©2018 SEC Co. Ltd.
mykarte.com

ID Link データセンターとの接続方式 セキュリティ対策

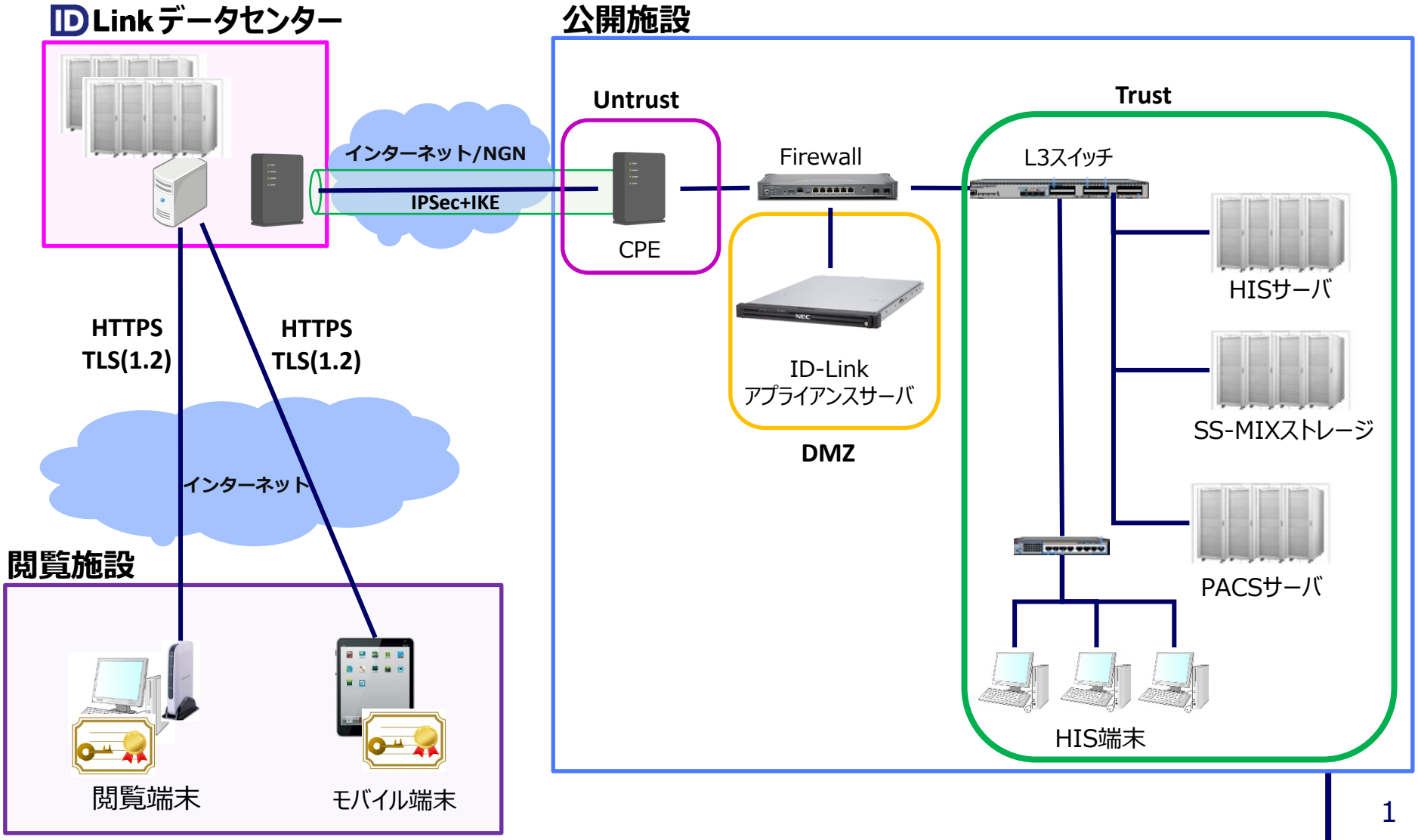
第2版 2023/2/28

株式会社エスイーシー
ID-Linkサポートセンター

©2018 SEC Co. Ltd.

全体接続イメージ図

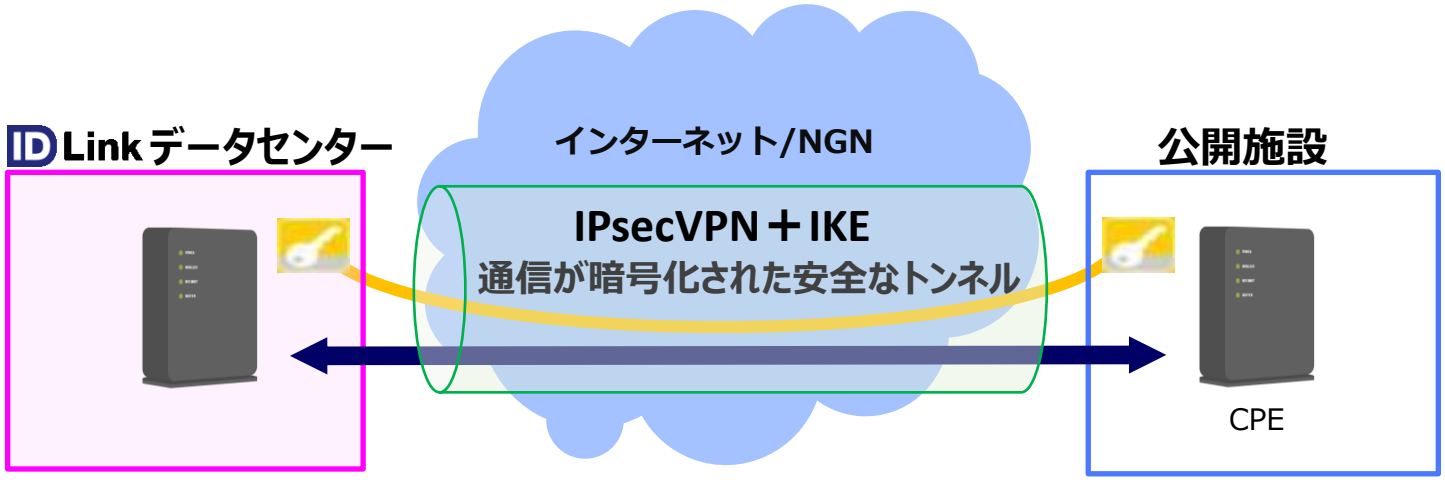
公開施設はインターネットVPN、もしくはNGNの閉域網で接続し、閲覧施設はTLSクライアント認証を用いて接続します。



