緊急

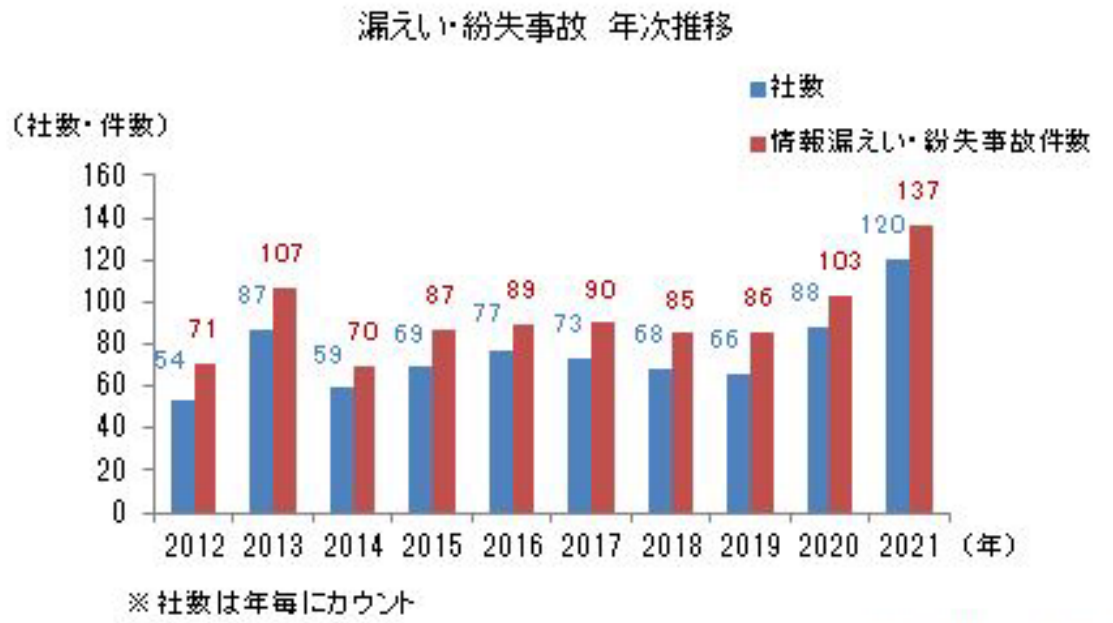
新しいセキュリティ対策の必要性

INDEX

01 新しいセキュリティ対策の必要性

コロナウイルスの流行、感染予防対策によって、働き方の常識は大きく変わりました。リモートワークが推奨され、いつでも、どこでも働けるようになったことでクラウドツールの利用は増えました。しかし、一方で、様々な場所・様々な端末から内部情報にアクセスできるようになったため、外からの脅威を主な警戒対象としていた従来のセキュリティ対策では安全を守れなくなってしまいました。そこで、新しいセキュリティ対策の概念である「ゼロトラストセキュリティ」は誕生しました。

