JISEC

Issued on March 31, 2014

Secure Guidance Documents
Guide for Developers

Even if an IT product is equipped with security functionality, unexpected security incidents might still occur if a user operates the product without a correct understanding of the product's usage. This document focuses on guidance documents (manuals) of IT products from the little-known viewpoint of IT security and explains the required descriptions in simple terms to ensure that users operate and handle IT products securely.

Information Security Certification Office
Security Center, Technology Headquarters, IPA
www.ipa.go.jp/security/jisec/

- Table of Contents -

1 Introduction

This document is concerned with “guidance documents,” a term that refers to the operating manuals and/or installation manuals provided with IT products. Guidance documents clearly describe usage conditions and methods of use for the security functionality that an IT product provides to ensure the IT product is operated and handled securely. As such, guidance documents have a crucial role in preventing security incidents caused by a user’s lack of understanding or misuse of the IT product.

However, there seems to be few references explaining how to write guidance documents with a focus on IT security, such as what to include in IT security descriptions and from what viewpoint.

Common Criteria (CC) is an international standard on IT security evaluation. The CC defines evaluation methodologies to inspect and judge the adequacy of the security functionality of an IT product — which includes the IT product’s guidance documents — for the secure operations and handling of the IT product. This document explains the details in simple terms, which the CC requires in guidance documents to ensure the secure operations and handling of IT products.

The CC’s approach to evaluating guidance documents to assure secure operations is valid regardless of whether there are plans to actually obtain CC certification or not. It is our hope that this document will aid the reader’s understanding of the CC and improve the security quality of IT products, including their guidance documents.

1.1 Intended readers of this document

The intended readers of this document are developers who either design the security functionality of IT products or create manuals for IT products, as well as evaluators who conduct vulnerability assessments based on the CC.

The explanations in this document focus on the IT security of IT products. Please refer to other references for more general explanations on how to write manuals.

1.2 Organization of this document

This document consists of five chapters, as described below.

■ Chapter 1 Introduction

This chapter explains the objectives of this document and its intended readers.

■ Chapter 2 Overview of Guidance Document Evaluations

This chapter provides a general overview of guidance document evaluations in the CC.

■ Chapter 3 Guidance on Product Operation

This chapter explains the details required for guidance documents for secure operations of products, from the viewpoint of CC evaluations.

■ Chapter 4 Guidance on Product Acceptance and Product Installation

This chapter explains the details required for guidance documents for secure acceptance and installation of products, from the viewpoint of CC evaluations.

■ Chapter 5 Summary

This chapter provides a general summary of and considerations for the explanations given in this document.

1.3 Common Criteria standards documents

The evaluation criteria and evaluation methodology in this document are based on the standards documents listed in Table 1-1 and Table 1-2 below. The evaluation criteria and evaluation methodology are referred to as “CC” and “CEM,” respectively, in their abbreviations.

Table 1-1: CC / CEM standards documents (Japanese translation versions)

CC / CEM Version 3.1 Release 4 (CC / CEM Version 3.1 Release 4)			
Evaluation criteria: Common Criteria for Information Technology Security Evaluation (CC Version 3.1 Release 4)			
Part 1:	Introduction and general model	Version 3.1	Revision 4 [Japanese Version 1.0]
Part 2:	Security functional components	Version 3.1	Revision 4 [Japanese Version 1.0]
Part 3:	Security assurance components	Version 3.1	Revision 4 [Japanese Version 1.0]
Evaluation methodology: Common Methodology for Information Technology Security Evaluation (CEM Version 3.1 Release 4)			
Evaluation methodology		Version 3.1	Revision 4 [Japanese Version 1.0]

Table 1-2: CC / CEM standards documents (original versions)

CC / CEM Version 3.1 Release 4			
Evaluation criteria: Common Criteria for Information Technology Security Evaluation (CC Version 3.1 Release 4)			
Part 1:	Introduction and general model	Version 3.1	Revision 4
Part 2:	Security functional components	Version 3.1	Revision 4
Part 3:	Security assurance components	Version 3.1	Revision 4
Evaluation methodology: Common Methodology for Information Technology Security Evaluation (CEM Version 3.1 Release 4)			
Evaluation methodology		Version 3.1	Revision 4

This document is based on the following sections of the CC/CEM standards.

- CEM, “12 Class AGD: Guidance Documents”
- CC Part 3, “13 Class AGD: Guidance Documents”

1.4 Terms and definitions

Table 1-3 lists the terms related to CC/CEM used in this document.

Table 1-3: CC / CEM terms and definitions

Term	Explanation
CC (Common Criteria)	The Common Criteria is the ISO/IEC 15408 international standard for evaluating, from the viewpoint of information security, that an IT product is adequately designed and that the design is implemented correctly.
CEM (Common Evaluation Methodology)	The Common Evaluation Methodology is the established evaluation methodology for consistent security evaluations based on the CC. It defines evaluation items and evaluation viewpoints to satisfy the CC standard.

2 Overview of Guidance Document Evaluations

The CC specifies evaluation contents that guidance documents for IT products should include. This chapter provides a general overview of guidance document evaluations in the CC.

