ADD VNTR.

製造業のコトづくりを支える強固な「製品セキュリティ」の実現へ

MACNICA

「コトづくり」に向けた変革の中で生じるセキュリティ対策を立案から実行まで

背景と課題

コトづくりへのシフトで変わるセキュリティの責任範囲

- 製品のコモディティ化が進み競争が激化する現在、「モノ」だけを売るビジネスは限界に近づきつつあります。
- ソフトウェア、データサービスで顧客体験価値を届ける、「コト」ビジネスの重要性が高まっています。
- 「コト」ビジネスでは、自社がソフトウェア環境を管理してサービスを提供する範囲が拡大します。
  これまで顧客の責任範囲だったセキュリティ領域の一部を自社が管理していく必要が生じます。

詳細≫ P6

これからのセキュリティ対策の方向性

「サービスイン後」のセキュリティ対策が必要に

- 「コト」ビジネス（サービスビジネス）では、サービスイン後こそ運用上のセキュリティ対策の重要性が高まります。脆弱性の懸念がある端末側のファームウェアアップデート、クラウドインフラへの攻撃に対する対応（検知・対応・復旧）が必要になります。
- セキュリティ対策はまず自社の現状を正確に洗い出し、リスクを特定し、優先順位を付けながら具体的な対策に落とし込んで実行すること、そしてそのプロセスを繰り返し改善し続けることが重要です。

詳細≫ P5

マクニカの強み

製造業の現場を熟知し、対策の実行まで伴走

- マクニカは、国内・海外の標準規格をベースに、独自の知見を盛り込んだリスクを評価を実施し、優先度に基づいて課題と改善策を提示する「製品セキュリティ成熟度調査」によって対策の第一歩を支援します。
- セキュリティ対策の運用が開始された後も、サイバーセキュリティに関する最新の知見と、長年にわたって製造業の現場を知り尽くしてきたメンバーやノウハウのもと、日々の対策の実行まで伴走します。

詳細≫ P7、8

コトづくりによる企業価値向上の可能性

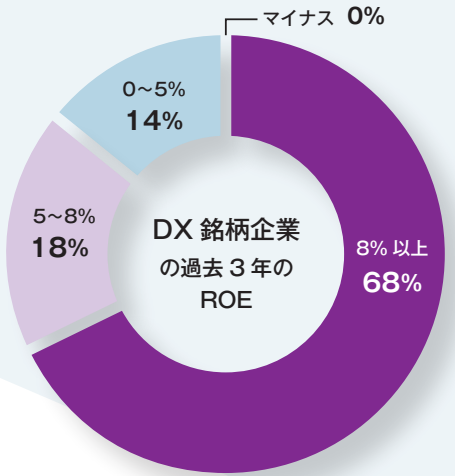
コトづくりによる顧客体験の創出

モノが得られるかではなく、モノを通じて上質な顧客体験が得られるかが重視される今日は、「コトづくり」への転換が必要です。そこに必要なのは、蓄積されたデータや優れたソフトウェア技術を駆使して継続的にサービスを提供して顧客のニーズへ的確かつ迅速に応え続ける仕組みです。それらデジタルに注力する企業のROEが高い傾向にあることが明らかになっています。

モノづくりから変革の課題

世の中にモノが飽和し、コモディティ化が進む中、ただ機器を開発・販売するだけでは、激化するコスト競争やデジタル技術を活用した新興企業との競争に勝ち抜くことは困難です。

デジタルへ注力する企業はROEが高い傾向が明らかに



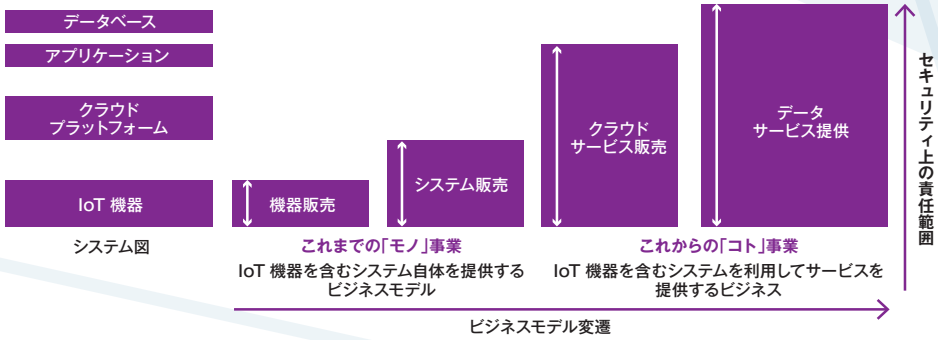
経済産業省「デジタルトランスフォーメーション調査 2021 の分析」より
※その他企業…経済産業省による「DX 銘柄」の制度における「DX 銘柄企業」「注目企業」「左記以外の認定申請企業」に含まれない企業

