

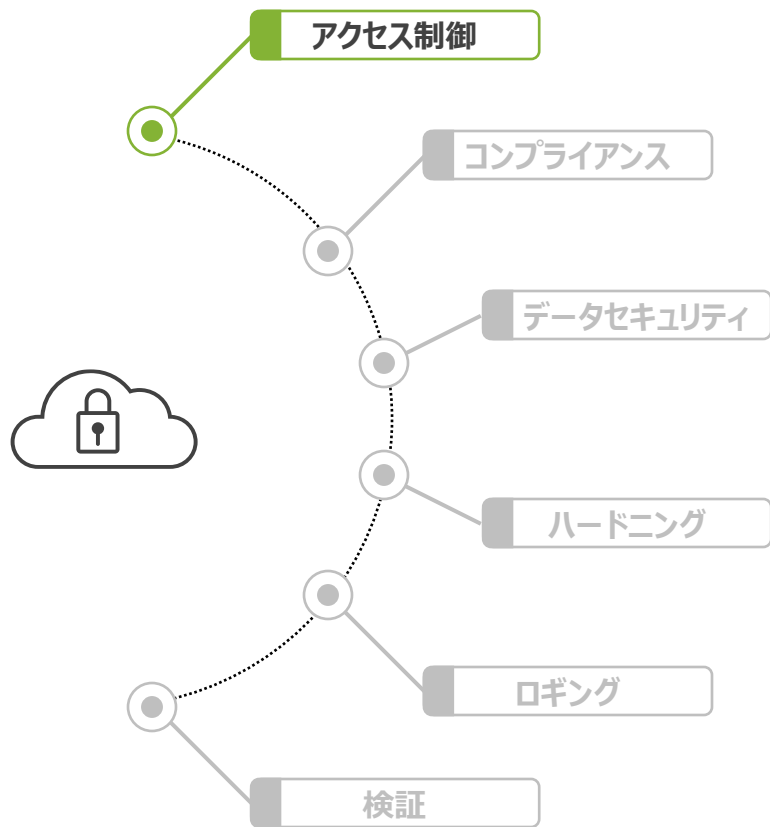
Mist セキュリティ セキュリティへの取り組み

ジュニパーネットワークス株式会社
2021年11月 Ver 1.0

JUNIPER
driven by Mist AI 

Mistクラウド プラットフォーム

Q: クラウドプラットフォームはどのように運営されていますか？



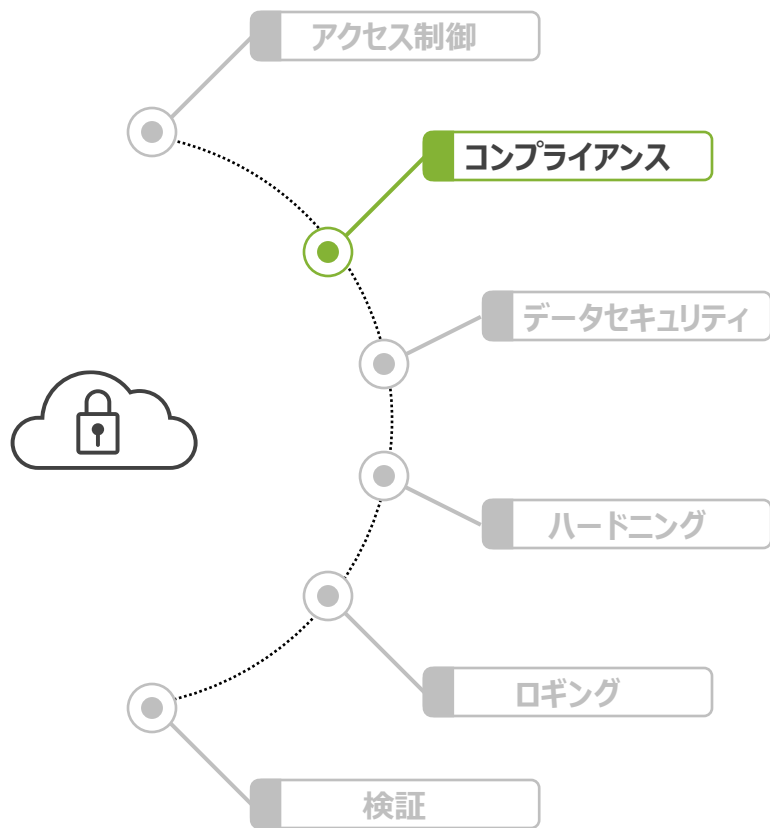
アクセス制御

- Juniper/Mist からクラウドへのアクセスは厳格に制限された環境下で運営されています

追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: クラウドプラットフォームはどのように運営されていますか?



