IPA Better Life with IT

テレワークの情報セキュリティ

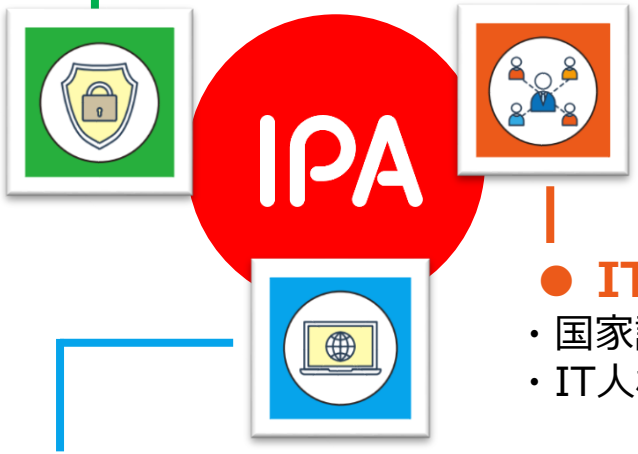
2021年10月

独立行政法人情報処理推進機構
セキュリティセンター　セキュリティ対策推進部
セキュリティ分析グループ

IPA（情報処理推進機構）のご紹介

Information-technology Promotion Agency, Japan

- 日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人
- 誰もが安心してITのメリットを実感できる「 **頼れるIT社会** 」を目指しています



● 情報セキュリティ

・ウイルス、不正アクセス等の届出機関
・情報セキュリティの調査研究、普及啓発活動
・標的型サイバー攻撃への情報共有・初動対応の実施

● IT人材育成

・国家試験「情報処理技術者試験」の実施機関
・IT人材の育成・発掘・スキル明確のとりくみ。若手人材育成。

● IT社会の動向調査・分析・基盤構築

・新たなIT社会の動向調査、新しい技術の安全性・信頼性の確保に向けた指針策定など

目次

1. 2020年の状況

2020年の状況

◆ 働き方の変化

- 勤務場所の多様化、テレワークや業務のオンライン化が定着

◆ テレワーク等のニューノーマルな働き方を狙った攻撃の増加

- テレワークを行うために必要なIT 機器・サービスの利用拡大に伴う、脆弱性の発見、テレワーク端末が原因となったウイルス感染や情報漏えいなど

◆ ガバナンスの低下によるセキュリティリスクの増加

- セキュリティに係るルール遵守の確認が困難
- 特例、例外により緩和された対策が見直されていない
- 働き方の変化に対応した規定やルールが整備出来ていない

情報セキュリティ10大脅威
2021 脅威ランキング

「個人」向け脅威	順位	「組織」向け脅威
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	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
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの個人情報の窃取	7	予期せぬIT基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの不正ログイン
不正アプリによるスマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

情報セキュリティ10大脅威 2021より

テレワーク等のニューノーマルな働き方を狙った攻撃事例

情報セキュリティ白書2021　P214より

◆脆弱性の悪用によりVPNのパスワード流出(※1)

- 2020年8月、VPN製品の脆弱性が悪用されて窃取された認証情報、約900件がインターネット上で公開されていた
- 悪用された脆弱性やその対策に関する情報は2019年4月に公開済みだった
- 更新プログラムを適用していないVPN製品が狙われた

◆テレワーク中にウイルス感染、社内に拡大(※2)

- 社有PCにて在宅勤務
- 社内ネットワークを経由せずに外部ネットワークに接続
- SNSを利用した際にウイルスに感染
- 当該従業員が出社した際に当該PCを社内ネットワークに接続
- 社内ネットワークにウイルス感染が拡大

【出典】

※1　VPN認証情報漏洩に見る脆弱性対策を浸透させる難しさ
https://www.security-next.com/117811

※2　在宅勤務時 SNS経由で社用PCが感染、社内ネットワーク接続で被害拡大（三菱重工業）
https://scan.netsecurity.ne.jp/article/2020/08/14/44439.html

