SecureDoc for Windows

Version 9.1

リファレンス マニュアル

WinMagic SecureDoc

2023 年 2 月

本ガイドの目的

本ガイドは、システム管理者が SecueDoc で暗号化されたデバイスを適切に運用するためのものです。

SES を使って SecureDoc をインストールしたデバイスでは、クライアント側で設定をしたり変更したりする必要はありませんが、クライアントでの設定を確認することで、SecureDoc が提供する機能について理解を深めることができます。

基本的な SES のインストール・初期設定手順、SecureDoc クライアントのインストール手順については

「SecureDoc Enterprise Server Version 9.1 クイックインストールガイド」をご参照ください。

使用頻度の低い機能については割愛しておりますので、予めご了承ください。

SecureDoc for Windows Version 9.1
リファレンスマニュアル

連絡先

WinMagic Inc. （カナダ本社）

200 Matheson Blvd West, Suite 201
Mississauga, Ontario, L5R 3L7
フリーダイヤル： 1-888-879-5879　電話 : (905) 502-7000　Fax : (905) 502-7001
テクニカルサポート : support@winmagic.com

ウィンマジック・ジャパン株式会社

〒105-0022　東京都港区海岸 1-2-3 汐留芝離宮ビルディング 21 階
電話 : 03-5403-6950　Fax : 03-5403-6953
営業 : sales.jp@winmagic.com
テクニカルサポート : support.jp@winmagic.com
URL : https://www.winmagic.co.jp/
https://winmagic.com/ja/home-jp/　(グローバル)

更新履歴

日　付	バージョン	更新内容
2024 年 2 月	v9.1 初版	

ご注意

目 次

1. プリブート認証の使用方法

デバイスの電源を入れると、Windows 起動前に、SecureDoc ブートログオンプログラムが起動します。ここでの認証をプリブート認証と呼び、認証に成功し暗号化されているディスクを復号化することで Windows を起動できます。
暗号化には 2 つの鍵が使われています。DEK（Data Encryption Key）は、デバイスのローカルディスク（SSD/HDD）またはリムーバブル・メディアのデータを暗号化するために使用され、ディスク内に保存されています。DEK は KEK（Key Encryption Key）によって保護され、データの暗号化に使用されている DEK を復号化するためには KEK が必要です。KEK はキーファイル内に保存されています。

ブートログオンプログラムによって表示されるプリブート認証画面には、「ユーザーID」と「パスワード」の入力フィールドがあります。正しい資格情報を入力して認証に成功すると、キーファイル内の KEK を復号化でき、KEK により DEK を復号化することができます。

キーファイルはデバイスに複数登録することができ、キーファイル毎に使用できる鍵や権限の設定がされています。
オーナーID のみのキーファイルが登録されているデバイスと、複数の ID のキーファイルが登録されているデバイスでは、以降の違いがあります。

1.1 カーソルの位置について

デバイスにユーザーが 1 人（ID が 1 つ）のみ登録されているデバイスでは、プリブート認証画面でのカーソル位置は「パスワード」フィールドにあり、ユーザーが 2 人以上登録されている場合、カーソルの位置は「ユーザーID」のフィールドにあります。
例えば、プロビジョニンルールで、オーナーの ID のみが展開されたデバイスでは、カーソルの位置は「パスワード」フィールドにありますが、管理者ユーザーを追加した場合は、デバイスに 2 つの ID があるので、カーソル位置は「ユーザーID」のフィールドにあります。

1.2 資格情報の入力について

プロビジョニンルールで登録されたオーナーは、「パスワード入力」だけでログインできます。
複数の ID が登録されているデバイスでも、プロビジョニンルールで登録されたオーナーは、ID を入力せずに、エンターキーや Tab キーで、ID フィールドからパスワードフィールドに移動し、パスワード入力だけでログインできます。
ID の入力を必須とする設定も可能です。

※ SES でのプロファイル設定 （ID の入力を必須とする）
[Boot configuration] -> [General]
Force user to input User ID at login

1.3 パスワード試行回数の上限について

プロファイル設定で、パスワード試行回数の上限の初期値は 15 回に設定されています。設定した回数に関係なく、3 回ログインに失敗すると、次のメッセージが表示されます。（表示されるメッセージが異なる場合があります。）

「コンピュータに正しくログインしていません。ユーザーID とパスワードが
分かっている場合は、Ctrl+Alt+Del キーを一緒に押して、もう一度お試しください。
ユーザーID またはパスワードが分からない場合は、ヘルプデスクに連絡して指示に従ってください。」

画面下の <リブート> ボタンを押すか、Ctrl+Alt+Del キーで、再起動が必要です。
再起動を繰り返し、誤入力の累計で、パスワード試行回数の上限値に達すると、ユーザーのキーファイルはロックされます。画面に表示されたヘルプデスクとは、SES 管理者のことを示しています。ロックされた場合、SES 管理者に連絡し、チャレンジレスポンスによる解除が必要です。
チャレンジレスポンスの操作方法については、「WinMagic SecureDoc Enterprise Server v9.1 リファレンスマニュアル」をご参照ください。

1.4 パスワード試行回数の上限以外でロックされるケース

デバイスの時刻設定（UEFI/BIOS）が時差を超えて変更された場合、不正な行為としてみなされ、キーファイルをロックします。海外渡航を考慮していますので、大幅に時刻設定を変更しなければ、ロックされることはありません。
デバイスの CMOS クリア等で、大きく時刻がずれた場合もロックされます。ロックされた場合は、チャレンジレスポンスによる解除が必要です。
キーファイルの保護方法で、パスワードではなく TPM 保護を選んでいる場合、TPM クリアをした場合や、マザーボード交換した場合もロックされます。このようなケースは、SES で該当デバイスに登録されているユーザー向けのキーファイルを作成し、USB メモリ等に保存します。ブートログオン画面で、ユーザーID の代わりに、USB 等に保存したキーファイル名と、キーファイルに設定したパスワードでログインすることができます。

1.5 キーボードレイアウトについて

画面右下に、キーボードレイアウトについての設定があり、ユーザーによるレイアウトの変更が可能です。SES で作成しデバイスに適用されたプロファイルで、デフォルトのキーボードレイアウトが設定されていますので、通常、設定変更する必要はありません。

※　パスワードに記号が含まれていた場合、日本語キーボードから他のレイアウトに変更すると影響があります。

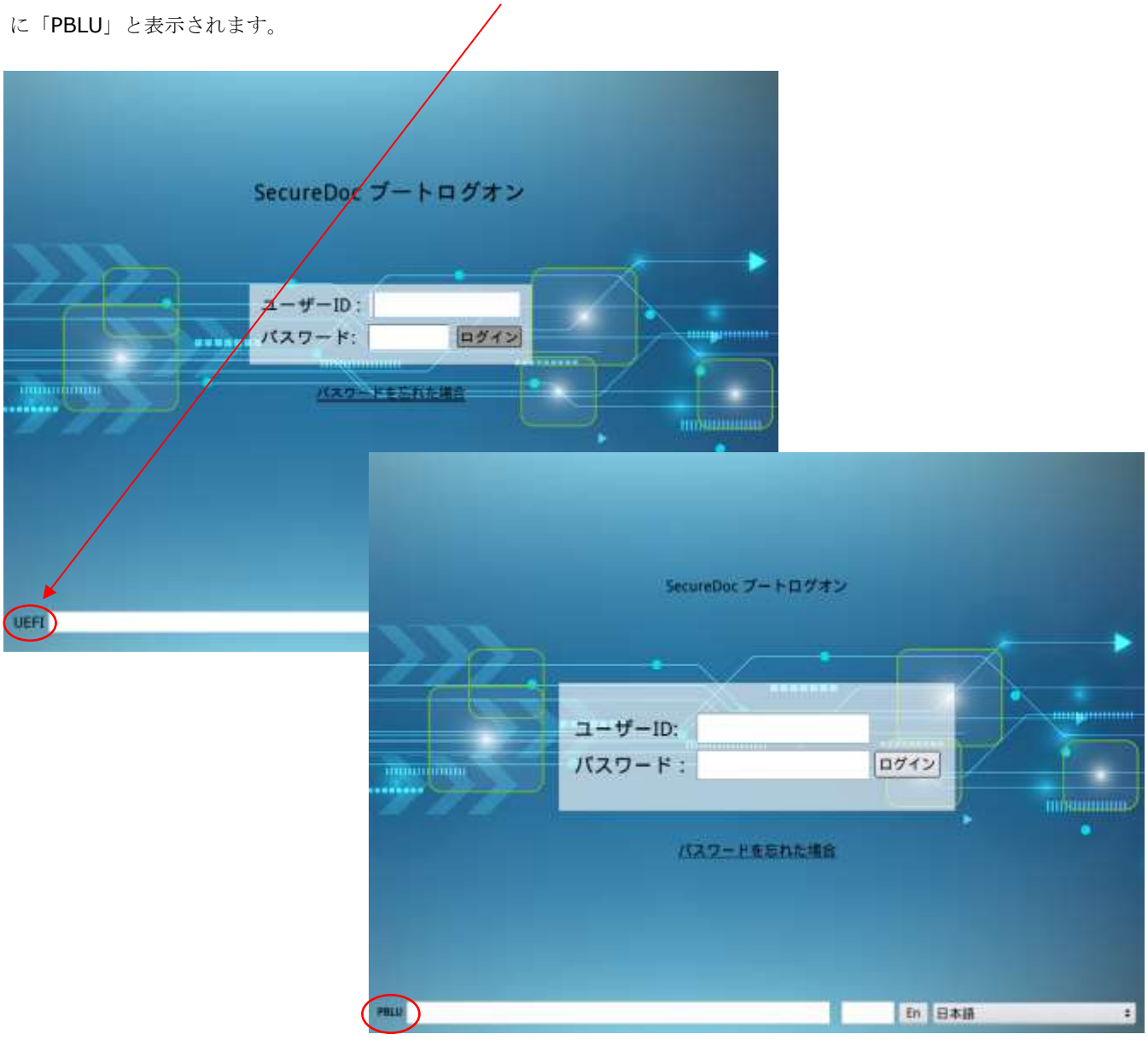
1.6 ファンクションキーについて

ブートログオンプログラムでのファンクションキーについては、次のテーブルを参照してください。

ファンクションキー	説　明
F3 キー	F3 キーを押すと、右下に「i」と「メディア」のアイコンが表示されます。 「i」をクリックするとブートログオンプログラムが検知した NIC を確認でき、プリブートネットワーク認証（PBN）で使用する NIC を設定できます。PBN で使用する NIC の設定は、SES によるプロファイルで設定できます。通常、クライアント側で設定する必要はありません。 メディアのアイコンを表示すると、F7 キーを押した時と同様にサポート情報を保存できます。
F7 キー	サポート情報を保存します。テクニカルサポートから指示があった場合に利用します。
F8 キー	チャレンジレスポンスによるパスワードリカバリ。 画面下に表示されている「パスワードを忘れた場合」をクリックするのと同じ機能です。
F9 キー	リカバリオプション セルフヘルプリカバリーは、日本語をサポートしておりません。

