

# PASOLOG Manager

## 操作マニュアル

2018/10

株式会社フーバーブレイン

## 目次

1. はじめに.....	5
2. 基本コンセプト.....	6
2.1. 動作環境.....	6
2.2. 設定と運用手順.....	7
2.3. ポリシー作成の基本的な考え方.....	7
3. 開始と終了.....	7
3.1. ログイン.....	8
3.2. ログアウト.....	9
4. ダッシュボード.....	9
5. 管理者設定.....	10
6. ライセンス設定.....	12
7. サーバー設定.....	13
7.1. プロキシ設定.....	13
7.2. メール設定.....	14
7.3. 印刷設定.....	15
7.4. 部署マスター設定.....	17
7.5. データメンテナンス.....	18
7.6. その他設定.....	19
8. ポリシー設定.....	19
8.1. 基本設定.....	20
8.1.1. クライアント表示設定.....	20
8.1.2. クライアント GPS 送信設定.....	20
8.1.3. デスクトップ画像送信.....	21
8.1.4. USB メモリ使用禁止.....	22
8.1.5. WPD 使用禁止.....	22
8.1.6. クライアント アンインストール時のパスワード入力.....	22
8.1.7. メッセージ送信.....	22
8.2. 印刷設定.....	23
8.2.1. 印刷制限(一ヶ月に印刷できる枚数).....	23
8.2.2. 透かし印刷設定.....	24
8.2.3. 透かし除外設定 - ドキュメント(ファイル名)除外.....	25
8.2.4. 透かし除外設定 - プリンターを指定して除外.....	25

---

8.3. 日報送信設定 .....	25
8.3.1. 送信対象 .....	25
8.3.2. 送信先 .....	25
8.3.3. 日報送信時間.....	25
8.3.4. 件名 .....	26
8.4. 利用禁止ソフトウェア .....	26
8.4.1. 禁止指定方法.....	26
8.5. 情報漏えい(マイナンバー等)対策 .....	28
8.5.1. 個人情報スキャン .....	28
8.5.2. クリップボード監視 .....	28
8.5.3. ファイル操作ログを取得する.....	30
9. クライアント .....	32
9.1. 作成した部署へ PC を移動 .....	32
9.2. 割り当てポリシーを変更する .....	33
9.3. 削除 .....	33
9.4. PC 位置情報一覧.....	33
9.5. 強制アンインストール .....	33
9.6. IE や、脆弱性報告の多いアプリケーションの確認 .....	34
9.7. その他のクライアント情報.....	34
10. ソフトウェア .....	37
10.1. ソフトウェア別 .....	37
10.2. 禁止ソフト .....	38
10.3. クライアント別 .....	38
10.4. Hotfix 別.....	38
10.5. 脆弱報告の多いソフトウェア別 .....	38
10.6. OS 導入.....	38
10.7. Office 導入 .....	38
10.8. ウイルス対策ソフト .....	39
10.9. ライセンス .....	39
11. 全体分析 .....	40
11.1. クライアント数推移 .....	40
11.2. ソフト使用率 .....	41
11.3. 作業内容 .....	42
11.4. 印刷.....	42
11.5. USB コピー操作 .....	42

11.6. ブラウザ操作 .....	43
12. ユーザー別(月) .....	44
12.1. グリッド形式 .....	44
12.2. ツリー形式 .....	46
13. USB 使用履歴 .....	47
13.1. ログデータ .....	47
13.1.1. 期間を指定して検索 .....	47
13.1.2. コンピューター名などの情報を指定して検索 .....	47
13.1.3 さらに絞り込む .....	48
13.2. 集計データ .....	48
14. USB 一覧 .....	48
15. 作業内容 .....	49
15.1. ログデータ .....	49
15.2. 集計データ .....	49
16. 印刷 .....	50
16.1. ログデータ .....	50
16.2. 集計データ .....	50
17. 禁止ソフト起動 .....	50
18. 個人情報 .....	50
19. Manager ログイン .....	51
20. ファイル操作 .....	51
21. クリップボード操作 .....	52
22. URL アクセス .....	53
23. サーバー監視 .....	53
24. メッセージ送信機能 .....	56
24.1. 前提条件 .....	56
24.2. メッセージ送信 .....	57
24.3. メッセージ受信 .....	58
24.4. メッセージ一覧 .....	59

本書に含まれるすべてのテキスト、図表は株式会社フーバーブレインの独占的所有物であり、顧客の個人的かつ非営利目的での使用に供するものです。弊社からの文書による承諾なしに、本内容のいかなる部分をも、いかようにも修正、複製、配布、送信、展示、実演、再生、出版、ライセンス、類似物製作、譲渡、使用もしくは販売することはできません。本書の情報は、通告なしに変更される場合があり、株式会社フーバーブレインに責任あ

るいは説明義務が生じることはありません。また、この文書に記載されるその他の登録済みならびに未登録の商標はすべて各々の商標の所有者の財産です。

## 1. はじめに

このマニュアルは、PasoLog Manager の操作手順について記述したマニュアルです。

PasoLog クライアントプログラムの動作手順については、PasoLog クライアントのマニュアルをご参照ください。

PasoLog Manager は、企業などの組織において、各クライアントにインストールされた PasoLog クライアントを一元管理するための管理者専用のツールです。

PasoLog Manager の主な特徴は、以下のとおりです。

1. クライアント PC にインストールされた PasoLog クライアントが定期的を取得し、PasoLog Manager に送信したログ情報を収集し、管理者にわかりやすい GUI で画面表示します。
2. 管理者がクライアント PC で印刷する印刷物に印刷情報(透かし)を自動的に挿入することや、印刷したユーザーや印刷物の情報をログ情報として取得することができます。万一、印刷物の情報が流出した場合に、流出経緯・範囲の追跡に活用することができます。
3. USB 接続の記憶機器や Windows Portable Device (WPD)への操作履歴を記録し、ファイルの持ち出しや持ち込みを検知することができます。
4. 個人情報に関するデータのコピー操作などのログ情報を取得し、個人情報の漏えいが発生した場合の流出経緯・範囲の追跡に活用することができます。
5. 管理者は PasoLog Manager で事前に設定することにより、クライアント PC に対して以下の制御を行うことができます。
  - ① USB 接続の記憶機器や WPD の使用禁止あるいは書き込み禁止の制御を行うことができます。
  - ② 印刷の禁止や強制的な透かし印刷の実施、印刷物の枚数制限の制御を行うことができます。
  - ③ ユーザーに意識されないよう PasoLog のアイコンをタスクトレイ等に表示させない設定ができます。
6. プログラムは手動、自動で簡単に更新することができます。

## 2. 基本コンセプト

この章は大変重要ですので、必ずお読みください。

PasoLog Manager は、誰でも簡単に導入、設定、運用ができるように、直感的に理解できる GUI を採用しています。ただし、製品の基本コンセプトである下記の「設定と運用手順」と「ポリシー作成の基本的な考え方」をお読みいただくことで、製品についてより深く理解していただけます。

ポリシーは、クライアント PC から 30 分間隔(初期値)で自動更新します。またいつでも手動で更新できます。

### 2.1. 動作環境

Web ブラウザ環境	Chrome(推奨)、または IE9 以上
画面解像度	1024 x 768 以上 (1280 x 1024 推奨)

## 2.2. 設定と運用手順

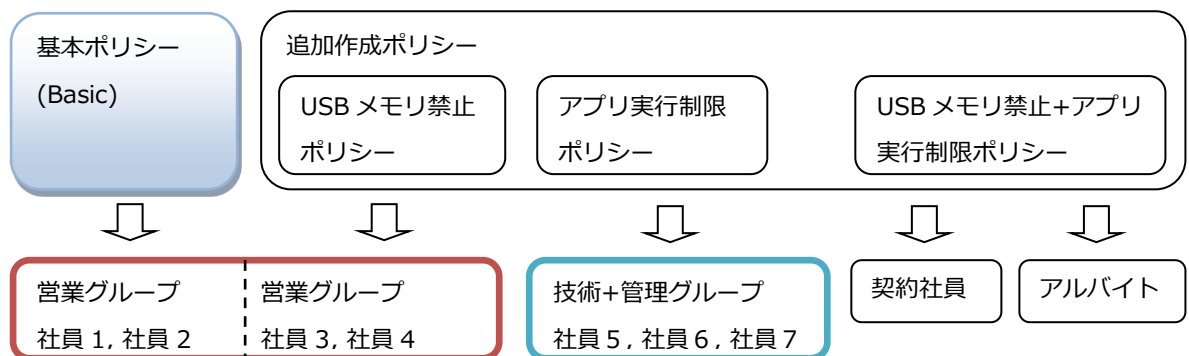
PasoLog Manager の設定と運用の手順は以下になります。

- 管理者のログイン(管理者 ID、パスワードが必要です)
- ライセンス設定・確認
- 管理者パスワードの変更
- 管理者の追加(作業レベルに応じて複数の管理者を追加できます)
- 通知メールの環境設定
- ポリシーの作成(複数作成できます)
- PasoLog クライアントプログラムのインストール情報を各クライアントに配信
- ユーザー情報の確認、または、各クライアント別の設定を変更
- ログの監視、分析
- ポリシーの見直し

## 2.3. ポリシー作成の基本的な考え方

全てのクライアントは、自動作成される Basic ポリシーが適応されます。

システム管理者は Basic 以外のポリシーを自由に追加作成し、クライアントに割り当てることができます。



## 3. 開始と終了

PasoLog Manager はブラウザベースの管理コンソールです。管理者はブラウザを利用して PasoLog Manager へログインして操作します。



### 3.1. ログイン

管理者はブラウザを利用して、PasoLog Manager へログインできます。

■ PasoLog Manager を社内に設置した場合。

<http://ip-address:7080/akad/>

**ip-address** は、PasoLog Manager に設定した IP アドレスに置き換えてください。



管理者 ID、パスワードの初期値は、「Admin」「Admin」です。大文字・小文字を正しく入力してください。  
初期パスワードは、ログイン後、「管理者設定」から速やかに、変更することを強く推奨いたします。

#### パスワードを忘れた場合

ログイン画面の「パスワードを忘れた場合」をクリックします。

表示された画面に、管理者のメールアドレスを入力し、「送信する」をクリックすると、該当の管理者のメールアドレスにパスワード再設定のメールが送信されますので、パスワードの再設定をしてください。

上記の機能は管理者のメールアドレスが正しく設定されている場合のみ有効です。

## 3.2. ログアウト

PasoLog Manager 画面の右上にある「ログアウト」ボタンをクリックすることでログアウトできます。

EX AntiMalware Managerへ | ヘルプ | デザイン変更 | 言語変更 | **ログアウト**

PasoLog Manager の操作が行われなまま一定時間を経過した場合は、自動的にセッションが切れます。その場合は、再度ログインしてください。

## 4. ダッシュボード

PasoLog Manager にログイン後「ダッシュボード」タブが最初に表示されます。

ダッシュボードでは PasoLog Manager の状況を確認することができます。

### 【主な項目】

#### ・作業内容(直近 3 ヶ月)

全クライアントの作業内容から、作業時間の多いものから表示します。

#### ・Office インストール状況

インストール済みのソフトウェアから、「Office」を含むソフトを抽出しインストール率を表示します。

#### ・ライセンス情報

ご購入いただきました「ライセンス数」や、インストール台数、残りライセンス期間等を表示します。

他にも PasoLog Manager の状態が確認できるダッシュボードがいくつかあります。

ブラウザへ表示するダッシュボードは、「ボード追加」から、追加できます。

またブラウザ上に表示しないダッシュボードは、「ボード削除」から、削除できます。

## 5. 管理者設定

「管理者設定」から、PasoLog Manager を管理するための管理者の作成、削除や編集などができます。



管理者ID	Admin
管理者名	管理者
新パスワード	新パスワード
新パスワード(確認用)	新パスワード(確認用)
メールアドレス	メールアドレス
ロック	<input type="checkbox"/>

複数の管理者の作成や、管理者の権限設定ができます。デフォルトで設定されている「Admin 管理者」の削除はできません。Admin 管理者には、管理者の追加 / 編集 / 削除とすべての操作ができます。

新しい管理者を追加するには、「新規」をクリックします。

新規作成する管理者の管理者 ID、管理者名、パスワード等を入力し、「保存」をクリックします。

管理者を追加したら、「戻る」をクリックして新しい登録内容を確認します。

管理者作成数の上限はありません。管理者 ID は、24 文字以内の半角大文字・半角小文字、数字、アンダーバー(\_)、ハイフン(-)が使用できます。管理者名は任意の 50 文字以内で入力します。

