The Border

自由な働き方には見える化+αを！

～クラウド時代の必修課題～



CLARA ONLINE

株式会社クララオンライン　SB部
竹西 宏真

本セッションの構成

- Part 1
  - クララオンラインセッション
- Part 2
  - Netskope Japan 様 セッション
- ゼロトラストへの移行・導入
- まとめ

© 2020 CLARA ONLINE, Inc.

ゼロトラスト実現への第一歩 ~おさらい~

© 2020 CLARA ONLINE, Inc.

ゼロトラスト

The Border

ゼロトラストとは

「暗黙的に信頼できるものは何もなく、継続的にリソースを評価し信用をゼロから積み上げていくという新しいセキュリティの考え方」です。

© 2020 CLARA ONLINE, Inc.

基本的な設計方針

The Border

ゼロトラスト
7つの基本的原則

①すべてのデータソースとコンピューティングサービスは、リソースとみなされます。

②ネットワークの場所に関係なく、すべての通信は安全に保護されます。

③個々の企業リソースへのアクセスは、**セッションごとに許可**される。

④リソースへのアクセスは**クライアントID**や**アプリケーション/サービス**、**要求する資産の観察可能な状態**および**その他属性(デバイスの特性やユーザの行動履歴など)**を含む**動的ポリシーによって決定**されます。

⑤企業は、所有(関連)するデバイスを可能な限り最も安全な状態であると保証するため継続的に監視します。

⑥すべての**リソースに対する認証と認可は動的に行われ**、アクセスが許可される前に厳格に実施されます。

⑦資産、ネットワークインフラとコミュニケーションの現在の状態に関する情報を可能な限り収集し、セキュリティ体制の強化に利用する。

出典:「NIST.SP.800-207」意訳

ゼロトラスト実現への第一歩 ~ID管理~

The Border



クラウド × ID管理/認証基盤 ＝ IDaaS

© 2020 CLARA ONLINE, Inc.

ゼロトラスト実現への必修課題
~次世代SWG~

© 2020 CLARA ONLINE, Inc.

