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”

デジタルアーツ株式会社

アジェンダ

情報セキュリティの脅威

重要情報をメールで送受信するなど、インターネットを介したビジネスのやり取りが当たり前となっている現在、
企業・団体が保有している情報資産は、不正な持ち出し、紛失、取引先からの二次漏洩、マルウェア攻撃、
サプライチェーン攻撃といったリスクが絶えずつきまとっています。

順位 ※( )内は前年順位	情報セキュリティ10大脅威2024(影響を受ける対象:組織)
1位(1位)	ランサムウェアによる被害
2位(3位)	サプライチェーンの弱点を悪用した攻撃
3位(4位)	内部不正による情報漏洩
4位(3位)	標的型攻撃による機密情報の窃取
5位(6位)	修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
6位(9位)	不注意による情報漏えい等の被害
7位(8位)	脆弱性対策情報の公開に伴う悪用増加
8位(7位)	ビジネスメール詐欺による金銭被害
9位(5位)	テレワーク等のニューノーマルな働き方を狙った攻撃
10位(10位)	犯罪のビジネス化(アンダーグラウンドサービス)

※出典:IPA「情報セキュリティ10大脅威2024」
https://www.ipa.go.jp/security/10threats/10threats2024.html

【ご参考】サプライチェーン攻撃とは

セキュリティ対策が脆弱なサプライチェーンの取引先企業(グループ企業、委託先企業など)を狙った攻撃

01

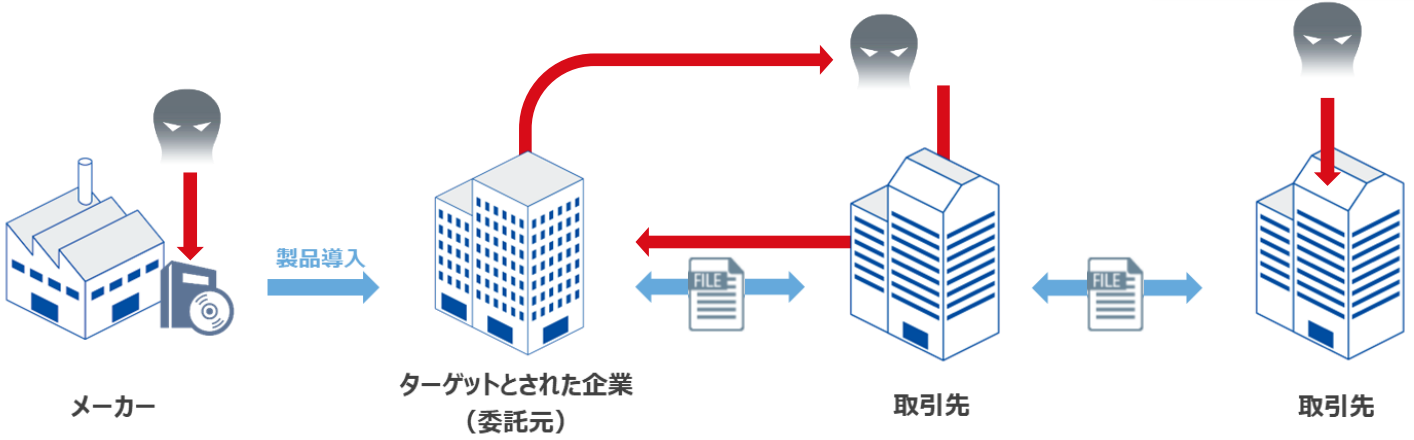
IT機器やソフトウェアの製造過程で、製品や更新プログラム等にマルウェアを仕込んで感染させる

02

取引先を攻撃し、それを足がかりにターゲットとする企業に侵入する

03

取引先からターゲットとする企業の情報を抜き取る



【ご参考】ゼロトラストセキュリティとは

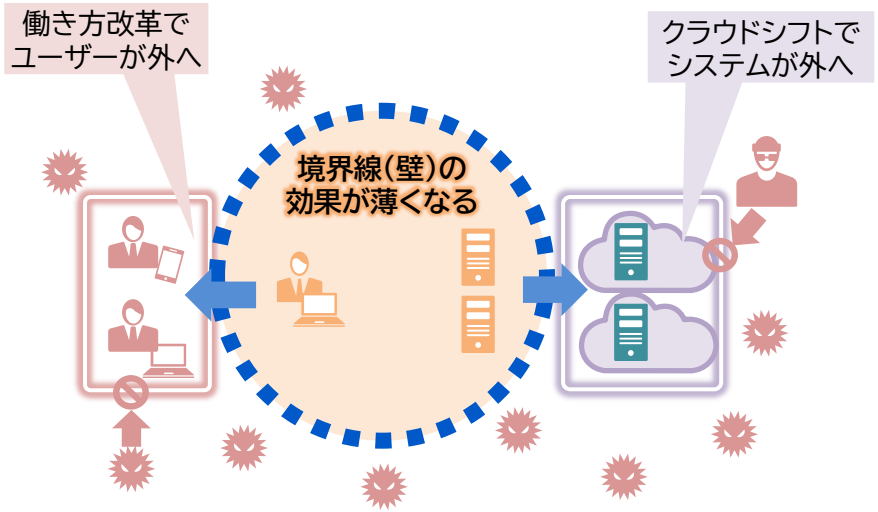
信頼できないことを前提として、セキュリティ対策を講じていくセキュリティモデル

従来

情報資産・従業員は、境界線の中

クラウド時代

情報資産・従業員は、あらゆる場所



従来の対策では守り切れない：運用面

必ずパスワードを
付けるようにしている

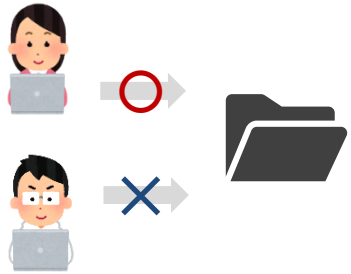
Password
○×△■×●◎▽

- パスワードごと
  誤送信してしまったら？
- ファイルの受信者が
  その後・・・

セキュリティ研修を行い
ルールを設ける

- 全員が厳密に守れて
  いますか？
- 外部攻撃で意図せず
  漏洩してしまったら？

適切なアクセス権限
管理をしている

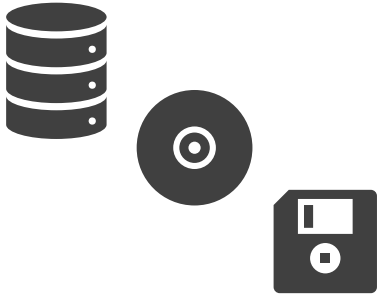


- フォルダから外に
  持ち出された後は？
- アカウントが
  乗っ取られた場合は？

従来の対策では守り切れない:システム面

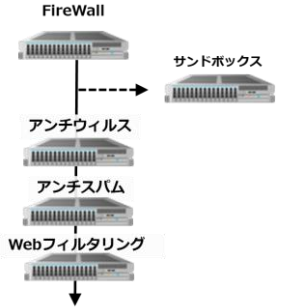
DigitalArts

データベース・HDDを
暗号化している



- データベースから
  出力した後は・・・
- データ廃棄が不十分
  だった場合は・・・

多層防御を
設けている



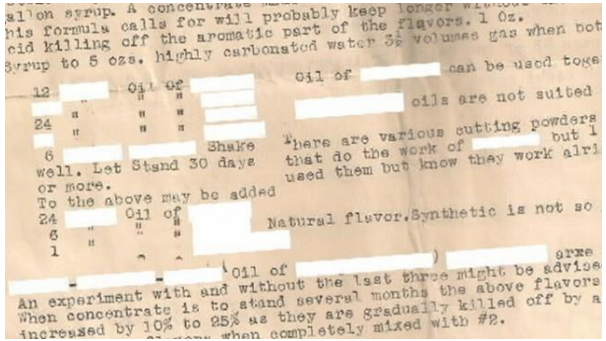
- 新種のウイルスが
  現れたら？
- 社外に渡した情報から
  漏洩してしまったら？

