For Improvement of Smart Home Appliance Security

2010

Smart Home Appliance Security Study Report

■ Challenges for and Approaches to Smart Home Appliance Security

■ Security Guide for Digital TV

Security Measures Matrix and Checklist

January 2011

Information-technology Promotion Agency, Japan

This guideline is available for download at:
2010 Smart Home Appliance Security Study Report
http://www.ipa.go.jp/about/press/20110201.html

<Contents>

<Figures and Tables>

1. Preface

1.1 Background, Challenges and Approaches to Solution

As embedded devices have become more and more networked, the ways they are used have changed as well. Smart home appliances are one of the fields affected by the course of events. The functions and convenience of home electronics have improved with their network connectivity and it has opened new chances for business for home electronics vendors. On the other hand, it also brought up security concerns and challenges as below:

1) Increase of security threats: Information security threats have been radically increasing due to the widespread use of all-purpose parts, general-purpose software and standard communications protocols such as TCP/IP and wireless LAN. The environment surrounding home electronics is becoming quite similar to that of the PCs and the same threats the PCs are facing may threaten the home electronics.
2) Approaches to secure home electronics: No common view has yet established in the home electronics industry and market over who (users or vendors) should take responsibility for implementing security (including the cost) to what level, and how to respond when a security incident does occurs.
3) Improvement of user literacy and awareness: The way to educate users and improve security awareness must be sought since it is necessary to change the user perspective and commonsense toward home electronics and build a consensus on the new era of smart home appliances.

Under this circumstance, Information-technology Promotion Agency (IPA) and the home electronics industry held 7 study group sessions to discuss the issues between March 2010 and December 2010, with the Ministry of Economy, Trade and Industry (METI) as an observer. The purpose of the study group was to clarify and share the challenges for smart home appliances that would become more popular and more networked, and create and develop a new market under a good harmony of vendors, users and necessary systems.

1.2 Overview and Meaning of This Report

This report summarizes the matters to concern, bottlenecks, challenges and approaches to solution, recommendations discussed in the study group sessions and provides a security guide for the digital TV as an example.

The chapter 2 discusses the matters to concern and security challenges for smart home appliances in general and how to approach them.

The chapter 3 presents a more concrete and detailed analysis on threats and security measures

focusing on the internet-connected digital TV, which has already been on the stores and is expanding its market. The functions, threats and countermeasures were covered exhaustively and neutrally. Some countermeasure must have already been implemented in the current smart home appliances. Nevertheless, they were included for the sake of completeness. IPA hopes that they will be used as a base to develop long-awaited security standards in this field.

Under the awareness that embedded device security would become an important issue, IPA has been working on the research and development of security guides for embedded devices since 2005 (refer to the reports on embedded systems and control systems[1] at IPA website). The following documents are especially related to this report and would be good supplement materials.

- Approaches for Embedded Systems Information Security (2010 Revised Edition)[2]:
  Security is a key issue for vendors when developing systems and products. The report provides guidance on organizational management and security measures during each phase of product lifecycle (planning, development, operation and disposal).
- Security for Devices with Embedded Software[3]:
  The report gives case studies of security incidents over the embedded devices and the overview of security efforts.

This report discusses security threats surrounding smart home appliances, especially the digital TV, and countermeasures against them in the concrete, and is expected to be used as a reference when vendors plan a product, consider and develop the necessary security functions.

It also aims to be utilized as a reference - a template to check the necessary security functions and a checklist for countermeasures to be implemented.

The chapter 3, Security Guide for Digital TV will need periodical update.

1.3 Study Group Members

7 study group sessions were held between March 2010 and December 2010. The following are the participants who gave approval to be published here.

Organization	Name (Titles Omitted)
SHAPR. Co.	Norio Ishikawa
	Takuya Ohkubo
	Kaoru Hieda
	Toshiyuki Tanaka
Sony Co.	Tadashi Morita
	Masakazu Kobayashi
Panasonic Corporation	Katsuhiko Tomita
	Kazuo Saiki
Hitahci Consumer Electronics Co., Ltd.	Yoshihiro Yamada
Mitsubishi Electric Corporation	Tadashi Fujishiro
IT Security Policy Office, Commerce and Information Policy Bureau, Minister of Economy, Trade and Industry <Observer>	Tomoharu Shimizu
	Haruka Naya
	Akio Sato
IT Security Center, Information-technology Promotion Agency	Hidehiro Yajima
	Hideaki Kobayashi
	Chisato Konno
	Manabu Nakano
	Tomoka Hasegawa
	Makoto Kayashima
	Yuji Ukai

2. Challenges for and Approaches to Solution for Smart Home Appliances Security

In 2010, the advanced functions of home electronics, such as access to the outside network and remote control via the Internet, were a hot topic in the news. While they make things convenient, the use application of the Internet-connected home appliances and their new functions is limited to certain uses because of the threats of cyber attacks that exploit their security vulnerability and possible information leak.

In what follows, the chapter 2 discusses the matters to concern and security challenges for smart home appliances observed in 2010.

2.1 Security Challenges for Smart Home Appliances

The security challenges to promote and expand the smart home appliances market are organized into the 4 aspects.

(1) Common Understanding on Security Threats and Necessity of Countermeasures

Security threats are attack methods to actualize the risk of incidents, such as the disruption of services provided by the functions or information leak. As the number of functions increase, so do the threats. It is not that the threats alone actualize the risk of incidents, but it is very important to take precautions against threats to mitigate the risks, for example, by identifying vulnerabilities and implementing security measures.

① Common Understanding on Security Threats

- As all-purpose parts are more and more used in the platform, a serious threat like arbitrary code execution is increasing.
- Including the network connectivity, the environment surrounding smart home appliances is becoming quite similar to that of the PCs and the same threats the PCs have been facing may threaten the smart home appliances as well.
- Security support for a product has a relatively short time limit due to some factors, such as the platform's product support period. How to cope with smart home appliances that are expected to be used for a long time of 10 years to 15 years is a challenge.

② Concerns and Bottlenecks of the Industry

- As a vendor, to what extent the vendor can ensure the safety and security of its product against the threats posed by the whole outside world.
- There needs to be a consensus on the liability of the vendor for information security incidents.
- Since misconfiguration can be a security threat, there needs to be a standard that defines what level of information should be provided in the manuals and instruction books.

③ Approaches: Security Standards, Guidelines and Certifications

- The concerned parties, including the users, will feel safe only if the industry has some kind of a

security standard developed and followed by the industry.

・There needs to be an guideline agreed by relevant parties that covers things like security measures, vulnerability response, checklist for selecting cryptographic algorithms.

・A system where a third-party certification body certifies a product's compliance with the aforementioned guideline would be desired. It is important to develop the system that ensures acquiring the certification is easy in terms of cost and timeline.

(2) Need for Formation of Smart Home Appliances Market

① Current Situation of Users

・Since most people believe that home electronics are safe, it is difficult to make the general consumers understand possible security threats to home electronics.

・A culture of understanding for the need of security has been nurtured in the PC market at long last. The user base for smart home appliances is both bigger and wider to propagandize.

・Security awareness for smart home appliances is not common, if not non-existence, and it is a challenge: how to explain, make the users understand, and improve their literacy.

・It is difficult to make the users see why security measures must be taken spending all that money for something they believe is safe.

② Bottleneck in Usage Phase

・Although ample information is provided in the instruction book, it is a question whether the users will and can configure the device appropriately.

・It is important to improve the user literacy for not only device operation but also for security response as in what to do when something happens to smart home appliances.

③ Response to Failure and Incident

・As a cause of failure or incident, a variety of things can contribute, such as misconfiguration, something related to using the Internet, remodeling and adding new functions. It is difficult to point out what did cause it and is necessary to make clear where the liability between the user and the vendor lies.

・The vendor needs to prepare for the case where a user is unaware of being attacked or being an attacker through his or her device that has been turned into a bot.

・Attacks that exploit vulnerability harm both the users and vendor. It is necessary to develop a framework to respond to vulnerability attacks, as to how to identify the attackers or how to follow up.

