# 중소 경호·경비업체의 개인정보 유출 방지를 위한 보안 체계 연구

강푸름* · 이동휘** · 김귀남***


## 요 약

최근 개인정보유출 사건이 빈번히 발생함에 따라 개인정보보호의 문제는 우리 사회의 가장 중요하고 민감한 사회적 의제로 급부상하고 있다. 실제로 개인정보는 그 종류나 유형, 경제적 가치와 민감성, 정보의 질 등에 따라 유출 시 심각한 사회적 위협을 야기할 수 있기 때문에 보다 정확하고 체계적인 개인정보보호 및 관리가 이루어지지 않을 경우 정보화 사회에 큰 혼란을 초래할 수 있다. 특히 업무에 있어 고객의 민감한 개인정보를 필요로 하는 중소 경호·경비업체의 경우, 수집한 정보가 유출 될 시 고객 신변이나 업체의 영업 비밀이 외부에 노출 되 심각한 위협이 있을 수 있어 더욱 큰 문제를 야기한다. 그러나 중소 경호·경비업체는 대기업에 비해 자금의 정도, 인력 부족 등의 문제로 인하여 자체 보안 시스템 구축에 많은 어려움이 있다. 따라서 본 연구에서는 경호·경비업체의 실정을 살펴보고, 그 중 중소 경호·경비업체들이 차지하는 규모와 정보보호의 현황, 특징들을 분석하여 정보보호 시스템 마련의 현실적 문제점 해결 방안으로 중소 경호·경비업체의 개인정보유출 방지를 위한 보안체계를 제안한다.


# Privacy leakage security system research for small physical companies

Poo-Reum Kang* · DongHwi Lee** · Kuinam J. Kim***


## ABSTRACT

Privacy of personal information disclosure incident occurs frequently as a problem to our society's most importan t and sensitive social agenda is emerging. Personal information is actually more accurate, depending on the type or types of economic value and sensitivity, the quality of the information, because it can cause a spill a serious social threat and systematic personal information protection and management are not carried out and the information societ y in a big mess can result. Customers my affairs when small guard security companies, especially the sensitive per sonal information of customers who need to work, the collected information be leaked or the company's trade secret s, are exposed on the outside, it could be a serious threat to a greater problem cause. Small escort guard companie s, however, compared with large companies to build its own security system, due to issues such as the extent of fu nding, staffing shortages, there are many difficulties. Status of Information Security, scale and analyze the character istics of small escort guard companies occupied by guard security companies in the present study, sleep, look at hi m in the solution of the practical issues of information protection system laid small guard. Expenses supplier of pro pose a security system for preventing the leakage of personal information.


**Key words : Private security, Information security, SPCIP, ISMS, ISO27001**

접수일(2012년 10월 10일), 수정일(1차:2012년 10월 15일), 게재확정일(2012년 10월 16일)

★ 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호특화센터 지원으로 수행되었음

* 경기대학교 산업보안학과

** 경기대학교 산업보안학과 (교신저자)

*** 경기대학교 융합보안학과

# 1. 서 론

개인정보보호의 문제는 정보사회의 고도화에 따라 우리 사회의 가장 중요하고 민감한 사회적 의제로 급부상하고 있다. 실제로 개인정보는 그 종류나 유형, 경제적 가치와 민감성, 정보의 질 등에 따라 유출시 심각한 사회적 위협을 야기할 수 있기 때문에 보다 정확하고 체계적인 개인정보보호 및 관리가 이루어지지 않을 경우 정보화 사회에 큰 혼란을 초래할 수 있는 것이다[1].

또한, 법 제정으로 새롭게 개인정보보호의 의무를 이행해야 하는 중소기업의 경우, 개인정보보호에 대한 인식이 매우 저조하고 개인정보보호를 위한 투자 여력도 대단히 부족하다. 즉 대부분의 중소기업이 최고경영자의 인식과 투자 부족, 부서간의 정보제공 및 공유의 미비, 정보보호 시스템 부재 등으로 개인정보보호 체계와 역량이 매우 부족한 것으로 파악되고 있다[2].

특히 업무에 있어 고객의 민감한 개인정보를 필요로 하는 중소 경호·경비 업체의 경우, 수집한 정보가 유출 될 시 고객 신변이나 업체의 영업 비밀이 외부에 노출 되 심각한 위협이 있을 수 있어 더욱 큰 문제를 야기한다. 그러나 중소 경호·경비 업체는 대기업에 비해 자금의 정도, 인력 부족 등의 문제로 인하여 자체 보안  시스템 구축에 많은 어려움이 있다. 따라서 본 연구에서는 국내 경호·경비 업체의 실정을 살펴보고, 그 중 중소 경호·경비 업체들이 차지하는 규모와 정보보호의 현황, 특징들을 분석하여 정보보호 시스템 마련의 현실적 문제점 해결 방안으로 중소 경호·경비업체의 정보보호 운영 프로세스 SPCIP(Small Physical Companies Information Security Process) 제안한다.

# 2. 관련연구

## 2.1. 중소 경호·경비업체의 정보보호 시스템 구축의 문제점

사이버 경찰청에서 자료에 따르면 2011년 12월 기준으로 경비업에 종사하는 경비원의 수는 146,286명으로 집계 되었다[3].

또한 통계청에서 집계한 자료에 의하면 2010년 전체 경호·경비업체 3,600여 곳 중 절반이 넘는 55%가 근로자 수 300명 이하의 중소 경호·경비업체인 것으로 나타났다. 매출액 또한 2010년 기준으로 국내 경호·경비업체의 총 매출액은 3조4천억 원으로 집계되었으며, 이 중 종업원 수가 300명 이하인 중소 경호·경비업체의 총 매출액은 2조 5천억 원, 종업원 수가 300명 이상인 대기업 규모의 경호·경비업체의 매출액은 절반에 가까운 8천 9백억 원으로 집계되었다[4].