©2018 SEC Co. Ltd.

公開施設 VPN接続（有料プラン）

インターネット回線を用いたインターネットVPNと、NGNを用いた閉域網VPNに対応しています。
『医療情報システムの安全管理に関するガイドライン 第5.2版』に基づいたIPSec+IKEプロトコルを利用しており、VPN装置に初期設置した鍵（事前共有鍵）を双方が交換しあう事により、盗聴、侵入、改ざん、妨害等を防ぐ安全なトンネルを作成します。



VPN装置に初期設定された鍵は一定間隔で自動更新
（AutoIKE ※オート インターネット キー エクスチェンジ）

AES暗号アルゴリズムにより、データは暗号化されインターネットを通過

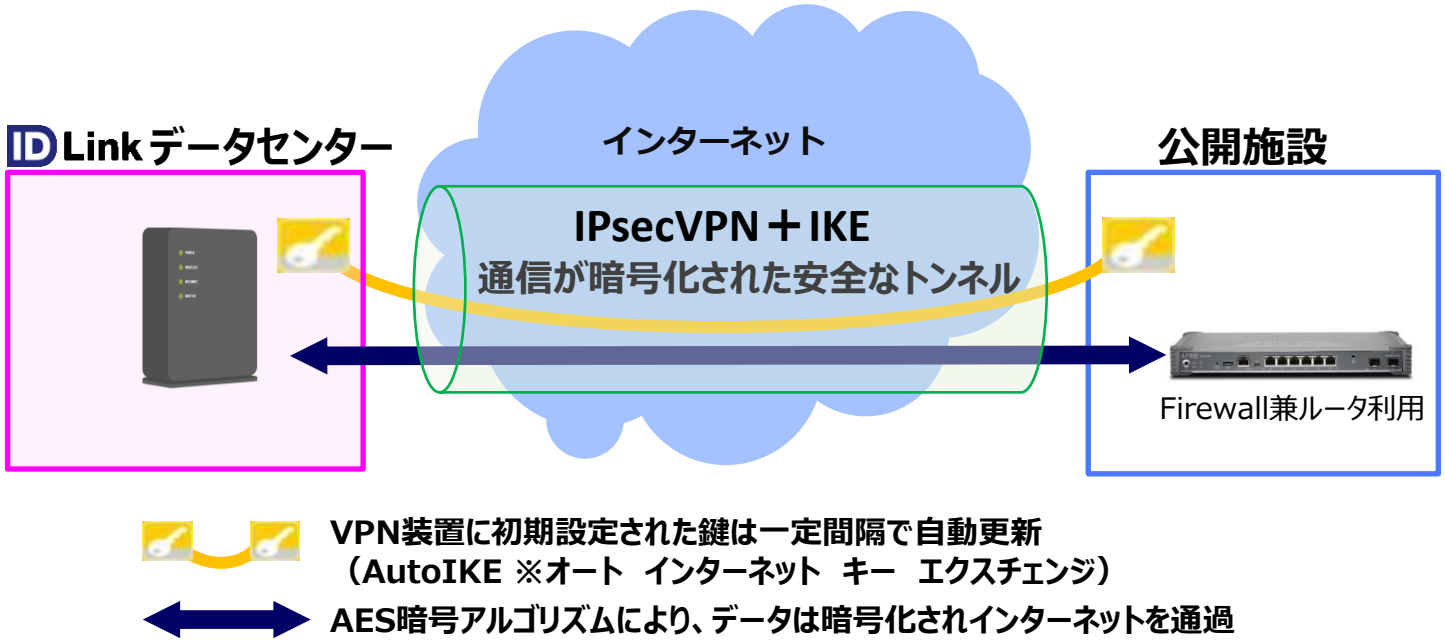
NGN：インターネットと同じIP(Internet Protocol)を基盤とするデータ通信技術を用いて構築された公衆交換電話網

CPE：利用施設内に設置されるVPNルータ

©2018 SEC Co. Ltd.

