DIGITAL HEARTS

産業分野別、企業の経営戦略と IT 活用

サイバーセキュリティ対策の動向調査

Research Report 2019

目次

はじめに

世界中で、デジタルトランスフォーメーション（DX）による、多様なIT テクノロジーをベースにしたビジネスモデルの変革が進んでいます。先進的なIT テクノロジーを駆使したデジタル製品やサービスが、短い周期で市場に投入／浸透し、競争の激化をもたらしています。ユーザーの購買活動は対面で行う人的サービスから時間の制約がないweb 利用へと場を移し、販売モデルも売り切りから継続性のあるサブスクリプション契約へと移行しています。このようなビジネス環境では、高品質な商品を長期で安定的に提供する従来のビジネスに加え、顧客のニーズが顕在化する前にその要素を組み入れた新サービスを投入し続けねばなりません。

この世界的なビジネス潮流の変化に加え、日本は他国に先立ち高齢化社会を迎えており、労働人口の不足など実にさまざまな対応を迫られています。人手を介さずに絶えず受発注を行うweb ベースのオンラインサービス拡大も、提供者側の都合と社会的な需要が合致した一つの例と言えます。これに伴い、システム連携による決済や、利用者属性と行動／購買情報、そして自社やグループ全体における需給／経営管理に至るまで、データ活用の範囲が急速に拡大しています。これまで企業は、IT 部門と事業部門に分かれて、IT システムの導入／運用と、ビジネス企画／展開を進めてきました。しかし、これからの商品／サービス開発や、その市場展開にIT 活用は不可欠です。そのため多様なデータを複層的に活用するデジタルサービスの展開では、企画運営する事業部門が主体となって、IT をベースにしたビジネス拡大とセキュリティ対策に取り組まねばなりません。

IT と通信によるあらゆるつながりが、ビジネスを醸成するスマート社会（Society5.0）では、自社資産と顧客を守るセキュリティ対策も、経営戦略の一部として認識する必要があります。日本企業が積極的に取り組むグローバルビジネスの場では、主要企業がすでにその認識を持ち対策を実践しています。今後は、ユーザーに安心で快適なサービスの利用経験を提供することが、競争力の源泉となるのです。そのため、経営者がIT とセキュリティのリテラシーを高め、全社あるいはサプライチェーン全体にガバナンスを発揮することで、顧客の信頼に基づく盤石なビジネス基盤を構築することができます。

国内企業にとって、事業強化と省力化などを目指すIT 活用、また企業全体における横断的なデータ活用に加え、脅威を増すサイバーセキュリティ対策が喫緊の課題となっています。

これらの背景と現状確認のために、デジタルハーツは「経営とIT 戦略、サイバーセキュリティ対策に関する企業動向」を調査しました。その結果を、主に企業経営やビジネスを企画運営する事業部門の方々に向け、本調査レポートにてご報告いたします。ぜひ、今後の参考としてご活用ください。

調査概要

本調査レポートは、デジタルハーツが 2019 年 6 月に実施した「経営と IT 戦略／サイバーセキュリティ対策の動向調査」において、国内企業の取り組みや課題、IT 活用とセキュリティ対策の実態を調査、分析したものである。

調査の目的

本調査レポートは、企業の IT 活用とセキュリティ対策を軸に、業績動向なども踏まえながら、回答企業の対策レベルや危機意識を確認し、今後の取り組みまで幅広く状況を把握することを目的とした。なお調査内容は、全体回答に加え、11 種類の産業分野別／業績別に集計および分析を行った。

調査方法

本調査は、国内企業および官公庁や各種団体を対象に実施した。1 社 1 回答となるように精査し、計 703 人からの回答を得た。調査は web アンケート形式で、下記の条件（立場）に当てはまる人物に協力を依頼した。

・経営および事業戦略の策定／推進／担当者で、IT 戦略も把握している方
・IT 戦略や IT 部門およびセキュリティ担当者で、事業戦略も把握している方

調査項目

本調査は回答企業／回答者の属性確認と、本調査に分けて実施した。属性確認では、回答企業の産業分野と規模、回答者の立場と所属および役職を把握し、本調査において経営戦略や業績推移、IT 活用とセキュリティ対策について詳細調査を実施した。

記載内容に関する留意点

本調査レポートにおける留意点は、下記の通りである。
・本調査レポートでは、年商規模 10 億円以上および従業員規模 10 人以上を調査対象とした。
・本調査レポート掲載の数値は、四捨五入した結果であり、合計値と一致しない場合がある。

回答企業と回答者の属性

回答企業の属性

回答企業は、従業員 500 人以上が 67.9%、年商 100 億円以上が 72.0%で、中堅規模以上の企業が中心である。

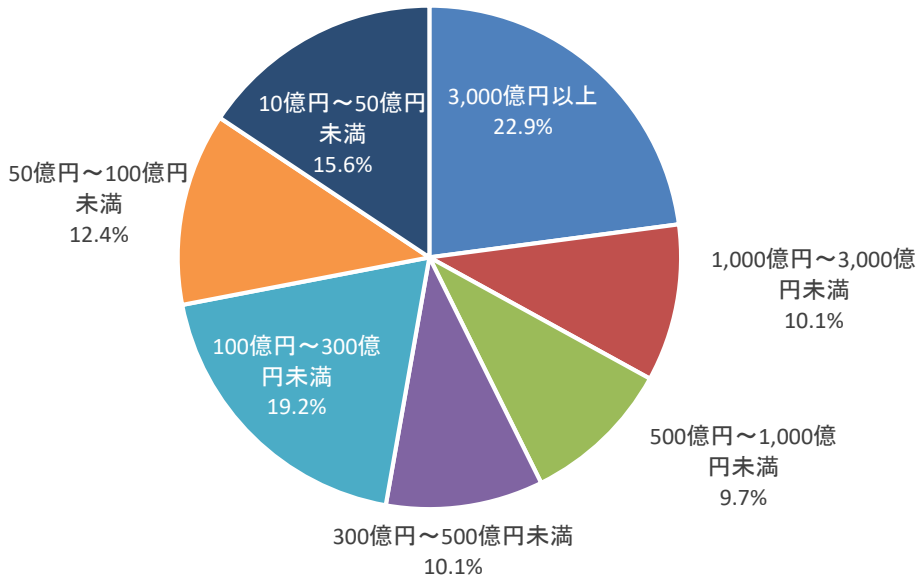
Table 1　産業分野別、従業員規模の分布

Note：回答数（%）

	全体	10,000人以上	5,000人～10,000人未満	3,000人～5,000人未満	1,000人～3,000人未満	500人～1,000人未満	300人～500人未満	100人～300人未満	50人～100人未満	10人～50人未満
全体(n=703)	100.0	17.1	8.7	7.5	18.8	15.8	8.3	16.5	5.0	2.4
製造(n=210)	100.0	22.9	6.2	8.1	15.2	20.5	6.7	15.7	2.9	1.9
金融(n=65)	100.0	26.2	15.4	12.3	16.9	13.8	9.2	4.6	0.0	1.5
流通／小売(n=79)	100.0	6.3	6.3	3.8	16.5	13.9	8.9	26.6	11.4	6.3
通信／メディア(n=28)	100.0	42.9	14.3	3.6	7.1	0.0	3.6	17.9	7.1	3.6
運輸／運輸サービス(n=29)	100.0	24.1	13.8	3.4	20.7	6.9	3.4	20.7	3.4	3.4
サービス(n=73)	100.0	6.8	6.8	6.8	21.9	15.1	8.2	23.3	8.2	2.7
ITサービス(n=69)	100.0	8.7	4.3	8.7	33.3	18.8	4.3	17.4	4.3	0.0
建設／土木(n=40)	100.0	10.0	0.0	2.5	22.5	15.0	20.0	12.5	15.0	2.5
公共(n=19)	100.0	26.3	10.5	5.3	5.3	5.3	26.3	10.5	5.3	5.3
医療／福祉(n=28)	100.0	10.7	7.1	17.9	21.4	25.0	7.1	10.7	0.0	0.0
政府／教育(n=63)	100.0	12.7	20.6	7.9	20.6	12.7	7.9	14.3	1.6	1.6

Source：Digital Hearts, 2019

Figure 1　年商規模別の分布



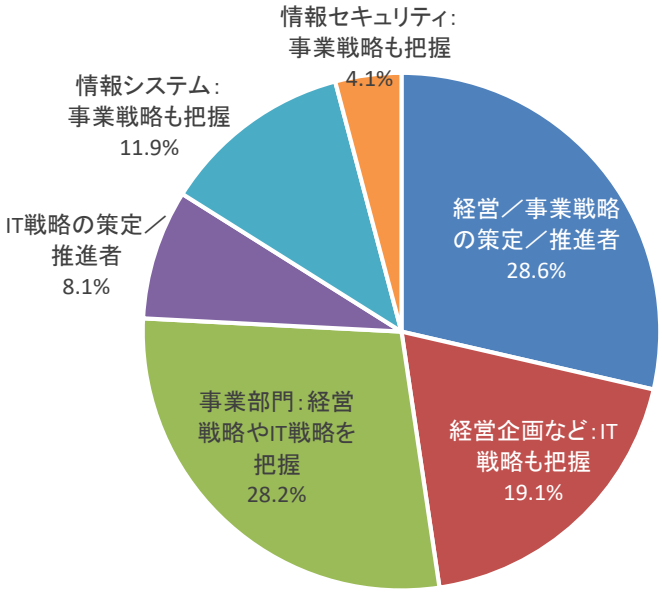
Note：回答数

Source：Digital Hearts, 2019

回答者の属性

主な回答者は、IT 部門以外の担当者（75.8%）で、課長以上が 68.4%（主任以上 88.1%）である。

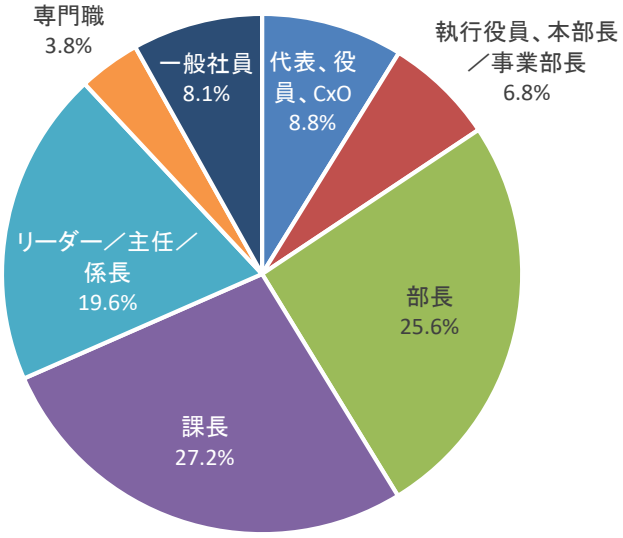
Figure 2　回答者の立場



Note：回答数

Source：Digital Hearts, 2019

Figure 3　回答者の役職



Note：回答数

Source：Digital Hearts, 2019

エグゼクティブサマリー

デジタルハーツは 2019 年 6 月に、官公庁を含む国内企業を対象に「経営と IT 戦略／サイバーセキュリティ対策の動向調査」を実施し、703 社の回答を得た。以下に、その集計と分析結果を報告する。

- グローバルビジネスが拡大しており、2018 年度の実績では、回答企業の 61.6%に海外売上がある。同年度の業績は、全体で前年比 5.0 ポイントの増加となり、通信／メディア（同 7.0 ポイント）と建設／土木（同 6.6 ポイント）を筆頭に、全産業で前年度より増加した。2019 年度の予想は、同 4.8 ポイントで依然として増加傾向を維持し、2020 年度には同 5.3 ポイントになるという回答結果を得た。なお、この期間を通じて 5%以上の業績増加を続けると回答した企業が 157 社（22.3%）おり、その海外売上比率は 88.5%と高く、海外ビジネスに成長軸がある様子を示している。

