KYOCERA 京瓷

京瓷

多功能复合机（一体机）与打印机

安全白皮书

版本 052025/2025年5月14号

© 2025 京瓷办公信息系统有限公司 版权所有

目录

前言 5
识别、身份验证和授权 6
识别和身份验证 6
用户身份验证 6
身份验证模式 6
多功能复合机（一体机）/打印机登录 7
授权 8
授权模式 8
用户授权管理 9
会话管理 9
网络安全 11
安全通信的设置 11
IP 过滤器设置 11
端口设置 11
安全哈希算法设置 15
验证协议 15
IEEE802.1x 15
SMTP 验证 17
POP before SMTP 17
通信信道保护 17
SNMP v3 17
IPv6 17
IPsec 17
TLS 18
S/MIME 19
Wi-Fi 19
电子邮件发送/接收限制功能 19
电子邮件发送目的地限制功能（许可/拒绝） 19
电子邮件发件人限制功能（许可/拒绝） 19
证书自动验证 20
从简单证书注册协议服务器获取由 CA 颁发的设备证书 20

© 2025 京瓷办公信息系统有限公司 版权所有

检查证书的吊销状态 20
每个协议的服务器证书验证级别设置 20
设备证书验证级别设置 21
存储数据保护 22
数据保护 22
HDD/SSD 加密 22
HDD 覆盖-擦除 22
HDD/SSD 安全数据清除 23
访问限制 24
用户文件夹 25
作业文件夹 25
传真文件夹 26
打印安全 28
安全打印 28
个人打印 28
防止未经授权的复印 28
文字印章/附加信息 28
安全水印 28
传真安全 29
传真加密通信 29
发送/接收限制 29
错误传输预防 29
确认输入 29
禁止用数字键直接输入传真号码 29
传输前的目的地确认 30
禁止使用时间 30
子地址通信 30
子地址机密传输（发送/接收） 30
子地址布告栏传输（发送/接收） 30
存储转发 31
防止未经授权的访问的安全措施 31
发送安全 32
发送前的目的地确认 32
禁止广播传输 32
新（地址）目的地输入 32
PDF 加密 32

© 2025 京瓷办公信息系统有限公司 版权所有

文件数字签名 32
FTP 加密发送 32
扫描安全 33
机密文档检测 33
设备管理 34
作业管理 34
授权查阅作业信息 34
审核日志 34
登录日志 34
设备日志 34
安全通信错误日志 35
日志管理 35
发送作业日志（电子邮件地址） 35
系统日志 35
安全功能的完整性验证 35
数字签名固件 35
安全启动 35
运行时完整性检查（RTIC） 36
允许列表 36
使用限制 36
接口阻止 36
USB 存储类逻辑块 36
锁定操作面板 36

© 2025 京瓷办公信息系统有限公司 版权所有

前言

京瓷的多功能复合机（一体机）/打印机均标配操作系统。和PC一样，多功能复合机（一体机）/打印机可以安装HDD或SSD。办公室使用的多功能复合机（一体机）/打印机可以处理各种类型的敏感信息。然而，多功能复合机（一体机）/打印机也会遭受近期先进的、多样化威胁的攻击，例如通过网络不经授权访问设备、通过网络窃取或更改信息、以及HDD泄漏信息等。京瓷办公信息系统（中国）有限公司（以下简称京瓷）为客户提供了拥有各种安全功能的多功能复合机（一体机）/打印机上的各种安全功能。我们始终积极采取安全措施来应对这些威胁，以便客户放心使用京瓷多功能复合机（一体机）/打印机。此外，京瓷还获得了通用标准认证（即ISO15408），该认证通过第三方客观验证了客户是否能够正确执行安全功能。此验证也适用于严格的流程，包括适当的产品设计、生产和交付。京瓷产品在设计之初便充分考了了必要的安全功能和性能。

本文件解释了安装在京瓷多功能复合机（一体机）/打印机上的安全功能如何抵御威胁，并使客户能够维持安全管理。我们衷心希望这份文件能被京瓷客户充分利用。

© 2025 京瓷办公信息系统有限公司 版权所有

识别、身份验证和授权

识别和身份验证

识别和身份验证是验证用户是否有权访问或使用设备的重要过程。用户需要输入访问凭证，例如登录用户名和密码、用于识别用户身份的用户ID，以及只有用户知晓的密码。(图1)

若要使用识别和身份验证功能，用户需要事先在多功能复合机（一体机）/打印机上注册登录用户名和登录密码。也就是说，只有已注册的用户才能访问多功能复合机（一体机）/打印机。京瓷多功能复合机（一体机）/打印机可以帮助管理员管理用户授权，他/她可以适当地为每人提供不同级别的授权，例如“普通用户”或“管理员”。而且，也可以为每名用户设定特定的多功能复合机（一体机）/打印机功能权限。在获得多功能复合机（一体机）/打印机访问权限之前，用户必须输入有效的登录用户名和密码来进行身份验证，从而防止未经授权人员的使用。可以根据用户访问日志稍后跟踪访问多功能复合机（一体机）/打印机的人员、时间和频率。

用户身份验证

该功能通过在识别多功能复合机（一体机）/打印机的授权用户后控制对信息的访问来保护信息。

实现资产的访问控制和资产的保护。

当用户输入的登录用户名和登录密码与预先注册的用户名一致时，用户将通过身份验证，然后被授予访问多功能复合机（一体机）/打印机的权限。

密码策略

可以设定密码策略，鼓励用户使用强密码，包括最小长度密码，防止使用非常短的密码。此外，该功能还能拒绝200 个最常用密码中列出的密码，从而帮助用户创建和管理更难猜测的密码。这有助于防止弱密码和未经授权的访问。

帐户锁定策略

帐户锁定是在预定时间内超过预定登录次数时暂时锁定帐户的功能。可设置锁定前的重试次数(1-10次），以及锁定时间(1-60分钟）。当错误密码重复登录次数超过预设次数时，用户帐户将被禁用。帐户锁定策略设置高度减少了对多功能复合机（一体机）/打印机成功的密码破解攻击。

身份验证模式

京瓷多功能复合机（一体机）/打印机有以下身份验证模式。

© 2025 京瓷办公信息系统有限公司 版权所有

本地身份验证

本地身份验证模式基于在多功能复合机（一体机）/打印机上的本地用户列表上注册的用户数据对用户进行身份验证。只有注册用户才能访问多功能复合机（一体机）/打印机。

网络身份验证

网络身份验证模式通过身份验证服务器对用户进行身份验证。用户可以使用在身份验证服务器上注册的用户数据进行登录。提供了诸如NTLM和Kerberos等服务器。也可以连接第三方服务器。例如，可以通过配置 LDAP 安全（即基于LDAP over TLS）、Kerberos、SASL（带/不带签名）以及 NTLM 来设置安全的用户认证。在安全的TLS连接中，传输数据是加密的，并且可以验证用户是否可靠，以确保双方通信的安全性。通过将 TLS 连接与 Kerberos/NTLM 用户关联起来，可以防止利用未经授权的凭据/令牌进行未授权访问。

