



TLD-OPS 是由 ccTLD 管理并服务于 ccTLD 的全球技术事件响应社群。它汇聚了众多负责 ccTLD 运营安全与稳定的人员。

# 189 名成员\*

160 个 ASCII ccTLD  
从 .ad (安道尔) 到 .zm  
(赞比亚)

29 个 IDN ccTLD  
从 .ভাৰত (印度) 到 .المغرب  
(摩洛哥)

人员  
340+ 位负责 ccTLD 运营安全  
与稳定的专家

管理  
由 ccTLD 通过 TLD-OPS 常务  
委员会全权管理

附加价值  
提高您在 ccTLD 事件响应情况  
下的联络通达性，接收和共享  
相关的安全警报和问题查询

TLD-OPS 社群的目标是让全球 ccTLD 运营商团结合作，共同检测和减少可能影响 ccTLD 服务和更广泛互联网运营安全与稳定的事件，如 DDoS 攻击、恶意软件感染和网络钓鱼攻击等。TLD-OPS 面向所有 ccTLD 开放，目前共汇聚了 340 多人，他们分别负责 188 个不同 ccTLD（覆盖范围 65%）的运营安全与稳定。TLD-OPS 进一步扩展了成员的现有事件响应结构、流程和工具，对它们进行了补充而非替代。

## 联系人存储库

TLD-OPS 社群以标准电子邮件列表为基础建立，该列表作为 ccTLD 的事件响应联系人存储库。订阅者每月都会收到一次来自列表的自动生成的电子邮件，其中包括所有成员 ccTLD 的事件响应信息（联系人、电话号码和电子邮箱）。这有助于提高 TLD-OPS 成员的联络通达性，因为每个人的收件箱都有其他所有人的联系信息，通常在离线紧急情况下也可以使用。

## 安全警报

TLD-OPS 覆盖了全球 65% 的 ccTLD，这使得成员还可以积极利用电子邮件列表共享安全警报和问题查询，例如 DDoS 攻击和使用 ccTLD 域名空间的恶意软件。由于事件响应经验可以相互学习，因此鼓励

成员分享他们如何处理某些事件，无论是通过电子邮件列表还是每年的 TLD-OPS 研讨会（与 ICANN “会议 A”在同一地点举行）。

## 管理

TLD-OPS 邮件列表于 2014/2015 年由 ccTLD 创建并为其服务[1]。ccTLD 社群通过 TLD-OPS 常务委员会对 TLD-OPS 邮件列表进行全权管理，该委员会由五大地理区域（非洲、亚太地区、欧洲、北美以及拉丁美洲和加勒比地区）的 ccTLD 运营人员以及来自 SSAC、IANA 和 ICANN 安全团队的代表组成。常务委员会的职责是监督邮件列表的日常运营以及“TLD-OPS 生态系统”的进一步发展。ICANN 通过 ccNSO 秘书处对此提供行政支持。邮件列表服务器在 DNS-OARC 的“neutral ground”上运行。

## 轻松加入！

TLD-OPS 列表作为一个电子邮件列表，要加入它很简单。但是，该列表仅供负责 ccTLD 运营安全与稳定的人员以及通过了 IANA 管理联系人认证的人员使用。

想要加入此列表，请让您的 IANA 管理联系人发送一封电子邮件给 ccNSO 秘书

\* 截至 2017 年 6 月 2 日。现有成员列表显示在 TLD-OPS 主页上。

长，邮件内容包括您 ccTLD 的安全与稳定联系人的姓名、电子邮箱和电话号码。请使用右边的订阅模板，该模板也可复制并粘贴在 TLD-OPS 主页上。

**重要提示：**您的订阅请求电子邮件必须通过您当前在 IANA 数据库 [2] 中登记的管理联系人地址发送。如果无法做到这一点，您必须将此电子邮箱地址复制到您的订阅请求电子邮件中。否则，我们不会同意让您加入列表。

## 个人信任

TLD-OPS 列表基于个人信任创建，这意味着订阅者只能使用自己的电子邮箱和电话号码加入。这样做的理论依据在于个人信任模式有益于进一步增进 ccTLD 社群内部的信任，例如，大家开始了解彼此的姓名，且已在 TLD-OPS 研讨会上见面。因此，基于角色的电子邮箱地址不允许加入此列表。

通常用于事件响应社群的核准模式不适用于 TLD-OPS 列表，因为 ccTLD 社群是一个很庞大的群体（共有 291 个 ccTLD），基于这一模式很难让相对陌生的人加入列表。

## 参与原则

为获取 ccTLD 的事件响应联系人信息而在列表中交换的所有信息都是保密的，切勿在 TLD-OPS 社群之外共享。

有关实际安全事件的信息必须使用交通灯协议 (TLP) [2] 标记出来：红色（仅供指定的收件人）、琥珀色（受限发布）、绿色（全社群发布）或白色（不受限发布）。

TLD-OPS 沿用 US-CERT [3] 中 TLP 的定义，其默认颜色为 TLP-AMBER。

列表中的成员不得共享列表中自动生成的信息。TLD-OPS 列表未加密，以便每一个 ccTLD 加入。 ■

## 订阅模板

请使用以下格式订阅 TLD-OPS 列表。也可从 TLD-OPS 主页复制并粘贴。

-- 邮件开头 --

发件人: ccTLD IANA 管理联系人或授权代表  
收件人: ccNSO 秘书长 <ccnsosecretariat@icann.org>  
抄送: ccTLD IANA 管理联系人地址  
主题: 请求加入 TLD-OPS 邮件列表

尊敬的 ccNSO 秘书长：

我希望让以下人员加入 TLD-OPS 列表。我在此证明他们都负责我的 ccTLD 的整体安全与稳定，并且我本人是我的 ccTLD 的 IANA 管理联系人或者已获得授权代表他/她行事。

此致，

<ccTLD> 的 IANA 管理联系人

== 事件响应联系人信息 ==

联系人 #1 (主要联系人) :

姓名: <名字 1> <姓氏 1>  
电子邮箱: <电子邮箱地址 1>  
移动电话号码: +<国家/地区代码> <号码>

联系人 #2 (次要联系人) :

姓名: <名字 2> <姓氏 2>  
电子邮箱: <电子邮箱地址 2>  
移动电话号码: +<国家/地区代码> <号码>

联系人 #3:

姓名: <名字 3> <姓氏 3>  
电子邮箱: <电子邮箱地址 3>  
移动电话号码: +<国家/地区代码> <号码>

-- 邮件结束 --

## 参考资料

[1] SECIR 工作组最终报告，

<http://ccnso.icann.org/workinggroups/secir.htm>

[2] IANA 根数据库，

<https://www.iana.org/domains/root/db>

[3] 交通信号灯协议，

[http://en.wikipedia.org/wiki/Traffic\\_Light\\_Protocol](http://en.wikipedia.org/wiki/Traffic_Light_Protocol)

[4] US-CERT 关于 TLP 的

定义，<https://www.us-cert.gov/tlp>

## 关于

TLD-OPS 常务委员会的宣传单。

第 2.5 版，2017 年 6 月 12 日。