情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

클라우드 서비스 기반의 기업 정보보호 강화 방안

이 향 진*, 손 경 호**, 이 재 일***

요 약

최근 3.20 전산망 장애 등 기업을 대상으로 한 대규모 사이버공격이 빈번히 발생함에 따라, 기업의 정보보호 수준을 강화해야 한다는 요구가 증가하고 있다. 이런 상황에서 보안 기능을 서비스로 제공받는 형태의 클라우드 서비스, SecaaS(Security as a Service)가 기업의 정보보호 수준을 강화하기 위한 비용효과적인 방법의 하나로 대두되고 있다. 본 고에서는 SecaaS에 대해 간단히 설명하고, 이를 구현하기 위한 기능 요구사항과 국내·외 관련 솔루션 및 서비스 개발현황 등을 소개하고자 한다.

Ⅰ. 서 론

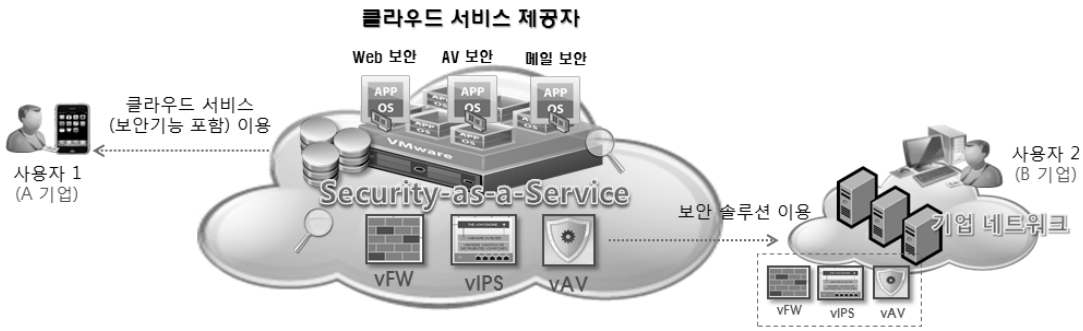
최근 DDoS, APT 등 다양한 형태의 사이버 공격이 끊이질 않는 상황에서 이러한 공격들이 대부분 개인정보 등 중요 정보의 유출로 이어지고 있어 기업들의 큰 피해가 예상된다. 특히, 최근 개인정보보호법 등으로 인해 기업이 적절한 보안조치를 취하고 있지 않은 상황에서 개인정보가 유출되는 경우, 기업 이미지 실추뿐만 아니라 막대한 법적 책임까지 지어야 하는 상황이다. 이에 따라, 많은 기업들이 최근 자사의 보안을 강화하기 위해 고가의 보안솔루션을 도입·운영하고, 보안컨설팅 및 ISMS 보안인증 수검 등의 활동을 하고 있다. 다만, 이러한 활동은 대부분 기업 규모가 큰 업체들을 중심으로 진행되고 있다. 영세한 업체의 경우 고가의 보안솔루션을 도입한다거나, 전사적 차원의 보안컨설팅 등을 받는다는 것은 현실적으로 어려운 것이 사실이다. 이런 상황에서 기업의 정보보호 강화를 위한 효과적인 방법의 하나로 떠오르고 있는 것이 바로 보안을 서비스로 제공하는 클라우드 서비스, SecaaS(Security as a Service)이다[1] [2].

본 고에서는 기업의 정보보호를 강화하기 위한 방안의 하나로 SecaaS가 등장하게된 배경과 SecaaS의 기본 개념을 설명하고, CSA(Cloud Security Alliance)에서 제시하고 있는 SecaaS의 주요 기능 및 구현 요구사항과 국내외 SecaaS 솔루션 및 서비스 개발·제공 현황을 소개한다. 마지막으로 기업이 정보보호 강화를 위한 방안으로 SecaaS를 이용하고자 하는 경우, 고려 해야할 사항들에 대해 소개하고자 한다.