Kerberos身份验证

Kerberos在网络上的客户端和身份验证服务器之间对用户进行身份验证。这统一了多个服务器和用户身份验证信息，并允许用户单点登录。通信通道可以在这里进行加密。

NTLM身份验证

当多功能复合机（一体机）/打印机与网络连接时，NTLM 用于网络登录。NTLM 认证在多功能复合机（一体机）/打印机和服务器之间通过质询-响应模式执行，以避免在网络上以非加密形式传输密码。服务器的质询数据已经过加密，NTLM 哈希被用作加密密钥进行加密。

图1

多功能复合机（一体机）/打印机登录

除了从操作面板输入登录用户名和登录密码外，还可以使用以下登录模式。

ID卡验证（选配）

有两种ID卡验证方式。一种是仅使用ID卡登录，另一种是将ID卡放在读卡器附近或上方，然后输入密码。ID卡验证

© 2025 京瓷办公信息系统有限公司 版权所有

可用于本地身份验证。(图2)

当ID卡信息已经预先注册在多功能复合机（一体机）/打印机的用户列表、外部验证服务器或第三方验证服务器上时，可以授权验证用户使用她/他的ID卡访问设备。

使用ID卡进行身份验证（例如当前使用的员工卡）可启用部门管理和用户管理功能。可以基于与ID卡相关联的用户信息来限制特定功能。(图3)。

图2

图3

授权

可以对授权用户限制特性的使用功能，如彩打、全色复印、发送、传真传输、文件夹存储、外部记忆存储等特定功能。这有助于显著降低多功能复合机（一体机）泄漏信息的可能性。根据各种用户级授权、“用户”、“管理员”或“设备管理员”，也可以限制对多功能复合机（一体机）/打印机的设置访问。某些多功能复合机（一体机）/打印机具有组合、双面和Eco打印限制功能。这十分有用，例如无权限设置“不组合”的用户必须设置“2合1”或更多来完成复印，否则用户不能进行复印。

授权模式

多功能复合机（一体机）/打印机具有以下授权模式。

本地授权

本地授权是一种授权功能，可以在执行本地身份验证时与多功能复合机（一体机）上注册的本地用户列表一起使用。用户可以限制使用此模式。

网络授权（组授权/服务器授权）

网络授权包括组授权和服务器授权。

© 2025 京瓷办公信息系统有限公司 版权所有

组授权是通过使用网络认证时获取的组信息以及预先存储在多功能复合机（一体机）上的组授权信息来完成的。可以根据认证服务器上注册的各自组应用限制。

服务器授权是通过使用网络认证时获取的用户信息以及预先存储在服务器*1上的用户授权信息来完成的。

可以根据认证服务器上注册的用户来设置限制。

可以通过组授权/服务器授权来限制多功能复合机（一体机）的使用，从而使特定组/用户使用多功能打印机更加安全。

*1：京瓷服务器必须在用户环境中配置

OAuth2

在OAuth授权后，授权服务器发出访问令牌，多功能复合机（一体机）接收该令牌。此令牌使Microsoft Exchange能够发送和接收电子邮件。过去，由于传统基本认证涉及将诸如ID和密码之类的认证信息链接到外部，因此存在安全风险。借助OAuth 2.0，用户可以使用京瓷设备，通过访问令牌进行认证，而无需传递认证信息，从而更加安全地使用设备。

按功能登录

登录受功能限制；访客授权设置后，如下功能会加以限制：打印限制、复印限制、Eco打印限制、传真限制、扫描至文件夹限制和扫描至发送限制。使用具有登录限制功能的用户必须进行登录验证。因此，只有在列表上注册的有限用户才能使用特定功能。安全性可以有效防止京瓷设备泄漏信息，同时维持用户友好性。

用户授权管理

关于用户授权管理，功能的使用权限是基于授予各个用户的不同的授权级别，仅授权用户可以使用。用户授权包括机器管理员、管理员和普通用户。此外，一些“管理员”授权也可以授予普通用户。因此，没有授权的用户无法非法使用特定功能，未经授权的用户是不允许使用这些功能的。

会话管理

会话管理是一种功能，它在从用户登录到多功能复合机（一体机）到用户通过身份验证后用户从多功能复合机（一体机）注销的时间之间管理一段会话。

可提供以下管理功能。

自动面板重置

自动面板重置是一种自动注销的功能：重置设置，然后在一段时间后没有操作时返回默认设置。用户可以指定上次

© 2025 京瓷办公信息系统有限公司 版权所有

操作后执行重置的时间。当最后一名用户无法注销系统时，自动面板重置有助于防止未经授权访问多功能复合机（一体机）的恶意攻击。

© 2025 京瓷办公信息系统有限公司 版权所有

网络安全

安全通信的设置

京瓷多功能复合机（一体机）/打印机只能从一定范围的IP地址和端口号范围内限制网络上的通信。强大的安全哈希算法也可用于 TLS 服务器证书。该算法可防止数据在网络中被篡改、窃听以及防止伪装行为。

我们希望京瓷多功能复合机（一体机）/打印机能够按照客户设定的安全策略来使用。通过使用安全快速设置功能，管理员可以根据其安全策略，从1级、2级和3级中选择一个合适的级别。根据所选级别，可以一次性集中执行多个安全功能，如网络设置、接口阻止设置和日志设置。然后，还可以分别调整某些有限安全功能的设置，使用安全设置功能。用户可以根据其安全策略，在最合适的环境下安全地使用京瓷多功能复合机（一体机）/打印机。

IP过滤器设置

IP过滤器通过设置IP地址范围或协议类型来限制网络访问多功能复合机（一体机）/打印机。此功能能够指定允许访问的IP地址范围（以及子网掩码组合），并且仅允许IP地址在指定范围内的客户访问。可以选择一些许可的通信协议，然后将其设置为主动的。对于IPv4和IPv6支持，可以设置来自单个PC的通信或来自多个PC的通信，以及IPP（用于远程管理打印作业的网络协议）和HTTP（用于在web服务器和web浏览器之间传输数据的协议）。因此，指定设置有助于防止无授权访问多功能复合机（一体机）/打印机。

端口设置

仅启用所需的端口号，以使用诸如 IPP 或 SMTP 之类的协议进行通信，从而禁用了未设置为启用的端口号。

协议	端口号	设置	注释
FTP服务	TCP 21	启用/禁用	FTP服务是用于接收文件的协议。
HTTP	TCP 80	启用/禁用	当从www服务器和浏览器之间的网页接收/发送数据时，使用HTTP协议。
NetBEUI	TCP 139	启用/禁用	NetBEUI是一种用于小型网络的协议，用于文件共享和打印服务、以及文件接收。
HTTPS	TCP 443	启用/禁用	HTTPS是使用TLS执行加密的协议。

