macnica networks

コロナ後に描くセキュリティのあり方

2020年11月27日

マクニカネットワークス株式会社
第1技術統括部セキュリティサービス室
勅使河原　猛

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

本日のセッションについて

- With コロナ：
  - リモートワーク可能な状態の構築

より安全な

より効率的な

- After コロナ：
  - デジタルトランスフォーメーション検討を開始
    - 従来の働き方に戻すのではなく、新しい形態への適用・促進
    - 新たな経済活動に向けたITの積極活用を検討

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

アジェンダ

1. DXに求められるインフラとセキュリティについて
   - ①境界外の端末のセキュリティ
   - ②パブリッククラウドのセキュリティ
   - ③潜在的なアクセス方法の課題
2. ゼロトラストにおけるエンドポイントの重要性について
3. まとめ

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

DX推進に必要なもの・こと

一方で・・・

＜燃料＞が漏れていたら、
そもそもそのロケットは飛ぶことができない。

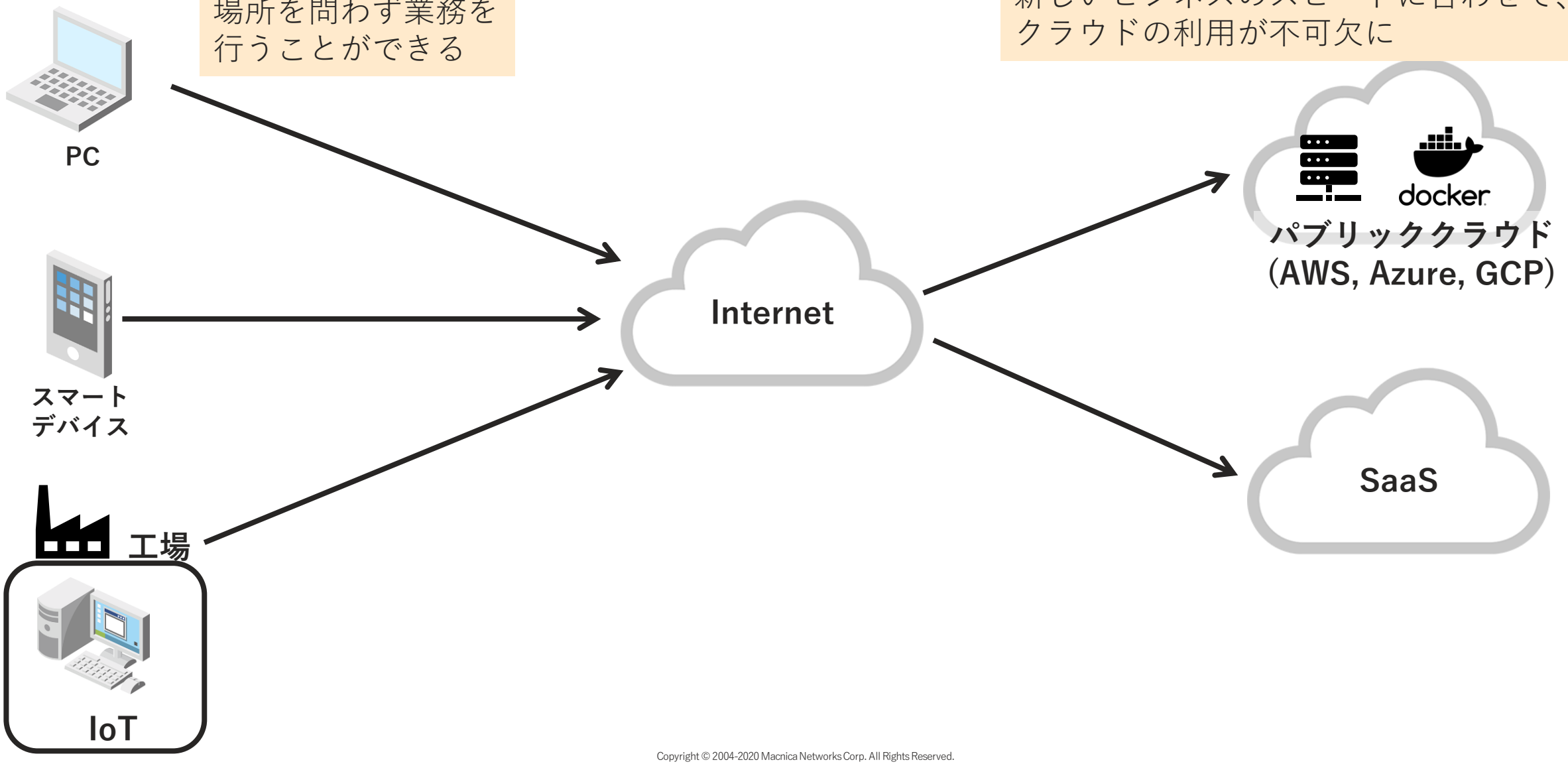
DXを推進するためには、燃料であるデータを
セキュリティで保護しながら進んでいく
必要があります。