Ⅱ. 클라우드 컴퓨팅 기반의 보안 서비스 (Security as a Service, SecaaS)

최근 IT 분야의 주요 이슈로는 빅데이터, 클라우드, 스마트홈·워크, HTML5 등이 있다[3]. 이 중, 클라우드 컴퓨팅의 경우, 국내 뿐 아니라 국제적으로도 활성화를 위한 다양한 정부 정책들이 시행되고 있고, 이로 인해 시장규모도 매년 크게 성장할 것으로 예상되고 있다. 특히, 그 외 주요 이슈로 거론되고 있는 빅데이터, 스마트홈/워크 등은 일반적으로 클라우드 컴퓨팅 기술을 기반으로 하고 있어 중요도 및 활용분야는 더욱 확대될 것으로 예상된다. 대표적인 클라우드 컴퓨팅 서비스로는 SaaS (Software as a Service), IaaS(Infra structure as a Service), PaaS(Platform as a Service), DaaS (Desktop as a Service) 등이 있으며, 최근 1~2년 사이에는 부각되고 있는 클라우드 서비스의 하나로 보안기능을 서비스로 제공하는 SecaaS(Security as a Service)

* 한국인터넷진흥원 연구개발팀 (jiinii@kisa.or.kr)
** 한국인터넷진흥원 연구개발팀 (khson@kisa.or.kr)
*** 한국인터넷진흥원 인터넷침해대응센터 (jilee@kisa.or.kr)



〔그림 1〕 SecaaS 개념도

가 있다[3].

SecaaS는 클라우드 서비스가 갖는 다양한 보안 위협을 해결하기 위한 대응책의 하나로 제시된 개념으로, 클라우드 컴퓨팅 기술을 기반으로 인터넷을 통해 보안서비스를 제공하는 것이다. SecaaS는 클라우드 서비스 사업자가 자사의 인프라(IaaS), 플랫폼(PaaS) 서비스와 같은 클라우드 서비스를 이용하는 고객에게 정보보호 기능을 부가적으로 제공하는 형태와 SaaS와 같이 클라우드 컴퓨팅 기반의 보안 솔루션을 서비스로 이용할 수 있도록 하는 형태로 나뉠 수 있다. 후자와 같은 보안 기능을 서비스로 제공하는 서비스 모델은 기존에도 있었다. 대표적으로 보안관제 서비스가 있는데, SecaaS의 경우, 제공하는 보안기능이 다양화 되었을 뿐만 아니라, 클라우드 컴퓨팅 기술을 기반으로 보다 비용 효과적으로 제공된다는 차이가 있다. 이처럼 SecaaS를 이용하는 경우, 기업은 초기 보안솔루션 구입・실치 비용이 필요 없고 해당 보안솔루션에 대한 지속적인 유지관리를 직접할 필요가 없다. 특히, 보안 서비스를 이용한 만큼만 비용을 지불하게 되므로 기업의 정보보호 방안 수립・운영을 위한 예산을 급격히 절약할 수 있다. 또한, 클라우드 서비스 사업자가 제공하는 보안기능 중, 자사에 필요한 보안 기능만을 선택적으로 이용할 수 있으며, 필요에 따라 수시로 서비스 변경이 가능해 기업의 비즈니스 환경 변화에 따른 정보보호 정책 변화에 따라 요구되는 보안기능을 동적으로 변경・제공할 수 있다는 장점이 있다.

