J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

사이버 공격에 능동대응하기 위한 사이버 자산의 지능형 자가복구기술 연구☆

A Study on Intelligent Self-Recovery Technologies for Cyber Assets to Actively Respond to Cyberattacks

최 세 호[1] 임 항 섭[2] 최 중 영[3] 권 오 진[4] 신 동 규[1,5*]
Se-ho Choi Hang-sup Lim Jung-young Choi Oh-jin Kwon Dong-kyoo Shin

요 약

사이버 공격 기술은 예측 불가할 정도로 진화하고 있으며, '언젠가는'이 아니라 '언제나' 일어날 수 있는 상황이다. 클라우드 컴퓨팅, 사물인터넷(Internet of Things) 등으로 초연결 글로벌화되고 있는 인프라는 그 어느 때보다 사이버 공격에 큰 피해를 받을 수 있는 환경이며, 사이버 공격은 지금도 진행 중이다. 사이버 공격이나 천재지변 등 외부적인 영향으로 피해가 발생하더라도 사이버 자산(OS, WEB, WAS, DB)의 다운 타임을 최소화하기 위해 사이버 레질리언스 관점에서 지능형 자가복구로 진화해야 한다. 본 논문에서는 사이버 자산이 사이버 공격을 받아 고유의 기능이 제대로 발휘하지 못할 경우 지속가능한 사이버 레질리언스를 보장하기 위한 지능형 자가복구기술을 제안한다. 평상시 사이버 자산의 원본 및 업데이트 이력을 타임슬롯 설계 및 스냅샷 백업 기술로 실시간 관리한다. 상용화된 파일 무결성 모니터링 프로그램과 연동하여 피해 상황을 자동 탐지하고 지능형 기반으로 피해 파일에 대한 백업 데이터의 연관성 분석을 통해 사이버 자산의 다운타임을 최소화하여 최적의 상태로 자가복구할 수 있는 기술을 확보해야 한다. 향후에는 사이버 자산이 피해 받은 상태에 적합한 자가복구 전략 학습 및 분석을 수행할 수 있는 운영모델과 자가복구기술의 고유기능이 적용된 시범체계 연구를 수행할 예정이다.

☞ 주제어 : 사이버 공격 기술, 사이버 자산, 다운타임 최소화, 지능형 자가복구기술

ABSTRACT

Cyberattack technology is evolving to an unpredictable degree, and it is a situation that can happen 'at any time' rather than 'someday'. Infrastructure that is becoming hyper-connected and global due to cloud computing and the Internet of Things is an environment where cyberattacks can be more damaging than ever, and cyberattacks are still ongoing. Even if damage occurs due to external influences such as cyberattacks or natural disasters, intelligent self-recovery must evolve from a cyber resilience perspective to minimize downtime of cyber assets (OS, WEB, WAS, DB). In this paper, we propose an intelligent self-recovery technology to ensure sustainable cyber resilience when cyber assets fail to function properly due to a cyberattack. The original and updated history of cyber assets is managed in real-time using timeslot design and snapshot backup technology. It is necessary to secure technology that can automatically detect damage situations in conjunction with a commercialized file integrity monitoring program and minimize downtime of cyber assets by analyzing the correlation of backup data to damaged files on an intelligent basis to self-recover to an optimal state. In the future, we plan to research a pilot system that applies the unique functions of self-recovery technology and an operating model that can learn and analyze self-recovery strategies appropriate for cyber assets in damaged states.

☞ keyword : Cyberattack technology, Cyber Assets, Minimize Downtime, Intelligent Self-Recovery Technology

1. 서 론

사이버 공격 기술은 예측 불가할 정도로 진화하고 있다. 피해는 개인 및 기업에서 벗어나 정부기관까지 대상

1 Department of Computer Engineering, Sejong University, Seoul, 05006, Korea.
2 Military Digital Convergence, Ajou University, Suwon, 16499, Korea.
3 Korea Institute for Defense Analyses, Seoul, 02455, Korea.
4 Department of Electronics Engineering, Sejong University, Seoul, 05006, Korea.
5 Department of Convergence Engineering for Intelligent Drones, Sejong University, Seoul, 05006, Korea.
* Corresponding author (shindk@sejong.ac.kr)
[Receive 13 October 2023, Reviewed 24 October 2023(R2 15 November 2023), Accepted 17 November 2023]

☆ 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1F1A1074773). 이 논문은 2023년도 세종대학교 교내연구비 지원에 의한 논문임.

