



■本書は、2017年8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サイトをご確認ください。■「FinalCode」が導入される機器は Editionごとにより異なります。■Adobe, Acrobat Reader, Illustrator, Photoshop LL, Adobe Systems Incorporated (アドビシステムズ)社の製品です。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特許です。Android は、Google Inc. 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. の子会社、関連会社の登録商標または特許です。Box, Box 107 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 MPAー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、米国およびその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、関連会社の米国およびその他の国における登録商標です。次の社名、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、ActiveRatingSystem、ACTIVE RATING、ZBRAIN、D-SPA、SP Cardie、NET FILTER、m FILTER、m FILTER Masterdier、m FILTER Archive、m FILTER Anti-Spam、m FILTER File Scan、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又は登録商標です。FinalCode はデジタルアーツグループの登録商標です。■その他、本書に記載されている各社の社名、製品名およびサービス名は、各社の商標または登録商標です。■本書に記載されている商標及び商品名等は、所記のためのイメージであり、実際の商標とは異なる場合がございます。本書に記載の内容は予告なく変更することがあります。予めご了承ください。

デジタルアーツ株式会社

www.daj.jp

〒100-0004 東京都千代田区大塚1-5-1 大塚ファーストスクエア ウェストタワー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.finalcode.com

※出版: 2016年6月1日発行「iTR Market View: 情報調査市場調査2016」
「Sales型CRM市場: ベンダー別売上貢献シェア (2015年度)」

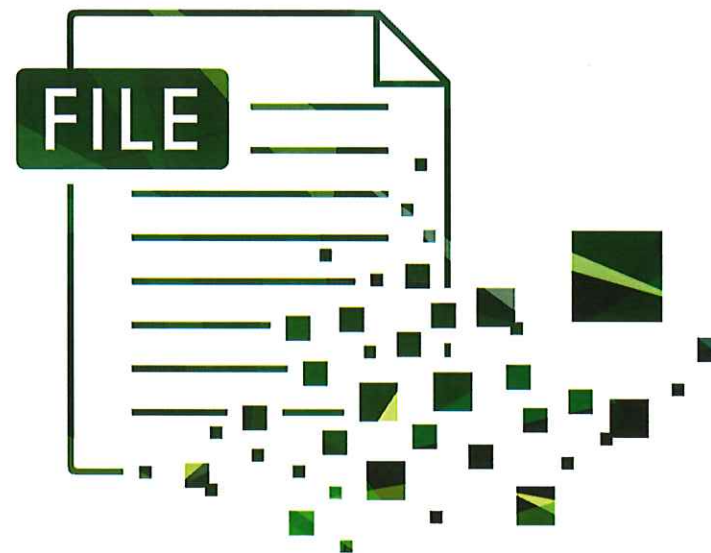
2017/08 P5002469-008



導入実績 No.1* のファイルセキュリティ

FINALCODE®

Ver.5



渡したファイルが“あとから”消せる
魔法のソリューション。

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。

あなたは今日、いくつのファイルを作りましたか？

あなたは今日、いくつのファイルを人に送りましたか？

重要な経営資産である情報は、作られ、共有され、加工されて、また別の人に渡っていきます。

グローバルで分業化が進む今日では、組織や国の境目無く、情報は絶え間無く流通していきます。

このような時代に、安全に情報を扱うにはどうすればよいのでしょうか？

「FinalCode」のアプローチは、普段の業務のなかで情報資産を当たり前を守り、

更には、社内から社外までボーダーレスに守り続けること。

そしていつでも「渡したファイルをあとから消せる」安心感があること。

そんな世界を実現するためのテクノロジーを搭載した「FinalCode」。

あらゆるファイルを守ります。

SaaS型(クラウド版)IRM市場でNo.1[※]の導入実績

「FinalCode」は、SaaS型IRM製品で市場シェア76.7%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、すぐに導入することができるため、業界・企業規模を問わず、広くご採用いただいています。

—— SaaS型(クラウド版)IRM市場：ベンダー別売上金額シェア ——



※ 出典：2015年6月1日現在
「ITR Market View：情報資産管理市場2016」「SaaS型IRM市場：ベンダー別売上金額シェア(2015年4月)」

日本語・英語の2か国語の表示言語

ユーザーインターフェースの表示言語を日・英2か国語から選択できます。他言語についても、順次対応予定です。

海外20か国以上の利用実績

「FinalCode」はアメリカ、ヨーロッパ、アジアなど20か国以上で利用実績があります。不安な海外拠点とのファイルのやりとりについてもサポートします。

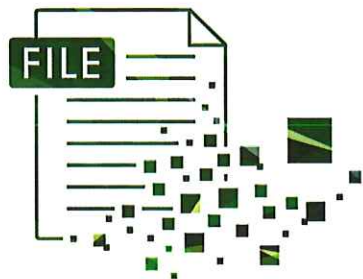


FIPS140-2の認証を取得

「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。



守る



指定した人以外は閲覧不可。
いつでも意のままに権限変更が可能。

- 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



追跡する

ファイルが手元を離れたあとでも、
アクセスログで追跡することが可能。

- アクセスログ確認
- 不正閲覧検知
- 操作ログ確認



あとから消せる

渡したファイルを
“あとから”削除することが可能。

- リモートファイル削除
- リモート権限変更

FINALCODE[®] Ver.5

指定した人やグループのみ閲覧でき、

アクセス履歴が完全に追えて、

渡したあとでも権限変更可能。

しかも、いざとなれば“あとから”消せる、

究極のファイルセキュリティ。

高度なテクノロジーで暗号化

通信セキュリティとしてRSA-2048、暗号化アルゴリズムとしてAES256を採用。高度な暗号化技術により、安全にファイルのやり取りを行うことが可能です。

※ FIPS180-2の認証取得済み

セキュリティポリシーの設定

ファイルの用途、機密性に合わせ、閲覧・編集・印刷可否など、きめ細やかなセキュリティポリシーをファイルごとに設定できます。

ユーザビリティ

パスワードレス暗号化技術により、ダブルクリックするだけで暗号化ファイルを開封し、いつものアプリケーションで、いつものようにファイルを開覧・操作できます。



ファイルの利用履歴を集中管理

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た都度、ログを取得します。不適切な権限設定も見逃しません。