2.1 Objectives of guidance document evaluations

Guidance documents for an IT product describe instructions and guidelines on the product's usage so that a user can appropriately operate the IT product. Incomplete, misleading, or unreasonable descriptions in a guidance document may cause the user to fail to take the necessary management measures for the IT product or lead the user to use the product incorrectly. As a result, the user may continue to operate the IT product in a manner that is insecure but the user believes is secure. Under such circumstances, critical information handled by the IT product may be exposed to tampering or leaked without user's being noticed.

In the guidance document evaluations of the CC, the following contents are to be evaluated in order to assist secure operations by users, which assure the guidance document descriptions not to be misunderstood or misused by users.

- Guidance documents shall clearly describe the assumptions, setting values, inputs, interactions between operations, and effects of operations pertaining to security, in such a way that users can understand these aspects prior to operating the product.

- Guidance documents shall explain those operations which might influence on security without omission so that users would be never at a loss about what to do next.

- Guidance documents shall describe critical matters that might influence on security in such a way that users would not overlook them, such as calling attention to critical matters with warnings.

2.2 Scope of guidance document evaluations

Guidance document evaluations in the CC cover all procedural guidance documents from product acceptance by the procurement personnel to product operation, as shown in Figure 2-1.

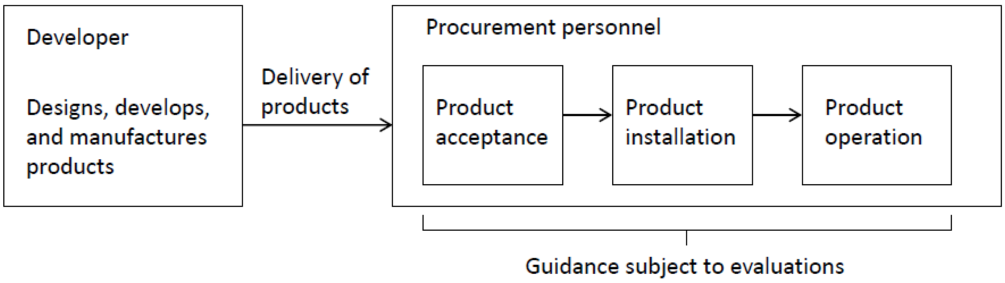

Figure 2-1: Scope of guidance

Procedures carried out by procurement personnel consist of the following three stages.

■ Product acceptance

In this stage, procurement personnel accept the purchased product. The concern here, from the viewpoint of security, is whether some vulnerability has been introduced to the product, either through tampering to the product during transport or because the product with an incorrect configuration has been mistakenly delivered, due to some errors. Guidance documents must describe the procedures by which the procurement personnel confirm that the received product is the correct version of the purchased product and that the product has been delivered without any mistakes.

■ Product installation

In this stage, procurement personnel set up and/or install the product. The concern here, from the viewpoint of security, is whether some vulnerability is introduced to the product due to the operational environment in which it is installed and the setting which the developer did not expect. Guidance documents must describe the requirements for operational environment and the procedure to install the product in such a way that procurement personnel can accurately install the product without misunderstandings.

■ Product operation

In this stage, procurement personnel operate the product. The concern here, from the viewpoint of security, is whether procurement personnel unintentionally operate the product in a state where the security functionality is compromised, due to a lack of understanding of the product or misuse of the product. Another concern is whether critical information is leaked from the product not just during operations but also after the product is no longer in use and discarded. Guidance documents must describe the requirements and usage for secure product operations in such a way that procurement personnel can accurately operate the product without misunderstandings.

The next two chapters explain in detail the CC requirements on guidance documents in these three stages; guidance on product operation, followed by guidance on product acceptance and product installation.

3 Guidance on Product Operation

This chapter explains what is required for product guidance documents for secure product operations, based on the guidance document evaluations in the CC.

3.1 Assumed user roles associated with the product

(1) Objectives

Guidance documents for an IT product describe the product’s method of operation so that users understand the product’s security functionality and handle the product securely. The contents, however, may vary depending on different user roles, such as administrators or general users. Therefore, guidance documents for an IT product must clearly describe the product’s assumed user roles and the security privileges given to each user role.

With these descriptions, each user should be able to clearly ascertain the scope of functions he/she is authorized to control and the security requirements he/she must pay attention to. The descriptions can also help the organization understand what form of management is needed to operate the product and what roles and privileges should be given to the organization’s users as a reference for developing operation plans.

(2) Details that should be stated in guidance documents

Guidance documents for an IT product must clearly describe the following details related to user roles.

■ Identifying user roles

In general, there are various roles for IT product users. Typical examples include administrators who manage the product and general users who use the product’s functions. For some products, the privileges of administrators and general users are further subdivided, such as providing separate privileges for administrators and auditors. Other possible roles include programmers who develop programs using interfaces provided by the product.

Guidance documents must identify all the assumed user roles for the operations of the product without omission.

