PBConnex

業界初のプリブート・ネットワーキングによるディスク暗号のセキュリティ向上と運用コスト削減

WINMAGIC®
DATA SECURITY

注意

本書の内容は予告なく変更される場合があります。本書に含まれる情報は、本書の発行時の WinMagic Inc.の見解を示すものです。WinMagic Inc.は本書発行時以降に存在するいかなる情報についても保証することはできません。
本書は情報提供のみを目的とするもので、本書の情報に関して明示、暗示にかかわらず、WinMagic Inc.が保証するものではありません。本書に記載されている SecureDoc の機能は、予告なく変更される場合があります。

WinMagic：日本国内の連絡先

ウインマジック・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
Tel：03-5403-6952
Fax：03-5403-6953
Mail：sales.jp@winmagic.com
URL: http://www.winmagic.com/jp

目次

見直しを迫られている PC の情報漏えい対策

2005 年に施行された「個人情報の保護に関する法律」（個人情報保護法）を機に、主に大企業を中心にクライアント PC — 特にノート PC の情報漏えい対策は急速に普及しました。中でもディスク暗号（ソフト、ハード含む）は、2005 年以来、爆発的な普及し、今や持ち出し PC の情報漏えい対策としてデファクトスタンダードと言っても過言ではないほど広く利用されています。

しかし、個人情報保護法の施行前後にクライアント PC の保護やコストばかりを重視して、運用性や管理性を顧みずに導入した結果、現在でもディスク暗号が PC の選定のボトルネックになっている、あるいは高い運用コストを支払っている企業も少なくありません。

一方で、ディスク暗号の仕様そのものが現行の PC の運用と相容れないため、ディスク暗号が導入できず、ノート PC の持ち出し許可に踏み切れないという企業も少なからず存在します。そういった企業では、ノート PC による業務の効率化を図ることができず、業種によっては顧客のニーズに応えることができず、新たな経営リスクにさらされています。

本書は、現在ディスク暗号を利用している企業を対象に、新世代のディスク暗号技術が従来のディスク暗号の課題をどのように解決するのかを解説するとともに、これから導入しようとしている企業がディスク暗号を検討するに当たり、どのようなことを考慮すべきかを説明します。

ディスク暗号：
ハードディスクや SSD をセクターレベルで暗号化する技術。そのドライブ上のすべてのデータが暗号化される。このホワイトペーパーでは、ハードディスク、SSD の暗号化も含めて「ディスク暗号」と呼ぶ。

セキュリティ対策の検討方法

PC の盗難・紛失対策を検討するとき、どのようにデータを守るかが重視されがちですが、実際に盗難・紛失が発生した際に企業としてどのような行動を取るかを検討することも重要です。

昨今、企業はその業種や取り扱うデータにより、情報漏えいが確認されていなくても PC や媒体が紛失した時点で、監督官庁や取引先への報告、あるいは Web サイトでの報告を行うことがあります。そのような報告の中で企業は、「紛失した PC 内のデータはセキュリティ対策がなされているのか？」、「どのような対策がされているのか？」「今 PC 内のデータは安全な状態にあるのか？」という厳しい問いへの説明が求められます。

紛失した PC は「パスワードがかけられていた」とだけ説明するのと、「全体が暗号化され、パスワードがなければ使用できないようになっていた。そして現在はもう使用できない状態になっている」と説明するのでは、その組織の信用に与える影響が大きく異なります。

つまり、情報漏えい対策は、データを安全に守る対策であるのと同時に、情報漏えいの可能性が発生した場合に取引先、顧客、社内に対して説明ができる対策である必要があります。

このことを考慮して、情報へのアクセスポイントをすべて保護できるもっとも優れたソリューションの導入を模索している企業は、以下の点を慎重に検討する必要があります。

デバイスのオペレーティング・システム（OS）を問わず、そのソリューションはネットワークに接続する多種多様なデバイスの全体を暗号化できるか？

IT 管理部門がそのソリューションを一元管理できるか？

USB メモリ、SD カードなどのリムーバブルメディアを暗号化できるか？ 暗号化されていないリムーバブルメディアへのアクセスを制限できるか？

エンドポイントあるいはサーバー上の機密データのファイルやフォルダを、複数のセキュリティ・レイヤーで保護可能か？

デバイスにポリシーを適用して、ユーザーが必要とする情報のみに限定した適切なアクセス権を付与することができるか？

プリブート認証機能を使用したセキュリティ・レイヤーを追加することができるか?

IT によるセキュリティ・システムの管理が容易であり、またパスワードの回復や OS 障害時の対策などエンドユーザを効果的にサポートする手段が備わっているか?

遠隔からの PC の起動不能化や PC が起動できる場所、期間を限定することで、所在が分からない PC へのアクセスをパスワード以外の方法で拒否できるか?

デバイスが暗号化されていることが証拠として残り、許可されていない使用者による暗号の解除やセキュリティポリシーの変更を禁止できるシステムか?

社会の変化により企業に求められるセキュリティのニーズも変わります。ここで挙げたリストは、現在のセキュリティ対策の傾向の中で求められるニーズです。先に挙げたリストは限定的なものですが、そのすべてが非常に重要であり、ディスク暗号技術でなければ満たせない仕様がいくつかあります。これこそ昨今ディスク暗号化(FDE-Full Disk Encryption)がデファクトスタンダード化しつつある最大の理由です。

しかし、すべてのディスク暗号化製品がこれらの仕様を満たすわけではありません。既に PC を暗号化している企業は、導入当時においてはそれが最良の手段・運用方法だったかもしれませんが、今日のインフラ、セキュリティのニーズ、PC の使い方に適しているかどうかを再検討する必要があります。ディスクの暗号化が PC の管理業務にもたらす影響を検証することなく導入したために、導入後にこれまでの PC の管理方法を維持することができなくなり、全組織的な PC の運用コストが跳ね上がるという事例は後を絶ちません。

これからクライアント PC のセキュリティ対策を導入する企業は、導入時のコストだけでなく、中長期的な運用コストも視野に入れて検討する必要があると言えます。

ディスク暗号の落とし穴

一般的に PC のディスク暗号は、「使用者が暗号を意識することなく利用することができる」という特徴があります。ユーザーは認証以外の操作をすることなく、暗号化された PC を使うことができるというメリットです。この特徴は、使い勝手の観点だけでなく、セキュリティの面でも非常に重要です。ユーザーが暗号を意識しないということは、すべてのデータが自動的にバックグラウンドで暗号化されることを意味するからです。多くのディスク暗号化製品は、この点を最大のメリットとしてプロモーションされています。

しかし、この"User Experience (ユーザエクスペリエンス)"が広く知られている一方で、管理者側における"Administrator Experience (アドミニストレーター・エクスペリエンス)" について語られることはほとんどありません。企業はそれぞれの環境や PC の利用方法に応じた PC のメンテナンス方法(パスワードリカバリー、OS のクラッシュ、ハードウェア障害、ソフトウェアのインストール、アップデート等への対応方法)を確立しています。最も重要なことは、ディスク暗号を導入すると、そのほとんどが今まで通りには実行できなくなるということです。

