JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 24 No. 11, pp. 99-107, November 2019
https://doi.org/10.9708/jksci.2019.24.11.099

The Integrated Cyber SRM(Security Risk Monitoring) System Based on the Patterns of Cyber Security Charts

Gang-Soo Lee*, Hyun Mi Jung**

*Professor, Dept. of Computer Engineering, Hannam University, Daejeon, Korea
**Researcher, Center for Development of Supercomputing System, KISTI, Daejeon, Korea

[Abstract]

The "Risk management" and "Security monitoring" activities for cyber security are deeply correlated in that they prepare for future security threats and minimize security incidents. In addition, it is effective to apply a pattern model that visually demonstrates to an administrator the threat to that information asset in both the risk management and the security system areas. Validated pattern models have long-standing "control chart" models in the traditional quality control sector, but lack the use of information systems in cyber risk management and security systems. In this paper, a cyber Security Risk Monitoring (SRM) system that integrates risk management and a security system was designed. The SRM presents a strategy for applying 'security control' using the pattern of 'control charts'. The security measures were integrated with the existing set of standardized security measures, ISMS, NIST SP 800-53 and CC. Using this information, we analyzed the warning trends of the cyber crisis in Korea for four years from 2014 to 2018 and this enables us to establish more flexible security measures in the future.

▸ **Key words**: Security risk monitoring, Control chart, Security Control, Cyber security chart, Security measure

[요 약]

사이버 보안을 위한 활동인 '위험관리(Risk management)'와 '보안관제(security monitoring)' 업무는 미래에 발생할 보안 위협에 대비하고 보안 사고를 최소화 하는 활동이라는 점에서 깊은 상관관계를 가지고 있다. 또한 위험관리와 보안관제 분야 모두 관리자에게 시각적으로 그 정보자산에 대한 위협을 보여주는 패턴 모델을 적용하는 것이 효과적이다. 검증받은 패턴모델로는 전통적인 품질관리 분야에서 오랫동안 사용되어온 '관리도'(control chart)모델이 존재하지만 정보시스템의 사이버 위험관리와 보안관제에서의 활용은 부족하다. 이에 본 논문에서는 위험관리와 보안관제 시스템을 통합한 사이버 SRM(Security Risk Monitoring)시스템을 설계하였다. SRM은 '관리도'의 패턴을 이용한 '보안대책' (security control)의 적용 전략을 제시한다. 보안대책은 기존의 표준화된 보안대책 집합인 ISMS, NIST SP 800-53, CC를 통합적으로 적용하였다. 이를 활용하여 2014~2018년 까지 4년간 우리나라사이버위기 경보동향을 분석하였고 이는 향후 보다 유연한 보안대책 수립을 가능하게 한다.

▸ **주제어**: 관리도(컨트롤챠트), 위험관리, 보안관제(monitoring), 보안관리도 패턴, 보안대책

• First Author: Gang-Soo Lee, Corresponding Author: Gang-Soo Lee
*Gang-Soo Lee (leegangsoo1@gmail.com) Dept. of Computer Engineering, Hannam University
**Hyun Mi Jung (hmjung@kisti.re.kr) Center for Development of Supercomputing System, KISTI
• Received: 2019. 09. 23, Revised: 2019. 10. 29, Accepted: 2019. 10. 29.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

측정할 수 있는 것만 관리할 수 있으므로, 정보시스템의 '사이버 보안관리'를 위해서는 현재와 미래의 보안성을 측정 및 예측해야만 최적적인 '보안관리'가 가능하다. 보안성을 측정하는 활동을 사이버 '위험평가'라 할 수 있고 정보시스템의 개발 및 운영 시 필수적인 활동이다. 위험평가의 결과에 따라서 '위험관리'가 이루어지며 적정수준으로 정보시스템 내의 '보안대책' (또는 보안통제, 보안기능)을 수립, 구현 및 운영한다. 특히, 운영 중인 정보시스템의 보안성을 강화하기 위한 활동인 '정보보안관리 시스템 (ISMS: Information Security Management System)'은 관리적, 물리적 및 기술적 보안대책들을 포함한다. 위험관리와 ISMS는 관점만 다를 뿐 유사한 개념이다. ISMS의 처음단계는 위험평가이며 운영 중 '보안관제 (SM: Security Monitoring)' 활동도 포함한다. 위험평가 보안 관제를 위해서는 정보시스템의 보안수준을 측정하고 운영프로파일을 나타나는 통신 트래픽 등을 측정해야한다. 또한, 측정결과는 수치로 보이는 것보다는 관리자 또는 모니터에게 도형이나 그래프같이 시각적인 효과로 보여주는 것이 훨씬 효과적이다. 이에, 대부분의 보안관리 및 보안관제 시스템에서는 각종 그래프를 통해 현재의 상황을 보여준다. 이는 전통적인 품질관리에서 오랫동안 사용된 '관리도'는 이들 중 하나이다.

그러나 정보시스템의 사이버 위험관리와 보안관제에서 관리도 모델을 활용한 예는 부족하다.

위와 같은 문제를 해결하기 위해 본 논문에서는 위험평가와 보안관제 관점에서 관리도(control chart) 모델인 '사이버 위험관리도 (CRCC: Cyber Risk Control Chart)' 모델을 제시하고 두 가지를 통합한 사이버보안 '보안 위험관제' (SRM: Security Risk Monitoring) 시스템을 제시한다. CRCC의 편집기를 구현하는 것은 아니며 SRM 분야에서 고전적인 관리도의 '패턴'을 활용할 수 있음을 보이고자 한다. 연구의 결과는 새로운 SRM 시스템 개발에 활용할 수 있을 것이다.

