



認証ゲートウェイ Griffas2 のご紹介

株式会社ステラクラフト
2011年 1月

Agenda

- Griffas2とは P 2
- Griffas2導入の効果 P 3
- 導入時のネットワーク構成例 P 4
- Griffas2の特長・機能一覧 P 5
- Griffas2の特長 P 6~12
- Griffas2の機能詳細 P 13~31
- Griffas2処理シーケンス P 32
- Griffas2RM 仕様 P 33
- 保守 P 34
- Griffas2 価格表 P 35

Griffas2 とは

- ・**認証されたユーザ／端末のみをネットワークに接続。**
- ・**制限されたサーバアクセスを実現。**

Griffas2は ネットワークを利用しようとするユーザに対して、端末認証とユーザ認証を行い、不正アクセスをシャットアウトします。また、ユーザグループ毎に接続可能なサーバを制限するなど、ネットワークの利用権限を一元管理できる認証ゲートウェイ アプライアンスです。

- ◆不正PCのネットワークへの接続阻止と検知、記録が可能です。
- ◆Webブラウザを利用してID/パスワードの認証を行う為、多くのネットワーク端末から利用できます。
- ◆ユーザグループ毎にネットワークの利用ルールを設定できます。
例) 営業部に所属する社員は営業関連サーバにのみ接続できる
派遣社員にはメールを利用させない... など



Griffas RM

Griffas2導入の効果

- ネットワーク上のユーザを把握することによる規制強化
 - 未許可PCのLAN接続の検知、不正利用の防止
 - セッション中(利用中)のユーザー一覧の表示
- 重要な企業内データの保護
 - アクセス制限による情報漏えい、データ損失の防止
- ネットワークにおける有害プログラムの拡散防止
 - Griffas上でACLを設定することで、接続先が限定されるため、万が一有害なプログラム(ウィルスやWinny等)が持ち込まれた場合の被害を抑止可能

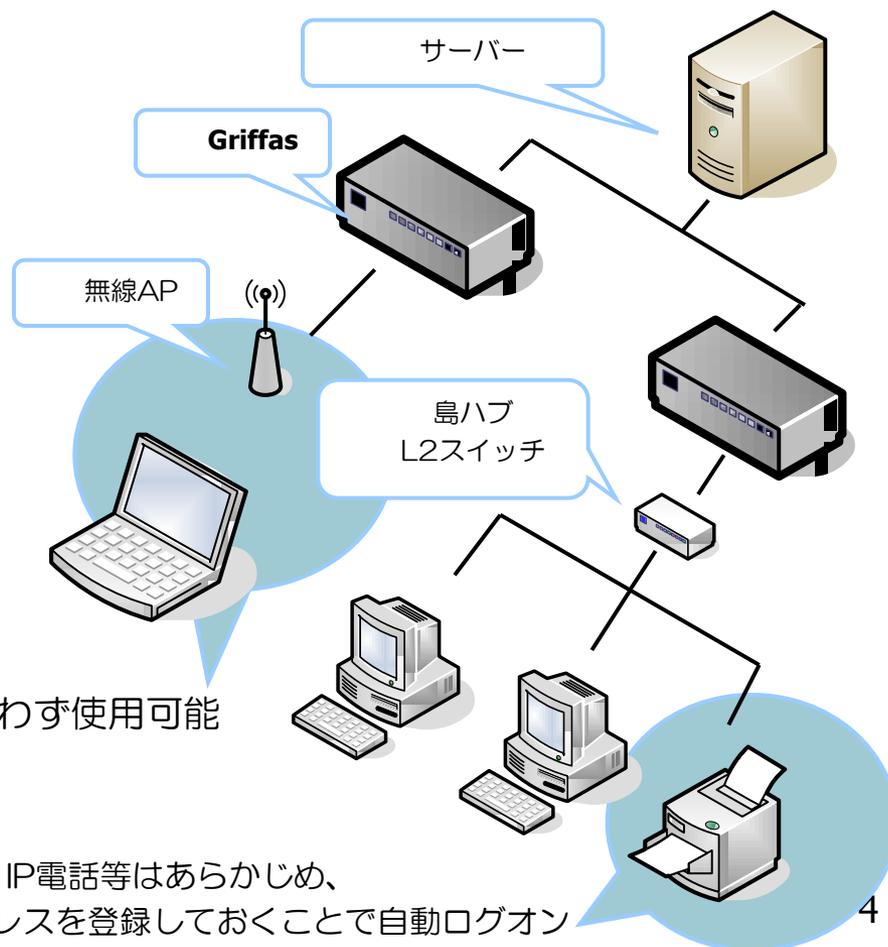
導入時のネットワーク構成例

ブリッジ接続

Griffasはブリッジとして機能します。

ブリッジによるメリット

- ・ ネットワークの再構成の必要が無く既存設備の無駄がありません。
- ・ 島ハブの使用しているネットワークに簡単に導入できます。
- ・ ネットワークのエッジに配置いただくことにより、場所を特定した利用も可能です。



有線・無線問わず使用可能

プリンタ・IP電話等はあらかじめ、
MACアドレスを登録しておくことで自動ログオン



Griffas2の特長・機能一覧

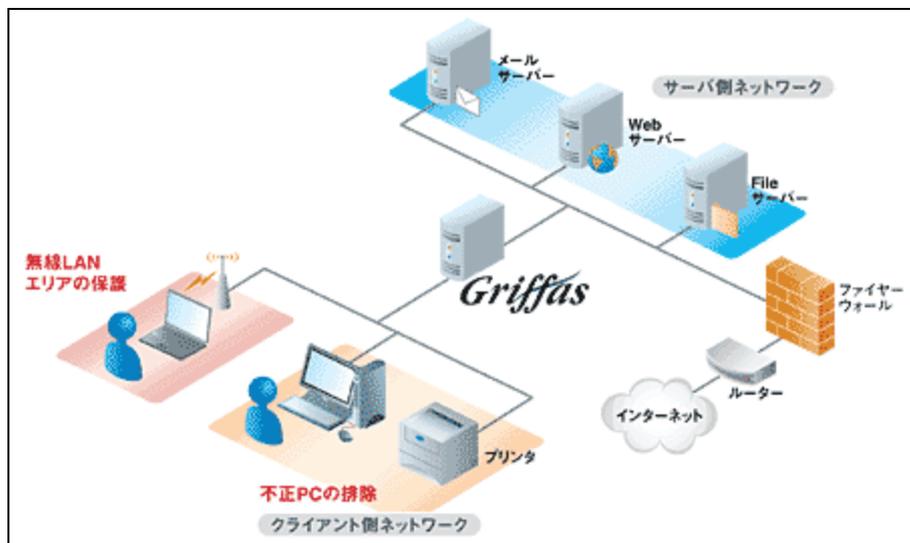
特長・機能	参照ページ
Web認証、ACL(アクセスコントロール)機能	P7～8
ログ機能(接続ログ、アカウントログ、管理者操作ログ、未登録PCエラーログ、アクセスログ)	P10～11
不正端末妨害機能	P12
IPアドレスベースでのクライアント機器管理	P14～16
セッション監視機能	P17
ユーザ管理、ユーザグループ管理	P18～20
サーバ管理	P21
ネットワーク機器認証(MACアドレス事前登録)	P22
バックアップ・リストア機能	P23
ログイン画面カスタマイズ	P24
時限ユーザ機能	P25～27
集中管理機能	P28
運用支援ツール(パケットキャプチャ取得)、Syslog転送機能	P29～30
エージェント機能、RADIUS・LDAP連携機能	P31

