

「社内でも社外でも守る」ファイルセキュリティ

FINALCODE®



■本書は、2020年4月現在の情報を基に作成されています。最新の情報は弊社Webサイトをご参照ください。■Adobe、Acrobat Reader、Illustrator、InDesign、Photoshop は、Adobe Systems Incorporated(アドビシステムズ社)の商標です。Active Directory、Excel、Microsoft、PowerPoint、Windows、Windows Media、Windows Server、Wordは、米国Microsoft Corporationの、米国およびその他の国における登録商標または商標です。Androidは、Google LLCの商標です。AutoCAD、AutoCAD LT、DWG TrueViewは、米国および/またはその他の国々におけるAutodesk、Inc.その子会社、関連会社の登録商標または商標です。BoxはBox、Inc.の商標または登録商標です。iOSは、Apple Inc.のオペレーティング・システムの名称です。iOSは、Cisco Systems、Inc.の商標または登録商標です。『JUST SYSTEM』『一太郎』は株式会社ジャストシステムの登録商標(商標)です。macOSは、米国および他の国々で登録されたApple Inc.の商標です。Marketoは、米国およびその他の国々におけるMarketo Inc.の商標または登録商標です。Oracleは、Oracle Corporation及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。SAPは、ドイツおよびその他の国々におけるSAP SEの商標または登録商標です。SolidWorks®は、Dassault Systemes SolidWorks Corporationの登録商標です。■デジタルアーツ、DIGITAL ARTS、i-FILTER、info board、ARS、Active Rating System、ACTIVE RATING、ZBRAIN、D-SPA、SP-Cache、NET FILTER、White Web、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER File Scan、Mail Detox、FinalCode、DigitalArts@Cloud、Chat@Cloud、Dアラート、Dコンテンツ、当社・当社製品関連の各種ロゴ・アイコンはデジタルアーツ株式会社の商標または登録商標です。■その他、本書に記載されている各社の社名、製品名、サービス名およびロゴ等は、各社の商標または登録商標です。■本書に掲載されている画面および画面設定例は、解説のためのイメージ図であり、実際の画面とは異なる場合がございます。■本書に記載の内容は変更することがあります。予めご了承ください。■見やすく読みまちがえにくいユニバーサルデザインフォントを採用しています。

デジタルアーツ株式会社
www.daj.jp

〒100-0004 東京都千代田区大手町1-5-1 大手町ファーストスクエア ウエストタワー14F
Tel 03-5220-1110 Fax 03-5220-1130

製品に関するお問い合わせ

Tel 03-5220-3090 【受付時間】平日9:00～18:00(土、日、祝日、弊社指定休業日を除く)

E-Mail sales-info@daj.co.jp URL www.daj.jp

お問い合わせ先

ファイルが作成された瞬間から“自動で守り”、
渡した後でも“あとから消せる”。

渡したファイルが“あとから消せる”、 世界ではじめての魔法のソリューション。

どんな会社にも公的機関にも、必ずひとつは重要なファイルがあるはずです。
仕事を進める上では、そのような重要ファイルを仕事の相手に渡さなければならないことがあります。

ファイルはたいていの場合、パスワードロックをかけて、
メールやクラウドサービス、共有フォルダー、オンラインストレージなどで相手に渡しますよね。

でも、ここからが問題でした。

いったん自分の手を離れた重要ファイルは、
そこからさらに他の人に渡されてしまっても、
また、共有サービスにアップロードされてしまっても、
もうコントロールすることや状況を把握することはできません。
つまり、ファイルの受け渡しには、不安とリスクがつきものでした。
重要なファイルであればあるほど、それは大きなストレスだったはずです。

「FinalCode」なら、
“権限のあるAさんが、開いた”
“権限のあるBさんが、印刷した”
“権限のないCさんが、開こうとした”など、
ファイルの状況を把握することができます。
さらに、どこに拡散したか分からないファイルを、いつでも削除することが可能です。

「FinalCode」は、その不安とリスクを解消します。

ファイルが作成された瞬間から“自動で守り”、
渡した後でも“あとから消せる”世界へ。



高度なIRM[※]で指定した人・権限のみ操作可能。
ファイルが作成された瞬間に守ることができます。

- パスワードレス
- 閲覧者指定
- 期間・回数指定
- 印刷・編集制御
- 不正時自動削除
- 印刷・画面透かし設定



ファイルが手元を離れたあとでも、
追跡することができます。

- アクセスログ確認
- 操作ログ確認
- 不正閲覧検知



渡したファイルを
“あとから削除”することができます。

- リモートファイル削除
- リモート権限変更

■ 運用に応じた様々な暗号化手段

ファイルは日常業務での利用頻度が高いため、「業務にどう浸透させるか？」の観点で、運用に応じた様々な暗号化手段を提供します。

- 透過暗号
- 共有フォルダー自動暗号化
- API
- m-FILTER連携
- Box連携

■ 暗号化されている環境を簡単に実現(透過暗号)

ファイルを作成・保存、ファイルサーバー・データベース(DB)・クラウドからダウンロードしたタイミングで自動暗号化。アプリケーションの連携機能(差込印刷、共同編集等)も使えるため、今までと同様の使い勝手でファイルセキュリティを実現します。



「ファイル操作権限の設定画面」

■ ファイルの利用履歴を集中管理

社内の全ファイルであれ、重要ファイルであれ、ファイルが手元を離れてもアクセスログを常に記録し続け、「いつ・誰が・どこから・どんな操作をしたか」をリアルタイムで捕捉することができます。

■ セキュリティポリシー設定履歴の可視化

ファイルの閲覧権限や操作権限の変更が行われるごとに、権限変更履歴をログとして残します。不適切な権限操作もわかります。

■ ステータス通知システム

閲覧権限を持たないユーザーによる不正アクセスがあった場合、ファイル所有者にメールで通知。異常を即時把握することができます。

■ いざとなったらリモートで消せる

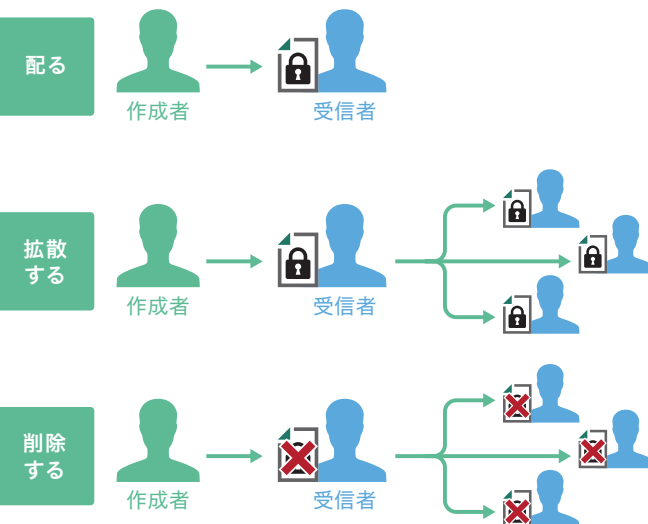
万が一、機密ファイルが流出しても、リモートで跡形もなく消すことができます。渡したファイルが拡散されたとしても“あとから削除”することができます。

■ 手元を離れたファイルを常にコントロール

ファイルそのものを渡しても、ファイルのオーナーシップは手元に残ったまま。セキュリティポリシーを変更することで、いつでも閲覧・操作権限を変更できます。しかも変更内容はリアルタイムに反映されます。

日時	アクセス日時	ファイル/フォルダー名	操作実行者のメールアドレス	アクセス元のIPアドレス	操作内容
Q	2019/01/29 10:43:36	test_20190118_1.pdf	test@example.co.jp	192.168.240.21	上書き保存(透過暗号)
Q	2019/01/28 18:22:08	test_20190118_1.pdf	test@example.co.jp	192.168.240.21	開封(透過暗号)
Q	2019/01/28 15:35:46	example.txt	test@example.co.jp	192.168.240.21	不許可
Q	2019/01/28 15:55:04	example.pdf	test@example.co.jp	192.168.240.21	不許可
Q	2019/01/28 14:40:33	example.txt	test@example.co.jp	192.168.240.21	不許可
Q	2019/01/24 14:38:33	example.txt	test@example.co.jp	192.168.240.21	暗号キャンセル
Q	2019/01/24 14:36:19	testname002.txt	test@example.co.jp	192.168.240.21	暗号キャンセル