통계에서 나타난 바와 같이 국내 경호·경비업체 중 50%가 넘는 중소 경호·경비업체는 대기업에 비해 자금부족과 인력부족 등의 문제로 정보유출 방지를 위해 업체 자체적으로 정보보호 시스템을 구축하는 것에는 무리가 있다.

## 2.2. 중소 경호·경비업체의 고객 정보 보관 환경에 따른 문제점

중소 경호·경비업체는 업무 특성 상 고객(경호대상자 또는 의뢰인)의 민감한 개인 정보를 상세하게 수집한다. 정보 수집은 경호대상자에 대한 이해를 증진시키고 경호업무 수행 중 불필요한 오해나 마찰 가능성을 최소화하고 보다 효과적인 업무 수행을 위해서는 꼭 필요한 단계이다.

그러나 이보다 더 중요한 부분은 수집한 정보가 유출되지 않도록 하는 것이다.

현재 대부분의 중소 경호·경비업체의 경우, 고객과의 상담일지, 계약서, 경호 계획서, 사전 조사일지 등의 고객 관련 서류를 수기로 작성하여 보관함에 보관한다. 일부 업체에서는 전산 보관을 하는 곳도 있으나, 정보 유출 방지 시스템을 마련하여 놓은 곳은 거의 없다.

(그림 1)중소 경호·경비업체의 사무실 내부 사진

(그림 1)은 중소 경호·경비업체의 사무실 내부 사진이다. 대부분의 중소 경호·경비업체는 정보보관실이 따로 마련되어 있지 않은 것이 현실이다.

경호 업무를 위해 수집한 정보는 고객 본인에 관련된 정보뿐만 아니라 가족사항, 지인 등의 정보가 상세하게 기록되어 있어 외부에 유출 될 경우 고객의 신변에 심각한 피해가 예상된다.

현재 등록된 사설 경비업체 숫자는 3,600여 곳으로 경비직원은 2011년 기준으로 15만 명에 달한다[5]. 하지만 경비업체가 늘어나는 데 반해, 경비직원들에 대한 관리가 부실하다는 지적이 많으며, 실제로 경비업체 직원에 의하여 개인정보가 유출 되는 사례도 적지 않다.

### 2.3. 국내·외 정보보호 관리체계

국외 정보보호 관리체계인 ISO27001 인증은 국제표준화기구(ISO)에서 제정한 국제규격으로 BS7799 영국 표준에서 2005년 11월 ISO 국제표준으로 승격되어 PDCA(Plan→ Do→ Check→ Act) 사이클에 따른 ISMS 효과성 측정, 인적보안 강화, 외부업체 보안강화 등을 특징으로 한다[6].
또한, 이 규격은 개별 조직 또는 조직 일부의 요구에 따른 보안통제의 구현을 위한 요구사항을 규정한다[7].

국내의 정보보호 관리체계인 ISMS(Information Security Management System) 인증 제도는 2001년 (구)정보통신부가 「정보통신망이용촉진및정보보호등에 관한법률」을 개정하여 공표함으로써 제47조에 근거를 두고 추진하였다[8].

즉 '정보보호관리체계(ISMS)'란 조직이 보존해야 할 정보자산의 기밀성·무결성·가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하여 지속적으로 관리하고 운영하는 체계를 말한다[9].

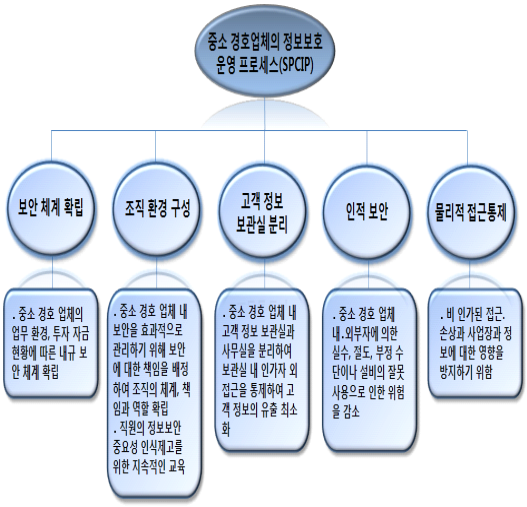
<표 1> ISO27001, ISMS 통제분야

| ISO통제분야 | ISMS통제분야 |
|---|---|
| 보안정책 | 정보보호 정책 수립 |
| | 관리체계 범위 설정 |
| | 위험관리 |
| | 구현 |
| | 사후관리 |
| | 문서요건 |
| | 문서의 통제 |
| | 운영기록의 통제 |
| | 정보보호 대책 |
| 정보보호 조직 | 정보보호 조직 |
| 자산 관리 | 정보자산 분류 |
| 인적자원 보호 | 외부자 보안 |
| | 정보보호 교육 및 훈련 |
| | 인적 보안 |
| 물리적 및 환경적 보호 | 물리적 보안 |
| 통신 및 운영관리 | 시스템개발 보안 |
| | 암호 통제 |
| | 운영 관리 |
| 접근통제 | 접근 통제 |
| 정보보호 사고관리 | 보안사고 관리 |
| 업무 연속성 관리 | 업무 연속성 관리 |

## 3. 중소 경호·경비업체의 정보보호 운영 프로세스(SPCIP) 연구

2장에서 조사한 결과, 경호·경비업체의 업무 특성상 상세하고 민감한 고객 정보를 다루고 있는 만큼 정보보호 대책마련이 시급한 상황이다. 그러나 국내 중소 경호·경비업체는 대기업에 비하여 자금 확보의 어려움과 인력부족으로 인하여 자체적인 정보보호 시스템을 구축하는 것에는 큰 무리가 있는 것으로 나타났다. 또한 획일화 되어 있는 ISO27001과 ISMS를 중소 경호·경비업체의 실정에 맞추어 적용하기에도 한계가 있었다.

