IDC ANALYZE THE FUTURE



COVID-19で加速するデジタル変革と高まるリスク

登坂 恒夫
リサーチマネージャー
IDC Japan

July 29, 2020

IDCは、ICT（情報通信技術）に関する調査・分析、アドバイザリーサービスおよびイベントをグローバル規模で提供



© IDC

Agenda

- デジタル変革によるデータへの信頼の重要性
- 新型コロナウイルス感染症（COVID-19）の影響下でセキュアなリモートワークを実現するために
- 提言

© IDC Visit us at IDC.com and follow us on Twitter: @IDC

デジタル変革によるデータへの信頼の重要性

© IDC Visit us at IDC.com and follow us on Twitter: @IDC

デジタル変革によるデータへの信頼の重要性

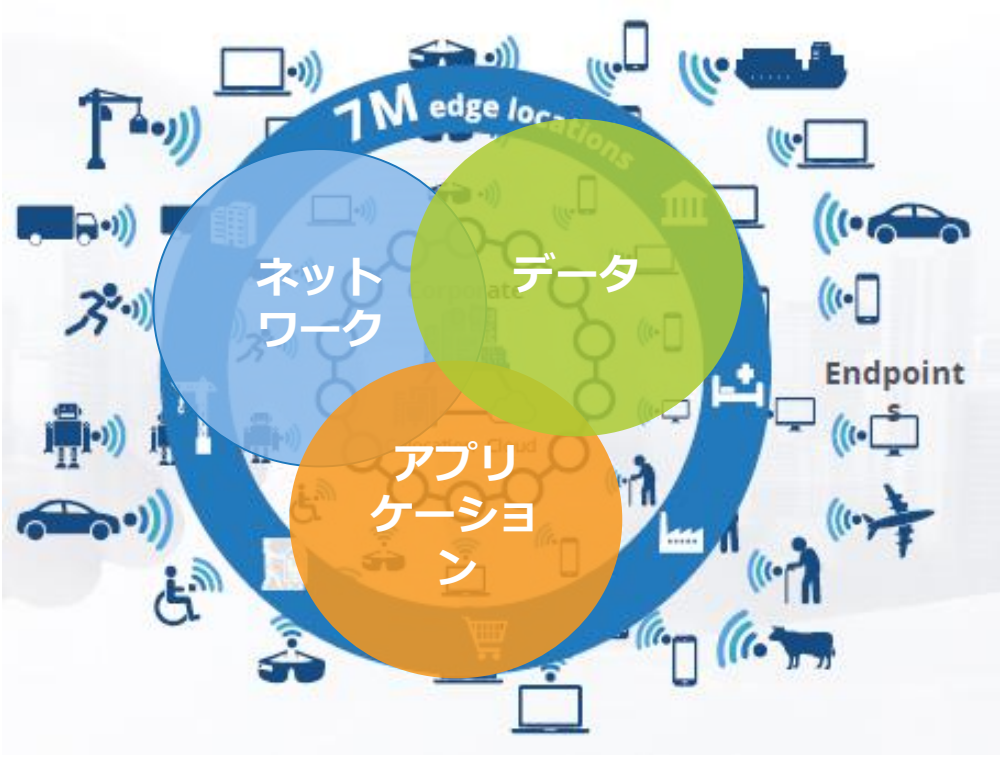
第２のプラットフォーム

デジタル変革

第3のプラットフォーム



データ量増大と
データ活用拡大



Source: IDC Japan, July 2020

© IDC

デジタル変革によるデータへの信頼の重要性

第２のプラットフォーム

デジタル変革

第3のプラットフォーム





2020年には50ZBのデータが世界中で生成される

データ量増大と
データ活用拡大

データへの「信頼」が重要となる

Source: IDC Japan, July 2020

IDC ANALYZE THE FUTURE

© IDC

ワークスペースの高度化による業務効率向上

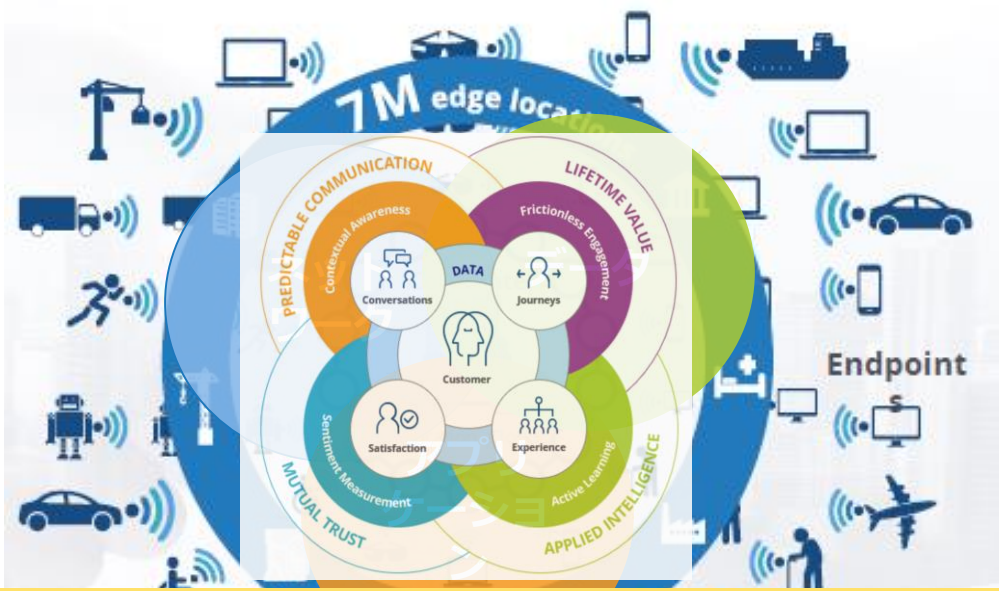
企業の内部プロセス 顧客中心のオペレーション	顧客中心の ソリューション設計	企業の外部プロセス 顧客中心のエンゲージメント

