「ストレージ応用技術部会」第一歩目
「ビッグデータとセキュリティ」

Storage Applied Technology部会
（ストレージ応用技術部会）

JDSF 新春セミナー
2018年 1月23日

はじめに

- １．昨年の新年交流会では、バズワード「ビッグデータ」第五歩目！と題して遠い未来のストレージについて、ご紹介しました。
今回はビッグデータWGがストレージ応用技術部会となったことを受け、その第一歩目として最近話題のセキュリティについて取り上げてみたいと思います。

- ２．本コンテンツはIT初心者の方が理解できるように、ベースの部分から解説をしております。上級者の方々には物足りない内容になっているかもしれませんが、お含みおきください。

- ３．本コンテンツの一部は後日公開予定でございます。

- ４．本コンテンツを転載されたい場合には、事務局までご一報ください。

ストレージ応用技術部会
(Storage Applied Technology：SAT)
活動方針と応用技術の研究

JDSF 新春セミナー
2018年 1月23日

おさらい

JDSF Japan Data Storage Forum

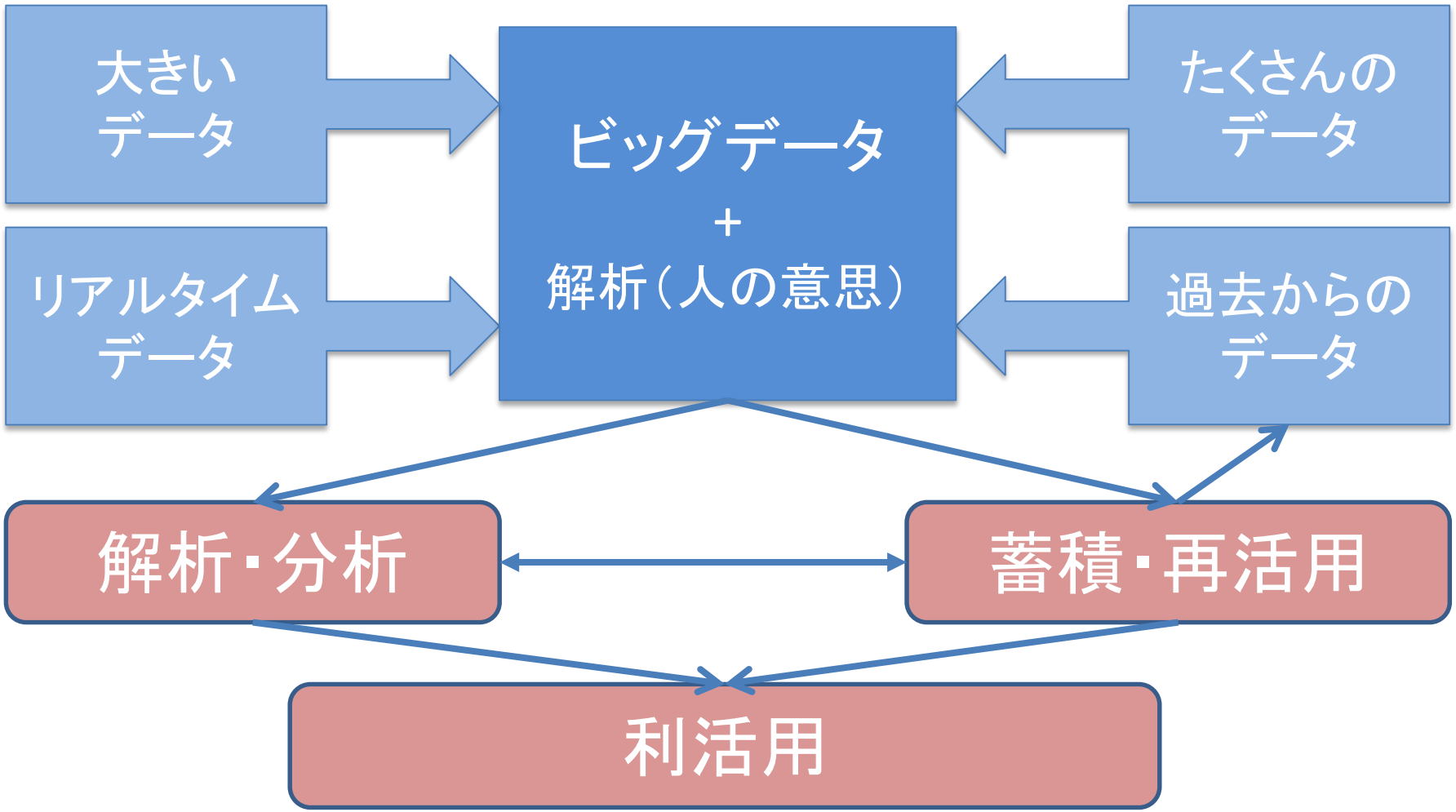
- ビッグデータワーキンググループの年度別活動テーマ（発表資料）
  - 2013年度 ビッグデータの分類とテクノロジー（初級編）
  - 2014年度 ビッグデータのライフサイクルとストレージ要件
  - 2015年度 ビッグデータの活用例から見る未来のストレージ
  - 2016年度 AI技術は未来のストレージに応用できるのか？

成果物はJDSFホームページのアクティビティをご確認ください

（図解）ビッグデータライフサイクルとストレージ要件

JDSF Japan Data Storage Forum

再掲



本年度の活動基本方針

■活動基本方針

- ストレージ活用に係る応用技術の整理と選択したテーマの深堀り、その提言・発信

ランダムにテーマを抽出

- ビッグデータの活用に関する新技術（データ分析など）
- データ保護の為のセキュリティ技術
- ストレージ利用の最適化の為の技術
- アーカイブのコアテクノロジー
  - ビッグデータ解析の元データとして
- クラウド環境に最適化されたデータ管理技術
  - マルチクラウドを上手に使う応用技術　　etc

今年度の活動テーマ

JDSF
Japan Data Storage Forum

応用技術発展
のコアベクトル

利便性向上

収益性向上

業務効率改善
生産性向上

ビッグデータ活用の為の技術

・IoT/M2Mでの活用技術
・データセキュリティ

ストレージ利用の最適化技術

・データ管理技術

最新のインフラ環境への対応技術

・マルチクラウド環境への対応
・アーカイブのコア技術

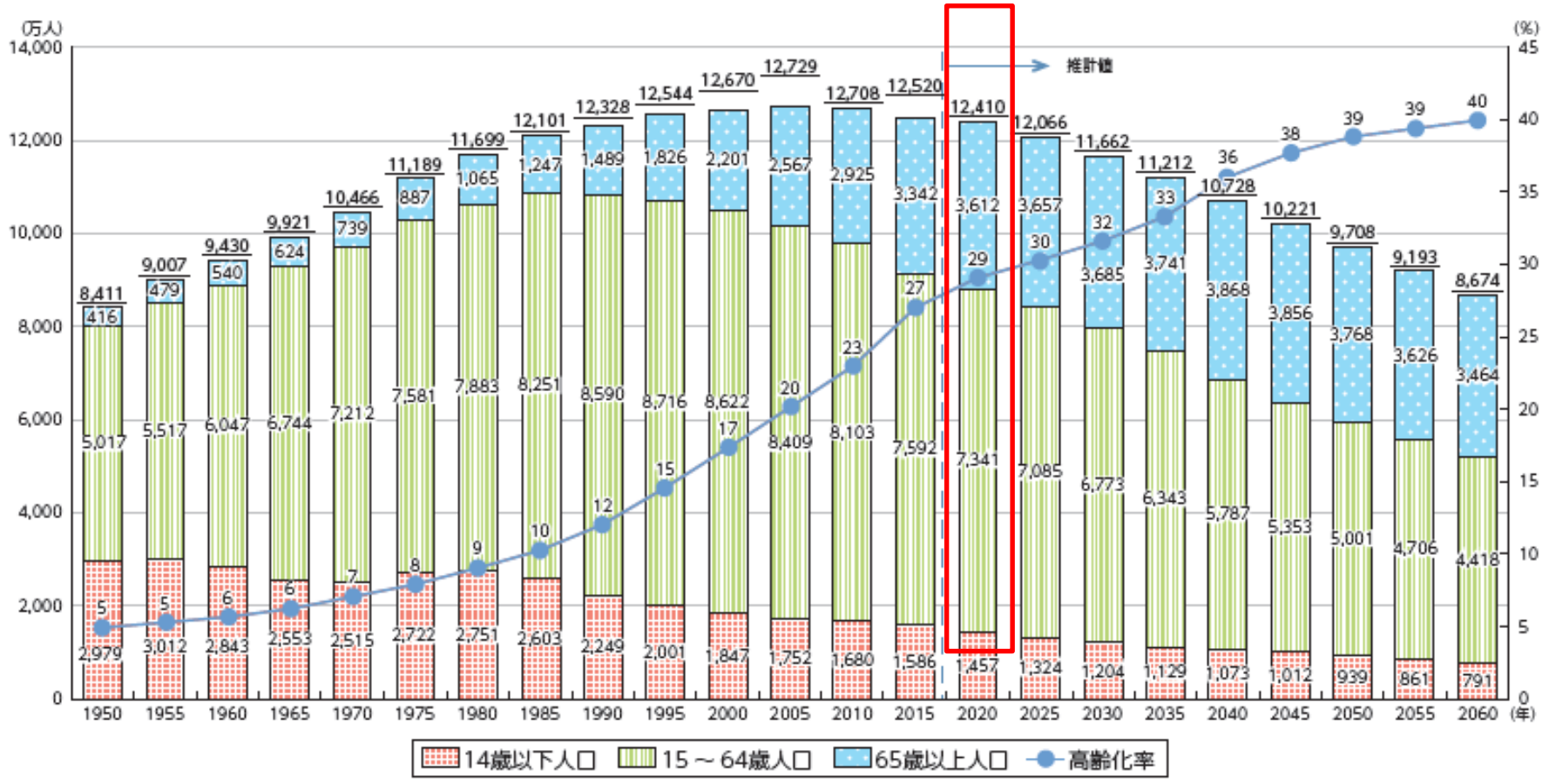
ビッグデータの潮流と考察

What is the Trend of Big Data?

