Tokyo Financial Information & Technology Summit

FINOLAB

Remote Working and Implication on Operating Models and Risk

在宅勤務と、オペレーティングモデルおよびリスクへの影響

2022-06-29

＜コロナ禍におけるオペレーションの変化＞

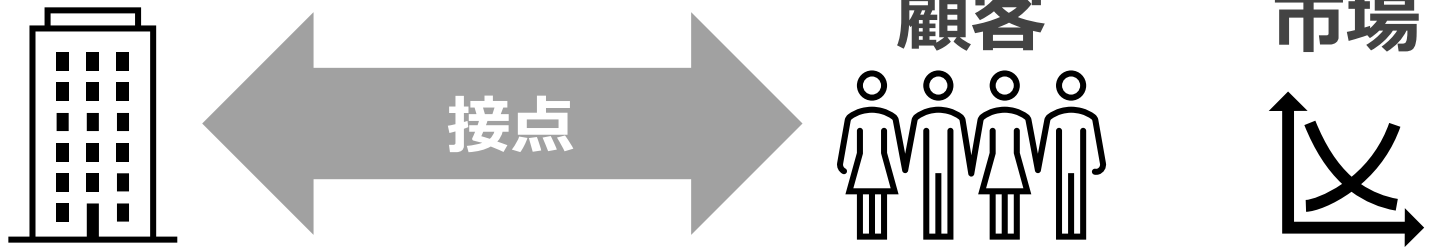
新型コロナウィルス感染拡大にともなう移動制限、自宅勤務に伴い、勤務や生活スタイルに大きな変化がもたらされ、金融機関におけるオペレーションについても見直しが迫られている

リモートワークへの切替
個別組織の都合とは関係なく、リモートワークの導入による出勤の制限が金融機関にも要請されるようになり、短期間での対応が迫られるようになった

感染者やクラスター発生への備え
出勤者から感染者が単独もしくは複数発生した場合に、業務継続が可能となるように出勤とリモート勤務のシフトを組んだ上で、効率的なオペレーションを実現することが必要となった

オペレーション連携の必要性増大
これまで、フロントオフィスのデジタル化が進んでいても、ミドルやバックオフィスでの手作業が多いというケースは多かったが、コロナを契機としてあらゆるレベルでのデジタル化の必要性が認識されるようになった

