GUARDIAN シリーズ

ACCESSGUARDIAN

アクセスガーディアン

■インターネット通信経路暗号化

■ユーザー認証機能

■アクセスコントロール機能

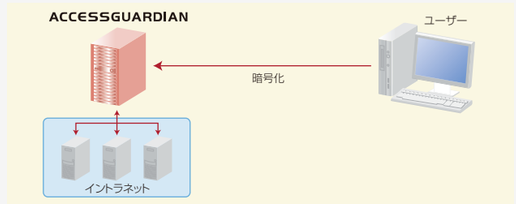
ACCESSGUARDIANは
理想のグループネット環境を構築します。

ACCESSGUARDIANは、イントラネット上のWeb情報を簡単かつ安全に、インターネットの特定ユーザーへ提供するシステムです。インターネットに接続可能なモバイルユーザー、顧客、グループ企業がイントラネット上にあるWeb情報へアクセスすることが可能となり、グループネットを構築できます。
インターネットへの接続口にファイアウォールを設置している企業ネットワーク環境では、Webによる情報公開に関して内部と外部という制約をもちます。Webサーバーは、内部利用者向けのものは社内LANに設置され、インターネット利用者向けのものは非武装地帯（DMZ）に設置するのが一般的な方法です。ACCESSGUARDIANはこのような物理的な設置制約を解消するとともに、インターネットからのアクセスを一元管理でき、また安全性が確保されてないインターネットの通信は暗号化することで仮想専用ネットワーク（VPN）を実現します。
また、クライアント証明書によるユーザー認証により、なりすまし防止とユーザーごとにアクセス可能な情報をコントロールできます。

ACCESSGUARDIANの特長

■インターネット通信路暗号化

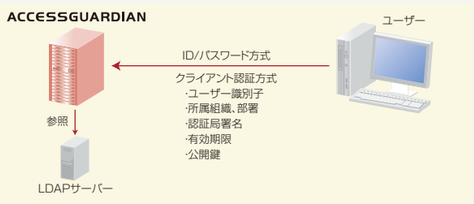
- インターネット上の通信は暗号化され、第三者による通信データの盗聴、改ざんを防ぎます。
- ユーザーはブラウザーがあれば安全にWeb情報にアクセス可能です。



■ユーザー認証機能

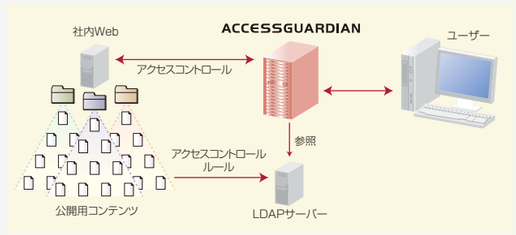
- クライアント認証方式*とID･パスワード方式の2つの方式による認証で不正なユーザーのなりすましを防ぎます。

