Security White Paper 2024

ITセキュリティトレンド概況

注目10業種の動向と今後

ソリトンが支援している幅広い市場および顧客について、10 の業種カテゴリーに分け、IT の観点におけるそれぞれの特性や注力分野、セキュリティに対する取り組みなどの現況を解説します。あわせて業種ごとの課題およびニーズに最適なソリトンの製品・ソリューション・サービスを紹介することで、これからのセキュリティ強化を実現する視点を示します。

2024 / 1

はじめに

本資料では、株式会社ソリトンシステムズ（以下、ソリトン）が支援している幅広い市場および顧客について、10 の業種カテゴリーに分け、IT の観点におけるそれぞれの特性や注力分野、セキュリティに対する取り組みなどの現況を解説する。あわせて業種ごとの課題およびニーズに最適なソリトンの製品・ソリューション・サービスを紹介することで、これからのセキュリティ強化を実現する視点を示すことを目的としている。

業種ごとの各論を紹介するに先立ち、次項では IT 分野における現状と今後についての見解を解説する。

目次

IT セキュリティトレンド概況［2023－2024］

IT投資とDXの進捗

- 経済は不安定な世界情勢、資源価格の高止まり、欧米の金融引き締め、円安による物価高の長期化などにより、不透明な状況が継続している。

- IT 投資については、企業、官公庁/自治体の DX（デジタルトランスフォーメーション）による業務プロセスやビジネスモデルの変革への取り組みが引き続き旺盛に推移し、レガシーな基幹系システムからクラウドを活用したシステムへの刷新が進み始めている。

- 2023 年は、2030 年までに DX が実現していくマイルストーンの中での 1 年と捉えることができる。DX の実現までのステップは、①デジタル化 ②効率化 ③共通化 ④組織化 ⑤最適化 とされる。各社の DX 推進の進捗具合を見ると、②～③に差し掛かっている企業が多いように見受けられる。

- DX やオートメーション化が進む中、これまではスタンドアロンでの利用用途が多く、属人的かつ閉鎖的な環境で利用、運用されてきた IT システムは、変わりつつある。システム同士が連携できることはもちろん、人と人との間でもコミュニケーションが図れ、繋がることができる、共存共栄できるものだけが生き残る時代へと変化していくことが予測される。

セキュリティにおけるトレンド

- セキュリティにおいては、あらゆる業種、業務において IT 活用が定着する一方、サイバー攻撃が増大し、被害が広がっている。中でもランサムウェア攻撃が悪質化し、企業等に金銭要求と機密暴露を行う「二重恐喝」の被害案件が急増した。

- 加えて、セキュリティ対策が手薄な企業を起点として、標的とする企業を入り口とするサプライチェーン攻撃も製造業をはじめ、被害が相次いだ。

- これらのことから、各企業・団体においてセキュリティ強化の需要も拡大している。

これからのセキュリティとソリトンの対応

こうした状況への対応策として、IT セキュリティのベースとなる「認証」や、脅威のひそむインターネットにおける「安全なWeb 閲覧・クラウド利用」、「安全なファイル受け渡し」といった、ソリトンが以前から得意とするソリューションが改めて注目されている。

さらに、課題点の抽出およびセキュリティ対応組織の構築には、ソリトンが提供する「Attack Surface Management サービス」や、「CSIRT 構築ベストプラクティス」などの利用も拡大してきている。

ソリトンはこれまで、認証の仕組みを個社単位で提供してきた。しかし多くのITシステムがクラウドに移行した現在、そこで適切な認証を提供するには、各社のITシステム単体としてだけではなく、ERP や経費精算、入出金など、あらゆるクラウドサービスとの連携が必要になる。
そして、今や認証はMaaSをはじめ、生活の中でも欠かせない存在となってきている。安全な認証でつながる対象が広がれば、クラウドの可能性はさらに増していく。クラウドサービスが企業間同士のITシステムのコネクターとしての役割を果たす上で、ソリトンはそのつながりに安心・安全を提供し支えていくことが役割であると認識し、活動していく。

[1] 製造業

素材を加工・組み立てし、製品として販売して利益を得る業態。大きく素材、加工・組み立て、自社生産・加工の3種類に分類される。扱う製品は、自動車や電気機器、医薬品や化学素材、食品など多岐に渡る。

業種の特徴

- 「インダストリー4.0」や「スマートファクトリー」のかけ声の下、「サービス化」「プラットフォーム化」などが製造業 DX のトレンドとなっている。これまでは工場内ネットワーク（OT：Operational Technology）と IT（Information Technology）は分離される（つながっていない）ケースが主だったが、近年では製造機械へのメンテナンスや加工データ入力などで IT 活用が進み、各機器・デバイスのインターネットへの接続も増加。工場ネットワークの IoT 化が進んでいる。

- 原材料の調達から製造、流通、販売までの流れをひとつの連鎖（サプライチェーン）とみなし、業務プロセスを最適化するサプライチェーンマネジメント（SCM）が求められ、IT システムもその内の重要な役割を占める。経済産業省や IT ベンダー各社が官民連携による IoT 等を通じてスマート化の取り組みを推し進める一方、変化に伴う脆弱性はサイバー攻撃の対象となることから、セキュリティ面の対応が急務となっている。

- セキュリティについては現在、脅威検知および可視化ソリューションへの関心が高い状況にある。

2023 年の動向

- セキュリティ対策がより脆弱なサプライチェーンを狙ったランサムウェアなど、サイバー攻撃被害が多発したことを受け、製造業においては関連するさまざまなガイドラインが設けられ、それらをベースに対応が進められている。

- 自動車産業では、日本自動車工業会が「自動車産業サイバーセキュリティガイドライン」（以下、自工会 CS ガイドライン）を 2020 年 3 月に発行。2023 年 9 月には V2. 1が公開され、企業規模を問わず、自動車産業に連なる企業は一定レベルの要求内容の達成を目指すよう号令が掛かった（法的な罰則はなし）。そのため、同ガイドライン掲載チェックシートを元に、LV2 に当たる「自動車業界として標準的に目指すべき項目（パスワード設定、ログ管理ほか）」の達成に向けた情報収集および、対応策を検討する企業が多く見られた。

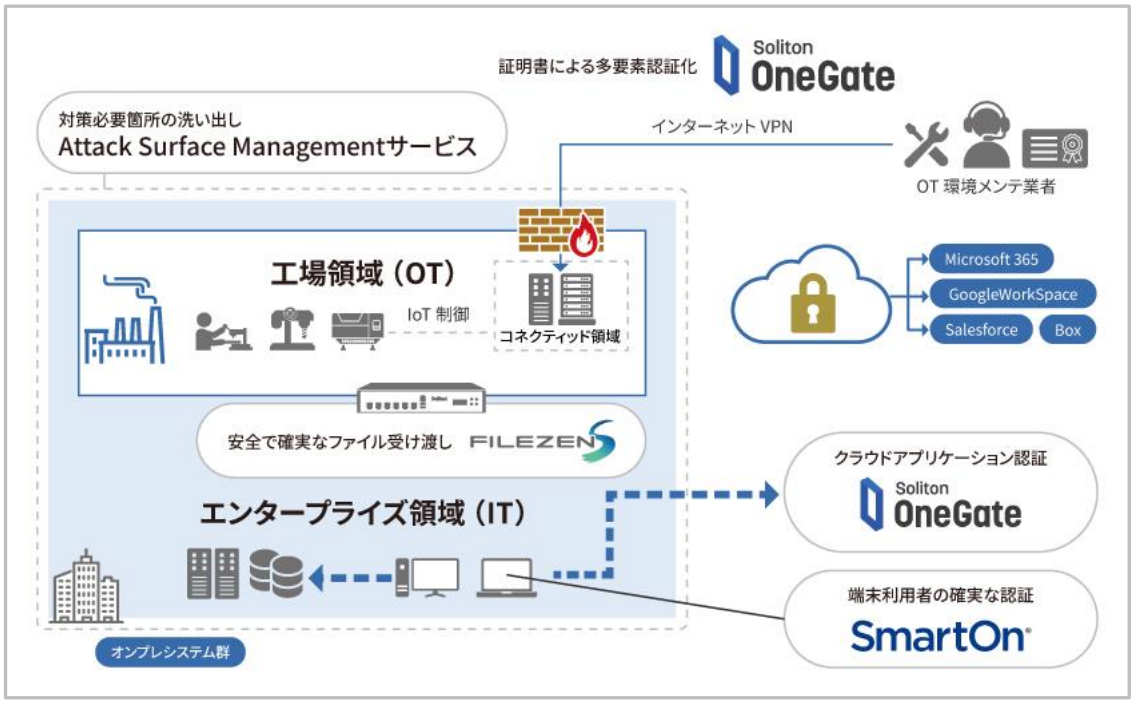
- その他、製造業全体としては、ユーザーが利用するパソコンやサーバー（エンドポイント）における不審な挙動を検知し、迅速な対応を支援する EDR（Endpoint Detection and Response）製品導入の動きがあった。

2024 年の動向予測

- 自動車産業では、「自工会 CS ガイドライン」のチェックシート LV3「自動車業界が到達点として目指すべき目標」に当たる、取引先を含めたセキュリティ教育や体制敷設、認証の強化などを実現するための取り組みが加速すると予想される。

