DXをリードするセキュリティ戦略
～ゼロトラストの時代へ～

テレワーク時代における境界線セキュリティの限界 分科会

2022年2月3日

分科会メンバー （９名）

リーダー	株式会社エムアンドシーシステム	伊藤　智
サブリーダー	株式会社日本テクノス	今野　亜由子
	株式会社IHIエスキューブ	高山　泰
	日本システム技術株式会社	竹内　千春
	東亜建設工業株式会社	浅野　造史
	日本放送協会	服部　多栄子
	株式会社アシスト	内田　泰司
	株式会社アシスト	片山　武志
	株式会社アシスト(事務局)	青木　裕明

アジェンダ

1．ゼロトラストとは？
2．なぜ今ゼロトラストなの？
3．必要なものは？
4．どうやって進めればいいの？
5．おわりに

突然ですが

1.『ゼロトラスト』って
なんのことか
わかりますか？

『ゼロトラスト』とは？

その名の通り

『すべての人やデバイスは**信頼できない**ことを前提としてセキュリティ対策を講じること』

うーーーーん。言葉だけだとうまくイメージできないなぁ。。。

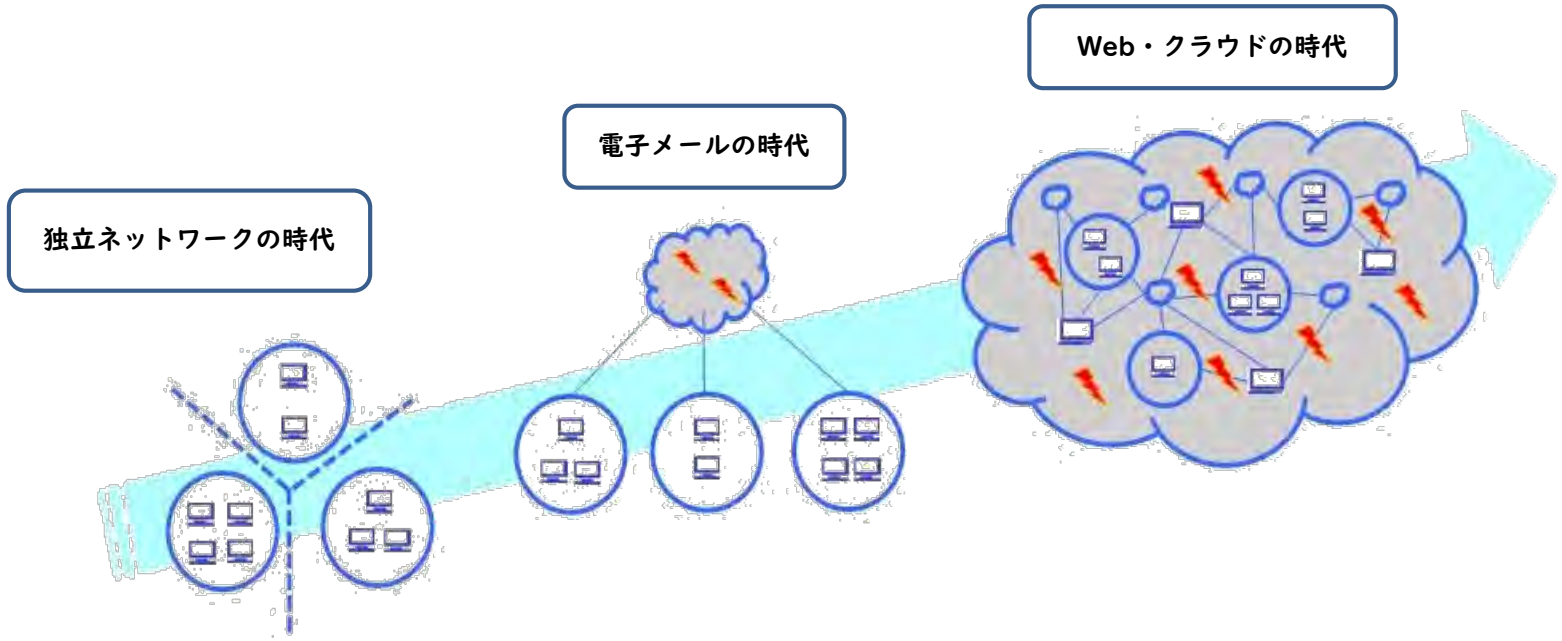
“振り込め詐欺”でイメージしてみよう！

家の外からの電話の声は
家の中で直接話をするのと比べ、
リスクが高い
(容姿・振舞いを見続けられない)