다만, 아직까지는 클라우드 환경에서 보안기능을 서비스로 제공하기에 몇 가지 한계가 있는 것은 사실이다. 클라우드 컴퓨팅 환경의 경우, 가상화, 자원공유(multi-tenancy), 정보위탁 등의 특징으로 인해 기존 보안솔루션을 바로 적용하기에는 무리가 있다. 예를 들어, 클라우드 컴퓨팅은 기존 컴퓨팅 환경과 달리 단일 물리적 컴퓨터에 다수의 가상 서버를 동작시키기 위한 하이퍼바이져 계층이 존재하는데, 이러한 하이퍼바이져 계층을 인지하지 못하는 기존 보안솔루션은 클라우드 환경에 적용할 수 없게 된다. 또한, 자원공유 및 정보위탁 등으로 인해 고객 기관별, 사용자 역할별 세분화된 접근통제가 요구되는데, 물리적 시스템의 IP/Port별 접근통제 수준의 기존 보안솔루션으로는 이러한 요구사항을 만족시키기 어렵다. 실제, ’12년 일본 클라우드 서비스 업체에서 발생한 고객 데이터 손실 사고의 경우, 사고 발생 이후에 복구 시스템을 통해 고객 데이터가 복구되었음에도 불구하고, 기존에 적용되어 있던 접근제어 정책이 너무 복잡했던 탓에 이를 다시 재적용할 수가 없어 복구된 데이터를 다시 삭제했다[4]. 그 만큼 클라우드 서비스에서 접근제어는 기존 IT시스템에서와 달리 보다 복잡하고 상세하게 적용이 되고 있다. 그 외에도 단일 물리적 서버 위에 존재하는 다수의 가상 서버 간 내부 해킹이나 동적으로 발생하는 자원 변동에 따른 보안관리 등은 기존 보안솔루션만으로는 쉽게 해결하기 어려운 것이 사실이다. 이런 이유로 최근에는 클라우드 환경을 고려한 전용 보안솔루션이 많이 개발되고 있으며, 이를 클라우드 환경에 적용함으로써 SecaaS 서비스를 제공하는 업체가 증가하고 있다. 관련 개발동향은 IV장에서 소개하도록 한다.

Ⅲ. 클라우드 기반의 보안 서비스, SecaaS의 구현 요구사항 및 현황

앞서 설명한 것과 같이, SecaaS는 클라우드 서비스가

갖는 다양한 보안 위협을 해결하기 위한 대응책의 하나로, 본 절에서는 클라우드 서비스의 주요 보안위협을 계층별로 분류하여 소개하고, 이러한 위협들을 최소화하기 위해 SecaaS에 요구되는 기능 요구사항을 소개하고자 한다.

〔표 1〕 클라우드 서비스 보안위협

영역	주요 보안위협
가상화 인프라 보안	• 가상화 시스템 내부 경로를 통한 신규 악성코드 감염·확산 - 호스트OS, 게스트OS 간 악성코드 감염 - 하이퍼바이저 감염 시 게스트OS로 확산 • 가상화 시스템에 특화된 새로운 유형의 해킹 공격 - 하이퍼바이저 루트킷, 가상화 자원고갈 공격 등 • 물리적 시스템 대비 상대적으로 보안관리가 미흡한 가상화 환경 - 기업고객이 임대한 클라우드 인프라의 보안 모니터링 한계
데이터 보안	• 정보를 위탁 관리하는 클라우드 제공자에 의한 정보 유출 가능 - 관리자의 권한 남용으로 이용자 정보 열람/수정/삭제 - 인증하지 않은 이용자의 정보 접근 • 정보유통으로 인한 사용자 데이터 통제의 어려움 - 데이터의 물리적 위치 통제 및 데이터 유통 히스토리 파악 어려움 - 데이터 유통·저장이 모바일 기기, 보안이 취약한 오픈된 무선 네트워크, 내부 클라우드 서버로 다양화
접근제어	• 다중임대, 가상머신 동적재배치로 인증/접근제어 복잡도 상승 - 자원공유의 특성으로 인한 접근제어 설정 복잡성 - 동적인 접근제어 설정 변경으로 인한 복잡성 • 개인용 스마트폰 등 사용자 및 모바일 단말 접근통제 한계 - 모바일 기기를 통한 원격 접속 시, 통제 어려움 - 자동 로그인 접속, 단순 ID/PW 사용으로 단말 분실, ID 유출 시 비인가자에 의한 기업 정보 유출 가능성이 커짐
보안 관리	• 정보위탁의 특징에 의해 보안제어를 위한 위험평가·관리 복잡 - 서비스 장애 원인의 빠른 파악과 복구가 어려움 - 이용자 스스로에 의한 복구 및 패치 어려움 ※ 서비스 제공자의 복구 및 패치 조치가 있어야 함 • 클라우드 서비스 모니터링, SLA 측정, 감사의 복잡성 - 다중임대로 인한 서비스 모니터링, SLA측정, 감사 증적 복잡 - 클라우드 서비스의 SLA 기준 부족 • 응용/웹서비스 보안 취약점 상속 - 기존 네트워크 기반 공격 및 악성코드 등에 대한 취약성
침해사고 대응	• 클라우드 침해사고 시 정보 수집, 교환 및 대응에 대한 규정 부족 - 클라우드 침해사고시 수집 정보 목록 및 대응 절차 불확실 - CERT간 클라우드 침해사고 정보 교환 절차 규정 불확실
법규 및 규제	• 정보 유출 및 손실 시 책임소재 불분명 • 해외 서버 사용시 국내법과 해당국 법과의 상충으로 인한 분쟁 발생 가능성 • 클라우드 점검을 위한 보안 점검 및 규제 항목 부재

