LogVillage 2.0 Lite

運用マニュアル

V2.3J

株式会社ワッセイ・ソフトウェア・テクノロジー

logVillage2.0　運用マニュアル

revision　:　MUL-23-20171215

*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。

株式会社ワッセイ・ソフトウェア・テクノロジー
〒540-0035
大阪市中央区釣鐘町１丁目3-4 ダイクウビル2F
TEL: 06-6944-8901　FAX: 06-6944-8885
http://www.wasay.co.jp

目次

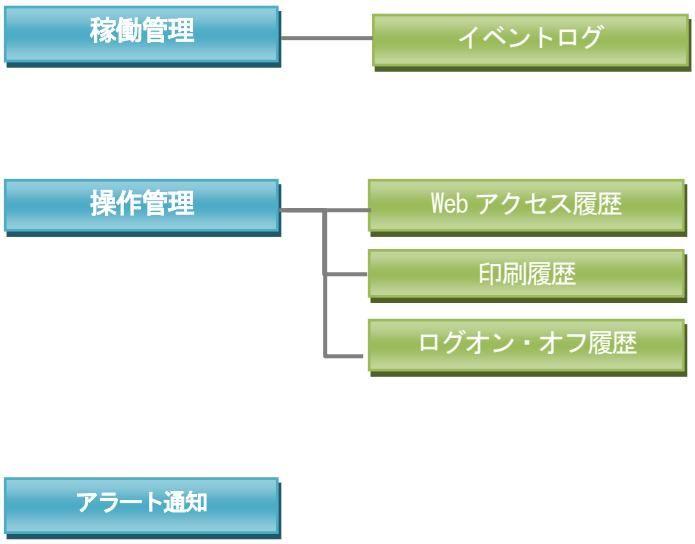
1. LogVillage2.0 Lite 機能概要 5
1．1 メニュー系統図 6
1．2 機能一覧 7
1．2．1 LogVillage の主な機能 7
1．2．2 LogVillage のシステム設定 8
1．3 グループとLogVillage ユーザーの関係図 10
2. 機能説明 11
2．1 トップ画面 11
2．1．1 ログイン画面 11
2．1．2 ログイン後の画面 12
2．2 稼働管理 13
2．2．1 イベントログ 13
2．3 操作管理 17
2．3．1 Web アクセス履歴 17
2．3．2 印刷履歴 20
2．3．3 ログオン･オフ履歴 23
2．4 アラート通知履歴 28
3. システム設定 31
3．1 共通設定 32
3．1．1 ポーリングサーバ 32
3．1．2 グループ 35
3．1．3 管理対象 PC 37
3．1．4 トップ画面 43
3．2 グループ単位設定 44
3．2．1 LogVillage ユーザー 44
3．2．2 ログ収集スケジュール 47
3．3 アラートポリシー設定 49
3．3．1 禁止 Web サイトアクセス 51
3．3．2 禁止印刷ファイル/枚数制限 54
3．3．3 禁止アカウントログオン 57
3．3．4 指定イベントログ発生 59
3．4 運用管理 62
3．4．1 ライセンスの登録･更新 62
3．4．2 LogVillage へのログイン履歴 63
3．4．3 ユーザー情報変更 64
4. LogVillage の運用 65
4－1. LogVillage の再起動 65
4－2. 設定ファイル 66
4－3. LogVillage の動作ログ 69
4－4. LogVillage2.0 のシステム監視 70
4－5. 管理対象 PC 環境変更時の対応 71
4－6. LogVillage2.0 のバックアップ＆リストア 72

5. お問合せ 75

１．LogVillage2.0 Lite 機能概要

LogVillage2.0 Lite は、PC の管理ソフトウェアとして、操作ログ収集などを行います。
この章では、LogVillage2.0 Lite 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

・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。

■操作管理

・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。

■アラート通知履歴

アラート通知履歴を表示します。

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ないます。

・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。

■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。

■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

禁止アカウントでのログオンを設定します。

・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。

■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。

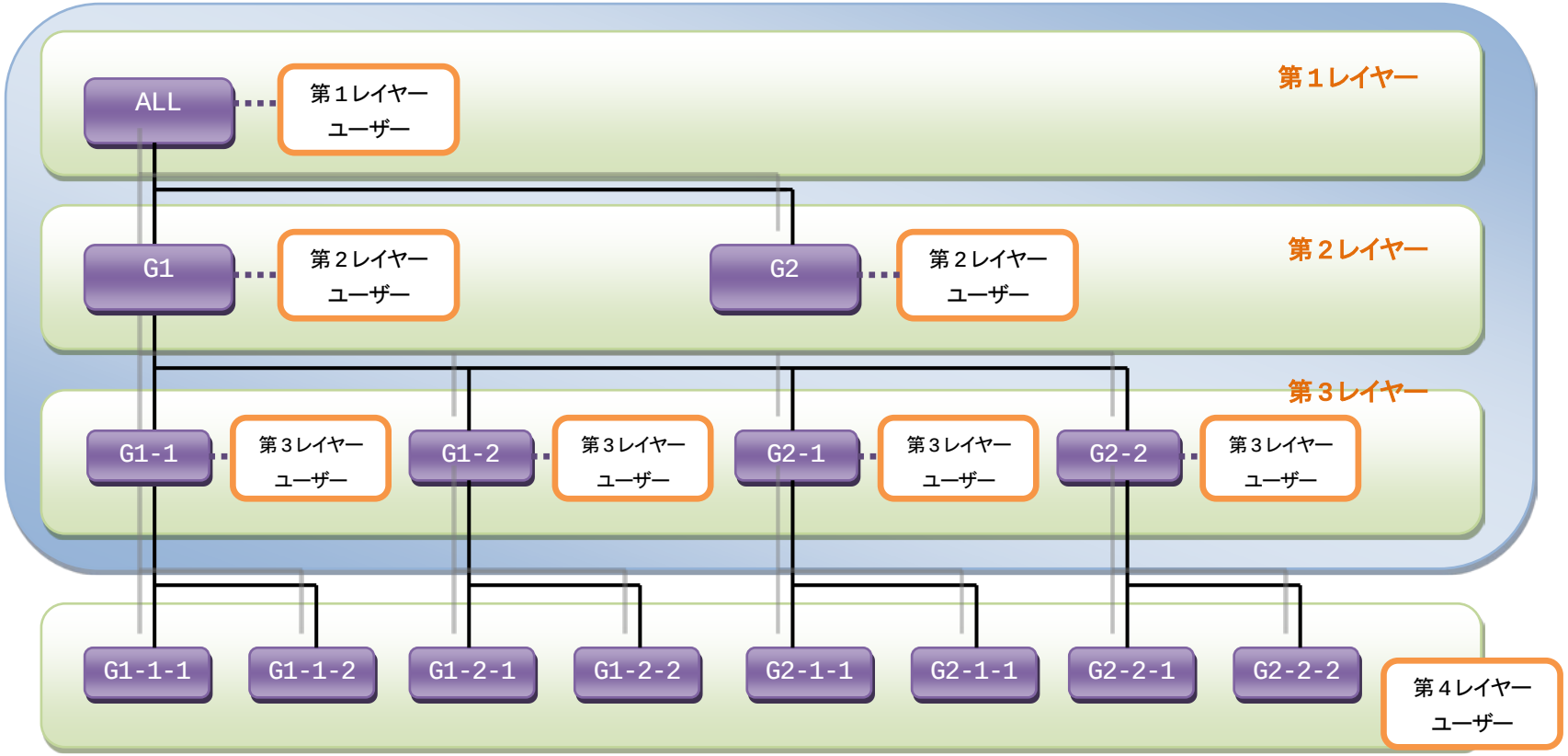
・LogVillage ログイン履歴

LogVillage へのログオン履歴を確認することができます。

・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　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

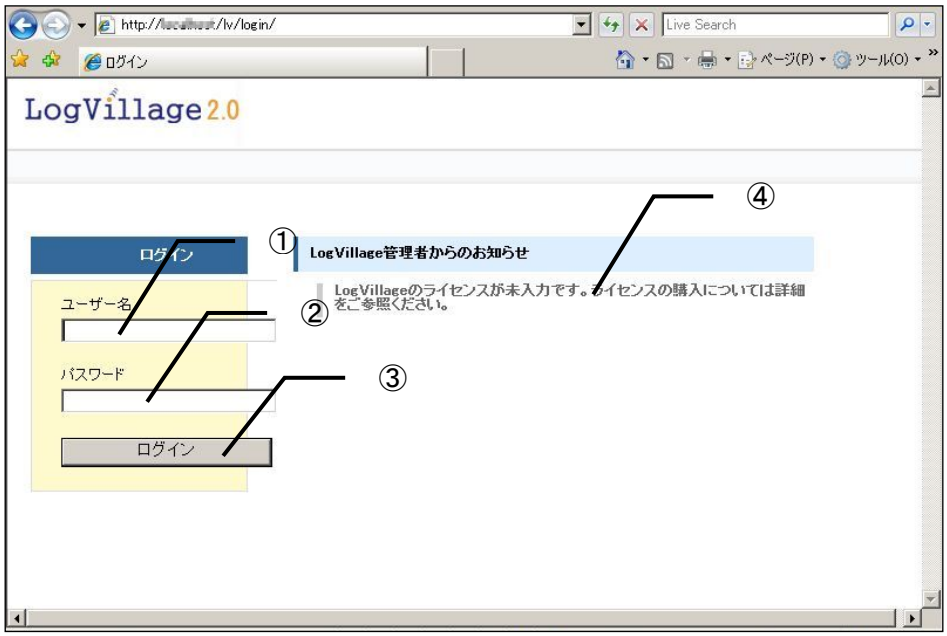
２．１．１　ログイン画面

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.43 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。

