

エンドポイントWebセキュリティ

i-FILTER®

ブラウザー & クラウド



標準提案書

デジタルアーツ株式会社

モバイル端末や持ち出しPCの課題

社員が利用する場合

営業社員に支給するスマートフォン



- ・移動時間に**業務外のサイト**を閲覧させたくない
- ・Webメールやワークフローに外出先からでも**迅速**に対応したい

在宅勤務やルート営業など社外で利用するPC、タブレット端末



- ・端末**OSに依存せず**使わせたい
- ・社外からでも**セキュア**に社内システムにアクセスさせたい

不特定多数が利用する場合

ホテルの客室やカフェの貸し出し端末



- ・お客様の**個人情報**を端末に記憶させたくない
- ・閲覧履歴から前のお客様の利用状況を**推測**させたくない

店舗利用のタブレット端末



- ・利用目的以外のサイトを閲覧させたくない
- ・ファイルの保存やブックマーク追加など**不要なデータ**を端末に残したくない

BYOD利用/児童利用

従業員の私物端末を業務利用



- ・シャドーITを撲滅し、BYOD端末を情シスの管理下に置きたい
- ・個人の端末に**業務情報**を保存させたくない

教育機関でのタブレット端末の活用



- ・自宅学習や校外学習など**学校の外でもセキュア**に利用させたい
- ・児童の学年に応じてフィルタリングの強度を変更したい

1



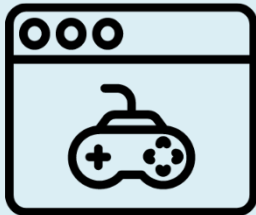
インターネットには学習に役立つWeb サイトがある一方で、カルトやテロ、アダルトといった不適切なWebサイトも数多く存在。

