IBM i 7.5「セキュリティレベル20」廃止のインパクトと対処法

旧態への決別を示す新OSの機能拡張と画期的なNVMeを、JBCC 藤原俊成氏が解説

JBCCが6月28日に開催したオンラインセミナー「Powerクラウド vs オンプレ“ガチンコ”セミナー2022」は2部構成で実施された。そのレポートはiMagazineサイトに掲載したが、第2部は紙幅の関係でポイントの紹介にとどめざるを得なかった。そこで本稿は、第2部の講演者である藤原俊成氏（JBCC PFS事業部プラットフォーム推進）にあらためて取材し、前回レポートの補足とした。

藤原氏は第2部で、❶IBM i 7.5の新機能、❷セキュリティレベル20の廃止、❸新しいストレージ環境「NVMe」、の3点に絞って解説を行った。

第1部の豊村洋二氏（JBCC PFS事業部プラットフォーム推進）の講演が、オンプレミスのIBM iをPower Virtual Serverへ移行する際のポイントの解説であったのに対して、藤原氏の講演は、オンプレミスで利用中のユーザーに向けてIBM i 7.5やNVMeをどう捉え、今後どのように対処していくべきかを示したものであった。

クラウドとオンプレミスという好対照の第1部と第2部だったが、“現場”での経験を踏まえた実践的な考え方や対処法の解説という点が共通していた。その意味で、セミナータイトルの“ガチンコ”は、クラウドvsオンプレミスの“ガチンコ”に加えて、ベテランの経験と知見がぶつかり合う“ガチンコ”でもあった。

IBM i 7.5のセキュリティ機能

藤原氏は、❶「IBM i 7.5の新機能」の中で、セキュリティ機能の強化について時間を割いて解説した。以下のような内容である。

（1）新しいパスワードレベル・システム値（QPWDLVL）レベル4の新設
（2）システム提供オブジェクトに対するデフォルトのPUBLIC権限の変更
（3）パスワードがパスワード・ルールに合っているかチェックする（QSYCHKPR）APIの提供
（4）パスワード認証メッセージとリターンコードの表示方式の変更
（5）セキュリティレベル20の廃止

そして❷は、上記（5）の詳細解説で、セキュリティレベル20の廃止の意味と対処法について説明した。つまり藤原氏は、第2部の2／3をIBM iのセキュリティに割いて解説したということである。

その理由について藤原氏は、「IBM iは内向きの閉じられた環境で運用されてきたために、特別なセキュリティ対策を講じなくても安全に利用できていました。しかし最近のように、IBM iをデータベースマシンとして外部から利用したり外部システムとの連携が増えると、さまざまな局面でセキュリティ対策が必要になっています」と指摘したうえで、「IBM i 7.5ではこうした状況を踏まえてセキュリティを大幅に強化しています。IBM iは従来、『セキュリティが強固なシステム』と言われてきましたが、むしろ『セキュリティを強固にできるシステム』と言うべきで、IBM iが備える高度なセキュリティ機能を正しく設定しないと、OS本来がもつセキュリティ機能を十分に活用できません」と説明する。