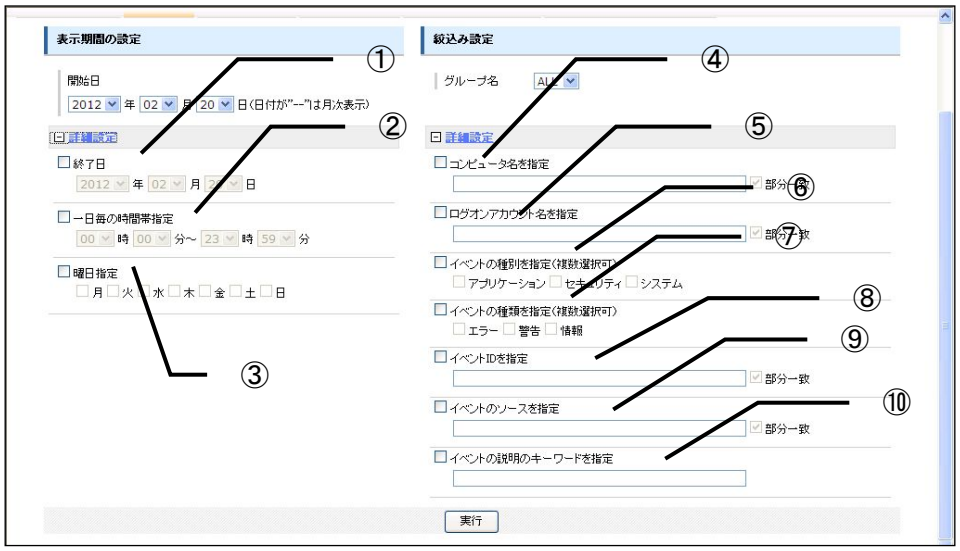
２．２　稼働管理

２．２．１　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。

■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）

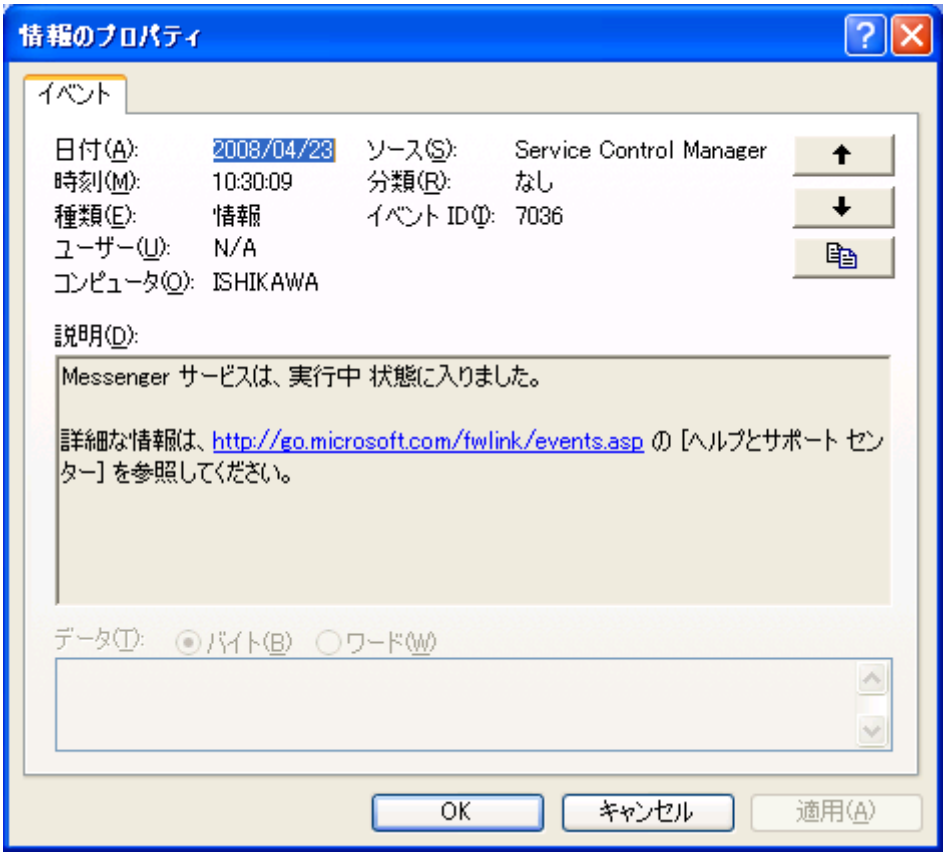
⑨イベントのソースを指定

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。- AML0x810x81 - 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: XX121 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 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: XX121 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	win2003-default	N/A	アプリケーション	エラー	439	ESENT	services (828) ファイル D:¥Installer¥PollingServer¥hisecws.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。- AMLI0x810x81 - 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
```

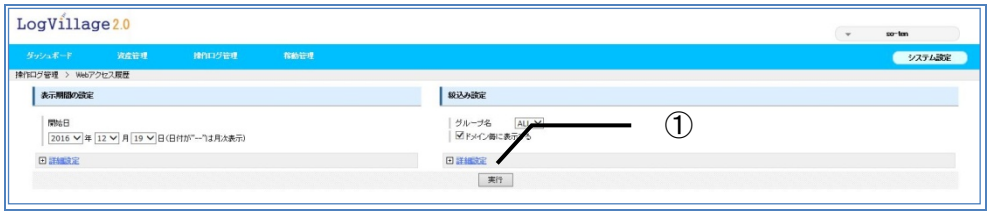
２．３　操作管理

ユーザーの操作ログ管理です。
」

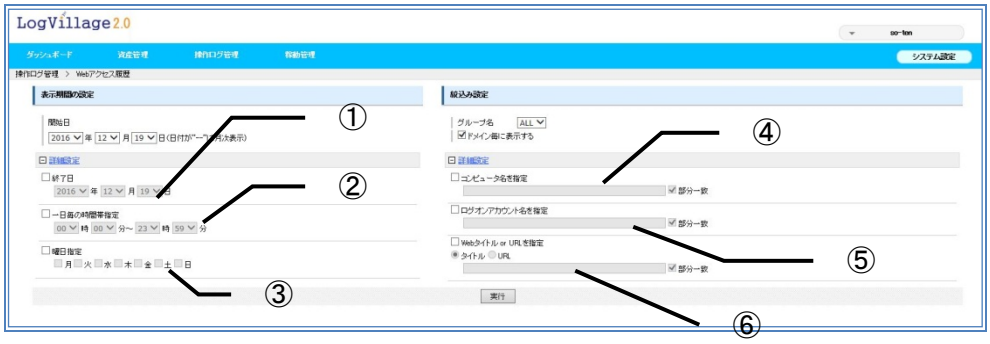
２．３．１　Web アクセス履歴

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。

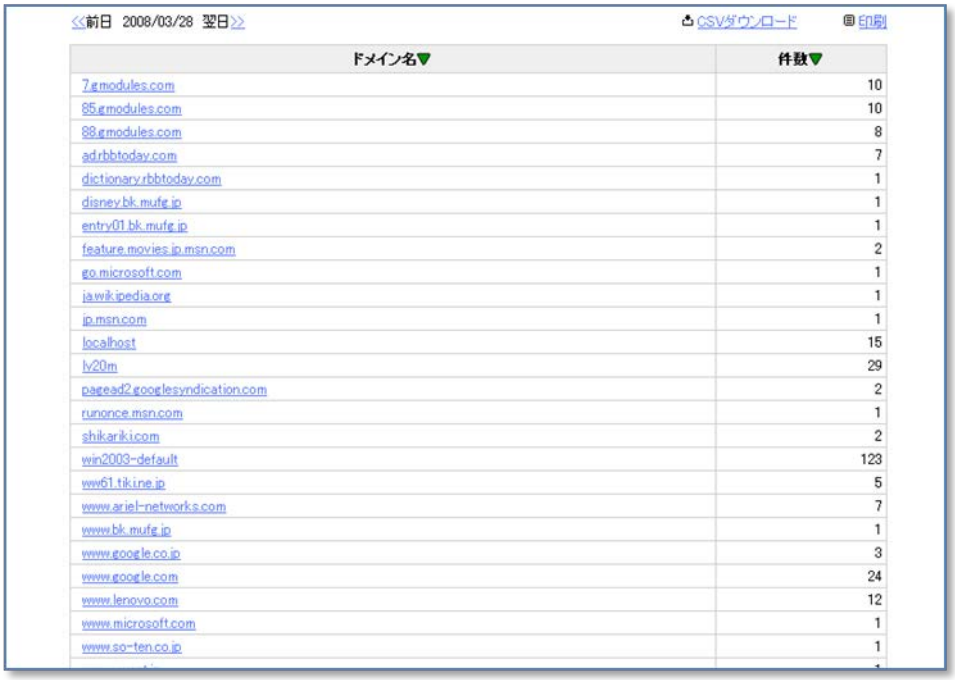


・表示期間の設定
①終了日
　　開始日と合わせて範囲指定することが可能です。

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



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
go.microsoft.com	1
ja.wikipedia.org	1
jp.msn.com	1
localhost	15
lv20m	29
pagead2.googlesyndication.com	2
runonce.msn.com	1
shikariki.com	2
win2003-default	123
ww61.tik.ine.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
        :
        :
```