JDSF 新春セミナー
2018年 1月23日

我が国の人口推移

再掲



(出典) 2015年までは総務省「国勢調査」(年齢不詳人口を除く)、
2020年以降は国立社会保障・人口問題研究所「日本の将来推計人口（平成24年1月推計)」(出生中位・死亡中位推計)

ストレージの近未来像（1つの回答と考える）

JDSF Japan Data Storage Forum

Artificial Intelligence

再掲

- AIによる自動化を実現したITシステムの中のストレージ
  - ストレージを意識しなくてもデータ管理・分析できる
    - 例）問題点を音声でヒアリングし調査結果を出してくれる
    - 例）必要になる性能指標を出してくれる
    - 例）アプリケーションに最適化してくれる
    - 例）地理情報や気象データから災害対策のリスクを数値化してくれる
    - 例）新旧技術の互換性を吸収
  - 適材適所にストレージリソースを自動分配（運用）してくれる
    - 例）データを最適配置しコストバランスを鑑みた構成を推奨してくれる
    - 例）必要なデータを必要な時に、必要なストレージリソース上へ移動させてくれる

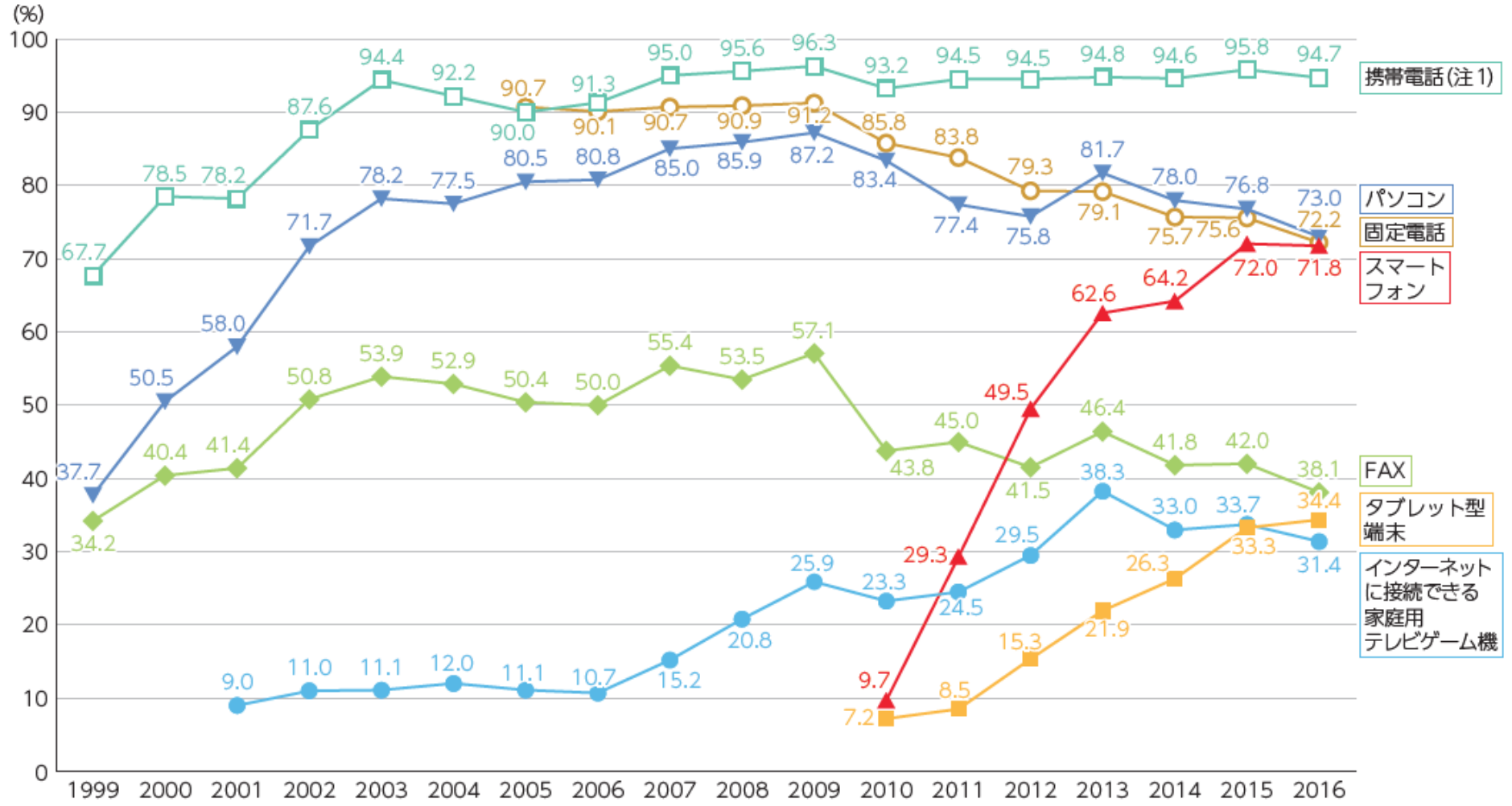
近未来のITインフラとストレージ考察

再掲

- ITインフラは言葉通り、インフラの一部となっていく。
  - 電気を使うときに、発電所を意識しますか？
  - ガスを使うときは、元栓を回すだけ
  - 水道は蛇口をひねれば出る
  - 電話は家庭に一台から、一人に一台へ
    - 家から個人に付随するという変化
- ストレージは容量が欲しければ、、、、WEBでちょいちょい
- ストレージを「買う」から「利用する」へ
  - 月々支払い

