ＮＴＴコミュニケーションズの
「働き方改革×セキュリティ」

2019年3月
情報セキュリティ部長
小 山 覚

https://4travel.jp/travelogue/11176281?page=2

NTTコムに出没するキョンシー達

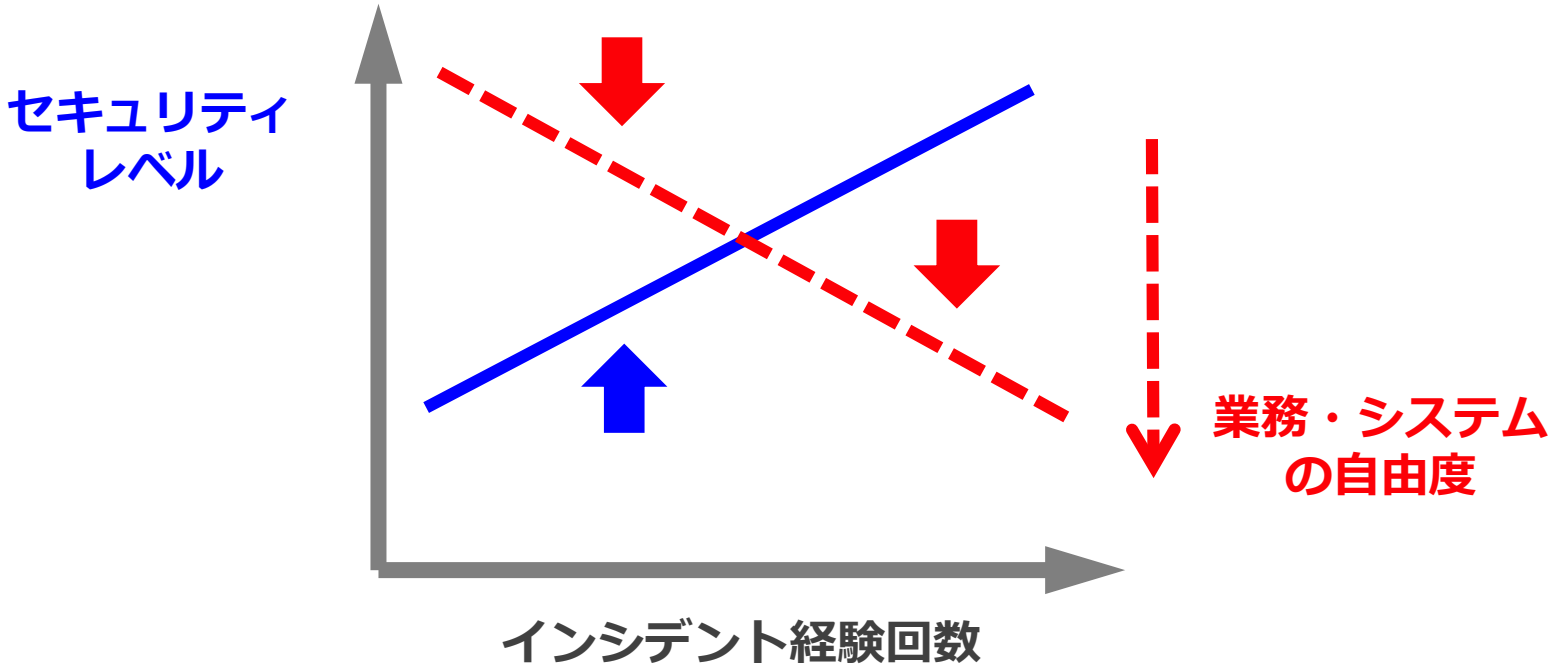
出展：Amazon：キョンシー コスチューム メンズ 180cm クリアストーン正規品

アジェンダ

1. セキュリティ対策のパラダイムシフト
2. 働き方改革に向けたセキュリティ対策の見直し
3. 費用対効果と歯止め（シャドーIT対策）

情報セキュリティ対策の現実 ≒ 弊害

セキュリティ原理主義は生産性低下や社員の思考停止を招く



クラウドに適したセキュリティ対策のリバランス

$$\text{セキュリティ推進力} = \frac{\text{① テクノロジー（新技術の導入）} \times \text{② オペレーション（監視・運用・社員教育）}}{\text{③ ユーザビリティ（利便性・自由度）}}$$

No ! → Yes !