④ Approaches: Market Formation

・Explaining the users about the risks of and cautions in connecting to the Internet is tough to do by individual vendors. It is necessary to do as the industry.

・The product quality and vulnerability are essentially two other things. The industry needs to establish a common understanding on how to think about and accept security incidents caused by third parties who viciously exploiting vulnerability. Vulnerability is a security weakness in software and

applications that may impair the device's functions or capabilities when being exploited by attacks, such as unauthorized access and computer viruses [7].

(3) Need for Collaboration and Information Sharing in the Industry

① Industry Collaboration

・Explaining the users about the risks of connecting to the Internet is tough to do by individual vendors. It is necessary to do as the industry.

・Evaluating the severity level of vulnerability is tough to do by individual vendors. A common standard is required.

② Need for Information Sharing

・A place and framework where the industry members can share attack information and discuss the matters continuously is needed.

・A database of threat and vulnerability information that the industry can share and utilize neutrally is needed. Two databases, one for the developers and another for the users, should be set up.

(4) Leading and Developing the Market

① Leading the Market

・Even under the fierce competition for low price and high capability products throughout the global market, it is not good for both the users and market formation if the low-security smart home appliances which are the result of a cost-first, leave-security policy get into the market.

・It is a challenge to develop the receiving inspection plans to respond to the increased use of overseas OEM products.

② International Standard and Certification

・It is recommended to propose a security standard for smart home appliances to the international standards body, such as ISO, and establish a culture and trend where the certified products are selected by the users.

2.2 Approaches to Solution for Smart Home Appliance Security

To solve the challenges and concerns addressed in the section 2.1, each of the following should be needed in the future.

(1) Developing a security standard for smart home appliances

(2) Nurturing the market and improving literacy for smart home appliances

(3) Developing information database (DB)

(4) Promoting a security standard from a local to global de facto, international standard

Table 1 summarizes the challenges and concerns addressed in the section 2.1 and corresponding approaches for solution to be discussed in this section.

In what follows, the overview of the discussion held for each of the actions listed above by the study group is presented. The point of the discussion and supplementary information are added in Notes.

(1) Development of Security Standard for Smart Home Appliances

It is recommended to develop a security standard that the industry should follow. It is expected that the standard will establish a social consensus on the liability of the vendor. However, since threats and the extent of the impact are quite different depending on the product category and the coverage of the functions being equipped on the products, a category-specific standard is necessary.

① Information Security Standard for Smart Home Appliances

Define the following for each product category and function (level).

- Clarification of assets to be protected [Note 1)] and threats
- Security measures implemented in the product (the level and phase should be clarified)
- The security management system at manufacturing floor
- The contents and the level of the information provided in the instruction book.
- Operation scheme after release (vulnerability management)
- Support for new technology (such as IPv6)

Table 1. Challlenges for and Approaches to Solution for Smart Home Appliances

#	Challenge			Approach to Solution	
	Category	Items		Security Measure	Target
1	Common View on Security Threats and Necessity of Countermeasures	＜Threats＞ ・As all-purpose parts are more and more used in the platform, a serious threat like arbitrary code execution is increasing. ・Including the network connectivity, the environment surrounding smart home appliances is becoming quite similar to that of the PCs and the same threats the PCs have been facing may threaten the smart home appliances as well. ・Security support for a product has a relatively short time limit due to some factors, such as the platform's product support period. How to cope with smart home appliances that are expected to be used for a long time of 10 years to 15 years is a challenge.		Security Standard for Smart Home Appliance	Development of Security Standard for Smart Home Appliances
		＜Concerns and Bottlenecks of the Industry＞ ・As a vendor, to what extent the vendor can ensure the safety and security of its product against the threats posed by the whole outside world. ・There needs to be a consensus on the liability of the vendor for information security incidents. ・Since misconfiguration can be a security threat, there needs to be a standard that defines what level of information should be provided in the manuals and instruction books.			
		＜Approaches: Security Standards, Guidelines and Certifications＞ ・The concerned parties, including the users, will feel safe only if the industry has some kind of a security standard developed and followed by the industry. ・There needs to be an guideline agreed by relevant parties that covers things like security measures, vulnerability response, checklist for selecting cryptographic algorithms. ・A system where a third-party certification body certifies a product's compliance with the aforementioned guideline would be desired. It is important to develop the system that ensures acquiring the certification is easy in terms of cost and timeline.		Certification/ Recognition System	
2	Need for Formation of Smart Home Appliances Market	＜Current Situation of Users＞ ・Since most people believe that home electronics are safe, it is difficult to make the general consumers understand possible security threats to home electronics. ・A culture of understanding for the need of security has been nurtured in the PC market at long last. The user base for smart home appliances is both bigger and wider to propagandize. ・Security awareness for smart home appliances is not common, if not non-existence, and it is a challenge: how to explain, make the users understand, and improve their literacy. ・It is difficult to make the users see why security measures must be taken spending all that money for something they believe is safe.		Understanding of the Threats Posed by the Network Connectivity	Reflect to Product Lifecycle Market Formation (Vendors) ・ Improvement of Literacy (Users)
		＜Bottleneck in Usage Phase＞ ・Although ample information is provided in the instruction book, it is a question whether the users will and can configure the device appropriately. ・It is important to improve the user literacy for not only device operation but also for security response as in what to do when something happens to smart home appliances.		Informed Selection of Functions by User	
		＜Response to Failure and Incident＞ ・As a cause of failure or incident, a variety of things can contribute, such as misconfiguration, something related to using the Internet, remodeling and adding new functions. It is difficult to point out what did cause it and is necessary to make clear where the liability between the user and the vendor lies. ・The vendor needs to prepare for the case where a user is unaware of being attacked or being an attacker through his or her device that has been turned into a bot.		Things to Remember during Usage Phase (Including Disposal Phase)	
		＜Approaches: Market Formation＞ ・Explaining the users about the risks of and cautions in connecting to the Internet is tough to do by individual vendors. It is necessary to do as the industry. ・The product quality and vulnerability are essentially two other things. The industry needs to establish a common understanding on how to think about and accept security incidents caused by third parties who viciously exploiting vulnerability.		Establishment of a Flow for Incident Response	
3	Need for Collaboration and Information Sharing in the Industry	＜Industry Collaboration＞ ・Explaining the users about the risks of connecting to the Internet is tough to do by individual vendors. It is necessary to do as the industry. ・Evaluating the severity level of vulnerability is tough to do by individual vendors. A common standard is required.		Information DB for Developers	Development of Information DB
		＜Need for Information Sharing＞ ・A place and framework where the industry members can share attack information and discuss the matters continuously is needed. ・A database of threat and vulnerability information that the industry can share and utilize neutrally is needed. Two databases, one for the developers and another for the users, should be set up.		Information DB for Users	
4	Leading and Developing the Market	＜Leading the Market＞ ・Even under the fierce competition for low price and high capability products throughout the global market, it is not good for both the users and market formation if the low-security smart home appliances which are the result of a cost-first, leave-security policy get into the market. ・It is a challenge to develop the receiving inspection plans to respond to the increased use of overseas OEM products.		Standardization of the Security Standard	Global De Facto /International Standardization
		＜ International Standard and Certification＞ ・It is recommended to propose a security standard for smart home appliances to the international standards body, such as ISO, and establish a culture and trend where the certified products are selected by the users.		De Facto Standardization of Certification and Recognition System	

A mechanism that allows to select the required security level accordingly to the functions to be used [Note 2)] is desired.

For the first product category to go ahead with developing a standard, it seems appropriate to choose the digital TV (hereinafter called "DTV"), which has a leading market.

As a precedent industry-led security standard, there is the PCI DSS (Payment Card Industry Data Security Standard) [6] by the payment card industry.

Note 1) It is critical to specify the scope of the assets to be protected, such as limited to smart home appliances or including a service framework to support the device (like the dedicated portal site). The assets that should be protected include the user's information assets (for example, personal information, intellectual property right protected contents) and it is important to identify them.