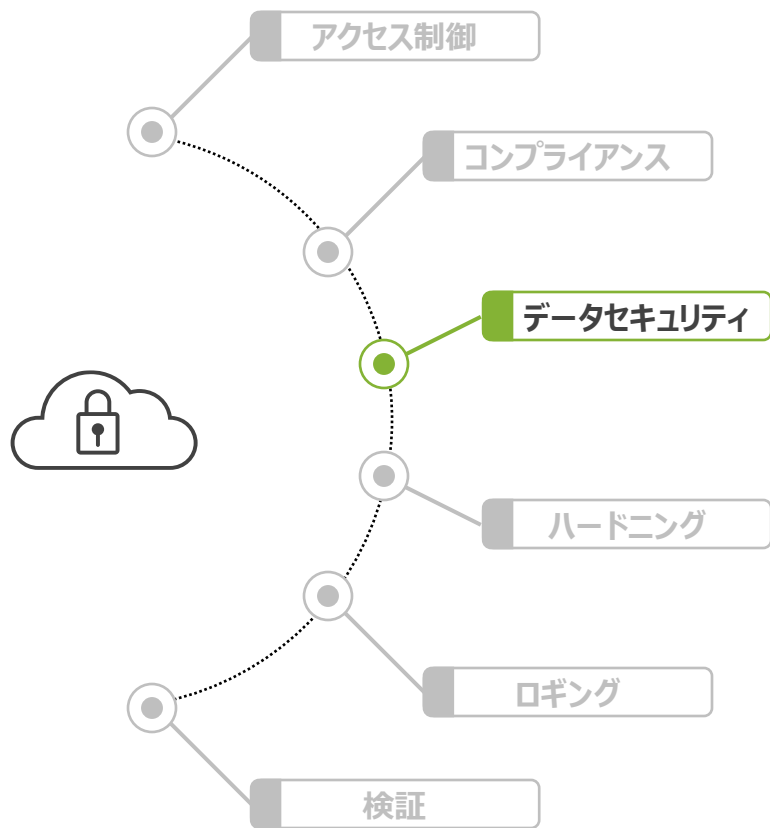
コンプライアンス

- サーバは複数のアベイラビリティゾーンにまたがり SOC2 type2 に準拠したデータセンターでホストされています

追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: クラウドプラットフォームはどのように運営されていますか?