本稿では上記（1）～（5）のうち、（1）と（5）および❷について藤原氏の解説をレポートする。

新しいパスワードレベル・システム値（QPWDLVL）レベル4の新設

IBM iのパスワードレベルは、IBM i 7.4まではレベル0～3が提供されてきた。レ

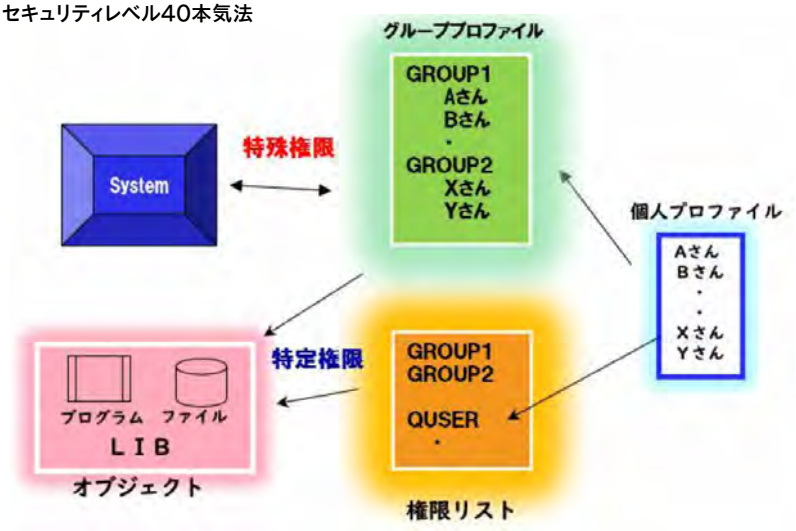
ベル3では最大128文字までのパスワードが設定可能で、大小の英文字、数字、記号、特殊文字を使って、SHA-1などで暗号化できた。ただしSHA-1は攻撃手法が発見されて危険性が高まっているため、それへの対処としてSHA-1後継のSHA-2を導入して暗号化できるようにした。それが今回の「レベル4」の新設である。

これについて藤原氏は、「IBM iへのログインで10文字以上のパスワードを使用しているお客様は、私の経験ではほとんどいません。レベル『0』か『1』が大半で、それゆえに、今回のレ ベル4の新設は多くのIBM iユーザーにとっ て現実味のない拡張だろうと思います」と話す。そして、「そうした状況のお客様に10文字以上のパスワードを推奨し、パスワードレベルを上げることをお勧めするのも現実的とは言えません」と付け加える。

とはいえ、セキュリティの脅威が高まりつつある中で、レベルの低いパスワードを使い続けるのは危険である。

藤原氏はそれへの対処として、セキュリティレベルを「40」へ上げることを推奨している。これは（5）と❷の解説へ続く話である。藤原氏によると、「日本のIBM iユーザーの約6割はセキュリティレベル20で運用中で、“隠れ20”（後述）を含めると、約8割のお客様がレベル20で運用していると推定されます」という。