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

DX時代のITインフラとは？

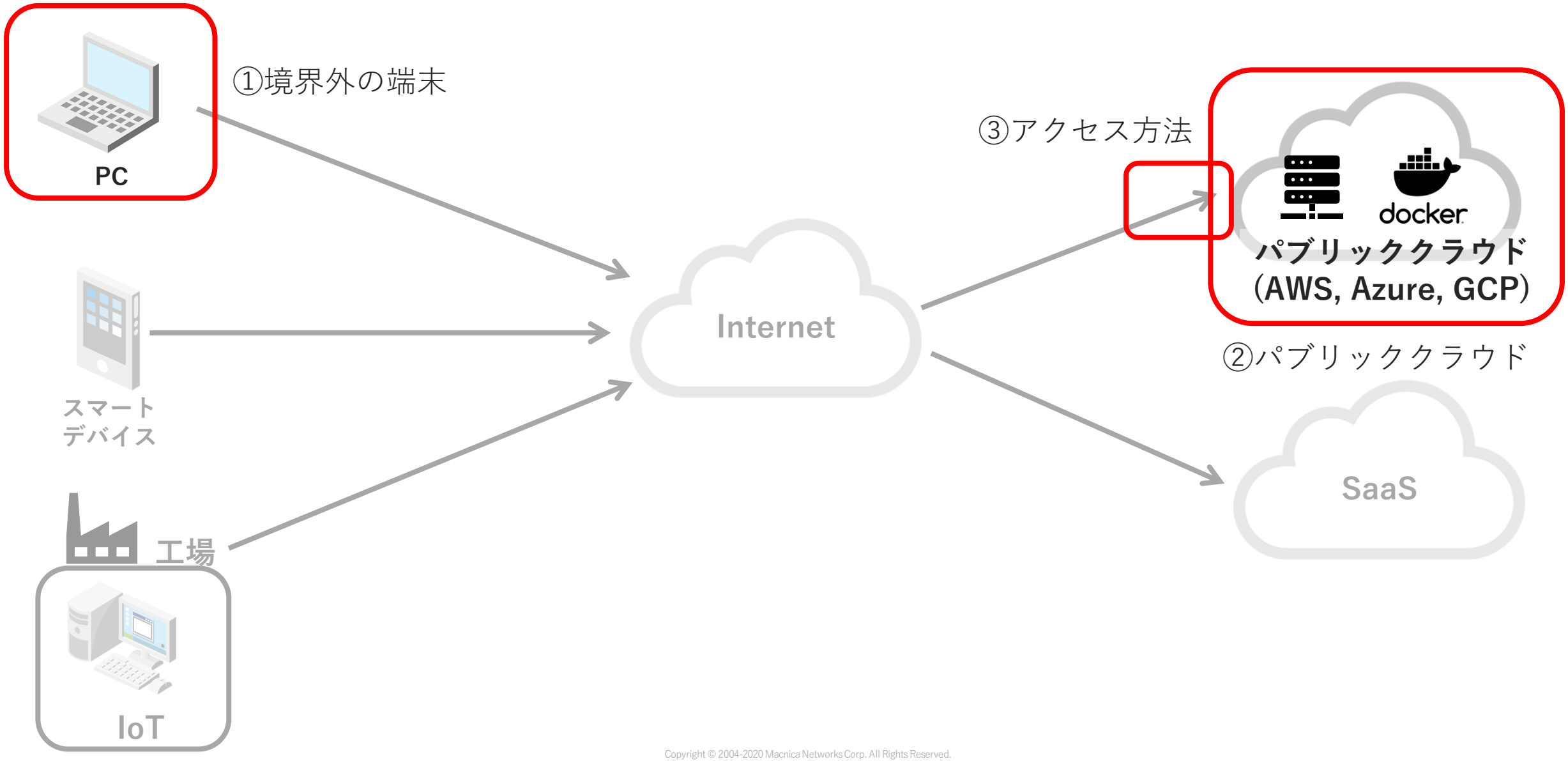
場所を問わず業務を
行うことができる

新しいビジネスのスピードに合わせて、
クラウドの利用が不可欠に



Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

DX時代のITインフラでの３つの注意点とは？

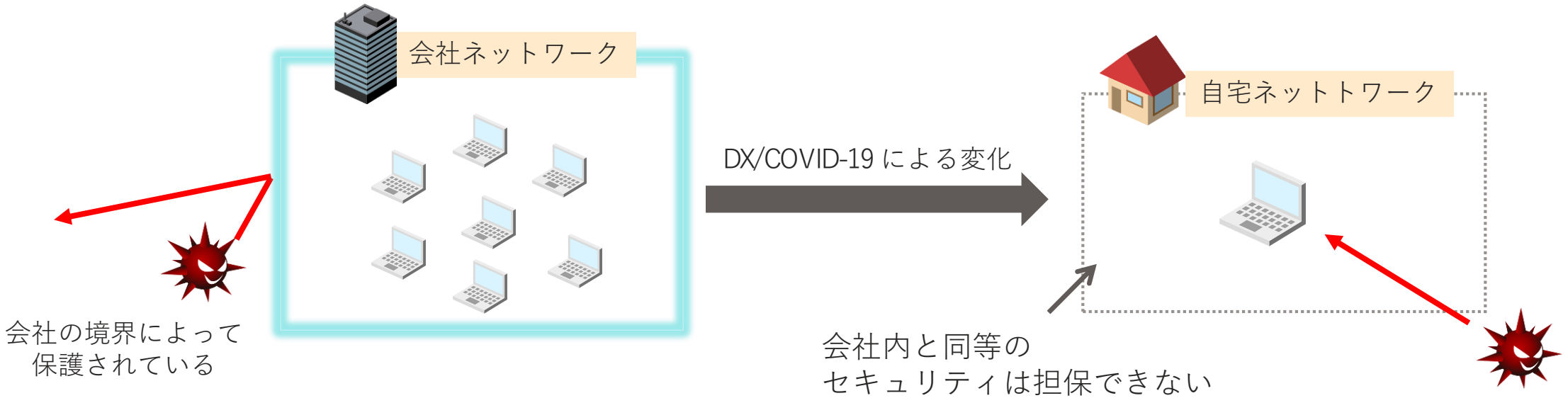


Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

①境界外の端末のセキュリティ

- **今後、働き方はより柔軟さが求められていく**
  - 地方で働く優秀な人材の確保や流出の防止の観点
  - 災害対策などにおける事業継続性の観点

- **必ずしも、会社から業務をするとは限らない**
  - リモートワーク、在宅勤務では、会社ネットワークの保護が効かない
  - 端末側でのセキュリティ担保が必要となる



Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

端末に求められるセキュリティの変化

- 従来のセキュリティ
  - 社内ネットワークを前提として、**ネットワーク境界前提のセキュリティ**
    - 万が一、ネットワークセキュリティで検出できなかった場合の補完な防御能力
  - 社内サーバで管理