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。



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。

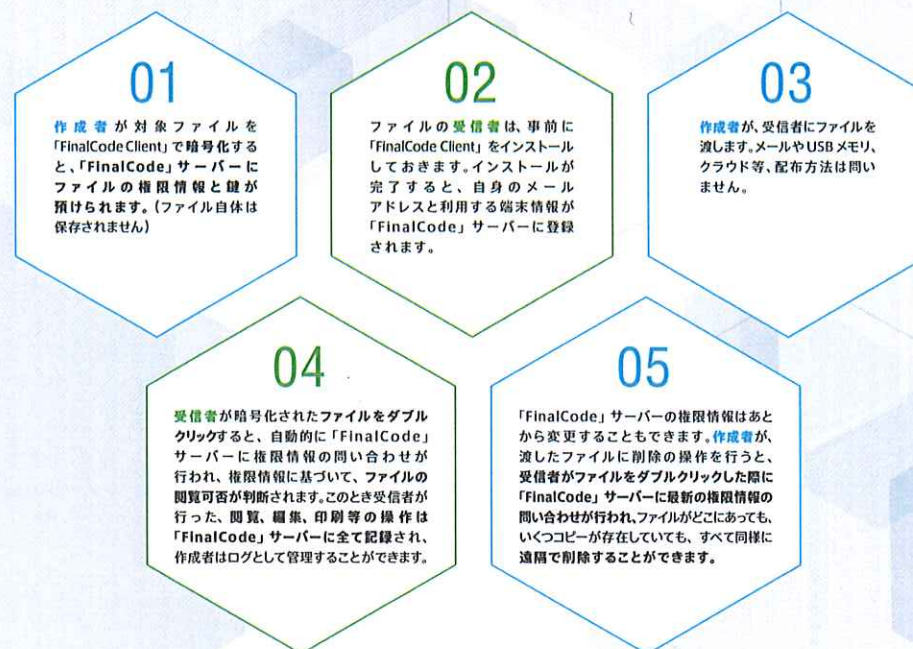
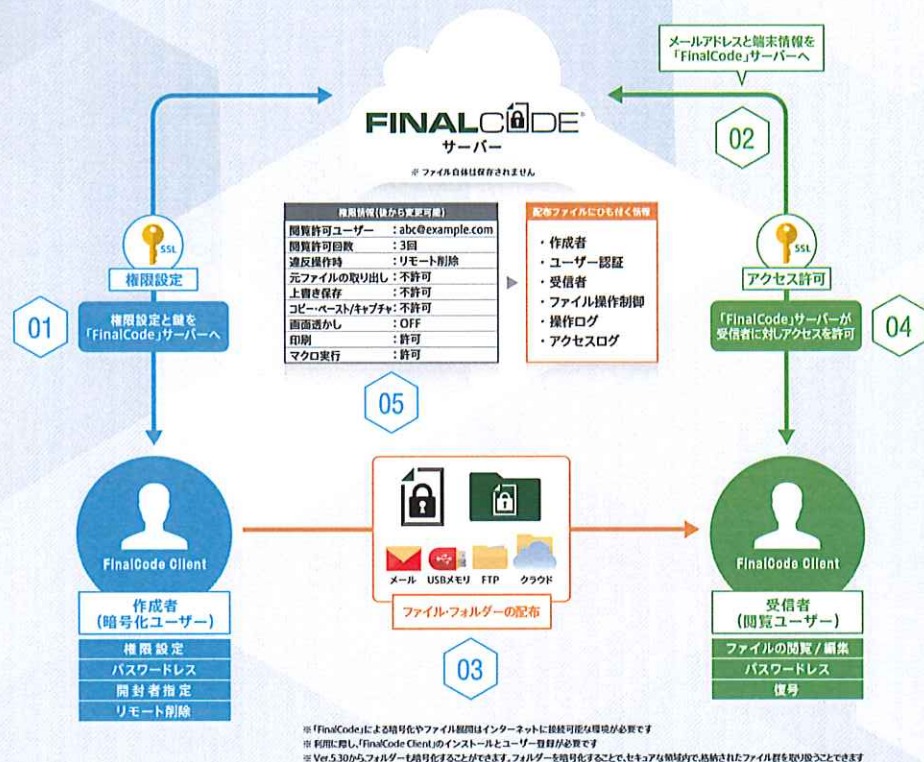
いざとなったらリモートで消せる

人に渡したファイルをリモートで跡形も無く消すことができます。万が一、機密ファイルが流出しても、中の情報は漏らしません。



魔法のようなソリューション。実は、タネも仕掛けもあります。

世界各国で特許取得済み



「FinalCode」のもうひとつの魅力、導入のしやすさで選ばれています。

01 Microsoft Active Directory (AD) との、より強固な連携

「FinalCode Client」の初回登録時の認証方法として、統合Windows認証やSAML認証もご利用いただくことができます。また、ADの設定情報を「FinalCode」に反映できるため、メンテナンスはADのみで済み、「FinalCode」での更新が不要です。



02 シンプルなライセンス形態

取引先や委託先など、企業・団体外の閲覧するだけのユーザーは無償

「FinalCode」を使用する「企業・団体内」ユーザー数^{※1}のライセンスをご購入ください。暗号化ファイル閲覧するだけの「企業・団体外」ユーザー^{※2}には、費用はかかりません。

※1 本社保有が既済の状態で独自ドメインを持つメールアドレスのユーザー、当該ドメインを持つメールアドレスを有して認証する「FinalCode」ユーザーは、「企業・団体内」ユーザーとして「FinalCode」にカウントされています。また、当該ユーザーが作成した「FinalCode」ファイルも閲覧することができます。 ※2 「FinalCode」に登録されたドメインと異なるドメインのメールアドレスを持つユーザーです

03 フレキシブルな導入形態ですぐにスタート

SaaS(クラウド版)

VA[®](オンプレミス版)

