Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.211

금융회사 단말PC 재해복구 효율에 관한 연구

이 승 철,† 윤 준 섭, 이 경 호‡
고려대학교 정보보호대학원

Study on Disaster Recovery Efficiency of Terminal PC in Financial Company

Seung-Chul Yi,† Joon-Seob Yoon, Kyung-Ho Lee‡
Graduate School of Information Security, Korea University

요 약

금융회사의 재해복구시스템은 관련 법과 규정에 따라 적정 수준 유지를 위해 많은 투자가 이루어져 왔고 매년 1회 이상의 훈련을 통해 그 적정성을 검증하고 있다. 그러나 2013년 3.20 사이버 공격 시 동시다발적인 대규모 PC(Personal Computer) 불능사태가 발생하였고 복구에 많은 시간이 소요되어 목표한 수준의 업무연속성을 유지할 수 없었다. 그 이유는 재해복구 영역 중 PC 복구의 중요성이 상대적으로 간과되었기 때문이다.

본 논문에서는 3.20 사이버 공격을 가정하여 금융회사의 대규모 단말PC를 비용 대비 효과적으로 복구할 수 있는 방안을 제시한다. 또한, 제시한 방안에 따라 대규모 단말PC의 동시 복구 시간을 측정하여 금융감독기관의 금융회사 재해복구 권고시간인 3시간 내 업무연속성을 유지할 수 있는 단말PC의 동시 복구가 가능함을 검증한다.

유사한 규모와 형태로 단말PC를 운영 중인 금융회사들은 본 논문이 제시하는 방안을 참조하여 3.20 사이버 공격과 같은 재난 발생 시 효율적으로 대처할 수 있는 방안을 수립하고 적용할 수 있을 것으로 기대한다.

ABSTRACT

Financial companies have invested a lot in their disaster recovery system and exercised training more than once a year to comply related laws and regulations. But massive PCs(Personal Computers) became disrupted simultaneously and it took a lot of time to recover massive PCs concurrently when March 20 cyber attack occurred. So, it was impossible to meet the tartgeted business continuity level. It was because the importance of PC recovery was neglected compared to other disaster recovery areas.

This study suggests the measure to recover massive branch terminal PCs of financial companies simultaneously in cost-effective way utilizing the existing technology and tests recovery time. It means that in the event of disaster financial companies could recover branch terminal PCs in 3 hours which is recommended recovery time by regulatory body.

Other financial companies operating similar type and volume of branches would refer to the recovery structure and method proposed by this study.

Keywords: Terminal, PC, desktop, disaster, recovery, cyber attack, malcode, APT, BCP, DRP

I. 서 론

1.1 연구배경 및 목적

2013년 3월 20일 일부 방송사와 금융회사에 대한 사이버 공격으로 총 48,773대의 서버, PC, 자동화기기가 피해를 입었다. 농협은행은 PC 26,693대의 최종복구까지 총 10일이 소요되었다. 이번 사태로 인한 전체 피해금액은 8,672억 원으로 추정된다[1].

금융회사들은 매년 BCP(Business Continuity

접수일(2014년 12월 8일), 수정일(2014년 12월 29일), 게재확정일(2014년 12월 30일)

† 주저자, futurex@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

Plan)와 DRP(Disaster Recovery Plan)를 위해 많은 비용을 지출하고 있다. 또한, 업무연속성계획을 포함한 위기대응 행동매뉴얼을 수립하고, 연 1회 이상 훈련을 실시하여 감독기관의 규제사항을 준수하고 있다[2].

그럼에도 불구하고 3.20 사이버 공격 시 대규모 단말PC 복구에 수일 이상의 시간이 소요됨으로써 금융감독기관 규제 준수 위주의 전산센터 재해복구체계에 문제점을 드러냈다.

3.20 사이버 공격과 같이 악성 코드에 의해 PC의 MBR(Master Boot Record), VBR(Volume Boot Record) 영역이 파괴되어 단말PC의 부팅 자체가 불가능한 상황이 발생하면, 전산센터 내 시스템 가동 정상화 여부와 관계없이 영업점에서의 대고객 서비스 제공이 불가능하게 된다.

이는 금융회사의 업무연속성을 매우 심각하게 침해하는 것으로서 금융감독기관의 금융회사 재해복구 관련 권고사항인 RTO(Recovery Time Objective : 복구목표시간) 3시간 준수를 위한 DR(Disaster Recovery : 재해복구) 투자와 훈련이 무의미하게 된다.

따라서 대규모 단말PC 불능화에 대비한 복구계획은 BCP(Business Continuity Plan) 측면에서 업무연속성을 위한 중요한 영역으로 전산센터 시스템에 준하여 준비할 필요가 있다. 3.20 사이버 공격에 대한 정밀한 분석 및 대책마련을 통해 금융회사 단말PC에 대한 실질적인 복구 대책을 BCP 차원에서 포함시켜야 한다.

본 논문에서는 동시다발적 PC 불능사태에 대비 금융회사 영업의 전통적 채널인 영업점 단말PC를 RTO 3시간 이내에 실질적으로 복구할 수 있는 방안을 제시한다. 이를 위해 복구를 위한 구성 및 절차를 수립하고 테스트를 수행하여 3시간 이내에 금융회사 단말PC의 복구가 가능함을 실증한다.

금융회사들은 업무 특성상 대규모 영업점 네트워크를 기반으로 전산센터와 연결된 전용 단말 프로그램을 사용해 영업하는 경우가 일반적이다. 금융회사들은 본 논문에서 제시하는 방안을 참고하여 3.20 사이버 공격과 유사한 상황에 비용 대비 효과적으로 대처할 수 있는 방안을 수립하고 적용할 수 있을 것으로 기대한다.

1.2 연구방법 및 구성

본 논문에서는 3.20 사이버 공격 시 문제가 되었던 단말PC 불능화 현상 및 복구 지연에 대해 관련 자료를 검토하고, 대안을 비교 분석한다. 이를 통해 비용 효율적인 개선 방안을 제시한 후 3.20 사이버 공격을 가정하여 A금융사의 영업점 단말PC 복구를 위한 구성 및 테스트에 개선방안을 적용해 효과 분석을 수행한다.

본 논문의 구성은 다음과 같다. 제I장 서론에서는 연구배경/목적, 연구방법 및 논문구성에 대해 기술한다. 제Ⅱ장에서는 3.20 사이버 공격에 대한 분석을 수행하고 기존 BCP, DRP에서 PC 복구와 관련된 영역의 한계를 검토하여 금융회사 단말PC 현행 복구방법의 문제점을 도출한다. 제Ⅲ장에서는 금융회사 단말PC의 복구 대안들을 검토하고 비교 분석하여 비용 대비 효과적 방안을 제시한다. 제Ⅳ장에서는 금융회사 단말PC의 효율적 복구를 위한 구체적 방법을 기술하고 제V장에서는 제안된 복구방법에 대한 테스트 및 효과분석을 수행한다. 마지막 VI장 결론에서는 본 연구의 시사점 및 한계와 향후 발전방향에 대해 기술한다.

II. 선행 연구

2.1 3.20 사이버 공격 분석

2.1.1 사이버 공격으로 인한 피해 규모 및 복구 현황

2013년 3월 20일 오후 14시 경, 국내 금융권 및 방송사를 대상으로 전산 장애가 동시 다발적으로 발생하였다. 6개 회사가 보유한 32,552대의 PC가 일시에 오작동을 일으켰고 16,191대의 자동화기기 및 30대의 서버가 손상되었다. 또한, 해당 기기에 저장된 데이터도 악성코드에 의해 손실되는 사태가 발생했다[1]. 합동대응팀에 따르면 피해기관의 모든 시스템은

Table 1. Damaged System of 3.20 Cyber Attack[1]

Company	Server	PC	CD/ ATM	Total
NH Bank	-	26,693	16,121	42,814
Jeju Bank	-	320	70	390
Shinhan Bank	4	169	-	173
KBS	6	4,000	-	4,006
MBC	18	1,000	-	1,018
YTN	2	370	-	372
Total	30	32,552	16,191	48,773

2013년 3월 29일 12시에 복구되었다.