シンクライアントを
導入している

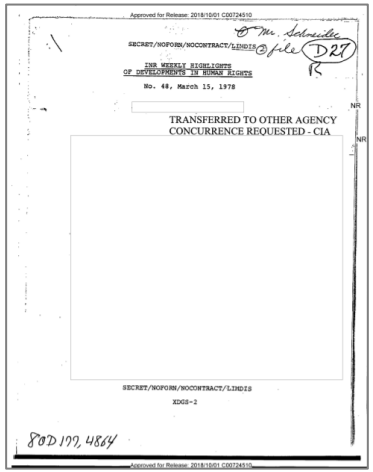
- メール誤送信して
  しまったら？
- シャドーITによる個人宛メールや
  クラウドストレージに保存されたら？

ゼロトラスト時代の情報漏えい対策

コカ・コーラ社：レシピ



CIA：大統領向けレポート



Microsoft 365にバンドル

グローバルでは、IRMの利用がスタンダードに

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

（類似概念）

DRM:Digital Rights Management

デジタル著作権管理。
マルチメディアコンテンツの著作権保護を目的としたソフトウェア

IRMの日本市場動向

情報漏洩対策としてのニーズが高まり、2018年度は前年度比17.2%増と好調に推移。マイクロソフトの急成長が市場を牽引し、シェアを拡大

- 国内IRM市場の2018年度の売上金額は65億4,000万円、前年度比17.2%増と好調に推移した（図表3-1-2）。有効な情報漏洩の対策のひとつとしてIRMのニーズが急速に高まっており、業種、従業員規模問わず、全方位的に導入が進んでいる。また、企業のクラウドシフトの進展に伴い同市場のトップベンダーであるマイクロソフトが急成長し、市場の伸びを牽引した。現在、各参入ベンダーともに好調に推移していることから、2019年度も同14.8%増と成長を維持することが予想される。

3-1-2　業種別市場シェア

図表3-1-6　IRM市場：業種別売上金額推移およびシェア（2017～2019年度予測）

（単位：百万円）

	2017年度		2018年度			2019年度（予測）		
	金額	シェア	金額	シェア	前年比	金額	シェア	前年比
製　造	920.4	16.5%	1,028.2	15.7%	111.7%	1,210.9	16.1%	117.8%
流　通	388.9	7.0%	460.8	7.0%	118.5%	514.6	6.9%	111.7%
金　融	1,168.2	20.9%	1,460.3	22.3%	125.0%	1,693.3	22.5%	116.0%
通　信	414.0	7.4%	498.6	7.6%	120.4%	643.1	8.6%	129.0%
サービス	832.6	14.9%	1,007.3	15.4%	121.0%	1,194.6	15.9%	118.6%
建　設	173.8	3.1%	203.0	3.1%	116.8%	298.7	4.0%	147.2%
公共・公益	1,682.2	30.1%	1,881.9	28.8%	111.9%	1,955.0	26.0%	103.9%
合　計	5,580.0	100.0%	6,540.0	100.0%	117.2%	7,510.0	100.0%	114.8%

※出典『ITR MARKET VIEW　情報漏洩対策市場2020』

アジェンダ

1 ファイルセキュリティが必要とされる背景

2 **FinalCodeが提供する価値**

3 FinalCodeの活用例

4 ファイル運用に合った充実機能

5 FinalCodeが選ばれる理由

6 Appendix

FinalCodeが提供する価値

FinalCode（ファイナルコード）とは、デジタルアーツ株式会社が開発・提供する
ファイル暗号化・追跡IRMソフトウェア です。
社内ファイルはもちろん、**従来では守ることができなかった社外に渡したファイルまで、**
守り、追跡し、万が一、情報漏洩が疑われる場合は、あとから消すことが可能です。

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

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

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

FinalCodeが提供する価値

守る

閲覧者・閲覧期間の
指定あり

上書き編集
OK

コピー＆ペースト
NG

印刷
NG

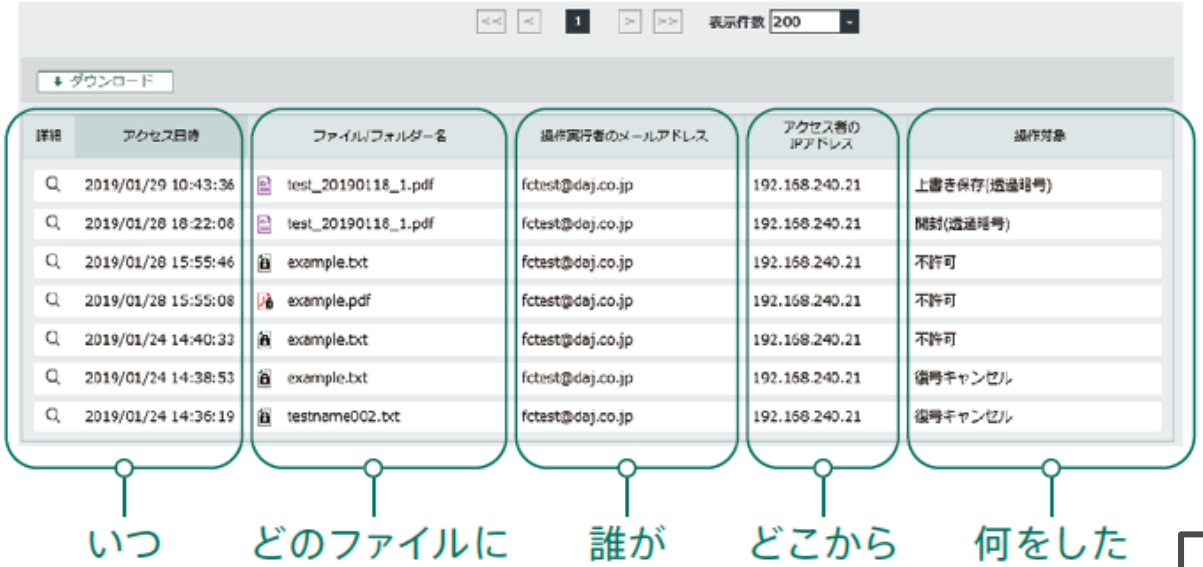
※設定の一例です。
※ファイル操作権限は、渡した後でも変更可能です。権限変更後に、ファイルを再送する必要はありません。