1.7 2 つのブートログオンプログラムについて

UEFI デバイス向けに、SecureDoc には、PBU と PBLU のブートログオンプログラムがあります。
どちらを使用するのかの選択は、インストレーションパッケージに含めるプロファイルで設定します。プロファイル作成時、デフォルトでは PBU が選択されています。プリブートネットワーク認証を設定したが、無線 NIC を利用できない場合、PBLU では利用できる場合があります。（PBLU がサポートする NIC のドライバーライブラリ内に該当する NIC が含まれている場合）
同様に、PBU でタッチパッドが利用できない場合なども、PBLU で動作する場合があります。
PBU が実行されているデバイスでは、画面左下に「UEFI」と表示され、PBLU が実行されているデバイスでは、画面左下に「PBLU」と表示されます。



プロファイルで、PBLU を指定したが、PBLU では正常に起動できないデバイスの場合、自動的に PBU に変更する機能もあります。

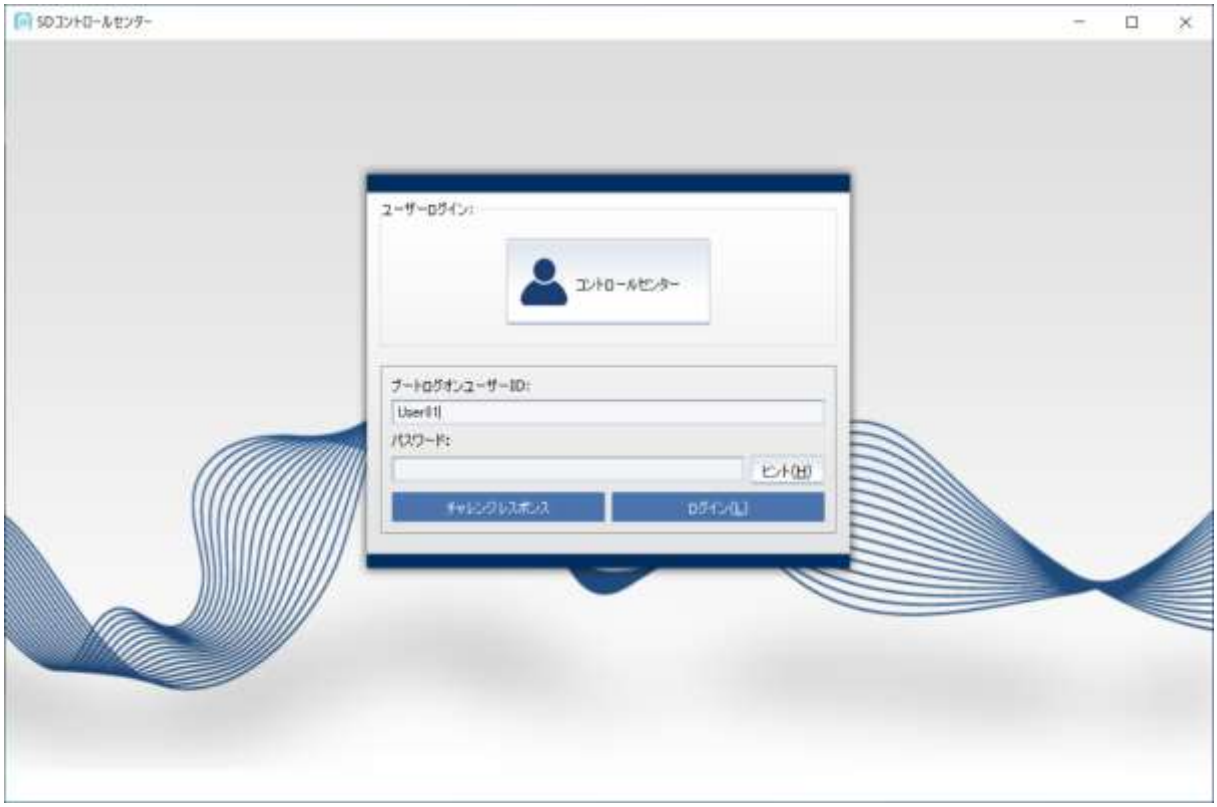
2. 通知領域（タスクトレイ）の SecureDoc 通知アイコンについて

プリブート認証に成功し、Windows が起動すると、SecureDoc クライアントは SDConnex との通信を試みます。通信が行われると、SecureDoc 通知アイコンは、「SecureDoc はサーバーと正常に通信しました」というメッセージを表示します。SDConnex との通信で、例えば、プロファイルの変更など、自分宛に命令（コマンド）があれば、それを受け取り処理します。クライアントのインベントリ情報が変更されている場合は、その情報を SDConnex に送り、SES DB に書き込まれ SES コンソールに反映されます。Windows 起動時の初回通信、あるいは最初のネットワーク疎通時以降は、プロファイルで設定された間隔（デフォルト設定では 60 分毎）で SDConnex との通信を試みます。
SecureDoc アイコンを右クリックして表示されるコンテキストメニューの内容については、下記のテーブルを参照してください。

項　目	説　明
暗号化ステータス	ドライブの暗号化状態を表示します。
SecureDoc コントロールセンター	SecureDoc コントロールセンターを起動します。
サーバーと通信する	SDConnex と通信をおこないます。 クリックすると、プロファイルで設定された間隔とは関係なく、すぐに SDConnex との通信をおこないます。 疎通確認にも役立ちます。
SecureDoc 言語の選択	ブートログオンプログラムと SecureDoc コントロールセンターの言語を個別に設定できます。
診断	SecureDoc がインストールされている状態・環境と、登録されているユーザーを確認できます。 トラブルシューティング時にデバッグログを取得することができます。 サポートから指示があった場合に、ログ取得の設定をおこないます。
ヘルプ	SecureDoc の機能について説明が書かれています。（英語のみ）
詳細	インストールされている SecureDoc のバージョンを確認できます。

3. SecureDoc コントロールセンターについて

SecureDoc コントロールセンターを起動すると、ログイン画面が表示されます。
[ブートログオンユーザーID] のフィールドには、プリブート認証で使用したユーザーID があらかじめ入力されています。
SecureDoc コントロールセンターにログインするには、パスワードを入力して、<ログイン> をクリックします。
他のユーザーID、例えば管理者 ID でログインする場合、ID 名を変更します。プリブート認証でログインしたユーザー以外の ID で、パスワードが不明な場合は、SES 管理者と連絡をとり、<チャレンジレスポンス> をクリックして、指示に従いログインすることもできます。
<ヒント> の機能は、推奨されず、通常使用しません。



SecureDoc コントロールセンターにログインすると、権限により表示される項目が異なります。

パスワード変更権限のみのユーザー**ID** でログインした場合の **SecureDoc** コントロールセンター

全ての権限が付与された **ID** でログインした場合の **SecureDoc** コントロールセンター

[全般] -> [開始ページ]

設　定	説　明
パスワードの変更	SecureDoc のパスワードを変更できます。  パスワードの変更は、<パスワードルール> に設定されているポリシーに従う必要があります。 Windows とのパスワード同期が設定されている環境で、ここでパスワードを変更すると、Windows のパスワードも変更されます。 パスワード同期が設定されている環境で、Windows 側でパスワードを変更した場合、SecureDoc に設定されている<パスワードルール> ではなく、Windows 側（一般には Active Directory）に設定されているパスワードルールに従います。
セルフヘルプ	セルフヘルプリカバリーは、日本語をサポートしておりません。
リカバリメディア	万が一、ブートログオンプログラム起動に問題が発生した場合のリカバリファイルを作成できます。  SES の DB に保存されているので、通常、ここで作成する必要はありません。
認証を変更する	

[全般] -> [監査ログ]

ディスク暗号化の完了やプリブート認証でのログイン結果など、SecureDoc に関連するログが蓄積されます。

<監査ファイルのエクスポート> をクリックすると、監査ファイルを保存することができます。

SES で管理されている SecueDoc クライアントは、起動後の SDConnex との初回疎通時に、ログを SES DB に送ります。管理者は、SES コンソールの [Logs] で、これらのログを閲覧することができます。

[全般] -> [バージョン情報]