Note 2) As for the functions to be used, security is broadly divided into 3 levels: no connection to the Internet, limited connectivity to the specific, trustworthy websites and free connectivity to the arbitrary websites. For example, there are the following 3 levels for the DTV.

A. A TV without Internet connectivity just like a traditional TV.

B. An Internet-safe TV that receives the services provided by a trustworthy server (in principle, the one provided by the TV maker)

C. A PC-type TV with which its access to the Internet is the responsibility of the user.

Internet connectivity can be enabled in a wired or wireless way and threats and security challenges are different for each of them. The security measures to be implemented and an operation scheme for the usage phase should be established for each way as well.

② Certification and Recognition System [Note 3)]

A mechanism to popularize and promote the compliance to the standard, the following requirements must be met.

- Comply with the business environment of the home electronics industry (such as global competition, long product lifecycle, short development cycle for new products).
- Make the cost and evaluation process reasonable.
- Make the certification system reasonably acceptable for the vendor's business development regardless of their size.
- Reflect the current condition surrounding the products (such as the level of its functions and the size of the market), set the levels of achievement from a self-declared compliance to a set of common rules (such as a checklist based on the standard) to acquisition of the certification and the use of certified mark for approved products.
- Establish a certification and recognition system operated by a third party.
- Make the worthiness of the accreditation clear for the users that the approved product has a good

value in reliability and safety.

Note 3) It evaluates and accredits a product's compliance to a predefined security standard and does not ensure security against the threats that may emerge in the future but unknown and unexpected by the current standard. The users need to be aware of it and understand it.

(2) Market Formation, Improvement of Literacy for Smart Home Applications

A mechanism to widespread the following ideas to overwrite the stereotype and preconception of home electronics (such as safe, operated by 24/7, no user maintenance required) is necessary. In addition, by this it is hoped to nurture a social consensus on the liability concerning smart home appliances.

In what follows, the matters to concern are addressed along the product lifecycle, such as product understanding, usage, disposal and incident response.

① Understanding of the Threats Posed by Network Connectivity

It is necessary to realize that smart home appliances will be exposed to the same threats as the PCs because of their network connectivity (in-house LAN, the Internet) and the use of external media. Taking into account that almost anyone can be the user of smart home appliances, it is important to find a mechanism to inform all possible users about the threats. The following means can be used to approach the users.

- Instruction book (clearly explain the functions and possible threats that come with using them)
- Pamphlet (materials to widely announce)
- Public website, education materials

② Informed Selection of Functions by User

A mechanism to establish and nurture a common understanding where the users understand the functions needed for them and possible threats to use the functions, and then select (enable) the functions on their own will (as part of their responsibility) [Note 4)].

- Terms and conditions regarding the contents and the level of information to be provided in the instruction book (such as danger, compliance requirements, countermeasures).
- A predefined rule to notify the vendor of the user's will to enable the provided functions (such as registering or enabling them on the service website).

Note 4) When confirming the users' will, make sure that the explanation is easy for the users to understand the functions and terms and conditions, and prevent the users from lightly clicking OK (or Agreed) when they do not in fact understand well enough.

③ Things to Remember during Usage Phase (Including Disposal Phase)

A mechanism is necessary to make the users aware of the things to abide and make sure that they do abide when using the device's network connectivity.

- Understand the necessity of security update (should be included in the instruction book as addressed in ②) and decide how to actualize the security update.
- Guide the users to update when they connect to the network or another option is to embed a mechanism to force it (as in allowing the access only via the service website (Trusted home))[Note 5].
- Provide a way to erase the information stored on the device when disposing.

Note 5) Concrete examples of the mechanism are given below.

- In North America, a pull-type, remote maintenance is actively adopted, but it is not in Japan.
- As for a device with a digital tuner, there is a mechanism to automatically update between broadcasts, but it requires that the power be on.
- On the game machines, the users cannot enjoy the service unless they upgrade the device via the Internet and the vendors successfully forcing the users to update.
- As for mobile phones, the carriers control device and patch management.

④ Establishment of a Flow for Incident Response

The vendors should prepare things like the following in case of security incidents.

- Terms and conditions regarding the contents to be provided in the instruction book.
- Contact Information
- Website

(3) Development of Information DB

Development of the information databases of vulnerability information, events and incidents, one for the product developers and another for the product users, and a mechanism to utilize them are needed. The former (DB for developers) is closely related to the above subsection (1) and the latter (DB for users) to (2).

① Information DB for Developers

For the products, since common platforms will be more and more used as their component parts, it is possible to use the JVN iPedia [4][5], which is a domestic vulnerability countermeasure information database. However, it is necessary to expand the scope of information to be collected by JVN iPedia and improve the usability (I/F) to encourage the developers of embedded devices and smart home appliances to use it [Note 6].

Note 6) With the current use situation and feedback from the developers for JVN (Japan Vulnerability Note)[4][5] in mind, an additional discussion to how to support smart home appliances is needed.

・The use of open source software is increasing, but not much information has been reported to JVN.
・There are some cases where the information is directly obtained from the parts makers.

② Information DB for Users

As for the individual parts, necessary information will be disclosed on the website of each parts maker when needed. For this DB, it is required to collect information about possible attacks against smart home appliances based on the incidents experienced by the PCs and smart phones. The DB for the general consumers must be simple to access, easy to understand, well-recognized and supported and shared by the industry.

・Vulnerabilities of and threats to smart home appliances in general or those common to product categories
・Events and Incidents that the users should be apprised of
・Know-hows to respond to incidents

(4) Global De Facto/International Standardization

At the current initial stage of development of smart home appliances, it will be valuable to take the lead in developing a security standard and promoting its international standardization in the field.

① Standardization of the Security Standard

By developing a security standard and following it by the industry, it is possible to make it a de facto standard and encourage the international standardization of the standard.

② De Facto Standardization of Certification and Recognition System

To make the standard a global de facto standard, the following actions can be suggested.

・Establish a culture and trend where the certified products are selected by the users.
・By promoting secure smart home appliances, enable the vendors to provide not only secure but also more high value-added services to the users.

3. Security Guide for Digital TV

Focusing on the DTV, an approach to develop a security standard addressed in the previous chapter is discussed in more detail in this chapter. The following sections list the possible threats and countermeasures that are covered exclusively based on the functions of the DTV. IPA hopes the guide is used as a baseline/reference when the vendors implement the necessary security measures to their products or develop their own security standard.

Compared to the traditional TV, the DTV is added with a various IT functions, such as the availability of using external media, built-in disk, LAN connectivity and Internet connectivity. Because of that, the same threats as the PCs have been facing may threaten the smart home appliances as well.

Depending on the IT functions added to the DTV, the new threats will emerge and countermeasures against them are required. Thus, although the DTVs are all DTVs, the necessary security measures will widely differ depending on the functions equipped on each DTV. Here, we take an approach to clarify the overall correlation between the IT functions, possible threats and required security measures. The section 3.1 lists up the IT functions on the DTV, and then possible threats and security measures are listed in the section 3.2 and 3.3, respectively, and the correspondence and correlation among them is summarized in the Table 2.

3.1 IT Functions of DTV

The Figure 1 shows the image of the overall DTV system framework. In this figure, the functions of the traditional TV that uses broadcast wave are called the home electronics functions (AV functions) and those newly added to the DTV that use the Internet and various media are called the PC functions (IT functions) to make the difference clear.

In what follows, the IT functions added to the traditional TV is explained. Here, the traditional TV functions (such as receiving pictures, displaying pictures, management functions) are called the basic functions in the Table 2.

＜→: Corresponding to the item number for the lower half of the Table 2＞

(1) Use of External Media

① Built-In Drive ＜→A1＞

An optical drive to read external media such as DVD.

② General-Purpose Interface ＜→A2＞

A media connectivity through the general-purpose external connection interfaces, such as USB (Universal Serial Bus) and Ethernet.

(2) Built-In Storage Media　＜→ B＞

An embedded HDD (Hard Disk Drive).

