欧州市場法規制（機械規則/CRA/EU AI法）への統合適合支援サービス

～複雑化するCEマーキング要件を満たし、製品の市場投入を加速～

Name	ベリフィケーションテクノロジー株式会社	CEO	竹内秀人
Establish	2003 年 4 月 1 日	Fund	60,550,000 円
Business Solution	◆ LSIデザイン/ベリフィケーションサービス　◆セーフティ/セキュリティサービス		

Location

◆ 本社
〒222-0033
神奈川県横浜市港北区新横浜 2-3-12 新横浜スクエアビル
5F Tel :(045)-470-8310　　Fax:(045)-470-8319

◆関西支社
〒600-8813
京都府京都市下京区中堂寺南町 134 KRP2 号館 2 階 202 号室
Tel :(075)-950-0430 Fax:(075)-950-0431

◆Verification Technology Philippines, Inc
UG15 Upper Ground Cityland Pasong Tamo,
6264 Calle Estacion St., Makati City Philippines

◆Verification Technology Germany, GmbH
Bamberger Strasse 7, 01187 Dresden, Germany

- はじめに
  - CEマーキング
  - 機械規則
  - CRA
  - EU AI法

- 機械規則/CRA/EU AI法で製造メーカが実施すべき内容
  - 機械規則における製造メーカの主要な実施内容
  - CRAにおける製造メーカの主要な実施内容
  - EU AI法における製造メーカの主要な実施内容
  - 機械規則/CRA/EU AI法の要求事項に対する具体的なアクション

- サービス概要
  - GAP分析
  - プロセス構築サポート
  - 技術文書作成サポート
  - 脆弱性試験
  - PSIRT代行サービス

はじめに

CEマーキング
機械規則
CRA
EU AI法

はじめに

現在、欧州市場への製品展開において、これまでにない大きな法規制の波が押し寄せています。

- 機械規則
- サイバーレジリエンス法 (CRA)
- EU AI法

これらは個別の法規制ですが、**重複適用**されます。

「サイバー攻撃によって機械の安全装置が無効化される」
「AIの誤判断が物理的な事故を招く」

といった複合的なリスクを想定されており、個別の対応では重複コストの発生や、適合性の漏れが生じるリスクがあります。

CEマーキング

EU域内で販売される製品が、欧州の共通基準（安全・健康・環境保護）を満たしていることを示すマークです。欧州市場で製品を流通させるための必須認証であり、消費者が安全な製品を識別するための重要な指標となっています。

機械製品にAIが搭載され、ネットワークに接続される場合、その製品は以下の全ての法規制を満たす必要があります。

- 機械規則
- CRA
- EU AI法

機械規則 (Machinery Regulation：MR)

製造業界を取り巻く環境は、2006年の旧機械指令 (Machinery Directive：MD) 制定時から劇的に変化しました。最大の要因は、AI（人工知能）やIoTによる「自律化」と「ネットワーク接続」の普及です。従来の機会指令では、ソフトウェアの更新やサイバー攻撃による誤作動といった現代的リスクを十分にカバーできませんでした。安全基準を現代化し、製品の設計段階からサイバーセキュリティの考え方を義務化した機械規則が、**2027年1月20日から全面適用**されます。違反に対する罰則は加盟国ごとに異なりますが、重い罰金などの罰則が科されます。

