

LogVillage 2.0

運用マニュアル

V2. 6J

株式会社 蒼 天

logVillage2.0 運用マニュアル

revision : MU-26-20210625

- *本書に記載の会社名および製品名は、各社の商標または登録商標です。
- *本ソフトウェアを無断で複製することを禁止します。
- *本書の一部または全部を無断転載することを禁止します。
- *本書の内容に関しては、将来予告なしに変更する場合があります。

株式会社蒼天

<http://www.so-ten.co.jp/>
support@so-ten.co.jp

〒135-0032
東京都江東区福住 1-14-4 山崎ビル 1F
TEL:03-5809-8406 FAX:03-5809-8495

Copyright © 2003-2021 SO-TEN, Inc. All Rights Reserved.

目次

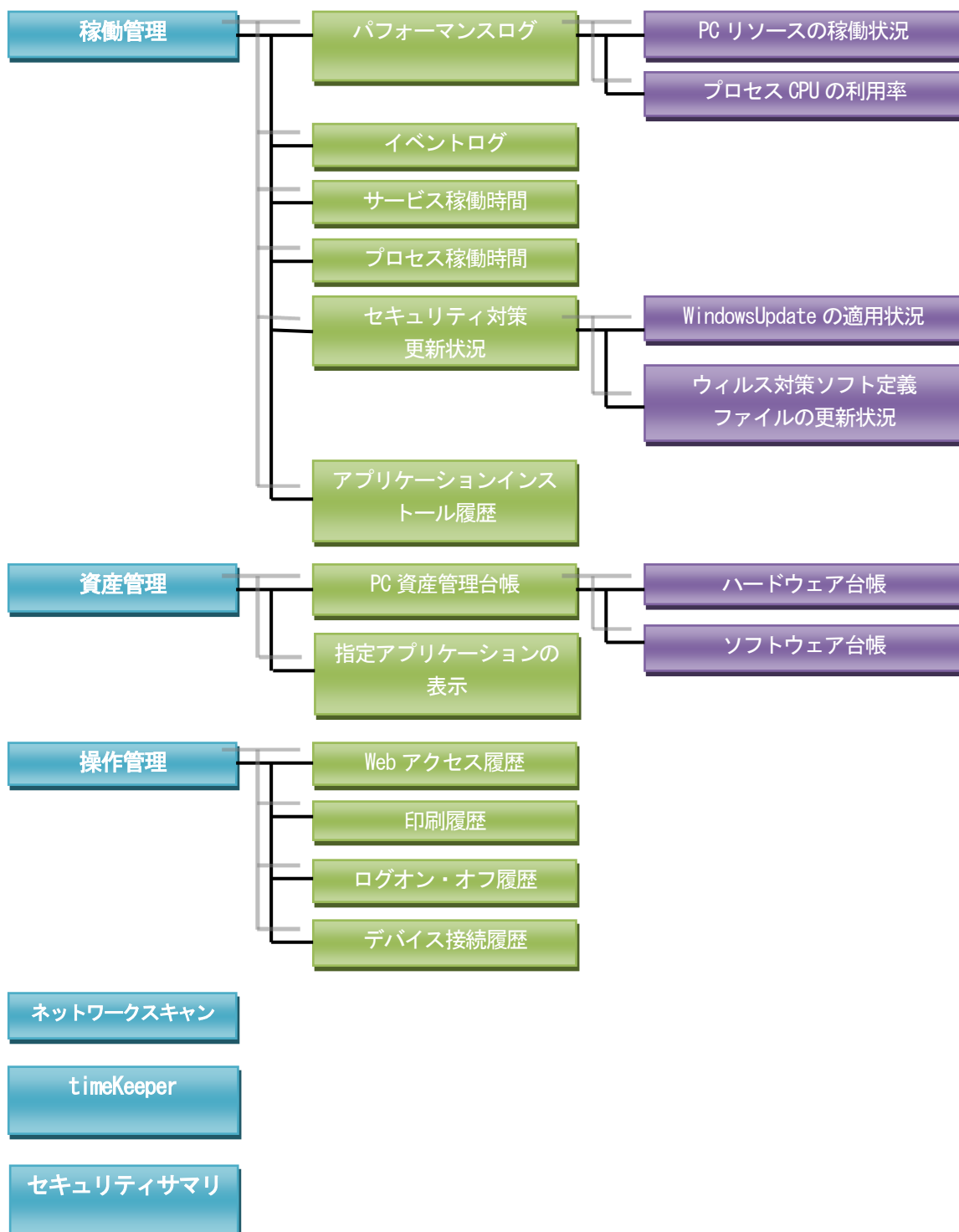
1. LogVillage 機能概要	5
1.1 メニュー系統図	6
1.2 機能一覧	7
1.2.1 LogVillage の主な機能	7
1.2.2 LogVillage のシステム設定	9
1.3 各機能画面とシステム設定画面との関係	11
1.4 グループとLogVillage ユーザーの関係図	13
2. 機能説明	14
2.1 トップ画面	14
2.1.1 ログイン画面	14
2.1.2 ログイン後の画面	15
2.2 稼働管理	16
2.2.1 パフォーマンスログ	16
2.2.2 イベントログ	23
2.2.3 サービス稼働時間	27
2.2.4 プロセス稼働時間	30
2.2.5 セキュリティ対策更新状況	32
2.2.6 アプリケーションインストール履歴	37
2.3 資産管理	40
2.3.1 PC 資産管理台帳	40
2.3.2 指定アプリケーションの設定	44
2.4 操作管理	47
2.4.1 Web アクセス履歴	47
2.4.2 印刷履歴	50
2.4.3 ログオン・オフ履歴	53
2.4.4 デバイス接続履歴	58
2.5 ネットワークスキャン	61
2.6 アラート通知履歴	62
2.7 セキュリティサマリ	66
3. システム設定	67
3.1 共通設定	69
3.1.1 ポーリングサーバ	69
3.1.2 グループ	72
3.1.3 管理対象 PC	74
3.1.4 トップ画面	82
3.1.5 WindowsUpdate 情報	83
3.1.6 ウィルス対策ソフト定義ファイル	86
3.1.7 プロセス名辞書	88
3.1.8 拡張項目名(資産管理)	91
3.1.9 ネットワークスキャン設定	92
3.1.10 ネットワークスキャンアラート設定	93
3.2 グループ単位設定	95

3.2.1 LogVillage ユーザー	95
3.2.2 ログ収集スケジュール	100
3.2.3 管理対象プロセス	103
3.2.4 管理対象サービス	105
3.2.5 指定アプリケーション	107
3.2.7 保有ソフトウェアライセンス	111
3.2.8 拡張項目データ登録(資産管理)	113
3.3 アラートポリシー設定	115
3.3.1 インベントリアラート設定	119
3.3.2 禁止 Web サイトアクセス	120
3.3.3 禁止印刷ファイル/枚数制限	123
3.3.4 禁止アカウントログオン	126
3.3.5 禁止デバイス接続	128
3.3.6 指定イベントログ発生	133
3.3.7 プロセス検知	136
3.3.8 サービス検知	140
3.3.9 ウィルス定義ファイル未更新	144
3.3.10 アプリケーション・インストール検知	146
3.3.11 PC リソースしきい値超過	150
3.4 運用管理	152
3.4.1 ライセンスの登録・更新	152
3.4.2 LogVillage へのログイン履歴	153
3.4.3 ユーザー情報変更	154
4. LogVillage の運用	155
4-1. LogVillage の再起動	155
4-2. 設定ファイル	156
4-3. LogVillage の動作ログ	159
4-4. LogVillage2.0 のシステム監視	160
4-5. 管理対象 PC 環境変更時の対応	161
4-6. LogVillage2.0 のバックアップ&リストア	162
4-7. 常駐エージェント用更新プログラムの設置	164
5. お問い合わせ	165

1. LogVillage 機能概要

LogVillage2.0 は、PC 管理ソフトウェアとして、アプリケーション&PC の稼働状況のレポート、障害・性能管理、セキュリティリスクの把握、PC 資産管理、操作ログ収集などを行います。この章では、LogVillage の機能概要について説明します。

1. 1 メニュー系統図



1. 2 機能一覧

1. 2. 1 LogVillage の主な機能

LogVillage の主な機能を説明します。

■稼働管理

PC 自体の動きを確認できる機能です。

・パフォーマンスログ

PC リソースの稼働状況

管理対象 PC のリソース稼働状況をグラフで示します。表示内容は、CPU、メモリ残、ネットワーク I/O、HDD 残、ディスク I/O です。

・イベントログ

管理対象 PC のイベントログのエラーと警告について表示します。

・サービス稼働時間

管理対象 PC のサービスが稼働した時間を表示します。

・プロセス稼働時間

管理対象 PC のプロセスが稼働した時間を表示します。

・セキュリティ対策更新状況

WindowsUpdate の適用状況

管理対象 PC の WindowsUpdate 適用状況を表示します。

ウイルス対策ソフト定義ファイルの更新状況

ウイルス対策ソフトウェアの定義ファイルの更新状況を確認することができます。

・アプリケーションインストール履歴

管理対象 PC のアプリケーションインストール履歴を表示します。

■資産管理

使用しているハードウェアやソフトウェアを管理します。

・PC 資産管理台帳

ハードウェア台帳

管理対象 PC のコンピュータ名、機種名、メーカー名、S/N、CPU、CPU 数、メモリ（総容量）、HDD 総容量、HDD 空き容量、OS、SP、Product ID、アクティベート、ユーザー拡張項目を表示します。

ソフトウェア台帳

管理対象 PC のソフトウェア一覧を表示します。

・指定アプリケーションの設定

管理対象 PC の任意に指定したアプリケーションを表示します。

・操作管理

ユーザーの操作ログ管理を行います。

・Web アクセス履歴

Web アクセス履歴を表示します。（IE6, 7 Firefox1.5, 2.0, 3.0, 3.5 での履歴を対象とします。）

・印刷履歴

管理対象 PC の印刷履歴を表示します。

・ログオン・オフ履歴

管理対象 PC のログオン・ログオフ履歴を表示します。

・デバイス接続履歴

管理対象 PC のデバイス接続履歴を表示します。

■ネットワークスキャン

検出したノードを表示します。。

■アラート通知履歴

アラート通知履歴を表示します。

■セキュリティサマリ

指定した期間のアラート通知履歴の集計の比較を表示します。

1. 2. 2 LogVillage のシステム設定

各種ログ取得の設定や管理対象 PC の設定を行うことができます。

■共通設定

・ポーリングサーバー

LogVillage マネージャに接続しているポーリングサーバーを確認・設定します。

・グループ

管理対象 PC をグループ化して登録することができます。

部署ごとにグループを作成するとわかりやすく管理ができます。グループごとに設定を行うこともできます。

・管理対象 PC

管理対象 PC の登録、削除、管理、ステータスの設定を行いません。

・トップ画面（

LogVillage のログイン画面でメッセージを表示することができます。

表示設定に文字列を入力し、変更ボタンをクリックしてください。

・WindowsUpdate 情報

管理対象 PC の WindowsUpdate 情報を設定します。

・ウィルス対策ソフト定義ファイル (p. 86)

ウィルス対策ソフト/定義ファイルの保存場所を設定します。

・プロセス名辞書

LogVillage は管理対象 PC のプロセス情報とインストールされているアプリケーション情報をそれぞれ取得することができますが、どのアプリケーションがどのプロセスか、という情報は保持していません。

したがって、プロセスの、プロセス稼働時間、システム管理画面のプロセス・アプリケーション登録やアラートリストにおいて、どのようなアプリケーションか把握するにはプロセス名とアプリケーション名を結びつける設定が必要になります。

・拡張項目名（資産管理台帳）

資産管理の追加項目の設定と HDD 残容量警告値の設定を行います。

ハードディスクの残容量警告値の設定

ハードディスクの残容量警告値の設定を行います。

空白の場合は残容量のチェックを行いません。

ハードウェア台帳の拡張項目の設定

ハードウェア台帳の拡張項目の設定を行います。

LogVillage の PC 資産情報は、WMI 情報より取得しています。WMI 情報以外の項目（例・リ

Copyright © 2003-2021 SO-TEN, Inc. All Rights Reserved.

ース期限、利用者名など)を管理する場合に使用します。

- ・ **ネットワークスキャン設定**

ネットワークスキャンを実行する IP アドレス範囲や時間を設定します。

- ・ **ネットワークスキャンアラート設定**

新規兼 sy つつノードや、検出されなくなったノードをアラート通知するための条件を設定します。

■グループ単位設定

- ・ **LogVillage ユーザー**

LogVillage を利用するユーザーの設定を行います。

- ・ **ログ収集スケジュール**

グループ毎のスケジュールの管理を行なうことができます。
どの項目をどのくらいの間隔で取るかを設定します。

- ・ **指定アプリケーション**

バージョン管理などのために、特定のソフトウェアをグルーピングして設定可能です。

- ・ **管理対象サービス**

稼働時間を確認したいサービスを登録します。

- ・ **管理対象プロセス**

稼働時間を確認したいプロセスを登録します。

- ・ **管理対象フォルダ**

ファイル管理でファイル更新履歴を取得するフォルダを登録します。

- ・ **保有ソフトウェアライセンス**

保有ライセンスの台数を登録します。

- ・ **拡張項目データ登録 (資産管理)**

資産管理の追加項目の入力を行ないます。

■アラートポリシー設定

- ・ **禁止 Web サイトアクセス**

禁止 Web サイトを設定します。

- ・ **禁止印刷ファイル/枚数制限**

禁止印刷ファイル/枚数制限を設定します。

- ・ **禁止アカウントログオン**

Copyright © 2003-2021 SO-TEN, Inc. All Rights Reserved.

禁止アカウントでのログオンを設定します。

- ・ **禁止デバイス接続**

禁止デバイスの接続を設定します。

- ・ **指定イベントログ発生**

指定イベントログの発生を設定します。

- ・ **サービス検知**

サービスの検知を設定します。

- ・ **プロセス検知**

プロセスの検知を設定します。

- ・ **ウィルス定義ファイル未更新**

ウィルス対策ソフトの定義ファイル未更新の設定を行います。

- ・ **アプリケーション・インストール検知**

アプリケーション・インストールの検知を設定します。

- ・ **PC リソースしきい値超過**

PC リソースのしきい値超過を設定します。

■運用管理

- ・ **ライセンス登録・更新**

使用オプションを変更したり、登録可能管理対象を変更したりする場合にはライセンスの更新が必要です。ライセンス情報の内容を変更する場合には、蒼天もしくは販売店までご連絡ください。

- ・ **LogVillage ログイン履歴**

LogVillage へのログオン履歴を確認することができます。

- ・ **LogVillage 稼働モニター (p. エラー! ブックマークが定義されていません。)**

稼働中の状況が確認できます。赤丸はエラーとなります。

- ・ **ユーザー情報変更**

現在ログオンしているユーザー自身のメールアドレスとパスワードを変更することが可能です。

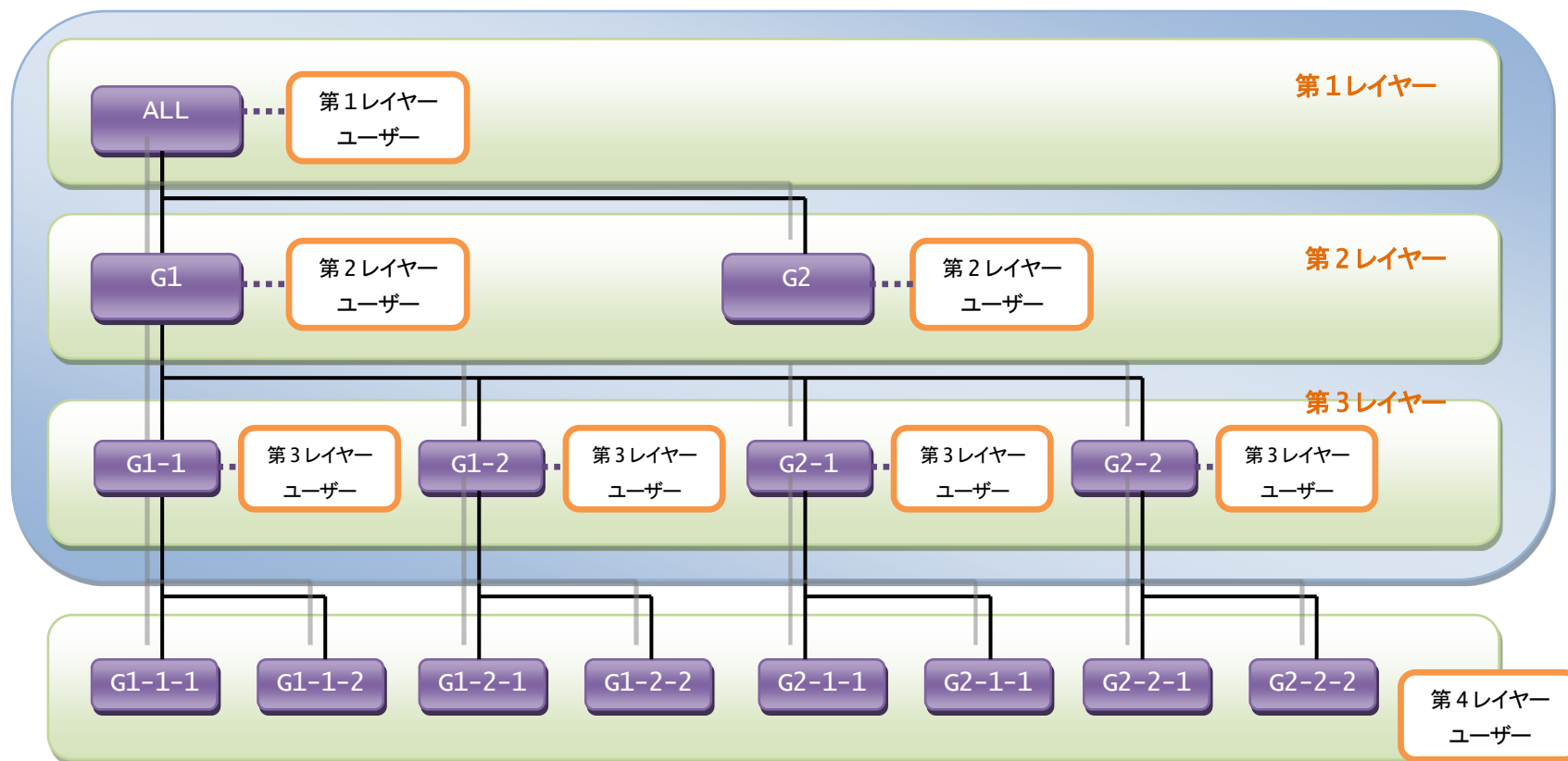
1. 3 各機能画面とシステム設定画面との関係

LogVillage では、初期設定しないとログが採取できない機能が存在します。

LogVillage の機能とシステム設定画面との関係を以下に示します。

ログ表示画面			[システム設定] 画面	
分類	画面名		「共通設定」画面	「グループ単位設定」画面
トップ画面			トップ画面	—
稼働管理	パフォーマンスログ		—	—
	イベントログ		—	—
	サービス稼働時間		—	管理対象サービス
	プロセス稼働時間		プロセス名辞書	管理対象プロセス
	セキュリティ対策更新状況	WindowsUpdate の適用状況	WindowsUpdate 情報	—
		ウィルス対策ソフト定義ファイルの更新状況	ウィルス対策ソフト定義ファイル	—
アプリケーションインストール履歴		—	—	
資産管理	PC 資産台帳	ハードウェア台帳 ※HDD 残要領警告値を設定した場合、台帳上に残容量不足の警告表示	拡張項目名（資産管理） ※拡張項目が必要ない場合は設定不要	拡張項目データ管理（資産管理） ※拡張項目が必要ない場合は設定不要
		ハードウェア詳細情報	拡張項目名（資産管理） ※拡張項目が必要ない場合は設定不要	拡張項目データ管理（資産管理） ※拡張項目が必要ない場合は設定不要
		ソフトウェア台帳	—	—
	指定アプリケーションの表示		—	指定アプリケーション
	操作管理	Web アクセス履歴		—
印刷履歴		—	—	
ログオン・オフ履歴		—	—	
デバイス接続履歴		—	—	
アラート通知履歴		—	—	
ファイル管理	ファイル管理			管理対象フォルダ

1. 4 グループと LogVillage ユーザーの関係図



LogVillage のグループとは？

管理対象 PC をグループ管理したり、LogVillage 操作画面のユーザーをグループに所属させ権限を管理することができます。導入直後は、第1レイヤーである「ALL」だけが設定されています。必要に応じてグループを作成してください。また、グループは階層構造（30 まで）にすることができます。会社の組織と対応させると管理がしやすくなります。

2. 機能説明

2. 1 トップ画面

2. 1. 1 ログイン画面

インターネットブラウザにて、「http://[ホスト名 or IP アドレス]/lv/login」にアクセスします。

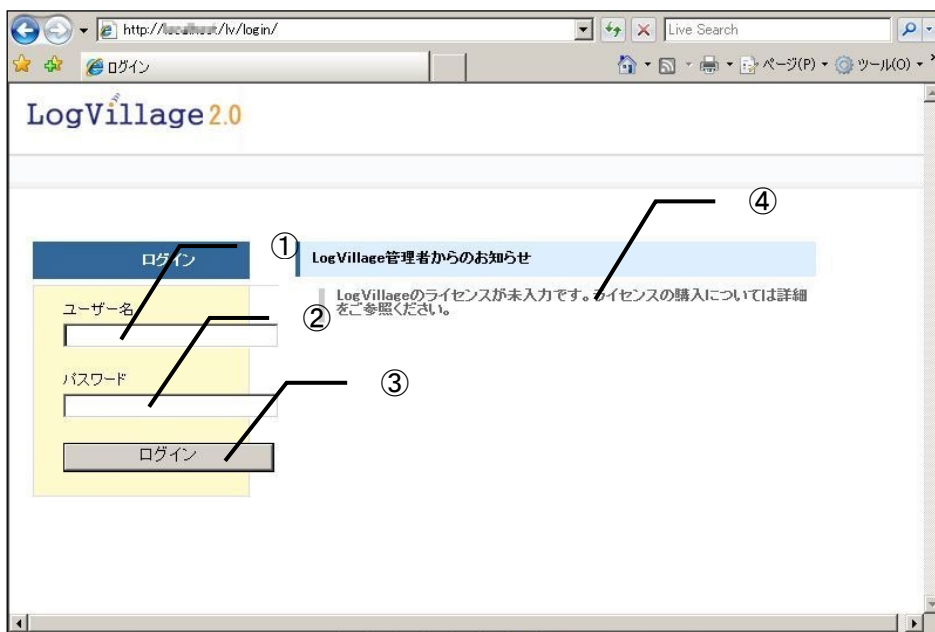
ログイン画面が表示されます。

- ①ユーザー名を入力します。
- ②パスワードを入力します。
- ③「ログイン」ボタンをクリックしてください。

- ・ユーザー名 so-ten
- ・パスワード so-ten

④LogVillage 管理者からのお知らせ

システム設定にて設定を行うことによってお知らせの表示が可能です。（p. 82 参照）



2. 1. 2 ログイン後の画面

ログインするとログイン完了のメッセージとともにメニューが表示されます。



2. 2 稼働管理

PC 自体の動きを管理する機能です。

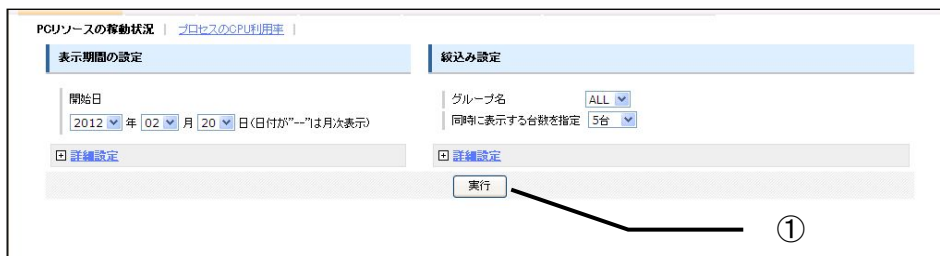


2. 2. 1 パフォーマンスログ

PC リソースの稼働状況

管理対象 PC のリソース稼働状況をグラフで示します。
表示内容は、CPU、メモリ残、ネットワーク IO、HDD 残、ディスク IO です。

①「実行」ボタンをクリックすると稼働状況が表示されます。



■絞り込み設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

・表示期間の設定

①終了日

開始日と合わせて範囲指定することが可能です。

②一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み設定

④コンピュータ名を指定

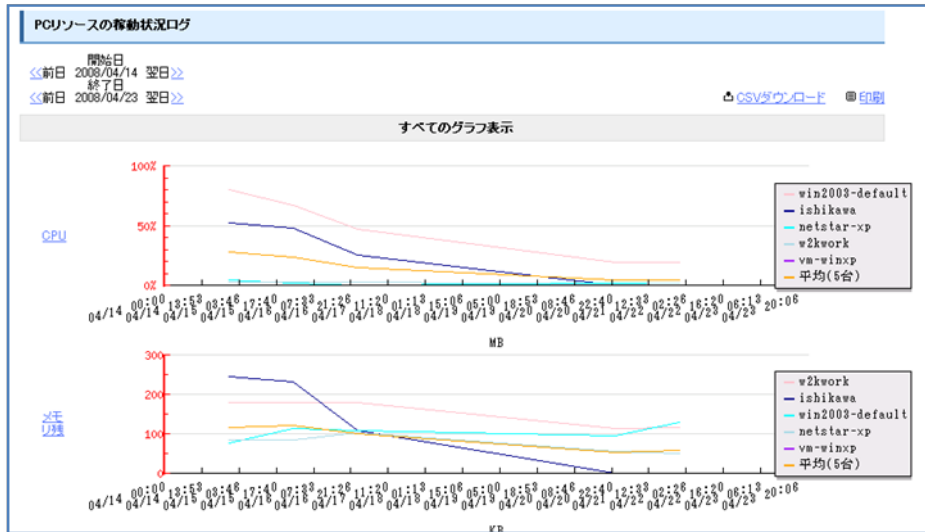
特定のコンピュータに絞り込んで結果を出力することが可能です。
(部分一致可)

⑤表示するリソースを指定（複数選択可）

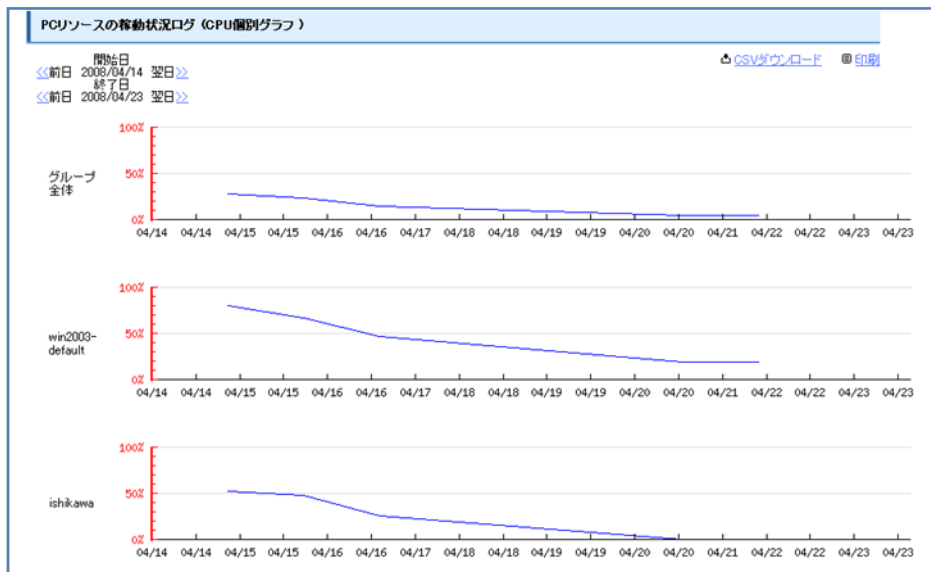
表示したい項目をチェックして絞り込むことが可能です。

CPU メモリ残 ネットワーク IO HDD 残 ディスク IO

■出力結果



CPU、メモリ残、ネットワーク I/O、HDD 残、ディスク I/O の各項目をクリックすると、各マシンの状況が個別に表示されます。



■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

"□ 検索条件"

開始日,2008-03-31

終了日,--

一日毎の時間指定,:~:

曜日指定,

グループ名,ALL

コンピュータ名,

"□ レポート"