(3) LAN Connection

① Wired LAN　< → C1>

A wired home LAN connected through IEEE802.3X (Ethernet) or PLC (Power Line Communication). Devices such as other home multimedia devices, printers and PCs are supposedly connected.

② Wireless LAN　<→ C2>

A wireless home LAN connected through IEEE802.11X, Bluetooth, or ZigBee. Devices such as other home multimedia devices, printers, PCs and home switches are supposedly connected.

(4) Internet Connectivity

①Specific Websites Only　<→ D1>

An Internet connectivity that allows to connect to only the specific websites or the website via the specific websites.

② Arbitrary Websites　<→ D2>

Just like for an ordinary PC, it is an Internet connectivity that allows to connect to arbitrary websites. To filter the websites, the users can use a filtering service provided by their ISP.

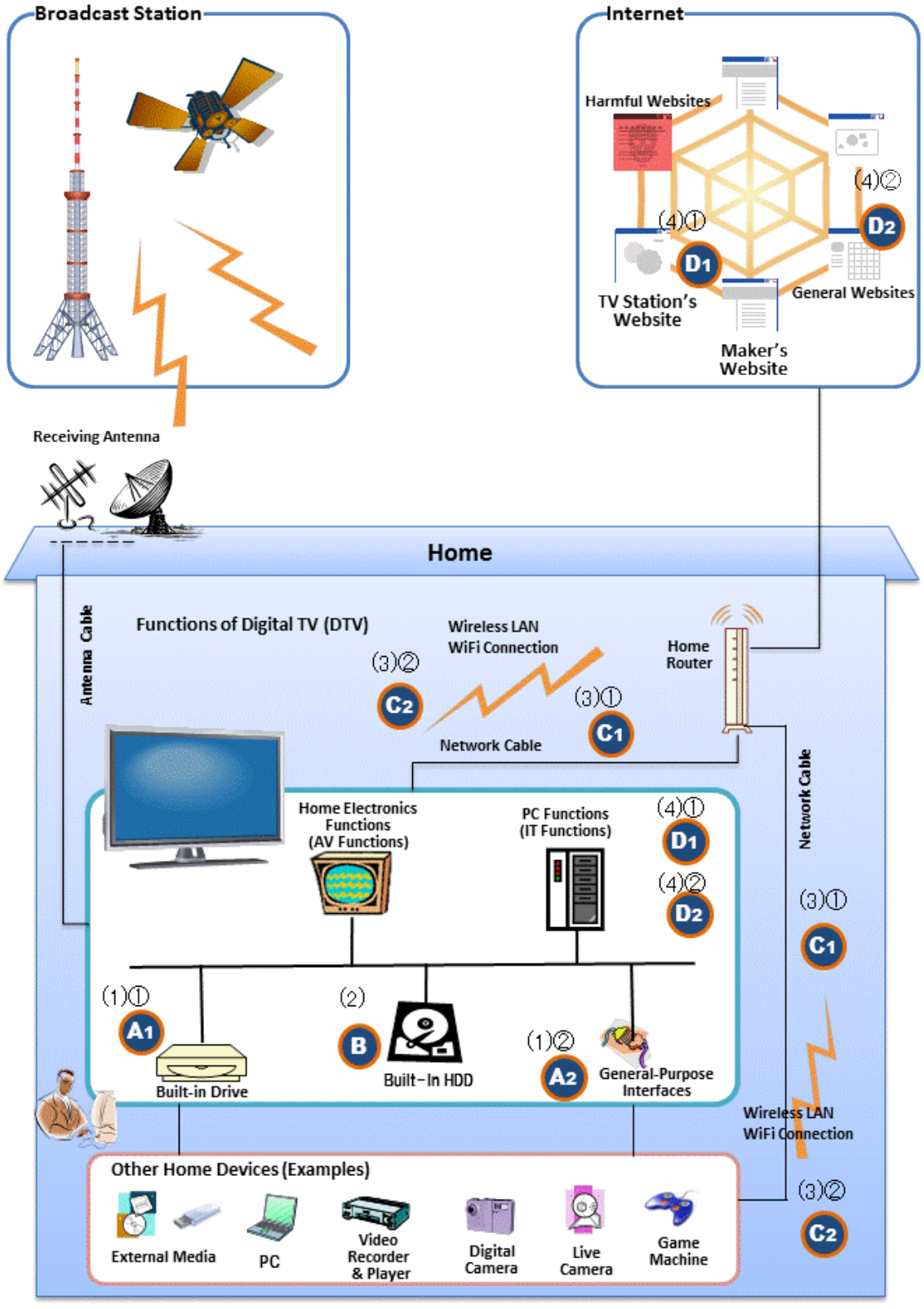

Figure 1 Image of Overall Digital TV System Framework

NOTE: (n)○ refers to a subsection of the Section 3.1,
and (A1)-(D2) refer to a corresponding No. in the Table 2 in the Section 3.4.

3.2 Possible Security Threats for Digital TV

Figure 2 shows the possible threats mapped on the functions of the DTV.

As more IT functions are added to smart home appliances, possible security threats become the same as the PCs with the Internet connectivity. Note that threats we are going to discuss here are limited to the primary threats. Thus, the secondary threats that may be caused by some primary threats, such as information leak caused by unauthorized access or eavesdropping, are not included as a primary threat.

In this section, threats are categorized and listed by functions and locations that may pose the risks, such as threats from the use of media, user operation, at home or via network.

(1) Threats from the Use of Media

① Virus Infection

Virus infection may occur due to a virus or malicious software (malware) included in the contents stored on the media.

(2) Threats from User Operation

The threats posed by user operation throughout the device's lifecycle can include the following:

① Misconfiguration

In a case such as where security parameters are configured inadequately when using wireless LAN or the Internet, it will increase the threats of eavesdropping and unauthorized access.

② Operation Error

Due to operation error of the available functions, there may be a case where the user may unintentionally disclose information (for example, sending an email to a wrong recipient or attaching a wrong file).

③ Information Leak of Stored Contents

The contents stored on the DTV by the user may be disclosed. It may happen through various ways and scenes, such as unauthorized access to the device or via network or when the contents are sent via network or when the data are left undeleted at the time of disposal.

④ Information Leak of User Information

The user information stored on the DTV may be disclosed. The user information means all the stored information that is created by the user and operation of the DTV, including personal information (personally identifiable information), confidential information (secret information such as ID and password) and privacy information (the data that may reveal something about the user, including operation log and service usage history). It may happen through the same ways and scenes described in ③.