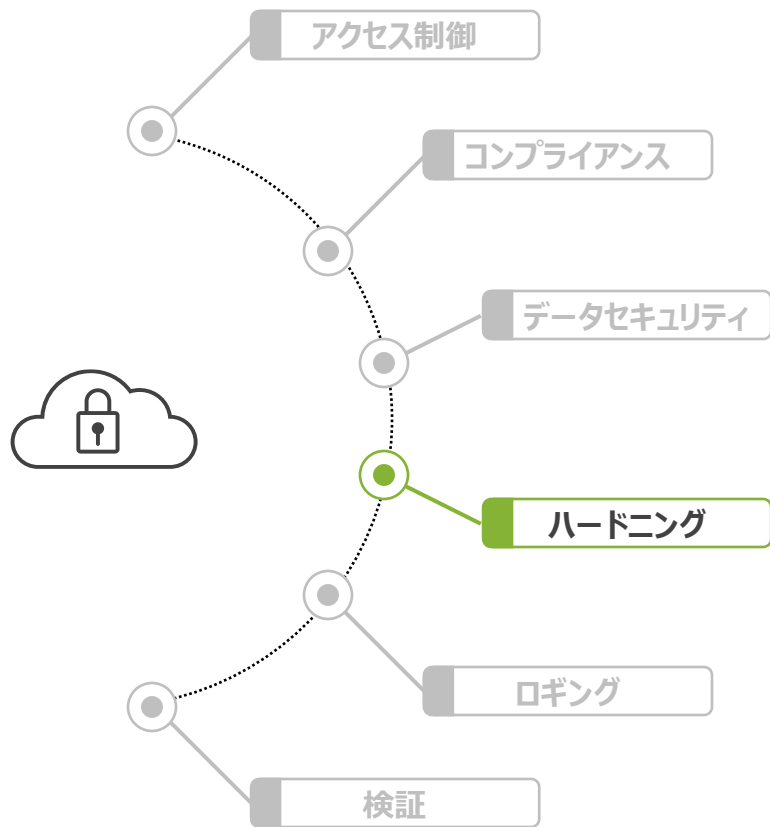
データセキュリティ

- 転送中のデータと保存中のデータには業界標準の暗号化手法が使用されます
- クラウドに保存されるクライアント情報は組織固有のキーで暗号化されます
- セキュリティは開発サイクルと密接に連携しており、コードを本番環境にリリースする前に脆弱性スキャンを実行し安全性の確認を行います
- サーバは AWS 上の複数の VPC 上でホストされ、セキュリティグループ、ファイアウォールで保護されます
- フロントエンドサーバまたはターミネータは外部から API または AP と直接通信する必要があるポートのみ許可します

追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: クラウドプラットフォームはどのように運営されていますか?



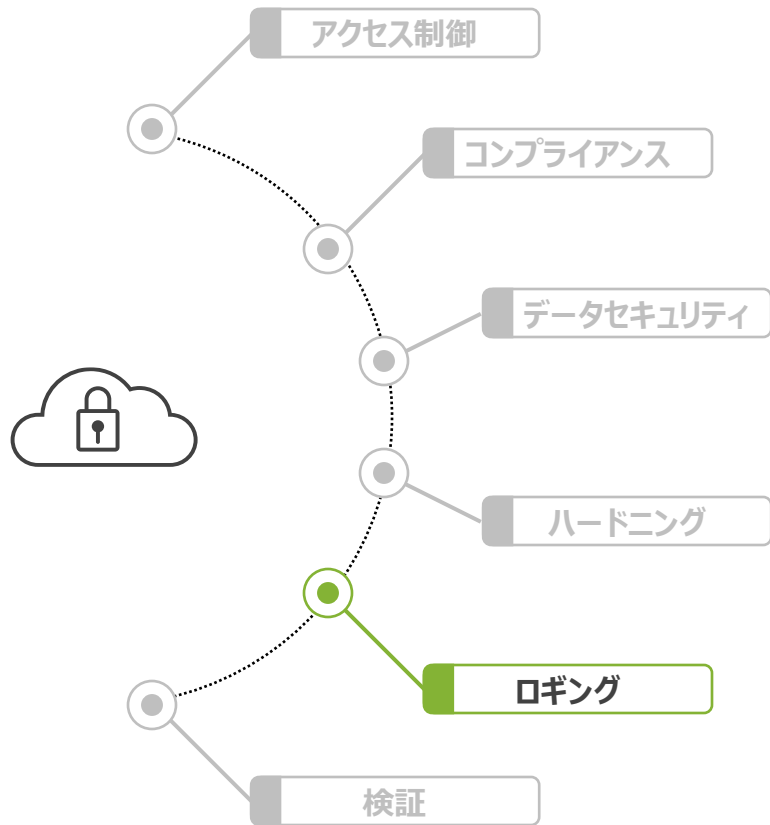
ハードニング

- すべてのサーバは Linux OS を実行し、業界のベストプラクティスに従ってハードニングされています

追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: クラウドプラットフォームはどのように運営されていますか?



