EPSON

Guide de sécurité

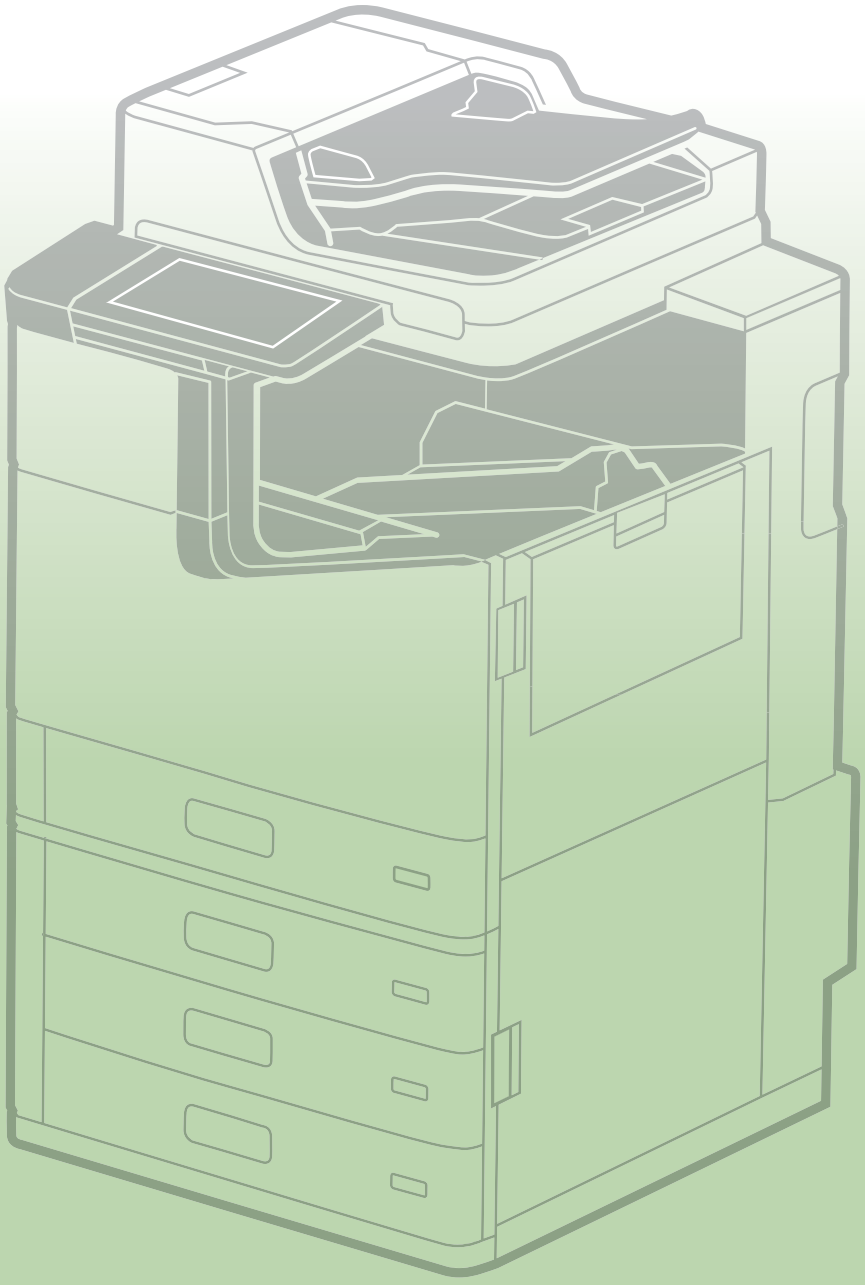


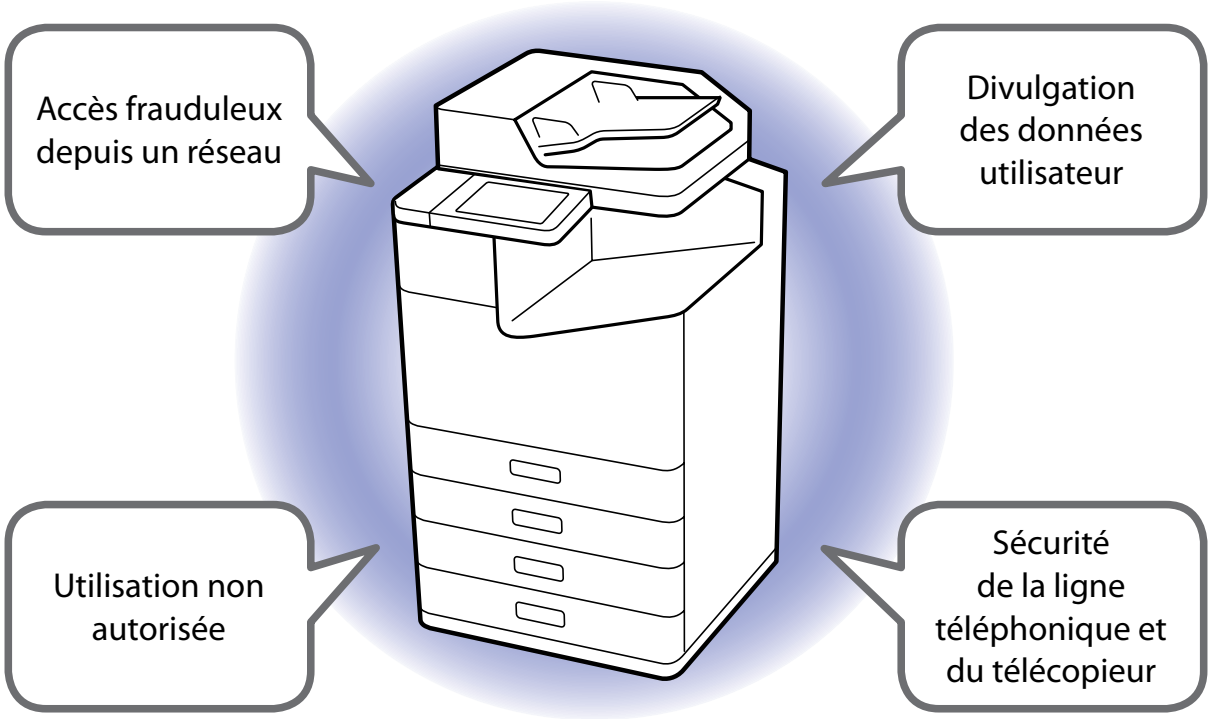
Table des matières

1. Introduction

Chez Epson, nous avons amélioré les fonctionnalités de nos produits compatibles avec le réseau afin d'optimiser le confort des clients.

Parallèlement, la complexité et la sophistication croissantes des cyberattaques de tiers malveillants ont amplifié les menaces pesant sur les appareils connectés au réseau, ce qui soulève des inquiétudes concernant les mesures de sécurité.

Les produits Epson étant équipés de nombreuses fonctionnalités, il est nécessaire de prendre en compte leur sécurité, surtout lorsqu'ils sont connectés à un réseau, comme les ordinateurs et les serveurs.



Ce guide présente l'approche d'Epson en matière de sécurité et de conseils pour le client, et vous guide à travers les fonctions de sécurité disponibles.

Les icônes en regard de chaque fonction dans le texte ont les significations suivantes.

: les fonctions de sécurité comportant cette marque sont les paramètres minimaux devant être exécutés par l'administrateur.

: les fonctions de sécurité comportant cette marque peuvent seulement être configurées par l'administrateur et sont disponibles pour les utilisateurs dans l'environnement de sécurité configuré.

: les fonctions de sécurité comportant cette marque peuvent être définies et utilisées par les administrateurs et les utilisateurs.

: autres fonctions de sécurité. Applicable aux dispositifs de sécurité intégrés dans les produits dans le cadre de leurs spécifications.

Consultez le manuel de votre produit pour savoir comment configurer la sécurité.

Veuillez noter que les fonctions de sécurité et la conformité aux normes de sécurité décrites dans ce guide varient en fonction du produit utilisé. Certains produits peuvent ne pas disposer de ces fonctions ou ne pas être conformes avec ces normes de sécurité. Aussi, assurez-vous de consulter la liste des fonctionnalités dans le Guide de sécurité séparé pour la compatibilité de chaque produit.

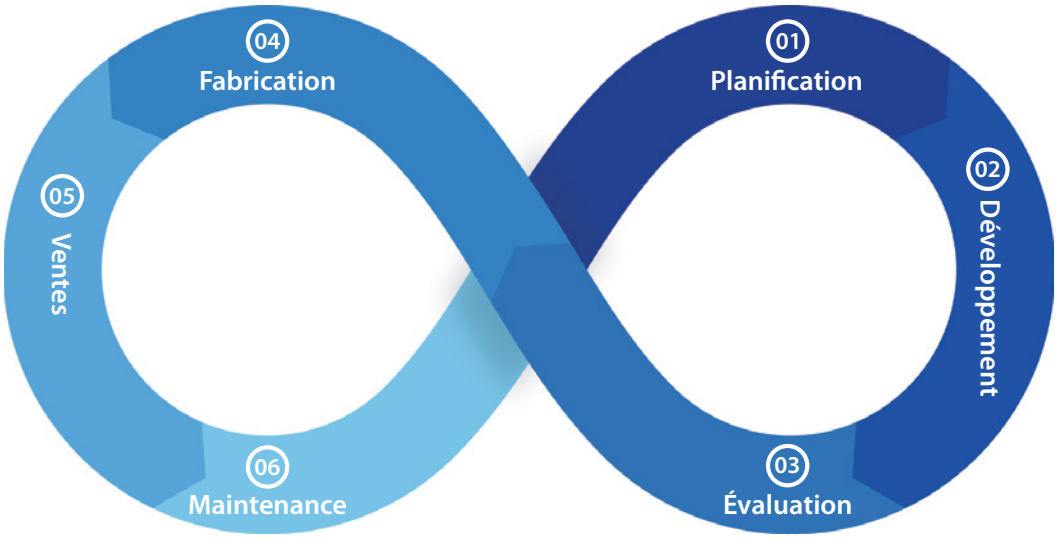
2. Politique de base de sécurité d'EPSON

Chez Epson, nous adoptons l'approche suivante en matière de sécurité afin que nos clients puissent utiliser nos produits en toute sécurité et avec facilité.

2-1. Politique de base

Epson considère la sécurité des produits comme le fondement de la qualité des produits.

Nous assurons la sécurité des produits (terminaux) tout au long du cycle de vie, de la planification, du développement, de l'évaluation, de la fabrication, des ventes, en passant par la maintenance pour garantir que les clients utilisent nos produits dans des conditions plus sûres, en examinant de près les divers environnements d'utilisation pour chaque type de produit.



