

Information Security Early Warning Partnership

- Overview of Vulnerability Handling Process -

■ Framework Establishment

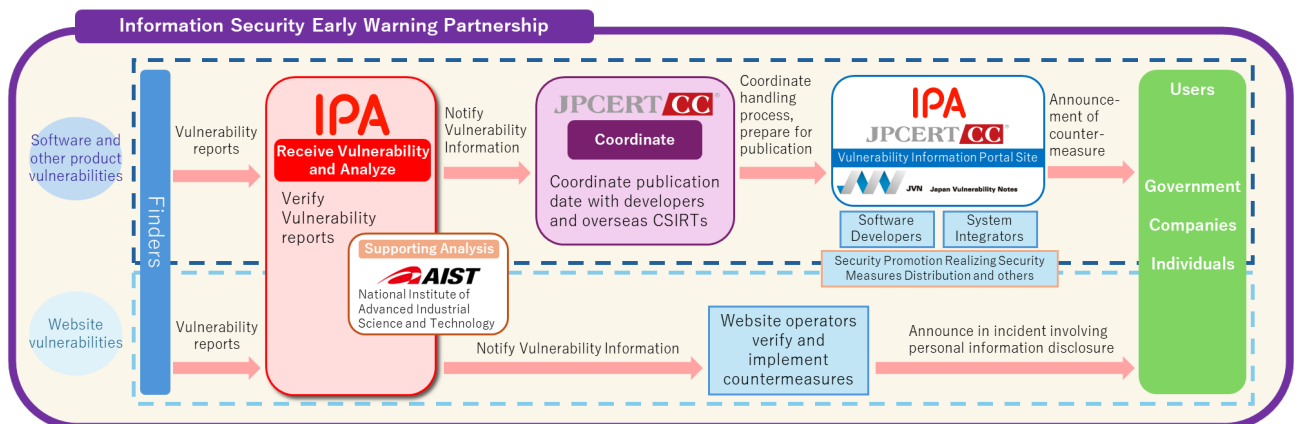
To ensure appropriate handling of vulnerability-related information when a vulnerability is reported in order to reduce the damages caused by unauthorized computer access, computer viruses and so on, the Public Notice from the Ministry of Economy, Trade and Industry on “Standards for Handling Software Vulnerability Information and Others” was issued in 2004. After its amendment in 2014, this Public Notice was shifted to “Standards for Handling Vulnerability-related Information of Software Products and Others” in 2017, which has been partially amended in 2024.

Based on these Standards, the “Information Security Early Warning Partnership Guideline” (referred to below as, “guideline”) stating the recommended actions to relevant parties was established, to achieve an appropriate flow of vulnerability-related information*1. Specifically, the Information-technology, Promotion Agency (IPA) serves as the contact organization, while the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) serves as the coordinating organization. These organizations make efforts to handle vulnerability-related information properly with all relevant parties, including finders, software developers and website operators. This process is in alignment with ISO/IEC 29147:2014 “Vulnerability disclosure.”

■ Scope of Framework

The guideline covers vulnerabilities that may affect many or unspecified persons; specifically, software products widely used in Japan and web applications that run on websites deemed to be accessed primarily from Japan (for example, websites written in Japanese, websites running on a “.jp” domain). This brochure has been prepared to provide the relevant parties an overview of the guideline, describing how vulnerability-related information should be handled. The table below shows the advantages of being a part of the Information Security Early Warning Partnership. These efforts can reduce the likelihood that software users and website operators will be affected due to vulnerabilities.

Relevant Parties	Advantages of Information Security Early Warning Partnership
Finders	<ul style="list-style-type: none"> • Can prompt software developers and website operators to take countermeasures against vulnerabilities through a public entity. • May be publicly credited on an advisory when the vulnerability countermeasure information is published.
Software Developers	<ul style="list-style-type: none"> • Can learn about non-public vulnerabilities that may affect their own products. • Can make users publicly aware of how to address vulnerabilities. • Can demonstrate that they are seriously engaged in addressing vulnerabilities.
Website Operators	<ul style="list-style-type: none"> • Can address their websites before the existence of a vulnerability becomes widely known. • Can check for and address previously unnoticed vulnerabilities. • Can improve user safety on their websites.



