

SASTIK Ⅲ Thin-Client Layer技術詳細資料

(R006)

株式会社サスライト

システム構成 概要

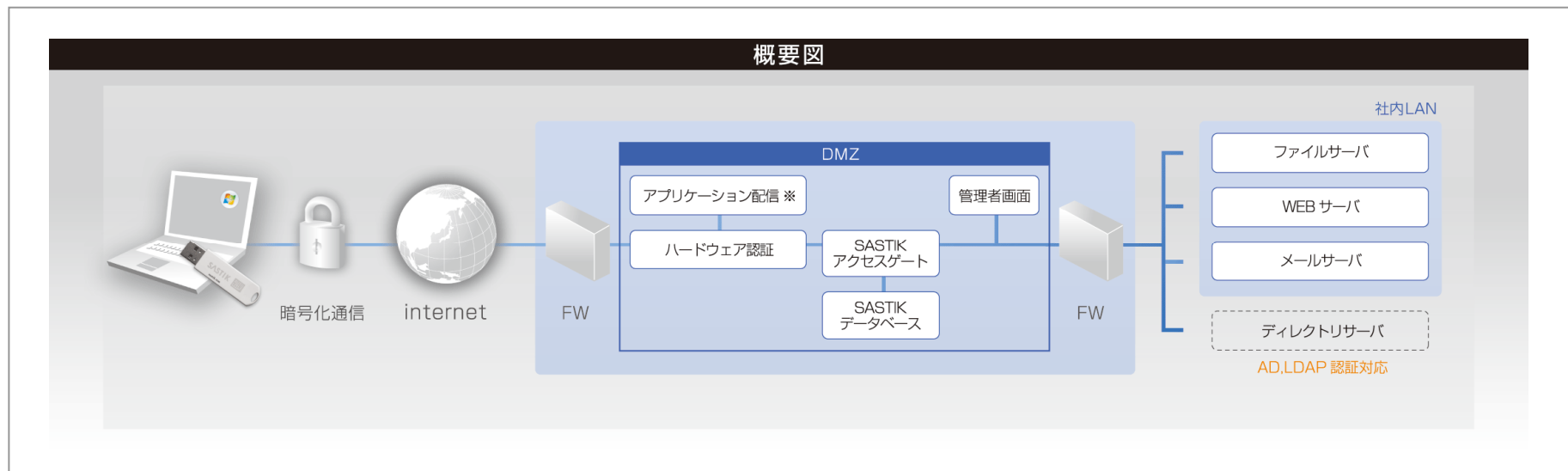


SASTIK III Thin-Client Layerは、WEBシステム、メール、ファイルサーバ、他のアプリケーションへのセキュアアクセスを実現する、アクセス権管理統合パッケージです。

- 成りすましを防御！ 物理的な鍵で守る**デバイス認証 + 暗号化通信**
- WEBサーバ、ファイルサーバへ、セキュアアクセス！
- キーを落としても大丈夫！ 重要なデータはサーバで一元管理 & ログ監視！

社内ネットワーク上の情報資産に、権限を持つ人だけをアクセスさせる、強力なアクセス権管理統合パッケージです。

遠隔地からのセキュアアクセスも可能で、内蔵したSSL-VPN、データベースにより、アクセス権限をきめ細やかに指定できます。認証手段にハードウェアや証明書等を選択すれば、より強固な本人認証も実現でき、また監査証跡に基づく4W1Hのアクセスログを取得できます。



| 対応OS

Linux

RedHat Enterprise Linux ES 4 update 7

RedHat Enterprise Linux ES 5 update 4

(VineLinux, WhiteboxLinux, CentOS等でも動作実績がございます)

※64bit版は現在非対応です。

| ハードウェアスペック目安(Linux OSの場合)

※ 500名程度での利用を想定

CPU	Xeon 3/5/7xxxシリーズ 推奨
メモリ	4GB以上 推奨
HDD	3GB(プログラム) ※アクセスログのDB格納領域に別途ハードディスク容量が必要となります。 ※ユーザー人当たり最低5MB程度のハードディスク容量が必要となります。
ネットワーク	GbitLAN 推奨

上記は、2010年7月15日現在の情報です。予告なく変更される場合がございますので、予めご了承ください。

また、導入構成によって変更となる場合がありますので、最新情報及び詳細につきましては、当社営業またはサポートに随時お尋ねください。

対応環境(クライアント)

対応環境

日本語版WindowsXP(SP3以上)/VISTA/ Windows7
Microsoft Internet Explorer 6 (SP1以上)~8
解像度800×600ピクセル 16bit(High Color)以上推奨
※Microsoft社のサポート対象製品が対象となります。
※64bit版は現在非対応です。

ハードウェア

DOS/V PC/AT互換機(OADG仕様) ※USB1.1以上搭載機
[CPU] IntelPentium4 プロセッサー以上を推奨
[HDD] 最低10MB以上の空き容量(OSが利用する以外の部分として)
[Memory] 各OSの推奨メモリに準じます
※ブラウザに関するメモリ使用量は閲覧しているページに依存します。

その他

ネットワーク接続環境(ブロードバンド環境推奨)

上記は、2010年7月15日現在の情報です。予告なく変更される場合がございますので、予めご了承ください。
また、導入構成によって変更となる場合がありますので、最新情報及び詳細につきましては、当社営業またはサポートに随時お尋ねください。

