

# Panasonic

## Manuel d'installation

---

## Trusted Platform Module (TPM)

---



Nous vous conseillons d'imprimer ce manuel d'installation.

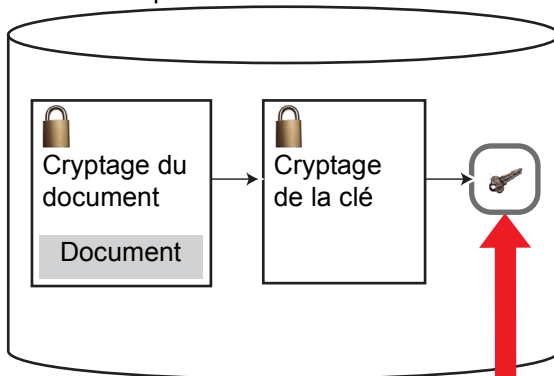
Les instructions dans ce manuel sont basées sur Windows 7. Les instructions pour Windows Vista et Windows XP peuvent être différentes de celles pour Windows 7. Les différences sont expliquées avec des annotations.

Les mesures de sécurité conventionnelles comme le cryptage de fichiers et le cryptage par clé publique enregistrent les clés de cryptage sur le lecteur de disque dur de l'ordinateur. Par conséquent, les clés et les mots de passe ainsi que les données cryptées sont exposés au risque de copie non autorisée et de piratage.

La méthode TPM enregistre les clés de cryptage sur la puce TPM, qui est séparée du lecteur de disque dur et de l'unité centrale. Pour accéder aux clés de cryptage, vous devez saisir le mot de passe enregistré dans Security Platform (→ [page 9](#)). Vous pouvez appliquer un réglage de sécurité différent à chaque compte d'utilisateur dans Security Platform.

## Cryptage conventionnel

La clé de cryptage est enregistrée dans un fichier sur le lecteur de disque dur.

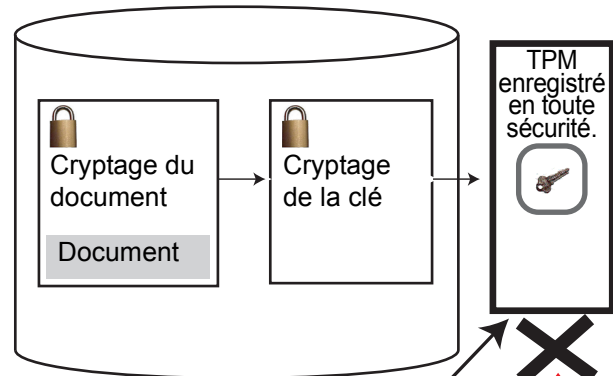


La clé reste non cryptée.

Piratage

## Cryptage TPM

La clé de cryptage est enregistrée sur la puce TPM.



La saisie du mot de passe est nécessaire pour accéder à la clé.

Piratage

## Fonctions de sécurité


- La méthode TPM ne garantit pas la protection des données dans toutes les conditions.
- La méthode TPM utilise des clés de cryptage multiples, des certificats et des mots de passe. Vous ne pouvez pas décrypter les données cryptées si vous les perdez. Gardez bien les clés, les certificats et les mots de passe. (Consultez “Sauvegarde” ci-dessous.)
- Nous ne pouvons être tenus responsables pour toute perte ou tout dégât causé par votre utilisation de TPM ou votre négligence de son utilisation, ou pour toute perte de données causée par des développements comme le mauvais fonctionnement de TPM.

## Sauvegarde

Les fichiers décrits ci-dessous sont nécessaires pour récupérer la fonction Security Platform. Effectuez une sauvegarde régulière de ces fichiers dans un endroit sûr, comme un disque amovible, pour éviter la perte de données causée par le mauvais fonctionnement de TPM ou d'autres accidents. Nous vous recommandons de sauvegarder les fichiers sur un disque amovible ou un lecteur de réseau car l'avantage de la sécurité de TPM peut diminuer si vous conservez les fichiers sur le lecteur de disque dur interne.

