サイバー戦略により改革の加速と信頼構築を図るハイテク企業

強靭なサイバー戦略にとって不可欠な
文化とテクノロジー

kpmg.com/techinnovation

序文

ハイテク企業のリーダーたちは、最大の脅威とオペレーション上の最優先事項の両方として、サイバーセキュリティを挙げています。その対応として、サイバーレジリエンス（サイバー攻撃からの回復力）を強化し、デジタルトランスフォーメーションとビジネスモデル改革を加速させ、利害関係者の信頼を高めるために、スキル、文化、テクノロジーへの投資を進めています。

新型コロナウイルス感染症（COVID-19）のパンデミックにおいても、ハイテク企業はデジタルトランスフォーメーションを促進し、世界中の産業が活動を維持できるよう製品とサービスを提供し続けています。しかし、このデジタル化の加速によって、サイバー攻撃に対する脆弱なポイントが爆発的に増えました。それは、ほぼバーチャルな働き方が普及し、クラウドの導入が増え、サプライチェーンの再形成が急ピッチで行われ、新たなビジネスパートナーシップが実現したことが要因です。新しいテクノロジーの急速な統合は、蓄積・保護すべき新しいデータも大量に生み出しました。

これらのトレンドのなかには、パンデミック前にすでに進行し、パンデミックによって劇的に加速したものもあります。ハイテク企業も例外ではなく、迅速な対応を取ることを余儀なくされました。この新たな現実において、多くのハイテク企業の最高経営責任者（CEO）は、組織の今後3年間の成長に対する最大の脅威として、サプライチェーンの混乱や気候変動、人材リスクよりも、サイバーリスクを挙げています[1]。

またCEOたちは、オペレーション上の最優先事項としてサイバーレジリエンスを挙げています1。別の調査では、データ漏洩により100万件のデータが侵害された場合に発生する平均コストは5,200万米ドルであることが判明しましたが、これはまだ最低レベルです。侵害されたデータが5,000万件を超えると、平均コストは4億100万米ドルに跳ね上がります[2]。

一方で、ハイテク企業のリーダーは機会が存在していることも認識しています。強力なサイバー戦略に基づいてデジタルトランスフォーメーションの恩恵を最大限に享受することで、企業はリスクが管理されていることを認識しつつ、急速にビジネスを成長させることができるのです。ハイテク企業の幹部の61%が自社の情報セキュリティを競争上の強みとして認識しており、半数超（57%）が自社のサイバーセキュリティ戦略は成長戦略と一体化していると回答しました[3]。

ハイテク企業のCEOの大多数（77%）は、強力なサイバー戦略は利害関係者の信頼を生み出すのに不可欠だと考えています1。強力なサイバー戦略は、人材とテクノロジーの両方を対象としています。サイバー分野における人材不足が続いているため、あらゆる部署のあらゆる従業員が自らのサイバー能力を高めることが求められています。最高情報セキュリティ責任者（CISO）であってもステップアップを図っています。自らの役割を拡大し、他のビジネス部門のリーダーとの連携を深め、リーダーたちに対する影響力を高めようとしています。テクノロジーの観点から見ると、企業のリーダーは組織の安全対策を強化するため、さまざまなソリューションへの投資を拡大しています。

サイバーセキュリティは、リスク管理とコンプライアンスに焦点を当てるという従来の枠を超えて、利害関係者からの信頼獲得を支援し、組織のレジリエンスを強化する競争上の強みになっています。もはやITだけに関わる問題ではありません。組織の文化とテクノロジー、業務全体に定着させなければならない戦略的優先事項なのです。

1. KPMGグローバルCEO調査2021、回答者数は120人。
2. IBM、2021年情報漏えい時に発生するコストに関する調査
3. KPMG Technology Industry Survey 2021、回答者数は802人。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

主な調査結果

KPMGが、2つのグローバル調査（KPMG Technology Industry SurveyとKPMGグローバルCEO調査）で寄せられた、サイバーセキュリティ問題に関するハイテク企業のCEOと幹部の意見を詳細に検討した結果、次のことが明らかとなりました。

