Software Security Across the Intelligent Edge

インテリジェントエッジソフトウェアに
求められるセキュリティとは

WNDRVR

セキュリティを左右する3つのトレンド

2025年までに、PCは20億台、IoTデバイスは420億台に達すると予測されています。

ほぼすべてのデバイスが何らかのクラウド経由で稼働するようになり、生成・利用するデータや日常生活を取り巻くデータの80%が、5Gクラウドを介して処理されるようになるでしょう。しかし現在、デジタルトランスフォーメーションに成功している企業は、全体のわずか11.5%に過ぎません[1]。つまり大半の組織は、来たるデジタル世界の成功に向けてクリアすべき難題を抱えています。

その中でもセキュリティは、最も重要な課題です。進化を続けるデジタル環境におけるセキュリティプロトコルの設計が、いかに複雑か想像してください。先進テクノロジー企業の半数以上が、デジタルトランスフォーメーションへの取り組みに直結するセキュリティの懸案事項を複数挙げています。その一例が、サイバーセキュリティリスクの増大（53%）、サイバー犯罪の巧妙化（56%）、攻撃対象領域の拡大（53%）です。CISO、CTO、CIOの40%が、こうしたセキュリティ脅威に加えて、組込みシステムと深く関連した柔軟性に欠けるインフラに起因する問題を懸念しています[2]。

40%

CISO、CTO、CIOの40%が、こうしたセキュリティ脅威に加えて、組込みシステムと深く関連した柔軟性に欠けるインフラに起因する問題を懸念しています。

今日の環境において絶えず変化する3つのトレンドを、次ページで詳しくご紹介します。

EMERSON
Network Power

Emersonは、分散制御システム「Ovation」の安全性と接続性をいかにして両立できたのでしょうか？

機械学習、フルシステムシミュレーション、そしてウインドリバーソリューションを活用し、この課題の解決を実現しています。

発電所の信頼性向上を支える同社のOvation™（分散制御システム）は、最新技術と共に進化するプラットフォームです。また、アメリカ国土安全保障省（DHS）により、米国安全法で定めるテロ対策技術として認定されています。

同社では、ウインドリバーのソリューションを活用してOvationのライフサイクル全体を管理しています。迅速な開発を支援する仮想ハードウェア、Ovationの動作基盤となるVxWorks®、プラントの実環境全体のシミュレーション機能、さらに運用面でのセキュリティに欠かせない制御システム操作のモデリング機能などを使って、システムのパラメータやパフォーマンスのベースラインを設定できるため、異常な挙動が本番システムに影響を及ぼす前に検知できます。

1 Forbes/Inc.Digital
2 media.nominet.uk/wp-content/uploads/2019/07/Cyber-Security-in-the-Age-of-Digital-Transformation.pdf

トレンドその1

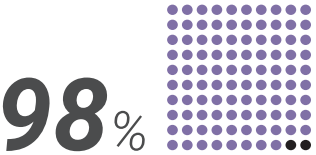
データの価値がより動的に。これまで、データ取得のチャンスはデバイスのライフサイクル全体の0.1%だったが、今はそれ以上の潜在性を秘める

デバイスを単体で考えるという設計手法は衰退していくでしょう。デジタル中心の時代では、情報の価値がこれまでよりはるかに動的に変化します。大手企業トップの75%が「これまでの倍以上のスピードでの経営判断が求められる」と述べています[3]。つまり意思決定の材料としてのデータを即入手できなければなりません。

今や何千〜何百万にのぼる様々な場所から、時には一斉に収集されるデータの特性は、かつてないほど動的になっています。何に利用できるかは、取得するタイミング（重要な一瞬）にかかっています。旧来の設計どおりに開発したデバイスであれば、そのタイミングはライフサイクル全体の0.1%に過ぎないかもしれません[4]。しかし、データが動的に変化する現代、残りの期間（99.9%）で収集した情報が、データインフラの別の要素にとって貴重なものになることもあります。様々なモノがつながる世界において、データは本来の設計で意図された以上の多面的な価値をもちます。