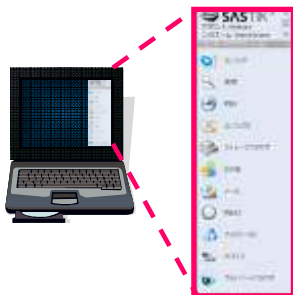
SASTIK Server



SASTIK Server

- アプリケーションマネジメント機能
⇒ 許容した特定のグループに対してのみ、任意のプラグイン(アプリケーション)を提供。
- ファイルサーバ機能
⇒ ユーザに対し、許容した容量のファイル保存領域を提供。
- 暗号化通信によるWebアプリケーション中継機能
⇒ 既に存在する社内のWebアプリケーションに、どこからでも安全にアクセス。
- ストレージプロキシ機能
⇒ 既存の社内のファイルサーバに、どこからでも安全にアクセス。

SASTIK ツールバー



ツールバー

- ツールバー基本機能
⇒ デスクトップに常駐する、表現力豊かなメニューバー機能。
- Webブラウザ機能
⇒ SASTIKⅢ標準のWebブラウザ機能。
- ストレージビューア機能
⇒ SASTIKⅢに登録されたストレージを一括表示する機能を持ったファイルビューア。

管理者用ツール



管理者用ツール



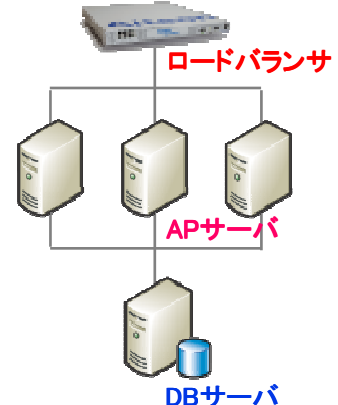
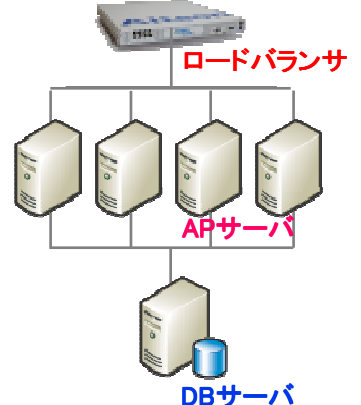
- アカウント管理機能
⇒ 新規ユーザの登録や停止、パスワードの再発行などを行なう機能
- プラグイン管理機能
⇒ SASTIK III Thin-Client Layer用プラグインの登録や削除を行なう機能
- ドメイン管理機能
⇒ ドメインをグループ化し、利用可能プラグインや各種設定を個別に設定する機能
- ハードウェア管理機能
⇒ SASTIK標準デバイスとアカウントを紐付け、管理するための機能
- ログ管理機能
⇒ アクセスログの閲覧、検索を行なうための機能



構築に必要なもの

1. サーバ用 OS	RedHat Linux ES 4 update 7 RedHat Linux ES 5 update 4
2. サーバ用ハードウェア	※次ページ参照
3. SASTIKパッケージ	SASTIK III ServerインストールCD SASTIK デバイス
4. ミドルウェア (OSに含まれていないもの)	Tomcat, MySQL, JDK, CPANモジュール 等 (詳細についてはインストールマニュアルを御参照下さい)
5. グローバルIPアドレス	外部接続の場合には、グローバルIP(固定IP)が必要となります。 既にある場合は必要ありません。
6. SSL証明書	安全な暗号化通信のためにはベリサイン社などのSSL証明書の取得が必要です。 ※SSL証明書の取得には、ドメインが必要となります。
7. ファイアウォール	別ネットワークとの接続にファイアウォールの設置を推奨します。

機器構成例 I

ユーザ数規模 (参考値)	(例)500ユーザ	(例)1000ユーザ	(例)2000ユーザ	(例)4000ユーザ
機器構成例	 <p>APサーバ + DBサーバ</p>	 <p>APサーバ DBサーバ</p>	 <p>ロードバランサ APサーバ DBサーバ</p>	 <p>ロードバランサ APサーバ DBサーバ</p>
アプリケーション (AP) サーバ	同一筐体 CPU:Xeon 3/5/7xxxシリーズ推奨 メモリ:4GB以上推奨 HDD:70GB以上 SASディスク推奨 RAID1以上推奨	1台 CPU:Xeon 3/5/7xxxシリーズ推奨 メモリ:4GB以上推奨 HDD:70GB以上 SASディスク推奨 RAID1以上推奨	3台 CPU:Xeon 3/5/7xxxシリーズ推奨 メモリ:4GB以上推奨 HDD:70GB以上 SASディスク推奨 RAID1以上推奨	4台 CPU:Xeon 3/5/7xxxシリーズ推奨 メモリ:4GB以上推奨 HDD:70GB以上 SASディスク推奨 RAID1以上推奨
データベース(DB) サーバ		1台 CPU:Xeon 3/5/7xxxシリーズ推奨 メモリ:4GB以上推奨 HDD:250GB以上 SASディスク推奨 RAID1以上推奨 冗長構成推奨	1台 CPU:Xeon 3/5/7xxxシリーズ推奨 メモリ:4GB以上推奨 HDD:250GB以上 SASディスク推奨 RAID1以上推奨 冗長構成推奨	1台 CPU:Xeon 3/5/7xxxシリーズ推奨 メモリ:4GB以上推奨 HDD:250GB以上 SASディスク推奨 RAID1以上推奨 冗長構成推奨