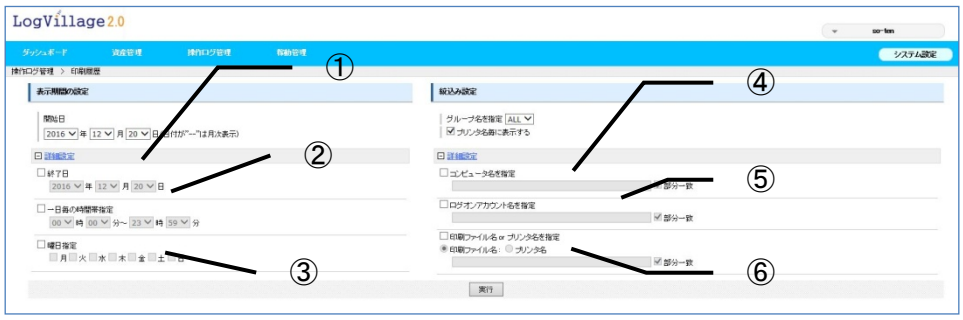
■印刷
画面の内容が印刷されます。

２．３．２　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。

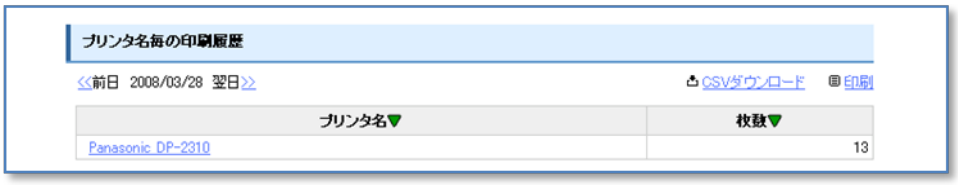
■詳細条件の設定
さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。



・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。

■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。

２．３．３　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。

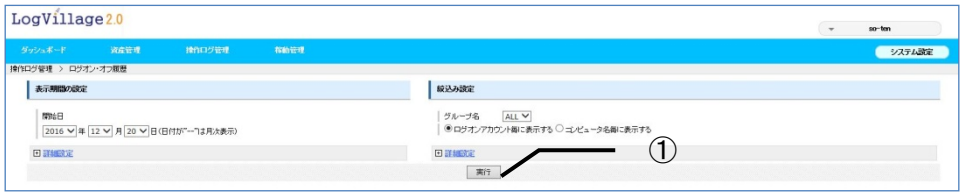
	PC 利用シーン			LogVillage2.0 でのログ情報	
1	8:50	PC 起動⇒ログオン	⇒	8:50	ログオン
	12:00	休止モード		18:30	ログオフ（正常）
	13:00	休止モード解除			
	18:30	PC シャットダウン			
2	8:50	PC 起動⇒ログオン	⇒	8:50	ログオン
	12:00	シャットダウン		12:00	ログオフ（正常）
	13:00	PC 起動⇒ログオン		13:00	ログオン
	18:30	PC シャットダウン		18:30	ログオフ（正常）
3	8:50	PC 起動⇒ログオン	⇒	8:50	ログオン
	10:00	スタンバイモード⇒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

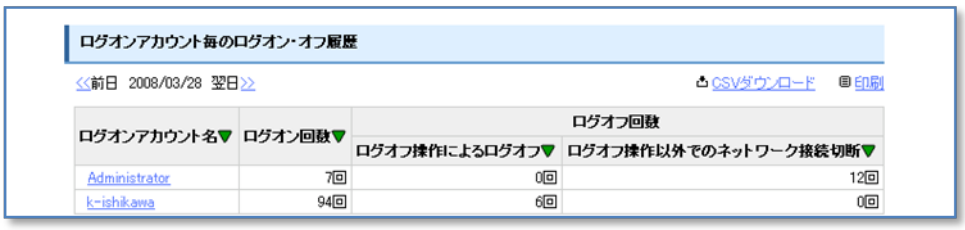
④コンピュータ名を指定

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）

■出力結果



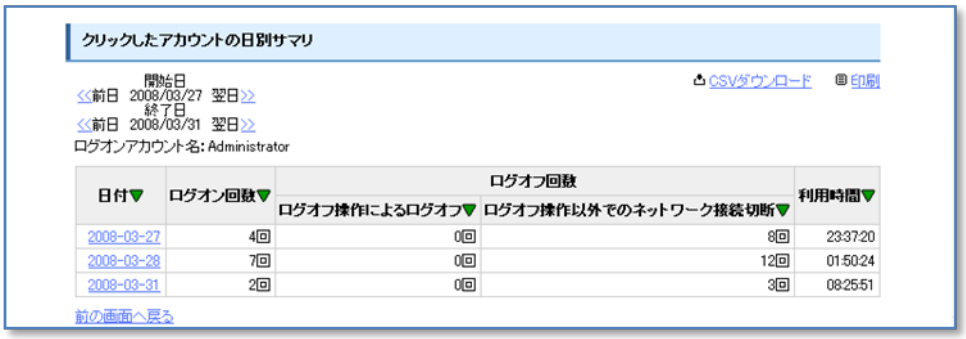
ログオンアカウント毎のログオン・オフ履歴

<<前日 2008/03/28 翌日>>　CSVダウンロード　印刷

ログオンアカウント名	ログオン回数	ログオフ回数	
		ログオフ操作によるログオフ	ログオフ操作以外でのネットワーク接続切断
Administrator	7	0	12
k-ishikawa	94	6	0

%UserProfile%¥AppData¥Local¥Google¥Drive

ログオンアカウントをクリックするとログオンアカウント毎の日別サマリの確認が可能です。



クリックしたアカウントの日別サマリ

開始日
<<前日 2008/03/27 翌日>>
終了日
<<前日 2008/03/31 翌日>>
ログオンアカウント名: Administrator

CSVダウンロード　印刷

日付	ログオン回数	ログオフ回数		利用時間
		ログオフ操作によるログオフ	ログオフ操作以外でのネットワーク接続切断	
2008-03-27	4	0	8	23:37:20
2008-03-28	7	0	12	01:50:24
2008-03-31	2	0	3	08:25:51

前の画面へ戻る

■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　アラート通知履歴

アラート通知履歴を表示します。

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。

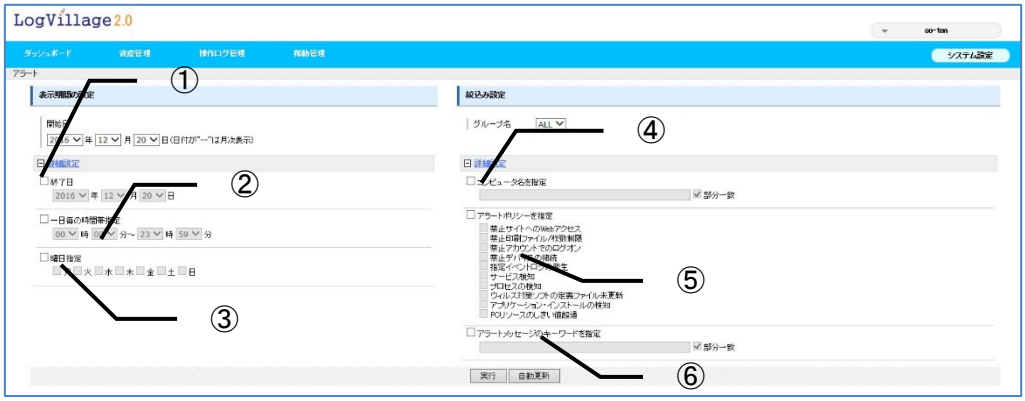
■詳細条件の設定
さらに条件を絞り込みたい場合は、詳細設定をクリックし詳細設定を開いて条件を設定してください。