- 2023 年後半から製造業全体で、「OT セキュリティガイド改訂 3 版《SP 800-82r3》」（NIST：米国国立標準技術研究所 2023 年 9 月公開）に対して、「対象は何か」「どこから対策が必要なのか」などの情報収集の動きが多く見られた。2024 年以降はより活発な情報収集、および具体的対策の検討が始まると想定される。製造工場および OT ネットワークのあり方が大きく変化していく中で、IT との OT の接点におけるセキュリティ意識は、さらに高まっていくと考える。

ソリトンからの提言・提案



- セキュリティ対策の検討段階では、まずどこを対策すべきかの調査・現状把握が重要となる。自社の外部公開サーバーや VPN ゲートウェイといった攻撃されやすい IT 資産の状況や、インターネット上に漏洩したユーザーID・パスワードといったクレデンシャル情報などを、専門的な手法で独自に調査・報告する「Soliton Attack Surface Management サービス」は、ファーストステップとして間違いなく推奨できるサービスだ。

- セキュリティガイドラインの要求項目として多く見られる「多要素認証」への対応には、ネットワークやクラウドサービスなどへの接続認証を多要素化する「Soliton OneGate」、または端末を使用する人物を多要素認証で確認できる「SmartOn ID」の検討をお勧めする。どちらも導入・運用負荷を抑えつつ、セキュリティ強化を実現してくれるソリュー

ションだ。

- OT セキュリティでは IT と OT をつなぐユーザーが増えているため、その接点の部分においては、分離ネットワークにおける安全な『ファイル受け渡し』と『無害化』を実現する「FileZen S」が有効だ。

- また IT と OT の環境を新たにつなぐ場合、外部からのサイバー攻撃や、内部のサイバー犯罪といった脅威に対し、個社で抜け目なく対応することは難しい。「Soliton サイバーセキュリティ・サービス」など、サイバーセキュリティ対策を幅広く支援する専門サービスの活用も検討いただきたい。

製造業まとめ

日本の製造業は現在、人手不足をはじめとするさまざまな課題を抱えているものの、IoT 活用、スマートファクトリー化など、製造業 DX の推進によってあらゆるデータを有効活用し、業務の自動化や効率化、設備最適化やエネルギーコストの削減を達成できるものとして、期待が寄せられている。
一方で、サイバー攻撃の標的になりやすく、またサプライチェーンにおいて多くの企業が関り合う業界であるため、業界全体のセキュリティレベルの底上げもまた、必須という状況にある。

ソリトンは、小規模なユーザーでも無理なく導入可能な多要素認証サービス「Soliton OneGate」をはじめ、規模を問わず実績のあるセキュリティソリューションを幅広く提供している。長らく IT セキュリティを専門にしてきた国産メーカーとして、製造業における DX や最適化を止めることなく、安全な企業活動の継続に貢献していきたい。

[2] 金融業

事業として金融(資金の融通)を行う機関、企業が属する業界。銀行(メガバンク、地方銀行、信用金庫、信託銀行)、証券会社、保険会社、クレジットカード会社、信販会社のほか、政府系金融機関や不動産金融、リース会社、アセットマネジメントなどが属する。

業種の特徴

- 監督官庁である金融庁の統制が厳格であることから、他の業種と比べセキュリティ意識は高く、FISC/金融庁演習/金融 ISAC など、業界としてのセキュリティ指針の策定および強化への取り組みも活発である。

- 金融庁は 2022 年 2 月に「金融分野におけるサイバーセキュリティ強化に向けた取組方針」の最新版を公開、3 大メガバンクをはじめとする大手銀行に対し、欧米諸国の取り組みを見習って対応することを求めている。

- 社会におけるデジタル化の加速やコロナ禍による非対面取引へのシフト、ブロックチェーンや金融 DX など事業環境変化への対応が加速する中、各地域での横のつながりや、勘定系システム共同化など、交流機会も多い。そのため、業界内での他社との情報共有も活発に行われている。

2023 年の動向

- インターネット分離、ゼロトラスト/MFA(多要素認証)、サイバーセキュリティ(ランサムウェア対策)への関心が高かった。

- インターネット分離環境については、Microsoft365 をはじめとするクラウドサービス利用を前提として、行内/行外にどのシステムをどのように配置するべきか、また位置づけをどのように考えるべきなのか、ゼロトラストセキュリティの考え方を踏まえての検討が続いた。

- また、クライアント PC について、更改時期が迫るシンクライアント/VDI を継続すべきか、機能性と利便性を優先して FAT に戻して新たなセキュリティ対策を施すか、インターネットブレイクアウトや SASE、SD-WAN 化も視野に入れながら、自社にとって最適な環境を模索中の企業も多い。

2024 年の動向予測

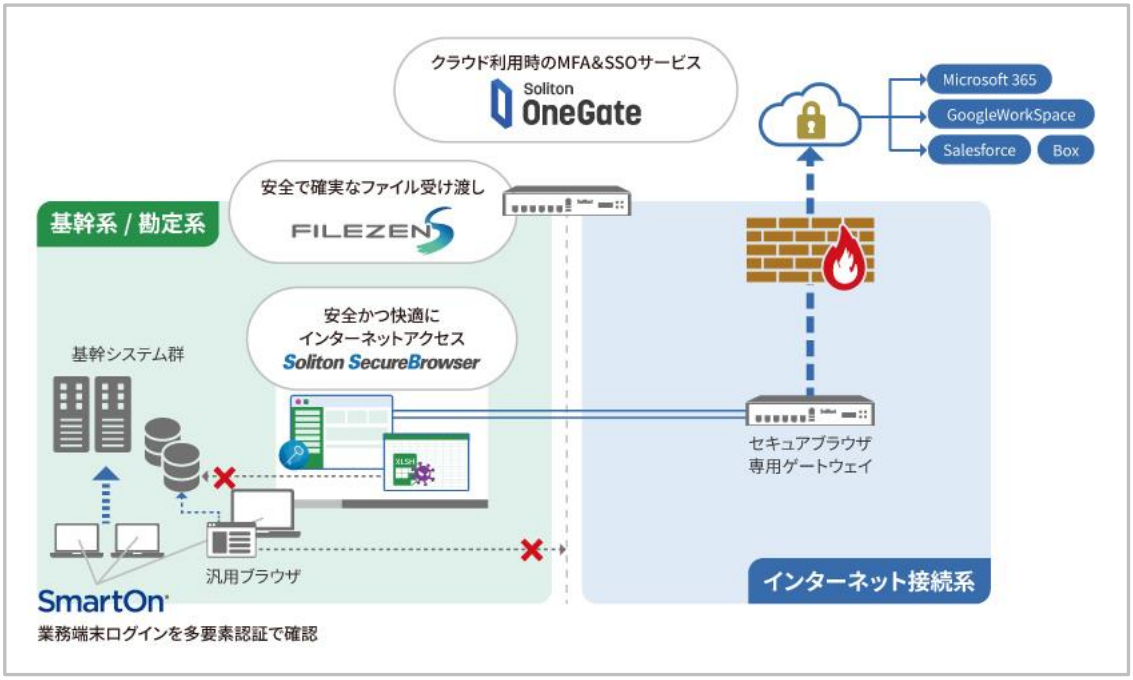
- メガバンクや大手生保の事例などを参考に、中小規模の金融企業においてもインターネット分離環境への方針、Microsoft365 をはじめとするクラウドサービスの活用や関連システムの位置付け/すみ分けが大まかに固まりつつあり、2024 年はいよいよインターネット分離環境の更改/改変、クラウドサービス利用時の MFA(多要素認証)や SSO(シ

ングルサインオン）の導入がさらに加速すると予想される。

- また、Windows10 のサポートが 2025 年 10 月に終了することから、PC 更改に向けた予算確保のための情報収集など、動きが活発化すると予想される。

- 加えてメガバンクから、不正端末接続防止を目的として、従来の無線に加えて有線についてもデジタル証明書を用いてセキュリティを強化したい要望が増加している（オフィスの在り方が変わり、有線ポートがセキュリティホールになるという懸念が増大）。そのため、2024 年はその動きが他の金融企業にも広がる可能性がある。

ソリトンからの提言・提案



- インターネット分離環境でのセキュリティ強化と利便性向上ニーズについては、低コストで安全・便利に利用できる、「Soliton SecureBrowser」と「FileZen S」の組み合わせをお勧めする。

- クラウド利用時の MFA/SSO としては「Soliton OneGate」、PC 更改で FAT 化する企業には、生体情報などを用いた強固な認証でログオンできる「SmartOn ID」をそれぞれ、お勧めする。いずれもセキュリティだけでなく導入・展開のしやすさ、運用のしやすさにもこだわったソリューションだ。なお SmartOn ID は、シンクライアント/VDI 環境におけるログオン認証強化にも対応している。

- 無線、有線の行内 LAN 不正端末接続防止には、ネットワークの安全性・安定性を大きく向上させる「NetAttest EPS」「NetAttest D3」の 2 製品が、金融業界での実績も豊富でありお勧めできる。

