情報通信技術面における留意点

ネットワンシステムズ株式会社
シニアエキスパート　尾形誠治
（ 総務省地域情報化アドバイザー／テレワークマネージャー）

目 次

ネットワンシステムズ会社概要

お客様の成長を支援するための価値を共創

マルチベンダー・インテグレーション

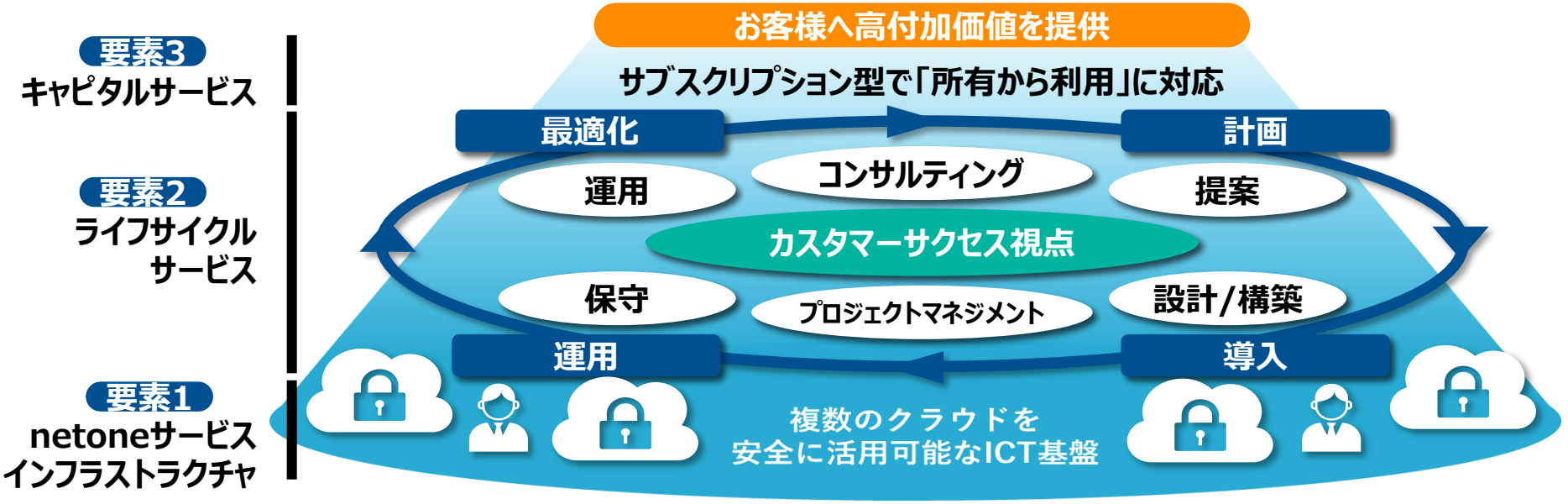
最先端の製品を組み合わせ、
性能・効果を独自に評価した上でご提案

付加価値

ICT利活用の成功・失敗の知見

お客様に提案するICTをまず社内で実践
- 働き方改革・マルチクラウド・セキュリティ -

ネットワングループの活動全てを「統合サービス事業」と定義
新たにカスタマーサクセスの視点を導入し、お客様への付加価値を追求



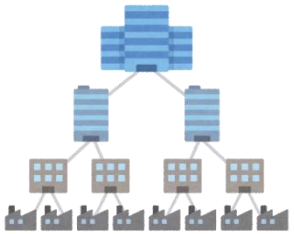
01 背景

コロナ禍による急激な環境変化

キャッシュレス化

危機管理
健康意識の高まり

事業のオンライン化
サプライチェーンの見直し



人口減少
働き方改革

ESG
投資
SDG's

障害者雇用
リカレント教育

東京
一極集中

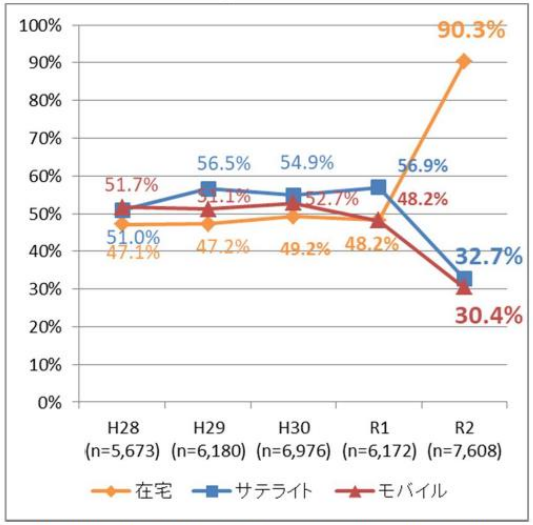
移住
促進

テレワークの実態

実施場所として在宅型が約90%と突出して多くなっている。

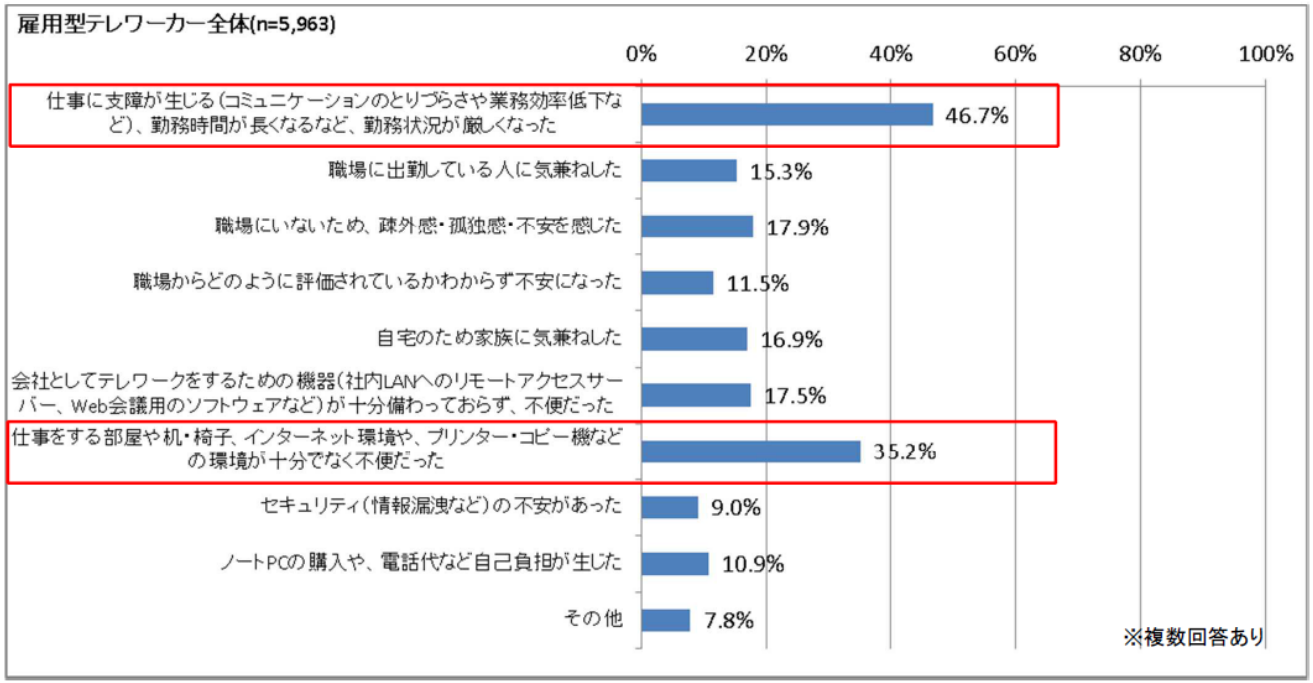
- コミュニケーション不足
- 業務効率の低下
- 勤務状況の悪化
- 環境が不十分

