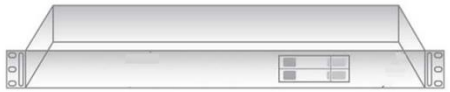

遅いVPNはリバースプロキシで代替
ゼロトラストをリバースプロキシで
運用する方法も紹介
2021-03-02 (火) 14:00 - 15:00

株式会社　ムービット

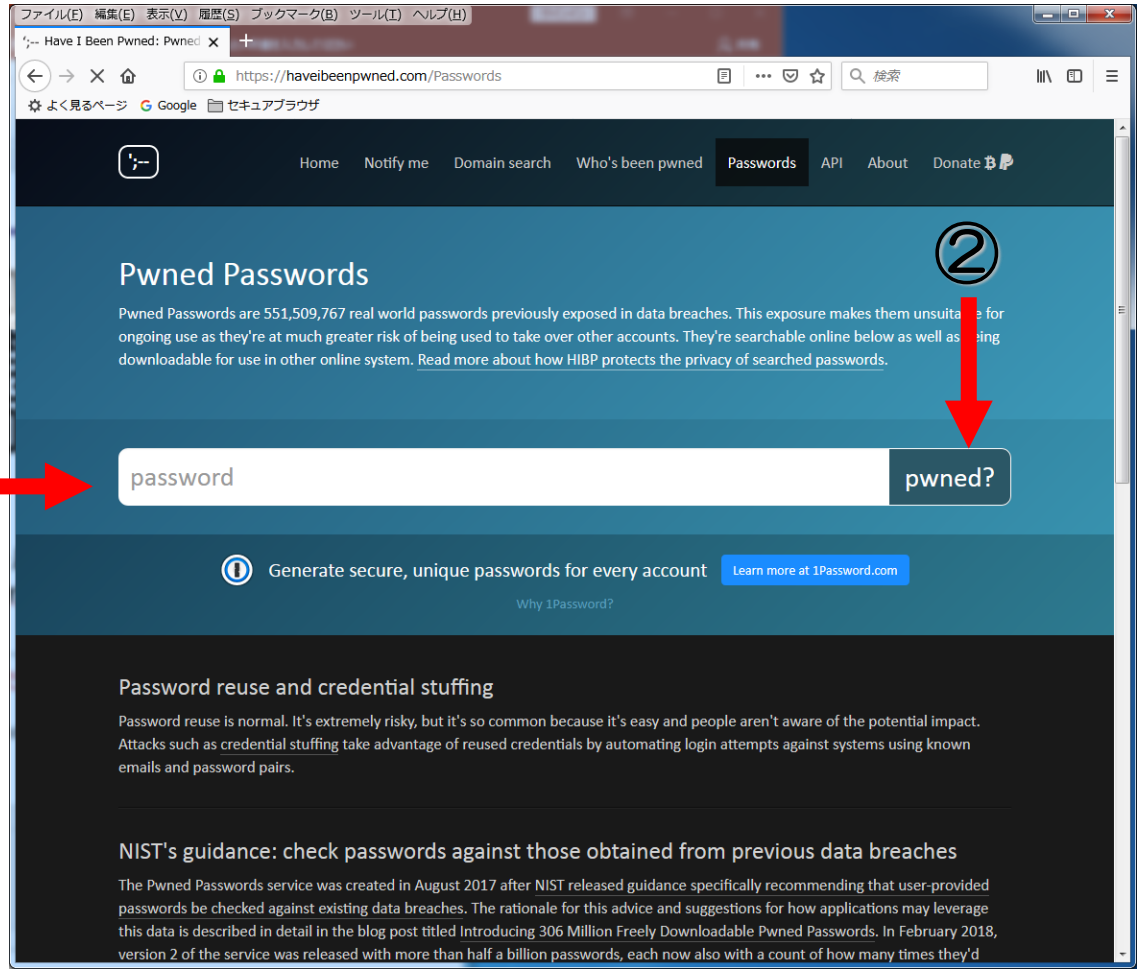
会社概要

社名	株式会社ムービット
設立	1995年12月8日
所在地	東京都北区王子1－28－6
主な製品	Powered BLUE シリーズ アプライアンスサーバー（Linux） ソフトウエア開発



パスワード流出チェックサイト

https://haveibeenpwned.com/



① パスワードを入力
② pwned？　を押す

Oh no --- pwned !
残念でした

Good news — no pwnage found!
大丈夫

社内LAN側 への アクセス手法

項目	ターゲット	主な特徴
●VPN	network	VPNソフトが必要
●リバースプロキシ	Web	既存のWebへのアクセスに利用 複数の認証が適用できる
●ゼロトラスト	Web アプリ	idPとID認識型プロキシ型が必要

