

業務端末のセキュリティ対策、テレワーク導入による利便性向上、コスト抑制の三重苦を
今あるIT資産を活用しながら解消する方法

業務端末の選択肢の一例と設定情報などユーザーデータの所在について



方法	各PCに残る方式	自社内で集中管理する方式	クラウドサービス上で管理
	 ・ 個人に配布した業務用PCにデータが残る方式 ・ 端末にセキュリティソフト入れる ・ 傍受されにくい回線機器を選ぶ	  ・ サーバーで集中管理する方式 ・ 仮想化するケースが多い ・ データセンターにサーバーを預ける場合もある	 ・ MicroSoftやAWSなどサービス事業者の重量課金制のサービスで管理する。
ギョーカイ人的には？	セキュアPC・SASE(サッシー)※指原莉乃ではない	VDI※ドメスティックバイオレンスではない。	Daas(ダース)※チョコレートではない
コスト面	最新のセキュリティソフト入れたり、秘匿性の高いネットワークサービスを契約したり、カッコいいサーバーを購入したり、今風なクラウドサービスを契約したり、、、結局、いろいろ揃えると似たり寄ったりな金額感ではか？と悟りの境地に...orz...賃貸vs持ち家論争くらいひとによる。		
メリ・デメ	挙げるとキリがない、販売会社やE/U担当者の好みの問題ではないか？と悟りの境地に...orz...マンションvs一軒家論争みたいなw		
端末管理で気を付ける点	 PCの紛失対策  端末側のOSの更新	 PCの紛失対策  端末側のOSの更新	 PCの紛失対策  端末側のOSの更新
	ユーザーのデータが端末側に残る、自社のサーバーに残る、クラウドサービス上に残る、どの場合にもosの更新の管理工数や紛失した際のリスクがあります。		

IPAの発表資料

情報セキュリティ10大脅威 2024

IPA

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した脅威	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃(ゼロディ攻撃)	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化(アンダーグラウンドサービス)	2017年	2年連続2回目

Copyright © 2024 独立行政法人情報処理推進機構

参照元:独立行政法人情報処理推進機構「情報セキュリティ10大脅威2024」

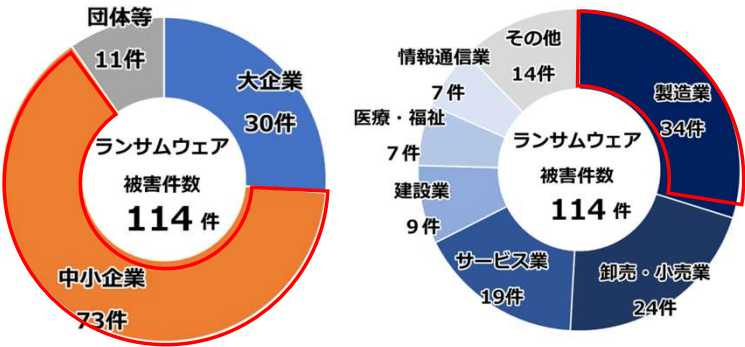


驚異の水トアナ越え

警視庁サイバー警察局発表資料

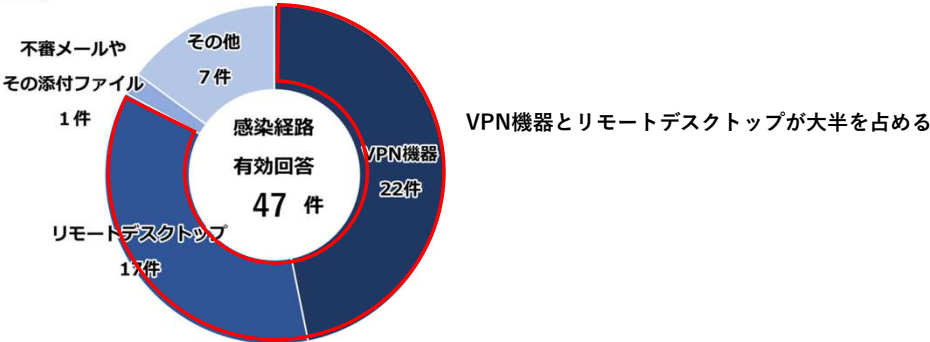
ランサムウェアの被害に係る統計②

3 被害企業・団体等の規模別／業種別報告件数



4 ランサムウェア被害にあった企業・団体等へのアンケート調査の回答結果

● 感染経路



参照元:警視庁サイバー警察局 令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について

セキュリティ事故は

テレワーク環境下で様々な要因でOSの更新ができなかったり、
外出先でたまたま接続したWi-Fiなど
何らかの弱ったところを突かれてウィルス感染した端末を経由して
社内に侵入されて発生する可能性が高いです。。。

