KONICA MINOLTA

多功能复合机

bizhub 950i

使用说明书 安全操作

2023. 3
Ver. 1.03

目录

1 安全

2 管理员操作

3 用户操作

1 安全

1 安全

1.1 序文

感谢您购买我们的产品。

本使用说明书包括使用 bizhub 950i/850i/AccurioPrint 950i/850i 机器所提供的安全功能时的操作程序和保护措施。为保证机器的最佳性能和有效使用，在使用安全功能前，请认真阅读本说明书。机器管理员应保管好本说明书，以便随时参考。在遇到操作问题并有疑问时，使用本手册非常有助于找到解决方案。

本使用说明书 （1.03 版本）阐述如下内容。

TOE 名	KONICA MINOLTA bizhub 950i/bizhub 850i/AccurioPrint 950i/AccurioPrint 850i with FK-516
版本	G00-09

1.1.1 机器使用人员

使用机器的人分为用户和管理员。特别是已经在机器中注册的用户称为注册用户。管理员分为两种：一种是预先导入计算机；另一种则是由导入的管理员进行注册。前者称为机器管理员，后者称为用户管理员。

用户管理员是获授权可作为管理员操作机器的用户。机器管理员或用户管理员可注册用户管理员。在机器的 ISO15408 认证中，对用户管理员指定 “ 全权授予 ”，由他们进行评估。请注意，用户管理员应负责操作控制注意事项。关于详细信息，请参照第 1-11 页。

与机器管理员的区别如下：

- 在更改密码或认证失败时，用户管理员适用和用户相同的步骤。
- 要更改用户密码，请登录到用户模式。

下表列出了各用户和管理员可执行的操作。

模式	说明	显示	可用操作
用户模式	已通过用户或用户管理员认证的用户界面登录的状态	用户	• 作业显示画面功能 • 用户画面功能 可用操作取决于各界面
	已通过供用户管理员或机器管理员访问用户模式的界面 * 登录的状态	管理员	• 管理员画面功能 • 作业显示画面功能 • 用户画面的部分功能 （信息显示、作业显示和 Box） 可用操作取决于各界面以及用户管理员或机器管理员
管理员模式	已通过供用户管理员或机器管理员访问管理员模式的界面 * 登录的状态		

* 此界面用于对用户管理员和机器管理员进行认证

提示

- 作业列表中不显示正在接收由密码加密的 PDF 这一作业。
- 此后，管理员是机器管理员和用户管理员的统称。
  管理员模式用于可由机器管理员 （管理员模式）和用户管理员 （管理员模式）操作的管理员画面说明中。
- 在 HTML 版本的 User's Guide 中，将机器管理员 （管理员模式）表示为管理员设置模式。

1.1.2 用户和作业删除之间的关系

作业	界面	模式（显示）	作业删除
打印 *1 接收传真（打印收到的文件）	控制面板 **Web Connection**	用户模式（用户）	从作业列表中选择用户所执行的作业后删除。
		用户模式（管理员）	从作业列表中选择一个作业并将其删除。
扫描 *2 复制 *2 发送传真 *2	控制面板	-	当扫描单元正在读取文档时，执行停止或在屏幕上触摸［停止］，从所显示的当前已停止的作业列表中选择一个作业并删除。
	控制面板 **Web Connection**	用户模式（用户）	从作业列表中选择用户所执行的作业后删除。
		用户模式（管理员）	从作业列表中选择一个作业并将其删除。
储存在用户 Box 中	控制面板	-	当扫描单元正在读取文档时，执行停止或在屏幕上触摸［停止］，从所显示的当前已停止的作业列表中选择一个作业并删除。*3
	控制面板 **Web Connection**	用户模式（用户）	从作业列表中选择用户所执行的作业后删除。
		用户模式（管理员）	从作业列表中选择一个作业并将其删除。
阅读存储在用户 Box 中的文档	控制面板 **Web Connection**	用户模式（用户）	从作业列表中选择用户所执行的作业后删除。
		用户模式（管理员）	从作业列表中选择一个作业并将其删除。
打印存储在私人 Box 中的文档 *4	控制面板	-	在打印过程中触摸［停止］从所显示的当前已停止的作业列表中选择一个作业并删除。