通信の見える化

The Border

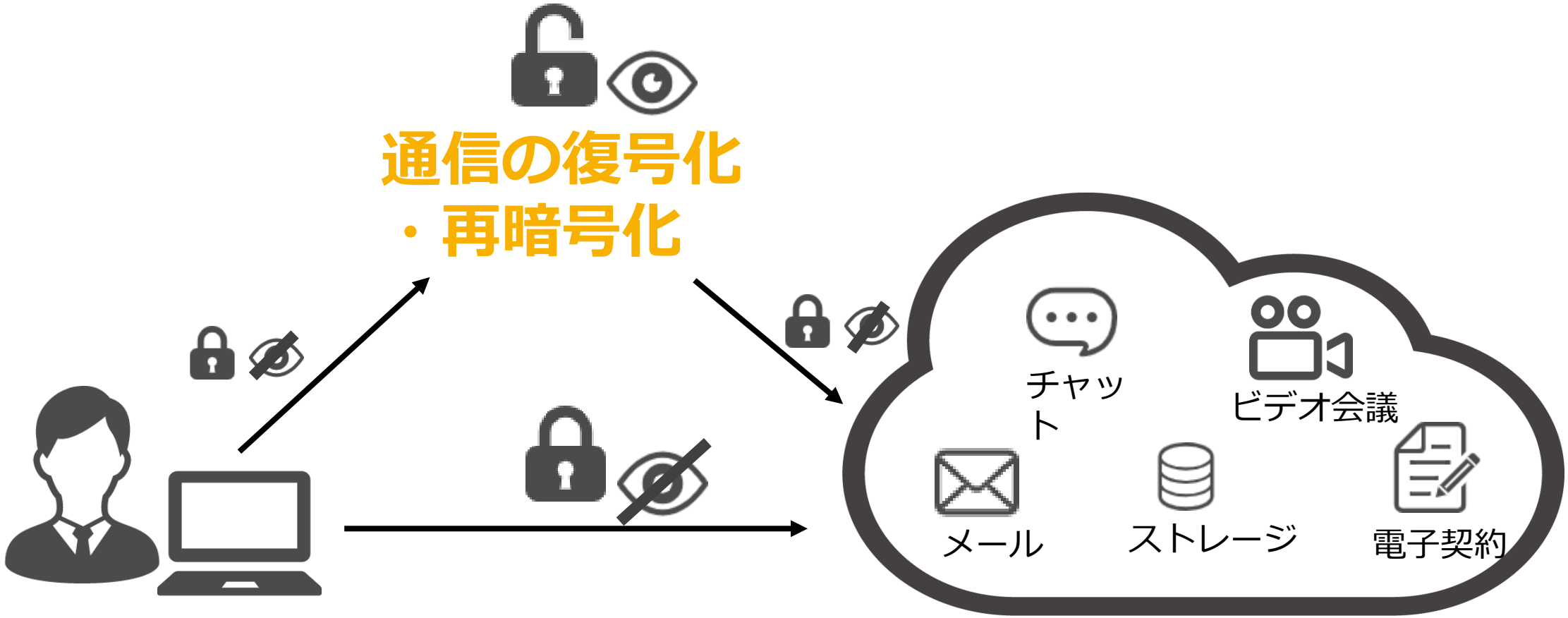
「誰が・誰に・いつ・どこで・何を」

ID　　通信内容

© 2020 CLARA ONLINE, Inc.

暗号化通信の見える化のために

The Border



© 2020 CLARA ONLINE, Inc.

通信の見える化メリット

- カテゴリ・コンテンツ把握
- シャドーITの把握
- マルウェアの検知
- 脅威検知
- 機密情報の流出検知

etc…

© 2020 CLARA ONLINE, Inc.

ポリシーによるリアルタイムアクセスコントロール

The Border

④リソースへのアクセスはクライアントIDやアプリケーション/サービス、要求する資産の観察可能な状態およびその他属性(デバイスの特性やユーザの行動履歴など)を含む動的ポリシーによって決定されます。

⑥すべてのリソースに対する認証と認可は動的に行われ、アクセスが許可される前に厳格に実施されます。

- 信用スコア
- ネットワークエージェント

手動でもきめ細かく・柔軟なポリシー設定を

© 2020 CLARA ONLINE, Inc.

