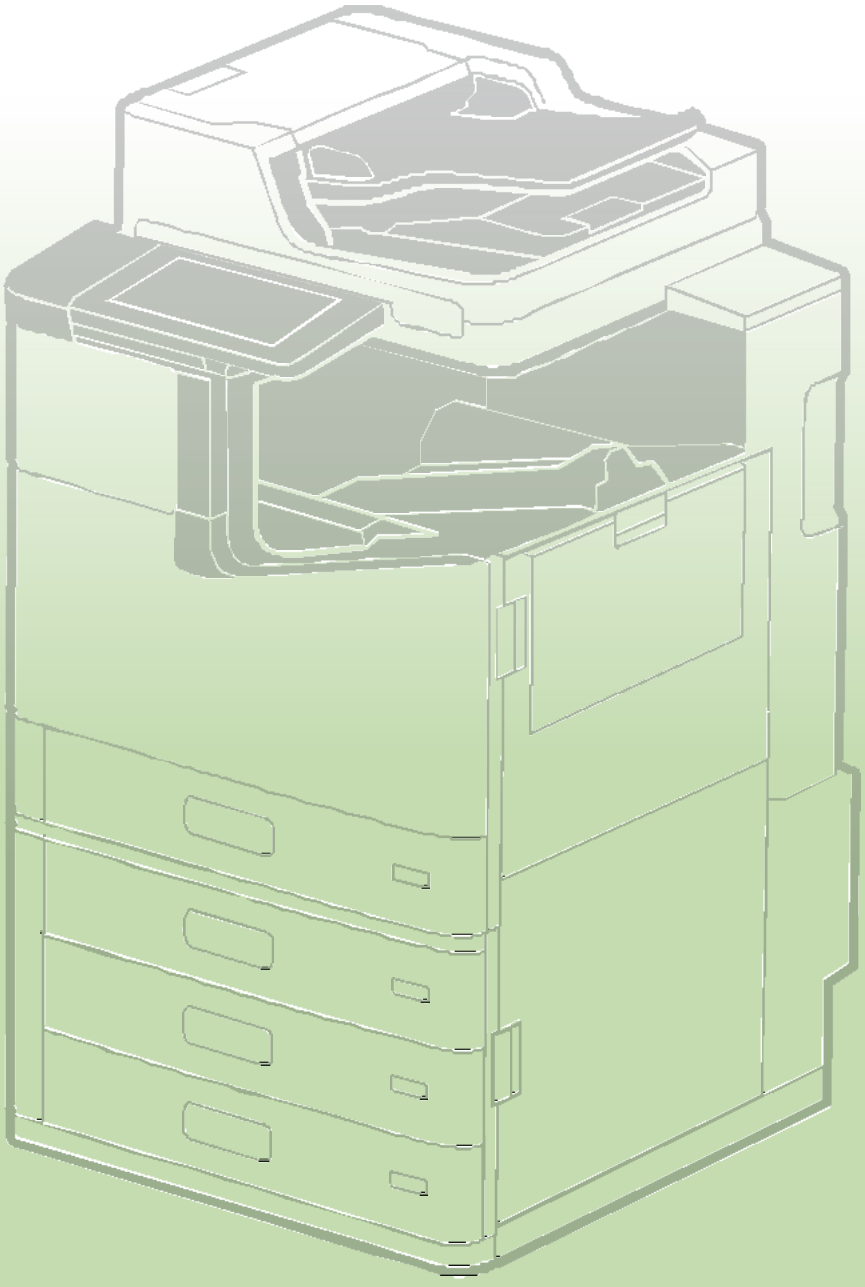
EPSON
EXCEED YOUR VISION

安全性指南



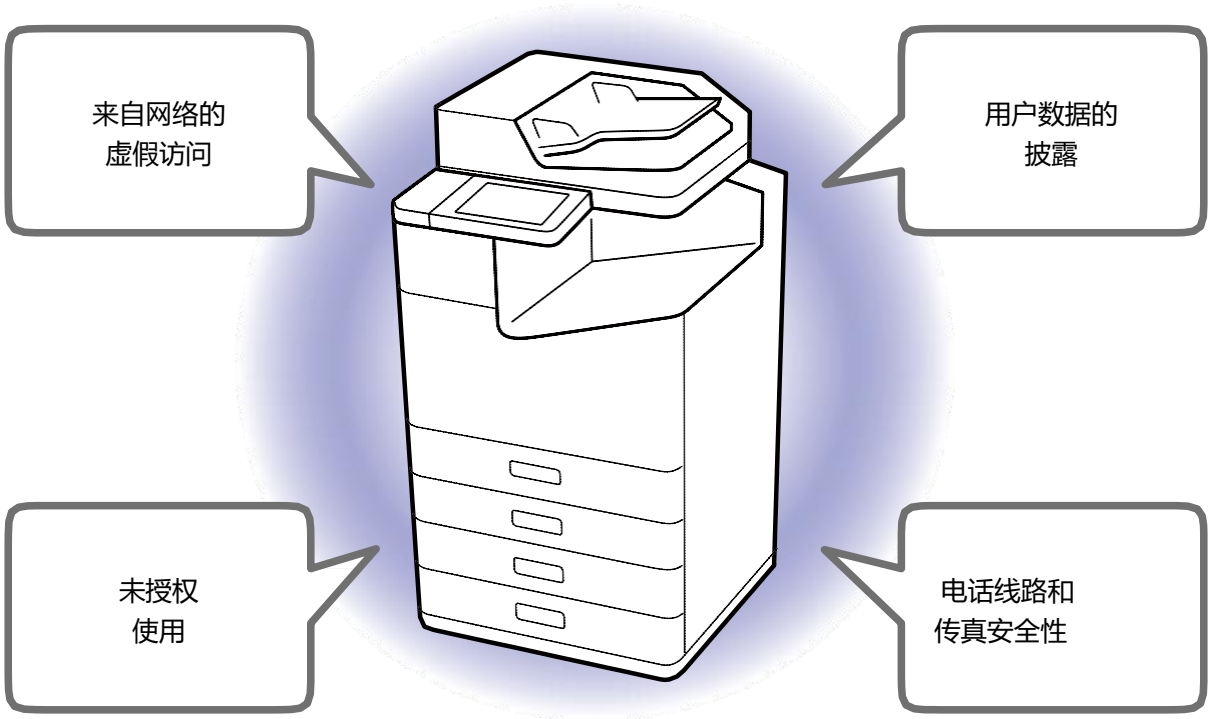
目录

1. 简介

随着信息社会的不断发展，各种机器被连接到网络。

爱普生不断强化产品的功能网络，提高用户友好性。

爱普生产品配备了多种功能。当连接和使用网络时，尤其需要考虑电脑和服务器等设备的安全性。



本指南介绍了爱普生的安全性方法和客户建议，并指导您使用可用的安全功能。请查看您的产品手册，了解如何设置安全性。

2. 爱普生的安全性基本政策

爱普生在安全性方面采取以下方法，帮助客户安全、轻松地使用我们的产品。

1. 我们视产品安全性为产品质量的基础。

   我们的制造流程从产品整个生命周期角度考虑安全性，包括设计到客户成功使用的整个过程。

2. 我们积极为客户提供有关安全性的信息和知识。

3. 我们努力创建针对漏洞的对策。

   - 我们的工作集中于使用行业标准工具实现漏洞测试，并努力交付没有漏洞的产品。
   - 我们定期监控产品固件中使用的开源软件的漏洞信息。
   - 当发现新的漏洞时，我们会及时分析，并提供信息和对策。

4. 我们应用安全性标准。

   ISO/IEC 15408，IEEE 标准 2600.2™

   ISO/IEC 15408 是一套国际标准，用于独立和客观地评估 IT 产品和系统地安全性措施。该认证是指经独立评估确认的安全性功能，符合多功能打印机的 IEEE 标准 2600.2™ 简介。

