HITACHI
Inspire the Next

# RSA SecurID ソリューションのご紹介

株式会社 日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

RSA SecurID ソリューションのご紹介

# Contents

HITACHI
Inspire the Next

# 1.パスワードの課題

# 1-1　固定パスワードの弱みと限界

HITACHI
Inspire the Next

- パスワードメモの盗難・紛失
- パスワード情報のシェア
- 推測される簡単なパスワード
- キーロガー等のツール
- 長期間同じパスワード
- フィッシングによる窃取
- トロイの木馬による窃取


など

# 1-2　パスワード運用　負のループ

HITACHI
Inspire the Next

ユーザへの定期的なパスワード変更案内

時間・労力・
経費の負担

パスワードを
紛失する
忘れる
シェアする

IT担当者やヘルプデスクへの
問い合わせ

ヘルプデスクコールの約20-50%が
パスワードリセットに関わるもの
(Gartner Group)

パスワードリセット1件にかかる
平均労働コストは・・

# 1-3 パスワード運用に関する課題

HITACHI
Inspire the Next

- 固定パスワードに関する脅威は継続
  - 複雑な文字列でも流出すれば脅威
  - 他サイトでの使い回しも企業の脅威に
  - 再利用されるパスワードは危険

- 一部だけのパスワード強化では安心できない
  - 低いセキュリティレベルがその企業のレベルに

- パスワードへのコスト負担は依然として高い
  - ヘルプデスクのコストなどトータルで考える

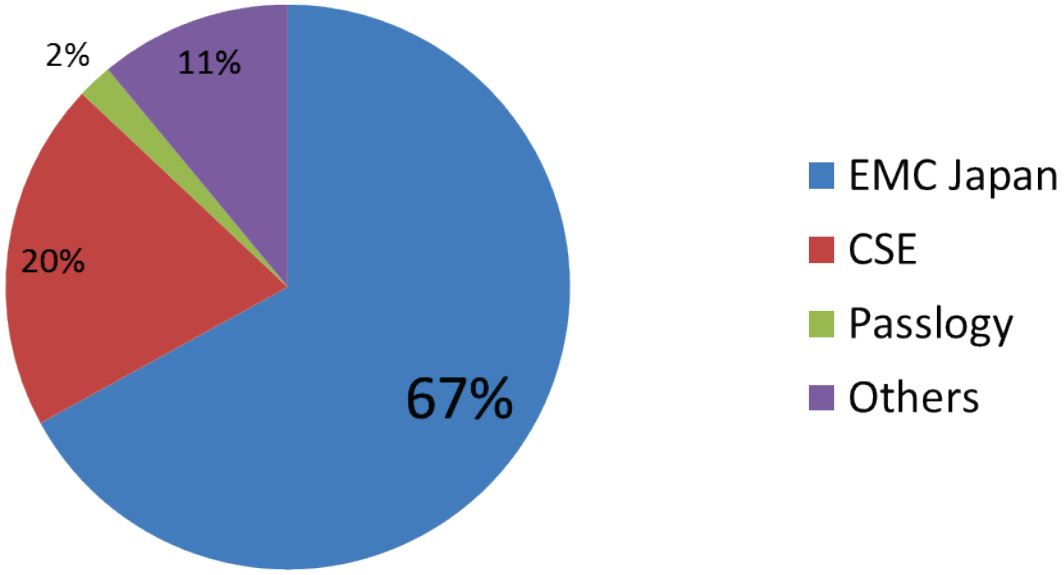
HITACHI
Inspire the Next

# 2.RSA SecurID認証のご紹介

# 2-1　RSA SecurIDの実績

HITACHI
Inspire the Next

- 全世界で**4,000万個、30,000社以上**の導入実績。
- 販売から**27年**に及ぶ実績により、今やビジネス・データを保護する認証の**デファクトスタンダード**。
- 日本でのマーケットシェア数量・金額ともに**約70%**を占める。




2011年実績 (金額)