新しいパスワードは、4 文字以上、24 文字以内の半角大文字と半角小文字、数字、アンダーバー(\_)、ハイフン(-)が使用できます。

メールアドレスは、管理者への通知メールが送信されます。

ログイン画面の「パスワードを忘れた場合」で、送信される送信先のメールアドレスはここで設定されたメールアドレスです。

ロックは、一時的に特定の管理者をログインできない状態にします。なお、Admin 管理者はロックできません。

管理者権限は、管理コンソールで管理者がアクセスできる機能の設定です。デフォルトではすべての機能が無効になっています。有効にするにはチェックを入れてください。

2) 管理者権限  すべてチェック

クライアント情報	<input checked="" type="checkbox"/> クライアント	<input checked="" type="checkbox"/> ソフトウェア
USB管理	<input checked="" type="checkbox"/> USB使用履歴	<input checked="" type="checkbox"/> USB一覧
作業分析	<input checked="" type="checkbox"/> 全体分析	<input checked="" type="checkbox"/> ユーザー別(月)
ログ情報	<input checked="" type="checkbox"/> 作業内容	<input checked="" type="checkbox"/> 印刷
	<input checked="" type="checkbox"/> 禁止ソフト起動	<input checked="" type="checkbox"/> 個人情報
	<input checked="" type="checkbox"/> Managerログイン	<input checked="" type="checkbox"/> ファイル操作
	<input checked="" type="checkbox"/> クリップボード操作	
サーバー監視	<input checked="" type="checkbox"/> サーバー一覧	<input checked="" type="checkbox"/> ファイル操作
各種設定	<input checked="" type="checkbox"/> ポリシー設定	<input checked="" type="checkbox"/> 管理者設定
	<input checked="" type="checkbox"/> サーバー設定	<input checked="" type="checkbox"/> ライセンス設定

## 6. ライセンス設定

「ライセンス設定」は、本製品を使い始める際に必要です。

以下の手順によりライセンスを設定してください。

この作業は、インターネット接続環境が必要です。

プロキシをお使いの場合、次ページの「サーバー設定」の「プロキシ設定」を先におこなってください。

各種設定 - ライセンス設定から、(株)フーバーブレインが発行したライセンスキーを入力し、「更新」をクリックしてください。ライセンスキーは、大文字/小文字を区別します。

ライセンス情報	
ライセンスキー	12345-6789
開始日	2015-04-14
ライセンス数	20
インストール数	0
サーバーバージョン	1.02

「更新」が成功すると、画面に、開始日、ライセンス数等の情報が表示されます。

## 7. サーバー設定

### 7.1. プロキシ設定

PasoLog Manager を社内設置し、インターネットに接続する際に認証プロキシを経由する場合、「サーバー設定」「プロキシ設定」をおこなってください。

インターネット接続にプロキシが必要かは、システム管理者にお問い合わせください。

印刷コスト設定	メール設定	プロキシ設定	部署マスター設定	データメンテ
プロキシサーバー	192.168.253.161			
ポート番号	8888			
ユーザー名	test			
パスワード	.....			
通信テスト	テスト開始			

必要な情報入力後、「テスト開始」をクリックします。入力情報が正しければ「テストが成功しました」を表示します。

設定を保存するには、「保存」をクリックします。

## 7.2. メール設定

PasoLog Manager の各種通知を受け取るために、メールサーバーを設定します。

**重要**

メールサーバーを設定しないと、PasoLog Manager からの各種通知メールが送信されません。  
下記のメール設定は、忘れずにおこなってください。

印刷コスト設定	メール設定	プロキシ設定	部署マスター設定
送信元名前	AutoDaily		
送信元アドレス	autodaily.ahkun@gmail.com		
SMTPサーバー	smtp.gmail.com		
ポート番号	465		
ユーザー名	autodaily.ahkun		
パスワード	.....		
SMTP over SSL	<input type="radio"/> 制御しない <input checked="" type="radio"/> 有効 <input type="radio"/> 無効		
STARTTLS	<input type="radio"/> 制御しない <input checked="" type="radio"/> 自動 <input type="radio"/> 無効		
サーバー設定SMTP認証	<input type="radio"/> 制御しない <input checked="" type="radio"/> 自動 <input type="radio"/> 無効		

情報を入力し終えたら、「送信テスト」をクリックして送信先にメールが送れるか確認してください。  
問題なければ「保存」をクリックしてください。

## 7.3. 印刷設定

印刷設定は、クライアントの印刷情報から、印刷コスト等を集計します。

印刷コストは、プリンターの機種や、モノクロ印刷、カラー印刷により異なるため、個別に設定します。

印刷ログは、「ログ情報」「印刷」の「集計データ」から確認できます。

1) 印刷コスト設定(既定)

カラー印刷(1ページ) 15 円

モノクロ印刷(1ページ) 2 円

2) プリンターコスト設定

プリンター登録方法  自動  手動

※自動 : クライアントが印刷したプリンター名を列挙してユーザーが金額を自由に  
 ※手動 : 登録したプリンターのみコスト計算対象にします。それ以外は、コスト計

プリンター	モノクロコスト(円)	カラーコスト(円)
Canon Inkjet MP980 series	1.05	5.25
OneNote 2013 に送る	0.00	0.00

プリンター毎にコストを設定するには、**モノクロコスト(円) / カラーコスト(円)** を変更します。

### プリンター登録方法

「自動」は、PasoLog 導入後、印刷情報がサーバーに送られると、印刷したプリンターが表示されます。プリンター毎に、印刷コストが設定できます。表示のないプリンターは「印刷コスト(既定)」の金額が自動で適用されます。

「手動」は、登録したプリンターのみコスト計算対象にします。それ以外は、コスト計算対象になりません。

設定例) カラー 15 円、モノクロ 2 円、 プリンター登録方法 ●自動 ○手動

設定を保存するには、「保存」をクリックします。



## モノクロプリンター登録

PasoLog は、プリンタードライバーのうち、PostScript (PS) を完全サポートしています。

PCL など、PS 以外のプリンタードライバーを使用された場合は、モノクロプリンターで印刷したものがカラーと表示される場合があります。

この場合、「モノクロプリンター登録」からモノクロプリンターを登録してください。

登録したプリンターの印刷は、全てモノクロ印刷として扱います。

3) モノクロプリンター登録

プリンター名

 追加  削除

## 7.4. 部署マスター設定

会社の部署を設定すると、部署単位で設定や、集計ができます。

新規に部署を作成するには、「サーバー設定」「部署マスター」を選択します。



部署は4階層まで作成できます。本部、支店、支社、部、課、グループなど。

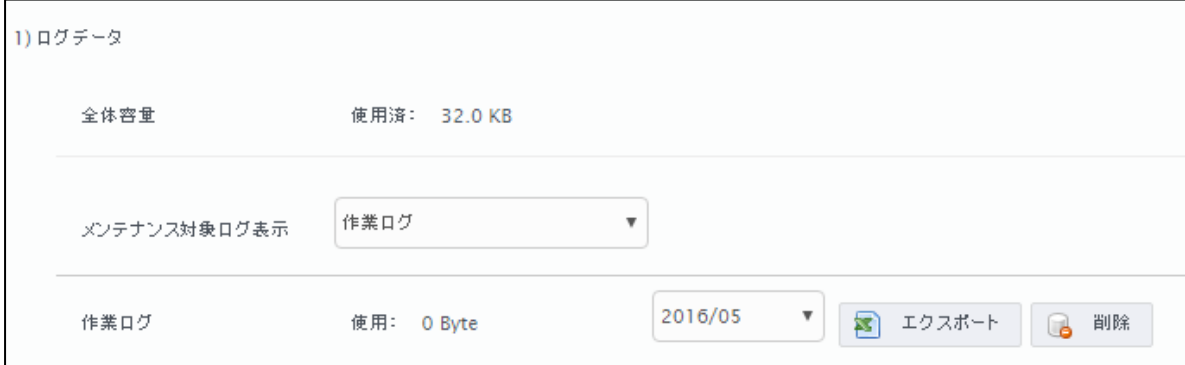
作成できる部署の数に制限はありません。

ここで作成した部署に、クライアントPCを割り当てるには、「クライアント情報」「クライアント」からおこないます。

## 7.5. データメンテナンス

PasoLog Manager 保存データのメンテナンスは、「サーバー設定」「データメンテナンス」からおこないます。

### 1) ログデータ



プルダウンからメンテナンス対象ログを選択して、対象ログを表示します。表示した対象ログのヶ月分のデータのエクスポートと削除ができます。

「エクスポート」は、指定した年/月のデータを CSV 形式で取得する際に使用します。

「削除」は、指定した年/月のデータをサーバーから削除し、空き容量を増やします。

### 2) データ保管



	保管日時	保管先	サイズ	処理
1	2016/05/19 15:34:46	/ahkun/backup/20160519153445.backup	116.6 KB	削除
2	2016/05/19 16:05:40	/ahkun/backup/20160519160539.backup	116.7 KB	削除

「データ保管開始」ボタンをクリックして、マネージャー全体のデータの保管を行います。

データ保管先 : /ahkun/backup

※注) 保管先の変更はできません。

保管したデータを削除する場合は、削除対象データの「削除」ボタンをクリックします。

## 7.6. その他設定

「サーバー設定」「その他設定」から、下記の設定がおこなえます。

### クライアント・ダウンロード時のパスワード設定

PasoLog クライアントをブラウザからダウンロードするための、パスワードが設定できます。

パスワードを設定すると、パスワードを知らないユーザーが勝手に PasoLog クライアントをインストールすることを制限できます。

印刷コスト設定    メール設定    部署マスター設定    データメンテナンス    **その他設定**

1) クライアント・ダウンロード時のパスワード設定

無効(既定)     有効    パスワード :

### PasoLog の自動更新

(株)フーバーブレインのサーバーから、最新版プログラムをダウンロードし、お客様のシステムソフトウェアを常に最新にする設定です。

#### 2) PasoLogの自動更新

自動更新     手動更新     更新を禁止

※手動更新 …… クライアントのタスクトレイから更新が可能

自動更新	PasoLog Manager、クライアントとも、最新版を 30 分毎にチェックし自動更新します。(推奨)
手動更新	PasoLog クライアントは自動更新しません。手動でタスクトレイアイコンから更新します。 PasoLog Manager は、最新版を 30 分毎にチェックし自動更新します。
更新を禁止	PasoLog Manager, クライアントとも、プログラムは更新されません。

### 備考

コメントが記入できます。

## 8. ポリシー設定

「各種設定」「ポリシー設定」から、PasoLog クライアントプログラム用のポリシーを作成、編集、削除することができます。ポリシーはクライアント PC から 30 分間隔で自動取得されます。すぐ更新したい場合は、クライアント PC のタスクトレイにある PasoLog アイコンを右クリックし、「ポリシーの更新」をおこなってください。

新しいポリシーを作成するには、「新規」をクリックし「ポリシー名」を入力します。設定が完了したら「保存」をクリックして保存します。

## ポリシー設定



作成したポリシーを編集するには、編集するポリシー名を選択して「編集」をクリックします。ポリシー設定画面の各項目を修正し、「保存」をクリックすると設定を保存します。

作成したポリシーを削除するには、削除するポリシー名を選択して「削除」をクリックします。基本ポリシー「Basic」は削除することができません。

## 8.1. 基本設定

### 8.1.1. クライアント表示設定

#### ■タスクトレイにアイコンを表示しない

クライアント PC のタスクトレイに PasoLog アイコンを表示しません。

#### ■スタートメニューや、コントロールパネルにプログラム情報を表示しない

この機能が有効な場合、スタートメニュー、コントロールパネル等へ PasoLog の項目を表示しません。PasoLog の導入をユーザーに知らせたくない場合、タスクトレイのアイコンを表示しない、と一緒に有効にします。

#### ■タスクトレイアイコンの右クリック「サーバー設定」を表示しない

タスクトレイアイコンの右クリックでサーバーを変更できないように「サーバー設定」を非表示にします。ユーザー操作で、PasoLog Manager サーバーを変更させたくないときに有効にします。タスクトレイアイコン非表示の場合、この設定は無視されます。

### 8.1.2. クライアント GPS 送信設定

位置情報は Windows 8 以降の PC で使用可能です。Wifi や GPS から位置情報を取得し 30 分間隔(初期値)でサーバーへ送信します。位置情報は PC 電源 OFF や、サスペンド状態のときは送信されません。

位置情報は、「クライアント情報」「PC 位置情報一覧」などから閲覧できます。



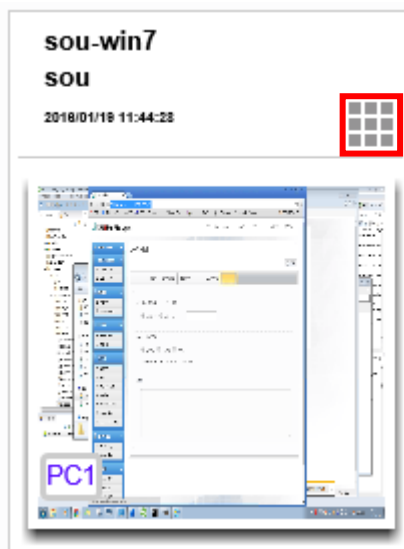
### 8.1.3. デスクトップ画像送信

デスクトップ画像を 30 分間隔(初期値)でサーバーへ送信します。画像は、「ダッシュボード」「クライアントデスクトップ」などから閲覧できます。

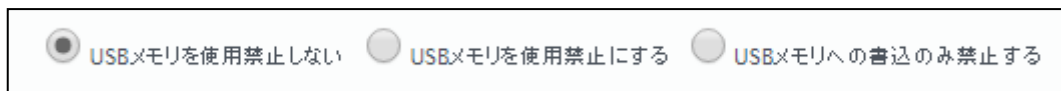


「クライアントデスクトップ」タブをクリックすると、下記の PC 画像が表示されます。

右の四角(■)をクリックすると、保存しているデスクトップ画像を一覧表示します。

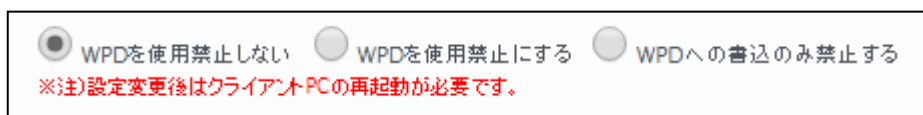


#### 8.1.4. USB メモリ使用禁止



情報漏えいや、ウイルス感染の入り口となる USB メモリ等のデバイスを管理者が禁止、又は書込みのみ禁止することができます。禁止対象デバイスは Windows からドライブ(E:,F:等)が割り当てられるデバイスです。マウス、キーボード、プリンター、スキャナ等、ドライブが割り当てられないデバイスは、通常通り使用できます。

