

제조 전문 국제기업 인사관리와 국내 인사관리 클라우드 서비스 운영 개인정보정책과의 연계 및 괴리에 대한 연구

서우석
시큐리티 컨설팅

A Study on the Linkage and Gap in Personal Information Policy in Cloud Services between Multinational Companies' Human Resource Management and Domestic Companies' Human Resource Management

Woo-Seok Seo
Security Consulting

요약 국내 개인정보 보호를 위한 법률은 공공 기관의 개인정보 보호에 관한 법률을 바탕으로 개인정보 보호에 대한 전문 법안으로 제정 및 개정되어 왔다. 그러함에도 불구하고 법률에서 안전성 확보 제한 사항이 명확하지 않고 일부는 폭넓게 제시되어 있어 위협이 지속적으로 발생해 왔다. 이처럼 국제 제조 기업들이 보유한 다양한 내부 및 외부 고객의 개인정보에 대한 기업마다의 고유 식별 Key 값을 연계하는 방식으로 보호 접근 방식을 제안하고 정책적인 측면과 관리적 접근을 동시에 시도함으로써 개인정보 보호를 위한 인력과 비용에 대한 부담을 줄이고자 활용 했던 적용 기술인 인사 관리 국내 ISP 서비스인 클라우드 인사 정보 관리 서비스가 점차 축소되고 시장이 점차 직접 기업이 운영하는 방향으로 변화하고 있다. 따라서 완벽한 안전성 확보를 보장을 위한 연계 관리의 편리성은 보장하되 연계함으로써 발생하는 해외의 국제 제조 기업 인력에 대한 관리 운영 포인트 융통성과 안전성에 대한 괴리를 본 논문을 통해 확인하고 연구를 하고자 한다.

Abstract Laws concerning the protection of personal information have been enacted and revised as the legislation on personal information protection on the basis of the Act on the Protection of Personal Information Maintained by Public Institutions. Nevertheless, there have been continuing threats resulting from the fact that restrictions on security subject to laws remain unclear. By proposing protected access utilizing a unique identification key of enterprises, regarding the personal information of various internal and external clients held by international manufacturing companies and attempting to make policy aspect and management access at the same time, there is a change of gradual decline in cloud personnel information management service, which is the domestic ISP service for personnel management as the technology facilitated to reduce the burden on personnel and cost for the protection of personal information and the market is also changing to the direction for companies to directly operate. Therefore, this study intends to examine the convenience of integrated management for ensuring security, while confirming the gap on flexibility and safety on management point regarding the human resources of international manufacturing companies arising from its interactions.

Keywords : cloud service, estrangement, international company, personal information protection act, personnel management, policy, production

*Corresponding Author : Wool-Seok Seo(Security Consulting)

Tel: +82-70-8202-7055 email: ssws2000@nate.com

Received December 8, 2017

Revised (1st January 3, 2018, 2nd January 4, 2018)

Accepted January 5, 2018

Published January 31, 2018

1. 서론

국내 제조시장에 진입한 다양한 다국적 기업의 현황은 대기업을 비롯하여, 단순 조립에 따른 납품업체까지 운영비용 현황은 정확한 확인이 불가능할 정도로 기업의 수와 기업에 속해 있는 인력의 현황 파악이 불가능 하다. 이와 같은 문제는 국내에 존재하는 개인에 대한 정보에 대한 안전성 확보와 관리 및 운영을 위한 가장 큰 위협 인자로 부각되어지는 문제점이 발생했다. 즉, 제조업에 근무하는 근로자에 대한 개인정보에 대한 현황을 전혀 감지하고 이를 안전성 확보조치 기준에 준하는 안전성 확보 기술을 적용하기란 현실적으로 관리적, 물리적 그 논리적 차원에서 불가능한 부분에 대해 본 논문에서는 해당 문제점에 대한 연계를 통해 객관성을 확보하되 그 안에 존재하는 또 다른 문제점과의 괴리를 파악하는데, 그 목적을 두고 있으며, 본 논문은 1장에서는 연구의 목적과 현황을 2장에서는 침해사례와 전문 해외 제조사의 대규모 근로자 개인정보에 대한 현황파악과 안전성 확보 기술 확인, 3장에서는 국내 ISP가 제안하는 기반기술을 활용함으로써 Global기업이 국내에 구축 못한 전산기반 기술에 대한 활용, 4장에서는 문제점 해소 및 현황 파악, 적용기술에 대한 연구 신화에 대한 논의를 하고 마지막으로 최종 제안하는 연구결과를 제시하고자 한다[1-2].