コトづくりでは責任を負う範囲が拡大する

コトづくりでは
セキュリティ対策領域が変わる

「コト」ビジネスへの転換にあたってデータサービスやクラウドを活用したサブスクリプションサービスに乗り出す企業が増えています。しかしそれは、自社がいままで管理する必要がなかったデータやクラウドインフラに対するセキュリティの責任を負う必要になったことを意味します。セキュリティが不十分であれば、提供する製品の脆弱性を原因とするサイバー攻撃でお客様に被害を及ぼし、自社が加害者になってしまう恐れもあります。DXはセキュリティ対策と両輪で進める必要があります。

「コト」ビジネスでは、製造業自身でインフラやデータを抱えるため、
セキュリティ対策の強化が必要



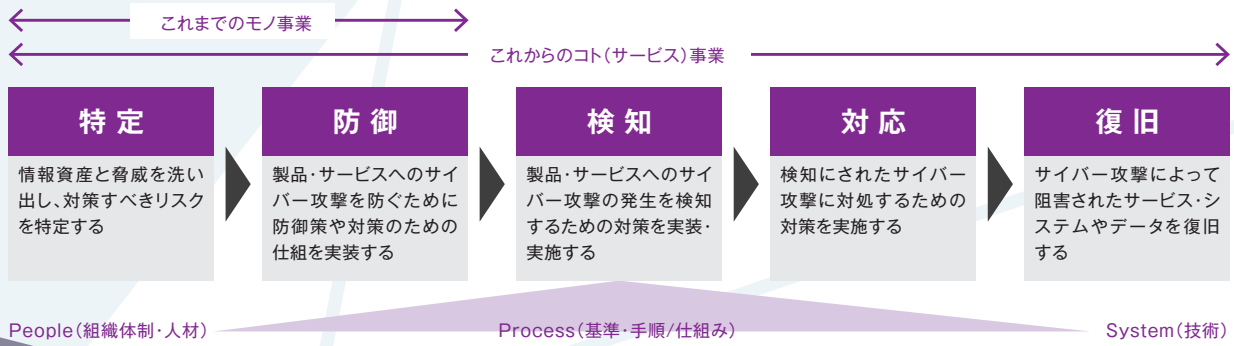
コンサルタントからの注意ポイント

新規事業の立ち上げにおいては、サービス開発やその事業活動に向けて、クラウドを活用したシステム開発が優先され、セキュリティが二の次にされる傾向にあります。その原因は経験のなかった技術分野における知見・経験の不足やセキュリティ人材の不足が上げられます。コトづくりにおいては、対象のサービスの事業継続としてセキュリティは必須です。経営者として必要な投資の判断が必要となります。

脅威の「特定」から「復旧」までの仕組み化と体制運用が急務に

「侵入はあり得る」を前提に検知・対応・復旧までの対策を

これまでは、悪意ある攻撃者による攻撃を防ぐための「防御」に重きが置かれがちでした。それは従来のモノづくりのビジネスでも同様です。しかしデジタル技術の発展と共にサイバー攻撃の高度化も進み、すべての攻撃を防ぐことは困難になりつつあります。そこで、サイバー攻撃を受けてしまうことを前提に、検知・対応・復旧のプロセスを整備して被害を最小にとどめる、サイバーレジリエンスという考え方が重視されるようになっています。製品セキュリティにもこの考え方を取り入れ、新たな脆弱性が発覚した際にいかに素早く対応できるか、サービスに対する攻撃が発生した際にいかにサービスの復旧を素早く行えるかが重要になります。



特に強化するべきは、製品セキュリティ独自の方針・体制・プロセスの融合

日本の製造業は、モノづくりにおける品質確保を得意としてきました。しかし、より顧客と長いフェーズにまたがるコトづくりの中で新たなセキュリティリスクをとらえ、対処するための人や体制、プロセス、そして技術が整っていないことが課題です。中でも多くの製造業が直面している課題として、以下の3つの切り口が考えられます。

