NTT DATA
Trusted Global Innovator

開発者の在宅勤務率を90%にするだけで終わらせない
「ゼロトラスト」セキュリティ実現へのステップ

2021年1月
NTTデータ 先端技術株式会社
チーフコンサルタント　佐藤 雄一

本日お伝えしたいこと

1．ゼロトラストとはなにか
2．ゼロトラスト実現への進め方
3．実施事例（ゼロトラストの最初の一歩）

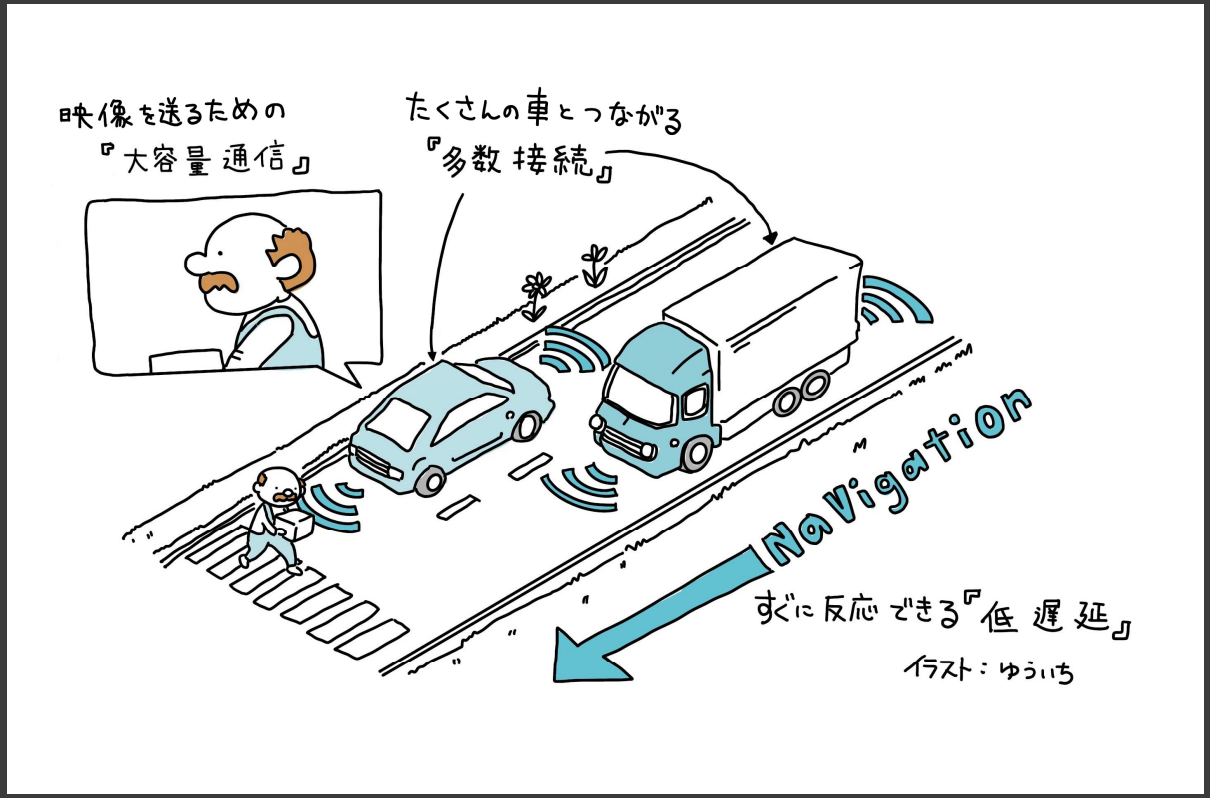
NTTデータグループ で 唯一の
ITインフラとセキュリティを専門とした技術者の集団です。

NTT DATA

NTTデータ 先端技術株式会社

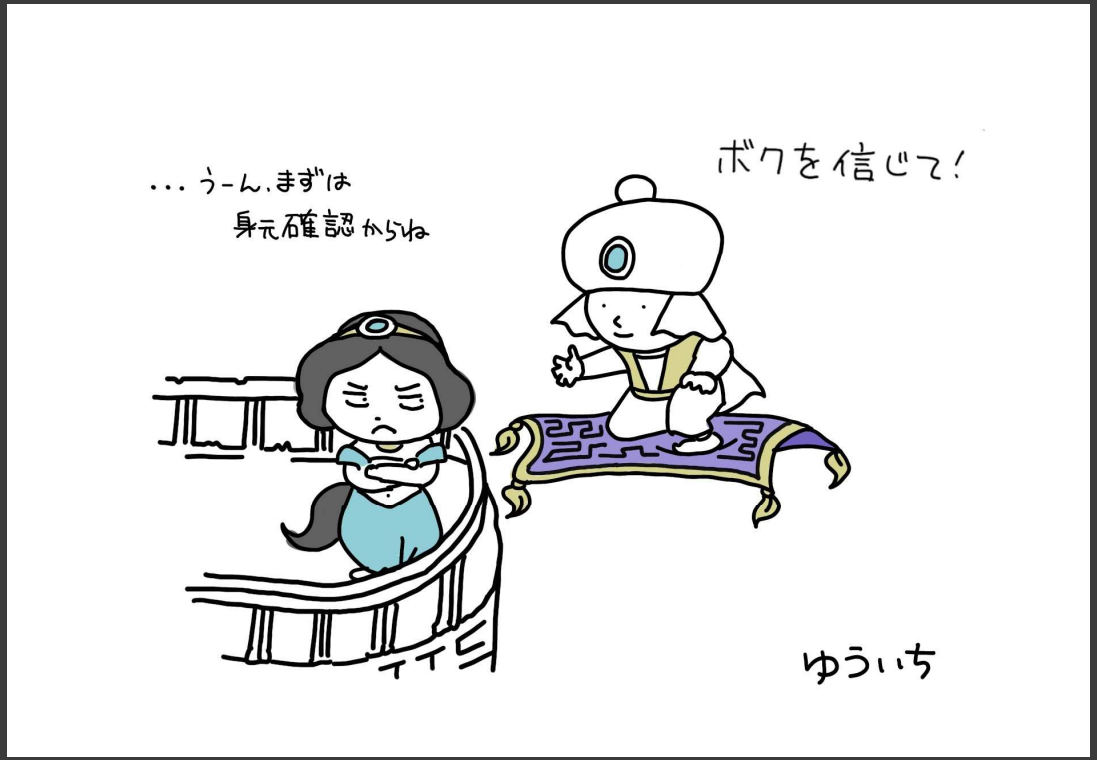
佐藤雄一（セキュリティコンサルタント　CISSP, Ph.D., IPA　情報処理試験作成委員）

IoTを飛躍させる「ローカル5G」の
セキュリティを考える
【Tech Republic】



NTT DATA

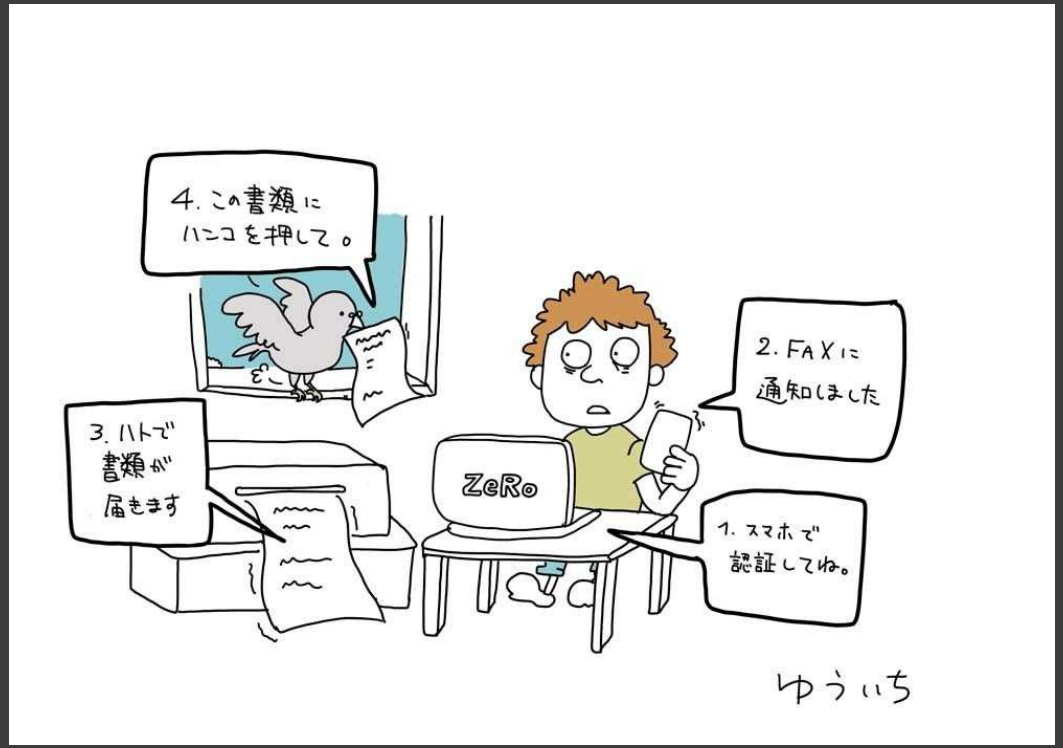
佐藤雄一（セキュリティコンサルタント　CISSP, Ph.D., IPA　情報処理試験作成委員）



