韩国网络安全法律重点制度及对我国的立法思考

姚财福（中国信息通信研究院互联网法律研究中心研究员）

0 引言

2016 年 11 月 7 日，第十二届全国人民代表大会常务委员会第二十四次会议于通过了《网络安全法》，一方面，标志着我国以《网络安全法》为核心和统领的网络安全法律体系得以建立；另一方面，《网络安全法》提出的关键信息基础设施保护、数据跨境提供、网络安全认证等重要制度还有待配套立法加以细化。

综观我们邻国韩国，近年来为应对网络攻击、保障网络安全、促进数字经济发展，基于其先进的信息通信技术，构筑起日益完备、行之有效的网络安全法律制度体系。本文希望通过考察韩国网络安全立法重点制度，为我国《网络安全法》配套规定的推进制定提出立法参考。

1 韩国网络安全法律体系概貌

韩国建立了由网络安全管理、关键信息基础设施保护、信息通信网络稳定性保障、数据安全等各相关专门性法律和综合性立法组成的，涵盖面广，却又重点突出的网络安全法律体系。

1.1 建立国家网络安全管理机制

韩国《国家网络安全管理规定》[1] 以专门法律文件形式，确立了韩国网络安全管理基本的管理、组织、运作机制，明确了总统国家安保室、国家网络安全中心等机构的网络安全保障职责，对组织国家网络安全战略会议、制定网络安全对策、加强网络危机应对训练、设立安全管制中心等作了规定。

1.2 加强信息通信网络稳定性保障

韩国《信息通信网络的利用促进与信息保护等相关法》[2] 规定了制定信息通信网络安全保护措施指南、保护集成信息通信设施、禁止信息通信网络侵害行为，特别是建立信息保护管理体系认证制度等信息通信网络安全保障机制。

1.3 突出关键信息基础设施保护

为重点加强“关键信息基础设施”——韩国法律称“主要信息通信基础设施（Main Information and Communications Infrastructure）”[3] 的保护，韩国专门制定了《信息通信基础设施保护法》及其实施细则[4]，明确了主要信息通信基础设施保护体系、信息通信基础设施保护委员会的职责、主要信息通信基础设施的指定与弱点分析、侵害事件的应对、技术支持和民间合作等内容。另外，由于能源设施的特殊重要性，韩国还专门制定了《原子能设施等防护和放射性防灾对策法》[5] 明确原子能设施的保护。

1.4 加强数据管理和保护

韩国《个人信息保护法》、《信息通信网络的利用促进与信息保护等相关法》、《位置

信息的保护与利用等相关法》、《信用信息的利用与保护法》等法律对一般个人信息保护、信息通信领域个人信息保护、金融领域信息管理等作了规定。

1.5 各相关领域立法补充完善网络安全法律制度

在新技术新业务方面，2015年3月制定的《云计算发展与用户保护法》[6]要求云服务提供者在发生侵害事故、用户信息泄露、服务中断的事件时，应即时通知用户。在电子政务方面，《电子政府法》[7]明确政府部门建立保障信息通信网络、行政信息等安全性与稳定性措施。在信息化推进方面，《国家信息化基本法》规定了保障信息使用安全和可靠性相关要求。在工业技术方面，《工业技术泄露预防与保护等相关法》[8]对工业技术的防止泄露与管理、工业技术保护基础设施的建立等进行了规定。

2 关键信息基础设施的保护制度

韩国《信息通信基础设施保护法》明确了主要信息通信基础设施管理、指定、弱点分析、防范电子侵害[9]、加强信息共享等制度，以实现主要信息通信基础设施的安全稳定运转。

2.1 主要信息通信基础设施的指定

《信息通信基础设施保护法》界定了“信息通信基础设施”的含义，包括两方面，一是与国家安全、行政、国防、公共安全、金融、通信、交通运输和能源相关的电子控制和管理系统，二是信息通信网络[10]。在此基础上，由中央行政机关在其职责范围内将信息通信基础设施指定为主要信息通信基础设施。指定时需考虑下列因素：（1）相关信息通信基础设施管理机构执行的事务对国家和社会的重要性；（2）设施管理机构执行信息通信基础设施事务的依赖度；（3）与其他信息通信基础设施互联互通情况；（4）发生侵害事件[11]情况下，侵害事件对国家安全、经济和社会造成损害的范围和程度；（5）侵害事件的可能性和恢复的容易性。

