Note: This document is a tentative translation of "IT 製品の調達におけるセキュリティ要件リスト (Japanese)" issued by Ministry of Economy, Trade and Industry. IPA translated this document for the purpose of reference, and its accuracy is not guaranteed.

February 28, 2018

Ministry of Economy, Trade and Industry (METI)

List of Requirements for Ensuring Security in Procurement of IT Products

- Applicable Product Areas

Applicable Product Areas	Definition of a Product Area
Multifunction Printer (MFP)	Multifunction Printer products equipped with Printing function, with two or more functions out of Scanning, Facsimile (FAX) or Copying function
Firewall	Products that are located in the border of the Internet and the Intranet and control the passage of packets based on the content of packets and the pre-defined rules
Intrusion Detection/ Protection System (IDS/ IPS)	Products that monitor the network or the operational conditions of the system, report an intrusion from outside and prevent it from entering
OS (only Server OS)	Basic software for the hardware control/ operation of the computer
Database Management System (DBMS)	Products that manage the database as common data and responds to access requests for the data
Smart Cards (IC Cards)	Products of plastic cards on which IC chips are embedded to store information
Cryptographic USB Memory	Products of flash-memory-incorporated portable storage device with a USB connector that have a cryptographic function for the stored data
Router/ Layer 3 Switch	Communication line equipment having the function to relay data on the information system and the network base using the OSI-base reference model Layer 3
Full Disk Encryption System	A system that encrypts the entire data in the storage such as the semiconductor drive or hard disk drive or of a note PC, etc.
Mobile Device Management System	A system that safely operates/ controls mobile devices such as smart phones, tablet PCs, etc.
Virtual Private Network (VPN) Gateway	The terminal device in a Virtual Private Network System using the public network services

To Be Applicable	Definition of a Product Area
-	-

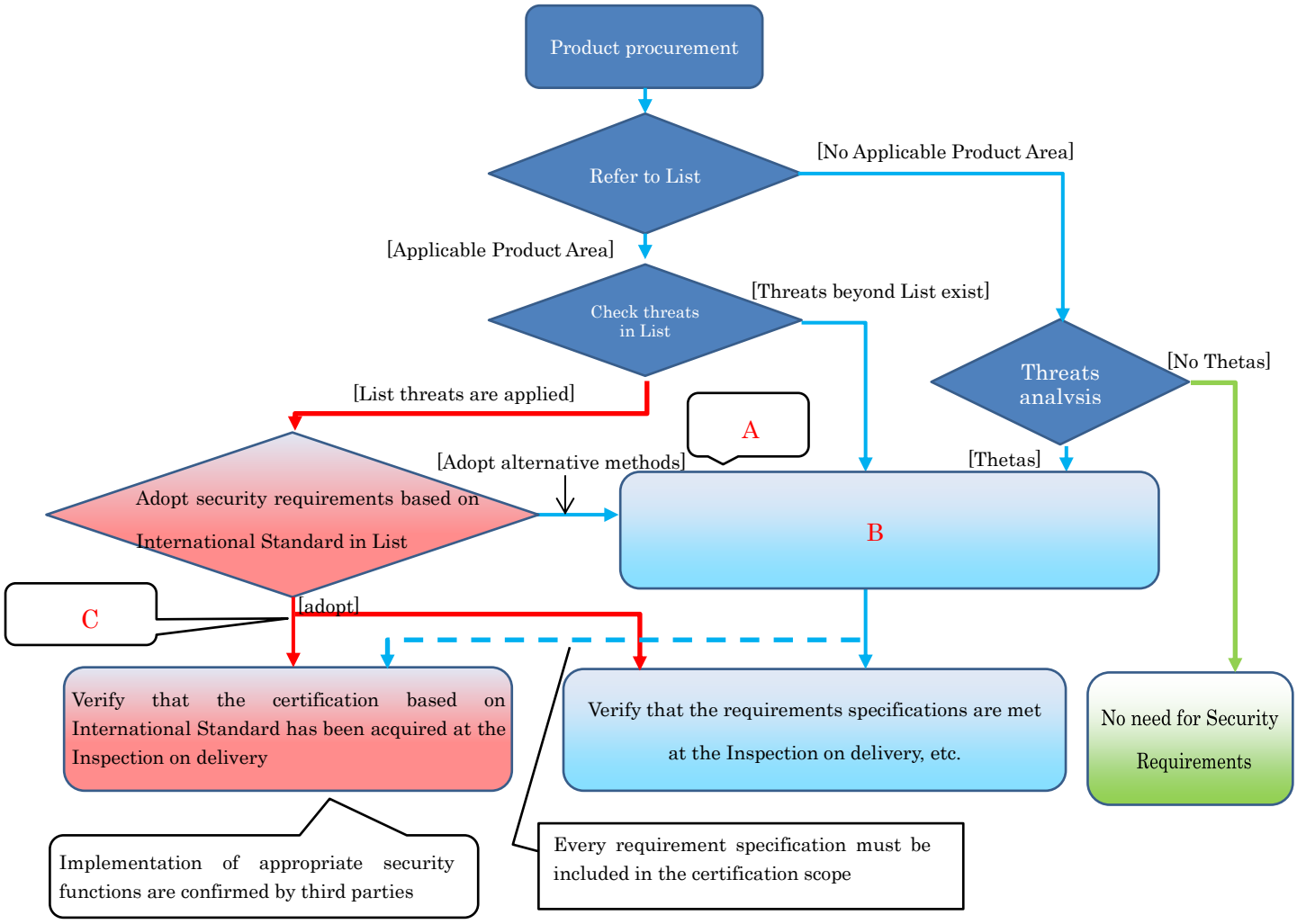
- Purpose and Usage of this List

“Cybersecurity 2016” (decided by the Cybersecurity Strategy Headquarters, August 31 2016) requires that "promotion of use of secure, trustworthy IT products, etc." and "ensuring information security in governmental procurement."
This List is the revision of “List of Requirements for Ensuring Security in Procurement of IT Products” published by Ministry of Economy, Trade and Industry (METI) on June 27 2013 incorporating responses to the above-mentioned requirements.
This List shows threats on security and their measures for the product areas for which appropriate security requirements are established out of products areas that need appropriate information security measures from the following points.

(1) Product areas that are likely to be exposed to threats of attacks due to the composition of information system
(2) Product areas that become the infrastructure for an information system
(3) Product areas for which many attack incidents were reported because the product retains highly important information to be protected in the information system

In addition, out of product areas specified by the above points, this List includes product areas for which prerequisites (like that a product is procurable because it meets the security requirements) are fulfilled.

The following workflow shows procurement of secure IT products using this List:



A: Countering all the threats existing in the use environment is necessary

B: - Individually specify security requirements as requirement specification and designate security functions ("user/ entity authentication functions", "access control function," "security requirements in List +α," etc.)
- Countering threats not by the product but by protecting methods with IT environments, etc.

C: Int'l frame has confirmed those threats can be countered

Overview: Workflow of Procurement of Secure IT Products

[Analysing threats and establishing measures]

In procuring IT products, the procurement entity needs to analyse if threats exist to the information assets to be dealt with in the use environment. This List shows what kind of "threats on security" is assumed for each product area. The procurement entity will refer to this List and determine if there are applicable threats in its own use environment, and if threats exist, their measures should be taken.

Though countering measures are left to the procurement entity, this List shows recommended "Security Requirements based on the International Standard" and requirements to counter which threats.

The procurement entity can designate a product that has the functions to counter the assumed threats on security by using [1] "Security Requirements based on the International Standard" at the time of procurement.

However, even if the product that meets the applicable requirements, it is recommendable that the procurement entity will confirm if there is no inconsistency with the assumed use environment referring to "ASSUMPTIONS" and "Prerequisites" written on "Security Requirements based on the International Standard", because coordination or arrangements due to the use environment may be needed when the product is used.

Note that "Security Requirements based on the International Standard" are the "baseline" requirements to prevent loopholes in implementing functional measures against threats of the product to be procured. If the following conditions are confirmed due to things like a use environment (dependency relationship with other configuration items of the information system), the procurement entity will not need to use "Security Requirements based on the International Standard," or will need to establish individual security requirements.