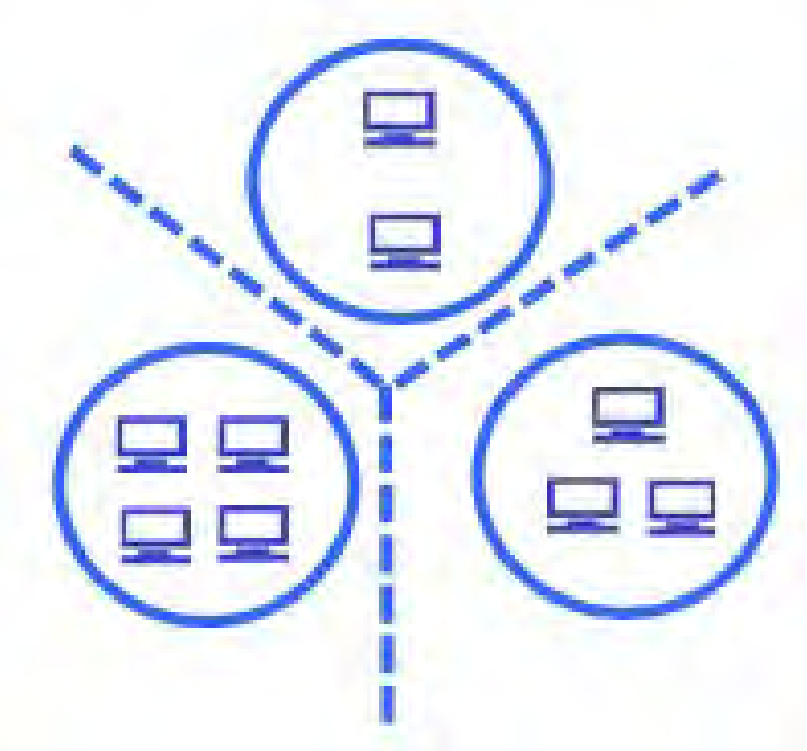
リスクを軽減するため
折返しコールなど新たな確認方法が
推奨されている

情報セキュリティの環境変化

日常生活と同様に、情報セキュリティの世界も環境が移り変わってきた

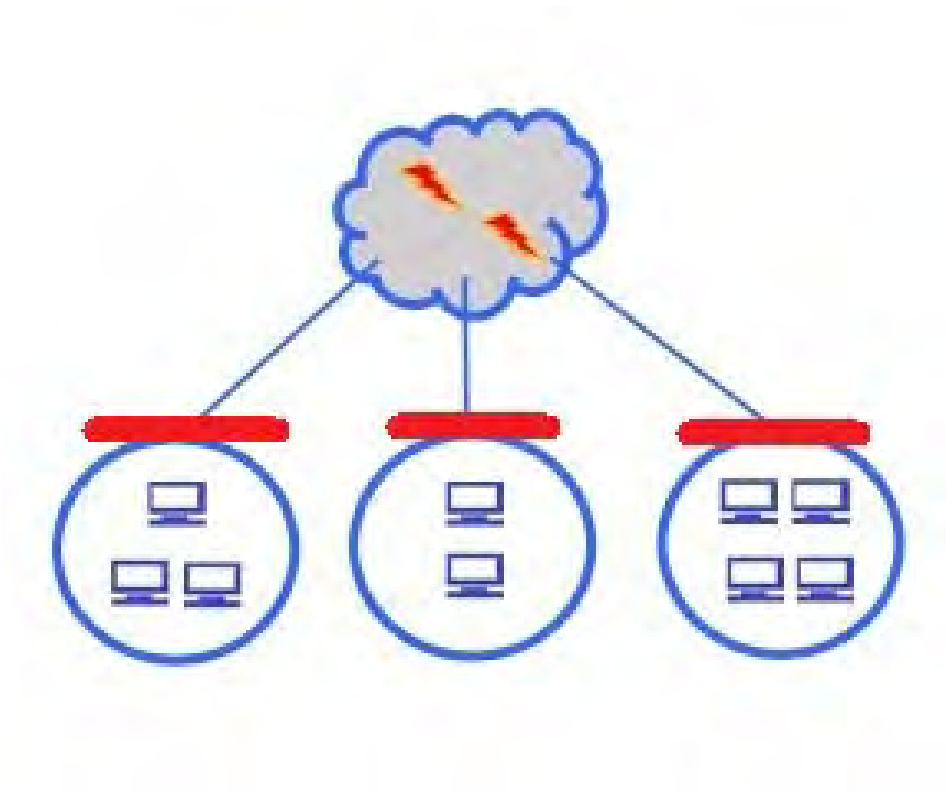


情報セキュリティの環境～①独立ネットワークの時代



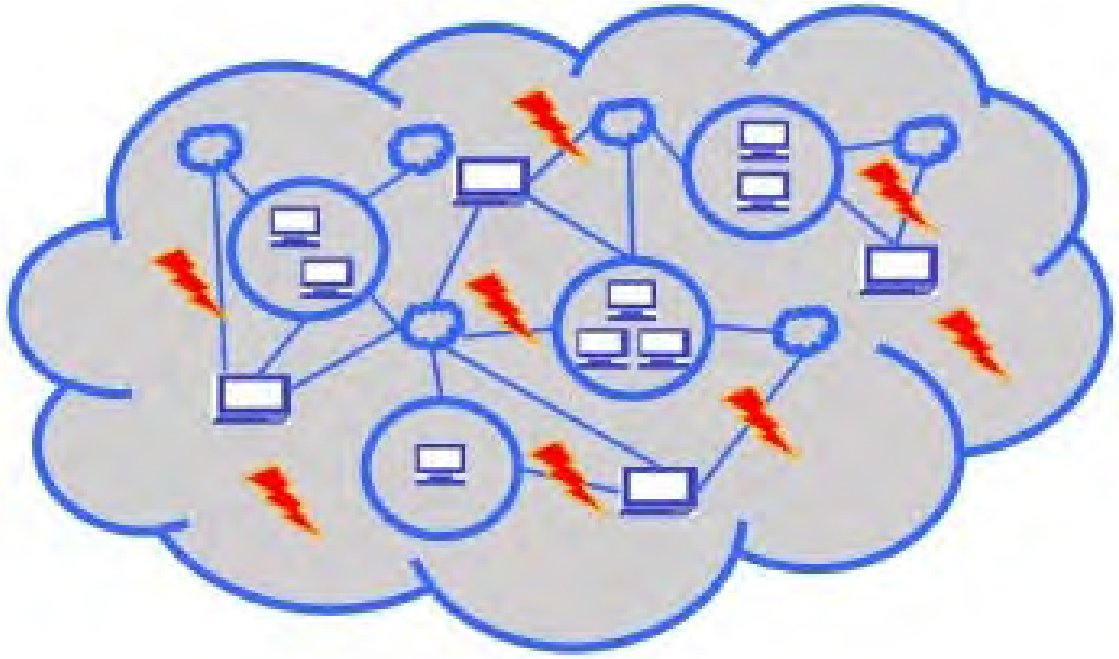
ネットワーク間で
オンライン通信・データ授受は
存在しなかった
(テープ・ディスクの時代)

情報セキュリティの環境②～電子メールの時代



ネットワーク間で少量・低頻度の
オンライン通信・データ授受が
開始された
(境界(赤線)を監視することで
内部は安全)