2. 관련연구

본 관련연구에서 최종 제안하고자 하는 내용으로 개인정보에 대한 침해 및 사고사례를 기반으로 다양한 위협으로부터 발생되어진 문제점에 대한 세부적인 현황과 이슈를 파악하고 명확한 단계적 위협을 제시하고 연구함으로써 향후 방향성을 제시해야 하는 결론에 대한 기초 자료 확보, 시장조사를 진행하고자 한다[3].

2.1 국제 · 국내 개인정보 침해사례

개인정보에 대한 위협으로부터의 침해와 사고사례에 대한 명확한 현황을 확인하는 단계로는 2가지 형태의 범주로 구분이 가능함에 따라 사례로써 국제사회에서의 문제점과 국내사회에서의 이슈로 구분함으로써 최종 개인정보보호를 위한 위협과 문제점 및 사고사례를 확인 가능하다.

다만, 해외의 경우는 개인을 식별하는 다양한 식별자가 있으나 이는 다수가 유동적이고 특정인을 지칭하는 단계가 객관성 보다는 논리적인 연계를 통한 방식으로 병결과 수정 및 보완을 통한 조정으로 특정인에 대한 정보도용이 원시적인 차단이 가능한 사례도 있다. 또한 국내 유출 사례로는 약 1억 3천 건 이상의 사례를 보이고 있다.

하지만 국내사회의 경우는 Table 1과 같이 주민등록번호라는 개인의 출생으로부터 사망 이후까지 관리 되어지는 1인 1식별자가 존재함으로써 수정과 보완 및 변화를 통한 특정인에 대한 지칭을 조정이 불가능한 상태이며, 위반사례가 지속적으로 발생한다. 물론 2017년 5월 30일자 기준으로 Table 2와 같이 일부 특정한 사유로 인한 변경을 요구하는 법적 제도가 일부 반영되고 있으나, 이로 인한 개인정보보호에 대한 최종 위협으로부터의 문제점을 해소하고 사전에 차단하는 부분에 대한 위험성 감소 정책 등은 아주 미미한 상태로 지속적인 법 개정과 지침 및 고시의 빠른 고지가 이루어져야 하는 이슈가 일부 잔존하고 있다[4-6].

Table 1. Personal information infringement cases

No	Division	Violations (example)
1	Agree	Agreeing Not Convergence, Paper Notice and Convergence Not Convergence, Over Information Collection, Comprehensive Consent, Ignore Statutory Representative Consent Agreement
2	Offer	Provided, Purpose, Information, Time of Use, Not Conforming
3	Destruction	Excessive period other than the purpose
4	Process	Possession violation of legal basis
5	Consignment	Information subject notices, consignment management
6	Encryption	Unencrypted processing of legal identification information
7	Management	Lack of control over one person with access rights

2.2 국제 전문기업 인사관리 상의 개인정보 구성분류와 보안기술

국내에 제조시장에 진입한 기업의 형태로 보면, 제조제품의 특성이 공통성보다는 다양성을 가지고 제조업을 운영하는 기업형태를 가지고 있어서 내부 고객정보에 대한 관리와 제품 및 제조기술 등과 같은 모든 원천정보를 관리가 가능하도록 Package가 아닌 개발을 통해 운영한

다. 이는 곧 제조사마다 각각의 개인정보에 대한 보안 및 운영과 활용 Software를 갖는 다는 것을 의미한다[7]. 따라서 국내에서 제공하는 보안성과 안전성을 보장하는 제품과 솔루션으로는 국제 제조사가 가진 원천 정보에 대해 정확하고 안전한 관리와 보존이 힘들다는 것을 의미한다. 이에 ISP 기업들은 원천정보를 생성으로부터 가공, 운영, 파기에 이르는 일련의 과정과 보안성을 보장하는 Cloud 서비스를 제안하기에 이르렀다[8].

Table 2. Applicable criteria for change of resident registration number

No	Object
1	An individual (person) who is recognized as having a risk of being injured or injured by a resident registration number leak
2	Victims of child and youth sexual crimes
3	Victim of sexual violence
4	Victim of prostitution
5	Victim of domestic violence
6	Public interest returner
7	Victims of child abuse Crime victims
8	A specific criminal complainant
9	Victims of certain violent crimes
10	Students who suffered from school violence
11	Victims of arson and defamation
12	Victim of insulting crime

2.3 인사관리 Cloud 서비스 기반 서비스 현황

국내에 존재하는 ISP 및 네트워크 서비스 기반 소프트웨어 개발사들은 Cloud를 이용한 인사관리 서비스를 다양한 다국적 기업과 대규모 인력이 근무하는 제조사를 대상으로 Human Resource를 발굴하고 이중 적재적소 배치 및 교육훈련에 이르기까지 능동적인 AI형태의 살아 있는 서비스를 제공하기 위해 노력하고 있다. 또한 다국적 기업의 특징인 자체 구축 형 전산기반을 위해 해당 Cloud 서비스를 구축형태로 제공하는 것까지 서비스의 한 품목으로 제공하는 등의 다변화된 운영 서비스까지 확대한 상태이다[9-10].