■ Functions and privileges for each user role

Guidance documents must describe, for each assumed user role, the user-accessible functions of the IT product, the assigned privileges, the details of functions and privileges that must be controlled, and the types of commands required for them.

Regarding the specific structure of guidance documents, note that separate documents may provide guidance for administrators and guidance for general users, or a single guidance document may contain descriptions for each user role. The CC does not specify any rules on the structure of guidance documents, but it is important to describe the required details for each user role in a comprehensible manner.

3.2 Calling attention with warnings

(1) Objectives

Even if the guidance documents for an IT product contain all the required contents without omission, users may overlook critical details, which may lead to incorrect operation of the IT product.

It is necessary that guidance documents include warning statements, which are distinguished in some way from ordinary details, in order to call the user's attention to critical matters on the IT product's security. By adding such warning statements, the developer can ensure that users will be aware of critical security matters and not overlook them. It is also important for the developer to supply warnings about any operations that cannot be securely assured as a means of clarifying the scope of product liability.

(2) Details that should be stated in guidance documents

The sections below explain the details of warning statements that guidance documents should describe.

1) When warnings are required

Warning statements are understood to be necessary when there is reasonable concern that a user operation may compromise the product's security assurance or cause disadvantages to the user. The following examples illustrate cases where warnings are required.

■ Assumptions about the security functionality of a product

The security functionality of a product is designed to protect the user's critical data from various threats. However, there are still some conditions on the user's side that the product's security functionality cannot address.

For instance, consider a security function that authenticates users with a user ID and password and permits only users who successfully pass the authentication to use the product. In this case, the developer must not merely implement an ID and password authentication function, but the developer is required to implement the security function in such a way that it can prevent attacks that exploit the authentication function's vulnerabilities, such as repeatedly guessing passwords. However, no matter how strong the developer enhances the product's security function, the product's security function cannot address a situation where the password is leaked to another person due to the user's carelessness. In other words, in case of authentication function using IDs and passwords, it is an assumption that users will not reveal their passwords to other people, in order for the security functions to effectively work.

Warnings are necessary to call attention to any assumption like this for the effective operations of the product's security functions.

■ Operations that may deteriorate or disable the product's security functions

Some products may provide functions that allow the administrator to enable or disable the product's security functions or customize the behavior of the product's security functions. Should a product provide such functions, there is concern that security functions may not efficiently work depending on administrator's settings.

Warnings are necessary to call attention to such operations that may deteriorate or disable the product's security functions.

■ Constraints to avoid product vulnerabilities

When a product has a known vulnerability, the developer may choose to address the vulnerability by placing constraints (commonly called "workarounds") on the product's method of operation to prevent the vulnerability from occurring rather than improving the product. Warnings are necessary to call attention to any constraints placed to avoid product vulnerabilities.

For instance, consider a product whose security function cannot protect it from attacks via a LAN from the time when the product is powered on until it reaches a fully operational state. As a security measure during this start-up period, the developer may state a warning in the guidance documents not to connect the product to a LAN until the product has reached the operational state.

Nevertheless, the workaround must be reasonable to the user in terms of content, as explained later in Section 3.6 "Considerations for descriptions." The workaround cited in the example above — not to connect to a LAN until the operational state is reached — cannot possibly be accepted by users for a product designed to be operated remotely. When the workaround is not reasonable in terms of content, the developer must address the problem by improving the product so that it does not occur any more.

■ Operations that cannot be undone

Products may have a function that, once executed, causes a loss of user data that cannot be undone. For example, consider a hard disk encryption setting that involves initializing the disk prior to the encryption, which may delete user data on the disk.

Warnings are necessary to call attention to any operations that cannot be undone and may influence on users.

2) Notation of warnings

Warning statements must be described in guidance documents in such a way that they are clearly distinguishable from ordinary statements and that they will not be overlooked by users. In general, warning statements are emphasized by using a mark, etc., highlighting that the statement is a warning.

There is concern that a simple warning notation — such as "Warning: Do not ..." — will not be followed by users because users do not fully comprehend the warning's significance. Therefore, warning statements must be given along with a supporting explanation so that users can comprehend the necessity of following the warning. For example, compare the following two statements:

(a) Warning: When turning on the product, do not connect the product to a LAN until the start screen appears.

(b) Warning: When turning on the product, do not connect the product to a LAN until the start screen appears. Because the security functions are not running during this time, attackers may be able to access your critical information if the product is connected to a LAN during this time.

Statement (a) does not explicitly mention why the warning must be followed. Therefore, some users may continue to power up the product while connected to a LAN until some obvious malfunction occurs in the product's operation. With statement (b), on the other hand, users can clearly understand the significance of the warning from the supporting explanation.

There are three types of supporting explanations for warnings:

- Possible side effects
- Expected effects
- Interactions with other functions and privileges

There are no clear criteria on which of the three types should be selected. The developer should select the appropriate type that best explains the warning statement.

Instead of using the word "warning," guidance documents typically use "important" or "caution" to indicate important statements. On occasion, a guidance document may use several terms to indicate different levels of importance. The CC does not specify any rules on what words should be used to indicate a warning.

