Hewlett Packard Enterprise | Microsoft | intel

Business white paper

セキュリティ対策が重要な調達基準に!

増加するハード/ファームウエア攻撃から中堅・中小企業がビジネスを守る方法は?

巧妙化するサイバー攻撃、中堅・中小企業が踏み台になる

悪質化・巧妙化し続けるサイバー攻撃。既存のシグネチャ型対策では防げない「ファイルレス攻撃」など、新たな手法が次々と生まれ続けている。

中でも特徴的なのが、ハードウエアやファームウエアを狙う「PDoS（Permanent Denial-of-Service）攻撃」だ。これまでサイバー攻撃というと、ネットワークやアプリケーション、OSを狙うものだというイメージが強く、実際、対策のほとんどがこれらに対して行われてきた。そのため、ハードウエアやファームウエアは“盲点”になっていたが、それが攻撃者にとって格好のターゲットになっているのだ。

また、こうした攻撃は企業の国籍や業種、規模に関係なく起こっている。「有名な大手企業ならいざ知らず、自社が狙われることはないだろう」と考えている中堅・中小企業も、決して他人事にはできないのである。

守りが手薄なことで“踏み台”にされ、取引のある大手企業に損害を与えてしまうリスクは無視できない。こうした状況を踏まえて、セキュリティ対策の実施レベルを取引条件に絞り込む企業も増えている。つまり、十分な対策を講じていない企業は、それだけで取引対象から除外される可能性すら出てきているのである。

もはや既存の対策だけでビジネスの安全を守ることは難しい。しかし、中堅・中小企業のリソースはひっ迫している。「守りのIT」の負担は極力抑え、できるだけ多くのリソースを「攻めのIT」に投入したい、というのが本音だろう。この要求を満たす、解決策はあるのか。日経BP総研の桔梗原 富夫が、ハードウエアセキュリティのキーパーソンに話を聞いた。

日本ヒューレット・パッカード株式会社
ハイブリッドIT事業統括
事業推進統括本部
ハイブリッドIT技術本部 本部長
及川 信一郎 氏

限られたリソースで、最新の対策を実施する方法は

――セキュリティ脅威は時々刻々と変化を続けています。守りが手薄な企業を踏み台にして関係各社を狙う「サプライチェーン攻撃」や、IoT機器の脆弱性といった問題が注目されている中、多くの中堅・中小企業がセキュリティ対策の見直しを迫られていますね。

及川：おっしゃる通りです。セキュリティというと、いままでネットワークやメールをターゲットにした攻撃が注目されてきましたが、ハードウエアへの攻撃も考慮する必要が出てきています。ハードウエアは無条件に信用できるもの、という認識が崩れ始め、OSやアプリケーションへのセキュリティ対策と同じ目線で、徐々に危機感を持つ政府機関や企業が増えてきているようです。

――ハードウエアの脆弱性を狙った攻撃について、もう少し詳しく教えてください。

及川：例えば、書き換えが可能なPCサーバーのファームウエア領域に悪意のあるコードを埋め込み、ハードウエアを乗っ取る手法があります。ファームウエアはOS起動前に実行されるため、通常のセキュリティ対策ソフトウエアでは検知が困難です。OSを再インストールしてもファームウエアのコードは残るため、復旧にあたっては基盤やマシンそのものの交換が必要になります。この攻撃を受けると半永久的に脅威が続くため、PDoS攻撃と呼ばれています。

米国政府機関の調達基準になっているNIST（米国国立標準技術研究所）のレポートSP800でも、ハードウエアセキュリティに関する項目が盛り込まれたほか、当社の年次イベントでも、FBIのコンピュータ・サイエンティスト、ジェームズ・モリソン氏がファームウエアへの攻撃増加に警鐘を鳴らす発言をしました。サイバー犯罪自体が急増していますが、この種の攻撃は今後さらに増えるだろうとみています。

――中堅・中小企業は、この脅威にどう立ち向かえばよいのでしょうか。

及川：後付けでの対策は難しいため、ハードウエア/シリコンレベルのセキュリティを踏まえてつくられた製品を採用しておくことが大事になってきます。シリコンレベルでの対策は、ハードウエアに対する攻撃を防ぐ上で、とても有効です。

HPEは、5年以上前からハードウエアセキュリティの必要性に着目し、長い開発期間を経て、Silicon Root of Trust（シリコンレベルの信頼性）と呼ばれるセキュリティ機構をサーバーに組み込みました。そして、サイバーセキュリティへの注目が高まってきた2017年から、「HPE ProLiant Gen10 サーバー」（以下、Gen10）としてリリースしています（写真）。