2012年8月 富士キメラ総研調べ

# 2-2 RSA SecurIDのトークンラインアップ

HITACHI
Inspire the Next

## ハードウェアトークン

－トークンを持つことで社員のセキュリティに対する意識を向上させます。
　インストールが不要で登録したその日から使用が可能です。


キーホルダータイプ


カードタイプ


PINPADタイプ

## ソフトウェアトークン

－PCのデスクトップや携帯にパスワードを生成することができるので、トークンを持ちたくない
　ユーザ様に最適です。

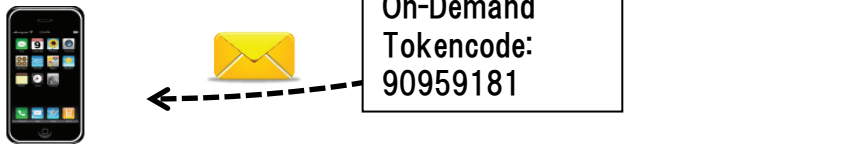
Android用


iPhone用


パソコン用

## On-Demandトークン

－お手持ちのパソコンや携帯端末にワンタイムパスワードをメールベースで受け取れるトークン
　有効期限がなくパンデミック時や災害時にも有効です。

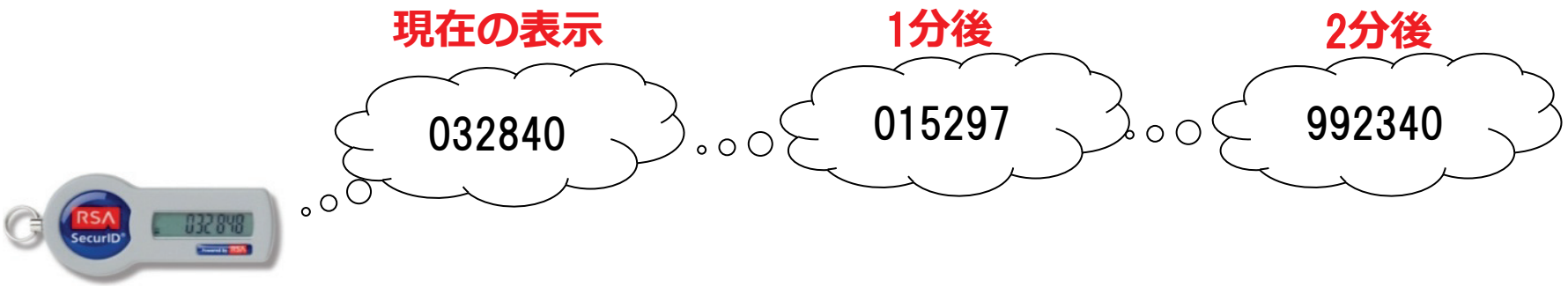


# 2-3 RSA SecurIDとは

HITACHI
Inspire the Next

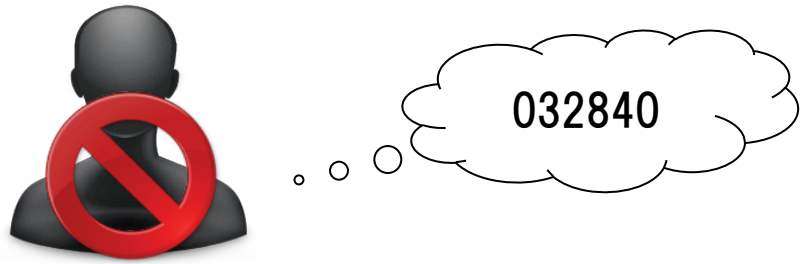