본 논문의 2장에서는 관리도, 위험관리 및 보안관제에 대한 기초 연구결과를 기술한다. 이를 통해, 위험관리와 보안관제 업무를 통합할 수 있고 CRCC 모델이 SRM 시스템에서 활용될 수 있음을 보인다. 3장에서는 사이버 위험관리와 보안관제기능을 통합한 통합형 SRM 시스템을 설계하고 SRM 시스템에 CRCC 패턴을 활용하는 방법을 설명한다. 또한 이를 활용할 수 있는 사례로 한국의 국정원 사이버위기경보 동향 (2014년 ~ 2018년)을 바탕으로 제안된 방법들의 사용 가능성을 보인다. 4장에서는 결론을 맺는다.

II. Related works

2.1 Overview of Control Chart

관리도는 1920년대에 Walter A. Shewhart 박사가 개발한 오랜 모델이며 통계적 품질관리, 제어, 관리, 경영, 자산관리, 품질관리 등 다양한 분야에서 활용되고 있는 모델이다[1, 2, 3, 4]. 관리도는 런챠트나 시계열[5]과 함께 사용되어 왔다. 이들은 공정(예; 정보시스템의 운영)의 안정성(예컨대, 보안성) 여부를 시간 축 상의 점(선)의 패턴을 통해 분석할 때 사용한다. '관리도'는 공정(예; 정보시스템의 운영)의 품질(예컨대, 보안성) 수준의 변동을 관리하여 공정에 이상(예컨대, 보안사건) 요인의 유무를 조사하기 위한 관리 한계선(관리상한, 관리하한)이 있는 그래프이다. 여기서, '관리 한계선'은 품질 특성 값의 평균과 표준편차로 결정되며, 추정 값을 사용하기도 한다. 공정에 이상 요인의 유무는 공정에서 추출된 부분군에서 얻어진 통계량(즉, 측정값)과 그들의 패턴에 의해 결정한다. 관리상태 하에 있지 않은 경우, 공정에 이상요인이 존재하는 것으로 간주하여 이상요인을 조사 및 제거한다. '런차트'는 패턴으로부터 자료의 랜덤 유무를 판단하여 추세나 군집 등을 통계적 분석한다. '시계열'은 단순히 추세 등을 확인하는 그래프이다. 런챠트나 시계열은 관리도의 특수한 경우(즉, 측정값을 그대로 이용할 때)라 할 수 있으므로, 본 연구에서는 관리도로 통일한다.

관리도는 100년의 역사를 가진 모델이므로, 지원패키지 등 지원 환경이 우수하며 특히 MINITAB은 가장 널리 사용되는 도구이다[2]. [표 1]은 MINITAB에서 지원하는 관리도의 종류를 보인다[2]. 관리도는 최근에는 정보보안 분야에도 활용되고 있고[6, 7, 8] 통신 트래픽의 가시화에도 활용되었다. 패킷 전체/그룹별 평균크기와 편차, 시간당 패킷오류수, 패킷오류 발생간시간, 오류율을 가시화한다[8]. 또한, 정보시스템의 응용수준의 성능평가를 위해 트랜잭션 전체/그룹별 '트랜잭션' 평균시간과 편차 등을 가시화할 수 있다.

보안 위험관리나 보안관제시에도 활용할 수 있으며 다음 사항들을 감시할 수 있을 것이다.

- 조직 전체/그룹별 '보안사건' 발생시간, 발생간시간, 발생건수, 발생율
- 시스템 전체/그룹별 '보안결함(취약성)' 비율, 결함수, 결함발생간시간, 결함율
- 시스템 보안 도메인전체/도메인별 '보안수준'의 목표대비 값, 절대값, 평균, 편차
- 2개 이상의 보안변수(예: 취약성수준, 위협수준, 자산가치 등)를 동시에 관제

