내부 네트워크의 성능저하요인에 따른 이산화탄소배출에 관한 연구

종신회원 전 정 훈*

A Study of Carbon Dioxide Emissions due to the Performance Degradation Factors of An Inner Network

Jeon-Hoon Jeon* *Lifelong Member*

요 약

최근 지구온난화 문제는 전 세계의 매우 심각한 환경문제로 대두되고 있으며, 이를 해결하기 위한 방안으로 '그린 IT'가 이슈화되고 있다. 이러한 상황에서 네트워크는 진화와 함께 다양한 공격기술들이 나타나고 있어, 대부분의 여러 보안장치 및 시스템들을 추가 배치하고 있다. 그러나 이와 같은 네트워크 구축방법은 내부 네트워크의 성능과 보안에 큰 영향을 미치며, CO_2의 배출량을 증가시키고 있다. 따라서 본 논문은 내부 네트워크의 성능저하 요인에 따른 CO_2배출을 분석하여, 향후 내부 네트워크의 성능 및 보안성 향상과 IT분야의 CO_2배출을 경감하기 위한 자료로 활용될 것으로 기대한다.

Key Words : Security System, Carbon Dioxide Emission, Network Performance, Firewall, VPN, Inner Attack

ABSTRACT

Recently, The Problem of Global Warming around the world, is emerging as a very serious environmental problems, and as a way to fix it 'Green IT' is becoming an Issue. In these situations the evolution of network technologies with a various attacks, it appears, add the different security devices and systems are deployed. But, Deployment methods such a network, the performance and security of the internal network will affect on the greater and it will be increase Carbon Dioxide emissions. Therefore, In this paper, it will be to analyze Carbon Dioxide Emissions due to the Performance Degradation Factors of An Inner Network. and In a future, This paper is expected to serve as a valuable Information for the Network Performance and Security improvements and to reduce Carbon Emissions in the Field of IT.

Ⅰ. 서 론

최근 녹색 기술에 대한 관심이 전 세계적으로 확대되고 있는 가운데, 세계 여러 나라들의 기업 및 단체들은 저탄소 배출을 위해 다양한 그린(Green)정책들을 제시하고 있다[1]. 또한 이와 같은 그린정책들은 IT 부분에까지도 확대되어 에너지 효율을 고려한 다양한 연구가 진행 중에 있으며, 제품의 부품 및 자재뿐만 아니라, 생산 및 응용에 이르기까지 범위가 매우 광범위하게 전개되고 있다[2].

특히 네트워크는 IT분야에서 비교적 많은 양의 CO_2를 배출하고 있는 부분으로써, 전송매체와 중계장비, 그리고 보안시스템 등의 복합구성으로 이루어져 있기 때문에 시스템의 자체 부하가 크고, 이에 따르는 전기 소모량도 매우 높게 나타나고 있다. 이중, 보안시스템은 [3]의 성능저하 실험에서와 같이 하부 네트

* 동덕여자대학교 컴퓨터학과 (nerdrandy@hanmail.net)
논문번호 : KICS2011-09-393, 접수일자 : 2011년 9월 7일, 최종논문접수일자 : 2011년 11월 4일

워크의 시스템에 부하를 전이시키고, 전력의 소비를 증가시킴으로써 많은 양의 CO_2를 배출하고 있다. 이러한 원인으로는 네트워크의 성능저하요인들이 직접적인 영향을 미치고 있어, 성능 및 구조개선 등의 원인해결을 통한 탄소배출량의 경감이 필요한 실정이다.

따라서 본 논문은 네트워크의 성능저하 요인인 '내부 공격'과 '보안시스템', '네트워크의 구조'로 인한 CO_2배출을 분석함으로써, 향후 네트워크의 효율적인 구축 및 확장뿐만 아니라, IT분야의 저탄소 배출을 위한 자료로 활용될 수 있을 것으로 기대한다. 연구내용에 대한 논리적 근거를 위해 논문의 2장은 그린IT의 동향에 대해 알아보고, 3장은 네트워크의 성능저하 요인을 분석한다. 그리고 4장은 네트워크의 성능저하 요인에 따른 CO_2배출과 5장의 결론 부분으로 이글을 마치도록 한다.