3. 安装产品时您应该做什么

产品的出厂默认安全设置可能没有针对您的安全环境进行优化。为了确保最佳安全性，请在安装过程中阅读以下内容，并根据您的使用环境进行必要的设置。

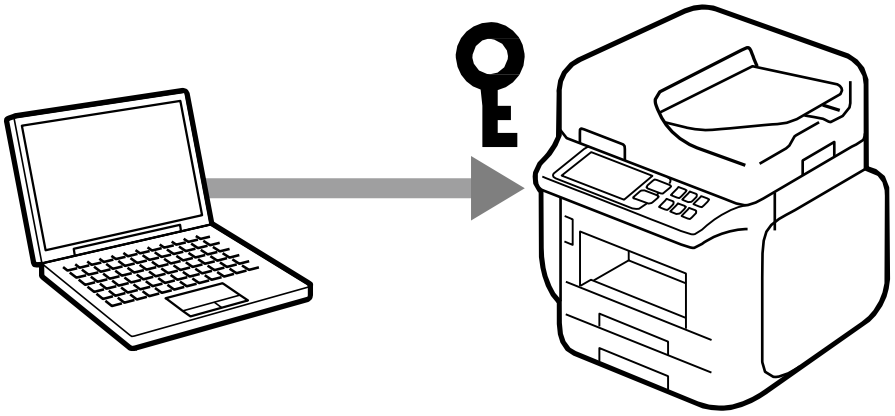
3-1. 管理员密码

我们强烈建议在安装每件产品时设置管理员密码。

如果未设置管理员密码或产品保留出厂默认设置，则存储在产品中的一般设置和网络设置可能被非法访问或更改。此外，个人和机密信息（如地址簿、ID 和密码）也有失去保护的风险。

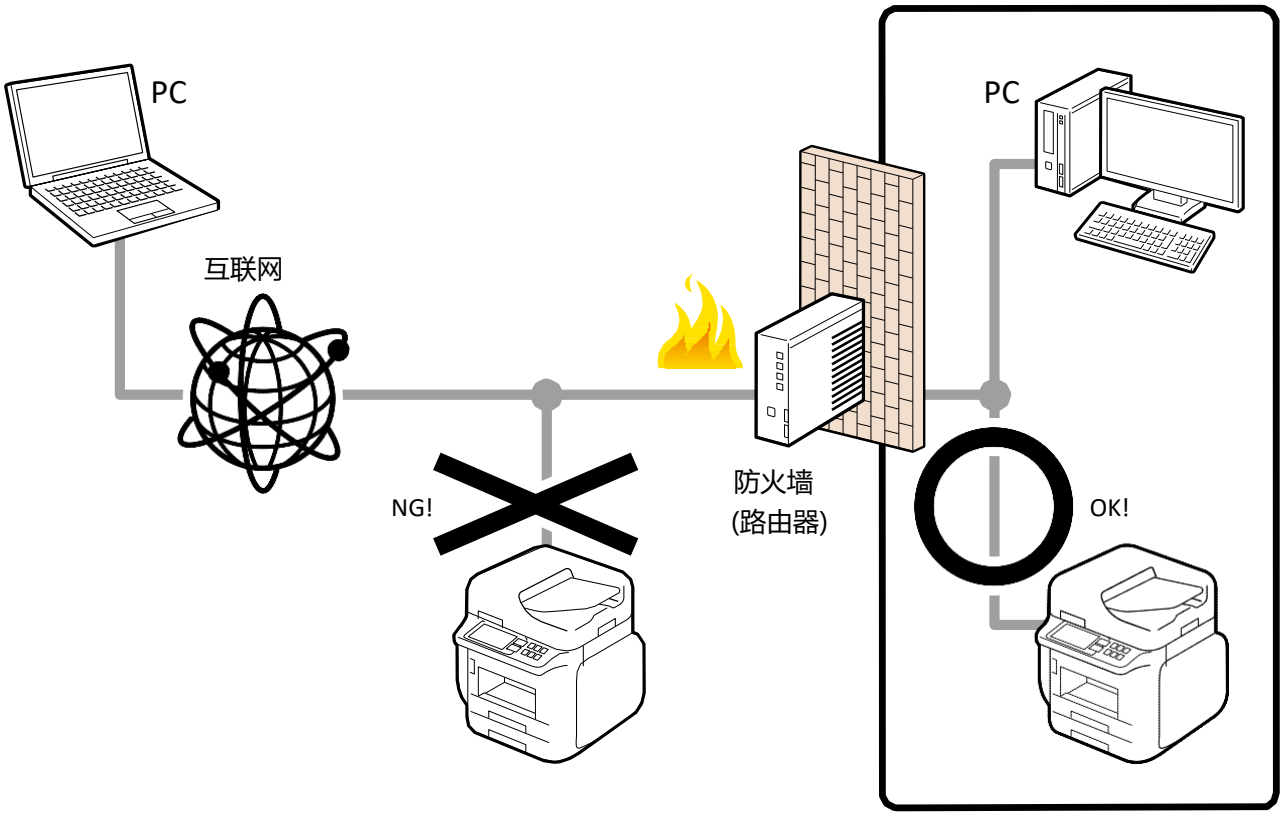
管理员密码应该是一串复杂的字符，不易被其他用户猜到。它应该由 8 个或 8 个以上的字符组成，不仅包括英文字母，还包括符号和数字。管理员密码可以直接在产品控制面板设置中设置，也可以通过网络设置。

为了提高安全性，一些型号在出厂时就设置了单独密码。



3-2. 互联网连接

将产品安装在受防火墙保护的网络上，不能直接连接到互联网。我们建议您在执行此操作时设置并使用私有 IP 地址。



管理界面，如 Web 管理屏幕，用于产品的网络功能和打印。爱普生实施漏洞测试并努力提供无漏洞的产品，但当爱普生设备直接连接到互联网时，您的网络将面临不可预见的安全风险，例如未经授权的使用和信息泄露。

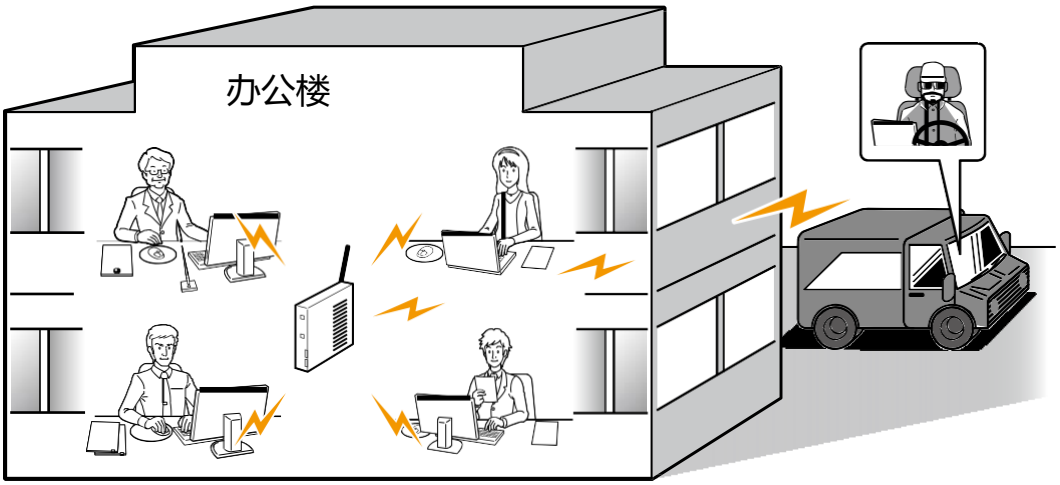
3-3. 无线局域网

使用无线局域网时，应适当设置无线局域网的安全性。

您也可以通过使用 WPS（Wi-Fi 保护设置）和 AOSS™ 设置无线局域网，轻松连接到使用高度安全和复杂密码短语和加密密钥的无线局域网环境。

无线局域网的优点是，只要在信号范围内，就可以通过网络自由连接到产品，与电脑和智能手机终端通信。另一方面，如果安全性设置不当，可能会因恶意第三方而出现以下问题。

- 个人信息，例如您的打印数据、扫描数据、ID 和密码，可能被其他人看到（拦截）
- 通信内容可能被欺骗性地改写（伪造）
- 某些人或设备可能被冒充并用于通信（身份盗窃）



