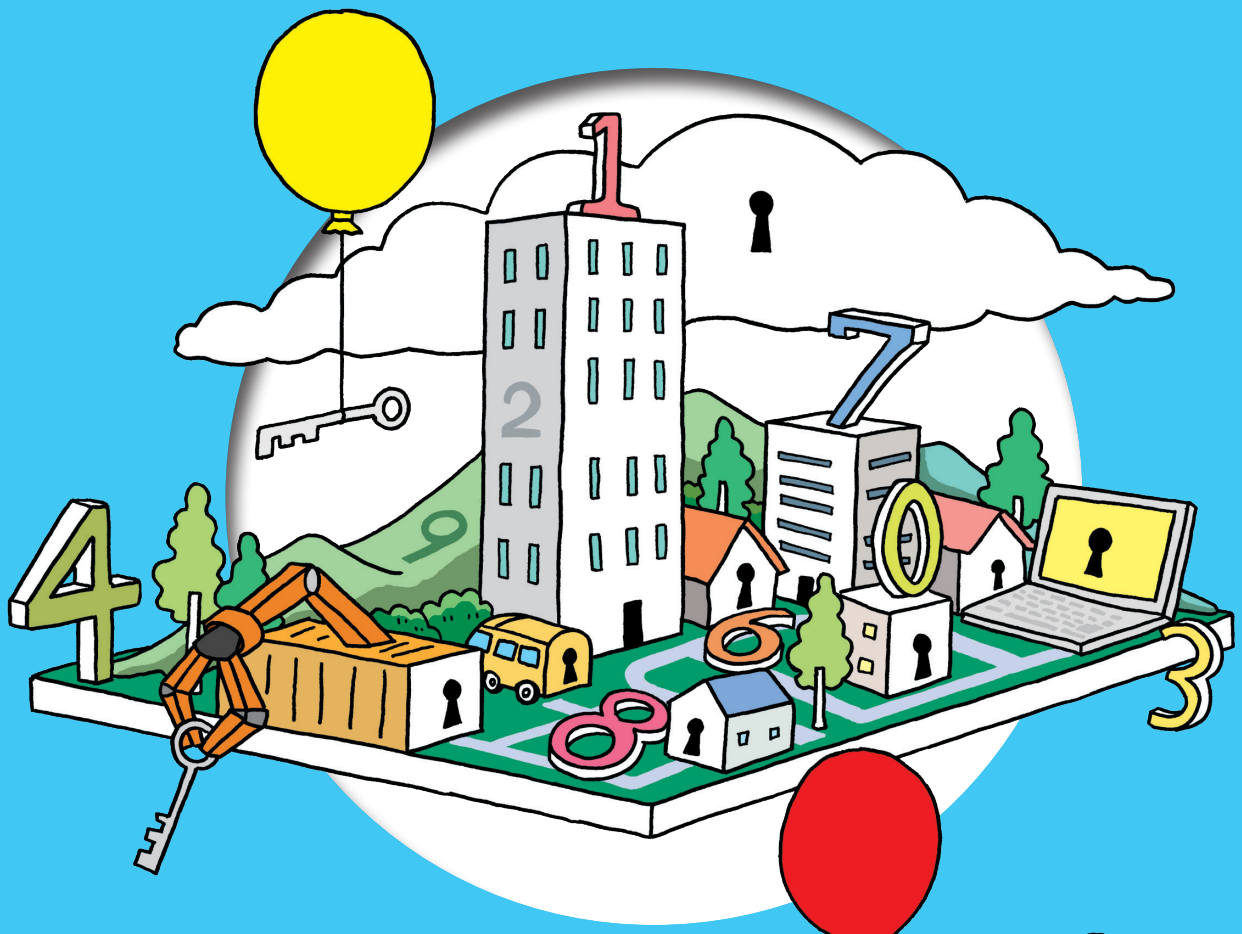
STiC ×Dream

お客さまと共にデジタルイノベーションを創造する

［スティックバイドリーム］
by Canon IT Solutions

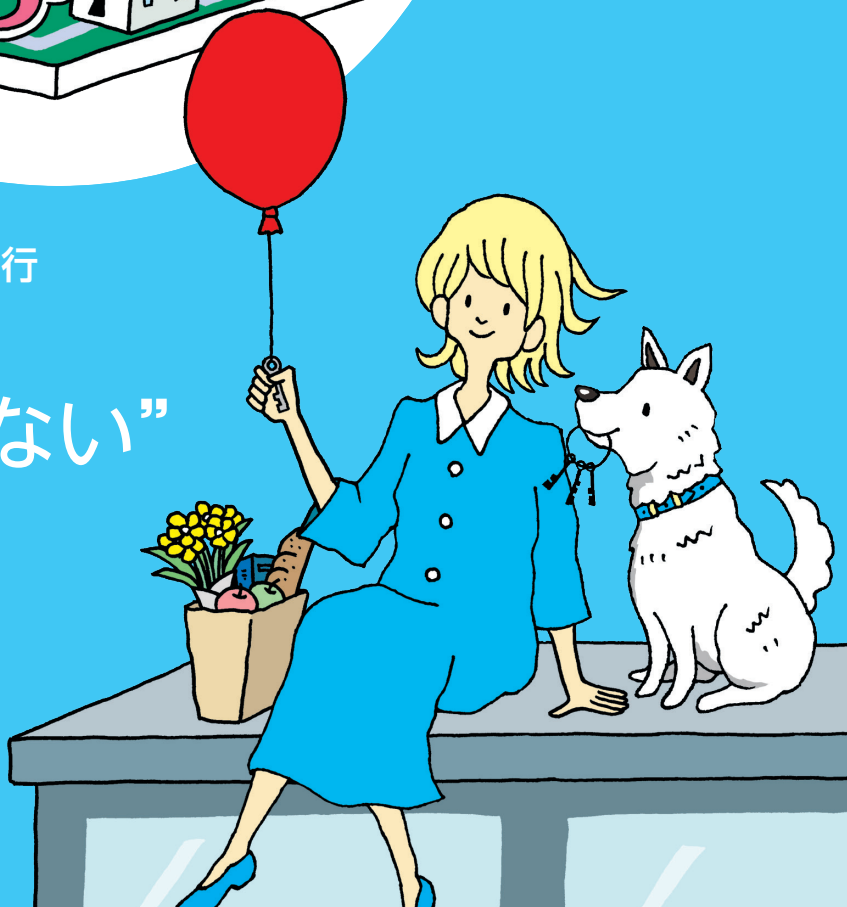
Vol.11
SPRING/SUMMER
2024



特集

経営者の意識改革とゼロトラストへの移行

企業に求められる“一人で抱え込まない”セキュリティ対策



STIC ×Dream Vol.11
SPRING/SUMMER 2024

C O N T E N T S

イラスト（表紙・特集）：高田茂和

特集

経営者の意識改革とゼロトラストへの移行

企業に求められる“一人で抱え込まない”セキュリティ対策

社会でAI（人工知能）活用が進み、企業にDX（デジタルトランスフォーメーション）推進が求められる中、セキュアなサイバー空間の構築と情報セキュリティ対策の重要性はますます高まっています。セキュリティインシデントは後を絶たない状況にあり、今後は企業の経営・マネジメント層における意識改革や、企業の枠を越えた業界全体での取り組みが必須となります。こうした状況を捉えて本特集では、攻撃者視点でのセキュリティ対策の第一人者である株式会社トライコーダ 代表取締役の上野 宣氏に日本における情報セキュリティの現状と課題、解決策を伺うとともに、注視すべきサイバーセキュリティのトレンドを解説します。また、キヤノンITソリューションズが重点事業領域としているクラウドセキュリティの事業概要および事業戦略も紹介します。