Ⅱ. 그린 IT의 동향

2.1 그린 IT의 동향

세계의 여러 국가와 기업들은 지구의 온난화 문제를 해결하기 위해, 저마다의 다양한 저탄소 솔루션들을 제안 및 실현하고 있다. 최근 가트너[1]사와 세계 자연보호기금(WWF)의 스웨덴 지부는 세계적인 ICT기업 19개를 대상으로 기업들의 저탄소 솔루션들을 평가한 결과를 발표함으로써, 더 많은 기업들의 참여와 인식변환에 큰 기여를 하고 있다[2]. 그리고 이와 같은 그린 IT에 대한 기업들의 자발적인 실천으로 '산업간 파트너 쉽'이 점차 활성화되고 있는 가운데, ICT분야의 저탄소 관련 솔루션 개발이 활발히 진행 중에 있다. 이러한 그린 IT의 동향에 발맞춰 그린화를 실천하고 있는 대표적인 기업들(IBM, Fujitsu, HP, Cisco, BT)중, Fujitsu사가 유일하게 환경운동의 장기적인 전략을 수립한 기업으로 나서고 있다.

또한 일본을 제외한 아시아의 ICT기업들은 아직까지 글로벌 대기업들에 비해 미흡한 부분들이 많지만, 많은 노력들을 기울이고 있다[1,2,4].

그러나 가트너 사의 여론조사 결과에 따르면, 저탄소와 관련한 솔루션들에 대해 공공 및 민간부분의 투자미비로 인해, 핵심 사업에서 제외되고 있는 실정에 처해있음을 기술하고 있어[2], 그린 IT와 관련한 국가와 기업, 사용자 간에 긴밀한 협조가 중요함을 알 수 있다.

1) IT분야의 산업, 분석, 평가, 컨설팅, 교육, 구축 경영관리, 솔루션 정보 등을 서비스를 제공하는 리서치 및 자문 회사

표 1. 2010년 10대 전략기술

	2010년
1	클라우드 컴퓨팅
2	고도화된 분석(Advanced Analytics)
3	클라이언트 컴퓨팅
4	IT를 활용한 친환경활동(IT for Green)
5	데이터센터 개조
6	소셜 컴퓨팅(Social Computing)
7	보안 (액티비티 모니터링)
8	플래시 메모리
9	가용성을 위한 가상화
10	모바일 응용프로그램

한편 가트너사는 최근 3년(2008~2010)간의 10대 전략기술을 표 1과 같이 선정 및 발표하였으며, 이중 '그린 IT'는 2008년 발표부터 연속해서 선정될 만큼 전 세계적인 관심을 불러일으키고 있다. 이밖에 주목할 만한 10대 전략 기술로는 클라우드(cloud) 컴퓨팅, 클라이언트(client) 컴퓨팅, 그린 데이터센터(Reshaping the Data Center), 가상화 등이 있으며, 이들 모두는 그린 IT와 관련한 기술들을 함께 포함하고 있다[4].

그러나 IWR[2]에 따르면 2008년의 CO_2배출량이 1990년보다 오히려 40%나 늘어난 상황이어서, 2012년까지 CO_2배출량을 5.2% 낮추는 것을 목표로 하는 '교토 의정서[3]'가 현실적으로 여러 국가들에 있어, 지켜지지 않고 있음을 시사하고 있다. 따라서 이러한 환경문제들을 효과적으로 해결하기 위한 여러 방안들 중에 하나로 네트워킹을 기반으로 한, 서비스 및 기기를 중심으로 빠르게 발전하고 있는 IT분야의 그린화가 주목을 받게 되었으며, 이에 대한 전력소비의 절감을 통해 CO_2의 배출량을 경감하고자하는 다양한 프로젝트들이 진행 중에 있다[5].

Ⅲ. 네트워크의 성능저하요인

IT분야는 네트워킹 기술을 기반으로 기술과 기기들이 빠르게 진화하고 있으며, 규모의 확장으로 많은 전력소모가 불가피한 실정이다. 따라서 네트워크의 전력누수 부분이라 할 수 있는 네트워크의 성능저하 요인들에 대해 알아본다.

3.1 내부 공격에 따른 성능저하

최근 내부 네트워크에 대한 공격이 증가함에 따라,

2) IWR : Internationales Wirtschaftsforum Regenerative Energien 재생가능에너지 국제경제포럼

3) 지구 온난화의 규제 및 방지를 위한 국제 협약인 기후변화협약의 수정안

성능저하 및 데이터의 손실에 따른 피해가 증가하고 있다. 이와 같은 공격유형으로는 바이러스(virus)나 봇(bot), DNS 스푸핑(spoofing), 스니핑(sniffing)과 다양한 인터넷 서비스를 악용한 전자메일 및 ActiveX, P2P, DoS 등이 있다. 이에 대해 [6]은 다양한 내부 공격들이 점차 지능화되고 있으며, 공격의 빈도가 증가하고 있음을 기술하고 있다. 그리고 [7]의 2008년 사고유형별 현황보고 자료에서는 전체공격의 44%가 내부자에 의해 이뤄지고 있음을 그림 1과 같이 나타내고 있다.