3分でわかるゼロトラスト
【現代ビジネス】

NTT DATA

佐藤雄一（セキュリティコンサルタント　CISSP, Ph.D., IPA　情報処理試験作成委員）



なぜ、いまゼロトラストなのか
【マイナビニュース】

NTT DATA

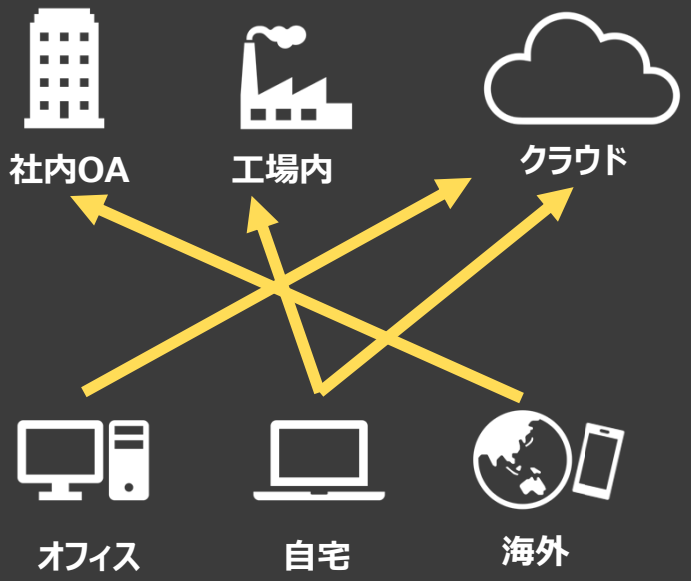
１．ゼロトラストとはなにか

２．ゼロトラスト実現への進め方

３．実施事例（ゼロトラストの最初の一歩）

背景：新型コロナウイルス対策として、テレワークが浸透

テレワークにおけるセキュリティ対策が課題



取引先がテレワークを
実施している場合、不安がある

51.0%

IPA アンケート結果(中間報告) 2020年12月

社内に情報資産があるという前提が崩れている

境界防御モデルでは限界が来ている

これまでの環境

機密データは社内

社内にPCがある

社内から社内にアクセス

境界防御モデルにより保護

テレワーク環境

機密データがクラウド上にも

社外に端末がある

社外から社内にアクセス

境界防御モデルだけでは、保護できない

NTT DATA

ゼロトラストとは

「決して信用せず（ゼロトラスト）、常に検証する」

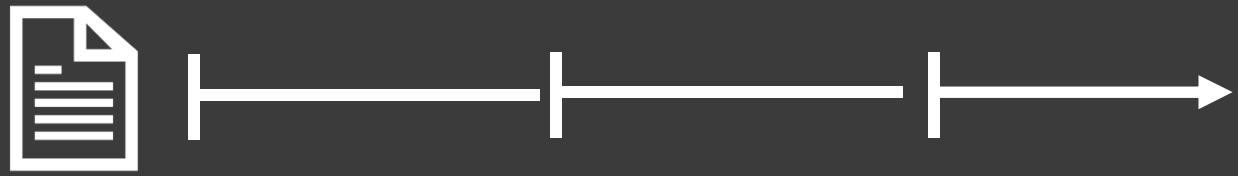
情報資産

全てのユーザ/デバイス

必ず検証

外部から接続できることを前提としたセキュリティの考え方

ゼロトラストのコンセプト

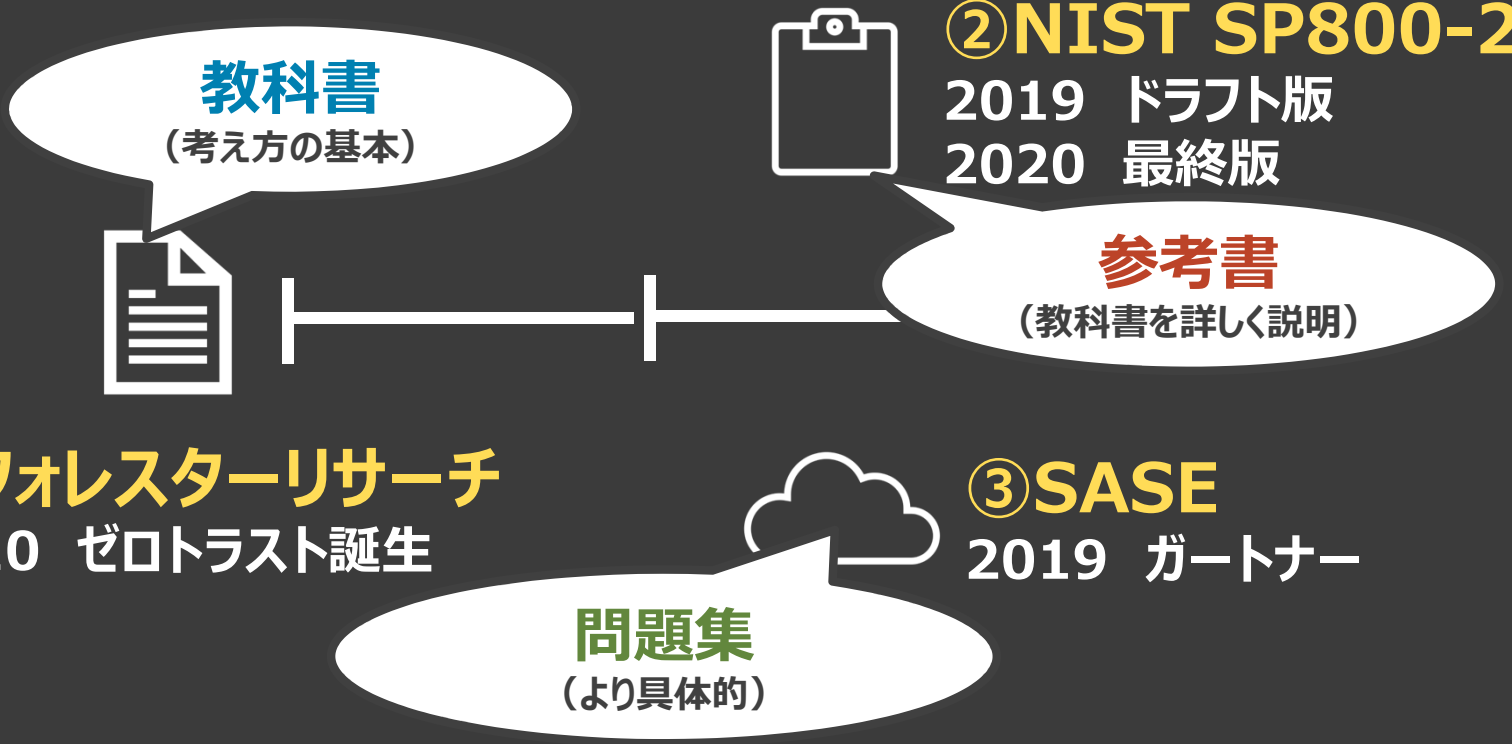


①フォレスターリサーチ
2010　ゼロトラスト誕生

②NIST SP800-207
2019　ドラフト版
2020　最終版

③SASE
2019　ガートナー

ゼロトラストのコンセプト



NTT DATA

教科書：ジョン・キンダーバーグ によるゼロトラストの概念