具体的な説明をする前に、ここでディスク暗号技術の一般的な特徴を確認しましょう。ハードディスク暗号化ソフトウェアは、ハードディスク全体をセクターレベルで暗号化し、Windows が起動する前にプリブート認証と呼ばれるログイン画面を表示させるという共通の機能を持っています。PC の電源を投入すると、直後にプリブート認証画面が表示され、正しく認証を行わなければ Windows が起動しないという仕組みです。

複数のレイヤーでの保護:
ここで言う複数のレイヤーとは、セクターレベルで行われるディスク全体の暗号と、OS 上で行われるファイル・フォルダの暗号を指す。盗難された PC の起動を防ぐにはプリブート認証を伴うディスク暗号は最適だが、OS が起動した後のネットワークからの不正アクセスに対しては、OS 上でデータを個別に暗号化する方法が有効である。このように、セキュリティに対する脅威が多様である以上、それぞれのレイヤーでのデータ保護を検討する必要がある。

プリブート:
Windows が起動する前の PC の状態のことをプリブートという。通常、ディスク暗号化製品は、このプリブートの時点でユーザー認証を要求し、正規のユーザーのみが Windows を起動できる(つまり PC を利用できる)ようにする仕組みを持っている。この機能は「プリブート認証」と呼ばれる。

プリブートの状態では、Windows は暗号化されているため、ネットワークインターフェース等の周辺機器は利用できない。パスワード認証が基本だが、SecureDoc では指紋、トークン、IC カード等の二要素認証、プリブート認証を省略するオートブート機能が備わっている。

プリブート認証には以下の重要な特徴があります。

- ユーザーID とパスワードはローカルに保存されていて、常にローカル認証が行われること
- OS が起動していないので、OS にインストールされているドライバが使えないこと（つまり、ネットワークカードや無線 LAN 等の周辺機器が利用できないこと）
- ユーザーのパスワードを知らない管理者が起動するには、チャレンジ・レスポンスと呼ばれるワンタイムパスワードを管理サーバーから発行して起動するか、マスターパスワードを事前にローカルに保存しておく必要があること

では、これらの特徴が、PC のメンテナンスに影響を与える具体的な例を挙げましょう。

管理者が PC のメンテナンスを行う度にパスワードリカバリーの実行が必要になる

例えば管理者自らが、ユーザーの PC を起動し、PC のメンテナンスをする機会が多い企業を想定します。ディスク暗号をしていない場合、Active Directory などのサービスが導入されていれば、管理者は Windows ログイン画面で自分の ID とパスワードを使って、管理者としてログインすることができます。

では、ここで PC のディスクが暗号化され、プリブート認証がインストールされていることを想像してみてください。暗号化の導入前は、管理者は Active Directory（もしくはその他のディレクトリサーバー）に登録されている自分の ID/パスワードさえ知っていれば、その PC のメンテナンスを行うことができました。ところが、今は目の前にプリブート認証画面が表示されています。その場に PC の使用者がいなければ、管理者はディスク暗号ソフトの管理サーバーにアクセスし、チャレンジ・レスポンス等によって PC を臨時起動しなければなりません。一台につき 2 回起動をする作業を 100 台で行うには、チャレンジ・レスポンスを 200 回実行することになります。

この問題は、ローカルにのみ ID とパスワードが保存されていること、さらにプリブートの状態ではクライアント PC はネットワークにアクセスできないというディスク暗号技術のデメリットによるものです。

この課題はマスターパスワードによって解決するかのように思われます。しかし、全ての PC にアクセスできるパスワードを知っている管理者が退職した時のことを考えると、セキュリティ対策ソフトの運用方法としては現実的ではありません。一般使用者がマスターパスワードを知るリスクもあります。また、**「マスターパスワードを使っているという事実」**が外部に知られただけでも（ソーシャルネットワークなどを通じて）、その組織の信用を下げることになります。

課題 1. ディスク暗号はローカル認証しかできないため、PC のメンテナンス時に管理者が PC を起動させる度にパスワードリカバリーを実行する必要が生じる。その結果、メンテナンスコストが大幅に増える。

事業継続性を妨げるプリブート認証

チャレンジ・レスポンス：
ディスク暗号化ソフトウェアで一般的に使われるパスワードリカバリーの方法。使用者がパスワードを忘れた場合、プリブート認証の画面で「チャレンジ値」と呼ばれるランダム値を表示させ、管理者に伝える。管理者は管理サーバーで「チャレンジ値」を入力すると「レスポンス値」と呼ばれる値が表示される。レスポンス値を使用者に伝え、プリブート認証の画面で入力すると、Windows が起動するという仕組み。チャレンジ値は起動の度に変わるため、レスポンス値も毎回異なる。一種のワンタイムパスワード。プリブートの時点でネットワークへのアクセスができないため、電話等を使って口頭でそれぞれの値を伝える必要がある。

マスターパスワードのリスク：
組織全体、あるいは部門全体の PC にマスターパスワードが保存されていると、いずれ「マスターパスワードを使っている事実」が従業員に知られるリスクがある。一度、知られてしまうと、ソーシャルメディア、懇親会の席等の様々な経路でその事実が外部に漏れる可能性が生じる。また、情報システム部門の従業員が退職すれば、その事実は外部にもれることになってしまう（仮にマスターパスワードを変更したとしても）。

PC の盗難や紛失が発生した場合に、強固なセキュリティ対策を採用していることをどれだけ説明しても、マスターパスワードが使われていることを指摘されてしまうと、「信用の低下を最小限に留める」というセキュリティ対策の目的のひとつが果たせなくなる。

近年、突然の災害、停電、疫病、交通機関のマヒ等が発生した場合の事業継続マネジメントが注目されています。リスク発生時に、企業や組織の業務の停止を最小限に留め、事業を継続させるためのソリューションが様々なシステムインテグレーター、IT 機器メーカーより提案されています。遠隔からの PC 起動や、起動している PC に遠隔からログインするシステムがその例として挙げられます。このようなシステムを使えば、ユーザーがオフィスに出社できない場合でも遠隔地から業務を継続させることができるようになります。

では、遠隔から起動しようとする PC にディスク暗号化ソフトウェアがインストールされているとどうなるでしょうか？やはり、ここでもプリブート認証は Windows が自動的に起動するのを防ぎます。つまり、遠隔からPCを起動させようとしてもディスク暗号化製品の機能により、遠隔操作の目的であった遠隔からの業務の継続が実現しなくなってしまいます。

オフィスに管理者が残っていたとしても、当然プリブート認証は表示されます。管理者はパスワードリカバリーを行わなければPCを起動できません。組織が大きければ大きいほど、起動しなければならない PC は増えます。これでは自宅にいるユーザーは PC にアクセスする準備ができていても、自分の PC が起動されるまで待機しなければならないという状態が続きます。

SecureDoc のように「オートブート」機能が備えているディスク暗号化製品があります。オートブートはプリブート認証を省略して、ユーザー認証を行うことなく Windows を起動させる機能です。ここで重要なのが、オートブート機能はクライアント PC への設定によって有効になり、予め設定しておく必要であるという点です。事業継続を問われる事態の多くは突発的に起こることを考えると、オートブートはこの問題の解決策にはなりそうにありません。