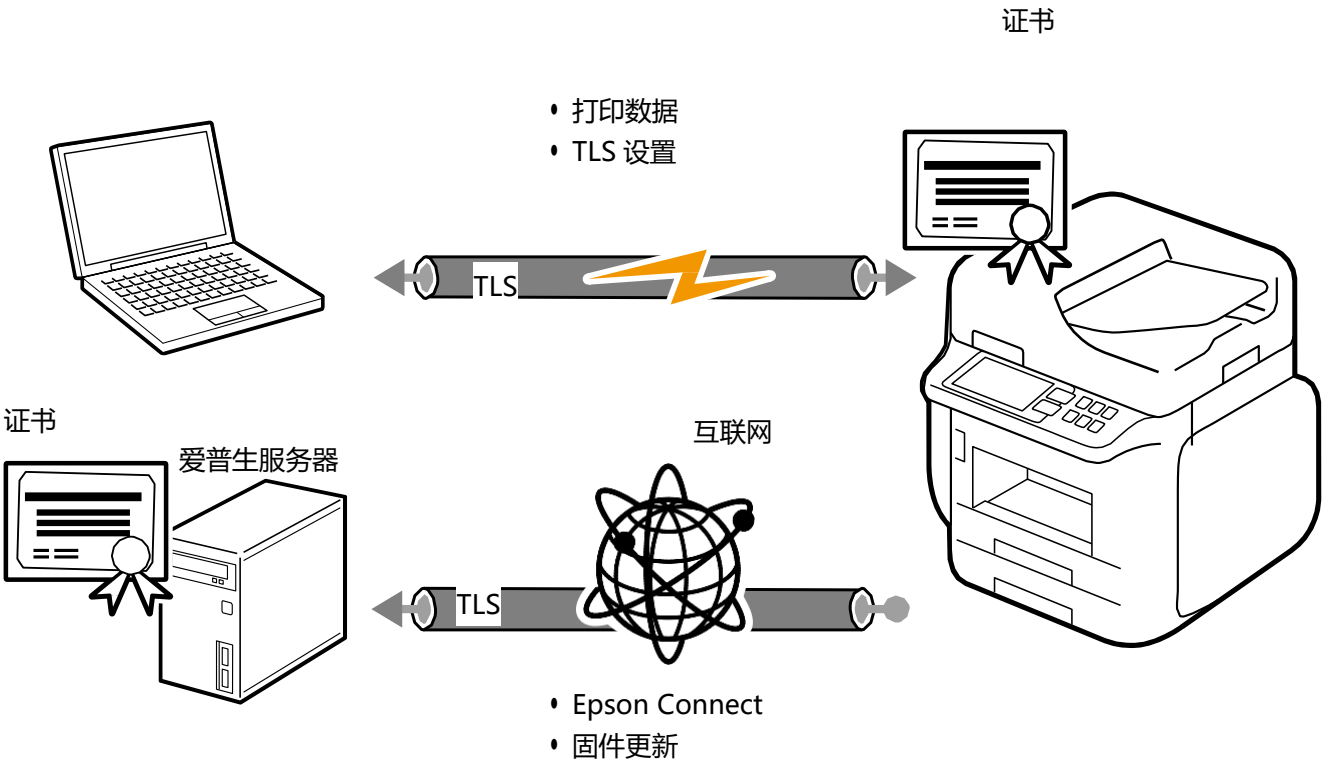
请参见产品手册，了解设置无线局域网的步骤。

4. 网络安全性

4-1. TLS 通信

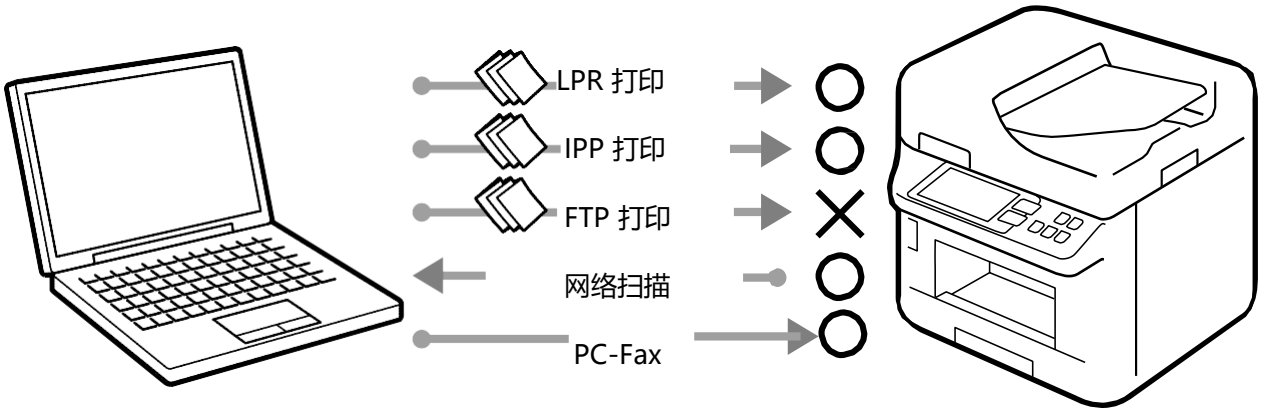
由于传输受 TLS 保护，您可以使用 IPPS 协议通过浏览器打印和配置您的产品，防止暴露设置信息和打印数据内容。您还可以使用服务器验证功能、导入 CA 签名的证书以及使用内部的公钥基础设施 (PKI) 来防止信息被发送到未授权的设备。加密强度可以配置为使用更安全的加密算法。当您通过用于 Epson Connect 和固件更新的产品在互联网上访问爱普生服务器时，还能受到 TLS 保护。

本产品支持 TLS 协议版本 TLS 1.1、TLS 1.2 和 TLS 1.3。请选择加密强度和所使用的 TLS 版本。



4-2. 控制协议权限和排除

本产品在打印、扫描和发送 PC-FAX 时通过各种协议进行通信。您可以通过为每个协议设置单独的权限和禁止条件来预防意外使用的安全性风险。



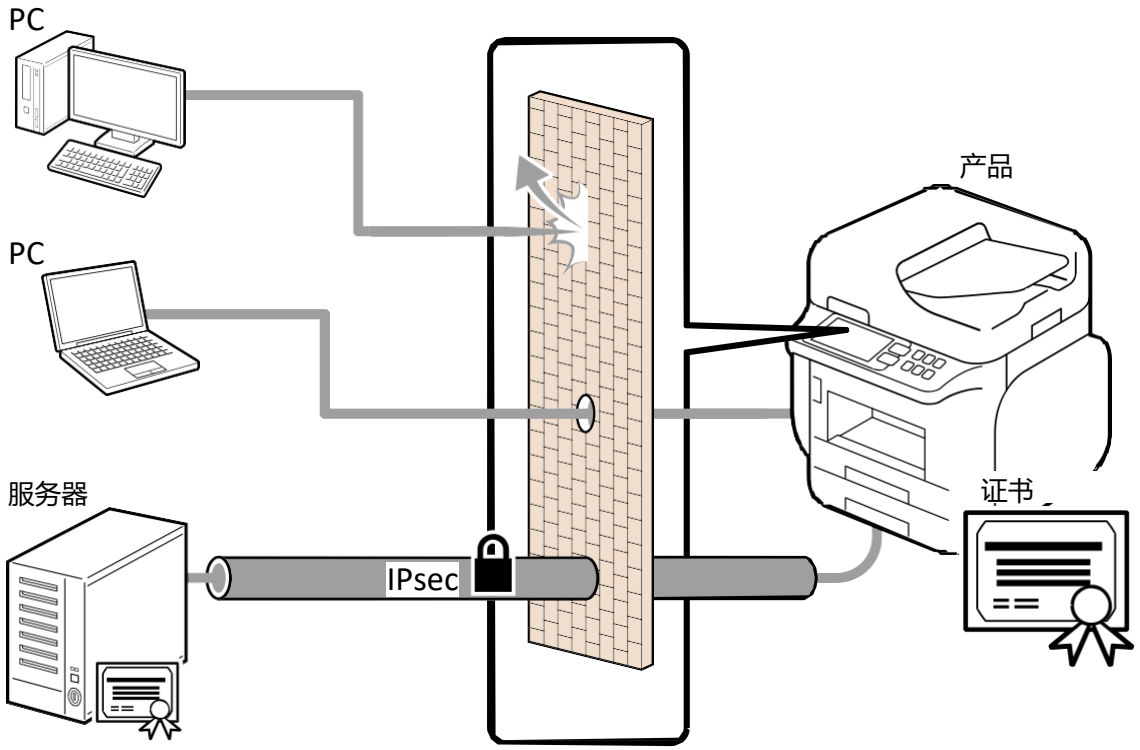
以下功能和协议的权限可以单独配置和设置：

- Bonjour
- SLP
- WSD
- LLTD
- LLMNR
- LPR
- RAW（Port9100/自定义端口）
- IPP/IPPS
- FTP
- SNMP
- SSL/TLS
- Microsoft 网络共享
- 网络扫描 (EPSON Scan)
- PC-FAX