3. 인사관리 Cloud 서비스 운영 개인정보정책과의 연계 및 괴리에 대한 안전성 확보 정책 제안

3.1 인사관리 Cloud 서비스 운영 개인정보정책과의 연계

2017년 현재는 대규모 인력을 운영하는 제조사의 인사관리는 Cloud기반의 원래의 형태를 벗어난 자체 지원 형태로 서비스 임대 형태로 볼 수 있다. 물론 별도의 Cloud 서비스가 제공하는 모든 기능을 동반하여, 구축하고 일정기간 임대하는 방식으로 이용하고 있다.

다만, 서비스 만료 시에는 해당 서비스에 제공된 솔루션은 반환되는 형태가 아닌 영구적으로 삭제되어 서비스 만료 형태를 제공한다. 즉, 기업의 인사관리 성과와 결과를 다국적 기업의 경우 해당 Cloud 서비스가 만료되는 시점에 전부 폐이퍼 형태로 변환 관리하기 때문이다.

3.2 정책과 운영 기반의 괴리

주요 국제적 제조사가 갖는 내부 및 외부 개인정보에 대한 운영과 관리 및 활용에 대한 목적과 기획 기준의 설계에 있어서는 국내 기업과 다소 다른 면들을 보이는데, 그 중 가장 큰 차이는 국제 제조사들은 Marketing 목적을 가장 주요한 관리 주요핵심 역량으로 이해하고 관리하는 반면, 국내는 Marketing을 비롯한 일상 전반에 걸친 전사적인 관리와 운영의 효율성보다는 관리의 안전성을 목적으로 하는 결론의 차이인 괴리감을 갖게 된다. 즉 국내에서 요구하는 관리적인 차원은 국내에서 주요한 개인정보인 법적 개인 식별 정보를 기준으로 모든 안전성 확보 조치를 요구하는 다소 까다로운 관리적, 물리적, 논리적 행정절차와 조사 등이 수반됨에 따라 해외 Global 기업의 국내 진입 후 대규모 투입 인력과 대규모 구매 고객에 대한 정보 관리의 포인트와 관점의 차이가 발생하게 된다. 이는 곧 문화적 차이에서 발생하는 부분 또한 인정하고 이해해야할 과제이기도 하다.

3.3 안전성확보를 위한 제안

국내에서는 개인정보보호를 위한 법제도적인 면에서는 사업의 분류에 따라 개인정보보호법과 방송통신망법과 안전성확보조치 기준 고시 및 지침에 따라 기술적, 관리적 안전성 확보를 위한 정책과 이슈에 대한 변화를 반영한 위협에 대한 문제점 인지를 위한 환경과약을 위한 의식변화 조성은 국내는 다양한 개인정보 들에 그 초점이 맞추어져 있음을 인식, 인지하고 있으나, 해외 대규모 제조사가 갖고 있는 투입인력의 정보 및 제품 구매 고객의 정보 중 상호 주요 개인정보에 대한 차이가 무엇인지를 확인하고 대외적인 국제 기업에 대한 법률의 의 예외 또는 별도의 안전성 확보조치를 위한 지침이 재개발되어

적용하는 부분을 제안하고자 한다. 물론 해외에서 국내로 사업을 위한 진입 시 해당 기업이 속한 각 나라마다 개인정보 또는 개인정보를 포함한 정보보안에 대한 법률과 지침들을 이미 보유한 기업도 있으나 국내 개인정보 보호를 위한 결과를 도출하는 부문에 있어서는 이질적인 성과를 보이고 있어서 위협으로부터 안전성확보를 위한 국내화가 어려운 실정이다. 따라서 국내와 국외의 법률 및 지침 등에 대한 이질성을 최소화함으로써 안전성확보를 증대시키고자 한다.

