Ｐマークニュース

＜２０２３年爽秋号＞　Vol. ４５

株式会社トムソンネット　Ｐマークコンサルティンググループ

目 次 と 記 事 概 要

１．個人情報保護の JIS 規格が改正されました(2023.9.20)

「個人情報保護マネジメントシステム-要求事項」(JIS Q 15001)が 2023.9.20 付で改正になり、公表されました。改正の背景、内容、その影響について、JIS Q 15001:2023 を考察します。

（１）今回改正の経緯

この規格は、当時の通商産業省が作成した「民間部門における電子計算処理に係る個人情報の保護に関するガイドライン」(1997.3.4 通産省告示 98)を基礎として作成された **JIS Q 15001:1999**「個人情報保護に関するコンプライアンスプログラムの要求事項」を初版として、その後 2006 年、2011 年、2017 年の改正を経て、今回の改正に至っています。

この JIS 規格は 1998 年 4 月 1 日に運用を開始した **JIPDEC「プライバシーマーク制度」の認証基準**です。

今回の改正は、この規格の要求事項の解釈に関し、個人情報保護法改正(最新改正平成 3 年(2021)5 月 19 日公布)に整合する規格とするための改正です。この改正では、「この規格の要求事項の解釈に関し個人情報保護法の取組との関係において、より明確化が求められてきた部分について、要求事項本体の改正でなく、高度で精緻を求められる記載内容を修正し、充実化を図る改正を行った」(JJIS Q 15001:2023　81 頁)としており、「**要求事項の基本的な考え方を変更せず、旧規定に基づいて構築された個人情報マネジメントシステムがこの規格の改正によって不適合を生じないことに配慮した。**」(JIS Q 15001:2023　81 頁)としています。

しかしながら、細部については随所に改正がみられます(後述)。JIPDEC の審査基準での取扱いについては、現在(2023.10.22)のところ、今後公表するとしており、その詳報が待たれます。

（２）改正 JIS の構成

改正された **JIS Q 15001:2023** は、JIS Q 15001:2017 と比較すると 94 頁(改訂前は 66 頁)と頁数が増量になっています。

構成は下記の章立てとなっていますが、解説が詳細に加わって、法令等の「ガイドブック」のようです。

本文規定(0 から 10 まで)
附属書 A(規定)個人情報保護に関する管理策
附属書 B(参考)マネジメントシステムに関する補足
附属書 C(参考)付属書 A の管理策に関する補足
附属書 D(参考)安全管理措置に関する管理目的及び管理策
附属書 E(参考) JIS Q 15001:2023 と JIS Q 15001:2017 との対比

参考文献　解説

JIS Q 15001:2017 では、「附属書 B(参考)管理策に関する補足」となっていた部分を、改正して、「附属書 B(参考)マネジメントシステムに関する補足」と 「附属書 C(参考)付属書 A の管理策に関する補足」とに分けています。

（３）主な改正点

①個人情報保護に関する改正点・・・JIS Q 15001:2017 規格(以降旧規格と呼ぶ)では、個人情報保護方針を外部向けと内部向けとに分けて制定するよう規定されていますが、旧規定における「内部向け個人情報保護方針」と「外部向け個人情報保護方針」を「個人情報保護方針」に統合しています。(本文規定 5.2.1)

②リスク基準に関する規定の変更・・・個人情報保護リスクアセスメントにおいては、旧規定がそのリスク基準の最初に「リスク受容基準」を考慮することとしていますが、改正規定では、**「リスク受容の可否ではなく、本人の権利利益の侵害」及び「関連する法令、国が定める指針その他の規範に対する違反」が生じないことが、リスク優先順位付けの基準になるため、**リスク基準に関する規定を変更しています。(6.2.2a)の 1)

③残留リスク対応の明確化・・・組織は、個人情報保護リスクのリスク対応を行い、残留リスクが許容可能かどうかを判断し、許容した場合も、残留リスクはモニタリング及びレビューの対象として、必要に応じて追加対策を行うが、旧規定では、リスク受容基準を前提に残留リスク対応について「残留している個人情報保護リスクの受容について、リスク所有者の承認を得る」(旧規定 6.1.3e))と規定するだけであつた。改正規定では、さらに明確化し「組織は残留リスクを管理しなければならない」旨の規定を追加しています(6.2.3 の f))。

