

新世代の外部攻撃 & 情報漏洩対策

DigitalArts @ Cloud®



■本書は、2022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。■ActiveDirectory、InternetExplorer、MicrosoftEdge、Microsoft365およびWindowsは、MicrosoftCorporationの登録商標または商標です。■Android、GmailおよびGoogleChromeは、GoogleLLCの登録商標または商標です。■IOSは、AppleInc.のオペレーティング・システムの名称です。■IOSは、CiscoSystem、sln.cの登録商標または商標です。■デジタルアーツ、DIGITAL ARTS、i-FILTER、i-FILTER@Cloud Anti-Virus & Sandbox、info board、Active Rating System、D-SPA、NET FILTER、SP-Cache、White Web、ZBRAIN、クレデンシャルプロテクション、ホワイト運用、m-FILTER、m-FILTER MailFilter、m-FILTER Archive、m-FILTER Anti-Spam、m-FILTER Anti-Virus & Sandbox、m-FILTER@Cloud Anti-Virus & Sandbox、m-FILTER File Scan、Mail Detox、m-FILTER EdgeMTA、EdgeMTA、FinalCode、i-フィルター、DigitalArts@Cloud、Desk@Cloud、Desk、DアラートおよびDコンテンツその他の弊社・弊社製品関連の各種名称・ロゴ・アイコン・デザイン等はデジタルアーツ株式会社の登録商標または商標です。■本書に記載されている製品の各種ライセンスの定義およびライセンス別の価格については、各製品の価格表をご参照ください。■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される場合があります。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

Web・メール・ファイル・コミュニケーションを  
網羅したクラウドセキュリティ

~テレワークも、「ホワイト運用」で外部攻撃対策&業務効率化~

# Web・メール・ファイル・コミュニケーション、 いずれも、セキュリティを意識させない 「ホワイト運用」を、クラウドで実現します。

Webサービスやメール環境が急速にクラウド化し、セキュリティもクラウドでの運用ニーズが高まる中、「DigitalArts@Cloud」は、導入実績No.1\*のWebセキュリティ「i-FILTER」、メールセキュリティ「m-FILTER」、ファイルセキュリティ「FinalCode」に加え、社内コミュニケーションから「堅苦しさ・煩わしさ」をなくし、「ホワイト運用」されている空間で、安全に使えるオンライン会議システム「Desk@Cloud」を提供します。

「i-FILTER@Cloud」では、ホワイト運用が可能なデータベースで、安全なWeb環境を実現します。また、業務を阻害しない、Surface Webの網羅率の高さを誇ります。

「m-FILTER@Cloud」でもホワイト運用を可能にし、安全なメールだけを受信できる環境を実現します。また「クラウドメール環境」では対応できない誤送信対策も実現します。

「FinalCode@Cloud」では、ファイル閲覧範囲の管理、アクセス履歴の把握、渡したあとのファイル操作権限変更および削除が可能のため、各種漏洩(内部不正持ち出し・二次漏洩・サプライチェーン攻撃等)から守ります。セキュリティを意識させない世界を、クラウドで実現します。

「Desk@Cloud」では、テレワークが当たり前の時代に、業務効率を下げずに効果的にコミュニケーションを行え、意思決定を迅速化します。

## 「DigitalArts@Cloud」でできること

### i-FILTER@Cloud

- 水飲み場攻撃などの外部攻撃対策とWebの情報漏洩対策を1つの製品で実現
- ホワイト運用が可能なDBで安全な業務を実現
- 業務の邪魔をしない、Surface Webを網羅したDB

### m-FILTER@Cloud

- 外部からの攻撃対策と内部からの情報漏洩(誤送信)対策を1つの製品で実現
- ホワイト運用が可能なDBで安全な業務を実現
- パスワード付きのファイルも解析可能な、きめ細かい機能「特許取得済み(特許6882217号)」

### FINALCODE@Cloud

- サプライチェーン攻撃など外部攻撃対策と不正持ち出しなどの内部漏洩対策を1つの製品で実現
- 利用シーンに合わせて使い分け可能な暗号化機能
- 万が一の場合には、「渡したファイルが“あとから消せる”」究極のファイルセキュリティ

