Xage Security Fabric

産業分野における
アイデンティティ/アクセス管理

FEBRUARY 2019 XAGE SECURITY

www.xage.com | hello@xage.com

xage SECURITY

産業界で、モノのインターネット (IIoT) やIndustry 4.0として知られる革命が起こっています。企業は、リアルタイムでデバイス同士または人とのやり取り、協調が可能となるインテリジェントなシステムの構築を行なっています。そのようなシステムでは、堅牢なセキュリティ制御が備わった最新のデバイスだけではなく、現在稼働中のPLC、RTU、HMI、メータ、センサなどセキュリティ面の機能が制限されたデバイスが混在しています。

IIoTによって、幅広い産業や政府機関に多くの良い影響が与えられることになります。それはより効率的な生産、より高い製品品質、顧客満足度の向上、そして公益事業者、再生可能エネルギー供給者、石油およびガス会社、製造業者、輸送機関、政府などに対する安全性の向上をもたらすことになります。IIoTによって、サプライヤ、サービスプロバイダおよび顧客などの外部組織にまで及ぶ連携を可能にします。

IIoTでは何百万というデバイスが連携することになります。その構成要素の中に1つでもセキュリティ面に問題があるものがあるだけでも、システム全体にその影響が及ぶ可能性があります。コアからエッジまでをカバーするセキュリティが必須となりますが、その実現には多くの課題があります。IIoTデバイスは地理的に広範囲に渡って実装されることもあります。本質的なセキュリティ機能を欠いているデバイスもあります。ネットワークへの接続速度が遅いものや常にネットワークへは接続できないデバイスもあります。ピアツーピアで接続されるデバイスとアプリケーションとの間の通信も保護する必要があります。

IIoTでは、攻撃の対象となる領域が企業ネットワークと比べて大幅に拡大します。 IIoTコアからエッジまで、あらゆるデバイスやアプリケーションに対応するセキュリティファブリックが必要となります。

IIoTのセキュリティ問題を解決するには分散化が必要

分散化とは産業界とIIoTに固有のものです。一般的な機械やその他の形態の産業用装置、例えばユーティリティ向けのインテリジェントな電子装置、石油およびガス用のポンプオフ制御装置が普及しています。そういった機械や装置同士のやり取りは分散されています。次のような理由から、セキュリティも分散させる必要があります。

- 分散化による単一障害点の回避：フィールドにある資産は、本質的に公開されています。セキュリティデータを配布して実施することで、局所的な侵害が発生した場合の感染を回避できます。
- スケール： IIoTシステムには、リアルタイムでの通信が必要となる何百万もの分散デバイスが存在することがあります。そのような大規模システムにおいて、計算、通信、制御およびセキュリティの集中化は実現不可能です。
- 複数対地間データ交換：現場での操作では、ローカルデバイスとアプリケーション間のフィールド内での連携を可能にするために、分散型の複数対地間データ交換が必要です。
- 即応性：ローカルで実施されているセキュリティサービスは、現場におけるリアルタイムでのやり取りを可能にし、ワイドエリアネットワークでのセキュリティのやり取りに固有となる待ち時間を回避します。
- 連続運用：フィールドでセキュリティサービスが実施されるため、ネットワーク接続に制限があったり、断続的となるワイドネットワーク経由の接続の場合でも連続運用が可能になります。
- 複数事業体によるアクセス：IIoTの1つの利点は、複数の事業体間の協力によって共通の目標を達成できることです。分散化により、各参加者が許可された機器とシステムにのみアクセスできるようになり、データとシステムの所有者がそれぞれの共有とアクセスポリシーを定義できるようになります。

Xage Security Fabric：IIoTのセキュリティ保護に最適

Xage Securityは、コアからエッジ、エッジからエッジまで、IIoTに接続するすべてのデバイス、アプリケーションおよび人を保護する分散型ファブリックによって、独自の方法でIIoTにおけるセキュリティを実現します。

- Xage Security Fabric – Xage Security Fabricは次のようなコンポーネントによって構成されています。
  - Xage Broker - Xage Brokerにより、Active Directoryや証明書サーバなどの企業システムと連携が可能となります
  - Xage Gateway – Xage Gatewayにより、セキュリティポリシーが強化されます
- Xage Policy Manager – Xage Policy Managerにより、セキュリティポリシーが設定され、Xage Security Fabricが管理されます。

Xage Security Fabricは、ポリシー作成の一元化を含む一元管理をサポートしています。これにより、Xage Security Fabricでは、フィールドへの改ざん防止ポリシーの複製およびフィールドでの分散型ポリシー実行が可能となります。

次のようなセキュリティサービスが、分散型Xage Security Fabricによって提供されます。

- ロールベースのアクセス制御 (RBAC) の強化
- デバイス、アプリケーションおよび人に対する信頼の構築
- 自動プロビジョニングの有効化
- アクセスや変更を記録したログの管理、改ざん防止
- 規制および規格への準拠の自動化と文書化
- データのプライバシーと整合性の保護
- 不正な変更を防ぐためのセキュリティポリシーと資格情報の改ざん防止