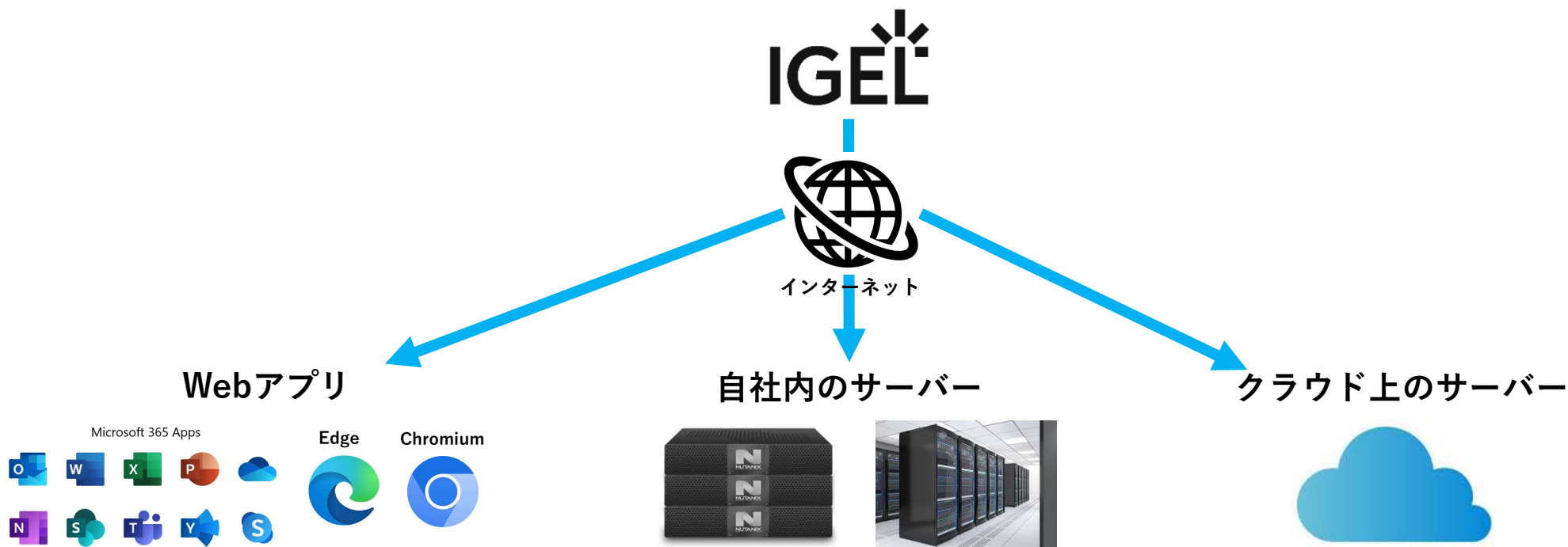
多くの端末で採用されている**Windows OSの脆弱性**は恐らくはなくなることはなく、

今後もハッカーとOS提供事業者、セキュリティ屋さん

イタチごっこな状況は続くと予想します…。

ゼロトラストOS 『IGEL』 で端末に一切データを残さない運用が可能です。

データが残らないOS



※何もインストールできないので端末側にEDR等のセキュリティ製品を入れる必要もなくなります。
昨年のCloudStrike Falconのブルースクリーンの障害からIGELへ切り替えた企業様もいらっしゃいます。