ご活用シーン

従業員情報は、人事部のみ閲覧できるように制限したい。
議事録の改ざん（上書き編集）を防ぎたい。

FinalCodeが提供する価値

追跡する

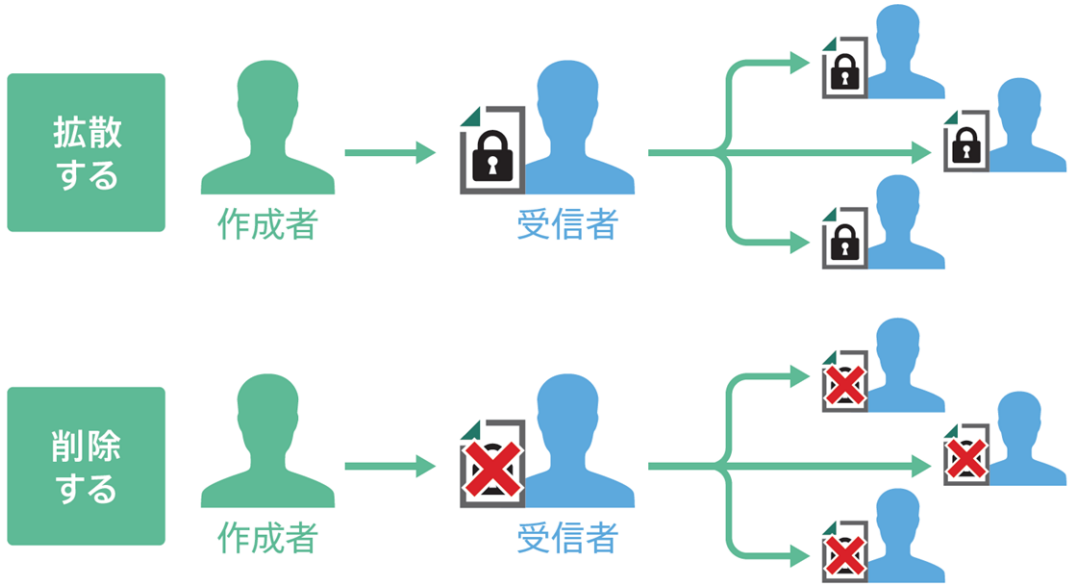


ご活用シーン

提供したファイルがきちんと閲覧されたか、確認したい。
適切に情報を取り扱った証跡として、レポート報告したい。

FinalCodeが提供する価値

あとから消せる

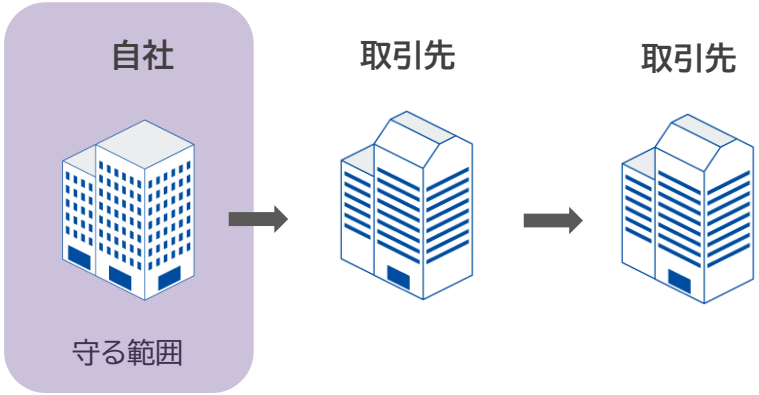


ご活用シーン

手元を離れたデータファイルを、削除したい。
プロジェクト終了後に、協力会社に提供したファイル削除を徹底したい。

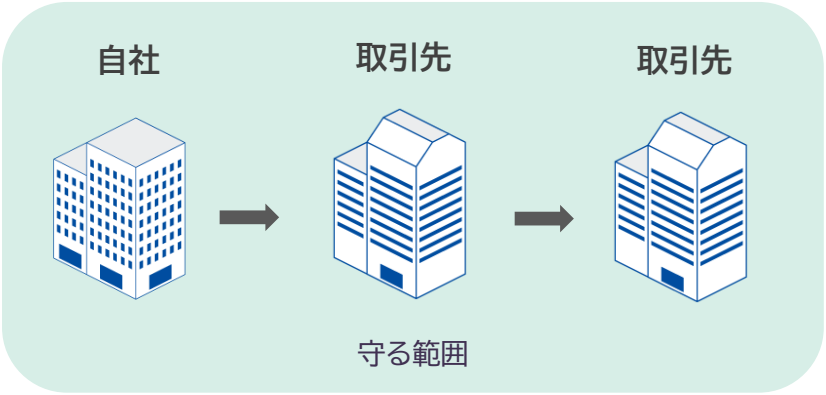
FinalCodeは社内も社外も守る

パスワード付ファイルや一般的な暗号化製品



社内や受け渡し時だけ守り、
社外や受け渡し後はコントロールできない

FINALCODE

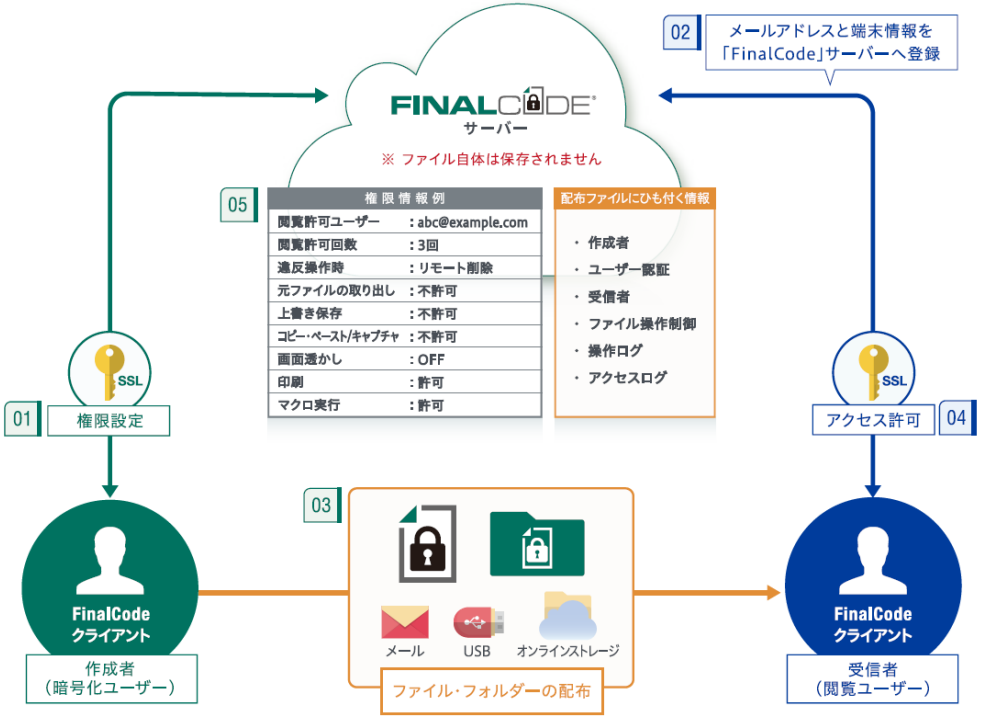


暗号化されているファイルは
どこまでもコントロールし続ける

FinalCodeの仕組み

特許技術
特許5404030号
特許5840180号

FinalCodeは、ファイルの暗号化/閲覧を行う『FinalCode クライアント』と、ファイルの権限情報等を管理する『FinalCode サーバー』とで構成されます。
クラウド版ご利用の場合、『FinalCode クライアント』を、**利用PC端末にインストールするだけでご利用**いただけます。



01 FinalCode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 FinalCodeクライアントをインストールすると、メールアドレスと端末情報が登録されます。これによりユーザーの特定ができ、ファイル開封時の**パスワード入力が不要**になります。

03 通常通り、メール・USB・オンラインストレージ等で配布します。
受け渡し手段は、今まで通り自由です、

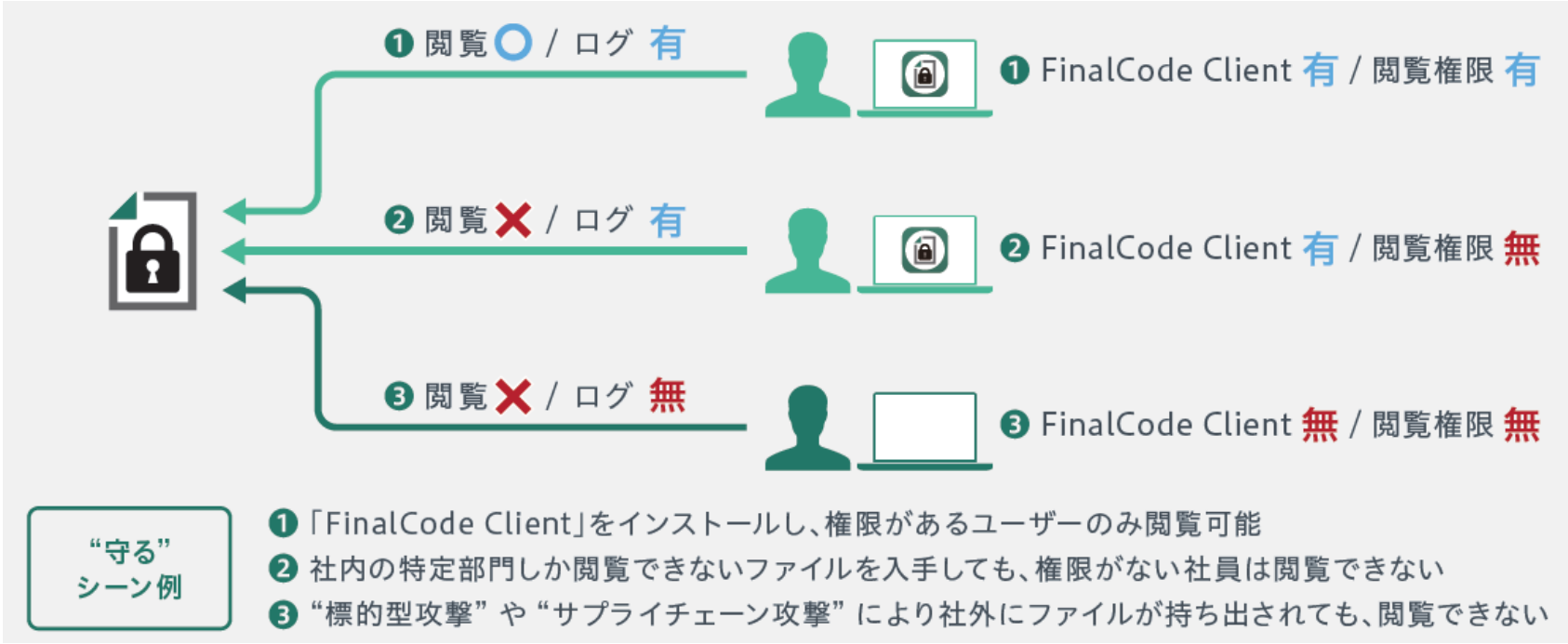
04 暗号化ファイルをダブルクリックすると、FinalCodeサーバーに権限情報の問い合わせが行われ、**権限情報に基づいたファイル操作**ができます。