公開施設 VPN接続（無保証）

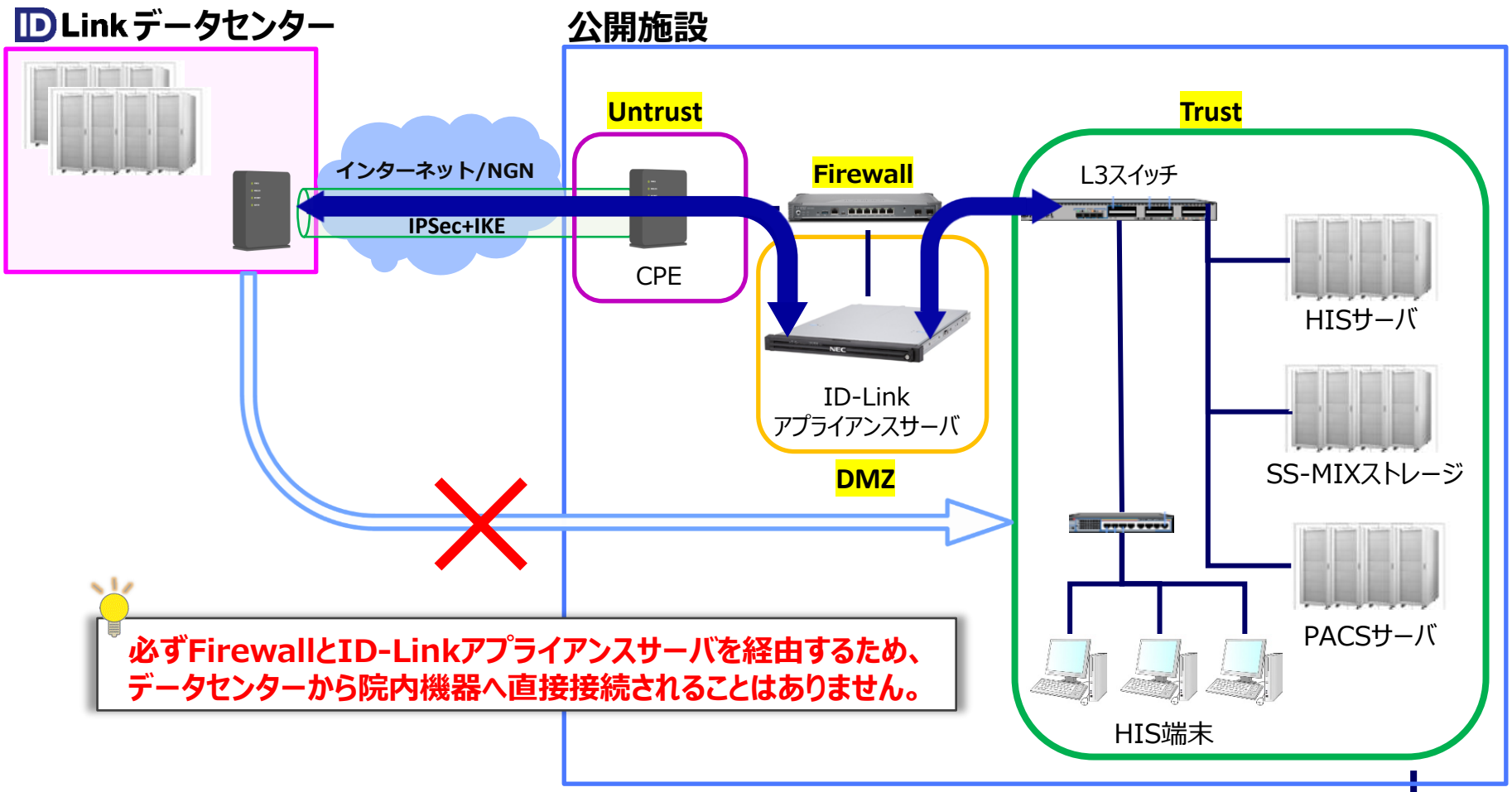
ID-Linkアプライアンスに付属するFirewallのルータ機能を用いて、IPsecVPNを構築する事も可能です。『医療情報システムの安全管理に関するガイドライン 第5.2版』に基づいたIPSec+IKEプロトコルを利用していますが、チャネルセキュリティなどの秘匿性等の保証はありませんので、VPN事業者として秘匿性等の保証が必要な場合は、前頁の有料プランをご利用ください。



©2018 SEC Co. Ltd.

公開施設 Firewallによる通信制限

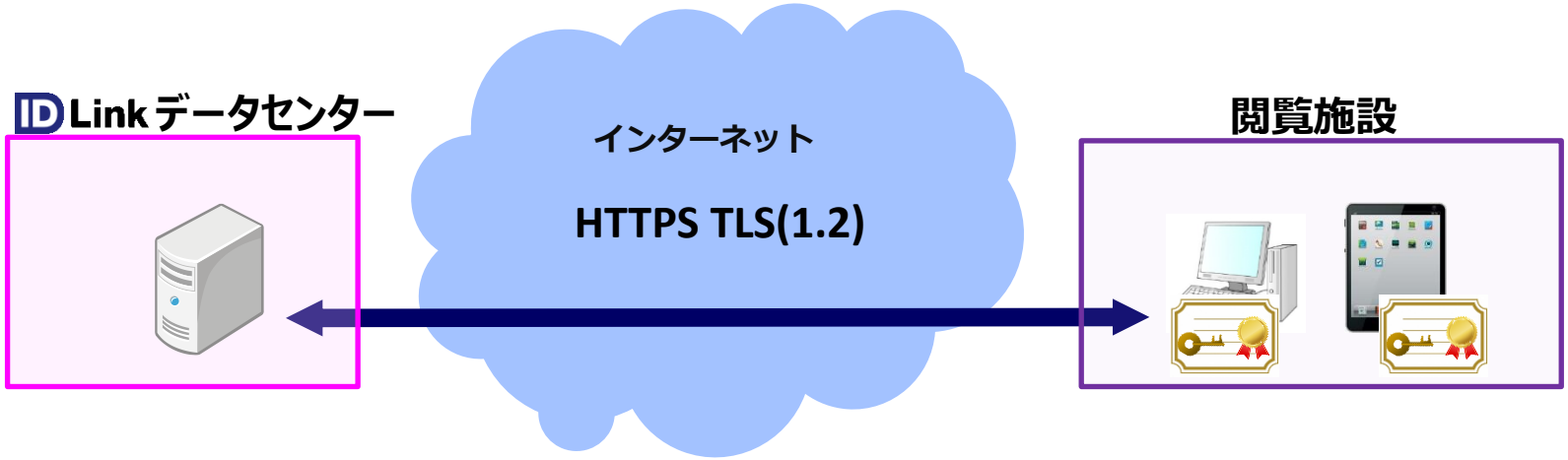
公開施設内にFirewallを設置し、Untrust・DMZ・Trustの3つのセキュリティゾーンを構築します。
院内ネットワークと分けることができるため、万が一、ID-Linkアプライアンスサーバに障害が発生した場合でも、院内側への影響を抑制する事が可能です。また、Firewallで必要最小限のIPアドレスとポートのみを通信可能とし、それ以外のIPアドレスとポートは通信制限します。



