CENEMO(CErtificated Network Model)

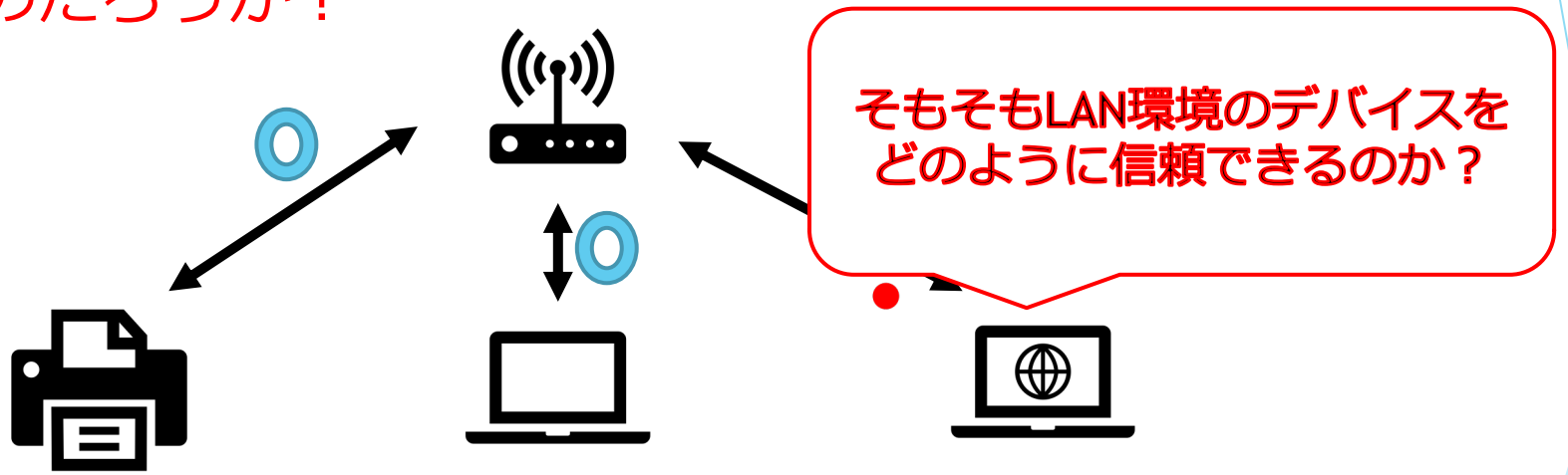
制限されたL２層と
統合型証明書による仮想L３層
を利用した安全なLANネットワーク

Limited L2 and Managed
Certificated Secure Virtual L3

HunsLaB

従来のLANアクセス環境

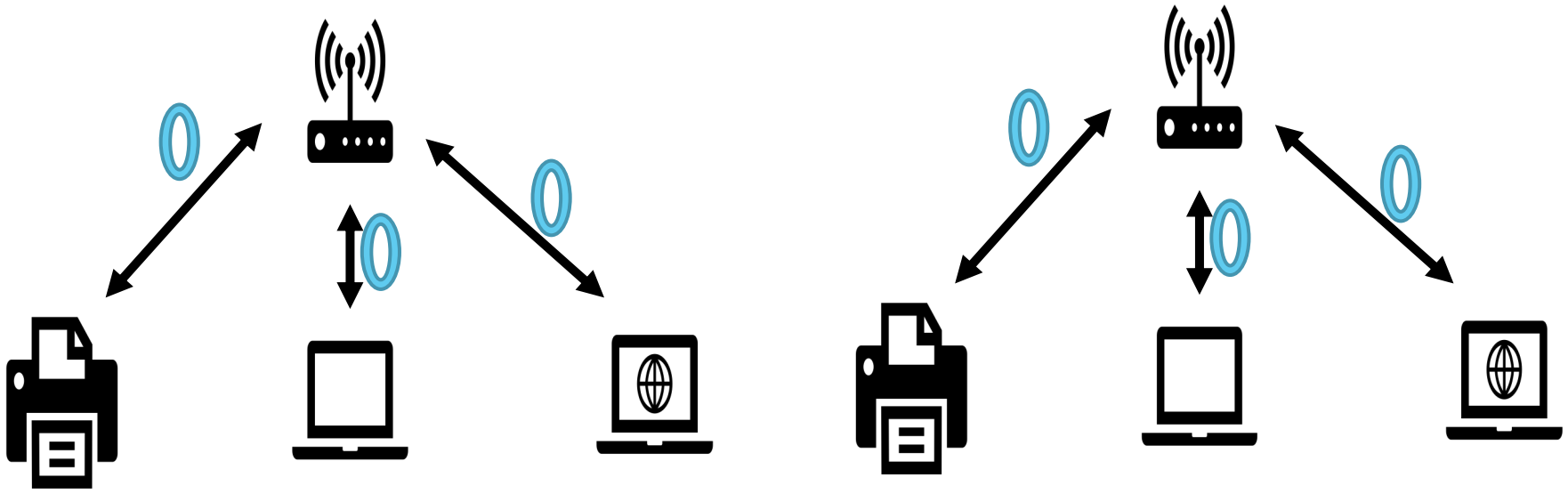
フラットなL2 LANネットワークでは安全なネットワークの分離が行えない為、ハードウェアによるL3環境などを構築し、接続できるデバイスをMACアドレスで制限を加えている。ではLAN環境に接続されるデバイスは誰がいつ認証しているのだろうか？