그리하여 국내 중소 경호·경비업체의 정보유출을 방지하기 위한 해결 방안으로 ISO27001과 ISMS의 세부 통제항목을 분석하여 필요한 항목을 도출하고 세분화 시켜 중소 경호·경비업체의 실정에 맞춘 정보보호 운영 프로세스 SPCIP(Small Physical Companies Information Security Process)를 아래 (그림 2)와 같이 제안한다.




(그림 2) 중소 경호·경비업체의 정보보호 운영 프로세스(SPCIP)

### 3.1. 보안 체계 확립

중소 경호·경비업체의 업무 환경, 투자 자금 현황 등 각 업체의 특성에 맞게 내규 보안 체계를 확립한다.

<표 2> 보안 체계 확립 점검항목 및 평가

| | |
|---|---|
| **보안전략** | (1) 보안의 정의, 포괄적 목적과 범위 설정<br>(2) 범위설정<br>a. 업무환경, IT환경, 물리적 환경 등에 대한 범위 선정<br>b. 업체에 관련된 모든 환경, 내부 직원, 외부 방문자 등을 포함하여 범위 설정<br>(3) 보안계획 구현을 위한 지침, 표준 절차 설정<br>a. 모범적 실무사례나 접근방법을 제시하는 지침이나 구체적 기술, 방법론, 구현절차 등을 정의 |
| **항목 평가** | (1) 보안의 정의, 포괄적인 목적과 범위, 정보 공유를 가능하게 해주는 기법으로서의 보안의 중요성 등의 내용이 포함되어 있는 항목이 명시되어 있는가? (1점)<br>(2) 정책을 구현하기 위해 필요한 지침, 표준, 절차 등의 항목이 명시되어 있는가?[10] [ISMS 정보보호정책 1.2.2 점검항목 인용] (1점)<br>(3) 정보보호정책의 내용이 사업목표 및 정보기술정책과 같은 상위 정책이나 전략문서와의 일관성 검토 항목이 명시되어 있는가?[10] [ISMS 정보보호정책 1.212 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 보안 체계 확립 기준이 명시되어 있는가? (2점) |
| **취약점 분석** | (1) 위험 분석<br>a. 범위에 포함되는 자산의 식별 및 중요도 평가<br>b. 자산에 영향을 미치는 위협의 식별 및 위협도 평가<br>c. 자산의 관리적, 물리적, 기술적 취약점 식별 및 취약도 평가<br>d. 자산, 위협, 취약성으로 연계되는 위험분석 |
| **항목 평가** | (1) 위험분석 관련 항목이 명시되어 있는가? (1점)<br>(2) 자산에 영향을 미치는 위협의 식별 및 위협도 평가 관련 항목이 명시되어 있는가? (1점)<br>(3) 자산의 관리적, 물리적, 기술적 취약점 식별 및 취약도 평가 관련 항목이 명시되어 있는가? (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 취약점 분석 항목이 명시되어 있는가? (2점) |
| **보안계획 수립** | (1) 마스터플랜·상세보안계획 수립<br>a. 업체 내 행정 현실에 맞게 마스터플랜과 상세 보안 계획을 목표 및 정책, 법적 요구사항 등을 고려하여 조직, 역할, 책임, 주요과정을 포함한 정보보호 활동에 대한 방향을 설정하여 구성원의 정보보호에 대한 책임과 역할이 명확히 규명될 수 있도록 작성 |
| **항목 평가** | (1) 보안 계획을 수립하기 위해 적합한 관련 항목이 명시되어 있는가? (1점)<br>(2) 마스터플랜 수립 관련 항목이 명시되어 있는가? (1점)<br>(3) 상세보안계획 수립 관련 항목이 명시되어 있는가? (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 보안 계획 수립 항목이 명시되어 있는가? (2점) |
| **보안계획 구현** | (1) 정보보호 정책 및 지침 수립<br>(2)보안 프로세스 구축<br>(3)보안 프로세스 운영 |
| **항목** | (1) 보안 계획을 수립 후 구현을 위해 적합한 |

| | |
|---|---|
| **평가** | 관련 항목이 명시되어 있는가? (1점)<br>(2) 보안 계획 구현 이행을 위해 필요한 세부 계획과 절차 등의 문서처리의 의무화 관련 항목이 명시되어 있는가? (1점)<br>(3) 보안 프로세스 구축에 관한 항목이 명시되어 있는가? (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 보안 계획 구현 항목이 명시되어 있는가? (2점) |

## 3.2. 조직 환경 구성

중소 경호·경비업체 내 보안을 효과적으로 관리하기 위해 직원들에게 보안에 대한 책임을 배정하여 조직의 체계, 책임과 역할을 확립한다.