#### 8.1.5. WPD 使用禁止



USB メモリの他、近年機密情報持ち出しの原因となっている、WPD(Windows Portable Device)として OS に認識されるスマートフォン等へのファイルコピーを禁止、又は書込みのみ禁止することができます。この設定が有効な場合、スマートフォン等へのファイル読み書きが禁止されます。**この設定は、クライアント PC 再起動後に有効になります。**

#### 8.1.6. クライアント アンインストール時のパスワード入力

PasoLog クライアントをユーザーが勝手にアンインストールできないように、パスワードを設定できます。パスワードを設定すると、コントロールパネル - プログラムの機能(または「プログラムの追加と削除」)から、PasoLog をアンインストールすると、パスワード入力ダイアログが表示され、管理者が設定したパスワードを入力しないと、アンインストールができなくなります。

#### 8.1.7. メッセージ送信



こちらにチェックを入れた場合、クライアント側にメッセージを送信することが可能です。詳細については、「23.メッセージ送信機能」をご参照ください。

## 8.2. 印刷設定

### 8.2.1. 印刷制限(一ヶ月に印刷できる枚数)

印刷枚数上限(モノ)  制限なし  制限する

印刷枚数上限(カラー)  制限なし  制限する

< 指定枚数を超える場合アクション >

何もしない  警告を表示  印刷を禁止する

< 指定枚数を超える場合メール送信 >

送信しない  送信する

枚数制限は、モノクロと、カラーで個別に設定できます。

「制限なし」は、印刷枚数制限をしません。

印刷制限するには「制限する」を選択し、一ヶ月に印刷できる枚数を入力します。

印刷枚数を超えた場合のアクションは、何もしない・警告を表示・印刷を禁止する、が選択できます。

何もしない、は印刷枚数制限を超えても、クライアント PC 側に通知はなく印刷が可能です。

警告を表示は、印刷枚数制限を超えたことをユーザーに通知するダイアログを表示します。印刷はできます。

「印刷を禁止する」は、ユーザーに枚数制限を超えたため、印刷できない通知を表示し、印刷を失敗させます。

指定枚数を超えた場合のメール送信は、「ポリシー設定」「日報送信設定」の日報送信先が設定されている場合に有効です。設定したメールアドレスへ印刷枚数制限を超えたことを知らせるメールを送信します。

印刷枚数制限は、印刷開始前に判断します。たとえば 50 ページ印刷可能なとき、計 100 ページのドキュメントを印刷すると、50 ページで印刷を中止するのではなく、100 ページ全て印刷できます。

次の印刷から枚数オーバー処理をします。

これは 100 ページのドキュメントの 50 ページだけを印刷し、残りが印刷できないと、ドキュメントとして不完全で、最初の 50 ページも無駄になってしまうためです。



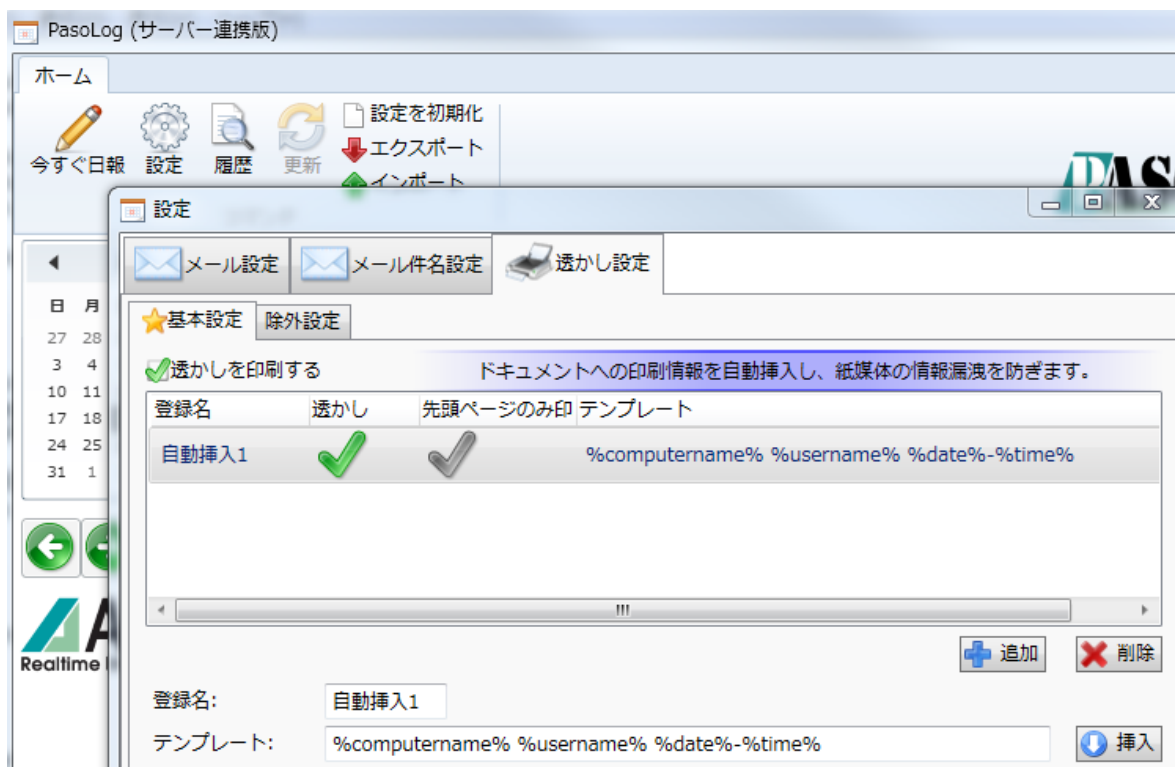
## 8.2.2. 透かし印刷設定

紙媒体の情報漏えいを防ぐため、PasoLog では、印刷物の所有者を明確にするため、誰が、いつ、どのプリンターから、何を印刷したか等の印刷情報を、自動で印刷物に「透かし」として挿入することができます。通常、透かしは、印刷物の隅にごく小さなフォントで、ごく薄い色で印刷しておきます。

透かしを印刷するには「透かしを印刷する」をチェックし、「透かし設定テキスト」へ情報を入力します。

「透かし設定テキスト」は、下記手順により PasoLog クライアントで生成します。

1. タスクトレイアイコンの PasoLog アイコンをクリックします。
2. 「設定」->「透かし設定」をクリックし、「挿入」ボタンをクリックして表示する情報のテンプレートを作成します。



3. 次にテンプレートテキストをコピーして、マネージャーの「透かし設定テキスト」に貼り付けます。

作成テンプレート例：

**`%computername% %username% %date%-%time% %printer%`**

### 8.2.3. 透かし除外設定 – ドキュメント(ファイル名)除外

印刷するドキュメント名に含まれるキーワードを指定して、透かしを入れない設定をします。

注文書、見積、など、透かしを入れないドキュメントをキーワードで指定するとキーワードを含むドキュメントの印刷には透かしが入りません。

### 8.2.4. 透かし除外設定 – プリンターを指定して除外

特定のプリンターへの印刷に透かしを入れない設定をします。

「プリンター」は、クライアントが過去使用したプリンターが表示されます。リストから選択するか、プリンター名を入力して透かしを入れないプリンターを指定します。

## 8.3. 日報送信設定

クライアント PC の作業をメールで受信したい場合は、この設定をおこないます。

メールを送るには、「サーバー設定」「メール設定」でメールサーバーを指定しておく必要があります。

詳しくは、本ドキュメントの「メール設定」をご参照ください。

### 8.3.1. 送信対象

#### 日報・週報・月報

日報は、毎日 PC 操作があればメールで作業内容を送信します。

週報は、週が変わると、先週の作業内容を集計したデータを送信します。

月報は、月が変わると、先月の作業内容を集計したデータを送信します。

### 8.3.2. 送信先

日報送信先を TO, CC, BCC で指定します。また週報だけを送る、月報だけを送る送信先が指定できます。

週に一度、月に一度、集計をメールで確認したいとき、週報のみ送信、月報のみ送信をお使いください。

### 8.3.3. 日報送信時間

「日付が変わったら、前の日報を自動的に送信」は、前日の PC 操作が日報メールとして送られます。

通常、こちらを選択してください。

「指定の時間に日報を送信する」は、例えば 18:00 に指定すると、18:00 から 23:59 までのデータが日報メールとして送られません。就業時間後は、社員の PC 利用のログは日報メールで送らない、といった用途に使用できます。

「制御しない」は、この設定をサーバーで制御せず、PasoLog クライアント側の設定を優先します。

### 8.3.4. 件名

%date%等、%で挟まれた値は、変数でメール送信日付や、コンピューター名などが入ります。  
件名は、特に変更する必要はありません。

## 8.4. 利用禁止ソフトウェア

クライアント PC で実行を禁止したいプログラムを指定します。

### 8.4.1. 禁止指定方法

禁止指定方法は直接入力する方法とカテゴリから選んで追加する方法があります。

#### 1) 直接入力して追加

「ファイル」は、ファイル名でプログラムを指定します。ファイル名はワイルドカード(?)が指定できます。  
「パス」は、指定フォルダ以下のプログラム実行を禁止します。パスはワイルドカード、%USERPROFILE%  
などクライアント PC の環境変数が指定できます。

「ハッシュ」は、MD5 を指定します。16 進数 A-F は、大文字/小文字どちらでも構いません。

「アクション」は下記 3 つから選択できます。

1. 警告を表示し、実行を禁止する
2. 警告を表示し、実行を許可する
3. 警告を表示せず、実行をサーバーに通知

「ファイル」を指定して設定した例を以下に例示します。

#### ポリシー設定

戻る 削除 保存

基本設定 印刷設定 日報送信設定 **利用禁止ソフトウェア** 情報漏えい(マイナンバー等)対策

入力して追加  カテゴリから指定して追加

禁止指定方法

ファイル/パス/MD5

アクション

追加

選択した行を削除

	ファイル/パス/MD5	禁止指定方法	アクション	カテゴリ
1	winny	ファイル	警告を表示し、実行を禁止する	

設定を追加するには「追加」をクリックします。

## 2) カテゴリから指定して追加

入力して追加
  カテゴリから指定して追加

カテゴリ選択
 ファイル交換ソフト ▼ ※登録済のソフトウェアはフォント色青で表示しています。

ソフトウェア一覧		
	ファイル	備考
1	Winny.exe	Winny
2	winny2.exe	Winny
3	winnyp.exe	Winny
4	perfect dark.exe	Perfect Dark
5	share.exe	Share
6	Shareaza.exe	Shareaza
7	LimeWire.exe	LimeWire
8	emule.exe	eMule

アクション
 警告を表示せず、実行をサーバに通知 ▼

	ファイル/パス/MD5	禁止指定方法	アクション	カテゴリ
1	Winny.exe	パス	警告を表示せず、実行をサーバに通知	ファイル交換ソフト
2	winny2.exe	パス	警告を表示せず、実行をサーバに通知	ファイル交換ソフト
3	winnyp.exe	パス	警告を表示せず、実行をサーバに通知	ファイル交換ソフト
4	perfect dark.exe	パス	警告を表示せず、実行をサーバに通知	ファイル交換ソフト
5	share.exe	パス	警告を表示せず、実行をサーバに通知	ファイル交換ソフト

カテゴリ選択プルダウンから追加するカテゴリを選択すると対象カテゴリのソフトウェアが一覧画面に表示されます。ソフトウェア一覧から追加するソフトウェアにチェックを入れて、禁止アクションを指定して「追加」ボタンをクリックして追加します。

追加した設定を削除するには、削除対象行にチェックを入れてから「選択した行を削除」ボタンをクリックします。

最後に設定を保存するには、「保存」をクリックします。

クライアントのデスクトップ画像送信が有効なポリシーでは、禁止プログラムを実行したときの画像を取得して、サーバーへ送信します。

画像は「ダッシュボード」「クライアントデスクトップ」を下へスクロールし、「アラート状態」から閲覧できます。

## 8.5. 情報漏えい(マイナンバー等)対策

### 8.5.1. 個人情報スキャン

個人情報やマイナンバーを含むファイルは、安全なクラウド環境や、ファイルサーバーに暗号化保管し、アクセスできるユーザーを限定し、アクセスしたログを取得する等のセキュリティ管理が推奨されます。

しかしサーバーで厳密に管理していても個人情報が、クライアントにコピーされると、管理が難しくなります。クライアントに個人情報ファイルがあると、PC を持ち出した際の紛失や盗難、USB メモリでのデータ持ち出し、ウイルス感染による情報漏えい等のリスクが高くなります。

本機能は、氏名、住所等の個人情報を含む可能性のあるファイルが、クライアントに存在しないかをチェックし、もしあれば PasoLog Manager へ情報を送信します。