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。

自社サーバーで運用可能

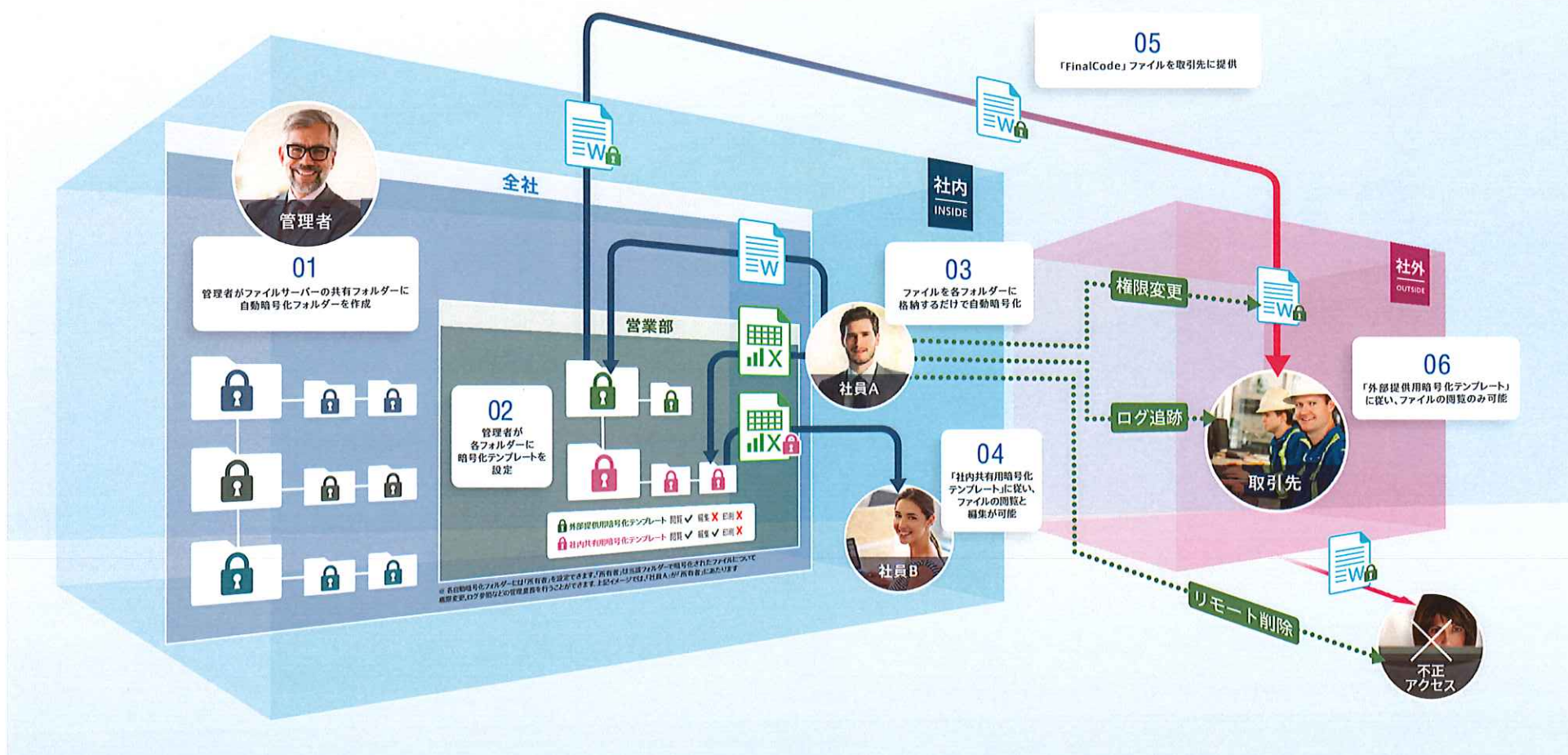
自社で独自にサーバー構築していただくことができます。すべてを社内で完結したい場合に適しています。

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

ボーダーレスなセキュリティで、情報資産 がどこにあってもコントロールし続けます

- 01 管理者は、ファイルサーバー上の共有フォルダーに暗号化テンプレートを設定することで「自動暗号化フォルダー」を作成します。
- 02 企業・団体内で共有するファイルを暗号化するには、社員・職員のみ閲覧権限を設定した暗号化テンプレートを使用します。
また、企業・団体の外部取引先にファイルを提供するためには、取引先を閲覧者として指定した暗号化テンプレートを使用します。
- 03 社員・職員はフォルダーに投入するだけで、フォルダーに設定された暗号化テンプレートに沿って、ファイルが自動的に暗号化されます。

- 04 社員・職員は「社内共有フォルダー」内の暗号化ファイルを開覧・編集することができます。
- 05 企業・団体の外部にファイルを提供するときは、外部提供用のフォルダー内のファイルを「そのまま」取引先に渡すだけ。
- 06 取引先は、外部提供用の暗号化テンプレートに基づき、閲覧のみが可能となるようにファイル操作が制限されます。万が一、取引先からファイルが流出し、閲覧権限が無いユーザーに暗号化ファイルが渡っても、自動でファイルが削除されるので安心です。



目的に合わせて機能を追加できる「FinalCode Express Edition」

Express Edition

「FinalCode Express Edition」は、ベースとなる「FinalCode」の基本機能にさらに必要なオプションを追加していく「アラカルト方式」でご購入いただくことができます。必要な機能を、必要なときに追加することが可能なため、将来的なニーズの変化や従業員数の増加にも、柔軟に対応することができます。まずは「あの課のあのファイルから」という導入に最適です。

- のオプションは、「FinalCode Express Edition」のユーザー数と同数をご購入ください
- のオプションは、各機能を利用されるユーザー数分をご購入ください
- のオプションは、ユーザー数に関係なく年額のご購入となります

OPTION

共有フォルダー自動暗号化機能

共有フォルダーにファイルを入れるだけで自動で暗号化。運用の手間を省きます。

OPTION

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。

OPTION

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。

OPTION

削除・不正通知機能

手元を離れたファイルについても、リモート削除、不正アクセス通知を実現します。

OPTION

大規模運用機能

大規模な運用に合わせて、基本機能を大幅にグレードアップすることができます。

※「FinalCode API」オプションを組み合わせ

OPTION

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。

OPTION

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。



ご利用シーン USE CASE

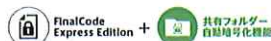


Case 01 標的型攻撃によってファイルが盗まれるのが心配...



