Microsoft

Microsoft DIGITAL TRUST SECURITY

#digitaltrust

Microsoft Security Forum 2020

～変化に備える、2020 年のセキュリティ対策～

Microsoft
DIGITAL TRUST SECURITY

Microsoft
Security Forum 2020

山崎 善寛
Yoshihiro Yamasaki

日本マイクロソフト株式会社
Microsoft 365 ビジネス本部
本部長

新型コロナウイルス影響下のマイクロソフトの取り組み

マイクロソフト全体の取組み

- 在宅勤務の活用を強く推奨

日本マイクロソフトの取組み

- 「小・中・高等学校、特別支援学校の臨時休業」を受けて、ファミリーケア休暇（年間 5 日付与）の利用範囲を拡大

DIGITAL TRUST

お客様へのご支援

リモートワークに取り組む組織に向けて、無料相談窓口を開設

セキュア リモートワーク相談窓口 (無料)
お電話でのご相談は 0120-167-400 まで
Web からのご相談こちら >

無償ライセンス・サービスを提供

法人向け

- Office 365 E1 ライセンスの 6 ヶ月無償提供
- Microsoft Teams トレーニングの無償提供
- Microsoft Teams Live Event サービスの実施支援

教育機関向け

- Office 365 A1 ライセンスの無償提供
- オンラインイベント配信用機材として、Surface を無償貸与
- Minecraft: Education Editionを無償提供（A1アカウントが必要）

DIGITAL TRUST


DIGITAL
TRUST

Digital Trust Summit 2019 を踏まえた活動

ゼロトラスト環境への理解

Sentinel Cloud Native SIEM への注目

パートナーアライアンスの充実

変化に備えるための
広範囲にわたる
ソリューション提供

Microsoft

DIGITAL TRUST SECURITY

Microsoft Security Forum 2020

NTTコミュニケーションズ株式会社
情報セキュリティ部長
小山 覚 様

働き方改革とセキュリティを両立させるゼロトラストとは？

2020年 3月 12日

情報セキュリティ部長
小 山 覚

1.働き方改革やDXを支える

高度な攻撃に備える

クラウド化を推進する

2017年5月 個人情報保護法改正を契機に取り組み開始

高度な暗号化等の秘匿化がされている場合は、情報が外部に漏えいしていないと判断される

高度な暗号化等の秘匿化：

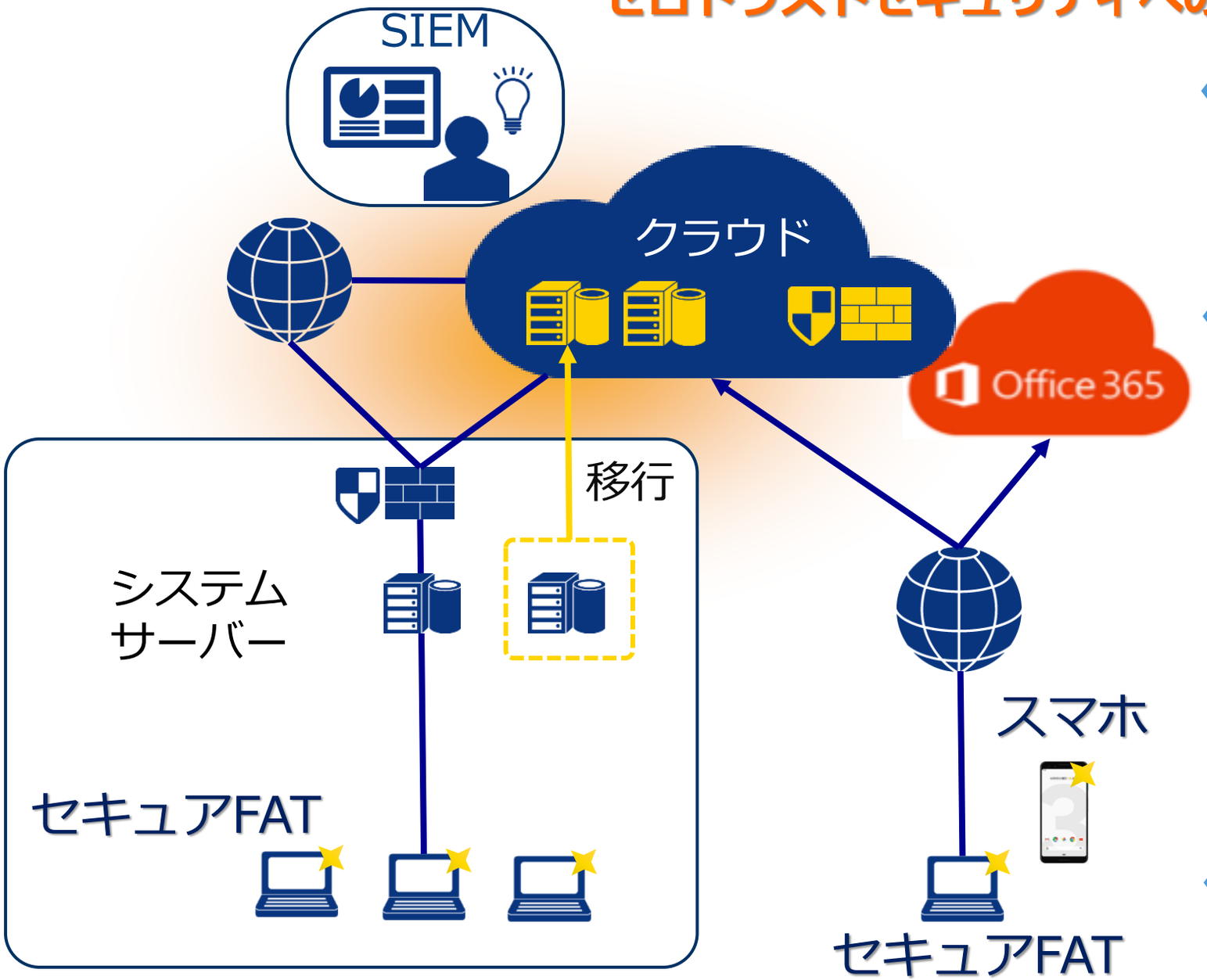
ｉ）漏えい情報が第三者が見読不可能な状態にする暗号化等の技術的措置が講じられており
ii）そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要

① 適切な評価機関等により**安全性が確認されている電子政府推奨暗号リストやISO/IEC 18033等に掲載されている暗号技術**が用いられ、それが適切に実装されていること

② 下記いずれかの要件を満たすことが必要
- **暗号化した情報と復号鍵を分離するとともに復号鍵自体の漏えいを防止**する適切な措置を講じていること
- **遠隔操作により暗号化された情報若しくは復号鍵を削除**する機能を備えていること
- 第三者が復号鍵を行使できないように設計されていること

2018年 セキュアFATとクラウド利用を開始

ゼロトラストセキュリティへの序章



オンプレ＋クラウドのログの総合分析を実施

Microsoft Defender ATP（EDR）
Azure RMS
Cloud Proxy
CASB（導入予定）
クライアントPCフォルダ同期
SCCM（パッチ配信）

Windows FireWall
端末暗号化（IRM）
生体認証
ファイル暗号化
クライアントPCフォルダ同期
マルウェア対策
Microsoft Defender ATP（EDR）