④情報の利用期限及び保管期限・・・旧規定の「利用期限」と「保管期限」と、個人情報保護法上の利用との対応がわかりにくく、また、「利用期限」及び「保管期限」の意味のちがいについて説明不足であるとされ、審議された。その結果個人情報管理台帳に記載する事項の例示は、「保管期限」だけとした注釈を本文規定 3.3.12 の「注釈 1」に加えています。

⑤その他の主な改正点(変更点)・・・下記の事項について改正ないし補足説明が追加されています。

・個人情報、個人データ及び保有個人データの取扱い
・共同利用
・EU 補完的ルールにおける個人情報の取扱い
・消費者本人への配慮
・行動履歴及びプロファイリング情報
・本人への通知又は明示事項
・クラウドサービスの利用

（4）Pマーク審査はどう変わるか？

JIPDEC のホームページでは、下記の案内がされており、P マーク審査基準の変更については、現在(2023.10.22)のところ明らかではありません。

「プライバシーマークにおける個人情報保護マネジメントシステム構築・運用指針」（以下、「構築・運用指針」）については、JIS Q 15001 の改正内容を踏まえて改定する予定です。構築・運用指針の改定版の公表につきましては、今しばらくお待ちください。

なお、プライバシーマーク制度は「構築・運用指針」に基づいて、個人情報について適切に保護措置を講ずる体制を整備している事業者を評価して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度です。

付与事業者様には、「構築・運用指針」に基づいた個人情報保護マネジメントシステムの構築・運用を求めております。内部規程の見直し等につきましては、構築・運用指針の改定版の公表をお待ちください。

P マーク審査基準については、2021 年 8 月 30 日公表された基準が、2022 年 4 月 1 日から施行され現在に至っており、今回 JIS 規格の改正に基づいて P マーク審査基準が変更になると、ほぼ 3 年に一回、その**「内部規程類の見直し、運用の変更」が P マーク取得事業者に課せられる事になり、その負担の重さを感じざるを得ません。**

２．事例に学ぶ：Wi-Fi ルータのセキュリティについて

事例シリーズの第 22 弾です。今回は『Wi-Fi ルータのセキュリティ』について検討してみたいと思います。

最初に、「Wi-Fi」と「無線 LAN」ですが、「Wi-Fi」は無線 LAN 機能を搭載する製品のうち「Wi-Fi Alliance」という団体が定める規格を満たした製品に付与される認定を指します。通信規格で言えば「IEEE802.11」に適合したものとなります。一方、「無線 LAN」には Bluetooth や 4G や 5G、LTE といったモバイルの通信規格も含まれます。従って、本稿では PC 等のインターネット接続に使われる「Wi-Fi ルータ」をテーマに挙げます。

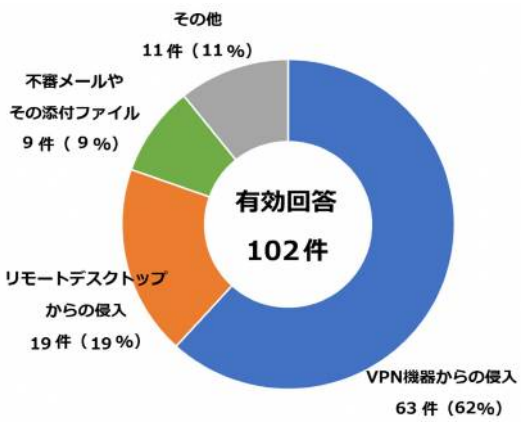
(１)警視庁のレポート

警視庁は 2023 年 3 月に「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」を公表しました。

それによると“ランサムウェア被害の報告件数は過去最多の 230 件に上り、脅迫手口の悪質化や、被害復旧の難しさなどの実態が浮き彫りになった”としています。

「感染経路」で見ると、有効回答 102 件の中で“VPN **機器からの侵入**”が 63 件(62%)と突出して首位を占めています。次に多いのが“リモートデスクトップ”(19 件)で、1 位と 2 位がいずれも**リモートワークの基盤であることに注目**すべきです。

