ゼロトラストをめぐる企業・業界動向

IIJ
Internet Initiative Japan

2020年10月29日

株式会社インターネットイニシアティブ
サービスプロダクト推進本部 副本部長
三木 庸彰

目次

- はじめに
- “ゼロトラスト”が注目される背景
- “ゼロトラスト”とは
- “ゼロトラスト”の7つの信条
- “ゼロトラスト”の基礎
- ベンダ各社のアプローチは様々
- 気になる“ゼロトラスト”の説明
- “ゼロトラスト”と国内企業のいま
- “ゼロトラスト”のリアル

はじめに

- “ゼロトラスト”で、画期的な新技術が出た！というわけではない
- ただ、境界防御型セキュリティの考え方だけでは不十分になっている

① コロナ禍におけるテレワークの需要急増で“ゼロトラスト”の注目度がアップ
② 脆弱性を突いて起きるセキュリティ侵害が後をたたない
③ IIJにおいて“ゼロトラスト”の実現を支援するサービスが揃ってきた

そこで、IIJとしての“ゼロトラスト”の捉え方をまとめてみました

IIJ
Internet Initiative Japan

“ゼロトラスト”が注目される背景

- 社内システムがクラウドへ
- ワークプレースが社外へ
- デバイスが多様化
- 働き方の多様化（副業・兼業の受け入れ）
- 侵害を前提とした対策の必要性

IIJ
Internet Initiative Japan

“ゼロトラスト”とは

- 2010年に、フォレスターリサーチ社の元アナリストが考案した概念
- NIST（米国国立標準技術研究所）でも提唱されているセキュリティモデル
  （NIST SP800-207「Zero Trust Architecture」 2020年8月に最終版が公開）
- “守るべき企業のITリソース/情報資産”は、様々なクラウド上に分散されていき、それらにどのようにアクセスを許可していくか、という考え方を示したもの

「信頼する、けど検証する」から「信頼せず、常に検証する」へ

IIJ
Internet Initiative Japan

“ゼロトラスト”の7つの信条

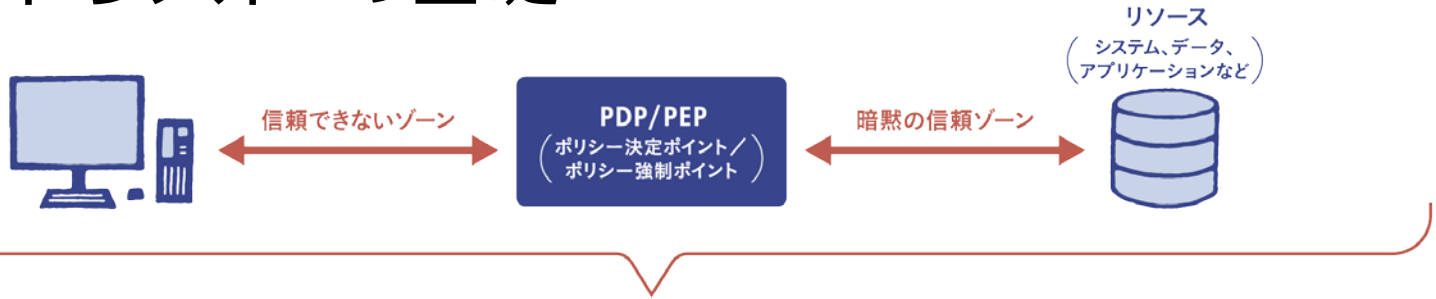
- NIST SP800-207 で提唱されている 7つの信条

① アクセス対象のデータ、SaaS等は「全て」リソースとみなす
② ネットワーク的なロケーションを信用しない
③ リソースへのアクセスは「セッション毎」に認可するべき
④ リソースへのアクセスポリシーは動的に決めるべき
⑤ 企業のデバイスはセキュアな状態に維持・監視すべき
⑥ 確実で強固な認証と、認可の仕組み
⑦ できる限り多くの情報収集を行い、ポリシー策定に反映

これが全部できていないとダメというものではない。進むべき方向性である

IIJ
Internet Initiative Japan

“ゼロトラスト”の基礎



ゼロトラストを「航空機への搭乗」に喩えると

①

- 空港ではさまざまな人が行き交う。
- 航空機に搭乗するには、複数のチェックにパスしなければならない。

②

- 搭乗前に必ず保安検査を受けなければならない。
- 正規のパスポート・チケットを持っていても、危険物を持っていたら通過できない。
- 問題のないことが確認されれば、これより先のエリアでは、暗黙的に信頼が担保されたものとして扱われる。

③

- 搭乗には正規のチケットが必要。
- 搭乗口でもう一度チェックを受け、座席に着くことができる。

このゾーンは可能な限り小さくする

IIJ
Internet Initiative Japan

ベンダ各社のアプローチは様々

- 同じ“ゼロトラスト”を謳うものでも、<u>得意分野やアプローチが異なる</u>

例えば…

- ✓ **ID管理/SSO をベースにしたサービス**
- ✓ **Webゲートウェイを ベースにしたサービス**
- ✓ **Firewall/UTM をベースにしたサービス**
- ✓ **EDRやMDM をベースにしたサービス**
- ✓ **CASB をベースにしたサービス**