2. テレワークのセキュリティ実態調査

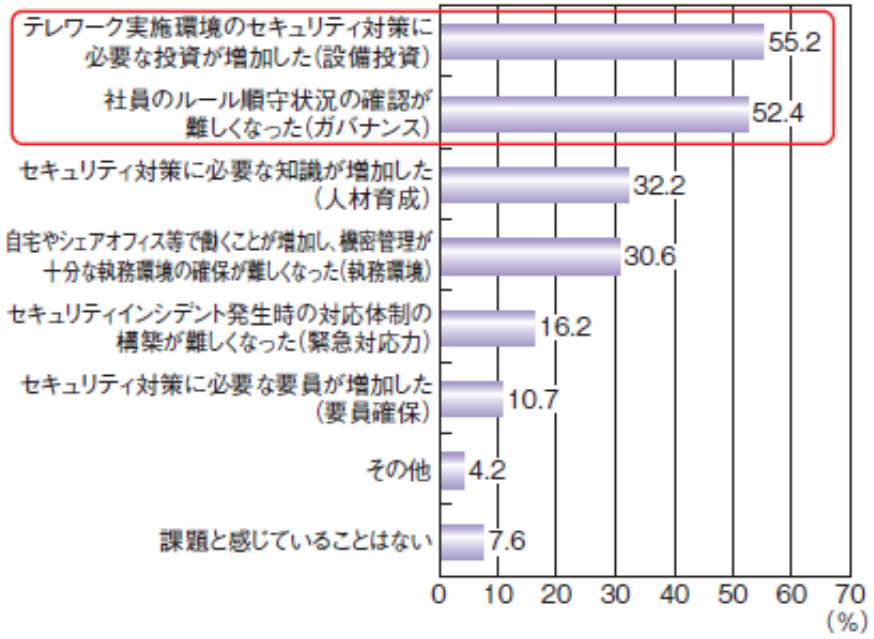
IPAでは2020年度にニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査を実施。本資料では、その結果から見えたテレワークのセキュリティ実態について抜粋して説明。

「ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査」
https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html

テレワーク実施のセキュリティ上の課題

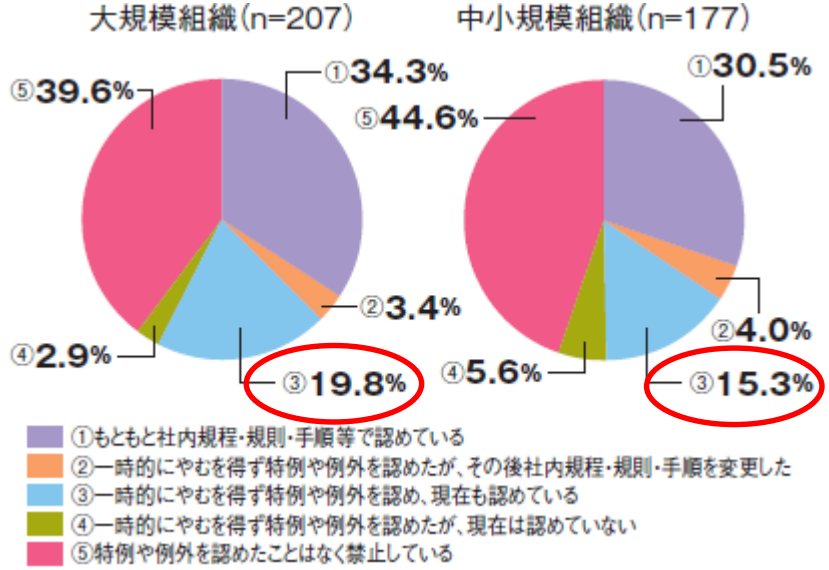
ルール遵守の確認が困難　・　一時的な特例の継続

セキュリティ対策費用の増加
ルール遵守の確認が困難



■図 3-3-5　テレワーク実施時のセキュリティ上の課題(複数回答)
(出典)IPA「ニューノーマルにおけるテレワークとIT サプライチェーンのセキュリティ実態調査」を基に編集
(情報セキュリティ白書2021　P216より)