※上記機器構成は参考資料になります。ご利用方法によって、アプリケーションの快適な動作環境・レスポンスが変わるため、詳細は別途お問い合わせください。

※上記ユーザ数は、システム規模を示す参考値となります。同時接続数を示すものではありません。

※インフラ(回線、スイッチ等)の冗長化については図示しておりません。既存ネットワーク状況を含め、別途お問い合わせ下さい。

※64bitOSには対応していません。

※サーバハード及びOS、SSL証明書、ロードバランサ、クラスタソフト等に関しましては別途ご用意いただく必要がございます。

※5000ユーザ以上でご利用の場合は、別途ご相談ください。

SASTIK III Thin-Client Layerの特徴



✓ 独自の、URLマッピング拡張機能により絶対URLや<BASE>タグ等のコンテンツに対応。

✓ バックエンドサーバ中継に、SSL(https)も対応。サーバ間の通信もよりセキュアに運用が可能。



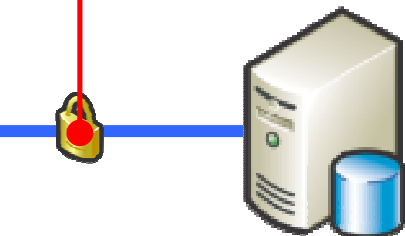
ユーザ側



Internet

暗号化通信

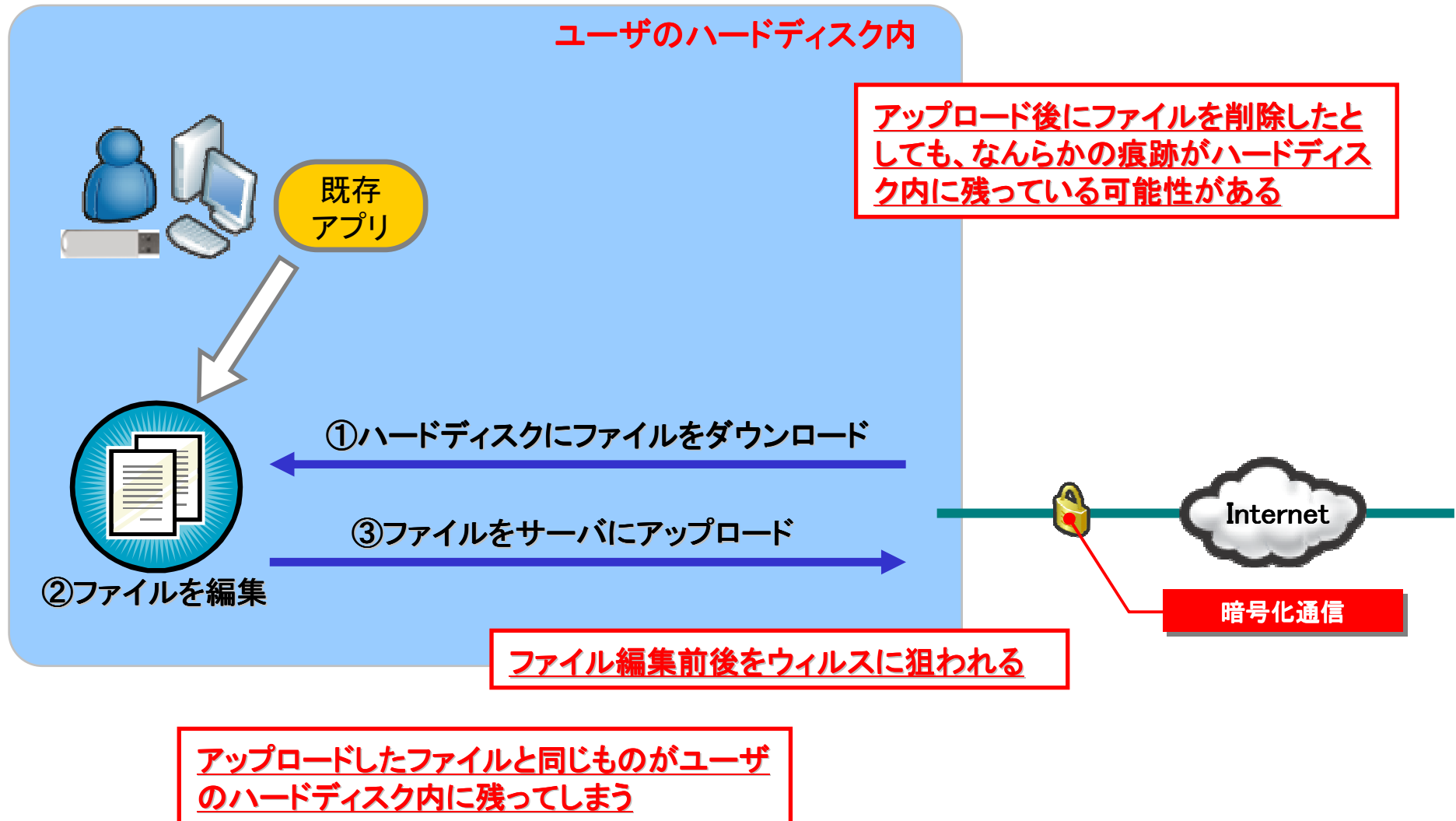
SASTIK Server



✓ 接続元IPアドレスによるアクセス制御に対応。デバイス+パス+接続IP等、組み合わせアクセス制御が可能に。

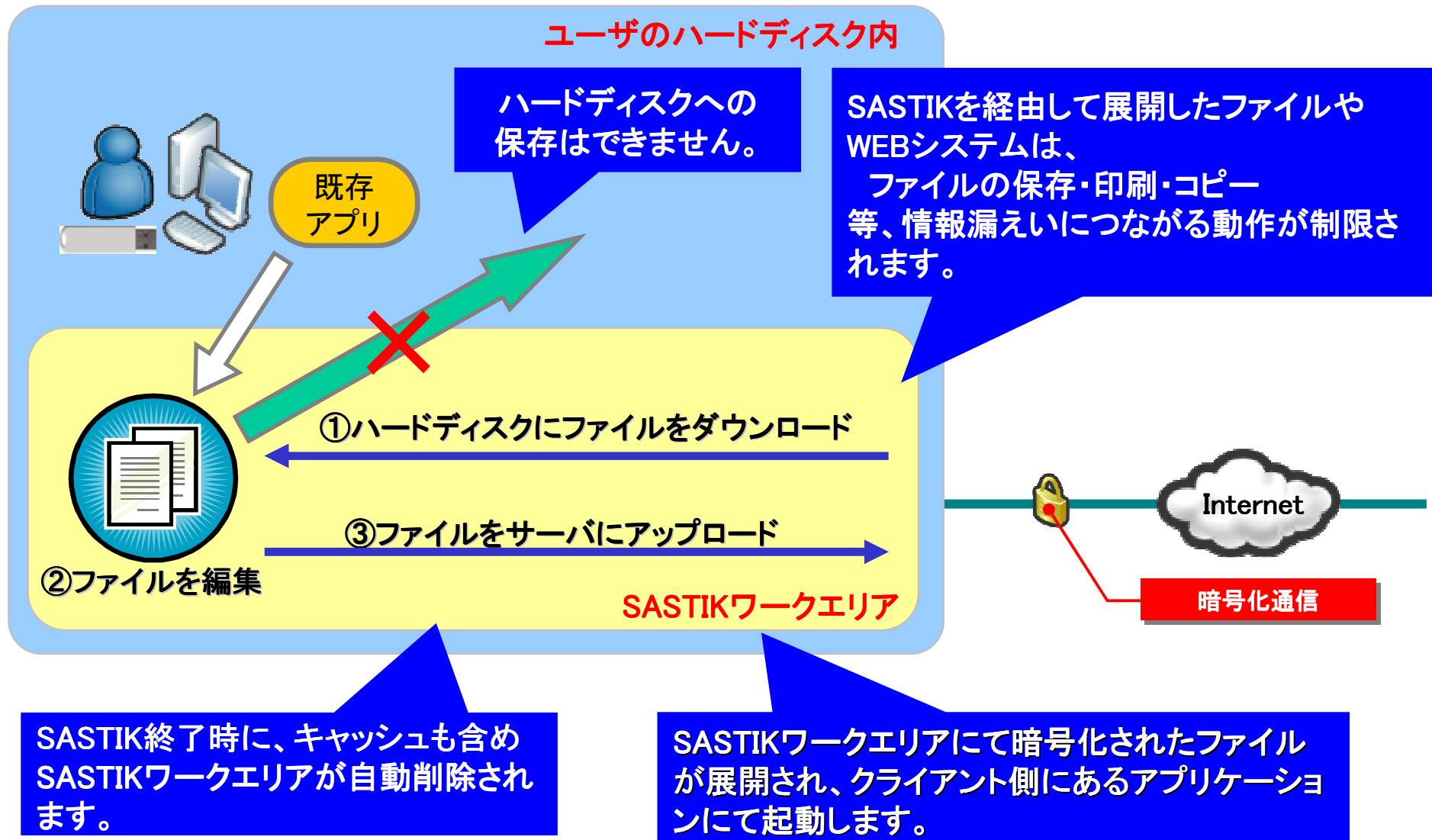
✓ ディレクトリ認証(ActiveDirectory, LDAP等)に対応。LDAPS(LDAP over SSL)にも対応。Z

