課題発掘セッション

ざんねんなエンタープライズ・アイデンティティ

～あなたの会社のゼロトラストは大丈夫？～

2021年11月26日
デジタルアイデンティティWG　渥美淳一
https://www.jnsa.org/active/std_idm.html

アジェンダ

【前半】アイデンティティの "外側" の課題発掘（20分）

1. Re：ゼロトラストとは
2. アイデンティティが「無いゼロトラスト」と「あるゼロトラスト」
3. 外側（アイデンティティを使うソリューション）からみた課題を整理したい

【後半】アイデンティティの "内側" の課題発掘（20分）

1. ゼロトラストにおけるアイデンティティって？
2. アイデンティティって具体的に何を考えれば良い？
3. アイデンティティの難しさ
4. アイデンティティの課題を体系的に整理したい

前半担当

渥美 淳一

JNSA デジタルアイデンティティWGメンバー

ネットワンシステムズ株式会社 ビジネス開発本部 第１応用技術部 セキュリティチーム

プロフィール

オンプレミスとクラウドを結ぶセキュリティアーキテクト。
アイデンティティ中心のゼロトラスト実装に注目している。

保有資格

- Microsoft Azure Solutions Architect Expert
- Microsoft Azure Security Engineer Associate
- AWS Certified Security - Specialty

記事・コラム

Software Design 2020年11月号 特集記事
https://gihyo.jp/magazine/SD/archive/2020/202011

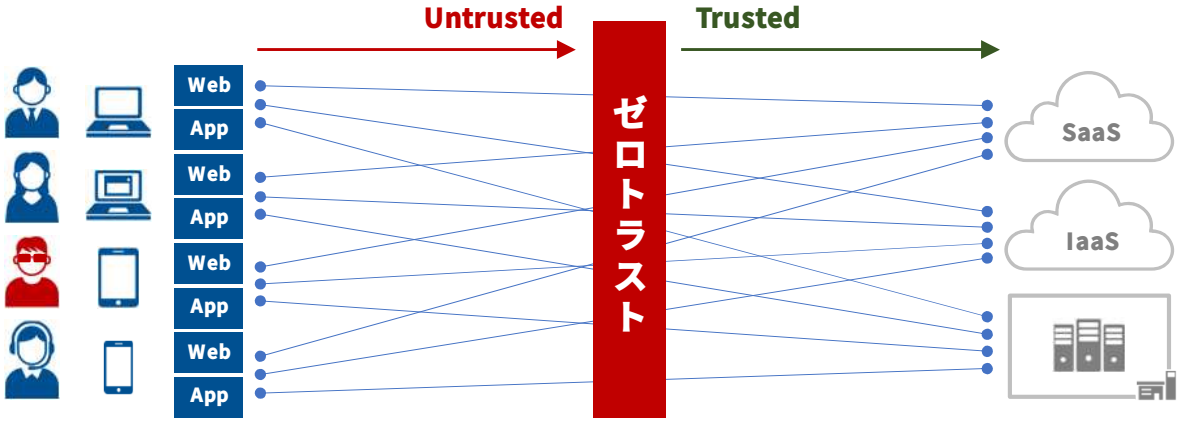
クラウド時代の「認証」再考論
https://techtarget.itmedia.co.jp/tt/series/3244/

統合 ID 管理
https://www.netone.co.jp/knowledge-center/blog-column/20210729-1/

パスワードレス認証
https://www.netone.co.jp/knowledge-center/blog-column/20210817-1/

Re：ゼロトラストとは

コロナ禍。クラウド隆盛。働き方の多様化。デジタル化と自動化。企業間コラボレーション。
ビジネスにおいて境界が曖昧となり、「場所で信頼する」という境界防御が通用しません。
では、何をもって「Untrusted」を「Trusted」と見なすべきでしょうか？



