u.trust LAN Crypt Windows (Classic)

JP

utimaco®

Imprint

Copyright 2023	Utimaco IS GmbH
	Germanusstr. 4 D-52080 Aachen Germany
	AMERICAS +1-844-UTIMACO (+1 844-884-6226)
Phone	EMEA +49 800-627-3081
	APAC +81 800-919-1301
	https://support.hsm.utimaco.com/
Internet e-mail	support@utimaco.com

u.trust LAN Cryptとは何ですか？

*u.trust LAN Crypt*は、透過的なファイル暗号化により、小規模から大規模組織における承認グループ内での機密データの交換を可能にします。*u.trust LAN Crypt*はユーザーの操作を必要とせず動作します。セキュリティオフィサー（SO）の役割をサポートし、*u.trust LAN Crypt*で暗号化されたファイルへのアクセス権を制限することが可能です。マスターセキュリティオフィサー（MSO）は、*u.trust LAN Crypt*の管理権限、または権限委任を行う権限を有します。これにより、あらゆる企業のセキュリティ要件を満たすセキュリティオフィサーの階層構造を構築することが可能です。

u.trust LAN Crypt バージョン4.0.0では、暗号化機能向けに初めて、現代的で将来性のあるミニフィルター技術が実装されました。バージョン4.1.0以降、*u.trust LAN Crypt*クライアントにはレガシーフィルタードライバーが含まれておりません。

> ご注意 *u.trust LAN Crypt* バージョン4.1.0以降をインストールされる場合、新しいモダンなミニフィルタードライバーが自動的にインストールされます。このバージョンでは、従来のレガシーファイルフィルタードライバーへの切り替えはサポートされません。

暗号化されたファイルは、個々のユーザーに割り当てる必要はありません。必要なキーを持つユーザーであれば、誰でも暗号化されたファイルを操作できます。これにより、管理者は暗号化されたファイルへのアクセスを共有し、操作できる論理的なユーザーグループを作成できます。このプロセスは、日常生活で使用されるキー束のようなものと比較できます。*u.trust LAN Crypt* は、ユーザーおよびユーザーグループにキー束を提供し、その個々のキーを異なるフォルダーやファイルに使用できます。

ユーザーがファイルを暗号化フォルダに移動するたびに、そのファイルはユーザーのコンピューター上で暗号化されます。同じ権限グループ内の別のユーザーがフォルダからファイルを読み取る場合、ファイルは暗号化された状態で転送されます。ファイルは受信者のコンピューター上で初めて復号され、そこで編集が可能となります。ファイルが暗号化フォルダに戻される前に、再度暗号化されます。

権限のないユーザーは（*u.trust LAN Crypt*がインストールされていないワークステーションからのみ）これらの暗号化されたファイルにアクセスできる可能性がありますが、対応する*u.trust LAN Crypt*の認証がない場合、暗号化された内容のみが表示されます。これにより、ファイルシステム自体にアクセス保護が定義されていなくても、ネットワークが攻撃されても、従業員が組織のセキュリティガイドラインに従わなくても、ファイルは常に保護された状態を維持します。

u.trust LAN Cryptによるデータ保護

*u.trust LAN Crypt*は、機密ファイルをファイルサーバーやワークステーション上で暗号化して保存することを保証します。同様に、ネットワーク（LANまたはWAN）上での送信も保護されます。これは、暗号化と復号がユーザーのワークステーションのメインメモリ内で実行されるためです。ワークステーション上では、すべての暗号化と復号が透過的に行われ、ユーザーの操作をほとんど必要としません。ファイルサーバー自体に特別なセキュリティソフトウェアをインストールする必要はありません。

セキュリティオフィサーは、フォルダやファイルに対して異なるアクセス権を設定できます。これらの権限は、ユーザー向けの暗号化プロファイルにまとめられます。暗号化プロファイルはポリシーファイルを介してユーザーに配布されます。ポリシーファイルには、透過的暗号化に必要なすべてのルール、アクセス権、キーが含まれています。ポリシーファイルは証明書によって保護されています。ユーザーが自身のコンピュータ上で*u.trust LAN Crypt*で暗号化されたデータを処理するには、ポリシーファイルへのアクセス権が必要です。証明書に属する秘密キーを所有することで、ユーザーは暗号化プロファイルが保存されているポリシーファイルにアクセスできます。

*u.trust LAN Crypt*では、ユーザーを異なる権限グループに分類することが可能です。ポリシーファイルに同一の暗号化プロファイルを保存しているすべての*u.trust LAN Crypt*ユーザーは、同一の権限グループのメンバーとなります。暗号化やキー交換についてご心配いただく必要はございません。ポリシーファイルにアクセスできる環境さえ整っていれば、ファイルの開閉時に自動的に暗号化または復号が行われます。ユーザーを一元管理するLANモデルから、ノートパソコンのみを利用する分散モデルまで、あらゆる組織形態に対応可能です。

バージョン4.03以降、*u.trust LAN Crypt*ミニフィルタードライバーは、*SafeGuard Enterprise*（ファイル共有）で暗号化されたファイルも処理可能です。これらのファイルの復号は不要です。*SafeGuard Enterprise*の対応するキーは、キーエクスポートおよびインポートツールを使用して*u.trust LAN Crypt*へ移行するだけで十分です。

ご注意

- この点に関しまして、*SafeGuard Enterprise Fileshare* で暗号化されたファイルを *u.trust LAN Crypt* で編集した場合、そのファイルは *SafeGuard Enterprise Fileshare* で読み取ることができなくなりますので、ご注意ください。

- 通常の動作時においても、Windows は作業メモリの一部をハードディスクにスワップすることが頻繁にあります。クラッシュやいわゆる「ブルースクリーン」などの状況では、メモリ内容全体がハードディスクに書き込まれる可能性すらあります。その結果、通常はメインメモリにのみ存在する機密情報（開いているドキュメントの内容など）が、ハードディスク上のファイルとして保存される可能性があります。ハードディスク暗号化（例：*BitLocker* や *Utimaco DiskEncrypt*）は、こうした機密性の高いデータのコンテンツが、いかなる場合でも暗号化された状態でハードディスクに保存されることを保証し、スパイ行為から最適に保護します。このため、ハードディスク暗号化は重要な基本保護策として、また *u.trust LAN Crypt* をご利用の際の有用な追加対策として、その使用をお勧めいたします。

SafeGuard Enterprise：ファイル暗号化の移行

SafeGuard Enterpriseは、Sophos社のセキュリティスイートであり、複数のモジュールで構成されています。Data Exchange（DX）、Cloud Storage（CS）、File Encryption（FE）はいずれもファイルレベルの暗号化を提供します。しかしながら、ソフトウェアスイート全体が提供終了となるため、ユーザーは暗号化された文書へのアクセスを失うリスクに直面しています。セキュリティ製品から別の製品への移行は、特にデータの復号を伴う場合、煩雑で追加のリスクを伴う可能性があります。しかし、u.trust LAN Crypt への移行においては、そのような懸念はございません。

u.trust LAN CryptとSophos SafeGuard Enterpriseは完全な互換性を有しています。両製品は同一の技術基盤とファイル暗号化サブシステムを共有しています。従いまして、SafeGuard Enterpriseで暗号化されたファイルはu.trust LAN Cryptと完全な互換性を持ち、ネイティブに読み込むことが可能です。暗号化キーは各インストール環境に固有のものであり、移行が必要なのはこれらのキーのみとなります。

ステップ1：**SafeGuard Enterprise**からのキーのエクスポート

ファイルの暗号化に使用されるキーは、SafeGuard Enterpriseの各インストール環境ごとに固有のものでございます。Sophosでは、SafeGuard Enterpriseでファイルの暗号化に使用される全ての暗号化キーを簡単にエクスポートできるツールを提供しています。全てのキーは、便利なことに単一のパッケージにまとめてコピーされます。

ステップ2：**u.trust LAN Crypt**へのキーのインポート

別途パッケージとして提供されるようになったキーは、既存のu.trust LAN Cryptシステムに簡単にインポートできます。インポートが完了すると、u.trust LAN Cryptのインストール環境は、SafeGuard Enterpriseで暗号化されたファイルにアクセスするために必要なすべての要素を備えることになります。

ステップ3：ポリシーの更新／キーの割り当て

新たにインポートしたキーを、SafeGuard Enterpriseで暗号化されたファイルへのアクセスが必要な全ユーザーに割り当ててください。これらのキーにより、ユーザーは過去にSafeGuardファイル暗号化モジュールで暗号化されたファイルを読み取ることが可能となります。これは、キーインポート後にSafeGuard Enterpriseで暗号化されたファイルにも適用されます。

ステップ4：**SafeGuard Enterprise**ファイルへのアクセス

u.trust LAN Cryptクライアントは、SafeGuard Enterpriseと技術基盤を共有しています。キーがクライアントに展開されると、SafeGuard Enterpriseのファイル暗号化モジュール（DX、CS、FS）のいずれかで暗号化されたすべてのファイルを読み取ることが可能です。個々のファイルを復号する必要はございません。ファイルが暗号化されてからどれほど時間が経過していても、u.trust LAN Cryptで読み取ることが可能です。

完全なファイルレベルの互換性により、スムーズな移行が可能です。社内で一部がSafeGuard Enterpriseを引き続き使用している場合でも、そこで作成されるすべての暗号化ファイルは、既にu.trust LAN Cryptに移行したユーザーが読み取ることが可能です。

ご注意

- SafeGuard Enterprise をインストール済みで、*u.trust LAN Crypt* への移行をご検討の場合は、u.trust LAN Crypt サポートまでお問い合わせください。詳細はhttps://utimaco.com/file-encryption-migration-five-easy-steps-safeguard-enterpriseをご覧ください。

暗号化

透過的暗号化

ユーザーにとって、透過的暗号化とは、暗号化された形式（暗号化されたフォルダーやドライブ内）で保存されているすべてのデータが、アプリケーション（Officeなど）によって開かれるとすぐにメインメモリ上で自動的に復号されることを意味します。ファイルが保存されると、自動的に再暗号化されます。透過的暗号化はすべてのファイル操作を対象とします。すべての処理がバックグラウンドで実行されるため、ユーザーは暗号化されたファイルを操作している際にそのことを意識することはありません。

ご注意

- *u.trust LAN Crypt* は、Windows の NTFS ファイルシステムにおいて **NTFS** 圧縮 または **EFS** 暗号化 が適用されているファイルを暗号化することはできません。ただし、初期暗号化ウィザードでは、暗号化ルールが存在する場合、初期暗号化時に NTFS 圧縮および/または EFS 暗号化が施されたファイルを解凍または復号するオプションを提供します。その後、ファイルは暗号化ルールに従って*u.trust LAN Crypt*によって暗号化されます。ユーザーが必要に応じてNTFS圧縮ファイルを解凍したり、EFS暗号化ファイルを復号したりできるかどうかは、事前にセキュリティオフィサーが決定する必要があります。