顧客データ、アナリティクスをベースにしたコンテンツ流通

第3のプラットフォーム上で展開されるワークスペース

バックオフィス

- **BPM**ソフトウェア
- **HCM**アプリケーション
- **SCM**アプリケーション
- 製造アプリケーション
- 在庫管理アプリケーション
- 財務管理アプリケーション
- 研究開発
- 製品設計



チャネル

- マルチチャネルマーケティング
- デジタルセールス
- エクスペリエンスマーケティング
- **Web**サイト／アプリ
- コミュニティサポート
- 顧客サービス
- コンタクトセンター
- デジタルコマース

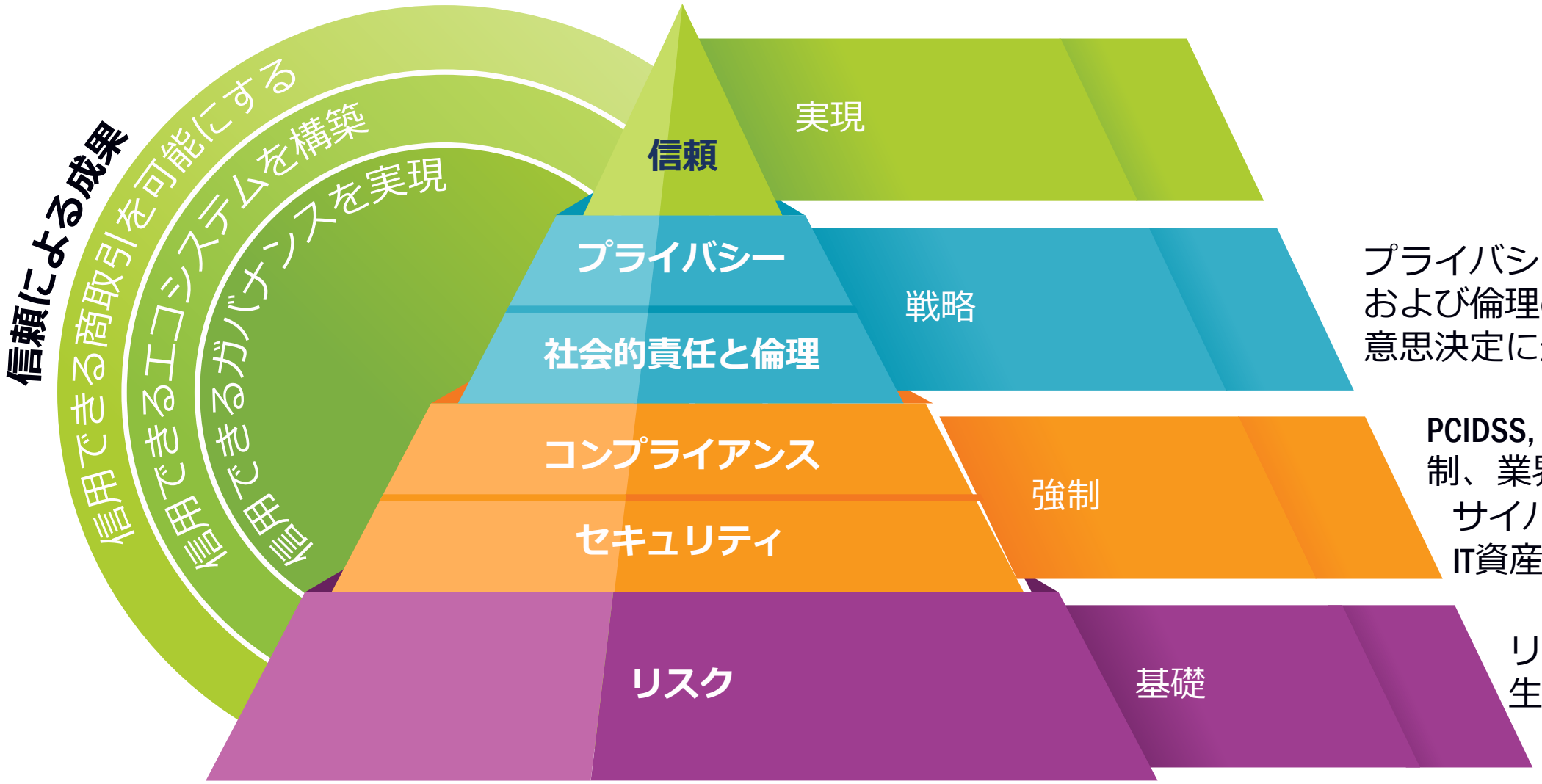
社内だけでなく、社外との活用も加速し業務効率を向上させる役割を果たす