VPNの負荷　増大

Before コロナ　→　With　コロナ

VPN

VPN

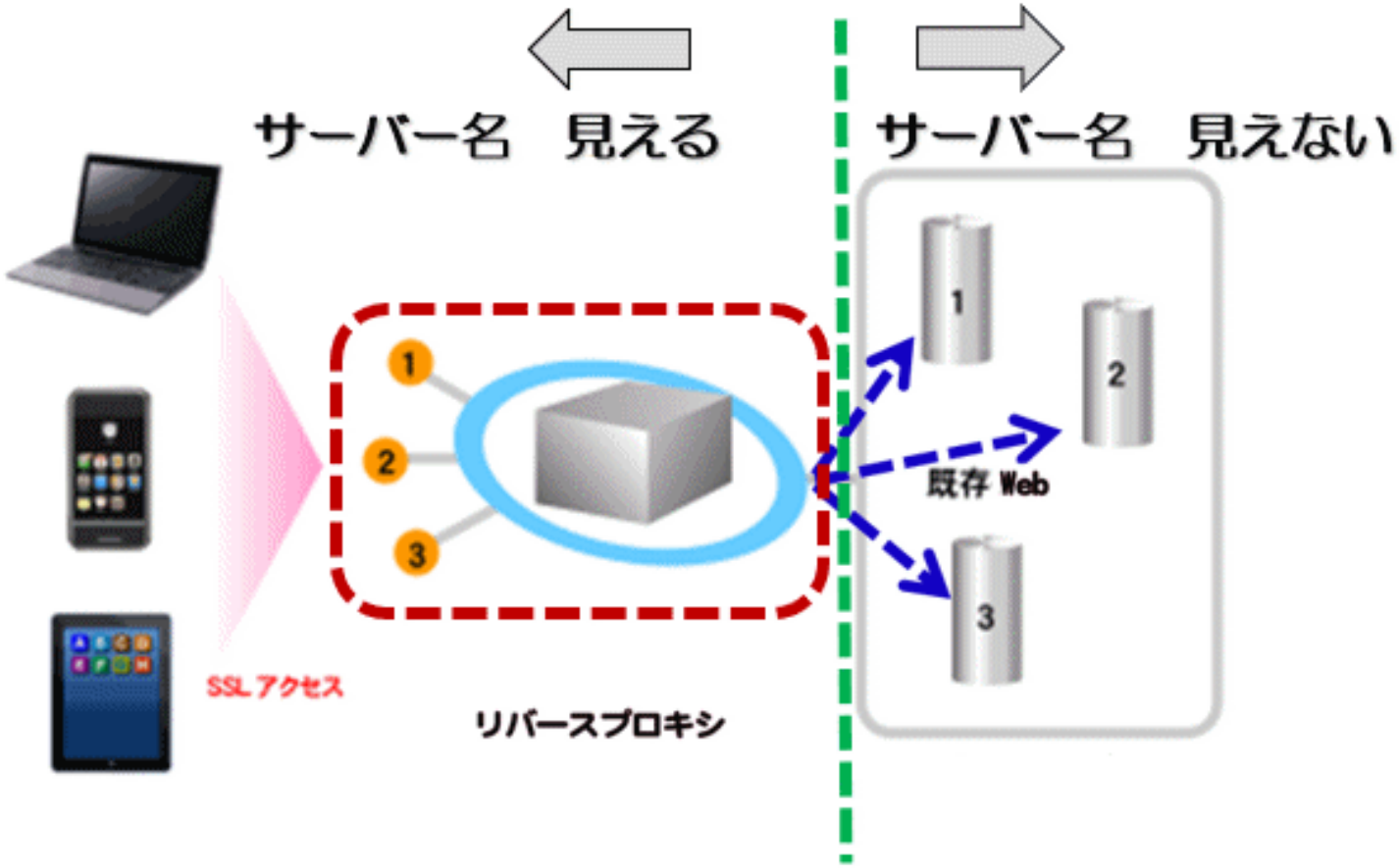
遅い

つながらない

VPNの特徴

- ソフト
  クライアントソフトが必要
- アクセス
  ネットワークへのアクセス
- 使い勝手
  ネットワーク内にすべてアクセス可能
- セキュリティ
  ログイン後のセキュリティは無し

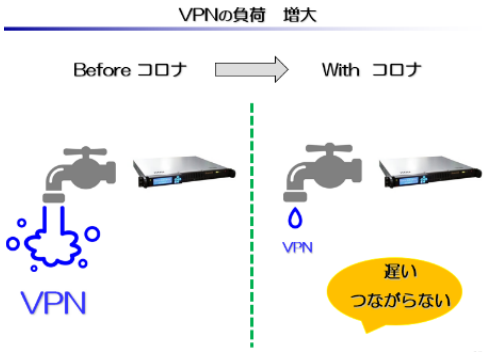
リバースプロキシ　　リダイレクト先Web の 隠蔽



リバースプロキシ先を隠蔽

VPNとリバースプロキシの比較

項目	VPN	リバースプロキシ
アクセス	Network内全体	ターゲットサーバー
ソフト	専用クライアント	ブラウザ
ターゲットサーバー	任意	Web
負荷	高い	低い
同時アクセス	閾値が低い	閾値が高い