LAN環境に接続できるデバイスをMACアドレスや無線認証で制限している

従来のLANアクセス環境

複数のネットワークを構築する場合には、APを分離しそれぞれを別セグメントで利用する方法などを考えることになる。



営業部　　技術部

分離させるためには、それぞれの管理が必要、
またAPもそれぞれに用意しなければならない。

従来のLANアクセス環境

管理する側の負担

1. 利用者の管理
   LDAPやADサーバへの登録

2. ハードウェアの管理
   利用者のハードウェア情報の管理（MACアドレス）
   APの管理
   L3デバイスの管理

3. 維持管理
   高コストであるL3デバイスの保守、交換

従来のLANアクセス環境

LAN環境に接続できてしまうと、LAN環境内で制限なく通信が行えてしまう。

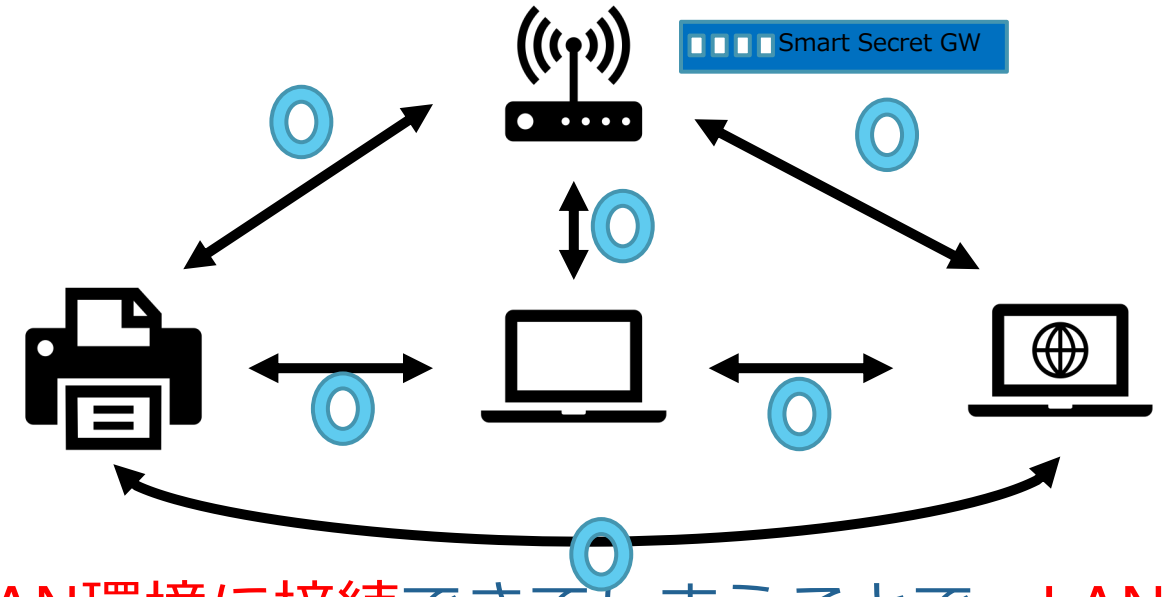
1. 有線ネットワーク
   居室に入り接続されてしまうと。。。。

2. 無線ネットワーク
   暗号方式に脆弱性が発見されてしまうと。。。

1. 一旦、LAN環境に入れてしまうと重要なデータにアクセスできる権限を与えてしまっていることで起きる問題。
2. LAN環境内には、FWが存在しない。
   ネットワーク感染の問題が必ず残る。