ラストへの移行

られる抱え込まない”セキュリティ対策

注視すべき4つのトレンド

――クラウドサービスやIoTの利用が拡大し、情報セキュリティへの脅威も増大しています。そうした中で注目すべきトレンドを教えてください。

上野宣氏（以下、上野氏）　私はこれまで主にオフェンス（攻撃者）側の視点からサイバーセキュリティ対策に取り組んできました。その経験と知識から挙げておきたいトレンドは、「ASM（攻撃対象領域管理）」「ゼロトラスト」「サプライチェーン攻撃」「AIの活用」の4つです。

Interview

株式会社トライコーダ
代表取締役
上野 宣氏
Sen Ueno

奈良先端科学技術大学院大学にて情報セキュリティを専攻、2006年にサイバーセキュリティを専門とする同社を設立。株式会社Flatt Security社外取締役、一般社団法人 セキュリティ・キャンプ協議会 理事・顧問、OWASP Japan代表、国立研究開発法人情報通信研究機構（NICT）実戦的サイバー防御演習 CYDER 推進委員なども務める。

――なぜこの4つが重要なのでしょうか。

上野氏　攻撃者側視点に基づいたセキュリティ対策と申しましたが、その一環としてお客さまのシステムに対して「ペネトレーション」と呼ばれるテストを行うことがあります。実際に攻撃者が実行する手法に基づいてシステムへの侵入を仕掛け、昨今のサイバー攻撃に対してどれくらいの耐性があるのかを検証するものです。そこで重点的に評価するのが、この4つのトレンドなのです。

　中でも基本となるのは1つ目に挙げたASMです。システムに侵入しようとする攻撃者は、どこが“入口”となるのか、ターゲットとする企業を徹底的に調査します。公開されているWebサイトを糸口にドメインやIPアドレス、従業員数、組織体制などの基本情報をつかみ、さらにネット上のさまざまな情報からも、重要システムを担当している責任者や関係者のメールアドレスなど、あらゆる情報を収集します。その上で、誰に扮して、どんな手段で、どのルートからアクセスすれば欺けるのかを考えながら侵入ルートを探るのです。

　例えば、従業員数が数千人以上で、海外にも複数の拠点があるといった規模の大きな企業となると、利用しているエンドポイントやアプリケーションの数も膨大になり、そのすべてを把握してガバナンスを効かせるのは非常に困

難です。裏を返せば攻撃者は、そういった監視の目から漏れた弱点をしっかり調べ尽くした上で、侵入してきます。

今後の基本戦略はゼロトラスト

―― そういった攻撃に対抗するため、企業にはどのようなセキュリティ戦略が求められますか。

上野氏　戦略的な意味でのキーワードとなるのは、2つ目のトレンドに挙げたゼロトラストです。従来のセキュリティ対策は、いわゆる境界型防御の考え方に基づいて、社内ネットワークの内側の安全性を担保することである程度対応できました。

　しかし、現在のようにモバイルデバイスやクラウドサービスの利用が拡大し、データが社外に分散して置かれるようになると“境界”は曖昧になり、すべてのアクセスに対して目を光らせる必要が出てきます。

―― エンドポイントに潜んでいる脆弱性も大きなリスクとなりますね。

上野氏　そこで注視しなければならないのが、3つ目のトレンドとして挙げたサプライチェーン攻撃です。一般的にサプライチェーン攻撃というと、製造業に見られるような取引先との業務上のつながりを悪用し、連鎖的な攻撃の踏み台とする攻撃手法を指しますが、それだけではありません。近年ではソフトウエアに巧妙に仕組まれたバックドアを介した不正侵入などの、“ソフトウエアサプライチェーン”への攻撃も大きな問題となっています。

　先般もLinux向け圧縮ユーティリティに、バックドアとして悪用される恐れがある深刻な脆弱性が発見されました。同様に半導体チップの製造工程においてファームウエアレベルで仕組まれるマルウエアやバックドアも危険視されています。

―― 効果的な対策はあるのでしょうか。

上野氏　データはアプリケーションを含め、エンドポイントには“何も置かない”ことが、ゼロトラストの1つのゴールになると考えています。Webブラウザのみしか利用できないシンクライアントに近いイメージです。

　それでも侵入リスクを100%回避することはできません。攻撃者側の視点からいえば、最終のターゲットは人間であるからです。重要人物に成り代わることができれば、基本的にその人ができることは何でも可能であり、欲しい情報も意のままとなります。実際に人をだますテクニックもますます高度化しています。

生成AIが人をだます時代

―― 具体的には、どんな新手のテクニックが使われはじめているのですか。

上野氏　4つ目のトレンドとして挙げた「AIの活用」は、そ

の代表的なものです。例えば高度なフィッシングのために生成AIを活用するケースも見られます。

これまでのフィッシングメールは文法が間違っていたり、日本では見かけない書体が使われていたりなど、見た目からして“怪しい”ものが多々ありました。ところが生成AIを使って作成された最近のフィッシングメールは日本語も流ちょうで違和感がなく、簡単には見破れない内容になっています。

―― 高度化するサイバー攻撃から情報資産を守るため、企業は何から始めればよいのでしょうか。

上野氏　セキュリティ対策のフェーズは企業ごとに異なりますが、まず必須となるのはリスク分析です。難しく聞こえるかもしれませんが、例えばIPA（独立行政法人情報処理推進機構）が公開している「サイバーセキュリティ経営可視化ツール」を利用するのも手です。

セキュリティ対策で特に重要な10項目の実施状況について、簡単な質問に答えていくと現時点の成熟度が5段階のレーダーチャートで表示されます。同業他社と比べて自分たちのセキュリティ対策はどれくらいのレベルにあるのかを客観的に把握することで、サイバーセキュリティに関する方針の策定や、適切なセキュリティ投資などが可能となります。