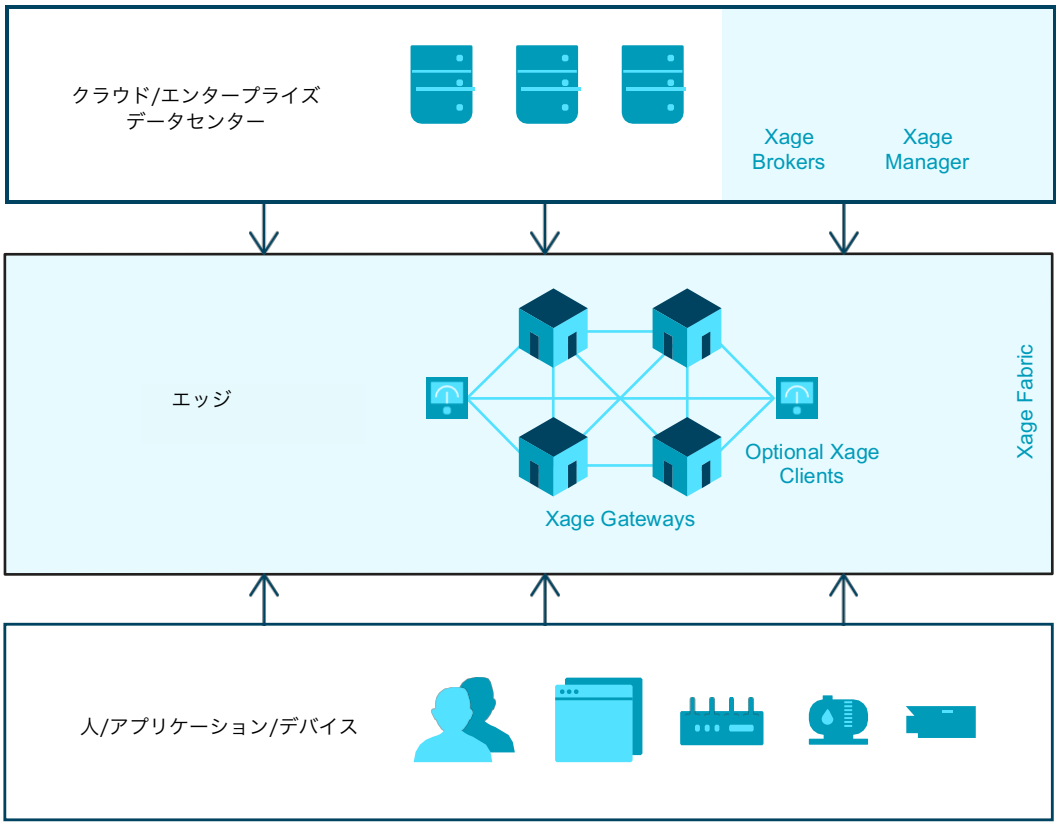
Xage Brokerは通常コントロール/オペレーションセンターに設置されます。しかし、ドメインコントローラなどのセキュリティサービスが運用ネットワークに紐付けられている場合は、フィールドに設置されることがあります。Xage Brokerが、LDAP、Active Directory、認証当局（CA）などのセキュリティサービスと連携します。これらのサービスが利用できない場合でも、Xage Brokerが内部的にLDAPをホスティングし、ユーザおよびデバイスディレクトリサービスを提供できます。さらに、Xage Brokerによって、フィールドにあるXage Gatewayが改ざんできないよう、Xage Fabricにセキュリティポリシーを引き渡します。

Xage Gatewayは、フィールドと製造現場に実装されます。油田やガス田の場合、坑井パッド上に設置されます。配電事業の場合、変電所およびフィーダに沿って設置されます。Xage Gatewayは、堅牢なコンピュータ、産業用IoTゲートウェイ（デル製）、ネットワークデバイス（Ciscoルータ/スイッチ、ABBルータ、Palo Alto Networksファイアウォールなど）および非常に軽量なコンピューティングデバイス（Raspberry Pi 3）上で動作します。

Gateway は、ホストシステムのリソースをほとんど消費しません。この分野で既存の多くのコンピューティング機器およびネットワーキング機器上で動作させることが可能です。ほとんどの場合、Gateway は 100 MB 未満のメモリしか必要とせず、わずか 10 kbps の帯域幅でナローバンドの環境で動作します。インラインフィルタリングとプロキシ処理のみが可能な Xage Enforcement Point（XEP）は、設置面積がさらに小さいため、リモートターミナルユニット（RTU）やプログラマブルロジックコントローラ（PLC）の前に設置するのに適しています。それらを多重化して複数のデバイスを処理し、冗長性のために並行して展開することができます。

情報は Xage Security Fabric 経由で双方向に流れます。認証デバイス、ユーザリストおよび特権といった識別およびその他のポリシー情報は、システムのコアにある Broker からエッジにある Gateway へ送られます。資産インベントリやデバイスプロファイルなどの運用情報は双方向に送られます。（図 1 参照）

