Soliton®

オールインワン認証アプライアンス

NetAttest EPS

ネットアテスト イーピーエス

Network

RADIUS、プライベートCA、ワンタイムパスワード
ネットワーク認証に必要な機能を一台に

- 高度なネットワーク認証環境を短期間で構築したい
- 運用負荷やコストを抑えてセキュリティを強化したい
- デジタル証明書を社内で発行、運用したい
- 既存のユーザーデータベースを利用して認証したい
- スマートデバイスの導入・運用をもっと楽にしたい

NetAttest EPS

基本機能

RADIUS機能

様々な認証に対応

NetAttest EPSは様々なタイプの認証方式に対応します。
ID/パスワードを利用した認証からデジタル証明書を利用した強固な認証、ワンタイムパスワードを併用した認証環境まで、NetAttest EPSなら1台で構築可能です。

デジタル証明書	ID・パスワード	MACアドレス	ワンタイムパスワード

利用可能なユーザー情報データベース

ローカル	NetAttest EPSに内蔵されたデータベースです。
Active Directory	Active Directoryに登録されたユーザーを参照できます。主にMS-PEAP認証で利用します。
LDAP	X.500準拠のLDAPサーバーに登録されたユーザー情報を参照し認証できます。主にPAPで利用します。
RADIUS	RADIUSプロキシ機能により、受信した認証要求を他のRADIUSに転送し、認証できます。

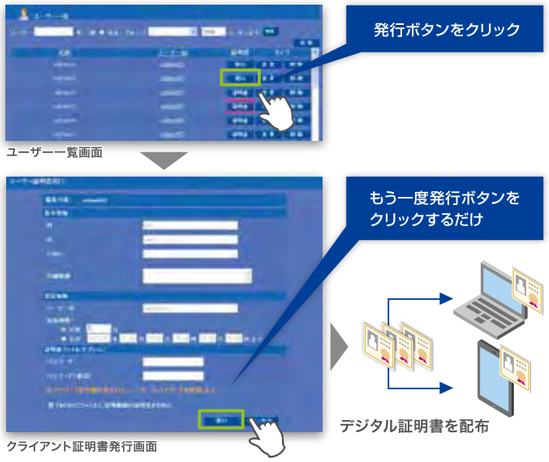
ゲストユーザー登録機能

認証アカウントの登録を、来訪者自身や来訪者対応する社員が行なえる機能です。ゲストアクセス環境の構築や、(半)公開Wi-Fiでの利用履歴の取得が可能です。

プライベートCA機能

デジタル証明書を簡単発行

NetAttest EPSは、本格的なプライベートCA機能を標準搭載しており、デジタル証明書の安全な発行・運用をサポートします。管理者は、最短2回のクリックでクライアント証明書を発行でき、また、「証明書一括生成ツール(無償オプション)」を用いて大量の証明書の一括発行も行えます。IEEE802.1XやVPN接続において、証明書を用いた強力な認証を実現し、持ち込み端末、不正ユーザーからLANを守ります。



ALL-in-one Authentication Appliance

この1台が、ネットワークの入り口を守ります

有線/無線LANはもちろん、VPN、リモートアクセスも安全に

LANは、企業に蓄積された あらゆる情報への入り口です。
誰もが、無秩序に接続できる状態ではなく、決められた人、決めら れた端末だけが、接続できるように鍵をかけておく必要があります。
NetAttest EPSは、LANへの接続 時にユーザーや端末を特定するための
ネットワーク認証に必要な 機能が詰め込まれています。
LAN接続時に認証を行えば、正規のユーザーの利便性 を損なわずに不正なユーザーやPCをシャットアウトできます。
もちろんLANへの直接接続だけでは なく、VPNやリモートアクセス接続など
ネットワークの入り口を1台で守る 統合認証サーバーとして活躍します。

RADIUS アプライアンス 国内シェア No.1

株式会社富士キメラ総研「2006, 2007, 2008, 2009, 2010 ネットワークセキュリティビジネス調査総覧」、
「2012, 2013, 2014, 2015, 2016, 2017 コミュニケーション関連マーケティング調査総覧」
RADIUSサーバー(アプライアンス)市場における調査結果より

