2021 エンドポイントリスクレポート

# データとデバイスの安全に影響を与える4つのトレンド

最大の影響を評価および監視するに
あたっての重大なギャップ

ABSOLUTE

# 概要

ニューノーマルでの働き方をサポートするために急速な移行が行われる中、最も洗練された組織にとっても、健全なセキュリティ体制を維持することは大きな課題となっています。脅威が絶えず進化する状況で、ITチームとセキュリティチームは、わずか2年前には想像もできなかった環境でリスク管理戦略を展開するために急激な対応を迫られています。

サイバーセキュリティ技術への投資はかつてなく高まりましたが、データ侵害もそれ以上に増加しています。侵害による平均費用はリモート環境を持つ組織のほうがはるかに高くなりました[2] 。

最近のCSO調査では、回答者の73%が、パンデミックの影響により少なくとも今後5年間はビジネスにおけるリスク評価の方法は変化するだろうと述べています[3] 。Absoluteのエンドポイントリスクレポート第3版は、組織が注目すべきポイントを理解することを目的としています。

**76%** ITセキュリティ意思決定者の76%が、COVID-19によるパンデミックが始まって以来、組織内でのエンドポイントデバイスの利用が増えたと答えています。[1]

**82%** ITセキュリティ意思決定者の82%は、セキュリティポリシーを再策定する必要に迫られました。[1]

1 Take a Proactive Approach to Endpoint Security: Absoluteの依頼によりForrester Consultingが実施した委託調査　2020年
2 2020 Cost of a Data Breach Report: Ponemon Institute　2020年
3 Pandemic impact Report: CSO Online　2020年

## エンドポイントの可視性は、実態把握と制御を実現するためのカギとなる

今年のレポートのトレンドに結びつくテーマをひとつ指摘するとするならば、組織がすべてのエンドポイント環境の実態把握と制御を失っていることからくる制御不能の不慮のリスクがあげられるでしょう。

残念ながら、エンドポイントの完全な可視化の達成は多くの組織にとって依然として重大な課題です。最近のCybersecurity Insidersレポートでは、60%の組織がネットワーク上のデバイスの75%未満しか認知できておらず、重大な侵害から24時間以内に組織内の脆弱な資産のすべてを特定できたのは58%の組織に過ぎないことがわかっています[4]。

今年の注目すべき4つのトレンドは、実態把握がなければ組織は (多くの場合は知らないうちに) 危険にさらされているということを示しています。

- 特定されていない脆弱性が存在する
- より多くのデバイスにより機密性の高いデータが存在する
- エンドポイントの複雑化はリスクの増大を招く
- セキュリティ管理の侵害により攻撃対象領域が拡大する

4 2020 State of Endpoint Security Posture Report: Cybersecurity Insiders 2020年

## 戦略がリスクを削減する

これらのトレンドは普遍的なものではありません。多くの組織が今年からセキュリティ体制を強化し、同業他社に比べて堅牢化しようとしています。Gartner CFOによると、組織の74%が継続的なリモートワークに移行することを計画しています[5]。このようにトップパフォーマーが際立つような戦略を理解し採用することが重要です。

Absoluteの2021年エンドポイントリスクレポートは、組織環境内のサイバーセキュリティトレンドを調査したものです。このレポートは約500万社のグローバル組織のデバイスと業種に特化した洞察を分析した広範な一次調査の結果を示しており、リスク分析のベンチマークおよび今後のアクションのブループリントとなることを意図して作成されています。

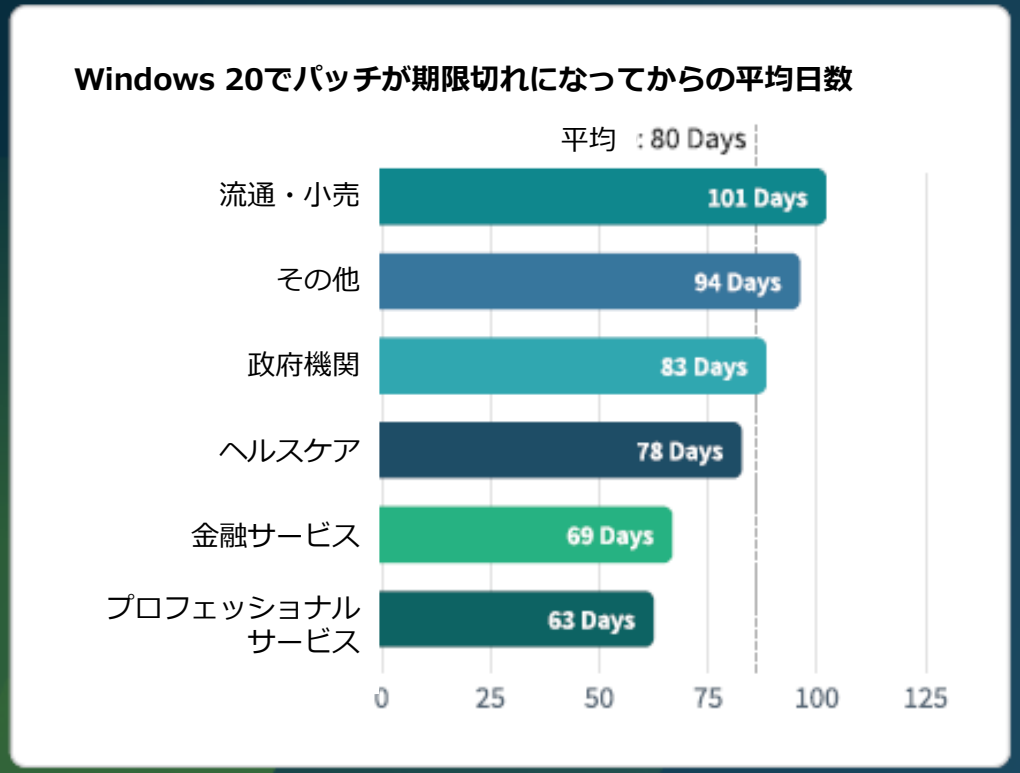
5 CFO Actions in Response to COVID-19: Gartner　2020年

TREND 1

# 特定されていない脆弱性が存在する

今年は予想通りWINDOWS 10の適用が増加しました。リモートデバイスを保護するための課題を考えたときに注目すべきこととして、エンドポイントが利用可能なOSパッチが期限切れになる期間が昨年の95日から80日に削減されました。

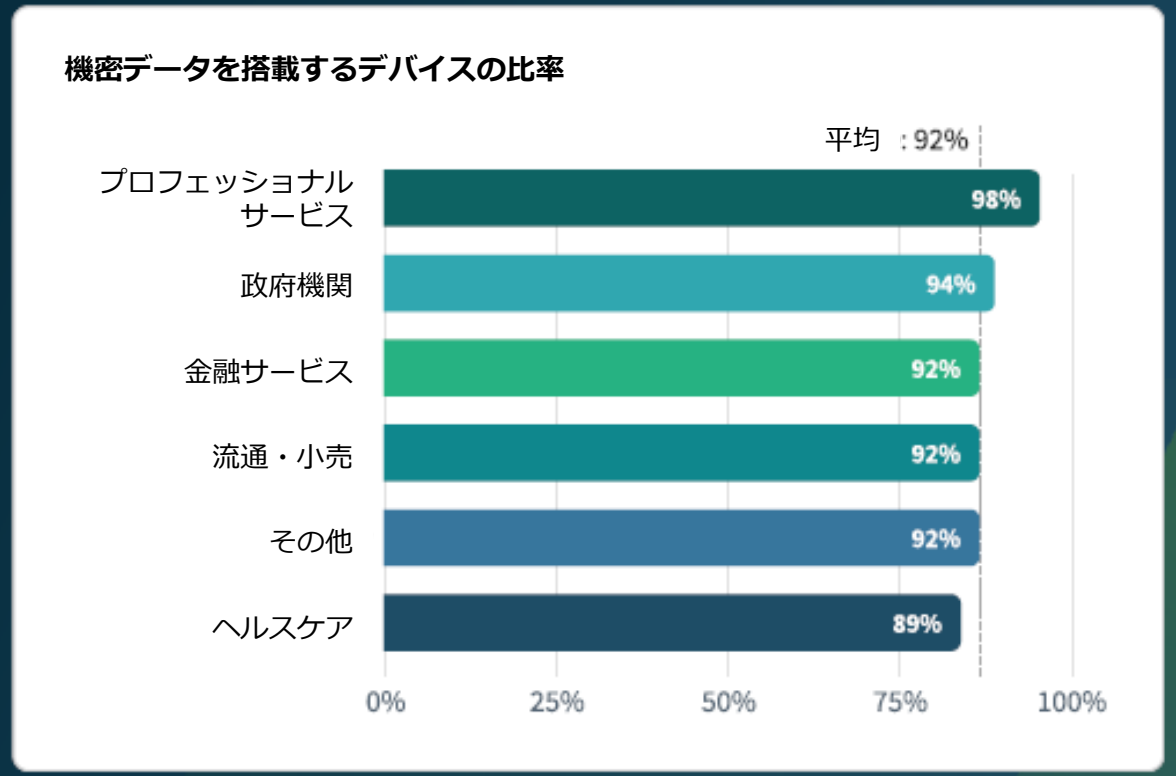
分析されたWINDOWS 10デバイスの40%がバージョン1909を実行しています。このバージョンは1,000を超える既知の脆弱性に対応しています*。




