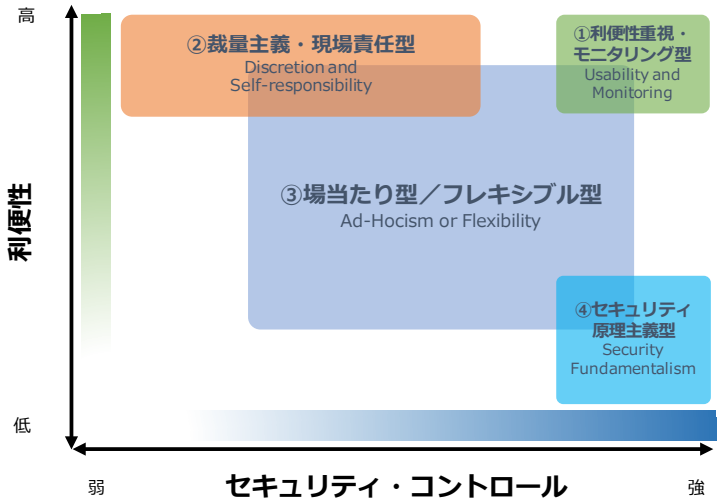
2021 年 2 月

2025 年に向けた利便性とセキュリティのリバランス

【要旨】

- 新型コロナウイルス感染症の拡大により、多くの企業や組織では、**テレワークを想定していなかった部署にも在宅勤務を推し進めたことで、利便性とセキュリティリスクのバランスが崩れた**。
- 来たるべき非接触型社会に向けて企業の持続的成長や柔軟な働き方を推進するためには、現状の利便性とセキュリティのバランスを見直す必要がある（以下、「リバランス」という）。**このリバランスを実現しなければ、生産性低下やリスク顕在化などビジネスに多大な影響を与える恐れがある**。
- 手の届く未来といえる 2025 年は、IT システム「2025 年の崖 [1]」や Windows10 Pro サポート終了など、技術的に大きなチャレンジを迎える時である。加えて、2025 年以降はデジタルとセキュリティの理解がなければ経営者にふさわしくないとステークホルダーから言われる時代となり、経営者にも「プラス・セキュリティ人材」が求められるであろう。そうであれば、**利便性とセキュリティのリバランスを早急に着手しなければ手遅れになる** [2]。
- JCIC が各企業の動向についてインタビューや文献調査を実施したところ、各社で利便性とセキュリティ・コントロールの考え方に大きな違いがあることがわかった。各社のデジタル化の理念や哲学を分析すると、**4 つのタイプ（利便性とセキュリティのバランスモデル）に分類できる**（図表 1）。なお、本バランスモデルのタイプを企業の事業部や部門単位で変えることもできる。



図表 1 利便性とセキュリティのバランスモデル

- セキュリティ責任者などが「利便性とセキュリティのバランスモデル」を用いて自社の現状を把握し、今後の経営戦略と整合性を取ることで、中長期的に目指すタイプを社内合意しやすくなるはずだ。その結果、**テレワーク環境下であっても、「生産性向上」や「顧客満足度向上」などの目的を達成することができる**。ぜひ、本レポートを将来に向けたワークスタイル変革、デジタル・トランスフォーメーション（DX）、セキュリティ管理などの戦略策定のヒントとして役立てていただきたい。

[1] 経済産業省の「DX レポート」では、2025 年までに既存システムの複雑化・老朽化・ブラックボックス化を放置すると、DX の足かせとなり経済損失が拡大するだけでなく、データ流出などのリスクが高まるとした。2025 年の崖を克服するためには、システム刷新を集中的に推進する必要があるという。

[2] JCIC「サイバーセキュリティ情報公開のポイント」、「セキュリティ人材不足の真実と今なすべき対策とは」、「DX 化を実現し、企業が生き残るためには　～キーは「攻めのプラス・セキュリティ人材」育成～」より