図表1 セキュリティレベル40本気法



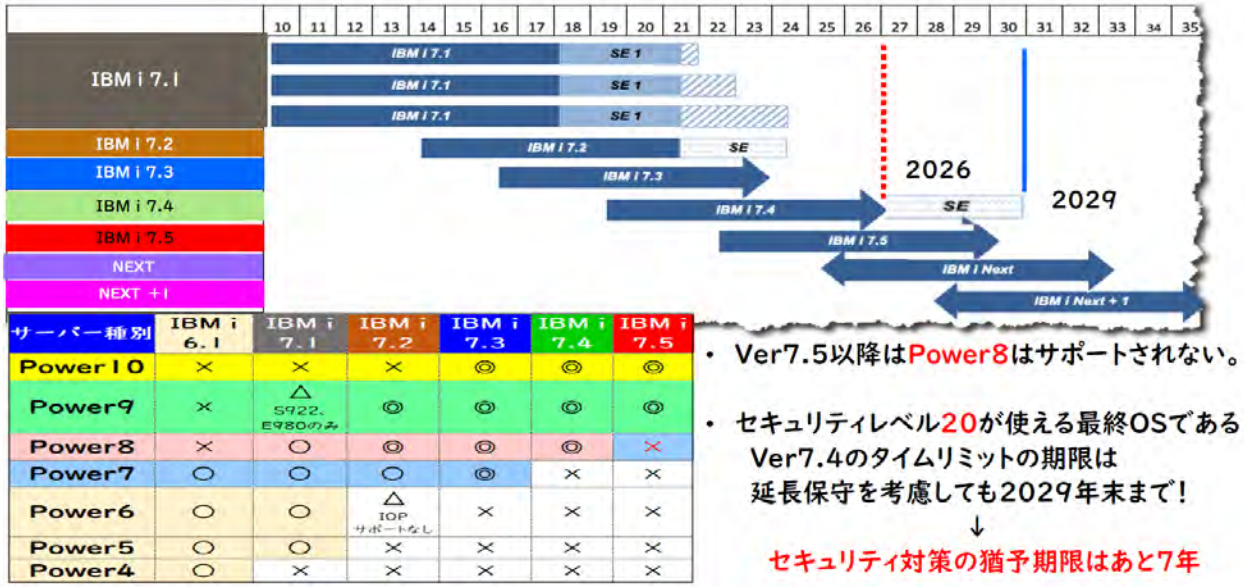
セキュリティレベルの内容は、次のとおりである。

- **レベル10：セキュリティなし**
- **レベル20：IDとパスワード認証**
- **レベル30：レベル20 ＋ オブジェクト認証**
- **レベル40：レベル30 ＋ 経路チェック**
- **レベル50：レベル40 ＋ 個々の権限付与式認証**

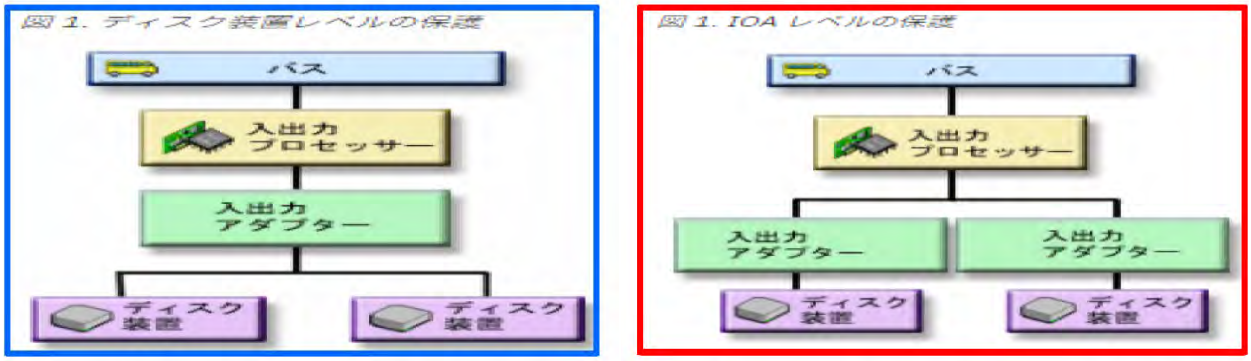
藤原氏は、このセキュリティレベルを20から40へ上げることが、10文字以下のパスワードを使い続けることの「安全性の担保になる」という。

「レベル20は、IDとパスワードが一致しさえすればすべてのシステムリソースにアクセスできるという“万能の”セキュリティルールでしたが、レベル40にすると個々のオブジェクトに対して誰がアクセス可能かを設定する必要があり、さらにIBM iへのア

図表2 IBM iサポート・ロードマップ



図表3 1ランク上の可用性を実現するNVMeデバイス



クセス経路の設定・管理も必要になります。オブジェクトへの認証とアクセス経路の管理ができれば、パスワードが10文字以下であっても、少なくとも外部からの攻撃には強いシステムとすることができます」と、説明する。

セキュリティレベル20廃止の意味と対処法

今回のIBM i 7.5では、セキュリティレベル20が廃止になった。今回のハイライトの1つと言える機能強化で、今後、IBM i 7.5上でアプリケーションを新規に稼働させる場合は、レベル30以上の設定が必要になる（IBM i 7.4以前の環境をIBM i 7.5に移行する場合は、レベル20のまま利用可能）。

この「セキュリティレベル20の廃止」の意味について藤原氏は、「IBM iのセキュリティレベルは2006年のV5R4（IBM i 5.4）からレベル40がデフォルトになっていますが、ユーザーの多くはレベル20に落として運用してきたのが実態です。しかしID・パスワードだけですべてのリソースにアクセスできるのは、さすがに今の時代にはそぐわないとIBMは考え、重い腰を上げたのだろうと見ています。たとえば、最近増えているオープン系のIFSゾーンを狙ったサイバー攻撃には、ユーザープロファイルでアクセス制限を行わない限り、完全なプロテクトは困難です」と説明する。