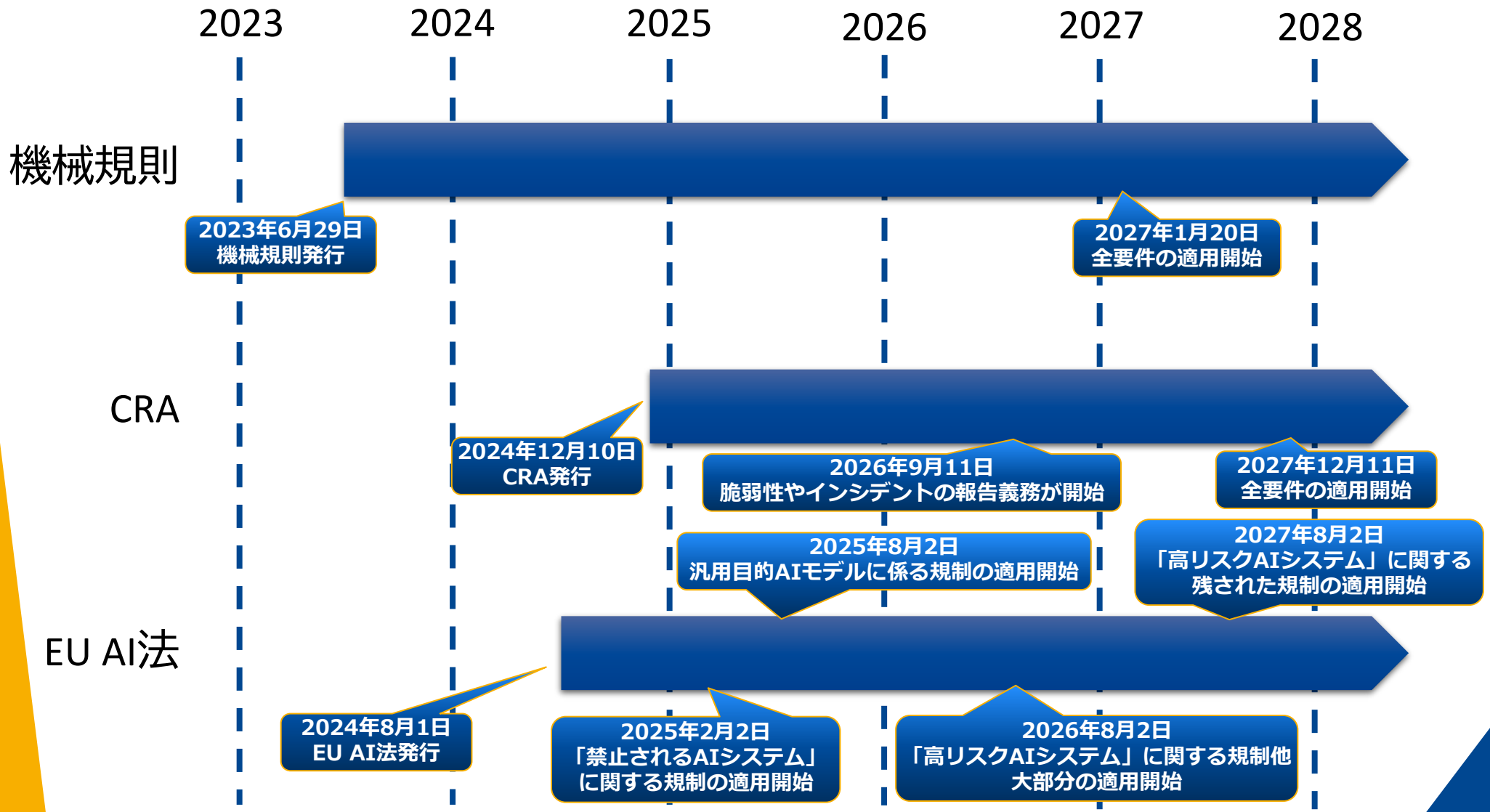
サイバーレジリエンス法 (Cyber Resilience Act：CRA)

現代の製造現場や消費者の生活において、デジタルの利便性が高まる一方で、IoT機器やソフトウェアの脆弱性を突いたサイバー攻撃は年々巧妙化・激増しており、社会インフラ全体を揺るがす脅威となっています。これまでのセキュリティ対策はメーカーの自主的な判断に委ねられていましたが、デジタル要素を持つすべての製品に対して、設計段階からの安全確保と、製品寿命を通じた脆弱性管理が「法的義務」されたサイバーレジリエンス法が、**2026年9月11日から報告義務開始、2027年12月11日から全面適用**されます。CEマーク取得にはサイバーレジリエンス法への適合が不可欠です。違反に対する罰則は、制裁の上限で、最大1,500万ユーロ(およそ28億円)または前年度の全世界売上高の2.5%
(例えば、売上高1000億円の場合は25億円)のいずれか高い方とされております。

EU AI法 (EU AI act)

2024年8月に施行された世界初の包括的なAI規制法で、AIの危険度に応じて4段階（禁止、高リスク、限定的、低/最小リスク）に分類し、安全性、透明性、人権保護を義務付けるEUの法律です。**段階的ではありますが既に適用が始まっており、2026年8月2日から原則適用**され、EU内でサービスを提供する日本企業も対象となります。違反に対する罰則は、全世界売上高の最大7% (例えば、売上高1000億円の場合は70億円)または3,500万ユーロ(およそ65億円)のいずれか高い方の制裁金が科されます。