写真 ● HPE ProLiant Gen10サーバー シリーズ

シリコンレベルの信頼性と、「Integrated Lights-Out」による高度な自律運用機能を備える高性能サーバー。タワー型のMLラインとラックマウント型のDLラインがある

シリコンレベルの信頼性と運用負荷軽減を両立

――Gen10の強みを教えてください。

及川：シリコンレベルの信頼性を確保したPCサーバー製品です。CPUとは別に「Integrated Lights-Out（iLO）」という小型コンピューターを内蔵しています。iLOは改変不可能なシリコンチップ（ASIC）のため、脅威の影響を受けません。このiLOがファームウエアを監視し、改ざんされていないことが確認できた場合のみファームウエアの起動を行います。また稼働中も定期的にチェックを行います。もちろん、メインのCPU上で動いているOSの動作に影響は及ぼしません（図1）。

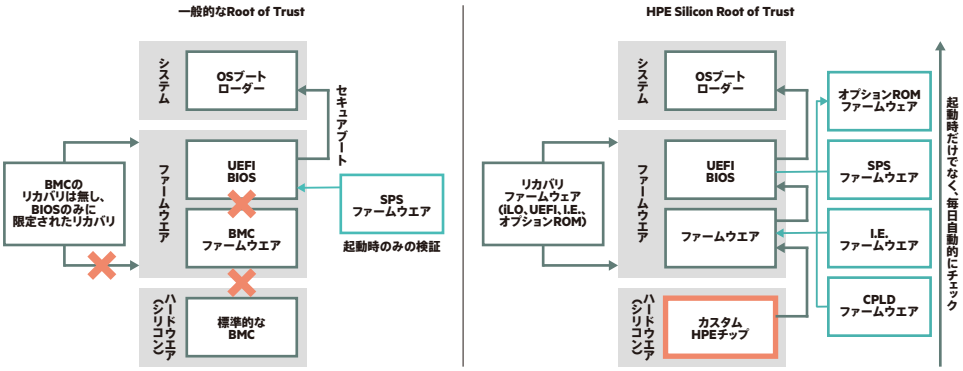

図1 ● シリコンレベルの信頼性

iLOが自律的にファームウエアの異変を検知する。起動時はもちろん、 稼働中にも定期的にチェックを行い、不審な点があれば自動で修復する

――稼働中もチェックが行われるのですね。万一、改ざんが認められた場合はどうなるのですか。

及川：iLOが改ざんや破壊を検知すると、改ざんされていない正当なファームウエアをロードして、自動で復旧します。管理者が手をかける必要はありません。

また、工場出荷後の移送中に物理的にマルウエアを仕込まれるのを防ぐ仕組みもあります。出荷後に何者かが筐体を開けると、電源を入れた際に警告メッセージが表示されるのです。意外に見落としがちですが、移送経路は忘れてはならない対策ポイントの1つだと考えています。

――世界中に拠点を持つ製造業などが、PCサーバーを移送する際も安心ですね。

及川：その通りです。さらに最新のiLOは、ハードウエアの稼働データをHPEのクラウドに送信する役割も果たします。データは、HPEのデータサイエンティストが分析し、最適なモデルにして提供します。当社は、かねて「HPE InfoSight」というAIによる自律運用の仕組みをストレージ製品向けに提供してきましたが、Gen10は、これをサーバー向けにした「HPE InfoSight for servers」に対応しています。

現在、世界中で、InfoSightに接続するサーバーから情報の収集・学習を開始しており、既にシステム情報、標準保証やサポート契約といった、サーバーシステムのヘルス状態やステータスを一元監視する「サーバーシステムの状態の可視化」までが可能となっています。今後、AI機能の学習成果に応じて、順次、パフォーマンスの最適化・問題の予測／防止に加え、セキュリティ対策の高度化も自動化できるようになっていく予定です（図2）。