ランサムウェアの【感染経路】



引用：「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」

また、被害企業の規模別では“中小企業”が 54%で、“大企業”の 34%をしのいでトップになっています。中小規模の企業だから狙われることはないと考える訳にいきません。

(２)ブレーン・アシスト社のレポート

中小規模の企業向けにレンタルサーバや情報セキュリティ関連のサービス等を展開している同社(本社：川口市)が 2023 年 9 月 30 日に「PC を無防備でインターネットに晒してみた」結果を公開しました。URL は https://www.brainassist.com/ba-online/archives/2328 です。

PC のファイヤウォールやウィルス対策ソフトを無効化した結果は、掻い摘まんで言えば次のようなものです。

① 晒して(PC 本体をインターネット接続して)瞬時にインターネット対応機器であるかのチェックが入り、1 分程度で Windows 機器であるかが評価され、

② 25 分経つとブルートフォースアタック(ID、パスワードの総当たり攻撃)が始まった。

と言うことです。この後、安易な ID やパスワードを設定していた場合には数日程度で侵入される、と結論しています。PC や Wi-Fi ルータも、(例え話になりますが)**公道に金庫を直置きし**

ている状態と言っても過言ではありません。

（3）Wi-Fi ルータのパスワード設定

Wi-Fi ルータにパスワードの設定箇所がいくつかあります。代表的なのは次のものです。

① 端末(PC 等)の接続用・・・Wi-Fi ルータ本体のシールもしくはセットアップカードに記載されている暗号化キー

② 本体のログイン用・・・管理者用パスワード。Wi-Fi ルータ本体のシールもしくはセットアップカードに記載されているパスワード

③ VPN サーバの設定用・・・外出先から自宅や社内のネットワークにアクセスするためのパスワード

この中で①については、工場出荷状態で製品個体ごとに複雑な文字列が設定されているため、部外者に見られない限り変更する必要はないと考えますが、**②は是非とも変更すべき**です。何故なら、これは Wi-Fi ルータ全体の設定を変更できるオールマイティのパスワードで、一般に初期設定で“password”等の“安易な”文字列が設定されているからです。③には初期設定はなくユーザが自由に設定するもののため、例えば、12 文字以上・英数記号混在で“読めない”文字列にしましょう。年 1 回程度の定期更新もお勧めです。

①、③ともに②のパスワードを使用して Wi-Fi ルータに(管理者として)ログインして変更や設定をしますが、アクセス方法は下図のようにブラウザの **URL 入力欄に「198.168.0.1」**(メーカーによっては「198.168.1.1」もあり)と入れ Enter を押します。ログインに成功すると各種の設定メニューが表示されます。

（4）ファームウェアのアップデート

Wi-Fi ルータに内蔵されているソフト(ファームウェア)のアップデートも重要です。IPA(独立行政法人情報処理推進機構)セキュリティセンターから毎日のように公表している「IPA メールニュース」の【セキュリティ対策情報】に、年に数回 Wi-Fi ルータの脆弱性に関することが混じっています。使用している Wi-Fi ルータが該当した場合には即刻アップデートしましょう。或いは、年に数回メーカのサポート情報を入手するように努めましょう。「IPA メールニュース」の申込みは、https://ipa-mn-web.ipa.go.jp/f/interim/register/s/00001 から行います。アップデートも Wi-Fi ルータ本体にログインし、「メンテナンス」メニュー等からになります。

（5）まとめ

政府の「働き方改革」方針で示された在宅やサテライトオフィスでの勤務が、図らずもコロナ禍で一気に常態化しました。そこで使用される機器は会社の管理下にないものもあることでしょう。PC と同様、Wi-Fi ルータに脆弱性があった場合には会社や社会に重大な脅威となることも考えられ、従業者全員のセキュリティリテラシーの向上が望まれます。

