<ホワイトペーパ>

**株式会社テリロジー**


# Airwall™とは

Tempered Networks は更なる市場での課題に寄り添ってビジネス拡大を図るため、2019 年 11 月に製品名を従来の「HIP services」から「Airwall Edge Services」に変更した。産業系分野では長期にわたり、外部からのセキュリティ脅威をシャットアウトするため閉域網ネットワークで構築されてきた”**AirGap（エアギャップ**”の世界と呼ばれている。最近では、デジタルトランスフォーメーション(DX)が普及し始め、IT/OT 融合で生産設備の稼働状況、産業制御システムの異常通知等を社内情報システムとかクラウドで集約管理する動きが出てきた。そして、IT/OT 環境を分離するためにその境界線上に Firewall を設置したり、産業制御システムの多層防御として DMZ でセグメント化する産業系企業も増えてきた。一般的に、Firewall は企業ネットワークエッジに設置して、ネットワークの North-South トラフィックのセキュリティ脅威を防御するものが殆どで、企業内の East-West トラフィックセグメントを守るものではなかった。

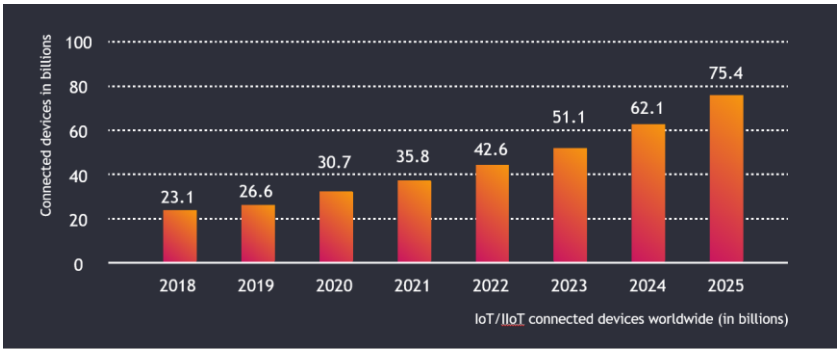
Tempered Networks はこうしたネットワークセキュリティ課題を解決するソリューションを展開。上記で述べた AirGap と Firewall というそれぞれの利点を組み合わせて Airwall と新しいソリューション名に改名した。

Airwall 中核の HIP オーバーレイは ID(Identification：利用者識別)の強力な概念に基づいてきわめて高度なセキュリティを担保する技術で、2015 年に IETF 承認の HIP(Host Identity Protocol)をベースにしている。

Airwall アーキテクチャは、各製品モデルの **Airwall edge services** で構成される暗号化ネットワークファブリック。**Airwall Conductor** と呼ばれるオーケストレーションエンジンにより、“**ハブアンドスポークトポロジー**”、メッシュのトポロジーで“**守りたい**”セグメント間をオーバーレイで通信するしくみである。これは従来の HIP ソリューション“HIP services”製品と何ら変わるものではない。（注）**ハブ アンド スポーク**は、一般的な通信またはセキュリティ要件をより効率的に管理するためのネットワーク モデル。

## “Everything is connected”

以下グラフ表示は驚異的な数字を示している。上記でも述べたが DX は今後 IoT/IIoT の投入がきっかけに益々拡大が予想される。この数字はアプリケーションにアクセスするエンドユーザ数ではなく、ネットワーク接続のデバイスの数である。特に、OT デバイスはセキュリティパッチが当てられないためきわめて脆弱で、セキュリティ保護は困難。




## Airwall Edge Services

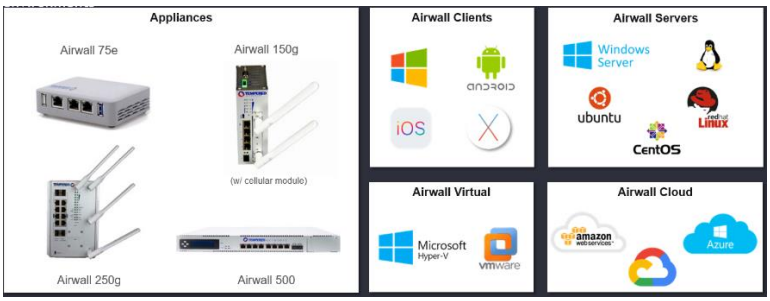
### 特徴

- “クローク インフラ”：“ハッカーは見えないものをハッキングできない”
- East-West ネットワークセグメントのマルウェア感染伝播を排除
- 物理、仮想、クラウド（AWS,Azure,Google）のインフラ全体でセキュリティポリシーを統合
- 信頼できる ID で、すべてのセキュアなネットワーク接続を認証および暗号化