などなど…

<u>「ゼロトラストを実現するには様々な実装形態がある」＝1つではない</u>

IIJ
Internet Initiative Japan

気になる“ゼロトラスト”の説明

- 「境界防御型セキュリティが不要になります」
  → **それほど簡単に、かつ完全に無くせるわけではない**
- 「拠点間ネットワークやVPNが不要になります」
  → **完全に無くすことは難しい（広帯域・高信頼を求める場合には必要だし、社内システムをフルクラウド化できない現実も）**
- 「ゼロトラスト対応製品」
  → **“ゼロトラスト”は技術仕様やRFCではないので、“この製品・サービス（だけ）を導入すればゼロトラスト対応！”にはならない**

IIJ
Internet Initiative Japan

“ゼロトラスト”と国内企業のいま

- 先進的な企業では、先行して取り組みを開始している
- ただ、多くの企業では「**キーワードは知ってるけど、実際どうしたらよいかわからない**」「**いろいろサービスがあるのは目にしてるけど、どれを選べば良いのか判断つかない**」といった状況

お客様の感じ方と比べて、ベンダ側の主張/アピールの色合いが濃く、
“バズワード”的な見え方になっている印象

IIJ
Internet Initiative Japan

“ゼロトラスト”のリアル

- **”ゼロトラスト”を追求するには時間とコストがかかる**

  全ての社内システムやネットワークを一気に変えることまでは難しい

  認証・認可の強化やログ収集・相関分析など多くの追加コストがかかる

- **サービスや製品を導入したら終わり、ではない＝その後の“運用”が肝心**

  適切なアクセス先のリソースの設定や重要度の管理、デバイスのパッチ適用状況の管理、脅威情報の収集と判断、などが欠かせない

何年もかけてじっくり実現に向けた取り組みをしていくものと考える

IIJ
Internet Initiative Japan

Internet Initiative Japan

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――――――――IIJはいつもはじまりであり、未来です。

ゼロトラスト実現に必要なサービスのポイントと IIJ Omnibusが目指すこれからの企業ITシステム

IIJ
Internet Initiative Japan

2020/10/29

株式会社インターネットイニシアティブ
ネットワーククラウド本部長 城之内 肇

Ongoing Innovation

Agenda

1. ゼロトラストを目指す企業に必要なサービスとは
2. ゼロトラストを実現する IIJ Omnibus
3. IIJ Omnibusで実現するゼロトラストの将来像
4. 新しいデジタルワークプレース

1. ゼロトラストを目指す企業に必要なサービスとは

◆ ゼロトラスト推進の課題

ゼロトラストを実現することは簡単ではない

→ 現在のアーキテクチャからシステムの大幅な改変が必要

サービスや製品を導入したら終わりではない

→ 新たに発生する脅威への対応や定期的なポリシの見直しなど運用が不可欠

1. ゼロトラストを目指す企業に必要なサービスとは

- IIJが目指すゼロトラストモデル
  - ユーザ、デバイス、場所、時間、通信先、アプリケーション、データなどの複合情報に基づく認証認可
  - エンドポイント、ゲートウェイセキュリティなど複合的な機能による高セキュリティ
  - 継続的なセキュリティ対策を実行できる環境と継続的な運用管理可能な環境