① Planification

Au stade de la planification des produits, nous surveillons en permanence les dernières tendances en matière de sécurité et les vulnérabilités potentielles. Nous sommes également à l'écoute des demandes de nos clients, et identifions et analysons les exigences liées à la sécurité. Ainsi, nous éliminons les problèmes potentiels dans nos produits avant que les risques ne se matérialisent.

② Développement

En utilisant nos plateformes et technologies communes d'origine cultivées tout au long du développement d'une large gamme de produits, des imprimantes de bureau/domicile aux imprimantes professionnelles/industrielles de petit et grand format, nous nous efforçons d'améliorer la protection contre les risques de sécurité.

③ Évaluation

En plus de tests internes approfondis, nous faisons également appel à des organisations tierces pour une évaluation objective de la sécurité. Avec notre système de vérification de sécurité strict, nous réalisons l'évaluation sous différentes approches afin de garantir une sécurité élevée pour nos produits.

④ Fabrication

Afin de garantir la plus haute qualité de nos opérations de fabrication, nous avons mis en place un système complet de gestion des actifs d'information dans nos usines, où nous installons des logiciels qui permettent à nos produits d'être fonctionnels.

⑤ Ventes

Nous nous engageons à accompagner nos clients en proposant et mettant en œuvre des solutions pour minimiser les risques de sécurité en fonction de l'environnement d'utilisation et des conditions opérationnelles. Nous veillons également à remédier rapidement aux éventuelles vulnérabilités qui pourraient survenir après l'installation de nos produits.

Lorsque les produits doivent être remplacés et éliminés, nous nous assurons de réinitialiser les appareils aux paramètres d'usine par défaut pour éviter des fuites d'informations confidentielles.

⑥ Maintenance

Nous répondons rapidement aux problèmes liés à la sécurité et aux préoccupations signalées par les clients qui achètent nos produits.

2-2. Fournir des informations

Nous fournissons activement des informations à nos clients et les tenons informés des questions de sécurité.

2-3. Assistance pour répondre aux vulnérabilités

Nous luttons constamment contre les vulnérabilités.

- Nous testons la vulnérabilité en utilisant les outils standard de l'industrie et nous nous efforçons d'expédier des produits sans vulnérabilités.
- Nous surveillons régulièrement les informations sur les vulnérabilités des logiciels open source utilisés dans les micrologiciels de nos produits.
- Lorsque de nouvelles vulnérabilités sont détectées, nous les analysons rapidement et fournissons des informations et des contre-mesures.

2-4. Conformité aux codes et normes

Nous nous efforçons de respecter et d'obtenir des normes de sécurité.

3. Ce que vous devez faire lorsque vous installez votre produit

Pour assurer une sécurité optimale, lisez ce qui suit lors de l'installation et configurez les paramètres nécessaires en fonction de votre environnement d'utilisation.

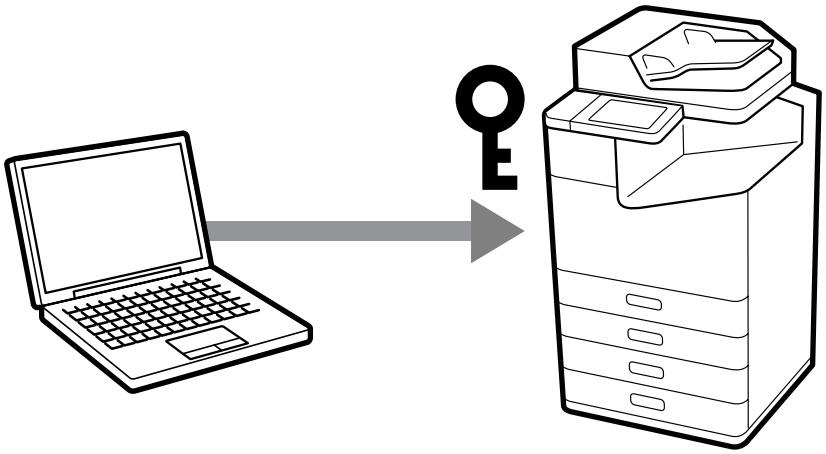
3-1. MdPasse administrateur

Nous vous recommandons fortement de configurer un MdPasse administrateur lors de l'installation de chaque produit.

Les paramètres généraux et les paramètres réseau stockés dans le produit peuvent être consultés ou modifiés illégalement si un MdPasse administrateur n'est pas défini ou si le produit est laissé à ses paramètres d'usine par défaut. Il y a aussi le risque de ne pas protéger les informations personnelles et confidentielles, comme les carnets d'adresses, les noms d'utilisateur et les mots de passe.

Le MdPasse administrateur doit être une chaîne de caractères complexe difficile à deviner pour les autres utilisateurs. Il doit être composé de 8 caractères ou plus, comprenant non seulement des caractères latins, mais aussi des symboles et des chiffres. Vous pouvez configurer le MdPasse administrateur directement dans les paramètres du panneau de commande du produit ou via le réseau.

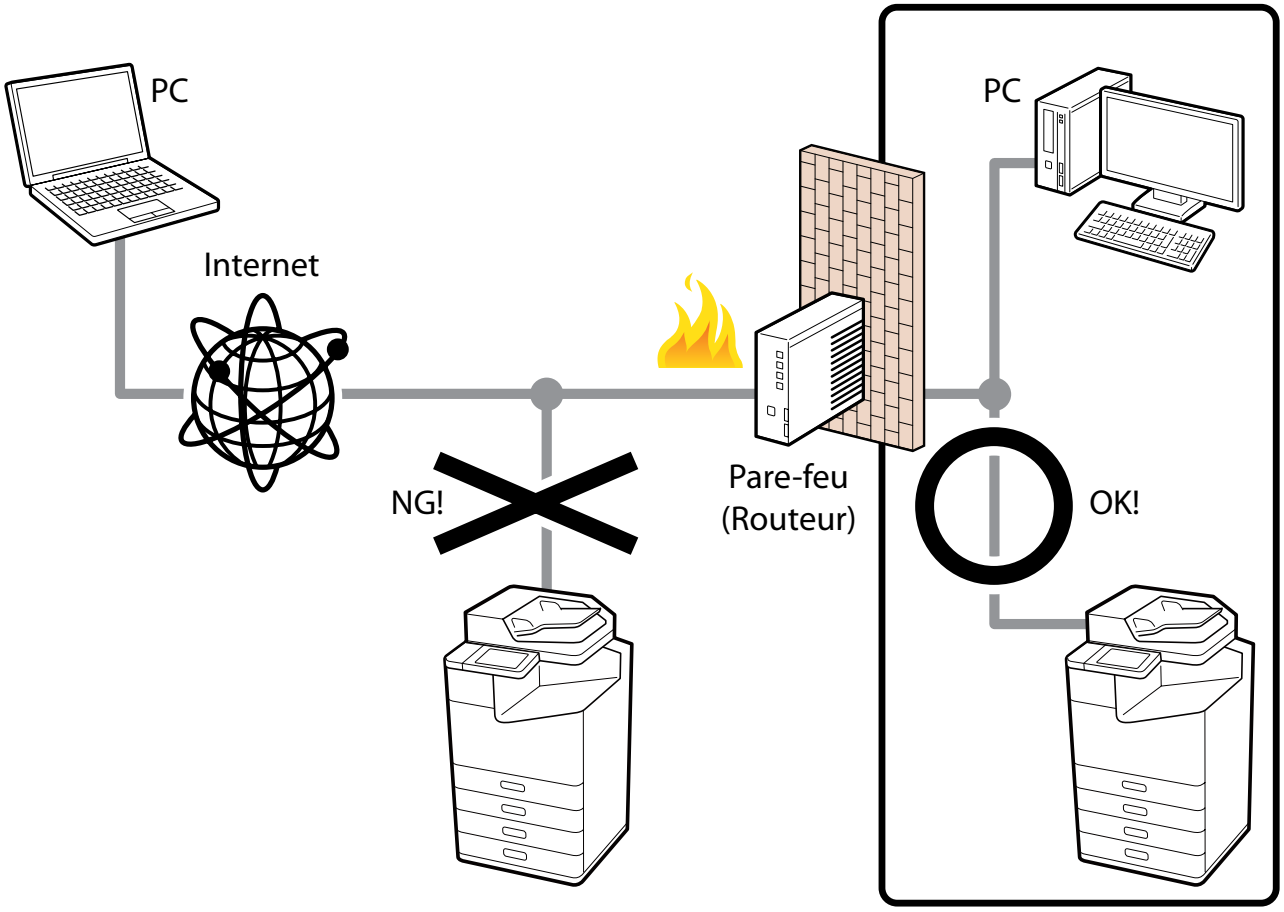
Ainsi, certains produits ont des mots de passe individuels définis à l'usine pour améliorer la sécurité.



3-2. Connexion Internet

Installez les produits sur un réseau protégé par un pare-feu sans vous connecter directement à Internet. Nous vous recommandons alors de configurer et d'utiliser une adresse IP privée.

Même lorsque vous utilisez le produit dans un environnement IPv6, veillez à restreindre l'accès au produit en utilisant un pare-feu ou d'autres moyens pour empêcher l'accès direct au produit depuis Internet.



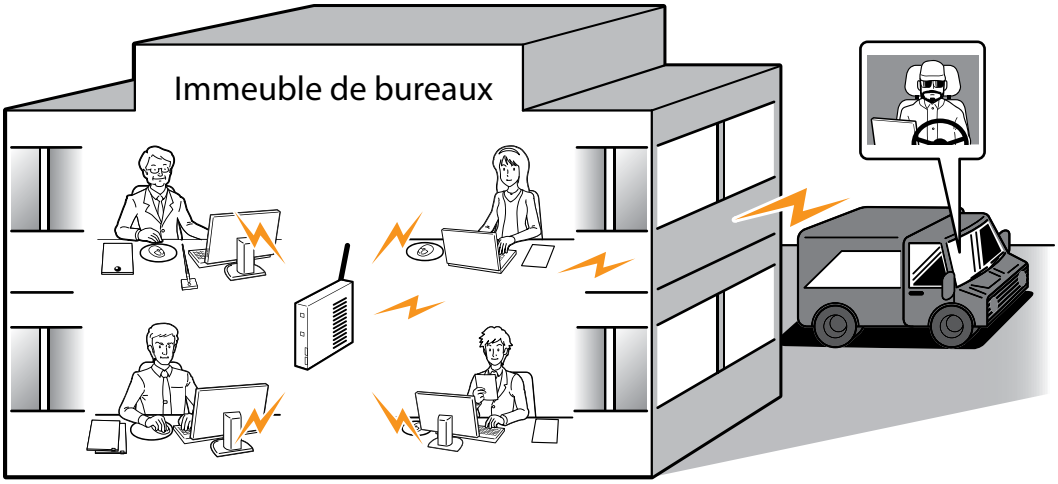
Des interfaces de gestion, comme un écran de gestion Web, sont incluses pour les fonctions réseau des produits ainsi que pour l'impression. Bien qu'Epson effectue des tests de vulnérabilité et s'efforce d'expédier des produits exempts de vulnérabilités, la connexion directe à Internet pose des risques de sécurité inattendus, tels que des opérations non autorisées et des fuites d'informations, pour le réseau du client et les appareils connectés au réseau.