2



パソコンと同様にタブレット端末にもマルウェア（ウイルス）が存在し、そのほとんどがアプリとして侵入。

3



タブレット端末を学習以外の用途に使用してしまうケースもある。利用状況を把握し、不適切な使い方が多い場合には注意を促せるような仕組みも必要。

4



運用における管理者への負担が心配。
端末を管理するツールは、
わかりやすく直感的に使えることが重要。

製品概要

Webフィルタリング

柔軟かつ強固なインターネットアクセス制御を提供します。



私的利用の抑制
業務効率の向上

モバイル端末の課題

情報漏洩対策
店舗端末・BYOD活用

セキュアブラウザー

端末内にWebアクセスデータを残さないよう、管理者があらかじめ設定しておくことができます。

▶ 設定の対象となるデータ例

設定の対象となるデータ例			
キャッシュ	閲覧履歴	ID、パスワード	Cookie
画像、コンテンツ	文書ファイル	位置情報	検索履歴



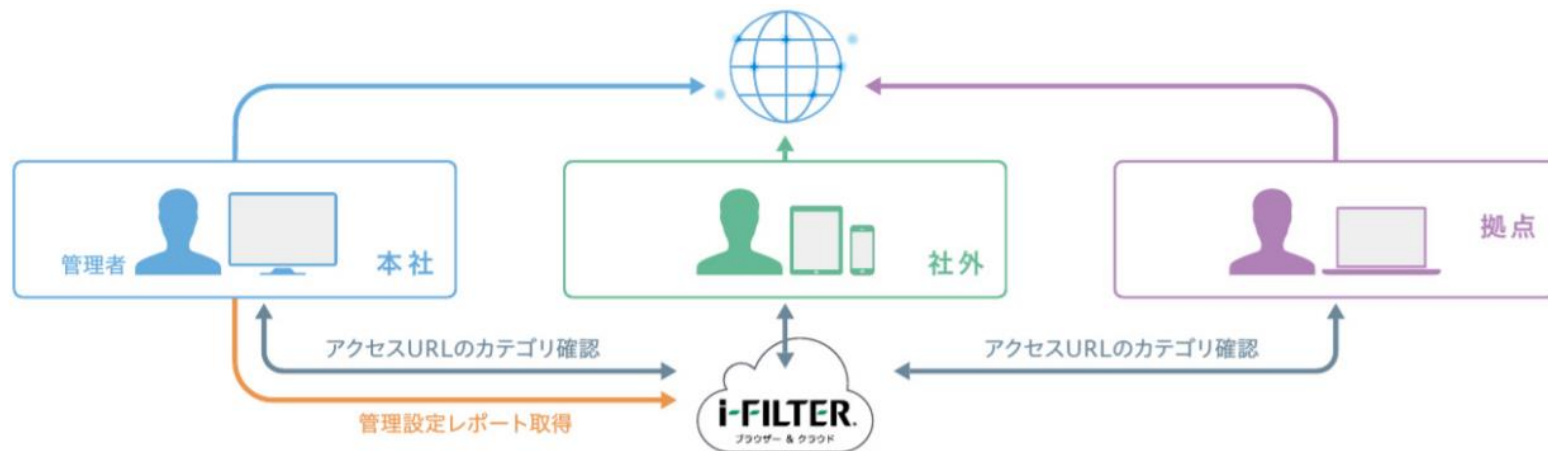
社内外のあらゆる端末の、SSL通信の内容まで含めてすべて可視化します。

ログ・レポート

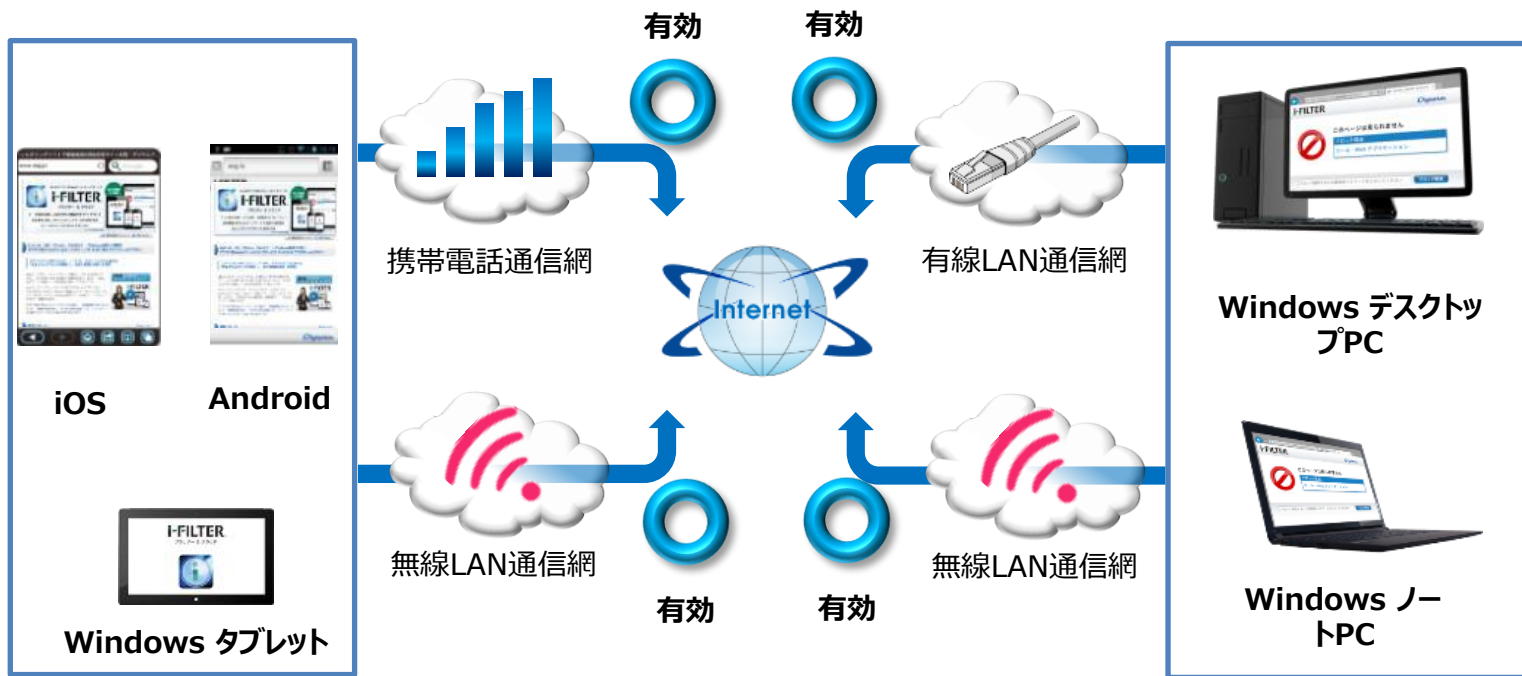
内部統制強化
Webアクセスの可視化



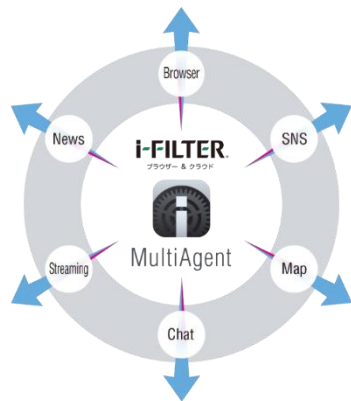
クラウドサービスだから、 複数の事業所も社外も全てサーバーレスで運用可能



従来の携帯電話で利用している通信網以外にも、**Wi-Fi技術**を利用した無線LANによる通信でもフィルタリングが可能です。**社内LAN環境**も、もちろん**有線・無線**に対応しているため、**通信環境に依存しません。**