在具体程序上，中央行政机关制定指定相关评估标准和指南，向其管辖的信息通信基础设施管理机构发布。中央行政机关要求被认为适合指定为主要信息通信基础设施的设施管理机构，选定一个基本单位（basic unit）来指定主要信息通信基础设施。中央行政机关审查基本单位的选定和设施范围的可行性，必要时可进行调整。为作出指定决定，中央行政机关可要求相关管理机构提交必要资料。地方政府管理的相关机构的信息通信基础设施，由行政自治部与地方政府协商指定。经信息通信基础设施委员会审议后，中央行政机关作出指定或撤销指定的决定。

由于按照法律规定条件指定主要信息通信基础设施带来的压力，现实中存在中央行政机关怠于指定的情况，许多中央行政机关指定的主要信息通信基础设施数量很有限。为防止此现象发生，2007年《信息通信基础设施保护法》修订，增加有关信息通信主管部门和安全部门就主要信息通信基础设施的指定提出建议的规定。

最后，中央行政机关作出指定或撤销主要信息通信基础设施决定的，应当立通知相关管理机构，并在政府官报上公布以下事项：指定号码、主要信息通信基础设施的名称、管理机构的名称、执行业务、指定或撤销指定的事由。但经信息通信基础设施保护委员会审议并出于保障国家安全必要的，可不公示该情况。[12]

表 1 韩国未来创造科学部 2015 年指定的主要信息通信基础设施目录（部分）

指定号码	管理机构名称	主要信息通信基础设施名称	执行业务	指定事由
第 1 号	KT 公司	互联网连接网	互联网连接服务提供	为互联网服务提供时互联网连接网络基础设施的安全运用
第 2 号	LG U+ 公司	同上	同上	同上
第 3 号	SK broadband 公司	同上	同上	同上
第 4 号	SK 电信公司	移动电话（无线网络）	无线网络连接服务提供	为无线网络服务提供时无线网络基础设施的安全运用
第 5 号	KT 公司	同上	同上	同上
第 6 号	LG U+ 公司	同上	同上	同上
第 7 号	LG U+ 公司	公共互联网	为公共机构提供超高速信息通信服务	为超高速国家网络基础设施的安全运行
第 8 号	韩国信息认证公司	公认认证系统	提供公认认证服务	为电子签名服务提供时信息认证系统基础设施的安全运用
第 9 号	韩国互联网振兴院	互联网地址资源管理系统	互联网地址资源管理	为 KR 域名使用时互联网地址资源管理系统基础设施的安全运用
第 10 号	邮政事业信息中心	邮局金融系统	提供邮局金融系统	为邮局金融服务提供时金融系统基础设施的安全运用

2.2 其他相关制度

2.2.1 管理机制

《信息通信基础设施保护法》规定在总理下设立信息通信基础设施保护委员会，[13] 审议主要信息通信基础设施保护具体事项。委员会设立公共和民间部门的工作委员会，负责委员会的具体运作。前者由国家情报院负责，审议中央、地方政府及其所属机构等公共部门管理的主要信息通信基础设施事项。后者由未来创造科学部负责，审议上述以外的，主要是私营领域的主要信息通信基础设施的保护事项。

2.2.2 弱点分析

《信息通信基础设施保护法》建立了主要信息通信基础设施弱点分析和评价制度。规定主要信息通信基础设施管理机构在其管辖范围内成立负责弱点分析和评价小组，定期分析和评价主要信息通信基础设施的弱点。未来创造科学部负责制定弱点分析和评价的标准并告知相关中央行政机关。

2.2.3 信息共享制度

《信息通信基础设施保护法》规定，金融、通信等相关领域可设立信息共享与分析中心，就主要信息通信基础设施的弱点、遭受侵害的因素和对策相关信息，实时预警和分析系统的运行等进行共享。在信息共享与分析中心设立之日起 30 日内，应当向未来创造科学部和相关中央行政机关报告组织名称、设立地、企业代表和管理人员个人信息、基本业务、融资方式、公司章程等事项。

3 网络稳定性保障中的安全认证制度

韩国《信息通信网络的利用促进与信息保护等相关法》第 47 条确立了信息保护管理体系（ISMS-Information Security Management System）的认证制度。

