

信用ゼロ?!
ゼロトラスト時代はこれだ!

働き方改革を支えるデジタルワークプレイス

Box まるわかりガイド —セキュリティ編—

Digital Workplace Security Perfect Guide



創業150年
老舗メーカー
てつ社長

社員思い。持ち前のリーダーシップと決断力で会社の成長に貢献。好きな食べ物はどらやき。



営業本部長
ムラさん

冷静沈着なリーダー。お客様に働き方改革を浸透させる使命に静かに燃えている。影に日向に部下をサポートし、見守ってくれる。



ソリューション
アーキテクト
サトちゃん

課題解決に、きっちりテクノロジーで応える。確かな技術力に社内外で信頼が厚い。



情シス出身の
営業マネージャー
ゴーさん

穏やかな物腰でお客様現場の課題に寄り添う。大胆なチャレンジを提案し、一緒に成し遂げようと奮闘。



エバンジェリスト
ツッチー

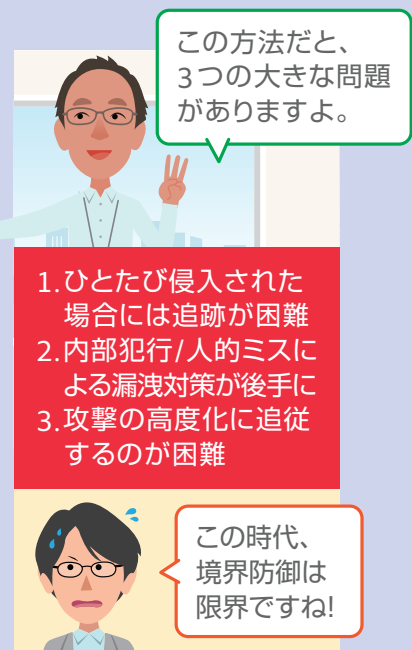
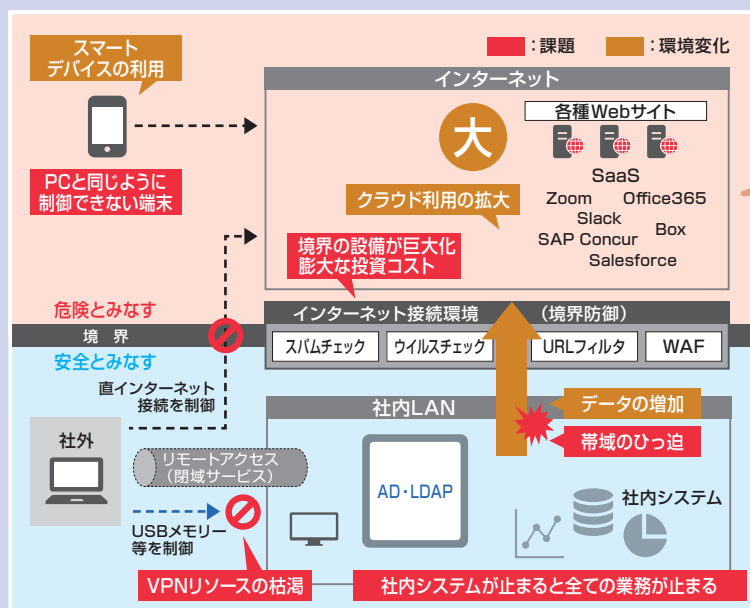
進化するITに並走するも、一方でDXに走り出す企業に馴染むITを提案し伴走している。リアリストだが、ハートはととても熱い!



情報システム
メンバー
アッコ

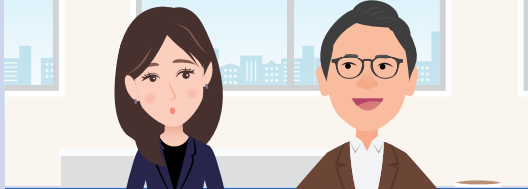
仕事はきっちり、合理的な発想でみんなを支える影のリーダー。好きな食べ物はステーキ。

大きく変わる働き方、 システムが追従できていない!