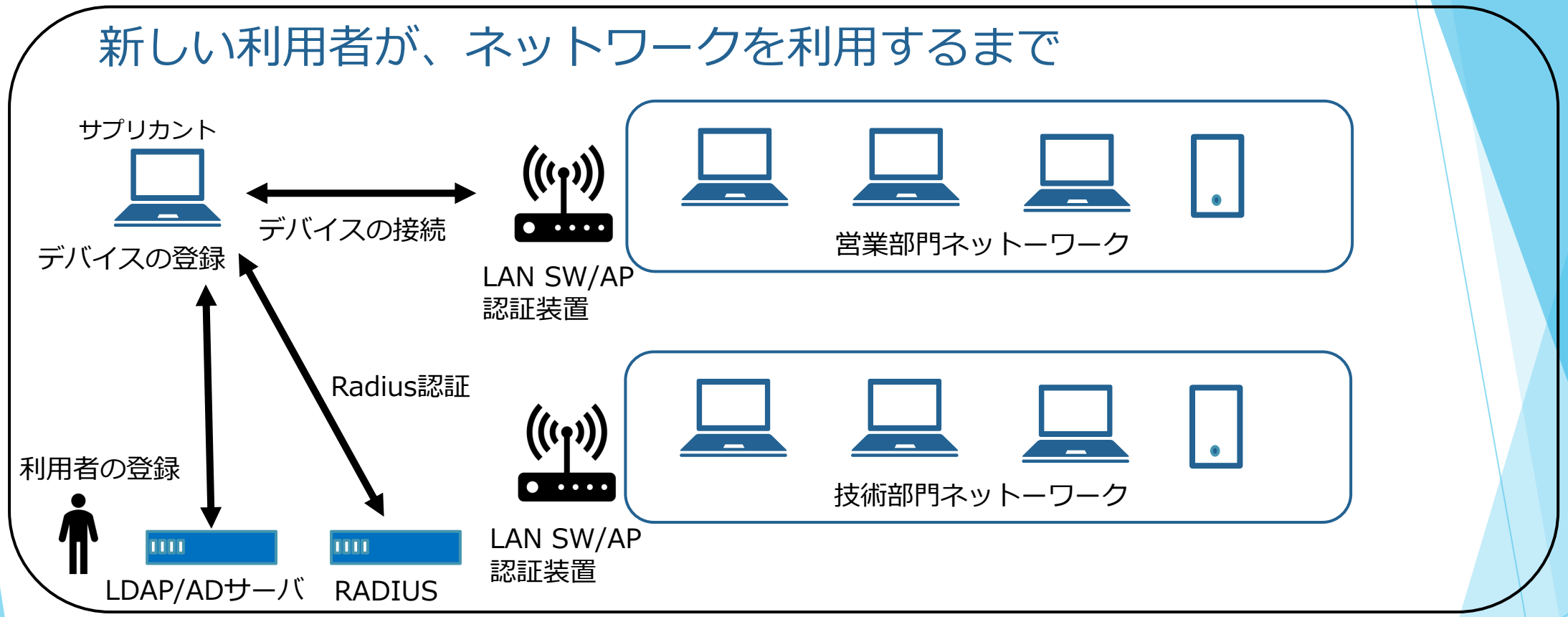
従来のLANアクセス環境

LAN環境とは、相互に通信して良いデバイスが利用できる。
ゆえに、その前段として通信してはいけないデバイスを選別する。という方式



一旦LAN環境に接続できてしまうことで、LAN全体へのアクセス権限を持ててしまう設計となっている。
果たして、この方法で良いのだろうか？

従来のSecure LANアクセス環境



1. IEEE802.1X認証を行うためにはサプリカント、認証装置、認証サーバの3つの構成要素が必要。設定や運用管理が煩雑になる。
2. 複雑で、高価なハードが必要になり運用保守も膨大に。

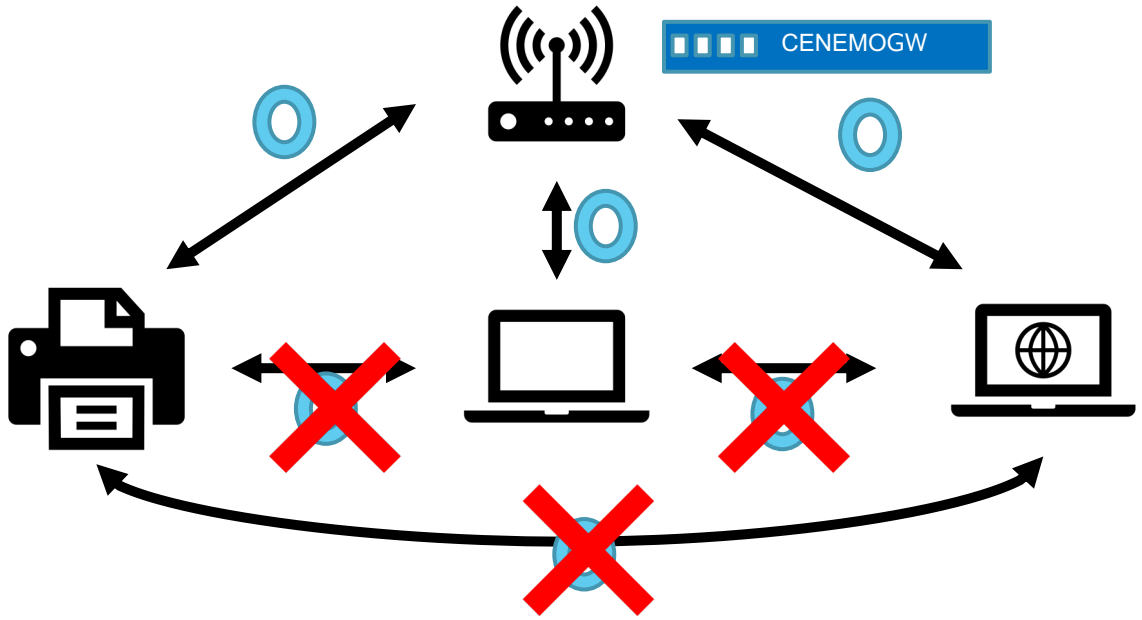
CENEMO(CErtificated Network Model)

限定されたアクセスがベース
証明書によって仮想ネットワークに接続
接続時は全てのトラフィックが暗号化
　LAN間通信が盗聴ができない
MACアドレス認証は不要
LDAP/AD連携によって証明書を自動配布可能
暗号強度のビット数を変更可能
スケーラビリティに対応