＜オペレーション対応とデジタル化の推進＞



フロントオフィス
- 営業
- 顧客サポート
- トレーディング

ミドルオフィス
- リスクマネジメント
- 営業サポート
- プロジェクト管理

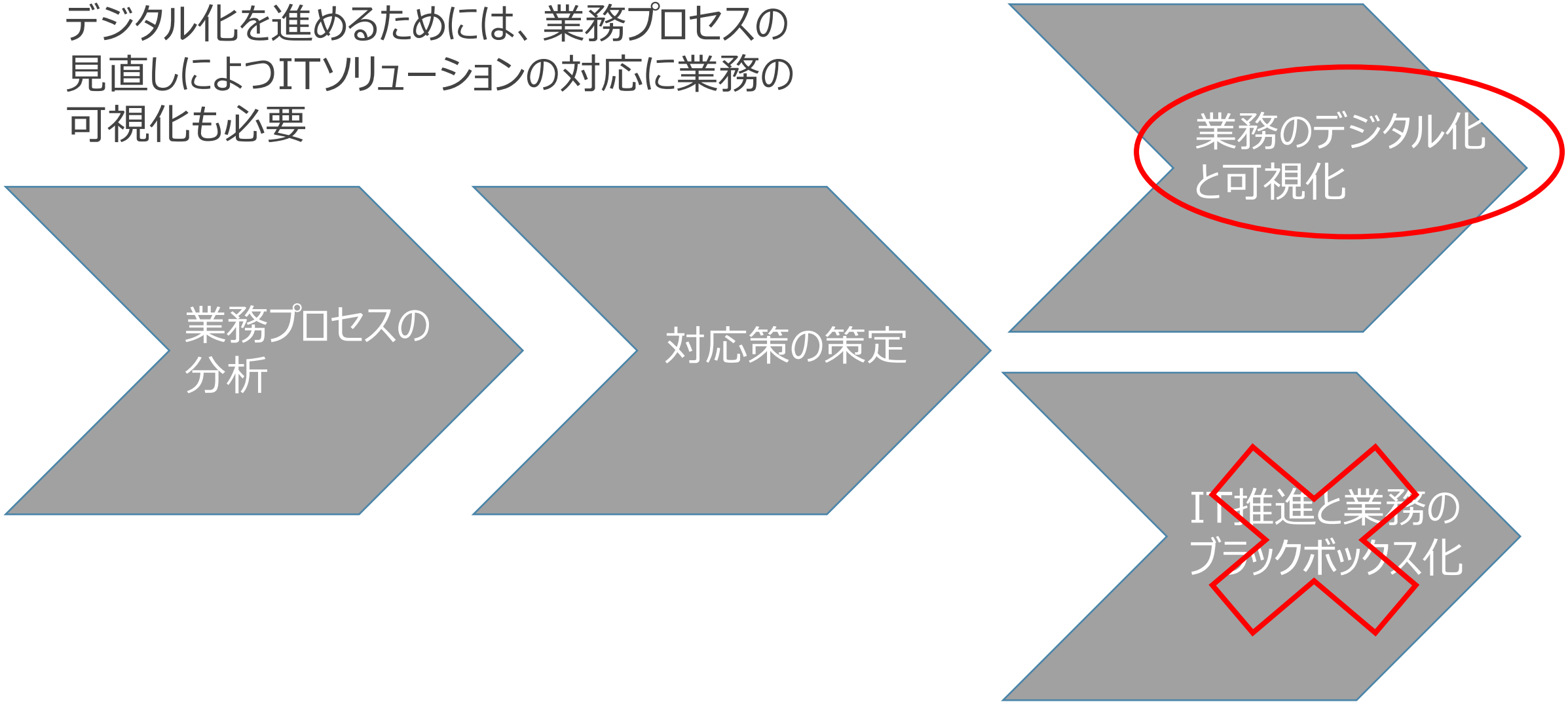
バックオフィス
- 取引執行
- 記帳事務
- 契約管理

プロントオフィスのデジタル化は進んでいるが、オフィスと同じレベルのモニタリングをリモートワークで行うことは容易でない

多くの金融機関においてミドル・フロントオフィスにおけるオペレーションはまだ紙ベースの作業や押印が必要なプロセスが多く、リモートワークに対応するために、デジタル化の必要性が増大

＜デジタル化とプロセス見直し＞

デジタル化を進めるためには、業務プロセスの見直しによつITソリューションの対応に業務の可視化も必要



＜DX推進の注意点＞

「DX推進のためにオペレーション再編が必要」という論が多く聞かれるが、短期での実現は難しい

人員削減の難しさ

例えば、従来人間が１分かかる作業480件／日をRPA等で代替すると業務量1人分になるが、それを8人で分担していたとすると、実際にはそれぞれの作業が1時間／日減ることにはなるが、人員を1人も削減できないように、業務量削減は自動的に人員削減につながる訳ではない

万能ではないデジタル化

RPAやAIなどのデジタル化はどんな業務でも代行してくれる訳ではなく、適切な適用領域選択、既存システムとの適切な連携、既存プロセスの見直し、等の条件が整わないと効率化につながらずに、失敗に終わるプロジェクトの例も出るようになっている

ネガティブイメージによる従業員の抵抗心理

デジタル化の進展は人間の仕事を奪うのではないかと危惧されているが、多くのリストラが発表されていることもあり、現場の懸念は大きい。人員再配置や従業員の再教育を進めていくことが提唱されているが、まだ具体的な方法論や成果を示すことができている事例は限定的