© 2025 京瓷办公信息系统有限公司 版权所有

协议	端口号	设置	注释
IPP over TLS	TCP 443	启用/禁用	IPP over TLS 是一种结合了用于加密通信通道的TLS和用于互联网打印的IPP的协议。此外，IPP over TLS可以使用有效证书。
LPD	TCP 515	启用/禁用	LPD是一种用于打印文本文件或PostScript文件的打印协议。
IPP	TCP 631	启用/禁用	IPP是一种控制通过TCP/IP（包括互联网或打印设备）发送/接收打印数据的协议。
ThinPrint	TCP 4000	启用/禁用	ThinPrint是Thin客户端环境中可用的打印技术，也支持TLS。
WSD Scan	TCP 5358	启用/禁用	Windows Vista WSD是一种用于网络连接的多功能复合机（一体机）/打印机的协议。这使得用户能够更轻松地检测（安装）多功能复合机（一体机）/打印机设备或发送/接收数据。通过多功能复合机（一体机）/打印机扫描的原始文档图像可以作为文件存储在WSD电脑中。
WSD Print	TCP 5358	启用/禁用	Windows Vista WSD是一种使多功能复合机（一体机）/打印机能够进行网络连接的协议。这也使用户能够更轻松地检测（安装）多功能复合机（一体机）/打印机设备或发送/接收数据。
Enhanced WSD	TCP 9090	启用/禁用	Enhanced WSD服务发现采用了一种程序，用于轻松连接到网络的各种设备并进行使用。多功能复合机（一体机）/打印机的状态可以通过状态监视器通过该端口 9090 进行监控。
Enhanced WSD over TLS	TCP 9091	启用/禁用	Enhanced WSD (TLS)，这是一种安全协议。它提供加密、身份验证和安全性（防止篡改）。
RAW	TCP 9100-9103	启用/禁用	RAW 协议在打印方面与 LPR 协议采取不同的步骤。通常，多功能复合机（一体机）/打印机使用端口号 9100，并且还使用SNMP或MIB来配置和监控打印机状态。
SNMPv1/v2	UDP 161	启用/禁用	SNMP协议用于网络管理系统。利用读写区域名称执行正常通信。

© 2025 京瓷办公信息系统有限公司 版权所有

协议	端口号	备注	注释
SNMPv3	UDP 161	启用/禁用	SNMP协议用于网络管理系统。利用用户名和密码执行正常通信。可以使用身份验证选项或加密选项。
DSM扫描		启用/禁用	DSM（分布式扫描管理）使用Windows Server 2008 R2，用以处理大型公司中的大量用户数据。
FTP客户端		启用/禁用	FTP客户端是用于通过网络转发文件的通信协议。
LDAP		启用/禁用	LDAP服务器上的通讯簿称为外部通讯簿。传真号码和邮件地址可以指定为目的地。
LDAP over TLS		启用/禁用	LDAP over TLS是一种使用TLS加密信道以保护LDAP通信的协议。
POP3		启用/禁用	POP3是用于接收电子邮件的标准协议。
POP3 over TLS		启用/禁用	POP3 over TLS是一种协议，它结合了用于接收电子邮件的POP3和用于加密信道的TLS。
SMTP		启用/禁用	SMTP是用于发送电子邮件的协议。
SMTP over TLS		启用/禁用	SMTP over TLS是一种协议，它结合了用于发送电子邮件的SMTP和用于加密信道的TLS。
SMB客户端		启用/禁用	SMB是一种通过网络执行文件或打印机共享的协议。SMB客户端支持V3.0。
eSCL		启用/禁用	eSCL是一种用于从Ma OS X进行远程扫描的协议。
eSCL over TLS		启用/禁用	eSCL over TLS是使用TLS证书的eSCL通信协议。所有eSCL over TLS通信都是加密的。
LLTD		启用/禁用	LLTD是用于网络拓扑发现和服务质量诊断的协议。

© 2025 京瓷办公信息系统有限公司 版权所有

协议	端口号	设置	注释
Privet		启用/禁用	Privet是一种允许在本地网络上发现云连接设备的协议，它还提供接口以获取有关设备的信息并执行某些操作，例如在本地发送打印作业
DNS over TLS	TCP 853	启用/禁用	DNS over TLS 是一种使用 TLS 加密 DNS 请求和响应的协议，TLS 用于加密通信通道。
SCEP		启用/禁用	简单证书注册协议（SCEP）为一种自动向设备颁发证书的协议。
OCSP/CRL		启用/禁用	证书吊销列表（CRL）是由CA提供的一份列表，上面记载了已被吊销的证书的序列号。 在线证书状态协议（OCSP）是一种协议，它允许网络浏览器及其他客户端实时查询单个证书的状态。
REST		启用/禁用	REST是一种支持多个软件的web应用程序的软件架构分布式超媒体系统。
REST over TLS		启用/禁用	REST over TLS是使用TLS证书的REST通信协议。所有REST over TLS通信都是加密的。
Bonjour		启用/禁用	Bonjour是一种网络技术，使用户可以自动发现设备。
VNC		启用/禁用	虚拟网络计算（VNC）是一种远程控制软件，它使用RFB协议通过网络连接远程控制设备的图形用户界面（GUI）。
VNC over TLS		启用/禁用	通过TLS进行的虚拟网络计算（VNC over TLS）是一种远程控制软件，它使用RFB协议通过客户端电脑和设备之间的TLS网络连接远程控制设备的图形用户界面（GUI）。

© 2025 京瓷办公信息系统有限公司 版权所有

协议	端口号	设置	注释
Enhanced VNC over TLS		启用/禁用	Enhanced VNC over TLS是京瓷自己的远程控制软件，它使用RFB协议通过一次性密码（OTP）访问设备，并远程控制设备的GUI，只有授权管理员才允许这样做。基于OTP的设备安全访问增加访问控制的安全强度。
XJMF		启用/禁用	交换作业信息格式(XJMF) 是 XJDF 工作流中使用的通信协议。
XJMF over TLS		启用/禁用	XJMF over TLS是用于安装了XJMF通信所需的应用程序（如 Kyocera Production Print Suite 和 Kyocera Print Job Manager）的客户端PC与设备之间通过TLS进行安全通信的协议。

安全哈希算法设置

TLS 加密技术中使用的强大安全哈希算法支持自签名证书和CSR证书。此功能也可用于将采取安全措施的用户环境。

验证协议

验证协议是一种旨在实现安全通信认证的通信协议。京瓷多功能复合机（一体机）/打印机支持具有邮件发送功能的IEEE802.1x网络验证、SMTP验证和POP before SMTP验证协议。这可以防止伪装行为。

IEEE802.1x

IEEE802.1x 是由IEEE (电气电子工程师学会)定义的关于基于端口认证的标准。此协议仅允许授权用户（已认证设备）在连接网络时进行通信，从而防止未授权设备连接网络。如上所述，京瓷设备支持IEEE802.1x，这将不允许未认证客户端未经授权访问网络，从而防止信息的未授权泄露。京瓷多功能复合机（一体机）/打印机采用以下所述的四种认证模式。