HunsLaB

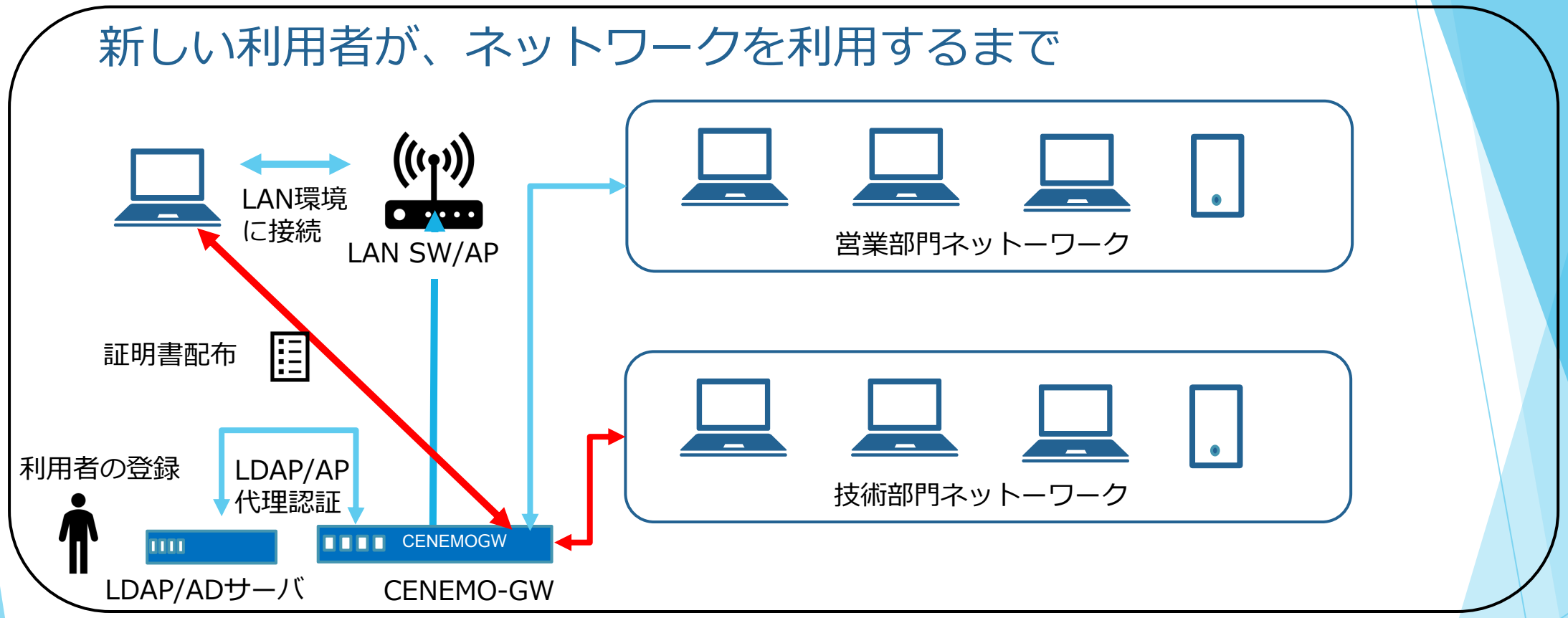
制限LAN機能　IOT,持込デバイスのアクセス制限

新らしいLAN環境とは、LAN環境を信頼しない。
ゆえに、通信してはいけないデバイスが接続されても
良いようにネットワークを利用した活動を禁止させる。



WiFiのアクセスポイントの標準機能であるプライバシー
セパレーション機能、LAN環境であればインテリSWを利用

CENEMOが提供するSecure LANアクセス環境



1. 利用者は制限LANに接続
2. CENEMO-GWのLDAP/AD認証画面から代理認証
3. 認証成功なら利用者毎にリアルタイムに証明書を発行
4. 利用者はその証明書で特定の仮想ネットワークに接続
5. 接続後は全てのトラフィックを暗号通信化
6. RADISや高価な認証SWやAPが不要

CENEMO Agent
(CErtificated Network Model Agent)

EndPointであるクライアントにインストールすることで、LAN環境から接続されるデバイスの特徴を元に、仮想ネットワークへの接続を許可したり、また禁止したりすることができます。
例えば、バックドアが作られているデバイスを検知できます。また証明書と連動させることで証明書をコピーされたりした場合でもその検知を行い仮想ネットワークへの接続を拒否することが可能になります。

HunsLaB

CENEMO Agent
(CErtificated Network Model Agent)

ローカルドライブ上に置かれたファイルの更新状況をリアルタイムで追跡し、不審な作業を検知し、該当プロセスを強制的にサスペンドを実施します。
例えば、オフィスドキュメントを更新できるのは、オフィスアプリとエクスプローラーだけであるとルールをもとに、不正なランサムウェアの活動を即時に検知が可能です。日常の作業ベースを学習することで、第三者がパソコンを利用している状況を検知し、ログオフを強制的に実施します。