<표 3> 조직 환경 구성 점검항목 및 평가

| | |
|---|---|
| **정보보호 책임자 지정** | (1) 정보보호조직 체계를 통해 정보보호관리 활동을 계획, 관리<br>a. 중소 경호·경비업체의 인원규모를 고려하여 정보보호 전담팀을 책임자, 관리자, 담당자 3명으로 구성하여 최소의 인원으로 정보보호 정책과 세부 지침이 업무와 연계되어 실용적으로 활용할 수 있도록 구성<br>(2) 정보보호관리자에 대한 역할 및 책임 규명<br>a. 정보보호 정책 수립<br>b. 위험분석 및 관리<br>c. 보안사고 대응 및 복구 등 총괄 업무 |
| **항목 평가** | (1) 정보보호 활동을 계획, 관리하는 정보보호 관리자 지정 항목이 명시되어 있는가?[11] [ISMS 정보보호조직 2.1.1 점검항목 인용] (1점)<br>(2) 정보보호관리자에 대한 다음과 같은 역할 및 책임이 규명되어 있는가?[11] [ISMS 정보보호조직 2.2.1 점검항목 인용] (1점)<br>a. 정보보호 정책 수립<br>b. 위험분석 및 관리<br>c. 보안사고 대응 및 복구 등에 대한 총괄 업무<br>(3) 정보보호정책 수립, 위험분석·평가, 통제사항의 선택과 구현, 보안사고 대응 등 중요한 정보보호관리 활동에 도움을 얻기 위해 외부 전문가의 조언을 받는 항목이 명시되어 있는가?[11] [ISMS 정보보호조직 2.1.2 점검항목 인용](1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 정보보호전문가 지정 기준 항목이 명시되어 있는가? (2점) |
| **정보보호 위원회 구성** | (1) 정보보호조직 체계를 통해 각각의 책임과 역할을 지정<br>a. 최소 인원으로 구성된 책임자, 관리자, 담당자가 정보보호 위원회의 구성원이 되며 개인정보 및 산출물에 대한 관리 및 이를 담고 있는 매체의 관리, 이동 등 정보보호에 관련 된 정책 수립 및 운영 등을 관리<br>(2) 중요한 정보보호 관련 심의 및 승인 |
| **항목 평가** | (1) 정보보호 위원회의 구성 및 운영이 명시되어 있는가? (1점)<br>(2) 정보보호위원회의 역할 및 책임이 규명되어 있는가?[11] [ISMS 정보보호조직 2.2.2 점검항목 인용] (1점)<br>(3) 조직간의 정보보호를 위한 활동의 협조에 관한 항목이 명시되어 있는가?[12] [BS7799 보안조직 2.1 조직간의 협조 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 정보보호 위원회 구성 기준 항목이 명시되어 있는가? (2점) |

## 3.3. 인적 보안

중소 경호·경비업체 내·외부자에 의한 실수, 절도, 부정 수단이나 설비의 잘못 사용으로 인한 위험을 감소할 수 있도록 하고, 직원들의 정보보안 중요성 인식제고를 위한 지속적인 교육을 실시한다.

<표 4> 인적보안 점검항목 및 평가

| | |
|---|---|
| **정보보호 교육 및 훈련** | (1) 전직원 보안교육<br>(2) 보안 책임자 특성화 교육 |
| **항목 평가** | (1) 정보보호 교육 및 훈련에 관한 항목이 명시되어 있는가? (1점)<br>(2) 정보보호 교육 및 훈련의 대상에 관한 항목이 명시되어 있는가?[13] [ISMS 정보보호교육 및 훈련 5.1.2 점검항목 인용] (1점)<br>(3) 정보보호 교육 및 훈련 대상자의 직위 및 담당하는 업무의 특성에 따라 적절히 분리되어 필요한 별도의 교육을 받을 수 있도록 하는 항목이 명시되어 있는가?[13] [ISMS 정보보호교육 및 훈련 5.1.3 점검항목 인용] (1점) |

| | |
|---|---|
| | (4) 중소 경호·경비업체의 실정에 맞는 정보보호 교육 및 훈련 기준 항목이 명시되어 있는가? (2점) |
| **보안서약서 관리** | (1) 직원 입·퇴사 시 보안서약서 작성<br>(2) 외부 출입자에 대한 보안서약서 징구<br>(3) 보안서약서 작성 내용 위반 시 법적 처벌 |
| **항목 평가** | (1) 인사규정 또는 인사보안정책에 직원이 보안책임을 이행하지 않는 경우의 처벌규정이 포함되는가?[14] [ISMS 인적보안 6.1.2 점검항목 인용] (1점)<br>(2) 보안서약서를 작성하는 대상자의 범위가 명시되어 있는 항목이 있는가? (1점)<br>(3) 임시직원이나 제 3자에게 접근권한을 부여할 경우 비밀유지에 관련된 사항이 포함된 보안서약서를 작성하도록 하는 항목이 명시되어 있는가?[14] [ISMS 인적보안 6.3.1 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 보안 서약서 관련 항목이 명시되어 있는가? (2점) |
| **내·외부자 논리·물리적 접근** | (1) 민감 직무를 분류하여 등급별 접근 인가<br>(2) 접근 인가자의 정기적인 타당성 적격심사<br>(3) 정보에 대한 보안 규정에 따라 통제(정보의 보관과 접근통제 등)<br>(4) 정보에 대한 물리적 접근 통제 |
| **항목 평가** | (1) 인력에 대한 보안정책이 다음과 같은 사항을 포함되어 있는가? - 적격심사, 민감 직무 분류, 내·외부자 보안[15] [ISMS 인적보안 6.1.2 점검항목 인용] (1점)<br>(2) 정보자산에 대한 제3자의 접근을 통제하는 항목이 명시되어 있는가?[15] [ISMS 외부자보안 3.1.2 점검항목 인용] (1점)<br>(3) 주요/민감한 직무에 대한 정의 관련 항목이 명시되어 있는가?[14] [ISMS 인적보안 6.2.2 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 인적보안 관련 항목이 명시되어 있는가? (2점) |

## 3.4. 물리적 접근통제

물리적 접근 통제를 통해 비 인가된 접근을 통해 사업장의 손상과 고객정보에 대한 유출을 방지한다.