(1) Measure against the "threats on security" can be uniquely implemented

[1] In this List, in an item of [Supplementary for each product area], as a description example for procurement specifications, the expression, "security requirements equivalent or higher to "Security Requirements based on the International Standards" is used. This is because there is a case that product vendors may uniquely devise security requirements other than security requirements for the measures required in "Security Requirements based on the International Standards" against threats (or more significant threats) that are assumed by "Security Requirements based on the International Standard." If the procurement entity (customer) can obtain corroboration in that, it can be determined that the requirements are met.

(2) Unique threats not listed on “threats on security” exist
However, when it is determined that there is no threats on security in the use environment, considering security requirements or their measures is unnecessary.

[Inspection on delivery, etc]

In procuring a product, an inspection to confirm that the procured product meets the requirement specifications is necessary. If security requirements are individually designated on procurement, an inspection on delivery or such to verify that the requirements are met, according to the procedures of confirmation/ inspection stipulated by each organization will be necessary.
When the product has acquired the third-party certification based on the International Standard related to “Security Requirements based on the International Standard”, it shows that the third-party certification has proved that the security requirements are met thorough the certification process based on the International Standard. Therefore, the procurement entity can substitute the third-party certification for an inspection on delivery and such, once acquisition of the third-party certification is confirmed.

For example, for ISO/IEC 15408-based certified products, it is confirmed that experts of information security have evaluated the product according to the security evaluation methods (ISO/IEC 18045) and the security requirements are met.
Therefore, third-party certifications can be effectively used in procurement of IT products. However, note the following points:

(1) Security Requirements except for “Security Requirements based on the International Standard” in this List
There are some products in the market with third-party certification based on “Security Requirements based on the International Standard” except for the “Security Requirements based on the International Standards” recommended in this List or on security requirements uniquely established by product vendors.
Even for such products, if vendors can prove that the product is certified and the certification includes the security requirements to counter every threat assumed by the procurement entity, and the procurement entity can verity its validity, the third-party certification can be substituted for an inspection on delivery or such with confirmation of acquisition of the certification.

(2) Version upgrade (patch application)

In IT products, it is common that enhancing/ fixing problems on security are continuously implemented as vendors provide patches. However, a third-party certification based on International Standard is given to the specific version of a product. Therefore, the certification will no longer be applied to the product after a version upgrade by security patches, etc.

Then, for version-upgraded products, a system called "Assurance Continuity" is prepared. If changes such as version upgrade or so are made to an evaluated and certified product, the procurement entity can know that the changes have no impact on the certified security items by confirming if Assurance Continuity is applied. (In Assurance Continuity, vendors create Impact Analysis Report (IAR) of analysing those changes due to version up or so have no impact on security, and the Certification Body verifies its validity.)

On inspection, if the version of the product to be procured has been upgraded and the version differs from that of the certified product, the procurement entity will need to confirm that Assurance Continuity is applied to the certified product. Unless Assurance Continuity is applied, the procurement entity needs to request the vendor of evidence to prove that the changes due to version upgrade or so have no impact on the security functionality and to verify its validity.

Acquisition of certification is useful in procurement, and in operation, applying security patches as needed is important.

(3) Products for which certification process hasn't been completed at the time of procurement (products in evaluation)

Since it takes time to acquire third-party certification based on International Standard, there may be a case that "certification-acquisition-assumed product" (certification of the product is currently being acquired (during security evaluation)) should be included in the requirements for procurement.

Then, cases should be assumed that the applicable certification cannot be acquired in time to the delivery or the operation start of the product (or that acquisition of certification will be impossible after all). Therefore, if "certification-acquisition-assumed product" is included in the requirement, the specification should also include "warranty against defects" for the risks.

(4) Others

On the other hand, for certified products with the following cases: the procurement entity needs to verify that the security requirements of the delivered product are met.

- Part of the security requirements that the procurement entity assume important does not seem to be included in the evaluation scope of the product
- Product's third-party certification cannot be used because the International Standard for the product areas is not listed in this List
- The product is not traded on the market,

However, if it is difficult for the procurement entity to conduct the inspection on delivery due to problems regarding the security requirements level (the level is too high to handle), the skill sets of the inspectors or man-hour, etc., outsourcing can be selected as an option. Outsourcing patties include those dealing with security diagnosis, etc. or Evaluation Facilities [2] under IT Security Evaluation, and Certification Scheme approved based on the ISO/IEC 17025 requirements.

[Revision of this List along with expansion of product areas]

In this List, "To Be Applicable" whose product area is expected to be applicable in the future is also mentioned. "To Be Applicable" product areas are products for which "Security Requirements based on the International Standard" have just been established or are being established, which means procurement of certified products based on the International Standard in those product areas in no time is difficult. These product areas should be well recognized as appropriate security measures should be implemented, and therefore, analysing "threats on security" and taking their measures are desired. In the future review, depending on the state of certification acquisition in a product area, the product is to be moved to "Applicable Product Area."

Internationally, IT-product vendors, Evaluation Facilities, Certification Bodies, Government Agencies and Experts are continuously proceeding with establishing "Security Requirements based on the International Standard" (cPP: collaborative Protection Profile) for government procurement based on the cutting-edge technologies in various technological areas. According to development of establishing those requirements, multiple "Applicable Product Areas", "To Be Applicable," and "Security Requirements based on the International Standard" recommended in this List will be updated. By doing that, "Security Requirements based on the International Standard" and certified products based on them will be widely used for procurement. This List is periodically reviewed as needed.

[2] IPA site: https://www.ipa.go.jp/security/jisec/eval-list.html

Product area Name	Multifunction Printer (MFP)

Threats on security	(1) <u>Malicious operations by unauthorized users</u> When users operate MFP, leaking, manipulation, etc. of the stored documents or documents-related data will occur unless the documents are appropriately protected (data access permission, control of each operation, etc.).
	(2) <u>Tapping, manipulation of communication data</u> Communication data on the network between the PCs/ File Server for functioning MFP functions (Printing, Scanning, etc.) and the MFP may be wire tapped or manipulated.
	(3) <u>Unauthorized access to management functions</u> If the user identification and authentication cannot be appropriately performed for the rules set for the document data (Security Policy) or for the functions managing the users' information of the MFP, etc., malicious operations may be performed.
	(4) <u>Manipulation/ damaging of software of MFP</u> If the software of a MFP is manipulated or damaged, the established Security Policy may not be appropriately performed.
	(5) <u>Manipulation/ unauthorized deleting of audit log</u> If audit logs collected for tracking occurrence of malicious operations are not protected, the logs may be manipulated or deleted. As a result, if an unauthorized operation occurs, it cannot be detected.
	(6) <u>Leaking of document data stored in MFP (when lease ends or MFP is discard)</u> Document data for the functions of Printing, Copying or Facsimile may be temporarily or continuously stored in the storage media such as HDD or SDD of the MFP, which may lead to leaking of document data when the MFP is returned due to the end of the lease or is discarded. If these document data are not encrypted or physically deleted, they may be able to be restored even if accessing those data seems superficially impossible.

Security Requirements based on the International Standard	Threats that can be countered

[1] : IEEE Std 2600.1 ™ -2009,Protection Profile for Hardcopy Devices, Operational Environment A Version 1.0[3] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3) (4), (5), (6)
[2] : U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2 ™ -2009)[4] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria)	(1), (2), (3) (4), (5), (6)
[3]: Protection Profile for Hardcopy Devices (Version 1.0[5] or upper) (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3) (4), (5), (6)

(Remarks) the security requirements of [3] require the function to ensure safe update of the software.

[Supplementary for Multifunction Printer (MFP)]

In this product area, so-called large Multifunction Printers for office use equipped with Printing function, with two or more functions out of Scanning, Facsimile (FAX) or Copying function and with the network communication and management function are applicable.

Digital MFPs are implemented with various functions. However, FAX function is not equipped with some MFPs, for example, and therefore, security requirements may differ depending on a product type.