이 확대되어 사회 혼란과 국가안보를 위협하고 있다. 정부는 사이버 공격뿐만 아니라 사이버 자산의 장애, 파괴, 위협에서 벗어나 지속가능한 시스템 운영환경을 유지해야 한다. 오늘날의 사이버 공격은 '언젠가는'이 아니라 '언제나' 일어날 수 있는 상황이다. 사이버 공격이나 천재지변 등 외부적인 영향으로 피해가 발생하더라도 사이버 자산을 복구할 수 있는 전통적인 관리자 중심의 복구 솔루션에서 벗어나 지금은 사이버 레질리언스 관점에서 지능형 자가복구로 진화해야 한다[1].

사이버 레질리언스는 사이버 공간에서의 복구 활동으로 예상되거나 예상치 못한 모든 위협의 부정적인 요소들을 흡수하여 원상태로 복구[2]할 수 있는 조직의 역량이다. 하루가 다르게 진화하고 있는 사이버 공격을 발생하기 전에 탐지하고 예방하는 것도 어렵고, 특정 사이버 공격에 대해 알려진 하나의 방어기술로 대응하는 것도 쉽지 않다[3]. 모든 인프라에 공통으로 적용되어 대응할 수 있는 통합된 단일 시스템도 없으며, 사이버 공격 및 위협으로부터 사이버 자산을 보호할 수 있는 단일 접근 방식도 없다[4]. 사이버 자산이 공격을 받아 고유의 기능이 제대로 발휘하지 못할 경우 지속가능한 사이버 레질리언스를 보장하기 위한 지능형 자가복구기술이 필요하다. 평상시 사이버 자산의 원본 및 업데이트 이력을 타임슬롯 설계 및 스냅샷 백업 기술로 실시간 관리한다. 상용화된 파일 무결성 모니터링 프로그램과 연동하여 피해 상황을 자동 탐지하고 지능형 기반으로 피해 파일에 대한 백업 데이터의 연관성 분석을 통하여 최적의 지능형 자가복구 기술을 제안하고자 한다.

이어지는 본 논문의 2장에서는 사이버 레질리언스 메커니즘과 재해복구시스템의 설명, 자가치유시스템과 관련된 연구를 요약한다. 3장은 사이버 자산 피해로 시스템 다운타임이 발생한 사례를 살펴보고 4장에서는 지속가능한 시스템 운영환경을 보장하기 위한 지능형 자가복구기술에 대해서 제안한다. 마지막으로 5장은 결론 도출 및 향후 연구방향에 대해 제시한다.

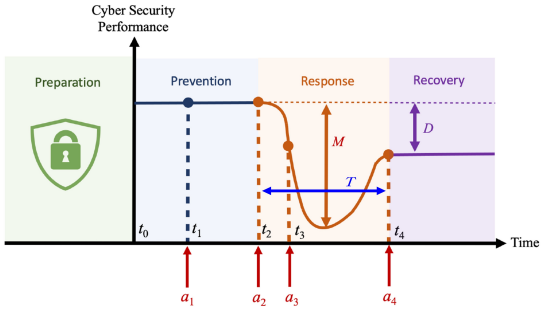
2. 관련 연구

이번장에서는 사이버 레질리언스 메커니즘과 재해복구시스템을 소개하고 운영자의 도움없이 피해 및 장애를 자동으로 탐지하여 치유하는 자가치유시스템에 대한 연구 동향을 요약한다.

2.1 사이버 레질리언스 메커니즘

사이버 레질리언스 메커니즘(Cyber-Resilient Mechanism 이하 CRM)은 준비(Preparation), 예방(Prevention), 대응(Response) 및 복구(Recovery)의 4단계로 구분할 수 있다. 준비는 사이버 시스템의 보안 위험을 평가하고 허니팟(honeypots) 또는 속임수 메커니즘의 배포, 탐지 시스템의 구성 등과 같은 적절한 보안 정책을 설계한다. 예방은 설계된 보안 정책을 구현하고 사이버 시스템을 보호한다. 대응은 공격을 저지하지 못할 때 공격을 방어하는 중요한 단계이다. 복구는 공격의 파급 효과를 줄이고 사이버 시스템 성능을 최대한 원래의 상태로 돌아가는 마지막 단계이다[5].

타임라인에 따른 일반적인 사이버 레질리언스 메커니즘(CRM)의 4단계는 다음 그림 1과 같으며, 사이버 시스템은 운영 전에 예상되고 알려진 공격과 자체 시스템의 위험을 고려하여 보호 메커니즘을 설계했다.