* **Global 기업 안전성 기준** : 국내 안전성확보조치 기준 + a (a : 대상의 조정 또는 기술의 조정 등을 의미)

4. 안전성 확보 정책 제안에 대한 확인과 구현서비스

4.1 구현 정책 제시

안전성확보조치 기준의 다변화와 각기 다른 환경에서 생성된 기업의 Life-Cycle을 인정하는 차원에서의 변화를 반영한다.

* **고유 식별 Key 구성** : 국내 근로 인력의 투입에 따라 식별 값이 주민등록번호로부터 이름, 전화번호 등의 형태로 존재함에 따라 선정 Key 변환 식별자는 기업마다 임의선정 하여 알고리즘을 구성한다. 예를 들어 전화번호를 선정한 경우 전화번호 a, 기업국가 b, 기업대륙 c, 생산라인 d, 입사순서 e, 라인순번 f, 투입순서 g 등과 같이 제조 기업만의 특성 값을 활용 및 융합함으로써 최종 1인 구성은 (1) $Identity(A)=a*b$, $B=A*(c*d)/f$, $C=B*g$ 로 임의의 정의와 해당 발생 가능 정수 값을 표로 구성 및 값의 범주를 임의 선정하여, 개인보다는 Group을 인지하고 식별자로 구성하도록 연계한다.

* **Global 기업** : 국내 투입 인력에 대한 별도의 기업 내부 자체 인식 Key를 구성함으로써 관리하는 방안으로 이는 곧 해당 국가가 관리하는 식별 기술을 활용하고 퇴사 또는 이직 발생 시에 해당 Key를 삭제 하는 방식으로 국내 안전성확보조치 기준 중 암호화 부분에 중점을 둔 관리를 제안

* **개인정보보호법 개정(예시)** : 별도의 법안을 구성하기 보다는 시행령 또는 시행규칙 아니면, 실무 운영 및 관리 방안으로 제안되는 지침을 “기업 내부 자체 인식 Key” 생성 및 관리, 과거까지의 운영관리 지침을 보완함으로써 효율성과 국제 기업의 국내 정착과 개인정보보호에 대한 법률의 이해를 기술과 관리로 운영할 수 있도록 지원

4.2 정책의 변화와 최적화 기준 제시

주요 핵심 변화를 위한 정책 기반의 변화와 최적화 안전성확보조치 기준의 국제 대규모 제조사가 보유한 투입 인력과 제품 구매 고객에 대한 개인정보 관리 방안 기준은 제시와 같다.

* 해당 기업이 존재하는 국가의 임시 해당기업 근무 또는 구매에 따른 내국인(우리나라) 임시 자체 인식 Key 생성 및 제공(고유 식별 Key)

4.3 제안 구현서비스의 안전성 정책효과 제시

제시되어진 기준에 의해 생성된 정책 하에 Key에 대한 관리는 국내에서 보유한 개인정보보호법 및 동법 시행령과 시행규칙 그리고 안전성확보조치 기준에 따라 관리함으로써 Global 기업과 국내 관리 방안과의 중간에 제3의 식별 Key가 있기 때문이다. 따라서 아래와 같은 지침으로부터 다양한 형태의 정책을 재조정하고 각 기업들이 인용할 수 있게 개정된 재구성 Key를 반영함으로써 최종 구성 단계에서와 같이 최종 운영과 관리에 활용하도록 한다.

* **지침** : 물리적, 관리적, 논리적 기술에 대한 국내 지침을 철저히 기준으로 삼고 준수함으로써 최종 인사관리 서비스를 제공하는 ISP업체의 안전성 확보 기준과 기술의 향상 및 안전도를 신뢰 이상의 수준으로 향상시키기 위한 정책적 지원 또한 진행이 필요

* **재구성 Key** : Global 자체 알고리즘에 따른 구성 Key를 100% 활용, 별도의 재식별 보완 및 수정은 일체 진행하지 않음

* **구성** : Global 기업 보유 개인정보 -> 자체 식별 Key로 재구성(단, 해당 국가가 운영하는 식별 기술 적용, 국내의 경우는 식별 기준 Key 값이 주민등록번호 등과 같은 이미 개인을 식별 가능한 값들을 활용하는 단

제로써 비식별화라는 새로운 기술까지 적용해야 하는 단계임) -> Key생성 -> 국내 보호법 및 안전성확보조치 기준 적용 -> 운영 및 관리, 활용

5. 결론

본 논문에서는 국제 주요 제조기업의 수익과 연관되는 대규모 투입인력의 개인정보를 안전하게 보호하고 효율적인 인사관리를 위한 무형자산 활용과 운영에 대한 위협수준을 낮추는 안전성 향상을 목적으로 하고 있으나, 국내에 존재하는 개인정보보호법에 따른 인사관리의 지침은 안전성을 위한 비용이 100% 준거성을 요구함에 따라 국제 기업들은 국내 우수 ISP 서비스 기업 중에 안전성을 보증하는 Cloud 서비스 기업에 의뢰하는 형태로 전환되고 있다.