暗号化はフォルダに依存せず、暗号化ルールのみに基づきます。暗号化の仕組みは以下の通りです。

- 暗号化ルールが設定されているすべてのファイルは、自動的に暗号化されます。
- ファイルが暗号化フォルダに移動またはコピーされると、そのフォルダに定義された暗号化ルールに従って暗号化されます。セキュリティ管理者は、*u.trust LAN Crypt* 管理ツールを通じて、同一フォルダ内の異なるファイルタイプやファイル名に対して複数の暗号化ルールを定義できます。例えば、Wordファイルと Excelファイルが同じフォルダ内に存在する場合でも、異なるルールで暗号化することが可能です。
- 暗号化されたファイルの名前を変更した場合、そのファイルは暗号化されたままとなります（新しいファイル名または拡張子に対して別の暗号化ルールが存在しない場合、または暗号化ルールが存在しない場合を除きます）。
- ユーザーが暗号化されたファイルを、以前の暗号化ルールが適用されなくなった場所にコピーまたは移動した場合、自動的に復号されます。

  ご注意

  - 同一ネットワーク共有内の別のフォルダへファイルを移動した場合、この処理は適用されません。この場合、暗号化ルールが存在しない場合でも、ファイルは暗号化されたままとなります。
- セキュリティオフィサーまたはシステム管理者が、*u.trust LAN Crypt* グループポリシー（GPO）を通じて永続的暗号化機能を有効にしている場合、暗号化されたファイルは、暗号化ルールが存在しない別のフォルダーや場所（例：USBメモリ）に移動またはコピーされた場合でも、暗号化された状態を維持します。
- ユーザーが暗号化されたファイルを暗号化ルールが適用されている場所にコピーまたは移動した場合、ファイルはまず復号され、その後その場所に定義されている別のキーを使用して暗号化されます。

暗号化データへのアクセス

特定のフォルダーに対して、ユーザーの暗号化ポリシーにキーも暗号化ルールも設定されていない場合、そのフォルダー内の暗号化ファイルへのアクセスは許可されません。ユーザーは、そのフォルダー内の暗号化ファイルに対して、読み取り、コピー、移動、名前変更、削除などの操作を行うことができません。

ただし、ファイルの暗号化に使用されたキーをユーザーが所持している場合、その場所またはフォルダーに対する暗号化プロファイルに暗号化ルールが含まれていなくても、ファイルを開くことが可能です。

ご注意

- LAN Crypt Administration Windows バージョン 13.0.0 以降では、CBC-uIV 形式での暗号化が利用可能となります。旧式の Classic LAN Crypt クライアント（バージョン 13.0.0 以前）はこの形式を認識しないため、該当するファイルを復号できません。常に最新のクライアントバージョンをご利用いただくようお願いいたします。

u.trust LAN Crypt 2Go の統合

u.trust LAN Crypt 2Go によってパスワード暗号化されたファイルは、バージョン 4.2.0 以降の *u.trust LAN Crypt for Windows* で開いて編集することが可能です。ただし、ユーザーの暗号化ポリシー内に必要なキーが存在していることが条件となります。

ファイルの閲覧または編集後も、*u.trust LAN Crypt 2Go* および *u.trust LAN Crypt 2Go* またはパスワードベースの暗号化・復号をサポートするその他の *u.trust LAN Crypt* アプリケーションでは、同じキーを使用して自由に暗号化および復号が可能です。

フォルダの名前変更または移動

パフォーマンス上の理由により、*u.trust LAN Crypt* は、Windows エクスプローラーを介してドライブ内でフォルダ全体を移動した場合、暗号化状態を変更いたしません。これは、フォルダ全体を移動しても、暗号化、復号、再暗号化は発生しないことを意味します。

該当するフォルダ内のファイルが暗号化されていた場合、新しいフォルダ名または新しい場所でも暗号化された状態が維持されます。ユーザーが対応するキーをお持ちであれば、これらのファイルを通常通り操作することが可能です。

ただし、暗号化ルールが設定されていない別のパーティションやUSBストレージデバイスへファイルやフォルダを移動する場合、動作が異なります。*u.trust LAN Crypt*の機能である永続的暗号化が有効化されていない場合、そのようなメディアへ移動するとファイルは復号されます。セキュリティオフィサーまたはシステム管理者がクライアント向けに永続的暗号化を有効化している場合、ファイルは暗号化されたままとなります。

セキュア移動

*u.trust LAN Crypt*は、ファイルやフォルダのセキュア移動をサポートしています。*u.trust LAN Crypt*を介してファイルを移動する際、該当する暗号化ルールに基づき、ファイルは暗号化され、新しい場所で復号または再暗号化されます。その後、元のファイルは安全に削除されます。

この機能は、*u.trust LAN Crypt* の Windows エクスプローラー コンテキスト メニューにある **u.trust LAN Crypt** -> セキュア移動 からご利用いただけます。ダイアログ ボックスで、ファイルを移動する先を選択することができます。

ファイルの明示的な復号

ファイルを復号するには、暗号化ルールが適用されていないフォルダにファイルをコピーまたは移動するだけで結構です。ファイルは自動的に復号されます。

前提条件：

- 対応する暗号化プロファイルが読み込まれていること
- ユーザーが必要なキーを所持している
- アクティブな暗号化プロファイルに、新しい場所に対する暗号化ルールが含まれていない場合
- 永続的暗号化 が有効になっていません

  ご注意

  - *u.trust LAN Crypt* は、Windows のオフラインフォルダも暗号化できます。ただし、ウイルススキャナに関連して問題が発生する可能性があります。ウイルススキャナに関する既知の問題の詳細な情報は、*u.trust LAN Crypt* クライアントのバージョン情報でご確認いただけます。

暗号化されたファイルの削除

暗号化ルールが読み込まれた後、キーをお持ちの暗号化されたファイルはすべて削除することが可能です。

ご注意

- 実際のファイル削除は、Windowsのごみ箱への移動を指します。最高水準のセキュリティを確保するため、*u.trust LAN Crypt*で暗号化されたファイルは、ごみ箱内でも暗号化された状態を維持します。ごみ箱を空にする際にキーは必要ありません。

暗号化対象外となるファイルとフォルダ

以下のファイルおよびフォルダは、暗号化ルールが定義されていても、自動的に暗号化の対象外となります。

- u.trust LAN Crypt のインストールフォルダ内のファイル。
- Program Files および Program Files (x86) フォルダ内のファイル。
- Windowsのインストールフォルダ内のファイル。
- Program Files および Program Files (x86) フォルダ内のファイル。
- Windows.oldフォルダ内のファイル。
- Windowsのインストールフォルダ内のファイル。
- ポリシーファイルのキャッシュ。
- Windows.oldフォルダー内のファイル。

その場所は、*u.trust LAN Crypt* 管理画面で指定され、ダイアログのステータスタブのプロファイルタブに表示されます。

- システムドライブのルートディレクトリです。サブフォルダは除外されません。
- インデックス対象の場所 (search-ms)。
- *u.trust LAN Crypt* で除外または無視ルールが定義されているフォルダ内のファイル。
- インデックス対象の場所 (search-ms)。

永続的暗号化

u.trust LAN Crypt では、セキュリティオフィサーまたはシステム管理者が、*u.trust LAN Crypt* グループポリシー（GPO）を通じて永続的暗号化を設定できます。通常、ファイルは暗号化ルールが適用される場合にのみ暗号化されます。

例えば、ユーザーが暗号化されたファイルを暗号化ルールが定義されていないフォルダにコピーした場合、そのファイルはコピー先のフォルダで復号されます。しかし、永続的暗号化が有効になっている場合、ファイルは暗号化ルールが定義されていない別の場所に移動またはコピーされても、暗号化された状態を維持します。

セキュリティオフィサーまたはシステム管理者は、*u.trust LAN Crypt* グループポリシー（GPO）を通じてこの動作を設定できます。永続的暗号化が無効化されている場合、暗号化ルールが存在しない場所にファイルがコピーまたは移動されると、ファイルは復号されます。これにより、例えばメールの添付ファイルとして送信するためにファイルを復号することが可能です。ただし、永続的暗号化を有効にしたまま、そのようなファイルを無視ルールまたは例外ルールが設定されたフォルダーにコピーすることをお勧めいたします。これにより、永続的暗号化の保護機能を維持しつつ、ユーザーが明示的にファイルを復号できる保存場所（例：メール送信時）を確保することが可能となります。

以下の規則は、永続的暗号化に適用されます。

- *u.trust LAN Crypt* ドライバーは、パス情報を含まないファイル名のみを保持します。比較に使用できるのはこのファイル名のみであるため、ソースファイルとターゲットファイルの名前が完全に一致する場合のみを検出します。コピー操作中にファイル名が変更された場合、結果として生成されたファイルは「異なる」ファイルと見なされ、永続的暗号化の対象外となります。
- ユーザーが暗号化されたファイルを「名前を付けて保存」で暗号化ルールの適用対象外の位置に保存した場合、そのファイルは復号された状態で保存されます。

- ファイルに関する情報は、一定期間のみ保持されます。操作に時間がかかりすぎる場合（15秒以上）、新しく作成されたファイルは別の独立したファイルと見なされ、永続的暗号化の対象外となります。

永続的暗号化と暗号化ルールの違い

永続的暗号化は、暗号化されたファイルがその暗号化状態、すなわち元の暗号化キーを維持することを保証します。ファイルが暗号化ルールの適用されていないフォルダにコピーまたは移動された場合、永続的暗号化は正常に機能します。ただし、ファイルが異なる暗号化ルールの適用されている場所にコピーまたは移動された場合、その暗号化ルールが永続的暗号化よりも優先されます。その場合、ファイルはその場所の暗号化ルールに従って変換されます。具体的には、その場所用に定義された暗号化アルゴリズム（例：AES）とキーが使用されます。 例：AES）およびその場所に定義されたキーを使用して変換されます。

永続的暗号化とパス除外ルールの比較

パス無視ルールは永続的暗号化を上書きします。これは、適用可能なパス無視ルールが設定されたフォルダにコピーされた暗号化ファイルが復号されることを意味します。

パス除外ルールは、主に頻繁にアクセスされるファイルや、特に暗号化する必要性がないファイルに対して使用されます。これによりシステムパフォーマンスが向上します。

永続的暗号化と除外パスルールの比較

除外パスルールは永続的暗号化を上書きします。これは、適用可能な除外パスが設定されたフォルダにコピーされた暗号化ファイルが復号されることを意味します。

永続的暗号化の制限事項

永続的暗号化にはいくつかの制限がございます。

暗号化されないはずのファイルが暗号化される

暗号化されていないファイルは、暗号化ルールを適用する場合と適用しない場合の両方で、複数の場所にコピーされます。

- 暗号化されていないファイルが同時に複数の場所にコピーされ、そのうち1つの場所に暗号化ルールが適用されている場合、そのファイルのすべてのコピーも暗号化される可能性があります。
- 暗号化されていないファイルが暗号化された場所にコピーされた場合、そのファイルは暗号化ツールの内部リストに追加されます。ファイルの2つ目のコピーが作成されると、暗号化ツールはそのリスト内でファイル名を見つけ、2つ目のコピーも同様に暗号化します。