いつ どのファイルに 誰が どこから 何ををした

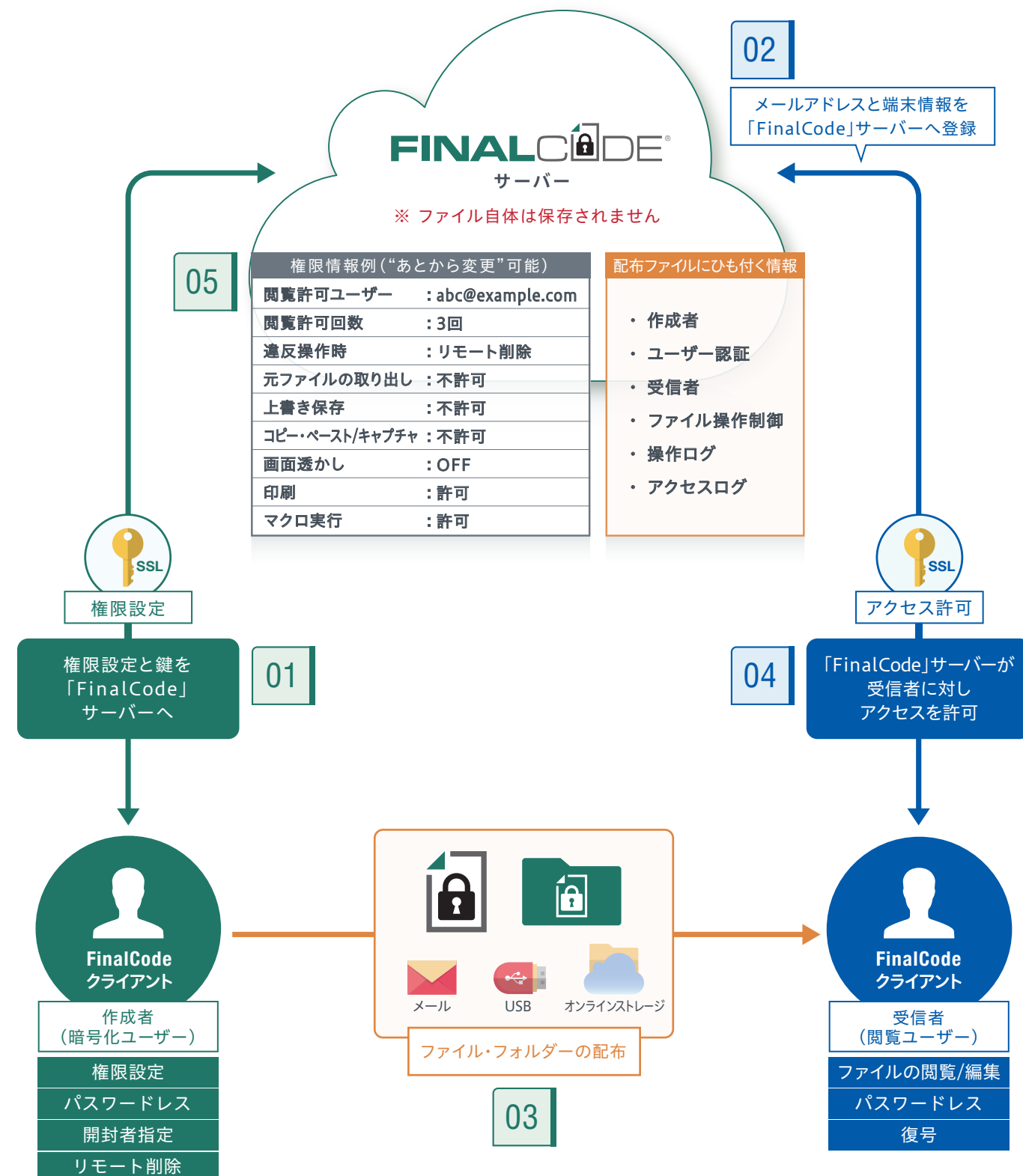


※ IRM: Information Rights Management. (情報資源管理) 文書ファイルを暗号化し、閲覧や編集を制限したり開封・操作履歴を取ることができるソフトウェア

魔法のようなソリューション。独自技術と 先進性で実現しました。

世界各国で
特許取得済み

ファイルの暗号化/閲覧を行う「FinalCode Client」※と、ファイルの権限情報等を管理する「FinalCode Server」とで構成されます。
暗号化ファイルの閲覧権限者、ファイルへのアクセス権限等、全ての権限情報がクライアント——サーバー間で管理されるため、
ユーザーは意識することなく強固な暗号化ファイルを利用できます。



01 作成者が対象ファイルを「FinalCode Client」で暗号化すると、「FinalCode」サーバーにファイルの権限情報と鍵が預けられます。

※ ファイル自体は保存されません

02 ファイルの受信者は、事前に「FinalCode Client」をインストールしておきます。インストールが完了すると、自身のメールアドレスと利用する端末情報が「FinalCode」サーバーに登録されます。サーバーに登録されることで、ファイル閲覧ユーザーが特定でき、さらに次回以降ファイル閲覧時にパスワードを入力する必要はありません。

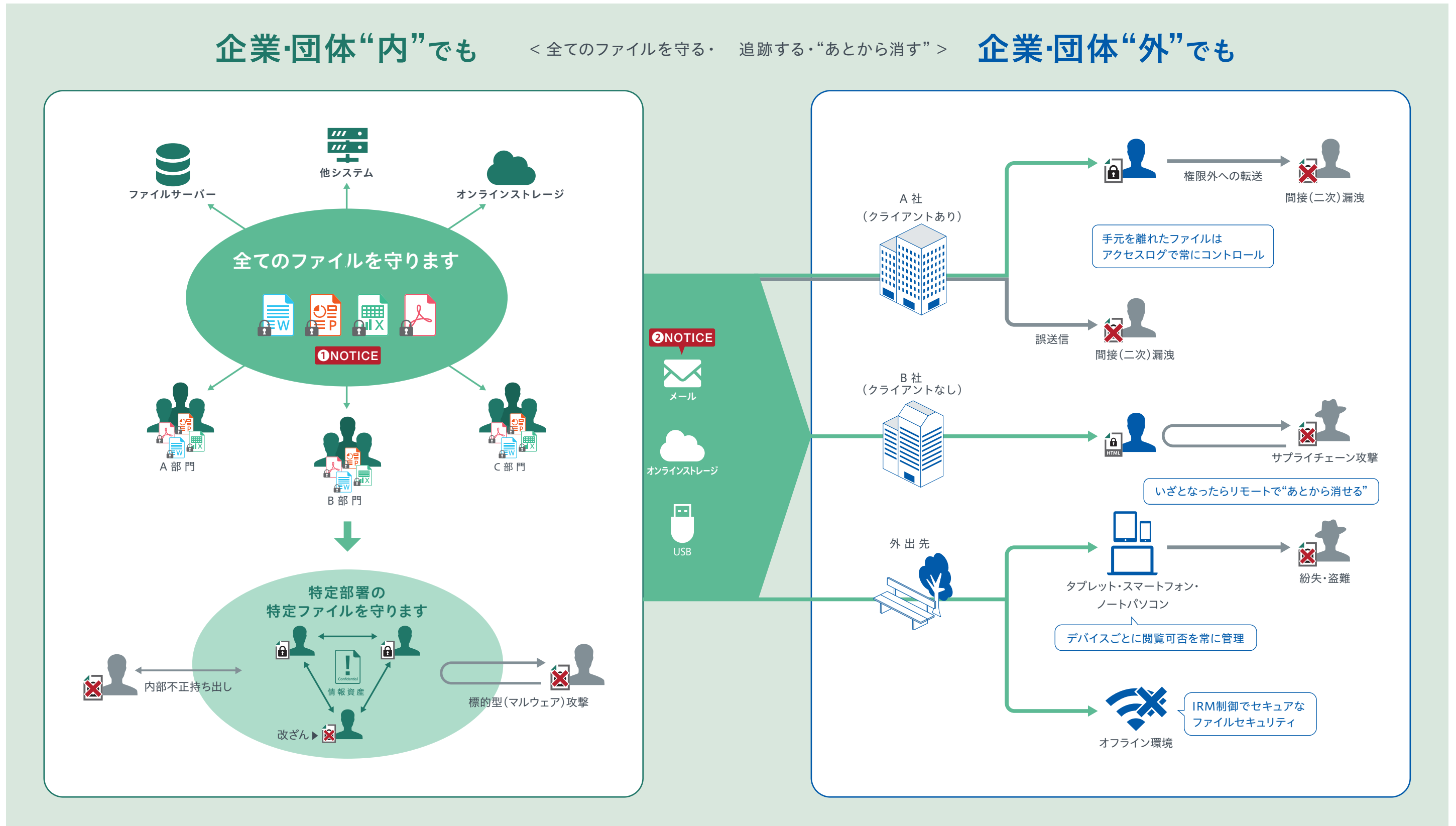
03 作成者が、受信者にファイルを渡します。メールやUSB、オンラインストレージ等、配布方法は問いません。

04 受信者が暗号化されたファイルをダブルクリックすると、自動的に「FinalCode」サーバーに権限情報の問い合わせが行われ、権限情報に基づいて、ファイルの閲覧可否が判断されます。このとき受信者が行った、閲覧、編集、印刷等の操作は「FinalCode」サーバーに全て記録され、作成者はログとして管理することができます。

