Asian Journal of Innovation and Policy (2015) 4.3: 307-327
DOI: http//dx.doi.org/10.7545/ajip.2015.4.3.307

Use of Patent Analysis for the Future Skills-needs in Information Security

Gyu-hee Hwang[*], In-Joong Ju, Ga-woon Ban[**], Kack-Hee Lee[***]

Abstract This study attempts to develop a methodology that analyzes patent applications to identify future skills, in particular in the sector of information security, recently into the spotlight. Matching skill elements from the International Patent Classification (IPC) with skill units from job analysis, the study tries to track trends in the skills needs based on IPC time-pattern. It then verifies the validity of the outlook for future skills needs by addressing the situation through the use of patents. The research assesses the usability of patent information for this type of analysis. While this study is limited to the information security sector by using Korean patent information, it can be expanded in the future to other areas and patents in the United States and Europe.

Keywords Patent analysis, technology forecasting, future skills needs, information security

I. Introduction

At the 2012 Seville International Conference on Future-oriented Technology Analysis (FTA), FTA was regarded as a method to better prepare for the future and/or shape it in order to achieve a favorable outcome. This study attempts to broaden the FTA to identify future skills needs, which constitutes a critical subject for education and training. It is noted that there is still no research on the future skills needs linked to FTA, including patent analysis.

In the study of future skills needs, the crucial issue is how to proceed to identify future skills needs. On that matter, this study argues that some information derived from patent data can be used in the identification of future skills needs as a measurement of future technological trends.

As for forecasting and/or anticipating future skills, conventional studies analyze or 'interpret' changes of skills needs already occurring. By contrast,

Submitted, May 26, 2015; 1st Revised, August 22; Accepted, September 14.
* Korea Research Institute for Vocational Education and Training (KRIVET), Sejong, Korea; g.hwang@krivet.re.kr
** ijju@krivet.re.kr; gwban@krivet.re.kr
*** Kuwoo Information Technology, Seoul, Korea; kaylee@kuwoo.co.kr

this study attempts to search for future skills needs directly derived from technological innovation. Conventional skills analysis focuses on labor market information. This information is useful for the analysis of the present and near future, but it has limitation on the analysis of newly emerging technology beyond information (CEDFOP, 2012; Lowery et al., 2008; Schmidt et al., 2004). This is a common limitation because conventional forecasting of workforce demand and supply is mainly focused on quantitative demand changes by industry and occupation.

The analysis of future skills needs that is required should contain tangible contents of skills needed; this analysis can be called a qualitative forecast, which is different from existing quantitative forecast on workforce demand and supply (Hwang, Coh and Lee, 2011; Hwang, Joo and Coh, 2011; Hwang and Lee, 2010). This qualitative supplement to a quantitative study can normally be altered through expert panel discussions, but it faces several challenges from the shortage of verification instruments. So, this study attempts to conduct a verifiable qualitative analysis on the specific and measurable basis of patent information. However, such analysis might be regarded as another quantitative approach or, despite the use of patent data, it might simply be called a limited quantitative approach in the interpretation and linkage carried out by experts on job and curriculum analysis.

Section 2 reviews the feasibility of analysis of future skills needs through patent data at theoretical level. It discusses a knowledge base and a knowledge network along with the possibility of examining future skills needs through patent data, and suggests a forecast methodology of future skills needs.

Section 3 proposes analytical statements on issues related to initial skills needs derived from the examination of current jobs in information security occupations. It links International Patent Classification (IPC) of information security technology to the skills needs.

Section 4 analyzes trends in the timescale of IPC on information security technology, carries out forecasting on skills needs, and verifies the appropriateness of actual forecast skills needs. In conclusion, the study discusses the achievements, limitations and future research directions of investigating future skills needs through patent data.

II. In Using Patent Data to Detect Future Skills Needs

1. Skills and Knowledge

In this study, skills include technology and dexterity, and thus can be considered an interchangeable concept with knowledge. Knowledge in this context focuses on knowledge as competence and acquaintance rather than propositional knowledge. On top of knowledge as competence and acquaintance, there are transcendent knowledge and logical knowledge that are closely related to propositional knowledge. As regards epistemology, knowledge can be classified into three categories (Balconi et al., 2007): Firstly, knowledge means an ability to do something (knowledge as competence) ranging from simple behaviors to complex cognitive behaviors, i.e. from use of simple hammers to use of complex languages. Secondly, knowledge is a familiar behavior of getting to know someone or something through past experiences (knowledge as acquaintance), like remembering the faces of frequently encountering people. Thirdly, propositional knowledge is recognition of the necessity of modifying certain information at hand. This is an inherent nature of mankind as an advanced species.

Knowledge as competence and knowledge as acquaintance are discussed by Gibbons et al. (1994), who analyze, in a useful fashion, the changes in knowledge production methods with a focus on modern science and technology. Gibbons et al. examine the transition of knowledge production method, naming knowledge production in a traditional method as Mode 1 knowledge and knowledge production in a new method that transformed traditional knowledge production as Mode 2 knowledge. While Mode 1 indicates knowledge forming that occurs within the boundary of certain disciplines, Mode 2 indicates knowledge forming that occurs through inter-discipline or trans-discipline. Nowotny et al. (2003) regard Mode 1 knowledge forming as a further development of existing science and technology measured on an academic standard, while they regard Mode 2 knowledge forming as a new paradigm of knowledge creation.