### REMARQUE

- Avec les réglages par défaut, l’“Archive de sauvegarde du système”, le “Dossier de sauvegarde du système”, le “Jeton de récupération d’urgence”, le “Jeton de réinitialisation de mot de passe” et le “Fichier secret personnel pour la réinitialisation de mot de passe” sont enregistrés dans “C:\Utilisateurs\(\compte d'utilisateur)\Documents\Sécurité\Platform”<sup>\*1</sup>. Si un disque amovible est raccordé, les fichiers à l’exception de l’Archive de sauvegarde du système et du Dossier de sauvegarde du système sont automatiquement enregistrés sur le disque amovible en priorité.
- Fichiers et dossier utilisés par l’administrateur de l’ordinateur
  - **Archive de sauvegarde du système**  
(Nom par défaut : SPSystemBackup.xml)
  - **Dossier de sauvegarde du système**  
(Nom par défaut : SPSystemBackup)Vous avez besoin du fichier et du dossier lorsque vous remplacez la puce TPM intégrée ou le lecteur de disque dur, ou lorsque vous réinstallez Windows.  
Le fichier et le dossier contiennent la sauvegarde des données de récupération d’urgence, ainsi que les clés, certificats et réglages de tous les utilisateurs.  
Si vous configurez le réglage de récupération régulière, la sauvegarde du réglage de chaque utilisateur sera automatiquement enregistrée à l’intervalle programmé. Pour être sûr d’avoir la sauvegarde la plus récente, effectuez une sauvegarde manuelle à chaque fois que vous créez ou modifiez le réglage utilisateur.  
Pour plus d’informations, consultez “Comment effectuer la sauvegarde et la restauration”-“Comment configurer des

sauvegardes automatiques (“Sauvegarde du système”) dans le menu Help d’Infineon Security Platform. (Cliquez sur  (Démarrer)<sup>\*2</sup> - [Tous les programmes] - [Infineon Security Platform Solution] - [Help] - [Bienvenue dans la solution Infineon Security Platform] - [Fonctionnement avancé de Security Platform] - [Sauvegarde et restauration de données Security Platform])

\*1 Windows XP : “C:\Documents and Settings\(\compte d'utilisateur)\Mes documents\Security Platform”  
Windows Vista : “C:\Utilisateurs\(\compte d'utilisateur)\Documents\Security Platform”

\*2 Windows XP : [démarrer]

- **Jeton de récupération d’urgence**

(Nom par défaut : SPEmRecToken.xml)

Vous avez besoin de ce fichier lorsque vous remplacez la puce TPM intégrée.

Utilisez le fichier pour la récupération à l’aide des données de récupération d’urgence. (Les données de récupération d’urgence sont contenues dans l’Archive de sauvegarde du système et le Dossier de sauvegarde du système, et protégées par ce fichier.)

- **Jeton de réinitialisation de mot de passe**

(Nom par défaut : SPPwdResetToken.xml)

Vous avez besoin de ce fichier pour créer le Code d’autorisation de réinitialisation requis pour réinitialiser le mot de passe d’un utilisateur spécifique.

Vous ne pouvez pas réinitialiser le mot de passe sans ce jeton.

- Fichier utilisé par chaque utilisateur

- **Fichier secret personnel pour la réinitialisation de mot de passe**

(Nom par défaut : SPPwdResetSecret.xml)

Vous utilisez ce fichier en association avec le Jeton de réinitialisation de mot de passe pour réinitialiser le Mot de passe utilisateur de base.

## Précautions pour le cryptage

- Ne cryptez pas des fichiers décrits dans “Sauvegardage” (→ [page 3](#)). Si vous les cryptez, vous ne pourrez pas restaurer les réglages de Security Platform. Avec les réglages par défaut, ces fichiers sont enregistrés dans “C:\Utilisateurs”<sup>\*3</sup>. Ne cryptez pas “C:\Utilisateurs”<sup>\*3</sup>.

