

**SYSTÈMES NUMÉRIQUES MULTIFONCTIONS COULEUR/
SYSTÈMES NUMÉRIQUES MULTIFONCTIONS**

Manuel d'Utilisation du Mode Haute Sécurité

e-STUDIO2000AC/2500AC

e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC

e-STUDIO2508A/3008A/3508A/4508A/5008A

e-STUDIO5506AC/6506AC/7506AC

e-STUDIO5508A/6508A/7508A/8508A

e-STUDIO3508LP/4508LP/5008LP

Préface

Merci d'avoir choisi la gamme de systèmes numériques multifonctions ou la gamme de systèmes numériques multifonctions couleur TOSHIBA.

Ce manuel décrit les conditions et les paramètres d'une utilisation des systèmes numériques multifonctions conforme à la certification CC.

Lisez attentivement le présent manuel avant toute utilisation des systèmes numériques multifonctions en mode Haute sécurité. Pour connaître les précautions de sécurité permettant une utilisation du système d'exploitation conforme à la certification CC, reportez-vous à la section "Précautions de sécurité" dans les "Informations de sécurité".

Gardez ce manuel à portée de main et utilisez-le de manière à garantir une utilisation du système conforme à la certification CC.

Remarque

Si les cartons reçus présentent des ouvertures suspectes ou si vous n'êtes pas sûr de la manière dont ils ont été emballés, contactez votre représentant commercial.

■ Pour lire ce manuel

☐ Symboles utilisés dans ce manuel

Dans ce manuel, certains points importants sont signalés au moyen des symboles ci-dessous. Prenez connaissance de ces points importants avant d'utiliser le système.

AVERTISSEMENT

Indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, peut entraîner le décès, des blessures graves, des dommages importants ou l'incendie du système ou de son environnement.

ATTENTION

Indique une situation potentiellement dangereuse qui, si elle n'est pas évitée, peut provoquer des blessures mineures ou légères, des dégâts partiels au niveau du système ou du matériel environnant, ou encore des pertes de données.

Remarque

Fournit des informations auxquelles vous devez porter une attention particulière lors de l'utilisation de ce système.

Conseil

Fournit des informations auxquelles vous devez porter une attention particulière lors de l'utilisation de ce système.



Pages décrivant des éléments en rapport avec l'action en cours. Consultez-les en fonction de vos besoins.

☐ Public cible de ce manuel

Ce manuel est destiné aux administrateurs du système. Les utilisateurs généraux n'ont pas besoin de lire ce manuel.

☐ Nom du modèle et de la série utilisés dans ce manuel

Dans ce manuel, chaque nom de modèle est remplacé par le nom de série présenté ci-dessous.

Nom du modèle	Nom de série utilisé dans ce manuel
e-STUDIO2000AC/2500AC	Série e-STUDIO5005AC
e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC	
e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A	Série e-STUDIO5008A
e-STUDIO5506AC/6506AC/7506AC	Série e-STUDIO7506AC
e-STUDIO5508A/6508A/7508A/8508A	Série e-STUDIO8508A
e-STUDIO3508LP/4508LP/5008LP	Série e-STUDIO5008LP

Équipement en option

Pour voir les options disponibles, reportez-vous au *Guide de prise en main rapide*.

Marques

Pour plus d'informations concernant les marques, reportez-vous aux *Informations de sécurité*.

TABLE DES MATIERES

Préface	3
Pour lire ce manuel	3

Chapitre 1 LE MODE HAUTE SÉCURITÉ

Précautions d'utilisation du mode Haute sécurité	8
Confirmation du mode	9
Conditions de fonctionnement.....	10

Chapitre 2 FONCTIONS UNIQUES

Mot de passe temporaire	14
Conditions d'utilisation du mot de passe temporaire	14
Utilisation par un utilisateur en cas de recours à un mot de passe temporaire.....	14
En attente (Fax)	15
Impression d'un travail dans la file d'attente En attente (Fax)	15

Chapitre 3 LES VALEURS INITIALES

Précautions relatives aux valeurs initiales	18
Connexion	18
Liste des valeurs initiales.....	19

LE MODE HAUTE SÉCURITÉ

Précautions d'utilisation du mode Haute sécurité	8
Confirmation du mode	9
Conditions de fonctionnement	10

Précautions d'utilisation du mode Haute sécurité

Ce mode de fonctionnement protège les informations importantes des clients contre l'accès non autorisé au système et les fuites.