IIJ Omnibus により、
ゼロトラストモデルを実現していきます

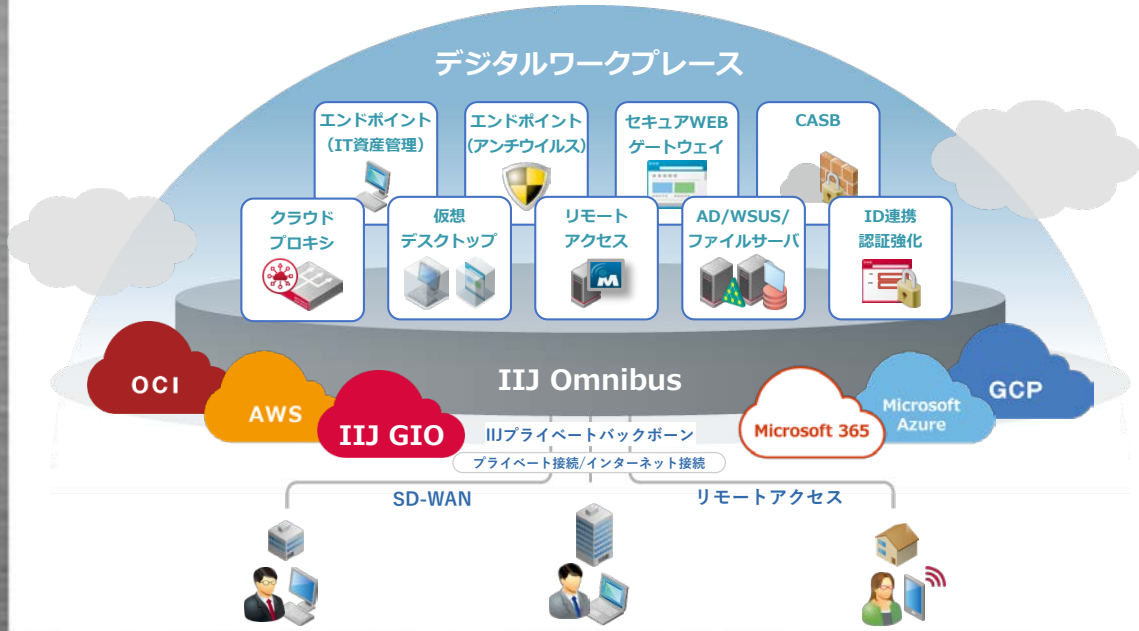
現在提供可能なモデル

2. ゼロトラストを実現する IIJ Omnibus

◆ IIJ Omnibus とは？

デジタルワークプレース

デジタルを利用し、場所や時間にとらわれない、
多様なワークスタイルが可能な世界



IIJ Omnibus

デジタルワークプレースを
支えるプラットフォームサービス

1. 快適なクラウド利用環境
   - インターネット接続およびクラウドダイレクト接続
2. 快適なネットワーク環境
   - SD-WANにより本社・支社などをシームレスに接続
   - 様々なネットワーク環境に対応（専用線・モバイル・インターネット）
   - 安定したリモートアクセス環境
3. 快適なオフィスIT環境
   - 仮想デスクトップやActive Directory、ファイルサーバなど

