FORTINET

WHITE PAPER

金融機関 / 金融サービス向け サイバーセキュリティソリューション

高度な脅威からサービスを保護するとともに、コストと効率の最適化を実現

概要

金融機関および金融サービス提供会社（以降金融機関）は、ほぼ恒常的に攻撃や不正侵入の標的となっています。これらの機関のサイバーセキュリティチームでは、高い競争力を維持するためにコストの削減や運用の効率化、そしてコンプライアンスレポートの作成が求められており、その実現には可視化が不可欠です。フォーティネットの金融サービス向けサイバーセキュリティソリューションは、包括的な保護機能を提供してさまざまなユースケースに対応します。FortiGate 次世代ファイアウォールのパフォーマンスは、電子取引インフラストラクチャの特殊なニーズにも対応が可能です。フォーティネット セキュリティ ファブリックは、組織全体を網羅する多層型防御の状況を一元的に可視化し、ポリシーを一元制御する機能を提供します。フォーティネットはさらに、スケーラブルかつ高性能のセキュアネットワーキングソリューションを提供し、支社のネットワーク接続環境も支援します。

「オンラインバンキングサービスを専門に狙うサイバー攻撃への対策コストとして、金融機関は平均 180 万ドルを支出しています [5]」

あるレポートでは、金融サービスはサイバー攻撃者にとって価値の高い標的であり、世界中で最も多くの攻撃を受けている分野だとされています [1]。継続的な侵入の試行やその他の攻撃の標的になる金融機関の多くが、リアクティブ型からプロアクティブ型のサイバーセキュリティへの移行の困難さという問題に直面しています。この目標達成は、攻撃対象領域の継続的な拡大によって複雑化が進んでいますが [2]、その要因としてデジタルイノベーションのイニシアチブから生まれた新しいテクノロジーの採用が挙げられます [3]。このような複雑さに加えて、次々と制定される金融データや個人データの使用に関連する法規制へのコンプライアンスも義務付けられています [4]。

ビジネスとコンプライアンスの両方の理由から、機密性が極めて高いデータの保護に最優先で取り組む必要がある一方で、オンラインバンキングやモバイルバンキング、そして高頻度取引に至るまで、個人や企業を対象とするあらゆる商品にリアルタイムアクセスが要求されるようになっていることから、セキュリティによってネットワークパフォーマンスが損なわれることも許されません。また、競争が激しい業界で高い競争力を維持するには、コスト管理を徹底し、運用効率を最適化する必要もあります。

金融サービスのサイバーセキュリティの主な課題

コスト削減

金融機関は、IT 環境のコストの抑制と削減というプレッシャーに常にさらされています。サイバーセキュリティ予算は、財政的リソースと人的リソースに対して戦略的に配分する必要がありますが、コストも作業時間も無限ではないことから、リスクへの耐性とセキュリティ態勢のトレードオフを考慮し、適切なバランスを判断しなければなりません。これらの課題に加え、サイバーセキュリティの人員不足も深刻な問題であり [6]、特定の能力を持つ人材を見つけるのは難しく、見つかった場合も多額の費用が必要です。

可視化

攻撃対象範囲の継続的な拡大が、保護をますます困難にしています。IoT（Internet of Things）デバイスの急増、ビジネスサービスにおけるマルチクラウドの採用、顧客や従業員によるモバイルデバイスの利用によって、攻撃対象領域が急速に拡大しています。その結果、金融機関は単機能のセキュリティ製品を次々と追加導入し、拡大する攻撃対象領域によって生じたギャップを解消しようとしています。結果として生じるセキュリティのサイロ化によって可視性が損なわれ、運用効率が低下すると同時にリスクが増大します。