IoTデバイス全体の半分以上が、重大な攻撃（重篤度：中〜高）に対して脆弱です。また、医療機器を含むIoTデバイス通信の98%が暗号化されていません[5]。このように、デバイス上のデータを保護することは大変困難なため、現在進行中の「データ革命」がますます重要になります。動的な特性をもつデータは、不用意に個人識別情報（PII）に変換される恐れがあり、世界各国のさまざまな規制の対象となるため、特定のクラスのデータは、プライバシー保護の観点から慎重に取り扱う必要があります[6]。

> データにはネットワーク効果があります。リアルタイム接続するデバイスの数が増えるほど、組織にとっての情報やデータの価値も大きくなります



医療機器を含むIoTデバイス通信の98%が暗号化されていません。

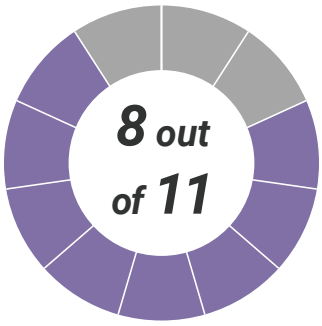
3 Forbes/Inc.Digital
4 The Digital Helix
5 threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609
6 www.varonis.com/blog/data-privacy

トレンドその2

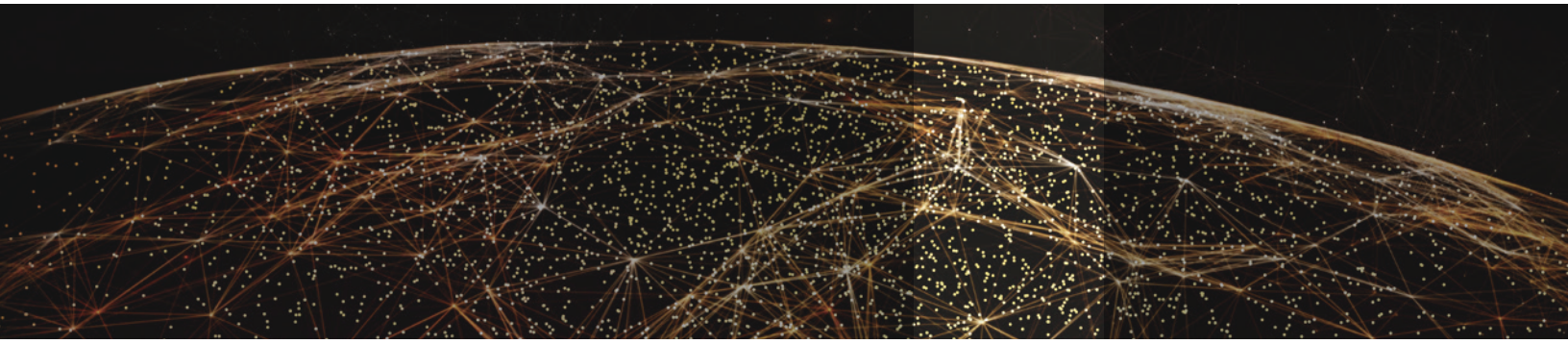
セキュリティは（組織の内外を問わず）パートナーシップの垣根を越えて機能しなければならない

送電網全体の複雑な電力供給を管理する産業機械に内蔵されたコンポーネントを想像してみてください。このデバイスは、エコシステムパートナー10社の製品とともに、統合環境の一部となって動作しているかもしれません。その場合、コンポーネントの動作状況だけでなく、リアルタイムで利用できる付加価値情報がデータエコシステム全体からどのように生成されるのかについても理解しなければなりません。また、そのデータを今後どのように活用していくかについて検討する必要もあります。デバイスが本来の機能以上の力を発揮する様々な業種（エネルギー、流通、医療機器製造、航空・防衛などの分野）で、こうしたナレッジを活用する機会が生まれています。