本機能をご使用になるには「個人情報スキャンを有効」をチェックします。

個人情報スキャンを有効

個人情報(「氏名や住所、12桁の数字など」)を指定数以上含むファイルがクライアントにあれば、サーバーへ通知する

5件  10件  50件  100件

**個人情報(氏名や住所、12桁の数字など)を指定数以上含むファイルがクライアントにあれば、サーバーへ通知する**、をチェックし、5,10,50,100等の件数を指定します。例えば50件とした場合、氏名、住所等のキーワードを50件以上含むファイルの情報を PasoLog Manager へ送信します。

**指定キーワードを含むファイル名がクライアントにあれば、サーバーへ通知する**、をチェックし、キーワードを入力します。例えば、「マイナンバー」を登録すると、「社内マイナンバー.xls」などのファイルがクライアントにあれば PasoLog Manager へ送信します。通常ファイルのスキャンは1日1回自動実行されます。

指定キーワードを含むファイルがクライアントにあれば、サーバーへ通知する

源泉徴収

マイナンバー  
個人番号

報告されたデータは、PasoLog Manager の「ログ情報」「個人情報」から参照できます。

### 8.5.2. クリップボード監視

クリップボードは、プログラム間でデータのコピーをおこなう機能です。

文章のコピーを監視します。

本機能を有効にするには、**クリップボード監視を有効、をチェックします。**



クリップボード監視を有効

個人情報スキャンで選択した個人情報数(5件,10件など)を含む文字や文章をクリップボードにコピーしたらサーバーへ通知する

**クリップボード監視を有効**にチェックすると、ユーザーがクリップボードへコピーした文章を監視します。

PasoLog Manager へ情報を送信するのは、コピーデータの中に、名字等の個人情報が、個人情報スキャンで選択した数(5件,10件など)以上を含む場合です。

個人情報を含まないデータのコピー操作は、PasoLog Manager へ送信しません。

PasoLog Manager へ送信されたデータは、「ログ情報」「クリップボード操作」から参照できます。

**\*クリップボードは、ユーザーが非常に頻繁に使う機能のため、記録データが膨大にならないよう、ポリシー設定に合致したログのみをサーバーへ送信・保存する仕様になっております。**

### 8.5.3. ファイル操作ログを取得する

ファイル操作ログ取得機能は「ファイル実行ログ」と「ファイルコピー、削除ログ」取得の二つがあります。

#### 1) ファイル実行ログ

本機能を有効にすると、指定した拡張子のファイルをユーザーが開くと、サーバーへ報告します。

サーバーに報告されたデータは、「ログ情報」「ファイル操作」から参照できます。

下記画面から、報告するファイルの拡張子を指定できます。拡張子は、複数指定する場合、コロン(:)で区切ります。コロンを含めた拡張子は、最大半角 260 文字まで指定可能です。

以下の拡張子の操作(実行)を記録する

コロン(:)区切りで入力してください。(例:txt.csv:pdf.doc:xls)

一般的に使用される文書ファイルを一括で記録を残す場合、

**デフォルト拡張子セットを使用する**、をチェックします。



デフォルト拡張子セットを使用する

以下の拡張子が監視対象になります。

■Microsoft製品

csv,rtf,doc,docx,docm,xls,xlsx,xlsm,ppt,pptx,pptm

■その他製品

Adobe(pdf)、一太郎(jaw:jtw:jbw:juw:jfw:jvw:jtd:jtt)

OpenOffice(sxw:svc:sxi:sxd:odt:ods:odp:odg)

OASYS(oas:oa2:oa3)、松(bun)、Lotus123(wj2:wj3:wk3:wk4:123) など

デフォルト拡張子は、今後予告なく、追加・変更することがあります。

拡張子は、デフォルト拡張子+ユーザー指定を両方同時に指定できます。

デフォルト拡張子と、ユーザーが指定した拡張子に重複があっても問題ありません。

指定した拡張子と、デフォルト拡張子に同じものがあっても、問題ありません。

## 2)ファイルコピー、削除ログ

本機能を有効にして、監視対象ファイル名、又はファイルパスを追加すると、追加したファイル名、又はファイルパスが含まれるファイルのコピー、削除操作を監視してサーバーへ報告します。

下記例はCドライブの「重要書類」フォルダ配下のファイルのコピー、削除操作を監視する設定になります。

ファイルコピー、削除を監視する

監視対象ファイル名、ファイルパス

c:\重要書類

上記設定を入れた場合、管理マネージャーの「ログ情報」->「ファイル操作」に下記のようなログが記録されます。

ファイル操作ログ						
	処理日時	コンピューター	ユーザー	操作	ファイル名	ファイルパス
1	2015/11/26 09:37:08	pc	user	削除	個人情報.csv	c:\重要書類\個人情報.csv
2	2015/11/25 14:51:24	pc	user	読込	個人情報.csv	c:\重要書類\個人情報.csv
3	2015/11/25 14:46:41	pc	user	読込	個人情報.csv	c:\重要書類\個人情報.csv
4	2015/11/25 14:46:18	pc	user	実行	個人情報.csv	c:\重要書類\個人情報.csv
5	2015/11/25 14:44:46	pc	user	書込	個人情報.csv	c:\重要書類\個人情報.csv

1 ページ中 1 ページ目 20

5件中 1 -



## 9. クライアント

「クライアント情報」「クライアント」から各種データが参照できます。  
表示はグリッド、ツリーが選択できます。

クライアント

検索条件

キーワード

表示内容

PC負荷  所有者  アンインストール対象  再インストール禁止  部署名  コンピューター名  IPアドレス  
 MACアドレス  ドメイン名  メモリ  ログオンユーザ  ポリシー名  OS  最終アクセス日  
 位置情報  ウイルス対策ソフト  クライアントID  バージョン  プロセッサ  インストール日  SP  
 メーカー  モデル  CPUID  システム種別  BIOSメーカー  BIOSシリアル  BIOSバージョン  
 SMBIOS  マザーメーカー  マザー製品名  マザーシリアル  マザーバージョン  位置情報取得時刻  OSライセンス  
 プロダクトID  パスワード設定  Java  IE  Flash  AdobeReader  AdobeAcrobat

クライアント一覧

画像	状態	PC負荷	所有者	アンインストール対象	再インストール禁止	部署名	コンピューター名	IPアドレス	MACアドレス	ドメイン名	メモリ	ログオンユーザ	ポリシー名	OS
		45		<input type="checkbox"/>	<input type="checkbox"/>		WIN-HR1D6KAI	192.168.253.30	08:00:27:85:53:17	WORKGROUP	2.0GB	foxtest	Basic	Windows
		73		<input type="checkbox"/>	<input type="checkbox"/>		Vista-vPc	10.0.2.15	08:00:27:8D:ED:7D	WORKGROUP	2.0GB	vista-user	Basic	Windows

「検索条件」から検索できます。表示内容から、表示項目が選択できます。  
「CSV 出力」で情報を CSV へ出力できます。

### 9.1. 作成した部署へ PC を移動

部署の作成は、「サーバー設定」「部署マスター」でおこないます。  
作成した部署へ PC を移動するには、部署名から選択します。変更を保存するには「保存」をクリックします。

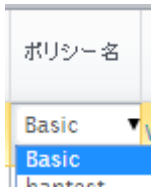
保存

クライアント一覧

画像	状態	PC負荷	所有者	アンインストール対象	再インストール禁止	部署名	コンピューター名
		45		<input type="checkbox"/>	<input type="checkbox"/>	技術部	WIN-HR1D6KAI
		73		<input type="checkbox"/>	<input type="checkbox"/>	技術部	Vista-vPc

## 9.2. 割り当てポリシーを変更する

「ポリシー設定」から追加、作成したポリシーを PC に適用するには、ポリシー名から選択します。  
設定を保存するには「保存」をクリックします。



## 9.3. 削除

「削除」は、指定したクライアントを無効化し、未使用クライアントライセンスを 1 つ増やします。  
例えば、破棄済みの PC が表示されていれば、削除してライセンスを増やすことができます。  
削除後、クライアントから通信がありライセンス数の上限を超えていなければ、元の状態に自動復帰します。  
削除をおこなうと状態に X マークが表示されます。この状態からもう一度削除すると、該当 PC に関する保存データを削除します。一度削除したデータは復元できませんのでご注意ください。



## 9.4. PC 位置情報一覧

「PC 位置情報一覧」をクリックすると、クライアント PC の位置を地図上に表示します。  
位置情報は、Windows 8 以上で対応しています。Wifi や GPS から位置情報を取得し 30 分間隔(初期値)でサーバーへ送信します。位置情報は PC 電源 OFF や、サスペンド状態のときは送信されません。  
地図表示はインターネット接続が必要です。インターネットに接続していないと地図は表示できません。



## 9.5. 強制アンインストール

「アンインストール対象」をチェックすると、PasoLog クライアントをアンインストールできます。  
「再インストール禁止」をチェックすると、アンインストール後の PasoLog のインストールを禁止します。  
アンインストール対象と組み合わせると、アンインストールして、さらに再インストールを禁止します。  
設定を有効にするには「保存」をクリックします。  
これらの設定は、ポリシーとしてクライアントへ配信されるため、設定を反映させるには、クライアント-サーバー通信を正常におこなう必要があります。

## 9.6. IE や、脆弱性報告の多いアプリケーションの確認

アプリケーションの脆弱性を基に不正プログラムが実行されるケースが多く報告されています。脆弱性を修正するパッチがメーカーからリリースされていても、適用しないユーザーがいます。

脆弱性報告が比較的多いアプリケーションの導入有無、バージョンを確認することができます。

現在、IE, Flash, Adobe Reader, Adobe Acrobat, Java が対象です。



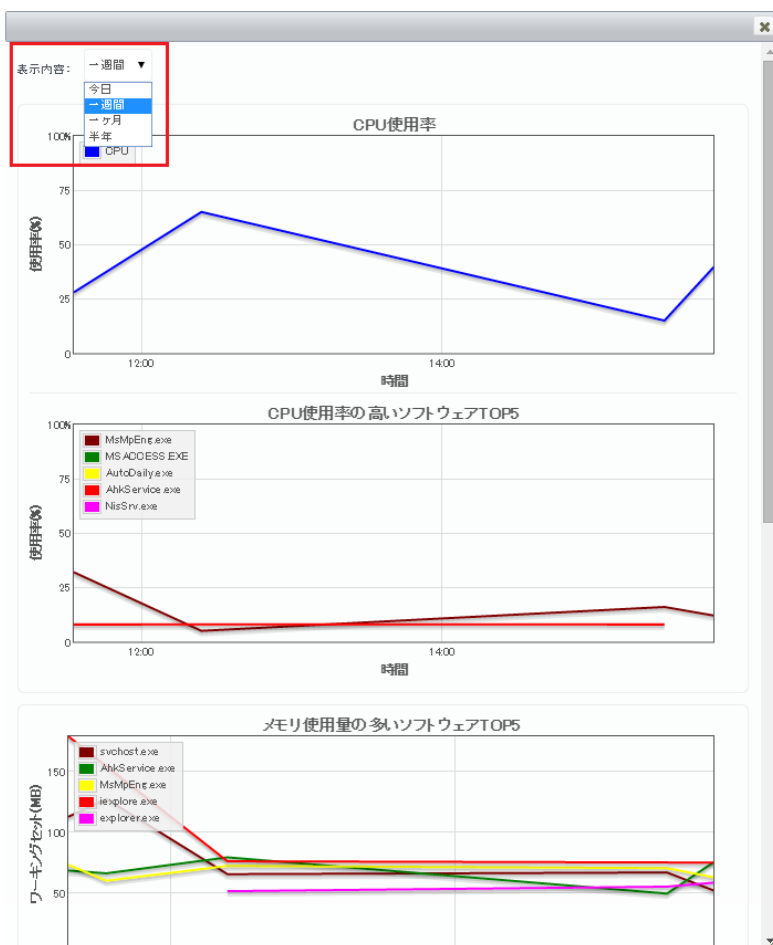
## 9.7. その他のクライアント情報

「PC 負荷」は、クライアントの最近の CPU 使用率を 0-100 の範囲で表示します。

平均して CPU 使用率の高い PC は、業務に必要な PC スペックが不足しているか、CPU 負荷の高いアプリケーションが実行されています。

この項目をクリックすると下記のような CPU 使用率等のグラフを表示します。

今日、一週間、一ヶ月など、集計期間が選択できますので、負荷の高い日時を特定するのに役立ちます。



「所有者」は、任意の文字列が入力できます。日本語も入力できます。

入力文字は、PC 位置を地図上で表示する際に表示されます。またデスクトップ画像等にも付加情報として表示します。

「ウイルス対策ソフト」は、ウイルス対策ソフトの導入状況を表示します。

○・・・ウイルス対策製品で保護されています。自動更新が有効で、リアルタイム保護も有効です。

△・・・自動更新、またはリアルタイム保護が無効です。

無・・・ウイルス対策製品が導入されていません。

リアルタイム保護は、ウイルスを検知した瞬間に動作を停止し警告する常駐機能です。

リアルタイム保護を無効にするとセキュリティが低下します。

○や△のアイコンをクリックすると詳細が表示されます。



#### ご注意

ウイルス対策製品の検出は、Windows WMI という機能で取得しています。WMI のウイルス対策製品検出は、Windows の仕様により、Windows Server 系 OS (Windows Server 2012 など) ではサポートされていないため、本製品においても Server 系 OS で、ウイルス対策製品が検出されませんが仕様となります。Windows 7, 8, 10 等のクライアント OS は、ウイルス対策製品検出をサポートします。

