校務系ネットワークのクラウド化に向けた

# Web・メール・ファイル セキュリティ

## 危険なWebサイトからのマルウェア感染を対策

i-FILTER@Cloud

- Webフィルタリング
- Webサービス制御
- 不審な通信の遮断
- 改ざんサイトからの感染対策
- ファイルのダウンロード制御
- 端末隔離

## 攻撃メールによる感染やうっかり誤送信を対策

m-FILTER@Cloud

- メール無害化
- 添付ファイル検知
- 脱PPAP対策
- 攻撃メール対策
- 誤送信対策
- メールアーカイブ

## 個人情報や校務に関わる重要ファイルを守る

FINALCODE@Cloud

- ファイル暗号化
- パスワードレス
- 印刷・編集制御
- 情報漏洩対策
- 閲覧者指定
- 内部不正対策

DigitalArts@Cloud

**「政府情報システムのためのセキュリティ評価制度」(ISMAP)に登録**

クラウドセキュリティサービス「DigitalArts@Cloud」は政府機関をはじめ、地方自治体、企業のお客様にとって信頼できるクラウドサービスとして、安心してご導入いただくことができます。
※「i-FILTER@Cloud GIGA スクール版」は ISMAP 対象外となります

## サイバーリスク情報提供サービス

「i-FILTER@Cloud」「m-FILTER@Cloud」の機能を利用して、マルウェア感染の疑いのあるお客様や弊社のお客様以外へも感染情報やホームページの改ざん情報を無償でお知らせします。

Dアラート® サイバーリスク情報提供サービス　特許※取得済み

※ 特許6716051号/改ざんの検知で特許を取得

## 「情報リテラシー授業」全国各地で実施中！

デジタルアーツでは、スマートフォン活用やインターネットにおけるルール＆マナー、インターネット上に存在するさまざまな危険とその対策を知っていただくための、情報リテラシー授業を行っております。


