보안 모니터링과 감청의 차이점에 관한 연구

A Study on the Differences between Security Monitoring and Wiretap

홍창화*, 최민규**, 김태훈**

Chang-Hwa Hong*, Min-Kyu Choi** and Tai-hoon Kim**

요 약

통신비밀보호법상의 감청과 보안모니터링은 유사한 것으로 간주될 수 있으나, 실제로는 전혀 다른 개념이라고 할 수 있다. 하지만 감청과 보안모니터링의 개념상 차이점에 대한 연구가 부족한 현 시점에서 두 용어가 혼용되고 있으며, 이로 인해 다양한 부작용이 나타나고 있다. 본 연구에서는 목적, 범위, 대상, 정보활용방법 등의 분야에서 통신감청과 보안모니터링을 비교함으로써 이 두 가지 개념의 차이점을 비교, 설명하였다.

Abstract

Even though security monitoring and wiretap seem to be same things from the current legal point of view, these two concepts are different. But because the researches related to the differences between wiretap and security monitoring, there are some confusions about these concepts, so there are some side effects. In this paper, we try to explain the differences between wiretap and security monitoring in the aspects of object, scope, target and application method.

Key words : Security Monitoring, Wiretap, Side effect

I. 서 론

통신비밀보호법상의 감청과 보안모니터링은 유사한 것으로 간주될 수 있으나, 실제로는 전혀 다른 개념이라고 할 수 있다. 본 장에서는 우선 통신감청이란 무엇인지를 기술하고, 목적, 범위, 대상, 정보활용방법 등의 분야에서 통신감청과 보안모니터링을 비교함으로써 이 두 가지 개념의 차이점을 비교, 설명한다.

Ⅱ. 통신비밀보호법상의 감청

통신비밀보호법상의 감청과 도청, 그리고 보안모니터링은 유사한 행위이면서도 법률적 측면에서 보았을 때 의미가 확연히 다르다.

우선 도청이란, 유선 또는 무선의 방법으로 타인의 사적인 대화를 동의없이 은밀히 청취하여 그 비밀성을 침해하는 행위를 뜻하는 용어로서[1], 좁은 의미로는 공개를 예기하지 않은 개인과의 대화를 당사

* 산성공사(Sanseonggongsa)
** 한남대학교 공과대학 멀티미디어학부(Dept. of Multimedia, Hannam University)
· 교신저자 (Corresponding Author) : 김태훈
· 투고일자 : 2008년 12월 1일
· 심사(수정)일자 : 2008년 12월 3일 (수정일자 : 2009년 1월 14일)
· 게재일자 : 2009년 2월 28일

자 동의없이 은밀히 청취하거나 통신의 내용을 청취하는 것을, 넓은 의미로는 외부에서 제 3자의 대화를 청취하거나 대화의 일반당사자들의 승낙 하에 청취한 경우를 포함한다[2]. 또한 미국 연방대법원의 '블랙(Hugo L. Black)' 판사는 도청의 정의를 "도청이란 사적이라고 생각하면서 행하는 대화나 토의를 비밀리 또는 은밀히 경청하는 행위이다"[3]라고 규정하였는데, 중요한 것은 이 행위가 불법적으로 행해진다는 것이다. 도청은 일반적으로 타인간의 비공개의 대화나 전화통화 등을 기계적 · 전자적 수단을 사용하여 통화의 당사자가 모르게 엿듣거나 녹음하는 것을 의미하는 수단인데, 타인의 사생활의 비밀을 아무런 법률적 근거없이 침해하게 되는 특성 때문에 불법적인 것으로 간주된다.

감청은 일반적으로 도청과는 구별되는 개념으로 이해되고 있는데, 도청이 타인간의 대화 혹은 통신을 청취하는 일반적인 행위를 의미하는 반면, 감청은 이러한 행위 중에 법적인 근거를 가지는 행위를 말하는 용어로서, 법적인 근거를 가지는 정보통신상의 수사행위를 말한다[4].

법적인 근거를 갖는다는 것에 대해서는 조금 더 확실하게 정의할 필요가 있다. 감청은 일반적으로 전화와 같은 전기통신 내용의 감청과 대화감청으로 구분된다. 전화감청은 주로 현행 헌법 제18조에서 '모든 국민은 통신의 비밀을 침해받지 아니한다.'라고 규정한 통신비밀의 불가침성과 제17조의 '사생활의 비밀과 자유'와 관련하여 기본권 침해의 문제를 야기하고 있고, 특히 대화감청은 헌법 제16조의 '주거의 자유'와도 관계되어 있다. 또한 통신의 불가침성은 일반적으로 열람의 금지, 누설의 금지, 정보의 금지 등을 그 내용으로 하고 있기 때문에 통신의 비밀을 침해하는 것은 통신의 불가침성은 물론 그것을 내포하고 있는 사생활의 비밀과 자유를 침해하는 것이 된다.