Re：ゼロトラストとは

・便利なモノをどう使うか？はヒト次第
・境界の外にも中にも不正するヒトはいる

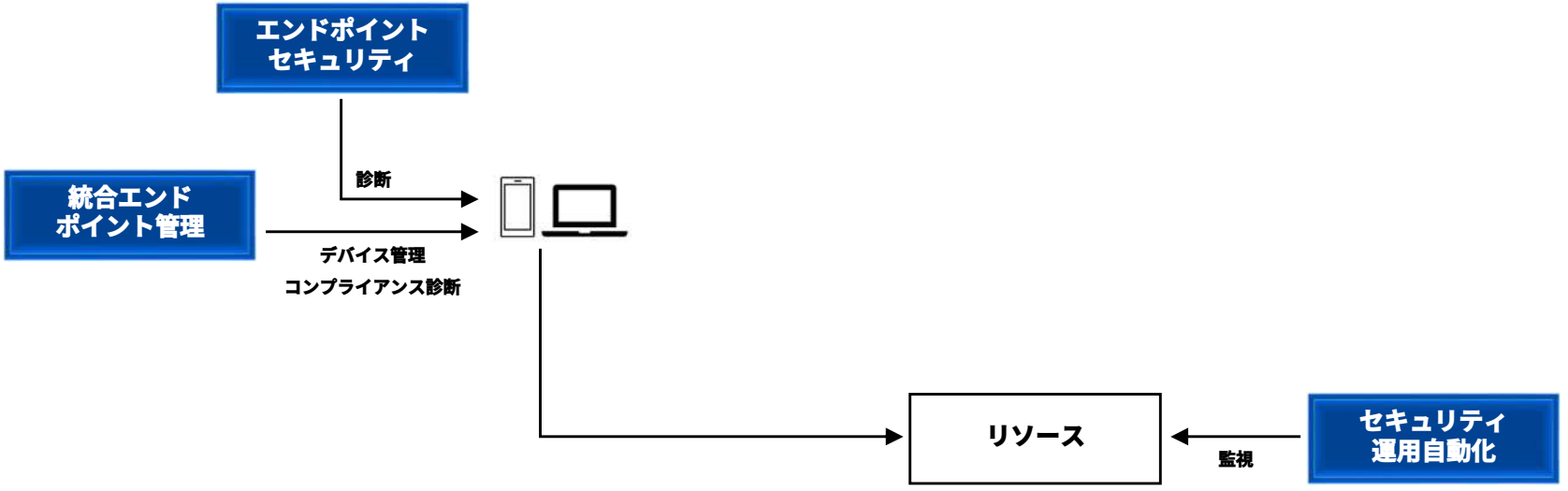
セキュリティの「戦略」です。企業や組織によって最適解（守るべきリソース）は異なります。

ゼロトラスト例

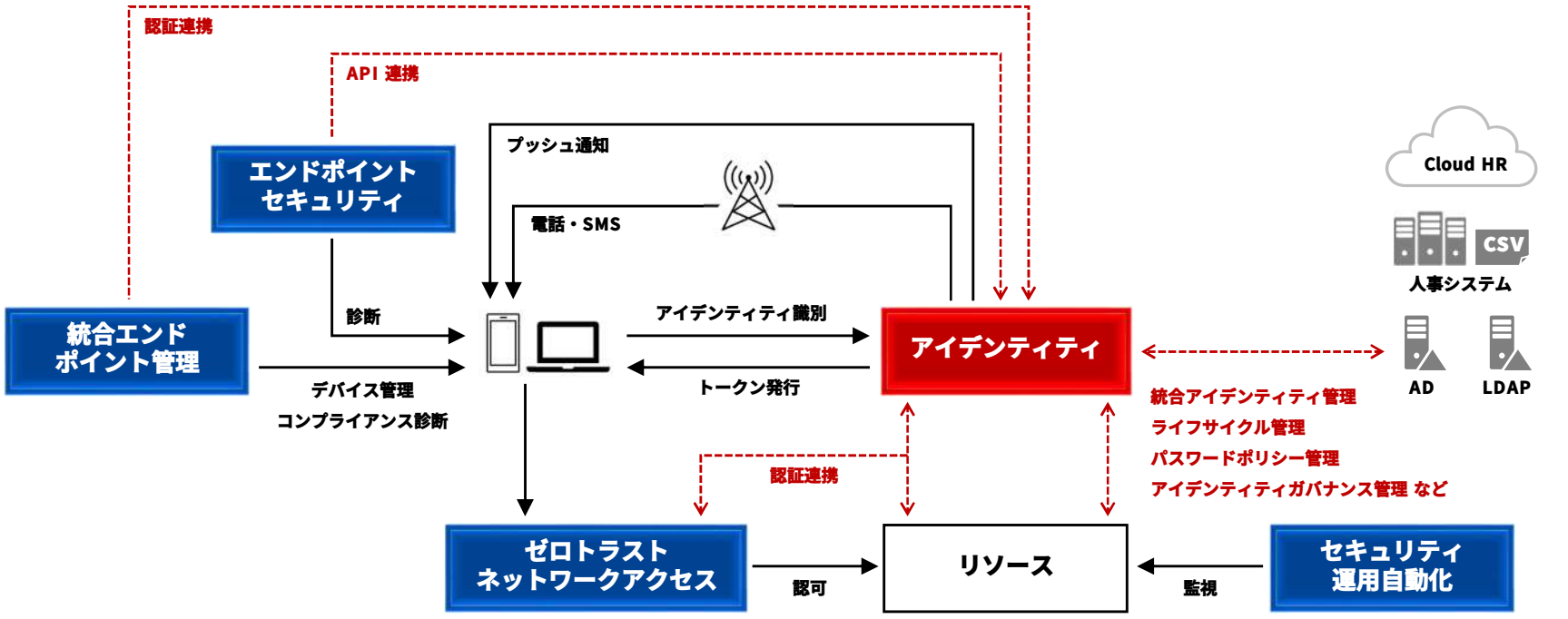
戦略	戦術	武器
米国国立標準技術研究所 (NIST) SP 800-207	Software Defined Perimeter	アイデンティティ管理
Forrester Zero Trust eXtended	Identity Aware Proxy	統合エンドポイント管理
Gartner Zero Trust Architecture	Secure Access Service Edge	エンドポイントセキュリティ
		セキュリティ運用自動化