Table 2.에서는 3.20 사이버 공격 시 전체 PC의 복구 시간에 따라 계산된 시간 당 PC복구 대수를 보여준다. 가장 큰 피해를 입은 농협은행은 전체 직원수가 약 19,000명(2014년 5월 기준)이고 불능화된 PC가 26,693대로서 영업점에서 대고객 서비스를 제공하는 단말PC 대부분이 피해를 입었음을 알 수 있다.

농협은행은 시간당 복구된 PC의 대수가 333대로 타 회사에 비해 높은 편이다. 이것은 PC유지보수 가용 인원에 따라 달라질 수 있다. Table 2.에서는 복구시간을 정상 업무시간인 1일 8시간으로 계산하였으나 24시간 복구를 가정했을 때 농협은행의 시간당 복구 PC는 111대로 산정된다.

Table 2. PC Recovery Status of 3.20 Cyber Attack[1]

Company Name	No. of PC Halted	Recovery Time (Days)	No. of Recovered PC per Hour
NH Bank	26,693	80h(10)	333
Jeju Bank	320	40h(5)	8
Shinhan Bank	169	1h 45m	96
KBS	4,000	56h(7)	71
MBC	1,000	56h(7)	17
YTN	370	48h(6)	7

2.1.2 3.20 사이버 공격의 시사점

최근 10년 간 해킹공격의 트렌드는 목적, 기술, 목표 측면에서 변화해 왔다. 2000년대 초기 해커는 자기과시가 주된 목적이었으나 점차 금전적인 이득을 추구하는 것으로 변화해 왔고 최근에는 사회적 혼란을 목적으로 국가 기반 인프라를 파괴하는 사이버 테러의 양상으로 바뀌었다[3]. 또한, 내부 시스템 침투 후 장기적인 분석을 통해 취약점을 찾는 APT(Advanced Persistent Threat)공격이 증가하고 있다.

3.20 사이버 공격은 국내 다수의 기관을 공격대상으로 한 대표적인 APT공격이다. 3.20 사이버 공격 시 발견된 악성코드는 실행파일 형태로 다수의 변종이 존재한다. 해당 악성코드들의 주요 특징은 특정 프로세스를 종료시키고, 하드디스크의 MBR(Master Boot Record) 영역, VBR(Volume Boot Record) 영역, 데이터 영역을 일정간격마다 특정 문자열로 Overwriting 한 후 시스템 재부팅을 유도한다는 점이다[4]. 이로 인해 악성코드에 감염된 PC는 부팅 자체가 불가능했다.

금융회사는 3.20 사이버 공격 시와 유사한 동시다발적 대규모 PC 불능사태 발생 시 현행과 같이 한정된 수의 PC유지보수 인력을 통한 수기 복구 방식을 사용할 경우 신속한 대처가 불가능하다. 결국, 전산센터 내 서버 등 시스템을 정상화시키더라도 대고객 채널 말단에서의 서비스 제공 불가로 업무연속성을 보장할 수 없게 된다.

2013년 7월 금융위원회와 금융감독원은 "금융전산 보안강화 종합대책"을 발표하여 3.20 사이버 공격의 원천적 차단방법으로 금융회사의 망분리 의무화 방침을 내놓았다. 이에 따라 금융회사는 2014년 말까지 전산센터의 물리적 망분리 시스템 구축을 완료해야 하고 본점과 영업점은 단계적으로 추진될 예정이다[5].

그러나 금융회사가 물리적 망분리 시스템을 구축하더라도 모든 사이버 위협으로부터 안전하다고 할 수는 없다. 대외기관과의 인터페이스를 위한 중계서버 이용 망연계 및 PC간 자료이동을 위한 이동식 저장매체 사용 시 보안취약성 발생 개연성은 여전히 존재한다. 또한, 물리적으로 분리된 내부망에서 저장매체에 대한 보안통제를 무력화하여 악성코드를 배포하려는 악의적 의도를 가진 내부자의 범죄행위 가능성도 배제할 수는 없다.

따라서 금융회사는 업무연속성 확보를 위해 3.20 사이버 공격과 유사한 대규모 PC불능사태에 대비하여 체계적이고 효율적인 복구체계를 구축하고 지속적인 검증을 통한 보완을 수행해야 한다.

2.2 BCP, DRP에서의 PC 복구 영역 현황

BCP는 DRP를 포함하는 개념으로 재해 발생 시에도 핵심적인 비즈니스 기능을 지속할 수 있도록 전사적인 정책 및 절차를 수립/이행하는 것이다. BCP는 단순히 IT영역뿐만 아니라 비즈니스 영역까지 포함한다. 과거에는 전산부서 주도하에 IT시스템과 데이터를 복구하는데 중점을 두었으나 현재는 고객에게 중단 없이 서비스와 상품을 제공하기 위한 비즈니스 연속성에 중점을 두고 있다[6].

DRP는 재해/재난 시 전산센터 내 핵심 업무 시스템에 대한 복구 및 네트워크 복구에 대한 부분에 주로 초점이 맞추어져 있다. 국내 금융회사들은 전자금융감

독규정에 따라 RTO 3시간을 목표로 핵심 업무에 대한 재해복구시스템을 구축하고 매년 1회 이상 주센터와 재해복구센터 간 전환훈련을 수행하고 있다[2].

현행 BCP, DRP 관련 연구에서 PC 복구의 영역은 매우 작은 비중을 차지하고 있다. 화재나 홍수 등의 재해로 인한 물리적 불능사태에 대비해 가용자원을 확보하는 방안수립을 권고하는 수준에 그치고 있다. 3.20 사이버 공격 시와 같이 대규모 PC가 동시에 마비되는 사태는 전례가 없던 것으로서 복구계획 중요성에 대한 인식이 쉽지 않았기 때문이다.

A금융사는 재해복구 대상 단위업무로 "단말"이 포함되어 있고 RTO 0시간 부여를 통해 즉시 복구가 필요한 시스템으로 정의되어 있다. 또한 정기적 재해복구훈련을 통해 RTO 3시간 이내 복구능력을 검증하고 있다. 그러나 A금융사에서 "단말"이란 단위업무는 전산센터 내의 단말서버를 말하는 것으로 클라이언트, 즉 단말PC복구를 의미하지는 않는다. 3.20 사이버 공격과 유사한 사태 발생 시 대규모 단말PC의 복구 관련으로 대고객 서비스의 연속성에 차질이 생길 수도 있음을 의미한다. 따라서 사이버 공격 시 대규모 단말PC를 효과적으로 복구하는 방안을 최종사용자 관점에서 적극 검토하여 BCP에 포함시킬 필요가 있다.

2.3 사이버 공격에 의한 동시다발적 PC 불능화 시 금융회사의 현행 복구 현황(A금융사 사례를 중심으로)

A금융사는 1,000개 이상의 영업점 네트워크를 가진 국내 대표 금융회사이다. 금융회사 영업점의 PC유지보수는 유사한 방식으로 운영되므로 동시다발적 PC 불능화 시 A금융사의 현행 복구방법을 검토하여 금융회사의 복구 현황 수준을 가늠할 수 있다.

A금융사의 PC는 크게 2가지로 구분할 수 있다.

- 단말PC : 대고객 금융업무 처리 전용 단말프로그램이 설치되어 영업점 직원들이 사용하는 PC로서 통장프린터, 이미지 스캐너, PIN PAD 등 각종 주변기기들이 연결되어 있다.
- 일반PC : 대고객 금융업무 처리 전용으로 단말프로그램을 사용하지 않는 PC로서 본부부서 직원들이 주로 사용한다.

A금융사의 단말 프로그램은 엄격한 사용자 권한관리를 적용하여 특정 업무거래에 대해 인가된 직원만 시스템 이용이 가능하도록 운영하고 있다. 본부부서 직원들도 정보성 업무처리를 위해 단말 프로그램을 설치하여 사용하고 있으나, 이 경우 단말PC로 분류하지 않는다.

본 논문에서는 대고객 서비스 제공을 위한 영업점 단말PC를 업무연속성 차원에서 가장 중요한 복구대상으로 간주하였다. 따라서 일반PC에 대한 복구는 논외로 한다.

