 고유 ID를 부여하고(`Indicator_ID`), 시계열 데이터를 별도로 관리하며(`timeseries_ind.xlsx`), 시나리오와 지표를 체계적으로 연결하는(`scenario_indicator_link.xlsx`) 방식은 다음과 같은 장점을 가집니다.

- **확장성:** 새로운 지표나 시나리오가 추가되더라도 기존 시스템에 쉽게 통합할 수 있습니다.
- **자동화:** 구조화된 데이터를 기반으로 Bloomberg API나 뉴스 API를 통해 데이터를 자동으로 수집하고, 임계치(Threshold)를 초과할 경우 자동으로 경보를 발생시키는 시스템 구축이 용이합니다.
- **분석의 깊이:** 각 지표의 가중치(Weight)나 상관계수(Correlation_Coeff)를 관리함으로써, 단순한 개별 지표 모니터링을 넘어 시나리오 전체의 위험도를 종합적으로 평가하는 '위기 경보 지수' 개발이 가능해집니다.

정량적 지표와 정성적 정보의 결합

디지털 블랙스완과 같은 예측 불가능한 리스크는 전통적인 계량 모델만으로는 포착하기 어렵습니다. 따라서 시장의 '숫자'와 시장 참여자들의 '심리'를 동시에 읽는 것이 중요합니다.

- **정량적 지표 (Quantitative Indicators):** 은행 간 신용 위험을 가장 민감하게 반영하는 **FRA-OIS 스프레드**, 시장의 공포를 측정하는 **VIX 지수**, 금융 시스템의 건전성을 나타내는 **은행주 지수(KBW Bank Index)**, 달러 유동성 경색을 보여주는 **통화 스왑 베이시스** 등은 위기의 객관적인 증거를 제공합니다.
- **정성적 정보 (Qualitative Information):** `News_Keywords.xlsx`의 개념처럼, 뉴스 기사, 보고서, 소셜 미디어 등에서 특정 키워드(예: 'CCP outage', 'state-sponsored cyber threat', 'interbank market freeze')의 빈도와 맥락을 분석하는 것은 숫자로 나타나기 전의 잠재적 위협 '징후'를 포착하는 데 결정적 역할을 합니다. 이는 시장의 불안 심리가 어떻게 형성되고 확산되는지를 파악하는 중요한 단서가 됩니다.

연결성 분석: 리스크의 우선순위 결정

`Scenario_Indicator_Link.xlsx` 파일의 개념은 리스크 관리의 핵심적인 질문에 답을 줍니다: "수많은 지표 중 무엇을 가장 중요하게 보아야 하는가?" 특정 시나리오(SC003)와 각 지표(IND011, IND012 등) 간의 연관 강도(Weight)와 상관계수(Correlation_Coeff)를 정의함으로써, 우리는 제한된 자원과 관심을 어디에 집중해야 할지 결정할 수 있습니다. 예를 들어, '디지털 블랙스완' 시나리오에서 FRA-OIS 스프레드(IND011)의 가중치를 0.95로 높게 설정하는 것은, 이 지표의 변화가 다른 어떤 지표보다 시나리오의 현실화 가능성을 강력하게 시사한다는 분석적 판단을 시스템에 반영하는 것입니다. 이러한 연결성 분석은 리스크의 우선순위를 정하고 대응 자원을 가장 효율적으로 배분하는 나침반 역할을 합니다.

실행 보고서: '디지털 블랙스완' 리스크 분석 및 대응 전략

앞선 심층 분석을 바탕으로, 신한은행 리스크 관리 부서가 즉시 활용할 수 있도록 구조화된 종합 분석 보고서를 제시합니다. 본 보고서의 모든 데이터와 분석은 제공된 참고 자료와 사용자 요청 형식에 따라, '디지털 블랙스완' 시나리오(Scenario_ID: SC003)를 중심으로 작성되었습니다.

1. 시나리오 설명 및 전개 흐름

본 표는 '디지털 블랙스완' 시나리오의 핵심 정의와 단계별 위기 전개 과정을 요약하여, 시나리오에 대한 공통된 이해를 제공하는 것을 목적으로 합니다.