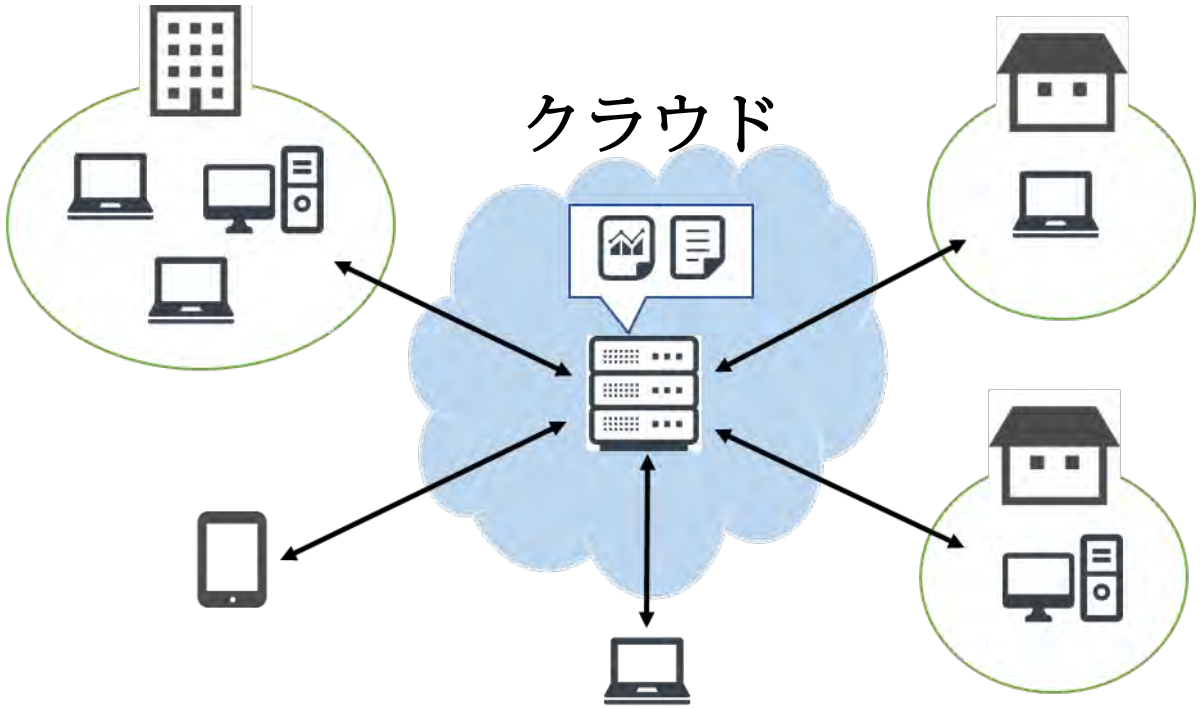
情報セキュリティの環境③～Web・クラウドの時代



クラウドサービス利用など

大量・高頻度のオンライン通信・
データ授受が行われるようになる

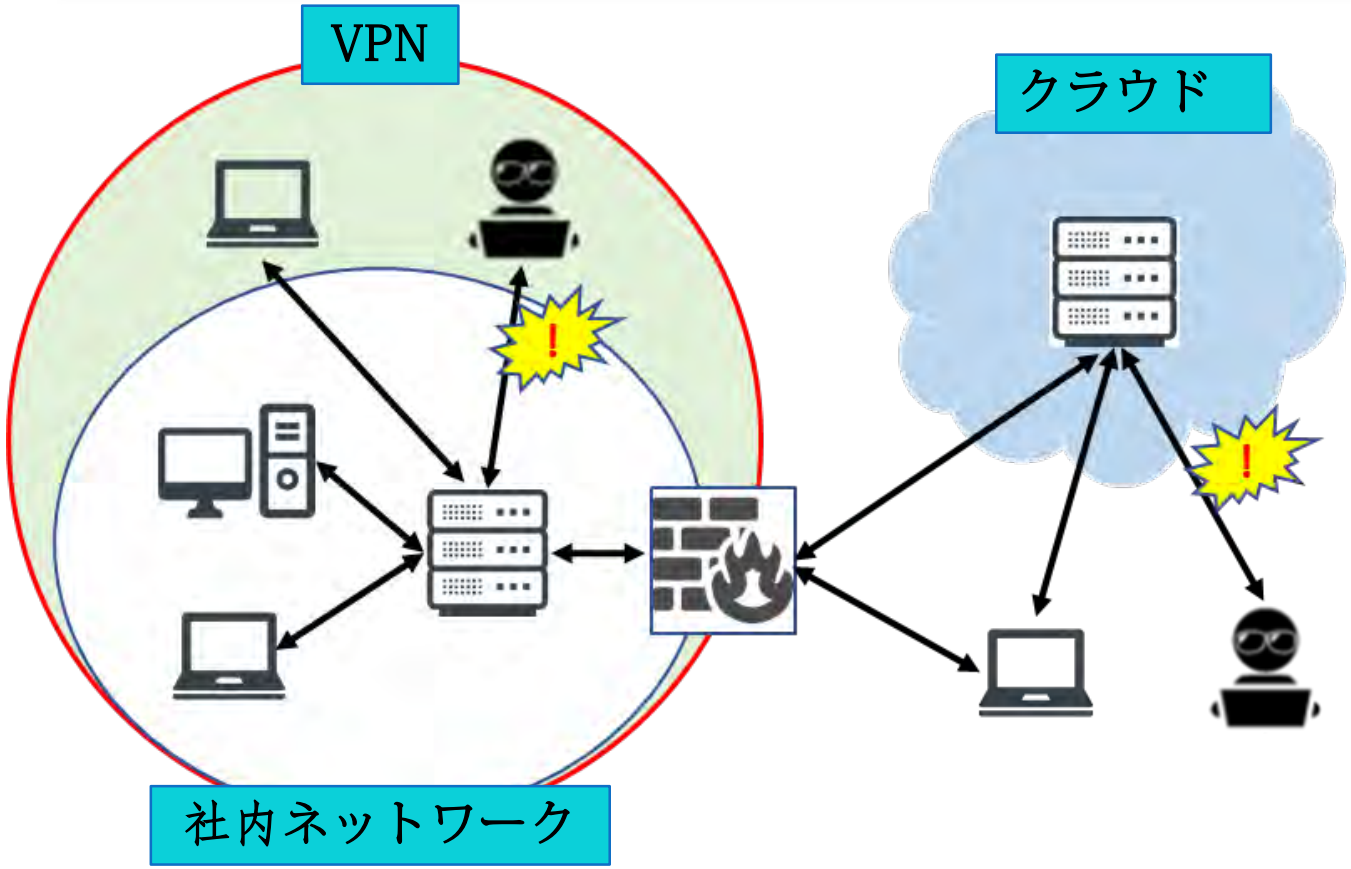
クラウド利用とテレワーク



クラウドサービス利用により社内データはネットワークの外に保存される

テレワークの普及でクラウドサービスのデータはどこからでも利用されるようになる

境界線型防御の限界～問題点



- 従来は社内ネットワークと外部との境界線を監視する「境界線型防御」で社内データを守っていた
- しかし、クラウドサービスをテレワークで利用する際には境界線を通ることがないため、境界線型防御だけで社内データを守れなくなった

