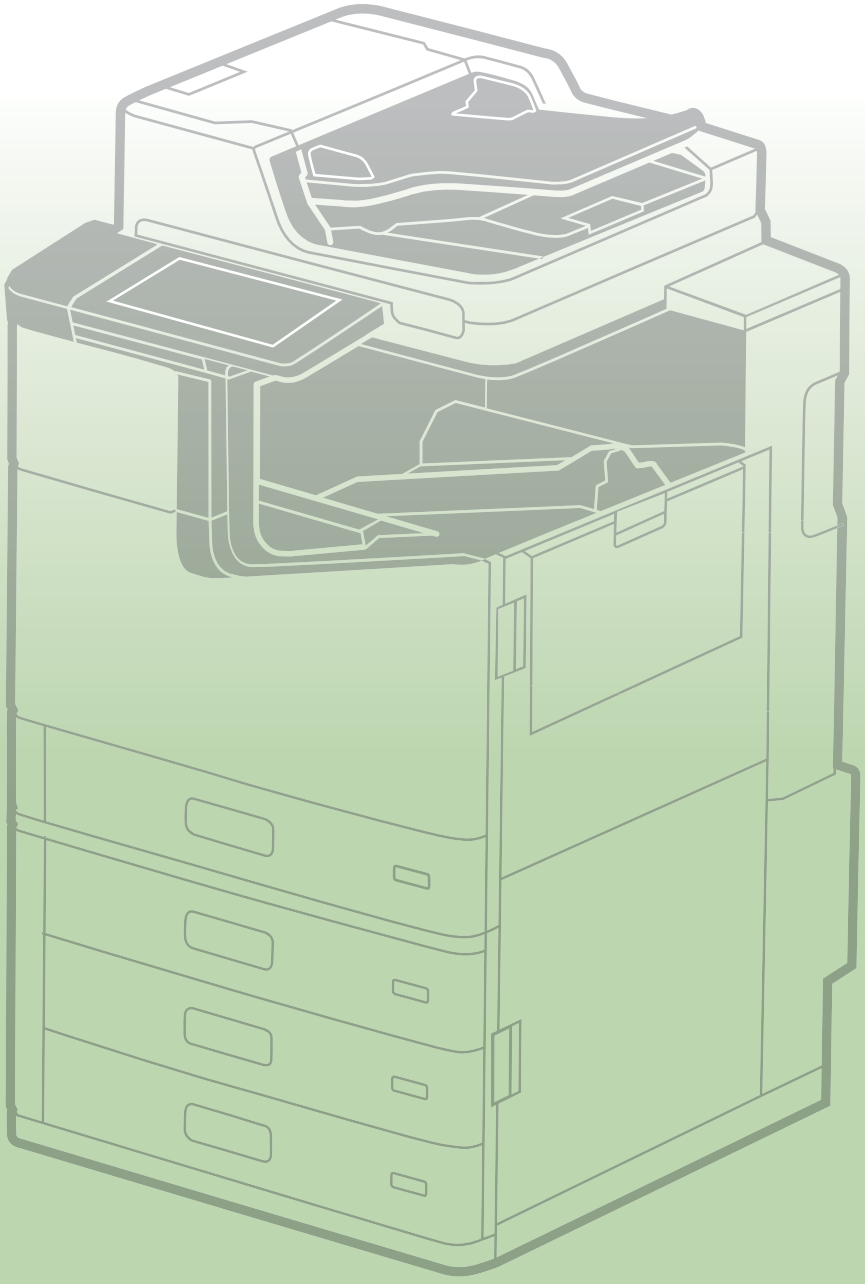
EPSON

Sicherheitshandbuch



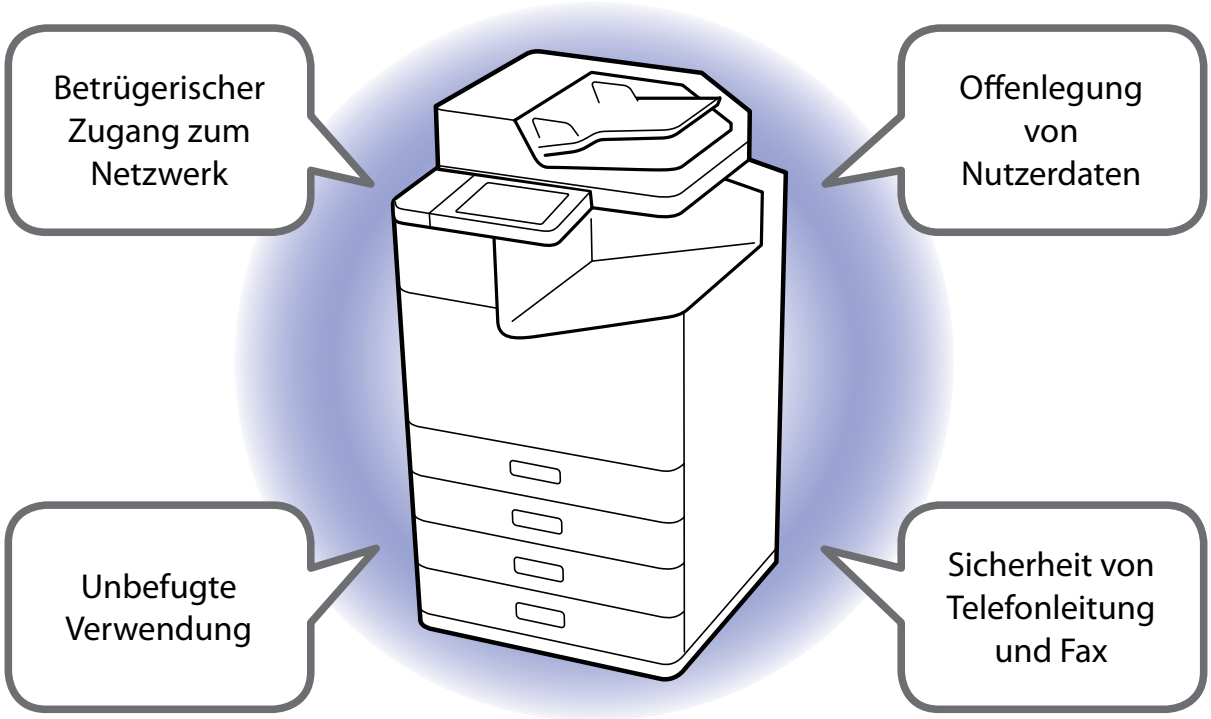
Inhaltsverzeichnis

1. Einführung

Epson hat die Netzwerkkompatibilität seiner Produkt, um den Kundenkomfort zu erhöhen.

Die zunehmende Raffinesse und Komplexität von Cyberangriffen durch böswillige Dritte stellt eine neue Bedrohung für Netzwerkgeräte dar und hat die Sicherheitsbedenken weiter verstärkt.

Die Produkte von Epson sind mit vielen Merkmalen und Funktionen ausgestattet.
Bei der Verwendung von Computern und Servern sind jedoch eine Reihe von Sicherheitsaspekten zu berücksichtigen, insbesondere bei der Verbindung mit einem Netzwerk und der Nutzung des Netzwerks.



Dieses Handbuch ist eine Einführung in das Sicherheitskonzept von Epson und ein Ratgeber für die Kunden. Es führt Sie durch die verfügbaren Sicherheitsfunktionen.

Die Symbole neben der Funktion im Text haben die folgenden Bedeutungen.

: Sicherheitsfunktionen mit dieser Kennzeichnung sind die minimalen Einstellungen, die vom Administrator eingerichtet werden müssen.

: Sicherheitsfunktionen mit dieser Kennzeichnung dürfen nur vom Administrator konfiguriert werden und stehen den Benutzer in der konfigurierten Sicherheitsumgebung zur Verfügung.

: Sicherheitsfunktionen mit dieser Kennzeichnung können von Administratoren und Benutzern eingerichtet werden.

: Andere Sicherheitsfunktionen. Das sind Sicherheitsmerkmale, die Teil der Spezifikationen und in die Produkte integriert sind.

Lesen Sie in Ihrem Produkthandbuch, wie die Sicherheit eingerichtet wird.

Beachten Sie, dass die Sicherheitsfunktionen und die Einhaltung der in diesem Handbuch beschriebenen Standards je nach Produkt variieren. Bestimmte Produkte haben diese Funktionen möglicherweise nicht oder erfüllen diese Sicherheitsstandards nicht. Achten Sie deshalb auf die Funktionen, die im Sicherheitshandbuch aufgeführt sind und die Kompatibilität der einzelnen Produkte.

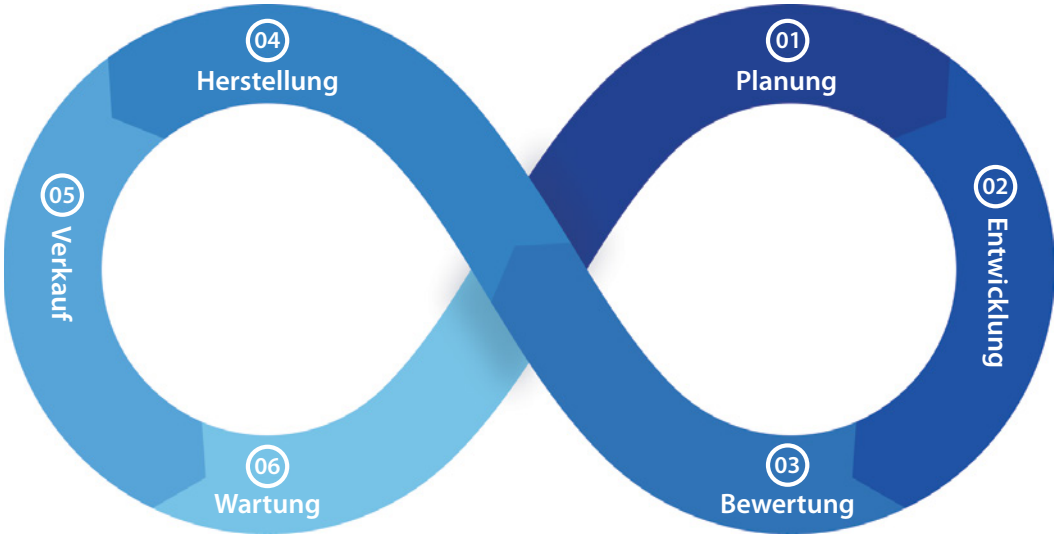
2. Grundlegende Sicherheitsrichtlinie von EPSON

Das Herangehen von Epson in Sicherheitsfragen stellt sicher, dass unsere Kunden unsere Produkte sicher und leicht nutzen können.

2-1. Grundlegende Richtlinie

Epson betrachtet die Produktsicherheit als Eckpfeiler der Produktqualität.

Wir praktizieren Produktsicherheit (Endpunkt) im gesamten Produktlebenszyklus, von der Planung und Entwicklung bis zu Bewertung, Herstellung, Verkauf und Wartung und wir überprüfen die Sicherheit der unterschiedlichen Nutzungsumgebungen unserer Produktreihen, damit die Kunden die Produkte unter sicheren Bedingungen verwenden können.



① Planung
In der Produktplanungsphase überwachen wir kontinuierlich die neuesten Sicherheitstrends und potenzielle Sicherheitsrisiken. Wir hören auch auf die Anfragen der Kunden, wenn wir die sicherheitsrelevanten Anforderungen identifizieren und analysieren. Dadurch können wir potenzielle Probleme bei unseren Produkten beseitigen, bevor sich die Risiken materialisieren.