In addition, regarding measures against disclosure of document data stored in the MFP, some products counter by the data purging function in the storage area, and others may counter by cryptographic functions.

Due to the above-mentioned property of digital MFP, in order to counter threats

---

[3] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp_hcd_br_v1.0.pdf
The translated version downloadable from the IPA site:
https://www.ipa.go.jp/security/publications/ieee/documents/2600.1/index.html

[4] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp_hcd_eal2_v1.0-add1.pdf

[5] Downloadable from the IPA site:
https://www.ipa.go.jp/security/publications/pp-jp/hcd.html

assumed according to a function equipped with a product, vendors may uniquely establish their own requirements to counter these assumed threats, different from the functionality requirements of the "Security Requirements based on the International Standard." In this case, it is important that the procurement entity needs to confirm that the vendor has defined the security requirements assuming what kind of threats.

[How to check products with the third-party certification for the security requirements in this List]

Products that have acquired the third-party certification in these security requirements: products listed as "Certified Products" by "Security Requirement based on the International Standard." They can be searched by referring "conformance product information" (Multifunction Printers (MFP)) in the "List of Requirements for Ensuring Security in Procurement of IT Products" of the following IPA website.

https://www.ipa.go.jp/security/it-product/mfp

[Examples of describing the procurement specification for using "Security Requirements based on the International Standard" and an inspection method]

(1) When security requirements equivalent or higher to "Security Requirements based on the International Standard" and the third-party certification conforming to the requirements are required:

(An example of description)

It shall be required that ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to any of the followings has been acquired.[6] - IEEE Std 2600.1 ™ -2009, Protection Profile for Hardcopy Devices, Operational Environment A Version 1.0 - U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2 TM -2009) - Protection Profile for Hardcopy Devices (Version 1.0 or upper)

(An example of an inspection method)

Request to submit the certificate (including material explaining to prove equality as

[6] In the product area of Digital Multifunction Printer, the following case should be well noted: if a change is made to a configuration item (e.g. with or without FAX option) of the certified product, the product may no longer be able to be regarded as the certified product in the ISO/IEC 15408 (Common Criteria) certification. However, if a device is composed of only configuration items of the certified device, it will be assumed that the same security level is realized as much as that of the device with the applicable certification, and if the procurement entity (customer) can obtain corroboration in that, it will be OK to be determined that the requirements are met.

needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, "Assurance Continuity," is prepared for a product whose version is changed, which may be able to be applied as complemented with "Assurance Continuity Maintenance Report." (Refer to (2) on P5)

In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on security functions and verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.

(Note) in IT products, it is important that continuous version upgrade for enhancing or fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to "Security Requirements based on International Standard" are required, but the third-party certification is not requited (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):

(An example of description)

Security functionality requirements equivalent or higher to any of the followings shall be met. - IEEE Std 2600.1 ™ -2009, Protection Profile for Hardcopy Devices, Operational Environment A Version 1.0 - U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2 ™ -2009) ・Protection Profile for Hardcopy Devices (Version 1.0 or upper)

(An example of an inspection method)

The procurement entity will understand the content of "Security Requirements based on the International Standard" and then inspect if the security functionality requirements are met by an inspection on delivery, etc.. Note IPA publishes Japanese-translated versions of these "Security Requirements based on the International Standard."

https://www.ipa.go.jp/security/publications/pp-jp/index.html

Product area Name	Firewall

Threats on security	(1) <u>Occurrence of unauthorized communication by unauthorized access to management functions, etc.</u> If a person without access permission to the functions managing the rules for controlling unauthorized communication (Security Policy), etc. can impersonate an authorized user, malicious operations may be possible. The Information Flow Control that is supposed to be processed will not work due to the unauthorized operation, which may lead to security intrusion because unauthorized communication from the outside/ inside of the organization cannot be prevented. For example, if the Intranet that an organization manages is accessed from an "open environment" such as Internet, internal servers, etc. connecting to the Intranet may receive some damage. In addition, by having the Intranet communicated with a service whose use is prohibited existing in an "open environment" such as Internet, confidential information may be lost or leaked.
	(2) <u>Information leakage form residue of networking processing</u> When network packets were sent, the sent data may remain in the buffer or memory area that the sent packets used. The sent data may be included into other packets when those packets re-use the buffer, which may lead to leakage of confidential information or its relevant data.
	(3) <u>Tapping, manipulation of communication data when remotely managed</u> When the administrator controls remotely, data including security-related information communicated with the product may be wire tapped or manipulated. If the administrator's password, etc. is stolen by tapping, the configuration of Firewall may be altered.
	(4) <u>Manipulation / unauthorized deleting of audit log</u> If audit logs collected for tracking occurrence of malicious operations are not protected, the logs may be manipulated or deleted. As a result, if an unauthorized operation occurs, it cannot be detected.

Security Requirements based on the International Standard	Threats that can be countered

[1]: Protection Profile for Traffic Filter Firewall In Basic Robustness Environments Version 1.1[7] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria)) (to be deleted in one year)	(1), (2), (3), (4)
[2]: Protection Profile for Network Devices Version 1.1[8] and Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall (Version 1.0[9] or upper) (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3), (4)
[3]: collaborative Protection Profile for Stateful Traffic Filter Firewalls (v1.0 (CPP_FW v1.0) or upper) (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3), (4)

(Remarks) the security requirements of [3] require the function to ensure safe update of the software.

[Supplementary for Firewall]

In this product area, traffic-filter type (packet filter type) Firewall products that are located in the border of the Internet and the Intranet and control the passage of packets based on the content of packets and the pre-defined rules are applicable.

Regarding Firewall, though the three requirements as "Security Requirements based on the International Standard" are posted, [1] was already abolished, no new products have been certified since three products were certified in 2012, and therefore this security requirement is to be deleted in February 2019. As for [2], one product in 2014, 7

[7] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp_fw_tf_br_v1.1.pdf

[8] Downloadable from the NIAP (National Information Assurance Partnership) website:
https://www.niap-ccevs.org/pp/pp_nd_v1.1.pdf
IPA site (the translated version downloadable):
https://www.ipa.go.jp/files/000015354.pdf

[9] Downloadable from the NIAP site:
https://www.niap-ccevs.org/pp/pp_nd_tffw_ep_v1.0.pdf
IPA site (the translated version downloadable):
https://www.ipa.go.jp/files/000015352.pdf

products in 2015 and 3 products in 2016 were certified. As for [3], this security requirement was established in 2015. No product having the third-party certification based on the International Standard has not come onto the market, and therefore, if the third-party certification based on the International Standard is required for procurement, using both [2] and [3] as requirements and claiming conformance to either of the requirements are desired. (As of February 2018)

Note: As for devices controlling multiple security functions including Firewall in an integrated manner like UTM (United Threat Management), analysing threats and establishing security requirements shown in this List are necessary.

[How to check products with the third-party certification for the security requirements in this List]
Products that have acquired the third-party certification in these security requirements: products listed as “Certified Products” by “Security Requirement based on the International Standard." They can be searched by referring “conformance product information” (Firewall) in the “List of Requirements for Ensuring Security in Procurement of IT Products of the following IPA website.
https://www.ipa.go.jp/security/it-product/fw

[Examples of describing the procurement specification for using “Security Requirements based on the International Standard” and an inspection method]
(1) When security requirements equivalent or higher to “Security Requirements based on the International Standard” and the third-party certification conforming to the requirements are simultaneously required:
(An example of description)

It shall be required that ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to any of the followings has been acquired. - Protection Profile for Network Devices Version 1.1 and Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall (Version 1.0 or upper) - collaborative Protection Profile for Stateful Traffic Filter Firewalls (v1.0 (CPP__FW_v1.0) or upper)

(An example of an inspection method)
Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party

certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after version upgrade. “Assurance Continuity” is prepared for a product whose version is changed, which may be able to be applied as complemented with “Assurance Continuity Maintenance Report.” (Refer to (2) on P5)

In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.

