iBRESS cloud

VPNを使わない
セキュアなIIoTの構築

スクエアFreeセミナー

March,22 2018

Ver.1.0

会社概要

社 名	株式会社　ベルチャイルド
代表者	代表取締役　藤田 好邦
本社	〒530-0037 大阪府大阪市北区松ヶ枝町1-3 いちご南森町ビル3F
東京オフィス	〒101-0021 東京都千代田区外神田4-7-5 石川興産ビル8F
創　業	平成11年4月1日
資本金	5,000万円
従業員	149名

当社の強み

創業以来、金融/保険システムを中心としたシステム開発に携わって参りました。「堅牢なインフラ開発技術」「高度な運用ノウハウ」を強みとして、近年、物流システム、ＭＥＳシステム開発へＳＩ事業を展開し、M2M/IoT市場にもこの強みを活用してまいります。

VEC（Virtual Engineering Community）の事務局をしております。

積乱雲プロジェクト　関東 / 関西

Industrial Automation Forum
（一般財団法人製造科学技術センター内設置）

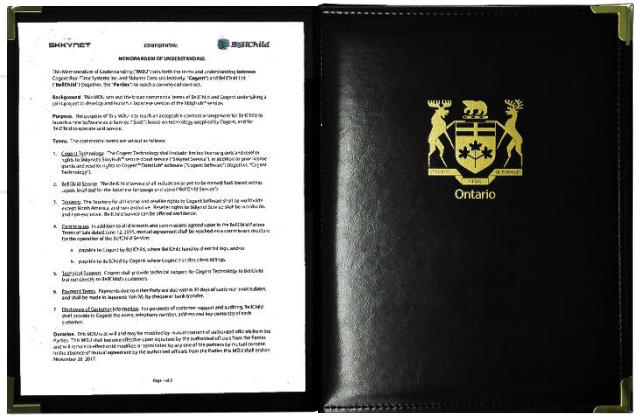
駐日カナダ大使、オンタリオ州首相立ち合いの基

次世代クラウドの共同開発の覚書締結

2016年11月28日 於;カナダ大使館

SKKYNET

SOLUTIONS | PRODUCTS | PARTNERS | LIBRARY | INVESTORS | ABOUT US



Cogent and BellChild to Launch Next Generation iBRESS Service

December 7, 2016 / by Bob McIlvride

Skkynet subsidiary Cogent Real-Time Systems signs memo of understanding with BellChild to offer next generation cloud service for Industrie 4.0 and Industrial IoT.

Mississauga, Ontario, December 7, 2016 – Skkynet Cloud Systems, Inc. ("Skkyr
leader in real-time cloud information systems, announces that Cogent Real-Tin
subsidiary, signed a memo of understanding with BellChild Ltd. of Osaka, Japar
generation iBRESS™ cloud service. This MOU supports the rollout of an Asian-
(Software as a Service) for secure, real-time data communication suitable for Ir
(IIoT) applications.

2017年11月8日(水)

次世代クラウドサービス「iBRESS Cloud」の提供開始

～VPNを使わない、安全で高速・双方向可能なデータ通信サービス～

株式会社ベルチャイルド（本社：大阪市北区、代表取締役：藤田好邦　以下 ベルチャイルド)とSkkynet Cloud Systems, Inc. (本社：カナダ、オンタリオ州、CEO ：Andrew Thomas　以下Skkynet)は、産業用システムや組み込み機器のデータを、VPNを使わずインターネット回線で安全にかつ高速・双方向に送受信し、見える化・障害通知・予知保全などに活用できる『iBRESS Cloud』について、2017年12月1日からサービスの提供を開始いたします。

IIoTに求められるクラウド

- 安全性
- 経済性
- 高速性
- 拡張性
- 柔軟性
- 先進性

IIoTが求めるクラウド

■ 安全性

・WEB技術を用いたデータ通信
・セキュリティポリシーに影響を与えない

■ 経済性

・インターネットを安全に利用
・短期間でのシステム導入と容易なシステム構築

■ 高速性

・高速で双方向なリアルタイムデータ通信

IIoTが求めるクラウド

■ 拡張性

・PC１台から大規模システムへの拡張の容易性
・デバイス／フィールドバスへの対応

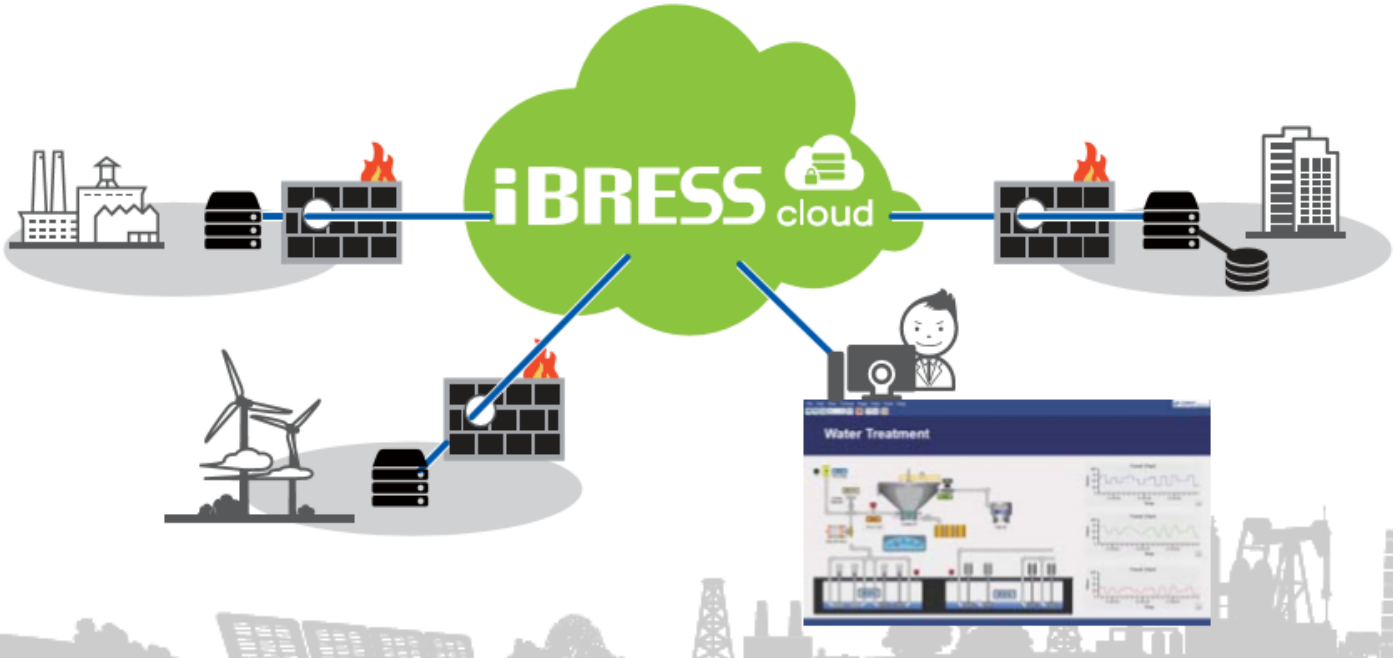
■ 柔軟性

・他クラウドサービス／オンプレ環境／閉域網（専用線）との連携
・容易なHMIの構築

■ 先進性

・OPC-UA 対応
・WebSocket 技術利用

VPNを使わない
安全・高速・双方向可能な
リアルタイムデータ通信



01 安全・高速・双方向通信

Secure Connection Point 1

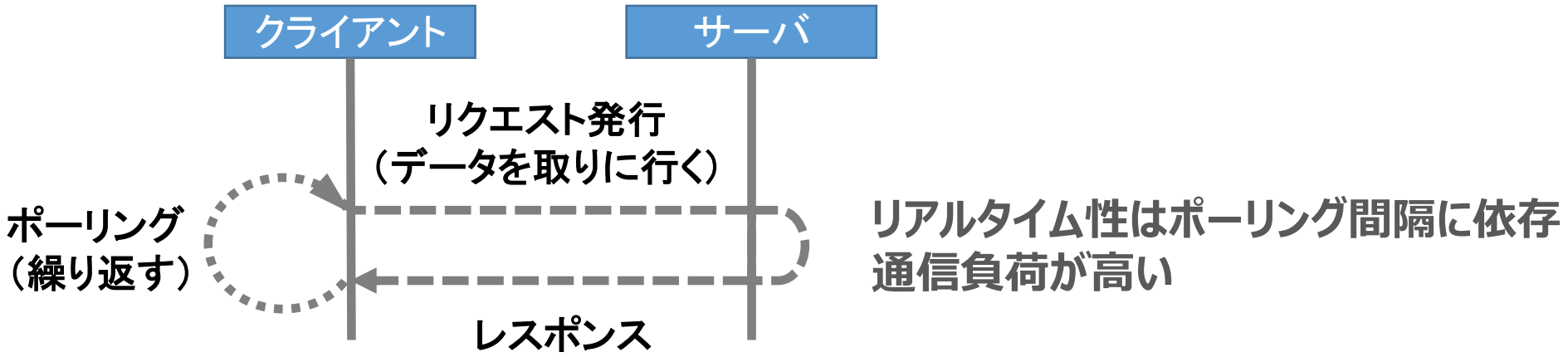
アウトバウンド接続のみの安全設計

Firewall の内側⇒外側へ**WEB接続**が許されるセキュリティポリシーであれば
Firewallの**インバウンドポート**をオープンする必要なくクラウド接続できます
アウトバウンド接続のみのアーキテクチャなので**今よりセキュリティリスクが高まることはありません**