<표 5> 물리적 접근통제 점검항목 및 평가

| | |
|---|---|
| **보호(통제) 구역 지정** | (1) 보호(통제)구역 지정<br>a. 특별한 보호가 필요한 시설 및 장비를 보호하기 위한 보호구역 정의<br>(2) 보호(통제)구역 보안대책 수립<br>(3) 각 구역별 보안 등급을 지정하여 접근 인가자 분류<br>(4) 보호(통제)구역 출입대장 작성 |
| **항목 평가** | (1) 특별한 보호가 필요한 시설 및 장비를 보호하기 위한 보호구역을 정의하고 있는 항목이 명시되어 있는가? (1점)<br>(2) 보호구역 정의에 따른 보안대책을 수립하여 이행할 수 있도록 기준 하는 항목이 명시되어 있는가?[16] [ISMS 물리적 보안-1보안대책 7.1.1 점검항목 인용] (1점)<br>(3) 물리적 보호 구역이 필요한 보안 등급에 따라 정의되고 각각에 대한 보안 조치와 절차가 수립되는 기준 항목이 명시되어 있는가?[16] [ISMS 물리적 보안-1보안대책 7.1.1 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 보호(통제)구역 지정 기준이 명확히 설명되어 있는가? (2점) |
| **보안점검** | (1) 보안 관리 일지 작성<br>a. 업체에 관련된 모든 환경, 내부 직원, 외부 방문자 등을 포함하여 범위 설정<br>b. 각 보호 구역 내의 중요한 장비, 문서, 매체 등을 반출입 할 시 절차 마련<br>c. 보안 관리일지의 정기적인 점검 |
| **항목 평가** | (1) 보안 관리 일지 작성 기준 항목이 명시되어 있는가? (1점)<br>(2) 각 보호 구역 내의 중요한 장비, 문서, 매체를 반출입 할 시 절차에 관한 항목이 명시되어 있는가?[16] [ISMS 물리적 보안-1보안대책 7.1.1 점검항목 인용] (1점)<br>(3) 보안 관리일지의 정기적인 점검을 의무화 하는 항목이 명시되어 있는가?[16] [ISMS 물리적 보안-1보안대책 7.1.2 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 보 |

| | |
|---|---|
| | 안 관리 일지 작성 기준이 명확히 설명되어 있는가? (2점) |
| **접근 인가자 관리** | (1) 인가된 자만 접근 할 수 있도록 접근 통제<br>(2) 모든 출입자의 기록 관리 |
| **항목 평가** | (1) 출입 정책과 절차에 관한 항목이 명시되어 있는가? (1점)<br>(2) 출입증이나 허가의 타당성이 정기적으로 검토될 수 있도록 하는 기준 항목이 명시되어 있는가?[16] [ISMS 물리적 보안-2 데이터센터보안 7.2.2 점검항목 인용] (1점)<br>(3) 보호 구역에 출입자가 식별되고, 기록 관리될 수 있도록 관련 항목이 명시되어 있는가?[16] [ISMS 물리적 보안-2데이터센터 보안 7.2.2 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 접근 인가자 관리 기준이 명확히 설명되어 있는가? (2점) |
| **시설 경비** | (1) CCTV의 설치 기준 마련<br>a. 설치 구역의 타당성 검토<br>b. 촬영 범위 설정<br>(2) 출입카드 등 출입 허가<br>a. 구역별 출입 허가 등급 분류<br>b. 정기적 출입 정보 업데이트<br>(3) 시설에 관한 정기적 점검 |
| **항목 평가** | (1) 보호 구역에 CCTV, 출입통제시스템 등 시설경비에 관한 항목이 명시되어 있는가? (1점)<br>(2) 시설경비에 관한 정기적 점검에 관한 항목이 명시되어 있는가? (1점)<br>(3) 시설경비 설치 기준에 관한 항목이 명시되어 있는가? (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 시설경비 기준이 명확히 설명되어 있는가? (2점) |

## 3.5. 정보 자산 분류/보관실 분리

정보 자산 대장을 작성한 후 정보 보관실과 업무실을 분리하고 보관실 내 인가자 외 접근을 통제하여 정보유출을 최소화 할 수 있도록 한다.

<표 6> 정보 자산 분리 점검항목 및 평가

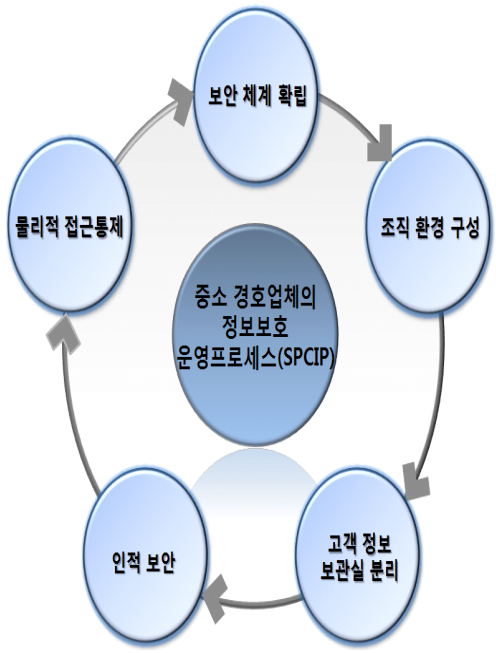
| | |
|---|---|
| **정보 자산 대장 관리** | (1) 중요도에 따른 정보 자산 분류<br>(2) 정보자산의 정기적 업데이트<br>(3) 정보자산 별 표식<br>(4) 자산에 대한 책임 분류<br>a. 자산의 중요도 등급에 따라 책임자의 지정 |
| **항목 평가** | (1) 식별된 정보자산에 대해 법적 준수사항이나 업무에 미치는 영향 등을 고려하여 식별된 정보자산의 중요도 결정 관련 항목이 명시되어 있는가?[17] [ISMS 정보자산분류 4.1.1 점검항목 인용] (1점)<br>(2) 정보자산의 정기적 업데이트에 관한 항목이 명시되어 있는가?<br>(3) 자산에 대한 책임 분류 관련 항목이 명시되어 있는가?[17] [ISMS 정보자산분류 4.1.2 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 정보 자산 대장 관리 항목이 명시되어 있는가? (2점) |
| **정보 데이터의 분리** | (1) 내부 정보<br>a. 임직원 정보(비밀유지서약서 등)<br>b. 고객정보(주민등록번호, 주소, 이름 등)<br>c. 영업정보(제안서, 계약서 등)<br>d. 기술정보(방법론, 세부절차 등)<br>(2) 외부 정보<br>a. 고객정보(고객 동의를 얻은 외부 공개용 정보)<br>b. 협력업체 정보(협력업체의 동의를 얻은 외부 공개용 정보) |
| **항목 평가** | (1) 하드웨어, 소프트웨어, 통신/네트워크, 데이터, 직원, 물리적 시설 등 주요 정보자산 조사 관련 항목이 명시되어 있는가?[17] [ISMS 정보자산분류 4.1.1 점검항목 인용] (1점)<br>(2) 내부 정보(임직원, 고객정보, 영업정보, 기술정보) 분리 관련 항목이 명시되어 있는가? (1점)<br>(3) 외부 정보(고객정보, 협력업체 정보) 분리 관련 항목이 명시되어 있는가? (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 정보 데이터 분리 항목이 명시되어 있는가? (2점) |