이와 같은 관점에서 볼 때에는 감청과 도청의 차이가 없어 보이지만, 헌법상 보장되는 통신의 자유는 헌법 제37조 제2항의 이른바 법률유보조항에 의해 '국가안전보장, 질서유지 또는 공공복리를 위해 필요한 경우'에는 법률로서 제한될 수 있다는 것이므로, 헌법에 근거하여 제정된 통신비밀보호법에 의거하여 시행되는 감청은 도청과 달리 합법적인 것이 되며, 이것이 도청과의 근본적인 차이점이 된다.

Ⅲ. 미국 육군 규정상의 보안모니터링의 특성

미국 육군규정 380-53에 따르면, 보안모니터링이란 '분석 자료를 제공하기 위해 어떤 이의 공식적인 원격통신 내용을 듣고 읽고 복사하고 기록하는 행위'를 말한다. 또한 이 규정에서는 원격 통신 시스템의 범위로 전화기(일반적인 전화선, 야전, 휴대), 무선전화기, 팩시밀리(내부 및 외부), 컴퓨터(독립망과 연결된 모든 것), 전송 수단으로 원격 통신 회선을 이용하는 자동화 정보체계, 비디오 화상 회의 시스템, 호출 장치 및 전술적인 라디오 시스템(음성, 무선텔레타이프, 데이터 등)을 포함하며, 이에 국한되지 않는다고 정의함으로써 현존하는 대부분의 통신체계를 대상으로 하고 있다.

즉, 보안모니터링을 수행하기 위해서는 미국 육군의 통신체계라는 특정 범위 안에서 도청 혹은 감청과 마찬가지로 통신의 내용을 듣고, 기록하고, 분석하는 내용을 포함하게 된다.

얼핏 법적인 문제를 야기할 것으로 판단되는 보안모니터링이 중요한 이유는, 대부분의 보안 문제가 기술적인 약점이 아니라 운용중에 사용자의 고의나 실수에 의해 발생하는 경우가 많으며, 정보는 다양한 통신 수단을 통해 유출되어 각국 또는 범죄조직, 테러조직, 혹은 경쟁조직에게 유출될 수 있기 때문이다.

이러한 위험을 최소화하기위해 보안모니터링이 수행되며, 보안모니터링은 사전 예방 단계 (특정 범위의 통신 수단에 대한 지속적인 감시를 통해 정보의 흐름을 탐지, 분석함으로써 중요한 정보에 대한 탈취를 사전에 차단), 인지 단계 (중요 정보의 유출 시도 혹은 유출 상황을 파악), 대응 단계 (중요 정보 유출 상황을 강제로 억제), 복구 및 회귀 단계 (어떠한 정보가 유출되었는지를 파악함으로써 이로 인한 파급효과를 최소화)로 구성된다(그림 1 참조).

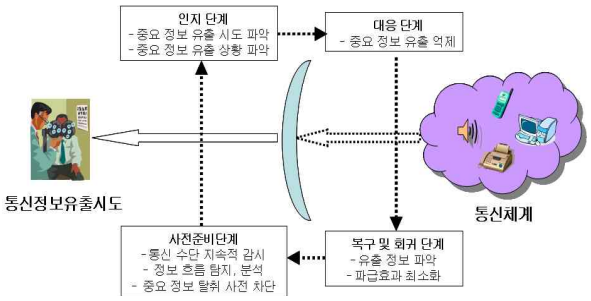

그림 1. 보안모니터링수행단계
Fig. 1. Security Monitoring Process

보안모니터링을 수행하기 위해서는 특정 범위에 포함된 모든 통신 수단에 대한 고려가 필요하며, 구두로 전달되는 기본적 행태와 함께 전자적 신호로 전달되는 첨단 행태에 대한 고려까지 모두 함께 진행되어야 한다.

시스템에 저장된 정보와 달리 통신중인 정보는 다양한 위험에 처할 가능성이 더 높아지게 되는데, 이것은 3중 잠금장치가 된 금고안에 보관된 현금보다 휴대중인 현금이 도난위험이 더 높은 것과 유사하다. 하지만 통신을 통해 유통되지 않는 것은 이미 정보라고 할 수 없을 정도로 활용도가 낮은 데이터에 불과한 것이 될 것이므로, 통신을 통해 정보를 전달하는 것은 불가피한 행위이다.