特長1: 透過的な設置

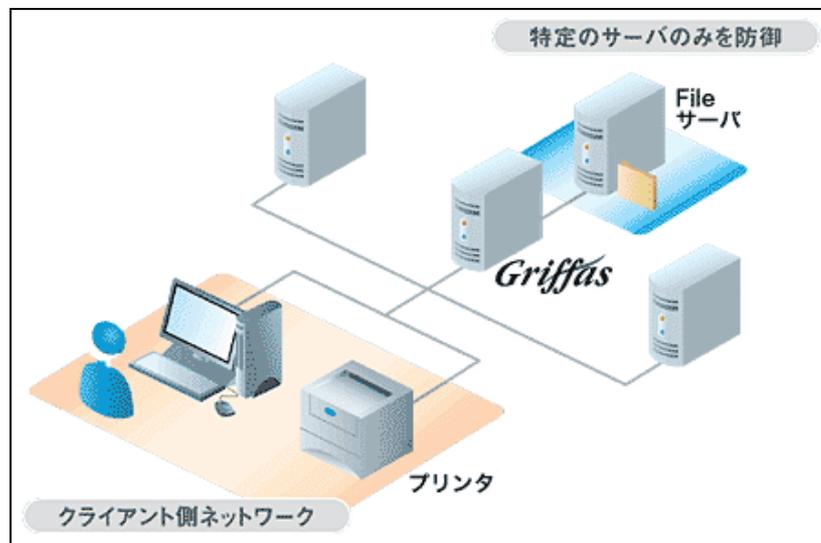
Griffas2はネットワーク全体や、特定サーバのみを認証させることが可能です。

Griffas2はブリッジとして機能するため、アクセスを防御したい環境とクライアントの環境間に設置するだけでよく、現在利用しているネットワーク環境の大幅な変更は不要です。

＜ネットワーク全体を守るパターン＞



＜特定のサーバ(群)のみを守るパターン＞



特長2: Webブラウザでの認証

Griffas2はWebブラウザを使って認証を行うため、クライアントに特別なアプリケーションをインストールすることなくお使い頂けます。

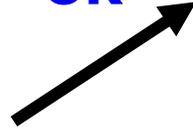
認証画面にてID/パスワードを入力するだけで、ログインが可能です。※

※プリンタ・IP電話等はあらかじめ、MACアドレスを登録しておくことでID/パスワードの入力を省略可能です。

<ログイン画面>



OK



NG

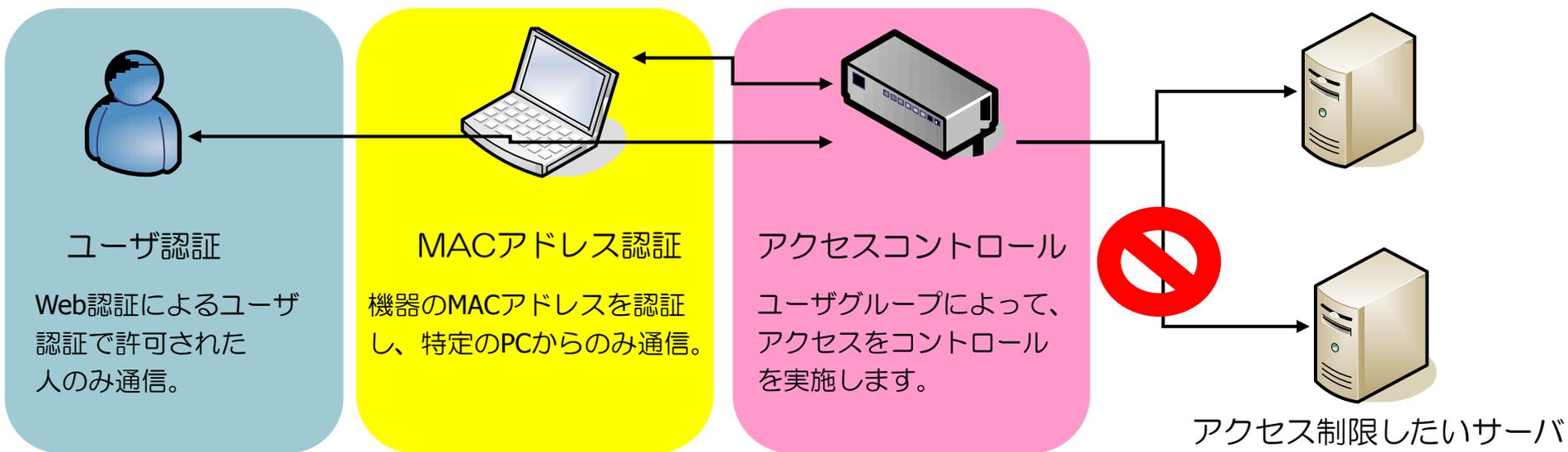


<認証結果>



特長3: アクセスコントロール

事例: サーバの保護



アクセスコントロールを使用することにより、営業・総務といったユーザグループ毎に、閲覧・ダウンロード可能なサーバ等、各グループによって、利用の制限が行えます。

特長4: 使いやすい管理ツール

ユーザ管理はWebインターフェースによる簡単な設定が可能

Web GUIベースでユーザ登録やその他設定ができますので、より簡単に環境設定を行うことが可能です。はじめて設定を行う場合、画面のように初期設定項目は赤字で表示されます。

指定箇所をクリックすることで、その設定画面に遷移します。画面左には各設定項目が選択できるメニューが配置されています。

また、メニュー最上部にはGriffasの稼働状況が表示されています。

設定後の再起動、停止などはこの画面より行うことが可能です。

尚、Web設定画面は一定時間のアクセスが無い場合自動的にログオフを行います。



特長5: ログ管理

Griffas2 では多彩なログの管理を行なうことができます。

Griffas2では4種類のログを記録しています。
 ログの保存期間も設定が可能です。

ログの種類

- ・認証ログ
- ・アカウントングログ
- ・管理者操作ログ
- ・未登録PCエラーログ

< 検索画面(認証ログ) >



< 検索結果表示(結果部分抜粋) >

検索結果

5件のログがあります。1-5件を表示
 表示ページ 1

#	年月日 時刻	認証	ログイン名	メッセージ	IPアドレス	MACアドレス	ログ取得ホスト名
1	2007-02-21 19:16:19	成功	stellar	認証しました(DB)	192.168.	00:e0:4c:	griffas
2	2007-02-21 19:13:17	失敗	stellar	パスワードが間違っています。	192.168.	00:e0:4c:	griffas
3	2007-02-08 15:45:23	成功	stellar	認証しました(DB)	192.168.	00:01:4a:	griffas
4	2007-01-25 14:27:08	成功	stellar	認証しました(DB)	192.168.	00:11:25:	griffas
5	2007-01-25 14:26:47	失敗	stellar	パスワードが間違っています。	192.168.	00:11:25:	griffas

表示ページ 1
 ダウンロード 10,000件を超える場合は新しい方から順に10,000件をダウンロードします

表示した結果ログをダウンロードすることが可能(CSV形式)