(그림 1) 사이버 레질리언스 메커니즘의 4단계. Ref의 허가를 받아 재인쇄함[5]

(Figure 1) The Four Stages of a Cyber-Resilient Mechanism. Reprinted with permission from Ref[5]

사이버 시스템은 t_0 에서 작동을 시작한다(Preparation). 시간 t_1 에서 공격자는 공격 a_1 을 시작하고 사이버 시스템이 이를 준비함에 따라 이 공격은 성공적으로 차단하고 공격자가 시간 t_2 에서 새로운 공격 a_2를 시작할 때까지 시스템을 보호한다(Prevention). 시간 $t_2 \sim t_3$ 는 공격 목표를 달성하여 사이버 위험이 증가하거나 사이버 보안 성능이 저하된다. 공격 a_2 와 후속 공격 a_3 에 대해 시간 t_3 에 대응해야 한다(Response). 사이버 시스템은 공격자의 footprint에서 빠르게 학습한 후 적대적인 환경에 재구성하고 적응하기 위한 전략적 결정을 내리고 시스템의 보안 상태를 점진적으로 개선한다. 그리고 적응된 시스

템은 공격에 더욱 강력해진다. 시간 t_4 에서 계속되는 공격 a_4 는 적용된 보호 메커니즘을 통해 저지될 수 있으며, 시간 t_4에서 공격 후 최고의 성능으로 복원한다(Recovery).

그림 1 에서 첫 번째 공격부터 복구까지 걸리는 시간(즉, $T = t_4 - t_2$)을 기준으로 4단계에 걸쳐 사이버 복원력을 측정할 수 있으며, 이 시간 간격은 응답 속도를 나타낸다. 구간 t_2 와 t_4 사이의 최악의 성능 저하를 M 이라고 한다[5]. 복원된 성능과 초기 또는 계획된 성능 간의 격차, 즉 D 는 복원력의 유효성을 나타낸다. 이렇게 사이버 레질리언스 메커니즘(CRM)의 목표는 T, M, D 를 최소화하는 것이다.

2.2 재해복구시스템

2.2.1 재해복구시스템의 개념

재해(Disaster)는 시스템이 외부적인 영향을 받아 예방 및 통제가 불가능한 사건으로 인해 시스템의 서비스가 중단되거나, 시스템의 장애로부터 복구소요시간이 예상되었던 허용 가능한 범위를 초과해서 정상적인 업무를 수행하는데 지장을 초래한 피해를 의미한다[6].

장애(Incident)는 통제 불가능한 천재지변과 인적 재해를 제외한 발생원인 관점에서 직접적으로 영향을 미치는 휴먼 장애(행위자가 바라는 대로의 결과를 기대하고 계획적인 행위를 하였으나 기대한 대로의 성과를 얻지 못하는 경우로 시스템의 효율이나 안전을 저해하는 부적절한 행동[7]), 시스템 장애, 인프라 장애(운영 설비 포함) 등과 같은 통제 가능한 요인들에 의한 시스템의 성능 저하 및 동작 오류, 고장을 의미한다[6].

재해복구(Disaster Recovery)는 갑작스런 자연현상의 변화로 인하여 멈추어진 하드웨어와 응용체계 서비스를 재기동하는 것을 의미한다. 재해복구를 위해서는 사전에 피해 상황에 맞는 복구절차가 반영된 재해복구계획과 이를 지원하는 재해복구시스템(Disaster Recovery System)이 준비되어야 한다.

2.2.2 재해복구시스템 구축 유형

재해복구시스템은 구축 유형에 따라 일반적으로 미러사이트(Mirror site), 핫사이트(Hot site), 웜사이트(Warm site), 콜드사이트(Cold site)로 구분된다.

미러사이트는 주센터와 동일한 수준의 데이터베이스 관리 시스템(Data Base Management System, 이하 DBMS)을 원격지에 구축하여 주센터와 예비센터 모두 Active-Active 상태로 실시간에 동시 서비스를 하는 방식이다. 핫사이트는 주센터와 동일한 수준의 DBMS를 대기상태(Standby)로 예비센터 정보시스템에 사이트를 보유하면서(Active-Standby), 동기적(Synchronous) 또는 비동기적(Asynchronous) 방식의 실시간 미러링(Mirroring)을 통하여 데이터를 최신의 상태로 유지하고 있다가, 주센터 재해시 예비센터의 정보시스템을 Active로 전환하여 서비스하는 방식이다. 웜사이트는 핫사이트와 유사하나, 예비센터에 주센터와 동일한 수준의 DBMS를 보유하는 대신, 중요성이 높은 DBMS만 부분적으로 예비센터에 보유하는 방식이다. 콜드사이트는 데이터만 원격지 예비센터에 보관하고, 서비스를 위한 정보자원은 확보하지 않거나 장소 등 최소한으로만 확보하고 있다가, 재해시에 데이터를 바탕으로 필요한 정보자원을 조달하여 정보시스템의 복구하는 방식이다.