運用の効率化

セキュリティ要素の統合が不十分で、アーキテクチャが断片化している状態では、運用の効率性が大きく損なわれます。統合されていない環境では多くのセキュリティワークフローを手作業で管理する必要があるため、対応が遅れミスが発生する可能性も高まります。アーキテクチャのサイロは、脅威の検知、保護、レスポンスを遅らせるだけでなく、対応業務の重複を作り出し、運用コストを増加させ、結果としてセキュリティホールが生じる可能性もあります。

柔軟性

金融機関におけるクラウドアプリケーションやインフラストラクチャの採用増加に伴い、セキュリティアーキテクチャにはスピード、セキュリティ、コンプライアンス、さらにはパブリック / プライベート / ハイブリッドのクラウドベースのサービスと同時に従来型のオンプレミスサービスの保護も可能にする、高い俊敏性が求められるようになりました。

コンプライアンスレポート

金融サービスは世界で最も規制の厳しい分野の 1 つであり、キャンパスからデータセンター、エッジ、クラウドまでのネットワークのあらゆる場所に個人や企業の金融データが存在します。この分野の組織は、戦略的イニシアチブに携わる人材に手作業で監査レポートを準備させることなく、複数の法規制や標準へのコンプライアンスを実証できるようにしておく必要があります。

「金融機関が 2018 年に FCA（金融行為監督機構）に報告したサイバーインシデントは 819 件に上り、2017 年の 69 件から 1,000% 以上も増加しています [7]」

ユースケース

電子取引インフラストラクチャのサイバーセキュリティ

電子取引は金融サービスの専門分野の 1 つであり、そのインフラストラクチャは極めて高いパフォーマンスが保証されるものでなければなりません。具体的には、電子取引プラットフォームおよび他の金融機関、顧客にリアルタイムの情報を提供するシステム等との間のトラフィックを保護するファイアウォールなどが挙げられます。取引開始後の最初の数秒間に不正確な情報が金融機関側に送信されたり、情報に遅延が発生したりすると、顧客満足度が低下します。多くの場合、これらの問題を追跡するとデータの小さいパケットがファイアウォールを順不同で通過する、「ジッター」と呼ばれる現象にたどり着きます。

世界最大手の 2 つの銀行で実施したテストでは [8]、**FortiGate 次世代ファイアウォール**で発生する遅延は業界で最も低く、ジッターもほぼゼロであることが確認されました。それと同時に、電子取引インフラストラクチャと企業システムの間を移動するトラフィックに対して、高度な拡張性を備えた保護を提供します。内蔵の侵入防止システム（IPS）、ゼロトラストアクセスによるインテント ベースド セグメンテーション、モバイルセキュリティの機能を備えているため、個別の単機能製品を購入する必要がなくなります。一元的な可視化によって運用効率が向上するとともに、API（アプリケーションプログラミングインタフェース）が実現する自動化を通じて、電子取引に固有のニーズに応えるポリシーとワークフローのカスタマイズが容易になります。

これらのサイバーセキュリティ機能は、次のようなビジネス要件の達成を支援します。

- パフォーマンス指標で妥協することなく、パートナー間のトラフィックインスペクションに関する政府の法規制を遵守
- 顧客やビジネスの重要なデータをセグメント化し、セキュリティ効果を向上
- 可視性を高め、自動化の推進および管理の簡素化を実現