3.1 认证范围

根据法律规定，ISMS 认证由未来创造科学部实施，具体认证对象包括三大类：一是信息通信网络稳定性和可靠性综合性管理体系（简称“信息保护管理体系”）的建立和运营者。二是电信业务经营者。三是满足下列情况的使用电信业务经营者的电信服务或以中介方式提供信息的服务提供者：（1）已获得《电信事业法》规定许可的信息通信服务提供者；（2）集成信息通信设施业务经营者；（3）以下年销售额或收入达到1500亿韩元以上的人员:《医疗法》规定的高级综合医院；《高等教育法》规定的截至 12 月 31 日上一年度在校生达到 1 万人以上的学校。（4）上一年度的信息通信服务全年销售额达到100亿韩元以上的，但金融公司除外。（5）近3个月的每日平均用户数超过100万名的，但金融公司除外。

3.2 认证的豁免

对于上述电信业务经营者或通过使用电信业务经营者的电信服务提供或以中介方式提供信息的人员的认证，根据未来创造科学部规定，获得符合国际信息保护标准认证或采取信息保护措施的，未来创造科学部可免于部分认证审查。

3.3 认证标准和有效期

法律规定涉及认证必要事项，如管理、技术和物理保护应对措施在内的认证标准，可由未来创造科学部确定并公告。信息保护管理体系认证的有效期应为 3 年，对于获得信息保护管理等级的，认证应视为在该等级有效期内有效。

3.4 认证和审查机构

未来创造科学部可授权韩国互联网振兴院（KISA) 或由未来创造科学部指定的任何机构，作为“信息保护管理体系认证机构”执行认证相关事项，包括（1）审查申请人的信息保护管理体系的认证是否符合认证标准（简称“认证审查”）；（2）审议认证审查的结果；（3）发放和管理证书;（4）授予认证的事后管理;（5）认证审查员的培训及资格管理；（6）其他认证相关事项。

为确保认证审查的有效实行，未来创造科学部可指定机构，作为“信息保护管理体系审查机构”执行认证审查相关事务。

为保障信息保护管理体系的高效运转，韩国互联网振兴院（KISA）、信息保护管理体系认证机构及信息保护管理体系审查机构，应当每年至少 1 次向未来创造科学部报告事后管理情况。

3.5 认证的撤销

存在以下情形的未来创造科学部可撤销认证：（1）以造假或非合理方式取得信息保护管理体系认证的；（2）未满足认证标准的；（3）拒绝或妨碍事后管理的。

4 跨境数据流动管理的区别对待

韩国信息保护、数据管理相关法律对不同类型数据建立不同的跨境流动管理模式。

4.1 个人信息跨境提供的要求和例外

韩国《个人信息保护法》并不阻止个人信息的跨境提供，但应首先通过制定相关政策措施，保障跨境个人信息传输不侵犯信息主体的权利。[14] 如果个人信息管理者向位于境外的第三人提供个人信息，应告知信息主体下列事项并取得同意，即保障信息主体的知情同意：（1）

个人信息的接收者；（2）个人信息接收者使用该信息的目的；（3）提供的个人信息的项目；（3）个人信息接收者持有和使用该信息的期限；（4）信息主体有权拒绝同意的事实和因其拒绝同意带来的不利情况。并且不得达成违反法律进行跨境个人信息传输的合同。[15]《信息通信网络的利用促进与信息保护等相关法》进一步细化信息通信服务提供者向国外转移用户个人信息应告知用户的事项，并应采取技术和管理、个人信息侵害相关投诉的处理及纠纷解决等措施。[16]

但对于向国外委托处理或保管个人信息的情况，《信息通信网络的利用促进与信息保护等相关法》规定，在为履行合同、增进用户便利条件等必要情况下，应事先告知用户的事项已公开的，委托国外处理或保管用户信息可不需征得用户同意。[17]

4.2 金融信息跨境提供存在的无需同意的情形

韩国法律规定，在特定情形下，如国际公约规定、国际金融合作的需要等，跨境传输相关金融信息可不需事先获得同意。《信用信息使用与保护法》规定，信用信息提供者或使用者拟向其他人提供借贷、担保等信息在内的个人信用信息的，应事先获得个人同意。但是存在例外情形，包括根据国际公约，当金融机构持有的个人信用信息向国外金融监管机构提供时，可不需获得个人事先同意。[18]《金融实名交易与秘密保障法》规定了出于有限使用目的的必要性时可提供或披露交易信息的例外。[19] 2015 年金融委员会新修订的《金融公司信息处理业务委托相关规定》放松了金融机构对信息处理业务进行离岸委托的限制。但个人消费者的固有识别信息不得向国外转移。

