プレスリリース: 2016年04月25日
トピック: ソフトウェア/ ITサービス

ヒューレット パッカード エンタープライズ、「Build it In（組込み）」と「Stop it Now（直ちに食い止める）」アプローチによりサイバー防御の変革をリード

- 新しいリファレンスアーキテクチャ、製品サービス、およびパートナーシップにより、エンタープライズITへのセキュリティの組込みと攻撃の阻止を実現 -

2016年4月25日

日本ヒューレット・パッカード株式会社

本リリースは、ヒューレット パッカード エンタープライズ（本社：米国カリフォルニア州パロアルト、以下：HPE）が、2016年3月1日（現地時間）に米国で発表した英文リリースに基づいて作成した日本語抄訳です。ここに紹介されているソフトウェア、ソリューションの日本語版の提供開始は未定です。

ヒューレット パッカード エンタープライズ（HPE）は、企業が自社のITに保護機能を組込み、包括的な検出と対応機能を通じて攻撃を食い止められるよう設計された、新たなセキュリティソリューションを発表しました。HPE Securityが発表した新しいサイバーリファレンスアーキテクチャ、モバイルセキュリティ関連ソリューション、およびパートナーエコシステムの強化により、企業によるセキュリティとリスク管理プロセスのIT運営への組み込みを支援し、今日の高度な攻撃に対処すると共に、明日のビジネスニーズに応える、より安全な環境を提供します。

IoT（Internet of Things）の登場に加え、デジタルおよびコンバージドシステムの急速な進展により、セキュリティ分野の専門家はイノベーションを妨げることなくビジネスクリティカルな資産に対するリスクを検出するという課題に直面しています。IDCによれば、IoT機器の検証とIoTに付随するリスク軽減のニーズに伴い、企業はインターネット接続機器から生成されるネットワークトラフィックに対する可視性を高める必要に迫られています。最新技術の導入時に企業がセキュリティと分析機能を組み込もうとするため、IDCはこれらが大きな成長要因となって、セキュリティ情報とイベント管理の市場が2014年の17億ドルから2019年には26億ドルにまで拡大すると予想しています（*1）。

HPEのHPE Security 製品担当シニアバイスプレジデント兼ジェネラルマネージャーのスー・バーサミアン（Sue Barsamian）は、次のように述べています。「ネットワーク防御と周辺部の制御を重視した従来の後付け型のエンタープライズセキュリティは、今日の急速に変化する脅威に対しては不十分です。企業はこれまで主に対象としてきた分野だけに留まらず、インフラからアプリケーションやデータまでITのあらゆる層にセキュリティを組み込むと共に、次世代のインテリジェンスベースのセキュリティ運用を推進する包括的な検出および応答機能を備えたリスクと回復力のロードマップを必要としています。」

〈サイバー回復力構築のための枠組みを提供〉
企業が急速に変化する脅威の中でのリスク管理を求められていることに伴い、HPEは今日の最も複雑な攻撃も食い止めるため、組織に回復力を組み込むため設計された包括的な情報セキュリティの枠組みである「HPE Cyber Reference Architecture（CRA）」を発表しました。この「HPE Cyber Reference Architecture」は12のドメイン、63のサブドメイン、および350種類を超えるセキュリティ機能から構成され、クラウド、モバイル、M2M（Machine-to-Machine）、およびIoT（Internet of Things）を含む、今日の複雑なセキュリティ課題に対応するソリューションを定義しています。

HPEのHPE Security サービス担当シニアバイスプレジデントのアート・ウォン（Art Wong）は、次のように述べています。「新たに登場した技術の成長と昨今の攻撃の高度化により、企業はイノベーションに遅れることなくリスクを特定し、それを管理するという課題に直面しています。HPE Cyber Reference Architectureはセキュリティを組み込み、攻撃をその途上で食い止めるために必要なコアとなるコンポーネントとイニシアティブに対応した350種類のセキュリティアーキテクチャの設計図を活用し、企業が回復力を獲得するためのフレームワークを提供します。」

〈セキュリティをモバイルに組み込む〉
HPEが発表した調査結果では、モバイルアプリが不安を覚えるほどの量のデータを利用者から収集しているにもかかわらず、機密情報を保護するために必要な手段を講じていないことが判明しました。この調査は「HPE Security Fortify on Demand」を使用して36,000を超えるiOSとAndroidのモバイルアプリをスキャンし、データ収集の拡大が与えるインパクトを明らかにすると共に、組織、モバイルアプリの開発者、および企業がセキュリティへのアプローチをどのように変革すればデータの保護を改善できるかについての推奨を行っています。

企業によるモバイルアプリへのデータセキュリティ組み込みを支援するため、HPEはモバイル環境で機密情報を保護するために設計された、エンドツーエンドのデータ暗号化ソリューションである「HPE SecureData Mobile」も発表しました。このソリューションを使って企業はデータセキュリティを自らのモバイルアプリに組み込み、静止時、移動時、利用時などデータをそのライフサイクル全体にわたって保護し、TLS、VPN、ストレージ暗号化などの従来の技術よりもはるかに広い範囲にセキュリティを拡大できるようになります。規格ベースの暗号化である「HPE Format-Preserving Encryption」を使用することにより、既存のアプリに最小限の修正を加えるだけでモバイルアプリやモバイル購入時のデータセキュリティを実現します。