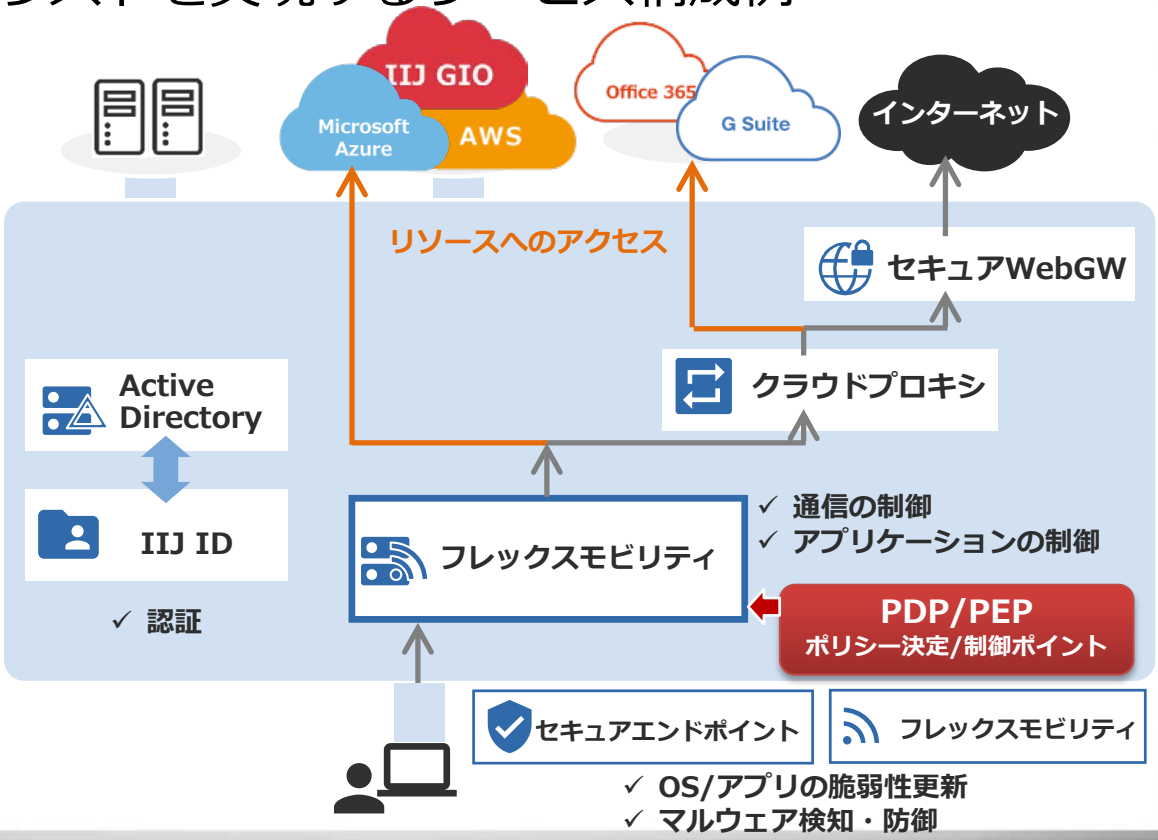
現在提供可能なモデル

2. ゼロトラストを実現する IIJ Omnibus

◆ IIJ Omnibusでゼロトラストを実現するサービス構成例

ゼロトラストを実現するサービス群（一部）

- **IIJセキュアエンドポイントサービス**
  アンチウイルス、IT資産管理
- **IIJフレックスモビリティサービス**
  快適リモートアクセス
- **IIJ仮想デスクトップサービス**
  VDI、Web分離
- **IIJディレクトリサービス for Microsoft**
  AD、WSUS、AADC
- **IIJ IDサービス**
  SSO、多要素認証、FIDO
- **IIJ セキュアWebゲートウェイサービス**
  URLフィルタ、アンチウイルス、ログ保管



現在提供可能なモデル

2. ゼロトラストを実現する IIJ Omnibus

◆ 例えば、業務形態や雇用形態に合わせた選択

会社支給の業務端末

エージェント あり

フレックスモビリティを使って実現 (前述)

会社で管理された業務端末は、デバイスにフレックスモビリティや、資産管理、ウイルス対策のエージェントをインストール。**デバイスの状態によって**アプリの利用を許可、拒否するというアプローチ。

ポリシー例

- 業務利用のアプリは、勤怠アプリ、営業管理アプリ、Teams、ブラウザ(Chrome) のみに限定
- 業務を行う時間帯は 9:00～17:30
- デバイスの状態として、会社支給PCである事、ウイルス検知ソフトバージョンをチェック
- ログイン時に、強制的にVPNトンネルを張り、上記以外の私用のPC利用は許可

特定業務のみ実施する

持込端末、非正規ユーザ

エージェント なし

仮想デスクトップを使って実現

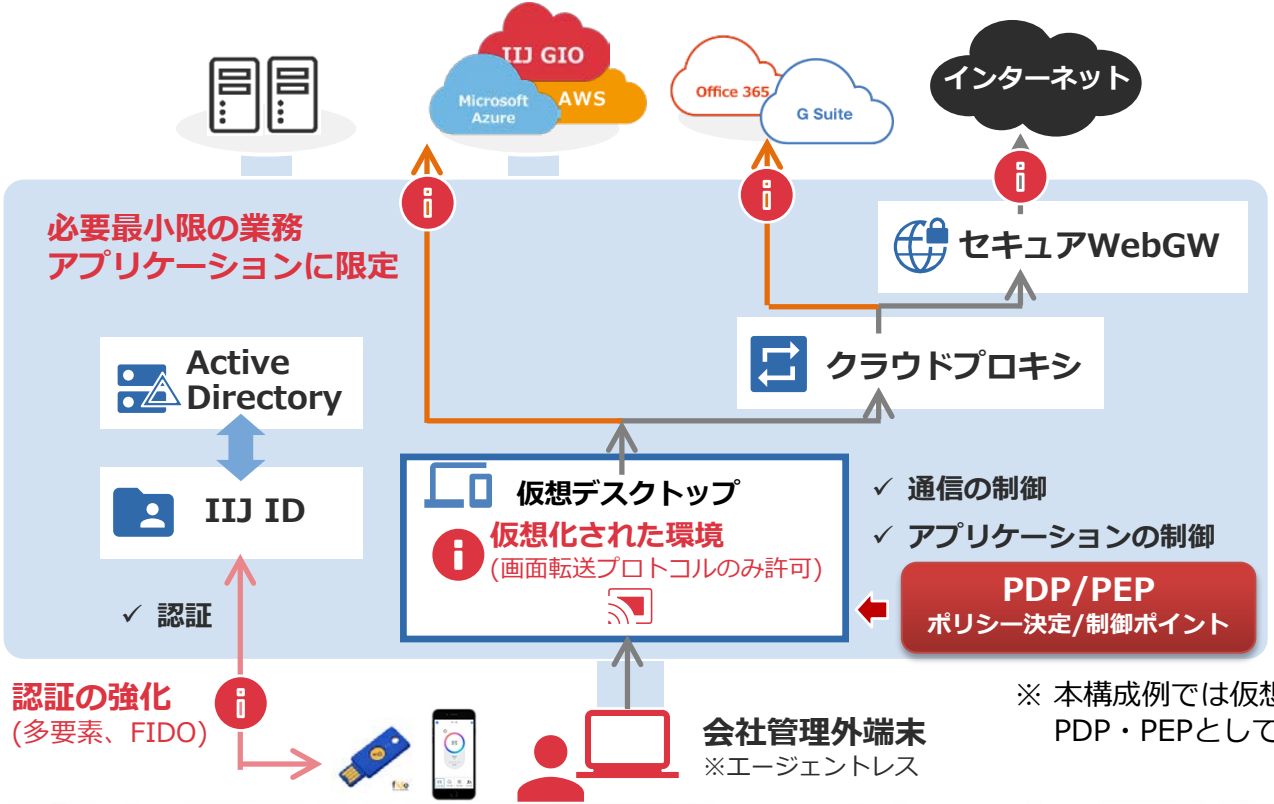
予め利用する人・グループを、条件によって許可されたアプリをサーバ側から配布。画面転送のプロトコルのみが許可され、**デバイスから完全に分離した仮想化された環境**で利用。