*1：使用 ID & 打印用户 Box，作业中包含的文档也将被删除。

*2：作业中包含的文档也被删除。

*3：不保存文件。

*4：不删除文件。

1.2 遵照 ISO15408 标准

当本机器上的 [加强安全设置] 设为 [开启] 时，即有更多加强安全功能可用。

本机器的安全功能应符合下述 PP 和勘误表。

PP Name: Protection Profile for Hardcopy Devices

PP Version: 1.0 dated September 10, 2015

Errata: Protection Profile for Hardcopy Devices-v1.0 Errata #1.June 2017

1.2.1 硬件和软件

以下列出了用于此机器的 ISO15408 评估的软件、硬件及其版本。

用户应自负责任对本机所用的硬件和软件进行妥善管理。

硬件 / 软件	版本等
打印机驱动程序	(c) 2003 KONICA MINOLTA, INC. Universal / Generic Universal PCL: 版本 3.9.303.0
	(c) 2003 KONICA MINOLTA, INC. Universal / Generic Universal PS: 版本 3.9.303.0
外部认证服务器	Windows Server 2019 Std
DNS 服务器	Windows Server 2019 Std
WebDAV 服务器	apache2 2.4.46
检查日志服务器	
SMB 服务器	samba 4.13.5
SMTP 服务器	Postfix 3.5.6

* 为传输邮件服务器安装符合 SMTP 协议 (符合 RFC2821) 的服务器。服务器和 MFP 之间的 SMTP 认证设置必须匹配。请参照 HTML 版本的 User's Guide 以了解详细步骤。

* 由打印机驱动程序可以显示版权和打印机驱动程序名。有关显示方式的详细资料，请参照 HTML 版本 User's Guide 中的 “主屏幕 - 打印 - 在打印机驱动程序中设置项目 - 初始设定选项中的可用操作”。

1.2.2 操作保护措施

在机器运转过程中执行错误操作或错误输入时，机器将显示警报信息或发出警报声 (PEEP)。(如果辅助功能的声音设置中的各设置音为 [关] 时，将不发出 “PEEP” 的警报声。) 如果发布警报信息或警报声，请根据以信息或其他方式提供的指示内容，进行正确操作或正确输入。

管理员在访问各模式之前 / 期间 / 之后，不要在各设置画面显示的状态下离开机器。如果在各设置画面显示的状态下离开机器，将会使设置和重要信息遭受被伪造的危险。如果必须离开时，请务必退出访问，返回认证画面。

管理员务必告诫各常规用户，在访问各模式之前 / 期间 / 之后，要在各模式画面尚在显示的情况下离开机器时，需退出访问并返回认证画面。

在机器运行过程中出现错误信息时，请按照信息的指示处理。关于错误信息的详细情况，请参照附带的使用说明书。处理不了时，请与维修代理联系。

如果在使用机器过程中网络连接失败，请检查 LAN 电缆连接和网络设置，或者关闭 / 打开电源。

如果在使用 **Web Connection** 的过程中机器的控制面板上显示错误并停止，请关闭 / 打开机器的**主电源开关**，然后重启。

作为针对高信赖度通信连接失败的对策，要确定错误原因并进行响应，请检查电缆连接状态、检查日志、通信对方的状态、设置等。无法确定如何处理错误时，请与您的维修代表联系。

如果输入了非法参数，请重新启动机器。

Web Connection 功能仅在设置为接受 “Cookie” 时才可使用。

如果对机器有任何疑问、要求或相关意见，请联系所购买机器的经销商或维修代表。
有关这台机器的任何通知将由您购买机器的经销商或维修代表以书面形式发出。

1.3 安装步骤

如果要使用加强安全模式，管理员应按本章所述设置步骤，按顺序执行 "1.3.1 密码规则的设置 " 和 "1.3.17 检查设备信息 "，然后执行 "1.5.7 机器的操作和控制 " 来完成安装步骤。如果不能执行所定的步骤，请联系维修技术员 （CE）。