経営層の理解でセキュリティ対策は確実にゴールに近いところから始められます

求められる経営層の危機感を持った関与

――担当者レベルでの取り組みには限界があり、やはり経営・マネジメント層が危機感を持って積極的に関与することが欠かせないと思われます。

上野氏　おっしゃるとおりです。経営層がセキュリティに理解があるのかどうかで、スタート地点から違ってきます。経営層の理解でセキュリティ対策は確実にゴールに近いところから始められますが、何らかのインシデントが起こってから、ようやく腰を上げるという経営層が多いのも現実です。

そんな孤立無援の状態にある担当者にぜひおすすめしたいのが、経済産業省が公開している「サイバーセキュリティ経営ガイドライン」の活用です。経営ガイドラインというタイトルですが、経営層が直接読む内容というよりも、経営層に対してサイバーセキュリティに関する考え方を理解してもらうために、どのように進言すれば効果的なのかというノウハウが豊富に書かれているので役立つはずです。

―― 経営・マネジメント層の意識を変えるために、国も動き始めているのですね。

上野氏　その意味では、先のIPAでは「サイバーセキュリティお助け隊サービス」という支援制度もスタートさせています。サイバーセキュリティ対策を支援するための相談窓口のほか、異常の監視、事案発生時の駆け付け支援を含む初動対応、簡易サイバー保険などのサービスを、主に中小企業の事業環境や実情に即した内容で、安価かつ効果的なワンパッケージにまとめて提供するものです。

さらに経済産業省では、中小企業・小規模事業者向けに同サービスの導入を「IT導入補助金」によって支援する制度も用意しており、セキュリティ対策への投資を後押ししています。セキュリティ対策の重要性は分かっても、その原資を確保できずに投資に至らない企業も少なくないだけに、これらの支援制度を積極的に利用してほしいものです。

コミュニティを通じて他社とも連携

―― 孤軍奮闘しているセキュリティ担当者に向けても、アドバイスをいただけないでしょうか。

上野氏　仮に一人であってもサイバーセキュリティに高い意識を持った人材がいることは、その企業にとっての重要な戦力となります。

そんなセキュリティ担当者に今後ぜひ取り組んでいただきたいのが、“一人で抱え込まない”セキュリティ対策です。業界団体に参加したり、作ったりといった大げさな話ではありません。例えば「情シスSlack」というコミュニティは現在4000人を超えるメンバーが参加しており、サイバーセキュリティに関する悩みの相談も気軽に投げかけられます。

私が代表を務めている「OWASP(※1) Japan」にも奮ってご参加をいただけたらと思います。全世界で活動しているNPO団体「OWASP」の日本支部であり、セキュリティ

※1：Open Worldwide Application Security Project。Webをはじめとするソフトウエアのセキュリティ環境の現状、またセキュアなソフトウエア開発を促進する技術・プロセスに関する情報共有と普及啓発を目的に活動する非営利団体。世界各地に支部があり日本でもOWASP Japanなどが活動している。

啓発活動のほか、約3カ月に1回のペースで勉強会も実施し、さまざまな課題に取り組んでいます。

「Hardening Project(※2)」とのコラボイベントでは、実際のケースを設定した課題にチームを組んであたり、セキュリティインシデントを体験することが可能です。講師陣があの手この手で攻撃を仕掛けるので、最新のサイバー攻撃とはいかなるものなのか、対策を含めて身をもって学べます。もちろん参加費は無償です。

そして何よりも大きなメリットとして、共に学んだメンバーは今後のセキュリティ対策を進めていく上で、かけがえのない“仲間”となるはずです。“一人情シス”のセキュリティ担当者も孤立無援ではなくなります。

IT Security Trend Keywords［セキュリティトレンドキーワード］

キヤノンITソリューションズのセキュリティエバンジェリストが解説

上野 宣氏が注目する 最新セキュリティトレンド

キヤノンITソリューションズ株式会社
ITインフラ技術統括本部
サイバーセキュリティ技術開発本部
サイバーセキュリティラボ
セキュリティエバンジェリスト
西浦 真一,CISSP
Shinichi Nishiura

Keyword 01 ASM／攻撃対象領域管理 [Attack Surface Management]

インターネット上に公開されているなど組織の外部からアクセス可能で、サイバー攻撃を受ける可能性があるIT資産をアタックサーフェスといいます。ASMとは、組織のアタックサーフェスを把握し、それらに存在する脆弱性などのリスクを継続的に検出・評価することで、リスクを管理することを指します。クラウドサービスの普及、コロナ禍によるテレワークの拡大等を通じたリモート化が進んだ結果、アタックサーフェスも増加しているため、ASMの必要性はますます高まっています。

Keyword 02 ゼロトラスト [Zero Trust]

ゼロトラストとは、その言葉のとおり“暗黙の信頼(Trust)はしない(Zero)”という前提に立ったセキュリティ対策の考え方です。従来のセキュリティ対策は、ネットワークを“安全な内部”と“危険な外部”に区別し、その境界で対策を行う境界型防御でした。それに対してゼロトラストでは、社内ネットワーク内のデバイスからのアクセスであっても暗黙に信頼せず、常にアクセスの信頼性を検証することで、組織の情報資産やIT資産を保護します。

Keyword 03 サプライチェーン攻撃 [Supply Chain Attack]

サプライチェーン攻撃とは、組織間の業務上のつながりを悪用する攻撃手法です。標的組織の関連組織や子会社、取引先などを侵害し、それを踏み台として標的組織に侵入するケースのほか、標的組織が導入しているIT製品やサービスを踏み台として標的組織を侵害するケースなどが確認されています。外部に対して強固なセキュリティ対策を行っている組織であっても、サプライチェーンを足掛かりとされることで、攻撃者の侵入を許してしまう恐れがあるため、注意が必要です。

Keyword 04 AIの活用 [Attack using AI／Attack by AI]

AIの活用に期待が寄せられる一方、攻撃者による悪用も懸念されています。悪用例としては、フィッシングメールやマルウエアの作成、虚偽の動画や音声、画像を生成するディープフェイクの増加などがあります。米連邦捜査局(FBI)が就職のオンライン面接で別人になりすますといったディープフェイクの増加を発表しているほか、英国では、2019年に企業の最高経営責任者(CEO)を装った電話でディープフェイクの音声が使われ、22万ユーロ(約2600万円)を送金してしまう事件が報告されています。

※2：サイバーセキュリティの実践力を強力に向上することを目的に開催されるセキュリティ堅牢化競技会「ハードニング競技会」を運営するボランティア・プロジェクト。2012年から毎年継続開催されている。