- 経営戦略として、全体的に最も注力するのは「新商品やサービス開発の強化」と「新規顧客の獲得」だが、製造はさらにグローバルビジネスを強化し、金融や建設／土木などいくつかの産業では新規顧客の獲得に注力すると回答している。なお、新製品の開発やグローバルビジネス強化によって、直接的に収益増強に注力する傾向が、5%以上の業績増加企業に特に強く表れていた。

- 経営戦略に必要な IT テクノロジーとして、最も回答率が高いのは「AI（人工知能、16.4 ポイント）」と、「IoT（16.3 ポイント）」である。その他、上位にランクインしたのは、「クラウド（15.1 ポイント）」と、「ビッグデータ分析（14.4 ポイント）」など、主にデータの収集と解析／共有といった、Society5.0 の実現に必要とされる IT テクノロジーが占めている。また各種の web サービスが、顧客や取引先あるいは自社業務に至る、幅広い用途で利用されており、重要なビジネスインフラとして普及している。各用途における準備／検討中の回答も一定数あり、さらなる需要増加が見込まれる。

- このような IT 活用を行う上で、最も深刻な課題かつ外部支援を要するものとして挙がったのは「サイバーセキュリティ対策」である。だが回答者の認識とは別に、本当に深刻なのは、IT リテラシーや人材不足という根本的な課題であり、高度なセキュリティ対策やデジタルトランスフォーメーション（DX）以前の IT 活用そのものに、IT サプライヤーの積極的な支援を必要とする国内企業の状況を、改めて明白にした。

- 「サイバー攻撃に対する脅威」には、33.6%が Level.5 の「非常に強い危機意識」を持っており、同 29.4%の「プライバシー情報の流出」よりも深刻に捉えている。危機意識を持つ理由の多くは、実害よりも自社対策や被害想定に対する確証のない不安であった。これは、現状の対策でよいのか、第三者による検証が必要な状況を表している。産業分野別では、両者に対する「非常に強い危機意識（Level.5）」の回答率が高いのは通信／メディアで、金融と政府／教育がこれに続いている。その一方で、流通／小売、運輸／運輸サービス、医療／福祉の危機意識が、他より低い傾向にあることが明らかとなった。

- サイバー攻撃やプライバシー情報の流出に対する「危機意識」と、5 段階の「セキュリティ対策レベル（利用ツールやルールの共有範囲による分類）」を比較してみた結果、総じてセキュリティ対策レベルが低いほど危機意識は高くなり、自社状況に対する危機感を認識していることを表していた。

- 「セキュリティ対策レベル」の全体平均は、現状が 2.2 ポイントであり「標準化」の段階をやや上回っている。3 年後の目標は 3.1 ポイントで「可視化」の段階になる。産業分野別では、医療／福祉の現状が平均 1.8 ポイント、3 年後の目標も平均 2.5 ポイントで、全産業中で最も低い結果を示している。また、現状の平均レベルが最も高いのは、通信／メディア（2.6 ポイント）である。前述の危機意識も含め、大規模な個人情報を管理し、安定した通信サービスを提供するための努力の結果が対策レベルにも反映されている。

- 第三者による客観的な指標となる 4 種類のセキュリティテスト（脆弱性診断、ペネトレーションテスト、ダーク web の情報漏えい調査、セキュリティ監査／アセスメント）は、回答企業全体の 78.4%（551 社）が、いずれかのセキュリティテストを実施／検討している。一般認知の進んでいる「脆弱性診断」は 66.4%で、金融や IT サービスを始めとした過半数以上に実施経験がある。実施率の低い医療／福祉でも、25.0%が今後の取り組みとして検討している。その他の実施率は、「ペネトレーションテスト」が 57.0%、「ダーク web の情報漏えい調査」が 48.2%、「セキュリティ監査／アセスメント」が 50.1%であった。その理由は「セキュリティ被害に遭った」と「他社の被害ニュース（市場動向）」が 33.0%でトップであった。また社外の専門スキルを持つ人材活用として、「バグバウンティ」の利用について調査したところ、27.5%に利用経験があり、医療／福祉の 39.3%、製造の 33.8%がすでに利用していた。医療／福祉は従来型の人的支援なのか、テクノロジーベースのサービスか、その事業内容次第で、IT とセキュリティ対策に大きな差があることを示している。

- サイバーセキュリティ対策における各項目の必要性では、脆弱性診断の実施率が示す通り、状況把握に対する需要が他の項目よりも高い。これに次いで、コンプライアンスやガイドラインの適合状況に対する必要性も感じている。しかし、同業者の水準を知りそれを対策に生かす点では、企業による考え方やリテラシーの差が回答にも反映されている。

- 積極的な海外展開を図り、業績の増加傾向を維持する企業は、各種の脅威に対する危機意識がその他の業績企業よりも高く、サイバーセキュリティ対策の必要性と、その効果がビジネスにもたらす影響に気づいている。攻撃対象となりやすいのは、金融や政府、通信／メディアに限ったことではない。今後は、攻撃を受けることを前提に、守るべき情報やシステムを特定し、被害の最小化とビジネスを止めない仕組みをセキュリティ対策においても検討すべきである。

これからの IT と通信による、あらゆるデジタルなつながりがビジネスを醸成するスマート社会では、IT テクノロジーをベースにした新領域の市場が多数形成される。その利用において、ユーザー側の IT リテラシーや情報セキュリティ意識が向上している。これからのサービス選定では、提供内容と並び高度な情報セキュリティが重視される。そのため、経営者はこれまで以上に IT とセキュリティのリテラシーを高め、全社あるいはサプライチェーン全体にガバナンスを発揮することで、顧客の信頼に基づく盤石な事業基盤を構築できる。自社資産と顧客を守るセキュリティ対策は、ビジネス拡大に必要な IT 活用と同様に、経営戦略の一部として捉えるべきである。

概況

日本の企業（以下、国内企業）は、少子高齢化や労働力不足による国内市場の縮小懸念から、積極的な海外展開や、業務の自動化など、多方面でその対策を図っている。

世界では、多様なITテクノロジーの出現と通信環境の整備、その産物であるデジタル製品やサービスを日常的に活用するカルチャーがコンシューマー市場に浸透し、シェアリングエコノミー（Uberや Airbnbなど）のような新たなビジネスモデルが出現した。またエンタープライズ市場でも、自動運転や遠隔医療、各種交通や設備の制御とメンテナンスなどの取り組みで、主にインターネットを介して、サイバー空間と現実（フィジカル）世界の融合が進んでいる。国内では、東京オリンピック／パラリンピック開催を翌年に控え、各地で本格化に向けた動きを見せている。

今後は人手やインフラ不足が深刻な地域支援と同時に、国境も時差もないインターネット上で、精度の高い情報を武器に、より戦略的に「面」を取る効率的な経営が求められるようになる。この動向はさらに加速し、新たなITとデジタルによる経済圏を育成する。そのため、外部エコシステムである市場や顧客の動向に即した、デジタル製品やサービスの開発が急がれるが、その源泉となるデータ活用と、これを実現するIT活用に多くの企業が課題を感じている。また情報保護の領域では、国内法やEU圏でのGDPR（General Data Protection Regulation：一般データ保護規則）などのガイドライン対応にも配慮が必要だ。データ活用時代における経営では、戦略の実現にIT活用とセキュリティ対策を度外視することはできない。

これらの背景と実態把握に、デジタルハーツでは、2019年6月に官公庁を含む国内企業を対象とした「経営とIT戦略／サイバーセキュリティ対策の動向調査」を実施し、703社の回答を得た。主にビジネスを推進する回答者を対象に調査した結果を、産業分野や業績別に分析し、見解も含め報告する。

Table 2に示したように、グローバルビジネスが拡大しており、2018年度の実績では、回答企業の61.6%に海外売上がある。海外売上比率の上位は製造が81.9%、金融が67.7%、流通／小売が60.8%である。また図解は省くが、年商規模で見ると1,000億円以上（n=232）の75.9%、100～1,000億円未満（n=274）の60.2%、100億円未満（n=197）の46.7%に海外売上があり、年商規模が上がるに従い高い海外売上比率を示している。

Figure 4に、産業分野別の業績の増減ポイントを示す。2018年度の実績は、全体で前年比5.0ポイントの増加となり、通信／メディア（同7.0ポイント）と建設／土木（同6.6ポイント）を筆頭に、全産業で前年より増加した。2019年度は、同4.8ポイントで依然として増加傾向を維持し、2020年度には同5.3ポイントになるという回答結果を得た。2018年度～2020年度で見ると、2018年度に好業績だった通信／メディア、建設／土木、運輸／運輸サービスで、増加傾向は維持するものの、緩やかな伸びとなる業績予想を示している。また、この期間を通じて常に5%以上の業績増加を維持すると回答した企業が157社（22.3%）おり、その海外売上比率は88.5%と高く、海外ビジネスに成長軸がある様子を示している。

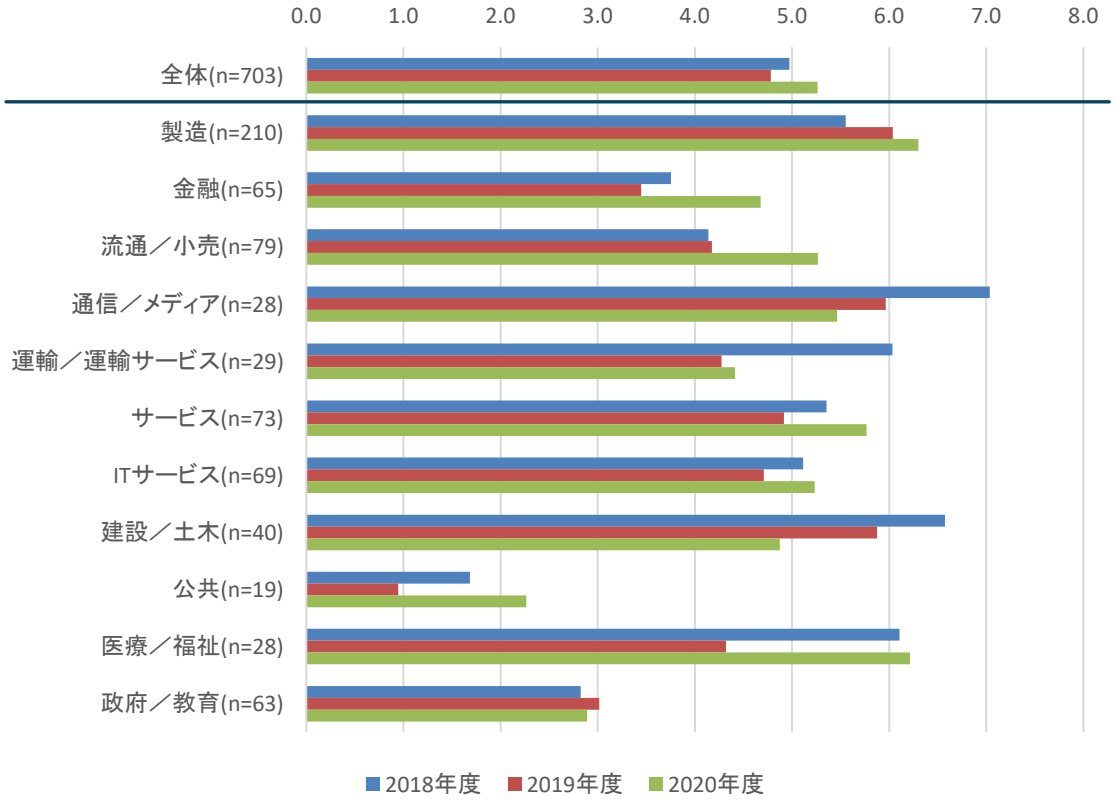
Table 2　産業分野別、海外売上比率

	全体	50%以上	30%～50%未満	20%～30%未満	10%～20%未満	5%～10%未満	5%未満	なし
全体(n=703)	100.0	7.0	8.8	8.1	8.1	16.5	13.1	38.4
製造(n=210)	100.0	12.4	18.1	12.9	10.0	17.1	11.4	18.1
金融(n=65)	100.0	3.1	7.7	6.2	9.2	26.2	15.4	32.3
流通／小売(n=79)	100.0	3.8	5.1	8.9	12.7	17.7	12.7	39.2
通信／メディア(n=28)	100.0	0.0	3.6	7.1	7.1	7.1	21.4	53.6
運輸／運輸サービス(n=29)	100.0	0.0	6.9	6.9	3.4	13.8	17.2	51.7
サービス(n=73)	100.0	5.5	2.7	6.8	8.2	11.0	19.2	46.6
ITサービス(n=69)	100.0	4.3	4.3	4.3	5.8	18.8	14.5	47.8
建設／土木(n=40)	100.0	10.0	7.5	5.0	5.0	20.0	10.0	42.5
公共(n=19)	100.0	0.0	5.3	0.0	5.3	26.3	15.8	47.4
医療／福祉(n=28)	100.0	7.1	3.6	14.3	7.1	10.7	3.6	53.6
政府／教育(n=63)	100.0	7.9	3.2	1.6	3.2	9.5	7.9	66.7