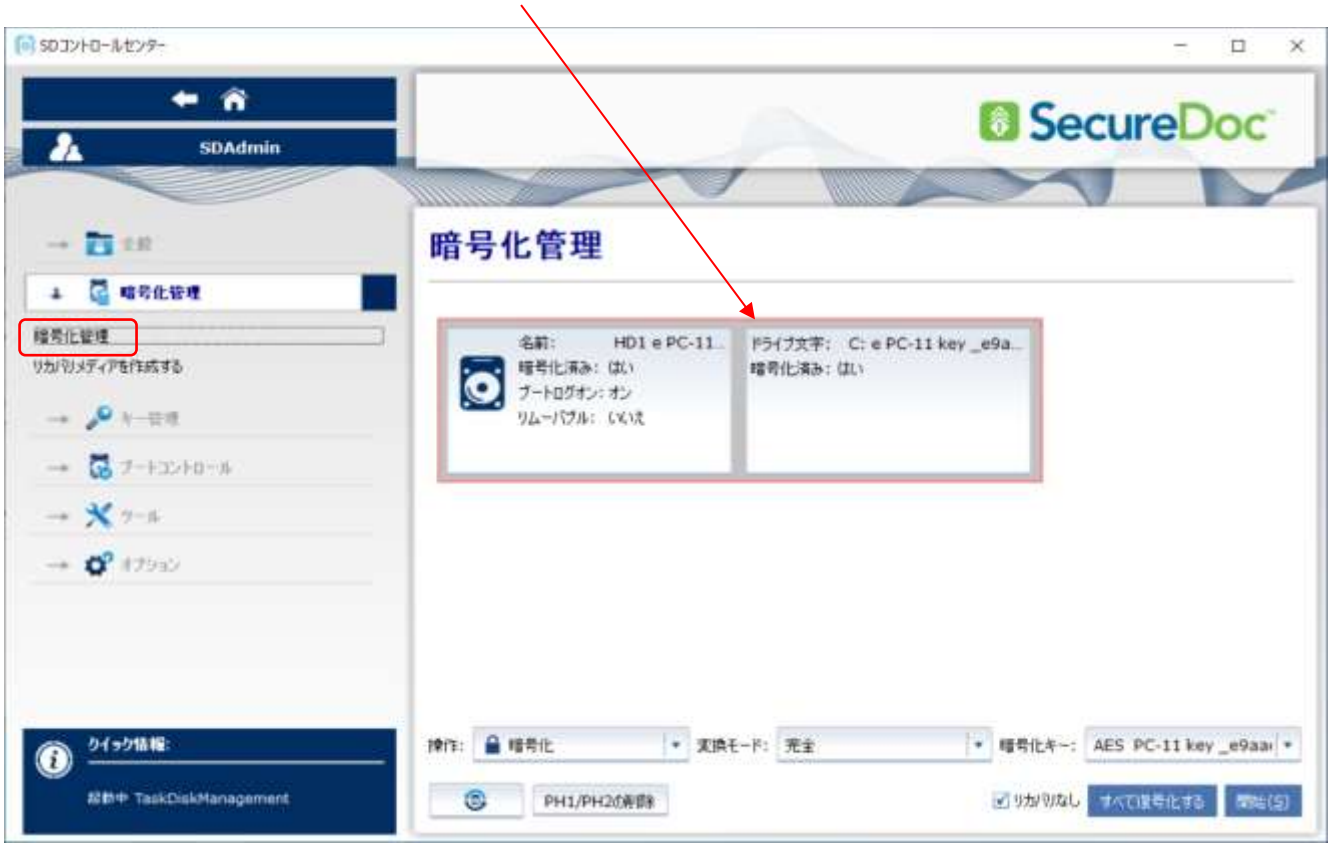
インストールされている SecureDoc のバージョンが表示されます。

[全般] -> [ヘルプ]

HTML 形式での SecureDoc 操作マニュアル。英語のみです。

[ディスク暗号化] -> [暗号化管理]

暗号化管理のパネルでは、ディスクの状態を確認できます。



設　定	説　明
操作:	プルダウンメニューから、[暗号化] あるいは [復号化] を選択します。
変換モード:	[完全] と [標準] から選択できます。 [完全] は、ディスク全体を、[標準] は使用している領域のみを暗号化します。 [標準] を選択した場合、暗号化完了後、暗号化されていないセクタ領域にデータが書き込まれると、都度、自動で暗号化されます。
暗号化キー：	SecureDoc をインストールすると、そのデバイス上で一意の鍵を生成し、デバイス毎に異なる鍵を使ってディスクを暗号化しています。 ユーザーが USB 接続のストレージやメディアを暗号化する場合、暗号化に使用する鍵を選択することができます。SES 管理者によって鍵が付与されていない場合、デバイスのディスク暗号化に使用した鍵だけです。
	リフレッシュボタン ディスクの表示を更新します。
<PH1/PH2 の削除>	SecureDoc は暗号化プロセス中に、一時ファイル（PH1/PH2）を生成します。暗号化プロセスが何らかの理由 （シャットダウンなど）で中断された場合、これらの PH1/PH2 ファイルはそれぞれのディスクあるいは USB ストレージなどに残り、暗号化を再開できなくなる可能性があります。 そのような場合、<PH1/PH2 の削除> をクリックし、一時ファイルを削除できます。
リカバリなし	暗号化時、万一の不具合に備えてリカバリデータを作成し暗号化しますが、このオプションを選択するとリカバリデータを作成せずに暗号化を実行します。ドライブの暗号化を早く完了さ

設　定	説　明
	せたい場合に役立ちます。 既にユーザーが使用している、重要なデータがあるデバイスの場合、このオプションは推奨されません。選択した場合、暗号化が完了するまで、電源コードを接続し、OS のシャットダウンや電源を切らないようにしてください。
すべて復号化する	管理者権限を持つユーザーは、デバイスのすべてのディスクを 1 回のプロセスで復号化できます。

[ディスク暗号化] -> [リカバリメディアを作成する]

ブートログオンプログラム起動に問題が発生した場合のリカバリファイルを作成できます。

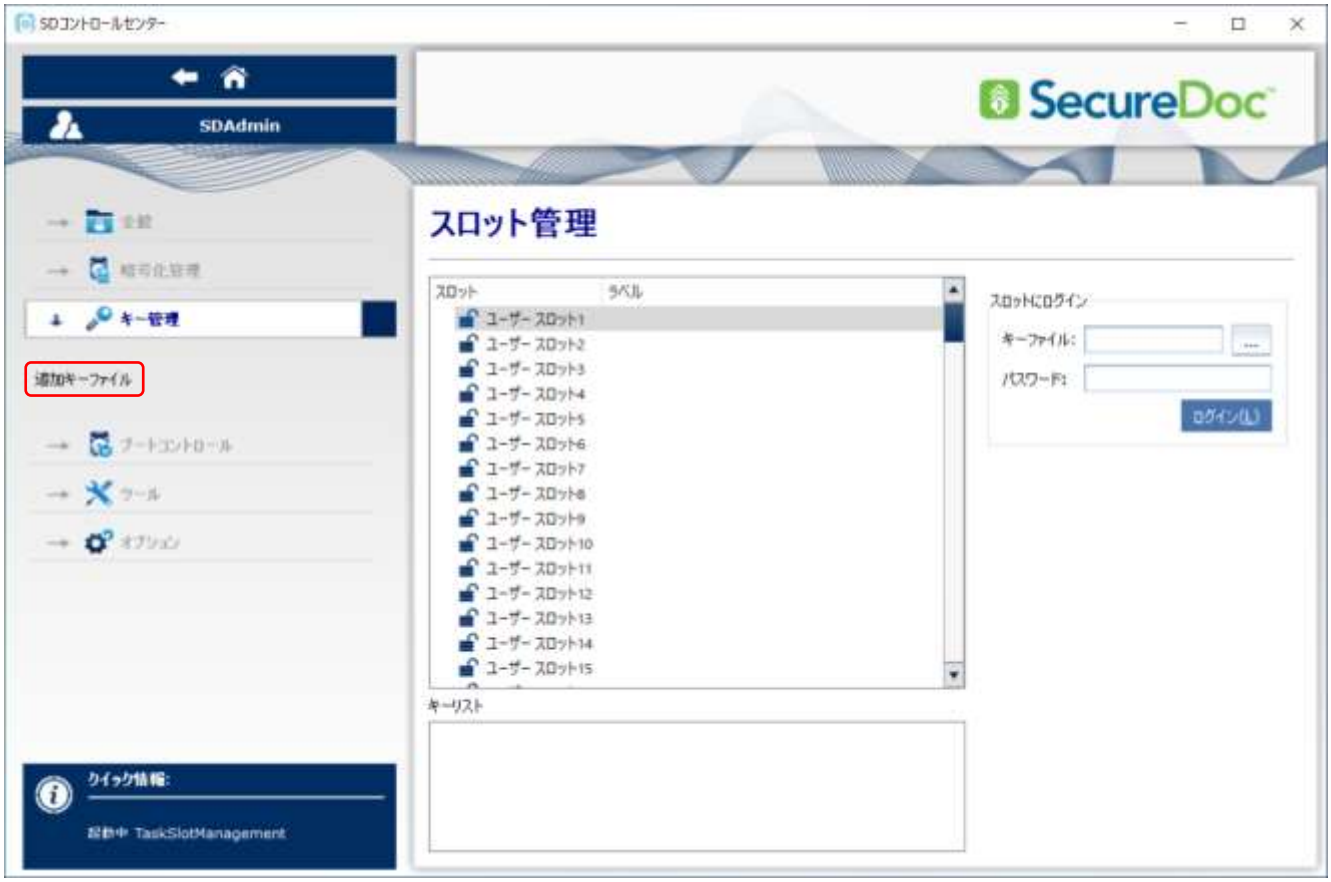
SES で管理されているクライアントは SES の DB に保存されているので、通常、ここで作成する必要はありません。

[キー管理] -> [追加キーファイル]

現在のスロットからキーファイルを削除するには、そのファイルを選択して [ログアウト] をクリックします。

キーファイルをスロットに追加するには、スロットを選択後、キーファイルを選択し、パスワードを入力し、 ログインをクリックします。

通常、これらの操作は、管理者が SES コンソールで操作し、SDConnex を経由してクライアントデバイスに追加します。



[ブートコントロール] -> [ブートログオンのインストール/アンインストール]

このパネルでは、ブートログオンプログラムのインストールやアンインストール、更新をおこなうなうことができます。

[ブートコントロール] -> [ブートログオンのインストール/アンインストール] -> [インストール]