Canon IT Solutions Security Solutions［セキュリティソリューション］

拡大するクラウド利用に応える ASM、ゼロトラスト対応ソリューションを拡充

西東京データセンターを生かした運用サポートにも注力

キヤノンITソリューションズ株式会社
上席執行役員
ITプラットフォーム事業部門 副担当
ITプラットフォーム営業統括本部長
山岸 弘幸
Hiroyuki Yamagishi

IT利用環境の変化に対応

セキュリティといっても幅広く、お客さまのニーズも多岐にわたりますが、キヤノンITソリューションズとして重点的に取り組んでいくべき領域として、クラウド関連のセキュリティを位置付けています。

周知のとおり、いまやクラウドは業界業種や規模の大小を問わずあらゆる業界の企業に浸透しており、さまざまなサービスの利用が拡大しています。日本企業が利用しているSaaSは平均して5つ前後という調査結果もあります。これは諸外国と比べると10分の1程度で、日本企業のクラウド利用には大きな“伸びしろ”があると見ています。

今後ますます多様化していくお客さまのニーズや、高度化する要件を先取りする形で、お客さまがより安全かつ快適にクラウドを利用できる環境を提供することが、当社の使命と考えています。

IT環境の多様化に向けたASM、ゼロトラスト

ASM、ゼロトラストセキュリティへの対応拡充も大きな柱です。これまで多くの企業は、いわゆる境界型防御の考え方に基づいて社内ネットワークのセキュリティを担保してきました。

それがコロナ禍を機に働き方改革やリモートワークが急拡大したことで、ユーザーが各種クラウドサービスを利用する場所は社内に限定されず、自宅をはじめ社外に広がっており、利用する端末も多様化しています。

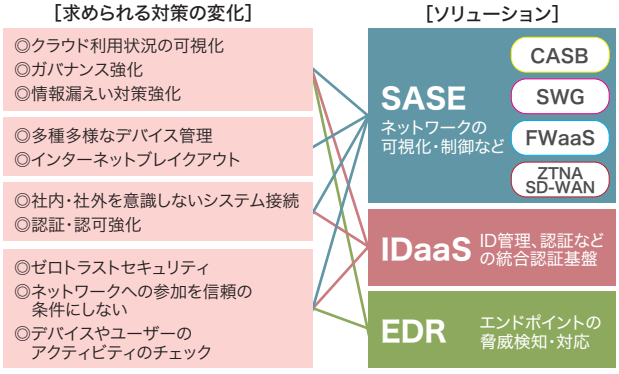


図1　キヤノンITソリューションズの中核セキュリティソリューション

こうしたIT利用環境の変化に対応するのがASMであり、ゼロトラストセキュリティです。当社ではその中核ソリューションとして、ネットワークの可視化・制御などを担うSASE(※3)、ID管理やユーザー認証などの統合認証基盤であるIDaaS(※4)、エンドポイントの脅威検知・対応を担うEDR(※5)といった製品やサービスを取りそろえるとともに、今後に向けてもポートフォリオをさらに拡充していこうとしています(図1)。

コンサルや運用サポートにも注力

これらのセキュリティ製品をただ提供するだけでは、お客さまの課題解決に資することはできません。

そこでキヤノンITソリューションズでは、ソリューション導入前のお客さまの社内システムおよびクラウドサービスの運用・利用環境のアセスメント(現状分析・評価)を経て、あるべきセキュリティ対策を設計するトータルなコンサルティングも提供しています。

セキュリティは一度導入すればそれで終わりではなく、脅威の動向やシステム利用状況の変化に合わせて継続的に見直しを行っていく必要があります。当社では、こうしたセキュリティ運用面のサポートにも注力しています。

そのバックグラウンドとして、他社にはない独自の強みとなっているのが「西東京データセンター」の存在です。ティア4レベルの高性能ファシリティ、世界基準の運営品質を証明する「M&O認証」取得、充実したSEサービスを特徴とするデータセンターとして、世界トップクラスの強固なセキュリティを誇っています。この西東京データセンターを基盤として、社内のITインフラやクラウドサービスへのアクセス環境をアウトソースしたいといった、お客さまの幅広いニーズに応えます。

※3：Secure Access Service Edge　※4：Identity as a Service　※5：Endpoint Detection and Response

事例 CASE STUDY

株式会社フコク 様

グローバル市場で勝つために 個別最適な基幹システムを標準化

標準化とDXでフコクがめざす新たな成長ステージ

自動車のワイパーに使われるワイパーブレードラバーで世界シェア１位を誇るフコクは、ゴム製品を主軸としながら、新規ビジネスにも積極的に取り組んでいます。同社は現在、業務とシステムの標準化を推進しています。その中核となるのが基幹システムの刷新です。長期にわたる大規模プロジェクトは前半を終え、後半に入りました。大規模プロジェクトならではの工夫などについて、フコクのキーパーソン２人に話を伺いました。

内製システムの部分最適と属人化が課題に

1953年に創立したフコクは、ゴム製品を主軸とする製造業です。国内に5カ所の工場を持ち、海外にも拠点を展開。医療、バイオ関連の製品も提供しています。自動車のワイパーに用いるワイパーブレードラバーでは世界トップシェアを誇り、経済産業省の「2020年版グローバルニッチトップ企業100選」にも選ばれました。フコク管理本部システム戦略部部長の目木滋氏は次のように話します。

「当社は中期経営計画（2024～26年度）で、2026年度の売上高1200億円という目標を掲げています。既存事業の強化はもちろん、新規事業の開発も欠かせません。そのためにもデジタル活用と、その土台を支える基幹システムは非常に重要となります」

フコクが基幹システムの刷新を検討し始めたのは、2019年のことでした。フコク管理本部システム戦略部システム企画開発課マネージャーの安積宏氏はこう説明します。

「従来、当社のシステムは、現場担当者がIT部門にニーズを伝え、その要求に沿ってシステムを開発するというスタイルでした。部分最適化されており、今以上の価値をITで実現するのは困難でした。また、担当者ごとの属人化も進んでいました。こうした課題を解決してグローバル市場での競争力を高めるため、トップダウンで業務と基幹システムを標準化するという方針が決まりました」

プロジェクトはコロナ禍でいったん足踏みしたものの、2021年から本格的に再開しました。生産や販売などを含め、ほぼすべての基幹システムを刷新する全社的な取り組みです。基幹システムのコアとなるパッケージソフトとしては、海外製品を含めていくつか検討しましたが、フコクは日本の製造業で多くの実績を持つ「mcframe」を採用しました。

システム	PP(※1)	内容	期間	現フェーズ
基幹システム（SCM）	mcframe 7 SCM	ステップ1：生産、販売	2021年9月～2023年9月	完了
		ステップ2：原価	2024年4月～2025年6月	実施中
PLM	mcframe PLM	技術開発本部　E-BOM	2022年5月～2023年5月	完了
		生産技術部　M-BOM	2024年9月～2025年9月	予定
人事給与	SuperStream-NX	人事給与	2022年9月～2023年6月	完了
インフラ	SOLTAGE	IaaS	2022年4月～2023年6月	完了