ゲートウェイでのセキュリティ対策だけでは標的型攻撃から情報を守りきることはできません。「共有フォルダー自動暗号化機能」によって社内の全てのファイルがもれなく暗号化されていれば、万が一ファイルが流出しても、大切な「情報」が漏洩することはありません。

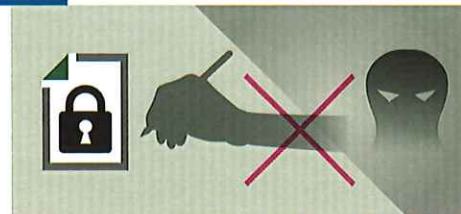
▼これで解決



必要とする企業・部門 業種・業界・企業規模の大小を問わず守るべきファイルが存在するすべての部門、PマークやISMS取得企業など

守るファイル 経営情報、社員個人情報、顧客情報、知財特許・機密情報、生産計画、研究データ、取引先から預かった情報など

Case 03 データの不正改ざんに備えたい



見積り、売上、実験データ、臨床データなどの改ざんは企業の信用失墜を招きます。「FinalCode」は、データを保全する仕組みとともにファイルへの操作履歴を残すことができます。

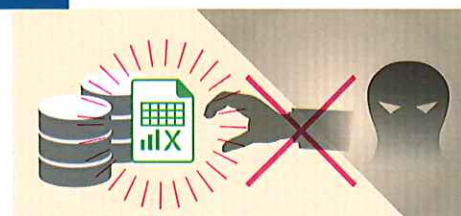
▼これで解決



必要とする企業・部門 銀行、証券、機械、化学、食品、精密機器、製薬、建設、公営、医療、農業などデータの信頼性が重要な企業

守るファイル 見積り、売上、与信情報、実験・測定・観測データ、設計データ、製造データ、レシピ、臨床データなど

Case 04 社内システムのデータも守りたい



社内システムのデータベースに格納されたデータは、多くの場合ひとたび抽出されてしまうと無防備な状態のファイルに書き出されてしまいます。「FinalCode API」を利用すれば、書き出されたファイルを自動的にAPIで暗号化することができます。

▼これで解決



必要とする企業・部門 Oracle®、Microsoft、Salesforce、SAP®、Marketo®等の各社のデータベースやERP、CRM、マーケティングツールを利用している企業のデータ抽出を行う部門

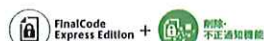
守るファイル データベースから抽出され、CSVなどの形式でファイルに保存された売上情報、個人情報、顧客情報、与信情報、人事給与情報など

Case 02 退職者や内部不正による漏洩が心配...



退職者の持出し、金銭を目的とした情報売買など、悪意ある犯行によって、企業・団体が甚大な損失を出す事件が多発しています。「削除・不正通知機能」を利用すれば、外部に持ち出されたファイルをリモートで削除することができるため、安心・安全です。

▼これで解決



必要とする企業・部門 業種・業界・企業規模の大小を問わず、経営部、営業部、経理部、人事部、研究開発部、企画部、知財部、コールセンター、支社、営業所

守るファイル 社外秘、社員情報、顧客情報、知財特許・機密情報、研究データ、公開前のIR情報など、競合や市場で買手がつく情報

Case 05 Box を安心できる状態で活用したい



Box で社内外とファイルを共有する際、Box からダウンロードされた後のファイルも守る必要があります。「Box 連携機能」を利用すれば、Box にアップロードしたファイルを自動暗号化し、ダウンロード後のファイルの追跡と、コラボレート設定と連動した権限制御を可能にします。

▼これで解決



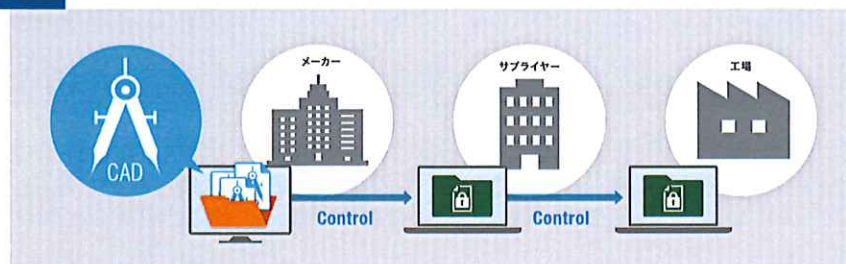
必要とする企業・部門 Box をご利用または検討されている企業

守るファイル Box に格納して、社内外と共有する重要な情報

Case 06

取引先から、設計ファイルが漏洩しないか不安... [製造 / 建設]

特許出願中



大切な図面ファイルも、取引先からさらに別の取引先へとデータが拡散するほどセキュリティガバナンスは薄れていきます。「FinalCode」は、プロジェクトで扱う図面ファイル群を「セキュアコンテンツ」として保護し、セキュリティポリシーをコントロールできます。「セキュアコンテンツ」として共有することで、管理性を高め、拡散した先でもセキュリティガバナンスを維持することが可能です。

▼ これで解決

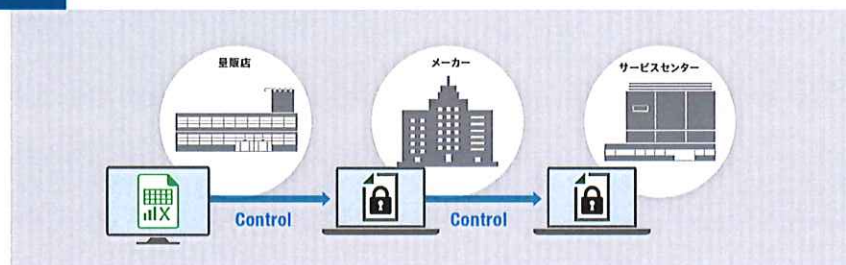


必要とする企業・部門 製造業、建設業、それにかかわる取引先、企業規模の大小を問わず営業部、研究部、設計部、生産管理部、資材調達部、知財部など

守るファイル 設計仕様書・部品仕様書、システム設計図、デザイン図、回路図などの図面、技術資料、調達仕様書、取引先から預かった資料など

Case 07

取引先との顧客情報のやりとりで常に漏洩リスクがつきまとう... [流通 / 小売 / 運輸 / 公益業]



主に個人情報が入り込んでいる業界、企業群において、情報の紛失、盗難、持取を防止するのは、喫緊の課題です。「FinalCode」は、渡したファイルがどこにあって、いつでも追跡、操作、万が一のリモート削除が可能です。

▼ これで解決



必要とする企業・部門 流通業、小売業、運輸業、公益業、通信業、その他サービス業とそれにかかわる取引先、サービス部、ロジスティクス部、コンタクトセンター、業務支援部、管理部など

守るファイル 個人情報、顧客情報

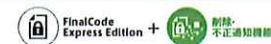
Case 08

人的 / 管理ミスによる漏洩が心配...