3) Examples of warning statements

The following explain three types of example warning statements:

■ Example of a warning accompanied by a possible side effect

In the example below, the warning statement includes a possible side effect. With this statement, users can understand the significance of the warning and comprehend the influence on security that might cause disadvantage to themselves. This is the most common form of warning statements.

[Warning]
Do not change the default values. Changing the default values will disable the security functions, which may unintentionally leak your critical information.

■ Example of a warning accompanied by an expected effect

In the example below, the warning statement includes an expected effect. With this statement, users can understand the significance of the warning.

[Warning]
Always restart the product after changing any settings. Only changing settings will not change the behavior of the product. The new setting will be reflected after the restart.

■ Example of a warning accompanied by an interaction

In the example below, the warning statement includes an interaction with another function. With this statement, users can understand the significance of the warning.

[Warning]
Configure the setting for the encryption function in advance before enabling this function. Data used by this function are encrypted according to the encryption function settings.

3.3 Secure usage for user interfaces

(1) Objectives

"User interfaces" refer to interfaces provided by the product for user operations, such as operation panels, commands, and programming interfaces.

If a user operates a user interface in a manner different from the usage assumed by the developer, the product, even if it is equipped with security functions, may behave incorrectly, leaving the product in an insecure state.

Consequently, guidance documents must clearly describe methods of securely using user interfaces in a way that is understandable to users.

(2) Details that should be stated in guidance documents

Guidance documents must, for each user role, describe the overview of the security functions provided by the product as well as the secure usage of all user interfaces provided by the product. The sections below explain the details that guidance documents should describe.

1) Overview of the security functionality

Guidance documents must, for each user role, describe the overview of the security functions provided by the product, along with the description of the related user interfaces. With this overview, users can obtain an overall picture of the security functions and understand the relationships between the operations available to the users and the security functions.

2) Purpose, behavior, and interrelationships of the user interfaces

Guidance documents must describe the purpose and behavior of user interfaces as well as interrelationships with other interfaces.

User interfaces generally have the functionality related to the interfaces' original purposes and their associated security functions. Developers tend to focus on explanations of the former functionality. However, when interface operations by a user trigger actions associated with the security functions, these details must be described without omission.

Example (in case of a command that prints files)

Purpose: This command prints the file specified by the user.

Function: This command performs the following steps:

(1) It checks the access privilege to the specified file.

(2) It prints the file if the user privilege allows access to the file.

* The result of the access privilege check is recorded in an audit log. Refer to the audit command to see how to view audit logs and the recording formats.

* The statement above not only describes file printing, which is the original purpose of the interface, but also describes the interface's security functions, such as the access controls and recording audit logs that are performed at the same time. The statement also contains the interrelationship with other interfaces, such as how to view audit logs.

3) How to invoke the user interfaces

Guidance documents must describe the method of invoking each of the user interfaces to eliminate any confusion on the user's behalf. Below are some examples of descriptions depending on the types of user interfaces.

- In case of a screen
  The guidance describes the procedure to display the intended screen.
- In case of a command
  The guidance describes the format of initiating command lines. It also includes descriptions of how to specify any options.
- In case of a programming interface
  The guidance describes the format of invoking functions and methods, etc. When there are any necessary declarative statements to use functions, etc., such as #include statements in the C programming language, the guidance also includes the specification.

4) User interface parameters

It is necessary to describe the following details about the user interface parameters so that users can understand the meaning and their influences on security.

- The parameters that users can set and their purposes
- Each parameter's valid values and default values
- Each parameter's secure values and insecure values

The following is an example of a parameter description.

Example (in case of an administrator command that sets the minimum password length)

Parameter: Minimum password length

Purpose: It restricts the minimum length of passwords when users set.

Valid values: Integers between **4** and **16** (default value is **8**)

[Warning]For security purposes, a value must be **8** or higher.
Setting a value less than **8** will increase the risk of unauthorized login.

* In the example above, the parameter’s valid values are between 4 and 16; the default value is 8; the secure values are between 8 and 16; and the insecure values are between 4 and 7.

Parameters on some products may have valid values or secure values that could change due to the combination of several parameters, instead of having a single parameter setting. Guidance documents clearly describe such combination conditions on the parameter values as well.

For example, consider an administrator command, in which the first parameter is the encryption algorithm and the second parameter is the encryption key length. In this case, the valid values and secure values of the encryption key length will vary according to the encryption algorithm selected — DES, AES, or RSA.

5) Output messages and responses of user interfaces

Guidance documents must describe the output messages and responses when using user interfaces. With these descriptions, users can ascertain that the operation they invoked was executed correctly or, in the case of a failure, confirm what kind of error occurred.

It is also required that guidance documents describe the method of handling errors in case they occur. Refer to Section 3.4 “Methods of handling security-relevant events” and Section 3.6.1 “To describe methods of secure operations for all operations” for more information.