금융회사 중 국내 18개 은행의 영업점 운영 현황은 Table 3.과 같다. A금융사는 영업점 당 약 16대의 단말PC를 운영 중이므로 이를 적용 시 은행권 단말PC는 약 119,184대(은행권 전체 지점수 7,449 X 단말PC 16대)로 추정된다.

반면, 한국은행의 금융정보화 추진현황에 따르면 은행권에서 부분 아웃소싱을 하고 있는 PC등 기기의 유지보수 인원은 196명이며 이는 부분 아웃소싱 전체 영역의 9.1%를 차지하고 있다. 은행권 토탈 아웃소싱 인원은 542명으로 부분 아웃소싱 내 PC등 기기 유지보수 인원비율 9.1%를 단순 적용하면 약 50명으로 산정된다[8]. 따라서 은행권에서 PC 등 유지보수를 위한 외부직원은 약 246명으로서 다수의 은행과 중복해 유지보수 서비스를 제공하는 것으로 추정할 수 있다. 사이버 공격으로 은행권 단말PC 약 119,184대가

Table 3. Number of Branches at Banks(as of Jun. 2014) [7]

Name	No. of Branches
B Bank	1,192
C Bank	1,157
D Bank	991
E Bank	895
F Bank	628
G Bank	608
H Bank	349
I Bank	314
J Bank	264
K Bank	252
L Bank	168
M Bank	151
N Bank	134
O Bank	120
P Bank	92
Q Bank	82
R Bank	39
S Bank	13
Total	7,449

동시다발적으로 불능화 될 경우를 가정하면 유지보수 업체 직원 1인당 약 485대를 복구해야 하는 상황이 발생할 수도 있다.

비대면 채널의 급속한 확산으로 단말PC가 전체 채널에서 차지하는 거래 비중은 점차 줄어드는 추세이나 Table 4.의 A금융사 현황과 같이 단말PC의 거래 비중은 여전히 높은 편이다. 향후, 영업점 단말PC의 규모는 줄어들 가능성이 있으나, 전체 단말PC 차원에서는 급속한 변동이 있지는 않을 것이다. 왜냐하면, 금융회사는 이동식 지점의 개념으로 휴대용 장비를 통한 단말 프로그램 사용을 점차 확산시키고 있기 때문이다.

장기적으로 대고객 단말 프로그램을 사용하는 휴대용 장비도 단말PC의 범주에서 복구전략을 가져갈 필요가 있다. 따라서 국내 금융회사의 대고객 서비스 채널로서의 단말PC 중요성은 당분간 지속될 것으로 예상된다.

A금융사는 2014년 7월 말 기준으로 1,217개의 영업점을 운영 중이고, 19,381대의 단말PC가 영업점에 설치되어 있다. 또한, 영업점 단말PC의 유지보수를 위해 전국적으로 약 170여명의 출동직원을 보유한 외주업체 W사와 계약을 체결하고 있다. 지역별 특성 및 점포 밀집도에 따라 W사의 지사 별 유지보수 인원과 담당 지점 수는 차이가 있다.

3.20 사이버 공격과 유사한 상황 발생시 A금융사는 유지보수 업체직원이 영업점으로 출동하여 미리 준비된 부팅 가능한 USB 또는 CD 등의 복구매체를 통해 단말PC를 수동으로 복구한다. 이때, IP주소, 단말환경, 주변기기 설정 등 부가적인 작업이 필요하다. 이와 같이 대고객 서비스 개시를 위한 단말 프로그램 등 기본적 준비가 완료되기까지 단말PC 1대 당 약 80분이 소요된다.

Table 4. A Company's Transaction Portion of Channels Including Card System(As of Jun. 2014)

Channel	Portion of Transaction
Terminal PC	40.1%
ATM	10.5%
Internet Banking	22.1%
Mobile Banking	25.7%
Phone Banking	1.6%
Total	100 %

Table 5.는 윈도우XP 지원 중단에 따라 A금융사가 추진했던 단말PC 운영체제 업그레이드 작업내용과 소요 시간을 보여준다. Step 2의 메모리 증설을 제외하면 유지보수 업체직원이 불능화 된 단말PC를 복구하는 것과 동일한 과정임을 알 수 있다. 따라서 1대의 단말PC를 수동으로 복구 시 약 80분이 소요되는 것으로 산정할 수 있다. 이는 유지보수 업체 직원

Table 5. A Company's OS Upgrade Procedure and Required Time for Terminal PC

Step	Work Description	Time
1	▶ Check and Record Target Device and Information • CMOS P/W, Security Token P/W • Peripheral Device Connection and Setting Info.(Printer Port and IP, Scanner, etc.)	10m
2	▶ Add Additional Memory	10m
3	▶ OS Upgrade(Windows7) • OS Copy through the Terminal Program Deployment Image or USB	50m
4	▶ Terminal Environment and Network Setting • Install Security Token and Check the Status • Check the Terminal Program Loading • Check Peripheral Device Setting(Bankbook Printer, Normal Printer, Card Issuer, PIN Pad, etc.) • Reboot and Download Updates for Terminal Program	15m
5	▶ Online Test • Register Terminal Program User Transaction	5m
Total		90m

Table 6. A Company's Manual Recovery Time Estimation_Full Scale

No. of Maintenance Staff	No. of Terminal PC	No. of Terminal PC Per Maintenance Staff	Recovery Time
171	19,381	113.3	6.3 days

의 이동시간은 제외한 것이다.

이 때 현행 복구방법에 따라 전체 영업점 단말PC를 복구하기까지 Table 6.에서 보는 바와 같이 약 6.3일이 걸린다. 이는 단말PC 복구완료 시까지 복구작업을 24시간 풀가동 했을 경우를 가정한 시간이다.

III. 대규모 단말PC 복구 방법 비교

대규모 단말PC의 복구방법은 다음과 같은 방법들이 있다.

- 가상화 기술을 활용한 VDI(Virtual Desktop Infrastructure)

A금융사는 영업점 단말PC에 대해 논리적 망분리가 기 적용되어 운영 중에 있다. 그러나 단말 프로그램 사용 등 내부업무를 위한 부분은 PC기반으로 운영되고 인터넷 사용을 위한 영역이 가상 OS에서 실행되는 방식으로 VDI와는 차이가 있다.

- 개별 단말PC에 부팅 가능한 물리적 하드디스크 추가(데이터를 제외하고 기사용중인 하드디스크와 동일)
- WDS(Windows Deployment Services), DHCP(Dynamic Host Configuration Protocol) 서비스를 활용한 예약IP 할당 및 단말 프로그램/주변기기 개인화 설정 등 자동화 개발(본 논문에서 제안하는 방법)
- 유지보수 업체 직원이 이동식 저장매체를 휴대하고 영업점으로 출동한 후 수작업으로 단말PC를 복구하는 현행 방법

Table 7.은 대규모 단말PC에 대한 복구방법 대안들에 대해 다음과 같은 7가지 척도를 기준으로 정성적인 평가를 수행한 내용이다. 본 논문에서 최적의 방안을 선택한 가장 중요한 기준은 비용, 보안수준, 동시복구 수준이다.

- 비용 : 금융회사의 현행 PC기반 영업점 인프라를 기준으로 단말PC 불능화 시작 시점부터 복구시점까지 소요되는 TCO(Total Cost Ownership)
- 보안 : 복구방법에 내재된 위험에 대한 CIA(Confidentiality, Integrity, Availability) 측면 평가
- 동시복구 : 단말PC 복구 작업이 병렬로 동시 진행 가능한 수준
- 유지보수성 : 단말PC 문제발생시 원인파악 및 해결이 신속하게 가능한 수준
- 기술적 성숙도 : 복구방법 적용 시 기술적 제약사항 존재 여부
- 복잡성 : 복구방법 구현 및 운영 관련 기술적 고려사항 수준
- 구축기간 : 복구방법 적용을 위한 프로그램 개발 및 시스템 구성 기간

Table 7. Comparison of Massive Terminal PC Recovery Methods

Criteria	VDI	Cloned HDD	Proposed Method
Cost	High	Moderate	Very Low
Security	Good	Poor	Moderate
Simultaneous Recovery	Good	Moderate	Good
Maintainability	Good	Poor	Good
Technical Maturity	Moderate	High	High
Complexity	High	Moderate	Low
Construction Period	Long	Short	Short

VDI는 당초 목적이 기존 PC를 전면 대체하는 방안으로서 2014년 1월 외주직원 USB를 통한 카드사 정보유출 사건 이후 보안적 측면에서 많은 주목을 받고 있으며 기술적 성숙도가 높아짐에 따라 확산 추세에 있다. 그러나 VDI는 고가의 스토리지가 필요하고, 이중화, DR 구축이 필수적이므로 많은 초기 비용이 소요된다. 보안성이 가장 우수한 제로 클라이언트를 설치할 경우 가상화 PC 1대당 최소 300만 원 정도 소요되며 A금융사의 영업점 단말PC 19,381대를 대체할 경우 580억 원 이상 소요될 수 있다.