ディスクを選択して、ブートログオンプログラムのインストールをします。

既に SecureDoc がインストールされているデバイスでは、ブートログオンはインストールされています。

[ブートコントロール] -> [ブートログオンのインストール/アンインストール] -> [更新]

ブートログオンプログラムを更新する必要がある場合や、登録できるユーザー数を変更することができます。

SecureDocSe クライアントをバージョンアップした場合、ブートログオンプログラムは自動で更新されます。

[ツール] -> [ディスクアクセスコントロール] -> [アンインストール]

ディスクを選択して、ブートログオンプログラムのアンインストールができます。

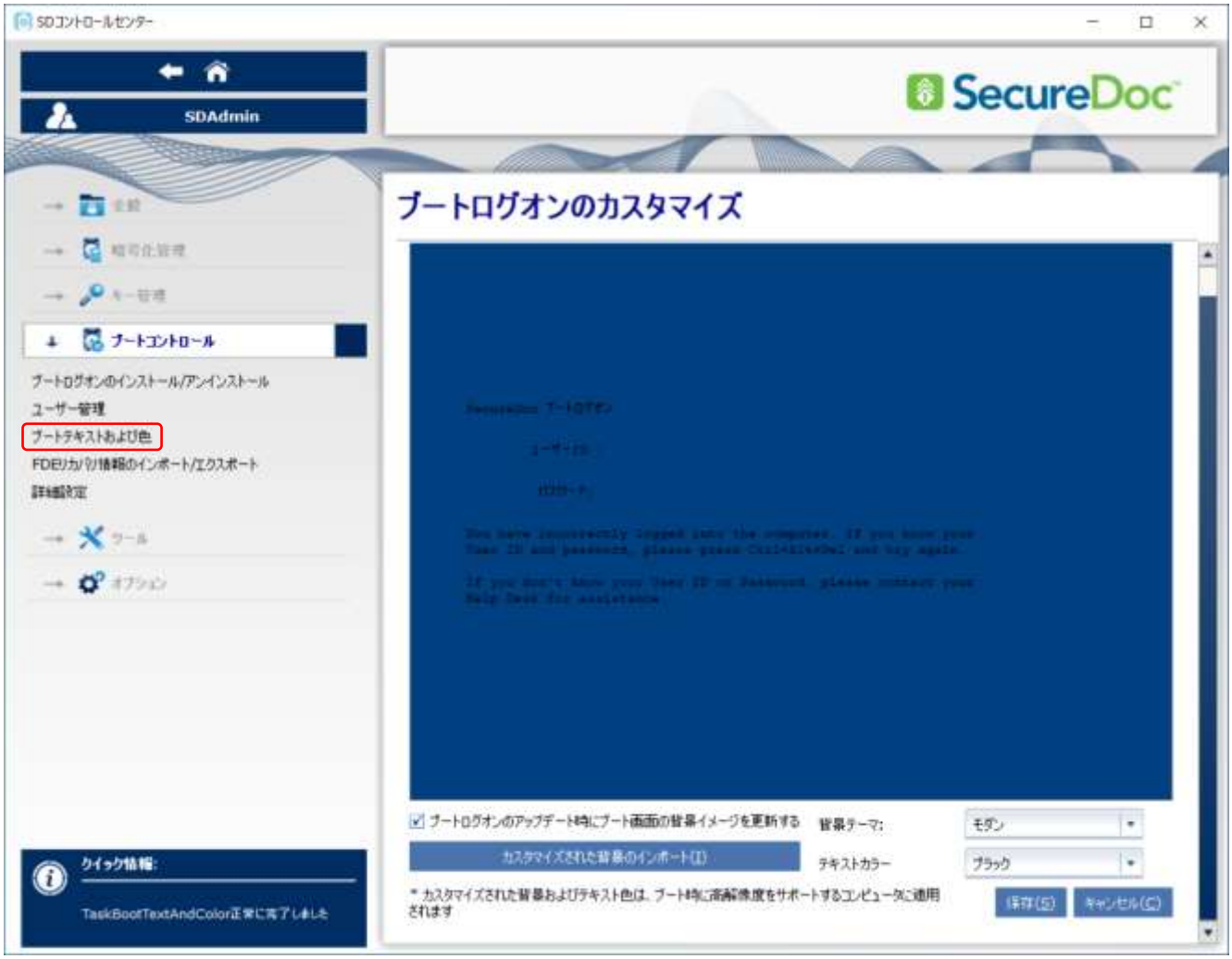
アンインストール前にディスクの復号化が必要です。

[ブートコントロール] -> [ユーザー管理]

　このパネルでは、ユーザーの追加やロックされたユーザーのロック解除がおこえなます。
SES クライアントでは、管理者が SES コンソールを使って、ユーザーの追加やロックされたユーザーのロック解除（チャレンジレスポンス）が可能です。

[ブートコントロール] -> [ブートテキスト及び色]

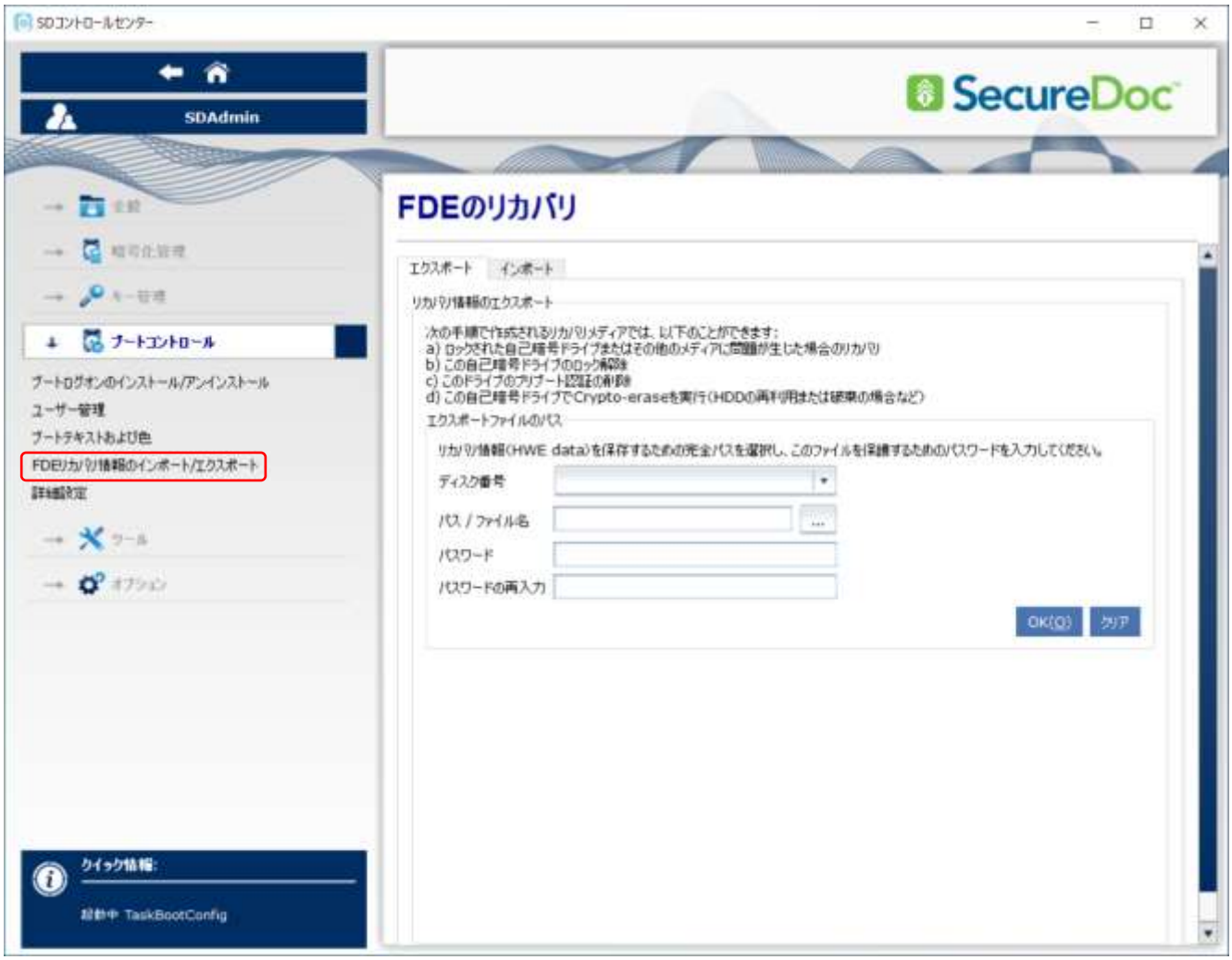
プリブート認証画面をカスタマイズできます。



[ブートコントロール] -> [FDE のリカバリ情報のインポート/エクスポート]

このパネルでは、TCG Opal ディスクのリカバリディスクを作成できます。

SES で管理されているクライアントでは、SES DB に自動で作成されています。



[ブートコントロール] -> [詳細設定] -> [全般設定]

このパネルでは、ブートログオンの基本設定をおこないます。

項　目	説　明
Legacy ブートローダー	BIOS デバイス向け　ブートログオンプログラムの選択
○ V5 ブートローダーだけを使用する	V5 ブートログオンプログラムのみ設定します。
○ デフォルトで V5 ブートローダーを使用し、オプションとして V4 を使用する	V5 ブートログオンプログラムを使用し、それがうまく動作できないときに旧 V4 ブートログオンプログラムをフォールバックとして使用するように設定します。（デフォルト設定）
○ V4 ブートローダーだけを使用する	旧 V4 ブートログオンプログラムのみ設定します。
○ デフォルトで V4 ブートローダーを使用し、オプションとして V5 を使用する	旧 V4 ブートログオンプログラムを使用し、それがうまく動作できないときに V5 ブートログオンプログラムをフォールバックとして使用するように設定します。
UEFI ブートローダー	UEFI デバイス向け　ブートログオンプログラムの選択
○ PBU: ネイティブ UEFI プリブート環境	デフォルトのブートログオンプログラム