機械規則、CRA、EU AI法のスケジュール



非常にタイトなスケジュールとなっており対応は急務となっています。

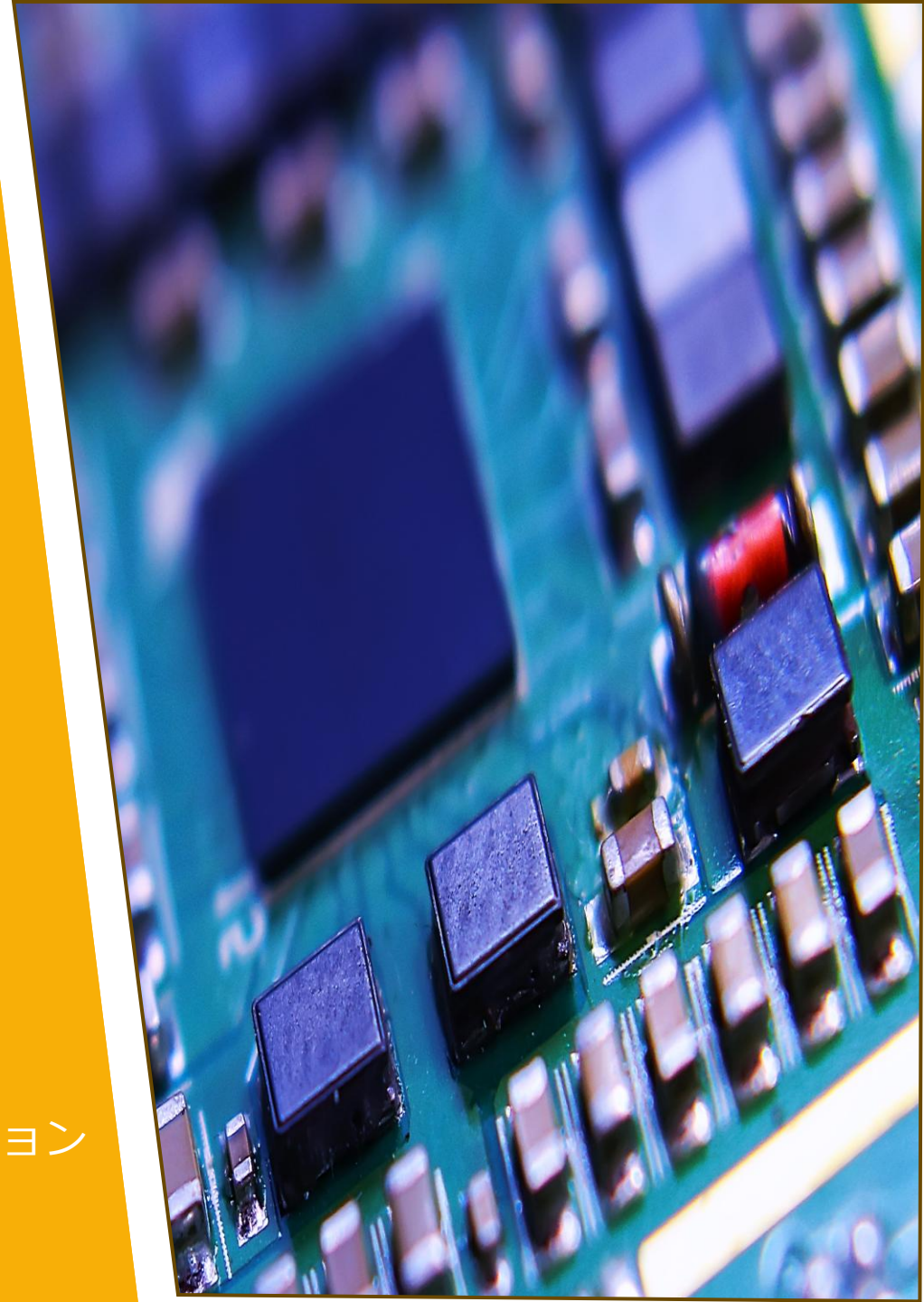
機械規則/CRA/EU AI法で製造メーカが実施すべき内容

機械規則における製造メーカの主要な実施内容

CRAにおける製造メーカの主要な実施内容

EU AI法における製造メーカの主要な実施内容

機械規則/CRA/EU AI法の要求事項に対する具体的なアクション



機械規則における製造メーカの主要な実施内容

① 設計・開発段階

- **必須安全衛生要求事項への適合**: 安全衛生要求事項を完全に満たすように設計・製造する。
- **リスクアセスメントの実施**: 製品の全ライフサイクルにおける危険源を特定し、評価を行う。
  機械同士の相互作用（組立品）によるリスクも評価対象に含める。
- **技術文書の作成と維持**: 適合性を証明するための技術文書を作成し、製品の上市から10年間保管する。
  当局の正当な要請がある場合は、ソースコードやプログラム論理も提供可能な状態にしておく。

