Ⅲ－３　ビジネス機器業界各社のセキュリティ関連技術動向

浦川 豊*

１．はじめに

デジタル活用が経営の中核に位置付けられる現在、企業を取り巻くセキュリティリスクはかつてないほど高まっている。クラウドサービスの利用拡大やテレワークの定着により、業務の柔軟性と生産性は向上した一方で、情報資産の管理範囲は広がり、情報資産を狙うサイバー攻撃は年々高度化・多様化している。ひとたび情報漏えいやシステム停止が発生すれば、事業継続に深刻な影響を及ぼすだけでなく、企業の社会的信頼が大きく損なわれるリスクも否定できない。こうした背景から、セキュリティ対策は IT 部門だけの課題ではなく、経営課題として捉えられるようになっている。ビジネス機器業界においても、複合機やプリンターといった製品そのものの機能向上に加え、セキュアな運用管理や情報資産の保護を支えるソリューションの提供が強く求められている。

これらのことを踏まえて、各社のセキュリティ観点での対応を行っているソリューションや製品について、2024 年以降の JBMIA 会員企業のニュースリリースや一般公開されている技術情報などを情報源として調査した。本記事では、第 2 章でセキュリティ関連ソリューション、第 3 章で複合機のセキュリティ関連技術について、それぞれの事例を紹介する。

２．セキュリティ関連ソリューション

情報資産の予期せぬ流出を防止し、安全に情報資産を活用できるようにするためのセキュリティ関連ソリューションがビジネス機器業界各社より提供されている。

2.1　リコー

高セキュリティなオンプレミス環境での生成 AI 活用を、導入から運用までワンストップで支援する「RICOH オンプレ LLM スターターキット」を 2025 年 4 月より提供開始すると発表した。近年、企業のさまざまな業務への生成 AI 活用が検討されており、AI 活用にはデジタル人材の確保や開発にかかる工数・費用への対応など、さまざま課題が存在している。また、セキュリティやプライバシー、ガバナンスなどの観点から、オンプレミスや自社データセンターなどの社内専用環境で AI を利用したいと考える企業も多く、オンプレミスでの LLM 活用に対するニーズが高まっている。こうした背景から、「RICOH オンプレ LLM スターターキット」は、オンプレミスでセキュアに生成 AI を活用するのに必要な環境構築、導入、運用支援までをパッケージで提供するソリューションとなっている。顧客の社内ネットワーク環境下に GPU サーバーを設置し、オンプレミス LLM をローカル環境で利用でき、プロンプトを含むすべての情報を社内ネットワークのみで処理するため、高いセキュリティを確保し、安心して利用できる。また、オンプレミス LLM の動作環境の構築、設置、導入時の教育に加え、メールでの問い合わせサポートや LLM モデルの追加情報提供など、継続した運用支援を行うとのことである。

（2025 年 4 月 7 日のニュースリリース
https://jp.ricoh.com/release/2025/0407_1）

リコージャパン株式会社（以下、リコージャパン）と、株式会社セキュア（以下、セキュア）は、フィジカルセキュリティ分野の事業拡大を目的とした、資本業務提携契約を締結したことを 2026 年 3 月に発表した。ハイブリッドワークの普及やデータ活用の進展に

伴い、オフィスや工場、物流施設などのワークプレイスでは、利用状況の可視化による働き方改革や安全管理の需要が高まっていることが協業の背景として挙げられる。協業を通じて、セキュアが持つ専門的な知見やシステムインテグレーションのノウハウを活用し、リコージャパンのフィジカルセキュリティ分野の提案力と導入体制を強化する。両社は、データ活用と AI 分析により、ワークプレイスの DX とセキュリティ強化を同時に実現できるソリューションの創出を目指し、直近では、セキュアが提供するフィジカルセキュリティ分野のデータと、ワークプレイスを統合的に管理するデジタルプラットフォーム「RICOH Spaces」とのデータ連携を予定している。セキュアのセキュリティソリューションがワークプレイスにおける人の活動を捉える“目”となり、そのデータを「RICOH Spaces」と組み合わせることで、“はたらく”の質を高める新たな価値創出を目指すとのことである。

