マトリクス認証®を使ったワンタイムパスワード

# SECUREMATRIX®

## 覚えやすいパスワードには大きなリスクが潜んでいます。

**そのパスワード覚えられますか?**

- 不正アクセス
- 機密情報の流出/漏洩
- 企業価値/競争力の低下
- コンプライアンス違反

破られにくいパスワードが必要

- 8桁以上の長いパスワード
- 数字と記号を併用
- 大文字も小文字も併用
- 辞書にある文字列は禁止
- しかも1ヶ月ごとに変更

## 既存の認証ソリューションは様々なコストが掛かります。

**認証に多大なコストを掛けますか?**

### 初期コスト

既存の認証ソリューションは、「デバイス」を購入する必要があります。

- ワンタイムパスワードトークン
- ICカード
- USB等

### 買い直しコスト

電池の消耗、破損、紛失の場合にデバイスを買い直す必要があります。

### 運用コスト

デバイスの配置、棚卸し、メンテナンス、初期設定等、多額の運用コストが掛かります。

## コストを削減したい「企業」
## セキュリティを高めたい「IT管理者」
## 面倒なことはしたくない「社員」
# 選ばれるのは「マトリクス認証®」

複雑なパスワードをもう覚える必要はありません。また高価な認証デバイスを利用する必要はありません。「マトリクス認証®」は、ユーザがあらかじめ設定した「位置」と「順番」(=イメージパスワード)を使って、毎回ランダムに表示されるマトリクス表から数字を抜き出しワンタイムパスワードとして認識させる、まったく新しい認証システムです。様々な立場の方が抱えるパスワードの悩みを一気に解決するのが「SECUREMATRIX®」です。

**毎回変わるマトリクス表(乱数表)**

**覚えるのは、本人が設定した「位置」と「順番」**

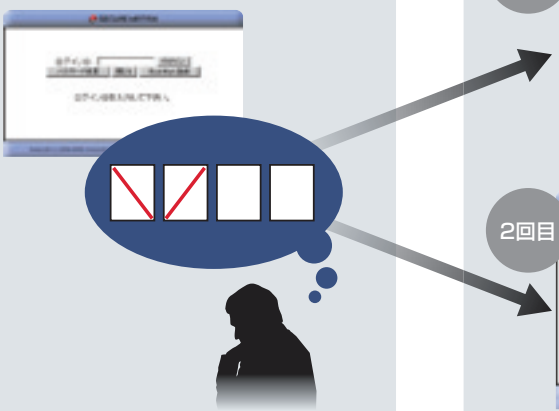
**パスワードは「ワンタイム(使い捨て)」になる!**

## マトリクス認証®のしくみ

### 自由な組み合わせができる「位置」と「順番」。

#### ● パスワードイメージ

あらかじめ自分の好きなパスワードイメージを登録しておきます。



#### ● アクセスごとに異なるマトリクス表 ▶ 異なるパスワード

1回目

マトリクス認証®は、アクセスの度に表示される数字が変わるマトリクス表を使用しています。
たとえば「V」というイメージのパターンを、あらかじめ登録しておきます。

入力するパスワード
**74894354** (一度だけ)

2回目

マトリクス認証®は、毎回マトリクス表に表示する数字が変わるので、二度と同じパスワードを入力することはありません。

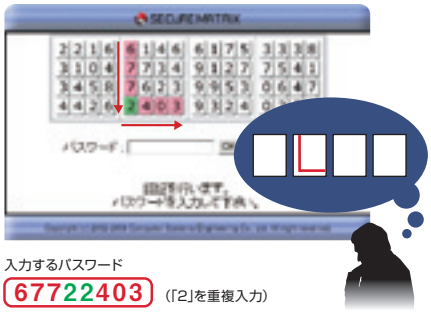
入力するパスワード
**41406182** (一度だけ)

### 「形」で覚える。それは「忘れにくい。覚えやすい。」

頭に思い描くどのようなイメージでも、
マトリクス表から抽出することができます。

入力するパスワード
**43655724** (一度だけ)