可以以经 ISO/IEC15408 认证的配置使用机器。

本机 （bizhub 950i、bizhub 850i、AccurioPrint 950i、或 AccurioPrint 850i）以安装了固件和传真组件的配置 TOE 版本 G00-09 通过了认证。验收时，确认传真组件已由维修技术员 （CE）组装好。

管理员应以以下方式确认机器具有兼容的配置。

- 技术管理员 （CE）：请事先向经销商确认技术管理员 （CE）的名字。由此，在访问时就可以通过核实名字来确定为授权的技术管理员 （CE）。
- 主机：验收主机时，检查是否有未经授权的安装或不经意的改造。如发现异常，请与经销商联系。检查主机前门部是否标有 “bizhub 950i”、“bizhub 850i”、“AccurioPrint 950i”、或 “AccurioPrint 850i” 中的任一型号名称。
- 软件：检查固体版本是否兼容。

	MFP 卡版本
bizhub 950i/bizhub 850i/AccurioPrint 950i/AccurioPrint 850i	ACVX0Y0-F000-G00-09

备注
通过了 ISO15408 审评的机器固件版本符合上述版本。

要注意如果随固件更新而改变了版本，将不保证其功能正常运行。

参考
关于版本的确认方式，请参照第 1-17 页。

- 传真组件：要验证标识，请要求技术管理员 （CE）取出传真组件。FK-516 （A92D）的电路板表面有一个条形码，前 4 位以 “A92D” 开头。如果号码不同，请要求维修技术员 （CE）安装正确的传真组件。请确认安装已核实了标识的传真组件 FK-516 （A92D）。

参考
关于传真功能的详细内容，请参照 HTML 版本的 User's Guide 的 “Home > About This machine > Specifications of Optional Components”，或第 1-16 页。

- 指南：检查电子签名以确认所提供的指南是否与本 MFP 相符。经 ISO15408 认证的数据均拥有电子签名。为了确认数据的完整性，在您使用的电脑环境下在所提供的数据文件的属性中检查电子签名。适合本 TOE 的指南如下所示。适用语言为英文。

- bizhub 950i/850i User's Guide Ver. 1.00 （ACVX-9990BA-00）
- AccurioPrint 950i/850i User's Guide Ver. 1.00 （ACVX-9990BB-00）
- bizhub 950i/850i/AccurioPrint 950i/850i User's Guide Security Operation 2023. 3 Ver. 1.03 （ACVX-9990B-00）

- 如果安装了或激活了以下选购件，将不保证作为 ISO/IEC15408 认证设备使用。

- 图像打印控制器 （IC-xxx）
- 认证单元 （AU-xxx）
- 键小键盘 （KP-xxx）
- 安全组件 （SC-xxx）
- 传真组件 （不适用于本机的传真选购件）
- i-Option （LK-xxx）
- 升级组件 （UK-xxx）
- 本地接口组件 （EK-xxx）
- 扩展内存 （EM-xxx）

备注
在完成 “ 网络设置 ” 之前，切勿将机器连接于外部网络或因特网。

否则，由于网络保护功能无效，机器将面临可能受到外部的未授权访问的危险。

在通过 **Web Connection** 进行设置时，确保机器未连接于外部网络。

管理员应执行下述安装步骤。

1.3.1 密码规则的设置

重新启动机器后，请执行密码规则设置。

如果在 ［机器设置］中不显示 ［管理员］，机器有可能仍处于启动过程中，或其他管理员已登录。

等待机器启动完毕并可以操作，或等待其他管理员退出。

参考

关于设置方式的详细内容，请参照 HTML 版本的 User's Guide 的 “Home > Descriptions of Functions/Utility Keys > Password Rules”，或第 1-15 页。

1.3.2 IP 地址及 DNS 域名的设置

请执行 IP 地址和 DNS 域名的设置。

在使用 **Web Connection** 引进用于 IPsec 的证书时需要执行此设置。

参考

关于设置方式的详细内容，请参照 HTML 版本的 User's Guide 的 “Home > Descriptions of Functions/Utility Keys > TCP/IP Setting”。