©2018 SEC Co. Ltd.

閲覧施設 HTTPS接続

ハッシュアルゴリズムSHA-2対応のクライアント証明書を利用端末へインストールし、『医療情報システムの安全管理に関するガイドライン 第5.2版』に基づいたTLS1.2プロトコルを利用する事で、盗聴、侵入、改ざん、妨害等を防ぐ安全なトンネルを作成します。

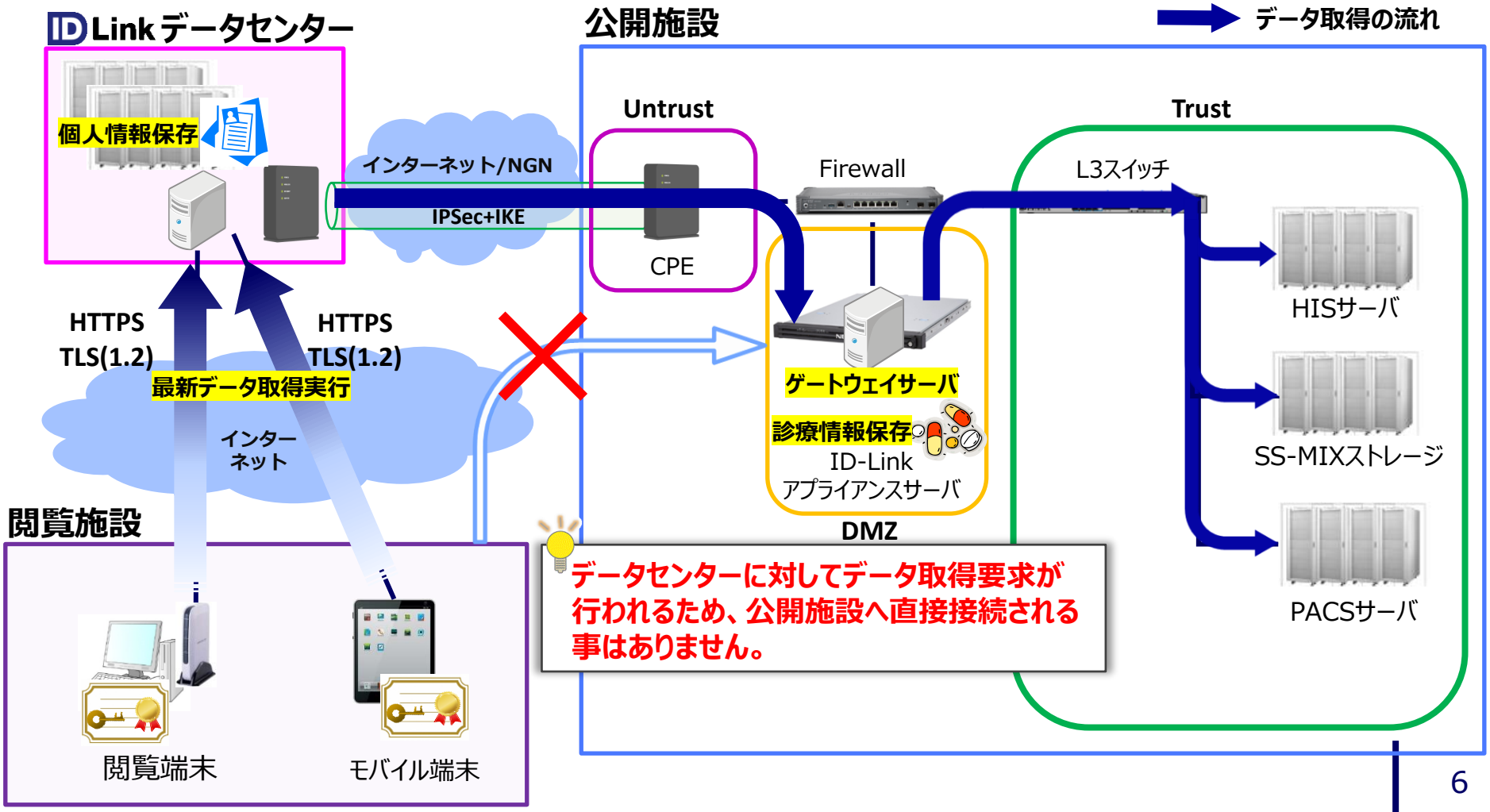


ID-Linkサポートセンターで発行するクライアント証明書はペアで存在し、その片方を利用施設へ配布。クライアント証明書のインストールにはパスワードが必要になるため、証明書のみ入手してもインストールできません。

©2018 SEC Co. Ltd.