- クレジットカード業界の国際的セキュリティ基準 PCI DSS v4.0 における多要素認証要件については、既にカード業界大手企業でも多く採用されている「SmartOn ID」が、準拠可能。今後は、中小規模のクレジットカード会社でもニーズが高まると予想される。

金融業まとめ

他業界と比較しても、高い水準のセキュリティが求められる金融業界ではさまざまな取り組みが進められているが、多くのセンシティブなデータがあり攻撃者のターゲットで在り続ける限り、ランサムウェア攻撃等による大きな被害を受ける可能性は否定できない。

ソリトンでは、基本の考え方として「多層防御」を改めて推奨するとともに、脅威の「分離」と「認証」を軸として、各企業が実現すべき強固なセキュリティ環境の構築に貢献していきたい。

[3] 建設業

住宅をはじめ、超高層マンションやビル、空港やダムなどあらゆる建築物の建設や土木工事を担う。スーパーゼネコン、ゼネコン、中小工務店などから構成される。

業種の特徴

- DX の取り組みをはじめ、先進 IT 活用に積極的な業界。背景として日本国内の人口の約 3 割が高齢者となるいわゆる「2030 年問題」など、高齢化に伴う就労人口減少への危機感がある。『将来の担い手確保』や『働き方改革の実現』が喫緊の課題。

- いわゆる「3K（危険・汚い・きつい）」の代表職種として若い世代から敬遠される傾向にあることから、「労働環境のための新 3K（給与・休暇・希望）」を掲げるなど、業界としての魅力向上に取り組んでいる。

- 協調領域においては各社共同で技術開発を行い、業界全体で共通のシステムや AI、RPA（ロボット）を利用することで現場の生産性向上を目指す「共創」および、「建設 DX」の推進により、業務効率化と省人化およびノウハウの継承などを実現させ、高騰する原材料費や技能労働者不足、生産性の向上、働き方改革の実現といった建設業界のさまざまな課題を解決しようという機運が高まっている。

2023 年の動向

- 2024 年 4 月からスタートする「働き方改革関連法」（時間外労働時間の上限規制）による人手不足のさらなる深刻化への対応策として、各社ではクラウド利活用およびゼロトラストセキュリティへの移行が、急速に進んだ。

- また、各社は DX を冠する専門部署を設立、ICT 活用による新たなビジネススタイルの模索も多く見受けられた一方で、それと比例するように機密情報の漏えいやランサムウェアによる被害報告が目立った。

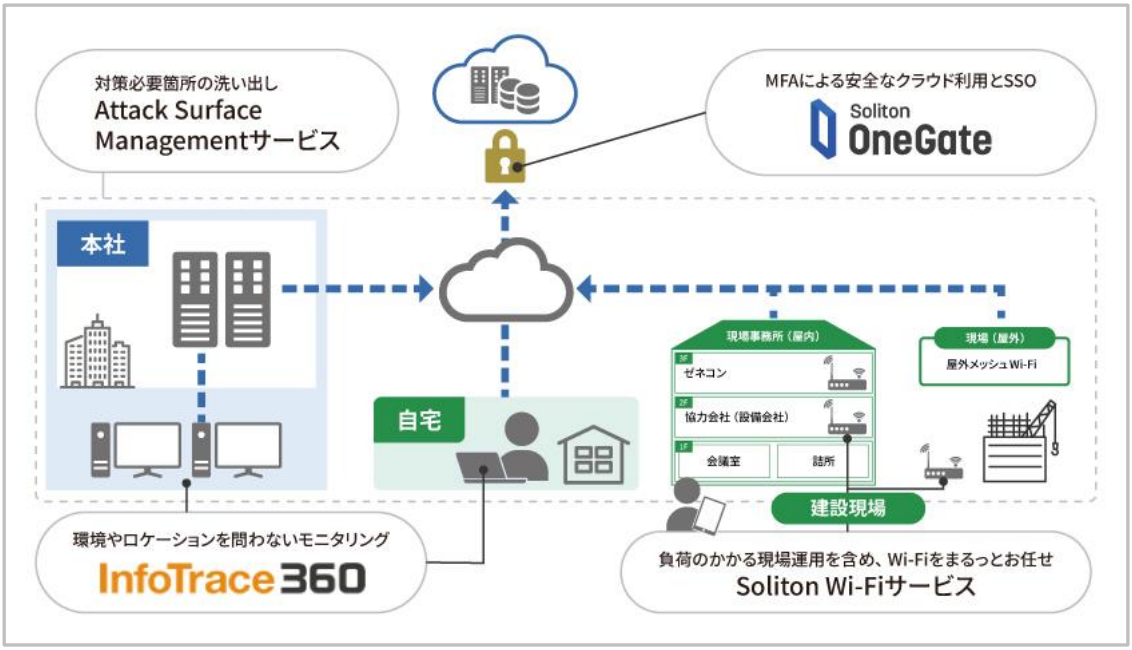
2024 年の動向予測

- クラウド環境での情報共有化が加速、同時進行でサイバー空間での活動量が増加したことで、データの損失・流出などサイバーリスクへの懸念も高まっている。

- そのため、2024 年はクラウドを中心として、適切なアクセスコントロールおよびゼロトラストなどのセキュリティ構築が、さらに進むと予測される。

- 加えて大手ゼネコンでは機器導入や資産管理、保守工数の削減を目指し、データセンターをフルクラウドに移行する動きもあり、さらなる推進が予測される。

ソリトンからの提言・提案



- 拡大するサイバー空間における脅威対策としては、まずは自社が保有する IT 資産を適切に管理し、攻撃を受けやすい箇所を洗い出し、現状のリスクを把握する必要がある。こうした現状把握や対策の検討段階では、外部公開サーバーや VPN ゲートウェイといったインターネットに直接接続された外部公開 IT 資産や、インターネット上に漏洩したユーザーID・パスワードといったクレデンシャル情報を、サイバー攻撃者がターゲット組織を調べる際に用いるものと同じ OSINT（OpenSource INTelligence）手法で調査する「Soliton Attack Surface Management サービス」を活用いただきたい。

- 実効的な攻撃対策としては、クラウド利用拡大で煩雑になるアカウント情報を一元管理し、ゼロトラストの考え方に基づいた多要素認証（MFA）を実現できるクラウドサービス「Soliton OneGate」にて、セキュリティリスクおよび管理工数を低減することが可能だ。

- さらに内部でのリスクにも対処できるよう、監視体制の強化も重要といえる。多様化する業務環境の“可視化”と“最適化”を支援する「Soliton InfoTrace360」は、ロケーションを問わないクラウド型のモニタリングサービスだ。10 ユーザーからはじめられるため、小規模や、範囲を限定した使い方にも対応できる。

- また、若手社員に任されがちな現場の無線 LAN などの運用という負担の大きい IT 業務を、ソリトンにアウトソースできる「Soliton Wi-Fi サービス」も有効だ。同サービスは回線や Wi-Fi 機器の運用のみならず、DNS セキュリティなどのセキュリティ対策もマネージドで提供する『建設現場向け』のソリューションとなっている。

建設業まとめ

安全で効率的な現場づくりを推進していくためには、IT・クラウドの有効活用と共に、セキュリティと利便性の両立が重要となる。

大手ゼネコンをはじめ建設業界でも高い導入実績を誇るソリトンは、限られた予算の中でも確実に建設業 DX が推進できるよう、安全・便利・低コストをバランスよく実現するソリューションやサービスを提供できる。業界全体の IT インフラを支えていきたい。

[4] 運輸業

食品、生活雑貨などの日常品や、大型貨物などの運搬サービスを提供。鉄道輸送、自動車輸送、バイク便などの陸運、フェリー、コンテナやタンカーなどの海運、航空機による空運に加えて、運搬に関わる工場や倉庫、物流センターなどの幅広い業務を担う業種。

業種の特徴

- 社会ニーズの変化により少量多品種の配送が求められる現代の運輸業では、配送の効率化や省人化を図るために倉庫管理や集配管理、貨物追跡などを自動化するシステムを導入する企業が増加した。一方、これらのシステムはネットワークに多くの機器を接続するため、利便性が向上する一方でサイバー攻撃を受けるリスクも高まっている。

- NISC（内閣サイバーセキュリティセンター）の「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」（2018 年 4 月）では、大手物流事業者が重要インフラ事業者に指定された。この中で「集配管理システム」「貨物追跡システム」「倉庫管理システム」が対象となる重要システムである。さらに、国土交通省「物流分野における情報セキュリティ確保に係る安全ガイドライン（第 4 版）」（2019 年 3 月改訂、以下、「安全ガイドライン」）にて、上記 3 システムの情報資産保護が明記されている。

- しかしながら目下、2024 年 4 月からトラックドライバーの時間外労働の 960 時間上限規制と改正改善基準告示が適用され、労働時間が短くなることで輸送能力不足が懸念されるいわゆる「2024 年問題」に直面する同業界は、その対応に追われている。全日本トラック協会の「トラック運送業界の働き方改革実現に向けたアクションプラン」（2018 年 3 月）では、「IT 導入補助金（サービス等生産性向上 IT 導入支援事業）」の支援対象システムの導入も明記されているものの、他業界に比べてセキュリティへの投資を含む意識は、高いとは言い難い状況にある。