項　目	説　明
○ PBLU: UEFI デバイス用 Linux プリブート	PBU では正常に動作しない、あるいはブートログオン時にスマートカードや NIC が動作しない場合、PBLU をお試しください
☐ UEFI BootOrder を使用する	UEFI のブートオーダー機能を使用し、順番 1 から起動します。 1. SecueDoc Boot Logon 2. Windows Boot Loader
☐ UEFI ドライバフックを使用する	UEFI のドライバーバインディングが実装されている UEFI デバイス向けの設定です。UEFI ドライバーバインディングは特別なプロトコルであり、ドライバーを起動および停止するための機能と、特定のドライバーが特定のコントローラーを管理できるかどうかを決定するための機能があります。
☐ キーファイル入力をマスキングする (***)	ユーザーの入力した文字がアスタリスクに置き換えられます。 （パスワードはデフォルトで常にこの方法で処理されます。）
☐ 簡易サインオンを有効にする	ユーザー資格情報を統合サインオン DLL に渡します 。 (SecureDoc Enterprise クライアントのみの機能) SecureDoc からのパラメーターを受け入れるように DLL をセットアップしており、その DLL がブート ログオン時に入力されたユーザー名とパスワードを取得するようにする場合は、このオプションをオンにします。
☐ ゼロの場合、PCMCIA I/O アドレスを変更する	ブートログオンがノート PC の PCMCIA リーダーを検出できない場合、アドレス指定に問題がある可能性があります。また、場合によっては、SecureDoc でアドレスを正しく検出できるように、ノート PC の PCMCIA I/O アドレスをデフォルトアドレスの「D0000000」に変更する必要があります。
☐ ログイン時にユーザーID の入力を強制する	ブートログオン時にユーザーID の入力を必ず必要とする。 選択していない場合、デフォルトのユーザーID では入力を必要としません。
☐ スマートカード + パスワード認証。 Windows で使用しているスマートカードから派生したユーザーID	スマートカードとパスワード認証の場合、ユーザーID は Windows で使用されているスマートカードから取得します。
☐ オートブート機能を無効にする	オートブート機能を無効にして、プリブート認証のバイパスを防ぎます。
☐ サイレントオートブートを有効にする（ブートログオン認証を省略）	オートブート機能を有効にします。 チェックを入れると、ユーザーがまだブートログオンを通して認証されていない場合でも、オートブートを実行できるようになります
☐ユーザーがパスワードを入力せずに SecureDoc コントロールセンターにログインするのを許可する	認証なしで Secure Doc コントロールセンターにログインできるようにします。必要に応じて常時オートブートが有効なデバイスに適用します。オートブートの場合、ユーザーのキーファイルを使用せずに実行されるため、ID/パスワードの資格情報を知らないユーザーは SecureDoc コントロールセンターにログインできません。
☐リモートコマンドによってパーマネントオートブートをアクティブにした後、自動的にマシンをリブートする	SES からリモートコマンドで永続的なオートブート機能を有効にした後、マシンを自動的に再起動します。
ブートログオン時のログイン最大許容回数 X	プリブート認証で許可されるログイン失敗回数の最大値を設定できます。累計で設定された回数に達すると、キーファイルは自動的にロッ

項　目	説　明
	クされます。 初期値「15」 デバイスのロックを解除するには、管理者キーファイルまたはパスワードリカバリが必要です。別のキーファイルでログインが成功した場合でも、ロックされたキーファイルは解除されません。
MBR アクセスモード；	Master Boot Record へのアクセスに関する制御が可能です。 BIOS 向けの機能です。UEFI デバイス向けの機能ではありません。 [アクセスモード 0] 他のプログラムに MBR を変更させないように保護します。 [アクセスモード 1] MBR の変更を許可します。 [アクセスモード 2] MBR への変更操作をしようとしているプログラムを操作して、MBR が実際には変更されていないのに、変更されていると認識させます。(ほとんど使用されません) [アクセスモード 3] パーティションテーブルの変更を許可します。
仮想 MBR	拡張ブートレコードの設定で、常に初期設定値「はい」のままにしておきます
Special BIOS Mode	ハードウェアのコントローラーがデバイスの起動に影響を与えている場合に使用します。 WinMagic テクニカルサポートに相談した上で利用してください。
Special Y Mode: X	MBR の優先順位を変更する必要がある場合に使用します。 WinMagic テクニカルサポートに相談した上で利用してください。
☐ SUSAM を有効にする	ハードウェアがプリブート環境にサポートされているかどうか不明な場合にチェックを入れます。

[ブートコントロール] -> [詳細設定] -> [詳細設定]

このパネルの設定は、テクニカルサポートから指示があった場合のみ設定を変更してください。

項　目	説　明
X Start:	デフォルト設定；040
X Size:	デフォルト設定；7c40
X After:	デフォルト設定；0000
X Size:	デフォルト設定；7c40
X-Mode:	デフォルト設定；45
DVD mode:	0
Boot Parameters:	ブートログオンプログラム起動時に、ここで設定したパラメーターを実行します。
プリブート機能	
☐ 詳細 ATR モード（ほとんどのカードで非推奨）	スマートカードで、Advanced ATR (Answer-To-Reset) 属性を有効にする場合（ほとんどのカードには推奨されません）

[ブートコントロール] -> [詳細設定] -> [タブレット PC]

項　目	説　明
タブレット PC のサポート	「自動検出」が選択されています。 インストールプロセス中にタブレット PC を検出した場合、スクリーンキーボードを設定します。 不要な場合、「いいえ」を選択できます。

[ブートコントロール] -> [詳細設定] -> [Crypto-erase 設定]

次のオプションを有効にすると、プリブート認証画面で、設定したキーを押すことで鍵を削除できます。
鍵を削除すると、復号化できなくなりますので、OS は起動できず、データへのアクセスはできなくなります。

☐　キーストロークシーケンスを使用してユーザーがプリブート時にデバイスを crypto-erase することを許可する

設定する場合、１つのキーで実行することも、複数のキー（キー１、キー２、キー３）を組み合わせることもできます。

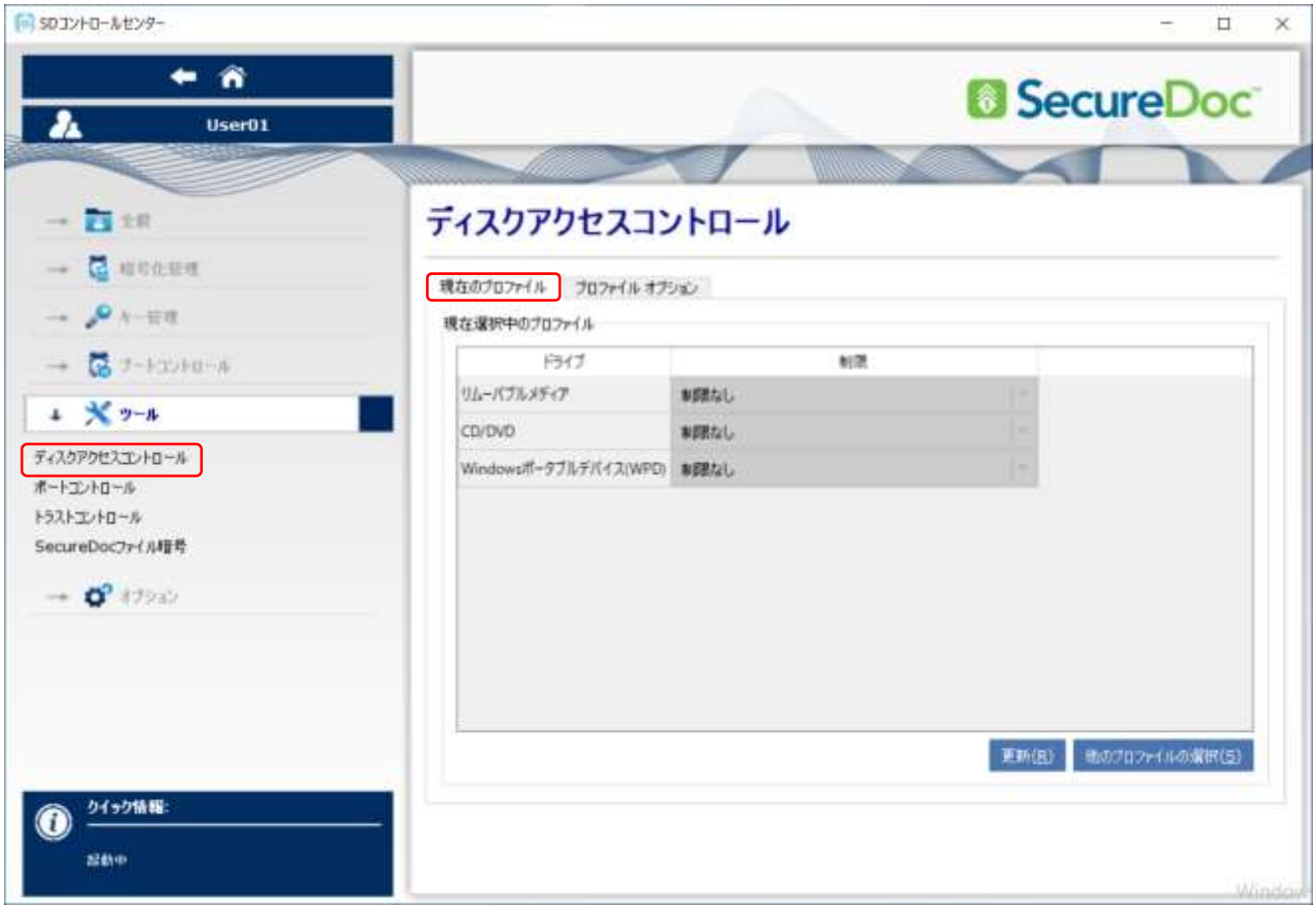
例えば、F4 キー ＋ SHIFT キー ＋ Ctr キー

誤ってキーを押した場合など、中止までの時間（秒）を設定できます。

[ツール] -> [ディスクアクセスコントロール] -> [現在のプロファイル]