이러한 내부 공격의 증가원인으로는 대응에 필요한 보안시스템의 배치가 비교적 외부 공격에 비중을 두고 있다는 점과 내부 네트워크를 트러스티드 네트워크(trusted network)로 전제하는 데에 따른 취약점들을 원인으로 꼽을 수 있다. 특히 트러스트 네트워크 내에서는 내부 사용자를 보안 정책상 인가된 자로 '자원의 공유' 및 '데이터 송수신'과 '기타 접근' 등에 대해 허용하고 있기 때문에 감지 및 차단이 어려우며, 네트워크의 확장에 따른 관리가 매우 취약하다. 또한 내부 공격은 공격 대상을 특정 시스템으로 제한하고 있지 않아 내부 네트워크의 불필요한 트래픽을 증가시켜 내부 네트워크의 성능을 저하시키고 있다[8].

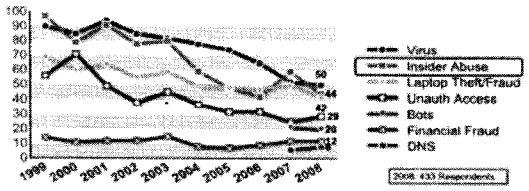


그림 1. 주요 사고유형별 현황

3.2 보안시스템으로 인한 성능저하

앞서 내부 공격으로 인한 성능 및 보안성 저하에 대해서 알아보았다. 이번에는 내부 공격의 예방 및 대응을 위해 사용하고 있는 보안시스템이 전체 네트워크의 성능에 어떠한 영향을 미치는지를 알아본다.

보안시스템은 가장 보편적으로 사용되는 공격 대응 수단으로써, 네트워크와 기타 정보자산을 보호하는 역할을 수행한다. 그러나 보안시스템은 배치위치와 정책, 연결 수 등에 따라 전체 네트워크의 효율성 및 성능의 저하와 경제적인 손실을 야기 시키고 있다. 이에 대해 [3]은 내부 네트워크의 성능저하요인을 알아보기 위해 보안시스템의 사용유무와 정책 수, 연결 수에 대한 성능을 실험하였다.

그림 2는 방화벽의 사용유무에 따른, 응답시간에 대해 방화벽을 사용하지 않을 때보다 약 1.35배의 지연을 나타내고 있으며, 그림3은 VPN의 사용유무에 따른 응답속도에 대해 VPN을 사용하지 않을 때보다 약 3.6배의 지연을 나타내고 있다[3].

또한 그림 4는 방화벽의 보안레벨(가장 낮은 레벨인 1과 가장 높은 레벨인 7)과 연결 수(3~300)의 변화에 따른 지연시간의 측정에서 보안레벨을 높이거나 연결 수를 증가시킴에 따라, 최대 509.66배의 전송지연을 나타냈으며, 그림5는 VPN의 연결된 네트워크(최소3~9)와 연결 장치(20~100개의 장치)의 변화에 대해 그 수를 증가시킬수록 최대 9배의 속도 저하를 나타내고 있다[3].

마지막으로 방화벽과 VPN의 정책 수 변화에 따른 전송속도 및 응답지연 시간의 비교에서도 방화벽은 그림 6과 같이 정책(최소10~30개)과 방화벽 수(2~5대)의 변화에 대해 최대 4배의 속도 지연을 나타냈으