＜コロナ禍におけるサイバーリスクの顕在化＞

新型コロナウィルス感染拡大によって、オペレーションの変化とともに、新たなサイバーセキュリティリスクも顕在化する結果となっている

リモートワークの環境
多くの企業がリモートワークに移行しているが、自宅のネットワーク環境が脆弱なために、サイバー犯罪者のターゲットとなるケースが目立っている

企業内個人の脆弱性
出社する機会が減り、コミュニケーションギャップが生じている企業内の従業員を、個別ターゲットとした不正事案も増えている

自宅でのネット購買拡大
外出できないことによってインターネット購買（e-commerce）が拡大することによって、新たな不正事案も増加している

FINOLAB RESEARCH

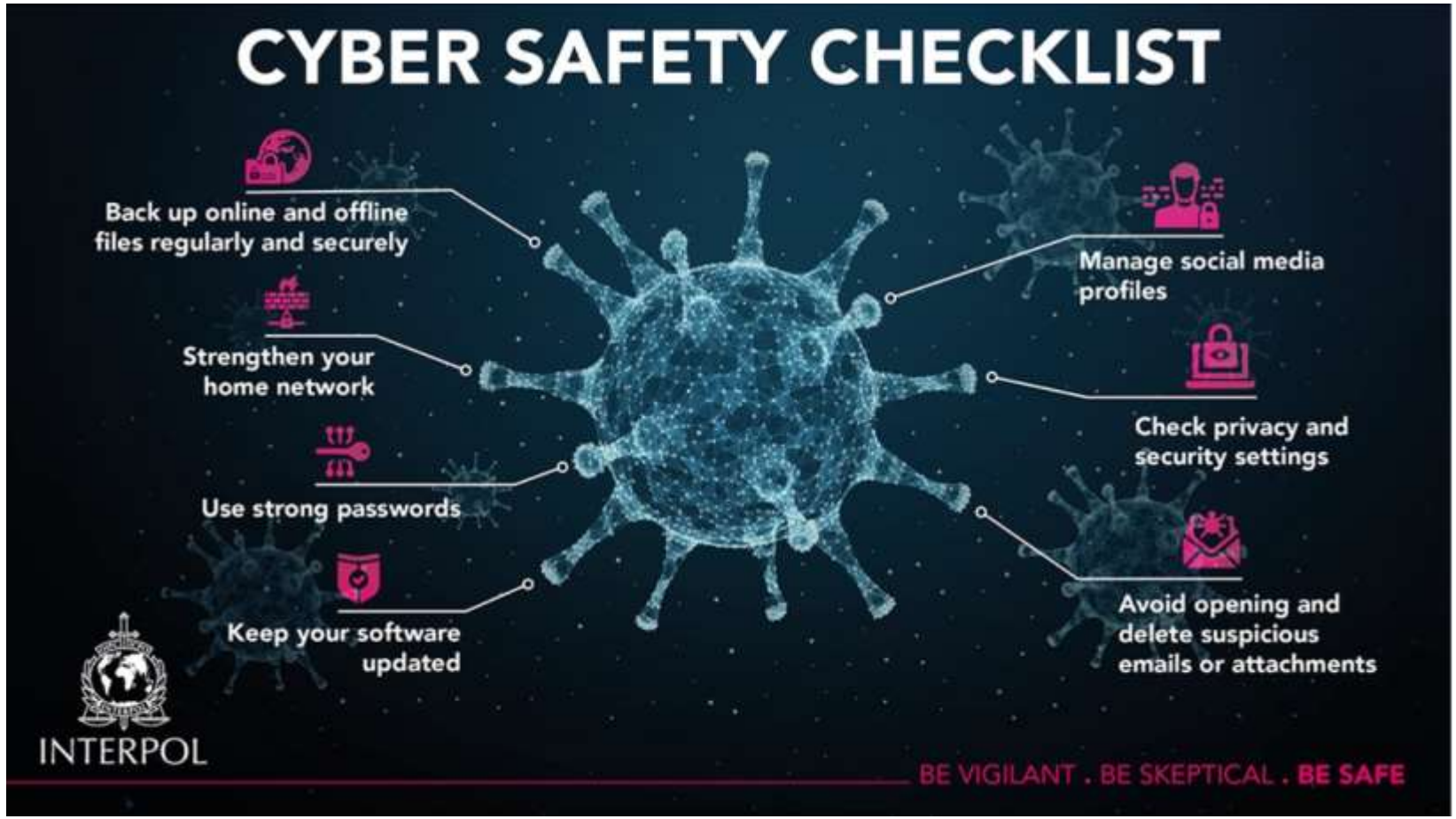
国際警察刑事機構（Interpol）の警告

- **不正事例の増加**
  経済状況悪化・ビジネス環境変化により、犯罪に手を染める人も増える可能性が高い
- **進む不正インフラ整備**
  犯罪をサポートする地下インフラ（Cybercrime-as-a-service)の整備が進んでおり、サイバー犯罪への参入が容易となりつつある
- **メインターゲットとなる個人情報・機密情報**
  アドレス偽装やネットサービス事業者からの漏洩による個人情報や機密情報の不正取得によって犯罪者のマネタイズ手段も多様化
- **オンラインコミュニケーションへの依存**
  リモートワークへのシフトは今後も継続が予想され、政府・企業・学校とあらゆる組織がオンラインコミュニケーションに依存することになり、サイバー犯罪者のつけいる余地も拡大

出典：Interpol “Global landscape on COVID-19 cyberthreat”

FINOLAB RESEARCH

＜サイバー犯罪対策のチェックリスト＞



オンラインセキュリティIのチェックリスト（Interpol作成）

- ✓ ファイルのバックアップ
- ✓ 家庭のネットワークの強化
- ✓ 「強いパスワード」の設定
- ✓ ソフトウェアの最新アップデート
- ✓ SNSのプロファイル管理
- ✓ プライバシー設定とセキュリティ設定の確認
- ✓ 怪しいメールや添付ファイルを開封せずに削除