（2026 年 3 月 9 日のニュースリリース
https://jp.ricoh.com/release/2026/0309_1）

2.2　富士通

AI サービス「Fujitsu Kozuchi」のコア技術として、攻撃や防御などのセキュリティに特化したスキルやナレッジを持つ複数の AI エージェントを連携させることで、企業や公共団体の IT システムにおいて脆弱性を悪用する攻撃や生成 AI への攻撃、といった新たな脅威へのプロアクティブなセキュリティ対策を支援する、マルチ AI エージェントセキュリティ技術を開発した。組織や拠点をまたぐ複数の AI エージェントを透過的に連携できるマルチ AI エージェント連携技術、プロアクティブなセキュリティ対策に必要な AI エージェントを実現するセキュリティ AI エージェント技術、生成 AI のセキュリティ耐性について自動で網羅性高く確認を行って攻撃を自動的に防御・緩和する生成 AI セキュリティ強化技術、という 3 つの技術で構成されている。マルチ AI エージェントセキュリティ技術により、セキュリティの専門家ではない IT システム管理者や運用担当者が、プロアクティブなセキュリティ対策を実現するアプリケーションを構築できるようになり、今後、急速な普及が見込まれる生成 AI の企業 IT システムでの活用においても、生成 AI の効果を享受しながら、安心・安全に IT システム運用を行うことが可能となる。本技術により、世界の繁栄と安定が両立する、信頼性のあるデジタル社会を共に創るという「デジタル社会の発展」に貢献する価値を顧客や社会に提供するとのことである。

（2024 年 12 月 12 日のニュースリリース
https://info.archives.global.fujitsu/jp/news/2024/12/12.html）

富士通のグループ会社であるエフサステクノロジーズは、大日本印刷（DNP）と共同で、官公庁・金融機関・製造業など高いセキュリティ要件を持つ分野向けにオンプレミス型の生成 AI ソリューションを 2025 年 11 月より提供開始すると発表した。本ソリューションは、クラウドを介さず自社内のサーバー環境で生成 AI を活用できる点が特長であり、官公庁、金融機関、製造業など、機密データを外部に出せない業種での利用を想定している。具体的には、DNP が独自に開発した「DNP ドキュメント構造化 AI サービス（AI-Ready Data）」を、エフサステクノロジーズの「Private AI Platform on PRIMERGY」に搭載した構成である。PDF や Word といった非構造化文書を、生成 AI が扱いやすいデータ構造に変換することで、文書検索やナレッジ活用の精度向上を図れる。技術の伝承、各種文書の検索、品質管理など幅広い業務に応用が可能である。また、生成 AI 基盤はオンプレミス環境で稼働するため、内部文書・顧客情報・生産データなどの機密情報も安全に処理できる。さらに、エフサステクノロジーズの「Private AI Platform on PRIMERGY」は、スモールスタートから大規模展開まで対応可能な複数モデルをラインアップし、エフサステクノロジーズの「uSCALE サブスクリプションモデル」も利用可能である。導入検討から運用・保守までをワンストップで支援し、企業の AI 導入負荷を大幅に軽減できる。今後、両社は官公庁や金融、製造業に加え、教育・医療・自治体など厳重な情報管

理が求められる分野にも生成 AI の活用支援を拡大し、企業や自治体の DX を加速させる。クラウド環境に依存しない新たな選択肢として、日本発のセキュア AI 基盤の普及を推進し、安全・安心で利便性の高い社会の実現に貢献するとのことである。

（2025 年 11 月 12 日のニュースリリース
https://www.fsastech.com/ja-jp/resources/press-releases/2025/1112.html）