SWG/CASB

通信の見える化

＋

ポリシーによるリアルタイムアクセスコントロール

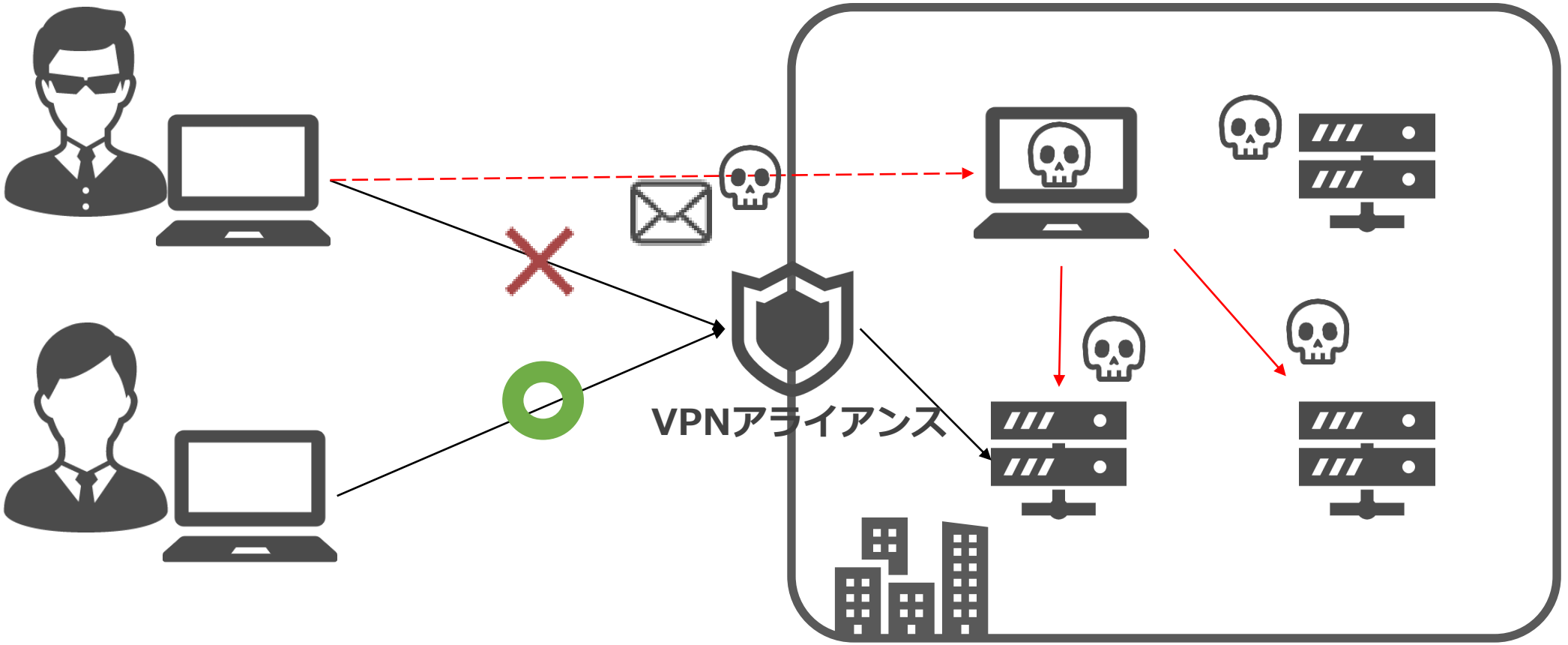
＝

SWG/CASB

© 2020 CLARA ONLINE, Inc.

VPNと問題点

境界型セキュリティモデルの危殆化
VPNアライアンス増強が難しい。。。

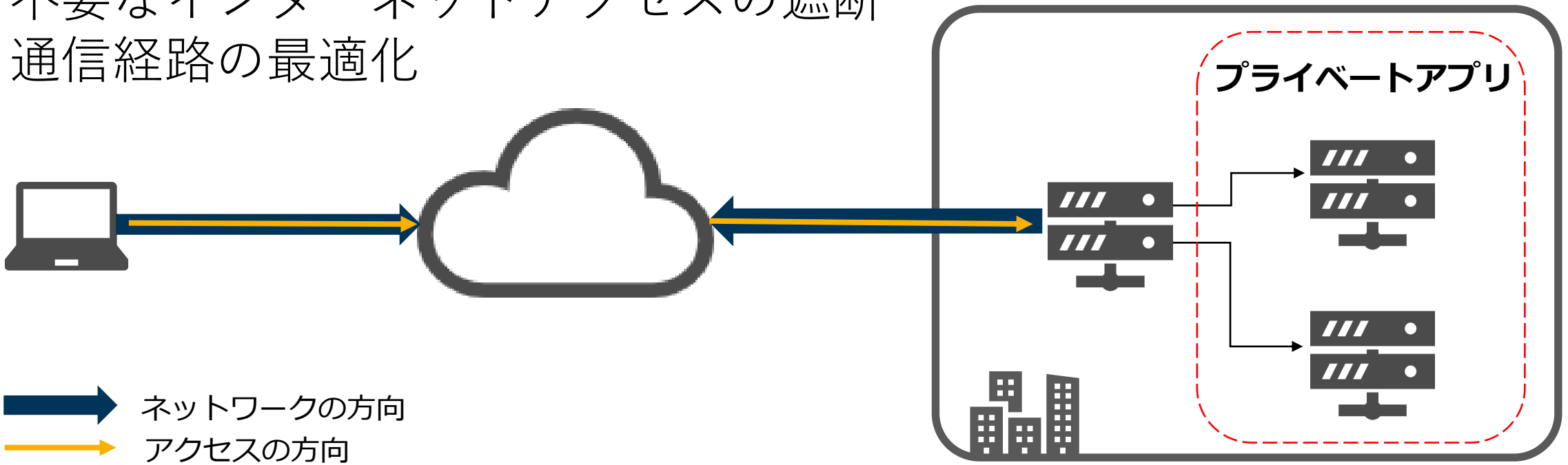


© 2020 CLARA ONLINE, Inc.

ゼロトラストネットワーク(プライベート)アクセス

The Border

リソース単位のアクセス許可
クラウドベースで柔軟に拡張が可能
不要なインターネットアクセスの遮断
通信経路の最適化



© 2020 CLARA ONLINE, Inc.