・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
・ウィ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。

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。

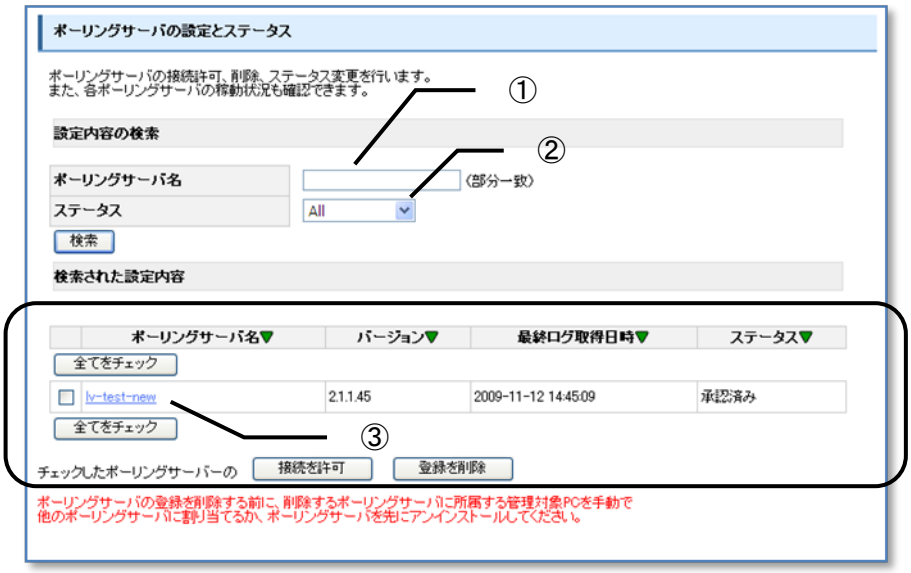
システム設定をクリックしたら表示されるプルダウンメニューより目的の設定項目を選択します。

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ーを確認・設定します。
接続されているポーリングサーバーが表示されます。

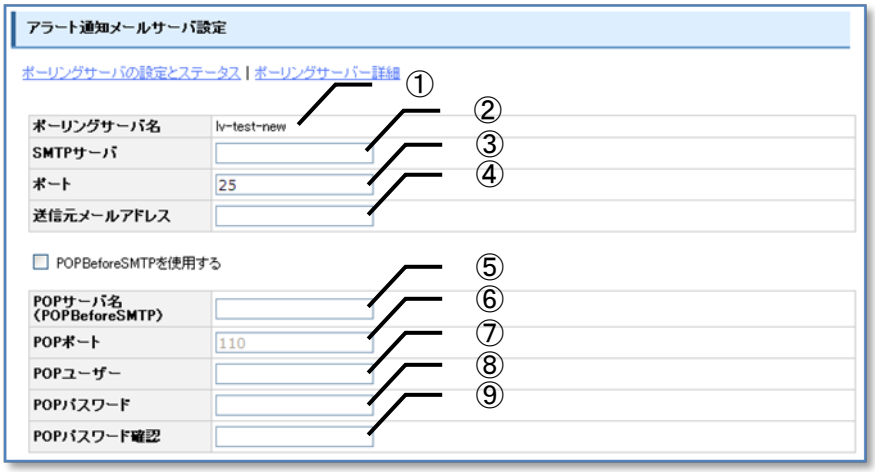
・ポーリングサーバー名
・ポーリングサーバーのバージョン
・最終ログ取得日時
　　ポーリングサーバーよりログを受け取った日時が示されます。
・ステータス
　　承認済　　マネージャーサーバーより認識され、管理対象 PC の割り当て待ちです。
　　接続許可待ち　ポーリングサーバーが承認待ちです。



・設定内容の検索
①ポーリングサーバー名
　　特定のサーバー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。

・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。



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
　　STMP 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

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

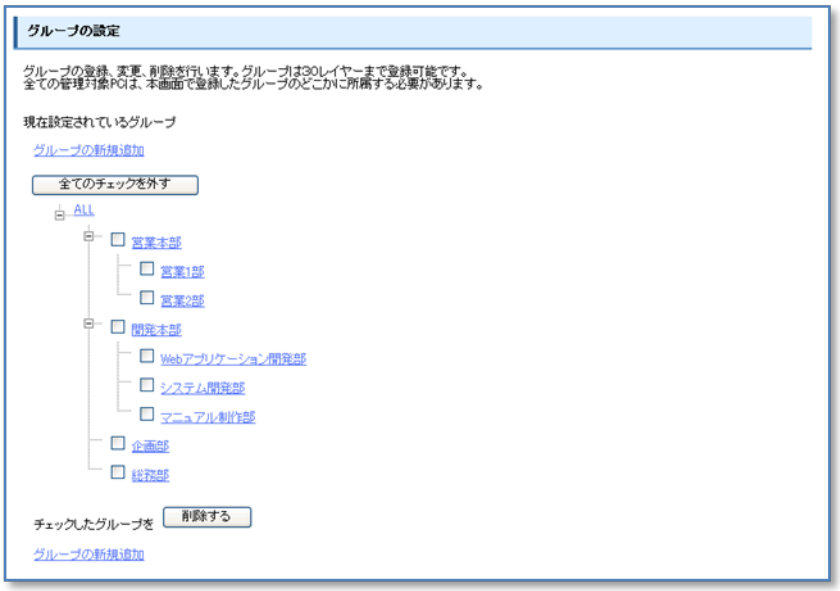
グループの登録、変更、削除を行ないます。

・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。

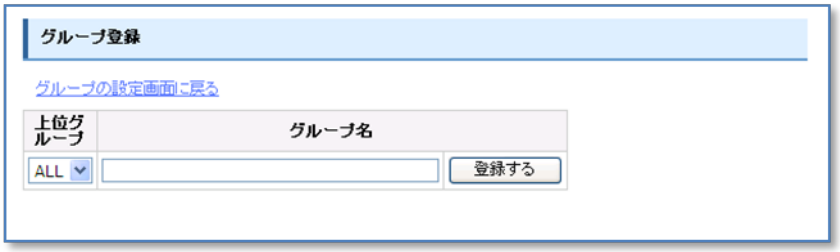
・階層構造
階層構造を持たせることができます。階層は 30 までとなります。

・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。



・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、設定ツール（ActiveX 版）、設定ツール（ダウンロード版）、csv によるインポートで行なうことができます。
管理対象 PC をポーリングサーバーに割り当てることにより、ポーリングサーバーのステータスが稼働中となります。

■手動登録
必要な情報をすべて手入力します。

・コンピュータ名（必須）
・ユーザー名（必須）
・パスワード（必須）
・グループ名（任意・未入力の場合は第一レイヤーグループ）
・ポーリングサーバー名（任意・未入力の場合は「自動」）
・ステータス（「稼働」または「停止」）

■自動設定ツール（オプション）による登録
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。

■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。

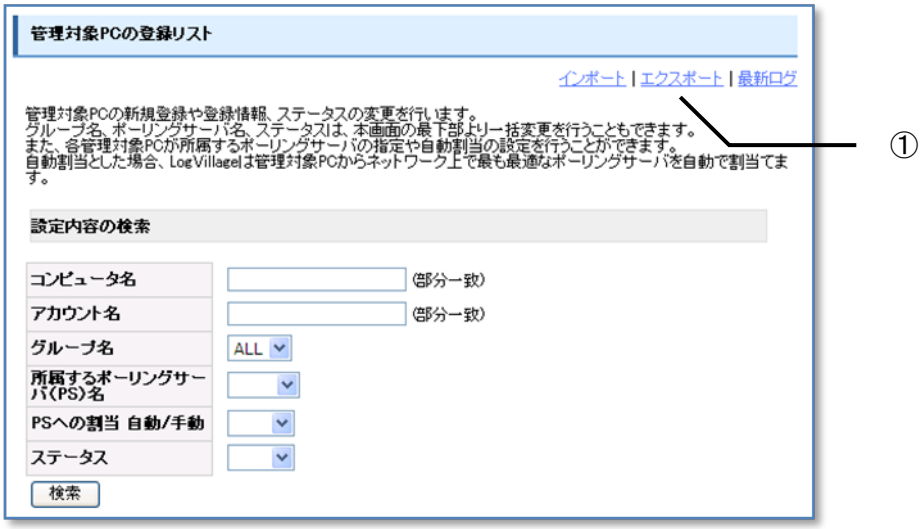
※フォーマット

項目名	記述法など
コンピュータ名	必須
ユーザー名	必須
パスワード	必須
グループ名	任意・未入力の場合は第一レイヤーグループ
ポーリングサーバー名	任意・未入力の場合は「自動」