### Desk@Cloud

- 社内コミュニケーションの堅苦しさ・煩わしさをなくし、スピーディーな情報伝達を実現
- テレワーク環境など業務や場所を問わないコミュニケーションや会議を実現

\*【Webセキュリティ】株式会社富士キメラ総研「2021 ネットワークセキュリティビジネス調査総覧」Webフィルタリングツール市場占有率(2020年度)(2021年9月発行) 【メールセキュリティ】出典:デロイト トーマツ ミック経済研究所株式会社「内部脅威対策ソリューション市場の現状と将来展望 2020年度(https://mic-r.co.jp/mr/01910/)」電子メールフィルタリング・アーカイブツール出荷本数(社数)(2019年度)(2020年12月発行)

## 導入における3つのバリュー

VALUE  
01

### Webもメールも意識せずに、すべてを安全に閲覧

人の目で判断できない攻撃も、「i-FILTER@Cloud」と「m-FILTER@Cloud」が自動で無害化。ひとつの製品で外部攻撃対策と内部からの情報漏洩対策の両方をカバーし、圧倒的なコストパフォーマンスを発揮します。

VALUE  
02

### ファイルを自動で暗号化し、コントロールを継続

社内業務で利用するファイルに対して自動で暗号化。運用やポリシーを考える必要なく漏洩対策を実現。また、社外に渡したファイルについてもコントロールし続けることで外部への漏洩も防ぎます。

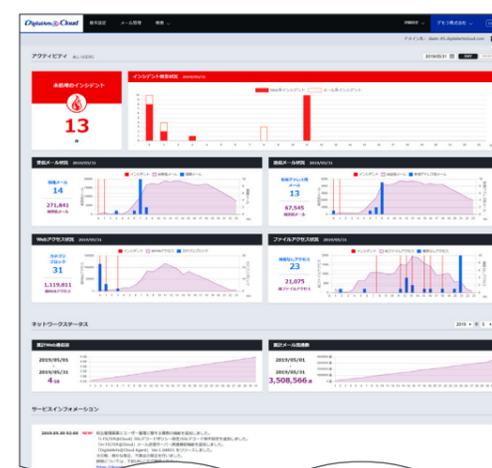
VALUE  
03

### Web・メール・ファイルのインシデントを即座に確認

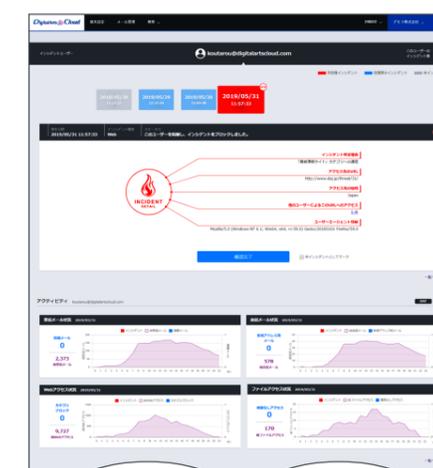
「DigitalArts@Cloud」なら、統合レポート画面によりWeb・メール・ファイルにおける外部攻撃、内部情報漏洩の可能性を1画面で横断的に表示します。業務利用せざるを得ないWebとメールとファイルの間隙を突く攻撃も即座に確認できます。

## 標準搭載の統合レポート

不正なサイトへのアクセスが発生した場合や、メールやファイルへのインシデントが発生した場合に、管理者へのアラートがメール通知されます。管理者はメール通知が届いた際に「統合レポート」からWebのインシデント・アクセス状況、メールのインシデント・送受信状況、ファイルのインシデント・トレースログを把握し、対策を講じることができます。



トップ画面



インシデント詳細レポート画面

## TOPICS

### Dアラート サイバーリスク情報提供サービス

「i-FILTER」Ver.10・「m-FILTER」Ver.5の機能で、不正なURLとメールを解析し、ホームページの改ざん<sup>※2</sup>や危険なメールの受信、マルウェア感染の疑いのあるお客様に、リスク情報を無償で提供します。