図1：Xage分散アーキテクチャ



Xage Brokerにより、セキュリティポリシーがデータセンターからエッジへ送信されます。

Xage GatewayとXage Client（オプション）により、ブロックチェーンで保護されたセキュリテイファブリックが形成され、その中に中央サービスから独立して動作するセキュリティ情報とプライベートアプリケーションデータが保持されます。

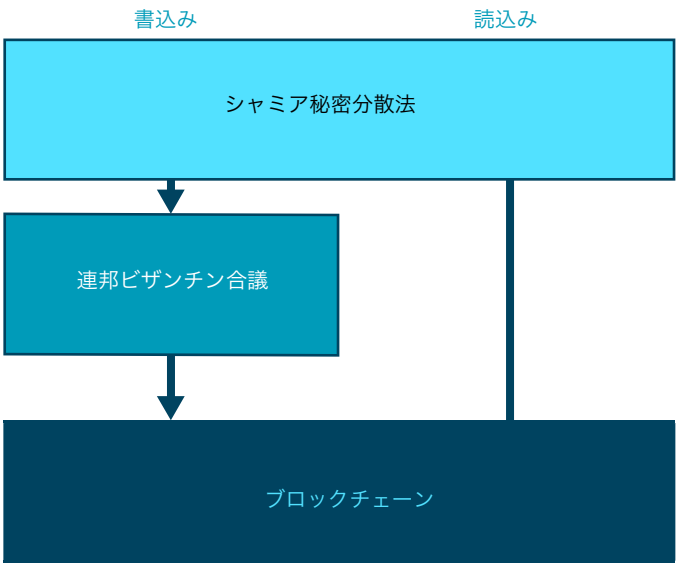
人、アプリケーションおよびデバイスは、Xage Security Fabricを介して認証およびやり取りを行います。

Xage Security Fabricを通るすべての情報は、Fabricの分散インフォメーションストアで保護されています。 3つの基盤技術により、Fabricによって保存された情報が維持されます。

- 安全で改ざんができない方法で情報を保管するためのブロックチェーン
- 承認された者だけが安全に読むことができることを可能にするシャミア秘密分散法
- 更新内容が有効かつ不変であることを保証する連邦ビザンチン合議 (FBA)

図2ではこれらの技術の関係について説明しています。

図2：Fabricで利用される技術の関係

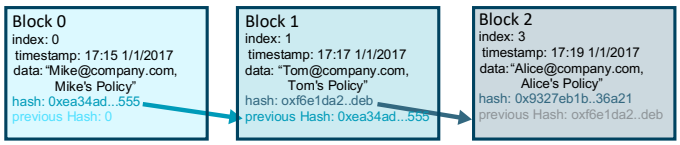


ブロックチェーン：IIoTセキュリティに最適な技術
エッジまでセキュリティを確保することが分散システムの課題となります。信頼できるかを確認することができない複数のエンティティ（エンドデバイス、制御システム、サードパーティのアプリケーション、ユーザ）がデータのやり取りを行い、他のエンティティを制御し、他のエンティティによる制御を受け入れる必要があります。改ざん防止でありながら、認証、承認、同期、プライバシーを提供できる分散システムが必要となります。

ブロックチェーン技術は、そのようなシステムのための情報基盤を提供するのに理想的です。ブロックチェーンは、暗号化を使用してリンクされているレコード（ブロック）のストアです。各ブロックには、前のブロックの暗号化ハッシュ、タイムスタンプおよびチェーンに追加される情報が含まれています。

ブロックチェーンは、検証可能かつ永続的に情報を記録する分散レッジャーを作成します。情報がブロックチェーンに追加されると、設計上、その情報を変更することは困難です。ブロックチェーンは、ブロックチェーンノードのピアツーピアネットワークによって管理されます。このネットワークは、新しいブロックの通信と検証に関する固定の規則に従います。 一度記録されたブロック内のデータは、その後のすべてのブロックを変更せずに遡及的に変更することはできません。これには、ブロックチェーンのノードの合意が必要となります。図3を参照。

図3：ブロックチェーンの例



ブロックチェーンは一般に暗号通貨に関連した技術として知られています。しかし、事前に信頼関係を確立していないエンティティから安全にアクセスできる改ざん防止分散データベースを必要とするアプリケーションでの利用に適しています。アイデンティティサービス、アプリケーション/デバイスインベントリ、デバイスプロファイル、監査ログ、ポリシーの複製/実行、ポイント間の認証などを必要とするIIoT向けセキュリティに最適です。

ブロックチェーン技術は、次のようなニーズを独自に満たすため、IIoTセキュリティに必要です。

- IDおよびセキュリティポリシー情報の改ざん防止データベースの提供
- データベース変更におけるルールの適用
- 数百万ノードまで拡張可能
- 分散アーキテクチャによる冗長性と信頼性の提供

Xage Security Fabricとブロックチェーンの関係
Xage Security Fabricを構成するXage BrokerとXage Gatewayは、ブロックチェーンネットワーク内のノードです。Fabricにはブロックチェーンを使用して以下のデータを格納されます。