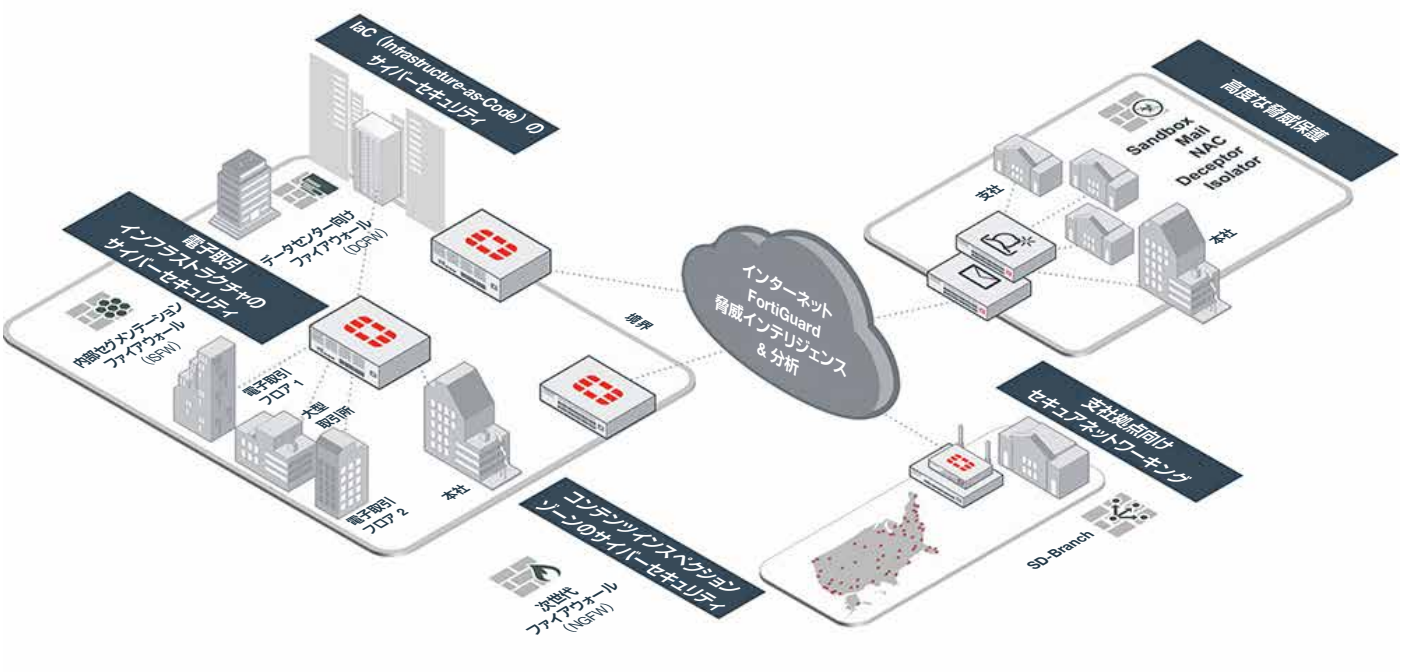
IaC（Infrastructure-as-Code）のサイバーセキュリティ

IaC（Infrastructure-as-Code）モデルを採用し、自動化プラットフォームを活用してインフラストラクチャの導入を進める企業は、無駄のない自動プロビジョニングモデルの確立による大きなメリットを享受できます。DevOps サイクルのサポートで採用されることが多い IaC は、組織のインフラストラクチャの迅速かつ容易な変更を可能にしますが [9]、運用の大幅な効率化が実現する一方で、企業組織は未知の潜在的な脆弱性にさらされることにもなります [10]。

セキュア IaC インフラストラクチャを提供する最良の方法は、DevOps アプリケーションの基礎となる構造に対して SaC（Security-as-Code）のアプローチを採用し、意図的にセキュリティを組み込むことです。**FortiGate 内部セグメンテーションファイアウォール**（ISFW）は、インテント ベースド セグメンテーションを活用し、ビジネスの目的に基づくインフラストラクチャのインテリジェントなセグメンテーション、適応型プロセス制御の適用、そして IaC 環境に対する脅威保護の自動化を実現します。**FortiManager** と **FortiAnalyzer** は、ネットワークとセキュリティの一元管理、ログの相関付け、分析の各機能を提供し、単一コンソールから高性能で堅牢なセキュリティを実現します。フォーティネットのオープンエコシステムは、ファブリックコネクタおよび堅牢な REST API（Representational State Transfer Application Programming Interface）を介して、サードパーティの自動化プラットフォームとのシームレスで緊密な統合を可能にします。