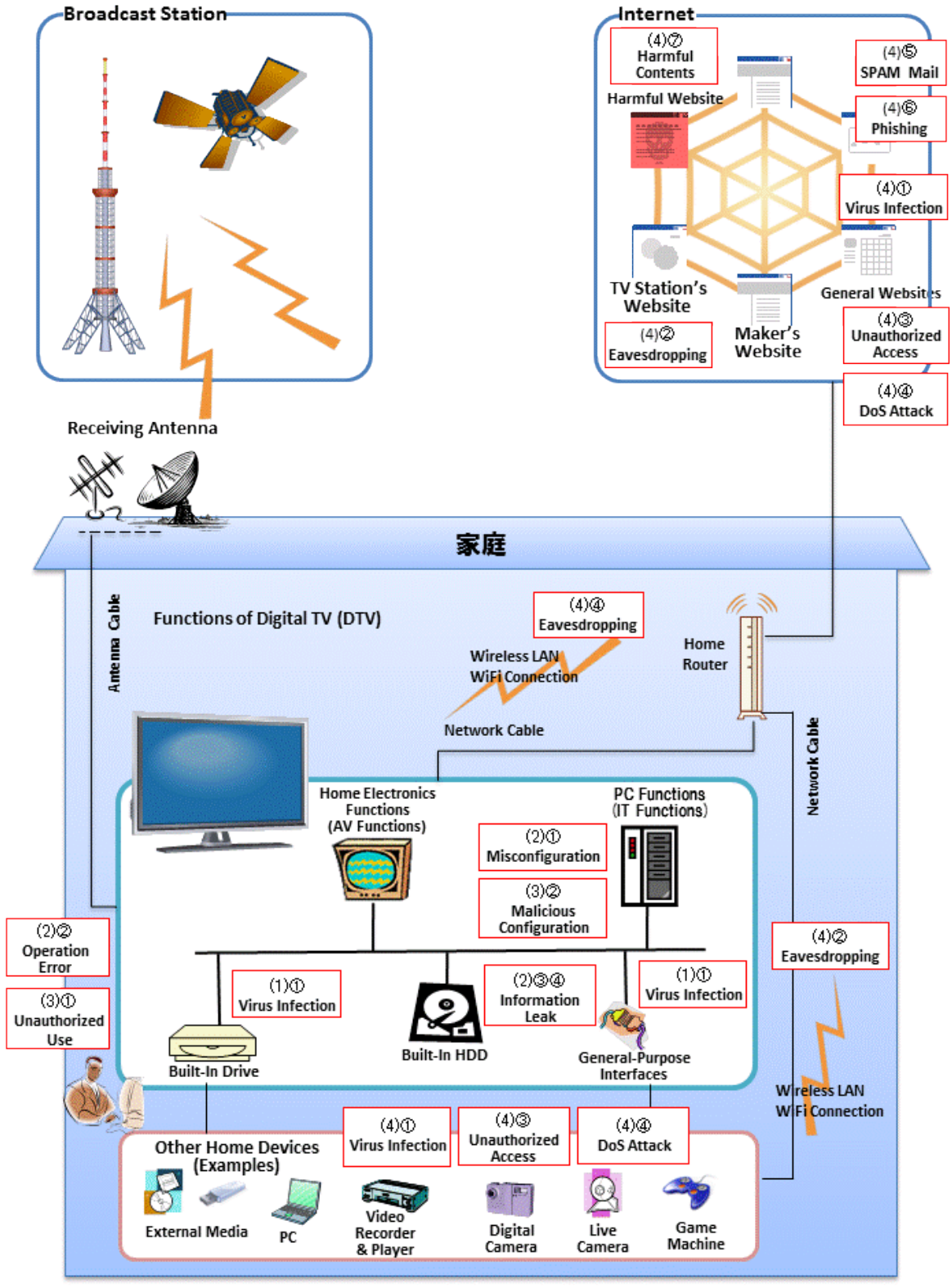

Figure 2 Whole Picture of Threats to Digital TV

NOTE 1: (n)○ refers to a subsection of the section 3.2.
NOTE 2: Not all threats are presented in the figure due to the space limitation. For complete information, see Table 2.

(3) Threats at Home

① Unauthorized Use (Spoofing)

Someone besides the authorized user may access the device. It can be not only the family members who live together, but also intruders.

② Malicious Configuration

When someone intrudes home or a serviceman accesses the device for repair, they may configure the device or install programs without the user's agreement.

(4) Via Network/on the Internet

① Virus Infection

The device may be infected with viruses when sending and receiving emails, accessing the websites and downloading the contents through the Internet.

② Eavesdropping

The communications between the DTV and other media devices at home or between the DTV and external web servers or broadcasting stations may be snooped or intercepted.

③ Unauthorized Access

The device may be attacked through port scan, exploiting vulnerability or spoofing to steal information or destroy the system.

④ DoS (Denial of Service) Attack

The device may be overloaded with malicious requests to disrupt the services or to shut down the system.

⑤ Spam Mail

The user may receive an endless stream of malicious or unwanted email via the Internet. It will not only hinder the usability of the Internet but also cause a secondary threat like virus infection and phishing.

⑥ Phishing

When using a web service, the user may be lured to a malicious website that is spoofed as the legitimate website that provides the expected service. The malicious website aims to steal confidential information or infect the user's device. Attackers often trap the users using spam mail addressed in ⑤. Since smart home appliances are used by elderly people and small children more than the PCs, it is concerned that the risk of their falling into a victim may be greater than that with the PCs.

⑦ Access to Harmful Contents

The users may be presented with undesired contents (such as pornographic images) or the family members may be unintentionally allowed to access harmful contents.

(5) Threats for the Portal Site

They are not the threats for the DTV itself but for the web server that provides the DTV services (operated by the DTV vendor). However, since the DTV connects to those services via the service website, they expose the DTV to the indirect threats through infection or alteration of the websites.

① Spoofing of Device and User

An unauthorized device or user may spoof the legitimate device or user and access the service websites. A spoofed device will expose the website to the threats of cyber attack and a spoofed user will bring up the threats of unauthorized use of the services and contents.

② Same Threats as the General Web Services

Since the digital broadcasting service works like a service provider and a web service, the threats such as DoS attack, unauthorized access, virus infection, eavesdropping, spam mail and phishing will apply as well. Also, attacks exploiting vulnerability in web application (such as cross-site scripting and SQL injection) will pose the risk and may cause virus infection and information leak.

3.3 Security Measure against Threats

In what follows, countermeasures against a various threats to the DTV are explained.

＜→: Corresponding to the item number for the upper half of the Table 2＞

(1) Vulnerability (Security Patch) Management ＜→ 1＞

It is a measure to apply security patch for OS, middleware, applications installed in the device. For the DTV, mainly the following functions can be required the management.

・Home electronics functions (AV functions)

・PC functions (IT functions)

Security patch can be obtained and applied in a several way, such as through broadcast waves or the Internet. In the case of using broadcast waves, it is distributed during the hours when the users likely do not using the services, such as in the small hours. In the case of using the Internet, if there is a specific service website, the service provider can let the users know that they need to update the software and guide them to the updating service when they access the website, or make the services unavailable unless software is updated.

(2) Firewall (FW) ＜→ 2＞

There are two ways to implement firewall on the DTV side.

① Specifying IP Address to Connect (Route Control)

If the services are provided at the specific IP addresses, the DTV can be configured in a way that only communication with those specific IP addresses is permitted.

② Preventing Unauthorized Access

By filtering, the users can limit the ports to only those needed for the use of the services.

(3) Anti-Virus Measure ＜→ 3＞

Anti-virus measure can prevent virus infection through removable media and the network (both in-house LAN and the Internet). As for pattern file update, if the DTV is connected to the Internet, update it through the Internet.

(4) IDS/IPS (Intrusion Detection System/Intrusion Protection System) ＜→ 4＞

IDS/IPS can detect and prevent unauthorized access and attack based on the signatures and rules. Client security tools available for the PCs can be also used when connecting the Internet. As for rule and pattern file update, if the DTV is connected to the Internet, update it through the Internet like the PCs.

(5) Communication Path Encryption (VPN (Virtual Private Network)) <→ 5>

The following information exchange can be candidates to be encrypted.

① Information exchange between the DTV and other home devices via wired/wireless network.

② Information exchange between the DTV and outside web services via the Internet.

③ Information exchange with the outside world using DTV

As for ①, if using a wired LAN, the risk of eavesdropping could be low just like for other home electronics since it is an in-house network. If using a wireless LAN, however, a strong encryption should be used when using the encryption function built in the wireless LAN considering the risk of eavesdropping. When providing a wireless LAN service, it is critical to warn the risk in the instruction book.

As for ②, it is common to protect the communication path using an encryption function on the server providing the services, such as SSL/TLS (Secure Socket Layer/ Transport Layer Security).

As for ③, it could happen through information exchange via email, and in that case, the same countermeasures expected for the PCs should be taken. For example, the users can encrypt the information to be sent, perform email encryption like S/MIME (Secure / Multipurpose Internet Mail Extensions) and PGP (Pretty Good Privacy).

(6) Authentication

① Device Authentication <→ 6>

It is a function to authenticate the DTV itself. It is mainly used by the server side that provides the services to authenticate a connecting DTV to see if its access is legitimate. It can be implemented in several ways, such as using the ID unique to each DTV, a USB key (to be inserted) or IC card, or built-in security chip (TPM (Trusted Platform Module)). Note that an ID can be spoofed and may not achieve its purpose of authenticating the device itself.