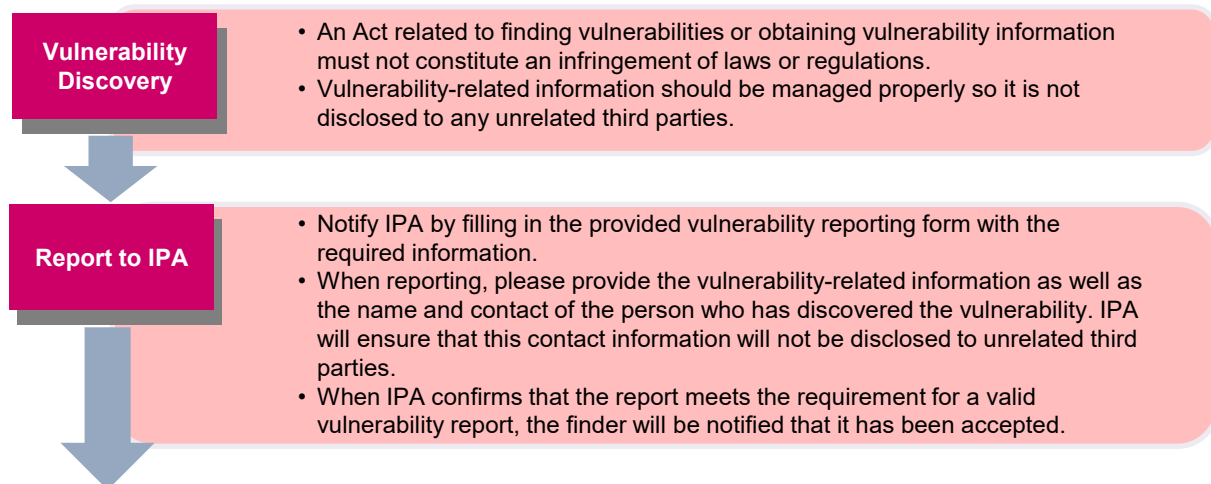
* JPCERT/CC: Japan Computer Emergency Response Team Coordination Center AIST: National Institute of Advanced Industrial Science and Technology

*1) Vulnerability-related information: Information on vulnerabilities (by nature and characteristics), verification methods or methods of attack.

To Finders

If you have discovered a vulnerability, please consider reporting to IPA.^{*2} If it is a software product vulnerability, JPCERT/CC will contact the software developer. If it is a web application vulnerability, IPA will contact the website operator.

【Recommended actions taken by the person who has discovered a vulnerability】



【Recommended actions for other relevant parties】

- IPA and JPCERT/CC will act as an intermediary for the exchange of information between software developers and website operators.^{*3}
- Software developers and website operators will verify the vulnerability.^{*4}
- When verification has been completed and the vulnerability has been confirmed, the software developer / website operator will examine methods to address the vulnerability.
- For a software product vulnerability, it will be published on the Japan Vulnerability Notes (JVN) portal site, and users will be provided with information on vulnerability countermeasures. When the information is published on JVN, IPA will notify the finder.
- For a web application vulnerability, IPA will notify the finder after the website operator notifies that the vulnerability has been addressed.
- IPA asks the finder to manage the vulnerability-related information properly so it is not disclosed to any unrelated third parties during the periods shown in the table below.

If both parties agree, the finder may exchange information directly with the software developer or website operator.

The finder may inquire to IPA about the progress of the handling process. The finder must make sure that information obtained is not disclosed to any unrelated third parties.

For a software vulnerability, after a year has passed since the initial report^{*5}, the finder may issue a withdrawal request to IPA. This will allow the finder to disclose information on the discovered vulnerability.

Type of Vulnerability Report	Effective Period of Non-Disclosure Request
Software product vulnerabilities	From report to announcement on JVN ^{*6}
Website application vulnerabilities	From report to correction of vulnerability

*2) A Finder can report vulnerability-related information directly to the software developer to accept direct reporting.

*3) IPA may make inquiries to the finder about the contents of the report.

*4) If the handling process is terminated because the vulnerability is already publicly known, IPA will notify the finder as such.

*5) The date when JPCERT/CC first attempted to notify the software developer of the vulnerability-related information.

*6) A portal site for vulnerability countermeasure information, operated jointly by IPA and JPCERT/CC. (<https://jvn.jp/en/>).

To Software Developers

When software developers^{*7} are notified that there is a vulnerability in their software product, they are expected to verify the vulnerability. If the vulnerability in question exists, they are expected to make sure users are aware of any available countermeasures. Please cooperate when you receive inquiries from JPCERT/CC on any technical matters and the progress in addressing with the vulnerability.

【Recommended actions by software developers (in advance)】

Establishment of a proper contact

- Set up a proper contact for the handling of vulnerability information and notify JPCERT/CC.
- Please contact JPCERT/CC immediately when the contact information changes.

Please tell JPCERT/CC whether you accept to post the software developer name on the developers public list, and whether you accept direct reporting from the finder.

【Response by IPA and JPCERT/CC】

- JPCERT/CC will register the developer to the list of software developers.
- When IPA receives a report of vulnerability-related information of software products, IPA will notify JPCERT/CC, and JPCERT/CC will contact the software developer that developed the product or technology.

