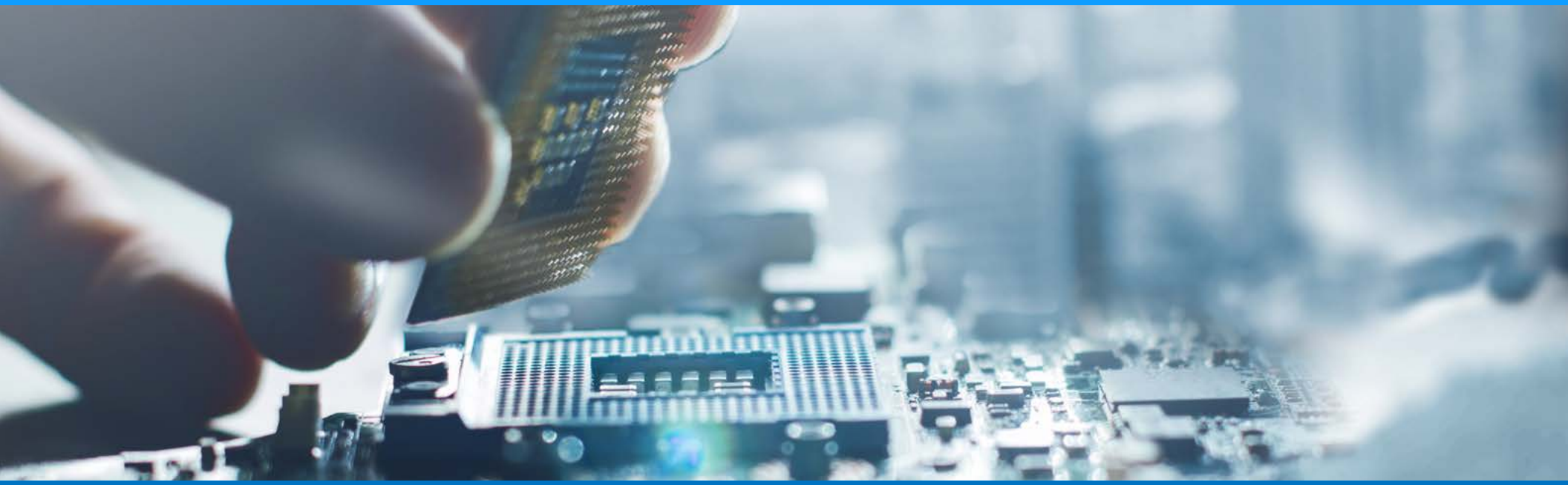
IoTセキュリティの現状に関する調査 (2018)



digicert®

機械の占める割合の急速な増加

今日、世界では一人につきおよそ 3 つのデバイスがインターネットに接続されています。これが 2025 年までには、一人あたり 10 のデバイスにまで膨れ上がります。[1] サーモスタットや車のセンサー、医療デバイス、電力会社のスマートメーターや工場の複雑な機器など、あらゆるデバイスがインターネットにつながるようになってきています。あらゆるものが接続されるこの状態を「モノのインターネット (IoT)」と呼ぶ人々も増えています。

なぜ IoT は急激に増えているのでしょうか？スマートメーターを使えば各戸毎に計器を読み取る労力を節約できるから、といった単に経費節約が目的の場合もあります。しかし、もっと大きな原動力は、ビジネス業界を席捲しているデジタルトランスフォーメーション (DX) です。DX は、「重要な瞬間」の顧客エクスペリエンスを最適化しようとするものであり、IoT はまさしくそれを実現することができるのです。デバイスが顧客エクスペリエンスをモニターすることで、企業は以前では考えられなかったような方法で、瞬時に変化を起こすことができるようになります。