6) Advice on secure usage for user interfaces

Guidance documents must provide advice on secure usage for user interfaces. Secure usage includes the following:

- Methods of using interfaces to securely operate the product
- Methods of using interfaces to effectively use the security functions

For secure usage, it tends to focus on explanations of the security functionality provided by the product. However, explanations for the secure operations and handling of the product are needed even for interfaces without security functionality.

Below are examples of advice on secure usage.

■ Advice example 1 (secure operations)

Suppose that a product provides both interfaces for receiving emails: a POP interface that does not use encryption and a POP over SSL interface that uses encryption. In this case, the advice on secure usage must include not only the description of the usage for the POP over SSL interface but also the explanation of the secure usage for the POP interface, even though the encryption function is not applied to this interface.

> **[Warning]**
> Using mailing software that supports POP over SSL is recommended for receiving emails. Emails received using POP may be intercepted because they are not encrypted under POP.
>
> If you have no choice but to use POP, pay particular attention to the network environments you use and the contents of your emails.

* In the example above, a secure usage for the POP interface is described after the warning.

■ Advice example 2 (effective use)

> **[Usage tip]**
> This product can be separately configured for administrators who manage users, etc., and auditors who can view audit logs. By using this function to separate administrators and auditors, objective audits can be conducted for the operations of administrators as well.

* In the example above, an effective usage of the product-specific functionality that is desirable from the viewpoint of security is described.

■ Advice example 3 (effective use)

> **[Usage tip]**
>
> It is recommended that the audit logs are regularly backed up. This product can store audit logs up to 10,000 records. The maximum number of days that the audit logs can be stored depends on the usage condition of the product. For example, you can estimate the required backup frequency by operating the product for a few days and observing the volume of output for the audit logs.

* in the example above, advice on an effective usage pertaining to the backup frequency, which many administrators may be concerned about, is described.

3.4 Methods of handling security-relevant events

(1) Objectives

"Security-relevant events" refer to events related to security that occur as a consequence of product operations and that the user must address, such as updating product user registrations or handling failures.

If a user encounters such a security-relevant event and attempts to address it by taking trial and error, instead of taking the appropriate actions or performing the required operations, the product's security may be compromised, leaving the product in an insecure state.

Guidance documents must adequately describe the method of handling each type of security-relevant event that users may encounter, so that users can continue to securely operate the product.

Such descriptions are useful not only when users encounter a security-relevant event but also when users want to know the management aspects that users must be prepared to address prior to operating the product.

(2) Details that should be stated in guidance documents

The sections below explain the details related to security-relevant events that guidance documents should describe.

1) Identifying security-relevant events

Guidance documents must describe without omission all the possible security-relevant events arising as a consequence of product operation that users may encounter.

This requires the developer to analyze the usage of the security functionality provided by the product and to work out all the possible security-relevant events that users may encounter. As shown below, events that require users to perform some operations, such as changing the configuration of the product, are considered security-relevant events.

■ Events arising from user circumstances

Due to user circumstances, the product's configuration may need to be changed. Some examples of this are:

- Registering, changing, or deleting users
- Changing the filtering rules, etc., of firewalls

■ Events arising from the security functionality

The security functionality provided by the product may cause events during operation. Some examples of this are:

- A user is locked out after repeatedly failing password authentication
- Alarm notification, such as audit logs

■ Failures

Various failures also fall into security-relevant events.

- Errors detected by the product and notified to users
- Other unexpected failures

In the guidance documents, the developer must describe the analyzed and identified security-relevant events, as shown above, as events arising from the user viewpoint, such as "when registering a user" or "when the password is locked."

2) Method of handling each type of security-relevant event

Guidance documents must describe, for each type of security-relevant event, which user role performs which operation. Care must be taken with the following aspects of descriptions:

- All necessary operations for each type of the security-relevant event should be described.
- All cautions related to security should be described without omission.

The following is an example of the description of a security-relevant event.

When registering a user

Log in with administrator privileges and register the new user's name with the USER_ADD command, and then set a password with the PASSWORD command.

The following shows an example of registering a user "taro."

```
# USER_ADD taro
   User "taro" has been newly created
# PASSWORD taro
   Enter the new password: ********
   Re-enter the new password for confirmation: ********
   The password for user "taro" has been set
#
```

[Caution] The character string of the password must be longer than the preset minimum password length and contain letters and numbers, including at least one special character. See the description of the PASSWORD command for details.

* The example above explains all necessary operations for user registration.

3.5 Operational environment conditions for secure operations

(1) Objectives

Many IT products, for secure operations and handling of the product, have conditions on the operational environment, such as the product's installation location, the product's users, and other IT devices. If the operational environment conditions are not complied with, the product, even if it is equipped with security functions, may not function correctly and may not be able to protect the user's critical data, etc.

Guidance documents must clearly describe not only how to use the functions provided by the product but also conditions on the operational environment that the product relies on for secure operations and handling of the product.

(2) Details that should be stated in guidance documents

Guidance documents must describe without omission all conditions on the operational environment for the secure operations and handling of the product. Many conditions on the operational environment must be called to the user's attention through warnings, etc., as explained in Section 3.2, so that users will be certain to follow the conditions.

Below are some considerations for conditions on operational environments.