ゼロトラスト　② ID認識型プロキシ は 2タイプ

透過プロキシ型

リバースプロキシ型

ゼロトラスト　ID認識型プロキシ＝透過プロキシ型 での 構成

透過プロキシ型

WAN側
① idP
② ID認識型プロキシ

idPは指定が多い
透過プロキシ

ターゲットネットワーク
③ プロキシコネクタが必要
④ エージェントが必要
対応のサービス

LAN側
動作するサーバーに制限
Web / 他

ゼロトラスト　ID認識型プロキシ＝透過プロキシ型 SaaS 構成

透過プロキシ型

SaaS

①	idP	idPは指定
②	ID認識型プロキシ	透過プロキシ

自社

③	プロキシコネクタが必要	LAN側
④	エージェントが必要	動作するサーバーに制限
	対応のサービス	Web / 他

ゼロトラスト　ID認識型プロキシ＝リバースプロキシ型での構成

リバースプロキシ型

WAN側
① idP　　idPはどこのサービスでも利用可能
② ID認識型プロキシ　　リバースプロキシ

ターゲットネットワーク
エージェント不要　　ターゲットサーバーのOS制限なし
対応のサービス　　Web のみ

ゼロトラスト　透過型とリバースプロキシ型の比較

項目	透過型	リバースプロキシ
ターゲット	Web	Webのみ
Web以外のアプリ	エージェントに依存	非対応
idPの選択	各社による	選択可能
ネットワークの変更	必要・プロキシコネクタ設置	不要
導入の敷居	高い	低い
導入までの期間	数週間	1日