メール誤送信、パスワード設定忘れ、USB紛失、印刷物放置など、ミスによる情報の漏洩は完全に防ぐことはできません。「FinalCode」は、ファイルの閲覧者、操作権限を設定することができ、いざとなったらリモート削除もできるため、万が一ファイルが流出しても「情報」の流出を食い止めることが可能です。

▼ これで解決

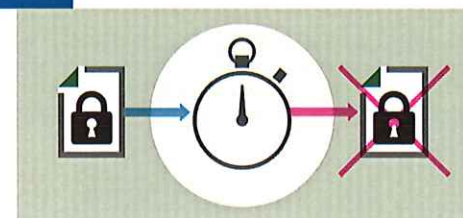


必要とする企業・部門 業種・業界・企業規模の大小を問わず守るべきファイルが存在するすべての部門、PマークやISMS取得企業など

守るファイル 情報を漏洩してしまった場合、会社および委託元や取引先にとっても、計り知れないほどの大きな影響と損害を与えてしまう情報

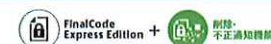
Case 09

取引先が渡したファイルを廃棄したか心配...



RFP、電子カタログ、NDAのもと開示した情報などは、期限を超えたら回収または廃棄の必要があります。「FinalCode」は、指定期限以降は自動的に閲覧不可にしたり、任意のタイミングでリモート削除も可能で、仮に不正操作が行われた際にはすぐに通知が届くので安心です。

▼ これで解決

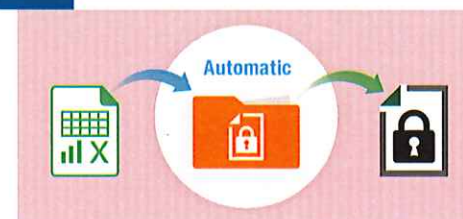


必要とする企業・部門 業種・業界・企業規模の大小を問わず、研究開発部、情報システム部、総務部、販売部、DTP部など配布物の製作および管理部門

守るファイル RFP、電子カタログ、NDAのもと開示した情報など有効期限付きの情報、期限を超えても参照されると諸問題や事故となる恐れのある情報

Case 10

自治体のセキュリティレベルを上げたい



ネットワーク分離だけでは、住民情報の漏洩を100%防ぐことは困難です。「共有フォルダー自動暗号化機能」を利用し、すべてのファイルを自動的に暗号化することにより、自治体内のセキュリティレベルを上げることができます。

▼ これで解決



必要とする企業・部門 自治体、官公庁、学校、教育機関

守るファイル 業種・業界・企業規模の大小を問わず、研究開発部、情報システム部、総務部、販売部、DTP部など配布物の製作および管理部門

01 多様な設定により、きめ細やかな暗号化が可能

基本のIRM[®]機能【ファイルごとの閲覧者指定、操作権限設定が可能】

「FinalCode」は、ファイルに閲覧者や操作権限を設定した上で暗号化します。万が一、暗号化ファイルが閲覧権限のないユーザーの手に渡ってもファイルは開封されないため、情報漏洩の心配はありません。ファイルの操作権限として閲覧期限・回数、コピー・ペースト/キャプチャなどの制御が可能で、ファイルの閲覧者や用途などによって柔軟に設定することができます。

© Information Rights Management: 文書ファイルを暗号化し、閲覧や編集を制限したり印刷・操作権限を設定することができるソフトウェア



最終画面

権限詳細

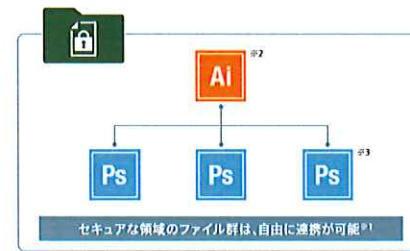
閲覧期限・回数	日時制限、日数制限、回数の3種類から選択し、設定することができます。
元ファイルの取り出し	暗号化前の元ファイルの取り出し可否を制御します。
上書き保存	暗号化ファイルのまま、編集、上書き保存を制御します。
コピー・ペースト/キャプチャ	ファイル内の情報のコピー・ペーストや画面キャプチャを制御します。
画面透かし	暗号化ファイルの閲覧時に、画面上に表示されるデータに透かしを追加することが可能です。透かしの文言として、ユーザー名、印刷日時、PC名などを表示することができ、スクリーンショットデータ流出の防止力となります。
印刷(透かし印刷)	ファイルの印刷を制御します。また、印刷した文書に透かしを追加することが可能です。透かしの文言として、ユーザー名、印刷日時、PC名などを表示することができ、印刷物流出の防止力となります。
マクロ実行	暗号化ファイルにマクロが含まれている場合、その実行を制御します。
ファイルの所有権譲渡	暗号化ファイルの権限を付け直す機能です。暗号化ファイルの受取者は、自分が所有者となる新たな暗号化ファイルを複製し権限を設定直すことができます。
テンプレート生成機能	カスタム設定の内容を保存し、自動でテンプレートを作成する機能です。
複数権限設定	ファイル閲覧者・操作権限の組み合わせ(権限セット)を、1つのファイルに複数設定できます。

セキュアコンテナ【業務で利用するフォルダーそのものを暗号化】 特許出願中

「セキュアコンテナ」は、重要ファイルが格納された「フォルダーそのもの」を暗号化し、セキュアにする機能です。フォルダーを監視し、ファイルを1つ0とつ自動暗号化する「共有フォルダー自動暗号化」機能とは異なり、フォルダーを1つのセキュアな領域として保護します。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。また、業務に関連するファイルをセキュアコンテナとしてシンプルに共有することができるため、セキュリティレベルを下げることなく管理性を向上します。



※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



セキュアな領域のファイル群は、自由に連携が可能^{※1}

共有フォルダー自動暗号化^{※1}【情報が集まるファイルサーバーを監視】

「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入れるだけ。特別に意識することなく、ファイルを守ることができます。