2.3　ブラザー工業

プリンターや複合機の印刷時にユーザー認証を行い、安全に紙文書を印刷できるソリューション「セキュリティ印刷アドバンス」を 2025 年 11 月に発売すると発表した。「セキュリティ印刷アドバンス」は、ブラザーのプリンター・複合機に連携させ、印刷時に社員証などの IC カードをかざす、または PIN コードを入力するだけでユーザー認証が可能である。認証するまで印刷が開始されないため、印刷物が第三者の目に触れるリスクを未然に防ぎ、印刷物の取り違えや放置によるセキュリティリスクを低減できる。また、同一ネットワークに接続され、セキュリティ印刷アドバンスが有効化されているプリンターであれば、場所を選ばずどの機器からでも印刷が可能である。使用中のプリンターを避けて空いている機器で印刷できるほか、異なるフロアやエリアでも近くの機器から印刷できるので、待ち時間の短縮や業務の効率化に貢献する。さらに、買い切り型なので、継続的な月額費用を気にすることなく導入が可能であることで予算管理が容易になり、コストの見通しが立てやすくなるとのことである。

（2025 年 11 月 12 日のニュースリリース
https://www.brother.co.jp/news/2025/secure-print/index.aspx）

2.4　キヤノン

キヤノン IT ソリューションズ株式会社(以下、キヤノン ITS)は、IT インフラサービス「SOLTAGE」の新たなセキュリティラインアップとして、株式会社 JSecurity が提供する個人情報漏えい対策ソリューション「PCFILTER」を 2024 年 6 月より提供開始した。組織による個人情報の厳格な管理が求められる一方、個人情報流出の事故は増加し続けており、漏えい対策は企業の責任として一層強化が必要となっているが、セキュリティ管理体制の整備は容易ではないため、効率よく個人情報漏えい対策を行うことが可能なソリューションが注目されている。「PCFILTER」は、個人情報を含むファイルを高速で自動検出し、管理者による適切な対処と管理を実現する。個人情報ファイルがどの端末にどれだけの件数を保有しているか確認することができ、管理画面上に個人情報保護アクション数の推移や個人情報検出状況などのグラフ表示も可能であり、組織内の個人情報の取り扱い状況を一元管理できるため、情報セキュリティ管理者の負担を軽減する。また、管理対象ファイルを隔離/暗号化して安全に保管し、保管が不要となったファイルは完全に削除できる。さらに、個人情報ファイルの保存媒体への転送/印刷指示/メール添付など、さまざまな外部流出経路を自動で遮断できる。IT インフラに関するすべての領域に対応するサービス「SOLTAGE」ブランドのもと、クラウドセキュリティ領域をはじめとするサービスラインアップの拡充に継続して取り組み、今後もセキュリティ対策や情報漏えい対策に課題を抱える顧客をワンストップで支援するサービス/ソリューションを提供するとのことである。

（2024 年 6 月 24 日のニュースリリース
https://www.canon-its.co.jp/corporate/newsrelease/2024/pr-0624）

キヤノン ITS は、IT インフラサービス「SOLTAGE」の新たなセキュリティラインアップとして「セキュリティ対策診断サービス」を 2025 年 6 月より提供開始した。サーバーやネットワークなどの IT インフラ領域へのサイバー攻撃によりセキュリティホールを攻撃者に悪用される事例も多く、セキュリティ対策の実施が急務であるが、セキュリティリスクがどこにあるか、何から対策していくべきかの判断ができないことには対策ができない。そのため、セキュリティ対策を実施

する以前に、自社のシステムが抱えるセキュリティリスクを把握して、優先順位をつけて対策のアクションを計画することが重要となっている。「セキュリティ対策診断サービス」は、キヤノン ITS においてマルウェア解析やセキュリティ技術研究などの専門組織である「サイバーセキュリティラボ」の専任エンジニアが、大学や業界団体との研究も踏まえた高度な知見をもとに、セキュリティリスクの見える化を実施する。最新の世界標準「NIST Cybersecurity Framework 2.0」に基づき、セキュリティリスクを「識別/防御/検知/対応/復旧」の 5 つに「統治」を加えた 6 段階で体系的に診断/評価し、診断結果をもとに分析した結果をレポートとして提供する。セキュリティ対策状況を 30 以上のヒアリング項目から可視化し、セキュリティの課題を抽出する。また、報告会を開催して課題に対する優先順位をつけてわかりやすく解説するとともに、各リスクに対する最善のセキュリティ対策を提案する。今後、ヒアリングに基づく診断に加え各種診断ツールを活用したより深く高精度な診断が可能なメニューの追加も計画しているとのことである。