データにはネットワーク効果があります。リアルタイム接続するデバイスの数が増えるほど、組織にとっての情報やデータの価値も大きくなります。デジタルトランスフォーメーション戦略に関するForbes Inc.Digitalの調査では、業界の大手企業11社のうち8社が、デジタルトランスフォーメーションが進む世界では、データの力が将来の成功を決定づける」と確信しています。エコシステムに関与するパートナー企業の数が増えるほど、データの潜在力も大きくなります。抽象的に聞こえるかもしれませんが、IBMのコグニティブ・コンピューティングシステムグループが最近行った調査によると、AIの機能は、4種類の形態（機械学習、深層学習、視覚認識、自然言語処理）すべてを同時に実行することで（つまり複数のデータセットがリアルタイムで連動することで）、最大の経済性および効果を発揮できるとされています。すべてのものにAIが組み込まれつつある現在、データ連携の力は、単独のエコシステムが提供できる価値よりもはるかに大きな価値をもたらします。



業界の大手企業11社のうち8社が、「デジタルトランスフォーメーションが進む世界では、データの力が将来の成功を決定づける」と確信しています。



トレンドその3

「デジタルトランスフォーメーションがもたらす未来」の定義は曖昧。不透明な時代に対応できるセキュリティ態勢をが求められる

曖昧性は、デジタル時代の代名詞です。デジタルトランスフォーメーションが困難であるのと同様、セキュリティの設計や実現方法を変革することも困難です。しかし、デジタルトランスフォーメーションに成功している大手企業（Fortune Global 2000掲載企業）は、こうした時代を舵取りできる環境が整っているため、将来に対する自信が同業他社よりはるかに高くなっています。

変動性、不確実性、複雑性、曖昧性の時代（通称VUCA時代）では、セキュリティを新たな視点で捉える必要があります。デジタルトランスフォーメーションの実質的な伸び率は2013年以降鈍化しているため（年間平均11.5%）[7]、この現実を受け入れて対処しなければなりません。我々が設計すべき未来は、データを保護しつつ、そのデータから得られたインサイトをリアルタイムで活用し、最終的に複数のエコシステムで共有可能な未来です。

デジタル化が浸透する前は、セキュリティの概念はわかりやすいものでした。しかし今は、セキュリティに組込むべき要素にもAIやクラウド、5G技術のように日々変化する適応性が求められます。開発者やアプリケーション管理者の使命は、適応性を前提とした時代に向けたインテリジェントエッジデバイスを設計することです。

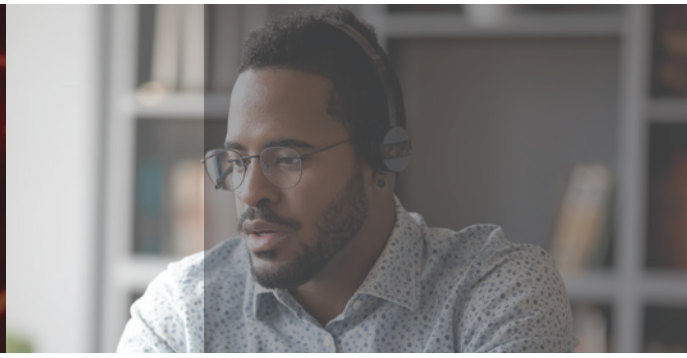
> 「シミュレーションモデル（VxWorksシミュレータ）をそれと等価な組込みハードウェアと併用することで、絶対基準としての役割をもたせることができ、システム障害を引き起こす前に異常動作を検出することができる可能性があります」
>
> **ーRick Kephart氏**
> Emerson
> ソフトウェア開発担当
> バイスプレジデント

デジタル時代への対応準備はできていますか？ 3項目の簡単なチェックリストで現状をご確認ください。

1. デバイス設計の際、新たなセキュリティ要件を順次取り入れていますか？
2. 我々を取り巻く不透明なVUCA時代は、貴社にとって有益な機会だとお考えですか？また、貴社にとって「セキュリティ要件の順守」は成功の阻害要因ですか、または成長を加速する要因ですか？
3. デジタルトランスフォーメーションに伴い、貴社における5年後のセキュリティ基本戦略はこれまでと大きく変わるだろう、とお考えですか？

7 Inc.Digital

エッジの未来



私たちは今、2つの大きな変化に直面しています。ひとつは、エッジコンピューティングへの大規模な移行。とりわけ、エンタープライズデータの収集、処理、保存において。もうひとつは、未来のミッションクリティカルなインテリジェントシステムを開発・運用する人材の世代交代という変化。