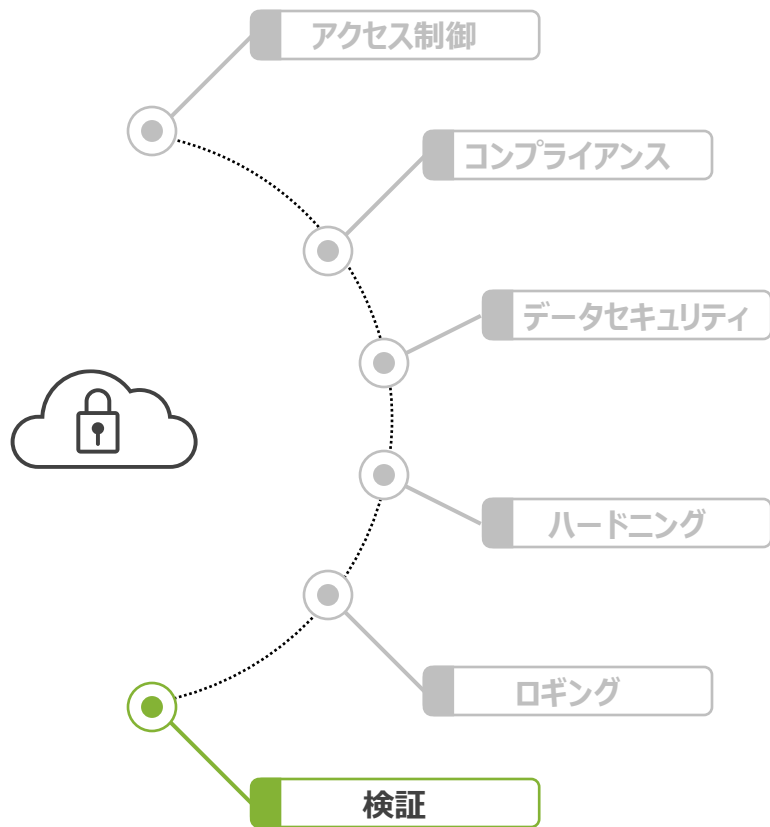
ログイング

- 監査ログは集中管理された場所でキャプチャされます

追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: クラウドプラットフォームはどのように運営されていますか?



検証

- Mistは、開発段階から実稼働段階までの各ステージにおいて Web セキュリティ試験を実行します
- SQL インジェクション、XSS、OWASP Top 10 を含む 700 以上の脆弱性をスキャンします
- 定期的な外部侵入テストによる検証を行います

追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: Mist はデータをどのように保護しますか?

AP とスイッチ

- TLS 1.2 とAES-128 暗号化
- 製造時に作成されたデジタル証明書とAPごとの共有キーの組合せを使用した相互認証
- 証明書署名には4096ビット鍵を使用

UI や API

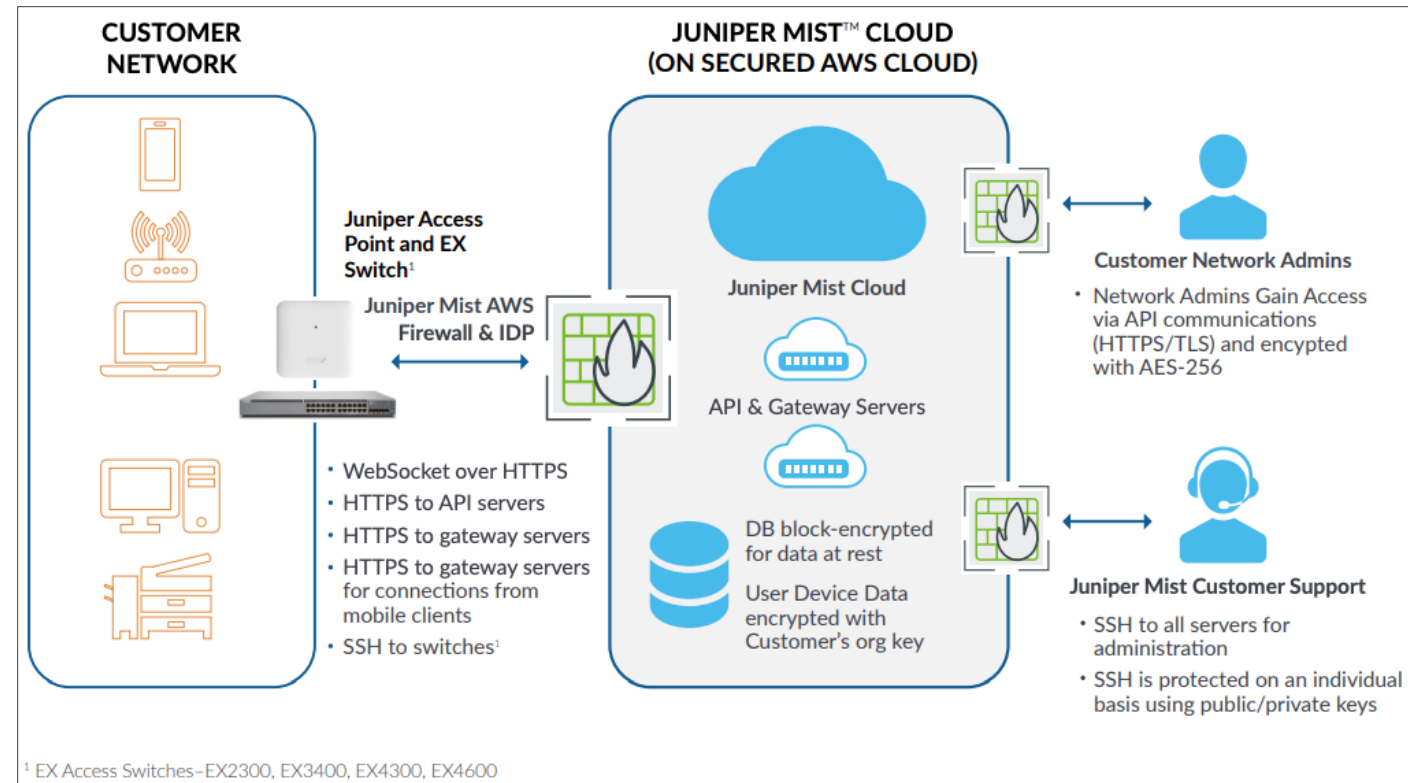
- API 通信(UI アクセスを含む) はTLS 1.2 を使用し、AES-256 で暗号化