※特許6716051号 ※2 改ざんの検知で特許を取得



特許  
取得済み

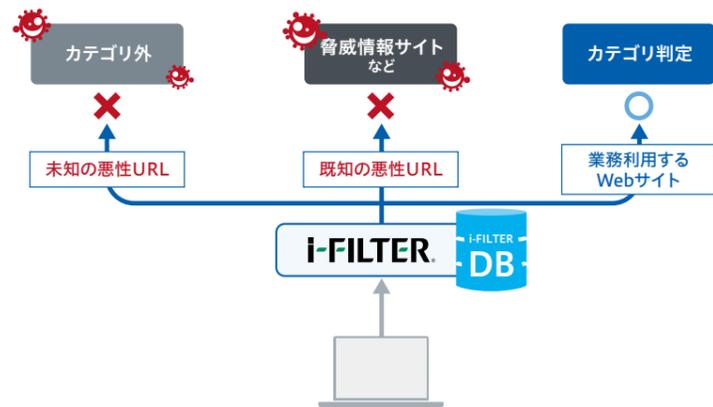
# i-FILTER@Cloud 「i-FILTER@Cloud」の機能と特長

## 01. 未知の脅威URLにアクセスさせない、「ホワイト運用」が可能なデータベース(DB)

「i-FILTER@Cloud」のDBは、「あらゆるURLをカテゴリ分類する方式」を採用しています。

### 「安全なWebの世界」を実現する仕組み 01

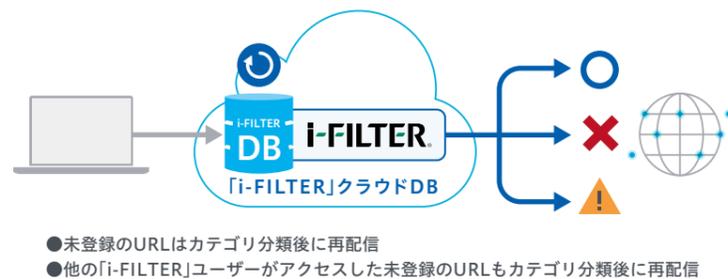
これまでの「ブロック対象となりうるURLをカテゴリ分類する方式」では、既知の悪性URLをDBに登録していました。DBに登録されていないURLはアクセス可能であったため、未知の悪性URLはブロック対象外となっていました。「ホワイト運用」では、安全と確認されたURLをDBに登録。DBに登録されていないURLはアクセス禁止となるため、未知の悪性URLもブロックが可能です。また、業務利用するWebサイトについては、「Surface Web(検索サイトで検索可能な国内のサイト)」のURLを、コンテンツのURLまで含めてDB登録することで、業務を阻害しないDBを作り上げています。



### 「安全なWebの世界」を実現する仕組み 02

検索サイトで検索可能な国内のサイトも日々新しいURLが追加されています。ユーザーが未登録のURLにアクセスしようとした場合、デジタルアーツにて、カテゴリ分類後に再配信することで、DBの網羅率を維持する仕組みを用意しています。

※一部のURLのカテゴリはクラウド上の「i-FILTER」のみに存在します



## 02. 安全なWebサイトからの安全なファイルダウンロードを実現 OPTION

「i-FILTER@Cloud Anti-Virus&Sandbox」の連携によりWeb経由でダウンロードしようとするファイルに対してマルウェア判定を行うことが可能。安全なWebサイトからの安全なファイルのダウンロードを実現します。

※「i-FILTER@Cloud Anti-Virus & Sandbox」オプションを別途ご購入いただく必要があります。 ※2022年5月10日販売開始



## 03. 「m-FILTER」との連携で、メールを隔離

メール受信時に本文や添付ファイル内のURLを「m-FILTER」が「i-FILTER」に通知し、DB判定の結果によってメールを隔離します。

※特許6768732号



### 「i-FILTER@Cloud」機能比較

	i-FILTER@Cloud	i-FILTER@Cloud 有害情報対策版
ホワイト運用(推奨フィルター)	○ (※変更不可)	×
Dアラート	○	○
Test Board	○	○
「m-FILTER」連携	○	×
レスポンスフィルター	○	×
VPN接続オプション	○	—
Outgoing IP固定	○	×
AD連携・SAML認証	○	○
ログ・レポート	○※1	○※1
ログ保存期間	標準で1年間	標準で1年間
i-FILTER@Cloud Anti-Virus & Sandbox ※2	○	×
i-FILTER@Cloud Splunk 連携 ※2	○	○