『ゼロトラスト』とはこういうこと！

どこから業務を行う人、どこからアクセスするデバイスであっても

『いかにして社内のデータを守るか』が重要課題となった。

『IDの振舞い』や『デバイスの状態』などを常に確認し、

必要なID・デバイスにだけ社内データのアクセス権限を与える

＝

ゼロトラスト

2.なぜ、今『ゼロトラスト』なの？

働く環境の変化

新型コロナウィルス感染拡大に伴い働き方を変えざるを得ない状況に・・・

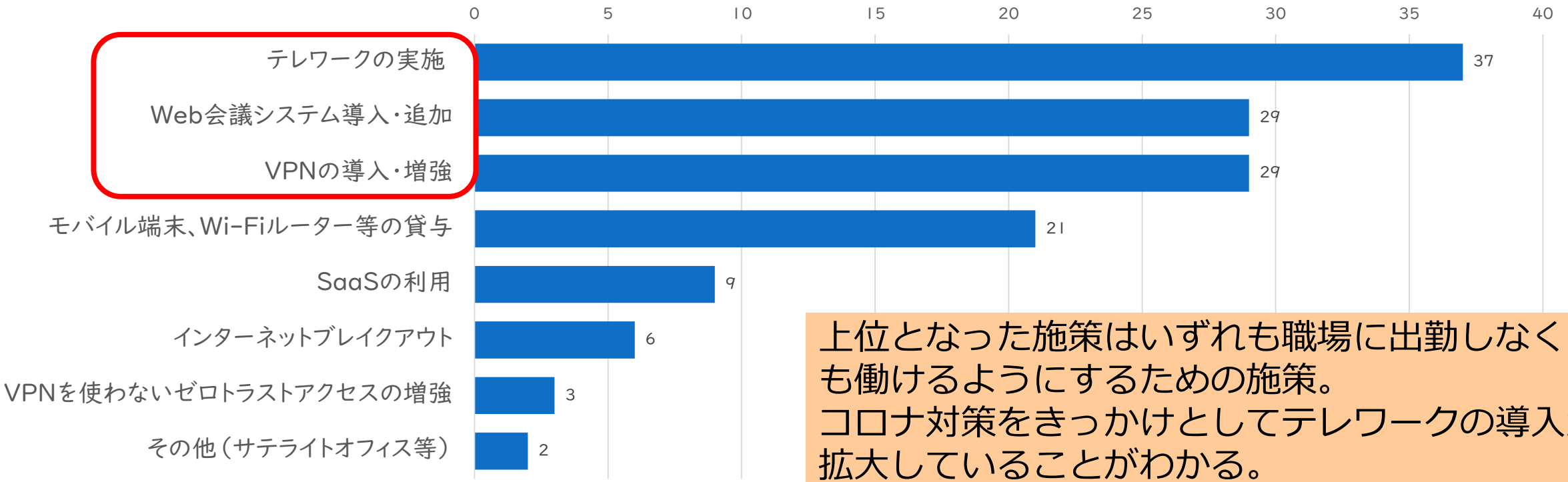
実際に、各企業ではどんな対応をとったのか？

ソリューション研究会メンバーに協力してもらったアンケート結果をもとに

見てみよう

テレワークの拡大　～企業のコロナ対策～

あなたの会社ではコロナ対策としてどのようなIT施策を実施しましたか（複数回答可）



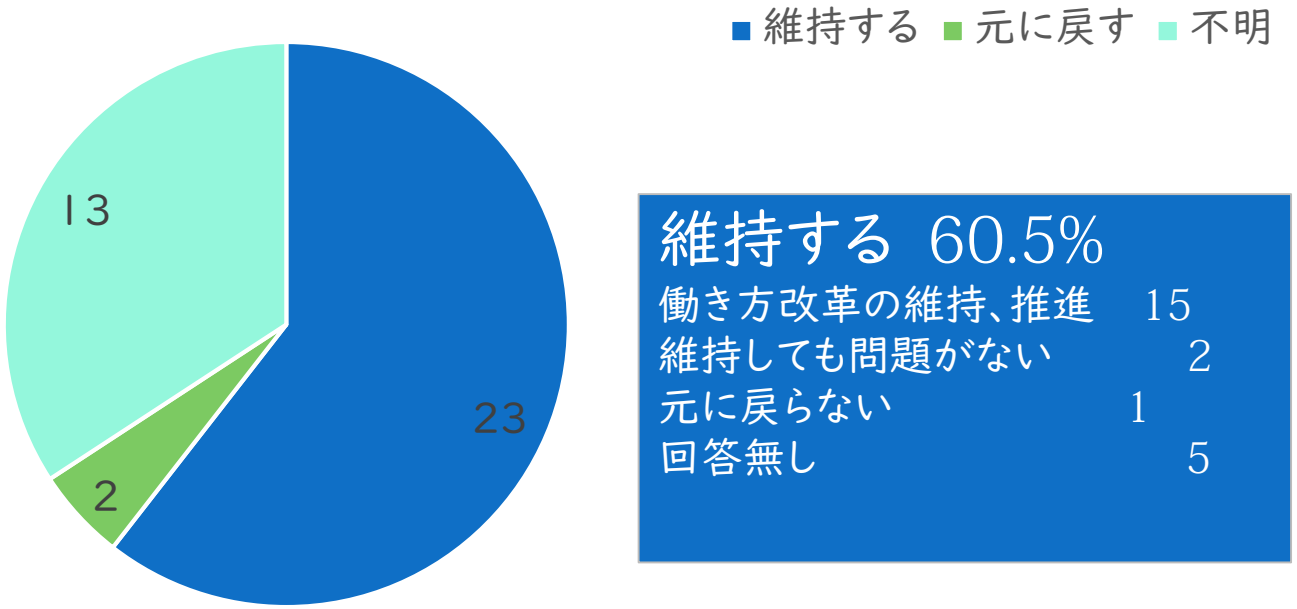
上位となった施策はいずれも職場に出勤しなくても働けるようにするための施策。
コロナ対策をきっかけとしてテレワークの導入が拡大していることがわかる。