内部からクラウド

- クラウド内のデータの保存には、AES-256 暗号化を使用

管理/インフラストラクチャコンソール

- 2048 ビット RSA キーを使用したHTTPS 接続でアクセス



追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

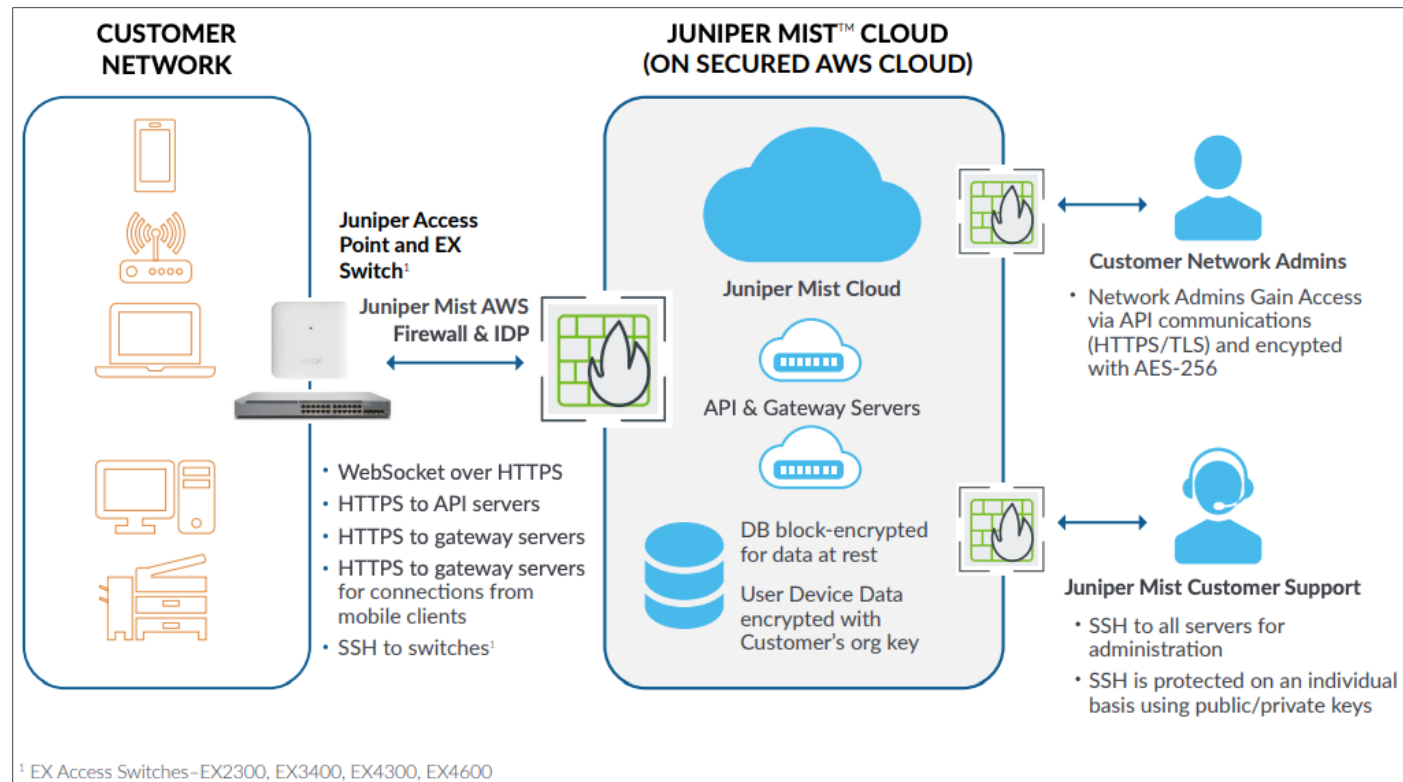
Q: 管理されているデバイスにアクセスできるようになっていますか?