## ワンタイムパスワードの仕組み①

1分ごとに6桁のランダムなパスワードを発生（ワンタイムパスワード）




## ワンタイムパスワードの仕組み②

1度きり有効な使い捨てパスワードなので入力時に盗み見されても、安心！



# 2-4 RSA SecurIDの認証方式

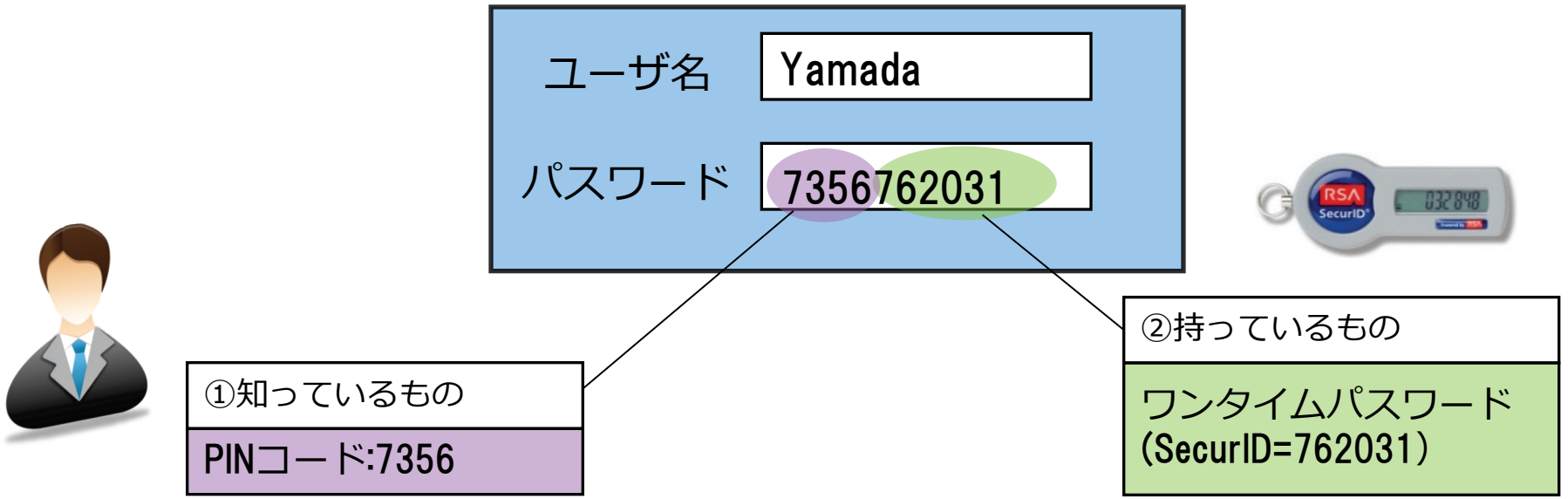
HITACHI
Inspire the Next

**二要素認証**で機密情報をしっかり守る

**①知っているもの： PIN、パスワード**

**②持っているもの： トークン**

## SecurIDの利用イメージ



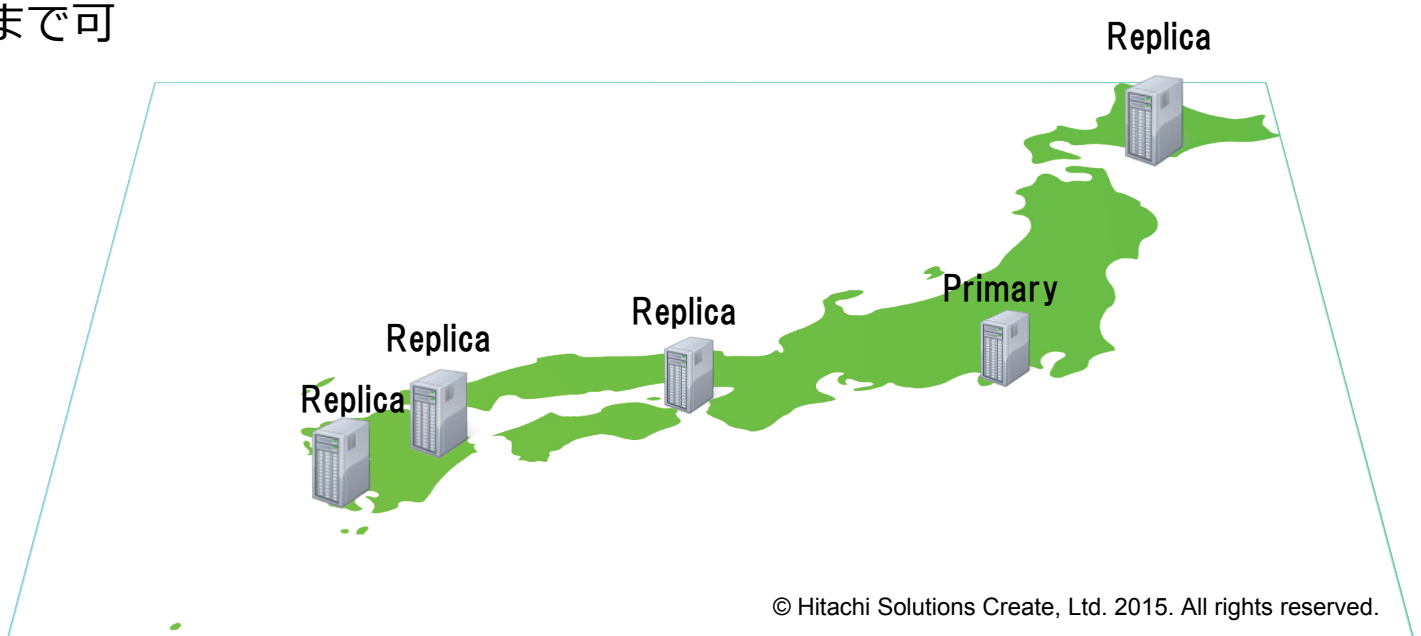
# 2-5 ライセンスについて

HITACHI
Inspire the Next

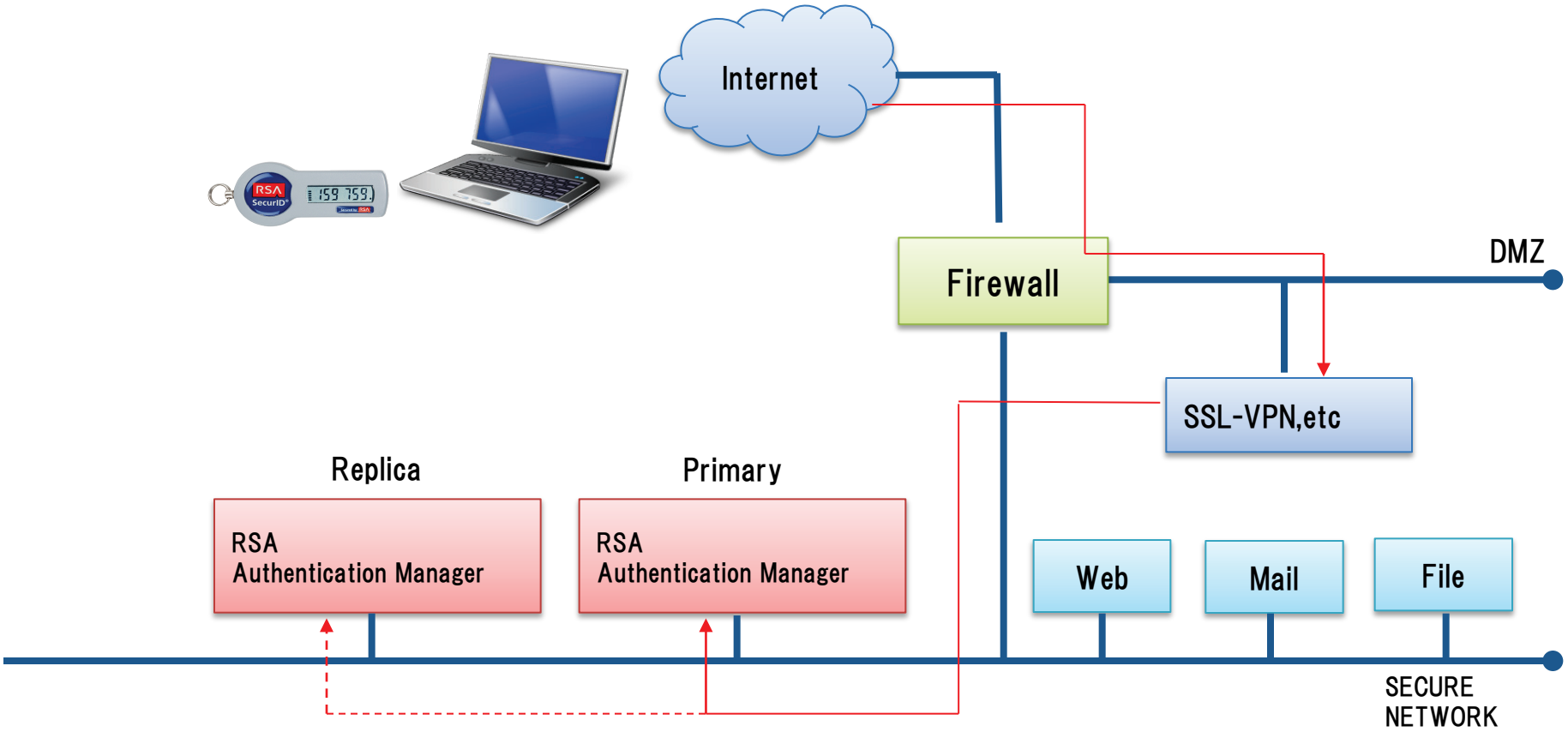
## ライセンスの種類

### 1. ベースエディション
プライマリ1台とレプリカ1台の構成

### 2. エンタープライズエディション
プライマリ1台とレプリカ1台以上の構成
1レルムあたりの最大構成はプライマリ1台とレプリカ15台の構成