VDI의 보안수준은 제로 클라이언트를 도입할 경우 매우 높은 편이다. USB 사용 등이 원천적으로 차단되고, 모든 데이터는 전산센터의 스토리지에 집중되어 백업정책에 따른 관리가 가능하기 때문이다. 그러나 중앙 집중적 관리의 특성 상 가상 PC가 저장된 서버 공격 시 모든 인프라가 위험해 질 수 있다.

VDI는 기술적 성숙이 진행 중에 있어 금융회사의 영업점 단말PC 적용을 위해서는 철저한 검증이 필요하다. 동영상, 주요 장표 이미지 파일 전송 등 대규모 트래픽 발생 시, 네트워크 대역폭에 대한 문제가 완전히 해결되지는 않았다. 또한 초기에 많은 투자가 발생하는 만큼 장기적으로 이동식 기기를 활용할 경우에 대한 확장성도 반드시 검토해야 할 부분이다. 가트너 보고서에서도 2014~2015년의 기간 도안 모든 조직

들이 HVD(Hosted Virtual Desktop)의 기술 적용이 가장 적합한 사용자 유형을 주의하여 산정할 것을 권고한다[9]. 따라서 전체 조직에 적용하는 사례는 많지 않고 콜센터 등 정형화된 체계를 갖춘 업무 또는 보안취약성이 높은 외주직원 업무 등에 선별적으로 적용하고 있다.

VDI는 구축대상 및 방법에 따라 구현 및 관리가 복잡하고 확장성 등에 대한 고려사항이 많은 편이다. 이런 특성으로 구축기간에 많은 시간이 필요하다.

현재 사용 중인 하드디스크와 동일한 복제 본을 준비 후 PC 본체 내 추가 장착하여 비상시 기존 하드디스크를 대체하는 방법은 영업점 단말PC마다 하드디스크의 구매가 필수적이다. A금융사 영업점 단말PC의 하드디스크 최소 요건은 500G, 7200rpm이다. 이를 기준으로 하드디스크의 대표적 브랜드인 S사의 오픈마켓 가격 28개를 조사하여 계산한 결과 평균 단가는 51,125원으로 산정되었다[10]. A금융사 단말PC의 개수 19,381을 곱하면 하드디스크 구매에만 약 10억 원이 소요된다. 운영체제의 라이선스에 대한 부분도 비용이 소요될 수 있으나 금융회사의 경우 EA(Enterprise Agreement, 기업총괄협약) 방식으로 계약되는 것이 일반적이고 금융회사별 개별성이 존재하므로 본 논문에서는 해당 비용 산정을 제외한다.

물리적으로 분리된 복제 하드디스크를 복구에 사용하는 것은 개념적으로 단순하고 적용이 용이한 장점이 있다. 따라서, 단기간 내에 구축이 가능하다.

그러나 평상시 하드디스크를 PC 메인보드에 연결하지 않은 상태로 유지해야 하며, 주기적으로 운영체제와 단말프로그램 간 패치를 유지해야 하는 관리공수가 필요하다. 운영체제 패치버전에 따라 단말 프로그램이 구동되지 않을 수도 있기 때문에 이런 부분은 사전에 준비가 되어야만 한다.

무엇보다도 수많은 지점에 분산되어 있는 대량의 단말PC를 분해하고 조립하는 과정이 필요하므로 보안적으로 매우 취약한 상황에 놓일 수 있다. 금융회사들은 USB, DVD 등 이동식 매체에 대한 통제를 강화하는 추세이므로 PC 내 하드디스크 탈부착은 보안정책에 위배될 수밖에 없다. 따라서 하드디스크의 복제본을 사용하는 방법은 가장 쉽게 적용할 수 있는 방법이지만 보안정책에 위배되기 때문에 적합하지 않다.

동시복구를 위해서는 영업점 직원들이 자신의 PC에 대해 하드디스크 연결 등의 작업을 자체적으로 수행하는 것이 가장 이상적이다. 그러나, 비상용 하드디스크 최신화를 위한 작업을 영업점 직원들의 관리 하에 맡기는 것은 현실적으로 쉽지 않다. 하드디스크의 연결/분리방법은 비교적 간단한 작업에 속하나 일정수준 교육/훈련이 필요하고, 연결 후 작동 오류가 생기는 경우 책임소재가 불분명해질 수 있다. 유지보수 업체가 비상용 하드디스크를 주기적으로 관리하는 것 또한 비용과 시간을 고려할 때 적합하지 않다.

본 논문에서 제시하는 단말PC 복구 자동화 방법은 기존 인프라를 최대한 활용하면서 수기 작업 부분을 자동화하는 프로그램을 개발하는 방법으로서 추가적인 자원도입 비용이 필요하지 않다. 금융회사 별로 차이는 있을 수 있으나, AD(Active Directory)서버, SCCM(System Center Configuration Management)서버 등은 윈도우 기반 단말PC의 관리를 위해서 필수적인 부분이므로 복구를 위한 추가 비용으로 산정하지 않는다.

단말PC 복구 자동화 방법은 VDI 제로클라이언트에 비해 보안 수준은 약한 편이다. USB를 사용할 수 있고, 데이터의 중앙 집중화는 구현되어 있지 않기 때문이다. 그러나 현행 단말PC에도 보안을 위한 많은 프로그램과 정책이 이미 적용되어 있고, 배포서버의 역할을 하는 영업점 파일서버의 경우 락다운을 통해 확인되지 않은 프로세스의 기동 자체가 불가능하다.

단말PC 복구 자동화 방법은 특정 PC의 복구 자체를 자동화 처리할 수도 있으므로 유지보수 측면에서도 이점을 갖는다. 또한 복구 자동화 프로그램은 스크립트 언어 기반 프로그램으로 작성이 심플하고 기존 자원을 활용하는 것이므로 단기간에 구축 및 적용이 가능하다.

현행과 같이 유지보수직원에 의한 수동 복구 작업은 복구에 수일 이상 걸리는 것으로서 업무연속성을 만족할 수 있는 방법이 아니므로 비교 대상에서 제외한다. 따라서 본 논문에서 제시할 개선된 대량 PC복구 방법은 현재 시점에서 가장 비용효율적인 방법이라고 할 수 있다.

IV. 개선된 대규모 PC 동시 복구 방법 제안

4.1 복구 우선순위 단말PC 규모 산정

대규모 PC를 동시 복구할 때 무엇보다 중요한 것은 우선 복구대상을 선정하는 것이다. 모든 단말PC를 동시에 복구하는 것이 가장 이상적이지만 주어진 자원과 환경의 제약이 존재하므로 가장 효율적인 방법을 고려해야 한다. 업무 별로 RTO를 산정하는 것도 이

런 이유 때문이다. 복구 우선순위 단말PC 규모를 산정하는 것은 효율적 복구를 위한 첫 번째 단계이다.

A금융사의 업무는 창구 특성에 따라 다음과 같이 크게 5가지로 구분할 수 있으며, 업무에 따라 사용자 권한이 분리되어 있다.

- 상품판매
- 온라인 입출금
- 가계여신
- 기업여신
- VIP

이중 VIP를 제외한 4개 창구 업무에 해당하는 4대의 단말PC를 우선적으로 복구할 필요가 있다. 또한, 복수 책임자 승인을 할 수 있는 최소 2대의 단말PC가 필요하다. 따라서 우선적으로 복구가 필요한 대수는 총 6대로 산정할 수 있으며, 이는 곧 영업점 업무연속성을 위한 단말PC 복구의 최소 수준이라고 말할 수 있다.