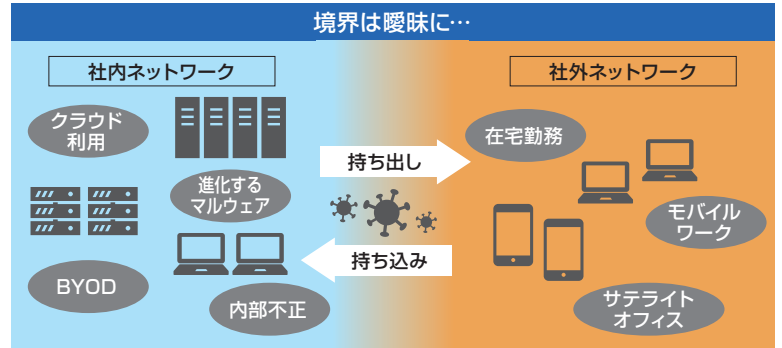


働き方が大きく変わっているのに、システムは古いまま…

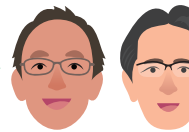
企業も新しい働き方に追従しないとイケません。



1. 社外での仕事増
2. 社外のアプリケーションや情報資産の利用増 (SaaSなどクラウド環境)
3. 社外の人とのコラボレーション増



境界が曖昧になるんです。



従業員は外にいることを前提に考える時代です！

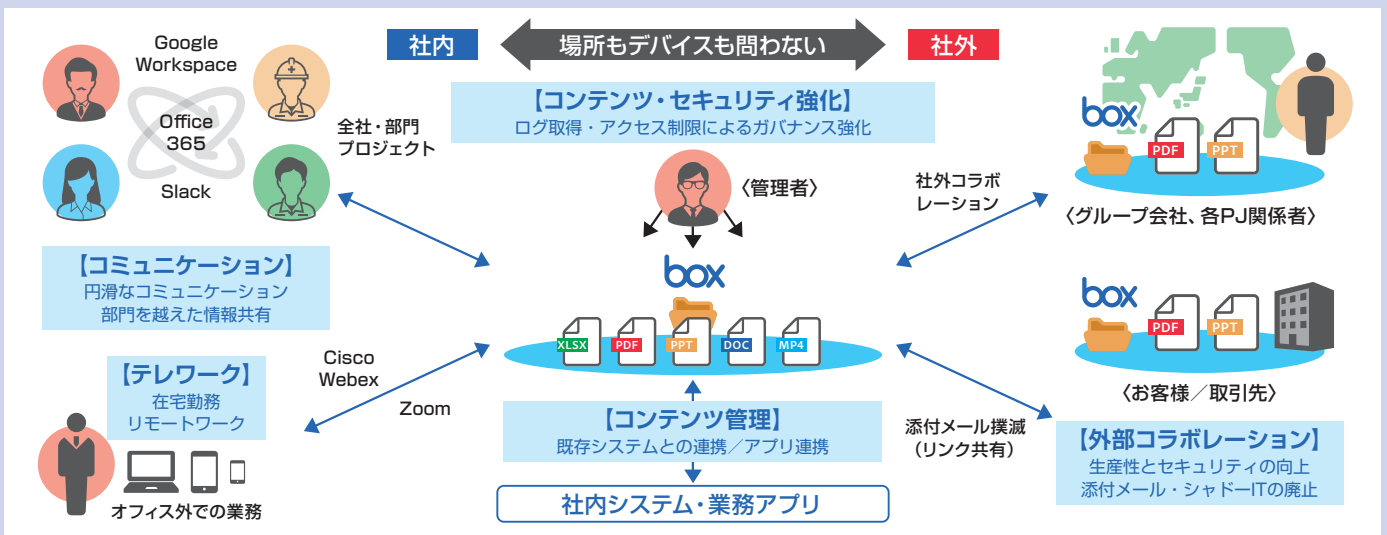
ということはSaaSしかなさそうですね。



そのため境界で守るのではなく、それぞれのポイントで守る**ゼロトラストセキュリティ**が必要になるんだ！



つまり、それぞれのSaaSアプリがしっかりとしたセキュリティを確保しておかないといけないということ！それがデジタルワークプレイスなんだ！



働き方改革で変わるオフィス環境!

デジタルワークプレイス

今、多くの企業が働き方改革に取り組んでいます。当初は働き方改革関連法案への対応から大企業を中心に進んでいましたが、新型コロナウイルス感染拡大による半ば強制的なテレワークシフトにより、あらゆる企業が働き方改革に取り組まざるを得ない状況になりました。

このように働く環境が大きく変化する中で、それらを支えるためのITインフラが必要不可欠であり、そのあり方も大きく変わろうとしています。働き方改革を実現する環境こそが「デジタルワークプレイス」なのです。

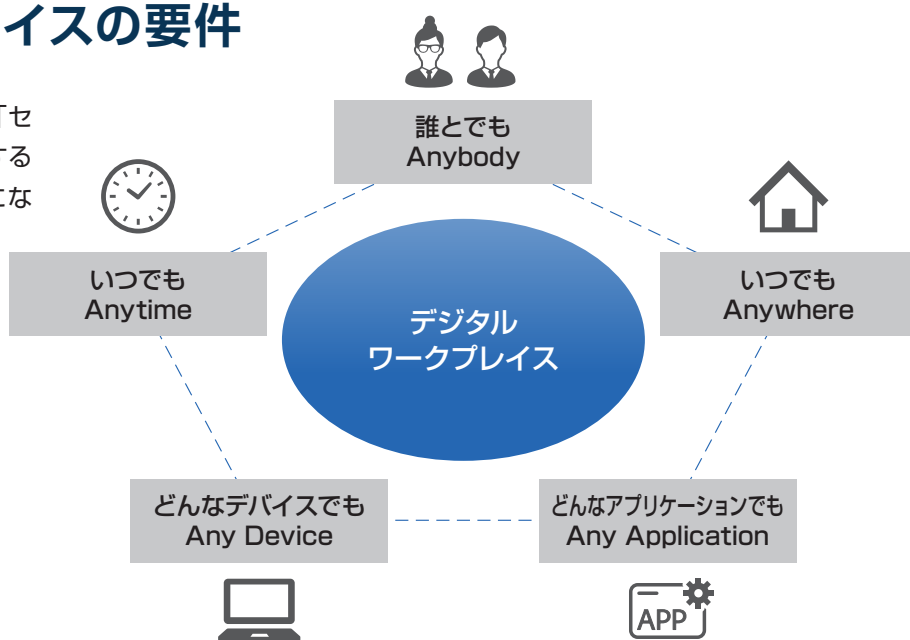
	これまで	今、そしてこれから
働く場所	オフィス	どこでも
就業時間	9時～17時	フレキシブル
端末	会社支給PC	幅広いデバイスの選択肢
IT	オンプレ	オンプレ/クラウド
ネットワーク	イントラネット (VPN含)	イントラネット インターネット
コラボレーション	社内	社内、社外問わず

デジタルワークプレイスの要件

デジタルワークプレイスは、「5つのAny」と「セキュリティ」、「コラボレーション」に対応することで、どんな働き方改革にも対応可能になります。



セキュリティと
社内外の円滑な
コラボレーション
が重要です！



働き方改革とは？

2019年に働き方改革関連法案（2018年6月29日可決・成立）が施行されたことを受けて企業における働き方改革への理解は欠かせないものになりました。働き方改革とは一億総活躍社会の実現に向けた取り組みであり、今までの企業の労働環境を大幅に見直す取り組みです。加速する労働人口の減少、低い労働生産性、新興国の台頭による競争力低下、非正規労働者や介護・子育て人材に対する待遇、常態化する長時間労働による過労死や疾病など、弊害はいたるところで浮き彫りになっており、企業は迅速な対応が求められています。

