

IBM Global Total Microcode Support (GTMS)

2025年 7月

日本アイ・ビー・エム株式会社
テクノロジー・ライフサイクル・サービス

IBM Global Total Microcode Support (GTMS)

マイクロコードの分析と定期的な更新で
脆弱性対策、システム安定性を向上

お客様の課題

- サイバー攻撃／セキュリティ侵害対策強化
- 計画外停止の最小化、可用性向上
- ハイブリッド環境下で複雑に接続されるシステム構成、相互接続関係考慮したマイクロコード選定、更新作業
- ITスタッフの負荷削減、DX/AIスキル強化、本業へ注力

分析サービス

- 契約されたすべてのシステム・マイクロコード、及び接続機器と搭載されたマイクロコード、デバイスドライバとOS関連情報を含めた分析を実施
- 分析結果をシステム安定化プランとして推奨事項を提供

サービスレベル；

- ST5 - 分析データ提供 + オンサイト・マイクロコード適用(年一回)
- ST9 - オンサイト更新(年一回)
- STC - 分析データ提供 + リモート・マイクロコード適用(年一回)

更新サービス

- 適用サービスの窓口一本化
- 年一回定期的マイクロコード更新
- IBM技術員のオンサイト対応
- お客様指定場所にて更新作業実施

メリット

- 関連NISTガイドライン^{*1}へ準拠すべくマイクロコードの適切な更新による脆弱性対策等
- 古いマイクロコード・レベルに起因する計画外ダウン・タイム削減
- 単独機器のみではなくシステム全体のパフォーマンスと可用性を向上
- ITスタッフを不慣れなマイクロコード選定／更新作業から解放しビジネスの優先事項へ集中

IBMの保守サービス

- AI/オートメーション活用の次世代保守サービス
- 情報セキュリティ、コンプライアンスを遵守した技術員による対応
- 世界130カ国、13,000人のサポート・スペシャリスト、IBM,IBM以外の23,000製品に対応し、企業のITインフラをトータルでサポート

IBM Global Total Microcode Support(GTMS)活用による担当者の負荷軽減、対応迅速化

全国技術部とグローバルのミッション・スペシャリストとの連携で複雑なIT環境下の推奨マイクロコードを迅速・確実に選定しご報告、更新します。

お客様の課題

NIST SP800^{*1}シリーズ参照し
ハードウェア・レベル、
ファームウェアでセキュリティ侵害/
脆弱性対策を検討しろって言われても・
NISTってナニ？・・・

マイクロコード更新のスキル習得より
強化しなきゃいけないスキルあるし・・・
そんな時間無いし、他に人いないし・・・

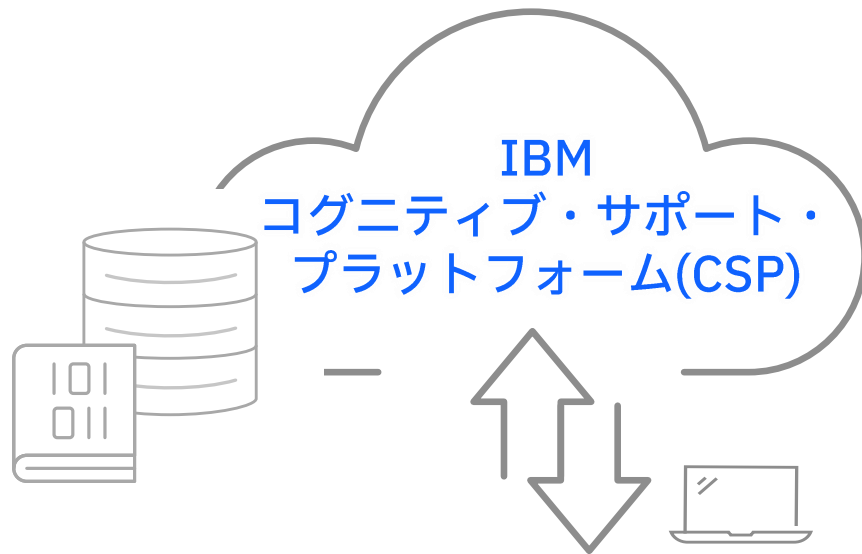
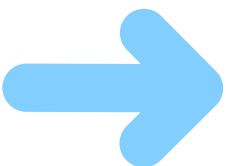
システム環境、
機器相互接続を考慮した
最適ファームウェアの選択？？？
Fix Centralって英語の専門用語だし・・・