新バージョンにて取得するログ情報を強化しました。
(認証成功したユーザのログも取得します)

アクセスログ

認証済みPCからのアクセスログを表示します。ログを絞りこむ場合は、「詳細検索」をチェックして検索条件を追加してください。

[注意]プロトコルがIP以外の場合には、IPアドレスは表示されません。
[注意]プロトコルがICMP,DNS,DHCP,ARPの場合は認証済みアクセス可能なため、ログイン名は表示されない場合があります。

検索条件

検索条件を入力して、「検索」ボタンをクリックしてください。

年	2008	月	9	日	7	時	15	分	00	秒	00
年	2008	月	9	日	9	時	15	分	00	秒	00

詳細検索

検索 リセット

検索結果

98件のログがあります。1-98件を表示

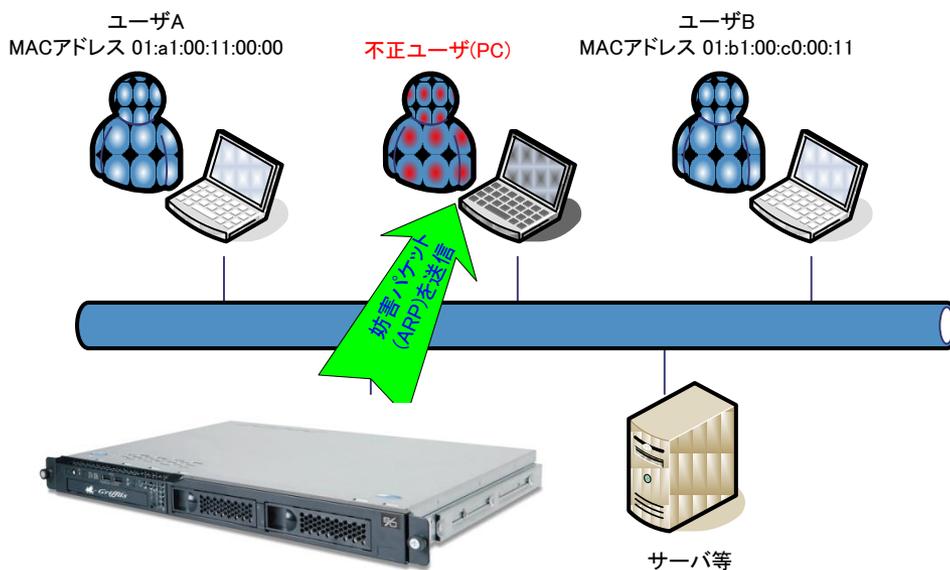
表示ページ 1

#	年 月 日 時刻	送信元 IPアドレス MACアドレス	送信先 IPアドレス MACアドレス	プロトコル	ログイン 名	ログ取得ホスト 名
1	2008-09-09 14:54:00	192.168.16.12 00:0b:97:32:38:b3	192.168.16.255 ff:ff:ff:ff:ff:ff	IP[UDP]netbios- dgm	stellar	GriffasVer2
2	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	203.179.83.12 00:a0:de:14:46:87	IP[TCP]1685->80	stellar	GriffasVer2
3	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	203.179.83.12 00:a0:de:14:46:87	IP[TCP]1686->80	stellar	GriffasVer2
4	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	203.179.83.12 00:a0:de:14:46:87	IP[TCP]1687->80	stellar	GriffasVer2
5	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	203.179.83.12 00:a0:de:14:46:87	IP[TCP]1698->80	stellar	GriffasVer2
6	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	203.179.83.12 00:a0:de:14:46:87	IP[TCP]1703->80	stellar	GriffasVer2
7	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	192.221.69.126 00:a0:de:14:46:87	IP[TCP]1708->80	stellar	GriffasVer2
8	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	207.46.19.190 00:a0:de:14:46:87	IP[TCP]1680->80	stellar	GriffasVer2
9	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	207.46.19.190 00:a0:de:14:46:87	IP[TCP]1681->80	stellar	GriffasVer2
10	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	207.46.73.60 00:a0:de:14:46:87	IP[TCP]1683->80	stellar	GriffasVer2
11	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	203.179.83.10 00:a0:de:14:46:87	IP[TCP]1688->80	stellar	GriffasVer2
12	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	203.179.83.10 00:a0:de:14:46:87	IP[TCP]1697->80	stellar	GriffasVer2
13	2008-09-09 14:48:00	192.168.16.12 00:0b:97:32:38:b3	65.55.15.123 00:a0:de:14:46:87	IP[TCP]1694->80	stellar	GriffasVer2

特長6: 不正端末妨害

登録されていないMACアドレスを持つPCに妨害ARPを送信して、通信を混乱させます。本機能は、公開側ネットワーク内の無許可PC同士（ピアツーピア）の通信を行わせないために利用します。（ARPを使うため、セグメントを越えた設定はできません）