https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

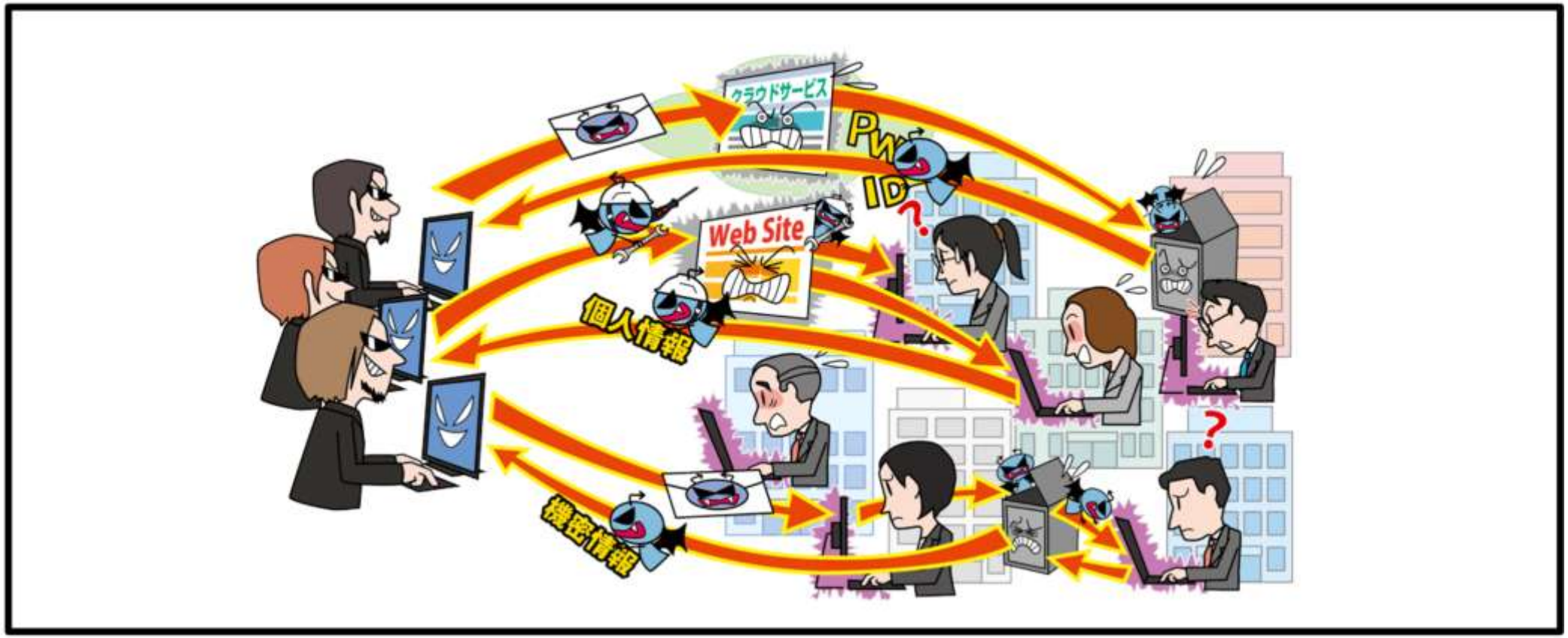
＜具体例１：ランサムウェアの被害＞

メール経由・ウェブサイト経由の場合があるが、PC等に保存されているファイルを暗号化され使用不可になり、復旧と引き換えに金銭を要求される。または、情報を窃取しそれを公開すると脅迫するケースも出現している。

