

信息安全前期预警协调指南 & JPCERT/CC 漏洞协调与披露政策

原文发布：JPCERT/CC

中文翻译：数字观星

审校：CNCERT/CC

观星译 是数字观星推出的长期公益翻译项目。

我们从国外众多安全厂商、咨询机构、媒体博客选取优秀的英文报告，翻译并适当排版后，以无偿免费的形式，进行分享与传播。

现公开招募翻译志愿者，有意者请联系 contact@shuziguanxing.com，来信请注明“观星译”。

免责声明

- 本报告，由北京数字观星科技有限公司（简称“数字观星”，下同），“观星译”公益翻译项目，翻译自 JPCERT/CC 与 2018 年 4 月 27 日发布的《JPCERT/CC Publishes "Vulnerability Coordination and Disclosure Policy"》，原文地址 <http://blog.jpcert.or.jp/2018/04/jpcertcc-publishes-vulnerability-coordination-and-disclosure-policy.html>。
- 望尊重译者的劳动和意愿，不得以任何方式修改本译文。
- “观星译”所翻译文章内容不代表数字观星立场，译者与数字观星亦对原文和译文的任何内容不承担任何责任。
- 译者与数字观星均与原作者与原始发布者没有联系，亦未获得相关的版权授权，本翻译项目为无偿公益项目，无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。
- 数字观星未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与数字观星无关。
- 本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与数字观星一律不予承担。

信息安全前期预警协调指南

-漏洞处理流程概述-

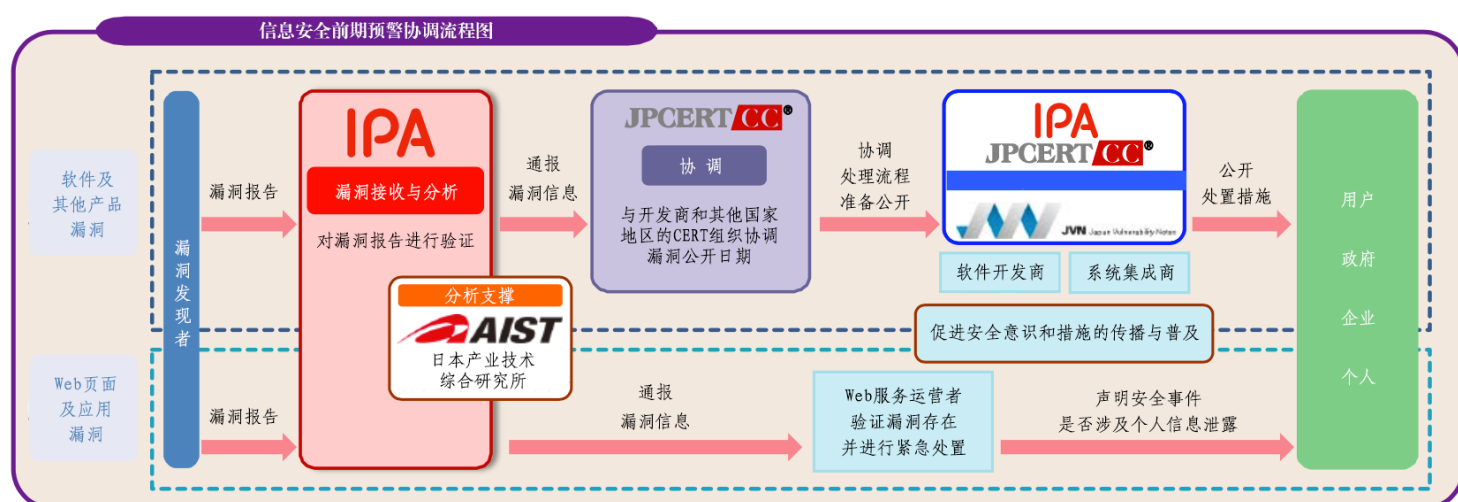
■ 框架建立

2004 年，为了降低计算机非法入侵以及病毒等造成的损失，确保漏洞通报后相关信息得到妥善处理，日本经贸与工业部颁布了《软件漏洞信息处理标准》。该标准于 2014 年完成修订，并于 2017 年升级为《软件产品漏洞相关信息处理标准》。基于以上标准，兹建立《信息安全前期预警协调指南》（以下简称“指南”），对相关各方行为提出建议，梳理漏洞相关信息^{*1}处理流程。需要着重声明的是，信息技术促进局（IPA）将作为各方之间的联络机构，而日本计算机应急响应处理协调中心（JPCERT/CC）将作为各方之间的协调机构。以上机构负责妥善处理所有各方的漏洞相关信息，包括漏洞发现者、软件开发商以及 Web 服务运营者。该流程符合 [ISO/IEC 29147: 2014《漏洞披露标准》](#)。