アンチウィルス
（AV）

- 新しいセキュリティ
  - 場所を問わないため、**ネットワーク境界を前提としないセキュリティ**
    - 高度な防御、検出と遠隔地からの対応能力
    - 想定外の脅威を想定した記録と能動的な脅威検出
  - クラウドで管理
  - 従来のネットワーク境界でカバーしていた部分も含め要求される
    - ファイヤーウォール機能の制御
    - （通信の制御）
    - 端末・ソフトウェア・ハードウェア（USB）などの管理・制御
    - OSやアプリケーションなどの脆弱性の管理　など

EDR

脅威ハンティング

AVの付随機能
＋α

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

②パブリッククラウドのセキュリティ

- **DXでクラウドの利用は増加傾向**
  - 不確実な時代に、柔軟かつスピーディーにデジタルをフル活用する必要がある
  - スケーラビリティ、展開の容易性からクラウドの利用は必須

- 一方、パブリッククラウド（AWSなど）へのサイバー攻撃は増加傾向
  - 展開や規模が大きくなることで、組織の想定以上の運用の複雑さが発生
  - 従来のオンプレミスで実現できていたようなアクセス管理や特権管理などの基本的な部分に問題が発生している

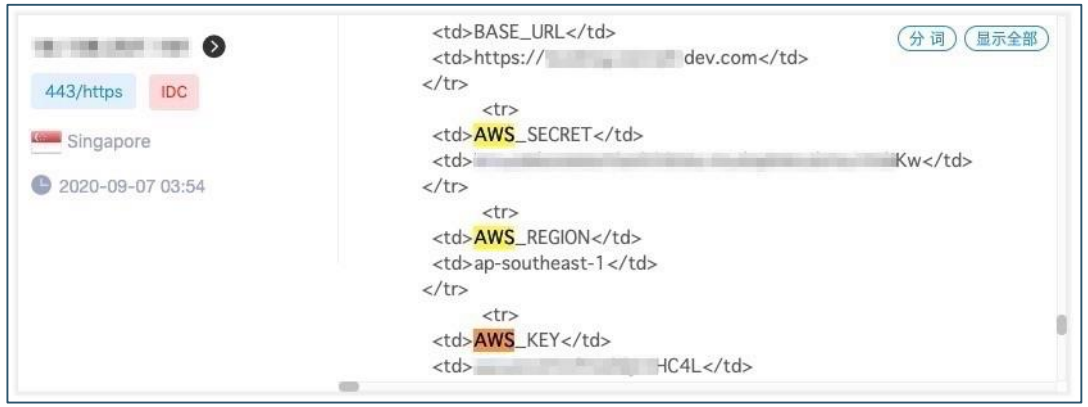
  - セキュリティベンダーによるインシデント調査レポートで共通のメッセージ

  1) CrowdStrike Services Cyber Frontlines Report
  2) FireEye M-Trend
  3) Verizon Data Breach Investigation Report

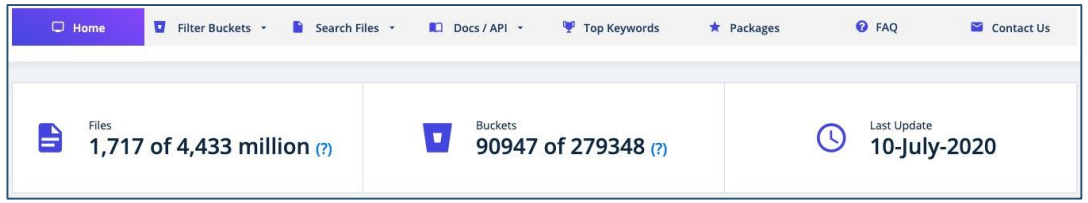
Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