日時,グループ名,クライアントPC名,CPU使用率,メモリ使用,ネットワーク
IO,HDD残,ディスクIO

"2008-03-31 08:00:00",ALL,win2003-
default,16.13772,281514,37,36396497,9.5

"2008-03-31 09:00:00",ALL,win2003-
default,10.069922,263663,59,36393472,5

"2008-03-31 11:00:00",ALL,win2003-
default,20.35264,195268,60,36378624,4.5

"2008-03-31 10:00:00",ALL,win2003-
default,12.41954,216792,58,36386508,3

"2008-03-31 11:00:00",ALL,ishikawa,0,0.,0,0.,0

"2008-03-31 09:00:00",ALL,ishikawa,0,0.,0,0.,0

"2008-03-31 08:00:00",ALL,ishikawa,0,0.,0,0.,0

"2008-03-31 10:00:00",ALL,ishikawa,0,0.,0,0.,0

"2008-03-31 10:00:00",ALL,vm-
winxp,0.251574,76887,5,17423360,0

:

:

■印刷

画面の内容が印刷されます。

プロセス CPU の利用率

管理対象 PC のプロセスの CPU 利用率を円グラフで示します。
どのプロセスが多く使われているかを知ることによって、利用者がどんな仕事をしているか知るヒントになります。

①「実行」ボタンをクリックすると利用率が表示されます。

■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

・表示期間の設定

①終了日

開始日と合わせて範囲指定することが可能です。

②一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み条件

④コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。

(部分一致可)

⑤アプリケーション名 or プロセス名を指定

特定のアプリケーション名、プロセス名などに絞りこんで結果を出力することが可能です。表示したい項目をチェックください。(部分一致可)

※アプリケーション名で検索する場合は、「システム設定→共通設定→プロセス名辞書」にて設定が必要です。

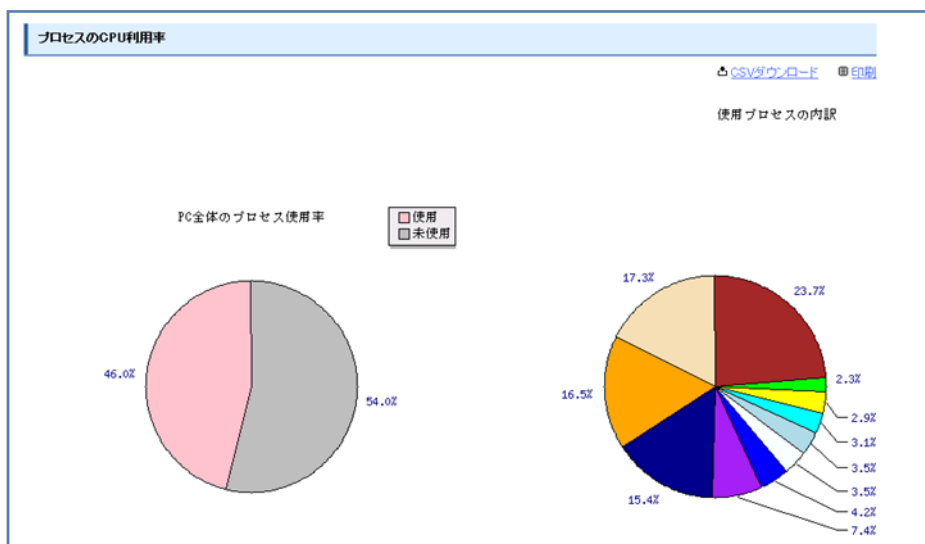
■出力結果

・PC 全体のプロセス使用率

PC の稼働状況が確認可能です。

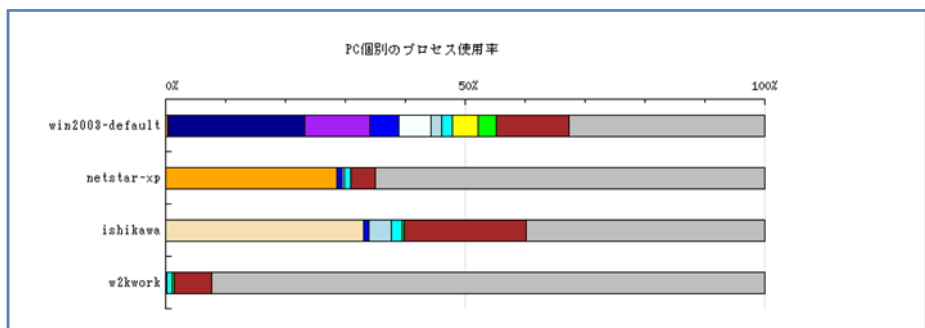
・使用プロセスの内訳

どんなプロセスがよく使用されているか確認可能です。



・PC 個別のプロセス使用率

PC 毎にどんなプロセスが使われているか確認可能です。



■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

"□ 検索条件"

開始日,2008-03-31

終了日,--

一日毎の時間指定,:~:

曜日指定,

グループ名,

アプリケーション名,

コンピュータ名,

プロセス名,

"指定アプリケーション名 ",

"□ レポート"

日時,グループ名,クライアントPC名 ,プロセス名,プロセスID,プロセスのCPU利用率

"2008-03-31 10:00:00",ALL,win2003-default,ALG,2540,0.00

"2008-03-31 11:00:00",ALL,win2003-default,ALG,2540,0.00

"2008-03-31 10:00:00",ALL,win2003-default,APACHEMONITOR,3580,0.08

"2008-03-31 11:00:00",ALL,win2003-default,APACHEMONITOR,3580,0.00

"2008-03-31 10:00:00",ALL,win2003-default,CSRSS,768,0.00

"2008-03-31 11:00:00",ALL,win2003-default,CSRSS,768,0.00

"2008-03-31 10:00:00",ALL,win2003-default,CTFMON,3560,0.00

:

:

■印刷

画面の内容が印刷されます。

2. 2. 2 イベントログ

管理対象 PC のイベントログのエラーと警告について表示します。

①「実行」ボタンをクリックするとイベントログ一覧が表示されます。

The screenshot shows the LogVillage 2.0 web interface. At the top, there's a navigation bar with tabs like '移動管理', '資産管理', '操作管理', 'ファイル管理', 'アラート通知履歴', and 'セキュリティサマリー'. Below this, there's a sub-navigation bar with 'パフォーマンスログ', 'イベントログ', 'プロセス移動時間', 'サービス移動時間', 'セキュリティ対策更新状況', and 'アプリケーションインストール履歴'. The main content area is divided into two sections: '表示期間の設定' (Display Period Settings) and '絞り込み設定' (Filter Settings). In the '表示期間の設定' section, there are fields for '開始日' (Start Date) and '終了日' (End Date), both set to 2012年02月20日. There's also a '詳細設定' (Detailed Settings) link. In the '絞り込み設定' section, there's a 'グループ名' (Group Name) dropdown set to 'ALL' and another '詳細設定' link. The '実行' (Execute) button is located at the bottom right of the '絞り込み設定' section and is highlighted with a circled 1 and an arrow.

■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

This screenshot shows the '詳細設定' (Detailed Settings) page for the 'イベントログ' (Event Log). It is divided into two main columns. The left column, '表示期間の設定' (Display Period Settings), includes: ① '開始日' (Start Date) set to 2012年02月20日; ② '終了日' (End Date) set to 2012年02月20日; ③ '一日毎の時間帯指定' (Specify time zone for each day) with a range from 00時00分 to 23時59分; and ④ '曜日指定' (Specify day of the week) with checkboxes for 月, 火, 水, 木, 金, 土, 日. The right column, '絞り込み設定' (Filter Settings), includes: ⑤ 'グループ名' (Group Name) set to 'ALL'; ⑥ 'コンピュータ名を指定' (Specify computer name) with a '部分一致' (Partial match) checkbox; ⑦ 'ログオンアカウント名を指定' (Specify logon account name) with a '部分一致' checkbox; ⑧ 'イベントの種類を指定' (Specify event type) with checkboxes for 'アプリケーション', 'セキュリティ', and 'システム'; ⑨ 'イベントの種類を指定' (Specify event type) with checkboxes for 'エラー', '警告', and '情報'; ⑩ 'イベントIDを指定' (Specify event ID) with a '部分一致' checkbox; and ⑪ 'イベントのソースを指定' (Specify event source) with a '部分一致' checkbox. At the bottom, there's an '実行' (Execute) button.

・表示期間の設定

① 終了日

開始日と合わせて範囲指定することが可能です。

② 一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③ 曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み条件

④コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。
(部分一致可)

⑤ログオンアカウント名を指定

特定のログオンアカウントに結果を出力することが可能です。
(部分一致可)。

⑥イベントの種別を指定 (複数選択可)

アプリケーション、セキュリティ、システムのイベントの種類が指定可能です。

⑦イベントの種別を指定 (複数選択可)

エラー、警告、情報のイベントの種類が指定可能です。

⑧イベント ID を指定

特定のイベント ID が指定可能です。(部分一致可)

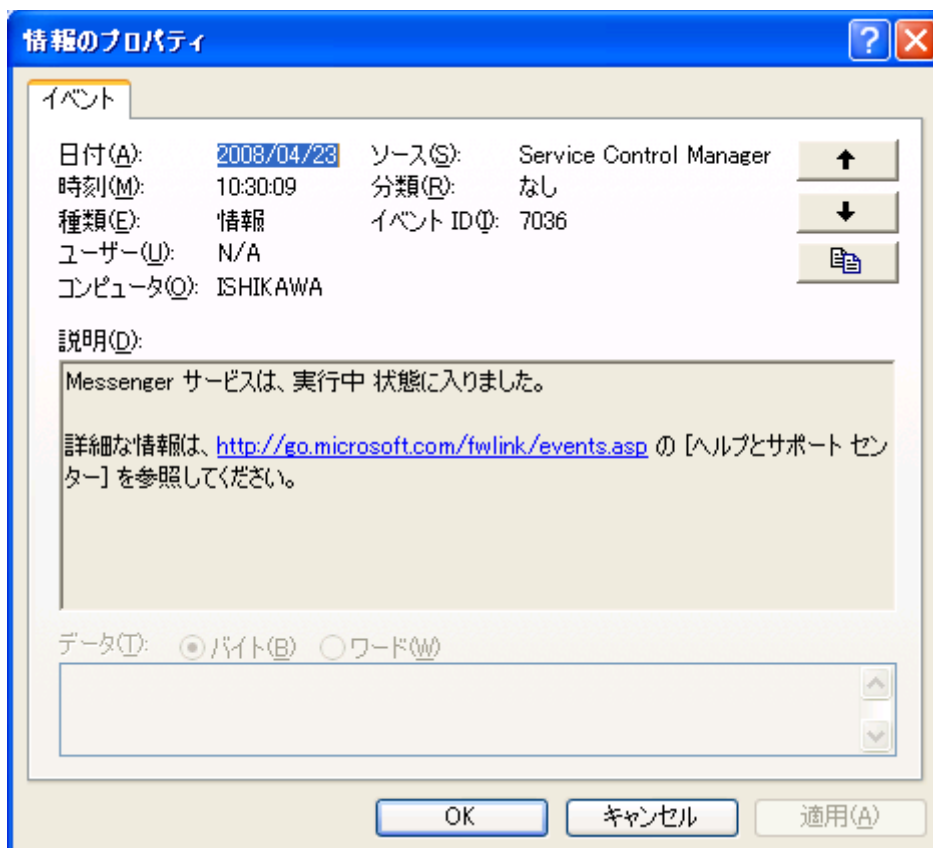
⑨イベントのソースを指定

特定のイベントソースが指定可能です。(部分一致可)

⑩イベントの説明のキーワードを指定

イベントの説明文字列から部分一致検索が可能です。

Windows 上のイベント情報の例を以下に示します。



■ 出力結果

イベントログ						
◀ 前日 2008/03/28 翌日 ▶		CSVダウンロード		印刷		
日時▼	グループ名▼	コンピュータ名▼	ログオンアカウント名▼	種類▼	イベントID▼	ソース▼
						説明▼
2008-03-28 08:43:04	ALL	ishikawa	N/A	システム 警告	4	b57w0k
次の情報はイベントの一部です。 - Broadcom NetLink (TM) Fast Ethernet						
2008-03-28 08:43:37	ALL	ishikawa	N/A	システム エラー	5	ACPI
次の情報はイベントの一部です。 - AMLIOx810x81 - 0x83						
2008-03-28 08:43:46	ALL	ishikawa	N/A	システム 警告	1003	Dhcp
ネットワーク アドレスが 0013E8234D49 のネットワーク カードに付いて、ネットワーク (DHCP サーバー) から割り当てられたアドレスを書き換えることができませんでした。次のエラーが発生しました。XXXI21 ネットワーク アドレス (DHCP) サーバーから引き続き、アドレスの取得を試みます。						
2008-03-28 08:43:56	ALL	ishikawa	N/A	システム 警告	1007	Dhcp
ネットワーク アドレスが 0013E8234D49 のネットワーク カードに付する IP アドレスを自動的に構成しました。使用している IP アドレスは 169.254.225.82 です。						
2008-03-28 08:44:02	ALL	ishikawa	N/A	システム エラー	2505	Server
ネットワークの別のコンピュータが同じ名前を使用しているため、サーバーはトランスポート \Device\NPF{40F1CBF9-2964-48AE-986D-2F94311B1A60} にコンバインドできませんでした。サーバーを起動できませんでした。						
2008-03-28 08:51:50	ALL	ishikawa	N/A	システム 警告	1003	Dhcp
ネットワーク アドレスが 0013E8234D49 のネットワーク カードに付いて、ネットワーク (DHCP サーバー) から割り当てられたアドレスを書き換えることができませんでした。次のエラーが発生しました。XXXI21 ネットワーク アドレス (DHCP) サーバーから引き続き、アドレスの取得を試みます。						
2008-03-28 11:03:37	ALL	wix2003-default	N/A	アプリケーション エラー	439	ESENT
services (820) ファイル D:\Installer\WinSecws.sdb のシャドウ ヘッダーを書き込めません。エラー -1032 が発生しました。						

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

```

開始日,2008-03-28
終了日,--
一日毎の時間指定,:~:
曜日指定,
グループ名を指定,ALL
コンピュータ名を指定,
ログオンアカウント名を指定,
イベントの種別を指定,
イベントの種類を指定,
イベントIDを指定,
"イベントのソースを指定",
イベントの説明のキーワードを指定,
日付,グループ名,コンピュータ名,ログオンアカウント名,種別,種類,イベント
ID,"ソース",説明
"2008-03-28 08:43:04",ALL,ishikawa,N/A,システム,警
告,4,b57w2k,"次の情報はイベントの一部です。- Broadcom NetLink
(TM) Fast Ethernet"
"2008-03-28 08:43:37",ALL,ishikawa,N/A,システム,エラ
ー,5,ACPI,"次の情報はイベントの一部です。- AMLIOx810x81 - 0x83"
"2008-03-28 08:43:46",ALL,ishikawa,N/A,システム,警
告,1003,Dhcp,"ネットワーク アドレスが 0013E8234D49 のネットワーク カ
ードに対して、ネットワーク (DHCP
サーバー) から割り当てられたアドレスを書き換えることができませんでした。
次のエラーが発生しました:
%%121
ネットワーク アドレス (DHCP) サーバーから引き続き、アドレスの取得を
試みます。"
"2008-03-28 08:43:56",ALL,ishikawa,N/A,システム,警
告,1007,Dhcp,"ネットワーク アドレスが 0013E8234D49 のネットワーク カ
ードに対する IP アドレスを
自動的に構成しました。使用している IP アドレスは 169.254.225.82 で
す。"
"2008-03-28 08:44:02",ALL,ishikawa,N/A,システム,エラ
ー,2505,Server,"ネットワークの別のコンピュータが同じ名前を使用している
ため、サーバーはトランスポート ¥Device¥NetBT_Tcpip_{40F1CBF9-
2964-48AE-986D-2F94311B1A60} にバインドできませんでした。サーバー
を起動できませんでした。"
"2008-03-28 08:51:50",ALL,ishikawa,N/A,システム,警
告,1003,Dhcp,"ネットワーク アドレスが 0013E8234D49 のネットワーク カ
ードに対して、ネットワーク (DHCP

```

2. 2. 3 サービス稼働時間

管理対象 PC のサービスの稼働した時間を表示します。

※サービス稼働時間を表示するためには、「システム設定→グループ単位設定→管理対象サービス」にて設定が必要です。

- ① 表示するサービス名を選択します。
- ② 「実行」ボタンをクリックするとサービス稼働時間が表示されます。

■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

・表示期間の設定

① 終了日

開始日と合わせて範囲指定することが可能です。

② 一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③ 曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み条件

④ コンピュータ名を指定

Copyright © 2003-2021 SO-TEN, Inc. All Rights Reserved.

特定のコンピュータに絞り込んで結果を出力することが可能です。
(部分一致可)

⑤表示色の設定

青・黄・赤の色表示のパーセント範囲が指定可能です。

ポーリングが実行された内、該当サービスの軌道が何回検知できたかをもとに算出します。

例) 10:00 - 10:59 の間にポーリング回数が10回実行された場合

<該当サービスの検知>	<稼働率>
10 回	100%
8 回	80%
6 回	60%
:	
:	

■出力結果

表示期間の設定

開始日

2008 年 03 月 31 日 (日付が"-"は月次表示)

☐ 詳細設定

絞り込み設定

グループ名を指定

ALL

表示するサービス名を指定

HTTPFilter

☐ 詳細設定

実行

サービス稼働時間

<前日 2008/03/31 翌日>

CSVダウンロード

印刷

サービス名 HTTPFilter

	00:00	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00
win2003-default	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ishikawa	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
vm-winop	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

"□ 検索条件"

開始日,2008-03-31

終了日,--

一日毎の時間指定,:~:

曜日指定,

グループ名,ALL

サービス名,HTTPFilter

コンピュータ名,

"□ レポート"

ホスト名,サービス名,ポーリング収集時間,時間内最小ポーリング時刻,時間内
最大ポーリング時刻,時間内ポーリング回数

win2003-default,HTTPFilter,"2008-03-31 08:00:00","2008-
03-31 08:24:40","2008-03-31 08:59:10",0

win2003-default,HTTPFilter,"2008-03-31 09:00:00","2008-
03-31 09:00:12","2008-03-31 09:59:11",0

win2003-default,HTTPFilter,"2008-03-31 10:00:00","2008-
03-31 10:00:13","2008-03-31 10:59:09",0

win2003-default,HTTPFilter,"2008-03-31 11:00:00","2008-
03-31 11:00:13","2008-03-31 11:59:55",0

win2003-default,HTTPFilter,"2008-03-31 12:00:00","2008-
03-31 12:00:30","2008-03-31 12:59:44",0

win2003-default,HTTPFilter,"2008-03-31 13:00:00","2008-
03-31 13:00:55","2008-03-31 13:01:29",0

ishikawa,HTTPFilter,"2008-03-31 08:00:00","2008-03-31
08:24:41","2008-03-31 08:59:14",28

ishikawa,HTTPFilter,"2008-03-31 09:00:00","2008-03-31
09:00:17","2008-03-31 09:59:11",60

:

:

■印刷

2. 2. 4 プロセス稼働時間

管理対象 PC のプロセスの稼働した時間を表示します。

①表示するプロセス名を指定します。

②「実行」ボタンをクリックするとプロセス稼働時間が表示されます。

■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

・表示期間の設定

①終了日

開始日と合わせて範囲指定することが可能です。

②一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み条件

④コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。
(部分一致可)

⑤表示色の設定

青・黄・赤の色表示のパーセント範囲が指定可能です。

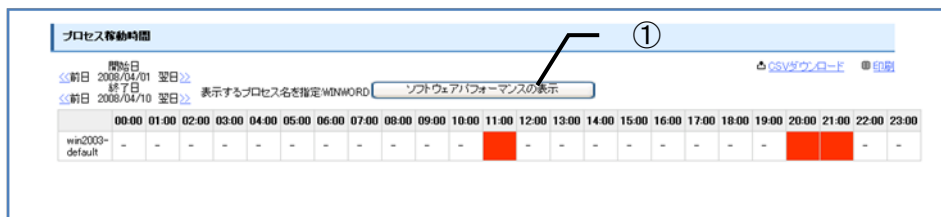
ポーリングが実行された内、該当プロセスの軌道が何回検知できたかをもとに算出します。

例) 10:00 - 10:59 の間にポーリング回数が 10 回実行された場合

<該当プロセスの検知>	<稼働率>
10 回	100%
8 回	80%
6 回	60%

:

■出力結果



① ソフトウェアパフォーマンスの表示

選択したプロセスを絞り込み条件に設定したプロセスのCPU使用率画面が表示されます。

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

条件設定を行った内容が CSV でダウンロード可能です。

“□ 検索条件”

開始日, 2008-04-01

終了日, 2008-04-10

一日毎の時間指定, : ~ :

曜日指定,

グループ名, ALL

プロセス名, WINWORD

コンピュータ名,

“□ レポート”

ホスト名, プロセス名, ポーリング収集時間, 時間内最小ポーリング時刻, 時間内最大ポーリング時刻, 時間内ポーリング回数, 時間内平均CPU利用率

win2003-default, WINWORD, “2008-04-07 00:00:00”, “2008-04-07

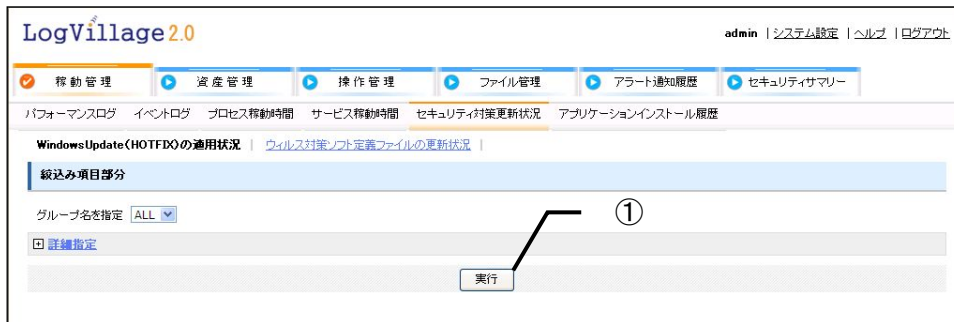
11:56:32”, “2008-04-07 11:59:29”, 2, 0

2. 2. 5 セキュリティ対策更新状況

WindowsUpdate の適用状況

管理対象 PC の WindowsUpdate 適用状況を表示します。

①「実行」ボタンをクリックすると WindowsUpdate 適用状況が表示されます。



■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。



・絞り込み検索

①コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。
(部分一致可)

②WindowsUpdate (HOTFIX) の種別

WindowsUpdate (HOTFIX) の種別をプルダウンメニューから選択します。

③WindowsUpdate の内容 or 文書番号で検索

プルダウンメニューから、「内容」または「文書番号」を選択します。

さらにプルダウンメニューから選択するか、キーワードを入力します。

適用されているものを表示させるか適用していないものを表示させるか選択します。

④〇〇日以上の上の HOTFIX がインストールされていない PC

日にちを入力します。

WindowsUpdate の例を示します。

[MS08-021] GDI の脆弱性により、リモートでコードが実行される

対象製品

目次

- はじめに
- このセキュリティ更新プログラムに関するヘルプとサポートを受ける方法
- このセキュリティ更新プログラムに関する既知の問題
- 現象
- 解決方法
- ファイル情報

はじめに

マイクロソフトはセキュリティ情報 MS08-021 を公開しました。このセキュリティ情報は、ファイルの一覧情報、展開オプションを始め、セキュリティ更新プログラムの関連情報がすべて記載されています。セキュリティ情報の詳細を参照するには、次のマイクロソフト Web サイトのいずれかにアクセスしてください。

- ホーム ユーザー向け
<http://www.microsoft.com/japan/security/bulletins/MS08-021e.msp>
- 詳細をスキップ：ご自宅のコンピュータまたはラップトップに、Microsoft Update Web サイトから更新プログラムを今すぐダウンロードします。
<http://update.microsoft.com/microsoftupdate/>
- IT プロフェッショナル向け
<http://www.microsoft.com/japan/technet/security/bulletin/ms08-021.msp>

↑ 先頭へ戻る

x64 ベースの Windows Server 2003 (SP1QFE)	Gdi32.dll Wgd32.dll Win32k.sys	Gdi32.dll Wgd32.dll
Itanium ベースの Windows Server 2003 (SP1QFE)	Gdi32.dll Wgd32.dll Win32k.sys	Gdi32.dll Wgd32.dll

解決方法

この問題を解決するには、セキュリティ情報 MS08-021 に記載されているセキュリティ更新プログラムを再インストールします。この更新プログラムをインストールするには、以下のマイクロソフト Web サイトにアクセスしてください。

<http://www.update.microsoft.com>

↑ 先頭へ戻る

ファイル情報

セキュリティ更新プログラム (日本語版) のファイル属性は、セキュリティ情報 MS08-021 の「ファイル情報」セクションをご覧ください。

↑ 先頭へ戻る

この資料は以下の製品について記述したものです。

- Microsoft Windows Server 2003 R2 Standard Edition (32-bit x86)
- Microsoft Windows Server 2003 R2 Enterprise Edition (32-bit x86)
- Microsoft Windows Server 2003 R2 Datacenter Edition (32-bit x86)
- Microsoft Windows Server 2003 R2 Standard x64 Edition
- Microsoft Windows Server 2003 R2 Enterprise x64 Edition
- Microsoft Windows Server 2003 R2 Datacenter x64 Edition
- Microsoft Windows Server 2003, Standard x64 Edition

■ 出力結果

WindowsUpdateの適用状況							
日付▼	グループ名▼	コンピュータ名▼	OS名▼	WindowsUpdate (HOTFIX)の種別	文書番号▼	WindowsUpdateの内容▼	未適用期間
	ALL	Vista-PC2					
2008-03-27 16:15:26	ALL	ishikawa	MICROSOFT WINDOWS XP PROFESSIONAL		923845		4
2008-02-14 03:01:24	ALL	vm-winxp	MICROSOFT WINDOWS XP PROFESSIONAL		946026		46
	ALL	w2kwork	MICROSOFT WINDOWS 2000 PROFESSIONAL				
2007-11-20 19:28:19	ALL	win2003-default	MICROSOFT(R) WINDOWS(R) SERVER 2003, STANDARD EDITION		911164		132

■ CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

"□ 検索条件"

グループ名を指定, ALL
 コンピュータ名を指定,
 windowsUpdate(HOTFIX)の種別を指定,
 "windowsUpdateの内容 or 文書番号で検索",
 " windowsUpdateを選択する",
 " windowsUpdateのキーワードを指定する",
 適用されているPC/適用されていないPC,
 期間(日),

"□ レポート"

日付,グループ名,コンピュータ名,OS名,windowsUpdate(HOTFIX)の種別,
 文書番号,windowsUpdateの内容,未適用期間(日)
 ,ALL,Vista-PC2,,,,,
 "2008-03-27 16:15:26",ALL,ishikawa,"MICROSOFT WINDOWS XP PROFESSIONAL",,923845,,4
 "2008-02-14 03:01:24",ALL,vm-winxp,"MICROSOFT WINDOWS XP PROFESSIONAL",,946026,,46
 ,ALL,w2kwork,"MICROSOFT WINDOWS 2000 PROFESSIONAL",,,,
 "2007-11-20 19:28:19",ALL,win2003-default,"MICROSOFT (R) WINDOWS(R) SERVER 2003, STANDARD EDITION",,911164,,132

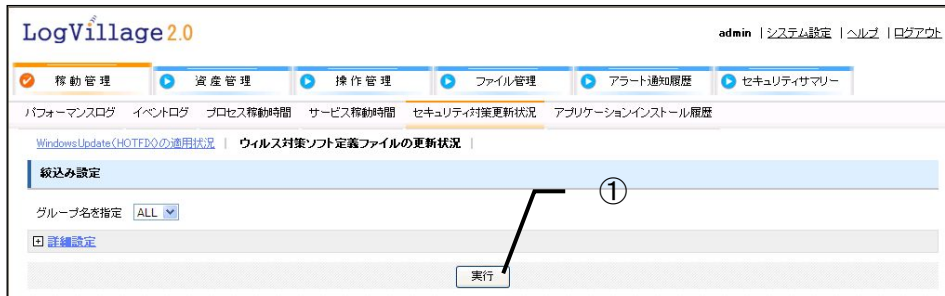
■ 印刷

画面の内容が印刷されます。

ウィルス対策ソフト定義ファイルの更新状況

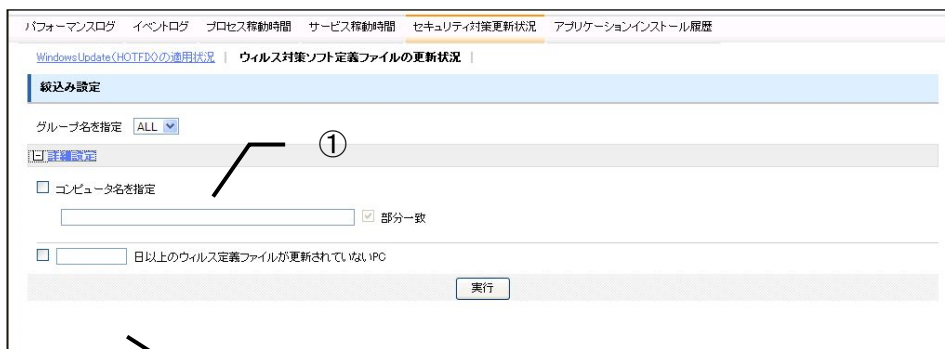
ウィルス対策ソフトウェアの定義ファイルの更新状況を確認することができます。

①「実行」をクリックします。



■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。



・絞り込み設定

①コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。
(部分一致可)

②〇〇日以上ウィルス定義が更新されていないPC

日にちを入力します。

■出力結果

定義ファイルの更新状況					
CSVダウンロード 印刷					
日付▼	グループ名▼	コンピュータ名▼	OS名▼	ウィルスソフト名▼	未更新期間▼
2008-03-07 21:06:28	営業本部	netstar-xp	MICROSOFT WINDOWS XP PROFESSIONAL	ウイルスバスター-2008	48日

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

グループ名を指定, ALL
コンピュータ名を指定,
未更新期間 (日) ,
日付, グループ名, コンピュータ名, OS名, "ウィルスソフト名", 未更新期間
(日)
"2008-03-07 21:06:28", 営業本部, netstar-xp, "MICROSOFT WINDOWS XP
PROFESSIONAL", "ウイルスバスター-2008", 48

■印刷

画面の内容が印刷されます。

2. 2. 6 アプリケーションインストール履歴

管理対象 PC のアプリケーションインストール履歴を表示します。

①「実行」ボタンをクリックするとアプリケーションインストール履歴が表示されます。

The screenshot shows the 'アプリケーションインストール履歴' (Application Installation History) tab. Under the '絞込み設定' (Filter Settings) section, the '実行' (Execute) button is highlighted with a circled 1.

