McAfee MPOWER
講演

NTT DATA
Trusted Global Innovator

経営層が理解しておくべき ディジタル時代のサイバーセキュリティ

2019年11月7日
NTTデータ先端技術（株）
相談役、最高技術顧問
工学博士、CISSP
三宅　功

本日のアジェンダ

１．何が起こっているか？
　　－　ディジタル時代の産業構造

２．ディジタル時代のITガバナンス
　　－　ディジタル時代を経営視点でどうとらえるか？

３．ディジタル時代に対応した企業のリスク管理と
　　サイバーセキュリティ

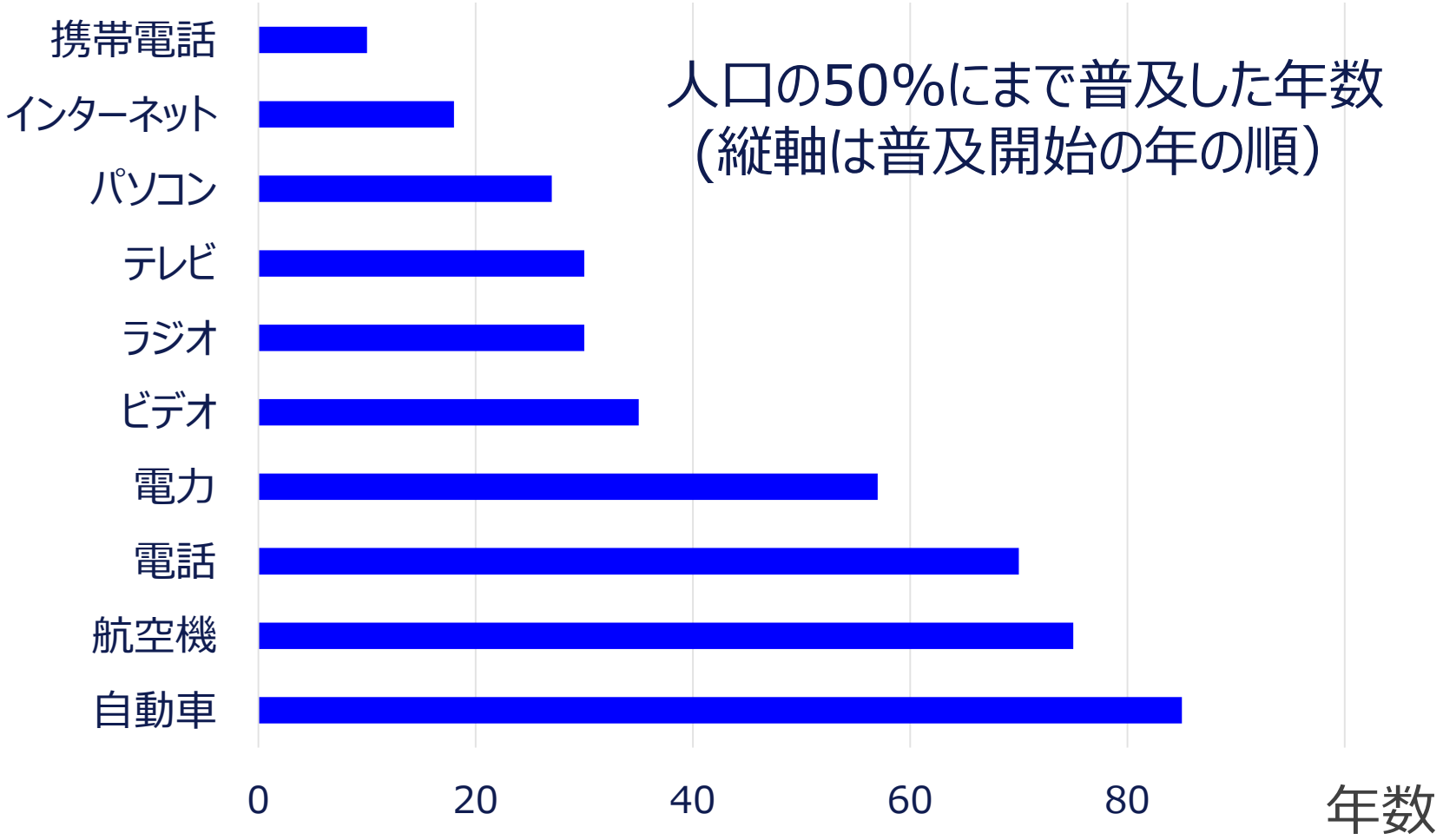
４．まとめ

１．何が起こっているか？

ディジタル時代の産業構造

新技術の急速な普及

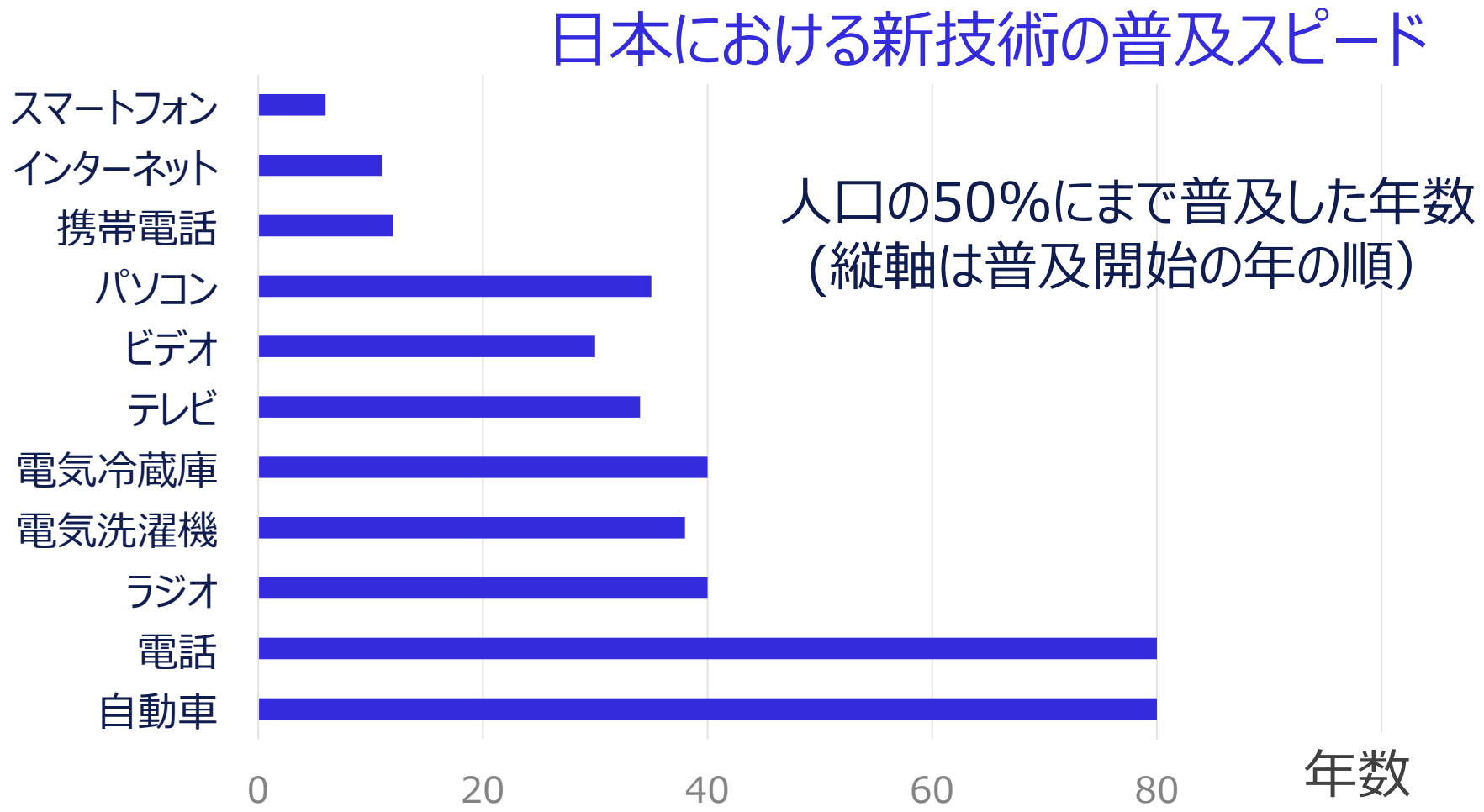
米国における新技術の普及スピード



Source: Human development report 2015, https://honkawa2.sakura.ne.jp/6350.html