※妨害ARPの影響を受けるOSはWindows系のみです。Linux, MacOSX、UNIXは利用できません。



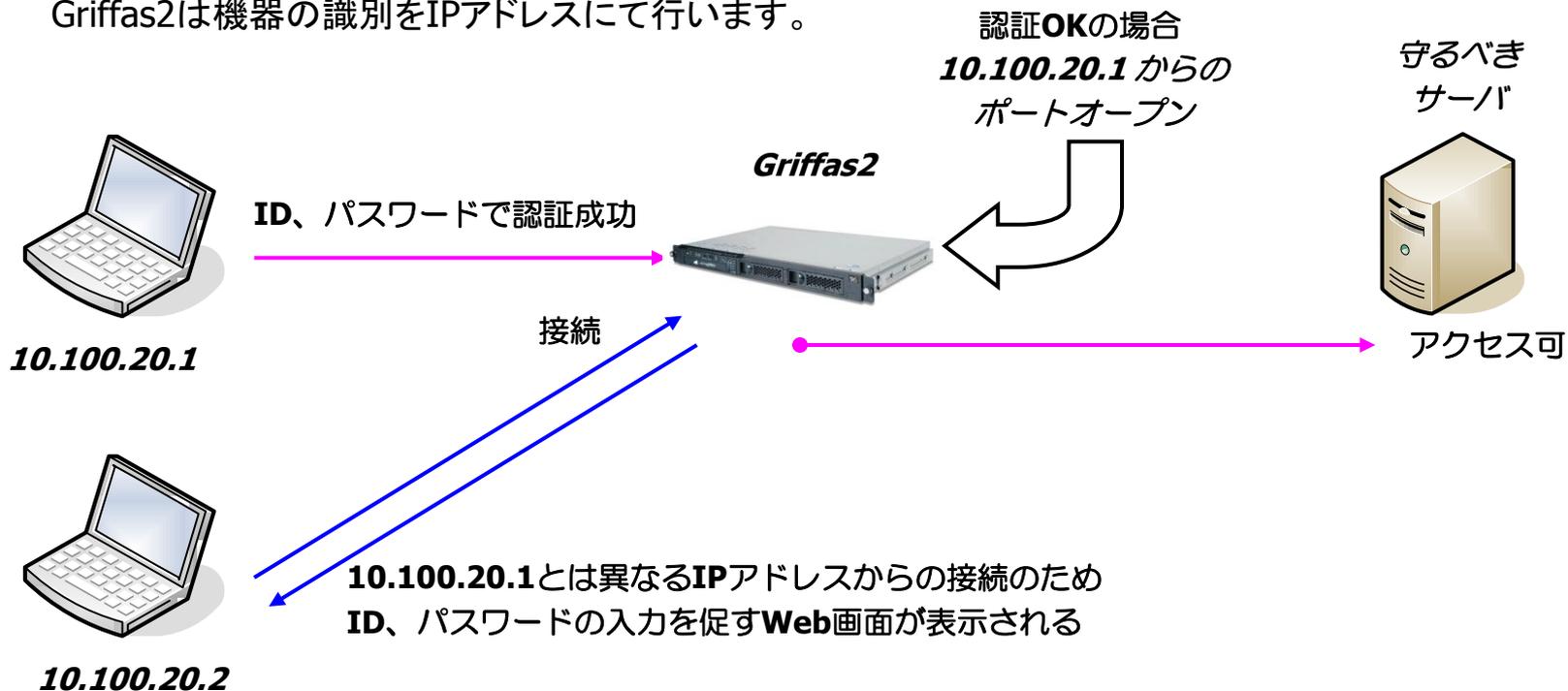
Griffas2の機能詳細

Griffas2の設定画面(機能)のご紹介

- IPアドレスベースの管理
- セッション監視
- ユーザ管理
- ユーザグループ管理
- サーバ管理
- ネットワーク機器管理
- バックアップ・リストア
- ログイン画面
- 時限ユーザ
- 集中管理構成
- 運用支援ツール
- ログ転送
- その他の機能

IPアドレスベースの管理 (1)

Griffas2は機器の識別をIPアドレスにて行います。



IPアドレスベースの管理 (2)

IPアドレスを用いて管理する為、アドレスの偽装対応として、セッション監視機能を実装しております。

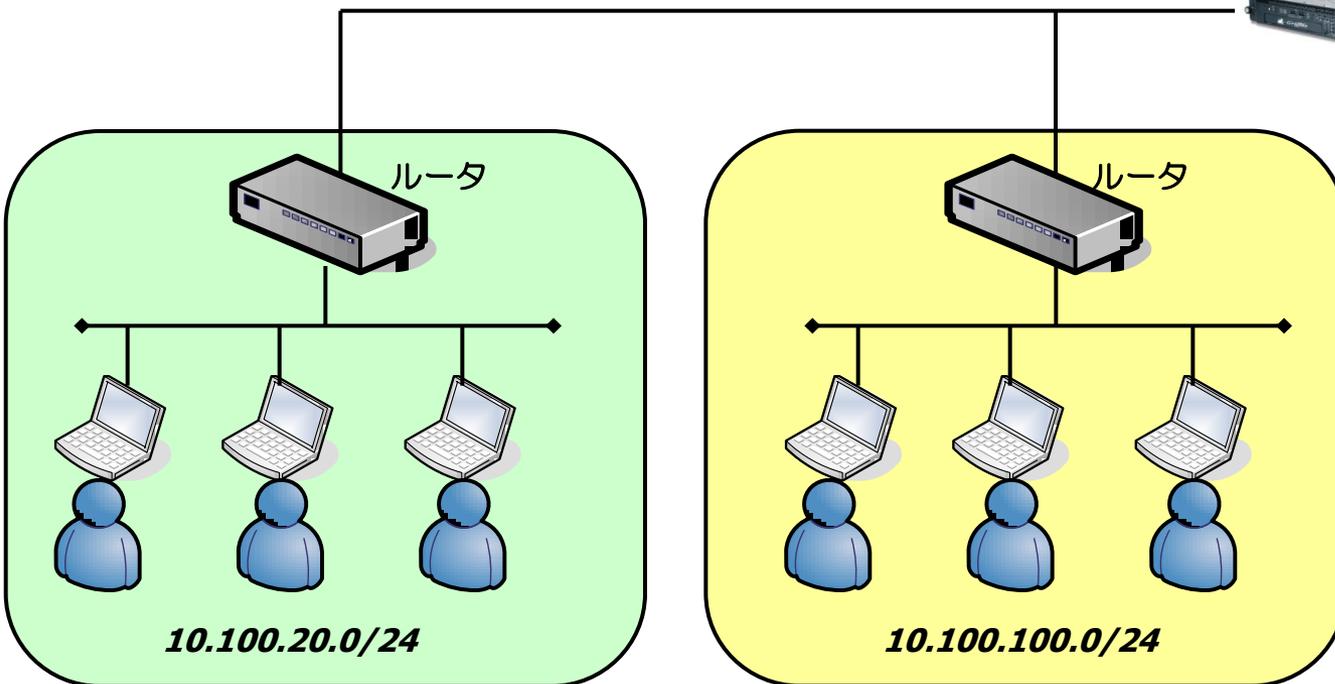


IPアドレスベースの管理 (3)

IPアドレスで端末を認識するため、セグメントやルータを越えて機器の特定が可能です。また、エージェント機能を利用することで、NAT等でIPアドレスを変換してしまうような機器がある場合でも、機器の特定が可能です。**注1**

守るべき
サーバ

Griffas2



注1

エージェント機能が利用できない場合、NAT配下の機器の識別はできません。

セッション監視

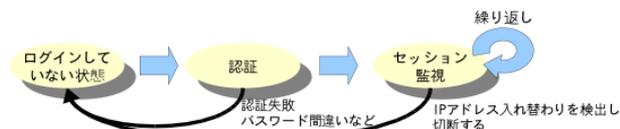
セッション監視設定画面

ユーザ認証設定

各種設定値を設定し、[設定]ボタンをクリックしてください。

セッション監視設定

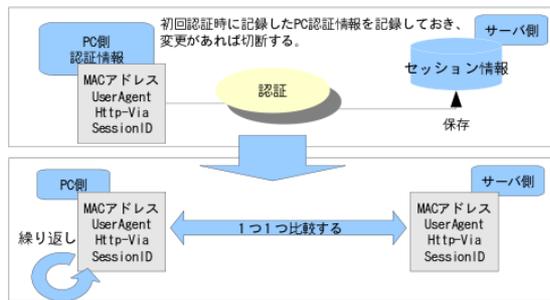
セッション監視:セッション監視を利用するかどうかを選択してください。利用する場合、繰り返し間隔を秒数で指定してください。
 [注意]サーバの再起動が必要です。
 デフォルト値:利用する。繰り返し間隔10秒



セッション監視	<input checked="" type="radio"/> 利用する <input type="radio"/> 利用しない
繰り返し間隔(単位:秒)	10秒
[設定]	

セッション監視詳細設定

セッション監視:セッション監視をセッションを維持するのに必要な情報を選択してください。
 [注意]サーバの再起動が必要です。
 デフォルト値:利用する



MACアドレスについては、セグメントを越えて Griffasを配置する際には、取得できない場合がございますので、ご利用のネットワークの構成によって、利用可能かどうかをご確認ください。