■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

The screenshot shows the '詳細設定' (Detailed Settings) section. Numbered callouts indicate the following settings: 1. Start date (開始日), 2. End date (終了日), 3. Day of week (曜日指定), 4. Computer name (コンピュータ名を指定), and 5. Application name (アプリケーション名を指定).

・表示期間の設定

①終了日

開始日と合わせて範囲指定することが可能です。

②一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み条件

④コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。(部分一致可)

⑤アプリケーション名を指定

特定のアプリケーションに絞り込んで結果を出力することが可能です。(部分一致可)

■出力結果

表示期間の設定

開始日
2008 年 04 月 -- 日(日付が"--"は
"この日"を表示)
[詳細設定](#)

絞り込み設定

グループ名を指定 ALL
☒ アプリケーション名番に表示する
[詳細設定](#)

実行

アプリケーション名番のインストール履歴

[前月](#) 2008/04 翌月

[CSVダウンロード](#)
[印刷](#)

アプリケーション名 ▼	件数 ▼
ADOBE READER 8.1.2 - JAPANESE	2
APACHE HTTP SERVER 2.2.4	1
CANON PIXUS IP7100	1
DNSキャッシュ FOR AIR-EDGE	1
GOOGLE TOOLBAR FOR INTERNET EXPLORER	1
LHAPLUS	1
LOGVILLAGE 2.0 HELPER PROGRAM	1
LOGVILLAGE 2.0 ボーリングサーバ	2
LOGVILLAGE 2.0 マネージャサーバ	1

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

""□ 検索条件"

開始日, 2008-04-

終了日, --

一日毎の時間指定, :~:

曜日指定,

グループ名, ALL

コンピュータ名,

アプリケーション名,

"□ レポート"

アプリケーション名, 件数

"ADOBE READER 8.1.2 - JAPANESE", 2

"APACHE HTTP SERVER 2.2.4", 1

"CANON PIXUS IP7100", 1

"DNSキャッシュ FOR AIR-EDGE", 1

"GOOGLE TOOLBAR FOR INTERNET EXPLORER", 2

LHAPLUS, 1

"LOGVILLAGE 2.0 HELPER PROGRAM", 1

"LOGVILLAGE 2.0 ポーリングサーバー", 3

"LOGVILLAGE 2.0 マネージャサーバ", 1

"MEGAPLUS VENTURI CLIENT", 1

"MICROSOFT OFFICE ACCESS MUI (JAPANESE) 2007", 1

"MICROSOFT OFFICE EXCEL MUI (JAPANESE) 2007", 1

"MICROSOFT OFFICE IME (JAPANESE) 2007", 1

"MICROSOFT OFFICE INFOPATH MUI (JAPANESE) 2007", 1

"MICROSOFT OFFICE OUTLOOK MUI (JAPANESE) 2007", 1

:

:

■印刷

画面の内容が印刷されます。

2. 3 資産管理

2. 3. 1 PC 資産管理台帳

ハードウェア台帳

管理対象 PC のコンピュータ名、機種名、メーカー名、S/N、CPU、CPU 数、メモリ（総容量）、HDD 総容量、HDD 空き容量、OS、SP、Product ID、アクティベート ユーザー拡張項目を表示します。

※拡張資産項目を表示するためには、「システム設定→グループ単位設定→拡張項目名(資産管理)」にて設定が必要です。

検索条件を入力し、「検索」ボタンをクリックするとハードウェア一覧が表示されます。

LogVillage2.0

[ダッシュボード](#)
[資産管理](#)
[操作ログ管理](#)
[稼働管理](#)

資産管理 > ハードウェア台帳

グループの指定 キーワード指定(部分一致)

日付で絞り込み 2016 年 12 月 19 日から 2016 年 12 月 19 日まで

検索対象PC ☒ 全て ☐ 全て(廃棄PC含む) ☐ 廃棄PCのみ

■出力結果

ハードウェア台帳												
表示対象PC数5 / 5台 <input type="button" value="すべて"/> <input type="button" value="CSVダウンロード"/> <input type="button" value="印刷"/>												
コンピュータ名	機種名	メーカー名	S/N	CPU	CPU数	メモリ(総容量)	HDD総容量	HDD空き容量	OS	SP	Product ID	アクティベート
Vista-PC2				INTEL(R) CORE(TM)2 DUO CPU T7100 @ 1.80GHz	2	1536MB	114.5GB	53.6GB 46%	MICROSOFT WINDOWS XP PROFESSIONAL	SERVICE PACK 2	76494-OEM-0011903-00107	○
vm-winse	VMware Virtual Platform	VMware, Inc.	VMware-56 4d 1b bb fd 89 a3 ce-24 78 aa a2 ec e4 cf c5	INTEL(R) CORE(TM)2 DUO CPU T7100 @ 2.40GHz	1	256MB	20.5GB	17GB 83%	MICROSOFT WINDOWS XP PROFESSIONAL	SERVICE PACK 2	55383-338-2489015-22059	○
vm-work	VMware Virtual Platform	VMware, Inc.	VMware-56 4d bc c2 88 0d fd 07-56 08 8d 35 c4 4d 7d 57	INTEL(R) CORE(TM)2 DUO CPU T7100 @ 2.40GHz	1	256MB	20.5GB	19GB 92%	MICROSOFT WINDOWS 2000 PROFESSIONAL	SERVICE PACK 4	52242-335-7644025-09229	×
win2003-default	VMware Virtual Platform	VMware, Inc.	VMware-56 4d 96 28 c9 6c 30 48-36 c1 42 ca 17 d3 b6 55	INTEL(R) CORE(TM)2 DUO CPU T7100 @ 1.80GHz	1	512MB	41GB	87.1GB	MICROSOFT(R) WINDOWS(R) SERVER 2003 STANDARD EDITION	SERVICE PACK 1	69833-296-0666803-44665	○

- ・コンピュータ名をクリックすると詳細リストが表示されます。
- ・コンピュータ名以外の展開可能な項目をクリックするとその項目内容を条件として絞り込み表示します。
- ・項目名の▽をクリックするとその項目でのソートが可能です。

■すべて

接続している管理対象 PC をすべて表示します。

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

```

グループの指定,ALL
キーワード指定(部分一致),

"□ ハードウェア情報",コンピュータ名,機種名,メーカー名,S/N,メーカー,
CPU,メモリ(総容量)MB,HDD(総容量)GB,HDD(空き容量)GB,HDD(残容量%),
OS,SP,"Product ID",アクティベート
,Vista-PC2,,,,,,,,,,,,,
,ishikawa,07644XJ,LENOVO,LV01294,"INTEL(R) CORE(TM)2 DUO
CPU      T7100  @
1.80GHZ",2,1536,114.5,53.6,46,"MICROSOFT WINDOWS XP
PROFESSIONAL","SERVICE PACK 2",76494-OEM-0011903-
00107,0
,vm-winxp,"VMware Virtual Platform","VMware,
Inc.,"VMware-56 4d 1b bb fd 89 a3 ce-24 78 aa a2 ec e4
cf c5","INTEL(R) CORE(TM)2 QUAD CPU      @
2.40GHZ",1,256,20.5,17,83,"MICROSOFT WINDOWS XP
PROFESSIONAL","SERVICE PACK 2",55383-338-2488015-
22659,0
,w2kwork,"VMware Virtual Platform","VMware,
Inc.,"VMware-56 4d bc c2 68 0d fd 07-56 08 8d 35 c4 4d
7d 57","INTEL(R) CORE(TM)2 QUAD CPU      @
2.40GHZ",1,256,20.5,19,92,"MICROSOFT WINDOWS 2000
PROFESSIONAL","SERVICE PACK 4",52242-335-7644025-09229,
x
:
.

```

■ 印刷

画面の内容が印刷されます。

ソフトウェア台帳

管理対象 PC のソフトウェア一覧を表示します。

検索条件を入力し、「検索」ボタンをクリックするとハードウェア一覧が表示されます。

※”コンポーネント SW の表示”がチェックオフの場合、コントロールパネル→プログラムと機能と同じ内容の表示となります。

■出力結果

ソフトウェア台帳				
表示対象PC数: 20/22 台				
CSVダウンロード 印刷				
ソフトウェア名	メーカー	保有ライセンス数	インストール数	ライセンス経過
*MORA WIN TYPE1 PLUG-IN	LabelGate	----	1	
*LHACA		----	3	
2007 MICROSOFT OFFICE SUITE SERVICE PACK 2 (SP2)	Microsoft	----	1	
ACCESS HELP		----	2	
ACTIVE PORTS		----	1	
ADOBE ACROBAT 8 STANDARD - JAPANESE	Adobe Systems	----	1	
ADOBE ACROBAT 5.0	Adobe Systems, Inc.	----	1	
ADOBE ACROBAT 8.1.3 STANDARD	Adobe Systems	----	1	

③にチェックを入れた場合の出力結果

ソフトウェア台帳

表示対象PC数: 20/22 台

CSVダウンロード

印刷

ソフトウェア名▼	バージョン情報▼	メーカー▼	保有ライセンス数	インストール数▼	ライセンス超過
*MORA WIN TYPE1 PLUG-IN	1.05	LabelGate	----	1	
+LHACA			----	3	
2007 MICROSOFT OFFICE SUITE SERVICE PACK 2 (SP2)		Microsoft	----	1	
ACCESS HELP	1.00		----	1	
ACCESS HELP	2.00		----	1	
ACTIVE PORTS			----	1	
ADOBE ACROBAT 8 STANDARD - JAPANESE	8.1.3	Adobe Systems	----	1	
ADOBE ACROBAT 5.0	5.1	Adobe Systems, Inc.	----	1	
ADOBE ACROBAT 8.1.3 STANDARD	8.1.3	Adobe Systems	----	1	

④にチェックを入れた場合の出力結果

ソフトウェア台帳				
表示対象PC数: 6/22 台				
CSVダウンロード 印刷				
ソフトウェア名	メーカー	保有ライセンス数	インストール数	ライセンス経過
MICROSOFT OFFICE ENTERPRISE 2007	Microsoft Corporation	----	1	
MICROSOFT OFFICE PROFESSIONAL 2007	Microsoft Corporation	----	1	
MICROSOFT OFFICE PROFESSIONAL PLUS 2007	Microsoft Corporation	----	4	

- ・ソート 項目名の▽をクリックするとその項目でのソートが可能です。

■CSV ダウンロード

条件設定を行った内容がCSVでダウンロード可能です。

```
"□ ソフトウェアリスト "
```

"ソフトウェア名",	バージョン情報,	メーカー,	導入数,	ライセンス数,	ライセンス未 確認数
"ACCESS HELP",	2.00,	1,	---	1	
"ADOBE READER 8.1.2 - JAPANESE",	8.1.2,	"Adobe Systems Incorporated",	1,	---	1
"APACHE HTTP SERVER 2.2.4",	2.2.4,	"Apache Software Foundation",	1,	---	1
"ARIEL MULTISCHEDULER",	11.000.1350,	"Ariel Networks",	1,	--	
					1
"BROADCOM GIGABIT INTEGRATED CONTROLLER",	10.15.13,	"Broadcom Corporation",	1,	---	1
"CANON PIXUS IP7100",			1,	---	1
"CLIENT SECURITY SOLUTION",	8.00.0114.00,	"Lenovo Group Limited",	1,	---	1
"CONEXANT HD AUDIO",	3.36.0.0,	Conexant,	1,	---	1
"CUTEPDF WRITER 2.7",			1,	---	1
"DISKEEPER LITE",	9.0.541,	"Diskeeper Corporation",	1,	---	1
GETPLUS(R)_OCX,			1,	---	1
GTONECARE,	2.0.38,	Microsoft,	1,	---	1
"INTEL(R) GRAPHICS MEDIA ACCELERATOR DRIVER",			1,	---	1
"INTERVIDEO INSTANTON (REMOVE ONLY)",			1,	---	1
"INTERVIDEO REGISTER MANAGER",	1.0.4.0,	"InterVideo Inc.",	1,	---	1
"INTERVIDEO WINDVD",	5.0-B11.1156,	"InterVideo Inc.",	1,	--	
					1
	:				
	:				

■印刷

画面の内容が印刷されます。

2. 3. 2 指定アプリケーションの設定

管理対象 PC の任意に指定したアプリケーションを表示します。

※アプリケーションを指定するには、「システム設定→グループ単位設定→指定アプリケーション」(p.107)にて設定が必要です。

- ①グループ指定、指定アプリケーションで絞り込むことができます。
- ②「実行」ボタンをクリックするとアプリケーション一覧が表示されます。

■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

①コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。
(部分一致可)

■ 出力結果

指定アプリケーションのログ		
CSVダウンロード 印刷		
グループ名▼	クライアントPC▼	MsOffice
ALL	vm-winxp	
ALL	Vista-PC2	
ALL	vm-ishikawa	
ALL	w2kwork	
ALL	win2003-default	○
営業本部	ishikawa	○
営業本部	netstar-xp	

アプリケーショングループ名をクリックするとアプリケーションごとの結果が表示されます。

グループ名▼	クライアントPC▼	MICROSOFT OFFICE ACCESS MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE EXCEL MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE IME (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE INFOPATH MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE OUTLOOK MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE POWERPOINT MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE PROFESSIONAL PLUS 2007 (12.0.4518.1014)	MICROSOFT OFFICE PROOF (ENGLISH) 2007 (12.0.4518.1014)
ALL	vm-winxp								
ALL	Vista-PC2								
ALL	vm-ishikawa								
ALL	w2kwork								
ALL	win2003-default	○	○	○	○	○	○	○	○
営業本部	ishikawa	○	○	○	○	○	○	○	○
営業本部	netstar-xp								

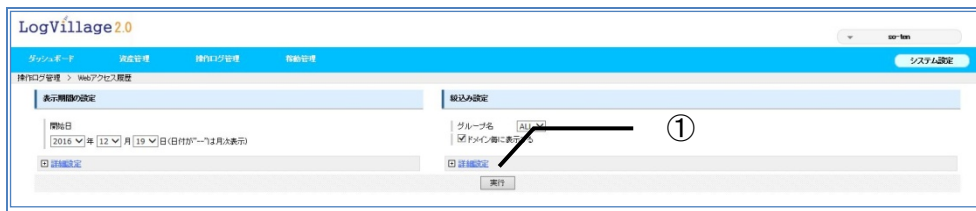
2. 4 操作管理

ユーザーの操作ログ管理です。

2. 4. 1 Web アクセス履歴

Web アクセス履歴を表示します。

- ①「実行」ボタンをクリックすると Web アクセス履歴が表示されます。
- ・「ドメイン毎に表示する」のチェックをはずすと、詳細を直接表示します。



■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。



・表示期間の設定

①終了日

開始日と合わせて範囲指定することが可能です。

②一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み設定

④コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。(部分一致可)

⑤ログオンアカウント名を指定

特定のログオンアカウント名に絞り込んで結果を出力することが可能です。(部分一致可)

⑥Web タイトル or URL

■ 出力結果

<<前日 2008/03/28 翌日>> [CSVダウンロード](#) [印刷](#)

ドメイン名▼	件数▼
7gmodules.com	10
85gmodules.com	10
88gmodules.com	8
adrbtoday.com	7
dictionary.rbtoday.com	1
disney.bk.mufg.jp	1
entry01.bk.mufg.jp	1
feature.movies.jp.msn.com	2
go.microsoft.com	1
ja.wikipedia.org	1
jp.msn.com	1
localhost	15
lv20m	29
pagead2.google syndication.com	2
runonce.msn.com	1
shikariki.com	2
win2003-default	123
www61.tikine.jp	5
www.ariel-networks.com	7
www.bk.mufg.jp	1
www.google.co.jp	3
www.google.com	24
www.lenovo.com	12
www.microsoft.com	1
www.so-ten.co.jp	1

各ドメイン名をクリックすると、ドメイン名以下の詳細の確認が可能です。

Webアクセス履歴					
<<前日 2008/03/28 翌日>>			CSVダウンロード	印刷	
日付▼	グループ名▼	コンピュータ名▼	ログオンアカウント名▼	Webタイトル▼	URL(フルパス表示)▼
2008-03-28 10:24:02	ALL	ishikawa	k-ishikawa	tcp - Google 検索	http://www.google.co.jp/custom?q=tcp&sa=...
2008-03-28 10:24:14	ALL	ishikawa	k-ishikawa	TCPポート - Google 検索	http://www.google.co.jp/custom?hl=ja&inl...
2008-03-28 10:24:36	ALL	ishikawa	k-ishikawa	TCP ポート 番号 - Google 検索	http://www.google.co.jp/custom?hl=ja&inl...

さらに、URL をクリックするとそのページにアクセスできどんなページか確認可能です。

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

"□ 検索条件"

開始日, 2008-03-28

終了日, --

一日毎の時間指定, : ~ :

曜日指定,

グループ名を指定, ALL

コンピュータ名を指定,

ログオンアカウント名を指定,

"Webタイトル or URLを指定",

"□ レポート"

ドメイン名, 件数

7.gmodules.com, 10

85.gmodules.com, 10

88.gmodules.com, 8

ad.rbbtoday.com, 7

dictionary.rbbtoday.com, 1

disney.bk.mufg.jp, 1

entry01.bk.mufg.jp, 1

feature.movies.jp.msn.com, 2

:

:

■印刷

画面の内容が印刷されます。

2. 4. 2 印刷履歴

管理対象 PC の印刷履歴を表示します。

①「実行」ボタンをクリックすると印刷履歴が表示されます。



■ 詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。



・ 表示期間の設定

① 終了日

開始日と合わせて範囲指定することが可能です。

② 一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③ 曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・ 絞り込み条件

④ コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。(部分一致可)

⑤ ログオンアカウント名を指定

特定のログオンアカウント名に絞り込んで結果を出力することが可能です。(部分一致可)

⑥ 印刷ファイル名 or プリンター名を指定

特定の印刷ファイル名やプリンター名に結果を出力することが可能です。(部分一致可)

■ 出力結果

プリンタ名毎の印刷履歴	
<<前日 2008/03/28 翌日 >> CSVダウンロード 印刷	
プリンタ名▼	枚数▼
Panasonic DP-2310	13

プリンタ名をクリックすると印刷したドキュメント名が表示されます。

※プリンター名はプリンタードライバー名となります。同じプリンターでも異なる名称であれば別のものとして表示されます。

ドライバ名の変更について（ヒント）

プリンターのプロパティにて変更可能です。

印刷履歴						
<<前日 2008/03/28 翌日 >> CSVダウンロード 印刷						
日付▼	グループ名▼	コンピュータ名▼	ログオンアカウント名▼	プリンタ名▼	印刷ファイル名 : ▼	枚数▼
2008-03-28 17:49:28	ALL	ishikawa	k-ishikawa	Panasonic DP-2310	server_vm_manual.pdf	12
2008-03-28				Panasonic DP-		

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

"□ 検索条件"

開始日,2008-03-28

終了日,--

一日毎の時間指定,:~:

曜日指定,

グループ名,ALL

コンピュータ名,

ログオンアカウント名,

検索対象,

"□ レポート"

日付,グループ名,クライアントPC,ログオンアカウント名,プリンタ名,印刷ファイル名

"2008-03-28 17:49:40",ALL,ishikawa,k-

ishikawa,"Panasonic DP-2310",server_vm_manual.pdf

"2008-03-28 17:49:28",ALL,ishikawa,k-

ishikawa,"Panasonic DP-2310",server_vm_manual.pdf

■印刷

画面の内容が印刷されます。

2. 4. 3 ログオン・オフ履歴

管理対象 PC のログオン・ログオフ履歴を表示します。

■ログオン/ログオフ履歴 OS 別取得可否一覧

以下に OS 別のログオン・ログオフ取得状態を示します。

No.	状態	Windows NT4.0	Windows 2000 Professional	Windows 2000 Server	Windows XP Professional	Windows Server 2003	Windows VISTA Ultimate
1	ローカルログオン	×	○	○	○	○	○
2	ローカルログオフ	×	×	×	○	○	○
3	シャットダウン (ログオフ)	×	○	○	○	○	○
4	ネットワークログ オン	×	○	○	○	○	○
5	ネットワークログ オフ	×	○	○	○	○	○

No.	状態	Windows VISTA Business	Windows 7 Professional	Windows 7 Enterprise	Windows 7 Ultimate	Windows Server 2008 Standard	Windows Server 2008 Enterprise
1	ローカルログオン	○	○	○	○	○	○
2	ローカルログオフ	○	○	○	○	○	○
3	シャットダウン (ログオフ)	○	○	○	○	○	○
4	ネットワークログ オン	○	○	○	○	○	○
5	ネットワークログ オフ	○	○	○	○	○	○

※ ” × ” 項目につきましては、OS に該当する状態のログを生成する機能がございません。
そのため、LogVillage ではログ情報を取得することが不可となっております。

■利用シーンによるログオン/オフの取得イメージ
ログオン・ログオフの取得イメージを示します。

	PC 利用シーン			LogVillage2.0 でのログ情報	
1	8:50	PC 起動⇒ログオン	⇒	8:50	ログオン
	12:00	休止モード		18:30	ログオフ（正常）
	13:00	休止モード解除			
	18:30	PC シャットダウン			
2	8:50	PC 起動⇒ログオン	⇒	8:50	ログオン
	12:00	シャットダウン		12:00	ログオフ（正常）
	13:00	PC 起動⇒ログオン		13:00	ログオン
	18:30	PC シャットダウン		18:30	ログオフ（正常）
3	8:50	PC 起動⇒ログオン	⇒	8:50	ログオン
	10:00	スタンバイモード⇒PC 持出し		18:30	ログオフ（正常）
		外出先で PC 操作		※ログオフ情報は、社内ネットワークへの再接続後の収集となります。	
	18:30	PC シャットダウン			
4	8:50	PC 起動⇒ログオン	⇒	8:50	ログオン
	18:30	電源断（強制終了）		翌 8:50	ログオフ（異常） [*1]
	翌 8:50	PC 起動⇒ログオン		翌 8:50	ログオン
	18:30	PC シャットダウン		翌 18:30	ログオフ（正常）

[*1] system プロセス情報により、前日の何時まで PC が稼働していたかを判別可能です。

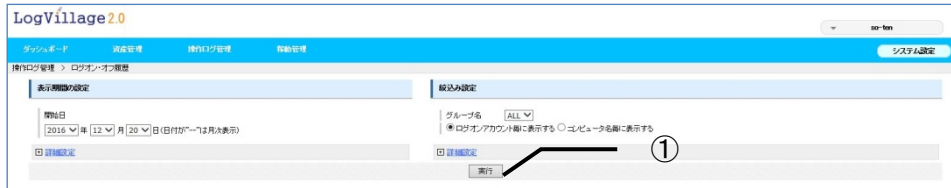
※ログオフ（例外）と表示される場合について

通常、PC のシャットダウンを実行するとイベントログにログオフが記録され、その後シャットダウンされます。

しかし、PC の状態によってはログオフが記録される前にシャットダウンされ、イベントログにログオフが記録されない場合があります。

その場合、LogVillage は、ログオフのイベントログではなく、イベントログサービスの停止のログを取得し、ログオフと判定し、“ログオフ（例外）”と表示しております。

- ①「実行」ボタンをクリックするとログオン・ログオフ履歴が表示されます。



■ 詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。



・ 表示期間の設定

① 終了日

開始日と合わせて範囲指定することが可能です。

② 一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③ 曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・ 絞り込み条件

④ コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。(部分一致可)

⑤ ログオンアカウント名を指定

特定のログオンアカウント名に絞り込んで結果を出力することが可能です。(部分一致可)

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

"□ 検索条件"

開始日,2008-03-27

終了日,2008-03-31

一日毎の時間指定,:~:

曜日指定,

グループ名,ALL

コンピュータ名,

ログオンアカウント名,

"表示","ログオンアカウント毎に表示する"

"□ レポート"

ログオンアカウント名,ログオン回数,ログオフ操作によるログオフ回数,ログオフ操作以外でのネットワーク切断回数

Administrator,13,0,23

k-ishikawa,94,6,11

■印刷

画面の内容が印刷されます。

2. 4. 4 デバイス接続履歴

管理対象 PC のデバイス接続履歴を表示します。

①「実行」ボタンをクリックするとデバイス接続履歴が表示されます。



■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。



・表示期間の設定

①終了日

開始日と合わせて範囲指定することが可能です。

②一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み条件

④コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。（部分一致可）。

⑤デバイス名を指定

特定のデバイスに絞り込んで結果を出力することが可能です。（部分一致可）

■ 出力結果

デバイス名毎のデバイス接続履歴	
◀前日 2008/03/28 翌日▶ CSVダウンロード 印刷	
デバイス名▼	件数▼
FUJITSU MHW2120BH	1
HL-DT-ST DVD+-RW GSA-H21N	1
HL-DT-ST DVD-RAM GMA-4082N	2
NECVMWare VMWare IDE CDR10	1
VMware Virtual IDE Hard Drive	1
VMware VMWare Virtual S SCSI Disk Device	2

デバイス名をクリックするとデバイス毎の接続状況の確認が可能です。

デバイス接続履歴				
◀前日 2008/03/28 翌日▶ CSVダウンロード 印刷				
最終更新日時▼	グループ名▼	コンピュータ名▼	デバイス名▼	接続時間▼
2008-03-28 18:00:22	ALL	win2003-default	HL-DT-ST DVD-RAM GMA-4082N	290分
2008-03-28 18:00:30	ALL	ishikawa	HL-DT-ST DVD-RAM GMA-4082N	280分

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

"□ 検索条件"

開始日,2008-03-28

終了日,--

一日毎の時間指定,:~:

曜日指定,

グループ名,ALL

コンピュータ名,

デバイス名,

"□ レポート"