- 業務はローカルから分離された仮想デスクトップ上のブラウザ、Teams からのみ
- ログイン時は、二要素認証が必須

現在提供可能なモデル

2. ゼロトラストを実現する IIJ Omnibus

◆ ネットワークエージェントを配布しない構成イメージ



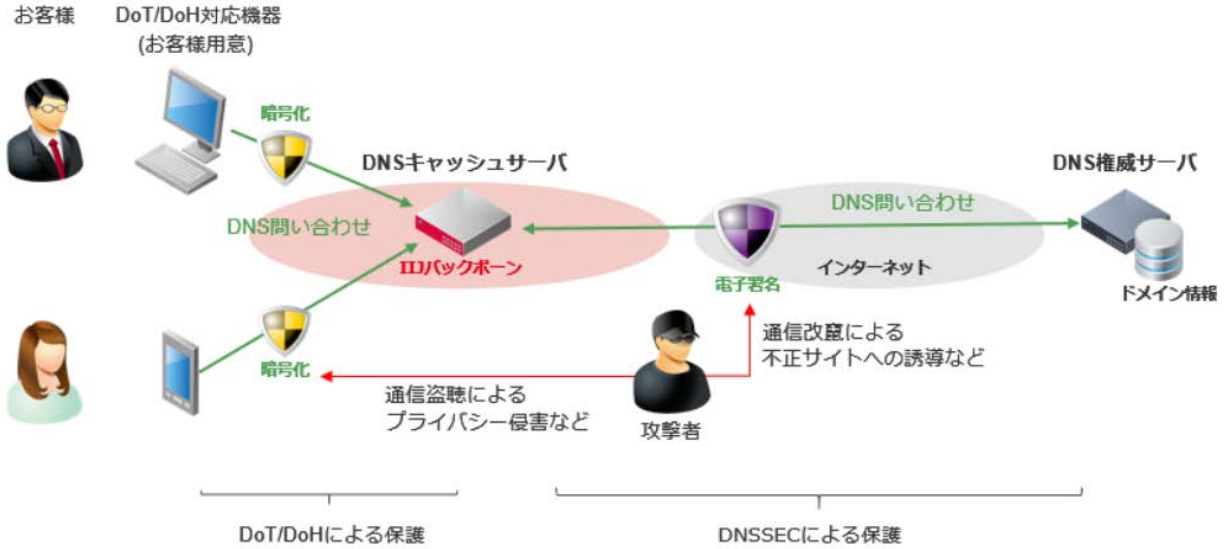
※ 本構成例では仮想デスクトップを
PDP・PEPとしている

ISP視点でのインターネットの脅威

DNS詐称の脅威

予期せぬ脆弱性が存在するDNS詐称の対策 **DNS暗号化**

※ 「DoT（DNS over TLS）」、「DoH（DNS over HTTPS）」および「DNSSEC（DNS Security Extensions）」



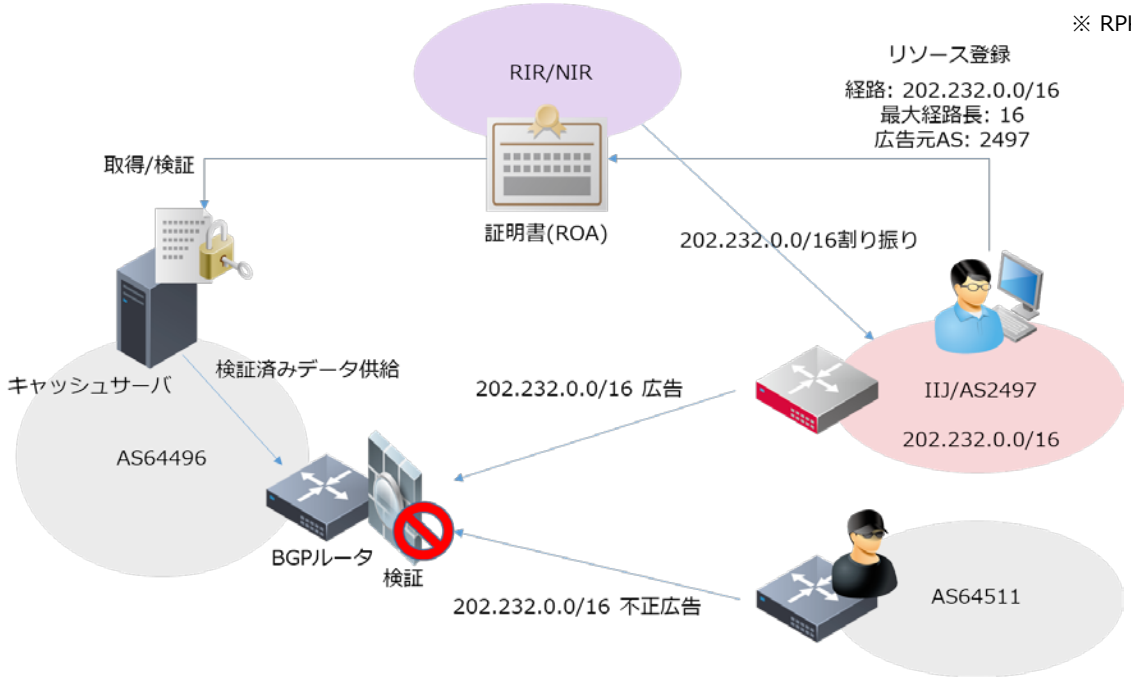
（参考）エンジニアブログ「IIJのDNS暗号化への取り組み」https://eng-blog.iij.ad.jp/archives/5298
2020年1月16日付報道発表資料「IIJ、接続サービスで提供するDNSのセキュリティを強化」
https://www.iij.ad.jp/news/pressrelease/2020/0116-2.html