PEAP-TLS/PEAP（受保护的可扩展身份验证协议-传输层安全性）

根据ID和证书对客户端进行验证，同时检查验证服务器的证书。

EAP-PEAP（可扩展身份验证协议-协议可扩展身份验证协议）

客户端根据ID/密码进行身份验证，并且仅检查身份验证服务器证书的通用名。

© 2025 京瓷办公信息系统有限公司 版权所有

EAP-FAST（可扩展身份验证协议 – 通过安全隧道进行灵活身份验证）

EAP-FAST是IEEE802.1.x/EAP身份验证方法。基于用户ID和密码为客户端和身份验证服务器执行相互身份验证，PAC（受保护访问凭证）基于唯一的共享密钥为用户建立隧道。

© 2025 京瓷办公信息系统有限公司 版权所有

EAP-TTLS（可扩展身份验证协议 - 隧道传输层安全性）

客户端根据用户ID和密码进行身份验证，还根据电子证书对身份验证服务器进行验证。

对于EAP-TLS，验证需要客户端和服务器电子证书；而对于EAP-TTLS，则使用用户ID和密码而不是客户端证书。与EAP-TLS相比，这使得EAP-TTLS更容易引入。电子证书用于证明验证服务器的有效性。因此，它有助于实现更安全和更可信的通信。

SMTP验证

SMTP验证允许仅在SMTP服务器上成功验证ID和密码后才发送电子邮件。通过限制对SMTP服务器的访问，该功能可防止未经授权的用户通过SMTP服务器发送电子邮件。

POP before SMTP

POP before SMTP在SMTP服务器发送电子邮件之前执行POP身份验证。POP身份验证完成后，可在指定的时间段内发送电子邮件。在发送电子邮件之前进行POP身份验证可防止伪装。

通信信道保护

通信信道保护是为了保证网络通信信道的安全保护。根据目的或加密方案，可以提供多种协议。京瓷多功能复合机（一体机）/打印机支持以下协议，从而有效地保护数据不通过网络进行更改或泄漏。

SNMP v3

SNMP是一种标准协议，用于监视和控制连接到网络的设备。此外，SNMPv3还可通过身份验证和加密来保护数据的机密性。

IPv6

与IPv4相比，IPv6是一种新的IP协议。京瓷多功能复合机（一体机）/打印机支持IPv6，能够连接到路由器，并使用诸如ping之类的的基本控制协议。除上述基本连接之外，通过实施严格的安全措施，确保了更加安全的连接。

IPsec

IPsec是一种协议，其功能是通过加密各个IP数据包，从而保护传输中的数据免遭窃听或篡改。要使用IPsec发送/接收数据，需将启用了IPsec功能的电脑连接到网络，同时将启用了IPsec功能的多功能复合机（一体机）/打印机连接到网络，然后将它们都设置为启用IPsec功能。对从电脑发送到多功能复合机（一体机）/打印机的打印数据，以及从多功能复合机（一体机）发送到电脑的扫描数据，均应用IPsec加密。因此，IPsec支持更安全的数据交换。此外，强大的安全哈希算法可用于一对主机（主机到主机）之间的通信。

© 2025 京瓷办公信息系统有限公司 版权所有

TLS

TLS是一种用于加密 Web 访问等数据传输的系统，还具有互相检查通信目标方是否可靠以进行相互通信的功能。京瓷多功能复合机（一体机）/打印机支持包括TLS1.0、TLS1.1、TLS1.2和 TLS1.3在内的TLS 加密协议，从而防止数据在网络中被篡改或窃听。此外，强大的安全哈希算法可用于服务器与客户端之间的通信。以下是TLS加密协议。

IPP over TLS

IPP over TLS是一种互联网打印协议，它将用于在互联网或TCP/IP网络上交换打印数据的IPP与用于加密通信通道的TLS相结合。这使得用户能够通过网络安全地向多功能复合机（一体机）/打印机发送打印命令。

HTTP over TLS

HTTP over TLS是一种协议，它结合了用于在TCP/IP网络上通过网络浏览器或其他方式发送和接收数据的HTTP以及用于加密通信通道的TLS。在电脑与多功能复合机（一体机）/打印机之间传输数据时，该协议能够降低数据被未授权用户篡改和泄露的风险。

FTP over TLS

FTP over TLS是一种协议，它结合了用于在TCP/IP网络上传输文件的FTP和用于加密通信通道的 TLS。当使用FTP协议从多功能复合机（一体机）/打印机发送扫描数据时，TLS加密应用于通信通道。FTP over TLS实现了更安全的数据传输。

ThinPrint over TLS（选配）

ThinPrint over TLS是一种协议，它结合了用于带宽控制和打印作业压缩的ThinPrint协议以及用于加密通信通道的TLS。因此，它提供了一个安全且高效的打印环境。

SMTP over TLS

SMTP over TLS是一种协议，它结合了电子邮件传输和加密服务器与多功能复合机（一体机）/打印机之间通信通道的TLS。这可以防止伪装、窃听或篡改传输中的数据。

POP3 over TLS

POP3 over TLS是一种结合了一种电子邮件接收协议POP3和用于加密服务器与多功能复合机（一体机）/打印机之间通信通道的TLS。这可以防止伪装、窃听或篡改传输中的数据。

© 2025 京瓷办公信息系统有限公司 版权所有

S/MIME

安全多用途互联网邮件扩展（S/MIME）是一种允许用户对其电子邮件进行加密和数字签名的技术。如果用户证书和中间证书已被导入京瓷设备，那么从该设备发送的消息可以使用用户的公钥进行加密。这可以防止消息在传输过程中被第三方截获。此外，如果在京瓷设备上安装了设备证书，可以附加使用设备的私钥（发送方[多功能复合机（一体机）/打印机]的身份）创建的数字签名。这可以防止消息被第三方伪造和篡改（发送方的保证）。

Wi-Fi

支持最新的无线网络安全标准WPA3-Personal和WPA3-Enterprise*2，它们提供了更强大的保护，从而防止 KRACK攻击和暴力破解。这可以防止未经授权的设备连接到多功能复合机（一体机）/打印机提供的独立网络，从而保护设备免受未经授权的使用。

Wi-Fi Direct设备可以在不经过接入点的情况下相互连接。也就是说，无需使用路由器。这是因为Wi-Fi Direct设备会根据需要自行建立临时网络。这些网络运行在一个独立于任何基础网络的安全域中。Wi-Fi Direct使用Wi-Fi Protected Setup，使用户能够轻松设置连接并支持WPA2-PSK（个人）。