■ Physical conditions

These are physical conditions, such as locations where the IT product is to be installed. For example, if a product has not been designed to prevent attacks in which the internal hard drive is removed and analyzed, a possible condition can be considered that the product must be placed in a computer room with controlled access where only trusted administrators can operate the product.

■ Personnel conditions

These are conditions that users of the IT product must comply with. For example, if a product provides an identification and authentication function using IDs and passwords, then a possible condition can be considered that users must control their own passwords so that the passwords are not revealed to anyone else.

■ Structural conditions

These are conditions on other IT devices that the IT product relies on. For example, if the IT product is an application program, then a possible condition can be considered that the operating system's user accounts and access privileges are configured properly and that there will be no known vulnerabilities in the operating system, so that the operating system, which provides the operational environment for the IT product, cannot be adversely exploited with attacks. Other structural conditions include specifications and configuration conditions required for other IT devices in order to assure the behavior of the IT product.

The developer must consider the viewpoints above and identify all conditions on the operational environment necessary for secure operations and handling of the product. It is useful, in doing this, to analyze whether the product's functions can prevent various attacks that tamper with or bypass the product's security functions. This will clarify the limits of attacks that can be dealt with by the product itself, and conditions on the operational environment are then derived to supplement the parts that cannot be addressed by the product's functions.

See the reference below for an analysis of attacks on security functions and the corresponding protection mechanisms.

IPA: Security Architecture Guide for Developers
http://www.ipa.go.jp/security/jisec/apdx/documents/SecurityArchitectureGuide_e.pdf

3.6 Considerations for descriptions

This section provides considerations to be followed in guidance documents when describing the security viewpoints explained in the previous sections.

3.6.1 To describe methods of secure operations for all operations

Guidance documents must clearly describe the influence on security and the method of secure operations for all operations that the product provides to users, so that users can fully understand them. If a user encounters a situation requiring the operations not described in the guidance documents and attempts to address it by trial and error or performs an operation without fully understanding the consequences of the operation, the product's security may be compromised, leaving the product in an insecure state.

When describing all operations, particular care must be taken with descriptions of the "operation modes." The sections below explain operation modes.

(1) Explanations of all the operation modes

"Operation modes" refer to operational states in which a product behaves in a different manner from other operational states. The following examples fall into operation modes:

- An operation mode like Windows’s Safe Mode
- An operation mode used for the product’s maintenance
- When the product is made to behave in a different manner by, for example, changing its configuration
  (such as a state with the security functionality disabled, or a state in which a function behaves differently)
- A state where a special operation is required that differs from ordinary behavior due to, for example, the occurrence of an error
  (this includes operations like a document editing program’s “file recovery mode” that runs when opening a damaged file)

Guidance documents must describe the purpose, the usage, and the method of confirming the current operation mode for all the operation modes provided by the product. Explanations of operation modes may be described separately in guidance documents, or they may be included in the usage, described in Section 3.3, or the methods of handling security-relevant events, described in Section 3.4.

(2) Explanations of the influence that affects security for operation modes

Guidance documents must describe any possible influences on security after executing an operation, so that they can be understood before executing the operation. For critical matters, the user’s attention must be called through warnings, etc.

(3) Methods of recovery after an operation

Guidance documents must describe how to restore the original secure operational state after executing an operation that has influenced on security or after transitioning to a special operation mode due to, for example, the occurrence of a failure.

Particular care must be taken with the following aspects of descriptions.

■ Recovery from all operations, including operation errors

Executing operations includes operation errors. Therefore, guidance documents must describe how to recover from expected situations where the user has accidentally executed an operation even though the operation is prohibited as an assumption of the product.

Many developers may feel that “they should not provide guidance on operations prohibited as assumptions of the product’s operations since the behavior of the product is not assured.” However, as long as the product provides these operations to users, it is the responsibility of the developer to provide guidance on all possible secure operations for users. This is no different from guidance for physical safety provided with everyday products. For example, strong cleansers usually have a warning — such as “Caution: Do not get into eyes. It may cause loss of vision.” — followed by a description of the method of recovery from the action prohibited in the warning — such as “If the product gets into eyes, flush eyes immediately with running water and make sure to consult a physician.” Similar descriptions are required in guidance documents for IT products as well.

■ Restoring a product to its secure operational state

Methods of restoring the product to its secure operational state vary depending on the security functions related to the executed operation.

For example, suppose a product is being operated with the transmission encryption function provided by the product disabled during the network transmission from the product to an external device. In this case, the transmitted data is the only thing that is being influenced. Consequently, in order to restore the product to its original secure operational state, all that is required is to reset the setting of the transmission encryption function to be enabled.

On the other hand, consider another example where the configuration of a product’s login function has been changed so that anyone can login with administrator privileges. In this case, various configurations or audit logs of the product may be changed while the product is in operation. Consequently, in order to restore the product to its original secure operational state, it is not sufficient to simply reset the configuration of the login function to its original setting. Guidance documents must provide the procedure needed to confirm that all settings operate as the administrator intended or else provide the procedure needed to restore the product to the factory settings and then reconfigure all settings.