② Entwicklung
Mit den ausgereiften Plattformen und Technologien, die wir für ein breites Spektrums an Produkten, von Büro- und Heimdruckern bis zu gewerblichen und industriellen Druckern für kleine und große Formate, entwickelt haben, sind wir bestrebt, den Schutz vor Sicherheitsrisiken zu verbessern.

③ Bewertung
Zusätzlich zu den umfassenden internen Prüfungen ziehen wir auch externe Organisationen zur objektiven Sicherheitsbewertung hinzu. Wir führen mit unserem strengen Sicherheitsprüfungssystem Bewertungen aus verschiedenen Perspektiven durch, um die hohe Sicherheit unserer Produkte sicherzustellen.

④ Herstellung
Zur Gewährleistung der hohen Qualität unserer Herstellungsprozesse haben wir in unseren Werken ein umfassendes Informations-Asset-Management implementiert und wir installieren Software, die Funktionalität unserer Produkte ermöglicht.

⑤ Verkauf
Wir unterstützen unsere Kunden beim Planen und Implementieren von Lösungen, die Sicherheitsrisiken in ihren spezifischen Nutzungs- Betriebsumgebungen verringern.
Wir sorgen auch dafür, dass mögliche Sicherheitsrisiken nach der Installation unserer Produkte schnell beseitigt werden.
Wenn Produkte ersetzt oder entsorgt werden müssen, setzen wir die Geräte aus Werkseinstellungen zurück, damit wertvolle vertrauliche Informationen nicht verloren gehen.

⑥ Wartung
Wir reagieren schnell auf sicherheitsrelevante Probleme und Bedenken, die von den Kunden gemeldet werden.

2-2. Informationen

Wir informieren unsere Kunden umfassend und machen sie bewusst auf Sicherheitsfragen aufmerksam.

2-3. Unterstützung bei Sicherheitsrisiken

Wir beseitigen kontinuierlich Sicherheitslücken und Risiken.

- Wir prüfen unsere Produkte mit den branchenüblichen Tools auf Sicherheitslücken, damit alle unsere Produkte frei von Risiken sind.
- Wir verfolgen regelmäßig die Informationen zu Sicherheitsrisiken der Open Source Software, die wir in der Firmware unserer Produkte verwenden.
- Wenn neue Sicherheitsrisiken entdeckt werden, analysieren wir sie und stellen Informationen und Gegenmaßnahmen zur Verfügung.

2-4. Einhaltung von Codes und Standards

Wir sind bestrebt, die Sicherheitsstandards einzuhalten und zu erreichen.

3. Vorgehensweise bei der Installation des Produkts

Lesen Sie bei der Installation die folgenden Hinweise und konfigurieren Sie die Einstellungen gemäß Ihrer Nutzerumgebung, um für optimale Sicherheit zu sorgen.

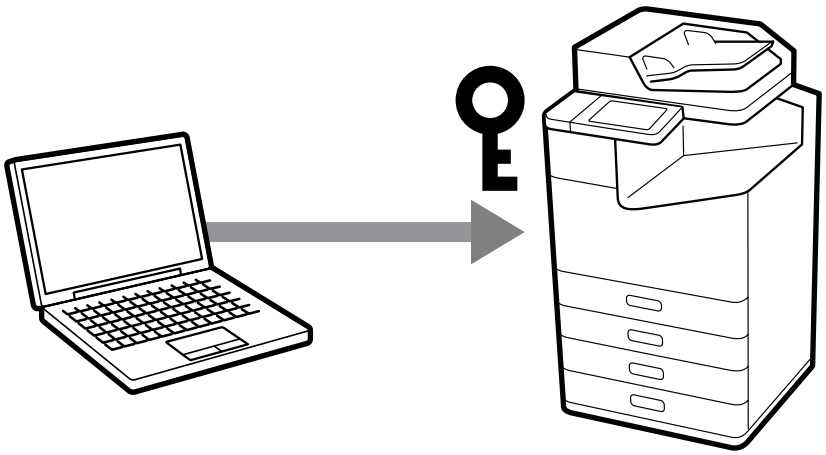
3-1. Administratorkennwort

Wir empfehlen, während der Installation jedes Produkts unbedingt ein Administratorkennwort einzurichten.

Wenn kein Administratorkennwort festgelegt ist oder die Werkseinstellungen des Produkts beibehalten werden, kann auf die allgemeinen Einstellungen oder die Netzwerkeinstellungen, die auf dem Produkt gespeichert sind, illegal zugegriffen oder sie können geändert werden. Es besteht auch das Risiko, dass persönliche und vertrauliche Information, wie z. B. Adressbücher, IDs und Kennwörter nicht ausreichend geschützt sind.

Das Administratorkennwort sollte eine komplexe Zeichenkette sein, die andere Benutzer oder Gäste schwer erraten können. Sie muss aus acht oder mehr Zeichen bestehen, einschließlich englischer Buchstaben, aber auch Symbole und Zahlen enthalten.
Sie können das Administratorkennwort auf dem Bedienfeld des Produkts oder über das Netzwerk einrichten.

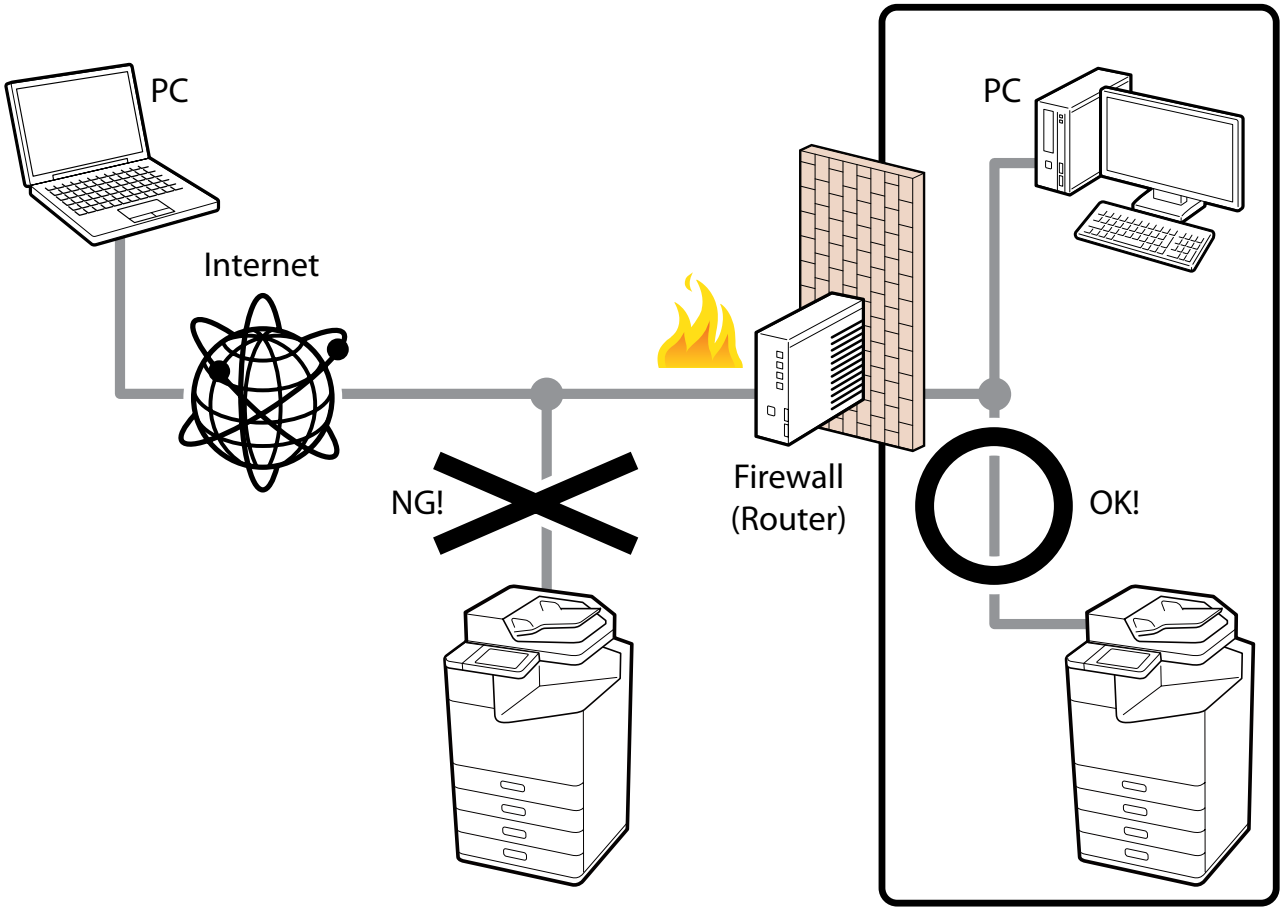
Einige Produkte haben werkseitig eingerichtete, individuelle Passwörter, um die Sicherheit zu erhöhen.



3-2. Internetverbindung

Installieren Sie Produkte in einem Netzwerk, das durch eine Firewall geschützt ist und verbinden Sie sie nicht direkt mit dem Internet. Wir empfehlen die Einrichtung und Verwendung einer privaten IP-Adresse, wenn Sie Produkte verbinden.

Auch wenn Sie das Produkt in einer IPv6-Umgebung verwenden, sollten Sie das Produkt durch eine Firewall oder andere Mittel schützen und den direkten Zugriff auf das Produkt aus dem Internet beschränken oder verhindern.



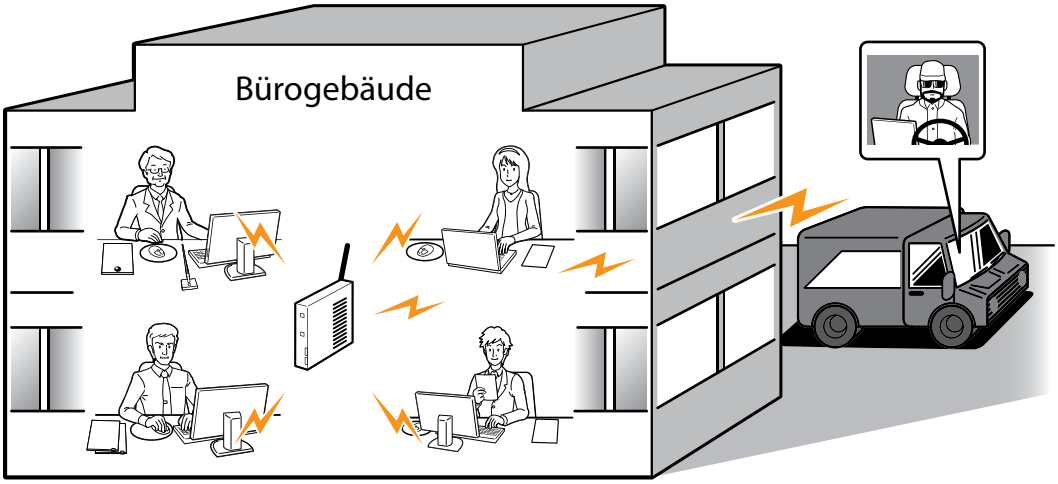
Sowohl für die Netzwerkfunktionen als auch für das Drucken enthält das Produkt eine Verwaltungsoberfläche z. B. einen Web-Verwaltungsbildschirm. Trotz der Sicherheitsprüfungen von Epson und unserem Bemühen, risikofreie Produkte zu liefern, birgt die direkte Verbindung zum Internet unerwartete Sicherheitsrisiken für das Kundennetzwerk und die Netzwerkgeräte z. B. durch unbefugte Bedienung und Datenverluste.