### 導入メリット

- 各拠点サイト設置での Airwall 製品のセキュリティポリシーはセンター側の Airwall conductor で一元的に設定および管理出来る
- ネットワークセグメントの攻撃対象領域を大幅に削減出来る
- レガシーソリューションよりも低コストで容易にかつ短期間で設定導入が出来る

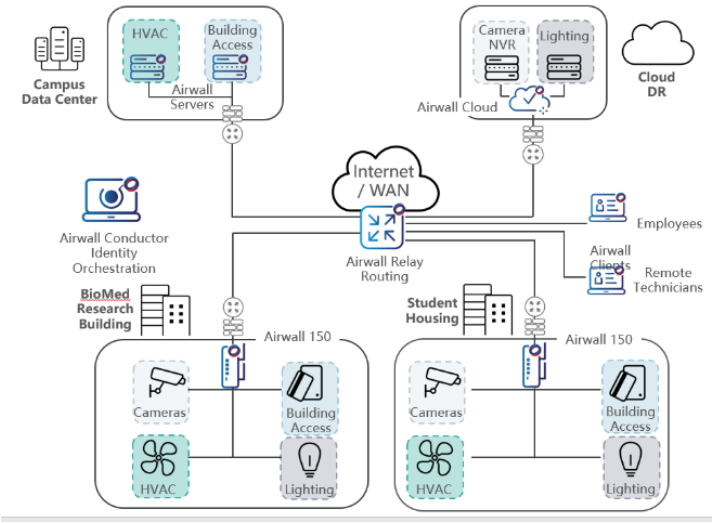
## Airwall Edge Services



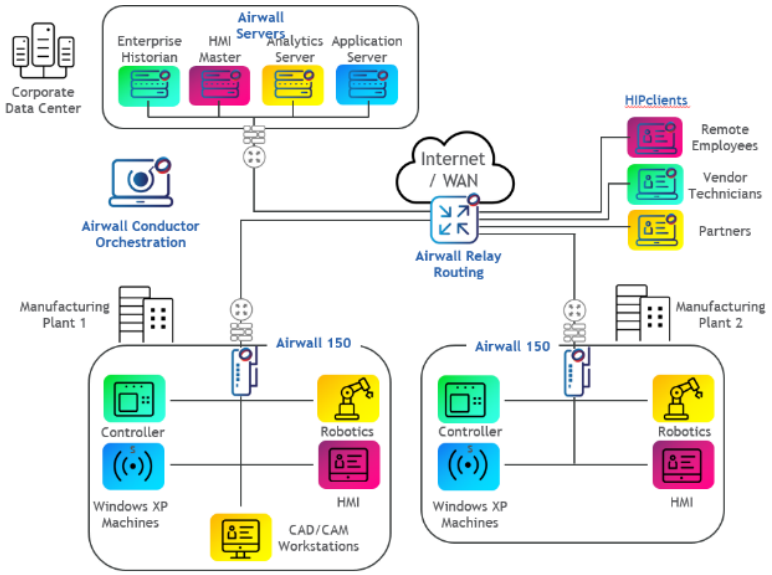
## ＜Airwall Edge Services の Use Case＞

### BAS(ビルオートメーションシステム)

ペンシルベニア州立大学(PSU)はマイクロセグメンテーション化を実現。640 以上のキャンパスビルでビルオートメーションシステムをネットワーク隔離し、クローキングを実施した。限られた人的リソースと短い作業期間で、PSU は共有キャンパスネットワーク上で細分化された暗号化オーバーレイセグメントを構築。PSU はセキュリティリスクを大幅に削減し、導入コストと継続的な管理コストを削減した。