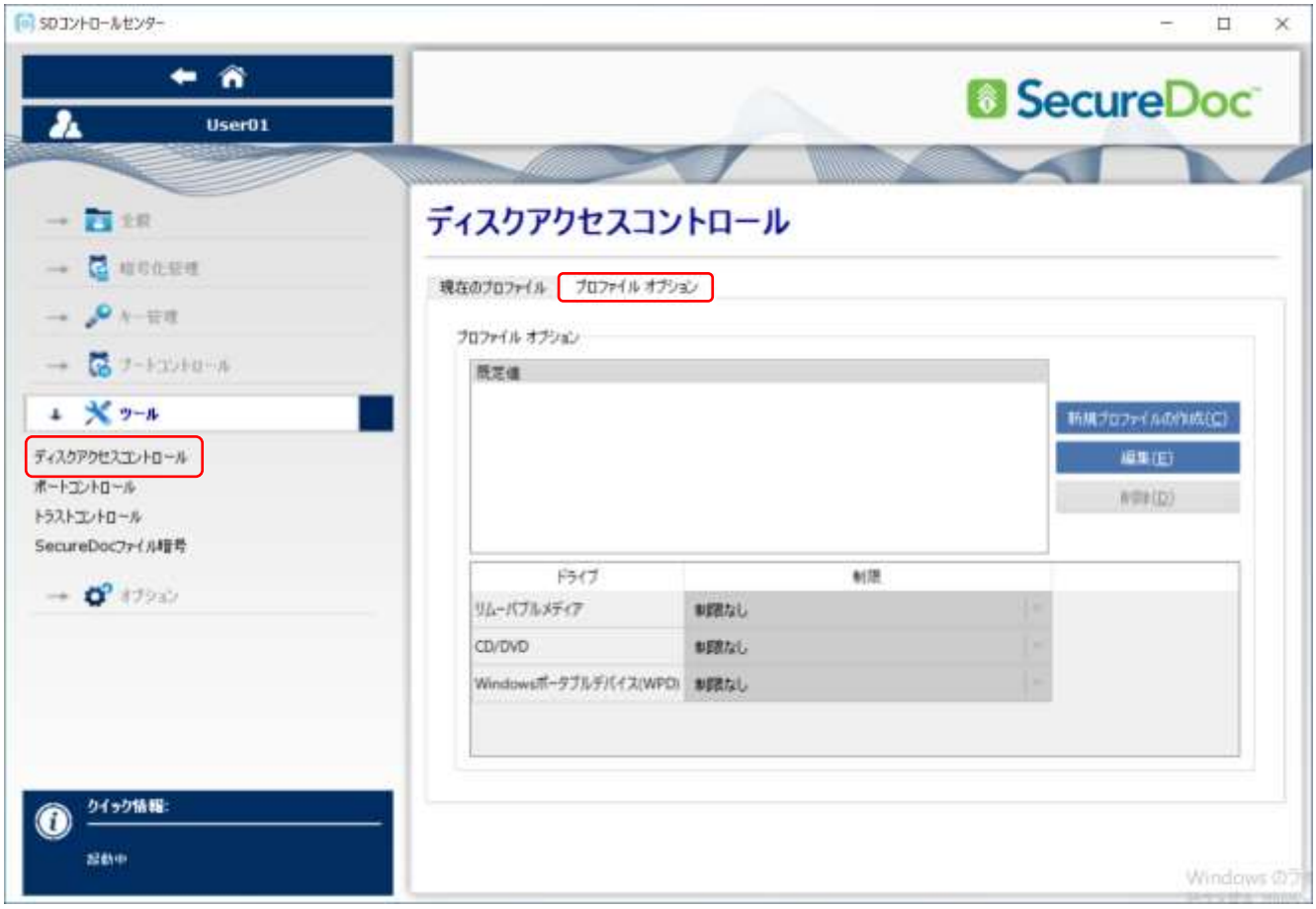
ディスクアクセスコントロール機能を使うと、リムーバブルメディア、CD/DVD、Windows ポータブルデバイス（WPD）へのアクセスを制限することができます。

現在のプロファイルタブでは、リムーバブルメディア、CD/DVD、Windows ポータブルデバイス（WPD）へのアクセスについて、現在の設定内容が表示されます。



リムーバブルメディア、CD/DVD、Windows ポータブルデバイス（WPD）へのアクセスを制限する場合は、[プロファイルオプション] タブをクリックしてプロファイルを作成します。
作成したプロファイルを適用するには、<他のプロファイルの選択> をクリックして、一覧から選択します。

[ツール] -> [ディスクアクセスコントロール] -> [プロファイルオプション]



プロファイルオプションで、規定値を変更する場合は、<編集> をクリックします。

新規に作成する場合は、<新規プロファイルの作成> をクリックします。

ドライブ	制　限
リムーバブルメディア	リムーバブルメディアへの制御方法を選択します。 ・ 制限なし ・ 読み取り専用、暗号化されている場合を除く ・ アクセスなし、暗号化されている場合を除く ・ 読取専用 ・ アクセスなし
CD/DVD	CD/DVD の制御方法を選択します。 ・制限なし ・読取専用
Windows ポータブルデバイス（WPD）	Windows ポータブルデバイスへの制御方法を選択します。 ・制限なし ・読取専用 ・アクセスなし

[ツール] -> [ポートコントロール]

本機能を使用すると、接続して使用するデバイスを制限することができます。

① <インストール> をクリックします。再起動を要求されます。

② 再起動後、<管理> をクリックします。

③ [○ ポートコントロールを有効にする] をクリックします。

初期設定で、「ヒューマンインタフェースデバイス」、「マウス」、「キーボード」が許可されています。

許可するものを登録するには、<追加> をクリックします。

④ 特定のデバイスクラス単位で承認する場合は、[デバイスクラスを許可] ラジオボタン、

特定のモデルのデバイス単位で承認する場合は、[デバイスモデルを許可] ラジオボタン、

特定のデバイスのみを承認する場合は、[個別のデバイスを許可] ラジオボタン

を選択し、<次へ> をクリックします。

[デバイスクラスを許可]を選ぶ場合

① <次へ> をクリックすると、次の画面が表示されます。

② 許可するデバイスクラスを選択し、<選択したデバイスクラスの追加> をクリックします。

③ 前の画面に戻ります。選択したデバイスクラスが「許可されたデバイス一覧」に追加されています。

[デバイスモデルを許可]を選ぶ場合

① 設定するデバイスを接続します。

② <次へ> をクリックします。次の画面が表示されます。
[□ これまでに接続されたデバイスを表示する] をクリックします。

③　許可するデバイスを選択し、<選択したデバイスモデルの追加> をクリックします。

④　前の画面に戻ります。選択したデバイスモデルが「許可されたデバイス一覧」に追加されています。

[個別のデバイスを許可] を選ぶ場合

①　設定するデバイスを接続します。

②　<次へ> をクリックします。次の画面が表示されます。
[☐ これまでに接続されたデバイスを表示する] をクリックします。

③　許可するデバイスを選択し、<選択したデバイスの追加> をクリックします。

④　前の画面に戻ります。選択したデバイスが「許可されたデバイス一覧」に追加されています。

[ツール] -> [トラストコントロール]

本機能を使用すると、IHV 製の暗号化機能付き USB メモリを、SecureDoc によって暗号化した USB メモリと同様に、「ディスクアクセスコントロール」機能で暗号化された USB メモリとして扱えます。

手動で、ベンダーID やプロダクト ID を入力して設定する方法と、デバイスに接続して検知した情報を利用して設定する方法があります。

① <追加> をクリックします。

② 次の画面が表示されます。

手動で入力して設定する場合

① [◎ 信頼する個別デバイスの詳細を入力する] を選び、<次へ> をクリックします。

② 次の画面が表示されます。
VIDA 名（ベンダーID 名）、PID 名（プロダクト ID 名）は、後で判別できるような名称を入力します。
VID、PID は、それぞれ正しい ID を入力します。
HWE 属性は、「読み取り専用」、「プライベート」、「インターセプトなし」の選択肢があります。通常は、「プライベート」を選択してください。

③ <デバイスの追加> をクリックします。

④ トラストコントールのトップ画面に戻り、入力したデバイスが追加されていることを確認します。

⑤ ポートコントロールで、期待する動作となることを確認してください。

デバイスに接続して検知した情報を利用

① [◎ デバイスモデルによる信頼する（例えば、...）] を選び、<次へ> をクリックします。

② 次の画面が表示されます。

③ [☐ これまでに接続されたデバイスを表示する] をクリックします。

④ [☐ これまでに接続されたデバイスを表示する] をクリックします。

⑤ 表示された一覧から、デバイスの HWE Attribute（属性）の設定で、通常は、プルダウンメニューから「プライベート」を選択します。

⑥ <選択したデバイスモデルの追加> をクリックします。

⑦ トラストコントールのトップ画面に戻り、入力したデバイスが追加されていることを確認します。

⑧ ポートコントロールで、期待する動作となることを確認してください。

[ツール] -> [SecureDoc ファイル暗号]

フォルダの暗号化機能を利用する場合

① [☐ ユーザによる特定のファイル及びフォルダの暗号化を許可する] にチェックを入れ、<適用> をクリックします。
フォルダ暗号を有効にするには、再起動が必要です。

② 通知領域（タスクトレイ）の SecureDoc 通知アイコンを右クリックすると、[SecureDoc ファイル暗号] が追加されており、[フォルダ暗号] を実行します。

③ SecureDoc フォルダ暗号化マネージャー 画面が表示されます。

※ SES 管理者が、SES コンソールでファルダ暗号を設定しクライアントに適用している場合、エンタープライズポリシーに、その設定が表示されます。（オプションライセンスが必要です。）