特長1
クラウドベースのAI主導型運用。ストレージで2010年から開始、長年のサービス実績があり、運用工数とコスト削減が可能

特長2
全世界のHPE製品から実稼働データを収集。最新機種のみならず、iLO　5、iLO4を搭載したGen10、Gen9、Gen8世代のサーバーで使用可能

特長3
すでに「サーバーシステムの状態の可視化」を実現。AI機能による学習を経て、今後段階的に「予測・推奨」機能を強化

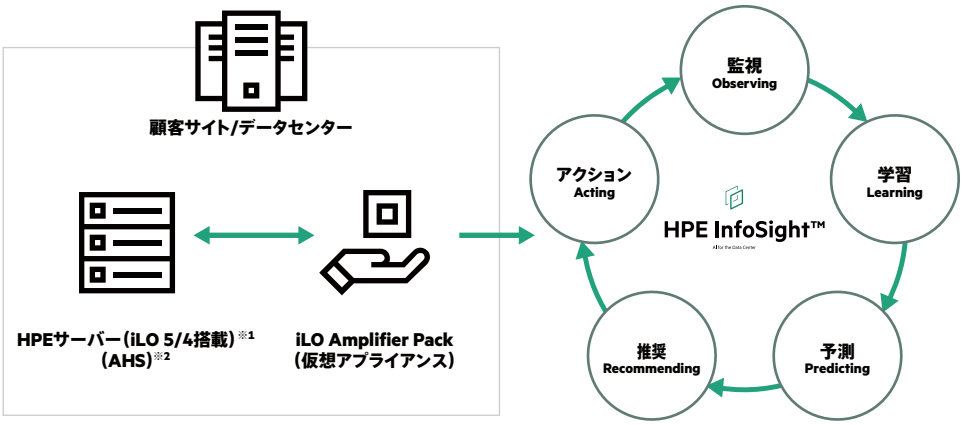

図2 ● HPE InfoSight for servers

HPEがストレージ領域で培ってきたAIによる運用自動化機能「HPE InfoSight」を サーバー向けに特化。Gen10が搭載するiLOはこれに対応している

※1 HPE ProLiantサーバー、HPE Synergyコンピュートモジュール、HPE Apollo（iLO 5、iLO 4を搭載したGen10、Gen9、Gen8）から開始
※2 Active Health System、サーバー上の数千のシステムパラメータおよび診断テレメトリを24時間365日記録し、診断に活用するツール

ビジネス競争力に直結するデータをGen10で安全に管理

――これらの特長を備えるGen10なら、人的リソースが限られる中堅・中小企業でも、ハードウエアレベルのセキュリティを確保しやすくなります。踏み台にされ、攻撃の起点となってしまうビジネスリスクも低減できそうですね。実際にユーザーの反応はいかがですか。

及川：既に複数のお客様に採用いただいています。例えば、年商約250億円のチルドデザートメーカー、モンテール様がその1社です。モンテール様にとって、デザートのレシピは競争力に直結する重要情報のため、社内サーバーで管理をされていました。サーバー選定ではセキュリティと信頼性が重視されましたが、ご紹介したような高度なセキュリティ性能がGen10採用の決め手になりました。

また、マンツーマン英会話教室を運営するGaba様も、Gen10を導入・活用しています。このお客様には、自律化による運用管理効率の良さを高くご評価いただいています。

――一方、サーバー領域で企業が直面するもう1つの課題に、Server OSのサポート終了があります。Windows Server 2008など、サポートが切れたOSを搭載したレガシーな機器を使っている企業はまだ多いようですが、そうした企業が、Gen10のような最新機種に、筐体ごとリプレースするのも手ですね。

及川：はい。ビジネスの安全を守る方法として、当社も強くお勧めしたいところです。

最新のセキュリティ対策は整備したいが、そのための要員を拡充することもままならない。そうした悩みを抱える中堅・中小企業にとって、Gen10は希望の光となる気がします。本日はありがとうございました。

CPUレベルで脆弱性対策を強化したインテル® Xeon® プロセッサー

HPE ProLiant Gen10にはもう1つ注目すべきポイントがある。それが、第2世代インテル® Xeon® スケーラブル・プロセッサーを搭載していることだ（※一部機種のみ）。

第2世代インテル® Xeon® スケーラブル・プロセッサーは、サイドチャネル攻撃対策や暗号化アクセラレーター、インテル・セキュリティ・ライブラリーなどのハードウエア支援型セキュリティ機能を実装。性能も高く、従来比で最大3.5倍のパフォーマンスを発揮し、AIのパフォーマンスを最大14倍に拡張できるIntel® Deep Learning Boostにも対応。Gen10を、セキュリティと性能の両面から支えている。

intel.co.jp/xeon

日本ヒューレット・パッカード株式会社
〒136-8711 東京都江東区大島2-2-1