- どのノード（BrokerとGateway）がFabricに参加できるかに関するFabricのトポロジとポリシー
- デバイス、アプリケーション、人およびデータのID、認証および特権情報
- Fabricを通過するセキュリティサービスデータおよびアクティビティレコード（IDグループ、ポリシー、インタラクションなど）の監査証跡

ブロックチェーン技術により、Fabricは、改ざん防止、フォールトトレラント、自己修復機能を備え、ピアツーピアのデータ複製を使用して更新されます。

- 改ざん防止：各ブロックに格納されているハッシュと、ブロックを変更するために必要なコンセンサスにより、Fabricが改ざんされることはありません。
- フォールトトレラント：各ノードにはブロックチェーンまたはサブチェーンのコピーが保存されます。シャミア秘密分散法と連邦ビザンチン合議により、一部のノードで障害が発生しても読取りと書込みが可能になります。
- 自己修復：ノードが危険にさらされた場合、Fabricによって、不正ノードが検出されたことが通知され、そのノードは隔離され、必要に応じて修復されます。
- ピアツーピアのデータ複製：バッテリ使用時や海で使用するアプリケーションの場合のように、データセンター内のノードと通信できない場合でも、ノードのサブセットを使って、ローカルでブロックチェーンまたはサブチェーンを更新できます。

Xage Security Fabricはサブチェーン付きの階層デザインを使用しています（図4参照）。Gatewayには必要な情報のみが保存されます。階層デザインにより、スケーラビリティが向上するとともに、処理時間を軽減することが可能となります。データのサブセットのみがサブチェーンに格納され、サブチェーン内で合意が得られるためです。IIoTのブロックチェーンを実装するために不可欠なこの最適化により、ミリ秒単位のレコード更新が可能となり、データストレージ要件が軽減されます。

サブチェーンは、場所、プロセスおよび組織ごとにデータを分割します。
知る必要のある場合にのみ情報を提供することにより、セキュリティは強化されます。階層を上に移動すると、最上位レベルのノードにマスターブロックチェーンが格納されるまでサブチェーンが集約されます。

シャミアの秘密分散法の基礎
シャミア秘密分散法では、秘密情報は複数のパーツとして分解されます。それぞれの参加者は固有のパートを受け取るのみです。元の秘密情報を復元するためには、最低限のパーツまたはしきい値が必要となります。しきい値の数はパーツの総数よりも少なく、設定することが可能です。参加者の任意のサブセットによって、元の秘密を復元することができるようになります。

シャミア秘密分散法の数学的根拠は、n個のサンプルが次数n-1の多項式を定義するのに十分であるという多項式の性質になります。多項式$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots a_{n-1}x^{n-1}$がある場合、少なくともn個の$(x, f(x))$のペアを持っていれば、秘密$a_0$を解くことができます。

Xage Security Fabricとシャミア秘密分散法の関係
Fabricは、指定された数のノードが要求されたアクセスが許可されることに同意した場合にのみアクセスを許可する方法でブロックチェーンを格納します。シャミア秘密分散法によって、この流れが実行されます。

図4：階層とサブチェーン

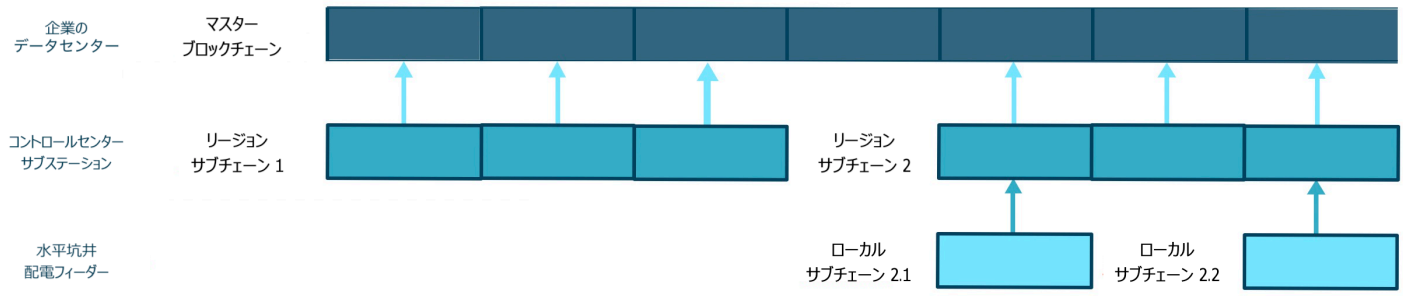
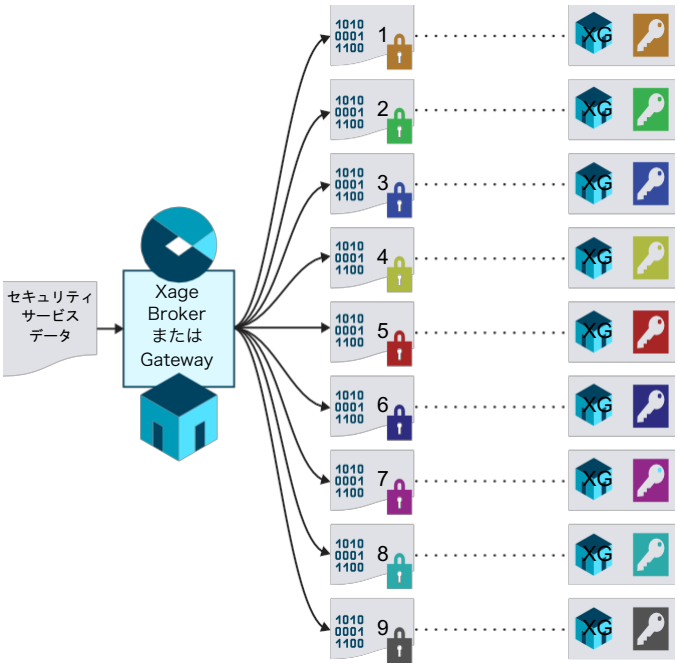