クライアントデバイスの所有者が、エンタープライズポリシーとは別に、フォルダの暗号化をおこなう場合は、"フォルダに鍵" が書かれているアイコンをクリックします。

④ 暗号化するファルダを選択し、暗号化をおこなうための鍵を選択します。鍵が 1 つかしかない場合、その鍵はディスクの暗号化に使われている鍵です。
<フォルダの暗号化> をクリックします。

⑤ SecureDoc フォルダ暗号化マネージャー の画面に戻ります。
更新のアイコンをクリックして、暗号化されたことを確認します。

※ フォルダ内のファイルには鍵のアイコンが付与されており、暗号化されていることを確認できます。

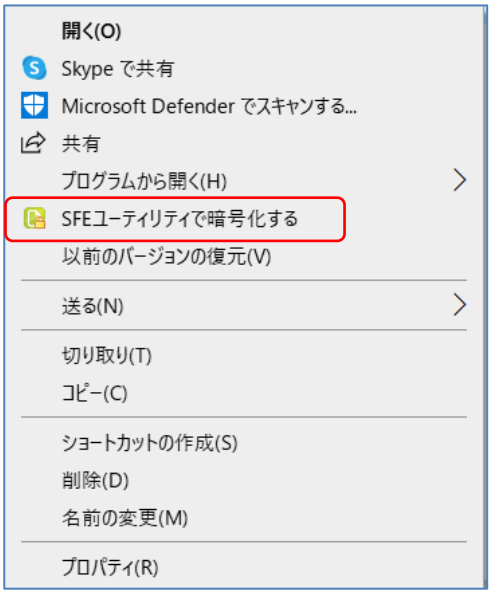
注　暗号化されていないフォルダにファイルを移動すると、自動で復号化されます。

⑥　フォルダ暗号化の設定を解除する場合は、”フォルダに開いた鍵” が書かれているアイコンをクリックします。
実行する前に、ファイルをフォルダ暗号化の設定をしていないフォルダに移動してください。

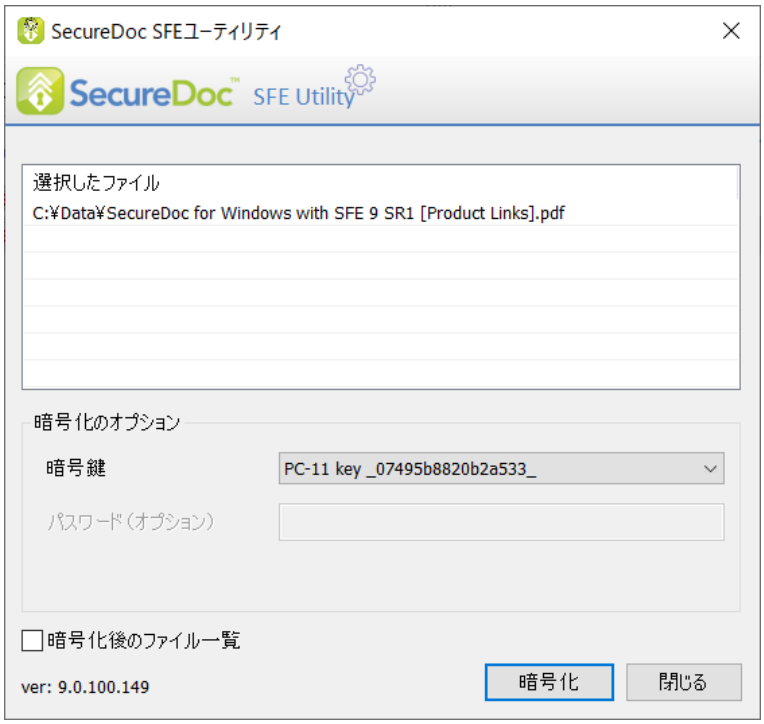
ファイルの暗号化機能を利用する場合

①　[☐ ユーザーが Windows のコンテキストメニューを使ってファイルを暗号化・復号化を許可する] にチェックを入れ、<適用> をクリックします。
ファイル暗号を有効にするには、再起動が必要です。

②　暗号化したいファイルを選んで、右クリックのコンテキストメニューから、[SFE ユーティリティで暗号化する] を実行します。



③ SecureDoc SFE ユーティリティ画面が表示されます。暗号鍵を選択して、<暗号化> をクリックします。
鍵が 1 つかしかない場合、その鍵はディスクの暗号化に使われている鍵です。



④ 保存先を選んで、保存します。

※ ファイルには鍵のアイコンが付与されており、暗号化されていることを確認できます。

注 暗号化したファイルを移動しても暗号化は維持されます。コピーした場合は復号化されます。

⑤ 復号化する場合、右クリックのコンテキストメニューから、[SFE ユーティリティで復号化する] を実行します。
SecureDoc SFE ユーティリティ画面が表示されるので、<復号化> をクリックします。
保存先を選んで、保存します。

注 次の機能は、EOL になる予定です。使用する場合は、事前にテクニカルサポートにご確認ください。

☐ 暗号化を維持する – 保存される場所にかかわらずファイルは暗号化されたままにする

☐ ユーザーが暗号化ファイルにアクセスするアプリケーションリストの管理を許可する

[オプション] -> [全般オプション]

設　定	説　明
カスタムエラー メッセージ	デフォルトのエラーメッセージをカスタマイズできます。
☐ ブートログオンのインストールの後に通常続くリブートを無効にする	SecureDoc のブートログオンインストール後、OS の再起動をおこなわないようにします。
☐ ブートログオン時に、デフォルトでトークン上のキーファイルを使用する	キーファイルの認証にトークンを使用することとし、パスワードによる認証を無効にします。チェックを入れると、プリブート認証時にディスクではなく、トークンを検索します。
☐ “トークン上のキーファイル”を使用する場合、次回も必ず使用する	プリブート認証でユーザーが認証情報を入力すると、プリブート認証プログラムはキーファイルをサーチします。キーファイルがディスク内ではなくトークンにある場合、それを記憶させます
☐ ユーザーのブートキーファイルはユーザのブートキーファイルで自動的にログインする	暗号化の設定で、 [Only encrypt Removable Media (RME)] を選択した場合に、プリブート認証を必要としない設定です。 「Boot Configuration」設定で、 [Force permanent Auto-Boot] オプションが有効になっている必要があります。
☐ 中断された暗号化を自動的に継続する	何らかの理由で暗号化が中断された場合でも、暗号化を自動的に再開させます。
☐ SecureDoc パスワードと Windows パスワードを同期化する（双方向）	チェックを入れると、ユーザーの Windows パスワードが、SecureDoc のキーファイルパスワードと自動的に同期されます。Windows パスワードの変更は自動的に SecureDoc に適用され、SecureDoc パスワードの変更も Windows に適用されます。 プロビジョニングルールを使用する場合は、チェックを入れる必要があり

設　定	説　明
	ます。チェックを入れていない場合、パッケージ作成時にアラートが表示され、プロファイルを変更するよう促されます
☐ Windows エクスプローラーコンテキストメニューで自己復号化ファイル暗号を表示する	ユーザーは、Windows エクスプローラーのコンテキスト メニューを使用して 自己解凍アーカイブを作成できます。
☐ Windows エクスプローラーコンテキストメニューで SecureDoc ファイル暗号を表示する	ユーザーは、Windows エクスプローラーのコンテキスト メニューを使用してファイルを暗号化できます。
☐ Windows Explorer コンテキストメニューで、[ファイルのワイプ]オプションを有効にする	このオプションを選択すると、エクスプローラーの右クリックコンテキストメニューにオプションが追加され、ファイルを上書きして消去できます。
☐ 連続した Windows ログオンのパスワード間違いを検出しデバイスを保護する	プリブート認証で許可されるログイン失敗回数の最大値を設定できます。累計で設定された回数に達すると、キーファイルは自動的にロックされます。 初期値「15」 デバイスのロックを解除するには、管理者キーファイルまたはパスワードリカバリが必要です。別のキーファイルでログインが成功した場合でも、ロックされたキーファイルは解除されません。
連続して Windows ログインに失敗した場合、再起動し.....回数:	パスワードの試行回数を許可する回数をさらに定義することができます。Windows ログインに連続して失敗した回数が、ここで設定した回数に達すると、再起動し、プリブート認証（BitLocker 回復コンソール）に切り替えます。
キーファイルの TPM 保護（TPM が使用可能なデバイスの場合）	・TPM を使用しないでください ・パスワードで保護されたキーファイルを自動的に TPM で保護します ・パスワードの代わりに TPM と PIN で保護されたキーファイルを作成する

[オプション] -> [通信]

設　定	説　明
通信設定	
☐ SDConnex を使用してサーバーと通信する	クライアントデバイスは、SDConnex との通信をおこないます。 特別な理由がない限り、この設定は解除しないでください。
デフォルトに設定/ボタンテキスト：	<編集> をクリックして、SDConnex がインストールされたサーバーの IP アドレスまたは FQDN 名を入力します。最大 16 台設置できます。 クライアントは、ここで指定された SDConnex と通信をおこないます。 複数の SDConnex が設置されている場合、接続先 SDConnex の優先順を設定できます。クライアントは、有線グループ 1 の SDConnex と接続できなかった場合、有線グループ 2 の SDConnex との接続を試みます。 

