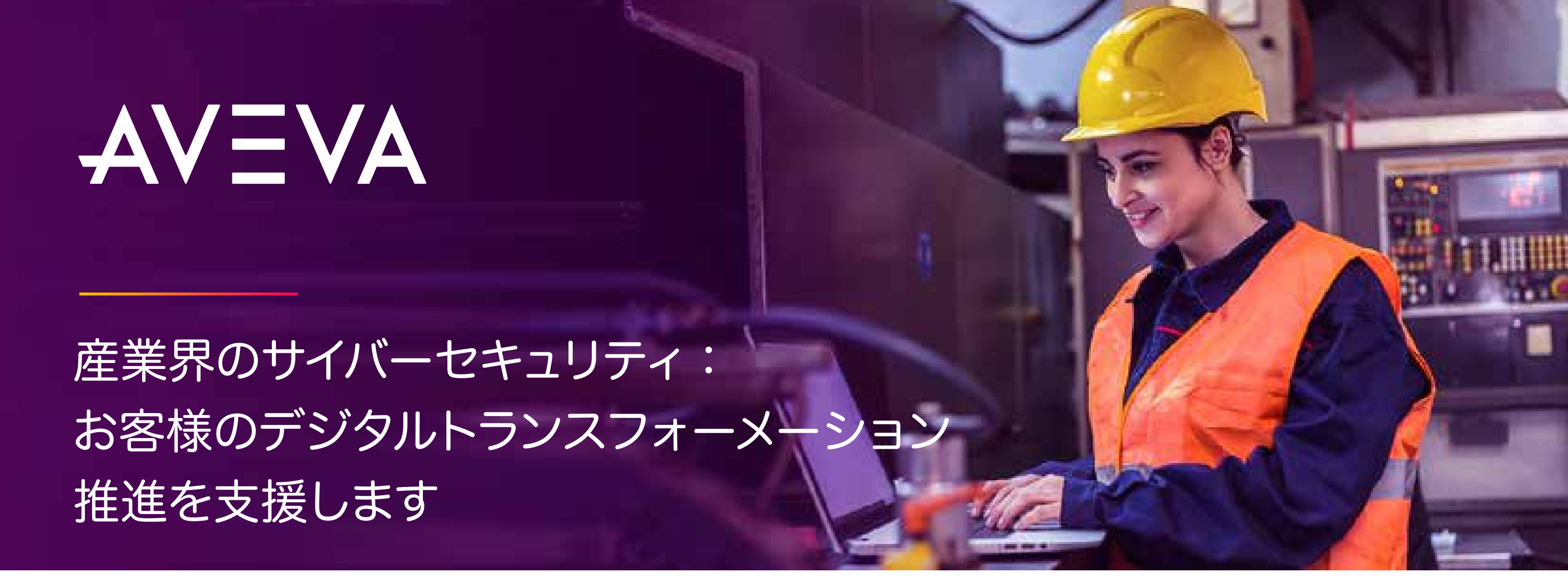

AVEVA

産業界のサイバーセキュリティ：お客様のデジタルトランスフォーメーション推進を支援します

今後の見通しが極めて難しい状況ではあるもののデジタルトランスフォーメーション推進には絶好の機会です。
リモートワークやチームでの共同作業のニーズを背景に、クラウド、エッジ、および IIoT は、
企業業績を拡大する新たな方法となるだけではなく、ビジネスプロセスの改善にもつながります。
また、サイバーセキュリティは、安全性とともに、この変革期において重要な鍵です。

数値で見るサイバーセキュリティ

2,100%以上	過去3年間の産業界におけるサイバー攻撃の増加率
5,200件	IoTデバイスに対する1カ月あたりの平均攻撃件数
279日	データ漏洩を特定し、封じ込めるまでの平均日数
392万ドル	1回のサイバー攻撃による典型的な財務上の損失 出典：IBM Security
1,337億ドル	2022年までにサイバーセキュリティに費やされる予想金額 出典：Gartner

テクノロジーの急速な進展に伴い、サイバーセキュリティのリスクも高まってきました。しかし、多くの専門家は、産業用システムの保護は不十分であると指摘しています。まだ漏洩がビジネスに及ぼすリスクや影響が軽視されるケースが多いためです。

サイバーセキュリティについては組織全体が事前に対応する姿勢で取り組む必要があります。さらにリスク軽減と新しいビジネスの間でバランスを取ることも必要です。これには従業員へのトレーニングだけでなく、適切なテクノロジーパートナーを選択することも重視してください。

データの安全とセキュリティは、AVEVAの最優先事項です。
産業用ソフトウェアポートフォリオの提供に
50年以上の実績を持つリーダー企業として、AVEVA はお客様のデータを
厳格なサイバーセキュリティポリシーと最高レベルの運用基準に沿って保護します。