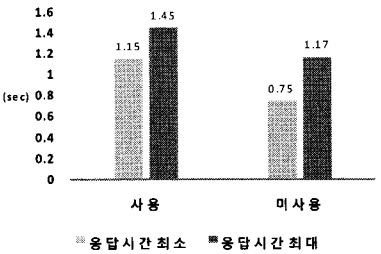


그림 2. 방화벽의 사용유무에 따른 응답시간 비교

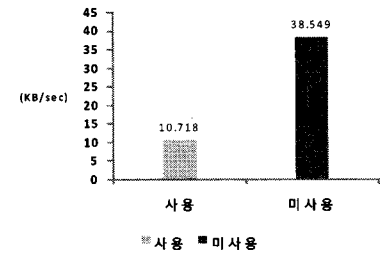


그림 3. VPN의 사용유무에 따른 응답속도 비교

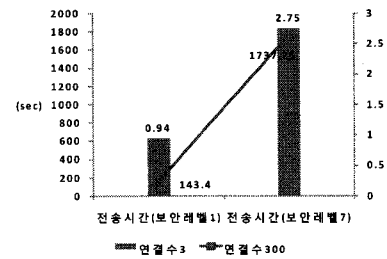


그림 4. 방화벽의 연결 수에 따른 전송시간비교

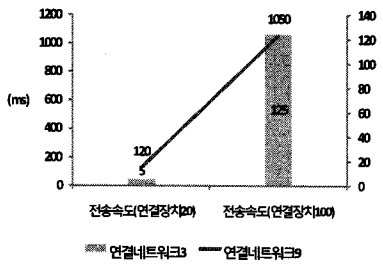


그림 5. VPN의 연결 수에 따른 전송속도 비교

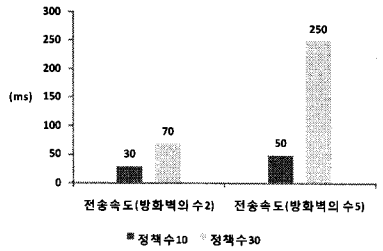


그림 6. 방화벽의 정책 수에 따른 전송속도비교

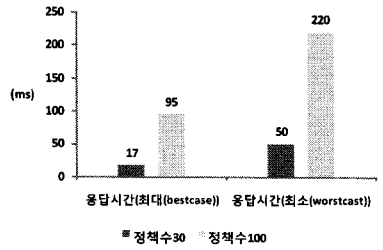


그림 7. VPN의 정책 수에 따른 응답시간 비교

며, VPN은 그림7과 같이 정책 수(최소30~100개)의 Worst와 Best Case에 대한 응답시간에서 약 4.7배의 차이를 나타내고 있다.

이러한 실험결과들을 종합해 볼 때, 방화벽과 VPN은 보안레벨이 높거나, 연결 호스트와 장치의 수, 정책 수가 증가할수록, 내부 네트워크의 성능이 저하됨을 알 수 있다[9].

3.3 네트워크 구조에 따른 성능저하

네트워크는 라우터와 게이트웨이, 스위치 등의 중계 장비들을 이용하여 토폴로지들 간에 다양한 결합들로 확장된다. 그리고 이와 같은 네트워크는 규모와 보안 요구사항에 따라, '전형적 구조'와 '이중화 구조', 'DMZ 구조'로 유형들을 구분해 볼 수 있으며, 각각의 특징들은 다음과 같다[3].

'전형적 구조'는 네트워크의 가장 기본적인 구조 모델로써, 트래픽 량이 비교적 적은 소형 네트워크에 적합하다. 그러나 네트워크의 확장 시, 병목현상으로 외부 네트워크와의 연결을 담당하는 시스템에 부하를 가중시키는 문제를 갖게 된다.

그림 8의 '시스템 A'는 네트워크의 관문(gateway)에 위치함으로써 모든 트래픽들이 집중되며, 하부 네트워크의 성능에 영향을 미치게 된다[3]. 이와 관련해 [9]의 보안시스템에 대한 부하실험에서도 전형적 구조의 병목현상에 대한 문제점들을 동일하게 언급하고 있으며, [10]과 [11]에서는 시스템 부하의 증가가 내부 네트워크의 성능저하 뿐 아니라, 네트워크 전체를 마비시킬 수 있음을 기술하고 있다.

그림 9는 '이중화 구조'를 나타낸 것으로 '전형적 구조'보다도 외부공격에 대한 가용성 기능을 보완하여 중·대형 네트워크에 널리 사용되고 있으며, 이중화를 통해 시스템의 부하를 일부 절감하였다. 이와 관련해 [8]은 특정 보안시스템의 부하가 일부 분산되는 효과를 얻을 수 있지만, 네트워크의 확장 시, '전형적 구조'와 마찬가지로 하부 네트워크의 성능에 영향을 미치고 있음을 기술하고 있다.

결과적으로 이중화 구조 또한 전형적인 구조와 마찬가지로 동일한 문제들을 포함하고 있으며, 적용할

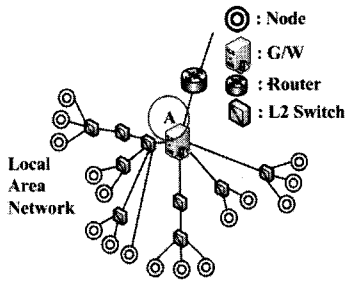


그림 8. 전형적 구조

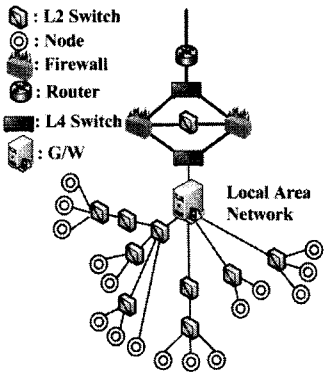


그림 9. 이중화 배치구조

네트워크의 규모에 대한 차이만 있을 뿐, 내부 네트워크의 성능저하가 불가피함을 알 수 있다[10,11].