Source: IDC Japan, July 2020

IDC ANALYZE THE FUTURE

© IDC

デジタル変革で求められるデータへの信頼



プライバシー、社会的責任および倫理の活動が組織の意思決定に影響を及ぼす

PCIDSS, HIPPA, GDPRなど法規制、業界規制対応
サイバーセキュリティ
IT資産の保護

リスク = 可視性 x 発生確率 x 重要性

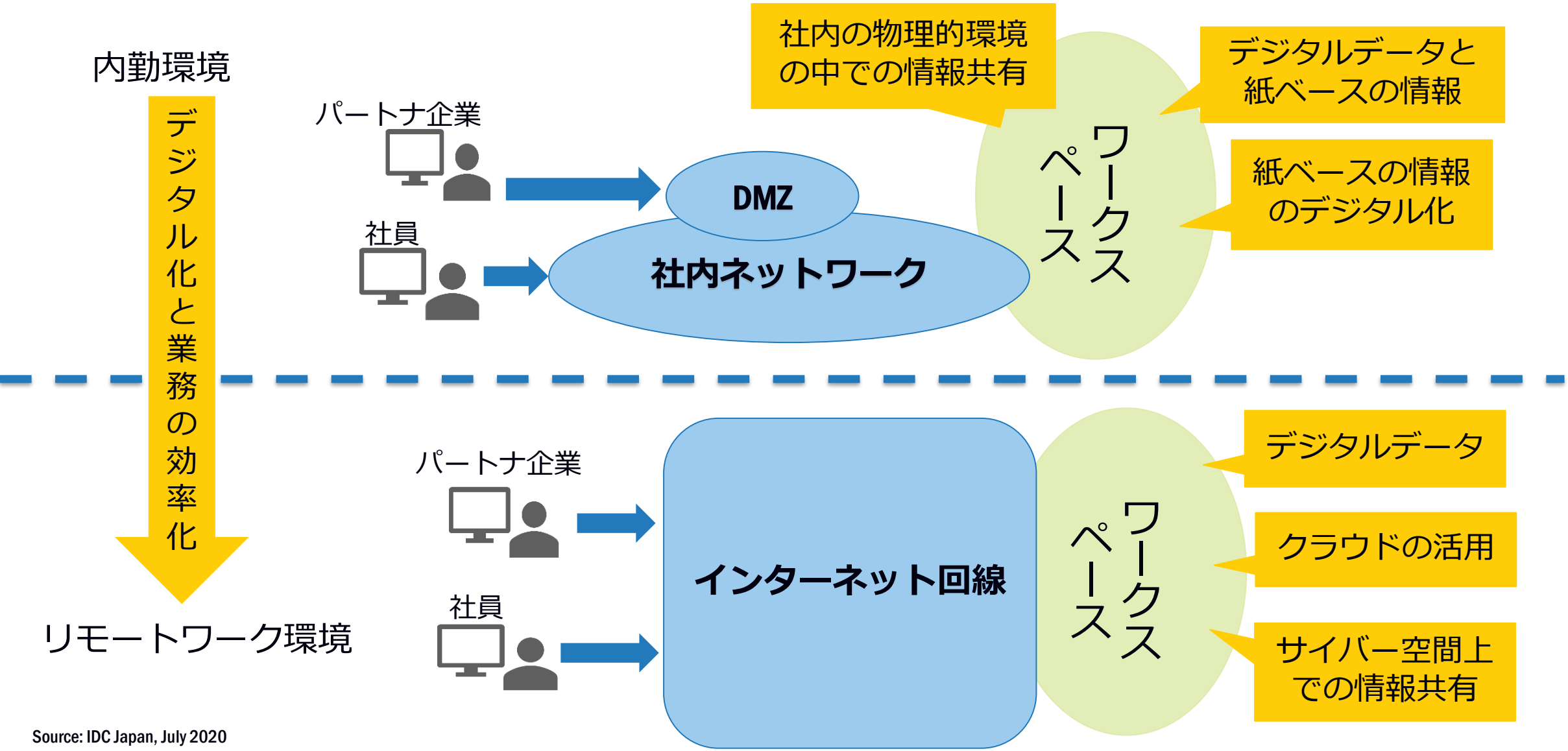
Source: IDC Japan, July 2020

© IDC

新型コロナウイルス感染症（COVID-19）の影響下でセキュアなリモートワークを実現するために

© IDC Visit us at IDC.com and follow us on Twitter: @IDC