オプション

NetAttest EPS-ap マルチOSへの証明書、Wi-Fi設定配布

管理者に代わり、スマートデバイスを自動設定

詳細はp.7へ

NetAttest EPS(要拡張CAオプション)と連携し、スマートデバイスやPCへのデジタル証明書の配布と利用ポリシーの適用を自動化します。また、モバイルデバイス管理(MDM)機能を利用することで、スマートデバイスに対しリモートからのデバイスロックやワイプが行えます。

機能拡張オプション

Windowsサーバーの機能とより密な連携

Windowsドメイン認証連携機能、グループプロファイル機能が利用可能になります。

※SXモデルではWindowsドメイン認証連携機能のみ利用可能です。DXモデルではオプションなしでご利用いただけます。

拡張CAオプション

より本格的なCA機能の利用

詳細はp.6へ

OCSPやSCEP、メールでの期限通知機能など、より細やかなCAの設定・運用機能を提供します。

MACアドレス認証拡張オプション

専用DBを利用したMACアドレス認証が可能に

基本機能で使えるユーザーDBとは別に 20万アドレスまで登録できるMACアドレス用DBが利用可能になります。

※本オプションなしでもユーザーDBに MACアドレスを登録することで MACアドレス認証は利用できます。

許可端末MACアドレス登録の手間を大幅削減

ネットワーク利用者による MACアドレス申請、権限を与えられたユーザーによる MACアドレス代理登録、RADIUS(PAP) 認証を利用したMACアドレス収集により、管理者の MACアドレス登録の手間を削減できます。

ワンタイムパスワード

VPN機器等にさらに厳格な認証を提供

詳細はp.6へ

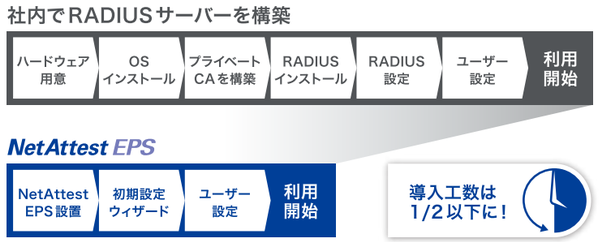
別途サーバーの用意が不要で、シンプルかつ低コストなワンタイムパスワード認証環境の構築が可能です。勿論、デジタル証明書とワンタイムパスワードを組み合わせた認証が可能で、VPN機器やWebサーバーへの接続などにおいて、厳格な認証を提供します。

NetAttest EPSを選ぶ、3つの“簡単”ポイント

オールインワンアプライアンス製品なので 特別な知識、技術がなくても短時間で導入可能

Point 1

ネットワーク認証に必要な機能がすべて揃った国産のアプライアンス製品です。サーバーの用意やソフトウェアのインストールなど、高度な技術やコマンドの習得は不要で、極めて短時間に認証システムを構築できます。運用フェーズにおいては、汎用OSのように頻 にセキュリティパッチを適用する必要はありません。また、機器専用のバージョンアップファイルを適用することで、パッチ適用によりシステムが不安定になる心配もありません。



誰でも簡単に設定・運用が可能

Point 2

直観的な日本語Web GUIで

管理画面はすべて日本語Web GUIで、設定や運用に特別なスキルは必要ありません。管理、運用も手軽なので、システム運用コストを低く抑えられるためTCO低減にも貢献します。

英語GUIにも対応 グローバル企業でも利用できる

NetAttest EPSはGUIの英語表示に対応しており、利用者のブラウザまたはシステム設定に応じて、表示言語を日本語・英語から自動的に選択し表示します。

日本語 Web GUI画面

英語 Web GUI画面

オールインワンアプライアンス製品なので 万一の時も短時間で復旧・稼動

Point 3

設定情報は１つのファイルに集約し、FTPサーバーへ定期的に自動でバックアップできます。障害発生時はバックアップされた設定情報を代替機にリストアするだけ。最短10分で正常稼働に復帰します。