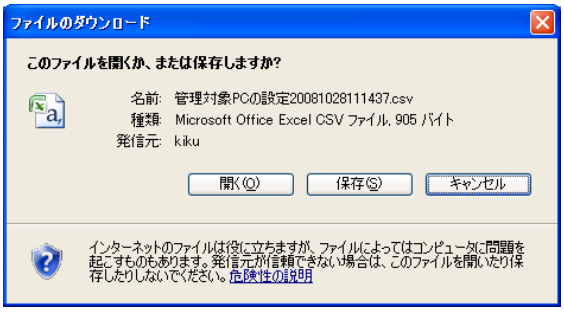
※ポーリングサーバー名の不一致、コンピュータ名重複の場合はエラーとなります。

○管理対象 PC のグループ名を一括で変更する方法（組織変更時など）

CSV インポートを行う際、インポート用 CSV ファイルにて、コンピュータ名の行のグループ名を　変更し、インポートを実行すると管理対象 PC のグループを一括で変更することができます。



①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。

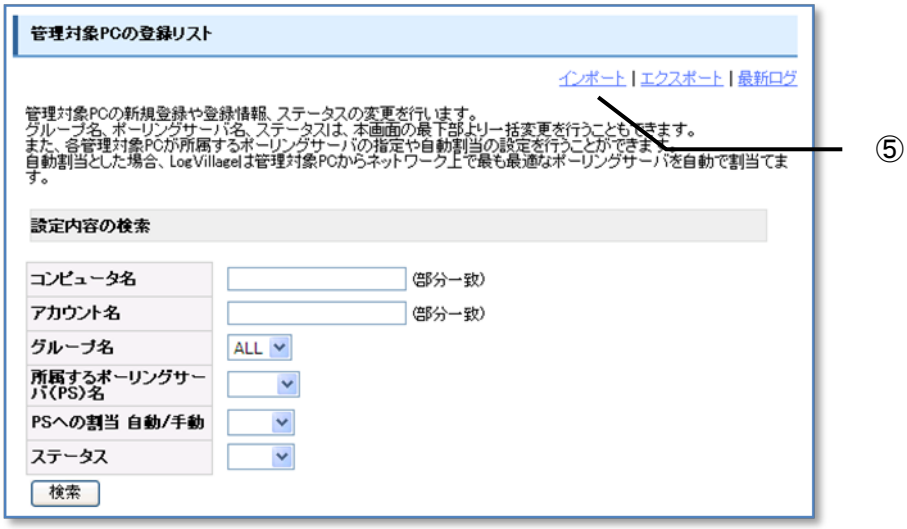
・管理対象 PC を新規登録する場合：
最後の行の後に、コンピュータ名、ユーザー名、パスワード、グループ名、所属するポーリングサーバー名を入力します。

*1　新た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「xxxxxxx」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。

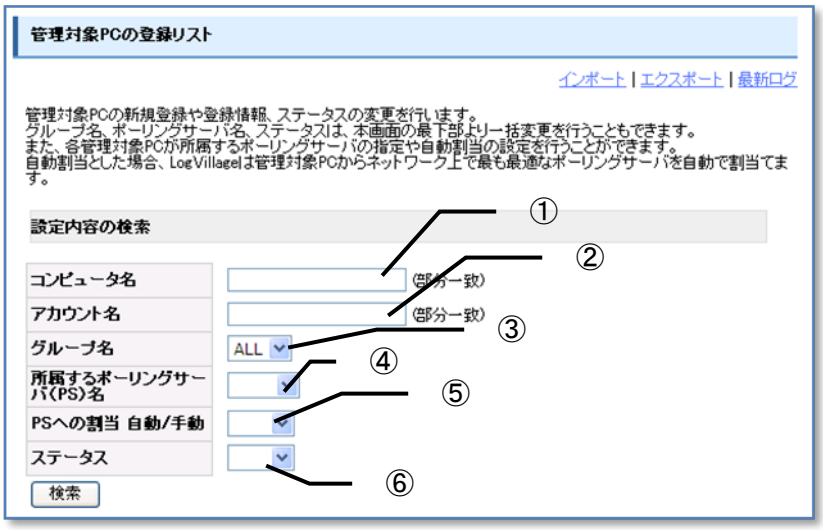
④インポート用 CSV ファイルを分割します。
一度に、インポートが行える CSV ファイルの行数は 300 行までです。
③で作成した CSV ファイルが 300 行（300 台）を超える場合、300 行以内の複数ファイルに分割を行ってください。



⑤［インポート］をクリックします。

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。
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。

■管理対象 PC の検索
管理用 PC 一覧の絞り込みが可能です。



・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ー（PS）名を指定
　　プルダウンでポーリングサーバー名を選択します。
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。

■変更・削除

・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、ポーリングサーバー名、ステータスを変更できます。

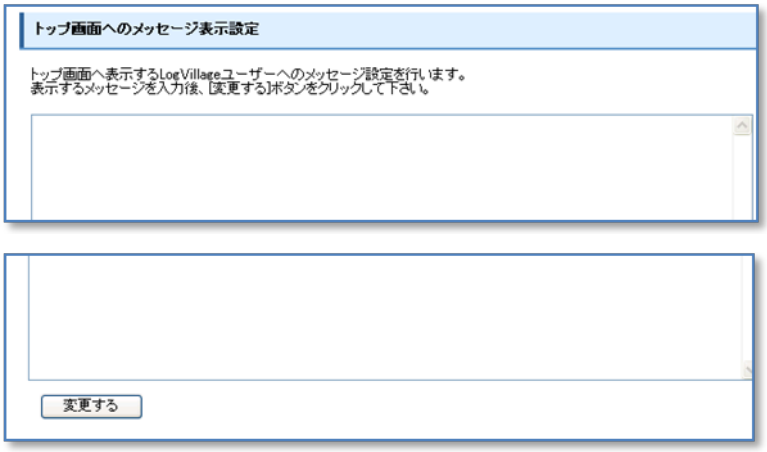
・削除
削除したい管理対象 PC をチェックし、「削除する」ボタンをクリックしてください。

■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 の設定変更後、以下の手順をご参照のうえ、接続確認を行って下さい。

・管理対象 PC 接続確認ツールのご利用手順
http://www.so-ten.co.jp/manual/lv20/
※上記 URL へアクセスすると、「LogVillage2.0 製品マニュアル」ページが表示されます。
“管理対象 PC 接続確認ツールのご利用手順”をご選択下さい。

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。

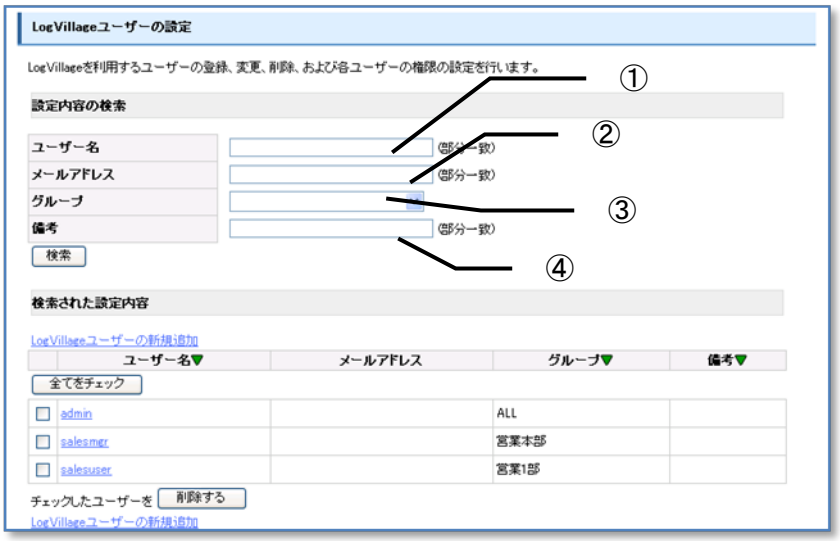


３．２　グループ単位設定

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。

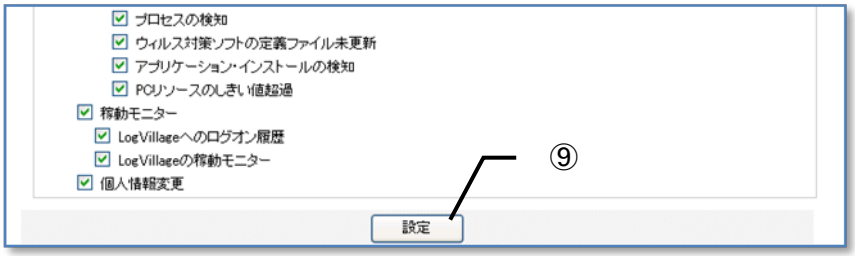


■設定内容の検索
①ユーザー名
　　特定のユーザー名に絞り込んで結果を出力することが可能です。（部分一致可）
②メールアドレス
　　特定のメールアドレスに絞り込んで結果を出力することが可能です。(部分一致可)
③グループ
　　特定の WindowsUpdate の内容に絞り込んで結果を出力することが可能です。(部分一致可)
④備考