※端末側での通信設定を規制していない際には対象外になる場合もあります。



すべてのアプリケーションに対応！ マルチアプリ対応エージェント

- 1 使い慣れた標準ブラウザでもフィルタリング
- 2 アプリケーションによらず通信を制御
- 3 メールのURLリンクを直接セキュアにアクセス可能

企業



アプリ内ブラウザで従業員が
業務時間内に**私的利用の
Web閲覧。**



専用ブラウザでは
メールリンクが開けない、
コピペする手間が面倒。



アプリケーションを問わないフィルタリングが必要

文教



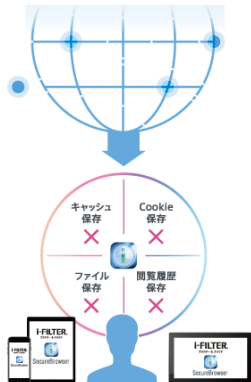
授業で使用する教材が
専用ブラウザーでは動かない。



授業で使用する教材アプリに
ブラウザー機能が付いているので
フィルタリングの抜道になる。



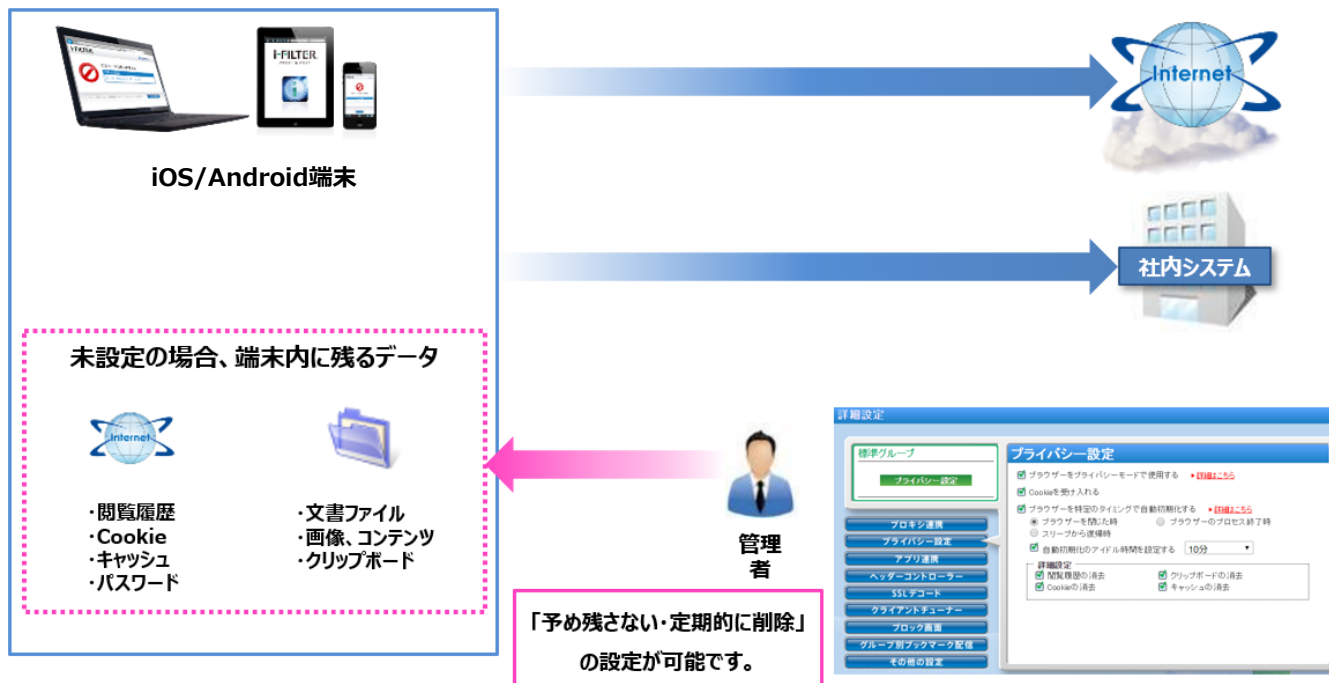
アプリケーションを問わないフィルタリングが必要