ストレージはエンドユーザーから見えなくなっていく

我が国の情報通信機器の保有状況の推移（世帯）



(注1) 携帯電話にはPHSを含み、2009年から2012年まではPDAも含めて調査し、2010年以降はスマートフォンを内数として含めている。

（出典）総務省 通信利用動向調査

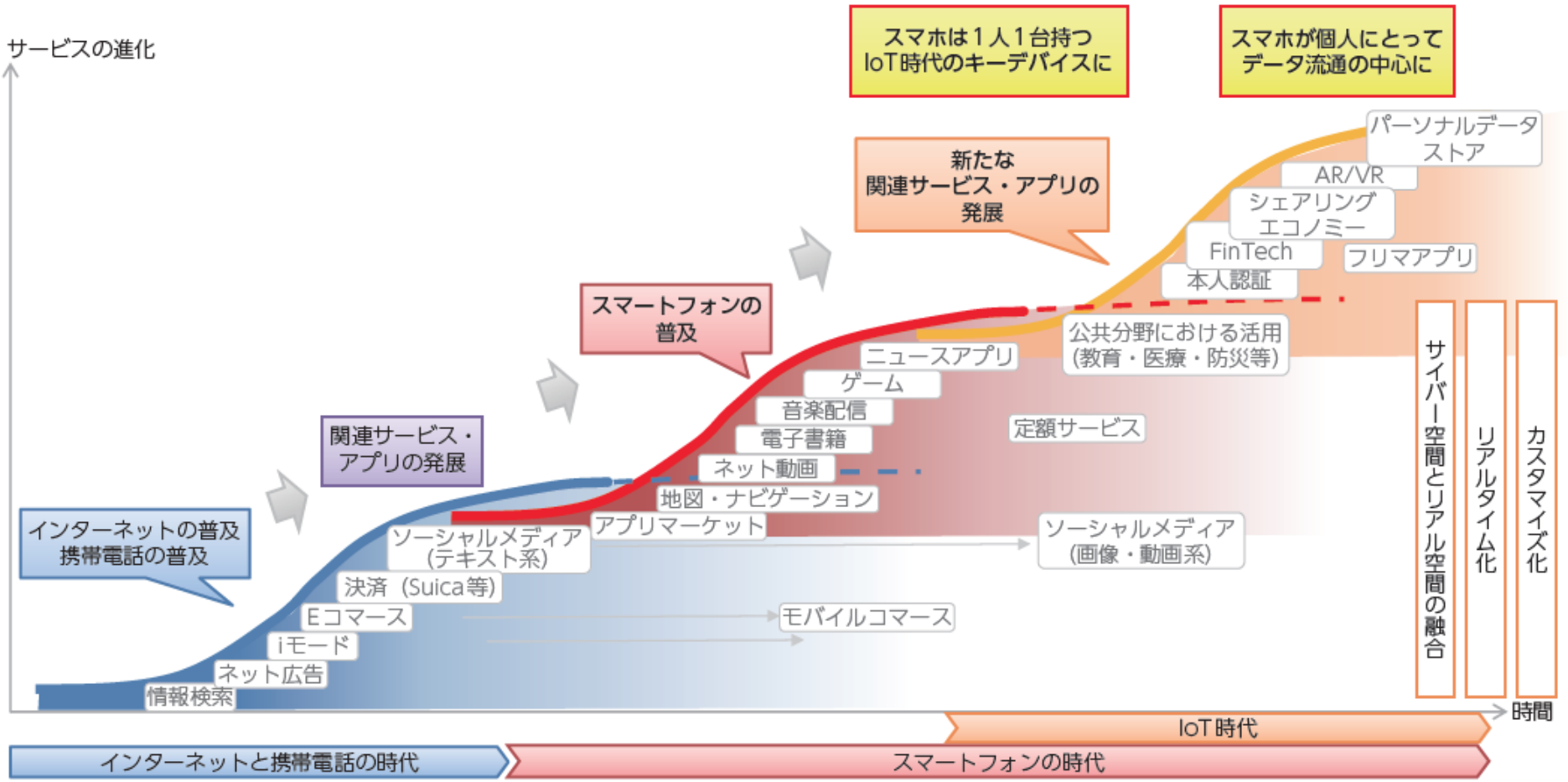
主なSNSの利用率（2016年 全体・性年代別）

JDSF Japan Data Storage Forum

	LINE	Facebook	Twitter	mixi	Mobage	GREE	Google+	YouTube	ニコニコ動画	Vine	Instagram
全体（N=1500）	67.0%	32.3%	27.5%	6.8%	5.6%	3.5%	26.3%	68.7%	17.5%	2.9%	20.5%
10代（N=140）	79.3%	18.6%	61.4%	2.9%	6.4%	3.6%	28.6%	84.3%	27.9%	5.7%	30.7%
20代（N=217）	96.3%	54.8%	59.9%	13.4%	9.2%	6.9%	29.5%	92.2%	36.4%	7.4%	45.2%
30代（N=267）	90.3%	51.7%	30.0%	9.4%	9.7%	4.5%	37.5%	88.4%	19.5%	3.7%	30.3%
40代（N=313）	74.1%	34.5%	20.8%	8.3%	4.8%	3.2%	30.0%	77.3%	15.3%	1.6%	16.0%
50代（N=260）	53.8%	23.5%	14.2%	5.8%	4.2%	2.7%	25.4%	55.4%	9.2%	1.2%	12.3%
60代（N=303）	23.8%	10.6%	4.6%	1.0%	1.0%	1.0%	10.2%	29.7%	6.6%	0.3%	1.3%
男性（N=756）	63.6%	32.0%	25.7%	6.5%	7.5%	4.2%	25.4%	72.0%	19.8%	2.1%	13.9%
男性10代（N=72）	70.8%	16.7%	54.2%	2.8%	9.7%	5.6%	23.6%	81.9%	27.8%	4.2%	20.8%
男性20代（N=111）	94.6%	50.5%	53.2%	14.4%	14.4%	9.0%	33.3%	91.0%	46.8%	4.5%	34.2%
男性30代（N=136）	86.0%	46.3%	30.1%	5.1%	11.8%	5.1%	34.6%	90.4%	20.6%	2.9%	18.4%
男性40代（N=159）	68.6%	36.5%	21.4%	8.8%	6.3%	5.7%	25.2%	78.0%	17.6%	1.9%	11.3%
男性50代（N=130）	49.2%	24.6%	11.5%	6.2%	4.6%	0.0%	23.8%	59.2%	6.9%	0.8%	6.9%
男性60代（N=148）	23.6%	14.2%	4.1%	1.4%	1.4%	1.4%	13.5%	40.5%	8.8%	0.0%	0.0%
女性（N=744）	70.4%	32.5%	29.3%	7.1%	3.6%	2.7%	27.3%	65.3%	15.1%	3.6%	27.3%
女性10代（N=68）	88.2%	20.6%	69.1%	2.9%	2.9%	1.5%	33.8%	86.8%	27.9%	7.4%	41.2%
女性20代（N=106）	98.1%	59.4%	67.0%	12.3%	3.8%	4.7%	25.5%	93.4%	25.5%	10.4%	56.6%
女性30代（N=131）	94.7%	57.3%	29.8%	13.7%	7.6%	3.8%	40.5%	86.3%	18.3%	4.6%	42.7%
女性40代（N=154）	79.9%	32.5%	20.1%	7.8%	3.2%	0.6%	35.1%	76.6%	13.0%	1.3%	20.8%
女性50代（N=130）	58.5%	22.3%	16.9%	5.4%	3.8%	5.4%	26.9%	51.5%	11.5%	1.5%	17.7%
女性60代（N=155）	23.9%	7.1%	5.2%	0.6%	0.6%	0.6%	7.1%	19.4%	4.5%	0.6%	2.6%

（出典）総務省情報通信政策研究所「情報通信メディアの利用時間と情報行動に関する調査」

スマホ関連サービス･アプリ変遷の概念図

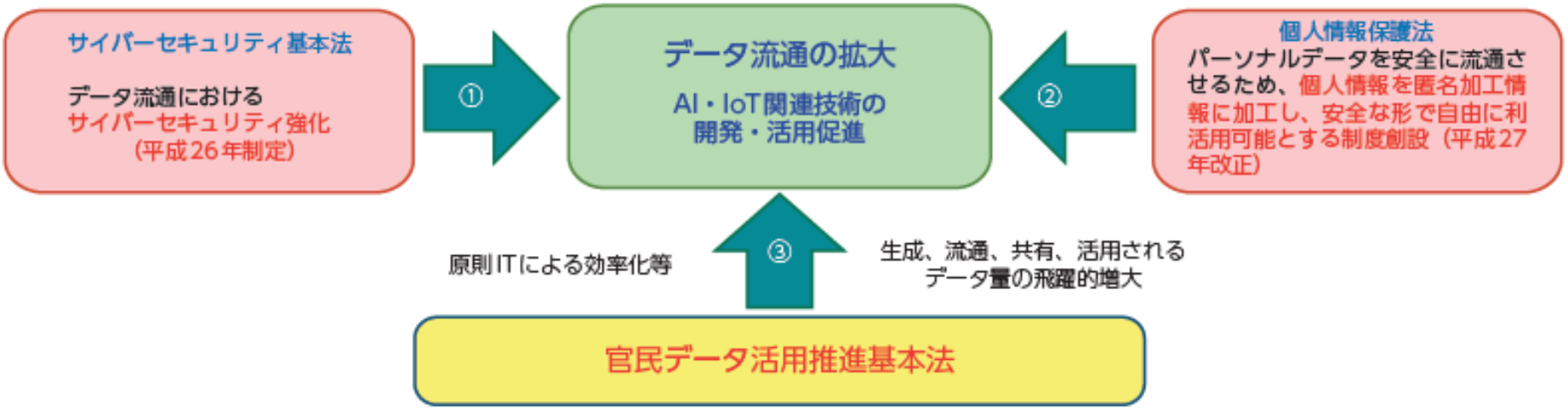


（出典）総務省「スマートフォン経済の現在と将来に関する調査研究」（平成29年）

注目しているキーワード

- FinTech
  - ブロックチェーン
  - 決済
  - 個人資産管理
  - 融資　等
- シェアリングエコノミー
  - Airbnb
  - Uber　等
- データローカライゼーション
  - GDPR　等

データ流通・利活用における課題



（出典）内閣官房情報通信技術（IT）総合戦略室「官民データ活用推進戦略会議の開催について＊2」より総務省作成

改正個人情報保護法の主なポイント

ポイント	内容
1. 個人情報の定義の明確化	・特定の個人の身体の一部の特徴をコンピュータで処理できるよう変換した符号又はサービス利用や書類において対象者ごとに割り振られる符号であって、政令又は個人情報保護委員会規則で定められたものは、「個人識別符号」として、個人情報に該当することが明確化された。 ・その他、本人に対する不当な差別、偏見等が生じないようにその取扱いに特に配慮を要する情報として、人種、信条、病歴、犯罪の経歴等を含む個人情報が「要配慮個人情報」（いわゆるセンシティブ情報）として規定され、一段高い規制の対象となった。
2. 匿名加工情報制度の導入	・個人情報の有用性を確保する観点から、「匿名加工情報」という新たな制度が設けられた。 ・「匿名加工情報」とは、特定の個人を識別することができないように加工し、かつ当該個人情報を復元することができないようにしたもの。匿名加工情報の作成は、個人情報保護委員会規則で定める基準に従って行わなければならない。
3. 個人情報を第三者に提供する場合の確認と記録の作成の義務化	・個人情報の流通の適正さを確保するための規定として、今後、個人データを第三者に提供する場合、提供した記録を作成し、また第三者から個人データの提供を受ける場合にも、取得の経緯などを確認した上で、記録を作成しなければならない。 ・事業者がオプトアウト手続（本人の求めに応じて個人データの提供を停止することとし、あらかじめ、その旨や提供する個人データの項目等を本人に通知又は本人が容易に知り得る状態に置くことで、個人データを第三者に提供できる手続）を利用する場合、個人情報保護委員会への届出が義務づけられた。
4. 個人情報保護委員会の設置	・新たに個人情報保護に関する独立した監督機関として個人情報保護委員会を設置した。 ・個人情報保護委員会は、報告徴収、立入検査、指導、助言、勧告及び命令の権限が付与され、個人情報の適正な取扱いを確保すべく、事業者に対する指導・監督を行う勧告や命令を行うことができる。
5. 外国にある第三者に対する個人データの提供に関する規定の整備	・個人情報の取扱いのグローバル化に対応すべく、1）外国にある第三者へ提供することについて、本人の同意を得ている場合、2）提供先の第三者が、個人情報保護制度が日本と同等の水準にあると認められる外国にある場合、又は3）提供先の第三者が個人情報保護委員会の規則で定める基準に適合する体制を整備している場合に限り、外国にある第三者に対して国内と同様に個人データを提供することが可能。