■ 框架范围

本指南涵盖的漏洞是指，可能对公众造成大范围影响的漏洞，特别是日本境内普遍使用的软件以及主要供日本民众访问的 web 网页及应用程序（例如日语 web 网页，“jp”域名的地址等等）。本指南将向相关各方简要描述如何处理漏洞相关信息。下表展示了相关方成为信息安全前期预警协调成员后的权益。这些权益能够显著降低漏洞对软件用户和 web 服务运营者带来的潜在损失。

相关方	信息安全前期预警协调成员的权益
发现者	● 能够从一个公开渠道，督促软件开发者和 web 服务运营者正视漏洞问题 ● 当漏洞处理信息披露的时候，能有一个可参照的公开文档
软件开发商	● 能够了解到可能对其产品造成影响的非公开漏洞 ● 能够帮助用户从权威渠道了解到如何应对漏洞 ● 能够向公众表明自己高度重视漏洞相关工作的态度
Web 服务运营者	● 能够在漏洞被广泛传播之前，对相关页面进行处理 ● 能够校验并处理之前未曾注意到的漏洞 ● 能够提升其 web 页面的安全水平，更好地保护用户



* JPCERT/CC: 日本计算机应急响应处理协调中心

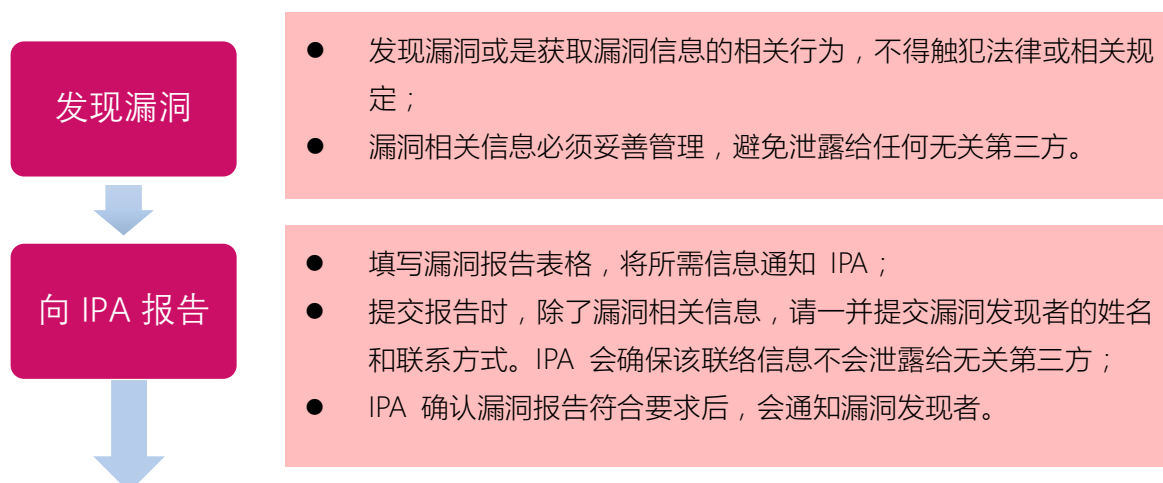
* AIST: 日本国家产业技术综合研究所

*1) 漏洞相关信息: 漏洞本身的信息(通用信息、特殊事项)、验证方式或攻击利用方式等。

漏洞发现者

如果你发现了一个漏洞，请考虑将其报告至 IPA^{*2}。如果这是一个软件产品漏洞，JPCERT/CC 将会联系软件开发商。如果这是一个 web 应用漏洞，IPA 将会联系 web 服务运营者。

