清水建設株式会社 様

User Profile

SHIMIZU CORPORATION 清水建設

清水建設株式会社

所在地：所在地:東京都中央区京橋二丁目16番1号

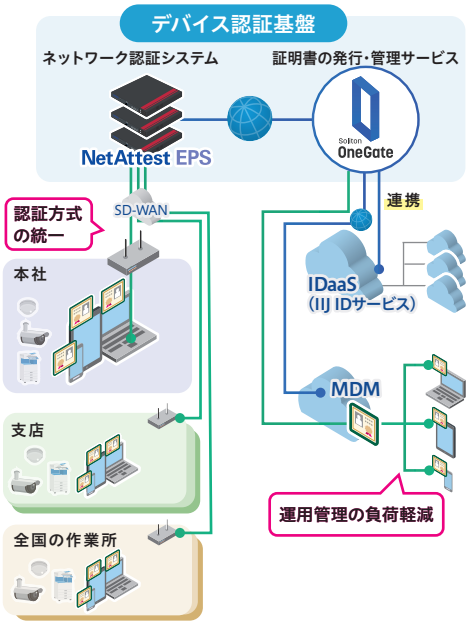
ＵＲＬ：https://www.shimz.co.jp/

1804年(文化元年)創業、220年の歴史を持つ大手総合建設会社(スーパーゼネコン)です。「SHIMZ VISION 2030」のもと、建設業界のデジタル化を加速させるため、BIM(ビルディング・インフォメーション・モデリング)、AI、IoTなどの最新技術を活用し、業務効率化と品質向上を推進。データドリブン経営を強化し、建設現場のスマート化を進めることで、持続可能な社会の実現に貢献しています。

クラウドシフトとゼロトラストの実現のために、デバイス認証基盤を刷新
端末の認証をクライアント証明書方式に統一、セキュリティ確保と運用管理負荷軽減を両立

課　題	導入効果
1 PC/iPad/スマートフォンのデバイス認証にMACアドレスを用いており、セキュリティ強度に懸念がある	PCにもクライアント証明書認証を導入し、セキュリティリスクを低減しながら認証方式を統一
2 デバイス認証システムの運用負担が大きく、効率化が求められる	デバイス認証システムの運用を最適化し、クライアント証明書配布を効率化。キッティング作業を1/10に短縮
3 今後のDX戦略を支えるクラウドシフト・ゼロトラスト対応の認証基盤を整備したい	国産のゼロトラスト対応認証基盤を導入し、長期的に運用可能な環境を確立

清水建設株式会社 様 イメージ図



セキュリティリスクと運用管理負担の観点から、MACアドレス認証の見直しを決断

清水建設は、「SHIMZ VISION 2030」のもと、事業構造・技術・人財のイノベーションを推進し、新たな価値を創出する「スマートイノベーションカンパニー」の実現を目指している。2024 年 7 月には 2 期目となる「中期 DX 戦略 2024-2026」を策定し、デジタル変革の取り組みを加速させている。

ITインフラのクラウド化と境界型防御からゼロトラストへの移行が進む中、DX経営推進室 基盤システム部 部長の室井俊一氏は、本プロジェクトの目的について次のように語る。

「ゼロトラストネットワークの実現には多くの要素が必要ですが、社内リソースには限りがあるため、優先的に取り組むべき課題として、長年懸案だったデバイス認証の整備に着手しました。当社では、業務用の iPad やスマートフォンにはクライアント証明書認証を採用していましたが、PC は無線 LAN と有線 LAN ともに MAC アドレス認証を使用していました。しかし、MAC アドレス認証において、MAC アドレス自体の詐称が容易でありセキュリティリスクがあります。また、iPad やスマートフォンではプライベート MAC アドレスが有効になると正しく認証できない等の課題もありました。クラウドシフトやゼロトラストへの対応、テレワークや SaaS の活用が進むことも考慮する必要があります。そこで、PC にもクライアント証明書認証を導入し、セキュリティ強化と運用負担の軽減を図る対策を進めるとにしました」

DX経営推進室
基盤システム部
部長
室井 俊一 氏

従来の MAC アドレス認証がもたらす運用負担について、DX 経営推進室 基盤システム部 インフラ企画グループ 主査の井上 悠氏は、次のように語る。

「新たな端末の出荷やリプレースのたびに、運用管理者が MAC アドレスの登録・削除を行う必要がありました。全社で数万台の端末を管理する中でその作業の負担が大きく、特に不要な MAC アドレスが削除されずに残存してしまう等の運用管理の課題が出てきていました」