この問題は、OS が起動していないプリブート認証の状態では PC はネットワークにアクセスできず、ディスク暗号製品の設定変更できないというディスク暗号化ソフトウェアの特徴によるものです。

課題 2.遠隔操作により PC を起動させるシステムを利用していても、ディスク暗号化製品のプリブート認証により OS の起動が妨げられてしまう。この問題は、組織の事業継続性の重大なボトルネックになる。

オートブート:
一部のディスク暗号化ソフトウェアが備える機能で、プリブート認証を省略させる。SecureDoc の場合、①恒久的なオートブート、②特定の日時から、特定の起動回数、あるいは時間帯のみ有効になるオートブート、の 2 種類の機能を持つ。②の機能は、予定が決まっている PC のメンテナンスに有効だが、事前にオートブートのポリシーを、クライアントに配信しておく必要がある。恒久的なオートブートは、ディスク暗号のセキュリティ効果を下げる可能性があり、推奨されない。

ローカル認証であるが故のプリブート認証の管理の難しさ

Active Directory 等のディレクトリサービスを利用して、定期的に管理者が決めたパスワードをユーザーにプッシュしたり、パスワードを強制的にリセットしたりする組織が時々見受けられます。このような運用では、管理者はディレクトリサーバーにあるユーザーのプロファイル情報を変更するだけで、ユーザーのパスワード管理ができます。それでは、このパスワード運用をディスク暗号のプリブート認証にも適用することができるのでしょうか？

前述の通り、ディスク暗号のプリブート認証の ID とパスワードは常にローカルに保存されます。これはユーザーのパスワードを変更するには、クライアント上のパスワードを変更しなければならないということを意味します。ディスク暗号化ソフトウェアに管理サーバーから新しいパスワードを配信する機能があっても、クライアント PC が起動して新しいパスワードを受信するまで有効にならない、という点に留意する必要があります。PC のプリブート領域に保存されているパスワードは管理者が設定した最新のパスワードではない可能性が生じるということです。

プリブート領域:
一般的なディスク暗号化ソフトウェアはプリブート認証を実現するために、ドライブ上にプリブート領域という独自の領域を作成し、そこにユーザーの認証情報や鍵の情報を保存する。プリブート領域が壊れると、その PC はアクセス不可能になるため、製品によってはこの領域をバックアップする機能が搭載されている。また、SecureDoc のように、この領域を遠隔から破壊することで、盗難にあった PC が起動不能にできる製品もある。

これはパスワードだけでなく、ユーザーID そのものや、ユーザーの権限にも言えます。例えば、ある従業員が退職した場合、Active Directory ではそのユーザーを停止、あるいは削除した時点でその従業員は Active Directory にログインできなくなります。しかし、プリブートでは、PC がディスク暗号の管理サーバーに接続するまで、場合によっては管理者自身がその PC の設定を変更するまでは、その従業員のログインは許可されてしまいます。

この課題は、課題 1、課題 2 と同様に「ローカル認証しかできない」というディスク暗号の特性に起因します。このように Active Directory 認証とプリブート認証には本質的な違いがあり、それぞれ異なる運用を強いられることになります。

ディスク暗号化製品によっては、Active Directory と管理サーバーを同期させて、パスワードを統一できる製品があります。しかし、それでも「ローカル認証」であることには変わりなく、クライアント PC とディスク暗号の管理サーバーが通信をするまでプリブート認証のパスワードは変更されないという課題は残ります。

課題 3. プリブート認証はローカル認証であり、パスワード変更にはクライアント内のパスワードを変更する必要がある。これは Active Directory 等のディレクトリサービスの認証とプリブート認証の大きな違いで、二重のパスワード運用を強いられる。

プリブート認証が PC とユーザーを強力に紐付けてしまう

病院で使われる PC を想像してみてください。病院のような 24 時間人が働く場所では、従業員全員に PC が 1 台ずつ配布されているケースは珍しく、1 台の PC に複数のユーザーがログインして利用することが一般的です。こういう組織では、複数のユーザーが利用できるという利便性を保ちながら、如何に PC 内のデータを保護できるかという点が、セキュリティを考慮する上で重要なポイントになります。

例えば 200 人の従業員が、100 台の PC を利用するという環境を想定します。この 200 人の従業員は、100 台の内の不特定の PC を毎日利用します。Active Directory のようなディレクトリサービスにログインするだけなら、運用上の支障は生じません。従業員は、Active Directory の ID とパスワードさえ知っていれば、どの PC でも許可された権限でログインすることができます。

では、この病院にディスク暗号を導入すると何が起きるでしょうか？先ず利用者はプリブート認証と OS へのログイン認証という 2 つのパスワードを覚えることになります。そして、各 PC のプリブート認証には 200 人の ID とパスワードを保存する必要があります。

前述の通り、共通パスワードは「共通パスワードを使っているという事実」が外部に漏れると、信用の低下、特に病院のような個人情報を取り扱う組織ではリスク管理に対する批判を招くことになります。

この病院は従業員の入社、退職、異動の度に、100 台の PC のユーザー情報を変更することになります。Active Directory だけなら Active Directory 内のユーザー情報を変更するだけですが、ディスク暗号のプリブート領域のユーザー情報はそうはいきません。プリブートのユーザー情報はローカルに保存されているので、各 PC 内の情報を更新する必要があります。

PC と従業員数が少ない組織であれば、管理者が手作業で管理をすることもできますが、大きな組織や部門が細かく枝分かれする組織は、ローカル認証では限界があります。特に病院は扱う個人情報が機密性を要するものなので、ひとつの運用のミスが被害者と病院の双方に重大な結果をもたらしかねません。このように共通 PC が多い環境においては、ディスク暗号の導入は PC の運用コストと管理ミスのリスクを大幅に増やすことになります。

課題 4. ディスク暗号はローカル認証を行うため、病院のように共通 PC を多く使う組織では、人事異動がある度に各 PC 内のユーザー情報の変更をすることになる。ディレクトリサービスを前提に PC を運用している組織では、ディスク暗号の導入により、これまでの PC 運用や管理体制の継続が困難になる。

OS がクラッシュすると業務が 1 日止まってしまう

大規模で PC を運用している組織にとっては、OS のクラッシュ（論理的故障）は、一般的で重大な障害と言えるでしょう。扱うデータの内容、オフィスの環境（拠点が多い等）、利用している PC の種類等により、様々な対策が取られています。どのような対策が取られていても、もし OS がクラッシュすると、データが永久に失われてしまう、あるいはデータが再び利用できるようになるまで 1 日要するということになれば、それは PC、およびデータを管理する上で重大な懸念になるでしょう。

PC のディスクを暗号化すると、その懸念が現実になります。ディスク暗号の前と後の違いに、「OS の修復ができなくなる」「システムドライブのリカバリーができなくなる」という点があります。一度、ディスクを暗号化すると、外部のツール（Windows の回復ツールやイメージリカバリーツール）はディスク上のデータだけでなく、パーティションテーブルやファイルシステムまで見えなくなります。これは特定の領域やドライブだけの修復ができなくなることを意味し、Windows のインストールメディアやリカバリーツールは、ディスク全体をフォーマットしようとします。実際にフォーマットすると、暗号化されたデータを元に戻すことはできなくなります。