② Software Authentication <→ 7>

It is a function to authenticate software to be installed to the DTV. It is used to see if an add-on software installed to the DTV is authentic to prevent installation of malicious or prohibited software. It can be implemented by using a digital signature to the program. If a strict authentication is required, a PKI (Public Key Infrastructure) authentication can be used.

③ User Authentication (for Devices) <→ 8>

It is a function to authenticate the users to use the DTV. It is important to authenticate the users to prevent unauthorized use or see if the user is indeed the said user when doing a special operation such as installing external software. For a device for in-house use, ID/PW is commonly used.

④ User Authentication (for Services) <→ 9>

It is a function of the server that allows the web services to authenticate the users when they access the services using the DTV. Although how it is implemented depends on the service provider, generally a preregistered ID/PW or if the services involve a contract or purchase, a credit card number, specific equipment (such as one-time password generator) or PKI can be used. In other word, it is the same as

when using the online services with the PC.

⑤ Authentication of Connecting Server　<→ 10＞

When it is necessary to ensure the connection between the server of a particular website or broadcast station, authentication of the connecting server can be used. It can be implemented by pre-installing the server certificate of the server the user wants to access in the DTV. The services that require downloading software or exchanging important information, authentication of the server can be used.

(7) Content Encryption　＜→ 11＞

It is an encryption function for stored information and can be used for copyrighted contents or user information stored on the device. With encryption, the encryption keys and how to store and manage the keys are critical when considering the security measures.

(8) Data Erasure Tool　＜→ 12＞

It is a function to erase the stored information. It is used for both HDD and flash memory to prevent information leak from a discarded device after its disposal. There are several ways to erase the data, such as overwriting with random numbers (multiple times), destroying the disk or applying a strong magnetic field. For home electronic devices, overwriting with random number is most common.

(9) Filtering Tool

① Web Filtering　＜→ 13＞

It is a function to filter information that is downloaded from the outside when the web services are provided through the Internet With this function, access to the harmful websites and virus infected websites can be filtered. Usually, filtering is implemented using a database of URLs. The function will not be implemented on the DTV itself and is provided as one of the network services.

② Email Filtering　＜→ 14＞

It is a function to filter email from the outside when the email service is provided through the Internet. With this function, spam mail, phishing mail, mail attached with the virus-infected attachments can be filtered. The function will not be implemented on the DTV itself and is provided as one of the network services.

As for outbound email, there is a risk of information leak but no countermeasure is implemented for the devices used as home electronics just like the PCs.

(10) Instruction Book　＜→ 15＞

By including the possible threats and what to do when an incident happens, and organizing them along the device's lifecycle (start of use, operation and disposal) in the instruction book, The vendor

should mitigate the threats and guide the users to solve the problems during the period of usage.

- How to avoid misuse
- How to select the functions
- How to configure security parameters
- How to maintain security (such as vulnerability management)
- How to respond to malfunction, failure and security incident
- How to dispose

3.4 Correlation of IT Functions, Security Threats and Countermeasures

The Table 2 shows the correlation among the IT functions, possible threats and security measures discussed in the previous 3 sections (3.1 - 3.3).

The table is organized in a following way:

① The IT functions are listed vertically on the second left column of the lower half of the table.

② The Threats are listed horizontally on the lower central line of the table.

③ The countermeasures are listed vertically on the second left column of the upper half of the table.

Their correlation - start with an IT function equipped on the DTV (①), the possible threats to the function (②) and the countermeasures against the threats (③) - is indicated with the following signs.

・For the function-threat matrix (the lower half of the Table 2), each sign indicates the possibility that the threat would emerge by implementing the selected IT function as below:

○ : high, △ : low, Blank : none

・For the threat-countermeasure matrix (the upper half of the Table 2), each sign indicates the effectiveness of the countermeasure as below:

○ : effective, △ : partially effective, Blank : N/A

In what follow, the judgment behind ○ and △ used for each correlation between the IT functions and threats, and the threats and countermeasures in the Table 2 is explained.

(1) IT Function and Threats (＜ ＞ indicates the item number for a function, and underline for the item number for a threat in the Table 2)

The basic functions mean those of the traditional TVs (such as receiving pictures, displaying pictures, management functions). For these functions, misconfiguration, operation error, information leak of user information, such as operation log and personal information created by the users, and malicious configuration by someone at home are a possibility, and each threat is marked with ○ in the table.

In what follows, the possible threats to the IT functions listed the section 3.1 are explained.

① Use of External Media/Built-In Drive ＜A1＞

The DTV uses external media such as DVD and Blu-ray disk, via the built-in drive. In these cases, virus infection when reading the contents into the internal disk or information leak of stored contents when copying them to the external media are possibility threats.

② Use of External Media/General-Purpose Interface ＜A2＞

Virus infection when reading the contents into the internal disk through the use of external media such as USB memory stick and other AV devices, information leak of stored information when copying the internal contents to the external media, virus infection by connecting virus-infected devices, DoS attack, unauthorized access are possible threats.

Table 2. Threats and Countermeasures based on Features on Digital TV

○ : countermeasure is effective　△ : countermeasure is partially effective　(blank) : N/A

15	Cleary Explained in Instruction Book			○	○	○	○				○ Wireless LAN								
14	Filtering Tool	For Email												○	○ email			○	Provided as one of the network services
13		For URL								○					○ site access	○		○	Provided as one of the network services
12	Data Erasure Tool					○ disk	○ flash												For both flash memory and disk
11	Content Encryption					△	△					△						○	
10	Authenti-cation	Connecting Server								△					○	△		○	
9		User (for Services)				△ via network	△	○	○							△	○	○	User authentication on the service provider side
8		User (for Devices)				○	○	○	○							△			User authentication for the use of the device (login)
7		Software	○							○									Authentication for software (including drivers) to be installed in the device
6		Device										△					○		Client authentication on the service provider side (e.g. device ID, TPM)
5	Communication Path Encryption (including VPN)										○							○	Provided by one of the website / network services
4	IDS/IPS									△		○	○					○	Mitigate viruses using virtual patch
3	Anti-Virus		○							○								○	
2	Firewall											○	○					○	e.g. Port control, IP address control
1	Vulnerability (Security Patch) Management		○							○		○						○	e.g. Satellite distribution, through terminal

Countermeasure / Threat (primary) / IT Function			Media	User Operation				Home		via Network							Portal Site		Note
			Virus Infection	Mis-configuration	Operation Error	Information Leak of Stored Information: Contents	Information Leak of Stored Information: User Information	Unauthorized Use (Spoofing)	Malicious Configuration (intrusion, repair)	Virus Infection	Eaves-dropping (on the net)	Unauthorized Access	DoS Attack	Spam Mail	Phishing	Access to Harmful Contents	Spoofing of Device & User	Same Level of Threats as General Web Services	
	Basic Function (DTV Function)			○	○		○		○										
A1	Use of External Media	Built-In Drive	△			○													e.g. optical drive such as DVD
A2		through General-Purpose Interface	△			○				△		△	△						e.g. USB, Ethernet (IP)
B	Built-In Storage Media					○	○												e.g. built-in HDD
C1	LAN	Wired								△	△	△	△						Connection between devices via LAN cable
C2		Wireless		○						△	○	△	△						Connection between devices and home router
D1	Internet Connec-tivity	Specific Websites		○	△	△ via network	△ via network	△	△	△	○	△	△	△	△	△	○	○	Mitigate the risks on the website (server) side
D2		Arbitrary Websites		○	△	○ via network	○ via network	○	△	○	○	○	○	○	○	○	—	—	

○ : possibility is high　△ : possibility is low　(blank) : possibility is none　: N/A

③ Built-In Storage Media ＜B＞

Storage media hold a wealth of contents and user information. Through unauthorized access to those data or by neglecting deletion of data at the time of disposal, information leak of stored information may occur.