* CVE Detailsによって算出された脆弱性

業界によっては最新のOSと互換性のないコアアプリケーションに依存しているため、サポートが切れた、あるいはサポートされていないOSを使用し続けることでのリスクを承知している組織もあります。

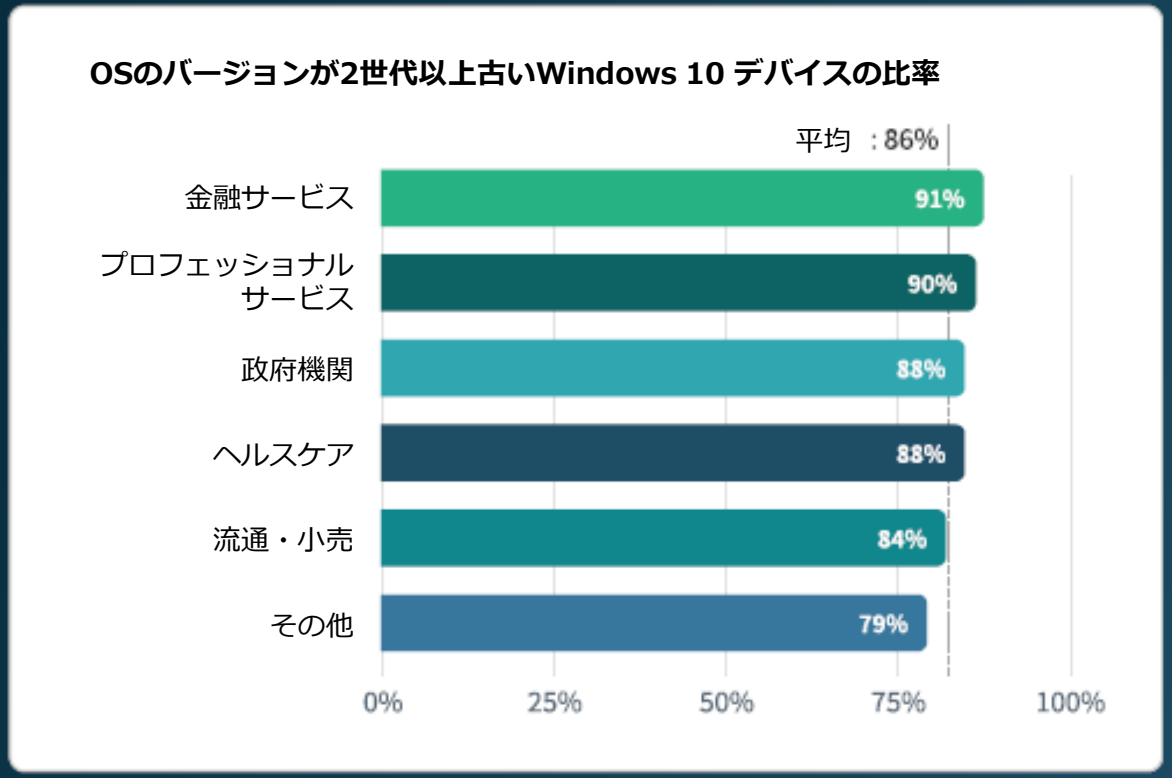
たとえば、ヘルスケア分野ではWindows 7が10%という高い稼働率を示しており、Windows 10の稼働は89%と、他分野に比べて最も低くなっています。サポートが切れたOSによるヘルスケアへのサイバーアタックの成功が増えていることをFBIが警告しているにも関わらず、その傾向は続いています[6]。




6 Ransomeware Activity Targeting the Healthcare and Public Health Secrots: Cybersecurity and Infrastructure Security Agency 2020年

Windows 10の導入においては金融サービスが最も遅く、デバイスの91%で2世代以上前のOSバージョンが使用されています。

厳格な規格に準拠し、攻撃者の標的となる可能性のあるデータを委託されている環境では、エンドポイントのセキュリティ制御の有効性を確保することでリスクを相殺することが重要です。



TREND 2

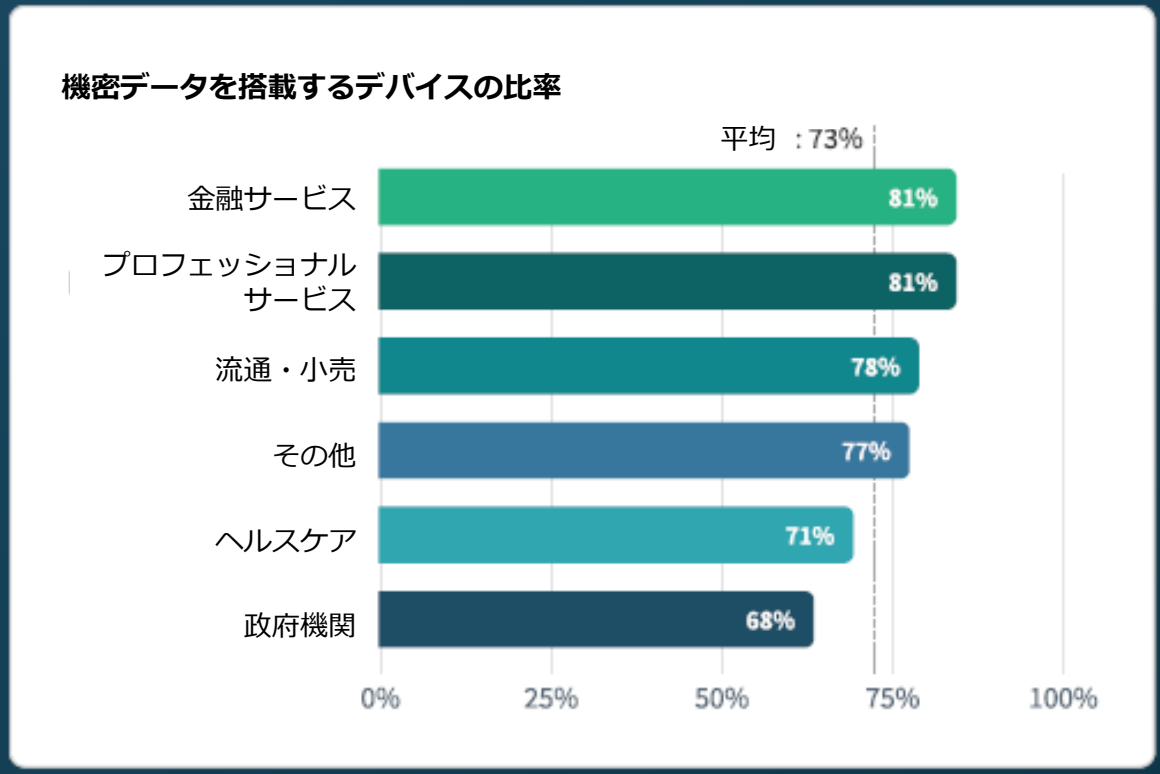
# より多くのデバイスに、より機密性の高いデータが存在する

すべてのエンドポイントはサイバー犯罪者の潜在的な標的になり得ますが、特に機密情報*を含むエンドポイントはより深刻な脅威をもたらします。今年はネットワーク外で作業する従業員が増え、より多くの情報がローカルPC上に保存されるようになったため、脅威も飛躍的に増大しました。