통신을 통해 정보가 유통될 때에는 다음과 같은 내용들에 주의를 기울여야 한다.

첫째, 각 통신망에는 해당 통신망에서 유통되는 정보의 수준이 미리 정해져 있다.
둘째, 각 통신망에는 해당 통신망에서 유통되는 정보의 유형이 미리 정해져 있다.
셋째, 각 통신망에는 해당 통신망에서 정보를 유통할 권한이 있는 주체가 미리 정해져 있다.

따라서 정보를 유통할 권한이 없는 주체가 정보를 유통하였거나, 정상적인 유형이 아닌 정보를 유통하였거나, 낮은 수준의 통신망에서 높은 수준의 정보를 유통하였다면 이러한 행위들은 모두 일상적인 예측 가능한 통신행위의 범주를 벗어난 것이 되고, 이는 보안침해와 관련이 있을 가능성이 높은 것이다.

보안모니터링을 통해 이러한 행위들을 확인, 방지, 통제할 수 있으며, 만일 내부의 정보가 원칙을 위배하여 외부로 유출되었다면 이에 대한 대책 수립할 수 있는 기회를 제공할 수 있기 때문에 보안모니터링은 중요한 의미를 갖게 된다.

예를 들어 네트워크를 통한 내부 정보의 전달을 생각해 볼 수 있다. 첨단기술이나 방위산업 정보를 다루는 중요 통신망은 암호화된 형태로 데이터를 저장함과 동시에 전송하고 있기 때문에, 이론적으로는 서울본사에서 부산지사로 보내는 데이터를 외부 경쟁기업에서 도청한다고 하여도 내용을 확인하기 어렵게 되어 있다. 하지만 어떤 이유에서인지 암호화되지 않는 정보가 네트워크를 통해 전달되고 있다면, 이 정보는 평상시 해당 통신망에서 유통되던 정보의 유형이 아닌 특이 유형의 정보로 간주될 것이고, 보안모니터링에 의해 탐지되어 분석되고 보고될 것이다.

이동중인 정보가 저장중인 정보보다 높은 위험도를 가진다는 사실을 고려하지 않더라도, 암호화되지 않은 형태로 전송된 정보는 이미 유출된 것으로 간주되어야 하며, 이 역시 다른 관점에서 본다면, 만일 보안모니터링이 진행되고 있지 않은 상태라면 이러한 정보의 노출 혹은 유출의 증거를 확보할 수 없게 될 것이고, 기업은 노출 혹은 유출된 정보를 파악하고 이에 대한 대응수단을 마련하기 힘들게 될 것이다.

Ⅳ. 감청과 보안모니터링의 차이

감청과 보안모니터링은 유사한 행위를 포함하고 있음에도 불구하고 동일한 개념으로는 볼 수 없는 바, 이것은 다음과 같은 차이점이 엄연히 존재하기 때문이다.

4-1 목적에서의 차이

통신감청의 목적 : 현행 통신비밀보호법은 1조에서 “이 법은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.”고 규정하고 있다.

앞서 언급한 바와 같이, 헌법상 보장되는 통신의 자유는 무제한하게 보장되는 것이 아니라 헌법 제37

조 제2항의 이른바 법률유보조항에 의해 '국가안전보장, 질서유지 또는 공공복리를 위해 필요한 경우'에는 법률로서 제한될 수 있는 것이므로, 통신비밀보호법에 근거하여 감청을 수행하는 것이 가능하다.

또한 이는 다시 말해서, 국가안전보장, 질서유지, 공공복리 등이 감청 행위의 직접적인 목적임을 나타내는 것이기도 하다.

급변하는 정보화시대에 국제사회의 경쟁에서 우위를 점하기 위해서는 보다 신속하게 정보를 입수하여 정책결정에 참고하는 것이 무엇보다 중요하다. 또한 점차 지능화되고 조직화되는 범죄를 효과적으로 억제하기 위해서도 감청 등의 전자감시를 이용한 수사가 불가피한 경우가 많은데, 이는 범죄를 감시하고 단속하는 국가기관이 첨단 과학장비에 의한 수사를 행할 수 없게 된다면 이러한 첨단장비를 이용하여 범죄를 행하고 있는 범죄조직은 사실상 형사절차의 적용범위 안에서 방치되어지는 것이나 다름없기 때문이다.

따라서 감청을 통한 수사방법은 국가의 대외안보를 위해서 뿐 아니라, 대내안보와 범죄수사를 위해서도 반드시 필요한 것이라 할 수 있다.

