FORTINET

フォーティネットで クラウドのセキュリティを確保

アーキテクトがクラウドネイティブの セキュリティツールを強化すべき 5 つの主要領域

目次

FORTINET

概要

企業においては DevOps チームがクラウドへの移行を主導しますが、移行において十分なセキュリティを確保することの重要性が見落とされているケースが多く見受けられます。クラウドプラットフォームで提供されるセキュリティツールをそのまま使用する場合、データを盗んだり企業ネットワークの他の領域に侵入するために攻撃者が悪用できるセキュリティのギャップが残ってしまう可能性が高くなります。セキュリティアーキテクトがクラウド内のセキュリティを確立して管理する場合、確実に網羅すべきセキュリティ領域が少なくとも 5 つ挙げられています。

フォーティネットは、より広範なセキュリティアーキテクチャと統合できる重要なセキュリティレイヤーを提供します。これには、Web アプリケーションやアプリケーションプログラミングインタフェース（API）の保護に加え、クラウドプラットフォームのセキュリティ管理ソリューション、クラウドプラットフォーム向けに専用設計されたセキュリティのネイティブ統合などがあります。また、DevOps チームがクラウド環境におけるセキュリティタスクを自動化する際に役立つ統合機能も提供されます。これらはすべて、専任のセキュリティスタッフを採用したり、開発スタッフが新しいツールに関するトレーニングに時間を費やしたりすることなく、一貫したセキュリティ態勢や効果的なセキュリティライフサイクル管理の運営モデルを確立する上で有効です。

はじめに：クラウドプロバイダーのセキュリティツールでは不十分

DevOps チームはクラウドの導入の最前線に立っています。クラウドモデルは、DevOps チームの CI / CD（Continuous Integration：継続的インテグレーション / 継続的デリバリ）の原則に適するものでもあります。多くの組織では、開発チームがクラウドのパワーユーザーであり、クラウドインフラストラクチャ（コンピューティング、ストレージ、ネットワーク、およびその他のリソース）を必要に応じて導入する権限を有しています。しかしながら、開発者がそれらの権限を行使する際には、セキュリティチームがリスクを負うことになります。事実、セキュリティアーキテクトたちは DevOps のセキュリティを本年の最優先課題として挙げています [1]。

こういったリスクの中で最も重大なのは、構成ミスの悪用によるサイバー脅威です。クラウドベースの環境が攻撃を受けてしまった場合、その影響は企業全体に及ぶ可能性があり、企業の評判が損なわれるだけでなく、オペレーションが中断され貴重なビジネスデータが失われることになりかねません。

昨今のサイバー犯罪では、DevOps と同様に人工知能（AI）やスウォームテクノロジーなどの高度なテクノロジーを利用して [2]、特定の組織の複数の攻撃対象領域を標的とする専用のマルウェアが作成されます。