テレワークの実施場所別のテレワーカーの割合※【H28-R2】
（雇用型・自営型を含むテレワーカー全体）



※図中の%は、R1以前は全テレワーカー（これまでテレワークをしたことのある人）に対する割合。今年度のみ、テレワーク実施場所回答者に対する、各場所でテレワークをしている人の割合。

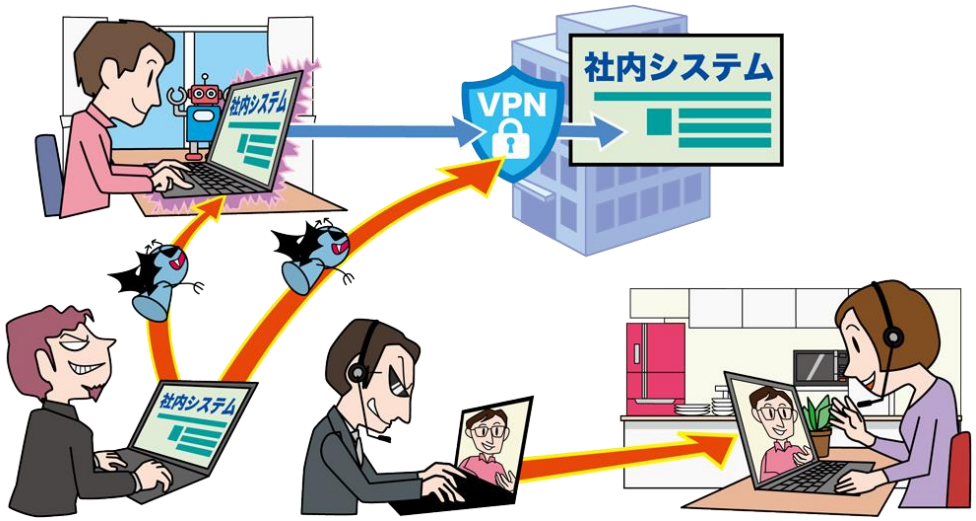
テレワークを実施して悪かった点（雇用型テレワーカー全体）



出典：国土交通省　令和2年度テレワーク人口実態調査

情報セキュリティ10大脅威 2021

第3位　テレワーク等のニューノーマルな働き方を狙った攻撃
（初めてランクインした脅威）



2020年は新型コロナウイルス感染症　（COVID-19）の世界的な蔓延に伴い、政府機関から感染症対策の一環として日本の組織に対してニューノーマルな働き方の一つであるテレワークが推奨された。組織のテレワークへの移行に伴いウェブ会議サービスやVPN等の本格的な活用が始まった中、それらを狙った攻撃が行われている。

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	標的型攻撃による機密情報の窃取
3	テレワーク等の ニューノーマルな働き方を狙った攻撃
4	サプライチェーンの弱点を悪用した攻撃
5	ビジネスメール詐欺による金銭被害
6	内部不正による情報漏えい
7	予期せぬIT基盤の障害に伴う業務停止
8	インターネット上のサービスへの不正ログイン
9	不注意による情報漏えい等の被害
10	脆弱性対策情報の公開に伴う悪用増加

出典：IPA情報セキュリティ10大脅威 2021

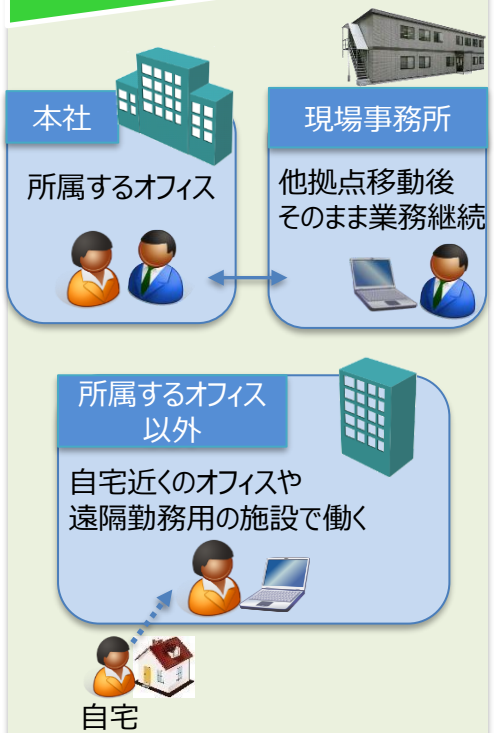
02 テレワークに必要なICTツール

テレワーク導入のフェーズ

少しずつテレワークの範囲を拡大していく

ペーパーレス
✓ 紙を無くすのが第1歩

サテライトオフィス
✓ 所属するオフィスから離れて働く
（セキュリティが確保されている）



モバイルワーク
✓ 移動中やその合間に働く
✓ 現場などから状況を伝える

在宅勤務
✓ 自宅を就業場所として働く

**どこにいても、従業員同士
コラボレーションしながら
業務を実施**

各フェーズで必要なICTツール例

net one

業務へのアクセスとコミュニケーション手段がポイント

	ペーパーレス ✓ 紙を無くすのが第1歩	サテライトオフィス ✓ 所属するオフィスから離れて働く	モバイルワーク ✓ 移動中や合間に働く ✓ 現場などから状況を伝える	在宅勤務 ✓ 自宅を就業場所として働く
				
① どうやって業務データにアクセスさせるか？	無線LAN ペーパーレス会議システム	無線LAN ＋ ノートPC 業務システムのweb化 データ統合基盤 ファイルサーバ／クラウドストレージ	モバイルデバイス配備 リモートアクセス（限定）	リモートアクセス
② どうやって社内のメンバーとコミュニケーションを取るか？		リモート会議（複数拠点）	チームメッセージング ビジネスチャット＋ファイル共有等 電話のモバイル化	リモート会議（社外）