アクセス制限

- AP へのアクセス :
利用者がアクセス可能なインターフェースなし
- スイッチへのアクセス :
お客様が管理する SSH/Web-UI
- AP/スイッチからクラウドへのアクセス :
お客様による Site 割り当てに基づく

アクセス制御

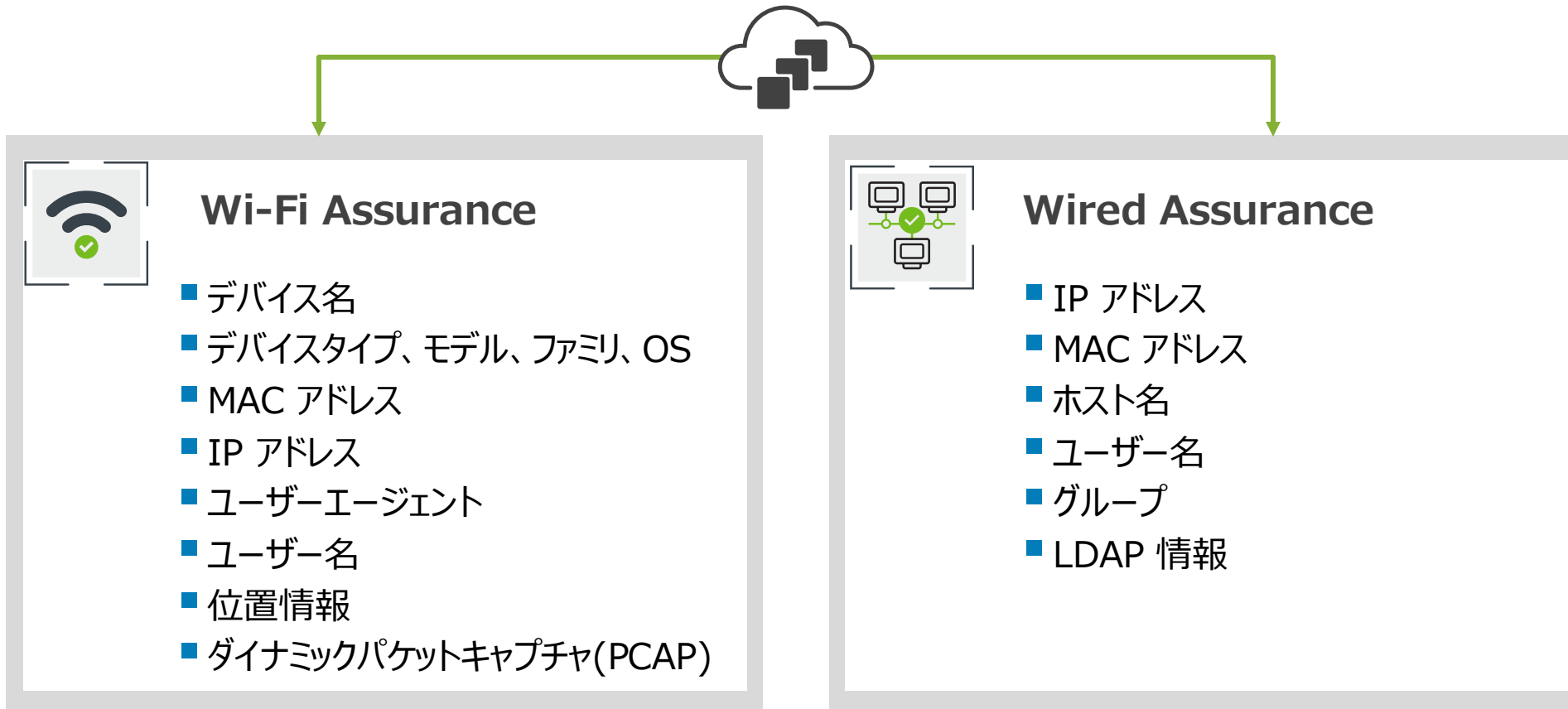
- 組織/サイトの設定に基づくロール
- ジュニパーは弊社社員に対し顧客およびデバイスへのアクセス権を付与する際に、最小権限の原則に従います



追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: Mist クラウドによってキャプチャされるデータのタイプは?



追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: データはどのように保護されますか?