※1 DigitalArts@Cloud統合レポート ※3 2022年5月10日発売

# m-FILTER@Cloud 「m-FILTER@Cloud」の機能と特長

## 01. 業務を阻害しない「安全なメール運用」は、「ホワイト運用」と偽装判定で実現する

特許取得済み

「m-FILTER@Cloud」では安全な送信元のIPアドレスとドメインの組み合わせを登録したDBを利用して「ホワイト運用」を実現できます。DBに登録済みである送信元からのメールは受信し、未登録の送信元からのメールは「送信元」「添付ファイル」「本文・URL」の偽装判定を行い、安全なメールだけを受信します。危険なメールは隔離するだけでなく、メール無害化を実施した上で受信することができるため業務効率を下げずに安全な運用を実現します。

※特許6669954号



## 02. 危険な可能性がある添付ファイルのセキュリティチェックが可能

OPTION

### m-FILTER Anti-Virus&Sandbox

アンチウイルス・サンドボックスでセキュリティ判定することが可能です。ホワイト運用と組み合わせた判定で強固なメール運用を実現します。

※「m-FILTER@Cloud Anti-Virus & Sandbox」オプションを別途ご購入いただく必要があります。 ※5月10日販売開始



## 03. パスワード付きZIPファイルも強制的に検査

特許取得済み

業務に必要なファイルをメールに添付する際に、パスワード付きZIPファイルを利用する企業が多いことを逆にとり、偽装したパスワード付きZIPファイルを送付し、受信者を安心させた上でマルウェアに感染させる巧妙なメール攻撃にも対応します。

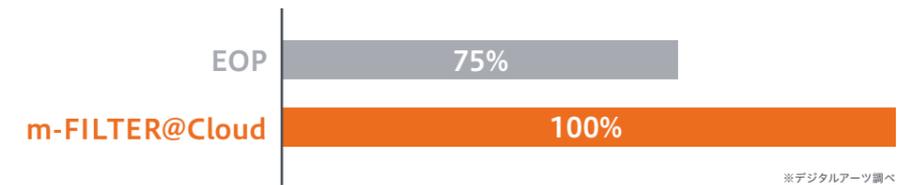


## 04. Microsoft 365 のメールセキュリティを強化 利便性も向上

多くの業界・業態の企業において導入が進んでいる総合グループウェア「Microsoft 365」と「m-FILTER@Cloud」を組み合わせることで、「Microsoft 365」の利便性・安全性が向上いたします。

### 外部からの攻撃対策

ExchangeOnlineで標準搭載されているEOPの検知率では、十分とは言えません。「m-FILTER@Cloud」を導入することで安全なメール環境を提供いたします。



### 脱PPAP対策

ZIPパスワードロックに替わる安全な添付ファイル受け渡しをFinalCode暗号化もしくは暗号化強固オプションで実現いたします。

### FinalCode暗号化 / 暗号化強固オプション

OPTION



※暗号化強固オプションはCADファイルの暗号化はできませんので「FinalCode」と「CADファイル暗号化機能」オプションの購入が必要です。詳しくは営業までお問い合わせください。

### 「m-FILTER@Cloud」機能比較

	m-FILTER@Cloud	m-FILTER@Cloud MailFilter & Anti-Spam	m-FILTER@Cloud 誤送信対策版 ※1
誤送信対策機能	○	○	○
外部攻撃対策機能	○	○	×
受信時メール無害化機能	○	○	×
スパムメール対策機能	○	○	×
受信メールフィルタリング	○	○	×
アーカイブ機能	○	×	○ ※2
アーカイブ個人管理機能	○	×	○ ※2
mFILTER@Cloud Anti-Virus&Sandbox ※3	○	○	×
m-FILTER@Cloud Splunk 連携 ※3	○	○	×