④ LAN (Wired and Wireless) ＜C1, C2＞

When using LAN, virus infection by connecting virus-infected home electronics or the PCs, DoS attack, unauthorized access and eavesdropping are possible threats. Yet, the threats posed by the in-house devices or wired network are considered low. When using wireless LAN, however, eavesdropping of radio waves outside the house is a seriously possible threat, and misconfiguration (which protocol to use or security parameter setting) can also be a big threat. For that, wireless LAN is marked with ○ in both threats.

⑤ Network Connectivity (Specific Websites Only) ＜D1＞

As for the threats from user operation, from connecting to home switch (including via wireless LAN) to using the Internet services, misconfiguration, operation error, information leak of stored information via the Internet are possible threats. Considering that wireless LAN may be used, misconfiguration is marked with ○, and other threats are marked with △, since the connecting IP addresses and the web service providers are identified and limited.

Within the home network, unauthorized use or malicious configuration by someone can be possible threats but the risk is considered low.

When using the Internet, the DTV is expected to face the same threats as PC. Namely, virus infection, DoS attack when using the server functions, unauthorized access, eavesdropping, spam mail, phishing, access to harmful contents are possible threats. Nevertheless, since the connecting IP addresses and the web service providers are identified and limited, the risk is marked as △ except eavesdropping. Eavesdropping is marked with ○ because it is commonly possible when using the Internet.

As for the portal site side that provides the services, spoofing of devices and users is a possible threat, and the same level of threats as the general websites providing services on the Internet should also be expected. If neglecting the countermeasures against the same level of threats as the general websites, that will indirectly endanger the DTV that connects to the services and may result in that the threat level (△) on the DTV side is unassured.

⑥ Network Connectivity (Arbitrary Websites) ＜D2＞

When connecting to arbitrary websites, the possible threats are the same as ⑤. However, since the connecting IP addresses and web service providers expand, the risk of threats increases and thus information leak of stored contents and other threats possibly occur addressed in ⑤ are changed from △ to ○.

(2) Threats and Countermeasures ([ ] indicates the item number for a countermeasure in the Table 2)

① Virus Infection through Media

To counter virus infection, anti-virus software against malicious software and virus-infected contents downloaded from the media [3], vulnerability management to prevent virus and malware from exploiting vulnerability [1], software authentication to confirm the authenticity when installing software [7] can be performed.

② User Operation (Misconfiguration, Operation Error)

As for misconfiguration and operation error, it is important to make the instruction book easy for the users to understand [15] to have them use the device correctly and improve the user literacy.

③ Information Leak of Stored Information (Contents, User Information)

To counter information leak, access control and content protection, and proper erasure of information can be performed.

For the former, user authentication that authenticates the users who access the device and information [8], content encryption that protects information itself in case of unauthorized access [11] can be done. In addition, to mitigate the risk of information leak, user authentication that authenticates the users who access the services [9] can be also performed.

For the latter, data erasure tools to delete the stored information at the time of disposal [12], and making sure to include the things that the users should do when disposing the device (such as deleting the data with a data erasure tool) in the instruction book [15] can be done. As for data erasure tools, if the data are stored in multiple locations such as HDD and flash memory, the tools that will erase the data in all locations are provided.

④ At Home (Unauthorized Use, Malicious Configuration)

To counter unauthorized use and malicious configuration at home, use user authentication to authenticate the users who uses the DTV. User authentication when using the device [8] and user authentication when using the services on the Internet [9] can be used. Although the latter is a function implemented on the server side that provides the services, if the authentication uses some mechanism or another device instead of ID/PW, the DTV needed to be able to support them.

⑤ Via Network (Virus Infection)

To counter virus infection, anti-virus software against the contents and email infected with virus [3], vulnerability management against virus attack via the Internet [1], and IDS/IPS [4] can be performed. [4] can counter the viruses for which pattern files are not yet distributed or it will also works for the variants.

For securing software download, software authentication that confirms the authenticity of the software [7] can be used. To mitigate the threats posed by arbitrary websites the device may connect to, server authentication [10] and URL filtering can be used to avoid to connect to the websites that are likely infected by malware.

⑥ Via Network - DoS Attack

To mitigate DoS attack, firewall that filters the service ports and packets used by the service [No.2], IDS/IPS that detects and discards malicious packets [No.4] can be used. If the source of attack is known, it is possible to discard malicious packets with the combined use of No. 2 and No. 4, but if the attack is coming from an unspecified number of unidentified sources, it is difficult to respond. Be that as it may, it seems unlikely that a DDoS (Distributed Denial of Service) attack is launched against a server for personal use.

⑦ Via Network - Unauthorized Access

To mitigate unauthorized access, firewall that filters the service ports and packets used by the service [No.2], vulnerability management [No.1], IDS/IPS that detects and discards malicious packets [No.4] can be used. In addition, as an insurance, in a case where unauthorized access does happen, data encryption that protects the information [No. 11] can be performed. When using LAN, authentication of connecting devices [No. 6] is also a security option (such as MAC (Media Access Control address) authentication), but it is not commonly done for home network environment.

⑧ Via Network - Eavesdropping

To mitigate eavesdropping on the networks, communication path encryption [No.5] can be performed. There are various ways to encrypt communication path depending on from where to where and techniques to encrypt (refer to 3.3(5)). When using wireless LAN, it is necessary to be clearly explained how to select an encryption method for wireless LAN in the instruction book [No. 15]. Also, when configuring the encryption strength for wireless LAN, some thought should be put into making the default setting a strong one.

⑨ Via Network - Spam Mail

Spam mail receiving from the email service may indirectly cause virus infection, phishing or other bad things. To mitigate the risk, email filtering [No. 13] can be used but it is usually provided by the IPS as one of its services.

⑩ Via Network - Phishing

To mitigate phishing attack, the users should check the URL he or she intends to establish a connection to on the DTV as a basic measure. In addition, in case the users neglects it or it does not

work, there are a few other countermeasures to mitigate the risk.

Email filtering [No. 13] can be used to block emails that may lead to phishing such as spam mail. Also, URL filtering [No. 14] that makes sure that the websites the user is trying to connect are not on the blacklist or server authentication of the websites [No. 10] can be used. These are usually provided by the IPS as one of its services.

⑪ Via Network – Access to Harmful Contents

To prevent access to harmful contents by the users and their family members, user authentication to use the device [No. 8] and to use the services [No. 9] to control access to the device and services can be performed. In addition, to prevent carelessly connecting to harmful websites, server authentication of the websites [No. 10] or URL filtering [No. 14] can be performed.

⑫ At Portal Site Side

For the security measures for the portal sites, the security measures implemented in the general web services are shown in the Table 2. Other security measures excluded in the Table 2 are listed below.

・The use of WAF (Web Application Firewall)[8] to mitigate attacks that exploit web application vulnerability.

・Adopting a redundant system architecture to ensure service availability.

3.5 References for Product Design <Template and Checklist>

As mentioned in the previous section, it is possible to look up the security measures for the DTV based on the IT functions using the Table 2 by looking up possible threats in the crosswise direction and then looking up the countermeasures against them in the longitudinal direction.

There will be 2 ways to use the table.

- Using the table as a template for the security planning
- Using the table as a checklist for the security functions of a product

(1) Using the Table as a Template when Planning and Designing a Product

In this case, the table can be used as a template to consider what security functions need to be implemented when planning and designing a product.

Focus on the functions that are going to be equipped and check the threats for the functions marked with ○△ in the crosswise direction, and then look up the security countermeasures against the threats marked with ○△ in the longitudinal direction to mitigate the threats.

Consider what kind of security functions to built in to actualize each security measure marked with ○△ or for some threats, the conclusion may be that it is not worth to implement a security measure since the risk is acceptable. For the details on the threats and security measures listed in the table, refer to the section 3.2 and 3.3, respectively, and decide what kind of security functions to implement.