【针对漏洞发现者的操作建议】



【其他相关各方的操作建议】

- IPA 和 JPCERT/CC 将会作为软件开发商与 web 服务运营者之间信息交换的中间人^{*3}；
- 软件开发商和 web 服务运营者将会对漏洞进行验证^{*4}；
- 验证完成后，如果确认漏洞存在，软件开发商/web 服务运营者会寻找针对漏洞的处理方法；
- 对于软件产品漏洞，漏洞会在日本漏洞通报（JVN）页面上公布，软件用户会收到漏洞处理意见的相关信息。信息在 JVN 上公布的时候，IPA 也会通知漏洞发现者；
- 对于 web 应用漏洞，IPA 则会在 web 服务运营者通知该漏洞已被处理后再通知漏洞的发现者；
- IPA 会要求漏洞发现者妥善管理漏洞的相关信息，避免泄露给无关第三方，要求的时间范围如下表所示

如果双方同意，发现者也可以直接与软件开发商或 web 服务运营者交换信息。

发现者可以向 IPA 询问处理进度，但必须保证获取的信息不会泄露给无关第三方。

对于软件漏洞，初始报告提交一年后^{*5}，开发者可以向 IPA 发起撤销请求。这意味着发现者可以将发现的漏洞向公众公布。

软件产品漏洞	从漏洞发现者提交报告到 JVN 上发布声明 ^{*6}
Web 应用漏洞	从漏洞发现者提交报告到漏洞被修复

*2) 发现者也可以直接向软件开发商报告漏洞相关信息

*3) IPA 可以向发现者询问报告的内容

*4) 如果漏洞已经被公开，导致流程终止，IPA 也会通知发现者

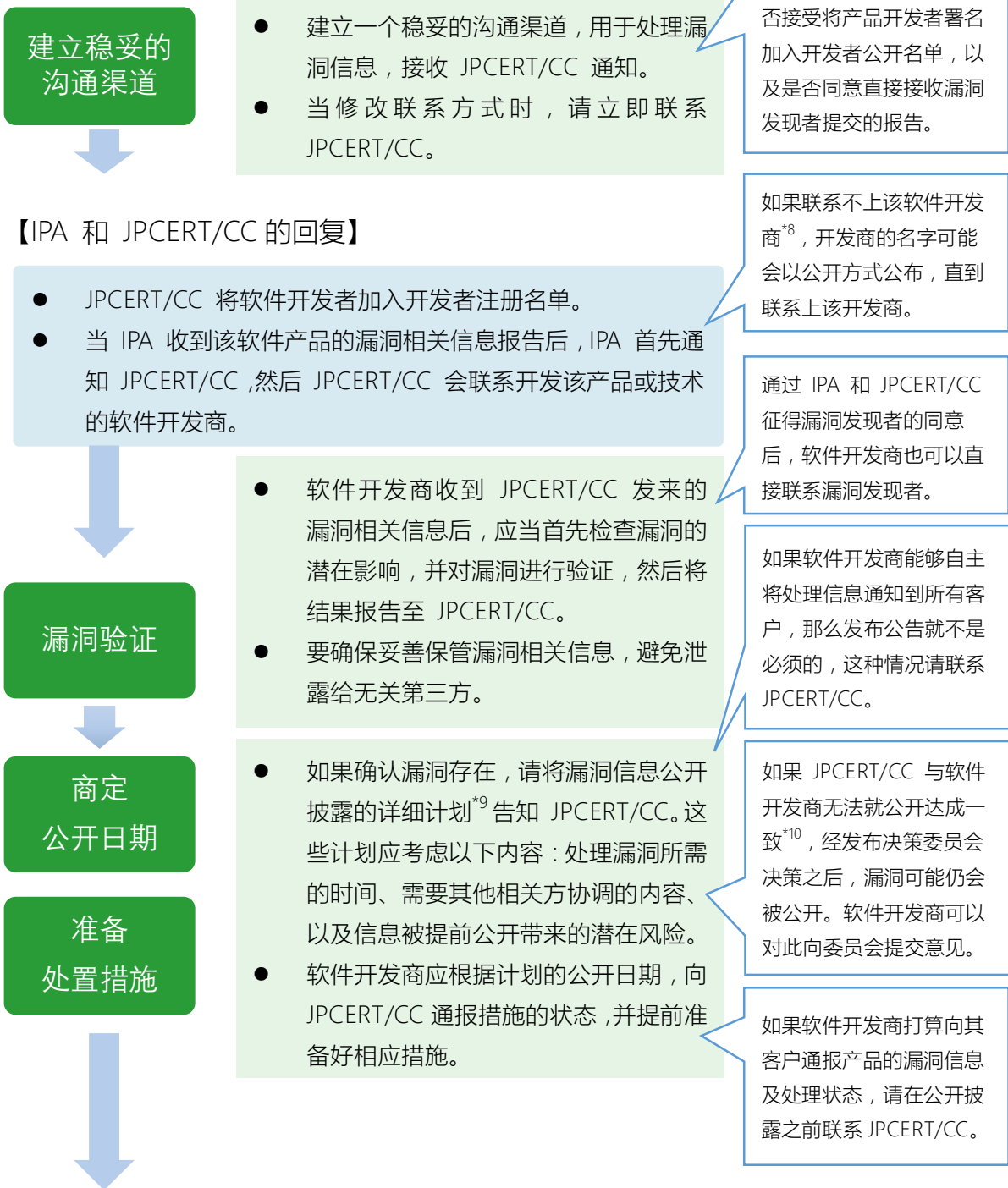