In the midst of rapid technological progress, Mode 2-type knowledge is also expanding (Cowan et al., 2000). Simple restructuring of existing knowledge is not sufficient, and it requires continuous knowledge creation. This kind of knowledge creation enhances knowledge convergence. In other words, the key to knowledge creation lies in the active participation in a continuous process of converging knowledge. In this context, simply absorbing convergent knowledge as a response has its limitation.

2. Usage of Patent as a Tool of FTA

For a while, patent data have been regarded as one of the most important sources or tools for FTA. With free accessibility in most countries, patent data provides valuable information on technological development and allows the analysis of emerging technologies, for instance, text mining in Yoon et al. (2004), Tseng et al. (2007) and An et al. (2011) and pattern recognition in Cong et al. (2010).

After reviewing several technology forecasting methodologies and models, Daim et al. (2006) propose the integration of multiple methodologies for forecasting in the areas of fuel cell, food safety and optical storage – integrating patent analysis and bibliometrics consisting of System Dynamics, Scenarios and Growth Curves. They insist on the need to develop such integrated tools for technology forecasting. Furthermore, Daim et al. (2006) suggest the inclusion of a Delphi methodology involving experts in FTA. Previously, after compiling several methods of analysis on future technology and considering recent changes in science and technology, including information technology, Porter et al. (2004) address several challenges related to the feasibilities and (current) limitations of FTA, and they offer steps for further advances.

Cagnin et al. (2013) insist that an appropriate combination of quantitative and qualitative methods should be made for specific purpose and context. It should enable confidence building through inclusiveness and transparency in all processes linked to rigorous methods. They warn that there is no uniform and proven FTA methodology, and that applying relevant methods in a rigorous manner is more important than assembling a set of highly sophisticated methods.

Even though combining quantitative and qualitative approaches is needed to bring about a better understanding of societal challenges and complex interrelated systems, Haegeman et al. (2013) explore aspects which ought to be considered in future analysis such as epistemological differences, cultural differences and conceptual differences.

3. Patent Analysis and Knowledge

Saviotti (2004, 2007) argues that knowledge has two different attributes in knowledge creation and utilization: (Proposition 1) knowledge has a co-relational structure; (Proposition 2) knowledge has a retrievable/interpretative structure. These attributes of knowledge can construct a (knowledge) network (Saviotti, 2009, 25-26). The ‘advent of new technology' and more recent

'convergence of knowledge' can be analyzed as this type of knowledge network.

Patent data could be used for examining this knowledge network. Due to skills resulting from a technological innovation, the examination of patent data - itself a product of technological innovation - could provide keys to the analysis of future skills needs. The structure of data embedded in patents could play a critical role as a "proxy meter" in understanding the structures of R&D activities and related knowledge. Quantifying and structuring patent data make it possible to understand the development and structure of knowledge.

4. Methodological Scheme in This Study

This study has selected the sector of information security that has witnessed considerable technological advances in recent years. It is also relatively well organized as to the skills needs identified through an analysis of jobs at a particular point in time, following a pilot.

This study is configured in five large schemes: (1) extraction of skill units based on job analysis; (2) extraction of skill elements based on patent analysis; (3) matching IPC skill elements with skill units from job analysis1 ; (4) tracking skills needs forecasting from patent trends; (5) verification of the validity of skills needs outlook.

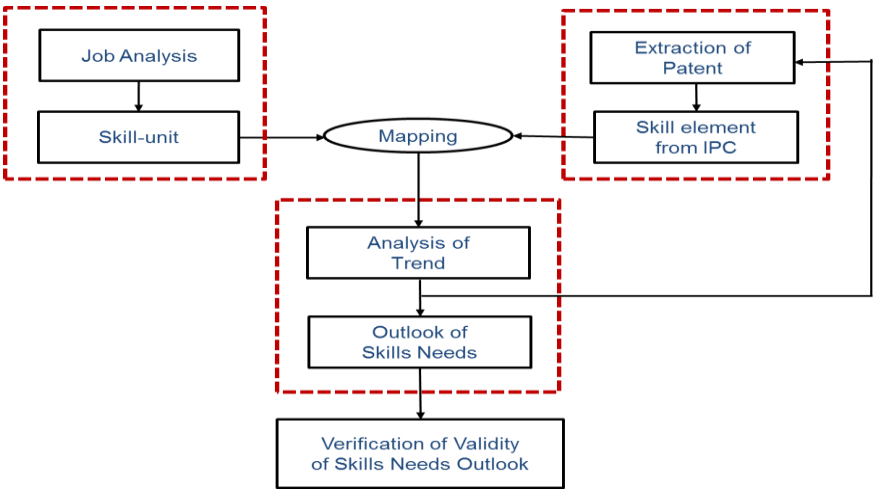


Figure 1 Methodological scheme

1 Here, intentionally, the two terminologies are adapted without rigorous definition: 'skill element' is used with IPC relation and 'skill unit' with job analysis relation.

Correcting a search formula recursively via IPC analysis carried out the identification of patent, and the final search formula was determined through skills analysis. From the initial formula setting, security professionals provided consultation in a repetitive corrective process. A total of 174,155 patents were finally identified.

The identification of skills unit from jobs was carried out through a meta-analysis of related domestic and international job configurations. Especially, a substantial level of support was secured from US job data.

The mapping and matching of skill elements from IPC code with skills units from existing job studies is conducted in collaboration with information security professionals. The mapping is key to analyze skills trend from a patent trend.

Future skills needs for information security is drawn from an exploratory analysis of the timeline trend of the skills elements based on patent data. Continuous consultation with professionals on the results of the analysis helped distinguish the broad case from a narrow case of connection between IPC code and skills units in the sector of information security[2]. Also, the distinction was arrived at between whole applied patterns and top 20 patent-applied companies.