同じ場所を重複して選択する設定も可能です。



入力するパスワード
**67722403** (「2」を重複入力)

固定パスワード(英数字)と組み合わせて、
さらに強固なパスワードを設定できます。


固定パスワード併用設定例

例1(英字例) **0007abcd**

例2(数字例) **01020374**

(組合わせ設定は自由)

# SECUREMATRIX®が選ばれる理由

## 認証デバイスの紛失は重大インシデント!!

認証デバイスは、企業のドアを開ける鍵と言えます。外出先での紛失、盗難は、情報資産をリスクにさらすことになります。

SECUREMATRIX® なら

**デバイス紛失のリスク**

**0(ゼロ)!**

## 認証デバイスの管理は大変な作業！

「どのデバイスを誰が持っているのか？」
「地方支社や海外拠点の配布は？」
「退職者のデバイスの返却は？」…等
デバイスを利用すると「人」「距離」「時間」の問題が管理者の負担につながります。

SECUREMATRIX® なら

**デバイス管理の負担が**

**0(ゼロ)!**

## 認証デバイスの買い直しは、コストの無駄遣い！

持ち運ぶ必要のある認証デバイスはこわれたら買い直し。無くしても買い直し…。
電池の消耗などにより定期的に買い直す必要があります。
…ランニングコストが高くなります。

SECUREMATRIX® なら

**デバイス買い直しコストは**

**0(ゼロ)!**

## 認証デバイスは地球に優しくない!!

認証デバイス(20gと想定)の製造→11Kgの$CO_2$が排出(成木の1年間の吸収量)認証デバイスを5,000ユーザ分の製造時に排出される$CO_2$は東京ドーム1個分以上となります。

※当社独自算出に基づきます。

SECUREMATRIX® なら

**デバイス製造時に排出される$CO_2$は**

**0(ゼロ)!**

SECUREMATRIX

## 固定パスワードもコストが掛かっている!!

複雑なパスワード→忘れやすい→パスワード再発行。
パスワードの再発行は、意外に大きな負担となります。
→本当に本人かどうか確認する必要があります。
→IT統制ポリシーに基づいた再発行承認フローを実施する必要があります。
認証デバイスに頼らず、固定パスワードでセキュリティを向上させても見えにくい「運用コスト」が掛かります。

※当社の事例による算出(5年間での比較)

SECUREMATRIX なら

**固定パスワード運用に掛かるコスト**
**＝**
**SECUREMATRIX 導入費用**

## コンプライアンスへの対応は今や常識!!

内部統制、IT統制が求められるなか、認証に対する細かいルールをユーザに徹底させる仕組み作りは、大変な作業です。定期的なパスワード変更や、大文字/小文字、記号の組合せ等、ユーザに徹底するのは、困難です。

SECUREMATRIX なら

**認証のルール、ポリシーを**
**一元管理**

## 「BCP(事業継続計画)」への取り組み

「パンデミック」や「災害」時には、オフィスではなく自宅等から業務を遂行しなければなりません。いつくるかわからない非常事態でも、仕事ができる環境が必要です。もはや仕事は場所を選びません。