Table 1. Examples of control chart types and security areas supported by MINITAB

관리도그룹	관리도	보안위험관제에 이용 예시
그룹별 계량형	Xbar-R (평균-범위)	• 소그룹별 패킷크기, 소그룹별 트랜잭션시간, 소도메인별 보안수준 • 예: 20시간 동안 매시간 단위 5개를 표본으로 추출하여 보안 강도를 감시
	Xbar-S (평균-편차)	• 대그룹별 패킷 평균크기와 편차, 대그룹별 트랜잭션 평균시간과 편차, 소 도메인별 보안수준(평균과 편차) • 예: 30시간 동안 매시간 패킷 10개로 구성된 그룹을 수집
	I-MR-R/S (부분군 평균-평균의 이동범위- 표본범위)	• 그룹별 패킷크기, 그룹별 트랜잭션시간, 도메인별 보안수준 • 예: 15개 도메인 3개 지점에서 보안수준을 측정
	Xbar (평균)	• 도메인별 보안수준 (평균값 이용)
	R (범위)	• 도메인별 보안수준 (범위 값 이용) • 예: 일정 시간 동안 매시간 보안제품 5개로 구성된 그룹을 추출하여 보안강도를 감시
	S (편차)	• 도메인별 보안수준 (편차 값 이용) • 예: 일정 시간 동안 매시간 도메인 10개로 구성된 도메인을 수집하고 보안수준 변동을 감시
	구역 (시그마구간 및 누적점수)	• 도메인별 보안수준 • 예: 4일 동안 3 교대 조 각각으로부터 10개의 보안도메인 표본으로 추출
개별값 계량형	I-MR (개별값-이동범위)	• 보안복구시간 • 예: 복구시간의 안정성 감시
	Z-MR (개별관측치-이동범위)	• 침투시험을 통한 보안강도 측정 • 예: 보안시험에서 각각 8회의 런을 사용하여 3회 런에서만 측정값 통해 보안강도의 평균과 변동을 감시
	I (개체, 개별값)	• 보안복구시간 • 예: 복구시간의 안정성 감시
	MR (이동범위)	• 보안복구시간 • 예: 수술 시간의 안정성 감시
계수형	P관리도 진단 (불량율)	• 취약성율, 전체 패킷 오류 관제 • 예: 데이터에 과대산포가 있는지 감시. 예컨대 관측된 변동과 기대 변동의 비율은 175.7%이며 이 값은 신뢰 상한 136.6%보다 크기 때문에 과대산포를 나타냄
	P (불량율)	• 보안결함(취약성)율, 전체 패킷 오류 관제 • 예: 결함 율을 두 달 동안 매일 모니터링
	Laney P′ (불량율)	• 보안 결함 율, 전체 패킷 오류 관제 • 예: 보안검사 시 오류로 인해 재검을 받아야 하는 장비의 비율을 감시
	NP (부분군당 불량수)	• 보안결함 개수, 전체 패킷 오류 관제 • 예: 보안장비의 보안결함 비율 달 동안 매일 감시
	U 관리도 진단	• 보안결함 개수, 전체 패킷 오류 관제 • 예: 대량이며 과대산포인 패킷의 오류수를 감시
	U (단위당 결점수)	• 취약성개수, 패킷그룹별 패킷오류 관제 • 예: 패킷 그룹별 평균 손상 패킷오류 감시
	Laney U′	• 전체 패킷 오류 관제 • 예: 대량이며 과대산포인 패킷의 오류수를 감시
	C (부분군당 결점수)	• 패킷 그룹별 손상 패킷 수 관제 • 예: 패킷 그룹별 평균 손상 패킷오류 감시
시간 가중	MA (이동평균)	• 보안도메인별 보안성 관제 • 예: 일정 시간 동안 보안도메인으로부터 보안성 변동을 감시
	EWMA (지수가중이동평균)	• 전체 보안도메인의 보안수준관제(절대 값) • 예: 보안도메인의 보안도메인 감시
	CUSUM (누적합)	• 보안도메인별 보안수준(목표대비 값)
다변량	T^2-일반화분산 (T^2-일반화분산)	• 2개 이상의 보안변수를 동시에 관제 • 예: 공격자 능력, 공격시간, 자산 가치 등 2개 이상의 보안변수를 동시에 감시
	T^2 (편차의 크기)	• 2개 이상의 보안변수를 동시에 관제 • 예: 공격자 능력, 공격시간, 자산 가치 등2개 이상의 보안변수를 동시에 감시
	EWMA (다변량 지수가중이동평균)	• 2개 이상의 보안변수를 동시에 관제 • 예: 공격자 능력, 공격시간, 자산 가치 등 2개 이상의 보안변수를 동시에 감시
	일반화 분산	• 2개 이상의 보안변수를 동시에 관제 • 예: 공격자 능력, 공격시간, 자산 가치 등 2개 이상의 보안변수를 동시에 감시
회귀 사건	G (사건발생간 수)	• 보안사건수 관제 • 예: 보안사건수를 감시
	T (사건발생간 기간)	• 보안사건간 간격 관제 • 예: 보안사건 날짜와 시간을 통해, T 관리도를 사용하여 보안사건 발생간시간을 감시

2.2 Risk Management, Security Control and Security Management Standard Process

위험관리, 보안관제 및 보안 관리는 관점만 다를 뿐 동일한 개념이다. 일반적으로, 위험관리 활동의 일부인 '위험평가'는 정보시스템의 개발 초기단계에서 정보시스템의 '보안기능요구사항'(즉, 보호프로파일 또는 보안목표 명세서) 도출을 위해, 예상되는 개발 프로세스 및 운영 환경(즉, 운영프로파일)을 분석할 때 실시한다. 위험평가를 통해 정보시스템의 최적의 개발 및 운영 보안 수준을 결정하여 '보안공학'에서 추구하는 과잉보호 문제를 예방한다. 개발된 정보시스템을 운영할 때 '위험관리'를 위해 주기적 또는 필요시에 위험평가를 실시한다. 즉, 보안수준을 파악하고 보안 문제가 발생하면 대응책을 실시한다. 인간의 정기 및 비정기 건강진단(위험평가)과 건강관리(위험관리)에 비유된다. '보안관제'와 '보안관리'는 주로 운영 중에 정보시스템을 대상으로 하는 위험평가 및 위험관리 활동에 해당한다. 다음은 위험관리, 보안관제 및 보안관리 활동을 위한 표준을 보인다. 특히, 보안 관리는 공정이나 절차가 아니라 보안대책(또는, 기능, 통제) 목록을 정의한 것이다.

- 위험관리: 800-30-R1 (위험평가 수행지침)[9], 800-37-R2 (위험관리 골격) [10,11], 800-39 정보보안 위험관리)[12], 800-53-R5 (3.17절 위험평가) [13]
- 보안관제: 800-137 (정보보안 연속 관제)[14], SP 800-53-R5 (CA-7 지속적관제, SI-4 시스템관제, IR-5 사고관제, PE-6 물리적 접근관제, PE-20 자산관제 및 추적, RA-5 취약점스캐닝) [13]
- 보안관리: CC[15], ISMS[16,17], SP 800-53[13], TRM 2.3 [18]

일반적으로, '위험평가'는 순차적 (인터리빙)이며 평가 중에는 본 평가대상 시스템은 정지하지만(사이클 스틸링), '관제'는 인터럽트('불수의적', '반사적') 방법으로 처리한다. 즉, 운영 중 보안사건 인터럽트(트리거 개념)가 발생하면, 인터럽트 핸들러(즉, 보안통제, 대응)가 작동하여 자동적(반사적)으로 보안대책을 수행한다.