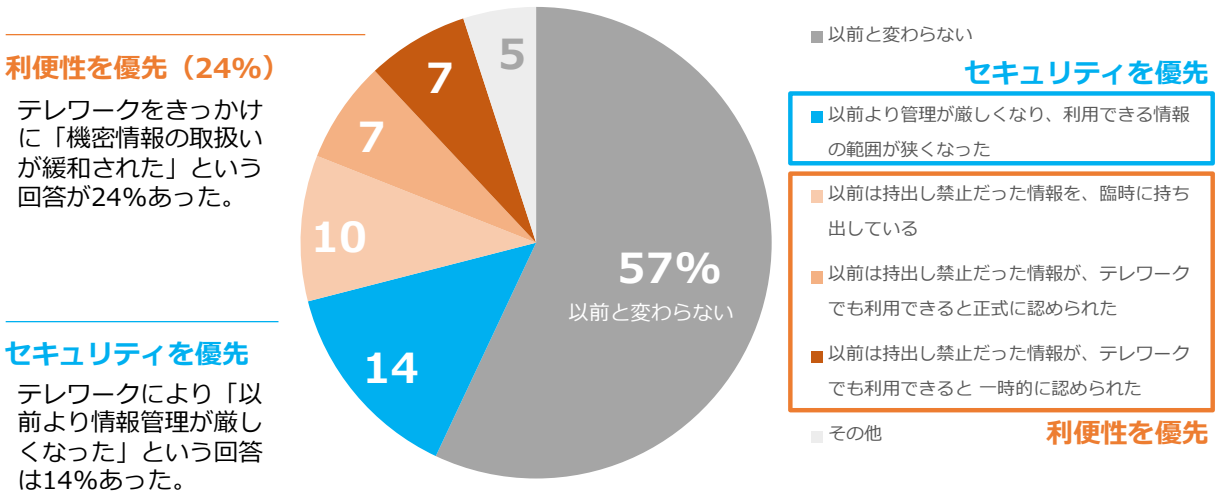
1. はじめに

新型コロナウイルス感染症の拡大により、多くの企業や組織では、テレワークを想定していなかった業務部門や派遣社員にも在宅勤務を推し進めたことで、利便性とセキュリティリスクのバランスが崩れた。急速なテレワーク推進において、利便性を優先した企業は、サイバー攻撃や内部犯行のリスクが高まっている。一方、セキュリティを強固にしすぎた企業は、業務上やむを得ず自宅 PC で作業したり、未許可のクラウドサービスを勝手に利用したりするなど、IT システムの裏口利用の常態化が懸念される。このまま利便性とセキュリティのバランス崩壊を見過ごしていては、情報漏えい、若しくはビジネス停滞のいずれかのシナリオで、数年後にビジネスに多大な影響が発生するであろう。本レポートは、アフターコロナの時代を見据え、利便性とセキュリティリスクのバランスを見直すための考え方を整理したものである。

本レポートの対象読者は、主にセキュリティ責任者（CISO、部門長など）を想定しているが、取締役/監査役/経営層/経営企画/リスク管理/情報システム/人事/総務/財務などのマネジメント層も読んでいただきたい内容になっている。ぜひ、このレポートを将来に向けたワークスタイル変革、デジタル・トランスフォーメーション（DX）、セキュリティ管理などの戦略策定のヒントとして役立てていただきたい。

2. 利便性とセキュリティのバランス崩壊により、ビジネスに多大な影響が発生する

日本スマートフォンセキュリティ協会（JSSEC）が行ったアンケート[3]によると、「今回の新型コロナウイルス感染防止のためのテレワーク推進をきっかけに、テレワークで利用できる機密情報の扱い方に変化はあったか」という質問に対して、「以前と変わらない」が半数を超える結果となったが（図表 2 の灰色）、今回をきっかけに「以前より情報管理が厳しくなった」という回答は 14%であった（水色）。一方、「機密情報の取扱いが緩和された」という回答が 24%あった（橙色）。つまり、テレワークを想定していなかった業務部門や派遣社員も在宅勤務を推し進めたことで、一部の企業ではセキュリティを優先したり、利便性を優先したりしたことがわかる。

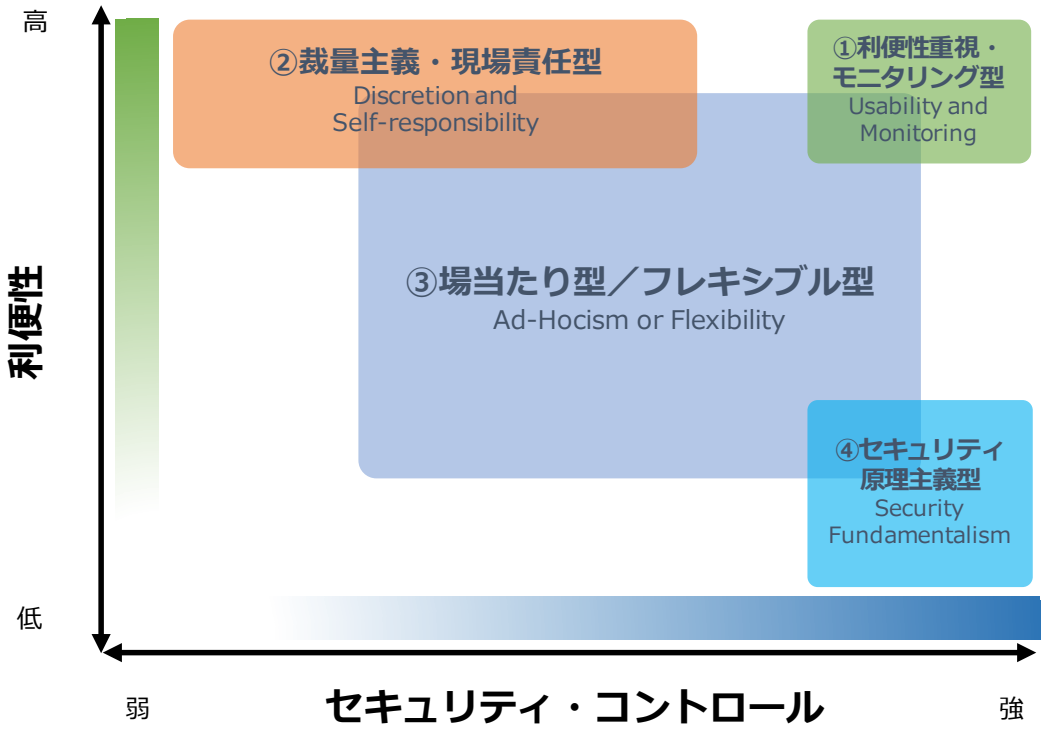


図表 2 テレワークでの機密情報の扱い方の変化

[3] 一般社団法人日本スマートフォンセキュリティ協会（JSSEC） 「テレワーク状況とセキュリティに関するアンケート調査レポート（n=432 人）」（2020 年 7 月）, https://www.jssec.org/report/20200722.html

3. 利便性とセキュリティのバランスモデル

企業はどのように利便性とセキュリティのバランスを検討すべきだろうか。この答えを導き出すために、JCIC が企業インタビューや文献リサーチなどを行ったところ、各社で利便性とセキュリティ・コントロールの考え方に大きな違いがあることがわかった。各社のデジタル化の理念や哲学を分析し、整理したところ、４つのタイプに分けることができた。これを「利便性とセキュリティのバランスモデル」と呼ぶ。なお、本バランスモデルのタイプを企業の事業部や部門単位で変えることもできる。