Table 8.은 복구 우선순위를 고려한 영업점 단말PC 총 6대를 현행 방법에 따라 수동 복구할 경우 소요되는 시간을 보여주고 있다. 이 경우도 2일 가량 소요됨에 따라 업무연속성이 보장되지 않음을 알 수 있다.

Table 8. A Company's Manual Recovery Time Estimation _Minimum Business Continuity

No. of Maintenance Person	No. of Terminal PC for Minimum Business Continuity	No. of Terminal PC/Maintenance Person	Recovery Time
171	7,302	42.7	2.4 days

4.2 구성방법

단말PC 복구 구성은 영업점 직원의 최소 작업만으로 다음과 같은 복구를 자동화하는 것을 목표로 한다.

- 운영체제 설치 및 네트워크 설정
- 필수 소프트웨어 설치
- 보안 프로그램 설치 및 업데이트
- 전용 단말 프로그램의 설정
- 주변기기의 설정

무엇보다 중요한 것은 영업점 단말PC가 개인화된 상태로 복구되어 추가적인 설정 작업이 필요하지 않아야 한다는 점이다. 이와 같은 영역은 네트워크 설정, 단말프로그램 정보 등록, IP주소관리시스템 사용 등록, 주변기기의 설정 등이 포함된다.

전산센터의 관리자는 SCCM서버를 통해 영업점 파일배포 서버로 보안소프트웨어를 포함한 단말 프로그램 설치 마스터 이미지를 배포한다. 이때 마스터 이미지의 크기가 10G Byte 이상으로 매우 크기 때문에 전산센터와 영업점간 네트워크의 회선 속도(A금융사의 경우 백업회선인 ADSL(Asymmetric Digital Subscriber Line) 대역폭 중 3Mbps 할당)를 고려하여 야간시간 대 영업점 배포를 스케줄링 한다.

영업점 단말PC는 작업스케줄러를 통해 해당 PC의 설정 데이터를 파일서버에 주기적으로 자동 전송하고 갱신한다(AD정책 일괄 적용). 이 작업이 중요한 이유는 단말PC별로 개인화된 설정정보들을 항상 최신으로 유지할 수 있기 때문이다. 단말PC 복구 자동화 프로그램은 이 정보를 활용해 수기복구 작업에 걸리는 시간을 획기적으로 줄여준다.

이때 수집하는 주요 데이터는 다음과 같다.

- IP주소
- 컴퓨터 이름
- MAC(Medium Access Control)주소
- 단말기기 점번

Fig. 1.은 영업점 파일서버에 주기적으로 저장되는 개별 단말PC 별 정보사항을 보여준다.

다음은 구성방법 중 핵심인 DHCP를 통한 예약IP 할당 및 WDS 구동 관련 복구 자동화 프로그램을 파일서버의 시작 프로그램에 사전 등록한다.

영업점내 파일 배포서버는 평시에 해당 영업점 직원들을 위한 단말 프로그램 배포역할을 수행하고, 모든 서비스와 프로세스는 화이트리스트 기반으로 제한

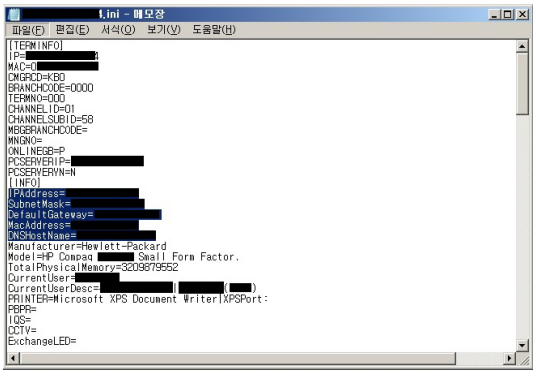


Fig. 1. Terminal PC Information Stored Periodically to File Server

되어 운영된다. 따라서 등록된 자동화 프로그램은 평시에 작동하지 않고 전산센터의 관리자가 영업점 파일서버를 비상 모드로 전환해야 자동으로 시작된다.

복구 자동화 프로그램은 Visual Basic 6.0을 통해 개발한 것으로서 개별 단말PC마다 수기로 작업할 수밖에 없는 다음과 같은 절차를 자동화하여 복구시간을 크게 단축시킨다.

- DHCP 서비스에 각 단말PC의 IP주소 할당 예약(유지보수 직원이 개별 단말PC에 수기 작업하는 부분으로서 기존 네트워크 정보의 확인 절차가 필요함. 모든 단말PC 불능화시 기존 네트워크 정보를 확인하기 어려우며, 신규 네트워크 정보 설정시 추가적으로 IP주소관리시스템에 수기 등록해야 정상적인 네트워크 사용이 가능함)
- 운영체제 배포 및 자동설치 Task Sequencing 구성
- AD 이행 자동화

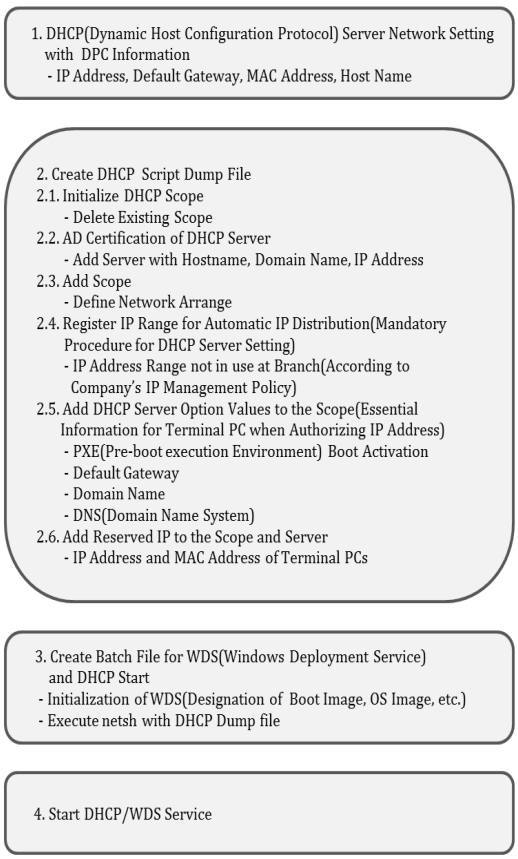


Fig. 2. Procedure of Recovery Automation Program for Terminal PC

- 전용 단말 프로그램 정보등록(모든 영업점 직원이 수기 등록하는 작업으로서 IP주소와 MAC주소 맵핑)
- IP주소관리시스템 등록 및 승인(기존 설정의 개인화 복원에 따라 개별 단말PC마다 수행되어야 하는 본 작업이 없어짐)
- 주변기기 드라이버 설치 및 포트 정보 등록

Fig. 2.는 단말PC 복구 자동화 프로그램의 내부에서 수행되는 절차를 보여준다.

먼저 영업점 파일서버의 네트워크 정보를 수집하여 DHCP서버를 구성한다. 다음으로 개별 단말PC에 예약된 IP를 DHCP 서비스에 세팅하기 위한 Dump파일을 Fig. 3.과 같이 생성한다.

마지막으로 WDS 및 DHCP 서비스를 실행하기 위한 Batch파일을 생성하고 실행시킨다. 이 과정에서 중요한 것은 netsh 명령어이다. netsh 명령어를 금융회사의 환경에 따라 적절히 활용하여 단말PC의 개인화 복구를 자동화하는 것이 단말PC 복구 자동화 프로그램의 핵심이다.

Fig. 4.는 복구 자동화 프로그램의 실제 소스코드 일부를 보여준다.