<一億総活躍社会>

50年後も人口1億人を維持し、職場・家庭・地域の誰しものが活躍できる社会

「働き方改革は、一億総活躍社会実現に向けた最大のチャレンジ。多様な働き方を可能とするとともに、中間層の厚みを増しつつ、格差の固定化を回避し、成長と分配の好循環を実現するため、働く人の立場・視点で取り組んでいきます。」

引用:働き方改革の実現

<http://www.kantei.go.jp/jp/headline/ichiokusoukatsuyaku/hatarakikata.html>

あなたの会社の働き方改革は万全ですか？

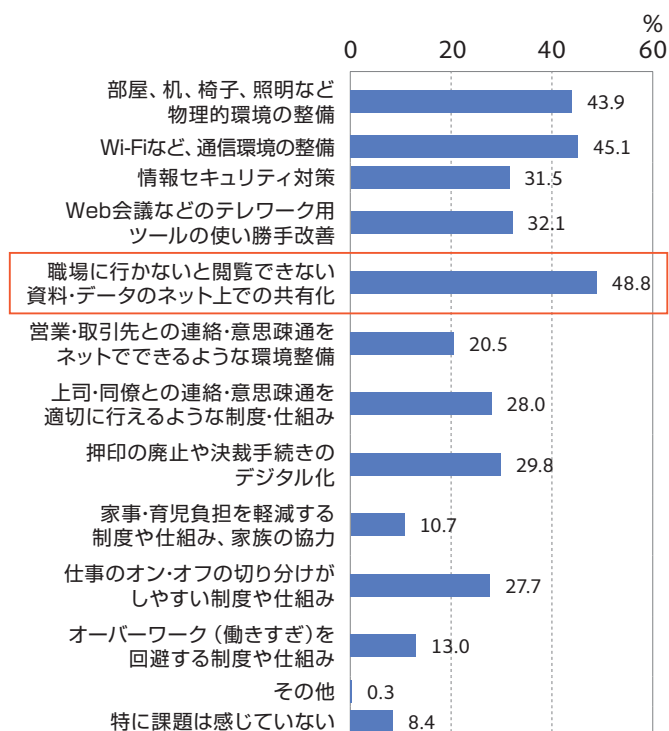
テレワークで浮き彫りになる課題

出社が必要な作業が意外と多い！ 情報アクセス課題が露呈

今、多くの企業がテレワークの課題に直面しています。公益財団法人 日本生産性本部が実施したアンケート調査では約50%の企業が、「職場に行かないと閲覧できない資料・データの共有」が問題であると指摘しており、テレワークにおける情報アクセスが最大の課題になっています。

テレワークの一番の課題は職場に行かないと閲覧できない資料やデータの共有化にあるんです

つまり、テレワークにおける『情報へのアクセス』が最大の課題という訳ですね。



公益財団法人 日本生産性本部 第1回 働く人の意識調査
『新型コロナウイルス感染症が組織で働く人の意識に及ぼす影響を調査』
(2020年5月22日)

<https://www.jpc-net.jp/research/detail/004392.html>

あなたの会社のテレワークの状況は？

働き方改革を実現するためにはITの力が必要不可欠な時代です。企業はITを活用しながら社員の働きやすい環境を整える必要があるとともに、働き方の変遷によるセキュリティ面でも万全なものにする必要があります。企業のテレワーク／リモートワークの状況を知ることによってデジタルワークプレイスがどの程度実装されているのか、そして働き方改革を実現する上でどのレベルなのかを測定することが可能です。多くの企業ではレベル3以上（あらゆる業務プロセスが遠隔地から問題なく実現できる）を実装することが望ましいと言えます。

☆☆☆☆

レベル1：できない

- そもそもリモートワークの仕組み(IT、制度)が整っていない

☆☆☆☆

レベル2：できるけどやりにくい

- ハンコ、紙がプロセスに入っていて、リモートワークできない(制度)
- VPNやVDIのキャパシティの問題から、パフォーマンスに難(IT)

☆☆☆☆

レベル3：問題なくできる

- プロセスも基本的にデジタル化されている

☆☆☆☆

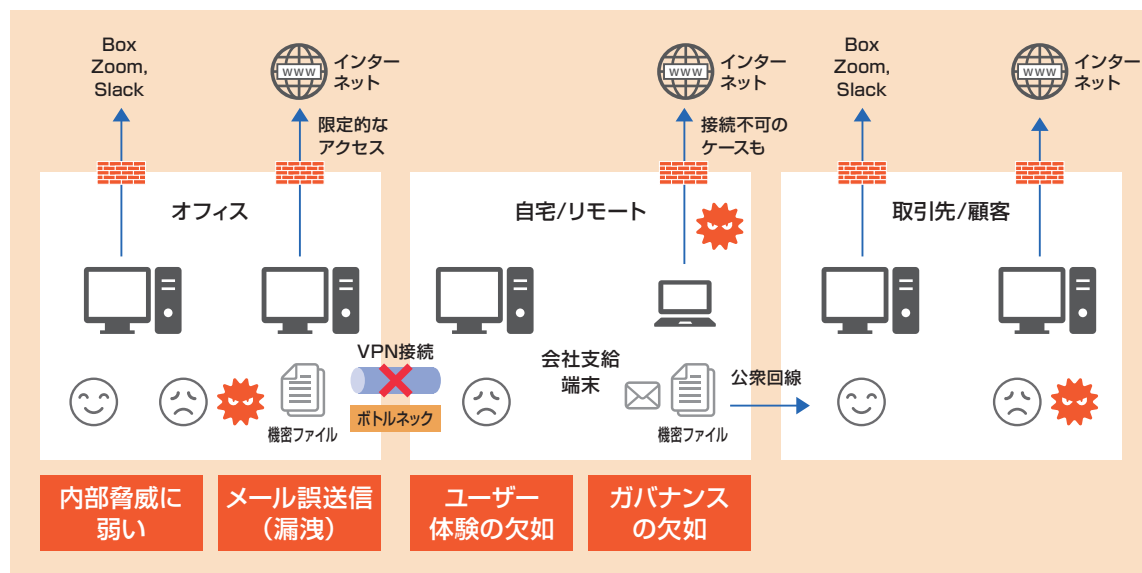
レベル4：オンラインファースト

- オンラインが主、リアルが補完的手段と考える
- 働き方のデジタル・トランスフォーメーション(DX)