MACアドレス	<input checked="" type="radio"/> 利用する <input type="radio"/> 利用しない 解説:MACアドレスは、同一ネットワークセグメントで利用できます。ブラウザ入れ替わりを検出できます。
User-Agent	<input checked="" type="radio"/> 利用する <input type="radio"/> 利用しない 解説:User-Agentには、Webブラウザの識別IDが格納されています。ブラウザ入れ替わりを検出できます。
Http-Via	<input checked="" type="radio"/> 利用する <input type="radio"/> 利用しない 解説:Http-Viaには、Proxy利用有無が格納されています。通信環境の変更を検出できます。
Session-ID	<input checked="" type="radio"/> 利用する <input type="radio"/> 利用しない 解説:Session-IDには、ログイン時にユーザ毎にユニークなIDが格納されています。PC入れ替わりを検出できます。
[設定]	

ユーザ管理

- ユーザ情報の管理
ログイン名、
パスワード等を
設定します。

ユーザ管理

ユーザ(利用者)の登録/変更/削除を行います。
 [注意]ログイン中のユーザ情報を変更した場合は、次のログインから有効になります。

▼ ユーザ登録

ユーザを新規作成するには、[上書きする]チェックボックスのチェックを外して[登録]ボタンをクリックしてください。
 ユーザ情報を変更するには、[上書きする]チェックボックスにチェックを入れて[登録]ボタンをクリックしてください。
 入力した情報を消したい場合は、[クリア]ボタンをクリックしてください。

所属グループ	デフォルトグループ ▼
ログイン名	<input type="text"/> <必須>
パスワード	<input type="text"/> <必須>
氏名	<input type="text"/>
メールアドレス	<input type="text"/>
専用PC [注意]指定しない場合は、いずれのPCでも利用できます。 MACアドレス: <input type="text"/> 備考: <input type="text"/> <input type="button" value="追加"/>	<input type="button" value="削除"/>
共有PC 名称: ▼ <input type="button" value="追加"/>	<input type="button" value="削除"/>
同時利用不可	<input type="checkbox"/> 不可
利用不可	<input type="checkbox"/> 不可
時限ユーザ	<input type="checkbox"/> 利用する
備考	<input type="text"/>

上書きする

ユーザグループ管理 (1)

ユーザグループ管理

ユーザグループ管理

グループの登録/変更/削除を行ないます。ユーザは、いずれかのグループに所属します。
 [注意]ログイン中ユーザのグループ情報を変更した場合は、次のログインから有効になります。

▶ グループ登録

グループを新規作成する場合は、「▶ グループ登録」をクリックしてください。

検索結果

グループ情報を変更するには、[グループ名]をクリックしてください。
 グループを削除するには、削除対象の[削除]チェックボックスにチェックし、[実行]ボタンをクリックしてください。
 表示されたすべてのグループの[削除]チェックボックスにチェックするには、[全削除チェック]ボタンをクリックしてください。
 表示されたすべてのグループの[削除]チェックボックスにチェックを外すには、[クリア]ボタンをクリックしてください。
 結果をCSVファイルにダウンロードするには、[ダウンロード]をクリックしてください。

1件のユーザグループ情報があります。1-1件を表示

表示ページ 1

削除	グループ名	アクセス可能なサーバ	利用可能ポート	アイドルタイムアウト	ログイン可能時間	認証期間	パスワードミスロック	時限ユーザ利用時間	利用可能	備考
<input type="checkbox"/>	デフォルトグループ			-	-	-	-	利用禁止	可	

表示ページ 1

ユーザグループ管理 (2)

- ユーザグループの管理

ユーザグループ管理

グループの登録/変更/削除を行います。ユーザは、いずれかのグループに所属します。
[注意]ログイン中ユーザのグループ情報を変更した場合は、次のログインから有効になります。

▼ グループ登録

グループを新規作成するには、[上書きする]チェックボックスのチェックを外して[登録]ボタンをクリックしてください。
 グループ情報を変更するには、[上書きする]チェックボックスにチェックを入れて[登録]ボタンをクリックしてください。
 入力した情報を消したい場合には、[クリア]ボタンをクリックしてください。

グループ名	<input type="text"/> <必須>
アクセス可能なサーバリスト [注意] 指定しない場合、すべてのサーバが利用できます。 サーバ名: <input type="text"/> <input type="button" value="追加"/>	<input type="text"/> <input type="button" value="削除"/>
利用可能ポートリスト [注意] 指定しない場合、すべてのポートが利用できます。 Well Known ポート一覧 種別: <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP 番号: <input type="text"/> <input type="button" value="追加"/>	<input type="text"/> <input type="button" value="削除"/>
アイドルタイムアウト	制限無し <input type="button" value="▼"/>
ログイン可能時間	<input type="checkbox"/> 制限する 9 時 0 分 ~ 17 時 0 分
認証期間	<input type="checkbox"/> 制限する 2008 年 9 月 9 日 18 時から 2008 年 9 月 9 日 18 時まで
パスワードミスロック回数	制限無し <input type="button" value="▼"/>
時限ユーザ利用時間 1日 <input type="button" value="▼"/> 選択 <input type="text"/> 分	
利用不可	<input type="checkbox"/> 不可
備考	<input type="text"/>

上書きする

サーバ管理

- サーバへの接続を制限します。

サーバ管理

サーバの登録/変更/削除を行ないます。

ユーザやネットワーク機器が、保護するネットワーク内の特定サーバへのアクセス許可する場合に設定します。

[注意]ログイン中ユーザに関するサーバ情報を変更した場合は、次のログインから有効になります。

[注意]ネットワーク機器に関するサーバ情報を変更した場合は、システムの再起動が必要です。

▼ サーバ登録

サーバを新規作成するには、[上書きする]チェックボックスのチェックを外して[登録]ボタンをクリックしてください。

サーバ情報を変更するには、[上書きする]チェックボックスにチェックを入れて[登録]ボタンをクリックしてください。入力した情報を消したい場合は、[クリア]ボタンをクリックしてください。

サーバ名	<input type="text"/> <必須>
IPアドレス	<input type="text"/> <必須>
利用可能ポートリスト [注意] 指定しない場合、すべてのポートにアクセスできます。 Well Known ポート一覧	<input type="text"/> 種別: <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP 番号: <input type="text"/> <input type="button" value="追加"/> <input type="button" value="削除"/>
備考	<input type="text"/>

上書きする

検索結果

サーバデータがありません。

ネットワーク機器管理

- IP電話、プリンタ等のネットワーク機器を登録します。

ネットワーク機器管理

ネットワーク機器の登録/変更/削除を行ないます。

ネットワーク機器とは、Web認証ができない「IP電話」や「プリンタ」などの機器です。

[注意]ネットワーク機器情報を変更した場合は、システムの再起動が必要です。

▼ ネットワーク機器登録

ネットワーク機器を新規作成するには、[上書きする]チェックボックスのチェックを外して[登録]ボタンをクリックしてください。

ネットワーク機器情報を変更するには、[上書きする]チェックボックスにチェックを入れて[登録]ボタンをクリックしてください。入力した情報を消したい場合は、[クリア]ボタンをクリックしてください。

ネットワーク機器名	<input type="text"/>	<必須>
MACアドレス	<input type="text"/>	<必須>
アクセス可能なサーバリスト [注意] 指定しない場合、すべてのサーバが利用できます。 サーバ名: <input type="text"/>	<input type="button" value="追加"/> <input type="button" value="削除"/>	
利用不可	<input type="checkbox"/>	不可
備考	<input type="text"/>	