リモートワークによるデジタル化と効率化の加速



Source: IDC Japan, July 2020

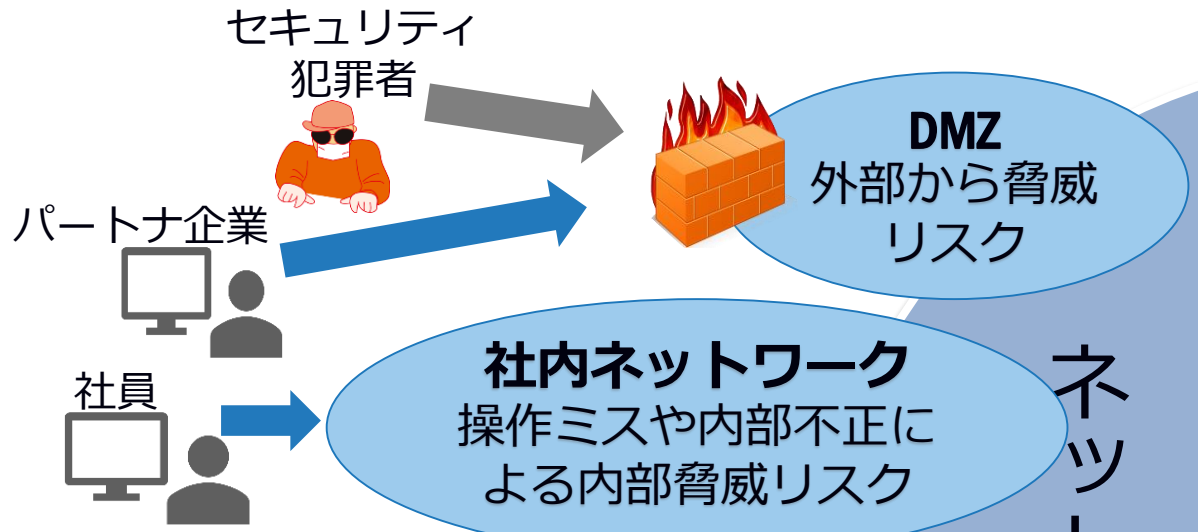
© IDC

リモートワークで高まるセキュリティリスク

内勤環境

内部脅威リスクは、性善説によって低くみている

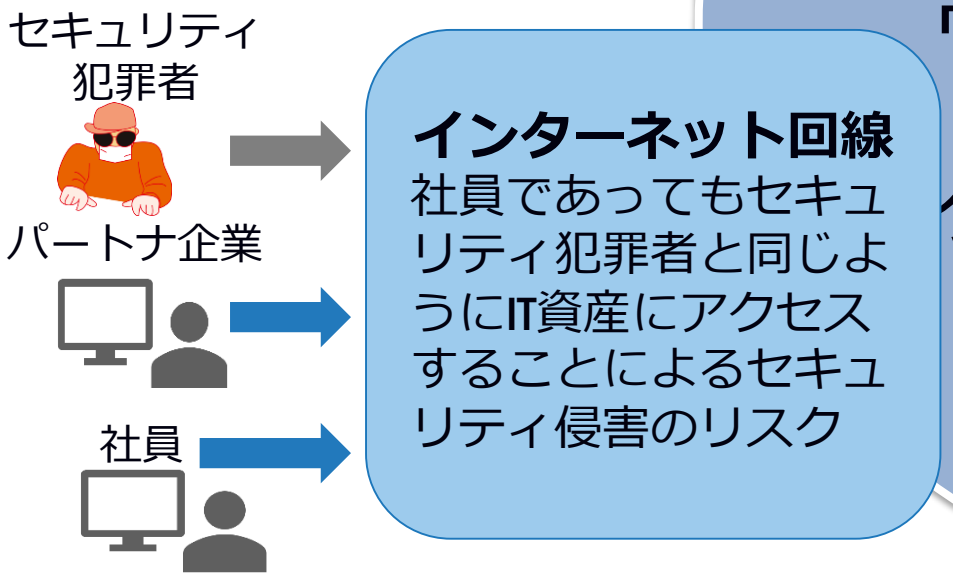
セキュリティリスクは、DMZを経由する外部からの脅威リスクが中心である

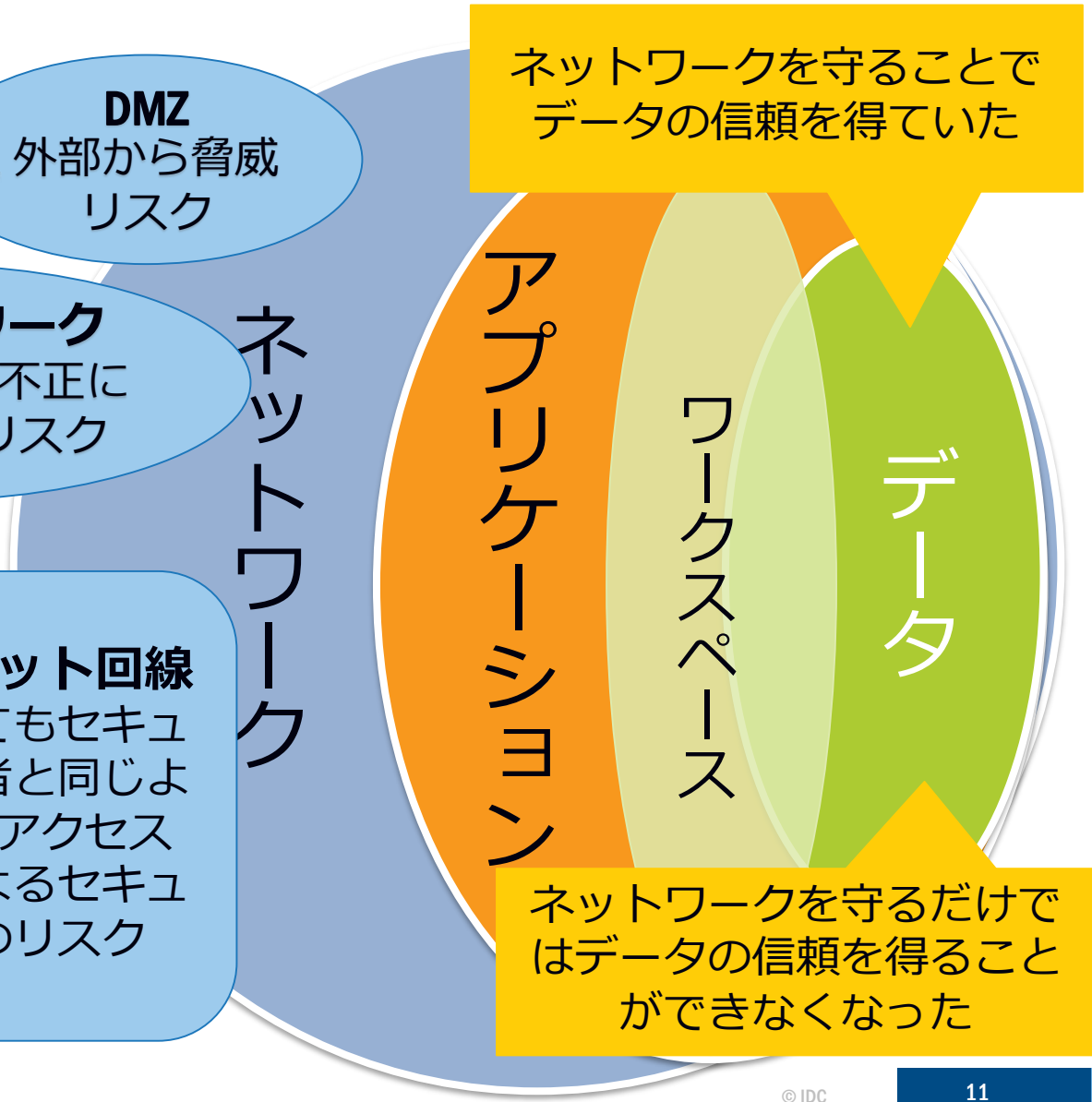


リモートワーク環境

境界防御が機能しなくなった

セキュリティリスクは、IT資産にアクセスする全てのユーザーが脅威対象となる





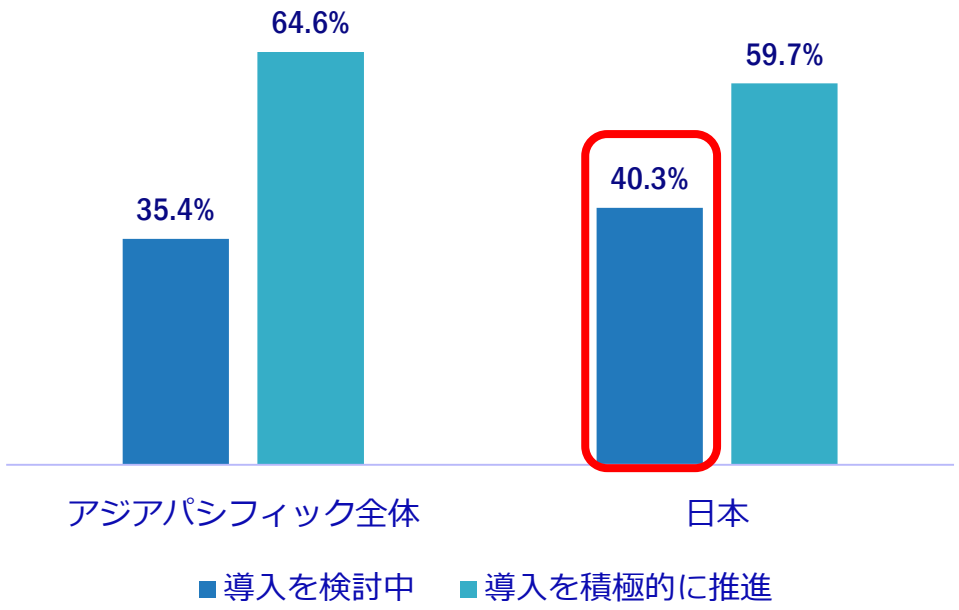