設　定	説　明
ポート番号：	クライアントが SDConnex と通信する際のポート番号を指定します。 規定値は「7100」です。
プロキシ	クライアントがプロキシサーバーを経由して SDConnex と通信する場合に設定します。 
☐ 優先グループ内でランダムに SDConnex サーバーと通信する	複数の SDConnex で有線グループの設定を 1 にし、このオプションを有効にすると、クライアントは 有線グループの設定が 2 の SDConnex へのアクセスを試みる前に、有線グループの設定が 1 の SDConnex へランダムにアクセスを試みます。
通信間隔設定：	
サーバーとの通信間隔 x 分	クライアントは、OS 起動時（サービス開始時）に SDConnex との最初の通信を試みます。その後は、ここで指定された間隔で SDConnex との通信を試みます。規定値は「60」分です。
次の期間サーバーと通信がない場合、コンピュータへのユーザーアクセスを無効にする x 日	指定した日数内にクライアントが SDConnex と通信しなかった場合、自動的に全てのユーザーのキーファイル（管理者キーファイルを除く）をロックさせます。ロック解除にはチャレンジ&レスポンス機能を使います。 クライアントは、OS 起動時（サービス開始時）に SDConnex との最初の通信を試みます。その後は、ここで指定された間隔で SDConnex との通信を試みます。規定値は「60」分です。
電子メールマシン情報オプション：	
電子メール：	SDConnex と通信できない場合、デバイス情報を登録するのに必要な情報をメールで送信する宛先を入力します。 プロビジョニングルールでは、SDConnex との通信が必要なため、通常は使用しません。
PBConnex	
☐ プリブート時に固定 IP 設定を使用する	プリブートネットワーク認証で固定 IP を利用できるようにします。 プリブートネットワーク認証で使用する IP アドレスの設定は、Windows の IP アドレス設定を参照します。Windows の IP アドレス設定が DHCP クライアントの場合、プリブートネットワーク認証をおこなうブートログオンプログラムは DHCP クライアントとして動作します。 このオプションを有効にすると、Windows の設定が DHCP ではなく固定 IP を使用している場合、Windows で設定されている固定 IP アドレスをプリブートネットワーク認証で使用する IP アドレスに設定します。

[オプション] -> [資格情報プロバイダ]

Windows サインインに関する設定で、Windows 標準の Credential Provider（クレデンシャルプロバイダー）から SecureDoc Credential Provider（資格情報プロバイダ）に変更します。シングルサインオン(SSO)に設定変更するには SecureDoc Credential Provider（資格情報プロバイダ）が必要です。

項　目	説　明
資格情報プロバイダ	
☐ ブートログイン資格情報を使って Windows に自動的にログインする	プリブート認証での資格情報を使用して Windows に自動的にサインインします。
☐ Windows ユーザーはスマートカードやトークンを使ってシングルサインオン可能	スマートカードまたはトークンを使用することで、シングルサインオンを利用できます。
☐ Windows への自動ログインのタイムアウトまでの時間 X 分	Windows への自動サインインは X 分後にタイムアウトします。
Windows ログイン時に SecureDoc 資格情報を使って認証方法を定義します	
☐ ブートログイン資格情報を使って Windows に自動的にログインする	プリブート認証での資格情報を使用して Windows に自動的にサインインします。
☐ トークンが抜かれたときにコンピュータをロックする	USB トークンを抜くと、Windows をロックします。

項　目	説　明
☐ スマートフォンの保護されたキーファイル（Bluetooth 経由）を使用して Windows にログインする。	スマートフォンに Authenticator をインストールする必要があります。
☐ SecureDoc クレデンシャルを持っているユーザーのみ、Windows ログオンとその他の構成済みサービスにログインできます	SecureDoc Credential Provider でのみ、Windows およびその他の構成済みサービスにサインインできます。 SecureDoc のユーザーである必要があり、Windows 標準のクレデンシャルプロバイダーは利用できません。
☐ ホームネットワークでのネイティブの Windows ログオンにト切り替える（SES サーバーが到達可能）	SDConnex と通信可能なネットワーク環境では、Windows 標準のクレデンシャルプロバイダーに切り替えます
多要素認証	
☐ Windows のログインで多要素認証を必須にする	Windows サインインに多要素認証を適用します。
☐ SecureDoc で保護されたデバイスにリモートデスクトップ接続するときに、多要素認証を利用する	SecureDoc で保護されたデバイスへのリモート デスクトップ接続に多要素認証を適用します。
☐ SecureDoc のクレデンシャルプロバイダー（オートログオン）拡張機能を Windows リモートデスクトップクライアントに追加します	リモート デスクトップクライアントに SecureDoc ログインの拡張機能を追加します。

[オプション] -> [メディア暗号化]

メディア暗号の方法には、「メディア全体」と「コンテナベース（RMCE）」があります。
用途や目的によって、暗号化の方法を選択します。

「メディア全体」：

復号化するためには、SecureDoc がインストールされている必要があります。
ユーザーのキーファイルに、暗号化に使われた鍵が含まれている場合、シームレスにアクセスできます。
鍵を所有していない場合、パスワードで保護されているメディアの場合は、パスワードによって復号化できます。
鍵を所有しておらず、パスワードも設定されていないメディアの場合は、SecureDoc がインストールされているデバイスでも復号化することはできません。

「コンテナ暗号」：

SecureDoc がインストールされており、ユーザーのキーファイルに、暗号化に使われた鍵が含まれている場合、シームレスにアクセスできます。鍵を所有していない場合、パスワードで保護されているメディアの場合は、パスワードによって復号化できます。
SecureDoc がインストールされていないデバイスでも、パスワードによって復号化できます。パスワードが設定されていない場合、復号化することはできません。

項　目	説　明
リムーバブルメディア暗号 　自動または手動暗号化	

項　目		説　明
☐ 接続時にリムーバブルメディアを自動的に暗号化する		リムーバブルメディアが接続されると自動的に暗号化を開始します。
☐ 手動によるリムーバブルメディア暗号を許可する（コンテキストメニューから）		コンテキストメニューを使用してメディアを暗号化します。
暗号化方法	○ メディア暗号	セクタレベルでメディアを暗号化します。 注　ユーザー間でメディアを共有する場合、条件があります。 ・メディアは共有鍵で暗号化されている、あるいはパスワードで保護されていること。 ・デバイスには SecureDoc がインストールされていること
	○ 接続直後に暗号化開始	接続されると、すぐに暗号化を開始します。
	○ X 秒後に暗号化を開始	接続された後、X 秒後に暗号化を開始します。
	○ すべてのセクターを暗号化する	すべてのセクターを暗号化します。
	○ 使用しているデータセクターのみ暗号化する	使用しているセクターのみ暗号化します。
	○ コンテナベース（RMCE）	コンテナベースの暗号化をおこないます。 注　ユーザー間でメディアを共有する場合、条件があります。 ・メディアは共有鍵で暗号化されている、あるいはパスワードで保護されていること。
	○ 使用する空き容量　X%	コンテナ暗号化の領域を指定します。
	○ スペース全体を暗号化し、ファイルをコンテナに移動する	全体をコンテナの領域として暗号化します。 暗号化前にデータを退避し、暗号化後、データを暗号化されたメディアに戻します。
	☐ リムーバブルドライブを安全にフォーマット化...	コンテナ暗号化を開始する前にメディアを初期化します。
メディア暗号で使用する暗号鍵		メディア暗号に使用する鍵を指定します
☐ デフォルトのメディア暗号化設定の変更を許可する		メディア暗号の設定内容の変更を許可します。
☐ メディア暗号化のため、デバイスキーの使用を禁止します		ユーザーがメディア暗号に使用する鍵を、ディスクの暗号化に使用した鍵以外にさせます。
☐ 暗号化されたリムーバブル（RME 監視ログ）への操作/ログ記録の操作		メディアのログを残します。
☐ ログ内のファイル名を暗号化する		ログ内のファイル名を難読化します。
☐ 外部 SED にブートログオンをインストールする		デバイスに内蔵していない外部接続の SED にブートログオンプログラムをインストールします。
☐ CD/DVD のコンテナ暗号を有効にする		コンテナ暗号で、CD/DVD を暗号化できるようにします。

[オプション] -> [詳細オプション]

項　目	説　明
全般	
☐ ユーザーのパスワードおよびセルフヘルプパスワードのリカバリの質問を SES に送信できるようにする	ユーザーのパスワードとセルフヘルプの回答を SDConnex を介して SES DB に送ります。 セルフヘルプリカバリーは日本語環境ではご利用いただけません。
☐ トークンの証明書から取得した情報をダイアログに表示する	トークン証明書のユーザー/日付情報がダイアログ/リストに表示され、本人確認を容易にします。
☐ システムトレイに SecureDoc アイコンを表示せず、通知も停止する	システムトレイに SecureDoc のアイコンを表示させません。 通知も抑止し表示させません。
☐ ユーザー認証の答えを管理者への補助として SES コンソール中にテキストで表示	管理者の補助として、SES コンソールにユーザーのセルフヘルプの回答を表示させます。 日本語環境ではご利用いただけません。
☐ Cryptoerase を有効にする（現地の SD 管理者はこのコンピュータのディスク…	Crypto Erase を有効にします。
☐ システムがスリープモードから再開する際に、自己暗号ドライブ（例: OPAL TCG …）をロック解除する	自己暗号化ドライブ（TCG Opal）で、スリープモードを利用できるようにします。 注　スリープモードの使用は推奨されません。

項　目	説　明
☐ システムがハイブリッドスリープ状態から再開する際に、自己暗号ドライブをロック解除する	自己暗号化ドライブ（TCG Opal）で、ハイブリッドスリープモードを利用できるようにします。
☐ Intel Enterprise Digital Fence が有効な場合、デバイスのスリープ状態を許可する	Intel Enterprise Digital Fence をサポートします。 Intel Enterprise Digital Fence では、デバイスが信頼できる LAN でウェイクアップすると、スリープが再開されます。しかし、帰宅途中の車内など信頼できる LAN がない場合、休止状態が強制されます。
Windows アカウント	
ブートキーファイルオプション：	
☐ ローカルユーザーのブートキーファイルを作成する	デバイス上で検出されたローカルユーザー向けに、ブートキーファイルを作成します。
☐ AD ユーザー用ブートキーファイルの作成	デバイス上で検出された AD ユーザー向けに、ブートキーファイルを作成します。
☐ 各 Windows ユーザーのパーソナル暗号鍵を作成する	個人キーファイルに自動でログインします。 注　プリブート認証を利用するユーザーでは使用しません。 主に「Only encrypt Removable Media（RME）」向けです。
以下の Windows アカウントを除く：	ここで指定したアカウントは作成しません、
☐ AD ユーザーのみアカウントを作成する	SecueDoc のアカウント作成を AD ユーザーに限定します。