3-3. Réseau local sans fil

Lorsque vous utilisez un réseau local sans fil, configurez la sécurité du réseau local sans fil de manière appropriée.

L'avantage du réseau local sans fil est que vous pouvez vous connecter librement au produit via un réseau pour communiquer avec un ordinateur et des terminaux de téléphone intelligent si vous êtes à portée d'un signal. D'autre part, des problèmes comme suit, causés par des tiers malveillants, peuvent se produire si la sécurité n'est pas correctement configurée.

- Des informations personnelles, telles que vos données d'impression, vos données de numérisation, votre nom d'utilisateur et votre mot de passe, peuvent être vues par d'autres personnes (interceptées).
- Le contenu des communications peut être réécrit frauduleusement (falsifié).
- Certaines personnes ou certains appareils peuvent subir une usurpation d'identité et être utilisés pour la communication (usurpation d'identité).



Consultez le manuel du produit pour connaître la procédure de configuration d'un réseau local sans fil.

3-4. Désactivation des protocoles et fonctions non utilisés

Désactivez les protocoles et fonctions qui ne sont pas utilisés.

Chaque protocole et fonction peuvent être autorisés ou interdits individuellement, ce qui évite les risques de sécurité s'ils sont utilisés involontairement.

3-5. Mise à jour vers les micrologiciels et logiciels les plus récents

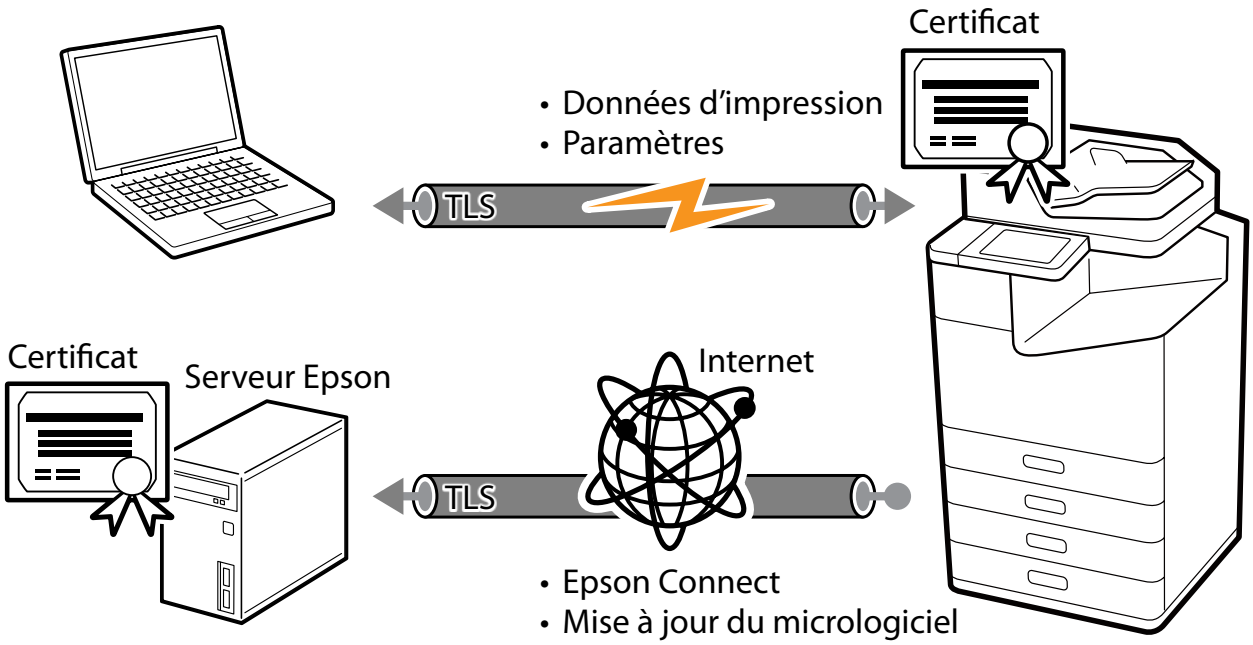
Nous fournissons les micrologiciels et logiciels les plus récents selon les besoins. Assurez-vous d'effectuer une mise à jour vers les micrologiciels les plus récents pour utiliser le produit.

Les micrologiciels et logiciels les plus récents incluent non seulement des fonctionnalités supplémentaires, mais aussi des corrections de défauts et de vulnérabilités. Pour plus d'informations sur les micrologiciels ou les logiciels, consultez l'historique des modifications des micrologiciels ou des logiciels.

4. Sécurité réseau

4-1. Communication TLS

Étant donné que les transmissions sont protégées par TLS, vous pouvez empêcher la divulgation des informations de configuration et du contenu des données d'impression en utilisant le protocole IPPS pour l'impression et la configuration de votre produit via votre navigateur. Vous pouvez également empêcher l'envoi d'informations à des périphériques non autorisés à l'aide de la fonction de validation du serveur, de l'importation du certificat signé CA et de l'utilisation de l'infrastructure à clés publiques (ICP) interne. La force du cryptage peut être configurée pour utiliser un algorithme de chiffrement beaucoup plus sûr. Vous êtes également protégé par TLS lorsque vous accédez au serveur Epson sur Internet via le produit pour Epson Connect et les mises à jour du micrologiciel.



Vous pouvez sélectionner la version et la force de cryptage du TLS à utiliser.

Les versions du TLS prises en charge et les forces du cryptage sont les suivants.

Version du TLS

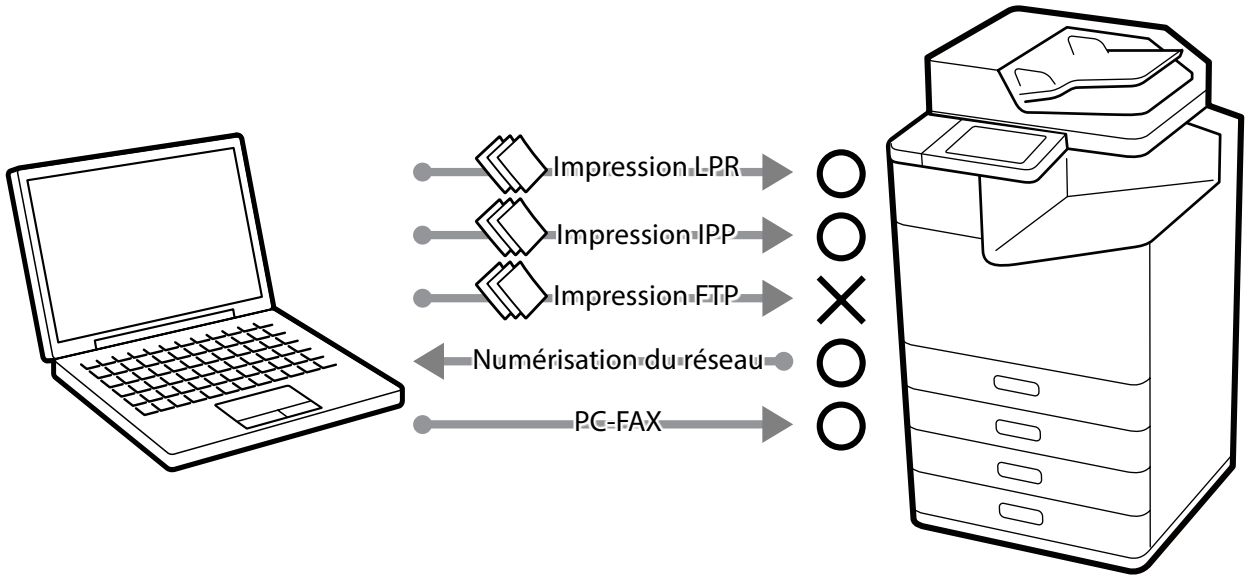
- TLS1.1
- TLS1.2
- TLS1.3

Force du cryptage

- 80 octets
- 112 octets
- 128 octets
- 192 octets
- 256 octets

4-2. Contrôle des autorisations et des exclusions de protocole

Le produit communique via différents protocoles lors de l'impression, de la numérisation et de l'envoi d'un PC-FAX. Vous pouvez prévenir les risques de sécurité liés à une utilisation non intentionnelle avant qu'ils ne se produisent en définissant des autorisations et des interdictions individuelles pour chaque protocole.



Voir l'annexe pour les risques de sécurité lorsque les protocoles et les fonctionnalités sont activés et pour les limitations lorsqu'ils sont désactivés.

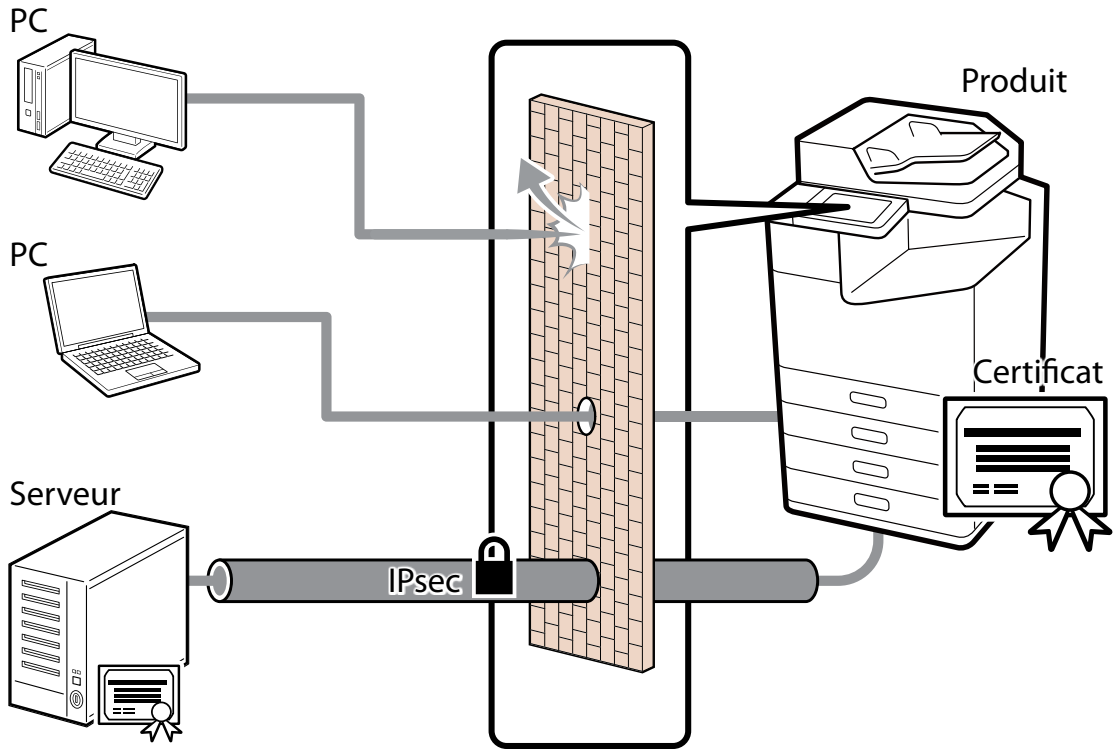
Les protocoles et fonctionnalités pouvant être autorisés ou interdits sont les suivants.

