特定端末からサーバアクセスするセキュリティ技術

佐賀県工業技術センター　生産技術部　福島章吾　辛川洋介

背　景

図１に示すようなシステムで生産設備等の状況を遠隔監視するにあたり、時間や場所を問わず利用できるインターネット環境のクラウド上に監視用サーバを構築する。この時、監視用サーバへは特定のPCやスマートフォンなどの端末からのみアクセスすることを想定している。そこで、悪意のある第三者による不正アクセスを防止するため、インターネット環境における特定の接続端末からのアクセス制御方法について検討を行った。

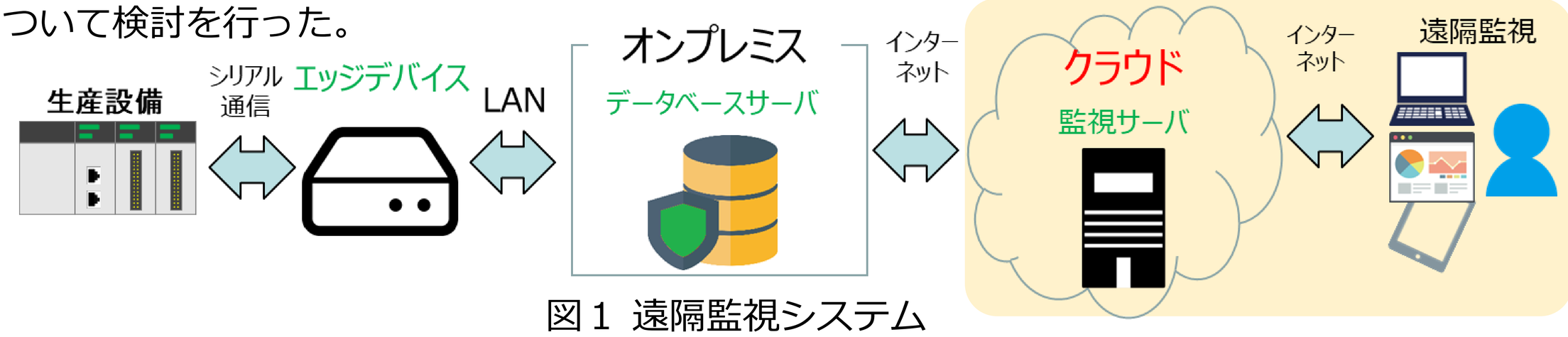

図１　遠隔監視システム

成　果

表1にクラウド上に構築した監視サーバの構成を示す。遠隔監視を行う端末から監視制御サーバにアクセスすると、WEBサーバが受信しAPサーバで処理した後、遠隔監視端末へWEBページを返す仕組みである。

表1　クラウド上の監視サーバの構成

構築環境	VPS
OS	CentOS 7.9
WEBサーバ	nginx
APサーバ	Django 3.2.10

①クライアント証明書による特定端末の接続

監視サーバ内に特定の端末のみを接続許可を行うため、クライアント証明書による認証を行った。

クライアント証明書をインストールした接続端末から監視制御サーバにアクセスしたとき、WEBサーバがクライアント証明書の整合性を確認し、整合できればアクセスを許可する（図２①）。

②IDとパスワードによる認証

IDとパスワードによる認証を行うことで、より強固なセキュリティ制御を構築した。証明書により接続できた特定の端末から、ログイン画面を経由しID認証できたとき、WEBページへアクセスされる（図２②）。

③ 暗号化による通信

インターネット環境を経由したアクセス制御において、第三者による盗聴、改ざん、なりすまし等を防ぐため、暗号化通信の一種であるhttps通信を用いる。https通信を行うために、サーバ証明書をWEBサーバに登録した（図２③）。

以上により、特定の接続端末からのみアクセスできる3段階のセキュリティ機能を構築した。

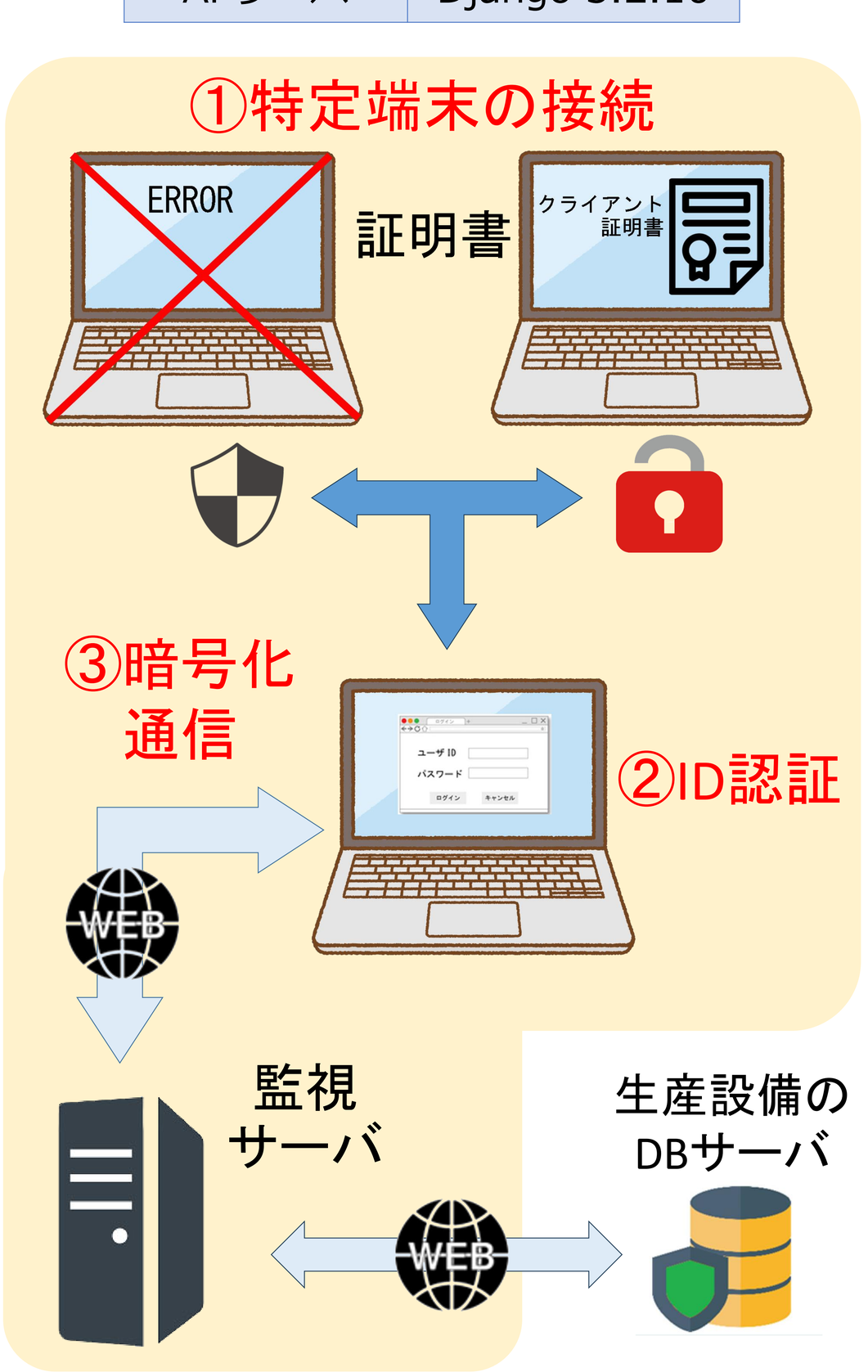

図２ クラウド上の監視サーバへのアクセス制御