＋ ＋

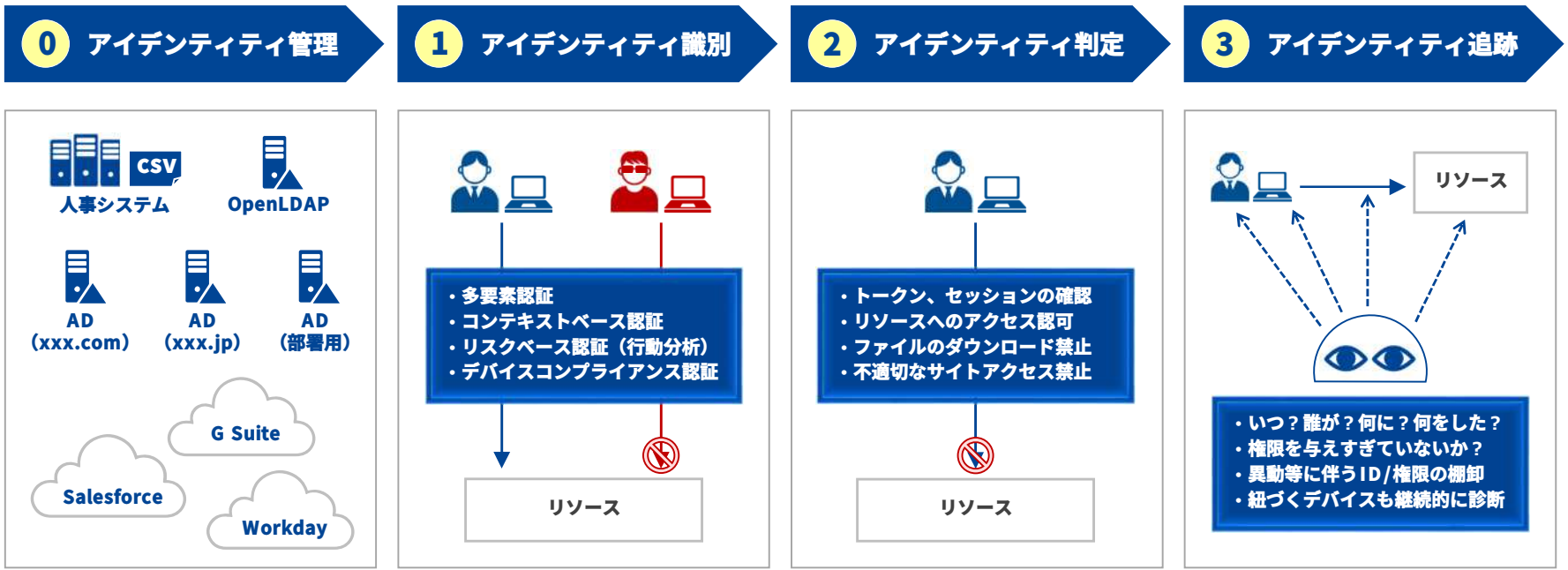
アイデンティティの無いゼロトラスト例



アイデンティティのあるゼロトラスト例

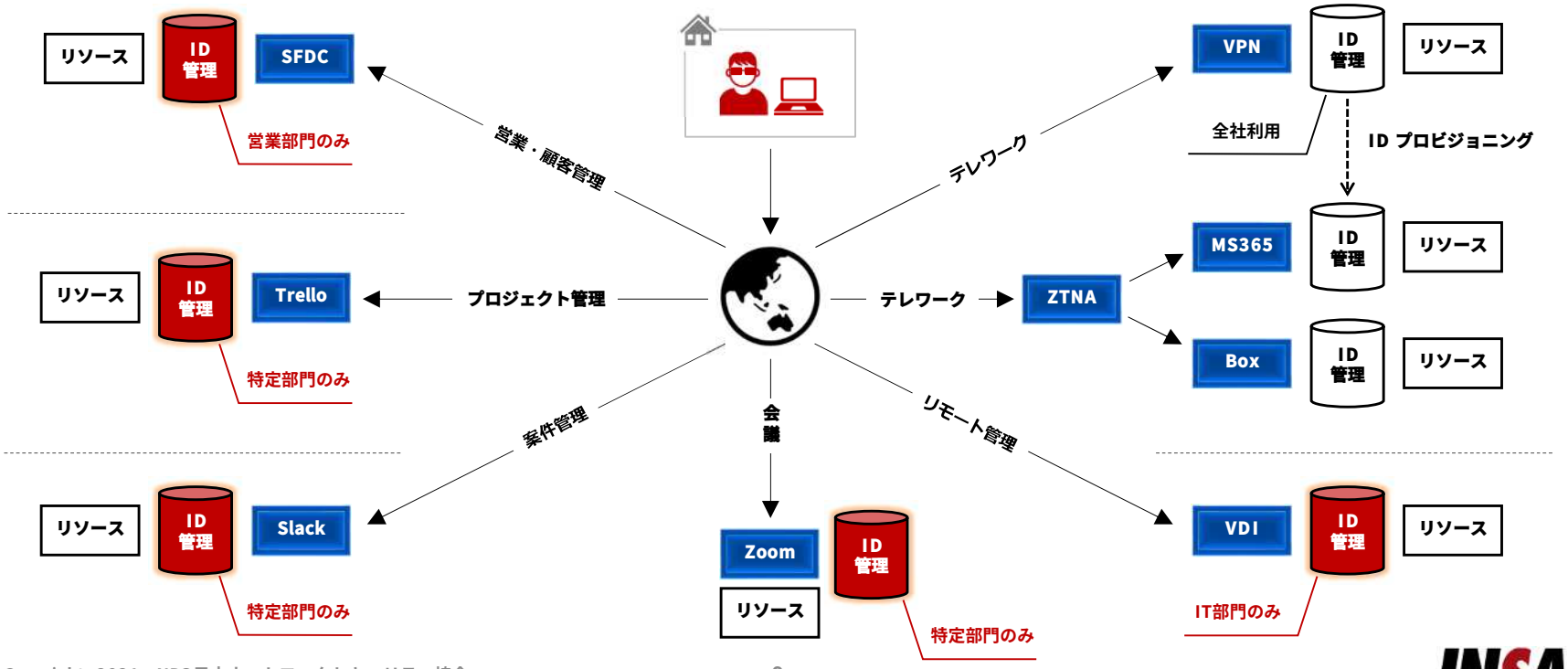


ゼロトラストに必要なアイデンティティ



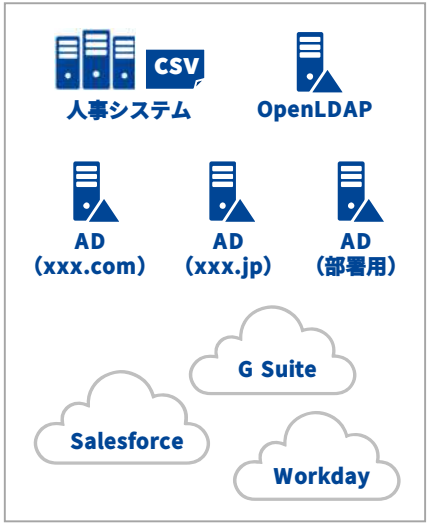
ゼロトラストで意識されがちなアイデンティティ