現在のシステム環境がテレワークを阻害 境界型セキュリティの限界

従来の企業が実施していたセキュリティ対策である境界型セキュリティは、外部からの侵入を防ぐための境界防御を特徴としていました。そのため悪意のあるウイルスが高度な攻撃手法によって社内に入ってしまった場合には、無力の状態

になります。また、多くの企業においてVPNによる安全なアクセスを構築していますが、VPN自体がボトルネックになりユーザー体験を損ねてしまうことが問題です。



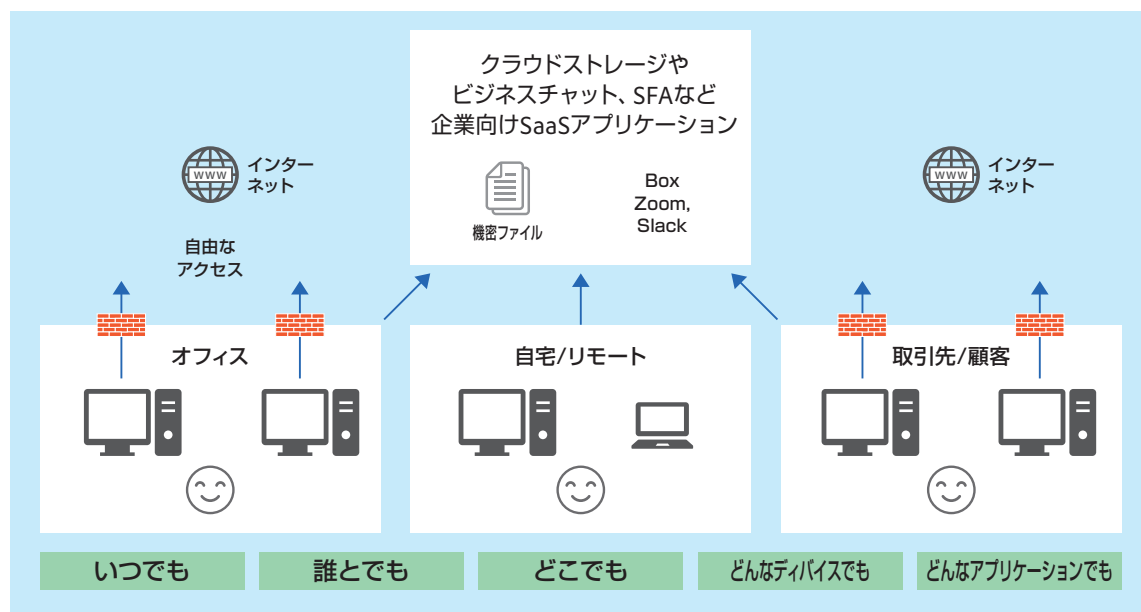
今の時代は
限界があります!



時代は境界防御からゼロトラストへ

境界防御は、ひとたび外部からの侵入された場合や内部犯行/事故を考慮していないと同時に、社外とのコラボレーションが不向きであり現代社会に即していない欠点があり

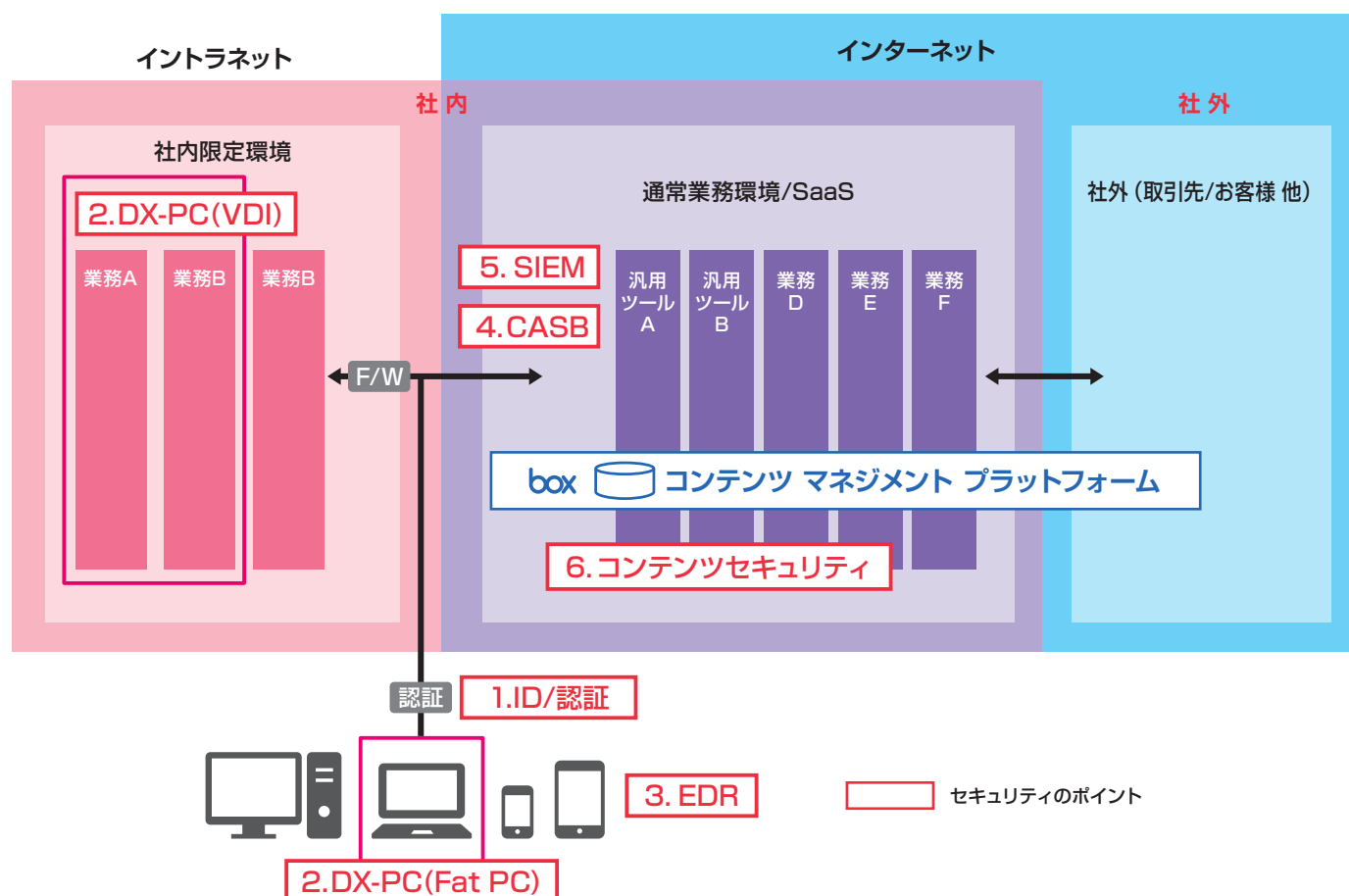
ます。脅威の実態と新しい働き方を考えると物理隔離やネットワーク隔離など、「ゼロトラスト」を前提としたセキュリティ対策が必要不可欠です。