2023 年の動向

- 国土交通省は、2023 年 1 月より車検証の電子化（IC タグ）をスタートした。

- Windows サーバーの更改に伴って、物流システムを刷新する動きが見られた。「集配管理システム」「貨物追跡システム」「倉庫管理システム」などの「安全ガイドライン」保護対象システムも含まれる。

- 近年、衛星通信を利用した船舶での Wi-Fi サービス提供が主流になってきており、DHCP サーバーなど、関連する機材の導入が増加傾向にある。

2024 年の動向予測

- 2023 年と同様、Windows サーバー更改を契機とした物流システムの更改あるいは新規導入が増加すると予測される。このタイミングで、「安全ガイドライン」に準拠したセキュリティ環境を模索していく可能性は非常に高い。

- 業界内において、クラウドサービスへの侵入を契機に攻撃を許した事例もあり、特にフィッシング耐性のある MFA(多要素認証)※1 の導入意識が高まると予想される。

  ※1 フィッシング耐性のある MFA(多要素認証):「FIDO 認証」、「電子証明書ベースの認証」等

ソリトンからの提言・提案

- 「安全ガイドライン」には保護対象システムの不正侵入防止策として主体認証機能(知識、生体、所有)が明記されており、それらを組み合わせた MFA(多要素認証)が推奨されている。他の業界同様、強く対応を求められるようになると考えられるため、保護対象システムの更改、導入を検討中の企業は留意して欲しい。ソリトンでは業務端末を使用する人物を多要素で認証する「SmartOn ID」、またはネットワークやアプリケーション接続時の多要素認証を実現する「Soliton OneGate」を提供している。

- さらに、同「安全ガイドライン」には「組織・体制の確立」も明記されており、CSIRT(Computer Security Incident Response Team:セキュリティインシデントが発生した際に対応するチーム)の構築も言及されている。ソリトンが提供する「CSIRT 構築ベストプラクティス」なども活用できる。

- また、将来の運輸業に影響を与え得る技術開発として、ソリトンは遠隔型自動運転システムを産業技術総合研究所、ヤマハ発動機株式会社、三菱電機株式会社と共同で研究開発を進めており、2023 年 5 月には国内初となる自動運転レベ

ル4でのドライバー無人運行サービスを開始した。経済産業省が進めるデジタルライフライン全国総合整備計画では、人流サービスとしての自動運転レベル 4 の実施を 2025 年度目標で全国 50 カ所、そして物流サービスとしての自動運転車用レーンの先行設置を 2024 年度に新東名高速道路の一部区間や茨城県日立市の一般道の一部で検討されている。今後、自動運転の社会実装が本格化していく流れに対しても、ソリトンの同技術は貢献できる。

運輸業まとめ

今後、物流分野における「情報セキュリティ確保に係る安全ガイドライン」での保護対象3システムについては、具体的な対応施策が求められていく。ソリトンは IT セキュリティのプロフェッショナルとして、効率化や省人化を諦めずにセキュリティを強化し、ガイドライン対応を実現する解決策を示したい。また、サイバーセキュリティに対する組織や体制の確立に対しても、パッケージサービスでの支援が可能である。

ソリトンは引き続き、人々の仕事や生活を支える重要なインフラのひとつである物流業界を狙ったサイバー攻撃に対し、有効なソリューションやサービスを提供することで、同業界の安心・安全なビジネスの発展に貢献していく。

[5] エネルギー業

石油・天然ガスなどの天然資源をエネルギーに変えて供給するインフラ産業。電力・石油・ガスの 3 業種を筆頭に、広義では太陽光、風力、バイオマス、地熱発電などの再生可能エネルギー、水素エネルギーなどを開発・提供する会社も含む。本稿では主に電力業界にフォーカスする。

業種の特徴

- エネルギー業界全体の課題として、地球温暖化や気候変動への対応、安定供給を担う人材の不足がある。それに加えて近年、重要インフラのひとつとしてサイバー脅威への対応が強く求められている。そのため電力業界では、将来への備えとしてのクラウド活用や IT 環境モダナイズといった取り組みに加え、サプライチェーンセキュリティの強化を推進している。

- 内閣サイバーセキュリティセンター(NISC)は 2021 年 9 月に閣議決定されたサイバーセキュリティ戦略に基づき、「重要インフラのサイバーセキュリティに係る行動計画(第 5 次行動計画)」を改訂、公表。重要物資の安定的な供給確保、サプライチェーン全体にわたる対応強化、経営層を含めたセキュリティ体制の強化などを求めている。

- 自治体や医療系と同様に、インターネット環境を普段の業務環境とネットワーク的に分離していることが多い。また電力大手では官庁などと同様に、ISMAP クラウドサービスリストに登録のクラウドサービスを優先して採用する意向がある。

- 電力会社は関連するグループ企業が非常に多いのも特徴で、従来は大規模なクローズドネットワークで業務を行ってきた。しかし、DX を積極推進する大手電力系 HD などでは、レガシーな IT 環境の刷新によるインフラコストの半減を目的に、2020 年にユーザー企業との共創によるコミュニティ型クラウド基盤を構築。削減したリソースで顧客体験価値(CX)の向上、バリューチェーン変革による価値創造を目指すなど、変化が起こり始めている。

2023 年の動向

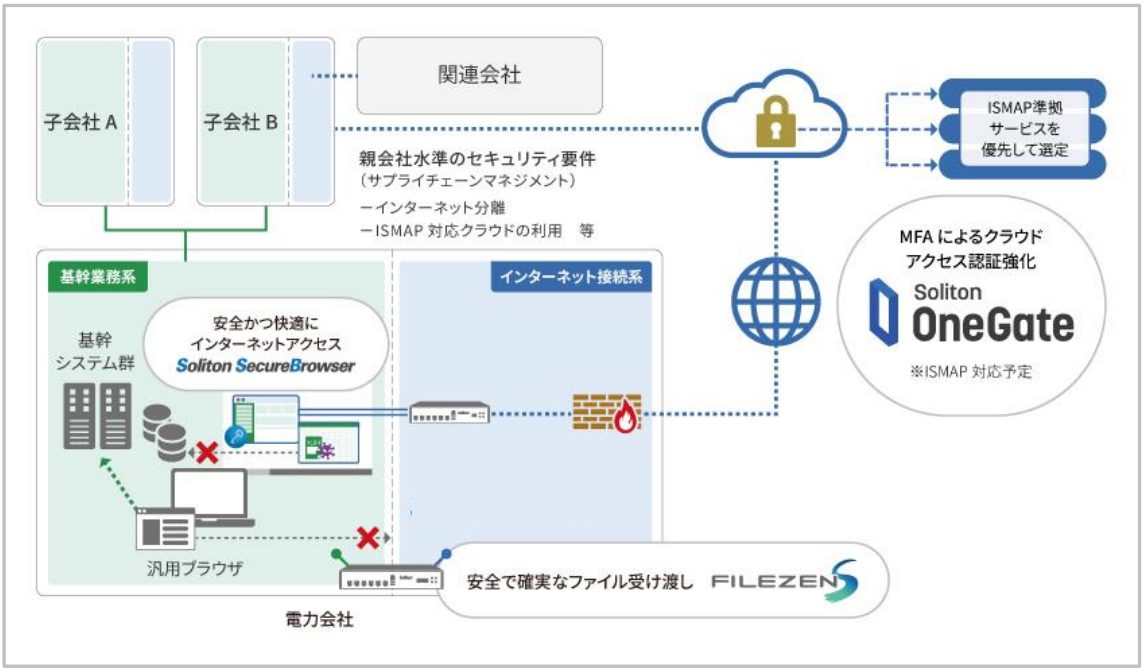
- 長らく閉域ネットワーク環境での業務が中心であったが、電力大手にて SaaS 採用条項が改編されるなど具体的な動きがあり、2023 年中盤以降、サプライチェーンを構成するグループ各社にもクラウド化の波が広がりつつある。

- 2022 年 10 月に経済産業省が公開した「自家用電気工作物のサイバーセキュリティの確保に関するガイドライン」への対応として、電力各社は電力システムを構成するサプライチェーン各社が等しくセキュリティ態勢を整えることを目指し、電気事業者、特定卸供給事業者、自家用電気工作物の設置者にそれぞれ保安規定の技術基準となるガイドラインを発行した。電力システムに関連する資産に対しては、包括的なセキュリティ要求が行われている。

2024 年の動向予測

- 2024 年も引き続き、各社でクラウドサービスの利用が広がっていくとみられる。電力大手が ISMAP 登録サービスを念頭に置いていることから、グループ各社を含め、クラウドサービスについては ISMAP 登録を気にした上で検討が進められると思われる。

ソリトンからの提言・提案



- これまで閉域ネットワーク環境下で業務してきた企業がクラウドの活用を進める上では、正しい利用者の確認が非常に重要となる。ソリトンは多要素認証を標準としたクラウド認証基盤「Soliton OneGate」を用意している。ISMAP 取得も予定しており、今後さらに導入しやすくなる。