Source: IDC Japan, July 2020

IDC ANALYZE THE FUTURE

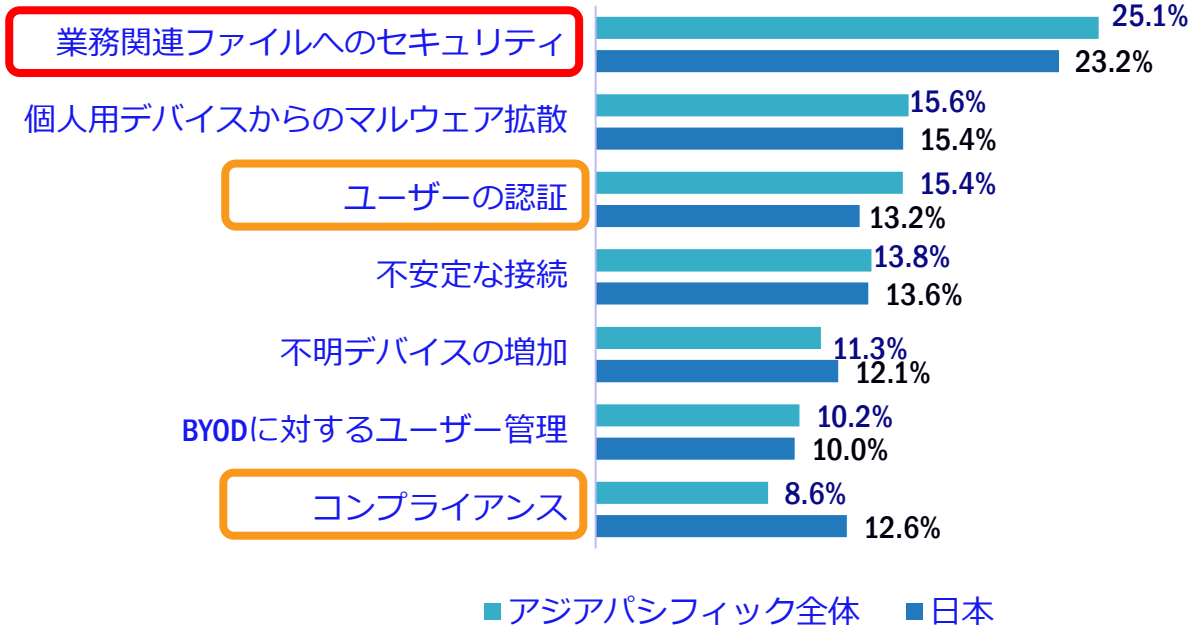
© IDC

リモートワークに対する技術導入需要とセキュリティへの懸念

リモートワーク技術の導入需要



リモートワークでのセキュリティへの懸念



日本は、一部の企業でまだリモートワークに対して消極的である。またリモートワークでの業務関連ファイルに対するセキュリティを懸念している企業が多い

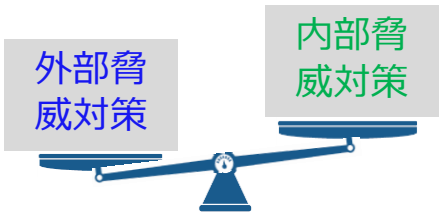
Source：IDC-Citrix Business Continuity Flash Study, 2020 (N=342 Asia/Pacific, 77 Japan)

