モダンワークスタイルに対応した ソリューションのご紹介

国内Ｂ２Ｂ営業本部　国内ソリューション営業部

2022年 1月

dynabook

質問：今のセキュリティ対策、十分と言えますか？

Index

１．ニューノーマル時代のセキュリティ …… 4
２．Dynabookが考えるゼロトラストのソリューション …… 16

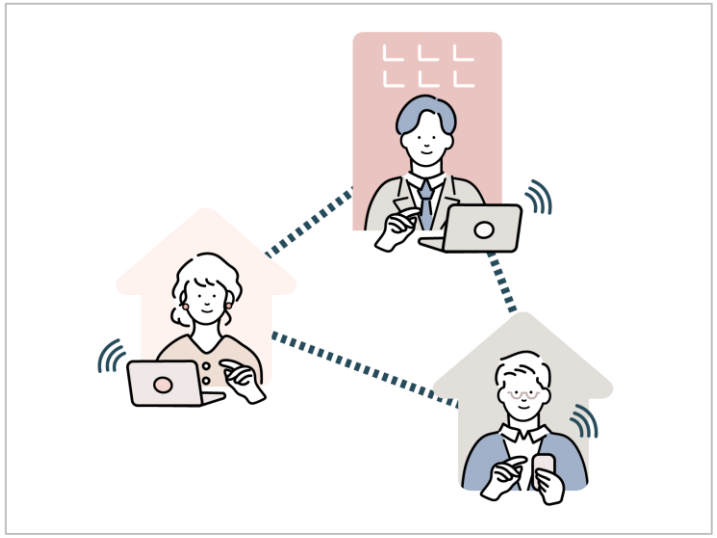
1.ニューノーマル時代のセキュリティ

ニューノーマル時代のビジネススタンダード

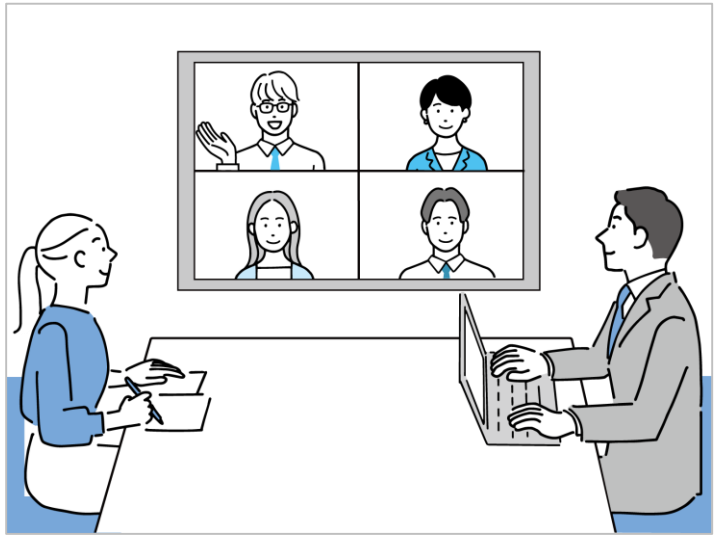
ニューノーマル時代のビジネススタンダードは「非対面・非接触」

※ニューノーマル時代とは従来の常識が大きく変わる時代のことです。近年でいうとコロナウイルスの流行により働き方の常識は大きく変わっています。

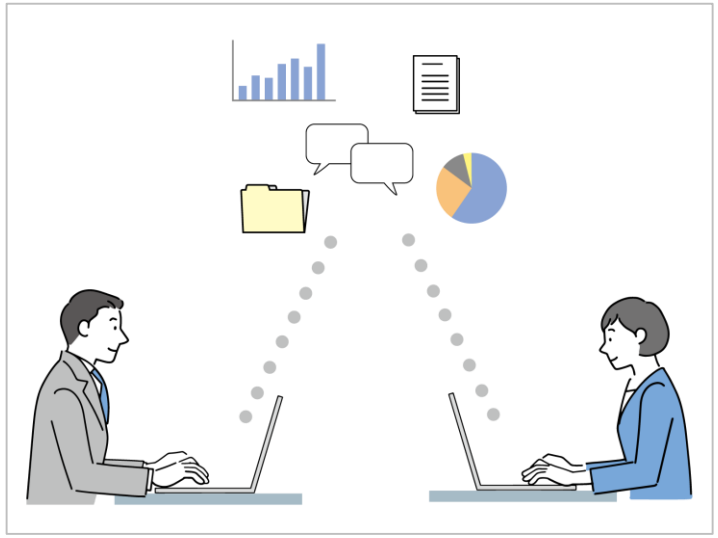
いつでもどこからでも働ける「モダンワークスタイル」



商談、打ち合わせも対面からオンラインへ



デジタルワークプレイス デジタル技術の活用



ニューノーマル時代の課題点

「非対面・非接触」で生じたテレワーク導入時の懸念事項や導入後の課題