上場企業の個人情報事故件数は、前年比3割増の137件、社数・事故件数とも調査を開始以降で最多。



東京商工リサーチ調べ

02 ちなみに、当てはまることありませんか？

従業員の私物端末を業務で使わせている

従業員のアプリ利用を制限していない

VPNを使って社外からアクセスさせている

クラウドサービスの利用が増えている

端末紛失時の対策が不明確

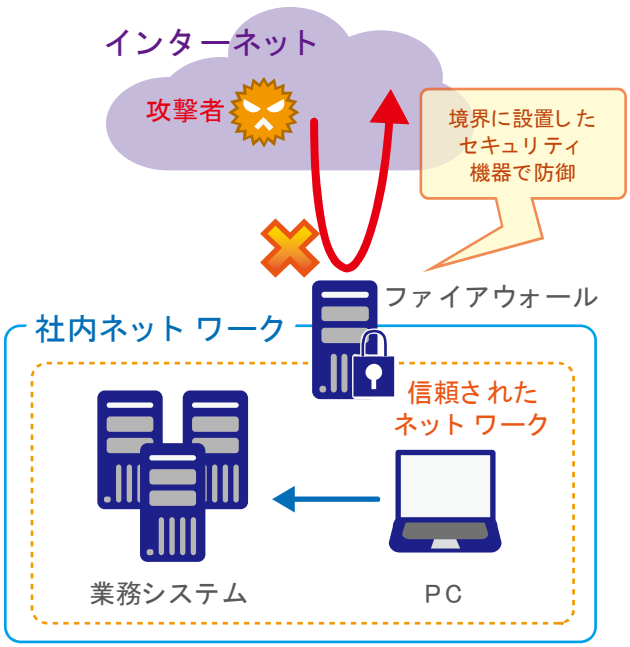
社用端末を在宅で利用している

１つでも当てはまると情報が流失している可能性があります。ゼロトラストセキュリティへの移行が必要かもしれません。

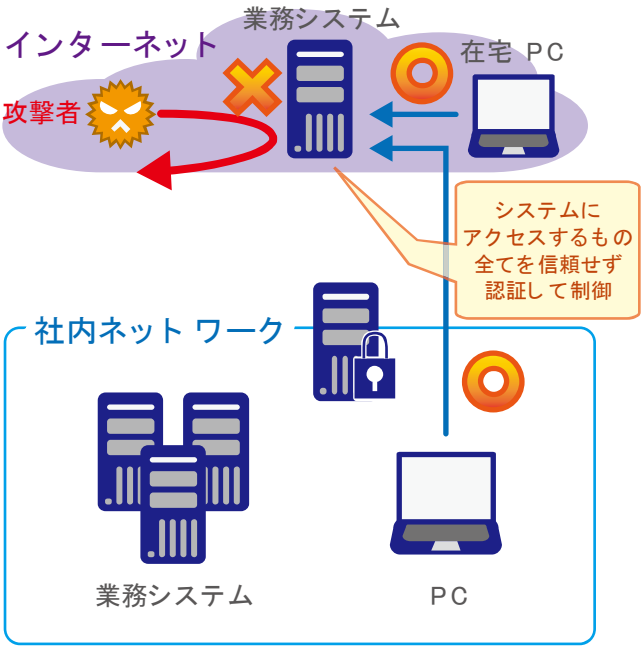
03 新しいセキュリティは何も信じない

「ゼロトラストセキュリティ」とはその名の通り、何も信じないといった概念のセキュリティ対策です。従来では外からの脅威のみに対抗していましたが、ゼロトラストセキュリティはエンドポイント（従業員が使っているスマートフォンやPCの総称）で脅威に対抗しています。脅威はどこからでも発生するものとして、システムにアクセスするもの全てに対し、認証するので安全性は高まります。

従来（境界型防御モデル）



ゼロトラストモデル



04 日本政府もゼロトラストセキュリティへ

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)

05 ゼロトラストセキュリティのメリット

① 強固なセキュリティの構築

従来型セキュリティよりもセキュリティが強固になります。複雑で対処が困難な攻撃に対処できる点に加え、セキュリティ面で不安視されているクラウドにも対応できます。

② 設定がシンプル

従来の境界型セキュリティの場合、VPNやファイアウォールの導入・運用に複雑な設定が必要となっていました。一方でゼロトラストの場合、比較的シンプルな設定や既存クラウドサービスの導入のみで実現可能になるため、セキュリティの管理を簡素化することができます。

③ 好きな場所・端末からアクセス可能

ゼロトラストセキュリティの場合は、端末やネットワーク、アクセスの 3 点すべてに対し、脅威の有無をチェックし、セキュリティ対策を講じます。社内と社外で境界を設定するわけではないので、どこからでも、どんな端末からでも安全に社内の情報にアクセスすることが可能になります。

06 ゼロトラストセキュリティ導入に際しての注意点

前述のメリットのようにゼロトラストセキュリティの導入には大きなメリットがあります。

しかし、もちろんゼロトラストセキュリティ導入の際に注意する点もあります。

①生産性や利便性を考える

ゼロトラストセキュリティの考え方は「すべてを信用しないこと」ですが、意味を正しく理解せずに設計し、運用をスタートしてしまうと生産性を大きく落とすことになりかねません。極端ですが、例えば、外部からのクラウドサービスをすべて禁止したり、漏洩しても問題ないような情報や業務に関しても徹底的にセキュリティ対策を講じるとどうなるでしょうか。従業員の生産性や利便性が大きく損なわれてしまいます。運用を明確に想定する必要があるため、ゼロトラストセキュリティの導入は設計が一番重要だともいえます。