05 「FinalCode」サーバーの権限情報は「あとから変更」することもできます。作成者が、渡したファイルに削除の操作を行うと、受信者がファイルをダブルクリックした際に「FinalCode」サーバーに最新の権限情報の問い合わせが行われ、ファイルがどこにあって、いくつコピーが存在していても、すべて同様に遠隔で削除することができます。

※ 「FinalCode」による暗号化やファイル展開はインターネットに接続可能な環境が必要です
※ オフライン閲覧機能オプションをご利用いただく、インターネット環境が無い場所でも、オンライン時と同様にパスワードでIRM制御を行うことができます
([Box連携機能]で暗号化されたファイルについては、本機能をご利用いただけません) ※ 利用に際し、「FinalCode Client」のインストールとユーザー登録が必要です

「FinalCode」が、業務で扱う全てのファイル^{*}を意識することなく守ります。



1 NOTICE Microsoft Active Directory(AD)との連携で、ADに設定されているメールアドレス、メーリングリスト、組織単位(OU)、セキュリティ

2 NOTICE メールセキュリティ製品「m-FILTER」との連携で、メール送付時に添付ファイルを自動暗号化(または自動ファイル変換)

グループ、アカウントを指定できるため、利用者がメールアドレスを持っていない環境でも「FinalCode」を容易に使い始めることができます
 ※ 動作検証済みアプリケーションは順次拡張中。最新情報は右記URLよりご確認ください <https://www.finalcode.com/jp/product/spec/>

ファイルセキュリティ運用を成功に導く4つの チェックリスト

- 1

守るべき情報資産は？

☐ 全ファイル

☐ 顧客・個人情報

☐ 経営情報、公開前のIR情報

☐ 見積、売上、与信情報

☐ 実験・計測・研究データ

☐ 住民情報

☐ 税関連や年金、国民健康保険などを含むファイル

☐ 議事録

☐ RFPやNDAのもと開示した有効期限ありの情報

☐ 生徒情報

☐ 問題集などの授業関連ファイル

☐ その他()
- 2

守るべき部門は？

☐ 全部門

☐ 経営企画

☐ 営業・マーケ

☐ 人事・総務・財務

☐ 研究・開発

☐ 市民・住民課

☐ 市民税・納税課

☐ 福祉・子育て支援課

☐ その他()

☐ 教職員・教授

☐ 生徒

☐ その他()
- 3

防ぎたい情報漏洩は？

☐ 標的型(マルウェア)攻撃

☐ サプライチェーン攻撃

☐ 内部不正持ち出し

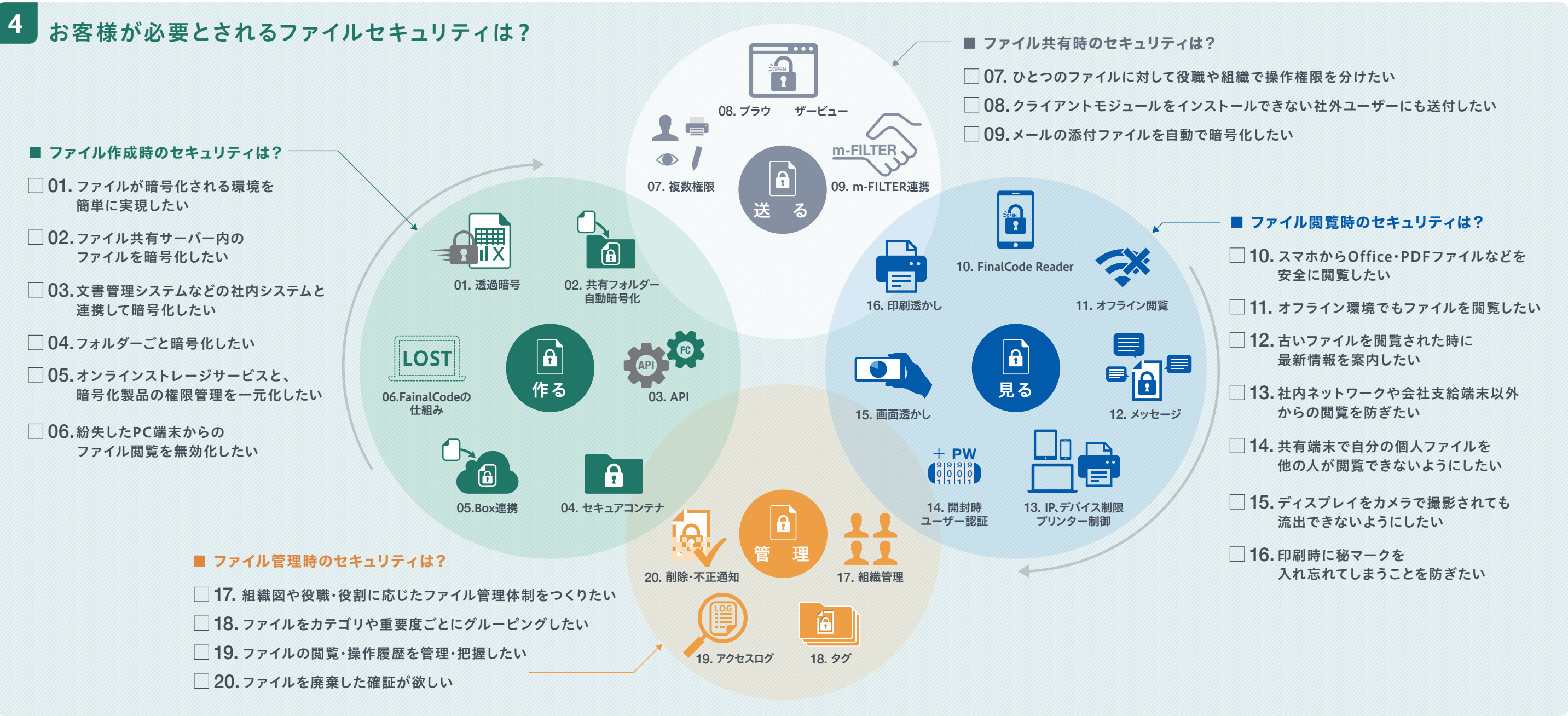
☐ 間接(二次)漏洩

☐ 紛失/盗難

☐ 誤送信

☐ 改ざん

☐ その他()

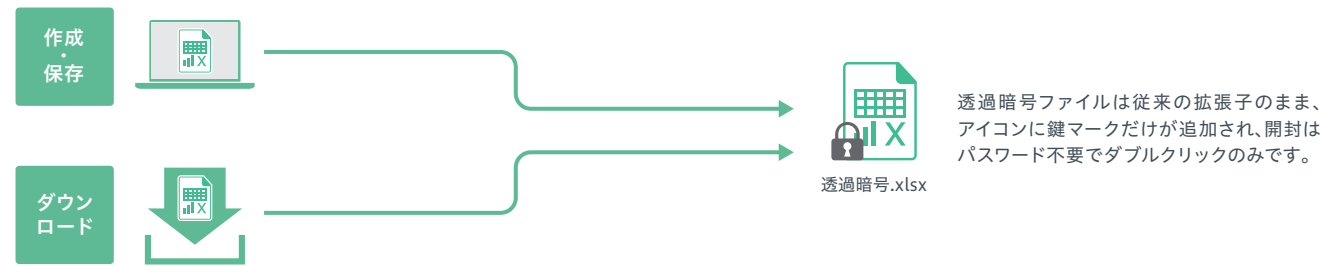


ファイルセキュリティ運用を充実させる主な 機能

暗号化ファイル作成時

01. ファイルが暗号化される環境を簡単に実現したい

ファイル作成・保存時や、ダウンロードした瞬間に自動暗号化します。
暗号化されていても、今までと同様の使い勝手のため、オペレーション教育の手間はありせん。また暗号化をユーザーに意識させないため、セキュリティリテラシーに関係なくご利用いただけます。



02. ファイル共有サーバー内のファイルを暗号化したい

ファイル作成・「FinalCode」がファイルサーバー上の共有フォルダーを常時監視し、フォルダーにファイルが格納された時点で、あらかじめ設定されたテンプレートに基づいて自動でファイルを暗号化します。
ユーザーはいつも通りにフォルダーへファイルを保存するだけで守ることができます。