新しい働き方
には新しい
考えが必要!



ゼロトラスト時代のセキュリティ全体像



1. ID/認証

システムを利用するユーザーのIDと氏名などをひも付けて保管する「IDデータベース」と、ユーザーが利用できるアプリケーションやデータなどを規定する「アクセスポリシー」に基づいて、クラウドと社内にまたがるアプリケーション認証を行い、正確なアクセス制御を行います。

2. DX-PC (Fat PC+VDI)

社内接続時はシンクライアント端末として仮想デスクトップ (VDI) へ接続し、内から外への通信を遮断。オンプレミス環境の機密情報の漏洩を防止。クラウドサービスはインターネットネイティブな環境で利用し、CASB/EDRにより厳重にガード。情報漏洩を防ぐために、公衆Wi-Fiや自宅LAN等への接続を遮断、紛失時にはリモートワイプされる。

3. EDR

PC やサーバー、スマートフォン、タブレットなどのネットワークに接続されているエンドポイントの監視を行い、サイバー攻撃を受けたことを発見して適切な対応をします。水際で防ぐ従来の手法と違い、エンドポイントが攻撃を受け、内部ネットワークへ侵入されることを前提として、その脅威をいち早く検知し、防御します。

4. CASB

管理者が意図しないクラウドサービスの利用が横行するとシャドーITのリスクが高まります。CASBは、ユーザーと複数のクラウドプロバイダーの間に単一のコントロールポイントを設けて、クラウドサービスの利用状況を可視化/制御することで一貫性のあるセキュリティポリシーを適用します。

5. SIEM

ソフトウェアなどの動作状況の記録 (ログ) を一元的に管理し、脅威となる事象をいち早く検知・分析します。SIEMは、単にログを一箇所に集めて管理するだけでなく収集された複数のログを横断的に分析し「相関分析」を自動で行うことが可能です。

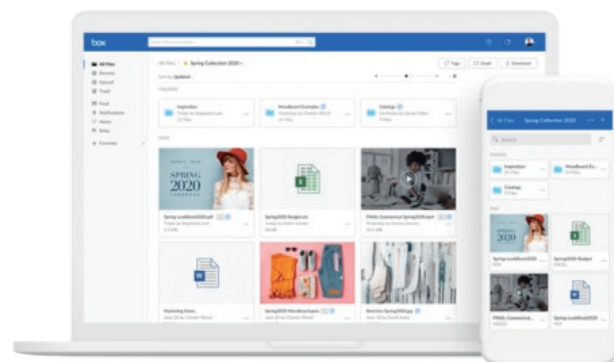
6. コンテンツセキュリティ

統合されたコンテンツ管理基盤で企業内のあらゆるコンテンツに対して共通のセキュリティポリシーを適用し保護します。また、通信やデータの暗号化やきめ細かな権限管理、リモートワークを前提にしたコンテンツ共有や脅威検出などを行うことが可能です。

セキュアなデジタルワークプレイスを実現するプラットフォーム Boxとは？

クラウドコンテンツマネジメントプラットフォームをリードするBoxは、ベスト・オブ・ブリード型アプローチで提供されるITスタックにより、企業のビジネスプロセスの加速、業務におけるコラボレーション強化、さらに企業が保有する情報の保護を支援します。2005年に設立され、Fortune 500企業に選ばれている企業の69%、日本の8,000社以上、グローバルの約100,000社を支援しています。