生産性向上や社員のチャレンジを支えるセキュリティ

アジェンダ

1. セキュリティ対策のパラダイムシフト

2. **働き方改革に向けたセキュリティ対策の見直し**

3. 費用対効果と歯止め（シャドーIT対策）

働き方改革に向けたセキュリティ対策の見直し

現状のセキュリティ対策

技術的な対策

- 多層防護による標的型攻撃対策
  - SIEMによる不正通信の検知
  - 脆弱性対策の徹底

人的な対策

- セキュリティ教育の推進
  - 階層別セキュリティ教育・啓発
  - 標的型メール攻撃対応訓練
- OJTによる実践的な人材育成

組織的な対策

- セキュリティレベル測定によるグループガバナンスの強化
- CSIRTによるレジリエンス強化

見直したセキュリティ対策

PC環境の見直し

- 高度暗号化による会社パソコンの持出し解禁、社内外シームレスな環境を提供
- 改正個人情報保護法対応

クラウドへの対応

- O365等クラウドに完全対応することで、快適で利便性の高い環境を提供
- SIEMによる不正通信の検知をクラウド型にも拡大

生産性の向上

- ネットワーク分離型から、相互接続・API連携型のセキュリティ対策へ

技術的な
対策

- 多層防護による標的型攻撃対策
  - SIEMによる不正通信の検知
  - 脆弱性対策の徹底

攻撃の特徴

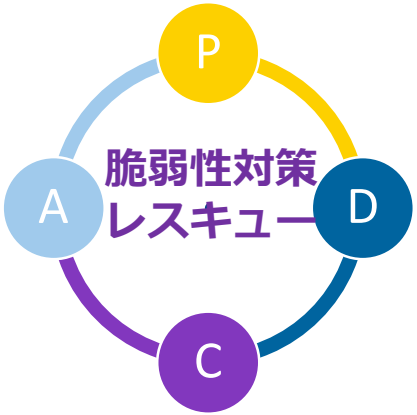
① URLブラックリストに登録されていないサイトから攻撃

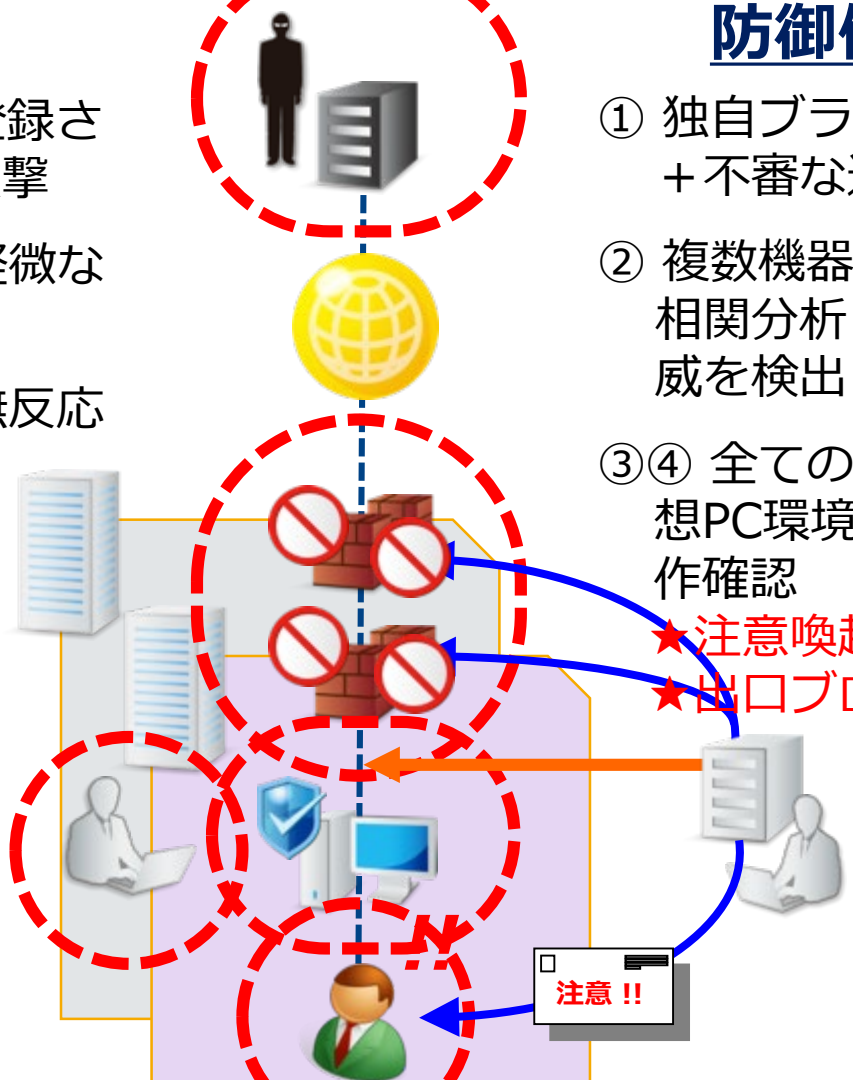
② 不正侵入検知装置では軽微な警報（常に新しい攻撃）

③ ウィルス対策ソフトも無反応

④ 標的（社員）も特定

⑤ システム環境も調査





防御側の対応策

① 独自ブラックリストの導入＋不審な通信先監視

② 複数機器の警報（ログ）を相関分析し、すり抜けた脅威を検出

③④ 全ての電子ファイルを仮想PC環境（Sandbox）で動作確認

★注意喚起メールの自動送信

★出口ブロック自動設定

Sandbox

2017年度実績

- マルウエアの感染対処件数　　132 件　（URLクリック含む）
- Webサイト等への不正通信件数　　90 件
- 情報漏洩等の被害件数　　0 件

PC環境の見直し

- 高度暗号化による会社パソコンの持出し解禁、社内外シームレスな環境
- 改正個人情報保護法対応

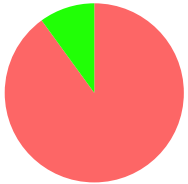
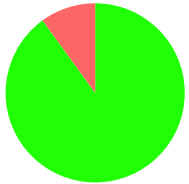
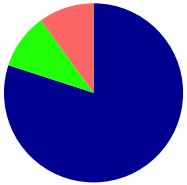
働き方改革に向けたクライアントPCの見直し

ファット・クライアント

シン・クライアント

セキュア・ファット・クライアント

移動中や自宅でも
ストレスのない作業環境

1999～（第１期）	2007～（第２期）	2018～（第３期）
		
ウィルス対策	ウィルス対策	ウィルス対策
	持出しPC	~~持出しPC~~
	持出し禁止	持出し解禁
	データレス	暗号化
	USB禁止	データバックアップ
		EDR

実装したセキュリティ対策の内訳

- 端末紛失・盗難による情報漏洩
- ユーザなりすましによるPC不正利用
- 外部記憶媒体による情報流出
- SaaSサービスを利用した情報漏洩
- メール誤操作による情報流出
- 不正アプリによる情報流出
- メール添付によるウィルス混入
- メール記載の悪性URLへの接続によるマルウェア感染
- ブラウザを活用した悪性サイトによるマルウェア感染
- 外部媒体USBによるウィルス混入
- ネットワークからの脆弱性攻撃
- アプリケーションの脆弱性を活用した攻撃
- 未知の攻撃（SIEM分析）