1.3.3 管理员密码的设置

设置满足密码规则条件的管理员密码。

如果输入了不满足密码规则条件的密码，将显示错误信息拒绝您的访问。

管理员密码的默认值为 ［1234567812345678］。

在显示机器使用信息确认画面时，选择 ［不允许］。如果错误地在机器使用信息确认画面选择了 ［允许］，请打开管理员模式，然后点击 ［系统设置］- ［列表 / 计数器］- ［抄表计数和设备确认 Tx 设置］- ［关闭］。

备注

妥善管理，不要忘记管理员密码。

一旦遗忘，则需对包括硬件在内的所有数据进行初始化。

参考

关于设置方式的详细内容，请参照 HTML 版本的 User's Guide 的 “Home > Descriptions of Functions/Utility Keys > Administrator Password Setting”，或第 2-29 页。

1.3.4 用户认证的设置

设置为 ［开启 （MFP）］、［开启 （外部服务器）］（只限活动目录）或 ［开启 （MFP + 外部服务器）］（只限活动目录）。

当设置为 ［开启 （外部服务器）］（只限活动目录）或 ［开启 （MFP + 外部服务器）］（只限活动目录）时，请确认已将票据保存时间 （活动目录）设置为 ［0 分钟］。

如果选择了一个不预期的认证方式，请重新进行此设置。

参考

关于设置方式的详细内容，请参照 HTML 版本的 User's Guide 的 “Home > Descriptions of Functions/Utility Keys > Authentication Type”，或第 2-20 页。

1.3.5 正确设置日期和时间

正确设置机器中的日期和时间。在受到攻击时检查的日志数据将以此日期和时间设置被记录。如果设置了错误的日期和时间，将有可能无法获取正确的信息。

如果未正确地设置日期和时间，请重新进行此设置。

参考

关于设置方式的详细内容，请参照第 2-55 页。

1.3.6 作业日志获取方式的设置

设置为 [自动]。

注意不要选择 [syslog]。

选择 WebDAV 作为 TX 协议。

如果已经设置了上述以外的其他设置，请重新进行此设置。

参考

关于设置方式的详细内容，请参照第 2-30 页。

1.3.7 ID & 打印功能操作的设置

设置为 [开启]。

参考

关于设置方式的详细内容，请参照第 2-22 页。

1.3.8 强制记忆 RX 的设置

设置为 [是]。

还需要设置 [强制记忆 RX 用户 Box 密码]。

如果此设置中不显示任何选项，则可能未正确安装传真组件。请联系维修技术员 (CE)。

正确安装传真组件，然后从 "1.3.1 密码规则的设置 " 重新确认。

参考

关于设置方式的详细内容，请参照第 2-28 页。

1.3.9 固件更新 (USB) 密码的设置

设置满足密码规则条件的固件更新 (USB) 密码。

如果输入了不满足密码规则条件的固件更新 (USB) 密码，将显示错误信息拒绝您的访问。

参考

关于设置方式的详细内容，请参照 HTML 版本的 User's Guide 的 “Home > Descriptions of Functions/Utility Keys > Firmware Update (USB) Permission Setting”。

1.3.10 FIPS 模式的设置

设置为 [开启]。

当 [加强安全设置] 设置为 [开启] 时，将无法更改此设置。

要更改此设置，请将 [加强安全设置] 设置为 [关闭]，然后将 [FIPS 设置] 设置为 [开启]。此后，将 [加强安全设置] 设置为 [开启]。

参考

关于设置方式的详细内容，请参照第 2-61 页。

1.3.11 自定义样式功能的设置

在管理员模式下将 ［系统设置］-［自定义样式功能］的 ［复印 / 打印屏幕样式］和 ［发送 / 保存屏幕样式］设置为 ［ISO15408］。如果选择了不同的模式，请重新进行此设置。