生産性の向上（作業時間）

24～40% 削減

セキュリティ（インシデント対応時間）

53～82% 削減

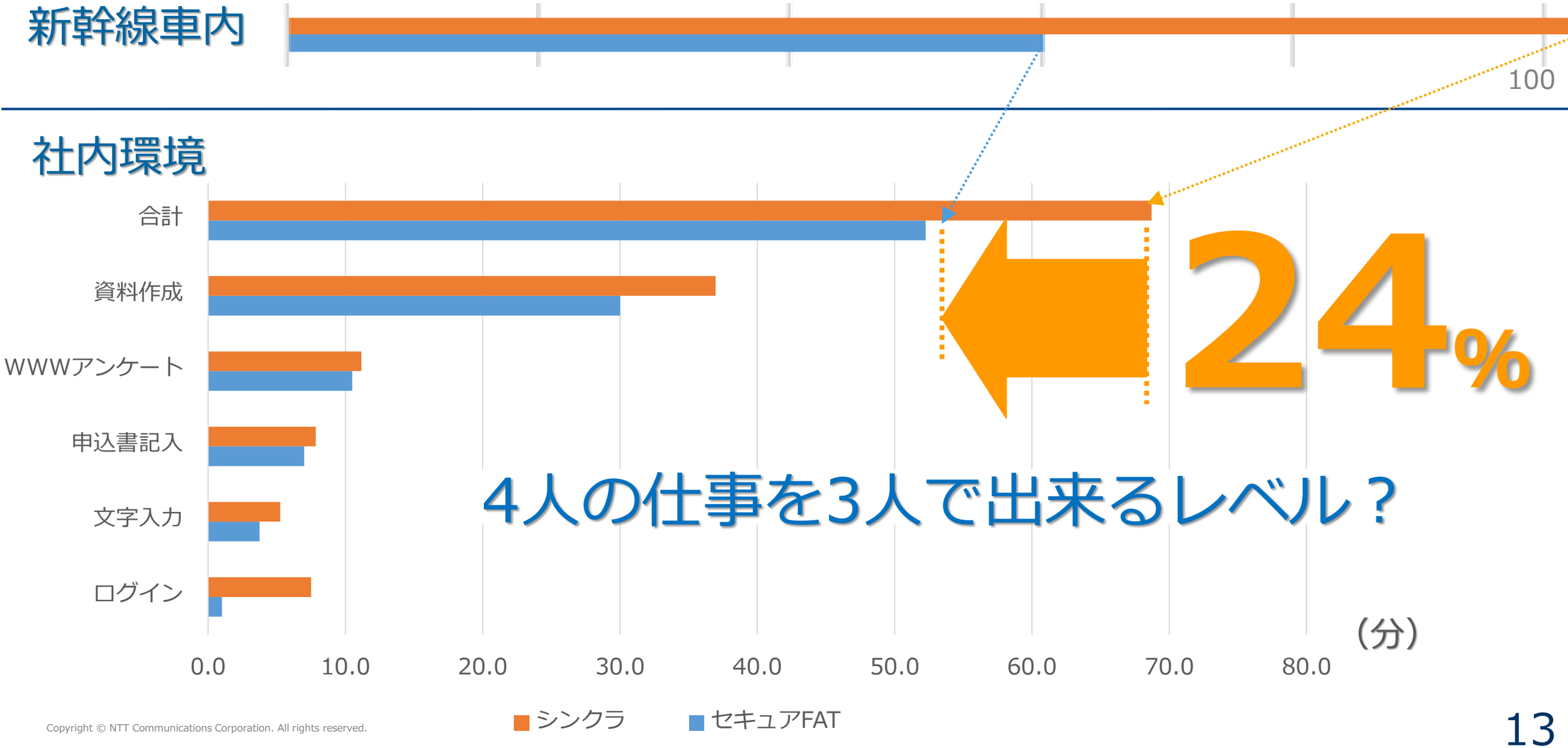
クライアント環境のコスト

65% 削減

作業の快適性

10ポイント向上

新幹線車内と社内環境で生産性を比較



24%

4人の仕事を3人で出来るレベル？

生産性の向上

（ ログオン → Outlook起動 → メール確認 までの時間 ）

シンクライアント：7-8 分

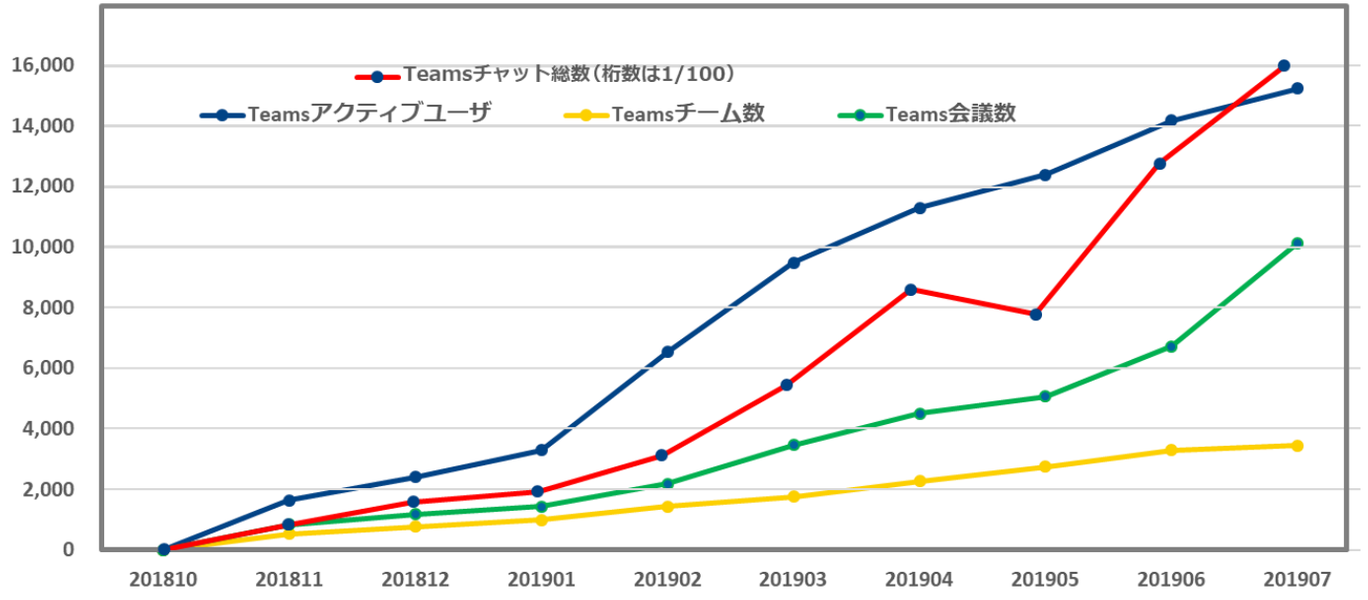
新セキュアFAT　　：　1 分

セキュアブラウザ：40 秒

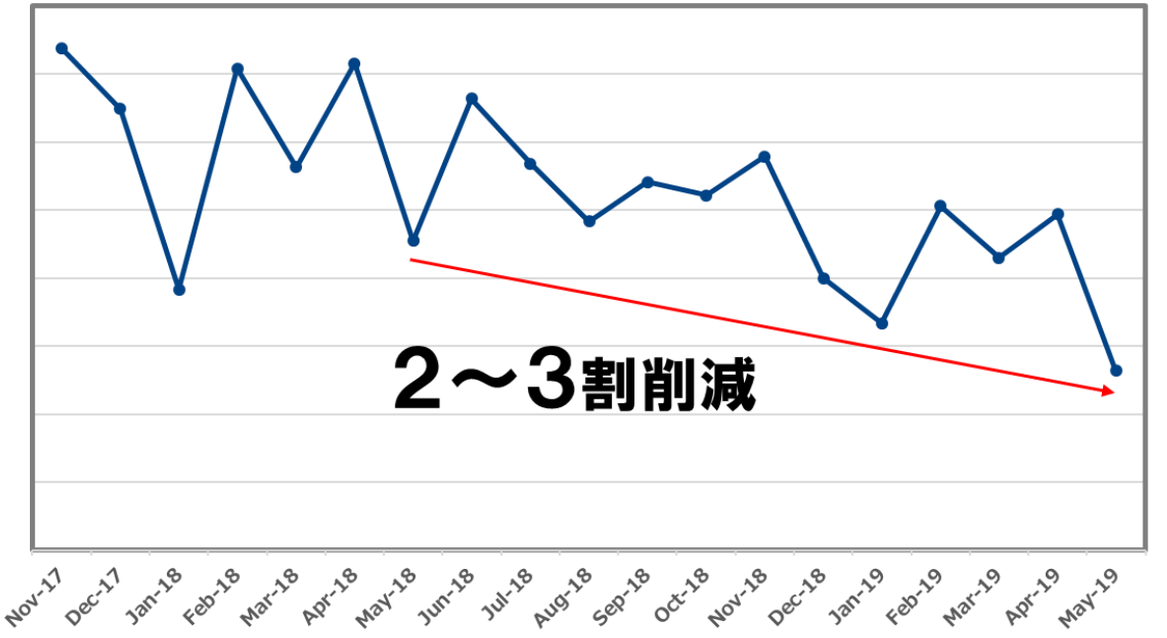
新セキュアスマホ　：10 秒

Teamsの利用者増加 → 紙資料の削減

Microsoft Teams 利用状況

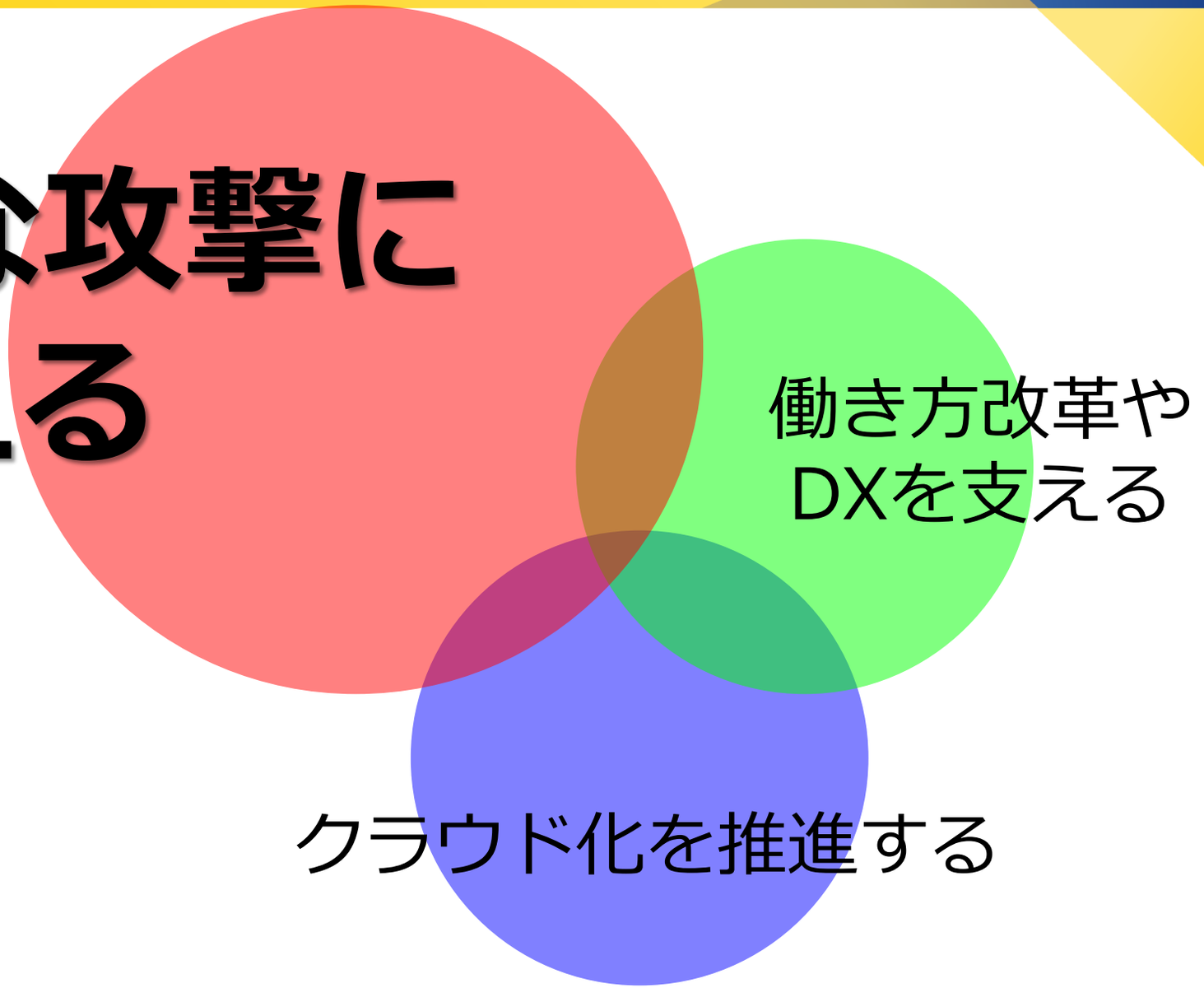


紙資料の印刷枚数の変化

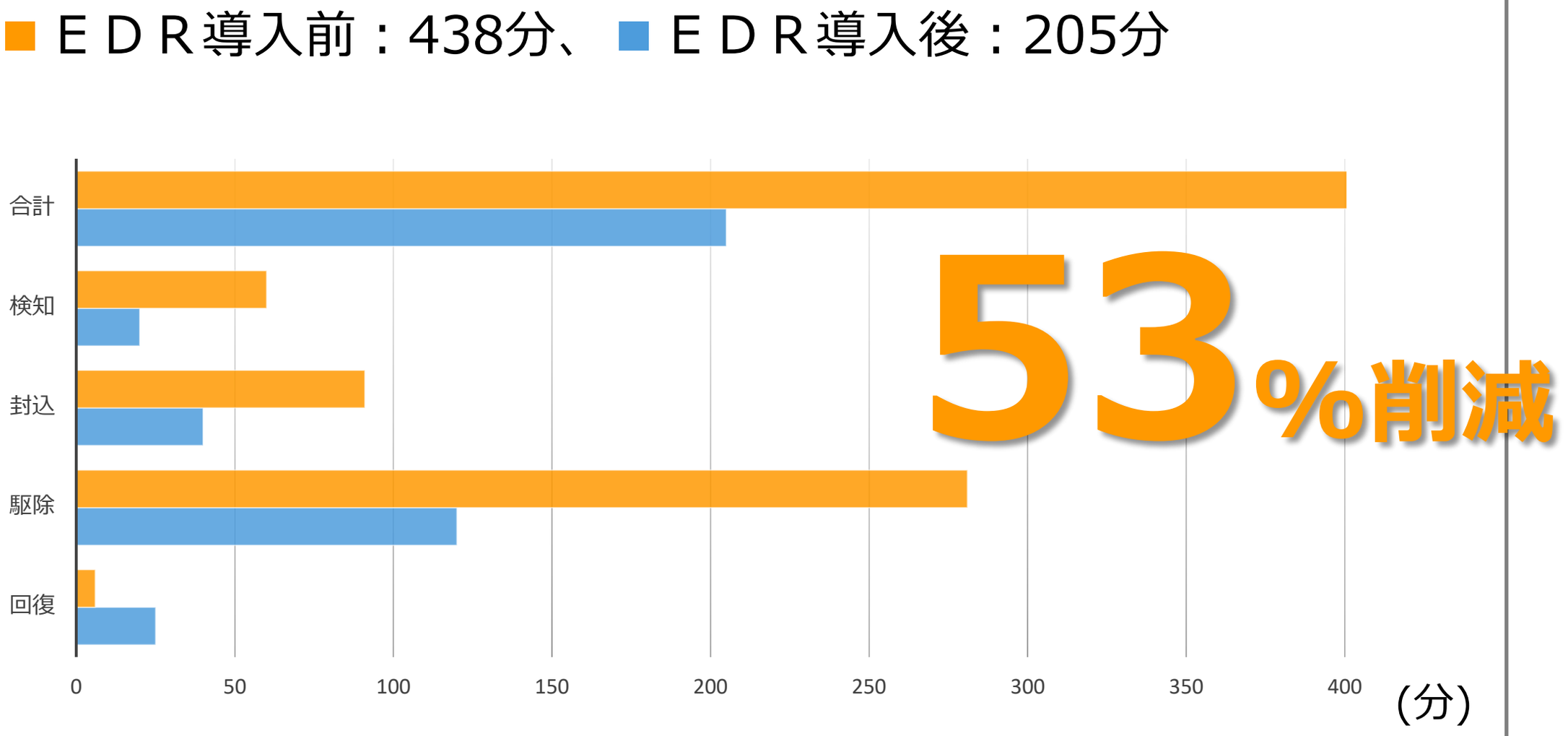


仕事の仕方が変わりだした瞬間・・・