個人情報保護法における情報漏洩の扱いについて

個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合*

＊詳細は「電気通信事業における個人情報保護指針」を参照のこと

【一部抜粋】

漏えい等事案に係る個人データ又は加工方法等情報について、**高度な暗号化等の秘匿化**がされている場合

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

改正個人情報保護法に対応した情報管理の見直し

	従前より配備されていたPC			セキュア FAT
	オフィス専用PC（FAT）	持出専用PC（FAT）	シンクライアントPC	
PCの社外への持ち出し	持ち出し不可	管理者の承認を得て、持ち出し	制限なし	**制限なし**
情報の閲覧・更新	制限なし	持ち出した情報のみ可能	制限なし	**制限なし**
情報の保存	重要度等に応じた保存	返却時に全て削除	保存できない	**一時的な保存は可能、必要が無くなり次第、削除または管理区域へ移動**
情報の持ち出し	持ち出し不可	お客様情報等、機密情報は持ち出し禁止	持ち出せない	**取扱中のものについては制限なし**
端末の保管	施錠保管、ワイヤーロック	施錠保管	適切に保管（物損防止の観点）	**オフィスでの保管時は施錠保管**
盗難・紛失時の対応	重大な情報漏洩インシデントとして対応		物損事故として対応	**情報漏洩時のインシデント対応は不要**

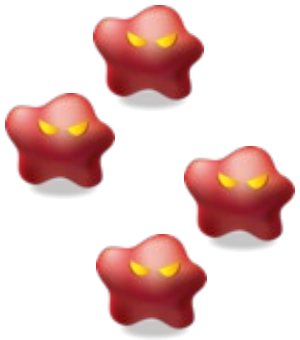
シンプルなゴールを設定して、トライアル開始

俺のMacを捨てさせてみろ！

セキュリティレベルは下げるな！

XXX 様に突っ込まれない理論武装

キョンシーを救え！

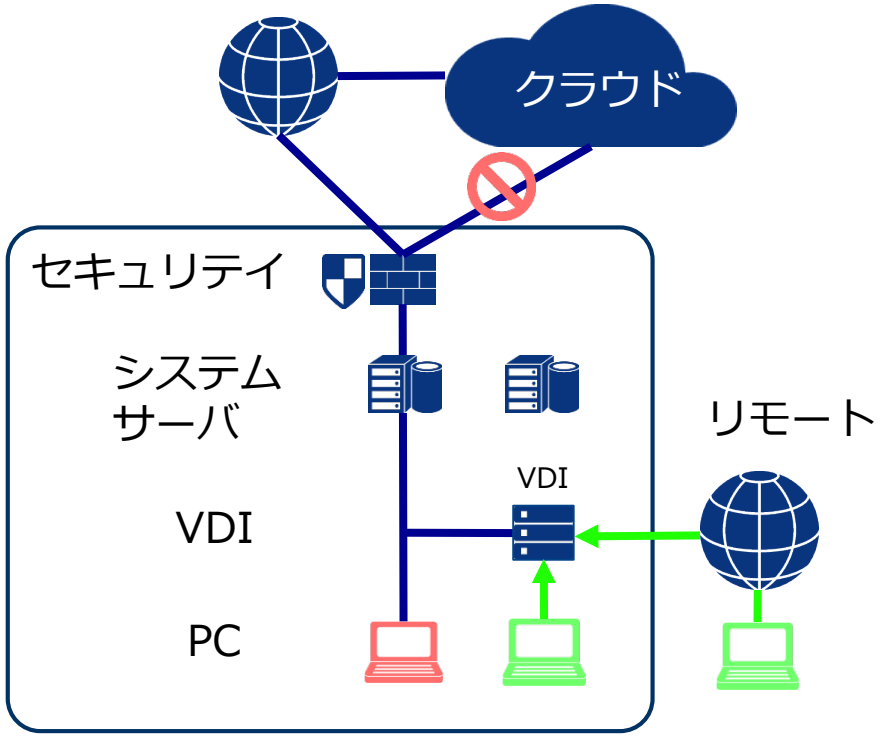


クラウドへの対応

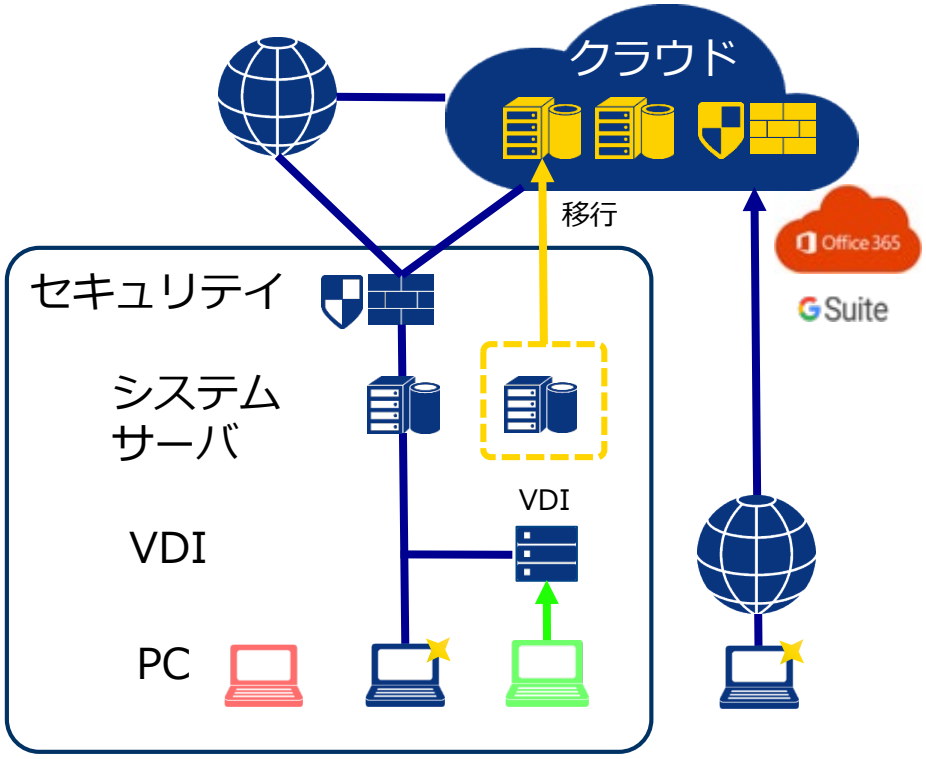
- O365等クラウドに完全対応することで、快適で利便性の高い環境を提供
- SIEMによる不正通信の検知をクラウド型にも拡大