調査によると、すべての業種が影響を受けており、平均して73%のデバイスに機密情報が含まれています。

この数値は、デバイスごとに最もリスクの高いデータ (PIIやPHIなど) の量が劇的に増加することとあいまって、今日のリモートワークが進む世界では自動検知と自己修復が重要であることを示しています。

* 「機密情報」はデータ侵害を起こす可能性のある情報と定義され、クレジットカードデータ、PHI（Protected Health Information：個人健康情報）、PII（Personally Identifiable Information：個人を特定できる情報）などが含まれます。Absoluteは機密情報を特定しますが蓄積はしません。



ほとんどの組織のデバイスには侵害された場合には申告な経済的被害あるいは信頼の損失を招く可能性のあるデータが含まれていますが、今年は特にデバイス上のリスクのあるデータが飛躍的に増加しました。侵害されるリスクのほか、ハイレベルな機密情報が格納されたデバイスの23%が暗号化されていないとの調査結果もでています。この結果も、今日のリモート化が進む社会の中で自動検知し自動修復する必要性の高さを示しています。

デバイスあたりの機密情報の量は、前年にくらべて大幅に増加しています。

**全体** 17%

COVID-19流行前に比べて10%アップ

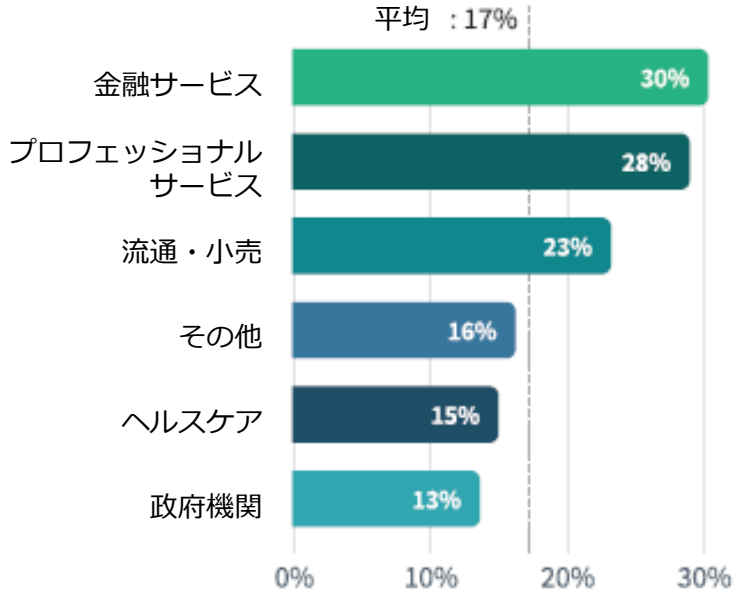
**金融サービス** 30%

COVID-19流行前に比べて15%アップ

**ヘルスケア** 15%

COVID-19流行前に比べて12%アップ
ヘルスケアでの機密情報の約半分が PHI (個人健康情報)

**機密データのインスタンスが500以上あるデバイスの割合**



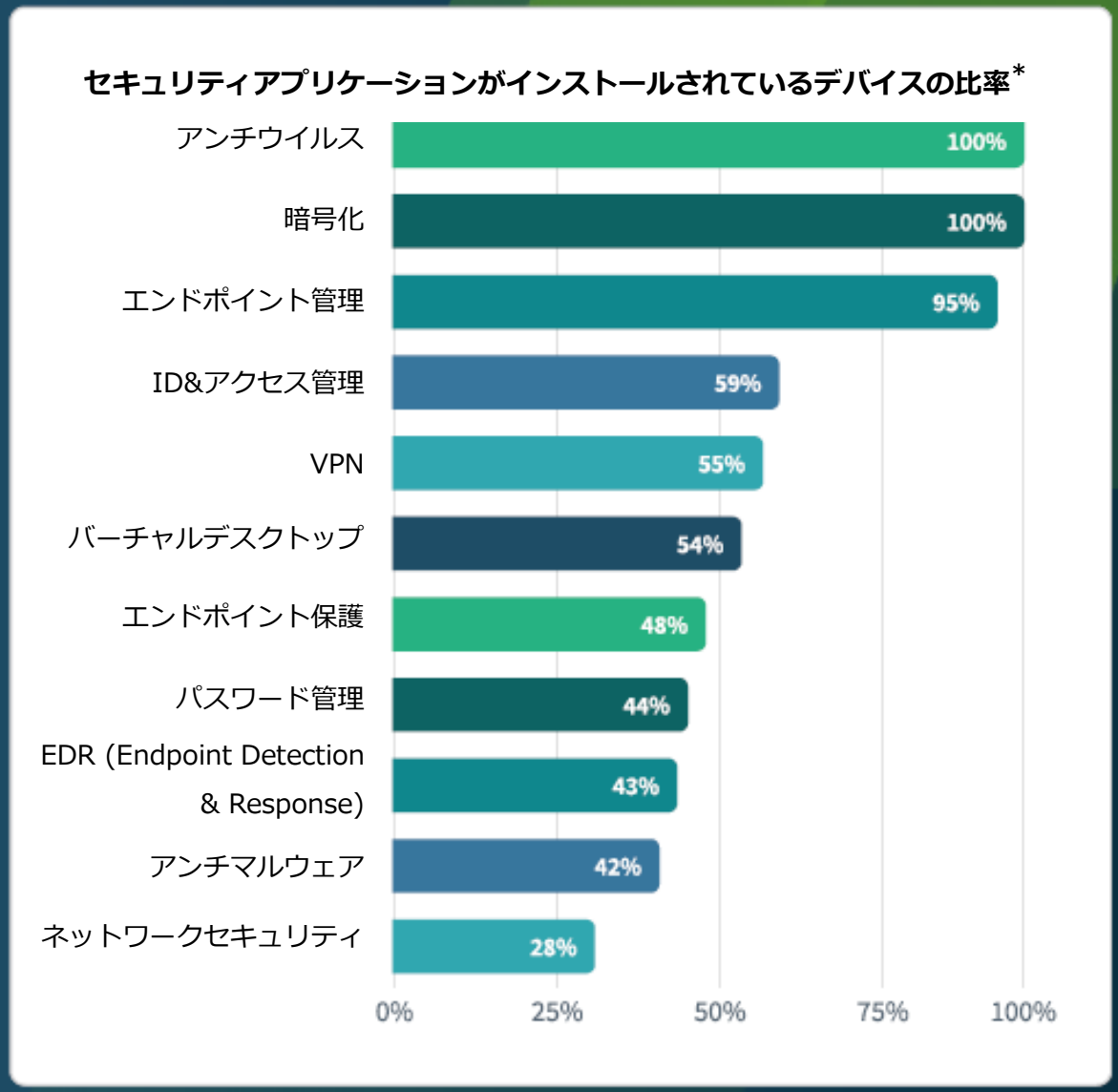
TREND 3

# エンドポイントの複雑化は リスクの増大を招く

リモートワーカーをサポートしセキュリティを確保しようとする中で、エンドポイントにインストールされるアプリケーションの平均件数は増加しました。その中で、不整合のリスク、エラー、コンプライアンス違反などの可能性も高まりました。