「パスワード設定」は、Windows ログインにパスワードが設定されているか表示します。

パスワードが設定されていない PC は、「パスワード未設定」を表示します。

電源 ON で、自動的に設定したユーザーでログインする PC は「自動ログイン」を表示します。

ログインにパスワードが必要な PC は「通常」を表示します。

セキュリティ上、Windows ログインパスワードを設定することを推奨いたします。

「OS ライセンス」は、Windows のライセンス・アクティベーションが実施されたかを表示します。

アクティベートされていれば、Licensed を表示します。

アクティベートが未実施なら、Notification などを表示します。

**「位置情報取得時間」** は、位置情報を PC から最後に受信した時間を表示します。  
位置情報の取得は、Windows 8 以降で有効です。

**「備考」** は、コンピューターにコメントが記述できます。  
所有部署や、設置場所、リース契約期間などの情報が自由に記述できます。

## 10. ソフトウェア

企業の導入ソフトウェアをリスト表示します。

### 10.1. ソフトウェア別

クライアント数と、導入ソフトウェア数が表示されます。

キーワード検索や、ベンダー一覧から、ソフトウェアの開発元を選び、絞り込みができます。

「ソフトウェア一覧」で表示されたソフトウェアをダブルクリックすると、導入 PC が表示されます。

#### ソフトウェア

	ソフトウェア名	ベンダー	バージョン	設定
<input type="checkbox"/>	AhkServerAgent	Ahkun	1.30	
<input type="checkbox"/>	IE		11.0.9600.16384	
<input type="checkbox"/>	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	Microsoft Corporation	10.0.40219	
<input type="checkbox"/>	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	Microsoft Corporation	10.0.40219	
<input type="checkbox"/>	OfficeLogAce	Saxa	1.0.83.0	
<input type="checkbox"/>	OfficeLogAceManager	Saxa	1.30.0000	
<input type="checkbox"/>	Oracle VM VirtualBox Guest Additions 4.3.10	Oracle Corporation	4.3.10.0	
<input type="checkbox"/>	PostgreSQL 9.3	PostgreSQL Global Development C	9.3	

※フォント色オレンジの行はソフトウェアパスが不明なため、禁止ソフトウェアに登録できません。  
 ※フォント色青の行はすでに禁止ソフトウェア登録設定があります。「設定有」ボタンをクリックして、詳細を確認できます。

企業内にどの開発元ソフトウェアが、どれくらい導入されているか、確認できます。またソフトウェアの禁止設定も可能です。禁止設定する場合、当該ソフトウェアの左チェックボックスにチェックを入れ、「チェックしたソフトウェアを禁止ソフトウェアに登録する」ボタンをクリックします。下記「禁止ソフト登録」画面が表示されたら、登録アクション、登録先ポリシーを指定して「登録」ボタンをクリックします。

登録パス情報	ソフトウェア名	ソフトウェアパス
1	PostgreSQL 9.3	C:\Program Files\PostgreSQL\9.3
2	Oracle VM VirtualBox Guest Additions	C:\Program Files\Oracle\VirtualBox Guest Additions

## 10.2. 禁止ソフト

禁止ソフトの設定情報を確認できます。

## 10.3. クライアント別

表示されたクライアントをクリックすると、インストール済みのソフトウェアを表示します。

業務に不要なソフトウェアを導入していないか確認できます。

## 10.4. Hotfix 別

Hotfix は、マイクロソフトの修正プログラムの名称です。KB は Knowledge Base(技術情報)の略です。

通常 Hotfix は、修正内容が記述された KB 番号が割り当てられます。

セキュリティに関する重大な問題を修正したものがあり、社内 PC に必要な修正パッチが適用されているかこの画面から調べることができます。

Hotfix 一覧の表示リストをクリックすると、適応済 PC と、未適応 PC を表示します。

## 10.5. 脆弱報告の多いソフトウェア別

IE, Flash, Adobe Reader, Adobe Acrobat, Java について、導入 PC を表示します。

重要な脆弱性が報告されているバージョンを使っているユーザーを見つけることができます。

Adobe Reader や Flash など業務に不可欠でないなら、アンインストールするとリスクが低下します。

## 10.6. OS 導入

導入済み Windows を表示します。

「対象クライアント」をクリックすると、コンピューター名などの詳細情報を表示します。

## 10.7. Office 導入

導入済み Office バージョンを表示します。

ソフトウェア名に、Office を含むものを表示します。Microsoft 以外の Office 製品も対象になります。

Office で検索するため、Office 本体ではなく、関連モジュールや修正パッチ等も表示されることがあります。

「対象クライアント」をクリックすると、導入コンピューター名などの詳細情報を表示します。

## 10.8. ウイルス対策ソフト

導入済みウイルス対策製品を表示します。

	ウイルス対策ソフト	インストール数	処理
1	Ahkun EX AntiMalware	16	対象クライアント
2	Windows Defender	12	対象クライアント
3	Microsoft Security Essentials	7	対象クライアント
4	ウイルスバスター クラウド	3	対象クライアント
5	TrendAntiVirusトレンドマイクロ ウイルスバスター コーポレートエディションウイルス対策	1	対象クライアント
6	マカフィー アンチウイルスとアンチスパイウェア	1	対象クライアント
7	Ahkun Ahkun EX AntiMalware	1	対象クライアント
8	未導入	16	対象クライアント

ウイルス対策製品が導入されていない PC は「未導入」に分類されます。

ウイルス対策製品の導入を強く推奨いたします。

「対象クライアント」から、コンピューター名、ログインユーザーなどの情報が表示できます。

## 10.9. ライセンス

ソフトウェア名をクリックすると、インストールしているコンピューターなどの情報を表示します。

使用数は、このアプリケーションを Windows 最前面で実行したことを PasoLog が検出すると、カウントします。インストール済みでも、Windows 最前面に表示しないアプリケーションは使用数にカウントされません。

Office などの製品が、実際、何ユーザーで使用されているか、チェックすることができます。



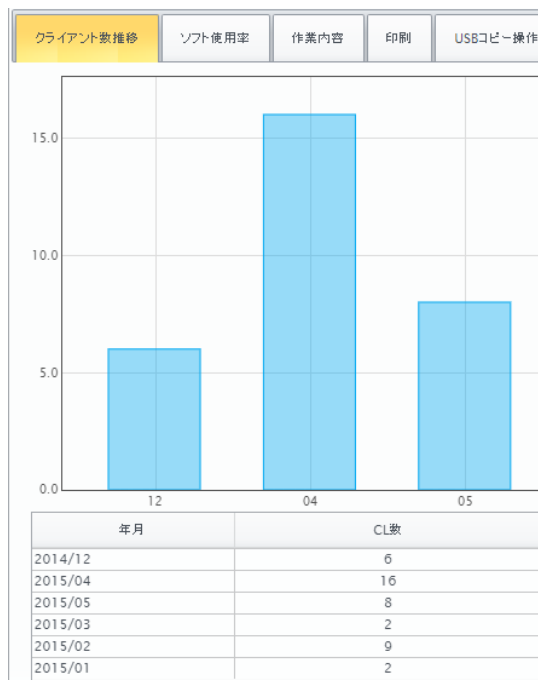
## 11. 全体分析

作業期間を指定し、会社全体の作業傾向を分析・表示します。

### 11.1. クライアント数推移

月単位のクライアント数の推移を表示します。

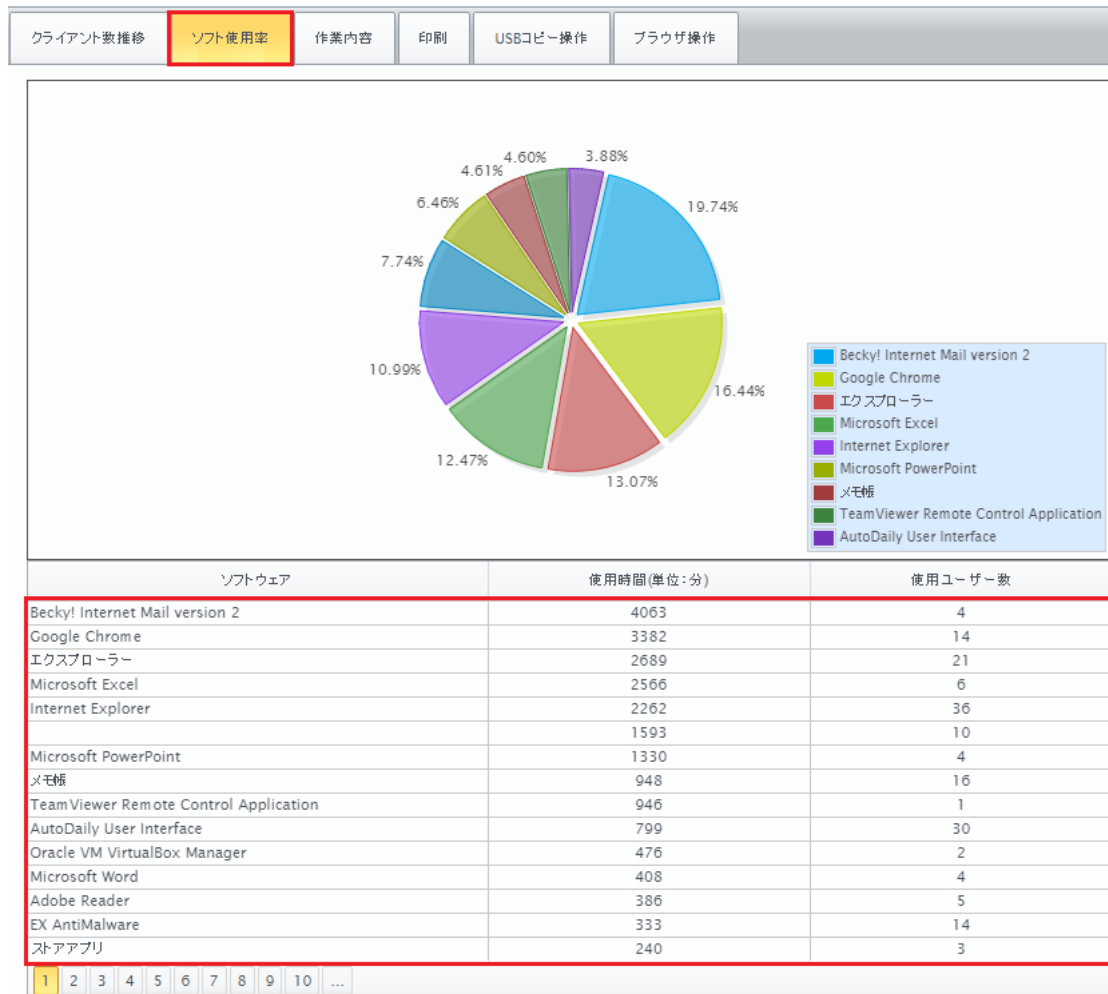
1ヶ月間でクライアントと一度でも通信すれば、有効なクライアントとして+1カウントします。



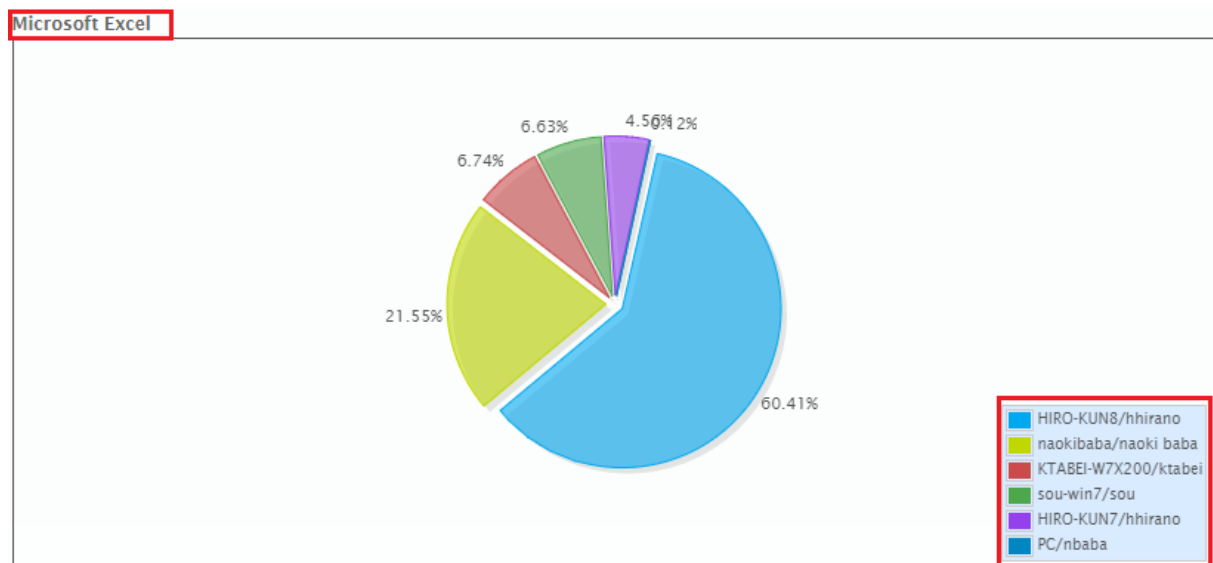
クライアントとの通信時間は、「クライアント情報」 「クライアント」の「最終アクセス日」で確認できます。