通常のファイルの読み書きの仕組み

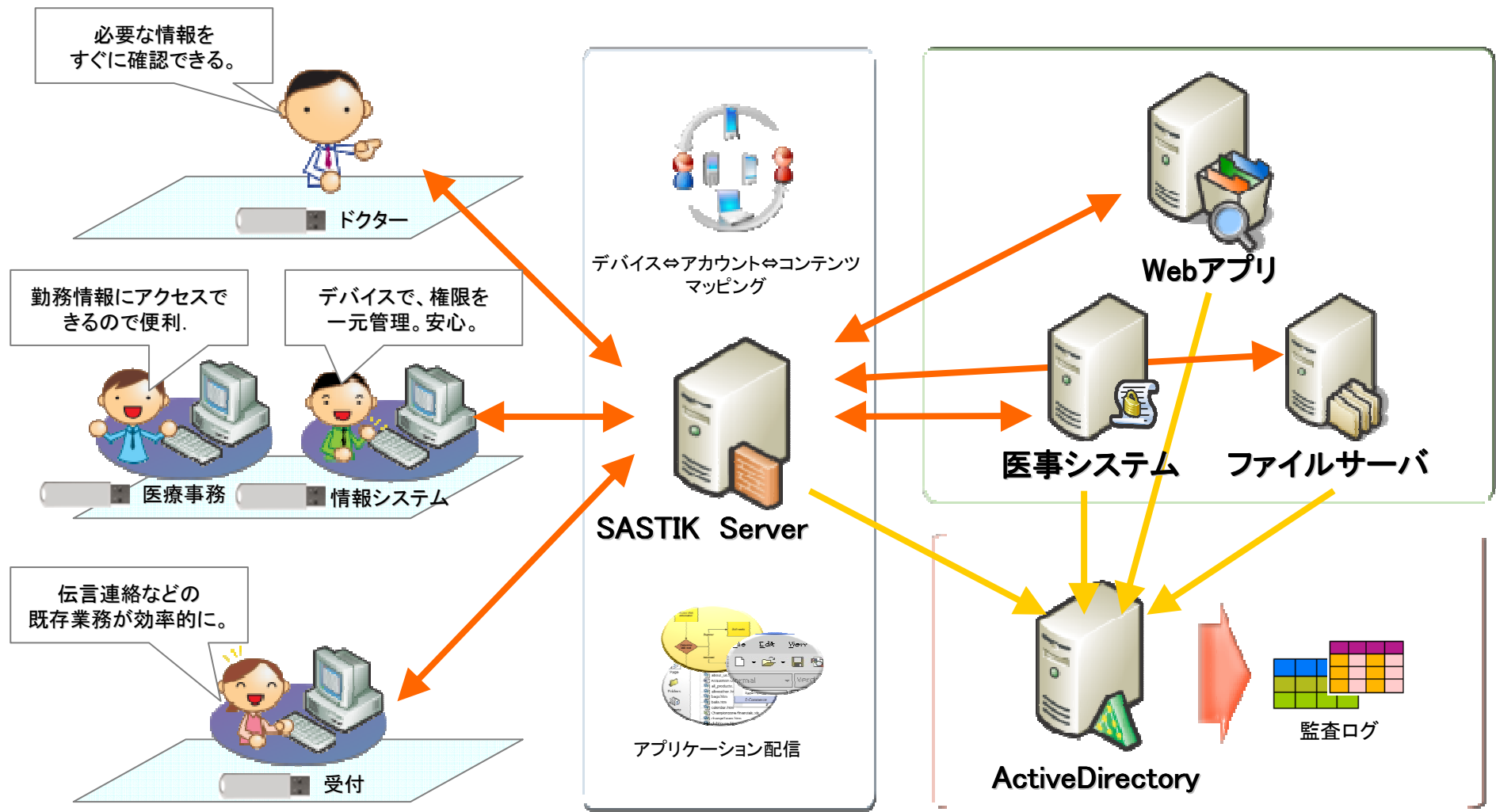


通常のファイルの読み書きの仕組み

⇒SASTIK起動時に「SASTIKワークエリア」が自動的に作成される



事例：医療系法人での導入形態

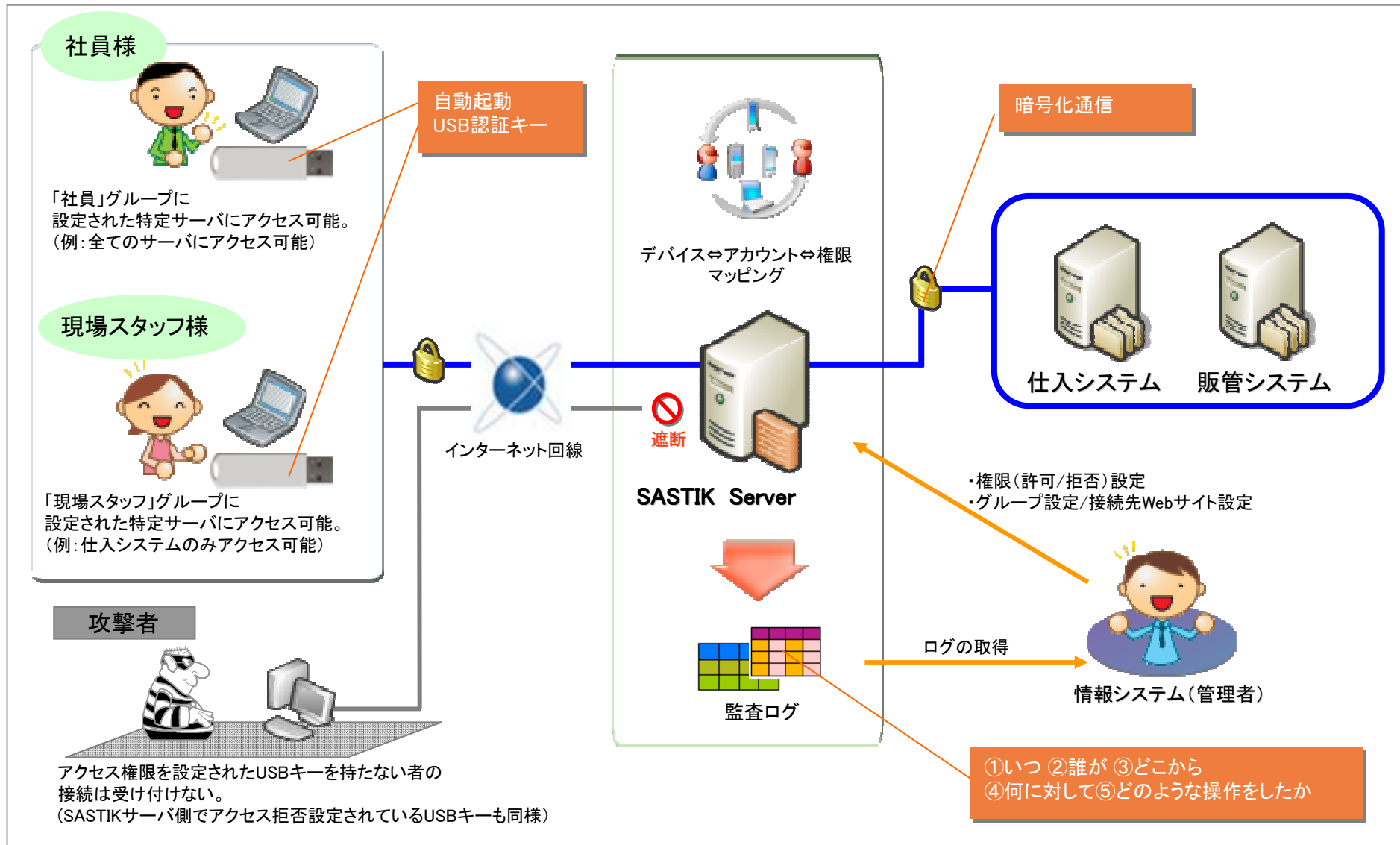


バックヤード業務を軽減
→医療業務への集中

権限情報の一元管理

事例：既存WEBシステムのデバイス認証拡張（流通大手）

USB自動起動キー(SASTIK-0MB)を使った**USBデバイス認証+暗号化通信**を実現します。
「管理者(Administrator)」、「社員(proper)」、「ゲスト(guest)」等のグループを作成でき、**グループに応じたアクセス権限を設定**できます。
複数のWebサーバを柔軟にマッピングする機能を搭載し、流動的な現場の権限変更への対応が可能です。



対応内容

- SASTIKサーバ内で行っているユーザ認証(ID、パスワード認証)をLDAPにて実施します。
 - ・ LDAP Ver2、Ver3をサポート
 - ・ パスワード認証方式としてSASLをサポート
(「PLAIN」、「DIGEST-MD5」、「CRAM-MD5」、「ANONYMOUS」)
 - ・ LDAPS(LDAP over SSL)にも対応

対応アプリケーション

- SASTIK III Server

注意事項

- ユーザ登録時のSASTIKアカウント名をLDAPに登録されているアカウントのPRINCIPALと同じにしておく必要があります。
- 一度ビジネスドメイン作成時に選択した認証方式を後で変更することはできません。
- LDAPサーバへの更新は行ないません

運用イメージ

- LDAP連携を行うためには、以下3つの管理者作業が必要です。
 - 1) LDAP自体でのユーザ登録(SASTIK外)
 - 2) ビジネスドメイン作成時に**ユーザ認証モード**(LDAP認証/SASTIK認証)で”LDAP認証”を選択し、**LDAP認証URL**、**SASL認証方式**の2つを設定する
 - 3) アカウント登録時にパスワードを空で登録する(CSVファイル内)



キャッシュクリア設定項目

- ✓ 終了時にAuto Complete Valuesを削除
- ✓ 終了時にクリップボードを削除
- ✓ 終了時にゴミ箱を削除
- ✓ 終了時にFlashローカル記憶領域を削除 (※)
- ✓ 終了時にインターネット履歴を削除
- ✓ 終了時に最近使用したファイル履歴を削除 (※)
- ✓ 終了時にユーザのTEMP領域を削除 (※)