この問題に対する一般的なディスク暗号化ソフトウェアのアプローチは、先ず OS がクラッシュしたディスク全体を復号化した上で、従来の方法により Windows の修復やイメージリカバリを行うというものです。しかし、この方法はディスクの復号に数時間、PC の環境によって 10 時間以上かかることを考えると、ユーザーや管理者にとって好ましいものではありません。

このように、ディスク暗号を導入すると、これまでの PC のメンテナンスプロセスの変更を余儀なくされます。PC 内のデータが一日使えないということは、その PC の利用者の業務が 1 日止まることを意味します。ディスク暗号を導入しようとしている組織は、このリスクを十分認識し、OS のクラッシュや PC の故障といった突発的な事態が発生した時に、最短でデータを退避できるプロセスを確立しておく必要があります。

課題 5. 暗号化されたディスク上の OS が論理的に壊れた場合、従来の OS の修復や C ドライブだけのリカバリーによる復旧ができなくなる。ディスク全体の復号化が必要になり、ディスクの容量により一日データが利用できなくなることもある。

暗号化されたディスクの状態：
ソフトウェアによるディスクの暗号化は、「I/O レベルでの暗号化」とも呼ばれ、ファイルシステムも含め暗号化を行う。Windows 修復ツール、イメージングソフト、データ復旧ツール等のソフトウェアは、暗号化されたハードディスク内のパーティションの情報も読み取ることができなくなる。そのため、例えば D ドライブ内のデータは残し、C ドライブだけイメージをリカバリーする、といったことができなくなる。

ディスクの復号に要する時間：
ディスクの復号化にかかる時間は、ディスクの容量、CPU、その PC のアプリケーションの稼働状況に大きく影響するが、特にディスク容量が決定的な要因になる。SecureDoc には、「使用領域のみ暗号化/復号化する」という暗号化方法があり、暗号/復号に要する時間を大幅に削減することができる。

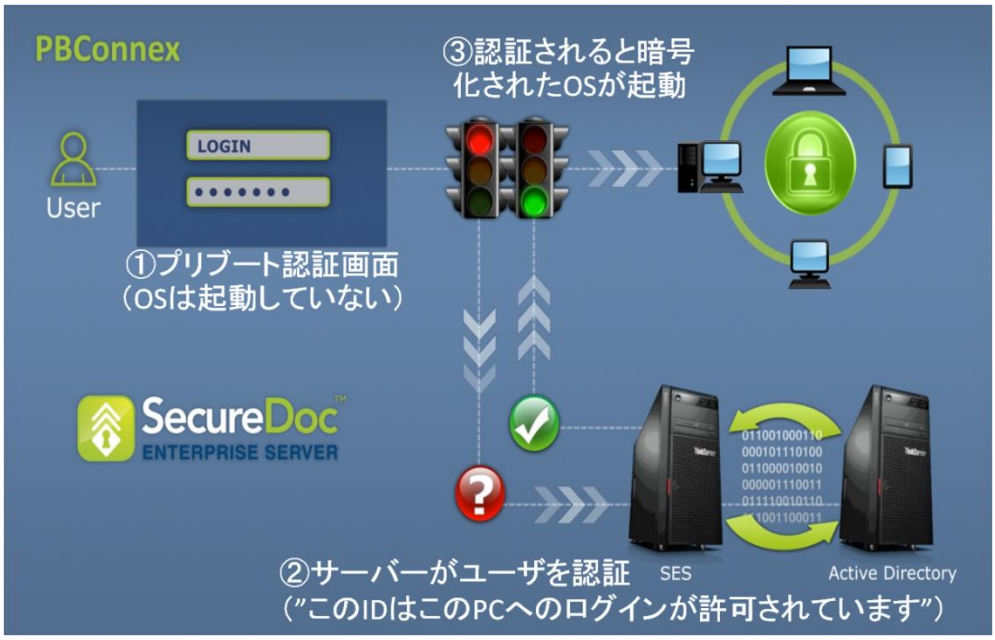
これらの課題を解決する PBConnex とは？

WinMagic が提供する SecureDoc には、これらの課題を解決する PBConnex（ピービーコネックス）という機能があります。この PBConnex がこれらの課題をどのように解決するのか具体的に説明する前に、先ず PBConnex とはどのような機能なのか説明します。

PBConnex は「プリブート・ネットワーキング（PBN）」という技術を利用した機能です。PBN とはどのようなものでしょうか？ プリブート・ネットワーキングでは、暗号化された PC の OS が起動する前に PC がネットワークに接続し、SecureDoc Enterprise Server(SES)によりログインを許可することができます。簡潔にいえば、プリブートの段階でユーザーはまず認証情報（パスワード）を入力してネットワークに接続された SES に認証される必要があり、SES により PC へのログオンが許可された後に OS が起動するというものです。

プリブートの状態とは OS が起動する前（OS も暗号化されている状態）なので、当然 OS にインストールされている PC のハードウェアのドライバを利用することはできません。つまり、本来はプリブートでは PC のネットワークインターフェースを利用することはできないのです。WinMagic の PBConnex がユニークな点は、このプリブートの状態でも PC がネットワークインターフェースを利用でき、さらに無線 LAN も利用できるということです。これは、WinMagic のプリブート認証の開発技術の結果によるものです。

では、なぜこの技術が重要なのでしょうか？PBConnex ではユーザー認証を SES で行います。ある PC にログインしようとしているユーザーの情報はローカルに保存されている必要はありません。SES で許可されていれば、PC にログインできるのです。これはまさに Active Directory 等のユーザー認証と同じ概念であり、「ローカル認証」という従来のディスク暗号の制約がなくなることを意味します。今まで、SES や管理者自身の手によってクライアント PC 上で変更しなければならなかったプリブートのユーザー情報が、SES だけで、さらには Active Directory だけで変更できるようなったのです。



PBConnex のイメージ。SES（管理サーバー）には、ID と PC の関係がデータベースとして登録されている。管理者はサーバーを操作するだけで、あるID がどの PC にログインできるのか、あるいはできないのかを決めることができる。

プリブート領域の品質：
ディスク暗号化ソフトウェアは、コンセプト自体はどの製品も共通する部分が多いが、「プリブート状態でできること」は製品によって大きく異なる。言い換えれば、OS が稼働していない状態で、どれだけの機能を実装しているか、どれだけの周辺機器を認識できるか、は製品を選定する上で重要な要素になる。