SECUREMATRIX なら

**ブラウザがあれば**
**どこからでも認証可能**

SECUREMATRIX®

# BROWSER LOGON

▸ for Active X ▸ for SUN JRE ▸ for Flash

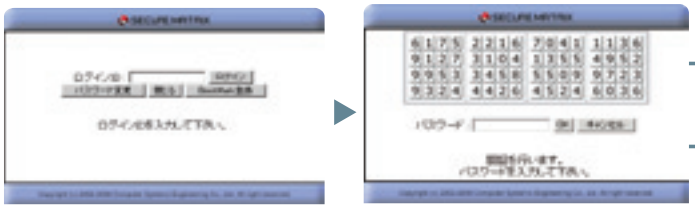
SECUREMATRIX 認証サーバ

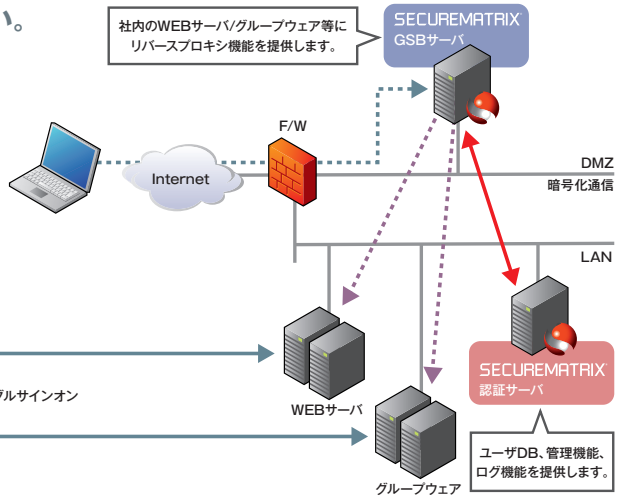
SECUREMATRIX GSBサーバ

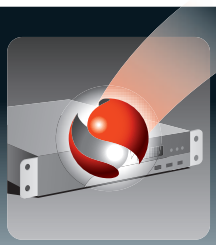
## どこからでもブラウザがあれば「マトリクス認証®」

### せっかくのWEBアプリケーション。何も配らずに安全に使いたい。

- WEBアプリケーションの認証を「マトリクス認証®」に
- 基本(ベーシック)認証/フォーム認証に対応したシングルサインオン機能
- グループや役職ごとに柔軟なアクセスコントロールを実現
- 信頼のおける他ネットワークとのやり取り相互間で「マトリクス認証®」を実現するローミング機能を実装





SECUREMATRIX®

# RADIUS LOGON

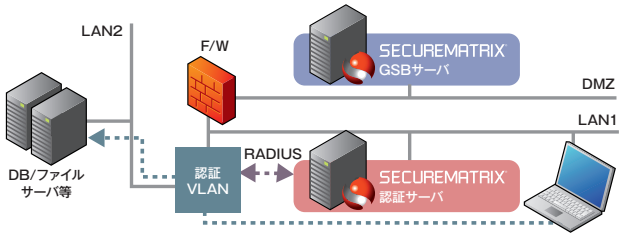
SECUREMATRIX 認証サーバ

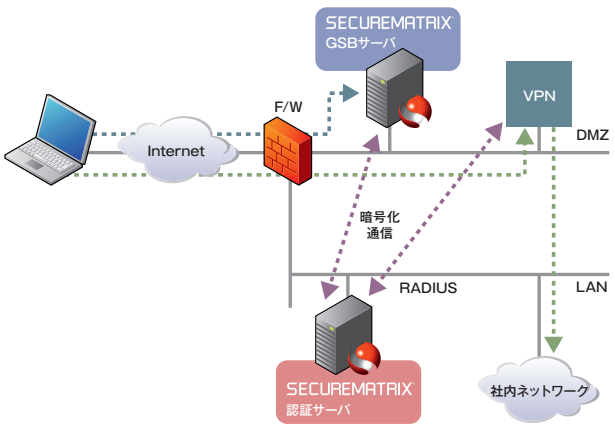
SECUREMATRIX GSBサーバ

## RADIUS対応機器の認証を「マトリクス認証®」に。

### 通信経路が安全でも、「認証」が脆ければ意味がない。

- VPNやファイアウォールと連携し、認証を強化
- SSL-VPNは、ブラウザだけでダイレクトログオン
- 独自のRADIUSサーバを実装。複数のRADIUSクライアントをサポート
- RADIUSアトリビュートに対応
- 認証VLAN等のRADIUS対応機器とも連携可能



SECUREMATRIX

# MOBILE LOGON

▶ for Apple iPhone / iPad

SECUREMATRIX 認証サーバ

SECUREMATRIX GSBサーバ

## どこにいても手のひらの上で「マトリクス認証®」を。

**機動力を、最大限に引き出す「セキュリティ」を。**

- iPhone等のスマートフォンから「マトリクス認証®」で社内リソースにアクセス
- DESKTOP LOGONとの併用で、スマートフォンでも同じ「マトリクス認証®」が可能
- WEBアプリケーションへのログオン、VPN接続のログオンのセキュリティを強化