마지막으로 'DMZ 구조'는 공격대응이 뛰어나고, 네트워크의 확장에 유리하여, 중·대형 네트워크의 모델로 널리 사용되고 있다. 그러나 그림 10과 같이 내·외부 네트워크를 연결하는 시스템에 부하가 집중되고, 하부 네트워크의 성능을 저하시키는 문제가 여전히 남아있다. 이에 대해 [8]과 [9]는 내·외부 네트워크를 연결하는 시스템에 대한 부하가 하부 네트워크에 전이되어 전체 네트워크의 성능에 영향을 미치고 있음을 기술하고 있다.

결과적으로 3가지 유형 모두가 특정 시스템에 대한 트래픽의 집중현상과 보안시스템의 배치위치 및 운용으로 성능저하가 불가피하며, 이는 네트워크의 규모에 따라 비례하는 것을 알 수 있다.

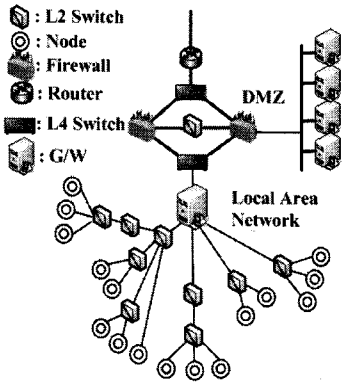


그림 10. DMZ 구조

Ⅳ. 네트워크의 성능저하요인들에 따른 CO_2배출

네트워크의 성능저하는 응답시간을 연장하고, 전기사용량을 가중시켜, CO_2배출량을 증가시킨다. 따라서 저탄소 배출을 위해, 성능저하의 요인들에 대한 CO_2 배출량을 알아본다.

4.1 내부 공격으로 인한 CO_2배출

앞서 3.1절에서 언급되었던 내부 공격의 증가는 네트워크의 성능저하 뿐만 아니라, 전체 소비전력을 함께 증가시키고, CO_2배출의 증가요인으로 작용하게 된다. 이에 대해 [12]는 국내 악성코드에 감염된 PC의 소비전력을 CO_2배출량으로 환산하여 표2와 같이 나타냈다.

표 2는 국내 악성코드 감염에 따른 PC의 연간CO_2량을 알아보기 위해, PC의 악성코드 감염 전과 후에

표 2. 악성코드 감염으로 인한 CO_2배출량 산출[12]

구분	평균소비 140W × 8h × 35만대	악성코드감염 175W × 8h × 35만대
일일전기소모량	392,000KWh	490,000KWh
연간전기소모량	94,080,000KWh	117,600,000KWh
악성코드로인한 연간전기소모 증가량*0.424	23,520,000KWh	
소모규모	국내1KWh 전기생산 424g CO_2발생	

대한 전기 사용량을 비교하였으며, 국내 PC사용에 따른 전기 사용량은 전체 호스트의 수(약 35만대)와 PC의 평균 소비전력(시간당 140W), 평균 사용시간(하루 평균 8시간)을 통해 총 전기 사용량을 계산하였다. 그리고 악성 코드에 감염된 PC에 대한 소비전력은 감염 전, PC의 소비전력인 140W 보다 약 25%가 증가한 정보통신연구진흥원의 실험결과를 근거하여 감염 후의 소비전력인 175W를 기준으로 일일 및 연간 전기 소모량을 계산하고 있다[12,13].