Les fonctions de sécurité suivantes doivent être observées pour une utilisation du système conforme à la certification CC.

- La fonction des paramètres d'authentification des utilisateurs
- La fonction de gestion des rôles
- La fonction de recherche et de collecte de journaux
- La fonction d'écrasement des données spécifiées dans le disque dur lorsque les travaux sont terminés ou que le système est mis sous tension
- La fonction de communication avec TLS
- La fonction de vérification de l'intégrité
- Les fonctions de gestion telles que :
Journal, Mots de passe, Utilisateur, Stratégie de mot de passe, Date et heure, Effacement automatique, Minuterie de session, Activer/désactiver TLS

Le certificat ISO/IEC15408 a été ou sera obtenu pour le système équipé de la combinaison des systèmes d'exploitation et navigateurs mentionnés ci-après et utilisant la version japonaise ou anglaise.

Identifiant PP : norme IEEE 2600.1™-2009

SE : Windows 7

Navigateur : Internet Explorer 9

MFP : e-STUDIO2000AC/2500AC
e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC
e-STUDIO2008A/2508A/3008A/3508A/4508A/5008A
e-STUDIO5506AC/6506AC/7506AC
e-STUDIO5508A/6508A/7508A/8508A

Identifiant PP : U.S. Government Protection Profile for Hardcopy Devices version 1.0 (norme IEEE2600.2™-2009)

SE : Windows 7

Navigateur : Internet Explorer 11

MFP : e-STUDIO3508LP/4508LP/5008LP

* Certification en cours (depuis avril 2017)

Pour une utilisation du système en mode sécurité conforme à la certification CC, les configurations doivent être effectuées en fonction de l'environnement d'utilisation comme le paramétrage du cryptage du protocole et la configuration d'une connexion destinée uniquement au serveur ou à l'ordinateur client autorisé.

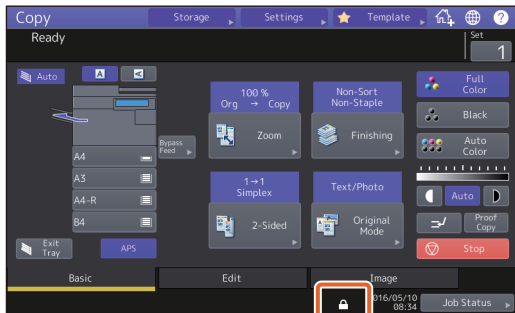
N'oubliez pas que si les conditions décrites dans le présent manuel ne sont pas remplies, vous ne pourrez pas utiliser le système conformément à la certification CC.

Conseil

Pour des informations relatives à chaque fonction de sécurité et sur la manière de configurer les éléments associés, reportez-vous au **Guide de TopAccess**.



■ Confirmation du mode

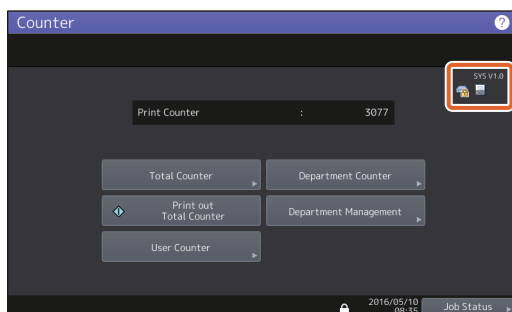
Lorsque le système est utilisé en mode haute sécurité,  s'affiche sur l'écran tactile du système.



Conseil

- Le disque dur du système utilisé en mode haute sécurité est crypté. Le système comprend également une option d'effacement des données (GP-1070). Afin de confirmer le fonctionnement de chaque fonction, consultez l'affichage situé dans la partie supérieure droite intitulée [Compteur (Counter)] de l'écran tactile du système.

Le disque dur est crypté.	 L'icône est affichée. Le disque dur est crypté dès lors que le système fonctionne en mode Haute sécurité.
Le kit d'effacement des données fonctionne correctement.	 L'icône indiquant que le kit d'effacement des données fonctionne correctement s'affiche. La version du système utilisé s'affiche. (SYS V1.0)



- Lorsque le kit d'effacement des données est installé, l'espace disque utilisé temporairement lors du processus de travail est utilisé par un autre travail une fois les données écrasées à la déconnexion de l'utilisateur.