本日のお話！

① テレワーク時のセキュリティリスク

ゼロトラストセキュリティ

SASEによるテレワーク時のセキュリティ

② コミュニケーション不足

ビジネスチャットによる

部門横断の活発な議論

③テレワーク時のマネジメントリスク

可視化ツールによる

労働時間の把握

情報流失事故件数の推移

上場企業の個人情報漏洩事故件数は、前年比2割増で7年ぶりに100件超え、社数別では調査開始以来最多。

近年、情報流失事故が起きている背景

クラウドサービスの利用増

働き方の多様化
（内部不正による情報漏洩の増加）

マルウェアの高度化

従来の境界型セキュリティでは、もう守れません。。。

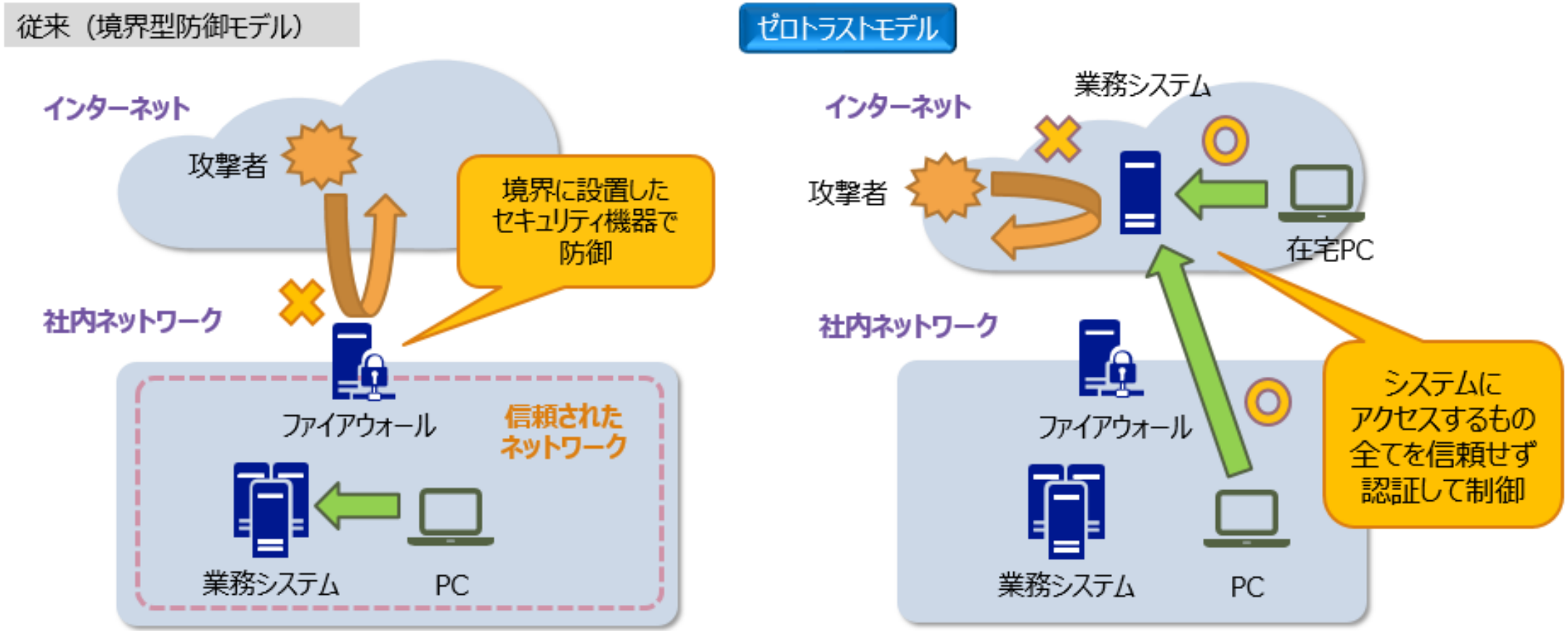
課題発生！

アクセス先、アクセス元、アクセス経路など各層で変化があるのでそれぞれに対応したセキュリティが必要

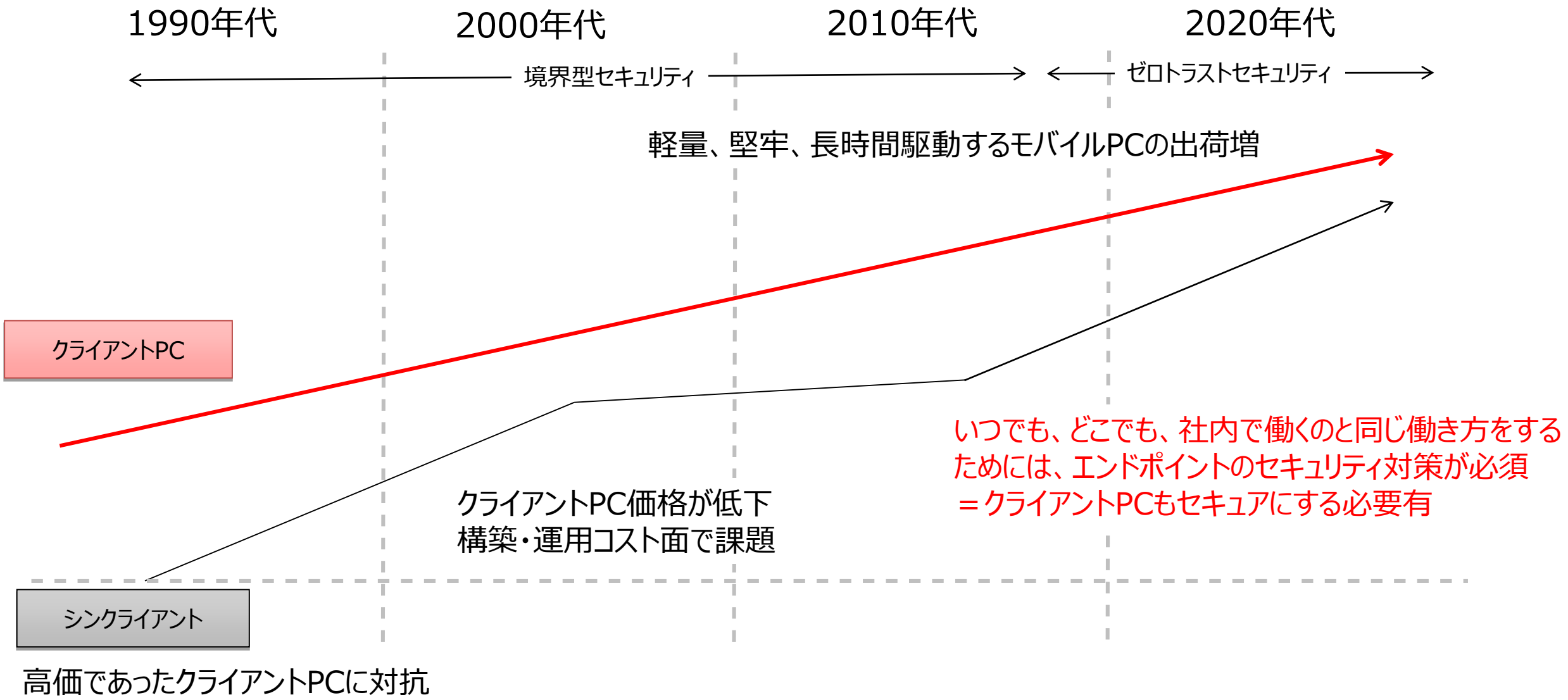
ゼロトラストという考え方の登場

ゼロトラストセキュリティとは？

従来は業務システムが社内ネットワーク上に配置されており、ネットワークはインターネットとの接続点のみを防御する形が主流でした。しかし、最近は業務システムがクラウド上に移行し、テレワークが普及したことにより、従来の考え方ではセキュリティ維持が困難です。そこで、ゼロトラストという考え方が注目されています。



ゼロトラストセキュリティの変遷



日本政府もゼロトラストセキュリティの適応へ

政府情報システムにおけるパブリック・クラウドの利用、府省 LAN の外部での活動がキーとなる働き方改革、デジタル・ガバメントにおける API による官民連携等が政策上の大きな実現目標となっていますが、これらを推進するには、 これまでのセキュリティの考え方だけでは、その実現が困難であり、十分なセキュリティレベルを確保できない場合もあります。 ゼロトラストとは利便性を保ちながら、クラウド活用や働き方の多様化に対応するため、ネットワーク接続を前提に利用者やデバイスを正確に特定、常に監視・確認する次世代のネットワークセキュリティの考え方です。セキュリティ対策は単に技術やソリューションが進化するだけではなく、その考え方も技術の進化に適応させていく必要があります。
（「政府情報システムにおけるゼロトラスト適用に向けた考え方」より抜粋） dp2020_03.pdf (cio.go.jp)