(2) Using the Table as a Checklist for Security Functions of the Current Products

In this case, the table is used as a checklist to look up the threats and security measures marked with ○△ that should be taken care of in the current products and see what kind of security measures are actually implemented. For each threat and countermeasure, if a product has a corresponding security function, examine the security level. If it has no security function, examine if the reason behind it is valid.

In addition, it is possible to use the table to explain to the user (purchaser) of the DTV about the possible threats that they should be aware of for using the IT functions in the product or help the users understand the security measures implemented in the product by attaching the table (or a modified version) to the instruction book. It can be used as an index to look up where to find about threats and countermeasures in the instruction book. It is important to provide the users with explanation and information on threats and security in an easy-to-understand way as much as possible.

3.6 Supplementary Note

This report has aimed to look at smart home appliances and the DTV in general (independent of specific products or functions) and list up threats and security measures to mitigate threats. Added below are issues that have been pointed out in the study sessions and need to be discussed further.

(1) DTV System Architecture (Structure)

Common to all smart home appliances, the AV system (home electronics functions) and the IT system (PC functions) coexist in the DTV and that brings up the following challenges for each system.

・Difference in the literacy level needed for the users for each system (such as security awareness and know-hows)

・Difference in expectation for the product lifetime (in general, 10 to 15 years for home electronics and 5 years for PCs)

・Difference in the threat level that each system are exposed to

How to help the users and solve these challenges will be key issues. Most of the concerns and bottlenecks addressed in the section 2.1 stem from this coexistence. Thus, seeking a way to separate them is a possible approach for solution but pursuing that path will be a trade-off with convenience, usability desired for smart home appliances and cost.

Security measures listed in the section 3.3 and 3.4 are those that can be implemented additionally, by installing another security functions or using some external security solutions. Meanwhile, reviewing the architecture of the DTV itself could also be an option that would tackle the fundamental cause. By logically separating the AV system and IT system, the security threats to the AV system will be mitigated. However, it depends on the functions and service level of the DTV and steps into a scope of the functions of individual product, which is not the scope of this report.

(2) Threats When Receiving Digital Broadcasting

As for digital broadcasting services, since the details, including what kind of information are exchanged and to what extent should the security threats be expected are still unclear at this point, they are not included in the threats addressed in the section 3.3 and 3.4. The possible threats can be as below:

・At the time of receiving digital broadcasting data

If the digital broadcasting data include malicious scripts, attacks or malicious acts through execution of the scripts may be performed.

(3) Verification of Threats to Digital TVs

Until the previous chapter, we have discussed the threats to the DTV that stem from the fact that the DTV is now equipped with the IT functions and network connectivity just like the PCs. Currently, the microprocessors, operation systems and libraries that compose the DTV are different from the PCs, thus

not all the threats to the PCs are applicable for the DTV. However, we must admit that every year it is getting easier for the attackers to write attack code because of the use of well-known microprocessors and open platform such as Android.

It is necessary to verify the threats taking into account those factors and develop countermeasures considering the impact of the threats.

<References>

1】 IPA Website Home/IT Security/Measures for Information Security Vulnerabilities
http://www.ipa.go.jp/security/english/third.html

2】 Approaches for Embedded Systems Information Security (2010 Revised Edition), IPA
http://www.ipa.go.jp/security/fy22/reports/emb_app2010/emb_guide_fy22_eng.pdf

3】 Security for Devices with Embedded Software, IPA
http://www.ipa.go.jp/security/fy17/reports/vuln_handling/documents/2_kiki.pdf,
(2006.8) (Japanese)

4】 JVN iPedia Website, IPA, http://jvndb.jvn.jp/

5】 MyJVN Website, IPA, http://jvndb.jvn.jp/apis/myjvn/

6】 JCB Grobal, PCI Data Security Standard (PCI DSS),
http://www.jcb-global.com/pci/index.html (Japanese)

7】 Information Security Early Warning Partnership Guideline,
http://www.ipa.go.jp/security/ciadr/partnership_guide.pdf (Japanese)

8】 Web Application Firewall Guide, IPA
http://www.ipa.go.jp/security/vuln/documents/waf_en.pdf

IPA Security Contents and Resources

To promote information security, IT Security Center of IPA provides the following security resources. IPA hopes these guides and tools will help you improve security.

●: For Users ▲: For Developers ◆: For Business Managers

Information Security Management Benchmark ▲◆

The Information Security Management Benchmark is a self-assessment tool to evaluate the organization's information security management system. By answering 40 questions, the organization can check its security level.

http://www.ipa.go.jp/security/english/benchmark_system.html

iLogScanner ●▲

iLog Scanner is a tool to check the attacks against a website by analyzing access log of the website. It will give an idea about how much the website has been attacked.

http://www.ipa.go.jp/security/vuln/iLogScanner/index.html (Japanese)

How to Run Secure Website ●▲

How to Run Secure Website is a software to learn web security through 7 case studies about the incidents, mainly the ones that exploited vulnerabilities in the website in a role-playing scenario.

http://www.ipa.go.jp/security/vuln/7incidents/index.html (Japanese)

What is Vulnerability? ●▲

What is vulnerability? explains 10 major website vulnerabilities using animation for website administrators and general users to help them understand vulnerability better.

http://www.ipa.go.jp/security/vuln/vuln_contents/index.html (Japanese)

JVN iPedia ●▲

JVN iPedia collects vulnerability countermeasure information from the domestic vendors and those released in the overseas vulnerability information database. By using the search function and RSS feeds, IT users can check vulnerability information efficiently.

http://jvndb.jvn.jp/en/

MyJVN ●▲

MyJVN is a tool designed to help users access the JVN iPedia vulnerability countermeasure information database more efficiently to save time and implement security measures faster.

http://jvndb.jvn.jp/en/apis/myjvn/index.html

Security Information RSS Potal ●▲◆

Security Information RSS Portal collects and organizes latest security information on the Internet and provides in one-stop. Users can check the security information scattered all over the Internet easily and efficiently.

http://www.ipa.go.jp/security/fy19/development/rss/ (Japanese)

●: For Users ▲: For Developers ◆: For Business Managers

e-Learning Materials for Encryption Technology ▲

e-Learning materials for encryption technology are education tools to gain knowledge about encryption technology required for selecting systems and writing procurement specification. They are provided online, which enables users to learn at their preferred time and place.

http://www.ipa.go.jp/security/fy19/development/e_Learning_Cipher/index.html (Japanese)

Secure Programming Course ▲

Secure Programming Course explains the security measures against expected attacks along each development phase. Programmers can learn how to practice secure programming.

http://www.ipa.go.jp/security/awareness/vendor/programmingv2/index.html (Japanese)

TCP/IP Vulnerability Assessment Tool ▲

TCP/IP Vulnerability Assessment Tool is a tool to systematically analyze software that uses TCP/IP for the known TCP/IP vulnerabilities to prevent from writing programs vulnerable to them. It can give a simple test whether a TCP/IP device has known vulnerabilities.

http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html (Japanese)

SIP Vulnerability Assessment Tool ▲

SIP Vulnerability Assessment Tool is a tool to systematically analyze software that uses SIP for the known vulnerabilities to prevent from writing programs vulnerable to them. It can give a simple test whether a SIP device has known vulnerabilities.

http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html (Japanese)

e-Learning Materials for IT Security Evaluation and Certification ▲

e-Learning materials for IT security IT security evaluation and certification is an entry–level education tools to help users to read and learn about professional books in this field. By going through the self-learning tasks, learners can practice to use the knowledge in real developments.

http://www.ipa.go.jp/security/fy19/development/e_Learning_CC/index.html (Japanese)

5 Minutes to Change! Points of Information Security ●▲◆

5 Minutes to Change! Points of Information Security is a learning tool for users who work for SME to learn about information security, theme by theme, 5 min a day to learn 1 theme. Through simulated experiences set in various daily business scenes, users can learn what they should do.

http://www.ipa.go.jp/security/vuln/5mins_point/index.html (Japanese)

IPA will continue its work to promote information security with close collaboration with relevant organizations. For comments and inquiry, please email below.

IT Security Center, IPA isec-info@ipa.go.jp