図表 1 利便性とセキュリティのバランスモデル（再掲）

図表 1 の横軸は「セキュリティ・コントロール」であり、右に行けば行くほど、強いセキュリティ管理を志向することを意味する。また、縦軸は「利便性」であり、上へ行けば行くほど、従業員の高い利便性を志向することを意味する。例えば、②裁量主義・現場責任型は、高い利便性を志向し、セキュリティ管理は強くしすぎない傾向の企業を指す。また、④セキュリティ原理主義型は、強いセキュリティ管理を志向し、利便性の低さはある程度許容する企業を指す。

また、①～④の四角の大きさは、それぞれのタイプが志向する利便性とセキュリティ・コントロールの許容範囲を図示している。タイプが重なり合う部分は、それぞれのタイプの中位を意味し、この位置にある企業も存在する。空白部分は、ここに該当する企業はほとんど存在しないことを意味する。

ここで、４ つのタイプの特徴と留意事項を整理する（図表 3）。どのタイプにも一長一短があり、正解はない。ただし、重要なことは、なぜそのタイプを選んだのかを説明できることである。経営者と現場のセキュリティ責任者が、今後の経営戦略に沿ったワークスタイルやセキュリティ管理を考え抜いた末に導き出した方向性でなければならない。他社の動向を見ながら時流に流されるのではなく、自らの意思で中長期的な方針を策定していかなければ、生産性低下やリスク顕在化、更には優秀な人材の流出など、ビジネスに多大な影響を与える恐れがあることを認識する必要がある。

	特徴	留意事項
①利便性重視・モニタリング型 Usability and Monitoring	• 従業員が快適で自由な働き方ができるが行動は監視されている • ネット企業・IT企業が該当	• 常に最新動向に対応し続ける必要があるため、多くのリソース（人・金）が必要
②裁量主義・現場責任型 Discretion and Self-responsibility	• 企業が最低限のベースは決めるが、従業員の自由度は高い • クリエイティブな社風で採用	• サイバー攻撃のリスク高 • 内部犯行リスク高
③場当たり型／フレキシブル型 Ad-Hocism or Flexibility	• セキュリティポリシーの例外対応を柔軟にできる • 多くの企業が該当	• 例外判定の意思決定が遅い • 方針の一貫性がなくなる
④セキュリティ原理主義型 Security Fundamentalism	• 外部とは閉ざされたIT環境で、従来通りの業務を遂行できる • 重要インフラ・規制業界に多い	• DXや働き方改革が進めにくい • 感染症などの危機発生時に対応しづらい

図表 3 バランスモデルの特徴と留意事項

① 「利便性重視・モニタリング型」は、利便性とセキュリティ管理を高い次元で実現しようとする企業である。IT 企業などが該当し、従業員がいつでも・どこでも・どの端末でも、快適で自由な働き方ができる一方で、常に行動は企業にモニタリングされている。このタイプは、企業は常に技術やトレンド変化などの最新動向に対応し続ける必要があり、非常に多くのリソース（人・金）が必要となる。また、途中で方針変更することは利便性とセキュリティ管理のどちらかを緩めることになるため、企業が一度このタイプを目指す方針を決めたら、突き進む必要がある。

② 「裁量主義・現場責任型」は、高い利便性を志向し、セキュリティ管理は強くしすぎない傾向の企業を指す。最低限のベースは決めるが、現場の自由度は高いため、クリエイティブな社風で採用されることが多い。別の言い方をすると、現場任せとも言え、サイバー攻撃により情報漏えいするリスクや、従業員が故意に情報を持ち出す内部犯行のリスクが高まる。

③ 「場当たり型／フレキシブル型」は、利便性とセキュリティ管理に一貫したポリシーがなく判断が場当たり的になっている企業、若しくは試行錯誤の結果としてフレキシブルにバランスを取っている企業のいずれかが該当する。多くの日本企業がこのタイプに該当するが、許可されていないクラウドサービスの利用などの例外が発生した場合、意思決定が遅くなる傾向がある。また、緊急事態宣言のような想定外の事象が発生した際は、テレワークの利便性とセキュリティのどちらを優先するかで社内の意見が分かれる懸念がある。

④ 「セキュリティ原理主義型」は、強いセキュリティ管理を志向し、利便性の低さはある程度許容する企業を指す。全従業員にはノート PC や業務用スマホが支給されておらず、テレワークは限定的に認めている傾向があり、公共団体、規制業界である重要インフラ事業者に多い。このタイプは、DX や働き方改革が進めにくく、感染症などの危機発生時に対応しづらい。

4. 利便性とセキュリティのバランスに関する取組み事例

ここで、利便性とセキュリティのバランスに関する取組み事例を紹介する。なお、企業の取組みの一部を紹介するものであり、各企業が全社的にどのタイプに該当するかを判定していないことに留意いただきたい。

「日本ユニシス」が事業継続とセキュリティのリバランスに取り組んだ事例 [4]

システムインテグレーターとして日本の情報化社会や産業を支えるシステムを構築する日本ユニシスは、もともとグループ社員全員が社外から安全に社内システムを利用できる環境の整備を進めていた。新型コロナウイルス感染症の発生拡大に伴い、2020 年 2 月からテレワーク・時差出勤を推奨し、4 月以降は出社を許可制とし、グループ社員全員がテレワーク標準の勤務体制にした。

また、これまでテレワークで対応できない業務も、デジタル化を進めることで、テレワーク環境で安全に実施できる業務を増やした。9 割近いグループ社員がテレワークで勤務することになるために、PC の持ち運び、社員の自宅・自宅ネットワーク利用のリスク、協力会社社員のテレワークやクラウドサービス利用ニーズ増加によるリスクなどの各種リスクを評価し、必要に応じ対策を講じたうえで推進した。

現在、同社が掲げるサイバーセキュリティ戦略に従い推進していたゼロトラストの考え方に基づくサイバーセキュリティ対策基盤の整備・実装を、さらに対応のスピードをあげて実施中である。同社は、このサイバーセキュリティ対策基盤を、コロナ禍を踏まえた新しい働き方への変革に必要なセキュリティ基盤と位置付けている。