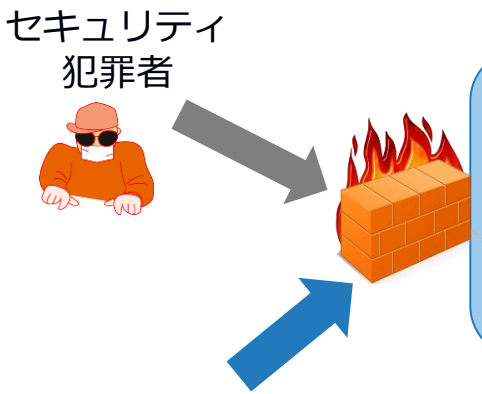
© IDC

境界防御の限界で複雑化するセキュリティ対策
COVID-19前（内勤環境）

ユーザーである社員に対して信用しているため、外部脅威対策中心である

性善説による対策



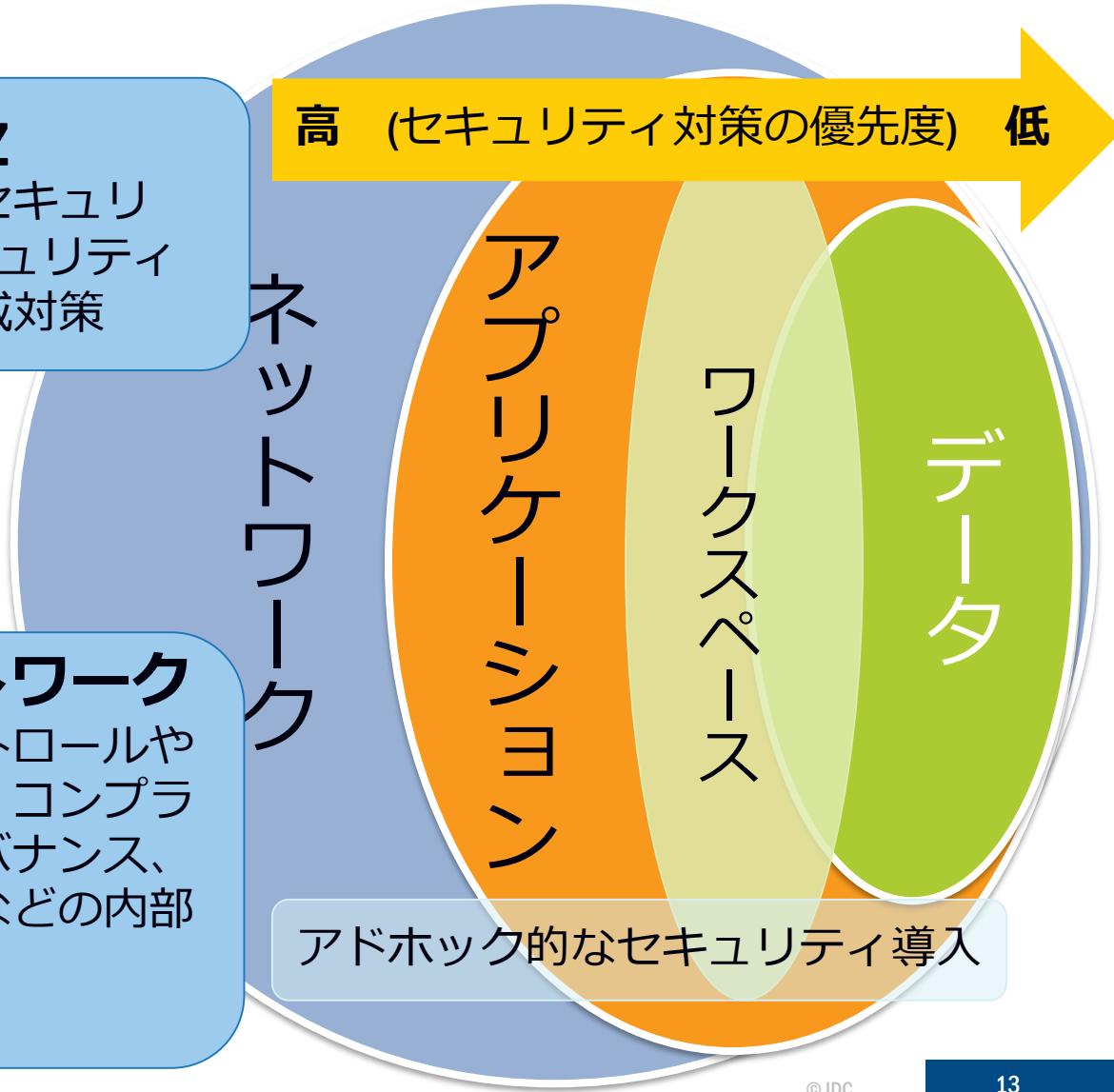


DMZ
ネットワークセキュリティやWebセキュリティなどの外部脅威対策



エンドポイントセキュリティ

社内ネットワーク
アクセスコントロールやポリシー管理、コンプライアンス／ガバナンス、情報漏洩対策などの内部脅威対策



Source: IDC Japan, July 2020

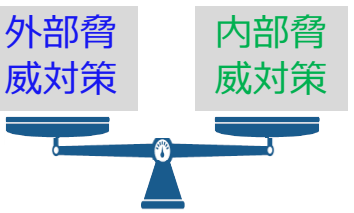
© IDC

境界防御の限界で複雑化するセキュリティ対策
COVID-19後（リモートワーク環境＝デジタル化）

アクセスする全て端末とユーザーをリスク対象としたセキュリティ対策

性悪説による対策

外部脅威対策　内部脅威対策



セキュリティ犯罪者



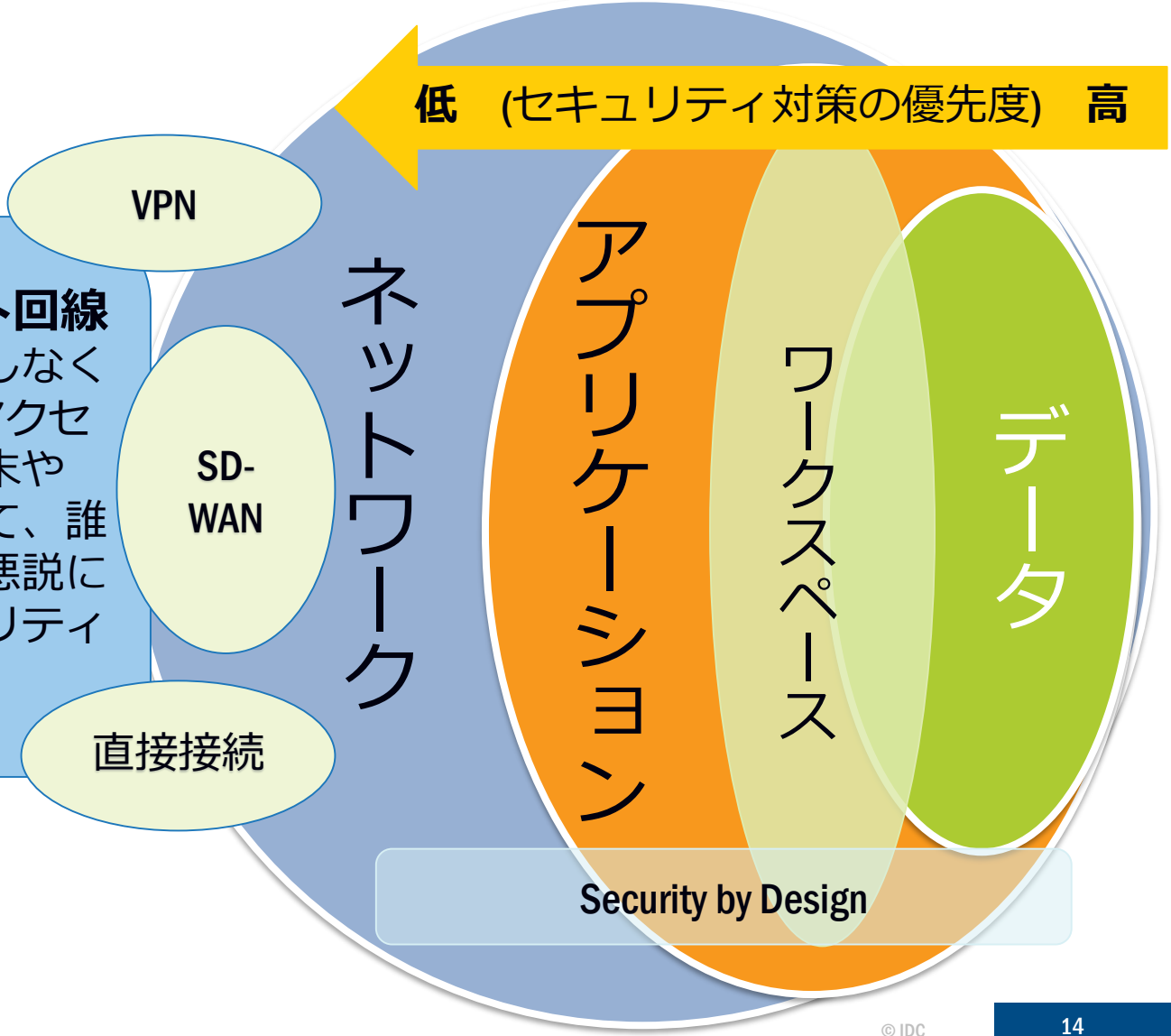
パートナー顧客



社員



インターネット回線
境界防御が機能しなくなり、IT資産にアクセスする全ての端末やユーザーに対して、誰も信用しない性悪説に基づいたセキュリティ対策が必要



Source: IDC Japan, July 2020

IDC ANALYZE THE FUTURE

© IDC

複雑化を集約化するパーベイシブセキュリティ

性悪説に基づいたセキュリティ
（総合的対策で複雑化）
- エンドポイントセキュリティ
- アクセスコントロール
- クラウドアプリケーションの防御と可視化
- 情報漏洩対策
- コンプライアンス対応と情報ガバナンス強化
- バックアップ／リカバリー

など

パーベイシブセキュリティ
（集約されたセキュリティ）

安心安全なデータ活用の実現

- ポリシーの統合化
- 管理コンソールの一元化
- レポーティングフレームワークの統合化
- テレメトリーの共有化
- コンテンツインスペクション
- プロアクティブ監視

運用の効率化と対処の迅速化

信頼できるワークスペースの構築

Source: IDC Japan, July 2020

IDC ANALYZE THE FUTURE

© IDC

リモートワークで必要なテクノロジー

リモートワーク技術導入を検討する上で必要なテクノロジーは何ですか？（回答率）

		TOTAL	ANZ	ASEAN	China	India	Japan