図5：秘密の共有



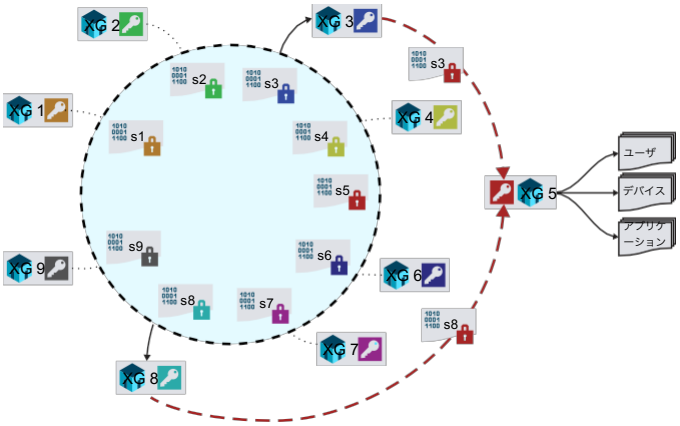
9つのGateway間で秘密を共有する例については、図5を参照してください。 この例では、BrokerまたはGatewayは2次多項式の座標(x, f(x))をGatewayに安全に配布します。

図6のXG 5のようなノードが情報を必要とする時、シャミア秘密分散法が使用されます。秘密は2次多項式を使用して共有されます。XG 5が情報を読み取るためには、3つの座標（自分自身に加えて2つの座標）が必要となります。XG 5は、他のブロックチェーンノードへ座標を要求します。XG 3とXG 8が応答することで、XG 5は必要となる3つの座標を入手し、情報が提供されます。

連邦ビザンチン合議の基礎

連邦ビザンチン合議 (FBA) とは、情報が受け入れられ、恒久的な記録にコミットされる前に、情報の一部が有効であることをシステム内の信頼できるノードの大多数が合意することを保証する合意プロトコルです。FBAは、オープンメンバーシップとシステムの系統だった成長をサポートしており、IIoTアプリケーションに最適です。

図6：秘密の入手



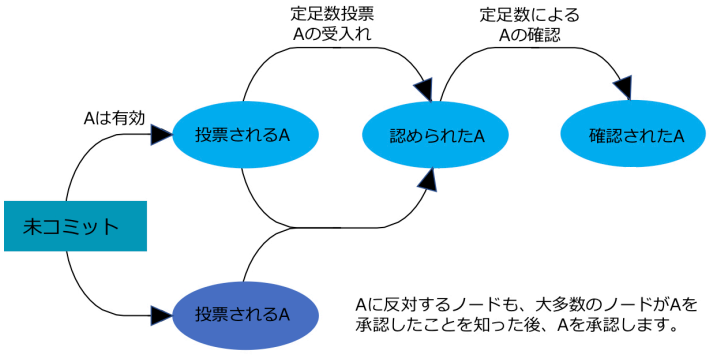
FBAでは、各ノードはそれが重要だと考える他のノードを知っています。情報を受け入れて記録する前に、他の大部分のノードが何らかの情報が有効であることに同意するのを待ちます。代わりに、それらの重要なノードは、彼らが重要であると考えるノードが同様に同意するまでその情報が有効であることに同意しません。最終的に、ネットワークがトランザクションを受け入れることは大変厄介なことになり、これに攻撃者が対抗することは不可能になります。そうなって、ようやく初めて参加者は情報を受け入れて記録します。

既存の重要なノードの大多数が合意すれば、新しいノードはネットワークのメンバーシップリストを更新するための一元化された権限を必要とせずにネットワークに参加できます。既存の重要なノードは、以前にブロックチェーンにコミットされたポリシーに基づいて決定を下します。これによりシステムの系統だった成長が可能になります。柔軟なメンバーシップにより、一部のノードが脱退してもネットワークは合意に達することができます。