当てはまることありませんか？

VPNを使って社外からアクセスさせている

従業員の私物端末を業務で使わせている

端末紛失時の対策ができていないかもしれない

クラウドサービスの利用が増えた

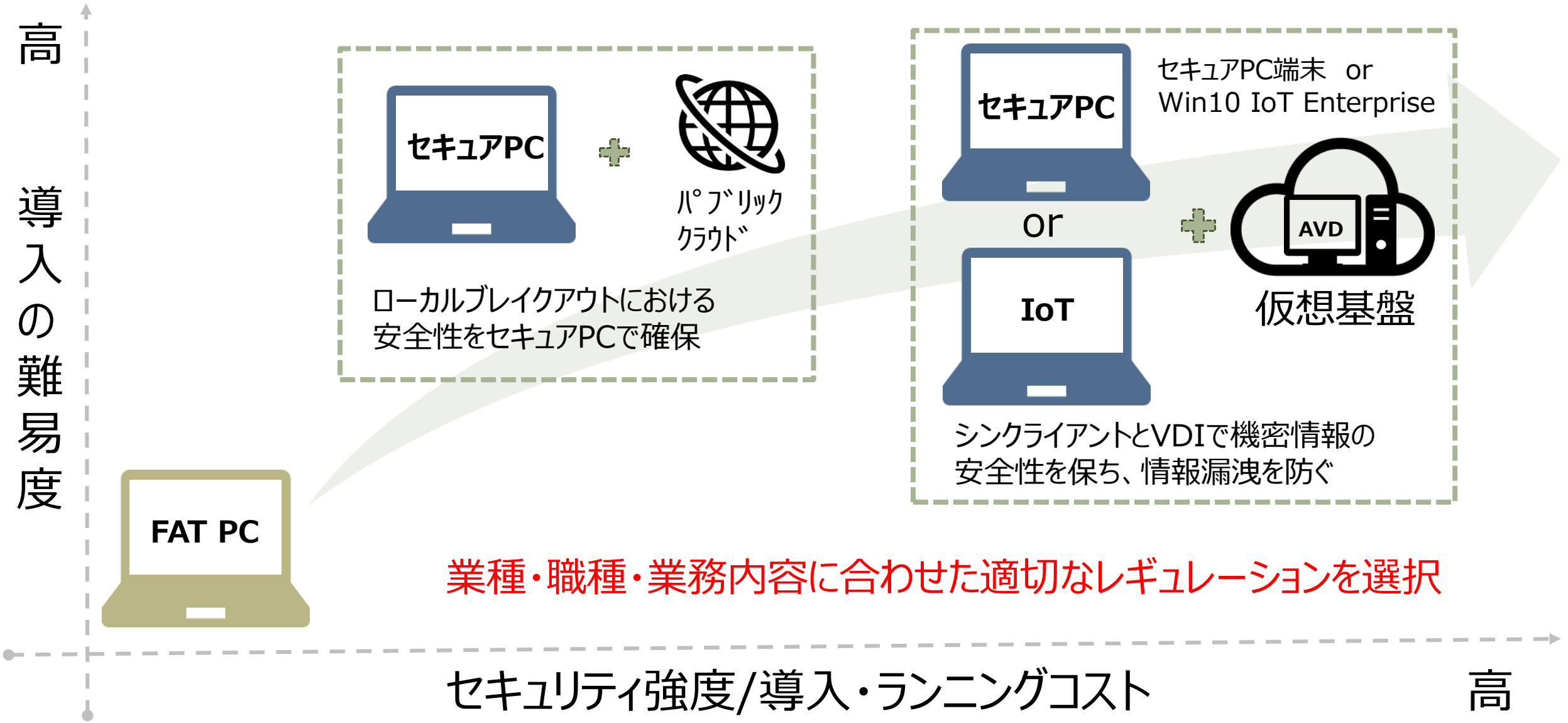
従業員のアプリケーション利用を制限していない
（メール、ファイル共有）

社用端末を在宅で利用している

１つでも当てはまる方は情報流失している可能性があります

2.Dynabookが考えるゼロトラストのソリューション

ニューノーマル時代におけるセキュリティエンドポイント



Dynabookが考えるゼロトラストのソリューション

Dynabook×Microsoft365

Dynabookは、ハードウエアメーカーとしての知見を活かし、端末とMicrosoft365の機能を組み合わせることで、エンドポイント（従業員が使っているPCやスマートフォンの総称）に必要なセキュリティの強化をし、ゼロトラストセキュリティの実現をご支援してまいります。