上書きする

検索結果

ネットワーク機器データがありません。

バックアップ・リストア

- バックアップ、リストア

バックアップ/リストア

サーバの全設定情報(初期設定、ライセンス、管理端末、システム監視グラフ、集中管理設定除く)、ログをバックアップします。
 バックアップファイルはお使いのコンピュータにダウンロードされます。
 リストアする場合は、あらかじめダウンロードしたバックアップファイルを使って行います。

バックアップ

サーバの全設定情報(初期設定、ライセンス、管理端末、システム監視グラフ、集中管理設定除く)、ログをバックアップするには[バックアップ]ボタンをクリックしてください。
 [注意]バックアップ中は、更新をともしない操作をできるだけ控えてください。

ログをバックアップする。

リストア

お使いのコンピュータにあらかじめ、ダウンロードしたバックアップファイルを使ってリストアします。
 全設定情報(初期設定、ライセンス、管理端末、システム監視グラフ、集中管理設定除く)、ログもバックアップ時点に戻ります。
 バックアップファイルを選択して、[リストア]ボタンをクリックしてください。
 [注意]リストア終了後、自動的にサーバを再起動します。

ログをリストアする。

バックアップファイル

バックアップ情報

お使いのコンピュータにあらかじめ、ダウンロードしたバックアップファイルの情報を表示します。
 バックアップファイルを選択して、[情報表示]ボタンをクリックしてください。

バックアップファイル

定期バックアップ

バックアップを定期的に行うには、実行する時間を設定し、[設定]ボタンをクリックしてください。
 [注意]バックアップ実行時刻は、更新作業が少ない時間帯を指定してください。

サーバの全設定情報(初期設定、ライセンス、管理端末、システム監視グラフ、集中管理設定除く)、ログを、サーバのディスク上にバックアップします。
 定期バックアップしたファイルをリストアするためには、お使いのコンピュータにダウンロードする必要があります。

定期バックアップ	<input checked="" type="checkbox"/> 有効にする
ログをバックアップ	<input checked="" type="checkbox"/> する
実行する時刻(0~23時 0~59分)	3 時 0 分
実行する曜日	毎日
保存する世代数	5

定期バックアップしたファイルの一覧です。
 ダウンロードを行うには、バックアップファイルを選択して[ダウンロード]ボタンをクリックしてください。

#	選択	バックアップ日付	ファイルの大きさ
1	<input checked="" type="radio"/>	2007年11月22日 04時00分	18.18 Kバイト

ログイン画面のカスタマイズ

- ログイン画面のカスタマイズが可能です。

ユーザ操作

ユーザ操作URL

ユーザ操作(ログイン、ログアウト、パスワード変更)は、下記のURLで操作できます。

<http://192.168.16.229/>

画面のカスタマイズ

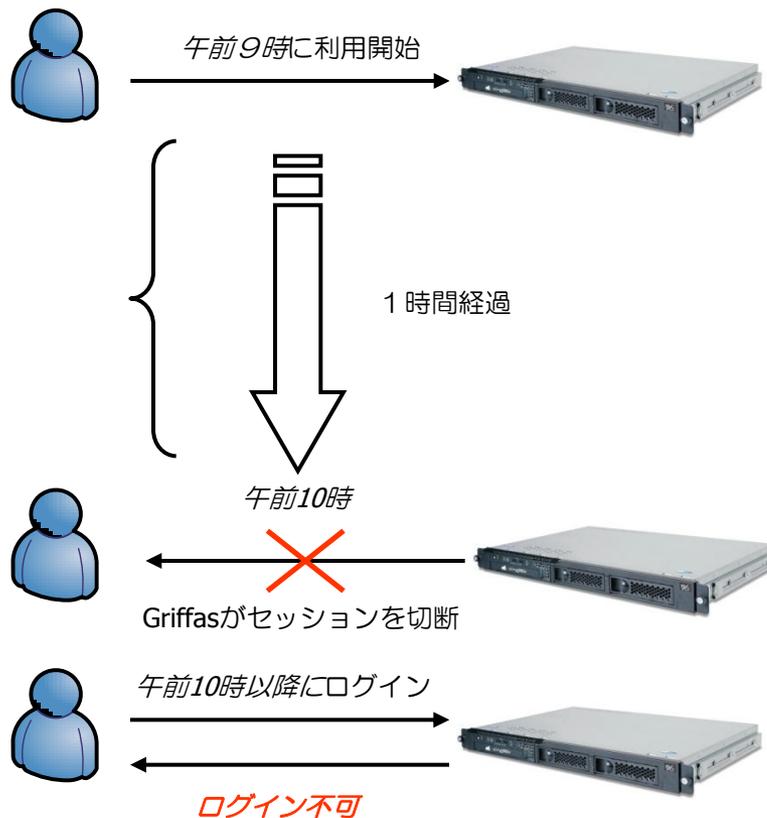
ユーザ操作画面の画像、タイトル、説明文、フッタをカスタマイズできます。
値を入力し、[設定]ボタンをクリックしてください。

ログイン画面のタイトル	<input type="text" value="ログイン"/> <必須>
ログイン画面の説明文	<input type="text" value="ネットワークを利用するには、ログイン名とパスワードを"/> <必須>
ログイン画面のユーザパスワード画面へのリンク	<input chgpaswrd\""="" type="text" value="パスワードを変更したい場合... <必須>
ログアウト画面のタイトル	<input type="text" value="ログアウト"/> <必須>
ユーザパスワード変更画面のタイトル	<input type="text" value="ユーザパスワード変更"/> <必須>
セッション監視画面のタイトル	<input type="text" value="セッション監視"/> <必須>
フッタ (HTMLタグ利用可)	<input type="text" value="<HR>"/> <必須>
左上の画像 (GIF形式)	 <input type="text" value=""/> <input type="button" value="参照..."/> <input type="button" value="アップロード"/>

時限ユーザ機能 (1)

指定時間しか利用できない、時限ユーザを作成することが可能です。

1時間利用できるユーザ



Griffas2は、該当ユーザの認証開始時間に利用可能時間を加算した「利用終了時刻」を設定。この例の場合であれば、午前10時が「利用終了時刻」となります。なお、午前10時までの間であれば、何度ログインログアウトを繰り返しても利用可能です。
「利用終了時刻」は一度設定されたら、その後は変化しません。

時限ユーザ機能 (2)

ユーザグループ単位で利用時間の設定が可能です。

ユーザグループ管理

グループの登録/変更/削除を行ないます。ユーザは、いずれかのグループに所属します。
 [注意]ログイン中ユーザのグループ情報を変更した場合は、次のログインから有効になります。

▶ グループ登録

グループを新規作成する場合は、「▶ グループ登録」をクリックしてください。

検索結果

グループ情報を変更するには、[グループ名]をクリックしてください。
 グループを削除するには、削除対象の[削除]チェックボックスにチェックし、[実行]ボタンをクリックしてください。
 表示されたすべてのグループの[削除]チェックボックスにチェックするには、[全削除チェック]ボタンをクリックしてください。
 表示されたすべてのグループの[削除]チェックボックスにチェックを外すには、[クリア]ボタンをクリックしてください。
 結果をCSVファイルにダウンロードするには、[ダウンロード]をクリックしてください。