보안모니터링의 목적 : 보안모니터링이란, 특정 대상의 특정 통신망에서 행해지는 통신 수단에 대한 지속적인 감시를 통해 정보의 흐름을 탐지, 분석함으로써 중요한 정보에 대한 탈취를 사전에 차단하거나, 중요 정보의 노·유출 시도 혹은 노·유출 상황을 파악하거나, 중요 정보 노·유출 상황을 강제로 억제하거나, 혹은 어떠한 정보가 유출 혹은 노출되었는지를 파악함으로써 이로 인한 파급효과를 최소화하기 위한 일련의 조치들을 포괄적으로 포함하는 것이다.

보안모니터링의 목적은 내부의 통신정보가 안전하게 유통되고 있는지를 확인함과 동시에 노·유출된 정보를 파악, 분석하고 이에 대한 대책을 강구하기 위한 것이다.

통신망은 자체의 보안대책을 수립하여 운용하고 있으며, 이를 통해 정보의 노·유출을 통제하고자 하고 있다. 하지만 일반적으로 보안대책은 외부로부터의 침입을 탐지, 억제, 방어하기 위해 수립되어 운용되고 있는 경우가 많기 때문에 내부로부터 노·유출되는 정보의 탐지에는 취약한 경우가 많게 되고, 이를 보완할 수 있는 것이 보안모니터링이다.

4-2 대상에서의 차이

보안모니터링의 대상은 일정하게 정해져 있는 것은 아니지만, 그렇다고 늘 변경되는 것도 아니다. 보안모니터링은 감청이나 도청과 비교하였을 때 다분히 기술 의존적인 것이므로, 모니터링을 수행할 대상과 범위가 정해져 있지 않으면 처음부터 적용하기가 힘들다.

또한 관리적 측면에서 볼 때에도, 보안모니터링을 수행하기 위해서는 모든 구성원으로 하여금 모든 공식적 통신이 모니터링되고 있음을 인식하게 하고 또한 이에 동의하도록 하여야 하기 때문에, 사전에 대상과 범위를 분명하게 결정할 필요가 있다.

통신감청의 대상 : 현행 통신비밀보호법은 제2조 제1호에서 '통신'이라 함은 우편물 및 전기통신이라고 정의하고 있으므로, 구체적으로 통신비밀보호법의 규율대상은 "우편물, 전기통신, 대화"라고 할 수 있다.

감청에 관하여 형법, 형소법 등 수개의 법률에 분산하여 관련 규정을 두고 있는 독일의 경우 처벌의 대상이 되는 행위와 예외적으로 허용되는 행위가 정확히 일치하지 않지만, 우리 법은 미국법의 예에 따라 통신비밀보호법에 통일적으로 규정하고 있기 때문에, '전기통신의 감청 또는 대화의 녹취·녹음'에 해당될 경우 통신비밀보호법에 정한 각종 규제 또는 제재의 대상이 된다.

통신비밀보호법에 의하여 "우편물, 전기통신, 대화" 등 거의 모든 통신수단이 감청의 대상이 될 수 있으나, 감청은 중대한 사생활 침해행위가 될 수 있기 때문에, 감청에 관한 법률을 가지고 있는 나라에서는 감청 대상범죄를 제한하고 있는 실정이다.

감청 대상범죄 목록은 대체로 위험한 범죄, 국가안보와 관련되는 범죄, 조직적인 성격을 가지고 있는 범죄 등이며, 우리나라의 통신비밀보호법은 제5조 제1항에서 감청 대상범죄를 열거하고 있다.

보안모니터링의 대상 : 보안모니터링의 영역은

특정 대상의 특정 통신망으로 정의할 수 있으며, 이는 필요한 수준 혹은 내용에 따라 필요한 순간마다 다르게 설정할 수 있다. 보안모니터링과 통신감청이 주된 차이점은, '사적영역' 혹은 '내심영역'에 대한 것인데, 이들 영역, 즉 공적인 영역을 제외한 모든 부분은 보안모니터링의 대상 혹은 범위에 포함될 수 없다. 이러한 이유로 보안모니터링은 프라이버시 문제와는 상관없는 별개의 관점으로 바라볼 수 있게 된다.

4-3 방법에서의 차이

4-3-1 통신감청의 방법

합법적인 수행 : 합법적으로 통신감청을 수행하기 위해서는 허가를 받아야 하고, 또한 적절한 절차를 따라야 한다.