(Note) in IT products, it is important that continuous version upgrade for enhancing or fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to “Security Requirements based on the International Standard” are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):

(An example of description)

Security requirements equivalent or higher to security functionality requirements of any of the followings shall be met. - Protection Profile for Network Devices Version 1.1 and Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall (Version 1.0 or upper) - collaborative Protection Profile for Stateful Traffic Filter Firewalls (v1.0 (CPP_FW _v1.0) or upper)

(An example of an inspection method)

The procurement entity will understand the content of “Security Requirements based on the International Standard” and then inspect if the security functionality requirements are met by an inspection on delivery, etc.

Product area Name	Intrusion Detection/ Protection System (IDS/ IPS)

Threats on security	(1) <u>Attacks to be monitored</u> For a system in which threats such as attacks to publication services (web applications, etc.) or DoS attacks by excessive access, etc. exist or for a system where urgent measure are needed when vulnerabilities are publicized, the functions to analyze/ detect/ alert this threats-related information are needed. Without such functions, traces of an attack will be lost, and appropriate treatments may not be able to be taken. As a result, a system where threats exist may receive some damage.
	(2) <u>Attacks to be protected against</u> In addition to monitoring attacks, implementation of automatic protection against or reducing the effects from attacks according to the environment is necessary. Without such function, those attacks will be highly successful, and the system under management may receive some damage.
	(3) <u>Invasion to security functions by unauthorized access to management function, etc.</u> If a person without access permission to the functions managing the rules for controlling unauthorized communication (Security Policy), etc. can impersonate an authorized user, malicious operations may be possible. As a result, the functions to analyze/ detect/ alert the information related to attacks to publication services or DoS attacks by excessive access etc., may not work or implementation of automatic protection against, or reducing the effects from attacks according to the environment may not be ensured.
	(4) <u>Destruction, manipulation, disclosure of illicit-or abnormal-detected data</u> If a product does not have the function to protect the data created when an intrusion or anomaly behavior is detected, the data may be fraudulently destroyed, manipulated or disclosed. As a result, the functions to analyze/ detect/ alert the information related to attacks to publication services or DoS attacks by excessive access, etc. may not work, or implementation of automatic protection against or reducing the effects from attacks according to the environment may not be ensured.
	(5) <u>Manipulation/ unauthorized deleting of audit log</u> If audit logs collected for tracking occurrence of malicious operations are

	not protected, the logs may be manipulated or deleted. As a result, if an unauthorized operation occurs, it cannot be detected.

Security Requirements based on the International Standard	Threats that can be countered
[1]: Protection Profile Intrusion Detection System - System for Basic Robustness Environments, (Version 1.7[10] or upper) (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3) (4), (5)
[2]: Extended Package for Intrusion Prevention Systems (Version 2.1 or upper) and collaborative Protection Profile for Network Devices (v1.0 (ND cPP v1.0) or upper) (Security Requirement Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3) (4), (5)

(Remarks) the security requirements of [2] require the function to ensure safe update of the software.

[Supplementary for Intrusion Detection/ Protection System (IDS/ IPS)]

In this product area, Intrusion Detection/ Protection System (IDS/ IPS) products which monitor the network or the operational condition of the system to report an intrusion from outside to the computer network of the organization and prevent it from entering are applicable.

For products having the third-party certification based on the International Standard currently on the market, there are multiple products with the third-party certification based on [1] "Intrusion Detection System - System for Basic Robustness Environments, Version 1.7," [1] is available for procurement. As for [2], though the security requirement was established in January 2016, no product having the third-party certification based on the International Standard has come onto the market. Therefore, if the third-party certification based on the International Standard is required for procurement, using both [1] and [2] as requirements and claiming conformance to either of them are desired. (As of February 2018)

Note: for devices controlling multiple security functions including IDS/ IPS in an integrated manner like UTM (United Threat Management), analysing threats and establishing security requirements shown in this List are necessary.

[10] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp_ids_sys_br_v1.7.pdf

[How to check products with the third-party certification for the security requirements in this List]

Products that have acquired the third-party certification in these security requirements: products listed as “Certified Products” by Security Requirement based on the International Standard." They can be searched by referring “conformance product information” (Intruding Detection/ Protection system (IDS/ IPS)) in the “List of Requirements for Ensuring Security in Procurement of IT Products” of the following IPA website.

https://www.ipa.go.jp/security/it-product/ids

[Examples of describing the procurement specification for using “Security Requirements based on the International Standard” and an inspection method]

(1) When security requirements equivalent or higher to “Security Requirements based on the International Standard” and the third-party certification conforming to the requirements are simultaneously required:

(An example of description)

It shall be required that ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to any of the followings has been acquired. - Protection Profile Intrusion Detection System - System for Basic Robustness Environments, (Version 1.7 or upper) - Extended Package for Intrusion Prevention Systems (Version 2.1 or upper) and collaborative Protection Profile for Network Devices (v1.0 (ND cPP v1.0) or upper)

(An example of an inspection method)

Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after version upgrade. “Assurance Continuity” is prepared for a product whose version is changed, which may be able to be applied as complemented with “Assurance Continuity Maintenance Report.” (Refer to (2) on P5)

In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.

(Note) in IT products, it is important that continuous version upgrade for enhancing or

fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to "Security Requirements based on the International Standard" are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):

(An example of description)

Security functionality requirements equivalent or higher to any of the followings shall be met. - Protection Profile Intrusion Detection System - System for Basic Robustness Environments (Version 1.7 or upper) - Extended Package for Intrusion Prevention Systems (Version 2.1 or upper) and collaborative Protection Profile for Network Devices (v1.0 (ND cPP v1.0) or upper)

(An example of an inspection method)

The procurement entity will understand the content of "Security Requirements based on the International Standard" and then inspect if the security functionality requirements are met by an inspection on delivery, etc...

Product area Name	OS (only Server OS)

Threats on security	(1) <u>Impersonating authorized user</u> If a user or process accessing the OS is not correctly identified, unauthorized accessing by impersonating an authorized user may be carried out. For example, if a person who is not registered as a user impersonates an authorized user of the OS and logs in the OS, an unauthorized access to the OS-managed resources (information leakage, information manipulation, etc.) will occur.
	(2) <u>Unauthorized access to resources and functions</u> If an operation for the OS-managed resources is not appropriately controlled according to the authority allocated to an identified user, unauthorized access beyond the original authority may be carried out. For example, if permission/denial of each operation (read, write, execute, etc.) is not controlled correctly according to the pre-set rules (Security Policy) for the resources (files, directories, services) or functions, information leakage/ manipulation, etc. will occur.
	(3) <u>Intercepting of communication data at OS level</u> If communication to the remote IT system to communicate with the OS is intercepted, the communication data may be disclosed or manipulated.
	(4) <u>Manipulation/ unauthorized deleting of audit log</u> If audit logs collected for tracking occurrence of malicious operations are not protected, the logs may be manipulated or deleted. As a result, if an unauthorized operation occurs, it cannot be detected.
	(5) <u>Occurrence of unauthorized communication</u> If the function setting/ managing the rules (Security Policy), etc. for controlling unauthorized communication is not appropriately controlled, unauthorized access to information in the servers may be carried out by unauthorized communication to the OS.

Security Requirements based on the International Standard	Threats that can be countered

[1]: Operating System Protection Profile (BSI-CC-PP-0067b) Version 2.0[11] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3) (4), (5)
[2] : PROTECTION PROFILE FOR GENERAL-PURPOSE OPERATING SYSTEMS IN A NETWORKED ENVIRONMENT Version 1.0[12] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria)) (to be deleted in a year)	(1), (2), (3), (4)
[3] : General-Purpose Operating System Protection Profile Version: 3.9[13] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3) (4), (5)
[4]: Protection Profile for General Purpose Operating Systems (Version 4.1, PP-OS-v4.1 or upper) (Security Requirement Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3) (4), (5)

(Remarks) the security requirements of [4] require the function to ensure safe update of the software.

[Supplementary for OS (only server OS)]

In this product area, basic software (Server OS) for the hardware control/ operation of the server is applicable.