3-3. WLAN-Netzwerk

Nehmen Sie die entsprechenden Sicherheitseinstellungen für das WLAN-Netzwerk vor, wenn Sie WLAN nutzen.

Der Vorteil von WLAN ist, dass Sie sich mühelos über das Netzwerk mit dem Produkt verbinden und mit dem Computer oder Smartphone kommunizieren können, wenn Sie sich in Signalreichweite befinden. Andererseits können Probleme auftreten, die durch böswillige Drittparteien verursacht werden, wenn die Sicherheit nicht ordnungsgemäß eingerichtet wird.

- Persönliche Informationen, wie z. B. Druckdaten, Scandaten, ID und Kennwort können von anderen eingesehen oder abgefangen werden.
- Inhalte der Kommunikation werden möglicherweise in betrügerischer Absicht überschrieben (falsifiziert).
- Angreifer können sich als bestimmte Nutzer und Geräte ausgeben und die gestohlene Identität zur Kommunikation nutzen.



Siehe Produkthandbuch zu den Verfahren der WLAN-Einrichtung.

3-4. Deaktivierung nicht verwendeter Protokolle und Funktionen

Deaktivieren Sie Protokolle und Funktionen, die nicht verwendet werden.

Protokolle und Funktionen können individuell zugelassen oder verboten werden. Dadurch vermeiden Sie Risiken, falls sie unbeabsichtigt verwendet werden.

3-5. Aktualisierung auf die neueste Firm- und Software

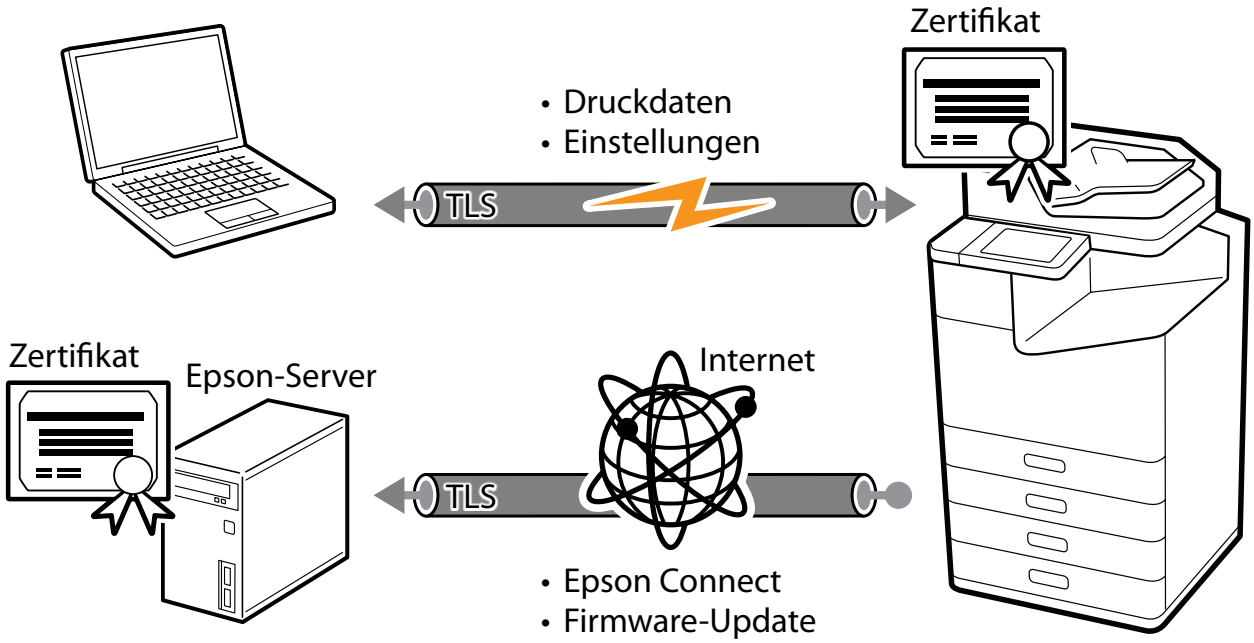
Wir stellen bei Bedarf die neueste Firm- und Software bereit. Aktualisieren Sie auf die neueste Firm- und Software für Ihr Produkt.

Mit der neuesten Firm- und Software erhalten Sie nicht nur zusätzliche Funktionen, sondern es werden auch Mängel und Sicherheitsrisiken behoben. Weitere Informationen zur Firmware oder Software finden Sie im Änderungsverlauf der Firmware und Software.

4. Netzwerksicherheit

4-1. TLS-Kommunikation

Übertragungen sind durch TLS geschützt, deshalb können Sie die Offenlegung von Einstellungsinformationen und Inhalten beim Drucken von Daten verhindern, indem Sie mit IPPS-Protokoll drucken und Ihr Produkt über Ihren Browser konfigurieren. Sie können auch verhindern, dass Informationen an nicht autorisierte Geräte gesendet werden. Verwenden Sie die Servervalidierungsfunktion, importieren Sie das CA-signierte Zertifikat und verwenden Sie die hauseigene Public-Key-Infrastruktur (PKI). Die konfigurierte Verschlüsselungsstärke ermöglicht einen sichereren Verschlüsselungsalgorithmus.
Sie sind auch durch TLS geschützt, wenn Sie mit dem Produkt auf den Epson-Server im Internet und Epson Connect und Firmware-Updates zugreifen.



Sie können die Version- und die Verschlüsselungsstärke des verwendeten TLS auswählen.

Unterstützte TLS-Versionen und Verschlüsselungsstärken:

TLS-Version

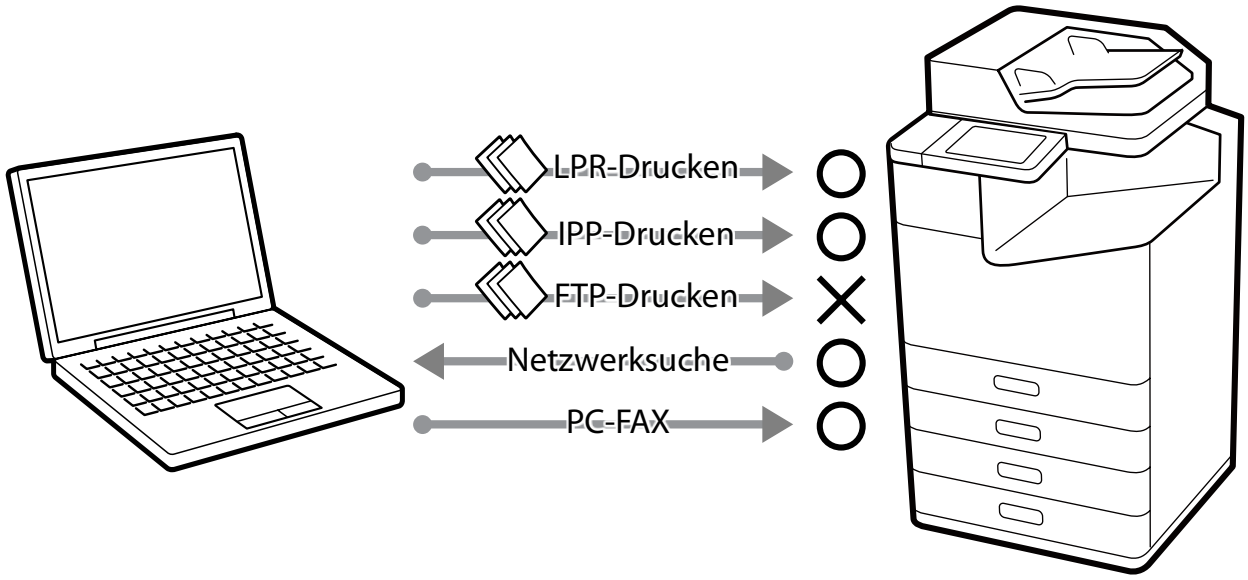
- TLS1.1
- TLS1.2
- TLS1.3

Verschlüsselungsstärke

- 80 bit
- 112 bit
- 128 bit
- 192 bit
- 256 bit

4-2. Steuerung der Berechtigungen und Ausnahmen des Protokolls

Das Produkt kommuniziert beim Drucken, Scannen und Senden an ein PC-FAX über verschiedene Protokolle. Sie können individuelle Berechtigungen und Verbote für jedes Protokoll einrichten, um Sicherheitsrisiken durch versehentliche Verwendung zu vermeiden.



Im Anhang finden Sie Informationen zu den Sicherheitsrisiken, wenn Protokolle und Funktionen aktiviert sind, und zu den Einschränkungen, wenn sie deaktiviert sind.

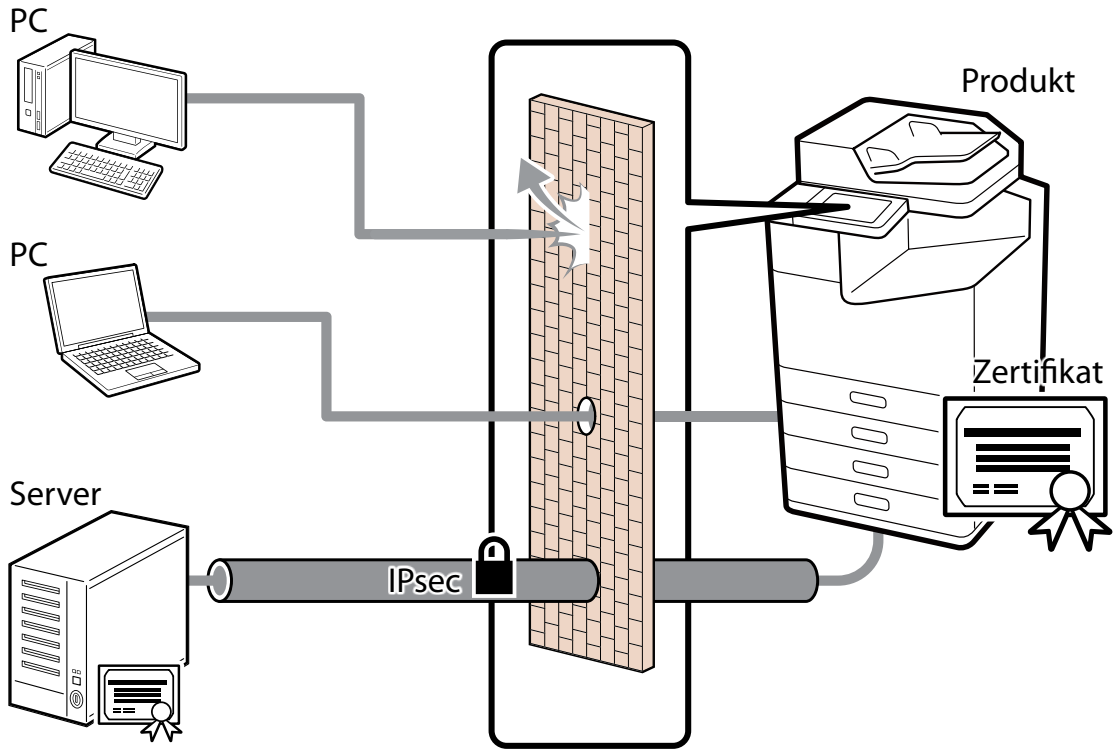
Protokolle und Funktionen können wie folgt erlaubt oder verboten werden.