IPA:　情報セキュリティ10大脅威 2022 [組織編]より

＜具体例２：標的型攻撃による機密情報の窃取＞

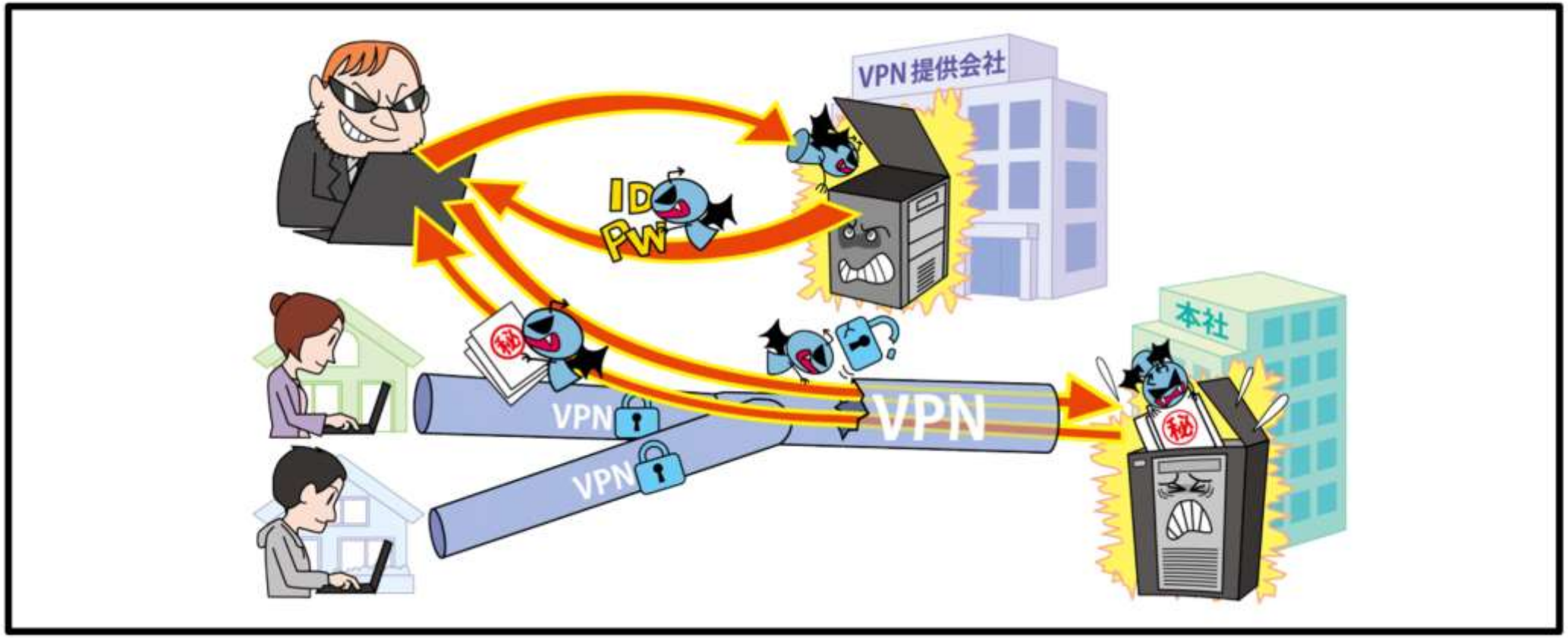
メール等を利用し特定組織のPCをウイルスに感染させるケースが多いが、組織内部に潜入し長期にわたって侵害範囲を徐々に広げていくこともある。組織の機密情報窃取やシステムの破壊といった被害が発生している。