여기서 이와 같이 계산된 감염 PC들의 전기 사용량(23,520,000KWh)은 CO_2환산계수(424g)를 통해, 연간 9,972톤의 CO_2가 배출되는 것을 알 수 있다. 또한 [13]은 DDoS 공격이 가해질 경우, 전력 손실과 이에 따른 CO_2의 배출에 대해 다음과 같이 계산하였다. 일일 전기 사용량(145,152KWh)을 환산계수로 계산하면, 일일 CO_2배출량은 61.5(145,152 KWh × 424g)톤이 되며, 연간 52,980,480KWh의 전기 사용으로 약 22,472(52,980,480KWh × 424g)톤의 CO_2가 배출된다. 다음 그림11, 12, 13에서는 PC의 감염 전과 후,

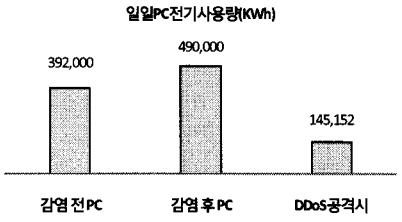


그림 11. 일일 PC전기사용량 비교

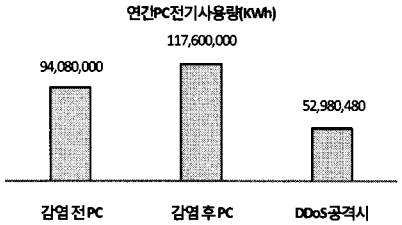


그림 12. 연간 PC전기사용량 비교

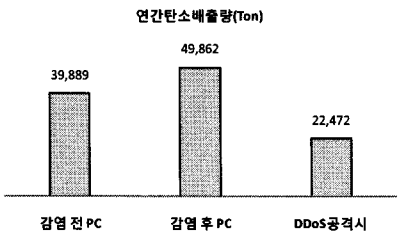


그림 13. 연간 CO_2배출량 비교

DDoS공격 시에 대한 전력 사용량과 CO_2배출량을 비교하고 있다.

결과적으로 공격에 따른 소비전력의 증가는 CO_2의 배출량과 비례하며, 사전 공격에 대한 예방만으로도 많은 양의 CO_2를 경감시킬 수 있음을 알 수 있다.

4.2 보안시스템의 CO_2배출

본 절에서는 보안시스템으로 인한 CO_2배출량을 알아본다. 보안시스템의 CO_2배출량을 산출하기 위해서는 시스템의 일일 전기사용량이 계측되어야 하며, 해마다 계측되는 CO_2환산계수와 사용시간이 요구된다.

보안시스템의 CO_2배출량은 표3을 근거하여 다음과 같이 계산한다. 보안시스템의 사용시간은 PC의 사용과 달리, 1년 내내 운영해야함으로 일일 평균 사용시간을 24시간으로 하고, 보안시스템의 일일 전기 사용량은 표3의 보안장비 성능 및 소모량을 비교한 자료에 근거하여, 2010년 CO_2의 환산계수인 1KWh당 424g을 적용한다. 따라서 보안시스템 1대의 일일 전기 사용량은 6KWh(250W ×24h=6000 Wh)로 연간 사용량(365일)은 2,190KWh가 소모되며, 이를 연간 CO_2배출량으로 환산하면, 928Kg (2,190 ×424g)이 배출된다.

또한 표 3의 통합관리시스템의 CO_2배출량을 산출

표 3. 보안장비 성능 및 전력 소모량 비교

보안기능	개별보안 장비	통합위협관리 제품	비고
Firewall	2Gbps/ 250Wh	1.6Gbps/ 400Wh	
VPN	1Gbps/ 250Wh	700Mbps/ 300Wh	H/W 암호가속기사용
IPS	2Gbps/ 250Wh	1.6Gbps/ 300Wh	
Anti-Virus	800Mbps/ 200Wh	240Mbps/ 300Wh	H/W Anti-Virus사용
Anti-Spam	시간당 150,000건 /200Wh	시간당 50,000건 /300Wh	

해보면, 시간당 전기 사용량이 300Wh로 일일 전기 사용량은 7.2KWh(300w ×24h=7200Wh)가 되며, 연간 사용량은 2,628KWh가 소모된다. 이는 연간 1,114Kg의 CO_2가 배출되는 것을 의미하며, 결과적으로 보안시스템의 CO_2배출량은 시간당 전기 소비량과 보안시스템의 수의 변화에 비례하고 있음을 알 수 있다. 그림 14는 이와 같은 보안시스템과 통합시스템의 일일 및 연간 전기 사용량과 연간 배출되는 탄소량을 비교하고 있다.