公開施設からデータを取得

最新データ取得を実行すると、センターサーバからID-Linkアプライアンスサーバ内のゲートウェイサーバに対して取得処理が実行されます。ゲートウェイサーバは院内の各連携サーバからデータを取得し、診療情報はゲートウェイサーバ内に保存、個人情報はセンターサーバに保存されます。
※情報公開の同意を得た患者のみ保存

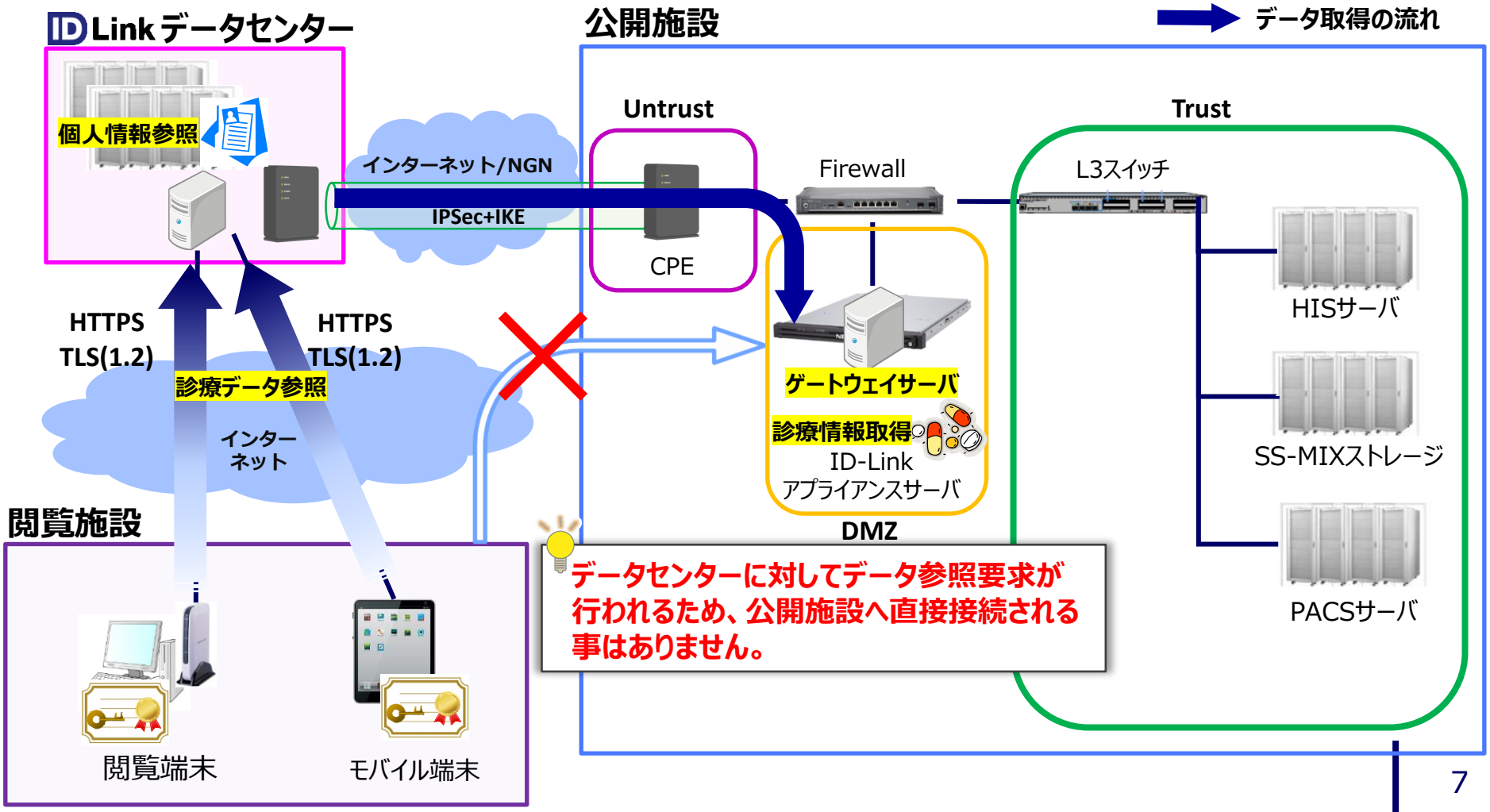


©2018 SEC Co. Ltd.

