탄소량 감축을 위한 보안 시스템의 기능적 구조 개선에 관한 연구★

전정훈*

요 약

최근 지구 온난화 문제는 전 세계적으로 중요한 이슈가 되고 있으며, 이와 같은 문제해결을 위한 방안으로 그린 IT에 대한 관심이 높아지고 있다. 이러한 가운데 IT분야는 다양한 서비스들과 해킹기술도 함께 진화하고 있어, 다양하고, 더 많은 보안시스템의 사용이 불가피하게 됨에 따라, CO_2배출량의 증가가 예상되고 있다. 따라서 본 논문은 보안시스템의 CO_2배출에 대한 실험 및 사례연구를 통해 요인들을 분석하고, 보안 시스템의 기능적 구조 개선을 통한, CO_2배출량의 경감 여부를 알아봄으로써, 향후, 보안 네트워크의 설계와 성능 향상, IT분야의 탄소배출량 경감을 위한 자료로 활용될 것으로 기대한다.

A study on the functional restructuring of the security system for the reduction of the amount of carbon dioxide

Jeon Jeong Hoon*

ABSTRACT

Recently, the problem of global warming has become a globally important issues. and To solve these problems, has been receiving increasing attention for the Green IT. In these situation, IT techniques are evolving with variety services and hacking techniques. so, it is inevitable to the use of a many and diverse secure system. As a result, Carbon Dioxide emissions are expected to increase. Therefore, in this paper is analyzed the factors of security system's CO_2 emissions through Experiments and A case study. and is proved that is reducing CO_2 emissions by improving the functional restructuring of the security system. In a future, this paper is expected to serve as a valuable Information for security network design and performance improvements and to reduce Carbon Emissions in the Field of IT.

Key words : Security System, Carbon Dioxide Emission, CO_2, Hacking Attacking, Performance

접수일(2013년 6월 2일), 수정일(1차: 2013년 6월 12일), 게재확정일(2013년 6월 13일)

★ 본 논문은 2011년도 동덕여자대학교 학술연구비 지원에 의하여 수행된 것임.

* 동덕여자대학교 컴퓨터학과

1. 서 론

전 세계의 여러 나라들은 지구 온난화에 따른 이상 기온 현상과 같은 대기 불안정의 원인으로 CO_2 배출을 꼽고 있다. 그리고 이에 대해, 몇몇 나라들이 주축이 되어, 전 세계적인 CO_2 배출량의 경감을 위한 다양한 방안들을 모색하고 있다. 특히, IT분야에 대한 그린(green)화 방안으로 다국적 국가들과 기업들은 IT분야의 CO_2배출량의 경감에 많은 노력들을 기울이고 있으며, 이와 함께, 최근 스마트 기기와 신기술(클라우드(cloud) 컴퓨팅, 그리드(grid) 컴퓨팅, 홈(home) 네트워킹 등)들의 등장으로 유비쿼터스(ubiquitous) 시대의 구현을 점차 앞당기고 있다. 이와 같은 신기술들은 기존 네트워크의 패러다임을 변화시키고 있으며, 이러한 변화가 기존의 네트워크 구조 및 설계의 변화뿐만 아니라, 서비스 및 시스템, 각종 하드웨어 및 소프트웨어에 이르기까지 순차적인 변화를 가져옴으로써, 앞으로의 많은 변화가 예상되고 있다.