自社にあったテレワークの接続方式を確認してみましょう

net one

テレワーク方式確認のフローチャート

自宅等から会社ネットワークに接続する

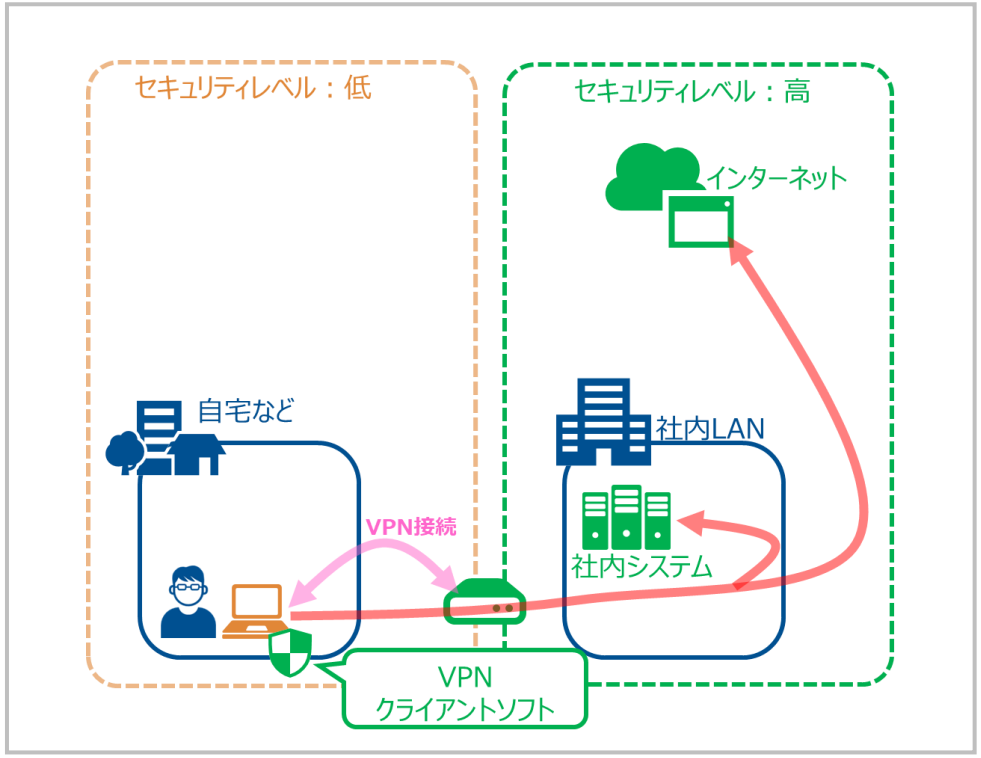
- 接続する
  - テレワーク時に会社データを端末に保存する
    - 保存する
      - テレワーク時にファイルをダウンロードして保存可能
      - → **【方式①】** VPN方式
    - 保存しない
      - テレワーク時にどのような業務を行うか
        - ファイルの編集・閲覧等を実施する → **【方式②】** リモートデスクトップ方式
        - ブラウザ利用のみ → **【方式③】** ・セキュアブラウザ方式
- 接続しない
  - テレワーク時にクラウドサービスを利用する
    - 利用する → **【方式④】** ・会社非接続方式（クラウドサービス型）
    - 利用しない → **【方式⑤】** ・会社非接続方式（手元作業型）

クラウドサービス例

※総務省「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」を参考に作成

方式①：VPN方式

VPN方式	持ち帰ったPCを利用して、自宅などから社内にVPNで接続し、社内の業務システムなどを利用する方式
メリット	低コストですぐに実装できるため導入しやすい
デメリット	情報漏えいや不正利用など、セキュリティリスクが高い

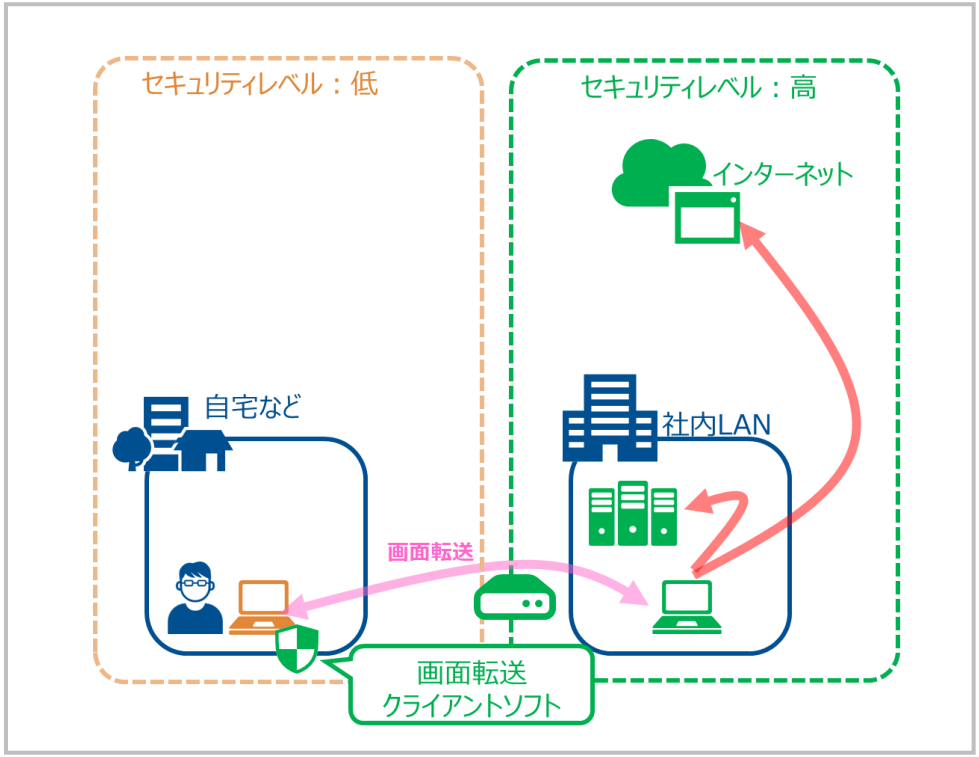


●VPNとは

Virtual Private Networkの略。あたかも自社ネットワーク内部の通信のように、自宅や外出先などの遠隔の場所から社内ネットワークにアクセスが行える技術のこと。

方式②：リモートデスクトップ方式

リモートデスクトップ方式	自宅などのPCから社内の自席PCに接続して遠隔操作する方式
メリット	データは社内の自席PCに保存されるため、情報漏洩のリスクをVPN方式より低減できる
デメリット	・リモートデスクトップが不正に利用された際の影響範囲が大きくなる ・自席PCが故障すると、リモートワークが出来なくなる