III. The Proposed Scheme

3.1 Security control chart and Design of the integrated security risk control process

3.1.1 Security management chart

관리도를 사이버보안 위험관리나 보안관제에 사용할 때 보안관리도라 한다. 보안관련 자료인 '보안사건'의 발생시간/발생간시간/발생건수/발생율, '보안결함(취약성)'의 비율/결함수/결함발생간시간/결함율, '위험수준'의 목표대비값/절대값/평균/편차 값을 이용하여 보안관련 분석을 수행한다. 예컨대, 위험수준의 변동과 동향을 시각화하고 유사한 동향을 그룹화(즉, 패턴화)하여 패턴별 보안대책을 수립하기 위해 사용한다.

3.1.2 The integrated Risk Control Process

본 연구에서는 기존의 위험관리와 보안관제 표준들의 프로세스를 통합한 'SRM-프로세스' 모델을 제시하였다. 이는 [표 2]와 같이 위험관제 프로세스는 반복 및 진화적 나선형 PDCA (Plan-Do-Check-Action)모델이다.

① 위험평가정책 수립 단계: 정보시스템 운영의 이전단계에서 위험평가를 준비한다. 위험평가의 '목적'을 정하고 평가 범위를 축소하기 위해 '가정'을 세운다. 위험에 대한 '대책'을 세우기 위한 정책을 수립한다. 정책에는 대책의 구현 '우선순위'를 포함한다. '보안대책 Plan'에 해당한다.

② 보안대책 구현 단계: 정보시스템 내에 보안대책을 '구현'한다. 필요시에, 구현된 보안대책에 대해 '인가'(사용승인)를 받는다. '보안대책 Do'에 해당한다.

③ 시스템 운영 단계: 구현 및 인가된 보안대책을 시스템에 적용한다. '보안대책 Do'에 해당한다.

④ 정기적 위험평가 단계 (취약성 및 수준 평가) : 보안대책이 포함되고 운영 중인 정보시스템에 대해 정기적인 위험 평가를 실시한다. 시스템의 구조와 운영프로파일로부터 시스템내의 보호대상 '자산 평가', 자산에 가해지는 '위협평가', 보안대책상의 '취약성평가'를 통해 전체 '위험수준'을 평가한다. '위험평가 Check'에 해당한다.

⑤ 보안문제 대응 단계 (취약성제거) : 위험평가 결과를 바탕으로 보안문제에 대응한다. 즉, 발견된 취약성을 제거하여 보안성을 강화한다. '보안대책 개선 Action'에 해당한다.

⑥ 상시관제(감시) 단계: 관제는 운영 중인 시스템에 위험(공격탐지, 취약성발견)을 실시간 탐지하여 공격을 방어하거나 취약성을 제거한다. '수시적' 위험평가라 볼 수 있다. '보안대책 개선 Action'에 해당한다.

3.2 The design of integrated security risk control system

3.2.1 SRM-system structure based on security management chart

'SRM-시스템'은 3장에서 제시한 SRM-프로세스를 지원하는 시스템이다. <그림 1>은 본 연구에서 제시하는 '관리도기반의 SRM-시스템'의 구조를 보인다. SRM 대상물은 위험관리와

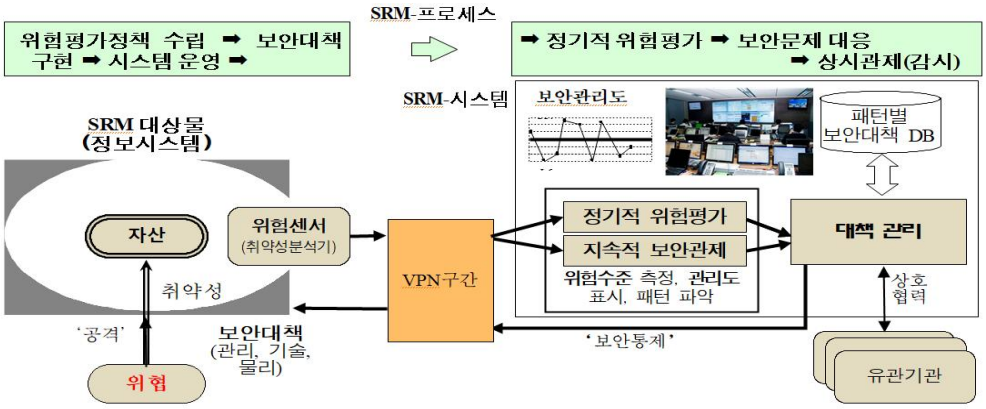


Fig. 1. Security management chart based SRM-system

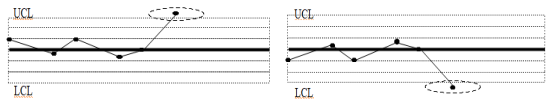
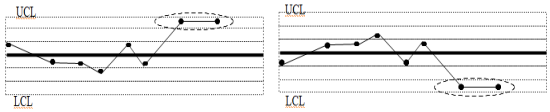
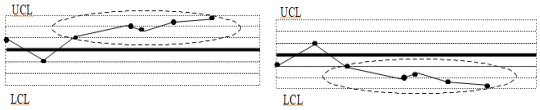
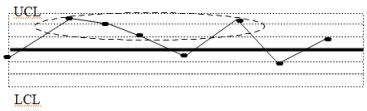
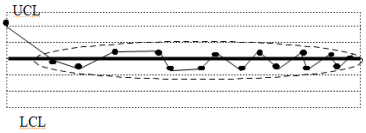
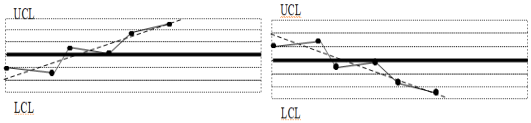
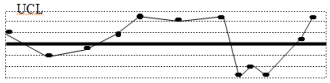
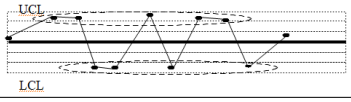
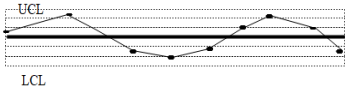
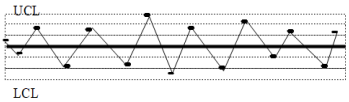
Table 2. Stage Comparison of Risk Management and Security Control and SRM-Process Model