■ Conditions de fonctionnement

Si vous ne suivez pas les instructions de fonctionnement ci-dessus, vos informations confidentielles ne seront pas protégées contre les fuites ou les accès non autorisés.



Veillez à définir [Authentification MFP LOCAL (MFP Local Authentication)] pour [Méthode d'authentification (Authentication Method)] dans l'écran [Gestion utilisateur (User Management)]. Si les options [Authentification de domaine Windows (Windows Domain Authentication)] ou [Authentification LDAP (LDAP Authentication)] sont définies pour l'authentification de l'utilisateur, le système ne sera pas conforme à la certification CC.

Sélectionnez manuellement [COMPLET (FULL)] et effectuez la vérification d'intégrité lors de l'installation, puis à intervalles réguliers lors de l'utilisation.

* Pour plus d'informations relatives à la vérification d'intégrité, reportez-vous au *Guide d'administration*.

Ne modifiez pas les valeurs d'origine des paramètres de communication du système. Si vous ne modifiez pas ces valeurs, la communication effectuée via un réseau peut être protégée par le TLS.

Dans l'un des cas suivants, contactez votre technicien.

- Si l'icône indiquant le cryptage du disque dur () ne s'affiche pas.
- Si l'icône indiquant le bon fonctionnement du kit d'effacement des données () ne s'affiche pas.
- Les versions affichée et réelle du système sont différentes.

En mode Haute sécurité, les fonctions suivantes ne peuvent pas être utilisées.

- Suspendre un travail de copie
- Fax en réseau
- Address Book Viewer
- Téléchargeur de fichiers
- Pilote TWAIN
- Utilitaire de sauvegarde/restauration e-Filing
- Impression programmée
- Stockage vers e-Filing à partir d'un pilote d'impression*

* La fonction est disponible à la sélection, mais le travail est supprimé en cas d'erreur. L'impression n'est donc pas lancée. Lorsqu'un travail est supprimé, il est enregistré dans le journal des erreurs. Confirmez-le dans l'onglet [Journaux (Logs)] dans TopAccess ou dans [Etat Trav. (Job Status)] - [Journal (Log)] - [Imprimer (Print)] du système.

- Désactivation de l'authentification du journal

La fonction de connexion automatique du logiciel client fournie avec ce système n'est pas disponible. Assurez-vous de saisir le nom d'utilisateur et le mot de passe lorsque vous utilisez le logiciel client.

Toutes les données envoyées vers ce système, telles que les fax ou les fax internet imprimés ou reçus à partir d'un pilote d'impression* peuvent être sorties uniquement si l'utilisateur connecté bénéficie des droits d'impression.

* Utilisez l'IPP SSL pour communiquer avec le système.

Lorsque l'impression IPP est effectuée, utilisez le port créé en saisissant “https://[adresse IP (IP address)]:[numéro port SSL (SSL port number)]/Print” dans le champ de l'URL.

(par exemple : https://192.168.1.2:443/Print)

* Pour plus de détails, reportez-vous à la section [Impression IPP (IPP Printing)] dans [Installation des pilotes d'impression pour Windows (Installing Printer Drivers for Windows)] - [Autres installations (Other Installations)] du *Guide d'installation des logiciels*.

Lors de l'importation de données telles que le carnet d'adresses, veillez à utiliser les données exportées du système.

N'utilisez aucune application nécessitant la modification d'un paramètre du sous-menu [ODCA] dans le menu [Configuration (Setup)] de l'onglet [Administration] sous TopAccess.

N'activez pas [Utiliser l'authentification par mot de passe pour les travaux d'impression (Use Password Authentication for Print Job)] lorsqu'une impression est lancée à partir du système avec l'un de ces pilotes d'impression : Universal Printer 2, Universal PS3 and Universal XPS.

Pour faire fonctionner ce système en toute sécurité, assurez-vous de définir les éléments suivants :

Remarque

Effectuez correctement le paramétrage en vous reportant à la liste des valeurs initiales (📖 P.19).

- Utilisez le format PDF crypté lorsque vous enregistrez ou envoyez un fichier et veillez à utiliser le niveau de cryptage 128bit AES.
- Spécifiez un ordinateur distant fiable comme emplacement d'enregistrement des données de scan.
- N'utilisez pas de boîte publique dans e-Filing étant donné qu'aucun mot de passe ne peut être défini.
- N'utilisez pas le MFP LOCAL étant donné qu'aucun mot de passe ne peut être défini.
- Les administrateurs doivent régulièrement exporter et stocker les journaux.