如果不显示 ［ISO15408］，则需要由维修技术员 （CE）进行设置。有关详细资料，请联系维修代理。

在维修技术员 （CE）进行了所需的设置后，从 "1.3.1 密码规则的设置 " 重新确认。

1.3.12 加强安全设置

在将 ［加强安全设置］设为 ［开启］之前，请执行以下操作。

如果省略了以下操作将 ［加强安全设置］设置为 ［开启］，请将 ［加强安全设置］设置为 ［关闭］。完成以下操作后，重新将 ［加强安全设置］设置为 ［开启］。

- 使用 ［管理员］-［网络］-［TCP/IP 设置］-［快速 IP 过滤］，将 IP 过滤设置设为 ［无过滤］。
- 使用 ［管理员］-［网络］-［TCP/IP 设置］-［TCP/IP 设置 （无线 LAN 接口组件）］将无线 LAN 设置设置为 ［有线设置］。
- 删除不必要的全局 CA 根证书。

备注
使用 LAN 电缆 （交叉）直接连接或经由网络集线器使用 LAN 电缆连接使用 **Web Connection** 的电脑与机器，来构建仅限连接机器和管理员个人电脑的网络。此时，请不要连接外部网络或因特网。否则，由于网络保护功能无效，机器将面临可能受到外部的未授权访问或被窃取密码等重要信息的危险。

使用 ［管理员］-［安全］将 ［加强安全设置］设置为 ［开启］。

参考
关于设置方式的详细内容，请参照第 2-11 页。

有关因将 ［加强安全设置］设置为 ［开启］而改变的各个安全功能设置的详细内容，请参照第 2-9 页。

1.3.13 IPsec 通信证书的设置

设置用于 IPsec 通信的设备证书。

备注
使用 LAN 电缆 （交叉）直接连接或经由网络集线器使用 LAN 电缆连接使用 **Web Connection** 的电脑与机器，来构建仅限连接机器和管理员个人电脑的网络。此时，请不要连接外部网络或因特网。否则，由于网络保护功能无效，机器将面临可能受到外部的未授权访问或被窃取密码等重要信息的危险。

参考
关于设置方式的详细内容，请参照第 2-15 页。

1.3.14 网络设置

配合客户的使用环境进行网络设置。

同时，执行各个服务器的设置，和对应各个设置的服务器侧的设置。

参考
关于设置方式的详细内容，请参照第 2-13 页。

1.3.15 检查是否执行了用于与各个服务器通信的 IPsec 设置

检查是否执行了用于机器和 DNS 服务器 /SMTP 服务器 /WebDAV 服务器 /SMB 服务器 / 检查日志服务器通信的 IPsec 设置。

此外，检查是否在必要时执行了用于机器和客户端电脑通信的 IPsec 设置。

如果未执行预期的 IPsec 设置，请从 "1.3.2 IP 地址及 DNS 域名的设置 " 重新确认设置，并从 "1.3.13 IPsec 通信证书的设置 " 进行确认。

