ビルシステムにおけるネットワーク構成と物理配置を統合した自動可視化技術の開発

Development of automated visualization technology that integrates network configuration and physical layout in building systems

太田　貴彦 Takahiko Ohta
古賀　宏 Hiroshi Koga
福本　喬彦 Takahiko Fukumoto
西村　将雄 Masao Nishimura

キーワード
ネットワーク可視化，セキュリティ，ビルシステム管理

ネットワーク探索技術をもとに把握したネットワーク構成情報と，スイッチングハブ（以下，スイッチ）から取得する物理的な配置情報を統合し，ITに不慣れなユーザが直感的にシステム全体を把握できる可視化技術を開発した。その技術をもとに，接続機器の断線，未許可機器の接続，通信量異常など様々な異常をリアルタイムで監視し，アラートをネットワーク構成ならびに物理配置を表したビュー上で表現できる自動監視システムを構築した。

また，このシステムに搭載した，スイッチのポート管理によるサイバーセキュリティ対応機能，ならびに新しい機器を追加する際の通信量の増加量，経路，機器への影響を事前に把握できるようにすることで，ネットワーク最適化に寄与する通信シミュレーションの実施例も紹介する。

Based on network discovery technology, we have developed a visualization technology that integrates network configuration information and physical layout information obtained from switching hubs, allowing users who are not familiar with IT to intuitively understand the entire system. Building on this technology, we have created an automated monitoring system that can monitor various anomalies in real time, such as disconnections of connected devices, unauthorized device connections, and abnormal communication volumes. Alerts are displayed on a view that represents both the network configuration and the physical layout. Additionally, we will introduce an implementation example of a communication simulation that contributes to network optimization. This is achieved by incorporating cybersecurity response functions through switch port management in the system. The simulation also allows for the prior understanding of the increase in communication volume, routes, and the impact on devices when adding new equipment.

1. 背景

近年，IoTやクラウドサービスの普及に伴い，ネットワークに接続する機器が増え，ネットワークの大規模化が進んでいる。また，ネットワーク機器のマルチベンダ化により，ビルシステムのネットワークが複雑化している。加えて，経済産業省からビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン等が出されているように，ビルシステムのセキュリティ対策が重要になっている。

一方，日本は少子高齢化が進み，企業は人手不足である。そうした中，ビル内でネットワークを利用している多くの組織や企業では，大規模化，複雑化するネットワークの構築や運用，保守に，より多くの手作業が必要なことが課題となっている。例えば，ネットワークの新規構築では，ネットワークが設計図どおりに構築されているか，接続機器が物理的にどこに配置されているかを目視や手作業で確認する必要がある。増改築時は，ネットワークの構成・物理的配置を変更した際に設計図の更新が必要となる。障害が発生した際には，原因特定のため設計図を参照し，目視や手作業による確認作業が必要となる。しかし，設計図が更新されていない場合は，さらに確認作業の時間を要する。

2. ネットワークシステム監視における課題

従来のネットワークシステム監視においては，IPv4ネットワークの場合，ネットワークアドレスの範囲内のすべてのアドレスに対してアクセスを試みる手法によりシステム内のネットワークに接続している機器を列挙して，監視するための機器の登録作業を軽減させていた。しかし，実際に構築したネットワーク全体を把握して監視するためには機器の列挙だけ

では不十分であり，スイッチの階層構造を含めて把握する必要がある。そこで3章で述べるネットワーク構成把握技術を用いることで，図1のようにツリー表現によりネットワーク全体を容易に把握可能としたが，ビルシステムの監視においては，以下に述べる理由から機器の物理的な配置情報が必要なため，十分とは言えない。