（2025 年 6 月 5 日のニュースリリース
https://www.canon-its.co.jp/corporate/newsrelease/2025/pr-0605）

キヤノン ITS は、IT インフラサービス「SOLTAGE」の新たなセキュリティ運用サービスとして、「Cato SASE クラウド」を対象とした SOC（Security Operation Center）サービスを 2026 年 3 月より提供開始した。近年、インターネットに接続された IT 資産に対するネットワークとセキュリティ管理の高度化を目的として、SASE（Secure Access Service Edge）の導入/利用が進んでいるが、SASE の運用には高度な専門知識と即時対応体制が不可欠であり、多くの企業にとって自社のみでの運用は困難となっている。このような状況のなか、常時異常を監視し、セキュリティログやイベントの適切な管理、脅威検出時の迅速な対処を行う SOC の役割を、外部の専門組織に委託する企業が増加している。「Cato SASE クラウド向け SOC サービス」では、「Cato SASE クラウド」による脅威検出およびその対策を顧客に提供し、インシデント発生時には初動対応から恒久対応の立案、提案までを一貫して担う。SOC に収集されたログ/発報されたアラートは AI により自動的に相関分析され、脅威度と緊急度を評価しインシデントをシナリオ化した上で、対処方法を提示する。AI による分析の結果、マルウェア感染などが疑われる端末については、SOC システムから端末にインストールされている MDR ソフトウェアに指示を出し、人手を介さず自動的にネットワークから隔離する。また、「Cato SASE クラウド」の利用状況を定期的に分析し、セキュリティ観点からのレポートも行う。連携対象サービスを順次拡充し、顧客のネットワーク環境を包括的に保護できるサービスへと拡大していくとのことである。

（2025 年 11 月 27 日のニュースリリース
https://www.canon-its.co.jp/corporate/newsrelease/2025/pr-1127）

2.5　コニカミノルタ

コニカミノルタジャパン株式会社(以下、コニカミノルタジャパン)は、Sophos(以下、ソフォス)と協働し、中小企業の IT 環境を総合的に支援するサービス「IT-Guardians（ガーディアンズ）」において、新サービス「IT-Guardians MDR サービス」を 2025 年 12 月に提供開始した。近年、ランサムウェアなどのサイバー攻撃はより高度になり、攻撃を防ぐだけでなく、迅速に検知し対応することが求められているが、こうした仕組みを自社で構築するには IT の専門人材や常時監視の体制が必要であり、多くの中小企業にとって負担が大きいのが現状となっている。そこで、企業のサーバーや全社員のパソコンへアプリを入れることでサイバー攻撃などを常に監視でき、安心して高度なセキュリティ運用を実現できるにした。①ウイルスやサイバー攻撃から守る EPP（Endpoint Protection Platform）、②脅威に対処する EDR（Endpoint Detection and Response）、③ソフォスの監視センターSOC（Security Operation Center）による 24 時間監視を提供することできるため、これまで導入を見送っていた中小企業で

も MDR（Managed Detection and Response）導入が可能となりあらゆる企業規模に応じたセキュリティ強化を実現できる。「IT-Guardians」では問い合わせに応える IT サポートサービスを提供しており、パソコンの操作方法からセキュリティ対策に関する困りごとの解決まで、幅広く請け負うことで IT 担当者の負担を軽減しながら業務効率を高めることができる。IT 人材が不足する中小企業でも、ソフォスが提供する EDR を含む高度なセキュリティ対策を利用可能となり、企業の重要なデータを守る強固なセキュリティ環境を構築できるとのことである。

（2026 年 1 月 22 日のニュースリリース
https://prtimes.jp/main/html/rd/p/000000096.000040232.html）