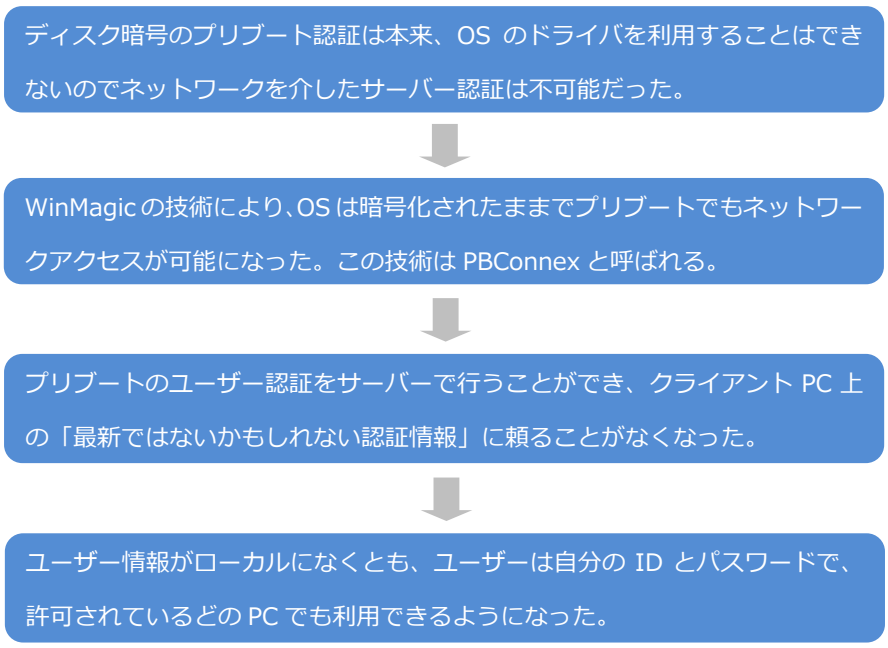
このプリブートの機能の違いにより、プリブートでの指紋認証、トークン認証、ネットワーク認証、オートブート、ユーザーロック等の機能の有無が生じる。また、例えばトークンや指紋認証装置のバージョンが変わると、プリブートで利用できなくなるのも、この OS 上のドライバを利用せずに独自で周辺機器を認識するというプリブート領域の仕様に起因する。

SecureDoc Enterprise Server（SES）：
SecureDoc クライアントのポリシー、PC 情報、鍵情報、ユーザー情報を一元管理するサーバー。すべての情報はデータベースに保存される。Windows、Mac OS、iOS、Android、デスクトップ PC、ノート PC、タブレット PC、ハードディスク、SSD、自己暗号ドライブといった様々な環境の暗号化、アクセス管理をひとつのコンソールで管理する。

PBConnex を使ったログイン：
「PBConnex を使ったログイン」では、プリブートの状態で SecureDoc の管理サーバーである SES にアクセスし、SES により許可されていれば PC にログインできる。つまり、PBConnex を使ったログインをするには、プリブートの状態で SES にアクセスできる環境にある必要がある。プリブート認証は、シャットダウン状態からの起動時、PC の再起動時、および休止状態からの復帰時に要求される。Windows が起動した後は、SES に常時接続している必要はない。

さらに PBConnex には、ユーザーや PC をグループとして管理することで、どのユーザーID がどの PC にログインできるのか、細かく指定することができます。例えば営業部のマネージャーは部下である営業部の社員の PC へのログインは許可され、経理部門の PC へのログインは許可されないものとします。さらに、営業部の一般社員は自身の PC へのログインだけが許可されるとします。ローカル認証では、このような複雑な認証ポリシーは現実的ではありません。しかし、PBConnex を使えば、管理サーバーを操作するだけで、動的に複雑な人と PC の関係を管理できるようになります。

分かりやすいように、以上のことを次のチャートにまとめます。



PBConnex による具体的な解決方法

それでは、それぞれの課題を PBConnex がどのように解決するか検証してみましょう。

課題 1. ディスク暗号はローカル認証しかできないため、PC のメンテナンス時に管理者が PC を起動させる度にパスワードリカバリーを実行する必要が生じる。その結果、メンテナンスコストが大幅に増える。

課題 1.は、管理者が各 PC のメンテナンスを行おうとすると、起動の度にプリブート認証画面が表示され、ここでログインをしないと OS が起動できないというディスク暗号の特徴によるものでした。

PBConnex を使えば、この課題は管理者が SES を数分操作するだけで解決されます。管理者は SES でメンテナンス対象である PC（のグループ）に対して自分の ID のログインを許可するだけです。または、**「PBConnex を使ったオートブート」**を許可することで、パスワードの入力も省略することができます。この設定は管理者が SES でオートブートの許可を解除するまで続きます。

PBConnex を使ったオートブート（AutoBoot via PBConnex）:
PBConnex の機能のひとつ。プリブートで、SES にアクセスできる環境であれば、つまり組織の LAN に接続できる環境であれば、ID とパスワードを入力することなく、PC を起動させる機能。オートブートの許可、禁止はサーバーで設定するだけなので、クライアントの設定変更をすることなく、動的に実行することが

課題 2.遠隔操作により PC を起動させるシステムを利用していても、ディスク暗号化製品のプリブート認証により OS の起動が妨げられてしまう。この問題は、組織の事業継続性の重大なボトルネックになる。

課題 2.は前述の PBConnex を使ったオートブート（右コラムの解説を参照）で解決されます。日常的には、PBConnex を使ったオートブートを使っていない組織でも、SES の設定を変更するだけで、LAN に接続している PC のプリブート認証を省略することができるようになります。SES では複数の PC をグループ化できるので、一度の設定ですべての PC にオートブートを許可することもできます。このように突然従業員がオフィスに出勤できなくなった場合でも、リモートから SecureDoc のサーバーを操作することさえできれば、オフィスに残されたクライアント PC を遠隔から起動させることができるようになります。

リモートからの SES の操作：
SES の情報はすべてデータベースに保存され、コンソールはこのデータベースにアクセスするための「窓」の役割を持つ。そのため、コンソールはデータベースサーバにインストールする必要はなく、管理者のノート PC にインストールして運用することができる。VPN 等により、データベースにアクセスできれば、管理者はリモートからコンソールを通じて SES（のデータベース）の操作を行うことができる。

課題 3. プリブート認証はローカル認証であり、パスワード変更にはクライアント内のパスワードを変更する必要がある。これは Active Directory 等のディレクトリサービスの認証とプリブート認証の大きな違いで、二重のパスワード運用を強いられる。

課題 3.は PBConnex の機能と、SES が持つ Active Directory との同期機能を利用することで解決されます。これらの機能には、パスワード変更が簡単になるだけでなく、Active Directory とプリブートのパスワードが動的に統合されるというメリットがあります。

SES を Active Directory と同期させると、Active Directory で実行されたユーザー情報の変更（パスワードの変更も含む）は、SES のデータベースにも反映されます。PBConnex を利用した環境では、プリブート認証はサーバーで行われるため、常に最新の Active Directory の情報に基づいた認証が行われることになります。この運用では、Active Directory のパスワード変更は、同時にプリブート認証のパスワード変更を意味します。

課題 4. ディスク暗号はローカル認証を行うため、病院のように共通 PC を多く使う組織では、人事異動がある度に各 PC 内のユーザー情報の変更をすることになる。ディレクトリサービスを前提に PC を運用している組織では、ディスク暗号の導入により、これまでの PC 運用や管理体制の継続が困難にな