Xage Security Fabricと連邦ビザンチン合議の関係

Xage Security Fabricは、ノードが書き込みを行うときにブロックチェーンの整合性を確保するためにFBAを使用します。例えば、GatewayがIIoTデバイスを資産インベントリに追加する必要がある場合、FBAを使用して、重要と見なされる他のノードへの追加を提案します。次に、これらのノードは、提案された追加がシステム全体に伝えられるまで、それらが重要であると考える他のノードへの変更を提案します。

図7：FBAで合意に達するまで



ノードは提案された追加を受け入れるか拒否するか、3段階のプロセスで投票します。図7を参照してください。Xage Security Fabricでは、このプロセスは階層的に実行されます。Fabricは、ファブリックのトポロジーに基づき、クォーラムと呼ばれる最適な承認者のセットを自動的に決定します。例えば、Xage Fabricは、ローカルのGateway、ローカルおよびリージョンのGatewayまたはローカルおよびリージョナルのGatewayとデータセンターにあるBrokerを定足数として選択します。

Xage Security Fabricのノードは、いくつかの理由で提案された変更を拒否することに投票するかもしれません。変更を要求しているGatewayはその特定のデバイス、ユーザまたはデータに変更を加えることを許可されません。その変化は、階層内の他のGatewayによってチェックされておらず、この変更はブロックチェーンのハッシュ構造などに反しているからです。

このプロセスが完了した後に初めて、提案された追加は、ブロックチェーンにブロックを追加することによって書き込まれます。ノードは投票を変更すると投票を変更できないため、追加が確認された後は不変です。

FBAでは、プルーフオブワークやプルーフオブステークスではなく、プルーフオブオーソリティに基づき機能します。プルーフオブワークシステムおよびプルーフオブステークスのシステムでは、大なり小なりマイニングに依存しています。マイニングにはかなりの処理能力と記憶容量が必要なため、IIoTでの使用には適していません。FBAで使用されるプルーフオブオーソリティシステムは、ほとんど計算能力とメモリを使用せずに、ブロックチェーンの有効性と不変性を保証します。Xage Gatewayで必要となる計算能力が最小限に抑えられるため、IIoTに適しています。

Xage Security Fabricの保護

未承認または侵害されたBrokerまたはGatewayが参加するのを防ぐことで、Xage Security Fabricは保護されます。最初にノードが参加しようとすると、そのフィンガープリント（ファームウェア、ソフトウェア、ファイルシステムなど）がチェックされ、承認され、妥協されていないことが確認されます。Fabricに保存され保護されているポリシーに従ってプロビジョニングする必要もあります。ノードがこれらのチェックに失敗した場合、参加は許可されません。

ファブリックに参加した後、周囲のノードから情報を要求しているノードは、その身元を確認するように求められます。 それができない場合は、Fabricからは削除され、Xage Policy Managerに通知されます。

同様に、不正なノードがブロックチェーンに書き込もうとすると、周囲のノードは自分自身のブロックチェーンのコピーを参照して、変更が許可されていることを確認します。許可されていない変更は周囲のノードによって拒否されます。不正ノードは、ブロックチェーンを更新するために必要なコンセンサスを生成できません。FabricはManagerに通知し、不正ノードを隔離し、必要に応じてクリーンにワイプして再同期することで修復します。

Xage Security Fabricのサービス

Xage Security Fabricにより、IIoT内でのアイデンティティ・アクセス管理の実施、強化のためのサービスが提供されます。各認証およびアクセス要求を処理するために中央リソースと通信する必要があるエンタープライズIDおよびアクセス管理システムとは異なり、Xage Security Fabricではこれらのサービスを配布します。Fabricは、ローカルにコアからエッジまでシステム全体に渡る認証とアクセス制御を提供します。ポイントソリューションとは対照的に、FabricはIIoT全体のセキュリティを自動化して実行の一貫性を保証します。

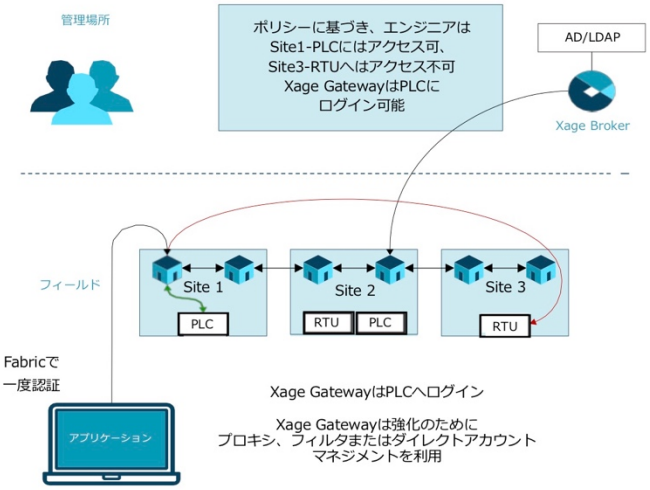
ロールベースのアクセス制御 (RBAC) の強化

Xage Security Fabricは、デバイスの基本機能つまりデバイスが管理パスワード、ローカルパスワードまたはパスワードなしをサポートしているかどうかにかかわらず、ユーザの管理IDに基づきロールベースのアクセス制御 (RBAC) を適用します。図8を参照してください。

