JSだより

連載　236

二つの「見えないインフラ」を守る
～下水道の視点で考える、事業を止めない備え～

DX戦略部 システムマネジメント課

1　はじめに

日本下水道事業団（JS）は、浸水から都市を守り、衛生的で快適な水環境を創出する「下水道」という、国民生活に欠かすことができない社会インフラを支えることを使命としています。

私たちは日常生活の場面で、下水道の存在を意識することがあるでしょうか。下水道事業に携わる私たちでも、ほとんど意識していないのではないかと思います。都市の静脈として、家庭や事業所から排出される汚水を処理し、公共用水域の環境を守り、近年頻発する豪雨による浸水被害から地域を守り、24時間365日、私たちの足元で黙々と機能し続けることが「当たり前」だからです。ひとたび想定を超える豪雨や地震などで、その機能が失われれば、都市機能は麻痺し、公衆衛生は深刻な状況となります。「当たり前」を維持することの重みを、下水道事業に携わる私たちは、強く感じています。

私たちの事業活動を支える「情報システム」もまた、下水道とよく似た性質を持つ、もう一つの「見えないインフラ」だと感じます。毎日、当然のように利用している情報システムは、全国の地方公共団体や工事現場や関係者の拠点やJSの拠点間で、膨大な数のメール送受信を行い、Web会議を行い、事業情報、施工管理情報、設計情報をやり取りし、積算システムを駆使し、会計処理を行うといった、すべての基盤です。正常に稼働していることが「当たり前」です。ひとたびサイバー攻撃やシステム障害や大規模停電に見舞われれば、何が起きるでしょうか。積算システムが止まれば入札公告が遅れ、契約手続きが滞り、工事の着手が遅れ、施設の供用開始も遅れます。設計情報を入手できなければ、建設工事を進めることができません。業務の停滞は、全国で進行中の下水道事業のみならず、関連する社会インフラの整備の遅れにも直結します。

普段は意識されることのない重要な「インフラ」を守り、その機能を維持し続けることは、下水道に携わる私たちに共通する、大きな使命の一つです。本稿では、事業継続の生命線である情報インフラをいかに守るか、JSの情報セキュリティの考え方と取り組みの一端をご紹介します。皆様の取り組みと、どこが同じで、どこが違うのか、比べながらお読みいただければ幸いです。

2　「守り」から「攻めの基盤」へ

皆様は、情報セキュリティをどのように捉えておられますか。ウイルス対策や不正アクセス防止といった「守り」の側面に注視されていませんでしょうか。「守り」は対策の根幹ですが、それだけではこれからの組織には不十分と考えています。「守り」を固めることで、はじめてDXの推進という未来に向けた「攻め」の施策に安心して取り組むことができます。

下水道事業に携わる組織にとって、取り扱う下水道施設の設計情報や、地方公共団体や関連機関・業者と共有する情報は、社会インフラの根幹に関わるものであり、その保護は私たち共通の課題と言えます。これらの情報が漏えい、改ざんされることは、単に一組織の損害にとどまらず、社会的な信頼を揺るがしかねません。

重要な情報を守りつつ、業務効率を向上させるための考え方が「ゼロトラスト」です。皆様も、庁舎やオフィス以外の場所で仕事をする機会が多いものと思います。施工管理を担当する職員が現場でタブレットやスマホを用いて図面を確認したり、出張先から業務システムにアクセスしたりすることが日常となった今、「社内は安全、社外は危険」という境界型の防御モデルは成立しません。「何も信頼しない（Trust Nothing, Verify Everything）」を前提として、すべてのアクセスをその都度検証することで、場所を問わずセキュアな業務環境を実現することが、私たちの業務の特性に合致したセキュリティのあり方です。

JSでは情報セキュリティを「技術」「プロセス」

「人」の３つの要素が一体となって機能するものと捉え、総合的な対策を進めています。雨水ポンプ場に例えるなら、最新のポンプ施設（技術）も、運転するための適切な操作マニュアル（プロセス）と、緊急時に臨機に対応できる経験豊富な職員（人）が揃って、初めてその能力を発揮するのと同じです。どれか一つが欠けてもダメで、この点は下水道施設の運用も、情報システムも同じです。