부문	표준	운영 이전			운영중			
위험 관리	800-30-R1 : 평가관점	평가준비 (목적➡ 영역➡ 가정/제약➡ 정보원➡ 정보모델과 분석적 접근)			평가실시 (위협원➡ 위협사건➡ 취약성/선행조건➡ 가능성 결정➡ 영향결정➡ 위험결정	평가결과 통신과 공유 (평가결과 통신 ➡ 위험정보 공유		평가유지 (위험요인 감시➡ 위협평가 갱신)
	800-39	위험구성(framing) (가정; 억제; 감래; 우선순위/절충)			위험평가 (위협/취약성 식별; 위험결정	위험대응 (위험대응식별; 대안평가; 위험대응 결정; 위험대응 구현		위험감시 (위험감시전략; 위험감시)
	800-53-R5 (3.17 위험평가)	위험평가 정책과 절차 ➡ 보안분류			위험평가 ➡ 위험평가갱신 ➡취약성 스캐닝	기술적 감독 대비책 조사 ➡위험 대응		프라이버시 영향평가 ➡ 심각성분석
	800-37-R2 (RMF): 대책(보안기능) 관점	대책분류	대책 선택	대책구현 ➡ 대책 인가	대책 평가	감시 (=관제)		
보안 관제	800-137 (보안관제)	전략정의	설립	구현	분석	대응		검토및갱신
	800-37-R2 (보안관제)	시스템 및 환경 변경			지속적 평가	권한부여 갱신	보안 및 개인정보 보호 상황 보고	지속적 권한부여 ➡ 시스템 파기
	관제일반	예방			탐지	분석	대응	
SRM-프로세스		① 위험평가정책수립	② 보안대책구현	③ 운영	④ 정기적 위험평가 (취약성 및 수준 평가)		⑤ 대응 (취약성제거)	⑥ 상시관제 (감시)
경영사이클(PDCA)		Plan	Do		Check		Action	

관제가 필요한 정보시스템이며, 그 내부에 보호해야할 가치 있는 '자산'을 포함하고 있다. 공격자(또는, 위협, threat)는 자산의 가치를 얻기 위해 '공격'(attack)하므로, 정보시스템의 소유자는 각종 보안통제(또는, 보안기능, 보안제품)를 통해 이를 방어하고 있다. 그러나, 보안통제에는 보안 '취약점(vulnerability)'이 있으므로, 공격자는 취약점을 악용(exploit)하여 자산을 공격(접근)하려한다. 시스템내의 위험센서(취약성분석기, 침입탐지시스템 등)는 취약점과 공격을 탐지하여 결과를 'SRM-시스템'에게 보낸다. SRM-시스템은 위험 '센서'로부터의 결과를 시각화, 정량화하여 관리패턴을 구하고 미리 저장된 '패턴별 통제규칙 DB'를 활용하여 보안통제를 실시한다. 이 경우, '보안통제'는 '엑츄에이터'(actuator)의 역할을 한다. 보안위험관제시스템 유관기관(보안 관제센터 등)과 정보를 공유한다. 과거에는 정보시스템 내부에 '방어' 기능(보안기능)과 '탐지(관제)' 기능이 있었지만, 현대는 정보 시스템 내에는 '탐지 센서'를 설치하고 SRM-시스템에서 원격으로 여러 정보시스템을 통합하여 위험관리, 보안관제 및 보안 관리를 함으로 노하우를 습득하고 경제성이 높아진다. <그림 1>은 보안관도 기반의 SRM 시스템의 구성도이다.

- SRM 대상물: Target of security risk monitoring (ToSRM)

Table 3. security chart patterns for information security risk control

패턴명	패턴 시그니쳐 UCL(Upper Control Level): 관리상한 수준(예: 위험등급 5단계) LCL(Lower Control Level): 관리하한 수준(예: 위험등급 1단계)	보안대책 전략 ([표4]참조)
PT1.이탈: 관리한계 상/하		- 긴급 '복구'형 보안통제 (차단, 우회, 조사, 백업 등) 실시 - '심각' 수준의 대책 - 관계기관에 즉시 통보 - 국가적 차원에서 공동 대처
PT2.근접: 관리한계 2점		- '탐지'형 보안통제 실시 - '경계' 수준의 대책 - 민.관 각 분야의 협조 및 공동 대응
PT3.이동: 중심선(5, 7, 8, 9점) 연속 상/하		- '회피'형 보안통제 실시 - '주의' 수준의 대책 - ISP/IDC, 일반 사용자, 기업 등의 긴급 대응 및 보안 태세강화
PT4.돌출: 동일구역 5점중 4점		- '예방'형 보안통제 실시 - '관심' 수준의 대책
PT5.층화: 동일구역 15점 연속		- '예방'형 보안통제 실시 - '관심' 수준의 대책
PT6.경향: 증가/감소 추세 (6점)		- '회피'형 보안통제 실시 - '경계' 수준의 대책 - 민.관 각 분야의 협조 및 공동 대응
PT7.특이한 변화		- '회피'형 보안통제 실시 - '관심' 수준의 대책
PT8.진동: 급격한 변화 (14점)		- '회피'형 보안통제 실시 - '주의' 수준의 대책 - ISP/IDC, 일반 사용자, 기업 등의 긴급 대응 및 보안 태세강화
PT9.동일구역 8점연속		- '예방'형 보안통제 실시 - '관심' 수준의 대책
PT10.주기성		- '회피'형 보안통제 실시 - '관심' 수준의 대책 - 주기의 특성 파악 - 주기별(상승, 하강) 대책
PT11.안정상태(관리 상태): 25개점이 특이사항 없음		- '예방'형 보안통제 실시 - '정상' 수준의 대책