ご提案のポイント



従業員の
利便性



対ウィルスへの
堅牢性



システム管理者の
保守性



既存のIT資産を活かす
コスト性

「IGEL OSはLinuxをベースに開発された、脆弱性の少ない堅牢なOS(端末)です。」

最近ではシンククライアントではなく**ゼロトラストOS**とも呼ばれています。

それ単体で動くことはなく、Webアプリや社内のサーバー、クラウドのサーバーにリモートアクセスして業務を行います。

あらゆるPCをシンククライアント端末化できます。



USB起動方式

個人利用のPCもUSBブートで起動させることで
シンククライアント専用端末に変身します。
自由度と保守性の両方を実現する方式

選べる2つの方式



OSインストール方式

完全にWindowsをなくしてしまう方式
端末の機能を限定させることができるので
官公庁や製造業で実績あり

普段使用しているHDD領域には一切アクセスしないため、Windows側のセキュリティ対策が不十分でもOK。
VPN接続してリモートアクセスするだけの専用端末に早変わり！USBを抜いて再起動すればWindowsに戻ります。

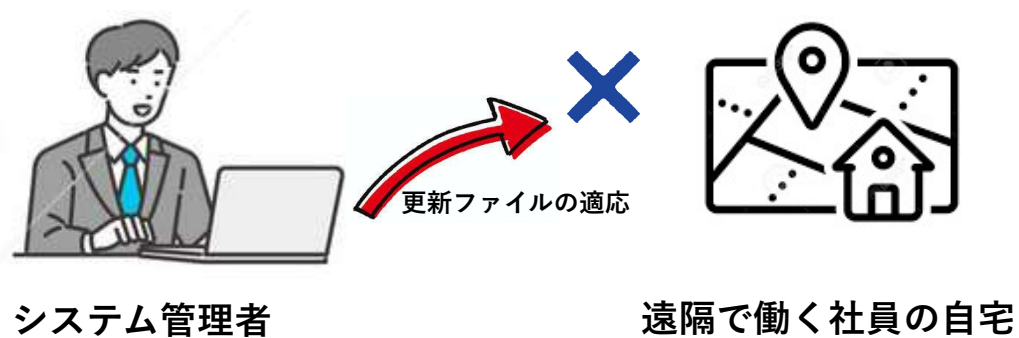
BIOSの起動キーは
Dellなら『F2』キーとか
Lenovoなら『F1』キーなど
メーカーによって異なります。

1.社内やクラウドに接続する為のリモート接続の認証機器は特定のメーカー製品に限られてしまうことが多かった。



既存のネットワーク認証機器やサーバーなどのIT資源を有効活用できない。。。

2.遠隔地にあるOSの更新や設定変更がリモートで行えない。



トラブルがあった時、
OSの更新や設定変更の度に出社を促す必要があり、
フルリモートで働く方へのサポートが困難になってしまう。
優秀な人材の確保が難しくなることも。。。