Un administrateur doit expliquer aux utilisateurs que le mode haute sécurité et les éléments suivants s'appliquent dans ce système, de sorte qu'ils les utilisent correctement.

- L'impression doit être effectuée selon les paramètres du pilote d'impression de l'impression IPP.
- Spécifiez un ordinateur distant fiable comme emplacement d'enregistrement des données de scan.
- N'utilisez pas de dossier partagé dans l'e-Filing.
- N'utilisez aucun dossier local du système.

Lors de la mise au rebut d'un MFP, veillez à contacter votre technicien de service pour supprimer complètement les données de votre disque dur.

FONCTIONS UNIQUES

Mot de passe temporaire	14
Conditions d'utilisation du mot de passe temporaire	14
Utilisation par un utilisateur en cas de recours à un mot de passe temporaire.....	14
En attente (Fax)	15
Impression d'un travail dans la file d'attente En attente (Fax)	15

Mot de passe temporaire

Dans le mode haute sécurité, les mots de passe que les administrateurs tentent d'attribuer afin d'autoriser l'accès utilisateur sont des mots de passe temporaires. Pour utiliser le système, vous devez enregistrer votre mot de passe après y avoir accédé à l'aide du mot de passe temporaire.

Remarque

Si vous continuez à utiliser le mot de passe temporaire, le niveau de sécurité ne sera pas suffisamment élevé. Enregistrez votre mot de passe le plus rapidement possible.

■ Conditions d'utilisation du mot de passe temporaire

Le mot de passe temporaire de l'utilisateur est utilisé dans les cas suivants :

- Lorsque vous vous connectez au système pour la première fois après avoir été enregistré par un administrateur.
- Lorsqu'un administrateur réinitialise le mot de passe d'un utilisateur.
- Lorsque le mot de passe pour les informations utilisateur importées par un administrateur est au format texte brut.

Remarque

Lorsqu'un administrateur réinitialise les mots de passe d'utilisateurs, ceux-ci doivent en être informés et être invités à les modifier à leur convenance.

Conseil

Pour empêcher l'altération des informations utilisateur exportées à partir d'un système, les informations sont hachées. Si vous modifiez le mot de passe pour les informations utilisateur exportées, le texte brut sera utilisé pour le mot de passe.

■ Utilisation par un utilisateur en cas de recours à un mot de passe temporaire

Si vous ne parvenez pas à enregistrer le mot de passe durant l'accès.

- Enregistrement de votre mot de passe dans le tableau de bord
Entrez le nom d'utilisateur et un mot de passe temporaire dans le menu Authentification utilisateur. Quand vous appuyez sur [OK] dans l'écran de confirmation du mot de passe temporaire, l'écran de saisie du mot de passe apparaît. Saisissez le mot de passe temporaire dans [Ancien MDP (Old Password)]. Saisissez le nouveau mot de passe dans [Nouveau Mot de Passe (New Password)] et [Retaper le nouv. Mdp (Retype New Password)] puis appuyez sur [OK]. Le nouveau mot de passe est enregistré et vous pouvez vous connecter au système.
- Enregistrement de votre mot de passe dans TopAccess
Lorsque vous accédez au système depuis TopAccess, l'écran de connexion apparaît. Saisissez le nom d'utilisateur et un mot de passe temporaire dans l'écran de connexion, puis appuyez sur [Connexion (Login)]. Lorsque l'écran d'enregistrement s'affiche, saisissez le nouveau mot de passe dans [Nouveau Mot de Passe (New Password)] et [Retaper le nouv. Mdp (Retype New Password)], puis appuyez sur la touche [Enregistrer (Save)]. Le nouveau mot de passe est enregistré et vous pouvez vous connecter à TopAccess.

Si vous ne parvenez pas à enregistrer un nouveau mot de passe en accédant au système.

Dans les utilitaires suivants, une erreur se produit lorsque vous tentez d'accéder au système à l'aide d'un mot de passe temporaire. Il est par conséquent impossible d'enregistrer un nouveau mot de passe. Avant d'utiliser ces utilitaires, enregistrez un nouveau mot de passe dans le panneau de configuration ou dans TopAccess.