ISP視点でのインターネットの脅威

インターネット経路詐称の脅威

インターネット経路（≒IPアドレス）の不正な乗っ取りの抑止 **RPKI**

※ RPKI（Resource Public Key Infrastructure）

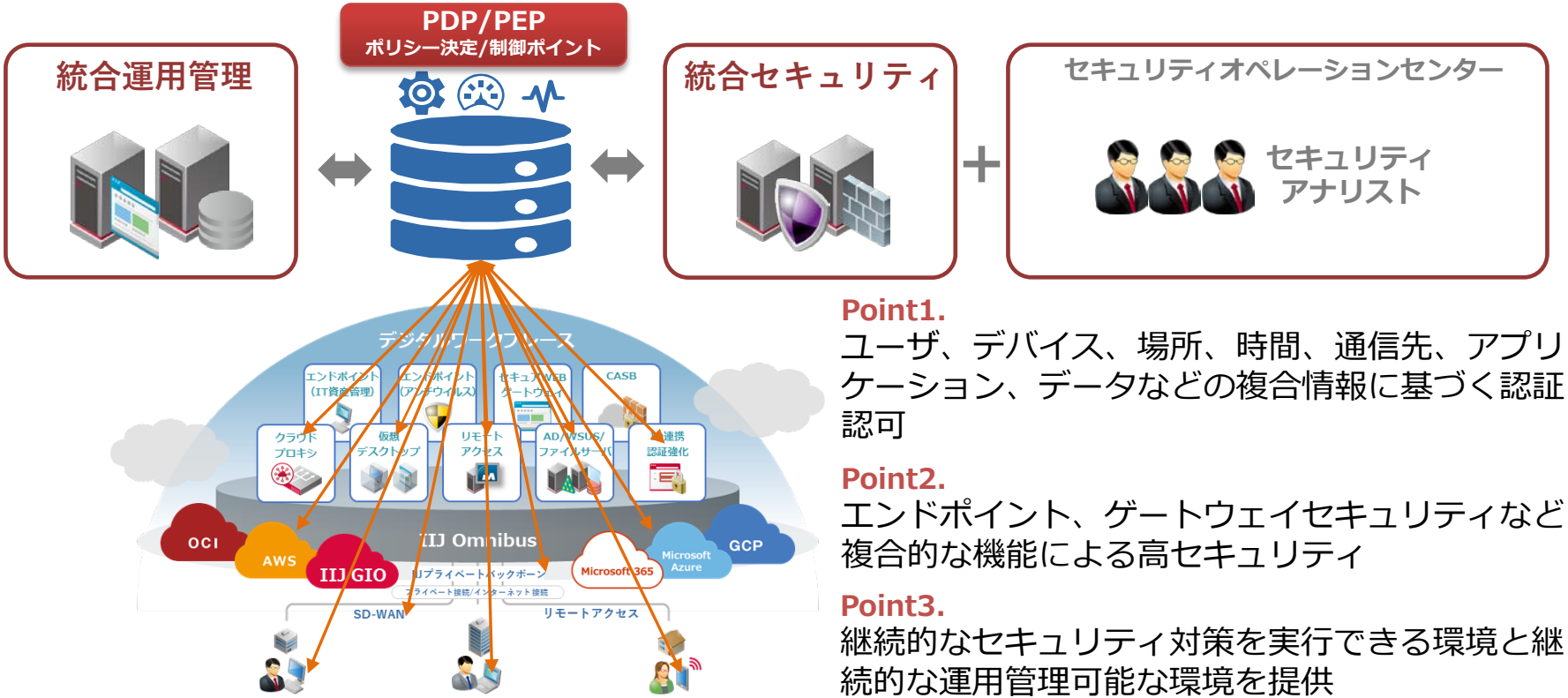


（参考）エンジニアブログ「インターネットをよりロバストに。RPKIはじめます」　https://eng-blog.iij.ad.jp/archives/6861

次世代構想モデル

3. IIJ Omnibusで実現するゼロトラストの将来像

◆ すべてのポイントのモニタリングによる統合運用管理及び統合セキュリティ



Point1.
ユーザ、デバイス、場所、時間、通信先、アプリケーション、データなどの複合情報に基づく認証認可