Note that, even if failures occur, the details that should be described in guidance documents may vary depending on the influences on security, instead of calling maintenance personnel, which is a stereotypical response.

For example, consider a situation where an error has occurred while reading and writing to a hard disk. Despite the error, it may still be possible to read other blocks on the hard disk than the location where the error occurred. Therefore, in consideration of the information leakage from the hard disk, some advice would be necessary on how to ensure the data on the hard disk that cannot be read, instead of just requesting maintenance personnel to replace the hard disk.

3.6.2 To give clear descriptions so that guidance is not misunderstood or misused

Guidance documents must provide descriptions of security viewpoints without omission, as explained in the previous sections. Missing or inadequate descriptions may cause the guidance to be misunderstood or misused.

Particular care must be taken with the following aspects of descriptions.

■ Insufficient descriptions of warnings

Users may not comprehend the importance of a critical matter and, thus, overlook the matter if no warnings are given despite the importance of the matter or if a description equivalent to a warning is given but not suitably emphasized.

■ Insufficient explanations of dependencies

If explanations of security functionality dependencies in a product are inadequate, users may change the configuration of the security functionality and operate the product without being aware of the influences on other security functions.

Furthermore, if a product’s security functionality or secure usage is dependent on other IT devices and those dependencies are not explained adequately, users may operate the product without being aware that it is in an insecure state due to the influence of the IT devices it depends on.

■ Functions that are easily misunderstood

If a product’s security functionality is not consistent and its explanation is not adequate, users may operate the product using a certain function believing, as a matter of course, that the same security functionality is applied.

Below are some examples of inconsistent security functions:

- A remote printer either applies or does not apply user authentication depending on the communication protocol selected in the printer’s configuration.
- Because of the difference between the product’s console and user interface, such as Web screen, the session timeout lengths and the number of password entry attempts may differ.

If there is such inconsistency in the security functionality, it is necessary to call the users’ attention in guidance documents so that users will not misunderstand. Essentially, however, it is not desirable to have inconsistent security functions. It is recommended that developers design and develop products so that a consistent security policy is applied to all functions.

In addition to the aspects given above, it is important that guidance documents themselves are described in a comprehensible manner from the user’s viewpoint and have consistent descriptions. Please refer to other references for more general explanations on how to write manuals.

3.6.3 Operations are to be reasonable

The contents of guidance documents must be reasonable to be acceptable by users. If the contents required for the product’s operation or the product’s operational environment, impose excessive burdens to users, it makes difficult to maintain secure operations, and these guidance documents are not considered reasonable.

In particular, when vulnerabilities are discovered in the product’s security functions, there is a case where special constraints are demanded in order to avoid the vulnerabilities with the operation of the product. When such a case occurs, the developer must examine the constrains whether they can be realistically addressed and whether they will be accepted by users. Even if a workaround is theoretically feasible, the developer must instead improve the product’s functionality when it imposes excessive burdens to operate in reality and is not accepted by users.

4 Guidance on Product Acceptance and Product Installation

For the secure acceptance and installation of products, this chapter explains the details that are required for guidance documents of the products, based on the guidance document evaluations in the CC.

4.1 Secure product acceptance

(1) Objectives

Procurement personnel may receive a product different from the one they intended to purchase. For example, the product may have been tampered with during transport or the product may have been mistakenly delivered with the wrong configuration or missing parts, due to some errors. As a result, the product is left in an insecure state and the procurement personnel operate the product without realizing it, which causes various security problems.

Guidance documents must describe the procedures for procurement personnel to confirm that the correct version of the product they purchased has been delivered without mistakes.

(2) Details that should be stated in guidance documents

The following sections explain the details that guidance documents should describe for the secure acceptance of products by procurement personnel.

■ Confirming that a product has not been tampered with

Guidance documents must describe the procedures for procurement personnel to confirm that a received product has not been tampered with during transport. The confirmation procedure at product acceptance depends on the security measures that the developer has taken to prevent product tampering when the product is delivered.

Regarding guidance for software products or digital data, procurement personnel can confirm that a received product has not been tampered with by, for example, verifying a digital signature or hash values sent prior to the product's delivery. For hardware products or guidance created in bound form, procurement personnel can confirm that a received product has not been tampered with or opened during transport by, for example, confirming the tamper-resistant seal affixed to the package when the product is sent. Guidance documents describe such confirmation procedures.

■ Confirming that a product contains all its parts

Guidance documents must describe the procedures for procurement personnel to confirm that a received product contains all its parts. With software products in particular, an optional license is sometimes needed to use security-relevant functions. Guidance documents must describe the procedures to confirm that the product contains all its parts, including such options.

For example, when a software product consists of a media and a license key, the guidance documents describe the procedures to confirm whether the license key and other configuration information entered when configuring the product are complete, in addition to confirming the media that contains the software product. When a software product has been delivered with an optional license already entered, the guidance documents describe the procedures to confirm whether the license has been entered correctly, such as starting the product and displaying the entered license.