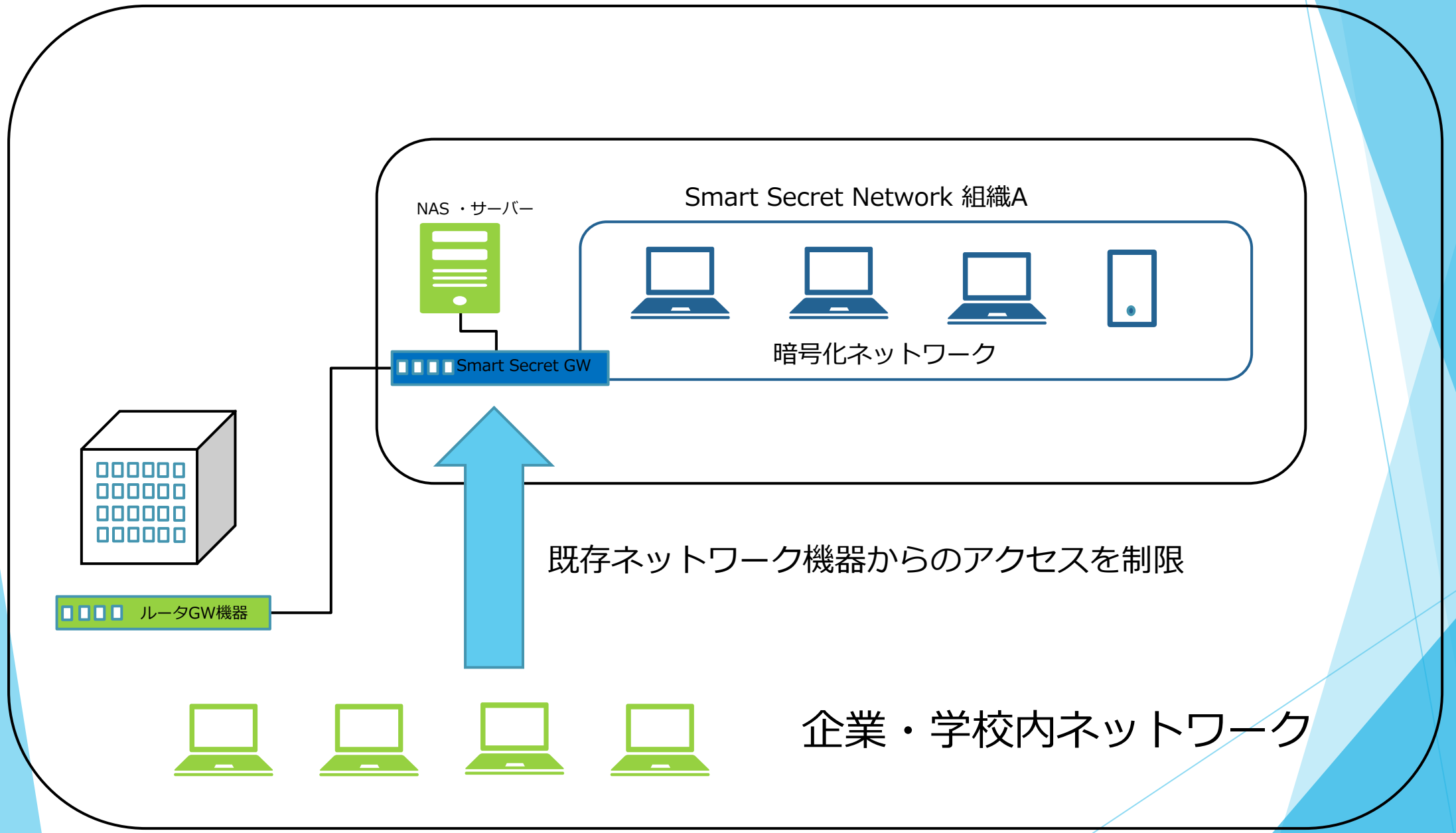
HunsLaB

Agentとコラボレーションすることで可能に

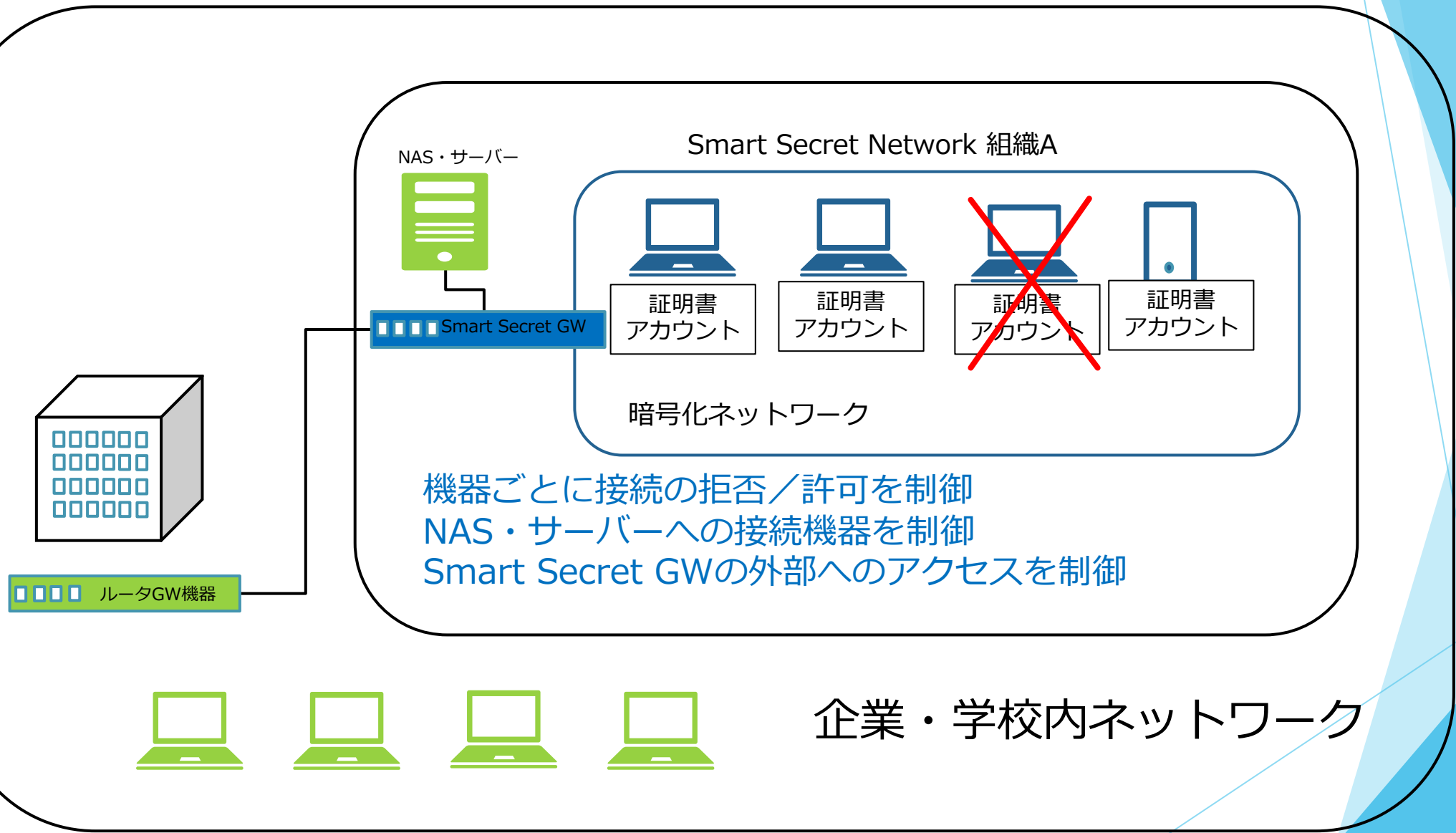
1. 利用状況を自動学習することで、異常状態の検知を行います
2. 複数のNICの利用など、情報漏洩する可能性を検知します
3. オフィスドキュメントの作業頻度から異常を検知します
4. CENEMO-GWと連携しリスクのある通信を検知します