現在、組織はデバイスごとに平均96種類のアプリケーションを動作させており、そのうち13種類がミッションクリティカルなアプリケーションです。セキュリティ制御の数も増え、デバイスごとに平均11.7種類のアプリケーションが動作し、大多数のデバイスでは同じ機能を持つ複数の制御機能が含まれています。暗号化アプリケーションはデバイスの100%にインストールされており、2種類以上がインストールされているエンドポイントは60%です。エンドポイント管理制御は100%のデバイスで1種類、52%では3種類以上インストールされています。IMAは59%で1種類、11%では2種類以上です。

* Microsoft Defender AntivirusおよびBitLockerはすべてのWindowsデバイスに工場でインストールされています。



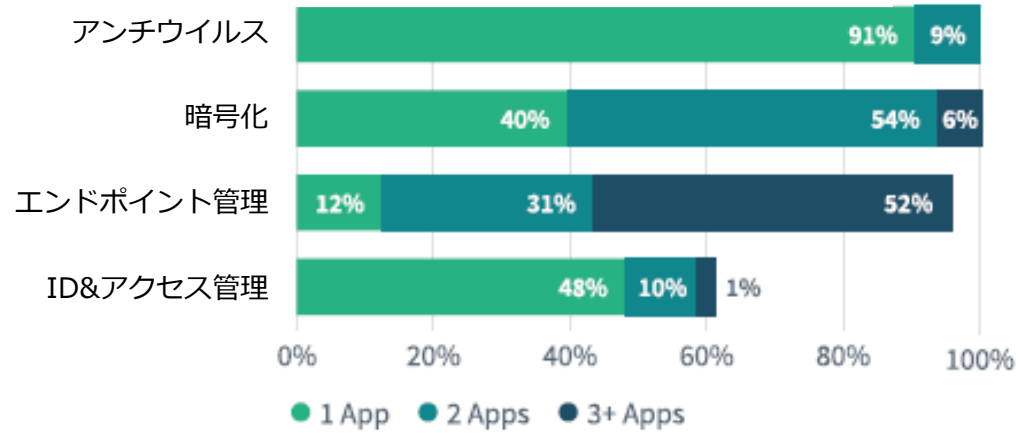
複雑化が進むことはそれ自体がセキュリティリスクです。新しく追加された制御機能はエンドポイント環境で軋轢を生みだし、競合や崩壊の危険性が高まるからです。アプリケーションの最新版をリモートでダウンロードするような場合（たとえばパッチをネットワーク外で展開するなど）にはリスクはさらに高まります。

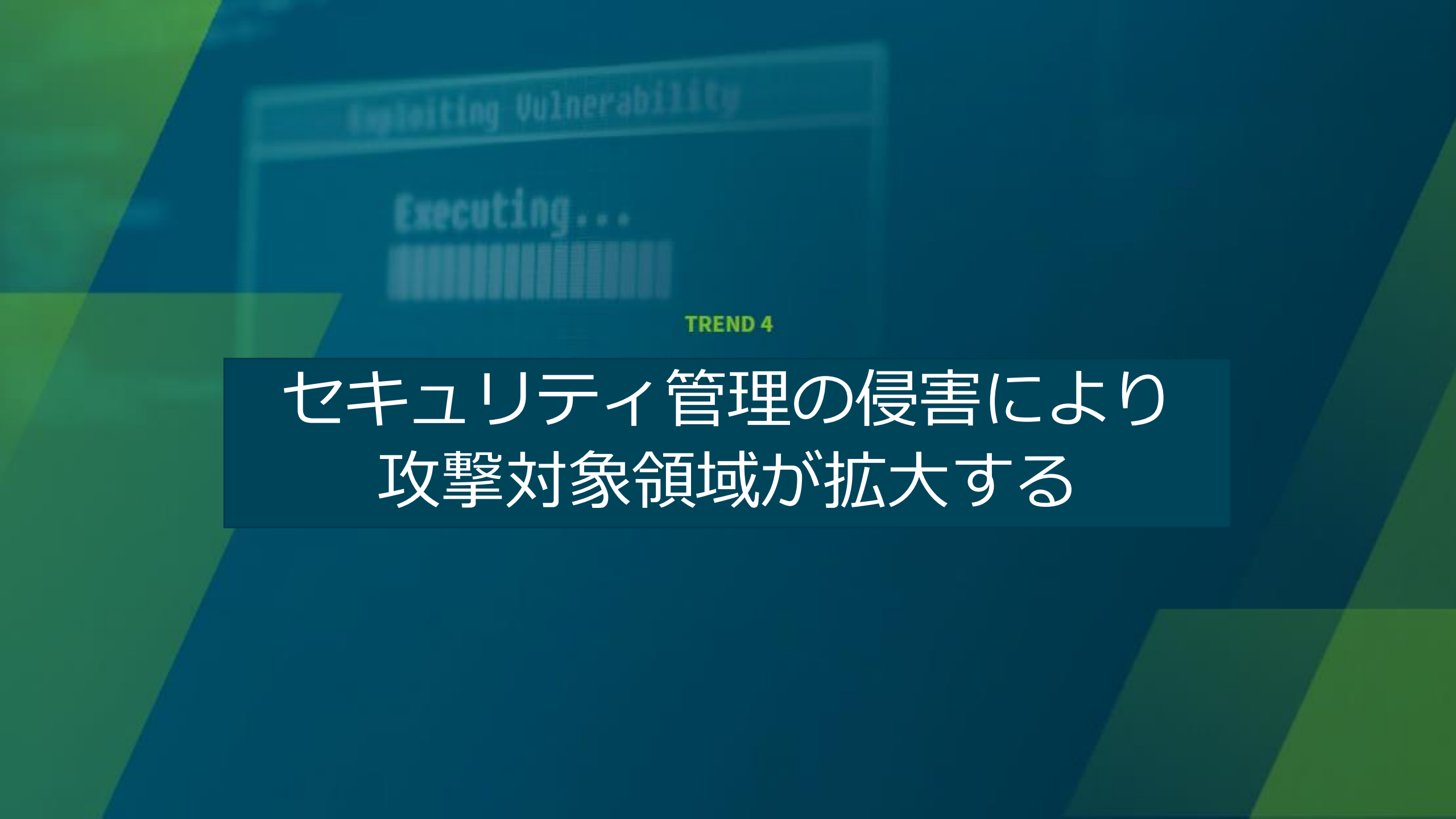
**60%** デバイスの60%に2種類以上の暗号化アプリケーションがインストールされている

**52%** デバイスの52%に3種類以上のエンドポイント管理ツールがインストールされている

**11%** デバイスの11%に2種類以上のIAMアプリケーションがインストールされている

**複数のセキュリティ制御が導入されているデバイスの比率（分野別）**






TREND 4

# セキュリティ管理の侵害により攻撃対象領域が拡大する

組織のセキュリティ体制の質は、そのために採用されているアプリケーションの質にかかっています。不適切なアプリケーションを導入していると、セキュリティチームの努力は無駄になりセキュリティ体制は弱体化します。

平均してエンドポイントごとに11.7種類導入されているセキュリティ管理アプリケーションのチェックをはずしたままにすると、そのすべてが潜在的な攻撃目的になってしまいます。複雑な環境では、セキュリティ制御機能同士が競合して保護機能が失われます。セキュリティ機能の有効性は時間の経過とともに目に見えて低下します。また、セキュリティ管理による制約を回避したいと考えるユーザーが、機能を無効化したり削除しようとしたりすることがあります。

高度な攻撃者は常に組織へのアクセスを狙っているので、暗号化、VPN、アンチウイルス、アンチマルウェアを単純に導入してその効果を信じるだけでは不十分です。エンドポイントを真に防御しセキュリティ対策への適切な投資対効果を得るためには、その有効性を継続的に監視し維持しなければなりません。

