



网络摄像机

防止非法访问的对策

重要 管理员请务必阅读。



非常感谢您平时对佳能产品的惠顾。本书记载了防止从外部网络非法访问网络摄像机的相关对策。管理员请务必阅读。

前言

本书，介绍防止非法访问佳能网络摄像机的对策的 4 个要点。

防止外部非法访问的对策要点

1. 在私人 IP 地址下运用
2. 利用防火墙限制通信
3. 用密码管理网络摄像机
4. 设置 SSL 加密通信

说明

本书中记载的设置步骤和图片只是一个示例，与您使用的网络摄像机会有差异。
详细请参照网络摄像机附带的操作指南。

在私有 IP 地址下运用

所谓 IP 地址，是指给网络上的机器分配的编号，互联网的连接所使用的 IP 地址称为“公有 IP 地址”，公司内部 LAN 等局域网所使用的 IP 地址称为“私有 IP 地址”。互联网上的所有不特定的用户都可以访问公有 IP 地址，若设置网络摄像机为公有 IP 地址，非法访问导致窥视等风险将增大。

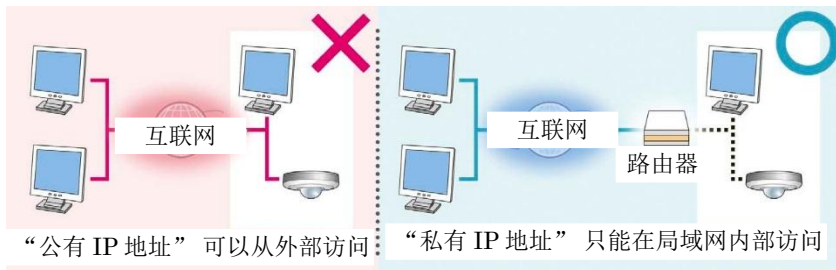
建议将网络摄像机设置为私有 IP 地址进行使用。可以设置为私有 IP 地址的 IP 地址的范围如下所示。

私有 IP 地址的范围

- 10.0.0.0 ~ 10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0 ~ 192.168.255.255

利用防火墙限制通信

防火墙，是防止从外部网络非法访问，防止攻击或侵入组织内网络的系统。推荐在设置了防火墙的环境下使用网络摄像机。



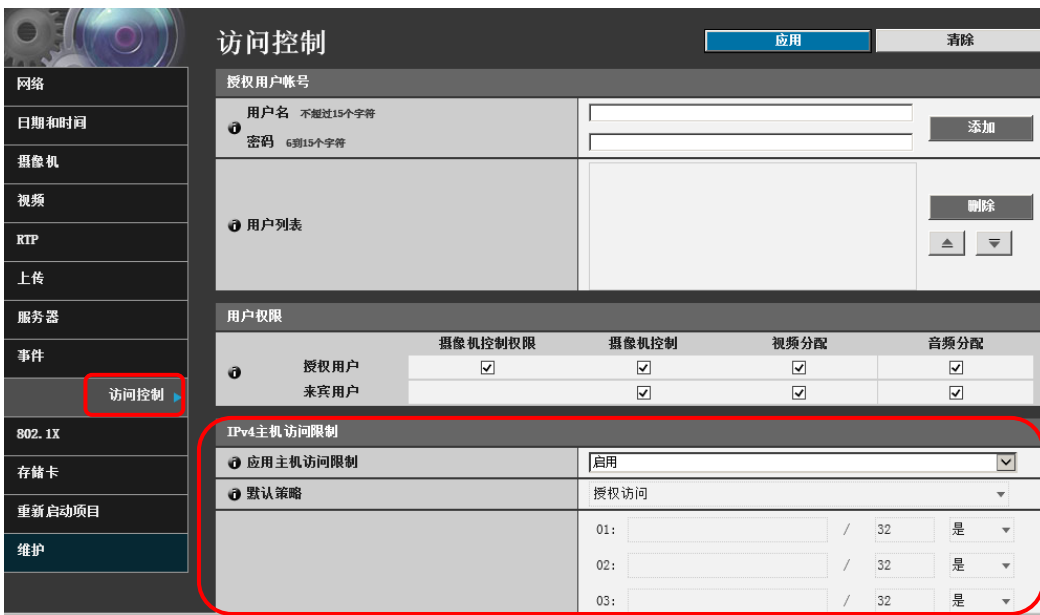
说明

即便网络摄像机设置了公有 IP 地址，
若通过防火墙等构筑了防御外部访问的环境，可以减轻非法访问的风险。
当想在网络相机上设置公有 IP 地址并运用时，
请与公司内部的网络管理员商谈。

佳能的网络摄像机上搭载的访问控制功能，也可以限制从指定 IP 地址访问。

为了在网络摄像机上限制 IP 地址的访问，
根据以下的步骤设置 IP 地址的访问限制。

1. 在设置页的 [访问控制] 的 [IPv4 主机访问限制] 或 [IPv6 主机访问限制] 中，将 [主机访问限制的适用] 设置为 [适用]。
 2. 在 [默认策略] 中，将默认的访问策略设置为 [允许访问] 或 [禁止访问]。
 3. 当 [默认策略] 设置为 [允许访问] 时，通过 [网络地址 / 子网掩码] 指定禁止访问的主机或网络，设置 [禁止]。当 [默认策略] 设置为 [禁止访问] 时，通过 [网络地址 / 子网掩码] 指定允许访问的主机或网络，设置 [允许]。
- ※ 可以指定子网掩码，设置网络单位或主机单位的访问限制。