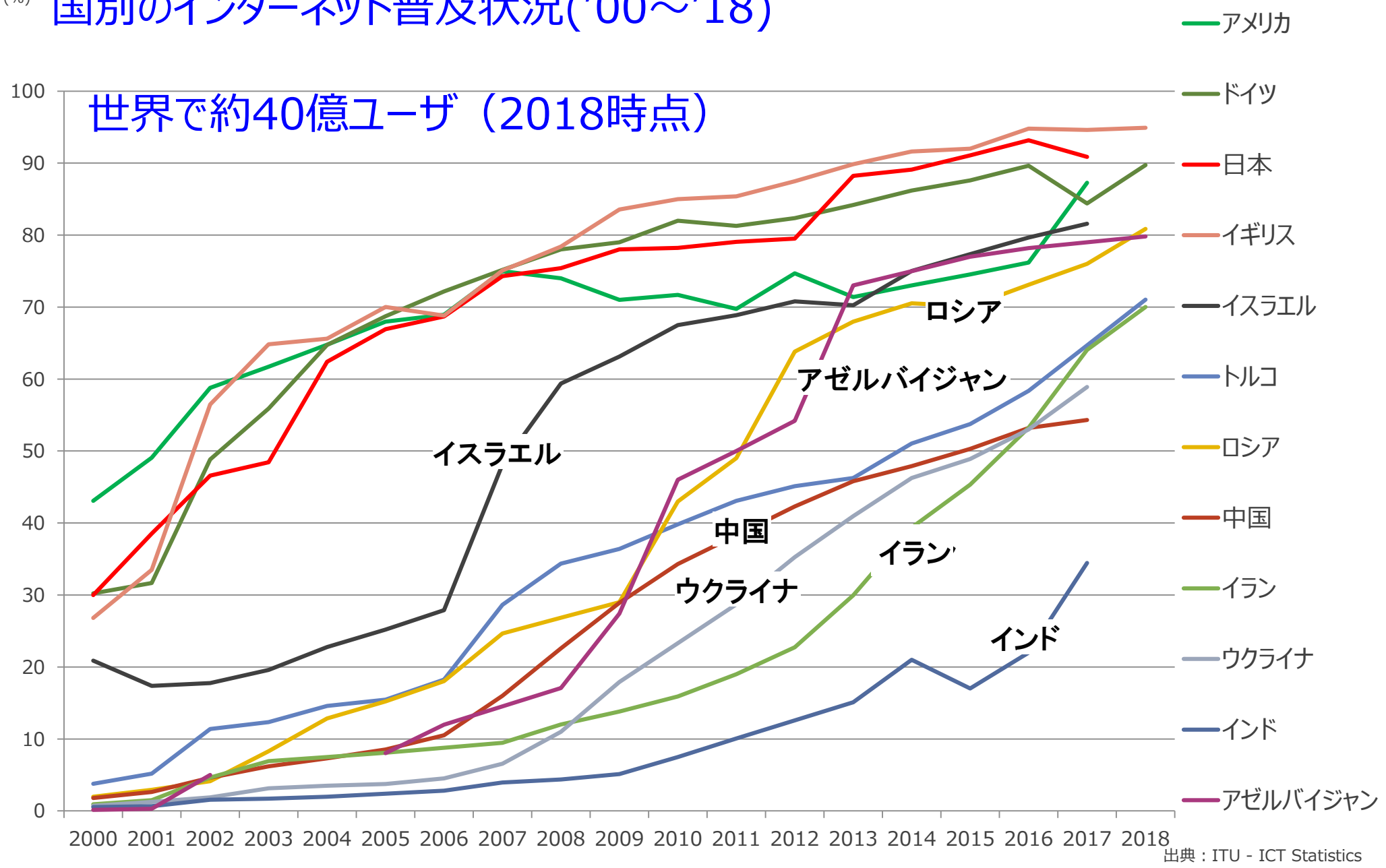
新技術の急速な普及

人口の50%にまで普及した年数



Source: Human development report 2015, https://honkawa2.sakura.ne.jp/6350.html

国別のインターネット普及状況('00～'18)

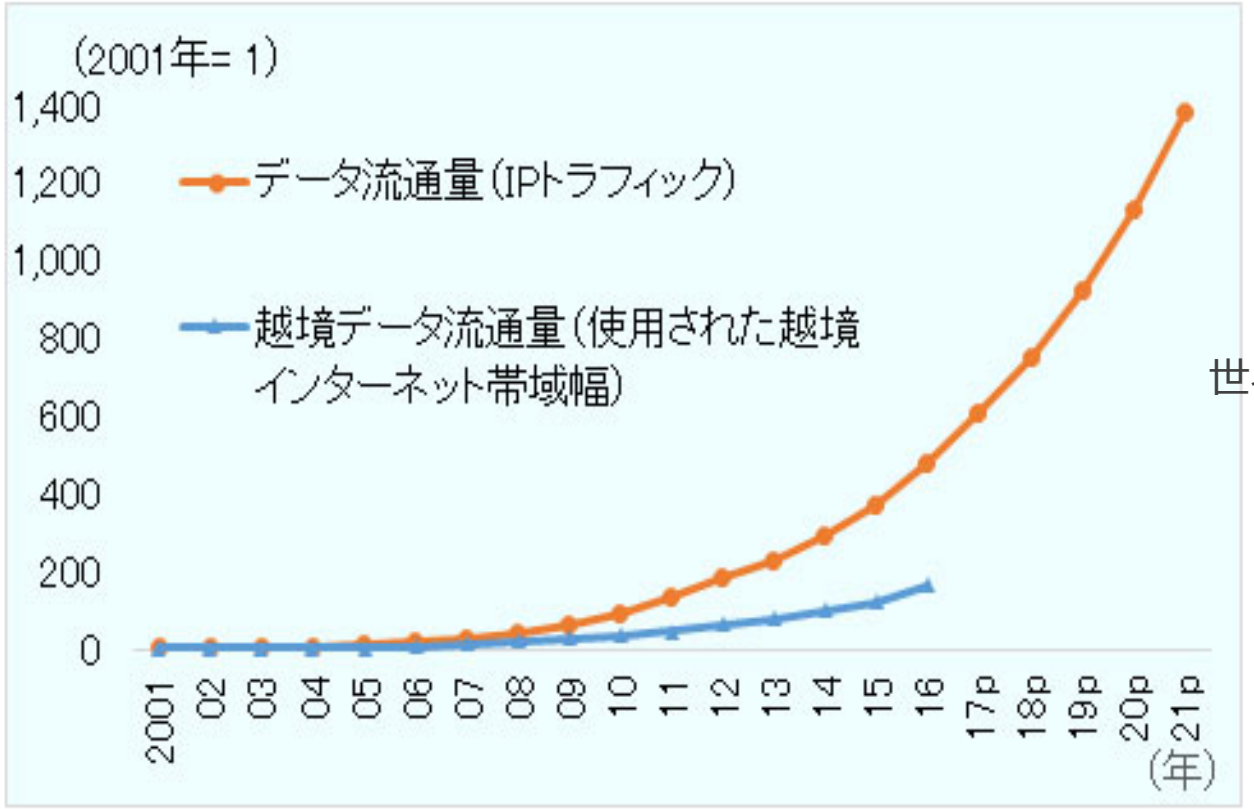


出典：ITU - ICT Statistics

NTT DATA
NTTデータ 先端技術株式会社

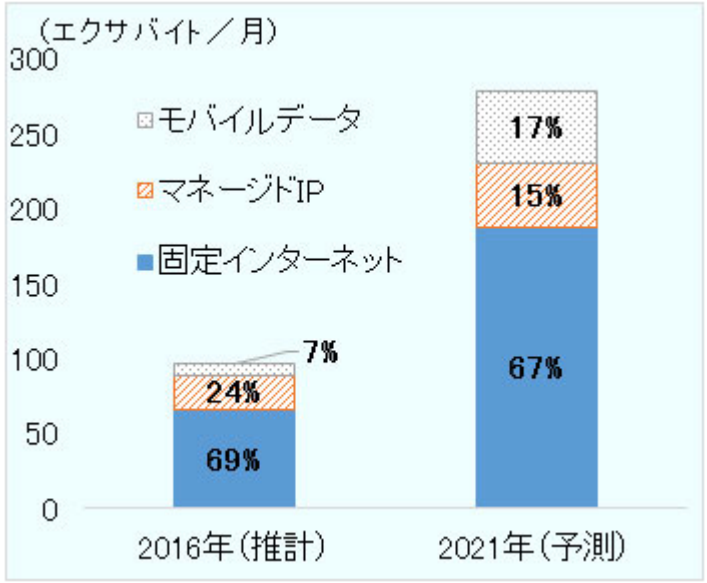
情報流通量の増大

世界のデータ流通量と越境データ流通量（2001年=1）

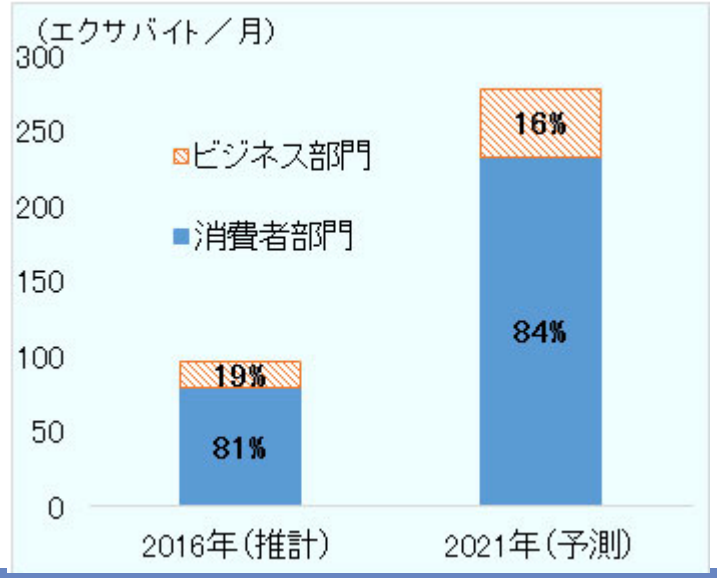


Source: JETROレポート
https://www.jetro.go.jp/biz/areareports/2018/380fd5f0d9c4bb4d.html