課題 4.も PBConnex により解決できますが、いくつかのアプローチがあります。

先に例として挙げた病院のケースを考えてみましょう。一般的には病院の PC が外部に持ち出されて利用されることは稀です。PC が有線/無線で LAN に接続できる環境にあり、PBConnex を使ったオートブートを利用すれば、従業員はプリブートでパスワードを入力することなく、PC を使うことができます。ただし、その PC が不正に持ち出されると（LAN に接続できない環境に持ち出されると）、

オートブートは有効にならずプリブート認証画面が表示されます。このアプローチでは、LAN に接続できる場所で不正な第三者が PC を操作した時のリスクを考慮する必要があります。

もうひとつのアプローチでは、ユーザーはプリブートでパスワードを入力します。ただし、認証はローカルではなく、SES で行われます。例えば 200 人が 100 台の共有 PC を使う環境では、SES でこの 200 人のユーザーに対して、100 台の PC へのログインを許可すれば、これらのユーザーはそれぞれ自身のパスワードで、各 PC にログインできるようになります。SES では PC だけでなく、ユーザーもグループ化できるため、200 人と 100 台を一括で紐付けることができます。

課題 5. 暗号化されたディスク上の OS が論理的に壊れた場合、従来の OS の修復や C ドライブだけのリカバリーによる復旧ができなくなる。ディスク全体の復号化が必要になり、ディスクの容量により一日データが利用できなくなることもある。

課題 5.は、これまでの課題とは違い、PBConnex が直接解決するわけではありません。しかし、PBConnex は以下の対応をより迅速にするのに役立ちます。

SecureDoc には、暗号化されたハードドライブを外付けにした場合、そのハードドライブの暗号鍵が接続先の PC のプリブート領域に保存されていればアクセスできる、という特徴があります。つまり、暗号鍵が共有されていれば、暗号化されていないドライブと同じように見えるということです。

問題は、どのように共通の鍵を配布するかです。SecureDoc では、SES から各 PC のプリブート領域のユーザーに鍵を配信する機能があります。この機能を利用すれば、論理的に壊れたドライブを暗号化した鍵を他の PC に配信することができます。しかし、この手法では、PC のローカルのユーザー情報と鍵情報を変更するという面倒があります（右コラムの解説参照）。

PBConnex を使えば、SES 上で、壊れたドライブの接続先の PC の暗号鍵と、壊れたドライブの鍵を持つユーザーを作成し、ドライブの接続先の PC へのログインを許可するだけで、そのドライブのデータを退避できるようになります。

少し分かり難いかもしれませんが、要するに PBConnex では、誰が、どの鍵を持って、どの PC にログインできるかを、管理サーバーである SES の操作だけで決めることができ、その決定内容が即時に反映されるということです。鍵の有無は、あるドライブにはアクセスでき、別のあるドライブにはアクセスできない、というそのユーザーがアクセスできる範囲を決定します。

この手法を利用すれば、PC に内蔵されているハードドライブが論理的に壊れると、1 日仕事ができなくなるという従来のディスク暗号の課題が、数分の作業で解決されます。

「ディスク暗号」よりも安全なディスク暗号

ここで、これまで挙げてきた課題の解決とは別に、PBConnex が実現する従来のディスク暗号よりも、さらに安全なディスク暗号ソリューションについて、社内用 PC、持ち出し用 PC とそれぞれ利用目的別に説明します。

ディスク暗号における鍵の配布：
通常、ディスク暗号化ソフトウェアは各 PC をそれぞれ異なる暗号鍵で暗号化することで、セキュリティを保つ。異なる鍵を使えば、ある PC の鍵が漏えいしたとしても（そのような事態は簡単には起きないものの）、他の PC へ不正にアクセスされる危険がなくなる。

SecureDoc のユーザーと鍵の概念：
SecureDoc にはユーザーに鍵を割り当てるという概念がある。A という PC は A'という鍵で暗号化されているとする。この PC にログインするユーザーには鍵 A'を割り当てる必要がある。1 人のユーザーに複数の鍵を割り当てることもできる。

B'という鍵で暗号化された PC：B があり、B のハードドライブが論理的に壊れたとする。この場合、PC：A に、鍵：A'と B'を持つユーザーを追加し、その ID とパスワードでログインすれば、壊れたハードドライブは通常のドライブのようにアクセスすることができるようになる。セキュリティを考慮すると、この臨時ユーザーは、後から削除することが望ましい。

社内利用 PC - PC が起動できる場所を限定する

省エネ、省スペース、仕事の環境の変化に伴い、PC 全体の出荷台数に占めるノート PC の割合は年々増加していて、2012 年には過去最高の 75.5%に達しました。これには、PC を外部に持ち出す組織が増えているだけでなく、持ち出しは許可していなくてもオフィス内でノート PC を利用するという組織が増えていることが背景にあります。官公庁、自治体や病院、金融機関等の企業は、ノート PC を利用していてもオフィス外への持ち出しを許可していないことが一般的です。また一般企業においても、例えば営業部門には持ち出しを許可し、人事、総務、経理等の部門には許可しないということは、よくあることです。

このようなオフィス内でのみ利用されるノート PC についても、取り扱うデータの種類や事業内容により外部に持ち出すのと同等のセキュリティが必要になるケースは珍しくありません。またオフィス内で PC が紛失した場合でも、所在が分からない以上は監督官庁への届け出が必要になる場合もあります。

それでは外部に持ち出すことを前提としていないノート PC に対する最適なソリューションとはどのようなものでしょうか？

ワイヤーロックを使って物理的に PC を固定することは、一見すると有効な手段に見えます。しかし、社内の会議でノート PC を利用する組織ではワイヤーロックは不完全な対策と言えます。PC の紛失はデスクからの持ち出しを繰り返すうちに発生するからです。

一般的なディスク暗号製品は、社内で利用される PC も外部に持ち出される PC も同様に保護することができ、さらに一元的な管理が可能です。しかし、SecureDoc の PBConnex の特徴を利用して、さらに高いセキュリティを実現することができます。

前述した PBConnex の機能を思いだしてください。PBConnex は、クライアントローカルの認証に頼らず、プリブートの状態でサーバーにアクセスし、サーバー上でユーザー認証を行うシステムです。では、ローカルのユーザーを削除するとどうなるでしょうか？ローカルにユーザーがいない PC を起動させるには、PBConnex を使うしかありません。つまり、**PC を起動させるには、プリブートの状態で SES にアクセスできるネットワークに接続している必要があります。**SES がイントラネットにあれば、PC はそのイントラネット上でしか利用できなくなります。

ここで分かりやすいように、ローカルにユーザーがいない PC を起動させるための条件を示します。ひとつでも条件を満たさなければ PC は起動しません。

- PC がプリブートの状態で SES にアクセスできること
- SES 上でその PC が PBConnex を使ってログインできるように許可されていること
- 入力する ID とパスワードが、SES 上でその PC に登録されていること

仮にこの PC が紛失しても、イントラネット外で起動されることはありません。また、紛失が発覚した場合、即座に SES 上でその PC の起動を拒否するように設定すれば、イントラネット内でも起動することはできなくなります。