DHCP 서비스만 사용할 경우 단말PC에 임의의 IP가 부여되게 된다. 이 경우, 단말 프로그램의 개별 정보세팅이 필요하게 되고, IP주소의 불법사용을 통제하는 IP주소관리시스템에 의해 네트워크 사용이 차단된다. 따라서 모든 단말PC 사용자는 IP를 등록하고 승인받는 절차를 거쳐야 한다. 또한, 개인화된 환

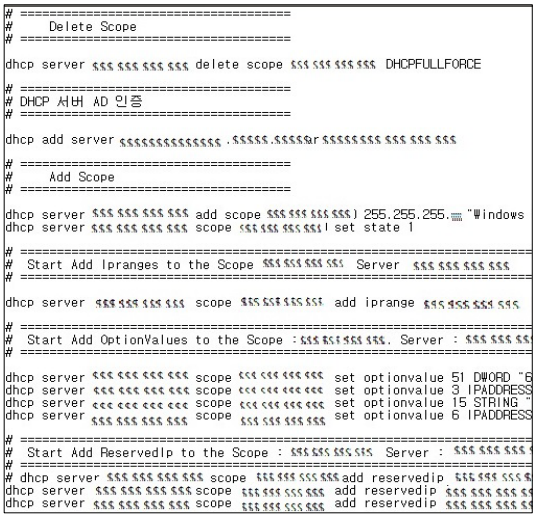
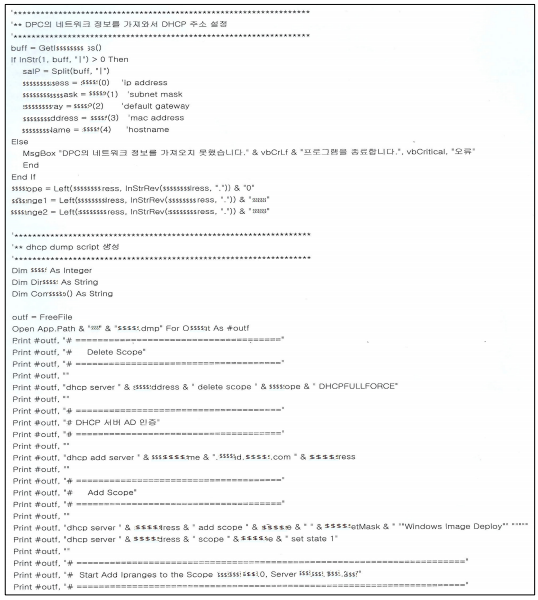


Fig. 3. Dump File for netsh



```
'**********************************************************************
'** DPC의 네트워크 정보를 가져와서 DHCP 주소 설정
'**********************************************************************
buff = GetIssssssss ss()
If InStr(1, buff, "|") > 0 Then
    salP = Split(buff, "|")
    sssssssssssss = sssss(0)    'ip address
    sssssssssssask = sssss(1)   'subnet mask
    sssssssssray = sssss(2)     'default gateway
    sssssssddress = sssss(3)    'mac address
    sssssssslame = sssss(4)     'hostname
Else
    MsgBox "DPC의 네트워크 정보를 가져오지 못했습니다." & vbCrLf & "프로그램을 종료합니다.", vbCritical, "오류"
    End
End If
ssssope = Left(sssssssssress, InStrRev(sssssssssress, ".")) & "0"
ss$singe1 = Left(sssssssssress, InStrRev(sssssssssress, ".")) & "ssss"
ssssinge2 = Left(sssssssssress, InStrRev(sssssssssss, ".")) & "sssss"

'**********************************************************************
'** dhcp dump script 생성
'**********************************************************************
Dim $$$$! As Integer
Dim Dir$$$$! As String
Dim Com$$$$$() As String

outf = FreeFile
Open App.Path & "\\" & "$$$$$:dmp" For O$$$$$t As #outf
Print #outf, "# ========================================="
Print #outf, "#     Delete Scope"
Print #outf, "# ========================================="
Print #outf, ""
Print #outf, "dhcp server " & $$$$$ddress & " delete scope " & $$$$ope & " DHCPFULLFORCE"
Print #outf, ""
Print #outf, "# ========================================="
Print #outf, "# DHCP 서버 AD 인증"
Print #outf, "# ========================================="
Print #outf, ""
Print #outf, "dhcp add server " & $$$$$$$me & ".$$$$d.$$$$:.com " & $$$$.ress
Print #outf, ""
Print #outf, "# ========================================="
Print #outf, "#     Add Scope"
Print #outf, "# ========================================="
Print #outf, ""
Print #outf, "dhcp server " & .$$$$$ress & " add scope " & $$$$$e & " " & $$$$:tetMask & " ""Windows Image Deploy"" """"
Print #outf, "dhcp server " & $$$$:ress & " scope " & $$$$%g & " set state 1"
Print #outf, ""
Print #outf, "# ========================================================================="
Print #outf, "#  Start Add Ipranges to the Scope  $$$$$$!$$$L0, Server $$$!$$$!, $$$!, $$$!"
Print #outf, "# ========================================================================="
```

Fig. 4. Source Code of Recovery Automation Program for Terminal PC

경설정 정보를 통한 자동복구가 아닌 경우 단말PC에서 필수적으로 사용하는 통장프린터, 이미지 스캐너 등 많은 주변기기에 대한 세팅도 수기로 설정해야 한다.

복구 자동화 프로그램은 최신화된 개별 단말PC의 정보를 수집하고 복원하는 방식을 사용하여 이러한 문제점들을 해결한다. DHCP에 단말PC IP 정보를 수기로 등록할 경우 Fig. 5. ~ Fig. 8.에 걸친 작업이 필요한 바, 자동화 프로그램은 복구시간 단축을 위해 이 작업들을 자동화시켰다.

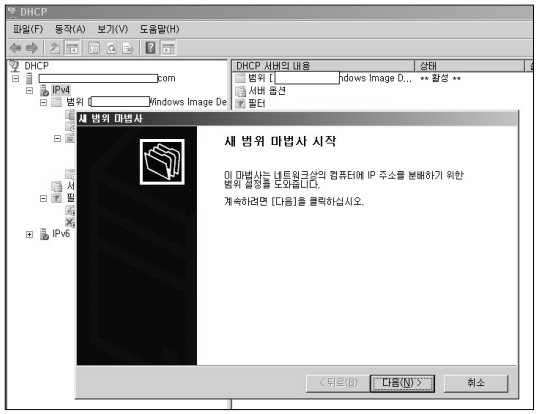


Fig. 5. DHCP Manual Setting Screen(1/4)

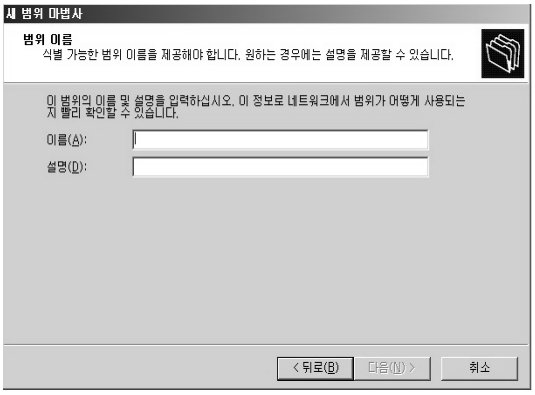


Fig. 6. DHCP Manual Setting Screen(2/4)

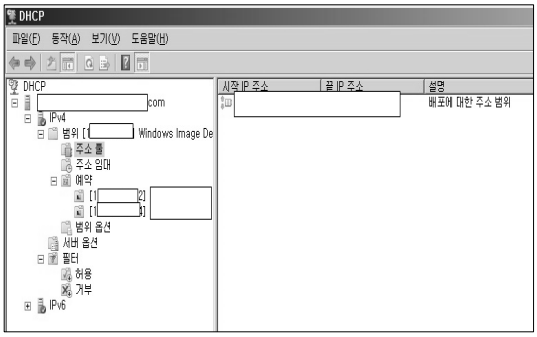


Fig. 7. DHCP Manual Setting Screen(3/4)

Fig. 8. DHCP Manual Setting Screen(4/4)

4.3 복구절차

Fig. 9.는 단말PC 복구와 관련된 전체 과정을 도식화하여 보여준다.