セキュリティ対策の適用が不十分な組織では、4台に1台のデバイスが重大なプロテクションを含めてアプリケーション上なんらかの不適合があると報告されています。

25%のデバイスのセキュリティ制御に課題があります。

- 34% アンチウイルス/アンチマルウェアが不適切
- 19% クライアント管理が不十分
- 22% 暗号化が不十分
- 27% VPNが不適切

「ビルトイン」は決して「より良い」を意味しません。MECM (Microsoft Endpoint Configuration Manager)* クライアントの21%は90日以内に修理や再インストールが必要でした。 BitLocker™と Microsoft Defender Antivirus の両方が導入されたデバイスの暗号化アプリケーションの有効性は全体中最も低いというレポートもあります。

デバイスの5台に1台でSCCMエージェントが正常に動作せず、90日以内に修理や再インストールが必要でした。

* SCCM (System Center Configuration Manager) の後継機能

# 時代に先んじて次へと進もう

IDCによると、調査対象の北米企業の3分の2以上が、リモートワークを行う従業員のフレキシビリティとセキュリティの両立に苦慮しているといいます[7]。

出張、対面での会議、あるいは新しいスタイルとなったWFA (work from anywhere: どこからでも職場にアクセス) があたりまえの世界へと進む中で、セキュリティ侵害を発生させない場所を知ることは重要です。

今年のレポートで取り上げた4つのトレンド（未対処の脆弱性、未保護のデータ、エンドポイントの複雑性、セキュリティ制御の破綻）は、先進の業務環境でのリスクの特定と軽減におけるデバイスの可視性とインテリジェンスが重要な役割を果たすことを示しています。

7 Remote Work in the COVID-19 Era: Accelerating Work Transformation: IDC　2020年

# 常に正確なエンドポイントテレメトリ、常に動作するエンドポイント制御

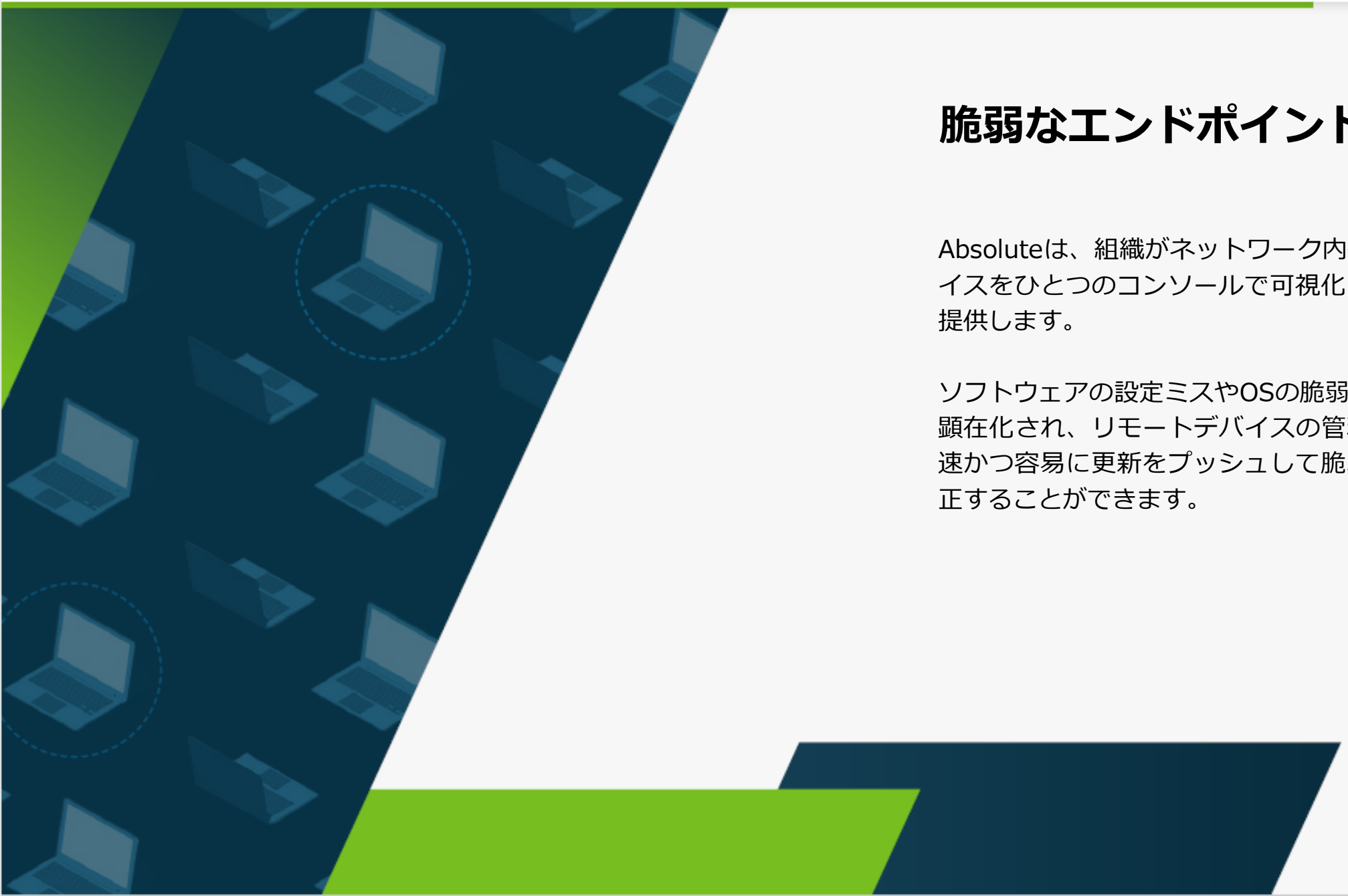
Forresterのレポートによると、組織の71%はリモートエンドポイントの検知と監視の機能を拡張しようとしているといいます[8] 。

これを達成するための基本は、死角を排除し、弱点を特定し、脅威を迅速に軽減するために必要なインサイト(洞察)と制御を提供するエンドポイントテレメトリ (遠隔測定) です。

Absoluteが維持するすべてのデバイスからのインテリジェンスストリームには詳細な地理的位置データ、機密データの検出、セキュリティ制御ステータス、ハードウェアパフォーマンス、ソフトウェアインベントリ、数百におよび追加のデータポイントなどが含まれます。チームはそれらのインテリジェンスを使用してセキュリティ体制を測定し、ほぼリアルタイムでインシデントを修正できます。

デバイスはネットワークの内外で監視され、データはSIEM (Security Information and Event Management: セキュリティ情報イベント管理) システムに容易に統合され、さらなる強化や調査が行われます。

8 Take a Proactive Approach to Endpoint Security: Absoluteの依頼によりForrester Consultingが実施した委託調査　2020年



# 脆弱なエンドポイントを特定

Absoluteは、組織がネットワーク内外のあらゆるデバイスをひとつのコンソールで可視化し管理する機能を提供します。

ソフトウェアの設定ミスやOSの脆弱性が自動的に識別、顕在化され、リモートデバイスの管理機能によって迅速かつ容易に更新をプッシュして脆弱性を大規模に修正することができます。

# 機密データを含むデバイスを検知し、修正

リモートワークが現実となった中、今年の機密データ侵害リスクへの懸念を鑑みると、あらゆるセキュリティ専門家にとって、当面はデータのリスク管理が最重要課題になりそうです。

Absoluteによって組織のあらゆるエンドポイント環境上に存在する機密情報を識別、監視、保護することができます。場所と分類のデータはデバイスの暗号化ステータスなどの重要な情報と一緒に表示されます。

リモート修復機能にはデバイスをフリーズやロックする機能、暗号化消去によってデータの取得を不可能にする機能などが含まれます。

コンソールで生成されるサニタイズ証明書は、政府、金融サービス、ヘルスケアなどの分野で重要となるNISTおよびHIPAAの要件に対応します。

# エンドポイントの複雑性を低減

リモートワークが一般化する前から、複雑化するエンドポイント環境の管理は組織にとっての大きな課題でした。リモートワークをサポートしつつ組織のデータを安全に保護するために購入し展開されるアプリケーションの数も増加しています。