Wi-Fi ルータにログインして設定情報を目にした人は少ないかもしれませんが、ファームウェアの脆弱性対策と併せ、ユーザオプション(ユーザが変更できるよう)になっている各種のパスワードや設定の見直しやファームウェアの更新情報に目を配りたいものです。

３．猛威を振るうランサムウェアの 2023 年上半期における動向

ランサムウェアは、2023 年、独立行政法人 情報処理推進機構（IPA；Information-technology Promotion Agency）によって３年連続で情報セキュリティ上の脅威第１位に位置づけられています。いったん感染すればその被害額は災害級ともいわれており、盤石の備えが不可欠です。

ランサムウェアは 200 種類以上が確認されておりますが、現在、猛威を振るっているのが「saikinLockBit 3.0」と呼ばれるもので、LockBit 3.0 は、近年増加している Raas（Ransomware as a Service）と言われるランサムウェアの運用形態をとっています。

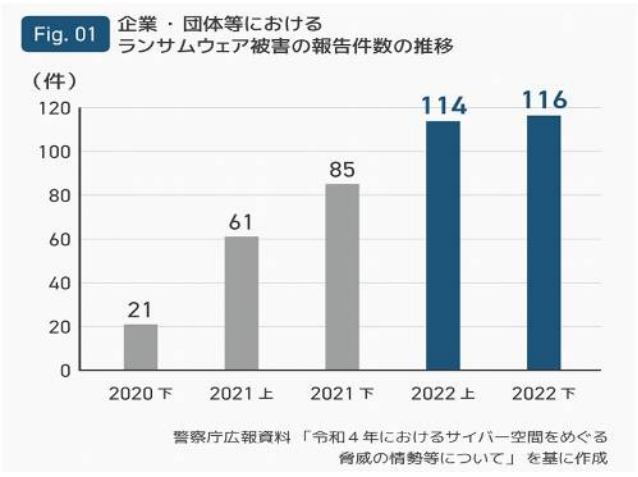
これは、ランサムウェアの開発組織が、実際に攻撃を行う攻撃者（アフィリエイトと呼ばれる）にサブスクリプション型でランサムウェアを提供し、攻撃者が獲得した身代金の一部を報酬として貰い受けるというビジネスモデルです。攻撃者自身にとっては、ランサムウェアを開発したり攻撃を成功させたりするための高度な技術がなくても、手軽に攻撃に参加できてしまうという点でメリットがあるため、被害が拡散してしまうとして大きな脅威となっています。

LockBit 3.0 は、ランサムウェアによって感染した端末のデータを暗号化してその復旧と引き換えに身代金を要求し、そこで支払いに応じなかった場合には、窃取したデータをリークサイトで公開するといったかたちで多重脅迫を行うことでも知られています。

（１）ランサムウェア 2023 年上期被害状況

近年の被害増加の原因としては、匿名性の高い暗号通貨の普及によって、攻撃から身代金受け取りが容易になったこともサイバー攻撃者側にとって有利に働いています。

また、最新の特徴として、**多重脅迫**が挙げられます。データの暗号化／機密情報の公開というように一度ランサムウェアに感染すれば、あらゆる方法で対価を要求されるというもので、その手口はきわめて凶悪です。



警察庁の統計では、2022 年のランサムウェア被害件数は**過去最多となる 230 件**。

これは、2021 年における件数の 1.5 倍以上に相当する数字です（左図）。背景として、新型コロナ禍以降の急速なテレワークの普及に伴いセキュリティホールが拡がり、サイバー犯罪者にとって侵入しやすくなったことが挙げられます。

当然ながら、社会的信用の失墜を恐れて警察に届けられないケースも多数あるとみられ、被害実数がさらに多いことは間違いありません。経済産業省サイバーセキュリティ課が公開した 2020 年の資料によれば、直近の一年間で日本の IT セキュリティ担当者 200 人のうち **52%**がランサムウェアによるサイバー攻撃を受け、実際にデータを暗号化されたことを報告しています。