#1 サイバーセキュリティリスクは成長への最大の脅威である。

74% 将来のサイバー攻撃に備えていると回答。

#1 サイバー関連のスキルと文化に重点を置いたサイバーレジリエンスは、オペレーション上の最優先事項である。

61% 情報セキュリティは戦略的な役割を持ち、競争上の強みになる可能性があると感じる。

87% サイバーセキュリティ文化の構築は、技術統制の構築と同じくらい重要だと思う。

57% 自社のサイバーセキュリティ戦略は、成長戦略と一体化されていると考える。

出典：KPMGグローバルCEO調査、回答者数は120人／KPMG Technology Industry Survey 2021、回答者数は802人。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

スキルとテクノロジーへの投資

人的ファイアウォールを築く

ハイテク企業のCEOは、脅威環境が絶えず変化していること、そして、高度なソリューションがサイバーセキュリティプログラムの基礎になりうることを認識しています。しかしながら、テクノロジーがすべてを守れるわけではありません。人間の行動により保護を強化する必要があります。

多くの調査により、報告されている違反の多くには、何らかの人的ミスの要素が含まれていることが明らかになっています。このことからも、企業にとって、全従業員のスキル向上を組み込んだ、包括的なサイバーセキュリティ戦略の策定と運用が極めて重要になっています。

人的ファイアウォールを構築することで、企業はサイバー意識を持つことから一歩前進し、サイバーセキュリティを巡る従業員のコミュニケーションと訓練のための統合的かつ全体的なアプローチを構築する、すなわち従業員の行動を、意識的な選択に基づくものから、身に付いた習慣へと進化させることができるのです。ハイテク企業のCEOはこのことを認識し、今後3年でサイバー面とデジタル面のレジリエンスを構築するために行う予定である重要な対応として、スキル向上と文化の醸成を挙げています。

今後3年でデジタルレジリエンスを構築するために、ハイテク企業が行う主な対応

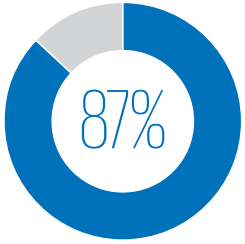
1 位タイ	**サイバーセキュリティおよびその他のテクノロジーリスク分野でのスキル向上に注力する**
1 位タイ	**上級幹部が支持する、デジタルとサイバーリスクの強力な文化を築く**
2	**オペレーション上のレジリエンスに関するガバナンスと重大なインシデントから回復する能力を強化する**
3	**安全で強靭なクラウドベースのインフラに投資する**

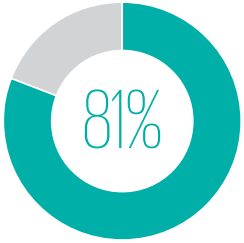
出典：KPMGグローバルCEO調査2021、回答者数は120人。

またハイテク企業は、シェアードデータとシェアードサービスを通して結びついた、サプライヤーとパートナーの複雑なエコシステムの一部でもあります。従来の契約と義務のモデルは、この急速に進化するサプライチェーンには適していないように思われます。あらゆる当事者に安全を届けるために、これらパートナーのサイバーに関する教育、行動、文化も変えなければなりません。

ハイテク企業のCEOの多くは、サイバーに関する高度なスキルと文化は極めて重要であり、企業は包括的な防衛計画を立てるために、パートナーおよびエコシステムと連携しなければならないと強調しました。

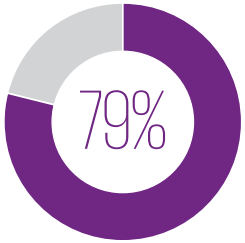
サイバーセキュリティ文化の構築は、技術統制の構築と同じくらい重要である。





ランサムウェアの身代金要求問題に適切に対処するには、産業全体のアプローチが必要である。

パートナーのエコシステムとサプライチェーンの保護は、自社におけるサイバー防衛の構築と同じくらい重要である。



出典：KPMGグローバルCEO調査2021、回答者数は120人。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