- Bonjour
- SLP
- WSD
- LLTD
- LLMNR
- LPR
- RAW (Port9100/Angepasster Port)
- IPP/IPPS
- FTP
- SNMP
- SSL/TLS
- Microsoft-Netzwerkfreigabe
- Netzwerkscan (EPSON Scan)
- PC-FAX

4-3. IPsec/IP-Filterung

Sie können IP-Adressen, Diensttypen, die Portnummern für Empfang und Übertragung usw. mit der Funktion IPsec/IP-Filterung filtern. Je nach Kombination dieser Filter können Sie festlegen, ob Daten eines spezifischen Kunden akzeptiert oder blockiert werden und spezifische Datentypen blockieren. Auf ähnliche Weise können Sie mit höherer Sicherheit kommunizieren, wenn Sie mithilfe von IPsec Schutzmechanismen kombinieren.

Auch unsichere Druck- und Scanprotokolle werden geschützt, denn der Schutz in IP-Paketeinheiten (Verschlüsselung und Zertifizierung) ist Teil des Schutzes durch IPsec. Vorinstallierte Schlüssel und Zertifikate werden von der IPsec-Authentisierungsmethode unterstützt.



Folgende Algorithmen und Schlüsselaustauschmethoden werden unterstützt:

Schlüsselaustauschmethode

- IKEv1
- IKEv2

ESP Verschlüsselungsalgorithmus

- AES-CBC-128
- AES-CBC-192
- AES-CBC-256
- AES-GCM-128
- AES-GCM-192
- AES-GCM-256
- 3DES

ESP/AH Verschlüsselungsalgorithmus

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

Die grundlegende Richtlinie gilt für alle Nutzer, die auf das Produkt zugreifen. Legen Sie individuelle Richtlinien zur Zugangssteuerung gemäß Ihren spezifischen Bedürfnissen fest.

4-4. Authentisierung gemäß IEEE 802.1X

IEEE 802.1X ist ein Standard für die Zugangssteuerung an jedem einzelnen Port des Netzwerkgeräts. IEEE 802.1X-Netzwerke bestehen aus RADIUS-Servern (Authentisierungsserver) und Schaltknoten, die eine Authentisierungsfunktion haben.

Die Produkte von Epson entsprechen IEEE 802.1X und können mit einer Netzwerkumgebung verbunden werden, die vertrauliche Daten enthält.

Folgende Authentisierungsmethoden und Verschlüsselungsalgorithmen werden unterstützt:

Authentisierungsmethode

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

Verschlüsselungsalgorithmus

- AES128
- AES256
- 3DES
- RC4

4-5. SNMP

SNMP ist ein Protokoll zur Überwachung des Status und zur Änderung der Einstellungen von unterstützten Geräten und Verwaltungstools.

SNMPv1 und SNMPv2c unterstützen die Verschlüsselung der Kommunikation nicht und müssen innerhalb eines mit einer Firewall oder anders geschützten verwendet werden. Ändern Sie außerdem den Standardwert des Kommunikationsnamens, wenn Sie SNMP-Kommunikation verwenden.

SNMPv3 kann zur Authentisierung und Verschlüsselung der SNMP-Kommunikation (Pakete) für die Überwachung des Status und die Konfiguration von Änderungen mit kompatiblen Geräteverwaltungsprogrammen verwendet werden. Dadurch wird die Vertraulichkeit sichergestellt, wenn Sie Einstellungen ändern oder den Status über das Netzwerk überwachen.

SNMPv3 unterstützt die folgenden Authentisierungs- und Verschlüsselungsalgorithmen.

Authentisierungsalgorithmen von SNMPv3

- MD5
- SHA-1

Verschlüsselungsalgorithmen von SNMPv3

- DES
- AES128

4-6. SMB

SMB ist ein Protokoll für die gemeinsame Nutzung von Dateien in einem Netzwerk.

SMB1.0 und SMB2.0 unterstützen die Verschlüsselung der Kommunikation nicht und müssen innerhalb eines mit einer Firewall oder anders geschützten verwendet werden.

SMB3.0 kann zur Authentisierung und Verschlüsselung der SMB-Kommunikation (Pakete) auf kompatiblen Geräten verwendet werden. Dadurch wir die Vertraulichkeit der Dateifreigabe im Netzwerk sichergestellt.

4-7. WPA3

Das Produkt unterstützt WPA3, die neueste Authentisierungs- und Verschlüsselungstechnologie für WLAN. WPA3 bietet einen robusteren und stärkeren Schutz Ihrer Daten im WLAN-Netzwerk.

4-8. Trennung zwischen den Schnittstellen

Das Produkt hat eine USB-Schnittstelle, eine kabelgebundene Standard-LAN-Schnittstelle, eine zusätzliche LAN-Schnittstelle, eine WLAN-Schnittstelle und eine Fax-Schnittstelle. Jede dieser Schnittstellen ist unabhängig und der Zugriff ist auf die spezifischen Protokolle dieser Schnittstelle beschränkt. Es gibt keine Funktionen für die direkte Übertragung oder Weiterleitung. Beispielsweise ist der Zugang von einer öffentlichen Telefonleitung (Faxleitung) auf die Verarbeitung gemäß den Faxkommunikationsverfahren beschränkt. Abweichungen von diesem Verfahren würden dazu führen, dass die Kommunikation durch einen Verbindungsfehler unterbrochen wird. Es besteht keine Gefahr eines unbefugten Zugriffs. Außerdem werden die Bilddaten der empfangenen Faxdaten überprüft, bevor sie importiert werden. Es besteht keine Gefahr, dass durch die Übertragungsfunktion schadhafte Software in das Produkt eingeschleust wird, die zu einer Kontamination mit Viren oder einem unbefugten Zugriff führen könnte. Die Übertragungsfunktion kann nur von autorisierten Benutzern ausgeführt werden. Wie z. B. Eindringen in das Netzwerk über eine öffentliche Telefonleitung über das Produkt, Zugang zum kabelgebundenen LAN über das kabellose WLAN oder der nicht autorisierte Zugang vom Internet auf das Produkt, das über USB mit einem Computer verbunden ist.

5. Schutz Ihres Produkts

5-1. Blockieren der USB-Verbindung auf dem Computer

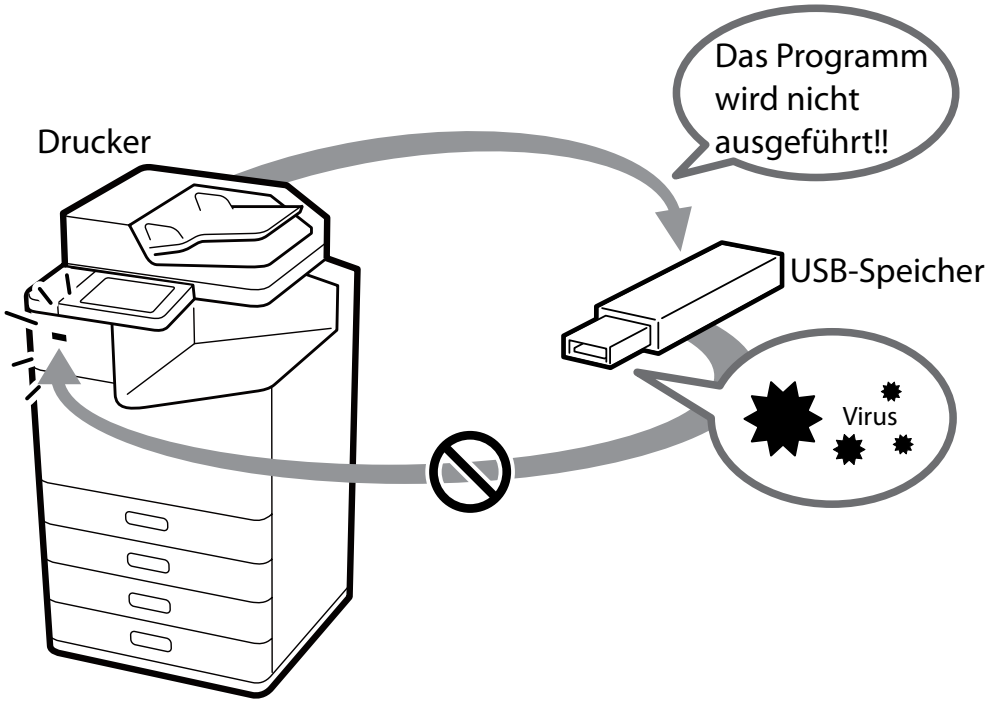
Sie können den Zugriff von einem Computer auf das Produkt über eine USB-Verbindung deaktivieren. Legen Sie diese Option fest, um das Drucken oder Scannen durch eine direkte Verbindung mit einem Computer über ein USB-Kabel zu verhindern.

5-2. Deaktivierung der externen Schnittstelle

Sie können Speicherkarten und USB-Speicherschnittstellen deaktivieren. So können Sie die illegale Vervielfältigung von Daten durch unbefugtes Scannen von vertraulichen Dokumenten im Büro verhindern.

5-3. Umgang mit Viren, die vom USB-Speicher übertragen werden

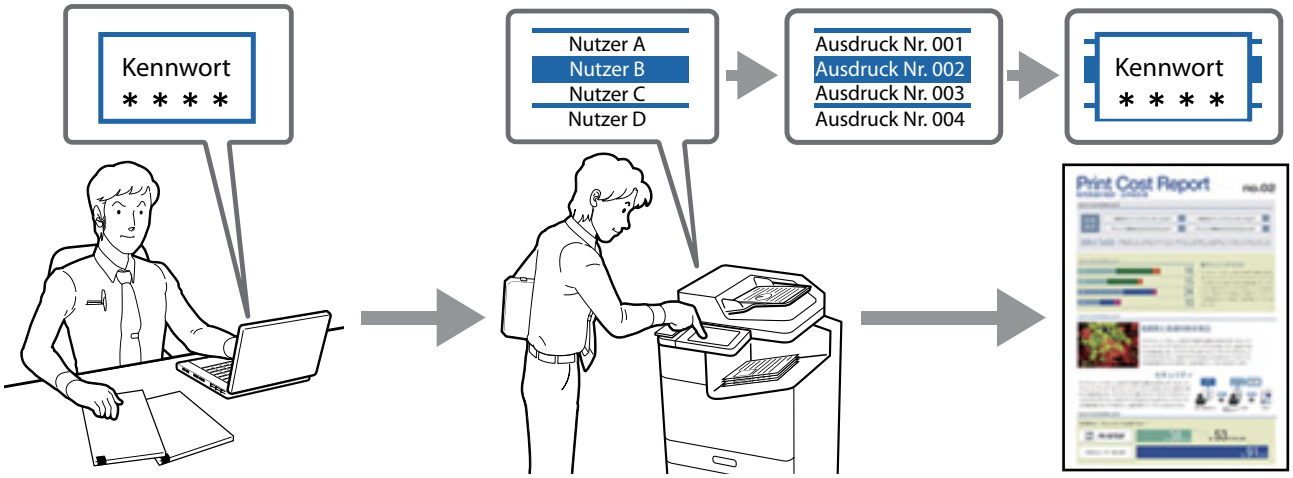
Es gibt keine ausführbaren Funktionen auf USB-Speichern für Epson-Produkte, deshalb besteht keine Gefahr, dass das Produkt über einen USB-Speicher mit Viren infiziert wird.



6. Druck-/Scan-Sicherheit

6-1. Vertrauliche Aufträge

Sie können die Vertraulichkeit von Dokumenten sicherstellen und verhindern, dass unbefugte Personen unbeaufsichtigte Ausgaben am Gerät einsehen, indem Sie Ihre Dokumente als „vertraulichen Auftrag“ übermitteln.