既存の社内Webへのアクセス

SSL アクセス

Webサーバー

Web認証が弱い

認証がない

Web側の変更したくない

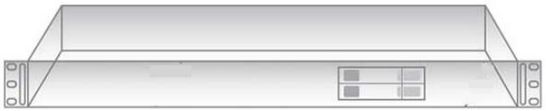
認証対応　「Powered BLUE」 アプライアンス

① Web / Mail / DNS 機能 / マルチドメイン対応 / GUI

② AD認証 / OTP認証 / SSLクライアント認証
ゼロトラスト対応 SAML認証

③ リバースプロキシ　ID認識型リバースプロキシ

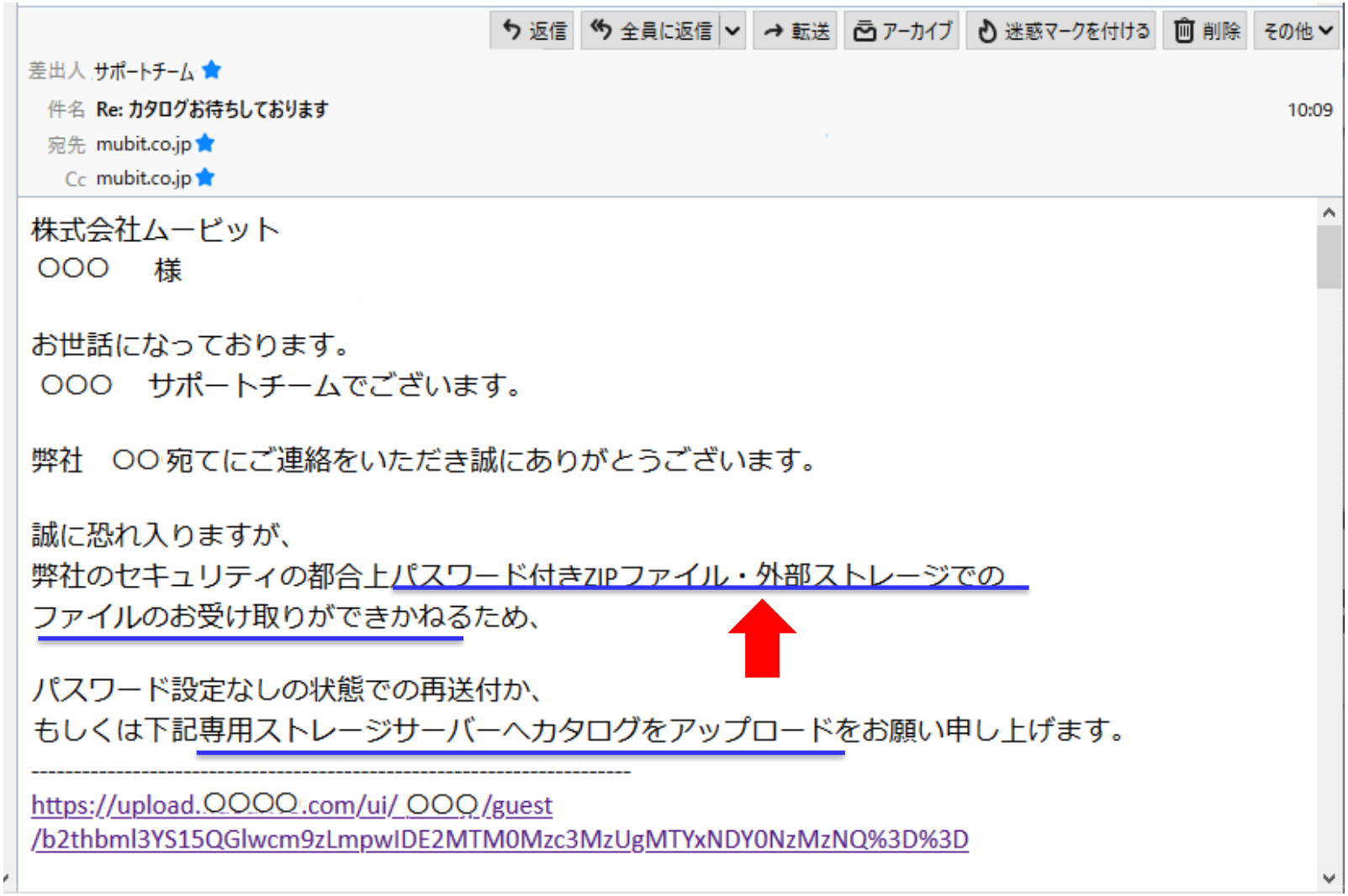
認証対応リバースプロキシ
①+②+③



POWERED BLUE

リバース
プロキシ

ZIPファイル拒否・外部ストレージ禁止の相手先



返信　全員に返信　転送　アーカイブ　迷惑マークを付ける　削除　その他

差出人 サポートチーム

件名 Re: カタログお待ちしております　10:09

宛先 mubit.co.jp

Cc mubit.co.jp

株式会社ムービット
〇〇〇　様

お世話になっております。
〇〇〇　サポートチームでございます。

弊社　〇〇宛てにご連絡をいただき誠にありがとうございます。

誠に恐れ入りますが、
弊社のセキュリティの都合上パスワード付きZIPファイル・外部ストレージでの
ファイルのお受け取りができかねるため、

パスワード設定なしの状態での再送付か、
もしくは下記専用ストレージサーバーへカタログをアップロードをお願い申し上げます。

---

https://upload.〇〇〇〇.com/ui/〇〇〇/guest
/b2thbml3YS15QGlwcm9zLmpwIDE2MTM0Mzc3MzUgMTYxNDY0NzMzNQ%3D%3D