- Ne cryptez pas les fichiers dans “C:\Program Files” parce qu’ils contiennent de nombreux logiciels d’application. Si vous les cryptez, les autres utilisateurs ne peuvent pas accéder au logiciel, et le logiciel peut ne pas démarrer ou un autre dysfonctionnement peut se produire.

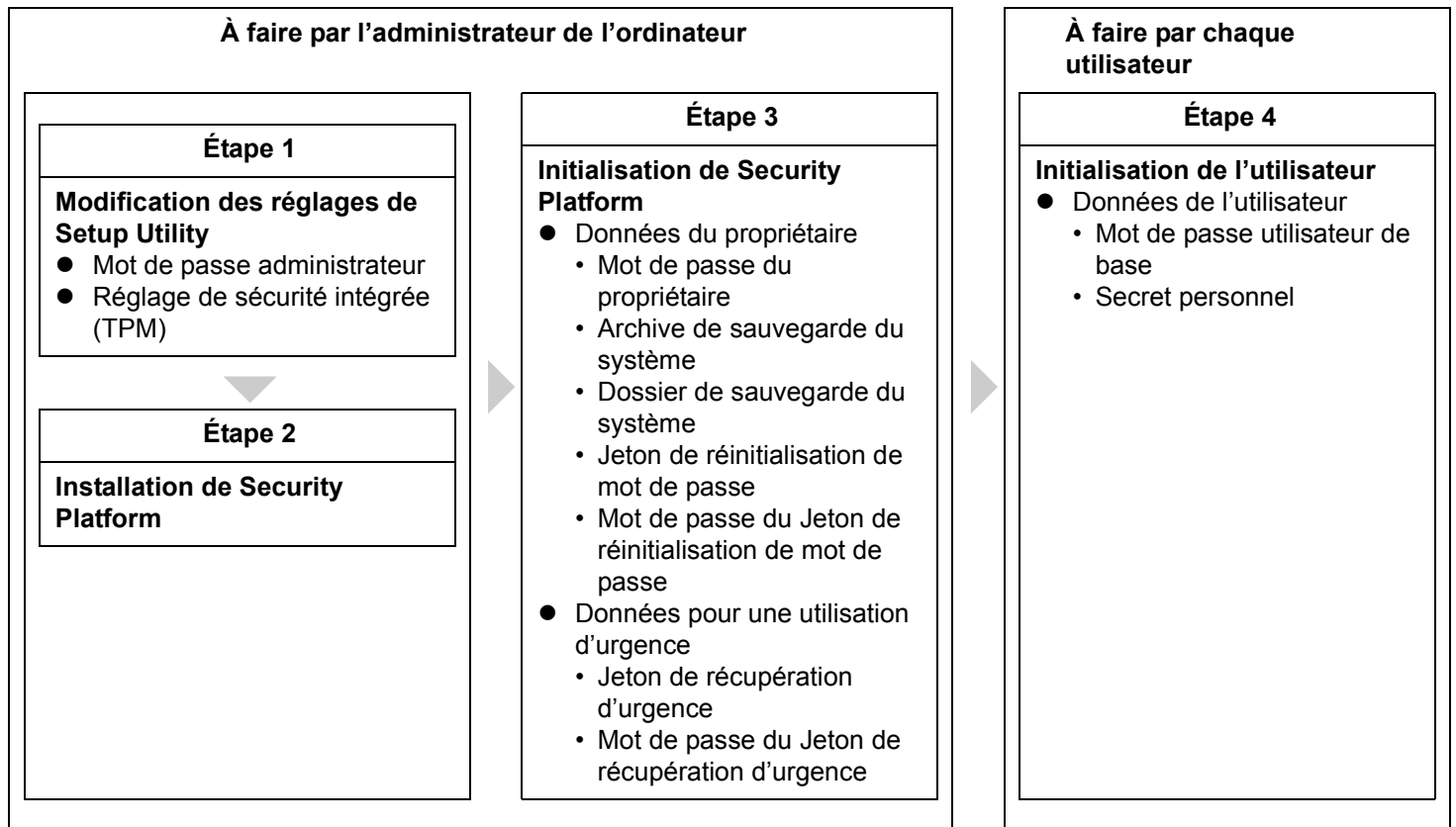
Notez que le cryptage d’autres fichiers comme “C:\” peut également provoquer des problèmes similaires.