Regarding OS, though the four requirements as "Security Requirements based on the International Standard" are posted, as for [2], [4] has been established as the security requirement instead of [2], and no products having the third-party certification based on the International Standard of [2] are currently on the market. Therefore [2] is to be deleted in February 2019. If third-party certification based on the International Standard is required at the time of procurement, using requirements of [1], [3] and [4] and claiming conformance to any of them are desired. (As of February 2018)

Note that, though any of [1], [3] or [4] is security requirements aimed at general-purpose OS, acquisition of third-party certification varies depending on which security requirements by OS type (product vendor). Therefore, selection of the best-suited security requirements considering requirement specifications besides the

[11] Downloadable from the CCRA portal site: https://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf

[12] Downloadable from the CCRA portal site: https://www.commoncriteriaportal.org/files/ppfiles/pp_gpospp_v1.0.pdf

[13] Downloadable from the NIAP site: https://www.niap-ccevs.org/pp/pp_gpos_v3.9.pdf

security is necessary.

[How to check products with the third-party certification for the security requirements in this List]
Products that have acquired the third-party certification in these security requirements: products listed as “Certified Products” by “Security Requirement based on the International Standard." They can be searched by referring “conformance product information” (OS (only Server OS) in the “List of Requirements for Ensuring Security in Procurement of IT Products” of the following IPA website.
https://www.ipa.go.jp/security/it-product/os

[Examples of describing the procurement specification for using “Security Requirements based on the International Standard” and an inspection method]
(1) When security requirements equivalent or higher to “Security Requirements based on the International Standard” and the third-party certification conforming to the requirements are simultaneously required:
(An example of description)

It shall be required that ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to any of the followings has been acquired. - Operating System Protection Profile BSI-CC-PP-0067 (Version 2.0) or - General-Purpose Operating System Protection Profile (Version 3.9) - Protection Profile for General Purpose Operating Systems (Version 4.1, PP-OS-v4.1 or upper)

(An example of an inspection method)
Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after version upgrade. “Assurance Continuity” is prepared for a product whose version is changed, which may be able to be applied as complemented with “Assurance Continuity Maintenance Report.” (Refer to (2) on P5)
In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.
(Note) in IT products, it is important that continuous version upgrade for enhancing or

fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to "Security Requirements based on the International Standard" are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):

(An example of description)

Security functionality requirements equivalent or higher to any of the followings shall be met. - Operating System Protection Profile BSI-CC-PP-0067 (Version 2.0) - General-Purpose Operating System Protection Profile (Version 3.9) - Protection Profile for General Purpose Operating Systems (Version 4.1, PP-OS-v4.1 or upper)

(An example of an inspection method)

The procurement entity will understand the content of "Security Requirements based on the International Standard" and then inspect if the security functionality requirements are met by an inspection on delivery, etc.

Product area Name	Database Management System (DBMS)

Threats on security	(1) <u>Impersonating authorized user</u> If a user or process to access the database is not correctly identified, unauthorized accessing by impersonating an authorized user may be carried out. For example, if a user who is not allowed to access the database impersonates an authorized user registered in the DBMS and accesses the database, an unauthorized access (information leakage, manipulation, etc.) to the database that the DBMS manages will occur.
	(2) <u>Unauthorized access to not-permitted operation objects and functions</u> If operations for the DBMS-managed resources or the functions for which operations are not permitted are not appropriately controlled according to the authority allocated to an identified user, unauthorized accessing beyond the original authority may be carried out. For example, if permission/denial of each operation (read, add, update, delete, execute, etc.) is not controlled correctly according to the pre-set rules (Security Policy) for operation objects (database, table, function) or functions, information leakage, manipulation, etc. will occur.
	(3) <u>Information leakage from released region</u> After DBMS releases the region on its disk/ memory, when another user or process creates a new database/ table in the released region, if the data that had existed there before release was not appropriately deleted, the data may be read by a user without access permission.

Security Requirements based on the International Standard	Threats that can be countered
[1]: PP for Database Management Systems (Version 1.3)[14] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria)) (to be deleted in one year)	(1), (2), (3)
[2]: Base Protection Profile for Database Management Systems (v2.07 (BSI-CC-PP-0088-2015) or upper) (Security Requirement Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)

[14] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp_dbms_v1.3.pdf

[Supplementary for Database Management System (DBMS)]

In this product area, Database Management System (DBMS) which manages database as common data and responds to access requests for the data is applicable.

For "Security Requirements based on the International Standard" for Database Management System (DBMS), quite a long time has passed since the establishment of [1]. Then [2] has been established. As there are multiple products with the third-party certification on the market, [2] is available at the time of procurement. Therefore, [1] is to be deleted in February 2019.

[How to check products with the third-party certification for the security requirements in this List]

Products that have acquired the third-party certification in these security requirements: products listed as "Certified Products" by Security Requirement based on International Standard." They can be searched by referring "conformance product information" (Database Management System (DBMS)) in the "List of Requirements for Ensuring Security in Procurement of IT Products" of the following IPA website.

https://www.ipa.go.jp/security/it-product/dbms

[Examples of describing the procurement specification for using "Security Requirements based on the International Standard" and an inspection method]

(1) When security requirements equivalent or higher to "Security Requirements based on the International Standard" and the third-party certification conforming to the requirements are simultaneously required:

(An example of description)

It shall be required that ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to Base Protection Profile for Database Management Systems (v2.07 (BSI-CC-PP-0088-2015) or upper) has been acquired.

(An example of an inspection method)

Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after version upgrade. "Assurance Continuity" is prepared for a product whose version is changed, which may be able to be applied as complemented with "Assurance Continuity Maintenance Report." (Refer to (2) on P5)

In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.
(Note) in IT products, it is important that continuous version upgrade for enhancing or fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to "Security Requirements based on the International Standard" are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):
(An example of description)

Security functionality requirements equivalent or higher to Base Protection Profile for Database Management Systems (v2.07 (BSI-CC-PP-0088-2015) or upper) shall be met.

(An example of an inspection method)
The procurement entity will understand the content of "Security Requirements based on the International Standard" and then inspect that the security requirements are met by an inspection on delivery, etc.

Product area Name	Smart Cards (IC Cards)

Threats on security	(1) Falsification of IC chip An IC chip may be falsified by writing the duplicated data of an IC chip into another IC chip that has the same functionality.
	(2) Leakage of confidential information by logical attack Confidential information (authentication data, etc.) stored in the machine-readable region may be readout fraudulently by using non-contact interface.
	(3) Leakage of confidential information by physical attack Confidential information (authentication data, etc.) stored in the IC chip may be readout fraudulently by a physical attack.
	(4) Handling when authentication fails When a user authentication is failed, the authentication may be penetrated by attempting user authentication with a number of authentication data unless the function to constantly invalidate the authentication data is supported.

Security Requirements based on the International Standard	Threats that can be countered
[1] Protection Profile for ePassport IC - Active Authentication - version 1.00[15] (Security Requirements Specifications for IC passport based on ISO/IEC15408 (Common Criteria)) (to be deleted in one year)	(1), (2), (3), (4)
[2] Protection Profile for ePassport IC - SAC support (PACE) and Active Authentication support - version 1.00[16] (Security Requirement Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3), (4)
[3] Protection Profile for ePassport IC - SAC support (BAC+PACE) and Active Authentication support - version 1.00[17] (Security Requirement Specifications based on ISO/IEC15408 (Common	(1), (2), (3), (4)

[15] Downloadable from the IPA site:
https://www.ipa.go.jp/security/jisec/certified_pps/c0247/c0247_pp.pdf
[16] Downloadable from the IPA site:
https://www.ipa.go.jp/security/jisec/certified_pps/c0499/c0499_pp.pdf
[17] Downloadable from the IPA site:
https://www.ipa.go.jp/security/jisec/certified_pps/c0500/c0500_pp.pdf

Criteria))	
[4] Protection Profile for Personal Number Cards version 1.00[18] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3), (4)
[5] Security IC Platform Protection Profile Version 1.0, BSI-CC-PP-0035-2007 (Security Requirement Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)
[6] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, BSI-CC-PP-0084-2014 (Security requirement specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)

[Supplementary for Smart Cards (IC Cards)]

In this product area, Smart Cards (IC Cards) on which IC chips are embedded on the plastic card to store information are applicable.