現在、組織のデバイスあたり平均12.9種類のミッションクリティカルなアプリケーションが導入されており、そのうちセキュリティ制御は平均11.7種類にのぼります。エンドポイントの複雑化が進むにつれて、アプリケーションが競合して互いに競合するケースも増えています。

Absoluteを採用することで、組織内のデバイスの可視性が高まり、最も脆弱なアプリケーションを特定することができます。Absoluteの自己修復機能を最も重要なアプリケーションに拡張して、ミッションクリティカルな制御を維持しつつ、生産性やセキュリティの課題を回避することも可能です。

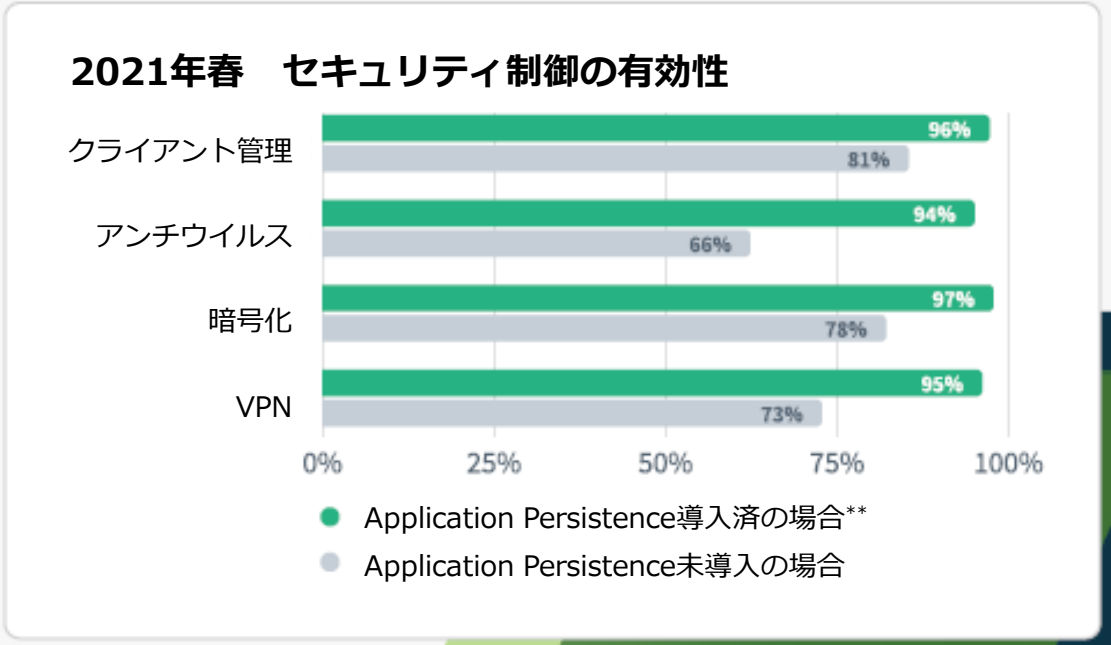
# セキュリティ管理の有効性を評価

従業員の過失または悪意、あるいは物理的なセキュリティ侵害のいずれであっても、データ侵害の大部分はエンドポイントから発生します[9] 。

そんな中で組織が取り組むべき課題は、監視されていないセキュリティ制御の把握と管理です。 Absolute の Application Persistence™は、セキュリティ制御の有効性を継続的に測定することでそれを維持し*、セキュリティが侵害された場合に制御を強化して自動的に修復または再インストールします。

AbsoluteのApplication Persistenceを実行しているデバイスは、実行していないデバイスよりも21%高いセキュリティ制御の有効性を報告します。

Application Persistenceは40種類のエンドポイントセキュリティ制御に対応し、今後さらに拡張される予定です。




9 2020 Cost of Data Breach Report:　Ponemon Institute　2020年
* 有効性は、制御の現在の状態と減衰の状態および攻撃、競合や損傷に反応する機能によって測定されます。
** AbsoluteのApplication Persistence™サービスを実装するお客様でのトップパフォーマンス

# セキュリティ＋回復＝安心

避けられないサイバーインシデントに直面した場合でも、AbsoluteのEndpoint Resilience™が組織のエンドポイント環境を守ります。Endpoint Resilienceは、エンドポイントとそのセキュリティ制御が安全な動作状態を自律的に維持する機能です。可視性と制御の機能が確保され、セキュリティのために投資したアプリケーションが、導入時に意図したとおりに機能して組織を守ります。

Absoluteが特許を持つPersistence®テクノロジーは、Dell、Lenovo、HPを含む28社のシステムメーカーのファームウェアに組み込まれています。

Absoluteのエージェントをアクティブ化すると、エンドポイントが潜在的な脅威を自動的に検出して回復できるようにするハードウェアレベルのインテリジェンスを使用して、ネットワーク内外のすべてのエンドポイントへの安全で破壊不可能なコネクションが確保されます。

組織のスタックを
どうやって把握したら
よいでしょうか？

カスタムデモをご予約いただき、
貴組織のリスクをどう特定するかを
ご覧ください。

**お問い合わせはこちら**
**Sales-Japan@absolute.com**

## 分析方法

北米および欧州の13,000件以上のお客様のAbsoluteが動作する約500万台のデバイスからの匿名化されたデータと、信頼できるサードパーティからのデータと情報を分析しています。

## Absoluteについて

Absolute Platform for Endpoint Resilience®をご導入いただくことにより、ユーザーの介在なしにデバイスとセキュリティ制御の安全な運用状態が自動的に維持されます。Absoluteは5億台を超えるデバイスのファームウェアに組み込まれており、データ、デバイス、アプリケーションなどのエンドポイント環境全体の継続的な可視性、制御、およびインテリジェンスを提供します。自己修復接続ときめ細かいエンドポイントテレメトリにより、お客様のデバイス管理を合理化、コンプライアンスの維持、脅威の修正を支援します。エンドポイントセキュリティ管理が常にインストールされ効率的な管理が行われることで、意図したROIが実現されます。