재해복구시스템의 구축 유형을 표 1과 같이 복구소요시간과 장·단점을 비교할 수 있다.

(표 1) 재해복구시스템 구축 유형 비교[6]
(Table 1) Comparison of Disaster Recovery System Construction Types[6]

유 형	복구소요시간	장 점	단 점
Mirror site	즉시	·데이터 최신화 ·높은 안정성 ·신속한 업무재개	·높은 초기투자비용 ·높은 유지보수비용 ·데이터 갱신이 많은 경우 과부하 발생
Hot site	4시간 이내	·데이터 최신화 ·높은 안정성 ·신속한 업무재개 ·데이터 갱신이 많은 경우 적합	·높은 초기투자비용 ·높은 유지보수비용
Warm site	수일 ~ 수주	·구축 및 유지비용이 핫사이트에 비해 저렴	·일부 데이터 손실 발생 ·초기복구수준이 부분적임 ·복구시간이 비교적 많이 소요됨
Cold site	수주 ~ 수개월	·구축 및 유지비용이 가장 저렴	·데이터 손실 발생 ·복구에 매우 긴 시간이 소요됨 ·복구 신뢰성이 낮음

2.3 자가치유시스템

자가치유시스템(self-healing system)은 인간의 건강을 유지하는 자가치유 능력과 같이 사이버 공격으로 인한

침입 및 시스템 운영간 장애가 발생할 때마다 운영자의 도움 없이 스스로 자동 탐지하고 치유하는 시스템을 의미한다. 시스템에서 발생 될 수 있는 에러나 오류를 미리 예상하거나 자동 탐지하고 이러한 오류를 시스템 스스로 백업파일을 이용하여 치유 또는 수정함으로써 시스템의 다운타임을 최소화하는 것이 목적이다[8].

현재 이기종 구성요소들이 복잡하게 결합하여 시스템이 설계되고 서로 다른 애플리케이션 소프트웨어 간의 의존성은 애플리케이션 우발장애(contingent) 및 상호 충돌의 요인이다. 그러므로 자가치유를 통해 시스템을 실시간 진단하며 대응해야 한다. 시스템이 자가치유되려면 먼저 피해가 발생된 구성요소를 신속하게 자동 탐지 및 격리하고, 오프라인으로 전환해야 한다. 피해가 발생된 구성요소를 수정 또는 격리하고, 고정 또는 교체 구성요소를 서비스에 다시 도입하여 피해가 발생된 구성요소에서 복구할 수 있어야 한다. 애플리케이션이 중단되지 않도록 시스템에서 문제를 예측하고 장애가 애플리케이션에 영향을 미치지 않도록 조치를 취해야 한다. 자가 복구 목표는 엔터프라이즈 애플리케이션을 항상 가동 상태로 유지하기 위해 다운타임을 최소화하는 것이다. 그러기 위해서는 시스템 구성요소 개발자는 지속적인 가용성을 위해 각 하드웨어 및 소프트웨어 제품의 안정성과 가용성을 극대화하는 데 중점을 두어야 한다[9].

압두라만 야부즈는 관계형 데이터베이스 관리 시스템(Relational DataBase Management System, 이하 RDBMS)을 통합하여 상호 연결된 마이크로 그리드간의 자가치유 기능을 향상시키는 동적 데이터 기반 애플리케이션 시스템 프레임워크를 제시했다. 상호 연결된 3개의 자가치유 마이크로 그리드에 대한 에이전트 기반 시뮬레이션 모델(Aagent-based Simulation Model)을 구축하고 관계형 데이터베이스 관리 시스템(RDBMS)가 있는 마이크로 그리드와 없는 마이크로 그리드의 자가 복구 작업을 비교했다[10].

조마 알드리니는 잠재적인 이상 및 결함을 신속하게 탐지하는 것이 중요하다는 것을 알고 지난 10년 동안 결함 진단 및 자가치유 접근법과 스마트 제조(Smart Manufacturing)에 관한 256개 이상의 관련 논문을 검토하고 분석하였다. 대부분의 논문은 돌발적이고 간헐적인 결함을 고려하는 반면, 일부 연구는 제조 과정에서 가장 자주 발생하는 결함인 초기 결함(일반적으로 시간이 지남에 따라 천천히 진행되는 장비의 성능 저하)에 초점을 맞추고 있다. 그래서 다중 결함 진단을 위해 물리적 모델과 데이터 기반 모델을 결합한 하이브리드 접근 방식을 제안했다[11].