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





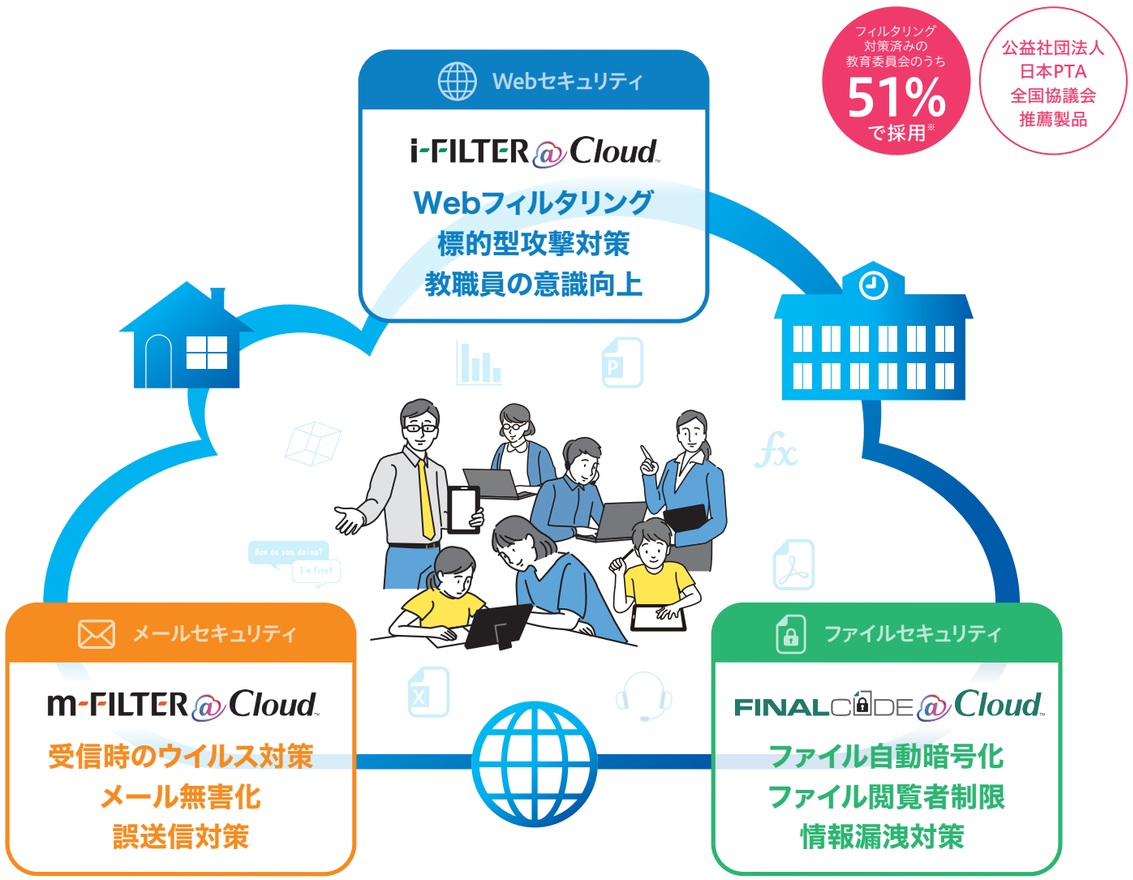
2022/10 DD-11570-001


DigitalArts

DigitalArts@Cloud

# 校務のクラウド化を安心安全に実現

## 校務・学習環境を守るWeb・メール・ファイルセキュリティ



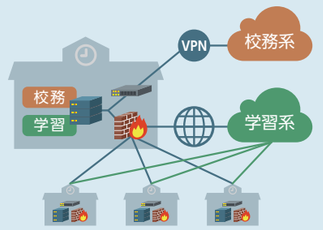

※ フィルタリング対策済みの教育委員会関係者へのヒアリング結果(2022年4月末時点)

## 校務ネットワークにおける「 教育情報セキュリティポリシーガイドライン 」の改訂ポイント

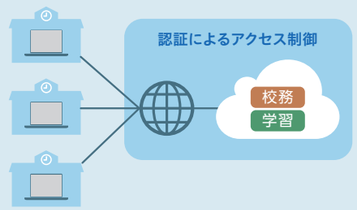
### ネットワークを分離しないことによる利便性向上を目指す

現在のローカルブレイクアウト構成から、今後はネットワーク分離を必要としない構成へ移行し、セキュリティ機器なども含めてクラウド化することで利便性の向上とコスト削減を推進していくことが求められます。

■ ローカルブレイクアウト構成




■ ネットワーク分離を必要としない構成



# ガイドラインに対応するデジタルアーツのWeb・メール・ファイルソリューション

## Guide Line 標的型攻撃対策

標的型攻撃による内部への侵入を防止するために対策を講じなければならない。また、内部に侵入した攻撃を早期チェックする対策が必要。

### デジタルアーツだけができる送信元の「ホワイト運用」により外部からのメール攻撃対策が可能

特許取得済み※ ※ 特許6669954号

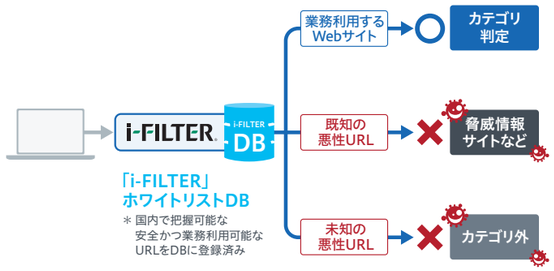
安全な送信元のIPアドレスとドメインの組み合わせを利用し、該当した安全な送信元からのメールのみを受信します。