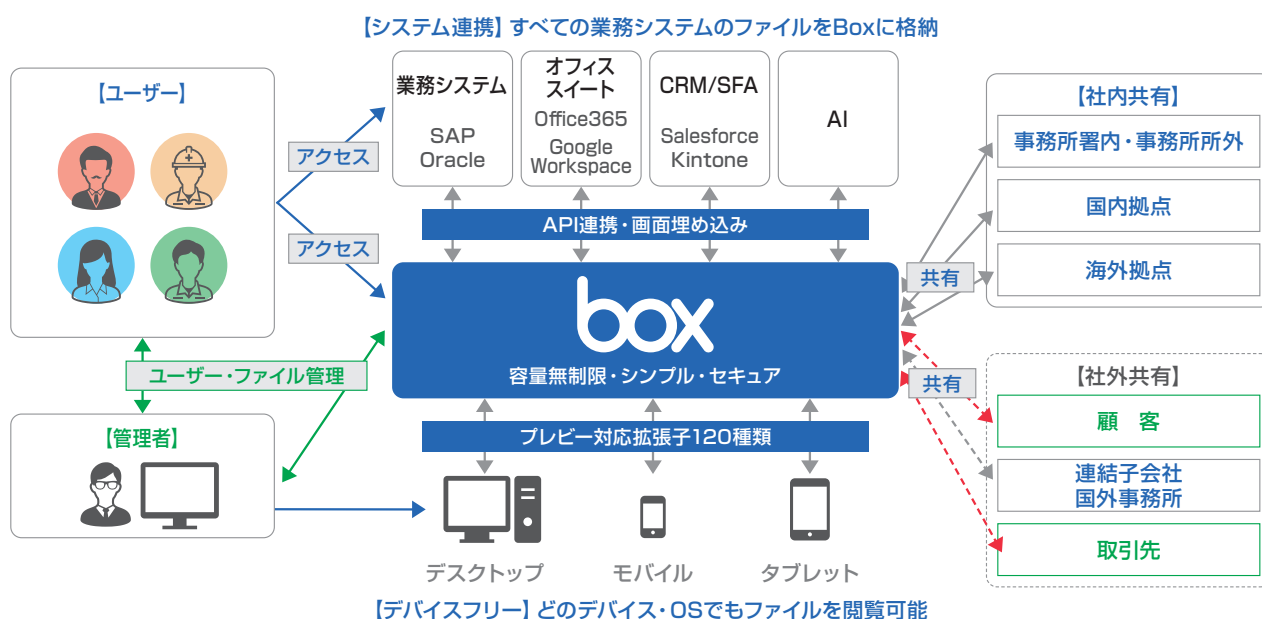
働き方を変え、業務効率や生産性の向上が強く求められるDX時代においては、従来からの物理的なワークプレイス(職場)から脱却し、既存の考え方やシステムにとらわれず、新しい考えのITを利用する必要があります。Boxのクラウドコンテンツ管理機能はデジタルワークプレイスを強力に支援します。



コンテンツセキュリティを実現するBox

「いつでも」「どこでも」「どんなデバイス」からでも必要な正しいコンテンツにアクセスができ、社内外問わず必要な人とコラボレーションし迅速にアウトプットを出せる。そして、それらは安全かつセキュアに管理されている。それが新しい働き方を支える新しいIT/ICTのあるべき姿「デジタルワークプレイス」。その核を担うのが「Box」です。

現代社会において多様な業務を効率的に支える「デジタルワークプレイス」はBoxだけでは完成しません。Boxはベストオブブリード戦略の下、全てのシステムスタックにわたり、国内外を問わず1,500社以上のソリューションと連携しています。そのため企業のコンテンツを一元化しやすくなるだけでなくセキュリティやガバナンス強化の観点でも貢献できるのです。

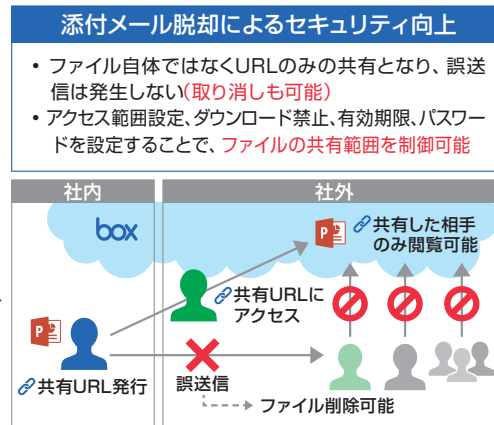
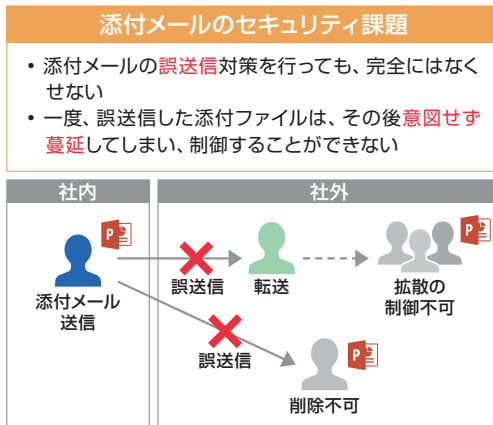


デジタルワークプレイス

Boxの活用で働き方はこう変わる!

セキュリティの向上

添付メールから脱却し、誤送信によるファイルの意図しない漏洩や
しっかりとしたファイルの権限管理でセキュリティが向上

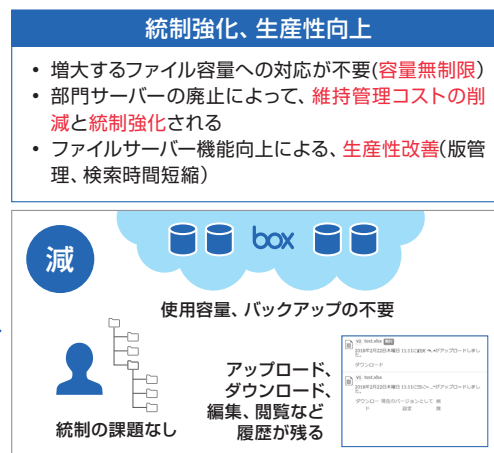
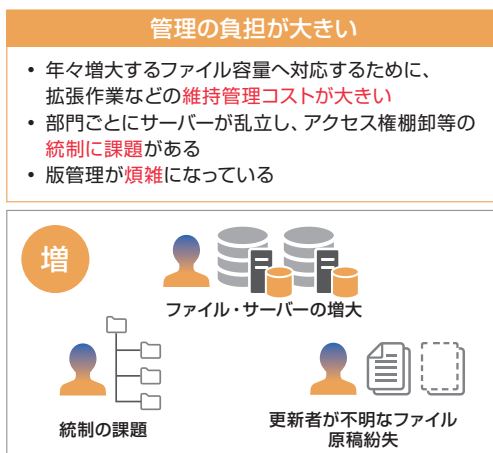


Boxの活用で
添付メールは
廃止できます!