① セキュアPC

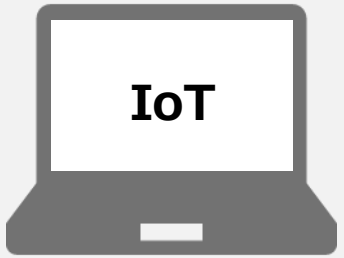
セキュアPCとVDIを組み合わせて
オンラインでもオフラインでもセキュアに

軽量・堅牢　モバイルパソコン

or

② セキュアPC for VDI

シンクライアントとVDIで機密情報の
安全性を保ち、情報漏洩を防ぐ



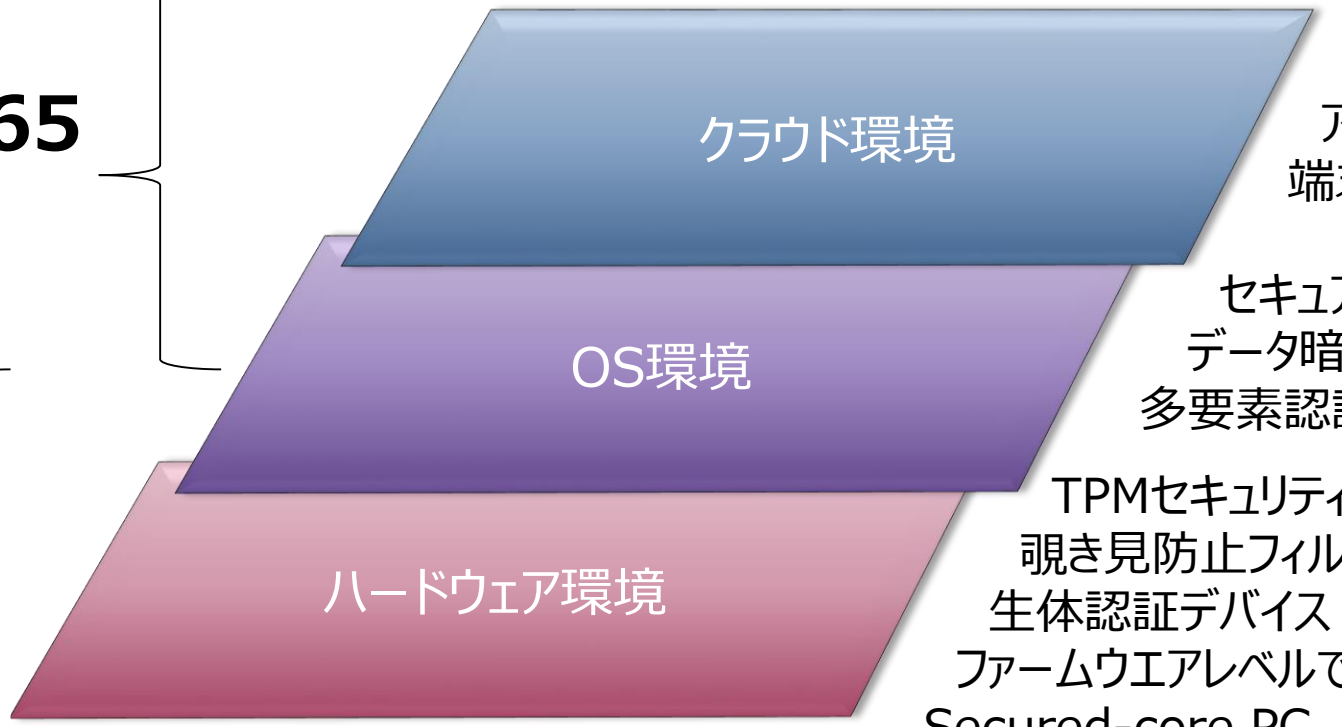
軽量・堅牢　モバイルパソコン

Dynabook×Microsoft365で実現できるセキュリティ設定

DynabookのPCとMicrosoft365の機能を組み合わせることで、モダンワークスタイルに必要なセキュリティ設定を実現し、
お客様環境を守ります。

Microsoft 365
（E3＆E5）

Dynabook PC



認可・認証管理
アクセス保護
端末管理

セキュアコアブート
データ暗号化
多要素認証

TPMセキュリティチップ
覗き見防止フィルター
生体認証デバイス
ファームウエアレベルでのコード制御
Secured-core PC

Dynabook PC & Microsoft 365で
お客様環境を守るトータルセキュリティ

ご参考：Dynabookの推奨セキュリティ設定値(抜粋)　標準推奨値