■追加

①Logvillage 新規ユーザーの追加　をクリックします。

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。



⑨権限設定を変更・確認し「設定」ボタンをクリックします。

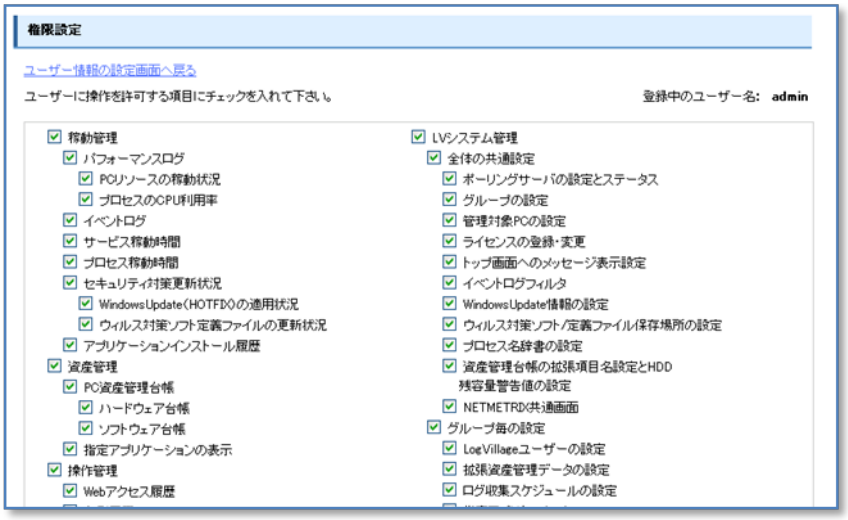
■変更

①該当ユーザー名をクリックします。

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

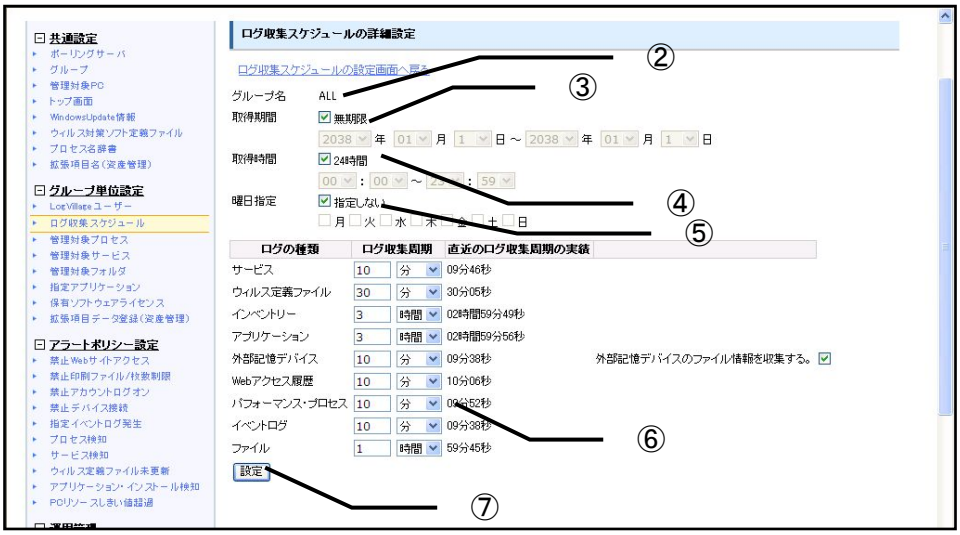


３．２．２　ログ収集スケジュール

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。

■追加

①スケジュールの新規追加　をクリックします。



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
・インベントリー
・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。

■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。

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。
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
	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

■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.32）

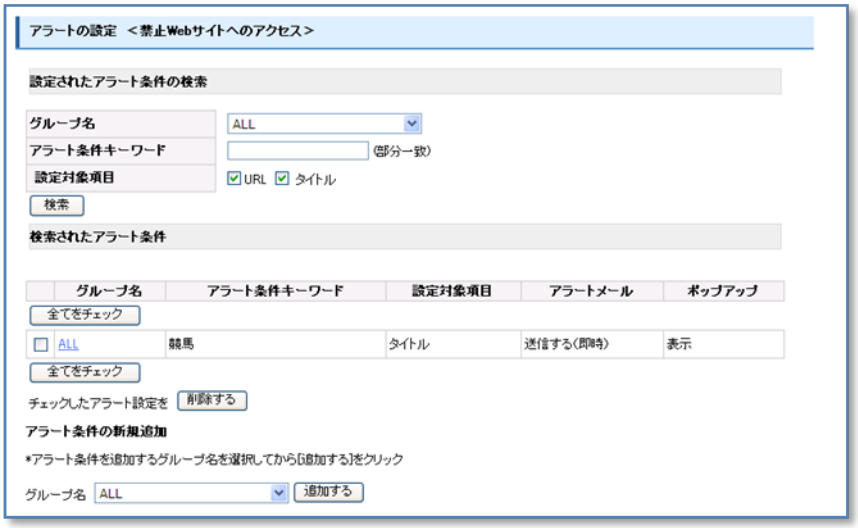
「下位グループのアラートメールを受け取る」にチェックが入っている場合
選択したグループ以下の下位グループにて発生したアラートメールも受信します。

■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　禁止 Web サイトアクセス

禁止 Web サイトを設定します。



■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

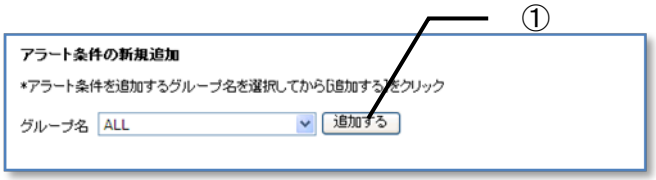
　　キーワードを入力します。部分一致で検索可能です。

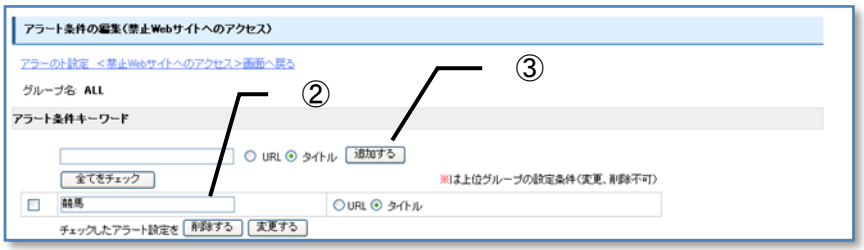
・設定対象項目

　　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。





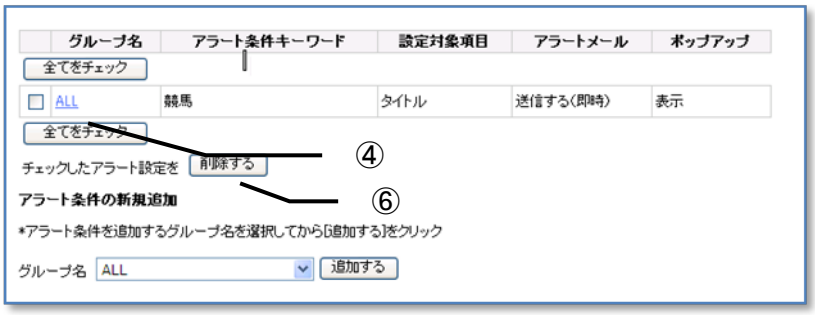
②アラート条件キーワード（部分一致での指定も可能）にて、アラート条件となる URL もしくはタイトルに含まれるキーワードを入力します。

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/

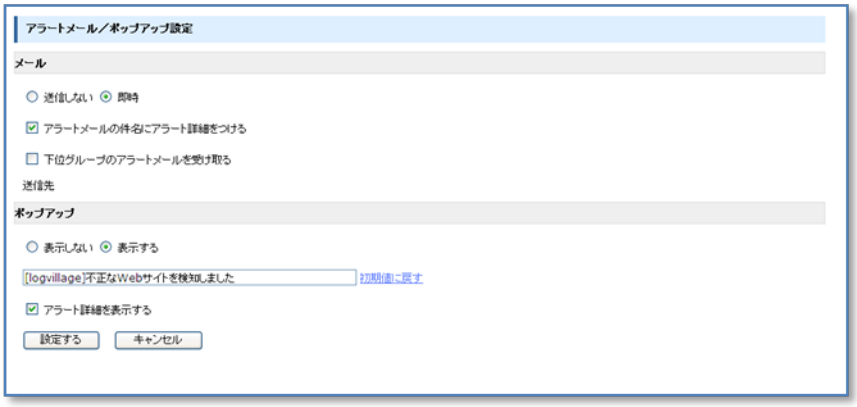
■変更
④変更したいグループをクリックします。
⑤変更したい項目を変更して「変更する」ボタンをクリックします。



