VPN Gate 反滥用政策

任何人都可以通过使用 VPN Gate 公共 VPN 中继服务器隐藏自己的 IP 地址。

预计大多数用户将此功能用于合法的目的。然而，一些用户可能会滥用此功能，用于不正当的目的。为了反击这种滥用行为， VPN Gate 项目定义了如下反滥用政策。

VPN 连接日志的保管和披露政策

我们始终保留 3 个月或以上的 VPN Gate 公共 VPN 中继服务器的 VPN 连接日志

当一个匿名用户从一个 VPN Gate 公共 VPN 服务器 连接 / 断开时，访问日志条目将被记录。访问日志条目将被存储在 VPN Gate 公共 VPN 服务器的日志文件中。相同的信息将通过类似系统日志协议以 SSL 加密通讯被发送到我们的日志服务器。

VPN 连接日志条目包括 :

- 日期和时间
- 目标 VPN 服务器的 ID、IP 地址和主机名称
- 活动的类型 (连接或断开)
- 源 VPN 客户端计算机的原始 IP 地址和主机名称
- VPN 协议的类型 (SSL-VPN、L2TP、OpenVPN 或 SSTP)
- VPN 客户端软件的名称和版本 (如果可用)
- 一个 VPN 连接的数据包数和字节数
- VPN Gate 通信的目标 HTTP / HTTPS 主机名 (FQDN)、IP 地址、主机名和端口号的日志记录

没有任何其他信息将被传送给我们，也没有被记录在我们的日志服务器上。

向警察、检察官、律师或法院披露

避免利用 VPN Gate 的滥用用户隐藏自己的 IP 地址进行不法行为是必要的。万一这种滥用情况发生，有必要跟踪这种非法用户的源 IP 地址。分析 VPN 连接日志有助于调查他的源全球 IP 地址。

我们将通过适用的法律披露 VPN 连接日志给授权的警察、检察官、律师或法院。

如果你是一名警察，检察官，律师或法院授权，并要要求披露的 VPN 连接日志，请与我们联系下面的 e-mail 地址。你需要附加的信息，它描述的目标日志的日期和时间，涉及 VPN 服务器的 IP 地址和其他材料，以供参考。

- More details of our disclosure policy is on this page in Japanese.

vpngate-mail@vpngate.net

Appending Session ID on User-Agent Value

When a VPN Gate user communicates with an HTTP server via a VPN Gate Public VPN Relay Server, a part of the VPN Session ID will be appended on the User-Agent value on the HTTP request header. This partial Session ID will be used to identify the VPN Session which was related to the abuse incident.

VPN 数据包日志的保管和披露

每个 VPN Gate 公共 VPN 中继服务器存有数据包日志

在 VPN Gate 实验服务里，很多志愿者 (加入到这个实验的) 在自己的电脑上提供 VPN 中继功能。在每个志愿者的每台计算机上， VPN 服务器程序总是记录每个 VPN 用户的数据包包头。你可以看到数据包日志，以知道哪种通信通过一个特定的 VPN 用户经由 VPN 服务器被建立。

每个 VPN 服务器上的数据包日志将在磁盘上保留至少两周或两周以上。它们包含了由 VPN 用户发起的、所有 TCP/IP 包头。两周以后，日志文件可能被压缩或删除，以节省磁盘的可用空间。

如何申请披露数据包日志？

如果你是被授权的警察、检察官、律师或法院，并想要求披露 VPN 数据包日志，您必须与目标 VPN 服务器的运营商联系。联系地址在 **VPN 服务器列表页面** 列出。

如果你联系的目标 VPN 服务器不在列表上，或者你找不到联系地址，请你联系负责管理 IP 地址的 ISP。如果您被法律授权，您可以通过 ISP 联系到相应的目标 VPN 服务器的管理员。

我们没有任何被保存在每个志愿者的 VPN Gate 服务器的 VPN 数据包日志。没有数据包日志从每个公共 VPN 中继服务器被提交给我们。请不要要求我们批露被存储在一个特定中继服务器的具体 VPN 数据包日志。在我们的设备中，我们不保存这样的日志，所以我们不能回复这样的要求。

如果当局要求，我们可以帮助分析数据包日志

如果你是被授权的警察、检察官、律师或法院，想要分析获得的数据包日志文件的内容，如果我们能提供的话，在合理的、务实的努力范围内，我们可以帮助您分析数据包日志。

如果你是被授权的警察、检察官、律师或法院，想要分析 VPN 连接日志，请通过下面的 e-mail 地址联系我们。

vpngate-mail@vpngate.net

如何阻止您的员工使用任何 VPN Gate 服务呢？

如果你是一个公司的网络管理员，希望禁止每位员工使用 VPN Gate ，可以通过以下步骤阻止 VPN Gate。

1. 通过你的防火墙阻止访问网址 **https://www.vpngate.net/**。
2. 通过你的防火墙阻止访问 **镜像站点列表** 上的所有网址。
3. 如果你进行了上述步骤，员工从外面不知何故通过 **VPN Gate 客户端** 仍然可以使用 VPN Gate。
   为了避免这样的使用，阻止你的防火墙上任何 TCP 或 UDP 数据包，除了为贵公司业务的必要通信。
   (高级防火墙产品可以做到这一点。例如，有些防火墙可以解密 SSL 通信应用白列表。)
4. 如果你进行了上述所有步骤，您的员工可以使用 3G 或 LTE 无线供应商的设备来绕过防火墙的限制使用 VPN Gate 服务。
   阻止这样的使用是非常困难的。如果你要阻止，你必须购买一个消声室。

任何建议？

这对我们来说是困难的挑战，以促进 VPN Gate 的合法使用，同时避免 VPN Gate 的错误滥用。

如果您有任何建议，**请在论坛上给我们反馈**。