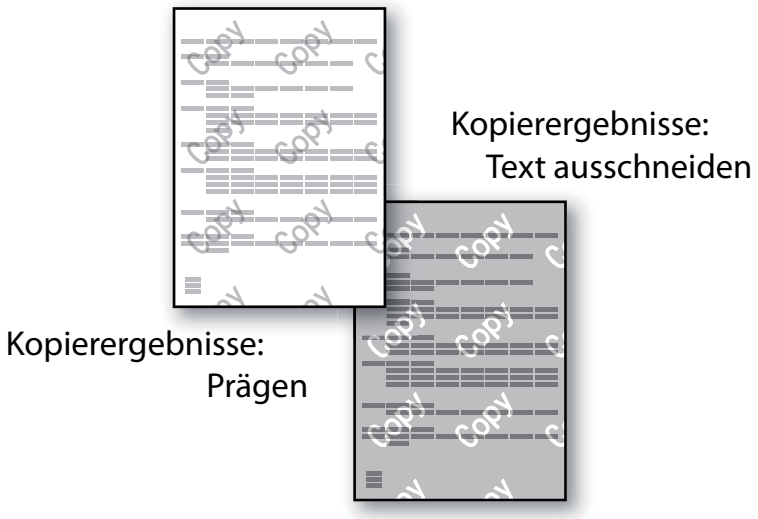
Kennwort eingeben, um zu drucken.

Wählen Sie einen Druckauftrag auf dem Produkt aus und geben Sie das Kennwort ein.

Das Drucken ist beendet.

6-2. Antikopierschutz-Muster

Sie können ein Originaldokument mit dem Anti-Kopier-Wasserzeichendruck schützen, der ein transparentes Wasserzeichenmuster auf der Originalausgabe erstellt. Das transparente Wasserzeichen wird sichtbar, wenn versucht wird, die Originalausgabe zu kopieren.

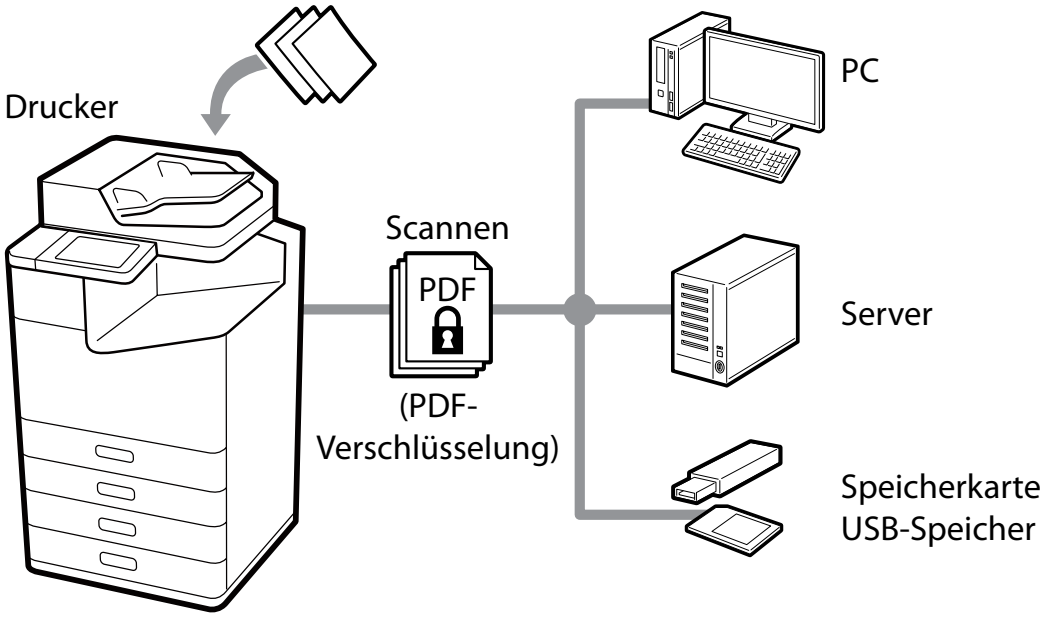


6-3. Wasserzeichen

Es können Wasserzeichen wie „klassifiziert“ oder „wichtig“ (als Text oder im BMP-Format) auf dem Dokument erstellt werden. Außerdem können Sie einen „Benutzernamen“ oder einen „Computernamen“ wählen. Indem Sie den Empfänger an den vorsichtigen Umgang mit dem Dokument erinnern, verhindern Sie die unbefugte Verwendung.

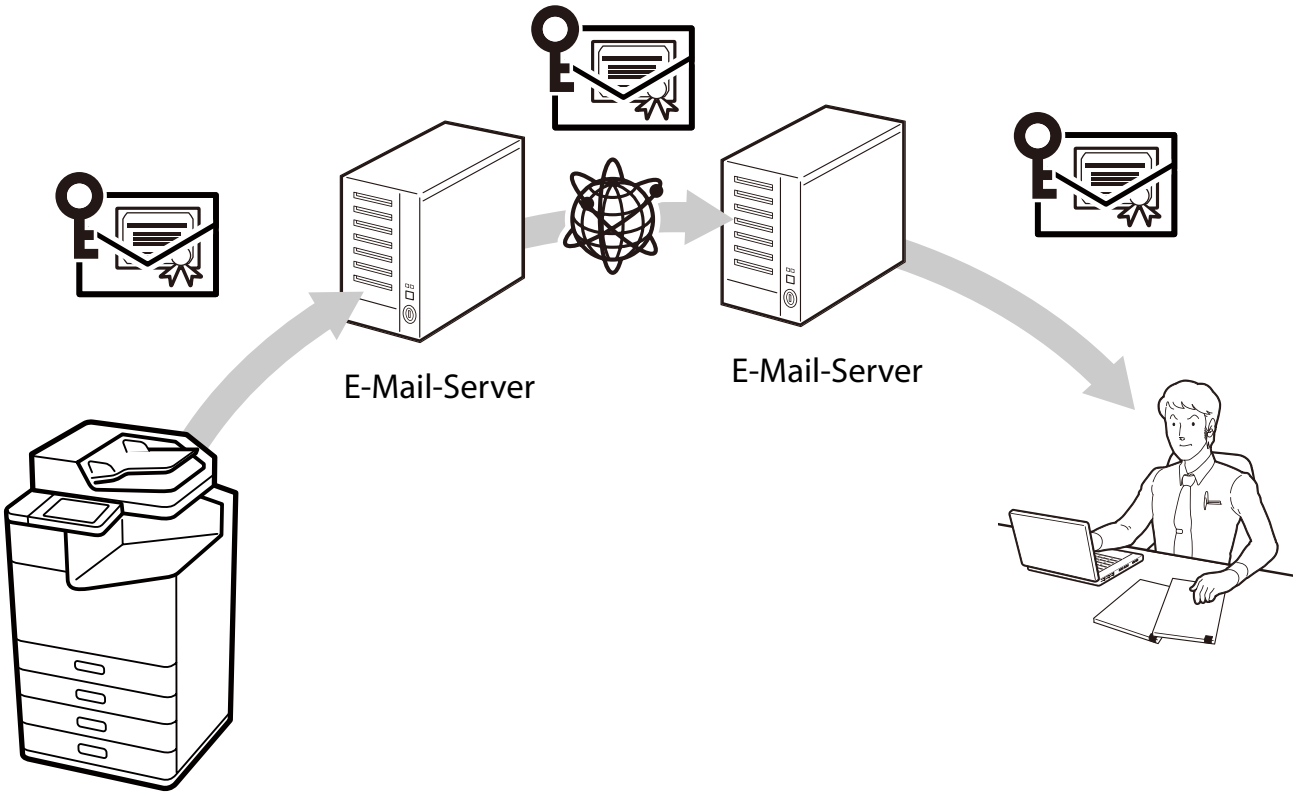
6-4. PDF-Verschlüsselung

Sie können ein Dokument in eine kennwortgeschützte PDF-Datei scannen.
Das verhindert, dass die Dokumente unbefugt von Dritten angezeigt werden.



6-5. S/MIME

Mit S/MIME können Sie eine digitale Signatur und/oder eine E-Mail verschlüsseln, wenn Sie „An eMail scannen“ oder „Fax an E-Mail“ verwenden. Auch wenn die E-Mails über mehrere Server übertragen werden, können Sie verhindern, dass sie falsifiziert, abgefangen oder manipuliert werden. S/MIME schützt die Authentizität und Integrität der Nachricht und bietet zugleich Datenschutz und Unverfälschbarkeit.



Folgende Algorithmen werden unterstützt.

Verschlüsselungsalgorithmus

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

Digitale Signatur mit Hash-Algorithmus

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

6-6. Domänenbeschränkungen

Durch die Anwendung von Beschränkungsregeln auf die Domänennamen von E-Mail-Adressen können Sie das Risiko von Fehlübertragungen und Datenverlust bei den E-Mail-Funktionen „An eMail scannen“ oder „Fax an E-Mail“ verringern.

6-7. Unterstützung für lange Authentisierungskennwörter

Heute werden lange Kennwörter empfohlen, um die Kennwortsicherheit zu erhöhen. Sie können maximal 70 Zeichen als Autorisierungskennwort für „In Netzwerkordner/FTP scannen“, „An eMail scannen“ und „eMail-Benachrichtigung“ verwenden. Sie können eine Kennwortrichtlinie für lange Kennwörter für Dateiserver und Mailserver festlegen.

6-8. Beschränkungen für den Dateizugriff vom PDL

Durch die Deaktivierung des Dateizugriffs von PDL (Seitenbeschreibungssprache) können Sie das Risiko von Datenverlusten durch böswillige Druckdaten verhindern, die Dateien aus dem Drucker stehlen. Selbst wenn böswillige Druckdaten übertragen werden, kann das Produkt sicher verwendet werden und die Dateien werden nicht gelesen.

6-9. Sicheres Drucken

Wenn Sie die Sicherheit der Übertragungsrouten beim Drucken schützen möchten, können Sie ein über TLS verschlüsseltes IPPS verwenden.

7. Faxsicherheit

7-1. Direktwahlbeschränkungen

Wenn Sie eine Faxnummer direkt auf dem Zifferntastenblock eingeben, können Sie einstellen, dass das Fax erst gesendet wird, nachdem Sie sie zweimal korrekt eingegeben haben. Sie können die Eingabe einer Telefonnummer direkt auf dem Zifferntastenblock verbieten und die Faxe werden nur über die Zielwahl und an Adressen in Ihrem Adressbuch gesendet. Dadurch kann das Risiko von Datenverlusten durch Fehler bei der Eingabe der Telefonnummer und falsche Übertragungen verhindert werden.

7-2. Bestätigung der Adressliste

Sie können die ausgewählte Adresse bestätigen, bevor Sie ein Fax senden. Dadurch kann das Risiko der Offenlegung von Informationen durch Fehler bei der Eingabe der Telefonnummer und falsche Übertragungen verhindert werden.

7-3. Wähltonerkennung

Sie können falsche Übertragungen vermeiden, indem Sie Faxe erst nach der Erkennung und Bestätigung eines Wähltons senden.

Abhängig von Ihrem Land oder Ihrer Region ist die Wähltonerkennung möglicherweise nicht verfügbar.

7-4. Maßnahmen gegen zurückgelassene Faxe

„Fax nach Ansicht drucken“ kann so eingestellt werden, dass ein empfangenes Fax im Posteingang gespeichert (Speicherempfang) und nachdem Sie es auf dem Bedienfeld bestätigt haben, gedruckt wird. So können Sie verhindern, dass Informationen offengelegt werden oder gedrucktes Material empfangener Faxe verloren geht, weil die gedruckten Faxe unbeaufsichtigt geblieben sind.