フォーティネットの SaC（Security-as-Code）ソリューションは、次のような優れた機能で IaC インフラストラクチャを保護します。

- 時間が重視されるクリティカルネットワークトラフィックを、パフォーマンスを犠牲にすることなく保護
- ビジネスの目的に基づいてネットワークトラフィックをセグメント化し、コンプライアンスの強化およびセキュリティ侵害からの保護を実現



フォーティネットの金融サービス向けサイバーセキュリティソリューションは、幅広い適用領域で（Broad）システム連携し（Integrated）、自動化された（Automated）アプローチをセキュリティに採用し、電子取引フロアから支社オフィスに至る攻撃対象領域全体を保護します。

コンテンツインスペクションゾーンのサイバーセキュリティ

組織のインフラストラクチャが社内のデータセンターインフラストラクチャにすべて置かれていた時代は過ぎ去りました。最近のある調査では、85% の企業がパブリックやプライベートの複数のクラウドを運用していることが明らかになりました [11]。SD-WAN（ソフトウェア制御によるワイドネットワーク）テクノロジーによって、組織のネットワークトラフィックは常に公共インターネット経由で移動するようになっており [12]、IoT デバイスがエッジに配置されるケースが急増しています [13]。

このような状況では、金融機関にとって境界ベースのサイバーセキュリティはもはや有効なアプローチではなくなっています。コンテンツインスペクションゾーンという観点から考えると、ネットワークトラフィックが企業のデータセンター、複数のクラウド、IoT デバイス、公共インターネットを移動する仮想境界がより有効なアプローチと言えます。

FortiGate 次世代ファイアウォール（NGFW）は、専用のセキュリティプロセッサと FortiGuard Labs の包括的な脅威インテリジェンスを活用することで、平文および暗号化されたトラフィックに対してトップクラスの優れたパフォーマンスのインスペクションが実現します。また、オンプレミスとクラウドベースの両方の環境の可視化と制御を一元化することで、運用の効率化とセキュリティの強化が可能になります。さらに、**フォーティネット セキュリティ ファブリック**では、ファブリックコネクタやオープン API を利用してフォーティネットやサードパーティの多様なセキュリティツールをエンドツーエンドで統合できます。人工知能（AI）を活用した堅牢な脅威インテリジェンスに基づくセキュリティアーキテクチャが、リアルタイムの攻撃の検知とレスポンスを可能にします。

フォーティネットが提供するエンドツーエンドの統合セキュリティアーキテクチャは、次のような多くのメリットを提供します。

- **運用の効率化：**手作業のセキュリティプロセスを排除
- **コスト削減：**サイバーセキュリティを統合し、ライセンスの重複を排除
- **コンプライアンスレポート作成の簡素化：**手作業に頼る監査準備のアプローチを回避
- **セキュリティの強化：**自動応答ワークフローとリアルタイムの脅威インテリジェンスを活用

支社 / 拠点向けセキュアネットワーキング

離れた場所にあるクラウド / データセンターとの間のネットワークトラフィックが増加する状況においても、支社と本社の間で許容できるレベルのネットワークパフォーマンスを維持しようとすると、コストの増加という問題に直面することになります。MPLS（マルチプロトコルラベルスイッチング）の帯域幅を追加購入する場合は、多くのコストと時間が必要であるだけでなく、ネットワークの将来のニーズに合わせて拡張することができません[14]。さらに、リモートの支社とそこに置かれたエッジデバイス[15]が、簡単に侵入できる標的としてサイバー犯罪者に狙われることにもなります。

FortiGate セキュア SD-WAN は、インターネットを含む支社と本社の間の複数の接続回線を行き来するネットワークトラフィックの保護を可能にします。インスペクションを実行するためにすべてのトラフィックをデータセンターにルーティングする必要がなくなるため、遅延の原因となるこのボトルネックを回避できます。また、支社と本社を接続するネットワークインフラストラクチャの拡張が可能となり、将来の帯域幅への投資を不要にします。