국가안보목적 감청의 경우, 통신당사자자의 성격에 따라 고등법원 수석부장판사의 허가를 받아야 하는 경우와 대통령의 승인을 받아야 하는 경우로 나뉘어질 수 있으며(법 제 7조 제1항 참조), 양 경우는 구체적인 허가 또는 승인절차에서 다소간의 차이가 있다. 그러나 기타의 요건이나 구체적 실행절차 등에서는 대동소이하다. 허가 또는 승인이 내려진 경우 구체적 감청행위의 실행은 감청허가를 신청한 정보수사기관의 장(허가를 요하는 경우), 또는 계획서를 제출한 정보수사기관의 장(승인을 요하는 경우)이 담당한다.

범죄수사를 위한 감청의 경우 감청에 대한 허가는 일종의 영장으로서 구속 등 다른 강제수사 방법과 동일하게 검사(군검찰관을 포함한다)만이 허가를 청구할 수 있다(법 제6조 제1항). 사법경찰관 및 군 사법경찰관은 법원에 직접 허가를 청구할 수 없으며 요건이 구비된 경우 검사 또는 군검찰관에 대하여 허가를 신청할 권한만을 가진다(같은 조 제 2항). 감청이 허가된 경우 일반적인 수사상 강제처분의 집행방법과 동일하게 허가를 청구 또는 신청한 검사 또는 사법재판관이 이를 집행한다. 다만 감청의 특성상 체신관서 기타 관련기관(이하 통신기관이라 한다)등에 그 집행을 위탁하거나 집행에 관한 협조를 요청할 수 있으며(법 제9조 제1항) 집행을 위탁하거나 집행에 관한 협조를 요청하는 자는 허가서 표지의 사본을 교부하고 자신의 신분을 표시할 수 있는 증표를 체신관서나 그 밖의 관련기관의 장에게 제시하여야 하며 이를 위탁받거나 이에 관한 협조요청을 받은 자는 허가서의 사본을 시행령 제15조의 2에 따라 3년간 보존하여야 한다(법 제9조 제2항, 시행령 제15조의 2).

은밀한 수행 : 감청은 감청을 당하는 대상자의 의지와는 상관없이 수행되는 경우가 대부분이므로, 감청을 당한다는 사실을 알지 못하도록 은밀하게 수행되는 경우가 많다.

감청의 집행방법과 관련하여, 감청허가를 받은 경우 별도의 수색영장없이 감청장치 부착을 위하여 임의로 대상자의 주거에 들어가는 행위에 대한 적법성 여부가 문제된다. 이에 대해서는 법률상 명확한 규정도 없고 법원에서 다툼이 있었던 적도 없기 때문에 실무상 혼란을 야기하기도 한다.

대법원은 「압수수색등영장실무편람」에서 "법에서 말하는 회화의 감청은 타인의 주거에 대한 물리적 침입없이 타인의 대화내용을 감청하는 것을 상정하고 있을 뿐이라고 보여지므로, 타인의 주거에 대한 물리적 침입을 수반한 회화의 감청은 통신제한조치의 처가 대상이 아니라고 할 것이고, 그 밖에 현행법상으로는 타인의 주거에 침입하여 도청기를 설치할 수 있는 방법이 없으므로 결국 타인의 주거 등에 침입하여 도청기를 설치하고 타인의 대화내용을 감청하는 것은 허용되지 않는다"고 해석하고 있다.

이와 관련하여 자세히 살펴보면 법 제14조 제2항에 의한 대화감청은 제조 제1항의 준용규정 "다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우" 또는 제7조 제1항의 준용규정 "국가안전보장에 대한 상당한 위험이 예상되는 경우에 한하여 그 위해를 방지하기 위하여 정보수집이 특히 필요한 때"에 한하여 인정되는 것이므로 결국 통신제한조치 허가를 근거로 타인의 주거에 몰래 들어가 감청장치를 부착할 수 있느냐 여부는 국가적·사회적 법익과 개인의 주거의 자유란 개인적 법익의 충돌에서 이익형량의 법칙에 따라 비교하여 어느 것을 우선하느냐 하는 것에 달려있다고 볼 수 있다.

4-3-2 보안모니터링의 방법

합법적인 수행 : 국가안보목적 감청의 경우 통신 당사자자의 성격에 따라 고등법원 수석부장판사의 허가 혹은 대통령의 승인이 필요하며, 범죄수사를 위한 감청의 경우 감청에 대한 허가로서 영장이 필요하지만, 보안모니터링은 이러한 허가, 승인, 영장이 필요하지 않다. 보안모니터링이 수행된다는 사실은 이미 모니터링의 대상이 되는 통신수단을 사용하는 사용자들에게 사전 공지된 상태이며, 공적인 내용을 통신하도록 홍보가 진행된 상태이기 때문이다.