후 아 칭 리앙은 자가치유시스템에 제어 아이디어를 결합하여 자가치유제어시스템을 구축하고 정의, 이론적 틀, 특성을 제안했다. 자가치유제어 프로세스는 자가최적화(self-optimization), 자가진단(self-diagnosis), 자가결정(self-decision), 자가복구(self-repairing)의 4단계로 구성한다. 자가치유제어 이론을 정립하기 위해 초기 단계인 자기치유이론을 제어시스템에 적용하려는 노력이 필요하다고 강조했다[12].

오빈나 존필은 최신 기술을 분석하고 기계 학습을 사용한 자가치유를 사이버 물리 시스템에 적용하여 보안을 강화하고 시스템 내 오류를 방지할 수 있다고 제안했다. 기계학습 자가복구 기능의 주요 구성요소인 이상 탐지(anomaly detection), 오류 경고(fault alert) 및 오류 자동해결(fault autoremediation) 세 가지를 모두 고려하여 사용하면 사이버 물리시스템에 원활한 자체 구성 및 자체 복원 기능을 제공하여 시스템 보안을 강화하고 사용자 경험을 향상시킬 수 있는 잠재력을 가지고 있다[13].

이와 같이 자가치유시스템과 관련된 연구를 조사한 결과 예측되는 위협 및 장애에 한정하여 자가치유가 원활히 진행되지만, 우발상황 및 잠재적인 위협은 최신 기술 및 대응사례를 연관 분석하여 피해상황에 알맞게 융통성 있는 복구 계획을 준비해야 한다는 것을 확인할 수 있다.

3. 사이버 자산 피해로 발생된 다운타임 사례

사이버 자산이 랜섬웨어 감염, 휴먼 장애, 전산 장애, 화재 등 피해가 발생하여 시스템이 다운타임된 사례를 살펴본다.

3.1 랜섬웨어 감염으로 발생된 다운타임 사례

2020년 11월 이랜드 그룹이 클롭(CLOP) 랜섬웨어 조직의 공격을 받아 NC백화점과 뉴코아아울렛, 2001아울렛 등 전체 오프라인 매장 48곳 중 절반가량인 23곳이 영향을 받아 휴점하는 다운타임이 있었다[14]. 원래 상태로 복구하기 위해 별도로 구분된 서버의 정보를 활용하여 하루가 지난 다음 날 대부분의 매장이 정상화됐다.

3.2 휴먼 장애로 발생된 다운타임 사례

2023년 5월 정부기관 ○○청의 자료교환체계 연동테스트 중 유지보수업체 인원이 인트라넷 NAS에서 테스트한 파일을 지우기 위해 “rm -rf /*” 명령어를 입력하여

/boot, /bin 등 시스템 파일과 /DBDATA/data 폴더에 저장된 데이터 파일을 과다하게 삭제한 휴먼 장애로 인해 자료교환체계가 다운타임이 발생하였다[15]. 원래 상태로 복구하기 위해 인터넷, 인트라넷 서비스를 다운하고 복구을 진행하였다. OS는 백업 설정되어 있었으나 데이터 파일은 백업이 안되고 있어 복구간 제한사항을 확인하였다. 시스템 정상화는 인터넷으로 송·수신된 로그파일을 동기화하여 엔지니어의 수작업을 통해 다운타임 8일이 지난 후 완료됐다.

3.3 전산 장애로 발생된 다운타임 사례

2022년 6월 인천에 위치한 대형병원 본관과 부속 건물에서 전산 장애가 발생했다. 이 사고로 진료 접수와 수납, 입·퇴원 절차 등 병원 업무 전반에 차질이 생기며 환자들이 불편을 겪었다. 전력 공급에는 문제가 없어 의료 장비는 정상적으로 가동[16]되었지만, 정상화는 90분이 지난 후 주요 기능 대부분이 완료됐다.

3.4 화재로 발생된 다운타임 사례

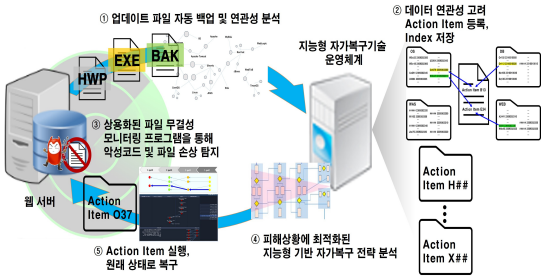
2022년 10월 SK주식회사 C&C 판교캠퍼스 무정전 전원 장치(UPS) 설비의 누전으로 화재가 발생하여 서버 작동에 필요한 전원 공급이 차단되었다. 이 과정에서 카카오톡, 멜론, 티스토리, 다음을 포함한 카카오의 대다수 서비스 및 네이버, SK의 일부 서비스 등 이용 불가하였다[17]. 카카오는 원래 상태로 복구하기 위해 예비용 데이터센터로 전환하는 작업을 진행하였지만, 카카오 메일은 장애기간 동안 수신된 이메일이 모두 수신불가로 반송처리되고 카카오 공인인증서 이용이 불가능했다. 모든 카카오 서비스의 정상화는 5일이 지난 오후 11시부터 완료됐다.