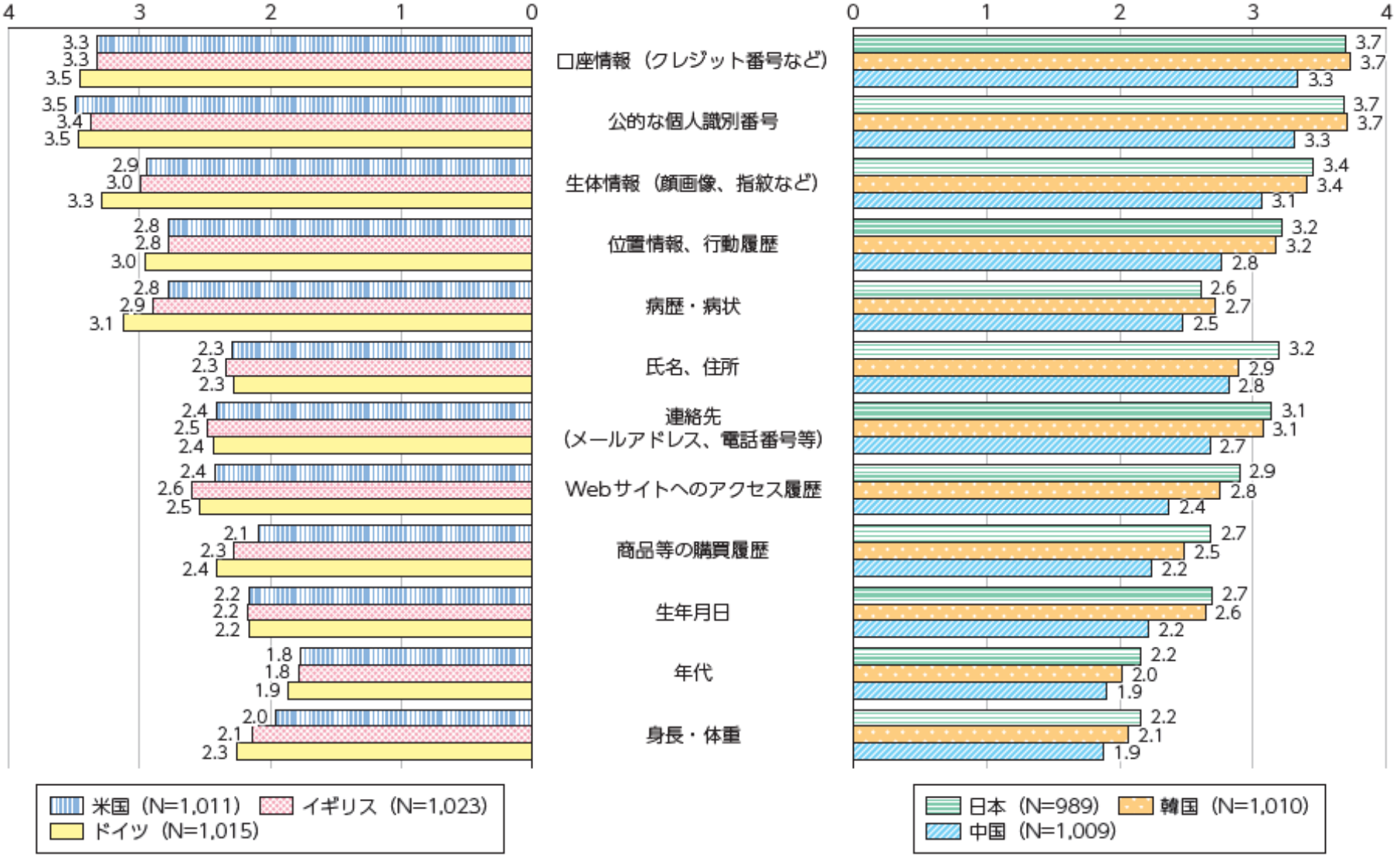
（出展）情報通信白書H29

主なデータ利活用例のイメージと想定される課題の例

産業	利活用例のイメージ	収集媒体	収集データ	主な課題の例	個人情報関係	対称特定	主な関係法令等
製造業	スマート工場による生産性向上やコスト削減等のためのデータ収集	工作機械 産業ロボット センサ等	機能状況（異常検知等） 環境情報等	・機械の所有者（リース元等）との法律関係	なし	○	民法 （事業者間の契約）
農業	農業の生産性向上のための気象データ等の観測	IoT環境センサ（温度計、湿度計等）	温度、湿度、照度等の環境データ、生育データ等	・センサ設置場所の所有者（農家等）との法律関係	なし	○	民法 （事業者・農家間の契約）
金融保険業	自動車損害保険における最適な保険商品提供のためのデータ収集	自動車、車載センサ等	走行データ（速度、ルート）等	・専用機器を取り付けて、走行することに同意した者との法律関係	△（※事業者と協力者（個人）間の契約の場合は以下と同様）	○	民法 （事業者間、事業者と協力者（個人）間の契約）
健康産業 （ヘルスケア）	ヘルスケアサービスのための体調データ収集	ウエアラブル機器	歩数、活動量、脈拍、体温等	・サービス契約の際の利用目的、第三者提供等の条件 ・診療情報、投薬情報や、要配慮個人情報（病歴等）との関係	○（※目的の明示、第三者提供の際の同意等が必要）	○	個人情報保護法 民法 （事業者・消費者間の契約（サービス約款等を含む）） 消費者契約法等
サービス	スマートハウス（省エネ、見守り）における家電制御のためのデータ収集	センサ付家電	家電の使用データ、消費電力データ等	・サービス契約の際の利用目的、第三者提供等の条件		○	
広告宣伝・小売・観光	広告宣伝・小売・観光等における、嗜好・需要に合わせた最適なサービス提供のためのデータ収集	ICカード スマートフォン等	購買データ、位置情報等			△（特定多数）	
自動運転関連	自動運転のための、公道での撮影データ収集	カメラ	画像データ等	・不特定多数の個人情報（顔画像等）や、著作物の画像が含まれてしまう可能性		不特定多数	個人情報保護法 著作権法

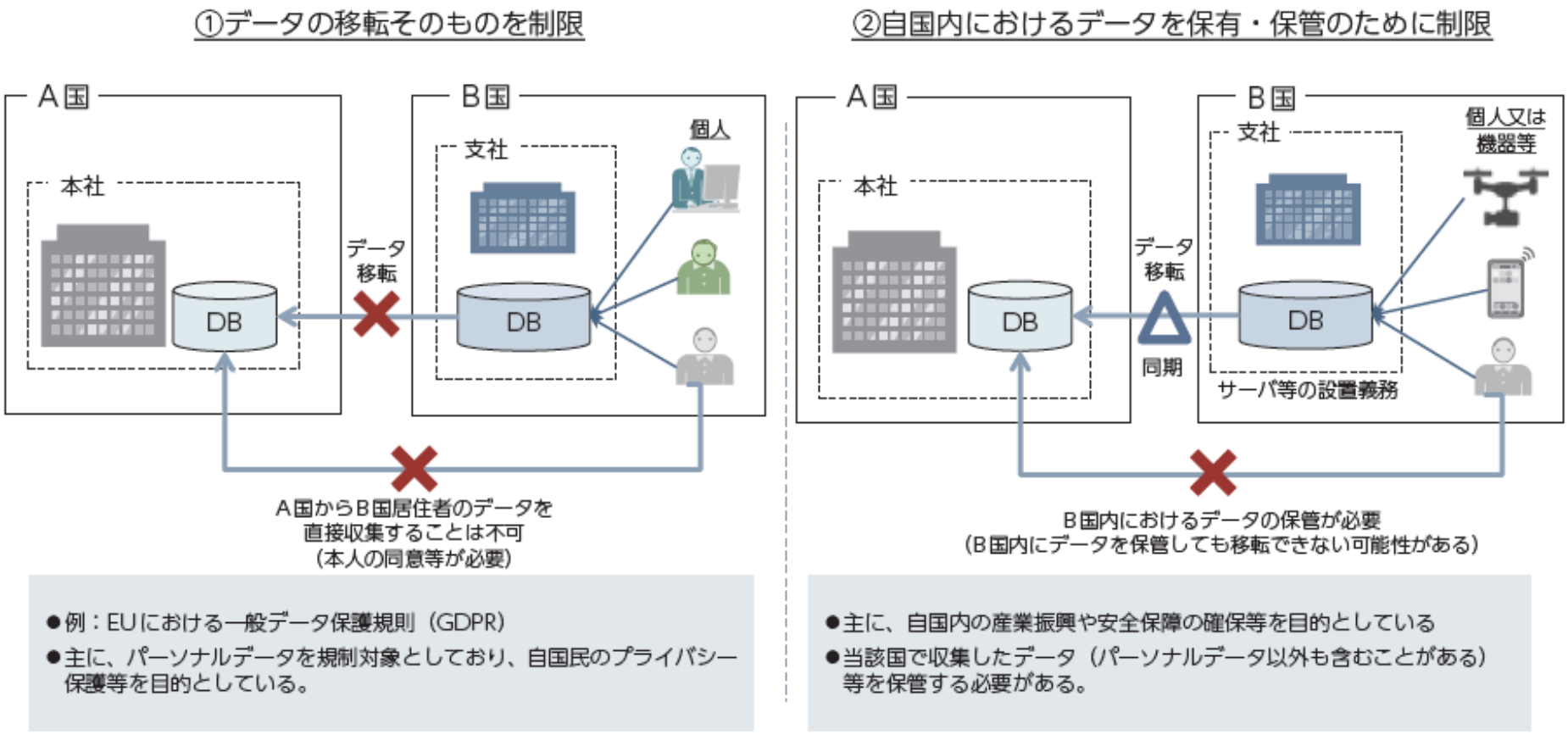
（出典）知的財産戦略本部「新たな情報財検討委員会報告書」より作成

各パーソナルデータに対する不安感



（出典）総務省「安心・安全なデータ流通・利活用に関する調査研究」（平成29年）

データローカライゼーションの例



（出典）総務省「安心・安全なデータ流通・利活用に関する調査研究」（平成29年）

EUのGDPRのポイントと第3国へのデータ移転条件

JDSF Japan Data Storage Forum

域外適用

EU域内の事業者だけでなく、EU域外からEU域内の居住者にサービスを提供又はモニタリングをしている海外企業にも本規則を適用

外部委託先への適用

個人データを管理するデータ管理者だけでなく、データ処理（収集、保管等）の委託先となるデータ処理者にも適用。

データ保護影響分析

新技術の利用によって個人の権利に対するリスクが高い場合、データ保護影響分析を実施すること。

第3国へのデータ移転制限

第3国への個人データ移転を制限。移転に対しては、一定の条件を満たすことが必要（十分性認定やBCRなど）

個人の権利保護強化

個人情報の収集、利用に際しての個人（≒情報提供者）による明確な同意の取得が必要。忘れられる権利についても明記。

データ保護責任者の設置

データ保護に関する知識、専門性を有するデータ保護責任者（DPO）を任命・設置し、監督当局に通知。

情報侵害時の公開義務

個人情報の侵害が発生した場合、72時間以内に侵害が発生した国の監督当局に報告し、個人にも遅滞なく通知。

高額な制裁金

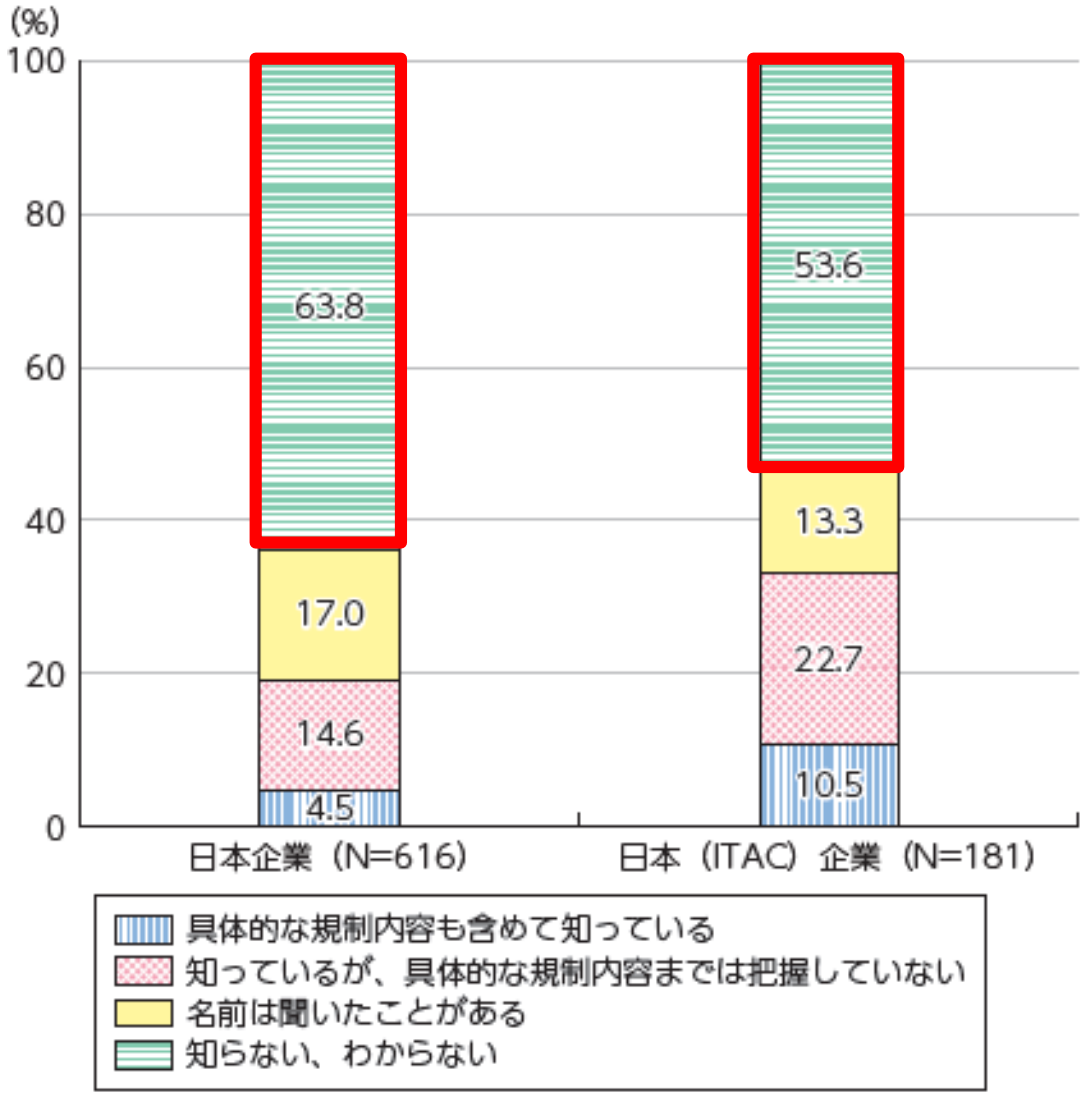
GDPR違反企業には、最大全世界の年間売上の4%または2,000万ユーロ（約25億円）のいずれか高い方の制裁金を科す。