内部不正を追跡できない



ゼロトラストに必要なアイデンティティ

0 アイデンティティ管理



統合

重要

- 便利なモノをどう使うか？はヒト次第
- 境界の外にも中にも不正するヒトはいる

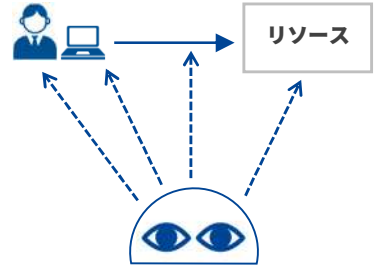
外部不正対策

1 アイデンティティ識別

2 アイデンティティ判定

内部不正対策

3 アイデンティティ追跡



- いつ？誰が？何に？何をした？
- 権限を与えすぎていないか？
- 異動等に伴うID/権限の棚卸
- 紐づくデバイスも継続的に診断

内部不正対策

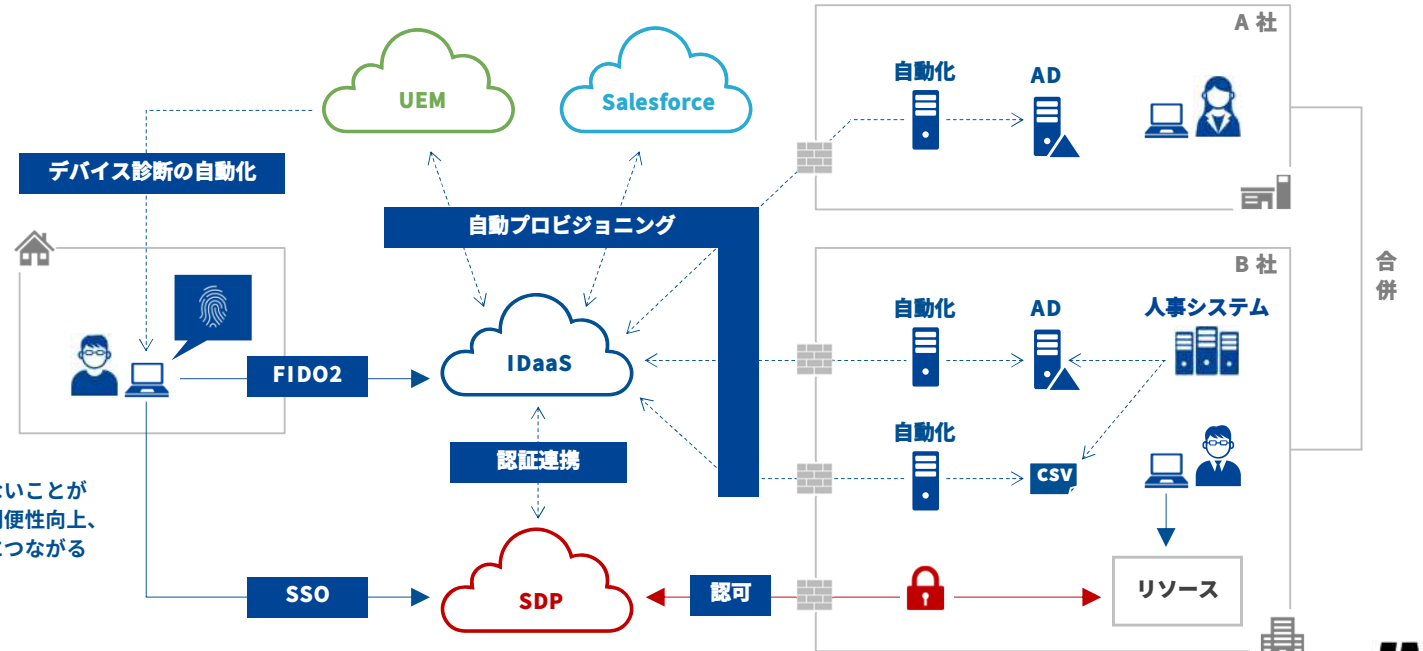
JNSA

ゼロトラストの課題発掘

- アイデンティティの運用負荷をどうしますか？
- 内部でもアイデンティティが必要ですか？
- 特権を持つアイデンティティは大丈夫ですか？
- 多要素認証したアイデンティティは安心ですか？
- ゼロトラストを実装すれば安心ですか？