ABSOLUTE.COM SALES@ABSOLUTE.COM NORTH AMERICA | EMEA

Linkedin Twitter Youtube

# Endpoint Resilienceの自己回復機能でデバイスを保護

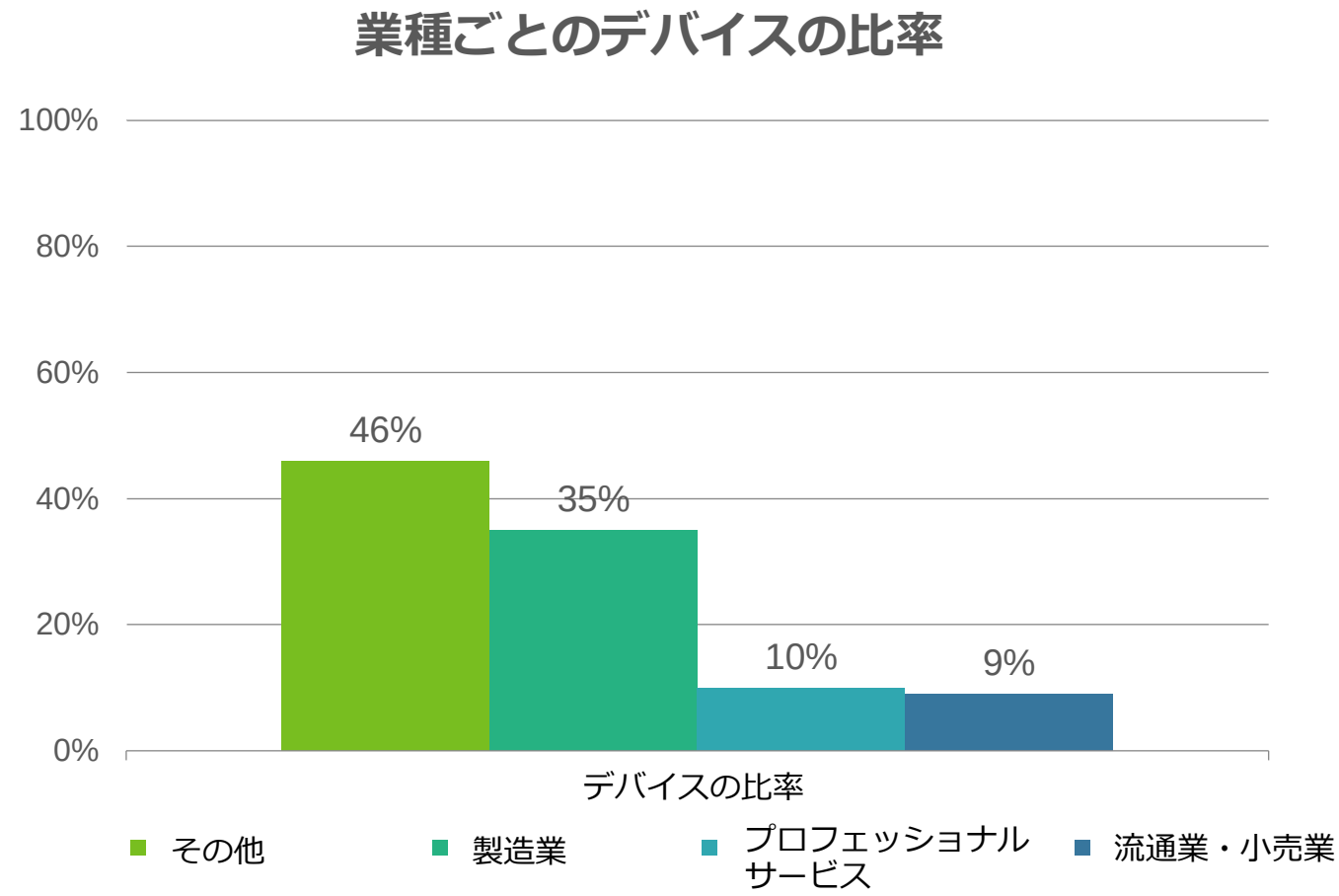
Emailまたはお電話にてご連絡ください。
E. Sales-Japan@absolute.com T. 03-6427-1976

# Appendix
# 日本におけるデバイスデータの調査結果

# 多くの日本の組織では、デバイスが所属する業種は「その他」に分類されている

## デバイスの3分の1以上が「製造業」に分類

デバイスは「製造業」「プロフェッショナルサービス」「流通業・小売業」「その他」の４種類のいずれかに分類することができます。日本の組織のデバイスは、46%が「その他の組織」、35%が「製造業」として分類されています。



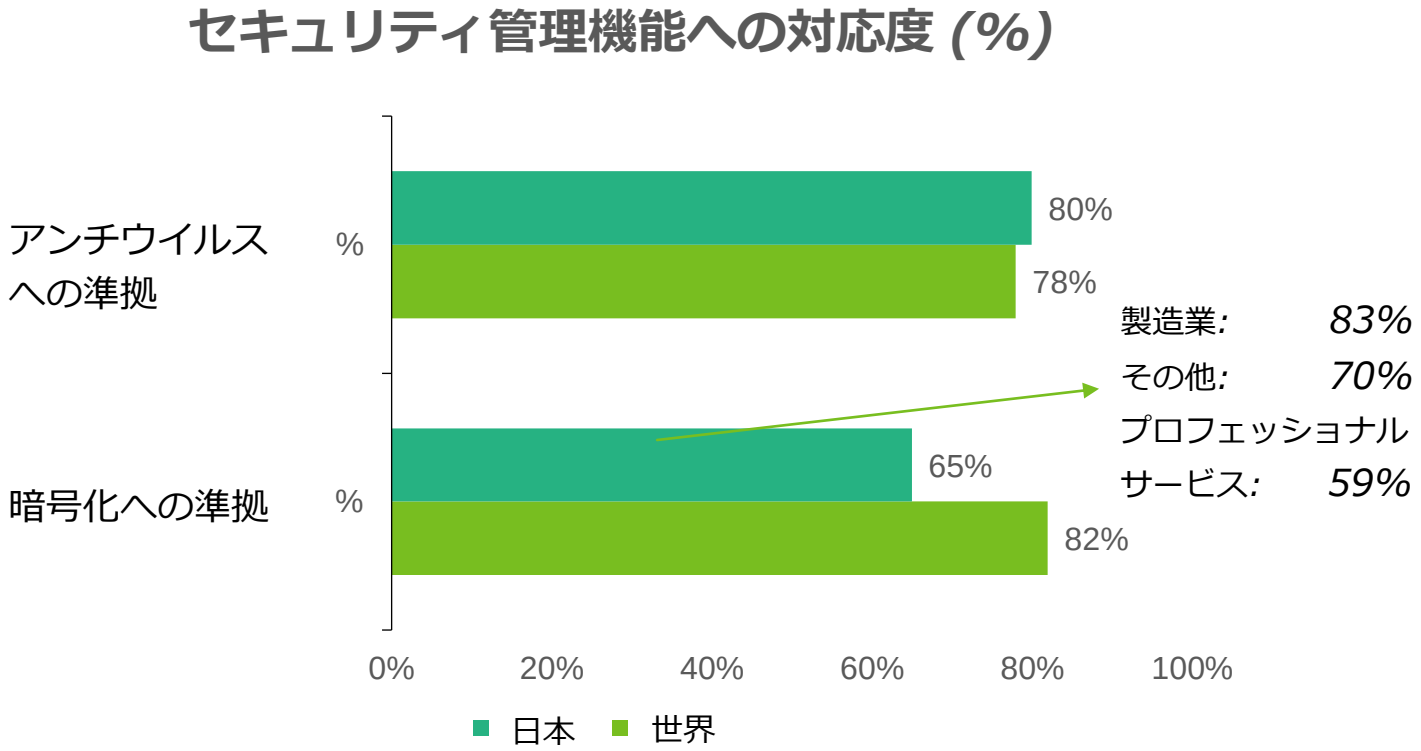

*2021年10月1日時点のデータ。30日間にアクティベートされたデバイス (21,000台中17,000台)*

# 日本の組織のデバイスセキュリティ管理の内部統制対応は、世界に比べて強化されている部分と遅れている部分がある

## アンチウイルスへの対応は進んでいるが、暗号化への対応は遅延

セキュリティ管理機能へのコンプライアンス状況を世界の組織と比較してみると、日本はアンチウイルスへのコンプライアンス対応度が80%であり、世界平均の78%に比較すると若干強化されていることがわかります。

その一方で、暗号化へのコンプライアンス状況を確認すると、世界平均が82%であるのに対して日本は65%と、かなり遅れていることがわかります。業種別でみると、製造業に分類されているデバイスでは83%、その他のデバイスが70%、プロフェッショナルサービスでは59%が暗号化機能を実装しています。