## 11.2. ソフト使用率

どのソフトウェアが最も長時間使われているか、ソフトウェア使用時間を分析表示します。



「ソフトウェア」をクリックすると、指定ソフトの使用時間が多いユーザー上位 10 名を表示します。



### 11.3. 作業内容

どの操作が最も長時間おこなわれているか、作業時間を分析表示します。

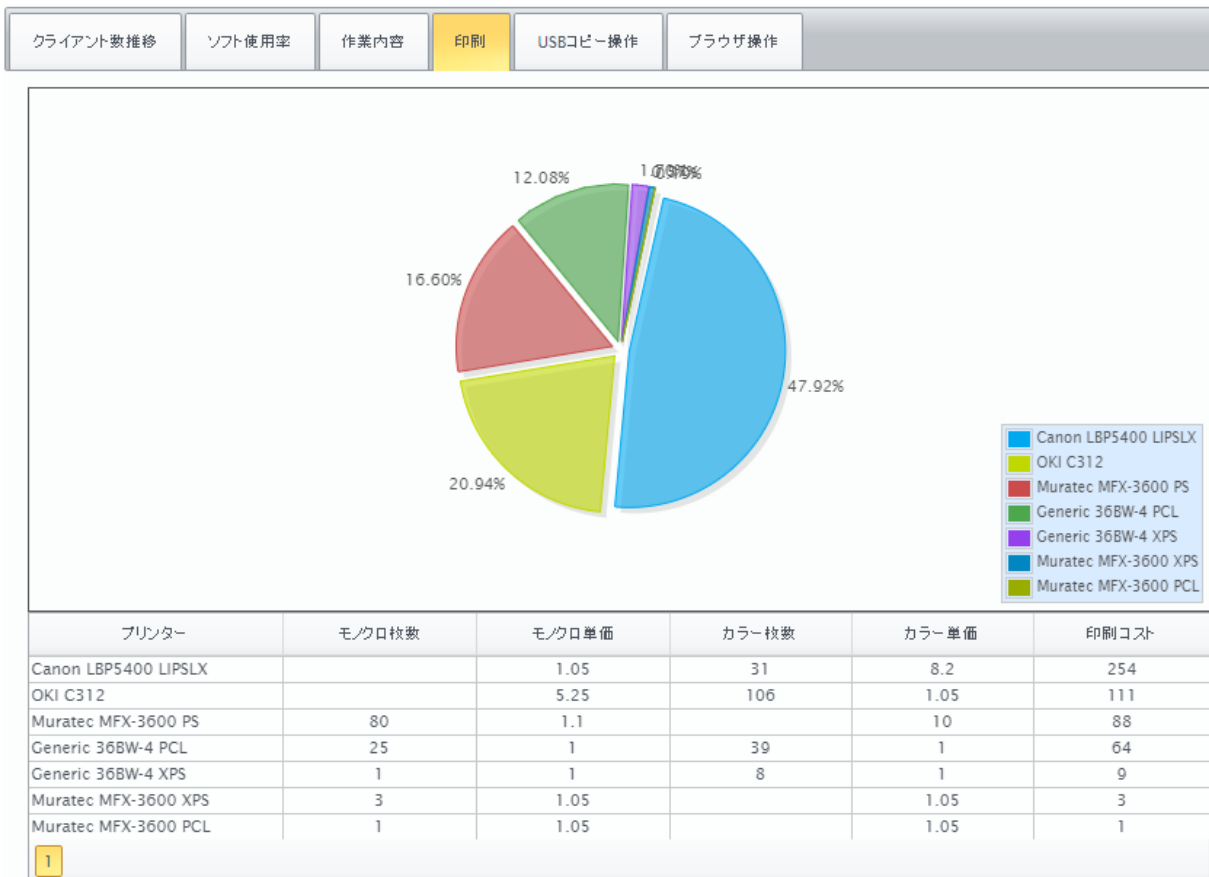
「作業内容」をクリックすると、作業時間の多いユーザー上位 10 名を表示します。

### 11.4. 印刷

どのプリンターからの印刷が最も多いか、分析表示します。

印刷はプリンター毎の枚数、カラー/モノクロ、印刷コストを表示します。

1 ページあたりの印刷コストは、「サーバー設定」「印刷コスト設定」から設定・変更できます。



どのユーザーが最も印刷しているかも、参照できます。

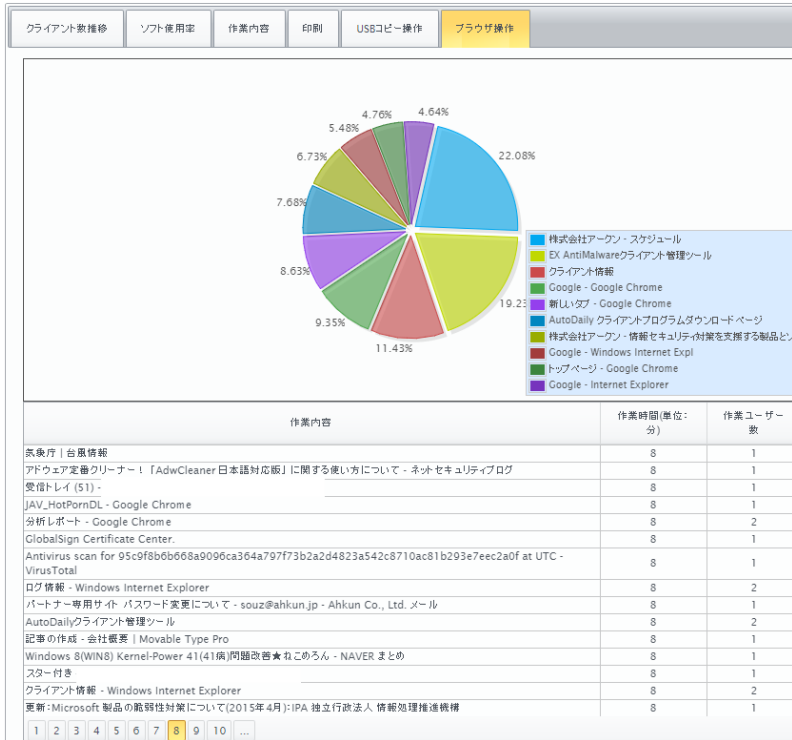
### 11.5. USB コピー操作

USB メモリ等の外部記憶装置へ、コピーしたファイル数が、多いユーザーを分析表示します。

USB へファイルをコピーする機会の多いユーザーを確認できます。

## 11.6. ブラウザ操作

ブラウザ操作の作業時間が多い順に分析表示します。ブラウザは、IE, Chrome, Firefox が対象です。



「作業内容」をクリックすると、操作をした時間が多いユーザー上位 10 名を表示します。

## 12. ユーザー別(月)

クライアント一覧から、特定ユーザーを指定し、作業が確認できます。

### ユーザー別 (月)

グリッド形式  ツリー形式

グリッド形式 …… PC を選択し、「集計」をクリックします。

ツリー形式 …… PC 単位、または「部署単位」で集計できます。

特定 PC の作業内容を確認するには、グリッド形式をご使用ください。

部署単位の集計データを確認するには、ツリー形式をご使用ください。

### 集計単位

集計単位  PC  PC/USER  USER

「PC」は、コンピューター単位で集計します。複数のログインユーザーが 1 台の PC を使用していても、合算集計します。

「PC/USER」は、1 台の PC を複数ユーザーで共有している場合、ユーザー毎、個別に集計します。

「USER」は、複数 PC で同じユーザー名でログインしている場合、1 ユーザーとしてまとめます。

PC1, PC2 にそれぞれ“USER-1”としてログインしている場合、PC1¥USER1 と PC2¥USER1 は、同じ USER-1 として合算集計します。ActiveDirectory など不特定 PC を同じユーザーでログインする環境は、「USER」で集計すると便利です。

### 検索条件

年月 :

検索条件で年月を選択し、「集計」をクリックします。

### 12.1. グリッド形式

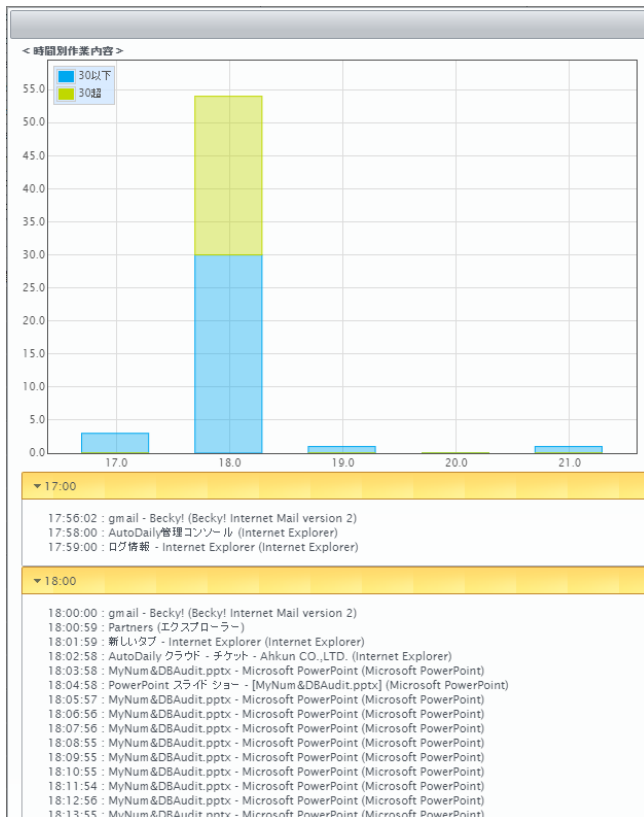
「集計」をクリックすると、月単位の作業履歴を表示します。

ユーザー一覧						
	コンピューター名	ユーザー名	OS	部署名	最終集計日時	処理
1	AHKUN-E20BEF159	AHKUN-E20BEF159/ahkun	Windows XP	その他	2015/05/27 12:49:22	<b>集計</b>

<作業時間>

	-	-	-	4/1 (水)	4/2 (木)	4/3 (金)	4/4 (土)
作業開始				00:00	00:00	00:00	00:00
作業終了				00:00	00:00	00:00	00:00
操作時間				0	0	0	0
	4/5 (日)	4/6 (月)	4/7 (火)	4/8 (水)	4/9 (木)	4/10 (金)	4/11 (土)
作業開始	00:00	00:00	00:00	00:00	00:00	00:00	00:00
作業終了	00:00	00:00	00:00	00:00	00:00	00:00	00:00
操作時間	0	0	0	0	0	0	0
	4/12 (日)	4/13 (月)	4/14 (火)	4/15 (水)	4/16 (木)	4/17 (金)	4/18 (土)
作業開始	00:00	00:00	00:00	00:00	17:56:02	13:32:35	12:11:41
作業終了	00:00	00:00	00:00	00:00	21:55:08	18:44:42	12:16:24
操作時間	0	0	0	0	1時間	4.7時間	0時間
	4/19 (日)	4/20 (月)	4/21 (火)	4/22 (水)	4/23 (木)	4/24 (金)	4/25 (土)
作業開始	00:00	12:51:50	09:26:30	09:42:12	11:52:00	19:01:58	00:00
作業終了	00:00	20:04:00	19:31:34	17:52:48	13:38:10	19:05:03	00:00
操作時間	0	4.8時間	5.1時間	0.8時間	0.2時間	0.1時間	0
	4/26 (日)	4/27 (月)	4/28 (火)	4/29 (水)	4/30 (木)	-	-
作業開始	11:25:59	09:25:04	01:19:18	00:00	01:41:20		
作業終了	22:44:33	19:13:29	18:29:24	00:00	23:40:02		
操作時間	5.4時間	5.5時間	6.1時間	0	7.4時間		

特定の日の作業を確認したいときは、日付をクリックします。PC 操作をした時間の作業が表示されます。グラフは、PC 操作量です。1 時間休まず PC 操作をした場合、最大 60 が記録されます。



インターネットに接続できないときの PC 操作履歴は、クライアントで一時的に保存され、サーバーと通信でき次第、サーバーへ送信します。

## 12.2. ツリー形式

ツリー形式では、会社全体や部署単位の作業を集計できます。

何人が PC 操作をおこなったか、その操作時間、操作人数などが閲覧できます。

-	5/17 (日)	5/18 (月)	5/19 (火)	5/20 (水)	5/21 (木)	5/22 (金)	5/23 (土)
作業開始	00:00	09:27:58	09:30:37	09:34:37	09:32:17	09:32:12	00:00
作業終了	00:00	23:35:48	19:24:03	18:38:12	22:37:36	23:37:39	00:00
操作時間	0	7.9時間	9.4時間	6.4時間	9.7時間	9.3時間	0
作業人数	0	3人	3人	4人	3人	3人	0

ツリーから部署や PC を選択し期間(年月)を指定し「集計」することができます。



## 13. USB 使用履歴

### 13.1. ログデータ

#### 検索内容

処理日時	<input type="text" value="2014/05/01"/>	<input type="text" value="0"/>	時0分	~	<input type="text" value="2015/05/27"/>	<input type="text" value="23"/>	時59分
コンピューター名	<input type="text" value="全て"/>	▼	ユーザー名	<input type="text" value="全て"/>	▼		
キーワード	<input type="text" value="検索文字"/>	タイプ	<input type="checkbox"/> open	<input checked="" type="checkbox"/> copy	<input checked="" type="checkbox"/> arrival	<input checked="" type="checkbox"/> remove	