＊X.509公開鍵証明書を利用



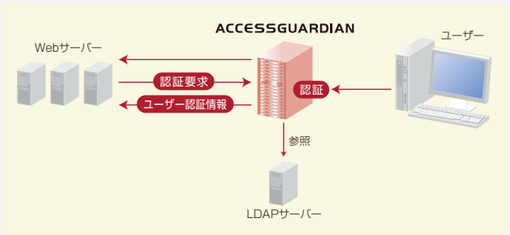
■アクセスコントロール機能

- HTTPプロトコルレベルのファイル･ディレクトリー単位での詳細なアクセスコントロールが可能です。



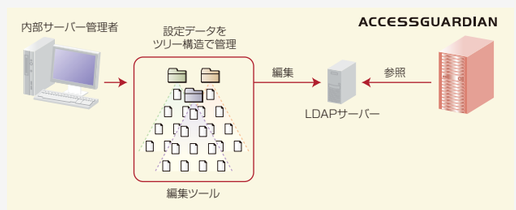
■代理認証/シングルサインオン環境

- ユーザーは一度の認証で複数のWebサーバーにアクセスできます。



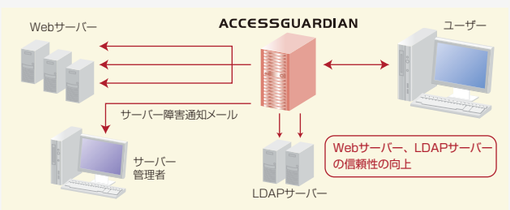
■LDAPサーバーによる一元管理

- LDAPサーバーと連携してユーザー、Webサーバー、アクセスコントロール情報を容易に一元管理することが可能です。

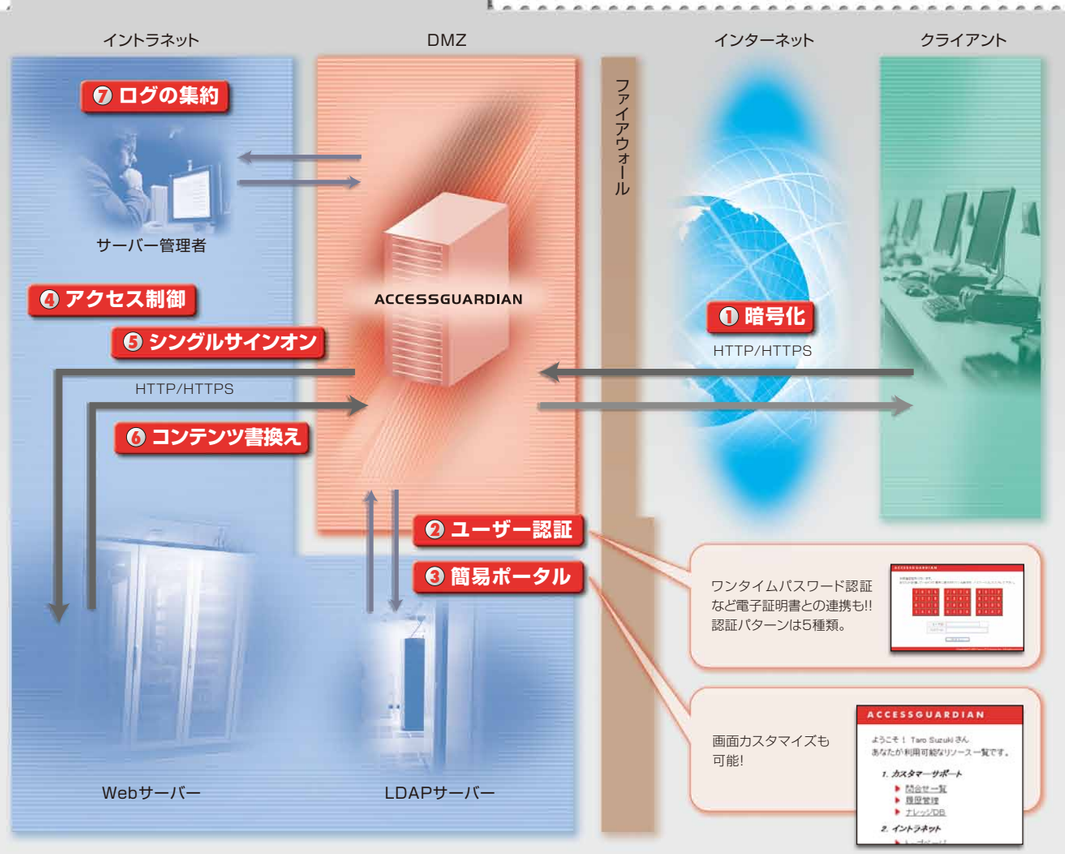


■信頼性の向上

- ACCESSGUARDIANはWebサーバー、LDAPサーバーの冗長化に対応します。また、負荷分散装置を用いたACCESSGUARDIAN自身の冗長化にも対応可能です。