01 安全・高速・双方向通信のひみつ

Secure Connection Point 2

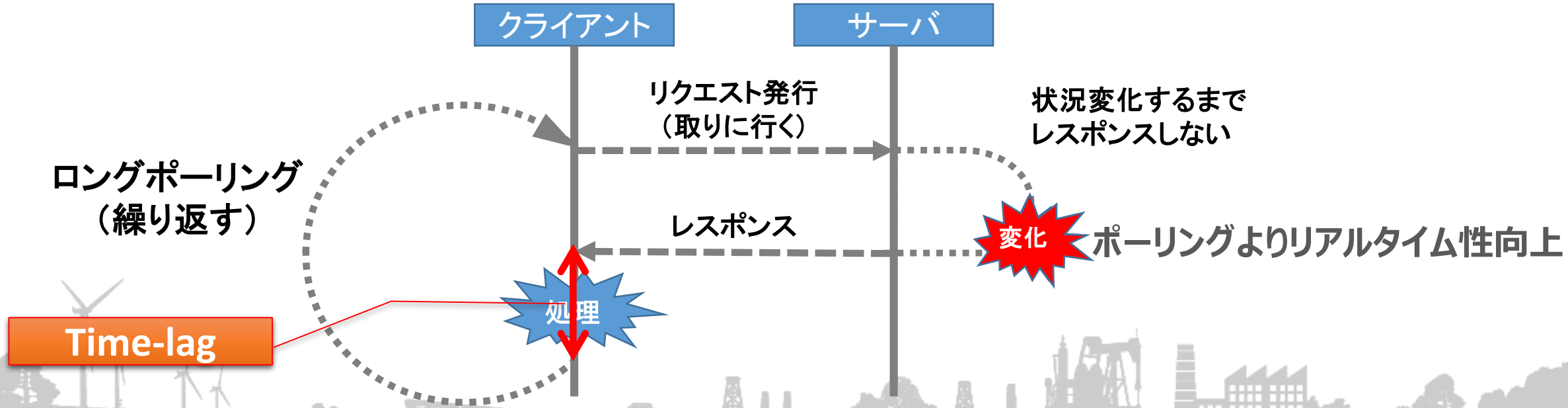
WEB環境での従来型データ取得方式



01 安全・高速・双方向通信のひみつ

Secure Connection Point 2

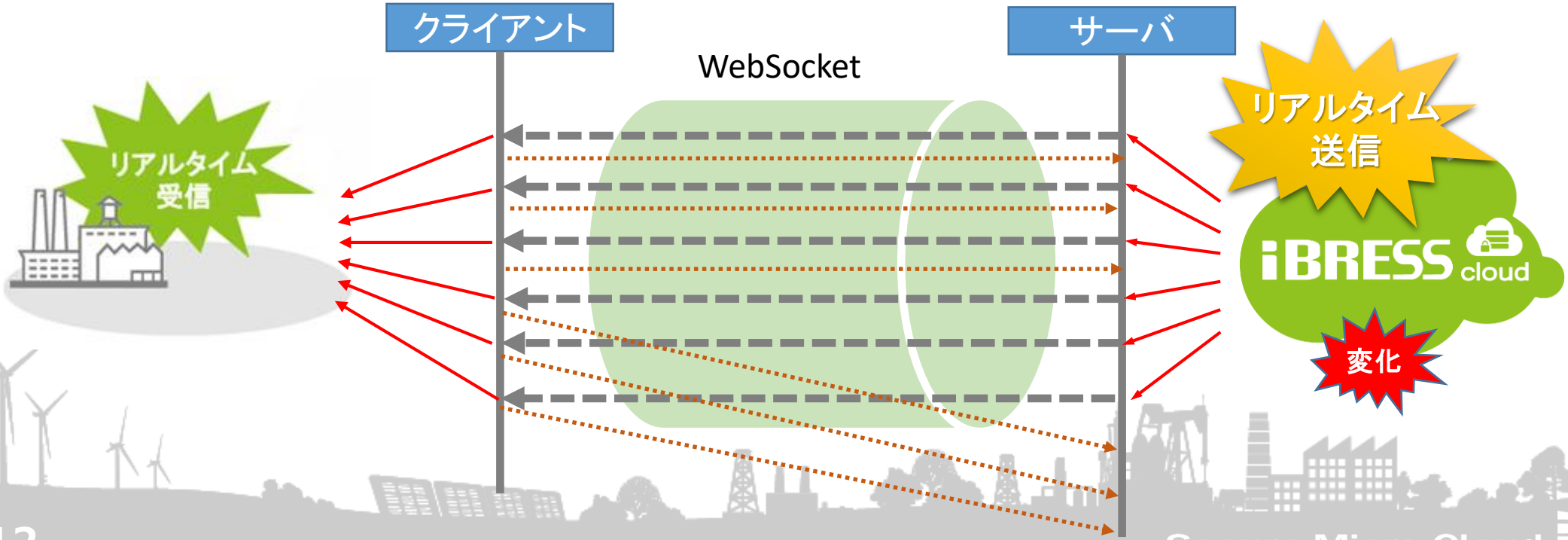
WEB環境での従来型データ取得方式



01 安全・高速・双方向通信のひみつ

Secure Connection Point 2

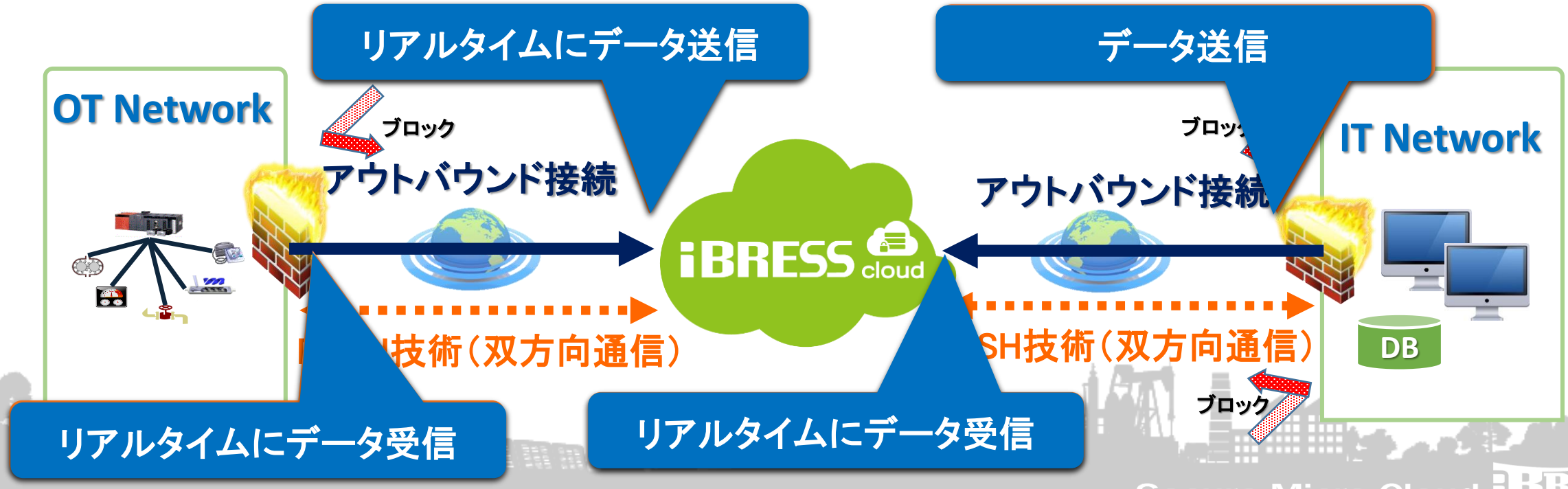
Push技術で高速通信を実現　（RFC6455 — The WebSocket Protocol）



01 安全・高速・双方向通信のひみつ

Secure Connection Point 3

Push技術で双方向通信を実現 （RFC6455 — The WebSocket Protocol）



02 IIoTをクイックスタート！構築リードタイムを大幅短縮

Quick Start Point 1

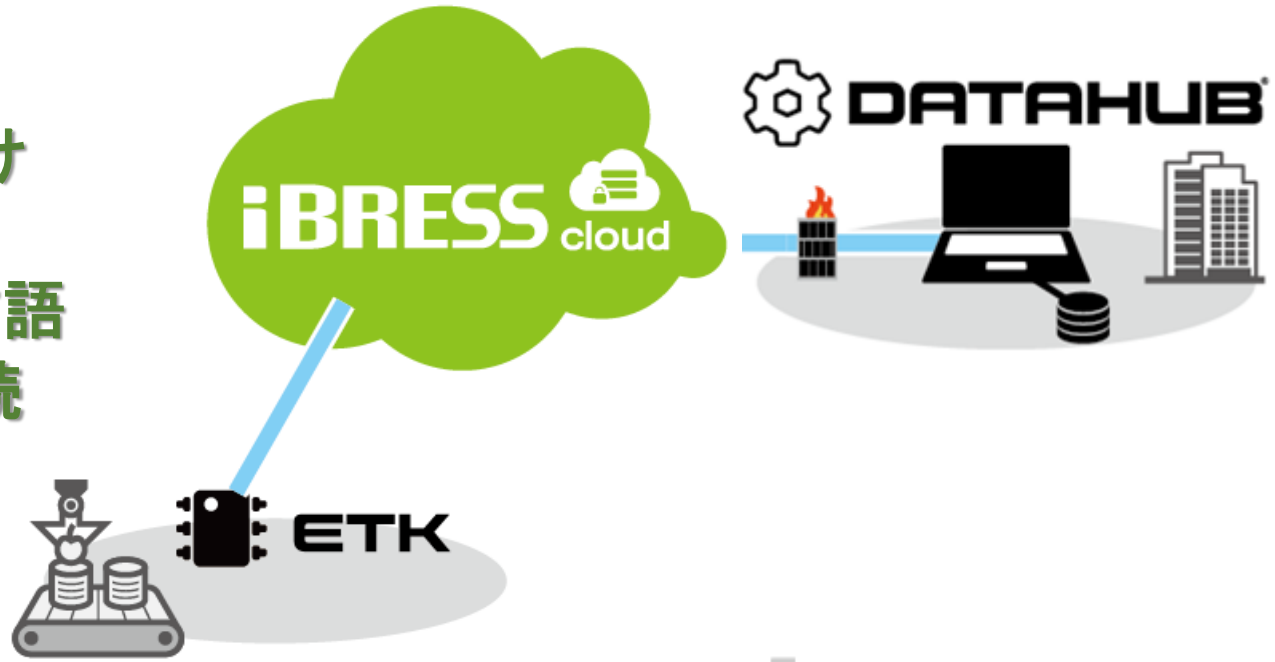
VPNを使用せずWEB技術を用いてインターネット回線を利用

回線工事が必要なく“iBRESS Cloud サービス“は
お申し込み後“数分”で利用可能

02 IIoTをクイックスタート！構築リードタイムを大幅短縮

Quick Start Point 2

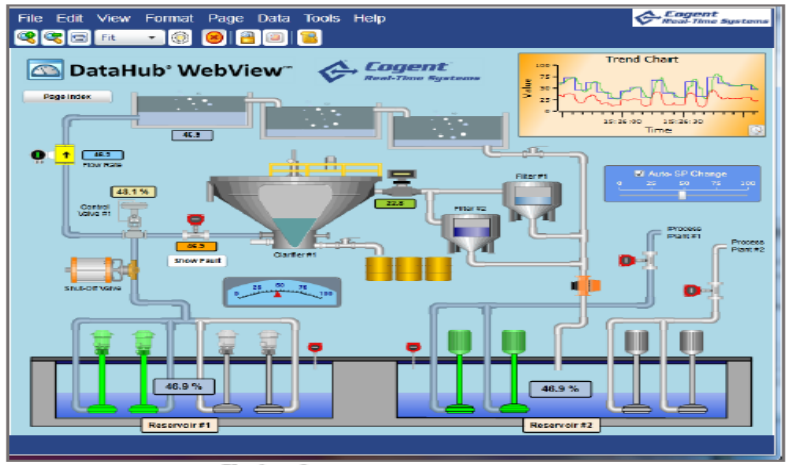
iBRESS Cloudとの接続は、PCにDataHubをインストールするだけで簡単につながります。
組み込み機器との接続はETK（C言語ソース）をインプリメントする事で接続頂けます。