하지만 현실적으로 이러한 환경을, 즉 전적으로 공적인 통신만을 수행하는 조직은 군대를 제외하고는 거의 없다고 할 수 있기 때문에, 무작정 보안모니터링을 수행하는 것은 있을 수 없는 일하다. 따라서 합법적인 보안모니터링 수행을 위해서는 적절한 절차에 따라야 하며, 이에 위배되는 행위는 개인정보의 침해 혹은 사생활 침해로 이어질 수 있으므로 주의하여야 한다.

보안모니터링을 수행하기 위해서는 그에 합당하는 이유가 반드시 존재하여야 하는데, 가장 명확한 이유는 해당 통신수단을 통해 유통되는 정보의 보안수준 혹은 중요성이다. 보안모니터링은 보안수준관리의 일환으로 진행되는 것이므로 해당 보안수준을 유지하기 위해 보안모니터링을 수행하는 것은 당연하며, 보안수준이 높은 통신수단일수록 엄격한 보안모니터링이 수행되어야 한다.

일반적으로 보안수준은 특정 시스템 (여기에서의 시스템은 물리적 시스템뿐만 아니라 이를 관리하는 정책이나 절차와 같은 무형의 요소들, 그리고 인적자원까지를 포함하는 광의의 개념 임)에 대하여 결정되므로, 통신수단은 그 일부가 된다. 따라서 보안모니터링을 수행할 대상을 결정하는 것은 보안수준이 결정된 그 다음 단계에서 할 일이 된다.

보안모니터링 대상의 결정과 보안모니터링 방법의 결정은 상호 보완적 관점에서 결정되어야 한다. 보안모니터링의 대상이라고 해도 적절하게 이를 수행할 방법이 없다면 보안모니터링의 대상으로 지정하는 것 자체가 무의미하기 때문이다. 특히 이러한 상황은 통신수단이 광범위하게 이미 사용 중인 상황에서 추가로 보안모니터링을 수행하고자 하는 경우에 발생할 수 있다.

보안모니터링을 수행하기위해서는 사용자들이 모두 이를 인정하고 동의하여야 하는데, 특정 방법의 경우에는 사용자들이 이를 어려울 수도 있다. 이러한 경우에는 보안모니터링 방법을 변경할 필요가 있으며, 경우에 따라서는 이로 인해 보안모니터링 대상이 변경되는 경우도 발생할 수 있다. 따라서 보안모니터링 대상의 결정과 방법의 결정, 그리고 사용자 동의에 이르는 과정은 피드백을 통해 최적의 결론을 얻을 수 있어야 한다.

이후에 사용자가 동의한 보안모니터링 방법을 구현하게 되는데, 기술적, 관리적 관점을 모두 고려하여야 한다. 구현된 방법을 통해 보안모니터링을 수행하고 있다는 사실은 계속 사용자들이 인지할 수 있도록 공지되어야 하며, 사용자들은 이를 통해 지속적으로 주의를 기울일 수 있게 된다. 또한 보안모니터링의 결과 문제가 있다고 판단된 사항은 사용자에게 피드백되어야 하며, 향후에는 유사한 문제가 발생하지 않도록 홍보하여야 한다.

공개적인 수행 : 감청의 경우는 일상적인 대화까지도 대상으로 할 수 있지만, 보안모니터링은 통신수단을 통해 이루어지는 통신내용만을 대상으로 한다. 따라서 보안모니터링을 수행하는 방법은 비교적 간단하며, 전기적/기계적 통신 장비에 보안모니터링을 지원하는 장치를 추가로 탑재하면 된다. 이러한 장비의 탑재 자체가 사생활 침해나 개인정보의 유출로 이어질 수 있다는 거부감을 줄 수 있으므로, 사용자의 사전 동의가 반드시 필요하다. 또한 보안모니터링은 현재의 통신이 모니터링되고 있다는 사실을 충분히 공지한 다음에 수행되어야 한다.

보안모니터링을 수행하는 방법은 모니터링의 범위와 대상을 어떻게 설정하였는지에 따라 다르게 된다. 예를 들어 전화통화를 모니터링의 범위에 포함하였다면, 군용 통신과 같이 처음부터 사적인 통신이 존재할 수 없는 특수한 경우를 제외하고는, 누군가가 전화통화를 감청하고 이 중에서 공적인 부분과 사적인 부분을 분류하여야 하며, 공적인 부분만을 모니터링하도록 하여야 하는데, 이는 다분히 사생활 침해

문제를 야기할 수 있으므로 이에 대한 조치도 함께 강구되어야 한다.