下記の USB メモリ等の外部記憶装置の操作ログを閲覧、集計できます。

ツリー形式では、会社全体や部署単位の作業を集計できます

「**open**」 USB メモリのファイルを開いたことを記録します。USB メモリから HDD へファイルをコピーした場合などに記録されます。

「**copy**」 USB メモリへファイルを作成したことを記録します。USB メモリ等の外部記憶装置へのファイルのコピーが記録されます。

「**arrival**」 USB メモリを PC に挿入した記録です。USB メモリを挿したまま Windows を起動した場合など、arrival が記録されないことがあります。

「**remove**」 USB メモリを抜いた記録です。USB メモリを挿したまま Windows をシャットダウンした場合など、remove が記録されないことがあります。

#### 13.1.1. 期間を指定して検索

処理日時の指定し、該当期間のログを抽出し表示します。

処理日時	<input type="text" value="2014/05/01"/>	<input type="text" value="0"/>	時0分	~	<input type="text" value="2015/05/27"/>	<input type="text" value="23"/>	時59分
------	---	--------------------------------	-----	---	---	---------------------------------	------

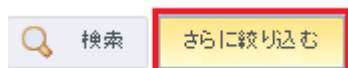
#### 13.1.2. コンピューター名などの情報を指定して検索

コンピューターやユーザーを指定してログを抽出します。

コンピューター名	<input type="text" value="全て"/>	▼	ユーザー名	<input type="text" value="全て"/>	▼
----------	---------------------------------	---	-------	---------------------------------	---



### 13.1.3 さらに絞り込む



「さらに絞り込む」機能から、コピー先フォルダ名、ファイル名や USB メモリのシリアル番号などからログを抽出できます。

## 13.2. 集計データ



「集計データ」は、USB メモリへのファイルコピーが多い、ユーザーなどを分析表示します。

ユーザー名	コピー数
ygoto-PC/ygoto	341
naokibaba/naoki baba	56

## 14. USB 一覧

社内で使用した USB の一覧を表示します。

USB一覧							
	USBID	ベンダー	プロダクト	シリアル番号	説明	使用開始日	最終使用日
1	168732	1687	3252	AA04012700	1.8GB Kingmax USB2.0 FlashDisk USB Devi	2015/01/19 16:38:30	2015/01/19 16:38:30
2	0EA068	0EA0	6828	230760A43F	30MB BUFFALO ClipDrive USB Device	2015/05/08 15:37:52	2015/05/08 15:37:52

USBID は、PasoLog Manager 内部で使用する ID です。

USB メモリは、ベンダーID, プロダクト ID, シリアル番号でユニークに識別できます。

### USB メモリの紛失確認方法

例) 月に一度、USB メモリを全て PC に挿入すると「最終使用日」が更新されるため、更新されない USB メモリは紛失の可能性がある、といった運用が可能です。

## 15. 作業内容

全クライアント PC の作業内容が閲覧できます。

### 15.1. ログデータ

クライアントから、1 分間隔で取得した最前面アプリケーション情報が送信されます。

「作業内容」は、ウィンドウタイトルです。どのような作業をしていたかの目安になります。

**検索内容**

処理日時   時0分 ~   時59分

コンピューター名  ユーザー名

キーワード

---

**操作ログ**

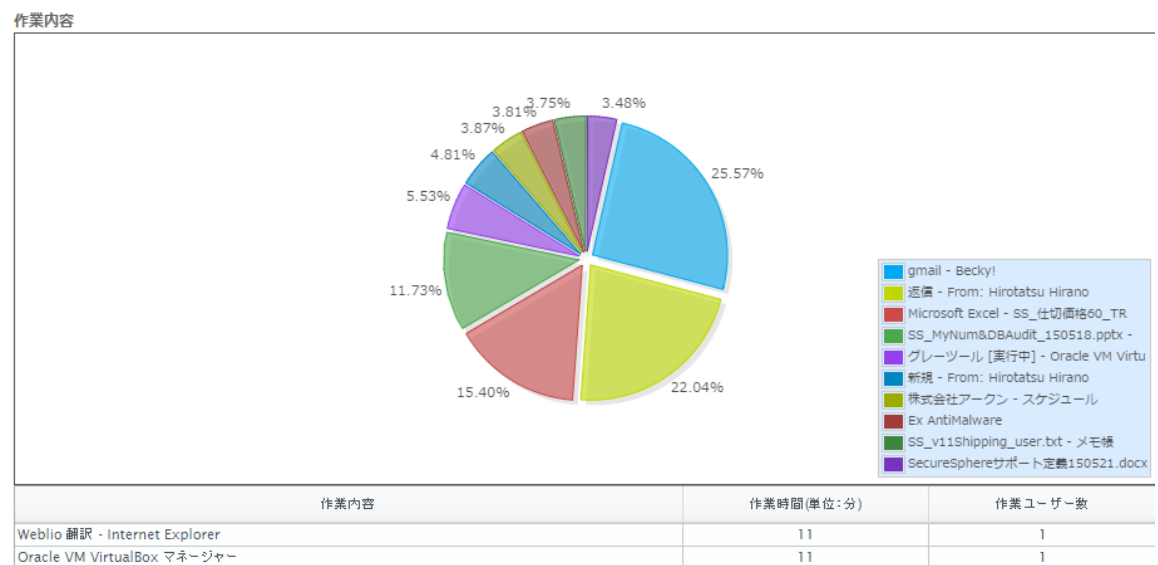
	処理日時	コンピューター名	ユーザー名	ソフト名	作業内容	実行ファイル名	
1	2015/05/27 13:31:49	vmwin8	Vpc-win8	AutoDaily User Interface	AutoDaily	ADUI32j.exe	7
2	2015/05/27 13:09:06	vmwin8	Vpc-win8	Microsoft InfoPath 2010	Microsoft InfoPath	INFOPATH.EXE	1
3	2015/05/27 13:08:00	vmwin8	Vpc-win8	AutoDaily User Interface	AutoDaily	ADUI32j.exe	7

日時や、コンピューター名、ユーザー名等での抽出ができます。

### 15.2. 集計データ

作業時間の多い順に集計し、グラフ表示します。

どのような作業に時間が使われているか可視化します。



## 16. 印刷

全クライアント印刷情報が閲覧できます。

### 16.1. ログデータ

クライアントの印刷情報が閲覧できます。

キーワード検索、印刷時間や、ドキュメント名、プリンター等で抽出できます。

### 16.2. 集計データ

印刷枚数の多いプリンター、印刷枚数が多いユーザーの集計が表示されます。

印刷コスト概算を表示します。印刷コストは「サーバー設定」「印刷コスト設定」から設定・変更できます。

## 17. 禁止ソフト起動

「ポリシー設定」「利用禁止ソフトウェア」で実行制限ソフトを設定し、制限したソフトウェアをユーザーが実行した場合、記録されます。

禁止ソフトの情報は、キーワード検索、処理時間や、ソフトウェア名等で検索できます。

ポリシーの「デスクトップ画像送信」が有効の場合、禁止ソフトを起動したデスクトップ画像を保存します。画像送信が無効であれば、禁止ソフト実行時の画像はサーバーへ送られません。

## 18. 個人情報

「ポリシー設定」「情報漏えい(マイナンバー等)対策」で検知したファイルが、閲覧できます。

個人情報は、「新規」「保持」「削除」の3つのステータスが割り当てられます。

初回検知したファイルは、「新規」となり、2度目以降も検知されると「保持」に変わります。

クライアントでファイルを削除し、検知されなくなると「削除」になります。

クライアントにある不要な個人情報ファイルは、可能であれば削除します。

検知種類は、以下 2 種類あります。

**個人情報数** : 名字、都道府県などが設定以上、含むファイル

**キーワード** : ユーザーが指定したキーワードがファイル名に含むファイル

キーワードは、検知されたキーワードを表示します。複数ある場合は ,(カンマ)で区切り表示します。

個人情報数は、名字や都道府県等のキーワードを検知した数です。

## 19. Manager ログイン

PasoLog Manager へのログイン情報が記録されます。管理者 ID、接続時間等の情報を記録します。

**検索内容**

キーワード

---

**ログインログ**

	管理者ID	ログイン日時	ステータス	
1	Admin	2015/05/27 14:12:16	成功	113.42
2	Admin	2015/05/27 14:11:10	成功	113.42
3	Admin	2015/05/27 14:03:38	成功	113.42

## 20. ファイル操作

ユーザーのファイル操作を記録します。

記録を残すための設定は、ポリシーで指定できます。PasoLog Manager の「ポリシー設定」「情報漏えい(マイナンバー等)対策」「ファイル操作ログを取得する」から設定できます。

ファイルの操作は、処理日時、コンピューター名、ユーザー名、操作、ファイル名、ファイルパスサイズ、及び

ファイル操作ログ						
	処理日時	コンピューター	ユーザー	操作	ファイル名	ファイルパス
1	2015/11/26 09:37:08	pc	user	削除	個人情報.csv	c:\重要書類\個人情報.csv
2	2015/11/25 14:51:24	pc	user	読込	個人情報.csv	c:\重要書類\個人情報.csv
3	2015/11/25 14:46:41	pc	user	読込	個人情報.csv	c:\重要書類\個人情報.csv
4	2015/11/25 14:46:18	pc	user	実行	個人情報.csv	c:\重要書類\個人情報.csv
5	2015/11/25 14:44:46	pc	user	書込	個人情報.csv	c:\重要書類\個人情報.csv

5 件中 1 -

ファイルサイズ、ファイル作成日時・更新日時・アクセス日時、ファイルを開いたアプリケーションのファイルパスが確認できます。

ファイル操作ログ					
サイズ	作成日時	更新日時	アクセス日時		ソフトウェアパス
95 KB	2015/02/25 16:37	2015/02/25 16:37	2015/02/25 16:37	C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	
95 KB	2015/11/25 14:49	2015/06/18 15:23	2015/11/25 14:49	C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	
95 KB	2015/06/18 14:46	2015/06/18 15:23	2015/06/18 14:46	C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	
95 KB	2015/06/18 14:46	2015/06/18 15:23	2015/06/18 14:46	C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	
95 KB	2015/11/24 09:53	2015/11/24 13:49	2015/11/24 13:49	C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE	

5 件中 1 - 5 を表示

\*パワーポイントなどで「～\$ファイル名.ppt」のように実際に開いたファイル名に～\$が付加されたログが残ることがありますが、これはアプリケーションが自動作成した作業用ファイルですので問題ありません。

ファイル操作は、日時等を指定して、検索できます。

検索内容

処理日時   時0分 ~   時59分

コンピューター名  ユーザー名

キーワード

## 21. クリップボード操作

ユーザーのクリップボード操作が記録されます。

処理日時はクライアントの操作時間です。コンピューター、ユーザー、コピー内容、キーワード、キーワード数等の情報を確認できます。

クリップボードログ						
	処理日時	コンピューター	ユーザー	コピー内容	キーワード	キーワード数
1	2015/11/24 12:15:28	pc	user	佐藤,鈴木,高橋,田中,渡辺,伊藤,山本	佐藤,鈴木,高橋,田中,渡辺,伊藤	7
2	2015/11/24 12:15:06	pc	user	佐藤,鈴木,高橋,田中,渡辺,伊藤,山本	佐藤,鈴木,高橋,田中,渡辺,伊藤	7

1 << 1 ページ中 1 ページ目 >> 20

2 件中 1 - 2 を表示

「ポリシー」「情報漏えい(マイナンバー等)対策」「個人情報スキャンを有効」で指定した個人情報数を超えたテキストをクリップボードへコピーした場合の記録です。

「コピー内容」はクリップボードにコピーした文章の先頭を表示します。「キーワード」は検出したキーワードです。

**\*クリップボードは、ユーザーが非常に頻繁に使う機能のため、記録データが膨大にならないよう、ポリシー設定に合致したログのみをサーバーへ送信・保存する仕様になっております。**

クリップボード操作は、日時等を指定して、検索できます。

検索内容

処理日時   時0分 ~   時59分

コンピューター名  ユーザー名

キーワード

## 22.URL アクセス

ユーザーのブラウザ閲覧ログを表示します。

操作ログ							
	処理日時	コンピューター	ユーザー	ブラウザ種別	ブラウザ Ver	URL	タイトル
1	2016/08/10 14:39:00	WIN-DTDOITV KR83	Administrator	IE	11.00.9600	http://localhost:7080/akad/	管理コンソール
2	2016/08/10 15:01:43	WIN-DTDOITV KR83	Administrator	IE	11.00.9600	http://localhost:7080/akad/	管理コンソール
3	2016/08/10 15:43:01	WIN-DTDOITV KR83	Administrator	IE	11.00.9600	http://localhost:7080/akad/	管理コンソール

1 ページ中 1 ページ目 3 件中 1 - 3 を表示

※対応ブラウザはIE、edge、Chrome、Firefox になります。

## 23. サーバー監視

サーバー監視機能は予め監視対象サーバーにサーバーエージェントをインストールする必要があります。

※サーバーエージェントインストール手順については、サーバーエージェント操作マニュアルをご参照ください。

### 1) サーバー一覧

メニューの「サーバー監視」->「サーバー一覧」をクリックしてサーバー一覧画面を表示します。

監視対象サーバーを選択して、サーバー毎に監視設定を行います。

### サーバー一覧

全社

WIN-R2LPDT5D56H

選択中サーバー：WIN-R2LPDT5D56H

サーバー監視を有効

1) サーバーのファイルへの以下操作ログを取得する

読出  書込  削除

2) 以下のアクションが発生した場合、アラートメールを送る

業務時間外でサーバーへのアクセスがあった場合、アラートメール送信

業務時間： 15 時 00 分 ~ 18 時 00 分

サーバーのファイルを削除した場合、アラートメール送信

<画面説明>

- ① サーバー監視を有効：こちらにチェック入れた場合のみ、サーバー監視を行います。
- ② サーバーのファイルへの以下操作ログを取得する
  - ・読出：監視対象サーバーの監視フォルダへの読出ログを取得します。
  - ・書込：監視対象サーバーの監視フォルダへの書込ログを取得します。
  - ・削除：監視対象サーバーの監視フォルダのファイルの削除ログを取得します。

※監視フォルダはサブフォルダも含みます。
- ③ 業務時間外でサーバーへのアクセスがあった場合、アラートメール送信
 

こちらにチェック入れた場合、上記②のアクションが設定した時間外に発生した場合、アラートメールを管理者宛てに送信します。
- ④ サーバーのファイルを削除した場合、アラートメール送信

監視対象フォルダのファイルの削除アクションが発生した場合、アラートメールを管理者宛てに送信します。

※上記③、④アラートメール送信間隔は30分単位(前回送信してから30分過ぎてから)になります。

※アラートメール送信ためには、事前に下記2つを設定する必要があります。

- ・送信元設定 : 「サーバー設定」->「メール設定」
- ・送信先設定 : 「管理者設定」-> 管理者 I D 「Admin」のメールアドレス設定

## 2) ファイル操作

メニューの「サーバー監視」->「ファイル操作」をクリックしてファイル操作画面を表します。


ファイル操作 ?