②費用対効果の最大化を考える

ゼロトラストセキュリティの構築にはある程度のお金がかかります。例えば、ゼロトラストセキュリティにおいて、すべてのシステムを自社で再構築しようとしたり、守る必要のないすべての情報にまでセキュリティ設定をしてしまうと得られる効果とコストが釣り合いません。そこで費用対効果を最大にするためにも、既存のゼロトラストセキュリティソリューションを活用したり、それぞれの自社の都合に合わせたセキュリティを切り分けることで得られる効果は払った額以上のものになります。

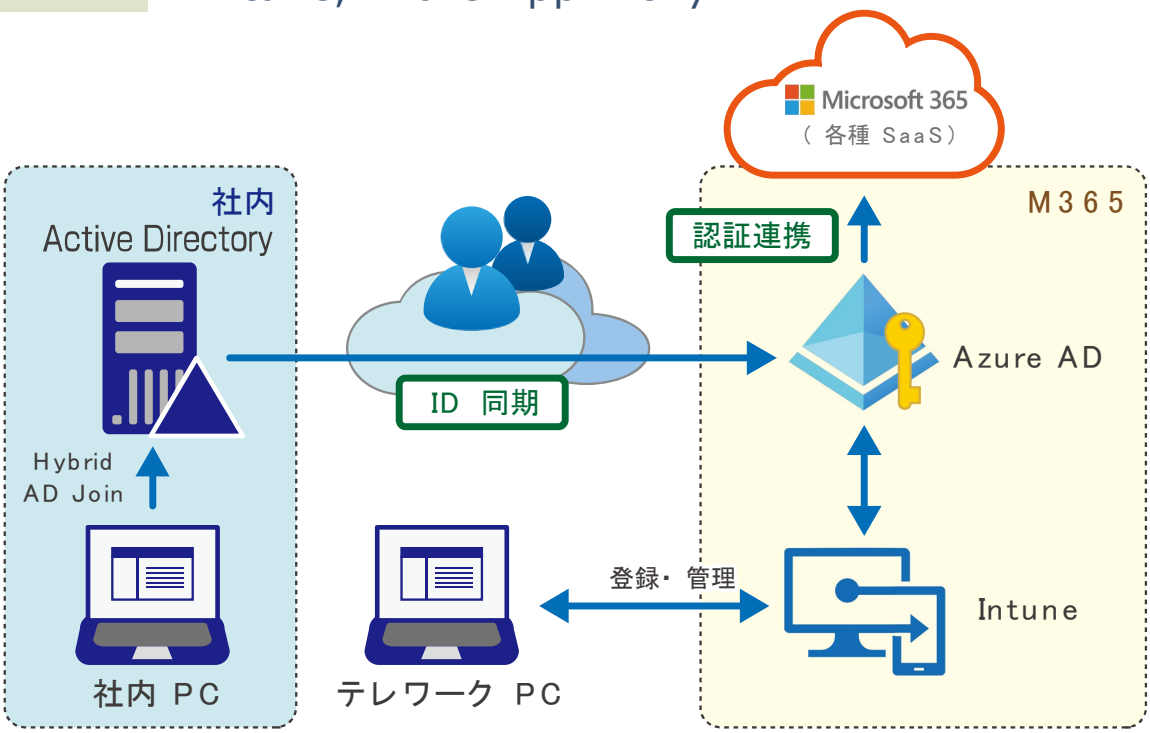
では、いったいどうしたらいいのでしょう？
「難しい。」「誰か助けて！」
そんな声が聞こえてきます

