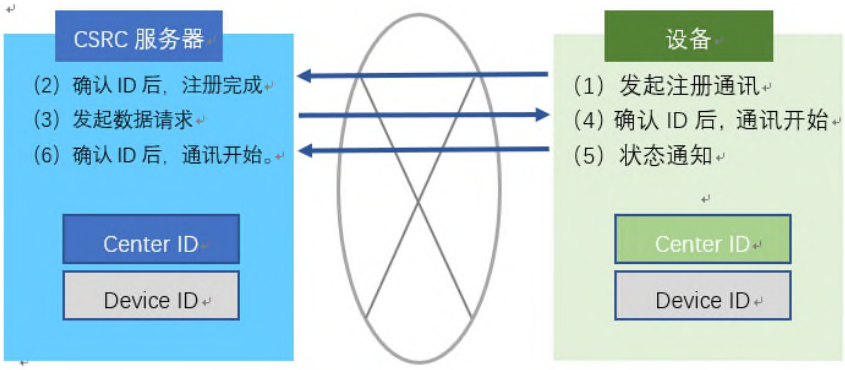
柯诊断（CS Remote Care）安全白皮书

1 使用公用线路（调制解调器、传真）

在远程诊断系统中使用公共线路，在设备主机和柯诊断（CS Remote Care,此后称为 CSRC）服务器之间建立连接，将主机的数据以及主机的设置变化发送到服务器。

为了在远程诊断系统里进行通信，设备使用 CSRC 服务器端和设备端注册的 ID 来建立通信连接。通信将确认 CSRC 服务器端注册的内容和设备发送的内容是否一致，在通信正常结束后，远程诊断通信即可就绪。远程诊断的通信每一次都会确认 ID，如果 ID 不一致，那么将不会建立连接。

CSRC 收集的数据包括计数器值在内的服务信息，不包含传真地址以及个人信息等细节。



2 电子邮件安全

- **传输数据加密**

CSRC 服务器机主机之间的数据使用加密秘钥（公共秘钥）进行加密。

*设备主机和通讯中心可以设置加密选项。使用公共秘钥的加密系统，通讯中心和设备主机使用相同的秘钥来进行加密及解密。这样可实现无第三方介入时邮件的安全发送和接收。

- **ID 的确认等**

发送/接收的邮件中包含的信息（通讯中心 ID 或是设备序列号）在源端和目的地端均可进行确认。对这些信息进行一致性检查，从而确认源端和目的地端的数据的正确性。

此外，从通讯中心发出的邮件均有 Email ID。MFP 端的响应邮件使用响应源端的 Email ID。检查此 ID 和通讯中心发出的 Email ID 是否一致来进行确认。

- **排除虚假邮件**

在源端和目的地端的信息（通讯中心 ID 或是设备序列号）能够被确认或是 Email ID 不匹配的情况下， 发送/接收的邮件会被认作虚假邮件被排除且不进行任何数据处理。

3 HTTP 通讯安全

- **传输数据的加密**

如同电子邮件方式，CSRC 服务器端和主机端的数据使用加密秘钥进行加密（公共秘钥）。

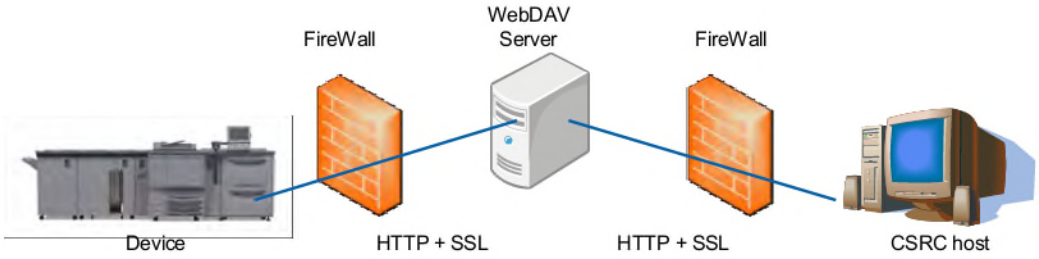
*主机和 CSRC 服务器可以设置加密选项。通过加密系统的公共秘钥，设备和 CSRC 服务器使用相同的加密及解密秘钥。此外，在 HTTP 通信中，可以设置 SSL（HTTPS)。通过 SSL， 将 WebDAV 服务器和 CSRC 主机间的通讯数据进行加密。