※年間サポート契約が必要です。

NetAttest EPSを選ぶ、3つの“安心”ポイント

専用アプライアンス製品なので 壊れにくく、安定稼働、サポートも安心

Point 1

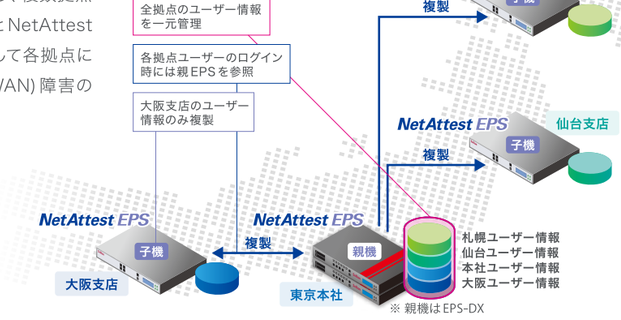
NetAttest EPSはソフトウェアもハードウェアも最適化された専用アプライアンス製品です。2003年に販売を開始して以来、プライベートCA機能を持ったRADIUSアプライアンス製品として 順調に実績を伸ばしてきました。ハードディスクレス※のため、トラブルが少なく、メンテナンスの手間もかかりません。また、長年培ったノウハウによる充実したサポート体制により、安定した運用を可能にします。

※ DX版を除く

冗長化または分散構成をすることにより ネットワークを常に利用可能な状態に維持

Point 2

NetAttest EPSは二重化に対応し、万が一の障害時にシステムが止まる事態を防止します。分散構成(親子連携)にも対応しており、複数拠点に展開したNetAttest EPSの登録ユーザーの一元管理とNetAttest EPS親子間での認証連携を実現します。また、分散構成として各拠点にNetAttest EPSを配置することで、拠点間ネットワーク(WAN)障害の場合でも拠点内のネットワークが止まることはありません。



国内に流通する多くの製品との連携実績

Point 3

有線LAN機器

●ALAXALA Networks ●Alcatel-Lucent ●Allied Telesis ●Brocade Communications Systems ●Buffalo ●Cisco Systems ●D-Link ●Enterasys Networks ●FUJITSU ●HANDREAMNET ●Hewlett-Packard ●Hitachi Cable ●Panasonic ●PIOLINK

無線LAN機器

●Alcatel-Lucent ●Allied Telesis ●ARUBA Networks ●Avaya ●Buffalo ●Cisco Systems ●D-Link ●ELECOM ●Fortinet ●FUJITSU ●FURUNO SYSTEMS ●Hewlett-Packard ●I･O DATA ●Meru Networks ●Netgear ●Proxim Wireless ●Ruckus Wireless ●SonicWALL

VPN機器 (IPSec/SSL-VPN)

●Allied Telesis ●Array Networks ●Check Point Software Technologies ●Cisco Systems ●Citrix Systems ●D-Link ●F5 Networks ●Fortinet ●FUJITSU ●Juniper Networks ●SonicWALL ●YAMAHA

※ 全ての環境において動作を保証するものではありません。

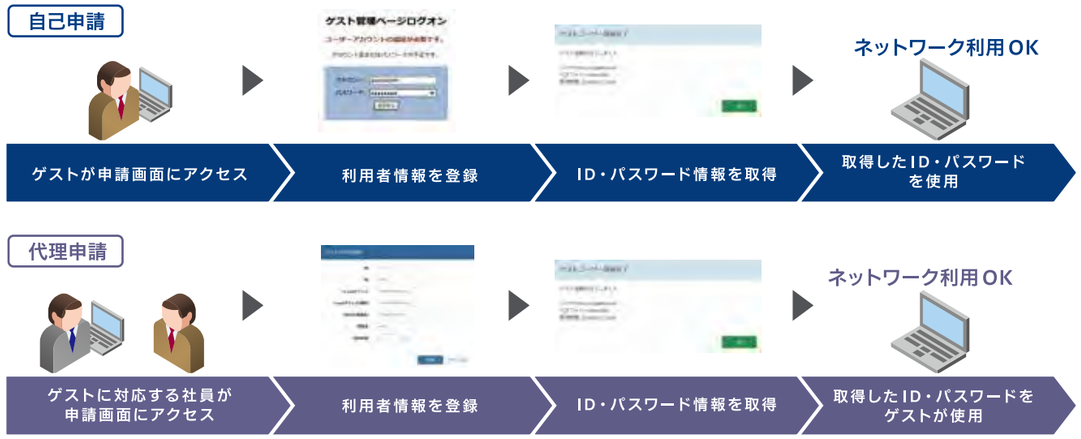
※その他、実績多数あります。

利用の幅を広げる便利な機能

ゲストユーザー登録機能 標準機能

一時的に認証アカウントを登録

ネットワークを利用したい方向けに、一時的に有効なアカウントを作成することができます。オフィス、店舗への来客や病院の患者に無線LANを利用させたい時に最適です。来訪者自身が登録する方式、自社従業員が代理登録する方式など、環境にあわせた方式を選択できます。