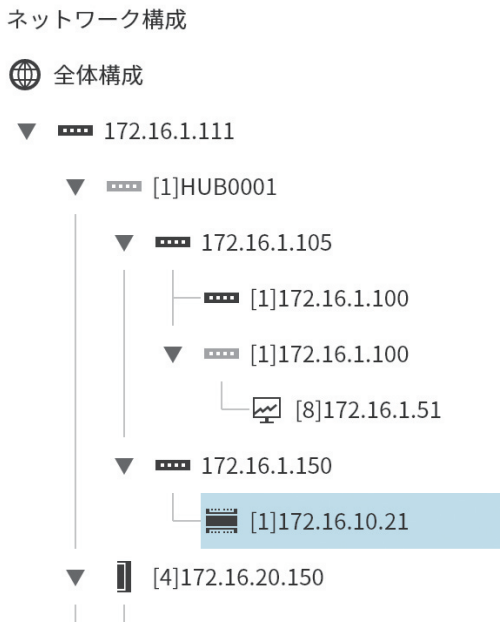

図1　ネットワーク構成のツリー表現

例えばサイバーセキュリティの観点では，不正アクセスが検知された場合，その機器の物理的な場所（建物の何階のどの自立盤から不正アクセスされたか）を把握し，早急に現場を確認・調査する必要がある。ネットワークの障害復旧においては，どのスイッチの何番ポートに不具合が発生しているかを把握し，そのスイッチが設置されている場所を特定して交換することが求められる。このように，早期の原因究明と復旧のためには，ネットワーク構成情報以外にもビルのどこで問題が起きているかという物理的な場所を早期に特定することが非常に重要となる。

しかし，現状のビルシステム管理においては，機器の配置は手動作成された2D/3Dの図面により表現されており，この作成および更新には大きな労力がかかっている。そのため，労力をかけずに機器の物理的配置を表示する仕組みが求められている。

また，経済産業省から出されているビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインによれば，不正機器の接続を防ぐためには，スイッチの空きポートを管理することが重要である。空きポートを物理的に塞ぐセキュリティポートロックが市販されているが，スイッチが大量にある場合はその設置に労力がかかるうえ，その鍵には単純な共通鍵が用いられているため，比較的容易に鍵を入手可能であるというセキュリティ面の問題がある。したがって，複数の空きポートを一括で使用できなくする簡易な手段とともに，外部の者が容易にポートの制限を解除できない仕組みが求められている。

3. ネットワーク構成把握

ネットワーク構成と物理配置を統合した可視化技術を説明する前に，最初にネットワーク構成の把握技術について説明する。

ネットワーク構成の把握技術では，ネットワーク上に接続されている全ての機器の把握に加えて，SNMP[注1]対応スイッチと連携することで，スイッチの多段構成の把握も可能である。

これにより，通信量の可視化，異常個所の特定，ポート無効化，通信量変化のシミュレーションなどが可能となる。

ネットワーク構成を把握する基本的な仕組みを以下に述べる。ネットワーク上の全スイッチからMACアドレステーブル情報を収集して解析を行う。MACアドレステーブル情報からネットワークの末端となるスイッチを判定し，その上位に接続しているスイッチの探索を繰り返すことにより，ネットワーク構成を把握する。

詳細は以下の通りである。はじめに，ネットワークの末端にあるスイッチを探索する。各スイッチのMACアドレステーブルを参照し，図2の赤枠のような任意の1つのポートに自身以外の全スイッチのMACアドレスが登録されているものを，ネットワーク末端のスイッチと判定する。図2ではMACアドレステーブルのうち，スイッチに関する情報のみを抽出している。

次に，この末端のスイッチと直接接続している上位のスイッチを探索する。各スイッチのMACアドレステーブルを参照し，任意の1つのポートに末端のスイッチのMACアドレスのみが登録されているスイッチを，末端のスイッチに直接接続しているスイッチと判定する。接続が確定したスイッチの情報を，各スイッチのMACアドレステーブル情報から削除し，前述の上位スイッチの探索を繰り返すことで，ネットワーク構成を把握できる。

