第25回 サイバー犯罪に関する白浜シンポジウム

境界はどこへ行った？
～曖昧化する境界とデータとヒトの守り方～

株式会社ラック
サイバーセキュリティサービス統括部
デジタルペンテストサービス部
兼　サイバー・グリッド・ジャパン
仲上竜太

LAC
ともに、イキル

アジェンダ

境界はどこへ行った？

～曖昧化する境界とデータとヒトの守り方～

- ニューノーマルで一変したデジタルビジネス環境
- 曖昧化した境界。境界はどこへ行った？
- これからのセキュリティモデル：ゼロトラスト

自己紹介

仲上　竜太

株式会社ラック
デジタルペンテストサービス部 部長
兼 サイバー・グリッド・ジャパン シニア・リサーチャー
情報安全確保支援士(登録番号第005254番)

IoT・情報システム・オンラインサービスなどに攻撃的手法で侵入し、リスク評価を行うデジタルペネトレーションテストサービスを運営。
進化し続けるデジタルテクノロジーについて、「作る面」「使う面」からの安全な利活用方法を研究しています。
研究分野：ブロックチェーン・xR・ゼロトラストセキュリティ

所属団体：
・日本スマートフォンセキュリティ協会 技術部会　部会長
・日本エンジニアリング協会 情報システム部会委員
・日本トラストサービス推進フォーラム
・日本バーチャルリアリティ学会

連載：
@IT「働き方改革時代のゼロトラストセキュリティ」
日経クロステックActive「予測不能時代のセキュリティキーワード」

アジェンダ

境界はどこへ行った？

～曖昧化する境界とデータとヒトの守り方～

- ニューノーマルで一変したデジタルビジネス環境
- 曖昧化した境界。境界はどこへ行った？
- これからのセキュリティモデル：ゼロトラスト

ニューノーマルで一変したデジタルビジネス環境

そもそもニューノーマルとは？

**社会に大きな影響を与える出来事が、
社会全体の変化をおこし、
新しい常識や常態が生まれること**

これまでに…

- **2000年代初頭：インターネットの普及**
  - ネットという新たな社会基盤が普及。生活や仕事の仕方が大きく変化。
- **2008年ごろ：企業的責任の追及、新たな価値観**
  - リーマン・ショック後の金融資本主義への批判と反省。CSR・SDGsなど企業活動の社会的責任が問われるように。

LAC
ともに、イキル

3度目の「ニューノーマル」

出来事：世界的なCOVID-19の流行

感染拡大防止のため人同士が近づけない状況

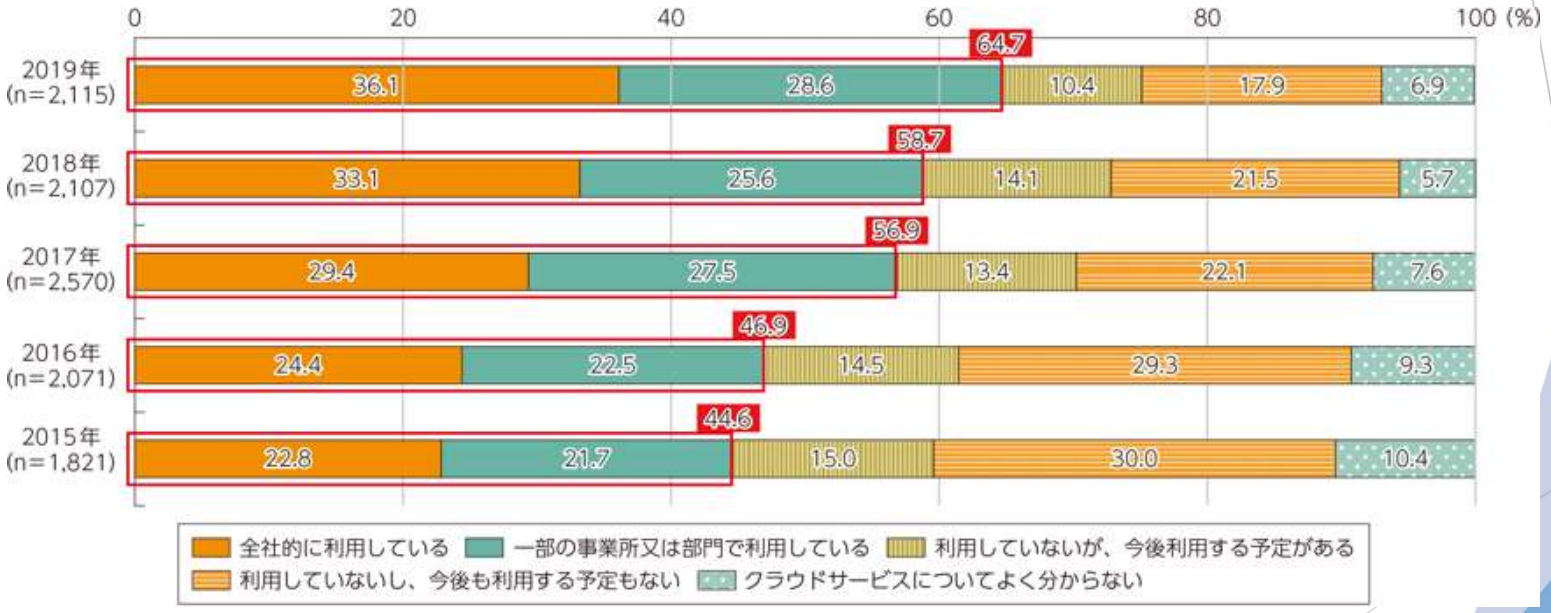
変化：生活や働き方のデジタルトランスフォーメーションが加速

オンラインミーティング、リモートワーク・テレワーク、電子マネー、電子印鑑、無人店舗、自動運転、AIによる自動化、IoT、オフィスレス、巣ごもり、ウェブ名刺、オンライン飲み会、5G…