デバイス名,件数

"FUJITSU MHW2120BH",1

"HL-DT-ST DVD+-RW GSA-H21N",1

"HL-DT-ST DVD-RAM GMA-4082N",2

"NECVMWare VMware IDE CDR10",1

"VMware Virtual IDE Hard Drive",1

"VMware, VMware Virtual S SCSI Disk Device",2

■印刷

画面の内容が印刷されます。

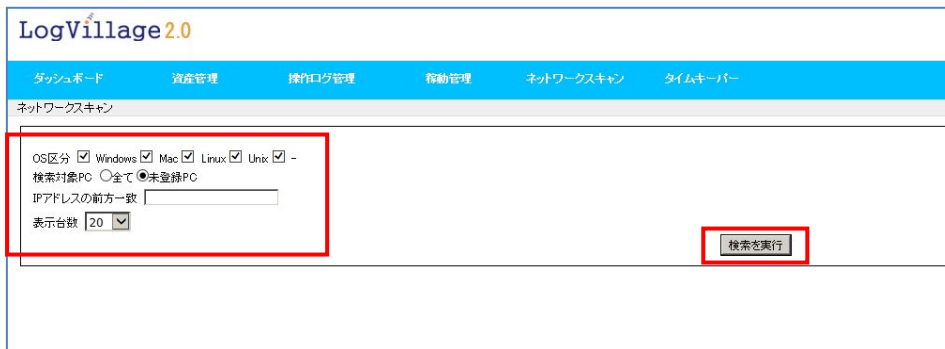
2. 5 ネットワークスキャン

ネットワークスキャンで検出されたノードの確認を行います。

① ネットワークスキャンを選択します。



② 表示条件を設定し[検索を実行]をクリックします。



<表示条件>

OS 区分	表示したい OS を選択します。 「-」は検出時に OS 判定が行えなかったノードとなります。
検索対象 PC	LogVillage の管理対象 PC として登録されていないノードを表示する場合は「未登録 PC」を選択します。
IP アドレスの前方一致	表示した IP アドレスの一部を入力します。 空白の場合は全ての IP アドレスを表示します。
表示台数	1 ページに表示する台数（行数）を選択します。

■CSV ダウンロード

表示内容を CSV でダウンロード可能です。

LogVillage2.0

admin

ダッシュボード 資産管理 操作ログ管理 移動管理 ネットワークスキャン タイムキーパー システム設定

ネットワークスキャン

OS区分 ☒ Windows ☒ Mac ☒ Linux ☒ Unix ☒ -
 検索対象PC ☐ 全て ☒ 未登録PC
 IPアドレスの前方向一致
 表示台数

検索を実行

ネットワークスキャン台帳

表示対象デバイス数: 250台 10 | 20 | 50 | 100 CSVダウンロード 印刷

IPアドレス	台帳 未登録	OS区分	MACアドレス	NICベンダー名	サブネット	ブロードキャスト	コンピュータ名	型式名	初回検出 日時	最終検出 日時
193.168.5.1	<input checked="" type="checkbox"/>	Linux	84:2D:C6:4E:5C:C0	Cisco	255.255.255.0	193.168.5.255	(unknown)	Cisco IOS Software, C8000M Software (C8000M-UNIVERSALK9-M), Version 15.5(3M), RELEASE SOFTWARE (fc1) Technical Support:	2017-08-28	2017-10-03

2. 6 アラート通知履歴

アラート通知履歴を表示します。

LogVillage2.0

ダッシュボード 資産管理 操作ログ管理 移動管理

アラート

セキュリティマニタリング

- ① 「実行」 ボタンをクリックするとアラート通知履歴が表示されます。
- ② 「自動更新」 ボタンをクリックすると別ウィンドウが表示され、指定した間隔で最新情報を自動表示します。

LogVillage2.0

admin

ダッシュボード 資産管理 操作ログ管理 移動管理 システム設定

アラート

表示範囲の設定

開始日: 2016年12月20日 (日付が"--"は月次表示)
 検索設定

絞り込み設定

グループ名: ALL

実行 自動更新

■詳細条件の設定

さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

・表示期間の設定

①終了日

開始日と合わせて範囲指定することが可能です。

②一日毎の時間帯指定

特定の時間に絞り込んで結果を出力することが可能です。

③曜日指定

特定の曜日に絞り込んで結果を出力することが可能です。

・絞り込み条件

④コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。
(部分一致可)

⑤アラートポリシーを指定

アラートポリシーでの絞り込みが可能です。

- ・禁止サイトへの Web アクセス
- ・禁止印刷ファイル・枚数制限
- ・禁止アカウントでのログオン
- ・禁止デバイスの接続
- ・指定イベントログの発生
- ・サービスの検知
- ・プロセスの検知
- ・ウイルス対策ソフトの未更新
- ・アプリケーション・インストールの検知
- ・PC リソースのしきい値超過

⑥アラートメッセージのキーワード指定

■ 出力結果

アラート通知履歴				
◀前日 2008/03/31 翌日▶			CSVダウンロード	印刷
日付▼	グループ名▼	コンピュータ名▼	アラート種別▼	アラート内容▼
2008-03-31 08:23:35	ALL	ishikawa	禁止印刷ファイル/枚数制限	2008/03/31 08:23:35 ALLの月額累積枚数が1を超えました。23枚
2008-03-31 08:24:33	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:24:33 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:34:20	ALL	ishikawa	禁止印刷ファイル/枚数制限	2008/03/31 08:34:20 ALLの月額累積枚数が1を超えました。23枚
2008-03-31 08:35:13	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:35:13 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:38:10	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:38:10 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:41:07	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:41:07 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:44:08	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:44:08 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:47:07	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:47:07 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:50:06	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:50:06 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:53:10	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:53:10 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:56:11	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:56:11 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 08:59:09	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 08:59:09 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 09:02:08	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 09:02:08 vm-winxpメモリ残容量が100MBを下回っています。
2008-03-31 09:05:08	ALL	vm-winxp	PCリソースのしきい値超過	2008/03/31 09:05:08 vm-winxpメモリ残容量が100MBを下回っています。

■CSV ダウンロード

条件設定を行った内容が CSV でダウンロード可能です。

```
開始日,2008-03-31
終了日,--
一日毎の時間指定,:~:
曜日指定,
グループ名を指定,ALL
コンピュータ名を指定,
アラートポリシーを指定,
アラートメッセージのキーワードを指定,
日付,グループ名,コンピュータ名,アラート種別,アラート内容
"2008-03-31 08:23:35",ALL,ishikawa,禁止印刷ファイル/枚数制限,
"2008/03/31 08:23:35 ALLの月額累積枚数が1を超えました。

23枚"
"2008-03-31 08:24:33",ALL,vm-winxp,"PCリソースのしきい値超過",
"2008/03/31 08:24:33 vm-winxpメモリ残容量が100MBを下回っています。"
"2008-03-31 08:34:20",ALL,ishikawa,禁止印刷ファイル/枚数制限,
"2008/03/31 08:34:20 ALLの月額累積枚数が1を超えました。

23枚"
"2008-03-31 08:35:13",ALL,vm-winxp,"PCリソースのしきい値超過",
"2008/03/31 08:35:13 vm-winxpメモリ残容量が100MBを下回っています。"
:
:
```

■印刷

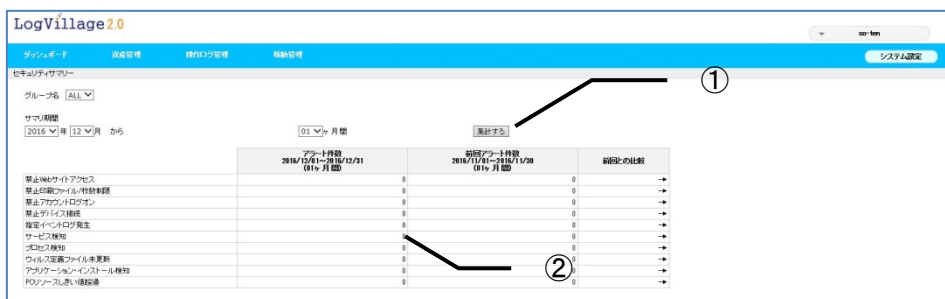
画面の内容が印刷されます。

2. 7 セキュリティサマリ

指定した期間のアラート通知履歴の集計の比較を表示します。

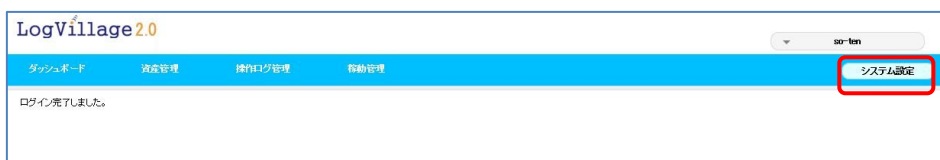


- ① 「集計する」ボタンをクリックすると指定された期間の集計と前回の比較が表示されます。
- ② アラートの数値をクリックすると該当アラートの詳細表示に移動します。



3. システム設定

システム設定では、各種ログ取得の設定や管理対象 PC の設定を行うことができます。
画面右上のシステム設定をクリックします。



システム設定をクリックしたら表示されるプルダウンメニューより目的の設定項目を選択します。



メニュー系統図

*** 初期設定が必須な設定

** その機能を使用する場合は設定が必要なもの



3. 1 共通設定

3. 1. 1 ポーリングサーバ

LogVillage マネージャに接続しているポーリングサーバを確認・設定します。
接続されているポーリングサーバが表示されます。

- ・ ポーリングサーバ名
- ・ ポーリングサーバのバージョン
- ・ 最終ログ取得日時
 - ポーリングサーバよりログを受け取った日時が示されます。
- ・ ステータス
 - 承認済 マネージャサーバより認識され、管理対象 PC の割り当て待ちです。
 - 接続許可待ち ポーリングサーバが承認待ちです。

ポーリングサーバの設定とステータス

ポーリングサーバの接続許可、削除、ステータス変更を行います。
また、各ポーリングサーバの稼働状況も確認できます。

①

設定内容の検索

②

ポーリングサーバ名 (部分一致)

ステータス

検索

検索された設定内容

ポーリングサーバ名▼	バージョン▼	最終ログ取得日時▼	ステータス▼
<input type="checkbox"/> h-test-new	2.1.1.45	2009-11-12 14:45:09	承認済み

③

チェックしたポーリングサーバの

ポーリングサーバの登録を削除する前に、削除するポーリングサーバに所属する管理対象PCを手動で他のポーリングサーバに群分けするか、ポーリングサーバを先にアンインストールしてください。

・ 設定内容の検索

①ポーリングサーバ名

特定のサーバに絞り込んで結果を出力することが可能です。
(部分一致可)

②ステータス

特定のステータスで絞り込んで結果を出力することが可能です。

- ・ 稼働中
- ・ 接続許可待ち

③ポーリングサーバー名をクリックするとポーリングサーバーの詳細を確認できます。

ポーリングサーバー詳細

[ポーリングサーバーの設定とステータス](#)

サーバー情報

ポーリングサーバー名	lv-test-new
バージョン	2.1.1.45
Macアドレス	00-0c-29-b4-71-bc
IPアドレス	192.168.5.60
ステータス	承認済み

ログ収集モジュール名	バージョン	最終ログ取得日時
WM情報	2.1.1.45	2009-11-12 12:52:44
ウイルスパターン情報	2.1.1.45	2009-11-12 12:50:20
アプリケーション情報	2.1.1.45	2009-11-12 13:52:10
デバイス情報	2.1.1.45	2009-11-12 14:50:07
イベントログ情報	2.1.1.45	2009-11-12 14:50:15
クライアントPC起動情報	2.1.1.45	2009-11-12 14:50:43
パフォーマンス・プロセス情報	2.1.1.45	2009-11-12 14:50:25
サービス情報	2.1.1.45	2009-11-12 14:50:18
Webアクセス履歴情報	2.1.1.45	2009-11-12 14:50:21

メールサーバー設定情報

SMTPサーバ	
ポート	
送信元メールアドレス	
POPサーバ名 (POPBeforeSMTP)	
POPポート	
POPユーザー	

[アラート通知メールサーバー設定](#)

・メールサーバーの情報を設定する

アラートメール送信時に利用する送信メールサーバー情報を設定します。

アラート通知メールサーバー設定

[ポーリングサーバーの設定とステータス](#) | [ポーリングサーバー詳細](#)

ポーリングサーバー名	lv-test-new	①
SMTPサーバ		②
ポート	25	③
送信元メールアドレス		④

☐ POPBeforeSMTPを使用する

POPサーバ名 (POPBeforeSMTP)		⑤
POPポート	110	⑥
POPユーザー		⑦
POPパスワード		⑧
POPパスワード確認		⑨

①ポーリングサーバー名

②SMTP サーバー名

SMTP サーバー名を入力します。(IP アドレスでも可)

③ポート

SMTP で使用するポート番号を入力します。

④送信元メールアドレス

Copyright © 2003-2021 SO-TEN, Inc. All Rights Reserved.

アラートメールの送信者となるメールアドレスを入力します。

※POP Before SMTP を使用する場合

⑤POP サーバー名 (POP Before SMTP)

POP サーバー名を入力します。(IP アドレスでも可)

⑥POP ポート

POP で使用するポート番号を入力します。

⑦POP ユーザー

POP ユーザー名を入力します。

⑧POP パスワード

POP パスワードを入力します。

⑨POP パスワード確認

確認のため POP パスワードを入力します。

3. 1. 2 グループ

グループの登録、変更、削除を行ないます。

- ・ ALL

初期状態の第一レイヤーグループです。グループの設定を行わない場合は全て全体グループに属します。

- ・ 階層構造

階層構造を持たせることができます。階層は 30 までとなります。

- ・ グループの権限

LogVillage ユーザーをどこに所属させるかでグループ階層構造における権限の設定が可能です。

第一レイヤーグループ（ALL）の権限を持つユーザーは全体設定とグループ毎の設定を行なうことができ、下層グループ（第一レイヤーグループ以外のグループすべて）の権限を持つユーザーは自分が属するグループと下位グループの設定を行なうことができます。

- ・ グループ毎の設定

下位グループの設定が存在しない場合は、上位グループの設定が反映されます。上位グループで行われた設定の変更・削除することは不可能です。

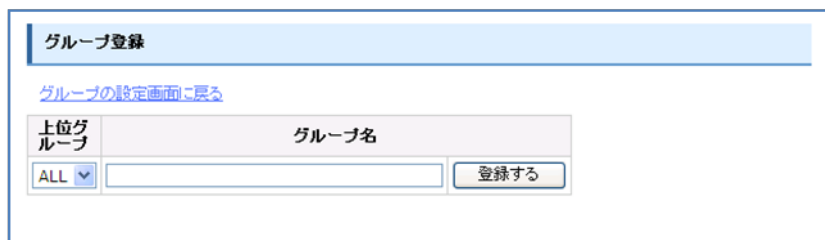
グループ毎のアラートメールの送信先が設定可能です。

また、送信先の複数登録が可能です。



- ・登録

「グループの新規追加」をクリックします。上位となるグループの選択を行い、グループ名を入力し「登録する」ボタンをクリックします。選択した上位グループの下位に新規グループが配置されます。



上位グループ	グループ名
ALL ▼	<input type="text"/>

登録する

- ・編集

グループ名をクリックするとグループ名、階層を変更できます。

- ・削除

削除したいグループをチェックし、「削除する」ボタンをクリックしてください。

3. 1. 3 管理対象 PC

管理対象 PC の登録、削除、管理、ステータスの設定を行ないます。

管理対象 PC の登録は、手動登録、自動設定ツール（Windows 用）、csv によるインポートで行なうことができます。

1) 手動登録

“管理対象 PC の新規登録” をクリックし、「管理対象 PC の新規登録・編集」画面を開きます。

必要な情報を入力します。

[< 管理対象PC](#)

アクセス名

アカウント名

パスワード

パスワード
(確認用)

OS 種別

☒Windows
☐macOS
☐Linux
☐その他

秘密鍵のパス

☐ 秘密鍵ファイルのチェック

グループ名

ALL ▼

所属するホーリングサーバ (PS) 名

ステータス

稼動 ▼

最終検出日時

設定する

項目名	必須/任意	
アクセス名	必須	<ul style="list-style-type: none"> ・コンピュータ名または IP アドレス ※固定 IP の場合のみ IP アドレスでの登録が可能
アカウント名	必須	<ul style="list-style-type: none"> ・管理対象 PC の管理者権限アカウント ※登録するアカウント名の詳細は、本項の“4) エージェントレス収集のためのアカウント要件”をご参照ください。
パスワード	必須	<ul style="list-style-type: none"> ・(OS 種別が Windows の場合) アカウント名のパスワード ・(OS 種別が macOS、Linux の場合) ○パスワード認証: アカウント名のパスワード ○SSH 公開鍵認証: 秘密鍵パスフレーズ ※秘密鍵パスフレーズが未設定の場合は空白可能
OS 種別	必須	<ul style="list-style-type: none"> ・管理対象 PC の OS 種別を選択
秘密鍵のパス	任意	<ul style="list-style-type: none"> ・OS 種別が macOS、Linux の場合のみ入力可能 ・管理対象 PC の認証方式が SSH 公開鍵認証に場合に秘密鍵のフルパスを入力 ・空白の場合、パスワード認証となります
秘密鍵ファイルのチェック	任意	<ul style="list-style-type: none"> ・チェックオンの場合、設定登録時に「秘密鍵のパス」に記述された秘密鍵ファイルの存在チェックを行います。

		※存在チェックは、LogVillage マネージャから行いますが、ログ取得時はポーリングサーバから登録された「秘密鍵のパス」の秘密鍵ファイルを使用して SSH 公開鍵認証が実行されます。 ポーリングサーバからのみアクセス可能な場所に秘密鍵ファイルが保管されている場合は、本チェックでエラーとなるためチェックオフにしてください。
グループ名	必須	・ 管理対象 PC に割り当てるグループ名を選択
所属するポーリングサーバ名	必須	・ エージェントレス方式でログ情報を収集するポーリングサーバを選択
ステータス	必須	・ 稼働：ログ取得を実行、停止：ログ取得を停止

2) 自動設定ツール(オプション)による登録(windows のみ)

別冊の「LogVillage2.0 導入マニュアル」の“管理対象 PC 自動設定ツール (オプション)”の項をご参照ください。

3) csv によるインポート

カンマ区切りの csv ファイルのインポートを行ないます。

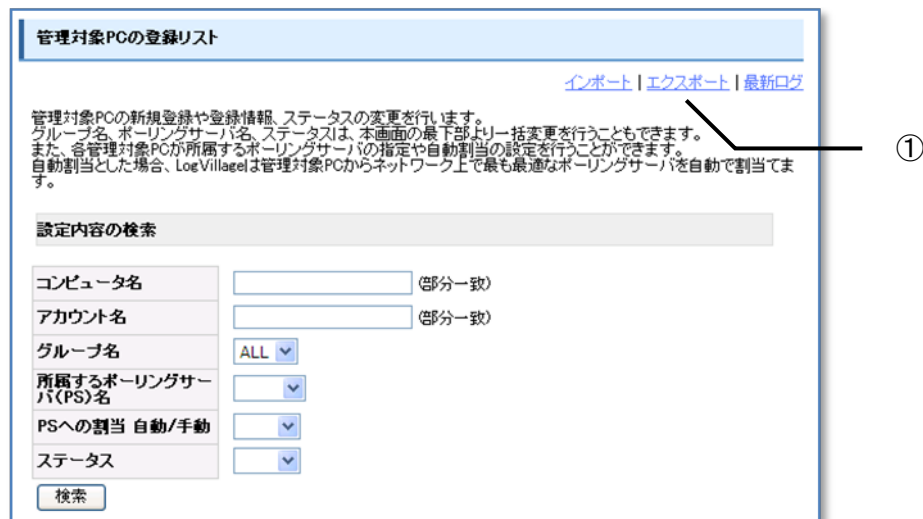
<CSV ファイル仕様>

前提条件	
文字コード	Shift-JIS
改行コード	CRLF
レイアウト	<ul style="list-style-type: none"> ・ファイルの1行目はヘッダ行とし項目名を入力する。 ・各項目は「,」で区切る。

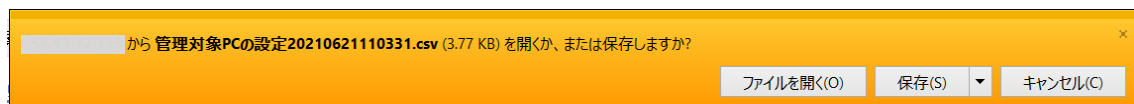
ファイル項目			
項目名	文字種/形式	必須/任意	記述法など
アクセス名	半角英数記号	必須	コンピュータ名 または IP アドレス
ユーザー名	半角英数記号	必須	
パスワード	半角英数記号	必須	
グループ名	半全角英数字記号	必須	グループ未作成の場合は “ALL”を入力
ポーリングサーバー名	半角英数記号	必須	
ID	入力不要		
OS 種別	半角数字	必須	1:Windows 2:macOS 3:Linux
秘密鍵のパス	全角・半角英数記号	任意	秘密鍵ファイルのフルパスを 記述。 C:¥ssh¥server.pem ※インポート時に秘密鍵ファ イルの存在チェックは行わ れません

※ポーリングサーバー名の不一致、アクセス名重複の場合はエラーとなります。

- ① ひな型となる CSV ファイルをダウンロードするため、エクスポートをクリックします。



- ② 「ファイルのダウンロード」ダイアログが表示されますので [保存] をクリックします。
その後、保存場所を指定し CSV ファイルを保存します。



- ③②で保存した CSV ファイルを開きます。

- ・グループを変更する場合：
各コンピュータ名の行のグループ名を変更します。
 - ・管理対象 PC を新規登録する場合：
最後の行の後に、コンピュータ名、ユーザー名、パスワード、グループ名、所属するポーリングサーバ名を入力します。
- *1 新しいグループ名を登録する場合、インポートを行う前に必ず「グループの設定」画面より、新しいグループの登録を行っておいてください。
グループの登録が行われていないグループ名や間違ったグループ名（カタカナの全角/半角、スペースの有無、等）を CSV ファイルに入力し、インポートを行うと“コンピュータ名「xxxxx」：グループ名「xxxxxxxx」が登録されていません。”とエラー表示され、該当管理対象 PC のグループ名を変更することができませんのでご注意ください。
- *2 グループ変更を行うコンピュータ名だけの CSV ファイルを作成することでも、インポートによる一括変更が可能です。
- *3 新規登録 PC だけの CSV ファイルを作成することでも、インポートにより一括登録が可能です。

- ④ インポート用 CSV ファイルを分割します。

一度に、インポートが行える CSV ファイルの行数は 300 行までです。

③で作成した CSV ファイルが 300 行（300 台）を超える場合、300 行以内の複数ファイルに分割を行ってください。

- ⑤ [インポート] をクリックします。

管理対象PCの登録リスト

[インポート](#) | [エクスポート](#) | [最新ログ](#)

管理対象PCの新規登録や登録情報、ステータスの変更を行います。
グループ名、ボーリングサーバ名、ステータスは、本画面の最下部より一括変更を行うこともできます。
また、各管理対象PCが所属するボーリングサーバの指定や自動割当の設定を行うことができます。
自動割当とした場合、LogVillageは管理対象PCからネットワーク上で最も最適なボーリングサーバを自動で割当てます。

設定内容の検索

コンピュータ名	<input type="text"/>	(部分一致)
アカウント名	<input type="text"/>	(部分一致)
グループ名	ALL ▼	
所属するボーリングサーバ(PS)名	▼	
PSへの割当 自動/手動	▼	
ステータス	▼	

- ⑥ [参照] をクリックし、インポート用 CSV ファイルを指定します。

管理対象PCのIDはインポート時に自動発番されます(CSVの値は破棄されます)。
1回の操作での取り込み可能な台数は300台までとなります。

CSVファイル:

- ⑦ [実行] をクリックし、インポートを開始します。

※未登録なグループ名が存在した場合、エラーメッセージが表示されます。

- ⑧ インポートが完了すると、「管理対象 PC の設定」画面に自動遷移します。

4) エージェントレス収集のためのアカウント要件

No.	OS 種別	アカウント要件	備考
1	Windows	アカウントの種類が「管理者」 (Administrators グループ) であること	ローカルユーザーの場合
2		Domain Admins グループに属していること	ActiveDirectory ドメインユーザーの場合
3	macOS	以下のコマンドの実行権限を持つアカウント であること。 ・ uname ・ system_profiler ・ sw_vers ・ getconf LONG_BIT	ユーザータイプが管理者となっているアカウント
4	Linux	sudo 権限を持つアカウントであること	メーカー名、型番、シリアルナンバー、マザーボード UUID 情報を収集するコマンド実行に必要な ・ /etc/sudoers に visudo で以下を追加 [アカウント名 *1] ALL=(ALL) NOPASSWD: ALL *1 LogVillage に登録する当該 Linux 機へのアクセス アカウント名
5		以下のコマンドの実行権限を持つアカウント であること。 ・ hostname ・ domainname ・ cat ・ ls ・ dmi decode ・ grep ・ egrep ・ getconf ・ lsblk ・ df ・ lspci ・ udevadm ・ ifconfig ・ repoquery (Fedora 以外) ・ rpm (Fedora のみ) ・ dpkg-query (Ubuntu のみ)	World Executable であればアカウントは不問

5) 管理対象 PC の検索

管理用 PC 一覧の絞り込みが可能です。

管理対象PCの登録リスト

[インポート](#) | [エクスポート](#) | [最新ログ](#)

管理対象PCの新規登録や登録情報、ステータスの変更を行います。
グループ名、ポーリングサーバ名、ステータスは、本画面の最下部より一括変更を行うこともできます。
また、各管理対象PCが所属するポーリングサーバの指定や自動割当の設定を行うことができます。
自動割当とした場合、LogVillageは管理対象PCからネットワーク上で最も最適なポーリングサーバを自動で割当てます。

設定内容の検索

コンピュータ名	<input type="text"/> (部分一致)	①
アカウント名	<input type="text"/> (部分一致)	②
グループ名	ALL ▾	③
所属するポーリングサーバ(PS)名	<input type="text"/> ▾	④
PSへの割当 自動/手動	<input type="text"/> ▾	⑤
ステータス	<input type="text"/> ▾	⑥

・絞り込み条件

① コンピュータ名を指定

特定のコンピュータに絞り込んで結果を出力することが可能です。

(部分一致可)

② アカウント名を指定

特定のログオンアカウント名に絞り込んで結果を出力することが可能です。

(部分一致可)

③ グループ名を指定

プルダウンでグループ名を選択します。

④ 所属するポーリングサーバ (PS) 名を指定

プルダウンでポーリングサーバ名を選択します。

⑤ ステータスを指定

プルダウンでステータスを選択します。

6) 変更・削除

検索された設定内容

[管理対象PCの新規登録](#)

コンピュータ名▼	アカウント名▼	グループ名▼	所属するポーリングサーバ(PS)名▼	PSへの割当 自動/手動	ステータス▼	最終検出日時▼
<input type="button" value="全てをチェック"/>						
<input type="checkbox"/> Vista-PC2	so-ten	ALL	LV-P	自動	移動	
<input type="checkbox"/> vm-winxp	administrator	ALL	LV-P	自動	移動	2008-03-31 20:44:40
<input type="checkbox"/> w2kwork	administrator	ALL	LV-P	自動	移動	2008-04-02 16:47:07
<input type="checkbox"/> ishikawa	k-ishikawa	ALL	LV-P	自動	移動	2008-04-02 16:47:09
<input type="checkbox"/> win2003- default	administrator	ALL	LV-P	自動	移動	2008-04-02 16:47:44
<input type="button" value="全てをチェック"/>						

チェックした管理対象PCを

[管理対象PCの新規登録](#)

一括設定 チェックした管理対象PCに対して一括更新

グループ 所属するポーリングサーバ(PS) ステータス
名 名 入

・ 変更

コンピュータ名をクリックすると管理対象 PC のコンピュータ名、ユーザー名、パスワード、グループ名、ポーリングサーバ名、ステータスを変更できます。

・ 削除

削除したい管理対象 PC をチェックし、「削除する」ボタンをクリックしてください。

7) 登録した管理対象 PC の接続確認

登録した管理対象 PC が、正常に LogVillage より接続（ログ取得）可能かを確認することができます。

管理対象 PC の設定後、以下の手順をご参照のうえ、接続確認を行って下さい。

- ・ ポーリングサーバから管理対象 PC への接続確認の実行手順

<https://www.so-ten.co.jp/products/logvillage/pc-connection-check>

- ・ 管理対象 PC への接続確認結果の対処法

<https://www.so-ten.co.jp/products/logvillage/pc-connection-result>

3. 1. 4 トップ画面

LogVillage のログイン画面でメッセージを表示することができます。
表示設定に文字列を入力し、変更ボタンをクリックしてください。

The screenshot shows a web-based configuration window titled "トップ画面へのメッセージ表示設定" (Message Display Setting for Top Screen). Inside the window, there is a text area for inputting a message, followed by a "変更する" (Change) button. The text area contains the following instruction: "トップ画面へ表示するLogVillageユーザーへのメッセージ設定を行います。表示するメッセージを入力後、[変更する]ボタンをクリックして下さい。" (Set the message to be displayed on the top screen for LogVillage users. After inputting the message to be displayed, click the [Change] button.)