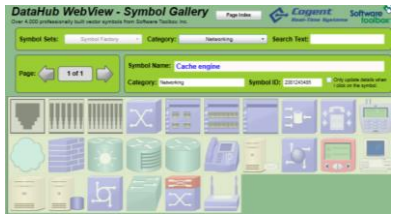


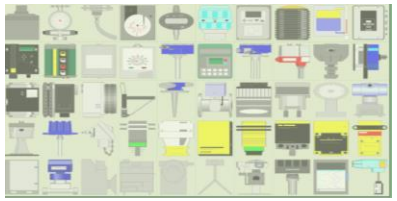
02 IIoTをクイックスタート！構築リードタイムを大幅短縮

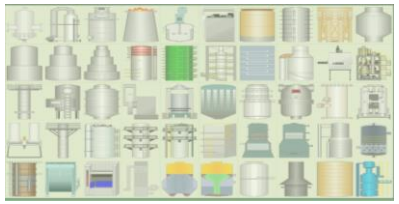
Quick Start Point 3

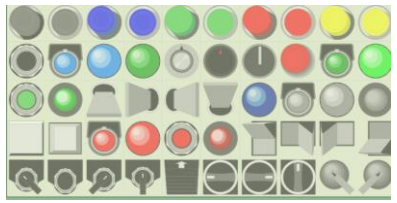
Webブラウザでモニタリング画面作成









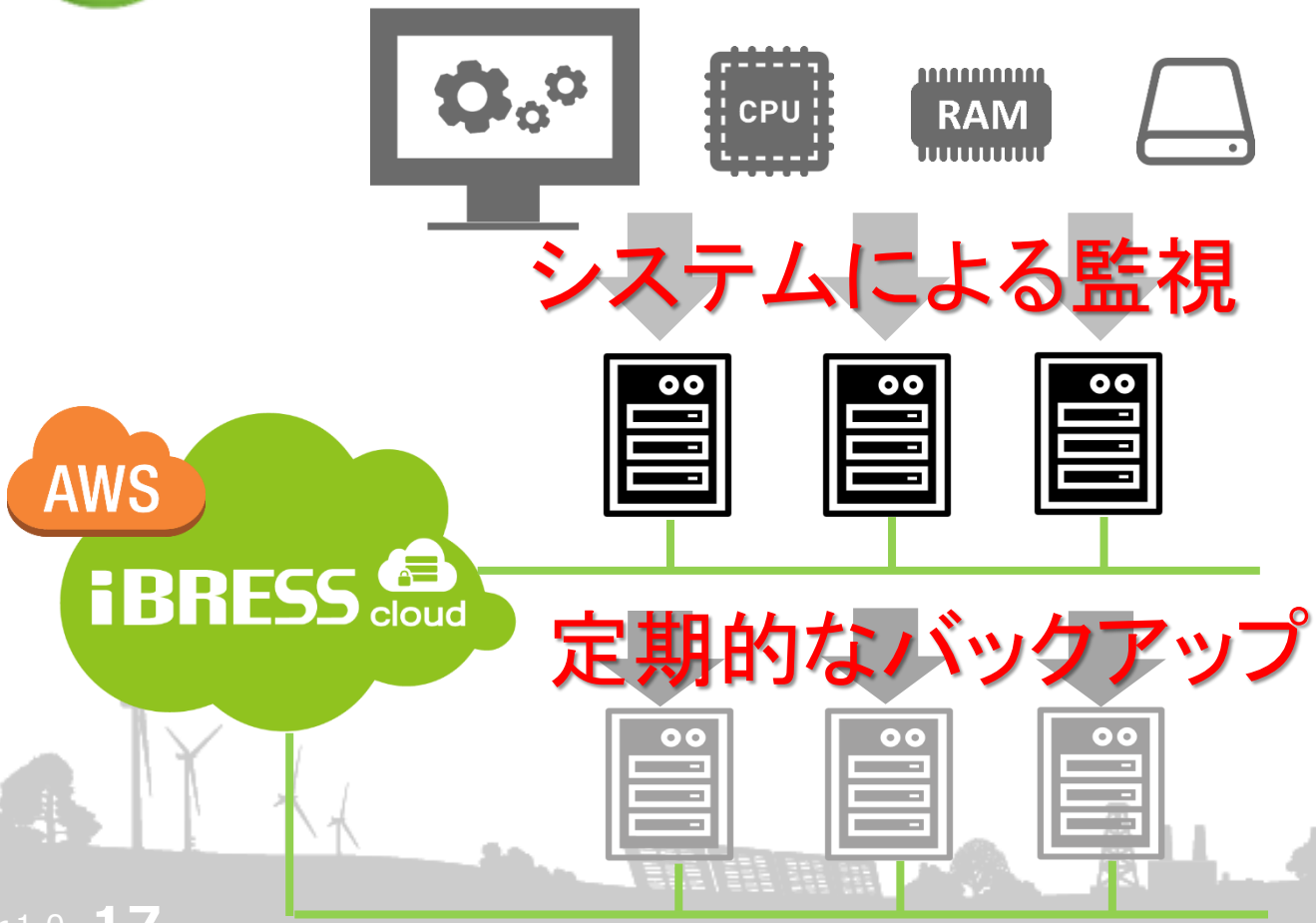


Webブラウザでモニタリング

WEBVIEW

iBRESS cloud

02 信頼のクラウドサービス！

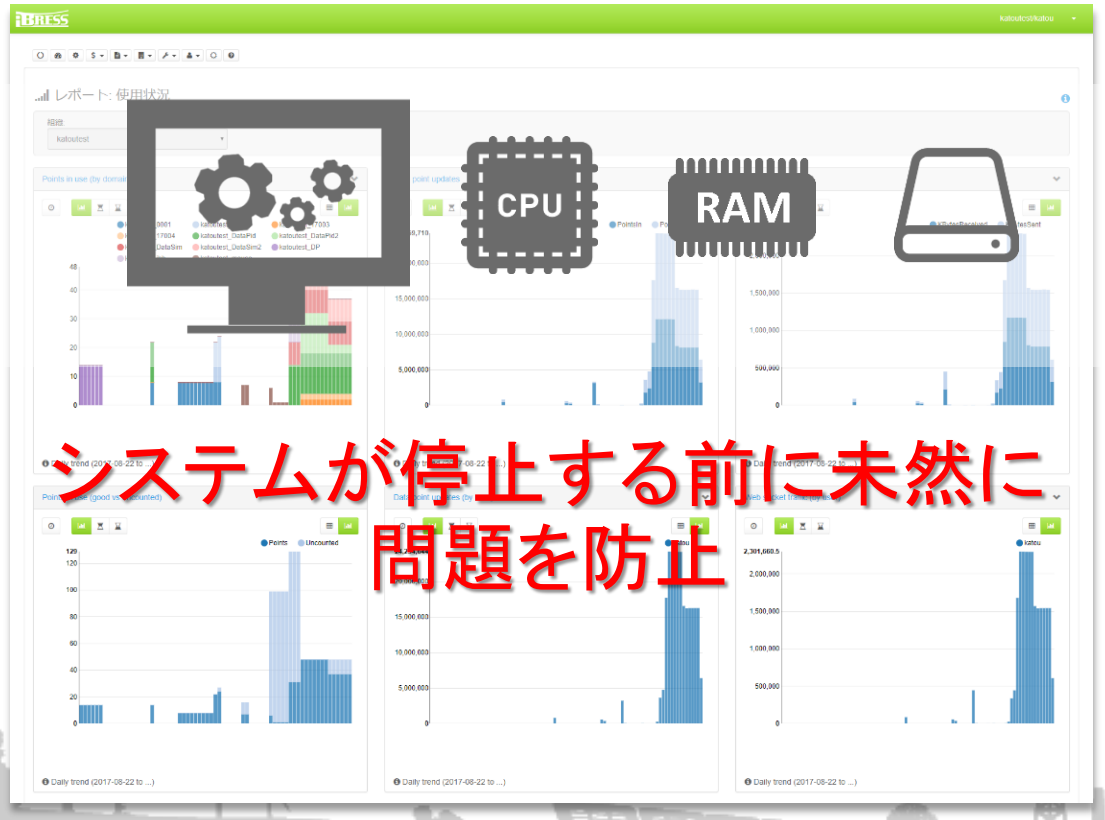


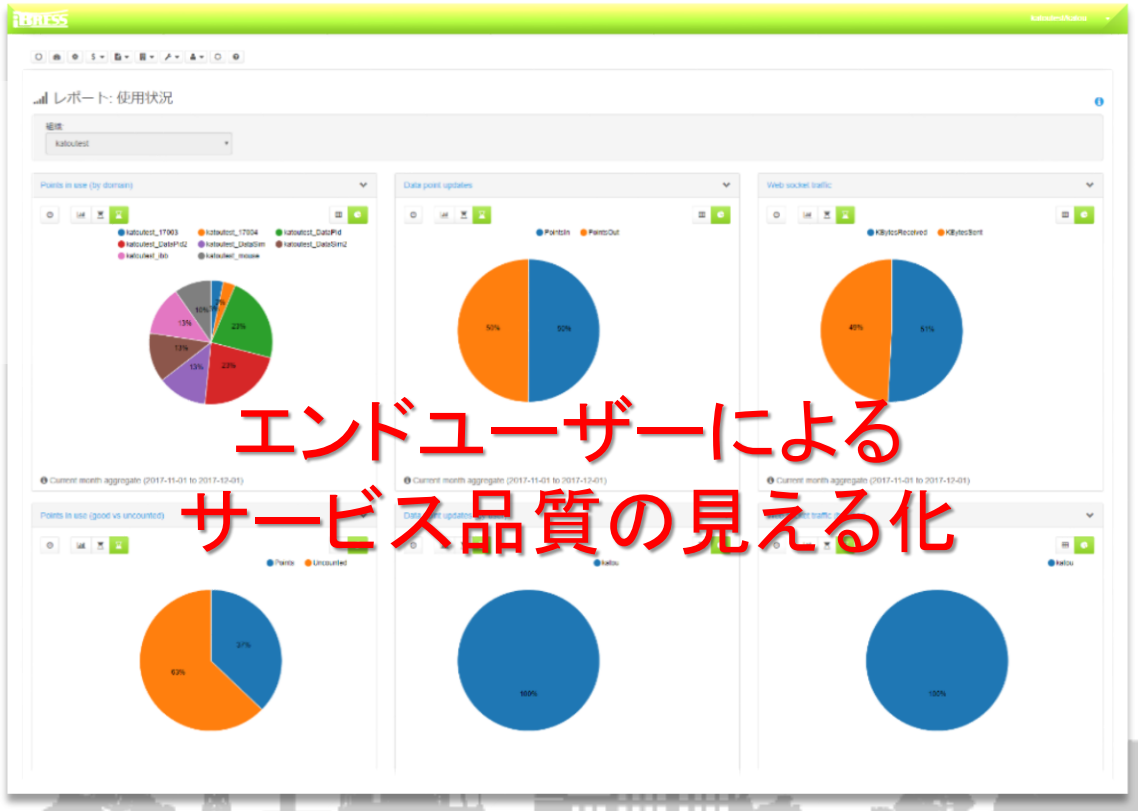