最大6レルムまで可



# 2-6 RSA Authentication Managerの冗長構成



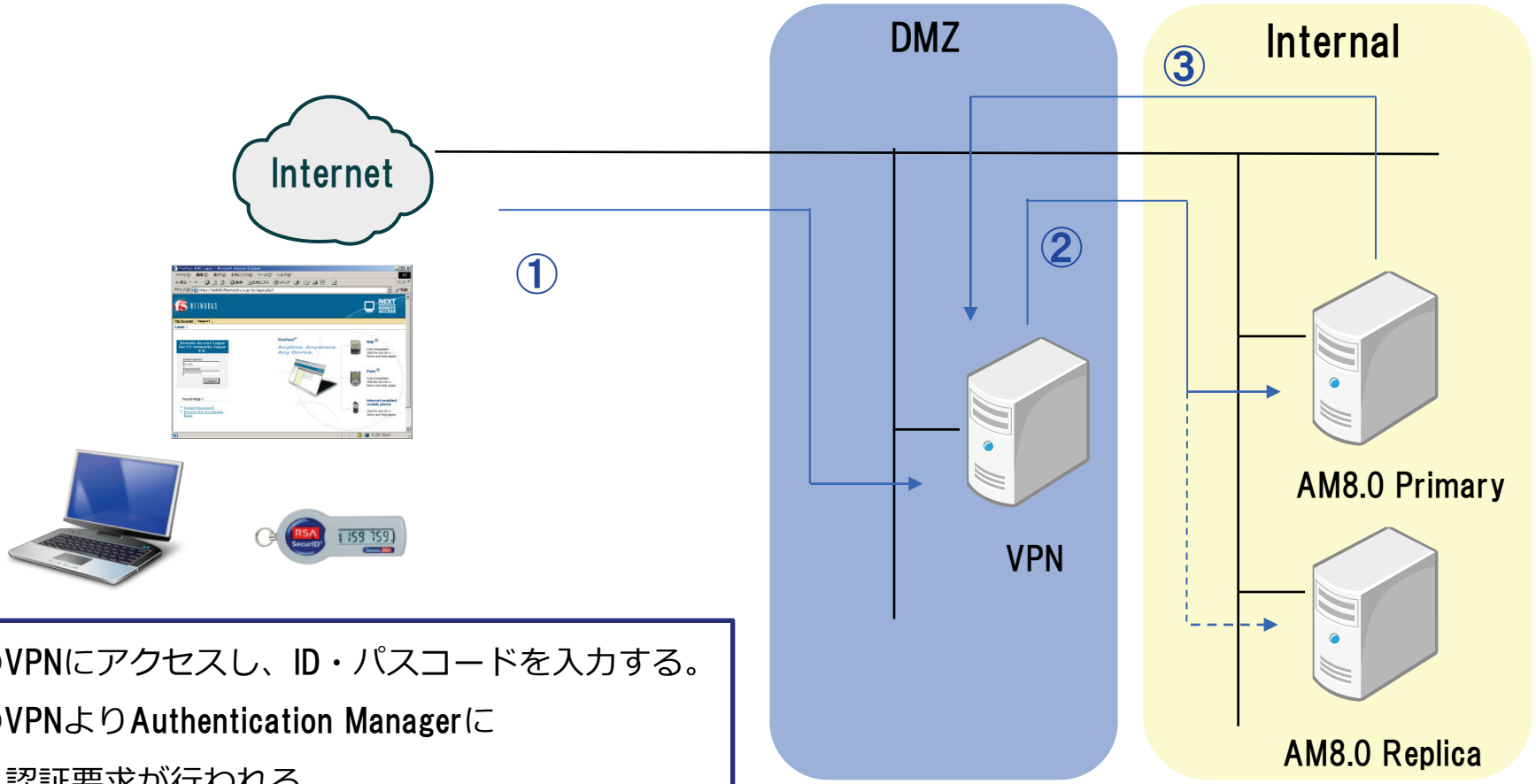

①**VPN、SSL-VPN等のリモートアクセス機器のその殆どには、既にRSA　Authentication　agentが実装されています。**

②Authentication Managerとリモートアクセス機器との連携は、リモートアクセス機器に実装されたagentと連携をおこないます。

③構成はアクティブ-アクティブの状態となります。Agentからの認証要求はPrimary、Replicaのいずれかに送信され、認証処理されます。
（優先順位を付けることも可能）

※設定情報,ユーザ情報の同期はPrimaryサーバへユーザの追加や削除など、管理操作が行われたタイミングでリアルタイムに同期されます。

# 2-7 VPN連携例




①VPNにアクセスし、ID・パスコードを入力する。
②VPNよりAuthentication Managerに
　認証要求が行われる。
③認証結果をVPNに返し、
　社内のリソースにアクセスが可能となる。