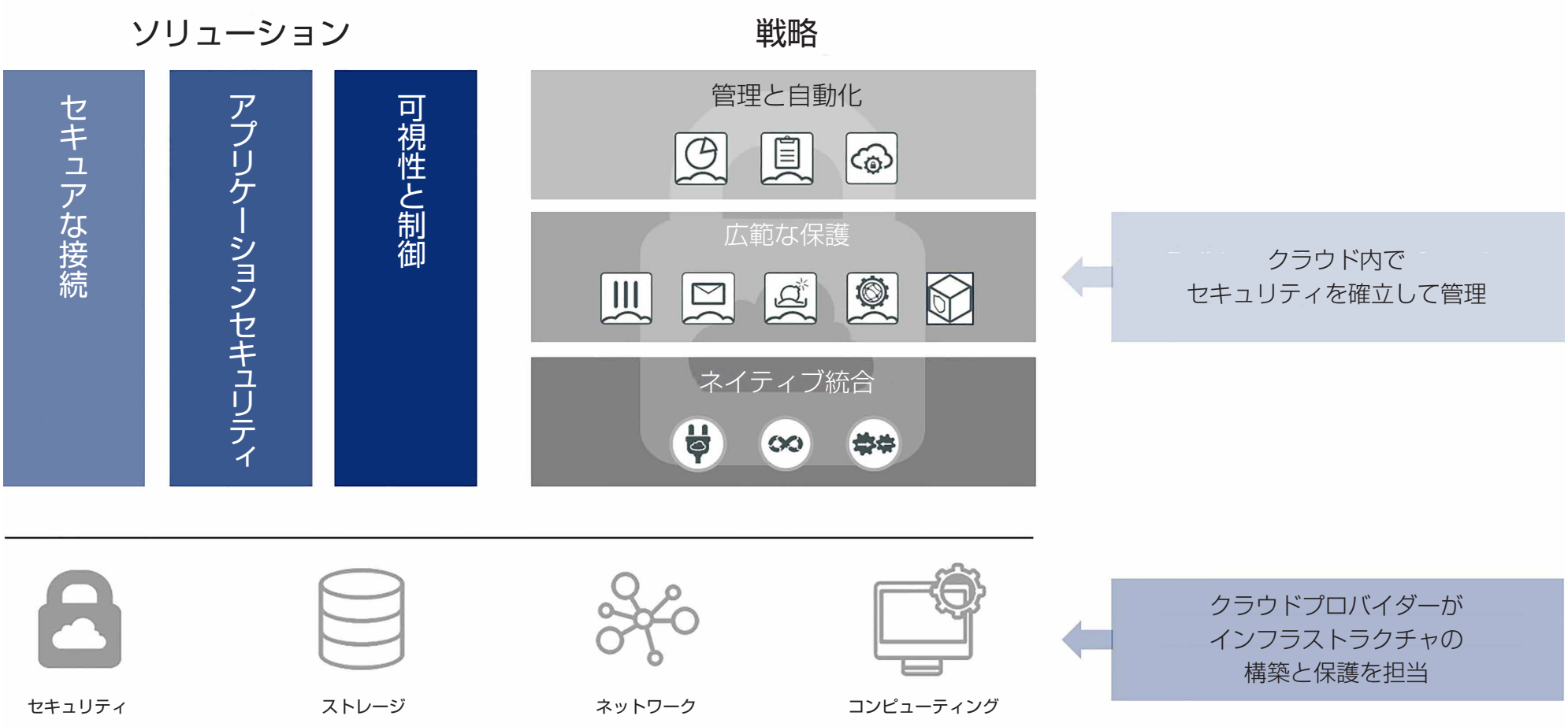

図 1：クラウドセキュリティソリューションは、セキュアな接続、アプリケーションセキュリティ、管理と自動化による包括的な可視化と制御、広範な保護、ネイティブ統合といった機能を提供する必要がある

構成の複雑化に伴うセキュリティリスクの増大

DevOps の責任者は、クラウド全体のセキュリティを確保する責任を負う場合があります。通常パブリッククラウドサービスには、クラウドを利用する顧客企業がサービスに対するアクセス権限を制御する際に有効となる、セキュリティグループやアクセス制御リスト（ACL）などのセキュリティ機能が含まれます。また顧客企業は、分散型の次世代ファイアウォール（NGFW）、Web アプリケーションファイアウォール（WAF）、サンドボックスソリューション、クラウドセキュリティ態勢管理、ワークロード保護ソリューションなど、サードパーティ製の各種クラウドベースツールを利用することもできます。あまりにも多数のオプションとベンダーが存在しているため、多忙な DevOps チームはまず特定のクラウド環境で提供されている基本的なセキュリティツールを活用することにして、見つかったギャップを解消するために必要に応じて単機能のセキュリティツールを追加するケースが多く見受けられます。

DevOps のセキュリティリスクを軽減する役割を担うセキュリティアーキテクトにとって、このような状況はさまざまな理由から問題になります。第一に、基本的なクラウドツールに多数の構成オプションが含まれていても、DevOps チームには、利用可能なありとあらゆるセキュリティサービスに固有の構成を実装するために必要な専門知識がないことが挙げられます。この場合、内蔵のセキュリティツールをデフォルト構成に戻してしまうケースが頻繁に発生し、リスクが高まることになります。