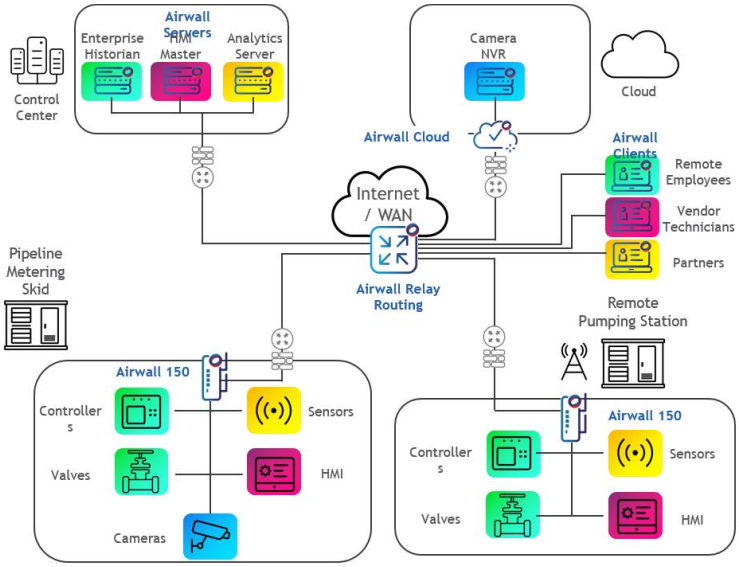



### Smart Manufacturing



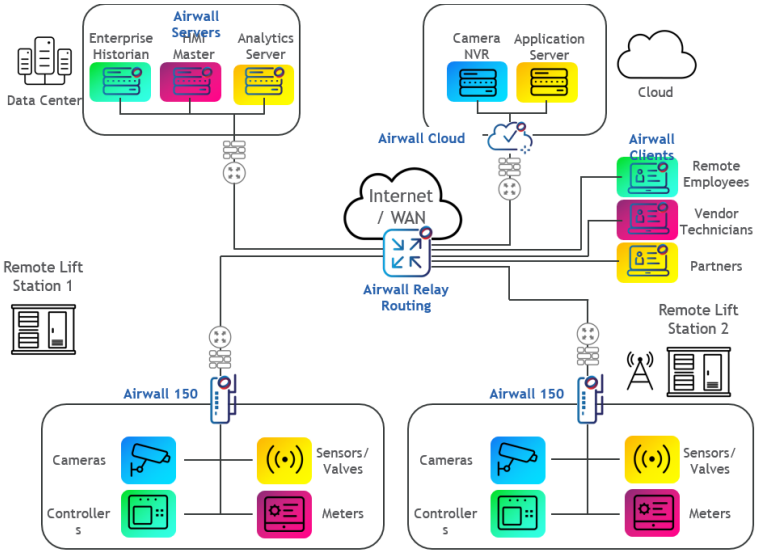

某大手製造メーカは工場制御システムとか各生産ライン設備の前に Airwall モデル 150 アプライアンスを設置して、企業 FA ネットワークを IT ネットワークから分離した。

## Smart Energy(化学プラント)




既存の分散制御システム(DCS)のセキュリティ対策により、Airwall Edge Services を採用して各エネルギーシステムをセグメント化し、企業 IT ネットワークから隔離した。

## Smart Water（水道・浄水場）



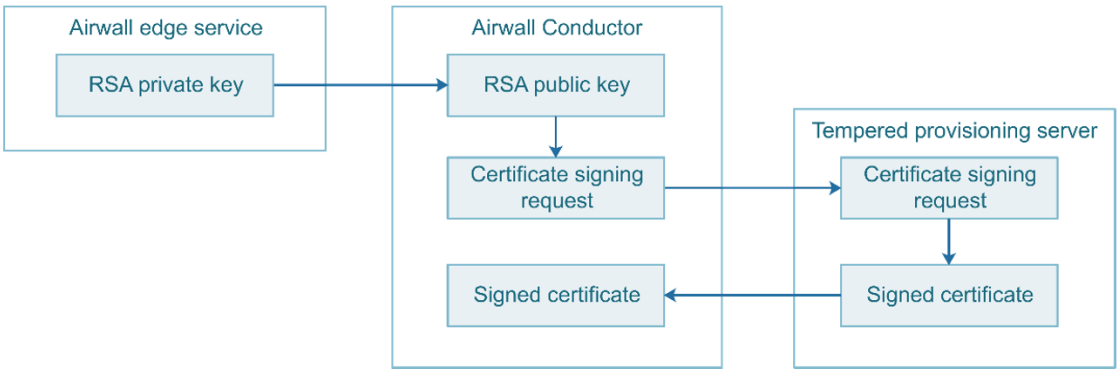

各種給水システムをセグメント化し、それらを企業 IT ネットワークから隔離し、モバイル通信とインターネット通信に置き換えた。

機能毎の分散制御システム(DCS/PLC)をセグメント化し、その各セグメントエッジのサイトに Airwall 150 を設置した。

## Airwall の ID によるセキュア認証のしくみとは

Tempered Networks Airwall ID は、各 Airwall Edge Services および Airwall Conductor が持つ暗号強度の高い RSA(Rivest–Shamir–Adleman)キーペアによって鍵交換でセキュア認証します。鍵ペアは、Airwall Edge Services の秘密復号化キーと、Airwall Conductor にある公開暗号化キーで構成される。


Airwall Conductor は、公開キーを各 Airwall Edge Services に配布する。公開キーに加えて、ID もそれぞれに割り当てられる。Airwall Edge Services は、通信ペアの ID を保証する暗号化手段によって相互間の信頼を確立する。ID 認証が確立されると、通常、生成されたキーを再交換する必要はない。




あとがき：

冒頭でも述べたが、Airwall Edge Services の HIP ソリューションは従来の Tempered networks が提供していた HIP Services の機能をすべて踏襲する。