- Ne cryptez ni le dossier “Security Platform” ni aucun fichier/dossier qu’il contient. Ce dossier est créé sur le lecteur (réglage par défaut : “C:\”) que vous avez spécifié lors de la configuration du Lecteur personnel sécurisé. Étant donné que Security Platform se réfère à ce dossier, son cryptage peut désactiver le Lecteur personnel sécurisé.


\*3 Windows XP : “C:\Documents and Settings”

## Lorsque des réparations sont nécessaires sur l'ordinateur

- Avant de faire réparer l'ordinateur, suivez les étapes décrites dans Initialisation des données du propriétaire. (→ [page 11](#))



Ce manuel décrit les étapes 1, 2 et la partie initiale de l'étape 3.

Pour le reste des étapes, consultez (→ [page 9](#) "Étape 3 Initialisation de Security Platform") et le menu Help d'Infineon Security Platform. (Cliquez sur  (Démarrer)<sup>\*1</sup> - [Tous les programmes] - [Infineon Security Platform Solution] - [Help].)

<sup>\*1</sup> Windows XP : [démarrer]

## Étape 1 Modification des réglages de Setup Utility

À faire par l'administrateur de l'ordinateur.

### REMARQUE

<Pour le modèle avec clavier numérique de la série CF-U1>

- Lorsque vous effectuez la procédure suivante, raccordez le clavier USB. Ensuite, appuyez sur la touche indiquée entre ( ) au lieu de la touche ou la combinaison de touche indiquée juste avant.

<Pour la série CF-H1>

- Lorsque vous effectuez la procédure suivante, placez l'ordinateur sur son socle et raccordez le clavier USB. Ensuite, appuyez sur la touche indiquée entre ( ) au lieu de la touche ou la combinaison de touche indiquée juste avant.

### 1 Enregistrez le mot de passe administrateur.

Vous devez enregistrer le mot de passe administrateur pour procéder à l'étape suivante.

- ① Allumez ou redémarrez l'ordinateur.
- ② Appuyez sur **Fn + F2 (F2)** ou **Fn + Suppr (Suppr)** pendant l'affichage de l'écran de démarrage [Panasonic] immédiatement après la procédure de lancement de l'ordinateur.  
Setup Utility démarre.
- ③ Sélectionnez le menu [Security].
- ④ Sélectionnez [Set Supervisor Password] et appuyez sur **Entrée (Entrée)**.
- ⑤ Saisissez votre mot de passe dans [Create New Password] et appuyez sur **Entrée (Entrée)**.
  - Pour connaître les restrictions sur la saisie du mot de passe, consultez le Manuel de référence de votre ordinateur.
- ⑥ Saisissez à nouveau votre mot de passe dans [Confirm New Password], et appuyez sur **Entrée (Entrée)**.

### 2 <Uniquement pour la série CF-U1>

Activez la puce de sécurité intégrée.

- ① Sélectionnez [Enable Embedded Security Chip (TPM)] et appuyez sur **Entrée (Entrée)**.  
Lorsque le message de confirmation s'affiche, sélectionnez [OK] et appuyez sur **Entrée (Entrée)**.
  - Une fois que TPM est activé, cet élément ne s'affiche plus.
- ② Lorsque le message de confirmation s'affiche, sélectionnez [OK] et appuyez sur **Entrée (Entrée)**.  
L'ordinateur redémarre automatiquement.
- ③ Appuyez sur **Fn + F2 (F2)** ou **Fn + Suppr (Suppr)** pendant l'affichage de l'écran de démarrage [Panasonic] immédiatement après la procédure de lancement de l'ordinateur.  
Setup Utility démarre.