特例として個人PCやスマホの利用を一時的に認め現在（※）も認めている

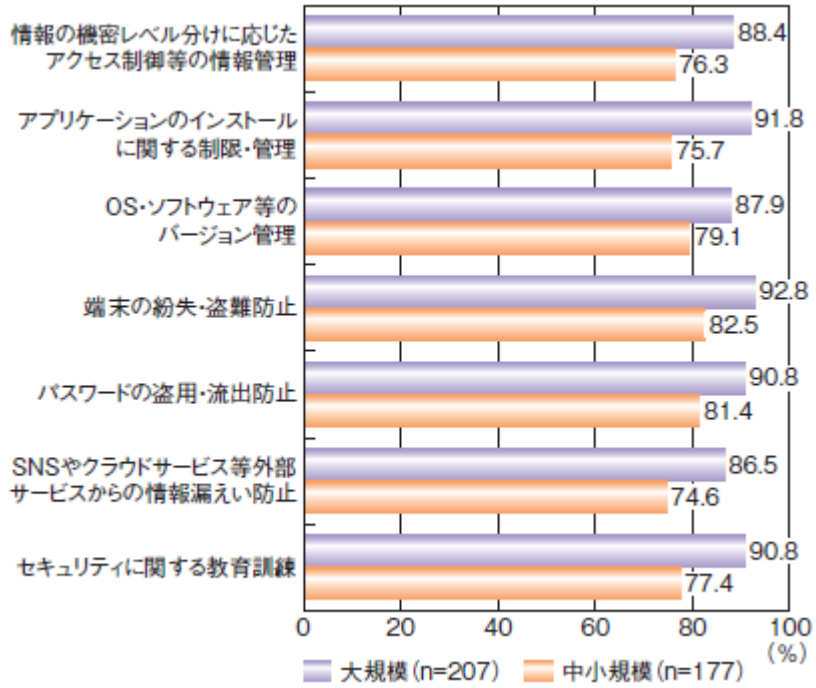


■図 3-3-6　緊急事態宣言中またはコロナ禍の影響により特例や例外を認めたセキュリティ対策の社内規定・規則(個人が所有する端末(パソコン・スマートフォン等)の業務利用)
(出典)IPA「ニューノーマルにおけるテレワークとIT サプライチェーンのセキュリティ実態調査」を基に編集
(情報セキュリティ白書2021　P216より)