05 暗号化ファイルの**権限はあとから変更も可能**です。
権限変更したファイルは**再送付する必要はありません。**

※インターネット接続が必要です。
オフライン閲覧オプションをご利用いただくと、インターネット環境がない場所でも、IRM制御を行うことができます。

クライアントインストールのメリット：自社

『FinalCode クライアント』をインストールすることで、暗号化ファイルの閲覧（パスワードレス開封・操作制御）・ログ取得・リモート削除が可能です。



「FinalCodeクライアント」は認証時・ログ出力時のみ起動・通信するため、常駐起動型のクライアントソフトのように、PCとネットワークのリソースを浪費することはありません。

クライアントインストールのメリット：取引先

取引ユーザーも『FinalCodeクライアント』をインストールすることで、以下メリットを享受頂いております。

FINALCODE

内部不正持ち出し　紛失/盗難　誤送信

企業・団体内ユーザー
（自社）

企業・団体ユーザー
（取引先）

取引先でIRM制御しているため、
自社でルールを作り、文書管理することの
プレッシャーから解放されました。

ダブルクリックで開封できるため、**面倒なパスワードの**
入力やパスワード管理が不要になりました。

専用スマホアプリからも安全に閲覧可能なため、
外出先でもすぐに確認できるようになりました。

改ざん

標的型攻撃

間接（二次）漏洩　サプライチェーン攻撃　ランサムウェア

アジェンダ

1 ファイルセキュリティが必要とされる背景

2 FinalCodeが提供する価値

3 **FinalCodeの活用例**

4 ファイル運用に合った充実機能

5 FinalCodeが選ばれる理由

6 Appendix

FinalCodeで守られているファイル例

経営企画
役員資料
戦略会議資料
M&A関連
売上実績・予実情報

法務・財務
M&A関連
調査報告書
特許関連
知的財産
IR

研究・開発
調査レポート
仕様書
設計図面
基準書
規格書

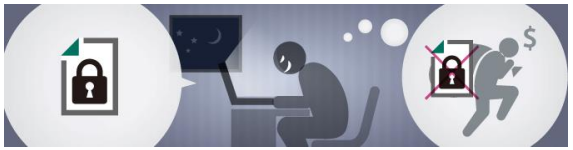
人事・総務
マイナンバー
人事給与
就業規則
社内規定
従業員情報
履歴書

サポート
個人情報
マニュアル

自治体・学校
公務・校務における機密文書
住民情報
生徒情報

営業・マーケティング
セールスノウハウ(マニュアル・トーク集)
日報
RFI・RFP
取引先情報
企画書
個人情報(申込者・会員情報・契約者情報)

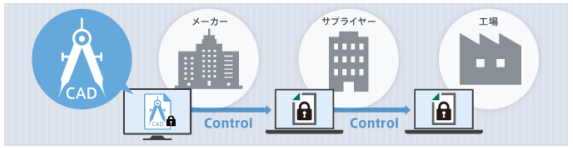
FinalCodeが防ぐ漏えいリスク



内部からの漏えい
－不正持ち出し
－紛失
－盗難
－誤送信
－改ざん

FINALCODE

外部による漏えい
－標的型攻撃
－ランサムウェア
－ビジネスメール詐欺



取引先からの漏えい
－サプライチェーン攻撃
－間接(二次)漏えい
－オンラインストレージからダウンロード後の漏えい

FinalCodeの活用シーン

より簡単に活用したい方へ

セキュアな運用を社内に徹底させることは大変ですが、ファイル作成・保存時や、ダウンロードしたタイミングで自動暗号化する手段を提供します。

ユーザーが意識することなく守るため、セキュリティリテラシーに関係なく、社内の情報を守ります。

より強固に活用したい方へ

社内において、閲覧者を制限したい場合や、社外に渡した情報に対しても漏洩リスクを検討しなければいけない場合もあります。

その際は、強固なIRM機能を使って、閲覧者の指定や、画面透かし、あとからリモート削除といった手段を使って漏洩防止を徹底します。

より柔軟に活用したい方へ

セキュリティレベルを向上させても、日々の業務生産性が低下しては意味がありません。

自社でご利用中の業務システムとFinalCode APIを連携させることで、現行フローを変える必要なく、業務にあったセキュアな運用が実現します。

FinalCodeの活用シーン：より簡単に

管理者

STEP1　自動暗号化対象を設定

・どのユーザーが扱うファイル？
・どのアプリ/拡張子のファイル？
・どこに格納されたファイル？

社内利用
ユーザー

STEP2　通常操作で自動暗号化

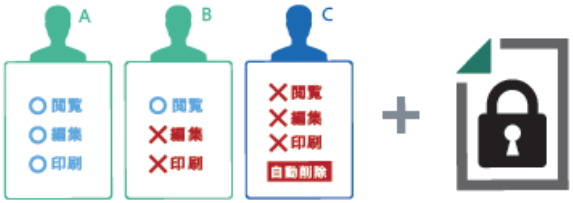
・作成/編集
・保存
・ダウンロード

FinalCodeが防ぐ情報漏えいリスク

・内部からの漏えい（不正持ち出し、紛失、盗難、誤送信、改ざん）
・外部による漏えい（標的型攻撃、ランサムウェア、ビジネスメール詐欺）
・取引先からの漏えい（サプライチェーン攻撃、間接（二次）漏えい、オンラインストレージからダウンロード後の漏えい）

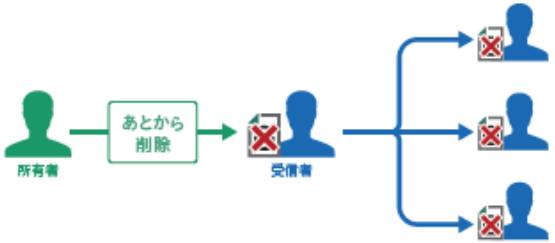
FinalCodeの活用シーン：より強固に

複数権限



画面透かし

削除・不正通知

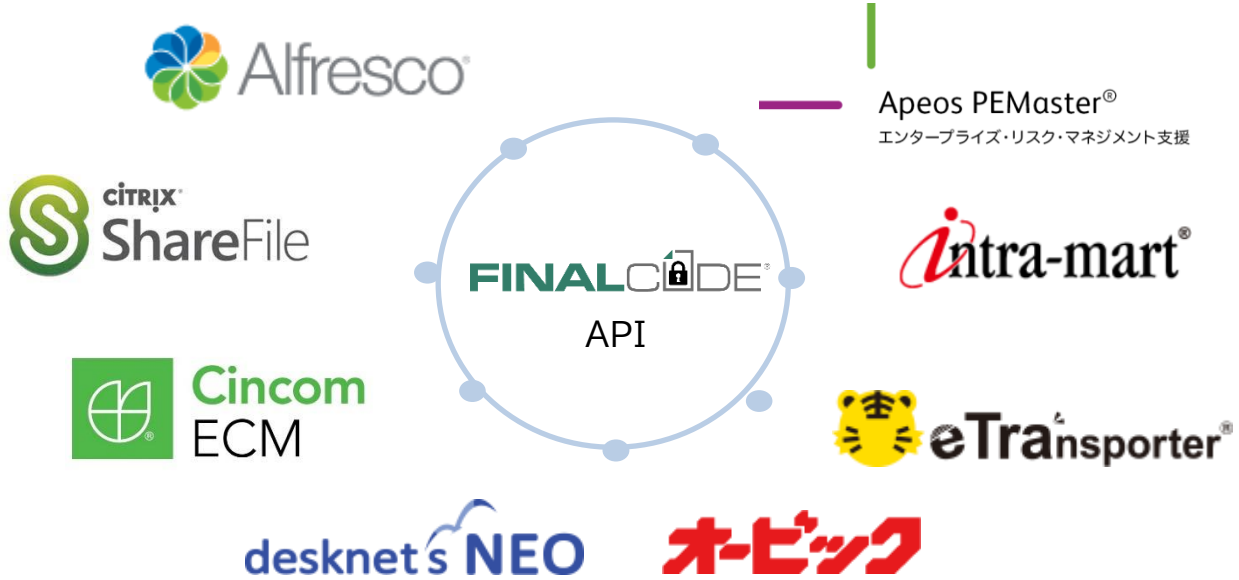


FinalCodeが防ぐ情報漏えいリスク

・内部からの漏えい（不正持ち出し、紛失、盗難、誤送信、改ざん）
・外部による漏えい（標的型攻撃、ランサムウェア、ビジネスメール詐欺）
・取引先からの漏えい（サプライチェーン攻撃、間接（二次）漏えい、オンラインストレージからダウンロード後の漏えい）