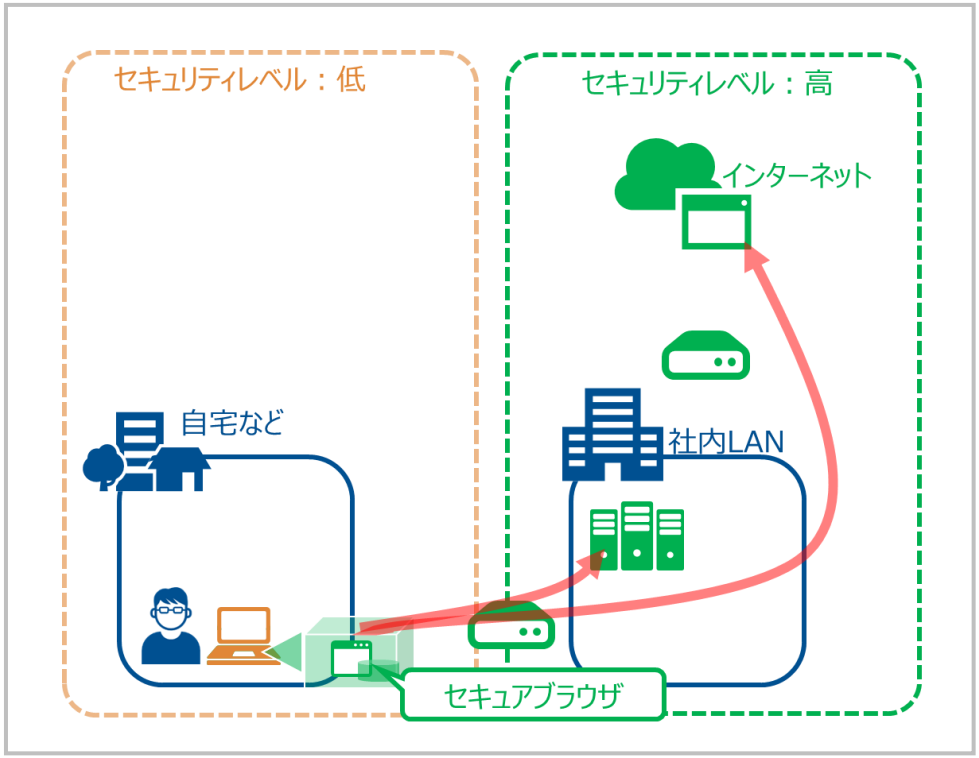


●リモートデスクトップとは

社内ネットワークに置いてあるPCの画面をネットワーク経由で手元PC（テレワーク端末）に転送して表示し、遠隔からネットワーク上のPCを操作する技術のこと。

方式③：セキュアブラウザ方式

セキュアブラウザ方式	特別なブラウザ（セキュアブラウザ）を利用し、手元の自宅PCなどから社内システムやクラウドサービスで提供されるアプリケーションソフトウェアにアクセスする方式
メリット	・大規模なサーバ基盤が不要であるためコストを大幅に低減できる ・情報漏洩などのリスクを抑えられる
デメリット	・Webページを正常に表示できない場合がある ・対応していないソフトなど、一部業務ができない場合がある



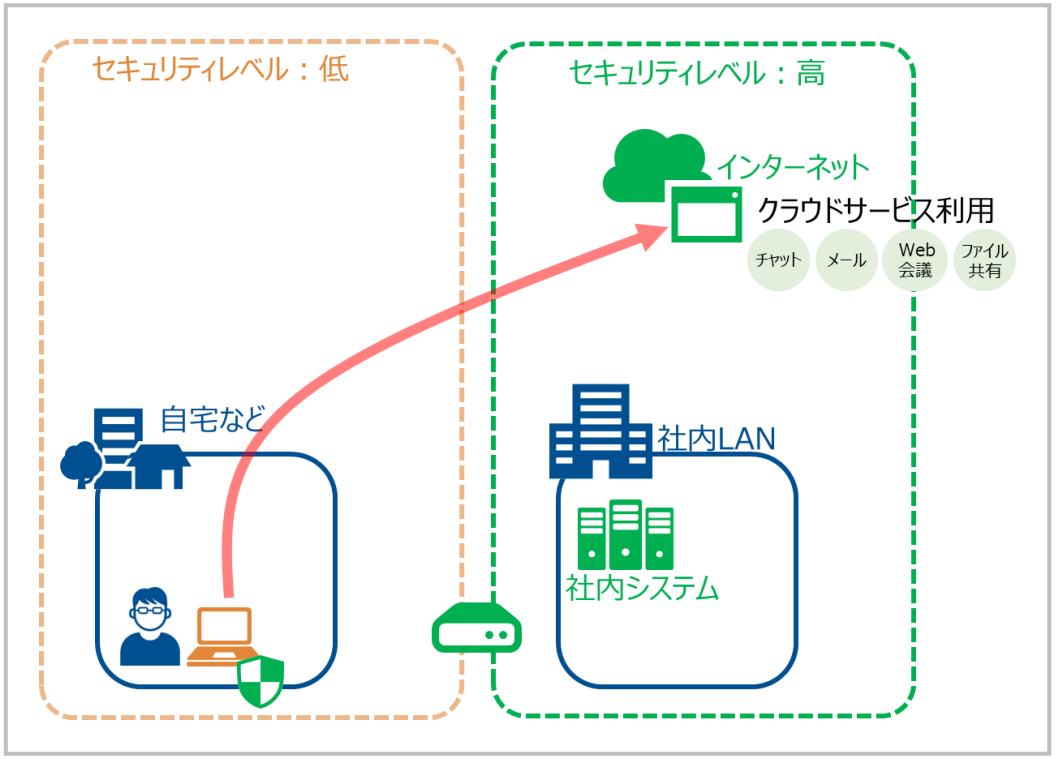
●セキュアブラウザとは

一般的なWebブラウザの基本機能を持ちながら、不正アクセスや情報漏えいを防止するための対策が施されている。ベンダー各社、特色のあるセキュアブラウザサービスを提供している。

端末へデータ保存をしないことが特徴。

方式④：会社非接続方式（クラウドサービス型）

クラウドサービス型	自宅などのPCからインターネット上のクラウドサービスで提供されるアプリケーションソフトウェアにアクセスする方式
メリット	・固定資産を社内に持つ必要がない ・場所や端末を問わず、どこでもサービスを利用できる
デメリット	・クラウドサービスが止まってしまうと、業務が継続できない ・設定に不備があると情報が公開されてしまう



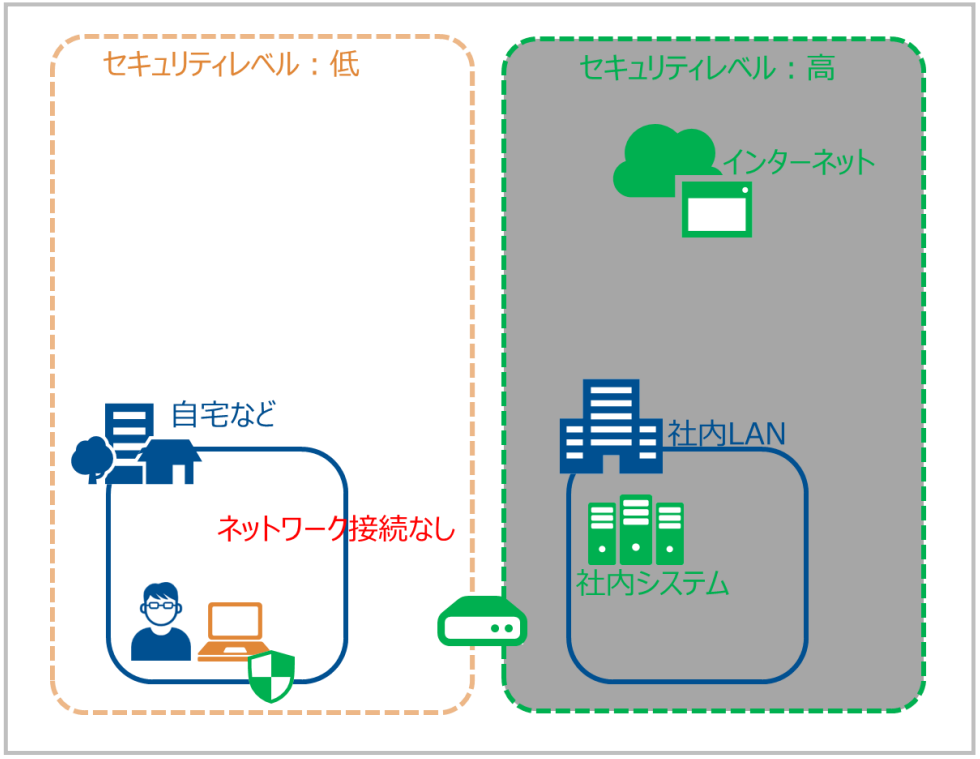
●クラウドサービスとは

従来は、PCやサーバで管理・利用していたようなソフトウェアやデータ等を、インターネット等のネットワークを通じて利用できるようにした様々なサービスの総称。

（例）メール、チャット、オンライン会議、ファイル共有など。

方式⑤：会社非接続方式（手元作業型）

手元作業型	持ち出しPCにあらかじめデータやファイルを保存し、自宅などの場所で作業を行う方式
メリット	既存のPCをそのまま利用でき、慣れている環境で業務が継続できる
デメリット	・PCの盗難や紛失による情報漏洩 ・公衆Wi-Fi接続によるウイルス感染