*5) 该日期指 JPCERT/CC 首次尝试通知软件开发商漏洞相关信息的时间

*6) 漏洞处理信息页面，由 IPA 和 JPCERT/CC 联合运营 (<https://jvn.jp/en/>)。

软件开发商

当软件开发商^{*7}收到通知，其软件产品存在漏洞时，开发商应当对通知的内容进行验证。如果漏洞问题确实存在，开发商要确保用户能够知晓任一可能的处理措施。并且当收到 JPCERT/CC 的任何技术要求或漏洞处理进程时，也请给予配合。

【针对软件开发商的操作建议（高级）】



公开披露

- 漏洞信息披露之后，软件开发商应当努力确保其产品的用户能够接收事件信息及相关处理措施。

*7) 指开发该软件的政府、企业、个人或社区。或是加工、引进、售卖或分发该软件的政府、企业、个人或社区。

*8) 无法联系上开发商一般包括下列情况：联络信息未知、联络方式已失效、或是开发商对联络无应答等等。

*9) 通常来说，建议的公布日期是从初始报告提交起 45 天。如果需要延长，请联系 JPCERT/CC。如果报告已经提交超过一年，漏洞发现者可以提请 IPA 撤销信息不公开的限制。请求一旦被批准，漏洞发现者即可以将漏洞信息公开。

*10) 指 JPCERT/CC 和软件开发商无法就漏洞信息披露达成一致意见，转而交由 IPA 进行仲裁的情况。

Web 服务运营者（收到通知其 web 应用存在漏洞的运营商）

Web 服务运营者收到通知其某个 web 应用可能存在漏洞时，应当首先对漏洞进行验证。若漏洞存在，则立即处置并评估其带来的潜在影响。另外，如果收到 IPA 的技术要求或漏洞处理进程时，请给予配合。