「ヤフー」の 1 万人規模の無制限テレワーク体制を構築した事例 [5]

2020 年 10 月 1 日より、ヤフーは回数制限やフレックスタイム制のコアタイムを廃止した“無制限のテレワーク制度”を導入した。同社は 2014 年からテレワーク制度を導入していたが、新型コロナウイルス感染症の影響で、原則在宅勤務へ切り替えていた。今回の新制度はコロナ禍の緊急的な体制をこれからの働き方として正式に定めたものである。業務委託先や派遣社員など約数千人、合わせて 1 万人規模の従業員がテレワークで働くことが前提となる。

無制限のテレワーク制度を始めるにあたり特に強化したのは、各端末の操作ログの取得強化である。以前もログ取得は行っていたが、今ほど厳密にはログを取得していなかったという。テレワークになると従業員が故意に情報を持ち出す内部犯行のリスクが高まるためログを厳密に取得する必要があった。また、何かあったときに疑われた社員の身の潔白を証明するのにも使える効果もある。また、同社は個人所有のパソコン利用（BYOD）は認めず、社内システムへのアクセスは会社からの貸与 PC からしか認めていない。社内システムへのログインも、ID とパスワードの他にもう一つ要素がないとできないようにしている。

このように無制限のテレワークという利便性と、ログ取得や強固な認証によるセキュリティ管理というメリハリをつけているのは、守らなければならない情報を特定し、それ以外はある程度のリスクを許容して業務の利便性を上げていくことが大事であるという考え方に基づくものだ。

「ネットフリックス」の独自のセキュリティアプローチ LISA [6]

映画やドラマなどのビデオストリーミングサービスを提供するネットフリックスは、自社保有のサーバを全く持たない 100%クラウド利用の企業である。同社は、場所に依存しない独自のセキュリティアプローチである「LISA（Location Independent Security Approach）」を理念として掲げている。LISA とは、オフィスネットワーク境界内は安全とい

[4] 日本ユニシス「統合報告書 2020」, https://www.unisys.co.jp/invest-j/ir/pdf/ir2020.pdf 及びインタビューより

[5] ITmedia「無制限テレワーク体制を構築したヤフー」, https://www.itmedia.co.jp/news/articles/2010/03/news019.html

[6] https://www.usenix.org/conference/enigma2018/presentation/zimmer

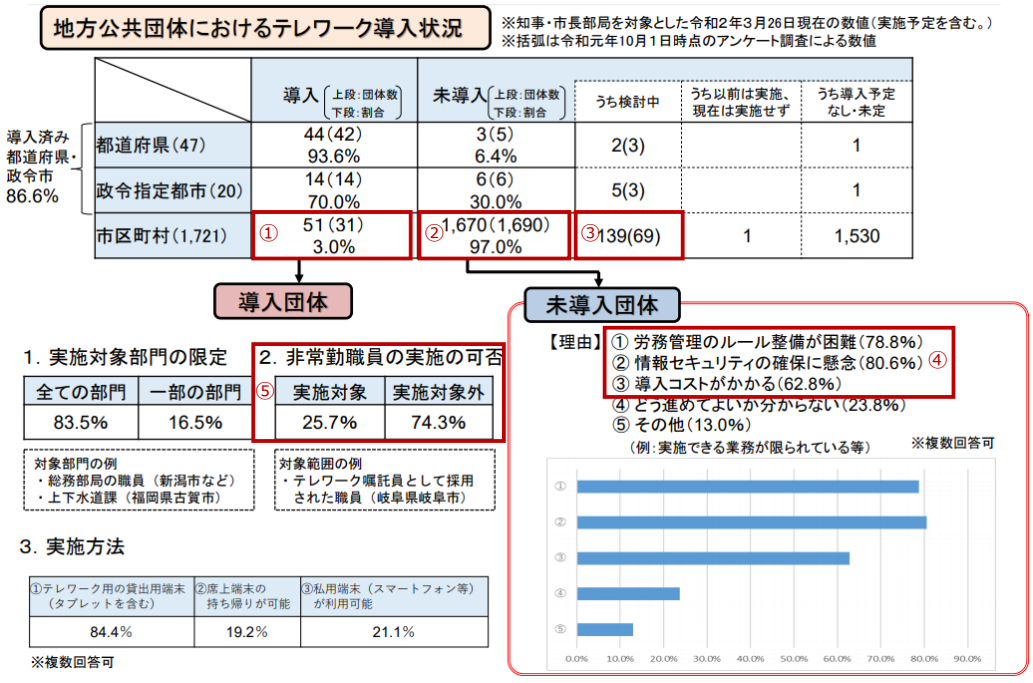
う考え方はやめ、どこからでも安全にリソースを利用するためユーザー認証と端末の信頼性を都度確認するという考え方である。つまり、ネットフリックス版の「ゼロトラスト・アーキテクチャ [7]」である。ネットフリックスは、この考え方を実現するため、独自のソフトウェアを開発し、無償で公開している。また、同社はコンテンツパートナーに対して「コンテンツセキュリティのベストプラクティス」を推奨事項として公開しており [8]、最小権限の原則（例：ゼロトラスト）や多要素認証（MFA）などを要求している。

同社の CEO は、「社員に自由と責任を与える脱ルール経営」が成長を支えていると考えている [9]。この経営哲学を実現するために、100%クラウド利用、場所に依存しないセキュリティアプローチ LISA、コンテンツパートナーに対するセキュリティ推奨事項要求を行っている。

「自治体」ではセキュリティ懸念のためテレワークが浸透していない [10]