検索内容

処理日時   時0分 ~   時59分

キーワード  🔍 検索

ファイル操作ログ

アラート	処理日時	操作	IPアドレス	コンピューター名	ユーザー	サーバー	ファイル名	
1	2015/11/25 17:57:08	読出	192.168.253.53	pc	user	SB2000STD	testText2.txt	D:\Data\SB-Station検証フォルダ\test
2	2015/11/25 17:57:08	読出	192.168.253.53	pc	user	SB2000STD	testText3+3.txt	D:\Data\SB-Station検証フォルダ\test
3	2015/11/25 17:53:51	読出	192.168.253.53	pc	user	SB2000STD	test test.txt	D:\Data\SB-Station検証フォルダ\test
4	 2015/11/25 17:53:51	削除	192.168.253.53	pc	user	SB2000STD	test (3).txt	D:\Data\SB-Station検証フォルダ\test
5	2015/11/25 17:32:33	読出	192.168.253.53	pc	user	SB2000STD	個人情報.txt	D:\Data\SB-Station検証フォルダ\個人
6	2015/11/25 17:32:33	書込	192.168.253.53	pc	user	SB2000STD	個人情報-1.txt	D:\Data\SB-Station検証フォルダ\個人

6 件中 1 - 6 を表示

## &lt;画面説明&gt;

## ① 「操作」

- ・ 読出：ファイルのコピー / ファイルのプロパティを見る / ファイルを開く
- ・ 書込：ファイルの貼付け / ファイルの上書き貼付け（既存ファイル名と同一ファイルを上書きする）
- ・ 読出/書込：ファイルを開く / ファイルを編集する
- ・ 削除：ファイルを削除 / 移動する

② 「IP アドレス」：IP アドレスは V4、又は V6 どちらかが表示されます。

③ 「アラート」：サーバー一覧で設定したアラート設定条件に一致するログはアラート画像を表示します。



## 24. メッセージ送信機能

マネージャー側で作成したメッセージを各 PasoLog クライアント側に送信して、クライアント側のデスクトップに表示する機能です。

### 24.1. 前提条件

こちらの機能を有効にするためには、Manager 側のポリシーの「メッセージ送信」の項目を有効にするため、チェックを入れる必要があります。

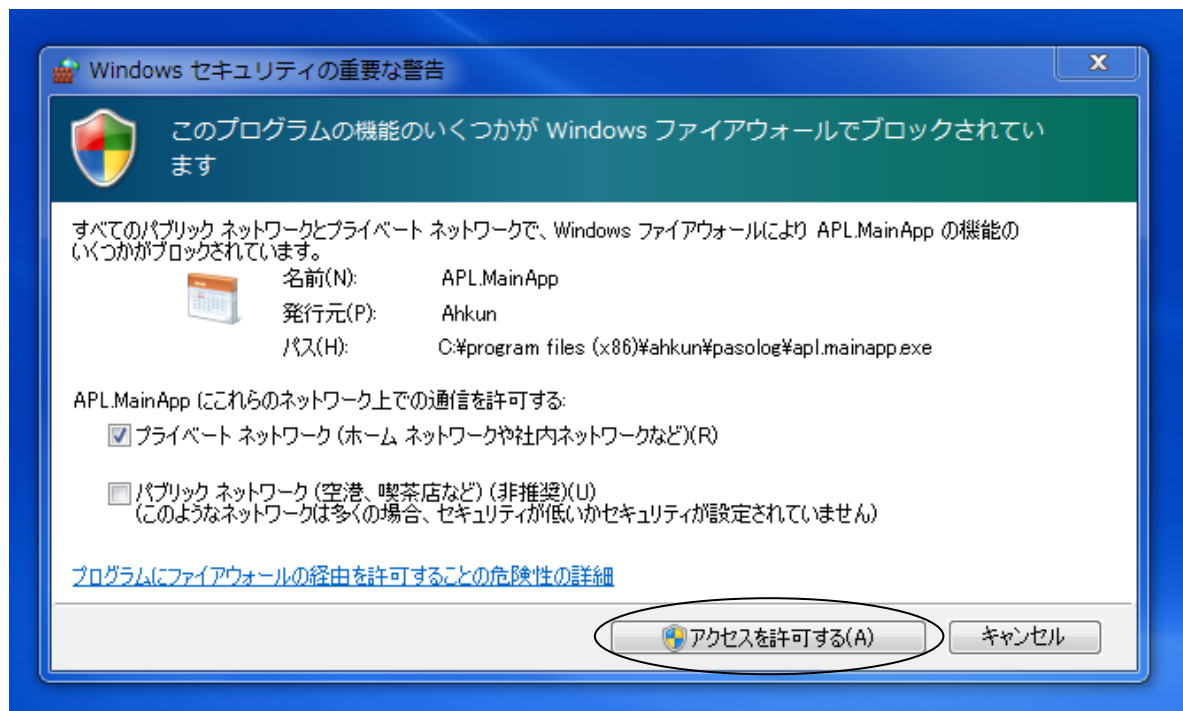
メニューの「各種設定」->「ポリシー設定」で、設定するポリシーを選択します。

「基本設定」->「8) メッセージ送信」にチェックを入れます。

#### 8) メッセージ送信

送信する

上記にチェックを入れた場合、対象ポリシーに該当するクライアント PC で名前「APL.MainApp」でファイアウォールアクセス許可確認メッセージが表示されますので、「アクセスを許可する」を選んでください。



## 24.2. メッセージ送信

トップメニューの「メッセージ一覧」をクリックします。



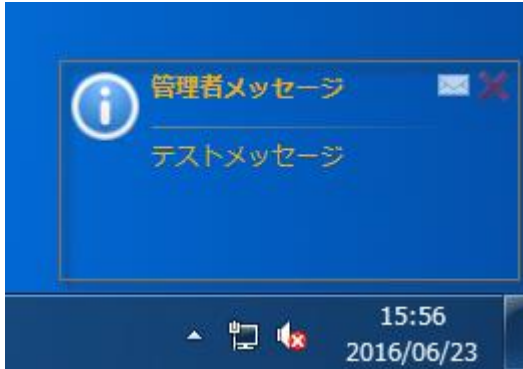
メッセージ一覧画面が表示します。「メッセージ作成」ボタンをクリックします。



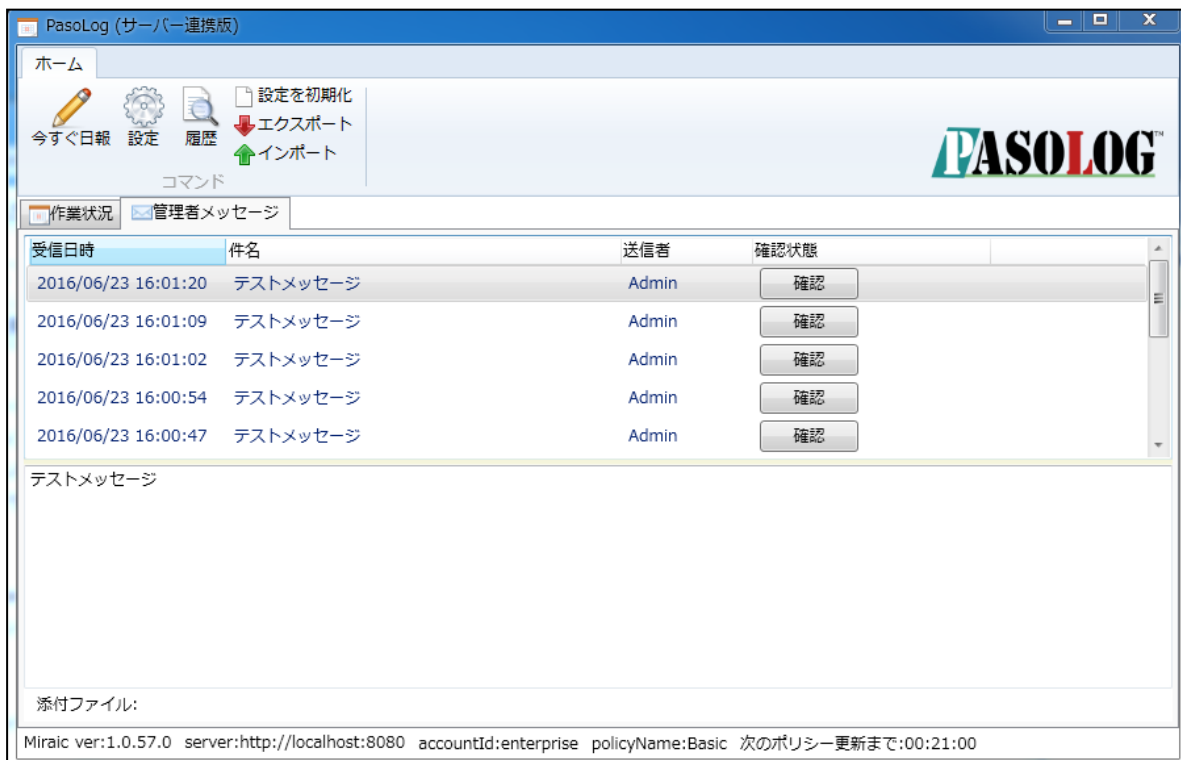
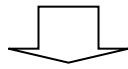
送信するメッセージの件名、本文を入力して、添付ファイルがある場合「ファイル選択」から添付します。送信先は送信区分にチェックを入れて指定します。一括指定、又は部署単位の指定も可能です。メッセージの入力、送信先の指定が完了したら、「送信」をクリックして送信します。

## 24.3. メッセージ受信

マネージャー側でメッセージを正常に送信できたら、受信側のデスクトップ画面に下記のようにメッセージが表示されます。



メッセージアイコンをクリックして、メッセージ詳細画面を開きます。



メッセージを確認したら、「確認」をクリックして、マネージャー側に確認通知を送信します。

## 24.4. メッセージ一覧

過去に送信したメッセージをメッセージ一覧画面に表示します。各メッセージの「詳細」ボタンをクリックして、メッセージ詳細を表示します。

メッセージ一覧

キーワード

	送信日時	件名	送信者	送信数	確認数	送信失敗数	詳細
1	2016/06/23 16:01:20	テストメッセージ	Admin	0	0	1	<input type="button" value="詳細"/>
2	2016/06/23 16:01:09	テストメッセージ	Admin	0	0	1	<input type="button" value="詳細"/>
3	2016/06/23 16:01:02	テストメッセージ	Admin	1	1	0	<input type="button" value="詳細"/>
4	2016/06/23 16:00:54	テストメッセージ	Admin	1	1	0	<input type="button" value="詳細"/>
5	2016/06/23 16:00:47	テストメッセージ	Admin	1	1	0	<input type="button" value="詳細"/>
6	2016/06/23 16:00:38	テストメッセージ	Admin	1	1	0	<input type="button" value="詳細"/>
7	2016/06/23 15:55:41	テストメッセージ	Admin	1	0	0	<input type="button" value="詳細"/>

1 - 7 を表示

メッセージ詳細

件名

本文

添付ファイル

	コンピューター名	OS	所有者	送信日時	送信フラグ	確認フラグ
1	PC1	Windows 7	佐藤	2016/06/23 16:01:02	成功	既読



株式会社フーバーブレイン

〒102-0094

東京都千代田区紀尾井町 4-1 22F

E-Mail: [info@fuva-brain.co.jp](mailto:info@fuva-brain.co.jp) URL: <https://www.fuva-brain.co.jp>