mykarte.com

公開施設のデータを参照

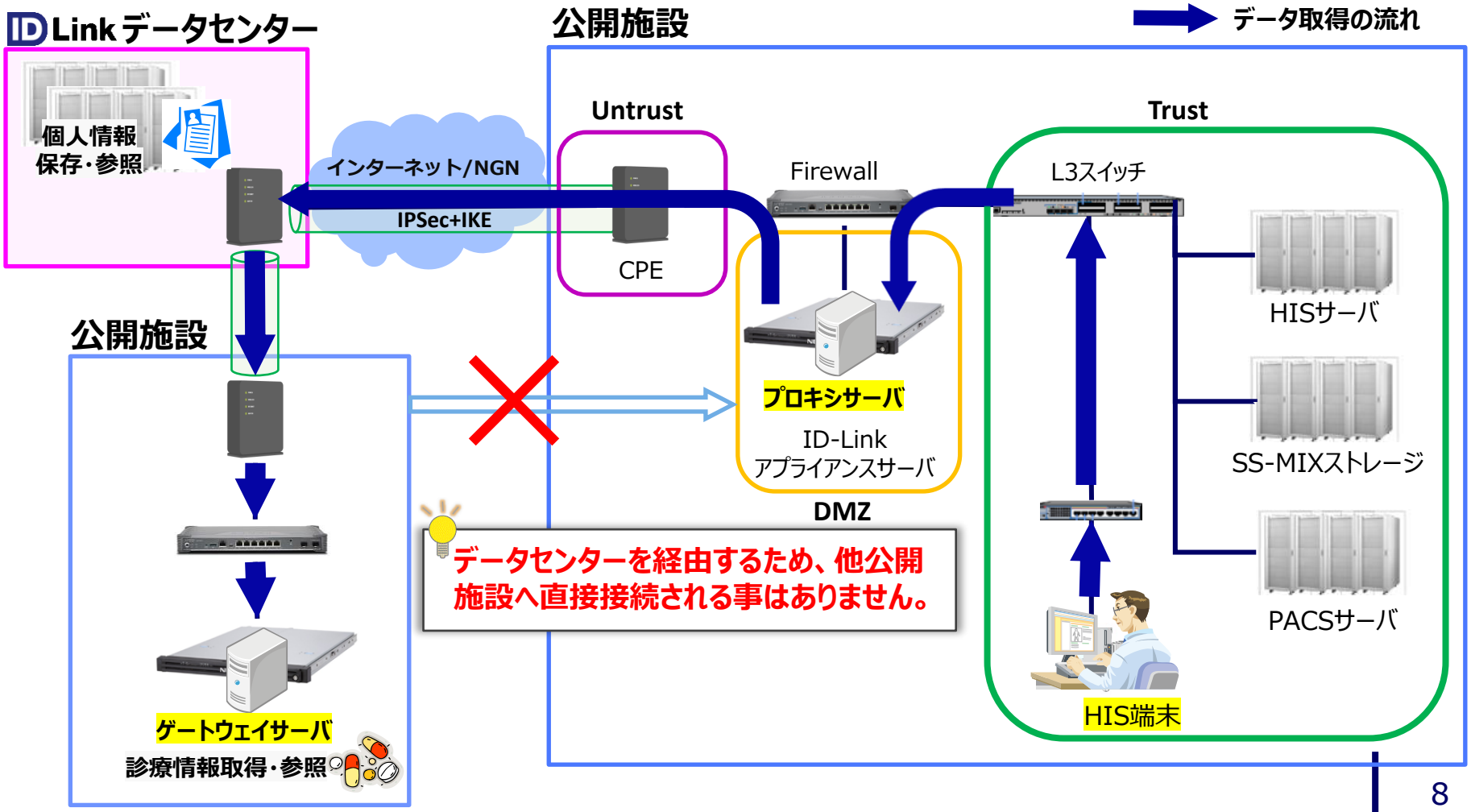
診療データを参照する場合は、センターサーバが対象施設のゲートウェイサーバに保存された診療情報を取得し、結果を返却します。データ取得時のみ公開施設内の連携サーバ（HISサーバ、PACSサーバ等）へアクセスする事によって、連携サーバへの負荷を最小限に抑えます。



©2018 SEC Co. Ltd.

公開施設同士の利用

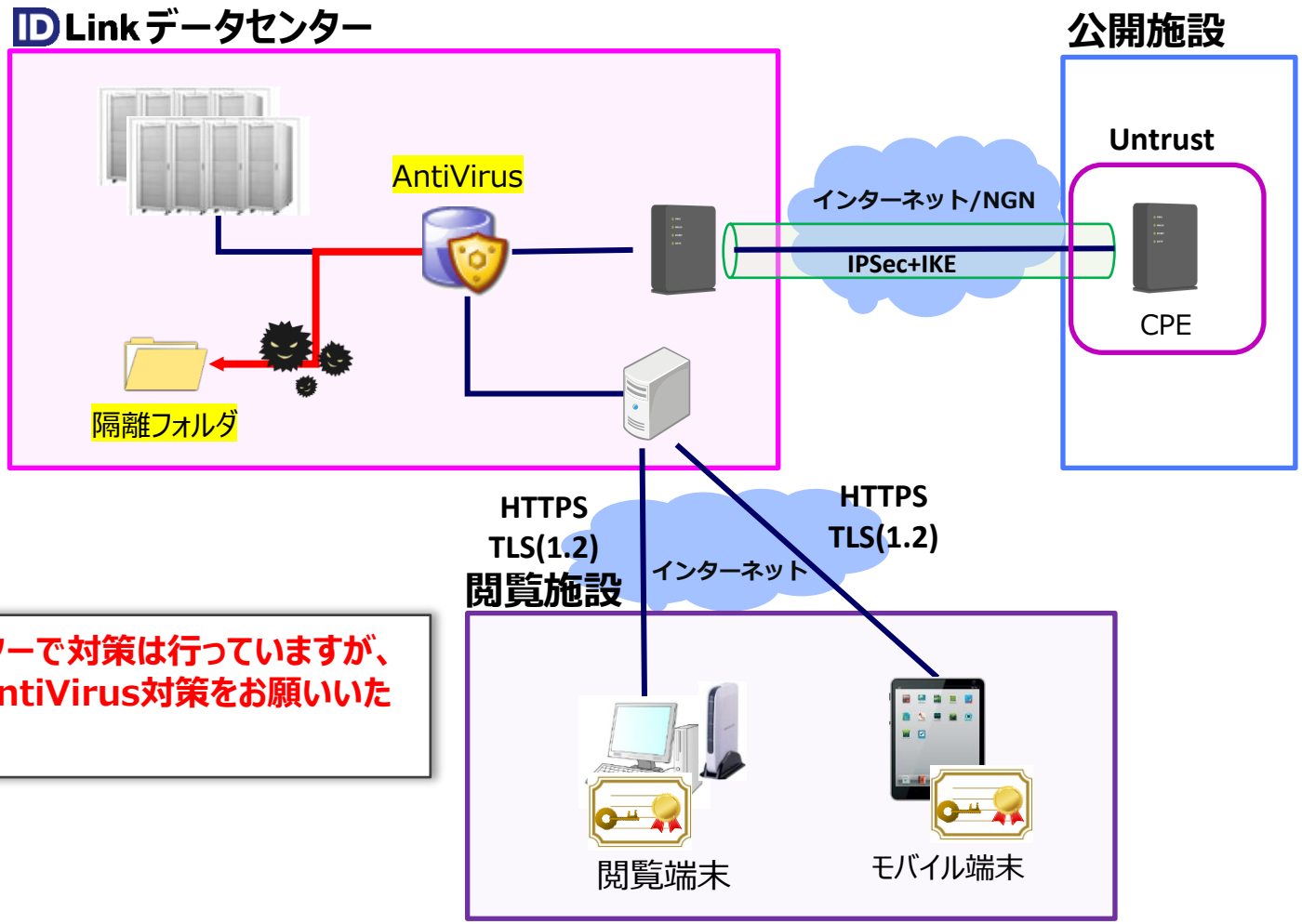
院内の端末から他公開施設のデータ取得・参照を行う場合は、ID-Linkアプライアンスサーバ内のプロキシサーバを経由し、データセンターへ取得・参照要求が行われます。
データセンターは、対象となる公開施設のゲートウェイサーバに対して要求処理を実行し、その結果を要求元に返却します。