ACCESSGUARDIANの基本機能

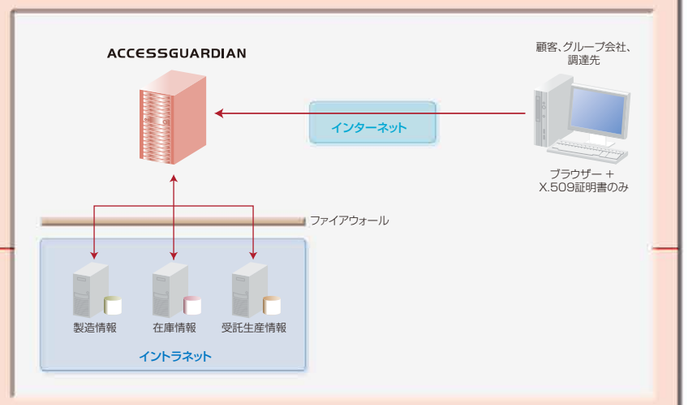


ACCESSGUARDIAN導入の利点

- リバースプロキシ型なので導入が容易。
- シングルサインオン機能によりユーザー管理コストを軽減。
- アクセス制御ポリシーやログをサーバー単体ではなくサイト全体として統合管理。
- Webサーバーを安全なイントラネットに設置可能。
- 暗号化通信や多様な認証パターンで、グループネットの高度なセキュリティを確保。