●テレワーク端末へのデータ保存

テレワークの際に、社内サーバやクラウドサービスにデータを保存するのではなく、テレワーク環境で利用する（持ち出して利用する）端末にデータを保存する場合を指す。

方式ごとの比較（可能な作業）

～製品選定における「見落としがちな穴を見つけて対策する」ための要素～

net one

表の見方

できる	できない

比較項目		①VPN方式	②リモートデスクトップ方式	③セキュアブラウザ方式	④会社非接続方式（クラウドサービス型）	⑤会社非接続方式（手元作業型）
可能な作業	Webページを見る	○	○	○	○	×
	任意のファイルサーバを利用する	○	○	×	○	×
	任意のファイルを編集する	○	○	×	○	×
	任意のアプリを利用する	○	○	×	○	×

▶赤塗箇所に関する特記事項：

- 手元作業型は、インターネットに接続できないため、手元のPCに入っている情報以外の作業は出来ず、効率が落ちる可能性が高い
- セキュアブラウザ方式では、例えば、ファイルサーバの操作やブラウザ以外のアプリの利用など、ブラウザを使ってできない操作は実行できない
- Windows統合認証など、Windowsに依存する機能も利用できないことが多い
- 印刷機能も製品ごとにサポート内容に差が出るため、確認が必要

方式ごとの比較（セキュリティの強度）

～製品選定における「見落としがちな穴を見つけて対策する」ための要素～

net one

表の見方

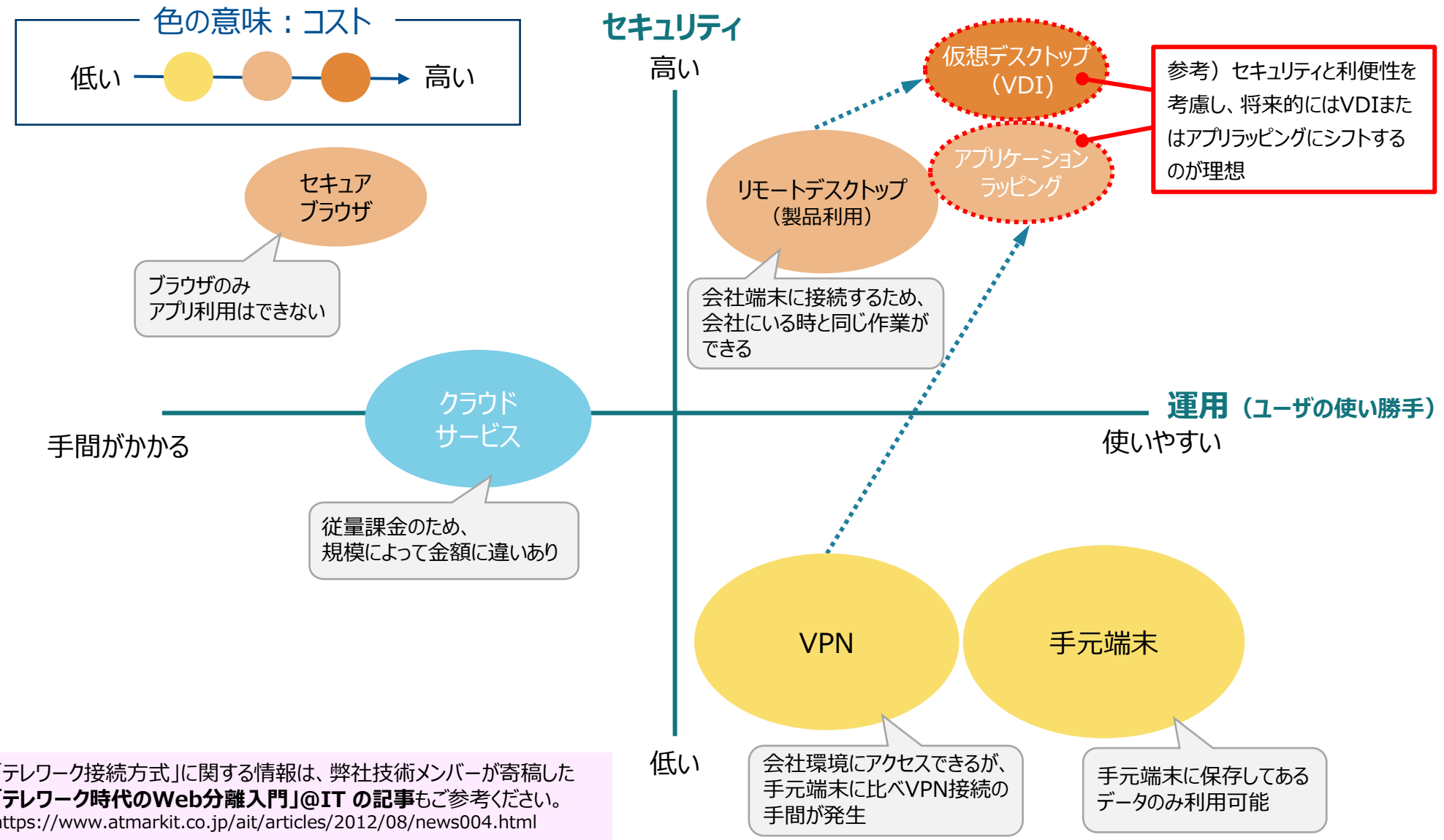
高い　低い

比較項目		①VPN方式	②リモートデスクトップ方式	③セキュアブラウザ方式	④会社非接続方式（クラウドサービス型）	⑤会社非接続方式（手元作業型）
セキュリティ面のポイント	マルウェア	×	×	○	×	○
	端末の紛失・盗難	×	×	○	○	×
	重要情報の盗聴	×	○	×	×	×
	不正アクセス	×	×	×	×	○

▶赤塗箇所に関する特記事項：

- マルウェア対策については、会社PC持ち帰り方式（VPN方式）やリモートデスクトップ方式は、EDRやアンチウイルスソフトの導入などが別途必要。一方、セキュアブラウザ方式は、「利用終了後に環境ごとデータを削除する」「exe形式のファイルの実行を禁止する」などの機能を標準で実装している
- 重要情報の盗聴については、リモートデスクトップ方式は、画面転送型なので、暗号化通信が仮に復号されたとしても、実データが盗聴されることはないという強みがある
- 不正アクセスは、多要素認証システムと組み合わせるなどの対策がどの方式でも必要。ログインに関わる操作が増えることで利便性は低下するが、昨今の状況を鑑みると、多要素認証の導入は必須といえる

テレワーク接続方式の選択イメージ



「テレワーク接続方式」に関する情報は、弊社技術メンバーが寄稿した**「テレワーク時代のWeb分離入門」@IT の記事**もご参考ください。
https://www.atmarkit.co.jp/ait/articles/2012/08/news004.html

その他主なテレワーク関連ツール①

コミュニケーションツール選択の主なポイント

- ▶ 操作が簡単で全員が使いこなせるか
- ▶ 自社のコミュニケーションにおける課題を解決できるか
- ▶ やりたいことを満たせる適切な機能があるか
- ▶ 業務情報をSNS等で共有しない

