Expand - Collapse

□ Bib10-03 【持続的発展のため】組織の発展を目指した戦略的なIT活用とサイバーセキュリティ対策 🗾

- 【2017年5月1日】
- □ ITの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に 競争力強化に活用しようとしている企業
 - □ デジタルトランスフォーメーション
 - 最先端の技術を生かし、コスト削減だけでなく、ビジネスの推進にどう貢献する か
 - □ DXの目指すところ
 - 「ITの浸透が、人々の生活をあらゆる面でより良い方向に変化させること」
 - □ DX時代には
 - 企業がこれからのビジネスで勝ち残っていくためには、新しい製品、サービス、パートナーシップ、ビジネスモデルなどを創造し、新たな価値を創出していく必要があるという
 - □ プラットフォームの構成
 - 「クラウド」「ビッグデータ/アナリティクス」「ソーシャル技術」「モビリ ティ」
 - □ プラットフォームの上にイノベーションアクセラレーター」の技術
 - イノベーションを後押しするIoT、AIや機械学習などの認知システム、ロボティクス、AR (Augmented Reality、拡張現実) / VR (Virtual Reality、仮想現実)、3Dプリンティングなど
 - □ デジタルトランスフォーメーション、インダストリー4.0、ソサエティー5.0、、、
 - データを効率的に集積し、それをAIのディープラーニング機能などを活用して認識・加工し、自らの企業活動に生かしていけるかが、木偉業の成長の可否を決める時代がすぐそこまで来ている【日経1月4日13面 佐藤康博】
 - IT化、デジタル化の進展を受入れ、それを活用して顧客との関係性強化を図る企業は、大きなビジネスチャンスを得ることが期待できる。
 - 人工知能(AI), ディープラーニング, ビッグデータ, IoT, M2M. 仮想現実 (AR), 3 Dプリンタ等を活用した新サービスが、一般化する前に先駆的に取り 入れるベンチャー的木偉業(イノベーター、アーリーアダプター)

□ CtoB

■ 多様な消費者ニーズに対応して、きめ細やかで丁寧なモノづくりが企業の持続的 発展に不可欠な要素となる【日経1月4日13面 佐藤康博】

□ 🗪 競争力強化

- 新サービス、新技術を活用した生産性の向上
- □ 新サービス、新技術を活用した新ビジネス展開
 - 大手企業と中小企業、ベンチャー企業との協業

■ 新サービス、新技術は新ビジネスのチャンスだが、セキュリテ Expand - Collapse きい

□ 企業経営のためのサイバーセキュリティの考え方の策定について【NISC】 <a>☑

- □ 基本方針 サイバーセキュリティは、より積極的な経営への「投資」へ -
 - グローバルな競争環境の変化
 - ITの発展によるビジネスの変革が、消費者向けのビジネスから企業間取引へと拡大
 - サイバー空間と実空間の融合がさらに進み、チャンスもリスクも一層増大
 - ⇒サイバーセキュリティをやむを得ない「費用」でなく、積極的な経営への「投資」と位置づけ、企業としての「挑戦」と、それに付随する「責任」として取り組むことが期待される

□ 基本的な考え方

- □ 二つの基本的認識
 - <①挑戦>サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく
 - <②責任>全てがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与する

□ 三つの留意事項

- □ <①情報発信による社会的評価の向上>
 - • 「セキュリティ品質」を高め、品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。
 - そのような取組に係る姿勢や方針を情報発信することが重要。
- □ <②リスクの一項目としてのサイバーセキュリティ>
 - ◆ 提供する機能やサービスを全うする(機能保証)という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。
 - ●経営層のリーダーシップが必要。
- □ <③サプライチェーン全体でのサイバーセキュリティの確保>
 - ● サプライチェーンの一部の対策が不十分な場合でも、自社の重要情報が流 出するおそれあり。
 - ● 一企業のみでの対策には限界があるため、関係者間での情報共有活動への 参加等が必要。