감청과의 차이점은, 감청은 은밀히 수행되기 때문에 당사자조차도 현재 감청이 진행되고 있다는 것을 인지할 수 없지만, 보안모니터링은 모든 당사자가 이미 통신의 내용을 누군가 듣고 있다는 것을 공지 받았기 때문에 이를 알고 있다는 것이다.

즉, 보안모니터링은 공개적으로 수행된다고 할 수 있다.

4-4 정보활용방법에서의 차이

4-4-1 감청으로 획득한 정보의 활용

합법적 절차에 따라 획득하지 않은 정보 : 감청으로 획득한 정보의 활용에 관한 법적논의는 선진 각국에서는 이미 오래전부터 논의되어 왔던 문제이다. 특히 미국은 1928년의 Olmstead 판결에서 감청에 관한 허용 여부 등이 최초로 논의된 이래 후속되는 판례 및 이들 판례에 의하여 제기된 내용을 입법화하는 과정에서 감청과 관련한 각종 법률적 문제점들이 매우 심도있게 논의되어졌다.

1928년 Olmstaed 판결에서 연방대법원은 수정헌법 제4조가 도청에 대하여는 적용될 수 없다고 판시하였지만 의회는 도청을 불법화하여 그 행위로 인하여 획득된 대화내용을 연방형사절차에서 증거로 사용할 수 없도록 하는 법률을 제정함으로서 대화비밀을 보호할 수 있다는 점은 인정하였다.

미국 의회는 6년 후인 1934년 통신의 도청 및 도청내용의 공개행위를 규제하는 내용의 연방통신법(Federal Communication Act) 제 605조를 제정하였다. 동 규정은 사인은 물론 주정부 및 연방정부공무원에 의한 도청에도 적용되고, 한 주에 국한된 통신은 물론 주간의 통신에도 적용되는 것으로 해석되었으며, 비록 동법이 동법에 위반하여 수집한 증거에 대한 증거배제법칙을 명백히 선언하는 규정을 두고 있지는 않았으나 그러한 효과를 가지고 있는 것으로 해석되었으며, 도청에 의하여 얻어진 정보의 결과로 발견된 파생증거에도 그 효력이 미친다고 판결되었다.

우리나라의 통신비밀보호법은 “전기통신의 감청”과 “공개되지 아니한 타인간 대화의 녹음 또는 녹취”를 그 규제대상으로 삼고 있는데, 정보수사기관이 전기통신 혹은 타인간의 대화를 녹음•청취하는 경우에 당사자가 동의하지 않는 한 그 대상자가 내국인인 경우에는 법원의 허가를 얻어야 하고, 그 대상자가 외국인인 경우 등에 대해서는 대통령의 승인을 얻도록 되어 있으며, 위의 허가 또는 승인없이 임의로 감청 또는 대화의 녹음•청취를 행한 경우에 그 행위는 위법한 행위로서 형사처벌의 대상이 되고, 그러한 불법감청으로 인하여 수집한 자료는 형사절차 등에서 증거로서의 자격을 상실하게 된다.

합법적 절차에 따라 획득한 정보 : 검사, 사법경찰관 또는 집행을 위탁받은 수탁기관의 종사자 등 감청을 집행하는 자는 감청으로 인하여 취득한 내용과 허가과정, 허가여부 및 허가내용 등에 관하여 외부에 공개하거나 노출할 수 없도록 되어 있다(법 제11조).

또한, 법 집행으로 인하여 알게 된 타인의 비밀을 노출하거나 대상자 명예를 훼손하는 행위도 금지된다(시행령 제12조 제2항).

미국법의 경우 감청을 집행함에 있어 본래의 목적과 무관한 통신에 대한 감청은 최소화하여야 한다는 규정을 두고 있으나, 그와 같은 규정을 두고 있지 아니한 우리 법 아래에서도 같은 취지로 해석하여야 할 것이다.

4-4-2 보안모니터링으로 획득한 정보의 활용

보안모니터링을 통해 획득한 정보는 합법적 절차를 통해 획득된 것으로 간주되므로, 이에 대한 활용은 전적으로 보안모니터링을 수행한 기관이 결정할 문제이다.

책임을 수반하는 경우 : 보안모니터링을 통해 획득한 정보에 기반하여 통신 당사자가 책임을 지는 경우가 발생할 수 있으며, 이는 몇 가지 판례를 통해서도 알려져 있다.