02 信頼のクラウドサービス！

サービスリードタイム
数分
以下
すぐに使える

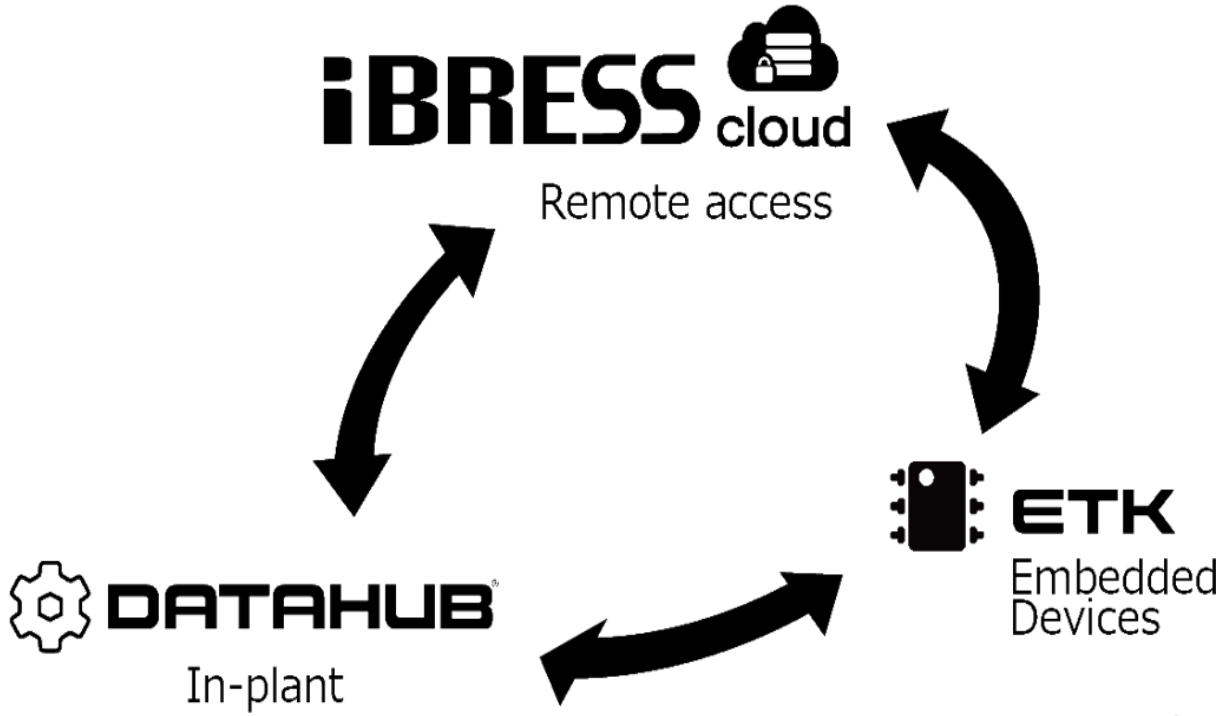
稼働率目標
99.9%
以上
安心して使える

02 信頼のクラウドサービス！





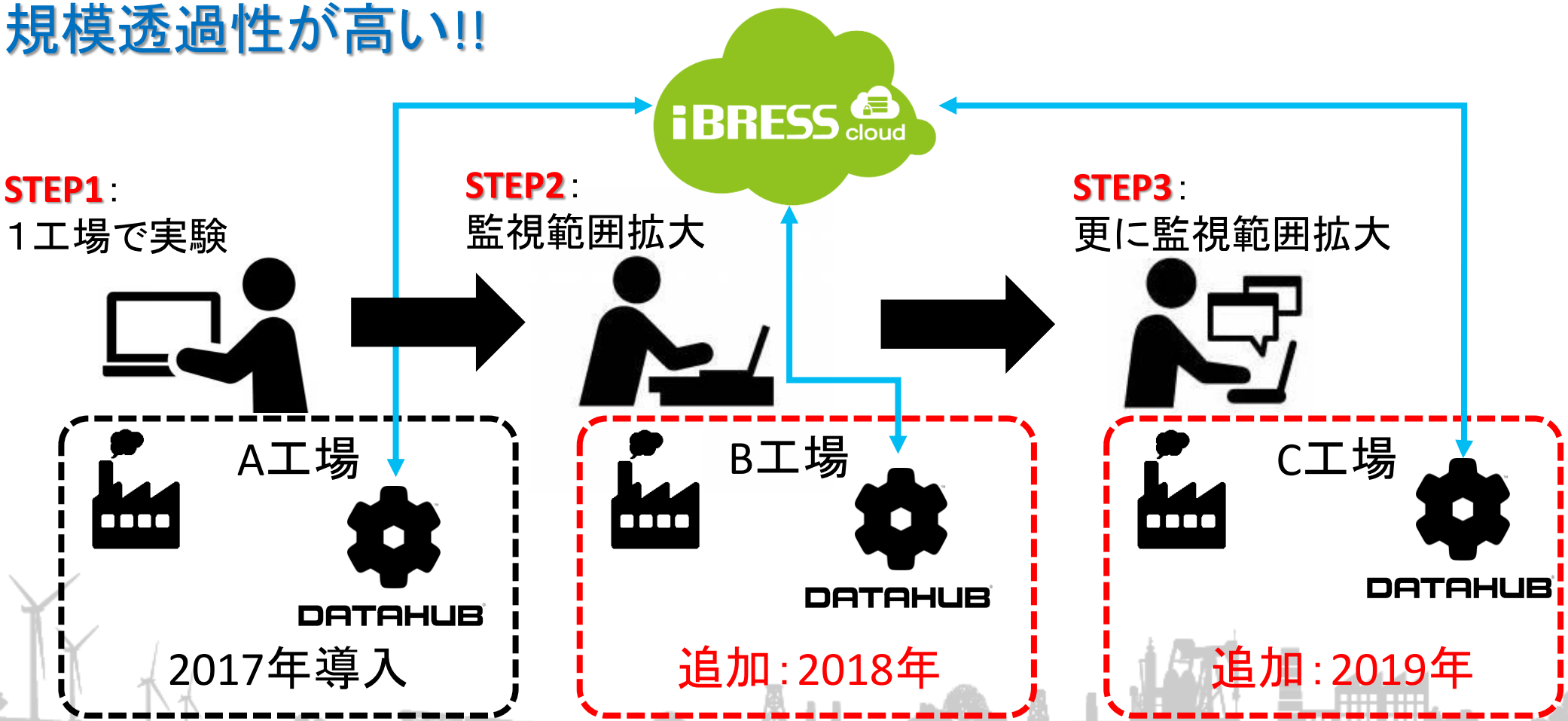
02 非常に Scalability の高いアーキテクチャ



Scalability（拡張性）： Easy approach

iBRESS Cloud + DataHub で拠点の拡大を低コストかつ短期間で実現

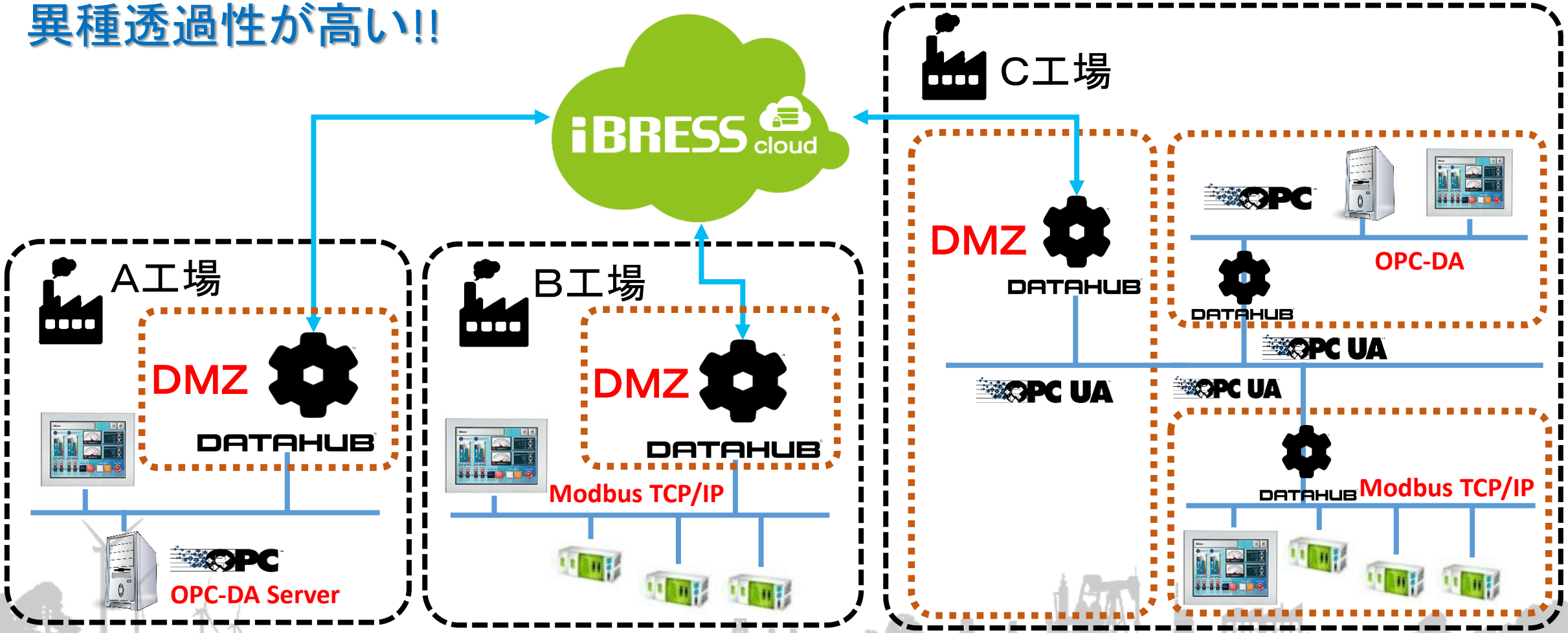
規模透過性が高い!!



Scalability （拡張性） : Protocol conversion

異なるプロトコルを**iBRESS Cloud**は接続（相互変換）できます

異種透過性が高い!!