トップ画面へのメッセージ表示設定

トップ画面へ表示するLogVillageユーザーへのメッセージ設定を行います。
表示するメッセージを入力後、[変更する]ボタンをクリックして下さい。

変更する

3. 1. 5 WindowsUpdate 情報

管理対象 PC の WindowsUpdate 情報を設定します。

■手動登録

必要な情報をすべて手入力します。

WindowsUpdate情報の登録

WindowsUpdate情報の登録リスト

※種別を複数入力する場合は「|」で区切ってください

文書番号

内容

種別

登録する

- ①文書番号 例) 931212
- ②内容 例) (MS07-040) .NET Framework の脆弱性により、リモートでコードが実行される
- ③種別 例) Windows XP Professional Service Pack 2;Windows XP Professional x64 Edition

④必要事項の入力後「登録する」ボタンをクリックします。

■csv によるインポート

カンマ区切りの csv ファイルのインポートを行ないます。

WindowsUpdate の設定ファイルは定期的に蒼天のホームページにアップしています。
下記 URL よりアクセスしてください。

<http://www.so-ten.co.jp/user/update/>

- ①上記リンク先で最新の WindowsUpdate 情報のご案内を確認してください。配布している WindowsUpdate 設定ファイルのリンク上で右クリックし、ポップアップメニューより「対象をファイルに保存」を選択します。
- ②LogVillage 画面上の「インポート」をクリックします。

②

WindowsUpdate情報の登録リスト

[インポート](#) | [エクスポート](#)

WindowsUpdate情報の登録、変更、削除を行います。
 (株)蒼天よりご提供するWindowsUpdateの最新情報をインポートすることにより最新の情報を登録することが出来ます。

設定内容の検索

WindowsUpdateの種類別 (部分一致)

WindowsUpdateの文書番号 (部分一致)

WindowsUpdateの内容 (部分一致)

検索された設定内容

③ダウンロードしたファイルを指定し、「実行」をクリックします。

③

CSVファイル: [参照...](#)

※取り込まれた WindowsUpdate 情報

<input type="checkbox"/>	887219	(MS05-004) ASP.NET バス検証の脆弱性	Windows 2000 Service Pack 3 Windows 2000 Service Pack 4 Windows Server 2003 Windows Server 2003 for Itanium-based Systems Windows Server 2003 Service Pack 1 Windows Server 2003 Service Pack 2 Windows Server 2003 with SP1 for Itanium-based Systems Windows Server 2003 with SP2 for Itanium-based Systems Windows Server 2003 x64 Edition Windows Server 2003 x64 Edition Service Pack 2 Windows Vista Windows XP Media Center Edition Windows XP Professional x64 Edition Windows XP Professional x64 Edition Service Pack 2 Windows XP Service Pack 1 Windows XP Service Pack 2 Windows XP Tablet PC Edition
<input type="checkbox"/>	889167	(MS06-010) PowerPoint 2000 の脆弱性により、情報漏えい が起る可能性がある	Windows Server 2003 Service Pack 1 Windows Server 2003 Windows Server 2003 with SP1 for Itanium-based Systems Windows Server 2003 for Itanium-based Systems Windows Server 2003 x64 Edition Windows XP Service Pack 2 Windows XP Service Pack 1 Windows XP Professional x64 Edition

WindowsUpdate情報の登録リスト

[インポート](#) | [エクスポート](#)

WindowsUpdate情報の登録、変更、削除を行います。
 (株)蒼天よりご提供するWindowsUpdateの最新情報をインポートすることにより最新の情報を登録することが出来ます。

設定内容の検索

WindowsUpdateの種類別 (部分一致) ①

WindowsUpdateの文書番号 (部分一致) ②

WindowsUpdateの内容 (部分一致)

③

検索された設定内容

■設定内容の検索

①WindowsUpdate の種別

特定の WindowsUpdate の種別に絞り込んで結果を出力することが可能です。
(部分一致可)

②WindowsUpdate の文書番号

特定の WindowsUpdate の文書番号に絞り込んで結果を出力することが可能です。
(部分一致可)

③WindowsUpdate の内容

特定の WindowsUpdate の内容に絞り込んで結果を出力することが可能です。
(部分一致可)

■変更・削除

・変更

文書番号をクリックすると文書番号、内容、種別が変更可能です。
※種別を複数入力する場合は「;」で区切ってください

Windows Update情報の設定

[Windows Update情報の登録リスト](#)

※種別を複数入力する場合は「;」で区切ってください

文書番号	947890
内容	((MS08-008) OLEオートメーションの脆弱性により、リモート
種別	Microsoft Office 2004 for Mac; Microsoft Visual Basic

・削除

削除したい文書番号をチェックし、「削除する」ボタンをクリックします。

<input type="checkbox"/>	947890	((MS08-008) OLEオートメーションの脆弱性により、リモートでコードが実行される	Windows Server 2003 Service Pack 2 Windows Server 2003 with SP1 for Itanium-based Systems Windows Server 2003 with SP2 for Itanium-based Systems Windows Server 2003 x64 Edition Windows Server 2003 x64 Edition Service Pack 2 Windows Vista Windows Vista x64 Edition Windows XP Professional x64 Edition Windows XP Professional x64 Edition Service Pack 2 Windows XP Service Pack 2
--------------------------	--------	---	---

チェックしたWindows Updateを

[Windows Updateの新規追加](#)

3. 1. 6 ウィルス対策ソフト定義ファイル

ウィルス対策ソフト/定義ファイルの保存場所を設定します。
設定することによって更新状況が確認可能です。

※おもなウィルス対策ソフトウェアについては定義ファイルの保存フォルダパスを設定済みです。
お使いのウィルス対策ソフトウェアの定義ファイルの保存フォルダパスを設定してください。

ウィルス対策ソフト/定義ファイル保存場所の設定

ウィルス対策ソフト/定義ファイル保存場所の登録、変更、削除を行います。

設定内容の検索

①

ウィルス対策ソフト名 (部分一致)

検索

検索された設定内容

ウィルス対策ソフト名	定義ファイルのフォルダパス	
<input type="checkbox"/> McAfee SecurityCenter	C:\Program Files\McAfee\VirusScan\DAT\	使用する
<input type="checkbox"/> カスベルスキー	C:\Documents and Settings\All Users\Ap	使用する
<input type="checkbox"/> ウィルスバスター Corp	C:\Program Files\Trend Micro\OfficeScan	使用する
<input type="checkbox"/> NOD32	C:\Program Files\Eset\updfiles	使用する
<input type="checkbox"/> Norton AntiVirus	C:\Program Files\Common Files\Symante	使用する
<input type="checkbox"/> ウィルスバスター-2008	C:\Program Files\Trend Micro\Virus Bust	使用する

チェックしたものを 削除する 変更する ④

② ③ 追加する

■設定内容の検索

①ウィルス対策ソフト名

特定のウィルス対策ソフトに絞り込んで結果を出力することが可能です。(部分一致可)

■追加

②ウィルス対策ソフト名

任意のウィルス対策ソフト名を入力します。

③定義ファイルの保存フォルダパス

定義ファイルの保存フォルダパスを入力します。

④「追加する」をクリックします。

■変更・削除

・変更

変更する内容を直接入力し、変更したい行にチェックを入れ、「変更する」ボタンをクリックします。

Copyright © 2003-2021 SO-TEN, Inc. All Rights Reserved.

・削除

削除したい行にチェックを入れ、「削除する」ボタンをクリックします。

■使用する・使用しない

設定した定義ファイルを使用するかしないか選択可能です。

3. 1. 7 プロセス名辞書

Logvillage は管理対象 PC のプロセス情報とインストールされているアプリケーション情報をそれぞれ取得することができますが、どのアプリケーションがどのプロセスか、という情報は保持していません。

したがって、プロセスの、プロセス稼働時間、システム管理画面のプロセス・アプリケーション登録やアラートリストにおいて、どのようなアプリケーションか把握するにはプロセス名とアプリケーション名を結びつける設定が必要になります。

この辞書は、稼働管理→パフォーマンスログ→プロセスの CPU 利用率画面の絞込み設定→詳細設定の中に、アプリケーション名指定にて使用されます

設定はすべての PC に適用されます。登録方法は、手動での登録と、インポートによる登録の 2 種類があります。

■追加（手動での登録）

- ①アプリケーション名を直接入力します。
- ②「追加する」をクリックします。

※アプリケーション名を一覧より選択する場合

- ③「ソフトウェア一覧よりアプリケーション名を選択して追加する」をクリックします。

ソフトウェア一覧

[プロセス名録書の設定画面へ戻る](#)

アプリケーション名

検索

- ☐ ACCESS HELP
- ☐ ADOBE READER 8.1.2 - JAPANESE
- ☐ APACHE HTTP SERVER 2.2.4
- ☐ ARIEL MULTISCHEDULER
- ☐ BROADCOM RABBIT INTEGRATED CONTROLLER
- ☒ CANNON PDI/LS IP7100
- ☐ CLIENT SECURITY SOLUTION
- ☐ CONEXANT HD AUDIO
- ☐ CUTEPDF WRITER 2.7
- ☐ DISKEEPER LITE
- ☐ DNSキャッシュ FOR AIR-EDGE
- ☐ GETPLUS(R)_OCX
- ☐ GOOGLE TOOLBAR FOR INTERNET EXPLORER
- ☐ GTONECARE

④

- ④アプリケーション名を選択し「追加ボタン」をクリックします。
- ⑤プロセス名を入力します。
- ⑥「追加する」をクリックします。

※プロセス名を一覧より選択する場合

- ⑦「プロセスリストから追加する」をクリックします。

プロセス名の設定

[プロセス名録畫の設定画面へ戻る](#)

アプリケーション名 ADOBE READER 812 - JAPANESE ⑤

登録済みプロセス 設定データはありません ⑥

新規登録

プロセス名 [プロセスリストから追加する](#) ⑦

- ⑧プロセス名を選択し、「追加ボタン」をクリックします。

プロセス一覧

[プロセス名辞書の設定画面へ戻る](#)
[プロセスの設定画面へ戻る](#)

アプリケーション名 SKYPE? 3.6

プロセス名	
<input type="text"/>	<input type="button" value="検索"/>
<input type="button" value="全てをチェック"/>	
<input type="checkbox"/>	OUTLOOK
<input type="checkbox"/>	RDPCLIP
<input type="checkbox"/>	READER_SL
<input type="checkbox"/>	REGSRVC
<input type="checkbox"/>	REGSVC

■ファイルをインポートする場合

すでにあるアプリケーション名とプロセス名が関連付けられたファイルをインポートすることができます。

①ファイルの準備をします。

CSV 形式

アプリケーション名, プロセス名

例)

"SKYPE 3.6", SKYPE

"SKYPE 3.6", SKYPEPM

②「インポート」をクリックします。

③ファイルのパスを指定します。

④「実行」をクリックします。

プロセス名辞書の設定(アプリケーション名→プロセス名辞書)

CSVファイル: 参照...

実行 キャンセル

■絞り込み検索

設定内容の検索

アプリケーション名 (部分一致)

プロセス名 (部分一致)

検索

①アプリケーション名

特定のアプリケーション名に絞り込んで結果を出力することが可能です。(部分一致可)

②プロセス名

特定のプロセス名に絞り込んで結果を出力することが可能です。
(部分一致可)

3. 1. 8 拡張項目名（資産管理）

資産管理の追加項目の設定と HDD 残容量警告値の設定を行います。

ハードディスクの残容量警告値の設定

ハードディスクの残容量警告値の設定を行います。
空白の場合は残容量のチェックを行いません。

ハードディスクの残容量警告値の設定

管理対象PCのハードディスク残容量が %以下になれば、ハードウェア台帳に警告を表示する

パーセンテージを入力して「設定する」をクリックします。

ハードウェア台帳の拡張項目の設定

ハードウェア台帳の拡張項目の設定を行います。
LogVillage の PC 資産情報は、WMI 情報より取得しています。WMI 情報以外の項目（例・リース期限、利用者名など）を管理する場合に使用します。任意の項目を登録してください。

ハードウェア台帳の拡張項目の設定

拡張項目名	ハードウェア詳細情報に追加	ハードウェア台帳に追加
<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
LogVillage拡張項目	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

① ② ③

■ 追加

- ① 拡張項目名を入力します。
- ② ハードウェア詳細情報に追加します。
- ③ ハードウェア台帳に追加します。
- ④ 拡張項目名の「追加する」ボタンをクリックします。

■ 変更・削除

・ 変更

該当する項目を変更してその行の「設定する」ボタンをクリックします。

・ 削除

該当する行の「削除する」ボタンをクリックします。

3. 1. 9 ネットワークスキャン設定

ネットワークスキャンの実行条件を設定します。

① ネットワークスキャンを実行する IP アドレスの範囲を設定します。

例) 192.168.5.1~192.168.5.100
192.168.5.1~192.168.6.255

② 実行する曜日を選択します。

③ 開始時刻を設定します。

ここで設定した開始時刻にネットワークスキャンが開始され、その後は次に設定するスキャン実行間隔毎にネットワークスキャンが実行されます。

④ スキャン実行間隔を設定します。

ここで設定した時間の間隔でネットワークスキャンが実行されます。

⑤ 複数の IP アドレス範囲を設定する場合に[+] ボタンをクリックすると 1 行追加されます。

⑥ [設定] をクリックすると設定が保存されます。

3. 1. 10 ネットワークスキャンアラート設定

ネットワークスキャンにて新たに検出されたノード、検出されなくなったノードがあった場合にアラートメールを送信する設定を行います。

本設定はポーリングサーバ単位の設定となります。

【ご注意ください】

事前に、「ポーリングサーバ」設定にて「アラート通知メールサーバ設定」が必要です。

①設定するポーリングサーバ名を選択し[追加する]をクリックします。
以下のアラート条件設定画面に遷移します。

②アラートを発信する条件を選択します。（複数選択可）

- ・新規検出ノード：新たなノードを検出したばあいアラートが発信されます。
- ・検出されなくなったノード：ネットワークスキャンで検出されていたノードの中で検出が行えなくなったノードがあった場合にアラート送信されます。

③アラートメールの送信先を設定します。

「; (セミicolon)」で区切ると複数メールアドレスを設定可能です。

④アラートメールのタイトル（件名）を設定します。

⑤アラートメールを送信する曜日を設定します。

⑥アラートメールの送信時刻を設定します。

アラートは、前回アラート送信から今回のアラート送信までの間で、アラート条件に合致するイベントがあればアラート発信されます。

⑦[設定する]をクリックすると設定が保存されます。

3. 2 グループ単位設定

3. 2. 1 LogVillage ユーザー

LogVillage を利用するユーザーの設定を行います。

一番最初に登録するユーザーはすべての権限をもつユーザーとなります。このユーザーの登録を行った時点で、初期管理者である so-ten（パスワード：so-ten）は利用できなくなります。

ユーザー登録時にアクセス権限を設定し、ユーザーは与えられた権限の機能を使用することができます。ただし、現在ログインしている LogVillage ユーザーが所属するグループおよびその下位グループとなります。グループが「第一レイヤー」の時のみ、「全体の共通設定」の項目を選択できます。

■設定内容の検索

①ユーザー名

特定のユーザー名に絞り込んで結果を出力することが可能です。（部分一致可）

②メールアドレス

特定のメールアドレスに絞り込んで結果を出力することが可能です。（部分一致可）

③グループ

特定の WindowsUpdate の内容に絞り込んで結果を出力することが可能です。（部分一致可）

④備考

■追加

①Logvillage 新規ユーザーの追加 をクリックします。

ユーザー情報の設定

[LogVillageユーザーの設定画面へ戻る](#)

② ユーザー名

③ パスワード

空白の場合はパスワードは変更しません

④ パスワード確認

セミコロン「;」区切りで複数登録

⑤ メールアドレス

⑥ グループ

ALL

⑦ 備考

⑧ 権限設定画面へ

- ②「ユーザー名」を入力します。
- ③「パスワード」を入力します。
- ④確認のため、もう一度「パスワード」を入力します。
- ⑤「メールアドレス」を入力します。
- ⑥グループをプルダウンメニューから選択します。
- ⑦「備考」を任意で入力します。
- ⑧「権限設定画面へ」をクリックします。

☒ プロセスの検知
☒ ウィルス対策ソフトの定義ファイル未更新
☒ アプリケーションインストールの検知
☒ PCリソースのしきい値超過
☒ 稼働モニター
☒ LogVillageへのログオン履歴
☒ LogVillageの稼働モニター
☒ 個人情報変更

⑨ 設定

⑨権限設定を変更・確認し「設定」ボタンをクリックします。

■変更

①該当ユーザー名をクリックします。

検索された設定内容

[LogVillageユーザーの新規追加](#)

ユーザー名▼	メールアドレス	グループ▼	備考▼
<input type="checkbox"/> admin	ishikawa@so-ten.co.jp	ALL	
<input type="checkbox"/> salesmgr		営業本部	
<input type="checkbox"/> salesuser		営業1部	

①

⑥

チェックしたユーザーを 削除する

- ②変更したい項目に変更値を入力します。
- ③「権限設定画面へ」をクリックします。
- ④権限設定を変更・確認し「設定」ボタンをクリックします。

■削除

- ⑤該当ユーザーにチェックを入れます。
- ⑥「削除する」ボタンをクリックします。

■権限設定画面

権限設定

[ユーザー情報の設定画面へ戻る](#)

ユーザーに操作を許可する項目にチェックを入れて下さい。

登録中のユーザー名: admin

<input checked="" type="checkbox"/> 移動管理	<input checked="" type="checkbox"/> IISシステム管理
<input checked="" type="checkbox"/> パフォーマンスログ	<input checked="" type="checkbox"/> 全体の共通設定
<input checked="" type="checkbox"/> PCリソースの移動状況	<input checked="" type="checkbox"/> ホーリングサーバの設定とステータス
<input checked="" type="checkbox"/> プロセスのCPU利用率	<input checked="" type="checkbox"/> グループの設定
<input checked="" type="checkbox"/> イベントログ	<input checked="" type="checkbox"/> 管理対象PCの設定
<input checked="" type="checkbox"/> サービス移動時間	<input checked="" type="checkbox"/> ライセンスの登録・変更
<input checked="" type="checkbox"/> プロセス移動時間	<input checked="" type="checkbox"/> トップ画面へのメッセージ表示設定
<input checked="" type="checkbox"/> セキュリティ対策更新状況	<input checked="" type="checkbox"/> イベントログフィルタ
<input checked="" type="checkbox"/> Windows Update(HOTFIX)の適用状況	<input checked="" type="checkbox"/> Windows Update情報の設定
<input checked="" type="checkbox"/> ウィルス対策ソフト定義ファイルの更新状況	<input checked="" type="checkbox"/> ウィルス対策ソフト/定義ファイル保存場所の設定
<input checked="" type="checkbox"/> アプリケーションインストール履歴	<input checked="" type="checkbox"/> プロセス名辞書の設定
<input checked="" type="checkbox"/> 資産管理	<input checked="" type="checkbox"/> 資産管理台帳の拡張項目名設定とHDD 残容量警告値の設定
<input checked="" type="checkbox"/> PC資産管理台帳	<input checked="" type="checkbox"/> NETMETRO共通画面
<input checked="" type="checkbox"/> ハードウェア台帳	<input checked="" type="checkbox"/> グループ毎の設定
<input checked="" type="checkbox"/> ソフトウェア台帳	<input checked="" type="checkbox"/> LogVillageユーザーの設定
<input checked="" type="checkbox"/> 指定アプリケーションの表示	<input checked="" type="checkbox"/> 拡張資産管理データの設定
<input checked="" type="checkbox"/> 操作管理	<input checked="" type="checkbox"/> ログ収集スケジュールの設定
<input checked="" type="checkbox"/> Webアクセス履歴	

以下の権限の設定が可能です。

設定項目		
稼働管理	パフォーマンスログ	PC リソースの稼働状況
		プロセスの CPU 利用率
	イベントログ	
	サービス稼働時間	
	プロセス稼働時間	
	セキュリティ対策更新状況	WindowsUpdate (HOTFIX) の適用状況
		ウィルス対策ソフト定義ファイルの更新状況
	アプリケーションインストール履歴	
資産管理	PC 資産管理台帳	ハードウェア台帳
		ソフトウェア台帳
	指定アプリケーションの表示	
操作管理	Web アクセス履歴	
	印刷履歴	
	ログオン・オフ履歴	
	デバイス接続履歴	
ファイル管理	ファイル更新履歴	
URL カテゴリ履歴	URL カテゴリ履歴	
アラート通知履歴	禁止サイトへの Web アクセス	
	禁止印刷ファイル/枚数制限	
	禁止アカウントでのログオン	
	禁止デバイスの接続	
	指定イベントログの発生	
	サービス検知	
	プロセスの検知	
	ウィルス対策ソフトの定義ファイル未更新	
	アプリケーション・インストールの検知	
	PC リソースのしきい値超過	
セキュリティサマリー		

設定項目		
システム設定	共通設定	ポーリングサーバー
		グループ
		管理対象 PC
		トップ画面
		WindowsUpdate 情報
		ウィルス対策ソフト定義ファイル
		プロセス名辞書
		拡張項目名（資産管理）
	グループ単位設定	LogVillage ユーザーの設定
		ログ収集スケジュール
		指定アプリケーション
		管理対象プロセス
		管理対象サービス
		管理対象フォルダ
		保有ソフトウェアライセンス
		拡張項目データ登録（資産管理）
	アラートポリシー設定	禁止 Web サイトへのアクセス
		禁止印刷ファイル/枚数制限
		禁止アカウントでのログオン
		禁止デバイスの接続
		指定イベントログの発生
		サービスの検知
		プロセスの検知
		ウィルス対策ソフトの定義ファイル未更新
		アプリケーション・インストールの検知
	運用管理	PC リソースのしきい値超過
		ライセンスの登録・変更
		LogVillage ログイン履歴
		LogVillage の稼動モニター
		ユーザー情報変更

3. 2. 2 ログ収集スケジュール

グループ毎のスケジュールの管理を行なうことができます。
どの項目をどのくらいの間隔で取るかを設定します。

ログ収集スケジュールの設定

グループ毎のログ収集スケジュールの設定を行います。
ログの種類別にログ収集スケジュールを設定することも可能です。

[スケジュールの新規登録](#)

グループ名	取得期間	取得時間	曜日指定	管理対象PC数	詳細	スケジュールの内容を変更する
<input type="checkbox"/> ALL	無期限	24時間	指定しない	5	詳細	スケジュールの内容を変更する
<input type="checkbox"/> 営業本部	無期限	24時間	指定しない	2	詳細	スケジュールの内容を変更する

チェックしたグループのスケジュールを [削除する](#) ①

[スケジュールの新規登録](#)

■追加

①スケジュールの新規追加 をクリックします。

ログ収集スケジュールの詳細設定

[ログ収集スケジュールの設定画面へ戻る](#)

グループ名 ②

取得期間 ☒ 無期限 ③

取得時間 ☒ 24時間 ④

曜日指定 ☒ 指定しない ⑤

☐ 月 ☐ 火 ☐ 水 ☐ 木 ☐ 金 ☐ 土 ☐ 日

ログの種類	ログ収集周期	直近のログ収集周期の実績
サービス	10 分	09分46秒
ウイルス定義ファイル	30 分	30分05秒
インベントリ	3 時間	02時間59分49秒
アプリケーション	3 時間	02時間59分56秒
外部記憶デバイス	10 分	09分38秒
Webアクセス履歴	10 分	10分06秒
パフォーマンス・プロセス	10 分	09分52秒
イベントログ	10 分	09分38秒
ファイル	1 時間	59分45秒

☒ 外部記憶デバイスのファイル情報を収集する。

[設定](#) ⑦

②スケジュールの所属する「グループ名」をプルダウンメニューから選択します。

③「取得期間」を入力します。

④「取得時間」を入力します。

⑤「曜日指定」を入力します。

⑥ ログの収集周期を入力します。

- ・ サービス
- ・ ウィルス定義ファイル
- ・ インベントリ
- ・ アプリケーション
- ・ 外部記憶デバイス

※外部記憶デバイスのファイル情報を収集する場合はチェックを入れます。

- ・ Web アクセス履歴
- ・ パフォーマンス・プロセス
- ・ イベントログ
- ・ ファイル

⑦ 「設定」ボタンをクリックします。

■ 変更

①該当するスケジュールの「スケジュールの内容を変更する」をクリックします。

②変更画面にて変更を行い、「設定する」ボタンをクリックします。

ログ収集スケジュールの設定

グループ毎のログ収集スケジュールの設定を行います。
ログの種類別にログ収集スケジュールを設定することも可能です。

[スケジュールの新規登録](#)

グループ名	取得期間	取得時間	曜日指定	管理対象PC数	詳細	スケジュールの内容を変更する
<input type="checkbox"/> ALL	無期限	24時間	指定しない	5	詳細	スケジュールの内容を変更する
<input type="checkbox"/> 営業本部	無期限	24時間	指定しない	2	詳細	スケジュールの内容を変更する

チェックしたグループのスケジュールを [削除する](#)

[スケジュールの新規登録](#)

■ 削除

③削除したいスケジュールにチェックを入れて「削除する」ボタンをクリックします。

■ ログ収集スケジュール関連表

ログ収集スケジュール 種別	稼働ファイル	関連レポート種別
サービス情報	05：サービス情報ファイル	稼働管理/サービス稼働時間
ウイルスパターン情報	07：パターンファイル 更新情報ファイル	稼働管理/セキュリティ対策更新状況/ ウイルス対策ソフト定義ファイルの更新状況
WMI情報	12：WMI情報ファイル	資産管理/PC資産管理台帳/ハードウェア台帳
アプリケーション情報	01：アプリケーション 情報ファイル	稼働管理/アプリケーションインストール履歴 稼働管理/セキュリティ対策更新状況/WindowsUpdate (HOTFIX) の適用状況 資産管理/PC資産管理台帳/ソフトウェア台帳
デバイス情報	02：デバイス情報ファイル	操作管理/デバイス接続履歴
Webアクセス履歴情報	11：URL履歴情報ファイル	操作管理/Webアクセス履歴
パフォーマンス・プロセス 情報	03：プロセス情報ファイル	稼働管理/パフォーマンスログ/プロセスのCPU利用率 稼働管理/プロセス稼働時間
	04：パフォーマンス情報 ファイル	稼働管理/パフォーマンスログ/PCリソースの稼働状況
イベントログ情報	08：イベントログ情報 ファイル	稼働管理/イベントログ
	09：印刷履歴情報ファイル	操作管理/印刷履歴
	10：ログオン情報ファイル	操作管理/ログオン・オフ履歴
HDDファイル情報収集	06：ファイル情報ファイル	ファイル管理/ファイル管理
—	13：アラート履歴情報 ファイル※1	アラート通知履歴
—	15：ポーリングサーバ の状態ファイル※2	システム設定/全体の共通設定/ポーリングサーバの設定 とステータス内「最終ログ取得日時」項目

※1：アラート対象となる情報が検出された際に生成される稼働ファイルとなります。

※2：PollingServer のログが規定値を超えた際に、定期的に Manager へ連絡するために生成される稼働ファイルとなります。

3. 2. 3 管理対象プロセス

プロセス稼働時間画面にて稼働時間を確認したいプロセスを登録します。

- ・設定情報はグループ毎に変更することができます。
- ・上位グループで設定されたものは変更・削除できません。

プロセス設定(プロセス稼働時間画面用)

稼働管理→プロセス稼働時間画面に表示するプロセスの設定を行います。
実際のプロセス名と画面表示用プロセス名の設定、表示するグループ名の設定を行います。

現在登録されているプロセス

グループ名	表示プロセス名	プロセス名	アプリケーション名
<input type="checkbox"/> ALL	ACRORD32	ACRORD32	
<input type="checkbox"/> ALL	FIREFOX	FIREFOX	
<input type="checkbox"/> ALL	HTTPD	HTTPD	

チェックしたプロセスを

新規に表示プロセスを登録する

☐ ALL

[プロセス稼働実績リストから選択して追加する](#)

■ 追加

- ・手動でプロセスを追加する場合

- ①所属させるグループをプルダウンメニューから選択します。(必須)
- ②「表示プロセス名」を入力します。
- ③「プロセス名」(必須)を入力します。
- ④「アプリケーション名」を入力します。

- ・プロセス稼働実績リストから選択して追加する場合(推奨)

- ⑤「プロセス稼働実績リストから選択して追加する」をクリックします。

プロセス稼働実績リストから選択して追加

プロセス設定(プロセス稼働時間画面)へ戻る ⑥

グループ名: ALL

設定するグループ名を選択し、プロセスの設定を行って下さい。

稼働実績のあるプロセスの検索

プロセス名 (部分一致)