パブリッククラウドへの攻撃可能性

- 検索エンジンを活用することで安全ではないクラウド利用を確認することができる



検索サービスにインデックスされている
AWSのアクセスキー

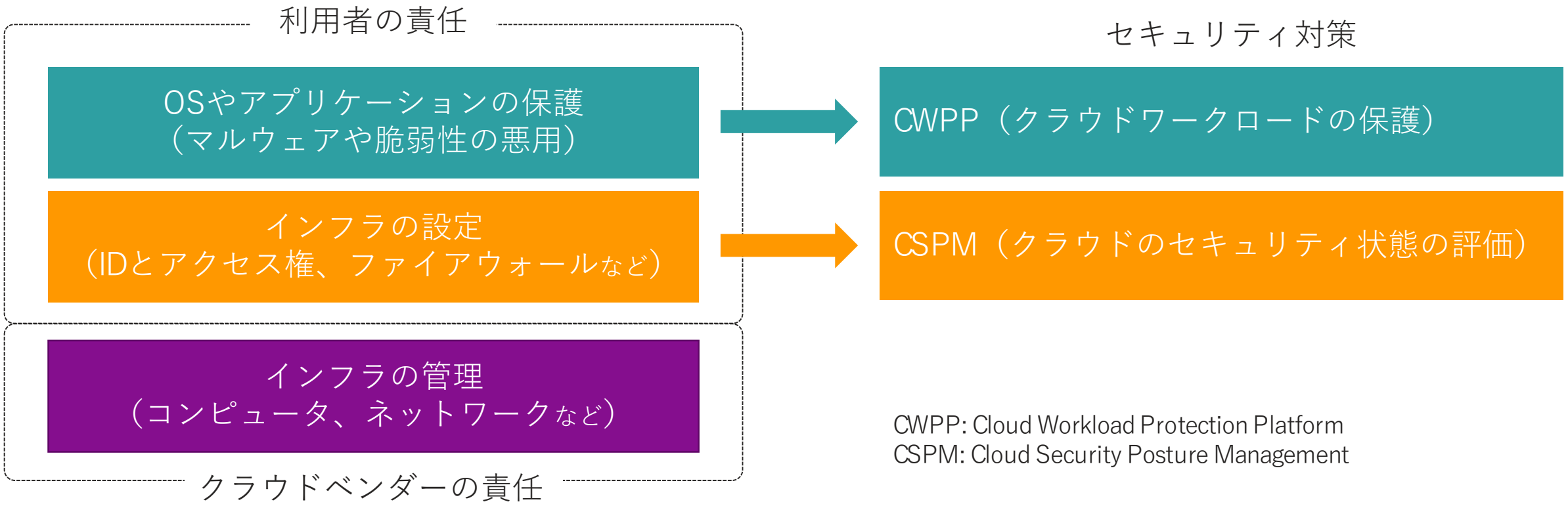


公開されているAWS S3バケットの検索サイト
（意図的に公開しているケースも含む）

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

必要なセキュリティ対策

- クラウドは機能が追加され、利用状況も変化していき、運用が煩雑となる
  継続的にリスクを生み出す設定や脅威からクラウドを保護していく必要がある
- 複数のクラウド基盤を利用している場合は、統合して監視できることが運用の観点から
  望ましい