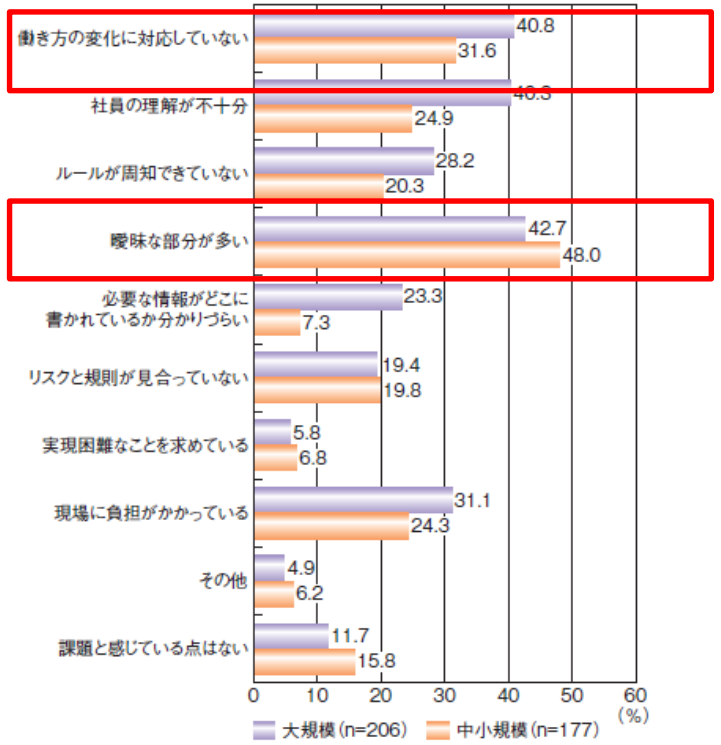
(※)2020/10/31時点

テレワーク実施に関する セキュリティ対策規定の課題

規則は高い割合で制定されている一方で 曖昧な点や変化への対応が課題



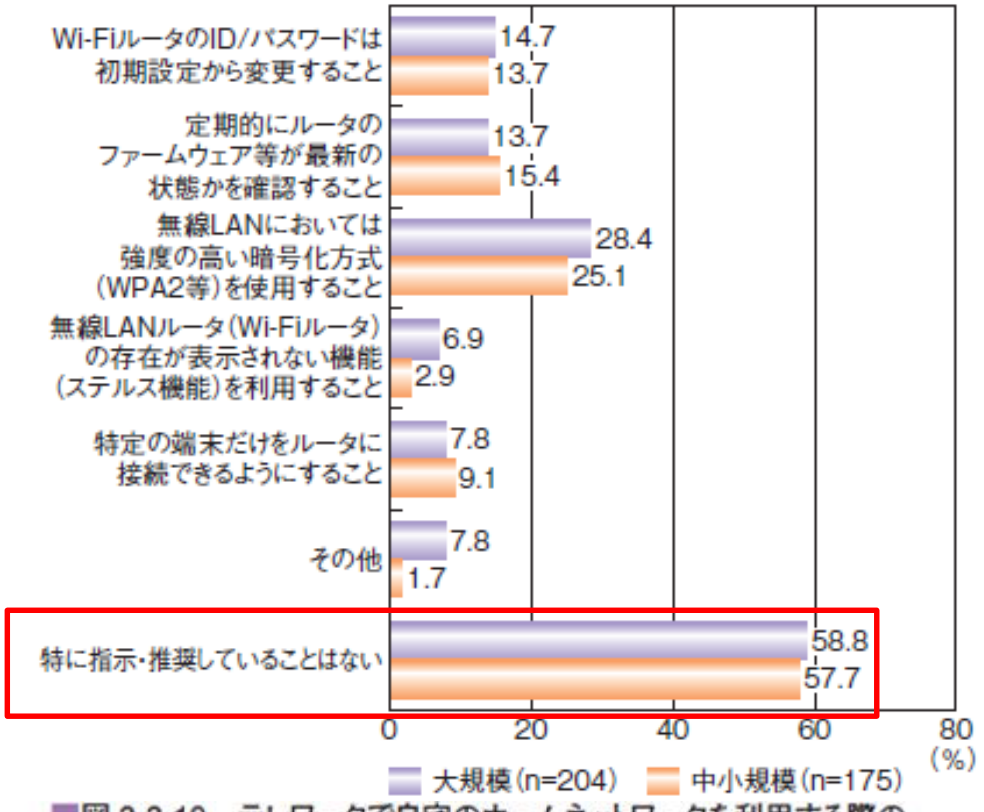
■図 3-3-8　テレワーク実施に関するセキュリティ対策規則の制定状況
(出典)IPA「ニューノーマルにおけるテレワークとIT サプライチェーンの セキュリティ実態調査」を基に編集
(情報セキュリティ白書2021　P217より)



■図 3-3-7　社内規定・規則・手順の課題
(出典)IPA「ニューノーマルにおけるテレワークとIT サプライチェーンの セキュリティ実態調査」を基に編集
(情報セキュリティ白書2021　P217より)

テレワーク実施に関する ホームネットワーク利用時の課題

約６割の企業が指示や指定をしていない



■図 3-3-10　テレワークで自宅のホームネットワークを利用する際の指示、推奨事項(複数回答)