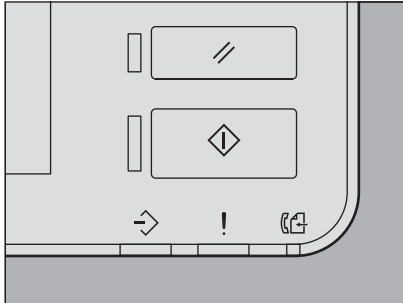
- Pilote Remote Scan
- Utilitaire Web e-Filing

En attente (Fax)

En mode haute sécurité, un e-mail vers lequel un fax, un fax Internet ou une image est transmis(e), n'est pas sorti automatiquement. Ces travaux sont stockés dans la file d'attente [En Attente (Fax) (Hold (Fax))] et seul un utilisateur autorisé à utiliser [Impression reçue par fax (Fax Received Print)] peut imprimer le travail.

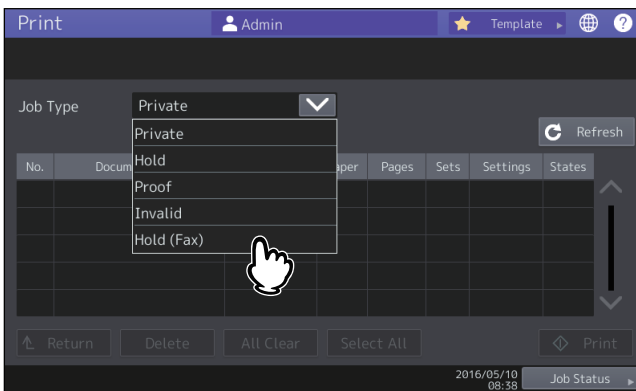
Conseil

Si un travail se trouve dans la file d'attente de travaux [En attente (Fax) (Hold (Fax))], le voyant Mémoire Rx clignote.



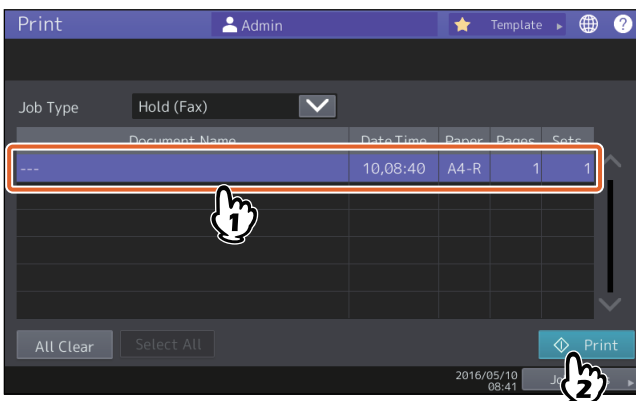
■ Impression d'un travail dans la file d'attente En attente (Fax)

- 1 Connectez-vous au système en tant qu'utilisateur bénéficiant du droit [Impression reçue par fax].
- 2 Appuyez sur [Imprimer (Print Mode)] dans l'écran principal.
- 3 Sélectionnez [En Attente (Fax) (Hold (Fax))].



- Tous les travaux situés dans la file d'attente [En attente (Fax) (Hold (Fax))] s'affichent.

- 4 Sélectionnez les travaux souhaités ou appuyez sur [Sélectionner tout (Select All)] puis sur la touche [Imprimer (Print)].



- Le travail imprimé est supprimé de la file de travaux [En attente (Fax) (Hold (Fax))].

LES VALEURS INITIALES

Précautions relatives aux valeurs initiales.....	18
Connexion	18
Liste des valeurs initiales.....	19

Précautions relatives aux valeurs initiales

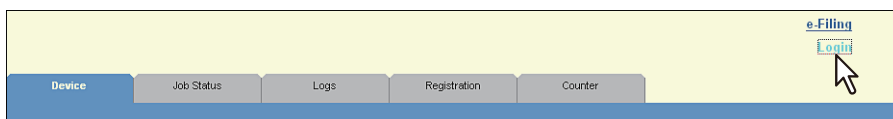
Pour une utilisation sécurisée de l'équipement, les valeurs initiales et disponibles à la sélection dans le système en mode Haute sécurité peuvent être différentes de celles du mode de sécurité normal. Ce manuel décrit uniquement les valeurs initiales et les éléments de paramétrage qui diffèrent de ceux utilisés dans le mode de sécurité normal. Pour une utilisation du système conforme à la certification CC, veuillez à modifier les valeurs initiales pour le mode haute sécurité indiquées dans ce chapitre en suivant les instructions décrites dans la colonne des remarques au début de l'utilisation. Par la suite, ne les modifiez plus.