2018年時点では、従来のデータセンター以外で収集・処理されたエンタープライズデータは全体のわずか10%でしたが、2025年にはこの比率が75%を超える見込みです[8]。また2020年には、世代別労働人口では、ミレニアル世代が最大の割合を占めるようになりました[9]。

経験の重要性

組込み開発のレガシーシステムに精通した開発者や運用担当者の世代は定年に近づいていますが、現行技術のスキルをもつ後継者はごくわずかしかいません。企業幹部の82%が「優秀なエンジニア不足」を問題視しており、企業の60%が「電気・電子系エンジニアの補充が最も困難だ」と考えています[10]。IoTシステムのセキュリティを維持するには、IoT技術の経験値が不可欠です。CVE（脆弱性情報）データベースによると、脆弱性を引き起こす最大の要因が「プログラミングエラー」となっています。「攻撃の影響が一番出やすいのがOSやファームウェアです。これらの領域でソフトウェアのプログラミングエラーやアクセス制御／認証チェックの不備があると、ソフトウェアベース基盤の最下層が攻撃にさらされてしまいます。表面化しない脆弱性もまた、これらのソフトウェア（OSやFirmware）に攻撃リスクを生じさせます[11]」という趣旨の論文もあります。

TOSHIBA

今後5年間、サイバー犯罪による企業の被害総額が5.2兆ドルと言われる市場で、TOSHIBAは個人データをどのように保護しているのでしょうか？　同社の取り組みをご紹介します。

2019年に発生したセキュリティ侵害の60%が「パッチ未適用」の脆弱性によるものでした。同社は、Wind River Linuxを活用し、この問題を克服しました。

2019年に公開されたCVEの件数は、1日あたり45件以上でした。電機・ITの総合大手であるTOSHIBAは、社内で管理する個人データへのCVEリスクを重く受け止め、ウインドリバーとのパートナーシップによりデータ保護およびコスト低減を図っています。ウインドリバーのセキュリティ担当チームは、VxWorksおよびWind River Linuxのカーネル機能やユーザーパッケージ、ツールに影響が出ないよう、CVEデータベースを常時監視しています。さらに、NISTやUS-CERTをはじめとする米国政府機関や当局が公布する通達のほか、公的／民間団体が配信するセキュリティアラートメールもチェックしています。

8 www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders
9 Forbes/Inc.Digital
10 www.semi.org/en/node/581
11 www.cse.psu.edu/~pdm12/cse597g-f15/readings/cse597g-embedded_systems.pdf

アクセス制御がすべての基本

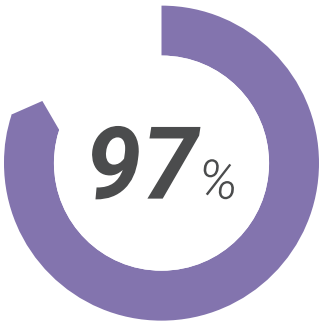
IoT接続機器を含むエッジデバイスは通常、外部から物理的にアクセス可能なため、制御された環境と異なり、様々なハードウェア攻撃にさらされています。こうしたシステムが市販され、サイバー犯罪者の手に渡ると攻撃手段の開発に悪用されてしまいます。これらのデバイスは、小型で、個人所有され、セキュリティが甘く、定期的な更新もされず、接続された広範なネットワークに容易にアクセスすることができます。Ponemon Instituteが2018年に実施した調査では、リスク管理専門家の97%が「安全でないIoTデバイスが、壊滅的なセキュリティ侵害の一因となる恐れがある」と回答しています[12]。

エッジコンピューティング実現の過程で確認すべき3項目

1. 今日のIoTデバイスおよび関連システムの開発、デプロイ、保守に必要な幅広いスキルを有する技術者を確保（採用・育成）できる状況ですか？
2. ミレニアル世代やデジタルネイティブ世代の人材が操作しやすいデバイスを実現するための「デジタルエクスペリエンス戦略」を整備していますか？
3. 自社製デバイスを取り巻くサプライチェーン（ソフトウェアの段階から市販後サポートのベンダーまで）の全体像を理解していますか？