For Smart Cards (IC Cards), threats to be countered significantly vary depending on its purpose of use. Therefore, the procurement entity needs to analyse threats by purpose of use of the Smart Card (IC Card) which it will procure and to establish security requirements based on the analysis.

This List describes threats against the IC passport and security requirements to counter those threats as reference to "Security Requirements based on the International Standard." As new security requirements [2] and [3] have been established, [1] is to be deleted in February 2019.

In addition, multiple security requirements depending on purpose of use are already established. Establish an individual security requirement as needed referring to the CCRA[19] portal site. https://www.commoncriteriaportal.org/pps/

("Protection Profile" shown on the "ICs, Smart Cards and Smart Card-Related Devices and Systems" tab is the security requirements for purpose of use.)

Though security requirements for the following areas are described in the above pages, security requirements for Smart Cards (IC cards) are established in consideration of the individual use environment, etc. Therefore, using the security requirements as they are

[18] Downloadable from the IPA site:
https://www.ipa.go.jp/security/jisec/certified_pps/c0431/c0431_pp.pdf

[19] CCRA (Common Criteria Recognition Arrangement) is a framework in which security of IT products, etc. is objectively evaluated by governmental organization of each country and the evaluation result is mutually recognized internationally.

is thought to be difficult in procurement. Note that the information here is just for reference.

- Cards for residence permit[20]
- Cards for health-related[21]
- Cards for monetary-related[22]

For Smart Cards, security requirements for the IC chip to be embedded on the card shall be also important. In general, it is assumed that the security requirements for an IC chip are designated by the card vendor to the IC chip vendor. However, when the procurement entity of the Smart Card designates the security requirements for the IC chip, refer to the security requirements[23] for IC chips as well.

[20] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp0069b_pdf.pdf
[21] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp0018_v3b_pdf.pdf
[22] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp0038b.pdf
[23] Downloadable from the CCRA portal site:
https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf

* The above URLs are just part of them. Other security requirements are also posted at the CCRA portal site, https://www.commoncriteriaportal.org/pps/.

Product area Name	Cryptographic USB Memory

Threats on security	(1) Leakage of confidential information If the cryptographic key/ authentication data are not appropriately protected, those data will be easily accessed/ guessed, which may lead to information leakage by exploiting those flaws.
	(2) Unauthorized access to cryptographic key/authentication data Cryptographic key/ authentication data may be accessed as malicious programs stored in the USB memory interferes with the control program of the USB memory. It may inactivate the cryptographic function or expose the cryptographic key/ authentication data to the attacker.
	(3) Unauthorized rewriting of software of USB memory Unless mechanism to verify that update programs of the product are valid is supported, uploading of unauthorized software or system files will be allowed. As a result, it may cause inactivation of the cryptographic function and such or introduction of unauthorized applications into the PC, etc. to which the USB memory connects.

Security Requirements based on the International Standard	Threats that can be countered
[1]: ISO/IEC19790 (supported JIS standard: JIS X 19790) [Security Level 2 or upper][24]	(1), (2)
[2]: Protection Profile for USB Flash Drives (Version 1.0 or upper)[25] (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)
[3]: Protection Profile for USB Storage Media (Version 1.4 (BSI-PP-0025-2006) or upper)	(1), (2), (3)

[24] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
At the "search for JIS with JIS standard number," of the JISC site, enter "X19790" and then it can be viewed.

[25] Downloadable from the NIAP site:
https://www.niap-ccevs.org/pp/pp_usb_fd_v1.0.pdf
IPA site (the translated version downloadable):
https://www.ipa.go.jp/files/000015355.pdf

(Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	
[4]: CSEC Protection Profile Encrypted Storage Device (Version 2.1 (FMV-PP-ESD) or upper) (Security Requirement Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)

[Supplementary for Cryptographic USB Memory (USB portable storage device)]

In this product area, a portable storage device which has the USB connector and flash memory in it (USB memory) and automatically encrypts the content of the flash memory by the hardware of the USB memory is applicable.

For Cryptographic USB memories, their requirements vary depending on a use/ operation style. Significance of threats on security or threats themselves will differ in the following cases, for example:

- when the information system end that connects to the USB memory controls the USB memory,
- when the USB memory is used in the management system where there is no possibility that any of the information in the USB memory will be taken out to the outside,
- when data to be stored are restricted,

In the extreme case, no threat can be assume. However in that case, the cryptographic functions required for this product area will be no longer necessary.

Since modules for performing encryption, etc. are embedded internally on a Cryptographic USB memory, certification based on ISO/IEC 19790 that is the International Standard regarding the requirements for the information security of the cryptographic module can be used as security requirements. (Multiple products with the certification of Security Level 2 of FIPS140-2 that is assumed to be equivalent to ISO/IEC 19790 are already on the market.)

In addition, security requirements based on ISO/IEC 15408 have been established for software products or products with hardware and software, in which the minimum security requirements with software-unique threats assumed are stipulated besides the security requirement based on ISO/IEC 19790.

Though these standards were originated separately, appropriate security requirements need to be selected according to the purpose of use of the product to be procured.

Note that collaborative Protection Profile for Cryptographic USB memories are

currently being created and will be completed in due course.

[How to check products with the third-party certification for the security requirements in this List]
Products that have acquired the third-party certification in these security requirements: products listed as “Certified Products” by “Security Requirement based on International Standard." They can be searched by referring “conformance product information” (USB Memory) in the “List of Requirements for Ensuring Security in Procurement of IT Products” of the following IPA website.
https://www.ipa.go.jp/security/it-product/usb

[Examples of describing the procurement specification for using “Security Requirements based on the International Standard” and an inspection method]
(1) When security requirements equivalent or higher to “Security Requirements based on the International Standard” and the third-party certification conforming to the requirements are simultaneously required:
(An example of description)

It shall be required that Cryptographic algorithms on E-Government Recommended Ciphers List are used and any of the following certifications has been acquired.
- Certification of Security Level 2 of ISO/IEC 19790 (JIS X19790) or its equivalent or higher certifications (such as the certification of security Level 2 of FIPS140-2)
- ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to Protection Profile for USB Flash Drives (Version 1.0)
- ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to “Protection Profile for USB Storage Media (Version 1.4 (BSI-PP-0025-2006) or upper)”
- ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to “CSEC Protection Profile Encrypted Storage Device (Version 2.1 (FMV-PP-ESD) or upper)”

(An example of an inspection method)
Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after

version upgrade. “Assurance Continuity” is prepared for a product whose version is changed, which may be able to be applied as complemented with “Assurance Continuity Maintenance Report.” (Refer to (2) on P5)
In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.
(Note) in IT products, it is important that continuous version upgrade for enhancing or fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to “Security Requirements based on the International Standard” are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):
(An example of description)

It shall be required that Cryptographic algorithms on E-Government Recommended Ciphers List are used and any of the followings is met.
- The test for Level 2 of ISO/IEC 19790 (JIS X19790) or tests assumed to be equivalent or higher to it (such as test for Security Level 2 of FIPS140-2) has been passed.
- Requirements equivalent or higher to security functionality requirements defined in “Protection Profile for USB Flash Drives Version 1.0” shall be met.
- Requirements equivalent or higher to security functionality requirements defined in “Protection Profile for USB Storage Media (Version 1.4 (BSI-PP-0025-2006) or upper)” shall be met.
- Requirements equivalent or higher to security functionality requirements defined in “CSEC Protection Profile Encrypted Storage Device (Version 2.1 (FMV-PP-ESD) or upper)” shall be met.

(An example of an inspection method)
The procurement entity will understand the content of “Security Requirements based on the International Standard” and then inspect if the security functionality requirements are met by an inspection on delivery, etc..