- ✓ 終了時にTemporary Internet Files (クッキー含む)を削除

管理画面メニュー

- ログアウト
- システム管理
- ビジネスドメイン管理
 - ビジネスドメイン一覧
- QMBキー管理
- アカウント管理
- SASTIKオブジェクト管理
- バックエンドサーバ管理
- 共有ストレージ管理
- アクセスログ管理
 - アクセスログ検索
 - アクセスログダウンロード
 - アクセスログ削除

ビジネスドメイン一覧

ビジネスドメイン[200_AcademicDemoTCL]に関連するパラメータを設定します。
※プロパティの変更を反映するためにはSASTIKサーバの再起動が必要となります。

[ビジネスドメイン設定](#) [標準利用オブジェクト設定](#) [SASTIK Configファイル設定管理](#)

クライアント設定	
項目	設定値
終了時にAuto Complete Valuesを削除するか否か	N
終了時にクリップボードを削除するか否か	N
終了時にゴミ箱を削除するか否か	N
終了時にFlashローカル記憶領域を削除するか否か	N
終了時にインターネット履歴を削除するか否か	N
終了時に最近使用したファイル履歴を削除するか否か	N
終了時にユーザのTEMP領域を削除するか否か	N
終了時にTemporary Internet Files(クッキー含む)を削除するか否か	N
ロゴ画像URL	
ログイン前に表示するメッセージ	学校現場からの情報漏えい"ゼロ"を目指
ツールバーの初期起動モード(1:通常表示(FIXED), 2:自動的に隠す(AUTO), 3:非表示(HIDDEN))	1
ツールバー未操作時の自動ログアウトまでの時間(分単位)(0:自動ログアウトしない)	0

管理者画面からビジネスドメイン毎に設定可能

※の項目は、ログイン以降に発生した情報のみ削除します。
その他の情報は全削除処理となります。

資料: 管理者画面例 (アクセスログ検索)

管理画面メニュー

ログアウト

- システム管理
- ビジネスドメイン管理
- OMB キー管理
- アカウント管理
- SASTIK オブジェクト管理
- バックエンドサーバ管理
- 共有ストレージ管理
- アクセスログ管理
 - アクセスログ検索
 - アクセスログダウンロード
 - アクセスログ削除

アクセスログ検索

登録されているアクセスログを検索します。

検索条件を入力してください。(AND検索)
※期間の指定は"YYYYMMDD"のフォーマットで指定してください。(例: 2006年1月2日の場合"20060102")
※実行APIとアカウントはあいまい検索が可能です。