アプリケーション名 (部分一致) ⑦

検索

表示プロセス名の設定と検索されたプロセス

⑧

表示プロセス名	プロセス名	アプリケーション名
<input type="checkbox"/> <input type="text"/>	ACPRFMGRSVC	
<input type="checkbox"/> <input type="text"/>	ACRORD32	
<input type="checkbox"/> <input type="text"/>	ACSVC	
<input type="checkbox"/> <input type="text"/>	ACTRAY	
<input type="checkbox"/> <input type="text"/>	ACWILCOM	

⑥設定するグループをプルダウンメニューから選択します。

⑦(必要であれば)プロセスの検索が可能です。

・プロセス名

特定のプロセス名に絞り込むことが可能です。(部分一致可)

・アプリケーション名

アプリケーション名で絞り込むことが可能です。(部分一致可)

⑧プロセスを選択してチェックを入れます。(ここで表示プロセス名を入力できます。空白の場合サービス名が表示プロセス名となります。)

⑨「チェックしたものを追加する」をクリックします。

<input type="checkbox"/>	<input type="text"/>	SCRNSAVE.SCR	
<input type="checkbox"/>	<input type="text"/>	SEARCHFILTERHOST	
<input type="checkbox"/>	<input type="text"/>	SEARCHINDEXER	
<input type="checkbox"/>	<input type="text"/>	SEARCHPROTOCOLHOST	
<input type="checkbox"/>	<input type="text"/>	SERVICES	
<input type="checkbox"/>	<input type="text"/>	SKYPE	

チェックしたものを追加する ⑨

前へ 1 2 次へ

■変更

⑩変更したいプロセスの内容を変更し、チェックを入れ、「変更する」ボタンをクリックします。

■削除

⑪削除したいプロセスにチェックを入れ、「削除する」ボタンをクリックします。

3. 2. 4 管理対象サービス

サブす稼働時間画面にて稼働時間を確認したいサービスを登録します。

- ・設定情報はグループ毎に変更することが可能です。
- ・上位グループでの設定は変更・削除できません。

■追加

- ・手動でサービスを追加する場合

- ①所属させるグループをプルダウンメニューから選択します。(必須)
- ②「表示サービス名」を入力します。
- ③「サービス名」(必須)を入力します。
- ④「サービスの説明」を入力します。

- ・サービス稼働実績リストから選択して追加する場合(推奨)

- ⑤「サービス稼働実績リストから選択して追加する」をクリックします。

サービス移動実績リストから選択して追加

[サービス設定\(サービス移動時間画面\)へ戻る](#)

設定するグループ名を選択し、サービスの設定を行って下さい。

グループ名:

移動実績のあるサービスの検索

サービス名 (部分一致)

サービスの説明 (部分一致)

表示サービス名の設定と検索されたサービス

表示サービス名	サービス名	サービスの説明
<input type="checkbox"/> <input type="text" value="AcPrfMgrSvc"/>	AcPrfMgrSvc	Ac Profile Manager Service
<input type="checkbox"/> <input type="text" value="AcSvc"/>	AcSvc	Access Connections Main Service
<input type="checkbox"/> <input type="text" value="AeLookupSvc"/>	AeLookupSvc	Application Experience Lookup Service
<input type="checkbox"/> <input type="text" value="Alerter"/>	Alerter	Alerter
<input type="checkbox"/> <input type="text" value="ALG"/>	ALG	Application Layer Gateway Service
<input type="checkbox"/> <input type="text" value="Apache2"/>	Apache2	Apache2
<input type="checkbox"/> <input type="text" value="AppMgmt"/>	AppMgmt	Application Management
<input type="checkbox"/> <input type="text" value="aspnet_state"/>	aspnet_state	ASP.NET State Service
<input type="checkbox"/> <input type="text" value="SCardSvr"/>	SCardSvr	Smart Card
<input type="checkbox"/> <input type="text" value="Schedule"/>	Schedule	Task Scheduler
<input type="checkbox"/> <input type="text" value="seclogon"/>	seclogon	Secondary Logon
<input type="checkbox"/> <input type="text" value="seclogon"/>	seclogon	RunAs Service
<input type="checkbox"/> <input type="text" value="SENS"/>	SENS	System Event Notification
<input type="checkbox"/> <input type="text" value="SharedAccess"/>	SharedAccess	Internet Connection Sharing
<input type="checkbox"/> <input type="text" value="SharedAccess"/>	SharedAccess	Windows Firewall/Internet Connection Sharing (ICS)

前へ 1 2 次へ

⑥設定するグループをプルダウンメニューから選択します。

⑦（必要であれば）サービスの検索が可能です。

- ・ サービス名 特定のサービス名に絞り込むことが可能です。
(部分一致可)
- ・ サービスの説明 サービス名で絞り込むことが可能です。
(部分一致可)

⑧サービスを選択してチェックを入れます。（ここで表示サービス名を入力できます。空白の場合サービス名が表示サービス名となります。）

⑨「チェックしたものを追加する」をクリックします。

■変更

⑩変更したいサービスの内容を変更し、チェックを入れ、「変更する」ボタンをクリックします。

■削除

⑪削除したいサービスにチェックを入れ、「削除する」ボタンをクリックします。

3. 2. 5 指定アプリケーション

バージョン管理などのために、特定のソフトウェアをグルーピングして設定可能です。

- ・設定情報はグループ毎に変更することができます。
- ・上位グループで設定されたものは変更・削除できません。

指定アプリケーションの登録は、グループ内 PC にインストールされたアプリケーション名、バージョン情報、ベンダー名がリスト表示されます。表示名を入力項目とし、未入力の場合はアプリケーション名＋バージョン名が自動で入力されます。リストを使用せず、手入力を行なうことも可能です。

また、指定アプリケーション設定は一括登録、一括削除が可能です。

■追加

- ①「指定アプリケーションの新規登録」をクリックします。

- ②設定したい「グループ名」をプルダウンメニューから選択します。
- ③「指定アプリケーション名」を入力します。
- ④「設定を保存する」をクリックします。

指定アプリケーション編集・直接登録

[指定アプリケーション一覧へ戻る](#) | [指定アプリケーション詳細](#)

グループ名: ALL
指定アプリケーション名: MsOffice
設定を保存する

アプリケーションリスト

表示アプリケーション名	アプリケーション名	バージョン	メーカー名
<input type="checkbox"/> MICROSOFT OFFICE WORL	MICROSOFT OFFICE WORL	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE PUBL	MICROSOFT OFFICE PUBL	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE POWE	MICROSOFT OFFICE POWE	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE OUTL	MICROSOFT OFFICE OUTL	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE EXCE	MICROSOFT OFFICE EXCE	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE ACCE	MICROSOFT OFFICE ACCE	12.0.4518.1014	Microsoft Corporation

チェックしたアプリケーションを

新規アプリケーションリスト追加
すべての項目を入力して「追加する」をクリックしてください。

・手入力の場合

- ① 「新規アプリケーションリスト追加」欄に項目名（表示アプリケーション名、アプリケーション名、バージョン、メーカー名）を入力します。
※表示アプリケーション名は任意です。（空白の場合、アプリケーション名と同一になります。）

- ② 「追加する」ボタンをクリックします。

・インストール済みアプリケーションリストから追加する場合

- ③ 「インストール済みアプリケーションリストから追加する」をクリックします。

指定アプリケーション登録(リストから)

[指定アプリケーション一覧へ戻る](#) | [指定アプリケーション詳細](#) | [指定アプリケーション編集・直接登録](#)

グループ名: ALL
指定アプリケーション名: MsOffice

インストール済みアプリケーションリスト

設定内容の検索

アプリケーション名: (部分一致)
バージョン: (部分一致)
メーカー名: (部分一致)

検索された設定内容

表示アプリケーション名	アプリケーション名	バージョン	メーカー名
<input type="checkbox"/> ACCESS HELP	ACCESS HELP	2.00	
<input type="checkbox"/> ADOBE READER 8.1.2 - JAPANESE	ADOBE READER 8.1.2 - JAPANESE	8.1.2	Adobe Systems Incorporated
<input type="checkbox"/> APACHE HTTP SERVER 2.2.4	APACHE HTTP SERVER 2.2.4	2.2.4	Apache Software Foundation
<input type="checkbox"/> ARIEL MULTISCHEDULER	ARIEL MULTISCHEDULER	11.000.1350	Ariel Networks
<input type="checkbox"/> BROADCOM GIGABIT INTEGRATED CONTROLLER	BROADCOM GIGABIT INTEGRATED CONTROLLER	10.15.13	Broadcom Corporation
<input type="checkbox"/> CANON PDLUS IP7100	CANON PDLUS IP7100		

- ④ グループ化したいアプリケーションにチェックを入れます。

<input type="checkbox"/>		SKYPE? 3.6	3.6.248	Skype Technologies S.A.
<input type="checkbox"/>		SMARTAUDIO		
<input type="checkbox"/>		SOFT DATA FAX MODEM WITH SMARTCP		
<input type="checkbox"/>		SONIC ICONS FOR LENOVO	1.0.2	Lenovo
<input type="checkbox"/>		SONIC UPDATE MANAGER	3.0.0	Sonic Solutions
<input type="checkbox"/>		SYNAPTICS POINTING DEVICE DRIVER	9.1.17.0	Synaptics

チェックしたアプリケーションを
追加する

※表示アプリケーション名が未入力の場合はアプリケーション名(バージョン)という表示になります

前へ 1 2 次へ

⑤「追加する」ボタンをクリックします。

設定内容の検索

アプリケーション名 (部分一致) ①

バージョン (部分一致) ②

メーカー名 (部分一致) ③

検索

■設定内容の検索

①アプリケーション名

特定のアプリケーション名に絞り込んで結果を出力することが可能です。
プルダウンメニューから選択します。(部分一致可)

②バージョン

特定のバージョンに絞り込んで結果を出力することが可能です。
(部分一致可)

③メーカー名

特定のメーカー名に絞り込んで結果を出力することが可能です。
(部分一致可)

■変更

①該当する指定アプリケーションの「変更する」をクリックします。

指定アプリケーションリスト

資産管理→指定アプリケーション画面に表示するアプリケーションの設定を行います。
アプリケーションをグループ化した名称(指定アプリケーション名)を設定し、実際のアプリケーション名と画面表示用アプリケーション名の設定、表示するグループ名の設定を行います。

[指定アプリケーションの新規登録](#)

グループ名	指定アプリケーション名	詳細	変更
ALL	MsOffice	詳細	変更する

チェックしたアプリケーションを [削除する](#)

[指定アプリケーションの新規登録](#)

②変更画面にてこの指定アプリケーションに関して、追加・変更・削除を行います。

指定アプリケーション編集・直接登録

[指定アプリケーション一覧へ戻る](#) | [指定アプリケーション詳細](#)

グループ名: ALL

指定アプリケーション名: MsOffice

アプリケーションリスト

表示アプリケーション名	アプリケーション名	バージョン	メーカー名
<input type="checkbox"/> MICROSOFT OFFICE WOR	MICROSOFT OFFICE WOR	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE PUBL	MICROSOFT OFFICE PUBL	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE POWE	MICROSOFT OFFICE POWE	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE OUTL	MICROSOFT OFFICE OUTL	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE EXCE	MICROSOFT OFFICE EXCE	12.0.4518.1014	Microsoft Corporation
<input type="checkbox"/> MICROSOFT OFFICE ACCE	MICROSOFT OFFICE ACCE	12.0.4518.1014	Microsoft Corporation

チェックしたアプリケーションを

新規アプリケーションリスト追加

すべての項目を入力して「追加する」をクリックしてください。

[インストール済みアプリケーションリストから追加する](#)

■削除

削除したい指定アプリケーションにチェックを入れて「削除する」ボタンをクリックしてください。

■詳細を確認する

「詳細」または、変更画面の「指定アプリケーションの詳細」をクリックしてください。

指定アプリケーション詳細

[指定アプリケーション一覧へ戻る](#)

グループ名: ALL

指定アプリケーション名: MsOffice

表示アプリケーション名	アプリケーション名	バージョン	メーカー名
MICROSOFT OFFICE WORD MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE WORD MUI (JAPANESE) 2007	12.0.4518.1014	Microsoft Corporation
MICROSOFT OFFICE PUBLISHER MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE PUBLISHER MUI (JAPANESE) 2007	12.0.4518.1014	Microsoft Corporation
MICROSOFT OFFICE POWERPOINT MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE POWERPOINT MUI (JAPANESE) 2007	12.0.4518.1014	Microsoft Corporation
MICROSOFT OFFICE OUTLOOK MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE OUTLOOK MUI (JAPANESE) 2007	12.0.4518.1014	Microsoft Corporation
MICROSOFT OFFICE EXCEL MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE EXCEL MUI (JAPANESE) 2007	12.0.4518.1014	Microsoft Corporation
MICROSOFT OFFICE ACCESS MUI (JAPANESE) 2007 (12.0.4518.1014)	MICROSOFT OFFICE ACCESS MUI (JAPANESE) 2007	12.0.4518.1014	Microsoft Corporation

3. 2. 7 保有ソフトウェアライセンス

保有しているライセンス数を登録します。

- ・設定情報はグループ毎に変更できます。
- ・ライセンス情報を取得したソフトウェア名のみ表示されます。
- ・登録した保有ライセンス数は「ソフトウェア台帳」に反映されます。

保有ライセンス登録

グループの指定 キーワード指定(部分一致)

ソフトウェア名▼	メーカー▼	保有ライセンス数	インストール数▼	ライセンス超過
MICROSOFT OFFICE ENTERPRISE 2007	Microsoft Corporation	---	1	
MICROSOFT OFFICE PROFESSIONAL 2007	Microsoft Corporation	---	1	
MICROSOFT OFFICE PROFESSIONAL PLUS 2007	Microsoft Corporation	---	5	

- ・ライセンス超過の場合、赤丸が表示されます。

保有ライセンス登録

グループの指定 キーワード指定(部分一致)

ソフトウェア名▼	メーカー▼	保有ライセンス数	インストール数▼	ライセンス超過
MICROSOFT OFFICE ENTERPRISE 2007	Microsoft Corporation	---	1	
MICROSOFT OFFICE PROFESSIONAL 2007	Microsoft Corporation	---	1	
MICROSOFT OFFICE PROFESSIONAL PLUS 2007	Microsoft Corporation	3	5	●

■追加

①追加対象のソフトウェア名をクリックします。

保有ライセンス登録

グループの指定 キーワード指定(部分一致)

ソフトウェア名▼	メーカー▼	保有ライセンス数	インストール数▼	ライセンス超過
MICROSOFT OFFICE ENTERPRISE 2007	Microsoft Corporation	---	1	
MICROSOFT OFFICE PROFESSIONAL 2007	Microsoft Corporation	---	1	
MICROSOFT OFFICE PROFESSIONAL PLUS 2007	Microsoft Corporation	---	5	

②「ライセンス情報」をクリックします。

保有ライセンス登録

ソフトウェア名▼	メーカー▼	ライセンス情報	保有ライセンス数	インストール数▼	ライセンス超過
MICROSOFT OFFICE PROFESSIONAL PLUS 2007	Microsoft Corporation	ライセンス情報	---	5	---

③登録対象の「グループ名」をクリックします。

保有ライセンス登録			
プロダクトID	95169-761-2041030		
アプリケーション名	MICROSOFT OFFICE PROFESSIONAL PLUS 2007		
メーカー名	Microsoft Corporation		
総保有ライセンス数	---		
総導入数	5		
差異	---		
グループ名 ALL 表示			
グループ名	保有ライセンス数	インストール数	差異
(内訳)	---	5	---
ALL	---	5	---
本社	---	---	---
営業部	---	---	---

④「総保有ライセンス数」を入力します。

保有ライセンス登録	
アプリケーション名	MICROSOFT OFFICE PROFESSIONAL PLUS 2007
バージョン名	---
メーカー名	Microsoft Corporation
グループ名	ALL
総保有ライセンス数	3
設定 戻る	

■変更・削除

登録した「総保有ライセンス数」を変更・削除します。

3. 2. 8 拡張項目データ登録（資産管理）

資産管理の追加項目の入力を行ないます。

資産管理台帳の拡張項目名設定にて設定を行った項目名に対応する情報の追加を行います。
登録方法は、個別に入力する方法と、csv によるインポートで行なうことが可能です。

■個別に入力する方法

- ①コンピュータ名をクリックします。
- ②拡張した項目に変更内容を入力します。
- ③「設定」ボタンをクリックします。

拡張資産管理データの登録

[拡張資産管理データの設定画面へ戻る](#)

グループ	営業本部
コンピュータ名	ishikawa
LogVillage拡張項目	<input type="text"/>

設定

■csv によるインポート

カンマ区切りの csv ファイルのインポートを行ないます。

- ・管理対象 PC 名（コンピュータ名）をキーに更新します。
- ・csv でインポートされた内容は上書きとなります。（値が空白の場合は空白となります。）
- ・csv にない管理対象 PC の情報はエラーとなります。
- ・管理対象 PC 名が自分が属するグループよりも上位グループ、別のグループの場合はエラーとなります。

○CSV フォーマット

“管理対象 PC 名”, “項目 1”, “項目 2”, “項目 3”, “項目 4” . . .

- ①CSV ファイルを選択します。

拡張資産管理データの読込

CSVファイル: (参照)

実行 キャンセル

- ②「実行」をクリックします。

拡張資産管理データの設定

[インポート](#) | [エクスポート](#)

拡張された資産管理項目のデータ登録を行います。
コンピュータ名をクリックするとデータ登録画面に移ります。

設定内容の検索

グループ名 ①

コンピュータ名 (部分一致) ②

LogVillage拡張項目 (部分一致) ③

検索された設定内容

グループ名▼	コンピュータ名▼	LogVillage拡張項目▼
ALL	Vista-PC2	
ALL	ishikawa	
ALL	netstar-up	
ALL	vm-ishikawa	
ALL	vm-winop	
ALL	w2k-work	
ALL	win2003-default	

■設定内容の検索

①グループ名

特定のグループ名に絞り込んで結果を出力することが可能です。

プルダウンメニューから選択します。

②コンピュータ名

特定のコンピュータ名に絞り込んで結果を出力することが可能です。(部分一致可)

③拡張した項目

特定の拡張した項目に絞り込んで結果を出力することが可能です。(部分一致可)

3.3 アラートポリシー設定

■自動アラート通知機能一覧

分類	設定するアラートポリシー	アラートポリシーの設定方法		管理者へのメール通知	管理対象PCへのポップアップ通知	アラート通知の設定例
		[システム設定] ⇒ 「アラートポリシー設定」画面	設定内容			
稼働管理	イベントログ発生に関する通知	指定イベントログ発生	1) イベントログ種別： システム、アプリケーション、セキュリティ 2) イベントログ種類： エラー、エラーと警告、情報 3) イベントログのソース： ソース名（部分一致 or 完全一致） 4) イベントログの説明： キーワード（部分一致 or 完全一致）	○	—	システムからの警告で、ソース=diskにて” Bus Error” を含むイベントログが発生した ※複数項目を設定した場合は and 条件での設定となります。
	サービス稼働に関する通知	サービス検知	1) 稼働を許可しないサービス 2) 稼働が必要なサービス	○	○	1) iPod Service が起動された 2) Emproxy (McAfee E-mail Proxy) が起動していない
	プロセス稼働に関する通知	プロセスの検知	1) 稼働を許可しないプロセス 2) 稼働が必要なプロセス 3) 定期的に稼働が必要なプロセス	○	○	1) winny が起動された 2) 業務で必至のプロセスが起動していない 3) 5 日以上一度も起動していない (バックアッププロセス等)
	ウィルス対策ソフト定義ファイル更新に関する通知	ウィルス定義ファイル未更新	1) ウィルス対策ソフト毎：xx 日以上	○	—	3 日以上、定義ファイルが更新されていない
	アプリケーションのインストール、アンインストールに関する通知	アプリケーション・インストール検知	1) インストールを許可しないアプリケーション 2) インストールを許可するアプリケーション 3) アンインストールを許可しないアプリケーション	○ 3 のみ	○ 3 のみ	1) SKYPE がインストールされた 2) ” Capture It!” を許可設定とすることで、その後はアラート通知は中止されます 3) NORTON360 がアンインストールされた

分類	アラートポリシー	アラートポリシーの設定方法		管理者へのメール通知	管理対象PCへのポップアップ通知	アラート通知の設定例
		[システム設定] ⇒ 「アラートポリシー設定」画面	設定内容			
操作管理	Web サイト閲覧に関する通知	禁止 Web サイトアクセス	1) 閲覧禁止 Web サイトの URL キーワード設定 2) 閲覧禁止 Web サイトのタイトルキーワード設定	○	○	1) " mail" を含む URL へアクセスした (Web メールの利用を抑止したい場合) 2) Web タイトルに" ショッピング" を含むサイトへアクセスした
	印刷に関する通知	禁止印刷ファイル/枚数制限	1) 印刷禁止ファイル名の設定 2) 印刷禁止ファイル拡張子の設定 3) 月間の印刷上限枚数の設定	○	○	1) " ユーザー" を含むファイル名が印刷された 2) 拡張子=" xls" のファイルが印刷された 3) グループ内で当月の印刷枚数が 5,000 枚以上となった "admin" を含むログオンアカウントでログオンされた
	ログオンアカウントに関する通知	禁止アカウントログオン	1) ログオン禁止アカウントの設定	○	○	
	記憶デバイスの接続に関する通知	禁止デバイス接続	1) デバイス種類別 : 接続を許可、許可しないを設定 2) デバイス名別 : 接続を許可、許可しないを設定 3) 管理対象 PC 別 : 接続を許可、許可しないデバイス名を設定	○ 許可の場合はー	○ 許可の場合はー	1) フロッピーが接続された 2) " HAGIWARA UD-Pure USB Device" (USB メモリー) が接続された 3) " USB 2.0 Flash Disk USB Device" を許可設定とすることで、その後はアラート通知は中止されます

分類	アラートポリシー	アラートポリシーの設定方法		管理者へのメール通知	管理対象PCへのポップアップ通知	アラート通知の設定例
		[システム設定] ⇒ 「アラートポリシー設定」画面	設定内容			
資産管理	インベントリ情報取得不可に関する通知	インベントリアラート設定	1) インベントリ情報が取得されなくなった管理対象PVC	○		1) 前日 10 時から本日 10 時までの間で一度もインベントリ収集が行えなかった管理対象PC
アラート通知メールの送信タイミングの設定		各アラートポリシー毎に設定可能	1) ログ情報のポーリング時と同時（即時）にアラートメールを送信 2) 毎日 xx 時に一括送信 3) 送信しない			
アラート通知を管理対象 PC の画面上へポップアップ表示させる設定		各アラートポリシー毎に設定可能	1) 表示する、しないを設定 2) ポップアップメッセージを編集			

■アラートメール送信先の登録は？

- ①「LV システム設定」→「全体の共通設定」→「LogVillage ユーザーの設定」
- ②「LogVillage ユーザーの新規追加」で作成されたユーザへ登録されているメール送信先を確認してください。

アラートメールが送信される条件

- ・選択したグループに登録されているアラート条件を満たしたログ情報が取得される。
- ・アラートメール設定にて「即時」が選択されている。
- ・アラート条件を満たすログを出力した管理対象 PC が所属するポーリングサーバーのメールサーバー情報設定が完了している。(p. 69)

「下位グループのアラートメールを受け取る」にチェックが入っている場合
選択したグループ以下の下位グループにて発生したアラートメールも受信します。

■ポップアップを管理対象 PC 上に表示させるには？

管理対象 PC 上に警告メッセージが記載されたポップアップメッセージが表示される条件

- ・管理対象 PC 上で、「Messenger」サービスのスタートアップの種類が「自動」もしくは「手動」となっている。(デフォルト設定では「手動」となっています)
- ・管理対象 PC が所属するグループに登録されているアラート条件を満たしたログ情報が取得される。
- ・ポップアップ設定にて「表示する」が選択されている。

3. 3. 1 インベントリアラート設定

インベントリ情報が取得できていない管理対象 PC を検知する条件を設定します。

①アラートを作成するグループを選択し[追加する]をクリックします。

②“取得されなくなった場合”に✓を入れる。

③アラート通知メールの送信先を確認

※①で選択したグループへの権限を持つ LogVillage ユーザーに設定されているメールアカウント宛てにアラートメールが送信されます。

④アラート通知メールの件名を編集します。

⑤インベントリ取得が行われていない管理対象 PC の抽出を行う実行曜日、実間を設定します。

(設定例)

「実行曜日：月、水、金」、「実行時間：10:00」の場合

- ・月曜 10:00 から水曜 10:00 までの間、一度もインベントリ取得が行えなかった管理対象 PC を抽出します。
- ・次に、水曜 10:00 から金曜 10:00 までの間、一度もインベントリ取得が行えなかった管理対象 PC を抽出します。
- ・設定曜日毎に上記を繰り返し抽出処理を実行します。

⑥[設定する]をクリックします。

3. 3. 2 禁止Web サイトアクセス

禁止 Web サイトを設定します。

アラートの設定 <禁止Webサイトへのアクセス>

設定されたアラート条件の検索

グループ名

アラート条件キーワード (部分一致)

設定対象項目 ☒ URL ☒ タイトル

検索されたアラート条件

グループ名	アラート条件キーワード	設定対象項目	アラートメール	ポップアップ
<input type="checkbox"/> ALL	競馬	タイトル	送信する(即時)	表示

チェックしたアラート設定を

アラート条件の新規追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名

■設定されたアラート条件の検索

- ・グループ名
プルダウンメニューからグループ名を選択します。
- ・アラート条件キーワード
キーワードを入力します。部分一致で検索可能です。
- ・設定対象項目
URL の設定かタイトルの設定かをチェックを入れます。

■追加（アラート条件の新規追加）

- ①アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

アラート条件の新規追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名

アラート条件の編集(禁止Webサイトへのアクセス)

[アラートの設定 <禁止Webサイトへのアクセス>画面へ戻る](#)

グループ名 ALL

アラート条件キーワード

☐ URL ☒ タイトル

☐ 競馬 ☐ URL ☒ タイトル

チェックしたアラート設定を

※は上位グループの設定条件(変更、削除不可)

- ②アラート条件キーワード（部分一致での指定も可能）にて、アラート条件となる URL もしくはタイトルに含まれるキーワードを入力します。
- ③URL とタイトルいずれかをチェックし「追加」をクリックします。

例) 「so-ten」というキーワードで URL アラート登録された場合、以下の URL 閲覧は全てアラート対象となります。

http://www. so-ten. co. jp/
 https://www. so-ten. co. jp/
 http://www. so-ten. jp/

■変更

- ④変更したいグループをクリックします。
- ⑤変更したい項目を変更して「変更する」ボタンをクリックします。

■削除

- ・グループごとに削除したい場合

- ⑥削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

- ・設定毎に削除したい場合

- ⑦削除したい項目を含むグループをクリックします。
- ⑧削除したい項目をチェックして「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

- ・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 3. 3 禁止印刷ファイル/枚数制限

禁止印刷ファイル/枚数制限を設定します。

アラートの設定<禁止印刷ファイル/枚数制限>

プリンタ毎の印刷枚数制限の設定

設定されたアラート条件の検索

グループ名: ALL (①)

アラート条件キーワード: (②)

設定対象項目: ☒ 拡張子 ☐ ファイル名 (③)

検索

検索されたアラート条件

グループ名	アラート条件キーワード	設定対象項目	アラート設定枚数	アラートメール	ポップアップ
ALL	himitsu	ファイル名(部分一致)	100枚	送信する(即時)	表示する

全てをチェック

チェックしたアラート設定を 削除する

アラート条件の新規追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名: ALL 追加する

■設定されたアラート条件の検索

- ①グループ名
プルダウンメニューからグループ名を選択します。
- ②アラート条件キーワード
キーワードを入力します。部分一致で検索可能です。
- ③設定対象項目
「拡張子」か「ファイル名」を選択します。

■追加（アラート条件の新規追加）

- ①アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

アラート条件の編集<禁止印刷ファイル/枚数制限>

アラートの設定 <禁止印刷ファイル/枚数制限> 画面へ戻る

グループ名: ALL

アラート条件キーワード: (②)

☒ ファイル名 ☒ 部分一致 ☐ 拡張子 追加する (③)

※は上位グループの設定条件(変更、削除不可)

☐ himitsu ☒ ファイル名 ☒ 部分一致 ☐ 拡張子

チェックしたアラート設定を 削除する 変更する

アラート設定枚数: 100 枚(上限 9999枚) 変更する

- ②アラート条件キーワードにて、アラート条件となるファイル名（部分一致での指定も可能）もしくは拡張子を入力します。
- ③「追加する」をクリックします。

■変更

- ④変更したいグループをクリックします。
- ⑤変更したい項目を変更して「変更する」ボタンをクリックします。

■削除

・グループごと削除したい場合

- ⑥削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

・設定毎に削除したい場合

- ⑦削除したい項目を含むグループをクリックします。
- ⑤削除したい項目をチェックして「削除する」ボタンをクリックします。

■アラート枚数の設定

月次で枚数を越えた場合、アラートを出力します。

アラート条件の編集(禁止印刷ファイル/枚数制限)