内部だから信頼できる、外部だから信頼できないといった、境界防御モデルはもはや通用しない

①フォレスターリサーチ

2010　ゼロトラスト誕生

内部	外部
信頼する	信頼しない

内部	外部
信頼しない	信頼しない

②NIST SP800-207

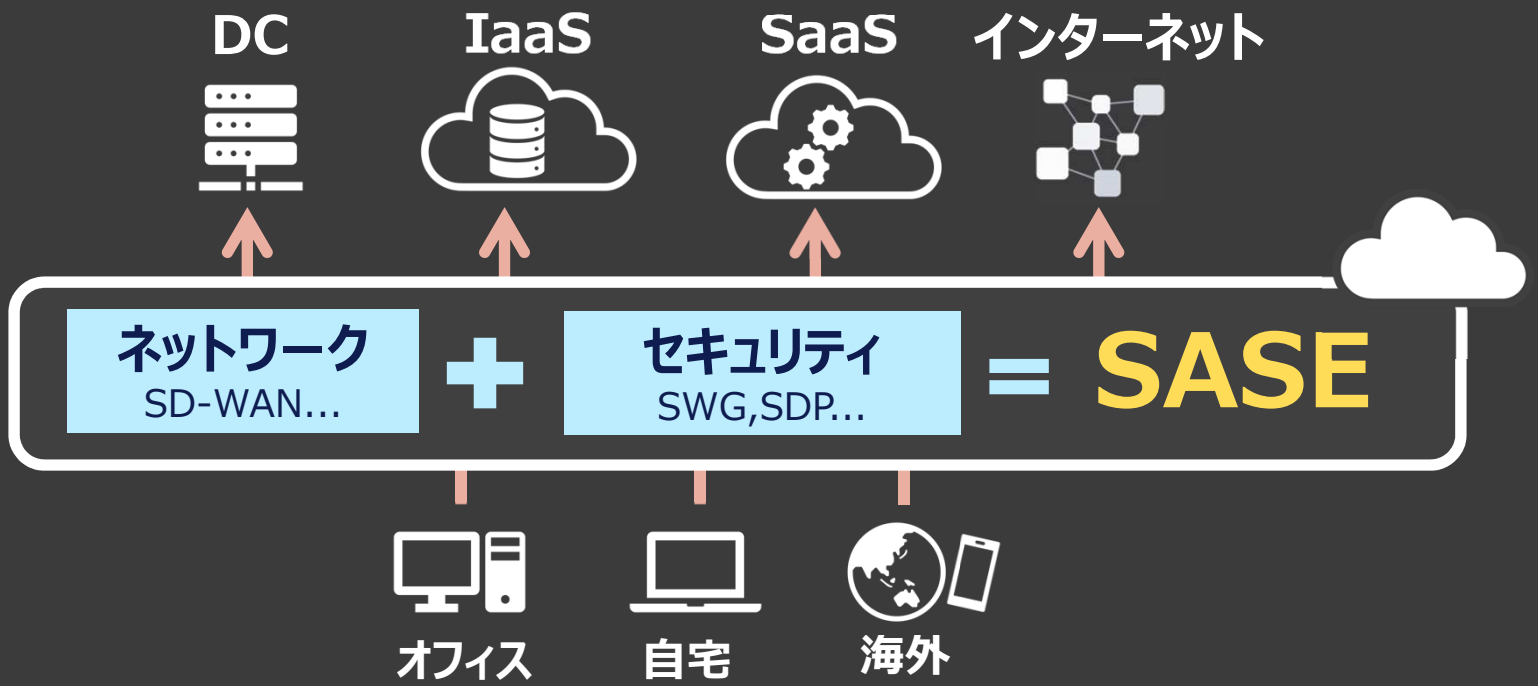
アクセスがあるたび、必ず検証し、そのためのログを集める

7つの原則	
	リソースへのアクセスは、動的ポリシーにより決定
全てのデータソースとコンピューティングサービスをリソースとする	
	全ての資産の整合性とセキュリティ動作を監視し、測定
ネットワークの場所に関わらず、すべての通信を保護	
	認証と認可を動的に行い、アクセスが許可される前に実施
リソースへのアクセスはセッション単位で付与	
	多くの情報を収集し、セキュリティの改善に利用

問題集：ゼロトラストを実現するための具体的な技術要素のまとめ

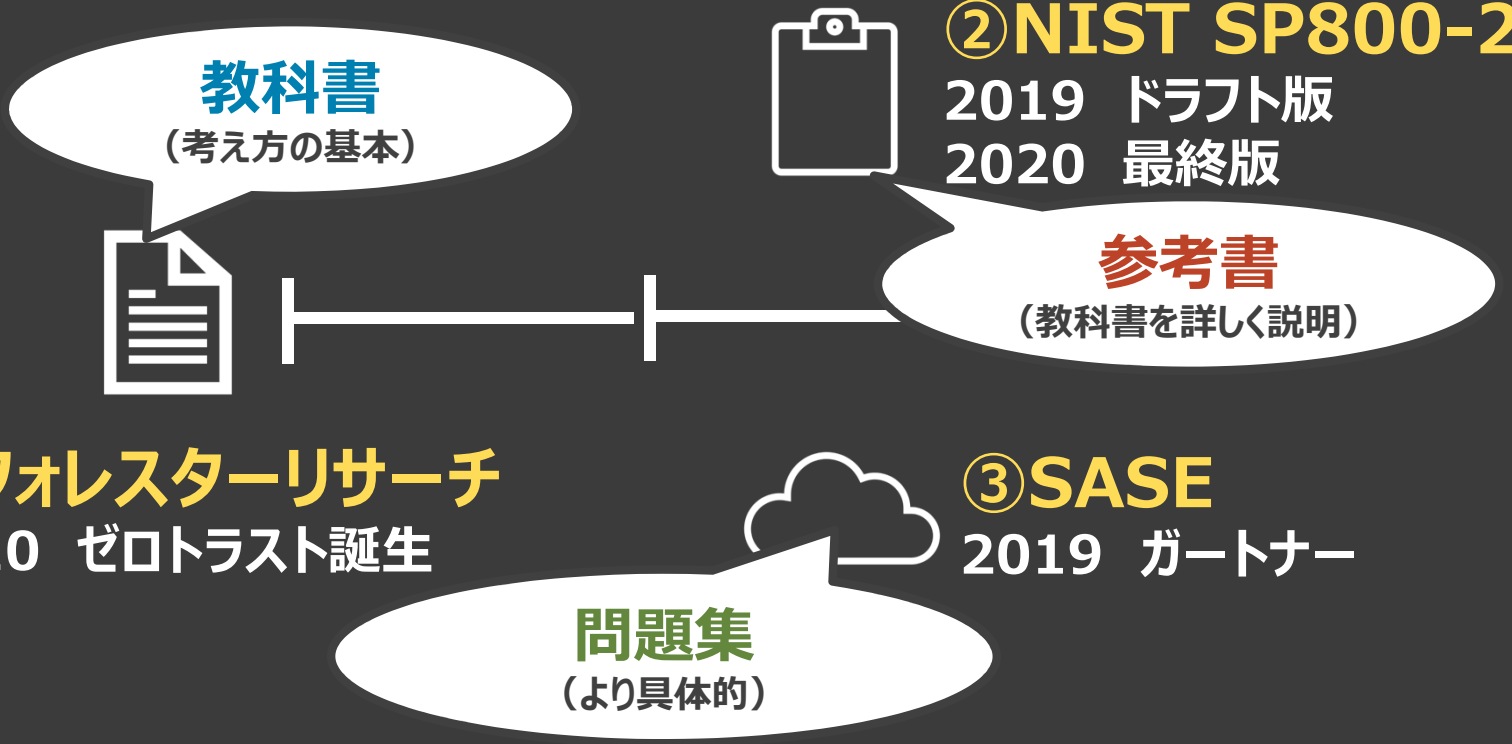
③SASE（セキュアアクセスサービスエッジ）

2019 ガートナー



NTT DATA

ただし、ゼロトラストのコンセプトを実現する、ただひとつのソリューションは今のところない



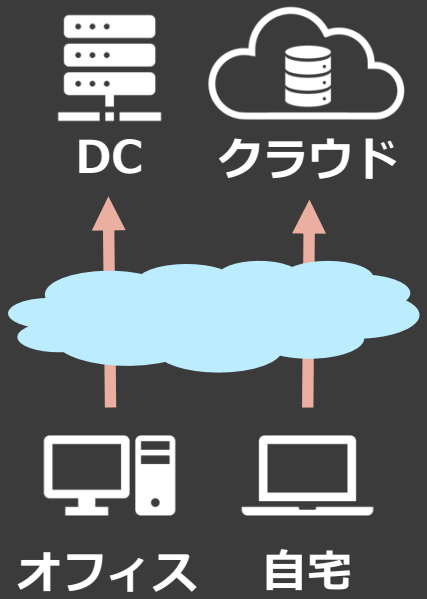
1．ゼロトラストとはなにか

2．ゼロトラスト実現への進め方

3．実施事例（ゼロトラストの最初の一歩）

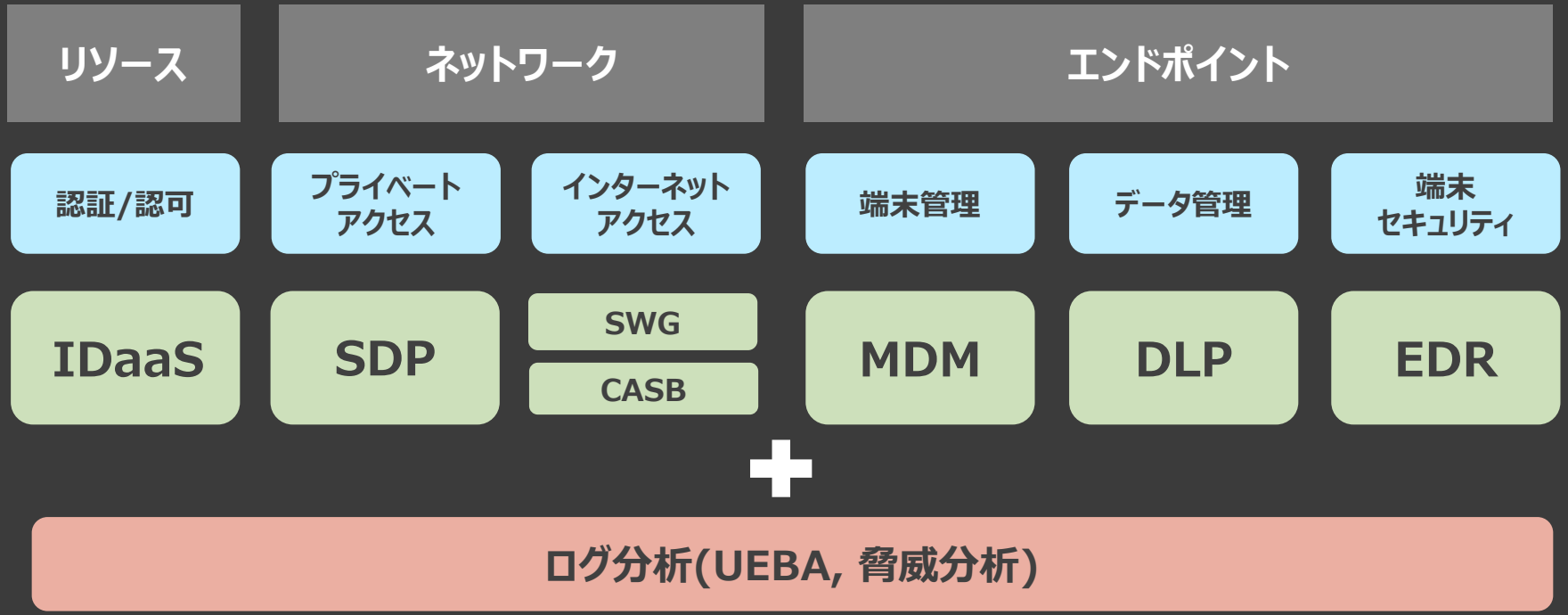
NTT DATA

テレワークの構成要素をモデル化して考える

モデル	分類	ポイント
	リソース	リソース（情報資産）への権限があるか、アクセスの度に検証
	ネットワーク	場所やネットワークに依存せず安全にアクセスする
	エンドポイント	情報漏えいの検知 ＆ エンドポイント監視