- Bonjour
- SLP
- WSD
- LLTD
- LLMNR
- LPR
- RAW (Port 9100/Port personnalisé)
- IPP/IPPS
- FTP
- SNMP
- SSL/TLS
- Partage de réseau Microsoft
- Numérisation en réseau (EPSON Scan)
- PC-FAX

4-3. IPsec/filtrage IP

Vous pouvez filtrer les adresses IP, les types de services, les numéros de port de réception et de transmission, etc. en utilisant la fonction IPsec/filtrage IP. Selon la combinaison de ces filtres, vous pouvez décider d'accepter ou de bloquer les données d'un client particulier et d'accepter ou de bloquer des types de données spécifiques. De même, vous pouvez communiquer avec une sécurité renforcée en combinant les protections en utilisant IPsec.

Les protocoles d'impression non sécurisés et les protocoles de numérisation deviennent également des objets protégés car la protection dans les unités de paquets IP (cryptage et certificat) est incluse dans la protection en utilisant IPsec. Les clés prépartagées et certificats sont pris en charge dans les méthodes d'authentification IPsec.



Les algorithmes et les méthodes d'échange de clés pris en charge sont les suivants :

Méthode d'échange de clés

- IKEv1
- IKEv2

Algorithme de chiffrement ESP

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

- AES-GCM-256
- 3DES

Algorithme d'authentification ESP/AH

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

La politique de base concerne tous les utilisateurs qui accèdent au produit. Configurez des stratégies individuelles pour contrôler l'accès en fonction de vos besoins spécifiques.

4-4. Authentification IEEE 802.1X

IEEE 802.1X est une norme destinée à contrôler l'accès à chaque port du périphérique réseau. Les réseaux IEEE 802.1X sont constitués de serveurs RADIUS (serveurs d'authentification) et de hubs de commutation dotés d'une fonction d'authentification.

Les produits Epson sont conformes à la norme IEEE 802.1X et peuvent être connectés à un environnement réseau contenant des informations confidentielles.

Les méthodes d'authentification et les algorithmes de chiffrement suivants sont pris en charge :

Méthode d'authentification

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

Algorithme de chiffrement

- AES128
- AES256
- 3DES
- RC4

4-5. SNMP

SNMP est un protocole de surveillance du statut et des modifications des paramètres des équipements et outils de gestion pris en charge.

SNMPv1 et SNMPv2c ne prennent pas en charge le cryptage des communications et doivent être utilisés dans un réseau protégé par un pare-feu ou quelque chose de similaire. De plus, pour utiliser les communications SNMP, modifiez le nom de la communauté par défaut.

SNMPv3 peut être utilisé pour authentifier et chiffrer les communications SNMP (paquets) pour surveiller l'état et configurer les modifications avec des outils de gestion de périphériques compatibles. Cela peut assurer la confidentialité lors de la modification des paramètres ou du statut de surveillance sur le réseau.

SNMPv3 prend en charge les algorithmes d'authentification et de cryptographie suivants.

Algorithmes d'authentification SNMPv3

- MD5
- SHA-1

Algorithme de chiffrement SNMPv3

- DES
- AES128

4-6. SMB

SMB est un protocole de partage de fichiers sur un réseau.

SMB1.0 et SMB2.0 ne prennent pas en charge le cryptage des communications et doivent être utilisés dans un réseau protégé par un pare-feu ou quelque chose de similaire.

SMB3.0 peut être utilisé pour authentifier et chiffrer les communications SMB (paquets) avec des périphériques compatibles. Cela peut assurer la confidentialité du partage de fichiers sur le réseau.

4-7. WPA3

Le produit prend en charge WPA3 qui est la dernière technologie d'authentification et de cryptage pour le Wi-Fi (réseau local sans fil). WPA3 fournit une protection plus robuste et plus forte pour protéger vos données sur le réseau sans fil.

4-8. Séparation entre les interfaces

Le produit comprend une interface USB, une interface réseau local câblée standard, une interface réseau local câblée supplémentaire, une interfacede réseau local sans fil et une interface de fax. Chaque interface est indépendante, limitant l'accès aux protocoles pouvant être traités par cette interface et ne fournissant aucune capacité de transfert ou de routage direct. Par exemple, l'accès à partir d'une ligne téléphonique publique (ligne de télécopie) est limité au traitement selon les procédures de communication par télécopieur. Toute déviation de cette procédure entraînera la déconnexion de la communication en tant qu'erreur, de sorte qu'il n'y a aucun risque d'accès non autorisé. En outre, les données de fax reçues sont vérifiées comme des données d'image avant d'être importées. Il n'y a aucun risque que des logiciels malveillants plantent à cause de la fonction de transfert via le produit qui pourrait conduire à une contamination par un virus ou un accès non autorisé. Seuls les utilisateurs autorisés peuvent exécuter la fonction de transfert. Par exemple, l'intrusion du réseau à partir d'une ligne téléphonique publique via le produit ; l'accès à un réseau local filaire à partir d'un réseau local sans fi ; ou l'accès non autorisé à partir d'Internet au produit connecté à un ordinateur via un port USB.

5. Protection de votre produit

5-1. Bloquer la connexion USB de l'ordinateur

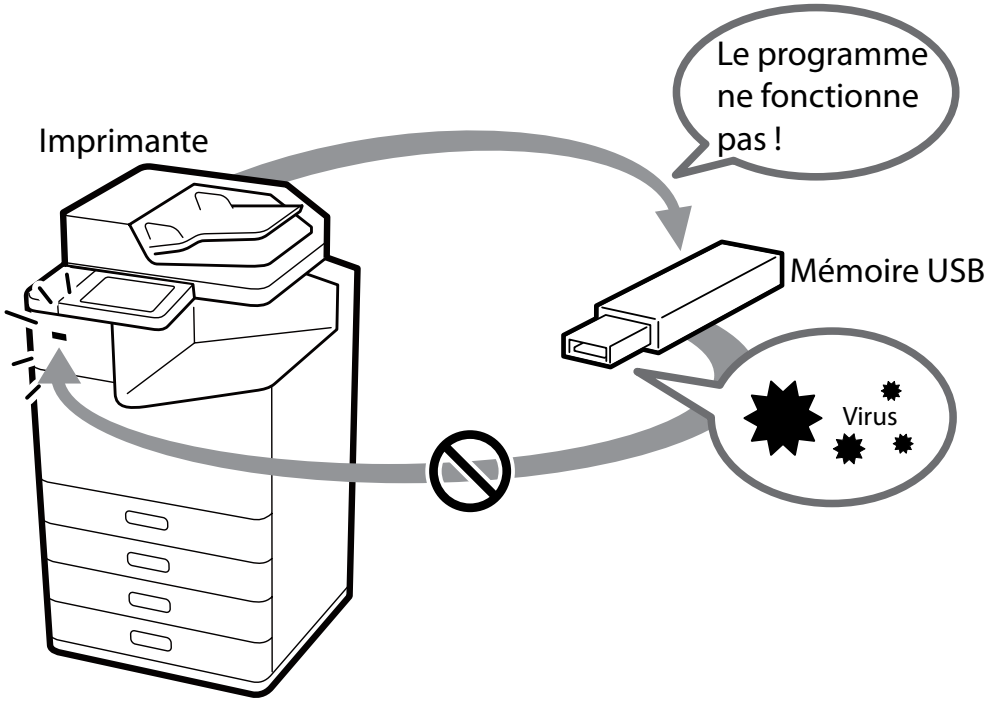
Vous pouvez désactiver l'accès au produit via une connexion USB à partir d'un ordinateur. Définissez cette option pour interdire l'impression ou la numérisation par une connexion directe à un ordinateur par un câble USB.

5-2. Désactivation de l'interface externe

Vous pouvez désactiver les cartes mémoire et les interfaces de mémoire USB. Cela vous permet d'éviter la duplication illégale de données par la numérisation non autorisée de documents confidentiels au bureau.

5-3. Gestion des virus introduits par la mémoire USB

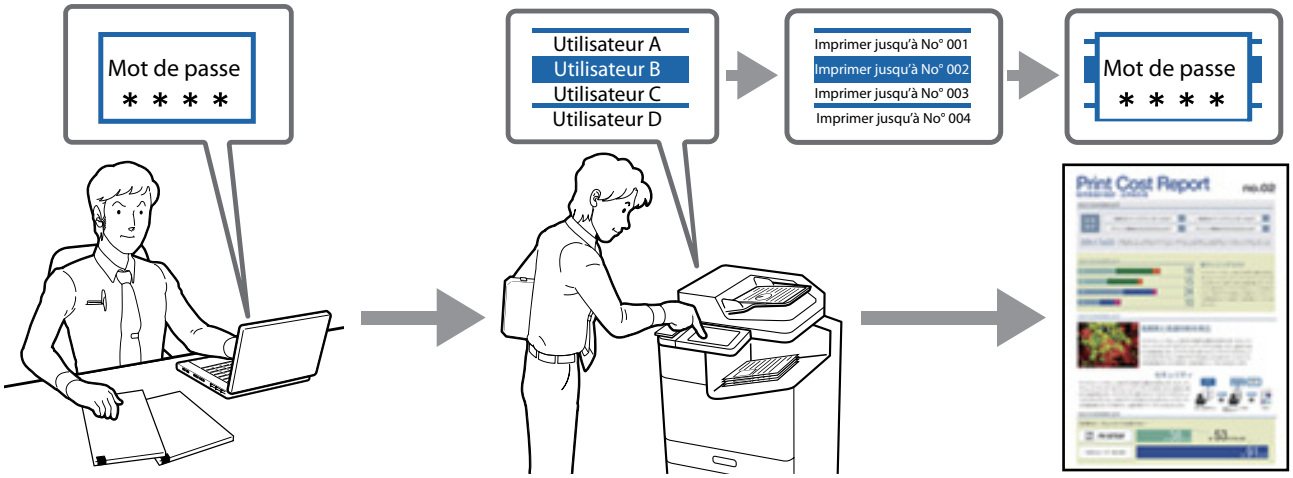
Comme il n'y a pas de fonctions exécutables sur les mémoires USB pour les produits Epson, il n'y a aucun risque que le produit soit infecté par des virus via la mémoire USB.