クラウドへの対応イメージ

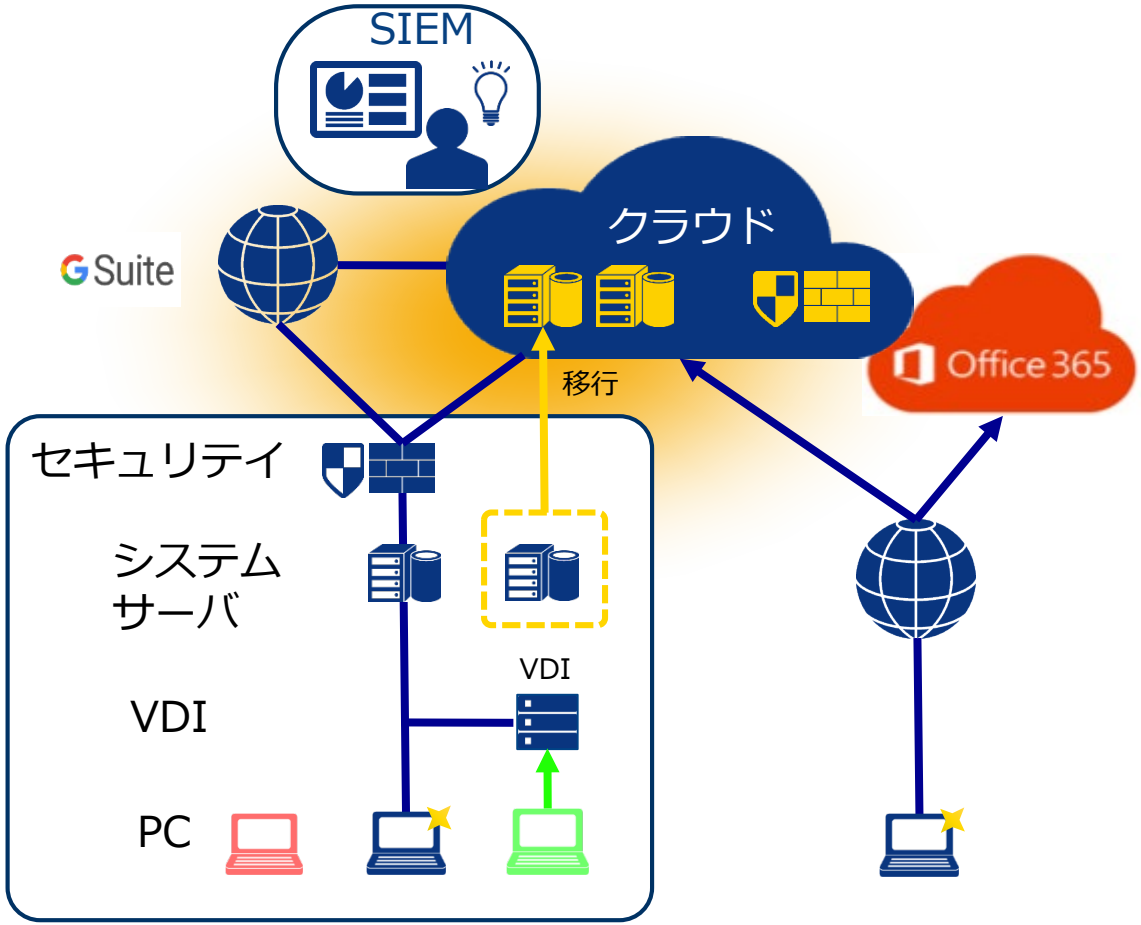
オンプレミス型（～2018）



クラウド型（2018～）



NTTコム版クラウド対応のレシピ



オンプレ＋クラウドのログの
総合分析を実施

Windows Defender ATP
Azure RMS
Cloud Proxy（CASB検討中）
O365
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
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
ATP/EDR