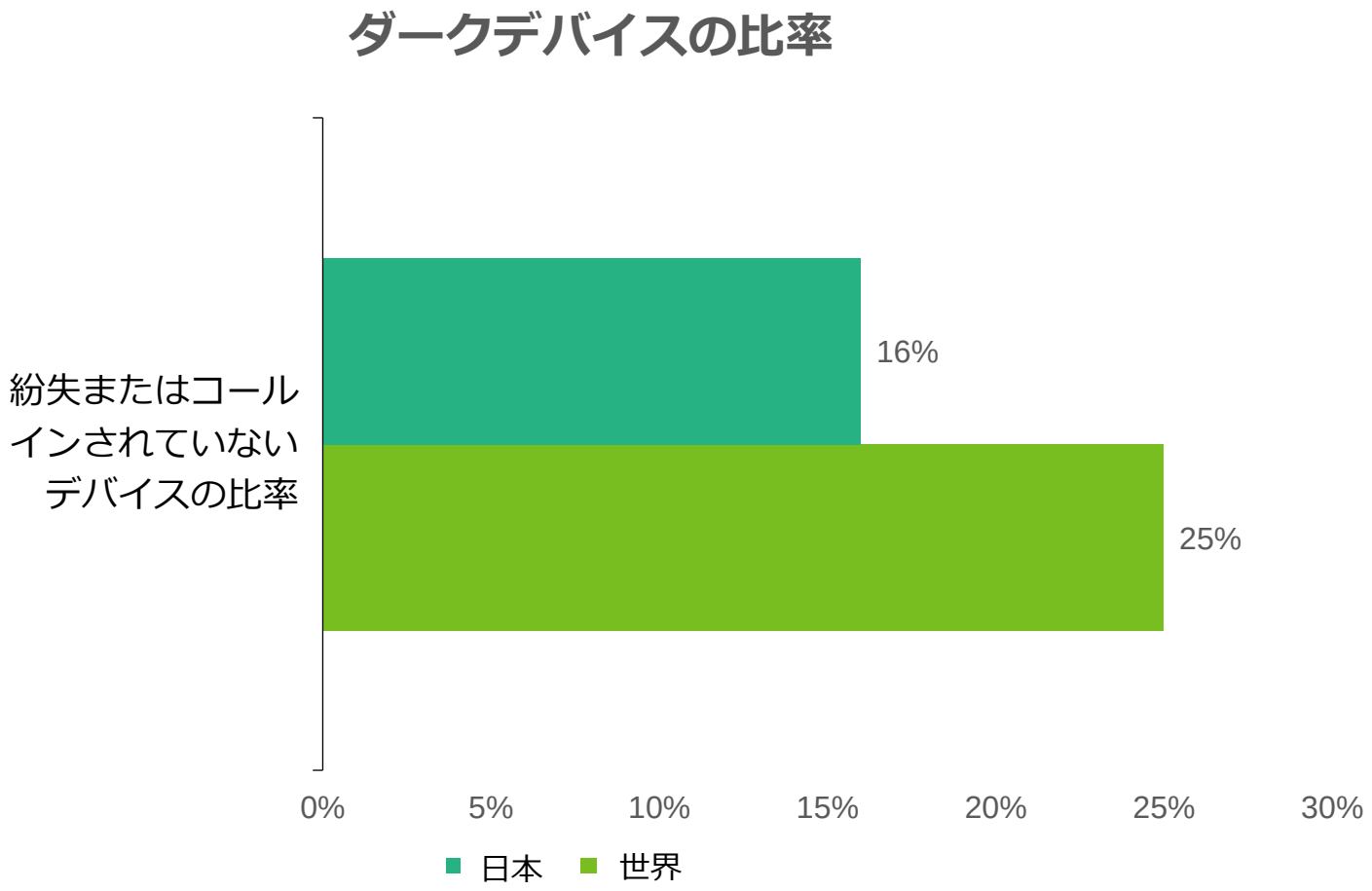



世界: 2021年8月10日時点のデータ。30日間にアクティベートされたデバイス (3,800,000台)

日本: 2021年10月1日時点のデータ。30日間にアクティベートされたデバイス (21,000台中17,000台)

# 日本のダークデバイスの比率は世界の平均よりも低い

紛失や、コールインされていないデバイスの比率をみると、世界の25%に対して日本は16%と、低い値がでています。このことは、紛失や盗難されたダークデバイスが他国に比べて低いことを表します。




世界: *2021*年*8*月*10*日時点のデータ。*30*日間にアクティベートされたデバイス *(3,800,000*台*)*

日本: *2021*年*10*月*1*日時点のデータ。*30*日間にアクティベートされたデバイス *(21,000*台中*17,000*台*)*

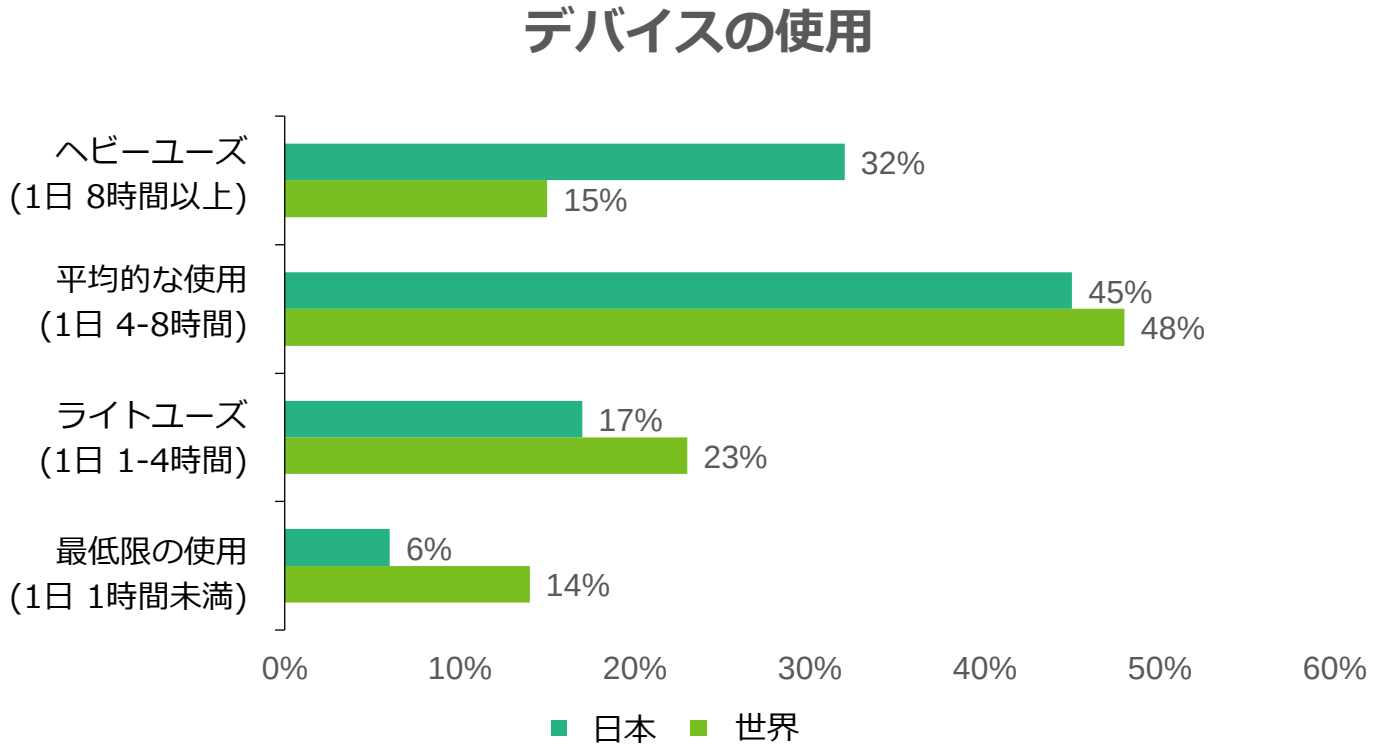
# 日本のデバイスの稼働状況は高い

## 日本のデバイスの稼働率は他国平均の2倍以上

デバイスの稼働状況を見てみましょう。日本のデバイスで1日8時間以上使用されているものは、他国の平均15%に比べて32%と、倍以上の数値を示しています。

その一方で、平均的な使用時間（1日4-8時間）を比較すると、世界の48%に比べて45%、ライトユーズ（1日1-4時間）は世界の23%に比べて17%、最低限の使用（1日1時間未満）は世界の14%に比べて6%と、いずれのケースでも世界に比べて低い比率を示し、特に最低限の使用にとどまるデバイスは世界の半分以下の比率を示します。

総じて、日本のデバイスは世界に比べて2倍以上、稼働しているとみることができます。




世界: *2021年8月10日時点のデータ。30日間にアクティベートされたデバイス (3,800,000台)*

日本: *2021年10月1日時点のデータ。30日間にアクティベートされたデバイス (21,000台中17,000台)*