- 자산: 공격 대상 (시스템, 자료, 서비스, 인적자원 등)
- 위험센서: 취약성분석기, 로그분석기, 침입 탐지기 등
- 취약성: 보안통제에 내재된 악용 가능한(exploitable) 취약점 (물리적 취약성, 논리적 취약성, 운영 취약성, 고유 취약성 등)
- 위협/위협원: 위협원 (공격자, 사용자, 운영자, 자연재해 등)에 의한 의도적 또는 비의도적 자산 접근 및 무결성/가용성/기밀성 파괴 행동
- 공격: 위협원의 행동이며 '공격시나리오'를 통해 표현
- 보안대책(통제, 기능, 제품):CC내의 보안기능, ISMS내의 보안대책, SP 800-53 내의 물리적, 관리적, 기술적 보안통제 또는 보안통제들이 포함된 정보보호제품(IPS, VPN, FW 등). 보안통제에는 항상 취약성이 존재
- 위험관리/보안관제: 패턴별 통제규칙을 적용하도록 정보시스템에 지시, 전략 (통제) (SP 800-53, ISMS, CC에서 선택)

Table 4. Security strategy

MTP관점 / PADR관점		관리적	기술적	물리적	우리나라 사이버위기경보 수준별 패턴의 연관
예방적		**PT1, PT4, PT9, PT11**			주의: PT9 관심: PT4, PT 5 정상: PT11
		의식/훈련, 감사/책임성, 비상계획, 계획, 인사보안, 정보보호 정책, 정보보호 조직, 정보자산 분류, 준거성, 일반 통제, 자원 활용	식별/인증, 시스템/통신 보호, 시스템/정보 무결성, 암호통제, 시스템개발 보안, 정보보호 대책 구현, 시스템 및 서비스 보안관리, 응용시스템 보안, 데이터 보안, 타임스탬프, 프라이버시, TSF 보호	접근통제(물리적), 매체보안, 물리적/환경적 보안, 물리적 보안, TOE 접근	
회피적		**PT3, PT6, PT7, PT8, PT10**		-	경계: PT6 주의: PT3, PT8 관심: PT7, PT10
		운영보안, 형상관리,	유지보수	-	
탐지적 (분석)		**PT2**		-	경계: PT2
		보안평가/인가, 위험평가	접근통제	-	
대응적 (복구)		**PT1**			심각: PT1
		침해사고 관리, 사후관리	IT재해 복구	사고대응, 백업 및 자료보관	
근거	800-53	의식/훈련, 감사/책임성, 보안평가/인가, 위험평가, 형상관리, 비상계획, 계획, 인사보안	식별/인증, 유지보수, 시스템/통신 보호, 시스템/정보 무결성	접근통제, 사고대응, 매체보안, 물리적/환경적 보안	
	ISMS (17799)	정보보호 교육, 정보보호 정책, 인적보안, 외부자 보안, 위험관리, 운영보안, 정보보호 조직, 정보자산 분류, 경영진 책임 및 조직구성, 침해사고 관리	암호통제, 시스템개발 보안, 정보보호 대책 구현, 사후관리, IT 재해 복구, 접근통제,	물리적 보안	
	ISMS (한국)	관리체계 기반 마련, 위험 관리, 관리체계 운영, 관리체계 점검 및 개선, 정책/조직/자산 관리, 인적보안, 외부자 보안, 사고 예방 및 대응	인증 및 권한관리, 접근통제, 암호화 적용, 정보시스템 도입 및 개발 보안, 시스템 및 서비스 보안관리, 재해복구	물리적 보안	
	TRM 2.3	보안정책 및 지침, 보안조직 구성 및 운영, 보안 운영 관리, 준거성, 일반 통제	응용시스템 보안, 네트워크 보안, 시스템 보안, 사용자 인증 및 권한 관리, 암호화 기술, 데이터 보안	접근통제, 방재 및 내부설비, 시스템 시설보호, 백업 및 자료보관, 물리적 재해 대책	
	CC	보안감사, 보안 관리, 자원 활용	사용자 데이터 보호, 암호지원, 식별 및 인증, 통신, 안전한 경로/채널, 타임스탬프, 프라이버시, TSF 보호	TOE 접근	

- 위험수준측정, 관리도 표시, 패턴 파악: 정보시스템내의 위험 센서로 부터 패턴을 파악 (관리도 등을 이용)
- 패턴별 보안대책 DB: 각종 위험 패턴(프로파일) 및 대책이 저장
- 위험수준: 자산 가치(피해 영향)와 공격가능성의 함수
- 유관기관: CERT 팀, 타 보안 관제센터 등

3.2.2 Database for Pattern-Specific Security Countermeasures Rules

(1) 보안관리도 패턴

본 연구에서는 [표 3]과 같이 기존의 연구결과[1, 2, 3, 4, 19]들을 참고하여 정보보안 위험관제를 위한 11개의 보안관리도 패턴을 도출하였고 각 패턴을 위한 보안대책을 제시하였다. 본 연구에서는 11개의 패턴을 제시했지만 SRM을 적용하는 조직의 보안정책에 따라 패턴을 추가할 수 있을 것이다.