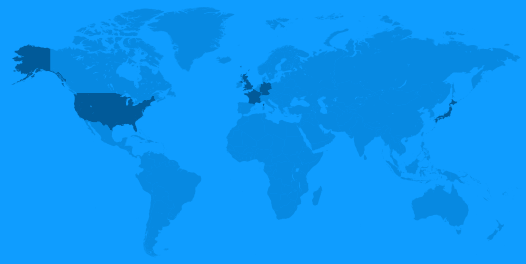
しかし、それにはリスクが伴います。800 億ものデバイスが接続されている世界は、[2] 強大な脅威に晒されている世界でもあるのです。すでにIoT デバイスが対象となった大規模な DDoS 攻撃を目にするようになっていますが、専門家は氷山のほんの一角に過ぎないと言っています。[3] セキュリティ研究者は、現在広範囲に使用されているデバイスの脆弱性を頻繁に指摘しています。

DigiCert では、毎日、260 億件ものインターネット接続の安全を確保しており、お客様が大規模な IoT セキュリティへの実装を進めることでその件数はさらに増えています。そのため、IoT に対して非常に高い関心を持っています。世界中の企業が IoT を活用するようになるにあたってセキュリティにどう対処しているのかを調べるため、DigiCert はテキサス州ダラスに本社を置く ReRez リサーチに依頼し、日本に所在地を置く 100 社を含め、世界の 700 社の企業を対象に調査を行いました。その結果は、IoT 戦略を採用している企業にとって、警鐘を鳴らすものになっています。

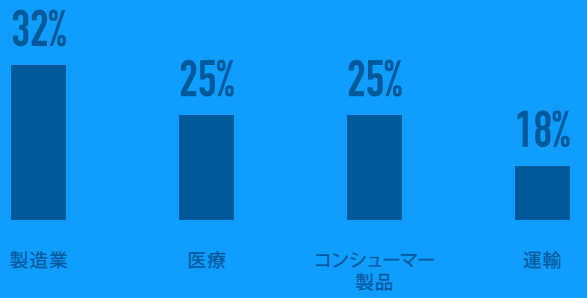
1. IDC 調査 , 国連の人口予測 (英語リンク)
2. IDC 調査 (英語リンク)
3. 注目される IoT セキュリティ (英語リンク)

調査方法

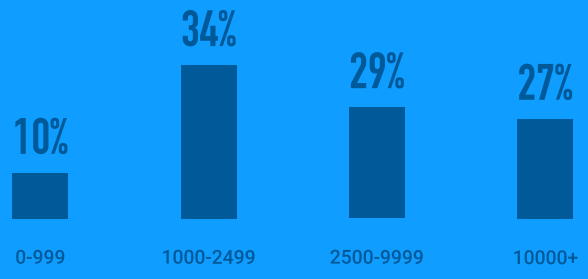
2018 年 9 月、ReRez リサーチは、日本にある 100 社を含め、世界 5 カ国、合計 700 社に対し、オンライン調査を実施しました。



早期に IoT を採用した 4 つの業界に的を絞りました。



対象となった企業は、非常に小規模のものから大企業まであり、また従業員数の中央値は 1 万人でした。



IoT セキュリティの重要性

世界中では、もっとも苦労している企業の 25% が、IoT セキュリティ関連の損失が少なくとも 3400 万ドルに上っていると報告しています。日本の調査対象企業では、過去 2 年間で少なくとも 8100 万ドルの損失が報告されています。何らかの対策を講じない限り、IoT の採用が増えるにつれ、その損失は増加すると予想されます。なぜこうした問題が起きるのでしょうか？そして、IoT セキュリティで成功している企業はどんな対策をとっているのでしょうか？この報告書では、そうした点を取り上げます。

まず、IoT への関心が非常に高いことがわかりました。99% の企業が、現在のビジネスにとって「IoT はある程度重要である」から「非常に重要である」と回答しています。61% が、IoT 戦略の導入が完了していると答えています。そして、39% が導入開始を始めたばかりと回答しています。