次世代SWG Netskope

The Border

~手動でもきめ細かく・柔軟なポリシー設定と拡張性の高いZTNAソリューションを~

- わかりやすいGUI
- 詳細なアクセスログ/分析
- リッチなCASB/SWG機能
- 迅速なリモートワーク環境構築

  etc…



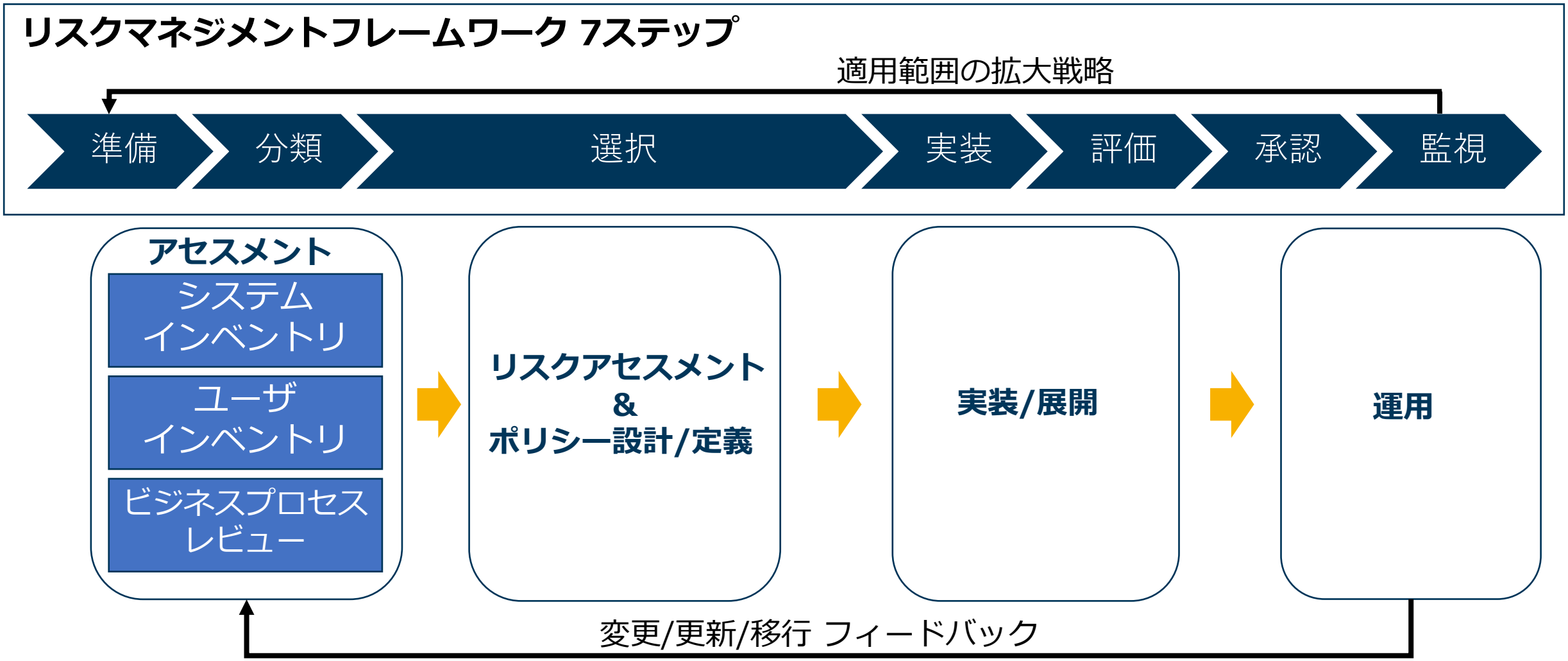
© 2020 CLARA ONLINE, Inc.

ゼロトラスト移行・導入

© 2020 CLARA ONLINE, Inc.

ゼロトラスト移行・導入ステップ

The Border



ゼロトラストアーキテクチャ デプロイメント サイクル

出典:「NIST.SP.800-207」意訳

© 2020 CLARA ONLINE, Inc.