３．複合機のセキュリティ関連技術

評価機関によるセキュリティ評価によって様々なセキュリティリスクに対して堅牢であることを証明する各種認証を取得した製品、機密性・完全性・可用性を担保するため各種セキュリティ機能を充実させた製品、がビジネス機器業界各社より提供されている。

3.1　シャープ

シャープの国内向けデジタル複合機である「BP-70/60/50/40/C5」シリーズほか、海外向けモデルを含む計 44 機種が、米国の独立評価機関 Keypoint Intelligence 社とテストパートナーである Agile Cybersecurity Solutions（ACS）による厳格なセキュリティ評価「Device Penetration Testing」に合格し、「Security Validation」を獲得したことを 2025 年 2 月に発表した。「Device Penetration Testing」は、デジタル複合機の潜在的なセキュリティリスクを包括的に評価し、ファームウェアやネットワーク接続経路などの脆弱性を診断するセキュリティテストである。セキュリティ機能の有無のみならず、実際に意図的なサイバー攻撃を加えて堅牢性を評価している。そのため、「Security Validation」は、対象の複合機がさまざまなサイバー攻撃から適切に保護され、推奨設定においてセキュリティ面で高い堅牢性があることを証明するものとなっている。長年、複合機のセキュリティ対策機能の強化に取り組んでおり、今後もよりセキュアな環境で企業の DX 推進や業務効率化に貢献するソリューション提案を進めていくとのことである。

（2025 年 2 月 10 日のニュースリリース
https://corporate.jp.sharp/news/250210-a.html）

3.2　富士フイルムビジネスイノベーション

デジタル複合機「Apeos」シリーズとプリンター「ApeosPrint」シリーズにおいて、サプライチェーンにおけるセキュリティの　の国際標準規格である「ISO/IEC20243」の第三者認証を取得したことを 2024 年 8 月に発表した。本規格の第三者認証の取得は、国内デジタル複合機メーカーでは富士フイルムビジネスイノベーションが初めてとなる。このことは、製品セキュリティのための技術的な対策だけでなく、サプライチェーン攻撃対策まで含めたライフサイクル全体での完全性確保を重視した対策であり、国際規格・第三者評価への対応を重要視している証拠と考えられる。今後も、先端情報技術の商品・サービスへの活用、高度な情報セキュリティサービスの提供ならびに適切な品質管理を通じて、顧客の情報セキュリティ確保に貢献するとのことである。

（2024 年 8 月 21 日のニュースリリース
https://www.fujifilm.com/fb/ja/news/244）

3.3　コニカミノルタ

多様化するセキュリティリスクに対処するため、複合機起点の情報セキュリティ対策技術のホームページにおいて 2 つの機能を紹介している。一つ目は「bizhub i シリーズ」にて業界で初めて複合機にウイルス検知技術を搭載した。AV-TEST で高検出率を誇るウイルススキャンエンジン(Bitdefender 社)を採用することで、複合機自身の感染防止にとどまらず他の PC やサーバーへの拡散を防御し、複合機が企業の情報漏洩の踏み台になることを防ぐ。また、複合機と外部環境との間で様々なインタフェースでやり取りするデータを常に

監視するため、オフィス内の複合機に侵入してくるウイルスやマルウェアを即座に検知し、ファイルの削除などの処理を自動的に行う。さらに、定期的に複合機内のファイルをスキャンし、リスクのあるファイルを発見し、潜在リスクを検知する。これらにより、オフィスのセキュリティを確保し、顧客のオフィスセキュリティ向上の要望に応えている。二つ目は IoT 機器などの動作状況を監督・管理する SIEM 連携である。複合機も IoT 機器の一つとして、SIEM で管理できるように、標準規格である「Syslog」によるログ送信機能を搭載している。これにより「深夜などの就業時間外にログインしている」、「深夜に大量にスキャンしている」といったアクセス監視が一元管理できるようになり、他の IoT 機器と合わせて IT 管理者が適切に対処することができる。また、CEF、LEEF といったログフォーマットが送信可能で、様々な SIEM アプリとの連携が可能となっている。これらのプリンターや IoT 機器などのネットワークに接続される商品を脅威から守る技術を搭載することで、顧客に安心と安全を提供するとのことである。