4-3. IPsec/IP 过滤

通过 IPsec/IP 过滤功能，可以对 IP 地址、业务类型、接收和传输端口号等进行过滤。根据这些过滤器的组合，您可以设置是接受还是阻止来自特定客户端的数据，以及接受还是阻止特定类型的数据。同样，通过 IPsec 组合保护，您可以使用更强的安全性进行通信。

不安全的打印协议和扫描协议也成为被保护对象，因为 IPsec 保护中包含了 IP 数据包单元保护（加密和认证）。IPsec 身份验证方法支持预共享密钥和证书。



支持的算法和密钥交换方法如下：

密钥交换方法

- IKEv1
- IKEv2

ESP 加密算法

- AES-CBC-128
- AES-CBC-192
- AES-CBC-256
- AES-GCM-128
- AES-GCM-192

- AES-GCM-256
- 3DES

ESP/AH 身份验证算法

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

该基本政策影响访问产品的所有用户。设置单独政策以根据您的需求控制访问。

4-4. IEEE802.1X 身份验证

IEEE802.1X 是控制网络设备各端口访问的标准。IEEE802.1X 网络由具有身份验证功能的 RADIUS 服务器（身份验证服务器）和交换集线器组成。

爱普生产品符合 IEEE802.1x 标准，可以连接到包含一些机密信息的网络环境。

支持以下身份验证方式和加密算法：

身份验证方法

- EAP-TLS
- PEAP-TLS
- PEAP/MSCHAPv2
- EAP-TTLS

加密算法

- AES128
- AES256
- 3DES
- RC4

4-5. SNMPv3

通过使用 SNMPv3 协议，可以对设备管理工具中用于设备设置更改和状态监控的 SNMP 通信（数据包）进行身份验证和加密，以确保数据在网络中传输时的保密性和安全性。

4-6. WPA3

该产品支持最新的 Wi-Fi（无线局域网）身份验证和加密技术 WPA3。WPA3 提供了更鲁棒和更强大的保护，可保护您通过无线网络传输的数据。

4-7. 接口间的分离

本产品包括 USB 接口、标准有线局域网接口、附加有线局域网接口、Wi-Fi 接口和传真接口。每个接口都是独立的，不包括任何直接传输或路由功能。因此，接口隔离将防止入侵者通过单个接口破坏整个系统，从而消除某些类型的安全性漏洞风险。例如，通过本产品从公共电话线入侵网络；从无线局域网接入有线局域网；或未经授权从互联网访问通过 USB 连接到电脑的产品。

5. 保护您的产品

5-1. 阻止电脑端 USB 连接

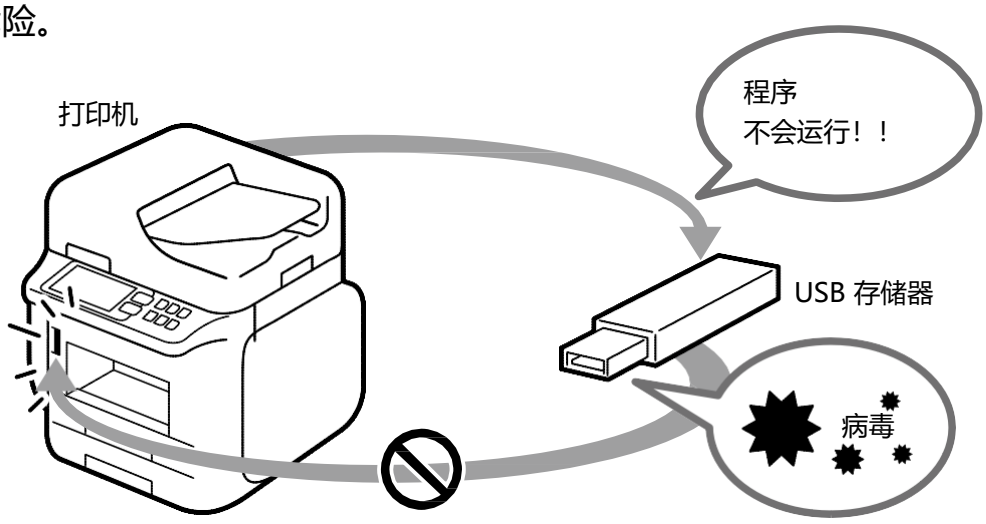
如果您希望禁止在不使用网络的情况下从计算机直接打印和扫描产品，可以禁止通过 USB 连接从电脑访问产品。

5-2. 禁用外部接口

您可以禁用存储卡和 USB 存储器接口。这样您就可以防止通过未经授权扫描办公室机密文档来非法复制数据。

5-3. 处理 USB 存储器引入的病毒

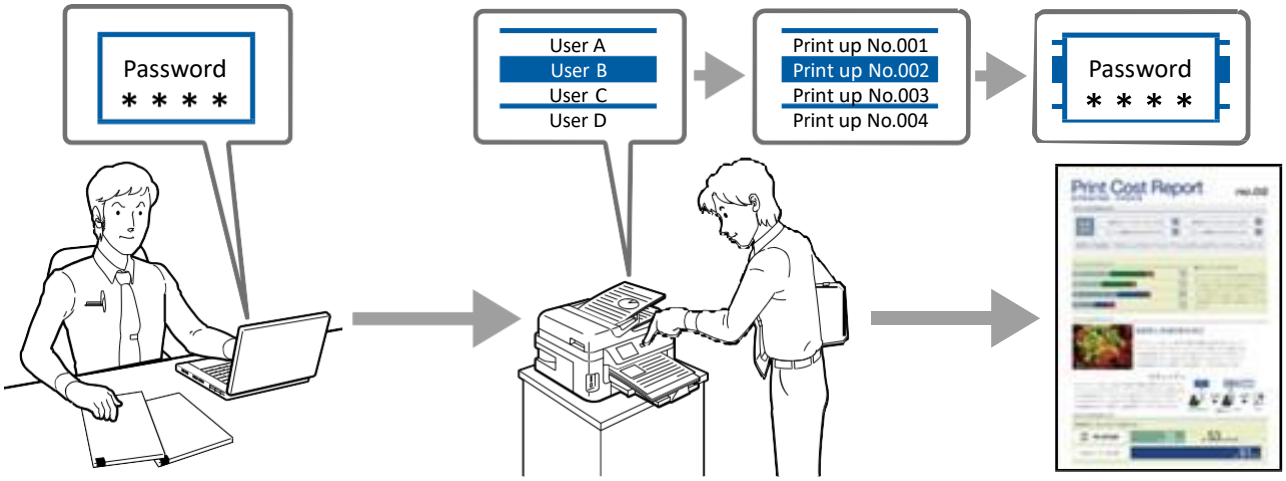
由于爱普生产品的 USB 存储器上没有可执行的功能，因此产品没有通过 USB 存储器感染病毒的危险。