Note：回答数（%）

Source：Digital Hearts, 2019

Figure 4　産業分野別、業績推移：2018 年度（実績）～2020 年度（予想）



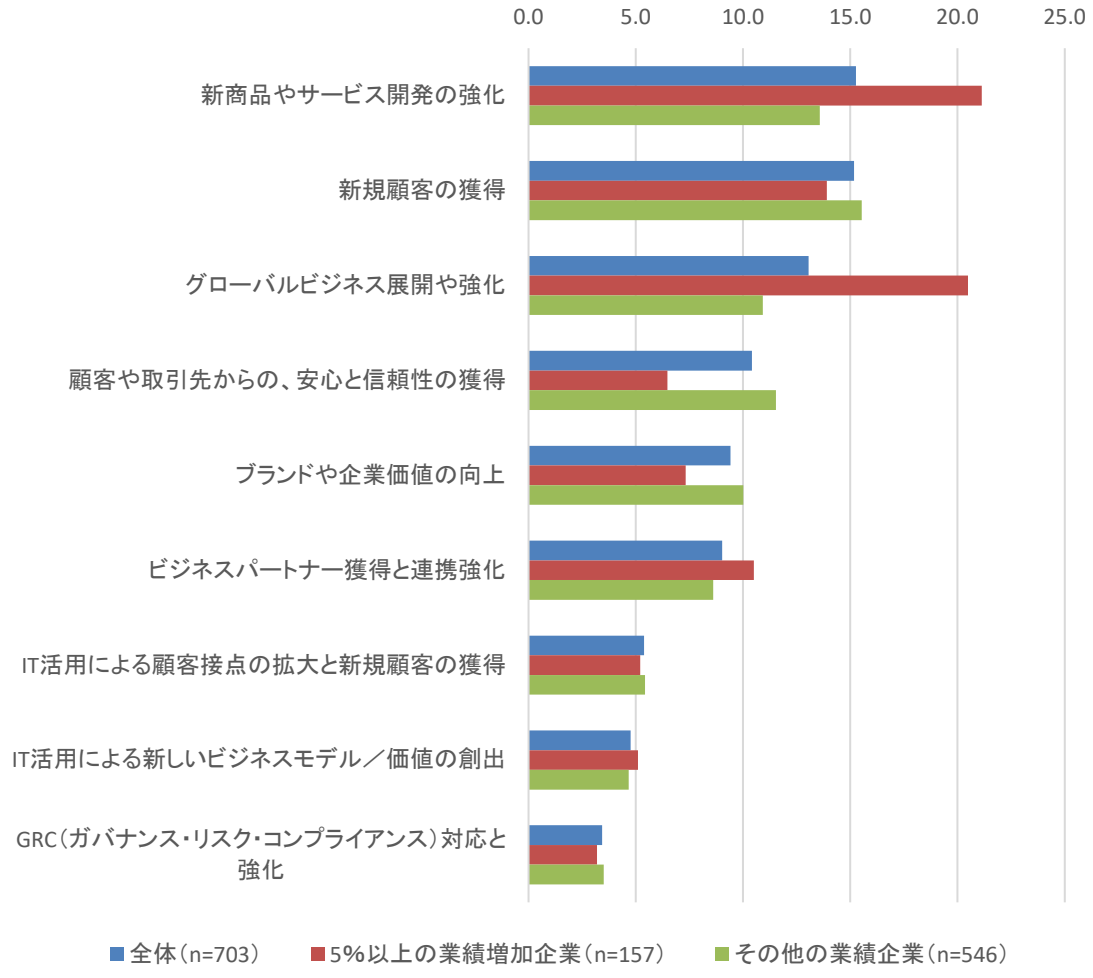
Notes：　・回答率（ポイント）
・前年比 20%～-20%の回答を、20～-20 のポイントに置き換え、加重平均値を算出した
・2018 年度は 2017 年度と比較した実績値、2019 年度以降は 2018 年度をベースにした予想値

Source：Digital Hearts, 2019

経営戦略と IT 活用、課題

Figure 5 に、経営戦略／課題対応として注力する内容を調査した結果を、業績別に示す。Figure 5 の並び順は、全体（n=703）の回答ポイントが高い順だが、2018 年度から 2020 年度で 5%以上の業績増加を続けると回答した企業（n=157）と、その他の業績企業（n=546）の回答も比較のために併記する。企業は常に、事業強化のための施策に取り組み、新規顧客を開拓、そして獲得した顧客の維持に注力することを繰り返す。今の状況としては、直接的に収益増強に注力する言わば「攻め」の傾向が、特に 5%以上の業績増加企業に特に強く表れている。また Table 3 に、産業分野別の集計結果を示す。全体では、最も注力する項目は「新商品やサービス開発の強化」と「新規顧客の獲得」だが、製造はさらにグローバルビジネスを強化し、金融や建設／土木などいくつかの産業では新規顧客の獲得と回答している。

Figure 5　業績別、経営戦略／課題対応の注力上位項目：1 位～3 位



Notes:　・回答率（ポイント）
・1 位～3 位の回答を、3～1 のポイントに置き換え、加重平均値を算出した
・下位の項目：労働力確保と CS 向上、IT 人材確保、情報活用経営（いずれも 3.2 以下）
・業績別は、2018 年度（実績）～2020 年度（予想）期間における、5%以上増加企業（n=157）とその他（n=546）に分けて集計した

Source：Digital Hearts, 2019

Table 3　産業分野別、経営戦略／課題対応の注力項目：1 位～3 位

	新商品やサービス開発の強化	新規顧客の獲得	グローバルビジネス展開や強化	顧客や取引先からの、安心と信頼性の獲得	ブランドや企業価値の向上	ビジネスパートナー獲得と連携強化	IT 活用：顧客接点の拡大と新規顧客の獲得	IT 活用：新しいビジネスモデル／価値の創出	GRC 対応と強化	労働力の確保と従業員の満足度向上	IT 人材：獲得、育成、ビジネス参画の促進	経営の意思決定に必要な社内外の情報活用	その他	ない
全体 (n=703)	15.3	15.2	13.1	10.4	9.4	9.0	5.4	4.8	3.4	3.2	3.1	2.8	3.2	1.7
製造 (n=210)	19.2	14.1	20.8	7.2	9.4	9.3	5.6	4.0	1.9	1.6	2.2	2.1	1.7	0.7
金融 (n=65)	14.1	20.3	8.5	12.6	12.6	8.2	3.1	6.4	5.1	2.8	1.3	2.6	1.5	1.0
流通／小売 (n=79)	15.0	17.3	13.5	9.7	10.3	6.8	7.0	4.2	2.5	3.2	1.9	2.7	4.6	1.3
通信／メディア (n=28)	17.3	17.9	1.2	12.5	6.5	8.3	8.9	6.5	3.6	1.8	4.2	2.4	7.1	1.8
運輸／運輸サービス (n=29)	7.5	17.2	5.7	16.1	14.4	3.4	4.6	1.1	4.0	9.2	4.0	4.0	6.9	1.7
サービス (n=73)	16.2	14.6	10.5	9.4	10.5	8.4	3.9	4.1	3.0	4.8	2.7	4.1	4.8	3.0
IT サービス (n=69)	13.0	11.8	11.6	11.6	4.6	12.6	8.0	8.2	1.4	1.7	8.9	2.2	2.9	1.4
建設／土木 (n=40)	10.4	19.2	7.1	14.6	8.3	11.3	3.8	2.1	7.5	4.2	2.5	2.5	5.0	1.7
公共 (n=19)	13.2	14.9	14.9	9.6	10.5	10.5	0.9	4.4	4.4	2.6	3.5	4.4	5.3	0.9
医療／福祉 (n=28)	10.7	16.1	8.3	13.1	5.4	9.5	6.0	4.8	5.4	6.5	3.0	4.2	1.8	5.4
政府／教育 (n=63)	13.5	10.1	10.1	12.4	10.1	9.5	4.8	5.8	6.6	4.8	2.6	4.0	2.4	3.4

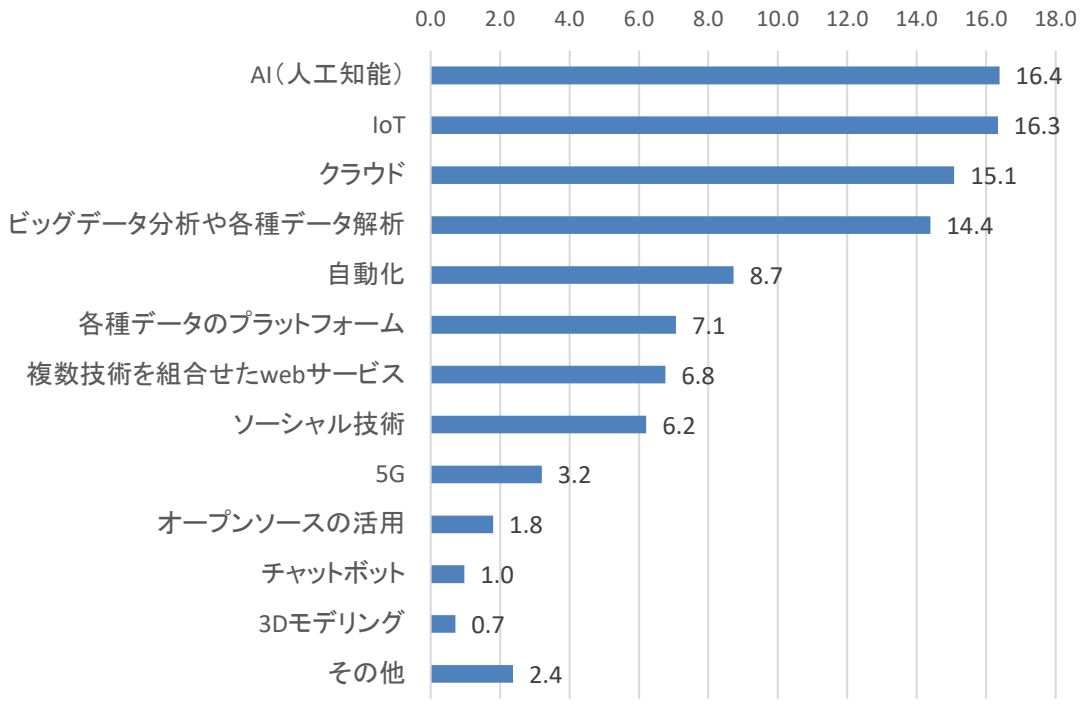
Notes:　・回答数（ポイント：集計方法は Figure 5 と同じ）
・GRC：ガバナンス・リスク・コンプライアンス
・その他の回答：製品強化、コンプライアンス準拠、顧客対応の強化、競争優位性の確保など