→コミュニケーションの急激なデジタル化

クラウドサービス利用の加速

- 2019年には64.7%の企業がクラウドサービスを業務に利用

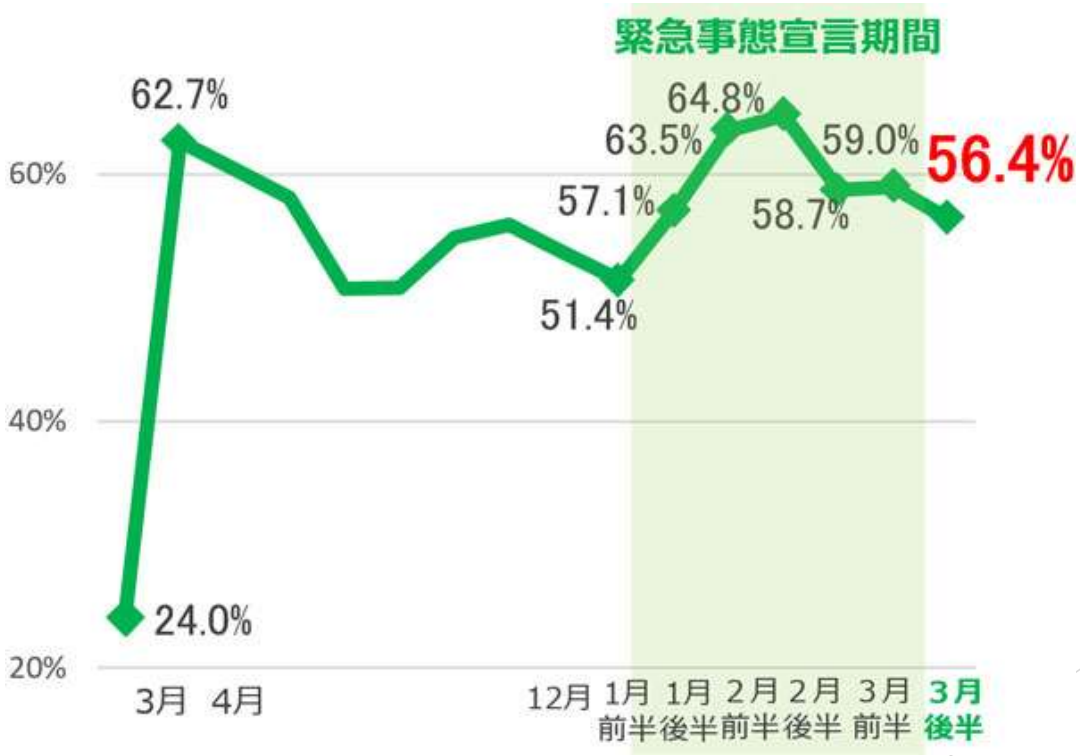


総務省「通信利用動向調査」
https://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html

LAC
ともに、イキル

テレワークの常態化

▶ コロナ禍を期にテレワークが定着

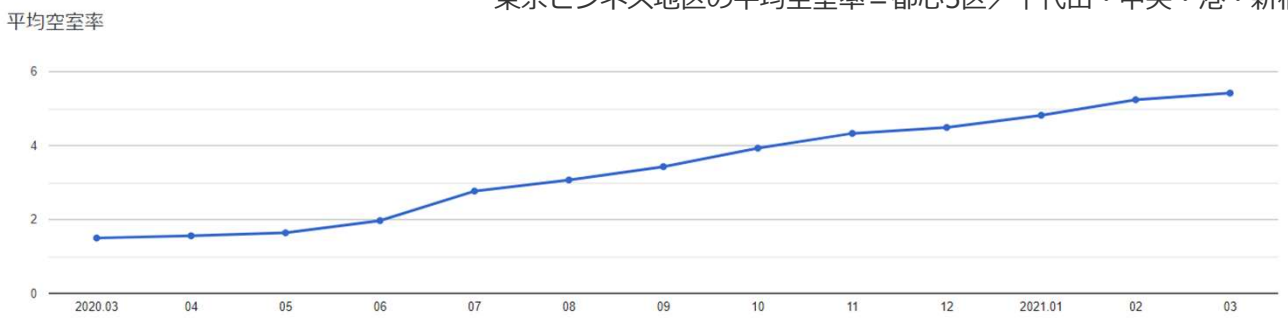


テレワーク導入率調査結果（3月後半）｜東京都
https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/04/02/11.html

LAC
ともに、イキル

ポストコロナ後のオフィス状況(東京ビジネス地区)

東京ビジネス地区の平均空室率＝都心5区／千代田・中央・港・新宿・渋谷区



東京ビジネス全体の
空室面積が1カ月間で
約2万6千坪増
※東京ドーム1.5個相当

	2020.03	04	05	06	07	08	09	10	11	12	2021.01	02	03	前月比
平均空室率	1.50	1.56	1.64	1.97	2.77	3.07	3.43	3.93	4.33	4.49	4.82	5.24	5.42	▲0.18
新築ビル	2.97	3.31	1.85	2.51	2.13	2.46	2.31	2.13	2.89	2.95	3.64	4.17	7.35	▲3.18
既存ビル	1.45	1.50	1.63	1.95	2.79	3.09	3.47	3.99	4.38	4.54	4.85	5.26	5.38	▲0.12

（単位：%）

東京都内での13か月連続で空室率上昇

出典：三鬼商事株式会社オフィスマーケットデータ 東京ビジネス地区/2021年3月
https://www.e-miki.com/market/tokyo/

LAC
ともに、イキル

ニューノーマルで一変したデジタルビジネス環境

- **働き方の多様化から在宅前提へ**
  - 緊急避難的なテレワークから、テレワーク常態化に変化
- **クラウドサービス利用の増加**
  - オンプレミスからクラウドサービスへの移行
  - クラウドリフトの推進やSaaSの活用
- **脱オフィス・オフィス縮小**
  - テレワーク常態化に伴う物理オフィスの縮小

たった1年で大きな変化が起こっている

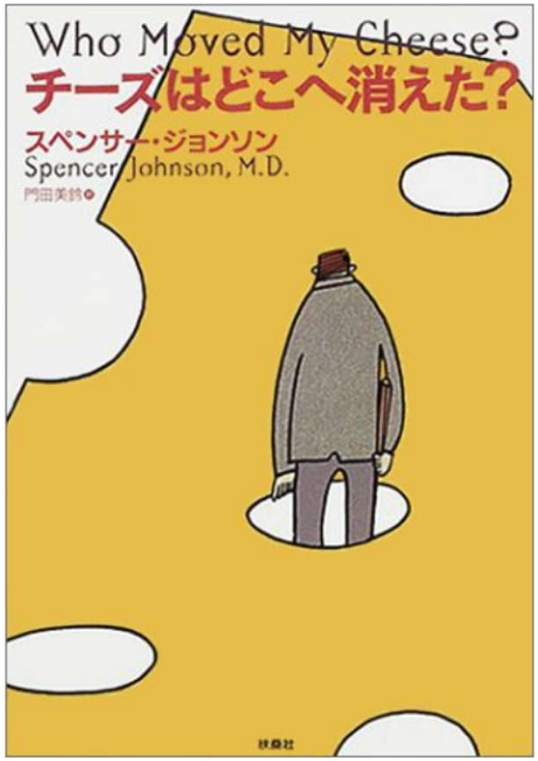
アジェンダ

境界はどこへ行った？

～曖昧化する境界とデータとヒトの守り方～

- ニューノーマルで一変したデジタルビジネス環境
- 曖昧化した境界。境界はどこへ行った？
- これからのセキュリティモデル：ゼロトラスト

チーズはどこへ消えた？

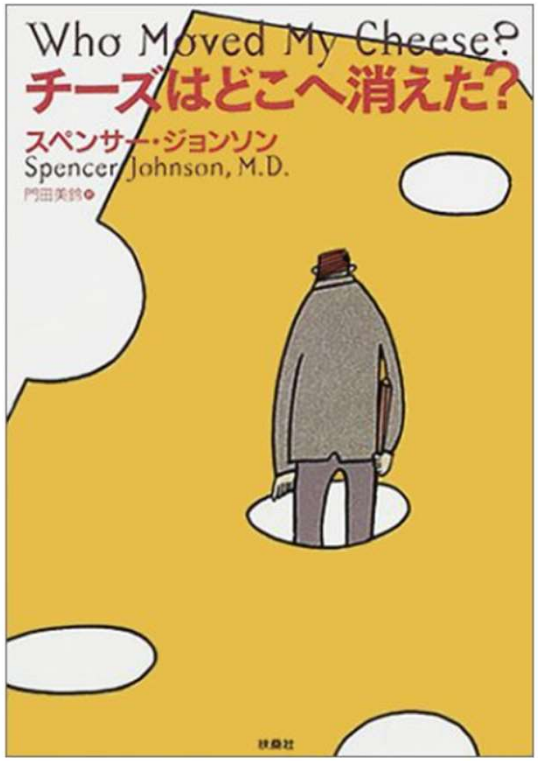


- スペンサー・ジョンソン著
- 全世界で2800万部以上
- 2000年に日本語版が発売されベストセラーに
- IBM、アップル・コンピュータ、メルセデス・ベンツ等、トップ企業が次々と社員教育に採用

チーズはどこへ消えた? 2000/11/27
スペンサー ジョンソン (著), Spencer Johnson (原著), 門田 美鈴 (翻訳)