ゼロトラストに必要な技術要素の例

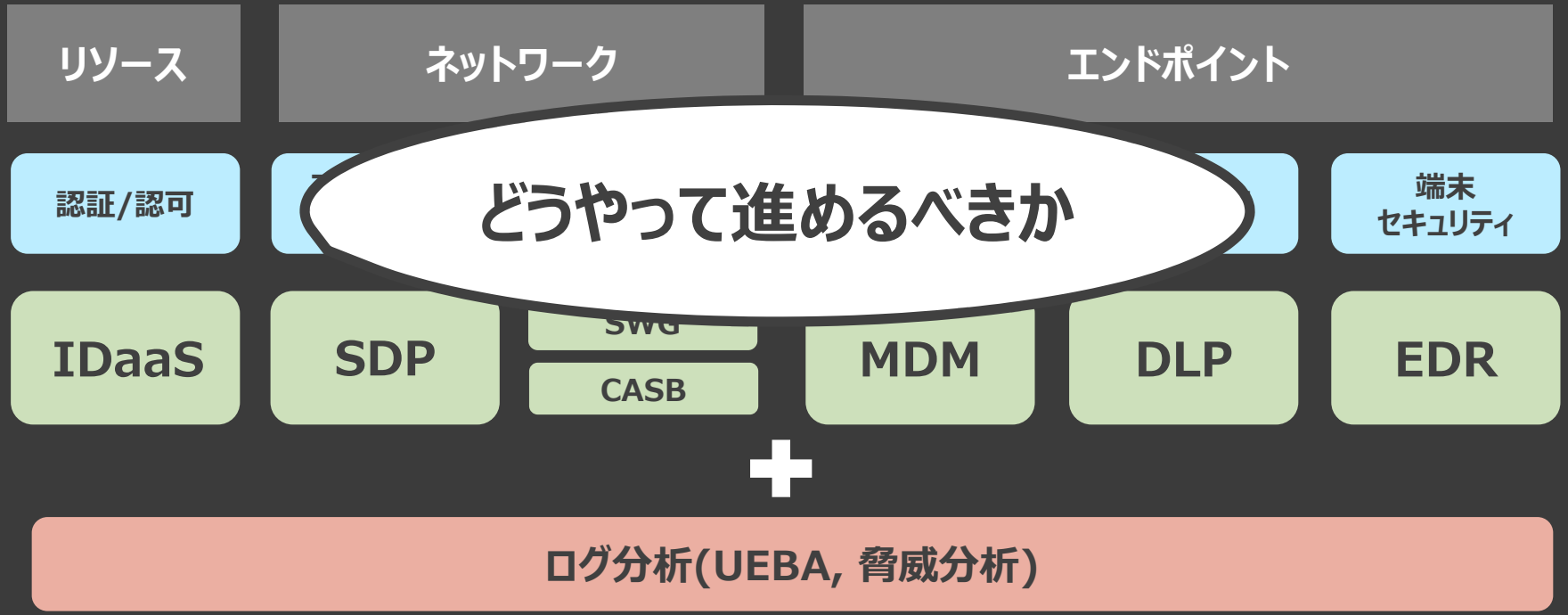
技術・ソリューションをどう組み合わせるかが重要



NTT DATA

ゼロトラストに必要な技術要素の例

技術・ソリューションをどう組み合わせるかが重要



NTT DATA

目指すゼロトラストの形（NIST SP800-207より)

従来のセキュリティ対策と組み合わせながら、段階的にセキュリティを高める

Pure Zero Trust Architecture

理想的なゼロトラストアーキテクチャのこと。
まっさらな状態（Green Field）から作るなら可能

Hybrid Zero Trust Architecture

ゼロトラストと境界防御モデルとが共存する環境
段階的にゼロトラストモデルを導入

どこから手を付けていくべきか

優先順位が前後することはあるが、まずは認証/認可から

リソース 1	ネットワーク 2		エンドポイント 3		
認証/認可	プライベート アクセス	インターネット アクセス	端末管理	データ管理	端末 セキュリティ
IDaaS	SDP	SWG CASB	MDM	DLP	EDR

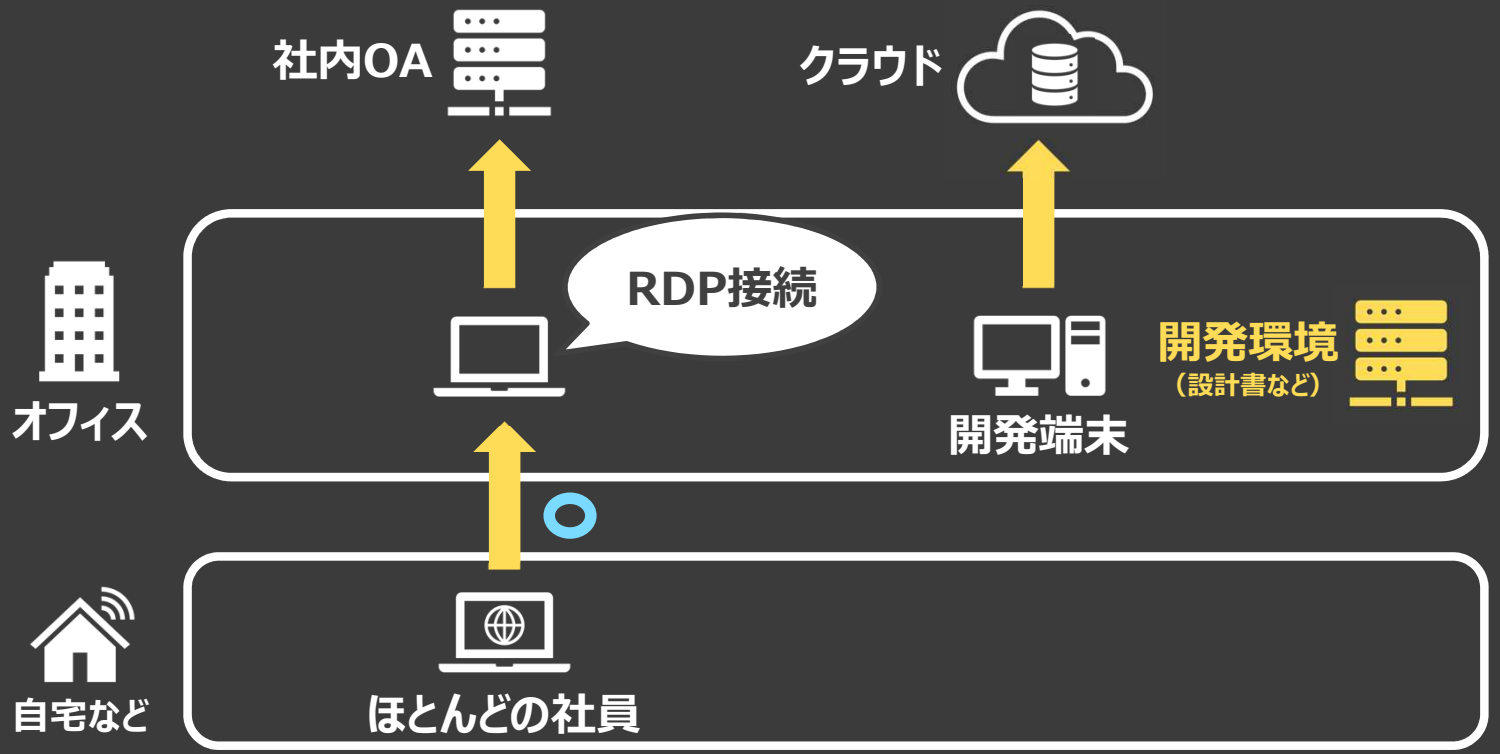
＋

4 ログ分析(UEBA, 脅威分析)

1．ゼロトラストとはなにか
2．ゼロトラスト実現への進め方
3．実施事例（ゼロトラストの最初の一歩）

リモートデスクトップ（RDP）方式のテレワークを全社導入(2020年2月~3月)