スキルとテクノロジーへの投資（続き）

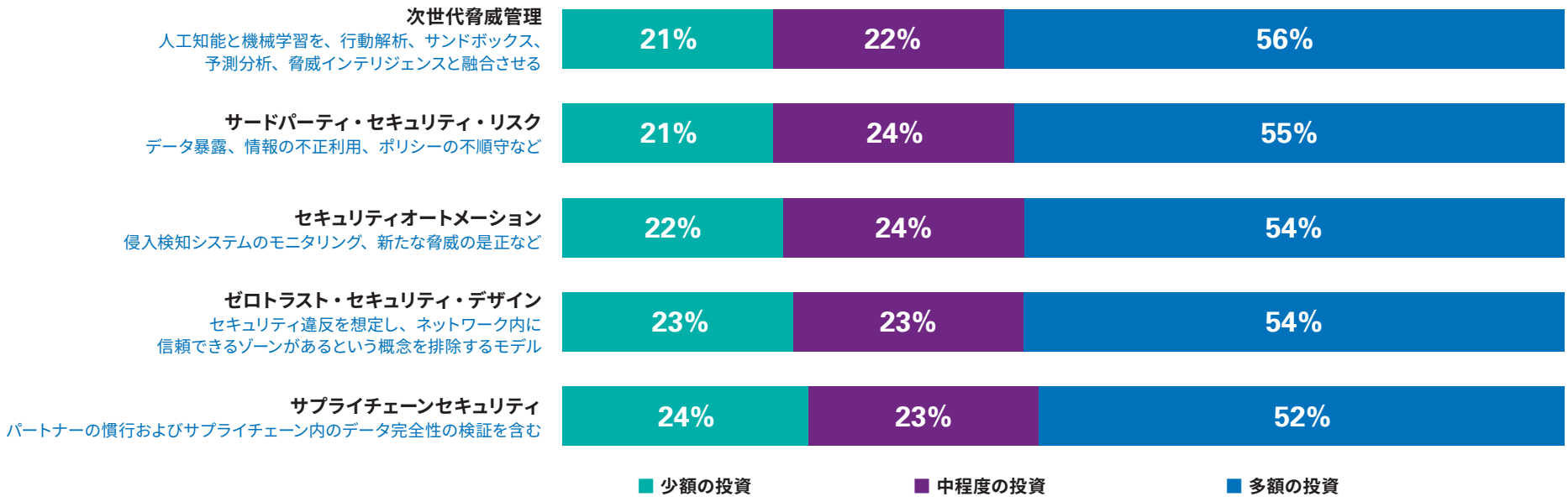
サイバーセキュリティには、テクノロジー集団が必要

企業はずっと以前から、1つのテクノロジーやプロセスだけではサイバーリスクを低減できないことを認識してきました。企業は、新たな脅威を特定し、組織の対応力を向上させ、セキュリティ関連部署とビジネス部門の効率を上げるために、継続的かつ広範囲に投資を行う必要があります。ハイテク企業のリーダーはまた、サイバーツールは企業の成功に必要である一方、業務効率または成長の妨げとならないよう、煩わしくない程度にとどめた方がよいとも感じています。

具体的なセキュリティ投資計画について尋ねたところ、ハイテク企業の幹部は、今後3年で複数の分野に多額の投資を行う計画だと答えました。特に、オートメーションへの投資により手作業の負荷を軽減し、スキル不足の影響を緩和し、効率性を高め、一貫性のある反復可能な方法によるコンプライアンス要件の拡大への対応を進めることができます。また、セキュリティの組込みを推進してユーザー体験を向上させるとともに、重大なサイバーインシデントへの対応時間を短縮することもできます。

私たちは、モノのインターネット（IoT）と5Gネットワークが効率性を大いに高め、これまでとはまったく異なるビジネスモデルを実現する、ハイパーコネクテッドな未来に向かっています。しかし、このような動きにより、企業は新たな攻撃にさらされ、プライバシーに関する懸念を抱えることになります。そのため、ゼロトラストなど新しいデータ中心のセキュリティモデルへの転換が求められます。KPMGの別の調査「データの緊急課題」では、回答者の44%が、効果的なデータ戦略は、サイバーセキュリティの改善において大きな影響力を持つと考えていることが明らかになりました。

今後3年のハイテク企業による予想投資レベル



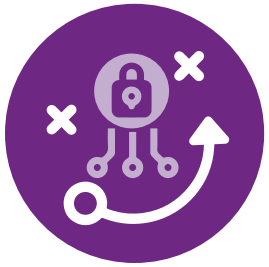
出典：KPMG Technology Industry Survey 2021、回答者数は802人。四捨五入により合計が100%にならない場合があります。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