フコクの基幹システム刷新プロジェクト（購買EDI、在庫管理システムはスクラッチで実施）

縦割り横断の処理・分析が新システムで高速化

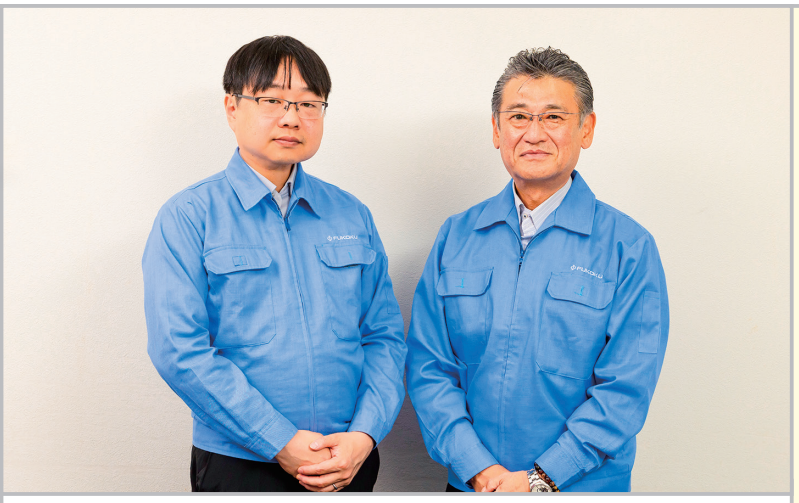
フコクはシステム構築を支援するパートナーを選定するにあたり、mcframeを提供するビジネスエンジニアリング（B-EN-G）に相談したところ、キヤノンITソリューションズを紹介されました。

「パートナーの決定に先立ち、2021年夏ごろ、キヤノンITソリューションズの皆さんが、当社に常駐してヒアリングなどを3カ月間実施しました。業務を深く理解しようという姿勢に感銘を受けました。また、キヤノンITソリューションズが提示した“as is”と“to be”を描いた成果物も、私たちは高く評価しました。こうした3カ月を通じて醸成された信頼感が、パートナー選定の決め手になりました」と目木氏は振り返ります。

※1 Program Product：カスタマイズが可能なソフトウエア製品

◎基幹システムの詳細はこちら

キヤノンITS 基幹システム　検索



株式会社フコク
管理本部
システム戦略部システム企画開発課
マネージャー
安積 宏氏

株式会社フコク
管理本部
システム戦略部
部長
目木 滋氏

株式会社フコク

設　　立　1953年12月24日
代 表 者　代表取締役社長　大城郁男
従業員数　正社員1157人（2024年3月末日現在）
所 在 地　埼玉県さいたま市浦和区高砂一丁目1番1号（本社）
事業内容　ゴム製品、金属・合成樹脂製品、セラミックス、
　　バイオ・医療関連製品の製造販売

基幹システム刷新は大きく2段階に分けて進んでおり、第1ステップでは販売管理および生産管理システムが対象になりました。旧基幹システムの課題はさまざまですが、安積氏が具体例として挙げたのは生産計画の問題です。

「部門ごとに縦割りのシステムだったので、それを横断して処理・分析するのは難しかったのです。例えば、どのような部品や材料をいつ、どれだけ購入し製造するかという、部門をまたがって計画を立てるのが困難でした」

第1ステップの販売と生産の領域は2023年7月に本稼働しました。導入された「mcframe 7 SCM」にはMRP(※2)機能が含まれており、安積氏が指摘した課題は解消に向かっています。

2024年4月にスタートした第2ステップは現在進行中です。在庫管理、原価計算の各システムの刷新が進められており、キヤノンITソリューションズはこれらのプロジェクトもサポートしています。また、第2ステップの最終段階では、管理会計システムの構築が予定されています。

第1、第2ステップのプロジェクトと並行する形で、いくつかのシステム構築も進められました。例えば、スクラッチ開発の購買EDIや、人事給与システム「SuperStream-NX」などがすでに稼働しています。基幹システムとこれらのシステムの基盤としては、ITインフラサービス「SOLTAGE」が活用されています。

必須機能のみアドオン開発
エース級がプロジェクト参画

4年目に差し掛かる基幹システム刷新プロジェクトは、さらに1〜2年続く予定です。とはいえ、その道のりは半ばを過ぎました。プロジェクトを推進する上での工夫について、安積氏は次のように話します。

「基幹システムが変われば、現場の業務も変わります。今までのやり方をあまり変えたくないのが現場の本音でしょう。アドオン開発の要求も多数寄せられました。ただ、それでは個別最適のままですし、属人性も残ります。標準システムに合わせて、業務をいかに標準化するかがポイントです。そこで、アドオン開発を最小化するよう工夫しました」

こうした方針を貫徹できた背景には、いくつかの要因がありました。まず、トップがリーダーシップを発揮し、この取り組みが極めて重要な全社的プロジェクトであるとの経営メッセージを社内に浸透させたこと。加えて、適切なプロジェクト体制を構築したことが重要な点として挙げられます。

「プロジェクトには各職場のエース級を配属しました。また、生産管理システムについては、各工場から1人ずつ指名して参画してもらいました。現場の理解が深く、影響力のある人たちなので、各工場の従業員を巻き込み変革をリードしてくれました」と目木氏は語ります。

将来的に、新基幹システムを活用してフコクがめざすのは、経営と現場におけるデータドリブンです。

「例えば、ある製品の生産をA工場からB工場に移すとしましょう。原価はいくらになるのか、売価は従来のままでいいのか。こうしたシミュレーションをするには、これまで時間も手間もかかっていました。新基幹システムをはじめとするデジタルの仕組みが整備されれば、経営層はデータに基づいて迅速に意思決定することができます」（目木氏）

基幹システム刷新により、フコクのDXが加速します。キヤノンITソリューションズはその取り組みに伴走しつつ、価値の高い提案を続けていきたいと考えています。

※2　Material Requirements Planning：資材所要量計画

日本語校正支援ツールを源流として進化してきた独自の言語処理技術

生成AIの汎用的な能力を人間のアシスタントとして利用するためには、コンピュータに人間の言葉を理解させる自然言語処理技術が不可欠です。当社では以前から独自に言語処理技術に取り組み、さまざまな製品を生み出してきました。キヤノンITソリューションズの言語処理技術について、R&D本部言語処理技術部部長の白川理が解説します。