Source：Digital Hearts, 2019

Figure 6 に、経営戦略の実現に必要な IT テクノロジーを調査した結果を示す。「AI（人工知能、16.4 ポイント）」と、「IoT（16.3 ポイント）」に加え、上位にランクインしたのは、「クラウド（15.1 ポイント）」と、「ビッグデータ分析（14.4 ポイント）」など、主にデータの収集と解析／共有といった、サイバーとフィジカルが融合したスマート社会（Society5.0）の実現に必要とされる IT テクノロジーが占めている。

現状、経営課題として注力する内容は市場獲得と競争力強化だが、さらなるビジネスの拡大と、マスカスタマイゼーションなどの個々の顧客の満足度向上に IT 活用は欠かせない。冒頭に述べたように、近年は、収益モデルが「物販」から「サービス料金」へと変化しており、継続的な顧客との関係性を支える IT 活用によるサービス化が、業種を問わず検討されている。また、日本の GDP（国内総生産）に占めるデジタル製品やサービスの効果に関する調査報告*にあるように、企業の事業強化には DX 推進は不可欠な要素であり、継続的に新たなビジネスモデルを創出し事業強化を図る必要がある。しかし現状は、業務の省力化や効率化など、目の前の課題対応に IT テクノロジーを採用するケースが多く、今回の調査回答に挙げられた IT 活用がどのように進むのか、今後の同業他社の差別化に向けた動向に注視すべきだろう。次項では、拡大する web ベースのサービス利用や提供内容などを確認する。

Figure 6　経営戦略／課題対応に必要な IT テクノロジー：1 位～3 位



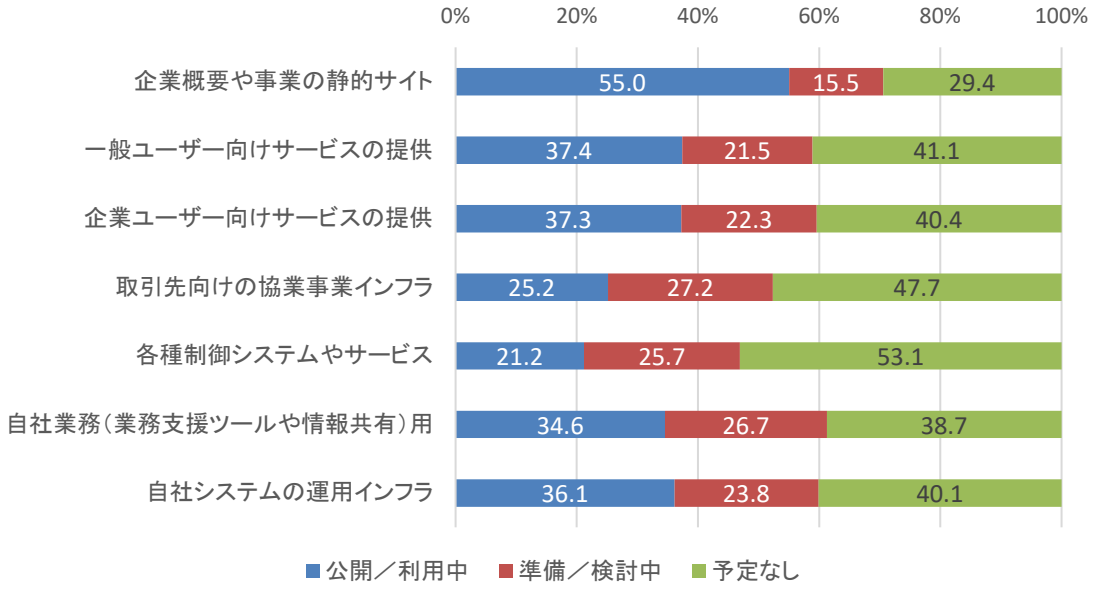
Notes：　・回答率（ポイント）
・1 位～3 位の回答を、3～1 のポイントに置き換え、加重平均値を算出した
・その他の回答：AI とセキュリティ、目的に適した IT が不明など

Source：Digital Hearts, 2019

*マイクロソフト社のプレスリリース：https://news.microsoft.com/ja-jp/2018/02/20/180220-idc-digital-transformation-asia/

Figure 7 に、業務の効率化などで事業部門での活用が拡大する web サービスなどの利用／提供の状況、Table 4 にサービス内容を示す。各種の web サービスが、顧客や取引先あるいは自社業務用に至る、幅広い用途で利用されており、重要なビジネスインフラとして普及している様子を表している。各用途における準備／検討中の回答も一定数あり、さらなる需要増加が見込まれる。産業分野別の集計結果は省略するが、公共が今後の対外的な情報公開や一般／企業向けサービス提供に意欲的であり、建設／土木も企業ユーザー向けサービスを、サービス業は取引先向けの協業インフラを検討している。

Figure 7　web サービスや情報管理の利用／提供状況



Note:　・n=703

Source：Digital Hearts, 2019

Table 4　利用／提供している web サービスの種類

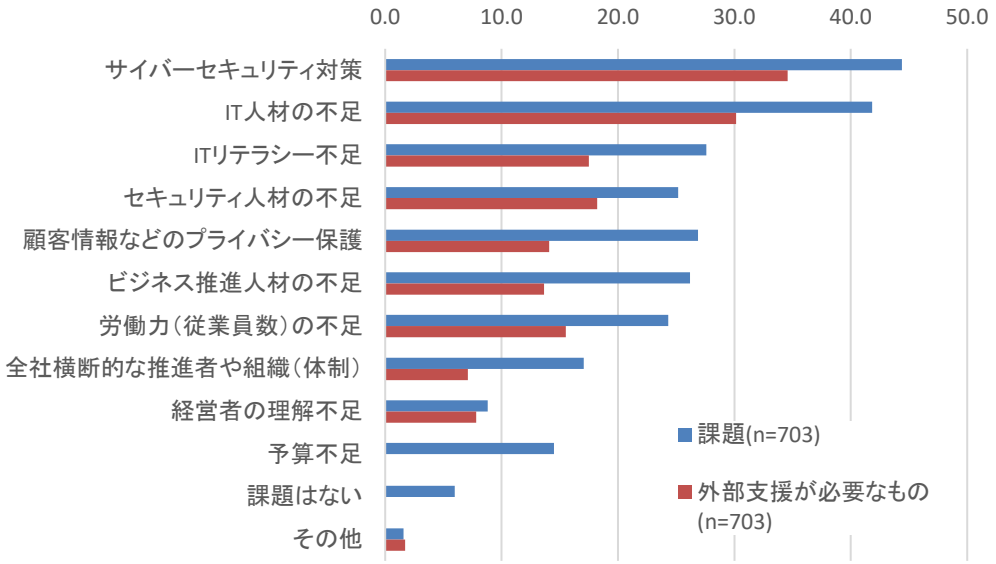
	金融関連（決済、オンラインバンキング）サービス	製造関連システムやサービス	ECなど流通（小売り）関連システムやサービス	情報サイト／ブログ／コンテンツ配信のメディア関連システムやサービス	通信関連システムやサービス	公共／エネルギー関連のシステムやサービス
利用（n=703）	39.5	23.9	26.6	28.2	23.0	18.9
提供（n=703）	11.1	11.1	13.8	15.8	10.1	9.1
	運輸関連のシステムやサービス	医療関連のシステムやサービス	教育関連のシステムやサービス	経費や人事管理の業務関連システムやサービス	CRMや社内SNSなど情報共有のシステムやサービス	利用／提供していない
利用（n=703）	16.4	12.9	15.5	25.9	22.8	21.2
提供（n=703）	8.1	6.1	7.1	6.0	5.8	45.7

Note:　・回答率（%）

Source：Digital Hearts, 2019

Figure 8 に、IT 活用を進める上での課題と外部支援を要するものについて調査した結果を、Table 5 に、産業分野別に集計した結果を示す。最も深刻な課題かつ外部支援を要するのは「サイバーセキュリティ対策」である。だが課題としてそこまで認識していなくとも、本当に深刻なのは、IT リテラシーや人材不足という根本的な問題である。国内企業の IT 活用そのもののレベルが依然未成熟であり、革新的なビジネスを生み出す DX の取り組みや、高度なセキュリティ対策などに支障が生じるため、差別化や競争力で諸外国に後れを取ることになる。IT サプライヤーの積極的な支援を必要とする国内企業の状況を、改めて明白にしたと言えよう。

Figure 8　IT 活用を進める上での課題、外部支援が必要なもの



Notes:　・複数回答、回答率（%）
・その他：経営陣の刷新、業績の改善、人員配置の変更、意思疎通など

Source：Digital Hearts, 2019

Table 5　産業分野別、IT 活用を進める上での課題

	サイバーセキュリティ対策	顧客情報などのプライバシー保護	ITリテラシー不足	IT人材の不足	セキュリティ人材の不足	ビジネス推進人材の不足	労働力（従業員数）の不足	全社横断的な推進者や組織（体制）	予算不足	経営者の理解不足
全体(n=703)	44.4	26.9	27.6	41.8	25.2	26.2	24.3	17.1	14.5	8.8
製造(n=210)	46.2	29.0	31.9	44.3	27.6	29.0	19.0	18.1	14.8	10.0
金融(n=65)	50.8	41.5	30.8	40.0	30.8	21.5	16.9	13.8	10.8	4.6
流通／小売(n=79)	40.5	21.5	20.3	45.6	20.3	31.6	24.1	16.5	7.6	12.7
通信／メディア(n=28)	42.9	35.7	21.4	42.9	28.6	28.6	17.9	25.0	17.9	7.1
運輸／運輸サービス(n=29)	48.3	34.5	20.7	34.5	27.6	20.7	41.4	24.1	10.3	13.8
サービス(n=73)	34.2	24.7	27.4	45.2	28.8	28.8	31.5	20.5	11.0	4.1
ITサービス(n=69)	42.0	24.6	30.4	56.5	21.7	29.0	29.0	13.0	11.6	8.7
建設／土木(n=40)	37.5	20.0	30.0	22.5	20.0	15.0	30.0	15.0	15.0	12.5
公共(n=19)	68.4	26.3	21.1	36.8	26.3	31.6	31.6	21.1	31.6	15.8
医療／福祉(n=28)	42.9	21.4	17.9	17.9	17.9	14.3	32.1	7.1	17.9	3.6
政府／教育(n=63)	47.6	15.9	27.0	38.1	20.6	20.6	22.2	15.9	27.0	6.3