Scalability （拡張性） : Protocol conversion

NIST（**アメリカ国立標準技術研究所**）

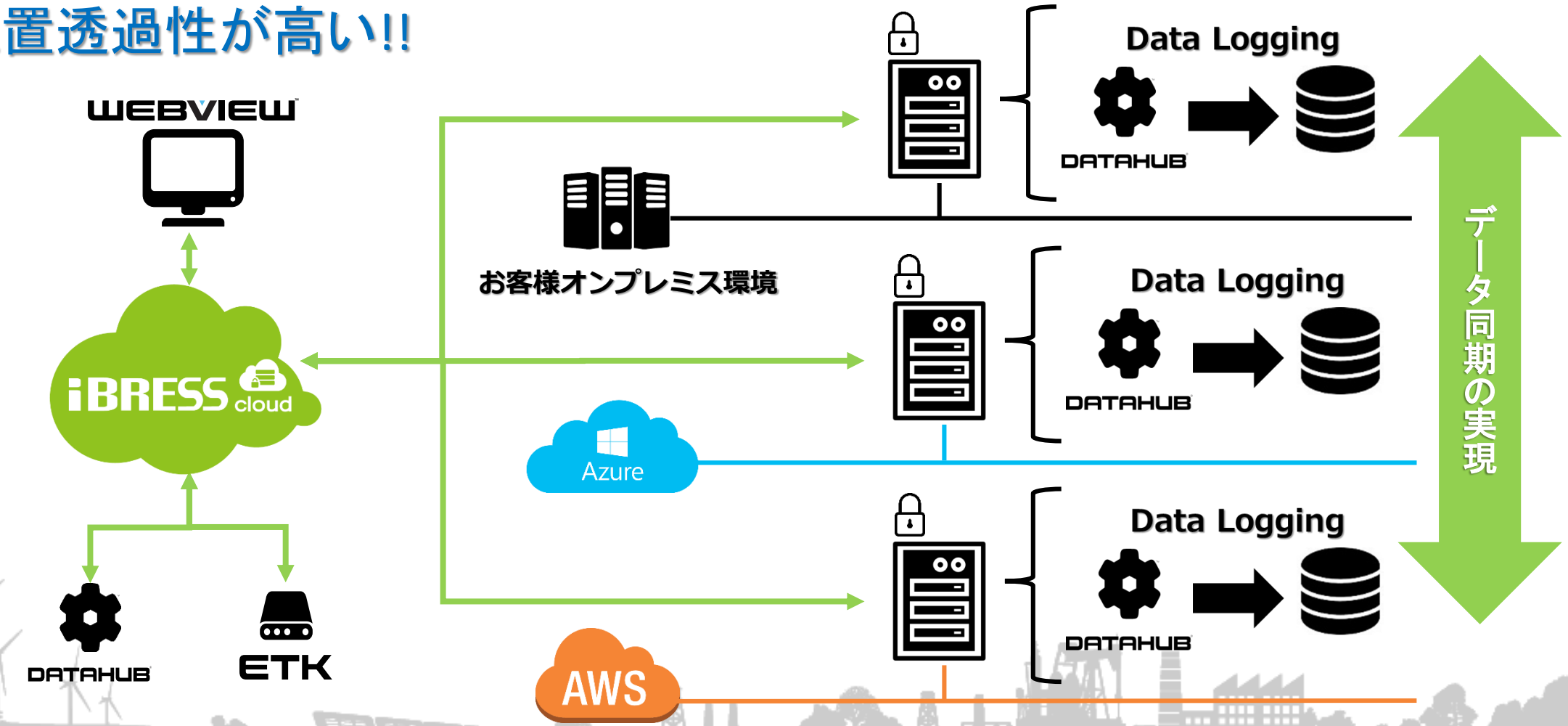
「コンピュータセキュリティ インシデント対応ガイド」
公にアクセス可能なサービスは、安全な非武装地帯(DMZ)ネットワークセグメントに置く。
こうすることで、外部ホストはDMZのホストだけにコネクションを確立でき、内部セグメントのホストにはコネクションを確立できないようにネットワーク境界を設定することができる。

内部ネットワークのすべてのホストでプライベートIPアドレスを使用する。
これにより、アタッカーによる内部ホストへの直接の接続確立が非常に制限される

Scalability （拡張性） : Data logging

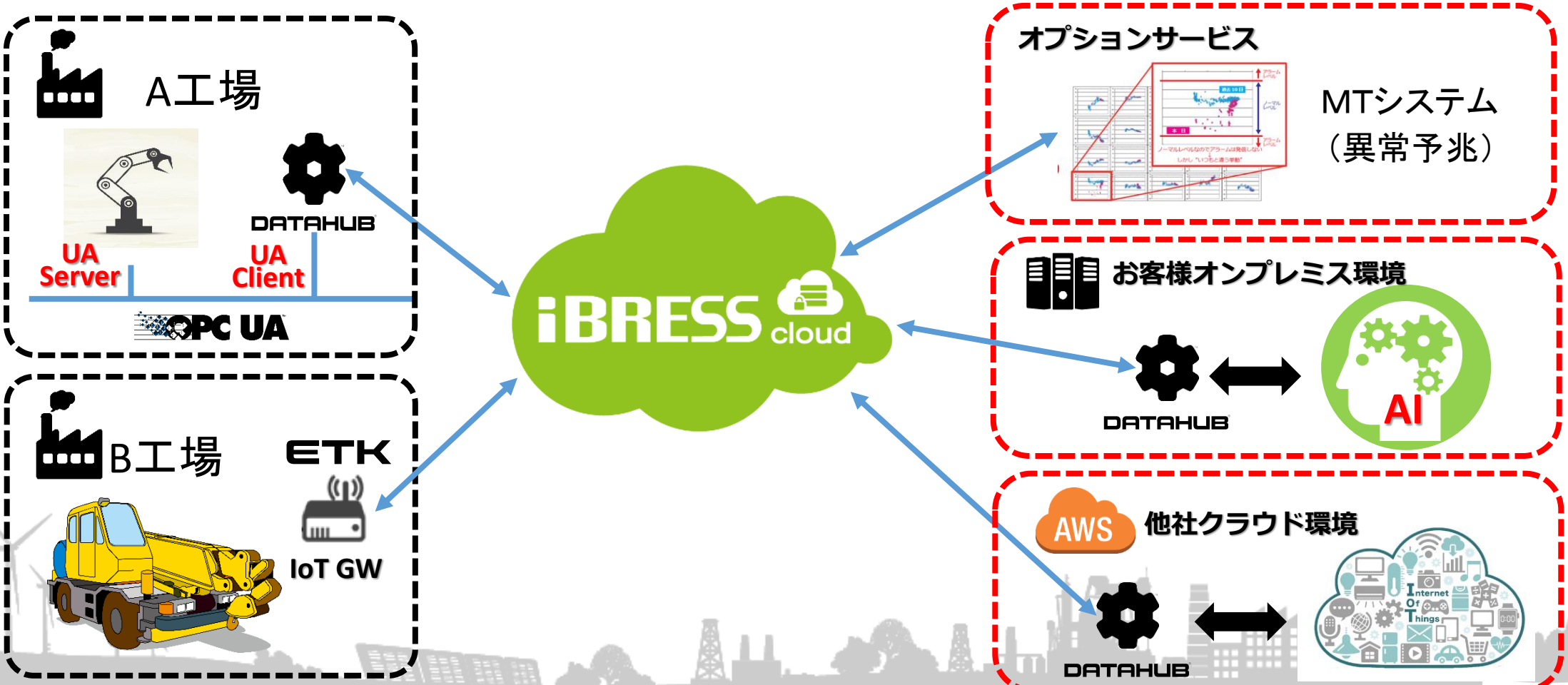
ディザスタリカバリ対応も低予算で実現 （異なるプラットホームを同じ使い勝手で利用）

位置透過性が高い!!