「潜在的なセキュリティリスクの情報は、日々更新されます。当社では、ウインドリバーとのパートナーシップによるセキュリティ専門チームが活躍しており、既知のリスクを徹底監視すると共に、顧客である小売業界のための迅速な対応に取り組んでいます」

—Gregg Margosian氏
東芝グローバルコマース
ソリューションズCOO



リスク管理専門家の97%が「安全でないIoTデバイスが、壊滅的なセキュリティ侵害の一因となる恐れがある」と回答しています。

12 sharedassessments.org/wp-content/uploads/2018/04/2018-IoTThirdPartyRiskReport-Final-04APR18.pdf

セキュリティポリシーの定義

設計担当チームの49%が「セキュリティポリシーの定義は、最も重要なプロジェクトのひとつだ」と考えています。

デバイスを、不正アクセス、不正利用、漏洩、運用妨害、改ざん、破壊から保護するための原則を定義した「CIAトライアド」は、セキュリティポリシー作成の指針となる業界標準モデルです。

CIAトライアドは、以下の3原則がベースとなっています。

- **Confidentiality（機密性）：**IoTシステムの個人データを保護するセキュリティ。保護対象は、通信中のデータ、デバイス静止時の保存データ、デバイスが処理中のデータ、デバイス間で送受信されているデータなどです。
- **Integrity（完全性）：**デバイスのデータが攻撃者によって改ざん／削除されていないことを徹底するためのセキュリティ。組込みデバイスが生成／使用するデータだけでなく、プログラミングデータ（OS、アプリケーション、設定用のデータなど）などが対象となります。
- **Availability（可用性）：**本来の想定どおりの機能をIoTデバイスに実行させるためのセキュリティ。攻撃者にデバイスの使途を改ざんされないよう保護します。生命にかかわる、またはミッションクリティカルなタスクを遂行するデバイスにとって、大変重要なセキュリティ機能です。

プロジェクトチームは、リスクレベル、規制要件、IP保護の必要性に基づき、コスト、パフォーマンス、デバイスのデプロイ／運用環境とのバランスを考慮して、CIAトライアドのどの要素が必要かを判断します。あらゆる攻撃を想定してデバイスやシステムを保護できる特効薬のソリューションはありません。単一ソリューションではなく、複数のリスク緩和策を組み合わせた階層型アプローチのほうが多面的な防御機能を提供できるため、圧倒的に強固なサイバーセキュリティを実現できます。

あらゆる攻撃を想定してデバイスやシステムを保護できる特効薬のソリューションはありません。単一ソリューションではなく、複数のリスク緩和策を組み合わせた階層型アプローチのほうが多面的な防御機能を提供できるため、圧倒的に強固なサイバーセキュリティを実現できます。

エッジコンピューティング実現の過程で確認すべき項目

変革の方向性は正しいですか？あるいは、知らないうちに攻撃対象領域が拡大していませんか？

デジタルトランスフォーメーション推進にあたり、確認すべき5項目

組込みシステム業界やオペレーショナルテクノロジー（OT）のデジタル化がますます進み、デバイスのライフサイクルに関する既成概念（固定機能／壊れたら修理）が通用しなくなった今、次世代ミッションクリティカルシステムのセキュリティ設計、デプロイ、オーケストレーション、適応の面でもこれまでとは全く異なる戦略が必要になります。