アジェンダ

1. セキュリティ対策のパラダイムシフト

2. 働き方改革に向けたセキュリティ対策の見直し

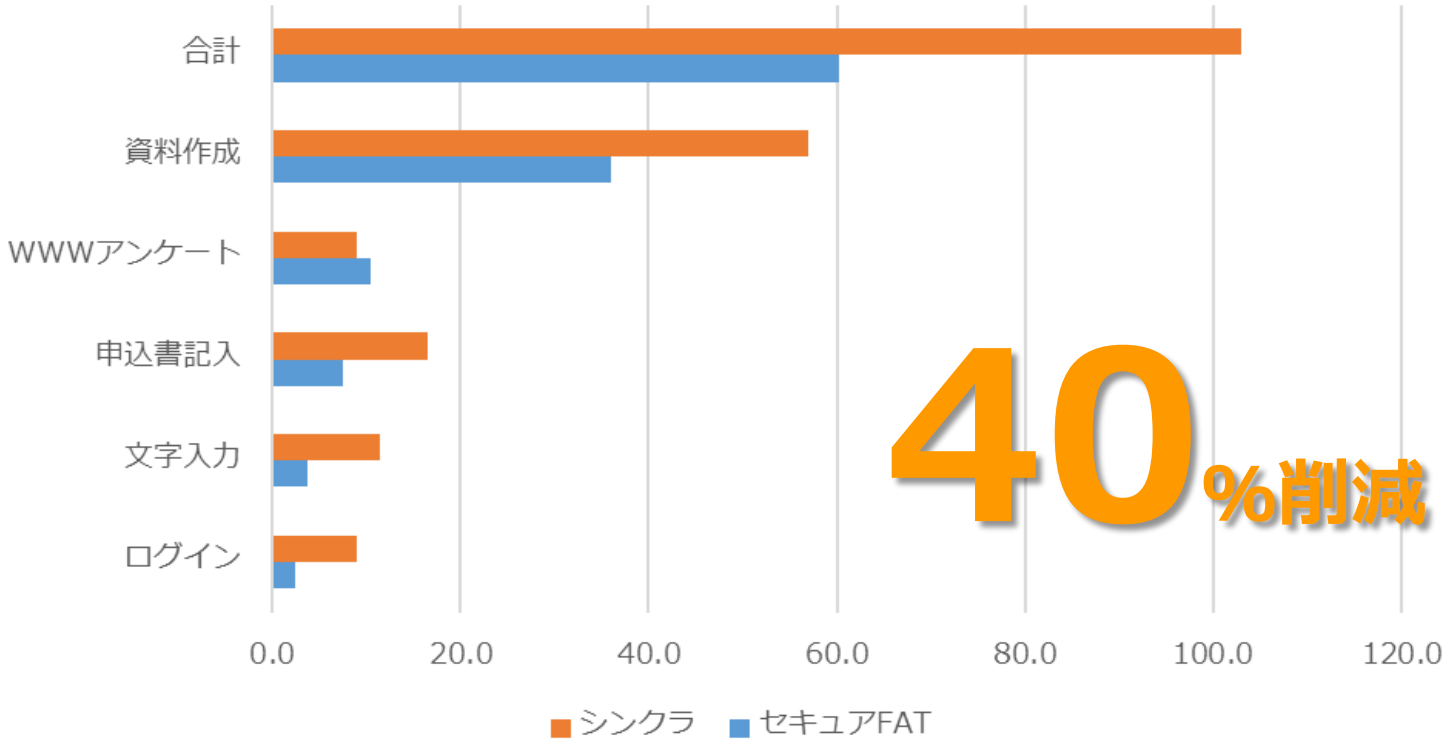
3. 費用対効果と歯止め（シャドーIT対策）

生産性の向上（作業時間）

24～40% 削減

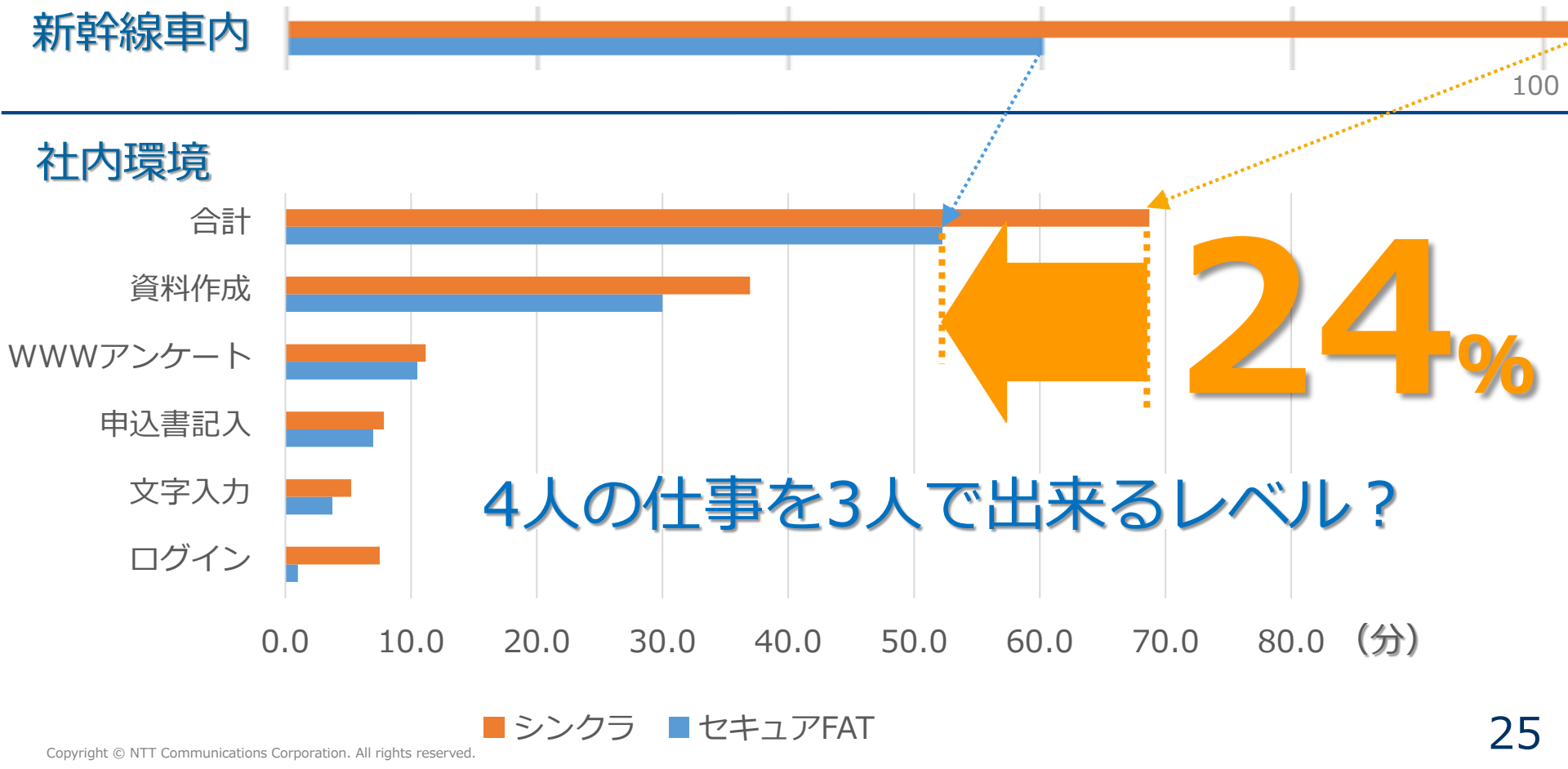
新幹線車内での作業効率の比較

シンクラ100分 → ファット60分



40%削減

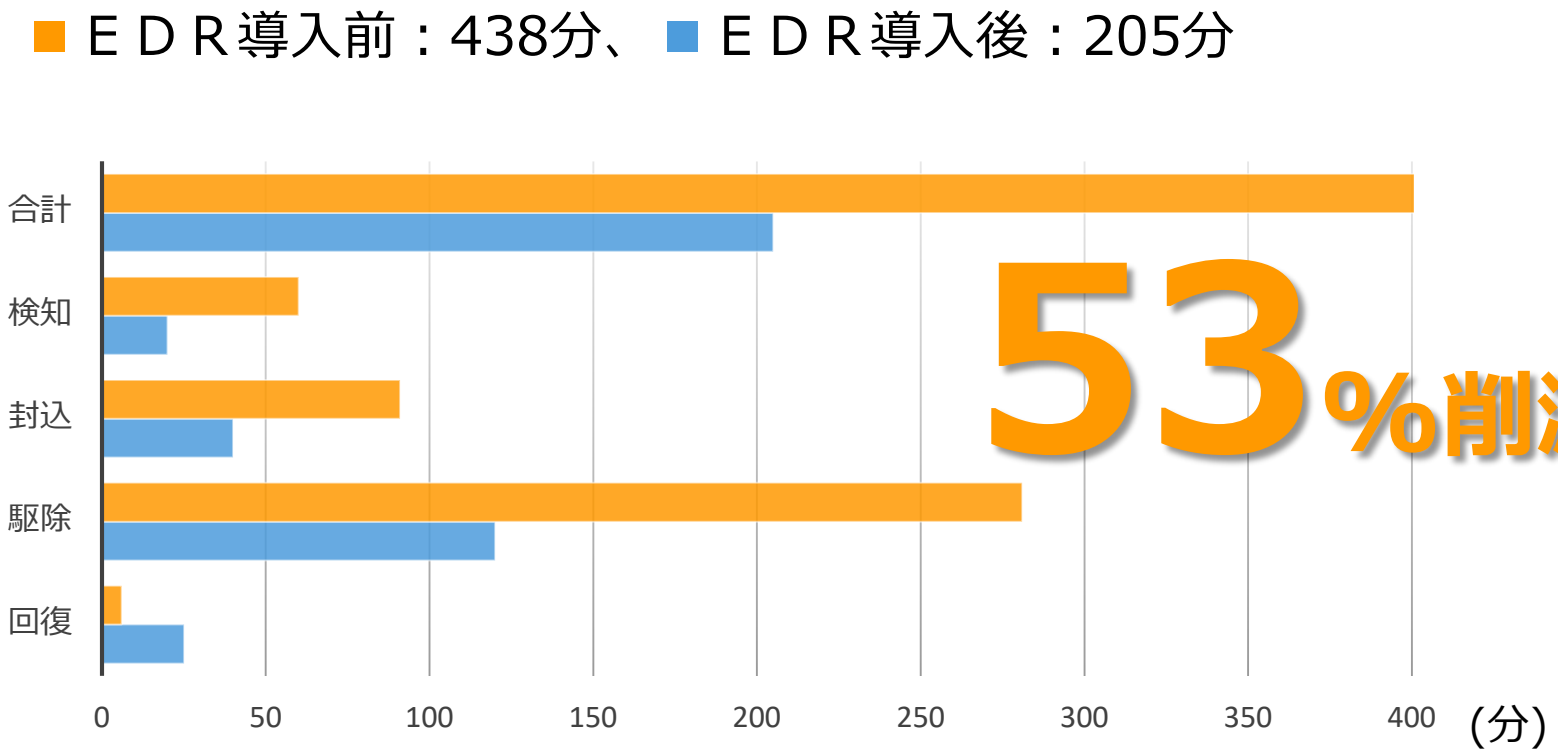