Multi-factor authentication	Column N %	53.5%	38.2%	58.5%	26.2%	58.8%	77.9%
Virtual Private Networking	Column N %	54.7%	30.9%	61.7%	43.1%	62.7%	67.5%
Firewall	Column N %	59.6%	49.1%	61.7%	61.5%	37.3%	77.9%
Endpoint protection	Column N %	50.3%	29.1%	59.6%	38.5%	39.2%	71.4%
End user monitoring/User Behaviour Analysis	Column N %	52.3%	40.0%	53.2%	40.0%	54.9%	68.8%
Network monitoring	Column N %	58.2%	49.1%	67.0%	41.5%	60.8%	66.2%
Increase internal capacity to ensure system availability	Column N %	45.6%	38.2%	52.1%	40.0%	58.8%	39.0%
Intrusion prevention and intrusion detection systems	Column N %	47.4%	30.9%	45.7%	52.3%	45.1%	58.4%
Virtual desktop infrastructure	Column N %	43.0%	34.5%	51.1%	33.8%	52.9%	40.3%
Network load balancing and Management	Column N %	42.7%	29.1%	46.8%	36.9%	39.2%	54.5%
Data loss prevention solutions	Column N %	54.7%	45.5%	63.8%	55.4%	49.0%	53.2%
Collaboration content security	Column N %	50.0%	36.4%	57.4%	49.2%	39.2%	58.4%
Governance, Risk and Compliance management	Column N %	47.4%	40.0%	57.4%	43.1%	37.3%	50.6%
Single Sign-On	Column N %	35.4%	30.9%	40.4%	26.2%	19.6%	50.6%
Other, please specify	Column N %	0.6%	0.0%	0.0%	0.0%	0.0%	2.6%
Total	Count	342	55	94	65	51	77