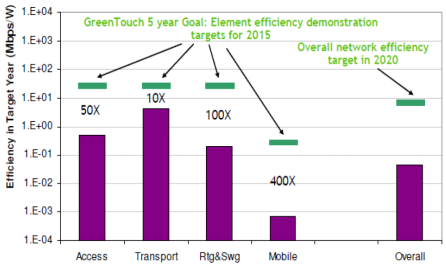
이와 같은 변화는 유독 신기술에만 적용되는 것이 아니라, 항상 공존해왔듯이, 해킹 기술도 함께 변화하고 있음을 염두해 두어야 한다. 해킹 기술의 변화는 기존의 보안 인프라의 변화를 예고하는 것이기도 하며, 새로운 환경에 적합한 보안 기술의 개발이 불가피하다는 것을 의미하기도 한다. 예로써, 클라우드 컴퓨팅 서비스는 가상 서버(virtual server)와 스토리지(storage)를 활용한 유동적 물리매체의 개념으로써, 스마트 폰이라는 통신기기를 이용한 서비스가 대중화 되고 있는 가운데, 클라우드 서비스의 편의성과 신속성, 이동성 등 다양한 장점과는 달리, 취약성으로 인한, 보안 기술들의 적용을 필요로 하고 있다. 그러나 취약성에 따른 보안시스템의 사용을 증가시킬 경우, 네트워크상에 큰 부하로 CO_2배출량의 증가가 불가피한 상황이다. 따라서 본 논문은 보안 시스템으로 발생되는 CO_2배출량의 경감을 위해, 배출 요인을 분석하고, 보안 시스템의 기능적 구조 개선을 통한 경감에 대해 알아봄으로써, 향후, IT분야의 그린화(green)에 기여하며, 보안 체계 및 네트워크의 구축에 필요한 자료로 활용될 수 있을 것으로 기대한다. 연구내용에 대한 논리적 근거를 위해서, 논문의 2장은 그린IT의 동향과 네트워크의 성능저하 요인에 대해 알아보고, 3장은 보안시스템의 성능저하요인을 분석한다. 그리고 4장은 보안시스템의 성능저하요인에 따른 CO_2배출 경감을 성능비교하고, 5장의 결론 부분으로 이글을 마치도록 한다.

2. 관련 연구

2.1 그린 IT

그린IT는 전 세계 여러 국가 및 기업들의 자발적인 참여를 통해, 저탄소 솔루션 및 다양한 제안들을 해왔으며, 여러 글로벌 기업들은 산업간 파트너 쉽을 통해, 인식의 변환뿐만 아니라, 중장기적인 전략들을 수립하는 등의 적극성을 보이고 있다. 대표적인 기업인 가트너사(gartner)는 그린IT의 10대 전략기술들을 발표함으로써, 연구의 방향을 주도하고 있으며, 세계적인 관심을 받고 있다. 특히, ICT분야는 저탄소 관련 솔루션 개발이 활발히 진행되고 있으며, 많은 기업들이 참여하고 있다[1][2][3]. 가트너사의 10대 전략으로는 클라우드(cloud) 컴퓨팅, 클라이언트(client) 컴퓨팅, 그린 데이터센터(Reshaping the Data Center), 가상화(virtualization) 등 그린 IT와 관련한 기술들을 함께 포함하고 있으며[4], 유럽을 중심으로 한, 여러 국가들은 네트워크 에너지의 소비 규제를 강화하는 등 통신사업자 및 산업체들의 에너지 절감형 구조로의 고도화가 예상되고 있다. 이러한 움직임의 일환으로 트래픽에 대한 운용상 피크(Peak)시간과 심야 시간대별 네트워크 에너지의 소비 효율을 개선하기 위한 노력들이 지속적으로 진행되고 있으며, WTO(world trade organization)의 통보문에 따른 규제도 점차 강화되고 있다. 그러나 각 국가들 간의 협조체계도 중요하지만, 국가별 정부 및 기업, 학계 등의 노력과 협력이 절실히 필요한 실정이다. 2010년 네트워크 에너지 소비 절감을 위해 설립된 Green Touch 컨소시엄에서는 그림1에서와 같이, 2020년까지 현재의 네트워크 에너지 효율 대비 1000배 달성을 목표로 Alcatel Lucent 사를 중심으로 진행 중에 있으며, 국내에서는 KAIST, KT, ETRI가 활동하고 있다[4][5]. 이와 같이, 그린IT에 대한 문제는 특정 기업이나, 국가에 한정된 것이 아니라, 전 세계 국가들의 해결해야할 공동의 과제로써, 중요

성이 점차 증가하고 있다.