※ 2010年7月リリース予定

マトリクス表の表示画面

キーボードによるパスワード入力画面

- SFA/CRM
- グループウェア
- Eラーニング
- WEBシステム
- 仮想デスクトップ

※ 別途スマートフォンの設定やネットワーク機器との連携を必要とする場合があります。

SECUREMATRIX

# DESKTOP LOGON

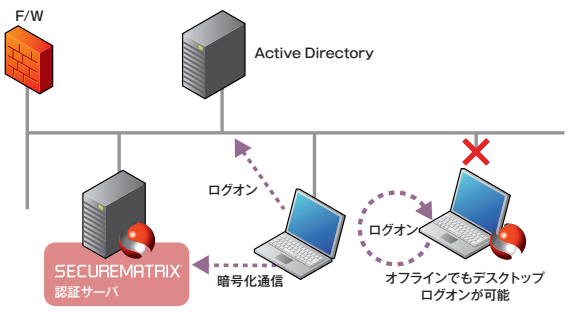
▶ for Microsoft® Windows XP® ▶ for Microsoft® Windows Vista®

SECUREMATRIX 認証サーバ

## 「社内」でもデスクトップへのログオンは「マトリクス認証®」で。

**社内も「マトリクス認証®」に統一すれば、使い勝手はさらに高まる。**

- 「Ctrl」+「Alt」+「Del」を押したら、「マトリクス認証®」が可能
- 意識することなくActive Directoryと連携が可能
- ネットワークに接続されていなくても、利用可能(オフライン認証)
- スクリーンセーバーのパスワードロック時にも利用可能



SECUREMATRIX®

# INTRANET LOGON

SECUREMATRIX 認証サーバ

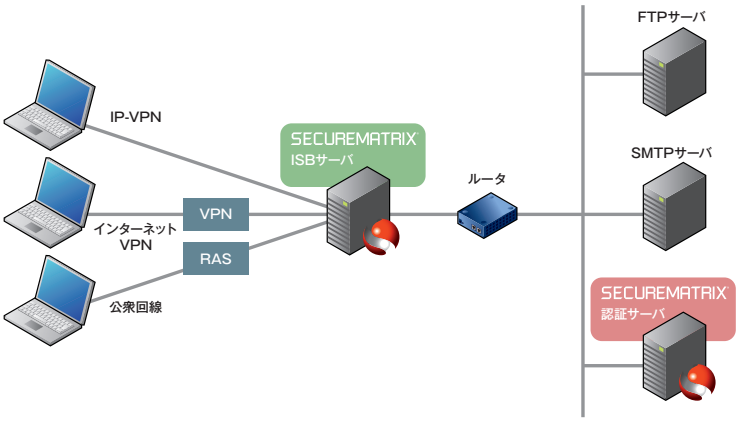
SECUREMATRIX ISBサーバ

## パケットのフィルタリングも「マトリクス認証®」を。

### セグメントを守るため、不要なパケットは通さない。

- IP-VPNやインターネットVPNから社内へのアクセスを制御
- LAN to LANで、サーバセグメントへのアクセスを制御
- 認証を受けたユーザのみが、登録された特定のアプリケーションとサーバにアクセス
- IPアドレスやポート番号によるコントロールが可能


パケット通信中表示




SECUREMATRIX®

# APPLICATION INTERFACE

▶ Windows DLL Version. ▶ JAVA Version.