LAC
ともに、イキル

チーズはどこへ消えた？

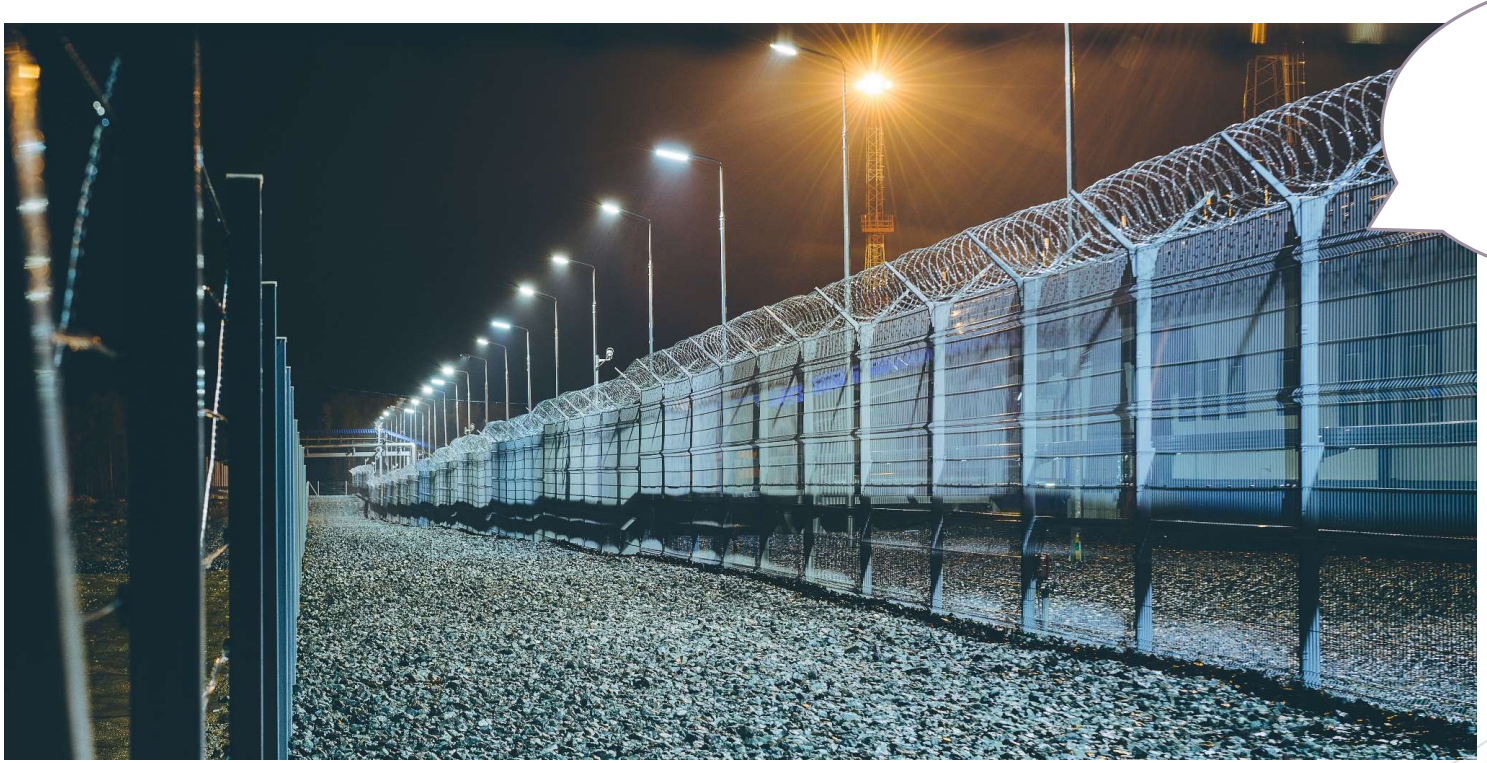


- 登場人物は２匹のネズミと２人の小人のヘムとホー
- 迷路の中でチーズを探すネズミと小人たち
- 無くなったチーズを前に小人のホーは...
- 外部環境の変化に対して、自発的な行動変容の重要さを説く一冊

チーズはどこへ消えた? 2000/11/27
スペンサー ジョンソン (著), Spencer Johnson (原著), 門田 美鈴 (翻訳)

LAC
ともに、イキル

「境界」はどこへ行った？



?