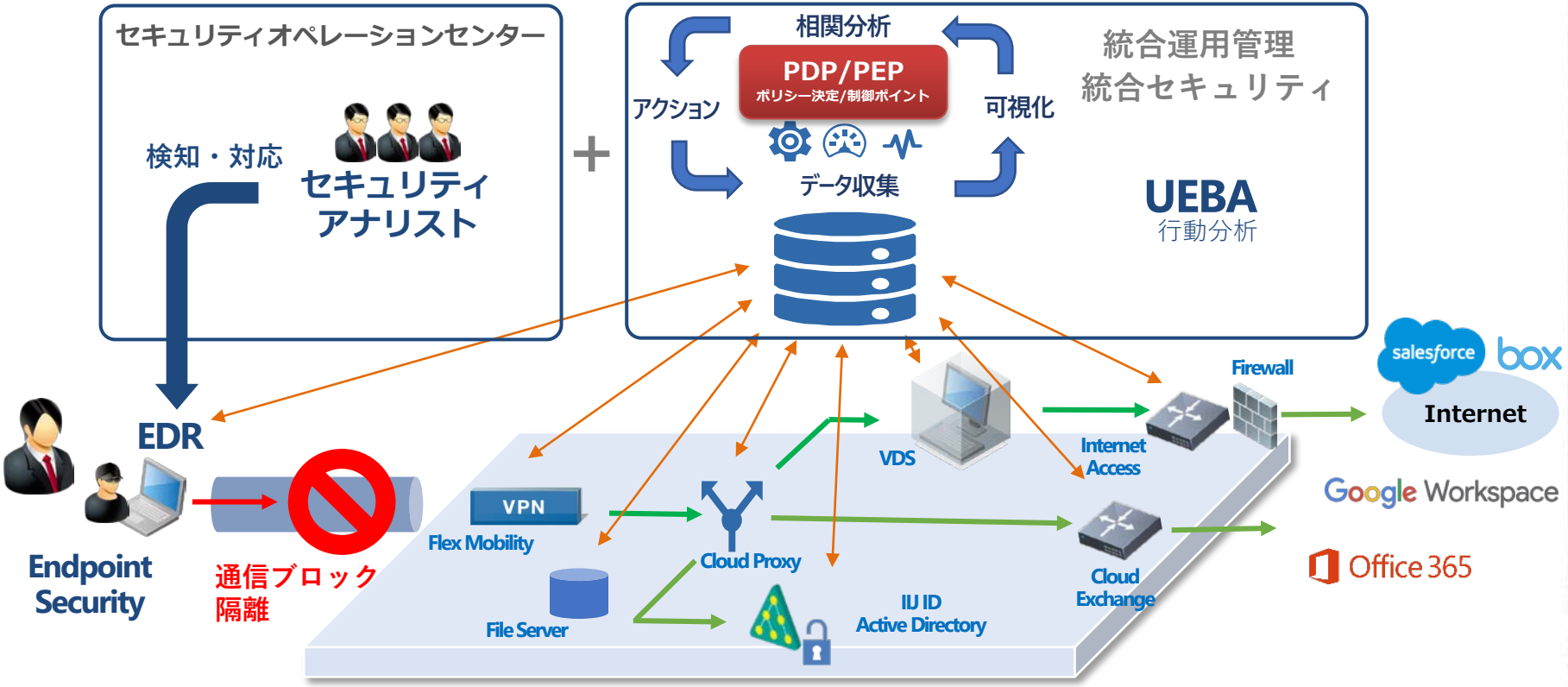
Point2.
エンドポイント、ゲートウェイセキュリティなど複合的な機能による高セキュリティ

Point3.
継続的なセキュリティ対策を実行できる環境と継続的な運用管理可能な環境を提供

次世代構想モデル

3. IIJ Omnibusで実現するゼロトラストの将来像

◆ ユースケース：セキュリティインシデントの早期発見とブロック



3. IIJ Omnibusで実現するゼロトラストの将来像

- ユーザ、デバイス、場所、時間、通信先、アプリケーション、データなどの複合情報に基づく認証認可
- エンドポイント、ゲートウェイセキュリティなど複合的な機能による高セキュリティ
- 継続的なセキュリティ対策を実行できる環境と継続的な運用管理可能な環境