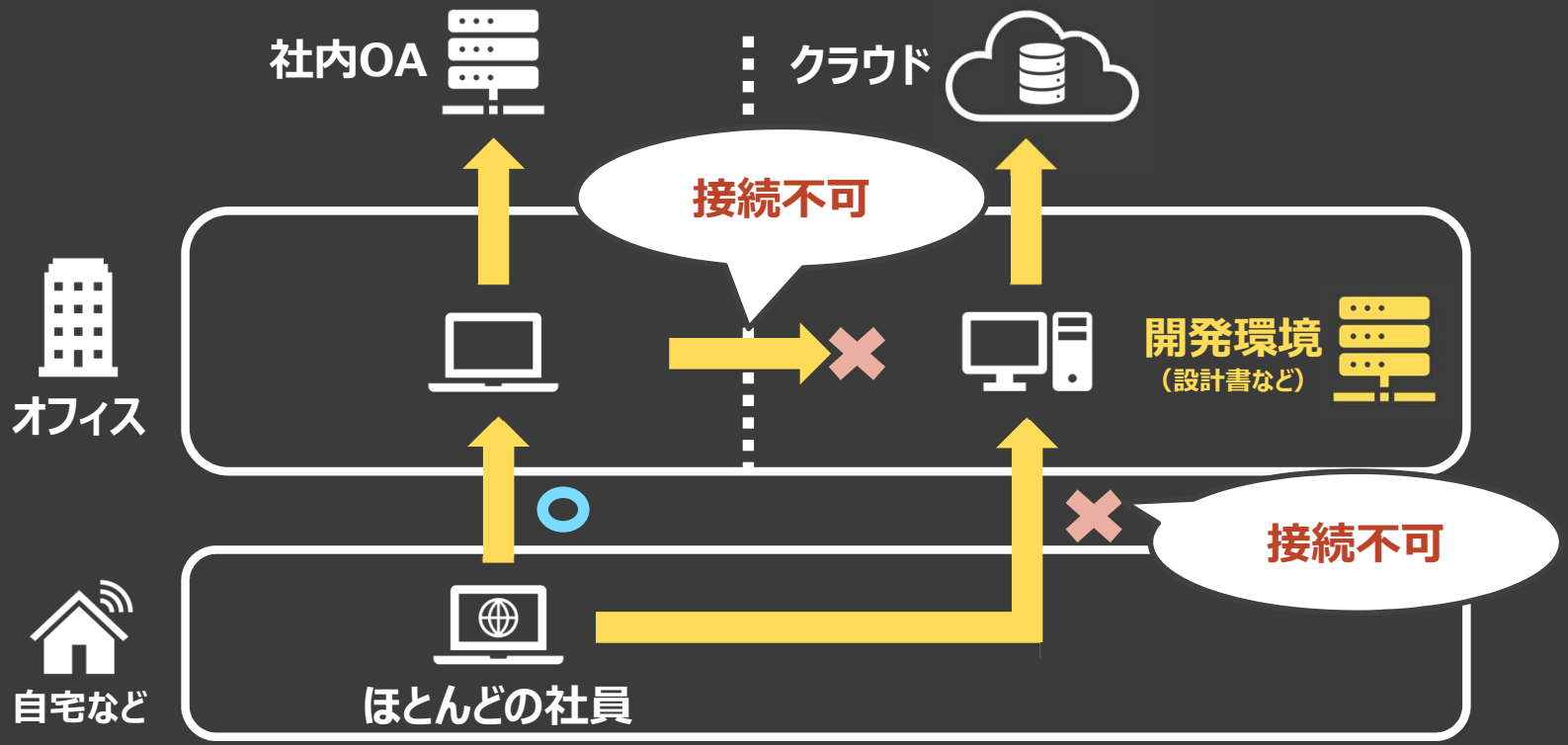
開発・保守担当のみ在宅率が低かった（~50%）



NTT DATA

境界防御モデルの限界に直面

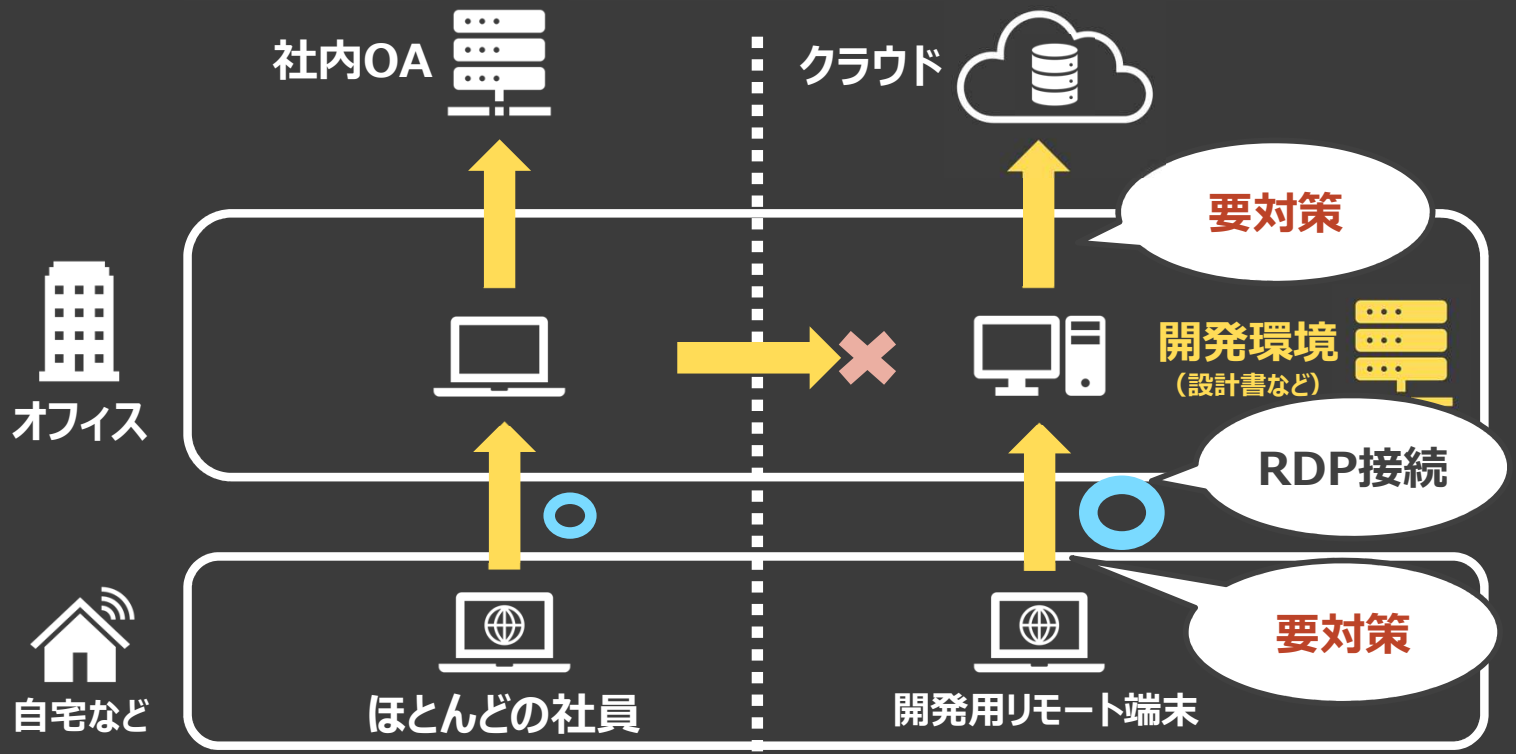
開発環境へは外部から接続できず、OA環境とはネットワーク分離しているため入れない