1. 利用環境の変化をネットワーク内のデバイスと情報を共有します。
2. ネットワーク内のエンドポイントで起きている事象を共有します。
3. ウィルスに感染しても影響範囲を局所化することが可能です。

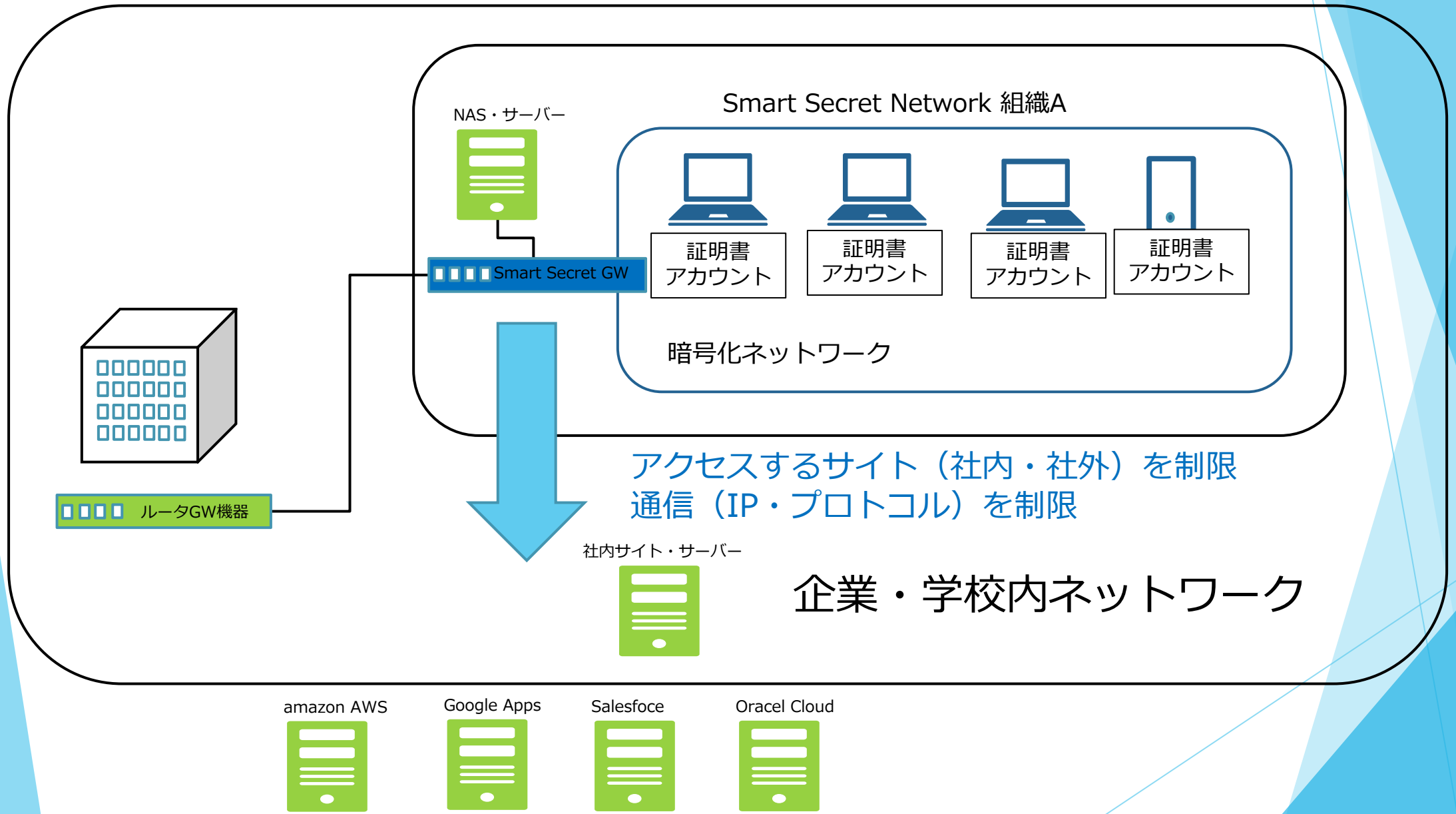
既存ネットワークからの通信を制限



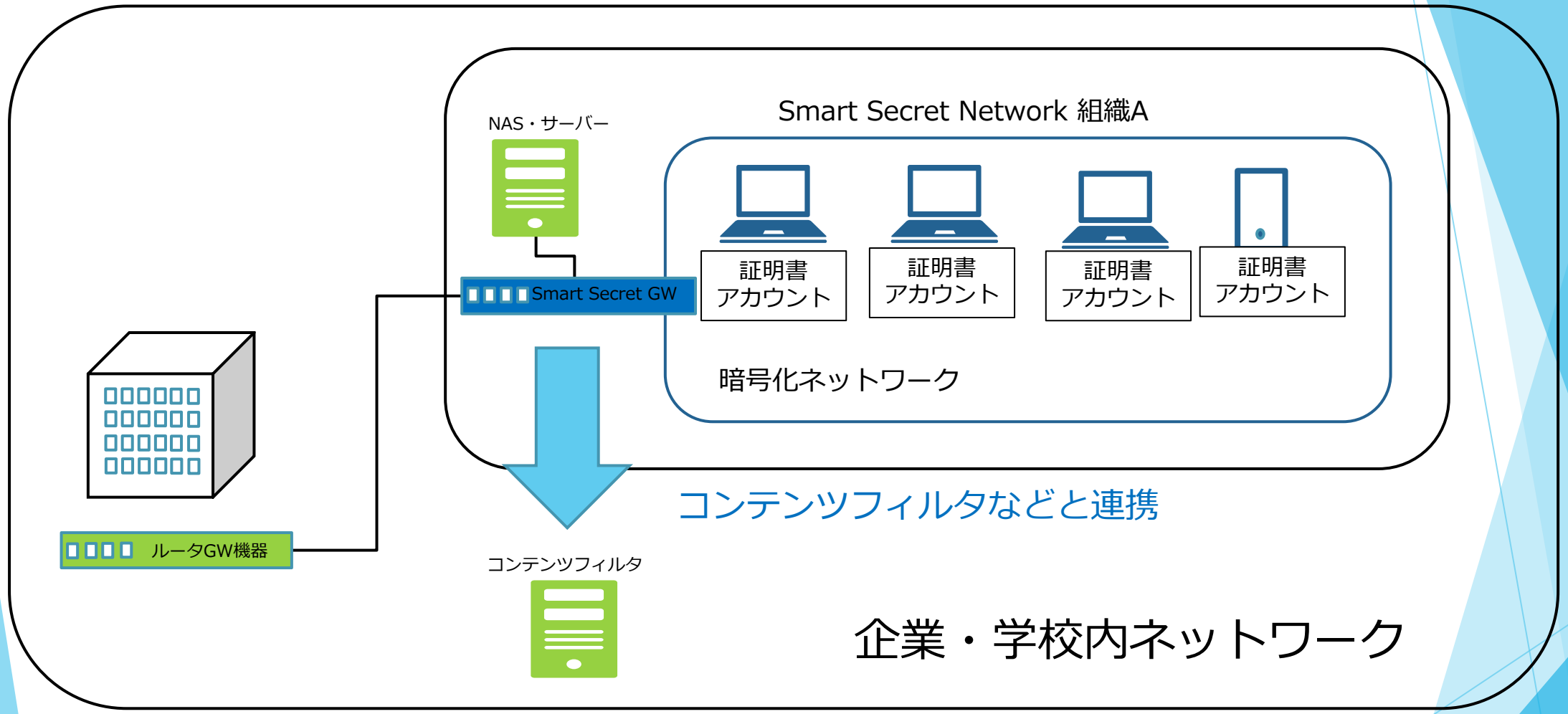