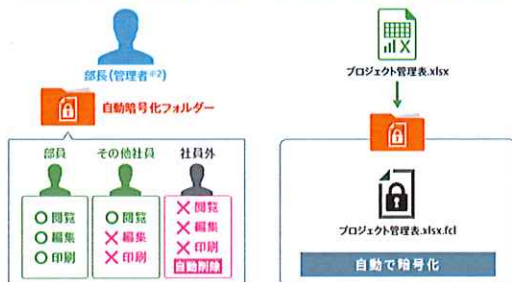
設定画面(専用メニュー)

※1 共有フォルダー自動暗号化モジュールをファイルサーバーにインストールし、当該モジュール専用の設定画面から暗号化を行います ※2 当該フォルダー内で暗号化されたファイルの所有権として権限変更やログ監視が可能です

自動暗号化手順

01 管理者「権限テンプレートをひも付ける」

02 部員「自動暗号化フォルダーに格納する」

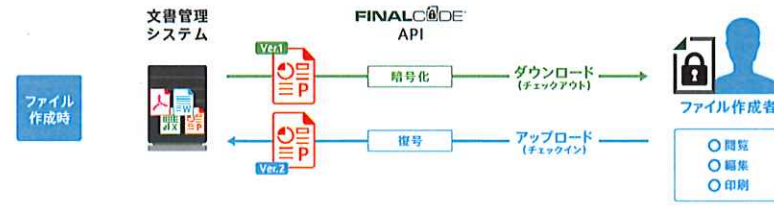


APIで外部システムと連携【業務を変えずにセキュアな運用】

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(FinalCode API[®])を提供しています。システムが自動で暗号化・復号するので、ユーザーが意識することなくご利用いただくことが可能です。

ダウンロードやアップロードする際に自動で暗号化・復号

「FinalCode API」を利用することで、文書管理システムからダウンロードする際に自動暗号化する仕組みを構築できます。これにより、ユーザーの手間を増やすことなく、文書管理システムの外部でもファイルを守ることが可能になります。また、アップロード時に自動復号することにより、文書管理システムの運用にも影響を与えることはありません。

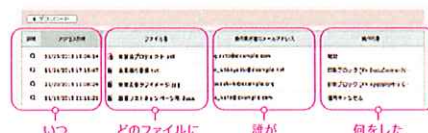


※ ファイルの暗号化や復号、権限の変更など、利用者が最終「FinalCode Client」や管理画面を通じて行う主要な操作を、コマンドラインから行うためのツールです

02 ファイルがどこにあっても守り続けます

ファイルがどこにあっても利用状況を把握【ファイル所有者によるログ監視】

「FinalCode」はファイルがどこにあっても、リアルタイムでファイルへのアクセスログを集中管理することが可能です。



暗号化ファイルをそのまま組織外に提供【間接(二次)漏洩の防止】

企業・団体外に出たファイルを守り、リモート削除可能

「FinalCode」で暗号化したファイルは、企業・団体の中でも外でも同じようにIRM制御を効かせることが可能なので、渡した相手から自社のファイルが漏れてしまう間接(二次)漏洩の対策にご利用いただけます。例えば、図面や仕様書、個人情報など、自社の情報資産を取引先や海外拠点に提供する場合でも、「FinalCode」で暗号化したままメールやクラウドストレージ、ファイル転送システムなどで渡すことができ、渡したあとも守り続けます。



「プッシュ型」の不正アクセス通知

不正アクセスがあった場合は、ファイル所有者に対して自動でメール通知するので、漏洩リスクを即時検知することができます。

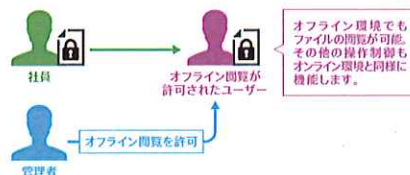
不正アクセスの例
・閲覧者に設定されていないユーザーによる暗号化ファイルの閲覧操作
・「閲覧自動・拒否」を超過した暗号化ファイルの閲覧操作



オフライン環境でも閲覧可能【場所を問わないセキュリティ】

工事や建設の現場、飛行機での移動中など、インターネット環境がない場所でも、暗号化ファイルを閲覧したいことはあります。「FinalCode」は、オフライン環境でもパスワードで暗号化ファイルを開けるように設定することが可能です。また、オンラインと同様にIRM制御を行うことができます。

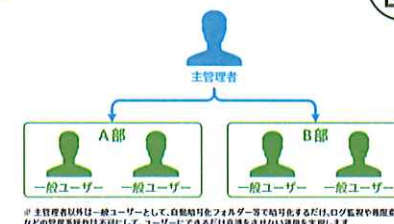
※ オフライン環境下での操作ログは、オンライン環境に戻った後、「FinalCodeサーバー」に送信されます。オフライン時に実行された権限変更やリモート削除処理は、その権限変更が初めてオンライン環境で実行されたときにシステムで適用されます。※ 100% 遠隔操作で暗号化されたファイルについては、本機でも閲覧はできません。オフラインが許可されたユーザーであっても、「FinalCode Reader」によるオフライン閲覧はできません。



03 組織構造や役割・役割に応じ、管理体制やセキュリティポリシーを柔軟に設計

AD連携と閲覧者指定【管理コストを削減】

暗号化ファイルの閲覧者として、ADに設定されているメールアドレス、メーリングリスト、OU、セキュリティグループだけでなく、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。ADとの連携強化により、異動・退職等に伴うメンテナンスはADのみで済み、「FinalCode」での更新が不要です。大規模導入のお客様も手間をかけずに運用することができます。管理者権限をシステム担当に集約し、ユーザーは決められたテンプレートで、あるいは自動暗号化フォルダーで暗号化するだけ。ユーザーの業務変化が少なく、シンプルな運用です。

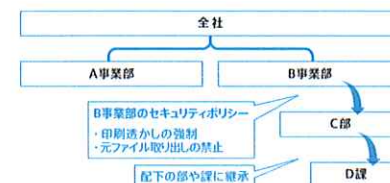


※ 主管理者以外に一般ユーザーとして、自動暗号化フォルダー等で暗号化するだけ、ログ監視や権限変更などの管理業務は許可して、ユーザーにできるだけ負担を軽減を実現します。