NTT DATA

自宅から開発環境へリモート接続するためには

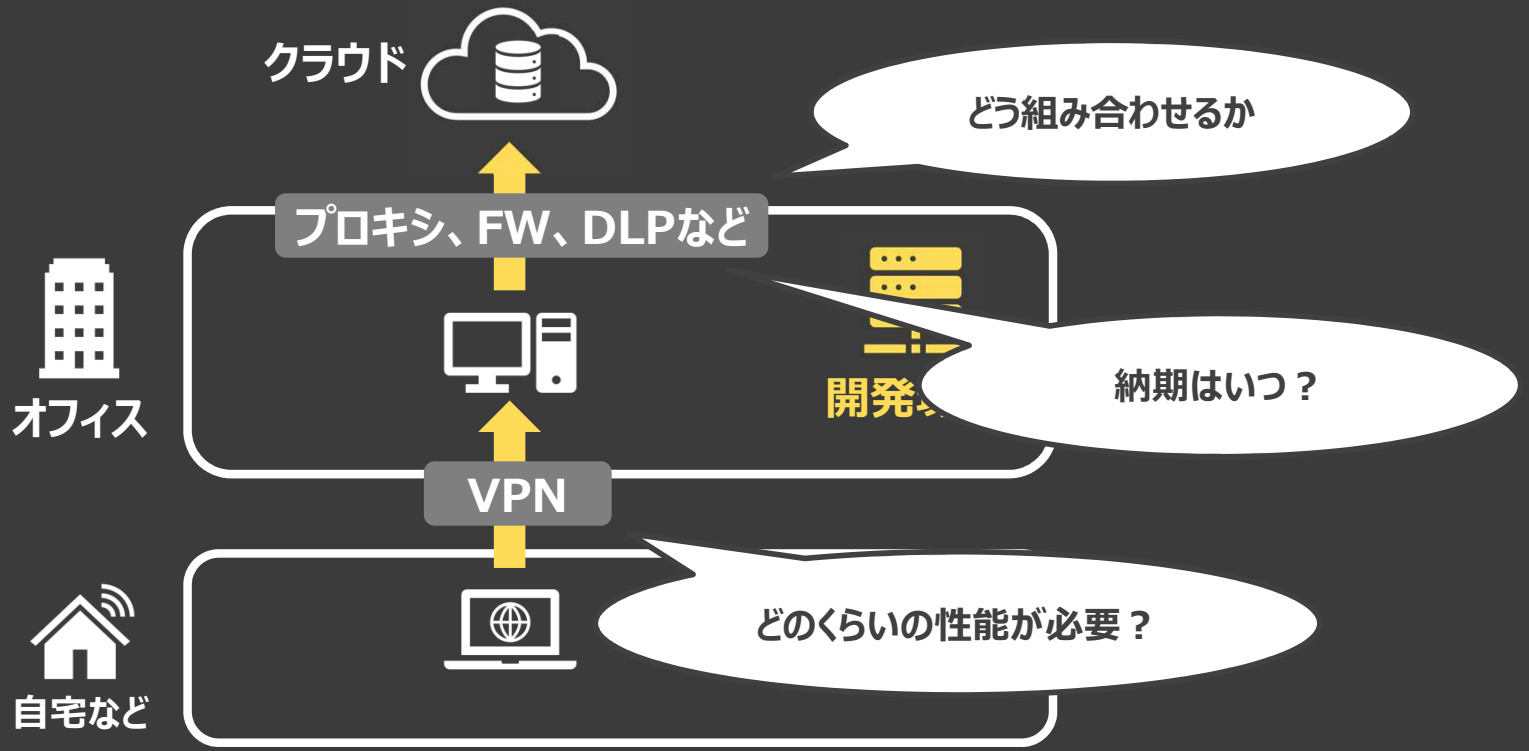
部門で管理するネットワークとなるため、独自にセキュリティ対策が必要



NTT DATA

従来どおりのセキュリティ対策だと、サイジングの検討・構築に時間がかかる

OA環境と同じ作り方・やり方では間に合わない



NTT DATA

自宅から開発環境へリモート接続するうえでの課題

ネットワークセキュリティ対策の準備とスケジュール

入口と出口のセキュリティ対策

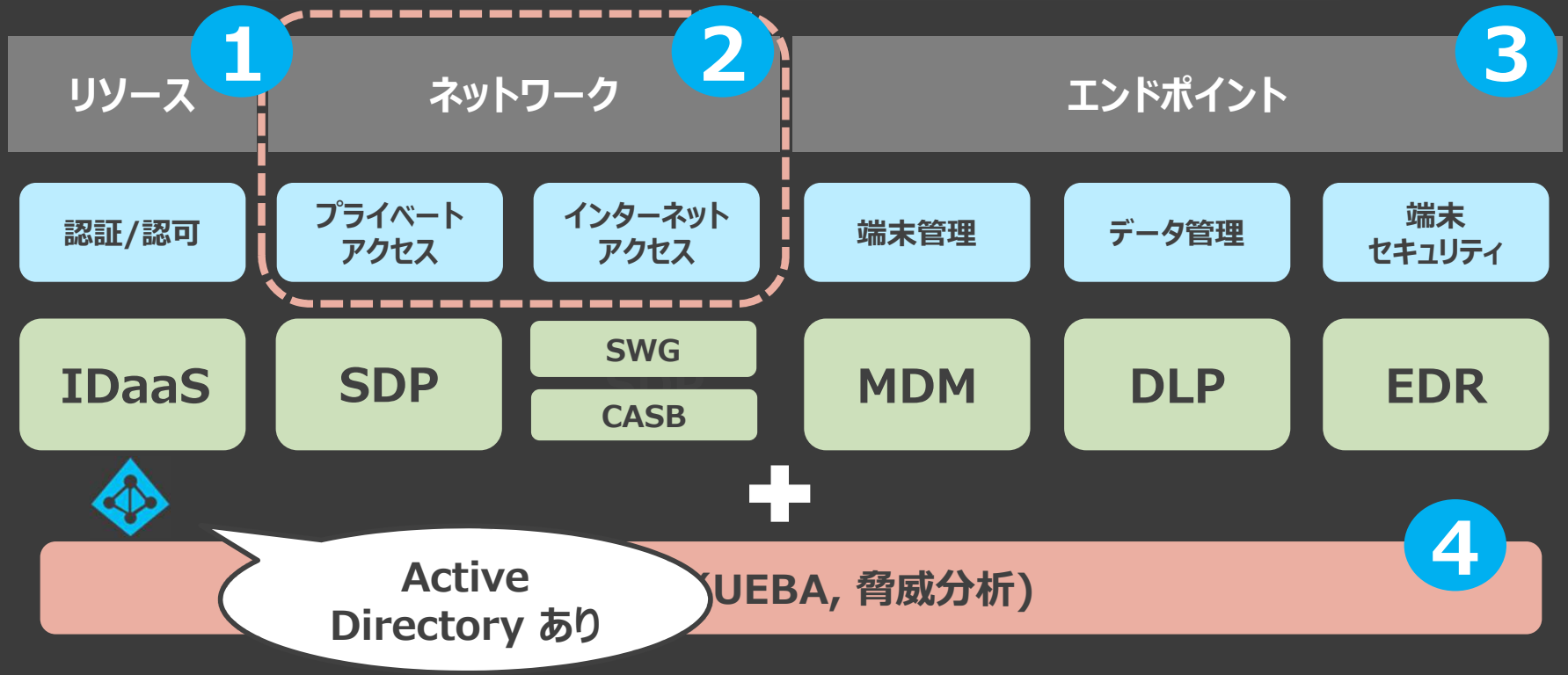
社内ネットワークから独立するため、社内システムの対策は利用できず、イチから設備が必要。