6. Sécurité d'impression et de numérisation

6-1. Tâches confidentielles

Vous pouvez assurer la confidentialité des documents et empêcher les personnes non autorisées de voir la sortie sans surveillance sur le périphérique en soumettant vos documents en tant que « Tâche confidentielle ».



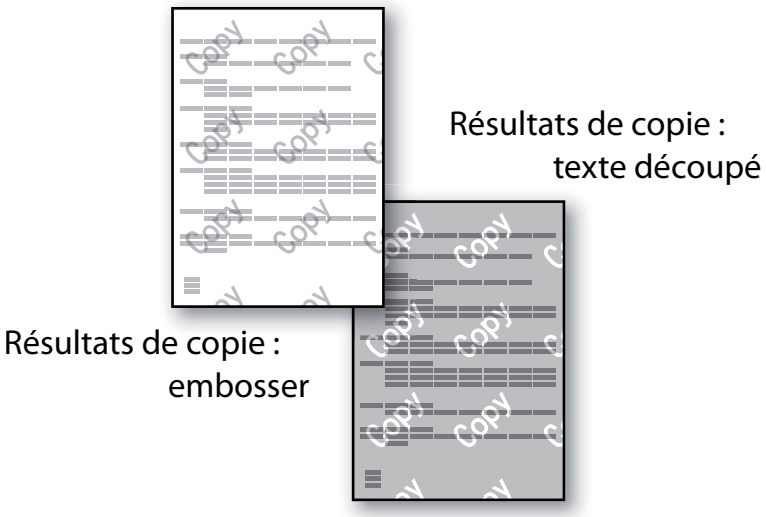
Saisissez un mot de passe à imprimer.

Choisissez une tâche d'impression sur le produit et saisissez le mot de passe.

L'impression est terminée.

6-2. Motif anti-copie

Vous pouvez protéger l'originalité d'un document avec l'impression de filigrane anti-copie qui crée un motif de filigrane transparent sur la sortie d'origine. Le filigrane transparent devient visible lorsque la sortie originale est utilisée pour réaliser des copies.



Résultats de copie : texte découpé

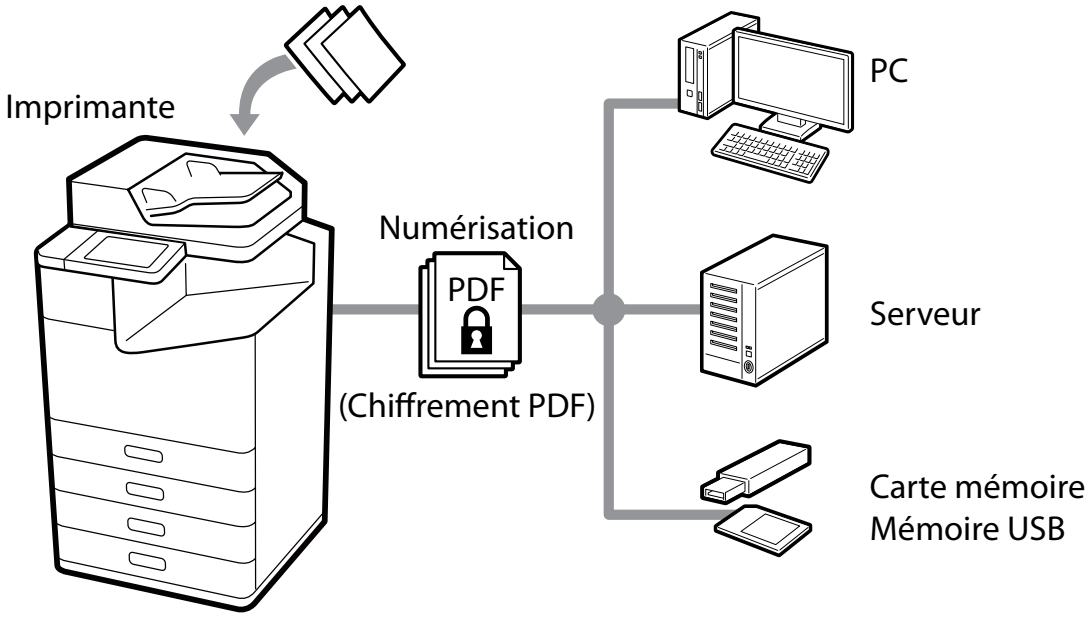
Résultats de copie : embosser

6-3. Filigrane

Des filigranes tels que classifiés et importants (au format texte ou BMP) peuvent être superposés sur les documents. Vous pouvez également choisir un « nom d'utilisateur » ou un « nom de l'ordinateur ». Rappeler au destinataire de manipuler les documents avec précaution dissuade toute utilisation non autorisée.

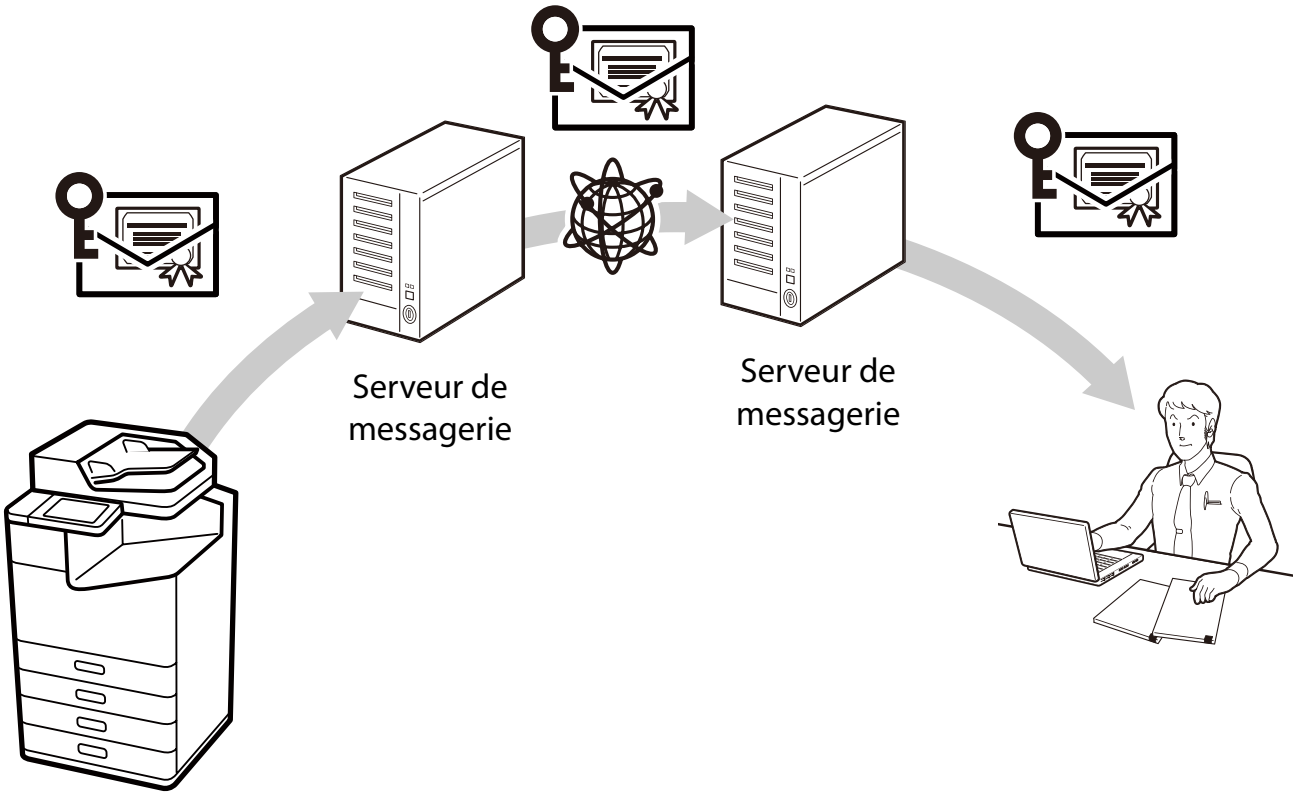
6-4. Chiffrement PDF

Vous pouvez numériser un document dans un fichier PDF protégé par mot de passe. Cela peut empêcher des tiers de consulter des documents sans autorisation.



6-5. S/MIME

L'utilisation de S/MIME vous permet d'ajouter une signature numérique et/ou de chiffrer un e-mail pour Numér. vers email et Fax vers e-mail. Même si un email passe par plusieurs serveurs de messagerie, vous pouvez protéger l'email contre la falsification, l'interception ou l'altération. S/MIME préservera l'authenticité et l'intégrité du message tout en protégeant la sécurité des données et la non-répudiation durable.



Les algorithmes pris en charge sont les suivants.

Algorithme de chiffrement

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

Algorithme de hachage de signature numérique

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

6-6. Restrictions de domaine

En appliquant des règles de restriction aux noms de domaine des adresses e-mail, vous pouvez réduire le risque de transmissions erronées et de fuites d'informations pour les fonctions Numér. vers email et Transfert de télécopies par email.

6-7. Assistance pour les mots de passe à longue authentification

De nos jours, il est recommandé de définir des mots de passe longs pour augmenter la sécurité des mots de passe. Vous pouvez définir un maximum de 70 caractères comme mot de passe d'autorisation utilisé pour Numér. vers dossier réseau/FTP, Numér. vers email, Notification par email. Vous pouvez définir une politique de mot de passe pour les mots de passe plus longs pour les serveurs de fichiers et les serveurs de messagerie.

6-8. Restrictions de l'accès aux fichiers à partir du PDL

En désactivant l'accès aux fichiers à partir de PDL (langue de description de la page), vous pouvez éviter le risque de fuites d'informations provenant de données d'impression malveillantes qui volent des fichiers à l'intérieur de l'imprimante. Même si des données d'impression malveillantes sont transmises, le produit peut être utilisé en toute sécurité sans que les fichiers ne soient lus.

6-9. Impression sécurisée

Si vous souhaitez protéger la sécurité des routes de transmission pour l'impression, vous pouvez utiliser un IPPS chiffré via TLS.

7. Sécurité de la télécopie

7-1. Restrictions de numérotation directe

Si vous souhaitez saisir un numéro de fax directement à l'aide du clavier numérique, vous pouvez le configurer de sorte que le fax n'effectue des envois que si vous saisissez le destinataire deux fois correctement. Vous pouvez également le configurer de sorte que la saisie d'un numéro de téléphone directement à l'aide du clavier numérique soit interdite et que les télécopies ne soient envoyées que par une seule touche de numérotation et aux adresses enregistrées dans votre carnet d'adresses. Cela peut réduire le risque de fuites d'informations dues à de mauvaises transmissions en raison d'erreurs dans la saisie des numéros de téléphone.

7-2. Confirmation de la liste d'adresses

Vous pouvez confirmer l'adresse sélectionnée avant d'envoyer une télécopie. Cela peut réduire le risque de divulgation d'informations provenant de transmissions erronées en raison d'erreurs lors de la spécification d'une adresse.