【针对 web 服务运营者的响应建议】

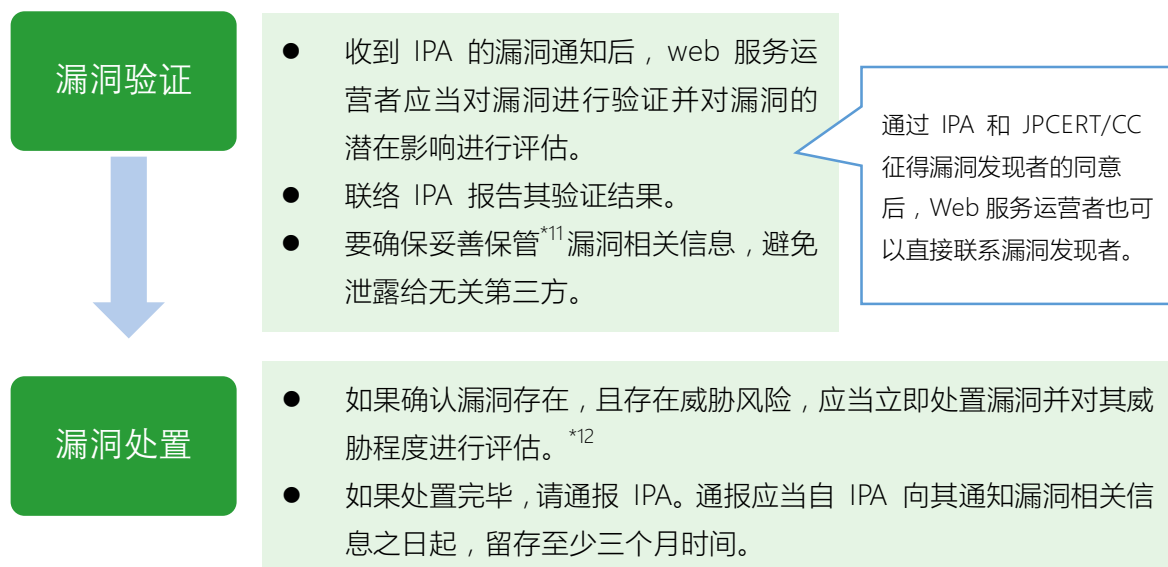
公布 联系方式

- 根据不同的 web 页面或应用，提供对应的联系方式。

【IPA 响应】

- IPA 收到某个 web 应用的漏洞报告后，会联系 web 服务运营者。

【针对 Web 服务运营者的操作建议】



*11) 建议 web 运营公司在沟通漏洞相关信息之前，先建立可信的加密通信方式。

*12) 并不是要求 web 服务运营者提前发布 web 应用的漏洞信息。而是如果由于漏洞原因，存在用户隐私泄露等二次损失或进一步安全事件时，web 服务运营者修复漏洞后，应当考虑将漏洞信息公开。受到漏洞影响的任何个体提出的合理诉求都应当得到及时响应。

IPA 与 JPCERT/CC 的联系方式：

Information-Technology Promotion Agency, Japan (IPA) Security Center, Technical Department
Bunkyo Green Court Center Office 16F, 28-8 Hon-komagome 2-chome, Bunkyo-ku, Tokyo 113-6591,
Japan <http://www.ipa.go.jp/security/english/> Phone: +81-3-5978-7527 FAX: +81-3-5978-7518

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
Hirose Bldg. 11F, 3-17 Kanda-nishiki-cho, Chiyoda-ku, Tokyo 101-0054,
Japan <https://www.jpcert.or.jp/english/> Phone: +81-3-3518-4600 FAX: +81-3-3518-4602

JPCERT/CC 漏洞协调与披露政策

■ 摘要

本着协助产品供应商处理漏洞、告知用户漏洞威胁风险以及如何降低这些风险，进而加强互联网安全的目的，JPCERT/CC 发布本政策指南。

基于以上诉求，JPCERT/CC 将依照《JPCERT/CC 漏洞协调政策》，对漏洞处理过程中的相关产品供应商以及其他利益相关方进行协调。JPCERT/CC 会尽全力协调报告相关各方，但依照指南，在某些情况下我们可能会婉拒某些报告的请求。

JPCERT/CC 会在日本漏洞通报平台(JVN)上对漏洞进行公开披露，依照《JPCERT/CC 漏洞披露政策》，披露的时间是在漏洞处置完毕后，或是经过各利益相关方的积极协商达成一致后，由 JPCERT/CC 决定的某个合适的时间。

本文档将对《JPCERT/CC 漏洞协调与披露政策》进行说明。

■ 协调政策

A) 如何联系 JPCERT/CC 提交报告（发起协调请求）

漏洞报告请发送至：vuls@jpcert.or.jp

建议使用 PGP。我们的 PGP 秘钥可以从以下地址获取到。

JPCERT/CC 漏洞协调 PGP 公钥地址：

<https://www.jpcert.or.jp/english/pgp/>

收到报告后，JPCERT/CC 会在 5 个工作日内针对提交的报告发送一封初次回复邮件进行确认。

B) 漏洞报告应包含哪些内容？

1. 报告提交的漏洞必须符合以下定义：

- 漏洞的定义指软件或其他产品中存在的计算机逻辑弱点，该弱点在至少一个场景下可被利用，且能够对机密性、完整性或可用性造成消极影响；
- 报告不得涉及软件的“debug 模式”或“开发模式”；
- 报告不得涉及专门用于漏洞训练为目的的应用程序或产品。