情報共有ツール選択の主なポイント

- ▶ 業務を行う上で何の機能が必要か
- ▶ 利用する端末に対応しているか
- ▶ 自社で使いこなせそうな操作画面か
- ▶ アップロードできる容量と期間
- ▶ シャドーIT利用を禁止する

No	ツール	概略	テレワーク形態との関係	製品例
1	Eメール	社内・社外を含めた業務コミュニケーションの中核ツール。 現在利用中のメールサーバのシステムが、外部からの接続が難しい状態になっている場合等、テレワークへ対応が難しい場合には、他のメールサービスへの転送や、新たなメールサービスの導入を検討する。	形態にかかわらず、全ての実施形態で必要。	Eメールについては、ほとんどの企業で導入済みであるため、サービスの比較は割愛する。
2	チャット	会話のように、単文のやりとりを行うソフトウェア。3名以上のグループでやりとりする場合もある。なお、社外へのデータ流出が起こらないよう、セキュリティ管理のしっかりしているビジネスチャットあるいはweb会議等付属のチャット利用が望ましい。	形態にかかわらずビジネスチャットあるいはweb会議付属のチャットの導入を検討する。	chatwork/chatwork(株) LINE WORKS/Works Mobile Japan(株) slack/Slack Japan(株) WowTalk／ワウテック（株） InCircle/AI CROSS（株） TopicRoom/NTTテクノクロス（株）
3	会議システム	会議システムを導入することで、対面コミュニケーションに近い状態での会議や打合せを気軽に実施することが可能になる。 移動にかかる交通費と時間の削減にも繋がる。 いずれかの製品の導入を検討する。	テレワーク実施形態が、在宅勤務/終日在宅の場合は職種や規模にかからず導入検討が必要。その他の実施形態でも導入が望ましい。	V-CUBE ミーティング/(株)ブイキューブ WebEx Meeting Center/シスコシステムズ合同会社 LiveOn/ジャパンメディアシステム(株) Zoom/Zoom Video Communications, Inc. Teams/日本マイクロソフト(株) Meet/グーグル合同会社
4	情報共有ツール（データ共有）	インターネット上にファイルを保存できる「オンラインストレージサービス」を使用することで、大容量ファイルの円滑なやり取りが可能になる。 なお、社外へのデータ流出が起こらないよう、利用する場合は運用方針を定めることが望ましい。	いずれの形態でも導入を検討する。	Dropbox、Googleドライブ（G Siute）、OneDrive（Microsoft365）、BOX等の多くのサービスがあり、一定容量まではいずれのサービスでも無料での利用が可能である。 グループウェア製品にもオンラインストレージサービスが含まれる。 一定容量までは無料でのサービスが多く、機能差も少ないため、サービスの比較は割愛する。
5	情報共有ツール（SNS）	メッセージ投稿と返信等を行うことによりコミュニケーションを円滑化する。 サービスによっては、企業単位ではなく、グループ単位等に制限した形でのメッセージのやりとりも可能。 なお、Twitter、Facebook、LINE等の社外にも広く拡散する可能性のあるSNSでは、機密情報を扱わないように運用方針を定めることが望ましい。	在宅勤務/終日在宅の場合は、気軽なコミュニケーションを円滑にするため、職種や規模にかかわらず導入を検討する。	Twitter、Facebook、LINEが代表的なサービス。Yammer（Microsoft365）はビジネス用途に特化している。また、グループウェア製品の多くにSNS機能が含まれる。 SNSのみを目的に有料ソフトを導入することは多くないと思われるため、サービスの比較は割愛する。

出典：日本テレワーク協会
テレワーク関連ツール一覧（第5.0版）

その他主なテレワーク関連ツール②

管理ツール選択の主なポイント

- ▶ 管理を行う上で何の機能が必要か
- ▶ 利用する端末に対応しているか
- ▶ 自社で使いこなせそうな操作画面か

No	ツール	概略	テレワーク形態との関係	製品例
1	勤怠管理ツール	勤怠管理については、労働時間の記録のみであればグループウェア等でも対応可能。給与計算ソフトや人事管理ソフト等との連携を重視する場合には、専用ツールの導入を検討する。 営業職がいつどこを巡回したかを明らかにするためにGPSでの位置情報を記録するサービスがある。 また、作業状況を確認するために、画面キャプチャを記録して、管理者に提示するサービスがある。	業務にあわせて導入を検討する。	cyzen/ レッドフォックス(株)
				MITERAS/ パーソルプロセス＆テクノロジー(株)
				F-chair+ /(株)テレワークマネジメント
				CYBER XEED就業等の勤務時間管理ソフト
				グループウェア等に付属する打刻ソフト
2	在席管理(プレゼンス管理)ツール	プレゼンスソフトは、各ワーカーが在席中か否か、話しかけて良い状態か等をリアルタイムで表示する。	業務にあわせて導入を検討する。	Sococo Virtual Office/ (株)イグアス
				Remotty/ (株) Sonic Garden
				Teams(Microsoft365)/日本マイクロソフト(株)
				グループウェア等による在席管理
3	業務管理(プロジェクト管理)ツール	テレワーク実施にあたっての基本的な機能としてスケジュールを共有できるツールを導入することが望ましい。 さらに、研究・開発・企画等のプロジェクト単位で動いている業務でテレワークを実施する場合には、プロジェクト管理・タスク管理まで行えるツールの導入も検討する。	形態にかかわらず、スケジュールを共有できるツールを導入検討する。 さらに、「研究・開発・デザイン職」では、プロジェクト管理ツールの導入を検討する。	サイボウズ/サイボウズ(株)
				desknet's NEO/(株)ネオジャパン
				NI collabo 360/ (株)ＮＩコンサルティング
				Microsoft365/日本マイクロソフト(株)
				G Suite/グーグル合同会社

出典：日本テレワーク協会
テレワーク関連ツール一覧（第5.0版）

03

弊社事例

ネットワンシステムズの働き方改革

ICTツールの普段使いが大切

災害時やパンデミック時に突然在宅勤務によるテレワークを実施しようとしても難しい。
いざという時のために、普段から**テレワークに慣れておく**ことがとても重要！

ネットワンで利用しているツール

社内利用	テレワーク時利用
デスクトップPC	BYOD（私物端末の業務利用）
通信環境（社内無線LAN）	会社支給 スマホテザリング／モバイルルーター
仮想デスクトップ（VDI）	仮想デスクトップ（VDI）
勤怠管理（社員証カード方式）	勤怠管理システム入力→Web打刻
紙業務	電子印鑑／ ワークフロー（ERP）システム
社内ファイルサーバ	クラウド型ファイルサーバ
メール・スケジュール	クラウド型グループウエア
会議室／対面でのコミュニケーション	Web会議／チャット
電話／FAX	会社支給 携帯電話/FAX転送