Upon observing the apparent gap between forecast results and actual results, a better methodology could be developed by raising the validity of actual data. To test the degree of attributing the entire forecast results, including consistent forecast results, to the validity of actual situations, surveys of experts and companies were carried out.

III. Job Analysis and Patent in Information Security

1. Information Security

The field of ICT, which has recently experienced significant technological advances and represents relatively well-organized necessary skills needs identified through an analysis of actual jobs, was selected through a pre-analysis. This helped select subjects and method application to develop a methodology. The consistently rapid technological advances in the ICT sector since the 1990s was confirmed by annual trends in the number of registered patents in the U.S. Patent and Trademark Office.[3]

2 Basic Skill element included vs. Specific Skill element only. For detail, see Table 3 below.
3 In the early stage of this study, analyzing U.S. patents was attempted, but it the examination switched to Korean patents in consideration of feasibility and correspondence

Table 1 Knowledge information security

2nd classification	3rd classification
Common base security	Encryption technology (Algorithm/Protocol)
	Authentication technology
	Additional channel attack prevention
	ID management & privacy information protection technology
Network & System security	Access control
	Secure communication
	Penetration defense technology
	Continuance management technology
	Accident responding technology
	Security management technology
Service/ Application security	Contents security
	Web/E-mail application service security
	VoOP/IPTV/LBS security
	Cloud security
Physical security	Facility audit
	Access control
	Electronic wave security
Convergence security	Intelligent car security
	Airliner/Ship building security
	u-Healthcare security
	Financial security
	Smart-grid security
	Industry control system security

Source: Ministry of Knowledge Economy (2011)

The pre-analysis has also gone through expert consultation to check the validity of identifying technological advances in ICT from patent data. Furthermore, due to the relative clarity of job description, the ICT technology sector was deemed suitable for the analysis of current skills needs. It was recognized that this sector, through an analysis of patent, allows for a relatively easy comparison of forecasting demands for significantly advanced ICT skills. On this basis, the focus on the sector of information security was finalized.

On Table 1, the physical security element is to be excluded from information security in this research because it goes beyond the brief of the study. Since

to skills needs according to Korean trend and specifics of security technology. Use of U.S. patents was left for a future project.

both the application service security and the convergence security can be regarded as instrumental in information security, the study defines the range of information security by focusing on network and system security, including common base security. The technology of common base security was not analyzed separately, but examined as a component in the analysis of the network and system security.

2. Skill Unit from Job Analysis

Before examining job configuration and skills needs for information security, the current and prospective status of human resources was considered by tapping into existing researches. The information for the analysis of job configuration and knowledge requirement was gathered through expert advice and material data from inside and outside of the country (Simpson et al., 2006; Yoo and Kim, 2009). After reviewing the knowledge requirement for the information protection and education certification program in the United States, relevant research material was collected to carry out the analysis of the information security job in Korea. As a final step, expert opinions were sought to identify the skills needs for information security jobs.

The result of identifying skills through a review of the nature of the jobs is presented in Table 2 as necessary skills corresponding to the sub-classification of job category. Patents are analyzed in response to these required skills.

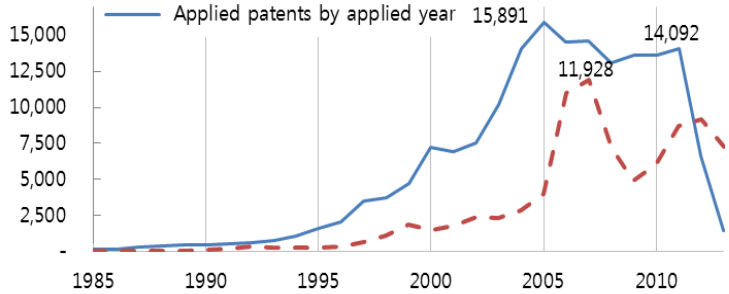
Table 2 Job configuration & required skills for information security sector

Classification		Skill unit (Limited to technical items)
Category	Sub-category	
Strategy & planning	(A) Risk analysis	(A-1) Security weakness analysis
		(A-2) Network security scanner
		(A-3) Pilot hacking, simulated infiltration
	(B) Establishing information protection policy & plan	(B-1) ISMS (Information security management system)
		(B-2) Security policy
		(B-3) Security management on outsourcing
		(B-4) Task identification
		(B-5) Inspection logging
		(B-6) PC security
		(B-7) Data security
		(B-8) Network security
		(B-9) Server security
	(C) Privacy protection management	(C-1) Privacy protection law
		(C-2) Privacy information encryption

Marketing & sales	(D) Marketing management	
	(E) Technical sales	
R&D, Implementation	(F) R&D	(F-1) Encryption algorism
	(G) Implementation	
Education & training	(H) Public & user education	
	(I) Expert education	
Management & operation	(J) Project management	(J-1) Security architecture
	(K) Information infrastructure security management	(K-1) Firewall configuration
		(K-2) Virus vaccine
		(K-3) Spyware
		(K-4) Phishing
		(K-5) Spam
		(K-6) (DB security encryption
		(K-7) OTP (One time password)
		(K-8) PKI (public key infrastructure)
		(K-9) VPN (Virtual private network)
		(K-10) DDoS (Distributed denial-of-service attack)
		(K-11) MDM (Mobile device management)
		(K-12) IPS (Intrusion prevention system)
		(K-13) Certification service
	(L) Physical security	
Emergency response	(M) Monitoring & responding	(M-1) Weakness analysis
		(M-2) Log analysis
		(M-3) Security control
		(M-4) APT (Advanced persistent threat)
	(N) Digital forensic	N-1) Understanding forensics
		(N-2) Cryptology
		(N-3) Hacking technique
		(N-4) Cyber attack
	(O) Job continuance management	
Evaluation & certification	(P) Evaluation certification & quality assurance	
	(Q) Information system security inspection	(Q-1) Security inspection
		(Q-2) Information security event management