3.ZoomやTeamsなどリモート会議が上手く動かないことが多かった。

自宅で起動したシンククライアントでWeb会議をするときの通信経路



社内のサーバーやPCを経由してWeb会議などのデータを送受信するので通信遅延が発生したり、マシンに負荷がかかり上手く動かなくなる。

シンククライアントは

「端末になにも保存できない！ なにもさせない！ だから堅牢です！」

（昔の先生が行っていた、「バカは風邪ひかない的な・・・？」）

という思想ゆえ、様々な利便性が損なわれており、あまり普及されませんでした。

ここからはIGELの特長を紹介しますが、
端的に言うと、IGELは堅牢性と利便性の良いとこどりができるゼロトラストOSです

IGELの特長 ①世界最強のテクノロジーアライアンス『IGEL Ready』

100社以上の主要なIT企業と技術提携。
シンクラOSにありがちな、特定のメーカーの環境には接続できない。といった心配はございません。



皆様の会社で利用されているPC、ネットワーク認証機器やサーバー、クラウドサービスを有効活用しながら
端末を強固にできます！

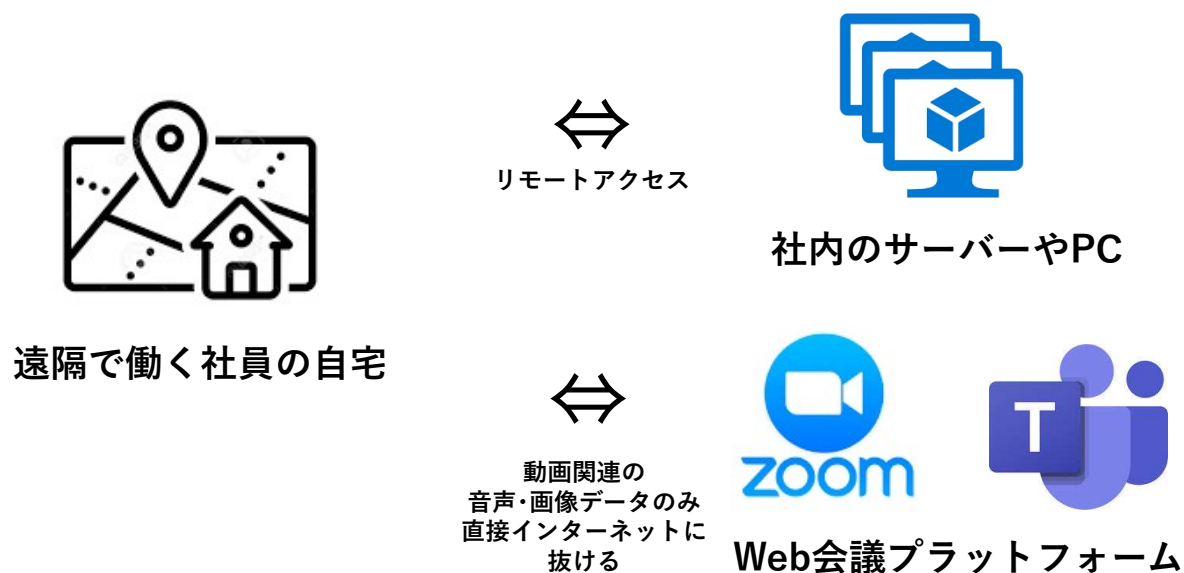
遠隔地にあるOSの更新や設定変更がリモートで行えます！



トラブル時の対応、部署移動に伴う設定変更なども全てリモートで対応可能です。

ZoomやTeamsなどの動画情報など
必ずしも社内サーバーを通す必要のないパケットは自宅から直接インターネットサービスに逃がす機能があります。

自宅で起動したIGELでWeb会議をするときの通信経路



社内の通信機器やサーバーの負荷も減り、従業員全員が快適な業務環境になります。

Microsoft社とも技術提携をしているので、AzureやIntune、M365、Win365との連携もばっちり



クラウド上の端末(DaaS)



Webアプリ(SaaS)