4.3 重要信息的限制跨境流动

《信息通信网络的利用促进与信息保护等相关法》明确限制重要信息向国外流出。规定政府可要求信息通信服务提供者或用户采取必要手段防止任何有关工业、经济、科学、技术等的重要信息通过信息通信网络向国外流动，这类的重要信息包括：（1）国家安全与主要政策相关信息；（2）国内开发的尖端技术或设备相关内容的信息。政府可要求处理这些信息的信息通信服务提供者采取下列措施：（1）安装可防止非法利用信息通信网络的系统性或技术性设备；（2）建立相关制度，安装相关技术设备；（3）可防止非法破坏或操作信息的系统性与技术性措施；（4）可防止信息通信服务提供者泄露履行职务过程中了解到的信息的措施。[20]

5 立法思考

5.1 确立关键信息基础设施的具体范围

我国《网络安全法》第 31 条对“关键信息基础设施”的定义采取涉及行业加危害影响的特征方式描述，即涉及“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施”。但“关键信息基础设施的具体范围和安全保护办法由国务院制定。”

下一步在制定《网络安全法》有关关键信息基础设施管理和安全保护的配套规定，明确关键信息基础设施的具体范围将是规定的一块重要内容。韩国有关主要信息通信基础设施的指定等保护相关制度将给我国如何确定关键信

息基础设施的具体范围提供参考方向：

一是明确关键信息基础设施认定的主体职责。韩国在总理下设立信息通信基础设施保护委员会，统筹负责关键信息基础设施保护重要事项，建立了职责分工明确的关键信息基础设施认定和撤销机制：各行业各领域中央行政主管部门负责本行业本领域内关键信息基础设施的认定或撤销，地方政府部门与有关中央行政主管部门协商后对相关设施进行认定，信息通信基础设施保护委员会对认定事项进行最终审议，信息通信主管部门或国家安全部门对中央行政主管部门的认定工作提出意见建议。

二是明确关键信息基础设施认定需要考虑的因素。韩国在确定哪些信息通信基础设施可纳入关键信息基础设施范围时，将信息通信基础设施对国家和社会的重要性、设施遭受网络攻击等危害时对国家安全、经济和社会造成损害的程度及危害发生后的可恢复性等作为考量要素。

三是制定并公布关键信息基础设施清单目录。韩国将认定或撤销的关键信息基础设施以清单目录的形式在官方文件上予以公布，清单目录载明具体关键信息基础设施的名称、所属管理公司或其他组织、所涉主管部门、认定或撤销的理由等事项，并根据认定或撤销情况及时调整清单目录的内容。

5.2 完善网络安全认证机制

我国《网络安全法》第 17 条和第 26 条规定鼓励有关企业、机构开展网络安全认证等安全服务，开展网络安全认证应当遵守国家有关规定。第 23 条要求进行网络关键设备和网络安全专用产品安全认证或检测。

目前，我国相关行业、领域的产品、设备已有相关安全认证和检测制度，但如何在现有制度基础上，建立《网络安全法》框架下的更加协调、统一、高效的网络安全认证机制，还需要配套规定予以确定。韩国 ISMS 认证制度对我国网络安全认证配套规定应该明确的部分基本问题将有一定的借鉴意义：

一是确定网络安全认证的基本事项。韩国法律明确了纳入 ISMS 认证体系的认证对象的具体范围，规定由信息通信主管部门韩国未来创造科学部主管认证工作，制定统一的认证标准，明确认证的有效期。

二是确定网络安全认证相关机构的范围、机构职责、机构审查的具体事项。韩国由信息通信主管部门指定可进行 ISMS 认证的机构，为了保障对认证事项的有效顺利审查，还专门指定相关机构负责审查工作。

三是推进认证结果互认。韩国对已取得国际信息保护标准认证或具备符合规定的信息保护措施的企业，可免于再行认证。

四是加强事中事后管理。韩国重视对取得认证的企业的管理，明确认证机构承担相关管理职责，要求认证机构将事后管理情况向主管部门报告。对不符合国家标准、违反相关管理要求的已认证企业，建立撤销认证的退出机制。

5.3 健全数据跨境流动管理制度

《网络安全法》第 37 条确立了关键信息基础设施中个人信息和重要数据境内存储要求，因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

目前我国有关数据跨境提供的规定还比较简单，《网络安全法》上述要求还需要配套规定进一步细化。而韩国在此方面建立的基本制度也将为我国未来完善数据跨境提供相关要求提供可参考的立法经验：