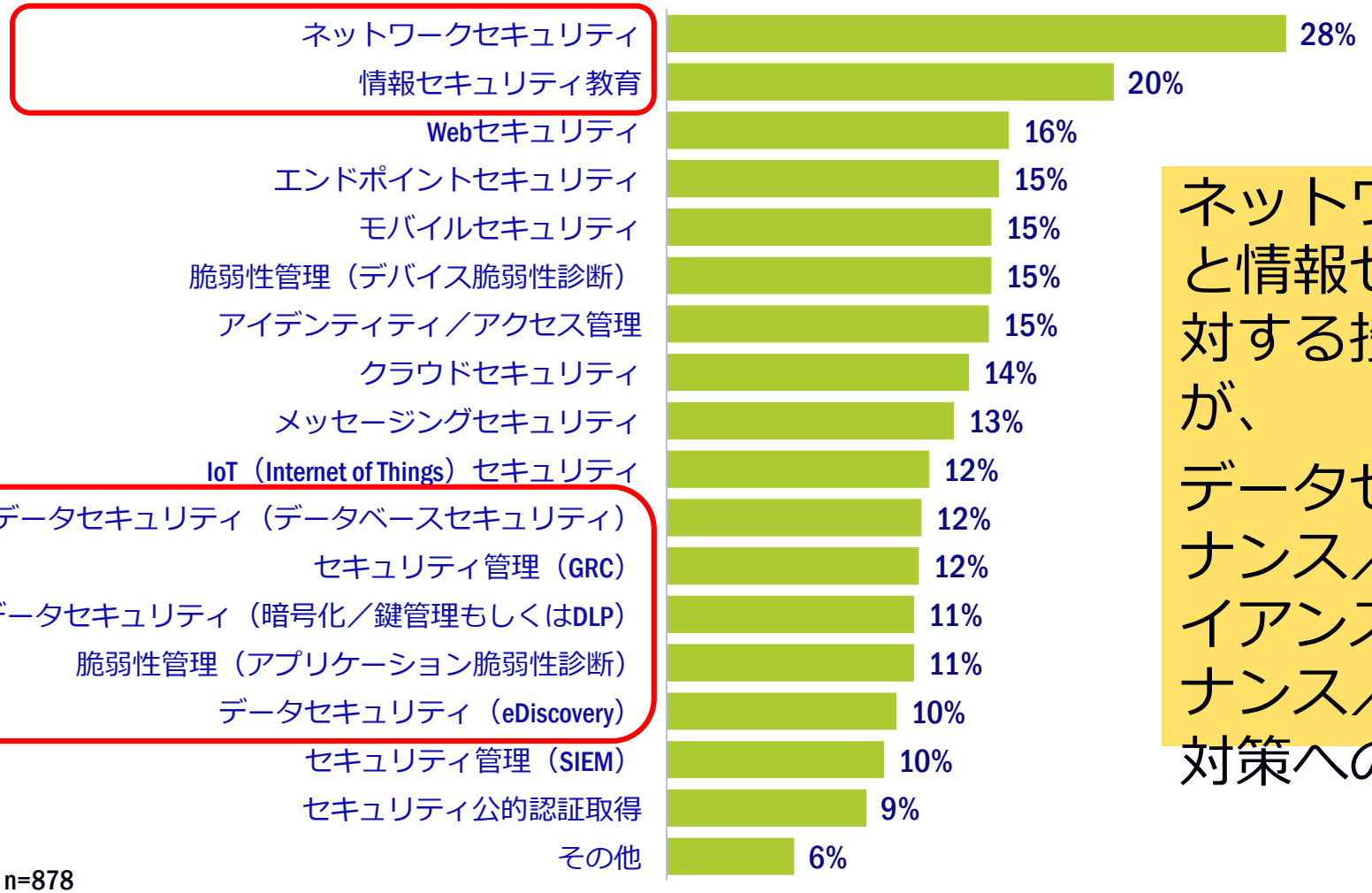
アジアパシフィックの中で日本はセキュリティの確保をより深刻に考えている。

また、外部脅威へ対策は積極的であるが、情報漏洩対策やGRCといった内部脅威対策へは消極的である

Source：IDC-Citrix Business Continuity Flash Study, 2020 (N=342 Asia/Pacific, 77 Japan)

© IDC

2020年 セキュリティ投資重点項目



ネットワークセキュリティと情報セキュリティ教育に対する投資優先度が高いが、
データセキュリティとガバナンス／リスク／コンプライアンスといった情報ガバナンス／コンプライアンス対策への投資優先度は低い

Notes
- 有効回答数 n=878
- 複数回答

Source：『2020年 国内情報セキュリティユーザー調査： 企業における対策の現状（Doc# JPJ45147220。2020年4月発行）』からの抜粋

IDC ANALYZE THE FUTURE
© IDC

提言

© IDC Visit us at IDC.com and follow us on Twitter: @IDC

信頼性できるワークスペースを構築するためには

- ✓ プライバシー法および業界規制へのコンプライアンス対応強化と情報ガバナンスの強化
- ✓ リスク／コンプライアンス／ガバナンスを考慮した企業戦略を策定し、意思決定を行う
- ✓ セキュリティの脆弱な部分を補うために計画的なセキュリティ投資を行う
- ✓ リスクアプローチによるサイバーセキュリティ体制の構築



データへの信頼性と業務効率が向上

© IDC

ユーザー企業への提言

1. 信頼できるワークスペースの基本は、コンテキストベースのセキュアなアクセスコントロールの活用である
2. リモートワークによるワークスペース活用は、セキュリティ強化と生産性向上の両面を実現する集約型セキュリティソリューションを導入すべきである
3. セキュアなリモートワーク環境を構築するために、リスクを低減させるべく、計画的なセキュリティ投資を行うべきである

© IDC

ご清聴ありがとうございました

メールでのお問い合わせは：

ttosaka@idcjapan.co.jp
登坂 恒夫

IDC Japan
ソフトウェア＆セキュリティ　リサーチマネージャー



本テキストの著作権はすべてIDC Japan株式会社に帰属しています。
本テキストの複製、または内容の流用、転載はIDC Japan株式会社の許可なしにはできません。