Webアクセス制御と情報漏洩対策機能を搭載した専用ブラウザ

- 1 Webアクセスデータを自動で削除
- 2 フィルタリングが標準搭載
- 3 クライアント証明書が必要なシステムも利用可能

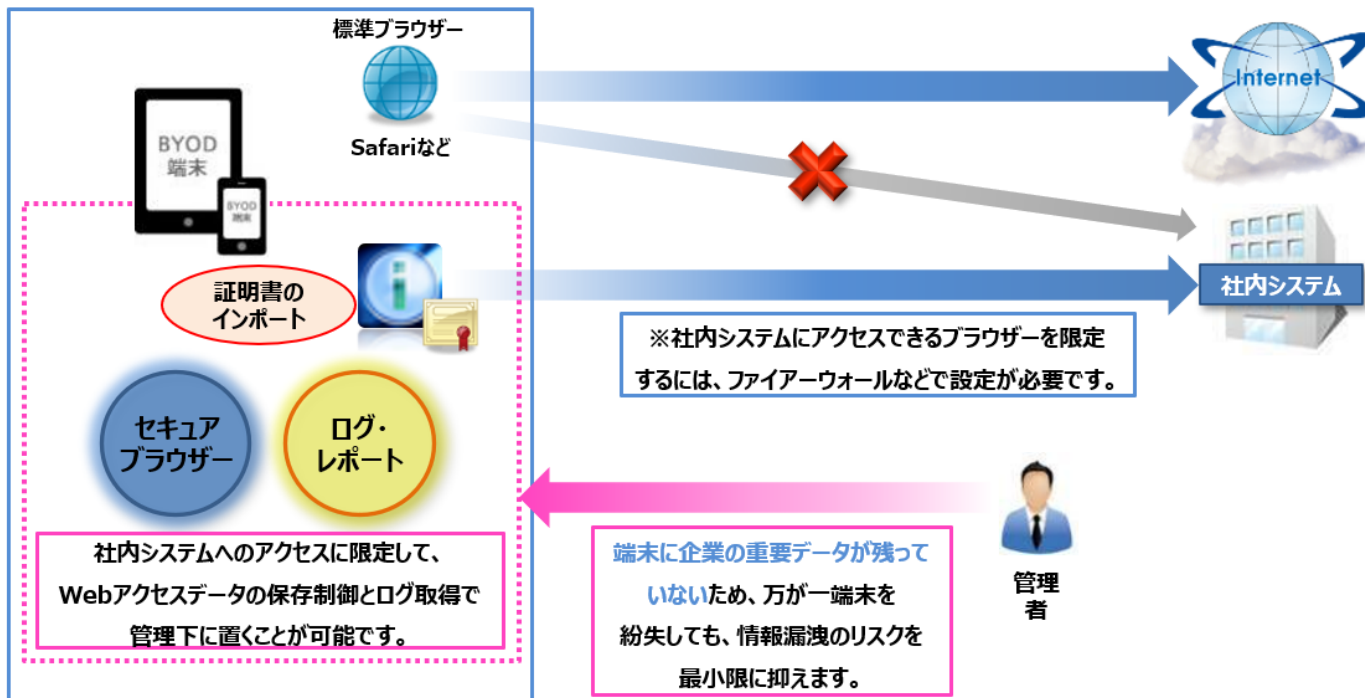
Webアクセスデータの端末保存を、管理者が予め制限可能



※掲載の図案は、資料作成用のイメージカットであり、実物とは異なる場合がございます。

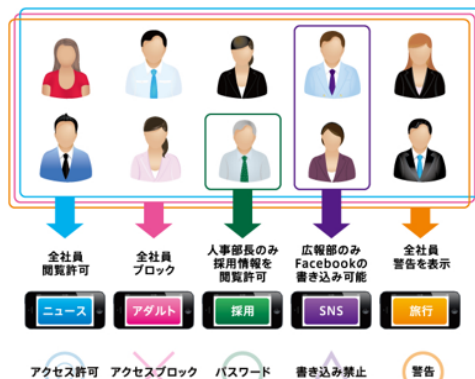
社内システムへのアクセスのみ管理下に！

※SecureBrowser for iOS、Androidが対象



その他機能

■グループごとのポリシー変更可能



許可/ブロック/警告/パスワード から
ブロックアクションを設定可能です。

カテゴリ毎にPOST(書き込み)の禁止や
POSTサイズの上限を設定可能です。

※MultiAgentが対象

■Web閲覧の利用時間帯も制御可能 (インターネットタイマー)