IPA:　情報セキュリティ10大脅威 2022 [組織編]より

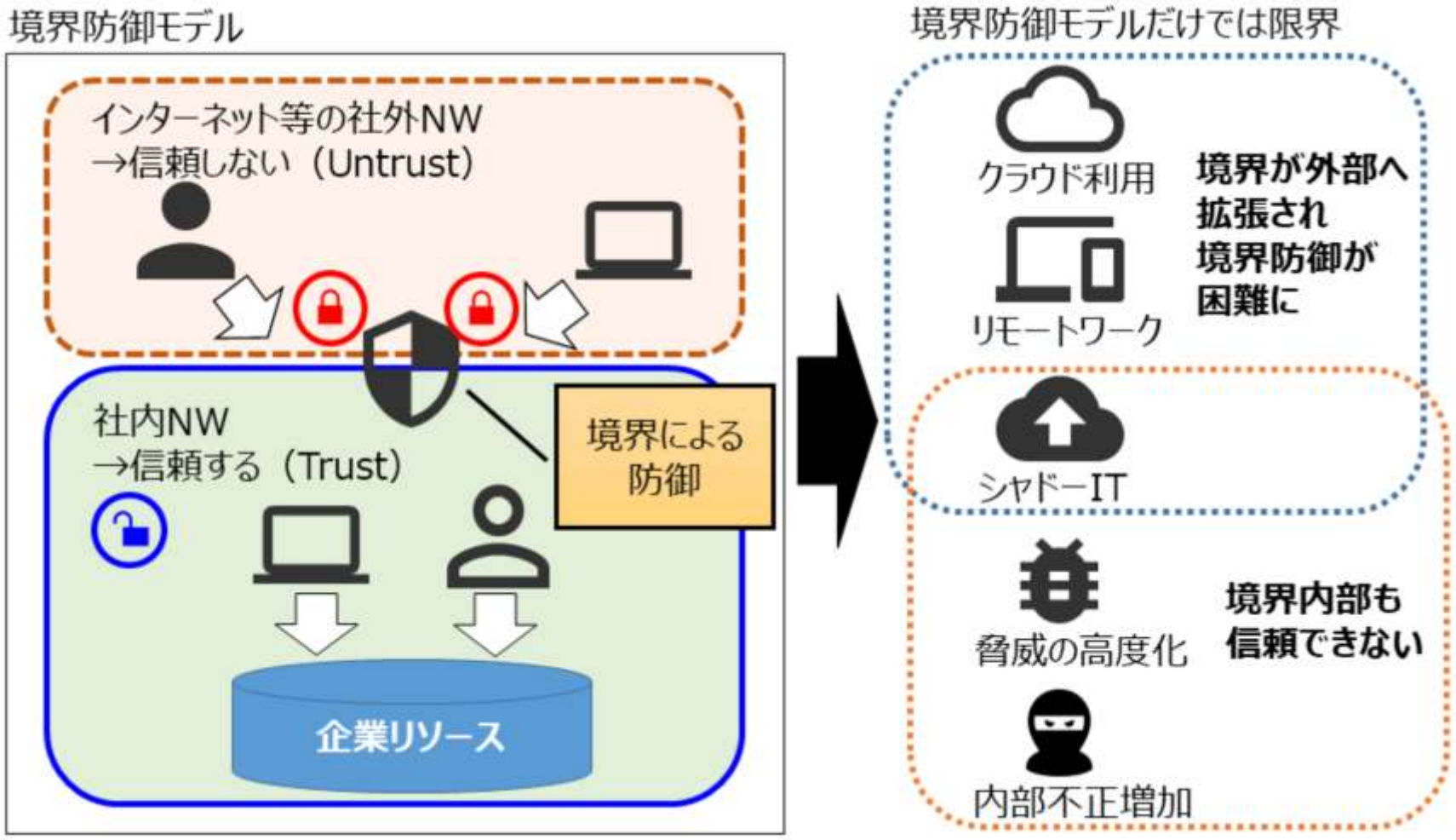
＜具体例３：新しい働き方を狙った攻撃＞

リモートワーク用ソフトウェアの脆弱性を悪用した不正アクセス、リモートワーク移行による管理体制の不備、私物PCや自宅ネットワークを狙った攻撃など、ウェブ会議ののぞき見やリモート用PCのウイルス感染といった被害が発生している。