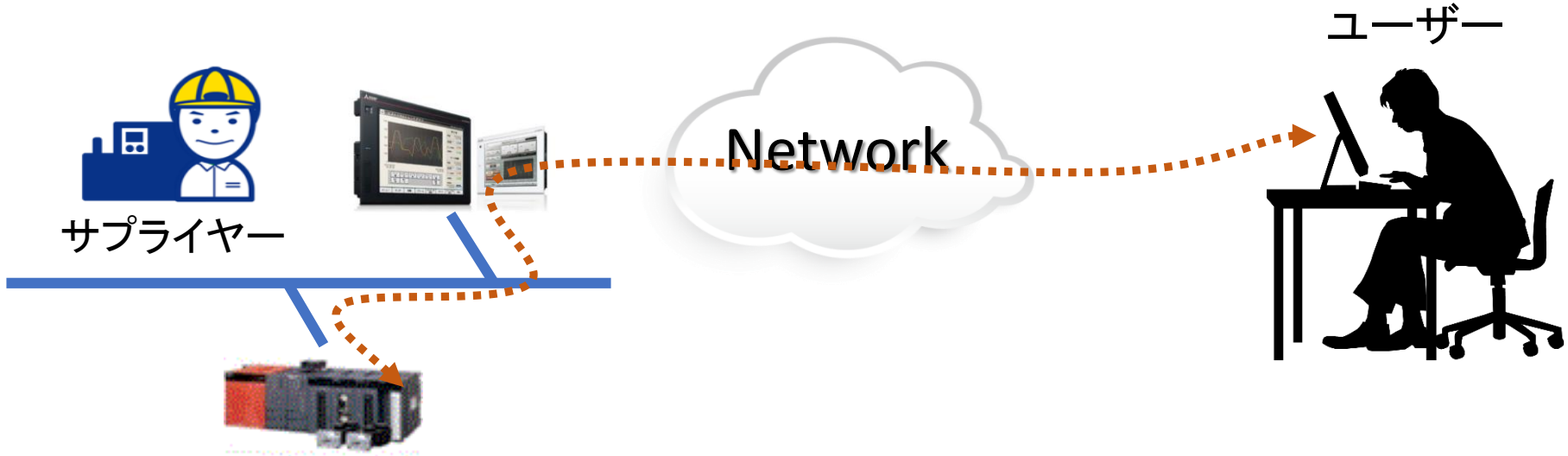
Scalability（拡張性）： Custom

iBRESS Cloud + DataHub +ETKでAIと接続するなどが可能となります
DataHubで機能拡張が可能なため、初期導入リスクが軽減されます



参考事例

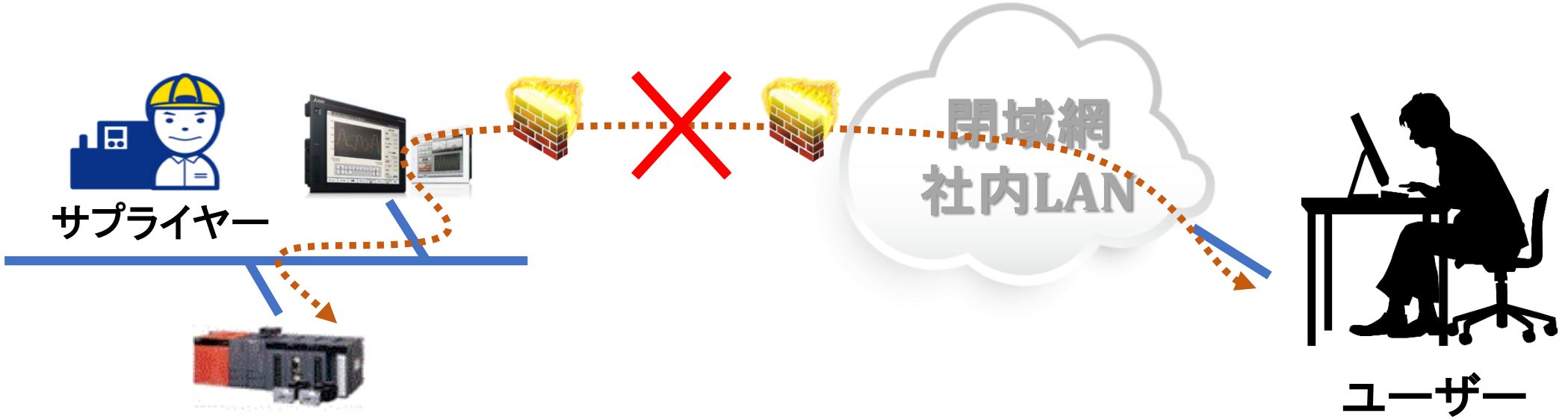
ユーザー側PCでサプライヤのPLCを遠隔監視／制御したい



データ収集を毎秒 アナログ XXX点 デジタルXXX点 行う

Security（安全性）

ユーザーの閉域網にサプライヤを接続する



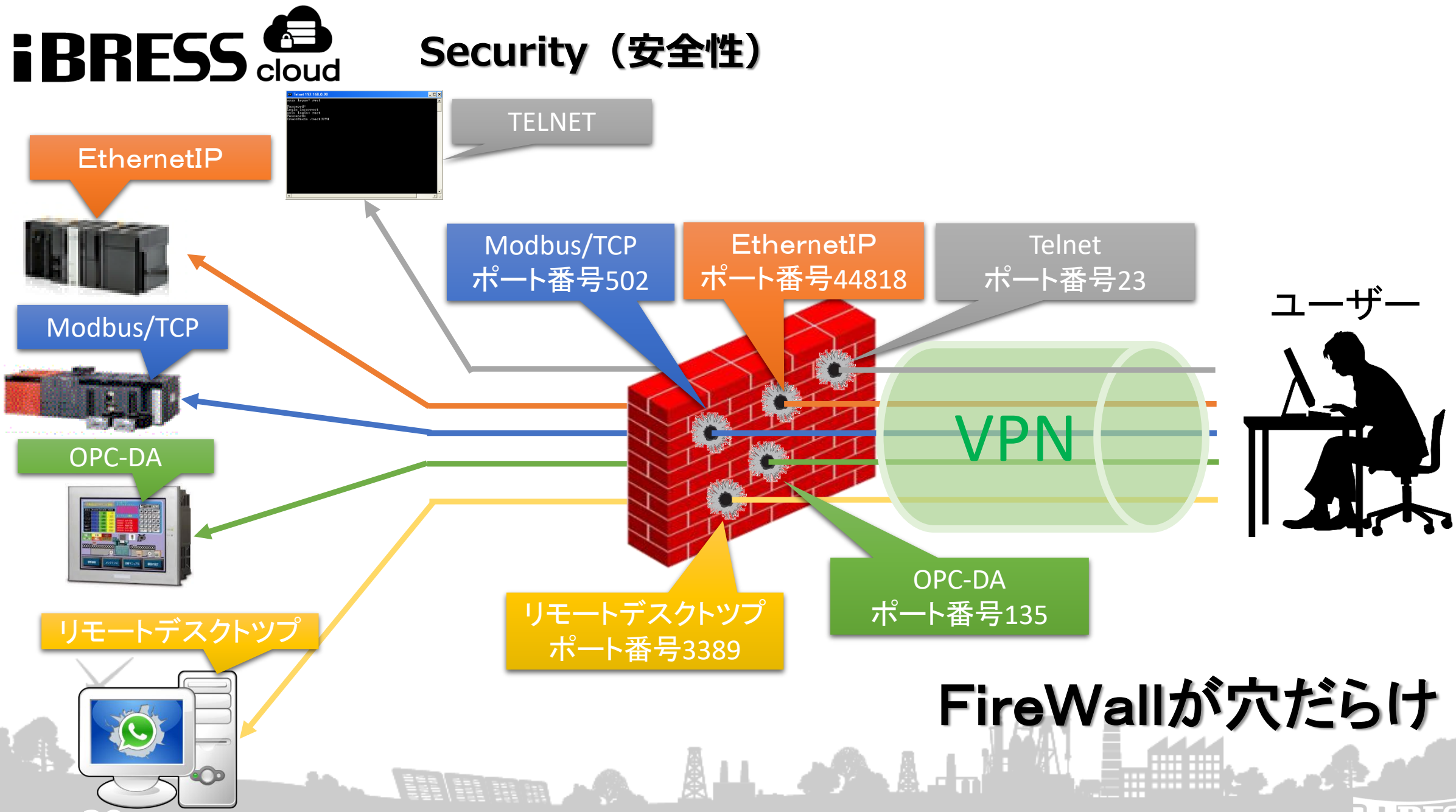
ユーザー側のネットワーク管理者が絶対に許さない

Security（安全性）

インターネットVPNでサプライヤとユーザを接続

FireWallポートのオープンが必要

Security（安全性）



FireWallが穴だらけ

Security（安全性）

ウェルノウンポート

TCP/IPによる通信で利用されるTCPやUDPのポート番号のうち、
著名なサービスやプロトコルが利用するために予約されている0番から1023番のポート番号　（一部抜粋）

ポート番号	TCP/UDP	サービス/プロトコル	ポート番号	TCP/UDP	サービス/プロトコル
20	TCP	FTP (File Transfer Protocol) (データ)	109	TCP	POP2 (Post Office Protocol version 2)
21	TCP	FTP (File Transfer Protocol) (制御)	110	TCP	POP3 (Post Office Protocol version 3)
22	TCP/UDP	ssh (secure shell)	113	UDP	Ident
23	TCP	Telnet	119	TCP	NNTP (Network News Transfer Protocol)
25	TCP/UDP	SMTP (Simple Mail Transfer Protocol)	123	UDP	NTP (Network Time Protocol)
42	TCP/UDP	WINS (Windows Internet Name Service)	135	TCP	Microsoft RPC (Remote Procedure Call)
43	TCP	WHOIS	137	TCP/UDP	NetBIOS (名前解決)
53	TCP/UDP	DNS (Domain Name System)	138	TCP/UDP	NetBIOS (データ転送)
67	UDP	BOOTP (Bootstrap Protocol) (サーバ)	139	TCP/UDP	NetBIOS (セッション制御)
68	UDP	BOOTP (Bootstrap Protocol) (クライアント)	143	TCP/UDP	IMAP2/4 (Internet Message Access Protocol version 2/4)
69	UDP	TFTP (Trivial File Transfer Protocol)	161	TCP/UDP	SNMP (Simple Network Management Protocol)
80	TCP/UDP	HTTP (Hypertext Transfer Protocol)	162	TCP/UDP	SNMP (Simple Network Management Protocol) (トラップ)
88	TCP/UDP	Kerberos	443	TCP/UDP	HTTPS (HTTP over SSL/TLS)

登録済みポート番号 (1024–49151)
OPC-UA:4840,Modbus/TCP:502, Omron FINS:9600, Microsoft Terminal Server (RDP):3389　など

IANA（アイアナ）
インターネットに関連する番号を管理する組織。IPアドレス・ドメイン名・ポート番号等の標準化・割り当て・管理を行う

Security（安全性）

INTERNET Watch
セキュリティ | LAN機器 | ストレージ | ビジネスソフト | 会計・業務ソフト | 教育/子ども
IoT | 仕事/ビジネス | サービス | ソフトウェア | 通信 | 業界動向 | イベント | ネッ

ニュース

IoT機器がマルウェアに感染する元凶は「Telnet」～横浜国大・吉岡克成准教授

岩崎 宰守　2017年3月3日 17:36

ツイート リスト　いいね！ 520　シェア　B! 67　Pocket 109

IoT機器を含むホームネットワーク向けのセキュリティ製品「Bitdefender Box」の製品発表会において、横浜国立大学大学院環境情報研究院／先端科学高等研究院准教授の吉岡克成氏が「IoT機器を狙ったサイバー攻撃の最新事情」のテーマで講演を行った。

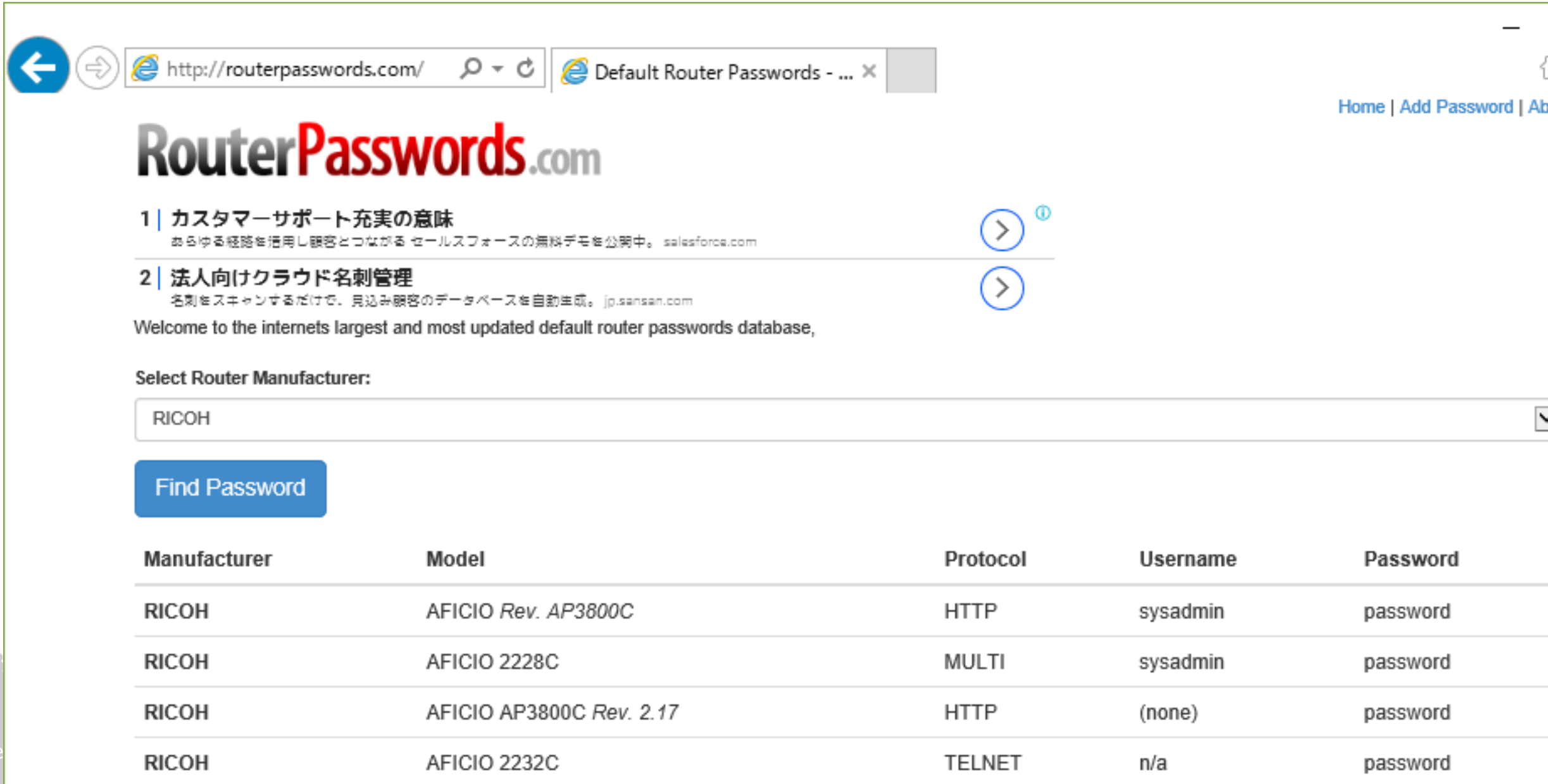
横浜国大では、マルウェアに感染したIoT機器の観測を行っている。このシステムで観測し、確認した機器は、2016年1～6月に500種類以上・60万台にも達するという。