※掲載の図案は、資料作成用のイメージカットであり、
実物とは異なる場合がございます。

曜日ごとにインターネットの利用時間帯
を設定したり、1日に利用可能な時間を
設定可能です。

■マルチOSの一元管理

iOS
Android
Windows



■ Gmailの個人アカウント利用をブロック

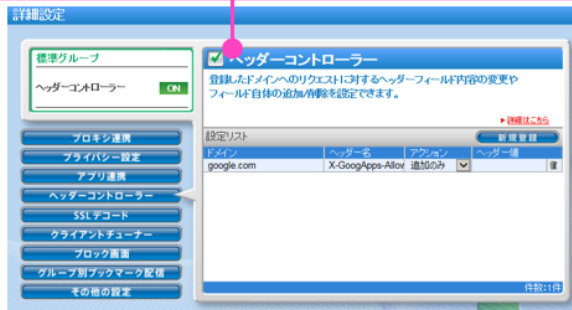


登録ドメインへのリクエストに対してヘッダーフィールドを編集することが可能です。

※MultiAgent for iOS、Windowsが対象。

※「i-FILTER ブラウザー&クラウド」からの接続時のみ有効です。

SecureBrowserはGmailアプリからの接続時はフィルタリングされません。



■ URL指定でブロックの対象・除外も判別可

カテゴリ設定と併用して、ブロック除外・対象サイトを登録することが可能です。

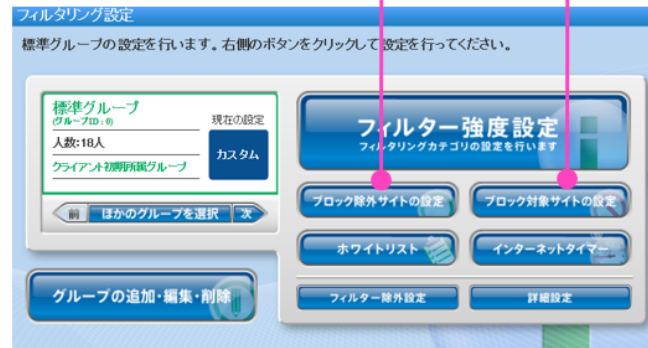
・URLの一致条件：部分一致

・登録上限値：2,000/グループ

※URLの一括インポート・エクスポートも可能

※登録されたサイトのみアクセスを

可能にするホワイトリスト機能も標準搭載。

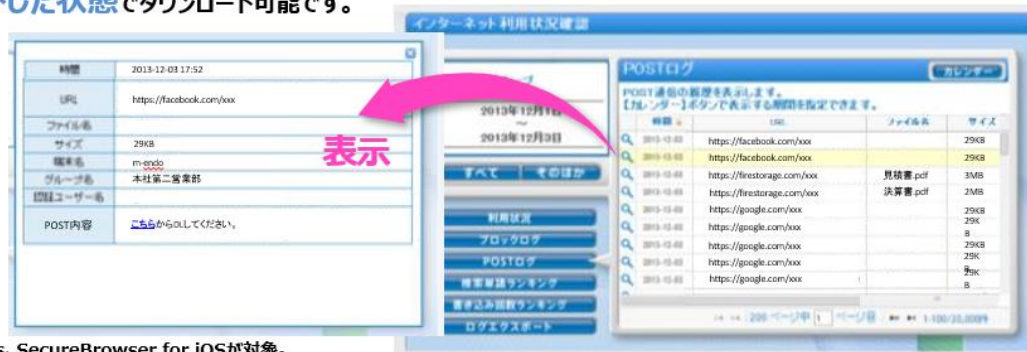


※掲載の図案は、資料作成用のイメージカットであり、実物とは異なる場合がございます。

■ POSTログ

従業員の掲示版やSNSへの書き込みの内容や、オンラインストレージへアップロードしたファイル名を、

SSLサイトでもデコードした状態でダウンロード可能です。



※MultiAgent for Windows、SecureBrowser for iOSが対象。
(SecureBrowser for iOSはPOST内容のダウンロードはできません)

■ SSLデコード設定

金融機関のWebサイトはデコード除外をしたいなど、

ドメインによってデコード設定を選択することが可能です。

※MultiAgent が対象。

※SecureBrowser は専用ブラウザのため、デコードの必要がありません。

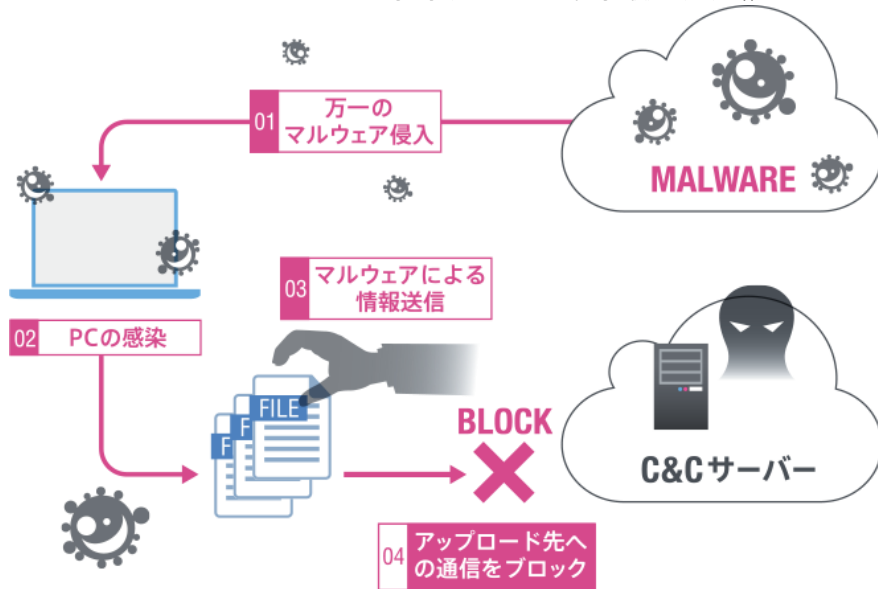


※掲載の図案は、資料作成用のイメージカットであり、実物とは異なる場合がございます。

エンドポイントにおける全プロセスの WEB通信を制御、インシデントの有無を「検知・遮断」

ドライブバイダウンロード攻撃に利用されるサイト、水のみ場攻撃に利用されるサイト、マルウェアを配布するサーバーへの通信を遮断し、入口・出口対策が可能です。

※ 感染したマルウェア等が行う特徴的な通信における、通信先サイトを遮断対象とします。
※ 全てのマルウェア等の挙動及び悪意ある行為の検知・遮断を保証するものではありません。