スケジュール

新型コロナウイルス対策のため、目処としては、1ヶ月くらいでテレワークに移行したい。

ゼロトラストの技術要素と合わせてみると・・・

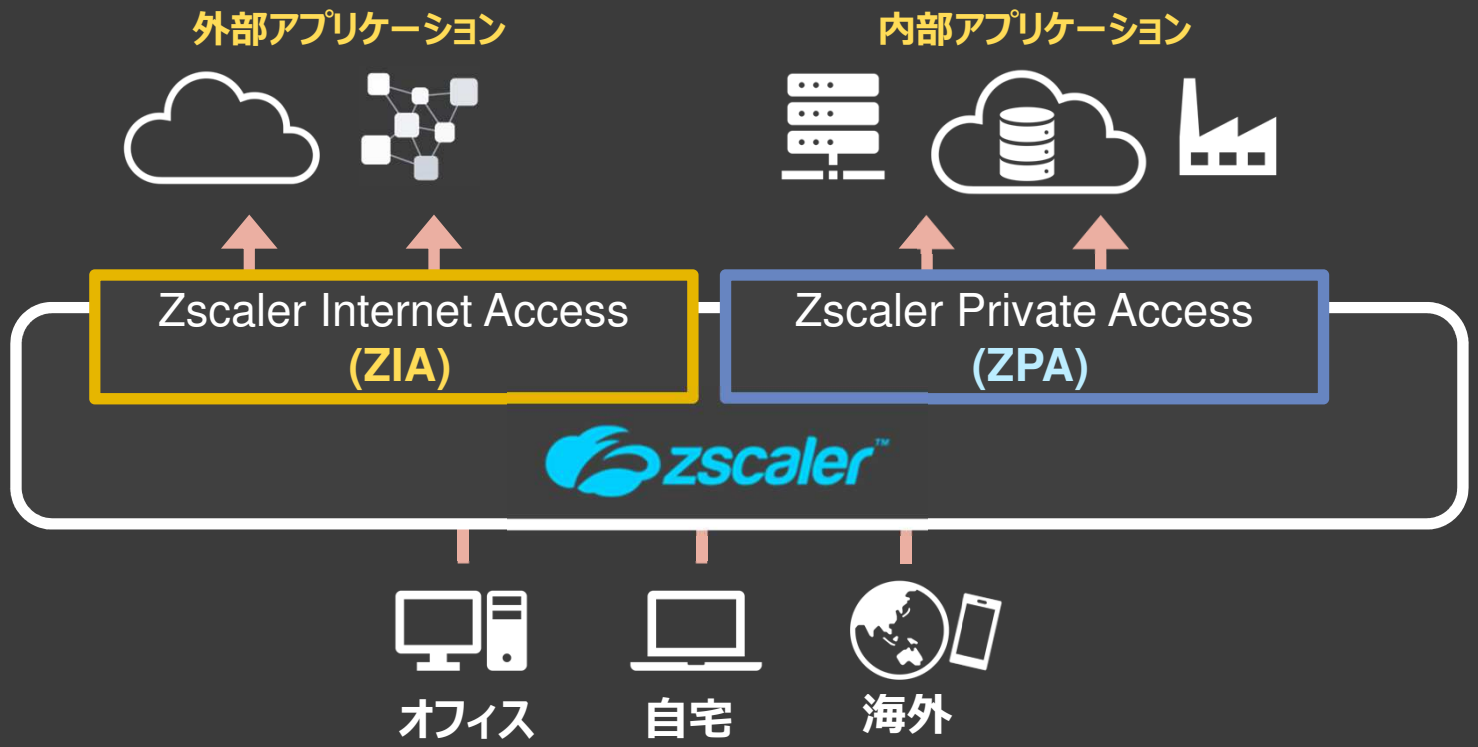
ゼロトラストの考えをベースにすると、次はネットワーク対策を検討する



NTT DATA

クラウド型プロキシソリューションである Zscaler を採用

場所やデバイスに縛られず、統一的なセキュリティ対策が可能



NTT DATA

理由①　クラウド型ソリューションだから

クラウドだから、どこでも使えて、すぐに利用できて、サイジングもすぐに可能

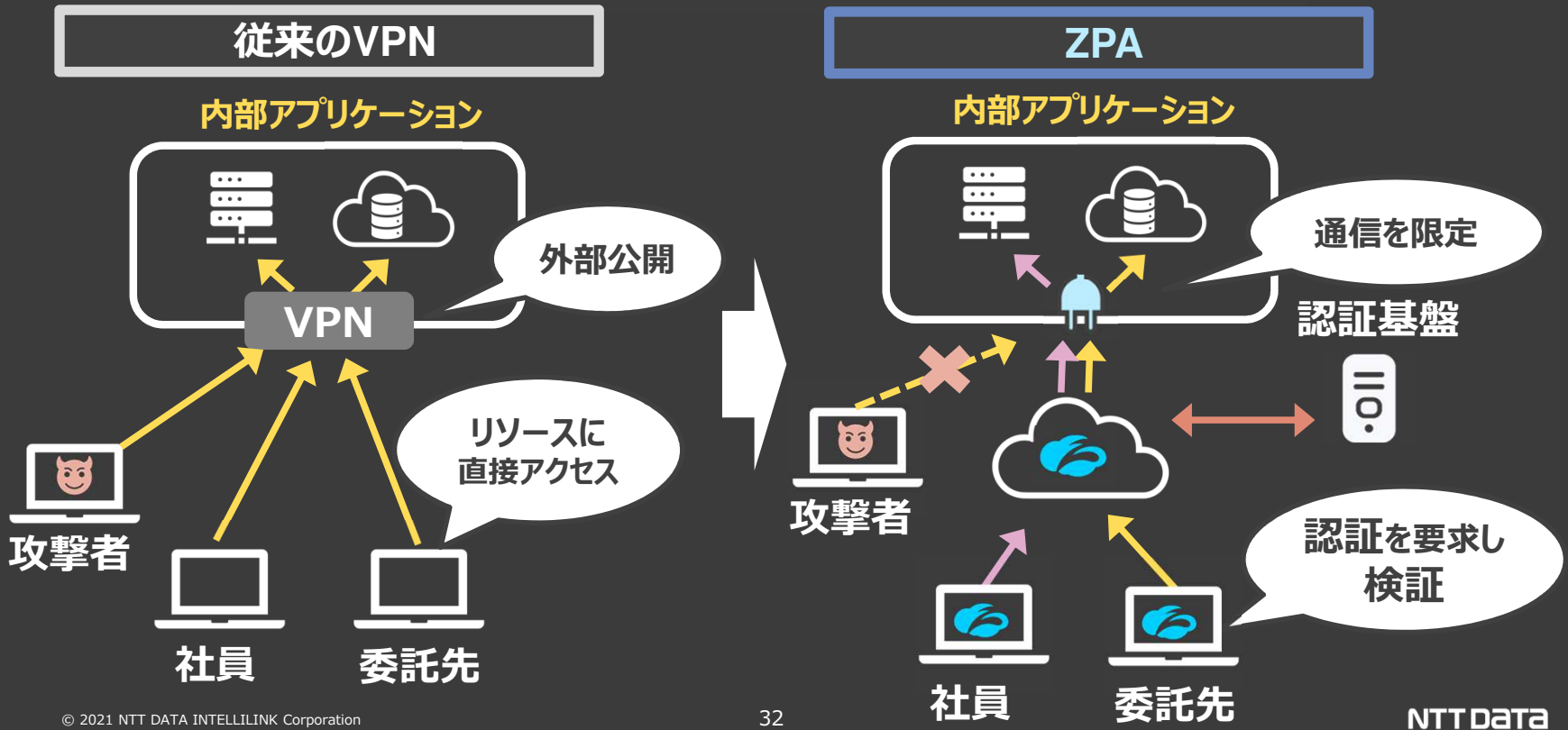
・入口と出口のセキュリティ対策

・スケジュール 

では、ZPAとZIAでどのようなセキュリティ対策ができるか？

理由②　ZPAは、ゼロトラストベースのアクセス制御を行うSDP製品

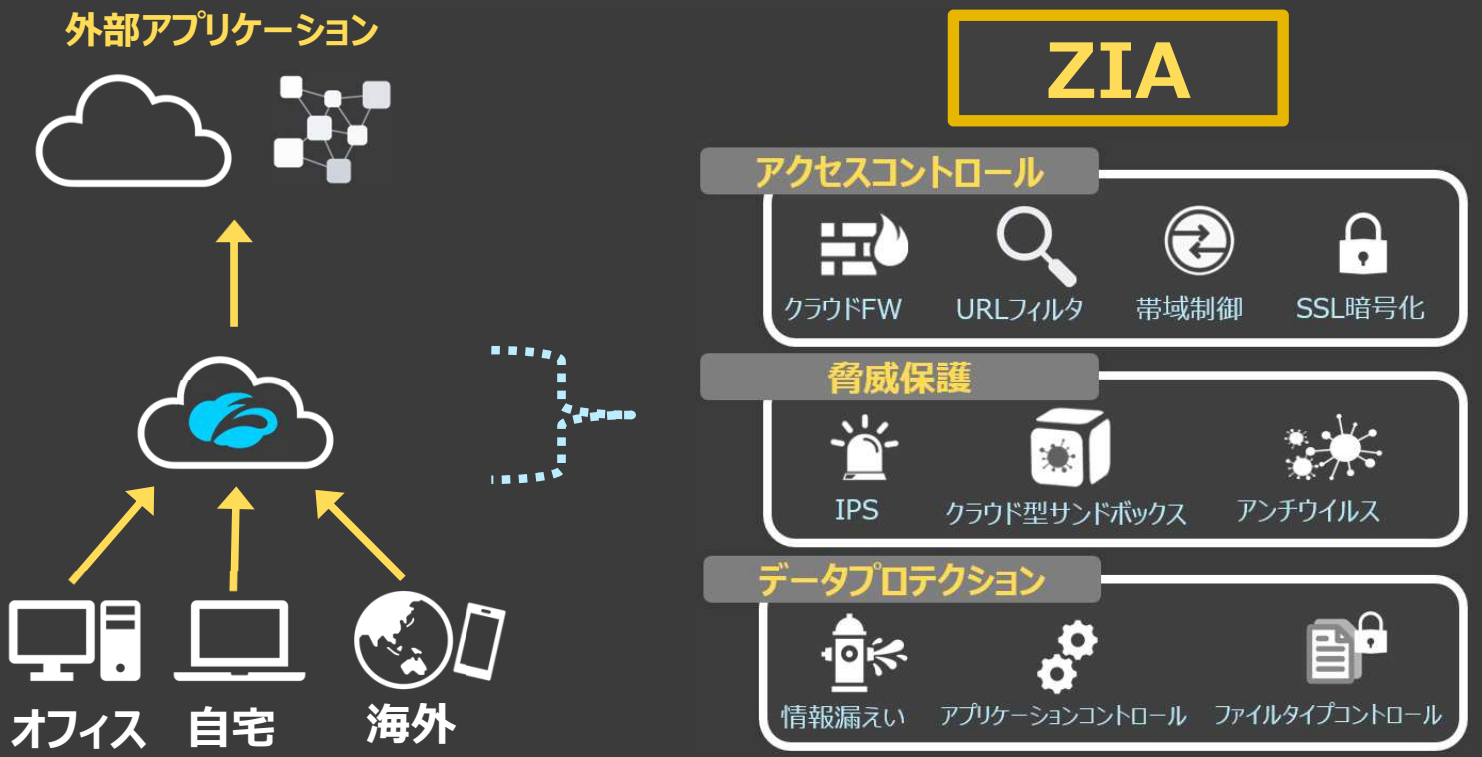
DDoS攻撃や不正侵入、そして内部不正のリスクを大幅に低減



NTT DATA

理由③　ZIAは多層防御をクラウドサービスで実現するSWG製品

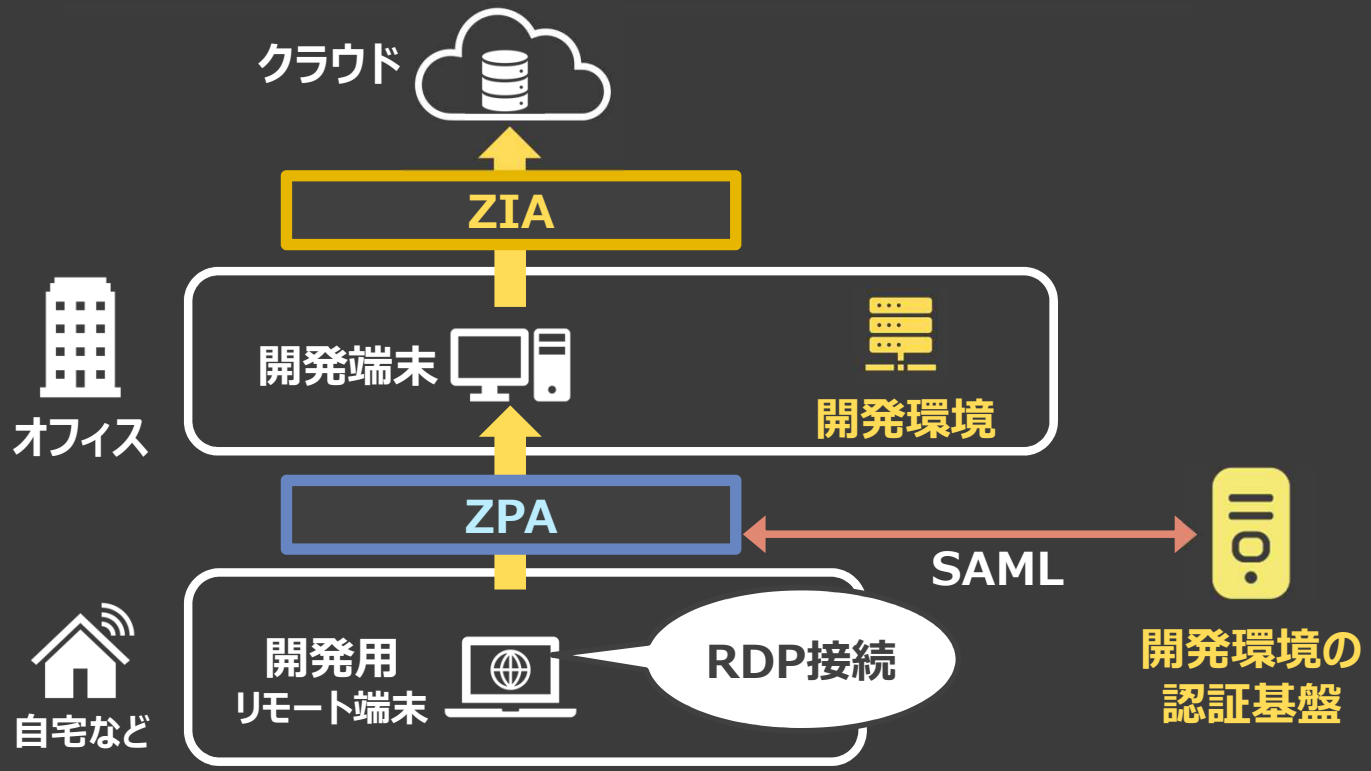
多層防御することで起こりがちな、処理遅延も抑制



NTT DATA

ZPA と ZIA を使うことでゼロトラストベースのセキュリティ対策を実施

自宅からリモートデスクトップ接続で、開発・保守作業を開始



NTT DATA

結果（2020年3月→４月）

検討から１ヶ月程度で、開発・保守担当のメンバがテレワークへ移行

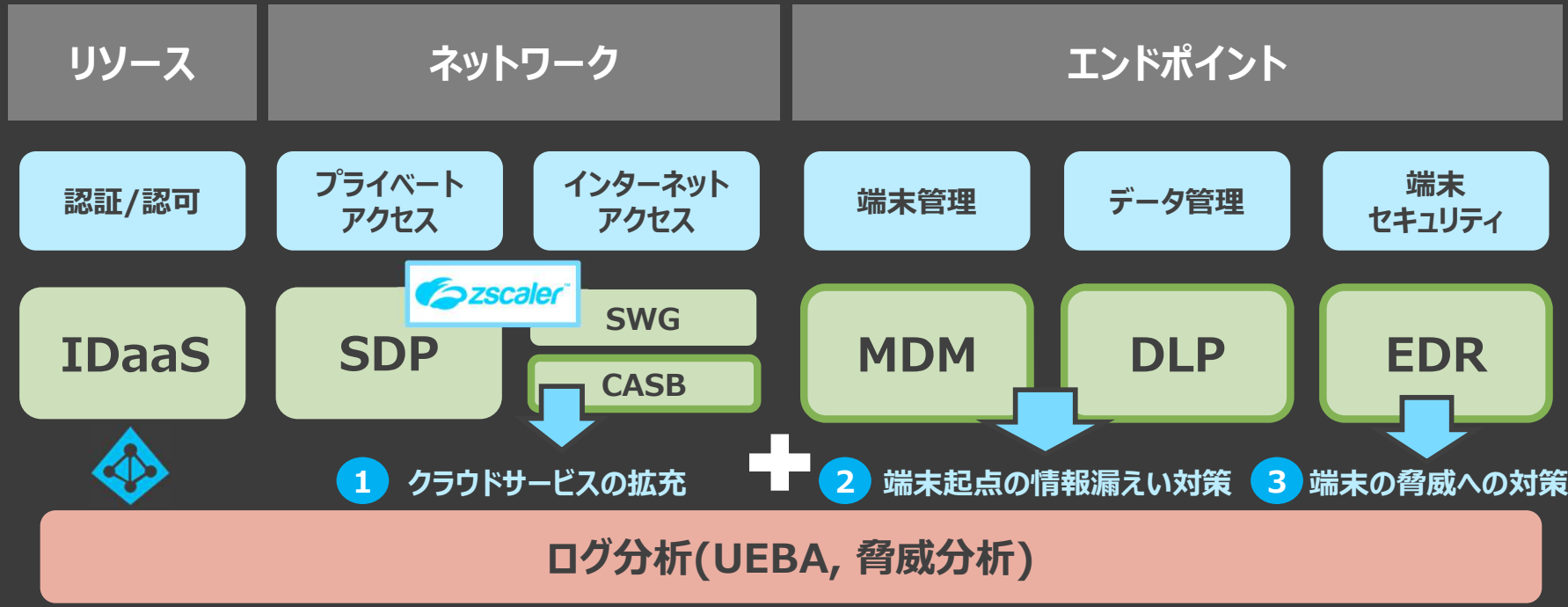
在宅率50%から

90%へ！

NTT DATA

次のステップ –クラウドサービスの利用範囲を広げつつ、エンドポイント対策を進める-

利便性を上げるため、セキュリティ対策を段階的に導入



NTT DATA

Zero Trust based Consulting & Support

お客様の要件に合わせ、当社取扱サービスを組み合わせて、ゼロトラストのモデルを提案

リソース	ネットワーク		エンドポイント		
認証/認可	プライベート アクセス	インターネット アクセス	端末管理	データ管理	端末 セキュリティ
IDaaS	SDP	SWG CASB	MDM	DLP	EDR
Active Directory	zscaler	MCAS	Microsoft Intune		cybereason