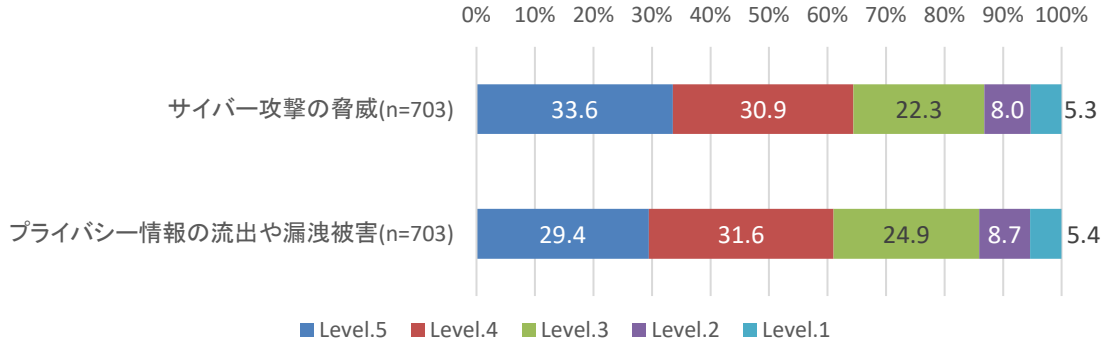
Notes:　・回答率（%）
・課題はない、その他を省略

Source：Digital Hearts, 2019

セキュリティ意識と対策

将来に及ぶ国内市場の縮小や労働力不足の懸念から、主要産業ではグローバルビジネスのさらなる拡大に注力している。海外におけるビジネスでは、規制対応やコンプライアンス、また日本の個人情報保護法とは異なるプライバシー保護が求められる。国内事業の強化を図る業界でも、今後のデータおよび通信／IT インフラ活用を推進する上で、もはやサイバー攻撃や情報漏えいなどの脅威は他人事ではない。関連する意識調査の結果を Figure 9～10 に示す。「サイバー攻撃に対する脅威」では、33.6%が Level.5 の「非常に強い危機意識」を持っており、同 29.4%の「プライバシー情報の流出」よりも深刻に捉えている。危機意識を持つ理由の多くは、実害を被ったことより、自社対策や被害想定に対する確証のない不安であった。つまり、現状の対策でよいのか、第三者による検証が必要な状況を表している。

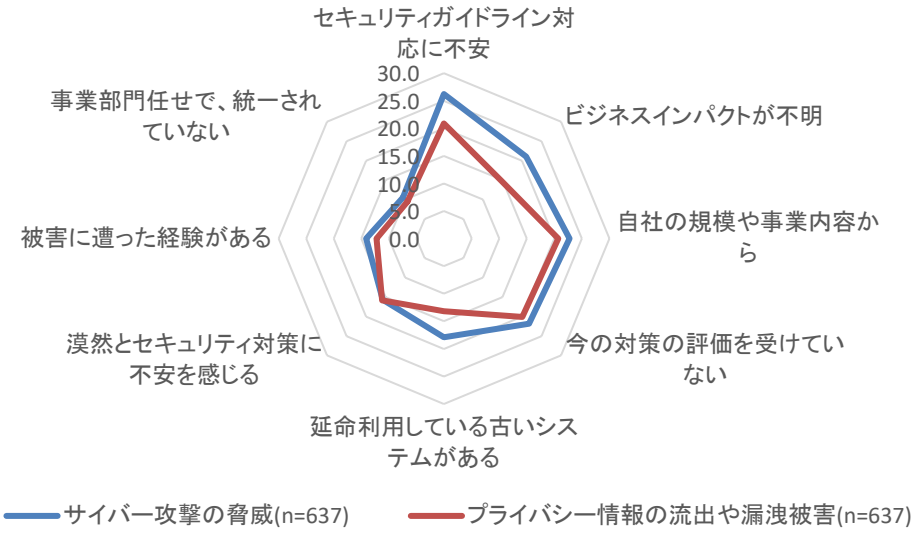
Figure 9　危機意識



Notes:　・回答率(%)
・Level:非常に強い危機意識＝Level5～危機意識はない＝level1

Source:Digital Hearts, 2019

Figure 10　危機意識を持つ理由（複数回答）

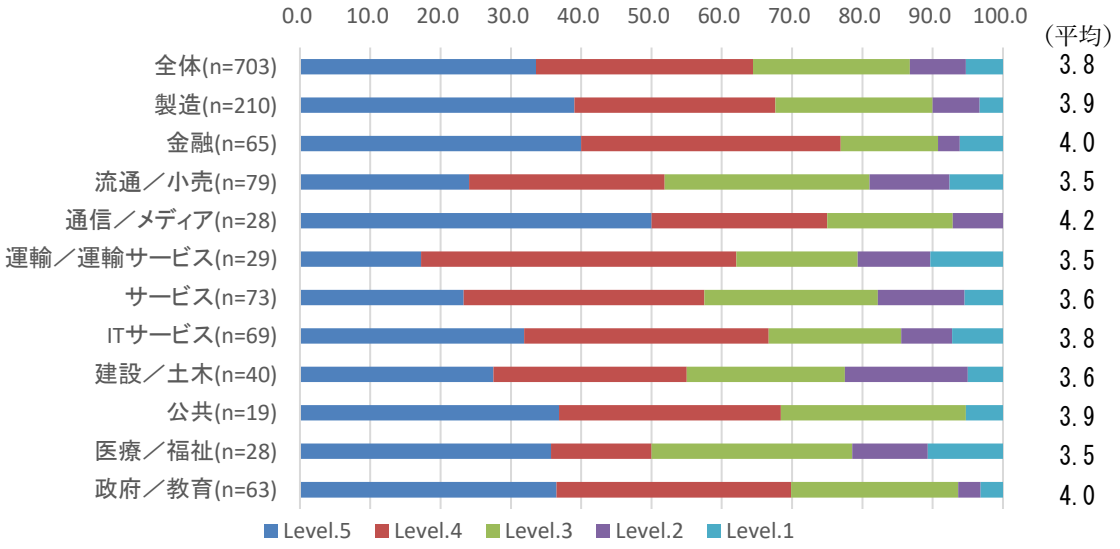


Notes:　・n=637、危機意識 Level.3 以上の回答率(%)

Source:Digital Hearts, 2019

Figure 11～12 に、産業分野別に集計したサイバー攻撃とプライバシー情報流出に対する危機意識を示す。両者に対する「非常に強い危機意識（Level.5）」の回答率が高いのは通信／メディアで、金融と政府／教育がこれに続いている。その一方で、流通／小売、運輸／運輸サービス、医療／福祉の危機意識が、他より低い傾向にあることが明らかとなった。参考値として、産業分野別に加重平均した結果を併記する。

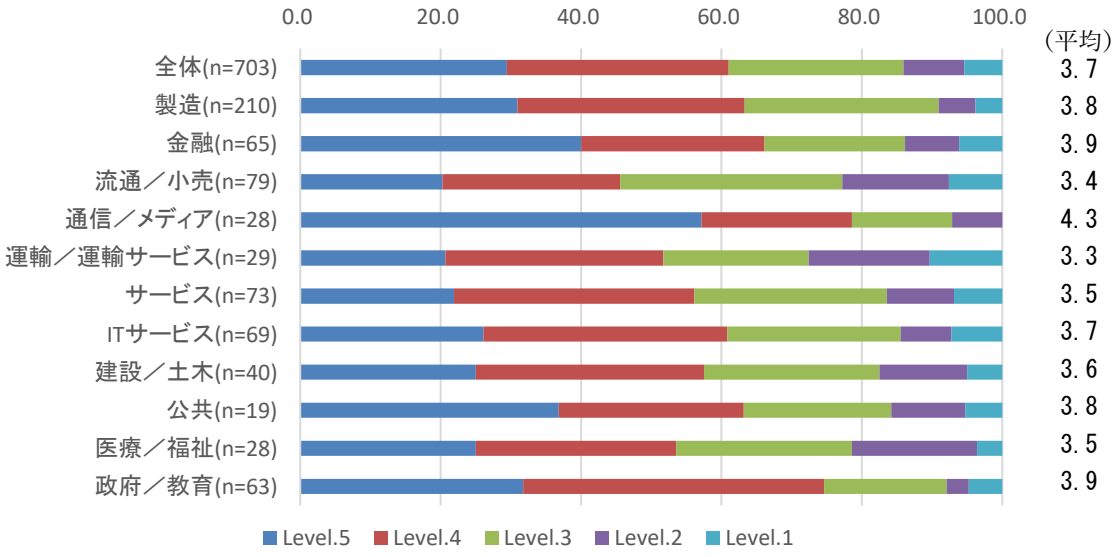
Figure 11　産業分野別、サイバー攻撃に対する危機意識



Note:　回答率（%）、Level:非常に強い危機意識＝Level5～危機意識はない＝level1

Source：Digital Hearts, 2019

Figure 12　産業分野別、プライバシー情報流出に対する危機意識

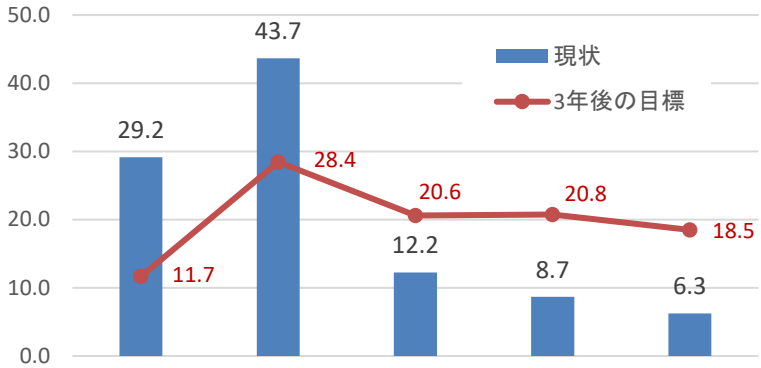


Note:　回答率（%）、Level:非常に強い危機意識＝Level5～危機意識はない＝level1

Source：Digital Hearts, 2019

Figure 13 は、前述の危機意識のレベルと、現状のセキュリティ対策レベルを比較してみた結果である。セキュリティ対策レベルは、利用ツールやルールの共有範囲と仕組みによる分類を行った。初歩的な「個別対応」段階にある企業では、最も高い危機意識の「level.5」を 41.5%が選んでいる。最も高度な対策レベル「最適化」にある企業では、最も低い危機意識の「level.1」が 27.0%という結果を示した。前述の通り、自社の状況に対する不安や安心が、危機意識と関連を見せている。また 3 年後のセキュリティ対策レベルの目標では、全体的に「標準化」の段階から、状況の「可視化」や「即時対応」段階へ取り組みの強化を図ろうとしている。しかし、3 年後は IT とデータ活用も今より複雑に高度化するはずであり、それらを踏まえたセキュリティ対策の強化には、経営者も含む全社横断的な取り組みが必要となる。

Figure 13　セキュリティ対策レベルと危機意識



		個別対応	標準化	可視化	即時対応	最適化
	全体(n=703)	29.2	43.7	12.2	8.7	6.3
危機意識	Level.5(n=236) 高	41.5	36.9	8.1	6.4	7.2
	Level.4(n=217) ↑	23.5	49.3	14.3	8.3	4.6
	Level.3(n=157) ↕	21.0	51.0	15.3	10.8	1.9
	Level.2(n=56) ↓	23.2	41.1	16.1	12.5	7.1
	Level.1(n=37) 低	27.0	27.0	8.1	10.8	27.0