第3国へのデータ移転条件

手段	概要
1）十分性認定	欧州委員会から個人データの十分な保護措置が確保されていることの認定を得ることで、データの越境移転が可能。
2）明確な同意の取得	データ主体の個人から個人情報の移転に関する同意を取得。
3）拘束的企業準則（BCR）	グループ内で統一された情報管理を実施している場合に適用可能。データ保護機関に情報管理方法の承認を得ることで、グループ企業を包括したデータ移転が可能。（※多国籍企業間に多い）
4）標準契約条項（SCC）	データ保護機関の承認を得た契約フォーマットで個別契約を交わした企業間に適用。

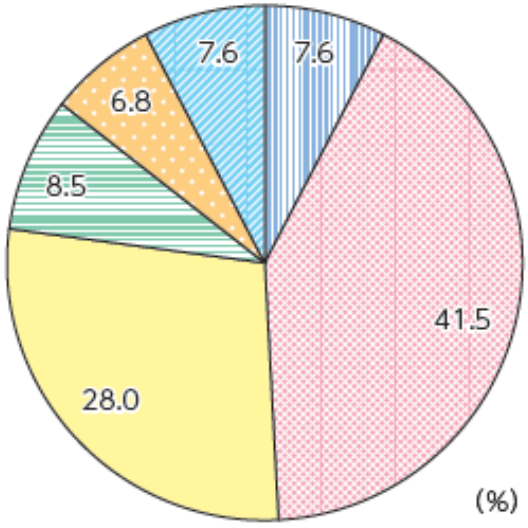
（出典）総務省「安心・安全なデータ流通・利活用に関する調査研究」（平成29年）

GDPRに関する企業の認知度



（出典）総務省「安心・安全なデータ流通・利活用に関する調査研究」（平成29年）

企業のGDPRへの対応・検討状況及び対応内容

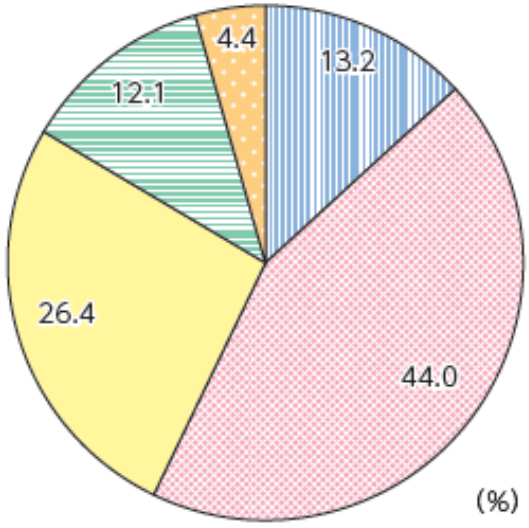


(N=118)

ベース：GDPRについて知っている

- GDPRに既に対応済みである
- GDPRへの対応方法について現在検討している
- GDPRへの対応方法について検討することを予定している
- GDPRへの対応方法について検討していない
- GDPRによるビジネスへの影響はない
- わからない

(出典)総務省「安心・安全なデータ流通・利活用に関する調査研究」(平成29年)



(N=91)

ベース：GDPRに既に対応済または対応方法について検討/検討予定

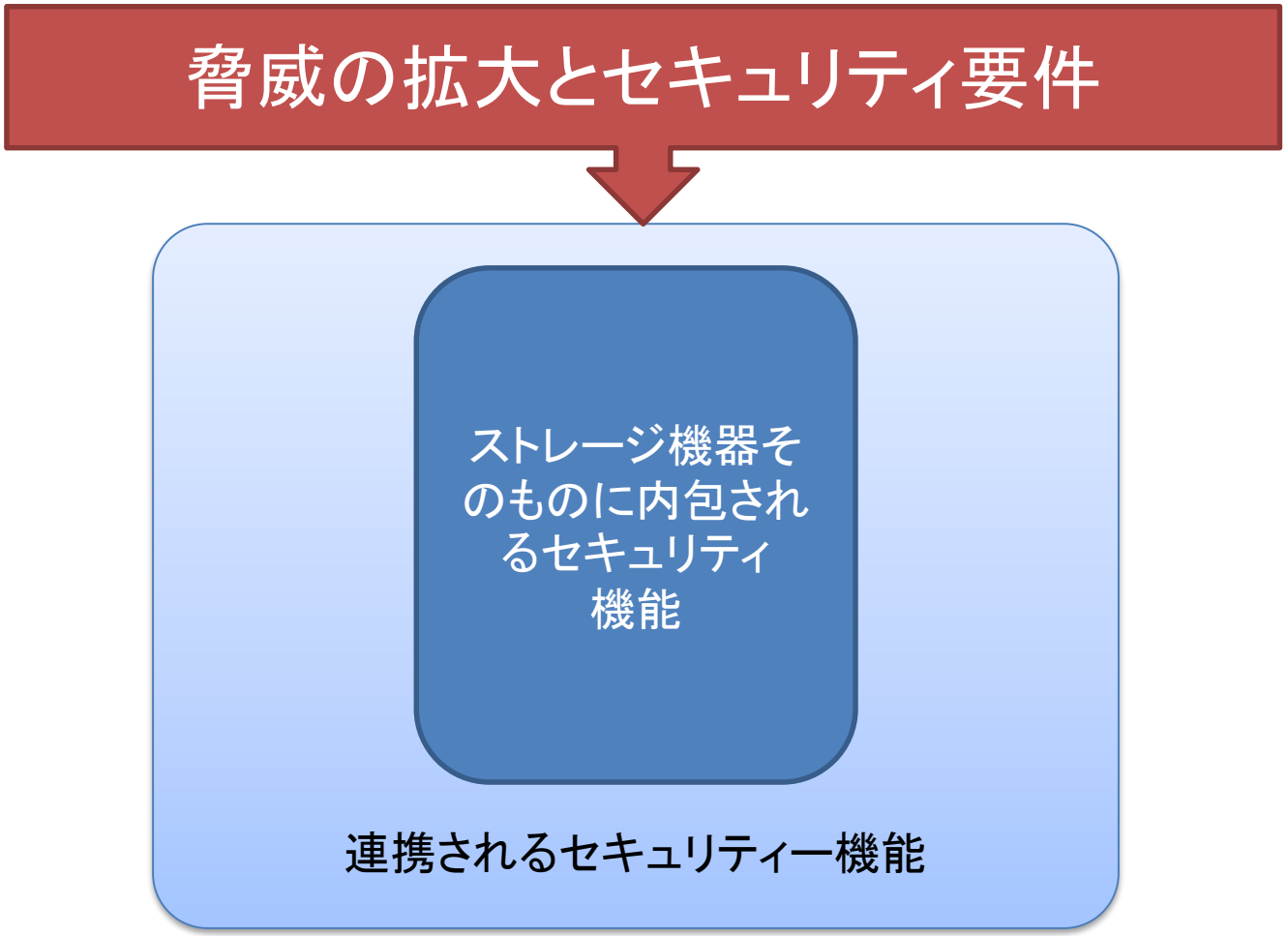
- 政府間交渉等に基づくデータ越境移転の枠組みの設定
- データの越境移転を図りたい事業者とデータ越境移転に関する契約を締結する
- 個人からデータの越境移転に関する同意を取得
- データ越境移転が発生しないように、EU域内の個人データをEU域内で管理
- よくわからない

(出典)総務省「安心・安全なデータ流通・利活用に関する調査研究」(平成29年)