[アラートの設定 < 禁止印刷ファイル/枚数制限 > 画面へ戻る](#)

グループ名: ALL

アラート条件キーワード

☒ ファイル名 ☒ 部分一致 ☐ 拡張子

※は上位グループの設定条件(変更、削除不可)

☐ ☒ ファイル名 ☒ 部分一致 ☐ 拡張子

チェックしたアラート設定を

アラート設定枚数 枚(上限 9999枚)

- ①枚数を入力します。
- ②「変更する」をクリックします。

■アラート枚数の削除

枚数のアラートを停止します。

アラート条件の編集(禁止印刷ファイル/枚数制限)

[アラートの設定 < 禁止印刷ファイル/枚数制限 > 画面へ戻る](#)

グループ名: ALL

アラート条件キーワード

☒ ファイル名 ☒ 部分一致 ☐ 拡張子

※は上位グループの設定条件(変更、削除不可)

☐ ☒ ファイル名 ☒ 部分一致 ☐ 拡張子

チェックしたアラート設定を

アラート設定枚数 枚(上限 9999枚)

- ①空白にします。
- ②「変更する」をクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

アラートメール／ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細をつける

☐ 下位グループのアラートメールを受け取る

送信先

ポップアップ

☐ 表示しない ☒ 表示する

[初期画面に戻す](#)

☒ アラート詳細を表示する

・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 3. 4 禁止アカウントログオン

禁止アカウントでのログオンを設定します。

■設定されたアラート条件の検索

①グループ名

プルダウンメニューからグループ名を選択します。

②ログオンアカウント

キーワードを入力します。部分一致で検索可能です。

■追加（アラート条件の新規追加）

③アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

④アラート条件キーワードにて、アラート条件となるログオンアカウント名に含まれるキーワードを入力します。

⑤「追加する」をクリックします。

■変更

①変更したいグループをクリックします。

②変更したい項目を変更して「変更する」ボタンをクリックします。

■削除

- ・グループごと削除したい場合

⑥削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

- ・設定毎に削除したい場合

⑦削除したい項目を含むグループをクリックします。

⑧削除したい項目をチェックして「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

アラートメール／ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細をつける

☐ 下位グループのアラートメールを受け取る

送信先

ポップアップ

☐ 表示しない ☒ 表示する

[初期値に戻す](#)

☒ アラート詳細を表示する

・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 3. 5 禁止デバイス接続

禁止デバイスの接続を設定します。

取得したデバイス情報を許可設定にする場合は、不許可設定を行います。

■追加（アラート条件の新規追加）

①アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

②新規アラート追加にて「デバイスの種類別表示」、「デバイス名別表示」、「管理対象 PC 別」のいずれかを選択します。

・ デバイスの種類別表示

アラート条件の編集(禁止デバイスの接続) > デバイスの種類別表示

アラートの設定<禁止デバイスの接続> | デバイスの種類別表示 | デバイス名別表示 | 管理対象PC別に表示

アラート設定されていないデバイスの種類

グループ名: ALL

デバイスの種類	件数	ステータス
全てをチェック		
<input type="checkbox"/> CDROM	21件	許可
<input type="checkbox"/> HDD	35件	許可

全てをチェック

アラート条件に追加する

変更したい「ステータス」をプルダウンメニューから変更後、「全てをチェック」ボタンで『全て』のデバイスの種類を選択し、「アラート条件に追加する」をクリックします。

※表示されているデバイスの種類を『全て』アラート条件に追加してください。アラート条件への追加漏れがある場合、予定外のアラートが発生する可能性があります。

※情報が複数ページになる場合は、全てのページで同じ操作を行ってください。

ステータス

許可 アラートに該当しません。

不許可 ポーリングサーバーが検知した時に接続されているとアラートに該当します。

・ デバイス名別表示

アラート条件の編集(禁止デバイスの接続) > デバイス名別表示

< 禁止デバイスの接続 | デバイスの種類別表示 | デバイス名別表示 | 管理対象PC別に表示

アラート設定されていないデバイスの種類

グループ名: ALL

アラート設定されていないデバイスの検索

デバイス名

デバイスの種類

検索

アラート設定されていないデバイス

直接指定(デバイス名を入力してください) ☐ 部分一致(許可) ☐ 追加する

デバイス名	デバイスの種類	件数	ステータス
全てをチェック			
<input type="checkbox"/> ELBY CLONEDRIVE SCSI CdRom Device	CDROM	1件	許可
<input type="checkbox"/> JLU TMVXSEJ SCSI CdRom Device	CDROM	1件	許可

WDC WD1600HLFS-75G6U1

HDD

1件

許可

全てをチェック

アラート条件に追加する

変更したい「ステータス」をプルダウンメニューから変更後、「全てをチェック」ボタンで『全て』のデバイス名を選択し、「アラート条件に追加する」をクリックします。

※表示されているデバイス名を『全て』アラート条件に追加してください。アラート条件への追加漏れがある場合、予定外のアラートが発生する可能性があります。

※情報が複数ページになる場合は、全てのページで同じ操作を行ってください。

ステータス

許可 アラートに該当しません。

Copyright © 2003-2021 SO-TEN, Inc. All Rights Reserved.

不許可 ポーリングサーバーが検知した時に接続されているとアラートに該当します。

アラート設定されていないデバイスの検索

- ・ デバイス名 デバイス名を入力します。
- ・ デバイスの種類 プルダウンメニューから選択します。

＜デバイス名の部分一致設定＞

デバイス名の部分一致でアラート設定を行うことができます。

(例) 「USB」を部分一致ワードとして設定。

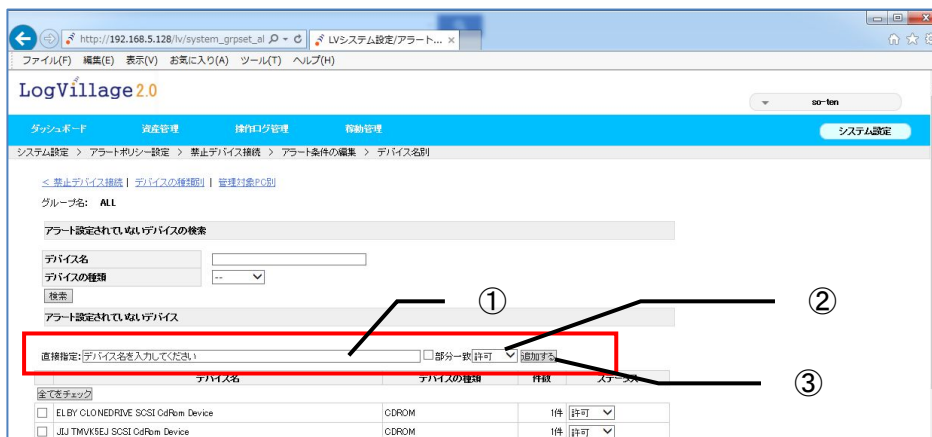
以下のようなデバイス名が接続された場合にアラートに該当します。

Sony-USB-xxxxxxx

USBstorage-xxxxxxxxx

■ デバイス名部分一致設定の方法

- ① 部分一致ワードを入力し、” 部分一致” をチェックオンにする。
- ② 許可、不許可を選択
- ③ [追加する] をクリック



・管理対象 PC 毎に表示

アラート条件の編集<禁止デバイスの接続> > 管理対象 PC 別に表示

[アラートの設定<禁止デバイスの接続>](#) | [デバイスの種類別表示](#) | [デバイス名別表示](#) | [管理対象 PC 別に表示](#)

グループ名: ALL

アラート設定されていないクライアント PC の検索

コンピュータ名

デバイス名

デバイスの種類 -- ▾

アラート設定されていないクライアント PC

	コンピュータ名	デバイス名	デバイスの種類	件数	ステータス
<input type="button" value="全てをチェック"/>					
<input type="checkbox"/>	ishikawa	FUJITSU MH62120BH	HDD	1件	許可 ▾
<input type="checkbox"/>	ishikawa	JetFlash TS10JF110 USB Device	HDD	1件	許可 ▾
<input type="checkbox"/>	netstar-zp	VMware Virtual IDE Hard Drive	HDD	1件	許可 ▾
<input type="checkbox"/>	m2kwork	VMware, VMware Virtual S SCSI Disk Device	HDD	1件	許可 ▾
<input type="checkbox"/>	win2003-default	VMware, VMware Virtual S SCSI Disk Device	HDD	1件	許可 ▾
<input type="button" value="全てをチェック"/>					
<input type="button" value="アラート条件に追加する"/>					

変更したい「ステータス」をプルダウンメニューから変更後、「全てをチェック」ボタンで『全て』のコンピュータ名を選択し、「アラート条件に追加する」をクリックします。

※表示されているコンピュータ名を『全て』アラート条件に追加してください。アラート条件への追加漏れがある場合、予定外のアラートが発生する可能性があります。

※情報が複数ページになる場合は、次のページでも同じ操作を行ってください。

ステータス

許可 アラートに該当しません。

不許可 ポーリングサーバーが検知した時に接続されているとアラートに該当します。

アラート設定されていないクライアントの検索

- ・コンピュータ名 コンピュータ名を入力します。
- ・デバイス名 デバイス名を入力します。
- ・デバイスの種類 プルダウンメニューから選択します。

■削除

- ・グループごとに削除したい場合

①削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

- ・設定毎に削除したい場合

①削除したい項目を含むグループをクリックします。

②削除したい項目をチェックして「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

アラートメール／ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細をつける

☐ 下位グループのアラートメールを受け取る

送信先

ポップアップ

☐ 表示しない ☒ 表示する

[初期画面に戻る](#)

☒ アラート詳細を表示する

・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 3. 6 指定イベントログ発生

指定イベントログの発生を設定します。

アラートの設定<指定イベントログ発生>

グループ名	アラート条件名	ログ種別	ログ種類	ソース	説明	アラートメール
<input type="button" value="全てをチェック"/>						
<input type="checkbox"/>	ALL	Webサービス	アプリケーション システム	警告とエラー 警告とエラー	Apache(部分一致) Apache(部分一致)	送信する(即時)
<input type="button" value="全てをチェック"/>						

チェックしたアラート設定を

アラート条件の新規追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名

■追加（アラート条件の新規追加）

- ①アラート条件を設定するグループ名を選択します。
- ②「追加する」をクリックします。

アラート条件の編集(指定イベントログ発生)

[アラートの設定<指定イベントログ発生>画面へ戻る](#)

グループ名: ALL ①

アラート条件名

アラート条件を新規追加する場合は
*アラート条件名を入力してから[追加する]をクリック ②

アラート条件名	ログ種別	ログ種類	ソース	説明
<input type="button" value="全てをチェック"/> ※は上位グループの設定条件(変更、削除不可)				
<input type="checkbox"/>	Webサービス	アプリケーション システム	警告とエラー 警告とエラー	Apache(部分一致) Apache(部分一致)
<input type="button" value="全てをチェック"/>				

チェックしたアラート条件を

アラート条件の編集(指定イベントログ発生)

[アラートの設定<指定イベントログ発生>画面へ戻る](#)

グループ名: ALL

アラート条件名: Webサービス 設定する

アラート条件詳細

ログ種別	ログ種類	ソース	説明
<input type="checkbox"/> アプリケーション	警告とエラー	Apache(部分一致)	
<input type="checkbox"/> システム	警告とエラー	Apache(部分一致)	

全てをチェック 削除する

アラート条件を追加

ログ種別 ☐ アプリケーション ☐ システム ☐ セキュリティ

ログ種類 エラーのみ

ソース ☒ 部分一致

説明

追加する

- ③アラート条件編集にて、アラート条件名（任意）を入力します。
- ④アラートの条件を追加にて以下の設定を行います。
- ・ログ種別 アプリケーション、システム、セキュリティ
 - ・ログ種類
 - ・ソース ソースのキーワードを設定します。（部分一致可能）
 - ・説明 説明を入力します。
- ⑤「追加する」ボタンをクリックします。

■削除

- ・グループごと削除したい場合

①削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

- ・設定毎に削除したい場合

②削除したい項目を含むグループをクリックします。

③削除したい項目をチェックして「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

アラートメール／ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細を付ける

☐ 下位グループのアラートメールを受け取る

送信先

ポップアップ

☐ 表示しない ☒ 表示する

[初期画面に戻す](#)

☒ アラート詳細を表示する

・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 3. 7 プロセス検知

プロセスの検知を設定します。

※タスクマネージャーのプロセスタブで表示されるプログラムとなります。

アラートの設定(プロセスの検知)

グループ名	プロセス名	アプリケーション名	コンピュータ名	ステータス	アラートメール	ポップアップ
<input type="checkbox"/> ALL	SKYPEPM		すべて	不許可	送信する(即時)	表示する
<input type="checkbox"/> SKYPE	SKYPE		すべて	不許可		

全てをチェック

チェックしたアラート設定を [削除する](#)

新規アラート追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名: [ALL](#) [追加する](#) ①

■追加（アラート条件の新規追加）

①アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

アラート条件の編集(プロセスの検知)

[アラートの設定<プロセスの検知>画面へ戻る](#)

グループ名: ALL

アラート設定

プロセス名	アプリケーション名	コンピュータ名	ステータス
<input type="checkbox"/> SKYPEPM		すべて	不許可
<input type="checkbox"/> SKYPE		すべて	不許可

全てをチェック

※は上位グループの設定条件(変更、削除不可)

チェックしたアラート条件を [削除する](#) ②

新規に追加する [プロセス名別表示](#) [管理対象PC別に表示](#)

②プロセス名別に表示か、管理対象PC 別に表示をクリックします。

・プロセス名別表示

アラート条件の編集(プロセスの検知) > プロセス名別表示

[アラートの設定<プロセスの検知>画面へ戻る](#) | [プロセス名別表示](#) | [管理対象PC別に表示](#)

アラート設定されてないプロセス

グループ名: ALL

設定されたアラート条件の検索

プロセス名 (部分一致)

アプリケーション名 (部分一致)

検索されたアラート条件

	プロセス名	アプリケーション名	ステータス
<input type="button" value="全てをチェック"/>			
<input type="checkbox"/>	ACPRFMGRSVC		不許可 ▼
<input type="checkbox"/>	ACRORD32		不許可 ▼
<input type="checkbox"/>	ACSVC		不許可 ▼
<input type="checkbox"/>	ACTRAY		不許可 ▼
<input type="checkbox"/>	ACWLICON		不許可 ▼
<input type="checkbox"/>	AIRBROWSERMS		不許可 ▼
<input type="checkbox"/>	AIRCAFE		不許可 ▼

設定するプロセス名をチェックしてステータスをプルダウンメニューから選択します。
「アラート条件に追加する」をクリックします。

ステータス

- 必須 ポーリングサーバーが検知したときに実行していなければアラート条件に該当します。
- 不許可 ポーリングサーバーが検知したときに実行されていればアラート条件に該当します。
- 定期 指定日数（任意の日数を指定します）以上、対象プロセスが未稼動の場合はアラート条件に該当します。

設定されたアラート条件の検索

- ・プロセス名 プロセス名を入力します。（部分一致可能）
- ・アプリケーション名 アプリケーション名を入力します。（部分一致可能）

・管理対象 PC 別に表示

アラート条件の編集(プロセスの検知)>管理対象PC別に表示

[アラートの設定<プロセスの検知>画面へ戻る](#) | [プロセス名別表示](#) | [管理対象PC別に表示](#)

アラート設定されていないクライアントPC

グループ名: ALL

設定されたアラート条件の検索

コンピュータ名 (部分一致)

プロセス名 (部分一致)

アプリケーション名 (部分一致)

検索されたアラート条件

	コンピュータ名	プロセス名	アプリケーション名	ステータス
<input type="button" value="全てをチェック"/>				
<input type="checkbox"/>	ishikawa	ACPRFMGRSVC		不許可 ▼
<input type="checkbox"/>	ishikawa	ACRORD32		不許可 ▼
<input type="checkbox"/>	ishikawa	ACSV		不許可 ▼
<input type="checkbox"/>	ishikawa	ACTRAY		不許可 ▼

設定するコンピュータ名とプロセス名の組み合わせをチェックしてステータスをプルダウンメニューから選択します。

「アラート条件に追加する」をクリックします。

ステータス

必須 ポーリングサーバーが検知したときに実行していなければアラート条件に該当します。

不許可 ポーリングサーバーが検知したときに実行されていなければアラート条件に該当します。

定期 指定日数(任意の日数を指定します)以上、対象プロセスが未稼働の場合はアラート条件に該当します。

設定されたアラート条件の検索

- ・コンピュータ名 コンピュータ名を入力します。(部分一致可能)
- ・プロセス名 プロセス名を入力します。(部分一致可能)
- ・アプリケーション名 アプリケーション名を入力します。(部分一致可能)

■削除

- ・グループごと削除したい場合

①削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

- ・設定毎に削除したい場合

①削除したい項目を含むグループをクリックします。

②削除したい項目をチェックして「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

The screenshot shows a settings window titled "アラートメール／ポップアップ設定" (Alert Mail / Pop-up Settings). It is divided into two main sections: "メール" (Mail) and "ポップアップ" (Pop-up).

メール (Mail) section:

- There are two radio buttons: "送信しない" (Do not send) and "即時" (Immediate). The "即時" option is selected.
- There is a checked checkbox "アラートメールの件名にアラート詳細をつける" (Attach alert details to the subject of the alert mail).
- There is an unchecked checkbox "下位グループのアラートメールを受け取る" (Receive alert mail from the lower group).
- Below these is a label "送信先" (Destination).

ポップアップ (Pop-up) section:

- There are two radio buttons: "表示しない" (Do not display) and "表示する" (Display). The "表示する" option is selected.
- Below the radio buttons is a text input field containing "[logvillage]不正なWebサイトを検知しました" (Detected an illegal website on [logvillage]). To the right of the field is a blue link "初期値に戻す" (Reset to default).
- Below the text field is a checked checkbox "アラート詳細を表示する" (Display alert details).
- At the bottom are two buttons: "設定する" (Set) and "キャンセル" (Cancel).

・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 3. 8 サービス検知

サービスの検知を設定します。

アラートの設定<サービスの検知>

現在登録されているアラート

グループ名	サービス名	サービスの説明	コンピュータ名	ステータス	アラートメール	ポップアップ
<input type="checkbox"/> ALL	AudioSrv	Windows Audio	すべて	不許可	送信する(即時)	表示する
<input type="checkbox"/> ALL	Fax	FAX Service	すべて	不許可		

全てをチェック

チェックしたアラート設定を [削除する](#)

アラート条件の新規追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名 [ALL](#) [追加する](#) ①

■追加（アラート条件の新規追加）

①アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

アラート条件の編集<サービスの検知>

[アラートの設定<サービスの検知>画面へ戻る](#)

グループ名: ALL

アラート設定

サービス名	サービスの説明	コンピュータ名	ステータス
<input type="checkbox"/> AudioSrv	Windows Audio	すべて	不許可
<input type="checkbox"/> Fax	FAX Service	すべて	不許可

全てをチェック

チェックしたアラート条件を [削除する](#) ②

新規に追加する: [サービス名別表示](#) | [管理対象PC別に表示](#)

②サービス名別表示か、管理対象 PC 別に表示をクリックします。

・サービス名を表示

アラート条件の編集(サービスの検知) > サービス名別表示

[アラートの設定<サービスの検知>画面へ戻る](#) | [サービス名別表示](#) | [管理対象PC別に表示](#)

アラート設定されていないサービス

グループ名: ALL

設定されたアラート条件の検索

サービス名 (部分一致)

サービスの説明 (部分一致)

検索されたアラート条件

	サービス名	サービスの説明	ステータス
<input type="button" value="全てをチェック"/>			
<input type="checkbox"/>	AcPrfMgrSvc	Ac Profile Manager Service	不許可 ▼
<input type="checkbox"/>	AcSvc	Access Connections Main Service	不許可 ▼
<input type="checkbox"/>	AeLookupSvc	Application Experience Lookup Service	不許可 ▼
<input type="checkbox"/>	Alerter	Alerter	不許可 ▼
<input type="checkbox"/>	ALG	Application Layer Gateway Service	不許可 ▼

設定するサービス名をチェックしてステータスをプルダウンメニューから選択します。
「アラート条件に追加する」をクリックします。

ステータス

必須 ポーリングサーバーが検知したときに開始していなければアラート条件に該当します。

不許可 ポーリングサーバーが検知したときに開始であればアラート条件に該当します。

設定されたアラート条件の検索

- ・サービス名 サービス名を入力します。(部分一致可)
- ・サービスの説明 サービスの説明を入力します。(部分一致可)

・管理対象 PC 別に表示

アラート条件の編集(サービスの検知) > 管理対象 PC 別に表示

[アラートの設定<サービスの検知>画面へ戻る](#) | [サービス名別表示](#) | [管理対象 PC 別に表示](#)

アラート設定されていないクライアント PC

グループ名: ALL

設定されたアラート条件の検索

コンピュータ名 (部分一致)
 サービス名 (部分一致)
 サービスの説明 (部分一致)

検索されたアラート条件

	コンピュータ名	サービス名	サービスの説明	ステータス
<input type="button" value="全てチェック"/>				
<input type="checkbox"/>	ishikawa	AcPrfMgrSvc	Ac Profile Manager Service	不許可 <input type="button" value="v"/>
<input type="checkbox"/>	ishikawa	AcSvc	Access Connections Main Service	不許可 <input type="button" value="v"/>
<input type="checkbox"/>	ishikawa	Alerter	Alerter	不許可 <input type="button" value="v"/>
<input type="checkbox"/>	ishikawa	ALG	Application Layer Gateway Service	不許可 <input type="button" value="v"/>
<input type="checkbox"/>	ishikawa	AppMgmt	Application Management	不許可 <input type="button" value="v"/>
<input type="checkbox"/>	ishikawa	aspnet_state	ASP.NET 状態サービス	不許可 <input type="button" value="v"/>

設定するコンピュータ名とサービス名の組み合わせをチェックしてステータスをプルダウンメニューから選択します。

「アラート条件に追加する」をクリックします。

ステータス

必須 ポーリングサーバーが検知したときに開始していなければアラート条件に該当します。

不許可 ポーリングサーバーが検知したときに開始であればアラート条件に該当します。

設定されたアラート条件の検索

- ・コンピュータ名 コンピュータ名を入力します。(部分一致可)
- ・サービス名 サービス名を入力します。(部分一致可)
- ・サービスの説明 サービスの説明を入力します。(部分一致可)

■削除

- ・グループごと削除したい場合

③削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

- ・設定毎に削除したい場合

④削除したい項目を含むグループをクリックします。

⑤削除したい項目をチェックして「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

The screenshot shows a configuration window titled 'アラートメール/ポップアップ設定' (Alert Email/Popup Settings). It is divided into two main sections: 'メール' (Email) and 'ポップアップ' (Popup).

メール (Email) Section:

- Radio buttons: ☐ 送信しない (Do not send) and ☒ 即時 (Immediate).
- Checkboxes: ☒ アラートメールの件名にアラート詳細を付ける (Attach alert details to the subject line) and ☐ 下位グループのアラートメールを受け取る (Receive alert emails from the lower group).
- Text: 送信先 (Send to).

ポップアップ (Popup) Section:

- Radio buttons: ☐ 表示しない (Do not display) and ☒ 表示する (Display).
- Text input: A message preview is shown in a box: "[logvillage]不正なWebサイトを検知しました" (Detected an unauthorized website on logvillage). To the right of the box is a link: [初期値に戻す](#) (Reset to default).
- Checkbox: ☒ アラート詳細を表示する (Display alert details).
- Buttons: 設定する (Set) and キャンセル (Cancel).

・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 3. 9 ウィルス定義ファイル未更新

ウィルス対策ソフトの定義ファイル未更新の設定を行います。

アラートの設定<ウィルス対策ソフトの定義ファイル未更新>

グループ名	更新されていない期間	アラートメール
<input type="checkbox"/> ALL	7日以上	送信する(即時)

チェックしたアラート設定を

アラート条件の新規追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名

①

■追加（アラート条件の新規追加）

①アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

アラート条件の編集<ウィルス対策ソフトの定義ファイル未更新>

[アラートの設定<ウィルス対策ソフトの定義ファイル未更新>画面へ戻る](#)

グループ名: ALL

アラート設定

更新されていない期間 日以上

アラートメール/ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細をつける

送信先

②

③

②アラート設定にて更新されていない期間に日数を入力します。

③「設定する」ボタンをクリックします。

■変更

①変更したいグループをクリックします。

②日数を変更して「設定する」ボタンをクリックします。

■削除

①削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

アラートメール／ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細をつける

送信先

・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

3. 3. 10 アプリケーション・インストール検知

アプリケーション・インストールの検知を設定します。

アラートの設定<アプリケーション・インストールの検知>

現在登録されているアラート

グループ名	アプリケーション名	コンピュータ名	ステータス	アラートメール
全てをチェック				
アラート設定がありません				
全てをチェック				

チェックしたアラート設定を [削除する](#)

新規アラート追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名 [ALL](#) [追加する](#)

①

■追加（アラート条件の新規追加）

①アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

アラート条件の編集<アプリケーション・インストールの検知>

[アラートの設定<アプリケーション・インストールの検知>画面へ戻る](#)

グループ名: ALL

アラート設定

アプリケーション名	コンピュータ名	ステータス
全てをチェック		
アラート設定がありません		
全てをチェック		

チェックしたアラート条件を [削除する](#)

新規アラート追加 [アプリケーション名別表示](#) | [管理対象PC別に表示](#)

②

②アプリケーション名別表示か、管理対象PC別に表示をクリックします。

・アプリケーション名別表示

アプリケーション名別表示

[アラートの設定<アプリケーションインストールの検知>](#) | [アプリケーション名別表示](#) | [管理対象PC別に表示](#)

アラート設定されていないアプリケーション

グループ名: ALL

設定内容の検索

アプリケーション名 (部分一致)

検索された設定内容

アプリケーション名	ステータス
<input type="checkbox"/> "MORA WIN" TYPE1 PLUG-IN	許可 <input type="button" value="v"/>
<input type="checkbox"/> +LHACA	許可 <input type="button" value="v"/>
<input type="checkbox"/> 2007 MICROSOFT OFFICE SUITE SERVICE PACK 2 (SP2)	許可 <input type="button" value="v"/>
<input type="checkbox"/> CATALYST CONTROL CENTER LOCALIZATION KOREAN	許可 <input type="button" value="v"/>

チェックしたものを

前へ 1 2 3 4 5 6 7 8 次へ

変更したい「ステータス」をプルダウンメニューから変更後、「全てをチェック」ボタンで『全て』のアプリケーション名を選択し、「アラート条件に追加する」をクリックします。

※表示されているアプリケーション名を『全て』アラート条件に追加してください。アラート条件への追加漏れがある場合、予定外のアラートが発生する可能性があります。

※情報が複数ページになる場合は、次のページでも同じ操作を行ってください。

ステータス

許可 アラートに該当しません。

不許可 ポーリングサーバーが検知した時にインストールされているとアラートに該当します。

必須 ポーリングサーバーが検知した時にアンインストールされている（削除されている）とアラートに該当します。

設定されたアラート条件の検索

・アプリケーション名

アプリケーション名を入力します。（部分一致可能）

・管理対象 PC 別に表示

管理対象PC別に表示

[アラートの設定<アプリケーション・インストールの検知>](#) | [アプリケーション名別表示](#) | [管理対象PC別に表示](#)

アラート設定されていないクライアントPC

グループ名: ALL

設定内容の検索

コンピュータ名 (部分一致)

アプリケーション名 (部分一致)

検索された設定内容

コンピュータ名	アプリケーション名	ステータス
<input type="button" value="全てをチェック"/>		
<input type="checkbox"/> HINOKI	MYSQL CONNECTOR NET 5.2.5	許可 <input type="button" value="v"/>
<input type="checkbox"/> HINOKI	BROADCOM NETXTRME ETHERNET CONTROLLER	許可 <input type="button" value="v"/>
<input type="checkbox"/> HINOKI	MYSQL SERVER 5.1	許可 <input type="button" value="v"/>

<input type="checkbox"/> LENOVO-CE430EA3	MICROSOFT OFFICE WORD MUI (JAPANESE) 2007	許可 <input type="button" value="v"/>
--	---	-------------------------------------