©2018 SEC Co. Ltd.

ウィルス対策

ID-Linkで公開されるデータは必ずデータセンターを経由するため、データセンター内の装置でAntiVirus対策を行っています。これにより、万が一ウィルスに感染したデータがアップロードされたとしても、連携関係にある他施設への侵入を防ぎます。

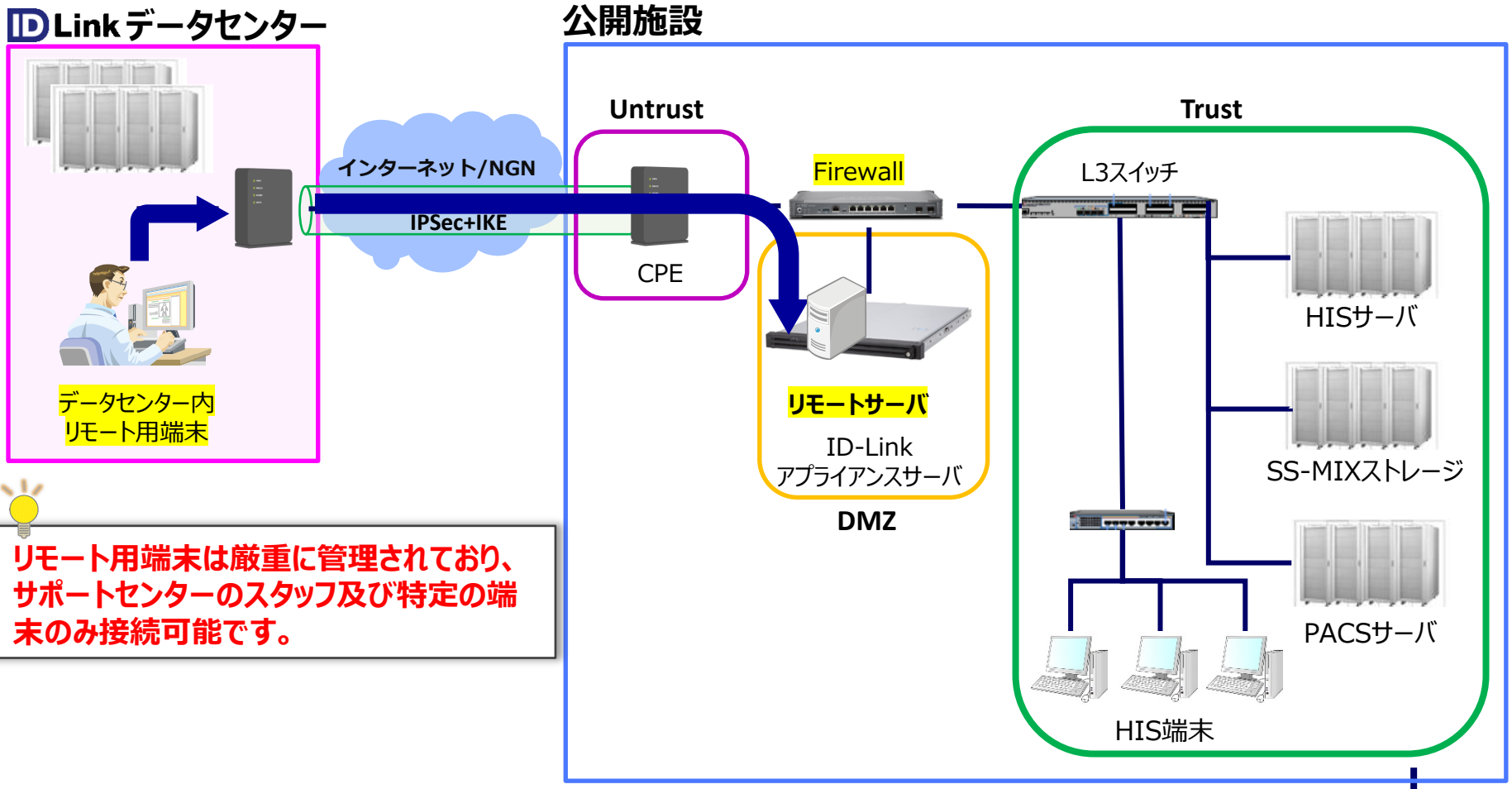


データセンターで対策は行っていますが、各施設でAntiVirus対策をお願いいたします。

©2018 SEC Co. Ltd.