進むデータ利活用と求められること

- IoT/ビッグデータ利活用にはセキュアな環境が必要
- GDPR等のコンプライアンス

忘れてはいけないこと＝セキュリティ



https://www.cyberscoop.com/forrester-iot-security-report-q1-2017/

ビッグデータ利活用とデータセキュリティ

JDSF 新春セミナー
2018年 1月23日

ストレージ運用・データ管理を取り巻く セキュリティーリスクと必要な対策

JDSF Japan Data Storage Forum

標的型攻撃対策

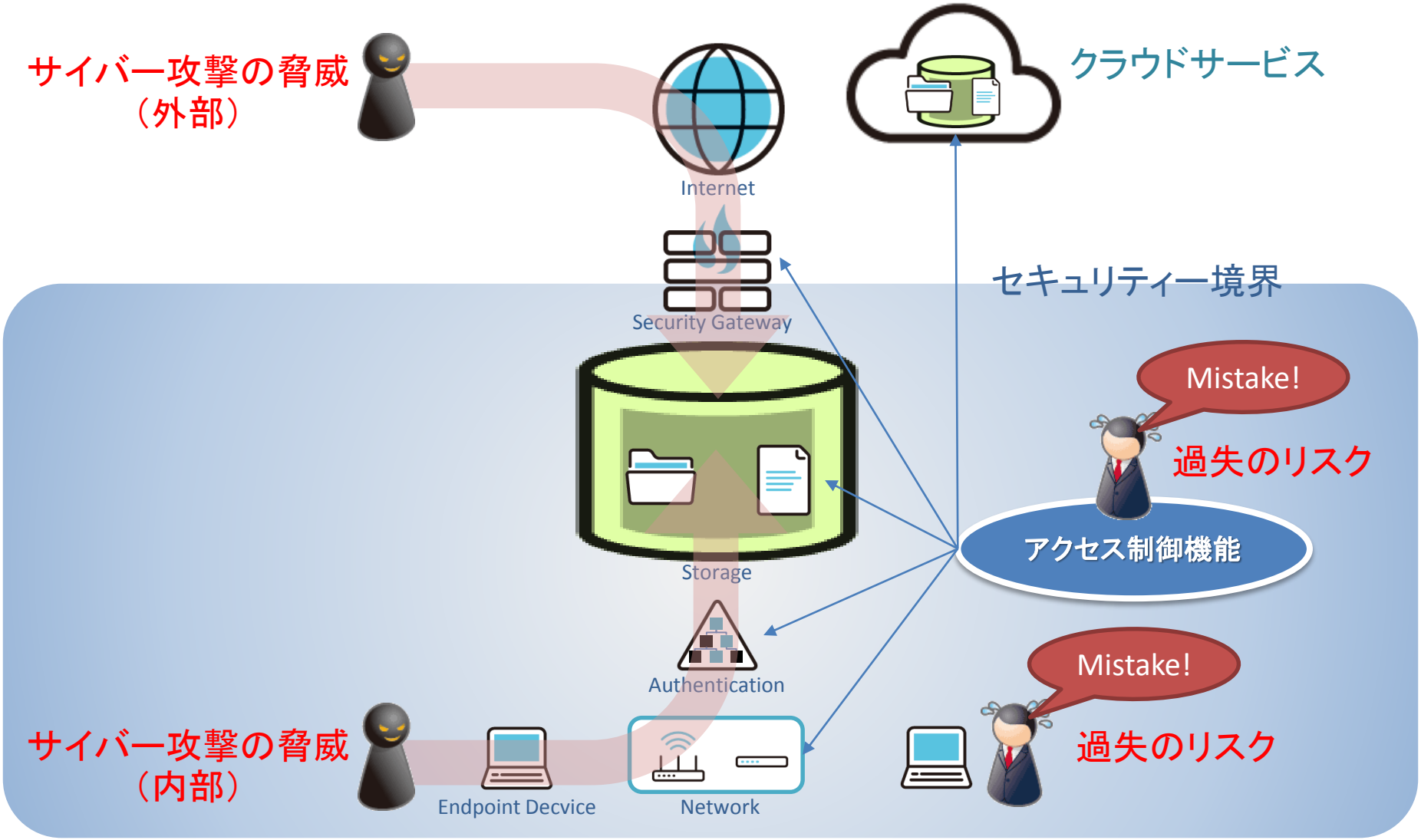
認証強化

- **「サイバー攻撃」　によるデータ窃取・改ざん**
  - ✓ マルウェア感染端末からの不正アクセス
  - ✓ ID/PSWD盗用による不正なアクセス
  - ✓ 正規権限を持った内部犯による不正アクセス
  - ✓ ディスクドライブ等メディアの持ち出し
- **「過失」　によるデータの漏洩・流出**
  - ✓ ストレージボリュームやフォルダへのアクセス権設定ミス
  - ✓ ファイルへの共有権設定ミス、コンテンツリンクの設定ミス
  - ✓ データの誤送信

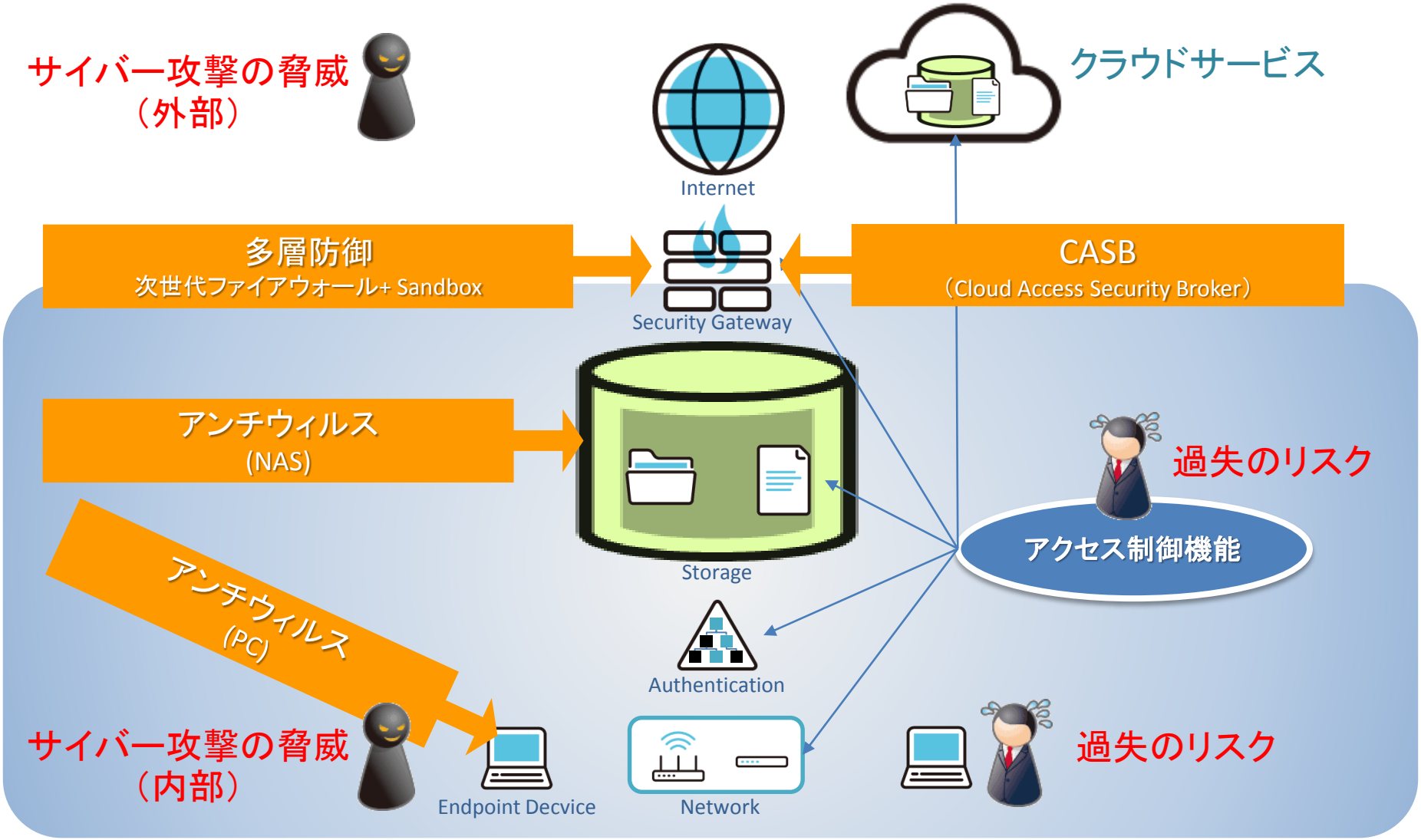
DLP
(Data Loss Prevention)

暗号化

セキュリティーリスクはどこにある？



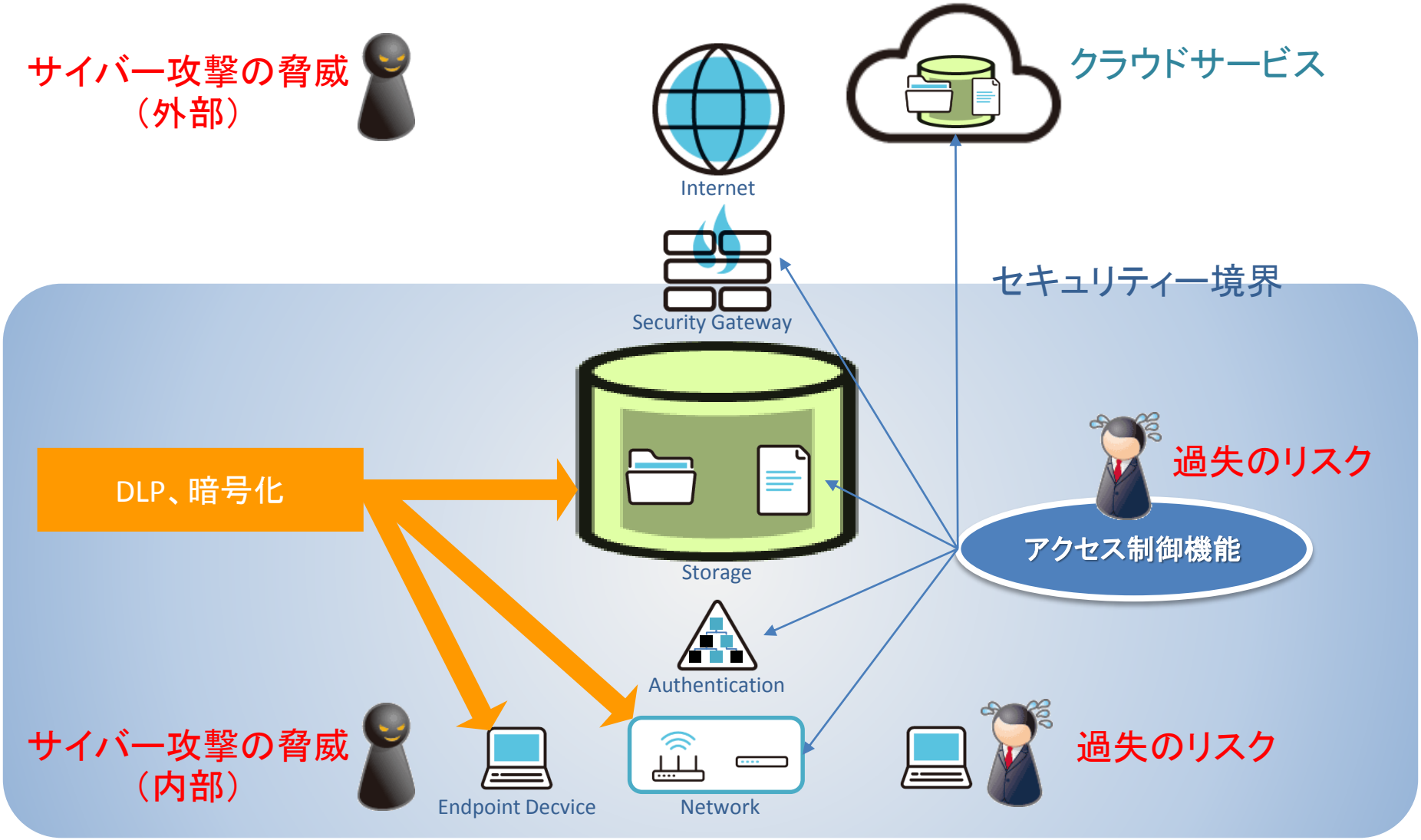
標的型攻撃対策


サイバー攻撃の脅威
（外部）
Internet
クラウドサービス
多層防御
次世代ファイアウォール+ Sandbox
Security Gateway
CASB
（Cloud Access Security Broker）
アンチウィルス
(NAS)
Storage
過失のリスク
アクセス制御機能
アンチウィルス
(PC)
Authentication
サイバー攻撃の脅威
（内部）
Endpoint Decvice
Network
過失のリスク