3. Extraction of Patent Information

The basic element for analyzing a patent is an examination of patent application to Korean Intellectual Property Office each year. This data was extracted from KIPRIS DB (http://kpat.kipris.or.kr/). In fashioning a search formula, the first step involved a basic search using IPC. In the second step, the IPC code was re-extracted (7-digit level) from the search results obtained in the first step. In the third step, a keyword search was carried out of the patent summary. After running the entire analysis process based on the third search formula, all the previous analyses were run again by modifying the search formula. The search results on information security patent eventually covered 174,155 patents filed as of September 30, 2013.



Source: http://kpat.kipris.or.kr/ (accessed on September 30, 2013)

Figure 2 Patents pending for information security

4. Mapping Skill Element to Skill Unit from Job Analysis

In matching IPC-extracted patents with required skills, the skills that could not be comprised within IPC were excluded, and the IPC that does not include information security was also disregarded. Meanwhile, matching multiple IPCs with one skill unit was allowed as well as matching one IPC with several skill units, with regard to IPC as a skill element.

Table 3 Mapping skill element from IPC to skill unit from job analysis

Skill element (Specific/ Basic) / Skill Unit (Limited to technical items)	Specific Skill element																	Basic Skill element						
	G06F21	G06K1	G06K7	G09C1	H04B1	H04J1	H04K1	H04L9	H04W4	H04W8	H04W12	H04W48	H04W60	H04W80	H04W84	H04W88	H04W92	G06F5	G06F9	G06F17	G06F19	G06T1	H04W28	H04W64
Frequency in extracted patents	5,866	134	1,839	153	48,330	290	276	6,461	28,163	8,676	7,586	3,844	507	1,772	6,225	13,255	2,630	266	14,022	20,378	4,358	2,405	3,665	1,986
(A-1) Security weakness analysis	1																							
(A-3) Pilot hacking, simulated infiltration	1																							
(B-1) ISMS									1	1	1										1		1	1
(B-2) Security policy											1										1			1
(B-6) PC security	1																							
(B-7) Data security	1	1	1															1		1		1		
(B-8) Network security					1	1	1	1	1	1		1		1	1	1	1						1	1
(C-1) Privacy protection law											1										1			
(C-2) Privacy information encryption																					1			
(F-1) Encryption algorism	1			1		1	1	1						1				1				1		
(J-1) Security architecture										1	1													
(K-1) Firewall configuration										1					1									
(K-6) DB security encryption																					1			
(K-7) OTP											1													
(K-11) MDM									1															1
(K-13) Certification service									1		1		1											1
(M-1) Weakness analysis									1															
(N-2) Cryptology								1																
(Q-1) Security inspection											1								1		1			
(Q-2) Information security event management											1								1					

Note: 1. Relevance is expressed as "1"

2. For code description, go to http://www.wipo.int/classifications/ipc/en/

G06F005 Methods or arrangements for data conversion without changing the order or content of the data handled
G06F009 Arrangements for programme control, e.g. control unit (programme control for peripheral devices G06F 13/10)
G06F017 Digital computing or data processing equipment or methods, specially adapted for specific functions
G06F019 Digital computing or data processing equipment or methods, specially adapted for specific applications (G06F 17/00 takes precedence; data processing systems or methods specially adapted for administrative, commercial, financial, managerial, supervisory or forecasting purposes G06Q)
G06F021 Security arrangements for protecting computers or computer systems against unauthorized activity (multiprogramming G06F 9/46; protection against unauthorized use of memory G06F 12/14; dispensing apparatus actuated by coded identity card or credit card G07F 7/08; equipment anti-theft monitoring by a central station G08B 26/00; secret or secure communication H04L 9/00; data switching networks H04L 12/00 G06K007 Methods or arrangements for sensing record carriers (G06K 9/00 takes precedence)
G06K001 Methods or arrangements for marking the record carrier in digital fashion
G06K007 Methods or arrangements for sensing record carriers (G06K 9/00 takes precedence; methods or arrangements for marking the record carrier in digital fashion G06K 1/00)
G06T001 General purpose image data processing
G09C001 Apparatus or methods whereby a given sequence of signs, e.g. an intelligible text, is transformed into an unintelligible sequence of signs by transposing the signs or groups of signs or by replacing them by others according to a predetermined system (cryptographic typewriters G09C 3/00) H04B001 Details of transmission systems, not covered by a single one of groups H04B 3/00-H04B 13/00; Details of transmission systems not characterised by the medium used for transmission (tuning resonant circuits H03J)
H04B001 Details of transmission systems, not covered by a single one of groups H04B 3/00-H04B 13/00; Details of transmission systems not characterised by the medium used for transmission
H04J001 Frequency-division multiplex systems (H04J 14/02 takes precedence)
H04K001 Secret communication (ciphering or deciphering apparatus per seG09C; systems with reduced bandwidth or suppressed carrier H04B 1/66; spread spectrum techniques in general H04B 1/69; by using a sub-carrier H04B 14/08; by multiplexing H04J; transmission systems for secret digital information H04L 9/00; secret or subscription television systems H04N 7/16)
H04L009 Arrangements for secret or secure communication
H04W004 Services or facilities specially adapted for wireless communication networks
H04W008 Network data management
H04W012 Security arrangements, e.g. access security or fraud detection; Authentication, e.g. verifying user identity or authorisation; Protecting privacy or anonymity
H04W028 Network traffic or resource management
H04W048 Access restriction; Network selection; Access point selection
H04W060 Registration, e.g. affiliation to network; De-registration, e.g. terminating affiliation
H04W064 Locating users or terminals for network management purposes, e.g. mobility management
H04W080 Wireless network protocols or protocol adaptations to wireless operation, e.g. WAP [Wireless Application Protocol]
H04W084 Network topologies
H04W088 Devices specially adapted for wireless communication networks, e.g. terminals, base stations or access point devices
H04W092 Interfaces specially adapted for wireless communication networks