# 2-8 Citrix NetScaler/Access Gatewayとの連携例

HITACHI
Inspire the Next


Citrix Access Gateway ログイン画面




①NetScalerにアクセスし、ID・パスコードを入力する。

②NetScalerよりAuthentication Managerに
　認証要求が行われる。

③認証結果をNet Scalerに返し、
　仮想デスクトップにアクセスが可能となる。

# 2-9 VMware View Security Serverとの連携例

HITACHI
Inspire the Next


VMware View ログイン画面




①View Security Serverにアクセスし、
ID・パスコードを入力。

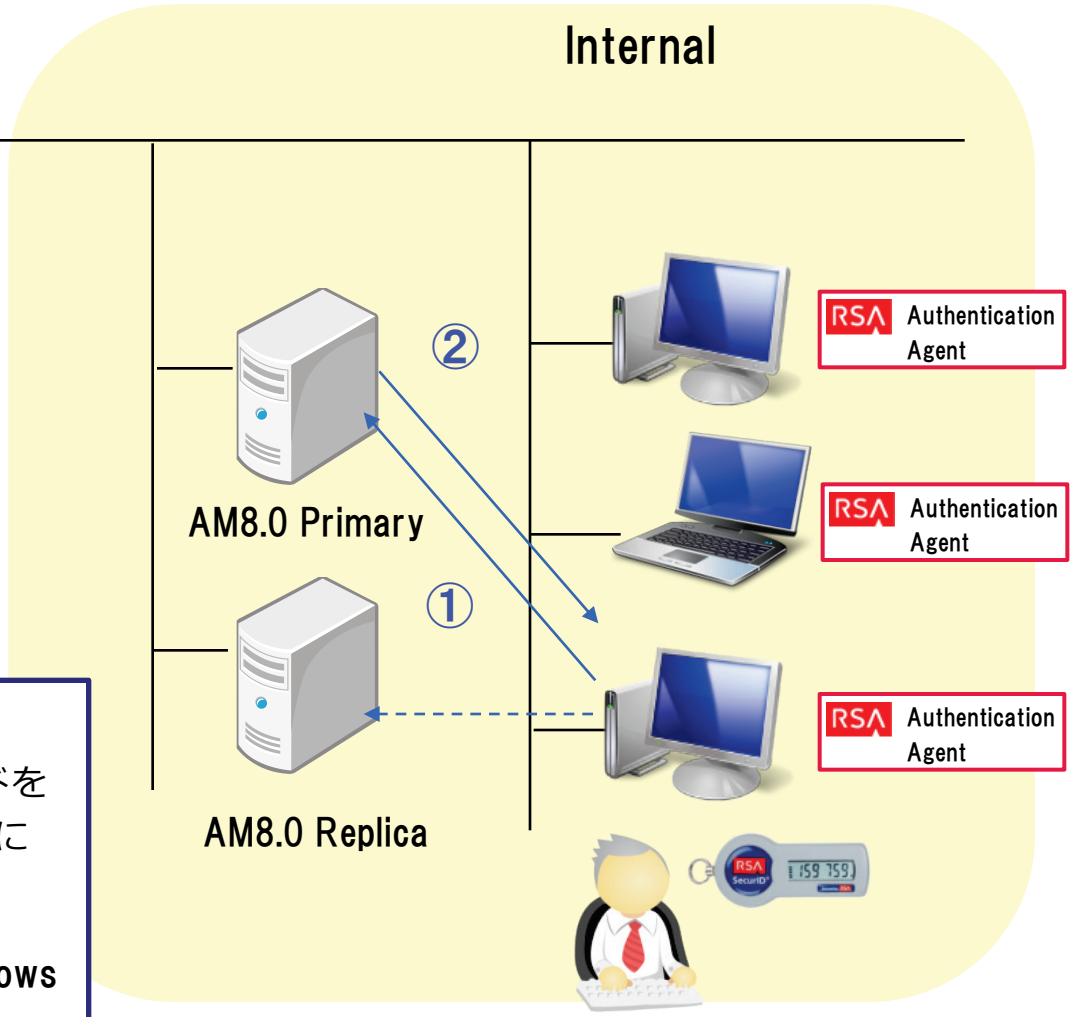
② View Connection Serverより
Authentication Managerに認証要求が行われる。

③認証結果をView Connection Server に返し、
仮想デスクトップにアクセスが可能となる。

# 2-10 ローカル認証例（Windowsログオン認証）

HITACHI
Inspire the Next


Windowsログイン認証をSecurID認証に




①Agentがインストールされた端末にて
Windowsを起動。認証画面にてIDとパスコードを
入力することにより、Authentication Managerに
認証要求が行われる。

②認証の結果を返し、認証成功であれば、Windows
ログオンが完了。

HITACHI
Inspire the Next

# 3.ソリューションメニューのご紹介

# 3-1　要件整理から構築・運用までトータルサポート

HITACHI
Inspire the Next

| フェーズ | サービス名 | サービス内容 |
|---|---|---|
| コンサルティング | 要件整理支援サービス | RSA SecurIDの適用に関する現行環境構成の確認、および要件定義書の作成など、要件整理を行います。 |
| 基本設計 | 設計支援サービス | お客さまのご要件に沿った基本設計、運用設計を行います。 |
| インテグレーション | 導入支援サービス | 設計支援サービスに基づいた詳細設計、環境設定、テストを実施します。 |
| | インテグレーションサービス | インストール，弊社規定の設定シートに従った簡易設定、製品の動作確認までを行います。 |
| | ユーザ登録サービス | RSA SecurID認証ユーザ登録の支援を行います。 |
| マネージメント | 操作教育サービス | RSA SecurIDの運用を中心とした操作教育の支援を行います。 |
| | サポートサービス | 問題点の解決支援、改良版の提供、および製品情報の提供を行います。 |