07 Dynabookが考える ゼロトラストセキュリティ

Dynabookは、「コンピューティングとサービスを通じて世界を変える」という企業ビジョンを掲げ、“ハードウェア（dynabook as a Computing）とサービス（dynabook as a Service）の融合”と、それを支えるテクノロジーの強化、事業のグローバル展開を新方針として、「人に寄り添う、社会を支える、真のコンピューティング」と「ユーザーを起点に考えた新しい付加価値・サービス」を追求してまいります。
現代では必須要件ともいえる、ゼロトラストセキュリティ対策においては長年のハードウェアメーカーとしての知見と今やゼロトラストセキュリティの第一人者であるMicrosoft社とのパイプを活かし、新しい時代のワークスタイルに適した最新のセキュリティ対策を提案してまいります。

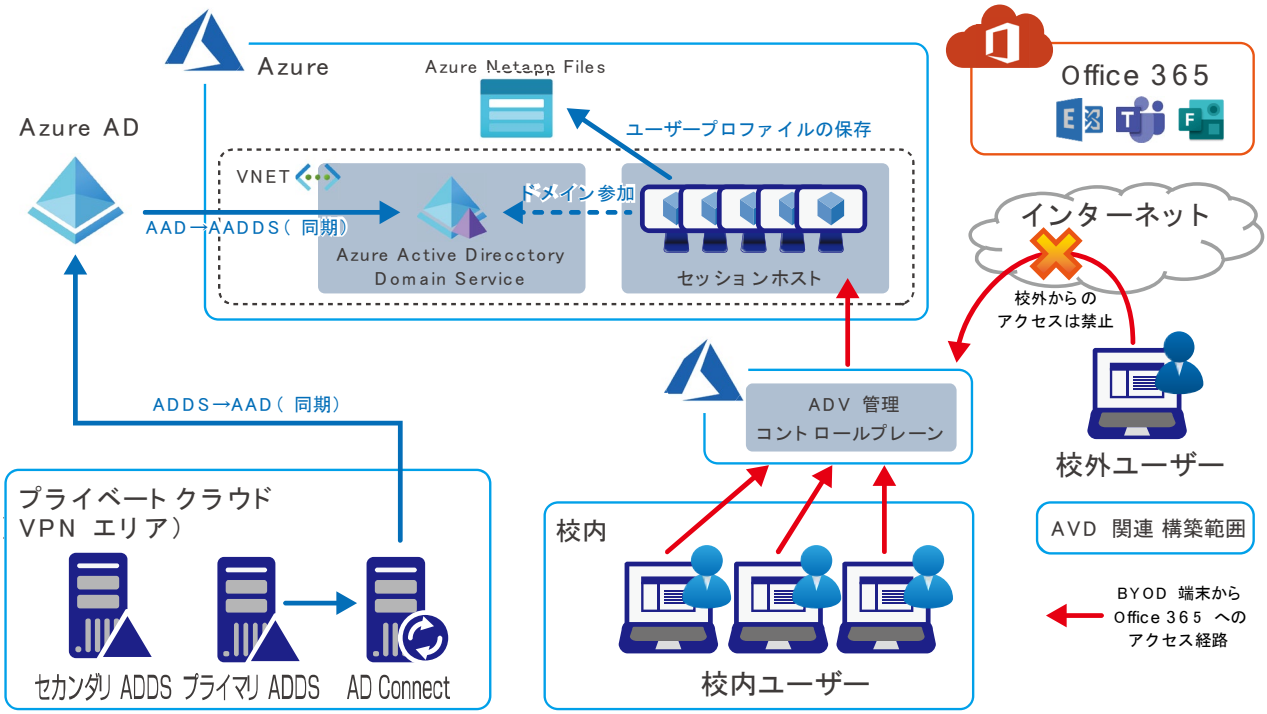
08 導入事例①

課題	クラウド認証の強度を強め、テレワークPCの管理・認証も統合したい
解決	オンプレミスのAvtiveDirectory(AD)とAzureADを同期・連携するよう構成し（Hybrid AD Join）、テレワークPCをIntuneで管理することで、クラウドサービスの認証条件としてPCがADまたはIntuneで管理されていること、管理ポリシーに適合していることを追加。
構成	AzureAD（Azure AD Connect, 条件付きアクセス）, Intune, Azure App Proxy