ランサムウェアの被害を受けた企業は、規模、業種ともに多岐にわたり、一定の傾向のようなものは認められません

（2）ランサムウェアの被害額は？

日本でランサムウェアの被害に遭った組織への調査によれば、暗号化されたデータを復元するために**32%**が「身代金を支払った」の回答でした。その支払った金額の平均は**110 万米ドル（約１億 1,400 万円）でした。**ただ多くの場合、実際の被害はこれに留まりません。

当然ながら、身代金以外にも、事件に関連する調査・復旧について費用が掛かります。警察庁が発表する身代金以外の総額については、**1,000 万円以上を要したケースが 46%**を占めているとのことです。

（3）ランサムウェアの国内被害事例

①金銭的な被害 ～A病院の事例～

VPN 装置の脆弱性からランサムウェアの侵入を許したA病院の事例は、特に深刻です。会計システムや電子カルテシステムがロックされ、診療報酬を請求できないばかりか、患者情報も閲覧できなくなりました。復旧までには２カ月を要し、その間、収入を得られない状態での診療を余儀なくされ、医療活動にも大きな支障をきたしたといいます。

A病院は身代金の支払いを拒否しましたが、システム復旧には**２億円以上の費用**がかかったと発表されており、身代金を支払っても自前で復旧しても、いずれにせよ高額の損害は避けられないことがわかります。多くの事業者は、自前での復旧よりむしろ身代金のほうが安いため、サイバー攻撃者の言い分に従うケースが多いようです。

②システム上の被害 ～B社の場合～

大手食品メーカーB社の事例では、海外からの不正アクセスによりシステム障害が発生、財務管理や販売管理といった基幹システムが暗号化される被害を蒙りました。システムの起動自体ができなくなったことで、四半期決算の報告も延期を余儀なくされ、復旧にはじつに６カ月を要しています。

現代ビジネスにおいて、**ERP** や**基幹システム**はデータの一元化やスピーディーな経営判断に必須のシステムです。、ERP や基幹システムが同時に被害を受けた場合、事業継続が危ぶまれることが好例といえます。

③情報漏洩の被害 ～C社の場合～

ゲームソフトメーカーC社では、やはり VPN 装置経由でランサムウェアの被害に遭い、**15,000 件以上の個人情報が流出**するという甚大な被害に遭っています。

個人情報の内訳は社員、取引先が主とはいえ、流出の可能性を確認した個人情報については採用応募者や顧客にまで及んでおり、顧客からの問い合わせやその後の対応に追われ、深刻な損害を蒙りました。

あらゆる規模、あらゆる業種がランサムウェアの標的となっており、対岸の火事ではありません。

４．お知らせ（トピックス）

（１）令和５年10月末のマイナンバーカードの交付率が７２．７％です。

個人番号カード交付状況（2023年10月31日現在／総務省）

区分	人口（R5.1.1時点）	交付枚数（R5.10.31時点）	交付枚数率
全国	125,416,877人	96,714,263枚	**７２．７％**

政府の懸命なマイナンバーカード普及への努力もあって、2022年10月時点のカード交付率が全国レベルで51%（発行枚数約5,000万枚）であったものが、この1年間で20%以上のアップを果たしています。

（２）ＪＩＰＤＥＣが公表した令和５年９月末におけるＰマーク取得事業者数は17,555社でした。 昨年の９月末のＰマーク取得事業者は、17,222社でしたので、年間増加は333社です。

以上

Ｐマークをはじめとして各種ご相談は下記で承っています。ご気軽にどうぞ！

連絡先　　株式会社トムソンネット　(https://www.tmsn.net/)
〒101-0062 東京都千代田区神田駿河台４－６　御茶ノ水ソラシティ１３階
電話　03-3527-1666　　FAX03-5298-2556

担当:　岩原 秀雄（Mail：iwaharahi1017@tmsn.net ）　　平泉 哲史（Mail：s.hiraizumi@tmsn.net）
本間 晋吾（Mail: s.honma@tmsn.net）