## 3 Activez la sécurité intégrée (TPM).

- ① Sélectionnez [Embedded Security (TPM)] dans le menu [Security] et appuyez sur **Entrée (Entrée)**.
- ② Sélectionnez [TPM State] et réglez-le sur [Enable].
  - Si le message de confirmation s'affiche, appuyez sur **Entrée (Entrée)**.
- ③ Appuyez sur **Fn + Échap (Échap)** pour fermer le sous-menu.
- ④ Appuyez sur **Fn + F10 (F10)**, sélectionnez [Yes] et appuyez sur **Entrée (Entrée)** pour quitter Setup Utility.

### REMARQUE

- Le réglage par défaut de [Sub-Menu Protection] est [Protected]. Si vous sélectionnez [No Protection], un utilisateur disposant uniquement d'un mot de passe utilisateur peut entrer dans [Embedded Security (TPM)] et modifier les réglages, y compris [Clear TPM Owner] (→ [page 11](#)). Faites particulièrement attention lorsque vous modifiez le réglage par défaut.

## Étape 2 Installation de Security Platform

À faire par l'administrateur de l'ordinateur.


**1** Ouvrez une session Windows en tant qu'administrateur.

**2** Fermez tous les programmes.

**3** <Windows 7>

Cliquez sur  (Démarrer) et saisissez [c:\util\drivers\tpm\infineon\setup.exe] dans [Rechercher les programmes et fichiers] et appuyez sur **Entrée**.


<Windows Vista>

Cliquez sur  (Démarrer) et saisissez [c:\util\drivers\tpm\infineon\setup.exe] dans [Rechercher] et appuyez sur **Entrée**.

<Windows XP>


Saisissez [c:\util\drivers\tpm\infineon\setup.exe] dans [démarrer] - [Exécuter] et cliquez sur [OK].

- Le message "Infineon TPM Professional Package requires that the following requirements be installed on your computer prior to installing this application. Click Install to begin installing these requirements:" peut s'afficher. Si ce message est affiché, cliquez sur [Install].
- L'écran [InstallShield Wizard] s'affiche.


- 4 Cliquez sur [Next].**
- 5 Lisez attentivement le contrat de licence. Sélectionnez “I accept the terms in the license agreement” et cliquez sur [Next].**  
L'installation commence. Suivez les instructions à l'écran.
- 6 Lorsque le message [InstallShield Wizard Completed] s'affiche, cliquez sur [Finish].**  
Lorsque le fichier Lisez-moi s'affiche, lisez-le attentivement et fermez-le.
- 7 Le message de confirmation de redémarrage s'affiche, cliquez sur [Yes] et redémarrez l'ordinateur.**
- 8 Ouvrez une session Windows en tant qu'administrateur.**  
L'icône “État Security Platform”  s'affiche dans la zone de notification.

## Étape 3 Initialisation de Security Platform

---


Le message “L'état de Security Platform est "Non initialisé". Cliquez pour l'initialiser maintenant.” est affiché par l'icône “État Security Platform”  dans la zone de notification.

- 1 Cliquez sur le message “L'état de Security Platform est "Non initialisé". Cliquez pour l'initialiser maintenant.” pour démarrer “Security Platform Assistant Rapide d'Initialisation”.**

Vous pouvez aussi double-cliquer sur l'icône “État Security Platform”  dans la zone de notification.

- 2 Cliquez sur [Initialisation Avancée (pour les utilisateurs experts)] puis cliquez sur [Suivant].**

Suivez les instructions à l'écran.