拡張CA機能 オプション

SCEPによる証明書のオンライン配布

証明書発行の標準方式であるSCEP(Simple Certificate Enrollment Protocol)に対応しています。NetAttest EPS-apや、SCEP対応のVPN機器等からの証明書発行要求に対して、自動的な証明書の発行、インポートを行うことができます。

用途に合わせた証明書プロファイルを用意

証明書の用途、鍵長、有効期限、CRL配布ポイント等の属性を、証明書プロファイルとして管理できます。用途に応じた証明書プロファイルのテンプレートも複数用意しています。

ワンタイムパスワード機能 オプション

ワンタイムパスワード機能を搭載、モバイル環境から安全なネットワーク利用が可能

ワンタイムパスワードとは、一度限り使用可能なパスワードです。認証の度に有効なパスワードが変化するので、一度使用したパスワードは無効となります。万が一ワンタイムパスワードが盗まれた場合でも、それを再利用し不正に取引されることはありません。NetAttest EPSが提供するワンタイムパスワードは、独自の生成アルゴリズムを採用して高い認証強度を持ったVASCO社製です。全世界で8000万個以上の販売実績があります。また、ハードウェアトークンは最大で7年間使用可能なため、電池切れによるトークンの買換えコストやユーザーへの配布の手間も最小限で済みます。

トークンの種類も豊富で、利用シーンに応じてトークンを選択できます。

- DIGIPASS GO 6（ハードウェアトークン）
- ソフトウェアトークン※

※ 対象OSは当社Webサイトをご覧ください。

VASCO THE AUTHENTICATION COMPANY
DIGIPASS GO 6

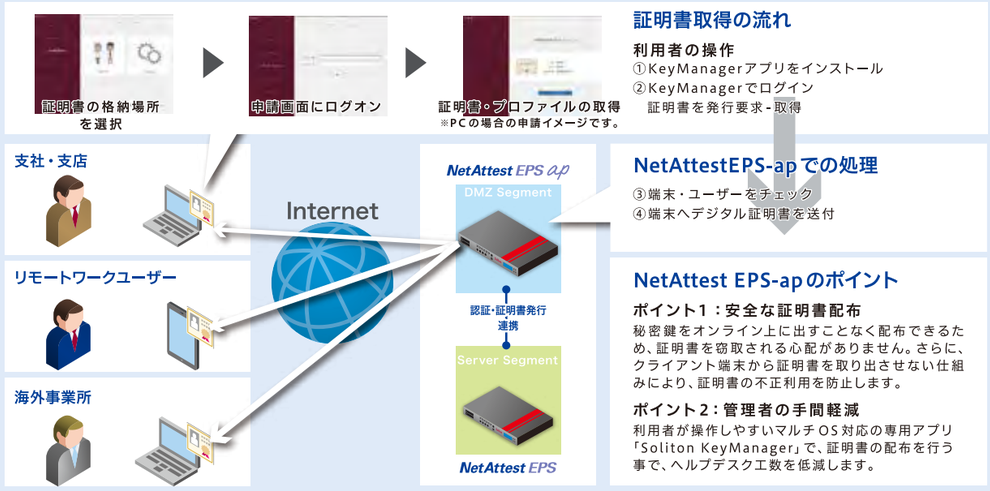
NetAttest EPS ap

インターネット経由で安全にデジタル証明書を配布

証明書配布オプション オプション

証明書発行～取得を自動化

NetAttest EPS-apは、マルチデバイス・BYOD環境におけるデジタル証明書の展開・運用をサポートするオプションアプライアンスです。
DMZにNetAttest EPSのプロキシとして設置する事で、社内LANにまだ接続していない端末にも、デジタル証明書を安全に配布できます。



証明書取得の流れ

利用者の操作
①KeyManagerアプリをインストール
②KeyManagerでログイン
　証明書を発行要求・取得

NetAttestEPS-apでの処理

③端末・ユーザーをチェック
④端末へデジタル証明書を送付

NetAttest EPS-apのポイント

ポイント1：安全な証明書配布
秘密鍵をオンライン上に出すことなく配布できるため、証明書を窃取される心配がありません。さらに、クライアント端末から証明書を取り出させない仕組みにより、証明書の不正利用を防止します。