다만, 이 또한 완벽한 안전성 확보를 보장하는 부분에 대한 명확한 결과와 운영현황을 제시하는 기준 값에 대한 연계기술은 인정 가능하지만 정책준수에 따른 국제 기업의 인사관리 내 개인정보 안정성과 효율성의 괴리는 아직까지 문제점으로 부각되어지고 있다.

따라서 향후 논문 주제에 대한 연구방향은 인사관리의 효율성과 안전성을 보존하는 기준 가이드라인을 준수 하면서 최적의 안전성을 확보하는 부분에 대한 괴리 값을 줄이는데 더욱 많은 연구가 필요하다.

References

- [1] S. M. Ryu, S. H. Kim, "The Impact of Human and Social Capital of HR Department on HR Outcome and Employee Attitude," *Korea Journal of Business Administration*, vol. 26, no. 7, pp. 1947-1969, 2013.
- [2] Y. J. Noh, "The Firm Performance Effects of Innovative HR Practices in Small Enterprises," *Korea Academy of Organization and Management*, vol. 2017, no. 1, pp. 87-105, 2017.
- [3] J. S. Bae, O. O. Park, "A case analysis on the effects of HRM on innovative performance," *Korea Academy of Organization and Management*, vol. 30, no. 1, pp. 177-209, 2006.
- [4] J. W. Kim, S. S. Kim, S. M. Ryu, "The Impact of HR Involvement on HR Effectiveness," *Korea Academy of Management*, vol. 12, no. 3, pp. 127-161, 2004.
- [5] S. M. Ryu, S. S. Kim, "Environment, HR Involvement, HR System, HR Effectiveness, and Firms' Performance," *Korea Academy of Management*, vol. 15, no. 1, pp. 1-43,

2007.

- [6] J. S. Shin, "A Study of Management Strategies for Overcoming the Personnel and Organizational Difficulties in the Foreign Enterprises Invested in China," *The Korea Society of Decision Sciences*, vol. 19, no. 1, pp. 175-201, 2001.
- [7] S. M. Ryu, J. S. Park, "HR Department's Competencies and HR Effectiveness: The Impacts of Human Capital and Social Capital," *Korea Academy of Organization and Management*, vol. 39, no. 1, pp. 1-36, 2015.
- [8] J. Y. Oh, D. J. Lee, "An Empirical Study on Relationship among Commitment Oriented HRM Characteristics, Organization Communication and Innovation," *Korea Academy of Human Resource Management*, vol. 22, no. 1, pp. 101-120, 2015.
DOI: <http://dx.doi.org/10.14396/jhrmr.2015.22.1.101>
- [9] J. S. Kim, "A Mobile-Sink based Energy-efficient Clustering Scheme in Mobile Wireless Sensor Networks", *Korea Academia-Industrial cooperation Society*, vol. 18, no. 5 pp. 1-9, 2017.
DOI: <http://dx.doi.org/10.5762/KAIS.2017.18.5.1>
- [10] Y. S. Kim, W. C. Lee, "Efficiency analysis of Oriental hospitals according to characteristics", *Korea Academia-Industrial cooperation Society* vol. 18, no. 5 pp. 59-67, 2017.
DOI: <http://dx.doi.org/10.5762/KAIS.2017.18.5.59>

서 우 석(Woo-Seok Seo)

[정회원]



- 2006년 8월 : 숭실대학교 정보과학 대학원 정보통신융합학과 (공학석사)
- 2013년 3월 : 숭실대학교 일반대학원 컴퓨터학과 (공학박사)
- 2006년 4월 ~ 2012년 12월 : 서울 특별시용산구시설관리공단 전산총괄
- 2012년 12월 ~ 2017년 1월 : 주식회사 이지서티 보안사업본부 본부장 (이사), 개인정보보호센터 센터장(이사)
- 2017년 2월 ~ 현재 : 시큐리티 컨설팅(Freelancer)

<관심분야>

4차산업, ICT, IOT, 정보경영, 정보보안, 개인정보, 비식별화, 정보화 전략기획(ISP), 정보화 관리체계, 실태점검, 빅데이터, 인공지능(AI), PIMS, ISMS 인증