楽観的主義をもたらすサイバー投資

ハイテク企業のリーダーたちは、自社の情報セキュリティ機能の状態、そしてそれが広範なリスク管理の取組み、第三者とのパートナーシップ、ビジネス部門のリーダーシップに与える影響に関して、全般的に楽観的な姿勢を示しています。将来のサイバー攻撃に備えていると回答したCEOの割合は、ハイテク企業では約4分の3（74%）となり、全産業の58%を上回りました[4]。

ハイテク企業のCEOは、投資拡大と注力によって、サイバーリスクを大幅に緩和する十分な能力を備えていると考えます。この自信と、それを得るのに求められる投資は必要なものです。というのも、ハイテク企業のCEOの77%が、強力なサイバー戦略は利害関係者から信頼を得るのに不可欠だとも考えているからです[4]。



ハイテク企業のCEOの

74%が、

将来のサイバー攻撃に備えていると回答[4]

ハイテク企業のリーダーたちは、このように考えています：

情報セキュリティは戦略的機能であり、競争上の強みになり得ると考えている。 **61%**

サイバーセキュリティリスクは、全体的な企業リスク計画に組み込まれている。 **60%**

重要なサービスの提供や機微情報へのアクセスを行うベンダーのサードパーティリスクを管理する準備ができている。 **58%**

サイバーセキュリティ戦略は、成長戦略と一体化されている。 **57%**

出典：KPMG Technology Industry Survey 2021、回答者数は802人。

4. KPMGグローバルCEO調査2021、回答者数は120人。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

CISOの再定義

テクノロジー企業が、オンサイトワーカーとリモートワーカー、IoTデバイス、サードパーティのパートナーやサービスプロバイダーを企業活動やエコシステムに統合することにより、CISOは、サイバーセキュリティの維持だけでなく、組織全体のレジリエンスにおいても、より幅広い役割を担うようになっています。

脅威や規制への期待が高まるにつれ、CISOはより大きな責任を負いながら、さまざまな部署やビジネス部門のリーダーたちと関係を築いています。CISOの役割は、「守って検知する」ことにとどまらず、インシデント発生直後に企業がただちに回復し、稼働するようにすること、そしてCEOが顧客、サプライヤー、規制当局、その他の利害関係者との信頼を維持できるよう支援することへと広がっています。

CISOは、最高技術責任者（CTO）や最高情報責任者（CIO）との従来の関係を維持しながら、CEOと取締役会とのやり取りを増やして、新たな脅威や緩和策に関する最新情報を常に提供しています。セキュリティをガバナンスと管理プロセス、教育、および認識に統合して適切なことを行うための企業と個人のインセンティブを適切に組み合わせることを支援しています。

またCISOはこの機会を活用して、自社のデジタルインフラ全体にセキュリティとプライバシーに焦点を合わせた設計原則を組み込むことで、組織のレジリエンスを強化しようとしています。こうした役割の拡大によって、企業はサイバー、規制、ビジネスのリスクをより効果的に低減する能力を高めることができます。

CISOが自身の役割強化のために検討すべき7つの対応

1. 顧客、収益、コスト、投資収益率を考慮し、**取締役会の考え方を理解する。**
2. **危機が発生した場合には、すぐに業務を正常化できるよう、オペレーションのレジリエンス向上に注力する。**
3. さまざまな部署を訪問し、実際のオペレーションを学ぶことで信頼を獲得していくという、自社内でのネットワーキングに**時間をかける。**
4. 役割や構造を固定するのではなく、ビジネスのサイバー関連ニーズに合わせた**組織づくりを行う。**従業員に対する外部業者の比率を考慮する。
5. **オートメーションのビジネスケースを策定**し、それがもたらす効率性と、従来の作業から解放されてより高度なレベルの仕事ができるようになった従業員がもたらす付加価値を反映させる。
6. 自社のビジネスにとっての**ゼロトラストの意味を探り**、それを1回限りのプログラムではなく、継続的な方針として捉える。
7. 既存の業界団体への参加やコミュニティーの結成などにより、同じセクターの企業に**接触する方法を探す。**

CISOの進化する役割について、詳しくはこちらをご覧ください。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