物理的な防御の方法論をネットワークに適用した
境界防御型セキュリティモデル

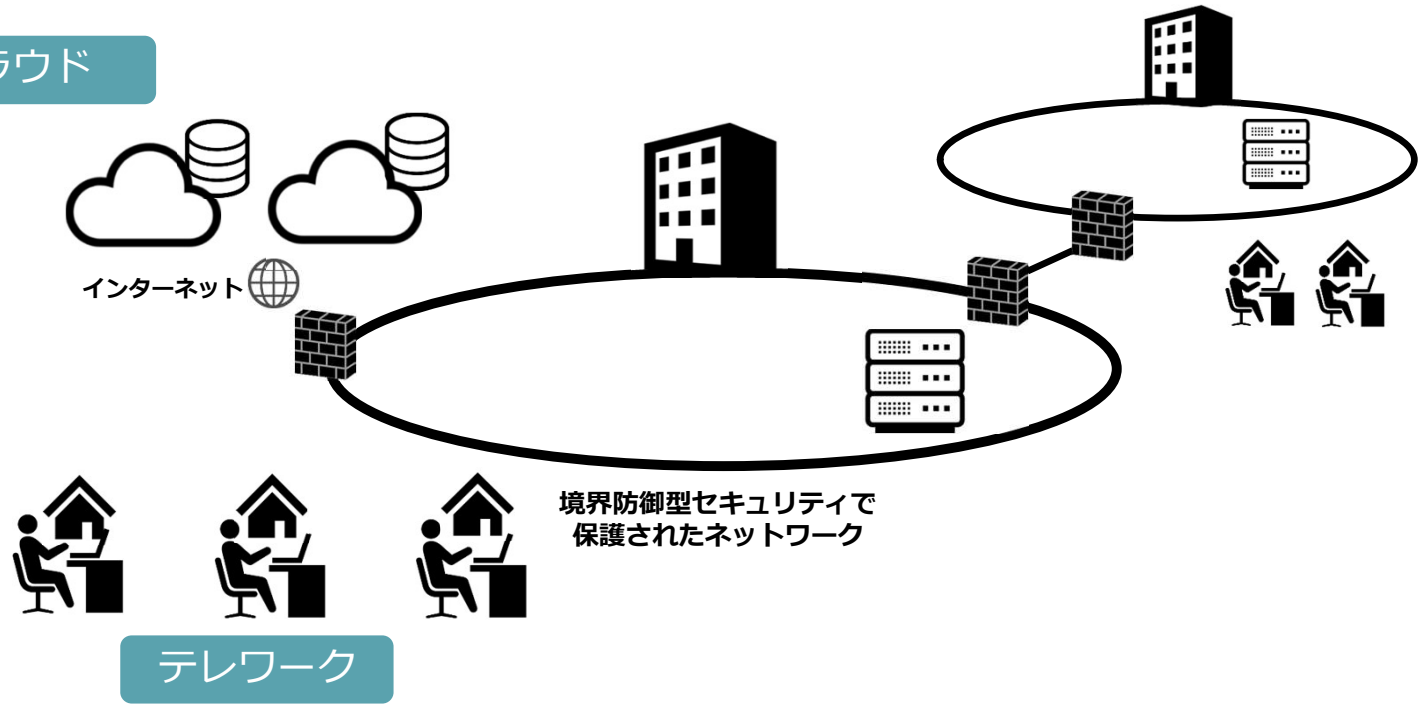
LAC
ともに、イキル

「境界」はどこへ行った？

物理的な拠点と物理的なネットワークによって保護された境界防御型セキュリティモデル

LAC
ともに、イキル

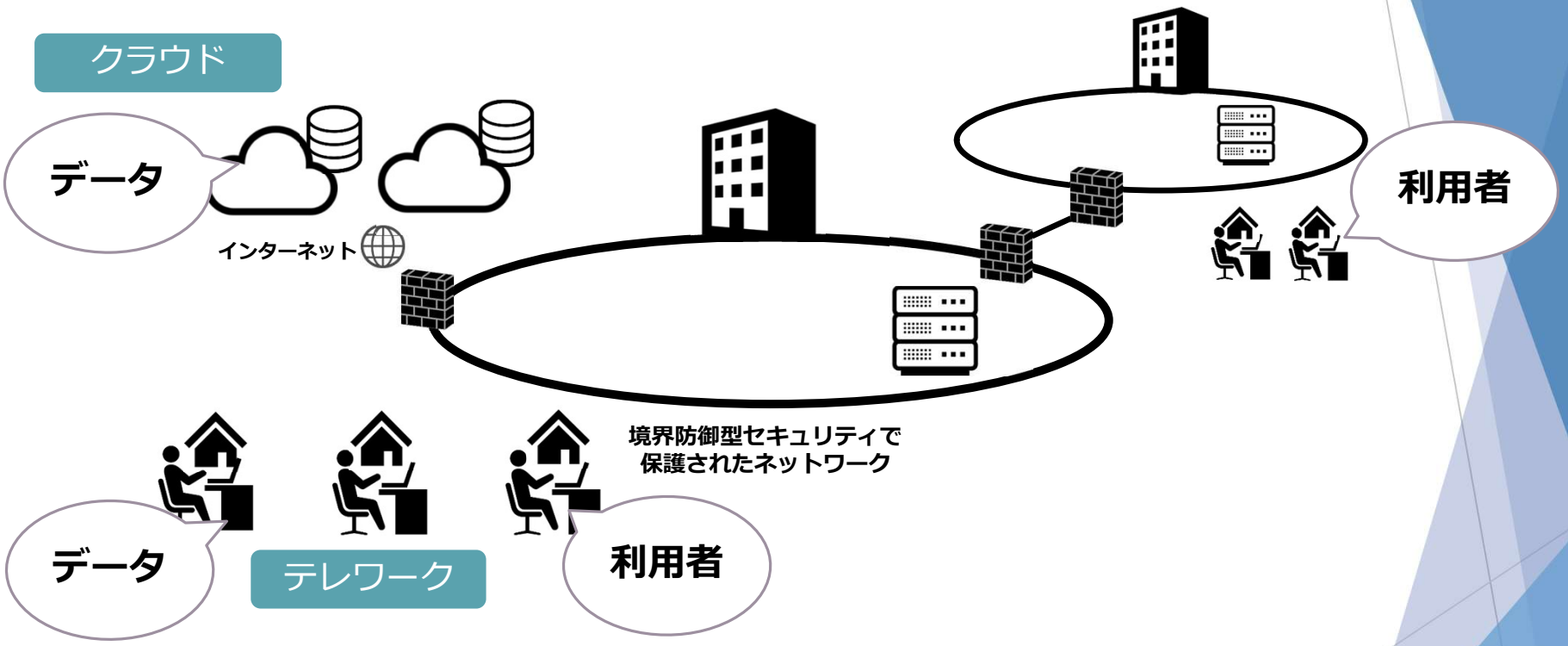
「境界」はどこへ行った？



テレワークとクラウドの利用により
オフィスの外側へ利用者やシステムが移動

LAC
ともに、イキル

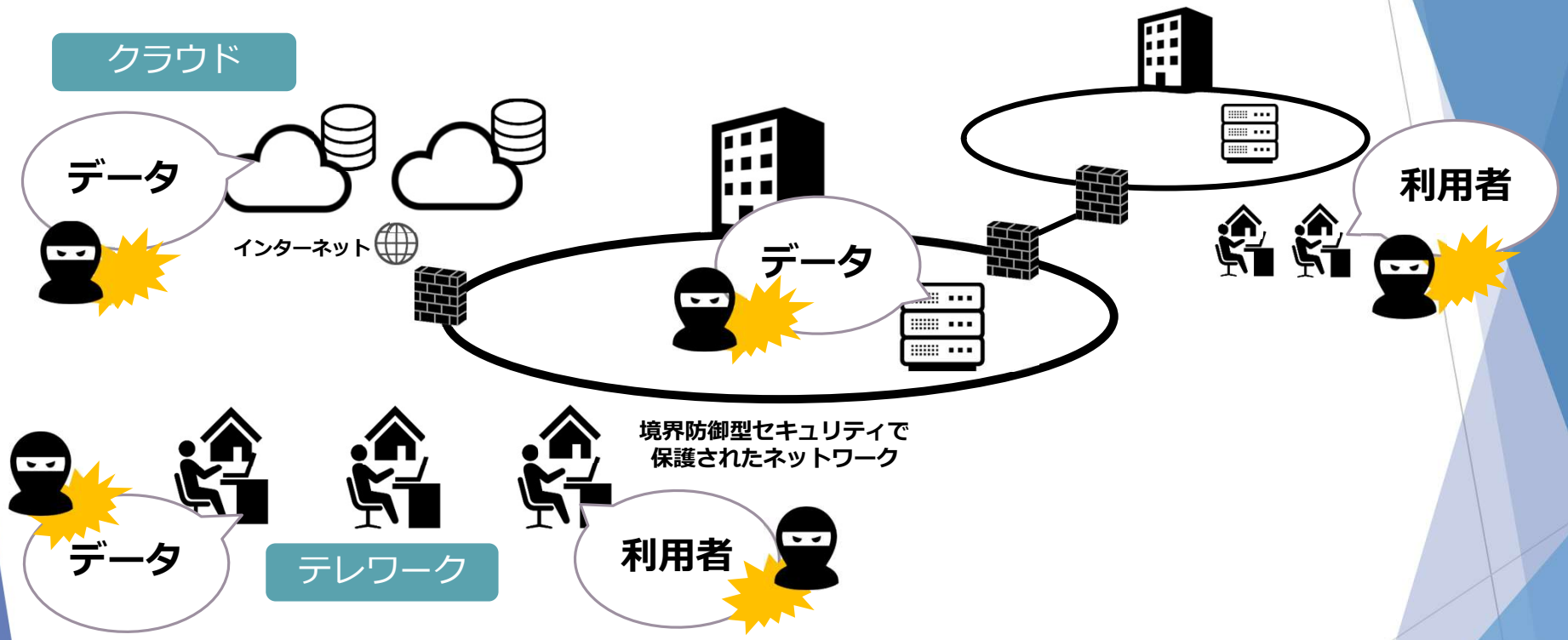
「境界」はどこへ行った？



ニューノーマルで進んだデジタルビジネス環境の変化により「ヒト」と「データ」が境界の外側へ

LAC
ともに、イキル

「境界」はどこへ行った？



アタックサーフェースの増大に伴う
サイバー攻撃機会の増加

LAC
ともに、イキル

「境界」はどこへ行った？

- **データと利用者の遍在による境界曖昧化と脅威の変化**
  - クラウドへの不正アクセス
  - クラウド設定ミスによる情報漏えい
  - 私物PCへのデータ持ち出し
  - ホームネットワークへのデータ共有
  - ネットワーク機器の脆弱性の悪用
  - ネットワーク侵害後の横展開

脆弱性の拡大　×　脅威の高度化

LAC
ともに、イキル

アジェンダ

境界はどこへ行った？

～曖昧化する境界とデータとヒトの守り方～

- ニューノーマルで一変したデジタルビジネス環境
- 曖昧化した境界。境界はどこへ行った？
- これからのセキュリティモデル：ゼロトラスト

ニューノーマルによるデジタル環境の変化

- **働く環境の変化**
  - クラウド利活用によりデータが分散
  - テレワーク常態化により利用者が分散
- **脅威の変化**
  - 新たな攻撃手法の登場
  - 企業や組織が利用するツールやサービスの悪用
  - デジタル環境の変化を悪用

多様性の実現や利便性向上とともに
サイバー攻撃の質も変化

未来：ニューノーマルで迎える2025年のデジタル環境

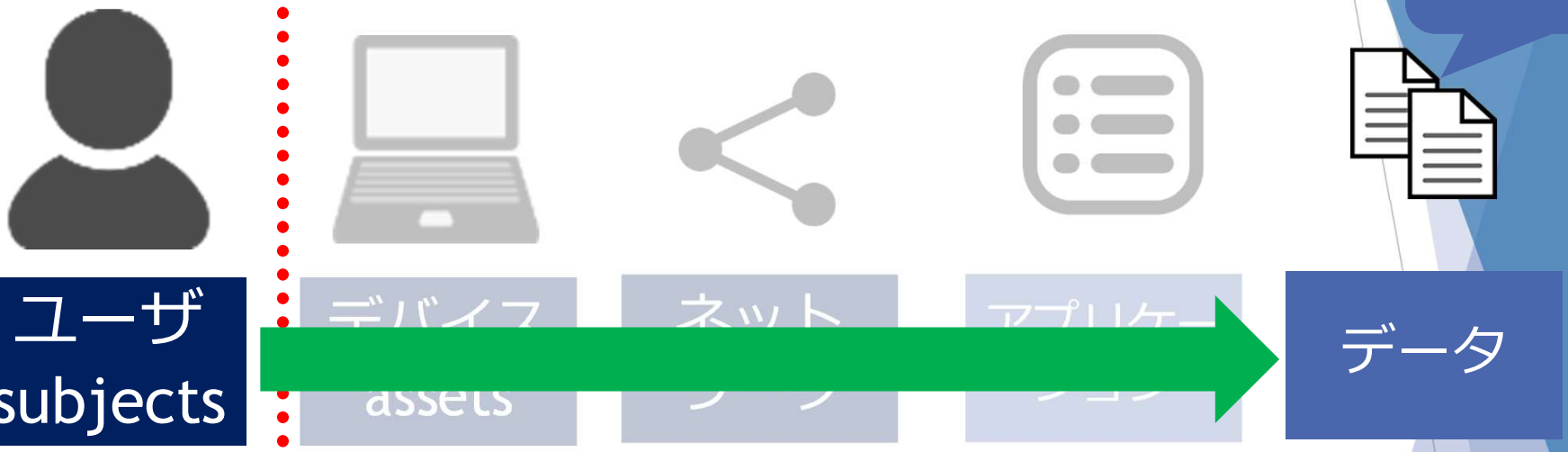
- **2025年の社会やデジタル環境**
  - 5G / IPv6などリッチなネットワークインフラの活用
  - メインフレーム志向からクラウドサービスへ
  - 場所にとらわれない働き方（自動運転で移動中も）
  - デバイスの多様化（スマホ・PC・VR・AI秘書）
  - 通信環境の多様化（ケータイキャリア・光通信）
- **データと利用者が点在し、従来の「境界」で守る考え方が通用しない状況**