ポイント2：管理者の手間軽減
利用者が操作しやすいマルチOS対応の専用アプリ「Soliton KeyManager」で、証明書の配布を行う事で、ヘルプデスク工数を低減します。

モバイルデバイス管理（MDM）機能※

デバイス情報の取得、プロファイルの適用・削除、リモートからのデバイスロックやワイプが行えます。デバイスロックおよびワイプは、管理者による実行のほか、デバイス利用者自らが実行するセルフメンテナンス機能も可能です。

※ Android、iOSデバイスのみ対応。

管理者によるデバイスロック/ワイプ実行

利用者による実行（セルフメンテナンス機能）

NetAttest EPS-ap

		EPSAP-DX04-A	EPSAP-ST05-A
モデル番号		EPSAP-DX04-A	EPSAP-ST05-A
対応スマートデバイス		Android/iOS/ Mac/ Windows ※1	
最大管理デバイス数		50,000	2,000
証明書・プロファイルの配布		○	○
企業内アプリの配布		○	-
MDM	MDM機能	○	○※2
	デバイス情報の取得	○（取得データを内部に保存）	○（一時表示のみ）
ネットワークインターフェイス		10/100/1000BASE-T(X) 自動認識&Auto-MDI-X×4	
形状		EIA19インチラックマウントタイプ	
外形寸法（W×H×D）		443mm×44mm×407mm	438mm×44mm×292mm
重量		7.8kg	4.2kg
電源		90～264Vac、47～63Hz (90～135Vacのみサポート)	
最大消費電力		121VA	28VA
発熱量		412.8BTU/h、104.1kcal、121W	95.5BTU/h、24.1kcal、28W
動作環境		温度0～40℃、湿度20～90% RH結露無きこと	
適合規格		VCCI(ClassA)、FCC(Class A)、CE、UL、RoHS、PSE(電源ケーブル)	

※1 動作環境の詳細は当社Webサイトをご参照ください。
※2 機器本体の他にモバイルデバイス管理オプションの購入が必要です。

Windowsで設定可能な項目

設定
・デジタル証明書取得
・無線クライアント(wi-fi)の設定

Macで設定可能な項目

設定
・デジタル証明書取得

iOSで設定・制御可能な項目

設定
・デジタル証明書取得(SCEP設定)
・パスコードポリシーの設定
・無線クライアント(wi-fi)の設定
・リモート接続クライアント(VPN)の設定
・ExchangeActiveSync設定
・その他

MDM（モバイルデバイス管理機能）
・デバイスロック
・リモートワイプ(端末情報消去)
・端末・アプリケーション情報の取得
・プロファイルの適用・削除

制御
デバイスの機能制御
・プロファイルの削除禁止
・アプリケーションのインストール禁止
・カメラの使用禁止
・画面の取り込み禁止(画面キャプチャ)
・AppStore内での購入禁止
・その他