(2) 보안관리도 패턴별 보안대책

보안대책 관련 표준 (예: NIST SP 800-53, ISMS, ISMS (한국), TRM 2.3, CC)이나 관점에 따라 보안대책(또는, 보안기능, 보안통제)의 분류체계가 다르므로, 본 연구에서는 이들을 통합한 '통합형 보안대책 분류체계'를 제시하였다. 또한, 기존의 보안대책들을 전통적인 MPT(관리-물리-기술) 관점뿐 아니라, 관제의 기본 단계인 PADR (예방-회피-탐지-대응) 관점으로 분류하였다. [표 4]는 본 연구에서 제시한 패턴별 보안대책 전략([표 3]의 내용 확장)을 보인다. [표 4]의 하단부분은 기존의 표준에서의 보안대책을 분류한 것이다. 또한, [표 4]의 가장 오른쪽 열은 국가정보원의 사이버위기경보 수준(즉, 정상, 관심, 주의, 경계, 심각)별 연관 결과를 보인다[20].

- PADR (예방-회피-탐지-대응) 관점의 각 단계는 다음과 같다.

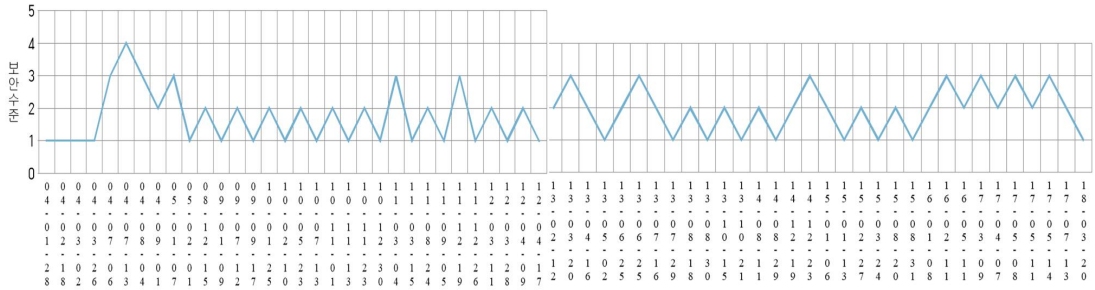


Fig. 2. Security chart of Korea's cyber crisis level(2004 ~ 2018)

- 예방(prevention) : 보호대상 자원(즉, 중요 시스템, 네트워크 및 홈페이지)에 대한 보안기능(즉, 관리적, 물리적, 기술적)을 수행하고, 보안기능 내부 및 운영상의 '취약점'을 사전에 파악하여 침해 사고를 예방.
- 회피(avoidance) : 식별된 취약점이 공격자에게 탐지 및 악용되지 않도록 함 (제로 데이 공격 방지).
- 탐지(detection)와 분석 : 보안 시스템의 보안 이벤트에 대한 24시간×365일 보안 전문 인력에 의한 실시간 감시 탐지. 분석에서는 보안 시스템 로그, 네트워크 패킷 및 다양한 보안 이벤트 등을 종합적으로 상관 분석하여 재발 방지 및 확산을 방지하기 위한 방안을 강구.
- 대응(respond) 및 복구(recovery): 비정상 네트워크 및 시스템에 대한 초기 대응, 사이버 공격 발생 시 신속히 조치 대응하는 것을 의미. 복구는 피해복구, 원인조사, 재발방지

3.3 Case Study: National Intelligence Service Cyber Crisis Alert Trends: 2014 to 2018

국가정보원은 2014년부터 2018년까지 사이버위기경보를 발령하고 있다. 경보단계는 정상단계 (1등급), 2등급(관심), 3등급(주의), 4등급(경계), 5등급(심각)으로 경보하고 있다 [20]. <그림 2>는 지난 4년간 사이버위기 수준의 관리도를 보인다. 이 관리도는 [표 1]에 따르면 '개별값계량형' 중 ' I (개체, 개별값)' 또는 ' Z-MR(개별관측치-이동범위)'에 해당한다. 2004년7월 6일부터 8월 4일동안 3, 4등급이었고 2017년 1월 8일부터 7월 13일 동안은 2등급과 3등급을 반복하고 있다. 보안관리도(또는 시계열)를 이용하면 보안수준의 동향(패턴)을 파악할 수 있고 이에 따른 보안대책 강구할 때 활용한다.

- 05년 1월부터 12년 4월까지는 **PT11**(안정 상태)를 유지하고 있고 '예방적'인 보안대책 (즉, 의식/훈련, 감사/책임성, 비상계획, 계획, 인사보안, 정보보호 정책, 정보보호 조직, 정보자산 분류, 준거성, 일반 통제, 자원 활용, 식별/인증, 시스템/통신 보호, 시스템/정보 무결성, 암호통제, 시스템개발 보안, 정보보호 대책 구현, 시스템 및 서비스 보안관리, 응용시스템 보안, 데이터 보안, 타임스탬프, 프라이버시, TSF 보호, 접근통제(물리적), 매체보안, 물리적/환경적 보안, 물리적 보안, TOE 접근)을 운영한다.
- 16년 1월부터 17년 7월까지 **PT3**(이동: 중심선 (5, 7, 8, 9점) 연속 상향) 패턴을 보이고 있다. 이 경우 표4에서처럼 '회피적'인 보안대책 (즉, '운영보안', ' 형상관리', '유지보수')을 세우고 주의 상태를 유지한다.

3.4 Analysis and Evaluation

본 논문에서는 미국 NIST의 SP 800-30, SP 800-39, SP 800-53, SP 800-37, SP 800-137과 같은 기존의 보안 위험관리와 보안관제(모니터링) 프로세스의 중복성을 줄이고 통합한 SRM-프로세스 및 SRM-시스템을 제시하였다. 기존 보안 분야에서 관리도를 이용하는 연구들은 주로 이상 징후 탐지 방법을 제시하고 있지만, 본 연구는 보안관리도와 관리도 패턴을 이용하여 보안대책을 수립하는데 적용하였다.

본 논문과 기존 연구와의 차별화된 연구내용은 다음과 같다.

첫째로 11가지 '보안관리도 패턴'을 제시하였다. 소프트웨어 패턴을 이용한 소프트웨어개발처럼 보안 관리에 '패턴'의 개념을 활용하여 보안대책을 세우도록 하였다.