## Guide Line 不適切なWebページの閲覧防止

不適切なWebページへの閲覧防止対策として「フィルタリングソフト」等を用いて、適切に整備することが重要。

### フィルタリングにより安全なサイトにのみアクセスを許可 業務に不適切なサイト閲覧などを細やかに制限することも可能

#### 推奨フィルター 圧倒的DB網羅率 99.88%※




「i-FILTER」ホワイトリストDB
＊国内で把握可能な安全かつ業務利用可能なURLをDBに登録済み

※2021年9月末時点の弊社調べ

#### Webサービス制御 特許取得済み※1


情報漏洩の観点で整理した国内外のWebサービスの機能を表示

Webサービスの機能を細かく制御 利便性への影響も最小限に

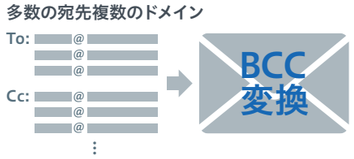
※1 特許5575341号 ※2「一般的なサービスであるかどうか（Popularity）」などの、リスクと無関係な指標とは性質が異なります

## Guide Line 電子メールの利用制限

業務上必要のない送信先への送信禁止、BCCの利用等の誤送信対策及び、電子メールのセキュリティ対策が必要。

### 誤送信対策やプライベートドメインへの送信を制御が可能 メールからの情報漏洩を対策

#### 強制BCC




多数の宛先や複数のドメインが宛先にある場合に、To・CcをBccに強制的に変換してメールを送信することが可能です。

#### プライベートドメイン宛送信制御


デジタルアーツのデータベースを利用し、プライベートドメイン宛の送信を制御することが可能です。

## Guide Line マルウェア対策

マルウェアを検知するためには、既存のパターンファイルから検出する手法に加え、ふるまい検知が有効。

### 「ホワイト運用」と「ふるまい検知」によりWeb・メールからのマルウェア感染を対策

「ホワイト運用」と「Anti-Virus & Sandbox」オプションと組み合わせることにより、Webとメールからのマルウェア感染を強固に対策できます。

ホワイト運用
安全なWebサイトとメールのみアクセス

＋

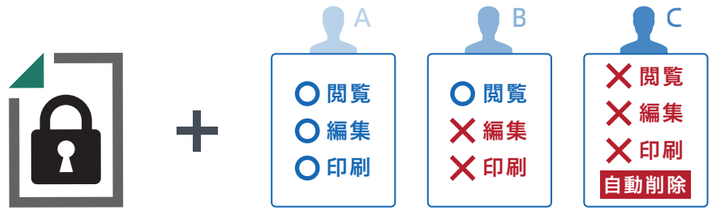
ふるまい検知
「ホワイト運用」と組み合わせて利便性向上

## Guide Line ファイルの暗号化

端末内のファイルを暗号化することで、暗号鍵を保持しない利用者は情報の閲覧等ができないようにする。

### ファイルを作成した瞬間から自動暗号化！閲覧や操作権限を制限することが可能

パスワードレスで強固な暗号化を実現し、ファイルの閲覧や編集等の制限を細かに設定できます。



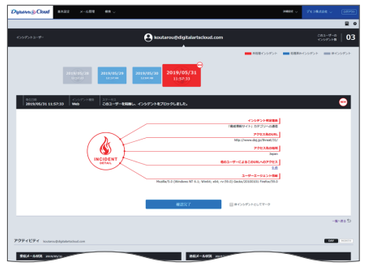

## Guide Line ログの取得等

各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

### Web・メール・ファイルの各種ログをグラフや件数ごとに検索することが可能

インシデント発生タイミング、該当ユーザー、判定理由等を分かりやすくグラフ表示します。


トップ画面




インシデント詳細レポート画面

### その他校務に役立つ便利機能

ITリテラシー教育を支援
**Test Board機能**

特許取得済み※1 ※ 特許5944568号


ユーザーが日々インターネットに初回アクセスする際に、ITリテラシーに関する選択問題を表示し、正解しないとインターネットにアクセスできないよう制御します。