IoT機器の多くは、組み込み型のLinuxで動作しており、Telnetが利用できるとうたわれていなくとも、実際には利用できる製品がほとんどを占めている。

認証を含むすべての通信を暗号化せずに平文で送信する仕様のため、セキュリティ面で問題があり

Telnetでは、簡単なIDとパスワードで管理者権限でログインでき、機器を操作できてしまう。こうした機器にデフォルトで設定されているIDとパスワードのリストは、「Googleで検索すると簡単に入手できる」ので、スーパーハッカーでなくても誰でも（IoT機器に）侵入できてしまう」のが現状だ。

Security（安全性）



Manufacturer	Model	Protocol	Username	Password
RICOH	AFICIO *Rev. AP3800C*	HTTP	sysadmin	password
RICOH	AFICIO 2228C	MULTI	sysadmin	password
RICOH	AFICIO AP3800C *Rev. 2.17*	HTTP	(none)	password
RICOH	AFICIO 2232C	TELNET	n/a	password

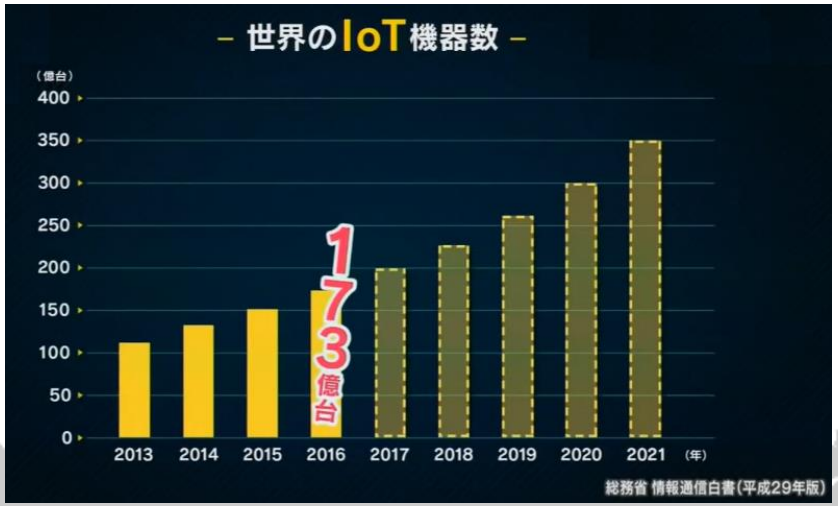
Security（安全性）

【NHKスペシャル】家電を狙うインターネット脅威！カメラ・レコーダー・医療機器など！

2017/11/26 パソコン

2017年11月26日放送「NHKスペシャル」の『あなたの家電が狙われている～インターネットの新たな脅威～』で、最新家電を狙う新手サイバー攻撃の脅威が紹介されました。インターネットに繋がったIoT機器を狙った、盗み見・悪用・攻撃などの新たな脅威は必見です。

画像出典：*Amazon*



insecam(インセカム)
世界中に設置されたセキュリティの甘い監視カメラ
無料で見ることができるサイトです。

https://www.insecam.org/en/bycountry/JP/?page=260

Watch live surveillance onli...

Insecam **Most popular** Manufacturers Countries Places Cities Timezones New online cameras FAQ Contacts

Google Custom Search

初期設定のままの監視カメラは
Insecamに公開されます

IP cameras: Japan

Facebook Twitter More

« 1 ... 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 »

Watch Panasonic camera in Japan,Nagano

Watch Panasonic camera in Japan,Nagano

Watch Panasonic camera in Japan,Tokyo

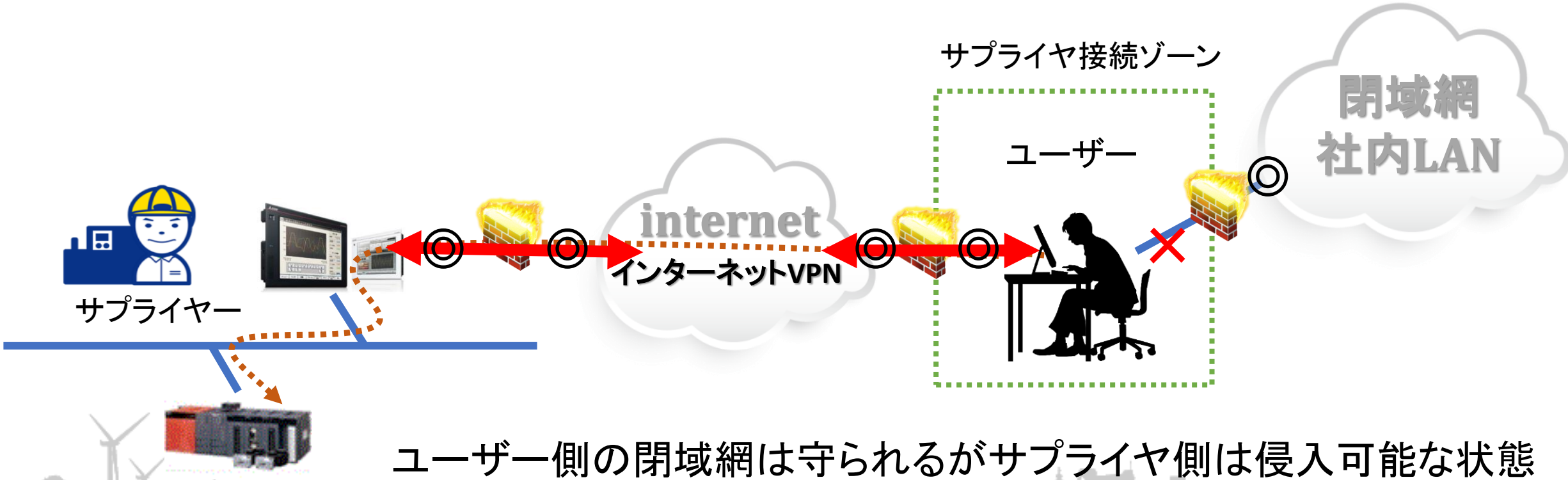
Watch Panasonic camera in Japan,Yamaguchi