4. 지능형 자가복구기술 제안

3장에서 조사된 사례를 능동대응 차원에서 다운타임을 최소화되도록 개선하기 위해 이번 장에서는 지속가능한 시스템 운영환경을 보장하기 위한 지능형 자가복구기술의 운영개념과 세부기술에 대해서 제안한다.

4.1 지능형 자가복구기술의 운영개념

장시간에 걸친 타켓형 사이버 공격을 완벽하게 보호하는데 한계가 있으므로 사이버 자산이 사이버 공격을 받아 피해가 발생할 경우 능동적인 복구 활동을 수행하여 가능한 빠른 시간내에 사이버 공격 전의 상태로 돌아갈 수 있는 지능형 자가복구기술을 제안한다. 지능형 자가복구기술은 그림 2와 같이 동일한 백업 파일에 대한 타임슬롯 설계 및 스냅샷 백업 기술 등을 적용하여 사이버 자산을 실시간 관리한다. 상용화된 파일 무결성 모니터링 프로그램과 연동하여 피해 상황을 자동 탐지하고 지능형 기반으로 백업 데이터 연관성 분석을 통하여 최적의 복구 전략을 제안하고 특정 파일 또는 폴더를 자가복구할 수 있는 사이버 자산의 회복탄력성을 보장할 수 있다.



(그림 2) 지능형 자가복구기술 개념도

(Figure 2) Intelligent Self-Recovery Technology Diagram

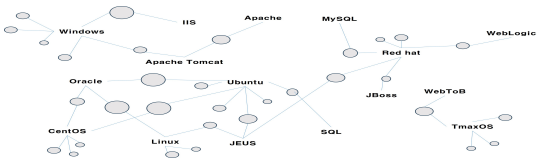
4.2 지능형 자가복구의 세부기술

4.2.1 사이버 자산 연관성 분석 기술

사이버 자산의 고유기능을 복구할 수 있도록 지지도(support), 신뢰도(confidence), 향상도(lift)를 통해 연관성을 분석한다.

지지도는 전체 사이버 자산의 Action Item 중 연관성 규칙을 구성하는 항목들이 포함된 Action Item의 비율이다. 신뢰도는 조건이 발생했을 때 동시에 일어날 확률을 의미하며 신뢰도가 1에 가깝다는 것은 일어날 확률이 높다는 것을 의미한다. 향상도는 지지도와 신뢰도를 동시에 고려한다. 향상도 값이 1이 나오면 연관성이 없고 1이 초과하면 연관성이 있다. 향상도 값이 1인 경우 조건과 결과는 예기치 않게 이루어진 관계라고 보며 1보다 클수록 의미있는 연관성을 가진 규칙이라고 해석한다[18].

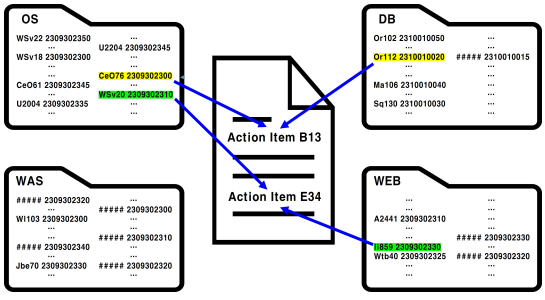
사이버 자산을 연관성 분석 결과를 원의 크기와 연결성을 이용하여 그림 3과 같이 그래프로 나타낼 수 있다.



