暗号化忘れを防止し、セキュリティ対策の徹底を実現

マスターキーのある暗号化ソフト

CyberCrypt® Ver.5

テレワーク、クラウドの活用が加速。
働く場所が広がると情報漏えいリスクが拡大する！

情報漏えいリスク 1

テレワークやリモートワークで使用するPCでのファイル管理

- ⚠ 移動時の**PC盗難・紛失**
- ⚠ VPNやシンクライアント接続前の**マルウェア感染によるファイル窃取**

情報漏えいリスク 2

クラウドストレージ上でのファイル管理

- ⚠ 誤操作による**機密ファイルの公開**
- ⚠ 不正アクセスによる**ファイル窃取**

社外やクラウドで、重要な情報を扱うシーンが増加。
大切なファイルを暗号化して守ることが重要です。

ニューノーマル時代の働き方を支える暗号化の切り札

「CyberCrypt®」なら

利用者が**意識することなく**重要なファイルを暗号化！
シンプルな運用で**コスト削減**と**効率化**を実現します。

企業規模や業界業種、官民を問わず導入が進む「CyberCrypt」

セキュリティと利便性の両立、シンプルな運用が高い評価を得ています。“情報を漏えいさせない”
最後の砦となる暗号化の切り札として、働き方改革を支え、生産性や競争力の向上に貢献します。

利用者に負担をかけることなく情報漏えいリスクを回避。

● ファイルの暗号化・復号は右クリックで簡単に設定

ファイルごとに右クリックで暗号化・復号が簡単に設定できます。また、ファイルの拡張子やフォルダ指定により暗号化の除外設定も可能です。操作は右クリックメニューだけなので簡単です。

● フォルダにファイルを格納するだけで自動的に暗号化

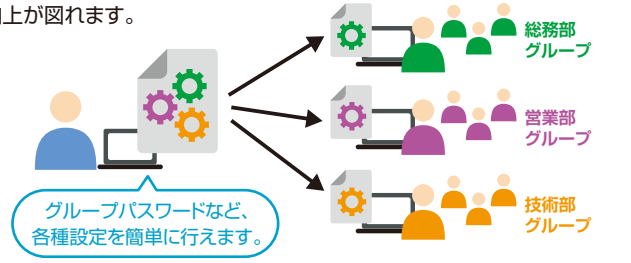
任意のフォルダを「自動暗号化フォルダ」として設定しておけば、このフォルダに格納するファイルは全て自動的に暗号化されるため、暗号化のし忘れを防止できます。

● 暗号化ファイルをダブルクリックで開いて編集、上書き保存で暗号化

暗号化されたファイルの編集、上書き保存は通常のファイル操作で行えます。暗号化のための手間を不要にするとともに暗号化を徹底できます。

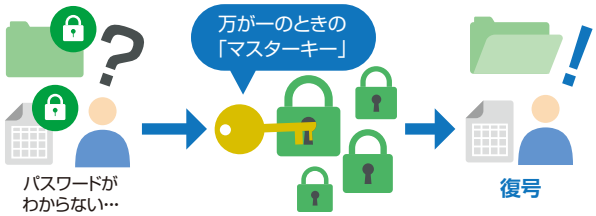
● グループパスワードでセキュアなコラボレーションを実現

共通グループの登録により、暗号化ファイルをグループ内で簡単に共有できます。テレワーク時もセキュアな環境のもとでグループの生産性向上が図れます。



暗号化のパスワードを忘れても安心の「マスターキー」。 パスワード管理サーバ不要で運用コストを削減。

暗号化した本人の不在、復号パスワードの紛失、人事異動や退職、機器変更など、暗号化ファイルの復号が困難な状況においても、企業に 1 つだけ配布される「マスターキー」を使えば全ての暗号化ファイルを復号できます。また、「マスターキー」によりパスワード管理サーバが不要となり、運用コストの削減、管理業務の効率化が図れます。



暗号化によりニューノーマル時代の働き方に 安心・安全を実現!

テレワークやリモートワークで

万が一、PCの盗難や紛失、マルウェア感染によるファイル窃取が発生しても、ファイルの中身が確認できないので、情報漏えい防止に!

クラウドストレージ上で

万が一、誤操作による機密ファイルの公開、クラウドサービスで不正アクセスが行われても、閲覧は不可能!

主な仕様

採用暗号化方式

- 公開鍵暗号方式：RSA暗号、鍵長 2048ビット
- 共通鍵暗号方式：AES暗号、鍵長 256ビット、ブロック長 128ビット
- ハッシュ方式：SHA-256

電子政府推奨暗号リスト（CRYPTREC暗号リスト）対応（2021年4月）

対応OS

- Windows 10（32ビット版/64ビット版）
- Windows 8.1（32ビット版/64ビット版）
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

株式会社 オーク情報システム　URL. https://www.oakis.co.jp/CyberCrypt/

C1021A1101PR