暗号化されたファイルにアクセスした後に同じ名前のファイルを作成した場合

- 暗号化されたファイルが開かれた（アクセスされた）後、直ちに同じ名前の新しいファイルが作成された場合、新しく作成されたファイルは最初のファイルと同じキーで暗号化されます。
- これは、暗号化されたファイルの読み取りと新規ファイルの作成の両方に、同一のアプリケーション／スレッドが使用された場合にのみ適用されます。

例： Windows エクスプローラーで、暗号化ルールが適用されているフォルダ内で右クリックし、[新規作成] -> [テキスト ドキュメント] を選択します。直後に、暗号化ルールが適用されていないフォルダ内で右クリックし、[新規作成] -> [テキスト ドキュメント] を選択します。2つ目のファイルも暗号化されます。

ファイルが暗号化されない場合

ファイルの複数コピーが作成されます

- 暗号化されたファイルのコピーが元のファイルと同じフォルダ内に作成された場合、これらのコピーは暗号化されません。作成されたコピーは異なるファイル名（例：doc.txt 対 docCopy.txt）を持つため、ファイル名の一致が失敗し、結果として永続的暗号化によって暗号化されません。

DLP製品向けクライアント**API**および暗号化タグ

データ漏洩防止（**DLP**）製品が暗号化が必要なデータを識別した場合、*u.trust LAN Crypt*クライアントAPIを使用してこれらのファイルを暗号化することが可能です。*u.trust LAN Crypt* 管理コンソール（管理ヘルプ参照）では、

使用する*u.trust LAN Crypt* キーを指定する異なる暗号化タグを定義できます。クライアント API は、これらの事前定義された暗号化タグを使用して、異なるコンテンツに特別なキーを適用することが可能です。例えば、DLP 製品によって機密扱いと分類されたすべてのファイルを暗号化するには、暗号化タグ `\<CONFIDENTIAL\>` を使用します。

透過的暗号化の無効化／有効化

u.trust LAN Crypt ユーザーメニューで透過的暗号化を無効化した場合、無効化後にアクセスされるファイルは自動的に暗号化・復号されなくなります。また、新規生成されたファイルも暗号化されません。これは、ユーザーの暗号化プロファイルに該当ファイルの暗号化ルールが含まれている場合でも同様です。

ご注意

- ユーザーメニューから選択可能な機能や要素の設定は、セキュリティオフィサーまたはシステム管理者が*u.trust LAN Crypt*グループポリシー（GPO）を通じて設定できます。これにより、ユーザーが透過的暗号化を無効化できないようにクライアントを設定することが可能です。

一方、永続的暗号化を無効化すると、暗号化されたファイルが暗号化ルールが存在しない場所やフォルダへコピー／移動された際に復号されます。フォルダやファイルに対するルールベースの自動暗号化・復号機能（透過的暗号化参照）は、永続的暗号化を無効化しても有効なままとなります。永続的暗号化の設定も、セキュリティオフィサーまたはシステム管理者により、*u.trust LAN Crypt* グループポリシー（GPO）を通じて行われます。

永続的暗号化機能を有効にしている場合、暗号化されたファイルは、暗号化ルールが存在しない場所やフォルダにコピーまたは移動されても暗号化されたままとなります。永続的暗号化をご利用の場合、暗号化されたファイルを別の場所にコピーする前に透過的暗号化を無効にする必要はありません。永続的暗号化は、ファイルが誤って別のフォルダに移動された場合や、ユーザーが移動・コピー前に暗号化を解除するのを忘れた場合でも、ファイルが暗号化された状態を維持することを保証します。永続的暗号化の設定変更（有効化または無効化）を有効にするには、コンピューターの再起動が必要です。

ご注意

- 永続的暗号化 が有効な状態で、ユーザーがファイルを 無視ルール または 除外ルール が適用されているフォルダーに移動またはコピーした場合、そのファイルは復号されます。また、永続的暗号化 設定の変更にはクライアントコンピューターの再起動が必要です。再起動が行われるまで、以前に定義された設定は有効なままとなります。

透過的暗号化とファイル圧縮ツール

ファイル圧縮ツールはファイルを開き、ファイルの内容を読み取って圧縮します。透過的な復号/暗号化が有効になっている場合、ファイル圧縮ツールは復号されたファイルを受け取り、そのファイルが圧縮されます。結果として生成されるアーカイブ内のファイルは、もはや暗号化されていません。アーカイブが暗号化ルールが存在しないディレクトリに保存されている場合、保存されているすべてのファイルは復号されます。

永続的暗号化が有効な場合、ファイルは暗号化された状態で圧縮されません。ただし、アーカイブファイル自体は暗号化されたままであり、必要なキーを持つユーザーのみが読み取ることができます。ただし、この前提条件として、アーカイブファイル自体にも暗号化ルールが適用されている必要があります。

ただし、暗号化されたファイルを圧縮プログラムでアーカイブファイルに圧縮したい場合は、そのようなプログラムを使用する前に透過的暗号化を無効にする必要があります。この手順は通常、作成するアーカイブファイルに暗号化ルールが存在しない場合にのみ必要となります。

ただし、そのような暗号化ルールが存在する場合、作成されたアーカイブファイル内のファイル自体は暗号化されませんが、アーカイブファイル自体は、この目的のために定義された暗号化ルールに従って暗号化され、不正アクセスから安全に保護されます。

ファイルを暗号化された状態でアーカイブファイルに圧縮する別の方法は、圧縮プログラムを未処理アプリケーションとして定義することです。必要に応じて、セキュリティオフィサー（MSO / SO）またはシステム管理者が*u.trust LAN Crypt*グループポリシー（GPO）を通じて設定できます。

クラウド同期

Microsoft OneDrive、Google Drive、Nextcloud、BoxDriveなどの主要なクラウド同期アプリケーションは、インストール時に自動的に自身を登録するよう設定されています。デフォルトでは、これらのアプリケーションおよび関連する子プロセスは、暗号化されたファイルの内容へのアクセスが禁止されています。

この制限を他のクラウドアプリケーションおよびその子プロセスにも適用し、暗号化されたファイルの内容を読み取れないようにしたい場合は、以下の手順に従ってシステムレジストリを変更することで実現できます。

キー: `HKLM\SYSTEM\CurrentControlSet\Services\cplcdt2\Parameters`

設定: `IgnoredCloudSyncApps` キー: `HKLM\SYSTEM\CurrentControlSet\Services\cplcdt2\Parameters`

タイプ: `REG_MULTI_SZ` 設定: `IgnoredCloudSyncApps`

初期暗号化と明示的暗号化

u.trust LAN Crypt のインストール後、初期暗号化処理を実施する必要があります。この処理では、読み込まれた暗号化プロファイルを使用してすべてのファイルが暗号化されます。この初期暗号化は以下の方法で実行できます。

- システムトレイアイコンの右クリックメニューから「初期暗号化」を選択
- *u.trust LAN Crypt* のシステムトレイアイコン（詳細はユーザーアプリケーションをご参照ください）
- u.trust LAN Crypt エクスプローラー拡張機能（エクスプローラー拡張機能 をご参照ください）
- *u.trust LAN Crypt* エクスプローラー拡張機能については、エクスプローラー拡張機能 をご参照ください
- u.trust LAN Crypt エクスプローラー拡張機能については、エクスプローラー拡張機能 をご参照ください
- **lcinit.exe** ツール（無人モードにも対応しています）。詳細は無人モードでの初期暗号化をご参照ください。
- *u.trust LAN Crypt* エクスプローラー拡張機能については、エクスプローラー拡張機能 をご参照ください。

フォルダ全体の初期暗号化を行うことに加え、**lcinit.exe** コマンドラインツールとエクスプローラー拡張機能を使用することで、個々のファイルの暗号化、復号、再暗号化も行うことが可能です。

ご注意

- 初期暗号化時、ファイルは辞書順に並べ替えて表示されます。

以下の場合には、対象を特定した明示的な暗号化、復号、または再暗号化が必要となる可能性があります。

- 暗号化ルールが設定されているディレクトリ内に、平文（暗号化されていない）ファイルが存在する場合。
- 暗号化ルールが存在しないディレクトリに暗号化されたファイルが存在する場合。
- 暗号化されたディレクトリ内のファイルが誤ったキーで暗号化されている場合。
- 暗号化プロファイル内の暗号化ルールが変更された場合。
- 複数のキーでファイルが暗号化されている場合。

初期暗号化ウィザード

初期暗号化ツールである**lcinit.exe**は、グラフィカルユーザーインターフェースを備えたウィザードを提供します。このウィザードは以下をサポートします。 以下の機能をサポートしています。

- ファイルの暗号化、復号、再暗号化
- ファイルの暗号化、復号、再暗号化
- ファイルの暗号化、復号、再暗号化
- ファイルの暗号化状態の確認（フォルダ内およびサブフォルダ内のファイルも含みます）
- ファイルの暗号化、復号、再暗号化

このウィザードを開始することができます

- タスクバーのアイコンをクリックすることで開始できます
- タスクバーのアイコンをクリックすることで開始できます

- タスクバーのアイコンをクリックして開始できます
- スタート/u.trust LAN Crypt Client/初期暗号化 を選択して
- タスクバーのアイコンをクリックして
- u.trust LAN Crypt プログラムフォルダ内の **lcinit.exe** をダブルクリックして。
- ［スタート］→［u.trust LAN Crypt Client］→［初期暗号化］を選択して実行してください。

  ご注意

  - 暗号化、復号、再暗号化のプロセスは常に暗号化プロファイルに従って実行されます。そのため、暗号化プロファイルを読み込む必要があります。

初期暗号化の実施

ステップ1： ウィザードを起動します。詳細はユーザーメニューをご参照ください。

ステップ2： ステップ1/5で「初期暗号化を実行する」オプションを選択してください。

ステップ3： 次へをクリックしてください。 ステップ4： 次に、ステップ2 / 5でファイルの処理方法を定義してください。

- プロファイルに従ってファイルを暗号化**:** このオプションを選択すると、ユーザーのプロフィールに含まれるルールに従ってファイルが暗号化されます（デフォルト設定）。システムが既に暗号化されているファイルを検出した場合、それらは無視されます。
- プロファイルに従ってファイルを再暗号化**:** このオプションを選択すると、プロファイルで定義されたキーとは異なるキーで暗号化されたファイルも復号され、正しいキーで暗号化されます。

  ご注意

  - この手順の前提条件として、最初にファイルの暗号化に使用されたキーがユーザーのプロファイルに含まれている必要があります。

ステップ5： 次へをクリックしてください。 ステップ6： 次に、ステップ3/5で、初期の暗号化または復号プロセスに含めたいドライブ、フォルダ、およびサブフォルダを指定してください。ルールで指定されたフォルダは、プロファイルルールボタンで選択できます。