世界のデータ流通量（IPトラフィック）：通信タイプ別

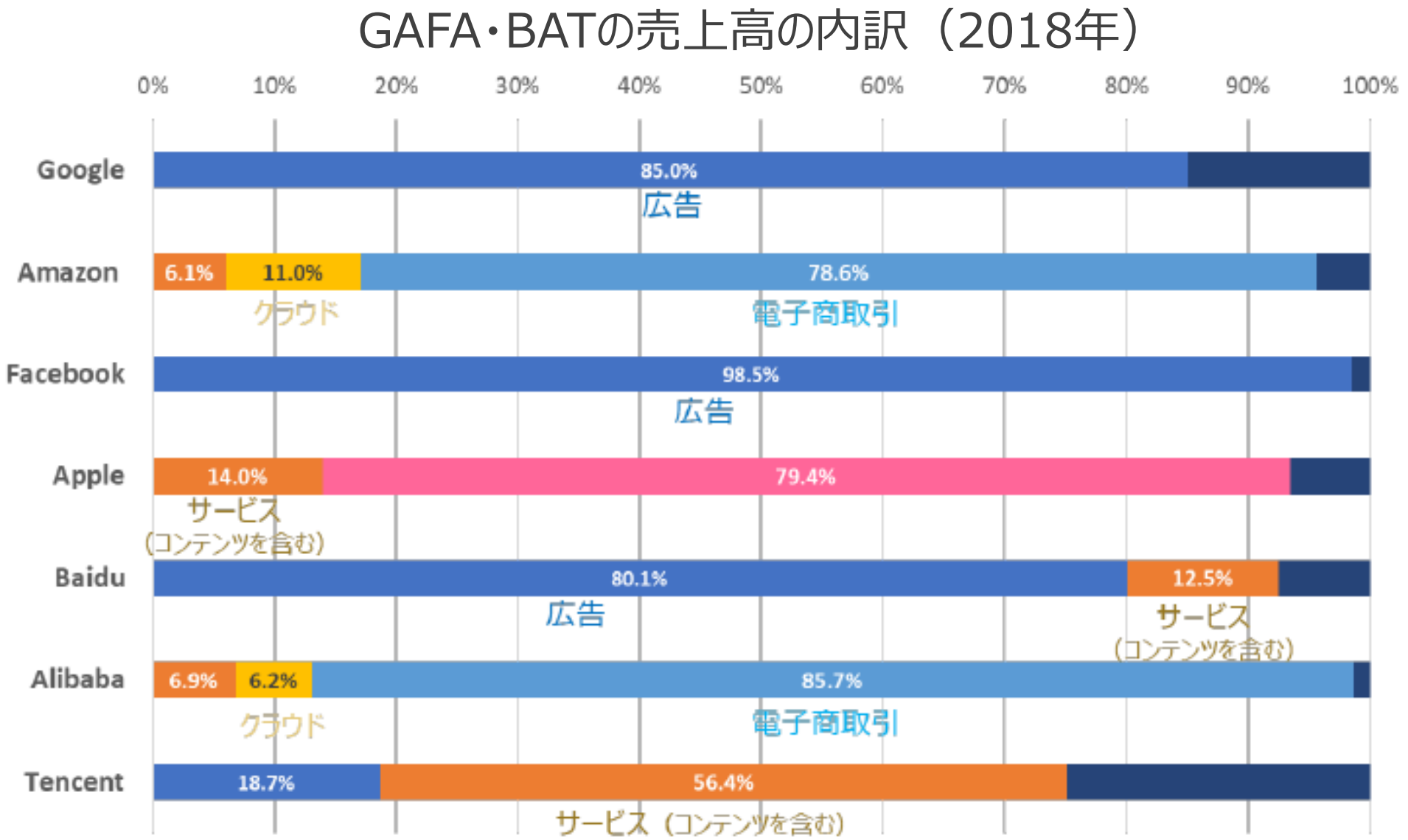


世界のデータ流通量（IPトラフィック）：部門別



NTT DATA
NTTデータ 先端技術株式会社

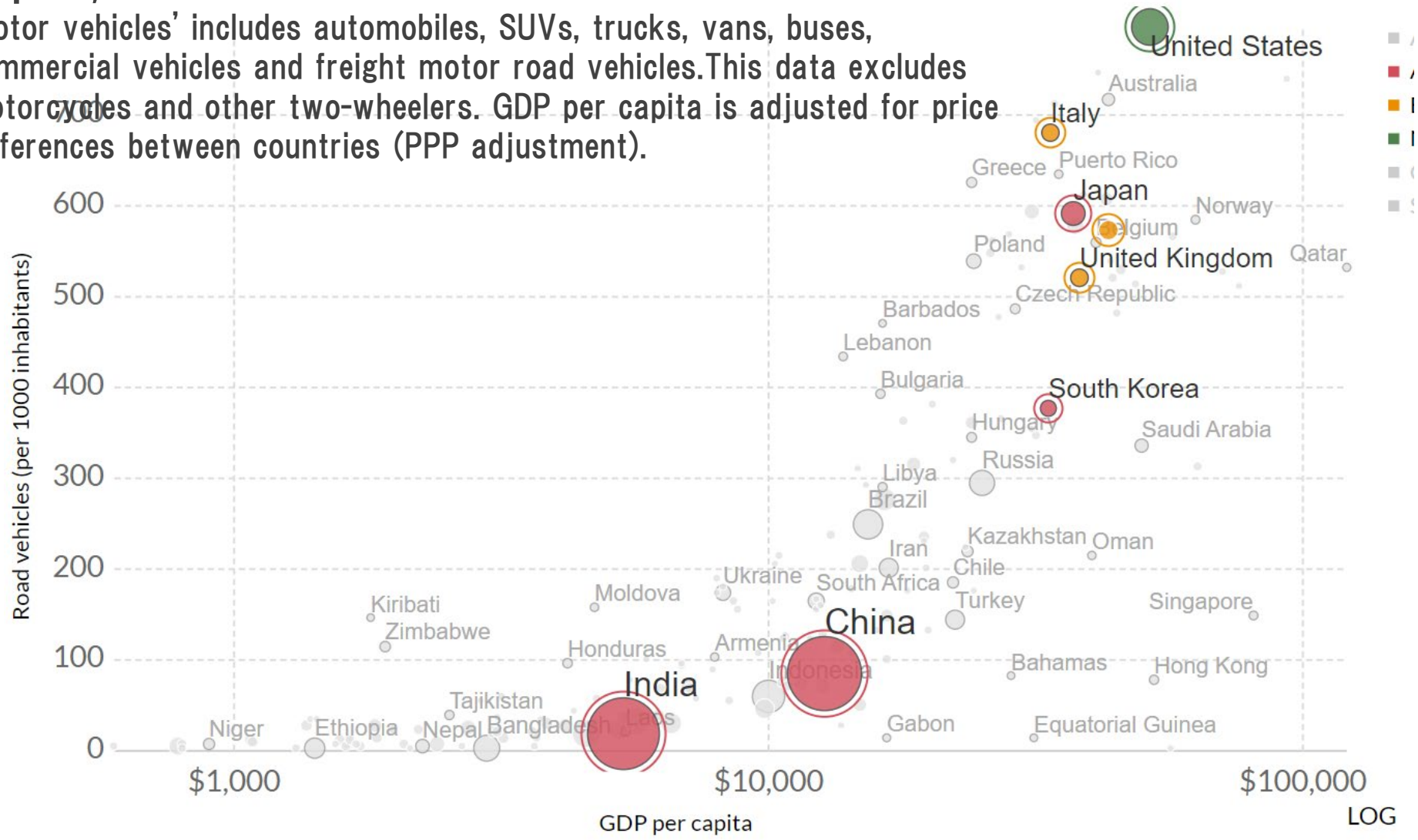
新しい市場の形成



デジタル経済の将来像に関する調査研究の請負報告書　三菱総研　2019.3 図4-3より

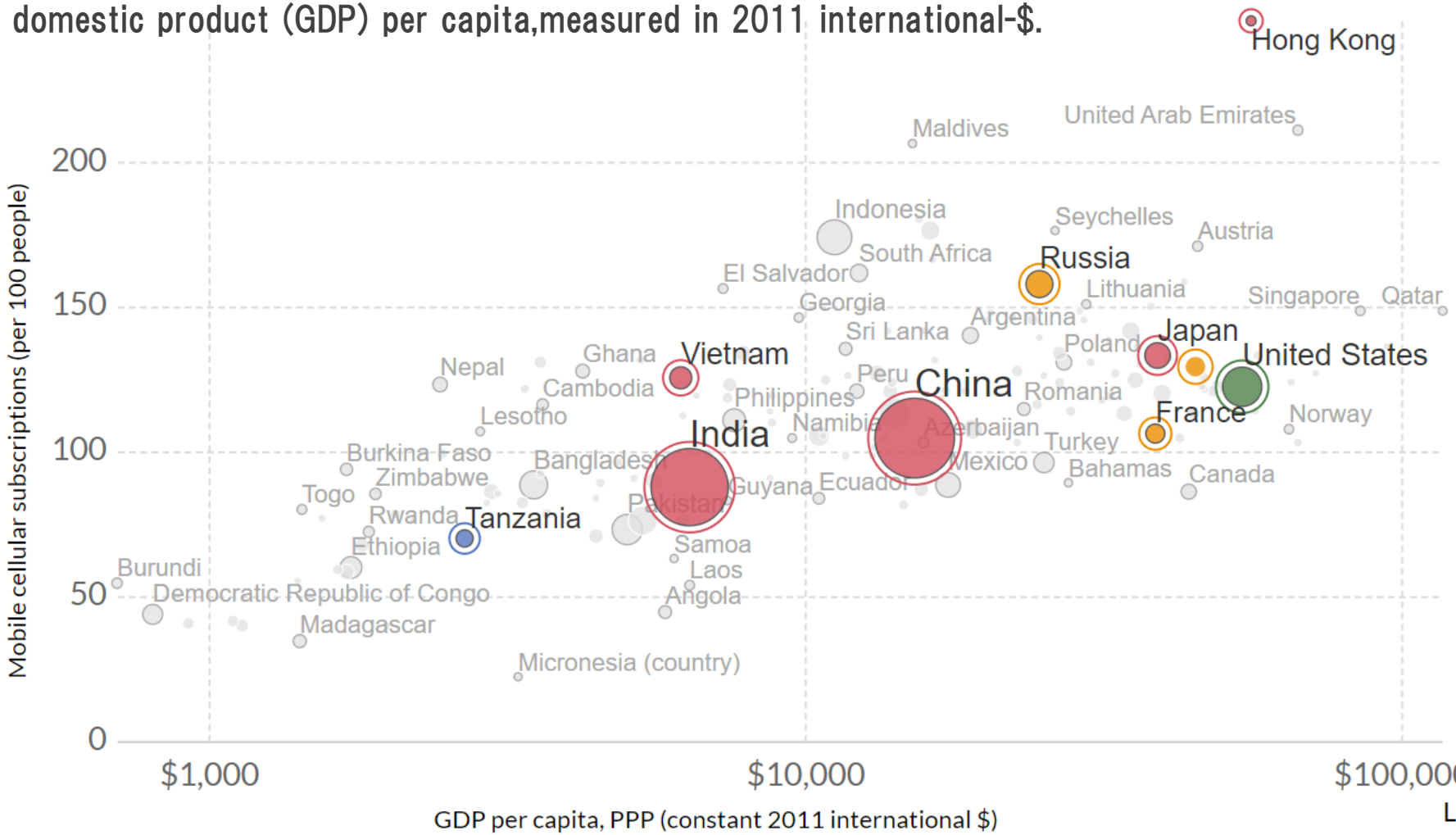
Motor vehicles per 1000 inhabitants vs GDP per capita, 2014

'Motor vehicles' includes automobiles, SUVs, trucks, vans, buses, commercial vehicles and freight motor road vehicles.This data excludes motorcycles and other two-wheelers. GDP per capita is adjusted for price differences between countries (PPP adjustment).



Mobile phone subscriptions vs. GDP per capita, 2017

Number of mobile phone subscriptions, measured per 100 people versus gross domestic product (GDP) per capita,measured in 2011 international-$.



Source: Our World in Data/World Bank.