exabeam ログ分析(UEBA, 脅威分析)

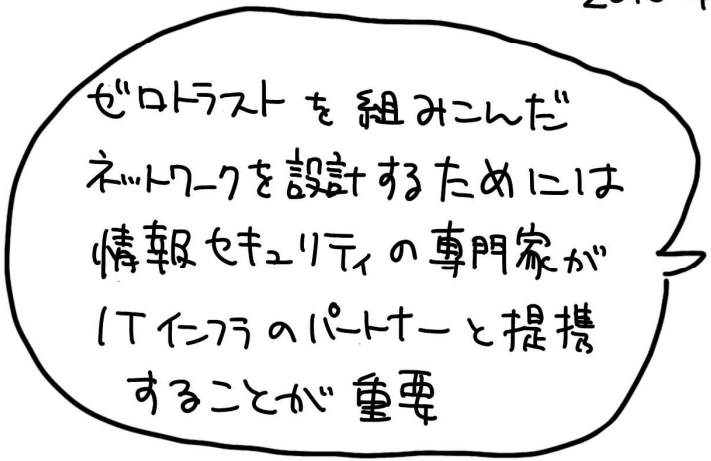
※すべてのサービスを導入するわけではありません。

NTT DATA

さいごに

「これひとつでゼロトラスト」はない。

ゼロトラストの提唱者のジョンは、
2010年のレポートで



John Kindervag
ジョン・キンダーバーグ

と言っています。

ゆういち

NTT DATA

Trusted Global Innovator

Appendix

はじめに

本オファリングは「ニューノーマル」、そして、「DX」というキーワードを念頭に置き、
NTTデータ 先端技術 に相談された様々なセキュリティ課題を解決する
パッケージをご紹介する資料となります。

各サービスの詳細については、別途お問い合わせください。

Total Security Assessments Service for DX / New Normal

潜在リスクを可視化し、効果的に対応できるようにすることで、IT活用を促進

1.社内セキュリティ組織

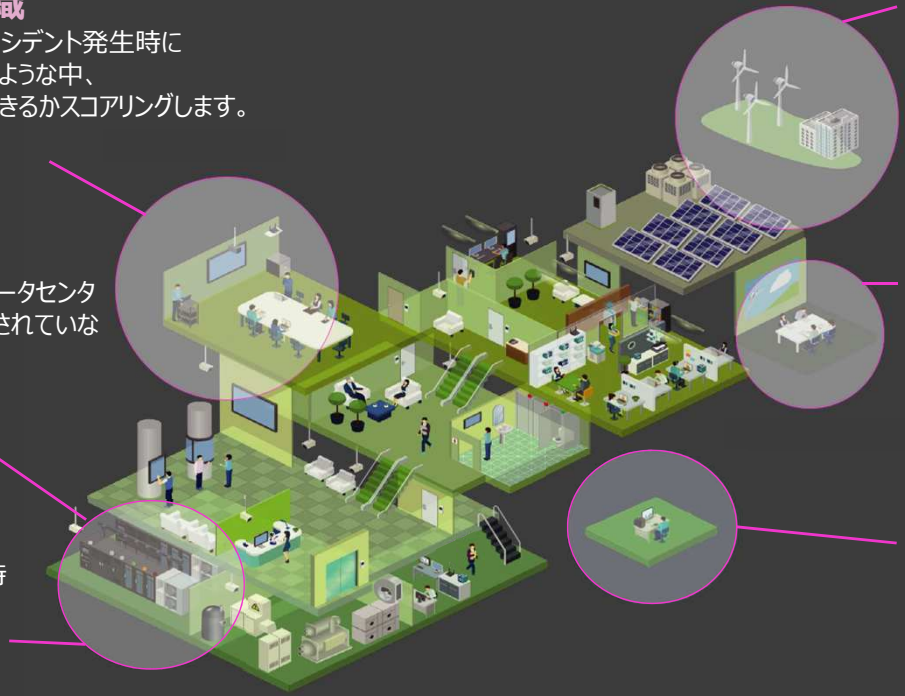
ニューノーマル環境下では、インシデント発生時に対面での対応はできません。このような中、貴社のセキュリティ組織が対応できるかスコアリングします。

2.社内システム

社内システムで利用しているデータセンタやクラウドサービスが、脅威にさらされていないか診断します。

3.パソコンなどの機器

通信情報からパソコンなどの機器を一覧化することで、情報の持ち出しなど組織内の不正な動きを取り締まります。



4.取引先

セキュリティ対策が脆弱な取引先や子会社等を経由して大企業に攻撃を仕掛ける「サプライチェーン攻撃」の被害は年々深刻化しています。

そのようなサプライチェーン攻撃へのリスクを点数化し、改善すべきポイントを可視化するスコアリングサービスを提供します。

5.従業員のセキュリティ意識

目の行き届かないテレワークにおいては、これまで以上に、従業員一人ひとりの自律した行動が必要です。

従業員個人のセキュリティ意識のアセスメントを行い最適な教育プログラムを提案します。

6.テレワーク環境

短期間でテレワーク環境を構築・運用を始めた場合、情報セキュリティに対する考慮が後回しとなり、テレワーク環境が不正侵入の入口となりかねません。そこで、組織・ITの面から情報セキュリティ対策を評価・分析し、課題と対策を提示します。

NTT DATA