■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。



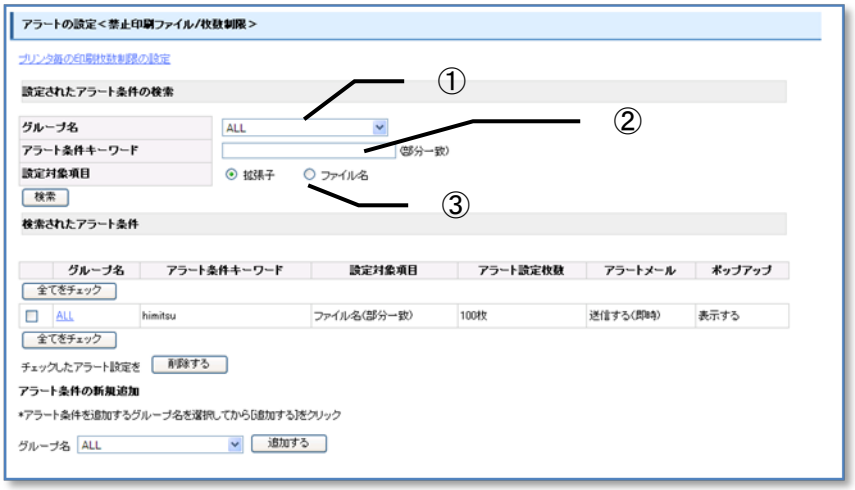
・メール

「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？

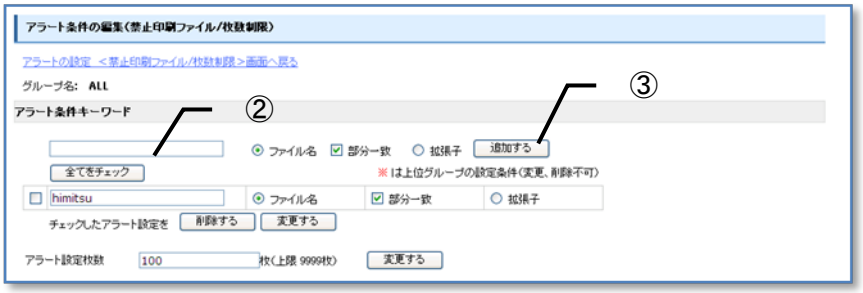
３．３．２　禁止印刷ファイル/枚数制限

禁止印刷ファイル/枚数制限を設定します。



■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。



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。

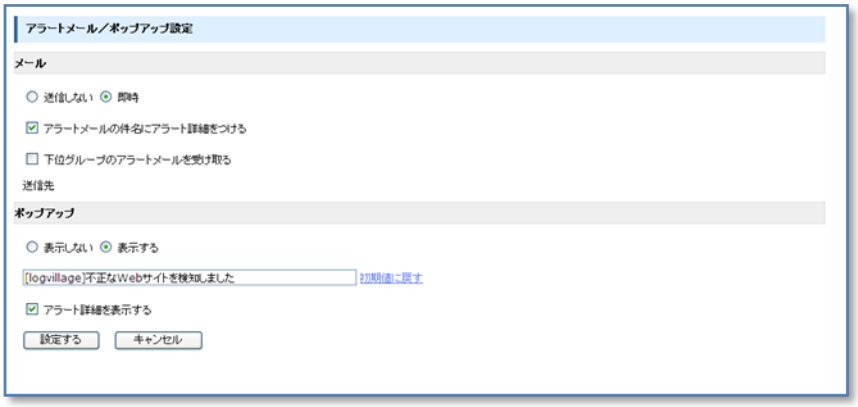
■アラート枚数の設定
月次で枚数を越えた場合、アラートを出力します。

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。

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。

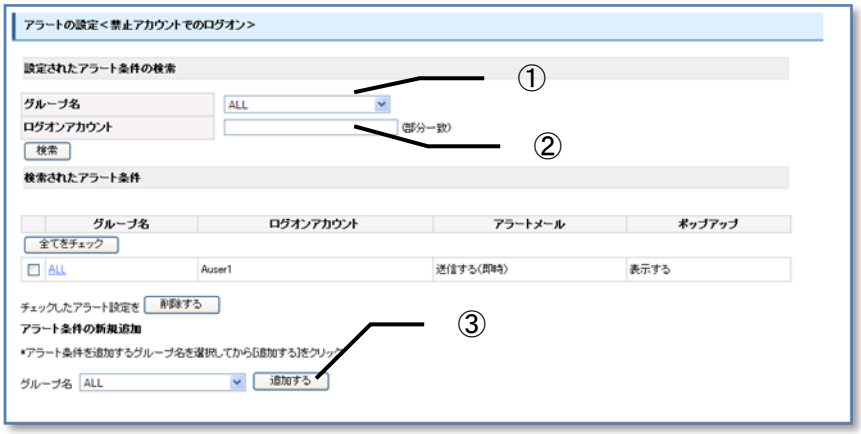


・メール
「送信しない」または「即時」
アラートメールの件名にアラート詳細を付けるか？
下位グループのアラートメールを受け取るか？

・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？

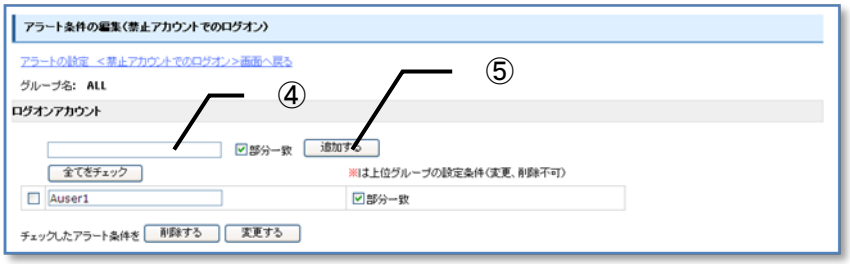
３．３．３　禁止アカウントログオン

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。

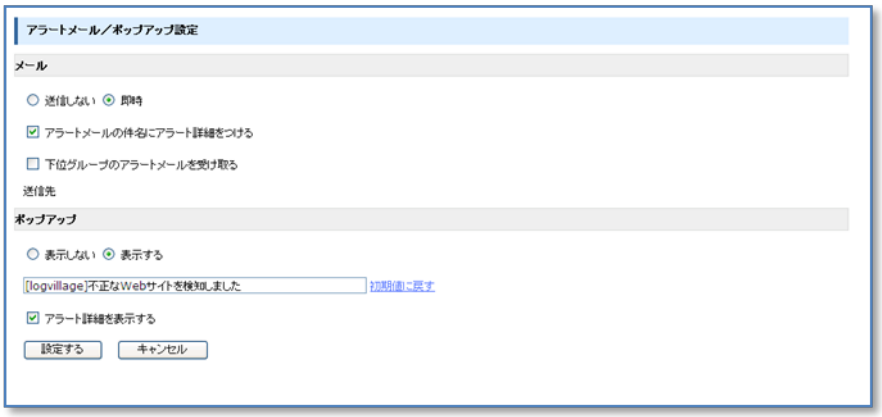
■変更
①変更したいグループをクリックします。
②変更したい項目を変更して「変更する」ボタンをクリックします。

■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。



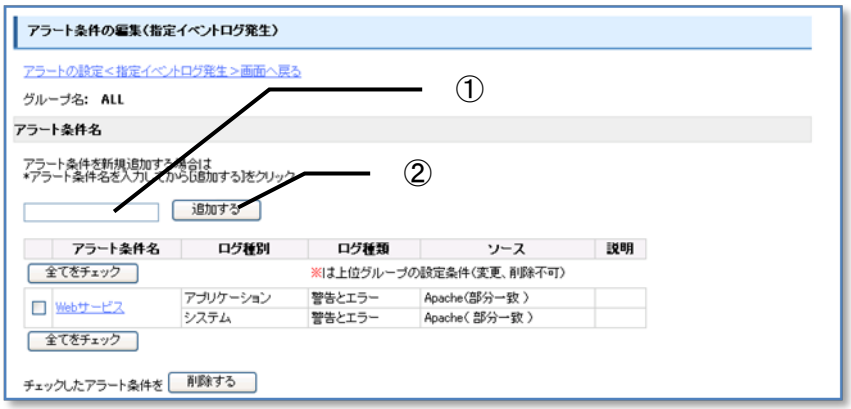
・メール
「送信しない」または「即時」
アラートメールの件名にアラート詳細を付けるか？
下位グループのアラートメールを受け取るか？

・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　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。