■ Confirming that all parts of a product are the correct versions

Guidance documents must describe the procedures for procurement personnel to confirm that a received product is the correct version. In addition, guidance documents must describe confirmation procedures of versions for all parts that can be individually identified, such as execution programs and their guidance documents.

For example, procurement personnel can verify the version of a product with labels affixed to the product itself or the media that stores the product, or with version information displayed within the software product. The developer describes these procedures to confirm those versions in the guidance documents so that procurement personnel can perform the procedures without mistakes.

4.2 Secure product installation

(1) Objectives

After accepting a purchased product, procurement personnel perform various installation operations, such as configuring the product, and start operating the product. If the procurement personnel, during the product installation process, configure or set the product up in a manner that the developer did not intend, the product's security functionality may not operate correctly, leaving the product in an insecure state.

Guidance documents must describe the requirements and the procedures on the operational environment to install the product, so that the procurement personnel perform these procedures correctly without misunderstandings.

(2) Details that should be stated in guidance documents

The following sections explain the details that guidance documents should describe for the secure installation of products by procurement personnel.

1) Requirements on product installation

Guidance documents must describe requirements on product installation for the reliable operation of the security functionality. Below are some examples of requirements:

- Minimum system requirements
- Operations assured with other IT devices that the product depends on
- Requirements on the operational environment, such as the installation location

2) Product installation procedure

Guidance documents must describe the procedures, including configuration operations that procurement personnel have to perform to get the product into a secure operational state.

The product installation procedure must be described in sufficient detail to meet the following:

- Each step that must be performed is described
- The user can confirm the success or failure of each step

- The user can clearly understand the next step to be performed in accordance with the results of each step

When the security functionality is stopped or deteriorated while the product is in its default configuration, guidance documents must include the procedures to configure the product in the product installation procedure so that the security functionality will sufficiently function.

It is recommended, however, that the developer design the default configuration of the product so that the security functionality will sufficiently function. Such "secure by default" products are in a secure state when delivered, and users will be responsible for any configuration changes, such as disabling the security functions for user convenience. This mitigates the risk of using products in an insecure state without users' realizing it.

3) Methods of handling problems when they occur

Guidance documents must describe methods of handling exceptional events and problems, such as when the product has transitioned to a state different from the ones in a procedure, or when an error is displayed.

For example, guidance documents should describe how to confirm contents that are easily misunderstood by users, or how to contact customer support if an unexpected problem occurs.

4.3 Considerations for descriptions

Developers must take the same care when describing the guidance documents on product acceptance and installation, as with the guidance documents on product operation in Chapter 3. However, the guidance documents on product acceptance and installation guidance center on descriptions of procedures that users must perform. Therefore, developers must be particularly careful about the following aspects of their descriptions.

■ To be complete

Guidance documents must include, without omission, all procedures and assumptions necessary for secure acceptance and installation. If descriptions of necessary procedures or assumptions are inadequate, users may operate the product in an insecure state.

Particularly, developers have already configured various settings to their own environments they use. For this reason, developers must pay attention to the fact that they may not notice some missing descriptions in guidance documents because problems do not appear, even if procedures that actually should be performed are omitted in their own environments.

■ To be clear

Every step of procedures in guidance documents must be clearly described so that users will not become confused in the middle of an operation. If the procedures are not clear, users may take trial and error and perform an operation unintended by the developer.

Particularly, developers must pay attention to the fact that they may not notice how difficult their descriptions are for the installing users, because the developers are very familiar with the product's operation.

■ To be reasonable

Descriptions in guidance documents must be reasonable, so that the contents of guidance documents can be performed without imposing excessive burdens on users. For example, it is not reasonable to demand that users confirm the product version by checking information that is displayed only momentarily during the start-up of the product.

5 Summary

This document has explained the descriptions and considerations for descriptions, required for guidance documents of IT products, to help users securely operate products, based on the CC, an international standard for evaluating IT security.

The important point is that users will not operate a product without realizing that the product has fallen into an insecure state.

This is why the CC requires developers to clearly describe the assumptions and usage for secure operations of the IT products, with warnings, etc., in such a way that users will not overlook or misunderstand the guidance.

For the secure usage of IT products, developers are required not only to describe how to use each operational menu or command, but also describe user roles, management operations that users should perform, and events that users may encounter. These must be described so that users can assume various use cases referring to the guidance, and users can operate the products in response to these use cases without mistakes and without taking trial and error.

Furthermore, descriptions in guidance documents must be consistent with the security functions and security architecture implemented in the product. Product operations in accordance with the guidance and the product’s functions also mean to protect the user’s critical data, etc.

It is important that developers, when developing a product, design the product’s security functions and security architecture in consideration of how the product will be operated. Furthermore, if the developed products are not supplied with adequate guidance, users may use the product’s functions incorrectly, leading to security incidents.

It is our hope that this document will help improve security, including how products are operated.

Secure Guidance Documents Guide for Developers

March 31, 2014 First edition

Author and Publisher Information-technology Promotion Agency, Japan (IPA)

Writers Information Security Certification Office