セキュリティ対策の段階：

個別対応：業務や部署によって、異なるセキュリティ対策ルールや IT ツールを利用している

標準化：　社内で共通するセキュリティ対策ルールと IT ツールを利用している

可視化：　対策に必要なログ情報などを収集し、社内状況が IT で可視化できている

即時対応：自動的にリスク（可能性）を発見し、管理者と関係者にリアルタイムな情報共有と対処する仕組みがある

最適化：　社内外の環境変化を踏まえ、継続的にセキュリティ対策の最適化を図れる仕組みがある

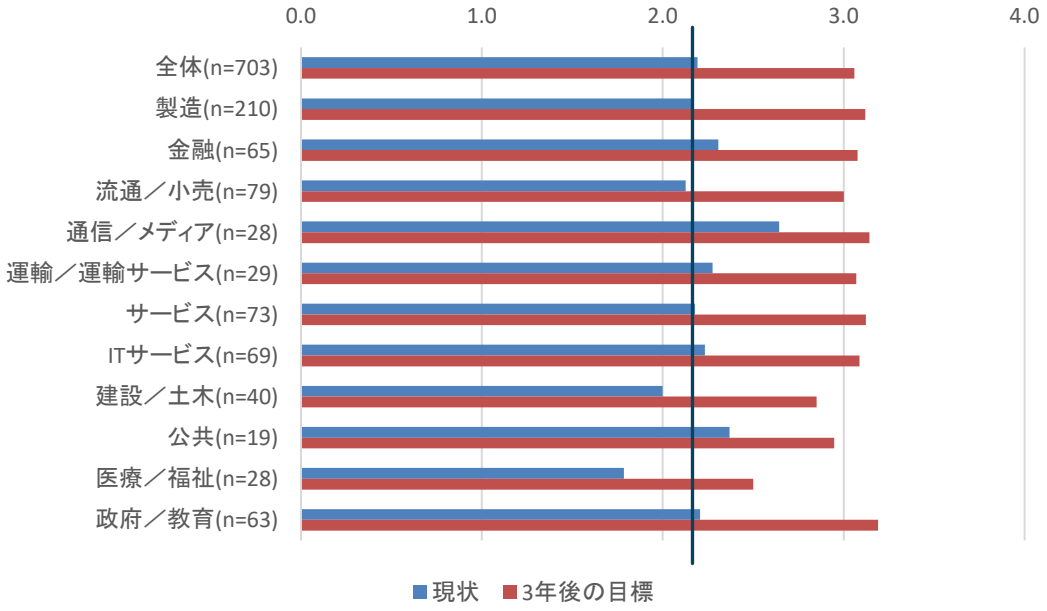
Notes:　・いずれも回答率(%)
・危機意識レベル:非常に強い危機意識＝Level5～危機意識はない＝level1

Source:Digital Hearts, 2019

セキュリティ対策には、企業を問わず共通する長年の課題がある。どこまで対策するのが正解なのか、または自社状況の対策の程度（十分か否か）が把握できないことである。一つの目安として、Figure 14 に、産業分野別のセキュリティ対策レベルの平均ポイント（現状と 3 年後の目標）を示す。

現状の全体平均は 2.2 ポイントで「標準化」の段階だが、3 年後の目標は 3.1 ポイントで「可視化」の段階である。産業分野別では医療／福祉が、現状 1.8 ポイント、3 年後の目標でも 2.5 ポイントと、全産業中で最も低い結果を示している。また、現状のレベルが最も高いのは、通信／メディア（2.6 ポイント）である。前述の危機意識も含め、大規模な個人情報を管理し、安定した通信サービスを提供するための努力の結果が対策レベルにも反映されている。

Figure 14　産業分野別、セキュリティ対策レベル平均値：現状／3 年後の目標



Notes:　・回答率（ポイント）
・平均値は Level1～5 の回答結果を加重集計してポイントを算出

Source：Digital Hearts, 2019

この対策レベルは、ツールやルールの共有範囲、仕組みによる分類だが、客観的な指標となるセキュリティ関連のテスト（以下、セキュリティテスト）の実施状況について調査した結果は次の通りである。

Table 6 に、4 種類のセキュリティテストの実施状況を、Figure 15 に、各種テストの産業分野別の実施頻度を示す。一般認知の進んでいる「脆弱性診断」は、金融や IT サービスを始めとして、66.4%と過半数以上に実施経験がある。実施率の低い医療／福祉でも、25.0%が今後の取り組みとして検討していた。その他の実施率は、「ペネトレーションテスト」が 57.0%、「セキュリティ監査／アセスメント」が 50.1%である。「ダーク web の情報漏えい調査」は、比較的新しい分野のセキュリティテストだが、全体で 48.2%、公共では 63.2%に実施経験があった。ダーク web は、インターネット（サーフェス web）の 500 倍ほどの情報量を持つと言われる。ここに自社の特権ユーザー（社員アカウント）や顧客情報がすでに流出していれば、侵入実績のある脆弱性の存在だけでなく、流出情報を悪用したサイバー攻撃によるさらなる被害が懸念される。非常に残念なことに、情報漏えいの被害を受けた企業／組織がこれに気づかず、数年間そのまま放置されるケースも珍しくない。これらは、第三者視点による自社状況の把握手段である。将来的な被害を防ぐためにも、脆弱性を早期発見する仕組みを取り入れるべきだろう。

Table 6　セキュリティテストの実施経験

	全体	年に1回以上、定期的に実施	リニュアル時など、不定期に実施	過去に実施したことがある	受けていないが、検討中	受けていない／予定もない	わからない
脆弱性診断	100.0	38.8	18.3	9.2	9.7	10.7	13.2
ペネトレーション（侵入）テスト	100.0	23.0	24.0	10.0	10.2	16.5	16.2
ダークwebへの情報漏洩調査	100.0	19.8	14.9	13.5	14.5	19.9	17.4
セキュリティ監査／アセスメント	100.0	26.9	13.1	10.1	17.2	18.2	14.5

Note:　・回答率（%）

Source：Digital Hearts, 2019

Figure 15　産業分野別、セキュリティテスト別の実施経験

脆弱性診断

	実施	検討中	予定なし	不明
全体(n=703)	66.4	9.7	10.7	13.2
製造(n=210)	69.5	6.2	11.9	12.4
金融(n=65)	81.5	4.6	1.5	12.3
流通／小売(n=79)	60.8	10.1	12.7	16.5
通信／メディア(n=28)	60.7	17.9	3.6	17.9
運輸／運輸サービス(n=29)	51.7	13.8	10.3	24.1
サービス(n=73)	54.8	12.3	15.1	17.8
ITサービス(n=69)	81.2	1.4	7.2	10.1
建設／土木(n=40)	70.0	10.0	12.5	7.5
公共(n=19)	63.2	10.5	10.5	15.8
医療／福祉(n=28)	46.4	25.0	14.3	14.3
政府／教育(n=63)	61.9	19.0	12.7	6.3

ペネトレーションテスト

	実施	検討中	予定なし	不明
全体(n=703)	57.0	10.2	16.5	16.2
製造(n=210)	58.6	11.9	15.2	14.3
金融(n=65)	75.4	9.2	3.1	12.3
流通／小売(n=79)	50.6	11.4	21.5	16.5
通信／メディア(n=28)	64.3	10.7	3.6	21.4
運輸／運輸サービス(n=29)	44.8	3.4	24.1	27.6
サービス(n=73)	49.3	8.2	21.9	20.5
ITサービス(n=69)	62.3	4.3	13.0	20.3
建設／土木(n=40)	50.0	10.0	22.5	17.5
公共(n=19)	52.6	10.5	21.1	15.8
医療／福祉(n=28)	46.4	14.3	25.0	14.3
政府／教育(n=63)	57.1	14.3	19.0	9.5

ダーク web の情報漏えい調査

	実施	検討中	予定なし	不明
全体(n=703)	48.2	14.5	19.9	17.4
製造(n=210)	50.5	15.2	20.5	13.8
金融(n=65)	56.9	20.0	9.2	13.8
流通／小売(n=79)	43.0	16.5	22.8	17.7
通信／メディア(n=28)	53.6	10.7	14.3	21.4
運輸／運輸サービス(n=29)	37.9	6.9	27.6	27.6
サービス(n=73)	42.5	15.1	20.5	21.9
ITサービス(n=69)	50.7	10.1	14.5	24.6
建設／土木(n=40)	50.0	7.5	25.0	17.5
公共(n=19)	63.2	0.0	21.1	15.8
医療／福祉(n=28)	50.0	17.9	21.4	10.7
政府／教育(n=63)	38.1	20.6	25.4	15.9

セキュリティ監査／アセスメント

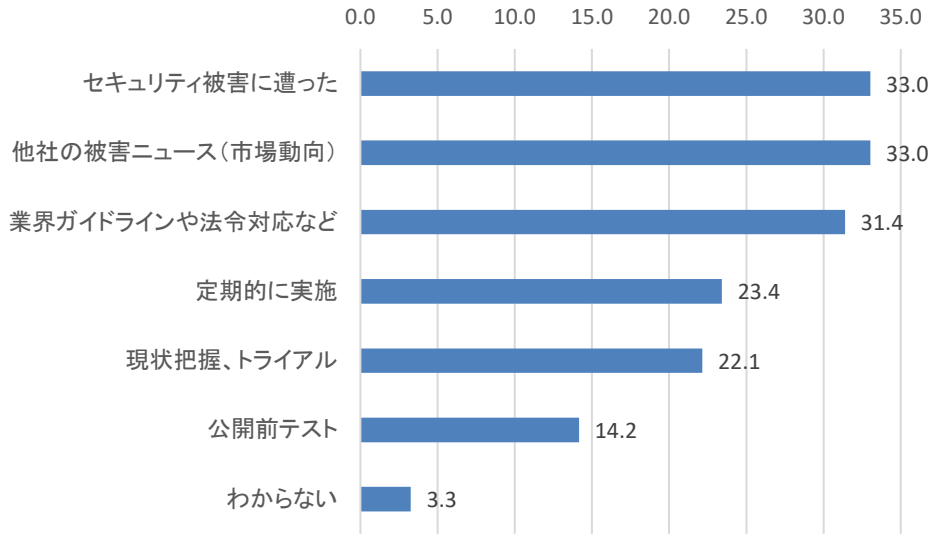
	実施	検討中	予定なし	不明
全体(n=703)	50.1	17.2	18.2	14.5
製造(n=210)	49.0	19.5	19.5	11.9
金融(n=65)	58.5	15.4	10.8	15.4
流通／小売(n=79)	44.3	13.9	24.1	17.7
通信／メディア(n=28)	57.1	14.3	10.7	17.9
運輸／運輸サービス(n=29)	48.3	13.8	13.8	24.1
サービス(n=73)	49.3	12.3	19.2	19.2
ITサービス(n=69)	62.3	7.2	11.6	18.8
建設／土木(n=40)	45.0	22.5	25.0	7.5
公共(n=19)	47.4	15.8	21.1	15.8
医療／福祉(n=28)	42.9	28.6	17.9	10.7
政府／教育(n=63)	44.4	27.0	20.6	7.9

Note:　・回答率（%）

Source：Digital Hearts, 2019

回答企業全体の 78.4%（551 社）が、いずれかのセキュリティテストを実施または検討している。Figure 16 に、セキュリティテスト各種の実施（検討）理由と、Table 7 に産業分野別の集計結果を示す。「セキュリティ被害に遭った」あるいは「他社の被害ニュース（市場動向）」が、いずれも 33.0%でその理由のトップである。web サービスの利用が拡大し、ユーザー側の情報管理に対する意識も向上している。少なくとも、サイトリニュアルや追加機能の公開前には、安全性を確認するセキュリティテストを実施すべきである。また定期的にセキュリティテストを実施している企業でも、形骸化を避けるために、外部環境の変化を踏まえた内容の見直しを勧めたい。