| | |
|---|---|
| **정보보관실 분리** | (1) 보안 등급 지정<br>a. 기밀성, 무결성, 가용성에 따라 상, 중, 하의 등급을 나누어 관리<br>(2) 등급별 자산 보관 구역 접근 인가자 분류 |
| **항목 평가** | (1) 보안 등급에 관한 분류 항목이 명시되어 있는가?[18] [BS7799 자산 분류 및 통제 3.1 점검항목 인용] (1점)<br>(2) 정보 보관실 안정성 확보에 관한 항목이 명시되어 있는가?[16] [ISMS 물리적 보안-2데이터센터보안 7.2.1 점검항목 인용] (1점)<br>(3) 출입 정책에 관한 항목이 명시되어 있는가?[16] [ISMS 물리적 보안-2데이터센터보안 7.2.2 점검항목 인용] (1점)<br>(4) 중소 경호·경비업체의 실정에 맞는 정보 보관실 분리 항목이 명시되어 있는가? (2점) |

### 3.5.1. 보안 등급 지정 기준

<표 7> 보안 등급 지정 기준

| 척도 / 수준 | 기밀성 | 무결성 | 가용성 |
|---|---|---|---|
| **상** | 자산에 대한 접근 권한이 있는 자 만이 접근 및 열람이 가능한 자산으로 기밀성이 상실되었을 때 회사에 상당한 손실을 입히는 자산 | 중요한 의사결정에 사용되는 데이터와 같이 무결성이 훼손되었을 경우, 회사에 상당한 손실을 입히는 자산 | 가용성이 상실되었을 때, 10분 이내에 가용성 보장이 필요한 자산 |
| **중** | 중요한 의사결정에 사용되는 데이터와 같이 무결성이 훼손되었을 경우 회사에 상당한 손실을 입히는 자산 | 무결성이 훼손되었을 경우, 부서나 팀에 상당한 손실을 입히는 자산 | 가용성이 상실되었을 때, 1시간 이내에 가용성이 필요한 자산 |
| **하** | 사외로 공개되어도 무방한 정보자산으로 기밀성의 상실이 있더라도 그 피해가 미비한 자산 | 무결성이 훼손되었을 경우라도, 그 피해가 미비한 자산 | 가용성이 상실되었을 때 24시간 이내에 가용성 보장이 필요한 자산 |




(그림 3) 중소 경호·경비업체의 정보보호 운영 프로세스(SPCIP)

## 4. 검 증

### 4.1. 검증을 위한 기본구성 및 평가 방법

<표 8>은 2012년 6월 1일부터 8월 30일까지 총 3개월간 중소 경호·경비업체 3곳에서 본 논문에서 제안한 SPCIP를 포함한 ISO27001과 ISMS를 적용·운영한 결과를 나타낸 것이다. 적용 기간은 각 1개월씩으로 6월 1일부터 6월 30일까지 SPCIP, 7월 1일부터

7월 30일까지 ISO27001, 8월 1일부터 8월 30일까지 ISMS를 적용하여 운영 후 업체별 최고 정보보호 관리자가 각 항목별로 평가하였다. 평가를 실시한 각 업체별 정보는 다음과 같다.

A. 중소 경호·경비업체의 직원 수는 최고 정보보호 관리자를 포함하여 15명이며, 현장 직원이 10명, 내근 직원이 5명으로 6대의 PC를 보유하고 있다.

B. 중소 경호·경비업체의 직원 수는 최고 정보보호 관리자를 포함하여 20명이며, 현장 직원이 14명, 내근 직원이 6명으로 6대의 PC를 보유하고 있다.

C. 중소 경호·경비업체의 직원 수는 최고 정보보호 관리자를 포함하여 12명이며, 현장직원 7명, 내근 직원 5명으로 5대의 PC를 보유하고 있다.

각 검정 항목별 평가 점수는 SPCIP에서 A업체 75점, B업체 73점, C업체 74점으로 평균 점수는 74점, ISO27001은 A업체 32점, B업체 33점, C업체 34점으로 평균 33점, ISMS는 A업체 47점, B업체 52점, C업체 49점으로 평균 49.33점으로 나타났다.