7-3. Détection de tonalité

Vous pouvez empêcher les mauvaises transmissions en envoyant des fax après avoir confirmé la détection d'une tonalité.

Selon votre pays ou votre région, il se peut que la détection de la tonalité ne soit pas possible.

7-4. Mesures contre les télécopies abandonnées

« Imprimer la télécopie après l'affichage » peut être configuré pour enregistrer une télécopie reçue dans la boîte de réception (réception en mémoire) et l'imprimer après l'avoir confirmée sur le panneau de commande. Cela empêche la divulgation d'informations et la perte de documents imprimés provenant des fax reçus du fait que les fax imprimés sont laissés sans surveillance.

En outre, vous pouvez empêcher l'impression et la suppression arbitraires par des utilisateurs non autorisés en le configurant de sorte qu'un mot de passe soit requis pour accéder à la boîte de réception.

7-5. Rapport de confirmation de transmission

Vous pouvez confirmer qu'une télécopie a bien été envoyée à l'adresse correcte en imprimant des rapports qui confirment les détails de la transmission, tels qu'un rapport de résultats d'envoi, un transfert de résultats d'envoi et un rapport de gestion d'envoi.

7-6. Suppression des données de sauvegarde pour les télécopies reçues

Les données de sauvegarde* pour les télécopies reçues peuvent être supprimées du panneau de commande. Vous pouvez également le configurer de manière à ce que les données de sauvegarde soient automatiquement supprimées, ce qui empêche les réimpressions non autorisées des données des télécopies reçues.

* Les données de sauvegarde pour les télécopies reçues sont enregistrées dans le produit (paramètres d'usine par défaut) afin que vous puissiez réimprimer les télécopies dans les cas où les résultats d'impression ne sont pas clairs ou où les résultats d'impression sont perdus.

7-7. Limite d'envoi à plusieurs destinataires

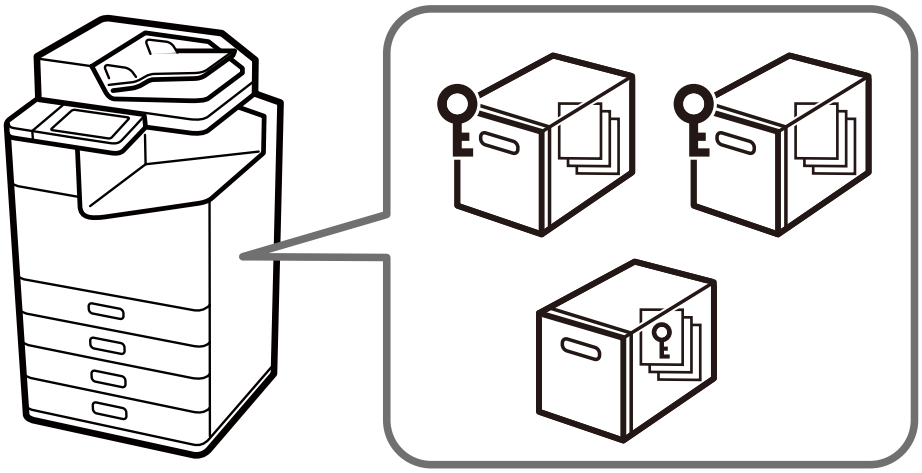
Vous pouvez définir le produit de sorte qu'un seul destinataire puisse être sélectionné.

En rendant impossible la spécification de plusieurs destinataires, vous pouvez réduire le risque d'envoyer une télécopie à un destinataire erroné et de divulguer des informations.

8. Protection des données des utilisateurs

8-1. Sécurité du stockage

Vous pouvez définir des mots de passe uniques pour les dossiers et les documents partagés sur des modèles avec des dossiers partagés. Ces mots de passe peuvent empêcher la divulgation d'informations, les pertes et la falsification non autorisée.
Le fonctionnement du dossier peut également être soumis à un contrôle d'accès. Si les dossiers partagés ne sont pas utilisés, vous pouvez également interdire l'utilisation de la fonction de dossier partagé.



8-2. Protection de votre carnet d'adresses

Vous pouvez empêcher la fuite et l'altération non autorisée des informations du carnet d'adresses car un MdPasse administrateur est requis pour la modification par lot des carnets d'adresses stockés dans le produit (lorsqu'un MdPasse administrateur a été défini). En outre, étant donné que les carnets d'adresses peuvent être exportés sous forme de fichier crypté, vous pouvez empêcher la divulgation de renseignements personnels, tels que des numéros de fax et des adresses e-mail, lors du remplacement ou de la sauvegarde du produit.

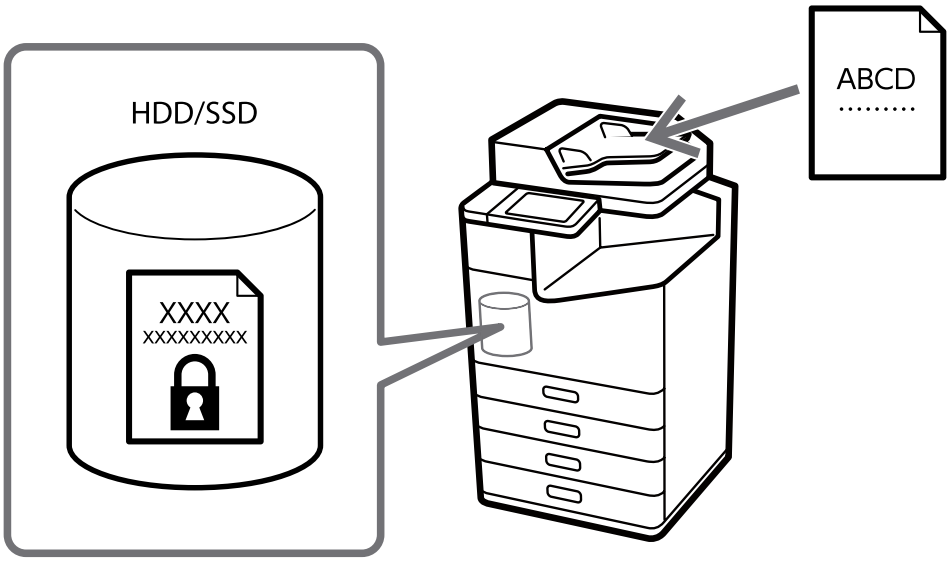
8-3. Traitement des données traitées par un produit

Les données des fonctions d'impression, de copie et de numérisation sont enregistrées temporairement dans un produit, puis effacées lorsqu'une tâche est terminée ou que le produit est désactivé. Les données de télécopie sont effacées lors de l'envoi ou de la réception de télécopie. Notez que même si les fax reçus sont enregistrés en tant que données et conservés par la fonction de sauvegarde, vous pouvez modifier le paramètre de sorte que les données soient automatiquement effacées (voir 7-6).

8-4. Chiffrement des données enregistrées sur le disque dur/SSD

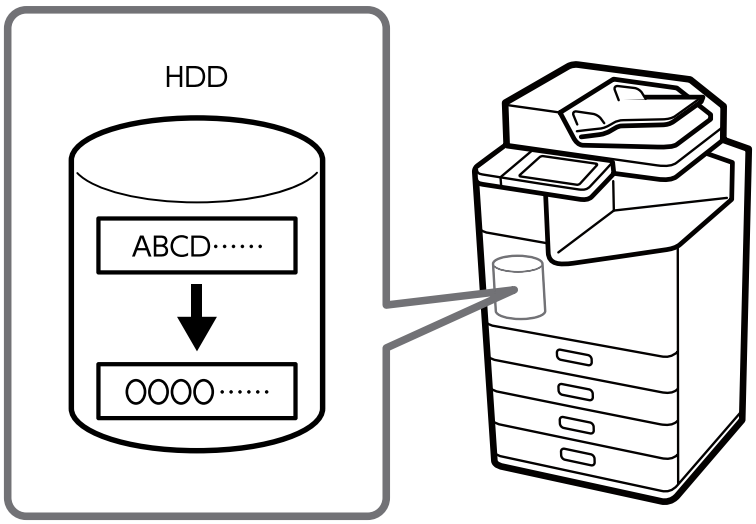
Nous protégeons toujours les données des clients avec un cryptage lors de l'enregistrement de données sur un disque dur/SSD interne sur un produit. Dans le cas peu probable d'une attaque par un tiers malveillant, le contenu des données stockées ne sera pas visible. Le disque dur/SSD est livré avec un lecteur auto-crypté et les données du document sont cryptées avec AES-256.

Le cryptage des données empêche tout accès non autorisé ou attaque malveillante des données personnelles en cas de vol du disque dur/SSD.



8-5. Suppression séquentielle des données de travail

Lorsque cette fonction est activée, les données de travail stockées temporairement sur le disque dur de l'unité sont automatiquement effacées après avoir été écrasées avec un motif spécial. Cela empêche les tiers malveillants de récupérer des données à partir de données résiduelles de la tâche.



8-6. Chiffrement mot de passe

Vous pouvez chiffrer les mots de passe stockés dans le produit. Les informations chiffrées sont les suivantes :