デバイスの機能制御
・Safariの使用禁止
・iTunes等のアプリケーションの使用禁止
・その他

Androidで設定可能な項目

設定
・デジタル証明書取得

MDM（モバイルデバイス管理機能）
・デバイスロック
・リモートワイプ（端末情報消去）
・端末・アプリケーション情報の取得

製品仕様 / 動作環境

NetAttest EPS

				
モデル番号		EPS-DX04-A	EPS-ST05-A	EPS-SX15-A
最大ユーザー登録数		100,000	200/500※1/2,000※2/5,000※2	200
最大RADIUSクライアント登録数		1,000/2,000※3	500	20
対応認証方式		EAP-TLS、EAP-MD5、EAP-PEAP (MS-CHAPv2、GTC、TLS)、EAP-TTLS (PAP、CHAP、MS-CHAP、MS-CHAPv2、GTC、EAP-MSCHAP v2、EAP-TLS)、Cisco-LEAP、EAP-FAST、PAP、CHAP、MS-CHAP、MS-CHAP v2		
二重化機能		○	○	-
RADIUS認証拡張	ワンタイムパスワード認証	○※4	○※4	○※4
	MACアドレス専用DBによるMACアドレス認証	○※5	○※5	○※5
	グループ・プロファイル	○	○※2	-
証明機関（CA）	クライアント証明書発行	○	○	○
	クライアント証明書発行可能数	200,000	400/1,000※1/4,000※2/10,000※2	400
	外部サーバー証明書発行	○	○	-
	拡張CA機能	○※6	○※6	-
外部DB連携	Windowsドメイン認証連携	○	○※2	○※7
	外部LDAPデーターベース参照	○	○	○
	RADIUSプロキシ	○	○	-
ログ	RADIUS簡易アカウンティングログ	○	○	○
	RADIUS詳細アカウンティングログ	○	-	-
	ログメンテナンス	○	-	-
その他機能		SNMP (エージェント)、NTP時刻同期、Syslog、UPS対応		
ネットワークインターフェイス		10/100/1000BASE-T(X)自動認識&Auto-MDI-Xx4		
形状		EIA19インチラックマウントタイプ		デスクトップ
外形寸法 (W×H×D)		443mm × 44mm × 407mm	438mm X 44mm x 292mm	165mm x 43mm x 106mm
重量		7.8kg	4.2kg	0.65kg
電源		90～264Vac、47～63Hz (90～135Vacのみサポート)		
最大消費電力		121VA	28VA	22VA
発熱量		412.8BTU/h、104.1kcal、121W	95.5BTU/h、24.1kcal、28W	75BTU/h、18.9kcal、22W
動作環境		温度0～40℃、湿度20～90%RH結露無きこと		
適合規格		VCCI (ClassA)、FCC(ClassA)、CE、UL、RoHS、PSE (電源ケーブル)		VCCI(ClassB)、FCC(ClassB)、CE、UL、RoHS、PSE(ACアダプタ、電源ケーブル)

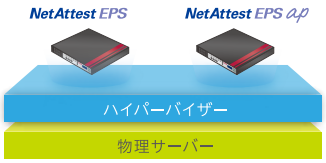
※1 ユーザー数拡張オプションが必要です。 ※2 機能拡張オプションが必要です。 ※3 RADIUSクライアント利用数拡張オプションが必要です。 ※4 ワンタイムパスワードオプションが必要です。※5 MACアドレス認証拡張オプションが必要です。
※6 拡張CAオプションが必要です。 ※7 Windowsドメイン認証連携オプションが必要です。

拡張 CA オプション

	拡張CAオプション有	拡張CAオプション無
証明書形式	X.509 Ver3	
公開暗号鍵方式	RSA相当、DSA、ECC　ECC楕円曲線：P-245、P38.4、P521	RSA/DSA鍵長：512、1024、2048、4096、8192bits
ダイジェストアルゴリズム	MD5、SHA1、SHA256、SHA384、SHA512	
Webエンロール(Xenroll、CertEnroll)による証明書配布	○	-
SCEPエンロールによる証明書配布	○	-
証明書失効情報伝達	OCSP、失効リスト(httpによる取得)	失効リスト(httpによる取得)
証明書失効リスト	PEM形式、DER形式	

仮想アプライアンス

VMWare対応の仮想アプライアンスもご用意しています。詳細は当社HPをご覧ください。



Soliton Products

NetAttest EPS と連携して安心・安全なITインフラを実現

安全・快適なモバイルWebアクセス

デジタル証明書を利用した認証を行い、端末内に情報を保存しない
リモートアクセスや、Webシングルサインオンの仕組みを提供します。

Soliton SecureBrowser
www.soliton.co.jp/ssb/

Smart eGate
www.soliton.co.jp/egate/

大容量ファイルの送受信

デジタル証明書を利用した認証を行い、安全・確実にファイルを
送受信する仕組みを提供します。

FileZen
www.soliton.co.jp/filezen/

機器にとらわれないセキュリティ

既設のネットワーク機器の仕様に依存せずに、
不正端末を接続検知し、排除する仕組みを提供します。

NetAttest LAP
www.soliton.co.jp/lap/

システム運用の快適さと効率を更に追求

日々のアカウント管理を自動化する仕組みを提供します。

Soliton ID Manager
www.soliton.co.jp/idmanager/

⚠ 安全に関するご注意　正しく安全にお使いいただくために、ご使用の前に必ず「取扱説明書」をお読みください。

Soliton®
株式会社ソリトンシステムズ　https://www.soliton.co.jp/
〒160-0022　東京都新宿区新宿 2-4-3
TEL 03-5360-3811　netsales@soliton.co.jp
大阪営業所 06-6821-6777　福岡営業所 092-263-0400
名古屋営業所 052-217-9091　東北営業所 022-716-0766
札幌営業所 011-242-6111

このカタログは 2018年5月現在のものです。仕様、デザインは予告なく変更することがあります。　EPS-1805A