統制強化と生産性

サーバー乱立を抑え、年々増大していくファイル容量への対応から
解放されることで統制強化および生産性向上を実現

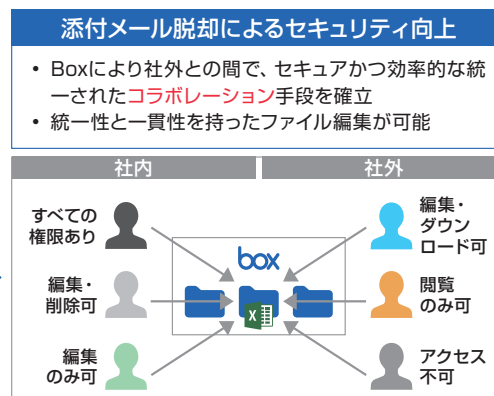
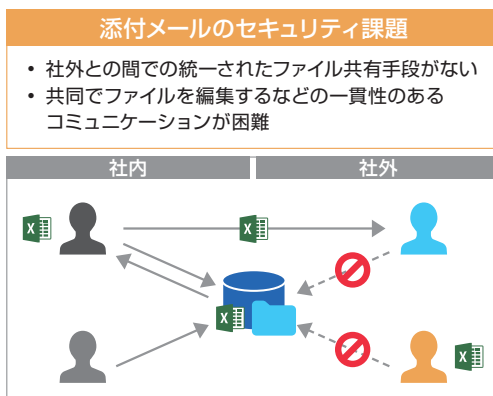


Box の利用で管理
負荷の軽減と生産
性向上の両立がで
きます!



ファイル共有の効率化

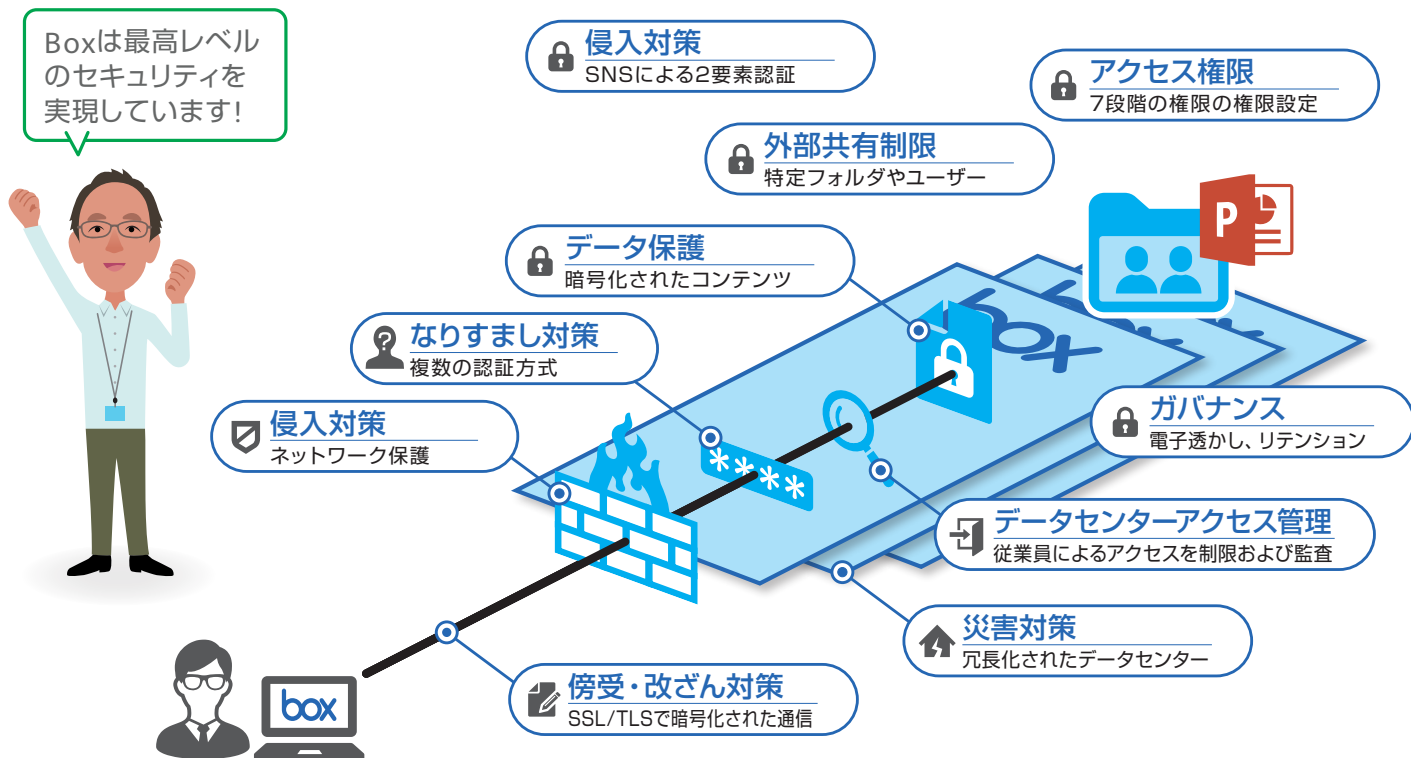
社内外のファイル共有の難しさを改善し、
セキュアで統一感のある効率的な社外コラボレーションを実現



Boxで社外
コラボレーションも
加速します!