新たなコミュニケーションツールへのトライアル

バーチャルオフィスツールを活用して、
コミュニケーション不足を解消！

チャットやWeb会議で埋められなかった挨拶、雑談やちょっとした相談、声かけなどカジュアルなコミュニケーションを実現できる。

離れた場所で働く人々が、**チームワークを発揮**し、より生産性の高い仕事をするためには、**「心理的安全性」が不可欠**。

画像提供： RISA（株）OPSION

オンライン上で仮想のオフィスを作り出し、
まるで実際のオフィスで働いているかの
ような距離感でチームメンバーと気軽に
コミュニケーションする

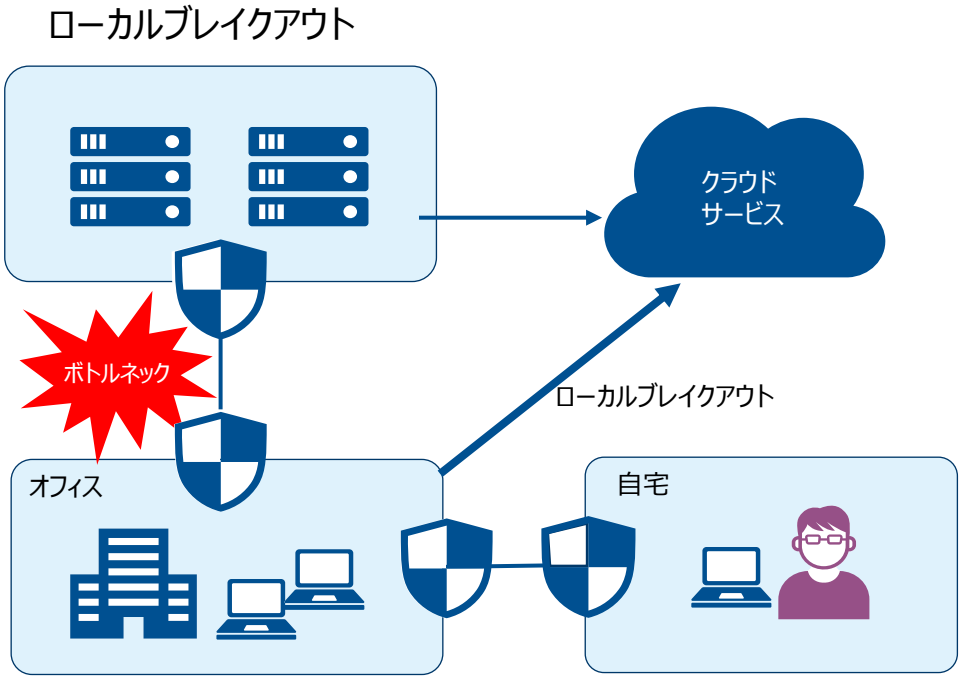
04 今後考慮すべきポイント

テレワークの新たな課題

① ローカルブレイクアウトの導入

② クラウドサービスの利用拡大

③ BYOD（私物端末の業務利用）の普及



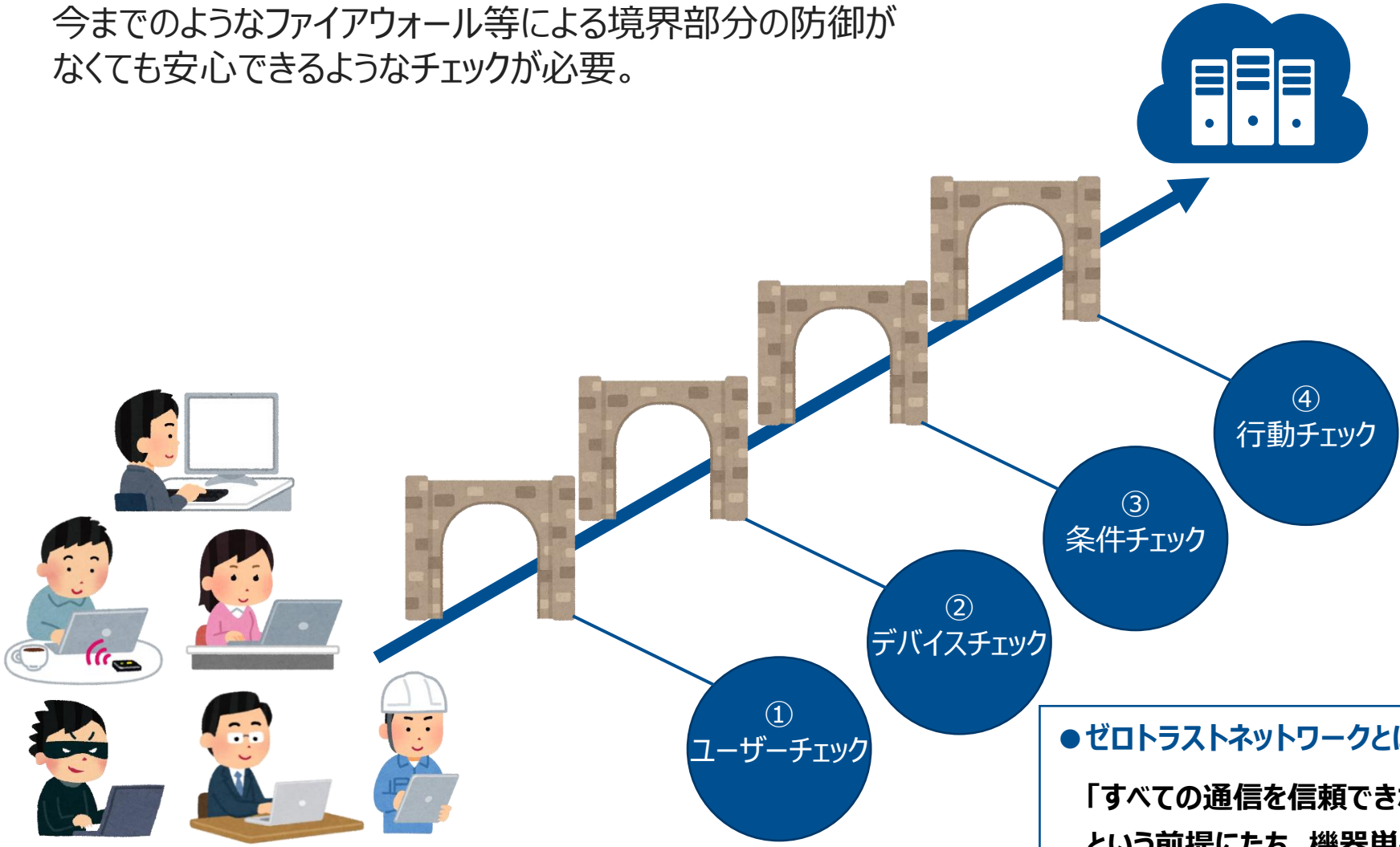
●ローカルブレイクアウトとは

テレワーク端末からWebページ閲覧等をする場合に、オフィスやデータセンター等の拠点を介することなく、テレワーク端末から直接インターネットサービスへアクセスするネットワーク構成。