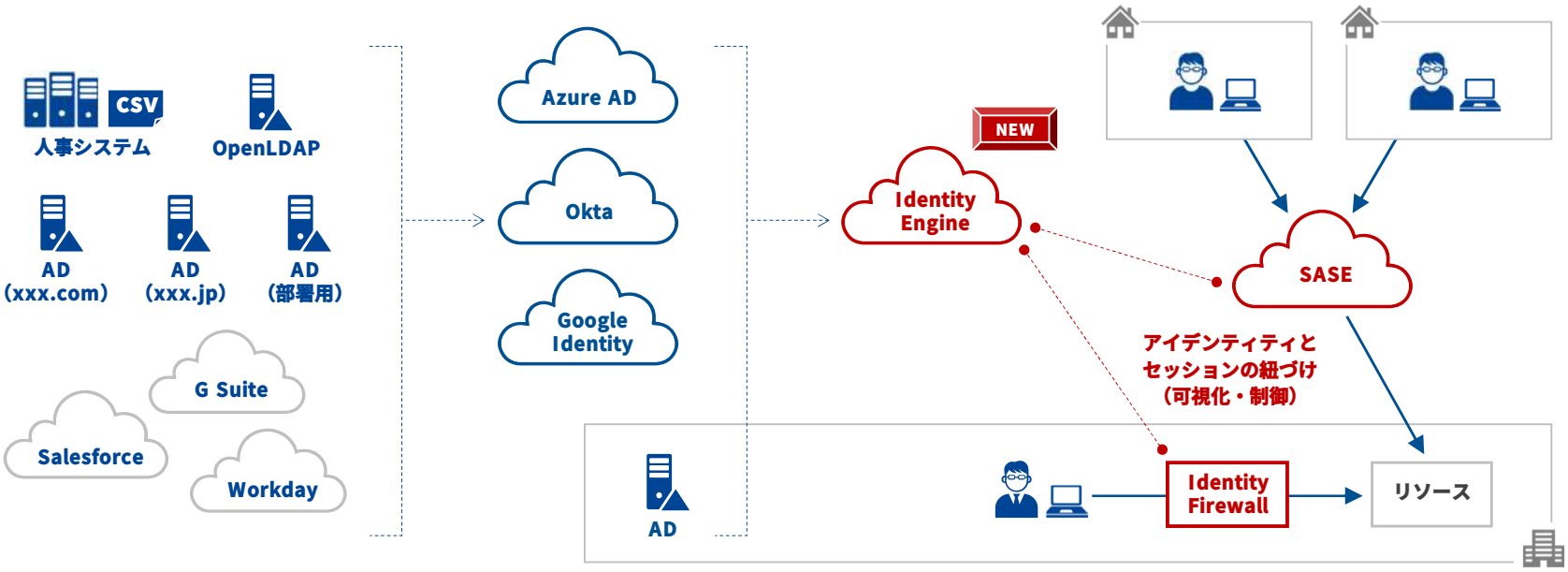
アイデンティティの運用負荷をどうしますか？

セキュリティ強化と同時に、自動化・省力化による管理者とユーザーの負荷軽減の検討が望ましい。



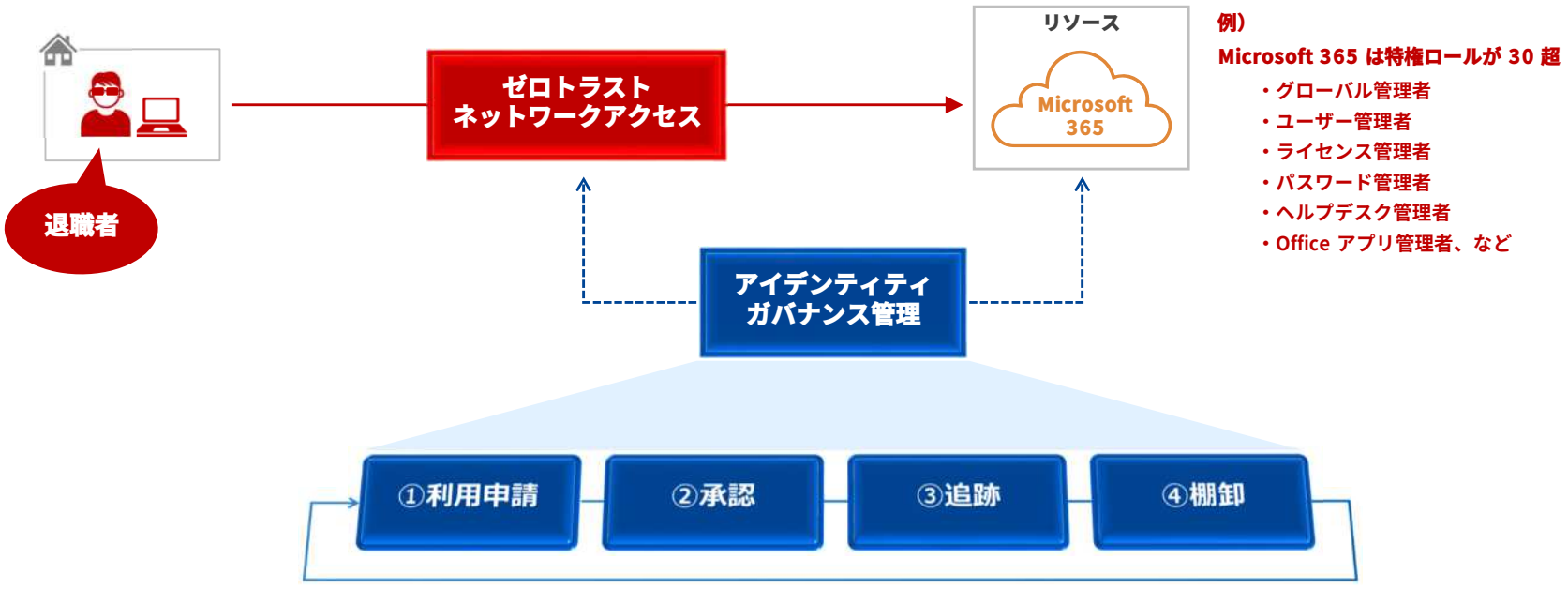
内部でもアイデンティティが必要ですか？

内部不正もゼロトラスト対象。内へも外へも同一アイデンティティベースのセキュリティを一貫して提供。



特権を持つアイデンティティは大丈夫ですか？

特権を自由に使わせることが「内部犯行」「不注意によるトラブル」につながる。攻撃者にも狙われやすい。



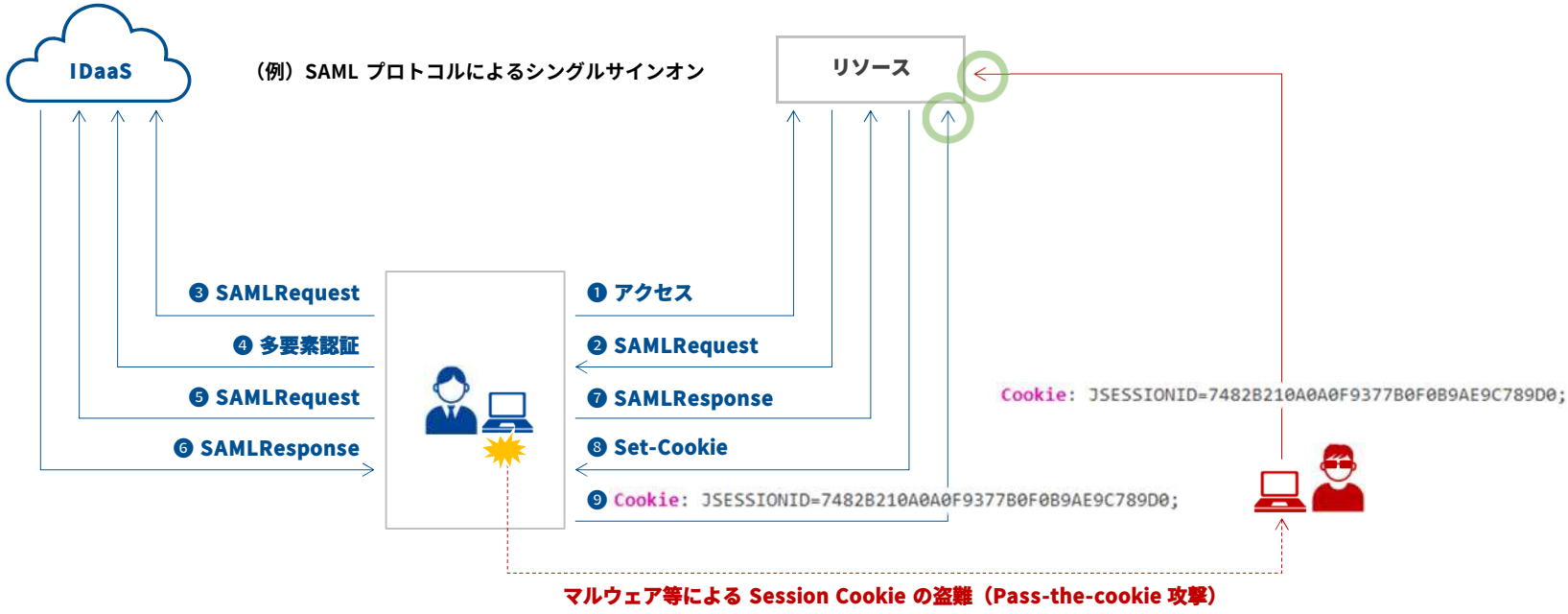
例）

Microsoft 365 は特権ロールが 30 超

- グローバル管理者
- ユーザー管理者