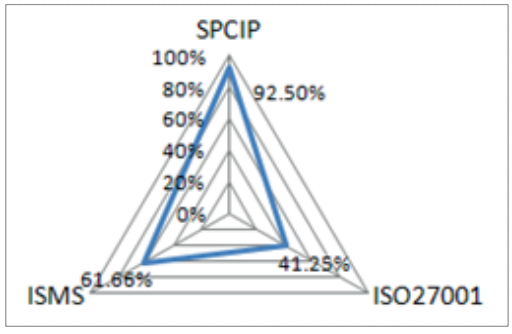
평가항목 계산 방법

$$\frac{\left\{(3.1.)+(3.2.)+(3.3.)+(3.4.)+(3.5.)\right\}_{\text{선택항목합}}}{\text{평가항목총합}} * 100$$

<표 8> 점검 항목 별 취득 점수

| 점검 항목 | 평가 업체 | 평가 점검 항목 | | |
|---|---|---|---|---|
| | | SPCIP | ISO27001 | ISMS |
| 보안 체계 확립 (3.1.) | A | 4 5 5 5 | 2 3 1 1 | 3 3 3 3 |
| | | 19 점 | 7 점 | 12 점 |
| | B | 4 4 5 5 | 2 4 2 1 | 2 3 4 4 |
| | | 18 점 | 9 점 | 13 점 |
| | C | 5 5 4 5 | 2 3 1 2 | 2 2 3 3 |
| | | 19 점 | 8 점 | 10 점 |
| 조직 환경 구성 (3.2.) | A | 4 4 | 3 1 | 3 3 |
| | | 8 점 | 4 점 | 6 점 |
| | B | 4 4 | 3 1 | 4 3 |
| | | 8 점 | 4 점 | 7 점 |
| | C | 4 4 | 2 2 | 3 4 |
| | | 8 점 | 4 점 | 7 점 |
| 인적 보안 (3.3.) | A | 5 5 5 | 1 3 2 | 3 3 3 |
| | | 15 점 | 6 점 | 9 점 |
| | B | 5 5 5 | 2 3 1 | 3 4 3 |
| | | 15 점 | 6 점 | 10 점 |
| | C | 5 5 5 | 1 2 3 | 4 3 3 |
| | | 15 점 | 6 점 | 10 점 |
| 물리적 접근 통제 (3.4.) | A | 5 5 4 5 | 3 1 1 1 | 3 3 3 2 |
| | | 19 점 | 6 점 | 11 점 |
| | B | 5 5 4 4 | 2 2 1 1 | 4 3 3 2 |
| | | 18 점 | 6 점 | 12 점 |
| | C | 4 5 5 4 | 3 1 2 1 | 3 4 3 2 |
| | | 18 점 | 7 점 | 12 점 |
| 정보자산 분류 / 보관실 분리 (3.5.) | A | 5 5 4 | 3 3 3 | 3 3 3 |
| | | 14 점 | 9 점 | 9 점 |
| | B | 5 4 5 | 2 4 2 | 4 3 3 |
| | | 14 점 | 8 점 | 10 점 |
| | C | 5 5 4 | 3 4 2 | 3 4 3 |
| | | 14 점 | 9 점 | 10 점 |
| A업체 총점 | | 75 점 | 32 점 | 47 점 |
| B업체 총점 | | 73 점 | 33 점 | 52 점 |
| C업체 총점 | | 74 점 | 34 점 | 49 점 |
| 총점 | | 222 점 | 99 점 | 148 점 |
| 평균 | | 74 점 | 33 점 | 49.33 점 |

## 4.2. 비교 검증




(그림 4) 평가 결과

(그림 4)는 위에서 제시한 계산 방법에 의해 표현되는 방사 그래프이다. SPCIP의 평가점수가 92.50%로 가장 높게 나타났으며, ISMS의 평가점수는 61.66%, ISO27001의 평가점수는 41.25% 순으로 나타났다.

제안 된 SPCIP를 ISMS와 ISO27001을 통해 비교 검증 해 본 결과 위와 같은 결과를 얻을 수 있었다,

획일화 되어 전 산업에 걸쳐 적용되는 ISO27001나 ISMS를 중소 경호·경비업체의 현재 운영 현실에 적용하기에는 다소 무리가 있었으나, 더욱 세분화 하여 중소 경호·경비업체의 실정을 반영하여 작성 된 SPCIP는 최소의 인원과 최소의 비용으로 정보유출을 효율적으로 방지할 수 있다.

또한 SPCIP를 통하여 단편적이고 일회적이었던 중소 경호·경비업체의 정보보호활동을 체계적이고 지속적인 관리가 가능하게 함으로써 전사적으로 균형잡힌 정보보호활동을 기대 할 수 있고, 특히 중소 경호·경비업체의 정보보호관리에 대한 표준적 모델 및 기준을 제시하여 중소 경호·경비업체의 정보보호관리체계 구축·운영을 촉진하고 정보보호활동에 대한 프로세스 개선을 통하여 동시에 중소 경호·경비업체의 주요 정보자산 유출 및 피해를 사전에 예방하고 대처할 수 있도록 할 수 있다.

## 5. 결 론

본 연구에서는 국내 경호·경비업체의 실정을 살펴보고, 경호·경비업체의 고객 정보 보호 실태와 현황, 그 중 중소 경호·경비업체들이 차지하는 규모와 특징들을 분석하여 정보보호 시스템 마련의 현실적 문제점의 해결 방안으로 중소 경호·경비업체의 정보보호 운영 프로세스 SPCIP(Small Physical Companies Information Security Process) 제안하였다.

앞서 살펴본 바와 같이 국내 중소 경호·경비업체는 대기업에 비해 자금부족과 인력부족 등의 문제로 인해 자체적인 보안 시스템을 구축하기에는 어려움이 있었다. SPCIP를 적용시키는 방안은 새로운 시스템을 도입하거나 하는 변동비용과 관련하여도 많은 이점을 안겨 줄 수 있다. 많은 자원이 투자되어야 가능 했던 일을 SPCIP 적용을 통하여 쉽게 접근이 가능하고 실현이 가능하며, 또한 일반적인 관리 등 대부분의 비용 측면에서 비용 절감 효과를 가져 올 수 있고 업무의 효율성 측면에서도 효과를 가져 올 수 있다.

그러나 SPCIP를 비용적 효율성만을 바라보고 시행하게 되면 업체의 업무에 비용적 효율성 이외에 절차적인 부분에 있어 문제점이 발생 할 가능성이 있다.