言語処理技術

幅広く活用されてきた日本語校正支援ツール

言語処理技術とは、コンピュータが人間の言語を理解して処理できるようにする技術であり、AI(人工知能)の分野の一つとして位置付けられてきました。カナ漢字変換や情報検索、機械翻訳など多くの人が日常的に利用するPCやスマホのアプリの中でも活用されています。私が言語処理技術と関わるようになったのは、旧住友金属工業時代に手がけたセキュリティ製品の開発がきっかけでした。

当時、新規事業のアイデアとして、メールの文面をチェックする製品を開発しようということになり、元々あった言語処理のチームと協力して開発に取り組みました。当時、住友金属工業では事業の多角化のためにソフトウエア事業に取り組んでおり、その一つとしてDTP製品を開発し、大学や他企業との共同研究を行い言語処理技術にも取り組んでいました。その一環で日本語の校正支援機能を搭載していましたが、この日本語校正支援ツールの分野で当社は強みを発揮します。研究レベルでは多くの企業が取り組んでいましたが、そんな中で当社だけが当時利用されていたPCのような限られたリソースでも動かすことができる、一般ユーザー向けの日本語校正支援ツールを開発して商品化することができたのです。

当社の日本語校正支援ツールは当時のMicrosoft Wordにも搭載され、新聞社などには各社のルールに対応したカスタマイズされた文章校正支援ツールを提供しました。そして、少ないリソースで実用的に機能する言語処理技術は、企業が送受信する大量のメールの解析にも応用できました。この技術をセキュリティに生かしたのが、私たちが開発した「GUARDIANWALL」です。

言語処理技術が変えたセキュリティの世界

「GUARDIANWALL」シリーズは、従業員の電子メールをフィルタリングしたりアーカイブしたりするツールです。「GUARDIANWALL」には、情報漏えいや誤送信を防止したり、情報漏えい事故が発生した際に調査したりするために、高速パターンマッチや個人情報検索、全文検索、類似文検索といった数々の言語処理技術が応用されています。

「GUARDIANWALL」のリリースは1999年です。当時はこのような仕組みを持ったセキュリティ製品は他にありませんでした。現在では当たり前の内部統制やコンプライアンス等の意識に乏しく、今ほど情報漏えい対策という観点がなかったと思います。技術的なハードルもありました。当時の一般的に運用されていたメールサーバーの能力ではメールの中継だけでなく文章までリアルタイムに解析させるのは難しかったのですが、当社には日本語校正支援ツールで培った高速にテ

図1 キヤノンITソリューションズの言語処理研究の歴史

キヤノンITソリューションズ株式会社
R&D本部
言語処理技術部 部長
大阪大学
大学院情報科学研究科 非常勤講師
白川 理
OsamuShirakawa

キスト解析を行う技術力がありました。

旧住友金属工業時代からUNIX/Linuxの技術者が多くいたことも追い風になりました。「GUARDIANWALL」は国産のセキュリティ製品の草分け的な存在であるとともに、Linux用商用ソフトウエア製品としても最初期のものだったのです。現在では企業のセキュリティの意識も高まっているために、「GUARDIANWALL」の競合製品も増えてきました。それでも「GUARDIANWALL」は国内ナンバーワンのシェア※を誇っています。

言語処理技術の応用範囲が拡大

現在は、企業内で取り扱う情報の量が爆発的に増大しました。しかも情報の多くは言葉として表現されています。企業内情報を利活用したり、大量の情報から有益な知識・ノウハウを抽出したりする目的にも言語処理技術が応用できます。当社は企業内情報検索システムやテキストマイニングツールを開発し、コンタクトセンターの膨大な顧客対応の分析などに活用しています。言語処理技術は、単にテキストを処理するだけでなく、利用者にとって有益で意味のある情報を取り扱う方向に応用範囲が広がってきています。

従来、テキストをコンピュータで処理する場合は、単語はただの記号でしかなく特に意味を持ちません。構文解析で文中の単語間の構造を処理し、辞書と照合することで意味を取り扱う処理を構築していきます。また、深層学習を用いた言語処理では単語をベクトル化して扱います。単語に意味を持たせ、単語同士の意味の近さをベクトルの類似度で表すことができ、意味の合成や単語間の構造の取り扱いをベクトルの演算として実現できます。さらに、機械学習技術の進展により、大量のデータを現実的な時間内で学習することも可能になってきました。生成AIの一つであるChatGPTやGPT-4などは以前では考えられなかったような膨大なデータを学習することにより、汎用的な課題処理能力を持ち、言葉の意味を理解しているかのような振る舞いを見せます。

生成AIを活用するため従来技術との連携

現在生成AIが非常に注目されています。特に大規模言語モデル(LLM)は言語処理技術の今後にも大きな影響を与えるでしょう。これまでは、言語処理技術の開発は常に地道な努力が必要でした。用途ごとに複雑な解析ルールや辞書を作るにしても大変な労力がかかっていました。しかし汎用的なLLMがクラウドサービスとして提供され、APIで必要な機能を手早く試すことができるようになったことは、大きなパラダイムの変化だといえます。

例えば、これまで手作りで取り組んできた実証実験をLLMで構築されたAPIを利用して実施できるようになれば、いろいろなビジネスのDXのスピードが加速するのは間違いないでしょう。しかし、LLMは万能ではなく、その動作原理が明確には解明されていません。ビジネスシーンで厳密な結果を求めるケースなどではそのまま活用できないという指摘もあります。

だからこそ、生成AIの特性・メリットを正しく評価して、従来の技術も合わせて使っていくことが必要になります。例えば、今まで日本語を英語に翻訳したり、長文から要約文を作成したりするような処理では、出力される文章の品質を高めるためには莫大なコストがかかってしまい、個別に構築することは非常に困難でした。生成AIを使うことで、ある程度の品質の出力を比較的低コストで得られる可能性があります。これは生成AIの特徴を生かした使い方といえるでしょう。

さらに生成AIの世界では言語だけでなく、映像や音も同じように扱えるマルチモーダルのAIが登場しています。コンピュータの入力や出力のあり方は大きく進歩しました。その領域でも当社は強みを持っています。AIの活用は業務の効率化や人材不足対応の決め手です。今後の当社の展開にご注目ください(談)。

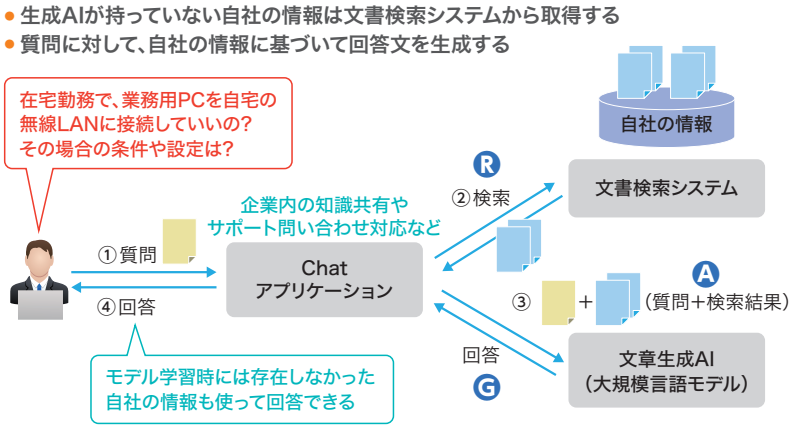


図2 生成AIを利用した問い合わせ応答システム(社内トライアル中)