選択されたドライブとフォルダにはチェックマークが付きます。フォルダの横に「+」記号が付いたチェックマークが表示されている場合、そのフォルダ内に処理対象外（つまり、ファイルの暗号化/復号が行われない）のサブフォルダが存在することを示しています。これらも処理対象とする場合は、マウスクリックでチェックマークを付ける必要があります。

プロファイルルールをクリックすると、ユーザーのプロファイルに暗号化ルールが設定されているすべてのディレクトリが自動的に選択されます。

詳細設定をクリックすると、追加オプションにアクセスできます。

ご注意

- ユーザーが変更可能な設定は、*u.trust LAN Crypt* クライアントの設定内容によって異なります。セキュリティオフィサーが設定を中央管理いたします。

- 必要に応じて**EFS**暗号化ファイルを復号： このオプションを選択すると、EFS暗号化ファイルを復号して再暗号化します。ただし、これらのファイルには暗号化ルールが適用されている必要があります。このオプションを選択しない場合、初期暗号化ウィザードはEFS暗号化ファイルを無視します。暗号化ルールが指定されていても、*u.trust LAN Crypt* による再暗号化は行われません。
- 必要に応じて**NTFS**圧縮ファイルを解凍する： このオプションを選択すると、NTFS圧縮ファイルを解凍し、暗号化します。ただし、暗号化ルールが適用されている必要があります。このオプションを選択しない場合、初期暗号化ウィザードはNTFS圧縮ファイルを無視します。暗号化ルールが指定されていても、これらのファイルは暗号化されません。
- 複数のキーで暗号化されたファイルの復号/再暗号化**:** このオプションを選択すると、複数のキーで暗号化されたファイルを再暗号化します。ファイルは1つのキーのみで暗号化されます。なお、これらのファイルには暗号化ルールが適用されている必要があります。

ご注意

- このオプションは、ステップ2/5でプロファイルに従ってファイルを暗号化またはプロファイルに従ってファイルを再暗号化が選択されている場合にのみ利用可能です。それ以外の場合は、このオプションはグレー表示となります。

- 以下のファイル形式のみを含める: 初期暗号化処理の対象を制限したいファイル形式を選択してください（例: .docx、.pdf、txt）。この設定は、暗号化ルールが存在するファイルにのみ適用されます。フォルダ内に異なる種類のファイルが存在する場合、初期暗号化処理の対象にはなりません。それらのファイルは、ユーザーが開いて保存した際にのみ暗号化されます。複数のファイル形式を指定する場合は、セミコロンで区切ったリストを使用してください。

ステップ 7: 次へをクリックしてください。 ステップ8： 次に、ステップ4/5で作成する初期暗号化レポートに含めるファイルを定義します。初期暗号化レポートでは、以下のオプションから選択できます。

- エラーのみを報告**:** ステータスレポートには、暗号化中にエラーが発生したファイルのみが含まれます。

- 変更されたファイルとエラーを報告する: ステータスレポートには、変更されたすべてのファイルと、暗号化中にエラーが発生したファイルが含まれます。

- すべてのファイルを報告する： ステータスレポートには、すべてのファイルが含まれます。

ステップ9： 次へをクリックしてください。 各ファイルの暗号化結果、使用されたキーのキー名、および暗号化アルゴリズムが、ステップ5/5に表示されます。

個々のファイルで暗号化に失敗した場合、再試行ボタンを押すことで、それらのファイルを直ちに再度暗号化することができます。

列見出しをクリックすると、結果をアルファベット順に並べ替えることができます。さらに、ステータスレポートを任意のファイル場所にXMLファイルとして保存することも可能です（エクスポートボタン）。このステータスレポートを活用することで、暗号化に失敗したファイルについて、後ほど暗号化を再試行することが可能です。

ステップ10： 完了をクリックしてください。ウィザードが閉じられます。

暗号化状態の確認

手順 **1:** ウィザードを開始します。

ステップ2: ステップ1/5で、暗号化状態の確認オプションを選択してください。

ステップ3： 次へをクリックしてください。

ステップ4： ステップ2/5で検証したいすべてのドライブとフォルダを選択してください。

ステップ5 ドライブとフォルダにチェックマークを付けて選択してください。

「+」記号は、そのフォルダにサブフォルダが含まれており、それらは処理対象外となるため、暗号化状態が確認されないことを示しています。

プロファイル規則をクリックすると、ユーザーのプロファイルに暗号化規則が含まれるすべてのディレクトリが自動的に選択されます。

特定のファイルタイプのみを検証対象に制限するには、詳細設定をクリックしてください。

- 以下のファイル形式のみを含める: ここで特定のファイル形式（例：.txt、.docx、.pdf）を指定すると、指定された形式のファイルのみがチェック対象となります。フォルダ内に指定されていない形式のファイルが含まれている場合、それらは考慮されません。複数のファイル形式を指定する場合は、セミコロンで区切ったリストを使用してください。

ステップ6： 次へをクリックしてください。

ステップ3／5において、各ファイルごとに検証の結果、使用されたキーのキー名、および暗号化アルゴリズムが表示されます。

列見出しをクリックすると、結果をアルファベット順に並べ替えることができます。

ステータスレポートを保存するには、エクスポートをクリックし、お好みのファイル保存先でXMLファイルとして保存してください。

ステップ7： 完了をクリックしてください。ウィザードが閉じられます。

ファイルの復号

u.trust LAN Crypt で暗号化されたファイルは、適用される暗号化ルールが一切存在しなくなった場合に復号が可能です。例えばユーザーのプロファイルにおける暗号化ルールの変更により、初期暗号化を再度実行する必要が生じた場合、暗号化ルールが消滅したファイルは本ウィザードを通じて復号できます。

ファイルを復号するには

1. ウィザードのステップ1/5で、初期暗号化を実行するを選択してください。
2. ステップ2/5の復号で、選択したキーでファイルを復号を選択してください。
3. その後、キーを選択いただけます。

選択されたキーで暗号化されたファイルのみが復号されます。ただし、それらのファイルに適用される暗号化ルールが一切存在しなくなった場合に限り、復号が行われます。

ご注意

- *u.trust LAN Crypt* は、暗号化ルールが適用されていないファイルのみを復号します。

例： ユーザープロファイルが変更されたため、初期暗号化ウィザードが起動されます。初期暗号化ウィザードを終了した後、すべてのファイルが意図した暗号化状態になるようにするには、以下の手順に従ってください。

1. プロファイルに従ってファイルを暗号化**:** を有効にします。これにより、すべてのファイルが新しい暗号化設定に従って暗号化されます。
2. プロファイルに従ってファイルを再暗号化**:** ファイルが新しいルールに従って異なるキーで暗号化される必要がある場合、再暗号化されます。
3. 選択したキーでファイルを復号を有効にし、その後すべてのキーを選択してください。暗号化ルールが一切存在しなくなった暗号化ファイルは復号されます。*u.trust LAN Crypt*は暗号化ルールが存在しないファイルのみを復号します。したがって、すべてのキーを選択しても問題が生じることはありません。

この処理を正常に完了しウィザードを閉じると、すべてのファイルが正しい暗号化状態になります。

永続的暗号化が有効になっている場合、ファイルを明示的に復号することが重要となる場合があります。この場合、暗号化ルールが適用されているディレクトリから暗号化ルールの適用されていないディレクトリへファイルをコピーまたは移動しても、ファイルは自動的に復号されません。

無人モードでの初期暗号化

lcinit.exeツールを無人モードで実行したい場合は、そのツールが配置されているフォルダ（例：`C:\Program Files\Utimaco\u.trust LAN Crypt\Apps\`）から、特定のパラメータを指定してコマンドライン経由で**lcinit.exe**を呼び出す必要があります。

コマンドライン構文：

``` LCInit <開始パス ｜ %Profile>[/S] {-DIgnoreDirectory}[/Tv][/Te][/Tr][/Td] [/Tdk {GUID}][/Dc][/De][/Dm][+FFiletype][/V1|/V2|/V3|/V4] [/X] [/Lログファイル] LCInit <開始パス ｜ %Profile

パラメータ：

開始パス

これにより、暗号化、復号、または再暗号化の対象となる単一ファイル（例：`C:\Data\sales.docx`）またはフォルダ（例：`D:\Data`）が生成されます。デフォルト設定では、サブフォルダはこの処理に含まれません。

**%Profile**

読み込まれた暗号化プロファイル内の絶対パスを持つすべてのルールを処理します。必要に応じてファイルの暗号化／復号または再暗号化を行います。
```

ご注意

- ファイルを復号する前に、プロファイルにそのファイルに対する除外ルールが含まれている必要があります。

/s

開始パスからすべてのサブフォルダを含みます。

/h または /?

lcinit.exeで使用される構文に関するヘルプを表示するウィンドウを開きます。

-DIgnoreDirectory 指定されたディレクトリを無視します。

このフォルダを無視します。

/Tv

タスクモード: v = ファイルの暗号化状態を表示します。

/Te

タスクモード: e = 必要に応じて、暗号化プロファイルに従ってファイルを暗号化します。

/Tr /Tr

タスクモード: r = 必要に応じて、暗号化プロファイルに従ってファイルを再暗号化します。

/Td /Td

タスクモード: d = 必要に応じて、暗号化プロファイルに従ってファイルを復号します。

/Tdk /Tdk

タスクモード: dk= 事前定義されたキーを使用して暗号化されたファイルを復号します。キーのGUIDを入力する必要があります。

注記

- すべてのタスクモードパラメータは、1回のコマンド呼び出しで同時に使用できます。

/Dc

このオプションは、NTFS圧縮ファイルを解凍し、その後暗号化します。このオプションが設定されていない場合、NTFS圧縮ファイルは無視されます。

/De

このオプションは、EFSで暗号化されたファイルを復号し、その後再度暗号化します。このオプションが設定されていない場合、EFSで暗号化されたファイルは無視されます。

/Dm

このオプションは、複数のキーで暗号化されたファイルを復号し、その後再度暗号化します。その結果、ファイルは一つのキーのみで暗号化されます。

+Fファイルタイプ **+F**ファイルタイプ

このオプションでファイルタイプを指定した場合（例：+Ftxt+Fdocx）、該当するタイプのファイルのみが処理されます。この設定は、暗号化ルールが存在するファイルにのみ影響します。

フォルダ内に、このオプションで指定されていない異なるファイル形式のファイルが含まれている場合、それらのファイルは初期暗号化の対象とはなりません。ユーザーがそれらを開いて保存した際にのみ暗号化されます。

例： 上記の例では、ファイル「*123.pdf*」は暗号化されません。この理由は、初期暗号化において「PDF」形式のファイルは暗号化対象外とされているためです。ユーザーがこのファイルを、例えばPDFエディタで開いて同じフォルダに保存した場合、そのファイルは暗号化されます。また、ユーザーがそのようなファイルをこのフォルダからコピーし、その後再び同じフォルダにコピーした場合も、ファイルは暗号化されます。ただし、これはフォルダに定義された暗号化ルールが「PDF」形式のファイルにも適用される場合にのみ可能です。