항목	내용
Scenario_ID	SC003
Scenario_Name	'디지털 블랙스완': 핵심 금융 인프라에 대한 시스템적 사이버 공격
Description	**발생 배경:** 국가의 지원을 받는 고도화된 해킹 그룹이 글로벌 금융 시스템의 핵심 노드(CCP, SWIFT, 주요 클라우드)를 공격, 단순 서비스 중단을 넘어 거래 기록의 대규모 위변조를 통해 시스템의 근간인 '신뢰'; 자체를 붕괴시키는 상황을 가정. **단계별 파급 경로:** 1. **운영 마비:** 핵심 결제/청산 시스템 마비로 거래 미결제(fail) 사태 속출. 2. **신용 시스템 붕괴:** 거래 상대방 리스크 폭증으로 은행 간 대출 시장 동결 및 유동성 증발. 3. **자산 투매:** 유동성 확보를 위한 모든 자산의 동반 폭락(Fire Sale) 발생. 4. **정책 무력화:** 중앙은행의 전통적 정책 수단이 무력화되고 신뢰도 시험대에 오름.

2. 모니터링할 시장 지표 (Bloomberg 데이터)

본 시나리오의 발생 징후를 조기에 감지하기 위해 실시간으로 모니터링해야 할 핵심 시장 지표 목록입니다. 각 지표의 임계치(Threshold)는 '주의(Yellow)';와 '경고(Red)' 단계로 구분되며, '경고' 임계치 초과 시의 예상 발생 확률(Probability)을 포함합니다. 이 지표들은 금융 시스템의 스트레스 수준을 객관적으로 측정하는 바로미터 역할을 합니다.

Indicator_ID	Indicator_Name	Bloomberg_Ticker	Data_Frequency	Threshold_Low (주의)	Threshold_High (경고)	Volatility(%)	Current_Value	Pr 초
IND011	FRA-OIS 스프레드 (3M)	USFRF3M Index	1D	**> 50bp**	**> 100bp**	8.5	15bp	5.0
IND012	CBOE 변동성 지수	VIX Index	1min	**> 40**	**> 60**	15.2	14.5	2.5
IND013	KBW 은행 지수	BKX Index	1min	**일일 -10%**	**일일 -15%**	2.1	95.8	3.0
IND014	미국 달러 유동성 스왑 (3M EUR)	EUSS03 Curncy	1D	**> 30bp**	**> 50bp**	6.4	5bp	4.0
IND015	미국채 10년물 금리	USGG10YR Index	1min	**기준일 대비 -100bp**	**기준일 대비 -200bp**	1.5	4.25%	1.5

3. 사전 감지(Yellow)·임박(Red) 뉴스 키워드

정량적 지표가 움직이기 전에 나타나는 시장의 '심리'와 '소문'을 포착하기 위한 뉴스 모니터링 키워드 목록입니다. 각 키워드는 위기의 진행 단계(Phase)와 시나리오와의 연관 강도(Weight)에 따라 분류되어, 정성적 정보 분석의 효율성을 높입니다.

Scenario_ID	Indicator_ID	Keyword	Phase	Weight(0–1)
SC003	IND011	financial system vulnerability, counterparty risk	Yellow	0.7
SC003	IND013	CCP outage, settlement failure	Yellow	0.8
SC003	IND012	state-sponsored cyber threat, APT group	Yellow	0.6
SC003	IND011	interbank market freeze, credit crunch	Red	0.9
SC003	IND014	dollar squeeze, emergency liquidity	Red	0.9
SC003	IND012	SWIFT network disruption, payment system halt	Red	1.0

4. 시나리오–지표 연계 정보

본 표는 ';디지털 블랙스완' 시나리오와 핵심 모니터링 지표 간의 상호 연관성을 정량화한 것입니다. 가중치(Weight)는 각 지표가 시나리오 발생을 예측하는 데 얼마나 중요한지를, 상관계수(Correlation_Coeff)는 방향성을, 변동성 영향(Volatility_Impact)은 시나리오 발생 시 예상되는 충격의 크기를 나타냅니다. 이는 리스크 관리의 우선순위를 결정하는 핵심 근거가 됩니다.