ディジタル時代の産業構造

市場と製品の激しい変化 ・新製品の急速な普及
・短期間での栄枯盛衰

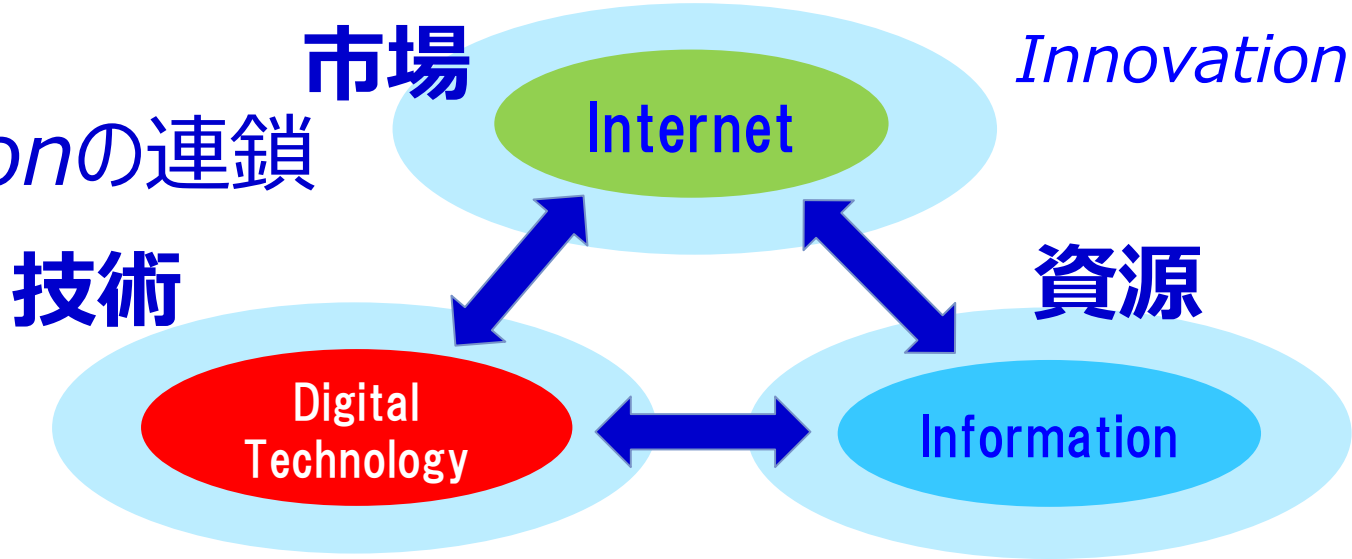
情報の資源化

グローバル市場のフラット化

***Innovation* ＝ 新市場と新技術･資源の新結合**

Innovation ≒ 技術革新

*Innovation*の連鎖



２．ディジタル時代のITガバナンス

- ディジタル時代を経営視点でどうとらえるか？

ITガバナンスと企業戦略

ITガバナンスとは？　企業戦略に従ったIT

① ITによるビジネス価値の提供 ⇒ 企業**戦略**との整合性
② ITのリスク低減 ⇒ リスク管理とアカウンタビリティ

参考:「企業が競争優位性を目的に、IT戦略の策定・実行をコントロールし、あるべき方向に導く組織能力」 経済産業省

企業戦略策定の時間軸

短期：事業目標を最適化するための資源配分

中・長期：市場環境、技術革新、法制度等の変化

ディジタル時代を経営視点でどうとらえるか？

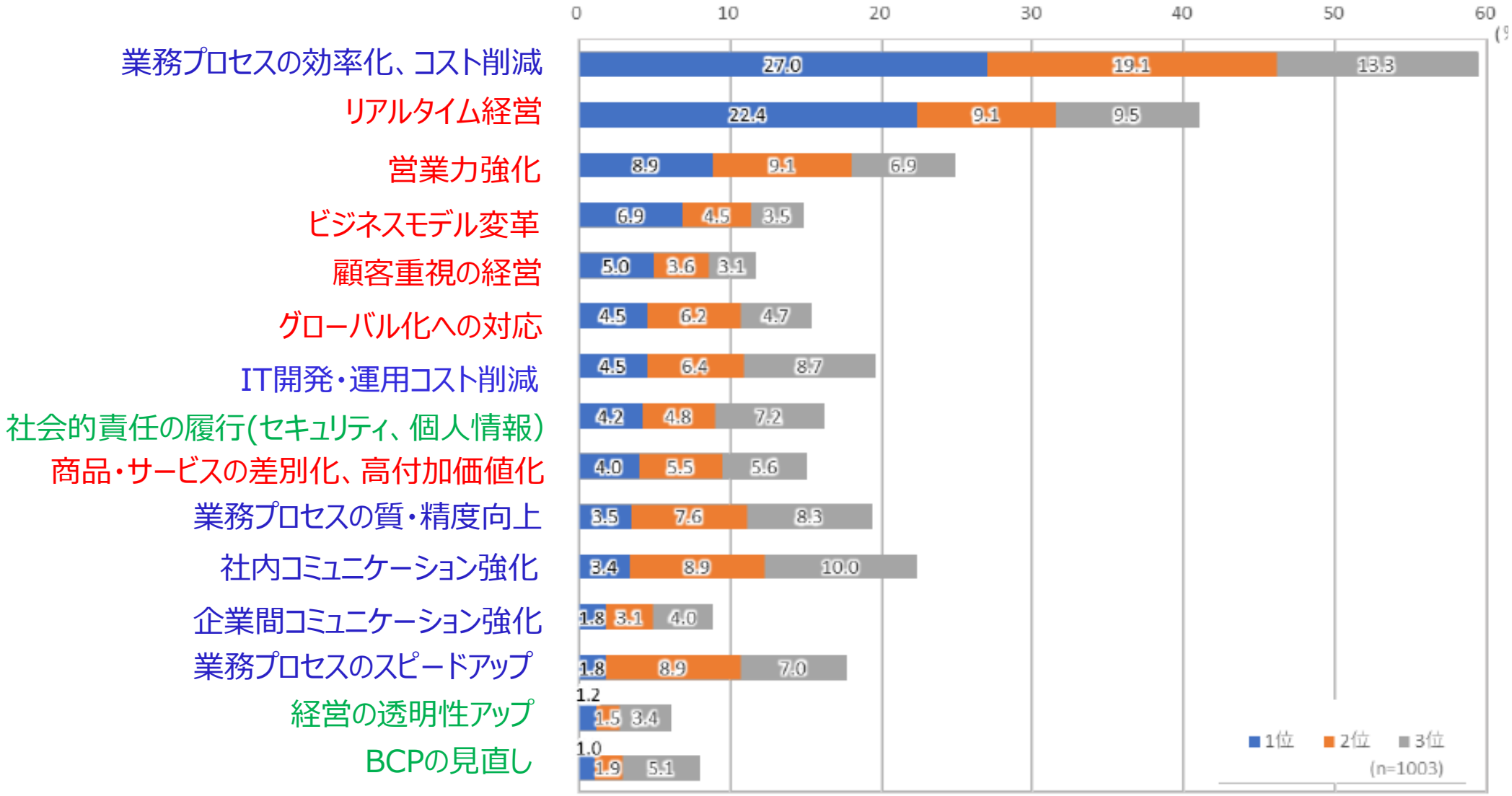
企業戦略

・ディジタルテクノロジーの積極的活用
→ 事業機会の創出
→ 既存業務の効率化

・Time to Marketの短縮
→ 戦略策定、実行サイクルの短縮
→ アウトソース、サプライチェーンの拡大

・新しい、グローバルな制度、法規制への対応

IT投資で解決したい中期的な経営課題



デジタル経済の将来像に関する調査研究の請負報告書　三菱総研　2019.3 図3-1より

ディジタル時代を経営視点でどうとらえるか？

企業戦略

・ディジタルテクノロジーの積極的活用
→ 事業機会の創出
→ 既存業務の効率化

・Time to Marketの短縮
→ 戦略策定、実行サイクルの短縮
→ アウトソース、サプライチェーンの拡大

・新しいグローバルな制度、法規制への対応

ディジタルを支えるTechnologyの進化

データサイエンス/AI

クラウド・マイクロサービス

インターネット

ソフトウェア

コンピュータ

利用者の視点
多様なサービスが次々に生み出され、必要な機能を迅速に組み合わせることで利用される

提供者の視点
提供する製品に必要な機能を多様なサプライチェーンを組み合わせることで迅速に提供する

コンピュータの進化を支えるもの

Domain Specific Computing

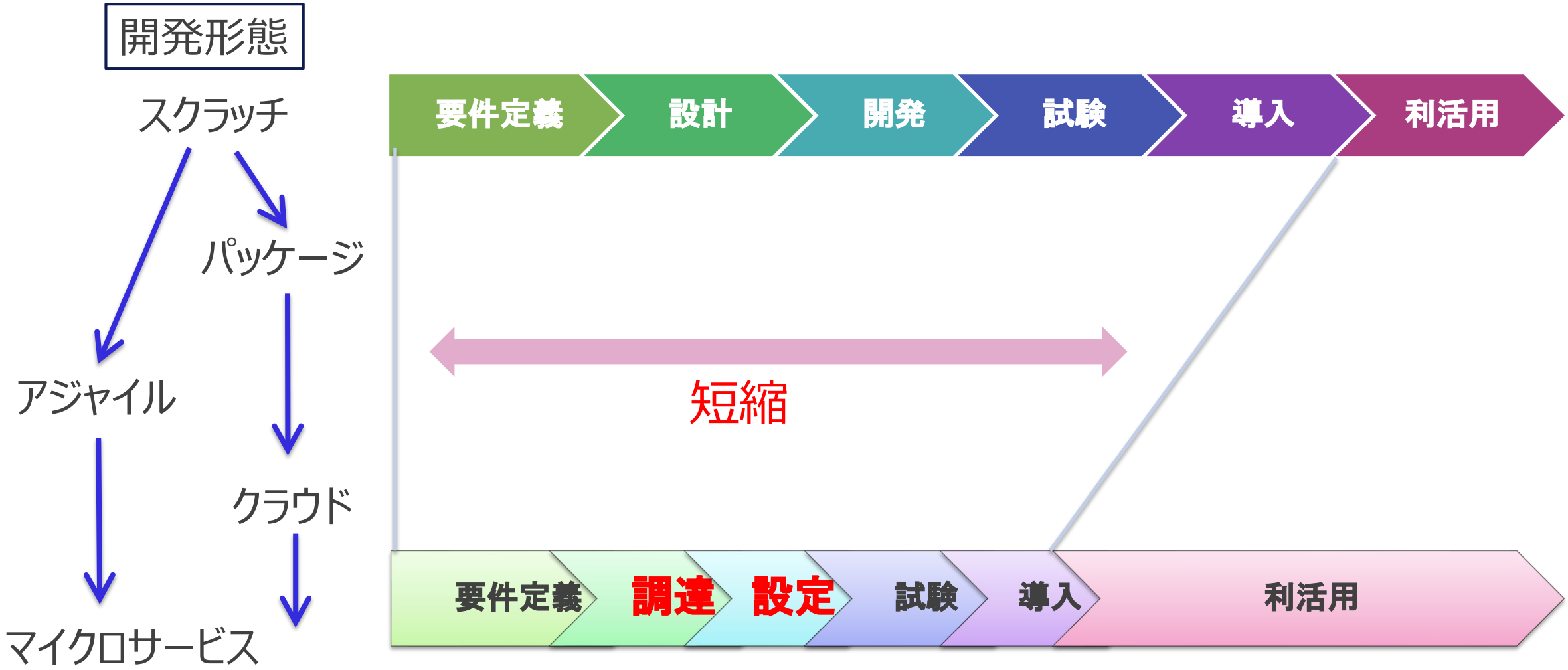
Google I/O 2018.5

https://project.nikkeibp.co.jp/atcldgl/feature/052700006/052800003/?P=1

・ハードウェアの小型・大容量化
・抽象化による設計の分業と再利用
・様々な高速処理技術
  汎用処理のハード化；
  並列処理
  パイプライン処理
  予測処理
・階層記憶
・高信頼化
  誤り訂正、
  冗長化
・低消費電力化