- ネットワーク分離環境におけるセキュアなインターネット利用については、自治体・病院などでも多く採用されている安全快適な仮想ブラウザ「Soliton SecureBrowser」と、安全なファイル受け渡しと無害化を実現する「FileZen S」をお勧めする。クラウドシフトを進めるうえでも、セキュリティを担保しながらインターネット接続の利便性を高めることは重要だ。

エネルギー業まとめ

今回は電力業界にフォーカスしたが、石油/ガスなど他のエネルギー業種においても、サプライチェーンの強化および、クラウド活用やセキュリティを含む IT 環境モダナイズといったニーズが存在する。

ソリトンは国産のセキュリティ専門ベンダーとして、官庁・自治体・病院をはじめ、多くの業界で豊富な導入実績を持っている。国民の生活を支える重要インフラであるエネルギー業界全体の安全な企業活動を支えるべく、信頼できる高品質なセキュリティソリューションで貢献していきたい。

[6] サービス業(コールセンター)

コールセンターとは、電話等による顧客対応を専門とする事業者・部門を指す。自社内にコールセンター部門を設置して社員が対応するインハウス型と、専門企業に外注するアウトソース(BPO)型がある。業務としては受電問い合わせに応対するインバウンドと、架電により顧客に情報を発信するアウトバウンドを行う。近年は電話以外のメールやチャット、SNS などのコミュニケーションにも対応し、コンタクトセンターとも呼ばれる。

業種の特徴

- 通販ビジネスの拡大に加え、労働人口減少による人手不足などからアウトソーシング需要が高まり、コールセンター市場はさらなる成長が予測されている。
- コロナ禍を経て在宅での業務対応も拡大傾向にあり、システムのクラウド化も進んできている。
- 個人情報を扱うため高いセキュリティ基準が求められるが、社員ではなくアルバイトの雇用形態が多く、さらにクレーム対応などを行うため離職率が高い。人の出入りが多いという特性から情報漏えいなどのセキュリティインシデントが後を絶たず、業界としての重要課題となっている。
- クレジットカード情報を取り扱う事業者では、PCI DSS 準拠等、必要なカード情報保護対策の実施が求められる。

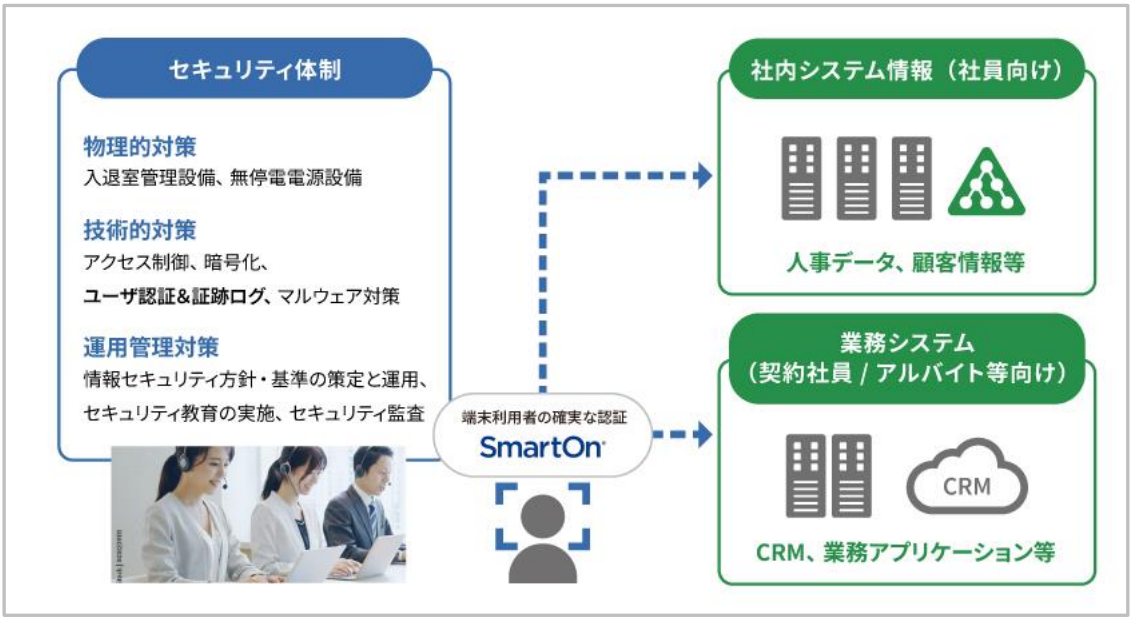
2023 年の動向

- 多くの企業では、端末操作時の個人認証として現在 IC カードを用いており、カードリーダーの調達に手間と工数がかかるため、生体認証に移行したいというニーズが高まっている。しかし、業務対応に追われ検討や移行にかけるリソースが捻出できない、端末がデスクトップ PC のため顔認証に必要なカメラがないなどの理由で、なかなか進まない現実がある。
- 2023 年 10 月に、大手コールセンター事業者で運用保守業務に従事していた派遣社員による大規模な個人情報不正持ち出しというセキュリティインシデントが発覚。業界各社では、同様の事態が発生しないための対策協議が行われた。

2024 年の動向予測

- 2025 年 10 月 14 日をもって Windows 10 のサポートが終了することを踏まえ、2024 年から PC 入れ替え需要が高まり、そのタイミングで生体認証化を推進する企業が増えることが予測される。
- また、各社のシステム更改の時期に合わせ、IT システムのクラウド化もさらに進むことが予測される。

ソリトンからの提言・提案



- 個人情報を取り扱うコンタクトセンターでは、PC 操作をする人の特定（生体認証）、アルバイトスタッフが多い中でのデータ取り扱い制御（役職に応じたデスクトップ制御）、PC 利用履歴の管理（共有 PC における認証ログ）が重要だ。ソリトンではこれらの課題に対し、「SmartOn ID」をお勧めする。SmartOn ID であれば、共有 PC における利用者情報が、Windows アカウントとは別で把握できるため、問題の特定もしやすい。

- またクラウド対応の多要素認証サービスである「Soliton OneGate」のデジタル証明書発行機能は、上述の SmartOn ID とともに、クレジットカード業界の国際的セキュリティ基準 PCI DSS v4.0 の準拠にも役立つことから、今後コンタクトセンター業界でのニーズが高まると予想される。

サービス業（コールセンター）まとめ

ソリトンは大手キャリアや公共、官公庁など、高いレベルの安全性・運用性・信頼性が求められる業界において多数の実績を残してきた。セキュリティを確保し、安心してコールセンター業務の本業に注力できるよう、支援できるソリューションが揃っている。

コールセンター業界での実績についても、ソリトンは１万人以上の規模から数百台規模まで、導入・運用ノウハウがある。PC の入口の認証だけでなく、クラウドにも利用可能な認証機能を提供することで、包括的なセキュリティ強化にも貢献していきたい。

［7］医療業

医療業界には、病院や診療所などの医療機関、製薬会社、医薬品卸、医療機器メーカーなどがある。ここでは、主に電子カルテを使用して医療行為を提供する病院を対象とする。

業種の特徴

- 他の業界に比べても、個人の病状等の記録があるため保有情報の機密性が高い。そのため、電子カルテなどの医療データを利用する HIS 系ネットワークと、インターネットが利用可能な情報系ネットワークは、基本的に分離された環境となっている。

- セキュリティが重要な業界ではあるものの、実態としては予算や人的リソースの問題を理由に、対策が不十分なケースも多い。しかしながら昨今、電子カルテシステムのダウンや、顧客データの暗号化などランサムウェア攻撃の被害が次々と明るみになったことから、セキュリティ対策に目を向ける病院が増加している。

- 国は医療機関におけるサイバーセキュリティ対策の強化を推進しており、2023 年 3 月の医療法施行規則の改正により、医療機関の管理者には必要な措置を講じることが義務化された。さらに 5 月には、安全管理ガイドラインが改訂され、医療機関等に求められる安全管理措置が最新化された。

2023 年の動向

- 厚生労働省「医療情報システムの安全管理に関するガイドライン」が 2023 年 5 月に改訂（第 6.0 版）。医療機関が利用する外部サービス経由でのサイバー攻撃を想定し、医療機関の責任において適切なリスク管理が求められた。具体的には、2027 年度時点で稼働していることが想定される医療情報を扱うシステムへの二要素認証の義務化、ランサムウェア対策の強化が追加され、二要素認証（MFA）および脅威検知ソリューションの導入検討および情報収集が活発化した。