IIJ Omnibus により、
ゼロトラストモデルを実現していきます

新しいデジタルワークプレース

4. 新しいデジタルワークプレース

◆ デジタルワークプレースとは

目指す姿

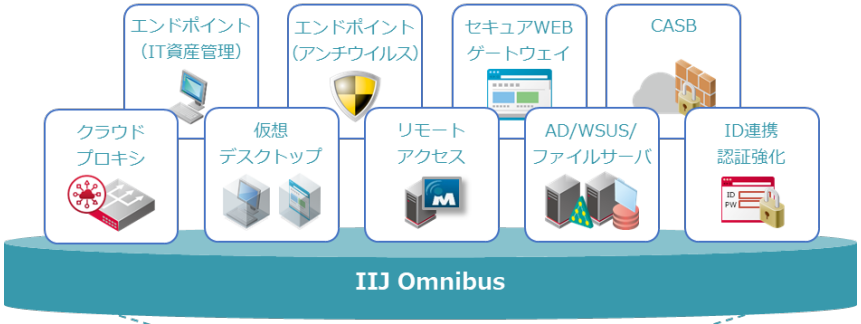
デジタルワークプレース

デジタルを利用し、場所や時間にとらわれない、多様なワークスタイルが可能な世界観。

実現するサービス

IIJ Omnibus

デジタルワークプレースの基盤に必要な機能をクラウドサービスでご提供。



ベースとなる概念モデル

ゼロトラスト、SASE

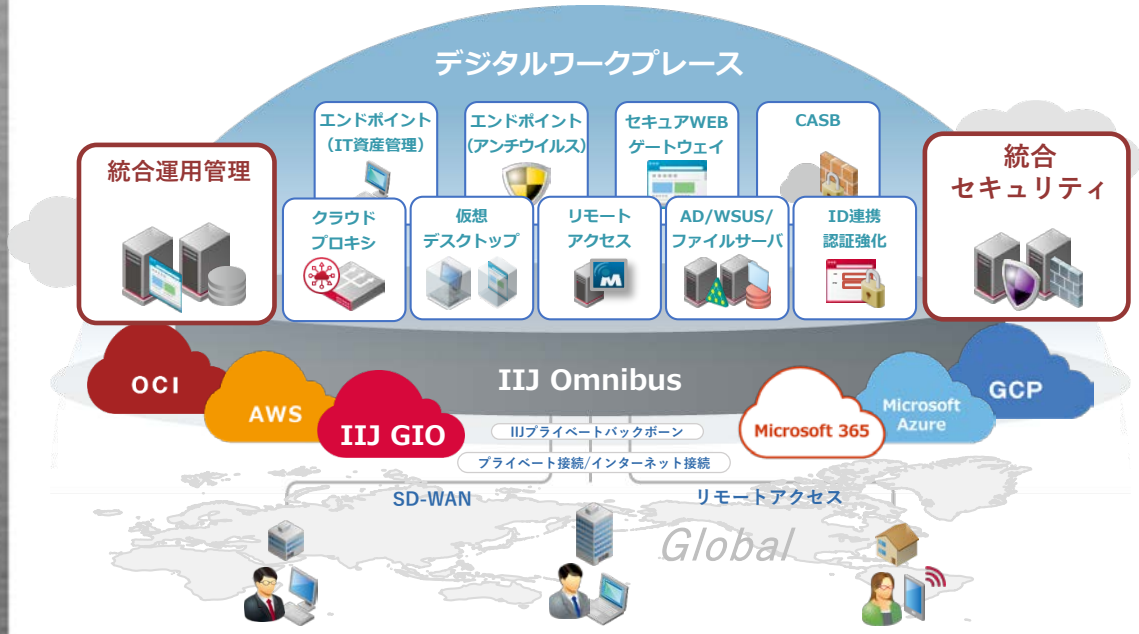
「ネットワークサービスとセキュリティサービス」が統合化・集約化されクラウド上で提供される。

境界型防御だけでは安全ではなく、すべてのアクセス元・ネットワークを信頼しない前提の構成。

4. 新しいデジタルワークプレース

◆ 新しいデジタルワークプレースを実現する4つの要素

快適なテレワーク環境	安心安全なテレワーク環境	業務管理	高い生産性
あらゆる場所から執務室のような快適なITシステムを利用可能な環境	マルウェアなどインターネット利用におけるあらゆる脅威の排除	勤務状況や業務状況の見える化	総合的なデータ分析による生産性の向上



IIJ Omnibus

1. 快適なクラウド利用環境
2. 快適なネットワーク環境
3. 快適なオフィスIT環境

4. グローバル分散
- グローバルにおいても快適な業務遂行

5. 統合運用管理
- 複雑化したITシステムを統合的に管理
- 早期にボトルネック個所や不具合個所の把握と対処

6. 統合セキュリティ
- 単一のセキュリティ機能に頼らず、複合的なセキュリティ
- インターネットの脅威に対してゼロトラストモデルによるトータルセキュリティ

Ongoing Innovation

IIJ Internet Initiative Japan

ご清聴ありがとうございました。