HITACHI
Inspire the Next

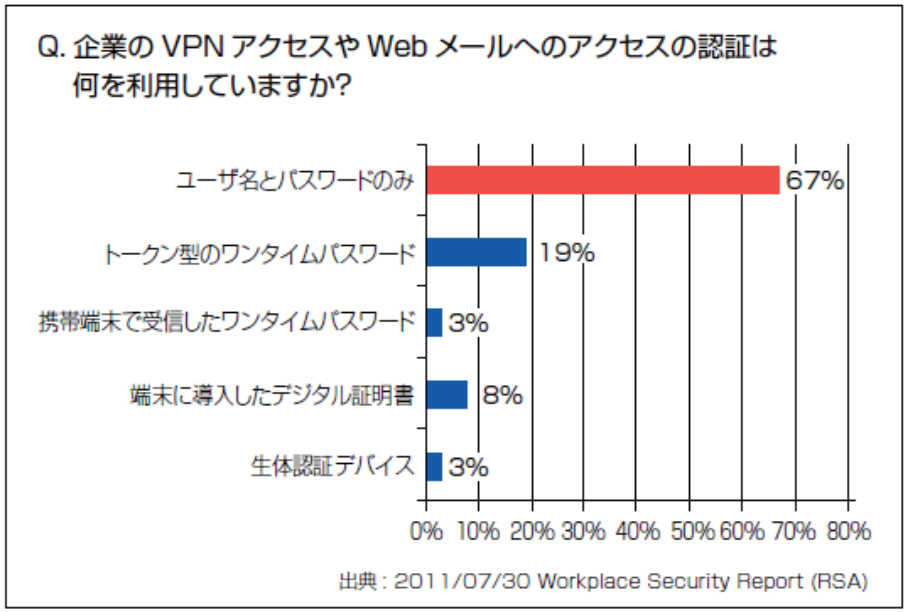
# 4.リスクベース認証のご紹介

# 4-1 アクセス時に行われているユーザ認証の割合

HITACHI
Inspire the Next

依然として固定パスワードでの認証が、
およそ3分の2を占めている

パスワードの強化が必要なのは
認識しているが・・・



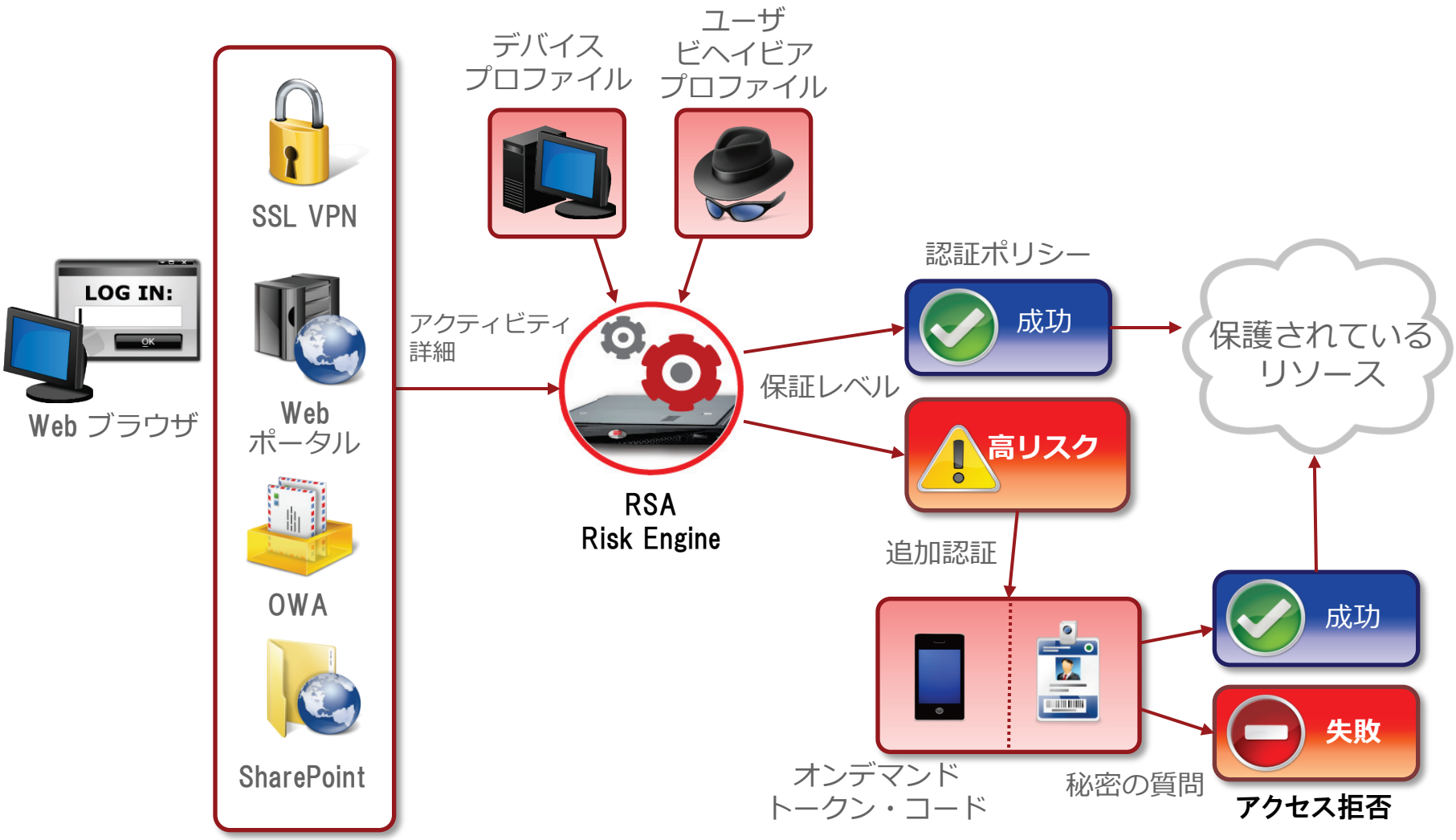

― 複雑な認証を採用して、エンドユーザから不満が出るのを避けたい
― ソリューション投資を抑えたい
― 人的リソースの不足で新しいことに手が回らない

# 4-2 リスクベース認証とは

HITACHI
Inspire the Next

- ユーザの利便性を保った**多要素認証方式**
- ユーザデバイスの持つ情報や行動を評価
- 評価には洗練された**リスクエンジン**を採用
- 追加認証に**秘密の質問**と**オンデマンドトークン認証**を装備
  （通常ライセンスへのオプション提供）
- 市場でも実績のある認証方式