検索条件	設定値
期間(from)	<input type="text"/>
期間(to)	<input type="text"/>
SASTIKオブジェクト	選択してください
実行API	<input type="text"/>
実行結果	選択してください
アカウント	<input type="text"/>

Ok

アクセスログ検索

以下の情報が確認できます。

- ✓ 日付
- ✓ イベント
- ✓ 実行結果
- ✓ 対象アカウント

以下の機能も利用できます。

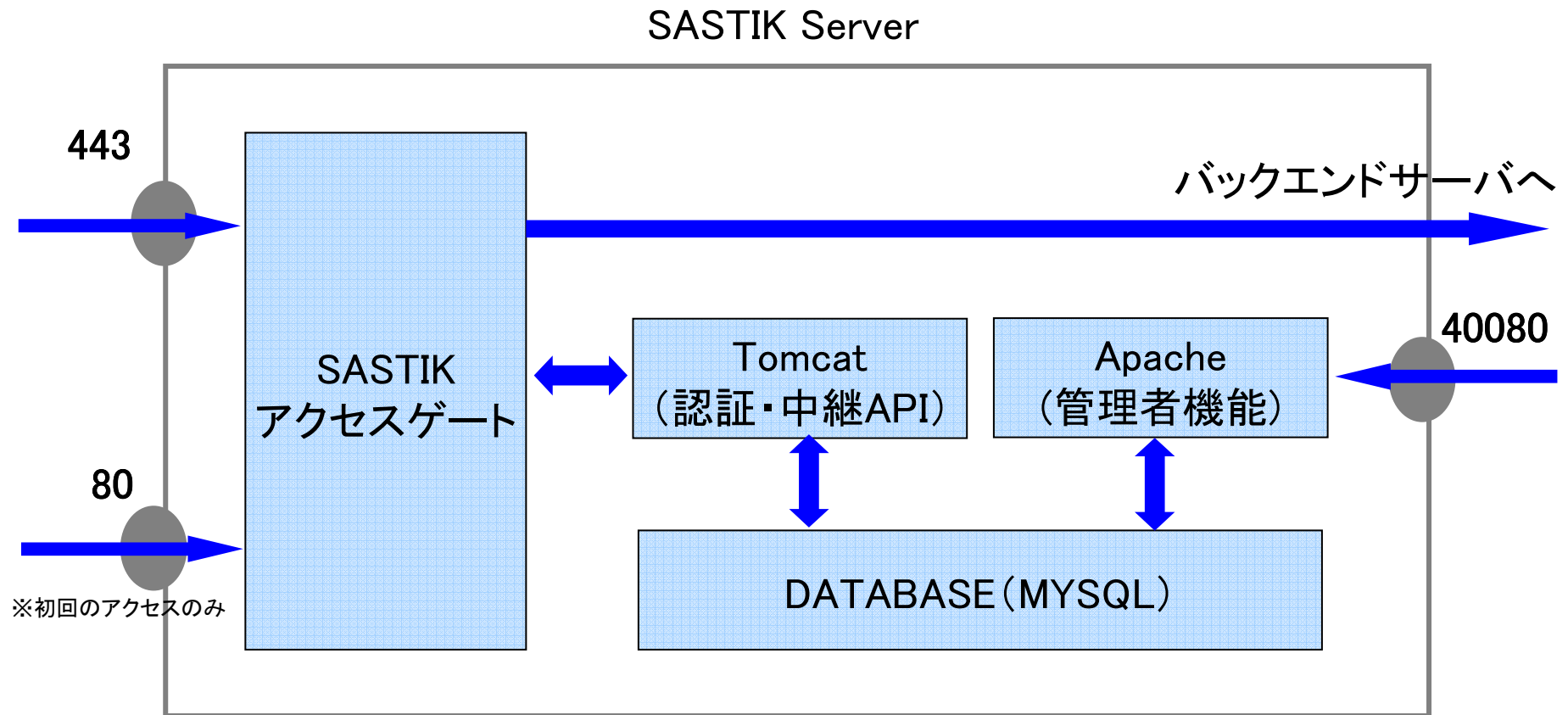


CSVダウンロード機能



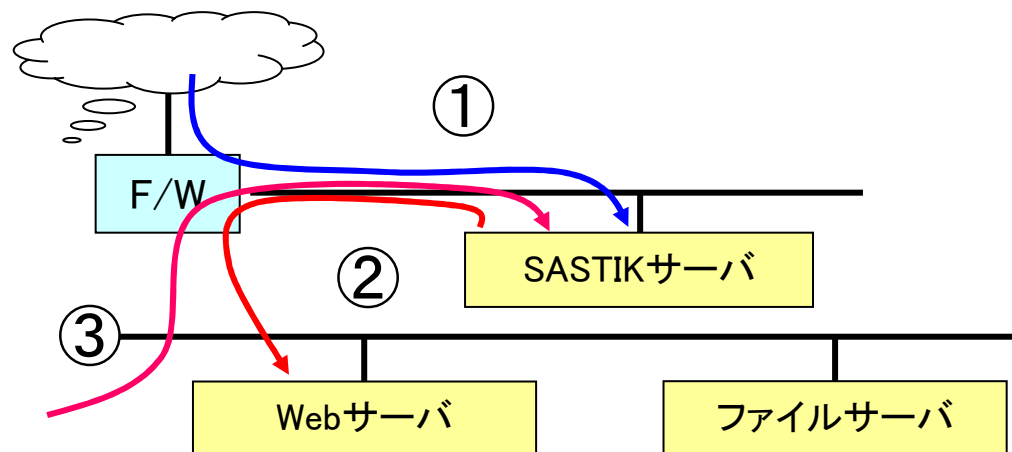
条件指定検索機能

資料：各ミドルウェアと通信ポートの概要



- ポート80は、USBキー(SASTIK OMB)が自動起動した際の最初の通信のみ利用されます。以降はすべてSSL通信(ポート443)で通信を行います。
- 外部向けの通信ポートは、SASTIKアクセスゲートのプロセスがLISTENしています。
- 管理者機能が、Webインタフェースで提供されます。ApacheがLISTENしています。