3.1 주요 보안위협

클라우드 서비스의 보안위협에 대한 보고서는 NIST, Gartner, CSA 등 국내·외 보안 전문기관, 관련 협회나 학계 등에서 다양한 형태로 발표되고 있다. [표 1]은 이러한 보안위협들을 계층별로 분류해서 소개하고 있다.

3.2 SecaaS 구현 요구 기능

클라우드 컴퓨팅에서의 보안을 촉진하기 위해 설립된 CSA(Cloud Security Alliance)에서 2011년 SecaaS를 위한 구현 지침을 제시하고 있다. [표 1]은 CSA의 가이드에서 소개하고 있는 클라우드 서비스에서의 보안위협과 SecaaS 구현을 위한 기능 요구사항을 소개한다[5]. [표 2]에서 제시하고 있는 10가지 보안위협 분류는 클라우드 보안과 관련하여 보안기업의 리더들과 보안전문가들의 의견에 따라 분류된 것으로 ID 및 접근 관리, 데이터 손실 방지, 웹 보안, 이메일 보안, 보안성 평가,

〔표 2〕 SecaaS 구현을 위한 기능 요구사항

보안이슈	핵심 요구 기능
ID 및 접근 관리	• Provisioning/de-provisioning of accounts • Authentication (multiple forms and factors) • Federated SSO & Web SSO • Authorization, Privileged user management, Role Based Access, etc
데이터 손실 방지	• Data labeling and classification • Identification of Sensitive Data • Traffic Spanning (data-in-motion) detection • Signing of Data, Cryptographic data protection & access control, etc
웹 보안	• Phishing site blocker & Email Security, • Fraud Prevention, Instant Messaging Scanning • SSL, Cryptographic data protection & access control • Web Filtering, Web Access Control, etc
이메일 보안	• Accurate filtering to block spam and phishing • Deep protection against viruses and spyware • Deep content scanning to enforce policies • Integration with various email server solutions, etc
보안성 평가	• Governance & Risk Management • Application Security Assessments • Vulnerability Assessmentsm, Penetration Testing, Security/risk rating. etc
침입대응 관리	• Identification of intrusions & policy violations • Automatic or manual remediation actions • Updates to address new vulnerabilities, exploits and policies, Integrity Monitoring OS • Deep Packet Inspection, System Call Monitoring • Integrity Monitoring VMM/Hypervisor, etc

〔표 2〕 SecaaS 구현을 위한 기능 요구사항〔계속〕

보안 정보 및 이벤트 관리	• Real time log/event collection, normalization, de-duplication, aggregation and visualization • Log normalization, Real-time event correlation • Compliance reporting & support, IR support, Email anomaly detection, etc
암호화	• Data protection & validation, Code Signing • Message authentication & integrity • Data Time-stamping, Identity validation, • Digital Fingerprinting, Forensic protection • Data destruction, Forgery detection, etc
사업 연속성 및 재해복구	• Flexible infrastructure, Secure backup, • Replicated infrastructure components & data • Third party service connectivity, • Data and/or application recovery • Alternate sites of operation, Network survivability • Tested & measured processes and operations • Geographically distributed data centers/ infrastructure, etc
네트워크 보안	• Data Threats, Access Control Threats • Access and Authentication controls • Security Gateways, Security Products • Security Monitoring and IR • DoS protection/mitigation, Traffic/netflow monitoring • Integration with Hypervisor layer, etc

침입대응 관리, 보안 정보 및 이벤트 관리, 암호화, 사업 연속성 및 재해복구 계획, 네트워크 보안이 있다.