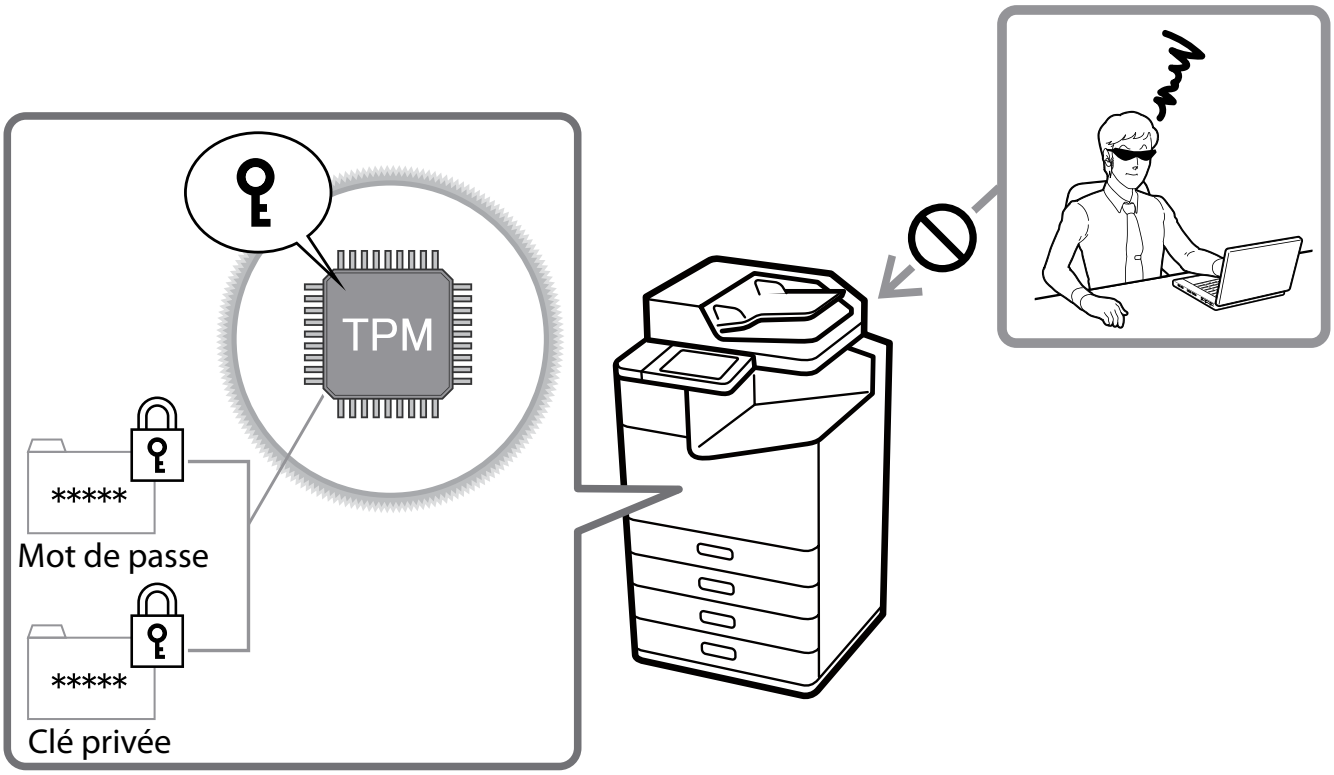
- MdPasse administrateur
- Mots de passe utilisateur pour le contrôle d'accès
- Clés d'authentification de disque dur, clés privées de certificat, etc. Mots de passe pour accéder à Numér. vers dossier réseau/FTP

8-7. TPM

Pour les modèles équipés d'un TPM (Trusted Platform Module), les clés de chiffrement pour la restauration des mots de passe cryptés et des informations de clé privée sont stockées sur la puce TPM. Il est impossible d'accéder à la puce TPM depuis l'extérieur de l'imprimante, ce qui la protège d'une analyse non autorisée au niveau du matériel.

Les nombres aléatoires réels du TPM sont utilisés pour les nombres aléatoires utilisés pour les configurations via des sessions de navigateur (Web Config). Les vrais nombres aléatoires du TPM sont également utilisés pour générer des clés d'authentification pour le disque dur/SSD chiffré.

Ces modèles sont équipés de puces de spécification TPM2.0.



8-8. Mirroring du disque dur

Si une option de disque dur supplémentaire est installée, même en cas de dysfonctionnement d'un disque dur, toutes les fonctions peuvent être poursuivies avec l'autre disque dur sans perte de données stockées.

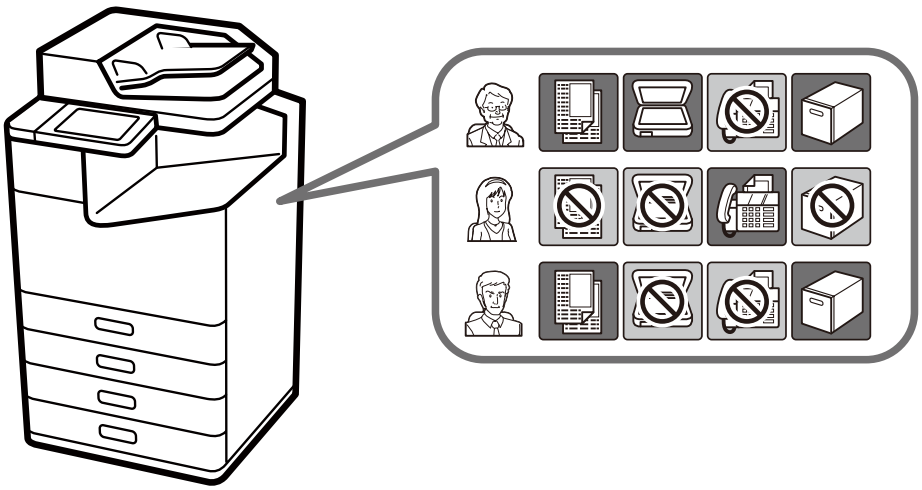
9. Limitation opérationnelle

9-1. Verrouillage du panneau

Lorsque vous utilisez le verrouillage du panneau, vous devez saisir le MdPasse administrateur pour accéder au panneau de configuration. Lorsque le panneau est protégé par le MdPasse administrateur dans les bureaux ouverts, les installations publiques et les endroits similaires, vous pouvez empêcher les utilisateurs de modifier les paramètres.

9-2. Contrôle d'accès

Vous pouvez restreindre l'utilisation des fonctions d'impression, de numérisation, de copie, de télécopie* et de box pour les utilisateurs individuels afin de minimiser les risques de sécurité en fonction de leurs rôles et fonctions. En outre, les utilisateurs sont automatiquement déconnectés après avoir été inactifs dans le panneau de configuration après une durée spécifiée.



* Il est seulement possible de limiter la transmission par télécopie.

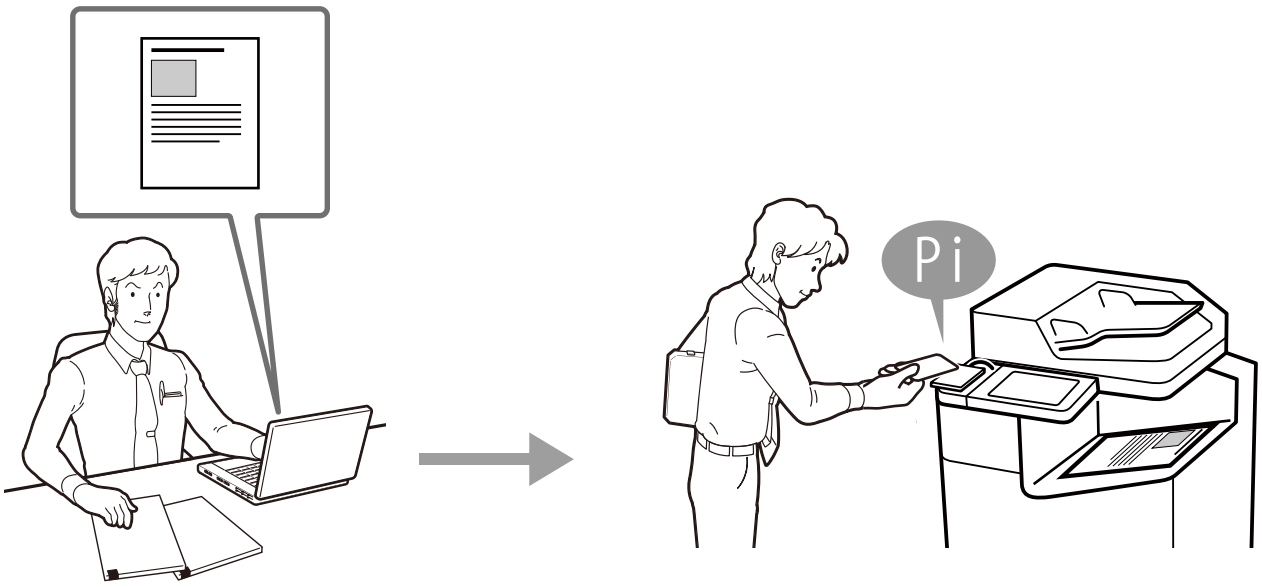
9-3. Impression et numérisation authentifiées

Lorsque l'option Epson Print Admin ou Epson Print Admin Serverless est installée, vous pouvez utiliser des dispositifs d'authentification, tels que l'authentification ID/mot de passe et les lecteurs de carte IC, pour authentifier les utilisateurs qui impriment ou numérisent. Les utilisateurs qui effectuent des opérations d'authentification et de contrôle devant le produit évitent la fuite d'informations provenant de documents imprimés ou non surveillés que des personnes ramassent par erreur.

Les utilisateurs liés par LDAP et enregistrés sur l'imprimante peuvent utiliser cette méthode d'authentification.

En outre, avec certains scanners autonomes, vous pouvez authentifier la numérisation par ID/mot de passe d'authentification ou des dispositifs d'authentification, tels que les lecteurs de cartes IC, en utilisant l'authentification de l'unité principale ou Document Capture Pro Server Authentication Edition.

Les utilisateurs liés par LDAP et enregistrés sur l'imprimante peuvent utiliser cette méthode d'authentification.



9-4. Politique de Mot de passe

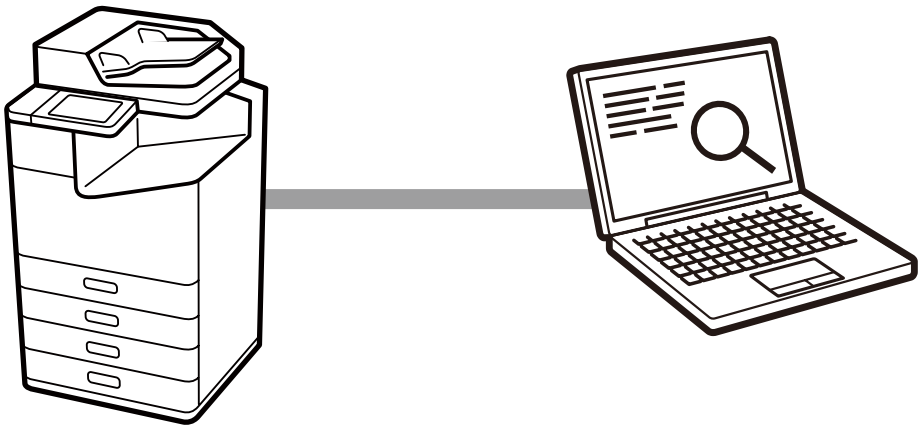
La politique de Mot de passe peut être appliquée pour les mots de passe de l'administrateur, le contrôle d'accès et le fax. Un mot de passe fort qui nécessite plusieurs des conditions suivantes peut aider à empêcher le craquage de mot de passe par des pirates.

- Nombre minimum de caractères pour les mots de passe.
- Inclure/ne pas inclure de lettres majuscules en anglais dans les mots de passe.
- Inclure/ne pas inclure de lettres minuscules en anglais dans les mots de passe.
- Inclure/ne pas inclure de chiffres dans les mots de passe.
- Inclure/ne pas inclure de symboles dans les mots de passe.

9-5. Journal d'audit

La fonction de journal d'audit peut enregistrer les historiques d'impression, de copie, de numérisation, de télécopie et de modification des paramètres à des fins d'audit. Elle peut aider les résultats précédents pour une mauvaise utilisation et la trace de problèmes de sécurité avec la confirmation périodique de ce journal.

Jusqu'à 20 000 journaux d'audit (5 000 pour certains modèles) sont conservés.