■ 脅威情報DB連携組織



LAC

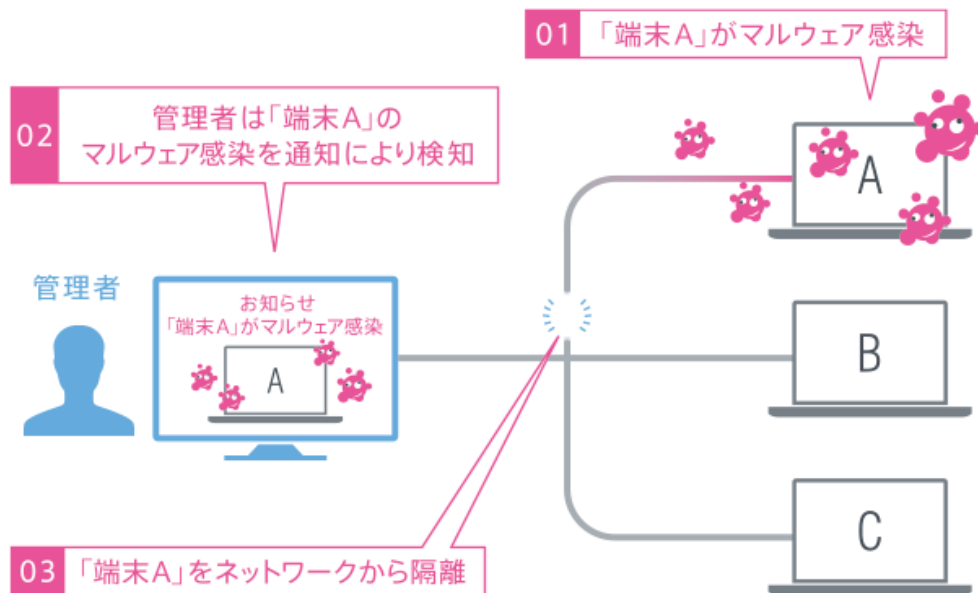
株式会社ラックのセキュリティ監視センターJSOCの解析による脅威サイト情報で情報詐取目的のWebアクセスを遮断します。



国立研究開発法人情報通信研究機構（NICT）

「NICTER」のハニーボットやWebクローラからマルウェアの機体を常時収集し、静的解析エンジン及び動的解析エンジンで解析、相関分析システムでマッチングしたマルウェアが持つ悪性URLのデータベースを提供いたします。

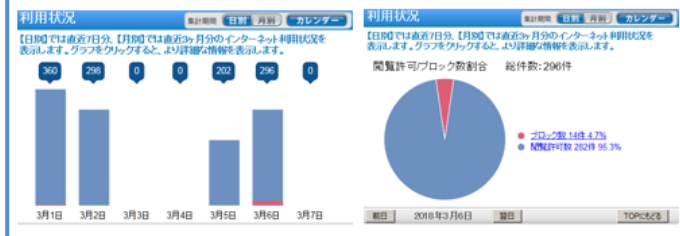
端末利用者が危険なサイトへアクセスした際に
管理者へ通知し、外部端末を遠隔操作でネットワークから隔離



■ アクセスレポート

アクセス数・ブロック数とそのカテゴリ内訳を表示可能です。

- ・日別アクセスレポート
- ・月別アクセスレポート



■ ランキング

掲示板やブログなどのコミュニティサイトで良く書き込まれるサイトのランキング、検索に使用した単語のランキングを表示可能です。

- ・日別書き込み回数ランキング(100位まで) ※1
- ・月別書き込み回数ランキング(100位まで) ※1
- ・日別検索単語ランキング(100位まで)
- ・月別検索単語ランキング(100位まで)

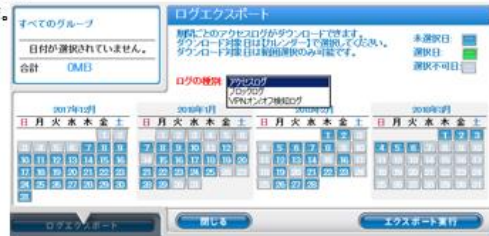
※1 MultiAgent, SecureBrowser for iOSが対象。

■ ログエクスポート

選択した日付のアクセスログ、ブロックログ、VPNオン/オフ検知ログを出力可能。

※過去90日から前日までが出力対象。

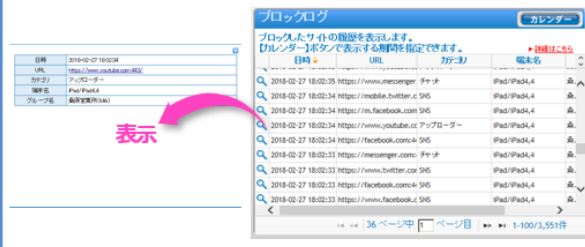
※当日のアクセスログ出力は不可。



※掲載の図案は、資料作成用のイメージカットであり、実物とは異なる場合がございます。

■ ブロックログ

ブロックされたログだけを抽出して、管理画面上で確認可能です。



Dコンテンツ

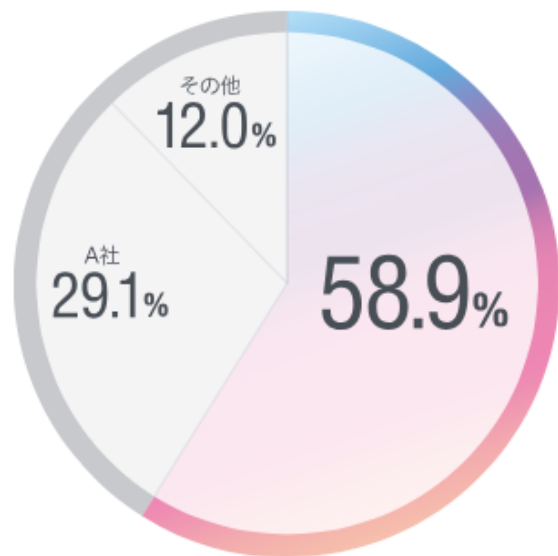
Web上の学習用動画を集約し、**学年や教科による検索が可能！**
児童・生徒の自由な学びをサポートします