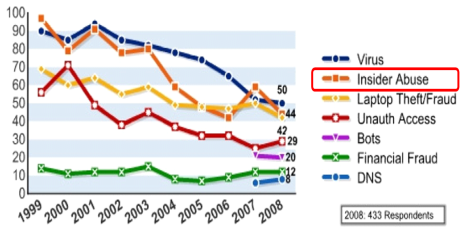
(그림 1) Green Touch에서 2020년까지 에너지 효율 1000배 달성 목표

2.2 그린IT를 위한 네트워크의 성능저하 요인 분석

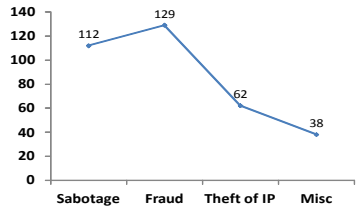
네트워크는 다양한 기능의 시스템과 중계 장비, 전송매체 등 여러 물리적인 요소들의 결합으로 구성되어 있으며, 하드웨어와 소프트웨어의 구성 요소에 따라, 성능에 차이를 갖는다. 그러나 이러한 성능 차이는 일반적인 요인으로 대부분의 네트워크에 존재하고 있어, 성능저하의 주된 요인에 대한 개선이 필요한 실정이다. 이에 대해 [1]은 네트워크의 성능저하요인을 보안 시스템의 자체 부하와 네트워크의 구조적인 문제로 내부 공격(insider attack)의 증가에 따른, 보안 시스템(security system)의 사용 증가를 원인으로 꼽고 있다. 이에 대해 [6]에서는 트러스티드 네트워크의 내부 공격의 빈도와 유형들에 대해 공격유형별로 구분하여, 내부 공격의 심각성을 다루고 있다. 이와 같은 자료들을 분석해 볼 때, 트러스티드 네트워크의 부하요인으로 내부 공격과 보안시스템의 사용은 성능과 반비례함을 알 수 있으며, 앞으로의 신기술 적용에 따른 추가적인 부하증가가 불가피함을 예고하고 있다.

2.2.1 내부 공격 증가에 따른 성능저하

다음의 그림2에서는 1999년부터 2008년까지의 사고 유형들을 비교하고 있다[1]. 사고 유형별 현황을 살펴보면, 바이러스에 의한 사고(50%)가 가장 높았으며, 내부자의 부주의(insider abuse)로 인한 사고가 44%로 다음으로 높았다. 이와 같은 자료는 외부로부터의 공격 대응에 비중을 두었던 기존 상식과는 달리[7], 내부 공격의 비중이 크다는 것을 알 수 있다. 이에 대해, 내부 공격(insider attack)의 범죄유형을 [6]에서 그림3과 같이 범죄 유형들을 분류하고 있다.



(그림 2) 주요 사고유형별 현황[7]



(그림 3) 내부 공격의 범죄 유형

[6]은 고장 및 파괴(sabotage)와 사기(fraud), IP도용, 기타 등으로 유형을 구분하고 있으며, 이중, 사기범죄가 39%로 가장 높았다. IT 관련 고장 및 파괴 범죄는 약 34%로 데이터베이스(이전 고용자, 관리자 또는 DB관리자)에 관련해 발생하였으며, 사기범죄는 재직중인 자에 의해, 데이터베이스 관련 사고가 발생한 것으로 나타났다. 이와 같은 자료를 분석해볼 때, 내부 네트워크의 보안을 위해서는 외부로부터의 대응뿐만 아니라, 내부 공격의 심각성에 따른 보안시스템의 추가 적용이 불가피함을 알 수 있다.