3.3 국내·외 SecaaS 구현 및 서비스 현황

클라우드 서비스를 이용하는 고객에게 정보보호 기능을 부가적으로 제공하는 SecaaS의 경우, 아마존, 세일즈포스닷컴, KT 등 국내외 주요 클라우드 서비스 사업자를 중심으로 제공되고 있다. [표 3]는 국내외 주요 클라우드 서비스에서 제공하는 주요 보안기능이다.

〔표 3〕 주요 클라우드 서비스 제공 보안기능

제공 기능	주요 내용
접근제어·인증	• 멀티팩터 인증, 전자서명 등 강력한 접근제어 및 인증 방법 제공
네트워크·시스템 보안	• 망이중화, 고대역폭 용량 확보, 방화벽 트래픽 분리, 미사용 프로토콜 차단 • 별도의 보안구역 설정, 웹방화벽 등을 통한 침입차단 및 탐지 • SSL/TLS를 통한 암호화 연결
침해사고 대응	• 주기적인 보안 취약점 진단 및 최신패치 적용, 보안패치 미적용 사용자에 대한 고지 • 클라우드 인프라 자체에 대한 관제 모니터링

〔표 4〕 국외 SecaaS 제공 보안기능

사업자·서비스	제공 보안 기능
CA Technologies CloudMinder	• Identity and Access Management(is hosted and monitored by CA)
Symantec O3 Cloud IAM)	• Indentity and Access Manamagent, Information Management(as a platform) • Single Sign On
QualysGuard)	• Vulnerability Management • Policy Compliance, Asset Management
Symplified	• Federated Single Sign On • Identity and Access Management

또한, SaaS와 같이 클라우드 컴퓨팅 기반의 보안 솔루션·기능 자체를 서비스로 제공하는 형태의 SecaaS를 제공하는 사업자로는 CA, 시만택, 국내 엘림넷 등이 있다. [표 4]는 국외 주요 SecaaS 사업자별 제공 보안서비스이다.

SecaaS에서 요구하는 기능을 제공하기 위한 보안 솔루션 개발은 트렌드마이크로, IBM, 맥아피, 시스코, 시만택 등 국외 유명 보안업체를 중심으로 진행되고 있다.

〔표 5〕 클라우드 보안솔루션 개발동향 및 주요 제품

영역	주요 기능	개발 동향	주요 제품
인프라 보안	가상화 방화벽 및 IPS/IDS	기존 SW 방화벽과 IPS, IDS를 가상화 환경 내부에서 하이퍼바이저 기반으로 구현	• Deep Security (트렌드마이크로) • vGW Virtual Gateway(주니퍼) 등
	가상화 환경 AV	AV 스톰 방지를 위한 agentless 형태의 가상 어플라이언스로서 안티바이러스 프로그램 구현	• Kaspersky Security for Virtualization (Kaspersky) 등
	가상화 환경 보안관리/관제	가상자원들에 관한 보안정보, 가상화 방화벽·IPS·IDS로 부터의 보안 이벤트의 취합·시각화, 정책기반 접근제어, 로깅, 감사, 컴플라이언스 준수 기능 등 구현	• vSecurity(캣버드) • vTrust for Virtual Management Center(리플렉스 시스템) 등
데이터 보안	데이터 암호화, 토큰화	데이터 위탁으로 인해 발생하는 기밀성·무결성 문제 해결을 위해 데이터의 저장과 네트워크 전송 시 암호화 기능 제공을 구현	• Encryption as a Service for WAN (Certes Networks) • CipherCloud (Cipher Cloud) 등
접근 제어	ID관리, 인증, 접근제어, SSO	다양한 사용자 및 단말과 가상화·다중임대 특성을 고려한 IAM 기능	• Intel Expressway Cloud Access 360(인텔) 등