- **HTTP 协议的诸多安全功能**

HTTP 协议不依赖于环境，可以使用诸如认证、代理、SSL 等诸多安全功能。

使用 SSL，复合的安全技术如公共秘钥加密算法，私用秘钥加密算法，数字证书以及哈希函数等可以阻止数据被窃听和数据被篡改及假冒。

在通讯中心，可以综合使用这些安全功能，提供适配于用户环境的安全措施。



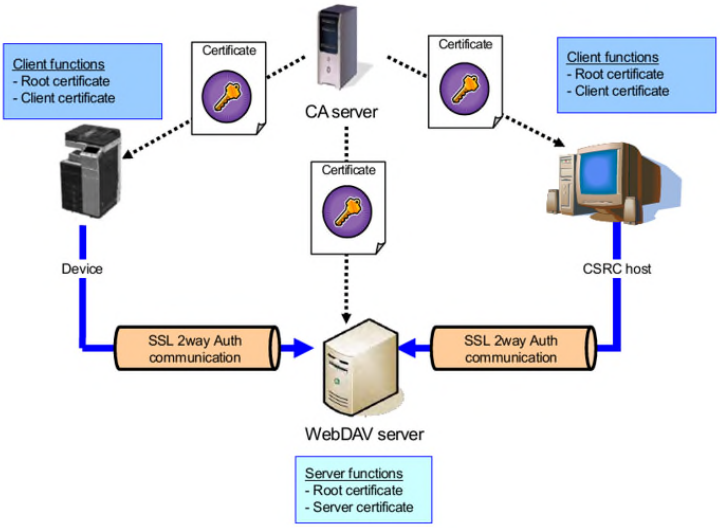
4 产品认证

- **端到端的数据安全**

在 HTTP 通信模式中，对 WebDAV 服务器的读和写都在网络上进行。因此，存在很小的信息泄露的安全漏洞存在可能性。在产品认证中，为了更高的安全性，采用 SSL 认证方式用来保证设备与 WebDAV 的服务器之间通信的合法性。

在产品认证中，基于许可证管理的服务器先发放一个唯一许可代码给客户端。在证书发放服务器中注册发放的代码后，即允许客户端证书和服务器端证书的发起。

当在通信中心和 MFP 端使用客户端证书时，服务器端证书会发送到用户在 WebDAV 中设置的邮箱地址中，设备和 WebDAV 服务器端的通信的数据安全得到增强。



5 DCA 的安全

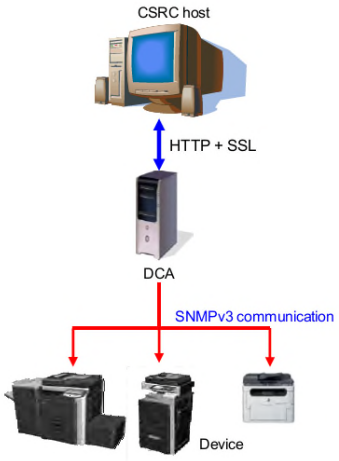
- **DCA 和设备之间的 SNMPv3 通信**

DCA（设备收集代理）支持 SNMPV1 以及 SNMPv3 通信方式。

在 SNMPv1 通信方式中，普通文本在网络路由器中进行流动，此环境下，传输过程中的数据可能被嗅探，存在数据包被外部捕获的风险。

因为“community name”是 SNMPv1 通信仅有的认证方式，它有可能同时被泄露。这样依赖，MIB 中存储的所有数据可能被泄露的“community name”进行欺诈访问。

在 SNMPv3 通信中，除了相对于 SNMPV1 通信中的“community name”外的“user name”外，新增了一个认证机制，用于增强设备访问的稳固性。所有的通信路链路上流动的数据都被加密，因此除非知道同一个加密系统/秘钥，否则数据很难被侦测。



- **DCA 和 CSRC 服务器之间的通信**

DCA 和 CSRC 服务器之间的通信使用 HTTP 中的 SSL 协议进行加密。而且，一个唯一 ID 会分配给 DCA 设备，每次通信时，数据传输会在 ID 检查通过后再进行。如果通信中发现 ID 不一致，将不会进行数据传输。