2. 软件的准确版本或受影响的模块版本（包含一个产品页链接）

- 漏洞必须在最新可用版本或至少是“官方支持”的产品版本中可复现；
- 必须是仍在持续维护中的产品；
- 不得涉及开发者声称“对其安全性不再进行维护”的产品。

3. 简单描述如何发现的漏洞（包括使用了什么工具）

4. PoC 代码或是漏洞利用演示

5. 漏洞威胁程度的描述或是描述攻击场景的威胁模型

6. 报告提交的必须是未公开的漏洞

通常来说，除非漏洞会造成十分严重的影响，否则跨站脚本攻击漏洞不会被采纳。

提交报告的时候，请确认是否有明确的时间要求（例如你准备在某次会议上对漏洞进行公开或演示，如果你知道确切时间的话，请在报告中告知）。

JPCERT/CC 可能作出不采纳报告的决定。原因包括但不限于以下情况：

- 产品已经超过 18 个月未更新
- 该漏洞对日本的影响很小

在对报告进行分析后，JPCERT/CC 会联系提交者告知报告是否被采纳，以及原因是什么。

最后，如果你已经联系过厂商或计划联系厂商提交漏洞，可以将我们的回复信息包含在你的报告里。

C) 什么样的漏洞报告可以获得高优先级？

JPCERT/CC 会给某些报告以高优先级。下面列出了一些能够获得高优先级的标准：

- 漏洞对日本造成广泛影响
- 影响关键基础设施

- 影响大批用户、众多产品、多个开发者
- 高危

D) JPCERT/CC 能帮报告提交者做什么？

JPCERT/CC 可以为提交者提供以下帮助：

- 提供身处日本的开发者的联系方式
- 帮忙尝试联络身处日本的联系不上的开发者

寻求更多帮助，请联系 JPCERT/CC。

E) 什么情况下，除了厂商 JPCERT/CC 还会联系第三方？

针对漏洞报告，JPCERT/CC 只会联系对应的厂商，但是有些情况下，JPCERT/CC 会联系可信的第三方，包括：

- 行业协会，以获得厂商的联系方式
- 某个漏洞涉及到多家厂商/实现协议，寻求协助技术分析

F) 为什么有些漏洞报告 JPCERT/CC 不采纳？

很不幸，并不是所有的漏洞都能最终协商披露。可能但不限于以下原因：

- 报告提交者与厂商开发者未就漏洞达成意见一致
- 开发者始终未对初次联络请求作出回应
- 开发者终止了协作请求的响应

在初次联络请求发出后 120 天内，以上任意一条成立，JPCERT/CC 会将报告“关闭”。报告提交者可要求 JPCERT/CC 继续协调，JPCERT/CC 保留驳回该请求的权利。

这种情况下，JPCERT/CC 可作出以下任一决定：

- 将漏洞公开（依据标准《JPCERT/CC 漏洞披露政策》）
- 通知报告提交者，JPCERT/CC 将终止协调尝试

G) 当某个漏洞影响多家厂商时，JPCERT/CC 如何处理？

当提交的某个漏洞同时影响多家厂商时，“多方协调”会被触发。针对该情况，JPCERT/CC 会同时联系多家厂商处理漏洞。下面是触发“多方协调”的典型场景列表：

- 供应链漏洞，需要多个开发者和潜在的服务提供商修复漏洞
- 共享库漏洞，涉及到上游开发者先修复漏洞，然后下游开发者再接受修复更新
- 某些协议漏洞，涉及到实现协议的开发者

针对所有多方协调场景，通知开发者的时间（上下游）和公开漏洞的时间都不尽相同。

涉及到多方协调的情况时，JPCERT/CC 会尝试平衡所有利益相关方的诉求，本着积极协作的态度，具体问题具体分析，领导漏洞的协作与披露。

■ 披露政策

漏洞协调完成后，JPCERT/CC 会在 JVN 上对漏洞进行公开，一般会附带厂商的处理方案。在协作披露的过程中，厂商和提交者协同工作，在修复准备好以后再同时公开漏洞。对所有漏洞，JPCERT/CC 都不会公开攻击代码或是任何不必要的细节，避免造成攻击者获取不公平的利益。

作为 CVE 编号授权单位（CNA），JPCERT/CC 对 JVN 上公开的所有漏洞都会授予一个 CVE 编号（其他 CNA 已编号的除外）。

除了披露协作漏洞，可能造成严重影响的漏洞或攻击相关的技术类预警也会在 JVN 上发布。

JPCERT/CC 保留未来修订本政策的权利。

JPCERT/CC 联系方式：

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

Hirose Bldg. 11F, 3-17 Kanda-nishiki-cho, Chiyoda-ku, Tokyo 101-0054, Japan

<https://www.jpcert.or.jp/english/> <mailto:vuls@jpcert.or.jp>