6. 打印/扫描安全性

6-1. 机密作业

通过将文档提交为“机密作业”，可以确保文档的隐私/机密性，并防止未经授权的人在设备上查看无人值守输出。



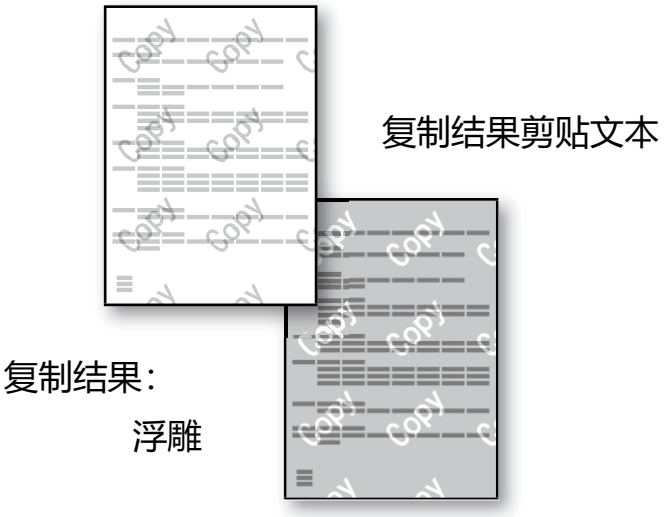
输入密码以进行打印。

在本产品上选择打印作业并输入密码。

打印完成。

6-2. 防拷贝图案

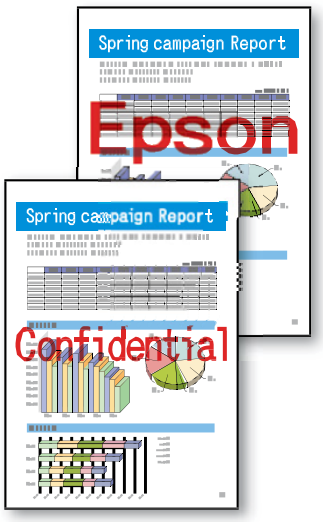
您可以使用防拷贝水印来保护文档的原创性，它会在原始输出上创建透明的水印图案。当原始输出用于复制时，透明水印将变得可见。



6-3. 水印

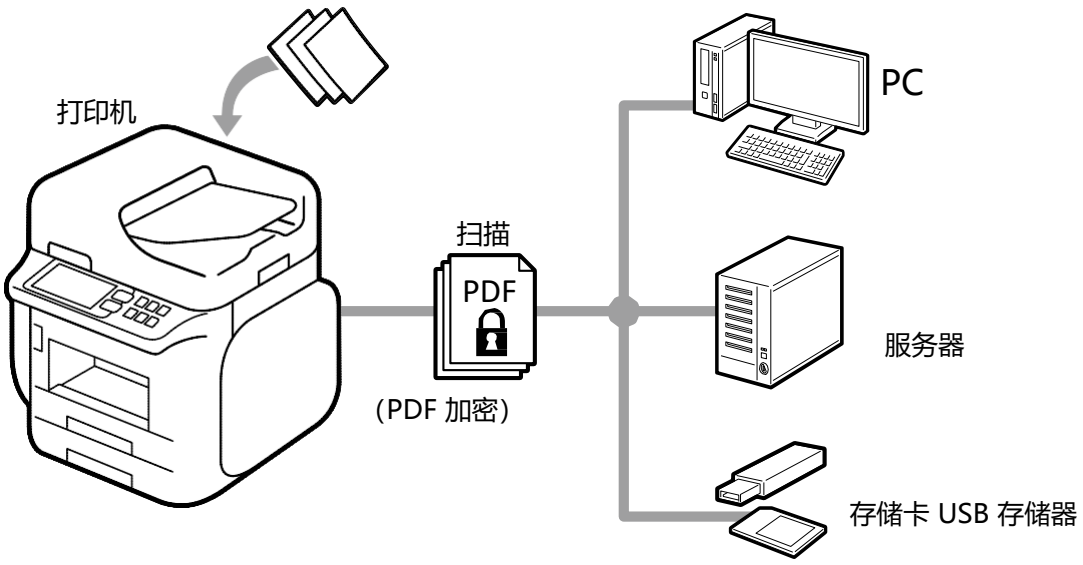
可以在文档上叠加“分类”和“重要”（文本或 BMP 格式）等水印。此外，您还可以选择“用户名称”或“电脑名称”。

提醒收件人小心处理文档，可防止未经授权的使用。



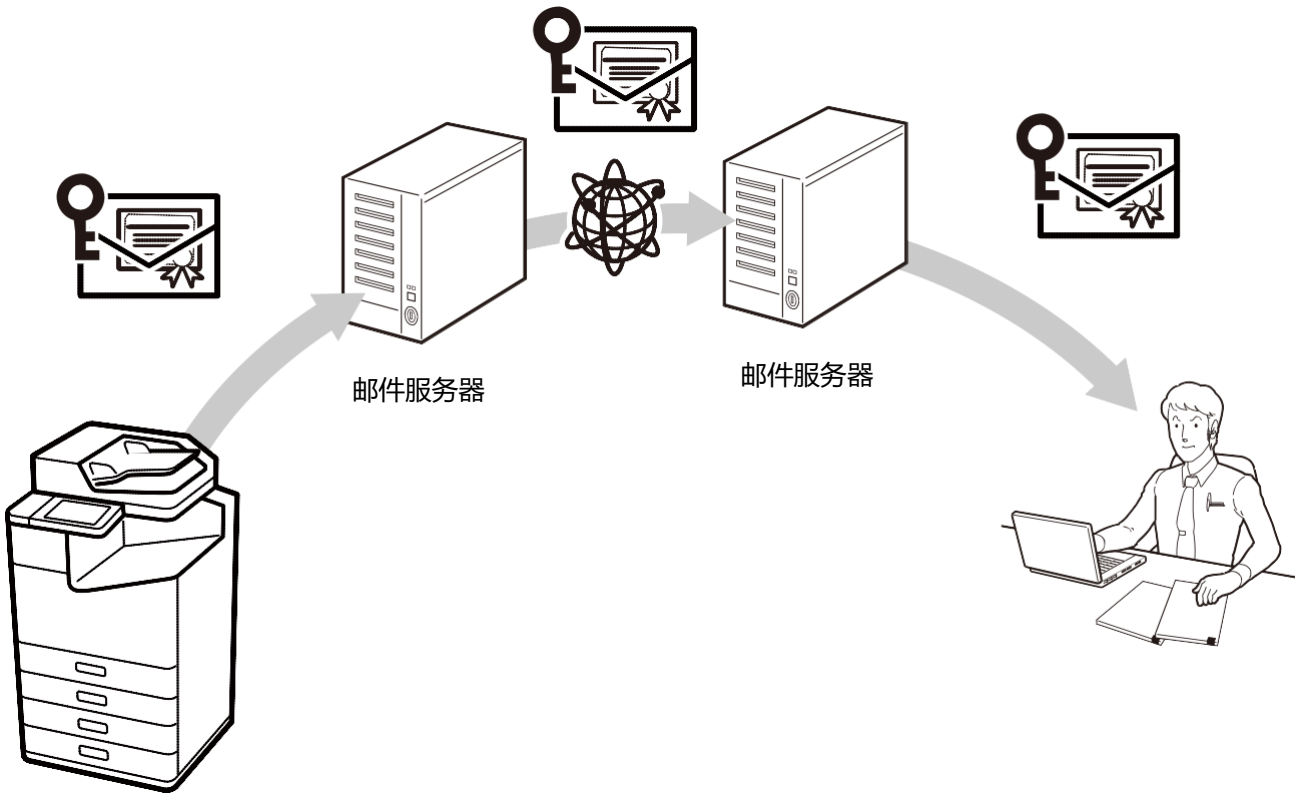
6-4. PDF 加密

您可以将文档扫描到有密码保护的 PDF 文件中。这可以防止第三方未经授权查看文档。



6-5. S/MIME

使用 S/MIME 允许您为“扫描至电子邮件”和“传真至电子邮件”添加数字签名和/或加密电子邮件。即使电子邮件经过多个电子邮件服务器，也可以保护电子邮件不被伪造、拦截或篡改。S/MINE 将在保护数据安全性和耐受不可否认性的同时，保障消息的真实性和完整性。