これまでの実績

全世界で **10万以上** の拠点に導入

1日あたり **10兆件以上** トランザクションを処理

パラメーターを **200億以上** 監視

1年あたり **12,000TB** の情報を保存、管理

オペレーションテクノロジーのセキュリティに関する重要事項

エンドツーエンドセキュリティ

接続デバイス

AVEVA はセキュリティを基礎から構築しています。実証され標準を満たすコンポーネントを使用し、暗号化も実施しています。

エッジ制御

AVEVA は、システム設計および開発プロセスにセキュリティ保護を組み込み、厳格なテストと検証などを実施しています。

アプリ、分析およびクラウドサービス

セキュリティは設計上不可欠な要素としてお客様のシステムオペレーションのサポートに、最初から組み込まれていなければなりません。

OT（Operational Technology）への侵害による潜在的なリスク

- 人命に関わる甚大な侵害
- 知的財産の情報漏洩
- 生産の停止と浪費
- 環境への重大な影響
- 高額の罰金と罰則
- 企業ブランドの低下

自社のサイバーセキュリティに関するチェックリスト

サイバーセキュリティは多角的な領域に企業全体で事前対応的なアプローチが必要です。
既に対応している企業は、これらを重視しています。

人

- 従業員、請負業者、サードパーティに対するセキュリティトレーニングに投資する
- USB、マルウェア、フィッシングについて教育する
- 積極的にサイバーセキュリティに協力するよう従業員を促す

ネットワーク

- ITシステムとOTシステム間に一方向ゲートウェイを設置する
- 脆弱性スキャンを実行し、定期的にパッチを提供する
- エンドポイント向けのマルウェア対策ソリューションをインストールする

パートナー

- パートナーとして、共に重要データの保護に取り組むベンダーを選択する
- パートナーのセキュリティ、プライバシーおよび法律に関するポリシーを理解する
- データ収集および保存場所を決定する

プロセス

- サイバーセキュリティの取り組みの策定、文書化および検証を行う
- 経営陣、IT部門、セキュリティ部門など、部門間での賛同を得る
- セキュリティ監査や脆弱性スキャンなど、さまざまな活動を網羅する

デバイス

- IoTデバイスのパスワードを、工場出荷時のパスワードから変更する
- セキュリティおよびパスワードのポリシーの対象を、モバイルデバイスにまで拡大する
- デバイスに対して定期的な侵入テストと異常検出を実施する

ベンダーのサイバーセキュリティに関するチェックリスト

サイバーセキュリティでは、パートナーとなるベンダー選択が重要です。
ソフトウェアベンダーは、お客様のサイバー防御戦略で重要な役割を果たします。
以下に示しているのは、クラウドパートナーまたは IIoT パートナーを検討する際の重要確認事項です。

物理的なセキュリティ

- クラウドサービスが配置されている物理的な場所はどこか？
- 自分のデータはどこに保存されるのか？
- 自分のデータがどこで、どのように取得、保存、使用されるのか？

データのセキュリティ

- 保存中および移動中の情報は、どのように保護されるのか？
- ベンダーは一方向のデータ転送に対応しているか？
- サプライヤーがどのようにしてネットワーク停止をするのか？

アプリケーションのセキュリティ

- どのようにして、認証、承認およびアカウント管理を処理するのか？
- ID およびアクセス管理（IAM）の手法は何か？
- 柔軟で拡張可能なソリューションを提供しているか？

継続的な監視

- 事前対応として監視ポリシーと積極的なセキュリティポリシーを整備しているか？
- 異常な挙動を識別し、特異な活動を捕捉できるか？
- オンラインで不審な活動を検出し、隔離する手順が用意されているか？

セキュリティの診断

- 事前対応的な取り組みとして、外部のセキュリティ監査を受けているか？
- どのようにして個人情報保護法などの規制に継続的に準拠していくのか？
- セキュリティに関する声明が公開されていて、参照できるか？

プロジェクトとデリバリー

- プロジェクトのデリバリーチームは、CMMI レベル 5 または ISO 9001 などの世界標準の認証を取得しているか？
- CSIRT（Computer Security Incident Response Team）チームが設置されていて、すぐに対応できるか？
- Cylance または Claroty などの重要なセキュリティ専門企業と戦略的パートナーシップを結んでいるか？

AVEVA は、デジタル分野でお客様の信頼獲得と維持に全力を尽くしています。
それが、当社がセキュリティに関する声明を積極的に公開している理由です。
https://www.aveva.com/en/legal/trust/ でご確認ください。

世界で最も信頼されている産業界のリーダー企業からの支持

550以上の	精製施設
4,600の	食品・飲料加工工場
上位10社中9社の	造船所
3,200以上の	インフラ企業
1,000以上の	発電所

今こそ IIoT およびクラウドテクノロジーを活用する絶好の機会です。
デジタルトランスフォーメーションとは、オートメーションに対する既存投資を変革し、
ビジネスを成功へ導く手段でもあります。

当社のエキスパートに問い合わせる

AVEVA

www.aveva.com
linkedin.com/company/aveva
@avevagroup
facebook.com/avevasolutions