次の3つの機能を使ってFabricはロールベースのアクセス制御 (RBAC) を実行します。

- アプリケーションのプロキシ実行
- インラインフィルタリング
- ダイレクトアカウント管理

図8：Xageにおけるロールベースのアクセス制御



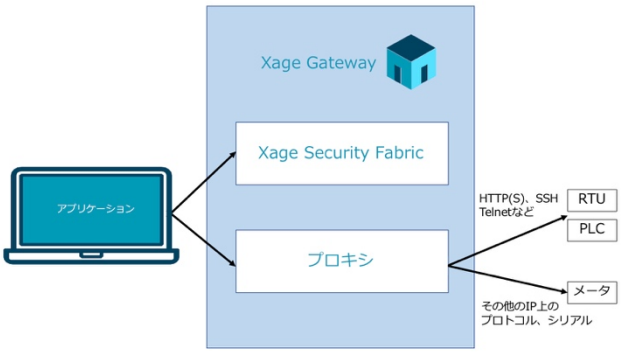
パスワードを利用できるデバイスの場合、Xage Security Fabricはアプリケーションプロキシとして機能することによってロールベースのアクセス制御 (RBAC) を実行します。 信頼できるユーザとアプリケーションだけがIIoT内のデバイスと通信できるように、すべてのアプリケーション接続とセッションをプロキシします。Fabricは自動的に暗号化された安全なデバイスパスワードを設定および保存し、デフォルトパスワード、紛失パスワード、共有パスワード、または盗まれたパスワードを利用不可とします。パスワードは複雑で、隠されており、Brokerで定義されたポリシーに従い、定期的に変更することができます。図9を参照してください。

Xage Security Fabricはインラインフィルタリングもサポートしています。これは、パスワードやその他のアクセス制御メカニズムなどのサポート機能に関係なく、すべてのデバイスにRBACを適用することができます。対話を許可されているデバイス、アプリケーションおよび人だけが通信できます。許可されていないデバイスによる接続試行は、攻撃者がネットワークにアクセスできることを示す可能性があるため、フラグが立てられます。 図9を参照してください。

Fabricは、WindowsおよびLinuxシステムのダイレクトアカウント管理を実行することもできます。ドメインコントローラを利用せずに、セキュリティポリシーに従って、アカウントの作成、変更、削除を自動化することができます。

人に対しては、Xage Security Fabricにより、ポリシーによって許可されたアクセスのみを許可し、アクセスを指定された地域の承認されたデバイスおよびアプリケーションのみに制限します。

図9：プロキスならびにインラインによる強化



FabricのRBAC機能は、悪意のある行為を働く者の検出に役立ちます。例えば、古くなったパスワードやポリシーに反する過度のログインを試行するマルウェアを発見し報告することができます。

デバイス、アプリケーションおよび人の検出
デバイス、アプリケーションおよび人がIIoTへの接続を要求した時に、Fabricにより、それらが検出され、保管されます。ModbusやDNP3などの選択されたプロトコルに対する受動的なネットワークベースのチェックおよびアクティブスキャンに基づいて検出されます。人の場合は、ログイン試行が監視されます。不正な資産がIIoTコンポーネントにアクセスするのを確実に阻止するために、検出はエッジで行われます。

デバイス、アプリケーションおよび人の信頼の管理
Xage Security Fabricは、以下のようなシステムと連携して信頼を管理します。

- Active Directoryとのグループおよび認証情報の共有を含む、Active Directory、LDAP、およびRADIUSなどのディレクトリおよび認証サービス
- 認証当局
- SAPなどの資産管理システム

デバイスとアプリケーションごとに、Fabricにより、証明情報（存在する場合）とフィンガープリントが保存されます。フィンガープリントには、ハードウェア、ソフトウェア、ファームウェアの識別子、一般的なメモリの使用、構成とレジスタの設定、ファイルシステムのハッシュなどの情報が含まれています。それらは証明書を強化し、固有の識別情報を保管することによって証明書がない資産に対する信頼を生み出します。Fabricでは、有効な証明書（使用可能な場合）と一致するフィンガープリントを持つデバイスとアプリケーションだけがシステムに参加できます。

Fabricは、侵害された資産を検出するために、フィンガープリントとパスワードを再確認します。フィンガープリントが不正に変更された場合、その資産は改ざんされたことになります。Fabricは、侵害されたデバイスまたは資産を隔離して通知します。パスワードが変更された後に古いパスワードが使用された場合、それは盗まれたことを意味し、Fabricは侵入の試みがあったことを報告します。

人の場合、Fabricは信頼を確立するためにADまたはLDAPを使用します。ユーザID管理と信頼作成を強化するためには、Fabricでは多要素認証がサポートされています。

自動プロビジョニングの有効化
Xage Security Fabricでは、デバイスの自動プロビジョニングをサポートしています。デバイスが現場に設置されると、Fabricは自動的に登録されたデバイス証明書、フィンガープリントまたは利用可能なものに応じたシリアル番号を使用してデバイスの信頼性と所有権を検証します。