2.高度な攻撃に備える

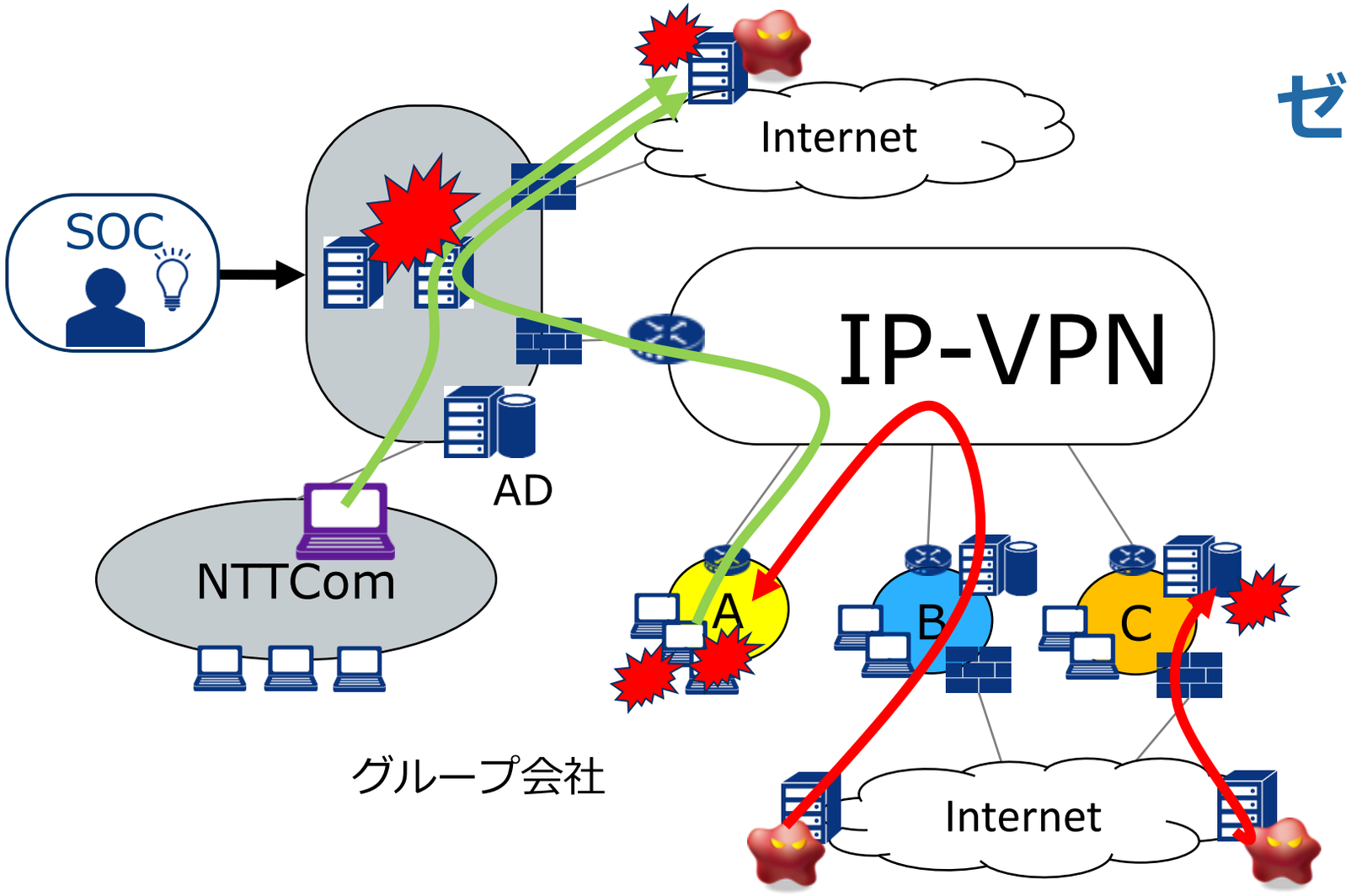


マルウェア感染時インシデント対応時間の短縮



グループ会社での攻撃検知の事例

グループ会社間の信頼関係 ≠ ネットワーク相互接続の可否

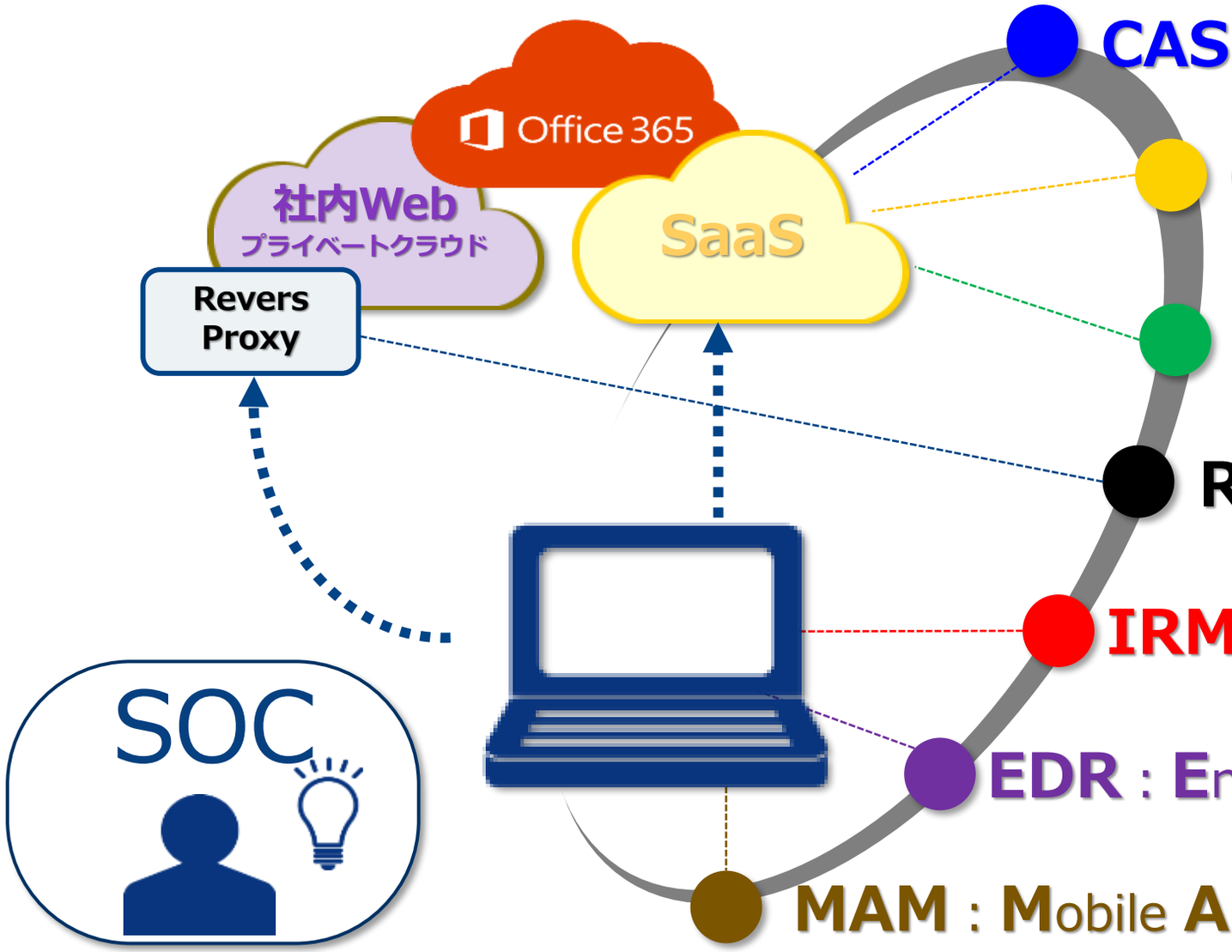


ゼロトラストで再構築

- ✓不要なネットワーク接続の切り離しと通信の絞り込み
- ✓ID管理の徹底と、各社ADの信頼関係を再点検
- ✓APT攻撃から会社を守るためEDRを全端末に導入

攻撃に備える→過度の信頼をしない「ゼロトラスト基盤」の実現

SaaSやクラウドにシームレスにアクセスするために



CASB : **C**loud **A**ccess **S**ecurity **B**roker

Cloud Proxy

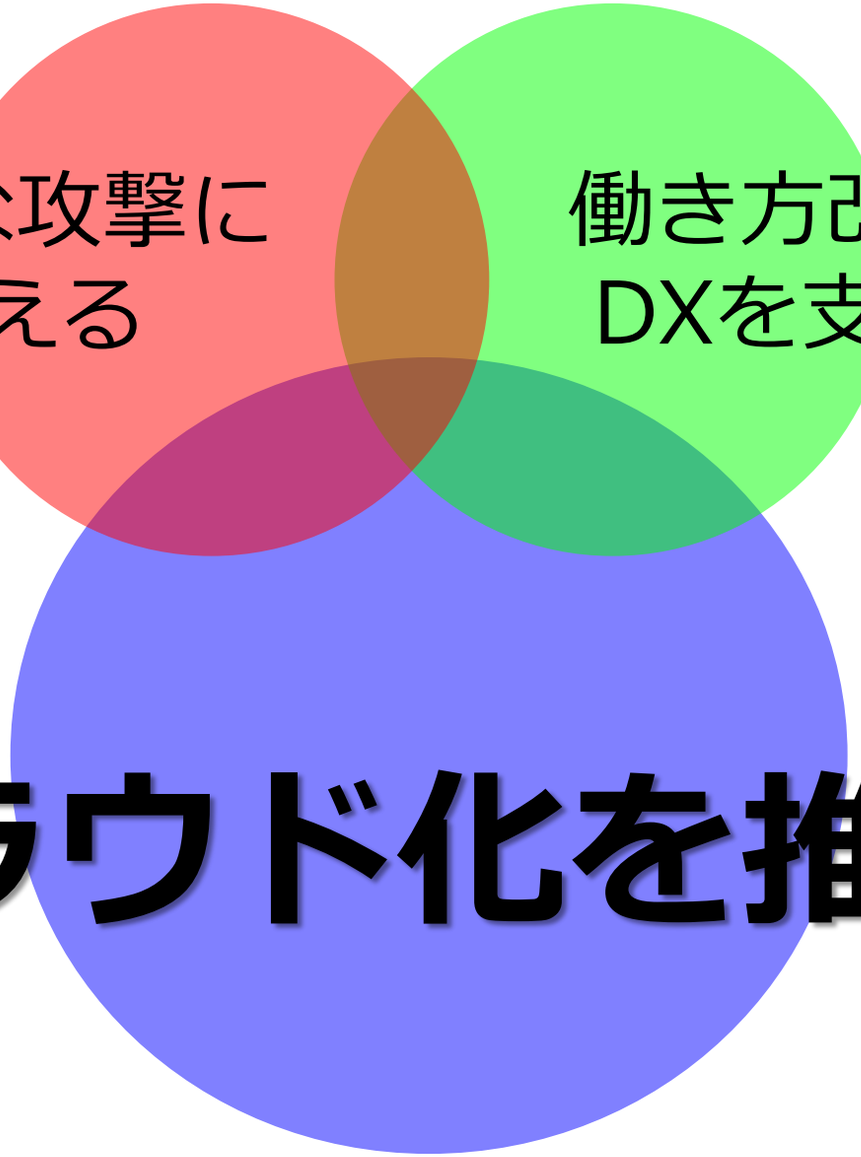
iDaaS : **Id**entity **a**s **a** **S**ervice

Reverse Proxy

IRM : **I**dentity **R**ights **M**anagement