Product area Name	Rooter/ Layer 3 Switch

Threats on security	(1) <u>Occurrence of unauthorized communication by unauthorized access to management functions, etc.</u> If a person without access permission to the functions managing the rules for controlling unauthorized communication (Security Policy), etc. can impersonate an authorized user, malicious operations may be possible. The Information Flow Control that is supposed to be processed will not work due to the unauthorized operation, which may lead to security intrusion. For example, if the Intranet that an organization manages is accessed from an "open environment" such as Internet, the internal servers, etc. connecting to the Intranet may receive some damage. In addition, by having the Intranet communicated with a service whose use is prohibited existing in an "open environment" such as Internet, confidential information may be lost or leaked.
	(2) <u>Tapping, manipulation of communication data when remotely controlled</u> When the administrator controls remotely, data including security-related information communicated with the product may be wire tapped or manipulated. If the administrator's password, etc. is stolen by tapping, the configuration of firewall may be altered.
	(3) <u>Manipulation / unauthorized deleting of audit log</u> If audit logs collected for tracking occurrence of malicious operations is not protected, the logs may be manipulated or deleted. As a result, if an unauthorized operation occurs, it cannot be detected.

Security Requirements based on the International Standard	Threats that can be countered
[1]: Protection Profile for Network Devices v1.1 (PP_ND_V1.1) (Security Requirement Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)
[2]: collaborative Protection Profile for Network Devices (v1.0 (CPP_ND_v1.0) or upper) (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)

(Remarks) the security requirements of [1] and [2] require the function to ensure safe update of the software as well.

[Supplementary for Router/ Layer 3 switch]

In this product area, Communication Line Equipment having a function to relay data on the information system and the network base using OSI-base reference model Layer 3 (network layer) is applicable.

The minimum security requirements for network devices including Routers/ Layer 3 Switches deployed as an important component in the network base have been established, and currently, products with the certification based on ISO/IEC 15408 (Common Criteria) are already on the market.

Besides, if there are other threats on security in the use environment, establishing security requirements individually for the threats or taking measures from the operational aspect will be necessary.

For example, when the Router/ Layer3 Switch has the firewall function, intrusion detection/ prevention function and/or virtual private network (VPN) function, threats on security indicated in each product area related to those additional functions may be assumed.

[How to check products with the third-party certification for the security requirements in this List]

Products that have acquired the third-party certification in these security requirements: products listed as “Certified Products” by “Security Requirement based on International Standard." They can be searched by referring “conformance product information” (Router/Layer 3 Switch) in the “List of Requirements for Ensuring Security in Procurement of IT Products” of the following IPA website.

https://www.ipa.go.jp/security/it-product/nd

[Examples of describing the procurement specification for using “Security Requirements based on the International Standard” and an inspection method]

(1) When security requirements equivalent or higher to “Security Requirements based on the International Standard” and the third-party certification conforming to the requirements are simultaneously required:

(An example of description)

It shall be required that ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to either of the followings has been acquired. - Protection Profile for Network Devices v1.1 (PP_ND_V1.1)

- collaborative Protection Profile for Network Devices (v1.0 (ND cPP v1.0) or upper)

(An example of an inspection method)

Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after version upgrade. “Assurance Continuity” is prepared for a product whose version is changed, which may be able to be applied as complemented with “Assurance Continuity Maintenance Report.” (Refer to (2) on P5)

In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.

(Note) in IT products, it is important that continuous version upgrade for enhancing or fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) <u>When security requirements equivalent or higher to “Security Requirements based on the International Standard” are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):</u>

(An example of description)

Requirements equivalent or higher to security requirements defined by either of the followings shall be met. - Protection Profile for Network Devices v1.1 (PP_ND_V1.1) - collaborative Protection Profile for Network Devices (v1.0 (ND cPP v1.0) or upper)

(An example of an inspection method)

The procurement entity will understand the content of “Security Requirements based on the International Standard” and then inspect if the security functionality requirements are met by an inspection on delivery, etc.

Product area Name	Full Disk Encryption System

Threats on security	(1) <u>Unauthorized data access</u> Attackers who acquired the drive from a lost or stolen PC, tablet, etc. may attempt accessing the data on the drive.
	(2) <u>Compromising of key material</u> Attackers may obtain the cryptographic key or key material such as parameter for creating a key by exploring the drive or the other peripheral devices in the operation environment. In addition, attackers may obtain the data-encryption key by guessing permit elements of password, PIN, etc. and disclose users' data. Furthermore, attackers may attempt brute force attack against the key space to obtain the key and the key material and disclose users' data.
	(3) <u>Unauthorized update of firmware</u> Attackers may attempt to implement an unauthorized update on the firmware, aiming to compromise the security function of the encrypted drive.

Security Requirements based on the International Standard	Threats that can be countered
[1] ISO/IEC 19790 (JIS X 19790) [hardware: Security Level 2 or upper, software: Security Level 1 or upper][26]	(1), (2)
[2] collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition (V1.0 or upper) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine (V1.0 or upper) (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)

[Supplementary for Full Drive Encryption System]

In this product area, a system that encrypts the entire data storage such as the hard disk drive of a note PC or semiconductor drive, etc. is applicable. In product procurement in a general IT system architecture, it is thought to be infrequent that a procurement entity directly procures this kind of product. However, if the encryption

[26] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
At the "search for JIS with JIS standard number," of the JISC site, enter "X19790" and then it can be viewed.

function is required for the hard disk drive (HDD) of a notebook PC, tablet, etc., application of the above security requirements is recommended.
Products with the certification based on ISO/IEC 15408 (Common Criteria) for the above security requirements are already on the market.
The certification based on ISO/IEC 19790, the International Standard regarding the information security of cryptographic module, is available as well.
Though these standards were originated separately, appropriate security requirements need to be established according to the property of the product to be procured.

[How to check products with the third-party certification for the security requirements in this List]
Products that have acquired the third-party certification in these security requirements: products listed as "Certified Products" by security requirement based on International Standard." They can be searched by referring "conformance product information" (Full Drive Encryption Technology) in the "List of Requirements for Ensuring Security in Procurement of IT Products" of the following IPA website. (if a product with the certification of FIPS 140-2 assumed to be equivalent to ISO/IEC 19790 is adopted, separate check will be necessary.)
https://www.ipa.go.jp/security/it-product/fd-enc

[Examples of describing the procurement specification for using "Security Requirements based on the International Standard" and an inspection method]
(1) When security requirements equivalent or higher to "Security Requirements based on the International Standard" and the third-party certification conforming to the requirements are simultaneously required:
(An example of description)

It shall be required that Cryptographic algorithms on E-Government Recommended Ciphers List are used and either of the following certifications has been acquired. - Cryptographic module certification of "ISO/IEC 19790 (supported JIS standard: JIS X 19790) [hardware: Security Level 2 or upper, software: Security Level 1 or upper][27] (for the time being, FIPS-140-2 will also be applicable.)" - ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to "collaborative Protection Profile for Full Drive

[27] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
At the "search for JIS with JIS standard number," of the JISC site, enter "X19790" and then it can be viewed.

Encryption - Authorization Acquisition (V1.0 or upper) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine (V1.0 or upper)"

(An example of an inspection method)

Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after version upgrade. "Assurance Continuity" is prepared for a product whose version is changed, which may be able to be applied as complemented with "Assurance Continuity Maintenance Report." (Refer to (2) on P5)

In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.

(Note) in IT products, it is important that continuous version upgrade for enhancing or fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to "Security Requirements based on the International Standard" are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):

(An example of description)

It shall be required that Cryptographic algorithms on E-Government Recommended Ciphers List are used and the followings are met. - The cryptographic module test of "ISO/IEC 19790 (supported JIS standard: JIS X 19790) [hardware: Security Level 2 or upper, software: Security Level 1 or upper][28] (for the time being, FIPS-140-2 will also be applicable)" has been passed. - Requirements equivalent or higher to security functionality requirements defined in "collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition (V1.0 or upper) and collaborative Protection Profile for Full Drive Encryption – Encryption Engine (V1.0 or upper)"

(An example of an inspection method)

[28] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
At the "search for JIS with JIS standard number," of the JISC site, enter "X19790" and then it can be viewed.

The procurement entity will understand the content of “Security Requirements based on the International Standard” and then inspect if the security functionality requirements are met by an inspection on delivery, etc.