The matching results were obtained through consultation with experts. On the Table 3, H04W008 Network data management[4] appeared to be the required skills element of (B-1) ISMS (Information Security Management System), (B-8) Network security[5], (J-1) Security architecture, and (K-1) Firewall configuration. While (B-1) ISMS (Information Security Management System) is a match not only to H04W008 'Network data management,' but also to H04W004 'Services or facilities specially adapted for wireless communication networks,' but also to H04W012 'Security arrangements and Authentication,' G06F019 'Digital computing or data processing equipment or methods, specially adapted for specific applications,' H04W028 'Network traffic or resource management' and H04W064 'Locating users or terminals for network management purposes.' In matching skill units (derived from job analysis) with skill elements (derived from IPC), the distinction of specific skill elements and basic skill elements is also considered, in order to allow for certain skill elements to become basic skill elements, thus, not necessarily becoming an element of specific skill needs.[6]

IV. Forecasting the Skills Needs from Patent Analysis

1. Trend of Expected Skills Needs from Patent Trend

Given a particular skill S_i, the required skill forecast for t period is defined as S_i^t, while the frequency of S_i^t is $N(S_i^t)$ which is the sum of the frequency that appeared[7] for multiple S_i related IPC during t period. For example, while IPCs related to the skill of (B-1) ISMS (Information Security Management System) are *G06F019*, *G06Q040*, *H04W004*, *H04W008*, *H04W012 H04W028*, and *H04W064*, $N(S_{B\text{-}1}^{2000})$ for *year 2005* and has a total frequency of 4,823 among the patents filed in 2005. The result is presented in Table 4 where the relative size of IPC is derived from the division of yearly total frequency on Table 5.

4 It is also expressed as H04W8 with omission of 0 and 00 after 4 digits expression. For the detail explanation, see the note under Table 3 and http://www.wipo.int/classifications/ipc/en/.
5 There could be criticism of the overloading of IPCs in specific skills. It could cause a biased distribution and bring distortion, particularly where the small number of specific IPC could be important. Different treatment will be attempted in further study.
6 During the analysis, this distinction has not revealed any big differences, and the exclusion of basic skill units is mainly reported on Table 6.
7 Here, applied patterns in detecting technological change are considered to avoid information loss and the unstable time lag that are caused by using registered patents.

Based on the relative size of IPC on Table 5[8], the trend in the skills needs is shown on Figure 3.

Table 4 Trend of skills needs from absolute size of IPC

(unit: frequency)

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
(A-1) Security weakness analysis	162	110	117	170	245	180	423	637	848	780	725	928	364	100
(A-3) Pilot hacking, simulated infiltration	162	110	117	170	245	180	423	637	848	780	725	928	364	100
(B-1) ISMS (Information Security Management System)	1795	2006	2585	3342	4081	4823	4811	4941	3652	4198	4241	3775	1489	330
(B-2) Security policy	262	309	449	484	735	1152	1556	1488	1086	1376	1528	1796	531	118
(B-6) PC security	162	110	117	170	245	180	423	637	848	780	725	928	364	100
(B-7) Data security	1750	1137	982	1139	1668	1852	2457	2904	2722	2885	2890	3175	1426	329
(B-8) Network security	4324	4857	5747	8462	11689	13171	10690	10516	8770	9607	8749	8590	3727	710
(C-1) Privacy protection law	190	244	361	385	641	1038	1440	1353	1002	1118	1156	1581	415	92
(C-2) Privacy information encryption	62	51	67	146	113	276	289	324	231	395	560	904	269	64
(F-1) Encryption algorism	559	460	503	572	998	1082	1348	1850	1886	1881	1629	2034	845	233
(J-1) Security architecture	522	615	853	968	1417	1723	1926	2045	1445	1333	1089	967	370	87
(K-1) Firewall configuration	524	619	835	978	1277	1474	1349	1768	1182	1284	994	749	413	83
(K-6) DB security encryption	62	51	67	146	113	276	289	324	231	395	560	904	269	64
(K-7) OTP	128	193	294	239	528	762	1151	1029	771	723	596	677	146	28
(K-11) MDM	1104	1174	1502	2016	2242	2563	2289	2174	1719	2148	2251	1660	659	120
(K-13) Certification service	1257	1384	1813	2272	2799	3370	3473	3240	2522	2924	2892	2374	845	155
(M-1) Weakness analysis	1032	1109	1414	1917	2148	2449	2173	2039	1635	1890	1879	1445	543	94
(N-2) Cryptology	199	157	188	219	506	539	506	702	654	650	565	763	317	71
(Q-1) Security inspection	571	591	668	807	1341	2027	2497	2373	2123	2448	2676	3095	1205	278
(Q-2) Information security event management	509	540	601	661	1228	1751	2208	2049	1892	2053	2116	2191	936	214
Total	15336	15827	19280	25263	34259	40868	41721	43030	36067	39648	38546	39464	15497	3370