金融機関のリモート環境においては、**フォーティネットセキュア SD-Branch** によって支社のネットワークとセキュリティを統合し、単一の FortiGate NGFW ですべてを管理できるようになります。**FortiSwitch LAN** スイッチ、**FortiAP** 無線アクセスポイント、**FortiExtender** LTE WAN エクステンダーで構成されるこのソリューションによって、支社においても安全かつ高性能のネットワーキングが確保されます。**FortiNAC** ネットワークアクセスコントロール（NAC）ソリューションは、ネットワークエッジで検知されるすべての IoT デバイスの完全な可視化と制御を実現します。

FortiGate セキュア SD-WAN とフォーティネット SD-Branch は、次のような機能によって、支社ネットワークのセキュリティの強化とネットワークパフォーマンスの向上を実現します。

- **セキュリティ ドリブン ネットワーキングの実現：**攻撃者が支社からネットワークに不正侵入することを困難にする
- **運用効率を向上：**ネットワーキングとセキュリティを製品に統合し、単一デバイスによる一元管理を可能にする

高度な脅威保護

攻撃の件数が増加し[18]、高速化[19]や巧妙化[20]も進むに伴って、金融機関は攻撃対象の上位に挙げられています[21]。手作業によるレスポンスで侵入する脅威に対抗しようするセキュリティチームは膨大な数のアラートに悩まされ、マシンスピードで活動する高度な脅威を阻止できません。さらに、金融サービスデータの価値が攻撃者にとって上昇している中で、意図的あるいは偶発的のどちらであるかを問わず、内部関係者による脅威が金融サービス分野のリスクをさらに増大させています[22]。

これらの脅威に対抗するには、2 本の柱によるアプローチでマルウェアとそれを作成した攻撃者の両方から防御する方法が最も有効です。**攻撃ベースの防御**の基盤となるのが、堅牢なリアルタイムの脅威インテリジェンスです。フォーティネット セキュリティ ファブリックのすべてのツールは、世界最大のインテリジェンスネットワークの 1 つである **FortiGuard Labs** が提供する、AI を活用した包括的脅威インテリジェンスを利用しています。ポリモーフィズムなどの高度なテクノロジーを利用する攻撃が増えている現状でも[23]、AI と機械学習（ML）の採用によって未知あるいはゼロデイの攻撃の特定が容易になります。

FortiSandbox は、ゼロデイ脅威に対する防御に新たなレイヤーを追加します。未知のファイルを安全な場所で検証した後、ネットワークへの転送が許可されます。マルウェアの 60% が暗号化されるようになりましたが[25]、**FortiGate NGFW** の SSL/TLS（セキュアソケットレイヤー / トランスポートレイヤーセキュリティ）インスペクション機能であれば、パフォーマンスを低下させることなく暗号化されたトラフィックのインスペクションが実行できます。

金融機関が経験した不正侵入[16]
（過去 12 ヵ月間）

- マルウェア：49%
- スパイウェア：37%
- 内部関係者による脅威：35%
- DDoS：31%
- モバイル：29%
- フィッシング：24%
- ランサムウェア：16%
- SQL インジェクション：13%
- ゼロデイ攻撃：12%
- 中間者攻撃：11%

金融サービスにおける侵入の影響[17]
（過去 12 ヵ月間）

- 40%：生産性に影響する運用停止が発生した
- 40%：ブランドの信用低下につながるブリーチが発生した
- 34%：売上に影響する運用停止が発生した
- 32%：従業員の生産性に影響する運用停止が発生した
- 32%：重要なビジネスデータを失った

「先進的な企業は、魅力的でパーソナライズされたカスタマーエクスペリエンスを提供すると同時に、データに基づく柔軟で拡張性あるサイバーセキュリティを構築して金融サービスを運用しています[24]」