組織階層の定義【ガバナンス強化を支援】

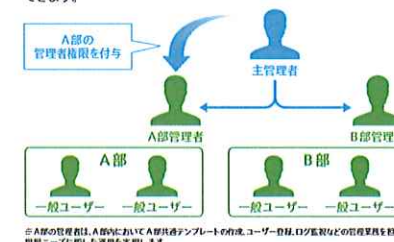
組織階層の定義と権限設定

権限の設定をおこなう際に、組織階層を定義します。また、AD連携することで、「FinalCode」の組織階層をOUで定義することも可能になります。組織階層を定義することで、セキュリティポリシーを配下の部や課に継承できます。シンプルな運用で情報セキュリティ責任者による統制を支援します。



管理者権限の委譲により、組織ごとに最適な運用を

管理者権限を各組織の担当者に委譲し、管理者を複数体制に、各組織の業務特性を考慮しながら、組織に合ったセキュリティを適用することができます。



※ A部の管理権限は、A部においてA部担当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い、現場ニーズに応じた運用を実現します。

ユーザー権限の定義【ユーザーの暗号化業務を統制】

管理者はユーザー登録の際、各ユーザーに権限レベルを割り当て、組織内における暗号化業務を統制できます。既定の権限レベルのほか、ユーザーごとの権限付与など柔軟な対応も可能です。さらにAD連携することで、ADのセキュリティグループ設定で「FinalCode」の権限レベルに反映できます。

※ 各種権限レベルとも、自動暗号化フォルダーでの暗号化が可能です。※ 閲覧画面ではログ監視や権限変更・削除等の操作が可能です。

権限レベル(ユーザータイプ)例

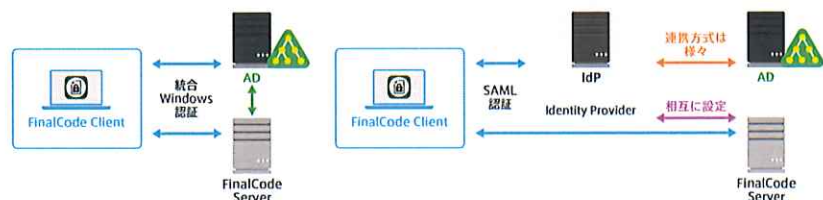
管理者	管理組織内ユーザーが作成した暗号化ファイルの閲覧、ログ監視が可能
監査者	暗号化、管理画面の利用が可能 / 管理組織内のログ監視が可能
標準ユーザー	暗号化、管理画面の利用が可能
制限ユーザー	テンプレートによる暗号化のみ可能 / 管理画面は利用不可
閲覧ユーザー	閲覧・編集のみ可能

04 利便性や利用シーンをさらに拡大する「FinalCode」の機能・サービス

選べる認証方法と、AD連携によるシームレスな導入

統合Windows認証、SAML認証対応

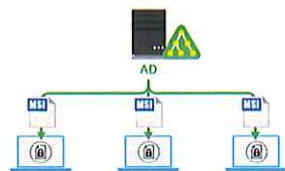
「FinalCode Client」の初回登録時の認証方法として、統合 Windows 認証や SAML 認証もご利用いただけます。



シームレスな導入を実現

AD連携することで、ユーザーが利用中のWindows PCにログインした際に自動で「FinalCode Client」をインストールすることができます（MSIの機能を利用）。さらに統合Windows認証もサポートし、メールアドレスを利用していない環境にも「FinalCode」が導入しやすくなりました。このように、リモートで一括インストールや認証ができ、ユーザーはOSを起動するだけで「FinalCode」のセットアップがスムーズに完了します。

※ インストール後、各ユーザーはメールアドレスの登録及び承認のため、ワンタイムパスワードでの認証を行う必要があります



個人のPCでも自動暗号化

各ユーザー自身が個人のPCで自動暗号化フォルダーの設定をすることが可能です。（ローカルフォルダー自動暗号化機能）暗号化作業の効率化、ミスの防止に役立ちます。なお、「ネットワークドライブの割り当て」を行うことで、ネットワーク上のフォルダーの自動暗号化設定を行うことも可能になります。^{※1}

01 自動暗号化フォルダーに保存する



02 設定された権限（テンプレート）で自動暗号化



※1 複数のユーザーから同一のフォルダーに対して自動暗号化設定をしないください
 ※2 自動暗号化フォルダーは、ユーザーのドライブにあり、最大15GBまで管理することができます（例：ユーザーで3デバイスご利用の場合、最大45GB）

iOS/Android™でも閲覧可能

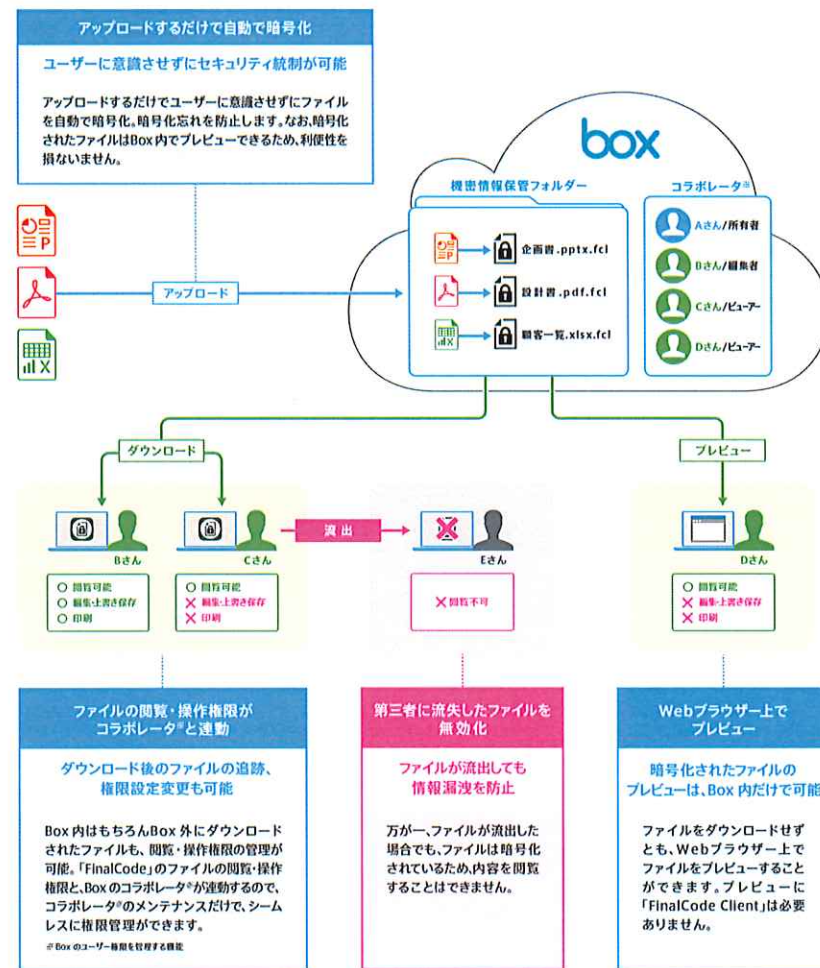
業務で利用するiOS/Android™のモバイル端末に、閲覧専用アプリ「FinalCode Reader」をインストールすると、「FinalCode」で暗号化されたPDFファイルを開覧することができます。また、もしもときは、端末にダウンロードされたファイルは遠隔で「あとから」削除することができるので、ファイルを提供した相手から間接（二次）漏洩のリスクを抑えることができます。