コロナ終息後、テレワークは・・・

コロナ収束後にコロナ対策として実施したIT施策は終了させ、
元に戻しますか。それとも維持しますか。

不明　34.2%
方針がまだ定まっていない　3
取捨選択が必要　2
経営陣がメリットを感じていない　1
その他　2

元に戻す　5.3%
メリットがない　1
無回答　1



維持する　60.5%
働き方改革の維持、推進　15
維持しても問題がない　2
元に戻らない　1
回答無し　5

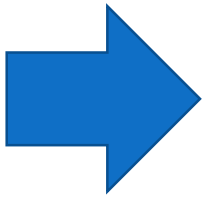
「維持する」の理由の第１位は
「テレワークを含む働き方改革の維持、推進」

テレワーク導入の意味

テレワーク導入はコロナ対策だけではなく、働き方改革およびDX推進にも影響

【働き方改革の推進】

- 通勤時間を削減することによる生産性向上
- 子育て・介護による離職の防止
- 勤務地に限定されない求人



優秀な人財の確保

【DX推進の第一歩】

- デジタル技術の導入による事業・経営の改革

デジタルトランスフォーメーション（DX）

デジタルトランスフォーメーション（DX）とは・・・

「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること」

これからの時代にすべての企業が取り組むべき**「事業・経営の改革」**である

テレワークから始めるDX

テレワークというデジタル化の第一歩を踏み出したことで、多くの企業がDXを推進する機運を高めやすい状況が整ったと言える

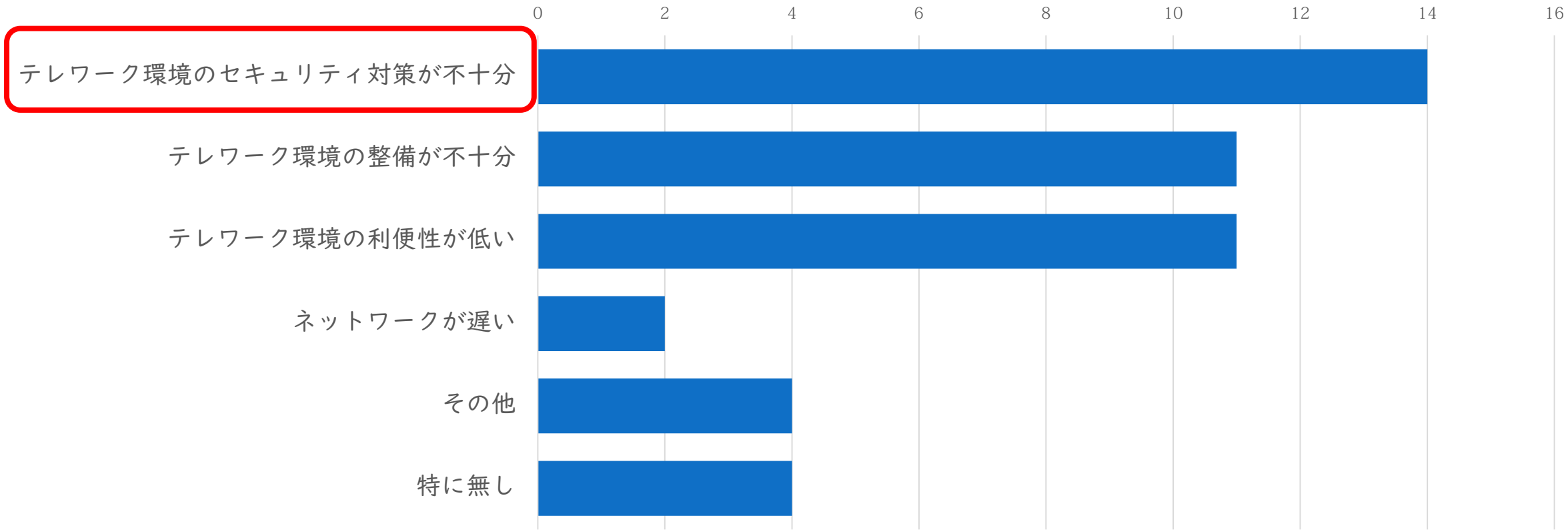
ん？ちょっと待って・・・

テレワークは拡大してきましたが・・・それだけでいいのでしょうか？

課題はないのでしょうか？

テレワークの拡大　～企業のコロナ対策～

現状のIT・セキュリティ課題はありますか（複数回答可）



テレワークセキュリティガイドライン

コロナ対策で、各企業がテレワークを導入していく中、

総務省は
「テレワークセキュリティガイドライン」の内容を大幅に改定

ここで**ゼロトラストセキュリティ**の有効性を提示

ゼロトラストが注目されるようになった理由は

- コロナ対策でテレワークが拡大し、クラウド化も進んでいる
- 働き方改革もDXも進めたい

デジタル化の推進と**セキュリティ**は
車の両輪のごとく同じスピードで回して前進する必要がある

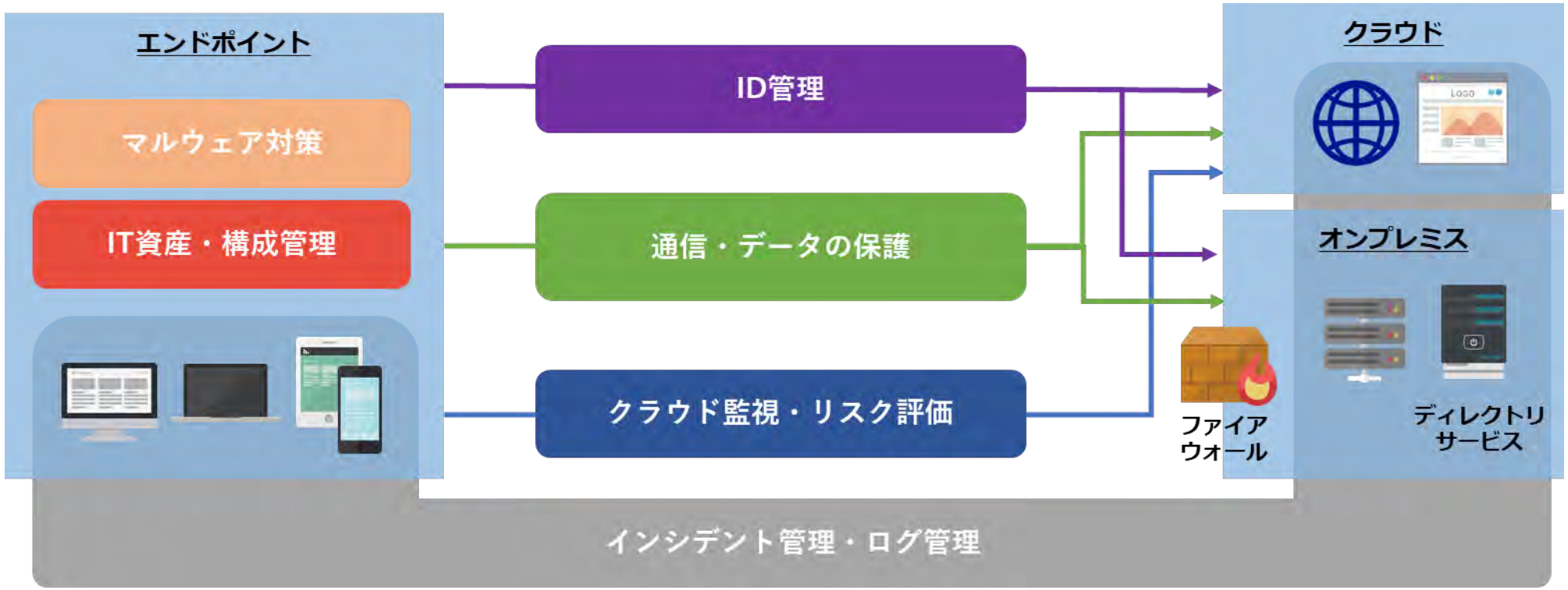
DXのセキュリティを実現するために必要なのが**ゼロトラストセキュリティ　・・・**