「コンピュータの構成と設計　第5版」より

ディジタル時代の新たなアプリケーション開発



様々な制度、法規制

・サイバー刑法
・不正アクセス禁止法

・特許、実用新案法
・著作権法
・不正競争防止法

・個人情報保護法(日本)
・GDPR（欧州）
・サイバーセキュリティ法
国家情報法（中国）

・通信傍受法
・プロバイダ責任制限法

・コーポレートガバナンス　コード
・IFRS(国際会計基準)
・金融商品、証券取引法

・PCI DSS
・FATF(Financial Action Task Force)勧告
・犯罪収益移転防止法

・スパイ活動法（米国、連邦法典第18編37章)
・反スパイ法、国家安全法（中国）
・特定秘密保護法(日本)

日本経済新聞

資金洗浄対策、仮想通貨業者に照準　威信かける金融庁

2019/5/18 1:30
日本経済新聞　電子版

国内外の仮想通貨交換業者で不正流出が頻発	
2014年2月	マウントゴックスで約480億円相当のビットコインが消失。経営破綻
18年1月	コインチェックで約580億円分の仮想通貨が不正流出
2月	イタリアのビットグレイルで200億円強の仮想通貨がハッキング
9月	テックビューロ（大阪市）でビットコインなど約70億円分が盗難
19年5月	香港系のバイナンスでビットコイン約45億円分が不正流出

金融庁が資金洗浄（マネーロンダリング）対策に躍起になっている。日本は今秋に国際組織の審査を受ける予定で、20カ国・地域（G20）会議議長国の威信にかけても対策で後手に回るわけにはいかない。金融庁の照準は銀行など伝統的な金融機関に加え、本人確認の甘さや取引の匿名性が指摘される仮想通貨交換業者に向く。

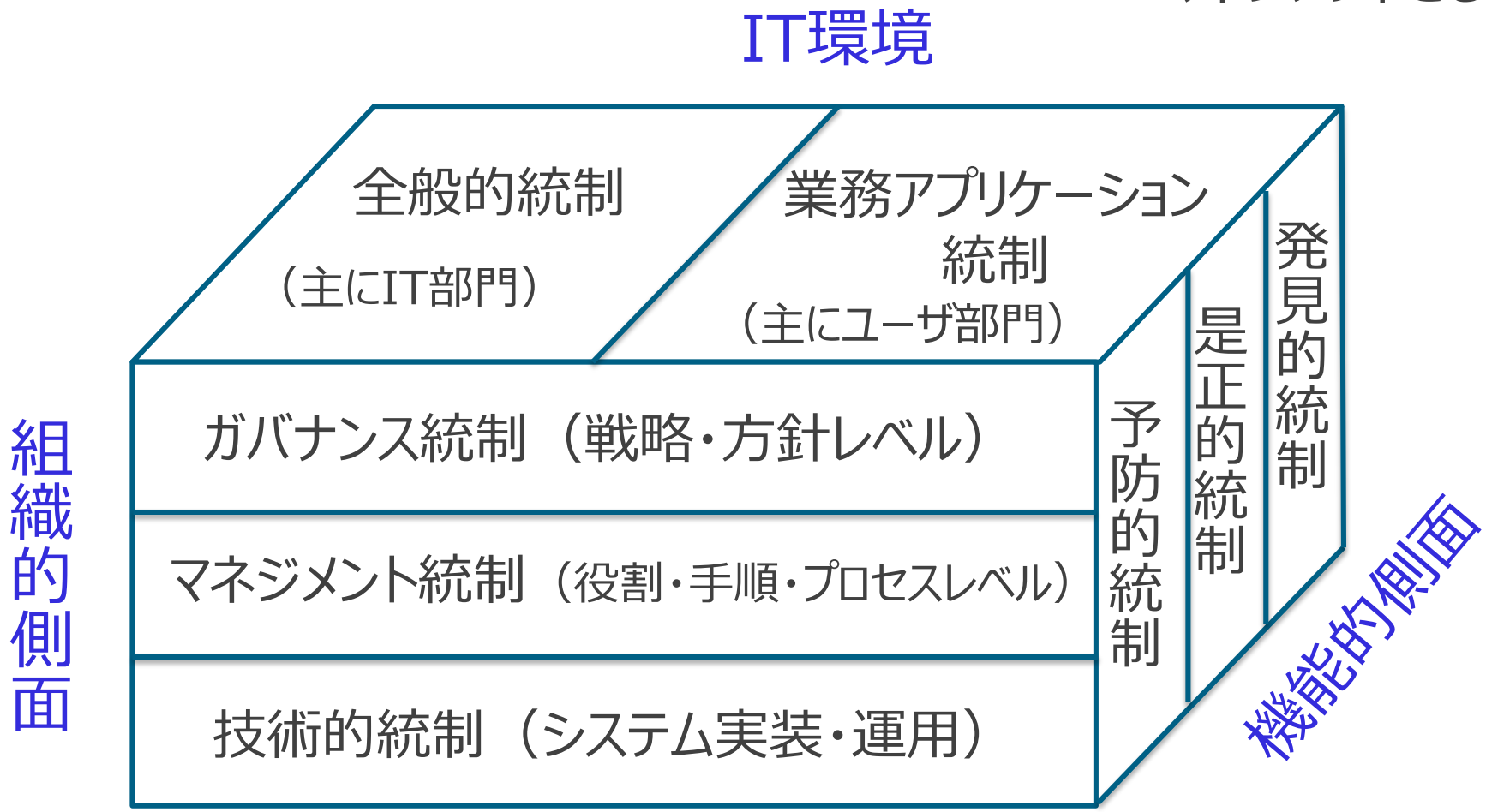
1989年の主要国首脳会議（仏アルシュ・サミット）で立ち上げが決まったマネロン対策などを審査する国際組織「金融活動作業部会（FATF）」が規制整備や実務面で大きな影響力を持つ。FATFは18年10月にルールを改め、仮想通貨交換業者などもマネロン規制の対象に加えると表明した。

今秋にはFATFの調査団が来日し、国内のマネロン対策が十分か審査する。銀行や信用金庫と同様に「仮想通貨交換業者も調査の対象になる」（金融庁幹部）とみて、対策づくりが急務になっている。