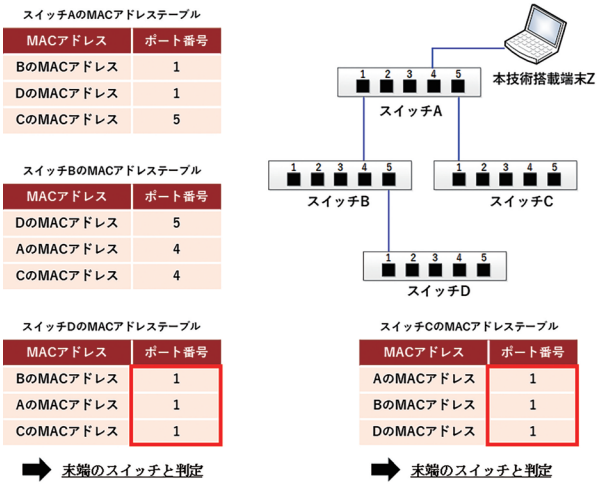

図2　末端のスイッチの判定

注1　SNMP（Simple Network Management Protocol）：ネットワークに接続された通信機器に対し，ネットワーク経由で監視，制御するためのプロトコル

4. ネットワーク構成情報と物理配置情報を統合した自動可視化技術

ネットワーク機器の物理配置情報があらかじめフロアマップ等の形で用意されている場合は，その情報を本システム内で利用できるが，ここではそのような情報が無い場合に，物理配置を自動描画する技術を紹介する。

ネットワークを構成するスイッチがSNMP対応であれば，あらかじめスイッチの設置階，位置，自立盤番号などのロケーションに関わる情報を書き込める。本システムの物理配置自動描画機能では，把握したネットワーク構成および複数のスイッチが持つロケーション情報を利用して，建物の何階のフロアのどの位置に存在する自立盤に設置されたスイッチであるかが分かるので，そこから建物の簡易的な外形および各階のフロア形状を推定する。さらにその上にスイッチを内蔵する自立盤を配置した物理配置図を生成する。

前章で説明したネットワーク構成把握技術により，スイッチの階層構造および，各スイッチに接続されている機器の有無を把握できるので，この建物図に重ねて，各機器の所在場所に応じて発見された機器のアイコンを配置する。

これらのアイコンを接続関係のあるもの同士「線」で結ぶことで，ネットワーク構成と物理配置とが融合した描画が実現する。

前述の物理配置図は，建物全体，フロア，スイッチといった表示範囲で作成することが可能であり，管理業務の目的に応じた粒度で表示レベルを切り替えられる（図3～5）。図中のグレーの四角形はスイッチが設置された自立盤を示している。