総務省が 2020 年 3 月に行った地方公共団体におけるテレワーク導入調査によると、テレワークを導入している自治体は 1,721 団体中、わずか 51 団体（3%）であった。それ以外の 97%の団体（1,670 団体）はテレワークを未導入であり、検討中の団体は 139 団体（8%）しかいなかった。

自治体がテレワークを導入しない理由は、「情報セキュリティの確保に懸念」が 80.6%と最多であり、「労務管理のルール整備が困難」（78.8%）、「導入コストがかかる」（62.8%）と続いた。つまり、情報流出を恐れ、ルール整備の手間を嫌い、予算もないという 3 つの要因が自治体のテレワークを阻害している。また、テレワーク導入自治体であっても、実務を行う非常勤職員の 4 人に 3 人がテレワーク実施対象外であり、テレワークの効果は限定的である。



図表 4 地方公共団体におけるテレワーク取組状況

[7] 信頼できないことを前提としてセキュリティ対策を講じる概念。ユーザーからの要求を常に信頼せず、都度検証を実施し、アクセス許可後は企業リソースに対して最小限のアクセスを提供するもの。米国国立標準技術研究所（NIST）が 2020 年 8 月に定義を公開。

[8] Netflix コンテンツセキュリティのベストプラクティス, https://partnerhelp.netflixstudios.com/hc/ja/articles/360001937528

[9] 第 22 回日経フォーラム「世界経営者会議」, https://www.nikkei.com/article/DGXMZO66027930Q0A111C2000000/

[10] 総務省「地方公共団体におけるテレワーク取組状況」, https://www.fdma.go.jp/laws/tutatsu/items/200630_syoukyu_188.pdf 及び 日本経済新聞「テレワーク難民の自治体職員」,https://www.nikkei.com/article/DGXMZO64142990T20C20A9000000/

JCIC が上記以外にも調査した取り組み事例を図表 5 に整理した。2 つのタイプ両方に該当する企業も存在しており、この場合は図表 1 の「利便性とセキュリティのバランスモデル」のタイプが重なり合う部分に該当する。

タイプ	テレワークの取組み	個人端末の業務利用（BYOD）	Web会議利用	行動監視	例外判断
①利便性重視・モニタリング型	原則、全社員・派遣社員テレワーク可	利用可（専用アプリ）	ブラウザ利用であれば制限なし	端末操作ログなどを取得し、監視を強化	セキュリティ部門と協議
②裁量主義・現場責任型	原則、全社員・派遣社員テレワーク可	利用可（制限なし）	ブラウザ利用であれば制限なし	ログは取得しているが常時監視なし	ベースを決め、現場で管理
③場当たり型／フレキシブル型	原則、全社員・派遣社員テレワーク可	不可	ブラウザ利用であれば制限なし	端末操作ログなどを取得し、監視を強化	セキュリティ部門と協議
④セキュリティ原理主義型	テレワークは未導入、若しくは一部職員に限定	不可	指定ツール以外は都度承認	ログは取得しているが常時監視なし	原則、許可されない

図表 5 代表的な取り組み事例

- テレワークの取組みについては、「④セキュリティ原理主義型」以外は原則全社員・派遣社員が認められている。
- 個人端末の業務利用（BYOD）は、「①利便性重視・モニタリング型」と「②裁量主義・現場責任型」が利用可能であり、前者は端末に機密情報が残らない専用アプリのインストールを必須条件になっていることに対して、後者はアプリの制限はない。
- Teams や WebEx、Zoom などの Web 会議システムの利用については、「④セキュリティ原理主義型」は組織で指定されたツール以外を利用する場合は、リモート会議の都度承認が必要になっている。④以外のタイプでは、ブラウザ利用であれば参加する Web 会議の種類に制限を設けていない。
- 行動監視については、「①利便性重視・モニタリング型」と「③場当たり型／フレキシブル型」は、パソコンやモバイル端末の操作ログ（イベントログ）やセキュリティログを厳密に取得し、常に監視をしている傾向がある。一方、「②裁量主義・現場責任型」と「④セキュリティ原理主義型」は一般的なログは取得しているが、常時監視は厳格に行っていない傾向がある。前者はリソース不足が原因と考えられ、後者はそもそもセキュリティを厳格にしているためログ監視は重要視していないことが考えられる。
- 既存のセキュリティポリシーではカバーされていない例外判断（例：一時的な未許可クラウドストレージ利用など）が必要な場合、「②裁量主義・現場責任型」は現場責任者による判断に任せる傾向がある。また、「④セキュリティ原理主義型」の場合、原則例外判断は許可されない。