SecureBrowserから
すぐにアクセス可能！

※画像は管理者の画面です

導入事例

SaaS型URLフィルタリング市場： ベンダー別売上金額シェア（2021年度）



※ 出典：ITR「ITR Market View：サイバー・セキュリティ
対策市場2023」SaaS型URLフィルタリング市場：ベンダ
ー別売上金額シェア(2021年度)（2023年5月発行）



🚩 梶山女学園大学附属小学校

🎓 常翔学園中学校・高等学校

🌸 瀧野川女子学園中学高等学校
Takinogawa Girls' School



学校法人桐蔭学園



関西大学初等部

事例紹介ページ：<https://www.daj.jp/bs/case/?product=ifb>



背景

- ・ 3万7000台のタブレットを業務活用
 - 駅員/ 乗務員/ 保線/ 電気設備/ 土木/ 建設などの現場業務において活用

脅威

- ・ インターネット利用時の情報漏洩や私的利用

万が一のセキュリティインシデントのフォレンジック解析

セキュリティ・インシデントが発生した場合、
履歴確認を行い迅速なフォレンジック調査を実施可能。



生徒がアプリや検索エンジンを主体的に選択し、 安心・安全に情報へアクセス可能な授業を実現



多くのタブレット端末導入校が抱える問題のひとつとして、Webブラウジング機能をもつアプリケーションに対してフィルタリングが機能せず、管理者が把握できない通信の抜け道ができてしまうことがありました。しかし、『MultiAgent for iOS』は、ChatやSNS、NEWS、MapなどiPadに導入されたすべてのアプリに対してWeb通信をフィルタリングできるため、インターネットへのアクセスが多い授業でも安心して活用できます。

ネットに関するトラブル防止を最優先「i-FILTERブラウザー&クラウド」の導入

④ 梶山女学園大学附属小学校

**アクティブ・ラーニングの実践・学びを
安心・安全に支えるツールとして活用し、
私物端末によるタブレットの一人1台体制を実現**

学習用途としてタブレットが有効であるとはいえ、情報モラルや情報リテラシーが発達段階にある小学生が使うことについては、教員も保護者も不安

年齢や学年ごとに情報リテラシーや情報モラルが異なる教育機関においては、児童の成長に合わせた柔軟なフィルタリングの設定が求められ、「i-FILTERブラウザー&クラウド」ならこうした要望にも対応

ご利用料金

初期費用	0円
月額費用	330円（税別）

■ご利用条件

※最低利用期間：6ヶ月 以降1ヵ月ごとに自動更新

※最低契約数:5IDとなります。

※契約月は月額費用がかかりません。契約月の翌月から月額費用が発生致します。

他製品との連携

スマートデバイスのリスクと対策ソリューション

分類	リスク	対策ソリューション
ネットワーク	不正アクセス	SSL-VPN/IP-VPN
	なりすまし	クライアント証明書認証 デバイス認証
エンドポイント	端末の盗難・紛失	MDM
	端末内データの漏洩	シンクライアント/DaaS
		リモートアクセス
		アプリケーション管理
		セキュアブラウザー Webフィルタリング
		DLP
	不正プログラム	ウイルス対策ソフト