※ ファイルサーバーにモジュールをインストールする必要があります ※ 自動暗号化設定ができるフォルダー数に制限はありません

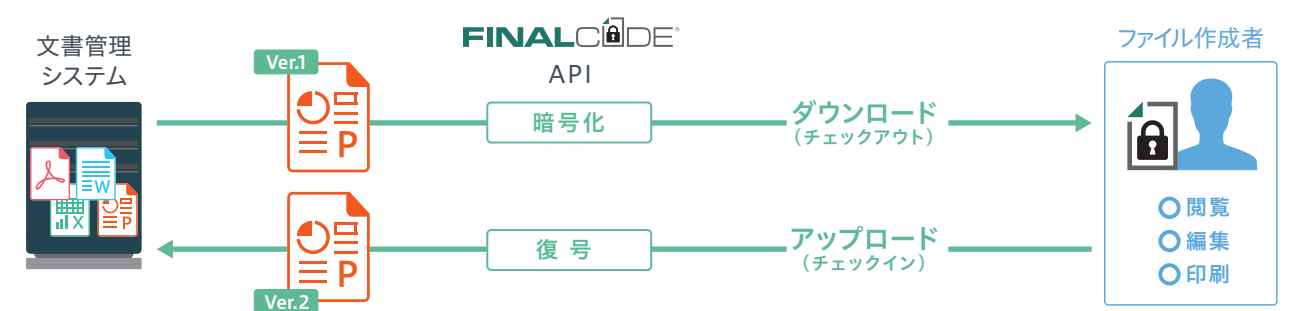
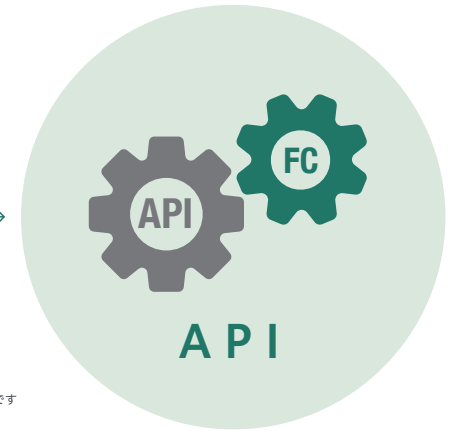


03. 文書管理システムなどの社内システムと連携して暗号化したい

オプション ▶ P.24

文書管理システムやファイル転送システムなどの外部システムから「FinalCode」の暗号化・復号の機能をコールできる実行形式のAPI※を提供しています。
システムが自動で暗号化・復号するため、現行の運用フローを変えることなくセキュアな運用が実現します。

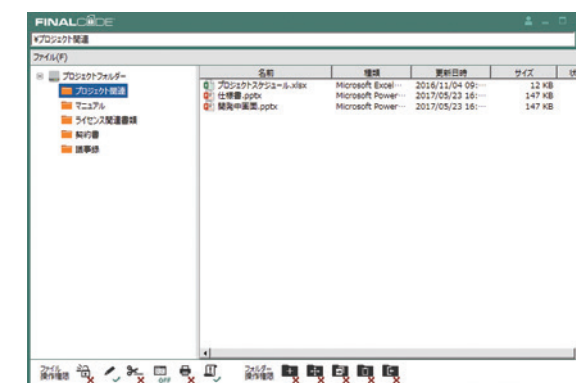
※ ファイルの暗号化や復号、権限の変更など、利用者が通常「FinalCode Client」や管理画面を通じて行う主な操作を、コマンドラインから行うためのツールです



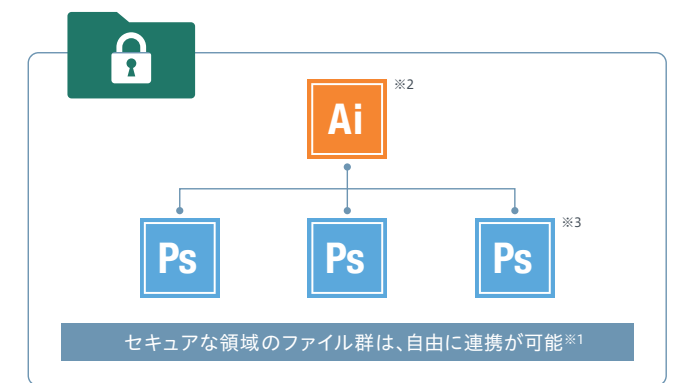
04. フォルダーごと暗号化したい

ファイル単位でなく、ファイルが格納された「フォルダーそのもの」を暗号化します。セキュアコンテナ内のファイル群は、設定された権限の範囲内でこれまでと同様の使い方ができ、ファイル同士の連携も可能※1になります。
「フォルダーそのもの」を暗号化することにより、ファイルの持ち出しやコピー、削除も制御します。

※1 ファイル間の参照や連携の、一部の機能は利用できません ※2 Adobe Illustrator ※3 Adobe Photoshop



「FinalCode エクスプローラー」で閲覧・操作します



ファイルセキュリティ運用を充実させる主な機能

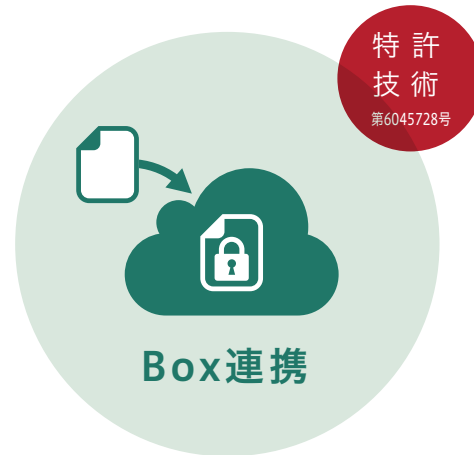
暗号化ファイル作成時・共有時

05. オンラインストレージサービスと暗号化製品の権限管理を一元化したい

オプション ▶ P.24

「FinalCode」の「Box連携オプション」があれば、Box内外のファイルアクセス権を一貫してコントロールでき、よりセキュアな権限管理が可能になります。
オンラインストレージサービスでは管理できないファイルダウンロード後も、セキュアな状態を保ちます。

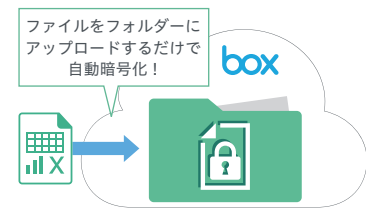
*「FinalCode@Cloud」(クラウド版)のみ利用可能なオプションです



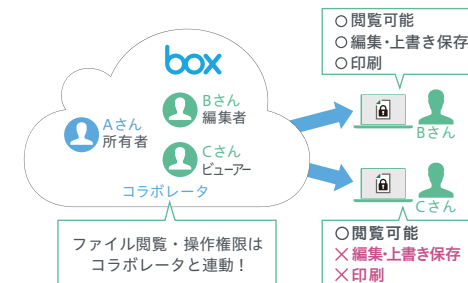
特許技術
第6045728号

Box連携

①「Box」にアップロードすると「FinalCode」で自動暗号化



②「コラボレータ」のメンテナンスだけで、ダウンロード後のファイルも管理



③ 暗号化されたファイルのプレビューは、「Box」内だけで可能



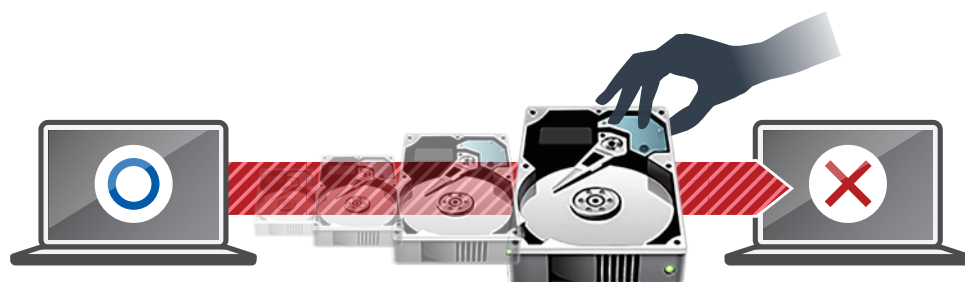
06. 紛失したPC端末からのファイル閲覧を無効化したい

「FinalCode」の管理者が、紛失したユーザーの端末情報を「FinalCode」の管理画面上から削除すれば、紛失した端末からの暗号化ファイル閲覧を防ぐことができます。
またハードウェア固有情報と関連付けられた認証を行うため、鍵ファイルのコピー、HDDの抜き取りが行われても、認証エラーとなりファイルは開けません。



特許技術
第5404030号
第5840180号

FinalCodeの仕組み

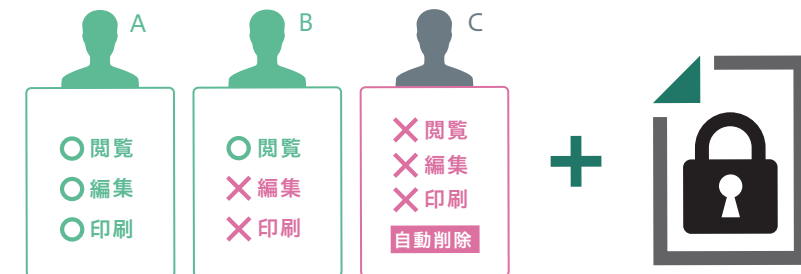


07. ひとつのファイルに対して役職や組織で操作権限を分けたい

役職者、一般社員、派遣社員など、権限レベルごとにファイル閲覧者・操作権限の組み合わせ(権限セット)を、ひとつのファイルにつき複数設定できます。
ひとつのファイルに複数権限を設定できるため、複数の暗号化ファイルを作成する必要はなく手間が省けます。