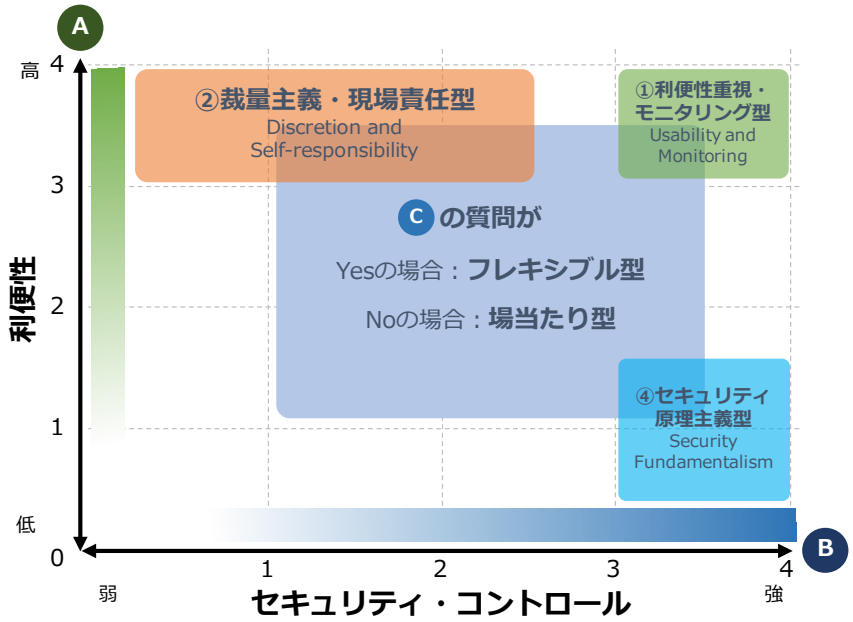
5. バランスモデルの活用方法

バランスモデルの活用方法を説明する前に、自社がどのタイプに属するのかを簡単に判定するための質問票を図表 6 に示す。まず、利便性の 4 つの設問に答え、Yes の回答数をカウントする（Ⓐ）。なお、企業内の一部だけに該当する設問は、Yes の数を 0.5 個分とカウントする。次に、セキュリティ・コントロールの設問に答え、同様に Yes の数をカウントする（Ⓑ）。そして、図の縦軸Ⓐに利便性の Yes の数、横軸Ⓑにセキュリティ・コントロールの Yes の数を位置づけると、現在自社が属するタイプがわかる。また、場当たり型とフレキシブル型の判定は、（Ⓒ）の質問で決まる。

利便性のスコア（縦軸の数値）	回答
従業員の生産性を最大限に向上させる姿勢が経営層にあり、十分なリソース（人・予算）を与えている	Yes / No
会社支給以外のパソコンやモバイル端末からでも、ルールに従えば社内のデータにアクセスできる	Yes / No
標準外のクラウドサービスやアプリの利用に関し、短期間で利用可否が判断される	Yes / No
全ての社員・派遣社員がテレワークが認められており、外でオフィスと同じ業務ができる	Yes / No
合計（Yesの数） ※一部だけで満たしている場合はYesの数を0.5個とカウント	**Yesの数** A

セキュリティ・コントロールのスコア（横軸の数値）	回答
自社独自のセキュリティ理念を確立し、不足するセキュリティ機能は独自開発するなど、多大なリソースをかけてでも理念の実現を目指す	Yes / No
機密データが厳しく管理されており、技術的に外部に持ち出せない状態になっている	Yes / No
自社システムにアクセスする全てのパソコンやモバイル端末の操作ログやセキュリティログを一元管理し、不正な操作は即時アラートを上げている	Yes / No
全社的なセキュリティポリシーを策定し、定期的なリスク評価結果をもとに改善に取り組んでいる	Yes / No
合計（Yesの数） ※一部だけで満たしている場合はYesの数を0.5個とカウント	**Yesの数** B

場当たり型／フレキシブル型の判定	回答
新しいニーズや変化が発生した際に、決められたルールにしたがい、許容できるリスクを判定し、社内の承認を得ている	Yes / No C



図表 6 バランスタイプ判定

自組織が現状どのタイプになるのかを把握した後のバランスモデル活用の流れは、以下の通りである。

1. 自組織の経営戦略がどのように変化していくのかを理解する
2. 自組織のありたい姿を前提として図表 6 のバランスモデル判定設問に答え、目指すべきタイプを明確にする
3. 中長期的に目指すタイプについて社内の合意を得る（図表 7 に例を示す）

特に、中長期的に目指すタイプを設定する際は、今後の経営戦略と整合性が取れていることが重要である。どのタイプにも一長一短があるため、目指すタイプは経営者の考え方に依存するが、現場のセキュリティ責任者が経営者を巻き込み検討することも有効である。なお、2 つのタイプが重なり合う中位を目指す選択肢もある。また、企業単位でタイプを検討するのではなく、各事業部や部門単位で検討することも可能である。

中長期的に目指すタイプが社内で合意が取れると、取るべき打ち手が具体化しやすくなる。例えば、社内システム・ネットワークの再構築、セキュリティポリシーや規程類の見直し、社内プロセスの見直しなどの具体的テーマを決め、それぞれの計画を策定し、実行に移す流れになる。