Product area Name	Mobile Device Management System

Threats on security	(1) Tapping of network Attackers may intercept communication on the network, gain its access and attempt to disclose or alter the data. Not only wired but also wireless communication may be intercepted.
	(2) Attack from network Attackers may attempt to alter the communication between the mobile device and the other endpoint on the wireless communication channel or the network base to perform spoofing. In addition, attackers may attempt to compromise the integrity of the mobile device by sending malicious administrative commands.
	(3) Physical access Confidentiality of users' data including authentication information may be compromised by loss or theft of a mobile device.
	(4) Malicious applications Among applications loaded into mobile devices, malicious codes or codes that can be exploited may be contained. With a malicious application, it may gain privileges by attacking the users' data or system software, which allows the attacker to obtain the rights to execute malicious activities. In addition, it may provide the attacker with methods of collecting peripheral information by controlling the sensors of the mobile device (GPS, cameras, microphones, etc.).

Security Requirements based on the International Standard	Threats that can be countered
[1] Protection Profile for Mobile Device Management (Version 2.0 or upper) and Extended Package for Mobile Device Management Agents (Version 2.0 or upper) (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3), (4)

[Supplementary for Mobile Device Management System]

In this product area, a Mobile Device Management system composed of two basic elements: one is the Mobile Device Management (MDM) server to manage the operation of mobile devices such as smart phone, tablet, etc., and the other is MDM agents

installed on the mobile device as an application that works in linkage with the MDM server, is applicable.
"Protection Profile for Mobile Device Management" is the minimum security requirements for what a MDM server must meet. In addition, since the management of a mobile device is realised by combination of the management server and the device agents, "Extended Package for Mobile Device Management Agents" has been established as additional security requirements that should be at least met.
Furthermore, if the product includes an IT product that is not provided on "List of Requirements for Ensuring Security in Procurement of IT Products," it is important for the procurement entity to individually establish security requirements to counter the threats that are assumed depending on the use environment.

[How to check products with the third-party certification for the security requirements in this List]
Products that have acquired the third-party certification in these security requirements: products listed as "Certified Products" by security requirement based on International Standard." They can be searched by referring "conformance product information" (Mobility) in the "List of Requirements for Ensuring Security in Procurement of IT Products" of the following IPA website.
https://www.ipa.go.jp/security/it-product/mobility

[Examples of describing the procurement specification for using "Security Requirements based on the International Standard" and an inspection method]
(1) When security requirements equivalent or higher to "Security Requirements based on the International Standard" and the third-party certification conforming to the requirements are simultaneously required:
(An example of description)

The Mobile Device Management System shall have ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to Protection Profile for Mobile Device Management (V2.0 or upper) and Extended Package for Mobile Device Management Agents (V2.0 or upper).

(An example of an inspection method)
Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after

version upgrade. “Assurance Continuity” is prepared for a product whose version is changed, which may be able to be applied as complemented with “Assurance Continuity Maintenance Report.” (Refer to (2) on P5)
In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.
(Note) in IT products, it is important that continuous version upgrade for enhancing or fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to “Security Requirements based on the International Standard” are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):
(An example of description)

The Mobile Device Management system shall meet the requirements equivalent or higher to security functionality requirements defined in Protection Profile for Mobile Device Management (V2.0 or upper) and Extended Package for Mobile Device Management Agents (V2.0 or upper).

(An example of an inspection method)
The procurement entity will understand the content of “Security Requirements based on the International Standard” and then inspect if the security functionality requirements are met by an inspection on delivery, etc.

Product area Name	Virtual Private Network (VPN) Gateway

Threats on security	(1) <u>Unauthorized data access</u> Via man-in-the-middle attack or replay attack against services in the protected network, unauthorized access by attackers from outside may be permitted, which may lead to compromise of the confidentiality and integrity of the users' data and/ or configuration data.
	(2) <u>Misuse of services</u> Due to an error in the configuration of the VPN tunnel, services may not appropriately work. In this case, communication data will not be protected as intended, and communication with unintentionally weak encryption or in plain text may be performed.
	(3) <u>Malicious update</u> Most of common attack vectors that are exploitable are ones that take advantage of attacks against vulnerabilities of software including a well-known flaw. Vulnerabilities can be removed by applying patches provided for the VPN software in a timely manner. In responding to this, attackers may attempt to trap the administrator into performing software update containing a root kit, bots or malicious codes, by which the security functions may be compromised.

Security Requirements based on the International Standard	Threats that can be countered
[1] Network Device Protection Profile(NDPP) Extended Package VPN Gateway (V1.1 or upper) and Network Device Protection Profile (v1.1 or upper) (Security Requirement Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)
[2] Extended Package for VPN Gateways (V2.0 or upper) and collaborative Protection Profile for Network Devices (v1.0 or upper) (Security Requirements Specifications based on ISO/IEC15408 (Common Criteria))	(1), (2), (3)

[Supplementary for Virtual Private Network (VPN) Gateway]

In this product area, a gateway device deployed at the end terminal of a Virtual Private Network (VPN) System that provides VPN communication is applicable.

As for the above security requirements, products with the certification based on ISO/IEC 15408 (Common Criteria) are already on the market.
Note that if there are threats on security due to the use environment other than the above-mentioned threats, establishing security requirements individually for the threats and/or taking measures from the operational aspect will be necessary. For example, when the Router/ Layer3 Switch has the Firewall function, Intrusion Detection/ Prevention function, VPN function, threats on security indicated in the product areas related to such additional functions may be assumed in addition to the threats for this product area.

[How to check products with the third-party certification for the security requirements in this List]
Products that have acquired the third-party certification in these security requirements: products listed as "Certified Products" by "Security Requirement based on International Standard." They can be searched by referring "conformance product information" (VPN Technology) in the "List of Requirements for Ensuring Security in Procurement of IT Products" of the following IPA website.
https://www.ipa.go.jp/security/it-product/vpn

[Examples of describing the procurement specification for using "Security Requirements based on the International Standard" and an inspection method]
(1) When security requirements equivalent or higher to "Security Requirements based on the International Standard" and the third-party certification conforming to the requirements are simultaneously required:
(Example of description)

It shall be required that ISO/IEC 15408 (Common Criteria) certification conforming to security requirements equivalent or higher to any of the followings has been acquired. - Network Device Protection Profile(NDPP) Extended Package VPN Gateway (V1.1 or upper) and Network Device Protection Profile (v1.1 or upper) - Extended Package for VPN Gateways (V2.0 or upper) and collaborative Protection Profile for Network Devices (v1.0 or upper)

(An example of an inspection method)
Request to submit the certificate (including material explaining to prove equality as needed) at the time of proposal or delivery and verify its validity. A third-party certification based on the International Standard is given to a specific version of a product. Therefore, the certification will be no longer applicable for the product after

version upgrade. “Assurance Continuity” is prepared for a product whose version is changed, which may be able to be applied as complemented with “Assurance Continuity Maintenance Report.” (Refer to (2) on P5)
In addition, without application of Assurance Continuity, the procurement entity will request the vendor of evidence to guarantee that the changes such as version upgrade have no impact on the security functions and then verify its validity, and if no impact is confirmed, the security requirements can be thought to be met.
(Note) in IT products, it is important that continuous version upgrade for enhancing or fixing problems on security should be implemented. Depending too much on Assurance Continuity is unnecessary.

(2) When security requirements equivalent or higher to “Security Requirements based on the International Standard” are required but the third-party certification is not requited at the same time (when the procurement entity confirms if the security requirements are met at the time of delivery of the product):

(An example of description)

Requirements equivalent or higher to security functionality requirements defined by any of the followings shall be met. - Network Device Protection Profile(NDPP) Extended Package VPN Gateway (V1.1) and Network Device Protection Profile (v1.1 or upper) - Extended Package for VPN Gateways (V2.0 or upper) and collaborative Protection Profile for Network Devices (v1.0 or upper)

(An example of an inspection method)
The procurement entity will understand the content of “Security Requirements based on the International Standard” and then inspect if the security functionality requirements are met by an inspection on delivery, etc.