ただし、IBM iのセキュリティレベルを20から40へ上げるには「いくつかの対処が必要です」と、藤原氏は語る。その対処を行わずにレベル40へ上げると、「アプリケーションの作動中に異常終了したり、必要なデータにアクセスできないなどの事態に直面します」と注意を促す。

藤原氏が推奨するレベル40への切り替え時の対処項目は、以下の6つである。

①組織全体のセキュリティポリシーの策定
②部門や業務単位を代表する代表ユーザーの決定（グループプロファイルの決定）
③一般ユーザーのグループ分け（グループ別にリストアップ）
④外部からSQLやFTPなどで接続してくる時の特定ユーザーの決定
⑤ファイルやプログラム、ライブラリなどの個々のオブジェクトに対する権限のリストアップ
⑥バックアップなどのシステム全体の運用にかかわる特殊権限の割り当てユーザーの特定

藤原氏はこの中の「①組織全体のセキュリティポリシーの策定」が「最も重要」と強調する。

「というのも、セキュリティポリシーを整備し実践している企業はきわめて少数だからです。セキュリティポリシーを策定すれば自ずから部門・業務を代表するユーザーが決まり、個々のオブジェクトを利用できるユーザーも決まってきます。これらが決ればセキュリティレベル40への対応は容易です」（藤原氏）

藤原氏はこれら①～⑥の作業に、「最低でも3カ月はかかります」と話す。ユーザーやオブジェクトの調査と権限関係の調整が必要になるからだ。そのため「時間に余裕をもって計画的に作業を進める必要があります」という。

藤原氏は、①～⑥の作業に時間を割けないユーザーに対して、「セキュリティレベル40もどき法」（以下、もどき法）という暫定的な対処法を説いている。前述の“隠れ20”がこれにあたる。

もどき法とは、①セキュリティポリシーの策定をスキップして、②代表ユーザーを先に決め、その代表ユーザーに＊ALLOBJなどの特殊権限を付与して、さらに一般のユーザー（子ユーザー）が代表ユーザーになりすまし てシステムを利用するという方法である。

オブジェクトへのアクセスを特定のユーザー（＝代表ユーザー）に制限しているので形式的にレベル40に対応していることになり、「システム監査を通すことも可能になります」と、藤原氏は話す。

ただし、もどき法はオブジェクト個々に対する特定権限を設定していないため、「内部からの異常なアクセスやセキュリティホールを突く攻撃には、まったく無力。IBM

参考

・「Powerクラウド vs オンプレ“ガチンコ”セミナー2022」レポート
https://www.imagazine.co.jp/jbcc-seminar-repot2022/

・セミナー「Powerクラウド vs オンプレ“ガチンコ”セミナー2022」(リプレイ動画)
https://www.jbcc.co.jp/event/2022/06/28/6495.html

・セキュリティレベル40への切り替えなどの問い合わせ先
https://www.jbcc.co.jp/contactlist.html

・JBCC「ITモダナイゼーションクリニック」(Power Systems関連の無償相談窓口)
https://www.jbcc.co.jp/products/solution/sol_service/modernization_clinic/

i 7.5でセキュリティレベル20が廃止になったのを機に、レベル40への切り替えに本腰を入れて取り組む時期にきています」と、藤原氏は述べる。

藤原氏は講演で、もどき法から「セキュリティレベル40本気法」(以下、本気法)への移行も解説した。次のような手順になる(**図表1**)。

①ファイル、プログラム、ライブラリなどの個々のオブジェクトに対して権限リストを使って特定権限を設計
②業務運用に必要に応じて代表ユーザー(グループプロファイル)を権限リストに登録
③ゲストユーザー(＊PUBLIC)には、＊EXCLUDE(拒絶)指定を行い、登録以外のユーザーからのアクセスを排除
④権限リストを対象となるオブジェクトに適用(GRTOBJAUTなど)
⑤代表ユーザー(グループプロファイル)に与えていた＊ALLOBJなどの特殊権限を必要に応じて段階的に剥奪
⑥テスト環境でパイロットテストを実施して、順次切り替え確認を実施。