標的型攻撃対策

- 標的型攻撃対策
  - 多層防御
    - Firewall, IDS/IPS,
    - DNS, Proxy
    - Filtering, WAF, DB Firewall
    - Sandbox, SIEM
  - アンチウィルス, アンチマルウェア
    - サーバー用
    - NAS用
    - Windows端末用
    - スマートデバイス用
  - クラウドサービス利用管理 (CASB)
    - 高リスクサービスへのアクセス検出
    - アクセス制御機能
    - DLP機能
    - 暗号化機能

DLP (Data Loss Prevention)、暗号化・無意味化

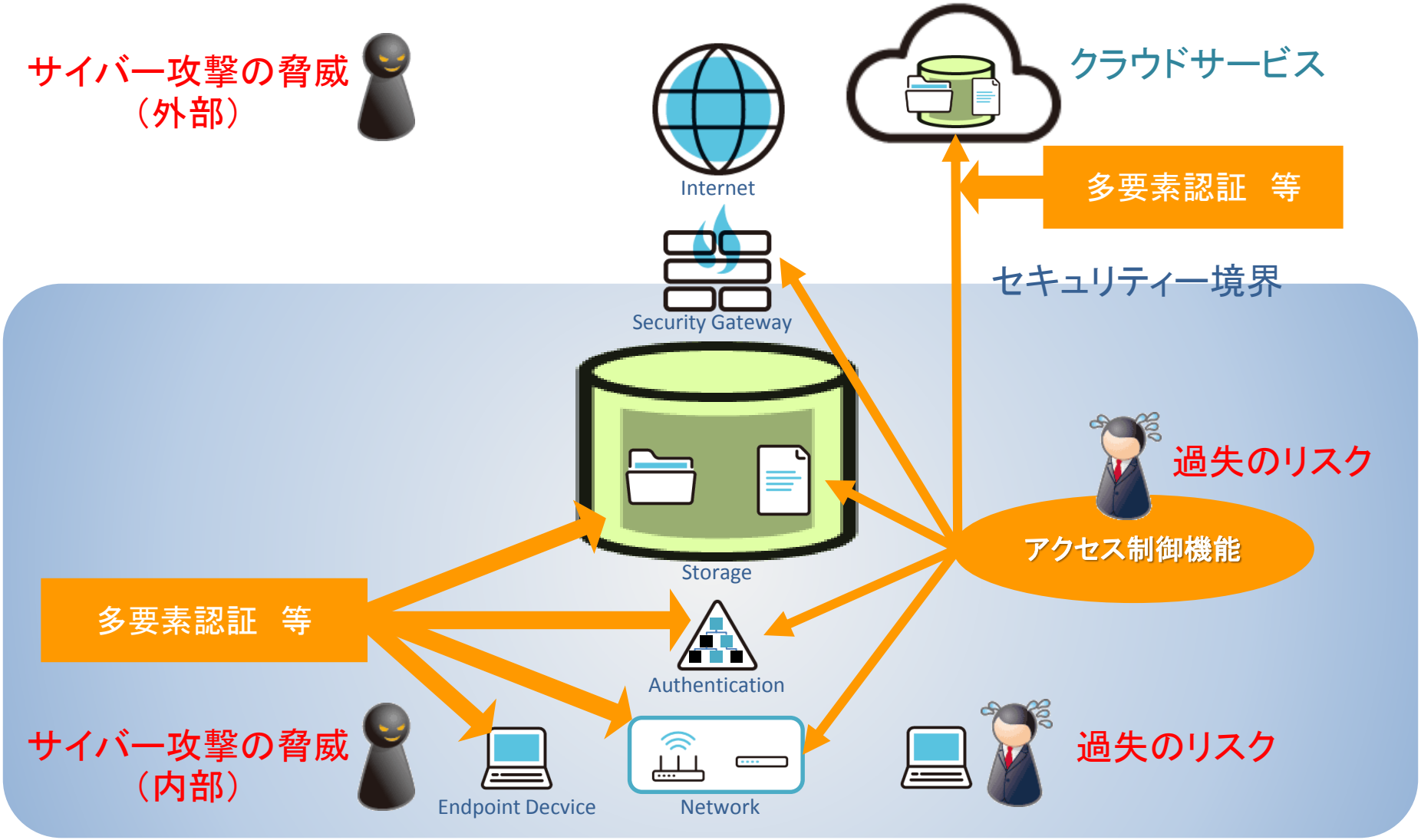


DLP、暗号化・無意味化機能

- DLP (Data Loss Prevention)
  - データ評価
    - リスク評価
    - 重み付け
  - 機密データの管理
    - 利用状況管理
    - 複製・編集・移動/送信 等の権限を制御

- 暗号化・無意味化
  - 暗号化
    - 格納されたデータの暗号化
    - デバイスそのものの暗号化（ディスク丸ごと暗号化）
  - 無意味化
    - 分散書き込み
    - 割符
    - 重複排除によるデータの断片化

アクセス権管理と認証強化



アクセス権管理と認証強化

- アクセス権管理機能
  - アクセス権限設定
    - ストレージシステムの管理者権限設定
    - ボリュームやディレクトリ・フォルダ・ファイルレベルのアクセス権限の設定
    - 閲覧・編集・削除・複製など、詳細な権限の設定

    ※ストレージが機能提供するケースと、OS・ネットワークの機能を利用するケースがある
  - ストレージ装置への物理的なアクセス制限
    - 入退室管理
    - ラック施錠
    - ストレージ装置への施錠
- 認証強化
  - アクセス権限に基づく認証レベルの設定と運用
    - 機密データを取り扱うシステムに対する多要素認証の適用
    - 認証機能と暗号/複合機能の連携
    - データ管理者に対するバイオメトリクス等の高度な認証システムの適用

セキュリティ分野ではこの辺りを深掘り

- ストレージレベルのセキュリティ
- ネットワークレベルのセキュリティ
- アプリケーションレベルのセキュリティ

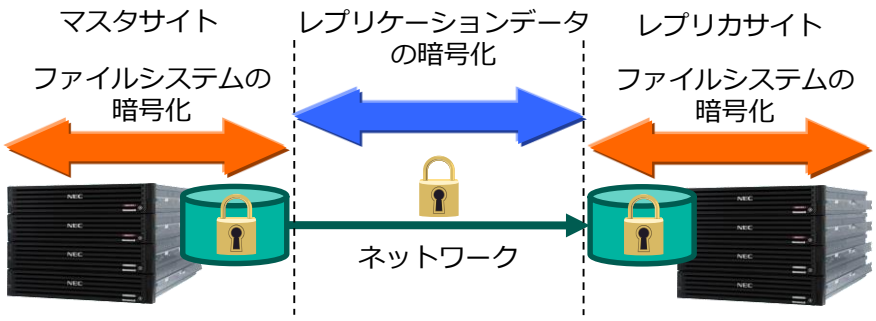
ストレージレベルのセキュリティ（例: NEC iStorage HS）

JDSF Japan Data Storage Forum

盗聴や盗難からデータを守る「暗号化機能」

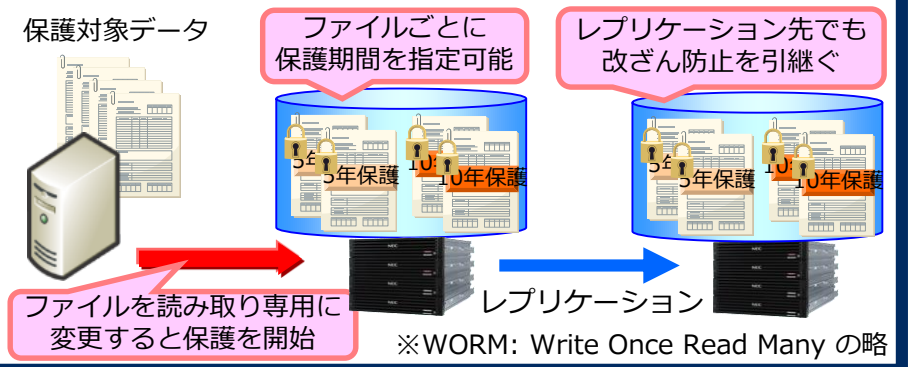
2種類の暗号化機能で機密データを保護

1. ファイルシステムの暗号化 … 盗難や故障交換したHDDのデータ保護
2. レプリケーションデータの暗号化 … 回線の盗聴からのデータ保護



改ざん防止機能(WORM)で法令・運用ルールを遵守

1. ファイルの書き換えや削除などの操作から保護
2. 法令や運用ルール等でデータ保護が義務付けられた環境で活躍



※WORM: Write Once Read Many の略

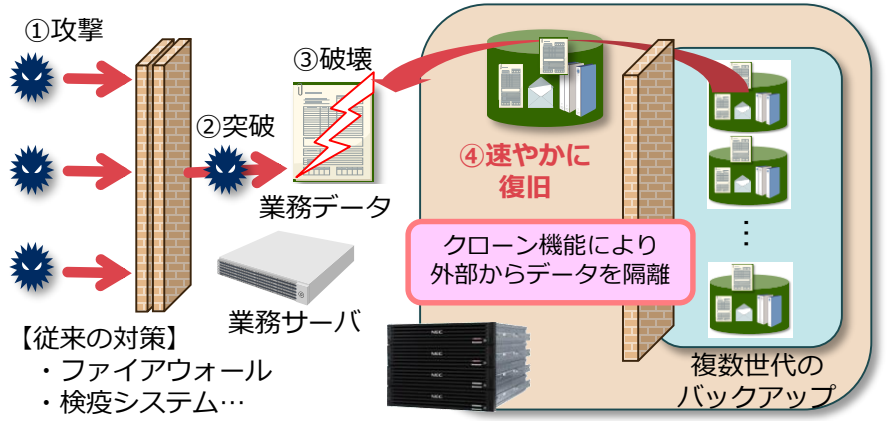
削除データの漏えいを防ぐ動的データ完全消去機能

1. 無停止で論理的に削除したデータをHDD上から完全消去*1
2. 個人情報の保護等、厳しい情報セキュリティポリシー(機密データの完全消去等)に対応

*1: 米国国防総省準拠方式(DoD5220.22-M)