1.3.16 检查是否已完成操作中禁止的各种设置

通过将各个功能设置为无效，以在无法使用的状态下使用机器，来对机器的操作进行管理。有关各个功能的详细内容，请参照第 1-12 页。

1.3.17 检查设备信息

检查是否执行了为了设置及应用机器的安全功能而禁止的各项设置，并确认在控制面板上显示［设备信息］（安全模式）。

如果不显示［设备信息］（安全模式），则需要由维修技术员（CE）进行设置。有关详细资料，请联系维修代理。

在维修技术员（CE）进行了所需的设置后，从 "1.3.1 密码规则的设置 " 重新确认。

1.4 加强安全设置

将［加强安全设置］设置为［开启］，使本机器的安全功能有效。关于通过［开启］[加强安全设置］变更的不同安全功能的设置详情，请参照第 2-9 页。

1.4.1 根据 IS015408 认证进行操作的主要安全功能

下面介绍在 IS015408 认证下操作的主要安全功能。

功能	说明
识别和认证功能	通过密码认证对管理员模式，用户认证模式，用户 Box，用户 Box 文件以及机密打印文件进行访问控制，只有认证的使用者才许可访问。只允许设置符合密码规则的密码。机器不接收一个易解读的密码设置。关于密码规则的详细信息，请参照第 1-15 页。 作为针对定义认证失败的对策，如果在密码认证期间输入了错误密码，且错误输入次数等于或大于管理员预先设置的次数（1 至 3 次）时进入访问锁定状态，禁止后续的密码输入操作。禁止密码输入操作，可防止机器被盗用或机器内数据被盗取。管理员负责重置密码输入操作禁止状态。关于详细信息，请参照第 2-19 页。
用户限制功能	各用户使用的特定功能可能会受到限制。关于详细信息，请参照第 2-24 页。
检查功能	机器执行的操作和作业历史记录等信息可以保存在存储或日志服务器中。设置作业日志（检查日志）可对机器上进行的非法操作和不规范行为进行追查。关于详细信息，请参照第 2-30 页。
网络通信保护功能	通过使用 IPsec 将机器和客户端电脑通信数据加密，防止网络窃听使情报流失。关于详细信息，请参照第 2-13 页。

1.5 操作控制的保护措施

本机应在符合如下条件的办公室环境下进行操作和数据处理。为保护应保护的数据，为了保护对象数据，请将以下的条件作为基础对本机进行管理。

1.5.1 机器所有者的作用

备注

管理员的启用不当，会造成安全功能弱化或失效。并且，为了维护用户使用机器时的安全性，务必执行以下对策。

机器所有者 （个人或组织）应承担控制机器的全部责任，从而保证不进行不正确的操作。

- 机器所有者应让管理员了解组织的安全方针和程序，对其进行教育以遵守制造商的指导和相关文件，并给予足够时间来获得所需的能力。同时，机器所有者应对机器进行操作和管理，使管理员可根据相关方针和程序对机器进行妥善配置和操作。如果管理员不遵守或无法遵守该方针和程序，将无法维护本机的安全功能。
- 机器所有者应让机器用户了解组织的方针和程序，并教育其遵守这些方针和程序，还要对机器进行操作和管理，使用户获得所需的能力。如果不具备充分的能力，将有可能无法保护用户的个人信息，及无法维护机器的安全运用。
- 机器所有者应授予用户根据组织安全方针和程序使用机器的权限。机器所有者应严格执行此项，以避免机器用户泄露安全信息。
- 机器所有者应任命值得信赖的，拥有丰富知识、技术及经验以能够维护机器的安全，并在发生问题时能够进行恰当处理的的合格的管理员，并委托其负责机器的控制。
- 机器所有者应对机器进行操作和管理，使管理员在合适的时候查看作业日志 （检查日志）以确定在运行期间是否存在安全隐患或故障状态。通过执行恰当的管理，就能防止问题的发生，或在发生问题时能够迅速采取措施。
- 机器所有者务必仅允许管理员处理已自动分发的作业日志 （检查日志）数据。机器所有者还应对机器进行操作和管理，确保作业日志 （检查日志）数据不被非法访问、删除或更改。否则，可能会意外泄露重要信息。

1.5.2 维护安全环境

建议机器所有者在使用加强安全模式的同时，维护下述使用环境。

- 在用于运用机器的客户端电脑上，针对操作环境和应用程序 （病毒软件、打印机驱动程序和浏览器等）应使用最新颁布的更新程序，以确保在安全的状态下使用。
- 应在有防火墙保护的内部网络环境下连接机器，以杜绝外部网络访问机器。此外，为避免未经授权的设备连接到内部网络，需要进行妥善管理。

备注

如果连接了无防火墙保护的内部网络环境，将会受到来自外部网络的攻击。

1.5.3 管理员的职责

管理员应承担控制机器的全部责任，以保证不进行不正确的操作。

- 机器管理员及用户管理员应任命值得信赖的，拥有丰富知识、技术及经验的合格的用户管理员，并委托其负责机器的控制。
- 在使用外部认证服务器、SMTP 服务器 （邮件服务器）、DNS 服务器、检查日志服务器、WebDAV 服务器或 SMB 服务器时，应由管理员对各服务器进行妥善管理，并应该定期检查确认没有未经允许改变设置。