FinalCodeの活用シーン：より柔軟に

文書管理システムだけでなく、人事・給与システムや、会計システム、ワークフローシステム等、日々利用している業務システムと連携することで、さらに業務に浸透したセキュアな運用が実現します。



お客様の声・導入効果

作業工数の削減

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でき、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。
別のメールでパスワードを送るという従来の手間もなくなり、工数の削減に繋がっています。

■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取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できるようになりました。

■カシオ計算機株式会社

セキュリティ強化

「Box連携オプション」によって、税務申告等に必要な情報を、安全に顧客から提出していただくことが可能になりました。
また、PPAP対策として、ファイルをメールに添付する際、ブラウザービューファイルを使用しています。

■パートナーズプロジェクト税理士法人

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事に対し「FinalCode」導入後は暗号化フォルダーにファイルを置くだけで自動で暗号化と透かしが適用され、生産性が向上しました。

■スズキ株式会社

国産ならではのサポート

「情報の開示範囲拡大」を実現しつつ
「情報漏えい対策」も一緒に実現できるソリューションを探していたところ、
「FinalCode」にたどり着きました。
サポートのレスポンスも非常に早く、本当に感謝しています。

■株式会社東海理化

漏えい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。

■社会保険労務士　小泉事務所

詳細はWebサイトをご参照ください。https://www.finalcode.com/jp/case/

第三者からの評価・受賞歴

総務省後援『ASPIC IoT・AI・クラウドアワード』において、
自社の重要な**情報財産を強固に守る**だけでなく、ファイル管理にかかっていた手間や時間からも解放されるため、
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。

＜支援業務系ASP・SaaS部門＞

賞名	会社名	サービス名
総合グランプリ	デジタルアーツ株式会社	渡したファイルが"あとから"消せる、世界ではじめてのIRM『FinalCode』
準グランプリ	セイ・テクノロジーズ株式会社	サーバー設定仕様書自動生成サービス「SSD-assistance」
準グランプリ	株式会社メディア4u	メディアSMS
ベンチャーグランプ	DXYZ株式会社	顔認証プラットフォーム「FreeiD（フリード）」
審査委員会賞	NTTコム　オンライン・マーケティング・ソリューション株式会社	空電プッシュ
先進技術賞	株式会社JIRAN JAPAN	法人向けエンドポイントセキュリティ「EXOセキュリティ」

その他受賞歴

NETWORKWORLD

CYBERSECURITY 500
WORLD'S HOTTEST SECURITY COMPANIES

https://aspicjapan.org/event/award/16/index.html

アジェンダ

1 ファイルセキュリティが必要とされる背景

2 FinalCodeが提供する価値

3 FinalCodeの活用例

4 **ファイル運用に合った充実機能**

5 FinalCodeが選ばれる理由

6 Appendix

ファイル運用の各シーンにあった充実機能

ファイルセキュリティは、業務に密接に関わるので『いかに業務に浸透させるか』 が成功の1つのキーになります。
単に「暗号化すれば良い」では、結局ユーザーに使われず・使い勝手の悪いままで終わってしまいます。
FinalCodeは、10年の実績の元、お客様の声とともに製品開発し、『作成・共有・編集・管理』といった
ファイル運用の各シーンに合った機能を提供しています。

作成

ファイルを作成・編集し、

共有

関係者に共有し、

閲覧

閲覧・編集し、

管理

適切に管理する

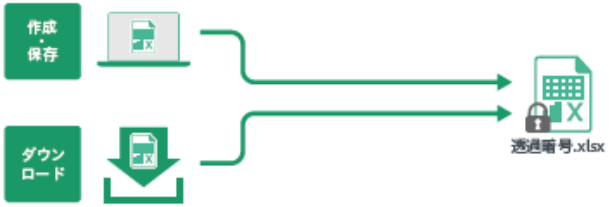
ファイルセキュリティ運用の充実機能（作成時）

作成 共有 閲覧 管理

特許技術

透過暗号

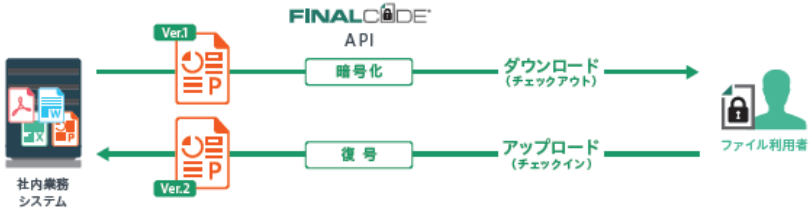
暗号化されていても、今までと同様の使い勝手のため、オペレーション教育の手間はありません。
また暗号化をユーザーに意識させないため、**セキュリティ**
リテラシーに関係なくご利用いただけます。



OPTION

API

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必要なく**セキュアな運用が実現します。



特許技術

共有フォルダー
自動暗号化

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。

特許技術

セキュアコンテナ

「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。

ファイルセキュリティ運用の充実機能（共有時）

作成 共有 閲覧 管理

ブラウザービュー

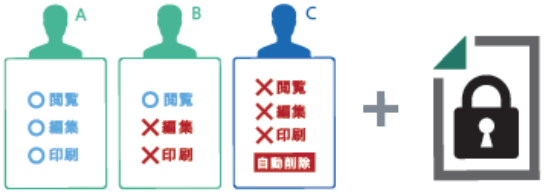
パスワード付きZIPファイルと異なり、閲覧者や閲覧期間の指定ができるため、セキュリティ対策も万全です。またファイル閲覧履歴も確認できるため**開封チェックとしてもご利用**いただけます。

m-FILTER連携

「m-FILTER」との連携で、送信メルの添付ファイルを自動的にFinalCodeで暗号化し、**送信者の負担を軽減**します。

複数権限

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。



Box連携

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。**

ファイルセキュリティ運用の充実機能（閲覧時）

作成 共有 閲覧 管理

画面透かし

文字・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。

オフライン閲覧

OPTION 特許技術

ネットワーク回線がない環境下においても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。

FinalCode Reader

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

開封時ユーザー認証

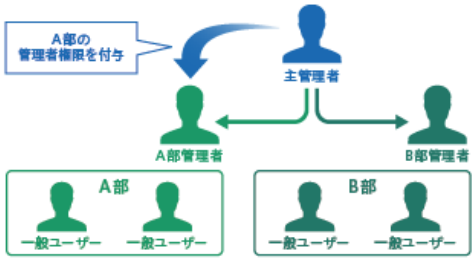
共有端末で作業する場合に、**自分の個人ファイルを他の人が閲覧できないようにします。**

ファイルセキュリティ運用の充実機能（管理時）

作成 共有 閲覧 管理

組織管理・AD連携

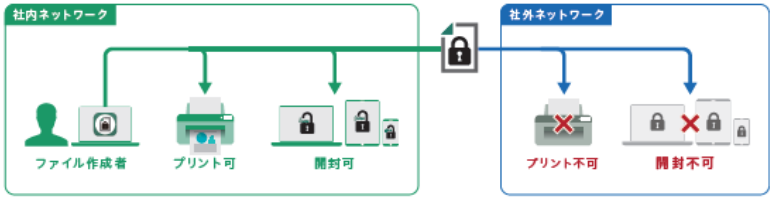
各組織の業務特性を考慮しながら**組織にあったセキュリティを適用**することが可能です。