2.2.2 보안시스템의 성능저하

보안 시스템은 네트워크의 내·외부 공격으로부터 정보자산(information asset)을 보호하기 위한 전용 보안 장비로써, 다양한 보안 기능들로 설계되어 있다. 이러한 보안 시스템의 종류에는 침입차단시스템이라고 불리는 방화벽(firewall)과 침입탐지시스템(ids), 침입방지시스템(ips), 가상사설망(vpn), 위협관리시스템(tms) 등이 있으며, 최근 내부 보안(insider security)을 위한 다양한 보안 시스템들이 지속적으로 개발되고 있다. 이와 같은 대부분의 보안 시스템들은 타 중계 장비와는 달리, 데이터에 대한 탐색(detect) 및 차단

(blocking), 암호(encryption & decryption), 인증(authentication) 등의 기능들을 수행하며, 정책(policy)에 따라, 동적으로 운용되고 있다. 그러나 보안 시스템의 대부분은 정책에 따라, 네트워크 내부의 모든 트래픽들에 대해, 차단 및 탐지 등의 기능을 수행하기 때문에 내부 네트워크의 성능을 저하시키는 요인이 되고 있다[1]. 이에 대해, [2]에서는 보안시스템의 사용유무와 정책의 수, 네트워크 연결 수에 따른 부하에 대해 실험하였다. 실험은 방화벽과 VPN의 사용유무에 따른 응답시간을 비교하였으며, 결과로는 사용전과 사용 후의 응답시간 비교에서 방화벽은 사용전보다 1.35배, VPN은 3.6배의 지연을 나타내고 있어, 보안시스템의 사용자체만으로도 네트워크에 부하를 주고 있음을 알 수 있다. 그리고 VPN의 연결 수에 따른, 전송시간을 비교한 실험에서도 방화벽의 보안레벨을 변화하여 연결 수를 증가시켜 보았을 때, 연결된 네트워크(최소3~9)와 연결 장치(20~100개의 장치)의 변화에 대해 그 수를 증가시킬수록, 최대 9배의 속도 저하를 나타냈다. 정책 수에 따른 방화벽의 전송속도와 VPN의 응답속도의 비교에서도 방화벽은 최대 4배의 전송속도 지연을 보였으며, VPN은 Worst Case와 Best Case에 대한 응답시간에서 약 4.7배의 차이를 나타냈다. 이러한 점을 살펴 볼 때, 정책 수에 따라 시스템의 부하가 증가함에 따라, 네트워크의 성능저하요인이 되고 있음을 확인할 수 있으며, 보안시스템의 성능개선을 위해, 정책 수와 연결 수, 보안시스템의 사용수의 최소화와 보안시스템의 대응범위를 축소하는 것이 성능향상에 큰 영향을 미치고 있음을 알 수 있다.

2.3 네트워크의 CO_2 배출 요인 분석

2.3.1 내부 공격으로 인한 CO_2배출

내부 공격은 네트워크의 성능저하로 이어지며, 전체 네트워크의 소비전력을 증가시키는 요인이 되고 있다. 따라서 이와 같은 소비전력을 통해, 대기 중에 배출되는 CO_2의 배출량에 대해 알아본다. 이에 대해 [2]는 국내 악성코드 감염에 따른 PC의 연간 CO_2배출량 산출 자료를 근거로, 내부 공격으로 인한 배출량을 계산하였다. 표1은 PC의 악성코드 감염 전과 후에 대한 전기 사용량을 요약한 것으로, 국내 PC사용에 따른 전기 사용량은 전체 호스트의 수(약 35만대)와 PC의 평균 소비전력(시간당 140W), 평균 사용시간(하루 평균 8시간)으로 계산하였다.