複数権限

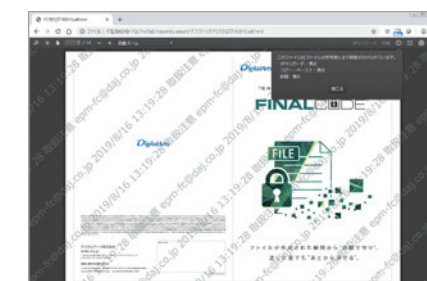
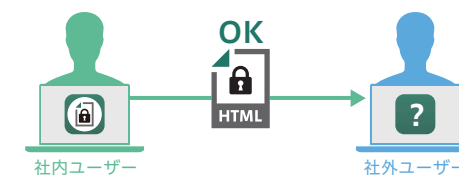


08. クライアントモジュールをインストールできない社外ユーザーにも送付したい

クライアントモジュールがインストールされていないデバイスでも、ブラウザー上で暗号化ファイルを開覧することができます。
PW+Zipファイルと違い、閲覧者や閲覧期間の指定ができるため、セキュリティ対策も万全です。またファイル閲覧履歴も確認できるため開封チェックとしてもご利用いただけます。



ブラウザービュー



設定例
・「印刷」「元ファイルの取り出し」を禁止
・画面透かし有り

ブラウザービュー機能のIRM制御:
閲覧者・閲覧期限・回数の指定/元ファイル取り出しの可否/コピー&ペースト・画面透かしの可否/印刷/印刷透かしの可否/タグ・メッセージの付与

ファイルセキュリティ運用を充実させる主な 機能

暗号化ファイル共有時・閲覧時

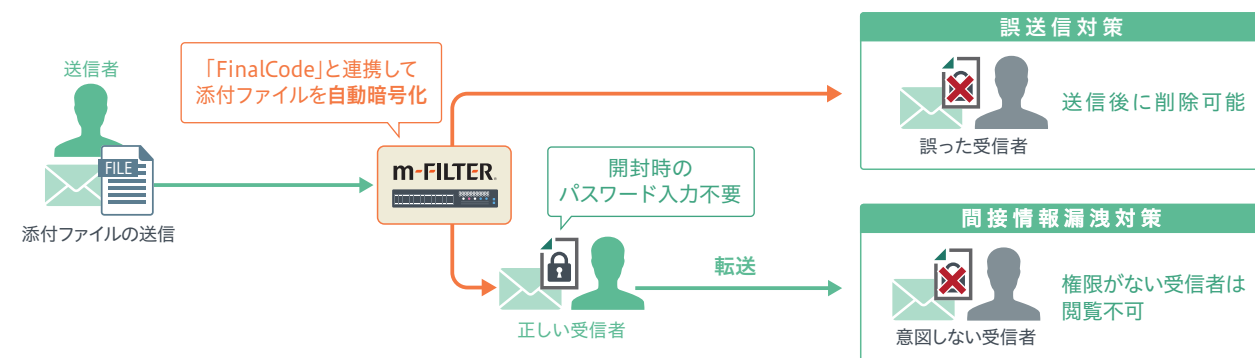
09. メールの添付ファイルを自動で暗号化したい

「m-FILTER」との連携で、メール送信時に添付ファイルは自動的に「FinalCode」で暗号化された状態で送信されます。

送信者の暗号化作業負担を軽減します。「FinalCode」で暗号化されたファイルであれば、閲覧権限のある受信者しかファイル閲覧を行えません。また、送信者は送信後にファイルを“あとから消す”ことも可能です。



特許
技術
第5939953号



10. スマホからOffice・PDFファイルなどを安全に閲覧したい

iOS/Android™の端末上で、OfficeファイルもPDF形式に変換して、指定されたユーザーのみ閲覧することができます。端末にダウンロードされたファイルは、遠隔で“あとから消す”ことができます。

過去に閲覧したファイルは、『ファイル一覧リスト』に掲載されるためメールアプリを開いてファイルを探す必要がありません。スマホ上で安全にファイル閲覧が可能のため、Zipファイルよりも高いユーザビリティを提供します。



11. オフライン環境でもファイルを閲覧したい

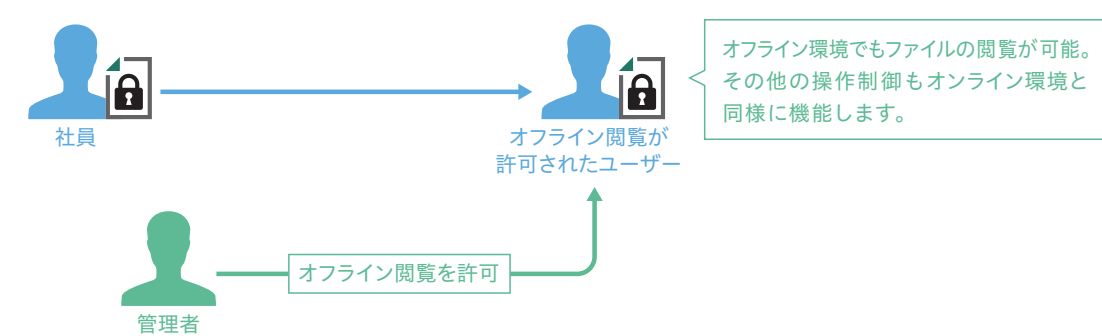
オプション ▶ P.24

建設や工事の現場、飛行機での移動中など、オフライン環境でもパスワードレスで暗号化ファイルを開けるように設定でき、オンラインの時と同様にIRM制御を行うことができます。

ネットワーク回線がない環境下に置いてIRM制御を行うことで、場所を問わないファイルセキュリティを提供します。



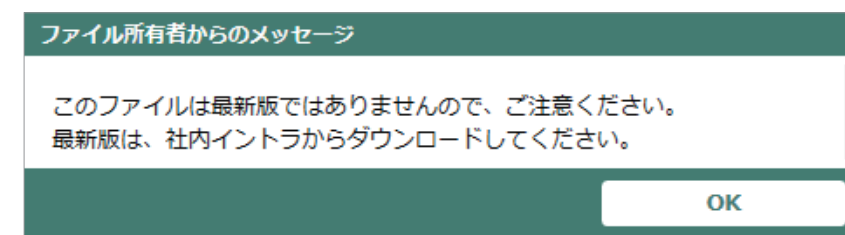
特許
技術
第6082130号



12. 古いファイルを開覧された時に最新情報を案内したい

暗号化ファイルの開封時に、作成者からのメッセージを表示できます。

ファイル送付後も閲覧者にファイルの誤植や更新をお知らせすることができます。都度メールや電話で共有する必要はありません。



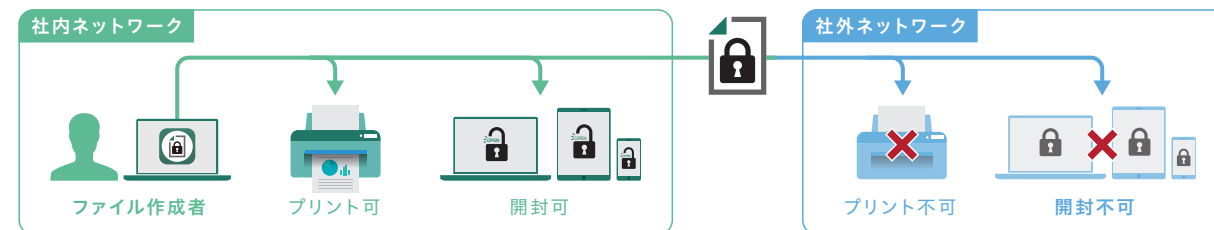
ファイルセキュリティ運用を充実させる主な 機能

暗号化ファイル閲覧時

13. 社内ネットワークや会社支給端末以外からの閲覧を防ぎたい

暗号化ファイルを閲覧できるデバイスのIPアドレス、OS種別、MACアドレスを制限することができます。また印刷を許可するプリンター制御(PDF作成用の仮想プリンターの使用を禁止する等)の管理もできます。
上記制御をすることで、以下を実現します。

- ①暗号化ファイルは、社内ネットワークや会社支給端末のみの開封とする。
- ②社内プリンターからの印刷のみ許可することで、社外で不正にコピーされることを防止する。

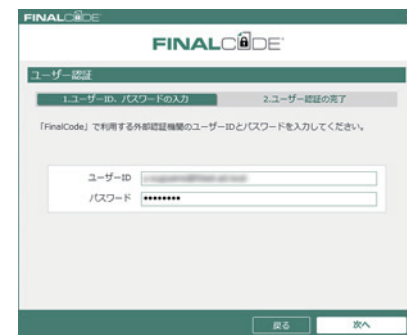
IP、デバイス制限
プリンター制御

14. 共有端末で自分の個人ファイルを他の人が閲覧できないようにしたい

「FinalCode」は基本パスワードレスで開封できますが、開封時にパスワードを入力させることもできます。
共有端末で作業する場合に、自分の個人ファイルを他の人が閲覧できないようにします。