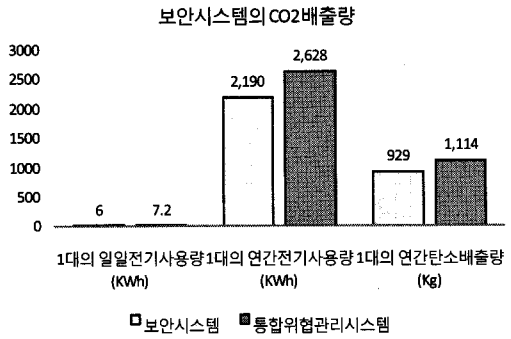


그림 14. 보안시스템의 CO_2배출량 비교

4.3 보안시스템의 성능저하로 인한 내부 네트워크의 CO_2배출

앞서 3.2절에서 보안시스템이 내부 네트워크의 성능을 저하시키고 있음을 살펴보았다. 이번에는 이러한 성능저하로 인해, 발생되는 CO_2의 배출에 대해 알아본다. 보안시스템은 네트워크의 성능을 저하시킴과 동시에 하부에 연결된 호스트의 사용시간을 증가시킨다. 그리고 보안시스템의 하부에 연결된 PC들 또한 일일 평균 사용시간이 증가하게 되어, 전기 사용량과 CO_2 배출량은 증가하게 된다. 이를 알아보기 위해 3.2절의 방화벽과 VPN의 사용유무에 대한 CO_2배출량을 계산해보면 다음과 같다.

PC 1대가 배출하는 CO_2의 배출량은 일일 전기사용시간 8시간과 소비전력 140W, 연간 일수 240일을 기준으로 일일 전기사용량 1.1KWh(140W ×8시간)와 연간 전기사용량 268.8KWh(1.1KWh ×240일)의 결과 값을 얻을 수 있다. 그리고 이를 CO_2환산계수(424g)로 환산해 보면, 연간 113Kg(268.8 KWh × 424g)의 CO_2가 배출되는 것을 알 수 있다.

이러한 결과 값은 3.2절에서 언급되었던 보안시스템의 응답지연으로 인한 산출 값(일일 및 연간 전기사용량과 CO_2배출량)과 비교해 보기 위해 다음과 같이 계산한다. 방화벽은 1.3배의 응답지연으로 일일 평균

사용시간이 10.4시간으로 늘어나며, VPN은 3.6배인 28.8시간이지만 하루 24시간을 기준으로 한다[3]. 그리고 방화벽의 응답지연으로 하부에 연결된 PC 1대가 배출하는 CO_2량을 계산하면, 연간 약 148Kg(140W × 10.6시간 × 240일 × 424g)이 배출된다. 이는 앞서 계산된 113Kg보다 30.9%(35Kg)가 증가한 것이며, VPN은 341.9Kg으로 202.5%(228.9Kg)가 증가하였다. 이에 대한 연간 CO_2배출량을 비교해보면, 다음의 그림 15와 같다.

그림 15를 통해 연간 전기 사용량이 증가할수록 CO_2배출량이 급격히 증가함을 알 수 있다. 따라서 내부 네트워크의 CO_2배출량은 보안시스템으로 인한 성능저하와 연결된 PC 및 보안시스템의 수에 비례함을 알 수 있다.

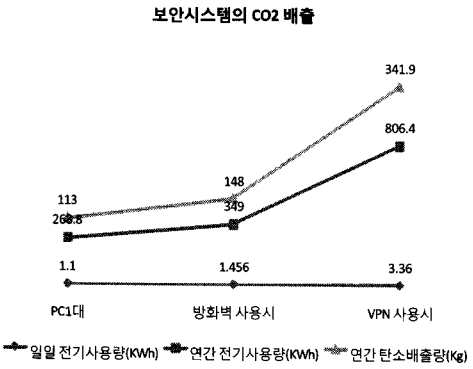


그림 15. 보안시스템에 따른 CO_2배출량 비교

4.4 네트워크 구조에 따른 CO_2배출

보안시스템은 서비스 및 특정 IP에 대한 차단과 탐지를 위해 여러 기능을 필요로 하고 있다. 방화벽은 패킷 필터링과 프록시, NAT, VPN 등의 기능을 포함하고 있으며, VPN시스템은 암호 및 메시지 인증 등의 기능을 수행하고 있다. 그리고 IPS (intrusion protection system)는 차단기능인 방화벽기능과 탐지기능인 IDS(intrusion detection system)기능을 함께 포함하고 있다[3]. 이와 같은 보안시스템의 다기능 구성은 '사용유무'와 '연결 수', '정책 수'에 대한 결과와 같이 다중 기능수행에 따른 정책 및 연결 수의 증가가 예상된다. 또한 다수의 보안시스템 구성은 시스템 부하에 많은 영향을 미칠 뿐만 아니라, 네트워크의 구조적인 병목현상으로 이어져, 전체 네트워크의 성능을 저하시키게 된다[3,8]. 따라서 3.3절에서의 3가지 구조 모델과 같이 특정 위치에 보안시스템의 배치가 집중될 경우, 앞서 4.2절의 보안시스템으로 인한 CO_2배출량이 증가할 뿐만 아니라, 4.3절에서의 전체 네트워크에 대한 CO_2배출량 또한 함께 증가하게 된다. 결과적으로 다기능 또는 다수의 보안시스템 배치와 네트워크의 확장은 CO_2배출량에 매우 큰 영향을 미치고 있음을 알 수 있다.