Sie können auch willkürliches Drucken und Löschen durch unbefugte Nutzer verhindern, indem Sie ein Kennwort für den Zugang zum Posteingang festlegen.

7-5. Übertragungsbericht zur Bestätigung

Zur Bestätigung, dass ein Fax definitiv an die richtige Adresse gesendet wurde, können Sie Bericht mit der Bestätigung der Übertragungsdetails ausdrucken, wie z. B. Sendebericht, Weiterleitungsbericht und Sendeverwaltungsbericht.

7-6. Löschen der Sicherungsdaten für empfangene Faxe

Sicherungsdaten* für empfangene Faxe können auf dem Bedienfeld gelöscht werden. Sie können auch einstellen, dass die Sicherungsdaten automatisch gelöscht werden und so das unbefugte Drucken der empfangenen Faxe verhindern.

* Die Sicherungsdaten der empfangenen Faxe werden im Produkt gespeichert (Werkseinstellungen) und Sie können die Faxe jederzeit erneut drucken, wenn die Druckqualität schlecht ist oder der Druck verloren geht.

7-7. Beschränkter Versand an mehrere Empfänger

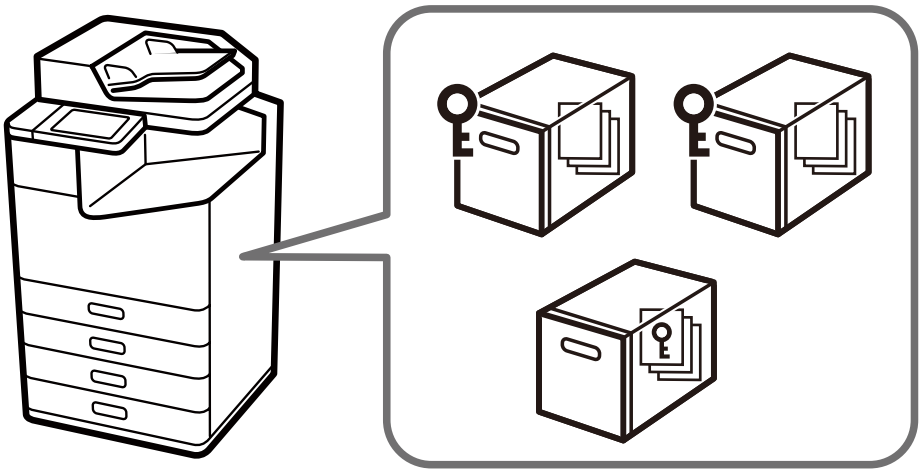
Sie können das Produkt so einstellen, dass nur 1 Empfänger ausgewählt werden kann.

Wenn Sie verbieten, dass mehrere Empfänger ausgewählt werden können, ist das Risiko geringer, dass ein Fax an einen unbeabsichtigten Empfänger gesendet wird und Informationen offengelegt werden.

8. Nutzerdatenschutz

8-1. Speichersicherheit

Sie können ein eindeutiges Kennwort für freigegebene Ordner und Dokumente auf Modellen mit freigegebenen Ordnern festlegen. Diese Kennwörter verhindern, dass Informationen offengelegt werden, verloren gehen oder unbefugt manipuliert werden. Auch der Speicherbetrieb kann einer Zugriffssteuerung unterliegen. Wenn freigegebene Ordner nicht verwendet werden, können Sie die Verwendung der Freigabefunktion des Ordners verbieten.



8-2. Schutz Ihres Adressbuchs

Für die Massenverarbeitung der im Produkt gespeicherten Adressbücher ist ein Administratorkennwort erforderlich (wenn ein Administratorkennwort eingerichtet wurde). Dadurch können Datenverluste und die unbefugte Änderung von Adressbuchinformationen verhindert werden. Weil Adressbücher als verschlüsselte Datei exportiert werden können, wird auch verhindert, dass persönliche Informationen, wie z. B. Faxnummern und E-Mail-Adressen beim Austausch oder bei der Sicherung des Produkts preisgegeben werden.

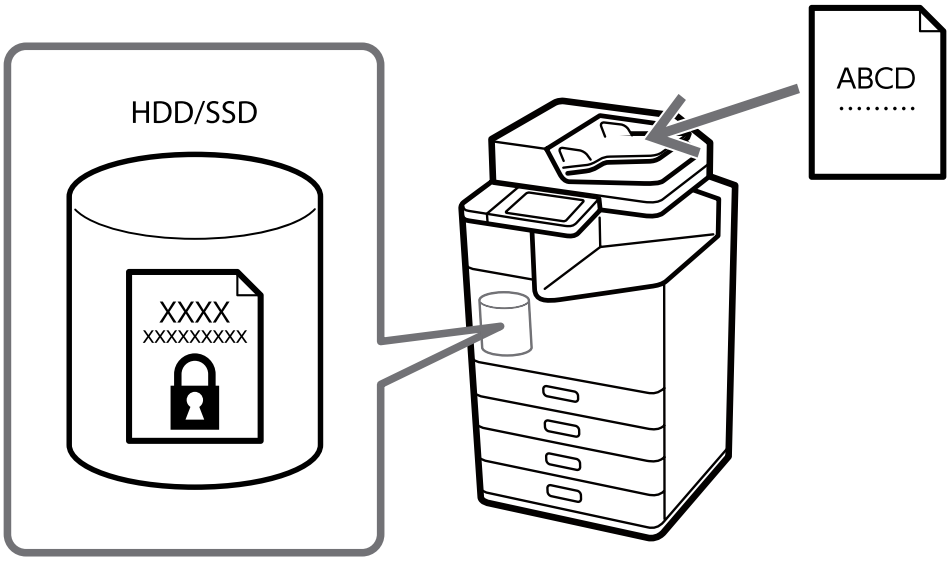
8-3. Datenverarbeitung des Produkts

Die Daten der Druck-, Kopier- und Scanfunktionen werden temporär im Produkt gespeichert und gelöscht, wenn ein Auftrag beendet oder das Produkt ausgeschaltet wird. Beim Versand und Empfang von Faxen werden die Faxdaten vollständig gelöscht. Auch empfangene Faxe werden als Daten gespeichert und durch eine Sicherungsfunktion aufbewahrt. Diese Einstellung können Sie ändern und die Daten werden automatisch gelöscht (siehe 7-6).

8-4. Verschlüsselung der gespeicherten Daten auf HDD/SSD

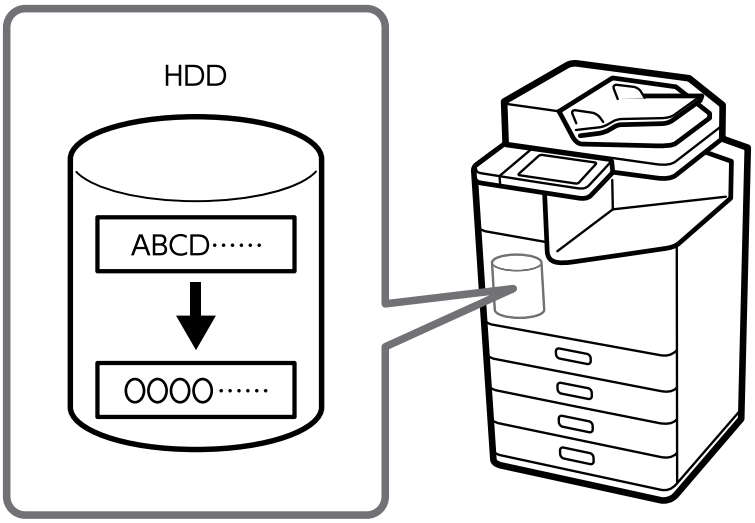
Wir schützen die Kundendaten immer mit Verschlüsselung, wenn die Daten auf einem internen HDD/SSD des Produkts gespeichert werden. Im unwahrscheinlichen Fall des Angriffs eines böswilligen Dritten sind die Inhalte der gespeicherten Daten nicht sichtbar. Das HDD/SSD hat ein selbstverschlüsselndes Laufwerk und die Daten werden mit AES-256 verschlüsselt.

Die Datenverschlüsselung verhindert unbefugten Zugang oder böswillige Angriffe auf personenbezogene Daten, wenn das HDD/SSD gestohlen wird.



8-5. Sequenzielles Löschen von Auftragsdaten

Wenn diese Funktion aktiviert ist, werden die vorübergehend auf der Festplatte des Geräts gespeicherten Auftragsdaten automatisch gelöscht, nachdem sie mit einem speziellen Muster überschrieben wurden. Dadurch wird verhindert, dass Dritte die verbliebenen Daten des Druckauftrags wiederherstellen.



8-6. Kennwortverschlüsselung

Sie können Kennwörter, die auf dem Produkt gespeichert sind, verschlüsseln.
Die folgenden Informationen sind verschlüsselt:

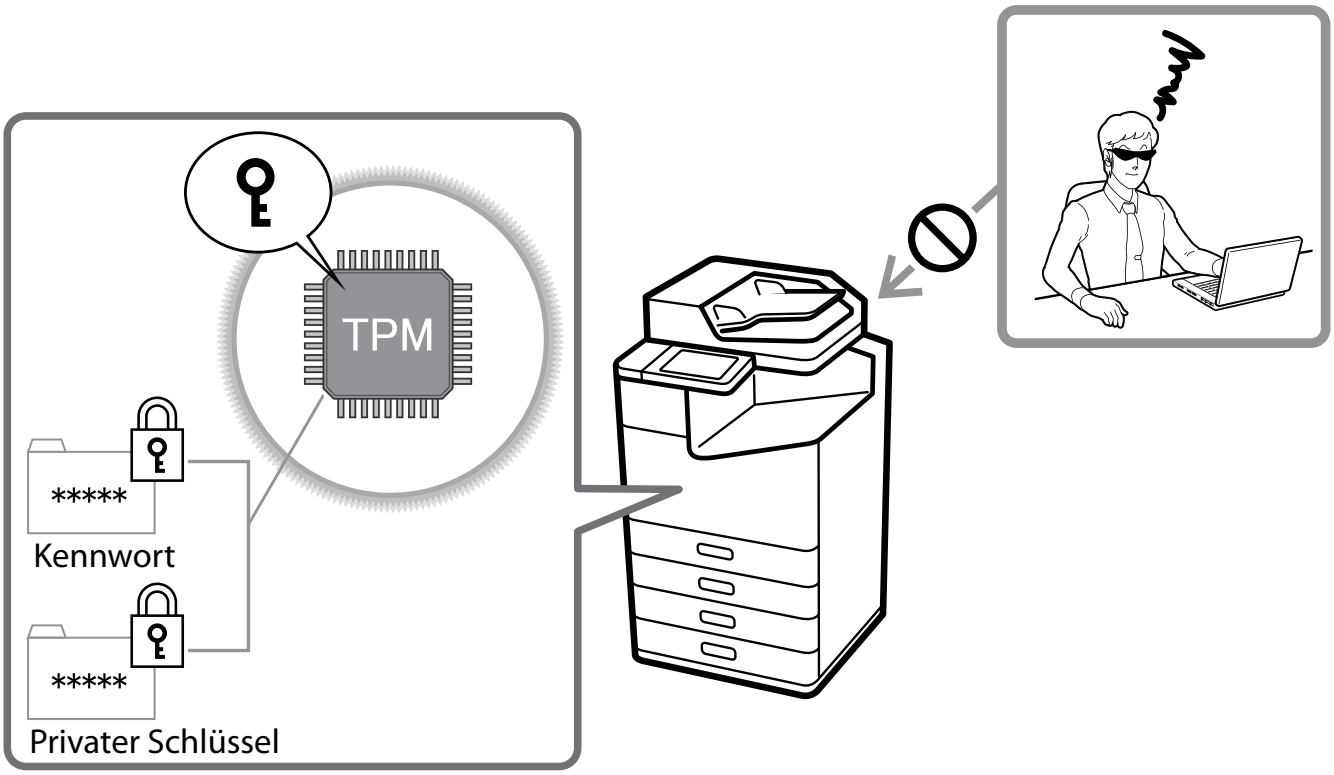
- Administratorkennwort
- Kennwort für die Zugangssteuerung
- Authentisierungsschlüssel für die Festplatte, privater Schlüssel für Zertifikate usw., Kennwörter für den Zugang zu „In Netzwerkordner/FTP scannen“

8-7. TPM

Bei Modellen, die mit einem TPM (Trusted Platform Module) ausgestattet sind, werden die Verschlüsselungsschlüssel für die Wiederherstellung verschlüsselter Kennwörter und die Informationen des privaten Schlüssels werden auf dem TPM-Chip gespeichert. Auf den TPM-Chip kann nicht von außerhalb des Druckers zugegriffen werden, denn er ist auf Hardware-Level vor unbefugtem Auslesen geschützt.