※株式会社富士キメラ総研『2023 ネットワークセキュリティビジネス調査総覧 市場編』、メールフィルタリングツール部門

NEWS & TOPICS

キヤノンITソリューションズにまつわる
さまざまな情報をピックアップしてお届けします

主な活動・行事

■ キヤノンマーケティングジャパングループが「未来マーケティング企業」としてパーパスを制定

2024年1月29日、キヤノンマーケティングジャパングループは、持続可能な社会の実現のために、マーケティングの力で未来を創る「未来マーケティング企業」を宣言し、キヤノンMJグループの社会的存在意義を定めたパーパス「想いと技術をつなぎ、想像を超える未来を切り拓く」を制定しました。

シンボルマークは、さまざまな想いと技術を大きさと色の違う1つ1つの輪で多様性と共に表現しています。それらがつながり続けていくことで、新しい未来が無限に循環していくことをイメージしています。

想いと技術をつなぎ、
想像を超える未来を切り拓く

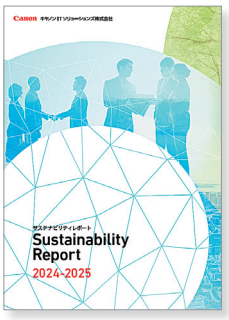
■ 「2024年度入社式」を開催

2024年4月1日、新入社員183名を迎え、入社式を執り行いました。金澤 明社長は、新入社員に向けて知識や組織の壁、過去の成功体験、自己の限界などの境界を越え、新しい世界を拓いてほしいとの想いを込めて、「Beyond Borders」というメッセージを送りました。

■ 「サステナビリティレポート2024-2025」を発行

2024年5月16日、「サステナビリティレポート2024-2025」を発行しました。

キヤノンITソリューションズでは、長期ビジョン「VISION2025」を実現する道筋として、中期経営計画とともに「サステナビリティ戦略」を定めています。サステナビリティレポートでは、新中計の指針である「共想共創カンパニーであるキヤノンITソリューションズは、お客さま課題の解決を通じて社会のサステナビリティを支援する」に基づいた取り組みを紹介しています。



リリース

■ 教職員の日々の業務を効率化する公立小中学校向け新サービス「in Campus School IS」の提供を開始

2024年2月9日、公立の小中学校向けの新サービス「in Campus School IS」の提供を開始しました。学校現場ではICT活用が定着しつつある一方で、教職員の業務負荷増大が課題となっています。本サービスは、学校現場でのニーズに合わせたモジュールの選択利用や校務支援システムとの連携により、効率的な運用で先生方の働き方改革を促進します。

■「SuperStream-NX デジタルインボイスオプション」記者発表会

2024年4月22日、財務会計／人事給与分野に特化した経営基盤ソリューション「SuperStream-NX」の新サービスである「デジタルインボイスオプション」の記者発表会を実施しました。

2023年10月より開始されたインボイス制度により、請求書のチェックが多岐にわたり、多くの企業から業務の効率化が求められています。「デジタルインボイスオプション」は、電子文書をネットワーク上でやりとりするための標準仕様であるPeppolに準拠したデジタルインボイスの発行／受取に対応し、すべての請求書を標準化することにより、お客さまの請求書業務の効率化をめざします。

出 展

■「第8回AI・人工知能EXPO【春】」に出展

2024年5月22日から24日までの3日間、東京ビッグサイトで開催された日本最大級のAI専門展示会「第8回AI・人工知能EXPO【春】」に出展しました。キヤノンITソリューションズは、ものづくり企業としての生い立ちを生かし、長年の研究開発で培った先端技術を強みに、AI技術を活用した先進的な画像・映像ソリューションを提供しています。

<キヤノンITソリューションズブース展示内容>

- **AI検査ソリューション**
  外観検査、非破壊検査の省力化を実現するAI検査プラットフォーム「Visual Insight Station」を紹介。
- **AI商品認識ソリューション**
  店舗商品のマーケティングやサイネージ活用を支援するAI商品認識プラットフォーム「StoreMotion」を紹介。
- **防災AIソリューション**
  「Bind Vision」で提供する、カメラ映像から煙や水位を検出／測定し発災時の迅速な対応に貢献する防災AIソリューションや、地図上での設置カメラの操作を可能にする「カメラ地図連携アプライアンス」を紹介。
- **AI開発支援ソリューション**
  画像とAI解析結果を手軽にダッシュボード表示できるSIer／AI事業者向けクラウドサービス「Bind Vision」を紹介。

告 知

「キヤノンITソリューションズ共想共創フォーラム2024」開催

2024年7月9日(火)～12日(金)にオンライン形式で「キヤノンITソリューションズ共想共創フォーラム2024」を開催します。「『共に想い、共に創るビジネスイノベーション』～これまでのDXを総括し未来を拓く～」を全体テーマにこれまでのDXを振り返ってファクトベースで総括し、現状の課題を明らかにし課題解決へのヒントを提供していきます。そして、キヤノンITソリューションズならではのお客さまへの寄り添い方を通じてビジネスイノベーションを推進し、ビジネスや社会課題に対して変革する姿勢を示していきます。

開催日 **2024年7月9日(火)～12日(金)** 開催形式：オンライン開催

［お申し込みはこちら］ https://news.mynavi.jp/techplus/lp/2024/enterprise/2024_CanonITSforum/
※見逃し配信も予定しています

ITやビジネスの分野で旬なキーワードを簡潔に解説！

3分で分かる！注目キーワード

第4回

モダナイゼーション

[Modernization]

「モダナイゼーション」とは、古くなった企業のITシステムをハード・ソフトの両面で刷新・改善して業務に適応させることです。それが必要な理由は、一度作った大規模ITシステムは長期間使い続けるため、やがてビジネス環境の進化に対応できなくなるからです（図1）。企業にとってモダナイゼーションは、DX（デジタルトランスフォーメーション）遂行のための重要なプロセスといえます。

モダナイゼーションの代表的なケースは、「レガシーシステム」のハードウエアを置き換えてパフォーマンスの向上を図り、合わせてソフトウエアを置き換えて最新の業界標準に最適化させることです。レガシーシステムとは、メインフレーム（大型汎用機）で構築された旧来のITシステムの総称で、肥大化、複雑化、ブラックボックス化や処理スピード不足、拡張性不足などが課題となっています。もちろんハードとソフトの両方で全システムを刷新できれば一気に最先端のIT環境を確立できますが、長年管理・運用してきた大量のデータや従業員の活用ノウハウを短期間で新システムに移行するのはかなりハードルが高いといえます。