ゼロトラスト時代を守るべきはコンテンツ コンテンツセキュリティを実現するBox



Boxのセキュリティ基本機能

1. きめ細かなアクセス権の設定

「閲覧できるがダウンロード不可」などきめ細かな7段階のアクセス権限。



2. セキュリティ分類

機密性に基づいてコンテンツを分類し、関連付けられたアクセスポリシーを適用します。



3. コンプライアンス対策

管理者であっても削除・改ざん不可能な7年分の監査ログ。



4. すべて暗号化

移動中は高強度のTLS 1.2暗号化、コンテンツ保存時も256ビットAES暗号化を使用してデータを保護します。



5. 多くの国際基準の認証を取得

BoxはISO 27001/27018やPCI DSSなど10以上の国際的なコンプライアンス・セキュリティ規格に準拠しており、その安全性が認められています。



6. ダウンロードせずにファイル共有

ビジネスファイルはBox上でプレビューできます。メール添付やコピー、ダウンロードなどのファイル拡散を防ぎます。



多様化する働き方にインテリジェントなセキュリティ

Box Shield

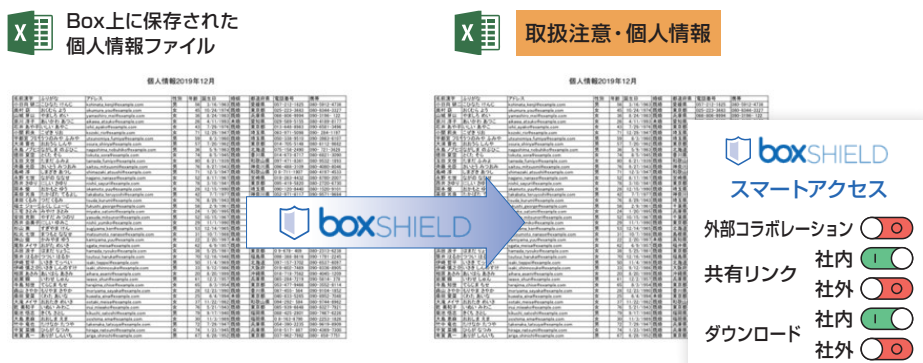


場所を選ばない働き方を推進する場合には、それに即したセキュリティ対策が必要です。

Box Shield は、このような時代の要請に応えるためのインテリジェントなセキュリティを提供します。

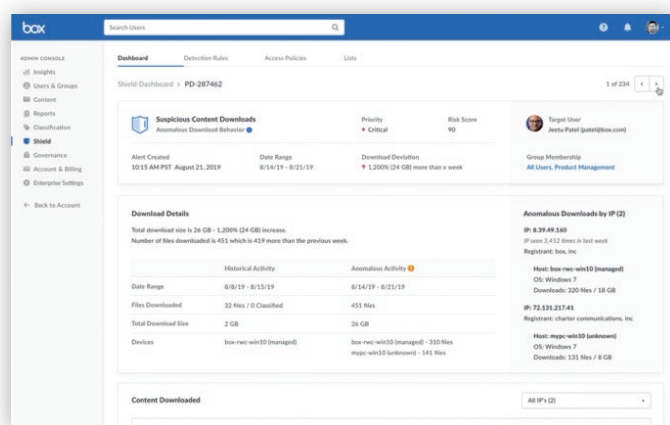
抜け漏れない情報漏洩対策を支援する「スマートアクセス」

手動または自動でコンテンツを分類し、分類ベースのセキュリティポリシーの適用が可能です。これにより高度なコンテンツ管理が可能になり情報漏洩を未然に防ぎます。



リモートワークを前提とした新たな「脅威検出」

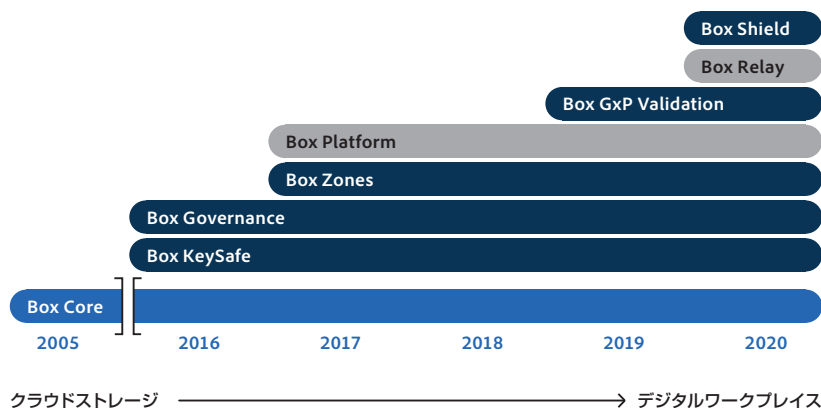
不審な場所、不審なアクセス、異常なダウンロードなどユーザーの行動に基づいてコンテンツ特有の脅威を自動で検出します。これらの設定は企業が細かくカスタマイズすることが可能です。



コンテンツセキュリティを強化するオプション機能

Box コア機能に加え、コンテンツセキュリティを強化するオプションを次々と提供しています。

暗号キーの管理 (Box KeySafe)、文書管理ルールなど情報ガバナンスを提供 (Box Governance)、データを特定の国・地域に保管する要件への対応 (Box Zones) など、必要なオプションを組み合わせることが可能です。



製品購入前のお問い合わせ

公式ホームページ

<https://www.box.com/ja-jp/home>

Boxの事例や各種記事・資料はこちら

<https://www.boxsquare.jp/>

こちらまで
お問い合わせを
お願いします!



デジタルワーク
プレイスの実現が、
働き方改革への
近道です!

これからはゼロ
トラスト前提で
セキュリティ構築
をしましょう!

Loren Ipsum

コンテンツ
セキュリティ
ならBoxが
おすすめです!

デジタルワーク
プレイスのご相談
はNRIとBoxに
お任せください!



box

株式会社 Box Japan

〒100-6510 東京都千代田区丸の内1-8-2

鉄鋼ビルディング15階

E-mail : japan-marketing@box.com

©2020 Box, Inc. All Rights Reserved. Boxおよび商品は、Boxの米国あるいはその他の国における登録商標または商標です。その他の社名、商品名はそれぞれの所有者の商標または登録商標です。記載された製品の仕様・機能等は改良のため予告なしに変更される場合があります。

/NRI SECURE/

NRIセキュアテクノロジーズ株式会社

〒100-0004

東京都千代田区大手町1-7-2 東京サンケイビル

E-mail : info@nri-secure.co.jp