재난발생시 전산센터 단말시스템 운영자는 원격으로 영업점 내 파일서버를 네트워크 접속이 가능한 비

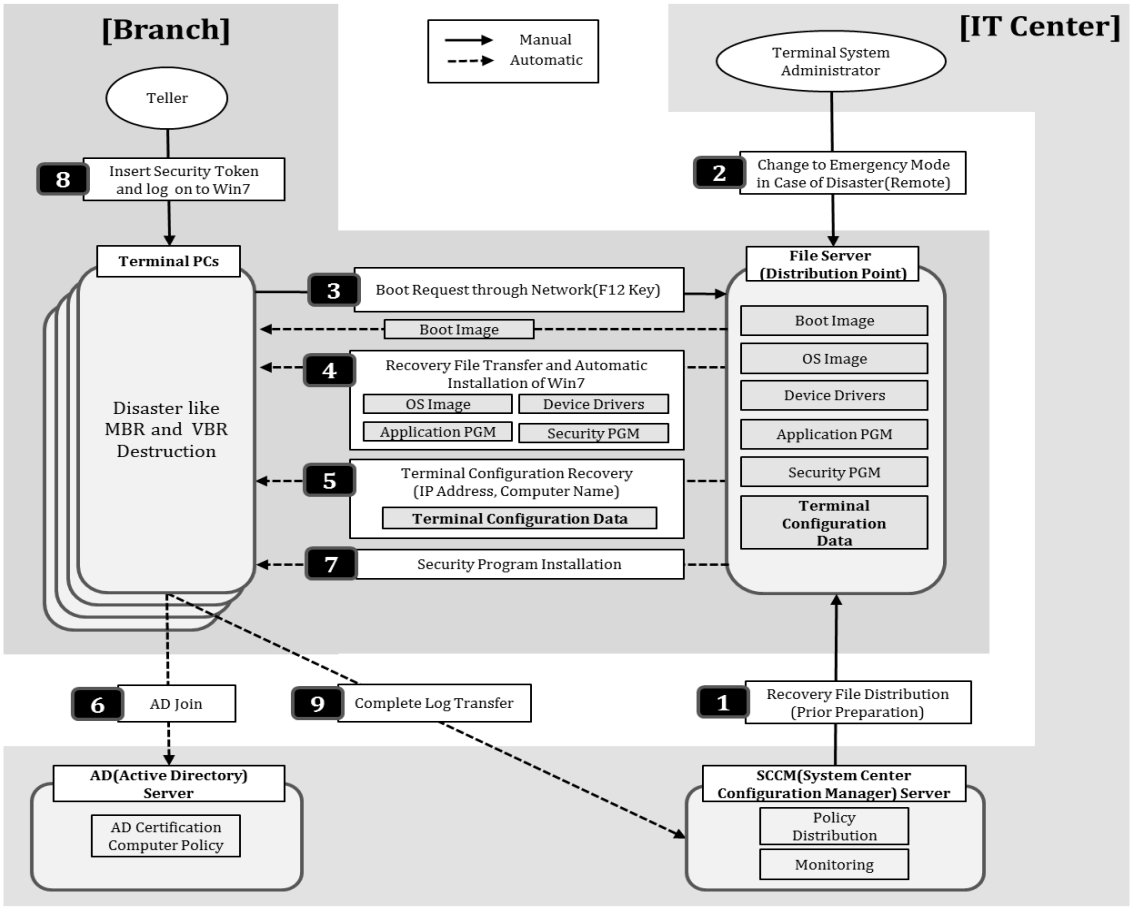


Fig. 9. Recovery Automation Process of Terminal PCs

상 모드로 변경한다. 비상 모드 전환에 따라 파일서버는 재부팅 되고 시작프로그램이 활성화되어 기존에 등록된 복구 자동화 프로그램이 구동된다.

복구 자동화 프로그램은 복구정보가 담긴 Dump파일을 생성한다. 또한 Dump파일을 참조해 복구진행을 수행하는 Batch 프로그램을 작성하여 구동시킨다. Batch 프로그램이 종료되면 예약된 IP 할당을 위한 DHCP서비스 및 운영체제 이미지 및 관련 프로그램 배포를 위한 WDS 서비스가 활성화 된다.

Fig. 10.은 비상 모드로 변환 시 영업점 파일서버의 복구 자동화 프로그램이 시작프로그램에 등록된 모습을 보여준다. 평시 파일서버 화면에는 모든 것이 비활성화 되어 있다.

Fig. 11.과 같이 영업점 직원이 단말 부팅시 F12 키를 눌러서 PXE(Pre-boot eXecution Environment)로 부팅하면 자동으로 운영체제 및

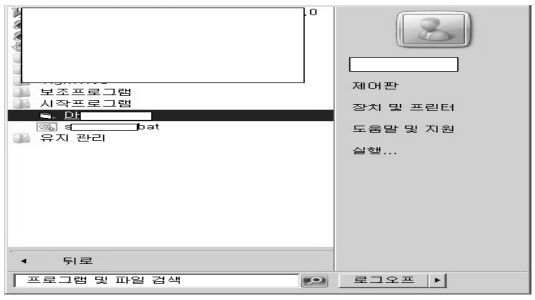


Fig. 10. Transition to Emergency Mode(File Server)

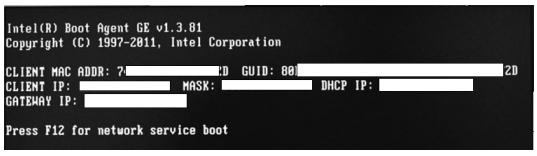


Fig. 11. Network Boot Mode

단말 프로그램 등 필수 프로그램이 설치된다. 또한, AD 가입이 순차적으로 자동 수행된다. 영업점 직원은 마지막 단계에서 소지한 보안토큰을 단말PC에 삽입하고 사용자 맵핑을 통한 윈도우 로그온이 완료된다.

보안토큰의 기능은 단말PC 사용자의 정당성을 체크하는 것으로서 네트워크를 통한 인증을 수행하지는 않는다. A금융사의 모든 직원들은 PC사용을 위해 보안토큰을 항시 휴대하도록 되어있다. 또한, 네트워크를 통한 모든 작업 시 보안토큰에 기반하여 초기화된 사용자 정보가 사용된다.

V. 실증

5.1 복구 테스트 결과 및 효과 분석

본 논문에서는 시범 영업점 1개를 대상으로 현행 운영중인 인프라인 100Mbps 네트워크에 테스트용 단말PC를 설치하여 총 3회에 걸친 테스트를 수행하였다.

Table 9.에서 보는 바와 같이 영업점 네트워크 내에서 동시에 접속하는 단말PC가 늘어남에 따라 복구시간이 지연됨을 알 수 있다.

그러나 앞서 언급한 바와 같이 영업점에서 업무연속성을 위한 최소 복구 대수를 6대로 가정한다면 90분 내에 업무 연속성 보장을 위한 최소 수준을 충족시킬 수 있다. 네트워크 대역폭은 90% 이상을 점유했으므로 6대를 초과하여 동시에 복구를 시도하는 것은 적합하지 않다.

따라서 단말PC 6대를 먼저 복구하여 대고객 서비스를 제공하면서 나머지 90분에 다시 6대를 복구하는 것이 네트워크 부하에 따른 추가 소요 시간을 줄일 수 있는 방안으로 결론지었다. 이 경우, 총 180분(3시간) 내에 12대를 복구할 수 있어 영업점 1개당 평균 16대의 단말PC를 보유함을 감안할 때 약 75%의 복구율을 예상할 수 있다. 업무연속성 측면에서 대고객 서비스를 제공하는 최일선 단말PC들은 신속하게 복구됨을 알 수 있다.

Table 9. Recovery Time of Current Terminal PCs at 100Mbps Branch Network

Tested Terminal PCs	Averaged Recovery Time
1	50 min
2	70 min
6	90 min

또한, 향후 노후기기 교체에 따라 도입 후보군에 있는 총 5종의 단말PC에 대한 테스트를 2015년 상반기 구축 완료 예정인 IPT(IP Telephony; 통신인프라 고도화) 테스트 환경(1Gbps 영업점 네트워크)에서도 수행하였다. IPT는 금융회사를 중심으로 수년 전부터 추진되어 온 사업으로서 전 금융권에 유사한 수준의 통신인프라 환경이 갖춰질 것이다.