EDR : **E**nd point **D**etection and **R**esponse

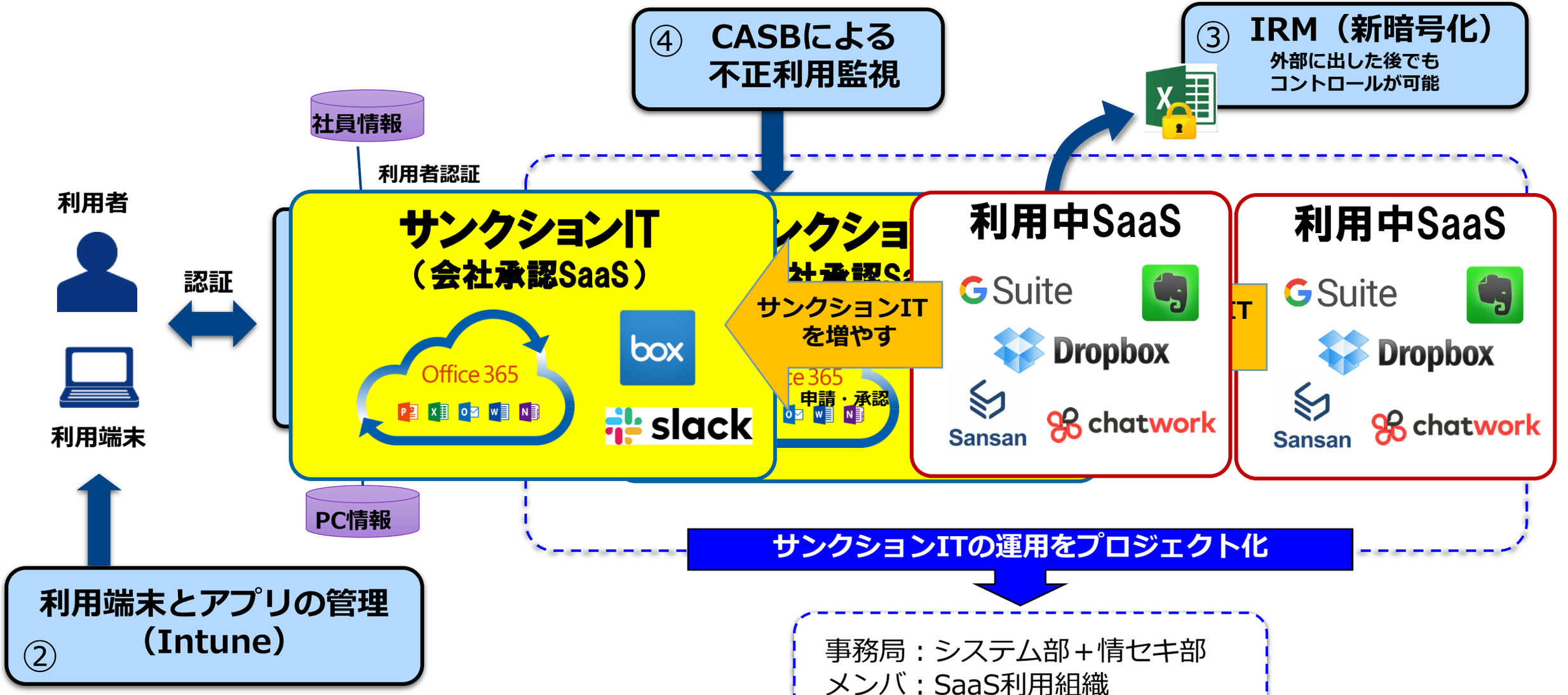
MAM : **M**obile **A**pplication **M**anagement



3.クラウド化を推進する

利用中SaaS → 会社承認「サンクションIT」≒ ゼロトラスト

ゼロトラスト基盤①②③④を活用し更なる生産性向上を目指す



クラウド化を推進するとは？

社内外で活躍するリテラシーの高い社員に最適なICT環境を追求していく

インフラ	オンプレミス中心	→	SaaS/クラウド中心
セキュリティ	境界防御のセキュリティ		ゼロトラストのセキュリティ
概要	インターネット境界を、IPSやサンドボックス等の多層防御で守る（外は危険・中は安全）		ノマドワークを前提に、クラウドと端末のセキュリティを強化し、アクセスの都度、認証・認可を行う
考え方	性弱説	→	性善説
マインド	不自由と閉塞感	→	適度な自由と緊張感

NTT Communications
Go the Distance.