IPA:　情報セキュリティ10大脅威 2022 [組織編]より

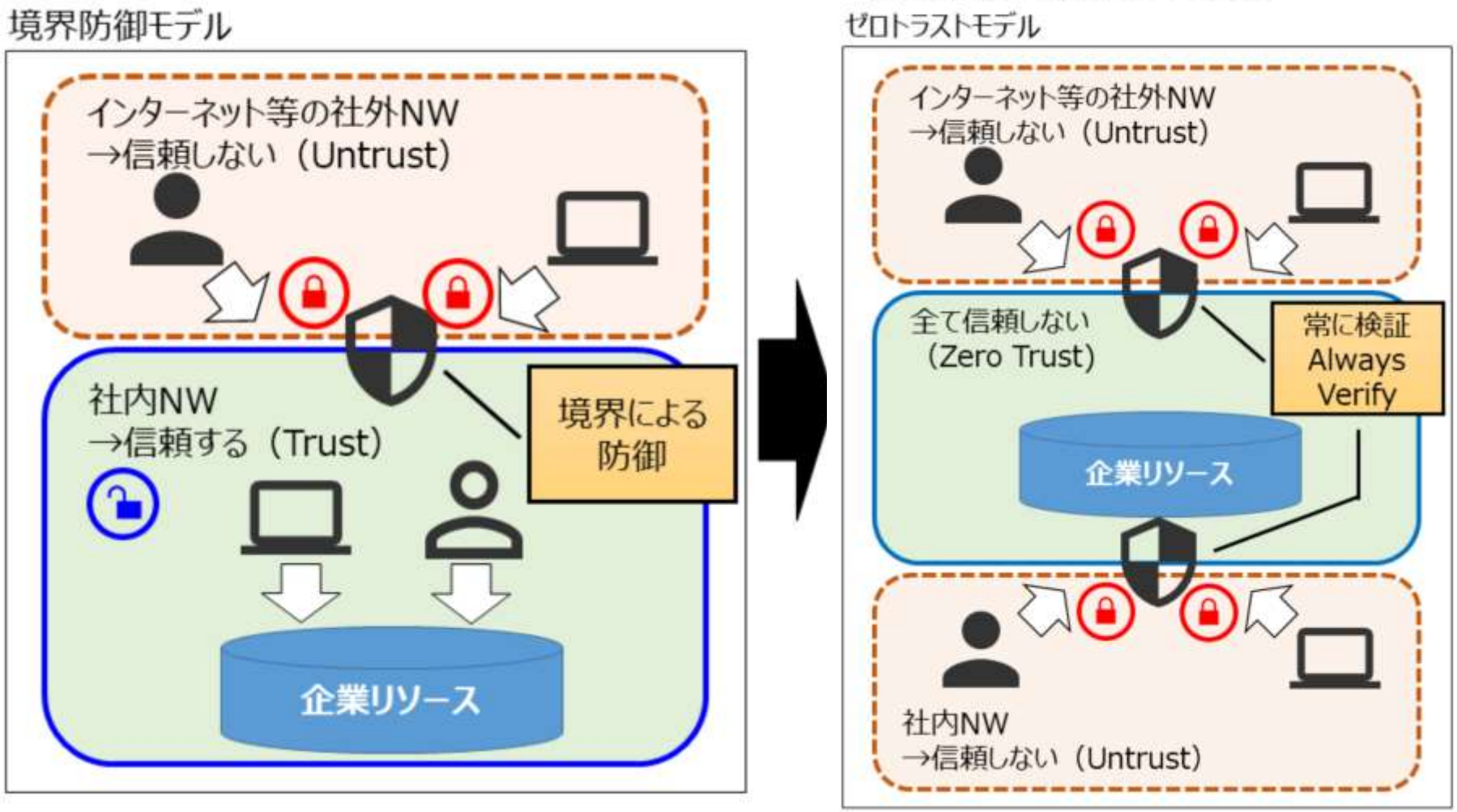
＜セキュリティ対策の限界＞



従来の考え方の限界
デジタル化の進展、不正事案の拡大、モバイル端末の普及などにより、企業のシステムやデータなどのIT資産の保護に焦点を当てた考え方において、ネットワークの境界を防御する従来のセキュリティ対策の限界が指摘されるようになった。

https://www.intellilink.co.jp/column/security/2020/052000.aspx

＜新しいセキュリティモデルの提唱＞



ゼロトラストの提唱：
境界線内は安全という考え方を捨て、境界を設けない考え方を進化させた「ゼロトラスト」というコンセプトが提唱されるようになった。つまり、「企業のネットワークやデバイスからのアクセスを暗黙に信頼せず、従業員の端末通信や情報資産へのアクセスなどについて、常にアクセスの信頼性を検証する」ことが基本となる。

https://www.intellilink.co.jp/column/security/2020/052000.aspx

<ゼロトラストの原則>

FINOLAB RESEARCH

基本概念：
アーキテクチャは多様な実現方法があり、用語や概念が統一されていない状況が続いていたため、米国国立標準技術研究所（NIST）が2020年8月に「**Zero Trust Architecture（NIST SP800-207）**」を発行したことによって、用語と概念の共通基盤が形成されている。

「NIST　SP800-207」で整理されている原則：

1. すべてのデータソースとコンピューティングサービスをリソースとみなす
2. ネットワークの場所に関係なく、すべての通信を保護する
3. 企業リソースへのアクセスは、セッション単位で付与する
4. リソースへのアクセスは、クライアントアイデンティティ、アプリケーション/サービス、リクエストする資産の状態、その他の行動属性や環境属性を含めた動的ポリシーにより決定する
5. すべての資産の整合性とセキュリティ動作を監視し、測定する