このように PBConnex を使えば、オフィス内でのみ利用される PC に対して、**①PC の起動をイントラネットに限定する、②紛失の可能性が発生すれば、管理サーバーで起動を拒否させる、**という強力な制御ができるようになります。この環境で「課題 2」で説明した「PBConnex を使ったオートブート（AutoBoot via PBConnex）」を利用すれば、ユーザーに新たなパスワードを要求することなく安全に PC を運用することができます。

持ち出し用 PC - 外部で PC が利用できる期間を限定する

持ち出し用の PC に対して、「ディスク暗号よりも安全なディスク暗号」は実現できるのでしょうか？営業部門の PC のように社内外で利用される PC は、起動をイントラネットに限定することはできません。社外で利用される PC はプリブートの状態でネットワークにアクセスできない以上、サーバーで動的に制御することはできません。従来のディスク暗号では、社外で紛失した PC は「パスワードが正しく入力されない限りは起動しない」というパスワードによる保護に依存していました。

紛失した PC からの情報漏えい対策を検討する際、紛失した PC から情報が漏えいする可能性をどこまで限定できるかが重要なポイントになります。その可能性の高低が、社内や状漏えいの被害者となり得る取引先や個人がさらされるリスクの大きさに直結するからです。そして企業が情報漏えいの可能性が極めて限定的なものであることを説明することができれば、信用の低下も最小限に留めることができます。

この「情報漏えいの可能性をいかに限定するか」という課題に対して、SecureDoc は以下のような解を持っています。

1. PC が利用できる期限を限定する（サーバーへの定期的な通信を要求する）
2. パスワードの誤入力の許容範囲を限定する（許容範囲を超えるとログインできなくなる）
3. リモートから PC を起動不能にするコマンドを送る

この中で特に 1.のアプローチは、紛失した PC が、一定の期間が経過すると無条件に起動しなくなるという明確な形で、情報漏えいの可能性を限定します。SecureDoc はどのように、この要件を満たすのでしょうか？

PBConnex にはログオン情報をキャッシュする機能があります。この機能は、一度サーバーで認証されたユーザーID とパスワードを既定の日数だけローカルに保存（キャッシュ）します。

キャッシュの保存期間を 7 日とします。この PC にローカルの ID がなければ、利用者は 7 日に一度はイントラネット上の SES に接続できる環境で、PC にログインしなければなりません。SES 上で利用している PC と ID が紐付き、さらにパスワードが正しければ、SES はこのユーザーによる PC の起動を認め、Windows が起動を開始します。キャッシュの保存期間は 7 日間なので、この ID とパスワードは 7 日間だけローカルに保存され、8 日目になるとログインができなくなります。このユーザーは、再びイントラネットに PC を接続し、同じ ID とパスワードを入力する必要があります（この時、管理者への連絡や管理者の介在は不要です）。

このポリシーでは、例え PC が紛失しても、**最後にイントラネットで認証をされてから 8 日目には PC は起動しなくなります。**紛失の発覚と同時に管理者が SES データベースで当該 PC へのユーザー登録をすべて解除すれば、紛失した状態のまま PC がイントラネットに接続されても、PC へのログインはできません。

このように PBConnex のキャッシュ機能は、持ち出し PC の利便性を損なうことなく、紛失した PC が起動される可能性を時間的に制限できるというメリットをもたらします。

ログオン情報のキャッシュ：
PBConnex の環境では、クライアントのローカルに ID とパスワードを持たないユーザーでも、SES で許可されていれば、ログインできる。デフォルトでは、このユーザーは PC がプリブート状態で SES にアクセスできなければ、ログインはできない。しかし一度でも SES で認証されれば、ID とパスワードを一時的にローカルに保存し、次回は SES にアクセスできなくてもローカル認証ができるようになる。この機能をログイン情報のキャッシュと呼ぶ。

この機能は、概念としては Active Directory が持つユーザーログイン情報のキャッシュ機能に似ている。

まとめ

ここで、PBConnex の技術がもたらす具体的なメリットをまとめます。

- PBConnex とは、ローカルにユーザーがいなくても、サーバーでユーザーを認証するという新しいプリブート認証の技術である。
- PBConnex を使えば、誰がどの PC に、どの権限でログインできるのかを、SES と呼ばれる管理サーバーで決定できるため、Active Directory のように、動的にユーザーのログインの許可、拒否を決めることができる。
- 従来のディスク暗号では、管理者が PC のメンテナンスを行おうとすると、PC を起動する度に、パスワードリカバリーを実行する必要があった。PBConnex を使えば、管理者 ID に対してメンテナンス対象の PC へのログインを許可するだけで、この問題は解消される。
- 事業継続を目的に遠隔からクライアント PC を利用するには、従来のディスク暗号ではプリブート認証で起動が妨げられるという問題があった。PBConnex を使えば、クライアントの設定を変更することなく、必要な時だけプリブート認証を省略することができるようになる。
- OS へのログインパスワードを管理者が決める組織が、プリブート認証に対しても同様の運用をしようとすると、ローカルにあるプリブート領域のユーザー情報を更新しなければならなかった。これでは管理者がユーザー情報を更新してから、クライアント PC に反映されるまでの時差が生じる。PBConnex ではユーザーはサーバーで認証されるため、新しいパスワードは即時利用されることになる。
- 病院のように 1 台の PC を複数のユーザーが利用する組織では、各 PC のプリブート領域にすべてのユーザー保存する必要があった。PBConnex でユーザーグループと PC グループを紐付けるだけで、ローカルに存在しないユーザーでも許可されたすべての PC にログインができるようになる。
- ディスク暗号には PC の内蔵ドライブが論理的に壊れると、ドライブ全体を復号化しなければならないという課題がある。PBConnex を使えば、例えば隣のデスクの PC にドライブを接続するだけで、ドライブ内のデータを退避させることができる。
- PBConnex は、社内だけで利用されるノート PC に対して、PC がイントラネットに接続できれば PC の起動を許可するというセキュリティを構築することができる。この時、ユーザーにパスワードを要求することもできるが、パスワードの入力を省略することもできる。いずれの場合も、イントラネット外で PC を起動させることはできない。
- 従来のディスク暗号は、「パスワードが破られない限り、PC を起動させない」という方法で PC の紛失からデータを守っていた。PBConnex を使えば、この方法に加え、特定期間を越えて SES に接続しなければ、PC が起動しなくなるという期間の制限により、更に安全性を高めることができるようになる。

このように、PBConnex はディスク暗号の導入後に発生する新たな運用コストを解消するためのソリューションです。それは、「アドミニストレーター・エクスペリエンス」と「セキュリティ」の向上を目的としていますが、結果的には、電話によるパスワードリカバリーの時間を削減し、PC 故障時の業務停止時間を短くすることで、ユーザーの生産性を高めることにも役立ちます。特に、Active Directory とのパスワード統合は、パスワードの運用という管理者、ユーザー双方の負担を劇的に軽減させることができます。

WinMagic の PBConnex の技術は、これまで PC の運用の側面からディスク暗号の導入を躊躇していた組織、あるいは導入範囲を限定していた組織、あるいは現在使っているディスク暗号システムによって膨れ上がった管理コストに悩む組織にとって、情報セキュリティ対策の見直しのきっかけを与えるでしょう。