※Microsoft Entra IDとの連携も可能です。

IP、デバイス制限 プリンター制御

社内ネットワークや会社支給端末でのみ暗号化ファイルを閲覧可能にしたり、**社外での出力を不可能**にしたりするなどのセキュリティポリシーを実現します。

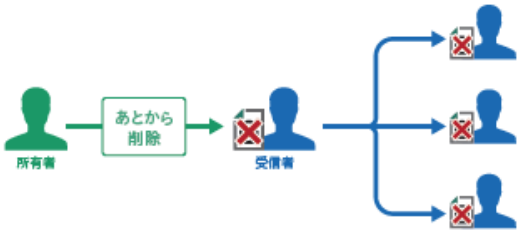


アクセスログ

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。

削除・不正通知

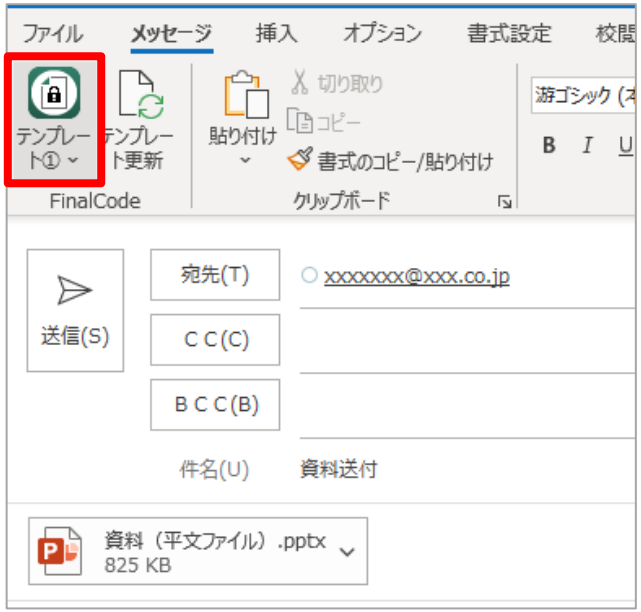
拡散されたファイルも削除し、ログとして残るため、廃棄したエビデンスを取得することもできます。



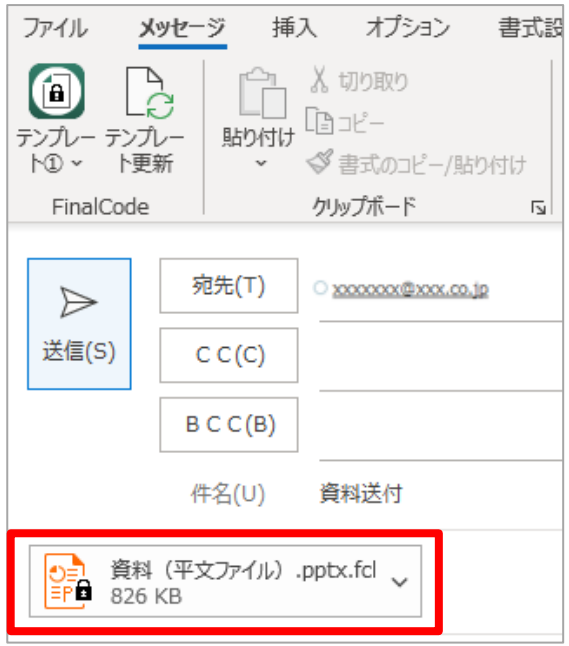
新機能：Outlookアドイン

Outlookを用いたメール作成時、添付ファイルに対して暗号化テンプレートを適用し、FinalCode暗号化を実施するOutlookアドインをご提供いたします。

■メール作成画面上にアイコンが表示され、
テンプレートを選択



■確認のポップアップが表示され、送信すると
テンプレートルールに従い自動で暗号化



アジェンダ

1 ファイルセキュリティが必要とされる背景

2 FinalCodeが提供する価値

3 FinalCodeの活用例

4 ファイル運用に合った充実機能

5 **FinalCodeが選ばれる理由**

6 Appendix

FinalCodeが選ばれる理由

使い勝手

使い勝手、運用、コストの面で優れていました。
ユーザー側の使い勝手はもちろんですが、管理者側の使い勝手も重要な要素のひとつでした

TOKAI RIKA

株式会社東海理化 様

価格

『社外ユーザー』は無償というライセンス体系も、
多数の販売店がいる弊社のニーズにマッチしていました

SUZUKI

スズキ株式会社 様

サポート

レスポンスが早いので非常に助かっています。
当初、『FinalCode』に不足している機能があり相談したところ、**しっかり要望が反映され、対応が早く驚きました**

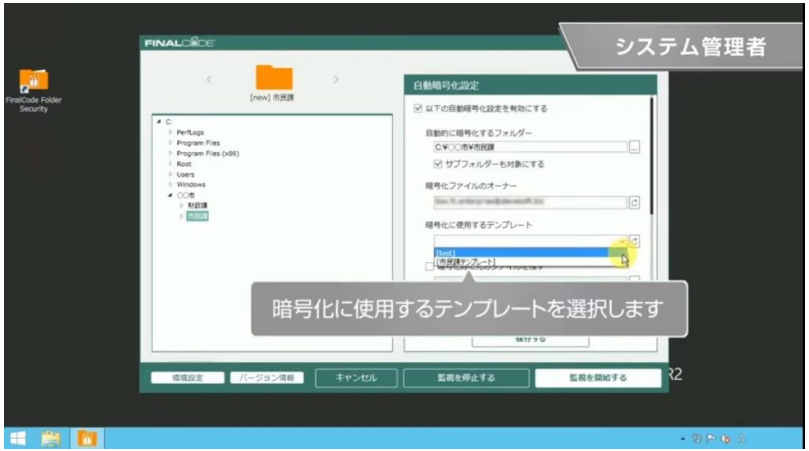
YAZAKI

矢崎総業株式会社 様

詳細はWebサイトをご参照ください。https://www.finalcode.com/jp/case/

FinalCodeが選ばれる理由：使い勝手

国産メーカーが提供するUIで管理画面の操作も簡単！



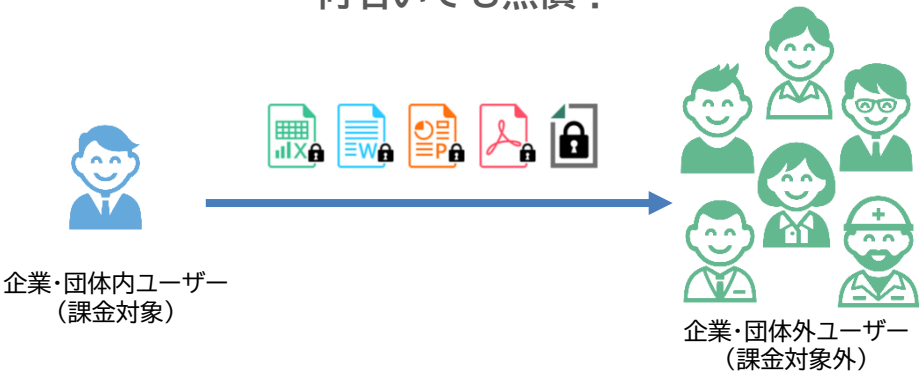
利用ユーザー向けの動画マニュアルや書籍もご用意！

詳細はWebサイトをご参照ください。https://www.daj.jp/bs/video/

FinalCodeが選ばれる理由：価格

企業・団体内ユーザーが課金対象です。
ライセンスは、メールアドレスまたはADアカウントを用いて認証するユーザーライセンスです。

企業・団体外ユーザーは何名いても無償！



※10ライセンスご購入の場合、以下ユーザー数がご利用可能です。
企業・団体内の、暗号化ファイル編集ユーザー：10名
企業・団体内の、暗号化ファイル閲覧ユーザー：90名
企業・団体外の、暗号化ファイル編集・閲覧ユーザー：無制限