Watch Panasonic camera in Japan,Tokyo

Watch Panasonic camera in Japan,Tokyo

Security（安全性）

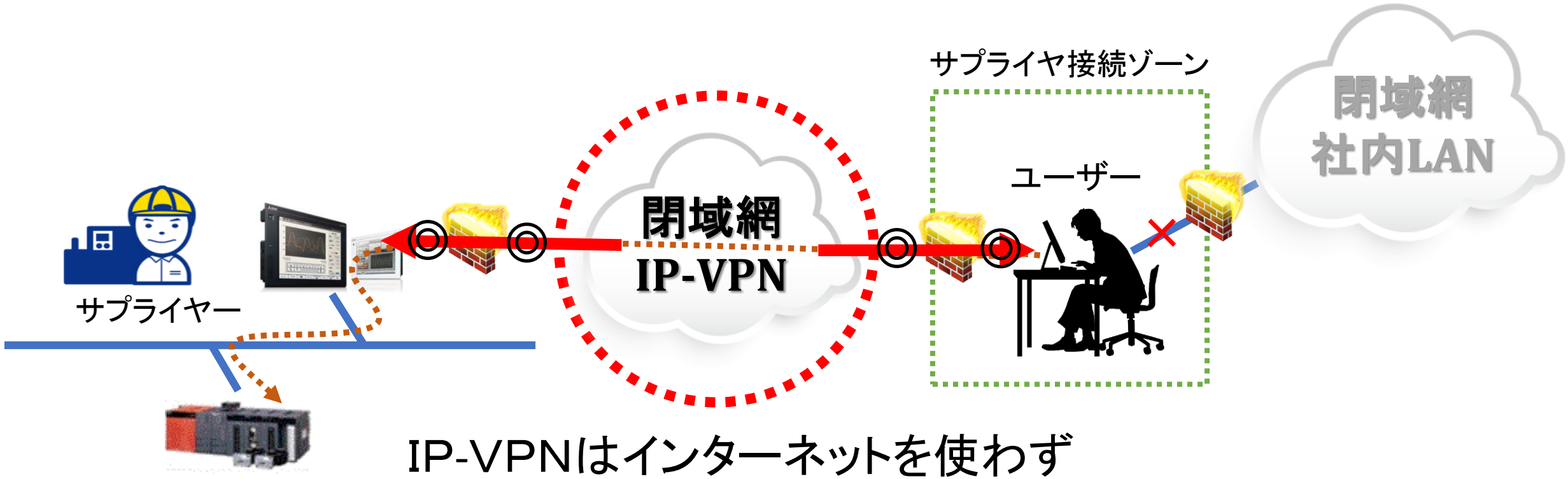
ユーザ側のDMZの内側にサプライヤ接続用ゾーンを作る



ユーザー側の閉域網は守られるがサプライヤ側は侵入可能な状態

Security（安全性）

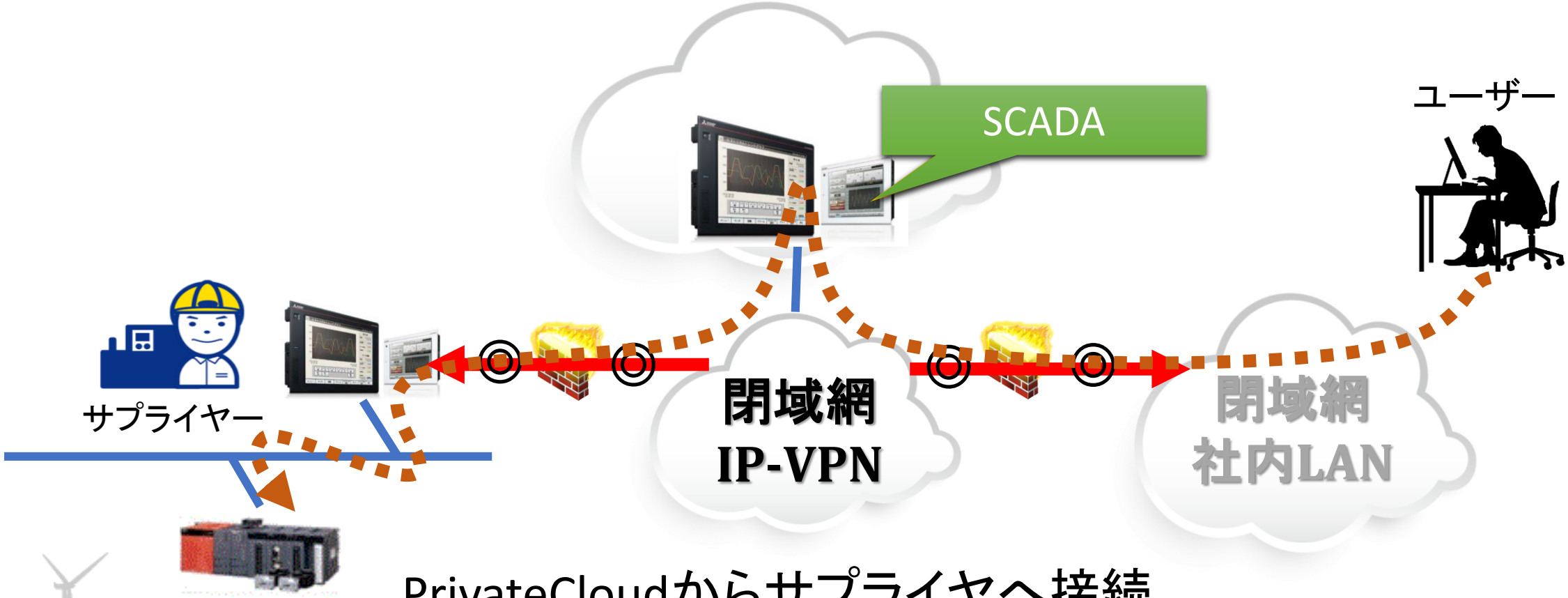
IP-VPNでサプライヤとユーザを接続



IP-VPNはインターネットを使わず
回線の秘匿性や帯域を回線業者が保証
構成的にはインターネットVPNと同様

Security（安全性）

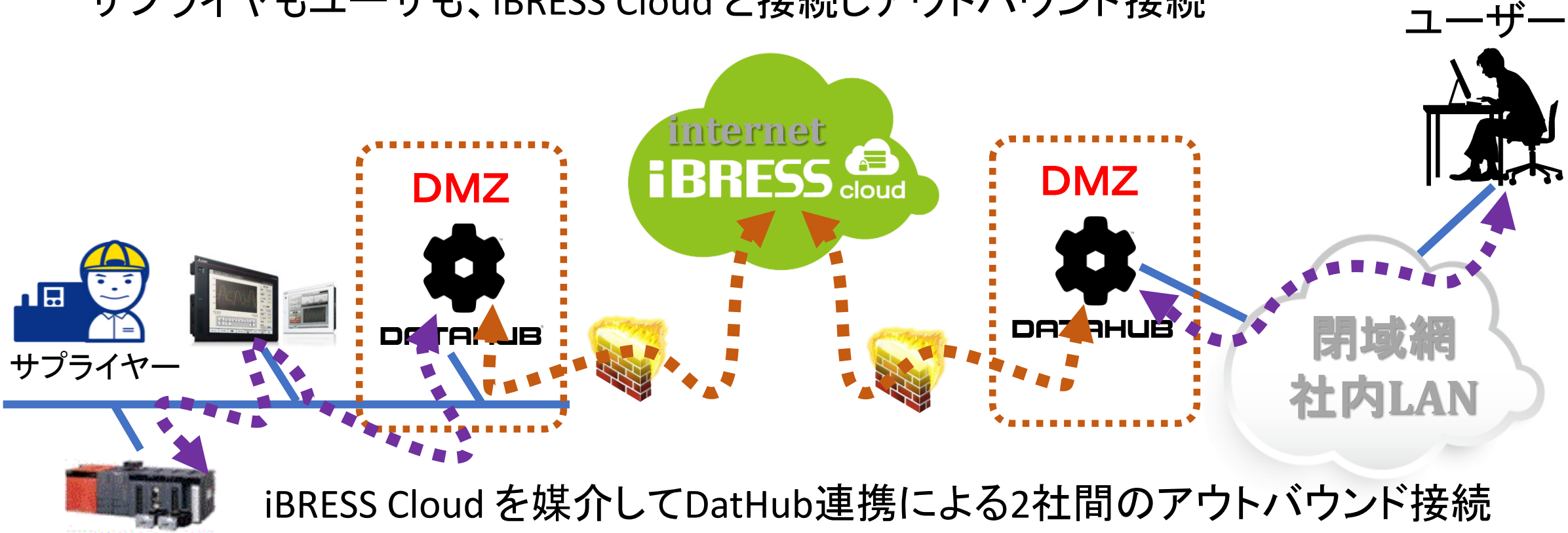
ユーザーとサプライヤだけが利用可能なPrivateCloud 空間を作る



PrivateCloudからサプライヤへ接続
SCADAソフトをPrivaetCloudに導入する事でも可能

Security（安全性）

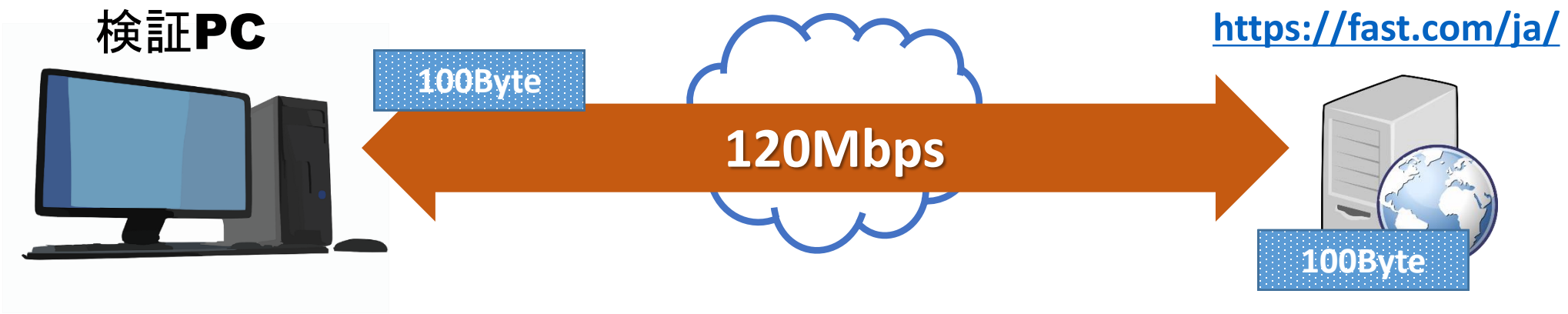
サプライヤもユーザも、iBRESS Cloud と接続しアウトバウンド接続



iBRESS Cloud を媒介してDatHub連携による2社間のアウトバウンド接続
ユーザーは自社内のDataHubに指示データ入力
サプライヤは自社内のDataHubの指示データを取り込んで処理
ユーザ、サプライヤ共にDataHubによってネットワークを分離

パフォーマンス

検証環境



プロセッサ：Intel® Core™ i7-6800K @ 3.40GHz 3.40GHz
RAM：32.0GB
OS：Windows10 Education 64bit
OSバージョン：1709
OSビルド：16299.64

10,000 送受信の時間測定

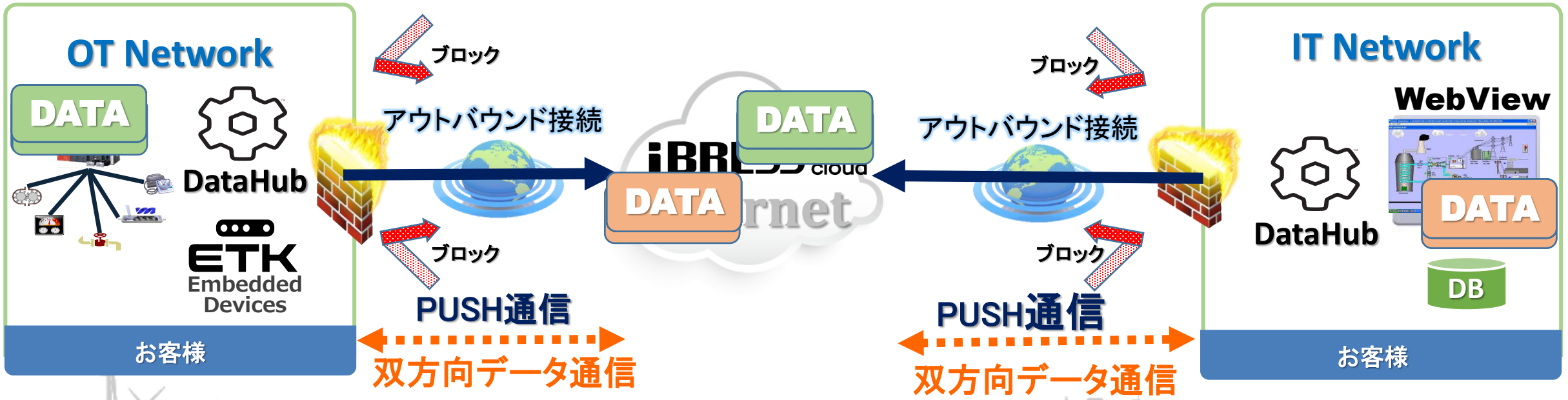
パフォーマンス

iBRESS cloud

プロトコル	1回目		2回目		3回目		平均	
	計測時間	送受信 / 秒	計測時間	送受信 / 秒	計測時間	送受信 / 秒	計測時間	送受信/秒
WebSockets	13.197	約757 /秒	13.091	763 /秒	12.982	約770 /秒	13.09	約763 /秒

Summary

ネットワークを共有するのではなく
データを共有するセキュアな仕組みです



iBRESS cloud

ご清聴ありがとうございました。

CONNECT DIFFERENTLY