開封時
ユーザー認証

【開封者が外部連携認証を利用していないユーザーの場合】

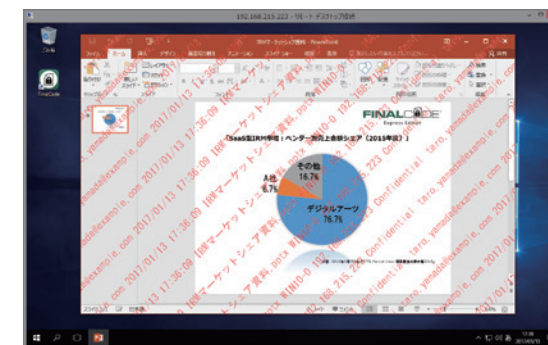


【開封者がAD認証を利用しているユーザーの場合】

15. ディスプレイをカメラで撮影されても流出できないようにしたい

暗号化ファイルの閲覧時に、画面上に表示されるデータに透かしを挿入することが可能です。ユーザー名、開封日時、PC名などを表示することができるため、スクリーンショットデータの流出を抑制します。
文字・サイズ・色の変更や、開いたタイミングの情報(日時、IPアドレス等)を表示できる“動的な”画面透かしのため、表示させたい情報が足りなかったり、透かし文字がファイル本文に被り中身が読めないということはありません。

画面透かし



16. 印刷時に秘マークを入れ忘れてしまうことを防ぎたい

印刷制限を付けた暗号化ファイルの印刷時に、ユーザーが指定した透かしを追加できます。
ファイル作成者側でプリンターを問わずに透かしを挿入することができるため、不要な印刷や秘マークの入れ忘れによる漏洩リスクを軽減することができます。

印刷透かし



ファイルセキュリティ運用を充実させる主な 機能

暗号化ファイル管理時

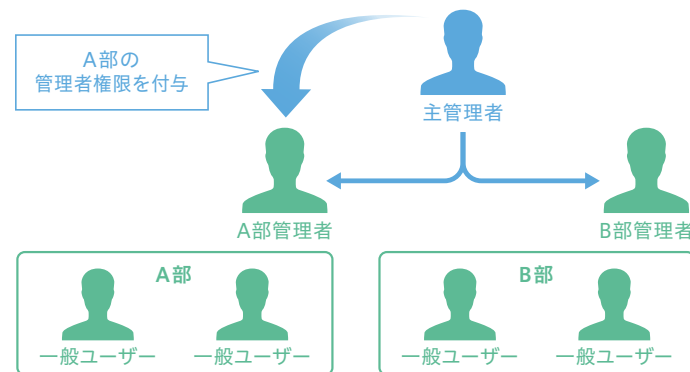
17. 組織図や役職・役割に応じたファイル管理体制をつくりたい

権限の設定を行う際に、組織階層を定義できます。

管理者権限を組織毎の担当者に委譲し、管理者を複数体制に。

各組織の業務特性を考慮しながら組織にあったセキュリティを適用することが可能です。

* A部の管理者は、A部内においてA部共通テンプレートの作成、ユーザー登録、ログ監視などの管理業務を担当。現場ニーズに即した運用を実現。

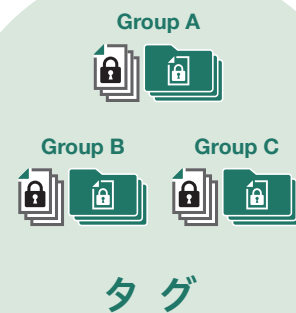


組織管理

18. ファイルをカテゴリや重要度ごとにグルーピングしたい

暗号化時にファイルやフォルダーにタグを付与できます。

部署別や重要度別のタグを付与することで、ファイルやフォルダーをグルーピングして、管理画面上からキーワードで検索できます。



タ グ



19. ファイルの閲覧・操作履歴を管理・把握したい

暗号化ファイル作成者のブラウザー上から、ファイルの閲覧・操作履歴を確認できます。また、不正な操作発生時には通知メールで把握できます。

閲覧・操作履歴の確認だけでなく、手元を離れたファイルでも権限変更が可能です。さらに権限変更後のファイルを再送付する必要はありません。

詳細	アクセス日時	ファイル/フォルダー名	操作実行者のメールアドレス	アクセス元のIPアドレス	操作対象
Q	2019/01/29 10:43:36	test_20190118_1.pdf	fttest@dej.co.jp	192.168.240.21	上書き保存(透過暗号)
Q	2019/01/28 18:22:08	test_20190118_1.pdf	fttest@dej.co.jp	192.168.240.21	開封(透過暗号)
Q	2019/01/28 15:55:46	example.txt	fttest@dej.co.jp	192.168.240.21	不許可
Q	2019/01/28 15:55:08	example.pdf	fttest@dej.co.jp	192.168.240.21	不許可
Q	2019/01/24 14:40:33	example.txt	fttest@dej.co.jp	192.168.240.21	不許可
Q	2019/01/24 14:38:53	example.txt	fttest@dej.co.jp	192.168.240.21	復号キャンセル
Q	2019/01/24 14:36:19	testname002.txt	fttest@dej.co.jp	192.168.240.21	復号キャンセル

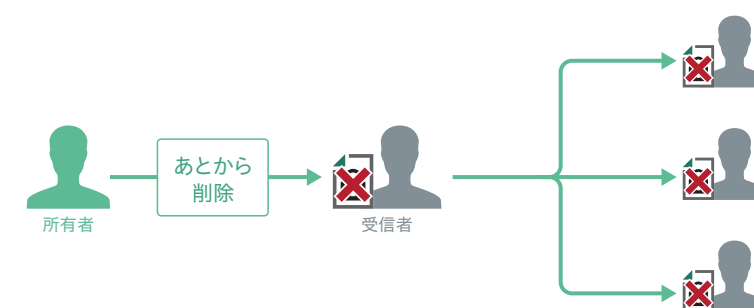
いつ どのファイルに 誰が どこから 何をした

アクセスログ

20. ファイルを廃棄した確証が欲しい

ファイルそのものを渡してもファイルをコントロールし続けるため、いざとなったら手元を離れたファイルでもリモートで”あとから削除”が可能です。

拡散されたファイルも削除し、ログとして残るため、廃棄したエビデンスを取得することもできます。



削除・不正通知



許可されていないユーザーがアクセスすると、そのタイミングでファイル所有者にアラート通知があり、万が一の場合には、リモートで“あとから消す”ことができます。

運用を柔軟かつ強固に支える「Final Code」の“柔”と“剛”。

柔

ファイルセキュリティは日常業務に密接に関わるからこそ、「FinalCode」は、実現したい運用に合わせて、3つの暗号化ファイルを提供します。

	FCLファイル 	ブラウザービュー (BV) ファイル 	透過暗号ファイル 
概要	“渡したファイルをあとから消す”など、ファイルに対して強力なIRM制御を付与することが可能	専用クライアントソフトがインストールされていない端末でも、暗号化ファイルをブラウザー上から閲覧可能	“ファイルを作成した瞬間から守る”ことができ、今までと同様の使い勝手で暗号化ファイル进行操作可能
適した利用シーン	・社内でも特定ユーザーしか開封させない極秘ファイルを守りたい場合 ・社外に渡したファイルの操作権限をコントロールしたい場合	社外の取引先等、専用クライアントソフトがインストールできないユーザーに対しても、安全にファイルを提供したい場合	社内の利用ユーザーには暗号化を意識させないため、ITリテラシーを問わず、幅広く守りたい場合
拡張子、アイコン	・元の拡張子の後ろに .fcl (例○○.xlsx.fcl) ・独自アイコン	・元の拡張子の後ろに .html (例○○.xlsx.html) ・ブラウザーのアイコン	・拡張子の変更なし (例○○.xlsx) ・元アイコンに鍵マーク

以下、暗号化制御の可否 (○: 制御可 / ー: 制御不可)

閲覧者の指定	○	○	ー (ドメイン固定)
閲覧期限・回数の指定	○	○	ー
元ファイル取り出し制御	○	○	ー
上書き保存制御	○	ー	ー
コピー・ペースト/ キャプチャ (画面透かし) 制御	○	○ (キャプチャ制御なし)	ー
印刷 (印刷透かし) 制御	○	○	○
マクロ実行制御	○	ー	ー
所有権限譲渡制御	○	ー	ー
ブラウザービューファイル変換	○	ー	○
FinalCodeファイル変換	ー	ー	○
Zipファイル変換	ー	ー	○
削除・不正通知	○	ー	ー
アクセスログ・操作ログ	○	○	ー (主管理者のみ)

剛

社内にあるファイルだけではなく“社外に出たファイル”までカバーする「FinalCode」だからこそ、ファイルを“完全に”コントロールするために、ファイルが”開かれる環境”もコントロールします。