ACCESSGUARDIANの事例

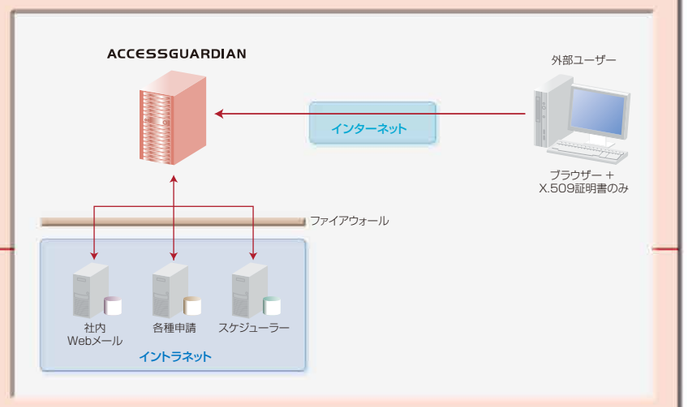
1. 社内の製品情報・在庫情報などを特定顧客に提供



採用の理由

顧客の負荷を極小化した上で、情報共有によるサービスの向上を図る。

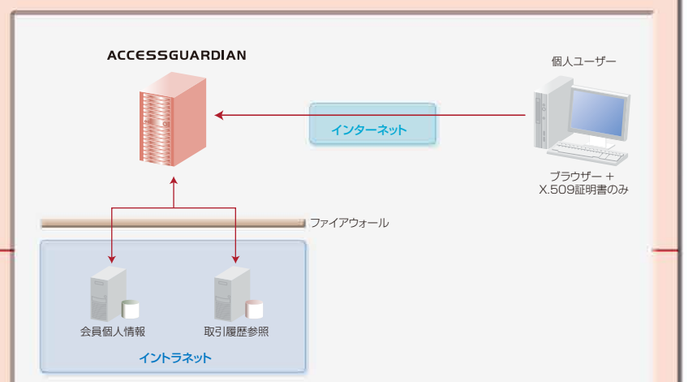
2. 外部勤務者やモバイルユーザーが社内システムを利用



採用の理由

特別なクライアントソフトが不要で通信環境への要求が少ない

3. 個人に応じた情報を公開



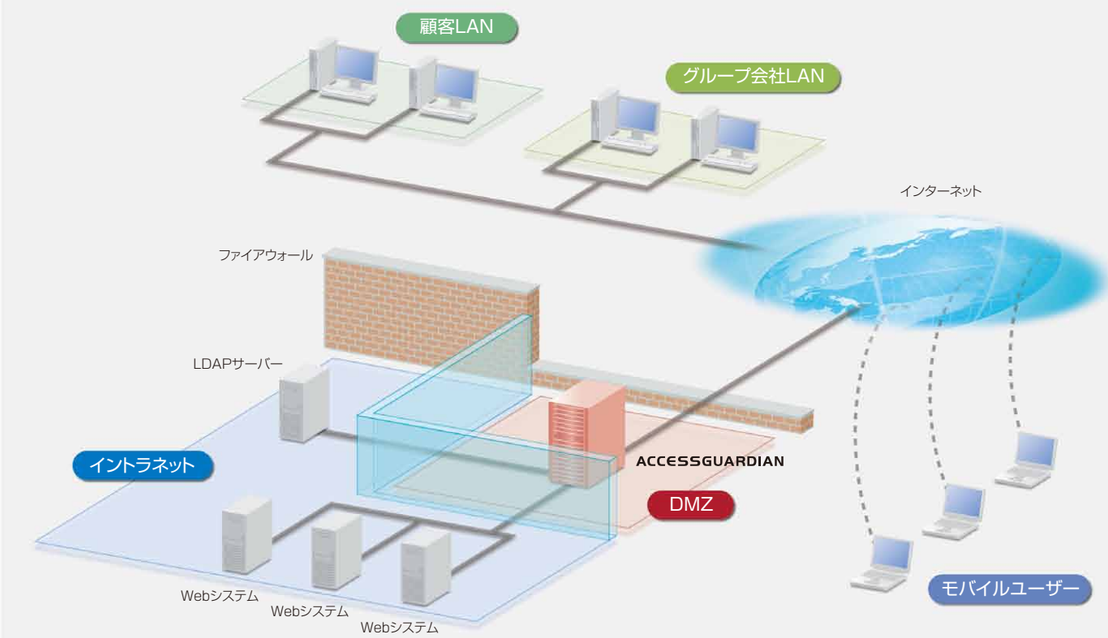
採用の理由

個人情報を集約することでシステムリソースを有効活用しながらも安全に情報を公開

その他の利用事例

- ●ホストエミュレーターのゲートウェイ（HTTP、HTTPSのみ対応）
- ●イントラネット内部でのアクセス制御とシングルサインオン

ACCESSGUARDIANの設置例



ACCESSGUARDIAN公開・利用の手順

情報公開手順

■Web情報提供者

- 公開Webサーバー情報をLDAPサーバーへ登録
- ユーザーのID･パスワード、クライアント証明書の作成
- ユーザー情報をLDAPサーバーへ登録
- ACCESSGUARDIANで公開するWebサーバーのURLをDNSへ登録

■ユーザー

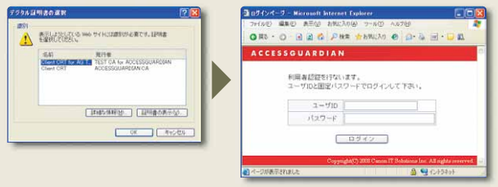
- ID･パスワード、クライアント証明書の入手
- クライアント証明書をブラウザーへインポート