※1 「m-FILTER@Cloud 誤送信対策版」はMicrosoft 365 / Google Workspace(旧 Office 365 / G Suite)のみの対応となります ※2 「m-FILTER@Cloud 誤送信対策版」のアーカイブ機能は送信済みメールのみが対象となります ※3 別途「m-FILTER@Cloud Anti-Virus&Sandboxオプション」の購入が必要です。 ※3 2022年5月10日発売

# FINALCODE@Cloud 「FinalCode@Cloud」の機能と特長

## 01. 暗号化したファイルは、指定した人やグループのみが閲覧でき、アクセス履歴が完全に追えて、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

「FinalCode」は、重要ファイルを暗号化し、利用状況の追跡と共に遠隔で削除もできるファイル暗号化・追跡ソリューション(ファイル暗号化ソフト)です。開封ユーザー・グループを限定してファイルを暗号化するため、転送による第三者への間接情報漏洩(二次漏洩)のリスクも生じません。暗号化ファイルは、配布後も動的に権限を変更できるため、従来では不可能だった重要ファイルの回収(削除)も簡単に実現します。

### 守る 高度なIRM※で指定した人・権限内でのみ操作可能。作成された瞬間に守ることができます

※IRM(Information Rights Management)とは、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です

- 🔒 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



**作成・保存**

ダウンロード

透過暗号.xlsx

透過暗号ファイルは従来の拡張子のまま、アイコンに鍵マークだけが追加され、指定されたドメイン名のメールアドレス保持者であれば開封はパスワード不要でダブルクリックのみです。

---

### 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できます

- 🔒 アクセスログ確認
- 🔒 操作ログ確認
- 🔒 不正閲覧検知



日時	アクセス日時	ファイル/フォルダ名	操作実行者のメールアドレス	アクセス先のIPアドレス	操作内容
Q	2019/01/29 10:43:36	test_20190118_1.pdf	fcnet@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	fcnet@dej.co.jp	192.168.240.21	印刷(透過暗号)
Q	2019/01/28 15:55:46	example.txt	fcnet@dej.co.jp	192.168.240.21	不可
Q	2019/01/28 15:55:08	example.pdf	fcnet@dej.co.jp	192.168.240.21	不可
Q	2019/01/24 14:40:33	example.txt	fcnet@dej.co.jp	192.168.240.21	不可
Q	2019/01/24 14:38:53	example.txt	fcnet@dej.co.jp	192.168.240.21	印刷キャンセル
Q	2019/01/24 14:38:19	testname002.txt	fcnet@dej.co.jp	192.168.240.21	印刷キャンセル

いつ    どのファイルに    誰が    どこから    何をした

---

### あとから消せる 渡したファイルを“あとから削除”することができます

- 🔒 リモートファイル削除
- 🔒 リモート権限変更



作成者 → 受信者

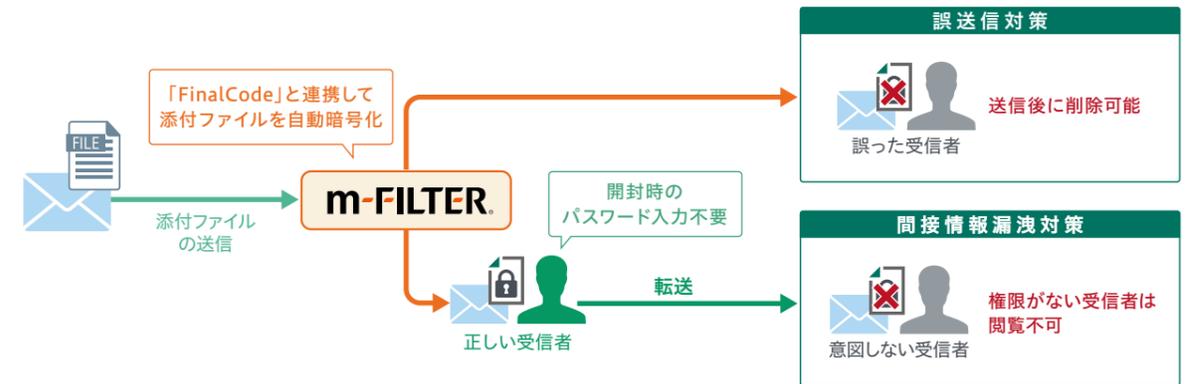
拡散する

削除する

## 02. 添付ファイルの暗号化をよりセキュアに

「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。送信者の暗号化の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5939953号