参考までに、②～④のタイプが目指すタイプの例を以下に示す。

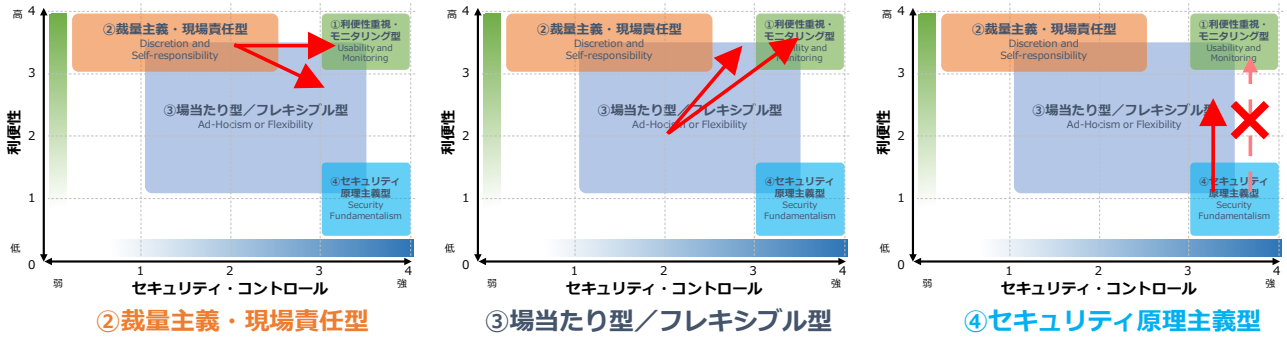


図 7 それぞれのタイプが目指すタイプの例

- 「②裁量主義・現場責任型」が目指すタイプは、主に 2 パターン考えられる。利便性を維持しながら、セキュリティ管理を強化し、①利便性重視・モニタリング型に近づける選択肢。もう 1 つは、株式上場などを契機に利便性に一部制約をかけ、セキュリティ管理を強化し、③場当たり型／フレキシブル型を目指す選択肢である。
- 「③場当たり型／フレキシブル型」については、現状の場当たり型／フレキシブル型の中で利便性とセキュリティ管理を高めるか、①利便性重視・モニタリング型を目指すかの選択肢が考えられる。
- 「④セキュリティ原理主義型」が、「①利便性重視・モニタリング型」を直接目指すことは、既存の企業文化や取引先などのステークホルダーの観点から難しい。よって、セキュリティ管理の強さを維持しつつ、③場当たり型／フレキシブル型を目指すことが現実的であろう。
- なお、「①利便性重視・モニタリング型」が利便性とセキュリティ管理のどちらかを緩め、他のタイプを目指すことも考えられるが、該当する企業は少ないため図 7 から割愛した。

6. まとめ

本レポートでは、アフターコロナの時代を見据え、利便性とセキュリティリスクのバランスを見直すための考え方を整理した。セキュリティ責任者などが「利便性とセキュリティのバランスモデル」を用いて自社の現状を把握し、今後の経営戦略と整合性を取ることで、中長期的に目指すタイプを社内合意するための一助にしていただきたい。

2025 年までにリバランスを実現し、運用を始めなければならない。2025 年までとした理由は、IT システム「2025 年の崖」によりデータ流出リスクが高まること、Windows10 Pro サポート終了によりパソコンの入れ替えがバランスの見直しの契機になることが挙げられる。また、JCIC「サイバーセキュリティ情報公開のポイント」で示した通り、2025 年以降、「デジタル化のビジネスメリットの理解」と「セキュリティの重要性の理解」がなければステークホルダーから経営者にふさわしくないと言われる時代になっていよう。つまり、経営者にも「プラス・セキュリティ人材」が求められるのだ。全社的なシステム・ネットワークの再構築を実施する場合、企画立案・予算確保・プロジェクト実行までに少なくとも 2 年以上かかることが多いため、利便性とセキュリティのリバランスを早急に着手しなければ手遅れになる。2025 年は、遠い将来ではなく、あっという間に迫る手の届く未来であり、生き残りをかけた競争はもう始まっているのだ。

最後に、利便性とセキュリティのリバランスを実現することは「手段」であり、「目的」ではないことをお伝えしたい。最終的な目的はあくまでも「企業ビジョンの実現」、「売上や利益の増加」、「生産性向上」、「顧客満足度向上」などであることを忘れてはならない。アフターコロナの時代には、これらの目的を達成するために、利便性とセキュリティのリバランスが必要とされるのである。

以　上

参考資料①　「サバイバル度」チェックリスト

アフターコロナの時代において、読者の皆様や皆様の所属する企業・団体がサバイバルできるかを判定するチェックリストを以下に示す。JCIC が会員企業などに調査したところ、83%の回答者が「ニューノーマル適用型」であり、17%が「見直し要」であった。なお、「要注意」はいなかった。（回答者数 36 名）

あなたが所属する企業・団体やあなた自身の考えについてお答えください。

#	カテゴリ	設問	回答
1	経営戦略	あなたの会社の経営戦略や働き方は、コロナ禍により大きく変わった	Yes / No / 不明
2		あなたは自社の経営戦略の概要を他者に説明できる	Yes / No / 不明
3	事業継続計画	再度、緊急事態宣言が発表されても、デジタル化やテレワークを進めているため、自社ビジネスに影響は少ない	Yes / No / 不明
4		サイバー攻撃などによる大規模なシステム停止は、事業継続計画（BCP）に含まれている	Yes / No / 不明
5	顧客価値	自社の製品サービスは、非対面でも提供できるようデジタル化を進めている	Yes / No / 不明
6		自社の製品サービスは、デジタル化・オンライン化されており、経営者が利便性とリスクのバランスを理解している	Yes / No / 不明
7	社員価値	オフィスや現場以外でも業務が可能であり、出退勤時間はある程度自由である	Yes / No / 不明
8		コロナ禍によるテレワーク推進に伴い、セキュリティポリシーや管理策はを見直した	Yes / No / 不明
9	情報システム	自社の情報システムは、従業員の生産性とセキュリティのバランスを考慮している	Yes / No / 不明
10	製品サービス	自社の製品サービスは、ユーザーの利便性とセキュリティのバランスを考慮している	Yes / No / 不明

Yesの数	サバイバル度
0～3個	要注意
4～6個	要見直し
7個以上	ニューノーマル適応型

図 8「サバイバル度」チェックリスト

参考資料②　「利便性とセキュリティの判断シート」

既存のセキュリティポリシーではカバーされていない例外判断に日々悩んでいるセキュリティ責任者は多いであろう。以下の図表は、利便性とセキュリティを意思決定する際の判断シートであり、意思決定時に役立つものである。

この例では、自社のデジタルサービス（会員サイトなど）におけるユーザー認証方式を検討する際の選択肢を示している。特に重要なポイントは、セキュリティリスクの影響と発生可能性だけではなく、ユーザーの利便性も 1 つの表で評価している点である。この判断シートを用いることで、多くの関係者の認識を統一できるメリットがある。