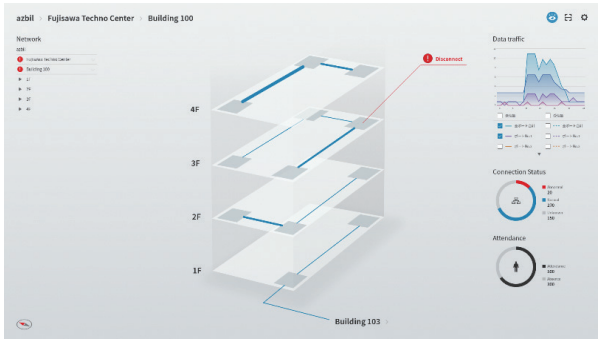

図3　建物全体図

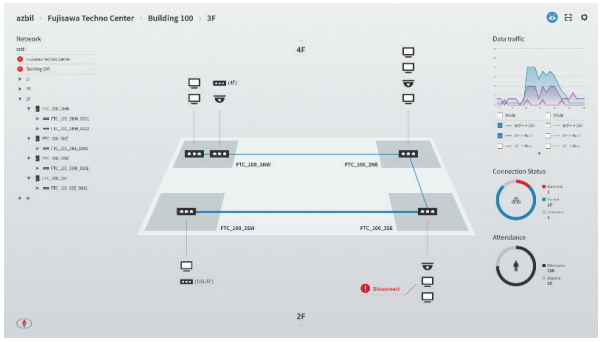

図4　フロア図

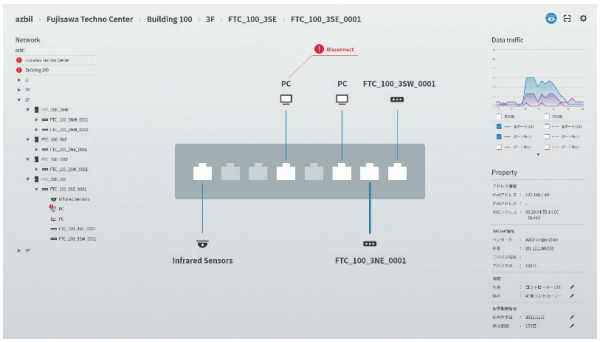

図5　スイッチ単体図

SNMPによる自動描画機能の利点は，スイッチを入れ替えたり新規に追加したりする場合に（各スイッチに正しくロケーション情報を登録することが前提ではあるが），ネットワークスキャンし直すだけで，ネットワーク構成と物理配置情報が現実と一致した状態に即時にアップデートする点である。

5. 適用事例

以上に紹介した技術を利用したネットワーク監視システムの事例を紹介する。以下に示すようなデータ表現手法や機能を備えることで，本システムはリアルタイムでのネットワーク監視や情報システムのメンテナンスがしやすくなるとともにメンテナンス工数の削減，セキュリティ性の向上，トラブル時の早急な対応ができるようになる。

5.1　通信量の可視化表現

近年の防犯への要望の高まりから，ネットワークへの防犯カメラなどのデータ通信量が多い機器の接続が増加している。ネットワーク設計が最適化されていない場合は，通信の集中による通信障害が発生するリスクがある。

本システムでは，接続経路ごとの通信量の違いを，管理画面上に表現する機器同士をつなぐ「線」の太さにより表示できる。例えば，通信量が他の接続経路よりも多い経路については，太い線分により表示する（図6）。

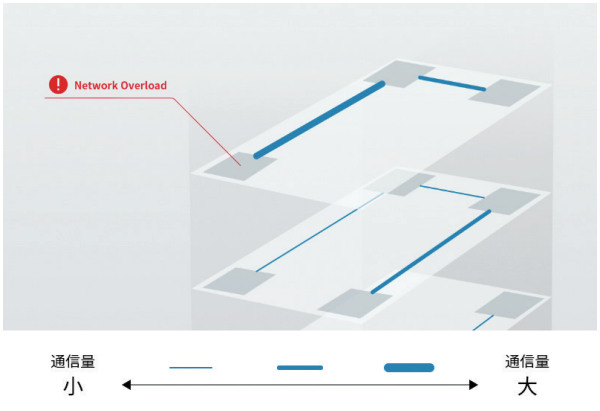

図6　線の太さでの通信量表現

あらかじめ設定した上限値を超えた場合には，アラート表示で知らせることもできる。これにより通信の混雑状況がひと目で分かるので，通信障害の未然回避に役立つ。

また，詳細情報として通信量のグラフを別の場所に表示することも可能なため，通信量の変化度合いを把握することも容易となる(図7)。

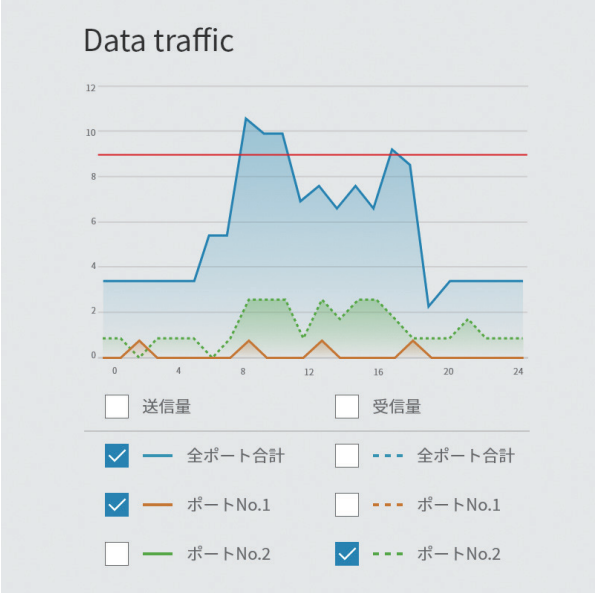

図7　通信量グラフ

5.2　異常箇所のハイライト表示

システムの通信状態を常に監視しているため，機器の通信が途絶えた場合や，事前に登録済みの機器以外のものがネットワークに接続された場合などは，システムに何らかの異常が発生したと判断し，管理画面上に異常表示を出す(図8)。これによりトラブルがあったことを早期発見でき，さらに物理配置情報を備えていることにより，現場に素早く駆け付けられるため，早期復旧につながる。