(그림 3) 사이버 자산 연관성 분석 그래프
(Figure 3) Cyber Asset Correlation Analysis Graph

4.2.2 Action Item 그룹 인덱스 기술

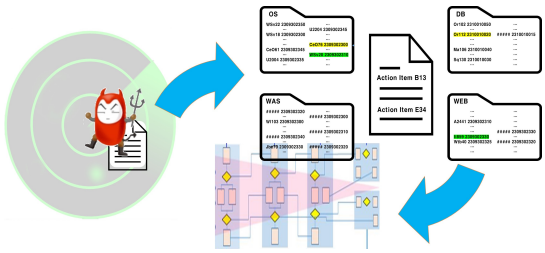
사이버 자산의 연관성을 고려하여 백업 공간의 그룹을 구분하고 동일한 파일은 타임슬롯으로 설계하여 특정 시간 및 인프라 환경에 맞게 사이버 자산의 백업 파일을 식별하는 기술이다. Action Item은 복구의 효율성을 높이기 위해 파일들을 묶은 객체를 말하며, 사이버 자산 특성에 맞게 약어 규칙을 정의하고 파일명에 백업일시를 색인하여 복구시 관련 대상 파일을 쉽게 찾을 수 있다. 반복적으로 활용되는 복구 파일들에 대해서는 Action Item으로 등록하여 그림 4와 같이 목록을 관리한다.



(그림 4) Action Item 그룹관리 개념도
(Figure 4) Action Item Group Management Conceptual Diagram

4.2.3. 자가복구 전략 분석 기술

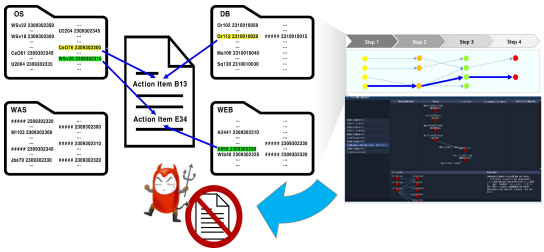
악성코드에 감염되었거나 피해가 발생된 파일의 고유기능을 원래 상태로 복구하기 위해 지능형 기반으로 사이버 자산의 연관성을 분석하여 최적의 복구 방안을 제시하는 기술이다. 악성코드에 감염되었거나 피해 파일을 원래 상태로 복구하기 위해 연관성을 분석하여 기존 Action Item 검증 및 신규 Action Item을 구성할 수 있다. 피해 받은 파일 중 고유기능 복구의 기여도를 판단하기 위해 그림 5와 같이 가중치와 복구 우선순위 지표화하여 자가복구 전략을 분석한다.



(그림 5) 자가복구 전략 분석 개념도
(Figure 5) Self-Recovery Strategy Analysis Concept Diagram

4.2.4. Action Item 배포 기술

자가복구 전략으로 분석된 결과를 바탕으로 그림 6과 같이 Action Item을 배포하는 기술이다. Action Item 특성에 따라 부팅 옵션이 추가되며, 관리자의 결정에 따라 배포 우선순위가 변경될 수 있다.



(그림 6) Action Item 배포 기술 개념도
(Figure 6) Action Item Distribution Technology Conceptual Diagram

5. 결 론

사이버 공격 기술은 하루가 다르게 예측 불가할 정도로 진화하고 있어 제한된 시간 내에 모든 사이버 공격을 완벽하게 예방하거나 대응할 수 없다.

그래서 본 논문에서는 사이버 자산이 공격을 받아 고유의 기능을 제대로 발휘하지 못할 경우 지속 가능한 사이버 레질리언스를 보장하기 위해 지능형 자가복구기술을 제안했다. 지능형 자가복구기술이 시스템에 적용된다면 랜섬웨어 감염, 휴먼 장애, 전산 장애, 화재 등으로 인해 사이버 자산에 피해가 발행하더라도 3장에서 살펴본 피해사례 복구소요시간 보다는 다운타임을 최소화하여 신속하게 시스템을 원래 상태로 복구할 수 있다.

향후에는 사이버 자산이 사이버 공격으로 받은 피해 상황에 맞게 자가복구 전략 학습 및 분석을 수행할 수 있는 운영모델과 지능형 자가복구의 세부기술이 적용된 시범체계 연구를 수행할 예정이다.

참고문헌(Reference)

[1] Choi, S.H. et al., “A Study on Cyber Resilience Evaluation Method Centered on Infringement Response Time,” Journal of Defense and Security, Defense Security Institute, Vol. 8, pp 87-110, December 2022.

[2] Ryu, J.G., “Respond to cyber security incidents that you don’t know when not if,” IDG Summary, October 2018. https://www.itworld.co.kr/techlibrary/111004.

[3] Lee, S.K. et al., “Resiliency of Mobile OS Security for Secure Personal Ubiquitous Computing,” Personal and Ubiquitous Computing, Vol. 22, pp. 23-34, 2018. https://doi.org/10.1007/s00779-017-1098-x.

[4] White Paper, “The Cyber Resilience Blueprint: A New Perspective on Security,” Symantec, pp. 1-12, 2014. http://www.ten-inc.com/presentations/Symantec-The-Cyber-Resilience-Blueprint.pdf.