個人データ

- ブロックレベルの暗号化を実行

デバイスデータ

- Organizationごとにユニークなキーを使用し暗号化

設定データ

- データベースの暗号化

ユーザートラフィック

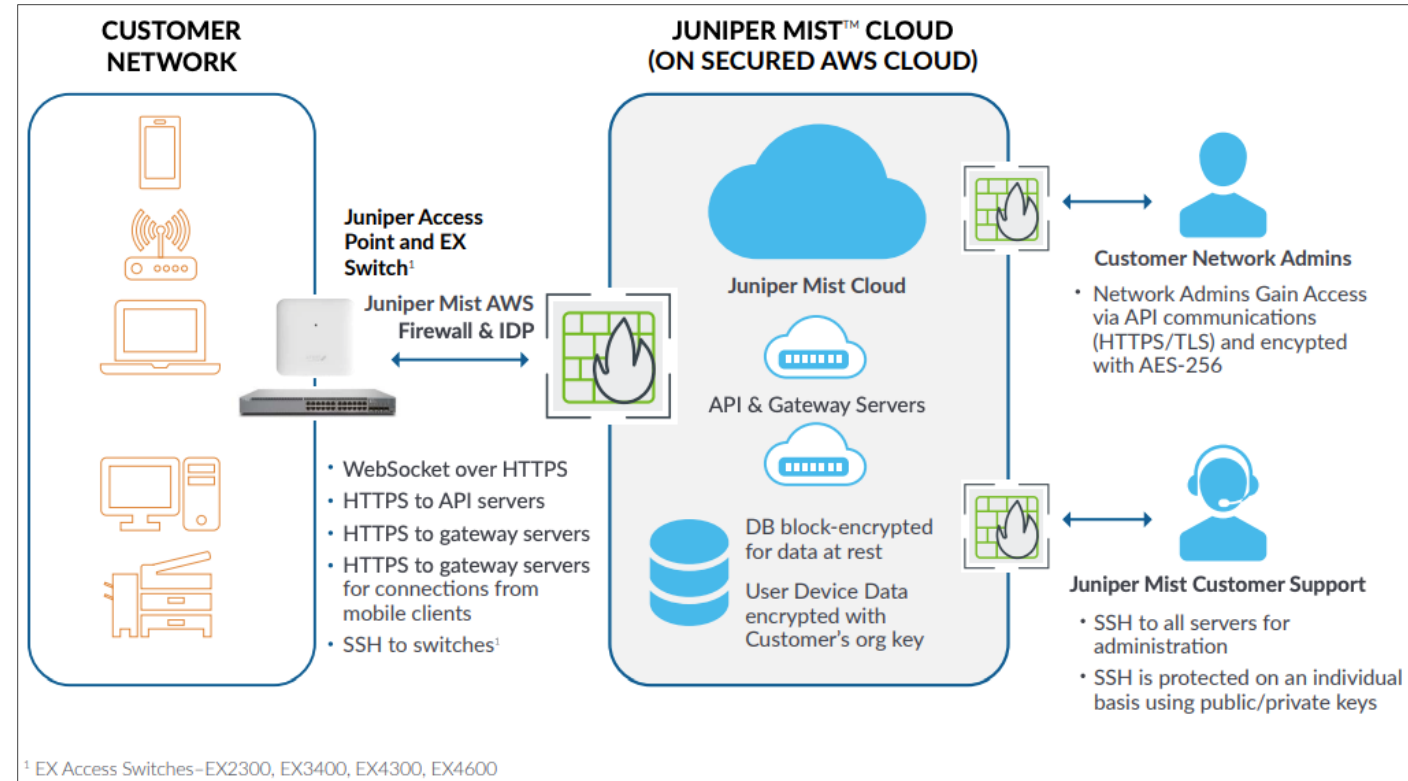
- クラウドには一切転送されません

ダイナミックパケットキャプチャ

- ヘッダのみがキャプチャされクラウドに転送

メタデータ 位置情報、統計

- Organizationレベルのアクセス制御



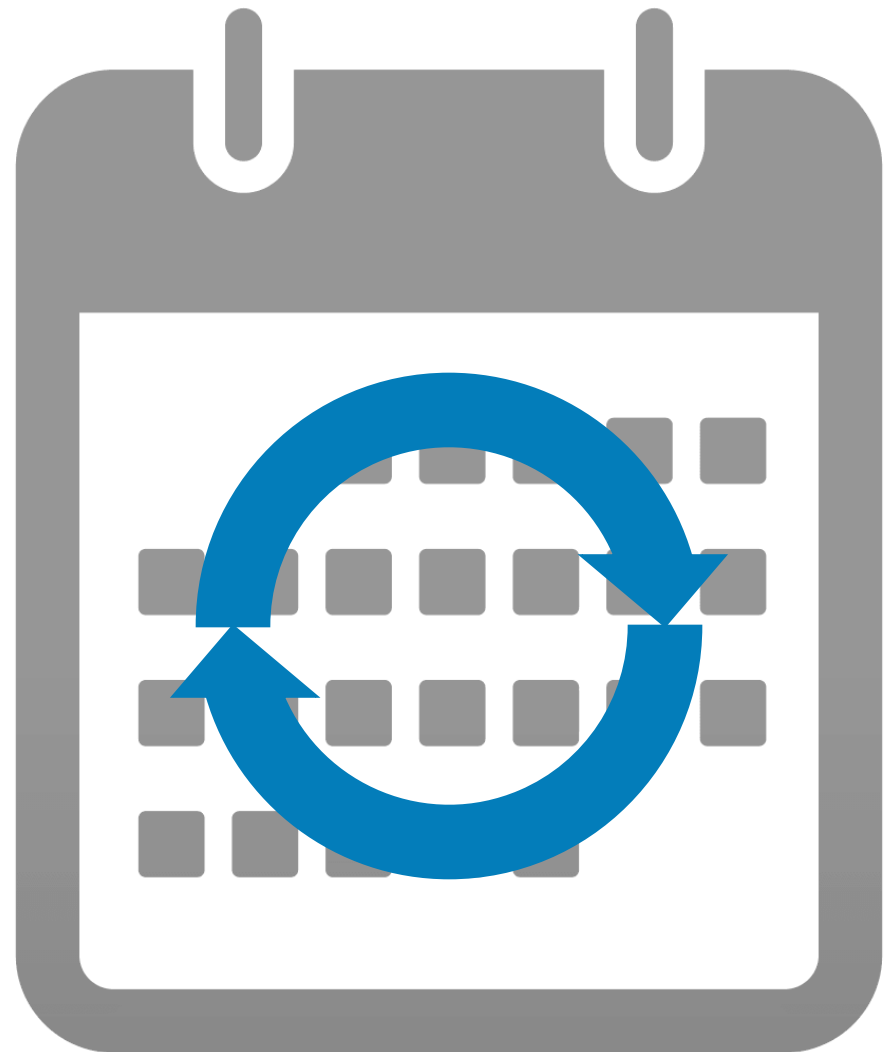
追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

Q: データはどのくらいの期間保持されますか?

データ保存

- 顧客データ（デバイスデータを含む）は60日間で順次削除
- 顧客の要求に応じて削除可能
- パケットデータは7日間保持
- プレミアムアナリティクスデータは長期間保持



追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Mistクラウド プラットフォーム