NAS　自社に共有ディスクがある場合

- NAS　Webベースでの動作に対応
  共有フォルダー

認証が脆弱　　ID / パスワード

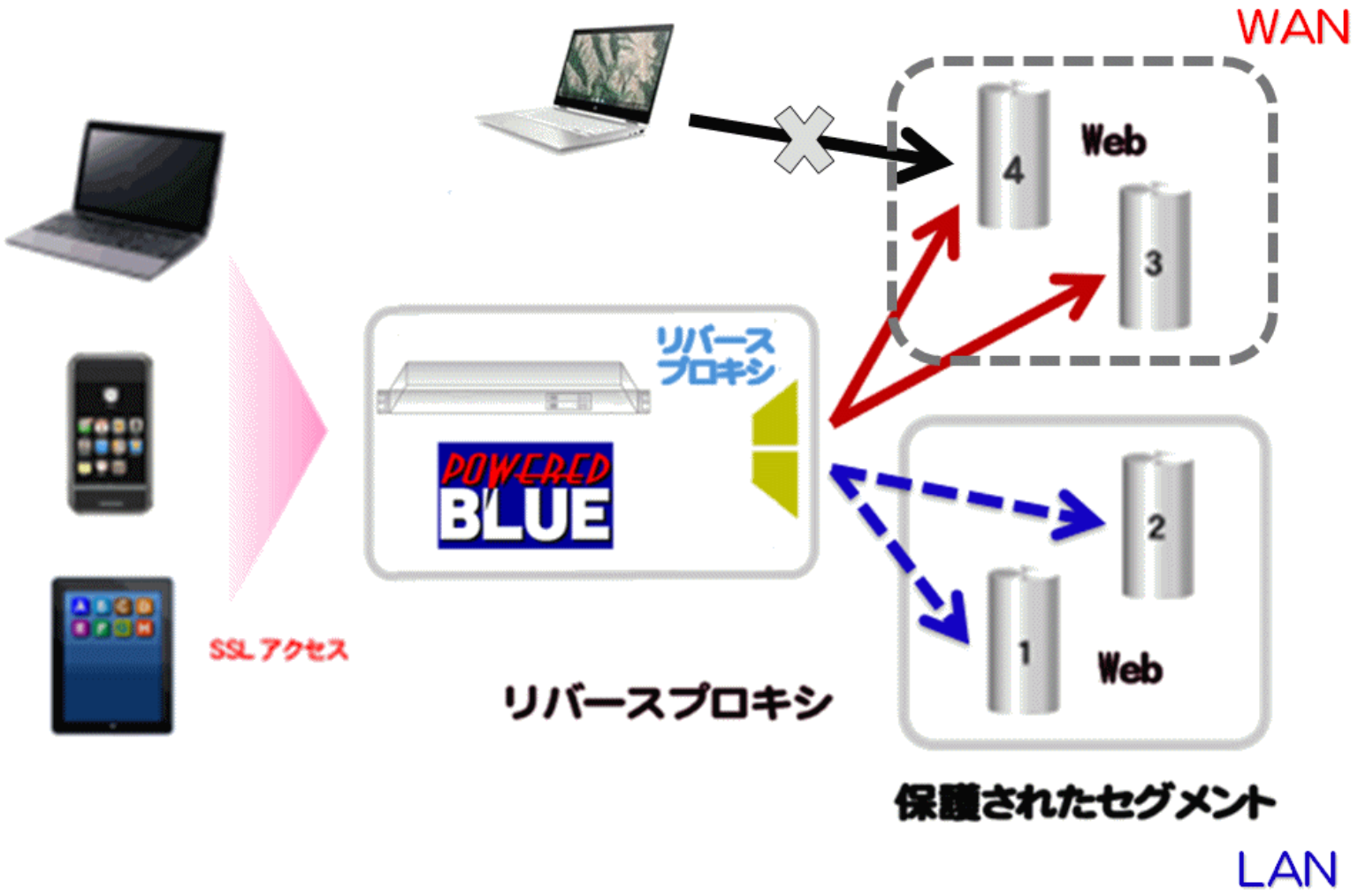
リバースプロキシ経由でアクセス

■ 認証対応のリバース・プロキシ

Powered BLUE Reverse-Proxy

SSLクライアント認証・OTP認証・AD認証・SAML認証

リバースプロキシ経由のアクセスのみを許可



WAN側へ設置のWebサーバーでもセキュリティを確保

認証１）　ワンタイムパスワード認証

ソフトウエアトークン

OSS や 無償 の ソフトウエアトークン

製品	ロゴ	iOS Android	PC	言語	備考
Google Authenticator		○		英語	オープンソース
IIJSmartKey		○		日本語	無償
Authy		○	○ Windows Mac Linux	英語	無償
WinAuth			○ Windows	英語	無償