두 번째로 '패턴별 보안대책'을 제시하였다. SRM에서 위험 관리도 '패턴'(주식의 동향과 유사)을 적용하여 패턴별 보안대책을 권고한다.

세 번째로 통합적 보안대책 분류하였다. NIST SP 800-53, ISMS, 한국 ISMS, 한국 TRM 2.3, CC를 통합하고 전통적인 MPT(관리-물리-기술) 관점뿐 아니라, 경영사이클인 PDCA(계획-실시-체크-액션) 관점 및 관제의 기본 단계인 PADR (예방-회피-탐지-대응)을 통합하였다.

마지막으로 기존의 통신 트래픽 패턴과 본 연구의 보안관리도 패턴의 차이점이다. 기존 통신 트래픽 패턴은 통신 패킷을 측정하여 이동량을 그래프로 나타내고 트래픽의 패턴(또는 시그니쳐)를 파악하고 이에 따라 침입을 탐지하고 관리행동을 실시하지만 본 연구의 결과인 보안관리도 패턴

은 시스템의 보안수준(위험수준)을 측정하여 변화를 관리도로 나타내고 패턴에 따른 보안대책을 세우는 것이며 보안관리, 위험평가 및 보안 관제를 통합하여 활용 가능하다.

IV. Conclusions

본 연구에서는 사이버 위험관리와 보안 관제를 통합한 '사이버보안 위험관제시스템' 모델을 제시하고 보안관리도와 관리도 패턴을 적용하는 방법을 제시하였다. 관리도는 오랜 역사를 지닌 통계적 품질관리 도구 및 시계열분석을 위한 표현 모델로 사용되어 왔으며, 이를 위험관제에 이용한 보안관리도와 패턴은 사이버 위험관제시스템에서 유연한 보안전략을 수립하는데 활용할 수 있다. 보다 많은 보안관리 및 위험관리 사례로부터 다양한 보안 관리도 패턴을 도출 (아키텍쳐 패턴과 유사)하고, 패턴별 보안대책 전략을 수립하여 위험관제 업무에 적용하는 것을 향후 연구과제로 남긴다.

ACKNOWLEDGEMENT

This work was supported by 2018 Han Nam University Research Fund.

REFERENCES

[1] Hyuck Moo Kwon, Sung Hoon Hong, Min Koo Lee, Sung Uk Lim, "Literature Review on the Statistical Quality Control," J. Korean Soc. Qual. Manag., Vol. 44, No. 1, March 2016. pp.1 ~ 16.

[2] Basic Tools for Process Improvement, Module 10 CONTROL CHART. https://support.minitab.com/ko-kr/minitab/18/.

[3] Process for statistical quality control, http://ebook.pldworld.com/_ebook/품질관리/hwcg.co.kr/.../통계적품질관리_교재.ppt.

[4] Taewoong Kim, " Quality Management," Sin-yeong sa, July 2017.

[5] Time series Forecasting in Machine Learning, https://medium.com/99xtechnology/time-series-forecasting-in-machine-learning-3972f7a7a467

[6] Jin-woo Park, Seok-hoon Yun, Jin-heum Kim, Hyeong-chul Jeong, "Developing the information security risk index using network gathering data," Korean Journal of Applied Statistics, vol7 no29, pp.1173 ~ 1183, 2016.

[7] Method for anomaly detection using statistical process control, https://patentimages.storage.googleapis.com/fe/4c/4e/f46728e1a007ef/KR101281460B1.pdf, 2013.

[8] KISA Report, "A study on a Scheme of Detecting Abnormal Traffic in Internet-based Architecture," 2004.

[9] NIST SP 800-30, Rev. 1, "Guide for Conducting Risk Assessments," Sep. 2012.

[10] NIST SP 800-37, Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Life Cycle Approach," Feb. 2010.

[11] NIST SP 800-37, Rev. 2, "Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy," May 2018.

[12] NIST SP 800-39, "Managing Information Security Risk," March 2011.

[13] NIST SP 800-53, Rev. 5, "Security and Privacy Controls for Information Systems and Organizations, NIST," Aug. 2017.

[14] NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," Sept. 2011.

[15] Common Criteria ver 5.1 ,http://www.itscc.kr, 2017.

[16] Notice regarding information protection and personal information protection management system certific-ation, https://isms.kisa.or.kr/main/ispims, 2018.

[17] SMS-P_Certification Standards_Detail Check Items, https://isms.kisa.or.kr/main/ispims.2018

[18] Governmental Technology Reference Model (TRM) https://www.geap.go.kr/real/, 2014.

[19] Stock Technical Analysis, file:///C:/Users/310/AppData/Local/Microsoft/Windows/INetCache/IE/42LWML2Z/techanalysis.pdf.

[20] NIS Cyber Crisis Alert Trends: 2014 ~ 2018, https://www.nis.go.kr:4016/AF/1_7_1_1/list.do

Authors

Gang-soo Lee received the B.S. degree on Computer Science from Hong-ik University, M.S. and Ph.D. degrees in Computer Science from Seoul National University Korea, in 1981, 1983 and 1989, respectively.

Dr. Lee joined the faculty of the Department of Computer Engineering at Han Nam University, Dae-jeon, Korea, in 1987. He is currently a Dean and Professor of College of Engineering, Han Nam University. He is interested in Security Engineering, Security Evaluation. Software Engineering, Web Engineering, Petri Net application.

Hyun Mi Jung received the B.S., M.S. and Ph.D. degrees in Computer Engineering from Hannam University, Korea in 1998, 2010 and 2014. Since 2012, she has been a Researcher with the Center for Development of Supercomputing System, Korea Institute of Science and Technology Information, Korea. Her main research interests include HPC security, H/W security and security monitoring.