If the software developer cannot be reached^{*8}, the name of the software developer may be published to solicit methods to contact the developer from the public.

Vulnerability Verification

- When the software developer receives vulnerability-related information from JPCERT/CC, the developer should examine the impact on its software products, verify the vulnerability and then report its findings to JPCERT/CC.
- Be sure to manage vulnerability-related information properly so it is not disclosed to any unrelated third parties.

With the approval of the finder through IPA and JPCERT/CC, the software developer may communicate directly with the finder.

Arranging announcement dates

- If the existence of the vulnerability is confirmed, please notify JPCERT/CC of any plans^{*9} to publicly disclose information on the vulnerability. These plans should take into consideration the following: time required to prepare the countermeasure, any coordination with other relevant parties, any risks that this information may be made public prematurely, and any risks of exploitation.

If the software developer is able to contact all users of its software of a countermeasures, then it does not have to be publicly released. In such a case, please contact JPCERT/CC.

Preparation of countermeasures

- The Software developer should notify JPCERT/CC the status of measures by the planned public release date and prepare countermeasures accordingly.

If it is impossible for JPCERT/CC to agree^{*10} with the software developer, the vulnerability may be published after the case is reviewed by the Release Decision Committee. The software developer can explain the opinion in the Release Decision Committee.

Public Disclosure

- After the vulnerability information is published, the software developer is expected to make efforts to ensure that its software users are aware of the issues and its countermeasures.

Contact JPCERT/CC when the software developer wants to notify its software users of the vulnerability and status of any countermeasures before the public disclosure.

*7) The office, corporation, individual or community that developed the software. Or the office, corporation, individual or community that processed, imported, sold, or distributed the software.

*8) Cases where the developer cannot be reached such as the following: contact information for the developer is unknown, an appropriate method to contact the developer does not exist, the developer does not respond to contact attempts, etc.

*9) In general, the recommended date of release is 45 days from the day of the initial attempt to contact the developer from JPCERT/CC. Please contact JPCERT/CC if more time is necessary. For reports that have been handled for over a year, the finder may inquire to IPA to withdraw its request for information non-disclosure. After the request is withdrawn, the vulnerability information may be made public by the finder.

*10) Cases that IPA judges that it is impossible for JPCERT/CC and the software developer to make further efforts to any coordination action concerning the disclosure of vulnerability information.

To Website Operators

When website operators are notified of the possibility that a vulnerability exists in one of their web applications, they are expected to verify the vulnerability. If the vulnerability exists, they are expected to address the vulnerability while considering the extent of its impact. Please also cooperate when you receive inquiries from IPA on technical matters and the progress in dealing with the vulnerability.

【Recommended response by website operators】

Publish Contact Information

- Provide contact information for inquiries regarding the website.



【Response by IPA】

- When IPA receives a report of a vulnerability in a web application, IPA will contact the website operator.



【Recommended actions taken by the website operator】

Vulnerability Verification

- When the website operator is contacted by IPA, the website operator should verify the vulnerability and determine its impact.
- Contact IPA and report the results of the verification.
- Be sure to manage^{*11} vulnerability-related information properly so it is not disclosed to any unrelated third parties.

With the approval of the finder through IPA, the website operator may communicate directly with the finder.



Address Vulnerability

- When you have confirmed that the vulnerability exists, determine its impact. Then address the vulnerability while considering the extent of its impact.^{*12}
- When the vulnerability has been addressed, please notify IPA. This notification should be issued within approximately three months from the time since IPA notified the vulnerability-related information.

*11) It is recommended that a confidentiality agreement be concluded with companies contracted to build and operate websites before communicating vulnerability-related information.

*12) It is not required for the website operator to proactively publish vulnerabilities in web applications. When there is a possibility of secondary damage or an incident such as a breach of personal data due to a vulnerability, then publishing of this information should be considered after it has been addressed. Inquiries from any individuals who have been affected by a vulnerability should be responded to in a prompt manner.

Please address inquiries regarding this brochure to:

Information-technology Promotion Agency, Japan (IPA) IT Security Center

Bunkyo Green Court Center Office 16F, 28-8 Hon-komagome 2-chome, Bunkyo-ku, Tokyo 113-6591, Japan

<https://www.ipa.go.jp/security/english/> Phone: +81-3-5978-7527 FAX: +81-3-5978-7552

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

8F Tozan Bldg, 4-4-2 Nihonbashi-Honcho, Chuo-ku, Tokyo 103-0023, Japan

<https://www.jpcert.or.jp/english/> Phone: +81-3-6271-8901 FAX : +81-3-6271-8908