<표 1> 악성코드 감염으로 인한 CO_2배출량 산출

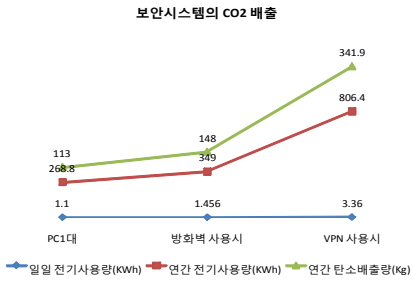
구분	평균소비	악성코드감염
일일전기 소모량	392,000KWh	490,000KWh
연간전기 소모량	94,080,000KWh	117,600,000KWh
악성코드로 인한 연간전기소모 증가량*0.424	23,520,000KWh	
소모규모	국내1KWh 전력생산 424g CO_2발생	

표1의 소비전력량은 CO_2환산계수를 통해, 배출량으로 환산되어지게 되는데, 이에 대한 계산과정을 살펴보면, 다음과 같다. 악성 코드에 감염된 PC에 대해, 평균 소비전력은 175W를 기준으로 일일 및 연간 전력소비량이 산출되며, 계산된 감염 PC들의 전력사용량(23,520,000 KWh)은 CO_2환산계수(424g)를 통해, 연간 9,972톤의 CO_2가 배출되고 있음을 알 수 있다. 또한 DDoS 공격이 가해질 경우, 전력 손실과 이에 따른 CO_2의 배출량으로는 일일 CO_2배출량 61.5(145,152 KWh × 424g)톤으로, 연간 52,980,480KWh의 전기 사용에 따른 약 22,463 (52,980,480KWh × 424g)톤의 CO_2가 배출된다[2]. 결과적으로 내부 네트워크는 내부 공격에 따라, 소비전력량과 이에 따른 CO_2의 배출량을 증가시키는 요인이 되고 있음을 알 수 있다.

2.3.2 보안 시스템으로 인한 CO_2배출량 증가

보안시스템은 사용유무와 정책 수, 연결 수에 따라 성능저하의 정도를 달리하며, 내부 네트워크의 성능을 저하시키고 있음을 앞서 알아보았다. 이에 대해 그림4를 통해, 보안시스템의 사용유무에 따른, CO_2배출량을 알아본다. 그림4를 살펴보면, 보안시스템은 암호기능을 사용할수록 비교적 높은 부하를 나타내며, 보안시스템의 사용 자체만으로도 부하가 증가함을 알 수 있다. 2.2.2절의 응답시간 측정실험 결과를 근거로, 방화벽은 1.35배, VPN은 3.6배의 지연을 나타냄으로써[2], 내부 네트워크는 규모와 보안시스템의 수에 따라, CO_2

배출량이 비례함을 알 수 있다.



(그림 4) 보안 시스템에 따른 CO_2배출량 비교

3. 네트워크의 CO_2배출 경감방안

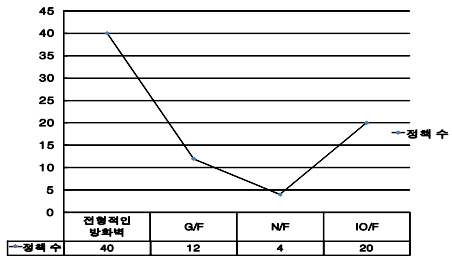
보안시스템은 다양한 기능을 포함함에 따라, 정책 수의 증가가 불가피하며, 정책 수의 증가에 따라, 관리가 어려워지는 문제점을 갖고 있다. 그리고 앞서 보안시스템의 부하 증가는 내부 네트워크의 성능저하 뿐만 아니라, CO_2배출량을 증가시키는 요인으로 작용하고 있음을 알아보았다. 이에 대해 본 장에서는 [3]에서 제안한 보안시스템의 주요 기능별 구조 개선을 통해, 보안시스템과 내부 네트워크의 CO_2배출량에 대해 알아본다.