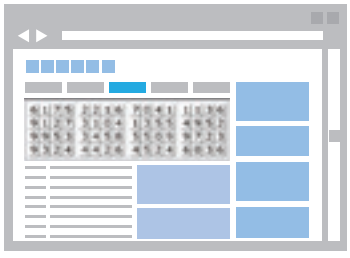
SECUREMATRIX 認証サーバ

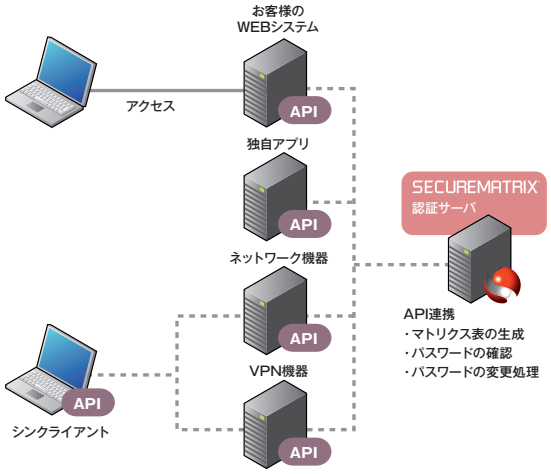
お客様のシステムやアプリケーション

## 既存システムやアプリケーションに「マトリクス認証®」を。

### 「マトリクス認証®」の可能性を思いのままに。

- CまたはJAVAに対応した「マトリクス認証®」用API
- 会員向けWEBサイトの認証や、既存システムの認証を強化
- API開発キットを提供
- セキュリティを考慮したシンプルなAPI



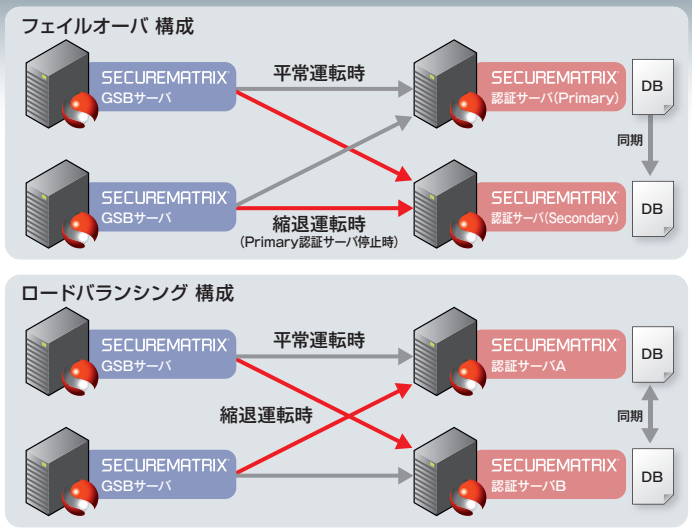


## SECUREMATRIX
# Easy Setup

SECUREMATRIX®は、GUIからインストールが可能です。「SECUREMATRIX® Easy Setup」を利用することで、各サーバの設定はもちろん、ドラック&ドロップによるSECUREMATRIX®サーバの追加/削除、サーバ証明書発行の為のCSR(Certificate Signing Request)の作成など様々な設定を、ネットワーク構成を確認しながら視覚的に実施することができます。

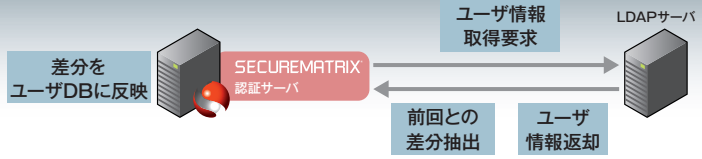
## SECUREMATRIX
# Cluster Manager

SECUREMATRIX®の認証サーバは、企業の大切な認証基盤を支えるために、独自クラスタ機能による冗長化構成で運用することができます。「SECUREMATRIX® Cluster Manager」を利用することで、認証サーバのクラスタ運用状況の確認やメンテナンスを実施することができます。




## SECUREMATRIX
# LDAP Interface

SECUREMATRIX®の認証サーバは、既存のLDAPサーバからユーザ情報を同期することが可能です。複数のLDAPサーバとの連携が可能で、ユーザ属性による特定ユーザ情報の抽出や、ユーザ情報項目のマッピング、スケジュール設定による定期同期など柔軟な連携を行い、ユーザ登録の管理負担を削減することができます。



# SECUREMATRIX®を安全にする様々な工夫と技術

## マトリクス認証®の安全性

### パスワードは使い捨て。二度使えない。

「マトリクス認証®」は、ランダムな数字列である「マトリクス表」とマトリクス表上の「位置と順番（=イメージパスワード）」を組み合わせることによりワンタイムパスワードを生成します。ワンタイムパスワードは、「使い捨てのパスワード」であるため、一度パスワードが盗まれたとしてもそのパスワードは二度と使えません。