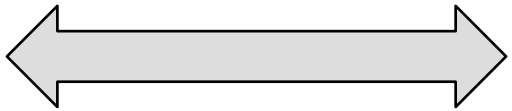
ワンタイムパスワード認証 + リバースプロキシ

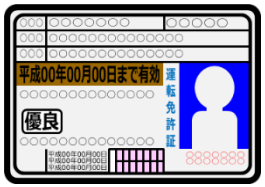
ワンタイムパスワード認証

ワンタイムパスワード　＋　任意パスワード　に対応

認証2) SSLクライアント認証

■ SSLクライアント証明書





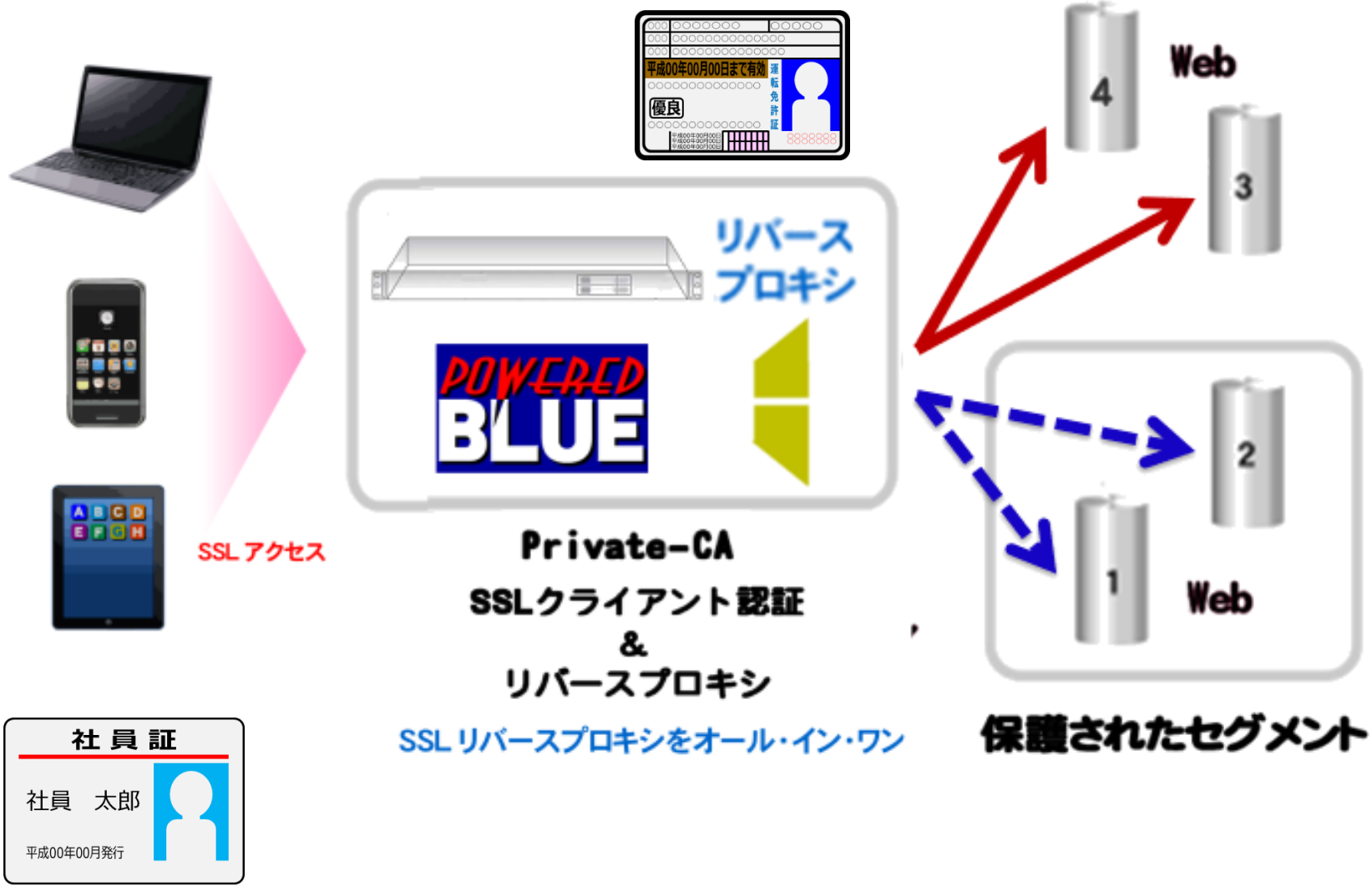
■ SSLサーバー証明書

SSLクライアント認証例　スマートフォン

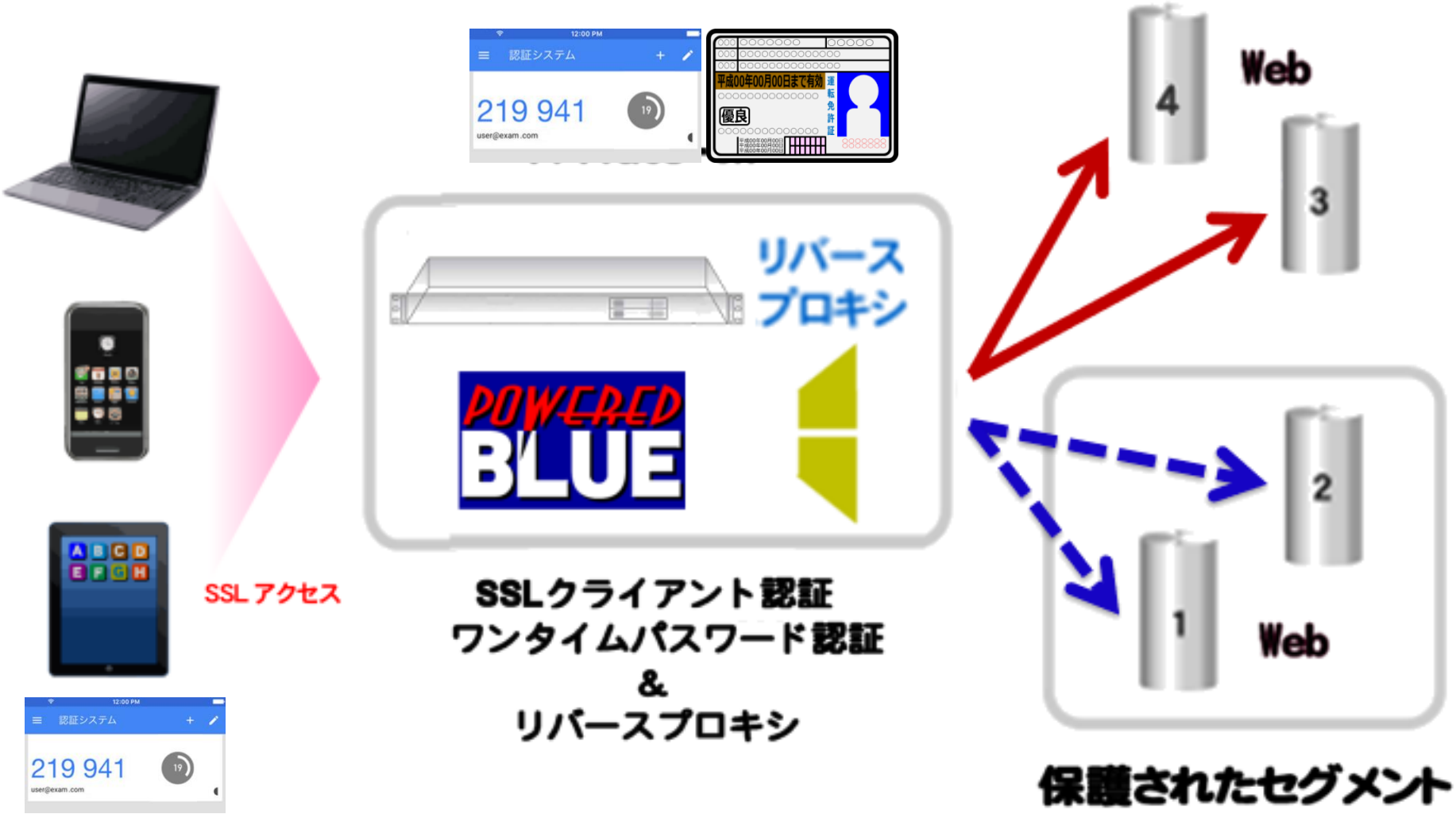
証明書　有効

証明書　なし・失効

SSLクライアント認証 + リバースプロキシ



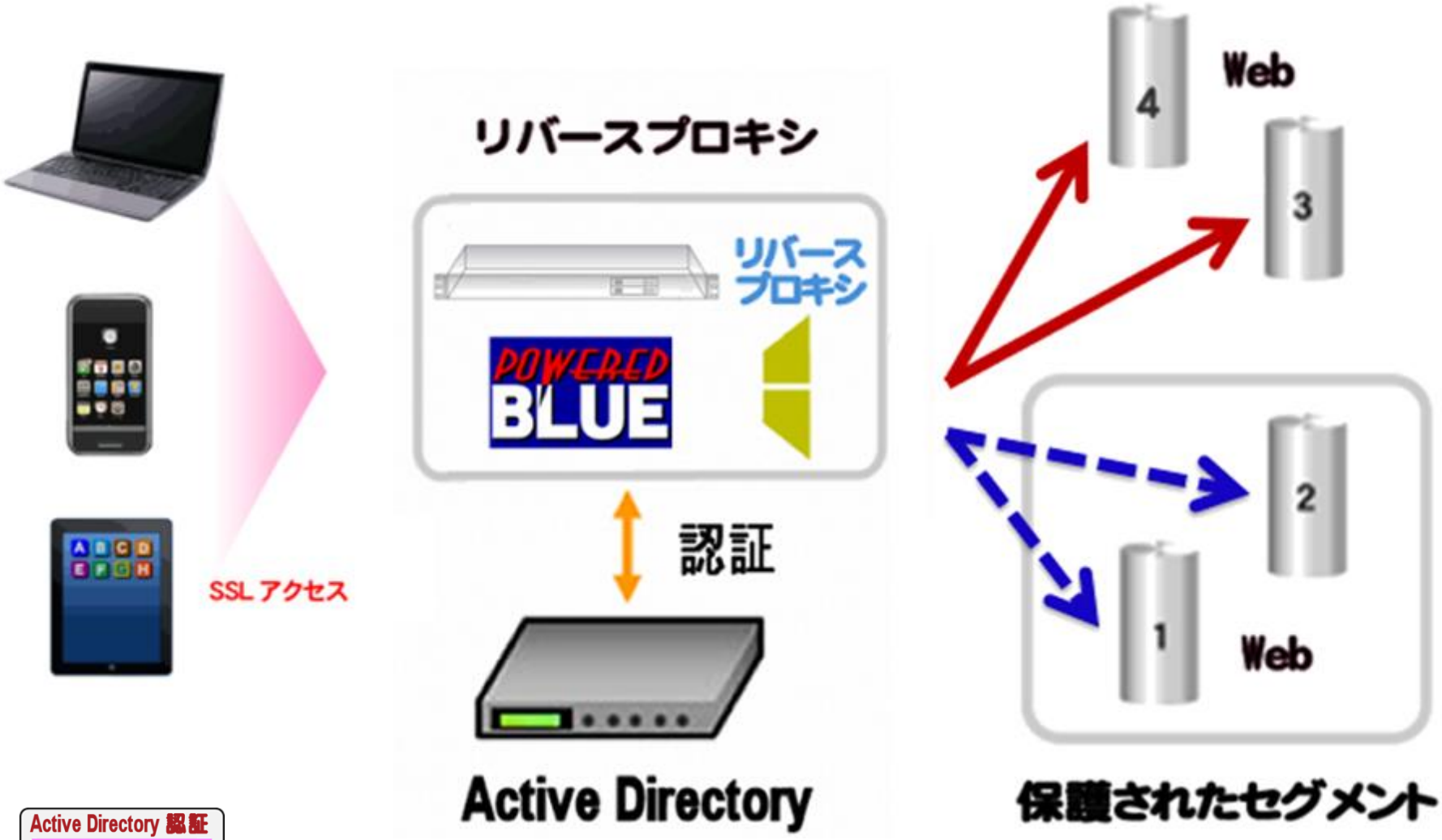
認証3) ワンタイムパスワード + SSLクライアント認証



ワンタイムパスワード認証 + SSLクライアント認証

SSLクライアント認証　＋ ワンタイムパスワード認証　＝　多要素認証

認証4) AD認証


リバースプロキシ
リバースプロキシ
POWERED BLUE
認証
SSL アクセス
Active Directory
4
Web
3
2
1
Web
保護されたセグメント
Active Directory 認証
社員　太郎
00年00月発行

認証5) AD + SSLクライアント認証

AD + SSLクライアント認証

認証6）ID認識型リバースプロキシ

リバースプロキシ・タイプ　（Webサービスのみ）

(親) SAML認証　idP / IDaaSなど