3.1 보안시스템의 기능적 구조개선

보안시스템은 여러 보안 기능들의 종합체라 할 수 있다. 대표적인 보안시스템으로 방화벽이 있다. 방화벽은 필터링기능 뿐만 아니라, 주소변환(NAT)기능과 프락시(Proxy), 기타 기능들을 포함하고 있으며, 게이트웨이 자리에 위치하여, 많은 트래픽들을 관리한다. 그러나 이러한 기능적, 구조적 조건들은 네트워크의 성능에 큰 영향을 미치고 있다. 이에 대해 [8]에서는 방화벽의 기능에 따라, 내부 네트워크를 보안 등급별로 구분하고, 기능적 구조 개선을 통한 기능성 보안시스템의 운영을 제안하였다. 이러한 제안내용은 방화벽의 성능 개선뿐만 아니라, 앞서 보안시스템의 성능저하의 요인이 되었던, 정책 수와 연결 수를 경감시킴으로써, 보안시스템에서 소요되는 지연시간의 단축에 따른 소비전력의 절감효과를 얻을 수 있었다. 이와 같은 결과를 통해, 보안시스템의 기능적 구조 개선을 통한 기능 경량화는 성능의 향상뿐만 아니라, 소비전력 및 CO_2배출량의 절감효과가 있음을 알 수 있다.

3.2 기능적 구조 개선에 따른 정책 수와 소비전력의 절감

전형적인 방화벽은 모든 트래픽을 감시 및 필터링하기 위해 게이트웨이(gateway)에 배치된다. 그러나 이러한 배치방법은 정책의 수와 이에 따른, 시스템 부하의 증가로 효율적인 운영 및 관리를 저해하는 요인이 된다. 이에 대해 [3]은 방화벽의 기능을 재구성함에 따른 정책 수의 변화를 그림5와 같이 나타내고 있다. 기능성 방화벽의 적용에 따른 정책 수의 변화를 살펴보면, 주요 기능인 패킷필터(packet filter)와 주소변환(nat), 프락시(proxy) 기능을 각각 IO/F와 N/F, G/F의 기능성 방화벽으로 운용할 때, IO/F는 약54%, N/F는 약43%, G/F는 약30% 절감되었으며, 하부 네트워크에 미치는 부하 또한 경감하였다.



(그림 5) 정책 수 비교

따라서 기능적 구조의 개선을 통한 기능성 방화벽의 사용은 정책의 중복과 수를 줄이고, 부하에 따른 소비전력의 절감이 가능하였다. 이러한 결과는 보안시스템에 연결된 PC 수의 증가에 따라, 정책과 연결 수가 증가함으로써, 내부 부하에 영향을 미치게 된다. 그리고 연결 PC 수의 증가는 전체 네트워크의 전력소비량을 증가시키고, 이에 따른 CO_2배출량도 증가하게 된다. 결과적으로 CO_2배출량의 절감을 위해서는 보안시스템에 연결된 PC 수의 경감과 보안시스템의 기능적 구조 개선에 따른 기능 축소 및 네트워크의 규모를 축소시킴으로써, 네트워크 전체 소비전력량과 CO_2배출량의 경감에 큰 영향을 미치고 있음을 알 수 있다[8].

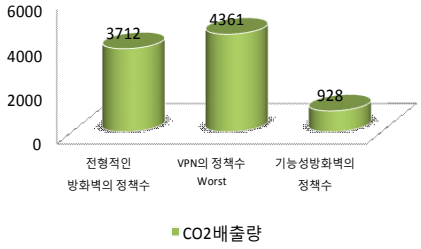
4. 보안시스템의 기능적 구조 개선에 따른 CO2배출량 비교

4.1 정책 수에 따른 CO_2배출량 비교

기능적 구조 개선에 따른 CO_2배출량의 비교를 위해, 전형적인 방화벽과 기능적 구조 개선을 통한 방화벽의 CO_2배출량을 비교한다. 전형적인 방화벽은 CO_2 배출량의 산출을 위해, [2]의 표2를 근거로 소비전력량을 산출한 후, 환산계수를 적용하여 CO_2의 배출량을 계산하고, 기능적 구조 개선에 따른 방화벽의 경우, 2.2.2절의 방화벽과 VPN의 사용유무 및 정책 수, 연결수에 따른 성능측정 자료를 근거로 전력소비량과 CO_2 배출량을 계산한다.