PCメーカーであるからこそ、Microsoftとの関係性において蓄積した同社製品に関する膨大な知見をもとに、推奨セキュリティ設定値をご提供いたします。

	課題	対応策	機能	機能概要
1	紛失・盗難	端末紛失対策	ディスク暗号化(BitLocker)	HDDやSSD、USBメモリ、外付けHDDなどのデータを暗号化
		起動保護	セキュアブート	OSの不正起動を防止
2	ウィルス・マルウエア感染	セキュリティパッチ適用	Microsoft Windows Updateによる最新OSパッチの配信	パッチ配信設定（QU：遅延なし、FU:180日遅延）
		ウィルス対策ソフト	Windows Defenderを導入	OSレベルで脅威を防ぐ
3	不正アクセス	なりすまし防止	多要素認証 生体認証	認証情報の漏洩に備えて、多要素によるPCログイン IDとパスワード以外に、指紋や顔によるPCログイン
		条件付きアクセス	クラウドアプリに対するアクセス制限	Microsoftのクラウドアプリに条件付きアクセスポリシーを割当て
4	認証情報の保護	PCローカル上の認証情報保護	Credential Guardを導入	ユーザの資格情報(認証情報)を保護

Dynabook社が推奨する、標準セキュリティ・レギュレーションを提供。
お客様のご要望に応じて、エンドポイント・セキュリティを更に強化する為のコンサルティングサービス、要件定義、構築、カスタマーサクセスも可能です。