ご購入ライセンス数に応じたボリュームディスカウントをご用意！

ライセンス	本体価格（ユーザー/年）	
	標準ライセンス（企業向け）	パブリックライセンス（公共・文教向け）
10 ～ 29	@12,000	@8,400
30 ～ 49	@11,800	@8,250
50 ～ 99	@11,500	@8,050
100 ～ 199	@11,000	@7,700
200 ～ 299	@10,500	@7,350
300 ～ 499	@10,000	@7,000
500 ～ 749	@9,500	@6,650
750 ～ 999	@9,000	@6,300
1,000 ～ 1,999	@8,500	@5,950
2,000 ～ 2,999	@8,000	@5,600
3,000 ～ 3,999	@7,500	@5,250
4,000 ～ 4,999	@7,000	@4,900
5,000 ～ 6,999	@6,500	@4,550
7,000 ～ 9,999	@6,000	@4,200

詳細はWebサイトをご参照ください。https://www.finalcode.com/jp/price/

アジェンダ

1 ファイルセキュリティが必要とされる背景

2 FinalCodeが提供する価値

3 FinalCodeの活用例

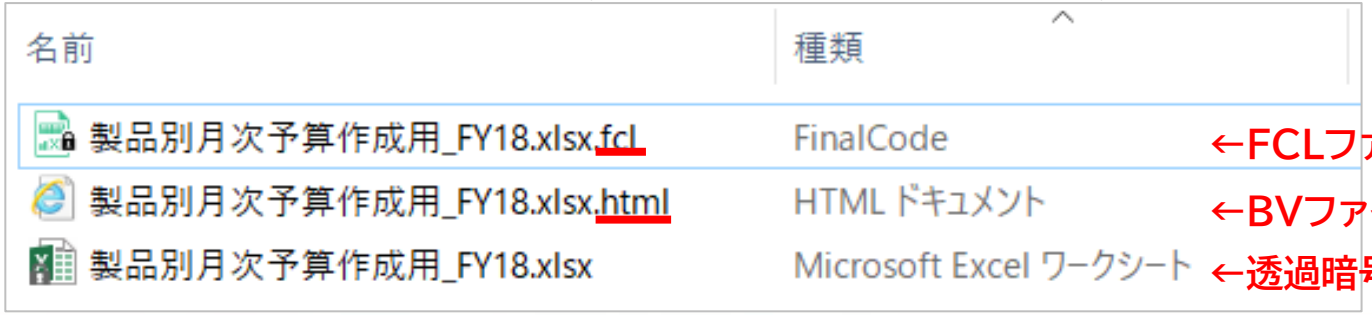
4 ファイル運用に合った充実機能

5 FinalCodeが選ばれる理由

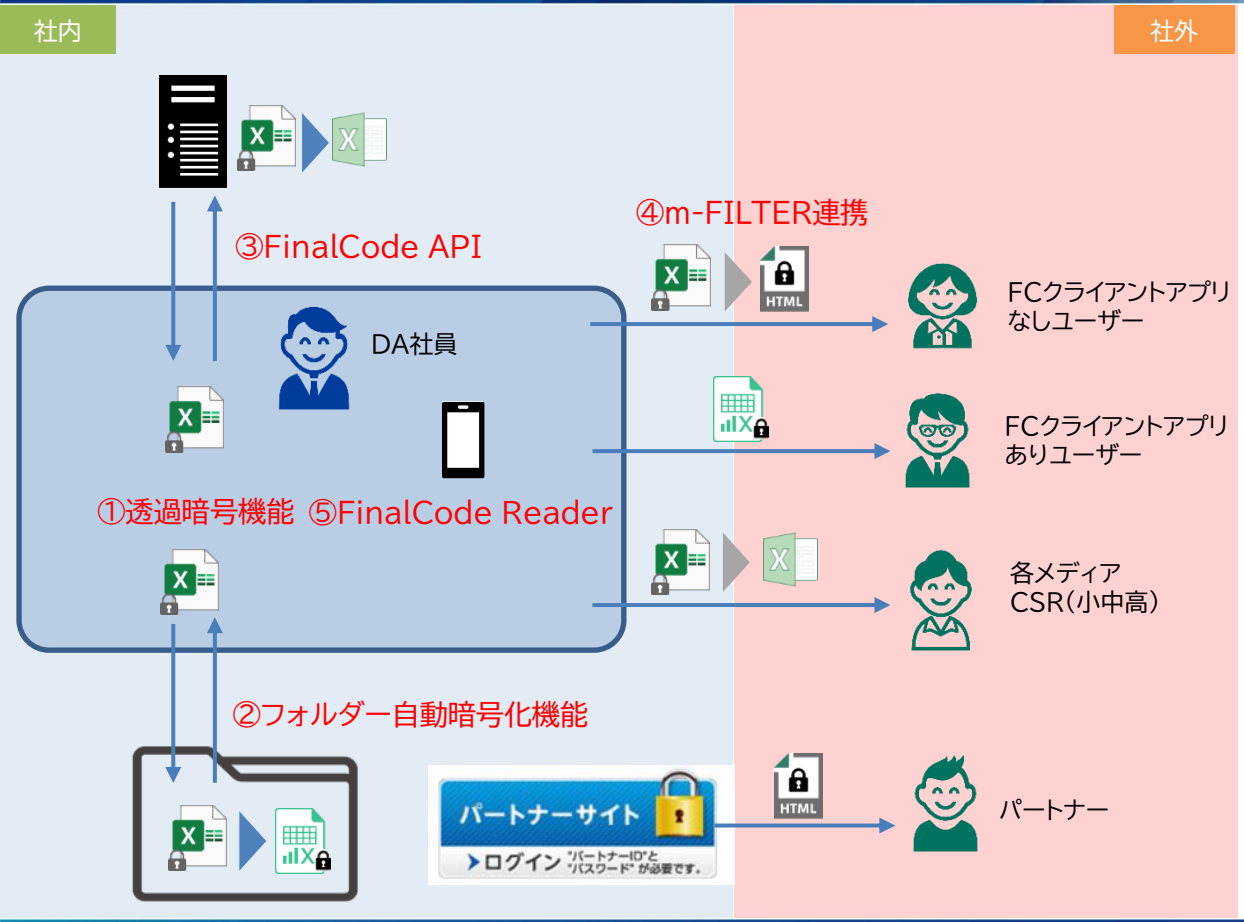
6 **Appendix**

FinalCodeがつくるファイルの種類

	FCLファイル	BVファイル（ブラウザービューファイル）	透過暗号ファイル
特徴	ファイル操作を完全に制御するIRM制御	クライアントがなくても安全に配布・閲覧できる	暗号化を意識しなくても、いつの間にか暗号化されている
閲覧可能ユーザー	社内・社外	社内・社外	社内のみ
デジタルアーツでの利用シーン	関係者内のみの情報を守る時 （ex.開発情報、人事考課、発表前IR情報）	社外へ送付する時 （ex.見積書、提案書、カタログ）	個人PC端末での業務時 （ex.データ分析、報告資料）



デジタルアーツでの社内運用イメージ



①個人PC端末上のファイルを、作成時・ダウンロード時に自動暗号化
【データ分析や報告資料 .etc】
暗号化を意識させず、業務に影響しないように守る。

---

②フォルダー格納時に自動暗号化
【開発情報、人事考課、発表前IR情報 .etc】
関係者のみ閲覧許可。改ざん防止のため編集禁止。

---

③業務システムが読み取る必要のあるデータファイルは、インポート時にAPIで自動復号
(＋ダウンロード時には自動暗号化)
【会計データ、給与明細 .etc】
暗号化ファイルも、通常操作で手間なく、自動復号。

---

④メール送付時に、添付ファイルを自動変換
【カタログ、見積書、プレスリリース .etc】
あとから「元ファイル取出し」することで、開封チェックと誤送信防止。

---

⑤社内端末紛失時の漏洩防止。

FinalCodeの高度な暗号化技術

- 電子政府推奨の暗号化技術(※)を採用
  暗号化アルゴリズム:AES 256bit形式
  暗号通信　　:SSL+RSA2048　※データ自体も独自に難読化されています。
  ※CRYPTREC HPより https://www.finalcode.com/jp/news/blog/2021/012501/
- 米国連邦政府標準規格「FIPS140-2」の認証を取得
- 独自の電子証明書を用いた端末認証
- ファイルアクセス時の都度認証で、常に最新のセキュリティポリシーを適用
- 常に暗号化されたままのデータを維持
- 暗号化ファイルを開くアプリケーションをホワイトリストで制限しつつ、
  情報を盗み取ろうとする外部アプリケーションをブラックリストで防御