特許
技術
第5750497号

メーカーとして動作検証したアプリケーションに対してIRM制御することで、サポートも含め、お客様は安心・安全にご利用いただけます。



一般的なファイル暗号化製品には、暗号化設定が効くことを確認できた動作検証済みアプリケーションがあります。例えば、よく使われているMicrosoft Office Wordは、各社とも動作検証済みです。しかし、docファイルが、渡した先でも当たり前のようにWordで開封されるとは限りません。海外では、知名度の低いアプリケーションを使っていることがあります。

もし、それが動作検証済みアプリケーションでない場合、完全な暗号化が保たれない可能性があります。それでは、暗号化したファイルでも安心して社外に渡すことはできなくなります。そこで「FinalCode」では、暗号化設定が必ず効くことが確認できている**動作検証済みアプリケーションで「のみ」暗号化ファイルを開くことができる制御**(ホワイトリスト方式)を採用しています。

また、様々なアプリケーションが日々開発されている今日、スクリーンキャプチャやアップロードなど、重要ファイルから情報を抜き取る可能性があるアプリケーションが大量に存在します。安心して重要なファイルを渡すには、相手のPCがそれらのアプリケーションを利用していたとしても問題ない仕組みが必要です。そこで「FinalCode」では、暗号化ファイルを開封するとき、または開封中のPCで、**セキュリティホールに繋がるアプリケーションが同時に利用されないような制御**(ブラックリスト方式)も採用しています。

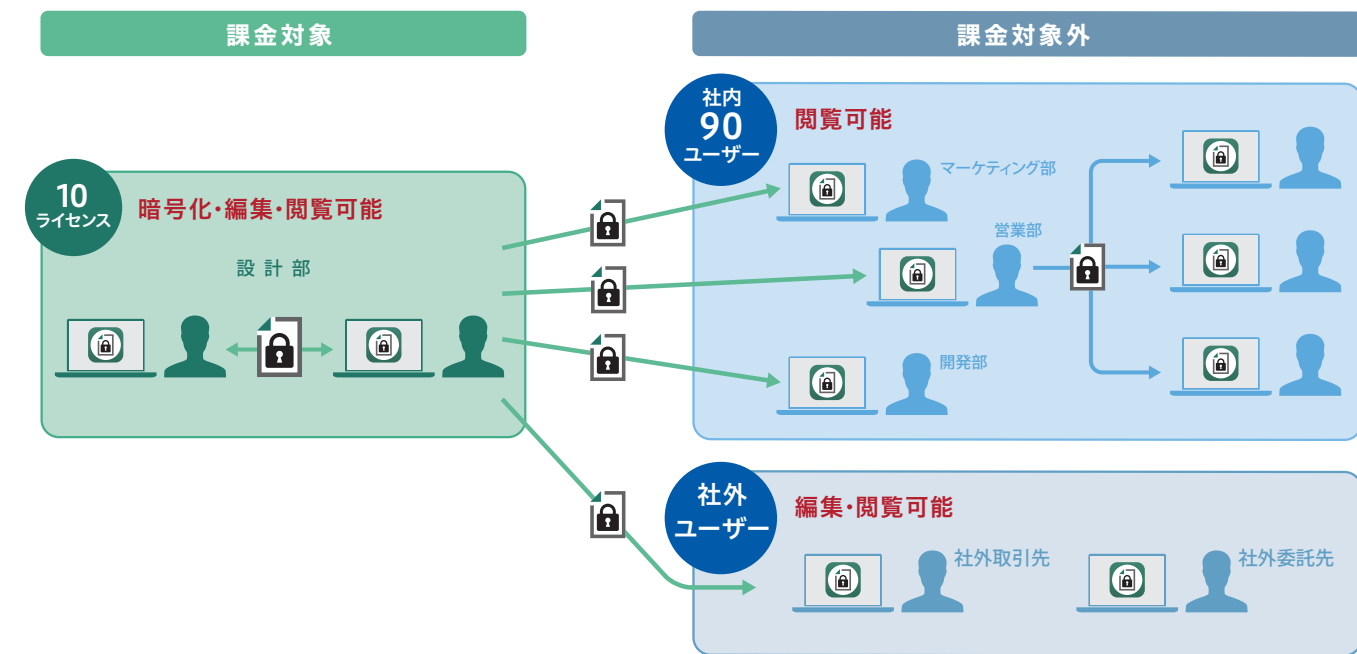
「FinalCode」は、導入のしやすさでも選ばれています。

01 課金対象は、企業・団体内ユーザー※1の「暗号化・編集ユーザー」のみ

「暗号化・編集」するユーザー数分のライセンスをご購入ください。FCLファイルを「閲覧」する、企業・団体内ユーザーは無償です。
また、社外の取引先や委託先などの企業・団体外ユーザー※2も無償でファイルを「編集・閲覧」できるので、ガバナンスを効かせづらい企業・団体外へも、安心・安価にファイルを展開できます。

※1「主管理者が管理画面にて登録した企業ドメイン」を持つメールアドレスのユーザー ※2「企業・団体内ユーザーとは異なるドメイン」のメールアドレスのユーザー ※「企業・団体内」の無償ユーザーは透過暗号化できないため、透過暗号ファイルの閲覧はできません。透過暗号ファイルを開覧するためには、有償ライセンスのご購入が必要です ※ひとつの契約で利用可能な企業・団体内ユーザー数は、無償閲覧ユーザーを含め、購入ライセンス数の10倍までです

利用例 設計図面 >>> 🔒 10ライセンスのご購入で、90ユーザー分は無償で閲覧可能

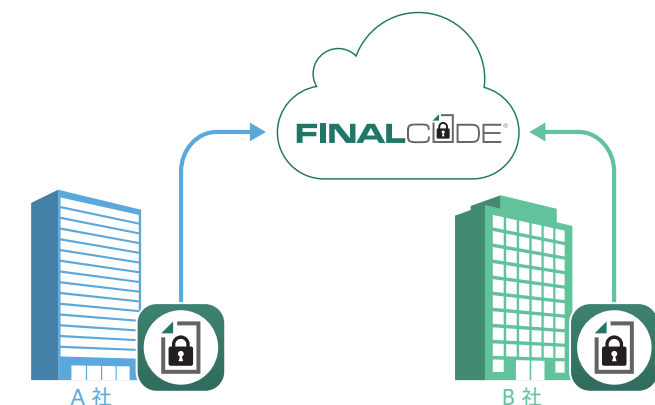


02 フレキシブルな導入形態ですぐにスタート

FinalCode@Cloud（クラウド版・SaaS）

サーバー構築コスト不要

サーバー構築の費用・準備が不要で、すぐにご利用いただくことができます。また、メンテナンスフリーのため、運用管理面での手間を大きく軽減することができます。なお、「FinalCode」はファイル自体はサーバーには格納されず、権限情報・ログのみ管理します。

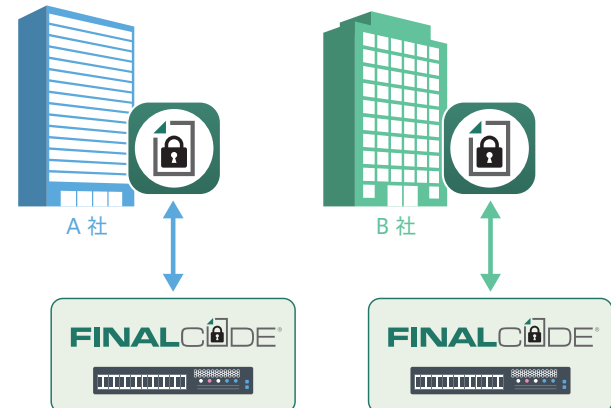


FinalCode Ver.6 VA（オンプレミス版・VA※）

自社サーバーで運用可能

自社で独自にサーバー構築していただくことができます。すべてを社内で完結されたい場合に適しています。

※ Virtual Appliance ※ 別途、データベースサーバーの構築が必要です

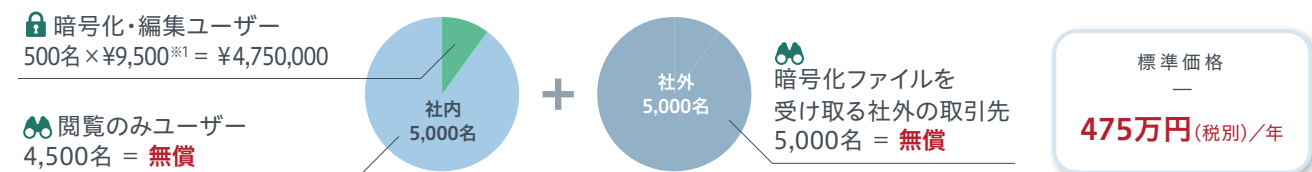


試算ケース

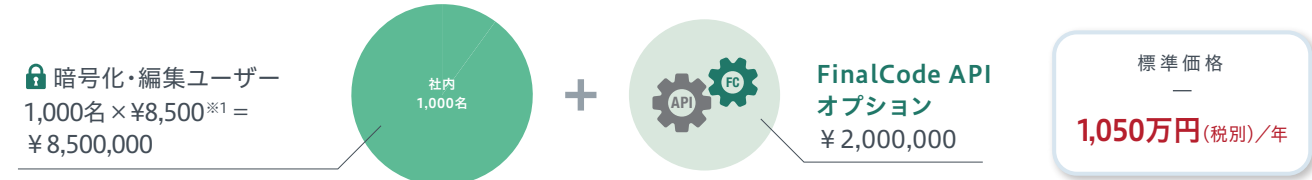
Case 01 社内100名規模のファイルを守りたいが、暗号化は限られた人数で行う場合の年間価格