〈「ArcSight」エコシステム拡大による検知と対応の強化〉
年率30%の成長を遂げている「HPE Security ArcSight Technology Alliances Partner（TAP）」プログラムに基づき、HPEはセキュリティ分野のリーダー企業によるコラボレーションを促進し、保護と対応能力を最大限に高める包括的な「Stop it Now」モデルを支えるための新しいArcSightベースのソリューションや戦略的パートナーシップを発表しました。

・「HPE Security ArcSight」とHPE Security Services：統合された防御
HPEは、「HPE Security ArcSight」をエンジンとして市場をリードしているSIEM（Security Information and Event Management）セキュリティ監視およびマネージドサービスなど、Threat Defense Servicesポートフォリオの継続的な進化を発表しました。このサービスポートフォリオの強化には、自動化されたセキュリティ警告サービス、セキュリティ調査と対応、攻撃者のプロファイリング、およびユーザーの行動とマルウェアの分析が含まれます。

・HPE と「Aruba ClearPass」：モバイルを安全に
「HPE Security ArcSight」と「Aruba ClearPass」との双方向の統合がさらに強化されました。リッチなイベント、ユーザー、および機器のコンテキストを「ClearPass」から獲得する「HPE Security ArcSight」の機能をベースとする、HPEの業界をリードするネットワークポリシー管理ソリューションである「ArcSight」を使い、セキュリティアナリストは悪意ある挙動を検出した際に「ClearPass」経由でネットワークからエンドポイントを隔離または除去できるようになりました。

・「HPE Security ArcSight」と vArmour：エンタープライズクラウドのセキュリティを確保
仮想化環境やクラウドのデータセンターでは、アプリケーションレイヤーでの行動の追跡および分析に、長年苦心してきました。vArmour DSSにより、「HPE Security ArcSight ESM」のユーザーはパブリッククラウドとプライベートクラウドの両クラウドにかかるすべてのワークロードについて、アプリケーションによる通信を把握できるようになりました。またvArmourのアプリケーションを認識したマイクロセグメンテーションを使い、「HPE Security ArcSight ESM」が検出したAPT攻撃にリアルタイムで対応し、攻撃を停止できるようになりました。

・「HPE Security ArcSight」とFortinet：機器の可視性を強化
「HPE Security Logger」とFortinet FortiGateを組み合わせることにより、ファイアウォールを超えて組織内のすべての機器について高度な可視性を確保する、拡張性に富んだソリューション連携が、セキュリティ分野の2社のリーダー企業から提供されます。このパートナーシップを通じて企業はセキュリティイベントのキャプチャ、保存および分析を行い、捜査やフォレンジック調査を高速化すると共にコンプライアンス上のニーズにも対応できるようになりました。

・「HPE Security ArcSight」とIT-ISAC：行動に移すことが可能なインテリジェンスを共有
コミュニティベースの、動的な脅威分析スコアリングを組み込んだセキュリティインテリジェンスプラットフォームである「HPE Threat Central」が、IT-ISACにより、メンバー間でインテリジェンスを共有するための主な脅威共有および分析プラットフォームに選ばれました。製品の種類を問わず、またSTIXやTAXIIなどの業界規格をサポートする「HPE Threat Central」は、機械と機械および人と人の両インターフェイスから派生した、意味のある、また行動に移すことが可能なインテリジェンスを提供します。

・「HPE Security ArcSight」と PwC: ネットワークの可視性を拡張
PwCのCyber Security & Privacyプラクティスにより、「HPE DNS Malware Analytics (DMA)」ソリューションが新たにSecurity Assessment Servicesポートフォリオに追加されしました。これによりPwCのクライアント企業におけるネットワークの可視性が高まり、マルウェア、ボット、あるいはその他の未知の脅威に感染したホストをさらに容易に検出および特定できるようになりました。

HPE Securityについて
HPE Securityは、企業がセキュリティを組織構造に組み入れ、高度な脅威を検出して対応し、継続性とコンプライアンスを保全してリスクを効果的に軽減することで、事業の根幹に関わるデジタル資産の保護をサポートします。市場をリードする製品、サービス、脅威対策、セキュリティ調査からなる総合的なパッケージを活用して、HPE Securityは企業が保護とイノベーションのバランスをとりながら今日のアイデアエコノミーに対応し続けることができるよう応援します。HPEセキュリティについての詳細は、https://www.hpe.com/us/en/solutions/protect-digital.html をご覧ください。

*1：IDC 「Worldwide Security and Vulnerability Management Forecast, 2015-2019」、Doc＃259615、2015年10月

■ プレスルーム
https://www.hpe.com/jp/ja/newsroom.html

＃ ＃ ＃

■ お客様からのお問い合わせ先
カスタマー・インフォメーションセンター
TEL：0120-268-186（携帯、PHS：03-5749-8279）
ホームページ：http://www.hpe.com/jp/