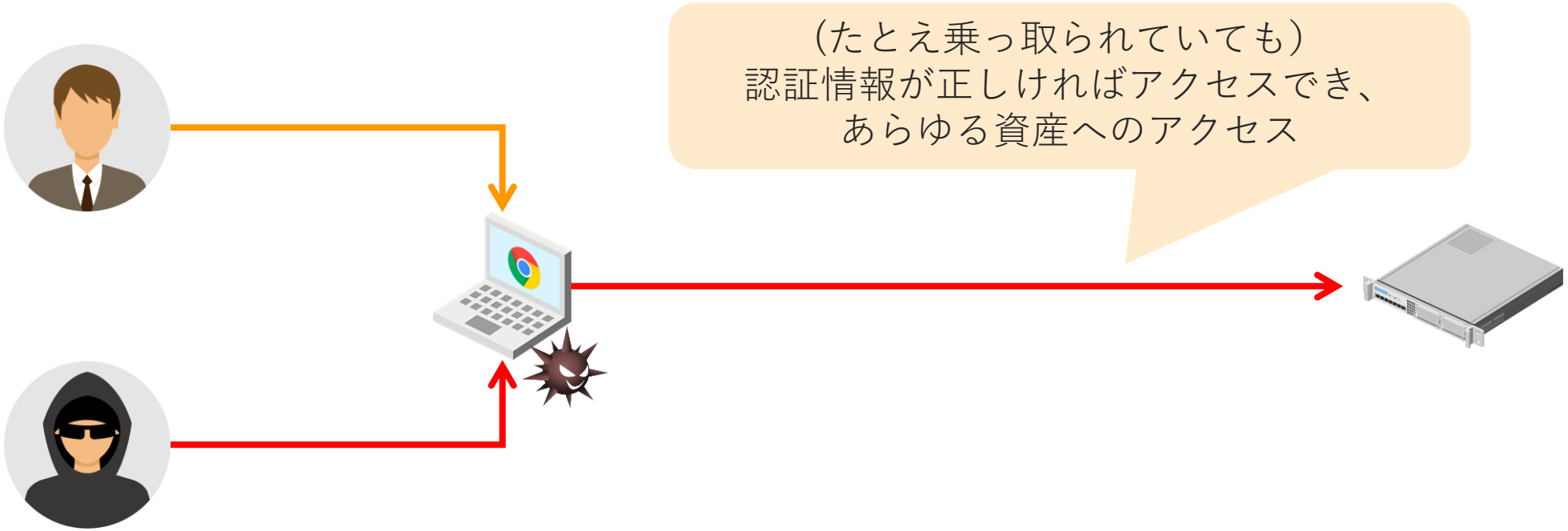


CWPP: Cloud Workload Protection Platform
CSPM: Cloud Security Posture Management

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

③潜在的なアクセス方法の課題

- VPNをはじめとしたトンネル技術は、遠隔から様々なリソースへのアクセスを可能とする
- その利便性は、攻撃者にとっても同様
  - VPNを突破することができれば、様々な情報資産を窃取・暗号化などが可能となる



Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

ゼロトラストにおけるエンドポイントの重要性について

- 世の中の変化する状況に適応するために、モバイル・クラウドの活用、新しいデジタルビジネス・働き方を可能にするためのセキュリティの考え方
  - 過度に付与されていた「信頼」を見直し、最低限の「信頼」を行うことでセキュリティを担保する

実空間でのゼロトラストの例
～コロナ禍での出社～

万が一、感染していても
うつさない

手指の消毒により
感染リスクを下げる

検温により感染の
リスクを想定する

社員証を持っていても、身体状態や感染が疑われる場合は自宅で勤務してもらう

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

ゼロトラストにおけるエンドポイントの重要性について

- 世の中の変化する状況に適応するために、モバイル・クラウドの活用、新しいデジタルビジネス・働き方を可能にするためのセキュリティの考え方
  - 過度に付与されていた「信頼」を見直し、最低限の「信頼」を行うことでセキュリティを担保する

ゼロトラストの例
～システムへのアクセス～

端末上の高度な脅威を
ブロックできる

端末の脆弱性などを
しっかり管理できる

端末の状態を客観的な
スコアで評価できる

認証情報が正しくても、 **「端末」** の状態に応じて、リソースのアクセスを動的にコントロール

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

まとめ

- 端末は境界の外へ
  「**EDR**」や「**脅威ハンティング**」などで強化が必要
- パブリッククラウドはDXで重要なインフラへ
  「**CSPM**」、「**CWPP**」などクラウドセキュリティが重要に
- 新しいビジネス、働き方を支える「ゼロトラスト」
  アクセス元である**「端末」のセキュリティ状態がキー**となる