ご清聴ありがとうございました


DIGITAL
TRUST

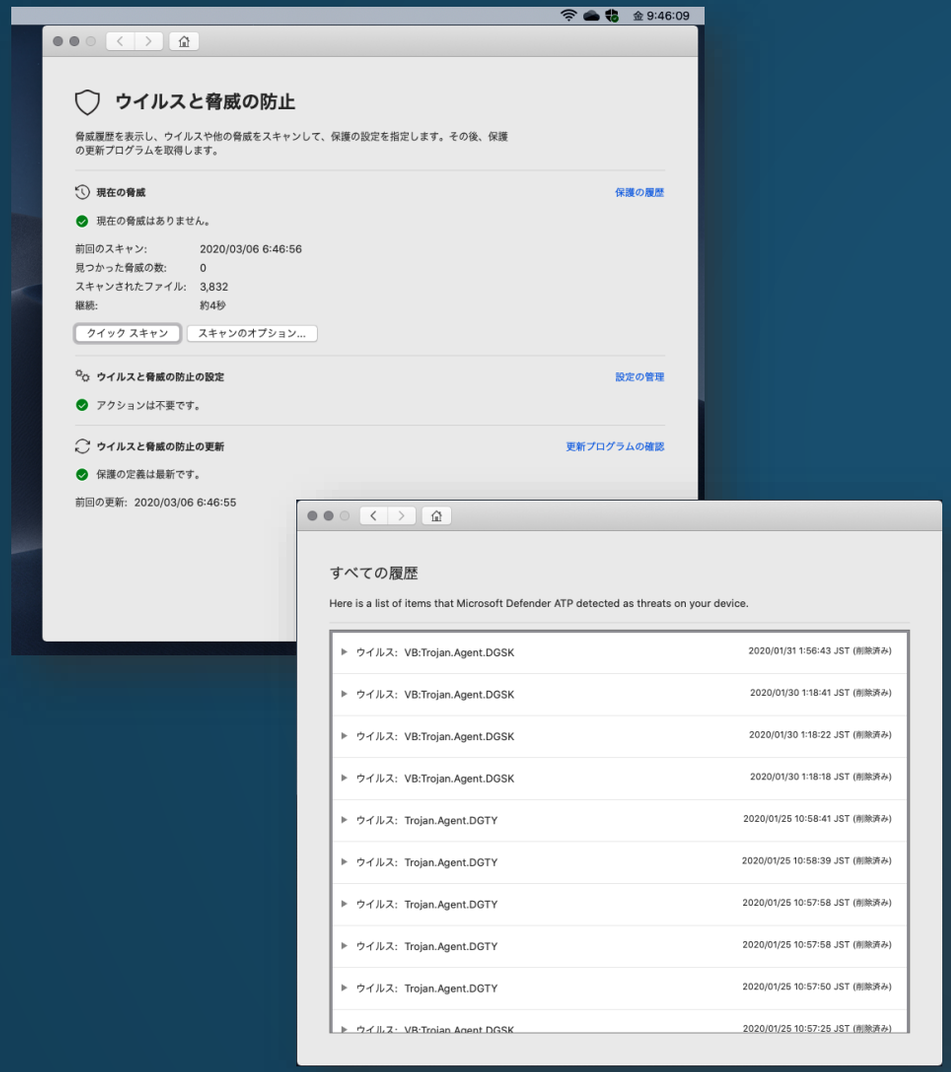
Microsoft Defender ATP のマルチプラットフォーム化

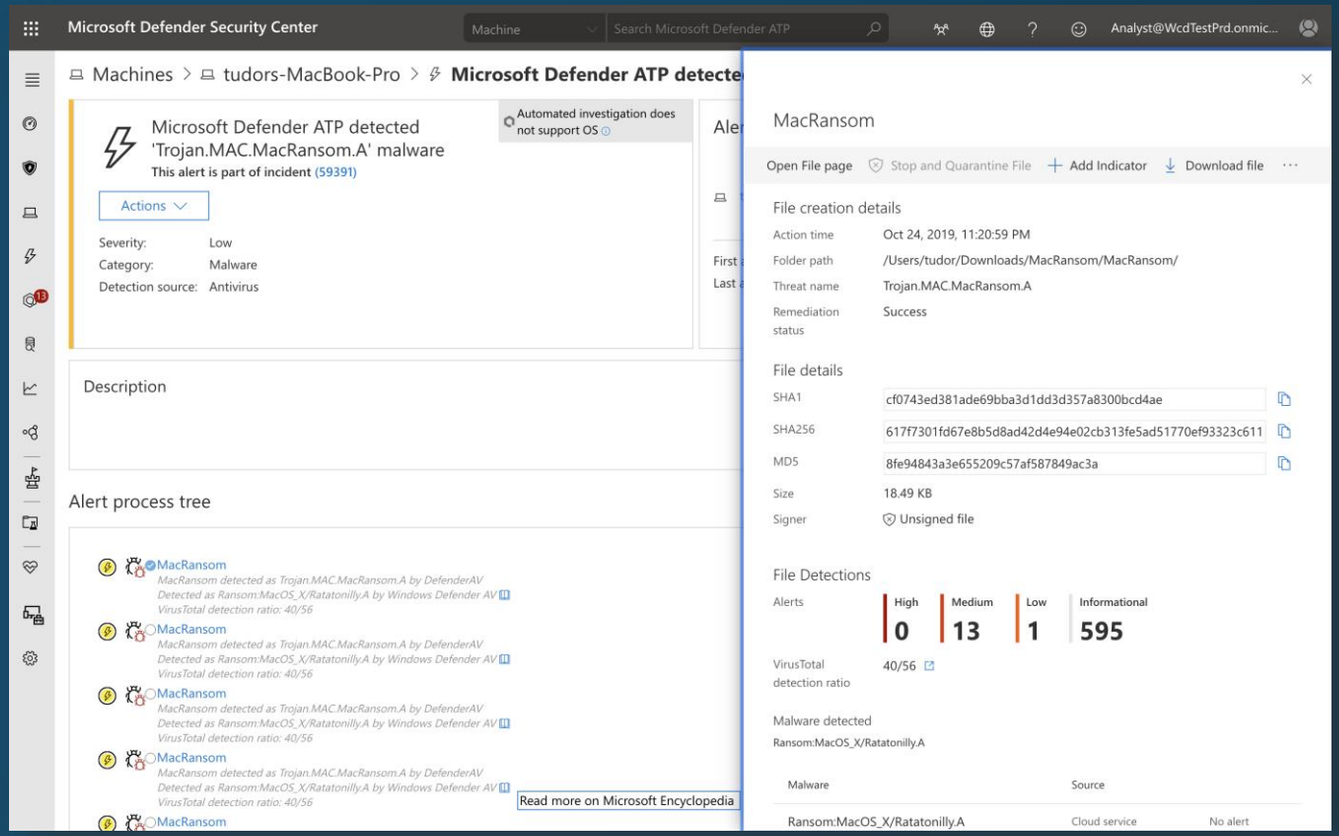
2016 年 **2019 年** **2020 年**

上記の全てのプラットフォームにおいて、アンチマルウェア機能と EDR 機能を提供
さらに、脅威・脆弱性管理や改竄対策なども提供予定

DIGITAL TRUST

Mac 本体でも、ダッシュボードでも統合化された環境で





DIGITAL TRUST

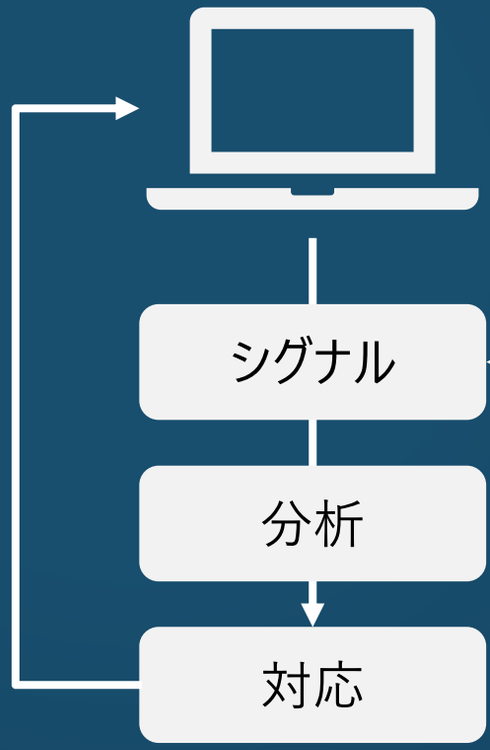
EDR の時代から、xDR の時代へ

2011 年

2015 年

2017 年

ゼロトラストによって、
ネットワークセキュリティから
エンドポイントセキュリティに



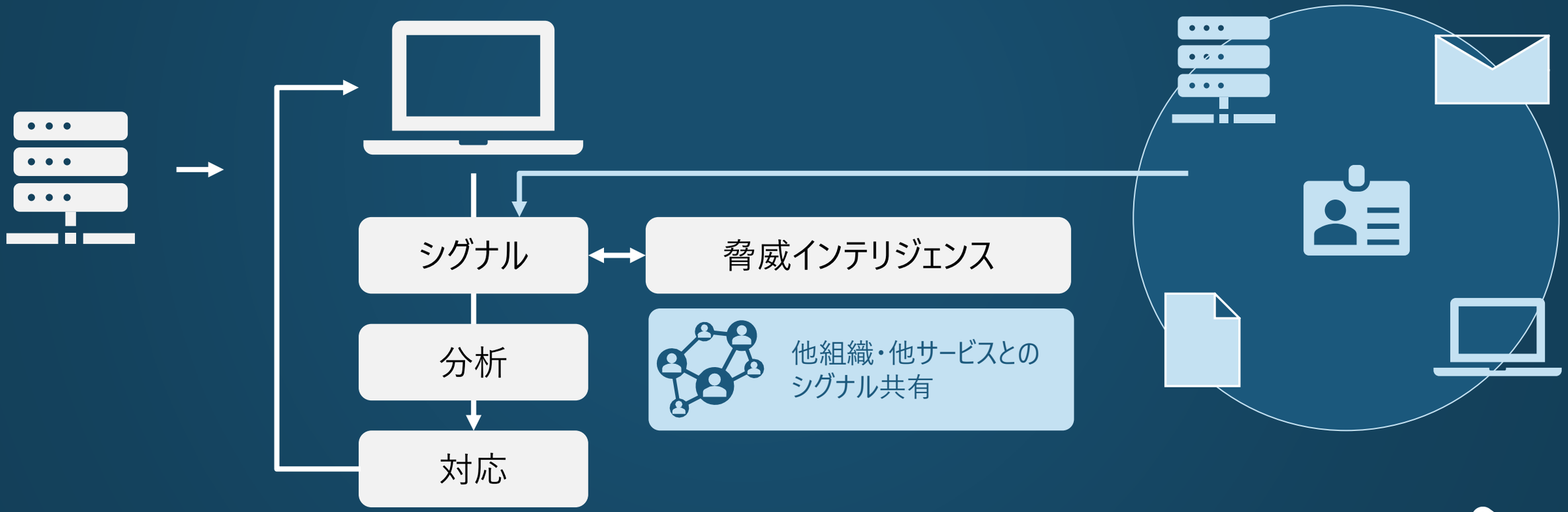
脅威インテリジェンス

他組織・他サービスとの
シグナル共有

DIGITAL TRUST

EDR の時代から、xDR の時代へ

2011 年　2015 年　2017 年　2019 年



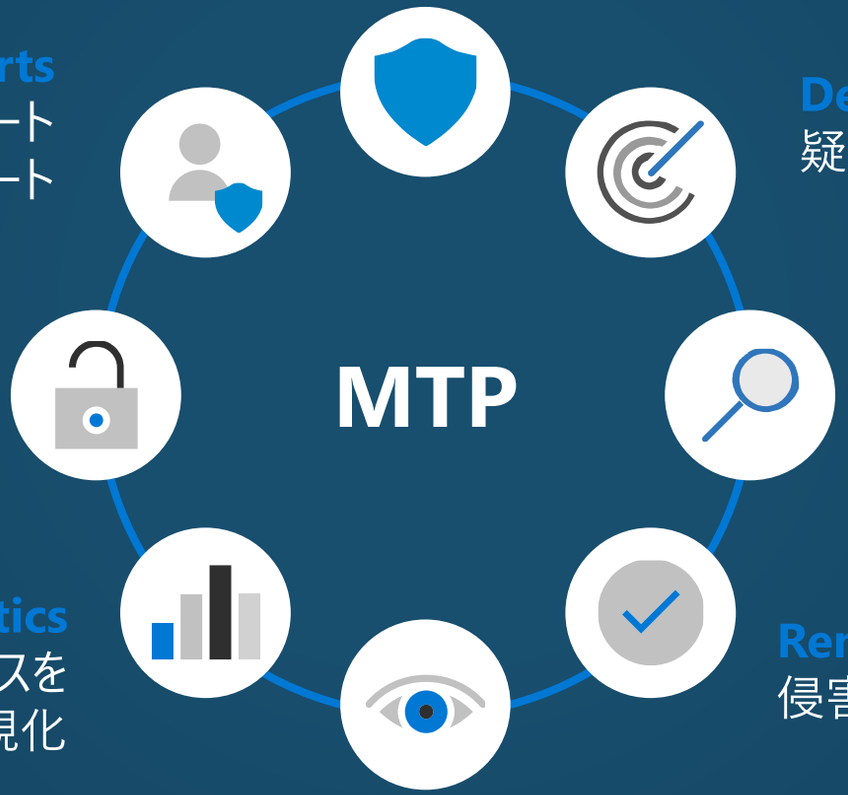
Microsoft Threat Protection の機能

Protection
脅威の防止とブロック

Threat Experts
ワールドクラスのセキュリティエキスパート
からのサポート

Detection
疑わしい動作の識別

Vulnerability
アプリ、OSの脆弱性と
構成ミスの発見



Investigation
攻撃全体の流れの可視化

Threat Analytics
豊富な脅威インテリジェンスを
活用した世界的な脅威の可視化

Remediation
侵害された資産を自動的に対処

Hunting
隠れた脅威の発見

DIGITAL TRUST

demo :
Microsoft Threat Protection

DIGITAL TRUST

Active incidents

18 active incidents

Last 30 days

Assigned incidents (6)

Unassigned incidents (12)

Informational Low Medium High

Incident name	Severity	Active alerts	Scope	Assigned to	Last activity
MTP Incident - 03/...	High	2/50	14 5 2	secops@MTPDem...	March 11, 2020
MDATP Incident - 0...	High	45/59	5 5 0	Unassigned	March 8, 2020 5:
MTP Demo Inciden...	High	10/10	4 1 1	Unassigned	March 8, 2020 4:
MTP Incident - 03/...	High	31/37	3 2 1	Unassigned	March 8, 2020 4:
3866	High	1/36	3 1 1	admin@MTPDemo...	March 2, 2020 8:

View all active incidents

Users with threat detections

Users with threat detections

User	Alerts
MTP Global Reader	30
SecurityOps Analyst	16
Barbara Moreland	12
MOD Administrator	9
Gail Erickson	3

Show more

Devices at risk

8 devices at risk

Device	Risk level
robertot-pc	High
barbaram-pc	High
mtp-air-dc01	High
aarifs-pc	High
lolas-pc	High
andrewf-pc	Medium
deborahp-pc	Medium
mtp-air-web01	Low

View details

Microsoft Secure Score

Secure Score: 41%

38/93 points achieved

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Score last updated 2020/03/10

60%

40%

Users at risk

12 users at risk

High Risk Medium Risk Low risk

Devices with active malware

4 affected device(s)

Intune-managed devices with active, unresolved malware

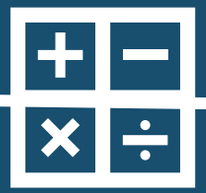
Updated Today at 7:11 AM

Active No Active Malware

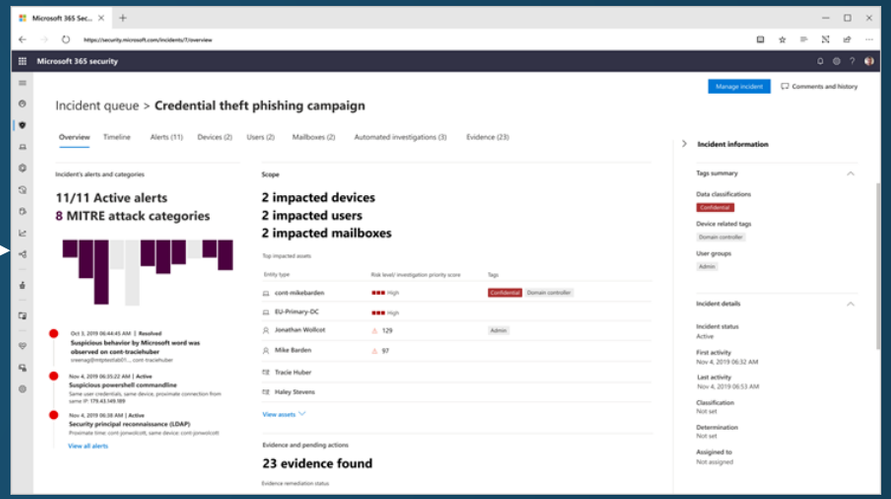
Give feedback

xDRによるアラート増加をAIとIdで集約してシンプルに

増え続けるアラートを
Idによるログの関連性の作成



AIによるアラートの
正当性の確認



アラートの集約による
対応の迅速化

DIGITAL TRUST

組織全体にわたって、資産を保護

インシデントの優先付け

- 重大な脅威情報をマイクロソフトのサービス内でリアルタイム
- 重大な脅威を優先的に表示

安全な状態の維持

- AIや自動化により脅威の調査や対応が行われ、侵害された資産を安全な状態に復旧
- インシデント対応にかかる時間やリソースを最適化

詳細な調査

- 組織固有の課題に対して、個別のクエリーを作成して詳細なログの調査を行う
- 組織に固有な脅威や脆弱性を発見

DIGITAL TRUST

Microsoft
DIGITAL TRUST SECURITY

Microsoft Security Forum 2020

株式会社資生堂
情報セキュリティ部長 (CISO)