クローン機能を使ったデータ保護（ランサム対策）

バックアップを隠蔽し、感染サーバからのアクセス防止



脆弱性検知および対策案提示型セキュリティ

製品概要

ITシステム全体の自動的なIT資産管理・深い脆弱性診断
および対策案を提供するアプライアンス。

Penetration Test | Audit | Compliance

主な特徴

■エージェントレスのIT資産管理
全体のITインフラの機器を自動的に検知が可能。

■脆弱性診断から対応案を提示
グレー/ブラックボックスで脆弱性検知及び設定欠如の指摘を実施。

■コンプライアンス管理
SOX,PCI-DSS,ISOをなどに準拠しコンプライアンスチェックを実施。

診断範囲

- ネットワーク機器(FW, IPS を含む)
- VoIP システム
- オペレーティングシステム
- デスクトップアプリケーション
- ミドルウェア
- 仮想化プラットフォーム
- セキュリティシステム
- ビジネスシステム (ERPなど)
- ICS/SCADA プラットフォーム
- データベース

未知の脆弱性に対してリスクを分析し　脆弱性DBを整備する能力

エピローグ

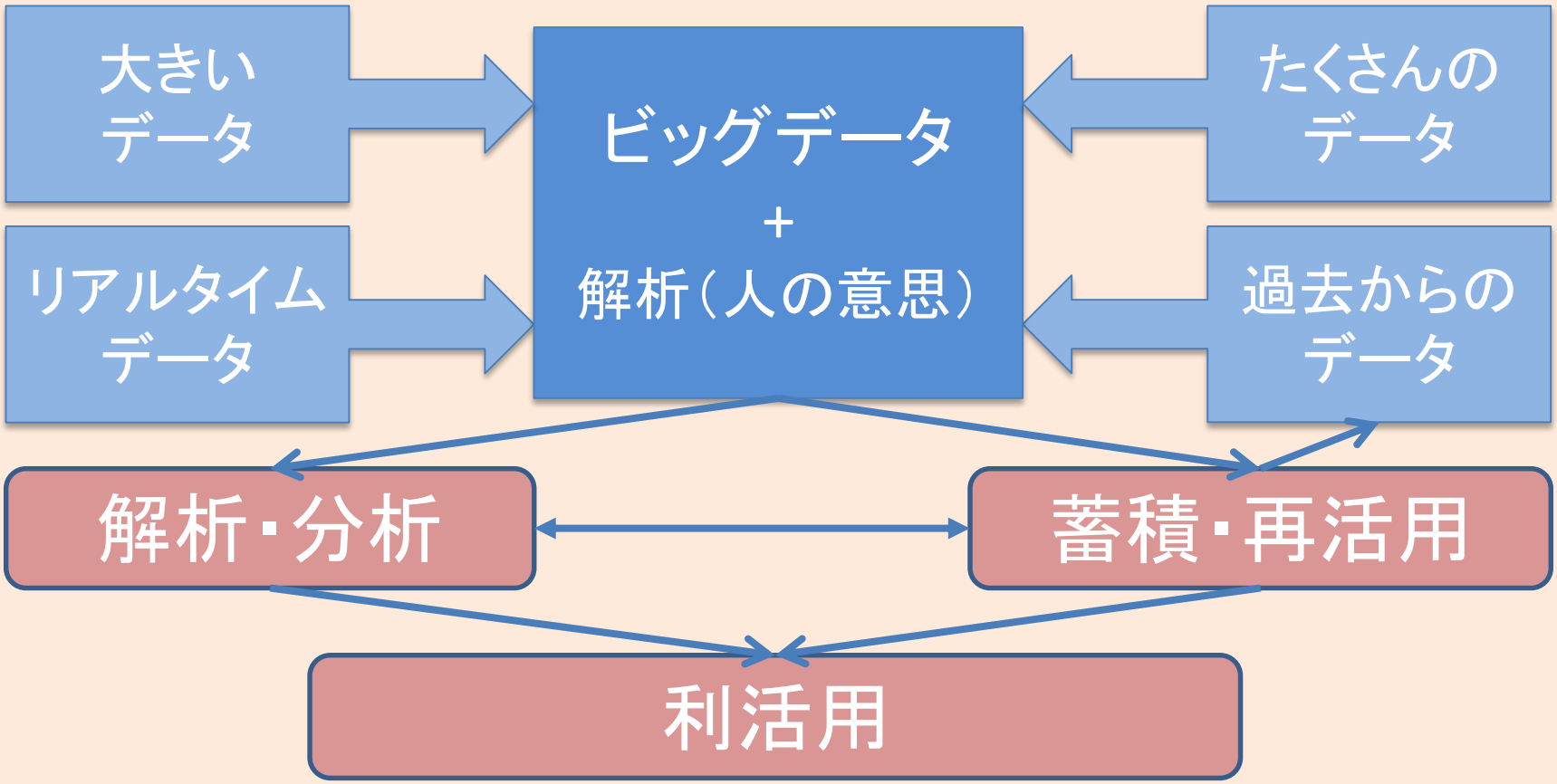
Epilogue

JDSF 新春セミナー
2018年 1月23日

（図解）ビッグデータライフサイクルとストレージ要件

JDSF Japan Data Storage Forum

セキュアなインフラストラクチャ



（おさらい）今年度の活動テーマ

JDSF
Japan Data Storage Forum

応用技術発展
のコアベクトル

利便性向上

収益性向上

業務効率改善
生産性向上

ビッグデータ活用の為の技術

・IoT/M2Mでの活用技術
・データセキュリティ

ストレージ利用の最適化技術

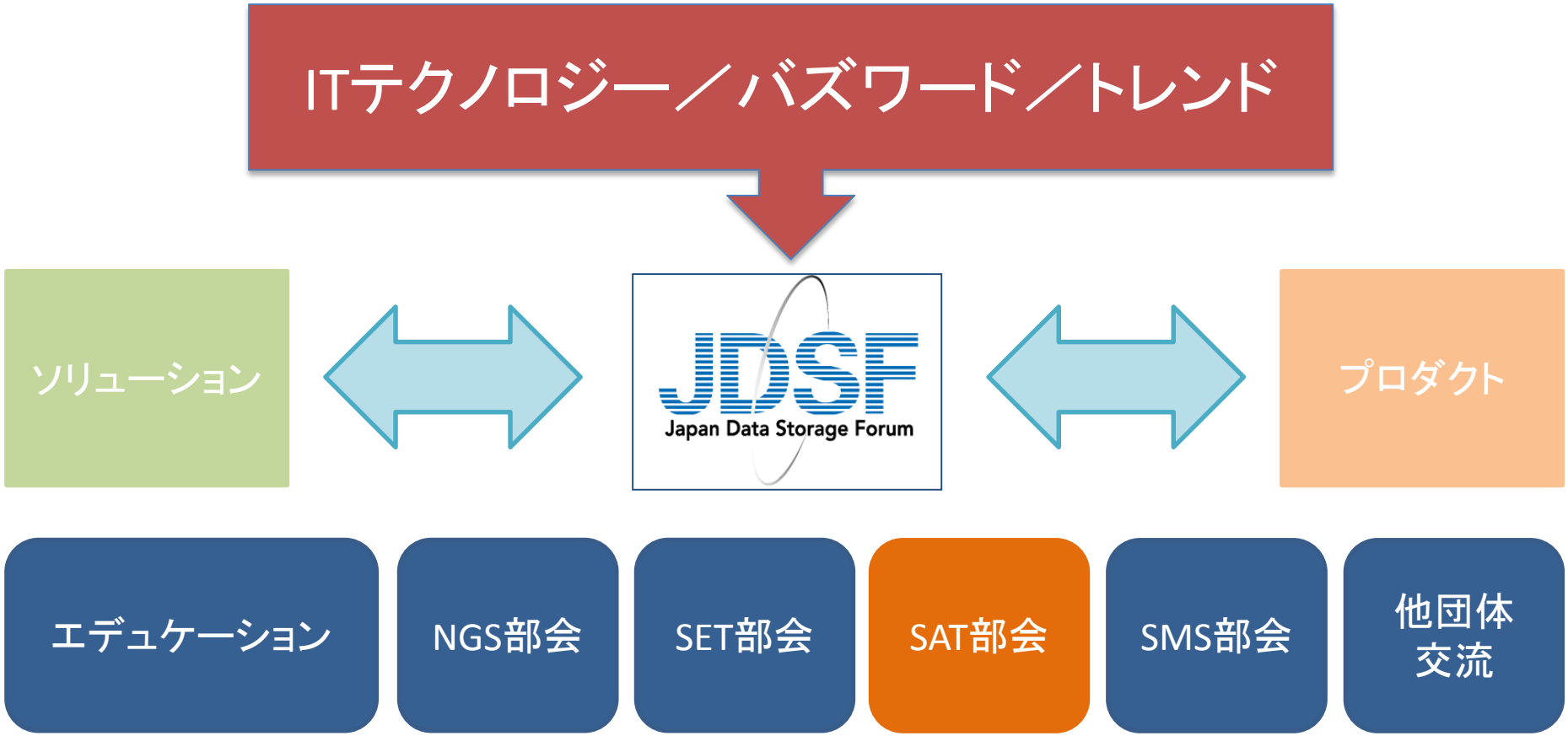
・データ管理技術

最新のインフラ環境への対応技術

・マルチクラウド環境への対応
・アーカイブのコア技術

ご参加お待ちしてます

- 市場情報や製品情報を取りまとめて一緒に発信しましょう
- ご参加されたい方は事務局へご一報ください



資料作成者

■ストレージ応用技術部会メンバー（敬称略）

- ユニアデックス　高木（部会長）
- MO　落合
- PIPELINE SECURITY　渡辺
- ソニーイメージングプロダクツアンドソリューションズ
  荒木、河村
- 日本電気　力石

ご清聴ありがとうございました。

Thank you!

JDSF 新春セミナー
2018年 1月23日