Die echten Zufallszahlen des TPM werden für die Zufallszahlen der Konfigurationen über Browser-Sitzungen (Web Config) verwendet. Mit den echten Zufallsdaten des TPM werden Authentisierungsschlüssel für das verschlüsselte HDD/SSD generiert.

Diese Modelle sind mit Chips der Spezifikation TPM2.0 ausgestattet.



8-8. HDD-Spiegelung

Wenn eine zusätzliche HDD installiert ist, können selbst bei einem Ausfall einer HDD alle Funktionen mit der anderen HDD fortgesetzt werden, ohne dass gespeicherte Daten verloren gehen.

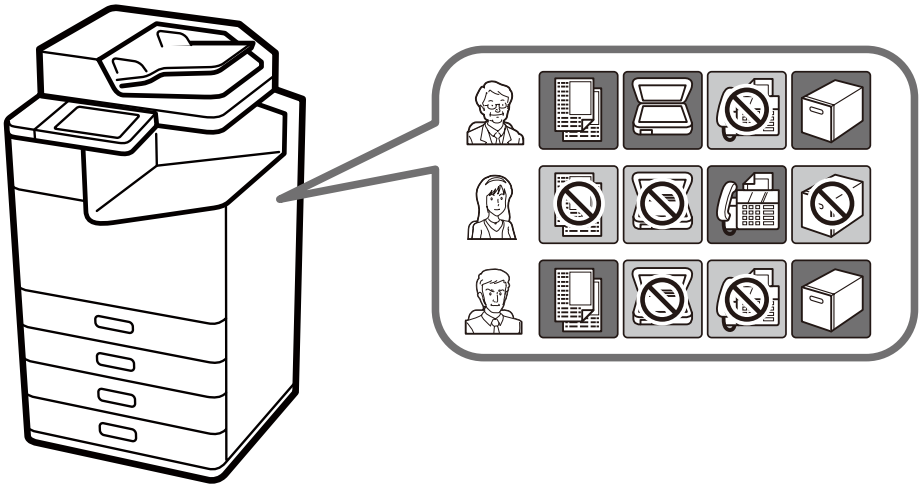
9. Betriebsbeschränkungen

9-1. Bedienfeldsperre

Wenn Sie ein Bedienfeldsperre verwenden, haben Sie nur mit einem Administratorkennwort Zugang zum Bedienfeld. Wenn das Bedienfeld durch ein Administratorkennwort geschützt ist, können Benutzer in offenen Büros, öffentlichen Einrichtungen oder an ähnlichen Orten die Einstellungen nicht verändern.

9-2. Zugriffssteuerung

Sie können das Drucken, Scannen, Kopieren, Faxen* und die Funktionen der Fächer individuell für Benutzer beschränken, um die mit ihren Rollen verbundenen Sicherheitsrisiken zu minimieren. Außerdem werden die Benutzer automatisch nach einem bestimmten Zeitraum abgemeldet, wenn sie am Bedienfeld inaktiv waren.



* Es kann nur die Faxübertragung beschränkt werden.

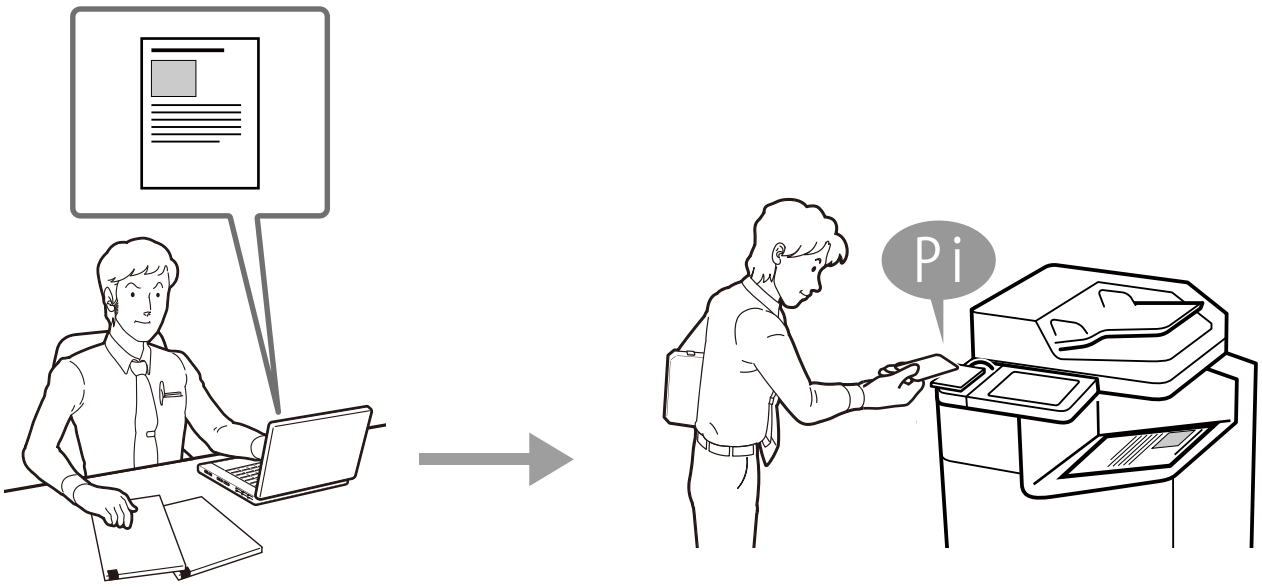
9-3. Authentisierte Druck-/Scaneinstellungen

Wenn optional Epson Print Admin oder Epson Print Admin Serverless installiert ist, können sich Benutzer beim Drucken oder Scannen mit Authentisierungsgeräte wie ID/Passwort-Authentifizierung und IC-Kartenleser, authentisieren. Dadurch, dass die Benutzer die Authentisierung und Bedienung vor dem Produkt vornehmen, wird verhindert, dass Informationen aus gedruckten Materialien oder aus unbeaufsichtigten Dokumenten, die versehentlich von anderen aus dem Drucker genommen werden, weitergegeben werden.

Diese Authentisierungsmethode können Benutzer verwenden, die mit LDAP verknüpft und am Drucker registriert sind.

Außerdem können Sie sich bei einigen Standalone-Scannern zum Scannen mit ID/Kennwort oder entsprechenden Geräten wie IC-Kartenleser authentisieren, wenn Sie sich am Hauptgerät authentisieren oder Document Capture Pro Server Authentication Edition verwenden.

Diese Authentisierungsmethode können Benutzer verwenden, die mit LDAP verknüpft und am Drucker registriert sind.



9-4. Kennwortrichtlinie

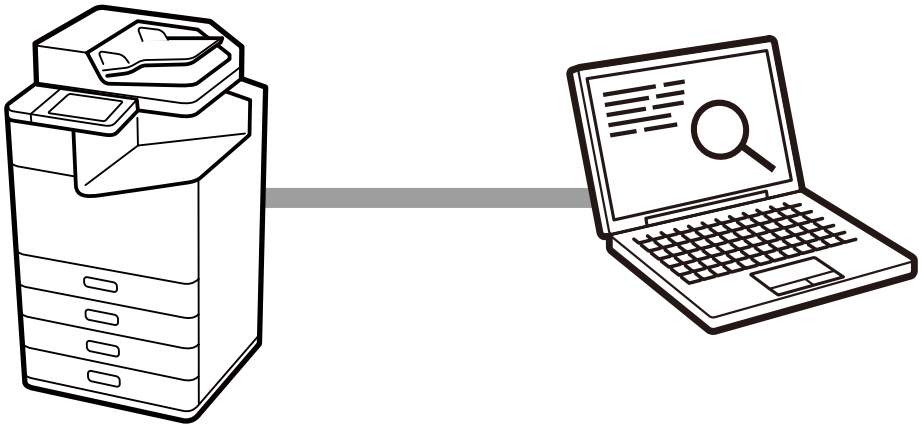
Die Kennwortrichtlinie kann auf die Kennwörter des Administrators, der Zugangssteuerung und Faxe angewendet werden. Ein sicheres Kennwort, das mehrere der folgenden Bedingungen erfüllt, kann verhindern, dass Kennwörter von böswilligen Angreifern gehackt werden.

- Minimale Anzahl der Zeichen von Kennwörtern.
- Kennwörter mit/ohne englische Buchstaben.
- Kennwörter mit/ohne englische Kleinbuchstaben.
- Kennwörter mit/ohne englische Großbuchstaben.
- Kennwörter mit/ohne Symbole.

9-5. Audit-Protokoll

Die Funktion Audit-Protokoll zeichnet den Druck-, Scan-, Faxverlauf und den Verlauf der Änderung zu Auditzwecken auf. Mit der regelmäßigen Bestätigung dieses Protokolls können Fehlbedienungen früher erkannt und Sicherheitsprobleme aufgespürt werden.

Es werden bis zu 20.000 Audit-Protokolle (bis zu 5.000 bei einigen Modellen) aufbewahrt werden.



10. Produktsicherheit

10-1. Automatische Firmware-Aktualisierungen

Wenn automatische Firmware-Aktualisierungen aktiviert sind, kann die Firmware automatisch zu einer bestimmten Zeit aktiviert werden. Da die Aktualisierungen stets zu einer angegebenen Zeit durchgeführt werden, verwenden Sie immer die neueste Firmware, ohne dass der Betrieb unterbrochen werden muss.

10-2. Schutz vor illegalen Firmware-Aktualisierungen

Bei der Firmware-Aktualisierung wird eine Authentisierung mit Administratorkennwort durchgeführt. Die Datenkommunikation mit dem Produkt ist außerdem durch HTTPS geschützt, und die an das Produkt selbst gesendete Firmware wird durch eine Signatur als legitim verifiziert, bevor die Firmware neu geschrieben wird. Dadurch wird die unbefugte Veränderung der Firmware durch böswillige Drittparteien verhindert.

10-3. Sicherer Systemstart

Wenn das System gestartet wird, überprüft es anhand der Signatur, ob die Firmware legitim ist. Wenn es feststellt, dass die Firmware überschrieben wurde und nicht autorisierte Firmware ist, wird der Systemstart gestoppt und der Nutzer wird aufgefordert, die Firmware zu aktualisieren.