不慣れなクラウトセキュリティユーザーを支援し、効果的なセキュリティ態勢を確保するため、DevOps チームは事前設定された構成サービスが含まれている「万能」な構成テンプレートを開発するケースが多くあります。残念ながら、そのような構成テンプレートにはコーディングエラーが含まれる傾向があり、古くなる可能性もあります。さらに、エラーによってもたらされるリスクは、このテンプレートが利用されるたびに増大します。容易に予測できるように、クラウドの構成ミスによるデータ侵害は前年比で 424% と急増しており、すべてのクラウドデータ侵害の 70% を占めています [3]。

クラウドの構成ミスによるデータ侵害は前年比で 424% と急増しており、すべてのクラウドデータ侵害の 70% を占めています [4]。

ソリューション：一貫性を備えたセキュリティレイヤーの追加

セキュリティチームに過度の負担をかけずにクラウドセキュリティのギャップによるリスクを最小限に抑えるため、セキュリティアーキテクトは広範で一元管理に対応する企業組織のセキュリティアーキテクチャにフォーティネットのクラウドセキュリティソリューションを統合し、さらに堅牢な保護機能を活用することができます。特に、フォーティネットの動的なクラウドセキュリティソリューションは、企業の知的財産やコンプライアンスを損なうことなく、俊敏性および顧客中心という競争優位性を DevOps に求めている組織に不可欠な、脅威保護の主要な 4 つの領域分野をカバーしています。

1. クラウドプラットフォームのセキュリティ

クラウドにおける DevOps 環境は急速に変化しており、組織は複数のクラウドプロバイダーが相互の調整や連携なしに行うこのような変更への対応に苦慮しています。セキュリティアーキテクトは、DevOps 担当者および CISO に対し、一元的な可視化、およびクラウドインフラストラクチャ全体の構成の状態とセキュリティ態勢を監視する、制御システムを提供する必要があります。

FortiCWP のクラウドワークロード保護（CWP）を利用することで、セキュリティチームと DevOps チームはクラウド環境のセキュリティ態勢を継続的に監視することができます。これにより、セキュリティ設定の構成ミスが引き起こす潜在的な脅威を検知すると同時に、クラウドインフラストラクチャ内の不審な活動の特定、クラウドリソースに行き来するトラフィックの分析、クラウド内に悪意あるデータや機密データが含まれていないかどうかの検査を実行することができます。

DevOps 責任者が必要としているのは、クラウドインフラストラクチャの構成状態と態勢の一元的な可視化と自動監視ソリューションです。

FortiCWP は、継続的に構成評価を実行してリスクスコアを生成し、それを改善するベストプラクティスとなる推奨事項を提供します。さらに構成を継続的に監視し、問題にフラグを設定して適時に解決されるようにします。またセキュリティアーキテクトは、FortiCWP の分析ツールを利用して DevOps 責任者がマルチクラウド環境全体にわたって構成変更のライフサイクルを把握できるように支援可能になります。

2. クラウドプラットフォームへの FortiGate ファイアウォールのネイティブ統合

クラウド内でのオペレーションを保護する方法を検討する場合、セキュリティアーキテクトは企業全体レベルでセキュリティの把握が可能なキテクチャを設計する必要があります。これは、FortiGate VM を仮想化（パブリックおよびプライベートクラウド）環境に、そして FortiGate アプライアンスを物理ドメインに配備することで実現できます。

仮想 / 物理両方の FortiGate ファイアウォールでは、組織で利用されている他のすべてのフォーティネット セキュリティ ファブリックのコンポーネントと同じく、タグとアノテーションのメタデータに基づいて論理情報の分類を使用します。これにより、セキュリティチームは動的なマルチクラウドインフラストラクチャ全体で一貫した運用モデルとセキュリティ態勢を維持できるようになります。その結果、対応可能なスタッフの有無を問わず、インフラストラクチャ全体で脅威への迅速なレスポンスが可能となり、多くの場合自動化が実現します。