- Pour plus d'informations, consultez le menu Help d'Infineon Security Platform. (Cliquez sur  (Démarrer)<sup>\*2</sup> - [Tous les programmes] - [Infineon Security Platform Solution] - [Help] - [Bienvenue dans la solution Infineon Security Platform] - [Outils de la solution Security Platform] - [Assistant Initialisation de Security Platform].)

Après avoir terminé la procédure ci-dessus, initialisez chaque utilisateur.

<sup>\*2</sup> Windows XP : [démarrer]

## ATTENTION

- N'oubliez ou ne supprimez aucun des mots de passe et fichiers. Si vous les perdez, l'administration ou la récupération de Security Platform devient impossible. Gardez bien les mots de passe et les fichiers.

## REMARQUE

- La création du Lecteur personnel sécurisé prend 1 à 2 minutes pour une capacité d'1 Go. Attendez la fin de la procédure.

Lorsque vous vous débarrassez de l'ordinateur ou transférez la propriété, initialisez les données du propriétaire pour empêcher les données cryptées par TPM d'être décryptées par une personne non autorisée.

## REMARQUE

<Pour le modèle avec clavier numérique de la série CF-U1>

- Lorsque vous effectuez la procédure suivante, raccordez le clavier USB. Ensuite, appuyez sur la touche indiquée entre ( ) au lieu de la touche ou la combinaison de touche indiquée juste avant.

<Pour la série CF-H1>

- Lorsque vous effectuez la procédure suivante, placez l'ordinateur sur son socle et raccordez le clavier USB. Ensuite, appuyez sur la touche indiquée entre ( ) au lieu de la touche ou la combinaison de touche indiquée juste avant.


- 1 Lancez Setup Utility (→ page 7).**
- 2 Sélectionnez le menu [Security] et [Embedded Security (TPM)] puis appuyez sur Entrée (Entrée).**
  - Lorsque vous ne pouvez pas entrer dans [Embedded Security (TPM)] à l'aide du mot de passe utilisateur, demandez le mot de passe administrateur à l'administrateur.
  - Vous ne pouvez pas entrer dans [Embedded Security (TPM)] si le mot de passe administrateur n'a pas été enregistré.
- 3 Sélectionnez [TPM State] et réglez-le sur [Disabled].**
- 4 Sélectionnez [Pending TPM operation] et réglez-le sur [Clear TPM Owner].**
- 5 Appuyez sur Fn + F10 (F10), sélectionnez [Yes] et appuyez sur Entrée (Entrée) pour quitter Setup Utility.**

L'ordinateur redémarre automatiquement.


Vous ne pourrez plus utiliser les données cryptées par TPM après cette procédure, mais elles resteront sur le lecteur de disque dur. Effacez ces données et toutes les données internes à l'aide de Hard Disk Data Erase Utility. Pour plus d'informations, consultez les Instructions d'utilisation de cet ordinateur.

## Peux-je désinstaller Security Platform ?


- Oui, vous pouvez.

Cliquez sur  (Démarrer) - [Panneau de configuration] - [Désinstaller un programme] \*<sup>1</sup> et supprimez [Infineon TPM Professional Package]. Avant de désinstaller Security Platform, sauvegardez ou décryptez les fichiers cryptés dans Security Platform. Si vous ne sauvegardez pas ou ne décryptez pas les fichiers, vous ne pourrez pas y accéder après la désinstallation.

Notez que même après la désinstallation, une partie des données restera dans l'ordinateur.


Pour plus d'informations, cliquez sur  (Démarrer) \*<sup>2</sup> - [Tous les programmes] - [Infineon Security Platform Solution] - [Help] - [Bienvenue dans la solution Infineon Security Platform] - [Questions répétitives et dépannage] - [Questions répétitives].