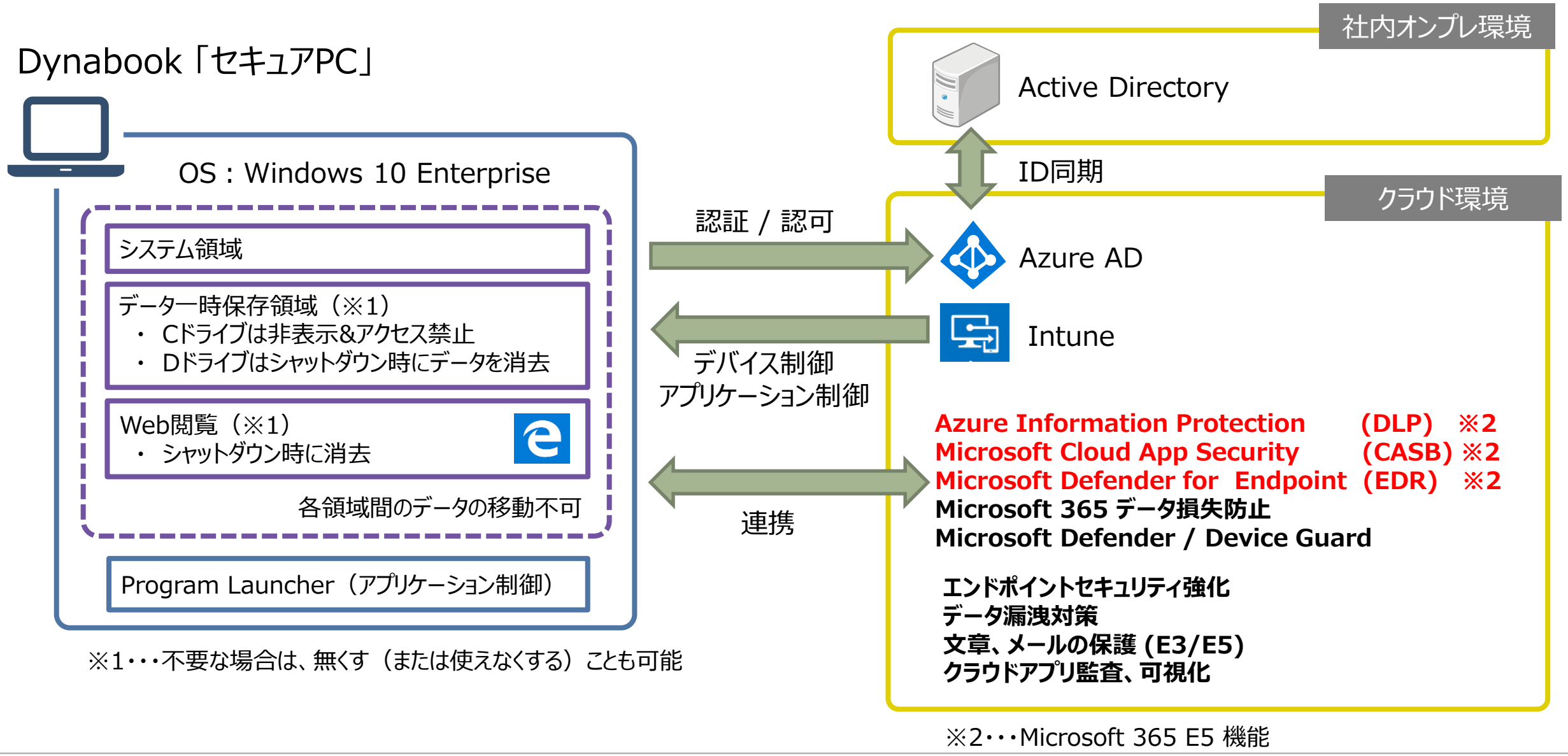
ご参考：Dynabookの推奨セキュリティ設定値(抜粋)　標準推奨値＋M365E5