8 The relative size (P(S)) is derived as follows:

$$P(S_i^t) \equiv \frac{N(S_i^t)}{\sum_i N(S_i^t)},\ t = 1,2,\dots,T$$

Table 5 Trend of skills needs from relative size of IPC

(unit: %)

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
(A-1) Security weakness analysis	1.1	0.7	0.6	0.7	0.7	0.4	1.0	1.5	2.4	2.0	1.9	2.4	2.3	3.0
(A-3) Pilot hacking, simulated infiltration	1.1	0.7	0.6	0.7	0.7	0.4	1.0	1.5	2.4	2.0	1.9	2.4	2.3	3.0
(B-1) ISMS (Information Security Management System)	11.7	12.7	13.4	13.2	11.9	11.8	11.5	11.5	10.1	10.6	11.0	9.6	9.6	9.8
(B-2) Security policy	1.7	2.0	2.3	1.9	2.1	2.8	3.7	3.5	3.0	3.5	4.0	4.6	3.4	3.5
(B-6) PC security	1.1	0.7	0.6	0.7	0.7	0.4	1.0	1.5	2.4	2.0	1.9	2.4	2.3	3.0
(B-7) Data security	11.4	7.2	5.1	4.5	4.9	4.5	5.9	6.7	7.5	7.3	7.5	8.0	9.2	9.8
(B-8) Network security	28.2	30.7	29.8	33.5	34.1	32.2	25.6	24.4	24.3	24.2	22.7	21.8	24.0	21.1
(C-1) Privacy protection law	1.2	1.5	1.9	1.5	1.9	2.5	3.5	3.1	2.8	2.8	3.0	4.0	2.7	2.7
(C-2) Privacy information encryption	0.4	0.3	0.3	0.6	0.3	0.7	0.7	0.8	0.6	1.0	1.5	2.3	1.7	1.9
(F-1) Encryption algorism	3.6	2.9	2.6	2.3	2.9	2.6	3.2	4.3	5.2	4.7	4.2	5.2	5.5	6.9
(J-1) Security architecture	3.4	3.9	4.4	3.8	4.1	4.2	4.6	4.8	4.0	3.4	2.8	2.5	2.4	2.6
(K-1) Firewall configuration	3.4	3.9	4.3	3.9	3.7	3.6	3.2	4.1	3.3	3.2	2.6	1.9	2.7	2.5
(K-6) DB security encryption	0.4	0.3	0.3	0.6	0.3	0.7	0.7	0.8	0.6	1.0	1.5	2.3	1.7	1.9
(K-7) OTP	0.8	1.2	1.5	0.9	1.5	1.9	2.8	2.4	2.1	1.8	1.5	1.7	0.9	0.8
(K-11) MDM	7.2	7.4	7.8	8.0	6.5	6.3	5.5	5.1	4.8	5.4	5.8	4.2	4.3	3.6
(K-13) Certification service	8.2	8.7	9.4	9.0	8.2	8.2	8.3	7.5	7.0	7.4	7.5	6.0	5.5	4.6
(M-1) Weakness analysis	6.7	7.0	7.3	7.6	6.3	6.0	5.2	4.7	4.5	4.8	4.9	3.7	3.5	2.8
(N-2) Cryptology	1.3	1.0	1.0	0.9	1.5	1.3	1.2	1.6	1.8	1.6	1.5	1.9	2.0	2.1
(Q-1) Security inspection	3.7	3.7	3.5	3.2	3.9	5.0	6.0	5.5	5.9	6.2	6.9	7.8	7.8	8.2
(Q-2) Information security event management	3.3	3.4	3.1	2.6	3.6	4.3	5.3	4.8	5.2	5.2	5.5	5.6	6.0	6.4
Total	100	100	100	100	100	100	100	100	100	100	100	100	100	100