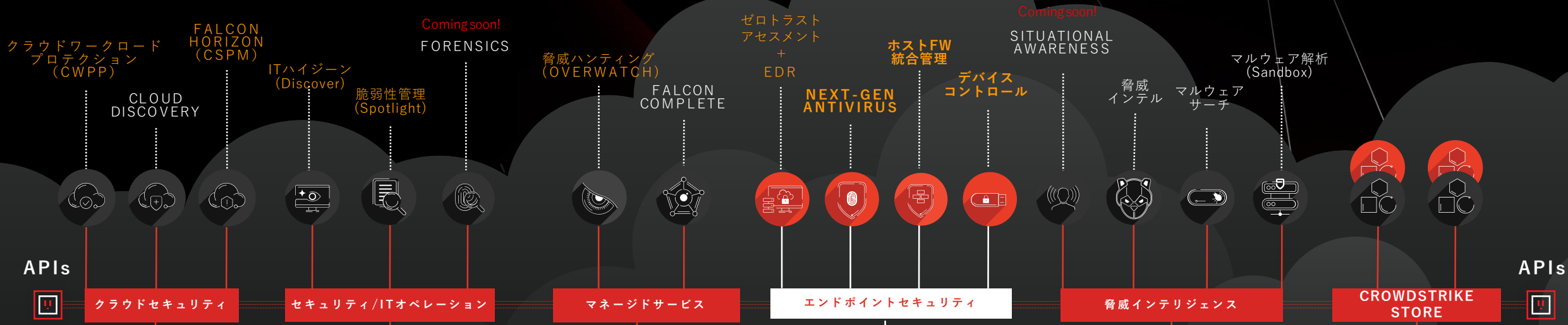
であれば、これらの多くの要件を満たすことができます。

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

CROWDSTRIKE

THE CROWDSTRIKE falcon platform

1つのプラットフォームですべての環境をカバー
セキュリティを守るのに複数のエージェント、複数の管理コンソールはもう必要ありません。



CROWDSTRIKE THREAT GRAPH

軽量なシングルエージェント

ワークステーション	サーバー	仮想マシン	コンテナ	クラウド	モバイル	IOT
クラウド環境に対する可視化と防御+CSPM	資産管理、脆弱性管理、+フォレンジック調査	専門家による24365脅威ハンティング	高度な標的型攻撃を自動検知/ブロック+FWとUSBの制御	脅威インテリジェンスによるプロアクティブな防御+自動解析		他ベンダーとのAPIによる自動連携

CrowdStrike製品まとめ

- １つのエージェント、コンソールで「EDR」や「AV機能」だけでなく「脅威ハンティング」をはじめとした様々な機能を提供
- ゼロトラストを実現する端末セキュリティー
- PCだけでなく、モバイル、クラウド、コンテナも保護可能

CROWDSTRIKE

で、DX時代に向けたセキュリティ対策を！

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

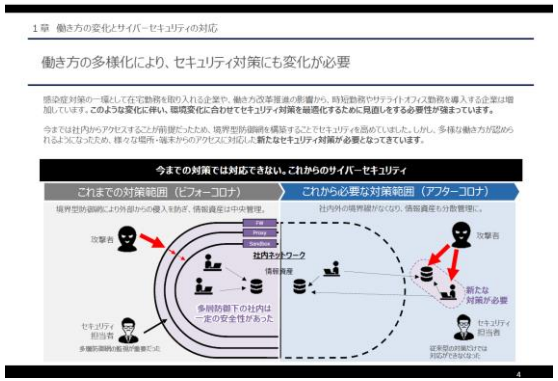
資料のご案内

テレワークソリューション CrowdStrike ホワイトペーパー

多様な働き方から企業を守る
次世代型エンドポイントプラットフォームとは？

目次

- １：働き方の変化とサイバーセキュリティの対応
- ２：改めて意識したいセキュリティポイントとその対応
- ３：次世代のセキュリティプラットフォーム「Falconプラットフォーム」



ユーザー事例記事提供中！ SanSan株式会社様

【最新事例】

導入のポイント

- アラート件数が激減し、より付加価値の高い業務への注力が可能になった
- テレワーク／リモートワークの状況下でも安全な業務環境を提供できる
- 強力な検索機能を駆使することで、運用管理業務の効率化にも貢献

アンケートのご回答で各種資料をご提供致します。

Copyright © 2004-2020 Macnica Networks Corp. All Rights Reserved.

ご清聴ありがとうございました。

- 本資料に記載されている会社名、商品、サービス名等は各社の登録商標または商標です。なお、本資料中では、「™」、「®」は明記しておりません。
- 本資料は、出典元が記載されている資料、画像等を除き、弊社が著作権を有しています。
- 著作権法上認められた「私的利用のための複製」や「引用」などの場合を除き、本資料の全部または一部について、無断で複製・転用等することを禁じます。
- 本資料は作成日現在における情報を元に作成されておりますが、その正確性、完全性を保証するものではありません。