社内環境の生産性比較



セキュリティ
（インシデント対応時間）

53～82% 削減

マルウェア感染時インシデント対応時間の短縮

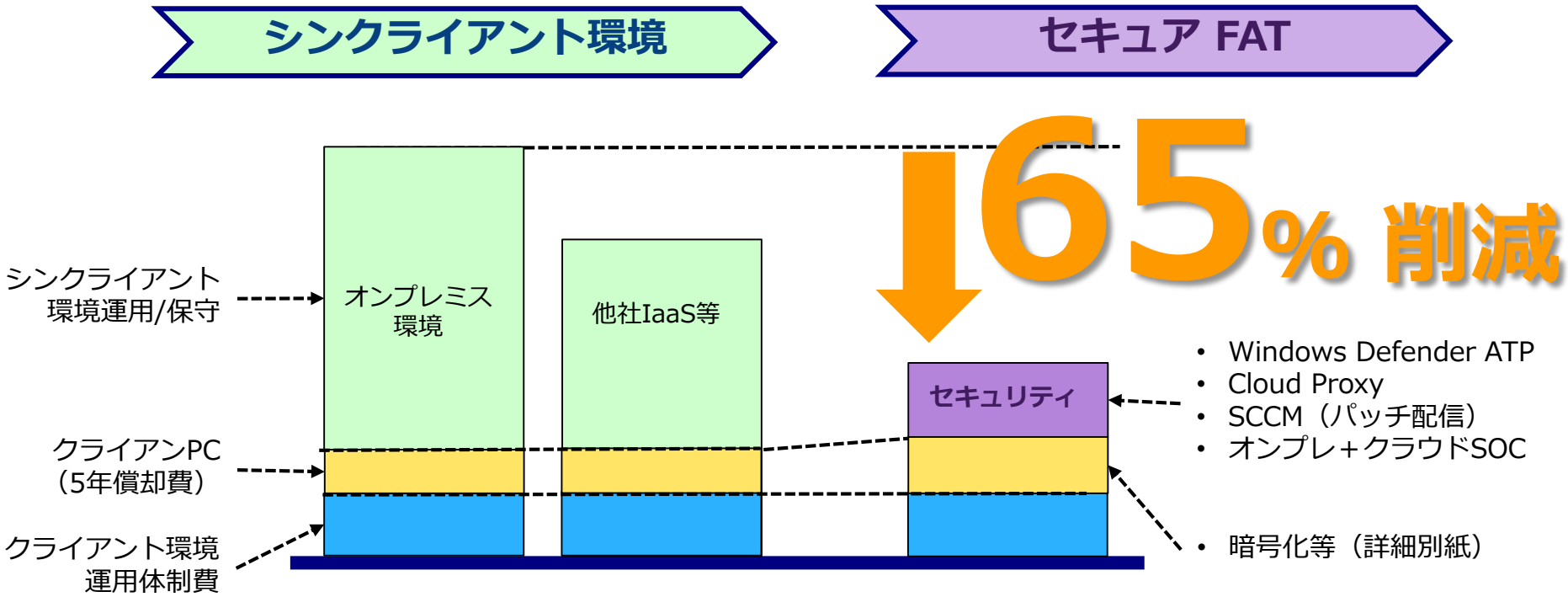


※2018年9月の数値、現在はEDRの運用習熟により更に時間が短縮している

クライアント環境のコスト

65% 削減

クライアントPC 10,000台規模での経済比較



作業の快適性

10ポイント向上

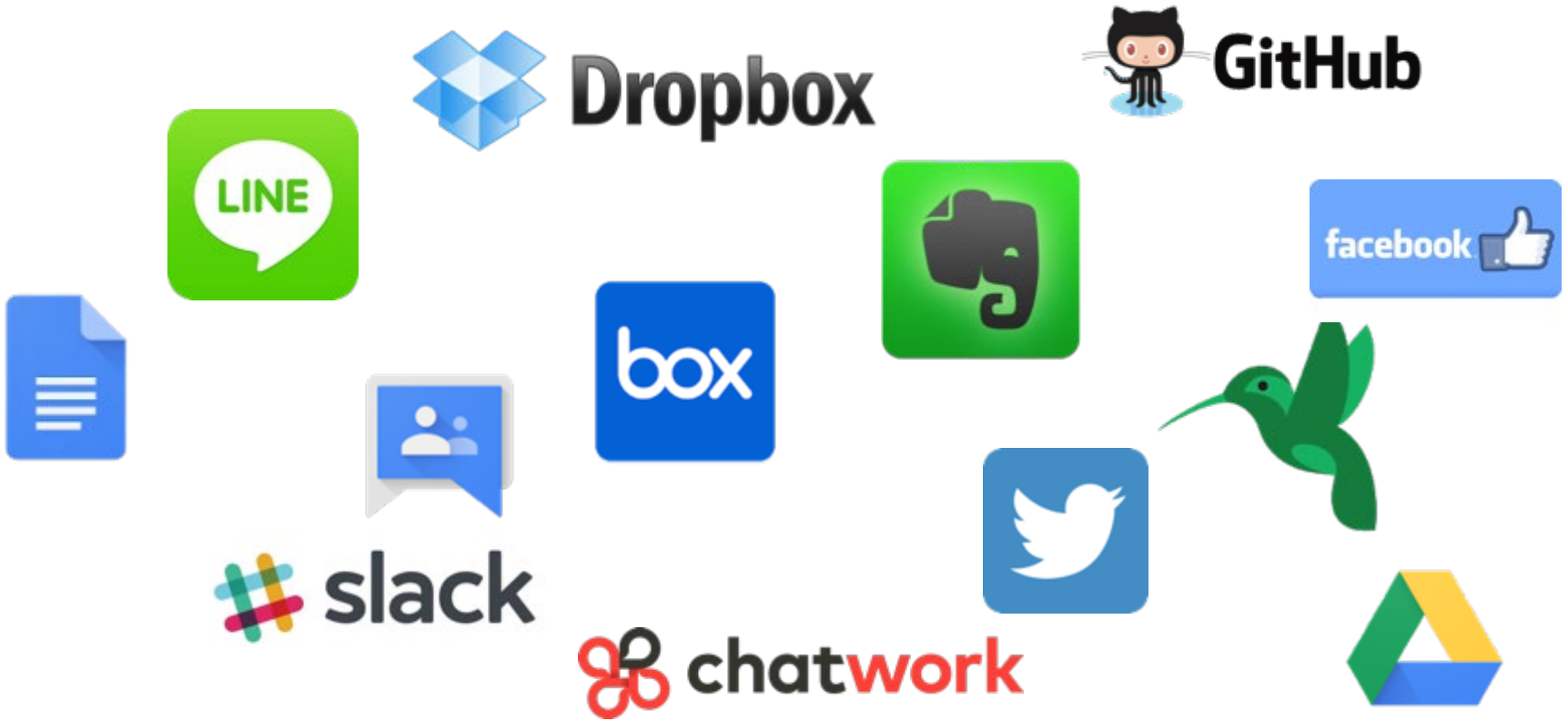