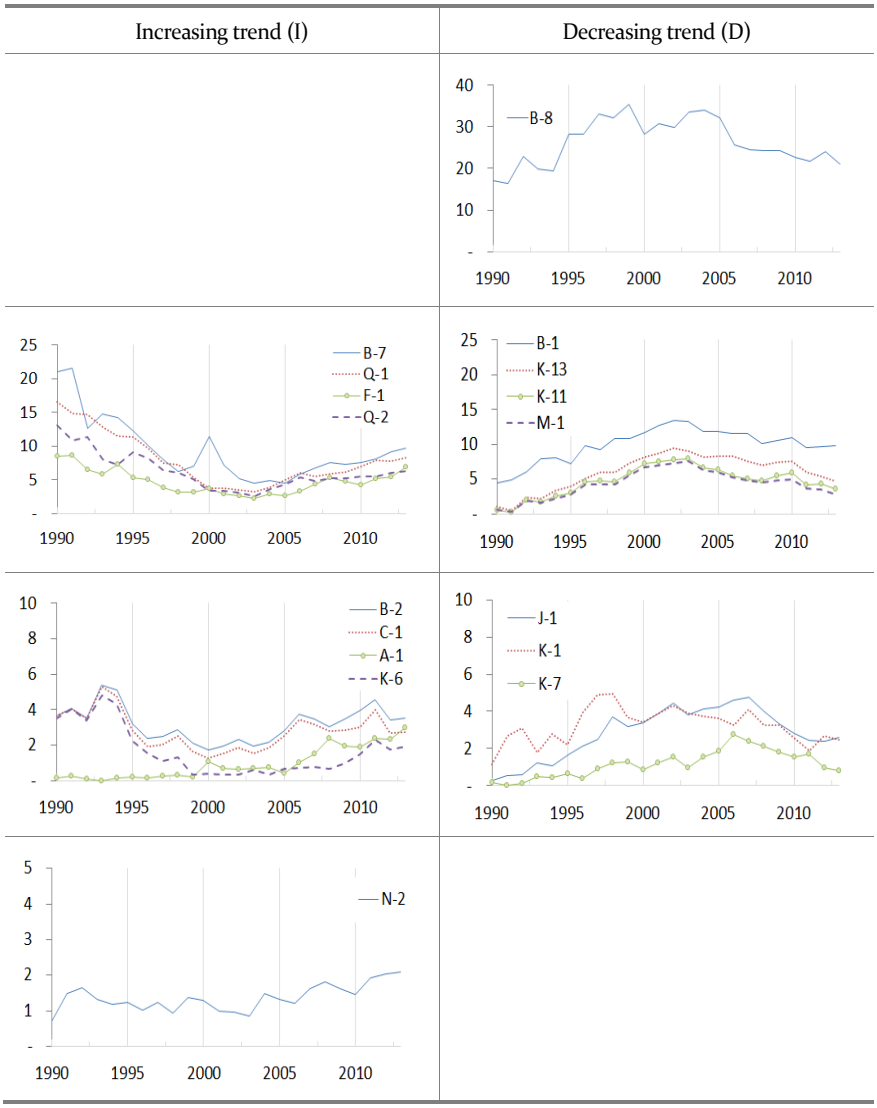


Figure 3 Trends of the skills needs based on IPC time-pattern

2. Forecasting and Verification of Skills Needs

Based on the timeline trend, mainly since 2005, two categories are examined as increasing and decreasing trends, on Figure 3. In the findings, the distinction between specific skill elements only and the inclusion of basic skill elements was made. Furthermore, the distinction between the whole pattern of patent application and top 20 patent-applied companies only was also made. After conducting 2×2 analyses with overall similar results in terms of trends, Table 6 shows the whole pattern of patent applications with specific skill elements only.

Regardless of the differences of treatment in the patent analysis, ① (B8) 'Network security' appears to be the skill that continues to hold a great deal of importance, while ② (F1) 'Encryption algorithm,' (B7) 'Data security,' (N-2) 'Cryptology,' (A-1) 'Security vulnerability analysis,' (A-3) 'Simulated hacking and simulated penetration' and (B-6) 'PC Security' were presented as newly-emerging skills. In addition, ③ (B1) 'Information security management system,' (K13) 'Authentication service,' (K -11) 'Mobile device management,' (M1) 'Vulnerability analysis,' (J-1) 'Security architecture,' (K-1) 'Firewall building' and (K-7) 'OTP' were presented as skills being incorporated into basic skills with receding independence compared to the past. Based on the forecast that includes general-purpose technology IPC, (B-2) 'Security policy,' (Q-1) 'Security audit' and (Q-2) 'Information security event management' are also expected to be newly emerging skills.

To verify the validity of the reality of these forecast results, a survey of information security companies and of relevant experts was conducted. Table 5 presents these findings as well as the forecast results that include a general-purpose technology IPC. The survey results were generally similar, with the exception of a high frequency for (B-6) 'PC security' in ② 'newly emerging skills' in the category of 'manufacturer only,' and ① 'skills that continue to hold importance' in the category of 'expert group.' These results can be interpreted as supporting the findings of the skills needs forecast carried out by examining the entire patent filings, including general-purpose technology IPC (Fisher's Exact-Test is significant, with the significant level of 5%).

Table 6 Survey for the validity of skills needs forecast

Forecasting	Skills	Corporate & Expert surveys on validity of forecast							
		Corporate only (6)				Corporate (6) + Expert (5)			
		①	②	③	④	①	②	③	④
①continuing importance	(B-8) Network security	100%	0%	0%	0%	100%	0%	0%	0%
②getting important	(A-1) Security vulnerability analysis	17%	83%	0%	0%	36%	64%	0%	0%
	(A-3) Simulated hacking and simulated penetration	17%	83%	0%	0%	40%	60%	0%	0%
	(B-2) Security policy	17%	50%	33%	0%	30%	50%	20%	0%
	(B-6) PC security	17%	50%	17%	0%	50%	40%	10%	0%
	(B-7) Data security	0%	100%	0%	0%	11%	89%	0%	0%
	(C-1) Privacy information protection law	0%	100%	0%	0%	0%	100%	0%	0%
	(C-2) Privacy information encryption	17%	83%	0%	0%	27%	73%	0%	0%
	(F-1) Encryption algorithm	33%	67%	0%	0%	36%	55%	9%	0%
	(K-6) DB security encryption	0%	83%	0%	17%	18%	73%	0%	9%
	(N-2) Cryptology	50%	50%	0%	0%	45%	45%	9%	0%
	(Q-1) Security audit	0%	100%	0%	0%	30%	70%	0%	0%
	(Q-2) Information security event management	0%	83%	17%	0%	10%	80%	10%	0%
③becoming general skills	(B-1) Information security management system	17%	0%	83%	0%	20%	20%	60%	0%
	(J-1) Security architecture	0%	0%	100%	0%	20%	0%	80%	0%
	(K-1) Firewall building	0%	0%	100%	0%	20%	0%	80%	0%
	(K-11) Mobile device management	0%	50%	50%	0%	9%	64%	27%	0%
	(K-13) Authentication service	0%	0%	100%	0%	18%	18%	64%	0%
	(K-7) OTP	0%	0%	100%	0%	0%	10%	90%	0%
	(M-1) Vulnerability analysis	17%	0%	83%	0%	40%	0%	60%	0%

Note: ① Skills that continue to hold importance
② Newly emerging skills
③ Converted to general purpose skills
④ Importance decreasing skills

V. Concluding Remarks

This study attempts to develop a methodology that analyzes patent applications to identify future skills, in particular in the sector of information security, recently in the spotlight. Matching skill elements from IPC with skill units from job analysis, the study tries to track trends of the skills needs based on IPC time-pattern. It then verifies the validity of the outlook for future skills needs by addressing the situation through the use of patents. The research assesses the usability of patent information by showing how it can be utilized in the analysis on future skills needs.