支持的算法如下。

加密算法

- AES-128
- AES-192
- AES-256
- 3DES

数字签名哈希算法

- SHA-1
- SHA-256
- SHA-384
- SHA-512
- MD5

6-6. 域名限制

通过对邮件地址的域名设置限制规则，可以降低扫描至邮件和传真转发电子邮件功能的错误传输和信息泄露风险。

6-7. 扫描至网络文件夹/FTP、扫描至电子邮件和电子邮件通知的授权密码

建议设置较长的密码来提高密码安全性。您现在可以设置最多 70 个字符作为授权密码，用于扫描至网络文件夹/FTP、扫描至电子邮件、电子邮件通知。这允许您为正在运行的文件服务器和电子邮件服务器设置较长的密码。

6-8. 默认禁用 PDL 文件访问

通过禁用来自 PDL（页面描述语言）的文件访问，可以防止恶意打印数据从打印机内部窃取文件，导致信息泄漏风险。　即使传输恶意打印数据，本产品也可以安全地使用，不会读取文件。

6-9. 安全打印

如果您希望保护打印传输路径的安全性，可以使用通过 TLS 加密的 IPPS。

7. 传真安全性

7-1. 直拨限制

如果您想直接使用数字键盘输入传真号码，可以设置为在两次正确输入目的地后才发送传真。您还可以设置为禁止直接使用数字键盘输入电话号码

传真只通过单键拨号发送到您地址簿中登记的地址。这可以减少由于电话号码输入错误造成错误传输并导致信息泄漏的风险。

7-2. 确认地址清单

您可以在发送传真前确认所选地址。这可以减少指定地址出错造成错误传输并导致信息泄露的风险。

7-3. 拨号音检测

确认检测到拨号音后再发送传真，可以防止错误传输。

根据您的国家或地区，可能无法检测拨号音。

7-4. 防止废弃传真的措施

可以设置“查看后打印传真”，将收到的传真保存到收件箱（存储器接收），并在控制面板上确认后打印。这可以防止信息泄露，以及由于打印的传真无人看管而丢失接收传真中的打印材料。

此外，通过设置需要密码才能访问收件箱，可以防止未经授权的用户任意打印和删除邮件。

7-5. 传输确认报告

您可以通过打印报告确认传输详细信息，例如发送结果报告、转发结果报告、发送管理报告等等，确认传真是否已明确发送到正确的地址。

7-6. 删除已接收传真的备份数据

接收传真的备份数据*可以从控制面板中删除。您还可以设置为自动删除备份数据，以防止接收到的传真数据被未经授权地重印。

*接收传真的备份数据保存在产品中（出厂默认设置），以便在打印结果不清楚或打印结果丢失的情况下重印传真。

7-7. 限制发送至多个收件人

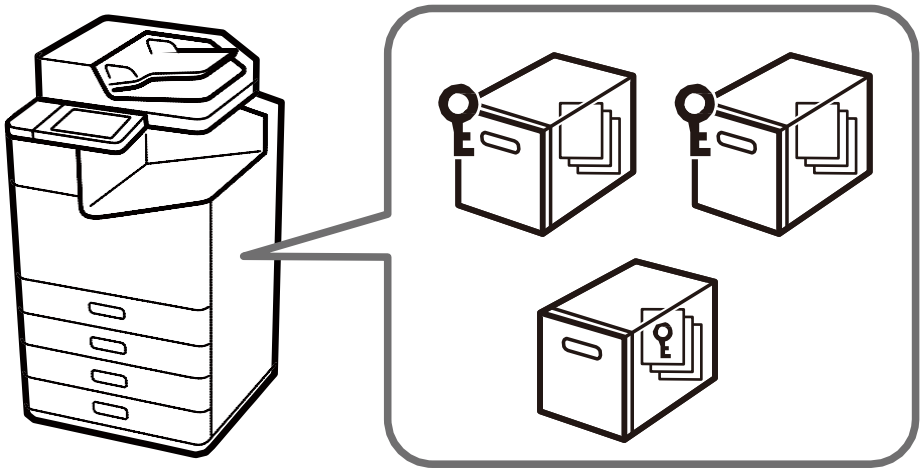
您可以将产品设置为只能选择 1 个收件人。

限制指定多个收件人可以降低向非预期收件人发送传真并泄露信息的风险。

8. 用户数据保护

8-1. 墨仓安全性

您可以为配备墨仓的型号上的共享墨仓和文档设置唯一的密码。这些密码可以防止信息泄露、丢失和未经授权的篡改。此外，墨仓操作还可以接受访问控制。如果无需使用共享墨仓，也可以禁止使用共享墨仓功能。



8-2. 保护您的地址簿

当批量编辑产品的地址簿时，您可以通过要求管理员密码（当已设置管理员密码时）来防止地址信息泄露和未经授权的操作。此外，由于地址簿可以导出为加密文件，因此在更换或备份产品时，可以防止泄露个人信息，例如传真号码和电子邮件地址。

8-3. 产品数据处理

打印、复制和扫描功能的数据暂时保存在产品中，当任务完成或产品关闭时，这些数据将被清除。

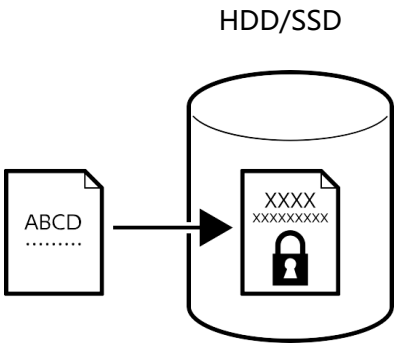
发送或接收传真时，清空传真数据。接收的传真可以通过备份功能保存，也可以通过设置更改自动删除（参考 7-6）。