検討項目	自社のデジタルサービスにおけるユーザー認証方式を検討すること

項番	選択肢	ユーザーの利便性		セキュリティリスク		補足事項	
		メリット	利便性評価	影響	発生可能性		
1-1	ID/PWのみ	多くのサイトの認証で慣れているため利便性は高い	○ 迷わず作業が可能	△ 不正アクセスにより、顧客情報や機微情報が漏えい	× 1年に2件以上、特殊技術要	認証を強固にするため、パスワードポリシーを厳格にする必要がある	
1-2	ID/PW＋メール認証	メールによる二段階認証は徐々に普及していることから、多くのユーザーが利用可能	△ 手順書が必要		△ 1年に1件程度	フリーメールを許可しない場合、発生可能性は「○」に変更	
1-3	ID/PW＋SMS認証	携帯電話番号に紐づいたSMSでの認証は徐々に普及していることから、多くのユーザーが利用可能	△ 手順書が必要		○ 数年に1件以下	SMS認証は堅牢ではないため、1人1個のアカウントに制限する必要がある	➡採用
1-4	ID/PW＋OTP認証	OTP（ワンタイム・パスワード）のアプリやデバイスが必要なため、利便性は高くない	× 人のサポートが必要		○ 数年に1件以下	ユーザーは専用アプリのインストールや専用デバイスが必要	

凡例

【利便性】
× 低：人に教えてもらわなければ、作業ができない
△ 中：手順書を見ることで、作業が可能
○ 高：一般的に手順書を見ることなく、迷わず作業が可能
◎ 優：直感的に操作が可能であり、作業効率が最大化される

【影響】
× 大：全社に深刻な金銭的な損害あるいは信用の失墜を免れない
△ 中：重大な損害を引き起こし、罰金または金銭的損失の可能性があるもの
○ 小：外部に開示されると軽微な損害を被るもの

【発生可能性】
×× 特大：1年に2件以上インシデント発生、特殊技術不要
× 大：1年に2件以上、特殊技術要
△ 中：1年に1件程度
○ 小：数年に1件以下

図 9 利便性とセキュリティの判断シート

参考資料③　「2025 年の主な出来事」

図表 10 は、2025 年の主な出来事を政治、経済、社会、技術の 4 つの観点からまとめたものである [11]。本レポートタイトルに記載した「2025 年」は、日本では少子高齢化が進み、働き手の金銭的・労働的な負担が増加していることがわかる。そのため、デジタル化や自動化による生産性を向上させる必要があり、利便性とセキュリティのバランスも見直さなければならない。

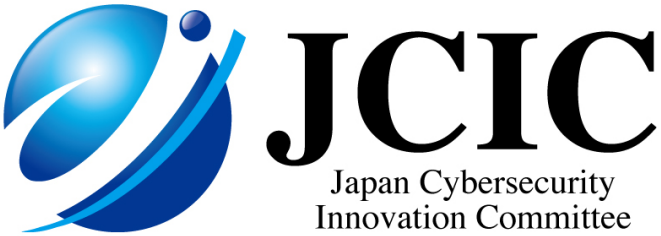
Politics（政治）	Economy（経済）	Society（社会）	Technology（技術）
会社員 1 人当たりの保険料が年収の約 3 割へ	キャッシュレス決済比率が 2017 年の倍の 4 割へ	2025 年大阪・関西万博開催	IT システム「2025 年の崖」
男性の厚生年金の受給が 65 歳に引き上げ	自動運転レベル 4（無人自動運転）のサービスが全国 40 か所以上に	日本国民の 4 人に 1 人が 75 歳以上（2025 年問題）	Windows 10 Home and Pro サポートライフサイクル終了
韓国で APEC 開催	商用水素ステーションが全国 320 箇所程度に整備	世界の人口が約 80 億人までに増加	昭和時代に構築したシステムで不具合が生じる「昭和 100 年問題」
EU、経済通貨同盟（EMU）完成	NTT の固定電話網が IP 網へ完全移行	EU、東アジアの人口が減少傾向へ	IoT 機器が 416 億台に達し、約 80ZB のデータを生成

図 10 2025 年の主な出来事

参考文献

- 一般社団法人日本スマートフォンセキュリティ協会（JSSEC）「テレワーク状況とセキュリティに関するアンケート調査レポート」（2020 年 7 月）, https://www.jssec.org/report/20200722.html
- 日本ユニシス「統合報告書 2020」, https://www.unisys.co.jp/invest-j/ir/pdf/ir2020.pdf
- ITmedia「1 万人規模の“無制限テレワーク”体制を構築したヤフー セキュリティ対策はどう変えた？」, https://www.itmedia.co.jp/news/articles/2010/03/news019.html
- Netflix コンテンツセキュリティのベストプラクティス, https://partnerhelp.netflixstudios.com/hc/ja/articles/360001937528
- 第 22 回日経フォーラム「世界経営者会議」, https://www.nikkei.com/article/DGXMZO66027930Q0A111C2000000/
- 総務省「地方公共団体におけるテレワーク取組状況」, https://www.fdma.go.jp/laws/tutatsu/items/200630_syoukyu_188.pdf 及び 日本経済新聞「テレワーク難民の自治体職員」,https://www.nikkei.com/article/DGXMZO64142990T20C20A9000000/
- NIST SP 800-207 Zero Trust Architecture, https://csrc.nist.gov/publications/detail/sp/800-207/final
- 社会保険料、25 年度に年収 3 割超, https://www.nikkei.com/article/DGXNASFS1602Z_W2A410C1MM8000/
- NRI 未来年表 2020-2100, https://www.nri.com/jp/knowledge/publication/cc/nenpyo/lst/2021/2021/2021
- SMBC 日興証券「2025 年問題」, https://www.smbcnikko.co.jp/terms/other/N0003.html
- IPSS「国連世界人口推計」, http://www.ipss.go.jp/publication/e/jinkomon/pdf/18557206.pdf
- Windows 10 Home and Pro サポートライフサイクル, https://docs.microsoft.com/ja-jp/lifecycle/products/windows-10-home-and-pro （2020 年 11 月閲覧）
- IDC IoT Research（2019 年 6 月）, https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[11] この 4 つの観点を用い、世の中の動向をマクロ的に把握する分析手法を「PEST 分析」と呼ぶ。



[本調査に関する照会先]

主任研究員　上杉謙二　uesugi@j-cic.com