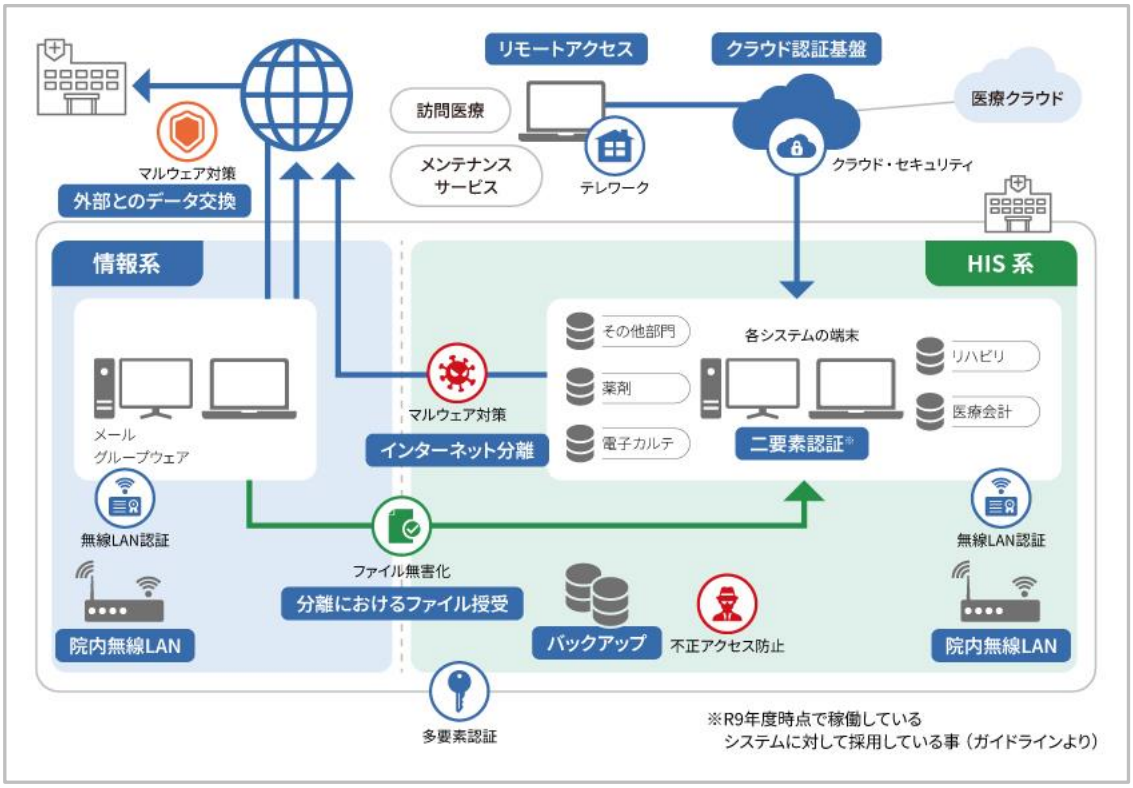
- 2024 年 4 月から医師の働き方改革の新制度が施行されることを受け、院内業務の効率化が求められている。電子カルテ端末とインターネット系端末を 1 台にまとめることで、コストを削減しつつ利便性の向上を図る等の要望が急増している。

2024 年の動向予測

- 医療業界へのランサムウェア攻撃をはじめとするサイバー攻撃の脅威は収まる気配を見せない。そのため、侵入対策・事後対策を強化する取り組みは意識高く継続すると考えられる。

- また、2024 年 4 月に施行される医師の働き方改革の本番に入ることから、電子カルテ端末とインターネット系端末を統合する動きも、2024 年中に増加すると予測される。

ソリトンからの提言・提案



- 重要なデータが多く保管されている電子カルテ端末を利用する際の二要素認証には、「SmartOn ID」の導入をお勧めする。「SmartOn ID」は、マスク着用のまま認証ができる顔認証にも対応しており、認証のたびにマスクの取り外しをする手間を省くことができる。また、すでに病院内で利用している、職員証を活用したICカード認証も職員への負荷がなく、お勧めだ。さらに、シングルサインオンの機能を活用すれば、医療業務のスピードを落とすことなくセキュリティの向上が可能だ。

- 注目度の高いランサムウェア対策のソリューションとしては、攻撃にいち早く気が付き、検知した攻撃に対してブロックを行い、その後、素早い復旧が可能な「VVAULT」があり、ランサムウェアの侵入対策・事後対策の両面から支援することができる。

- HIS 系端末でのインターネット閲覧ニーズについては、専用ブラウザアプリで安全かつ快適にインターネットへアクセスできる「Soliton SecureBrowser II」と、分離ネットワークにおける安全なファイル受け渡しを実現する「FileZen S」の組み合わせ利用が有効だ。

- ネットワークへの不正接続防止には、病院での実績も豊富な RADIUS 認証サーバーの「NetAttest EPS」、そして安定

したIPアドレスの払い出しには、DHCP アプライアンスサーバー「NetAttest D3」を活用いただきたい。

医療業まとめ

多忙かつ緊急性の高い医療現場では、医師の働き方改革の新制度が施行されることで、これまでよりもさらに利便性を損なわないセキュリティ対策が求められる。

ソリトンはセキュリティ専業ベンダーとしての高い知見と、日本全国 900 施設を超える医療機関での豊富な導入実績で得たノウハウを基に、セキュリティ強化と利便性を両立するソリューションを提供している。そして、ランサムウェア攻撃等のセキュリティ対策については、専門的な知識が必要なるためセキュリティ専業ベンダーへの相談が望ましいと考えている。我々もこれまで以上に、医療業界への貢献にまい進していきたい。

[8] 官庁・独法

1 府 11 省 3 庁(内閣府、デジタル庁、復興庁、総務省、法務省、外務省、財務省、文部科学省、厚生労働省、農林水産省、経済産業省、国土交通省、環境省、防衛省並びに国家公安委員会:警察庁)で構成される中央省庁および、その関連団体である 87 の独立行政法人・国立研究開発法人が対象。

業種の特徴

- 国家としての意思決定および公共サービスの根幹を担う団体群であり、サイバー攻撃の対象に非常になりやすい。組織として明確なセキュリティガイドラインが示されることから、同規模の民間団体と比較してもセキュリティへの意識は高い。DX についても率先して実証実験を行うなど、取り組みは比較的進んでいる。

- 官公庁のセキュリティ方針を取りまとめる内閣サイバーセキュリティセンター(NISC)がシステム・セキュリティの標準化を目指し「政府機関等のサイバーセキュリティ対策のための統一基準群」を隔年で発表。セキュリティの標準化・維持に努めている。

- 公平性の観点から基本的に入札を介した調達が行われる上、予算の取得にあたり予算の概算要求を上げて進める必要があり、期間が短い案件でも要求から導入まで約 2 年はかかってしまうという実態がある。

2023 年の動向

- 2022 年の閣議決定で中央省庁の共通システムについて、デジタル庁が提供するガバメント・ソリューション・サービス(GSS)に整備・統合し、システムおよびセキュリティの標準化を行う方針が打ち出された。しかし、検討時間の猶予がないことを理由に、GSS 基盤に移行しない団体も一定数存在した。

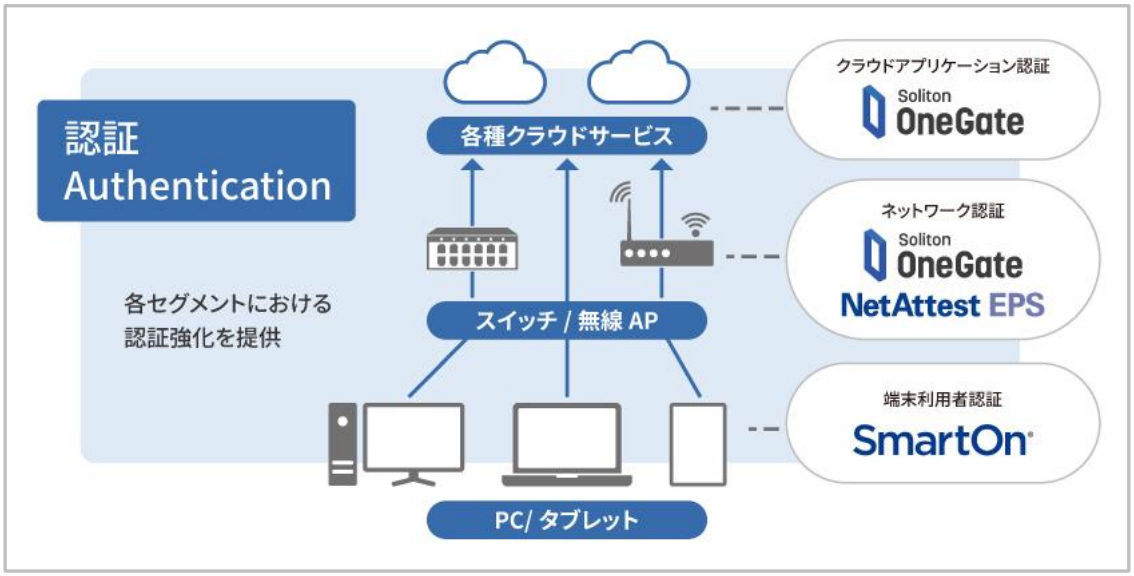
- 2022 年までは計画レベルであったクラウド移行について、2023 年から Microsoft365 をベースとして、クラウドシフトを推進する団体が増えてきている。ただし、クラウドサービスについてはデジタル庁が定める ISMAP クラウドサービスリストから採用する必要があり、選択肢が限られてしまう現状がある。

2024 年の動向予測

- 2023 年はクラウドシフトに伴いセキュリティ対策のニーズがたかかった。2024 年も同様にセキュリティ対策ニーズは高いと予測。中央省庁は GSS への統合が規程路線ではあるが、独立行政法人については GSS への統合は発表されておらず、引き続き独自調達範囲になっている。