資料:ファイアウォールの設定例



①WAN→DMZ(SASTIKサーバ)

Source	Destination	プロトコル	ポート番号	用途
Any	SASTIKサーバ	HTTP	TCP/80	クライアントからのアクセス
Any	SASTIKサーバ	HTTPS	TCP/443	クライアントからのアクセス

②DMZ(SASTIKサーバ)→LAN

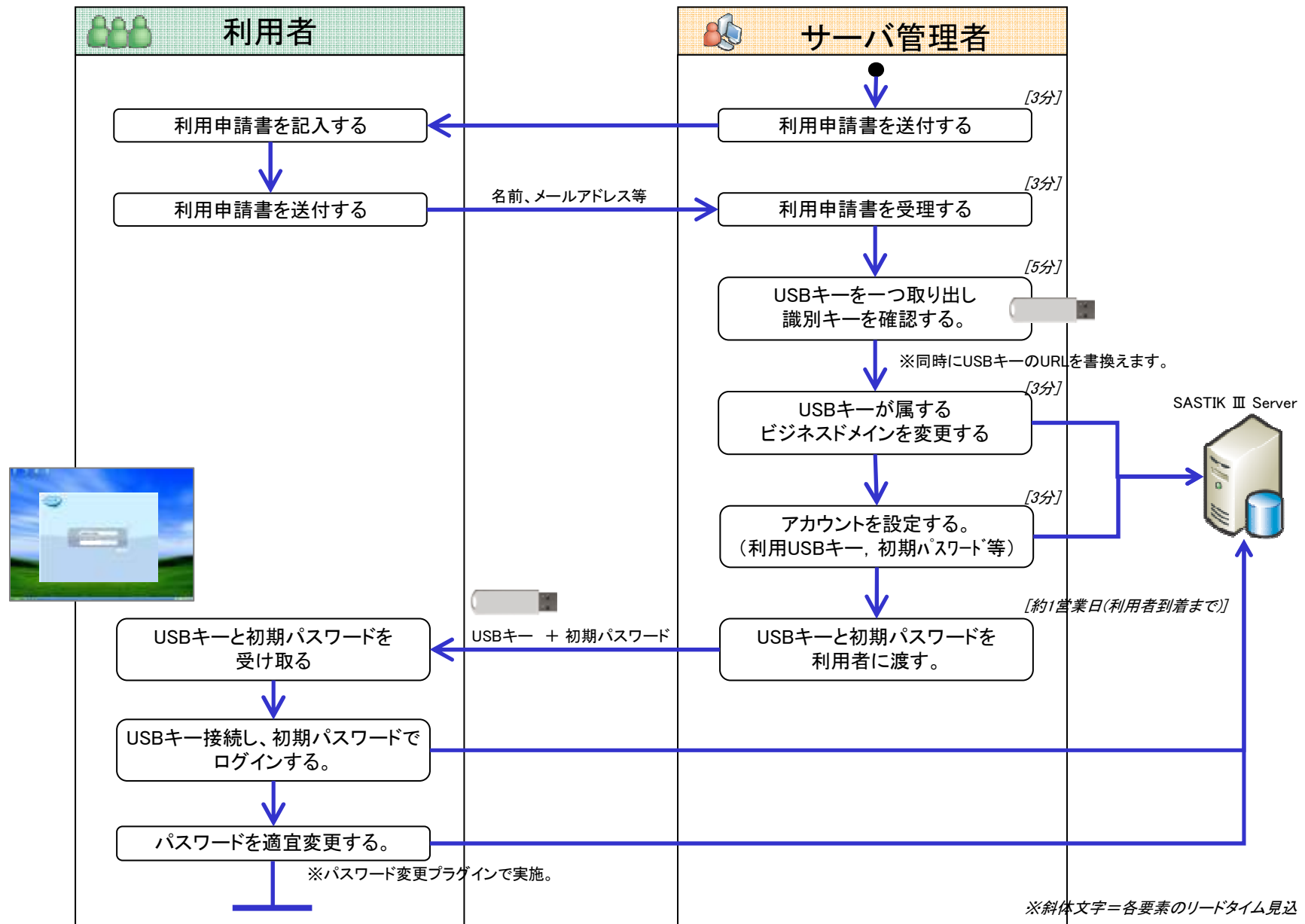
Source	Destination	プロトコル	ポート番号	用途
SASTIKサーバ	ファイルサーバ	HTTP/HTTPS	Udp 137,138 Tcp 139,445	ファイルサーバアクセス
SASTIKサーバ	WEBサーバ	HTTP/HTTPS	TCP/80 or 443	WEBサーバアクセス

③LAN→DMZ(SASTIKサーバ)

Source	Destination	プロトコル	ポート番号	用途
Any(※)	SASTIKサーバ	HTTP	TCP/40080	SASTIK管理者機能

※IPアドレス/セグメントなどで制御をかける場合はFireWallの設定に従って下さい。

資料: 運用例 (利用開始時のフロー例)



資料: 運用例 (紛失及び故障時のフロー例)