特許取得済み

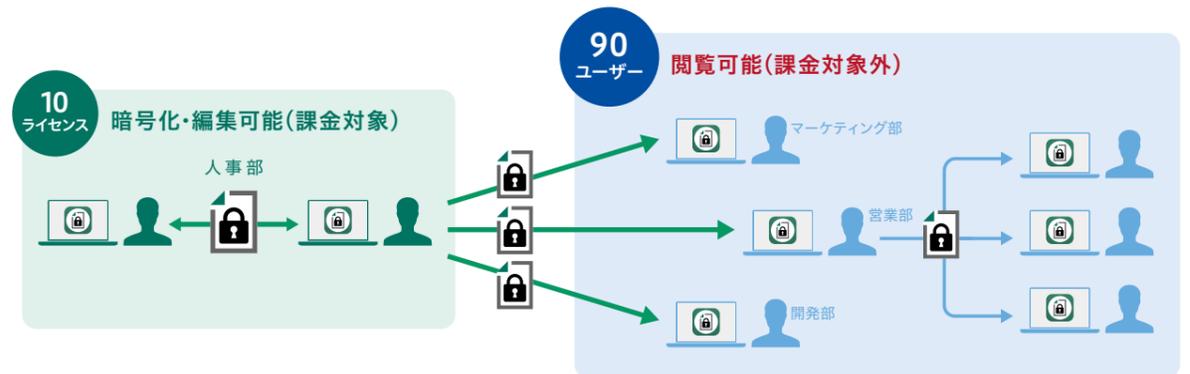
## 03. 「FinalCode」のもうひとつの魅力、利用のしやすさ・導入のしやすさで選ばれています

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」するのみの企業・団体内ユーザーは無償です。

※1「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  
 ※「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。透過暗号ファイルの閲覧するためには、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、有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 人事通達 >>> 🔒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



企業・団体外ユーザーは課金対象外

社外の取引先や委託先などの企業・団体外ユーザー※2も無償でファイルの閲覧ができます。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。