<표 2> 보안시스템 전력 소모량

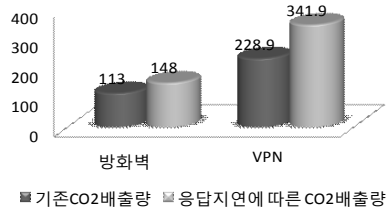
보안기능	개별보안장비	비고
Firewall	2Gbps/250Wh	
VPN	1Gbps/250Wh	H/W암호가속기



(그림 6) CO2배출량 비교

전형적인 방화벽의 CO_2배출량의 계산은 일일 소비전력이 6KWh(250W×24h=6000Wh)로 연간 2,190KWh의 전력이 소비되며, 2010년 1KWh당 424g의 탄산계수를 적용하여, 928Kg이 배출됨을 알 수 있다. 또한 이와 같은 배출량은 그림6과 같이 정책 수에 따라, 방화벽이 최대 4배 정도의 속도 지연으로 928Kg의 4배에 해당하는 3,712Kg가 배출되고, VPN은 약 4.7배의 정책 수가 증가하여, 속도 지연에 따른 약 4,361.6Kg이 배출됨을 알 수 있다.

4.2 응답지연에 따른 CO_2배출량 비교



(그림 7) 기존과 응답지연에 따른 CO_2배출량

보안시스템의 하부에 연결된 PC 1대가 소모하는 전기량은 연간 268.8KWh로 이에 해당하는 CO_2배출량은 약 113Kg이다[2]. 여기에, 보안시스템의 기존 CO_2배출량과 응답지연에 따른 배출량을 비교한 그림7을 근거하여, 방화벽과 VPN의 사용만으로 발생하는 응답지연(방화벽 1.3배, VPN 3.6배)결과를 적용해보면, CO_2배출량은 PC 1대당, 방화벽은 148Kg(140W×10.6시간×240일×424g)으로 기존의 113Kg보다 30.9%가 증가하며, VPN의 경우, 341.9Kg으로 기존 배출량의 202.5%(228.9Kg)가 증가하게 된다[2]. 결과적으로 내부 네트워크의 성능 대비 내부 시스템들의 소비전력은 보안 시스템의 수와 내부 네트워크의 규모에 따라 전력량이 증가하고, 이에 따른 CO_2의 배출량도 함께 증가함을 알 수 있다.

4.3 기능적 구조 개선에 따른 CO_2배출량

내부 네트워크 부하의 주요 요인으로 보안시스템의 사용과 정책 수의 증가를 꼽을 수 있다. 이에 대해 보안시스템의 기능적 구조 개선을 통해, 소규모의 보안시스템을 운영할 경우, CO_2배출량을 알아본다. 보안시스템의 기능적 구조 개선에 따른 CO_2배출량을 알아보기 위해, 그림5의 정책 수를 근거하여, 배출량을 계산한다. 우선 전형적인 방화벽의 경우, 40개의 정책이 필요하였지만, 기능에 따라 방화벽의 기능을 세분화할 경우, 3.2절에서와 같이 패킷필터 약54%와 주소변환 약43%, 프락시 약30%로 감소비율을 기존 방화벽의 배출량에 적용할 경우, 패킷필터는 1,856Kg, 주소변환은 371Kg, 프락시는 111.36Kg으로 절감됨을 알 수 있다. 그리고 PC 1대 당 적용할 경우, CO_2배출량은 140.008~143.56Kg으로 절감됨을 알 수 있다. 이와 같은 CO_2

배출량은 PC의 수가 증가할수록 CO_2배출량도 증가하기 때문에, 전체 네트워크에 대한 CO_2배출량의 경감효과는 매우 크다고 할 수 있다.