競争が激しいビジネスアプリケーション環境の急速な進歩に対応するため、フォーティネットのクラウドセキュリティソリューションは、オートスケーリング、高速なネットワーキング機能を装備する高性能フォームファクター、クラウドの高可用性（HA）スキーマ、クラウド構成テンプレートなどの各種クラウドサービスとネイティブ統合することができます。このような統合の結果、クラウドのセキュリティをクラウドインフラストラクチャの動的な性質に一層適応させることができます。

セキュリティアーキテクトは、スタッフの限られたセキュリティスキルで高度な脅威保護を維持するという課題に迫られています。FortiGate とクラウドインフラストラクチャのネイティブ統合は、そのような負担を軽減します。

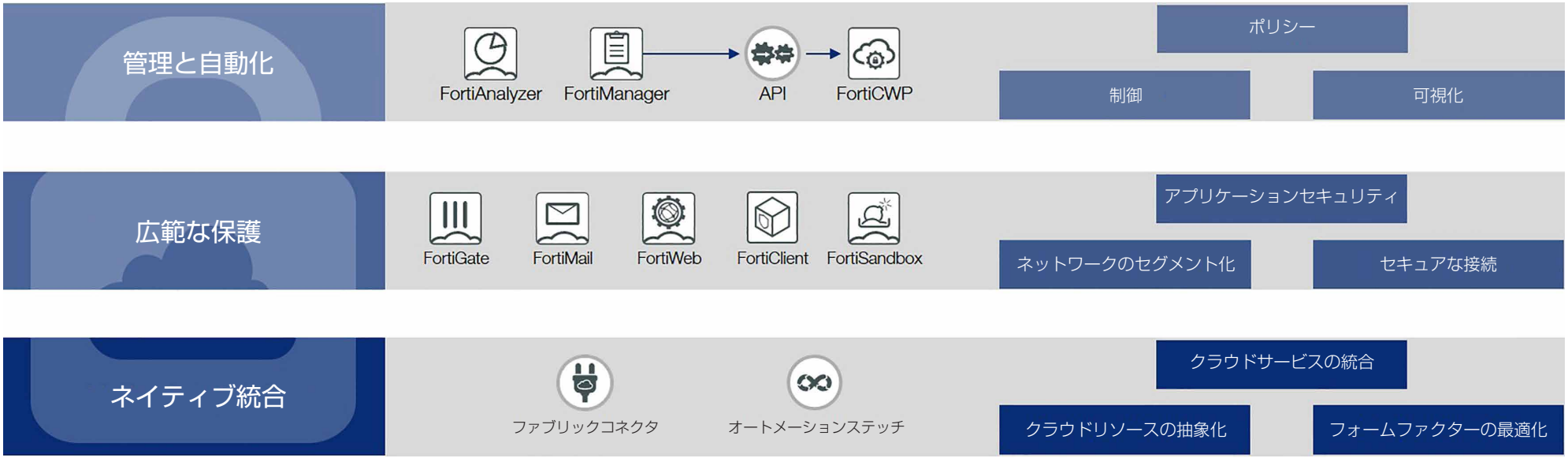

図 2：フォーティネットは、包括的なクラウドセキュリティ戦略と同時に、管理と自動化、広範な保護、ネイティブ統合を実現する、対象をしぼり込んだ統合ソリューションを提供

3. Web アプリケーションと API の保護

多くの企業では、共同責任モデルに関する理解が不足しているためクラウド環境が十分に保護されていません。クラウドプロバイダーは、クライアントサービスの基盤となるハードウェアとソフトウェアを含むインフラストラクチャを保護する責任を負っており、一般的にシステムの安全を維持するという点で十分な役割を果たしています。一方、クラウドを利用する顧客企業は、自らがクラウド内で展開するアプリケーションおよび保存データを保護することに関して、全面的な責任を負います。このような切り分けは、今後数年間のうちに拡大すると予測されており、ユーザー企業が共同保護契約における担当責務を効果的に順守できないことが原因で発生するクラウドのセキュリティ侵害が、2023 年までには全体の 99% を占めるようになると予想されています [5]。