Scenario_ID	Indicator_ID	Weight	Correlation_Coeff	Volatility_Impact(%)
SC003	IND011	0.95	0.85	+1500%
SC003	IND012	0.90	0.90	+430%
SC003	IND013	0.85	-0.80	-30%
SC003	IND014	0.80	0.75	+1000%
SC003	IND015	0.70	-0.90	-45%

5. 신한은행 영향 분석 (‘수익성’·‘유동성’)

본 시나리오가 현실화될 경우, 신한은행의 핵심 재무 건전성 지표인 수익성과 유동성에 미칠 수 있는 잠재적 영향을 분석한 것입니다. Impact_Level은 5단계로 구분되며, 본 시나리오의 극단적인 파괴력을 감안하여 모든 항목에서 최고 수준인 '5단계(위기)'로 평가되었습니다.

Metric_ID	Metric_Name	Baseline_Value	Current_Value	Threshold_Level	Impact_Level(1–5)
BM001	순이자마진(NIM, %)	1.55%	1.52%	1.20%	5 (위기)
BM002	유동성커버리지비율(LCR, %)	105%	103%	90%	5 (위기)
BM003	외화 LCR (%)	90%	88%	70%	5 (위기)
BM004	파생상품평가손실(조원)	-0.1	-0.2	-2.0	5 (위기)
BM005	운영리스크 손실액(조원)	0.05	0.05	1.0	5 (위기)

** Impact_Level 정의: 1단계(경미) → 2단계(주의) → 3단계(경계) → 4단계(심각) → 5단계(위기)*

6. 종합 발생 가능성 및 대응 권고

모든 분석을 종합하여, '디지털 블랙스완' 시나리오의 최종적인 위험 수준을 평가하고, 신한은행이 생존을 위해 반드시 실행해야 할 구체적인 대응 방안을 제시합니다.

> ***Overall Probability(%): 3.3%***
> *(개별 지표의 낮은 발생 확률에도 불구하고, 각 지표의 중요도(Weight)와 상호 연관성을 반영하여 산출한 가중 평균 확률. 이는 단순 평균보다 시나리오의 복합적인 위험성을 더 정확하게 반영합니다.)*
>
> ***종합 Risk Level(1–5): 5단계 (위기)***
> *(발생 확률은 낮으나, 일단 발생 시 은행의 존립 자체를 위협하는 최상(Extreme) 수준의 충격을 야기하므로 최고 위험 등급으로 분류합니다. 이는 확률과 결과의 곱으로 정의되는 리스크의 개념에 따른 것입니다.)*

대응 권고 (Action Recommendations)

이 시나리오는 전통적인 리스크 관리의 틀을 넘어서는 전사적인 대응을 요구합니다. 다음은 신한은행이 즉시 검토하고 실행해야 할 핵심 권고안입니다.

Portfolio (포트폴리오 관리)

- **역 스트레스 테스트(Reverse Stress Testing)의 정례화 및 심화:** "어떤 상황이 발생하면 우리 은행이 파산하는가?";라는 질문에서 출발하여, 은행의 생존을 위협하는 최악의 사이버 공격 경로를 역으로 추적해야 합니다. 예를 들어, '주요 클라우드 서비스(AWS/Azure)의 인증 시스템이 48시간 동안 위변조될 경우', '주요 CCP의 거래 데이터가 1% 위변조된 사실이 일주일 후 발견될 경우' 등 구체적인 시나리오를 설정하고, 이로 인해 발생하는 포트폴리오의 가장 취약한 연결고리(예: 특정 파생상품, 특정 거래 상대방에 대한 과도한 익스포저)를 식별하고 방어 체계를 구축해야 합니다.
- **비상 자산 매각 계획(Fire Sale Plan) 수립:** 궁극의 안전자산인 미국채를 제외한 모든 자산의 동반 폭락 가능성에 대비해야 합니다. 시장 기능이 마비된 상황에서 유동성을 확보하기 위해 어떤 자산을 어떤 순서로, 어떤 방식으로 매각할 것인지(예: 중앙은행 유동성 공급 창구 활용, 비공개 시장 거래 등)에 대한 구체적인 계획을 사전에 수립하고, 이를 기반으로 도상 훈련을 실시해야 합니다.