（注）ブラウザーの設定でcookieを有効にする必要があります。

ユーザーの利用手順

❶ ブラウザーからACCESSGUARDIANへアクセス

❷ ログイン認証（クライアント証明書 ＋ ID･パスワード）



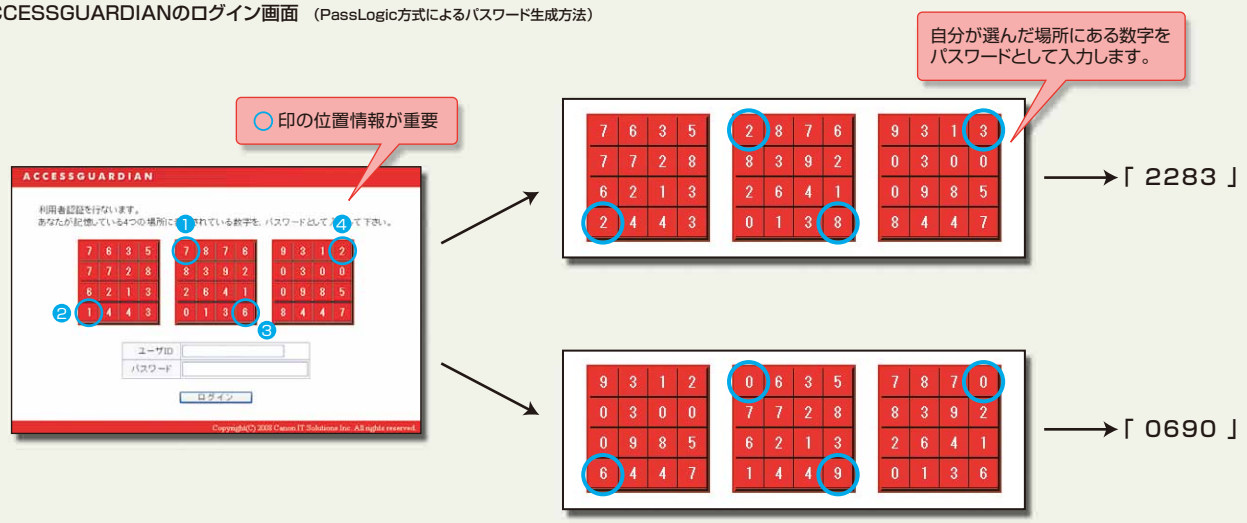
❸ ユーザーのアクセス可能なサーバーリストが表示

❹ リストからサーバーを選びアクセス

❺ ブラウザー終了でログアウト

ACCESSGUARDIANワンタイムパスワードオプション

●ACCESSGUARDIANのログイン画面 （PassLogic方式によるパスワード生成方法）



●乱数表から「任意の位置」を設定し、それがパスワードとなります。
●乱数表の数字は、ログイン画面を呼び出すたびに変化するので、パスワードとして使用する数字は毎回変化します。

◎余計な認証用デバイスなどを持ち歩く必要がありません。
◎ブラウザーさえあれば認証を受けられます。（閲覧する場所・OSを選びません）
◎簡単かつ安価で運用できます。

ACCESSGUARDIAN運用管理オプション

ACCESSGUARDIANの運用管理オプションには、下記の機能があり、運用管理コストを大幅に削減します。

運用管理項目	標　準	運用管理オプション
ユーザー情報保守	1）簡易登録 1件ずつ登録、更新 誤りはチェックせず、そのままサーバーに登録。	1）使い易いユーザーインターフェイス Excelをユーザーインターフェイスとした使い易いツール。 2）入力データの一貫性チェック LDAPサーバー登録、更新時に全てのデータの書式、一貫性を一括チェック。 3）一括登録、読出し、更新 LDAPサーバーへの一括登録、更新、LDAPサーバーからの読出しが可能。
稼動監視	1）稼動状況監視画面 LDAP、Webサーバーの稼動状況を管理者画面（Web）から確認可能。	1）障害時のメール通知 ACCESSGUARDIAN本体、LDAPサーバーの稼動状況を監視し、障害時にメール通知。 監視システムの無い環境でも簡単に監視が可能となる。 2）ACCESSGUARDIANサービスの非稼動時の自動復旧 3）ACCESSGUARDIANサーバーのディスク容量監視 4）不正ログイン監視（連続ログイン失敗を監視）

（注）アクセスログ解析は市販の専用ツールをご利用ください。

■動作環境

ACCESSGUARDIAN	対応ブラウザー
OS：Solaris 8 / 9 / 10（SPARC版） メモリ：512MB以上 LDAPサーバー（必須） CAサーバーまたは認証サービス*	1. SSLによる暗号化 Netscape Navigator 3.0 以降 Microsoft Internet Explorer 3.0 以降 2. X.509公開鍵証明書による認証 Netscape Navigator 3.0.3 以降 Netscape Communicator 4.0.5 以降 Microsoft Internet Explorer 4.0 以降
*ユーザー認証で X.509公開鍵証明書を利用する場合のみ必要	（注）ベリサイン社などの認証サービスから証明書を取得される場合には、有効期限の制約により上記バージョンでは対応できない場合があります。

販売元/
Canon
キヤノン ITソリューションズ株式会社
セキュリティソリューション事業部
http://canon-its.jp/
〒140-8526 東京都品川区東品川2-4-11
TEL：03-6701-3434 FAX：03-6701-3471

AG1112IDE-PDF