■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。



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

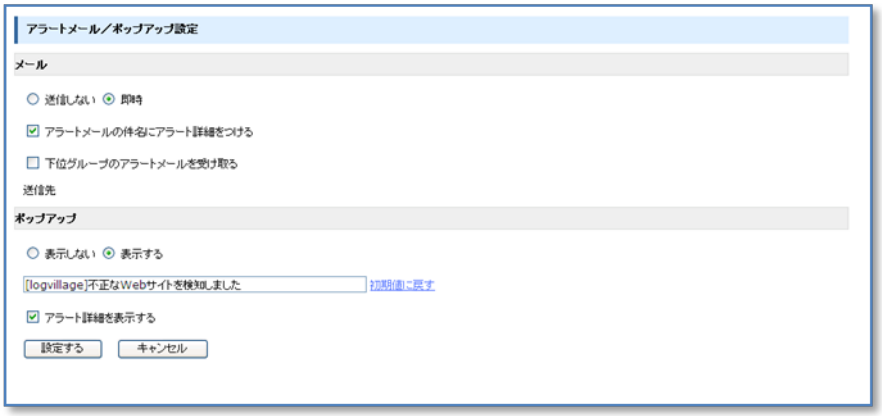
①削除したいグループにチェックを入れて「削除する」ボタンをクリックします。

・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。



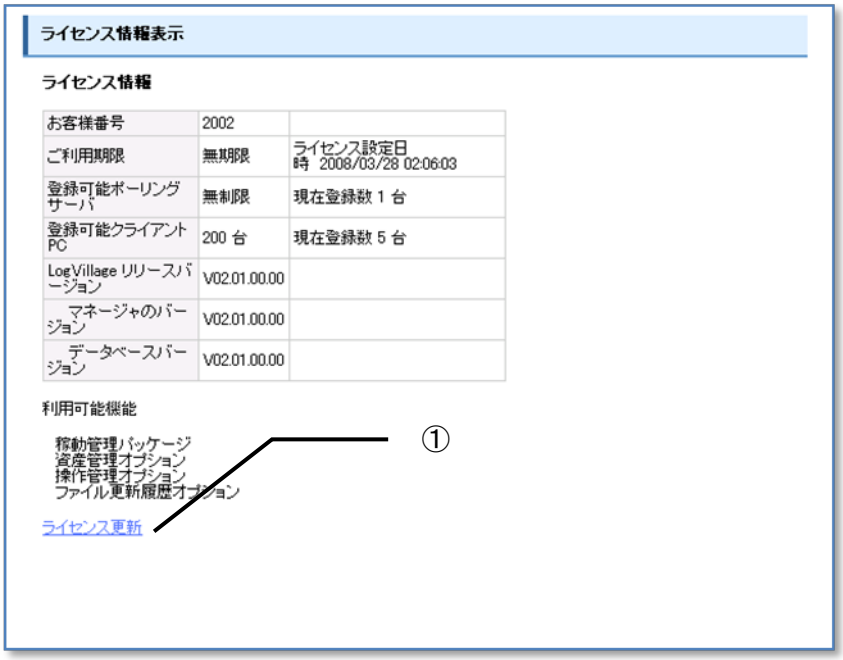
・メール
「送信しない」または「即時」
アラートメールの件名にアラート詳細を付けるか？
下位グループのアラートメールを受け取るか？

・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。

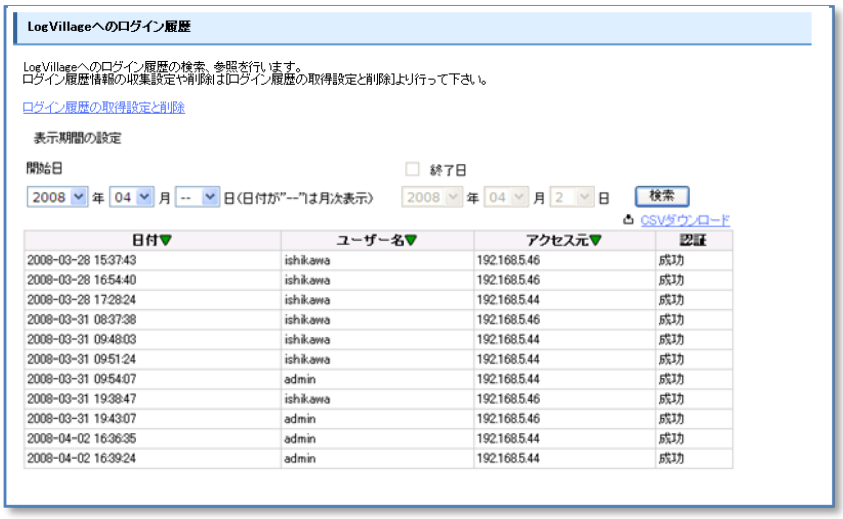


①「ライセンス更新」をクリックしてください。

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。

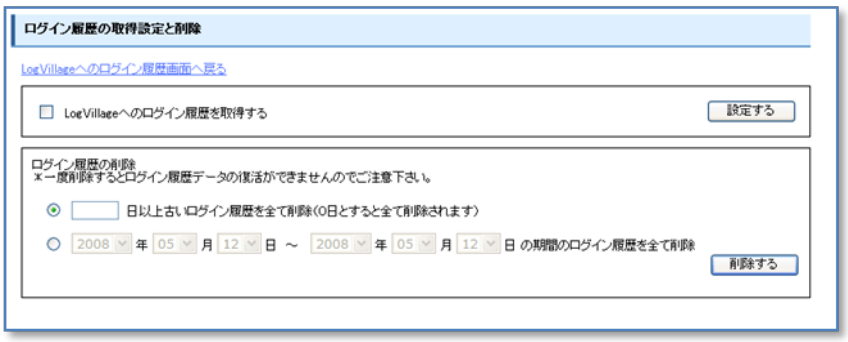
３．４．２　LogVillage へのログイン履歴

LogVillage へのログイン履歴を確認することができます。



■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。



・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

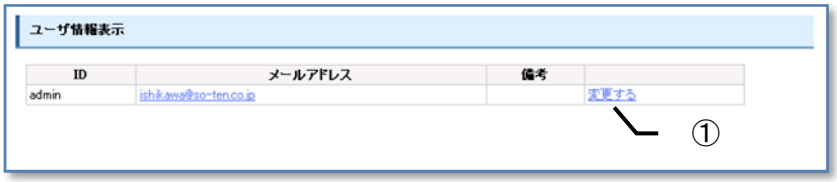
のどちらかを選択し、「設定する」ボタンをクリックします。

３．４．３　ユーザー情報変更

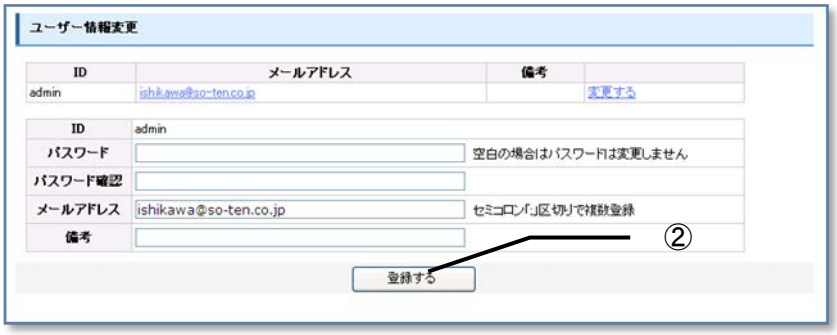
現在ログインしているユーザー自身のメールアドレスとパスワードを変更することが可能です。

■変更

①「変更する」をクリックします。



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。



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

① 「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

③ ［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	フォーマット	パラメータ	説明
[Correspondence Timing]			コメント行
[ModuleTimming]			セクション名
ReStartTimming	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

*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	フォーマット	パラメータ	説明
[Correspondence Timing]			コメント行

[ModuleTimming]			セクション名
ReStartTimming	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

*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I
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)¥SOTEN¥LogVillage¥Manager	[LV-MGR-Inst]
Apache2 インストールフォルダ	C:¥Program Files (x86)¥SOTEN¥LogVillage¥Apache2	[LV-Apache-Inst]
MySQL インストールフォルダ	C:¥Program Files (x86)¥SOTEN¥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)¥SOTEN¥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. お問合せ」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. お問合せ」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、ご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 フォルダー
   ・[LV-PS-Inst]¥conf フォルダー
   ・[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)

５．お問合せ

本製品に対するご意見、ご質問はメール、TEL、FAX にて下記までお問合せ下さい。
お問合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。

〒540-0035 大阪市中央区釣鐘町１丁目 3-4 ダイクウビル 2F
株式会社ワッセイ･ソフトウェア･テクノロジー
e-mail :
TEL :06-6944-8901
FAX :06-6944-8885
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

お問合せの際、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
お問合せの内容（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-23-20170927	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
		「4. LogVillage の運用」を追加