チェックしたものを

前へ 1 2 3 4 5 6 7 8 - 16 次へ

変更したい「ステータス」をプルダウンメニューから変更後、「全てをチェック」ボタンで『全て』のコンピュータ名を選択し、「アラート条件に追加する」をクリックします。

※表示されているコンピュータ名を『全て』アラート条件に追加してください。アラート条件への追加漏れがある場合、予定外のアラートが発生する可能性があります。

※情報が複数ページになる場合は、次のページでも同じ操作を行ってください。

ステータス

許可 アラートに該当しません。

不許可 ポーリングサーバーが検知した時にインストールされているとアラートに該当します。

必須 ポーリングサーバーが検知した時にアンインストールされている（削除されている）とアラートに該当します。

設定されたアラート条件の検索

・コンピュータ名

コンピュータ名を入力します。（部分一致可能）

・アプリケーション名

アプリケーション名を入力します。（部分一致可能）

■削除

- ・グループごと削除したい場合

①削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

- ・設定毎に削除したい場合

①削除したい項目を含むグループをクリックします。

②削除したい項目をチェックして「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

アラートメール／ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細をつける

☐ 下位グループのアラートメールを受け取る

送信先

ポップアップ

☐ 表示しない ☒ 表示する

[お気に入りへ追加](#)

☒ アラート詳細を表示する

- ・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

- ・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 3. 1 1 PC リソースしきい値超過

PC リソースのしきい値超過を設定します。

※期間を指定して設定する項目に関しては、間隔が狭いと突発的に高い値を示したログをすべてアラート対象としてしまうため、アラート数が増える可能性があります。

アラートの設定<PCリソースのしきい値超過>

グループ名	設定項目	アラート基準	アラートメール	ポップアップ
<input type="checkbox"/> ALL	CPU	60分間の平均が 80%以上	送信する(即時)	表示する
	メモリ残	256MB以下		
	HDD残	100MB以下		

チェックしたアラート設定を

アラート条件の新規追加

*アラート条件を追加するグループ名を選択してから[追加する]をクリック

グループ名

①

■追加（アラート条件の新規追加）

①アラート条件を設定するグループ名を選択し、「追加する」をクリックします。

アラート条件の編集<PCリソースのしきい値超過>

アラートの設定<PCリソースのしきい値超過>画面へ戻る

グループ名: ALL

アラート設定

CPU 分間の平均が %以上だった場合

メモリ残 MB以下だった場合

ネットワークIO 分間の平均が KB/秒以上だった場合

HDD残 MB以下だった場合

ディスクIO 分間の平均が %以上だった場合

アラートメール/ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細をつける

送信先

ポップアップ

☐ 表示しない ☒ 表示する

[初期値に戻す](#)

☒ アラート詳細を表示する

②

③

②アラート設定にて、CPU、メモリ残、ネットワーク I/O、HDD 残、ディスク I/O を設定します。設定する項目の値を入力してください。

③「設定する」をクリックします

■変更

①変更したいグループをクリックします。

②変更したい項目を変更して「設定する」ボタンをクリックします。

■削除

①削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

■アラートメール／ポップアップ設定

アラートメール／ポップアップ設定について、以下の設定が可能です。

アラートメール／ポップアップ設定

メール

☐ 送信しない ☒ 即時

☒ アラートメールの件名にアラート詳細をつける

送信先
ishikawa@so-ten.co.jp
ishikawa@so-ten.co.jp

ポップアップ

☐ 表示しない ☒ 表示する

[初期値に戻す](#)

☒ アラート詳細を表示する

・メール

「送信しない」または「即時」

アラートメールの件名にアラート詳細を付けるか？

下位グループのアラートメールを受け取るか？

・ポップアップ

「表示しない」または「表示する」

メッセージの入力

アラート詳細を表示するか？

3. 4 運用管理

3. 4. 1 ライセンスの登録・更新

使用オプションを変更したり、登録可能管理対象を変更したりする場合にはライセンスの更新が必要です。ライセンス情報の内容を変更する場合には、蒼天もしくは販売店までご連絡ください。

ライセンス情報表示

ライセンス情報

お客様番号	2002	
ご利用期限	無期限	ライセンス設定日時 2008/03/28 02:06:03
登録可能ホーリングサーバ	無制限	現在登録数 1 台
登録可能クライアントPC	200 台	現在登録数 5 台
LogVillage リリースバージョン	V02.01.00.00	
マネージャのバージョン	V02.01.00.00	
データベースバージョン	V02.01.00.00	

利用可能機能

移動管理パッケージ
資産管理オプション
操作管理オプション
ファイル更新履歴オプション

[ライセンス更新](#)

①

①「ライセンス更新」をクリックしてください。

ライセンス更新

[ライセンス情報表示](#)

ライセンス更新

ライセンスコード

登録する

②

②発行されたライセンスをライセンスコードの欄に入力し、「登録ボタン」をクリックします。

3. 4. 2 LogVillage へのログイン履歴

LogVillage へのログイン履歴を確認することができます。

LogVillageへのログイン履歴

LogVillageへのログイン履歴の検索、参照を行います。
ログイン履歴情報の収集設定や削除は[ログイン履歴の取得設定と削除]より行って下さい。

[ログイン履歴の取得設定と削除](#)

表示期間の設定

開始日 ☐ 終了日

2008 年 04 月 -- 日 (日付が"--"は月次表示) 2008 年 04 月 2 日

[CSVダウンロード](#)

日付▼	ユーザー名▼	アクセス元▼	結果
2008-03-28 15:37:43	ishikawa	192.168.5.46	成功
2008-03-28 16:54:40	ishikawa	192.168.5.46	成功
2008-03-28 17:28:24	ishikawa	192.168.5.44	成功
2008-03-31 08:37:38	ishikawa	192.168.5.44	成功
2008-03-31 09:48:03	ishikawa	192.168.5.44	成功
2008-03-31 09:51:24	ishikawa	192.168.5.44	成功
2008-03-31 09:54:07	admin	192.168.5.44	成功
2008-03-31 19:38:47	ishikawa	192.168.5.46	成功
2008-03-31 19:43:07	admin	192.168.5.46	成功
2008-04-02 16:36:35	admin	192.168.5.44	成功
2008-04-02 16:39:24	admin	192.168.5.44	成功

■設定方法

「ログイン履歴の取得設定と削除」をクリックします。

ログイン履歴の取得設定と削除

[LogVillageへのログイン履歴画面へ戻る](#)

☐ LogVillageへのログイン履歴を取得する

ログイン履歴の削除
ユーザー削除するとログイン履歴データの復活ができませんのでご注意ください。

☒ 日以上古いログイン履歴を全て削除(0日とすると全て削除されます)

☐ 2008 年 05 月 12 日 ~ 2008 年 05 月 12 日の期間のログイン履歴を全て削除

- ・履歴を取得する。

「LogVillage へのログイン履歴を取得する」にチェックを入れ、「設定する」をクリックします。

- ・ログオン履歴の削除
- ・〇〇日以上古いログイン履歴を全て削除
- ・日付指定

のどちらかを選択し、「設定する」ボタンをクリックします。

3. 4. 3 ユーザー情報変更

現在ログインしているユーザー自身のメールアドレスとパスワードを変更することが可能です。

■変更

①「変更する」をクリックします。

ID	メールアドレス	備考
admin	ishikawa@so-ten.co.jp	変更する

②変更のある項目を入力して「登録する」をクリックします。

ID	メールアドレス	備考
admin	ishikawa@so-ten.co.jp	変更する

ID	admin
パスワード	<input type="password"/>
パスワード確認	<input type="password"/>
メールアドレス	ishikawa@so-ten.co.jp
備考	<input type="text"/>

登録する

4. LogVillage の運用

4-1. LogVillage の再起動

LogVillage マネージャ、ポーリングサーバを強制終了、再起動は以下の手順にて行ってください。

■ LogVillage マネージャ

<終了手順>

- ① [コントロールパネル] → [サービス] から、下記のサービスを順に停止します。
 - 1) LV_M_MonitorSrv
 - 2) LV_ManagerServer
 - 3) Apache2
 - 4) Embedded Database - LOGVILLAGE2

<起動手順>

手動で終了した場合、以下の手順で起動を行ってください

OS を再起動した場合は自動起動されますので以下の手順は不要です。

- ① [コントロールパネル] → [サービス] から、下記のサービスを順に開始します。
 - 1) Apache2
 - 2) Embedded Database - LOGVILLAGE2
 - 3) LV_M_MonitorSrv
- ③ 「LV_M_MonitorSrv」 起動後、「LV_ManagerServer」 が開始される事を確認します。

■ LogVillage ポーリングサーバ

<終了手順>

- ① [コントロールパネル] → [サービス] から、下記のサービスを停止します。
LV_P_MonitorSrv
- ② [タスクマネージャ] → [プロセス] から、下記のプロセスを順に選択し、「プロセスの終了」をクリックします。
 - 1) LV_TaskTray.exe
 - 2) LV_PollingServer.exe

<起動手順>

- ① [コントロールパネル] [サービス] から、下記のサービスを起動します。
LV_P_MonitorSrv
- ② [タスクマネージャ] → [プロセス] にて、「LV_PollingServer.exe」が表示（起動）されることを確認します。
- ③ windowss スタートメニューから、「LV_TaskTray(PS)」を起動

4-2. 設定ファイル

以下の設定ファイルのコマンド編集により、LogVillage の動作を最適化することができます。
LogVillage の動作不良を起こす場合がありますので、コマンドの編集を行う際はご注意ください。
尚、設定ファイルの編集を行った場合、必ず LogVillage マネージャ、または LogVillage ポーリングサーバの再起動を実施ください。(再起動手順は、「4-1. LogVillage の再起動」をご参照ください。)
再起動を実施するまでは編集内容が動作に反映しませんのでご注意ください。

■LogVillage マネージャ

1) LogVillage マネージャ設定ファイル			
内容		LogVillage マネージャの詳細動作を設定します。	
場所 *1		C:¥Program Files (x86)¥SO-TEN¥LogVillage¥Manager	
ファイル名		Config.ini	
設定の適用方法		編集後、Logvillage マネージャを再起動(補足資料をご参照ください)	
コマンドの内容(お客様にて変更可能なコマンドのみ記載しています)			
コマンド	フォー マツト	パラメ ータ	説明
[Correspondence Timing]			コメント行
[ModuleTiming]			セクション名
ReStartTiming	10 進	24	LogVillage マネージャ起動後 24 時間毎に再起動(標準値)
		1~24	LogVillage マネージャ起動後設定時間(単位:時間)毎に再起動
		0	再起動なし
[CustomSetting]			セクション名
DoEventLogInfo	10 進	0	情報レベルのイベントログを保管する
		1	情報レベルのイベントログを保管しない(標準値)
DoNotUPPERString	10 進	0	DB 格納時に大文字変換する(標準値) *1
		1	DB 格納時に大文字変換しない
RefreshEventLog	10 進	0	イベントログ(セキュリティ)が管理対象 PC に保管されている場合 ※本パラメータが無い場合はデフォルト値"0"となります。
		1	イベントログ(セキュリティ)が再起動時に全て削除される場合

*1: デフォルトインストールの場所を記載していますので、変更している場合は読み替えてください。

■LogVillage ポーリングサーバ

1) LogVillage ポーリングサーバ設定ファイル			
内容		LogVillage ポーリングサーバの詳細動作を設定します。	
場所 *1		C:\Program Files (x86)\¥SO-TEN¥LogVillage¥PServer	
ファイル名		Config.ini	
設定の適用方法		編集後、LogVillage ポーリングサーバを再起動 (補足資料をご参照ください)	
コマンドの内容(お客様にて変更可能なコマンドのみ記載しています)			
コマンド	フ ォ ー マ	パラメータ	説明

	ット		
[Correspondence Timing]			コメント行
[ModuleTiming]			セクション名
ReStartTiming	10 進	24	LogVillage ポーリングサーバ起動後 24 時間毎に再起動(標準値)
		1~24	LogVillage ポーリングサーバ起動後設定時間(単位:時間)毎に再起動
		0	再起動なし
ADUser	10 進	0	ドメインユーザアカウント情報を取得しない。
		1	ドメインユーザアカウント情報を取得する。(標準値)
[Options]			セクション名
EventLog	10 進	0	windows イベントログ(セキュリティ)のログオン、ログオフ情報以外の取得条件 セキュリティログを取得しない(標準値)
		1	ANONYMOUS LOGON 以外のセキュリティログを取得する
		2	セキュリティログ情報を全て取得する
[SSL]			セクション名
SSLIsOn *2	10 進	0	マネージャと http 通信で接続(標準値)
		1	マネージャと https(SSL)通信で接続
[Thread] *3			セクション名
LV_CLS	10 進	1	管理対象 PC 起動確認モジュールの最大同時スレッド数
LV_SVC	10 進	4	サービス情報取得モジュールの最大同時スレッド数
LV_VIR	10 進	1	ウイルス定義ファイル情報取得モジュールの最大同時スレッド数
LV_WMI	10 進	4	インベントリ情報取得モジュールの最大同時スレッド数
LV_APP	10 進	1	App 情報取得モジュールの最大同時スレッド数
LV_DEV	10 進	4	デバイス情報取得モジュールの最大同時スレッド数
LV_WEB	10 進	4	web 閲覧履歴取得モジュールの最大同時スレッド数
LV_PFM	10 進	4	パフォーマンス情報取得モジュールの最大同時スレッド数
LV_EVT	10 進	4	イベントログ取得モジュールの最大同時スレッド数
LV_FIL	10 進	4	ファイル情報取得モジュールの最大同時スレッド数
LV_SETUP	10 進	4	timeKeeper 機能モジュールの最大同時スレッド数
[Initial]			セクション名
Scope	文字	day	初回ログ収集は、当日データまで遡って取得(標準値)
		all	管理対象 PC に保存されている全てのデータまで遡って取得
		month	当月まで遡って取得
		year	当年まで遡って取得
[NetScan]			セクション名
WinPort	10 進	3389	デフォルトでは本セクションは含まれていませんので追加ください。 ネットワークスキャンで、OS 判定処理でリモートデスクトップ接続の可否を判定するためのポート番号を記述します。 本セクションが無い場合、3389 番ポートのみに接続可否確認を行います。 3389 以外のポートも確認する場合、以下のように

			カンマ区切りで複数ポート番号を記述します。 3389,33389
[Inventory]			
LinuxLongFormat	10 進	0	Linux のソフトウェア名取得のオプション設定 %{name} ※本パラメータが無い場合はデフォルト値"0"となります。
		1	%{name} . %{arch}
Span	10 進	300	管理対象 PC 設定のアクセス名を IP アドレスとした場合に、当該管理対象 PC のコンピュータ名を取得するタイミング(秒)

*1: デフォルトインストールの場所を記載していますので、変更している場合は読み替えてください。

*2: https 接続を行う場合、その他ポーリングサーバや web サーバ(Apache)の設定変更が必要となります。

*3: 最大同時スレッド数を増やすことで1周期で取得できるログ情報が高速化されます。

但し、サーバやネットワークの負荷が増加しますので、パフォーマンスを確認のうえパラメータを設定ください。

1 項目の設定の最大値は「96」となり、[Thread]セクション内の全項目のスレッドの合計数の最大を 200 以下とする必要があります。

4-3. LogVillage の動作ログ

以下の動作ログが蓄積されており、弊社がサポートをご提供する際にご送付いただく場合がございます。

■LogVillage マネージャ

1) LogVillage マネージャ動作ログ	
内容	ポーリングサーバからアップロードされたログ情報ファイルの DB への取り込み、アラート判定等、LogVillage マネージャ全体の動作ログが蓄積されます。
場所 *1	C:\Program Files (x86)\SO-TEN\LogVillage\Manager\logs
ファイル名	(最新) LV-M-LOG.txt (過去) LV-M-LOG[最終更新日時].txt
蓄積期間	1ヶ月 (経過後自動削除)

*1: デフォルトインストールの場所を記載していますので、変更している場合は読み替えてください。

■LogVillage ポーリングサーバ

1) LogVillage ポーリングサーバ動作ログ	
内容	管理対象 PC からのログ情報取得、マネージャとの通信等、LogVillage ポーリングサーバ全体の動作ログが蓄積されます。
場所 *1	C:\Program Files (x86)\SO-TEN\LogVillage\PServer\Logs
ファイル名	(最新) LV-PS-LOG.txt (過去) LV-M-LOG[最終更新日時].txt
蓄積期間	1ヶ月 (経過後自動削除)

*1: デフォルトインストールの場所を記載していますので、変更している場合は読み替えてください。

2) LogVillage ポーリングサーバ ネットワークスキャン動作ログ	
内容	ネットワークスキャン機能が有効な場合、ネットワークスキャンの動作ログが蓄積されます。
場所 *1	C:\Program Files (x86)\SO-TEN\LogVillage\PServer\NetscanLog
ファイル名	(最新) netscan.log (過去) netscan[最終更新日時].log
蓄積期間	1ヶ月 (経過後自動削除)

*1: デフォルトインストールの場所を記載していますので、変更している場合は読み替えてください。

4-4. LogVillage2.0 のシステム監視

LogVillage2.0 が正常に動作を行っているかを監視する場合、以下のサービス、プロセスの監視を行ってください。

■LogVillage マネージャ

監視対象	区分	正常な状態	内容
LV_ManagerServer	サービス	実行中	ポーリングサーバからアップロードされたログ情報のDB ストアーを行うプログラム
LV_M_MonitorSrv	サービス	実行中	LV_ManagerServer を起動するプログラム
Embedded Database - LOGVILLAGE2	サービス	実行中	データベース(MySQL)
Apache2	サービス	実行中	web サーバ

■LogVillage ポーリングサーバ

監視対象	区分	正常な状態	内容
LV_PollingServer.exe	プロセス	実行中	ログ収集、マネージャとの通信を行うプログラム
LV_P_MonitorSrv	サービス	実行中	LV_PollingServer.exe を起動するプログラム

4-5. 管理対象 PC 環境変更時の対応

	変更内容	対応方法
1	管理者アカウントのパスワードが変更	「管理対象 PC」画面より、当該管理対象 PC のパスワード変更が必要となります。
2	管理対象 PC のコンピュータ名が変更	管理対象 PC のアクセス名にコンピュータ名を登録している場合は、「管理対象 PC」画面よりアクセス名を変更後のコンピュータ名に変更が必要となります。 IP アドレスで登録の場合は変更不要です。
3	管理対象 PC を設置しているネットワークセグメントが変更	変更後のネットワークセグメント上の他の PC のログ収集が行われている場合は作業不要です。 継続してログ収集が行われていることをご確認ください。 新規ネットワークセグメントの場合、ポーリングサーバからの接続が行えるかの確認が必要となります。
4	故障、更新等でハードウェアを交換	同一コンピュータ名、同一 IP アドレスの場合は作業不要です。 但し、ワークグループ環境の場合、導入時に行った管理対象 PC の設定変更を再度行う必要があります。

4-6. LogVillage2.0 のバックアップ&リストア

「LogVillage2.0」のバックアップ、リストア手順を記載しています。

リストア手順は、LogVillage マネージャ、LogVillage ポーリングサーバがバックアップ実行時と同じホスト名、IP アドレスのサーバへの復元を前提としています。

バックアップ場所は、以下の標準インストール場所でご説明しています。

インストール時に変更している場合は、変更後のフォルダに読み替えてください。

内容	標準インストール場所	本マニュアルでの記載
LogVillage マネージャインストールフォルダ	C:\Program Files (x86)\SO-TEN\LogVillage\Manager	[LV-MGR-Inst]
Apache2 インストールフォルダ	C:\Program Files (x86)\SO-TEN\LogVillage\Apache2	[LV-Apache-Inst]
MySQL インストールフォルダ	C:\Program Files (x86)\SO-TEN\LogVillage\MySQL	[LV-mysql-Inst]
spool フォルダ作成場所	C:\spool	[LV-spool]
LogVillage ポーリングサーバインストールフォルダ	C:\Program Files (x86)\SO-TEN\LogVillage\Pserver	[LV-PS-Inst]

■バックアップ手順

1) LogVillage 設定ファイルをバックアップ

内容	バックアップ場所	バックアップ対象ファイル名
LogVillage マネージャ設定ファイル	[LV-MGR-Inst]	Config.ini
spool フォルダ	[LV-spool]	フォルダ全体
LogVillage ポーリングサーバ設定ファイル	[LV-PS-Inst]	Config.ini
	[LV-PS-Inst]\temp	フォルダ全体
	[LV-PS-Inst]\conf	フォルダ全体
	[LV-PS-Inst]\TaskTray	Connect.ini
	[LV-PS-Inst]\TaskTray	log.ini

※マネージャ⇄ポーリングサーバ間を https 通信に変更している場合は、以下もバックアップ

内容	バックアップ場所	バックアップ対象ファイル名
Apache 設定ファイル	[LV-Apache-Inst]\conf	httpd.conf
	[LV-Apache-Inst]\conf	httpd-ssl.conf
	[LV-Apache-Inst]\conf	server.csr
	[LV-Apache-Inst]\conf	server.key
	[LV-Apache-Inst]\conf	server.crt

※server.csr、server.key、server.crt は SSL 設定時に変更している場合は変更後の名前に読み替えてください。

2) データベースをバックアップ

以下の手順でデータベース(MySQL)がオンライン状態で DUMP を取得できます。

- ① コマンドプロンプトを起動
- ② [LV-mysql-Inst]¥bin に移動
- ③ 以下のコマンドを実行

```
mysqldump -u root --password=[パスワード *1] logvillage -R --single-transaction >
"[任意のファイル名.dump]"
```

*1:パスワードは、お手数ですが「5. お問い合わせ」に記載のサポートセンターまでお問合せください。

■リストア手順

<LogVillage マネージャのリストア手順>

- 1) LogVillage マネージャをインストール。
- 2) LogVillage マネージャを停止(「4-1. LogVillage の再起動」をご参照ください)
- 3) バックアップした LogVillage マネージャの設定ファイルを上書きコピー
・[LV-MGR-Inst]¥Config.ini

※マネージャ⇄ポーリングサーバ間を https 通信に変更している場合は、以下の 4)を実施ください。

- 4) バックアップした Apache 設定ファイルを上書きコピー
・[LV-Apache-Inst]¥conf¥httpd.conf
・[LV-Apache-Inst]¥conf¥extra¥httpd-ssl.conf
・[LV-Apache-Inst]¥conf¥server.csr
・[LV-Apache-Inst]¥conf¥server.key
・[LV-Apache-Inst]¥conf¥server.crt

※server.csr、server.key、server.crt は SSL 設定時に変更している場合は変更後の名前に読み替えてください。

- 5) バックアップした spool フォルダを上書きコピー
・[LV-spool]
- 6) LogVillage マネージャを開始(「4-1. LogVillage の再起動」をご参照ください)
- 7) データベースを復元

以下の手順でバックアップで作成した DUMP からデータベース(MySQL)を復元します。

- ① コマンドプロンプトを起動
- ② [LV-mysql-Inst]¥bin に移動
- ③ 以下のコマンドを実行

```
mysql -u root --password=[パスワード *1] logvillage < [バックアップファイル名]
```

*1:パスワードは、お手数ですが「5. お問い合わせ」に記載のサポートセンターまでお問合せください。

また、1週間のローテートで dump を取得するバッチファイルのご提供も行っておりますので、必要な場合は合わせてお問合せください。

<LogVillage ポーリングサーバのリストア手順>

- 1) LogVillage ポーリングサーバをインストール
- 2) LogVillage ポーリングサーバを停止(「4-1. LogVillage の再起動」をご参照ください)
- 3) バックアップした LogVillage ポーリングサーバの設定ファイル/フォルダを上書きコピー
 - ・[LV-PS-Inst]¥Config.ini
 - ・[LV-PS-Inst]¥temp フォルダ
 - ・[LV-PS-Inst]¥conf フォルダ
 - ・[LV-PS-Inst]¥TaskTray¥Connect.ini
 - ・[LV-PS-Inst]¥TaskTray¥log.ini
- 4) LogVillage ポーリングサーバを開始(「4-1. LogVillage の再起動」をご参照ください)

4-7. 常駐エージェント用更新プログラムの設置

管理対象 PC に LogVillage 常駐エージェントをインストールしている場合、以下の場所に更新プログラム一式を設置することで常駐エージェントの自動アップデートを行うことができます。

・常駐エージェント更新プログラムの保管場所

C:¥Program Files (x86)¥SO-TEN¥LogVillage¥Apache2¥htdocs¥update¥agent

※上記は標準インストール場所でご説明しています。

インストール時に変更している場合は、変更後のフォルダに読み替えてください。

※更新プログラムは、必要に応じて別途蒼天よりご案内いたします。

5. お問い合わせ

本製品に対するご意見、ご質問はメール、TEL、FAXにて下記までお問い合わせ下さい。
お問い合わせの内容によっては、ご返答に多少お時間を頂戴する場合がありますので、予めご了承ください。

〒135-0064 東京都江東区福住 1-14-4 山崎ビル 1F
株式会社蒼天 サポートセンター

e-mail : support@so-ten.co.jp
TEL : 03-5809-8406
FAX : 03-5809-8495
受付・対応時間 : 月～金曜日（祝祭日、年末年始休暇除く）
10:00～17:00

お問い合わせの際、以下の内容をご記載下さいますようお願い申し上げます。

お客様番号

* 「システム設定」⇒「ライセンス登録・更新」画面に表示されます。

会社名（団体、学校名）、ご部署名

ご担当者名

メールアドレス

電話番号

FAX 番号

お問い合わせの内容（できるだけ詳しくお書き下さい）

実行環境

コンピュータメーカー名：

型番：

メモリー容量：

ハードディスク容量または種類：

OS バージョン：

サービスパック：



株式会社 蒼天

〒135-0064 東京都江東区福住 1-14-4 山崎ビル 1F
<http://www.so-ten.co.jp/>

改訂履歴 ※PDF ファイルには、このページを入れない事！

Revision	発行日	改訂履歴
MU-20-20091113	2009 年 11 月 13 日	3.1. ポーリングサーバーの設定とステータスの画面キャプチャを変更 3.2. グループ毎の設定に保有ライセンス登録を追加 3.3. アラートポリシーの一部にステータスを追加 プロセス: 定期を追加 アプリケーション: ステータスの記述を追加 補足資料に Mgr と PS の再起動方法を追加
MU-20-20101122	2010 年 11 月 22 日	2.3.1 PC 資産管理台帳に注意点を追加追加 ソフトウェア台帳画面キャプチャ変更 2.4.3 ログオン・オフ履歴に win7, 2008 を追加 管理対象フォルダ設定に Config.ini の情報を追加 保有ライセンスの画面キャプチャなどを変更 3.3 アラートポリシーの設定 禁止デバイスの接続、アプリケーション・インストールの検知の画面キャプチャなどを変更
MU-23-20120220	2012 年 2 月 20 日	画面デザイン変更に伴う修正 ファイル管理機能変更に伴う修正 システム設定の項目名変更、並び順の変更に伴う修正
	2012 年 4 月 16 日	2.4.3 ログオン・オフ履歴 ログオフ(例外)について追記。
MU-23-20120809	2012 年 8 月 9 日	補足資料 DB サービス名を「Embedded Database - LOGVILLAGE2」に変更
MU-23-20120918	2012 年 9 月 18 日	3.1.3. 管理対象 PC 自動設定ツールの内容を修正 ■登録した管理対象 PC のログ接続確認 を追加
MU-23-20161026	2016 年 10 月 26 日	3.3.2. 禁止印刷ファイル/枚数制限 枚数アラートの内容を修正
MU-23-20161220	2016 年 12 月 20 日	全般 新 UI 画像に変更 3.3.4 禁止デバイス接続 部分一致設定を追記
MU-23-20170927	2017 年 10 月 2 日	2.5. ネットワークスキャン 3-1-9. ネットワークスキャン設定 3-1-10. ネットワークスキャンアラート設定 を追加
MU-23-20171211	2017 年 12 月 13 日	補足説明を削除 ※MGR, PS の再起動手順を「4-1. LogVillage の再起動」に記載
MU-23-20171211		「4. LogVillage の運用」を追加
MU-23-20171222	2017 年 12 月 22 日	「3. 3. 1 インベントリアラート設定」を追加

	2017 年 12 月 22 日	「４－７．常駐エージェントの更新プログラム設置」を追加
	2017 年 12 月 27 日	「3.1.3 管理対象 PC」CSV ファイル仕様を修正
MU-26-20210618	2021 年 6 月 18 日	「3.1.3 管理対象 PC」アカウント要件、SSH 公開鍵認証を追加
MU-26-20210625	2021 年 6 月 25 日	「3.1.3 管理対象 PC」パスワード要件を修正