1 独自のセキュリティ方針の策定

情報セキュリティに関する方針やガイドラインを定め、開示している企業は多くありますが、製品セキュリティ方針となるとまだ少数派です。製品セキュリティにどのように取り組むかの全体的な指針やビジョンが示されていなければ、現場の姿勢も定まりません。方向性を明らかにし、それに基づいた対策基準や手順、組織を整備し、ガバナンスを確立することが第一歩です。

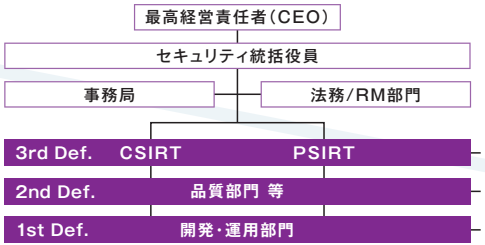
2 能動的なインシデント対処

「コトづくり」の世界では出荷後も継続的にサービスを提供していきます。また常に攻撃の手法も変化するので全てを防ぐことは困難です。サービス基盤がサイバー攻撃を受ければ顧客に大きな影響を与える恐れがありますので、攻撃を受けることを前提とした対処をしていく必要があります。そこで、受け身ではなく、サイバー攻撃を早期に検知し、製造部門と連携を取りつつ迅速に対処して影響を最小限にとどめるキュリティ監視が必要です。また攻撃を受けてからいかに早く復旧するかのインシデント対応体制が必要です。

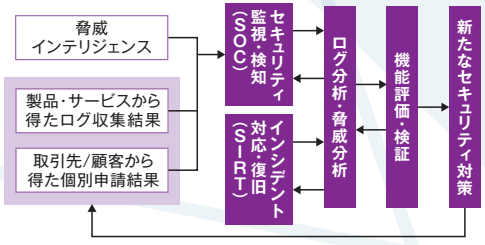
3 サプライチェーン攻撃への対策

製造業のサプライチェーンは複雑です。昨今、サイバー攻撃者はここに目を付け、パートナーや子会社側にまず侵入し、そこからシステムに影響を及ぼす事件が発生しています。パートナー企業から納品される部品やソフトウェアに脆弱性やバックドアが含まれているケースも出てきており、サプライチェーン全体で対処が求められてきています。

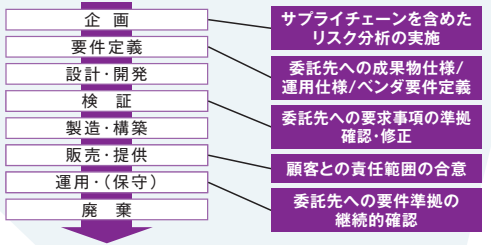
マネジメント体制の一例



分析を中心としたアクティブ監視体制



製品・サービスライフサークル



徹底的な現状把握、そして改善サイクルを自社で回すことが重要です

場当たり的な対策では次々に来るセキュリティ攻撃で手一杯になります。適切なステップを踏んだセキュリティ対策で、製品の信頼構築を実現することができます。

STEP 1

現状把握とセキュリティ成熟度評価

製品セキュリティは現状把握から始まります。例えばIoT製品、クラウド環境、ネットワーク構成等です。次に自社が提供するサービスに対して守られねばならない標準規格の洗い出しを実行します。その環境と規格で守るべきことから調査をすることで、セキュリティリスクの洗い出しができます。そのリスクを減らすために、セキュリティガイドライン修正や、社員の教育、事故～復旧対応プロセス整備、サプライチェーンリスク管理改善など様々な観点から対策項目を明らかにしていきます。

STEP 2

対策項目の優先順位付け

対策項目をむやみやたらに始めてはいつまで経っても効果は表れません。何から始めるかが重要です。はじめに取り組むべきは検知～対応～復旧についてWho・What・Howを決めることです。たとえば、一定のセキュリティ品質を担保する体制が不十分であれば、PSIRTと呼ばれるチームを組織する。また、セキュリティガイドラインの整備や製品開発プロセスに関係各所でチェックを必然化するなど、セキュリティに対してはシステム導入だけでなく、人、プロセスも含め、必要な対策を明確化していかなければならないのです。