1件のユーザグループ情報があります。1-1件を表示

表示ページ 1

削除	グループ名	アクセス可能なサーバ	利用可能ポート	アイドルタイムアウト	ログイン可能時間	認証期間	パスワードミスロック	時限ユーザ利用時間	利用可能	備考
<input type="checkbox"/>	デフォルトグループ			-	-	-	-	利用禁止	可	

表示ページ 1

時限ユーザ機能 (3)

ユーザ情報登録時の 時限ユーザ設定

ユーザ管理

ユーザ(利用者)の登録/変更/削除を行ないます。

[注意]ログイン中のユーザ情報を変更した場合は、次のログインから有効となります。

▼ ユーザ登録

ユーザを新規作成するには、[上書きする]チェックボックスのチェックを外して[登録]ボタンをクリックしてください。
 ユーザ情報を変更するには、[上書きする]チェックボックスにチェックを入れて[登録]ボタンをクリックしてください。
 入力した情報を消したい場合は、[クリア]ボタンをクリックしてください。

所属グループ	デフォルトグループ ▼
ログイン名	<input type="text"/> <必須>
パスワード	<input type="password"/> <必須>
氏名	<input type="text"/>
メールアドレス	<input type="text"/>
専用PC [注意]指定しない場合は、いずれのPCでも利用できます。 MACアドレス: <input type="text"/> 備考: <input type="text"/> <input type="button" value="追加"/>	<input type="checkbox"/> <input type="button" value="削除"/>
共有PC 名称: ▼ <input type="button" value="追加"/>	<input type="checkbox"/> <input type="button" value="削除"/>
同時利用不可	<input type="checkbox"/> 不可
利用不可	<input type="checkbox"/> 不可
時限ユーザ	<input type="checkbox"/> 利用する
備考	<input type="text"/>

上書きする

集中管理構成（分散配置）

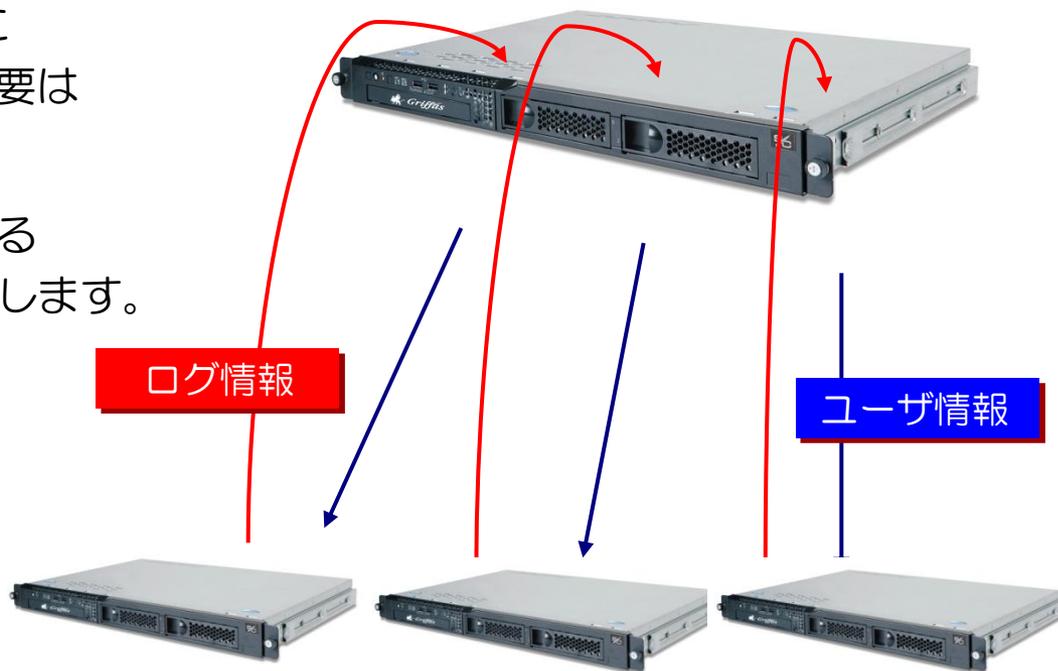
複数のGriffasを管理

セグメント毎に分散配置したGriffas2にそれぞれユーザを登録し、管理する必要はありません。

マスタサーバ（主機）に登録されているユーザ情報に基づいてクローンが稼動します。

複数のセグメントや、場所に配置する場合にも、管理者の有無を問わず一箇所での集中管理が可能です。

マスタサーバ



クローン

セグメントA

セグメントB

セグメントC

運用支援ツール

調査用に、Griffas2を通過する通信のパケットキャプチャを取得する機能を実装しました。

運用支援ツール

運用支援ツールを使用する場合、下記項目を指定し[設定]ボタンをクリックしてください。

パケットキャプチャ取得

パケットキャプチャ取得をします。
キャプチャ実行中は、他の操作ができません。
デフォルト値:10秒

パケットキャプチャ取得時間 10秒

開始

パケットキャプチャデータ

パケットキャプチャをダウンロード、削除、表示します。
合計が10Mバイトを超えるとキャプチャできなくなります。ダウンロードした後は削除するようにしてください。

#	選択	取得した日時	ファイルの大きさ
---	----	--------	----------

合計:0 バイト

ダウンロード

削除

表示

ログ転送機能

syslogを用いて認証の可否等の情報を、別サーバに転送することが可能です。

SYSLOG設定

SYSLOGを他のホストに転送したいときに転送先IPアドレスを指定します。
SYSLOGには、認証可否、ログイン、ログアウト、RADIUSへのアクセスを含んでいます。
デフォルト値: 利用しない

SYSLOGの転送先IPアドレス	<input type="text" value="192.168.32.202"/>
------------------	---