「セキュリティレベル20を継続して使えるのはIBM i 7.4までで、7.4の利用期限はあと約7年(2029年末)と考えられます(**図表2**)。それまでにレベル40へスムーズに切り換えられるよう、準備を進めることが必要です。何かお困り事があれば、当社ではレベル40への切り替えに対応した実績がありますので、ご相談いただければと思います」(藤原氏)

講演では、セキュリティレベル40に対応するための「もどき法」と「本気法」を詳しく解説しているので、リプレイ動画の視聴をぜひお勧めしたい。

標準内蔵ストレージとなったNVMeの特徴とメリット

7月12日に発表になったPower10サーバーのスケールアウトモデルとミッドレンジモデルでは、NVMeデバイスが標準の内蔵ストレージになった。「NVMeデバイスは可用性・高速性・コストで従来の内蔵ストレージを凌駕し、画期的」と、藤原氏は指摘する。

「NVMeとは、不揮発性メモリを使用したフラッシュストレージのための通信プロトコルで、それとSSDをセットしたものがNVMeデバイスです。従来との違いは、4KBの転送メッセージが2つではなく1つで済み、コマンドを処理するためのキューをSSDやHDDのような1つではなく、同時に複数(6万5000個以上)を走らせることができる点です。また、1つのNVMeデバイスは最大32個の名前空間に分割可能で(1つの名前空間はHDD1台分に相当)、64GB～16TBの範囲で設定できます。これによりパフォーマンスを考慮した、複数の名前空間から成るNVMeデバイスを設置することが可能です」(藤原氏)

藤原氏はNVMeのメリットとして、可用性、高速性、コストの3点を挙げる。

可用性については、ヘッドやモーターなどの駆動機構がないので、「HDDと比較して障害発生率が低い」のと、HDDやSSDではSASやFCなどのディスクコントローラが必要になり、そこが単一障害点になる可能性があるが、NVMeデバイスはディスク領域とディスクコントローラが一体となっているので、「1ランク上の可用性を実現します」と、藤原氏は説明する(**図表3**)。

パフォーマンスについては、HDD、SSD、NVMeデバイスの性能比を紹介する。JBCCの計測によると、「1：6：15」という。つまりNVMeはHDDに対して15倍、SSDに対しては2.5倍高速となる。

「当社の実績では、NVMeの導入によって“バッチ処理が速くなった”“オンライン処理のスピードが改善された”という反響をいただいています」(藤原氏)

またコストについては、従来のSSDの約半分の価格という。藤原氏は、コスト、可用性、パフォーマンスで従来製品を凌駕するNVMeデバイスは、「今後急速に普及していくと見ています」と語る。

一方、NVMeデバイスのストレージ部分であるSSDは、従来から「書き込み限界」が話題になる。これはSSDへの書き込みを重ねると機械的に故障するというものだが、これについて藤原氏は、「NVMeでは書き込み限界の心配はまったく無用です」と、次のような試算を基に説明する。

「1.6TBの5年保証付きNVMeで、1日に3回、1.6TBのデータを5年間書き込み続けると、総データ量は約8.7PB(ペタバイト＝8700TB)になります。つまり8.7PBの書き込み耐久性があるということで、現実的な運用を想定すると、15年以上の耐用年数があると考えられます。NVMeの書き込み限界を心配する必要はまったくありません」(藤原氏)

以上、「Powerクラウド vs オンプレ“ガチンコ”セミナー2022」第2部の追加レポートをまとめたが、藤原氏は講演の中で、IBM i 7.5のその他の新機能についても縦横に語っている。ベテランの円熟の解説を、ぜひリプレイ動画で確認していただきたいものである。