Microsoft
Entra ID

認証



Microsoft Intune

端末管理

既存のMicrosoftライセンスも最大限ご活用いただけます。

端末を紛失してしまった場合や遅い、繋がらないといった障害の切り分けなどに対応する機能が備わっています。

紛失した際のリモートワイプ機能



システム管理者



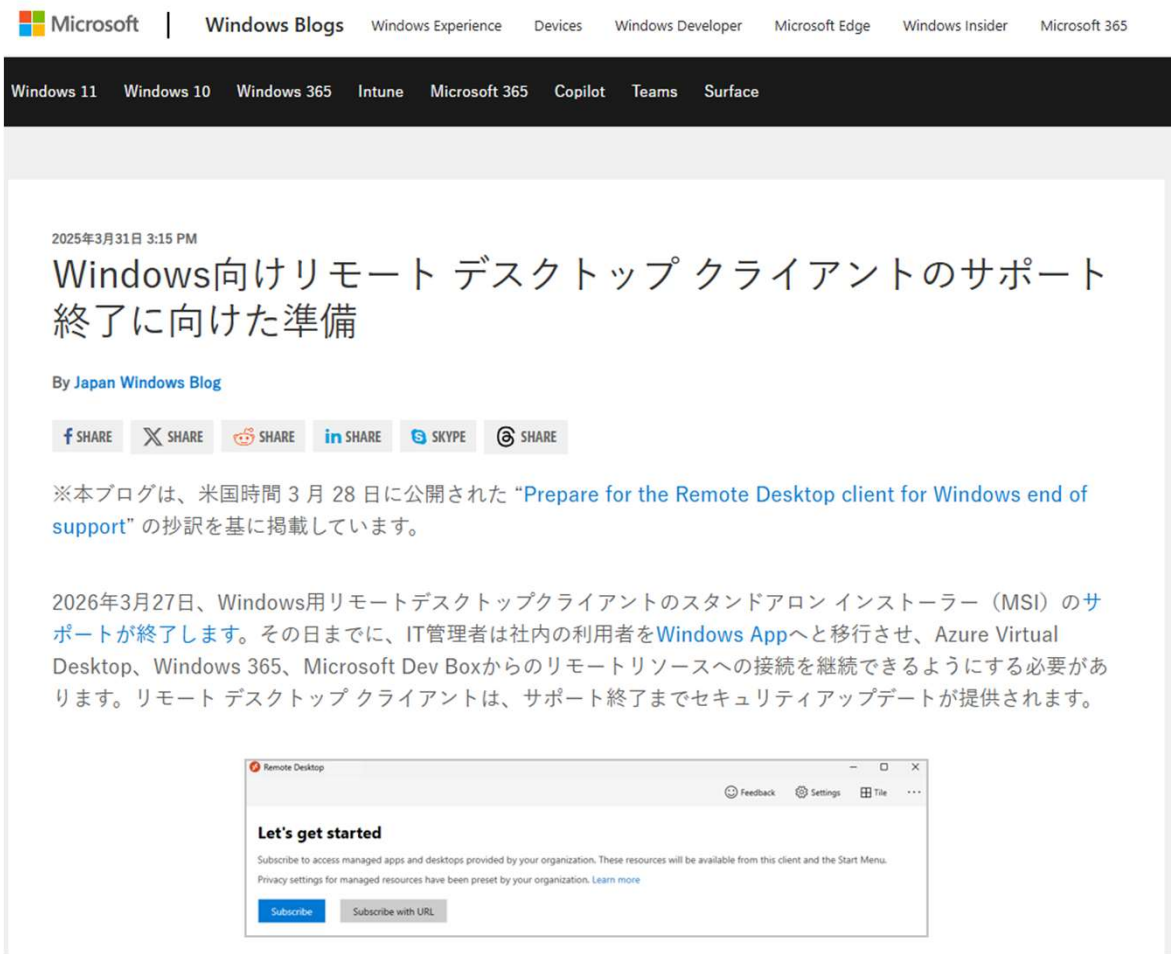
遠隔での無効化

Liquidware製品と組み合わせた リソースモニタリング



- ・ 端末or回線の障害の切り分け
- ・ Web閲覧履歴の参照
- ・ 勤怠情報の取得

RDPクライアントのサポート終了に向けた準備ということでIGELの情報も入れておきたいという動きも見受けられます。



参照元：<https://blogs.windows.com/japan/2024/03/31/prepare-for-the-remote-desktop-client-for-windows-end-of-support/>

ご提案のポイント



従業員の
利便性



対ウィルスへの
堅牢性



システム管理者の
保守性



既存のIT資産を活かす
コスト性

遠隔での設定変更可能
専用USBで私用PCを業務端末化

脆弱性がほぼないOS
(NASAや米国防も導入)

遠隔での設定変更可能
リモートワイプや
シャドーウィングが可能

どんな機器とも連携可能

既存のシステム環境・運用で適合するかなどを確認する為のトライアル環境のご利用のご相談も承っております。



導入目的

研究職の方が海外出張に行く際にシンクライアント端末を持たせて、万が一の際の政府によるPC押収に備えたい。

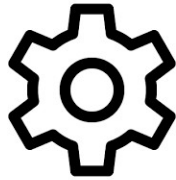
選定理由

端末にデータを残したくない
遠隔での設定変更が可能な点
リモートワイプができる点

補足 ユーザーデータとユーザーファイルについて

ユーザーデータ

端末の設定情報



Ex. 部署ごとの設定や役職ごとの権限管理、辞書やお気に入りなどPCを動かすための基礎となるデータ

保存先



PC



ユーザーファイル

Office系アプリやAdobeのファイル



保存先



PC



ファイル
サーバー



クラウド
ストレージ

ユーザーファイルはBoxやOneDriveなどのクラウドサービス上にリダイレクトをかけるケースが増えてきている傾向
本日の説明した「データ」というのはユーザーデータの意味合いが強いです。