iDaaS = iD As A Service

idP / iDaaS 比較

	SAML	AD連携	GUI 日本語対応	費用 月額･人
Azure AD 米国	○	○	○	672-1000円
OneLogin 米国	○	○	×	300-1000円
Okta 米国	○	○	×	300-1000円
KeyCloak RedHat	○	△	×	オープンソース
トラストログイン 日本	○	○	○	0-300円
CloudGate UNO 日本	○	○	○	100-1000円

ID認識型リバースプロキシ

- ID認識型リバースプロキシからのアカウント **漏洩の心配不要**

- **エージェント不要**
  - ●ターゲットのWebサーバーの変更不要
  - ●任意のidPと連携可能

- ゼロトラスト対応/ID認識型リバースプロキシの **設置運用は簡単**

ゼロトラスト対応 + ID認識型リバースプロキシ

- ターゲットのWebサーバーへ、ゼロトラスト＆SSOのリバースプロキシ経由でアクセス
- エージェント不要 / ターゲットのWebサーバの変更は不要

ゼロトラスト対応　SSO / SAML認証

1）ID認識型リバースプロキシへアクセス
2）初回のみidPへアクセス（ シングルサインオン ）
3）idPの認証後にリバースプロキシ先のWebにリダイレクト

ID認識型リバースプロキシ導入パターン

- iDaaS を利用の場合　（すでに親がある場合）

  Azure AD / トラストログイン /onelogin / G suite
  CloudGate UNO / HENNGE ONE / okta / OpenAM などを利用