Remarque

- Pour consulter les paramètres et les valeurs par défaut du mode de sécurité normal, reportez-vous au **Guide de TopAccess** et au **Guide d'administration**.
- Pour réinitialiser tous les paramètres via une initialisation de ce système, sauvegardez préalablement les paramètres du système et les données clientes. Pour plus d'informations, reportez-vous au **Guide de TopAccess** et au **Guide d'administration**.

■ Connexion

- Les onglets [Gestion des utilisateurs (User Management)] et [Administration] de TopAccess s'affichent lorsqu'un utilisateur bénéficiant de droits d'administrateur se connecte. Ouvrez TopAccess, cliquez sur "Connexion" dans la partie supérieure droite, puis saisissez le nom d'utilisateur et le mot de passe de connexion.



- Veillez à vous connecter en tant qu'utilisateur bénéficiant de droits d'administrateur dans l'onglet (Admin (Admin)) dans le mode [Fonction utilisateur (User Function)] du système.

■ Liste des valeurs initiales

Ecran d'accueil :

Menu [Fonctions utilisateurs -Utilisateur-(User Functions -User-)]

Onglet [Admin (Admin)]

Menu [Liste/Rapport (List/Report)]

Menu [Paramètre de rapport (Report Setting)]

Élément	Valeur initiale du mode haute sécurité	Remarques
[Rapport COMM. (COMM. Report)]		
Mémoire TX	OFF	Ne définissez pas le paramètre sur "MARCHE".

* TopAccess ne permet pas l'utilisation des menus ci-dessus.

TopAccess :

Onglet [Administration]

Menu [Config. (Setup)]

Sous-menu [Général (General)]

Élément	Valeur initiale du mode haute sécurité	Remarques
Informations sur le périphérique		
Impression USB directe	Désactiver	
Fonctions		
Enregistrer sous FTP	Désactiver	
Enregistrer sur le support USB	Désactiver	
Enregistrer sous SMB	Désactiver	
Enregistrer sous Netware	Désactiver	
Fax Internet en réseau	Désactiver	
Fax en réseau	Désactiver	
Services Web - Scan	Désactiver	
Scan Twain	Désactiver	
Restriction sur l'opération de répertoire téléphonique par un administrateur/ OpérateurDistantRépertoireTéléphonique		
Peut être opéré par l'administrateur/ OpérateurDistantRépertoireTéléphonique uniquement.		
Economie d'énergie		
Economie d'énergie : effacement automatique *	45 secondes	La valeur initiale est la même que pour le mode de sécurité normal. Toutefois, OFF ne peut pas être sélectionné.

* Vous pouvez modifier la valeur à partir de l'onglet [ADMIN] de l'écran tactile du système, dans le mode [Fonctions utilisateurs -Utilisateur- (User Functions -User-)].

Sous-menu [Réseau (Network)]

Élément	Valeur initiale du mode haute sécurité	Remarques
SMB		
Protocole serveur SMB	Désactiver	
HTTP		
Activer SSL*	Activer	
WSD		
Activer SSL	Activer	
Services Web - Impression	Désactiver	
Services Web - Scan	Désactiver	
Serveur SMTP		
Activer le serveur SMTP	Désactiver	
Serveur FTP		
Activer le serveur FTP	Désactiver	
Activer SSL	Activer	
Client SMTP		
Activer SSL	Vérifier avec le/les certificat(s) CA importé(s)	Le paramètre sécurisé est "Vérifier avec le/les certificat(s) CA importé(s)" ou "Accepter tous les certificats sans CA".
Authentification	AUTO	Assurez-vous que l'une des options "CRAM-MD5", "Digest-MD5", "Kerberos" ou "NTLM (IWA)" est appliquée à votre environnement d'utilisation.
Client POP3		
Activer SSL	Vérifier avec le/les certificat(s) CA importé(s)	
Client FTP		
Paramétrage SSL	Vérifier avec le/les certificat(s) CA importé(s)	
Bonjour		
Activer Bonjour	Désactiver	
SNMP		
Activer SNMP V1/V2	Désactiver	
Activer SNMP V3	Activer	
SLP		
Activer SLP	Désactiver	
Paramètre Syslog		
Activer SSL	Vérifier avec le/les certificat(s) CA importé(s)	

* Vous pouvez modifier la valeur à partir de l'onglet [ADMIN] de l'écran tactile du système, dans le mode [Fonctions utilisateurs -Utilisateur- (User Functions -User-)].