STEP 3

対策の社内浸透

「セキュリティガイドラインができた」、「開発プロセスができた」、「セキュリティ運用体制ができた」という時点で満足してしまいがちですが、ここからが本当のスタートです。策定したルールやマニュアルが適切に運用されるよう、自社内で浸透させることが、最も大変であり、最も重要なポイントです。企業のトップや情報セキュリティ担当だけでなく、製造現場や品質管理部門、DXに関する新規事業推進担当など多くのステークホルダーを巻き込み、協力を得ることが重要です。

STEP 4

定期に目標達成度の効果測定を実施し、継続的に改善

製品セキュリティ対策の難しいところはセキュリティ攻撃がアップデートされるため、日々対策も改善を進めなければならないことです。一度の対策を実行では終わりとなりません。もちろん、KPIに対する効果測定や振り返りも重要ですが、新たな脅威や課題から弱点を徹底的に深堀するなど、定期的な見直しが必要となってきます。最低でも1年に一度は関係者で効果測定のレビュー、課題認識、改善計画立案はする必要があります。

セキュリティと ものづくりの現場を 長年サポートしている マクニカだからこそできる 製品セキュリティ実行支援

マクニカは半世紀にわたり、半導体ビジネス「モノづくり」を展開し、製造業のお客様を現場からサポートしてきました。また、セキュリティに関してもほとんどの企業が課題認識をしていない時代から課題解決に取り組み、現場でサポートを続けています。更には専門の研究所を設立してセキュリティの知見を蓄積し、外部への発信も積極的に実施しています。現在我々はIoTやAIといった新たなデジタル技術に積極的投資を行い、これまでの強みを掛け合わせ、コトづくり時代の製品セキュリティ支援を実行しています。

マクニカ特有の 製品セキュリティにおける 成熟度調査

経済産業省の「サイバーフィジカルセキュリティ対策フレームワーク」やIEC 62443、NIST SP800-171といった国内外の標準から評価をするのはいわゆる及第点の調査です。日本の製造業独自の課題や日本特有のセキュリティ攻撃手法などの評価項目の追加が必要で、我々の知見があるからこそ更に深い調査が可能と考えています。

現場が実行できる コトづくりセキュリティ対策の 実行支援

左のような標準規格はあいまいな表現が多いため、実際評価するのは簡単ではありません。ましてや実行する現場は「何をしたらいいかわからない」ということになります。マクニカはこれまでの現場サポートの知見やノウハウをもとに、調査の回答者が明確に答えることができる質問項目の作成から実際の実行項目の落とし込みなど、「絵に描いた餅」ではない現場に寄り添ったセキュリティ対策の伴走型実行支援が可能です。

マクニカが提供する製品セキュリティ成熟度調査

国際標準のセキュリティ基準に独自の知見を融合

- 経済産業省 サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
- IEC 62443
- NIST SP.800-171

弊社知見 MACNICA

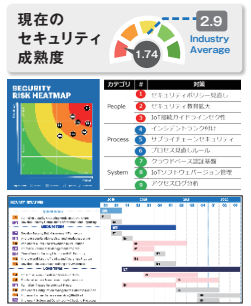
組織体制、人材、デバイス、システム、データ、プロセスなど多彩な観点から調査

ルール・運用 / 組織・ポリシー / ツール・技術

14のセキュリティ要件

1	アクセス制御	8	メディア保護
2	意識向上と訓練	9	人的セキュリティ
3	監査と責任追跡性（説明責任）	10	物理的保護
4	構成管理	11	リスクアセスメント
5	識別と認証	12	セキュリティアセスメント
6	インシデント対応	13	システムと通信の保護
7	メンテナンス	14	システムと情報の完全性

成熟度を定量値で評価



お客様の安心･安全を目指した製品セキュリティの実現

さまざまなプロフェッショナルの力を集約

製造業の「コトづくり」へのシフトに不可欠な製品セキュリティ対策については、方針や体制を作るだけではなくやはり現場への浸透が鍵となってきます。また、製品･サービス開発には多くのステークホルダーが関わることから浸透も簡単なものではありません。マクニカは長年にわたってモノづくりの現場を知り、プロセスの中にセキュリティを取り込む難しさと対峙しノウハウを積み重ねてきました。最新の脅威動向も踏まえながらプロフェッショナルとして支援できればと考えております。

ADD VNTR.

ものづくりコンサルティング
コンサルタント紹介

株式会社マクニカ
DXコンサルティング室　マネージャー

飯田 洋平

まずはお気軽にご相談ください

フォームでのお問い合わせ

メールからお問い合わせはこちら
add-venture@macnica.co.jp