やるなら今でしょ！！

3.『ゼロトラスト』って何が必要なの？

『ゼロトラスト』に必要な要素

従来のセキュリティの置き換えまたは追加により大切な情報を守っていく



『ゼロトラスト』に必要な要素

ユーザID・パスワード・利用端末情報等をクラウド上で一元管理

『ゼロトラスト』に必要な要素

インターネットアクセスおよびデータそのものの安全性向上

『ゼロトラスト』に必要な要素

クラウドを利用するユーザおよびクラウドサービスの安全性向上

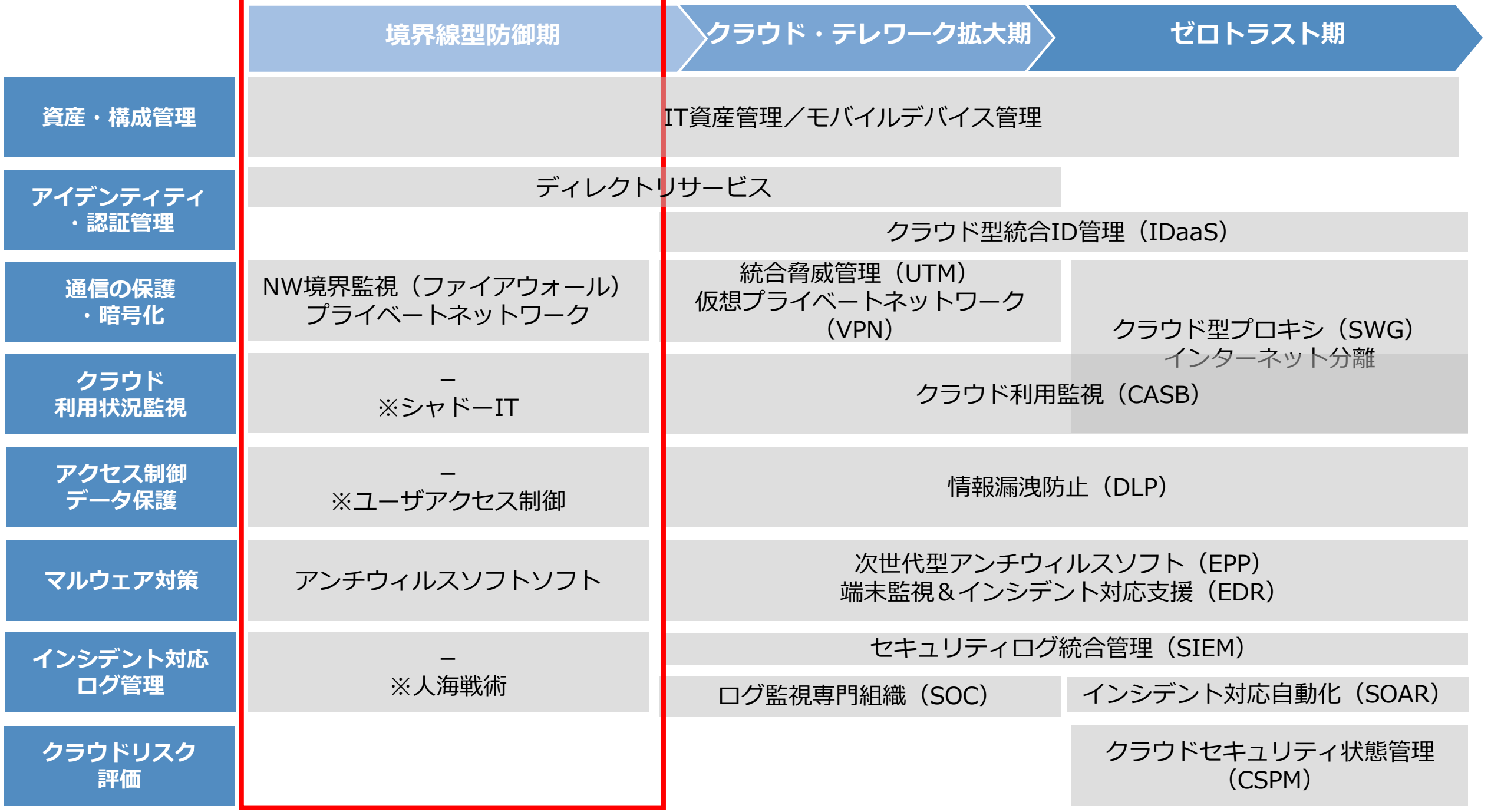
『ゼロトラスト』に必要な要素

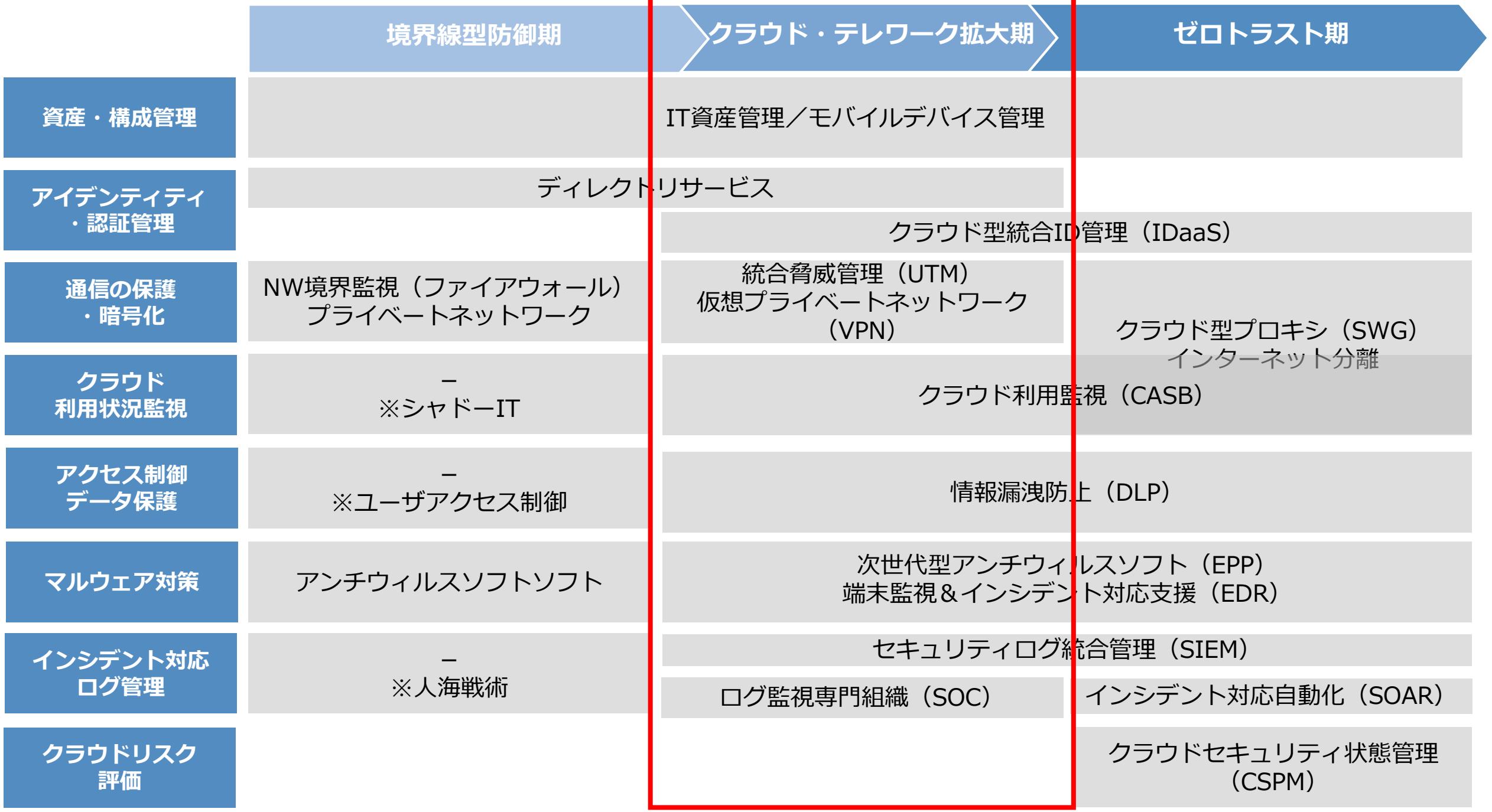
端末の動きを監視し、端末の安全性向上

4.『ゼロトラスト』ってどうやって進めるの？

ロードマップで意識すべき3つのフェーズ

	境界線型防御期	クラウド・テレワーク拡大期	ゼロトラスト期
要素１	ロードマップ		
要素２			
・ ・ ・	境界内部にファイルサーバや各種業務系アプリを設置。外部との接続を遮断してきた時代。	クラウドの利用が進み、働き方改革やテレワークの導入が一気に拡大してきた時代。	社内・社外関係なくすべてのアクセスがクラウド上のゲートウェイを経由する時代。


境界線型防御期
クラウド・テレワーク拡大期
ゼロトラスト期
資産・構成管理
IT資産管理／モバイルデバイス管理
アイデンティティ・認証管理
ディレクトリサービス
クラウド型統合ID管理（IDaaS）
通信の保護・暗号化
NW境界監視（ファイアウォール）
プライベートネットワーク
統合脅威管理（UTM）
仮想プライベートネットワーク（VPN）