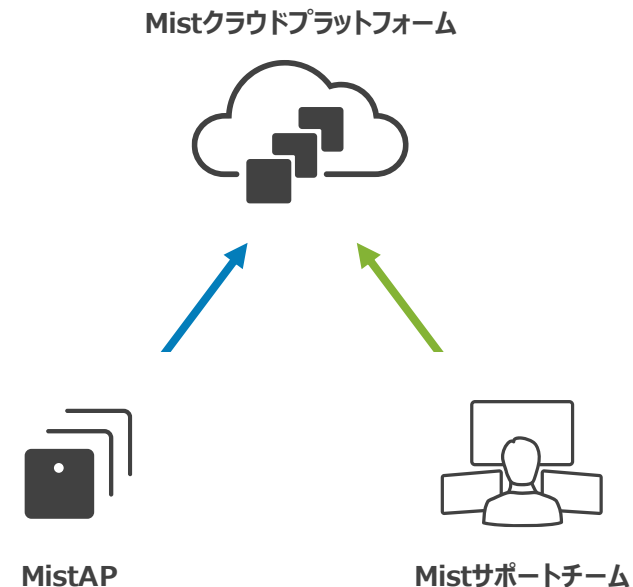
Q: Mist サポートチームはデータにアクセスできますか？

Mist サポートチームからのアクセス

- Organization へのアクセスとデバイス情報に対して制限が可能

ダイナミックパケットキャプチャへのアクセス

- SLE とインサイトに使用されるダイナミックパケットキャプチャ機能は有効・無効を設定可能
- パケットのペイロード部分はMistクラウドに送信されず、パケットヘッダのみ転送



Support Access

- Allow Mist Support Team to access your Mist Organization ?
- Allow Mist to capture packets in order to analyze errors and improve diagnostics

追加情報: https://www.mist.com/wp-content/uploads/Mist_AI_Trust_Tech_Brief_fin.pdf

Thank you

JUNIPER 
driven by Mist AI