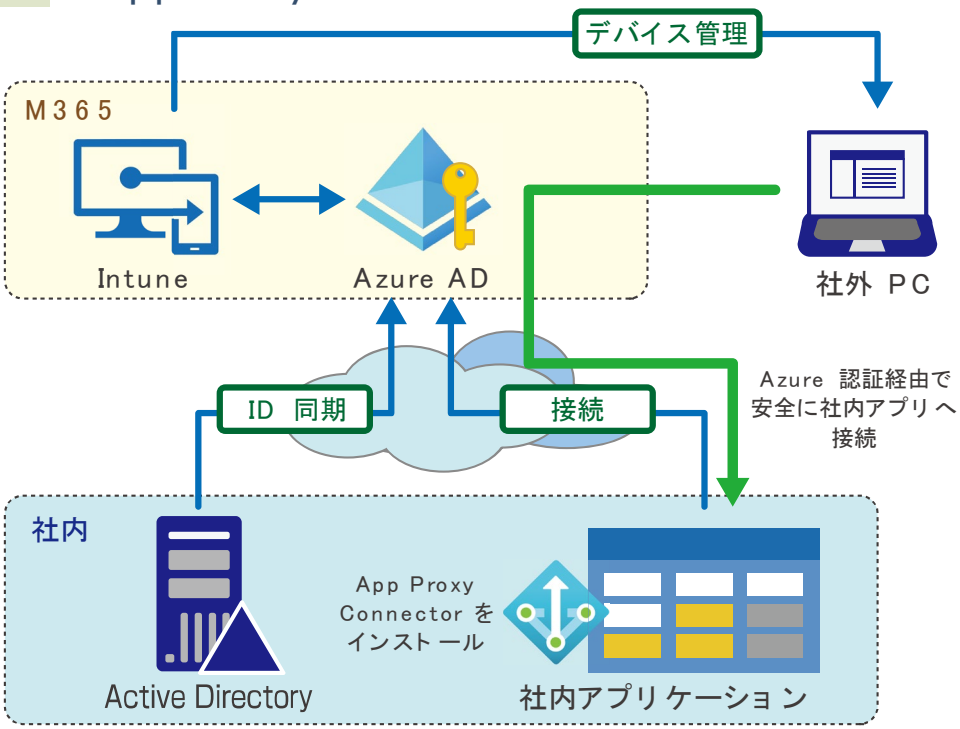
09 導入事例②

課題	教育機関において、BYOD端末を使った受講環境を校内でセキュアに実現したい。
解決	AVD(Azure Virtual Desktop)を使った仮想デスクトップ環境を構築。ユーザープロファイルはAzureFiles上に保存することでBYOD端末上にデータを残さないセキュアな構成を実現。また、AVD採用による効果として、仮想デスクトップ環境のリソースを柔軟に変更させることが可能になり、無駄なランニングコストの削減を実現。
構成	AzureAD（AADC, 条件付きアクセス）, Azure Virtual Desktop,AzureFiles



10 導入事例③

課題	持ち出しで使う社外PCを管理し、安全に社内アプリ（事務、ファイル閲覧）に接続させたい
解決	社外デバイスをIntuneで管理し、Azure App Proxyを構成して社内アプリをAzureに接続、多要素認証を経由した安全なアクセスだけ社内アプリに接続できるように設計。App Proxyは内部からAzureにセッションを張るために、社内ネットワークを直接公開する必要がなく、ネットワーク設計の変更が発生しない点も大きなメリット
構成	AzureAD（AADC, 条件付きアクセス）, Intune, Azure App Proxy



11 最後に

新型コロナウイルスが終息しても、働き方改革を実現するために「リモートワーク」は、ニューノーマル時代の新しい働き方として定着し、必要不可欠なソリューションになっていくと予測されています。そんな時代に対応したセキュリティ対策は企業を存続させるための**必須要件**といえます。
事故が起こってからでは遅いのです。

今回、少しでも気になった方はお気軽に**お問い合わせ**ください。
新しい時代の難局をともに乗り越えましょう。

■お問い合わせ先

Dynabook株式会社
国内事業統括部　国内B2B営業本部　国内ソリューション営業部
TEL: 03-5144-3602
e-mail: DBI-KAIHATSU-G@list.dynabook.com