※以下、転送されたsyslogの例

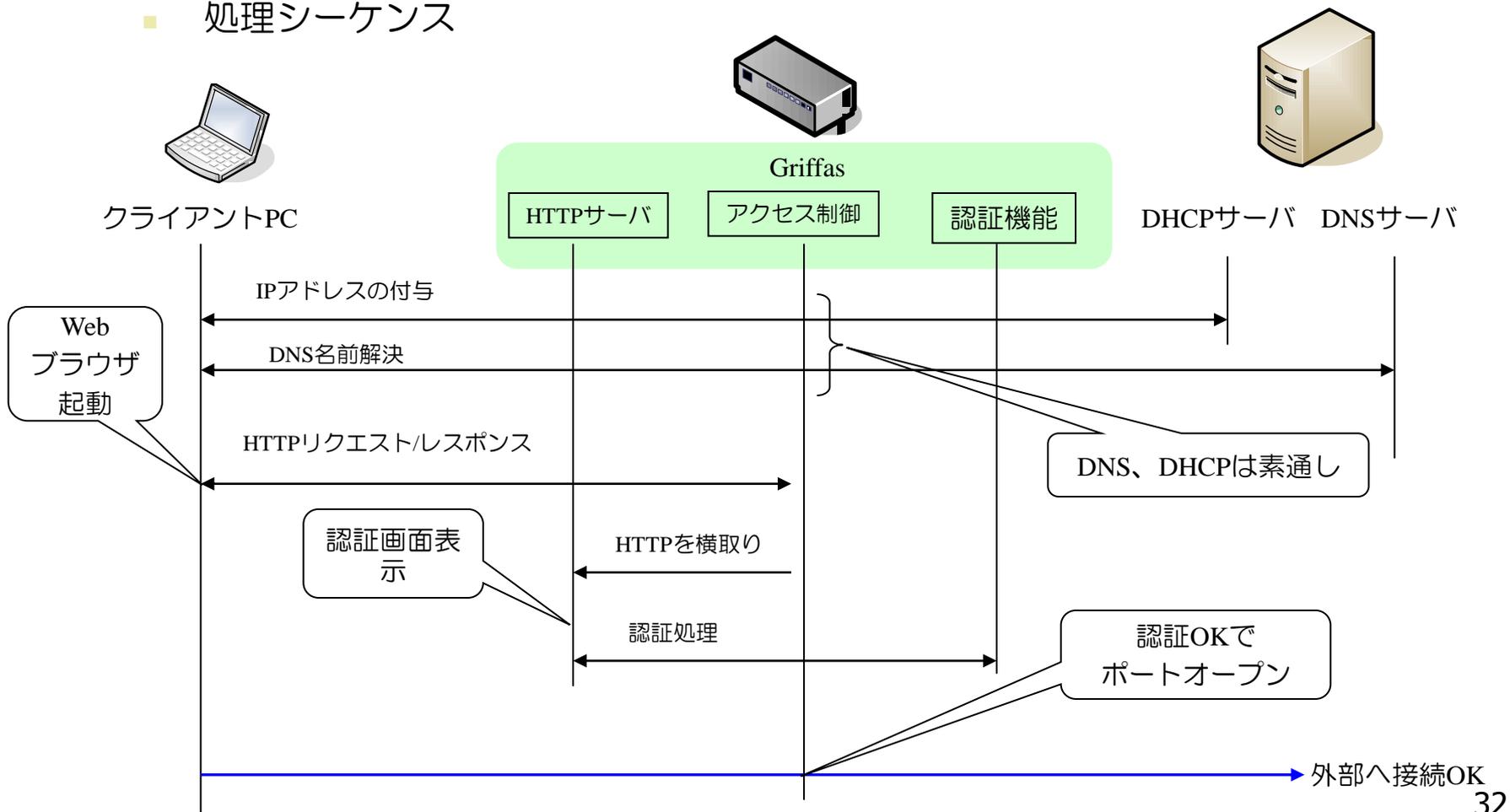
```
Jul 23 14:05:36 [192.168.16.200.2.2] GriffasAuth[7799]: acct login(stellar) ipaddr(192.168.16.12) msg:通常ログアウト
Jul 23 14:06:43 [192.168.16.200.2.2] GriffasAuth[7800]: auth login(stellar) ipaddr(192.168.16.12) result(ok) msg:
認証しました(内部DB)
Jul 23 14:07:27 [192.168.16.200.2.2] GriffasAuth[7800]: acct login(stellar) ipaddr(192.168.16.12) msg:通常ログアウト
Jul 23 14:19:11 [192.168.16.200.2.2] GriffasAuth[27286]: auth login(stttteer) ipaddr(192.168.16.12) result(fail)
msg:ログイン名が見つかりません。(内部DB)
```

その他の機能

- エージェント機能 (JavaWebStartを利用)
 - クライアントPCに対して、Griffas2からJavaのエージェントアプリケーションをダウンロードできるようにします。(配布の手間を軽減)
 - ダウンロードしたエージェントアプリケーションにて、クライアントPCのMACアドレス及び、IPアドレスを取得し、認証情報として利用します。
 - また、ダウンロードするエージェントアプリケーションのカスタマイズ等も、別途お受けする予定です。
- RADIUS連携機能
 - 外部のRADIUSサーバと連携する機能です。Accountingパケットの送信もサポートします。
- LDAP連携機能
 - 外部のLDAPサーバと連携する機能です。

Griffas2処理シーケンス

■ 処理シーケンス



Griffas2 RM 仕様

Griffas RMは中規模～大規模のエンタープライズ向けを想定したアプリケーション機です。

ハードウェアについては、最大で5年までの期間、翌営業日オンサイト保守サービスを日本全国で提供します。
(ソフトウェア保守は、メールでのお問合せや、サポートサイトによる情報提供がございます。)

仕様

- CPU: Intel Xeon-X3440 4コア 2.53GHz
- MEMORY: 4GB
- HDD: 250GB×2
- LAN: Gigabit Ethernet
- SIZE (mm): W440×H43×D560※突起物含まず

※機種・仕様については変更する場合がございますので、ご了承ください。



保守

■ Griffas2 RM

・ハードウェアサポートサービス

最大で5年までの期間、翌営業日または、翌々営業日（駆けつけ時間を保証するものではありません）
オンサイト保守サービスを日本全国で提供します。

（1）受付時間

平日の10：00～18：00（弊社休業日は除く）

（2）対応内容

現地で不具合品の交換作業を実施。（バックアップからのリストア作業、ソフトウェア設定作業は含まれません）

※オンサイト保守は製品のハードウェアのみを対象とした保守サポートです。

設定されていたデータの復旧等といった作業については、保守対象外となります。



Griffas2 価格表

Griffas2 RM 定価一覧 (税別)

タイプ	ユーザ数	2台目	型番	標準製品 1年間無償 保守コード	連続保守込み製品				単年保守
					2年間	3年間	4年間	5年間	1年間
ラックマウント	100		GRM20-100	1,180,000	1,345,000	1,485,000	1,620,000	1,750,000	174,000
	1000		GRM20-1000	1,780,000	2,015,000	2,225,000	2,420,000	2,610,000	254,000
	10000		GRM20-10000	2,980,000	3,355,000	3,705,000	4,030,000	4,320,000	414,000
		●	GRM20X	1,180,000	1,345,000	1,485,000	1,620,000	1,750,000	174,000

Griffas2 の価格は以下の要素に依存します。

1. 認証対象となるユーザ数
2. 同一システム内で複数台導入されるかどうか(2台目以降はユーザ数にかかわらず左表で 'X' の付いた型番)
3. 保守サービス連続年数。標準製品には 1年間の無償保守サービスが付いていますが、次年度以降の保守サービスをセットにした製品も用意しています。

保守込み製品の期間終了後の保守は1年毎の'単年保守'になります。(連続保守は製品購入時にのみ受け付けます)

'複数台割引' は同一システム内で複数台導入される場合に2台目を割引するものです。

スタンドアロンでお使いの場合、別システムで複数台導入される場合には適用されませんのでご注意ください。

Griffas2 RM ハードウェアの保守サービスは翌々営業日のオンサイト方式です。

ソフトウェアの保守サービスは以下の内容です。

- ・バッチの無償提供
- ・e-Mail, WebページによるQ&A対応 (当社休業日を除き 10:00~18:00 の時間帯)



株式会社 ステラクラフト

東京

〒100-0013

東京都千代田区霞が関3-7-1

霞が関ビジネスセンター404

Tel:03-5511-1151

FAX:03-5511-2122

大阪

〒532-0004

大阪市淀川区西宮原2-1-3

SORA新大阪21 13F

Tel:06-6391-7711

FAX:06-6391-7741

<http://www.stellar.co.jp/>
sales@stellar.co.jp



STELLAR CRAFT