- 具体的な課題としては、端末の二要素認証および、クラウドシフトに関する認証ニーズは引き続き高まると予測する。特に 2022 年 7 月に Microsoft より発表された「中間者攻撃の脅威(Microsoft365 利用企業に対して多要素認証を破る攻撃が行われている)」について Microsoft365 環境での多要素認証(MFA)をよりセキュアなMFAに切り替える動きが活発化すると予想される。

ソリトンからの提言・提案



- クラウドにおける標準システムとして Microsoft365 が普及している中、端末認証として Windows Hello が注目されはじめているが、特定環境で生体認証を PIN で回避できるなどのセキュリティの懸念がある。また、Microsoft365 環境での認証については、前述の通り中間者攻撃への耐性がないことが発覚しており、従来 Microsoft365 が提供していたMFAだけでのセキュリティ対応ではなくプラスアルファが必要と考える。

- ソリトンでは上記の課題について、「多要素認証」への対応として端末を認証する「SmartOn ID」、また Microsoft365 のアプリケーション認証として「Soliton OneGate」を用意しており、これからの官公庁においてベースとなるセキュリティ対応に貢献できると考えている。なお、「Soliton OneGate」については、ISMAP 登録が予定されており、官公庁のカテゴリーで認証サービスの選択肢を提示できると考えている。

官庁・独法まとめ

ISMAP クラウドサービスリストを見ても海外発のサービスが多い状況にある。サプライチェーンのリスクマネージメントが強く求められる状況の中、日本の公共サービスのセキュリティ対策ツールを国産のセキュリティメーカーであるソリトンが提供することで、貢献していきたい。

[9] 自治体

一定の地域でそこに住む人のために、法律で定めた権利を主張・行使し公共事務の処理やサービスを提供する行政機関。地方自治法に定められた、日本の都道府県や市区町村を統括する行政機関が対象。

業種の特徴

- 自治体は、行政機関のひとつとしてセキュリティとプライバシーの重要性を認識しており、また法令などに基づき住民の個人情報など多くの機微な情報を保有しているため、セキュリティ対策には他の業種以上に注視している。

- 2015 年の日本年金機構のサイバー攻撃事件を発端に、多くの自治体が『セキュリティ強靭化』施策としてネットワークを個人番号利用事務系、LGWAN 接続系、インターネット接続系に分ける「三層分離」構造を採用。しかし業務効率や利便性の低下に加え、クラウド化、オンライン手続、テレワークなど新たな時代の要請への対応が必要となり、2020 年 5 月に総務省よりガイドラインの見直しが表明された。

- また、高齢者人口の増加、生産年齢人口の減少など行政需要に大きな影響を及ぼす 2040 年問題といった人口縮減時代のパラダイムシフトに対し、政府はスマート自治体への転換を推奨している。働き方改革や 2025 年度末に運用開始が予定されているガバメントクラウドなどさまざまな動きを含みながら、自治体 DX の取り組みが模索されている。

2023 年の動向

- 各自治体が情報システムを個別に開発・運用・保守することで非効率とコスト高につながっているとの「自治体システム 1,700 個問題」を受け、2021 年 9 月に「地方公共団体情報システムの標準化に関する法律」が施行。すべての市町村は、基幹 20 業務をガバメントクラウドの標準システムに移行することとなり、現在、各自治体では情報システムのデータモデルや業務システムなどの標準化対応が、喫緊の課題とされている。

- また庁内の DX 化、AI、RPA、テレワークの活用といった業務改革のキーワードにも関心が寄せられたが、DX の定義が抽象的なため、「部署は作ったものの何から始めたらよいか分からない」という声も多く聞かれた。

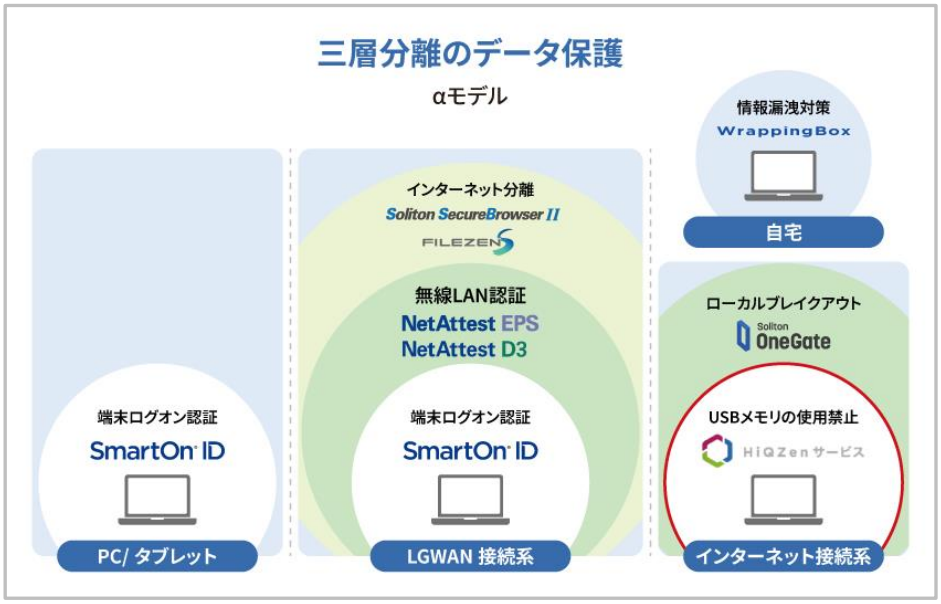
2024 年の動向予測

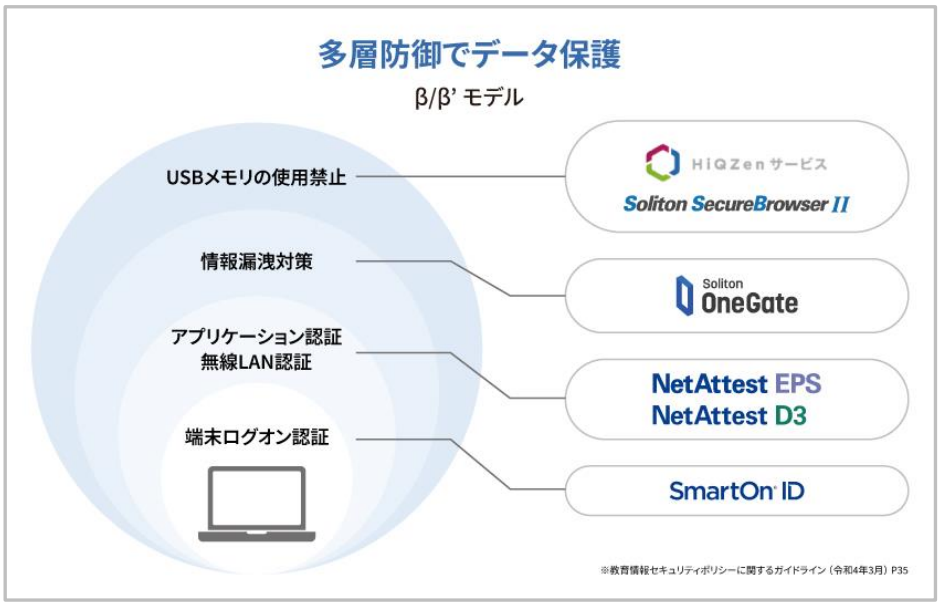
- ガバメントクラウドの運用が開始される 2025 年は、自治体にとって三層分離の見直しおよび、クラウドと向き合うこととなる転換の年。2024 年は、それに向けた準備の大詰めの年と言える。

- そのため、三層分離の見直しや自治体情報システムの標準化に向けた取り組みが、山場を迎えると予測される。

- Microsoft Office 2016/2019 Perpetual のサポート切れの期限も 2025 年に控えていることから、Microsoft365 への移行検討と共に、多要素認証(MFA)ニーズの高まりも予測される。

ソリトンからの提言・提案





- これまでインターネットと隔離した環境下で業務してきた自治体において、クラウド利用をどうしていくか、まだ政府から具体的な指針は示されていない。しかしながら、クラウド利用の波はもうそこまで迫っている。マイナンバー利用事務端末を守るために多要素認証が必須とされたように、クラウド利用においても同様に強固な認証は必須となるだろう。

- ソリトンは多要素認証を標準としたクラウド認証基盤「Soliton OneGate」を用意している。ISMAP 取得も予定してお

り、自治体においても今後さらに導入検討しやすくなる。

- LGWAN 端末からのインターネット閲覧ニーズについては、専用ブラウザアプリで安全かつ快適にインターネットへアクセスできる「Soliton SecureBrowser」と、ネットワーク分離環境における安全なファイル受け渡しと無害化を実現する「Soliton FileZen S」の組み合わせ利用が、自治体でもすでに多く採用されている。

- また、クラウドやインターネットの活用をより拡げるためのソリューションとしては、「WrappingBox」を提供している。端末内の仮想的な領域の中で、インターネットアクセスはもちろん、ファイルの編集や保存なども安全に行えるソリューションだ。セキュリティを担保しながらのクラウド利用を考える際に、ぜひ検討いただきたい。