デジタル環境変化に対応した
セキュリティコンセプトが必要

LAC
ともに、イキル

セキュリティの基本原則(CIA)

守るべきものは
データ



データにアクセスする権限を
もった「本人」のみが、
アクセスを許されること

機密性（confidentiality）
完全性（integrity）
可用性（availability）

LAC
ともに、イキル

ゼロトラストの基本

- 従来の境界防御型セキュリティモデル

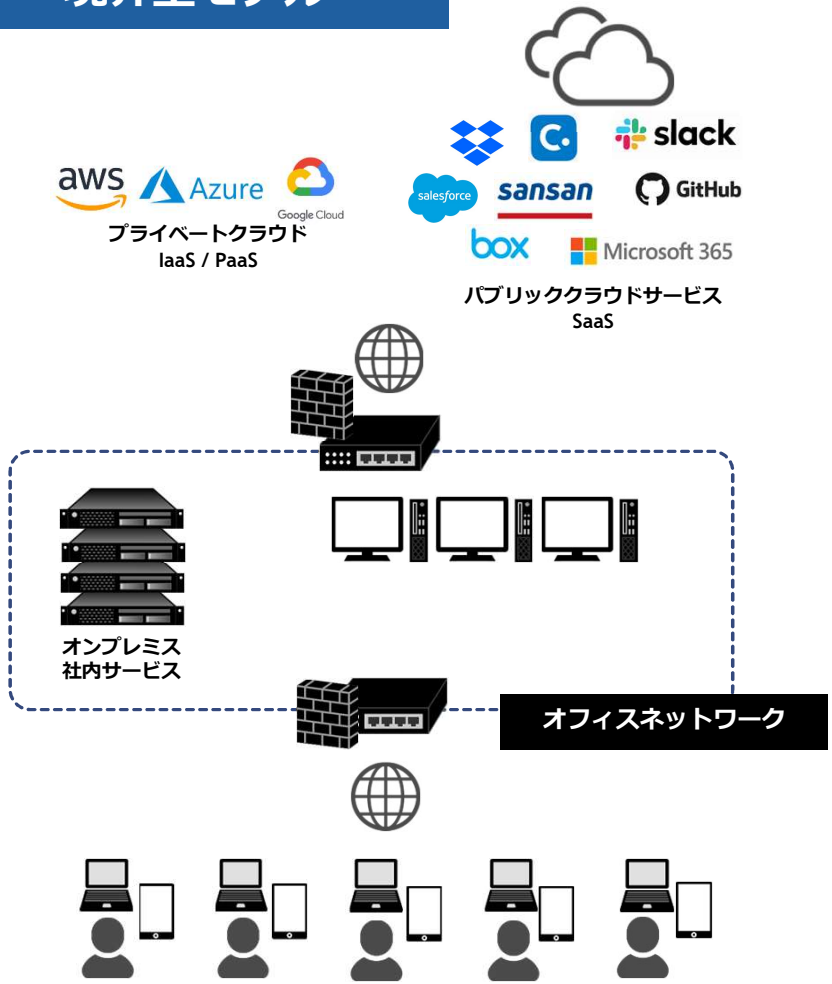
  ゾーンによる
  静的なアクセスコントロール
  「過去の認証を信用」

- ゼロトラストモデル

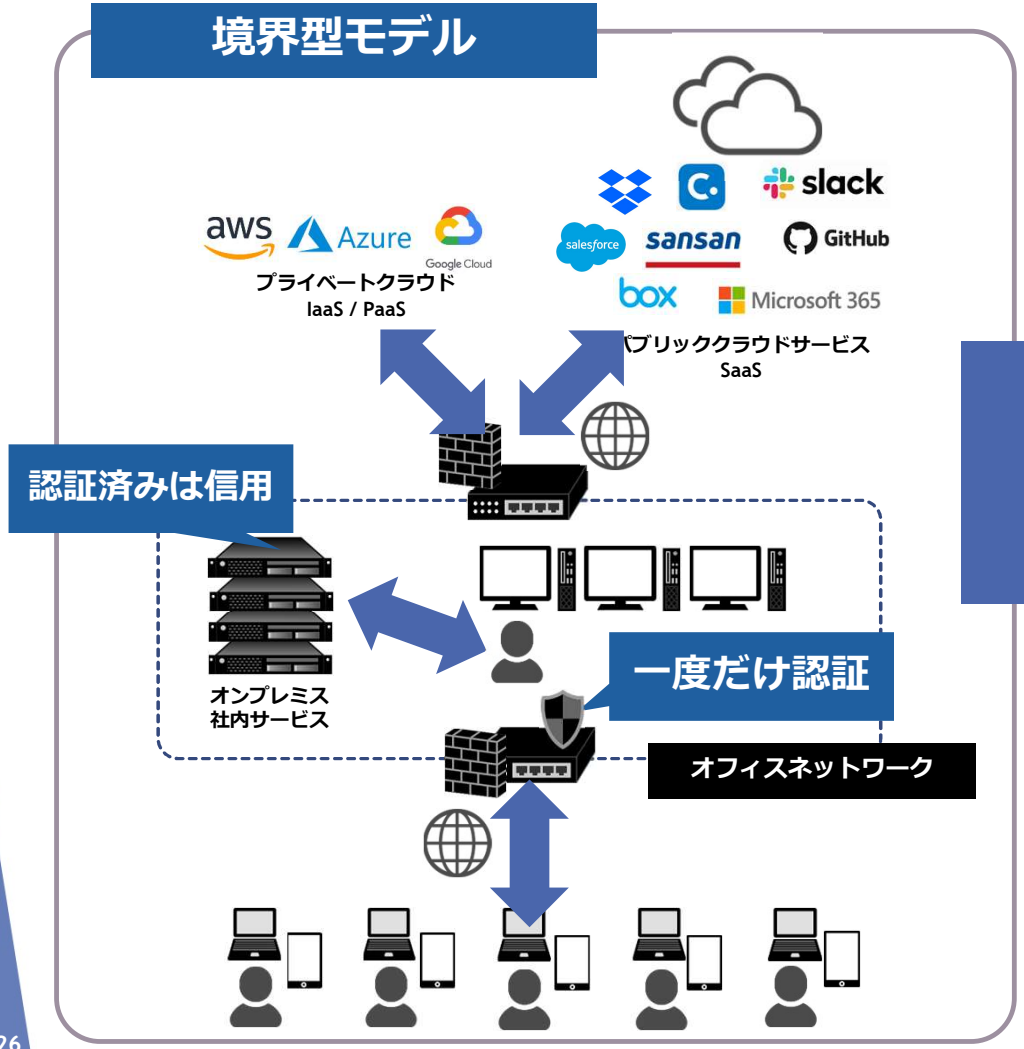
  ユーザ認証・デバイス認証・信頼度から
  動的なアクセスコントロール
  「過去の認証を信用しない」