/V0

詳細モード 0: 報告なし。

/V1 詳細モード 0: 報告なし。

詳細モード 1: エラーメッセージを表示します。

/V2 詳細モード 1: エラーメッセージを一覧表示します。

詳細モード 2: 変更されたファイルを一覧表示します。

/V3 /V3

詳細モード 3: すべてのファイルを一覧表示します。

/V4 /V4

詳細モード 4: プレーンファイルを一覧表示します。

/E /E

エラー発生時に停止します。 エラー発生時に停止します。

/X エラー発生時に停止します。

ウィンドウを表示せずに初期暗号化を行います。

/LLogfile /LLogfile

指定されたファイルに出力を書き込みます。

ご注意

- /Td パラメータは、復号対象のファイルがプロファイル内の除外ルールで指定されている場合にのみ、%Profile と組み合わせて使用してください。それ以外の場合は、開始パスと共に /Td を使用する必要があります。

```
lcinit.exe %PROFILE -DC:\ignore /S /Te /Tdk {1234ABCD-1234-1234-1234-1234ABCD}
{5678EFGH-5678-5678-5678-5678EFGH} /V1 /LC:\logfile.xml> lcinit.exe %PROFILE -DC:
\ignore /S /Te /Tdk {1234ABCD-1234-1234-1234-1234ABCD}
{5678EFGH-5678-5678-5678-5678EFGH} /V1 /LC:\logfile.xml> lcinit.exe %PROFILE -DC:
\ignore /S /Te /Tdk {1234ABCD-1234-1234-1234-1234ABCD}
{5678EFGH-5678-5678-5678-5678EFGH} /V1 /LC:\logfile.xml>
```

```
lcinit.exe D:\data /S /V4 lcinit.exe D:\data /S /V4 lcinit.exe D:\data /S /V4
```

D:\data およびそのサブフォルダ内のすべてのプレーンテキストファイルを一覧表示します。

ポリシー

証明書

ユーザーが暗号化プロファイルにアクセスするには、対応する証明書がコンピュータ上に存在している必要があります。セキュリティオフィサーがこれらの証明書をユーザーに配布します。ユーザーはその後、自身のマシンに証明書をインポートします。初回ログイン時に証明書が利用可能な場合、このプロセス全体はユーザーの操作を必要とせずに実行されます。

u.trust LAN Crypt には、暗号化プロファイルが初めて読み込まれる際に証明書を自動的にインポートするオプションがございます。この場合、セキュリティオフィサーはシステムを設定し、*u.trust LAN Crypt* がログオン時に証明書ファイルを検出し、自動的にインポートを開始できるようにいたします。ユーザーには、PKCS#12 キーファイルの PIN を入力するよう一度だけプロンプトが表示されます。

ご注意

- 証明書を自動的にインポートするために必要なPINの配布は、（マスター）セキュリティオフィサーの責任となります。

暗号化プロファイルが読み込まれるたびに証明書が確認されます。有効な証明書が見つかった場合、ユーザーは*u.trust LAN Crypt*にログインできます。有効な証明書が見つからない場合、ユーザーは暗号化されたデータを操作できません。

ご注意 ユーザーが*u.trust LAN Crypt*へのログオンを試み、ログオンに失敗した場合、ログオンできなかった理由を説明するエラーメッセージが表示されます。

*u.trust LAN Crypt*の暗号化プロファイルに含まれる特別な暗号化ルールにより、ユーザーは暗号化されたデータにアクセスできます。これらのルールは、特定のディレクトリ内のどのファイルが各キーで暗号化されるべきかを正確に定義します。ユーザーの暗号化プロファイルは読み込まれるだけで、暗号化と復号はバックグラウンドで（透過的に）行われます。

ユーザーは、暗号化／復号処理が行われていることに気付くことはありません。

ご注意

- CA証明書は、「信頼されたルート認証機関」の証明書ストアに保存されている場合にのみ、正しいものとして受け入れられます。*u.trust LAN Crypt*は、PKCS#12キーファイルに含まれる可能性のあるCA証明書を、ユーザー証明書とともに「My Certificates-Certificates」フォルダにインポートします。エラーメッセージを回避するためには、証明書ストア内のCA証明書を手動で「信頼されたルート認証機関」に移動する必要があります。*u.trust LAN Crypt*で生成された証明書をご利用の場合は、この手順は不要です。

ポリシーファイルの読み込み

u.trust LAN Crypt のデフォルト動作

ユーザーが Windows にログオンすると、まずキャッシュされたプロファイルが読み込まれます。*u.trust LAN Crypt* は、ポリシーファイルの指定された場所（ネットワークドライブまたは Web サーバー）への接続を確立し、ユーザー向けの新しいポリシーファイルが利用可能かどうかを確認します。新しいポリシーファイルが見つかった場合、キャッシュされたユーザープロファイルが更新されます。

ユーザーは、*u.trust LAN Crypt* が新しいバージョンのポリシーファイルの存在を確認している間も、暗号化されたファイルの操作を開始できます。指定された場所がアクセスできない場合、ユーザーは更新が可能な状態になるまでキャッシュされたユーザープロファイルを使用して作業を続けます。

注記

- *u.trust LAN Crypt* は、ユーザーおよび（マスター）セキュリティオフィサーの証明書を検証します。証明書に CRL 配布ポイントが含まれており、システムに有効な CRL が存在しない場合、Windows は指定されたアドレスから CRL をインポートしようと試みます。ファイアウォールがインストールされている場合、プログラム（*loadprof.exe*）がインターネットへの接続を確立しようとしているというメッセージが表示されることがあります。また、ユーザープロファイルのダウンロードが原因でこのメッセージが表示される場合もございます。

セキュリティオフィサーが定義する動作

セキュリティオフィサーは、中央設定を使用してデフォルトの動作を変更できます。セキュリティオフィサーは、クライアントコンピュータ上でキャッシュされたポリシーが有効な期間を指定できます。また、ポリシーファイルの更新間隔を定義できます。セキュリティオフィサーによって定義された設定は、クライアントステータスダイアログのプロファイルタブに表示されます。詳細はクライアントステータスダイアログをご参照ください。

ここで定義された期間内は、ポリシーファイルがクライアント上で有効であり、ポリシーファイルの保存場所への接続がなくても、ユーザーは暗号化されたデータにアクセスできます。

指定された期間が満了すると、*u.trust LAN Crypt* はネットワークドライブからポリシーファイルを読み込み、更新を試みます。これが不可能な場合、ポリシーファイルはアンロードされます。ユーザーは暗号化されたデータにアクセスできなくなります。

有効なポリシーファイルが利用可能になった場合（例えば、ポリシーファイルのクライアント場所への接続状態での次回ログオン時など）、ポリシーファイルは更新され、再度読み込まれます。ユーザーは暗号化されたデータに再びアクセスできるようになります。キャッシュ保存期間のカウンターはリセットされます。

キャッシュ保存期間を指定することにより、セキュリティオフィサーはクライアントコンピュータに定期的に最新のポリシーファイルが提供され、ユーザーが常に最新のポリシーを使用することを保証できます。ユーザーが同一のポリシーファイルを無制限の期間使用することを防止できます。なお、このオプションが未設定に設定されている場合、ユーザーはキャッシュされたポリシーファイルのバージョンを無制限の期間使用し続けることが可能です。

キャッシュ保存の許可期間のカウンターは、以下の状況でリセットされます。

- ポリシーファイルの保存場所がアクセス可能であり、有効なポリシーファイルがクライアントに転送された場合（例：ユーザーログオン時、または指定された更新間隔によってトリガーされた場合）。ただし、既存のファイルと比較して新しいファイルではない場合。
- ポリシーファイルの保存場所がアクセス可能であり、有効なポリシーファイルがクライアントに転送された場合（例：ユーザーログオン時、または指定された更新間隔によってトリガーされた場合）、ただし、そのポリシーファイルが既存のものと比べて新規ではない場合。
- 新しいポリシーファイルが利用可能であり、正常に読み込まれました。

キャッシュ保存の許可期間のカウンターは、以下の状況ではリセットされません。

- クライアントコンピュータが新しいポリシーファイルを受信しようとしますが、ポリシーファイルの保存場所がアクセスできない場合。
- クライアントコンピュータが新しいポリシーファイルの受信を試みる場合。ただし、ポリシーファイルの保存場所がアクセスできない場合。
- 新しいポリシーファイルが転送されました。しかし、エラーのため読み込むことができませんでした。
- 新しいポリシーファイルが利用可能です。ただし、新しい証明書が必要です。ユーザーはこの証明書をお持ちでないか、または読み込めません。

ポリシーファイルの更新に失敗した場合、キャッシュされたポリシーファイルの有効期限がクライアントコンピュータのバルーンツールチップに表示されます。ユーザーはその後、*u.trust LAN Crypt* トレイアイコンから手動更新を開始できます。詳細はユーザーメニューをご参照ください。

ポリシーファイルはキャッシュされません

セキュリティオフィサーは、ポリシーファイルをキャッシュしないよう設定できます。これにより、ポリシーファイルの保存場所がアクセス可能な場合、ユーザーはログオン時にプロファイルを取得します。ファイルがアクセス不可の場合、またはプロファイル読み込み時にエラーが発生した場合、ユーザーは暗号化されたファイルにアクセスできません。

u.trust LAN Crypt へのログイン

*u.trust LAN Crypt*の暗号化プロファイルは、セキュリティオフィサーが会社のセキュリティポリシーに従って作成し、ポリシーファイルに保存されます。暗号化プロファイルは、ユーザーが対応する証明書を所有している場合にのみ読み込まれます。

ポリシーファイルのパスは、システム管理者またはセキュリティオフィサーにより、クライアントマシンのレジストリに記述されます。これは*u.trust LAN Crypt*のグループポリシーを通じて行われます。ユーザーが*u.trust LAN Crypt*にログオンすると、ポリシーファイルに保存されている暗号化プロファイルがクライアントマシンに読み込ま

れます。*u.trust LAN Crypt*クライアントは、定義された場所（例：ネットワーク共有）からポリシーファイルを読み込み、ユーザーの証明書を確認することで、そのプロファイルを読み込む権限があるかどうかを検証します。

トークンを使用したログオン

ユーザーはトークンを使用して*u.trust LAN Crypt*にログオンすることも可能です。このログオン方法の前提条件として、ユーザーの*u.trust LAN Crypt*ユーザー証明書がトークンに保存されている必要があります。システムに接続されたトークン上でユーザー証明書が検出された場合、ユーザーはログオンされます。

トークンを使用したログイン時、*u.trust LAN Crypt* はオペレーティングシステムがトークンを識別する前にポリシーファイルの読み込みを試行する場合があります。この場合、トークンがシステムに接続されているにもかかわらず、ユーザー証明書が見つからない旨のメッセージが表示されることがあります。