[5] Y. Huang et al., “Reinforcement learning for feedback-enabled cyber resilience,” Annual Reviews in Control, Vol. 53, pp. 273-295, 2022. https://doi.org/10.1016/j.arcontrol.2022.01.001.

[6] Telecommunications Technology Associations, “Guideline for Disaster Management of Information Systems,” pp. 4-15, December 2007.

[7] Jeong J.U., “Concept, findings and consequences of human error,” Korea Industrial Health Association, Vol. 371, pp. 32-40, March 2019.

[8] Kang, Y.W., “Investigation of self-healing systems: approaches and systems,” The Global Network of Korean Scientists & Engineers, pp. 1-6, March 2012.

[9] A. G. Ganek et al., “The dawning of the autonomic computing era,” IBM Systems Journal, Vol 42, No 1, 2003. https://doi.org/10.1147/sj.421.0005.

[10] Abdurrahman Yavuz et al., “Microgrids via Dynamic Data Driven Applications System with Relational Database Management,” 2020 Winter Simulation Conference (WSC), March 2021.

[11] Joma Aldrini et al., “Fault diagnosis and self-healing for smart manufacturing: a review,” Journal of Intelligent Manufacturing, pp. 1-33, July 2023.

[12] H. Liang et al., “Self-Healing Control: Review, Framework and Prospect,” IEEE Access, Vol. 11, pp. 79495-79512, July 2023. https://doi.org/10.1109/ACCESS.2023.3298554.

[13] O. Johnphill et al., “Self-Healing in Cyber‐Physical Systems Using Machine Learning: A Critical Analysis of Theories and Tools,” Future Internet 2023, 15(7), 244, pp. 1-42, July 2023. https://doi.org/10.3390/fi15070244.

[14] Korea Internet & Security Agency, “Cyber Threat Trend Report for the first half of 2021,” pp. 25, 2021.

[15] Defense Integrated Data Center, “○○Office Data Exchange System File Transmission Failure Report,” pp. 1-2, May 2023.

[16] Yunhap news, “○Hospital, work was once disrupted due to computer failure... Recovery in 90 minutes,” 2023. https://www.yna.co.kr/.

[17] Namuwiki, “SInternet service failure due to fire at SK C&C Pangyo data center,” 2023. https://namu.wiki/.

[18] Truman(Association rules/Association analysis), 2023. https://truman.tistory.com/194.

◐ 저 자 소 개 ◑

최 세 호(Se-ho Choi)
2002년 육군3사관학교 전산정보처리학과(학사)
2022년 세종대학교 대학원 정보보호학과(석사)
2022년~현재 세종대학교 대학원 컴퓨터공학과 박사과정
관심분야 : 사이버 지휘통제, 사이버 레질리언스, 사이버 방어활동, etc.
E-mail : yeonwoo@sju.ac.kr

임 항 섭(Hang-sup Lim)
2002년 육군3사관학교 전산정보처리학과(학사)
2014년 아주대학교 대학원 정보보호학(석사)
2022년 아주대학교 대학원 국방디지털융합학과(박사 수료)
2023년~현재 국방부 서버/DB 감사관
관심분야 : 사이버보안, 사이버 위험관리, 사이버 레질리언스
E-mail : youandi1@ajou.ac.kr

최 중 영(Jung-young Choi)
2005년 중앙대학교 산업정보학과(학사)
2011년 고려대학교 대학원 정보보호학과(석사)
2022년 숭실대학교 대학원 IT정책경영학과(박사)
2011년~현재 한국국방연구원 연구위원
관심분야 : ICT융합, 인공지능, 사이버보안, 정보보호
E-mail : jychoi@kida.re.kr

권 오 진(Oh-jin Kwon)
1984년 한양대학교 전자공학과(학사)
1991년 남가주대학교 대학원 전기전자공학과(석사)
1994년 메릴랜드대학교 대학원 전기전자공학과(박사)
1999년~현재 세종대학교 전자공학과 교수
관심분야 : 이미지/비디오 퓨전, 압축, 워터마킹, 이미지 분석 및 프로세싱
E-mail : ojkwon@sejong.ac.kr

신 동 규(Dong-kyoo Shin)
1986년 서울대학교 계산통계학과(학사)
1992년 Illinois Institute of Technology 대학원 컴퓨터과학과(석사)
1997년 Texas A&M University 대학원 컴퓨터과학과(박사)
1998년~현재 세종대학교 컴퓨터공학과 교수
관심분야 : 머신러닝, 유비쿼터스 컴퓨팅, 생체신호 데이터, 정보보호, etc.
E-mail : shindk@sejong.ac.kr