93% の企業が 2020 年までに IoT がビジネスの重要な役割を果たすと考えています。

なぜ企業はそこまで IoT に興味を示すのでしょうか？企業が達成したいと報告している 4 つの目標は以下の通りです：

- 顧客エクスペリエンスの向上
- 収益の増加
- 業務効率の向上
- 迅速な業務対応の達成

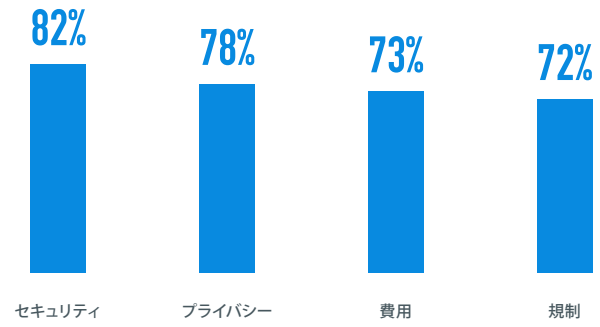
IoT は簡単ではない：懸念事項

同時に企業は IoT に懸念を抱いていることがわかりました。IoT に対して企業が持っている懸念事項の上位 4 つは、以下の通りです：

セキュリティ　費用
プライバシー　規制

次に、企業の IoT に対する努力がどの程度成功しているかを具体的に調査したところ、大きな差異があることがわかりました。つまり、非常に成功している企業がある一方、悪戦苦闘中の企業もあるのです。IoT セキュリティで最も成功している企業と最も苦労している企業を比較したところ、興味深い示唆を得ることができました。

その違いを明確にするため、弊社はクロス集計を実施しました（その方法の詳細については、補足を参照）。その結果わかったことは、これから IoT 導入を開始しようとしている企業に、貴重な情報を提供してくれるはずです。



最悪と最善を区別する

IoT セキュリティの進み具合に関しては、企業間でかなりのばらつきがあることがわかりました。成功している企業で何が原動力になっているのかを理解するため、DigiCert は調査結果を3段階に分類しました:

上位企業

これは、IoT セキュリティの問題をほとんど抱えていない企業です。IoT セキュリティの特定の処理に関する問題を報告する可能性も最も少なく、また実際報告している問題も僅かな数しかありません。

中位企業

これは、IoT セキュリティの調査結果のスコアが中程に位置する企業です。

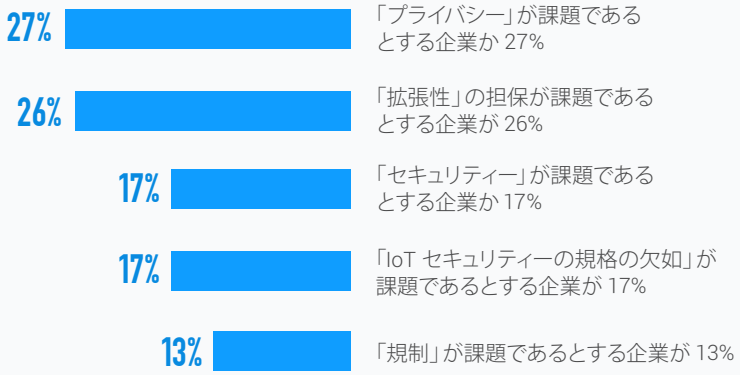
下位企業

IoT セキリュティの面で最も問題を抱えている企業です。IoT セキュリティの特定の処理に関する問題を報告する可能性が最も高く、また実際に最も多くの問題を報告しています。

IoT 関連のセキュリティの課題と失策

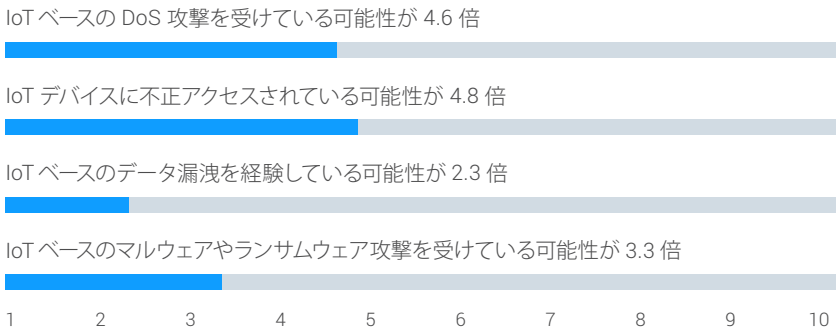
回答企業に、様々な IoT 関連のセキュリティ問題について、それぞれの側面の困難の度合いをランキングしてもらいました。その結果、上位と下位の企業がこういったセキュリティ面での回答に、非常に大きな違いがあることがわかりました。下位企業は、大きな課題として回答するケースが非常に多いことがわかりました。