他社製品連携の
導入事例について
は
提供元会社
にお問合せください。

クライアント証明書の読込が可能。

他社MDM製品のオプションとして購入も可能。

提供元	製品名
インヴェンティット株式会社	
株式会社オプティム	
富士通株式会社	

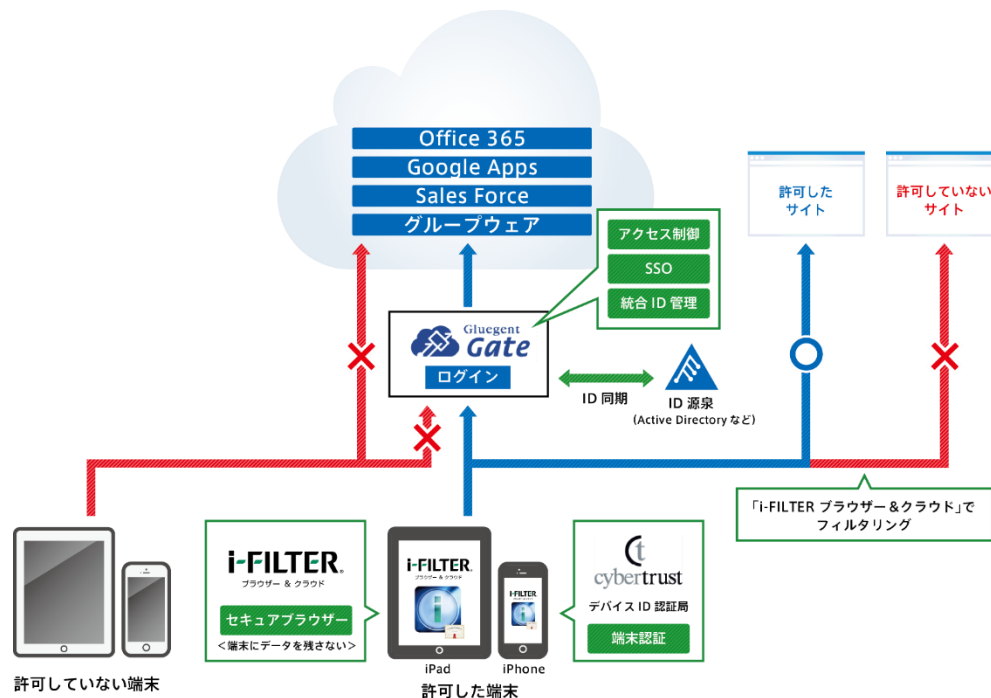
他社セキュアブラウザー製品のオプションとして購入も可能。

提供元	製品名
株式会社 アイキューブドシステムズ	

検証済みの他社サービス

提供元	製品名
サイボウズ株式会社	
e-Janネットワークス株式会社	CACHATTO

「Gluegent Gate」、「デバイスID」と連携し 利便性とセキュリティを両立



•iOSのみ
•Ver.4.6以降対応

FAQ

Q 質問	社内ネットワークを通して「i-FILTER ブラウザー&クラウド」を利用できますか？
A 回答	利用できます。 「i-FILTER ブラウザー&クラウド」でフィルタリングを行うためには、弊社サーバーへのアクセスを必要とします。プロキシサーバーや、上流のファイアウォールなどにおいて、弊社へのアクセスが遮断されている場合には正常な動作を得られない場合がございます。 設定内容については弊社サポートセンターまでお問合せください。
Q 質問	文字化けを起こすサイトがあります。なぜですか？
A 回答	文字コード(charset)が指定されていないサイトでは文字化けを起こす場合があります。 端末側で文字コードを変更しても解消されない場合があります。 こちらは制限事項となります。予めご了承ください。
Q 質問	iOS版/Android版で提供されている専用ブラウザーは何をベースに開発されていますか？
A 回答	iOS版はSafariのWebKit、Android版では標準ブラウザーのWebViewをエンジンとして開発しています。
Q 質問	Android版でPOSTフィルターやPOSTログが取得できないのはなぜですか？
A 回答	Android版は、Android OSに含まれる標準ブラウザーのエンジンを利用して開発されていますが、Android OSの制約により、メソッドを取得できないためです。

Q 質問

ログのフォーマットについて教えてください。

A 回答

■ エクスポートしたログの例

Feb 12 11:58:24 0 300/00 - 192.168.15.1 develop%2fiPhone4 testuser [12/Feb/2012:11:58:24 +0900]
 "GET http://abcdef.co.jp/ HTTP/1.1" http://www.abcdef.co.jp/search - 200 0 0 block 0 -1 90 businessgroup
 %2a%2f%2a - - - 00000000

ログフォーマットの項目は下記の通りです。

項目値	出力値
アクセスログを出力した時刻	Feb 12 11:58:24
プロセスID	0
「i-FILTER」バージョン情報	300/00/
上位プロキシサーバーのアドレス	-
クライアントIP アドレス	192.168.15.1
端末名	develop%2fiPhone4
認証ユーザー名	testuser
アクセス日時	[12/Feb/2012:11:58:24 +900]
METHOD URL HTTP バージョン	"GET http://www.abcdef.co.jp/ HTTP/1.1"
referer	http://www.abcdef.co.jp/search
URL エンコードされたUserAgent	-
レスポンスコード	200
レスポンスサイズ	0

項目値 (続き)	出力値
リクエストサイズ	0
フィルターアクション	block
当該リクエストを処理したルールに割り当てられたオブジェクトID の出力	0
フィルター理由番号	-1
URL カテゴリリスト	90
グループ	businessgroup
URL エンコードされたContent-type	%2a%2f%2a
SSL 内部パラメータ	-
POST 時のファイル情報	-
ウイルス名	-
チェックサム	00000000

※灰色の項目値は、「i-FILTER Server」Ver.8/8.5とログフォーマットを揃えるためのもので、出力値は固定値です。

エンドポイントWebセキュリティ

i-FILTER®

ブラウザー & クラウド



- 本書は2024年3月現在の情報に基づいて作成しております。（※記載内容は予告無く変更される場合があります）
- デジタルアーツ、DIGITAL ARTS、i-FILTER、i-FILTER Anti-Virus & Sandbox、i-FILTER@Cloud Anti-Virus & Sandbox、i-FILTER@Cloud Dアラート発信レポートサービス、info board、Active Rating System、D-SPA、Anti-Virus & Sandbox for 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@Cloud Dアラート発信レポートサービス、m-FILTER MailAdviser、MailAdviser、m-FILTER File Scan、Mail Detox、m-FILTER EdgeMTA、EdgeMTA、FinalCode、DigitalArts@Cloud、Desk、Desk Event、StartIn、i-FILTER、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。

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
Tel 03-5220-3090 Fax 03-5220-1130
sales-info@daj.co.jp www.daj.jp