10. Sécurité du produit

10-1. Mise à jour automatique du micrologiciel

Si les mises à jour automatiques du micrologiciel sont activées, le micrologiciel peut être mis à jour automatiquement à une heure spécifiée. Comme les mises à jour ont lieu à un moment précis, vous pouvez toujours utiliser le dernier micrologiciel sans interrompre les opérations.

10-2. Protection contre les mises à jour illégales du micrologiciel

L'authentification avec le MdPasse administrateur est effectuée lors des mises à jour du micrologiciel. De plus, la communication des données avec le produit est protégée par HTTPS et le micrologiciel envoyé au produit lui-même est vérifié comme étant légitime par signature avant que le micrologiciel ne soit réécrit. Cela empêche toute modification non autorisée du micrologiciel par des tiers malveillants.

10-3. Démarrage sécurisé

Au démarrage, le système vérifie que le micrologiciel du produit est légitime par signature. S'il détecte que le micrologiciel a été réécrit et qu'il s'agit d'un micrologiciel non autorisé, il arrête le démarrage et invite l'utilisateur à mettre à jour le micrologiciel.

10-4. Détection d'infiltration de logiciels malveillants

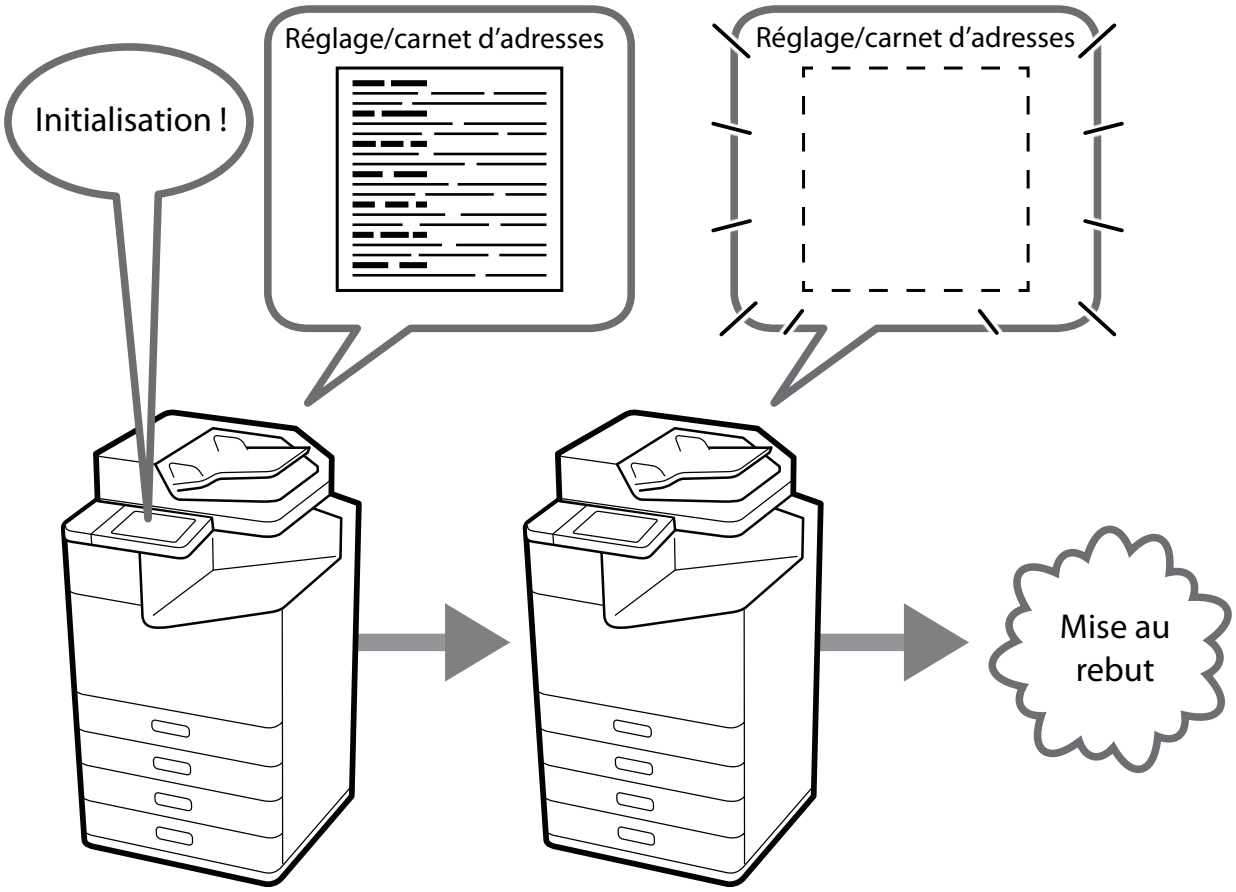
Le produit est constamment surveillé pour l'infiltration de logiciels malveillants dans le micrologiciel pendant le fonctionnement du produit. Si un malware est détecté, le produit est redémarré pour éliminer le malware.

11. Mesures de sécurité lorsque vous jetez votre produit

11-1. Restaurer les paramètres d'usine par défaut

Lors du transfert ou de la mise au rebut d'un produit, vous pouvez rétablir tous les paramètres (y compris sur le disque dur/SSD interne) par défaut (initialisation) pour empêcher la divulgation d'informations confidentielles.

De plus, le disque dur/SSD peut être effacé soit par « effacement en changeant la clé de chiffrement à l'intérieur du lecteur d'autochiffrement (High Speed) », soit par « effacement en changeant la clé de chiffrement et en écrasant avec un motif spécial (Overwrite, Triple Overwrite) ».



12. Certification et normes de sécurité

12-1. ISO15408/IEEE 2600.2™

Le produit a acquis la certification ISO/IEC 15408 pour la conformité avec IEEE Std. 2600.2™-2009[*1], une norme internationale pour la sécurité de l'information.

IEEE Std. 2600.2™

IEEE Std. 2600.2™ est une norme internationale qui spécifie des critères de sécurité de l'information pour les imprimantes multifonction. La sécurité des imprimantes multifonction peut être entièrement renforcée en fournissant des fonctionnalités de sécurité conformes aux normes, telles que l'identification et l'authentification des utilisateurs, le contrôle d'accès, l'écrasement des données, la protection du réseau, la gestion de la sécurité, l'auto-test et les journaux d'audit.

ISO/IEC 15408

ISO/IEC 15408, également appelée Critères communs (CC), est une norme internationale pour l'évaluation indépendante et objective des mesures de sécurité dans les produits et systèmes informatiques afin de déterminer si ces mesures sont correctement conçues et mises en œuvre.

Les versions spécifiées du micrologiciel, des manuels et d'autres composants sont évaluées pour la certification ISO/IEC 15408. La version du micrologiciel d'un produit acheté peut différer de la version certifiée.

Il peut y avoir des limitations sur la fonctionnalité du produit lors de l'utilisation d'une version certifiée.

Le logo de certification de l'ADRC indique que le produit a été évalué et certifié conformément au Système japonais d'évaluation et de certification de la sécurité des technologies de l'information (JISEC[*2]).
Il n'implique pas une garantie que le produit est complètement exempt de vulnérabilités. Cela ne signifie pas non plus que le produit est équipé de toutes les fonctions de sécurité nécessaires dans chaque environnement opérationnel.

*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 (Japan Information Technology Security Evaluation and Certification Scheme)

Risques de sécurité lorsque les fonctions du protocole sont activées et limitations lorsqu'elles sont désactivées

Protocole/ fonctions de sécurité	Risques de sécurité lorsqu'elles sont activées	Limitations lorsqu'elles sont désactivées
Bonjour	Il est possible que des informations sur les appareils du réseau puissent être lues par un tiers.	Les recherches par Bonjour ne seront pas possibles à partir de l'ordinateur.
SLP	Comme l'expéditeur n'est pas authentifié, si l'expéditeur est usurpé, il peut être exploité dans une attaque pour désactiver le service.	L'ordinateur ne pourra pas utiliser le SLP pour récupérer ou explorer des informations sur l'appareil.
WSD	Comme la communication n'est pas cryptée, il est possible que les données imprimées puissent être lues par un tiers.	Il ne sera pas possible d'imprimer et de numériser en utilisant WSD.
LLTD	Il est possible que des informations sur les appareils du réseau puissent être lues par un tiers.	Les appareils ne seront pas affichés dans « Périphériques et imprimantes » sous Windows.
LLMNR	Il est possible que des informations sur les appareils du réseau puissent être lues par un tiers.	Les recherches par LLMNR ne seront pas possibles à partir de l'ordinateur.
LPR	Comme la communication n'est pas cryptée, il est possible que les données imprimées puissent être lues par un tiers.	L'impression en utilisant le LPR ne sera pas possible.
RAW (Port 9100/n'importe quel port)	Comme la communication n'est pas cryptée, il est possible que les données imprimées puissent être lues par un tiers.	L'impression en utilisant le port RAW ne sera pas possible.
IPP/IPPS	Pour IPP, puisque la communication n'est pas chiffrée, il est possible que les données imprimées puissent être lues par un tiers. Pour IPPS, il n'y a aucun risque de sécurité.	Il ne sera pas possible d'imprimer à l'aide de IPP/ IPPS, comme l'impression depuis AirPrint ou Mac OS.
FTP	Comme la communication n'est pas cryptée, il est possible que les données imprimées puissent être lues par un tiers.	Il ne sera pas possible d'imprimer ou de transférer des fichiers via FTP.

Protocole/ fonctions de sécurité	Risques de sécurité lorsqu'elles sont activées	Limitations lorsqu'elles sont désactivées
SNMP	Pour SNMPv1 et v2c, puisque la communication n'est pas cryptée, il est possible que les informations de l'appareil et les données de paramétrage puissent être lues par un tiers. Pour SNMPv3, il n'y a aucun risque de sécurité.	Les outils de gestion qui utilisent SNMP ne peuvent pas être utilisés. De plus, les outils et applications de gestion fournis par Epson ne seront pas disponibles.
SSL/TLS	Selon la version TLS et la longueur de clé que vous définissez, la force du chiffrement peut être faible et le message chiffré peut être déchiffré.	La connexion via HTTPS à partir d'un navigateur ne sera pas possible.
Partage de réseau Microsoft	Il est possible que les données numérisées ou les données partagées par fichier puissent être lues par un tiers.	Le transfert de fichiers et le partage de fichiers sur le réseau à l'aide de SMB ne seront pas possibles.
Numérisation en réseau (EPSON Scan)	Comme la communication n'est pas cryptée, il est possible que les données numérisées puissent être lues par un tiers.	La numérisation via le réseau ne sera pas possible.
PC-FAX	Comme la communication n'est pas cryptée, il est possible que les données de télécopie sur le réseau puissent être lues par un tiers.	La fonction PC-FAX ne peut pas être utilisée.

EPSON

NPD6296-05 FR