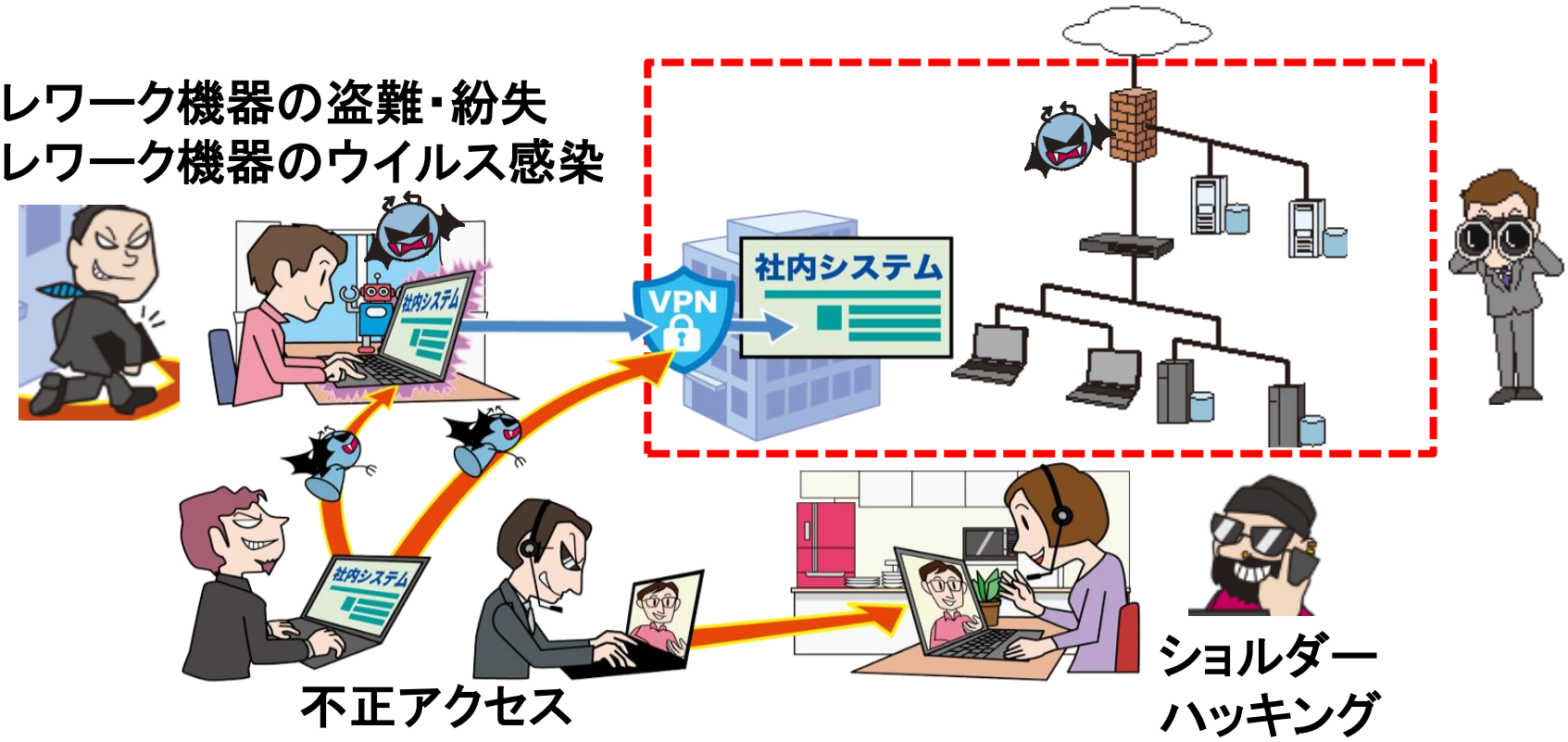
(出典)IPA「ニューノーマルにおけるテレワークとIT サプライチェーンのセキュリティ実態調査」を基に編集

(情報セキュリティ白書2021　P218より)

3. テレワーク環境を取り巻く脅威と対策

テレワーク環境の脅威

テレワーク機器の盗難・紛失
テレワーク機器のウイルス感染



セキュリティ対策が必要な範囲の広がり

個人が直面すると予想される脅威と対策の例

脅威の例	対策の例
不正アクセス ウイルス感染	・端末のOSやソフトウェアの最新化 ・セキュリティソフトのパターンファイルの最新化 ・自宅のルータのファームウェアの最新化 ・自宅のルータのセキュリティ設定の有効化
フリーWi-Fiからの盗聴	・フリーWi-Fiの禁止 ・VPN接続しファイアウォールを経由して通信する
ソーシャルハッキング	・カフェやレストランなどでの業務を禁止する ・自宅でも離席する際はPCをロック ・紙の書類やノートを放置しない
端末や業務資料の紛失	・ワイヤーロックなどの盗難防止対策 ・端末は施錠できるところに保管する