### 「位置と順番」は、天文学的な組み合わせ。

マトリクス表には、ランダムの64個の数字が表示されます。デフォルトの最低パスワード長は8桁（設定により最長64桁）となっています。またイメージパスワードには、マトリクス表の同じ位置を複数回含むことができます。よって、8桁の場合でさえ、イメージパスワードの組み合わせ数は、約280兆通り（$64^8$）と天文学的な数字となり、イメージパスワードが一致する可能性は極めて低いと言えます。

### イメージパスワードと固定パスワードを併用すれば、更に強固に。

イメージパスワードには、固定パスワードを含むことができます。SECUREMATRIX®の「パスワードポリシー」機能を利用して、固定文字（英数字や記号）の併用を強制することが可能です。この固定文字は、パスワード内のどの位置に利用してもかまいません。

固定パスワード（英数字）と組み合わせて、
さらに強固なパスワードを設定できます。


第三者が不正になりすましを行おうとした場合に、下記の情報を全て知り得なければなりません。

- イメージパスワードとして登録したマトリクス表の「位置」
- その位置を入力する「順番」
- 「固定文字」として利用される英数字や記号
- パスワード内での固定文字の場所

固定文字かイメージパスワードかは、一見して第三者が理解することはできません。
なりすましを行うことは、極めて難しくなります。

## その他の安全性

### 通信経路にも万全なセキュリティ対策。

サーバから送信される「マトリクス表」や、クライアントから送信されるパスワードは、盗聴を防止するために、SECUREMATRIX®の特許技術を利用して保護しています。またあわせてSSL通信も行いますので、二重の対策が施されています。

### キーロガー対策も万全。

キー入力を監視してそれを記録し、利用者の入力情報を盗むキーロガーの対策の為SECUREMATRIX®は、「SECUREMATRIX® Key Protect」機能を用意しています。ドライバレベルでキーボード入力した文字を特定の文字に置き換えるので、たとえキーロガーがインストールされていても置き換えた後の文字しか盗まれません。

# パスワード運用の安全性

## 柔軟なパスワードポリシーで用途に応じたセキュリティレベルを。

SECUREMATRIX®は認証サーバの管理画面から、ユーザが利用するイメージパスワードに対して適用する右記のポリシーを設定することができます。このポリシーを適用することで、更にセキュリティレベルの高い運用を実施していただくことが可能です。

- パスワード文字長(イメージパスワードの桁数、固定文字の桁数)
- パスワード有効期限
- パスワードの強制変更
- パスワードの履歴回数制限
- 利用不可イメージパスワードの設定
- 認証失敗回数の制限 等

## 推測されやすいイメージパスワードは、すぐ禁止に。

推測されやすい簡単なイメージパスワードや、重複頻度が高くなる傾向のイメージパスワードは、デフォルトで利用禁止イメージとして予め登録されております。
また、SECUREMATRIX®には「パスワードアナライズ」機能が実装されており、社内のユーザが重複して利用している「イメージパスワード」をランキングで確認することが可能です。この「パスワードアナライズ」機能を利用して、重複頻度が高いイメージパスワードを「利用不可イメージ」として登録し、ユーザに強制的にパスワード変更を促すことができます。

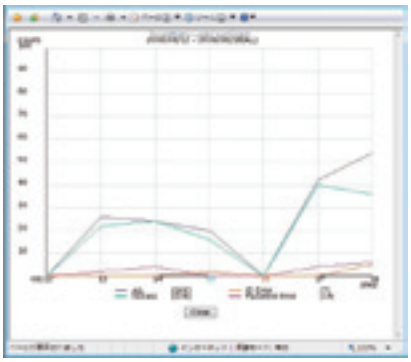
管理者は、推測されやすいイメージを
利用禁止に設定できます。

## パスワードアタックには、アカウントロックで対応。

SECUREMATRIX®は、パスワードアタック(ブルートフォースアタック)に対応するために「アタックロック(認証失敗回数制限)」機能を実装しています。一定回数の認証失敗が行われた場合には、SECUREMATRIX®はそのアカウントをロックし、管理者により解除されない限り、そのアカウントを利用することができなくなります。アカウントロックが行われたユーザには、SECUREMATRIX®がメールでその旨を通知します。これにより、第三者が自分のアカウントのパスワードを不正に取得しようとしていることが分かるようになっています。