※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

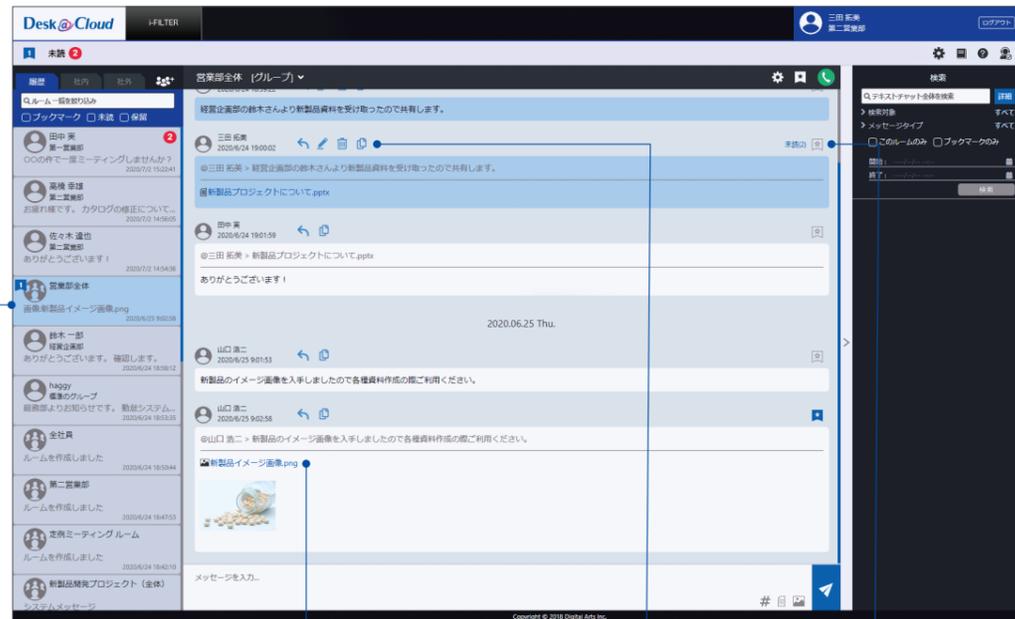
# Desk@Cloud 「Desk@Cloud」の機能と特長

## 高品質な通話、チャット、会議を、 どなたでも便利にセキュアに

テレワークが推進される昨今、社内会議やお客様との商談においてさまざまな手法が利用されていますが、デジタルアーツでは「純国産」のオンライン会議システムを開発し、場所を問わず「社内」「社外」のコミュニケーションシステムを提供しています。

### 01. テキストチャット

メールでの堅苦しさを削減したチャットによるコミュニケーションの導入によって、**情報伝達速度が飛躍的に向上します。**



社内タブに組織内のユーザーが一覧表示されるため、従業員によるユーザー登録が不要です

ファイル添付も可能。画像はサムネイル表示されるため、ダウンロードせずに閲覧可能です。また、「FinalCode@Cloud」のご利用で添付ファイルをFinalCode暗号化することも可能です

「返信」「編集」「削除」の機能が搭載されているため投稿ミスなども修正が可能です

「既読/未読」が表示されるため自分が投稿したチャットの状態把握が可能です。また、グループルームでは誰が「既読」かの把握ができるのでスムーズな情報伝達を実現できます

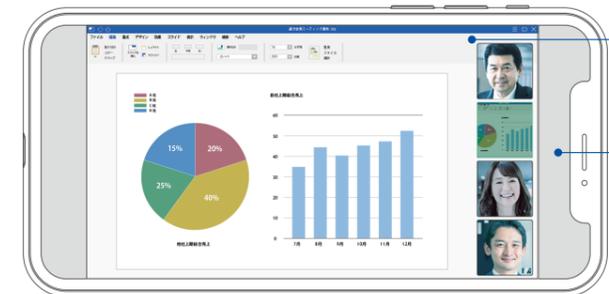
### 02. オンライン会議

「オンライン会議」を利用することで対面での打ち合わせと同様に、**資料を共有しつつお互いに表情を見ながら打ち合わせが可能です。**文字だけのコミュニケーションよりも細かいニュアンスの伝達に役立ちます。



カメラを利用することで、オンライン会議参加者の表情を確認することができるため細かいニュアンスの伝達も可能です

オンライン会議参加者が一覧表示されるため参加状態を一目で把握できます



デスクトップまたはアプリケーション（ウィンドウごと）の内容を共有できるため資料の事前配布なくオンライン会議が可能です

モバイルでのオンライン会議も可能なため、外出先からの参加もできます

#### 動作環境 (対応OS)

Windows用通知アプリ	Windows 10 Home, Windows 10 Pro, Windows 10 Enterprise, Windows 10 Education, Windows 11	対応ブラウザ	[Windows] Google Chrome, Mozilla Firefox, Microsoft Edge ※ Chromium版に限ります
iOS用「Desk@Cloudアプリ」	iOS 14 ~ 15.1		[iOS] Safari
Android用「Desk@Cloudアプリ」	Android 9 ~ 12		※ iOSでオンライン会議を実施する場合は「Desk@Cloudアプリ」で利用いただく必要があります

※オンライン会議につきましてはWindows, iOS, Androidでのみ動作保証いたします。オンライン会議をご利用いただくにはUDPの10000番ポートの開放を推奨いたします

#### ディスク拡張

標準の「Desk@Cloud」のディスク容量は3GBytes/ユーザーまで利用可能ですが、添付するファイルや写真などが多くなる場合はディスク容量を100GB単位で追加してご利用することが可能です。