8-4. 加密 HDD/SSD 中已保存的数据

在将数据保存到产品的内部 HDD/SSD 时，我们始终使用加密保护客户数据。

如果 HDD/SSD 被盗，数据加密可以防止个人数据被非法访问或恶意攻击。

HDD/SSD 附带自加密驱动器，文档数据采用 AES-256 加密。



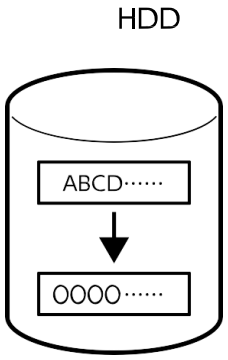
8-5. 作业数据的顺序删除

启用后，硬盘中已删除的数据将按以下方式覆盖，以防止恢复。有以下几种选项：

(1) 快速删除：修改加密密钥，防止恢复已删除的数据。

(2) 安全顺序删除：修改加密密钥，并将硬盘上已删除的数据覆盖为“0”，进一步确保已删除的数据无法恢复。

关于作业数据删除的详细说明，请参考产品的用户手册。



8-6. 密码加密

您可以加密存储在产品中的密码。加密后的信息如下：

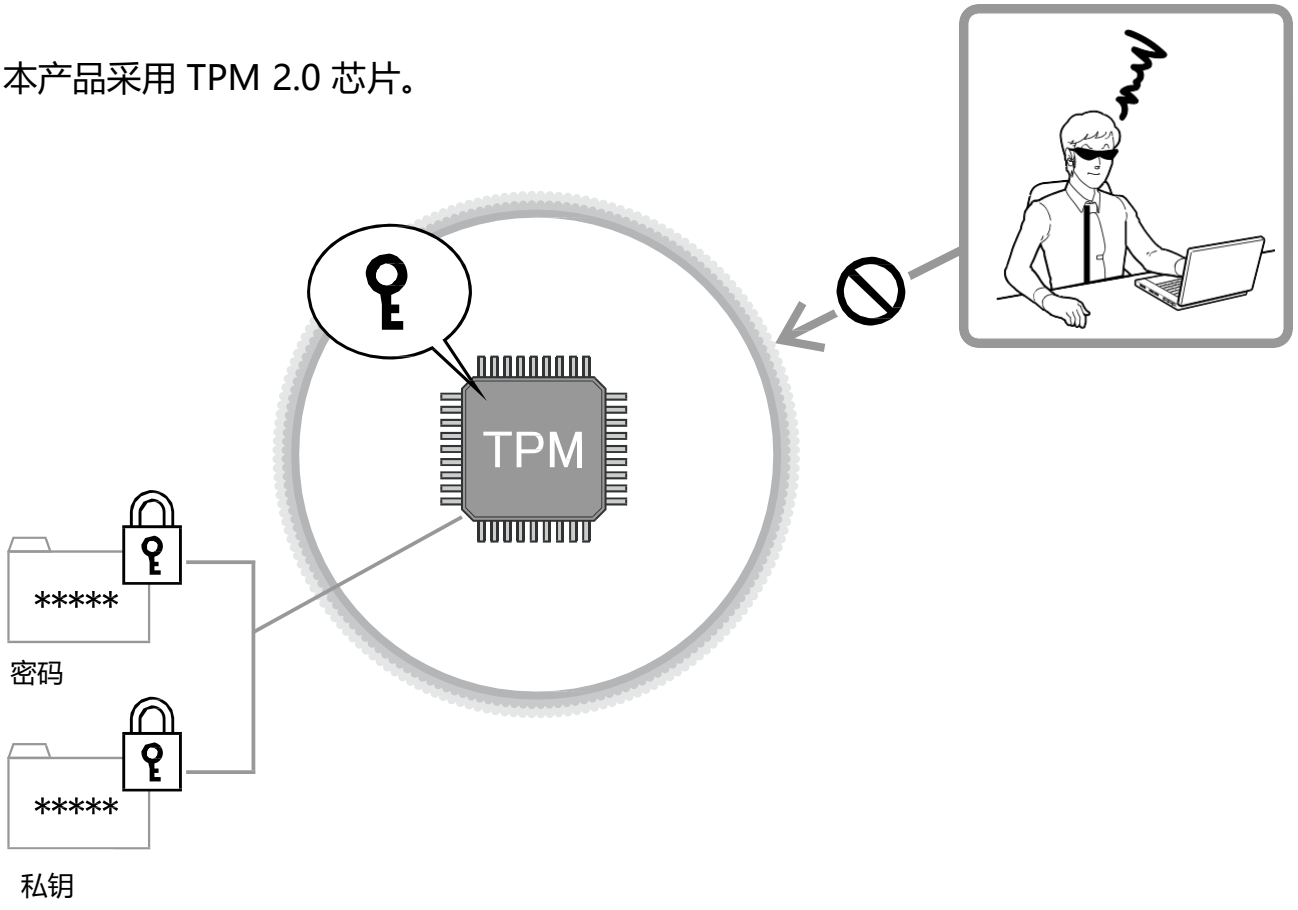
- 管理员密码
- 用于访问控制的用户密码
- 硬盘身份认证密钥、证书私钥等。 “扫描至网络文件夹/FTP”的访问密码。

8-7. TPM

在采用 TPM（可信平台模块）的模型中，安全级别提升如下：

- 用于恢复加密后的密码和私钥信息的加密密钥存储在 TPM 芯片上。
- TPM 芯片可以在硬件层面防止未经授权的分析，因为 TPM 芯片不能从产品外部访问。
- TPM 的真随机数被用作与浏览器通信的会话密钥 (Web Config)。
- TPM 的真随机数用于为加密的 HDD/SSD 生成身份验证密钥。

本产品采用 TPM 2.0 芯片。



8-8. 硬盘镜像

安装额外的硬盘选项后，即使一个硬盘发生故障，也不会丢失存储的数据，并且可以通过使用另一个硬盘继续执行所有功能。

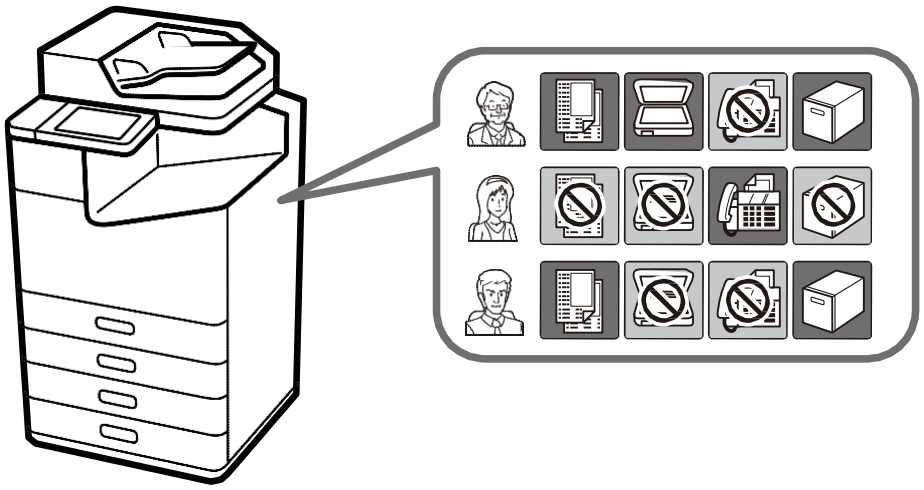
9. 操作限制

9-1. 面板锁

使用面板锁时，必须输入管理员密码才能进入控制面板。在开放式办公室、公共设施级类似场所，通过管理员密码保护面板时，可以防止用户更改设置。

9-2. 访问控制

您可以根据不同的角色和工作职能，限制单个用户使用打印、扫描、复制、传真* 和墨仓功能，以降低安全风险。此外，用户在控制面板中处于非活动状态达指定的时间后，用户将自动注销。



* 只能限制传真传输。

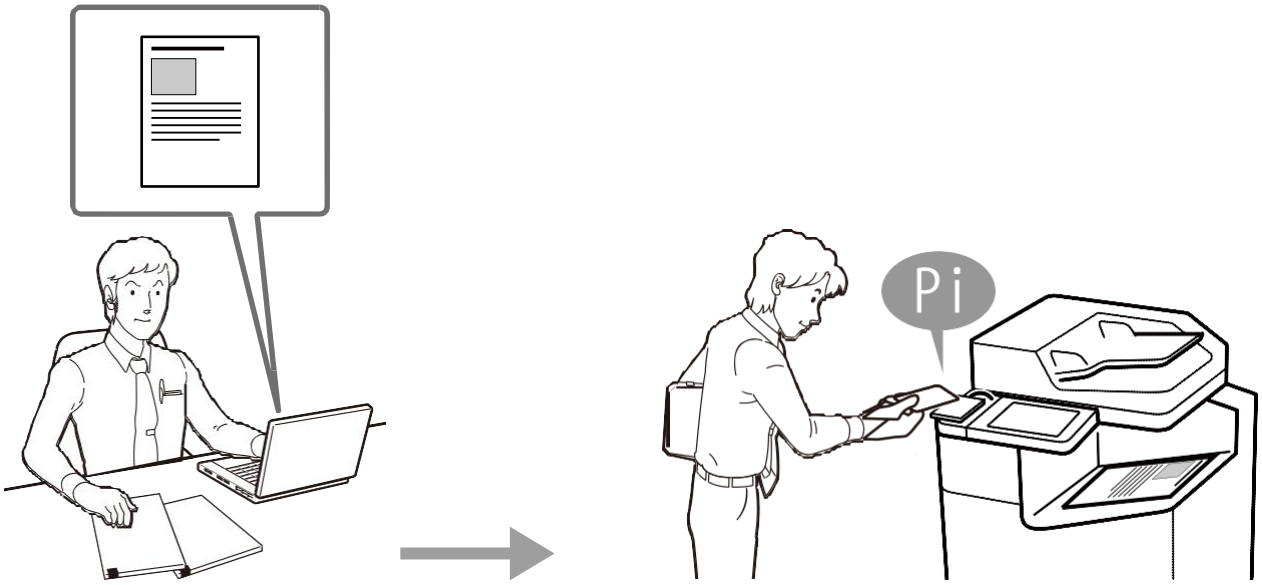
9-3. 经过身份验证的打印/扫描

当使用可选的“Epson Print Admin / Epson Print Admin Serverless”时，您可以在发布提交的文档进行打印之前要求在注册设备上进行身份验证。这可以防止非预期个体从设备输出托盘获取敏感和无人值守的文档。