LAC
ともに、イキル

境界型モデル



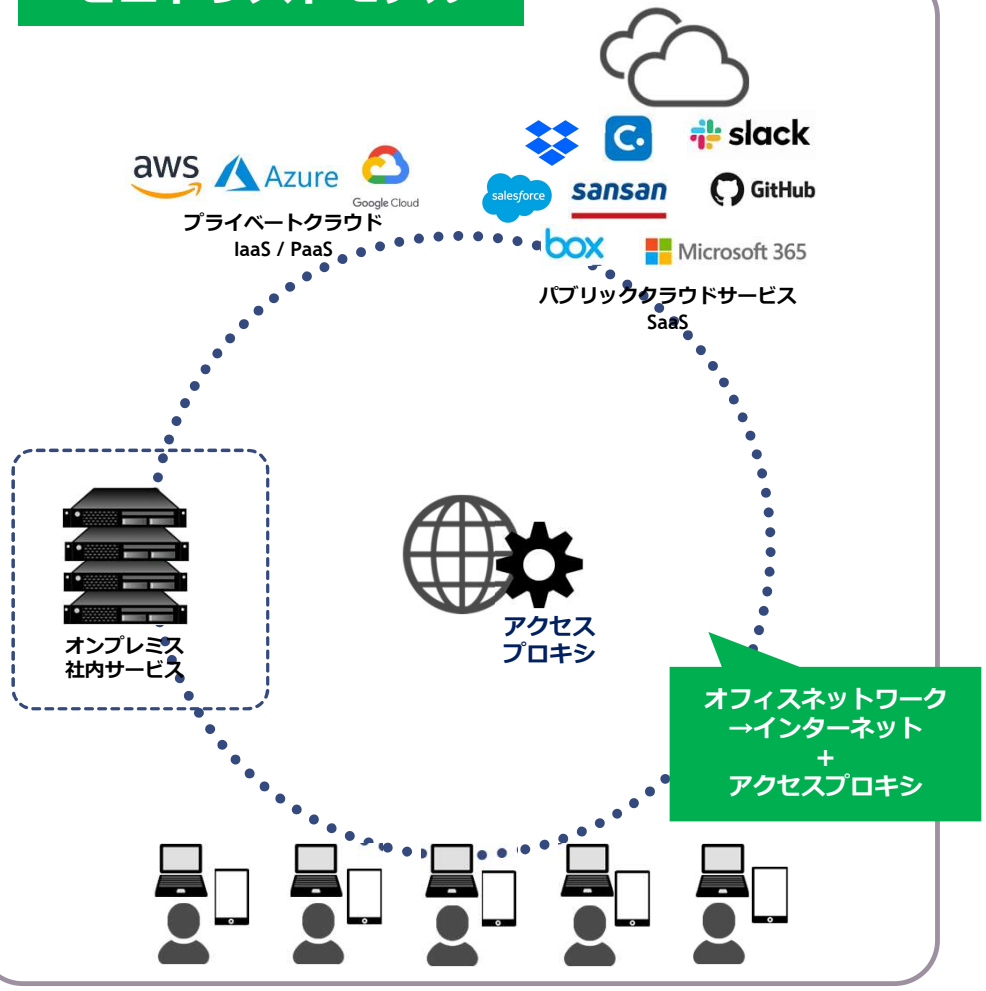
LAC
ともに、イキル



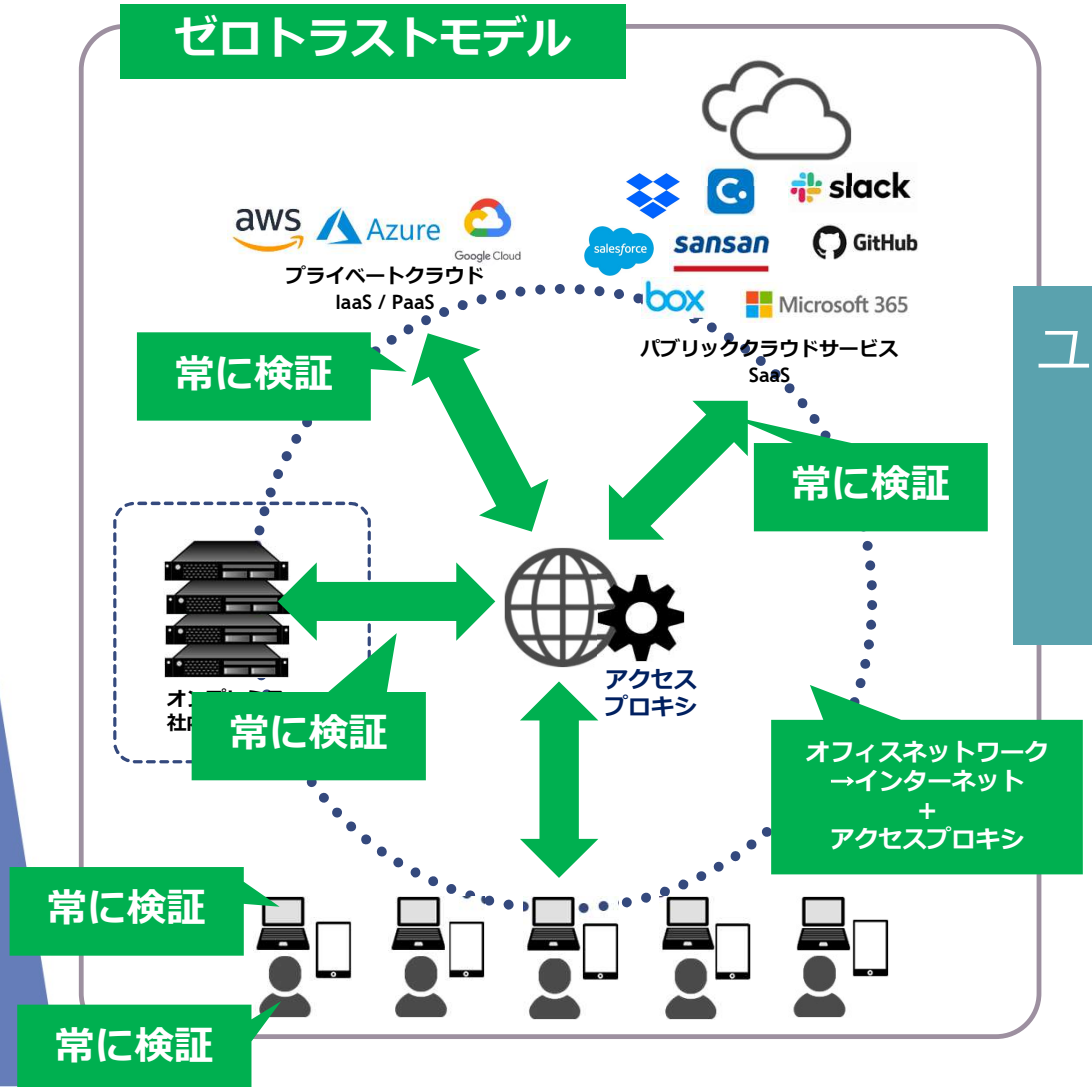
ゾーンによる
静的なアクセスコントロール
「過去の認証を信用」

LAC
ともに、イキル

ゼロトラストモデル



LAC
ともに、イキル



ユーザ認証・デバイス認証・信頼度から
動的なアクセスコントロール
「過去の認証を信用しない」
＝常に検証

LAC
ともに、イキル

ゼロトラストのコンセプト

Always Verify, Never Trust.
信頼せず、常に検証。

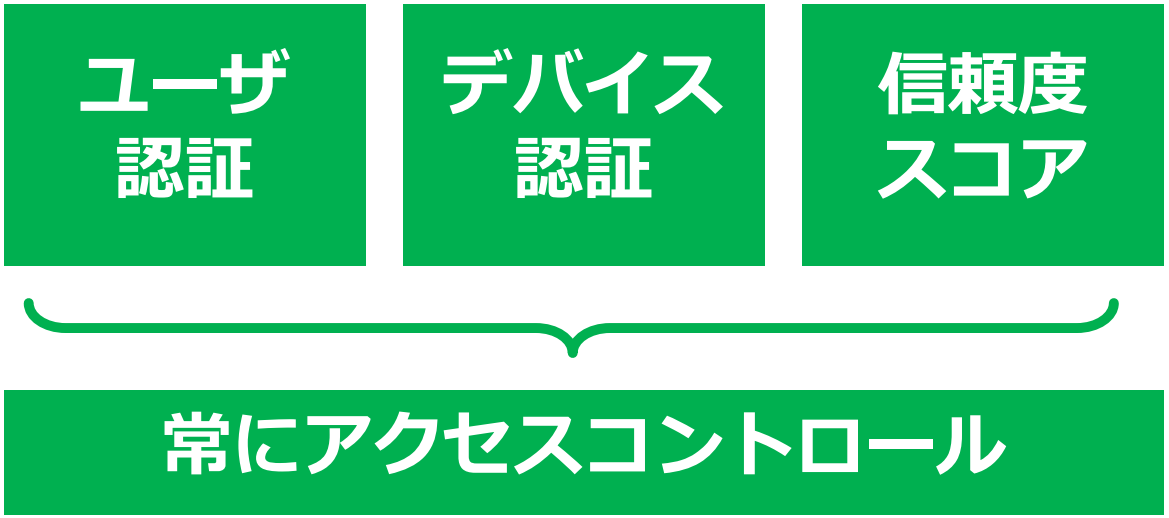
ゼロトラストは、何を信用しないのか？

- **実環境における現実的な課題**
  - ネットワークは常に敵意に晒されている
  - 常に外部と内部の脅威が存在する
  - 「ローカル」「プライベート」＝安全ではない
  - 過去に適用されたポリシーは信頼できない
  - 不正を行う正規アカウント利用者が存在する

Always Verify , Never Trust.