*2：京瓷已获得Wi-Fi CERTIFIED WPA3认证。

电子邮件发送/接收限制功能

发送/接收电子邮件时，京瓷系统提供如下所述的电子邮件发送/接收限制，从而可防止未经授权的用户发送错误的电子邮件或恶意攻击。

电子邮件发送目的地限制功能（许可/拒绝）

可以使用电子邮件发送限制功能限制电子邮件发送目的地以获得许可或拒绝。许可的发送目的地域须提前注册，以便电子邮件发送到先前注册的允许目的地域。拒绝发送的目的地域也须提前注册，以便拒绝之前已注册的被拒绝目的地域的电子邮件。这可防止发送错误的电子邮件。

电子邮件发件人限制功能（许可/拒绝）

京瓷多功能复合机（一体机）/打印机可以打印电子邮件附件。通过预设的电子邮件发件人限制功能限制电子邮件接收。许可的发件人域须提前注册，以便接收之前已注册的许可发件人域的电子邮件。拒绝的发件人域也须提前注册，以便拒绝之前已注册的被拒绝发件人域的传入邮件。这样便可针对垃圾邮件之类的恶意攻击实施安全措施。

© 2025 京瓷办公信息系统有限公司 版权所有

证书自动验证

用户可以使用CAV（证书自动验证）软件来管理复杂的操作，从而增强安全性。CAV包括身份验证和TLS加密功能，能够通过SCEP（简单证书注册协议）、OCSP（在线证书状态协议）和CRL（证书吊销列表）来监督证书的注册和重新注册验证，并监控证书的有效期。CAV通过验证证书的有效期并在证书过期时重新注册或续期，解决了使用无效证书的安全问题。此外，CAV提供的4096位证书加密能够有效抵御高级证书和PKI攻击。CAV还可以确保符合用户的安全策略。

从简单证书注册协议服务器获取由CA颁发的设备证书

向管理设备证书的SCEP（简单证书注册协议）服务器发送证书签发请求，同时附带一个基于管理员输入信息生成的CSR（证书签名请求）。从SCEP服务器获取的由CA颁发的证书将自动注册为设备证书。

通过这一自动化流程，简化了由CA颁发的证书管理，维持安全性。

只有具有管理员权限的用户才能选择SCEP设置。

检查证书的吊销状态

检查服务器证书吊销状态有两种方法：（1）向OCSP（在线证书状态协议）响应器发送请求；（2）将证书与多功能复合机（一体机）/打印机中注册的CRL（证书吊销列表）进行比对。

这两种方法皆是可用的，以便注重安全性的用户可以根据自身环境选择合适的方法。

只有具有管理员权限的用户才能选择OCSP/CRL（证书验证）

每个协议的服务器证书验证级别设置

服务器的证书验证级别可能会根据目标服务器在用户的安全环境中的不同而有所不同。此功能允许根据每个协议将服务器证书验证级别设置为0级到3级（例如，SMTP/POP3/FTP/LDAP/DNS）。服务器证书验证级别可设置为(0) 级无验证、(1)级仅验证有效期、(2)级验证有效期和证书链、(3)级验证有效期、证书链并确认吊销状态。

请注意，与目标服务器的连接必须通过TLS加密来确保安全。

可以确认合法的连接目的地和已授权的证书。

只有具有管理员权限的用户才能选择这些设置。

© 2025 京瓷办公信息系统有限公司 版权所有

设备证书验证级别设置

此功能可设置设备证书验证级别（0到3）。设备证书验证级别可设置为(0)级无验证、(1)级到期日验证、(2)级到期日和链验证、(3)级到期日、链验证和撤销确认。

请注意，到客户端的连接必须通过TLS加密进行保护。

可在多功能复合机（一体机）/打印机中维护受信任的证书。

只有具有管理员权限的用户才能选择这些设置。

© 2025 京瓷办公信息系统有限公司 版权所有

存储数据保护

数据保护

存储在HDD或SSD中的敏感或机密信息不得从多功能复合机（一体机）/打印机中泄露。京瓷通过以下功能对存储的信息采取了安全保护措施，从而确保我们的客户能够安全地使用京瓷的多功能复合机（一体机）/打印机。

HDD/SSD加密

HDD/SSD加密功能是一种安全功能，用于加密存储在多功能复合机（一体机）内部HDD或固态SSD中的文件用户设置和设备信息。该功能使用256位AES（高级加密标准）算法对数据进行加密。京瓷多功能复合机（一体机）具有加密模块[*3]。即使HDD或SSD被恶意人员从多功能复合机（一体机）中移除，存储在HDD或SSD的敏感或机密信息也不会泄露。

*3：加密模块由京瓷设计并实施。

HDD覆盖-擦除

HDD数据覆盖擦除功能是另一种安全功能，它防止第三方读取存储在HDD上的各种数据，例如用户设置、设备信息和图像数据等。

扫描数据会暂时存储在HDD中，然后在多功能复合机（一体机）上输出。用户还可以注册各种设置。即使在数据输出或被用户删除后，实际数据仍会保留在HDD中，直到被其他数据覆盖。因此，存在使用特殊工具恢复剩余实际数据的可能性，这可能导致信息泄露。HDD覆盖-擦除功能配置为用无意义的数据覆盖已输出或已删除数据的实际数据，从而无法恢复实际数据。

HDD覆盖-擦除过程将自动执行。所以不需要手动操作。即使在操作过程中或整个作业完成后取消相应作业，HDD数据也会立即被覆盖。

© 2025 京瓷办公信息系统有限公司 版权所有

以下两种覆盖方法可用于HDD覆盖擦除功能，并可用于多功能复合机（一体机）/打印机型号。

- 单次覆盖

单次覆盖方法使用固定值对不必要的数据进行一次覆写，从而使数据难以恢复或还原。

- 三次覆盖(A)

三次覆盖(A)覆盖HDD不需要的数据。不需要的数据是1）所有可寻址位置被覆写为固定值，2）所有可寻址位置被覆写为其补数，3）所有可寻址位置被覆写为随机数据最后，对最后一次覆写进行验证。经过这种彻底的擦除过程，数据几乎无法被恢复（图4）

当覆盖-擦除批量数据时，三次覆盖(A)方法可能比单次覆盖方法需要更长的时间。

图4

HDD/SSD安全数据清除

在多功能复合机（一体机）/打印机租赁结束或设备寿命终结时，如果设备内部仍残留有私人、敏感或机密数据，可能会导致数据泄露。为了避免数据泄露，“安全数据清除”是一种安全功能，能够彻底清除设备内保留的数据或残留数据。为了避免泄露数据，“安全数据清除”使用三次覆盖(A)，七次覆盖(A)，七次覆盖(B)，和/或SSD安全擦除如下所述。（具体情况取决于多功能复合机（一体机）/打印机型号）。

- 三次覆盖(A)

三次覆盖(A)覆盖HDD的所有数据区域。所有数据区域都用固定值覆盖， 然后用固定值的补值覆盖，然后用随机数据覆盖，最后对数据进行验证。因此，即使有一个复杂的修复过程，也很难恢复完全删除的数据。数据被覆盖三次，然后数据被验证一次。

- 七次覆盖(A)