３．ディジタル時代に対応した企業のリスク管理とサイバーセキュリティ

IT統制(リスク管理）のバランス

*統制はコントロール、或いは
マネジメントとも言う



「Global Technology Audit Guide」より著者改変

ディジタル時代のセキュリティリスク管理

事業継続性(Biasness continuity）のための

リスク ＝ ∑ 資産の価値 × 失われる可能性*1 ＜ 許容値

①情報・データ
②情報システム、施設
③人的資源
④サプライチェーン

*1 資産に対する脅威（攻撃者から見た価値）と脆弱性により想定される。「失われる確率」とも言われる。

経営判断：リスク対策に経営資源をどこまで配分するか？

失われる可能性 ＝ 固有リスク × コントロール*2リスク × 発見リスク

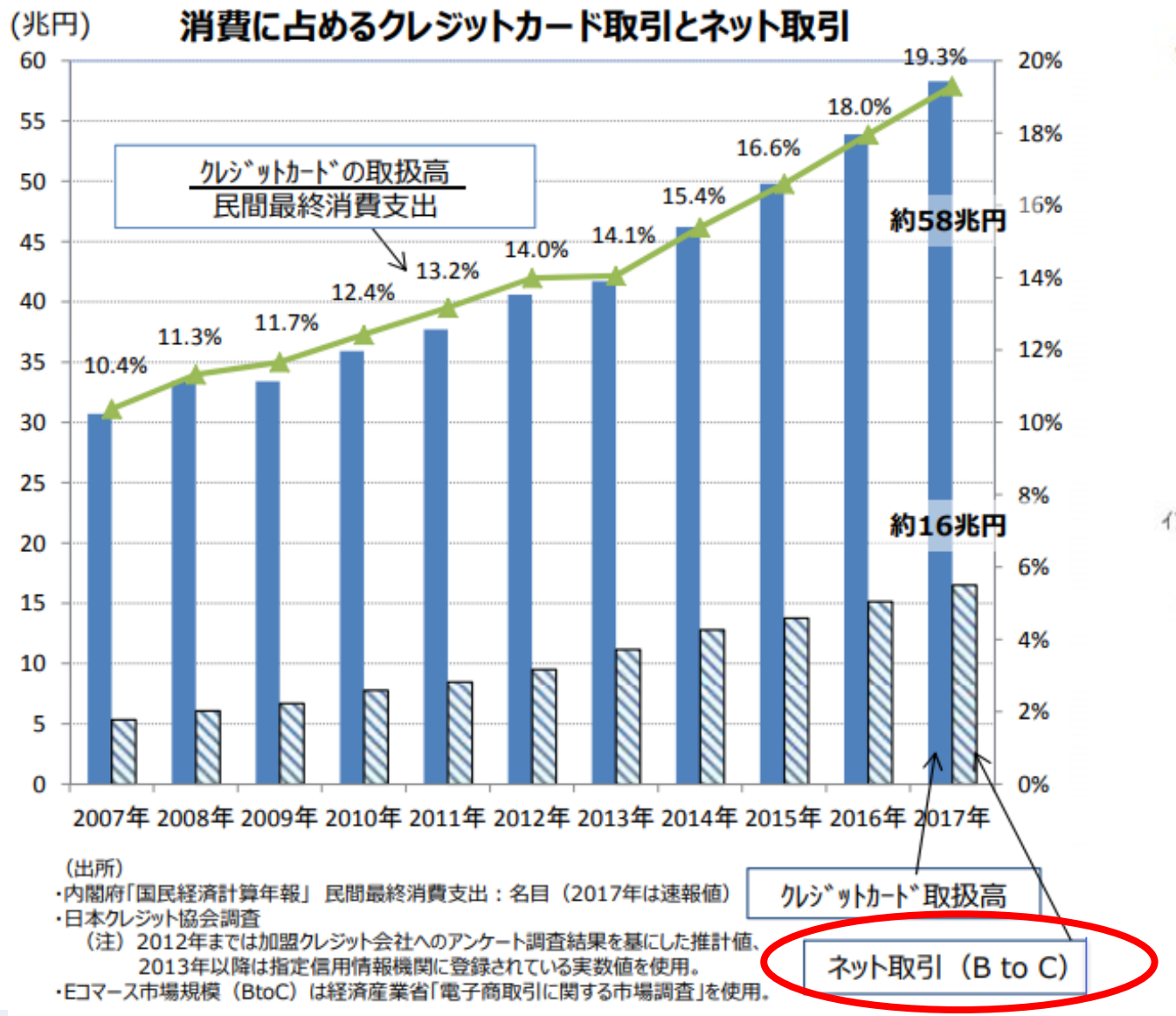
固有リスク：コントロールが無い場合の損失可能性

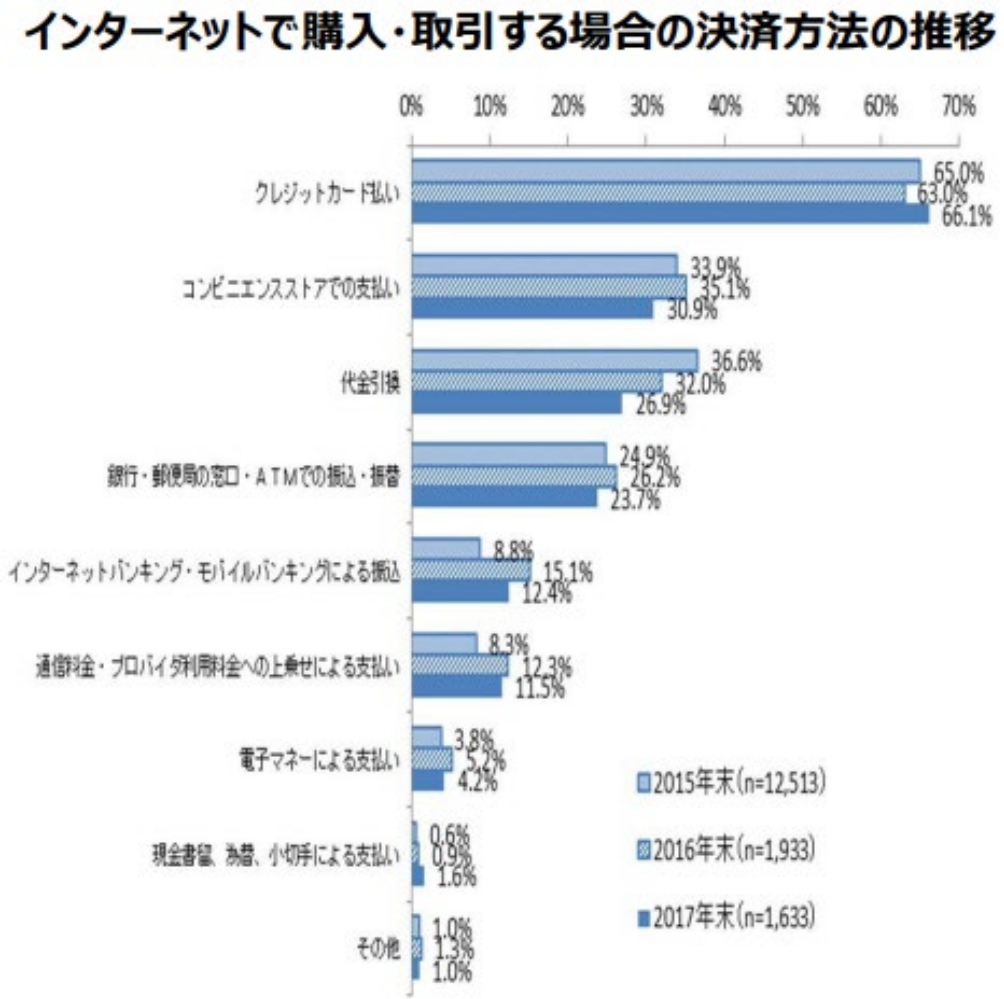
コントロールリスク：コントロールが失敗する可能性

発見リスク：監査で侵害を検知できない可能性

*2 或いは管理策, ISMS, NIST SP800-53等

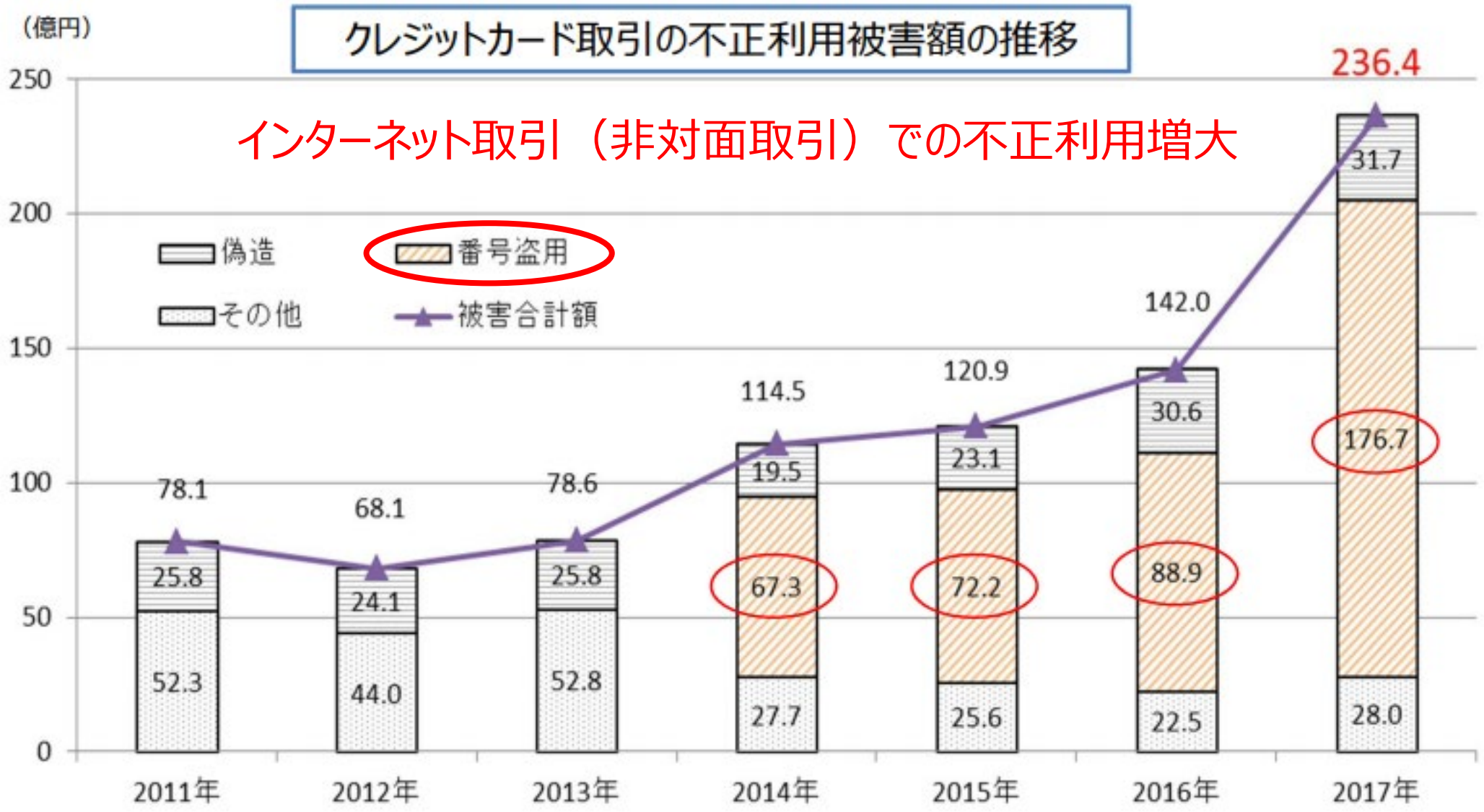
固有リスク拡大の例





Source クレジット取引セキュリティ対策協議会
https://www.j-credit.or.jp/security/pdf/overview_2019.pdf

固有リスク拡大の例



Source クレジット取引セキュリティ対策協議会 https://www.j-credit.or.jp/security/pdf/overview_2019.pdf