<표 3> 보안시스템의 기능적 구조 개선에 따른 CO2배출량

	CO2배출량(대역폭처리효율)		
	패킷필터 54%	주소변환 43%	프락시 30%
기존배출량 3,712Kg	1,856Kg	371Kg	111.36Kg

5. 결 론

최근 그린IT에 대한 관심이 증가하면서, 전 세계의 국가들과 기업들은 다양한 정책들을 진행 또는 계획하고 있으며, 지속적인 연구와 개발이 이어지고 있다. 이러한 동향과 함께 전 세계의 네트워크는 무선 단말기를 포함하여 확대되고 있는 가운데, 해킹공격기술 또한 다양한 진화를 하고 있으며, 공격 횟수도 점차 증가하고 있다. 이와 같은 네트워크의 확대와 해킹공격의 증가는 보다 많은 보안시스템의 배치를 필요로 하고 있어, 이에 따른 네트워크의 부하와 소비전력의 사용량을 증가시키는 요인으로 작용하게 된다. 또한 내부 네트워크의 CO_2배출량을 증가시킴으로써, 네트워크의 성능저하요인에 대한 개선과 CO_2배출량의 경감을 위한 정책 및 방안이 절실히 필요한 실정이다. 따라서 본 논문은 보안시스템의 기능적 구조 개선을 통해, 전형적인 보안시스템의 사용과 기능적 구조 개선에 따른 보안시스템의 CO_2배출량을 비교하여 기능적 구조 개선에 따른 경감효과를 확인하여 보았다. 이와 같은 결과는 향후, 클라우드 컴퓨팅 환경으로의 진화에 따른 네트워크의 구조적 변화에 대처할 수 있는 저탄소 배출을 위한, 보안시스템의 개발과 네트워크 구축 및 CO_2배출을 절감하기 위한 자료로 활용될 수 있을 것으로 기대한다. 그러나 앞으로의 클라우드 네트워크에 관련한 지속적인 연구를 통해, 기능성 보안시스템에 대한 문제점에 대한 추가적인 보완과 IT와 관련한 여러 기술분야에서 CO_2배출량의 절감을 위한 체계적이며, 지속적인 연구가 진행되어야 할 것이다.

참고문헌

[1] 전정훈, “내부 네트워크의 성능저하 요인에 관한 연구,” 한국통신학회, Vol.36, No.11, 2011.1

[2] 전정훈, “내부 네트워크의 성능저하 요인에 따른 이산화탄소배출에 관한 연구,” 한국통신학회, Vol.36, No.11, 2011.11

[3] 전정훈, “인바운드 네트워크의 성능 및 보안성 향상에 관한 연구,” 한국통신학회, Vol.33, No. 8, 2008.7

[4] 최준균 “에너지 소비절감을 위한 Green Touch 활동 소개” 한국정보통신기술협회, No.9, 2013.3

[5] 한국정보화진흥원, “CIO가 꼭 알아야 할 ICT 트랜드,” pp.161-162, 2010.3

[6] Dawun M. Cappelli, “The Key to Successful Monitoring for Detection of Insider Attacks,” RSA Conference2010 Software Engineering Institue CERT Program, 2010.

[7] Robert Richardson, "CSI & FBI CSI Computer Crime & Security Survey," 2008.

[8] 전정훈, “인바운드 네트워크의 성능향상을 위한 보안 클러스터링 기법과 기능성방화벽의 배치,” 한국통신학회, Vol.35, No.7, 2010.7

[저 자 소 개]

전 정 훈 (Jeong-hoon Jeon)

2000년 8월 숭실대학교 일반대학원
컴퓨터학과 공학석사
2008년 2월 숭실대학교 일반대학원
컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교
컴퓨터학과 교수

email : nerdrandy@dongduk.ac.kr