2022年に企業のリーダーが取り組むべきこと

戦略的セキュリティに関する議論の拡大

コストとスピードから、
より高い事業価値とユーザー体験を実現するための、
効果的なセキュリティに変える。

セキュリティオートメーションの活用

セキュリティオートメーションのスマートな配備を通して、
競争優位性を獲得する。

必要不可欠な人材とスキルセットの開発

サイバーセキュリティチームを、
オペレーターからインフルエンサーに変える。

プライバシーの保護

プライバシーとセキュリティを組み込んだ、
多分野にまたがるプライバシーリスク管理の
アプローチに移行する。

クラウドに適応したセキュリティの確立

導入、監視から修復まで、
オートメーションによりクラウドセキュリティを強化する。

境界を越えたセキュリティの確保

より広範なサプライチェーンが
サイバーセキュリティで保護されるようにすることで、
企業を守る。

本人確認をゼロトラストの中心に据える

今日のハイパーコネクテッドな職場において、
本人確認・アクセス管理およびゼロトラストを
有効に機能させる。

サイバーレジリエンスに関する議論の再構成

サイバー攻撃を受けた際に、業務を継続し、迅速に回復し、
影響を緩和する能力を拡大させる。

上記の検討事項について、詳しくはこちらをご覧ください。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

執筆者について

Alex Holtは、KPMGのテクノロジー・メディア・通信（TMT）セクターのグローバル責任者を務め、シリコンバレーに在住しています。高い実績と20年を超える国際経験を有するエグゼクティブであり、2012年に英国の最高執行責任者としてKPMGに加わり、2015年に英国TMTセクターのリーダーに就任しました。その後米国に拠点を移し、2018年にシリコンバレーに本社を置く複数の大手ハイテク企業を担当するグローバル・アカウント・エグゼクティブとして米国のKPMGに加わりました。2020年には数十億米ドル規模のグローバルTMTプラクティスを運営する大きな責任を任され、TMTセクターのクライアントにアドバイザリー、税務、監査の幅広いサービスを提供する、数千人のKPMGプロフェッショナルを率いています。alexanderholt@kpmg.com

Mark Gibsonは、KPMG米国のテクノロジー・メディア・通信セクターのナショナルセクターリーダーを務めています。公認会計士とアドバイザリーの専門家として30年の経験があり、監査・アドバイザリー担当パートナーとして、ハイテク・消費財・小売産業のクライアントを担当してきました。現在の役職に就く前は、シアトルオフィスのマネージングパートナーを務めていました。シアトルとシリコンバレーの複数の大手クライアントを担当するアカウントエグゼクティブおよび大手ハイテク企業のグローバル・リード・パートナーとして、15を超える国々の監査、税務、アドバイザリー担当KPMGプロフェッショナルと連携しています。mgibson@kpmg.com

Vijay JajooはKPMGサイバーセキュリティサービスチームのプリンシパルです。テクノロジーおよびマネジメントのリーダーとしての実績を持ち、IT戦略、エンタープライズ・セキュリティ・アーキテクチャー、ソリューション導入、本人確認・アクセス管理、クラウドセキュリティ、ならびに企業のガバナンス、リスクおよびコンプライアンスに特化した20年を超える経験を有します。世界のハイテク企業に対して、信頼確立や、製品・サービスへのサイバーセキュリティとプライバシーの実装を通した変革の支援を行っています。先進的な解析を用いて、革新的なソリューション確立に向けた部門にまたがる連携を推進するとともに、サイロ化されたデータの関連付けを行い、効果的なリスク緩和に向けた意思決定のために知見を提供します。vjajoo@kpmg.com

Contributors

Danny Le
Principal, Cyber Security Services
KPMG LLP
dqle@kpmg.com

Rik Parker
Principal, Cyber Security Services
KPMG LLP
rikparker@kpmg.com

Deepak Mathur
Managing Director, Cyber Security Services
KPMG LLP
deepakmathur@kpmg.com

Austyn McLoughlin
Managing Director, Cyber Security Services
KPMG LLP
austynmcloughlin@kpmg.com

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

KPMGによる支援

KPMGの各ファームは、進化する脅威に直面するなかでも、強靭で信頼性の高いデジタル世界を作るための支援を行います。KPMGのサイバーセキュリティ・プロフェッショナルは、リスクについてさまざまな分野にまたがる知見を提供することができるとともに、皆様が明日に期待を持て、迅速に動き、高い安全性と信頼性のテクノロジーで優位に立てるよう、組織全体にセキュリティを行き渡らせる支援を行うことができます。