1. 貴社のセキュリティ戦略は、主にエンドポイントを対象としたものですか？または、クラウドを取り巻く真のシステムレベルのアプローチで、デジタルトランスフォーメーションの中核となるデータの証拠保全を提供できますか？
2. IoTシステムの機能とセキュリティ要素を並行開発するための手法は確立していますか？その場合、デジタルトランスフォーメーションに伴って広がり続けるセキュリティ脅威に対応できる手法になっていますか？
3. 貴社のシステムアーキテクチャは、デプロイされたエッジデバイスの効率的な管理と更新をサポートすると共に、次世代のセキュリティ脅威を予測し、現場で何十年にもわたってセキュリティを確保するために必要な柔軟性を提供できる設計になっていますか？
4. お使いのセキュリティツールは、貴社のIoTシステムに適用される様々な業界固有プロトコルを認識可能ですか？そうでない場合、デジタルトランスフォーメーションによって企業のシスムとエッジの融合が加速する中、これらのプロトコルを介した侵入をどのように検知しますか？
5. 貴社のセキュリティペリメータ（境界）の範囲には、現場で稼働中のデバイスも含まれていますか？そうでない場合、デプロイ済デバイスとエンタープライズシステムとの安全な接続をどのように確保する予定ですか？

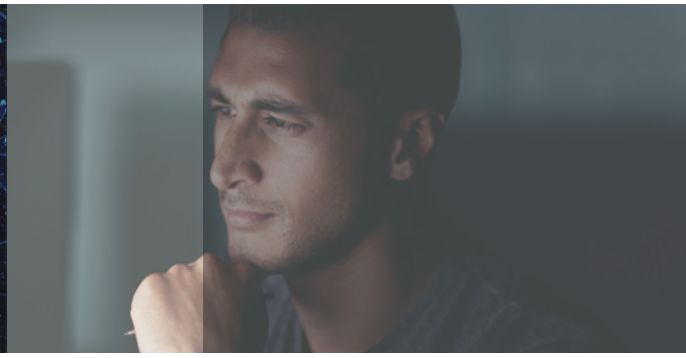
貴社のデータは安全に保護されていますか？

データ中心のデバイス開発およびデプロイにおいて考慮すべきセキュリティ3項目

デバイスメーカーは、デジタル時代の新たなパラダイムである「相互接続性」および「データのダイナミズム」を反映したセキュリティを設計する必要があります。その際、メモリやストレージにあるデータだけでなく、システム間やネットワークを経由して送受信されるデータ、さらにはデータ暗号化に用いるキーについても考慮しなければなりません。一方、改ざんによってデータの完全性が損なわれないよう、ソフト／ハードを堅牢化することも必要です。貴社は、データセキュリティおよびプライバシー保護における包括的なアプローチを整備していますか？あるいは、エンドポイントセキュリティだけに特化した開発を続けていますか？

1. 開発対象のシステムでは、平文形式のデータ送受信（IoTデバイス全体の98%がこちら）、暗号化によるデータ送受信のどちらを想定していますか？
2. システムがデプロイされる環境について、当該環境で想定される攻撃リスクやプライバシー保護対策の要否について、明確に理解していますか？
3. データセキュリティに関する様々な脅威をすべて網羅できるテスト戦略が整備されていますか？

ウインドリバーが選ばれる理由



ウインドリバーは40年近くにわたり、世界の主要なテクノロジー企業が、世界で最も安全なデバイスを何世代にわたって提供できるように支援してきました。

自律性とコネクティビティが主流になる新時代においても、ウインドリバーはテクノロジーリーダーとしての歩みを止めません。当社のソフトウェアは、必要不可欠なモダンインフラ上で稼働する航空システム、鉄道システム、車載システム、医療機器、製造業の工場、通信ネットワークなど、「止まることが許されない」ミッションクリティカルなコンピューティングシステムの運用を支えています。

ウインドリバーの技術は、世界各地で20億台以上のデバイスに採用されています。業界をリードするプロフェッショナルサービス、受賞歴を誇るカスタマーサポート、強力なパートナーエコシステムが、ウインドリバーの技術を支えています。

お客様は、プライバシーの保護、データの完全性の維持、シームレスなシステム統合と開発者のコラボレーションによる可用性の確保を実現する、最先端の堅牢で信頼性の高いソフトウェアプラットフォームを利用することができます。セキュリティに配慮したイノベーションを推進し、現在および未来の脅威からデバイスを保護するための「信頼の基盤」として当社プラットフォームをお役立てください。