斉藤 宗一郎 様

資生堂が目指す
情報分類・活用・監視のガバナンス

2020/3/12

(株)資生堂　CISO 斉藤宗一郎

SHISEIDO

Basic Rule of Security

You can’t MANAGE what you can’t SEE.
見えないものは管理できない。

You can’t PROTECT what you can’t Manage.
管理できないものは守れない。

SECURITY

AGENDA

1 規程類の形骸化という課題

2 ツールの活用の必要性

3 データの所在の変化

SECURITY

AGENDA

1 規程類の形骸化という課題

2 ツールの活用の必要性

3 データの所在の変化

1. 規程類の形骸化という課題

規程類が形骸化しないためにとるアクション

- 社内掲示板への掲載
- 部会などでの周知
- e-ラーニングなどを通じた研修・テストの実施

どうして規程類は形骸化するのか？

- 現場は千差万別で解釈が必要
- 守れないことをルールにしている
- アクションをとったことで満足

SECURITY

AGENDA

1 規程類の形骸化という課題

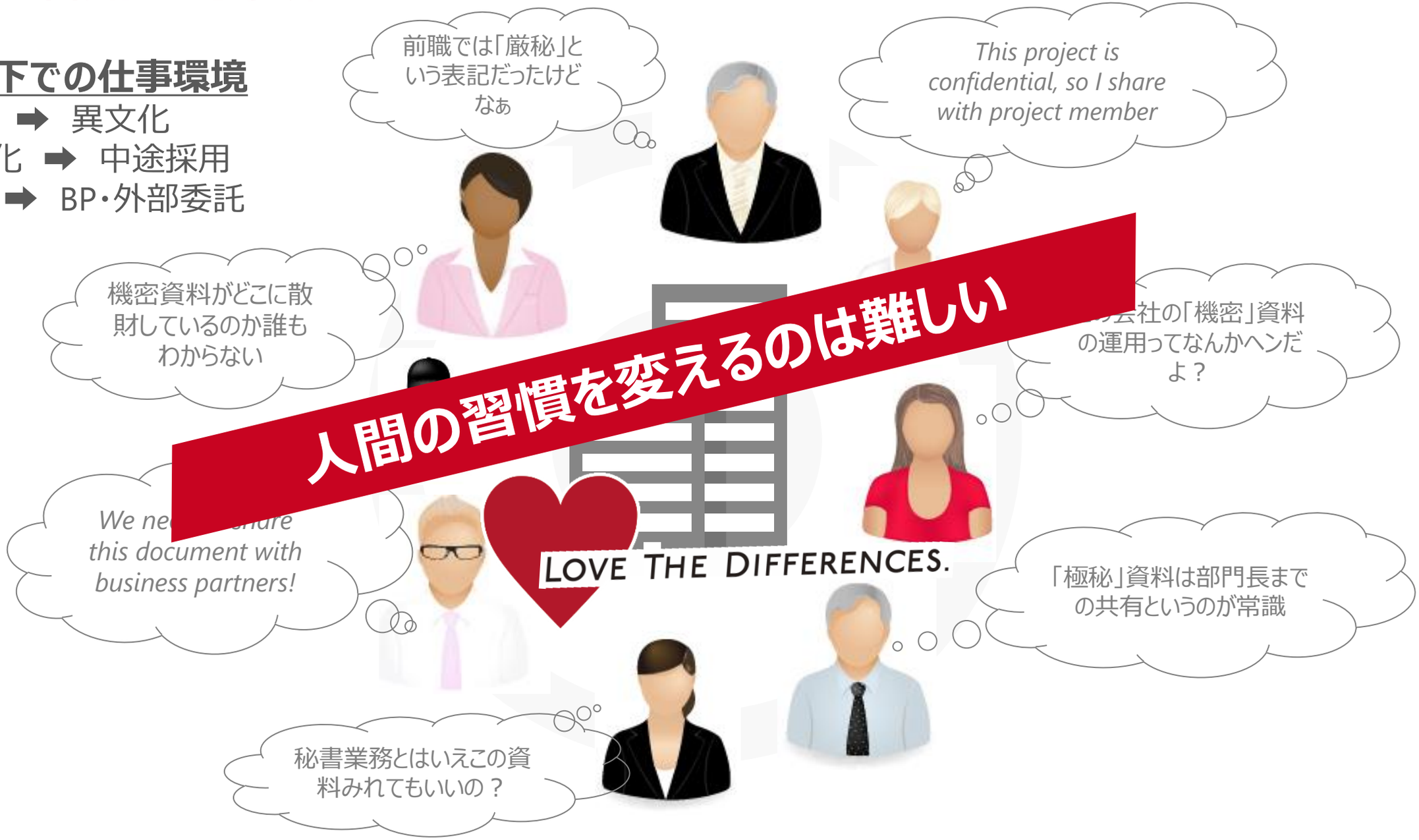
2 ツールの活用の必要性

3 データの所在の変化

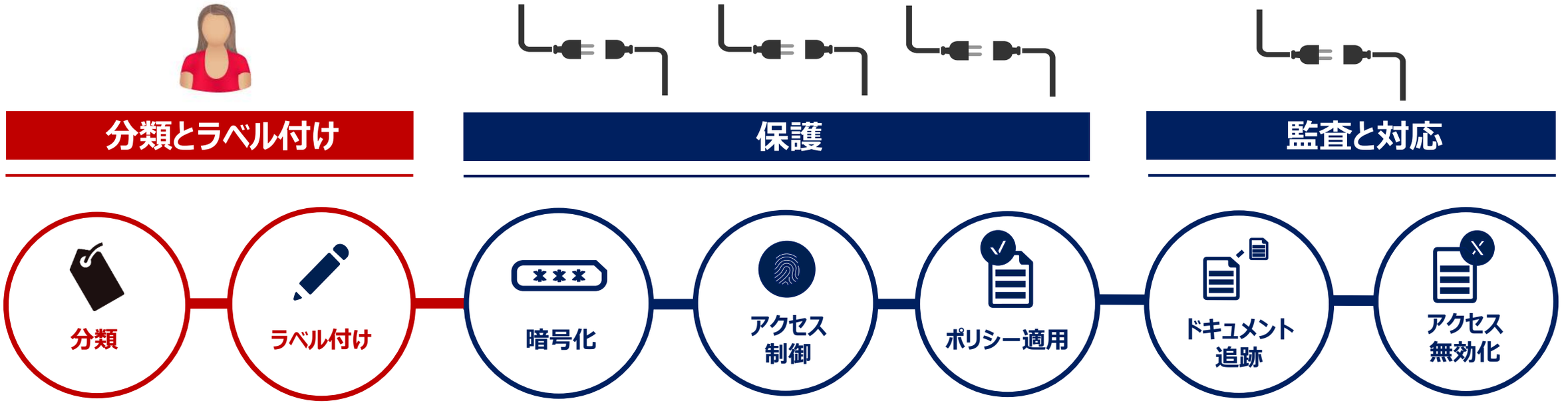
2. ツールの活用の必要性

ダイバーシティ下での仕事環境

- グローバル化 ➡ 異文化
- 人材の流動化 ➡ 中途採用
- エコシステム ➡ BP・外部委託



2. ツールの活用の必要性



- 従業員がそれぞれAzure Information Protection(AIP)を活用して、ドキュメントの機密レベルの分類をし、適切なラベルをつけるだけ
- ツール(AIP)がポリシーに従って適切にデータを保護してくれることにより、規程類の遵守が高まり形骸化を防ぐ

ツールによって規程類を意図せずとも遵守することが可能となる

SECURITY

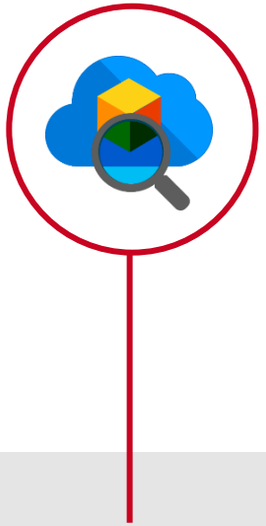
AGENDA

1 規程類の形骸化という課題

2 ツールの活用の必要性

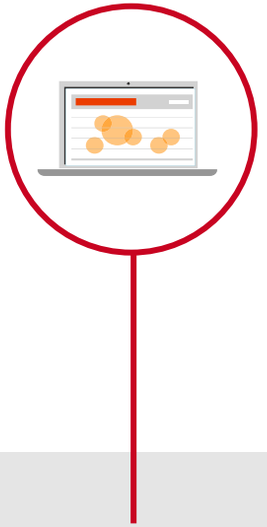
3 データの所在の変化

3. データの所在の変化



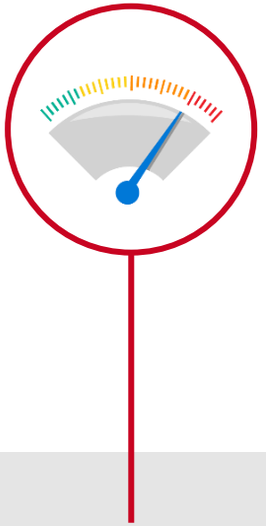
クラウド活用の急増

- ビジネス部門におけるクラウド活用のニーズの高まり
- スピード・コスト面が優先されやすい



外部委託先とのデータ共有の急増

- 多様化するデータの共有方法
- スピードや利便性が重要



シャドーITの問題

- 守るべき情報の可視化ができない
- IT部門としての統制の問題

データの所在が変化しても正しくラベリング・データ分類されていればリスクの低減ができる

SUMMARY


資生堂ではダイバーシティ
を積極的に進めています
LOVE THE DIFFERENCES.