## Je ne peux pas crypter des fichiers. Que dois-je faire ?

- Le lecteur de disque dur doit être formaté dans le volume NTFS. Si [NTFS] est affiché dans [Système de fichiers], vous pouvez crypter les fichiers. Pour vérifier l'état, cliquez sur  (Démarrer) - [Ordinateur] \*<sup>3</sup>, cliquez-droit sur [Disque local (C:)] et cliquez sur [Propriétés].
- Seuls les fichiers enregistrés sur le lecteur de disque dur formaté dans le système NTFS peuvent être cryptés.
- Il se peut que le système de fichier de cryptage (EFS) ne soit pas pris en charge selon les éditions de Windows 7.
- Lorsque vous supprimez le Lecteur personnel sécurisé (PSD), si vous copiez et enregistrez les données et les dossiers dans le PSD comme non cryptés, ils ne seront pas cryptés après la suppression du PSD. Envoyez ou copiez-les dans le dossier vous permettant de les crypter.

## <Windows 7/Windows Vista>

## Le dossier [C:\Utilisateurs] a été crypté par erreur. Puis-je le décrypter ?

- Vous pouvez décrypter le dossier, mais il se peut que les données ne soient pas complètement restaurées. Pour décrypter le dossier, vous devez ouvrir la session de l'utilisateur l'ayant crypté. Si vous ouvrez la session d'un autre utilisateur, il pourrait y avoir des problèmes comme un blocage lors de l'ouverture de session Windows ou un affichage anormal de l'icône des fichiers.
  - ① Ouvrez la session de l'utilisateur qui a crypté le dossier. (Le démarrage de l'ordinateur peut prendre un certain temps.)  
Si le Mot de passe utilisateur de base est demandé, saisissez le mot de passe.
  - ② Cliquez sur  (Démarrer) - [Tous les programmes] - [Accessoires] et cliquez-droit sur [Invite de commandes], et cliquez sur [Exécuter en tant qu'administrateur].
  - ③ Saisissez [cipher /d /s:\Users] et appuyez sur **Entrée**.

- Si le Mot de passe utilisateur de base est demandé, saisissez le mot de passe.

\*1 Windows XP : [démarrer] - [Panneau de configuration] - [Ajouter ou supprimer des programmes]

\*2 Windows XP : [démarrer]

\*3 Windows XP : [démarrer] - [Poste de travail]

## <Windows XP>

### Le dossier [C:\Documents and Settings] a été crypté par erreur. Puis-je le décrypter ?

- Vous pouvez décrypter le dossier, mais il se peut que les données ne soient pas complètement restaurées. Pour décrypter le dossier, vous devez ouvrir la session de l'utilisateur l'ayant crypté. Si vous ouvrez la session d'un autre utilisateur, il pourrait y avoir des problèmes comme un blocage lors de l'ouverture de session Windows ou un affichage anormal de l'icône des fichiers.
  - ① Ouvrez la session de l'utilisateur qui a crypté le dossier. (Le démarrage de l'ordinateur peut prendre un certain temps.)

Si le Mot de passe utilisateur de base est demandé, saisissez le mot de passe.
  - ② Cliquez sur [démarrer] - [Poste de travail] - [Disque local (C:)], cliquez-droit sur [Documents and Settings] puis cliquez sur [Décrypter].
  - ③ Cliquez sur [Confirmation des modifications d'attributs] - [Appliquer les modifications à ce dossier et à tous les sous-dossiers et fichiers] - [OK].
    - Si un message d'erreur s'affiche, cliquez sur [Ignorer] ou [Ignorer tout].
    - Si le Mot de passe utilisateur de base est demandé, saisissez le mot de passe.

### Que dois-je faire lorsque je reçois l'ordinateur réparé ?

- Effectuez "Étape 1 Modification des réglages de Setup Utility" (→ [page 7](#)) et suivez le menu Help de Security Platform pour restaurer les réglages de Security Platform.
- Lorsque vous supprimez le Lecteur personnel sécurisé (PSD), si vous copiez et enregistrez les données et les dossiers dans le PSD comme non cryptés, ils ne seront pas cryptés après la suppression du PSD. Envoyez ou copiez-les dans le dossier vous permettant de les crypter.

© Panasonic Corporation 2005-2009