ウインドリバーのプラットフォームは、デフォルトで安全な設計（secure-by-default）にもとづく基盤としての実績があり、業界における豊富なノウハウも反映されているため、セキュリティの問題を心配することなく、最新技術を取り入れたデバイスを構築していただけます。個人データの保護、クリティカルシステムの隔離、安全な形でエコシステムに統合されたシステム管理を実現する当社プラットフォームを活用することで、リスクを抑えて反復開発作業を迅速化し、ライフサイクル全体で安心安全な形で製品をデプロイしていただけます。

セキュリティに配慮したイノベーションを推進し、現在および未来の脅威からデバイスを保護するための「信頼の基盤」として当社プラットフォームをお役立てください。

ウインドリバーは、インテリジェントエッジ向けソフトウェアを提供する世界的なリーディングカンパニーです。そのテクノロジーは1981年の設立時より世界で最も安全かつセキュアなデバイスに搭載され、数十億台を超える製品に使用されています。ウインドリバーのソフトウェアと専門性は、最高水準のセキュリティ、安全性、信頼性を提供し、より優れたコンピューティングとAI機能が要求されるミッションクリティカルなインテリジェントシステムのデジタルトランスフォーメーションを加速しています。

Appendix（付録）

デジタル時代に即したセキュリティのチェックシート

来るべきデジタルの未来、およびVUCA（変動性、不確実性、複雑性、曖昧性の）時代に適したセキュリティ態勢は整っていますか？

1. デバイス設計の際、新たなセキュリティ要件を順次取り入れるようにしていますか？
2. 我々を取り巻く不透明なVUCA時代は、貴社にとって有益な機会だとお考えですか？また、貴社にとって「セキュリティ要件の順守」は成功の阻害要因ですか、または成長を加速する要因ですか？
3. デジタルトランスフォーメーション進展に伴い、貴社における5年後のセキュリティ基本戦略はこれまでと大きく変わるだろう、とお考えですか？

変革の方向性は正しいですか？あるいは、知らないうちに攻撃対象領域が拡大していませんか？

1. 貴社のセキュリティ戦略は、主にエンドポイントを対象としたものですか？または、クラウドを取り巻く真のシステムレベルのアプローチで、デジタルトランスフォーメーションの中核となるデータの証拠保全を提供できますか？
2. IoTシステムの機能とセキュリティ要素を並行開発するための手法は確立していますか？その場合、デジタルトランスフォーメーションに伴って広がり続けるセキュリティ脅威に対応できる手法になっていますか？
3. 貴社のシステムアーキテクチャは、デプロイされたエッジデバイスの効率的な管理と更新をサポートすると共に、次世代のセキュリティ脅威を予測し、現場で何十年にもわたってセキュリティを確保するために必要な柔軟性を提供できる設計になっていますか？
4. お使いのセキュリティツールは、貴社製IoTシステムに適用される様々な業界固有プロトコルを認識可能ですか？そうでない場合、デジタルトランスフォーメーションによって企業のシステムとエッジの融合が加速する中、これらのプロトコルを介した侵入をどのように検知しますか？
5. 貴社のセキュリティペリメータ（境界）の範囲には、現場で稼働中のデバイスも含まれていますか？そうでない場合、デプロイ済デバイスとエンタープライズシステムとの安全な接続をどのように確保する予定ですか？

貴社のデータは安全に保護されていますか？

1. 開発対象のシステムでは、平文形式のデータ送受信（IoTデバイス全体の98%がこちら）、暗号化によるデータ送受信のどちらを想定していますか？
2. システムがデプロイされる環境について、当該環境で想定される攻撃リスクやプライバシー保護対策の要否について、明確に理解していますか？
3. データセキュリティに関する様々な脅威をすべて網羅できるテスト戦略が整備されていますか？

エッジコンピューティングで成功するために必要な知識は備わっていますか？

1. 今日のIoTデバイスおよび関連システムの開発、デプロイ、保守に必要な幅広いスキルを有する技術者を確保（採用・育成）できる状況ですか？
2. ミレニアル世代やデジタルネイティブ世代の人材が操作しやすいデバイスを実現するための「デジタルエクスペリエンス戦略」を整備していますか？
3. 自社製デバイスを取り巻くサプライチェーン（ソフトウェアの段階から市販後サポートのベンダーまで）の全体像を理解していますか？