そしてプロジェクト開始のきっかけを、DX経営推進室 基盤システム部 インフラ企画グループ グループ長の須田 大士氏は語る。

清水建設株式会社 様

「デバイスごとの認証方式の違いも運用管理負担の増大につながっていました。ちょうど今回は、本社のネットワーク更改のタイミングと、既存の一部システムで利用していたクライアント証明書認証の有効期限が重なったことを契機に、iPad やスマートフォンと共通の新たなデバイス認証基盤を構築することとしました」

DX経営推進室
基盤システム部
インフラ企画グループ
グループ長
須田 大士 氏

DX経営推進室
基盤システム部
インフラ企画グループ
主査
井上 悠 氏

拡張性と運用管理のしやすさを評価し、Soliton OneGateを選定

同社は課題解決に向け、複数の製品を比較検討。最終的に Soliton OneGate および、NetAttest EPS の採用を決めた。

Soliton OneGate（以下、OneGate）は、MAC アドレスベースの認証では防ぎきれない不正アクセスやなりすましのリスクに対応するため、クライアント証明書を用いたデバイス認証と多要素認証（MFA）を組み合わせたゼロトラストセキュリティを提供するソリューション。デバイスのセキュリティ状態チェック（ポスチャーチェック）を行い、企業のポリシーに準拠した端末のみアクセスを許可する仕組みを提供する。

さらに、NetAttest EPS と組み合わせることで、社内外を問わず統一された端末認証基盤を構築し、認証管理を一元化することで運用負担の軽減が可能となる。また、社内アクセス時にもゼロトラストの考え方を適用し、不正な端末の排除やポリシー準拠の徹底を実現できる。

OneGate および NetAttest EPS の導入の決め手について、須田氏と井上氏は次のように語る。

「セキュリティ製品は導入して終わりではなく、運用管理のしやすさがポイントです。そこで、新たに導入するデバイス認証基盤には、これまで課題であったクライアント証明書の発行及び展開が容易であること、そして不要になったクライアント証明書の失効なども含めて管理しやすく、セキュリティがしっかり保てることを求めました。OneGate のデモを見て、管理画面がとても見やすく、クライアント証明書発行・失効などの操作も分かりやすく運用管理しやすそうだと感じました。さらに、国内企業への導入実績も多数あることも、決め手となりました」（井上氏）

「国産メーカーが提供するソリューションであり、外資系ベンダーのサービスと違って為替の影響による価格の変動リスクや、最初は売り切りで途中からサブスクリプション方式に変わるといった心配も少ないと考えてます。営業担当者からの提案も熱心できめ細かく、安心して長期間、利用できると感じました。さらに今回、同時期に導入が決まっていた IDaaS 製品の IIJ ID サービスとの連携性と、証明書の配布に当社が利用している MDM との連携も必須条件でしたが、この点もクリアできると確認できたことで、正式に採用を決定しました」（須田氏）

段階的な移行と自動化でスムーズに新認証基盤を展開

須田氏は、本プロジェクトの導入プロセスについて次のように語る。

「2023 年度下期に構想を立案し、2024 年 4 月に、IIJ ID サービスと OneGate を導入。約半年をかけて設計・構築を進め、まず iPad/ スマートフォンの Wi-Fi 認証を OneGate に移行。その後、PC の無線 LAN 認証を OneGate と NetAttest EPS の連携で実施し、10 月に完了しました。有線 LAN 認証については検証を進めた上で実環境に展開予定です。各支店は LAN の更改に合わせて導入を進め、全社のデバイス認証基盤整備の完了には約 2 年を見込んでいます」

今回、同社は証明書の社内展開においても工数削減の工夫を施した。DX 経営推進室 基盤システム部 インフラ企画グループの中村 航也氏は、そのポイントを次のように語る。

「当社の管理者が端末の収集や個別の設定作業等を行うことなく、遠隔で一斉に効率よく展開できるようにしました。その際、社内展開時の工数を可能な限り抑えられるように、あらかじめ NetAttest EPS で認証を行う設定プロファイルを作成し、MDM で配布することで工数を削減しました。設定も、当初は Wi-Fi 接続時にユーザーが証明書を選択する必要がありましたが、ワンタッチで完了するよう改善し、可能な限りユーザーにおける作業の手間を削減しました」

DX経営推進室
基盤システム部
インフラ企画グループ
中村 航也 氏

認証管理の効率化とセキュリティ強化を両立

現在、IIJ ID サービス+OneGate+NetAttest EPS を活用した新しいデバイス認証基盤を、段階的に全社展開中。その導入効果について、室井氏は次のように語る。