適切に規程類を策定し、周知活動を
行っても人材の流動化により
形骸化していきます


しかし、文化や価値観が異なる環境
下で重要な情報を適切に守ることは
容易ではありません


ダイバーシティ下でも従業員が最低
限の労力で規程を遵守できるよう
ツールを導入しました

Basic Rule of Security

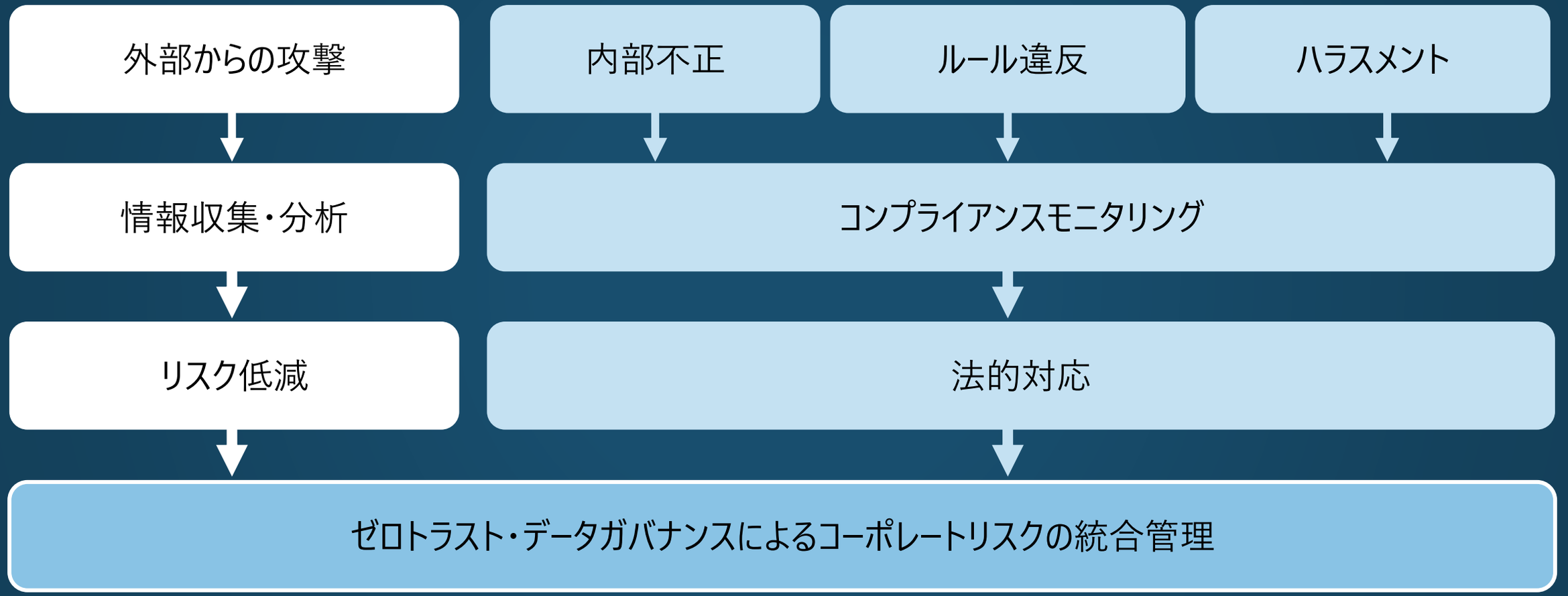
People are the fundamental
人は石垣、人は城

There is NO GOAL but Security is a Habit
セキュリティにゴールはなく習慣


SHISEIDO


DIGITAL
TRUST

安全の確保は外部からの攻撃だけではありません

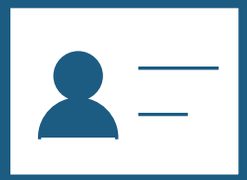


DIGITAL TRUST

内部不正検知ソリューションを提供開始

DX、データガバナンスによる
データの流れの把握

×



IDaaS による
人のふるまいの把握

＝

内部不正対策

インサイダーリスクマネジメント

内部不正

ルール違反

ハラスメント

DIGITAL TRUST

demo :
インサイダーリスクマネジメント

DIGITAL TRUST

内部リスクの管理

ナビゲーションから削除

内部リスクの設定

概要　アラート　ケース　ポリシー　ユーザー　通知テンプレート

ポリシーによって検出されるアクティビティをユーザーが実行したときに、ポリシーのアラートがトリガーされます。これらのアラートを確認して、詳細な調査のためにケースに追加するか、無視できる場合は消去します。詳細情報

確認対象のアラート

0 件のアラートが確認が必要です

過去 30 日間のオープンになっているアラート

アラートを解決するのにかかった平均時間

重要度 (高) のアラート
解決までの時間は利用できません

重要度 (中) のアラート
解決までの時間は利用できません

重要度 (低) のアラート
解決までの時間は利用できません

エクスポート　3 件のアイテム　検索　フィルター

アラート	状態	アラートの重要度	検出された時間	ケース	ケースの状態
Yu Shinagawa (3)					
顧客情報と売上情報の取扱事案	確認済み	中	1時間前	情報持ち出し確認A	アクティブ
データ漏洩監視	確認済み	中	4日前	情報持ち出し確認A	アクティブ
機密情報の取り扱い	確認済み	中	5日前	情報持ち出し確認A	アクティブ

ヘルプが必要ですか?　フィードバック

インサイダーリスクマネジメント

DX、データガバナンスによるデータの
流れの把握

×

IDaaS による
人のふるまいの把握

＝

働き方改革・生産性評価

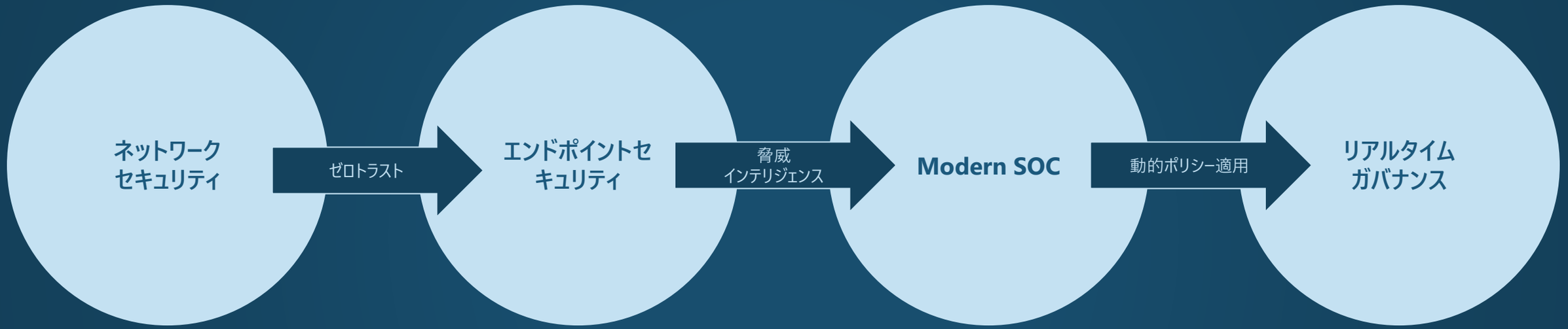
内部不正対策

同一リソースを活用した
部門連携によるリスク管理

DIGITAL TRUST


DIGITAL
TRUST

セキュリティの変化とこれから



Self-healing による、レジリエンスの実現

OS やアプリの進化、クラウド利用の推進によって、動的にガバナンスを構築でき、
動的ポリシー適用によって業務を止めることなく脆弱性対策を実行できるようになった

DIGITAL TRUST

ブレイクアウトセッションのご紹介

Session A		Session B	
A1	**ゼロトラストを DX の原動力に** ～ そのセキュリティ モデル、 DX の阻害になっていませんか? ～ 登壇者: クラウド & ソリューション事業本部 モダンワークプレイス統括本部　山野 学	**B1**	**Symantec 製品をご利用中のお客様に捧げる、 Microsoft セキュリティへの移行のススメ** クラウド & ソリューション事業本部 モダンワークプレイス統括本部 和田 健太
A2	**アクセス制御では防げない!? パスワード漏えいの仕組みと対策講座** クラウド & ソリューション事業本部 モダンワークプレイス統括本部　成田 翔	**B2**	**セキュリティ エコシステム時代の マネージド サービス パートナーの選び方** SB テクノロジー株式会社 松木 和彦 様 日本ビジネスシステムズ株式会社 秋葉 俊明 様 技術統括室 チーフ セキュリティ オフィサー 河野 省二
A3	**クラウドからエンドポイントまで 企業に内在するリスクを管理する** ～Microsoft Compliance ソリューションのご紹介～ クラウド & ソリューション事業本部 モダンワークプレイス統括本部　山本 明広	**B3**	**Azure セキュリティのキーポイント - ソリューションとベスト プラクティス** クラウド & ソリューション事業本部 テクニカルスペシャリスト 大井 喜智
A4	**本日限り! MS の失敗と経験から学ぶ 社内コンプライアンスの過去・現在・未来** 業務執行役員 政策渉外・法務本部 副本部長 弁護士　舟山 聡	**B4**	**ゼロトラスト徹底議論～トラストは何処へ～** Microsoft 365 ビジネス本部 プロダクトマーケティングマネージャー　山本 築 株式会社クラウドネイティブ 代表取締役社長 齊藤愼仁 様 株式会社LayerX シニアセキュリティアーキテクト 鈴木 研吾 様

DIGITAL TRUST

Microsoft

Microsoft
DIGITAL TRUST
SECURITY

#digitaltrust