② 適合性評価

- **適合性評価手続きの実施**: 製品カテゴリに応じた適切な手続きを実行する。
- **EU適合宣言書の作成**: 適合を証明する「EU適合宣言書」を作成する。
- **CEマーキングの貼付**: 適合が確認された製品にCEマークを貼付する。

③ 上市後の管理

- **不適合時の対応**: 製品が規則に適合していない疑いがある場合、直ちに是正措置を講じる。
- **EU適合宣言書の作成**: 適合を証明する「EU適合宣言書」を作成する。
- **CEマーキングの貼付**: 適合が確認された製品にCEマークを貼付する。

CRAにおける製造メーカの主要な実施内容

① 設計・開発段階の義務

製品を市場に出す前に、セキュリティを考慮した設計(Security by Design)が求められます。

- **サイバーセキュリティリスクアセスメントの実施**: 製品に関連するサイバーリスクを特定し、設計・開発プロセスに反映させる。
- **脆弱性のない設計と製造**: 既知の脆弱性がない状態で製品を上市できるよう、適切なセキュリティ対策を講じる。
- **デフォルトでのセキュリティ設定**: 製品が最初から安全な構成(セキュア・バイ・デフォルト)で提供されるようにする。
- **技術文書の作成と維持**: 製品の設計、製造、および脆弱性処理プロセスを証明する技術文書を作成する。

② 適合性評価

製品の重要度に応じた適合性証明が必要です。

- **適合性評価手続きの実施**:製品カテゴリに応じ、自己宣言または第三者認証による適合性評価を行う。
- **EU適合宣言書の作成とCEマーキングの貼付**: 要件を満たしていることを宣言し、製品にCEマークを表示する。
- **ソフトウェア構成表(SBOM)の作成**:製品に含まれているソフトウェアコンポーネントを特定できるSBOMを作成し、その内容を文書化する。

③ 上市後の管理

- **脆弱性の監視と修正**: 発見された脆弱性に対して、速やかにセキュリティアップデートを提供する。
- **悪用された脆弱性の報告**: 実際に悪用されている脆弱性を検知した場合、24時間以内にENISA(欧州機関)等へ報告を開始する。
- **インシデントの報告:** 製品の安全性に影響を与える深刻なインシデントが発生した場合も、同様にENISAへ報告する。

EU AI法における製造メーカの主要な実施内容

① 開発・設計段階

AIシステムの信頼性を担保するため、以下の要素を設計に組み込む必要があります。

- **リスク管理システムの運用**: 全ライフサイクルを通じてリスクを特定・評価・対策する継続的なプロセスの構築。
- **データガバナンスの徹底**: 学習・検証データの妥当性を確保し、バイアス（偏り）の特定と修正を行う。
- **技術文書の作成と維持**: アルゴリズム、開発プロセス、評価結果などを詳細に記した文書を整備する。
- **「人間による監視」の設計**: AIの動作を人間が監視し、必要に応じて介入・停止できる仕組みを実装する。
- **精度とセキュリティの確保**: 適切な精度の維持と、外部攻撃やエラーに対する堅牢性を備える。

② 適合性評価

製品をEU市場に出す前に、以下の法的手続きを完了させる義務があります。

- **品質管理体制の構築**: 法令遵守を確実にするための組織的なプロセス（文書化された戦略）を確立する。
- **適合性評価**: 定められた手順に従い、自己評価または公認機関による評価を実施する。
- **EU適合宣言とCEマーク貼付**: 適合性を自ら宣言し、製品にCEマークを表示する。
- **EUデータベースへの登録**: 市場投入前に、当局が管理するデータベースに製品情報を登録する。

③ 上市後の管理

販売して終わりではなく、運用中の安全性も監視し続ける必要があります。

- **市販後モニタリング計画の実施**: 実際の稼働データからリスクを収集・分析し、継続的な改善に繋げる。
- **重大インシデントの報告義務**: 重大な事故や規制違反を検知した際、速やかに当局へ報告する体制を整える。
- **迅速な是正措置**: 不適合が判明した場合、直ちに修正、出荷停止、または回収を実施する。