# 4-3 リスクベース認証のフロー



# 4-4 RSA Risk Engineとリスクの判断要素

HITACHI
Inspire the Next

## RSA Risk Engine

・認証が行われる毎に情報を収集する自己学習能力
　・ユーザ特性に基づいてリスクスコアを算定
　→追加認証の要否を判断


1.記憶情報


2.所有デバイス情報


3.行動履歴

| | 内容 | 具体例 |
|---|---|---|
| 要素1 | ユーザが知っている情報 | ID,パスワードなど |
| 要素2 | ユーザが所有しているもの | デバイスプロファイル<br>(クッキー情報、ブラウザ情報など) |
| 要素3 | ユーザの行動 | 認証可否の情報、アカウント更新情報、特異な行動（不明IPからアカウント情報を更新した直後アクセス）など |

# 4-5 追加認証(秘密の質問)

HITACHI
Inspire the Next

- 本人だけが知っている情報を用いた認証
- 回答はユーザが直接入力
- 質問内容や質問の数はポリシーにより、カスタマイズが可能

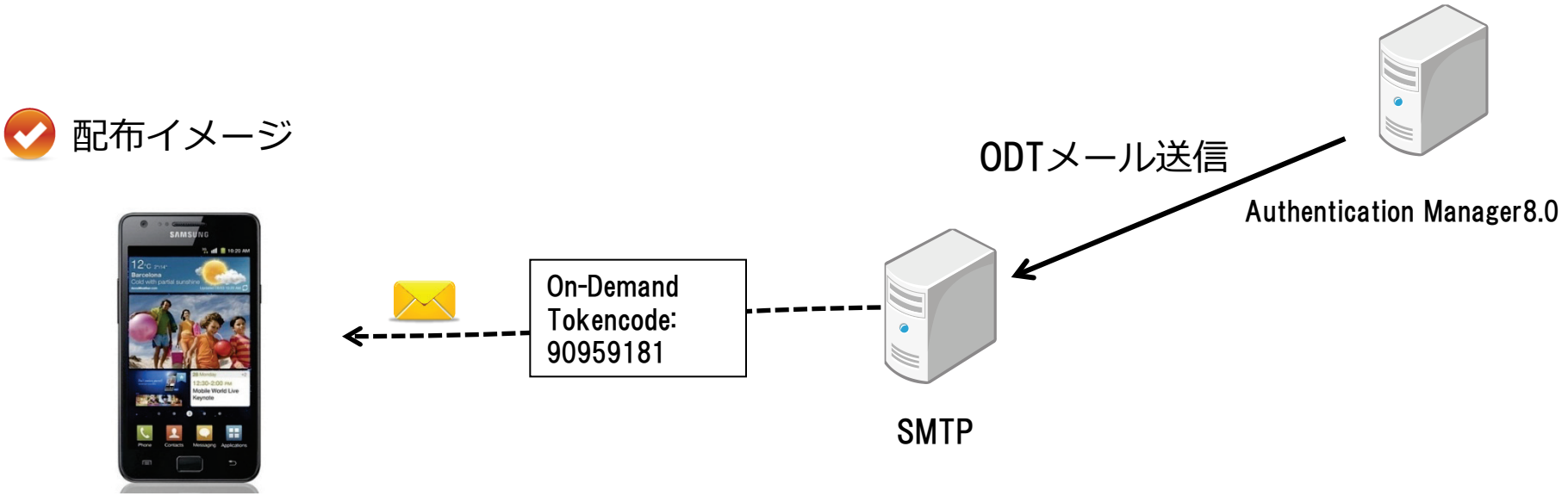
質問例
・ペットの名前は？
・お父さんの出身地は？
・お母さんの旧姓は？
・あなたの好きな食べにものは？
・初恋の人のファーストネームは？
・あなたの誕生日は？
・好きな映画は？