3 事業継続を支える３つの柱

社会インフラである下水道と同様に、事業活動を支える情報インフラもまた、安定稼働が「当たり前」のこととして求められます。「当たり前」を維持するため、JSでは前述の３つの観点から具体的な取り組みを講じています。

（１）技術的対策

JSでは、複数の防御策を組み合わせた「多層防御」によって脅威に備えています。ゼロトラストの考え方を土台とし、その上でネットワーク、端末、認証、通信のそれぞれに対して適切な対策を重ねることで、場所や端末を問わず、その都度の確認・許可により安全性を確保しています。

巧妙化するサイバー攻撃は、従来のパターンマッチング型のウイルス対策ソフトだけでは防ぎきれないのが現実です。皆様は、未知の攻撃への備えは万全でしょうか。JSでは端末における不審な挙動の把握や、異常な通信の早期検知など、ふるまいに着目した対策を情報システムの「免疫機能」として重視しています。また、庁舎内外で活動する職員が安全に業務情報へアクセスできるよう、通信の暗号化など、基本的な対策の徹底に継続して取り組んでいます。

（２）プロセスと体制

優れた技術も、それを適切に運用するルールと体制がなければ機能しません。JSでは「情報セキュリティ管理規程」を整備し、これに基づき定期的に関係者による会議体を運用しています。ここでは、最新の脅威情報の共有や対策の審議を行い、経営層を含めた迅速な意思決定の場として機能させています。

（３）人的対策

どれだけ技術やプロセスを整えても、結局、最後の砦となるのは「人」です。「うちの職員は大丈夫」と思っていても、巧妙なメールにはつい騙されてしまいます。JSでは役職員の意識と対応能力の向上が最も重要であると考えており、実践的な教育・訓練を実施しています。代表的なものが「標的型攻撃メール訓練」です。業務で日常的にあり得る連絡を装った訓練メールを用い、受信時の確認ポイントや通報・報告の行動を体験的に学ぶことで、不審メールへの対応能力を高めています。あわせて、自分のワンクリックがJSの業務全体にどれほどの影響を与えるのかを実感し、その緊張感を役職員全員で共有することを重視しています。

（４）万が一への備え

近年頻発する豪雨災害や、いつ起きてもおかしくない大地震、そうした有事の際に、下水道施設そのものの事業継続計画（BCP）と同様に、私たちの業務を支えるITシステムのBCPも極めて重要です。JSでは万が一の事態に備えるため、具体的な行動計画である「IT業務継続計画書（IT-BCP）」を策定しています。IT-BCPには、インシデント発生時の体制、業務への影響を考慮した整理、そして復旧に関する手順などをあらかじめ定めています。とはいえ、いざという時に計画どおりに動けるのか、BCPが書棚の肥やしになっていないか、その日が来た時に計画が絵に描いた餅とならないように、IT-BCPに基づいた訓練を実施しています。インシデント発生時の役割分担や手順を確認するウォークスルー訓練（机上訓練）を、システム管理を担当する部署で定期的に実施し、担当者の習熟度向上を図っています。

今後は、実際のシステムを用いた、より実践的な訓練へステップアップさせていくことを目指しており、IT-BCPの実効性を絶えず高めていきます。計画と訓練による備えを第一としつつ、それでもなお残るリスクに備えるために、その他の多角的な備えも講じています。

4 おわりに

本稿で紹介した取り組みは、結局のところ、基本的な対策の地道な積み重ねです。特別な方法などありません。社会インフラを支えるという共通の使命を持つ私たちにとって、これらの「当たり前」の対策を、自らの事業特性に合わせて地道に継続していくことが、何よりも重要だと考えます。本稿で紹介した取り組みが、皆様の情報セキュリティ対策の現状を、改めてご確認いただくきっかけとなれば幸いです。

JSはこれからも「下水道プラットフォーマー」としての責務を果たすべく、自らのセキュリティ対策に着実に取り組んでまいります。下水道施設の物理的なセキュリティと同様に、サイバー空間におけるセキュリティ確保に努めることが、下水道界全体の災害への備えや事業を継続していく力の向上につながるものと考えます。

引き続きJSの業務にご理解とご協力をお願い申し上げます。