有多种身份验证选项，包括使用 PIN 码、用户名和密码对、ID 卡读卡器，所有这些都可以与 LDAP 服务器集成。

通过独立扫描仪，您可以使用 Document Capture Pro Server Authentication Edition 或独立身份验证。

有多种身份验证选项，包括使用 PIN 码、用户名和密码对、ID 卡读卡器，所有这些都可以与 LDAP 服务器集成。



9-4. 密码政策

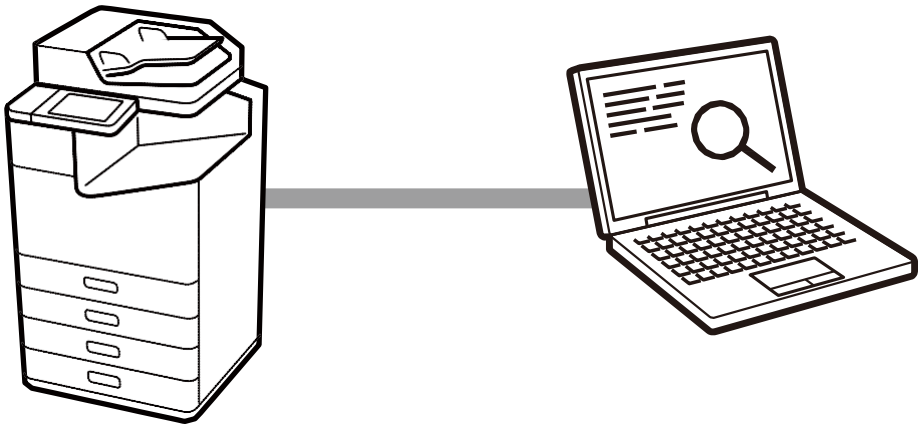
密码策略可应用于管理员密码、访问控制、传真密码。强密码需要满足以下多个条件，才能防止密码被恶意攻击者破解。

- 密码的最小字符数
- 密码中包含/不包含大写英文字母
- 密码中包含/不包含小写英文字母
- 密码中包含/不包含数字
- 密码中包含/不包含符号

9-5. 审计日志

审计日志功能可以记录打印、复制、扫描、传真、设置变更等的历史，供审计使用。定期确认该日志有助于早期发现错误使用和安全性问题征兆。

最多保留 20,000 条审计日志。



10.产品安全性

10-1.自动固件更新

如果启用自动固件更新，固件可以在指定的时间自动更新。更新在指定时间进行，因此您可以一直使用最新固件而不会中断任何操作。

10-2.防止非法固件更新

在固件更新期间使用管理员密码进行身份验证，并且在重写固件之前通过签名验证发送到产品本身的固件是否合法。此外，与产品的通信受 HTTPS 保护。这可以防止恶意第三方对固件进行未经授权的修改。

10-3.安全启动

启动时，系统通过签名验证产品固件是否合法。如果检测到固件已被重写并且是未经授权的固件，系统将停止启动并提示用户更新固件。

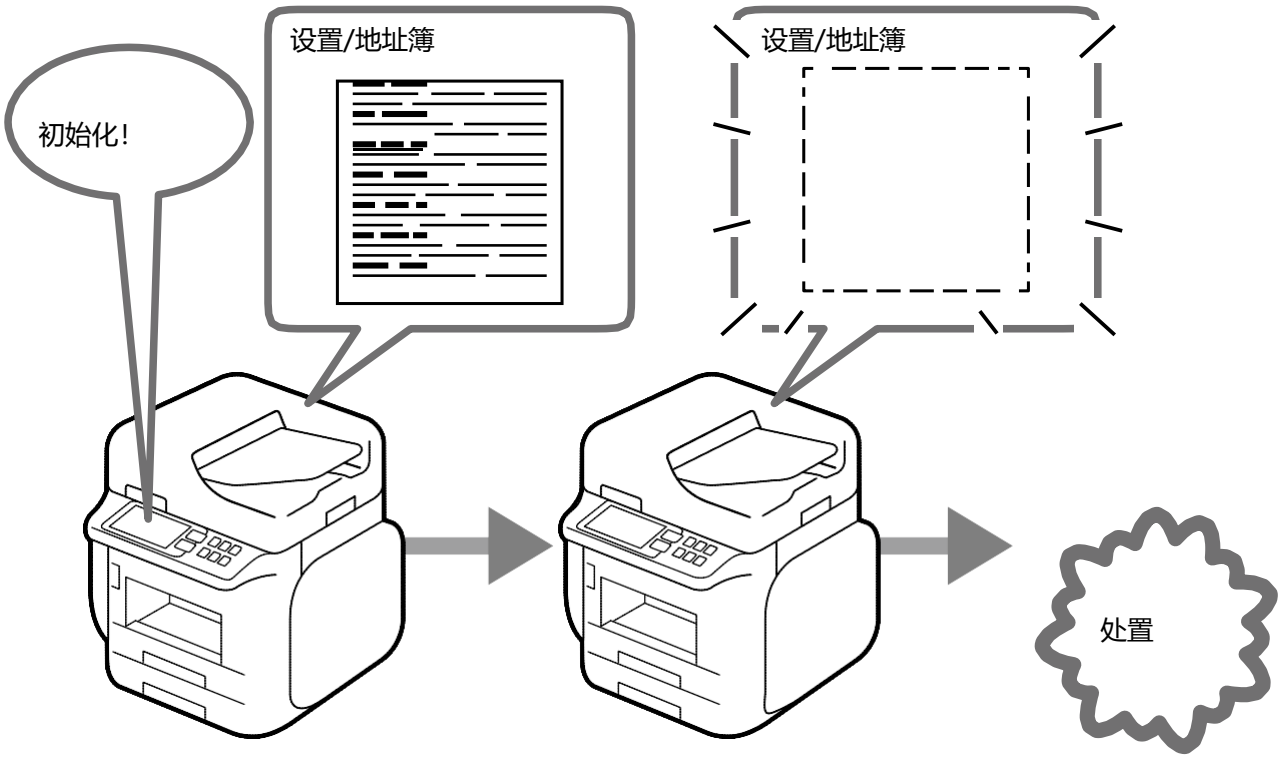
10-4.恶意软件渗透检测

在产品运行时，不断监控该产品是否有恶意软件渗透到固件中。如果检测到恶意软件，则重新启动产品以删除恶意软件。

11.处置产品时的安全性措施

11-1.恢复出厂默认值

在转移或处置产品时，可以将所有设置（包括内部 HDD/SSD 中的设置）恢复到出厂默认值（初始化），以防止机密信息泄露。



12.安全性认证和标准

12-1. ISO15408/IEEE2600.2™

该产品已通过 ISO/IEC 15408 认证，符合信息安全国际标准 IEEE 标准 2600.2™-2009*。

IEEE Std. 2600.2™

IEEE Std.2600.2™ 是一个国际标准，规定了 MFP 的信息安全标准。通过提供符合标准的安全功能，如用户识别和身份验证、访问控制、数据覆盖、网络保护、安全管理、自检和审计日志等，可以全面增强 MFP 的安全性。

ISO/IEC 15408

ISO/IEC 15408 也称为通用标准 (CC)，是一种国际标准，旨在独立和客观地评估 IT 产品和系统安全措施，以确定这些措施是否设计和实施得当。

指定版本的固件、手册和其他组件接受 ISO/IEC 15408 认证评估。已购买产品中的固件版本可能与认证版本不同。

使用认证版本时，产品功能可能会有一些限制。

CCRA 认证标志表示该产品根据日本信息技术安全评估和认证计划 (JISEC) 进行了评估和认证。

但并不保证产品完全没有漏洞。
也并不意味着产品在每个操作环境下都配备了所有必要的安全性功能。

* 美国政府批准的保护配置文件 - 美国政府对硬拷贝设备的保护配置文件 1.0 版 (IEEE 标准 2600.2™-2009)

EPSON

注意

- 禁止复制本文档的部分或全部内容。
- 本文档内容如有变更，恕不另行通知。
- 本文档仅供参考。关于使用的详细信息，请参见各产品的手册。

商标

- EPSON 和 EXCEED YOUR VISION 是精工爱普生株式会社的注册商标。
- Microsoft® 是微软公司的注册商标。
- AOSS™ 是 Buffalo Inc. 的商标。
- WPS 和 Wi-Fi Alliance 是商标或注册商标。
- 其他产品名称为各自公司的商标或注册商标。

NPD6296-02 EN