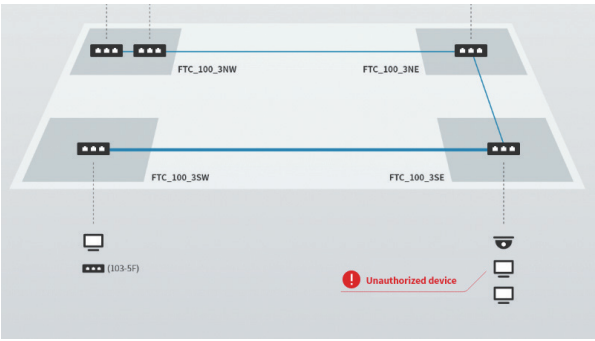

図8　異常箇所のハイライト表示

5.3　ポート無効化

近年，経済産業省が策定したビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインの発行やハッキングニュースなどによって，ビルシステムにおけるサイバーセキュリティの要求が高まっている。

サイバー・フィジカル・セキュリティ対策ガイドラインには，スイッチのポートの管理が有効との内容が記載されている。具体的には，スイッチの空きポートにLANケーブルをつないでハッキングされることを防ぐために，空きポートを無効にすることで，悪意ある人が勝手に接続することを防止する方法である。

大規模ビルで空きポートを一つひとつ無効化しようとすると膨大な工数がかかる。前述のネットワーク構成把握技術によりすべてのスイッチの未使用ポートを把握できるため，未使用ポートをまとめて一気に無効化できれば大幅な工数削減となる。

本システムでは，建物全体，フロアごと，スイッチごと，スイッチのポートごとといった複数の情報単位のビューを備え，それを用いて，未使用ポートの設定状況の確認および設定変更が容易にでき(図9，10)，また，本ツール以外の方法で，無効化された空きポートの制限を解除することが容易でないため，必要なセキュリティ対策を確実にかつ効率的に実施できる。

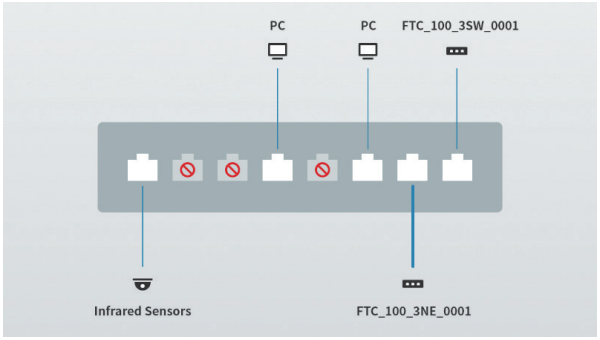

図9　ポートごとの無効化

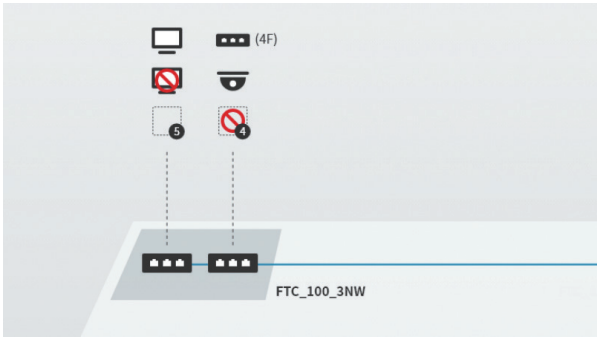

図10　機器ごとの無効化状態の表示

5.4　シミュレーション

既設のネットワークに，新しい機器を追加する場合，通信量増加によって，システム全体のパフォーマンスが低下し，他の機器の通信の不調をきたす可能性がある。それを防ぐために，ネットワークのどこにどのような通信量変化が生じるかをあらかじめ把握する必要がある。