機械規則/CRA/EU AI法の要求事項に対する具体的なアクション

各法規制には、製造メーカが遵守すべき要求事項が定められています。 しかし、その多くは原則論に留まり、具体的な実施手法までは明文化されていません。 そのため、「具体的に何を、どこまで実施すれば適合と言えるのか」という実務レベルの判断に苦慮されているケースが散見されます。
ここでは、セキュリティリスクアセスメントを例に、当社が考える「具体的なアクション」の一例を提示いたします。

セキュリティリスクアセスメント

守るべき資産の特定： 資産を洗い出し守るべき資産(分析対象)を決めます。
データフロー可視化：DFD(Data Flow Diagram)を作成して、データの流れを可視化します。
脅威の洗い出し：STRIDE※1を用いて脅威分析を実施します。
攻撃手段の調査：Attack Tree※2を用いて各脅威に対する攻撃手段を洗い出します。
リスクの評価：DREAD※3を用いて脅威が実現した際のリスク度合いを数値化します。
スコアの算出基準は予め明確にしておく必要があります。

要求事項への対応に課題や不安がございましたら、ぜひ当社へお声がけください。
具体的なアクションプランをご提示させて頂きます。

※1 STRIDE： Spoofing(なりすまし)、10 Tampering(改ざん)、Repudiation(否認)、Information Disclosure(情報漏えい)、Denial of Service(サービス拒否)、Elevation of Privilege(権限昇格)の六つの脅威の性質 の頭文字から構成され、これら六点の性質から脅威を洗い出していく手法
※2 Attack Tree：洗い出したセキュリティ脅威に対して、それが顕在化する条件を分解し、現状の設計に対して攻撃が成立する可能性があるかどうかを考察することで脆弱性の分析を行う手法
※3 DREAD： リスクを評価し、スコアを算出する手法。DREADはDamage、 Reproducibility、Exploitability、Affected users、Discoverability の五つの観点の頭文字

サービス概要

GAP分析
プロセス構築サポート
技術文書作成サポート
脆弱性試験
PSIRT代行サービス

サービス概要

3つの主要法規制(機械規則・CRA・EU AI法)を横断的に対応し、
効率的かつ確実にCEマーキング適合を達成するための
コンサルティング・実務支援を提供します。

- GAP分析
- プロセス構築サポート
- 各種技術文書作成サポート
- 脆弱性試験
- PSIRT代行サービス

導入メリット

- コストの最適化
  3つの法規制を個別に対応するのではなく、共通項目を統合して対応を進めることで、
  工数を大幅に削減します。
- コンプライアンスリスクの低減
  巨額の制裁金リスクを回避します。
- 市場投入の迅速化
  開発の初期段階から法規制を考慮することで、手戻りを防ぎスムーズなCEマーキング取得を
  実現します。
- 開発チームの負担軽減
  コンサルティングに留まらず開発チームに代わって実務を請け負うことで負担を軽減させます。

整合規格の正式発行をまって、設計変更の着手をすると2027年12月までのデッドライン
まで僅かな期間しかありません。

-ハードウェアの設計変更、金型修正
-サプライチェーンからの部品調達、検証
-第三者認証機関の予約と審査

規格案(prEN)やドラフト段階での先行着手にて進めていくことが重要です。

まとめ

当社では、 3つの主要法規制(機械規則・CRA・EU AI法)に対する支援サービスを提供しています。

これらの複雑な法規制をクリアすることは、次なる市場をリードするための必須条件です。
私たちは、貴社の開発スピードを損なうことなく、最短ルートでの市場投入を
強力にバックアップします。

また、国内ロボットメーカー様と共同開発し、自社製品化したセキュリティアダプタもございます。
当社のセキュリティにおける知見をもとに法規制や製品開発におけるご支援を致します。

より具体的なサービス内容は営業よりご案内させて頂きます。
お気軽にご相談ください。

ベリフィケーションテクノロジー株式会社

■本　社
〒222-0033　横浜市港北区新横浜2-3-12　新横浜スクエアビル5F
TEL：045-470-8310　　FAX：045-470-8319
お問合せ窓口 sales@vtech-inc.co.jp

□関西支社
〒600-8813　京都市下京区中堂寺南町134　KRP2号館2階
TEL：075-950-0430　　FAX：075-950-0431