특히, 최근 가상화 인프라 보안를 위해 하이퍼바이저 기반의 가상화 방화벽 및 IPS/IDS 기술, 가상화 환경에서의 안티바이러스 기술, 가상화 환경 보안관리・관제 기술 관련 제품들이 새롭게 개발보급 되고 있는데, 대부분 기존 보안솔루션을 클라우드 환경에 맞도록 구조 및 기능을 보완하고 있다. [표 5]은 클라우드 환경에서 보호 하고자 하는 대상(인프라, 데이터 등)에 따른 클라우드 전용 보안솔루션들의 개발동향과 주요 국외 제품들을 소개하고 있다[6].

Ⅳ. SecaaS 활용을 위한 고려사항

국외 유명 학회에서 발표된 논문에 따르면, 클라우드 기반의 네트워크 서비스로 Anti-virus 솔루션을 이용하는 경우, 단말에 개별적으로 설치한 솔루션에 비해 악성코드 탐지율이 35% 증가했다고 한다[7]. 이는, 단말에 개별적으로 설치된 Anti-virus 솔루션의 경우, 악성코드 패턴(signature)에 대한 실시간 업데이트나 솔루션 자체의 취약점에 대한 실시간 보완 이 어렵다는 문제점 등이 있는데, 네트워크 서비스로 이용 시에는 이러한 문제가 해결이 가능하기 때문이다. 또한, 악성코드 탐지를 위해 할당되는 리소스 문제도 무시할 수 없는 이유 중의 하나이다.

보안관제, 이메일・HTTP 필터링 서비스 등은 이미 많은 기업에서 서비스의 형태로 이용하고 있는 보안기능이다. 최근에는 ID 및 접근관리, 웹 보안, 이메일 보안, 데이터 암호화 등도 서비스 형태로 개발・제공되고 있다. 특히, 국내의 경우, 개인정보보호법 발효 등으로 인해 웹 보안, 네트워크 보안, 데이터 암호화 등에 대한 법적 요구사항을 만족시킬 수 있도록 기능을 제공해 주는 서비스도 일부 출시된 상태로, 기업이 선택・이용할 수 있는 보안 서비스의 종류가 증가하고 있다.

기업의 정보보호를 위해 SecaaS를 활용하는 것은 가장 비용효과적인 방안이긴 하나, 서비스 선택 시에는 몇 가지 고려되어야할 사항이 있다. 첫 번째로, 해당 기업의 비즈니스 환경이다. 하나의 예로, 기업이 중요한 정보를 다루는 경우, 정보의 관리에 직접 관련되는 데이터 유출방지, 암호화 기능 등은 단독 보안솔루션을 활용하는 것이 좋을 수 있다. 또한, 기업이 다양한 형태의 벤더들과 협업하는 경우에는 ID 및 접근관리, 이메일 보안 기능 등은 SecaaS를 이용하는 경우, 보다 효과적일 수 있다. 두 번째 고려사항으로는 기업에 적용되는 법률・규제이다. 특히, 국내의 경우, 개인정보보호법에 따라 타인의 개인정보를 보유한 경우, 그 규모에 상관없이 개인정보를 암호화해야 한다. 이러한 경우, SecaaS의 암호화 서비스를 이용하는 것이 가장 효과적일 수 있다. 그 외에도 해당 기업의 고객 요구사항이나, 기업의 기술적 수준, 보안인력의 보유여부 등도 고려 대상이 될 수 있다. 기업에서는 이러한 고려사항들을 염두에 두고, 필요한 SecaaS 서비스만을 선택・이용하면 된다.