6. すべてのリソースの認証と認可を動的に行い、アクセスが許可される前に厳格に実施する
7. 資産、ネットワークインフラストラクチャ、通信の現状について可能な限り多くの情報を収集し、セキュリティ態勢の改善に利用する

https://csrc.nist.gov/publications/detail/sp/800-207/final

＜ゼロトラストの現状＞

令和3年6月30日
金融庁

「ゼロトラストの現状調査と事例分析に関する調査報告書」の公表について

＜本調査からの抜粋＞
本調査では、金融機関におけるゼロトラストに関する検討状況や導入状況を、文献調査やヒアリング 調査の手法を用いて行ったものの、結果として、ゼロトラスト・アーキテクチャの導入あるいは積極採用に 向けた取り組みを進めている金融機関はまだ少数であった。
しかしながら、一部の金融機関では、リモートワーク拡大のためや IT システムのクラウド化を進めるた めにゼロトラストという考え方を踏まえた検討や導入を進めていることが確認された。
また、ゼロトラスト・アーキテクチャについて調査や検討は行ったものの、様々な理由から現時点では ゼロトラスト・アーキテクチャは導入しないとしている金融機関も確認された。

https://www.fsa.go.jp/common/about/research/20210630.html

まとめ

- コロナ禍において業務を継続させるため、各オペレーションレベルで課題が浮き彫りになり、デジタル化の推進が必要となるケースが多かった
- デジタル化の効果をあげるためには、業務プロセスの見直しを含めた最適化を中長期的に進める必要がある
- また、セキュリティリスク増大によって、従来モデルの限界がみえてきており、ネットワークの内外にかかわらず、従業員の端末や情報資産へのアクセスについても常に監視することでセキュリティを確保する「ゼロトラスト」モデルが提唱されるようになっている
- ゼロトラスト導入はまだ限定的であるが、まず基本的な考え方を理解した上で、汎用的な取組みにしていくことが必要

Tokyo Financial Information & Technology Summit

FINOLAB

Thank you

FINOLAB RESEARCH