说明

- 有的网络摄像机的机型没有 IP 地址访问限制功能。
- 摄像机的设置页的访问方法如下所示。
 1. 启动 Web 浏览器
 2. 在地址栏 中输入 IP 地址
 3. 显示照相机的首页，点击 [设置页]。

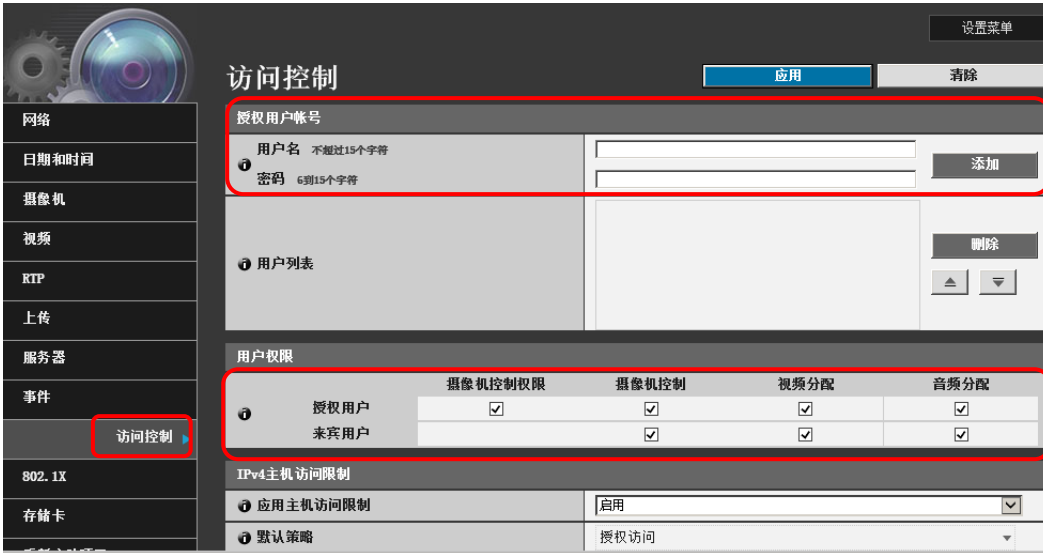
用密码管理网络摄像机

佳能的网络相机，有“管理员”“授权用户”“来宾用户”这3种用户权限。

通过密码保护管理员和授权用户的账号。通过给各用户设置合适的权限，可以降低非法访问时的风险。

管理员是具有所有权限的用户。[设置页] 和 [管理工具] 只有管理员才能访问。

注册用户通过设置页的 [访问控制] 的 [授权用户账号] 注册。



通过[访问控制]的 [用户权限]设置注册用户和普通用户的权限。

勾选允许利用的事项。

特权摄像机控制权	可以启动管理员阅读器
摄像机控制权限	可以通过 VB 阅读器操作相机
视频分配的权限	可以通过 VB 阅读器查看显像
音频分配的权限	可以通过管理员阅读器和 VB 阅读器接收声音

通过将来宾用户的所有权限设置为无效，可以禁止普通用户不需要密码访问摄像机。

重要

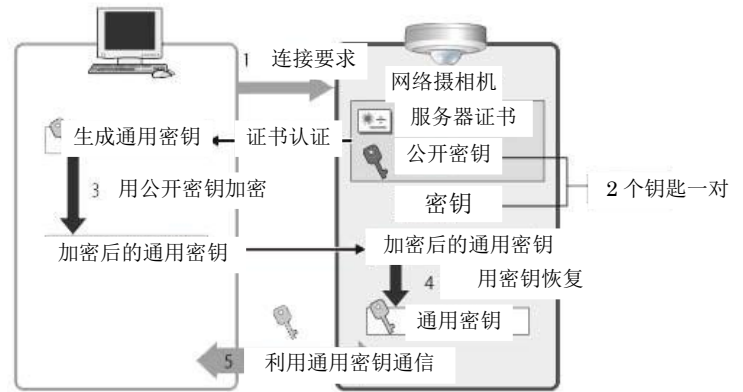
- 请务必更改管理员的初始设置密码。
- 安全起见，请定期更改密码。
- 请设置为第三方很难推测的密码。
- 设置方法和设置内容因网络摄像机的机型而异。

设置 SSL 加密通信

用户通过浏览器访问佳能的网络摄像机时，若在网络摄像机中导入服务器证书，即可通过 SSL 实现安全的加密通信。

SSL 通信的结构

1. 当用户从电脑访问网络摄像机时，要求 SSL 的服务器证书和服务器的公开密钥。
2. 网络摄像机给用户的电脑发送证书和公开密钥。
3. 使用从网络相机接收的公开密钥，给电脑内独自生成的共通密钥加密。
4. 将加密后的通用密钥发送给网络摄像机。
5. 网络摄像机使用密钥，恢复加密后的通用密钥。
6. 这样，通用密钥归用户的电脑和网络相机双方共同拥有，可以相互使用通用密钥交换数据。



若想在网络摄像机上设置 SSL 加密通信，在佳能的网络摄像机上，使用自己证书设置 SSL 加密通信，其步骤如下所示。

1. 在设置页的 [SSL/TLS] 中输入 [证书] 的各项内容以后，点击[适用]，然后点击 [执行]。
网络摄像机内做成自己证书和公开密钥。
2. 在[加密通信]的[SSL 通信]中选择[使用]，点击[适用后重启]。
网络摄像机将重启。自己证书有效。



3. 通过 HTTPS，从电脑访问网络相机。
开始 SSL 通信，该通信使用通用密钥。

说明

有的网络摄像机机型没有 SSL 加密通信设置的功能

重要

本操作指南中编制的服务器证书是私有证书。

Canon

© CANON INC. 2014