その他セキュリティ対策（リモートメンテナンス）

データセンターからリモートメンテナンスを行う場合は、リモート用端末を用いて、ID-Linkアプライアンスサーバ内のリモートサーバへ接続します。院内ネットワークに直接リモート接続は行いません。



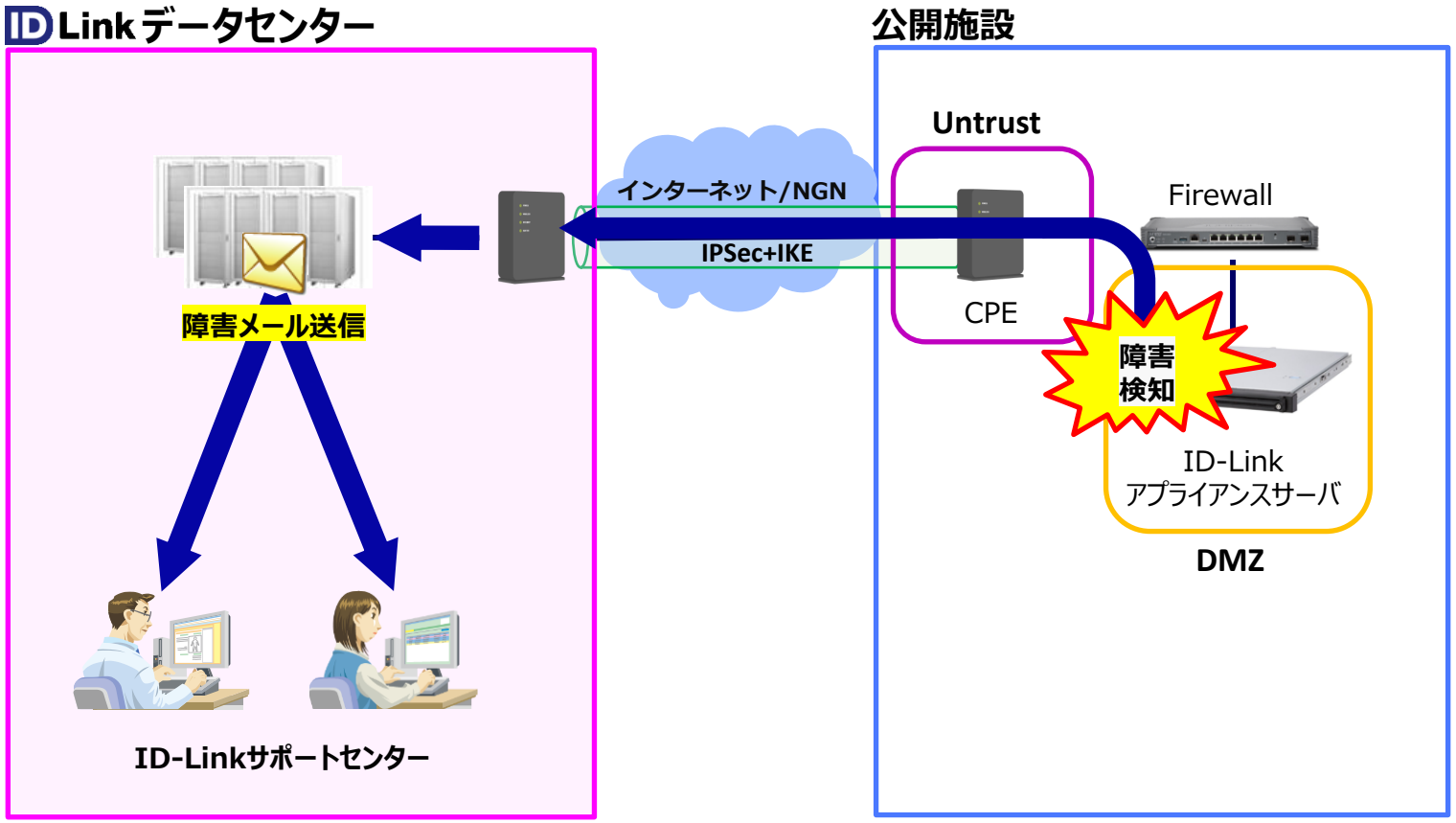
リモート用端末は厳重に管理されており、サポートセンターのスタッフ及び特定の端末のみ接続可能です。

©2018 SEC Co. Ltd.

mykarte.com

その他セキュリティ対策（サポートセンター体制）

全国のID-Linkアプライアンスサーバ導入施設に対して、24時間365日の監視ツールを構築しています。アプリケーションの動作不良やハード障害等を検知すると、サポートセンターのスタッフ宛にメールが送信され、調査等の対処を行います。



©2018 SEC Co. Ltd.

改版履歴

版数	項目	説明	日付
初版	全般	新規作成	2018/10/23
第2版	全般	全体のイメージ修正、セキュリティ対策追加	2023/2/28