ディスク暗号に対する要件と PBConnex のソリューション対応表

ディスク暗号に対する要件	PBConnex のソリューション
PC のメンテナンス時に、管理者が PC 個別にプリブートのパスワードを入力したり、都度チャレンジ・レスポンスを発行したりすることなく、円滑に PC の起動、メンテナンスが行えること。	SES 管理コンソールで対象になるすべての PC に管理者 ID を登録する。対象の PC がイントラネットに接続できる状態で、管理者 ID とパスワードをプリブートで入力すれば、管理者は SES で認証され PC が起動する。 もしくは、PBConnex を使ったオートブートを SES で許可する。クライアントの設定変更は不要。
災害時などを想定して、ユーザーが PC に遠隔でログインする際に、普段は入力しているプリブートのパスワードを入力することなく、PC を起動できること（遠隔からの PC のログインがプリブートにより妨げられないこと）。	PC がイントラネット（SES と同一のネットワーク）にあり、SES に接続できる状態であれば、管理者はクライアントの設定を変えることなく、SES から PBConnex を使ったオートブートを許可することができる。オートブートが許可されていれば、プリブート認証に妨げられることなく PC が起動するようになる。
Active Directory とディスク暗号のパスワード管理が統合できること。例えば、Active Directory でユーザーのパスワードを更新した場合、その時点でプリブート認証にも新たなパスワードでログインさせるようにすること。	PBConnex は Active Directory と連携する機能があり、管理者が Active Directory で新たなパスワードを設定すると、SES 上での認証はこの新たなパスワードが必要になる。PBConnex ではユーザーはローカルではなく、SES により認証されるため、管理者がパスワードを更新した時点で、ユーザーは新しいパスワードを使いプリブートでログインすることになる。
不特定多数の従業員が、不特定の複数の PC を利用する環境で、各 PC にローカルの ID とパスワードを登録することなく、円滑に ID の管理ができること。従業員が退職した場合は、各 PC から ID を削除することなく、管理サーバーの操作だけでログインの拒否ができること。	PBConnex では誰がどの PC にログインできるかの可否を、管理サーバーである SES で決定できる。例えローカルにユーザーがいなくても、SES でその PC へのログインが許可された ID は、正しいパスワードを入力すればその PC を起動することができる。逆に SES の操作だけで拒否することもできる。
暗号化されたディスク上の OS が論理的に壊れた場合、ディスク全体の復号をすることなく即座にデータの退避ができること。	SecureDoc には、「鍵を共有していれば暗号化されたディスクを外付けにしても、通常のドライブと同じようにアクセスできる」という特徴がある。基本的に各 PC はそれぞれ個別の鍵で暗号化されるため、ある PC の鍵を他の PC が持っていることはない。 SES 上に論理的に壊れたドライブの鍵を持つ ID とパスワードを作成し、任意の PC に登録する。その任意の PC に作成した ID とパスワードを入力すれば、サーバーでログインが許可され Windows が起動する。その後、データを退避させたいドライブを接続すると、内部のデータにアクセスできる。この作業は 5～15 分で終わる。
社内でのみ PC の起動を許可し、社外に持ち出した場合は PC を起動できないようにすること	ローカルの ID を削除し、PBConnex を利用して SES による認証のみを許可すれば、イントラネットに接続できない環境では PC は起動しなくなる。PBConnex を使った AutoBoot を利用すれば、ユーザーはパスワードを入力することなくイントラネット内で PC を利用することができる。
紛失した PC からの情報漏えいを防ぐために、定期的にイントラネットに接続しなければ PC を起動できなくすること	PBConnex のキャッシュ機能を使えば要件を満たすことができる。PBConnex は、「X 日 ID とパスワードをキャッシュする」という機能を持つ。クライア

	ントをイントラネットに接続し、SES 上で認証された ID は、規定の日数だけローカルに保存され、イントラネットに接続できない環境でも、ローカル認証ができるようになる。キャッシュが期限切れになると、ユーザーは再度 PBConnex による認証を行わなければ PC を起動できなくなる。

ウインマジックの強力なサポート

ウインマジックの SecureDoc が持つ PBConnex 機能は、プリブート・ネットワーク認証をサポートする唯一のデータ暗号化／管理ソリューションです。SecureDoc は高度なセキュリティと柔軟性を兼ね備えたソリューションで、ノート／デスクトップ PC、サーバーそしてリムーバブルメディアに保存されている機密データを強力に保護することで、企業や組織のプライバシーやセキュリティの法規制に対するコンプライアンスを支援します。

容易な導入展開が可能な SecureDoc は、ユーザーの生産性を低下させることなく、定常的なワークフローにおいて最大限のセキュリティと透過性を確保することができます。OPAL 準拠の自己暗号ドライブ（SED）、TPM やインテル®AES-NI といったハードウェア機能を有効活用し、異なるプラットフォームが混在する企業の IT 環境にも対応することが可能です。さらに、Windows、Mac、iOS や Android そして Linux など多様なプラットフォームすべてにわたるポリシーやパスワードのルール、暗号化の管理など、セキュリティに関係する要素を管理サーバーですべて一元管理します。

SecureDoc の核となるコンポーネントである PBConnex は、ネットワークベースのリソースを活用し、OS の起動前のユーザー認証、アクセス・コントロールの実行、そしてエンドポイント・デバイスの管理を可能にします。ディスク暗号の管理における PBConnex 特有のこのような革新的アプローチによって、IT 管理とエンドユーザの生産性が共に最適化され、大幅なコスト節約が実現します。PBConnex は、オートブート（自動起動）の利便性とプリブート認証によるセキュリティの 2 つのメリットをユーザーにもたらします。ウインマジックは、プリブート環境でのセキュアなネットワーク接続を可能にした最初のディスク暗号ベンダーなのです。

ウインマジックの SecureDoc について

ウインマジックの SecureDoc は、デスクトップ PC、ノート PC、タブレットデバイス、そして USB メモリや CD/DVD、SD カードをはじめとするリムーバブルメディアに保存されているデータすべての保護を容易に実現するディスク暗号化ソリューションです。Microsoft Windows 7、Vista、XP、Mac OS X、さらに Linux の各プラットフォームをサポートする SecureDoc では、Seagate Technology 社などの Opal 仕様準拠ドライブをはじめとする暗号化デバイスを容易に一元管理し、使用することができます。ウインマジックは、ビジネスのリスク軽減、プライバシーや法的規制のコンプライアンス要件への対応、さらに不正アクセスや PC の紛失・盗難からの大切な情報資産の保護を実現する高度なテクノロジーによって、世界中の何千もの企業や政府機関から高い信頼を得ています。SecureDoc は、Common Criteria(コモンクライテリア)、米国の FIPS140-2 等を取得しており、日本においても電子政府推奨リストに記載されている AES 128bit 以上に対応しています。充実したプロフェッショナルサービスとカスタマサービスを誇るウインマジックは、今日、43 ヵ国で 300 万以上におよぶ SecureDoc のユーザーを支援しています。ウインマジックと SecureDoc 製品に関する詳しい情報は、Web サイト www.winmagic.com/jp をご覧いただくか、お電話（03-5403-6952）、または E メール（sales.jp@winmagic.com）にてお問い合わせください。