ゼロトラスト移行・導入の三本柱

The Border

ゴール設定

継続的な監視と改善

コミュニケーション

© 2020 CLARA ONLINE, Inc.

サンプル: BeyondCorp への移行戦略

The Border

1. 職務、ワークフロー、場所に基づき、考えられる候補を洗い出す。

2. 非特権ネットワークのシミュレータ(トラフィックモニタ)をロギングモードで稼働させ、99.9%を超えるトラフィックが検証にパスする状態が30 日間にわたって続いたユーザやデバイスを特定する。

3. 99.99%を超えるトラフィックが検証にパスしたユーザとデバイスでは、シミュレータをエンフォースメントモードに切り替える。必要であれば、ユーザはシミュレータをロギングモードに戻すことができる。

4. シミュレータが30日間にわたってエンフォースメントモードで問題なく動作した場合、その事実をデバイスインベントリに記録する。

5. 候補セットへの追加と併せて、シミュレータが30日間にわたってエンフォースメントモードで問題なく動作していることは、そのデバイスを非特権的ネットワークに割り当てても問題がないことを示している。

出典「ゼロトラストネットワーク ―境界防御の限界を超えるためのセキュアなシステム設計」
「BeyondCorp: A New Approach to Enterprise Security」

© 2020 CLARA ONLINE, Inc.

サンプル: BeyondCorp への移行戦略

The Border

1. 職務、ワークフロー、場所に基づき、考えられる候補を洗い出す。

2. 非特権ネットワークのシミュレータ(トラフィックモニタ)をロギングモードで稼働させ、99.9%を超えるトラフィックが検証にパスする状態が30 日間にわたって続いたユーザやデバイスを特定する。

3. 99.99%を超えるトラフィックが検証にパスしたユーザやデバイスのシミュレータをエンフォースメントモードに切り替える。
必要であれば、ユーザはシミュレータをロギングモードに戻すことができる。

4. シミュレータが30日間にわたってエンフォースメントモードで問題なく動作した場合、その事実をデバイスインベントリに記録する。

5. 候補セットへの追加と併せて、シミュレータが30日間にわたってエンフォースメントモードで問題なく動作していることは、そのデバイスを非特権的ネットワークに割り当てても問題がないことを示している。

現状調査と段階的な移行

長期的なロードマップ

出典「ゼロトラストネットワーク ―境界防御の限界を超えるためのセキュアなシステム設計」
「BeyondCorp: A New Approach to Enterprise Security」

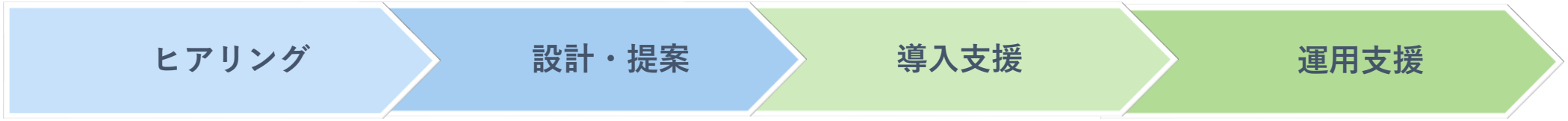
© 2020 CLARA ONLINE, Inc.

Clara WSI Solutionの設計・導入・運用支援

The Border

クララがワークスタイル変革をお手伝いします！

ゼロトラストネットワークの実現に向け、導入のお手伝いをいたします。
お客様の現状のヒアリング、システム構成のご提案、導入支援、運用までトータルサポートさせていただきます。