ゼロトラストは、何を信用するのか

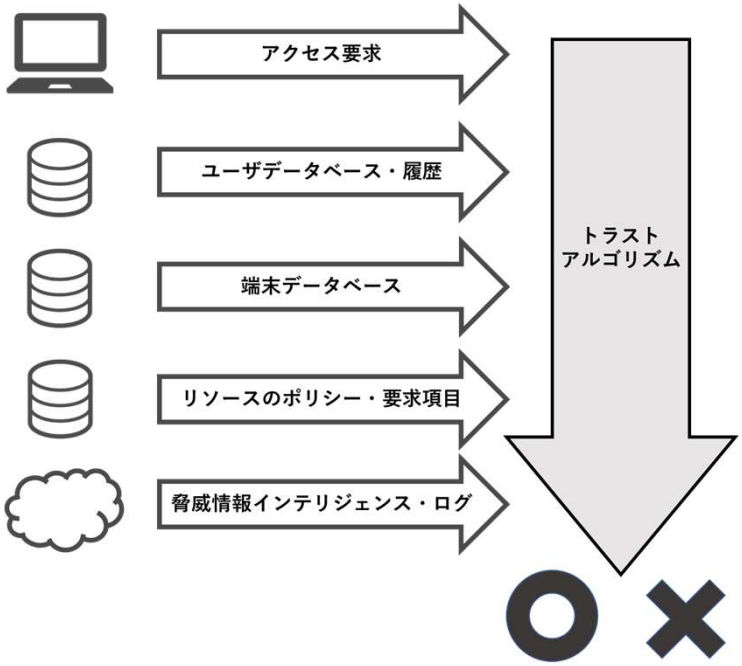
- **ゼロトラストモデルの信用の源泉**
  - 守るべき重要な資産＝「データ」
  - データへのアクセス認可をリアルタイム
    かつ動的にチェックし、適用する



LAC
ともに、イキル

ゼロトラストは、何を信用するのか

▶ トラストアルゴリズムによる信頼度の計算



- ✓ 登録された端末かどうか
- ✓ OSやアプリケーション、アンチウィルスソフトのパターンが最新かどうか
- ✓ 端末が感染していないか
- ✓ 時刻の設定が正しいか
- ✓ アクセス元は適切か
- ✓ 許可されていないアプリは導入されていないかなどなど

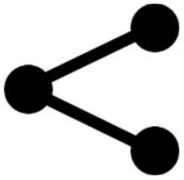
Always Verify, Never Trust.