V. 결 론

오늘날 지구 온난화 문제의 해결을 위해, 전 세계는 다양한 '그린 정책'들을 진행하고 있으며, 여러 국가 및 기업들은 여러 분야에서 CO_2배출량을 경감하기 위한 다양한 정책과 제품들을 내놓고 있다. 그러나 국가와 기업들 간의 협력 부족으로 큰 효과를 거두지는 못하고 있는 것이 현실이다. 특히 IT부분은 계속해서 증가하는 시스템과 네트워크의 확장으로 전기사용량이 지속적으로 증가함에 따라 많은 양의 CO_2가 배출될 것으로 예상되고 있어, 이에 대한 적절한 그린IT정책들이 필요하다.

본 논문은 내부 네트워크의 성능저하의 요인인 '내부 공격'과 '보안시스템', '네트워크의 구조'에 대해 CO_2배출량을 산출 및 비교해 봄으로써, 앞으로의 클라우드 컴퓨팅 환경에서의 네트워크 구축과 CO_2배출을 절감하기 위한 자료로 활용될 수 있을 것으로 기대한다. 그러나 향후 네트워크에 관련한 세부적인 정책과 제도, 규정 등의 마련과 성능저하요인의 구체적인 절감방안 및 네트워크 구조에 따른 CO_2배출량 비교에 대해 지속적이고 추가적인 연구가 이뤄져야 할 것이다.

참 고 문 헌

[1] 문형돈 *"IT기반 녹색성장을 위한 주요국 정책 및 IT산업동향분석"* 정보통신연구진흥원 주간기술동향 통권 1317호 2008. 11.5

[2] 한국정보화진흥원, "Green IT Review", no.37, 2010.12.2.

[3] 전정훈, "내부 네트워크의 성능저하요인에 관한 연구", *한국통신학회논문지* vol.36, no.1, 2011.1

[4] 신중현, "그린 IT 기술동향", *정보과학회지*, vol.27, no.11, pp30-41, 2009.11

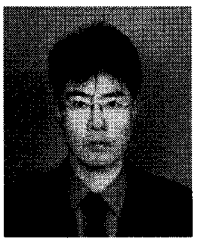
[5] 안중호, 김태하, 박철우, "올바른 국내 그린IT추진방향에 관한 소고", *한국전자거래학회지*, vol.15, no.2, pp.77-91, 2010.10.3.

[6] 한국정보보호진흥원 "2008년 인터넷 및 침해사고 동향 및 분석보고 월보(8월)" 2008.

[7] Robert Richardson, CSI Director "CSI &FBI

CSI Computer Crime & Security Survey" 2008
〔8〕 전정훈 "인바운드 네트워크의 성능 및 보안성 향상에 관한 연구" *한국통신학회논문지* vol.33, 제8호, pp727-734, 2008.
〔9〕 전정훈, 전상훈 "효율적인 네트워크 보안운영을 위한 Exclusive Firewall에 관한 연구", *한국컴퓨터정보학회논문지*, vol.12, 제2호, pp93-102, 2007
〔10〕 H. Garantla, Gemilkonakli "Evaluation of Firewall Effects on Network Performance" 2009.
〔11〕 Jens Mache, Damon Tyman, Andre Pinter, Chris Allick "Performance Implication of Using VPN Technology for Cluster Integration and Grid Computing" IEEE Computer Society. pp75-80. 2006
〔12〕 한국정보화진흥원 "CIO REPORT" Vol.13, pp3-4, 2009.5
〔13〕 한국정보화진흥원"CIO가 꼭 알아야 할 ICT트랜드" pp161-162, 2010.3

전 정 훈 (Jeong-hoon Jeon) 종신회원



1999년 2월 숭실대학교 컴퓨터공학과 졸업
2001년 2월 숭실대학교 컴퓨터공학과 석사
2004년 3월 숭실대학교 컴퓨터공학 박사 과정 수료
2005년 3월~현재 동덕여자대학교 교수

<관심분야>네트워크보안,시스템보안,무선보안,암호,컴퓨터 포렌식