NIM (순이자마진) 방어

- **비상 금리 및 여신 정책(Emergency Rate & Credit Policy) 수립:** 시장금리가 폭등하고 신용경색이 극심해지는 상황에서 NIM을 방어하고 자산 부실화를 막기 위한 비상 계획이 필요합니다. 여기에는 거래 상대방 리스크가 사실상 제로에 수렴하는 중앙은행과의 거래를 제외한 모든 신규 신용 공여를 일시적으로 중단하는 시나리오, 그리고 기존 대출에 대한 비상 LTV/DSR 재평가 및 담보 보강 요구 기준 등이 포함되어야 합니다.

Funding (자금조달 다변화)

- **비상 유동성 조달 계획(Contingency Funding Plan, CFP) 강화:** 극심한 달러 유동성 경색(Dollar Squeeze)은 이 시나리오의 필연적인 결과입니다. 이에 대비하여, 중앙은행과의 통화 스왑 라인 및 FIMA Repo Facility 등 비전통적 외화 유동성 조달 수단을 최우선으로 점검하고, 실제 위기 시 이를 즉각적으로 가동할 수 있도록 내부 절차와 담당자를 명확히 지정하고 반복적으로 훈련해야 합니다.
- **뱅크런(Bank-run) 대응 전략 마련:** 금융 시스템에 대한 신뢰가 붕괴될 때, 리테일 예금의 대규모 이탈은 불가피합니다. 이에 대비하여 고객을 안심시키기 위한 단계별 커뮤니케이션 전략, 영업점의 혼란을 최소화하기 위한 운영 계획, 그리고 필요시 유동성을 신속하게 공급하기 위한 방안을 사전에 마련해야 합니다.

Operations & Strategy (운영 및 전략)

- **핵심 금융 인프라 의존도 전면 재검토:** IT 아웃소싱, 특히 핵심 뱅킹 시스템의 특정 클라우드 서비스 제공자(CSP)에 대한 의존도를 전면적으로 재평가해야 합니다. 단일 CSP에 대한 의존도를 낮추기 위한 멀티 클라우드 전략, 그리고 최악의 경우를 상정하여 백업 시스템의 물리적/네트워크적 분리를 강화하고, 오프라인 데이터 백업(Air-gapped backup) 체계를 구축하는 방안을 검토해야 합니다. BCP(Business Continuity Plan)는 단순 서버 복구가 아닌, '데이터의 신뢰성'이 훼손된 상황을 가정한 시나리오로 재수립되어야 합니다.

- **위기대응 거버넌스(Crisis Governance) 구축:** 본 보고서에서 제시된 '위기 경보 지수'가 특정 임계치를 넘을 경우, 사전에 지정된 핵심 인력(리스크, IT, 자금, 전략, 준법, 홍보 등)이 참여하는 비상대책위원회(War Room)가 자동으로 소집되고, 사전에 정의된 역할과 책임(R&R)에 따라 즉각적으로 대응하는 체계를 구축해야 합니다. 이는 의사결정의 지연을 막고, 혼란 속에서 조직이 일사불란하게 움직일 수 있도록 하는 핵심적인 장치입니다.

참고 자료

[1] stress_test_scenarios_4
https://static-us-img.skywork.ai/prod/analysis/2025-07-21/6298450475799880160/1947441507058294792_347e12de2f0e9aa9c8281a342d00db45.pdf

[2] 4.scenario_indicator_link
https://static-us-img.skywork.ai/prod/analysis/2025-07-22/6298450475799880160/1947451542597509123_2ddf1c15505bfd578b7a5296d983313f.xlsx