□ IT活用の必然性

- □ IT活用するためにセキュリティ対策を実施する
 - セキュリティ対策は目的ではない。
 - □ 業務の効率化のためにITを活用する。

- 必要以上のサイバーセキュリティ対策は、業務の効率化を阻 Expand Collapse
- □ 単なる効率化だけではビジネスの競争に勝ち残れない
 - これまで企業のITシステムは、業務、生産工程等を効率化して、経営を安定化させることに重きが置かれてきた。
- □ 組織の発展のためにはITの活用が重要
 - これからはデジタルトランスフォーメーションの時代の時代と言われている。社会の進展に対応したサービスを展開するためにITを活用する
 - IT化、デジタル化の進展を受入れ、それを活用して顧客との関係性強化を図る企業は、大きなビジネスチャンスを得ることが期待できる。
- □ デジタルトランスフォーメーションに対応することが重要
 - 10分で分かる! 近未来予想図202X | nikkei BPnet 〈日経BPネット〉: 日経BP オールジャンルまとめ読みサイト <a>
 - デジタルトランスフォーメーション時代には、創造力、技術力を持ったベンチャー企業など、ビジネスチャンスあり
 - □ 柔軟にかつ大企業に先駆けて、デジタルトランスフォーメーションに対応してい くことが、組織の発展につながる。
 - 人海戦術、定型化した作業、精密作業は、匠の技レベルでなければはシステム、機械に置き換わっていく。
 - 「つながる工場」「インダストリー4.0」「自動運転」「スマートアグリ」
 - 人工知能(AI), ディープラーニング, ビッグデータ, IoT, M2M. 仮想現実 (AR), 3 Dプリンタ等のデジタルを、ITを駆使した新サービスを、一般化する前に先駆的に取り入れることが重要
- □ ITを活用したサービスを継続するためには、情報セキュリティ対策は必須
 - □ セキュリティ侵害は組織の存続が脅かす
 - ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率 化しても、緊急事態(自然災害、大火災、感染症、テロ、セキュリティ侵 害、、)が発生して、事業資産(人・もの(情報及び設備)・金)、社会的信用 が失われ、早期復旧ができない場合は、事業の継続が困難になり、組織の存立さ えも脅かされる可能性がある。
 - □ 事業を継続できるように
 - どんな緊急事態が発生しても、事業を継続できるようにする対策を明示しておく ことが必要
 - □ サービスの向上を図るために
 - 情報資産(保有情報(媒体に依らず)、情報機器、情報システム)に対する情報 セキュリティ上のリスクを低減させる
 - □ セキュリティ対策は先行投資
 - ITを活用したサービスの構築・運用に掛かる費用は、経費ではなく先行投資。リスクに見合った情報セキュリティ対策は、サービスの構築・運用の中で実施すべ

き先行投資であり、緊急事態が発生した後に対処する経費とし Expand - Collapse ない

- □ 情報発信とセキュリティ対策
 - 特に個人情報保護法等と情報公開法等との趣旨を理解した対策を
 - 的確なリスク分析に応じて必要な対策を
 - 個人情報の管理はその程度でいいのか
 - 公開を制限しているその情報はほんとに機密性があるのか
 - 公開してもいい情報は、その完全性、可用性の確保が重要
- □ 🔦 次世代サービス、技術の利用に当たってのサイバーセキュリティ対策
 - 人工知能(AI), ディープラーニング, ビッグデータ
 - M2M, 制御システム【情報セキュリティ白書2016】
 - □ IoT【情報セキュリティ白書2016】
 - IoT早期導入者のためのセキュリティガイダンス【CSA】
 - IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】
 - 安全なIoTシステムの創出【2016年3月1日NISC】
 - コンシューマ向けIoTセキュリティガイド【2016年6月24日JNSA】
 - IoT早期導入者のためのセキュリティガイダンス【2016年2月24日CSA】 🛮
 - □ クラウドサービス
 - ■クラウドセキュリティガイドライン活用ガイドブック2013年版【METI】 <a>☑
 - ●クラウドサービス提供における情報セキュリティ対策ガイドライン【2014年4月総務省】
 - □ ■クラウドセキュリティ関連ISO規格
 - ISO/IEC27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項(スライド) 【JIPDEC】 <a>Z
 - ISMSクラウドセキュリティ認証の概要(スライド)【JIPDEC】 🗾
 - ISO/IEC27017:2015に基づくクラウドセキュリティの構築のポイント (スライド) 【JIPDEC】 <a>I
 - □ スマートデバイス
 - スマートフォン、タブレット等
 - ■スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書【2015年 5月21日NISC】 <a>☑
 - □ VR, MR, AR
 - エンターテインメント、自動車業界、広告業界、教育、宇宙産業、、
 - VR/AR技術の将来展望【2016年6月MRI】
 - VR (Virtual reality:仮想現実)
 - AR (Augmented reality:拡張現実)
 - MR (Mixed Reality:混合現実)

■ SR (Substitutional Reality:代替現実)

Expand - Collapse

- □ ブロックチェーン
 - 仮想通貨
 - ブロックチェーンの安全性とセキュリティコンセンサス・ベイス(株) 🗾
- □ 3Dプリンタ
 - 危険物製造、著作権侵害
- **.** . . .