自治体まとめ

ソリトンの提供する製品やサービスは、自治体の皆様に広くご愛顧いただいており、全国の導入率も 50%を超えるものとなっている。

変革する時代にあわせて、自治体の皆様からの課題や要望をメーカーとして受けとめつつ、今後も利便性とセキュリティ強化を両立する課題解決の仕組みを引き続き提供していきたい。

[10] 教育業

学校教育法第一条で定められた幼稚園、小学校、中学校、高等学校、中等教育学校、教育委員会が対象。

業種の特徴

- 2019 年 12 月に打ち出された GIGA スクール構想はコロナ禍で前倒しとなり、生徒へ 1 人 1 台の学習端末を展開すると共に、校内ネットワークなどの整備や授業におけるクラウド活用も進んだ。次の段階では、膨大な学習データを元にした個別最適な学びや、協動的な学びの実現に向け、スタディログの活用が課題となっている。

- 文部科学省は 2022 年 3 月に「教育情報セキュリティポリシーに関するガイドライン」を改訂。従来のネットワーク分離施策から、クラウドバイデフォルトを目指すためのアクセス制御によるセキュリティ対策への移行が示され、教員の校務端末についても境界防御型からゼロトラストセキュリティへの移行が明記されており、現在、過渡期となっている。ゼロトラストの考えに基づき、アクセス制御によるセキュリティ対策を講じたうえで、校務系・学習系ネットワークの統合を目指している。

- また、現状では職員室に固定化されている校務端末をロケーションフリーで業務できるようにすることで育児や介護などと仕事の両立を可能にするなど、教職員の働き方改革の観点でも校務 DX の必要性が高まっている。

2023 年動向

- ガイドラインで目指すべき構成とされたフルクラウド構成の実現について、多くの教育委員会は段階を経て構成を変えていく方針を定め、限られた予算の中でどのように進めるか情報収集が盛んに行われた。ゼロトラストセキュリティを意識した構成、ハイブリッド構成にするなど、考え方は教育委員会によって異なる。

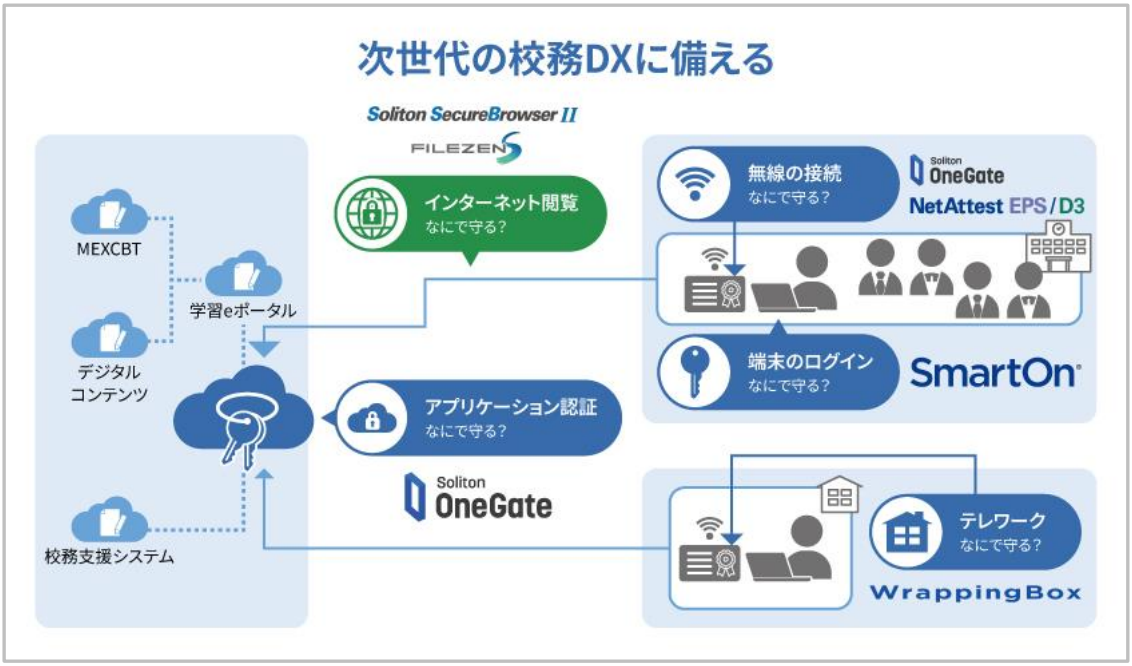
- 加えて、具体的な実行はこれからだが、これまで物理的に分けていた学習系・校務系の端末を統合し、1 台にまとめたいという要望が強まっている。

2024 年の動向予測

- 2022 年 3 月以降改訂がない文科省ガイドラインは、校務 DX 箇所を追記し、2024 年早々に改訂されると予測。ガイドラインが改訂されると、システムリプレイスに向け情報収集が活発になる傾向なため、2024 年は校務 DX 観点での校務端末の見直しに向けての動きが加速すると想定される。

- さらに、2026年にネットワーク機器のリプレイスを迎える GIGA スクール関連の情報収集や検討も活発化すると思われる。

ソリトンからの提言・提案



- 機微な情報を扱う校務端末へのログオン時には、操作している人の特定(多要素認証)、データ取り扱い制御、利用履歴の管理等が重要だ。ソリトンではこれらの課題に対し、自治体や教育委員会での実績が豊富な「SmartOn ID」の導入をお勧めする。認証の強化は、校務端末をロケーションフリーで扱えるようにするための第一歩としても重要といえる。

- クラウド利用時に求められる多要素認証(MFA)については、「Soliton OneGate」をご用意している。デジタル証明書を用いた強固な認証を手軽に展開できるだけでなく、校内に残るオンプレミスシステムへのシングルサインオン機能を備えているため、ハイブリッド環境にも対応できるのが強みだ。

- 境界防御型でのインターネット閲覧ニーズについては、専用ブラウザアプリで安全かつ快適にインターネットへアクセスできる「Soliton SecureBrowser」と、分離ネットワークにおける安全なファイル受け渡しと無害化を実現する「FileZen S」の組み合わせ利用が、教育委員会でも多く採用されている。

教育業まとめ

現在のネットワーク分離環境の不便さを解決したい、段階的にフルクラウド構成にしたいなど、教育委員会ごとにニーズは異なるものの、なりすまし対策や情報漏洩対策は、教職員のみならず子どもたちの個人情報を守るためにも欠かせない対策である。また、育児や介護と仕事との両立のため、ロケーションフリーで業務できる環境を実現することも、働き方改革の観点で重要だ。時代の流れに合わせたネットワーク構成にすることで、教職員の業務負担を減らし、柔軟かつ安全な働き方が可能となる。

その中で教育業界は予算や人的リソースの兼ね合いから、どうしてもセキュリティ対策が後回しになってしまうことも多いため、ソリトンは利便性とセキュリティ強化を両立する、誰もが使いやすいソリューションを提供することで、日本の教育分野を支えていきたい。

おわりに

今回、ソリトンシステムズの初の試みとして、同社が支援する製造、金融、建設、運輸、エネルギー、サービス、医療、官庁、自治体、教育の各業界の特徴から、セキュリティに関するこれまでの動向と将来予測、そしてそれらに対するソリトンの提言・提案を取りまとめた。

本資料が各業界でセキュリティ対策を検討中の方々にとって、なんらかの考え方や具体策のヒントになれば、幸いである。

また、こうして俯瞰して見てみることで、業界ごとの背景および直面する課題、特に喫緊の対策が求められる注力ポイントなどの「違い」が、改めて浮き彫りになったように思える。

冒頭でも申し述べた通り、各企業や組織ではいま、DX 推進、業務プロセスやビジネスモデル変革を目指し、レガシーシステムのクラウド化やマイグレーションが続いている。その中で IT システムは従来のスタンドアロン型の利用から進化し、さまざまなものと繋がり、「あらゆる場所から安全に利用できる」ことが求められるようになって来ている。さらには今後、いま話題の生成 AI やデジタルツインなどを活用した、「新たな価値を生み出す」ことも、強く求められていくだろう。

そのような状況下で、ソリトンシステムズがメーカーとして果たすべき役割は決して小さくないと考えられる。ソリトンシステムズが得意とする「認証」は、今後 IT システム同士が、オンプレミスとクラウドが、クラウドによって企業や組織同士が有機的に連携していく中で、その安心・安全を支えるための不可欠な仕組みであるためだ。

これからもソリトンシステムズは、さまざまな業界のユーザーに向けて、安全性と利便性を両立する、導入・運用・利用しやすいソリューション・サービスの開発と提供を続けていく。本資料で紹介できた内容はごく一部であるため、各商材の詳細について、また各種相談については、ぜひメール等での問い合わせをご検討いただきたい。

ネットアテスト.com運営事務局
問い合わせ先：netsales@soliton.co.jp

2024 年版

IT セキュリティトレンド概況　－注目 10 業種編－

SWP-IN2401-A

発行　2024年 1 月(第 2 版)

発行所　ネットアテスト.com 運営事務局

お問合せ先　netsales@soliton.co.jp