LAC
ともに、イキル

ゼロトラストの構成要素

ユーザ
subjects

デバイス
assets



ネット
ワーク

アプリケー
ション

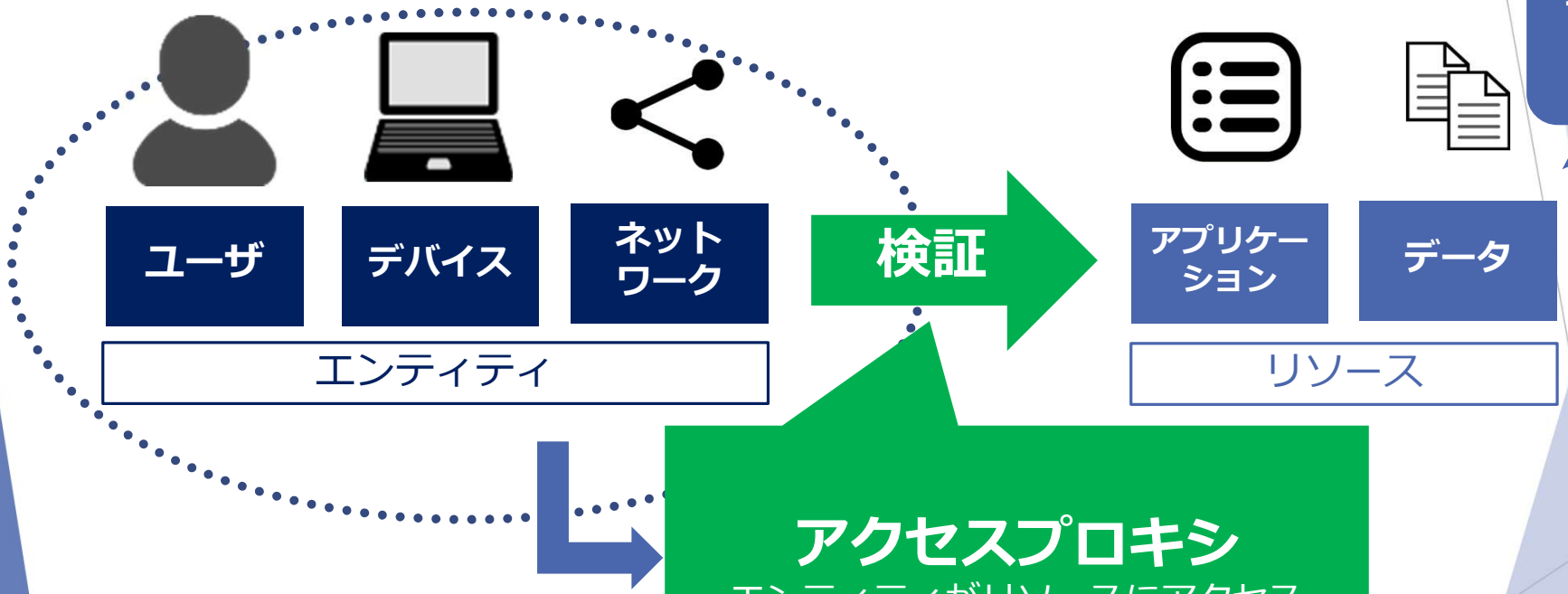
データ

エンティティ

リソース

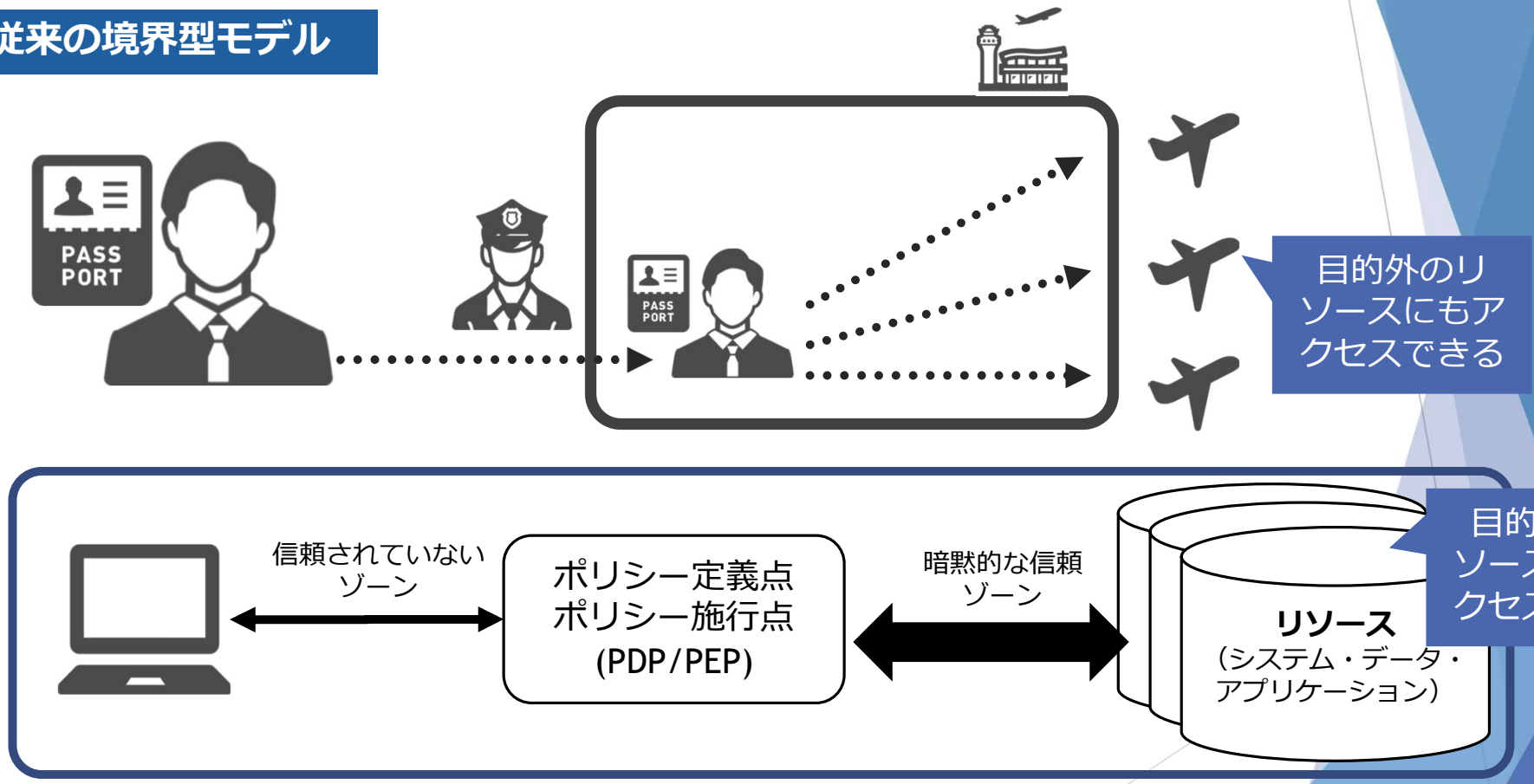
LAC
ともに、イキル

ゼロトラストの構成要素



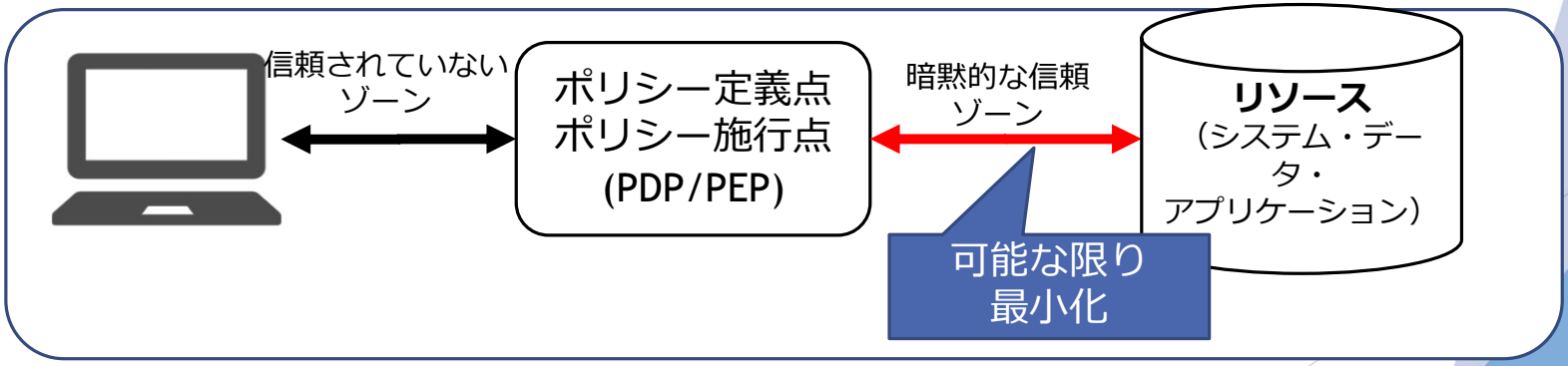
空港セキュリティと情報セキュリティ（SP800-207)

従来の境界型モデル



空港セキュリティと情報セキュリティ（SP800-207)

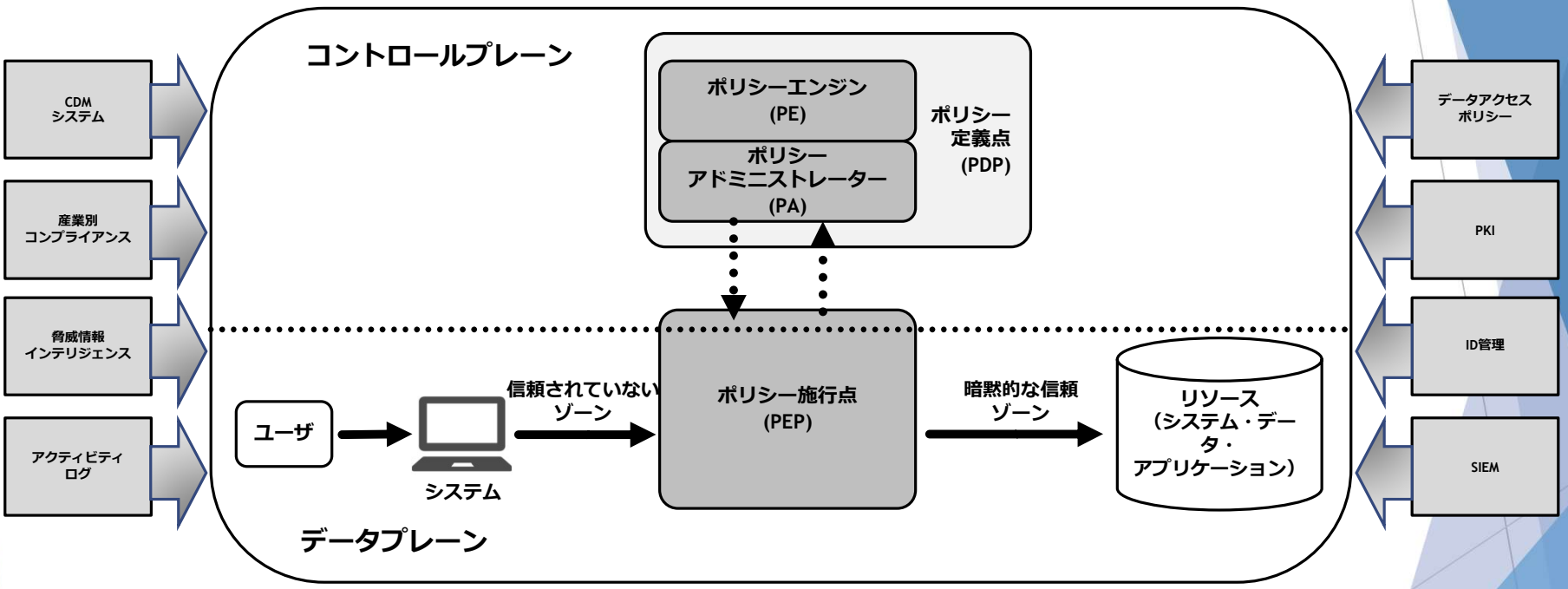
ゼロトラストモデル



マイクロセグメンテーション

LAC
ともに、イキル

ゼロトラストの論理モデル（SP800-207）



ユーザがリソースにアクセスする際に
ポリシーに従って情報を取得し検証を行う

LAC
ともに、イキル

ゼロトラストとは

暗黙のゾーンを信用しない

常に最新のポリシーで信頼度を検証する

全てのリソースへのアクセスを検証する

データやリソースへアクセスする際のポリシー適用の徹底により、「内・外」「VPN」といったネットワークセグメントへの依存をなくすことで、より多様な働き方に対応し、セキュリティを保って生産性の最大化(可用性の最大化）が目的。

ゼロトラストで目指す次世代SOC

- **境界が曖昧化した「ゼロトラスト時代」のSOC構築と運用**
- 日本マイクロソフトとラックが共同作成
- ゼロトラストの基本的な特徴とともに、ポリシーベースのアクセス制御、ユーザやデバイス別のリスク検証といった具体策、それを実現するEDRやID管理システムなどについて、詳しく解説
- SOCの機能や構築、設計と運用、「次世代SOC」という展望についても触れています

アジェンダ

境界はどこへ行った？

～曖昧化する境界とデータとヒトの守り方～

- ニューノーマルで一変したデジタルビジネス環境
- 曖昧化した境界。境界はどこへ行った？
- これからのセキュリティモデル：ゼロトラスト

Thank you. Any Questions ?

株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー
sales@lac.co.jp
www.lac.co.jp