ユーザーは、ツールバーのユーザーアプリケーションから手動でポリシーファイルを読み込む必要があります -> 暗号化ルールを読み込む。これによりトークンが識別され、ユーザーはログインできます。この現象を回避するには、設定でプロファイル読み込みの遅延時間を指定できます（プロファイル読み込み時の遅延設定）。

ユーザーアプリケーション

u.trust LAN Crypt の状態は、Windows タスクバー上のキーアイコンで表示されます。

緑色： 暗号化ルールが読み込まれ、透過暗号化が有効になっています。

黄色: 暗号化ルールは読み込まれていますが、透過的暗号化は無効化されています。 緑色： 暗号化ルールが読み込まれ、透過的暗号化が有効化されています。

赤: プロファイルが読み込まれていません。

ユーザーメニュー

キーアイコンを右クリックすると、*u.trust LAN Crypt* ユーザーメニューが開き、以下のオプションが提供されます。

- 暗号化ルールを読み込み / 暗号化ルールを更新
- 暗号化ルールの読み込み / 暗号化ルールの更新
- 暗号化ルールをクリアする
- 暗号化ルールの読み込み / 暗号化ルールの更新
- 暗号化の無効化／有効化
- 暗号化ルールの明確化
- プロフィールを表示する
- 暗号化の無効化 / 有効化
- クライアントステータス
- プロフィールを表示
- 初期暗号化
- クライアントの状態
- 閉じる
- 初期暗号化
- 概要について
- 閉じる

  ご注意

  - ご利用可能なメニューコマンドは、*u.trust LAN Crypt* クライアントの設定によって異なります。セキュリティオフィサーが設定を一元的に管理いたします。

暗号化ルールの読み込み/暗号化ルールの更新

このオプションは、現在有効な暗号化ルールを読み込みます。プロファイルが実行中に変更された場合に重要です。

暗号化ルールをクリアする

このオプションは、暗号化されたデータへのアクセスを防止します。これは、ワークステーションが無人状態のときに、暗号化されたデータを不正アクセスから保護するセキュリティオプションです。秘密キーの使用にはパスワードによる保護が必要です。そうしないと、暗号化ルールを読み込むコマンドを使用してプロファイルが再読み込みされる可能性があります。

暗号化の無効化 / 有効化

透過的な暗号化の有効化と無効化を切り替えます。暗号化を無効化するのは、ファイルを暗号化ルールが適用されないフォルダに移動またはコピーした場合でも、ファイルを暗号化したままにしておく場合に使用します。暗号化が有効な状態では、この種のフォルダにコピーされるとファイルは復号されます。

例えば、暗号化されたファイルを電子メールに添付した場合、透過的暗号化が有効であれば自動的に復号されます。透過的暗号化が無効の場合、暗号化されたファイルを電子メールの添付ファイルとして送信することが可能です。

ご注意

- システム管理者が永続的暗号化機能を有効にしている場合、暗号化されたファイルは、暗号化ルールが設定されていない場所にコピーまたは移動されても、暗号化された状態を維持します。

プロファイルを表示 暗号化情報に含まれる暗号化ルールとキーを、2つのタブで表示します。

有効な暗号化ルール タブには、ログイン中のユーザーに対して有効なルールの概要が表示されます。さらに、ユーザーには以下のオプションが利用可能です。無視ルールを表示、除外ルールを表示、暗号化タグを表示、バイパスルールを表示。

利用可能なキータブページには、現在のユーザーが利用可能なすべてのキーが一覧表示されます。

クライアントステータス

クライアント状態オプションでは、複数のタブを使用して*u.trust LAN Crypt*クライアントの現在の状態に関する詳細情報を表示します。詳細はクライアント状態をご覧ください。

初期暗号化

読み込まれた暗号化プロファイルを使用してすべてのファイルを暗号化するウィザードを開始します。詳細は初期暗号化と明示的暗号化をご参照ください。

閉じる 閉じる

u.trust LAN Crypt ユーザーアプリケーションを終了します。

概要

現在お使いの *u.trust LAN Crypt* のバージョンに関する情報を表示します。

ご注意

- 閉じる オプションは、*u.trust LAN Crypt* ユーザーアプリケーションのみを終了させます。*u.trust LAN Crypt* は現在の状態を維持します。これは、透過的な暗号化/復号が継続されることを意味します。ユーザーアプリケーションを閉じても、ファイルが不正アクセスから保護されるわけではありません（例：ワークステーションを離れる場合など）。

クライアント状態ダイアログ

クライアント状態オプションでは、ユーザーのマシンの暗号化設定に関する情報を提供する複数のタブが表示されます。

具体的には以下の通りです。

ステータス

このタブでは、ユーザープロファイルが読み込まれているか、暗号化が有効になっているかを確認できます。また、ポリシーファイルに関する詳細情報（作成日、ファイルを作成したセキュリティオフィサーなど）も表示されます。

ユーザープロファイルが読み込まれている場合、暗号化も有効になります。ただし、ユーザープロファイルが読み込まれている状態でも、暗号化を（一時的に）無効にすることが可能です。詳細は「ユーザーメニュー、コマンド暗号化の無効化/有効化」をご参照ください。

設定 このタブでは、現在クライアントに適用されている設定に関する情報を提供します。これらの設定は中央で定義され、暗号化、システムトレイアイコン、および初期暗号化ウィザードの設定を指します。このタブでは、永続的暗号化が有効化されているかどうかや、クライアントコンピューターで利用可能なメニューオプションなど、その他の詳細も表示されます。

プロファイル このタブでは、ユーザープロファイルの設定が表示されます。

証明書 このタブでは、ユーザー証明書の詳細（発行者、シリアル番号、有効期間）と、証明書検証に適用されるクライアントのルールが表示されます。

キー このタブでは、現在読み込まれているプロファイルで使用可能なすべてのキーに関する情報が表示されます。

ルール このタブには、現在のユーザーに適用されるすべての暗号化ルールが一覧表示されます。

未処理 このタブでは、未処理のアプリケーション、ディスクドライブ、およびデバイスに関する情報を提供します。また、現在のユーザーのアクティブな無視ルールとバイパスルールも一覧表示します。

u.trust LAN Crypt は、特定のアプリケーションをデフォルトで「未処理アプリケーション」として扱います。これらのアプリケーションも本タブに表示されます。

アプリケーション このタブには、動作特性により *u.trust LAN Crypt* による特別な対応が必要なプログラムが表示されます。

ウイルス対策ソフトウェア

暗号化されたファイルをスキャンするには、アンチウイルスソフトウェアはファイルの暗号化に使用されたキーを必要とします。このタブでセキュリティオフィサーが指定したアンチウイルスソフトウェアは、すべてのキーにアクセスできるため、暗号化されたファイルもチェックすることが可能です。

クライアント**API** このタブでは、クライアント API の設定が表示され、その使用が許可されているすべてのアプリケーションが一覧表示されます。

信頼済みベンダー クライアントAPIへのアクセスを信頼できるベンダーによって署名されたアプリケーションに制限する場合、これらのベンダーは*u.trust LAN Crypt*管理画面に登録する必要があります。登録済みの信頼できるベンダーと対応する証明書情報は、このタブに一覧表示されます。

エクスポートボタン

現在のクライアント設定をXMLファイルにエクスポートするには、エクスポートボタンをご利用ください。これにより、サポートチームに重要な設定情報を容易にご提供いただけます。

Explorer拡張機能

u.trust LAN Crypt エクスプローラー拡張機能では、以下の機能を提供しています。

- プロファイルに基づく暗号化（ファイル、フォルダー、ドライブ）
- プロファイルに基づく暗号化（ファイル、フォルダ、ドライブ）
- ファイル、フォルダ、ドライブの明示的な暗号化および復号
- プロファイルに基づく暗号化（ファイル、フォルダ、ドライブ）
- データの暗号化状態を簡単に管理できます。
- お客様のデータの暗号化状態を簡単に管理できます。
- ファイル、フォルダ、ドライブの明示的な暗号化と復号

u.trust LAN Crypt は、Windows エクスプローラーにメニューオプションを追加します。これらは、ドライブ、フォルダー、ファイルのコンテキストメニューに表示されます。さらに、ファイルのプロパティウィンドウに新しいタブが追加されます。この新しいタブには、暗号化ステータスに関する情報が表示されます。

ファイルまたはフォルダーを右クリックすると、コンテキストメニューに**u.trust LAN Crypt**の項目が表示されます。異なる色のキーがファイルの暗号化状態を示します。 *u.trust LAN Crypt* は、Windows エクスプローラーにメニューオプションを追加します。これらは、ドライブ、フォルダー、ファイルのコンテキストメニューに表示されます。さらに、ファイルのプロパティウィンドウに新しいタブが追加されます。この新しいタブには、暗号化状態に関する情報が表示されます。

緑色のキー： ファイルは暗号化されており、ユーザーはキーにアクセスできます。

赤キー: ファイルは暗号化されており、ユーザーはキーにアクセスできません。

灰色のキー： 灰色のキーは、ファイルが平文（暗号化されていない）であることを示しますが、読み込まれたプロファイル内の暗号化ルールに従って暗号化されるべきです。

黄色のキー: 黄色のキーが表示されている場合、ファイルは暗号化されていますが、透過的な暗号化が現在無効化されています。

疑問符付きの黄色のキー： ユーザーに十分なアクセス権限がないため、*u.trust LAN Crypt* は暗号化状態を確認できません。

ご注意

- オフライン属性が設定されているファイル（物理的に存在しないファイルなど）には、キー記号は表示されません。
- Windows エクスプローラー内のファイルにもキー記号が表示されます。ドライブ全体やフォルダー全体に暗号化ルールが適用されている場合、それらもキー記号でマークされます。そこでは、異なる色のキー記号が暗号化状態を示します。

フォルダ用メニューオプション

暗号化状態 暗号化状態

このオプションでは、このフォルダ内の全ファイルとその暗号化状態（色分けされたキーアイコン）が表示されます。表示されるのは最上位フォルダ内のファイルのみです。サブフォルダ内のファイルを表示するには、まずそのサブフォルダに移動してください。エクスプローラーでは、暗号化ルールが設定されているフォルダはキーアイコンで識別できます。

プロファイルに基づいて暗号化

このオプションは、読み込まれた暗号化プロファイルに従ってフォルダ内のすべてのファイルを暗号化します。既存の暗号化ルールが設定されているサブフォルダも暗号化の対象となります。進行状況バーにより、初期暗号化にかかるおおよその所要時間が表示されます。また、フォルダ内のファイル総数と、既に暗号化が完了したファイルの数も確認できます。さらに、現在暗号化処理中のファイルのパスも表示されます。

暗号化

このオプションは、アクティブな暗号化プロファイルで利用可能なキーを使用して、フォルダ内のすべてのファイルを暗号化します。利用可能なキーの一覧が表示され、そこからすべてのファイルを暗号化する際に使用するキーを選択することができます。