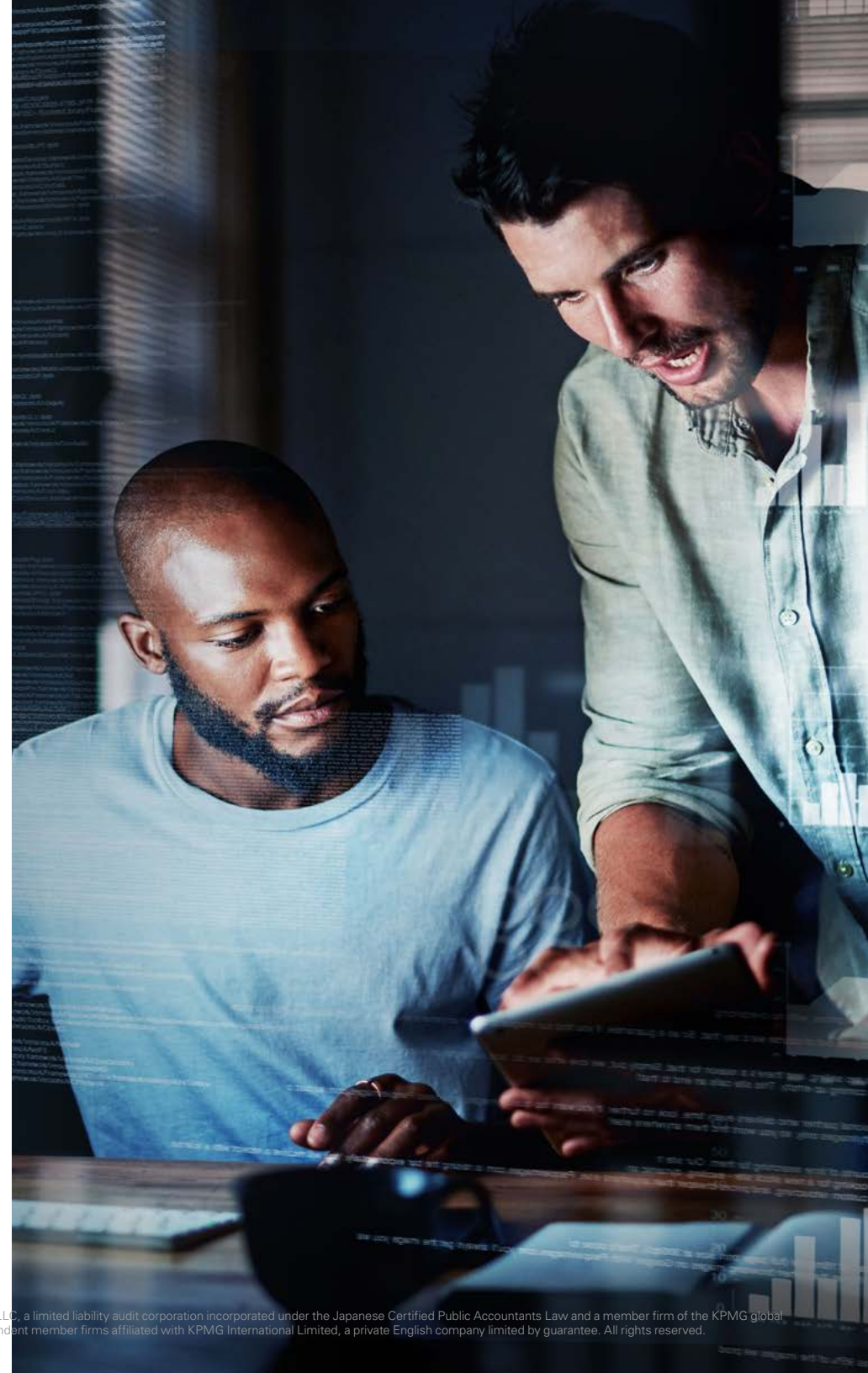
皆様がサイバーセキュリティの道程のどの地点にいようとも、KPMGの各ファームには、役員室からデータセンターまで全体にわたる豊富な経験とリソースがあります。サイバーセキュリティを評価し、それをビジネスの優先事項と調整することに加えて、高度なソリューションの構築とその導入を支援し、現在存在するリスクのモニタリングについて助言し、サイバーインシデントに効果的に対応する支援を行うことが可能です。