- ライセンス管理者
- パスワード管理者
- ヘルプデスク管理者
- Office アプリ管理者、など

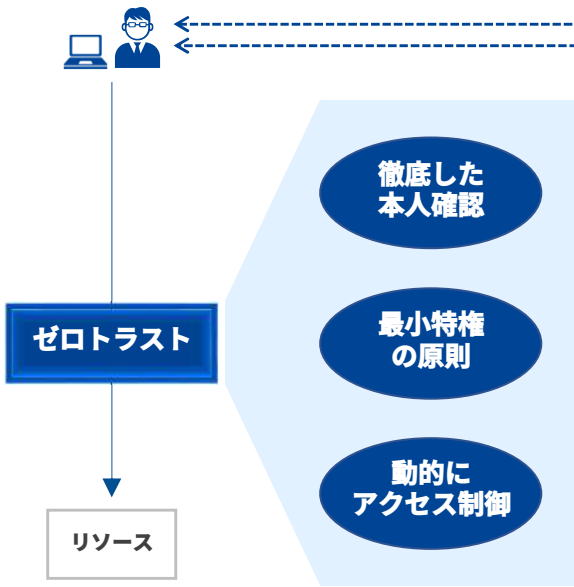
多要素認証したアイデンティティは安心ですか？

盗まれた Cookie が特権ユーザーのものだったら？ 多要素認証とシングルサインオンで万事解決ではない。



ゼロトラストを実装すれば安心ですか？

アイデンティティの持ち主（従業員等）の「教育」「セキュリティ意識改革」もゼロトラストの本質の一つ。



RBAC（ロール）

ビジネスロールを IT ロールにマッピング

ABAC（アトリビュート）

部署などのユーザー属性による制御

CBAC（コンテキスト）

デバイス信頼性、振る舞い等による制御

PBAC（ポリシー）

よりきめ細やかな ABAC / CBAC

あるべき姿の教育・意識改革

- 内部統制強化とアイデンティティ
- IT セキュリティとアイデンティティ
- クラウドにおけるアイデンティティ
- リスクのあるアイデンティティとは
- アイデンティティの正当性担保
- アイデンティティと権限の棚卸し
- アイデンティティ関連ログの利活用
- ロール等の管理のベストプラクティス
- ロール等の管理の大変さ、失敗例

前半まとめ

- ゼロトラスト実装へのアプローチは「守るべきリソース」によって変わる
- それでもアイデンティティは、ゼロトラスト実装に「なくてはならない」
- アイデンティティと権限を確認し、あらゆるアクセスを動的に制御、常に監視
- 多要素認証やシングルサインオンは重要だが、その後（セッション）への配慮も必要
- 体系的に整理されたアイデンティティが、ゼロトラストの「礎」となる

では、アイデンティティを整理するとは？ 何が良くなる？ 【後半へ】