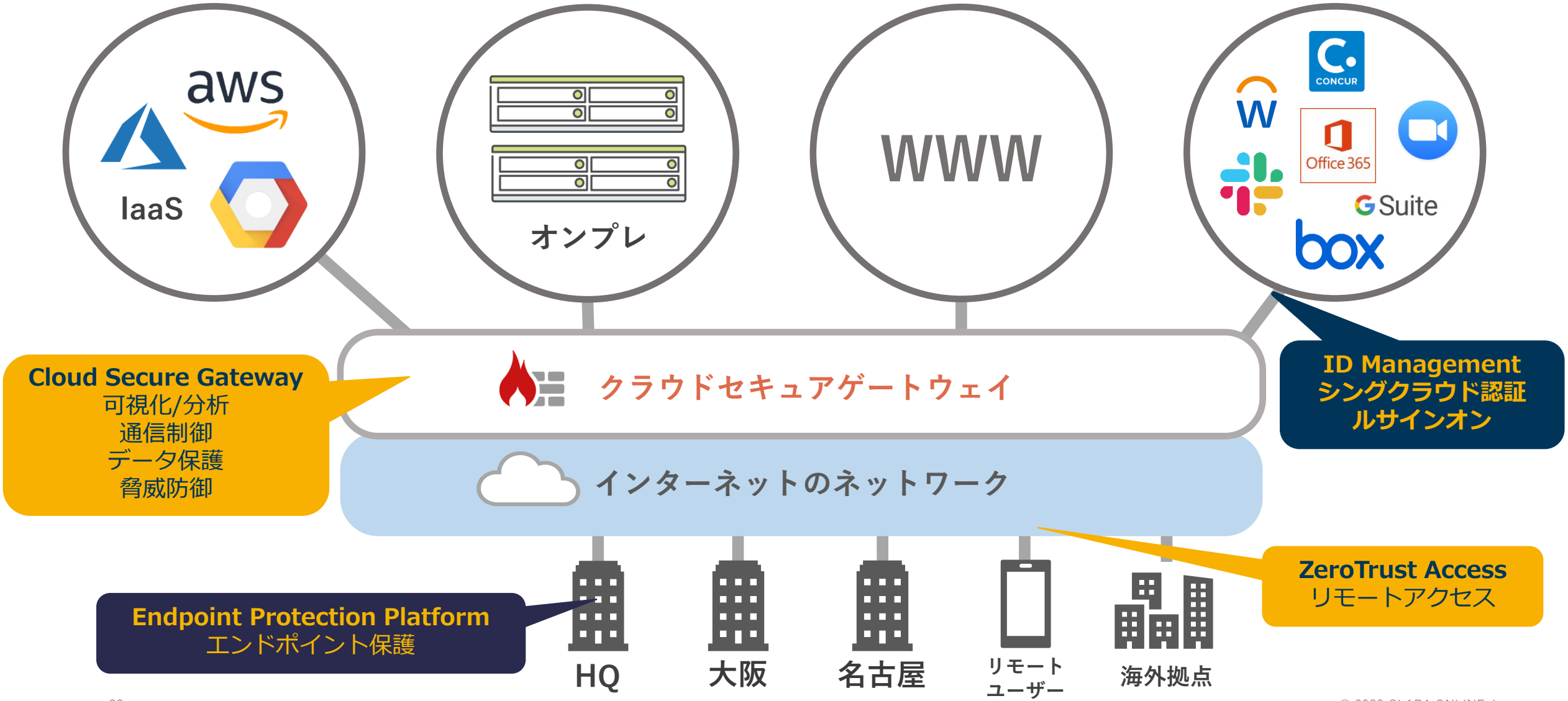
- ヒアリング
  - ・現状のヒアリング
  - ・要件確認
- 設計・提案
  - ・システム構成のご提案
  - ・サービス選定
  - ・ロードマップ策定
- 導入支援
  - ・PoC
  - ・操作方法のレクチャ
  - ・ライセンス提供
- 運用支援
  - ・定例会（定期的な見直し支援）
  - ・問い合わせサポート

https://www.clara.jp/wsi/

© 2020 CLARA ONLINE, Inc.

クララオンラインの描くゼロトラストイメージ

The Border



© 2020 CLARA ONLINE, Inc.

The Border

ゼロトラスト セッション紹介

13:40-14:20　「いつでも」「どこでも」「セキュア」を実現するITの新常識

14:20-15:00　まずID管理からはじめよ！～ゼロトラスト実現の第一歩～

15:10-15:50　自由な働き方には見える化+αを！～クラウド時代の必修課題～

16:00-16:40　クララオンラインの自社IT戦略とエンドポイント入れ替え実録

16:20-17:00　DXとこれからの働き方(Special対談)



CLARA ONLINE

© 2020 CLARA ONLINE, Inc.

CLARA ONLINE

The Border

ご視聴ありがとうございました