05 Box からダウンロードされたファイルに最高の安心を

「Box 連携オプション」で、より安全な情報資産の共有を

Box は強固なセキュリティ機能や管理機能を備えており、クラウドストレージ内の環境がセキュアに保たれていますが、いったんファイルがダウンロードされてしまうと管理は及ばなくなります。しかし、「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。



06 大規模組織の運用にも対応した充実の機能

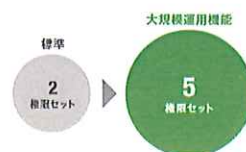
基本機能を拡充し大規模運用に対応

大規模運用に最適な充実の機能

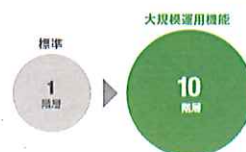
「大規模運用機能」オプションは、暗号化ファイルを閲覧することができるデバイスの、IPアドレスを制限する「IP制限設定」や、「FinalCode Client/Reader」を利用できるデバイスを、そのデバイスのOSの種別およびMACアドレスから指定できる「デバイス制限設定」など、厳しいセキュリティ要件に対応した機能を提供します。

「FinalCode Express Edition」標準機能との性能比較

「大規模運用機能」オプションは、「FinalCode Express Edition」標準機能で利用できる数値性能が拡張されているほか、標準機能にはない設定や機能が利用可能です。

1ファイルに設定可能な
権限セット数1ファイルに設定可能な
閲覧者数上限値

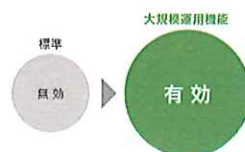
組織階層数の上限値



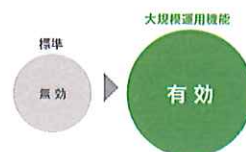
利用できるユーザータイプ



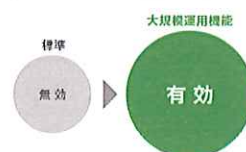
IP制限設定



デバイス制限設定



統合ログ管理連携



FinalCode API



製品エディション

EDITION

「FinalCode Express Edition」は、お客様のあらゆるニーズに対応できるパッケージです。
シンプルな運用に適した「Business Edition」、すべての機能が利用できる「Enterprise Edition」と合わせ、
用途に応じて3つのエディションからお選びください。

製品エディション

	FinalCode Express Edition	FinalCode Business Edition	FinalCode Enterprise Edition
月額	¥1,000/ライセンス/月(年割あり)	¥2,000/ライセンス/月(年割あり)	¥3,600/ライセンス/月(年割あり)
導入形態	SaaS	VA (Virtual Appliance)	SaaS
最低購入ライセンス*	10ライセンス	10ライセンス	50ライセンス
暗号化基本機能	標準	標準	標準
削除・不正通知機能	オプション	標準搭載	標準搭載
共有フォルダー自動暗号化機能	オプション	—	標準搭載
大規模運用機能	オプション (はFinalCode API)	—	標準搭載
Box連携機能	オプション	オプション	オプション
CADファイル暗号化・閲覧機能	オプション	オプション	オプション
オフライン閲覧機能**	オプション	オプション	オプション
FinalCode API	オプション	オプション	標準搭載

*1ご購入ライセンス単位は1ライセンスとなります。*2「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。

オプション価格

共有フォルダー 自動暗号化機能	削除・不正通知 機能	大規模運用 機能	Box 連携 機能	CADファイル 暗号化・閲覧機能	オフライン 閲覧機能	FinalCode API
¥500/ライセンス/月	¥600/ライセンス/月	¥1,500/ライセンス/月	¥300/ライセンス/月	¥500/ライセンス/月	¥500,000/年	¥2,000,000/年

課金対象は企業・団体内のユーザーのみ。取引先や委託先など、外部の閲覧するだけのユーザーは無償です。

暗号化ファイルを閲覧する「企業・団体外」ユーザーに費用はかかりません。*「FinalCode」に接続されたドメインとは異なるドメインのメールアドレスを付与するユーザー

動作環境(対応OS)

FinalCode Client	Windows 7 (32bit/64bit) ** Windows 8.1 (32bit/64bit) ** Windows 10 (32bit/64bit) ** macOS Sierra 10.12 **
共有フォルダー自動暗号化 モジュール	Windows Server 2008 R2 Windows Server 2012 R2 Windows Storage Server 2012 R2 Windows Server 2016

*1それぞれ日本語、英語、中国語に対応しています。*2 Windows版クライアントと比べ
利用できる機能に一部制限があります。詳細は下記URLよりご確認ください
<http://www.finalcode.com/jp/ftp/m31705/jst.php>

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 Acrobat® Reader® DC/XI/X, Acrobat® Pro DC/XI/X, Acrobat® Standard DC/XI/X JUST SYSTEMS™ 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, ワードパッド, メモ帳
デザイン・画像	Akobe Illustrator CS6/CC (2017), Adobe Photoshop CS6/CC (2017), 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 AutoCAD LT™ 2010/2011/2012/2013/2014/2015/2016 DWG TrueView™ 2013/2014/2015/2016 SolidWorks® 2013/2014/2015/2016

* 動作検証済みアプリケーションは販売契約中、最新バージョンに下記URLよりご確認ください
<http://www.finalcode.com/jp/product/pec/>