1993년 캘리포니아 항소법원의 Bourke vs. Nissan Motor Corp. 사건은 고용자가 근로자의 전자우편에 접근할 권리가 있음을 인정하는 것이다. 이 판례에서 법원은 ‘프라이버시의 기대가 있다고 할지라도 그러한 피용자의 프라이버시보다는 사업을 적절하게 이

끌어야 하는 고용자의 이익이 더 중요하다'고 하였다. 1994년에 선고된 Shoars vs. Epson America, Inc. 사건에서도 고용자의 보안모니터링 권한을 허용하고 있다.

책임을 수반하지 않는 경우 : 일반 기업의 경우, 피용자들이 업무에 지장을 초래하지 않는 수준에서 사적인 통신을 수행하는 것은 어느 정도 용인될 수도 있으나, 군용 통신과 같은 특별한 경우에는 사적 통신을 하는 것은 원천적으로 불가하다.

보안모니터링은 본래 누군가에게 책임을 묻기 위해 진행되는 것이 아니라, 정보의 유출을 방지하기 위해 수행하는 것이므로 정상적인 절차에 따라 수행된 통신에 대해서는 책임의 소재가 불분명하다.

암호화 통신을 하도록 되어 있는 통신 수단을 통해 평문 통신이 이루어지고 있는 경우에는 이를 탐지하여 조치를 취하여야 하지만, 정상적인 형태로 진행되고 있는 암호화 통신 데이터가 유출되어 해석된 경우에 대해서는 통신 수행자에게 책임을 지울 수 없으며, 오히려 이러한 경우에는 즉각 유출된 정보의 내용과 수준을 파악하여 대책을 마련하고 암호 체계를 수정하여야 할 것이다.

일상적인 환경에서의 보안모니터링을 통해 획득된 정보에 대해서는 크게 두 가지를 확인하여야 한다.

(1) 해당 통신수단에 지정된 형식에 따라 통신이 진행되고 있는가?
(2) 해당 통신수단에서 유통될 수 있는 수준의 정보가 유통되고 있으며, 자격을 갖춘 사용자에 의해 이루어지고 있는가?

이 두 가지 사항에 대하여 문제없이 진행되고 있는 경우라면 획득된 정보들은 모두 일상적인 것으로 분류되어 처리된다. 하지만 이 두 가지 사항에 위배되는 통신이나 통신시도가 보안모니터링에 의해 탐지된 경우, 이는 '책임을 수반하는 경우'로 분류되어 처리되어야 한다.

Ⅴ. 결론 및 향후 연구방향

현행 통신비밀보호법을 포함한 관련 법체계에는 보안모니터링에 대한 규정이 포함되어 있지 않으며, 이로 인해 보안모니터링은 감청의 일부분으로 간주되고 있다.

보안모니터링은 앞서 살펴본 바와 같이 감청과 많은 차이점이 있으나, 법률상 구별이 되어 있지 않기 때문에 자칫 근본적인 의도와 달리 사용될 가능성을 내포하고 있다.

따라서 향후에는 보안모니터링이 감청과 구분되어 있지 않기 때문에 발생할 수 있는 문제점들에 대하여 연구가 진행되어야 함과 동시에, 이 문제점들을 해결할 수 있는 방안에 대한 연구도 진행되어야 할 것이다.

참 고 문 헌

[1] 권영철, 도청의 헌법상 문제, 고시계 82.7, 29-36면
[2] 오영근/박미숙, 위법수집증거배제법칙에 관한 연구, 한국형사정책연구원, 1995, 103면
[3] Berger v. New York, 388U.S, 41 AT71 (1967)
[4] 원혜욱, "도청·감청 및 비밀녹음(녹화)의 제한과 증거사용," *한국형사정책연구원*, 2000년, 32면

홍 창 화 (洪昌和)

2005년 2월 : 국방대학교 정보보호관리전공(석사)
2009년 2월 : 고려대학교 정보보호대학원(박사)
2008년 11월~현재 : 산성공사
관심분야 : 보안평가 및 승인, 보안수준관리, 암호, 키관리시스템

최 민 규 (崔閔圭)

2009년 2월 : 한남대학교 멀티미디어학과(공학사)
2009년 3월 : 한남대학교 멀티미디어학과 석사과정
관심분야 : 정보보증, 보안성평가

김 태 훈 (金泰勳)

1995년 2월 : 성균관대학교 전기공학과(공학사)
1997년 2월 : 성균관대학교 전기공학과(공학석사)
2002년 2월 : 성균관대학교 전기전자컴퓨터학과(공학박사)
2007년 3월~현재 : 한남대학교 멀티미디어학부 조교수
관심분야 : 대형시스템보안, 정보보증, 보안성평가