快適性の比較

社員の気分を10分間隔で測定

デジタルトランスフォーメーション に向けた取り組み

シャドーITのすすめ

みなさん使ってますか？

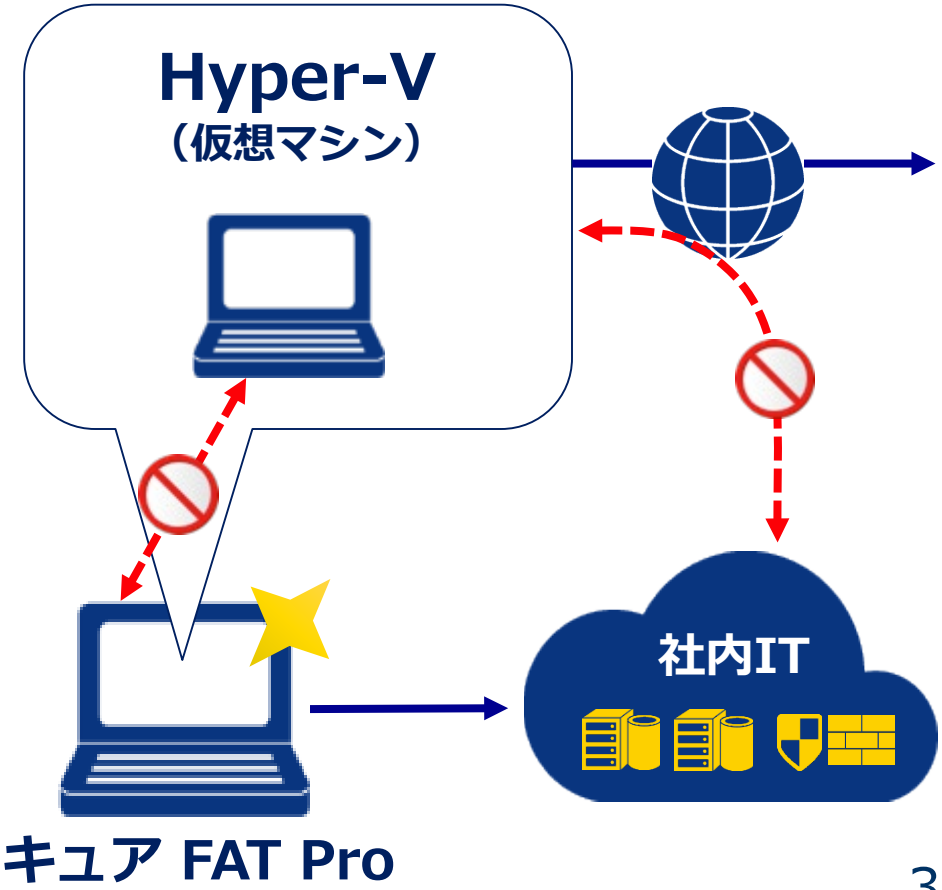


俺のMacを捨てさせてみろ！

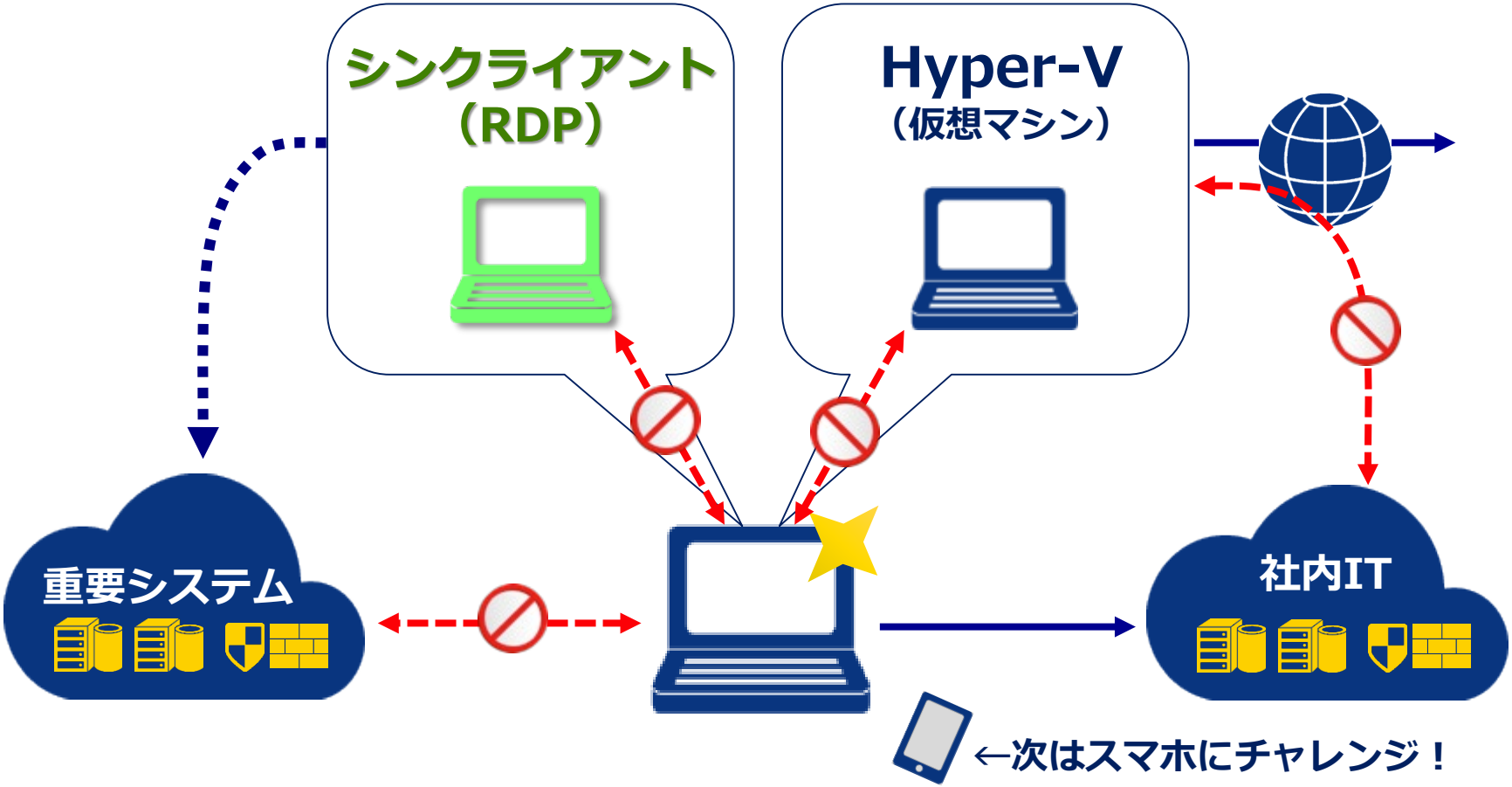
1. セキュリティ情報収集
2. ちょっと私的な情報取集
3. 新しいSaaSやアプリの試用
4. 社外とのコラボレーション
5. お仕事はシンクライアントで

パソコンの2台持ちをしなくてよい環境

1. セキュリティ情報収集
2. ちょっと私的な情報取集
3. 新しいSaaSやアプリの試用
4. 社外とのコラボ
5. お仕事はシンクライアントで



１台３役の セキュアFAT Pro でシャドーITを公式ITに！



NTT Communications

Transform. Transcend.

ご静聴ありがとうございました

出展：Amazon：キョンシー コスチューム メンズ 180cm クリアストーン正規品