デバイスまたはユーザをSSL証明書で管理、制限



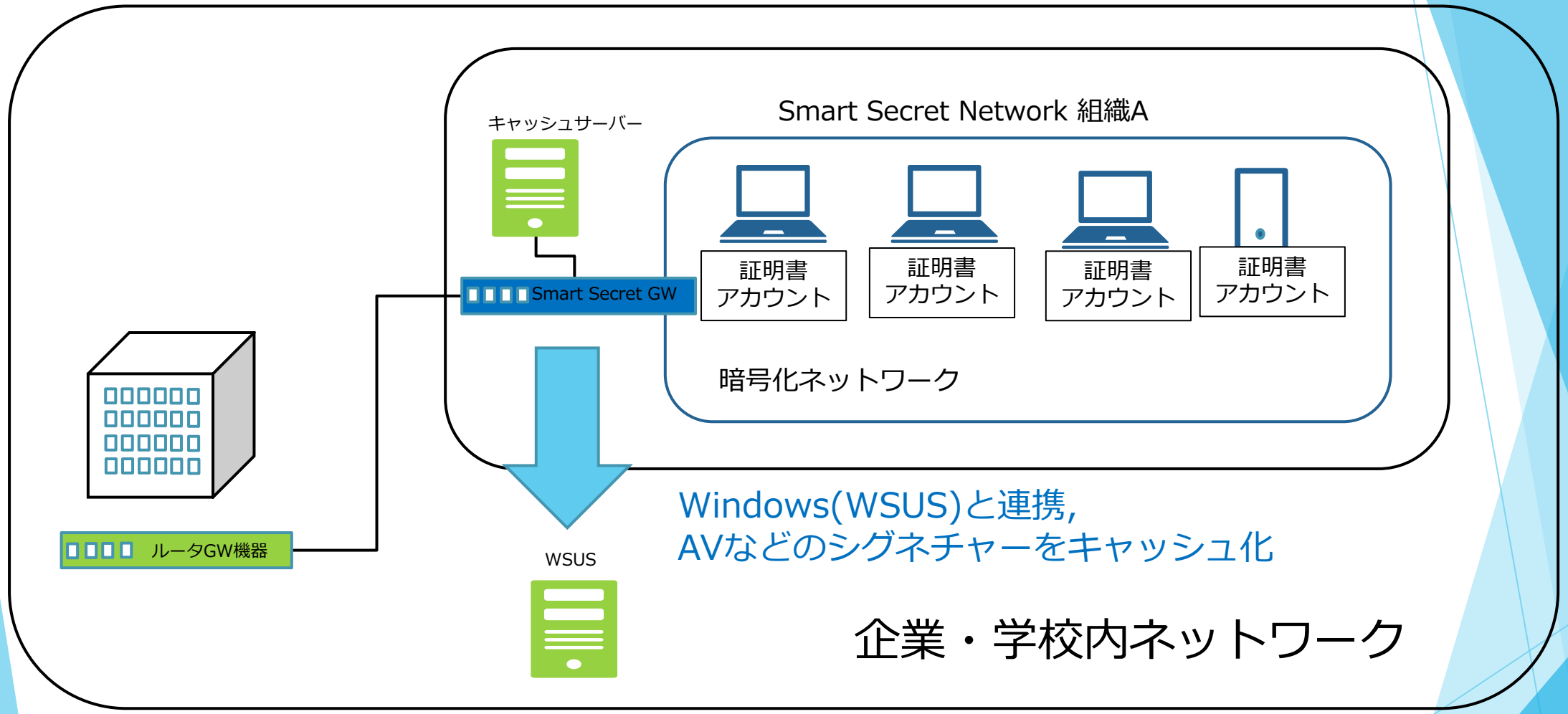
アクセスするサイト、通信（IP,プロトコル）を制限



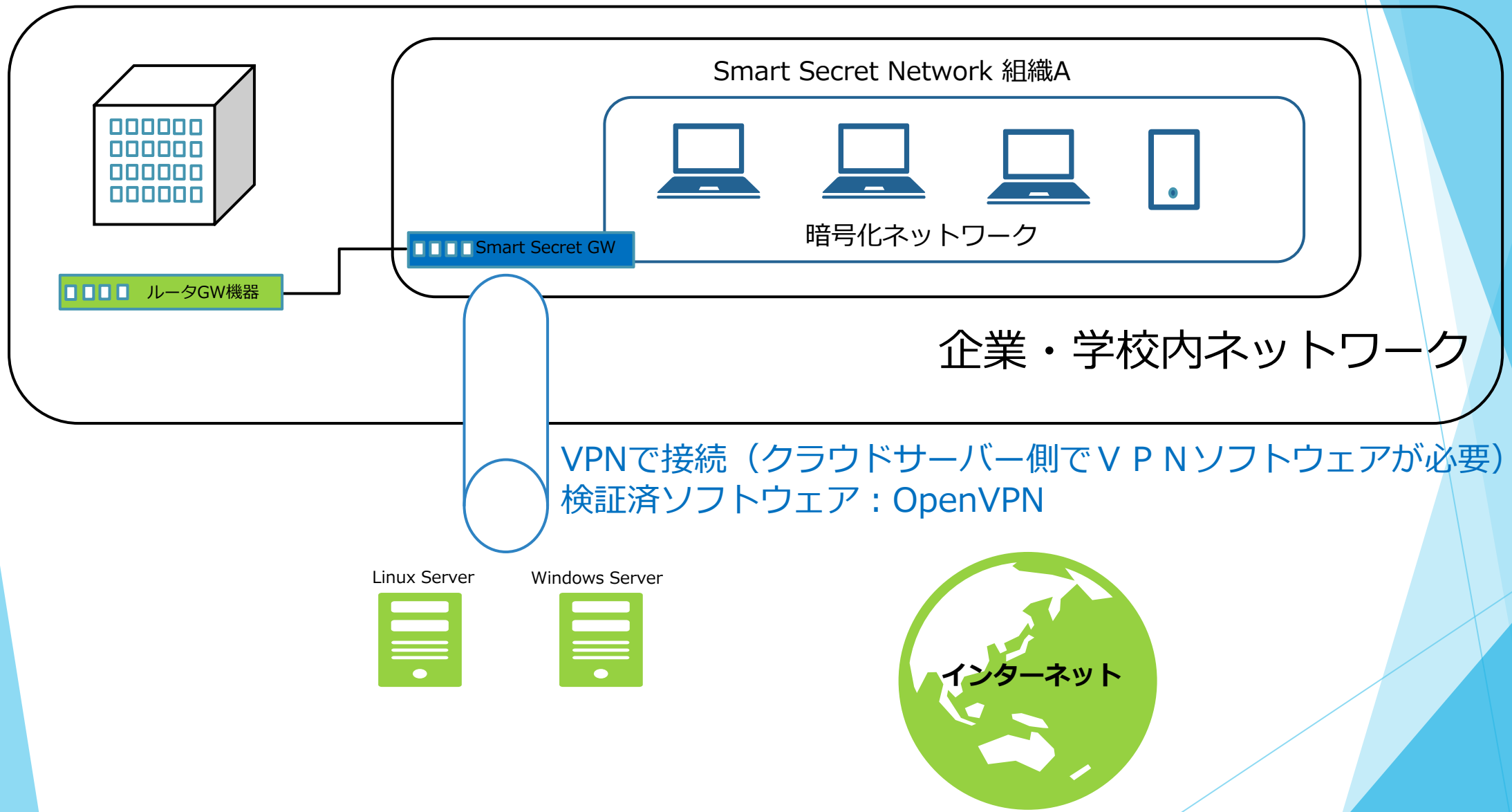
コンテンツフィルタなど、他のセキュリティと連携



WindowsUpdate(WSUS)など帯域制御とキャッシュ化



クラウドサーバー間ＶＰＮ接続



Smart Secret GWの設定の自動配信

Smart Secret Managerからの設定変更を自動配信
全Smart Secret GWへ一括配信
特定のSmart Secret GWへ個別配信

利用者アカウント制御

Ｗｅｂ画面による利用者追加
ＡＰＩシステム連携による利用者追加

Smart Secret Network for Secure LAN

Thank You

HunsLaB