Sous-menu [Imprimante (Printer)]

Élément	Valeur initiale du mode haute sécurité	Remarques
Configuration générale		
Restriction du travail d'impression	Retenu uniquement	

Sous-menu [Service d'impression (Print Service)]

Élément	Valeur initiale du mode haute sécurité	Remarques
Impression TCP brut		
Activer le support d'impression TCP brut	Désactiver	
Impression LPD		
Activer LPD	Désactiver	
Impression IPP		
Activer SSL	Activer	
Impression FTP		
Activer l'impr. FTP	Désactiver	

Sous-menu [ODCA]

Élément	Valeur initiale du mode haute sécurité	Remarques
Réseau		
Activer un port	Désactiver	

Menu [Sécurité (Security)]

Sous-menu [Authentification (Authentication)]

Élément	Valeur initiale du mode haute sécurité	Remarques
Paramètres d'authentification des utilisateurs		
Authentification utilisateur	Activer	Vous ne pouvez pas définir les paramètres sur "Désactiver".
Authentification utilisateur relative à la fonction	Désactiver	Ne définissez pas le paramètre sur "Activer".
Utiliser l'authentification par mot de passe pour les travaux d'impression	Désactiver	Ne définissez pas le paramètre sur "Activer".
Autoriser l'utilisateur hôte	Case non cochée (désactivée)	La valeur initiale est la même que pour le mode de sécurité normal. Toutefois, l'option ne peut pas être définie sur "Activer".
Type d'authentification	Authentification locale MFP	
Authentification par code PIN	Désactiver	Ne définissez pas le paramètre sur "Activer".
Gestion des utilisateurs partagée	Désactiver	Ne définissez pas le paramètre sur "Activer".

Sous-menu [Stratégie du mot de passe (Password Policy)]

Élément	Valeur initiale du mode haute sécurité	Remarques
Stratégie pour les utilisateurs		
Longueur minimale du mot de passe	8 (chiffres)	
Conditions requises à appliquer	Activer	
Paramétrage du verrouillage	Activer	(Similaire au mode de sécurité normal)
Nombre de tentatives	3 (fois)	
Durée du verrouillage	2 (minutes)	
Période de disponibilité	Désactiver	(Similaire au mode de sécurité normal)
Jour(s) avant expiration	90 (jours)	
Stratégie pour l'administrateur, l'auditeur		
Longueur minimale du mot de passe	8 (chiffres)	
Conditions requises à appliquer	Activer	
Paramétrage du verrouillage	Activer	(Similaire au mode de sécurité normal)
Nombre de tentatives	3 (fois)	
Durée du verrouillage	2 (minutes)	
Période de disponibilité	Désactiver	(Similaire au mode de sécurité normal)
Jour(s) avant expiration	90 (jours)	
Stratégie pour les boîtes e-Filing, les groupes de modèles, les modèles, le PDF sécurisé, le protocole SNMPv3, le clonage et la réception sécurisée.		
Longueur minimale du mot de passe	8 (chiffres)	
Conditions requises à appliquer	Activer	
Paramétrage du verrouillage	Activer	(Similaire au mode de sécurité normal)
Nombre de tentatives	3 (fois)	
Durée du verrouillage	2 (minutes)	

e-STUDIO2000AC/2500AC
e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC
e-STUDIO2508A/3008A/3508A/4508A/5008A
e-STUDIO5506AC/6506AC/7506AC
e-STUDIO5508A/6508A/7508A/8508A
e-STUDIO3508LP/4508LP/5008LP

**SYSTÈMES NUMÉRIQUES MULTIFONCTION COULEUR/
SYSTÈMES NUMÉRIQUES MULTIFONCTION**

Manuel d'Utilisation du Mode Haute Sécurité

e-STUDIO2000AC/2500AC

e-STUDIO2505AC/3005AC/3505AC/4505AC/5005AC

e-STUDIO2508A/3008A/3508A/4508A/5008A

e-STUDIO5506AC/6506AC/7506AC

e-STUDIO5508A/6508A/7508A/8508A

e-STUDIO3508LP/4508LP/5008LP

TOSHIBA TEC CORPORATION

1-11-1, OSAKI, SHINAGAWA-KU, TOKYO, 141-8562, JAPAN