特定の拠点を防御する境界型セキュリティだけでは対応が難しい

新しいセキュリティモデルとしてのゼロトラスト

今までのようなファイアウォール等による境界部分の防御が
なくても安心できるようなチェックが必要。



●ゼロトラストネットワークとは

「すべての通信を信頼できないもの」
という前提にたち、機器単位での
セキュリティ強化をうたった考え方。

まとめ

様々な課題への対応は自社では困難
（人材育成＆不足、運用管理負荷、セキュリティ対策・・）

運用を含めた総合サービスの利用やアウトソーシングも考慮

そのため
①情報の棚卸
②情報の可視化
③テレワークでどのような情報が流れているかの把握と整理

テレワーク対応を機会にICTセキュリテイ環境の見直しが必要

05

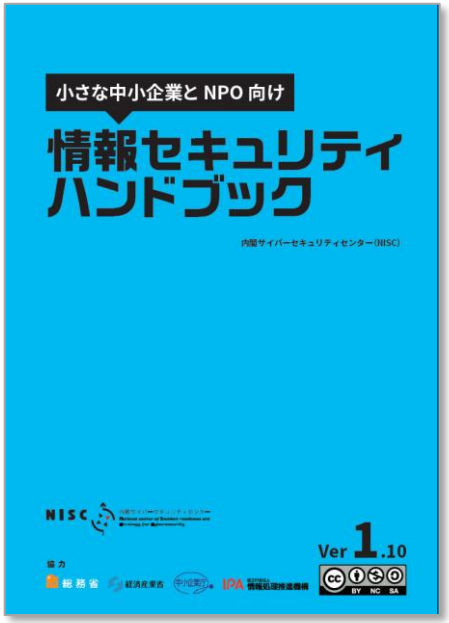
参考資料

セキュリティガイドライン関連情報

出典：総務省「テレワークセキュリティガイドライン」

出典：総務省「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」

出典：IPA「中小企業の情報セキュリティ対策ガイドライン」



出典：内閣サイバーセキュリティセンター（NISC）「情報セキュリティハンドブック」

テレワークセキュリティガイドラインの改定

- 総務省では従来から「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示してきた。
  → テレワークを取り巻く環境やセキュリティ動向の変化に対応するため**2021年５月**に**全面的に改定**
- ガイドラインを補完するものとして、セキュリティの専任担当がいないような中小企業等においても、テレワークを実施する際に**最低限のセキュリティ**を**確実に確保**してもらうための**チェックリスト**についても策定。

公表URL https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

テレワークセキュリティガイドライン

（2021年５月　第５版）

2004年12月初版
2006年４月第２版
2013年３月第３版
2018年４月第４版

- ✓ テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針
- ✓ 中小企業を含む全企業を対象
- ✓ システム管理者のほか経営層や利用者(勤務者)を幅広く対象

ガイドラインに記載の内容について、理解や検討が難しい場合

中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)

（2021年５月　第２版）2020年９月初版

中小企業等に向け**最低限のセキュリティを確実に確保**してもらうためのものに限定

【想定読者像】
- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本IT用語は聞いたことがあるレベル
- ✓ 設定作業は検索しながら実施可能

テレワークで活用される代表的なソフトについて、**設定解説資料**を作成し、具体的な設定を解説

【設定解説資料の対象】
CiscoWebexMeetings ／ Microsoft Teams／Zoom／Windows／Mac／iOS ／ Android ／ LanScope An ／ Exchange Online ／ Gmail ／ Teams_chat ／ LINE ／ OneDrive ／ Googleドライブ／Dropbox／YAMAHA VPNルータ／CiscoASA／Windowsリモートデスクトップ接続／Chromeリモートデスクトップ／Microsoft Defender／ウイルスバスター ビジネスセキュリティサービス

テレワークセキュリティガイドラインの改定（2021年５月）

【テレワーク環境・セキュリティ動向の変化】

- ✓ テレワークは「一部の従業員」が利用するものから、Web会議を含め、一般的な業務・勤務形態に
- ✓ クラウドサービスの普及やスマートフォン等の活用が進むなど、システム構成や利用形態が多様化
- ✓ 標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況も発生

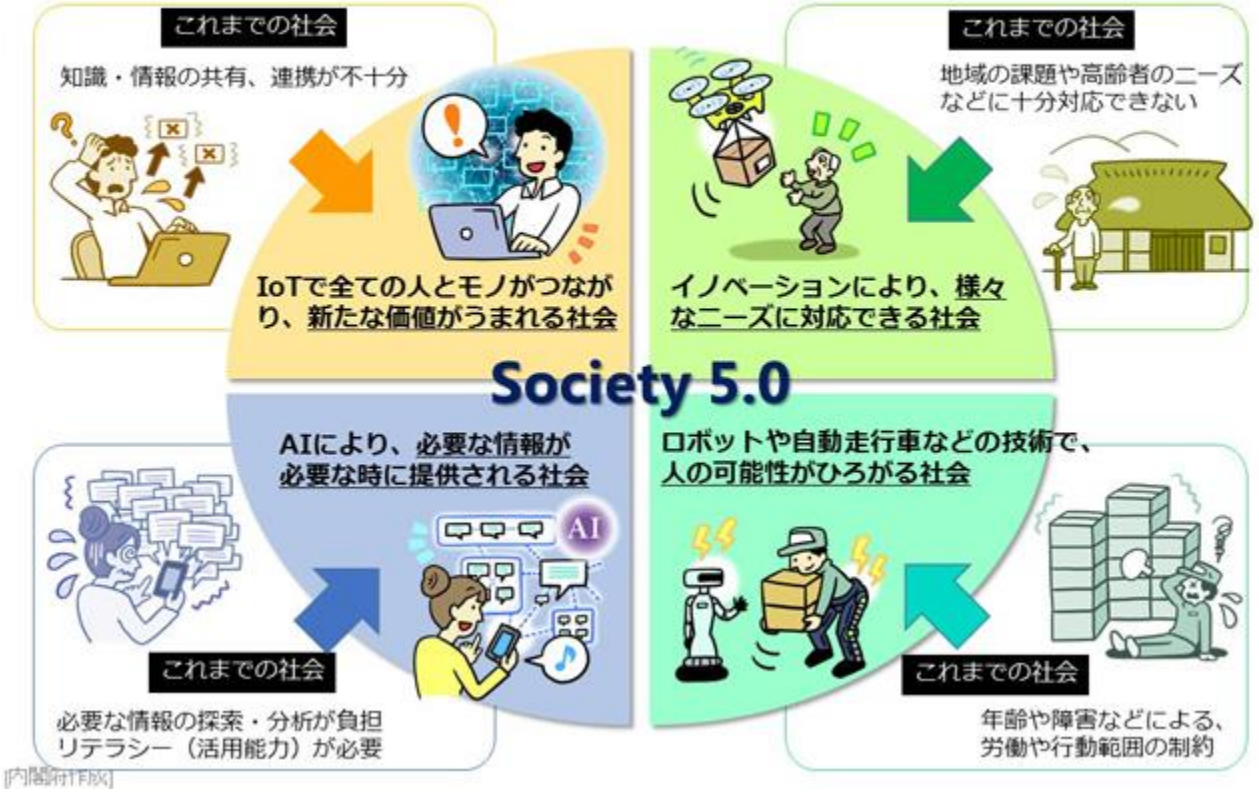
【ガイドライン改定の主要なポイント】

- ✓ テレワーク方式を再整理し、適した方式を選定するフローチャートや特性比較を掲載
- ✓ クラウドやゼロトラスト等のセキュリティ上のトピックについても記載
- ✓ 経営者・システム管理者・勤務者の立場それぞれにおける役割を明確化
- ✓ 実施すべきセキュリティ対策の分類や内容を全面的に見直し
- ✓ テレワークセキュリティに関連するトラブルについて、具体的事例を含め全面見直し（事例紹介のほか、セキュリティ上留意すべき点や、採るべき対策についても明示）

出典：総務省「テレワークセキュリティガイドライン」

Society 5.0 ビッグデータ連携がもたらす未来社会像

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）



出典：内閣府HP

ご清聴
ありがとうございました

つなぐ ∠ むすぶ ∠ かわる

net one