クラウド型プロキシ（SWG）
インターネット分離
クラウド利用状況監視
－
※シャドーIT
クラウド利用監視（CASB）
アクセス制御データ保護
－
※ユーザアクセス制御
情報漏洩防止（DLP）
マルウェア対策
アンチウィルスソフトソフト
次世代型アンチウィルスソフト（EPP）
端末監視＆インシデント対応支援（EDR）
インシデント対応ログ管理
－
※人海戦術
セキュリティログ統合管理（SIEM）
ログ監視専門組織（SOC）
インシデント対応自動化（SOAR）
クラウドリスク評価
クラウドセキュリティ状態管理（CSPM）

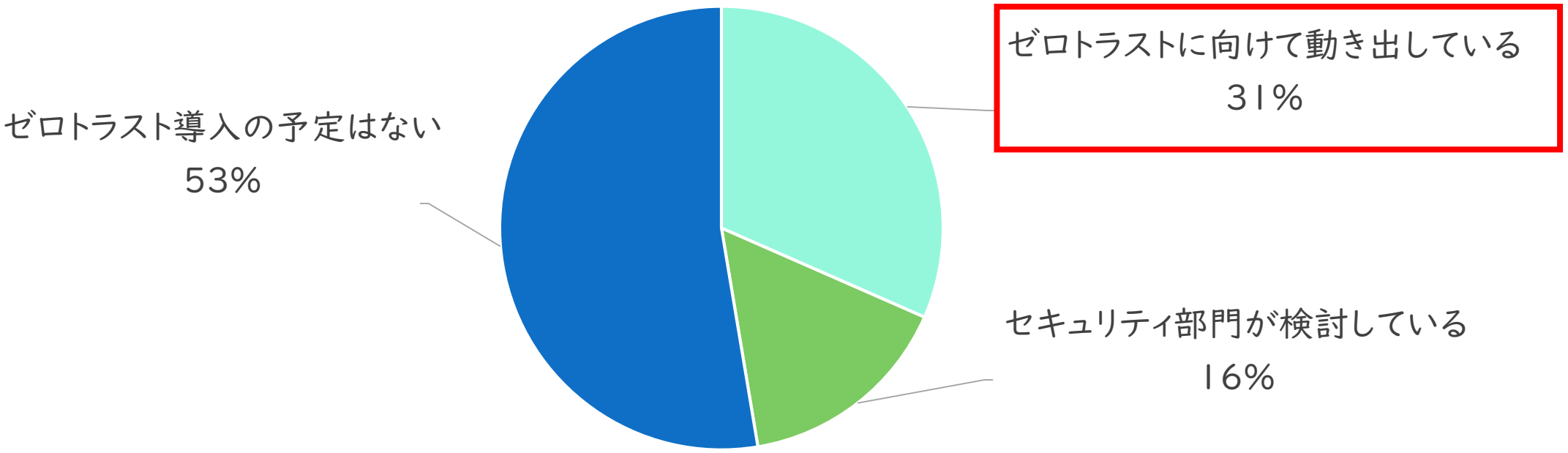

境界線型防御期
クラウド・テレワーク拡大期
ゼロトラスト期
資産・構成管理
IT資産管理／モバイルデバイス管理
アイデンティティ・認証管理
ディレクトリサービス
クラウド型統合ID管理（IDaaS）
通信の保護・暗号化
NW境界監視（ファイアウォール）
プライベートネットワーク
統合脅威管理（UTM）
仮想プライベートネットワーク（VPN）
クラウド型プロキシ（SWG）
インターネット分離
クラウド利用状況監視
－
※シャドーIT
クラウド利用監視（CASB）
アクセス制御データ保護
－
※ユーザアクセス制御
情報漏洩防止（DLP）
マルウェア対策
アンチウィルスソフトソフト
次世代型アンチウィルスソフト（EPP）
端末監視＆インシデント対応支援（EDR）
インシデント対応ログ管理
－
※人海戦術
セキュリティログ統合管理（SIEM）
ログ監視専門組織（SOC）
インシデント対応自動化（SOAR）
クラウドリスク評価
クラウドセキュリティ状態管理（CSPM）