特定の IP アドレスへのアクセスを制御することで保護できるオンプレミスアプリケーションとは異なり、Web 上のアプリケーショントラフィック（今やすべてのクラウドベースのトラフィックは Web 上を行き来します）にはそのようなセキュリティの「要所」がありません。クラウドでは、トラフィックフローが経由するポートからアプリケーションコンテンツやトラフィック自体のコンテキストへと、脅威検知のポイントをシフトさせる必要があります。

より詳細なこのレベルの分析情報を入手するには、Web アプリケーションのセキュリティポリシーに対する継続的できめ細かな調整が重要です。これは手作業で持続できるタスクではなく、実際のところ大規模環境での対応は不可能です。そのため、セキュリティアーキテクトには FortiWeb による AI（人工知能）ドリブンのアプローチが必要になります。**FortiWeb** は、多くの WAF が備えているシグネチャパターンによるマッチングに加え、デュアルレイヤーの機械学習（ML）エンジンを使用して Web アプリケーションをゼロデイ攻撃から保護します。ML が実現する機能を活用することで、ユーザーまたはアプリケーションの異常な振る舞いをこれまでにない精度で検知し、進化するボットネットを阻止できるようになり、環境の規模拡大にも容易に対応可能となります。

さらに、FortiWeb は脆弱性の悪用やボット、マルウェアによる既知 / 未知両方の攻撃だけでなく、OWASP（Open Web Application Security Project）のトップ 10 の脅威から Web アプリケーションを効果的に保護します。

アプリケーションからミドルウェア、そしてモバイルアプリケーションのバックエンドに至るまで、すべてが Web に接続されるようになったことで、Web 層での脅威保護の重要性が高まっています。しかしながら、保護機能を実装する際に選択されるアプローチはさまざまです。複数のアプリケーションを保護するために VM の実行が必要な場合もあれば、Web AppSec（アプリケーションセキュリティ）コンテナをマイクロサービスとして各アプリケーションに付加するコンテナアプローチが選択される場合もあります。その他にも、基盤となるインフラストラクチャの管理が不要で Web アプリケーションの包括的なセキュリティニーズに対応可能な、SaaS（Software-as-a-Service）型のソリューションが好まれる場合もあります。FortiWeb は、これらすべての運用要件に適応するさまざまなフォームファクターで提供されているため、セキュリティアーキテクトは柔軟な導入展開が可能です。

4. セキュリティ機能の自動化

DevOps は IT 部門のひとつですが、セキュリティに関してはスキル開発の面で大きなギャップがあることが複数の調査結果から判明しています。たとえば、コーディングのセキュリティについて指導を受けたことがある開発者は全体の 42% にとどまり、運用スタッフの 57% はセキュリティのベストプラクティスを実行していません[6]。DevOps チームのセキュリティスキル不足を補ったり、DevOps 専属のセキュリティ管理者の採用を回避したりするため、セキュリティアーキテクトは DevOps チームが可能な限りセキュリティオペレーションを自動化する手段を検討しなければなりません。

クラウドでは、脅威検知の焦点をネットワークコンテキストから
アプリケーションコンテキストにシフトさせる必要があります。

フォーティネット セキュリティ ファブリックは、クラウドプラットフォームからのオブジェクトを可視化するプラグイン（**ファブリックコネクタ**と呼ばれるもの）を介して、このような自動化を促進します。これにより、DevOps およびセキュリティのチームは、アプリケーション属性が変更される毎にセキュリティポリシーを更新することなく、アプリケーション変更への迅速な対応が可能になります。