The skills needs identified from the patent information in late 2000s in the information security sector substantially mirror the skills needs identified in 2013. However, the accuracy of matching the skills needs forecast in different fields or timeline with the actual skills needs is not guaranteed. Furthermore, differences in the speed and pattern of technological advances are revealed owing to differences in technological characteristics and differences in various socio-economic environments within which technologies are implemented. The most important issue in this study is 'Matching required skills with jobs within IPC', but it is worth noting that more specific and detailed methods beyond the current one utilizing the 0-1 matrix would be required.

Despite its limitations, this current study might be worth refining the methodology to identify future skills needs by using patent information, because there is still no research in this specific area. While this study is limited to the sector of information security by using Korean patent information, it can be expanded in the future to other areas and patents in the United States and Europe. Technological change is a global phenomenon, so the analysis of global patent information ought to be a valuable contribution.

References

An, X.Y. and Wu, Q.Q. (2011) Co-word analysis of the trends in stem cells field based on subject heading weighting, Scientometrics, 88, 133-144.

Balconi, M. et al. (2007) The 'codification debate' revisited: a conceptual framework to analyze the role of tacit knowledge in economics, Industrial and Corporate Change, 16(5), 823-849.

Cagnin, C., Havas, A. and Saritas, O. (2013) Future-oriented technology analysis: its potential to address disruptive transformations, Technological Forecasting & Social Change, 80, 379-385.

CEDEFOP (2012) Skills Supply and Demand in Europe-Methodological Framework, Luxembourg: Publications Office of the European Union.

Cong, H. and Tong, L-H. (2010) Pattern-oriented associative rule-based patent classification, Expert Systems with Applications, 37(3), 2395-2404.

Cowan, R. et al. (2000) The Explicit Economics of Knowledge Codification and Tacitness, England: Oxford University Press.

Daim, T. (2006) Forecasting emerging technologies: use of bibliometrics and patent analysis, Technological Forecasting and Social Change, 73(8), 981-1012.

Gibbons, M. et al. (1994) The New Production of Knowledge: The Dynamics of Science and Research in Contemporary Societies, London: SAGE.

Haegeman, K., Marinelli, E., Scapolo, F., Ricci, A. and Sokolov, A. (2013) Quantitative and qualitative approaches in Future-oriented Technology Analysis (FTA): from combination to integration? Technological Forecasting and Social Change, 80(3), 386-397.

Hwang, G. and Lee, J. (2010) Technological innovation & future skills - with focus on green car growth, Journal of Korea Technology Innovation Society, 13(3), 399-422. (in Korean)

Hwang, G., Coh, B. and Lee, J. (2011) Utilizing patent analysis in future skills need analysis - with focus on green technology of steel industry, Vocational Ability Development Study, 14(3), 79-104, (in Korean).

Hwang, G., Joo, I. and Coh, B. (2011) Future Skills Need Analysis by Patent Analysis - With Focus on Automobile Battery as Industry Convergence, KRIVET (in Korean).

Lowery, D. et al. (2008) Future Skill Needs - Projections and Employers' Views, NCVER.

Ministry of Knowledge Economy (2011) IT Information Technology Competitiveness Analysis. (in Korean)

Nowotny, H., Scott, P. and Gibbons, M. (2003) `Mode 2' revisited: the new production of knowledge, Minerva, 41(3), 179-194.

Porter, A.L. et al. (2004) Technology futures analysis: toward integration of the field and new methods, Technological Forecasting & Social Change, 71, 287-303.

Saviotti, P.P. (2004) Considerations about the production and utilization of knowledge, Journal of Institutional and Theoretical Economics, 160, 100-121.

Saviotti, P.P. (2007) On the dynamics of generation and utilization of knowledge: the local character of knowledge, Structural Change and Economic Dynamics, 18, 387-408.

Saviotti, P.P. (2009) Knowledge networks: structure and dynamics, in Andreas Pyka et al. (eds.) Innovation Networks: New Approaches in Modeling and Analyzing, Springer, 19-41.

Schmidt, S.L. et al. (eds.) (2004) Identifying Skill Needs for the Future: From Research to Policy and Practice, Office for Official Publications of the European Communities.

Simpson, H.K. et al. (2006) Development and Application of Skill Standards for Security Practitioners, USA: Defense Personal Security Research Center.

Tseng, Y-H., Lin, C-J. and Lin, Y-I. (2007) Text mining techniques for patent analysis, Information Processing and Management 43, 1216-1247.

Yoo, H. and Kim, T. (2009) Considering information security professionals' career to analyze knowledge and skills requirement, Journal of Korea Institute of Information Security and Cryptology, 19(4), 77-89. (in Korean)

Yoon, B. and Park, Y. (2004) A text-mining-based patent network: analytical tool for high-technology trend, Journal of High Technology, Management Research, 15, 37-50.