Figure 16　セキュリティテスト実施（検討）理由



Notes:　・n=551（セキュリティテストの実施経験がある、または検討中企業のみの回答）
・複数回答、回答率（%）

Source：Digital Hearts, 2019

Table 7　産業分野別、セキュリティテスト実施（検討）理由

	セキュリティ被害に遭った	他社の被害ニュース（市場動向）	業界ガイドラインや法令対応	定期的に実施	現状把握、トライアル	公開前テスト	わからない
全体(n=551)	33.0	33.0	31.4	23.4	22.1	14.2	3.3
製造(n=165)	38.8	33.3	29.7	20.0	26.1	17.0	3.6
金融(n=58)	34.5	32.8	25.9	24.1	20.7	12.1	5.2
流通／小売(n=57)	33.3	38.6	28.1	21.1	22.8	19.3	7.0
通信／メディア(n=22)	36.4	13.6	36.4	31.8	36.4	9.1	0.0
運輸／運輸サービス(n=19)	31.6	42.1	36.8	31.6	15.8	15.8	0.0
サービス(n=53)	32.1	22.6	28.3	22.6	11.3	15.1	3.8
ITサービス(n=57)	29.8	40.4	42.1	35.1	21.1	10.5	1.8
建設／土木(n=32)	34.4	40.6	31.3	15.6	31.3	15.6	3.1
公共(n=14)	28.6	42.9	35.7	21.4	14.3	0.0	0.0
医療／福祉(n=21)	28.6	38.1	33.3	14.3	19.0	14.3	4.8
政府／教育(n=53)	18.9	24.5	32.1	26.4	17.0	9.4	0.0

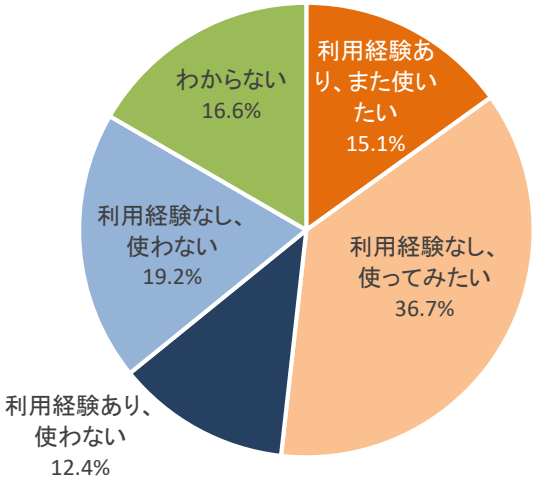
Notes:　・回答率（%）
・公共は回答数 15 以下のため、参考値

Source：Digital Hearts, 2019

労働人口の減少が進む国内では、IT やセキュリティ分野における人材不足も懸念されており、政府の発表では将来的にさらなる深刻化が指摘されるが、これは世界共通の課題でもある。ここでは、前述のペネトレーションテストに関連して、「バグバウンティ」の利用経験を調査した結果を Figure 17 に示す。「バグバウンティ」とは、報酬金を設けホワイトハッカーに脆弱性発見を依頼するプログラムで、マイクロソフトや、Amazon、Google、Facebook を始めとする先進的なテクノロジー企業が積極的に活用している。DX などの取り組みが進む近年、国や業界を問わずサイバー攻撃の被害も拡大し、特に IT やセキュリティ分野に精通した人材の需要が増している。このプログラムは、社外の専門スキルを持つ人材活用の一環としても注目され、この 5 年ほどで普及が進んでいる。

調査の結果、国内でも 27.5%の企業にすでに「バグバウンティ」の利用経験があり、医療／福祉では 39.3%、製造も 33.8%がすでに利用していた。一度だけ試してみた企業もあるようだが、全体としては、利用経験に関わらず、「バグバウンティ」を使いたいという企業が 51.8%で過半数以上を占めている。通信／メディアや政府／教育、金融など複数の産業に利用意向があるものの、自社システムに対するアクセスや費用感に懸念を示す 31.6%が利用しないと回答した。

Figure 17　産業分野別、バグバウンティの利用経験と今後の利用意向



	利用経験あり、また使いたい	利用経験あり、使わない	利用経験なし、使ってみたい	利用経験なし、使いたくない	わからない
全体 (n=703)	15.1	12.4	36.7	19.2	16.6
製造 (n=210)	17.6	16.2	34.3	17.6	14.3
金融 (n=65)	20.0	6.2	43.1	16.9	13.8
流通／小売 (n=79)	15.2	10.1	40.5	21.5	12.7
通信／メディア (n=28)	14.3	7.1	50.0	14.3	14.3
運輸／運輸サービス (n=29)	6.9	3.4	41.4	24.1	24.1
サービス (n=73)	13.7	6.8	31.5	24.7	23.3
ITサービス (n=69)	11.6	17.4	26.1	21.7	23.2
建設／土木 (n=40)	12.5	15.0	40.0	17.5	15.0
公共 (n=19)	5.3	21.1	31.6	10.5	31.6
医療／福祉 (n=28)	21.4	17.9	32.1	21.4	7.1
政府／教育 (n=63)	12.7	9.5	44.4	17.5	15.9

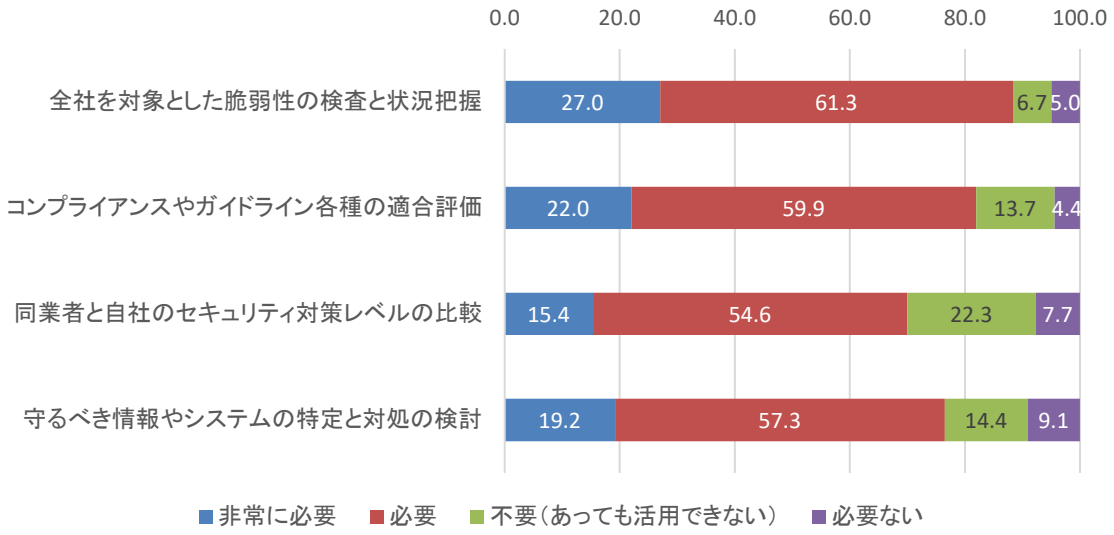
Note:　・n=703、回答率(%)

Source：Digital Hearts, 2019

Figure 18 に、サイバーセキュリティ対策における項目別の必要性を調査した結果を示す。脆弱性診断の実施率が示す通り、脆弱性の有無など状況把握に対する需要が他の項目よりも高い。次いで、コンプライアンスやガイドラインの適合状況に対する必要性も感じている。しかし、同業者の水準を知りそれを対策に生かす点では、企業による考え方やリテラシーの差が回答にも反映されている。いずれにしても、サイバー攻撃は年々手法が巧妙化し、攻撃者の数と攻撃レベルが向上している。残念なことに、この傾向はさらに加速し、デジタルサービスの普及に伴い被害規模も拡大すると考えられる。

従来型のエンドポイント対策など、各種のセキュリティ対策ツールで防御していても、会計ソフトの更新プログラムとして拡散した NotPetya のように、システム環境を回復不能に陥れるマルウェアを完全に防ぐことはできない。そのため今後のセキュリティ対策では、あらゆる手段の攻撃を受けることを前提に、守るべき情報やシステムを特定し、それらの保護と、ビジネスを止めない仕組みを検討すべきである。

Figure 18　サイバーセキュリティ対策における各項目の必要性



Note:　・n=703、回答率（%）

Source：Digital Hearts, 2019

主要産業の動向

サイバー攻撃などに関する危機意識とセキュリティ対策レベルの差を、業界動向と合わせ考察する。

危機意識の高い業界の動向

製造（n=210）:

製造は、長年、生産現場が独自の改善に取り組んできたが、より広範囲な取り組みとなる Industry4.0 の実現、世代交代や労働力不足を解決する働き方改革など、取り組み課題が多様である。生産拠点と商品を提供する市場獲得で、グローバル展開に積極的に取り組んでいる。IT とセキュリティの観点では、工場のスマート化や本社による可視化を検討しているが、工場と本社は全く別のシステムを導入しており、組織としての独立性も強いことから、その連携は容易ではない。特許関連など社外秘情報が多く、これまで外部接続を避けてきたが、設計／製造工程における各種情報の電子化や 3D モデリング、BOM や BOP（部品／工程表）の導入、省力化や制御管理に IoT を導入し始めたことで、ネットワークから分断されてきた生産現場も外部につながり始めている。今後の競争力強化には、サービス化を実現する IT 活用とセキュリティレベルの高度化が必須である。今回の調査では、製造は危機意識が高く、製造全体の 78.6%（165 社）でセキュリティテストが実施／検討されていた。その主な理由は「セキュリティ被害に遭った」が 38.8%と、全体（n＝551）平均である 33.0%を 5.8%も上回っており、深刻な状況にある。クラウド／インターネット／web 活用では、（準備中も含み）67.1%が自社業務インフラとして、同様に 68.1%が企業ユーザー向けサービス提供に取り組んでいる。最も海外展開が活発化している業界であり、本社と離れた各国の拠点に至るまで、包括的な対策強化が課題である。

金融（n=65）、通信／メディア（n=28）:

いずれも IT テクノロジーの積極的な採用で、早い段階からさまざまな種類のデータ活用に取り組んできた。その成果は、迅速な経営の意思決定や、多様な顧客向けサービスに反映され、異業種連携によるビジネス領域の拡大にも意欲的に取り組んでいる。事業特性から、監督省庁の規制も厳しく、個人情報などの取り扱いにも厳重で慎重な姿勢を取っている。そのため、IT 活用の成熟度もさることながら、セキュリティ対策レベルは全体平均を超えており、客観的な視点となる各種のセキュリティテストの実施／検討においても、金融では 89.2%（n=58）、通信／メディアも 78.6%（n=22）が取り組んでいる。両者ともサイバー攻撃の標的となりやすい業界であり、製造に続いて被害にあったという回答率が高く、セキュリティテストなど客観的な視点を対策に取り入れようとしている。新たな IT テクノロジーの活用を試みながらも、自社サービスが社会に及ぼす影響を考慮し、今回の調査でも高い危機意識でセキュリティ対策の精度向上を図り、大規模な顧客情報管理とサービスの安定稼働を追求してきた結果を表している。

公共（n=19）、政府／教育（n=63）:

これまで他の産業分野よりも、人手による業務対応とサービス提供に重きが置かれてきた業界である。しかし、IoT の普及でスマートメーターの導入が進み、マイナンバーなどによる電子的な住民管理、教育現場のスマートデバイス普及によるオンライン授業などが急加速で進んでいる。また単純な個人情報の

管理というよりは、その属性や生活習慣／生活保護の記録など、扱う情報に地域性やプライバシー性が高い特徴を持つ。クラウド／インターネット／web サービスの検討状況では、今後一般および企業ユーザー向けの強化を進めていく。特に公共が、幅広い取り組み強化を検討している。業界自体は新しい分野ではないが、IT を活用したサービスは近年の取り組みであり、後発であるが故にプライバシーなどを重視する傾向がセキュリティ対策にも反映されている。そのため「ダーク web の情報漏えい調査」でも、公共の実施率が 63.2%で、全体平均を 15.0%も上回り、検討中の回答率も政府／教育が全産業で最も高い 20.6%を示していた。