特許技術
第5750497号

詳細はWebサイトをご参照ください。https://www.finalcode.com/jp/news/blog/2021/012501/

ホワイトリスト・ブラックリストについて

特許技術
第5750497号

ファイルの開封までに二重のチェックをおこない、
開封後もファイルの安全を維持し続けます

01 同時起動アプリ制御
〈ブラックリスト方式〉

セキュリティホールになりうるアプリケーションの同時起動を制御

画面キャプチャ、クラウドストレージ、SNSへのアップロード・共有など、情報漏洩の抜け道になる機能を持ったアプリケーションをブロックします。また、ファイル開封後も該当アプリケーションの起動をブロックし続けます。

＊ 登録アプリケーション数：約3,600

- スクリーンキャプチャ
- ドライブシェア
- プロセスキラー
- アップロード
- コラボレーション
- レコーダー

02 開封アプリの限定制御
〈ホワイトリスト方式〉

ファイル閲覧は、安全に開くことができるアプリケーションに限定

暗号化設定が有効であることを検証したアプリケーションでのみファイルの開封を許可します。グローバルで標準的に使用されている主要なアプリケーションを継続的に動作検証済みアプリケーションリストに追加しています。

安全な環境でのみ開封許可

導入時には、お使いのアプリケーションが動作検証済ソフトウェア一覧（ホワイトリスト）に含まれていることを下記URLにてご確認ください。
https://www.finalcode.com/jp/product/spec/

ホワイトリスト・ブラックリストについて

特許技術
第5750497号

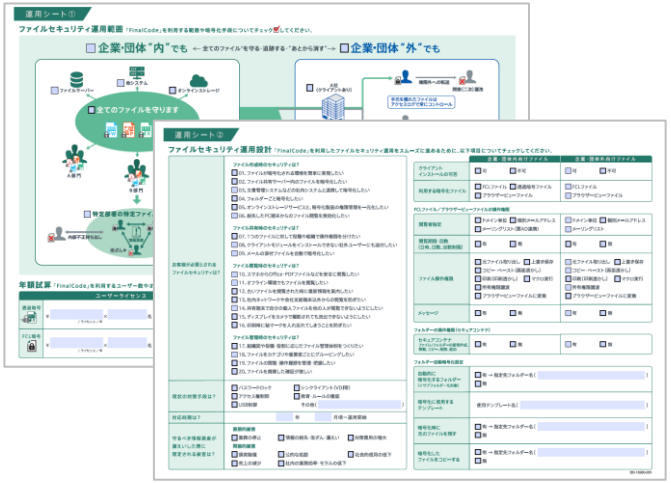
一般的なファイル暗号化製品には、暗号化設定が効くことを確認できた動作検証済みアプリケーションがあります。
例えば、よく使われているMicrosoft Office Wordは、各社とも動作検証済みです。
しかし、**docファイルが、渡した先でも当たり前のようにWordで開封されるとは限りません。**
海外では、知名度の低いアプリケーションを使っていることがあります。

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。

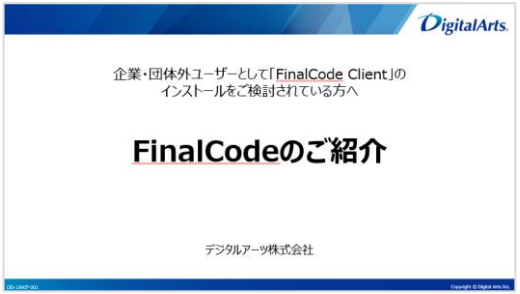
また、様々なアプリケーションが日々開発されている今日、**スクリーンキャプチャやアップデートなど、重要ファイルから情報を抜き取る可能性があるアプリケーションが大量に存在します。**
安心して重要なファイルを渡すには、相手のPCがそれらのアプリケーションを利用していたとしても問題ない仕組みが必要です。
そこで「FinalCode」では、暗号化ファイルを開封するとき、または開封中のPCで、**セキュリティホールに繋がるアプリケーションが同時に利用されないような制御（ブラックリスト方式）**も採用しています。

ご活用資料

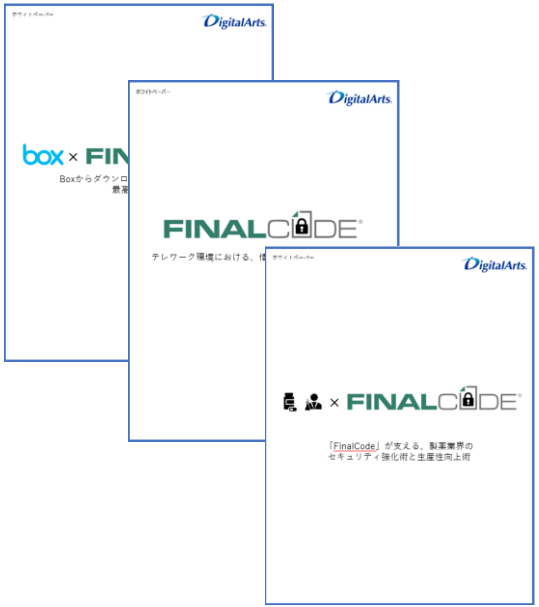
運用検討シート



企業・団体外ユーザー向け FinalCode説明資料



各種ホワイトペーパー 活用事例集



詳細はWebサイトをご参照ください。https://www.finalcode.com/jp/document/

ご利用にあたっての確認事項

- セキュリティ担保のため、編集・コピー＆ペースト・印刷等の制御があるFCLファイル(「名前を付けて保存」ができないファイル)は、動作検証済みアプリケーションでのみ閲覧することができるホワイトリスト方式を採用しています。最新の動作検証済みアプリケーションの一覧は、以下をご参照ください。
  https://www.finalcode.com/jp/product/spec/

- リアルタイムでのアクセスログ追跡、アクセス権限・操作権限変更、ファイル削除を可能にするため、FinalCode利用時はインターネット接続を必要とする仕組みになっています。インターネット接続ができない場合は暗号化・復号に失敗する、という挙動になります。FinalCode Clientのインストールによって通信の接続先を変更することはありません。

- FCLファイルの開封に関連してFinalCodeサーバーとの間で行われる通信は、すべてHTTPS(443/tcp)です。
  また、URLフィルタの設定条件によっては遮断の可能性がありますので、その場合はURLフィルタ側でアクセス許可設定が必要です。

- FinalCode Clientは、ファイル閲覧時にのみ起動、通信を行うため、常駐起動型のクライアントソフトのように、PCとネットワークのリソースを浪費することはありません。

- ユーザー登録時の端末認証ではサーバー／クライアント相互の鍵交換を行いますが、鍵生成時に取得する情報は、登録ユーザーを識別するために必要な情報のみです。
  鍵情報の詳細はセキュリティの関係上、公開しておりませんが、鍵ファイルやHDDの抜き取りによって意図しない相手が復号することがないように、ハードウェアの固有情報を含んでおります。

- FinalCodeでは、編集・コピー＆ペースト・印刷等を制御する機能を搭載しています。このことにより、ウイルス対策ソフト、資産管理ソフト、他社セキュリティソフトなどと併用された場合に、コンフリクトを起こす可能性がございます。万が一、FCLファイルが正常に復号できない場合は、FCLファイルを送付した取引先へご連絡ください。(デジタルアーツへのサポート問い合わせは、識別用のシリアルNO.が必要となるため、取引先経由で受け付けております。)

- ブラウザービューファイル暗号化時に[印刷許可]をONに設定している場合、[元ファイル取り出し許可]をOFFに設定していても、印刷タブより[PDFで保存]からPDFデータのダウンロードが可能となります。

最後までご覧いただき、ありがとうございました。

ご質問等がございましたら、お気軽にお問い合わせください。

メール：salesmktg-dc@daj.co.jp
問い合わせフォーム：https://www.finalcode.com/jp/contact/
FinalCode Webサイト：https://www.finalcode.com/jp/

デジタルアーツ株式会社
〒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
sales-info@daj.co.jp　　www.daj.jp