標準推奨値値に、Microsoft365 E5の機能を加えることでさらに、セキュリティを強化することができます。

※オレンジ網掛は、M365 E5の機能で実装

	課題	対応策	機能	機能概要
1	紛失・盗難	端末紛失対策	ﾃﾞｨｽｸ暗号化(BitLocker)	HDDやSSD、USBメモリ、外付けHDDなどのデータを暗号化
		起動保護	ｾｷｭｱﾌﾞｰﾄ	OSの不正起動を防止
2	ｳｨﾙｽ・ﾏﾙｳｪｱ感染	ｳｨﾙｽ対策ｿﾌﾄ	Windows Defenderを導入	OSレベルで脅威の防止
		ｳｨﾙｽ対策ｿﾌﾄ	Device Guardを導入	OSレベルで脅威の防止
		ｳｨﾙｽ対策ｿﾌﾄ	Microsoft Defender for Endpointを導入	「既知・未知のマルウェア」を検知・ブロックするだけでなく「ファイルレス攻撃」「プロセスの不審な振る舞い」などからデバイスを保護
3	不正アクセス	なりすまし防止	多要素認証,生体認証	認証情報の漏洩に備えて、多要素によるPCログイン IDとパスワード以外に、指紋や顔によるPCログイン
		条件付きｱｸｾｽ	ｸﾗｳﾄﾞｱﾌﾟﾘに対するｱｸｾｽ制限	Microsoftのクラウドアプリに条件付きアクセスポリシーを割当て
		なりすまし防止	Microsoft Defender for Identity を導入	Active Directory のアクティビティを監視・分析、ユーザーID に対する脅威や不審な操作を検知して不正アクセスから保護
		なりすまし防止	Azure Active Directory Identity Protectionを導入	Azure Active Directory のサインイン情報を分析、ユーザーID に対する脅威や不審な操作を検知して不正アクセスから保護
4	認証情報の保護	PCﾛｰｶﾙ上の 認証情報保護	Credential Guardを導入	ユーザの資格情報(認証情報)を保護
5	情報窃取	データ保護対策	Microsoft Cloud App Securityを導入	クラウドアプリ上のアクティビティを分析し、情報搾取につながる不審なふるまいや脅威をブロック・検知して保護

Microsoft365を利用したセキュアPCの構成例



でも、ゼロトラストセキュリティの
運用保守って聞くとやり切れるか不安じゃないですか？

オンボーディングカスタマーサクセス

ご安心ください。
Dynabookが御社IT担当者に代わり、ゼロトラストセキュリティの運用保守を代行します。

Point①　運用サポート（代行）

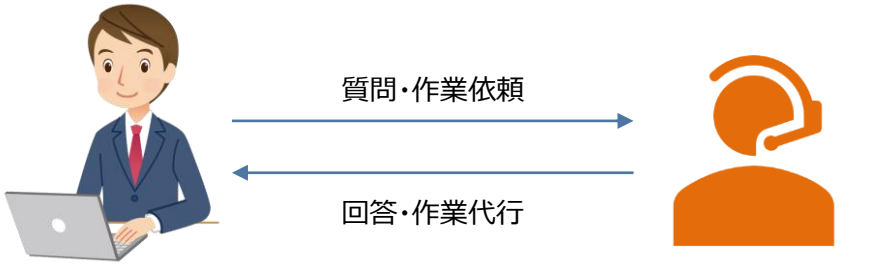
お客さまの運用を徹底サポート。
※ITご担当者様の代わりに設定や運用の代行も可能です。※セキュリティの仕様はお客様にて決定。

Point②　サブスクリプション型サービス

サブスクリプション型サービスなのでいつでも解約可能です。

Point③　最新のセキュリティを提供

長年のハードウェアメーカーとしての知見と長年のMicrosoftとの関係性を活かし
いつでも最新のセキュリティ情報をご提供します。



サービス内容
■エンドポイントセキュリティ
　お客様テナントへの設定（要許諾）
　　セキュリティ仕様　　登録
　　パソコンのハッシュ値 登録
■ご利用者様向け運用サポート（代行）
■各種ＳａａＳサービス
■パソコン保守サポート