「IIJ ID サービス と OneGate で多要素認証も実施し、ゼロトラストセキュリティの導入により、多方面で効果を実感しています。特に運用面では当初の狙い通り、MAC アドレスの登録や失効といった管理負荷が大きく削減されました。OneGate を導入することで、デバイスの種類や接続環境を問わず、一つのコンソールで統合管理できるようになり、大きなメリットが生まれました」

井上氏は、管理画面の見やすさを次のように評価する。

「OneGate のダッシュボードを活用し、デバイス認証の全体の状況を統計情報として直感的に把握できるようになりました。デバイス単位の詳細情報や認証通信のピーク状態等も視認しやすいレイアウトできれいに情報がまとまっており、管理者としては非常に助かります」

管理画面の見やすさと使いやすさは、本番稼働後の問い合わせ対応にも有効と中村氏は明かす。

「認証に関する問い合わせ対応の際、OneGate のダッシュボードを活用することで、対象デバイスを素早く検索でき、迅速な対応が可能です。さらにクライアント証明書の配布からインストール、接続の過程で発生する問題も素早く特定できるため、障害発生時におけるサポート対応の負担が軽減されました」

加えて中村氏は、デバイスの運用管理において管理者のみならず、ユーザー側のメリットもあると語る。

「キッティングセンターでの設定手順を簡素化でき、社給デバイスの配布作業を効率化しました。以前はクライアント証明書を手動でインストールし、その後プロキシの設定を行うため、1 台あたり約 10 分かかっていました。OneGate と NetAttest EPS 導入後は、このプロセスがほぼ自動化され、1 分ほどで完了するようになりました。当社は社員も多く、PC、iPad などのスマートデバイスもそれぞれ数万台が稼働しています。これまで、証明書が未インストールの端末を使用する場合、申請後に各自でインストールする必要がありましたが、今後はその手間が減ります。これは管理者のみならず、ユーザーにとっても大きなメリットです」

須田氏は、OneGate が証明書を 1 ユーザーあたり 10 枚まで発行できるメリットについても言及する。

「当社は、1 名で PC、スマートフォン、iPad など複数の端末を利用します。また、支店の総務担当者は会議室の共有 PC など、複数のデバイスを管理しています。さらに、端末の入れ替え時に一時的に新旧の端末を保有することもあります。OneGate では、1 アカウントにつき最大 10 枚の証明書を発行できるため、運用効率の向上とコスト削減の両面でメリットがあります」

今後もクラウド利活用とゼロトラスト認証基盤の最適化を目指す

デジタルゼネコンの進化、データドリブンと DX による経営・事業推進体制の強化など、建設業界を巡る環境はかつてない大きな変革の時期を迎えている。須田氏と井上氏は、今後の取り組みを次のように語る。

「リモートワークや現場での IT 活用など、社外からシステムにアクセスする機会が増え、働き方も、認証の対象となるデバイスも多様化しています。当社としては様々なクラウドサービス利用時に今回構築したデバイス認証基盤を連携させて、可能な限りシンプルにし、運用管理負荷を抑制しつつ、しっかりとセキュリティを強化していきたいと考えています」（井上氏）

「当社のゼロトラストの取り組みにおいては、ユーザーや組織の管理及びその認証・認可が残課題、最後のピースとなっています。建設業は社内だけでなく、協力会社など外部の方にもシステムを使ってもらう機会が増えています。人手不足をシステムで補い、業務効率化を図っていかなければなりません。そのようなケースにおいて、社外のユーザーも含めてユーザー ID 発行や認証が必要となり、ユーザー ID 管理や認証・認可のあるべき姿が変わってきているため、当社に限らず建設業界全体にとっての大きな課題となっています」（須田氏）

最後に須田氏は、ソリトンへの期待を次のように結んだ。

「ソリトンの国産のセキュリティベンダーとしての安心感は大きなものがあります。今後もぜひその強みを継続し、アピールしていただきたいと考えています。日本企業や建設業界の現場課題に適した技術・サービスの提供に、今後も期待しています」

Soliton®
株式会社ソリトンシステムズ　https://www.soliton.co.jp/
〒160-0022　東京都新宿区新宿 2-4-3　TEL 03-5360-3811
お問い合わせはこちら https://www.soliton.co.jp/contact/
大阪営業所 06-7167-8881　福岡営業所 092-263-0400
名古屋営業所 052-217-9091　東北営業所 022-716-0766
札幌営業所 011-242-6111

このカタログは 2025 年 5 月現在のものです。仕様、デザインは予告なく変更することがあります。　CS-SOGEPS-shimz-2505A