## 利用状況を把握して、不正の兆候を判断。

認証の利用状況を把握することで、不正なアクセスの兆候を発見できます。SECUREMATRIX®の管理画面から、認証成功回数と失敗回数をグラフで確認することができます。失敗回数が増えている場合には、不正アクセスが行われている可能性が考えられます。この場合、管理画面の強制パスワード変更機能を利用し、次回のユーザ認証時にパスワード変更をユーザに促し、不正アクセスを未然に防ぐことが可能となります。



## ■ SECUREMATRIX® クライアント環境

| | | |
|---|---|---|
| ユーザクライアント | DESKTOP LOGON対応OS | Microsoft Windows XP Professional SP3、Microsoft Windows Vista Business SP1/SP2 |
| | 対応ブラウザ | Windows Internet Explorer 8、Mozilla Firefox 3.6、Safari 3.0/4.0(Apple Mac OS X v10.5/v10.6のみ) |
| 管理者クライアント | 対応ブラウザ | Windows Internet Explorer 7/8 |

※上記クライアント端末へは、あらかじめAdobe Flash Player、またはSUN JREがインストールされ、設定が有効になっている必要があります。
※ActiveX 使用時には、Internet Explorerのみ対応となります。
※PDA、携帯電話、スマートフォンの対応機種については、お問い合わせ下さい。

## ■ SECUREMATRIX® サーバ環境

| システム名 | SECUREMATRIX®<br>認証サーバ | SECUREMATRIX® GSBサーバ<br>(Global Security Module) | SECUREMATRIX® ISBサーバ<br>(Internal Security Module) |
|---|---|---|---|
| 対応OS | Red Hat Enterprise Linux(日本語版) | Red Hat Enterprise Linux(日本語版) | Red Hat Enterprise Linux(日本語版) |
| CPU | Pentium Ⅲ 1GHz 1Way以上 | Pentium Ⅲ 1GHz 1Way以上 | Pentium Ⅲ 1GHz 1Way以上 |
| メモリ | 1GB 以上 | 1GB 以上 | 1GB 以上 |
| ハードディスク | 35GB 以上 | 30GB 以上 | 30GB 以上 |

※対応OSの詳細は、別途お問い合わせ下さい。

# SECUREMATRIX® Authentication Provider Edition(APE)

キャリア様およびサービスプロバイダ様向けに、
SECUREMATRIX® の基本機能に加え、
企業管理や課金などの専用機能を実装した製品です。

## ■ 専用機能

| | |
|---|---|
| 課金機能 | 登録ユーザ数、認証有効稼動期日、課金情報の管理等 |
| 企業管理機能 | 企業名、企業登録人数、管理お知らせ強制表示、レルム機能等 |
| 各企業管理者向け機能 | ユーザ管理、お知らせ設定、監査(アクセスログ検索)等 |
| 各企業別パスワードポリシー設定機能 | デフォルトパスワード、有効期限等 |

システム管理者向け画面

各企業管理者向け画面

# SECUREMATRIX® アプライアンスサーバ

**一体型モデルで簡単かつ短期で導入。**

OSインストール済みの1ユニットサーバに、SECUREMATRIX® のインストーラを組み込んだ一体型モデルと、OSおよびハードウェアのオンサイトサポートをセットにした製品です。



開発元
**株式会社シー・エス・イー**
**Computer Systems Engineering**

〒150-0044 東京都渋谷区円山町23-2 アレトゥーサ渋谷ビル
TEL.03-3463-5633　FAX.03-3496-7477
E-mail:sales@cseltd.co.jp
**http://www.cseltd.co.jp/**

| ●販売パートナー | ●お問い合わせ先 |
|---|---|
| | |