危機意識の低い業界の動向

運輸／運輸サービス（n=29）:

この分野には、鉄道や配車サービス、郵便や宅配事業者が含まれる（詳細は巻末の産業分野を参照）。大型の輸送機器の運航制御や、車両の位置情報も含む宅配システムなど、自社業務に特化した独自の IT システムが導入されてきたことから、汎用的な脆弱性を狙う攻撃を逃れてきた可能性はある。しかし、各種交通系の電子マネーやチケット購入、郵便と宅配の再配送の受付など、業務の一部で web サービスの活用が一般化しており、信用情報も含むこれらに対するシステム侵害は、社会にとっても身近で深刻なものとなる。開発会社以外による第三者視点のセキュリティテストが、web アプリケーション部分などの仕様や脆弱性に関する新たな知見をもたらす可能性がある。自社サービスの代替となる競合相手がいる場合は特に、料金や提供サービスの内容に加え、バックエンドシステムおよび web サービスの動作（レスポンス速度や使用感）と情報セキュリティを差別化要素として、強化すべきである。

医療／福祉（n=28）:

現状と 3 年後の目標とする「セキュリティ対策レベル」が、全産業中で最も低い回答結果となった。その一方で、「バグバウンティ」の利用経験は、全産業中で最も高い 39.3%であった。これは従来型の人的サービスかテクノロジーベースか、その事業内容による差が出ていると考えられる。また新規領域であるテクノロジーベースの場合でも、日常的なバイタル監視による健康維持から、地域におけるリモート医療、3D モデリングとシミュレーションを駆使した高度医療などサービス内容が多岐にわたる。しかし、事業内容に関わらず、個人情報よりも秘匿性の高い医療情報を扱うことに差はないため、安定したサービス提供と同時に、セキュリティ対策とプライバシー情報の保護にも細心の注意が必要である。現状のレベル感では、IT 活用やセキュリティ対策に課題を抱えており、今後の事業の高度化には提携先やパートナーも含めた IT とデータ活用における体制強化を図る必要がある。

他にも、「危機意識」の点では流通／小売（n=79）やサービス（n=73）が、全体より低い結果を示している。今回の調査は年商規模で 10 億円以上を対象としたが、両分野とも年商規模が下がるほど、IT 活用やセキュリティ対策に課題があることは想像に難くない。この点では、高価で質の高いサービスから、一定レベルへの到達を補助するような身近な内容まで、国内では幅広い支援が必要であると考える。

まとめ

これまで述べてきたように、産業分野を問わず「サービス化」が拡大し、Airbnb などのシェアリングエコノミー、ロボティクスと自動運転、遠隔医療など、IT テクノロジーをベースにした新領域の市場が多数形成されている。このような新市場に必要なのが、IT と通信である。そして、システム連携による高度なデータ活用が、その実現を支えていく。事業内容にかかわらず、社内外で取り扱うデータの量がますます増加し、その分析や共有によるデータドリブンな企業経営とビジネス支援が進行する。これは社内用途でも同様である。世代交代を迎えた企業や、個々の人材活用に取り組む企業の働き方改革では、社内データプラットフォームの導入や活用検討が積極化している。自社のタレント属性把握や、所属部署を超えたプロジェクトの発足と交流、そこから新製品や新規事業が生み出されることが期待されている。今後は、新領域のデジタル製品やサービスによる売上が、日本の GDP に占める割合を次第に増し、物販に代表される従来型の市場規模と並ぶ日もそう遠くはないだろう。

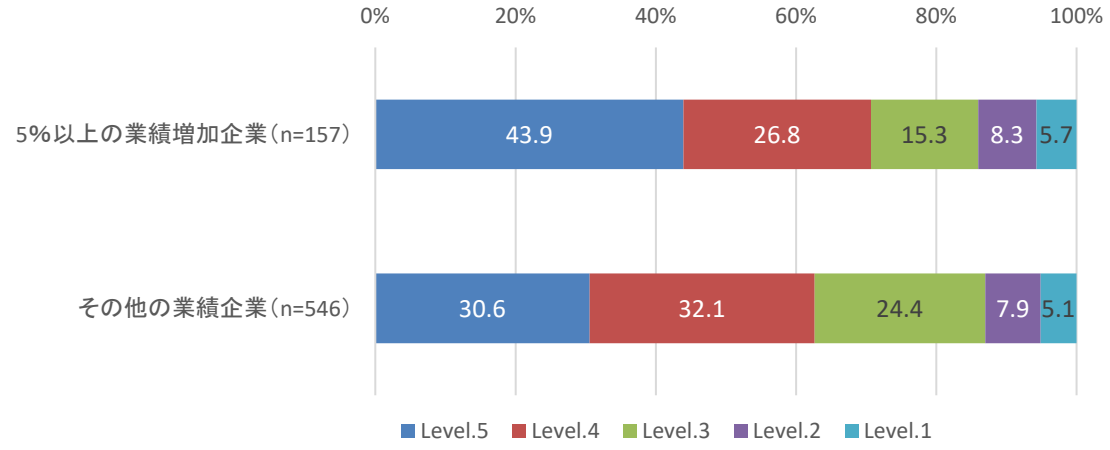
悪意ある攻撃者は、この大規模に集約されるデータと複雑な関連性を持つシステムを狙ってくる。サイバー攻撃とは、データドリブンな社会であるが故に懸念すべき脅威である。この便利さとリスクが存在する社会では、ユーザー側の IT リテラシーや情報セキュリティ意識も自ずと向上する。顧客やパートナーにとって、利用サービスの重要な選定基準となるのは、サービス内容と同時に信頼できるセキュリティ対策が施されているかどうかだ。

サイバー攻撃の対象となるのは、金融や政府、通信／メディアあるいは大企業とは限らない。本調査の結果にもあるように、経費精算や CRM、情報共有は SaaS など web 経由で提供されており、今後は効率化や省力化の取り組みとして全社／事業部単位でさらに多様なオンラインサービスの利用が拡大する。世の中の変化に伴って、必要とされるセキュリティ対策の内容やレベルも変化する。一般企業より IT リテラシーが高いサービスベンダーであっても、自社基準のセキュリティ対策が信頼に足りるものであるか、第三者の視点を適宜取り入れるべき段階にきている。

最後に、サイバーセキュリティに対する危機意識と対策の必要性の調査結果を、業績別に示す（Figure 19～20）。積極的な海外展開を図り、業績の増加傾向を維持する企業は、各種の脅威に対する危機意識がその他の業績企業より高く、サイバーセキュリティ対策の必要性と、その効果がビジネスにもたらす影響に気づいている。

繰り返しとなるが、デジタルなつながりによってスマート化が進む社会では、経営者はこれまで以上に IT とセキュリティのリテラシーを高め、全社あるいはサプライチェーン全体にガバナンスを発揮することで、顧客の信頼に基づく盤石な事業基盤を構築できる。自社資産と顧客を守るセキュリティ対策は、ビジネス拡大に必要な IT 活用と同様に、経営戦略の一部として捉えるべきである。

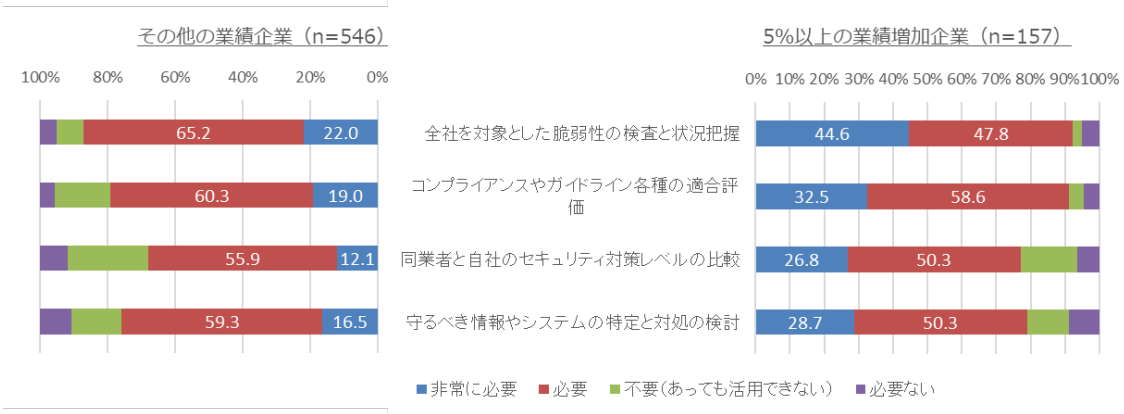
Figure 19　業績別、サイバー攻撃に対する危機意識



Notes:　・回答率（%）
・危機意識レベル:非常に強い危機意識＝Level5～危機意識はない＝level1

Source:Digital Hearts, 2019

Figure 20　業績別、サイバーセキュリティ対策における各項目の必要性



Note:　・回答率（%）

Source:Digital Hearts, 2019

補足：産業分野の定義

製造	組立製造：自動車、鉄道、航空機、ドローン
	組立製造：IoT デバイス関連
	組立製造：設備、機械、その他
	プロセス製造
金融	銀行
	保険証券
	その他金融サービス
流通／小売	流通
	小売
通信／メディア	電気通信
	メディア
運輸／運輸サービス	鉄道／航空機／船舶／配車サービス
	郵便、輸送サービス（宅配など貨物）
サービス	旅行／宿泊
	飲食／娯楽／エンターテイメント
	専門サービス、広告、調査研究機関、不動産、リース、その他
IT **サービス**	ハードウェア、ソフトウェアベンダー
	SIer／NIer
	リセラー、その他情報サービス
建設／土木	建設／土木
公共	電気、水道、ガス、熱供給など
医療／福祉	医療／福祉
政府／教育	学校、教育サービス
	官公庁、自治体、協同組合など

発行

株式会社 デジタルハーツ

2001 年に創業したデジタルハーツは、ソフトウェアの不具合を検出するデバッグとシステムテストを中心にサービス事業を展開し、間もなく 20 年の節目を迎えます。この間、約 8,000 人という豊富なテスト人材と、システムテストのノウハウを蓄えてきました。その中には、国内最大規模となる 300 人超の「ソフトウェアテスト技術（JSTQB）」資格保有者もおります。これらの豊富な人材が提供する、お客様の要望に柔軟かつ効率的に対応するシステムテストを最大の強みに、多様な業種業態における高品質な製品開発とシステム運用を支援しています。

現在デジタルハーツは、第二創業期の取り組みの一つとして、法人向けのセキュリティ分野で”SAVE the DIGITAL WORLD”の実現に向け、従来のツールを普及させるセキュリティビジネスとは一線を画すべく「検査」「監視」「人材育成」の 3 分野の取り組みを拡大しています。次世代のデータ活用に即したセキュリティ強化策として、脆弱性検出と対策には「検査サービス」を、またお客様が導入した高度なセキュリティ製品の運用には SOC（Security Operation Center：セキュリティ監視拠点）などによる「監視サービス」をご提供します。また、独自の教育プログラムである『デジタルハーツ・サイバーブートキャンプ』による、セキュリティエキスパートの育成にも取り組んでいます。

国内企業が抱える IT およびセキュリティ人材不足などの課題解決に向け、高度な知見によるお客様支援を、パートナー各社とともに継続的に強化してまいります。

本社所在地：
〒　163-1441　東京都新宿区西新宿三丁目 20 番 2 号 東京オペラシティビル 41 階
TEL 03-3379-2053
https://www.digitalhearts.com/

調査、執筆担当：　セキュリティ事業部　マーケティングマネージャー　もたい洋子

（略歴：トレンドマイクロやソフトバンクグループなどでマーケティング、IDC Japan のアナリストを経て、2019 年 4 月より現職）

DHSECRR201908


Digital Hearts