ファブリックコネクタの他にも、セキュリティチームは FortiOS の API を活用するセキュリティオペレーションの自動化が可能です。また、Terraform や Ansible などのオートメーションフレームワーク経由で FortiOS の構成スクリプトをダウンロードすることもできます。

Terraform は、IT ライフサイクルのオートメーションを実現するプラットフォームとして、最も広く採用されています。新しい Terraform FortiOS Provider Module を利用することで、物理 / 仮想両方の FortiGate デバイスにおける FortiOS 関連のオペレーションがすべて自動化されるようになります。この結果、開発者は FortiGate Terraform の構成を他のアプリケーションエレメントと統合し、セキュアなポータブルアプリケーションスタックを瞬時に稼働できるようになります。

Red Hat Ansible は、FortiGate VM の構成を自動化します。FortiOS 用の Ansible モジュールは GitHub で利用できるため、開発者は既存のスキルを有効活用して FortiGate の構成タスクすべてを Ansible Tower 環境内で完了させることができます。これにより、開発者向けトレーニングの負荷を大幅に軽減できます。

自動化に利用できるその他のリソースとして、Fortinet Developer Network（FNDN）があります。FNDN では、FortiOS の RESTful API を利用してフォーティネットの機能を直接自動化する方法を解説するドキュメントやチュートリアルを提供しています。

70%

の組織が、コードの作成と管理を自動化しています[7]。FortiOSは、自動化を念頭にゼロから徹底的な開発が行われています。

終わりに：クラウドネイティブツールにはフォーティネットのセキュリティの追加が不可欠で、その実現も容易

パブリッククラウドサービスで標準装備されるセキュリティツールは、動的なマルチクラウド環境の保護に関しては不十分です。構成ミスを防ぐことができず、それに伴うセキュリティギャップによって組織全体に損害がもたらされる可能性があります。それらのリスクは完全に目に見えるものではなく、ソフトウェア開発の初期段階で実感できるものでもないため、セキュリティアーキテクトはその存在を認識するまで放置しておくことはできません。

フォーティネットのソリューションによってクラウドネイティブのセキュリティを強化することで、セキュリティアーキテクトはセキュリティ管理の負担を軽減すると同時に、クラウドセキュリティのギャップを解消できるようになります。フォーティネット セキュリティファブリックの幅広い高度なセキュリティテクノロジー、シームレスに統合された機能、そして AI ドリブンの優れた能力が、企業のセキュリティ戦略を補完し、さらに強化します。

[1] 「The Security Architect and Cybersecurity: A Report on Current Priorities and Challenges」、フォーティネット、2019 年 6 月 29 日（英語）：https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report-security-architect-and-cybersecurity.pdf

[2] 「2019 State of DevOps Security Report」、フォーティネット、2019 年 5 月 10 日（英語）：https://www.fortinet.com/resources/resources-campaign.html?utm_source=social&utm_medium=blog&campaign=power-of&utm_term=devops#ufh-i-503777615-2019-state-of-devops-security-report

[3] 「Breached Records Fall 25% as Cloud Misconfigurations Soar」、Phil Muncaster 著、Infosecurity、2018 年 4 月 6 日（英語）：https://www.infosecurity-magazine.com/news/breached-records-fall-25/

[4] 同上

[5] 「Key Principles and Strategies for Securing the Enterprise Cloud」、フォーティネット、2018 年 12 月 3 日（英語）：https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-key-principles-and-strategies-for-securing-the-enterprise-cloud.pdf

[6] 「5 Reasons DevOps And Security Need To Work Together」、Daniel Newman 著、Forbes、2018 年 9 月 30 日（英語）：https://www.forbes.com/sites/danielnewman/2018/09/30/5-reasons-devops-and-security-need-to-work-together/

[7] 「Most organizations are not fully embracing DevOps」、Ian Barker 著、BetaNews、2018 年 6 月 14 日（英語）：https://betanews.com/2018/06/14/organizations-not-embracing-devops/

FORTINET

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

EB-Securing-the-Cloud-with-Fortinet-202001-R1