© 2025 京瓷办公信息系统有限公司 版权所有

七次覆盖(A)覆盖HDD的所有数据区域。所有数据区域都被覆盖两次，一次被随机数据覆盖。因此，即使有一个复杂的恢复过程，恢复完全删除的数据也是极其困难的。这些数据被覆盖了七次。

- 七次覆盖(B)

七次覆盖(B)覆盖HDD的所有数据区域。所有数据区域都用零（0x00）覆盖，然后用固定值（0xff）覆盖。这将被重复执行三次。然后，将用固定值（0xAA）覆盖数据区域。因此，即使有一个复杂的恢复过程，恢复完全删除的数据也是极其困难的。这些数据被覆盖了七次。

当覆盖-擦除批量数据时，七次覆盖(A)和(B)方法可能比三次覆盖(A)方法需要更长的时间。

- SSD安全擦除

两种方法，安全擦除和密码学擦除，被用于清理数据。（该方法的可用性取决于多功能复合机（一体机）/打印机型号）。

  - 安全擦除通过ATA命令SECURITY ERASE UNIT对所有数据区域进行擦除。该功能可提供对固态硬盘的可靠擦除。数据被擦除一次。
  - 密码学擦除完全擦除用于加密数据的加密密钥。这使得无法恢复多功能复合机（一体机）内部存储在SSD上的数据。

安全数据擦除功能具有以下特点：可以设置确保在预定时间进行擦除的擦除计划定时器；擦除前通知功能，可在擦除前通知管理员和服务人员；擦除完成后自动打印的擦除完成报告（包括擦除内容和擦除日期）；擦除后系统锁定功能，可在完成擦除后禁止用户使用多功能复合机（一体机）/打印机。管理员可以设置并执行这些功能，从而使设备设置恢复到出厂默认设置。

访问限制

可以在多功能复合机（一体机）内部创建用于存储数据的“用户文件夹”、“作业文件夹”和“传真文件夹”。可以限制对存储在这些文件夹中的数据的访问。

© 2025 京瓷办公信息系统有限公司 版权所有

用户文件夹

用户可以在多功能复合机（一体机）中创建“用户文件夹”，用于存储数据。可以分别为各个文件夹设置文件夹使用限制、数据保留期限和密码。（图5）

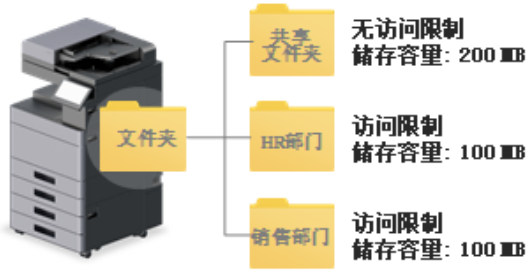

图5

文件夹密码

可以通过密码限制能够访问文件夹的用户。用户需要提前设置一个合适的密码，密码最多可设置为16个字符（可使用包括大写字母、小写字母、数字和特殊字符在内的多种字符）。

文件夹使用限制

可以限制文件夹的容量使用，以便管理HDD容量

所有者设置

用户文件夹只能由已注册为该文件夹所有者的用户访问，未经授权的用户无法访问。可以设置文件夹是否为“共享文件夹”。如果设置为共享，即使未设置为所有者的用户也可以访问该文件夹。考虑到易用性，文件夹可以高效地防止未经授权的访问，从而适当维护安全性。

文件保留期限

经过一段时间后，存储的文件数据可以自动删除，因此不必长时间保存。因此，数据泄漏的机会只会更少。

删除时间

打印作业完成后，存储在方框中的文件数据将被自动删除。因此，数据的删除将不会被遗忘。这可以防止未经授权的第三方查看这些数据。

作业文件夹

© 2025 京瓷办公信息系统有限公司 版权所有

“个人打印”、 “PIN打印”、“快速复印”、“校样保留校对和保留”以及“存储作业”数据可以存储在作业文件夹中，但是用户不能删除也不能创建该文件夹。该文件夹可以采用PIN码保护，以限制访问文件夹。（图6）

图6

自动删除临时文件数据存储

临时保存在“个人打印”、 “PIN打印”、“快速复印”、“校样保留”文件夹中的数据可以在数据存储指定时间段后自动删除。数据只保存所需的时间。因此，数据披露的风险就大大降低了。

传真文件夹

位于多功能复合机（一体机）内的存储传真接收数据的文件夹称为“传真文件夹”。通过内存转发功能，可将传真接收数据存储在传真文件夹中。此外，还根据发件人子地址或传真号码将传真接收数据分配到相应的文件夹，以便轻松对重要文件进行快速确认。可以通过多功能复合机（一体机）面板确认传真接收数据。可以立即打印所需的传真，同时删除不需要的传真。(图7)

图7

文件夹密码

可以通过密码限制能够访问文件夹的用户。用户需要提前设置一个合适的密码，密码最多可设置为16个字符（可使用包括大写字母、小写字母、数字和特殊字符在内的多种字符）。

所有者设置

用户文件夹只能由已注册为该文件夹所有者的用户访问，未经授权的用户无法访问。可以设置文件夹是否为“共享文件夹”。如果设置为共享，即使未设置为所有者的用户也可以访问该文件夹。考虑到易用性，文件夹可以高效地防止未经授权的访问，从而适当维护安全性。

© 2025 京瓷办公信息系统有限公司 版权所有

删除时间

打印作业完成后，存储在文件夹中的文件数据可以被自动删除。否则，保存数据超过必要的时间可能会造成风险。及时删除将有助于保持有效的安全状态。

© 2025 京瓷办公信息系统有限公司 版权所有

打印安全

安全打印

安全打印是多功能复合机（一体机）/打印机的一种打印功能。安全打印功能可用于打印公司机密文件或个人文件，以避免将无人监管的打印文件留给他人或由设备上的其他第三人查看。

个人打印

个人打印是一种打印功能，它一旦保存了从PC发送到多功能复合机（一体机）/打印机中的打印作业，直到用户通过多功能复合机（一体机）/打印机的操作面板输入其适当的密码为止。应用软件要求用户在从PC发送打印作业时在打印机驱动程序中设置访问代码，然后要求用户在打印文件时从设备的面板输入适当的访问代码。打印完成后，数据将被删除。即使在打印前关闭了主电源开关，数据仍然会被删除。这有助于保持在设备上的相对较高的安全性。

防止未经授权的复印

复印时，以下功能可以通过增强文件安全功能来防止未经授权的复印。

文字印章/附加信息

由于文字印章功能能够让用户在第一时间看到文件的重要性，用户可以选择一些印章，如“Confidential”、“Do not duplicate”“Privacy”，具体取决于各种印章的可用性。用户甚至可以根据自己的喜好编辑文字印章。附加信息功能中的“序列号”会打印用于打印输出的设备的序列号，而“插入页码”功能则会将页码按顺序打印在打印文件上。此外，“日期”和“用户名”功能也可供使用。