通信量変化のシミュレーションのために，本システムで生成されたネットワーク構成図を元に，ユーザはどのような機器をネットワークのどこに接続するのか(図11)，どの程度の通信量なのか(図12)，通信相手がどの機器かを設定する。

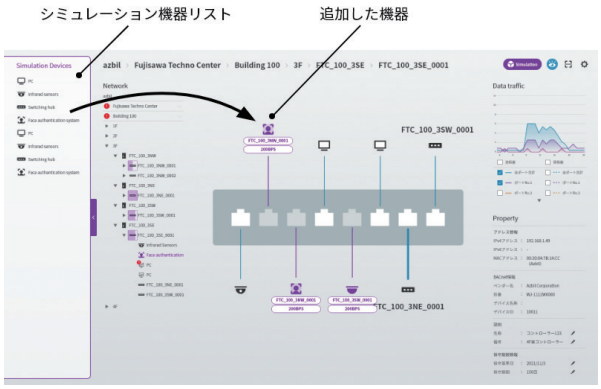

図11　追加する機器の設定

図12　追加デバイスごとの通信量設定

追加する機器を設定すると，ネットワーク構成把握技術によって，それにより影響を受けるネットワーク経路が特定できる。その経路に沿って追加する機器の通信量の増加分を自動算出し，算出された結果を構成図上にグラフィカルに表示する。またネットワーク構成上どの部分の通信量が問題になるかを一覧で表示することもできるため，追加機器の影響がどこにどの程度及ぶかがひと目で分かる(図13, 14)。

これにより，追加機器におけるネットワークトラブルを未然に防ぐことが可能になる。

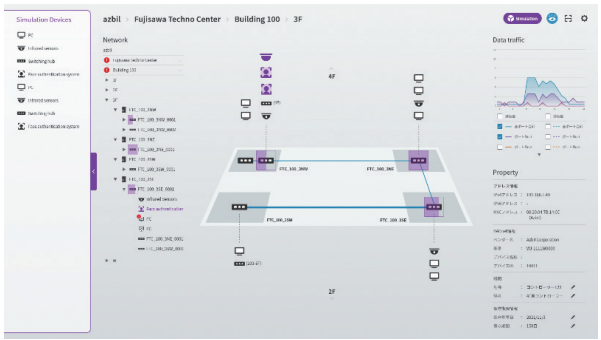

図13　通信量シミュレーション結果表示

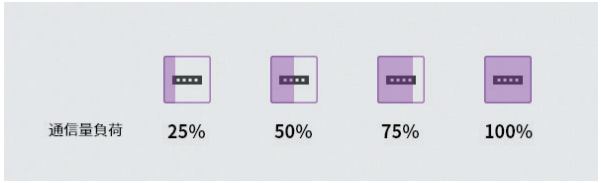

図14　追加機器の影響による通信量負荷の表現

6. おわりに

ネットワーク構成と物理配置を統合した自動可視化技術により，ITに不慣れなユーザでもビル内のネットワークシステム全体を直感的に把握できるようにした。この技術に基づいた適用事例として，リアルタイムでの異常監視やアラート表示，サイバーセキュリティ対策としてのスイッチのポート管理機能，通信シミュレーション技術等を紹介した。

これらの技術は，ネットワークの複雑化が進む現代において，管理者の負担を軽減し，システムの健全な運用を支える重要な役割を果たすことが期待できる。今後もさらなる発展と応用に向けて，開発を続ける。

＜参考文献＞

(1) 太田貴彦，神宮武志，ネットワーク構成把握技術の開発 azbil Technical Review，2021年，Vol.62，pp.48-52，アズビル株式会社

＜著者所属＞

太田　貴彦　アズビル株式会社
ビルシステムカンパニー開発本部開発3部
古賀　宏　アズビル株式会社
技術開発本部協働開発部
福本　喬彦　アズビル株式会社
技術開発本部協働開発部
西村　将雄　アズビル株式会社
ビルシステムカンパニー開発本部開発3部