KPMGの各ファームは、技術的専門性、深いビジネス知識、そしてビジネスの保護と構築の実現に情熱を燃やすクリエイティブなプロフェッショナルという、他にはないサービスを提供します。信頼性の高いデジタル世界の創造を支援することで皆様の可能性の限界を押し広げることができるでしょう。詳しくはこちらをご覧ください。

本調査について

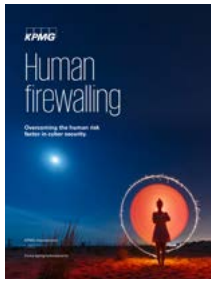
KPMG Technology Industry Surveyは今回で9年目となり、800人を超える世界のハイテク企業幹部から回答が寄せられました。調査は12ヵ国を対象にオンラインで実施され、回答者の約3分の2（65%）が最高レベルの経営幹部でした。本レポート執筆のためのデータ回収は、2021年第3四半期に完了しています。

KPMGグローバルCEO調査2021では、1,325人のCEOに経済・ビジネス状況の見通しとともに、現在のCOVID-19のパンデミックが組織の将来に及ぼす影響の見通しを尋ねました。調査は2021年6月29日～ 8月6日に実施され、11ヵ国・11産業のリーダーが対象になりました。このうちハイテク企業の回答者は120人でした。



© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

関連資料



人的ファイアウォール～ヒューマンリスクの克服

人的ファイアウォールを構築することで、企業はサイバーセキュリティにおける人的リスクファクターを抑えることができます。本レポートでは、意識を高めて、サイバーセキュリティを巡る従業員コミュニケーションの統合的かつ全体的なアプローチを構築するため、すなわち従業員の行動を、意識的な選択に基づくものから、身に付いた習慣へと進化させるために、組織が取るべき5つのステップについて検討します。

From enforcer to influencer（英語）

CISOとサイバーセキュリティチームの現在の責任は、信頼とレジリエンスを築き、実際的なセキュリティ文化を育み、セキュア・バイ・デザイン（設計段階で安全性を向上させること）の考え方をデジタルインフラとデータに組み込む支援をすることにあります。この責任を果たすためには、CISOとサイバーセキュリティチームは自らをイネーブラー（支援者）であり、ファシリテーター（促進者）であると考えなければなりません。本レポートでは、組織がレジリエンスと競争力を維持する支援をするために、CISOが取るべき7つの対応を特定します。

サイバーセキュリティ主要課題2022

パンデミックによって進んだデジタルシフトの先に目を向けると、このハイパーコネクテッドな世界が、世界中のさまざまな領域で、拡大するサイバーリスクに直面する可能性が高くなると思われます。本レポートでは、リーダーがサイバー攻撃の影響を低減して最小限に抑えつつ、顧客、データ、および持続可能性を守るために優先的に検討すべき8つの事項を特定します。

データの緊急課題

COVID-19が拡大しているなかで、大半の企業においてデジタルトランスフォーメーションが加速したものの、企業が十分に活用できていない新たなデータも大量に生まれました。本レポートでは、デジタルトランスフォーメーション投資から利益を得るために、いかにしてデータ戦略を優先し、再構築するべきかを示します。

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Contact

山根 慶太
テクノロジー・メディア・通信セクター
統轄パートナー
KPMGコンサルティング株式会社
パートナー
keita.yamane@jp.kpmg.com

和田 智
テクノロジー・メディア・通信セクター
テクノロジーセクター担当
KPMGコンサルティング株式会社
ディレクター
satoshi.wada@jp.kpmg.com

KPMGジャパン
セクター統轄室
Sector-Japan@jp.kpmg.com

テクノロジー・メディア・通信セクター
home.kpmg/jp/tmt

澤田 智輝
KPMGコンサルティング株式会社
Technology Risk Services
パートナー
motoki.sawada@jp.kpmg.com

home.kpmg/jp/socialmedia

本冊子で紹介するサービスは、公認会計士法、独立性規則および利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはあずさ監査法人までお問い合わせください。

本冊子は、KPMG LLPが2022年2月に発行した「Tech companies lean on cyber to go faster and gain trust」を、KPMG LLPの許可を得て翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点およびそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

© 2022 KPMG AZSA LLC, a limited liability audit corporation incorporated under the Japanese Certified Public Accountants Law and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. 22-1030

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.