安全水印

文件材料可以嵌入安全水印图案或文本。当复印嵌入图案的打印材料时，将显示安全水印图案。这清楚地表明复印操作未经授权。(图8)

图8

© 2025 京瓷办公信息系统有限公司 版权所有

传真安全

传真加密通信

这是一种在发送端发送原稿（数据）之前加密的通信方法。因此，在传输过程中的图像数据不能被第三方窃听。因此，第三方没有办法查看和了解这些内容。传入的数据首先被解密，然后在接收端打印。在传输不能向其披露的敏感和机密文件时，这是一种相对有效的沟通方法。

这只在支持相同加密通信功能的京瓷设备之间可用。

相同的加密密钥用于对发送和接收侧（设备）处的原始通信数据进行加密/解密。当发送端和接收端（设备）上的密钥不相同时，将无法执行加密通信。因此，双方（即发送方和接收方）在加密通信之前必须分别相互确定和注册相同的加密密钥。

发送/接收限制

此机能是指只有在满足预定通信条件（即许可传真号码和许可ID号码）时才能使设备发送/接收传真。该功能可以限制通信的传真目的地。当接收限制应用于拒绝列表时，在拒绝号码列表上注册的发件人以及未注册其本地传真号码的发件人发送的入站传真将被拒绝。传真只能发送到在许可号码列表和地址簿上注册的目的地。

错误传输预防

为了防止重要文件被发送到错误的目的地，在传真发送前，用户会被提示两次输入收件人的传真号码。错误发送预防功能可以设置在地址簿、数字键和快速拨号上。此外，该功能禁止再次调用地址目的地。之前的发送目的地不会被保留，从而防止将另一份文件发送到之前的发送目的地。这也有效地防止了信息泄露，因为目的地不会被其他人查看。此外，当用户认证功能启用时，用户注销后，目的地信息将立即被删除。

确认输入

当用户希望通过直接使用数字键输入传真号码来发送传真时，系统会提示用户两次输入相同的传真号码以进行确认。只有在两次输入的传真号码确认一致时，发送目的地才会被启用。这可以防止因误按按键而导致的错误发送。用户可以自行设置此功能。

禁止用数字键直接输入传真号码

可以通过限制通过操作面板使用数字键直接输入来发送传真。此功能允许用户仅向注册在目的地列表上的发送目的地发送传真。因此，用户将无法向地址簿和单触键以外的收件人发送传真。这有助于防止因输入错误传真号码而导致的错误发送以及未经授权的使用。

© 2025 京瓷办公信息系统有限公司 版权所有

传输前的目的地确认

当设置了传输前目的地确认功能时，按下[开始]键后，发送目的地将在屏幕上显示，供用户检查。只有当所有目的地都已在屏幕上显示后，完成确认键才会被启用。由于用户可以在发送传真前重新确认目的地，该功能将有助于预防错误传输。

禁止使用时间

这是一种安全功能，能够设置一个时间段，在此期间禁止打印接收到的传真。当设置了使用禁用时间后，包括打印、复印、接收邮件或USB、传输以及网络传真传输在内的所有操作，以及在指定时间段内打印传真的功能都将被禁用。此功能通过PIN码保护，并且可以临时取消。这可以防止未经授权的使用多功能复合机（一体机），例如在夜间人员较少时打印数据。

子地址通信

子地址通信可通过子地址和密码发送/接收数据，它符合ITU-T（国际电信联盟电信标准分局）的建议。子地址通信功能也可以与其他公司的设备进行通信，例如保密通信（即发送到接收设备的某个文件夹的通信）或轮询通信（即通过接收设备的操作在发送设备上接收原件的通信），但这些仅适用于京瓷设备之间的通信。当使用子地址通信功能时，输入数据将保存在子地址文件夹中。因此，该功能有助于执行相对安全的通信。

子地址机密传输（发送/接收）

在接收方机器中创建子地址机密文件夹后，可以通过识别子地址和密码将不得向其他人公开的重要文件发送到保密文件夹中。收到的文件保存在预先注册的文件夹中，且不会在收到后立即打印。因此，可以打印所接收的数据而不被任何人查看

子地址布告栏传输（发送/接收）

当接受机器支持子地址布告栏传输功能时，用户的文件将被安全传输，不会出现信息泄露。

© 2025 京瓷办公信息系统有限公司 版权所有

存储转发

有了这个功能，接收到的图像可以转发到其他传真机或计算机，也可以在传真接收时打印。当转发设置打开时，所有传入的图像将能够被转发到预定的地址（目的地）。这可以应用于另一个传真、发送邮件、SMB（发送文件）和FTP发送。此外，接收到的图像可以转发到多功能复合机（一体机）中设置的文件夹，然后存储。这样可以防止无人值守（接收的）传真单

留在设备的托盘上。（图9）

图9

防止未经授权的访问的安全措施

传真功能和网络功能在结构上是分开的是相互独立的。通过电话线传入的数据由传真功能处理。该结构可防止借助多功能复合机（一体机）传真功能，通过电话线肆意访问网络。

© 2025 京瓷办公信息系统有限公司 版权所有

发送安全

发送前的目的地确认

用户可以在发送之前在屏幕上确认发送目的地（即地址号码）和主题。这有助于防止发送到错误的地址。在以用户身份发送前，信息始终显示在操作面板上。

禁止广播传输

广播传输是指通过一次操作将同一文件发送到多个目的地的功能。管理员可以禁止或许可这一功能。禁止该功能时，则无法选择包含2个或更多发送目的地的组。这可有效防止由于意外向组增加发送目的地而导致发送到非预期目的地的情况。

新（地址）目的地输入

限制通过操作面板直接输入目的地；指定的目的地仅能为在目的地列表上提前注册目的地（例如地址簿或单触键）。这可有效防止因传真号码输入错误引起的未授权使用或错误发送。

PDF加密

利用PDF加密功能，用户可以选择PDF文件或高压缩PDF文件格式，并通过加密和设置密码保护扫描数据的安全。通过输入正确的密码打开、打印或修改收到的PDF文件时，可以应用这一限制。

文件数字签名

此功能允许用户通过为文件添加数字签名来增强安全性。

京瓷多功能复合机（一体机）预先注册了设备证书和一对私钥/公钥。扫描后，设备证书和密钥对用于生成数字签名，然后由多功能复合机（一体机）生成带有数字签名的文件。

这个过程使接收者能够验证生成带有数字签名文件的多功能复合机（一体机）的身份，以及文件在生成数字签名后是否被篡改。

FTP加密发送

使用TLS执行FTP加密发送以对通信信道进行加密。这样可以维护传输数据的安全。进而极大地降低在传输中篡改或窃取数据的风险。

© 2025 京瓷办公信息系统有限公司 版权所有

扫描安全

机密文档检测

机密文档检测功能可确保文档的机密性，防止文档被泄露或未经授权使用信息资产，并帮助用户遵守各种隐私法规。

指定为机密的纸质文档包含用户宝贵的信息资产。支持机密文档检测功能的京瓷多功能复合机（一体机）/打印机可限制未经授权扫描机密文档。该功能通过禁止执行作业直到完成机密文档检测，防止信息资产泄漏。