38% の下位企業が、IoT セキュリティーのスキルを社内に持たず、対応することが「ある程度難しい」または「非常に難しい」と上位企業より感じている。



今度は、こういった課題が、実際にセキュリティ上の失策に繋がるのかを調べました。結果は、その通りでした。IoT セキュリティ関連の失策には、これらの分類で大きな違いが見受けられました。実際、上位企業の 35% は何の問題も起きなかった一方、下位企業の 100% が少なくとも 1 件の問題を経験していました。

100% 下位企業の 100% が、少なくとも 1 件の問題に遭遇している。



また、それぞれの種類の失策がこの 2 年間で企業にどれほどの損失を発生させたのか調査しました。そして、世界中で、最も苦労している企業の 25% が、IoT セキュリティ関連の損失が過去 2 年間で最低 3400 万ドルあったと報告しています。

日本企業ではまた、過去 2 年間に IoT セキュリティの損失により与えられた金銭的ダメージのうち、法的、およびコンプライアンス違反による損失が中央値で約 255 万ドル (1 ドル＝112 円換算で約 **2 億 8560 万円**となっています。

調査対象の日本企業 100 社において、過去 2 年間に発生した IoT セキュリティ関連で発生したコストの内訳上位 5 項目は次のとおりです。

49%	金銭的損害
38%	生産性の喪失
26%	評価・評判の喪失
25%	株価への影響
21%	個人のキャリアに与える否定的影響

上位企業の行動

上位企業の実績が際立っていたため、IoT 関連のセキュリティに対してこれらの企業がどのようなセキュリティ対策を実施しているのか調査しました。上位企業もある程度のセキュリティ上の失策は経験していましたが、そのほとんどがそれによる損失はないと報告しています。上位企業が最も一般的に採用しているセキュリティ対策は、以下の通りです：

コードサイニング

デバイス間で
送受信されるデータの
完全性の確保

セキュリティ対策の
信頼性

OTA（オンライン）
アップデートによる保護

安全なハードウェアベースの
キーストレージ

IoTの爆発的利用に伴う安全性の確保

800 億ものIoT デバイスが使用される将来のために、IoT セキュリティに注意しておく必要があります。上位企業は、認証やアイデンティティー、暗号化、そしてデータ完全性について、徹底しています。DigiCert では、オンライン接続の保護という面で、長く経験豊かな歴史を誇っています。そこで、以下がIoT 導入を進める企業にとって、IoT のセキュリティを成功させる5つのベストプラクティスです。

1. **リスクを見直す：**接続デバイスに対するペネトレーション（侵入テスト）を実施し、リスクのアセスメント(評価) を行います。そして認証や暗号化などセキュリティの主要な懸念事項に対処するための優先リストを作成します。強力なリスクアセスメントによって、接続されたセキュリティ環境に漏れがないようにしておきます。

2. **すべてを暗号化する：**接続デバイスの使用方法を評価するにあたり、保管されたあるいは送信中のすべてのデータが暗号化されていることを確認します。エンドツーエンドの暗号化を製品の必須条件とすることで、すべてのIoT プロジェクトにこの重要なセキュリティ機能が導入されていることを確認します。

3. **常に認証する：**デバイスへのすべての接続を、デバイスとユーザーの両面から見直し、そして認証スキームが信頼できる接続だけを IoT デバイスに許可していることを確認します。電子証明書を使うことで、暗号プロトコルの利用と個体の認証を同時に提供します。

4. **完全性の実装：**デバイスとデータの完全性の基本として、デバイス起動時には常にセキュアブートを実行し、OTA（オン・ザ・エアー：オンラインで常に最新に）アップデートを行うことで安全を保ち、そしてコードサイニングを使用することによりデバイス上で実行されるすべてのコードの完全性を確保するようにします。

5. **拡張性を考量して戦略を立てる：**IoT 導入をサポートできる拡張性があるセキュリティフレームワークとアーキテクチャがあることを確認します。それに応じて計画を立て、そしてその目標達成を助けられるだけの規模と専門知識を持ったサードパーティの協力を仰ぎ、自社本来の業務に集中できるようになります。