# 4-6 追加認証(On-Demand Token)

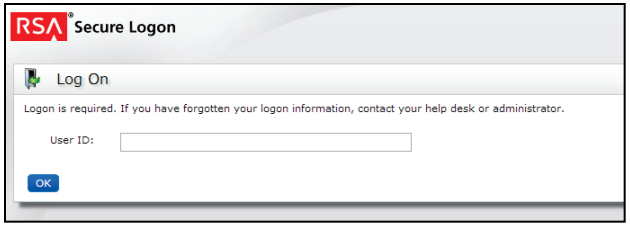
HITACHI
Inspire the Next

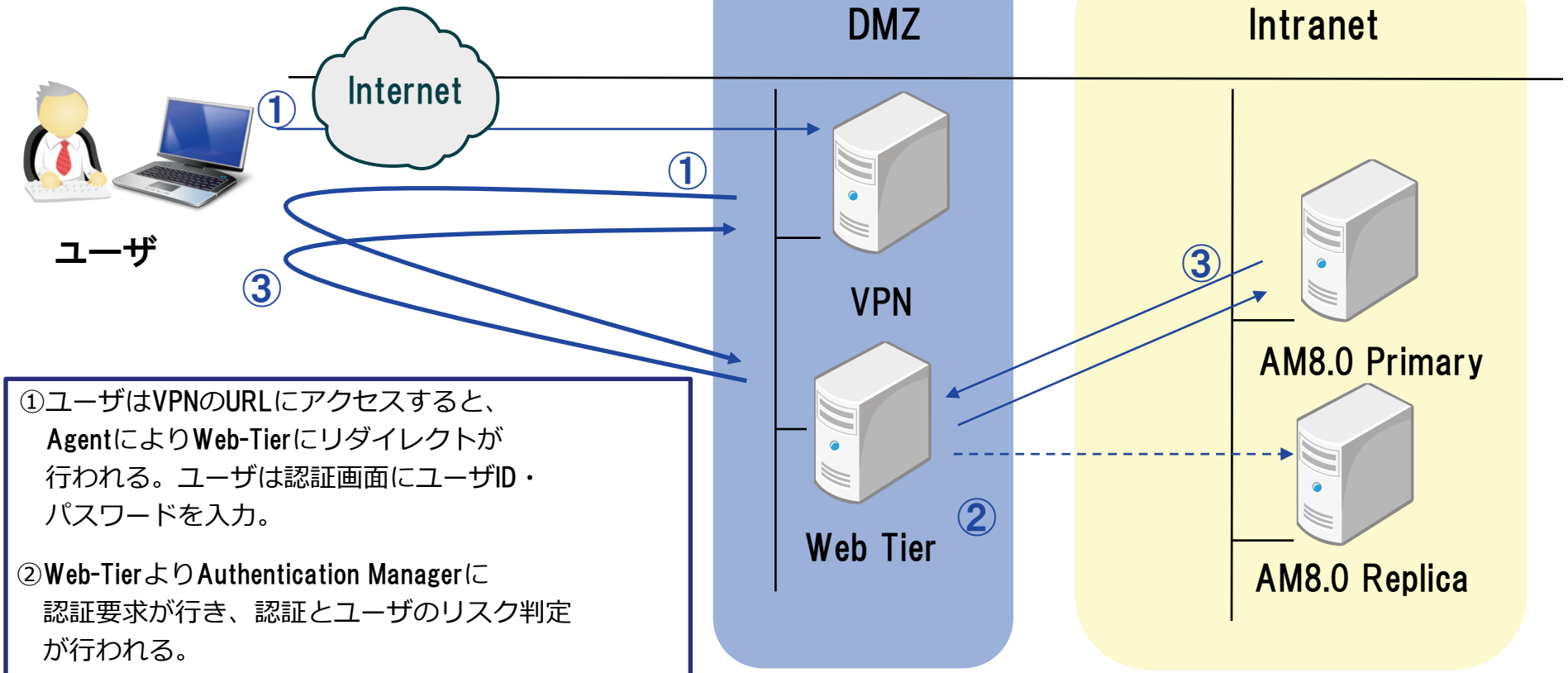
- ワンタイム・パスワードをメールで受け取るトークン
  スマートフォンや PC 等で受信可能
  端末へのアプリケーションのインストールは不要
- パスワードは8ケタでデフォルト60分有効

配布イメージ



# 4-7 リスクベース認証 構成例




①ユーザはVPNのURLにアクセスすると、
AgentによりWeb-Tierにリダイレクトが
行われる。ユーザは認証画面にユーザID・
パスワードを入力。

②Web-TierよりAuthentication Managerに
認証要求が行き、認証とユーザのリスク判定
が行われる。

③リスク判定に問題がなければ、認証結果が
ユーザに返され、認証成功。

# 4-8 RSA Authentication Manager サポート期間

HITACHI
Inspire the Next

| Products | Version | EOS Date | 1st Y Ext | 2nd Y Ext |
|---|---|---|---|---|
| Auth Manager 8.0 | | 2016年5月 | 2017年5月 | 2018年5月 |
| Auth Manager 7.1 | SP4 | 2014年3月 | 2015年3月 | 2016年3月 |
| Auth Manager 7.1*1 | SP2/SP3 | 2013年3月 | 2014年3月 | 2015年3月 |
| Auth Manager 6.1*2 | 6.1.4 | 2013年12月 | - | 2015年12月 |
| Auth Manager 6.1*3 | 6.1.4 | - | - | 2015年12月 |

※1 パッチリリースはSP4に対して実施します。SP4へのアップグレードをお願い致します。
※2 該当するプラットフォームは次の通りです。Windows 2003, RedHat 4/5, Solaris 9/10, AIX 5.3, HP-UX11i
※3 該当するプラットフォームは次の通りです。Windows 2000, SUSE 9, RedHat 3, AIX 5.2

First Year Extended Supportとは・・・
EOSから1年間、有償にてサポートを継続するサービスです。
このサービスはお客様のビジネスに致命的な影響をおよぼすケースに対して、
必要があればホットフィックスの提供を行います。
それ以外のケースにつきましては、ベストエフォートの対応となります。

Second Year Extended Supportとは・・・
有償にてサポート継続するサービスです。
このサービスは、お客様のビジネスに致命的な影響をおよぼすケースに対して、ワークアラウンド（回避策）の提供と製品に関するご質問をお受けいたします。但し、ホットフィックスの提供はございません。

# お問い合わせ

HITACHI
Inspire the Next

## 株式会社 日立ソリューションズ・クリエイト

### 電話でのお問い合わせ

**0120-954-536**

受付時間 9:00～17:00 月曜日～金曜日（祝日、弊社休業日を除く）

### メールでのお問い合わせ

**hsc-contact@mlc.hitachi-solutions.com**