情報セキュリティ白書2021　P218～219より

組織が直面すると予想される脅威と対策の例

脅威の例	対策の例
規則違反	・業務内容に応じた規則の設定（あるいは見直しの実施） ・従業員への教育（想定される被害の大きさを認識させ、被害防止のために実施すべきことを理解させる）
ソフトウェア等の資産管理不備	・端末のOSやソフトウェアが常に最新の状態に保たれるようにするためのテレワーク環境でのメンテナンス手順の整備 ・資管理ソフトウェアなどの導入 ・管理体制の見直し
サーバ等のID 漏えいによる不正アクセス	・ログイン情報の管理 ・ワンタイムパスワードを使用した認証 ・多要素認証 ・組織のネットワークへの接続はVPN を用いる
問い合わせ・報告先の不備	・情報提供窓口、インシデント発生時の通報窓口の整備 ・事象発生時にどのような情報を取得し、どのような形式で展開すべきかの整備

情報セキュリティ白書2021　P219より

テレワーク関連
ガイドライン・情報サイト概要

テレワーク関連ガイドライン・情報サイト名	発行元・運用者	概要
みんなでしっかりサイバーセキュリティ※201	NISC	テレワーク実施者を対象とし、情報セキュリティを確保するための対策や注意点を簡易に説明している。
テレワークセキュリティガイドライン第５版※202	総務省	テレワークにおける情報セキュリティ対策の考え方、ポイント、テレワークトラブル事例と対策一覧等をまとめている。2021 年５月に全面的に改定された。
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）※202	総務省	テレワークセキュリティガイドラインを補完する。セキュリティの専任担当がいない中小企業等がテレワークを実施する際に最低限のセキュリティを確保するためのチェックリスト。
テレワーク時における秘密情報管理のポイント（Q&A 解説）※203	経済産業省	テレワークに対応した規程の整備等について、Q&A 形式でまとめている。
テレワークモデル就業規則～作成の手引き～※204	厚生労働省	テレワーク導入の際に検討が必要な就業規則についての考え方や、参考とすべき規定例、組織におけるセキュリティガイドライン策定の必要性等をまとめている。
テレワークの適切な導入及び実施の推進のためのガイドライン※205	厚生労働省	テレワークの導入・実施にあたり、労務管理を中心に、労使双方の留意点、望ましい取り組み等を明らかにしている。
テレワークを行う際のセキュリティ上の注意事項※206	IPA	テレワーク環境提供の有無、使用場所の違い、テレワーク環境から職場に戻る際の注意点等、テレワーク実施時のセキュリティ上の注意を促している。
Web 会議サービスを使用する際のセキュリティ上の注意事項※207	IPA	組織の Web 会議主催者、情報システム部門を対象に、Web 会議サービス選定時に考慮すべきセキュリティ上のポイントを挙げている。
テレワークのガイド・事例等※208	一般社団法人日本テレワーク協会	テレワーク導入の際に参考となる各種ガイドラインや事例集等を掲載している。

■表 3-3-2　テレワーク関連ガイドライン・情報サイト概要
（出典）各組織の公開情報を基に IPA が作成

（情報セキュリティ白書2021　P213より）

（参考）資料や報告書の入手方法

IPAのサイトからダウンロードいただけます。

情報セキュリティ白書2021
https://www.ipa.go.jp/security/publications/hakusyo/2021.html

情報セキュリティ10大脅威2021
https://www.ipa.go.jp/security/vuln/10threats2021.html

ニューノーマルにおけるテレワークとITサプライチェーンのセキュリティ実態調査

個人編　中間報告
https://www.ipa.go.jp/security/fy2020/reports/scrm/index.html

組織編　中間報告
https://www.ipa.go.jp/security/fy2020/reports/scrm/index-soshiki.html

最終報告
https://www.ipa.go.jp/security/fy2020/reports/scrm/index-final.html