중소 경호·경비 업체의 SPCIP 적용은 업체의 업무를 효율적으로 하고 비용의 절감하는 부분에 있어 좋은 수단임은 검증방법인 ISMS와 ISO27001을 연구한 선행연구들이 말해 주듯 자명한 사실이나 장·단점에 대한 정확한 이해 없이 제시 한 운영 프로세스를 도입하는 것은 위험한 선택일 수 있다.

본 연구는 국내 중소 경호·경비업체의 현황을 알아보고 ISO27001과 ISMS의 세부 통제항목 중 중소 경호·경비업체에 적용 가능한 항목을 분석하고 세분화 하여 SPCIP를 제시하였다. 그러므로 자금력과 인적자원의 보유현황의 차이가 있는 모든 중소 경호·경비 업체에 일반화하여 적용하기엔 한계가 있다.

민감한 고객 정보를 다루는 분야인 만큼 업체의 경쟁력을 강화시키고 책임자와 직원들의 정보보안 인식을 제고시킴과 동시에 물리적 보안과 비 물리적 보안을 함께 다룰 수 있는 전문 인력의 양성이 앞으로의 중소 경호·경비업체의 발전 방향이 될 것이다.

## 참고문헌

[1] 황서종, “중소기업의 개인정보보호성과 영향요인에 관한 실증 분석”, 서울시립대학교 박사논문, pp. 1-2, 2012.2.

[2] 김병일, “중소기업의 정보 활용 극대화 및 보호에 관한 연구”, 한양대학교 석사논문, pp. 30-37, 2010.8.

[3] 사이버경찰청, http://www.police.go.kr/infodata/pds_07_totalpds_02_01.jsp#none, 검색일: 2012.9.14.

[4] 국가통계포털, http://kosis.kr/abroad/abroad_01List.jsp, 검색일: 2012.9.14.

[5] 사이버경찰청, http://www.police.go.kr/infodata/pds_07_totalpds_02_01.jsp#none, 검색일: 2012.9.14.

[6] 김태달, “ISO 27001의 ISMS 보안성숙도 측정 모델링에 관한 연구(ISO 27004 정보보호관리 측정 및 척도 체계)”, 한국컴퓨터정보학회지, p. 154, 2007.12.

[7] 임건묵,김인재, “정보보호 관리체계의 실증분석: ISO27001과 COBIT4.1의 비교”, 한국경영정보학회 추계학술대회, p. 226, 2010.11.
[8] 임건묵,김인재, “정보보호 관리체계의 실증분석: ISO27001과 COBIT4.1의 비교”, 한국경영정보학회 추계학술대회, p. 226, 2010.11.
[9] 전남재, “정보보호관리체계를 활용한 금융권 정보보호 모델 연구”, p. 24, 2010.6.
[10] 한국인터넷진흥원, http://isms.kisa.or.kr/kor/notice/dataView.jsp?mode=view&p_No=48&b_No=48&d_No=3, ISMS인증심사기준표 점검항목 (1)정보보호정책, 검색일: 2012.9.17.
[11] 한국인터넷진흥원, http://isms.kisa.or.kr/kor/notice/dataView.jsp?mode=view&p_No=48&b_No=48&d_No=3, ISMS인증심사기준표 점검항목 (2)정보보호조직, 검색일: 2012.9.17.
[12] 신정우, “BS7799에 근거한 정보보호 현황 평가를 통한 정보보호 체계 개선”, 서강대학교 석사논문, pp. 49-53, 2004.7.
[13] 한국인터넷진흥원, http://isms.kisa.or.kr/kor/notice/dataView.jsp?mode=view&p_No=48&b_No=48&d_No=3, ISMS인증심사기준표 점검항목 (5)정보보호교육 및 훈련, 검색일: 2012.9.17.
[14] 한국인터넷진흥원, http://isms.kisa.or.kr/kor/notice/dataView.jsp?mode=view&p_No=48&b_No=48&d_No=3, ISMS인증심사기준표 점검항목 (6)인적보안, 검색일: 2012.9.17.
[15] 한국인터넷진흥원, http://isms.kisa.or.kr/kor/notice/dataView.jsp?mode=view&p_No=48&b_No=48&d_No=3, ISMS인증심사기준표 점검항목 (3)외부자보안, 검색일: 2012.9.17.
[16] 한국인터넷진흥원, http://isms.kisa.or.kr/kor/notice/dataView.jsp?mode=view&p_No=48&b_No=48&d_No=3, ISMS인증심사기준표 점검항목 (7)물리적보안, 검색일: 2012.9.17.
[17] 한국인터넷진흥원, http://isms.kisa.or.kr/kor/notice/dataView.jsp?mode=view&p_No=48&b_No=48&d_No=3, ISMS인증심사기준표 점검항목 (4)정보자산분류, 검색일: 2012.9.17.
[18] 신정우, “BS7799에 근거한 정보보호 현황 평가를 통한 정보보호 체계 개선”, 서강대학교 석사논문, pp. 49-53, 2004.7.

## [저 자 소 개]

**강 푸 름(Poo-Reum Kang)**

2011년 2월 경기대학교
경호안전학과 학사
2011년 3월~현재 경기대학교
산업보안학과 석사 재학

email : prjjang5@nate.com

**이 동 휘(DongHwi Lee)**

2000년 경기대학교 컴퓨터과학과
(이학사)
2003년 경기대학교 정보보호기술공학과
(공학석사)
2006년 경기대학교 정보보호학과
(정보보호학박사)
2011년~2012년 5월 University of Colorado Denver, Dept. of Computer Science and Engineering
현재 경기대학교 산업보안학과

email : dhclub@naver.com

**김 귀 남(Kuinam J. Kim)**

Univ. of Kansas 수학과 학사
Colorado State Univ. 통계학 석사
Colorado State Univ. 산업공학 박사

현재 경기대학교 융합보안학과 교수
산업기술보호특화센터장

email : harap123@hanmail.net