ファームウェア、マイクロコード、
BIOSの管理、更新って
うちのIT部門で対応すべき作業なのか？

IBM
GTMS
なら！

IBM GTMS利用ケース

Step 1 専用データ収集ツールによる
システム情報取得



Step 2 データ分析

グローバル
専門家チーム



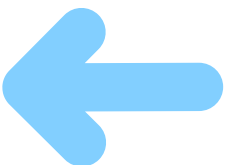
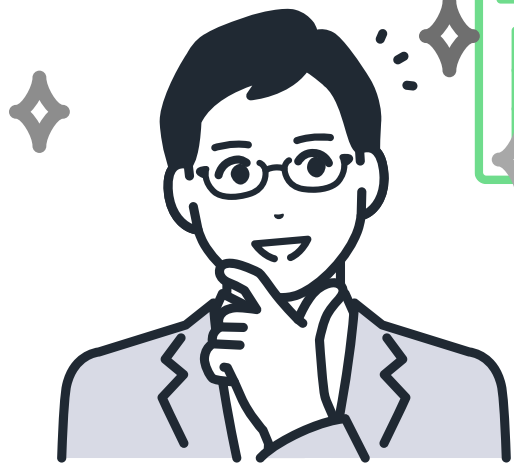
収集データの分析、
レポート作成

Step 3 分析結果ご報告

分析判定

要適用
55% 推奨

分析サマリー
推奨事項



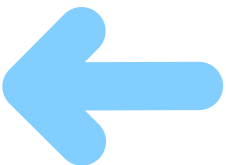
SME Work Complete!

CSP

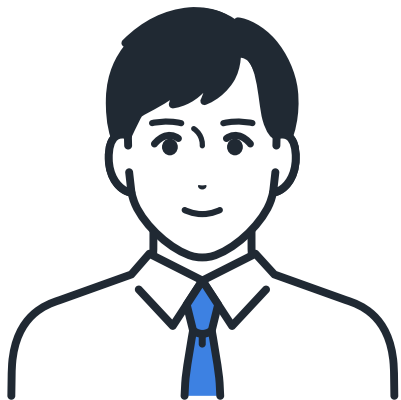
全国技術部

お客様担当技術部より
分析結果のご報告、対策実施

Step 4 推奨アクションの実施



マイクロコード適用



IBM Global Total Microcode Support (GTMS) ユースケース

NIST^{*1}推奨、ゼロトラスト・アプローチに求められるセキュリティ対策

万が一ファームウェアが改ざんされ、その上で稼働するOSやアプリケーションを危険にさらさないためにハードウェア・レベルからセキュリティを考え直す企業が増えています。

IBMは、マイクロコードの知的財産とマイクロコードを分析し更新するスペシャリストの専門知識により、独自の優位性を有しています。

金融業

金融庁が発行する調査報告書^{*2}内“ハードウェア管理”で考察された提言を踏まえ保守サービス・レベルを選定する必要がありました。

“ハードウェアやファームウェアの脆弱性管理は発展途上ではあるが、脅威が顕在化した場合の影響の大きさや検知の困難性を踏まえ、特に大規模な金融機関においては、より高度な攻撃手法を想定した先進的な対策として検討が望まれる領域である。また、規模に関わらず不正なハードウェアやファームウェアの混入を防ぐセキュアな調達の推進が望まれる。本邦金融機関における本領域における改善のステップとして、例えば、以下が挙げられる。i. 自社の ICT サプライチェーンのサイバーリスク評価において、ハードウェアに対する不正なファームウェアの導入のリスクが評価対象となっていることを再確認する。”

医療機関

厚生労働省が発行するガイドライン^{*3}に準拠すべくIoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施し、ファームウェアハッキングツールに対抗すべく対策の検討、運用が必要でした。



エネルギー関連行政法人

調達機器仕様(サーバー)「保守：平日 9:00～17:00 のハードウェアオンサイト対応、ハードウェアのシステム改ざんを検知し、正常に復旧する BIOS 保護機能を有すること」等が提示され、これを満たすサービス・レベルの選定が必要でした。



米国政府機関

サーバーに搭載されている BIOS が米国政府のガイドライン（NIST-SP800- 147他）に沿ったものであり、部品やファームウェアの出所と完全性の検証、さらにファームウェアの不正な変更を防止するよう定期的な修正対応、復旧作業を行う必要がありました。



^{*1} NIST; National Institute of Standards and Technology (米国国立標準技術研究所)

^{*2} 出典) 金融庁「金融セクターのサードパーティ・サプライチェーンのサイバーリスク管理に関する調査報告書 (令和5年12月)」

^{*3} 出典) 厚生労働省「医療情報システムの安全管理に関するガイドライン 第6.0版 (令和5年5月)」