  リバースプロキシ のみ 導入

- まだ親がいない場合

  トラストログイン （idP・無償）と リバースプロキシ を導入

トラスト・ログイン by GMO ＋

認証対応 の Web を 新規 に 構築

「Powered BLUE Web サーバー」

Web + ワンタイムパスワード認証

仮想サイト1

仮想サイト2

仮想サイト3

Web + SSLクライアント認証

仮想サイト1

仮想サイト２

仮想サイト3

Web + AD認証

仮想サイト1

仮想サイト２

仮想サイト3

Web + SSLクライアント認証+AD認証

仮想サイト1

仮想サイト２

仮想サイト3

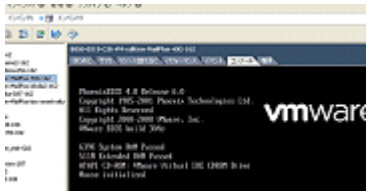
ゼロトラスト対応Web　idP認証

仮想サイト1

仮想サイト２

仮想サイト3

アプライアンスでの提供・動作環境



POWERED BLUE

POWERED BLUE

Microsoft® Hyper-V™

powered by amazon web services

- VPNの代替

  VPN機器増強よりも

  認証対応のリバースプロキシを併用

  ワンタイムパスワード認証
  SSLクライアント認証
  AD認証
  SAML認証

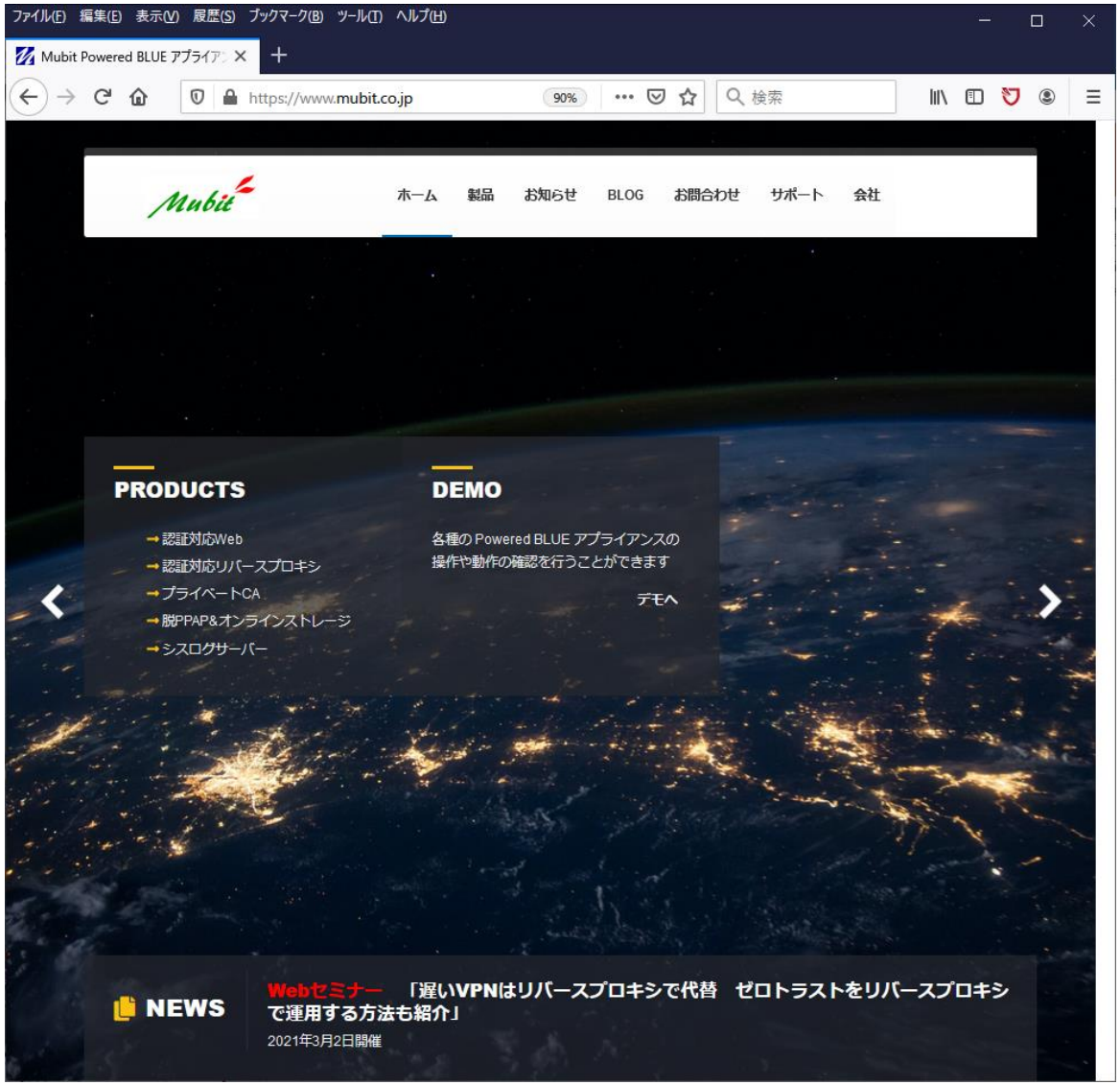
- ゼロトラストの導入

  リバースプロキシ型は導入が簡単

Webサイト

認証対応
Web

認証対応
リバース
プロキシ



https://www.mubit.co.jp/