Case 02 社内5,000名（暗号化・編集ユーザー 500名、閲覧のみユーザー 4,500名）と暗号化ファイルを受け取る社外の取引先5,000名が利用する場合の年間価格



Case 03 社内1,000名（暗号化・編集ユーザー 全社員1,000名）、APIオプションを利用して、社内文書管理システムと連携する場合の年間価格



※1 購入ライセンス数に応じた特別料金体系を用意しています。詳細は価格表をご参照ください

有償オプション

Box連携機能
Boxにアップロードするだけで自動暗号化し、ダウンロード後のファイルもしっかり守り続けます。
※ 本機能を利用される場合はユーザー数分をご購入ください

CADファイル暗号化・閲覧機能
製造業にとって重要な資産であるCADファイルに、暗号化と閲覧の機能を提供します。
※ 本機能を利用される場合はユーザー数分をご購入ください

オフライン閲覧機能
インターネット環境が無い場所でも、オンライン時と同様にパスワードレスでIRM制御ができます。
※ 「Box連携機能」で暗号化されたファイルについては、本機能をご利用いただけません
※ 本機能は、ユーザー数に関係なく年額でのご購入となります

FinalCode API
外部システムから「FinalCode」の暗号化・復号の機能をコールできる実行形式のAPIを提供します。
※ 本機能は、ユーザー数に関係なく年額でのご購入となります

ライセンス種別

企業のお客様には「標準価格」を、公共・文教のお客様には「パブリックライセンス価格」を用意しております

企業向け	公共・文教向け
標準ライセンス価格	パブリックライセンス価格

単なる暗号化にとどまらない革新的な ソリューション「FinalCode」

「FinalCode」により、お客様は情報資産を強固に守れるだけでなく、その先にある付加価値を享受し、ビジネス加速や業務効率化に大きく貢献します。

作業工数削減

パスワードを設定することなくファイルを暗号化して共有することが可能であり、暗号化されたファイルは、ダブルクリックで簡単に閲覧できます。そのため別メールでパスワードを送るといった従来のセキュリティ考慮の手間もなく、作業工数の削減につながっております。



YAZAKI
■ 矢崎総業株式会社

顧客満足度向上

「FinalCode」は、外部との間で安心して顧客データのやりとりが行えるだけでなく、顧客サービスの質向上にも一役買っており、自動暗号化することで、数日かかっていたフローが即日できるようになりました。



CASIO
■ カシオ計算機株式会社

生産性向上

従来、販売店に提供するファイルひとつひとつにパスワードと透かしを入れる作業が手動だったことに対し、「FinalCode」導入後は暗号化フォルダーにファイルを置くだけで暗号化と透かし挿入の処理が自動的に行われるようになり、生産性が向上しました。



SUZUKI
■ スズキ株式会社

スピード感のある導入・展開

顧客や求職者など社外の方とやりとりで利用する個人情報や企業の財務情報などのファイルが追跡可能なので、第三者への転送などの漏洩が事前に防ぐことができます。また、課金対象が従業員のみで展開がスムーズでした。



PASONA
■ 株式会社パソナ

使いやすさを維持したセキュリティ向上

当初目指した通り、エンドユーザーの利便性を一切損ねることなく、ファイル暗号化による情報漏洩リスクを大幅に低減できました。



豊見城市役所

漏洩防止による不安緩和

パスワードロックでは、パスワードが流出したらファイル内の情報を守りきれないため、マイナンバーを保護するには大きな不安がありました。ファイルが事務所外に出ても保護・管理し続けることができるという点で「FinalCode」は必要不可欠なソリューションです。



小泉事務所
■ 社会保険労務士 小泉事務所

デジタルアーツ製品を実際に導入されているお客様の事例をWebサイトでご紹介しています。

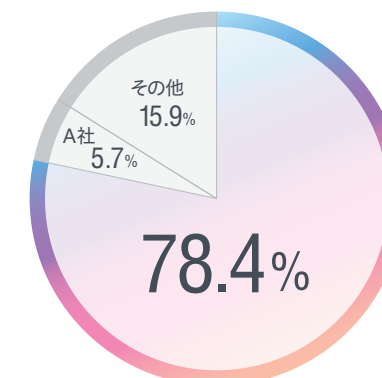
<https://www.daj.jp/bs/case/>

SaaS型(クラウド版)IRM市場で No.1^{※1}の導入実績

ファイル暗号化・追跡ソリューション「FinalCode」は、株式会社アイ・ティ・アールが発行する「ITR Market View:情報漏洩対策市場 2017」において、2016年度のSaaS型IRM市場でベンダー別売上金額のシェア78.4%を占める、デファクトスタンダード製品です。サーバー構築の費用・準備が不要で、すぐに導入できる「FinalCode」は、業界・企業規模を問わず、広くご採用いただいています。

※1 出典:ITR「ITR Market View:情報漏洩対策市場2017」SaaS型IRM市場:ベンダー別売上金額シェア(2016年度)
※2 出典:ITR「ITR Market View:情報漏洩対策市場2015~2017」SaaS型IRM市場:ベンダー別売上金額シェア(2013~2016年度)

SaaS型(クラウド版)IRM市場:ベンダー別売上金額シェア



「ASPIC IoT・AI・クラウドアワード2018」でグランプリを受賞

ファイル管理のセキュリティ対策と工数削減に有効な、導入企業のビジネス加速に大きく貢献する革新的なソリューションであるとの高い評価を得て、グランプリを受賞しました。



海外20か国以上の利用実績、日・英2か国語で表示可能

「FinalCode」は、アメリカ、ヨーロッパ、アジアなどの20か国以上で利用実績があります。ユーザーインターフェースは、日本語・英語の2か国語から表示言語を選択できます。

米国連邦政府標準規格FIPS140-2の認証を取得

「FinalCode」のAES256暗号化モジュールである、クライアント用の「FinalCode Crypto Module」と、モバイル用の「FinalCode Crypto Module for Mobile」は、National Institute of Standards and Technology(米国国立標準技術研究所、NIST)が規定・評価・認定を行っている暗号化モジュールのセキュリティに関する米国連邦政府標準規格「Federal Information Processing Standard(連邦情報処理標準、FIPS) 140-2」の認証を取得しています。

動作環境(対応OS)

FinalCode Client	Windows 8.1 (32bit / 64bit)※ Windows 10(32bit / 64bit)※
FinalCode Reader	iOS 9.3 ~ 13.1 Android 4.1 ~ 4.4 / 5.0 ~ 5.1 / 6.0 / 7.0 ~ 7.1 / 8.0 ~ 8.1 / 9.0 / 10
共有フォルダー自動暗号化モジュール	Windows Storage Server 2012 R2 Windows Storage Server 2016 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019

※ それぞれ日本語、英語に対応しています

主要な動作検証済みアプリケーション

ドキュメント	Microsoft Word, Excel, PowerPoint 2003 / 2007 / 2010 / 2013 / 2016 / 2019 Acrobat® Reader® DC / XI / X Acrobat® Pro DC / XI / X Acrobat® Standard DC / XI / X JUST SYSTEM® 一太郎® Pro / Pro 2 / Pro 3 / 2014 / 2015 JUST Office 3 富士ゼロックス DocuWorks Viewer 7.3 / 8.0 / 9.0 ワードパッド メモ帳
デザイン・画像	Adobe Illustrator CS6 / CC(2017, 2018, 2019) Adobe InDesign CS6 / CC(2017, 2018, 2019) Adobe Photoshop CS6 / CC(2017, 2018, 2019) Microsoft ペイント
動画	Windows Media Player(wma, wmv, avi, mpg, mpeg, mp3, mp4 等)
CAD	AutoCAD® 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016 / 2017 / 2018 / 2019 AutoCAD LT™ 2010 / 2011 / 2012 / 2013 / 2014 / 2015 / 2016 / 2017 / 2018 / 2019 DWG TrueView™ 2013 / 2014 / 2015 / 2016 / 2017 / 2018 / 2019 SolidWorks® 2013 / 2014 / 2015 / 2016 iCADMX V7L6 SolidMX V3.2

* 動作検証済みアプリケーションは順次拡充中。最新情報は弊社Webサイトをご確認ください <https://www.finalcode.com/jp/product/spec/>