一是区分数据的不同类型，分类施策。韩国针对个人信息、金融数据、相关重要数据等不同数据确立宽严有别的管理制度，并在此之上明确相应数据的跨境提供或转移的要求和例外规定。

二是对个人信息的跨境提供，韩国更注重保障信息主体的知情同意权，但存在无需同意的例外情形，如为履行合同、增进用户便利条件等必要性。

三是明确“重要数据”的定义。韩国采用行业领域描述加重要性列举的形式对重要数据加以界定，行业领域涵盖工业、经济、科学技术等，重要性因素则包括国家安全、科技进步等。同时明确禁止这类数据的跨境流动，相关主体应建立完备充分的、系统性、技术性的安全保障措施。

注释：

1.《国家网络安全管理规定》（National Cyber Security Management Regulation）为韩国国家网络安全中心（NCSC）于2005年1月31日制定，总统训令第141号颁布，最近一次修订为2013年9月2日，总统训令第316号修订，案文的韩文版见：http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2000000100482，2017年1月2日访问。

2.《信息通信网络的利用促进与信息保护等相关法》（Act on Promotion of Information and Communication Network Utilization and Information Protection, etc.）为2008年6月13日全面修订颁布（法律第9119号），在韩国一般简称为《信息通信网络法》。

3. 本文未特别指出的情况下，“关键信息基础设施”和“主要信息通信基础设施”两个用语在全文通用。

4.《信息通信基础设施保护法》（Act on the Protection of Information and Communications Infrastructure）为2001年1月26日制定颁布（法律第6383号），最近一次修订为2015年12月22日（法律第13590号修订），http://www.law.go.kr/LSW/lsSc.do?menuId=0&p1=&subMenu=1&nwYn=1&section=&tabNo=&query=□□□□□□□□%20그%20소속기관%20직제#undefined。其实施细则包括《信息通信基础设施保护法施行令》（2015年12月22日总统令第26728号修订）和《信息通信基础设施保护法施行规则》2013年3月24日未来创造科学部令第1号制定）。

5.《原子能设施等防护和放射性防灾对策法》（Act on Measures for the Protection of Nuclear Facilities, etc. and Prevention of Radiation Disasters）为2003年5月15日制定（法律第6873号）。

6.《云计算发展与用户保护法》（Act on Development of Cloud Computing and User Protection）为2015年3月27日制定颁布（法律第13234号），自2015年9月28日起施行。

7.《电子政府法》（Electronic Government Act）

为2010年全面修订通过（法律第10012号），旨在有效实现电子政务，增强行政能力、透明度与民主，并通过基本原则、程序、方法及其他行政事务电子化处理相关事项提升公民生活水平。

8.《工业技术泄露预防与保护等相关法》（Act on Prevention of Divulgence and Protection of Industrial Technology, etc.）旨在防止工业技术泄露并保护工业技术，以加强韩国工业竞争力、促进国家安全和国家经济的发展。

9.《信息通信基础设施保护法》第2条第2项规定，“电子侵害（electronic intrusions）”是指是以黑客、电脑病毒、逻辑或邮件炸弹、拒绝服务或高功率电磁波等方式对信息通信基础设施进行攻击的行为。

10.《信息通信网络的利用促进与信息保护等相关法》规定，“信息通信网络”是指利用《电信事业法》规定的电信设施和设备收集、处理、存储、搜索、传输、接收信息的信息通信系统，或计算机及适用的计算机技术。

11.《信息通信基础设施保护法》第2条第3项规定，“侵害事件（intrusion incident）”是指因电子侵害发生的事件情况。

12. 韩国各中央行政机关公布的主要信息通信基础设施的范围详见韩国行政自治部电子官报网页：http://www.moi.go.kr/frt/sub/a05/gwanboMain/screen.do。

13. 韩国信息通信基础设施保护委员会委员目前主要来自14个中央行政机关：企划财政部、未来创造科学部、外交部、法务部、国防部、行政自治部、产业通商资源部、保健福祉部、雇佣劳动部、国土交通部、海洋水产部、国家情报院、金融委员会、放送通信委员会（KCC）。

14.《个人信息保护法》第14条.

15.《个人信息保护法》第17条第3款。

16.《信息通信网络的利用促进与信息保护等相关法》第63条第1款。

17.《信息通信网络的利用促进与信息保护等相关法》第63条第2款。

18.《信用信息使用与保护法》第32条第6款第8项。

19.《金融实名交易与秘密保障法》第4条第1款第6项。

20.《信息通信网络的利用促进与信息保护等相关法》第51条。