Ⅴ. 결론

최근 빈번하게 발생하는 사이버공격으로 인해 기업이 입는 경제적, 사회적 피해는 지속적으로 증가하고 있는 실정이다. 특히, 개인정보보호법 시행 등 사회가 기업에 대한 정보보호 수준 강화를 요구하고 있는 상황에서, 기업들에 대한 사이버공격이 개인정보 유출로 이어지는 경우, 그 피해는 막대해 질 수 있다. 이런 이유로 이제 기업의 정보보호는 더 이상 선택이 아닌 필수가 되었다. 그럼에도 불구하고, 여전히 고가의 보안 솔루션 도입은 영세한 기업에게는 쉽게 택할 수 있는 선택이 아닌 상황에서, 최근 새로이 등장한 클라우드 기반의 보안서비스, 즉, SecaaS는 비용 효율적이면서도 보안을 강화할 수 있는 가장 현실적인 대안이 아닐 수 없다.

SecaaS는 다양한 보안기능을 제공할 수 있으므로 기업의 보안 정책 및 비즈니스 환경에 따라 선택적으로 보안기능을 이용할 수 있다. 다만, SecaaS는 아직까지는 기본적인 개념 정립 단계에서 구현 초기 단계에 있으므로 CSA에서 제시하고 있는 [표 1]의 SecaaS가 제공해야 하는 요구 기능을 모두 제공하고 있지는 못하다. 또한, 클라우드 서비스 자체가 갖는 보안위협에 대해서도 무시할 수는 없는 실정이다[8]. 다만, 이러한 보안위협은 현재 클라우드 환경에 특화된 전용 보안솔루션들이 활발히 개발되고 있어 이런 문제는 점차 극복될 수 있을 것으로 예상된다.

클라우드 서비스로의 전환이 거스를 수 없는 대세인 상황에서 보안 기능을 클라우드 서비스로 제공 받는 것 역시, 향후에는 기업의 정보보호를 위한 주요하면서도 가장 효과적인 방안 중 하나로 부각될 것으로 기대된다.

참고문헌

[1] Cloud Security Alliance, *"The SecaaS Implementation Guidance"*, 2011. https://cloudsecurityalliance.org/research/secaas/

[2] 이종훈, 정승욱, 정수환, "Security as a Service 동향", *한국정보보호학회지*, 22권 7호, pp. 54-60, 2012.

[3] Mohammed Hussain, Hanady Abdulsalam, *"SECaaS: security as a serivce for cloud- based application"*, ACM proceeding, 2011.

[4] 정보통신산업진흥원, *"2013년 IT산업 10대 이슈"*, 2012.

[5] http://www.zdnet.com/yahoo-japan-subsidiary-loses-5698-companies-data-2062305251/

[6] CSA Summit Korea, *"국내 클라우드 서비스 활성화를 위한 법률(안) 및 주요 보안정책 현황"*, 2012

[7] Jon Oberheide, Evan Cooke, Farnam Jahanian, *CloudAV: N-Version Antivirus in the Network Cloud"*, 17th USENIX Security Symposium, 2008

[8] 한국인터넷진흥원, "클라우드 서비스 정보보호 안내서", 2011.

〈著者紹介〉

이 향 진 (Lee Hyang Jin)
정회원

2000년 2월 : 성균관대학교 전기전자컴퓨터공학과 학사
2002년 2월 : 성균관대학교 전기전자컴퓨터공학과 석사
2012년 9월~현재 : 성균관대학교 전기전자컴퓨터공학과 박사과정
2002년 1월~현재 : 한국인터넷진흥원 인터넷침해사고대응센터 연구개발팀 책임연구원
<관심분야> 클라우드 보안, 암호, 정보보호 표준화

손 경 호 (Son Kyoung Ho)
특별회원

2001년 2월 : 성균관대학교 전기전자컴퓨터공학과 학사
2004년~현재 : 성균관대학교 컴퓨터공학과 석·박사과정 수료
2001년 1월~현재 : 한국인터넷진흥원 연구개발팀 팀장
<관심분야> 침해사고대응기술, 융합보안, 네트워크보안, 보안 시험·평가, 클라우드·빅데이터 보안

이 재 일 (Lee Jae Il)
정회원

서울대학교 계산통계학과 학사
서울대학교 계산통계학과 석사
연세대학교 컴퓨터과학과 박사
1996년 6월 한국 IBM
1996년 7월~현재 : 한국인터넷진흥원 인터넷침해대응센터본부장
<관심분야> 정보보호