当检测到机密文档时，它将被记录在审计日志或系统日志中，为用户提供文档审计跟踪，全面记录与文档相关的活动，如何时和谁访问了文档。

即使使用第三方公司的多功能复合机（一体机）/打印机打印了带有“机密 ”印章的文档，京瓷多功能复合机（一体机）/打印机仍有可能检测到机密文档。因此，在保护机密文件的同时，还能保持用户友好性。

© 2025 京瓷办公信息系统有限公司 版权所有

设备管理

作业管理

可以检查设备中有关作业信息的队列或日志。四类状态，包括“打印作业”、“发送作业”、“存储作业”和“预约作业”，以及包括“打印作业”、“发送作业”和“存储作业”三类的作业日志可供选择。可以引用用户名、时间和目的地等指定作业的详细信息，并根据需要使用它们进行跟踪。此外，当使用打印机驱动程序打印作业时，可以设置文件是否用于作业名称。（图10）

图10

授权查阅作业信息

可以根据用户的授权切换作业日志查阅界面。查阅作业信息和传真传输日志的授权分为详细的作业状态信息和作业日志。启用用户验证后，只有用户可以查看和检查自己的作业日志信息。如以管理员身份登录，所有作业日志信息都会显示在屏幕上。

审核日志

可以获取多功能复合机（一体机）/打印机的审核日志。可以检查用户名、日期和时间及其结果。审核日志包括登录日志、设备日志和安全通信错误日志。通过参考日志，多功能复合机（一体机）/打印机的管理员可以检查设备是否安全使用或没有暴露于风险。

登录日志

可以存储用户身份验证登录日志。如果发生未经授权的操作、更改或泄露多功能复合机（一体机）/打印机中的文件，则登录日志将用于调查和帮助跟踪未经授权的访问。

设备日志

可以记录多功能复合机（一体机）/打印机上的固件更新和设置更改。同样，管理员从系统菜单更改的内容也将被记录。

© 2025 京瓷办公信息系统有限公司 版权所有

安全通信错误日志

管理员可以通过检查安全网络通信错误日志来确认网络通信是否正确执行。如果发现频繁通信失败记录，则可以调查潜在的未授权访问。

日志管理

日志管理有助于管理审核日志和作业日志，并帮助跟踪安全事件的潜在致因。

发送作业日志（电子邮件地址）

当日志达到预定数量时，可以通过电子邮件将各个日志发送到管理员指定的电子邮箱地址。

系统日志

使用系统日志协议，可以将多功能复合机（一体机）/打印机的审核日志实时发送到SIEM（安全信息和事件管理）服务器*4。可以收集和集中管理审计日志。

*4：SIEM服务器必须在用户的环境中进行配置。

安全功能的完整性验证

以下功能用于验证我们产品上安全功能的完整性。这些功能用于验证安全功能的执行模块是否未被篡改且正常运行。同样，也可以验证安全功能所使用的数据的完整性。

数字签名固件

固件上附加了数字签名以确保其有效性。固件控制着多功能复合机（一体机）/打印机的操作。经过数字签名的固件可以防止恶意人员对其进行篡改。多功能复合机（一体机）/打印机可以被保护，防止其被用作入侵网络的跳脚石，从而避免损坏和未经授权的使用。

安全启动

安全启动是一种功能，它确保多功能复合机（一体机）在执行前使用经过授权的固件启动。通过在固件上应用数字签名，可以验证固件的有效性。当多功能复合机（一体机）启动时，固件会被加载到RAM中。此时，会确认上传到多功能复合机（一体机）的固件的哈希值与从签名生成的哈希值是否一致。即使恶意人员创建了未经授权的固件，也无法通过使用数字签名进行的有效性验证。因此，即使固件被恶意人员篡改，也无法被执行。安全启动功能可以防止多功能复合机（一体机）被用作入侵网络的跳板，从而保护设备免受破坏。

© 2025 京瓷办公信息系统有限公司 版权所有

运行时完整性检查（RTIC）

运行时完整性检查是一种功能，它定期验证多功能复合机（一体机）在运行过程中固件的有效性，确保在设备启动后加载到RAM中的固件未被篡改。即使固件被恶意重写，RTIC也能检测到这种情况，并以系统错误的形式发出警告。当与安全启动功能结合使用时，RTIC作为一种防止固件被篡改的安全措施将更加有效。

允许列表

允许列表是一种防范恶意软件的措施。如果出现未经授权的程序文件（包含恶意软件）被安装的情况，允许列表会阻止该程序文件在京瓷多功能复合机（一体机）/打印机上运行。安装在多功能复合机（一体机）/打印机中的允许列表仅包含京瓷认可的、授权的或已知可信的程序文件。如果发现未包含在允许列表中的不可信程序文件，允许列表将自动阻止该程序文件运行。

使用限制

以下使用限制可应用于京瓷多功能复合机（一体机）/打印机。由于多功能复合机（一体机）/打印机上的操作可以受到限制，因此对存储在多功能复合机（一体机）/打印机上的数据的访问也可以受到限制。

接口阻止

可以通过设备的接口如USB设备、USB主机、选购件端口（插槽1）和选购件端口（插槽2）分别进行访问限制。网络接口可以根据协议进行限制。

USB存储类逻辑块

当USB闪存连接到多功能复合机（一体机）/打印机的USB端口时，可能存在数据泄漏或对多功能复合机（一体机）/打印机上未经授权访问数据的风险。管理员可以启用USB存储类功能为关闭（禁用），但仍然允许使用连接到多功能复合机（一体机）/打印机的USB主机接口的身份证读卡器。另一方面，京瓷多功能复合机（一体机）/打印机具有限制USB闪存使用的功能，即使USB闪存被插入到多功能复合机（一体机）/打印机的USB主机接口中。这可以防止数据通过USB闪存从USB接口泄漏以及病毒的传播。

锁定操作面板

可以通过限制多功能复合机（一体机）/打印机的操作面板来控制操作。部分锁定功能分为三个阶段：与面板输入/输出相关的设置、与作业执行相关的设置以及与纸张相关的设置、与管理员希望的禁止等级相关的设置将被启用。锁定操作面板功能可以禁止系统菜单操作和作业取消操作。这可以有效防止对多功能复合机（一体机）/打印机的未经授权的操作。

© 2025 京瓷办公信息系统有限公司 版权所有

京瓷办公信息系统（中国）有限公司 版权所有

上海市黄浦区黄陂南路838弄2号3幢B座6层
电话：021-53011777
热线电话：400-601-6028

京瓷办公信息系统不保证所提及的任何规格将毫无错误。规格如有更改，恕不另行通知。信息在付印时是正确的。所有其他品牌和产品名称可能是其各自所有者的注册商标或商标，特此予以承认。

© 2025 京瓷办公信息系统有限公司 版权所有