Table 10.에서 보는 바와 같이 단말PC 6대의 복구에 30분이 소요되었으며 네트워크 대역은 약 50%를 점유했다. 이는 단말PC의 사양이 좋아진 점과 더불어 영업점 내 네트워크 대역폭 증가에 따른 결과이다.

따라서 2015년 상반기 이후에는 30분 내에 업무연속성을 위한 최소 수준의 영업점 단말PC 복구도 가능할 것으로 예상된다. 또한, 지점당 평균 16대의 단말PC를 보유하고 있으므로 적어도 1.5시간 내에 전체 영업점 단말 PC의 복구가 가능하다.

Table 10. Expected Recovery Time of To-be Terminal PCs at 1Gbps To-be Branch Network

Tested Terminal PCs	Recovery Time
1	20 min
6	30 min

5.2 개선 효과

3.20 사이버 공격과 같은 동시다발적 대규모 PC불능화시 본 논문에서 제안한 방법을 적용하면 업무연속성 측면에서 1시간 30분 내에 주요 단말PC를 복구하여 대고객 서비스를 제공할 수 있다. 또한, 통신 인프라 고도화에 따른 영업점 네트워크 대역폭 확대 시 1

Table 11. Comparison of Recovery Time

No. of PCs	As-is	Proposed Method	Proposed Method After IPT
Critical Terminal PCs(6EA per Branch)	2.4 days	90 min	30 min
Total Terminal PCs(16EA per Branch)	6.3 days	270 min	90 min

시간 30분 내에 전체 단말PC의 복구가 가능하다.

전체 영업점 단말PC를 대상으로 기존에 최소 약 6.3일 걸리던 것이 3시간 이내에 복구가 가능함을 알 수 있다. 또한, 격지에 위치한 영업점의 경우 유지보수 업체의 출동 전 1시간 전후로 복구하여 업무를 즉시 수행할 수 있다.

VI. 결론 및 향후 발전방향

6.1 결론

9.11 테러이후 재해복구시스템 및 BCP의 필요성이 제고되었고 감독기관들의 규제에 따라 금융회사의 업무연속성체계는 일정 수준 이상을 충족하는 수준에 이르렀다. 그러나 2013년 3.20 사이버공격 시 영업점 단말PC의 동시다발적 불능에 대처할 수 있는 준비가 되어 있지 않아 농협은행의 경우 최종 복구완료까지 최대 10일이 소요되는 사태가 발생하였다.

지금까지 재해복구시스템 구축은 전산센터 내의 서비스 제공에 중점을 두어 왔고 매년 실시하는 훈련도 전산센터 내 서비스 정상화 시간을 기준으로 RTO 충족여부를 측정하였다. 그러나 전산센터 내 서비스가 정상화되더라도 고객과 직접 대면하여 업무를 처리해야 하는 영업점에서 단말PC를 사용할 수 없다면 제대로 복구가 되었다고 말할 수 없다. 실제 대고객 서비스가 이루어지는 것은 채널의 말단인 영업점 단말PC이기 때문이다.

본 논문에서는 영업점 단말PC 복구를 위해 기존 자원을 활용함으로써 최소의 비용으로 최대의 효과를 얻고자 하였다. 영업점 창구 단말 프로그램 배포를 위한 파일서버 등 기존에 보유한 자원과 운영체제에서 기본적으로 제공하는 DHCP등의 현행 기술을 사용하여 단말 프로그램 사용에 필요한 설정정보 백업 및 복원, IP주소관리시스템의 보안 준수사항을 즉시 만족할 수 있는 방안을 마련하여 시스템을 구성하였다.

또한, 시범 영업점을 선정하여 복구시간을 테스트하고 IPT와 같이 향후 구성 완료될 환경 및 신규도입될 단말PC 기종에 대한 테스트도 실시하였다. 그 결과 3.20 사이버 공격과 같이 악성코드에 의한 동시다발적 하드디스크 파괴를 가정하였을 때 최소 6일 이상 복구 및 정상화에 걸리던 시간이 감독기관 규제 목표시간인 3시간 이내에 가능할 수 있음을 검증하였다.

실제 상황에 대비하여 영업점 직원들은 단말PC 복구방법에 대한 기본적인 내용을 숙지하여야 하고, 전산부서도 사전에 이와 같은 복구 시나리오를 적극적으로 알리고 교육하여 비상시 대응 프로세스를 최적화시킬 필요가 있다. BCP차원에서 단말PC의 복구 절차가 포함되어야 하는 것이다.

본 논문에서 제시한 영업점 단말PC 관련 구성 방법은 유사한 규모와 영업점 환경을 가진 금융회사에서 활용할 수 있을 것이다. 또한, 현행 재해복구의 미비한 점을 보완함으로써 실제 상황에서 업무연속성 유지 가능성을 더욱 높이는데 기여할 것이다.

6.2 한계 및 향후 발전방향

본 논문에서는 금융회사의 영업점에서 대고객 서비스를 제공하는 단말PC 복구에 초점을 맞추었다. 그러나 영업점 직원들이 단말PC에 개별적으로 저장해 놓은 데이터의 복구는 포함되지 않았다.

영업점의 경우 대고객 서비스 제공을 위한 데이터는 전산센터 내에 존재하며 단말 프로그램을 통해 제공받을 수 있다. 그 외 영업점 대고객 서비스에 필수적인 것이 아니지만 개인적 관리 자료들은 필요 시 그룹웨어 전자메일 등에 별도 저장이 가능하므로 개별 단말PC 데이터 복구에 대한 이슈는 일정부분 해소될 수 있다.

본점의 경우도 업무연속성 차원에서 중요한 PC들을 조사한 후 본 논문에서 제안한 방법을 응용하여 하나의 지점에 해당되는 복구방법을 구성할 수 있다. 또한, 장기간에 걸친 APT공격이 수행되는 최근의 트렌드를 감안하여 악성코드에 감염되었으나 탐지되지 않을 경우에 대비한 주기적 단말PC 포맷도 고려할 수 있다.

향후 연구에서 동시다발적 PC 데이터 파괴 시 신속히 데이터를 복구할 수 있는 방안이 추가적으로 포함된다면 보다 안정적인 업무연속성 확보에 도움이 될 것으로 기대한다.

References

[1] Youngyung Shin, Sanghun Jeon, Chaeho Lim, Myungchul Kim, "Economic Damages Assessment for National Cyber Security Measures," Journal of KANIS vol.6 no.1, 2013, pp.129-173, Oct. 2013

[2] Financial Services Commission, "Regulation on Supervision of Electronic

Financial Activities," Jan. 2014
〔3〕 Eungjae Lee, "3.20 Cyber Attack, and its Malwares," Korea Internet and Security Agency, Jun. 2013
〔4〕 Red Alert, "3.20 Cyber Terror Analysis Report v.1.7," NSHC, Apr. 2013
〔5〕 http://www.etnews.com/20141029000053, Oct. 2014
〔6〕 Financial Supervisory Service, "Detailed Guideline for Basel II Operation Standard," Oct. 2006
〔7〕 Korea Federation of Banks, http://www.kfb.or.kr/new_data/etc.html?S=GAE&m=view&table=PDS3&no=252&start=0&mode=search&field=title&s_que=%C1%A1%C6%F7, Jun. 2014
〔8〕 Committee on Financial Informatization Promotion, Payment & Settlement Systems Department, "Financial Informatization Promotion Status in 2013," The Bank of Korea, Jul. 2014
〔9〕 John P Morency, Carl Claunch, Pushan Rinnen, "Hype Cycle for IT Service Continuity Management, 2014," Gartner Inc., Sep. 2014
〔10〕 http://prod.danawa.com/info/?pcode=1464268&cate1=877&cate3=977&cate4=0, Dec. 26, 201

〈저자소개〉

이 승 철 (Seung-Chul Yi) 정회원
1999년 2월: 연세대학교 신문방송학과 학사
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융정보보안, 위험관리

윤 준 섭 (Jun-Seob Yoon) 학생회원
2014년 2월: 중앙대학교 컴퓨터공학부 학사
2014년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융정보보안, 위험관리

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, nhn, 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책