	境界線型防御期	クラウド・テレワーク拡大期	ゼロトラスト期
資産・構成管理	IT資産管理／モバイルデバイス管理		
アイデンティティ・認証管理	ディレクトリサービス	クラウド型統合ID管理（IDaaS）	
通信の保護・暗号化	NW境界監視（ファイアウォール） プライベートネットワーク	統合脅威管理（UTM） 仮想プライベートネットワーク（VPN）	クラウド型プロキシ（SWG） インターネット分離
クラウド利用状況監視	– ※シャドーIT	クラウド利用監視（CASB）	
アクセス制御データ保護	– ※ユーザアクセス制御	情報漏洩防止（DLP）	
マルウェア対策	アンチウィルスソフトソフト	次世代型アンチウィルスソフト（EPP） 端末監視＆インシデント対応支援（EDR）	
インシデント対応ログ管理	– ※人海戦術	セキュリティログ統合管理（SIEM） ログ監視専門組織（SOC）	インシデント対応自動化（SOAR）
クラウドリスク評価			クラウドセキュリティ状態管理（CSPM）

経営層へのアプローチ

本分科会で実施したアンケート結果より

あなたの会社でのゼロトラストに関する取組状況について教えて下さい



経営層へのアプローチ　-3つの視点-

①サイバーリスクの可視化

②リソースの活用によるコスト抑制

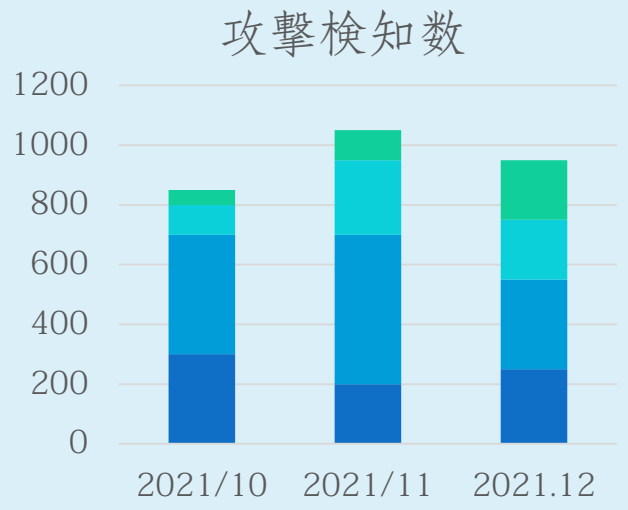
③投資に対する効果
- DX推進のためのゼロトラスト

①サイバーリスクの可視化

-サイバーリスク指標-

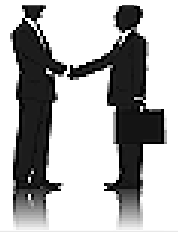
サイバーリスク指標 - リスクを客観的に評価するための情報 - を提示する

サイバー攻撃の種類・数・傾向



従業員の行動

資産・クラウドの数・利用状況



行動履歴

②リソースの活用によるコスト抑制

-既存セキュリティ製品の活用と見直し-

未導入・導入検討

今後必要となるソリューション

ゼロトラスト移行期に導入済み
(CASB・DLP・EPP・EDR・SIEMなど)

境界線型防御適用期に導入済み・不要製品の終了や入れ替え
(IT資産管理・モバイルデバイス管理など)

コスト抑制:
- 既存製品の活用
- 不要製品の終了

- 物理サーバ管理費
- オフィス運営費

③投資に対する効果

-DX推進のためのゼロトラスト-

DX推進

テレワーク環境整備

- **生産性の向上**
- **育児/介護離職防止**
- **勤務地に限定されない**

優秀な人財の確保

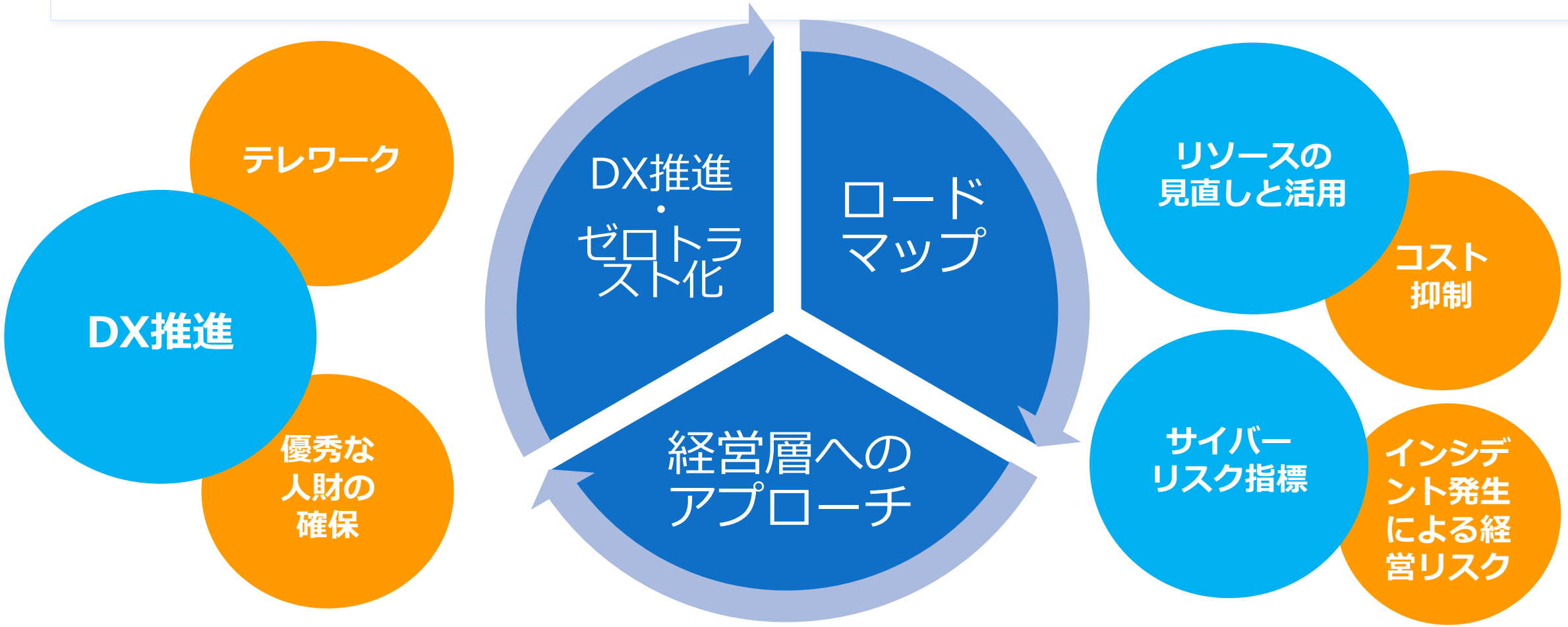
セキュリティ

情報漏洩防止

サイバー攻撃対策

ゼロトラストソリューション

ゼロトラストの進め方まとめ



5.おわりに

**企業はこれからもDXを推進し続けて
いかなければならない**

**デジタル化の推進とセキュリティは車の両輪のごとく
同じスピードで回して前進していくことが必要**

今こそゼロトラストでどこでもセキュリティを実現していかなければならない時代になっているのである！

ご清聴ありがとうございました