ご注意

- フォルダ内のファイルに対して暗号化ルールが存在し、それらのファイルがすべて（既に）そのルールに従って暗号化されていない場合、ディレクトリまたはフォルダを選択し、暗号化オプションを選択した後に暗号化を行うと、エラーメッセージが表示される可能性があります。

例： フォルダ内の少なくとも1つのファイルに「Key-1」などの暗号化ルールが設定されている状態で、そのフォルダを選択し、暗号化オプションから別のキー（例：「Key-2」）を選択して**OK**をクリックします。

ご注意

- 既に暗号化ルールが設定されているフォルダについては、代わりに「プロファイルに基づいて暗号化」オプションを使用して暗号化してください。あるいは、*u.trust LAN Crypt* ユーザーメニューの 初期暗号化 を使用してファイルを暗号化することも可能です。

復号

このオプションは、最初のフォルダレベルにあるすべてのファイルを復号します。そのため、関連するすべてのキーがアクティブな暗号化プロファイルで利用可能である必要があります。キーが欠けている場合、そのキーを使用しているファイルは暗号化されたままとなります。

セキュア移動

u.trust LAN Crypt を使用してフォルダを移動する際、そのフォルダ内のファイルは、適用される暗号化ルールに従い、新しい場所で暗号化、復号、または再暗号化されます。元のファイルは移動後に消去されます。

セキュア削除

このオプションは、ファイルの保存場所を複数回上書きします。これにより、ファイルはWindowsのごみ箱から復元できなくなります。

個々のファイルに対するメニューオプション

暗号化状態 暗号化状態

このオプションは、ファイルの暗号化状態を表示します。暗号化されたファイルの場合、ポップアップ情報ボックスに、暗号化に使用されたキーと、ユーザーがこのキーを使用する権限があるかどうかに関する追加情報が表示されます。

別のユーザーがログオンしている場合で、そのユーザーがこのキーを使用する権限がない場合、情報ボックスにはキー名の代わりにGUIDが表示されます。

暗号化されたファイルは、エクスプローラー上でファイル名の横に表示される小さな緑色のキーアイコンで識別できます。ユーザーがフォルダオプション -> 表示 をクリックすると、自身のプロファイルに対してファイルの暗号化状態およびフォルダの暗号化状態を表示するかどうかを指定できます。これらの設定変更は、ログオフしてから再度ログオンするまで有効になりません。

プロファイルに基づいて暗号化

このオプションは、現在読み込まれている暗号化プロファイルに従ってファイルを暗号化します。この項目は、ファイルの暗号化状態が暗号化プロファイルと一致しない場合にのみ、コンテキストメニューに表示されます。

暗号化

このオプションは、選択されたファイルを暗号化いたします。利用可能な暗号化キーの一覧が表示されますので、暗号化に使用するキーをお選びいただけます。

ご注意

- ドライブまたはフォルダ内のファイルに対して暗号化ルールが存在し、すべてのファイルが（既に）そのルールに従って暗号化されていない場合、複数のファイルを選択し「暗号化」オプションを選択した後に、暗号化中にエラーメッセージが表示される可能性があります。

例： フォルダ内の少なくとも1つのファイルに「Key-1」などの暗号化ルールが設定されている状態で、そのフォルダを選択します。次に、別のキー（例：「Key-2」）を「暗号化」オプションで選択し、**OK**をクリックします。

ご注意

- 既に暗号化ルールが設定されているフォルダについては、代わりに「プロファイルに基づいて暗号化」オプションを使用して暗号化してください。あるいは、*u.trust LAN Crypt* ユーザーメニューの 初期暗号化 を使用してファイルを暗号化することも可能です。

復号

このオプションは、選択されたファイルを復号します。アクティブな暗号化プロファイルに正しいキーが設定されている必要があります。そうでない場合、ファイルは暗号化されたままとなります。

セキュア移動

このオプションは、ファイルを新しい場所に移動する際に、読み込まれた暗号化ルールに従って選択されたファイルを暗号化、復号、または再暗号化いたします。選択された元のファイルは、移動後に削除されます。

セキュア削除

このオプションは、選択されたファイルの保存領域を複数回上書きします。このファイルは、Windowsのごみ箱から復元することはできません。

ご注意

- アクティブな暗号化ルールは常に優先されます。ユーザーが、暗号化ルールで異なる設定が定義されているファイルの暗号化/復号を試みた場合、そのコマンドは実行されず、エラーメッセージが表示されます。

メニューオプションを使用してファイルを暗号化しようとする際に、以下の状況ではエラーメッセージが表示されます。

- フォルダ内に、不明なキーで暗号化されたファイルが含まれている場合。
- フォルダ内に、不明なキーで暗号化されたファイルが含まれている場合。

- ユーザーが、暗号化ルールに反する形でファイルの暗号化/復号を試みている場合（例：暗号化ルールで使用されたものとは異なるキーが選択されている場合）。

暗号化情報

プロパティ ダイアログの暗号化状態タブでは、暗号化されたファイルに関する情報が表示されます。

ターミナルサーバー

本バージョンの*u.trust LAN Crypt*は、Windows ターミナル サーバーおよびCitrix ターミナル サーバーに対応しています。対応バージョンに関する詳細は、*u.trust LAN Crypt*のリリースノートをご参照ください。

ターミナルサーバー環境でのインストール

LAN Crypt クライアントのターミナルサーバーへのインストールは、基本的に通常の Windows システムと同様です。しかし、RemoteApp 環境（アプリケーション仮想化）で使用する場合、**LoadProf** がセッション全体ではなく RemoteApp のコンテキスト内だけで実行されるよう、追加の手順が必要となります。インストールの前後で次の 2 つの対策を行う必要があります。

セットアップ前の準備

インストールパッケージを開始する前に、既存の *loadprof.exe* の登録を削除する必要があります。
レジストリエディタを開き、次のキー内のエントリを削除してください：

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Appsetup
```

この値に *loadprof.exe* が含まれている場合は、完全に削除してください。

Transform ファイル（.**mst**）を使用したインストール

インストールパッケージを実行する際、Transform ファイル（.mst）を適用する必要があります。

この Transform ファイル内で、プライベートプロパティ **TerminalServer** を **1** に設定し、ターミナルサーバーモードで正しくインストールされるようにします。

Transform ファイルを使用したインストールコマンドの例：

```
msiexec /i LCClient.msi /qn <その他のパラメータ> TRANSFORMS="C:\Transform_File.mst"
```

この構成により、RemoteApp シナリオにおける正しい起動動作が保証されます。

ターミナルサーバー環境でのインストール

一般的に、インストール手順は非ターミナルサーバー環境と同様です（詳細は「インストールとアップグレード」セクションをご参照ください）。以前のバージョンの*LAN Crypt*とは異なり、特別な「ターミナルサーバー」版をインストールする必要はなくなりました。

ご注意

- ターミナルサーバーにインストールする場合は、管理者権限を持つローカルログオンセッションを使用して *u.trust LAN Crypt* をインストールしてください。
- Citrix Presentation Server または Citrix XenApp をご利用になる場合は、*u.trust LAN Crypt* のインストール前にこれらをインストールしてください。

制限事項

Citrix

- Citrixクライアントドライブリダイレクトとの組み合わせによる暗号化はサポートされていません。
- Citrix ストリーミングアプリケーションはサポートされていません。
- 暗号化とCitrixクライアントドライブリダイレクトの併用はサポートされていません。

インストールとアップグレード

ご注意

- LAN Crypt は、Windows の管理者権限でのみインストールが可能です。最新の LAN Crypt バージョンへアップグレードする前に、LAN Crypt クライアントをバージョン 4.2.1 へ、LAN Crypt 管理ツールをバージョン 4.2.0 へアップグレードすることをお勧めいたします。ユーザーのプロファイルファイルは、**xml.bz2** 形式である必要がございます。これは、LAN Crypt バージョン 4.0.0 以降がこの形式のみをサポートしているためです。

ご注意 *u.trust LAN Crypt* の両コンポーネント、すなわち管理コンソールとクライアントアプリケーションを同一のコンピューターにインストールされる場合、両方のバージョンが同一である必要があります。

手順 **1:** 解凍したインストールパッケージ内の *u.trust LAN Crypt* インストールフォルダにある **LCClient.msi** ファイルのいずれかをダブルクリックしてください。

ステップ2： 次へをクリックしてください。

ライセンス契約のダイアログが表示されます。

ステップ3： ライセンス契約 ダイアログで、ライセンス契約に同意します を選択してください。そうしないと、*u.trust LAN Crypt* をインストールすることはできません！

ステップ4： 次へをクリックしてください。

保存先フォルダ ダイアログが表示されます。

ステップ5： *u.trust LAN Crypt* をインストールする場所を選択してください。

ステップ6： 次へをクリックしてください。

インストール タイプの選択 ダイアログが表示されます。

ステップ 7: このダイアログでは、*u.trust LAN Crypt* クライアントのどのコンポーネントをインストールするかを選択します。

- 標準: *u.trust LAN Crypt* クライアントで最も一般的に使用されるアプリケーション機能をインストールします。
- 標準：*u.trust LAN Crypt* クライアントの最も一般的なアプリケーション機能をインストールします。
- 完全版: クライアントAPIを含む、完全なクライアントインストールを行います。
- 完全版: クライアントAPIを含む完全なクライアントインストールを行います。
- カスタム: ユーザーが異なるコンポーネントを選択できます。
- カスタム：ユーザーが異なるコンポーネントを選択できるようにします。
- 完全版: クライアントAPIを含むクライアントの完全なインストール。

ステップ8： カスタム を選択し、次へ をクリックしてください。

以下のコンポーネントをインストールできます。

ユーザーアプリケーション

u.trust LAN Crypt ユーザーアプリケーションをインストールします。詳細はユーザーアプリケーションをご参照ください。

ご注意

- u.trust LAN Crypt* クライアントのバージョン 3.97 と比較して、ユーザーアプリケーションのインストールは除外できません。いずれの場合もインストールされます。

シェル拡張機能

u.trust LAN Crypt エクスプローラー拡張機能をインストールします。

u.trust LAN Crypt は、Windows エクスプローラーに項目を追加し、ファイルやフォルダーの初期暗号化、ファイルやフォルダーの明示的な暗号化/復号を可能にし、データの暗号化状態を簡単に確認できるようにします。これらの項目は、ドライブ、フォルダー、ファイルのコンテキストメニューに表示されます。さらに、*Windows* プロパティ ページに 暗号化情報 タブが追加されます。

クライアント**API**

Utimaco ファイル暗号化機能にAPIを通じてアクセスするために使用されます。

ご注意

- DLP製品が*u.trust LAN Crypt*クライアントAPIを使用してデータにアクセスできるようにするには、クライアントAPIをインストールする必要があります。

ネットワークフィルター

APIを通じて*Utimaco*ファイル暗号化機能にアクセスするために使用されます。

ステップ9： インストールするコンポーネントを選択し、次へをクリックしてください。

ご注意

- バージョン4.1.0以降の*u.trust LAN Crypt*では、従来のフィルタードライバーはサポートされなくなりましたのでご注意ください。すべての暗号化および復号操作は、新しくより最新で将来性のあるミニフィルタードライバー技術を通じてのみ実行されます。

ステップ10：入力内容をご確認ください。その後、次へをクリックしてインストールを開始してください。

ステップ11：インストールが正常に完了した場合、ダイアログが表示されますので、完了ボタンをクリックしてインストールプロセスを終了してください。

ご注意

- すべての設定を適用するには、コンピューターの再起動が必要です。

無人インストール

無人インストールとは、多数のコンピューターに *u.trust LAN Crypt* を自動的にインストールできることを意味します。

インストールCDのInstallディレクトリには、クライアントコンポーネントの無人インストールに必要な*.msiファイルが含まれています。

f

インストール対象コンポーネント

以下のセクションでは、インストール対象となるすべてのコンポーネントと、無人インストール時にそれらを指定する方法について説明します。

キーワード（**Courier**、**bold**）は、無人インストールを実行する際、AddLocal= 内でコンポーネントを指定する方法を表します（オプションパラメータ をご参照ください）。コンポーネント名は大文字小文字を区別します！

例：

AddLocal= **ALL** は、利用可能なすべてのコンポーネントをインストールします。

コマンドライン構文 無人インストールを実行するには、特定のパラメータを指定して **msiexec** を実行する必要があります。

必須パラメータ：

/I

インストールするパッケージを指定します。

/QN

ユーザー操作を必要としないインストール（無人セットアップ）。

.msiファイルの名前：**LCClient.msi**

構文:

```
msiexec /i \<パス¥>\LCClient.msi /qn AddLocal=\<コンポーネント1¥>,\<コンポーネント2¥>,...
```

オプションのパラメータ

```
/Lvx\* \<パス + ファイル名\> /Lvx\* \<パス + ファイル名\>
```

指定された¥<パス + ファイル名\>の場所に、インストール手順の全過程を記録します。

AddLocal=

```
AddLocal= ALL
```

利用可能なすべてのコンポーネントをインストールします。

```
AddLocal= LanCrypt
```

利用可能なコンポーネントは一切インストールされません。

```
AddLocal= UserApplication
```

u.trust LAN Crypt ユーザーアプリケーションをインストールします。

```
AddLocal= NetworkFilter
```

ネットワークアクセスのパフォーマンス向上に役立つドライバーをインストールします。

```
AddLocal= ClientAPI
```

u.trust LAN Crypt クライアント API をインストールします。これは、API を通じて *Utimaco* ファイル暗号化機能にアクセスするために使用されます。

```
AddLocal= ShellExtensions
```

u.trust LAN Crypt エクスプローラー拡張機能 をインストールします。

u.trust LAN Crypt は、Windows エクスプローラーに項目を追加し、ファイルやフォルダーの初期暗号化、ファイルやフォルダーの明示的な暗号化/復号を可能にし、データの暗号化状態を簡単に確認できるようにします。これらの項目は、ドライブ、フォルダー、ファイルのコンテキストメニューに表示されます。さらに、*Windows* のプロパティ ページに 暗号化情報 タブが追加されます。

NOOVERLAY=

（新規インストール時のみ有効で、バージョンアップ時には適用されません） **NOOVERLAY=**

```
NOOVERLAY=0
```

ファイルおよびフォルダーのオーバーレイアイコンを有効にします。

```
NOOVERLAY=1
```

ファイルおよびフォルダーのオーバーレイアイコンを無効にします。

ご注意

- インストール後、ユーザーはオーバーレイアイコンを有効にすることができます。ユーザーがフォルダオプション -> 表示をクリックすると、自身のプロファイルに対してファイルの暗号化状態およびフォルダの暗号化状態を表示するかどうかを指定できます。これらの設定変更は、ログオフしてから再度ログオンするまで有効になりません。

製品言語=

u.trust LAN Crypt クライアント用の MSI 言語パッケージを、コンピューター上の既存の言語設定に関わらず、特定の言語でインストールします。この設定された言語は、インストール自体に使用されるほか、*u.trust LAN Crypt* のセットアップウィザードによる後の変更にも使用されます。現在、インストールパラメータ「Productlanguage=」を通じて以下の言語設定がサポートされています。

`Productlanguage=1031`

u.trust LAN Crypt クライアント用のドイツ語 MSI 言語パッケージをインストールします。

`Productlanguage=1033`

u.trust LAN Crypt クライアント用の英語 MSI 言語パッケージをインストールします。

`Productlanguage=1036`

u.trust LAN Crypt クライアント用のフランス語 MSI 言語パッケージをインストールします。

RESET*CONFIGURATION*= *RESET*CONFIGURATION=

`RESET_CONFIGURATION=1`

Windows レジストリ内の既存の LAN Crypt Client 設定をすべてリセットします。これまでの設定はすべて完全に削除されます。インストール時にすべてのデフォルトのレジストリキーが作成されます。

ONEDRIVE=

`ONEDRIVE=1` **ONEDRIVE=1**

設定対象となる各ユーザーに対して、Microsoft OneDrive のサポートを有効にします。

例：

```
msiexec /i C:\Install\LCClient.msi /qn AddLocal=ALL
```

u.trust LAN Crypt の完全なインストールが実行されます。プログラムはデフォルトのインストール先ディレクトリ（¥<システムドライブ¥>:¥Program Files\Utimaco\u.trust LAN Crypt）にインストールされます。

```
msiexec /i C:\Install LCClient.msi /qn AddLocal=UserApplication,ShellExtensions
Productlanguage=1033 msiexec /i C:\Install LCClient.msi /qn
AddLocal=UserApplication,ShellExtensions Productlanguage=1033
```

u.trust LAN Crypt のインストールが実行されます。プログラムはデフォルトのインストールディレクトリ（¥<システムドライブ¥>:¥Program Files\Utimaco\u.trust LAN Crypt）に、ユーザーアプリケーション、エクスプローラー拡張機能、および英語のMSI言語パッケージと共にインストールされますが、クライアントAPIは含まれません。

「.msiファイル」は、*u.trust LAN Crypt*のインストールフォルダ内にあります。

ご注意

- パラメータ「AddLocal=」の後の行が空欄のままの場合、またはパラメータの入力が誤っている場合、インストールプログラムは中止されますのでご注意ください。

u.trust LAN Crypt クライアントの削除

u.trust LAN Crypt クライアントの削除は、Windows の管理者権限をお持ちの場合にのみ実行可能です。

スタートメニューから「設定」→「アプリ」を選択してください。アプリの一覧から「u.trust LAN Crypt Client」をダブルクリックし、「アンインストール」ボタンをクリックします。表示されるダイアログでも再度「アンインストール」ボタンをクリックしてください。これで*u.trust LAN Crypt*クライアントのアンインストールが完了します。その後、コンピューターを再起動してください。

ご注意

- 必要な *Visual C++* ランタイム ライブラリ が一部のクライアント コンピュータにインストールされていない（またはインストールが解除されている）場合があります。このコンポーネントが不足しているため、該当するコンピュータでは *u.trust LAN Crypt* をアンインストールできません。アンインストール中に表示されるエラー メッセージは、Windows インストーラー パッケージに問題があることを示しています。この場合、影響を受けるクライアント コンピュータに必要な *Visual C++* ランタイム ライブラリ をインストールする必要があります。以下のURLから入手できます。

https://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170

https://aka.ms/vs/17/release/vc_redist.x86.exe

https://aka.ms/vs/17/release/vc_redist.x64.exe

クライアントコンピュータに必要な*Visual C++*ランタイムライブラリのインストールが正常に完了しましたら、*u.trust LAN Crypt*を再度エラーなくアンインストールできるはずです。

ご注意

- u.trust LAN Crypt* クライアントを削除すると、暗号化されたファイルは復号できなくなります。

ご注意 *u.trust LAN Crypt*クライアントをアンインストールした直後に、再度インストールしないでください。再インストール前に、必ず一度以上マシンを再起動する必要があります。

ユーザー操作を伴わないアンインストール

前提条件: アンインストールが必要なMSIパッケージがシステム上に存在している必要があります。

例：

```
msiexec /X {00000000-0000-0000-0000-000000000000} /qn /norestart msiexec /X
{00000000-0000-0000-0000-000000000000} /qn /norestart
```

このコマンドは、ProductCode {00000000-0000-0000-0000-000000000000} のMSIパッケージをサイレントモードでアンインストールし、システムの再起動を防止します。

コマンドラインオプション：

/X {製品コード**}**

アンインストール対象のMSIパッケージのProductCodeです。ProductCodeはMSIファイル自体から抽出できます。

/qn

ユーザーインターフェースを表示せずに、サイレントモードでアンインストールを実行します。

/norestart 再起動を行いません。

アンインストール後のシステムの再起動を防止します。

ご注意

- MSIパッケージのプロダクトコードは、以下のコマンドで抽出できます。`msiexec /i <MSIファイル> /qn /norestart /property ProductCode`

LAN Crypt Client のカスタムエラーメッセージ

LAN Crypt Clientでは、特定のエラーメッセージに対して個別にメッセージを保存するオプションを提供しています。これにより、標準メッセージに独自の注釈を追加することが可能となります。例えば、ITサポートへの参照情報などを記載いただけます。

注記

- 現在、独自情報の追加はプロファイルの読み込み（**LoadProf**）に関連するエラーメッセージのみ対応しています。

設定方法

ユーザー定義のテキストは、以下のレジストリパスに保存されます。 ‘HKEY*LOCAL*MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt\Customer Messages\Client’

追加するエラーメッセージごとに、以下の形式で個別のサブディレクトリを作成する必要があります。’ Client-MsgId-<エラーコード>'

〈エラーコード〉は、該当するエラーメッセージのエラーコードに対応します。例えば、エラーコード **1056** の場合、パスは次のようになります。’ HKEY*LOCAL*MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt\Customer Messages\Client\Client-MsgId-1056'

ご注意

- エラーコードは、リンクされたドキュメント（内容が変更される場合があります）またはエラーを再現することで特定できます。

このレジストリ内では、異なる言語のメッセージを保存することが可能です。言語と国コードがエントリ名として使用されます（例：`de-DE`、`de-AT`、`en-US` など）。

各値には、追加されるメッセージが含まれます。メッセージは最大**1000**文字を超えてはならないことにご注意ください。この文字数を超える場合、メッセージはエラーメッセージに表示されません。

テクニカルサポート

Utimaco製品の技術サポートをご利用になるには、以下の手順に従ってください。

すべての保守契約のお客様は、以下のリンク support.Utimaco.com から、詳細情報およびナレッジベースの記事にアクセスいただけます。 保守契約のお客様は、support@Utimaco.de のメールアドレス宛に技術サポートへメールをお送りください。その際、お使いのUtimacoソフトウェアの正確なバージョン番号、オペレーティングシステム、パッチレベル、および該当する場合は、表示されるエラーメッセージの詳細な説明または該当するナレッジベース項目をお知らせください。

法的通知

最終更新日：**2025**年**8**月**13**日