認証と承認の後、デバイスとアプリケーション向けに、システムの他の部分と連携するために必要なサービスに登録するために必要な追加の証明書が発行されます。例えば、電力会社では、スマートメーターを利用するためには、サブステーションシステムによって提供されるサービスに登録する必要があるかもしれません。

Fabricは、ブロードバンドの場合、HTTPSを介したSCEP、ナローバンドの場合、CoAP-DTLSを介したESTを介しての登録をサポートしています。キーと登録方法は、802.1xと同様のシステムと互換性があります。

Fabricは、エッジでの証明書失効リストなどの失効サービスをサポートしています。分散型の失効サービスは、コアへの通信が中断された場合でも、迅速なアクションを可能にし、ポリシー適用が可能です。

自動キー管理
多くのIIoTデバイスは、信頼性とユーザからアプリケーションまたアプリケーションからデバイスへの通信を保証するためにキーまたは証明書を使用します。 世界中に何百万ものIIoTデバイスが展開するために、効果的で分散型の利用しやすいキー管理ソリューションが求められています。

複数の製造施設や顧客サイトに鍵を配布および管理するために、Xage Security Fabricによって、非常にスケーラブルで安全で自動化されたアプローチが提供されます。Fabricは、複数サイトへの鍵配布を自動化し、デバイスのバインド、複数の同時アプリケーション、集中管理、および監査証跡の作成をサポートします。

変更のトラッキング、コンプライアンスの文書化
Fabricは、資産のインベントリとプロファイルの変更、デバイス、アプリケーションおよび人によるアクセスの試行を、成功したかどうかにかかわらず自動的に追跡し、監査ログを作成します。ブロックチェーンとFBAによって、ログが有効で、改ざん防止され、不変であることが保証されます。監査ログには、NERC-CIPを含む重要なインフラストラクチャセキュリティのための進化する規制および規格への準拠が文書化されています。

複数当事者間のデータのプライバシーと整合性の保護
Xage Security Fabricでは、IIoTにおける複数の当事者、例えばサプライチェーンのメンバーである異なる会社によって共有されるデータのプライバシーおよび完全性が保護されています。データの作成者または所有者は、データのアクセスポリシーを制御し、例えば、どのアプリケーションと人がデータを読み取りまたは変更できるかを指定します。Fabricは、アクセスポリシー、ハッシュ、および暗号化キーを安全に複製し、改ざんできないようにして、その内容を複数の当事者全体に適用します。

Xage Policy Manager

Xage Policy ManagerはXage Security Fabricを管理し、サイバーセキュリティを自動化します。 セキュリティポリシーを設定し、単一の自律型ダッシュボードからIIoT内のすべてのアセットとユーザのセキュリティパラメータを複製します。例えば、定義された時刻表とポリシーに従って複雑なパスワードを変更することができます。

管理者はManagerを使用して、デバイス、アプリケーションおよび人のグループを作成し、これらのグループがどのように相互作用するかを規定できます。Xage Security Fabric全体を一元管理することで、ネットワークおよびシステム管理者の生産性と正確性が向上します。

また、ManagerはNERC-CIPを含む重要なインフラストラクチャセキュリティに関する新たな規制やポリシーへの準拠を自動化し、確実にします。コンプライアンスの重要な部分は、ログの維持と監査証跡の作成です。Managerはブロックチェーンを使用して重要な履歴情報を自動的に保存し、それが有効かつ不変であることを確認します。

Xage Policy Managerは、Fabricのデータプレーンまたはコントロールプレーンからは独立しています。Managerに障害が発生したり、Fabricとの通信が途絶えた場合でも、Fabricは中断することなく完全に動作し続けます。

まとめ

Xage Security Fabricは、独自の方法でIIoTセキュリティのニーズを満たします。セキュリティポリシーと運用情報のために、プライベートで分散型、堅牢で改ざん防止されたインフォメーションストアが作成されます。インフォメーションストアは、ブロックチェーン、シャミア秘密分散法および連邦ビザンチン合議を使用して実装されています。

Xageは、デバイス、人そしてデータ間の安全な相互作用のために不可欠な信頼できる基盤を作り出します。Xageは、従来のセキュリティモデルを超えて、認証とプライベートデータをデバイスのネットワーク全体に分散させ、通信、認証および信頼のための改ざん防止ファブリックを作成し、大規模なセキュリティを保証します。

Xage Security Fabricは、複数対地間通信をサポートし、既存の産業用システムへのアクセスを保護し、断続的な接続に直面しても継続的なエッジコンピューティング操作を支えます。

Xage Security Fabricのポリシー適用と安全で不変の情報ストレージの組み合わせは、IIoTセキュリティだけでなく、新たなサイバーセキュリティ規制および標準への準拠を実証するのにも理想的です。

Xage Security Fabricに関するより詳しい情報は、ウェブサイトwww.xage.comをご参照いただくか、hello@xage.com宛にメールにてご連絡ください。