10-4. Erkennung der Infiltration von Malware

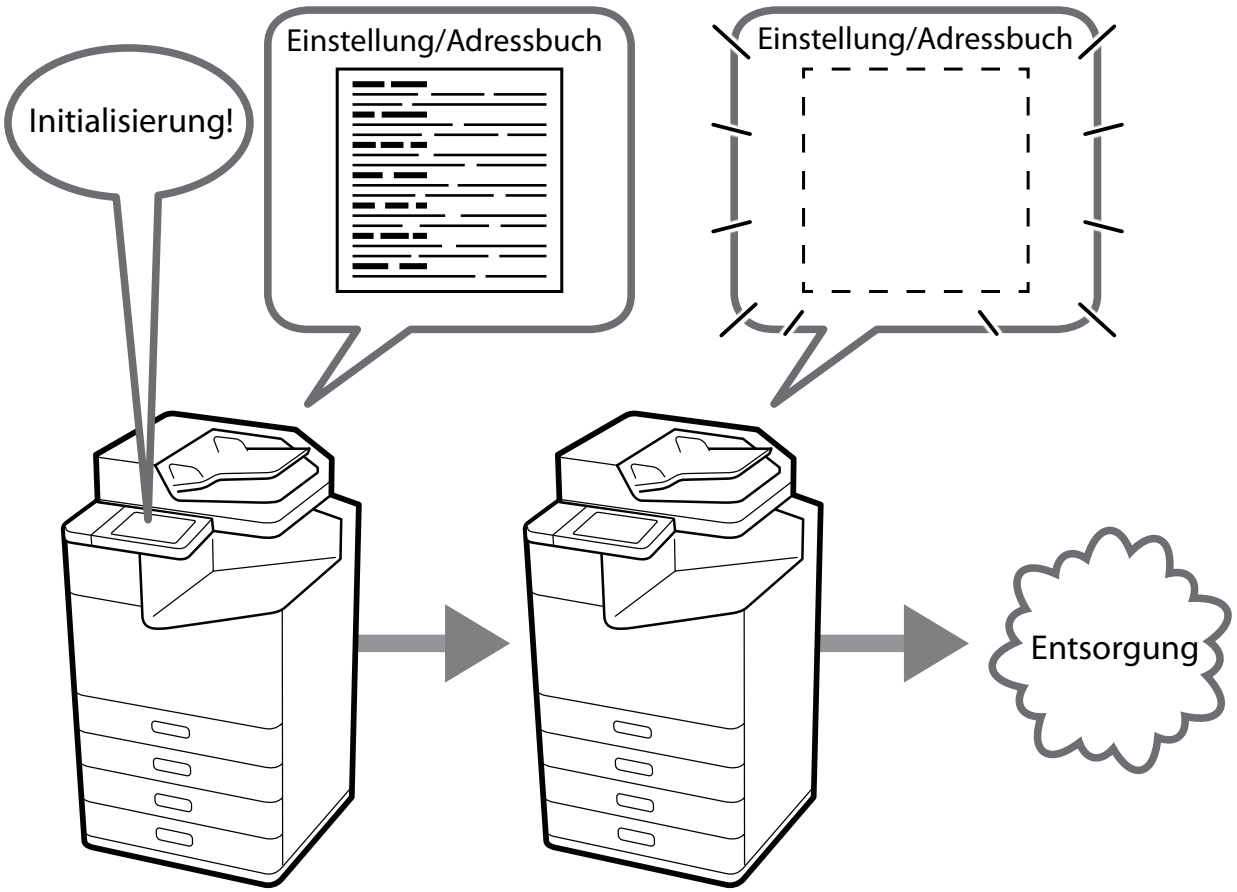
Das Produkt wird ständig auf Infiltration von Malware in die Firmware überwacht, während das Produkt ausgeführt wird. Wenn Malware entdeckt wird, wird das Produkt neu gestartet, um Malware zu beseitigen.

11. Sicherheitsmaßnahmen bei der Entsorgung Ihres Produkts

11-1. Wiederherstellen der Werkseinstellungen

Wenn Sie ein Produkt übertragen oder entsorgen, können Sie alle Einstellungen (einschließlich der Einstellungen auf der internen HDD/SSD) auf Werkseinstellungen (Initialisierung) zurücksetzen, um die Offenlegung vertraulicher Informationen zu verhindern.

Die HDD/SSD kann außerdem gelöscht werden, entweder mit „Löschen bei Änderung des Verschlüsselungsschlüssels im selbstverschlüsselnden Laufwerk (Hochgeschwindigkeit)“ oder „Löschen bei Änderung des Selbstverschlüsselungsschlüssel und mit einem speziellen Muster überschreiben (überschreiben, dreifach überschreiben)“.



12. Sicherheitszertifizierung und Standards

12-1. ISO15408/IEEE 2600.2™

Das Produkt ist gemäß ISO/IEC 15408 zertifiziert und erfüllt den internationalen Sicherheitsstandard IEEE Std. 2600.2™-2009[*1], ein internationaler Standard der Informationssicherheit.

IEEE Std. 2600.2™

IEEE Std. 2600.2™ ist ein internationaler Standard, der die Kriterien der Informationssicherheit für MFP festlegt. Die MFP-Sicherheit kann durch standardmäßige Sicherheitsfunktionen wie Nutzeridentifizierung und Authentisierung, Zugangssteuerung, Überschreiben von Daten, Netzwerksicherheitsverwaltung, Selbsttests und Audit-Protokolle verstärkt werden.

ISO/IEC 15408

ISO/IEC 15408, auch Common Criteria (CC) genannt, ist ein internationaler Standard für die unabhängige und objektive Bewertung der Sicherheitsmaßnahmen von IT-Produkten und Systemen. Er überprüft, ob die Maßnahmen ordnungsgemäß entwickelt und implementiert wurden.

Im Rahmen der Zertifizierung nach ISO/IEC 15408 werden die spezifizierten Versionen von Firmware, Handbüchern und anderen Komponenten bewertet. Die Version der Firmware eines gekauften Produkts kann von der zertifizierten Version abweichen.

Möglichweise sind bestimmte Funktionen eingeschränkt, wenn eine zertifizierte Version verwendet wird.

Das Logo der CCRA Zertifizierung zeigt, dass das Produkt gemäß Japan Information Technology Security Evaluation and Certification Scheme (JISEC[*2]) evaluiert und zertifiziert wurde.
Das impliziert jedoch nicht die Garantie, dass das Produkt völlig frei von Sicherheitsrisiken ist. Es impliziert auch nicht, dass das Produkt in jeder Betriebsumgebung mit allen notwendigen Sicherheitsfunktionen ausgestattet ist.

*1 U.S. Government Approved Protection Profile — U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009).

*2 JISEC (Japanisches System zur Bewertung und Zertifizierung der Sicherheit von Informationstechnologie).

Sicherheitsrisiken bei aktivierten Protokollfunktionen und Beschränkungen bei deaktivierten Protokollfunktionen

Protokoll/ Sicherheitsfunktionen	Sicherheitsrisiken bei Aktivierung	Beschränkungen bei Deaktivierung
Bonjour	Es besteht die Möglichkeit, dass Informationen auf den Geräten im Netzwerk von Dritten gelesen werden.	Die Suche über Bonjour ist auf dem Computer nicht möglich.
SLP	Da der Absender nicht authentifiziert ist, Es kann ein gefälschter Absender für einen Angriff genutzt werden, um den Dienst zu deaktivieren, weil der Absender nicht authentisiert ist.	Der Computer kann Gerätedaten und Informationen zum Gerät nicht mit SLP abrufen.
WSD	Die Kommunikation ist nicht verschlüsselt und es besteht die Möglichkeit, dass die ausgedruckten Daten von Dritten gelesen werden können.	Es kann nicht mit WSD gescannt oder gedruckt werden.
LLTD	Es besteht die Möglichkeit, dass Informationen auf den Geräten im Netzwerk von Dritten gelesen werden.	Die Geräte werden in Windows in „Geräte und Drucker“ nicht angezeigt.
LLMNR	Es besteht die Möglichkeit, dass Informationen auf den Geräten im Netzwerk von Dritten gelesen werden.	Die Suche mit LLMNR ist auf dem Computer nicht möglich.
LPR	Die Kommunikation ist nicht verschlüsselt und es besteht die Möglichkeit, dass die ausgedruckten Daten von Dritten gelesen werden können.	Es kann nicht mit LPR gedruckt werden.
RAW (Port 9100/alle Ports)	Die Kommunikation ist nicht verschlüsselt und es besteht die Möglichkeit, dass die ausgedruckten Daten von Dritten gelesen werden können.	Es kann nicht über RAW-Port gedruckt werden.
IPP/IPPS	Die IPP-Kommunikation ist nicht verschlüsselt und es besteht die Möglichkeit, dass die ausgedruckten Daten von Dritten gelesen werden können. Es bestehen keine Sicherheitsrisiken in Bezug auf IPPS.	Das Drucken über IPP/IPPS, wie z. B. das Drucken über AirPrint oder Mac OS, ist nicht möglich.

Protokoll/ Sicherheitsfunktionen	Sicherheitsrisiken bei Aktivierung	Beschränkungen bei Deaktivierung
FTP	Die Kommunikation ist nicht verschlüsselt und es besteht die Möglichkeit, dass die ausgedruckten Daten von Dritten gelesen werden können.	Es kann nicht mit FTP gedruckt werden und es können keine Daten mit FTP übertragen werden.
SNMP	Bei SNMPv1 und v2c ist die Kommunikation nicht verschlüsselt und es besteht die Möglichkeit, dass Gerätedaten und Einstellungsdaten von Dritten gelesen werden können. Es bestehen keine Sicherheitsrisiken in Bezug auf SNMPv3.	Die Verwaltungstools, die SNMP verwenden, können nicht verwendet werden. Außerdem sind die von Epson bereitgestellten Verwaltungstools und Anwendungen nicht verfügbar.
SSL/TLS	Abhängig davon, welche TLS-Version und Schlüssellänge Sie eingestellt haben, kann die Verschlüsselungsstärke unsicher sein und die Verschlüsselung entschlüsselt werden.	Die Verbindung über HTTPS ist in einem Browser nicht möglich.
Microsoft-Netzwerkfreigabe	Es besteht die Möglichkeit, dass gescannte Daten oder Daten im freigegebenen Ordner von Dritten gelesen werden.	Die Übertragung von Dateien und die Netzwerk-Dateifreigabe mithilfe von SMB ist nicht möglich.
Netzwerk-Scannen (EPSON Scan)	Die Kommunikation ist nicht verschlüsselt und deshalb besteht die Möglichkeit, dass die ausgedruckten Daten von Dritten gelesen werden können.	Es ist nicht möglich, über das Netzwerk zu scannen.
PC-FAX	Die Kommunikation ist nicht verschlüsselt und deshalb besteht die Möglichkeit, dass Faxdaten im Netzwerk von Dritten gelesen werden können.	Die Funktion PC-FAX kann nicht verwendet werden.

EPSON

Vorsicht

- Dieses Dokument und Teile dieses Dokuments dürfen nicht vervielfältigt werden.
- Der Inhalte dieses Dokuments kann sich ohne vorherige Ankündigung künftig ändern.
- Diese Dokument dient nur internen Zwecke. Lesen Sie das Handbuch jedes einzelnen Produkts zu den Details der Verwendung.

Trademark

- Microsoft is trademark of the Microsoft group of companies.
- Wi-Fi is trademarks of Wi-Fi Alliance.
- Other product names are the trademarks or registered trademarks of their respective companies.

NPD6296-05 DE