（https://research.konicaminolta.com/jp/technology/tech_details/itsecurity/）

3.4　京セラドキュメントソリューションズ

情報セキュリティマネジメントシステム（ISMS）、および ISMS クラウドセキュリティ認証の更新を 2025 年 10 月に完了したことを発表した。ISMS は Information Security Management System（情報セキュリティマネジメントシステム）の略で、情報資産に対するセキュリティ上のリスクを組織において管理するための仕組みとなっている。2017 年に複合機、プリンター業界で初めてクラウドセキュリティ認証を取得しており、リモートで複合機やプリンターの管理・メンテナンスを行うサービスである「KYOCERA Fleet Services」にて認証を取得済みである。また、ISMS の対象範囲をソフトウェア開発部門全体に拡大し、顧客の情報資産保護とセキュリティ強化に継続的に取り組んでいる。今後も、ドキュメントソリューションサービスの品質向上に努め、顧客が安心して利用できるサービスを提供することで、信頼される企業を目指すとのことである。

（2025 年 12 月 10 日のニュースリリース
https://www.kyoceradocumentsolutions.com/global/ja/news/rls_2025/rls_20251210.html）

3.5　キヤノン

「imageFORCE」シリーズはゼロトラストを前提としたデバイスセキュリティの強化を行っており、文書による情報漏えいを抑止するドキュメントセキュリティ、複合機本体を守るデバイスセキュリティ、盗聴やなりすましを防止するネットワーク＋クラウドセキュリティといった複合機活用の 3 つの側面すべてから様々な脅威に対応している。そのため、あらゆる面から安心・安全を確保して信頼性を向上させた製品となっている。デバイス内の環境推定エンジンが、データの流れのパターンを分析して環境推定を行い、最適なタイプを選択するだけで、80 以上のセキュリティ関連項目を一括で設定できる。暗証番号や IC カードなど、2 つ以上の異なる認証要素を組み合わせる多要素認証を強化しており、暗証番号に加えパターン認証も使用可能である。本体起動時は不正プログラムの混入がないかシステムを検証し、安全性を確認してから起動する。また、稼働中もプログラムの改ざんや未知のモジュールの実行を阻止して、様々な攻撃からデバイスを保護しシステムの信頼性を向上させている。さらに、NIST（米国国立標準技術研究所）が策定した暗号化規格に準拠し、FIPS140-3 認証を取得しているため、最新のハイレベルな技術で、ストレージの全データ、ネットワーク上を流れるデータを暗号化して保護している。

（　https://canon.jp/biz/product/printer/office-mfp/branding/features-common/reliability）

3.6　セイコーエプソン

プリンター・複合機・スキャナーを取り巻くさまざまな脅威から情報資産を守るため、製品の企画から開発・評価・製造・販売・保守までライフサイクル全体を通じた製品セキュリティを実践している。また、脅

威に対する様々な対策となる機能を搭載しており、ファームウェア署名検証・セキュアブート・監査ログ機能・ランタイム侵入検知・認証印刷・認証スキャンなどが挙げられる。独自開発したプリンター・スキャナー制御用 IC と、メカ制御、画像処理などさまざまな処理を最適に使い分ける独自のファームウェアを組み合わせることで、高性能かつ安全性に優れたプラットフォームを実現している。特にセキュリティリスクの高い通信部とその他の情報処理部を分離した制御によって、外部からの不正アクセスを防ぎ、情報資産を保護している。ライフサイクル全体を通じて、ソフトウェアとハードウェアの両面から最適な対策を施し、安心して利用できる製品を提供するとのことである。

（https://support.epson.net/security/ja/）

2025 年度「ビジネス機器関連技術調査報告書」“Ⅲ－３”部

発行　2026 年 6 月
一般社団法人 ビジネス機械･情報システム産業協会（JBMIA）
技術調査専門委員会
〒108-0073　東京都港区三田三丁目 4 番 10 号 リーラヒジリザカ 7 階
電話　03-6809-5010（代表） / FAX　03-3451-1770