リスクコントロールの考え方

固有リスク × コントロールリスク × 発見リスク ＜ リスクの受容

インターネット取引
固有のリスク
→取引量の増大
→脅威の増大

PCI DSS　準拠
→準拠できていない
→出来ていても侵害

強化

例えば、3Dセキュアの導入

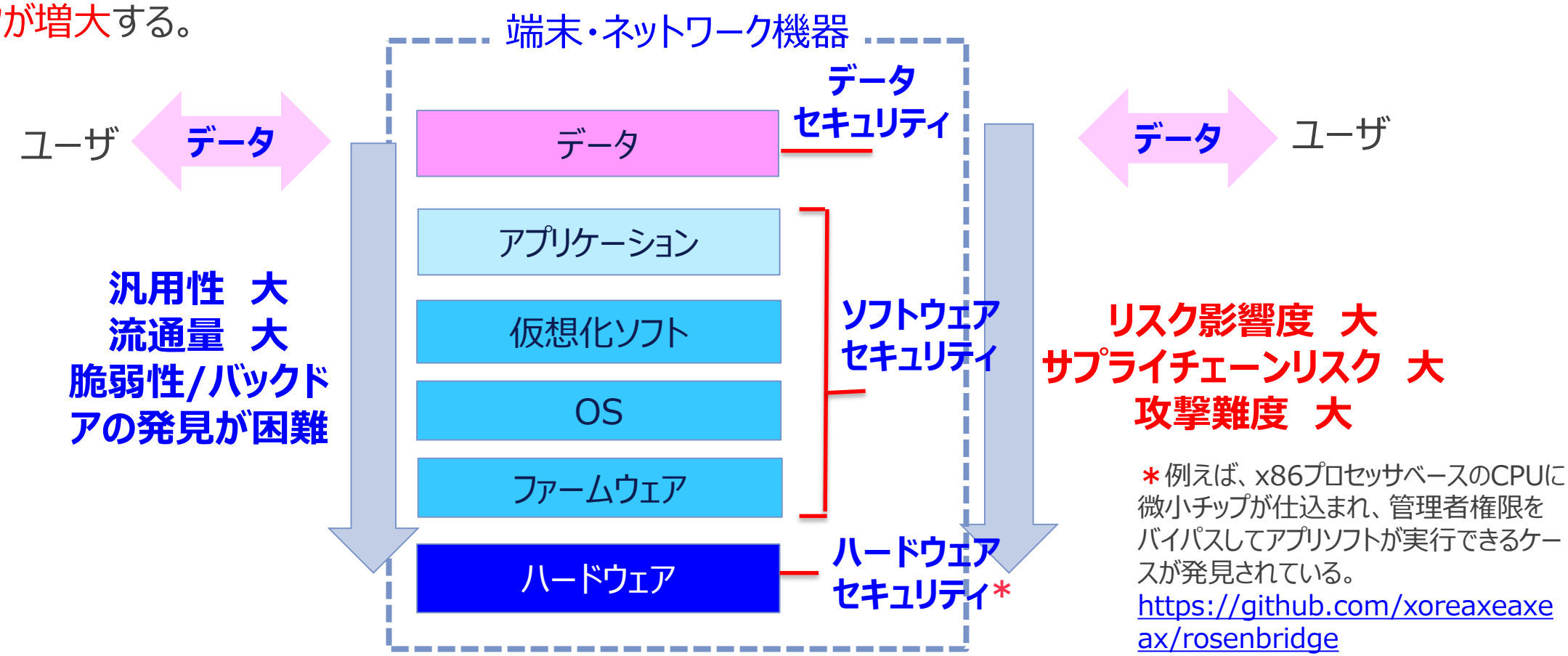
PCI DSS　QSA
SAQ(自己問診表)

→監査していても見逃す

ICTシステムのセキュリティリスクの分類

■端末・ネットワーク機器のセキュリティリスクは大きくハードウェア、ソフトウェア、データに分けられる。下位のレイヤの製品ほど汎用性が高く、流通量が多くなる。

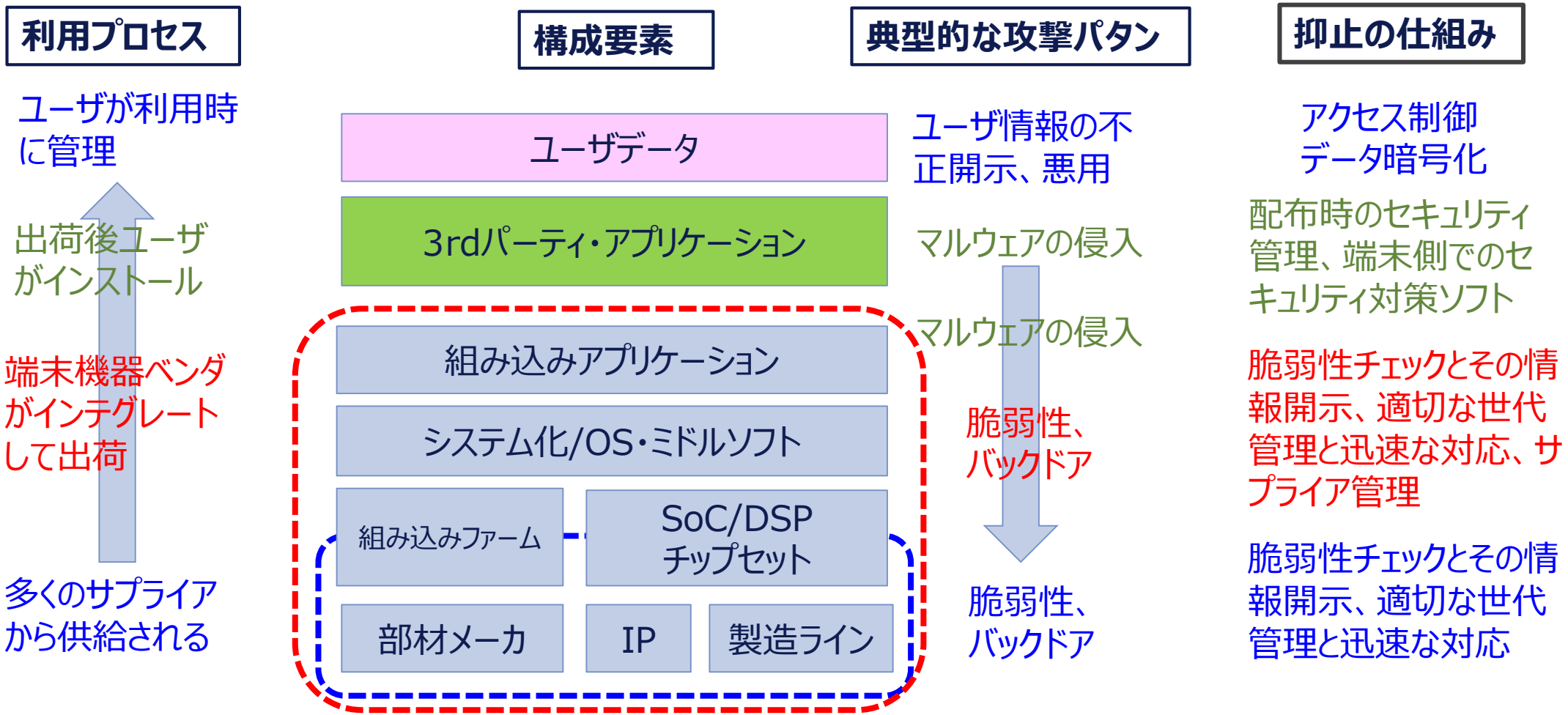
■バックドア及びバックドアにつながる脆弱性がハードウェア等基盤部分に存在する程、リスクの影響は大だが発見は困難。逆に攻撃の難易度は大きくなる。また、多くのサプライアが関与することから、サプライチェーン・リスクが増大する。



＊例えば、x86プロセッサベースのCPUに微小チップが仕込まれ、管理者権限をバイパスしてアプリソフトが実行できるケースが発見されている。
https://github.com/xoreaxeaxeax/rosenbridge

ICT機器のサプライチェーンとセキュリティ

■現代の情報機器は様々なサプライア、システムベンダを通じてエンドユーザに提供される。この環境下でセキュリティ侵害を防ぐには、ステークホルダ毎の責任分担と、リスクの大きい脆弱性と攻撃パタンを想定しこれを抑止するエコシステムが必要になっている。