1.5.4 密码使用规则

备注

密码的泄露，将有可能引发安全功能的丧失，信息的泄露、伪造等问题。

管理员必须妥当管理强制记忆 RX 用户 Box 密码，以免泄露。不设置容易猜测的密码。另一方面，用户应适当控制用户密码，以免被泄露。再次强调，密码应不易被猜测。除此之外，确保采取以下的措施。

妥善管理，不要忘记管理员密码。一旦遗忘，则需对包括硬件在内的所有数据进行初始化。另外，还有可能无法执行必要的设置和确认。

< 达到有效安全 >

- 机器管理员不得将管理员密码透露给除机器管理员以外的任何人。
- 机器管理员必须定期更改管理员密码。

- 管理员必须定期更改强制记忆 RX 用户 Box 密码。
- 机器管理员应确保未采用从生日、员工身份证号等容易猜测的任何数字作为管理员密码。
- 管理员应确保未采用从生日、员工身份证号等容易猜测的任何数字作为强制记忆 RX 用户 Box 密码。
- 如果用户密码已更改，管理员应让相应用户尽快更改密码。
- 如果管理员密码已被维修技术员更改，机器管理员应尽快更改管理员密码。
- 管理员应让用户确保设置用于用户认证和用户可使用的 Box 的密码仅限用户本人知晓。
- 管理员应让用户定期更改用于用户认证的密码设置。
- 机器管理员应在用户管理员更改密码时，让其登入至用户模式后在［机器设置］-［效用］-［信息］-［更改用户密码］中更改密码。
- 管理员应确保不要采用从生日、员工身份证号等容易猜测的任何数字作为用户认证密码。

1.5.5 外部认证服务器的管理条件

管理员和服务器管理员要对本机和连接至机器所在办公室 LAN 的外部认证服务器应用补丁或执行帐户控制，以确保进行适当的访问控制。

使用本机器的用户必须在外部认证服务器中进行注册后方可使用本机。另外，服务器管理员应定期检查注册用户，以确保未注册无关用户。

如果外部认证服务器不使用 Windows Server DNS，将无法使用机器。

1.5.6 安全功能操作设置的操作要求

管理员要遵守以下操作条件。

- 管理员应确保机器按照安装步骤中所描述的设置运行。
- 管理员应确保进行正确操作控制，使机器运行时［加强安全设置］设置为［开启］。
- 当［加强安全设置］为［关闭］时，管理员要再次将［加强安全设置］设为［开启］。关于设置方式的详细内容，请参照第 2-11 页。关于维修技术员所做设置的相关详情，请联系维修代理。

1.5.7 机器的操作和控制

管理员应执行如下操作控制。

- 无论何时，在完成管理员模式下的操作时，管理员应从管理员模式下登出。机器管理员应确保个人用户完成在用户认证模式的操作后退出用户认证模式，包括用户 Box 和用户 Box 文件的操作。
- 在进行用户注册和 Box 注册时，管理员应确保对适当的用户进行适当设置，其中包括功能限制和 Box 属性。
- 管理员应对已在机器中注册的用于 IPsec 通信的设备证书（IPsec 通信证书）和 CA（证书颁发机构）证书进行妥善管理。
- 管理员应该妥善管理包含已存储在（分发至）服务器中的作业日志（检查日志）数据的文件，并确保只有机器管理员才能处理此类文件。
- 作为使用检查日志及发现不正当行为时的对策，管理员应在适当时候检查作业日志（检查日志），以判定在操作期间是否存在安全隐患或故障情况。
- 在网页浏览器上进行预览时，因相关内容可缓存在电脑上，故管理员应按照各浏览器指定程序删除缓存，并确保用户执行相同程序。
- 作为检测到未经授权的传真发送和接收时的对策，管理员不得允许维修技术员设置 CS Remote Care。如果在未设置 CS Remote Care 的情况下从 CS Remote Care 中心接收到连接，则机器面板上会显示错误（R82）。
- 管理员应检查访问 MFP 的传真接收状态 / 用户状态，并查看检查日志以检测是否有受到攻击的可能。
- 管理员不得允许维修技术员将 RS-232C 界面设置为有效。设置为无效时，将不应答来自 RS-232C 界面的连接。