情報システムを最新のものに

そのような中、レガシーシステムを活用しながらモダナイゼーションを実施するための技術として、「クラウドコンピューティング」「コンテナ化」「AI（人工知能）活用」などが挙げられます。

クラウドコンピューティングは、クラウド上のソフトやサービスを活用してレガシーシステムのままで情報処理を迅速化させます。コンテナ化はアプリケーションとその実行環境をまとめる仮想技術で、アプリの開発や実装を容易にしてレガシーシステムの移植性を高めます。AI活用は、システムによる業務の自動化やプロセス改善などを行います。企業には「生産性向上」「セキュリティ強化」「システムが誰でも使えるようになる」などのメリットがあります。

PwCコンサルティングは2023年12月、売り上げ500億円以上の企業を対象にした「2023年DX意識調査-ITモダナイゼーション編-」を公開しました。それによると、「アジャイル開発（ソフトを縮小化して迅速化する開発）」「パブリッククラウド」「クラウドネイティブ技術（最初からクラウド上でシステム開発することを前提とした技術）」のすべてを活用する企業が61%にまで増えるなど、大企業のモダナイゼーションが進んでいることが明らかになりました。

労働人口の減少や激化する競争に直面している企業にとって、生産性の向上が必須とされています。そのためのIT施策として、モダナイゼーションは今後さらに重要になってくるでしょう。

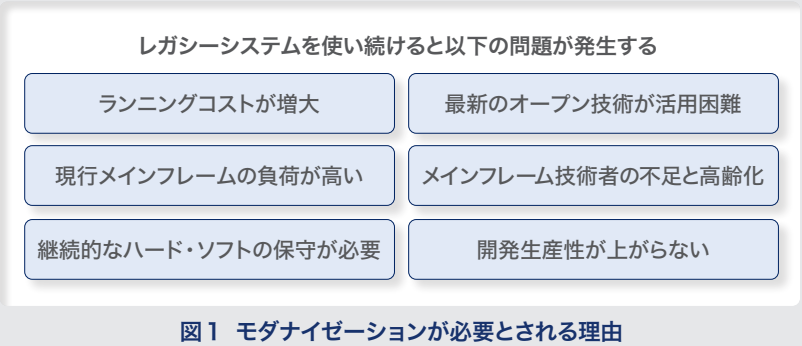


図1　モダナイゼーションが必要とされる理由

from キヤノンITソリューションズ

モダナイゼーションへのはじめの一歩は「脱レガシーシステム」です。進め方にマイグレーション（移植）とモダナイゼーション（近代化）があります。まずはマイグレーションで最新環境へ「経済的・短期間・安全」に移植し、その後にコンテナ化やクラウドネイティブ技術を活用し、レガシー言語を別言語へ変換することでモダナイゼーションへステップアップします。

キヤノンITソリューションズ株式会社
ビジネスソリューション統括本部
ビジネスソリューション第二開発本部 第二開発部 部長
戸村 浩明
Hiroaki Tomura

◎さらに詳しい内容はWebで
https://www.canon-its.co.jp/solution/migration/

富岡製糸場

上質な生糸の大量生産で絹の世界的な普及に貢献

明治維新後、欧米と肩を並べる近代化をめざす日本をけん引したのが繊維産業です。中でも輸出の主力品だった生糸の生産性と品質の向上のため、明治政府は1872年(明治5年)、群馬県富岡市に官営の「富岡製糸場」を設立しました。この地が選ばれた理由は、昔から養蚕が盛んだったことや、広大な敷地、大量の水を確保できたためです。設立にあたっては、民部・大蔵省の役人だった渋沢栄一が設置主任の一人として尽力しました。

最新器械繰糸の指南役として、フランスから生糸の検査技師ポール・ブリューナらが招聘されました。工女は全国から若い女性が集められ、会得した技術を故郷で広める責務も担っていました。当時、世界最大規模を誇った繰糸所には、300個の釜が設置されていました。釜で煮た繭から糸を繰るのは楽な作業ではありませんでしたが、「質の高い生糸の生産には労働環境の整備が必要」とのブリューナの理念に沿い、敷地内には診療所や夜間学校が設けられていました。工女たちは日々、入浴もできたそうです。

時代の変遷とともに製糸場は民営となり、繰糸所内の設備は自動繰糸機に代わりましたが、れんが造りの倉庫などを含めて建物はかつてのまま受け継がれました。上質な生糸の大量生産を実現した技術革新と海外との技術交流に加え、高価な絹を世界的に広く普及させたことが評価され、2014年(平成26年)には群馬県内の関連資産3件と併せて「富岡製糸場と絹産業遺産群」として世界文化遺産に登録されました。

住　所　〒370-2316 群馬県富岡市富岡1の1
アクセス　[電車] 上信電鉄 上州富岡駅から徒歩約15分
[車] 上信越自動車道 富岡ICから各駐車場まで約10分、駐車場より徒歩10分(近隣無料駐車場あり)

画像提供　富岡市／富岡製糸場

READER SURVEY
読者アンケート
ご協力のお願い

今後の企画の参考にさせていただくために、
読者アンケートにご協力ください。
皆さまからの忌憚のないご意見・ご感想を
お待ちしております。

［ご回答方法］
以下のURL（QRコード）からご回答ください。

STIC×DREAM読者アンケート　検索

https://reg.canon-its.co.jp/public/application/add/19440

次号STIC×DREAM Vol.12は、2024年12月発行予定です。
https://www.canon-its.co.jp/stic-dream/

Canon
キヤノンITソリューションズ株式会社

EDITOR'S NOTES［編集後記］

読者の皆さまにさらに有益な情報をお届けするため、「STIC×DREAM」をリニューアルいたしました。本号では、社会やビジネスなどさまざまな場面で重要性を増しているサイバーセキュリティの最新トレンドを特集します。さらに、キヤノンITソリューションズがどのような技術やソリューションを通じて社会課題を解決に導いているかを紹介する新企画もスタート。リニューアルを経て、さらに魅力的かつ実用的な内容で、皆さまのビジネスの一助となることをめざします。今後とも「STIC×DREAM」へのご期待、そしてご支援を心よりお願い申し上げます。

STIC×Dream［スティックバイドリーム］
Vol.11
SPRING/SUMMER
2024

編集・発行　キヤノンITソリューションズ株式会社 企画本部　〒108-0075　港区港南2-16-6　キヤノンSタワー　☎03-6701-3603
発行人 横坂一／制作 日経BP・日経BPコンサルティング／印刷 株式会社プレシーズ