ICT機器のサプライチェーンリスクコントロール

固有リスク × コントロールリスク × 発見リスク ＜ リスクの受容

↓ ICT機器の多様化
サプライチェーンの複雑化

↓ セキュリティリスクを考慮した機器選定
セキュリティパッチ管理
脆弱性管理

↓ 危ない物は使わない？

↓ 認証制度
コモンクライティリア

クラウドサービスの多様化

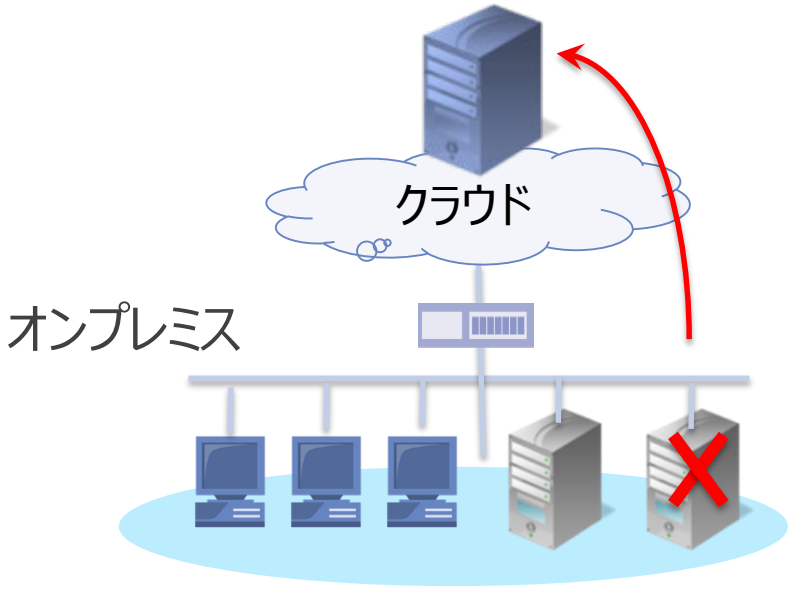
プライベートクラウド

アプリケーション	ユーザ
基盤設備	ユーザ

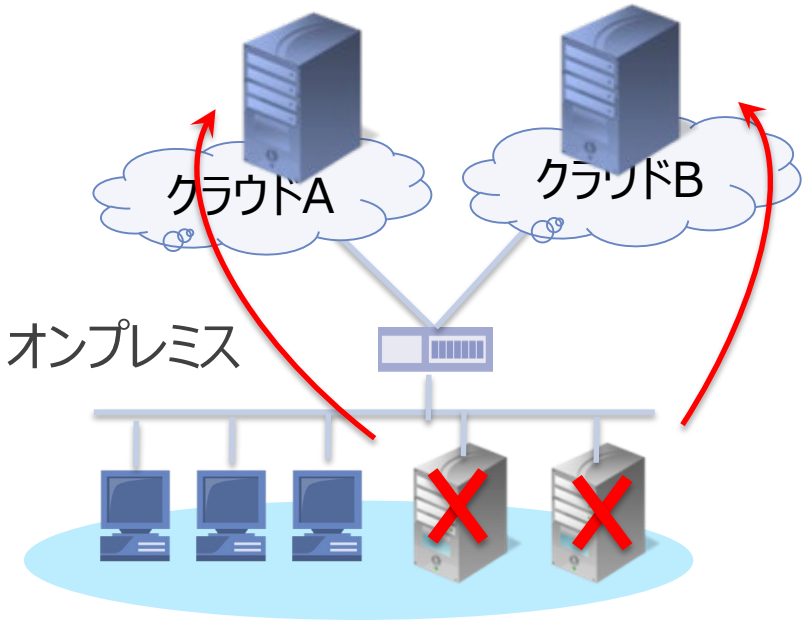
パブリッククラウド

IaaS/PaaS	SaaS
ユーザ	ベンダ
ベンダ	ベンダ

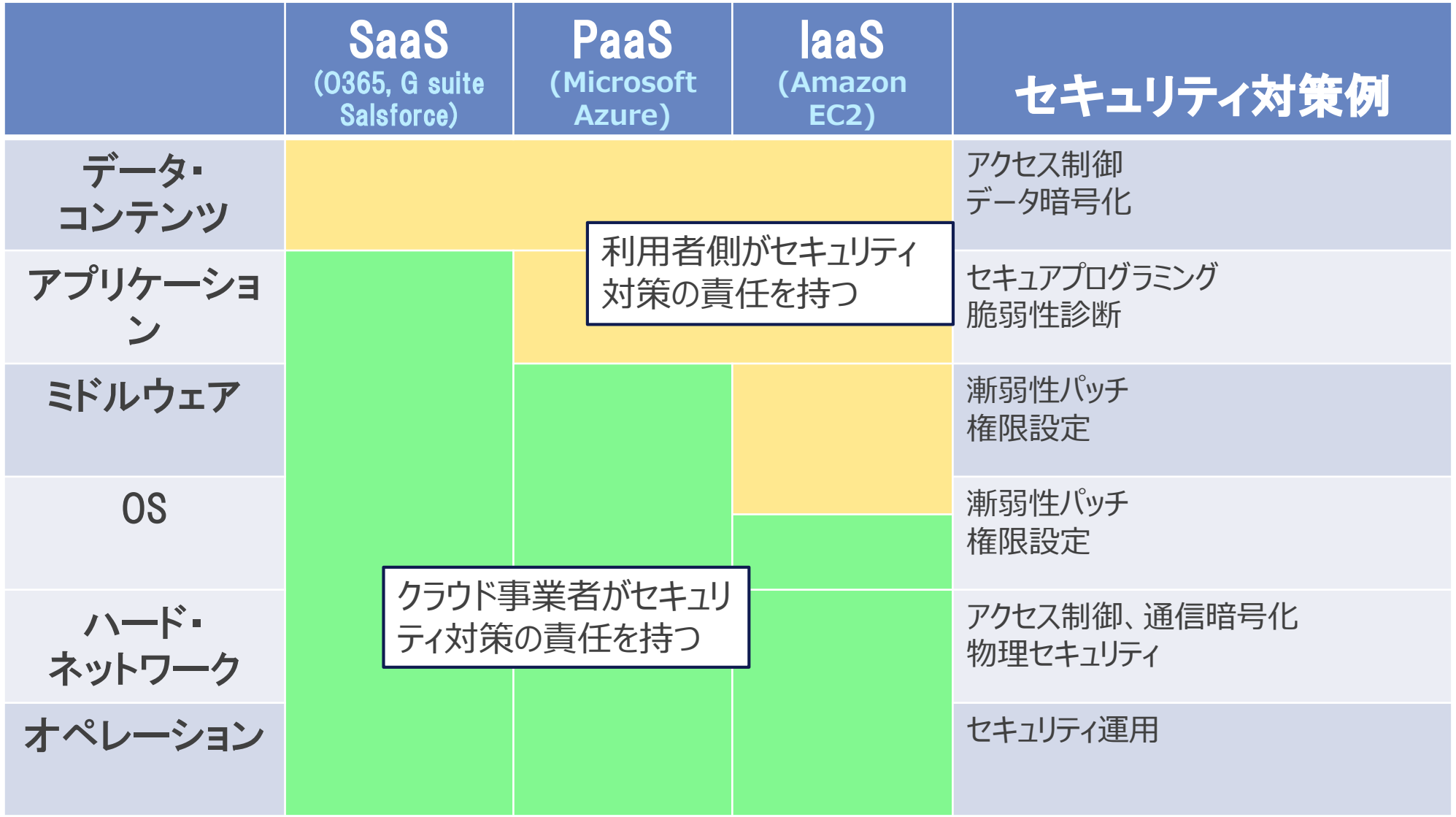
ハイブリッドクラウド



マルチクラウド

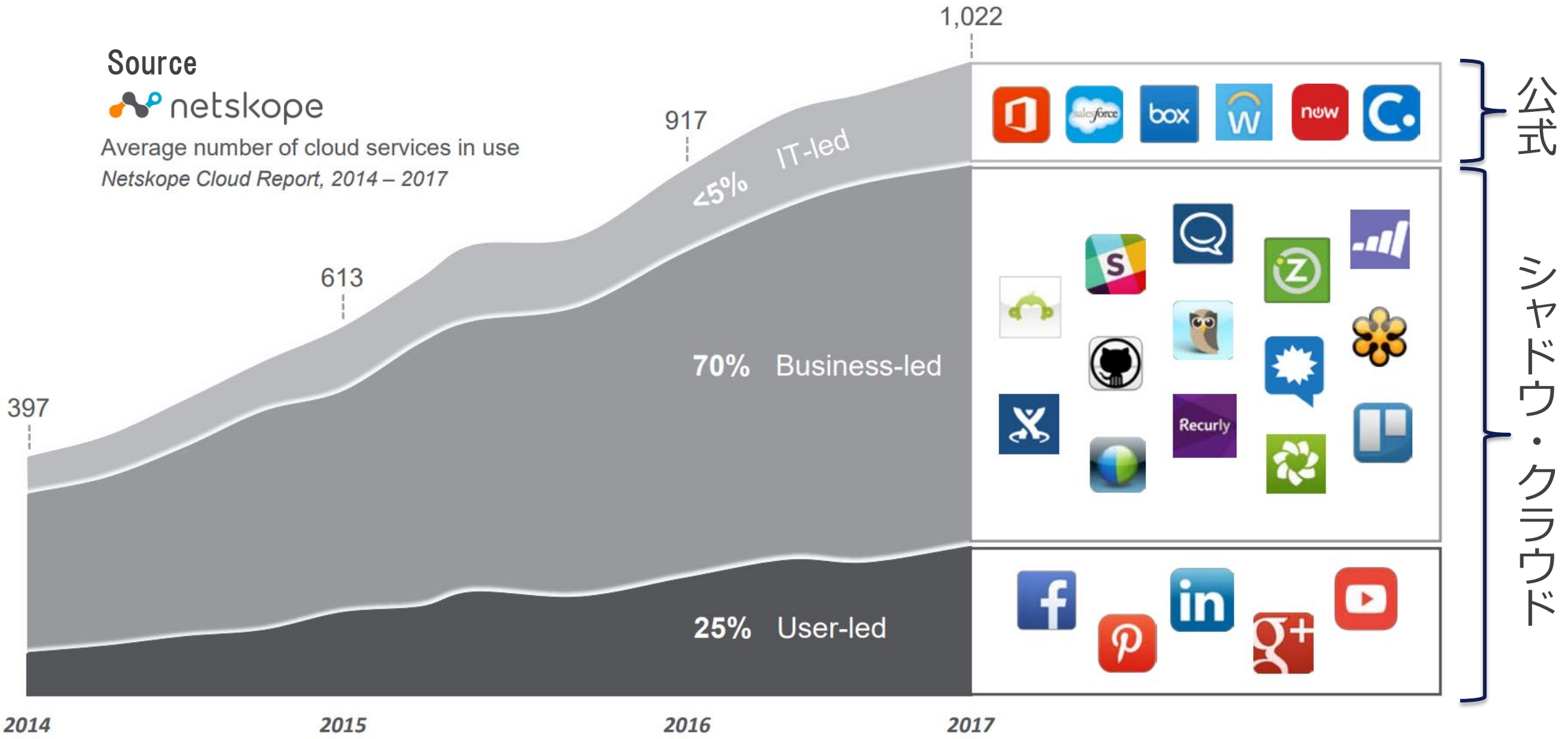


パブリッククラウドサービス利用におけるセキュリティ対策と責任分担



Source:「5分でわかるクラウドセキュリティ」 Symantec https://www.digicert.co.jp/welcome/pdf/wp_cloudsecurity.pdf

企業内でのクラウド利用の実態　シャドウ・クラウドのリスク



クラウドサービス利用時のリスクコントロール

固有リスク × コントロールリスク × 発見リスク ＜ リスクの受容

機能がデータセンタに集中配備されインターネット経由でアクセス

→Attack Surfaceは限定されるが、逆に攻撃対象も集中化

外部委託管理
責任共有モデル
アクセスコントロール
（アプリケーションフィルタリング, CASB, Zero Trust等）
データ暗号化

→利用側の統制不足
→コントロールが未成熟
→クラウド事業者のセキュリティコントロール不足

クラウドセキュリティ標準に基づく事業者監査
クラウド事業者の監査ガイドライン

→クラウド事業者に対する監査権？

ディジタル時代のサイバーリスク

データサイエンス/AI

クラウド・マイクロサービス

インターネット

ソフトウェア

コンピュータ

サプライチェーンの複雑化、技術の多様化によるAttack Surfaceの拡大

利用者の視点
多様なサービスが次々に生み出され、必要な機能を迅速に組み合わせることで利用される

提供者の視点
提供する製品に必要な機能を多様なサプライチェーンを組み合わせることで迅速に提供する

NIST Cybersecurity Framework 1.1 (2018.4)

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

サプライチェーンリスク管理（ID.SC）：
企業は自組織の優先順位、制約、リスク耐性、前提が確立され、サプライチェーンのリスク管理に関連したリスク判断に活用されている。
組織はサプライチェーンリスクを特定し、評価し、管理する仕組みが確立され、実装されている。

ID.SC-1：サイバーサプライチェーンリスク管理の仕組みが特定され、確立され、評価され、管理されかつ組織のステークホルダに認められている。

体制

ID.SC-2：サイバーサプライチェーンリスクアセスメントプロセスに従って、情報システム、そのコンポーネント及びサービスに対する供給者、3rdパーティパートナが特定され、重要度付けされ評価されている。

リスクアセスメント

ID.SC-3：サプライア及び3rdパーティパートナーとの契約は、組織のサイバーセキュリティプログラム及びサイバーサプライチェーンリスク管理計画に対応した適切な手段として構成されている。

コントロール

ID.SC-4：サプライア及び3rdパーティパートナーが契約上の責務を満たしていることを、監査、試験結果、或いは他の評価方法を用いて定期的に確認している。

監査

ID.SC-5：サプライア及び3rdパーティパートナーによる対応及び復旧の計画及び検証が行われている。

復旧

4. まとめ

- 新しい技術には、リスクがつきまとう。リスク対策はITガバナンスの一環としてとらえる。
- ディジタル時代に対応したITガバナンスは技術の多様化、提供の迅速化、複雑なサプライチェーンに対応する必要がある。
- サイバーセキュリティ対策は事業ドメインに対応したコントロールのベストプラクティスの採用が求められる

  →Attack Surfaceの局所化、サプライアとの信頼関係等

  →費用対効果、リスクの受容、PDCA
- 経営陣のコミットメントが必須
- CSA(Control Self Assessment)の適用

NTT DATA

Trusted Global Innovator