攻撃者ベースの防御は、社内あるいは社外のどちらか、また悪意があるかどうかを問わず、ネットワークに不正侵入しようとする人物を特定し、無害化するツールを提供します。**FortiDeceptor**は、攻撃者を誘導して特定することで実害の発生を防ぎます。**FortiInsight**は、ユーザーとエンドポイントを継続的に監視して、セキュリティ侵害の可能性があるコンプライアンスに違反した / 疑わしい / 異常な振る舞いを特定し、内部関係者による脅威から企業組織を保護します。

この 2 本の柱によるアプローチを採用することで次のような脅威対策が実現し、今日の高度な脅威環境に対処することが可能になります。

- **多層型防御を確立：**ゼロデイ脅威を検知
- **攻撃中の犯罪者を捕捉：**技術レベルを照合して攻撃者を識別し、その攻撃者によるキャンペーンを阻止

「顧客は、本当に信頼できる企業であればデータを共有しても構わないと考える傾向にあります。このため、セキュリティ対策が失敗した場合には、企業ブランドの評判、顧客からの信頼、さらには売上まで低下する危険性があります [26]」

フォーティネットの差別化要因

優れた性能

FortiGate は、マイクロ秒を争う電子取引インフラストラクチャにおいて業界**最小の遅延とジッターレート**を実現します。SSL/TLS 暗号化トラフィックのインスペクションを有効にした場合でも、ネットワークのパフォーマンスに影響することはありません。

可視性と運用効率

フォーティネット セキュリティ ファブリックは、さまざまなサードパーティ製品との統合を可能にする多数の API を提供しており、オープン API アーキテクチャを採用しています。これにより、金融機関は拡大し続ける攻撃対象領域に分散しているさまざまなセキュリティ要素を一元化された管理ビューに統合できます。

支社 / 拠点の保護

包括的な **SD-Branch インフラストラクチャ**が、スイッチングインフラストラクチャからデータセンターまでのあらゆる要素に最適なセキュリティを提供し、ネットワークパフォーマンスの向上を実現します。

結論

金融機関においては、企業データ、アプリケーション、そしてワークフローを高度化が続く脅威から保護することがこれまで以上に重要となっています。フォーティネット セキュリティ ファブリックは、優れたネットワークパフォーマンスを確実に維持すると同時に、金融機関全体で包括的な統合保護ネットワークの構築を可能にする、統合プラットフォームを提供します。

[1]「IBM X-Force Threat Intelligence Index 2019」、IBM、2019 年 11 月 6 日にアクセス時の情報（英語）：
https://www.ibm.com/security/data-breach/threat-intelligence

[2]「Protecting the Expanding Attack Surface」、フォーティネット、2019 年 11 月 6 日にアクセス時の情報（英語）：
https://www.fortinet.com/demand/gated/Newsletter-Protecting-the-Expanding-Attack-Surface.html

[3]「Industry leaders struggle to balance digital innovation and security」、Help Net Security、2018 年 4 月 4 日（英語）：
https://www.helpnetsecurity.com/2018/04/04/balance-digital-innovation-security/

[4]「Federal Regulations for Financial Institutions and Other Industries」、CSI、2019 年 11 月 6 日にアクセス時の情報（英語）：
https://www.csiweb.com/industries-we-serve/financial-institutions/regulatory-compliance/federal-regulations

[5]「The Impact of Cybersecurity Incidents on Financial Institutions」、Identity Theft Resource Center and Generali Global Assistance、2019 年 11 月 6 日にアクセス時の情報（英語）：
https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf

[6]「Is the cybersecurity skills shortage getting worse?」、Jon Oltsik 氏、CSO、2019 年 5 月 10 日（英語）：
https://www.csoonline.com/article/3394876/is-the-cybersecurity-skills-shortage-getting-worse.html

[7]「Financial services top cyber attack target」、Warwick Ashford 氏、Computer Weekly、2019 年 7 月 31 日（英語）：
https://www.computerweekly.com/news/252467639/Financial-services-top-cyber-attack-target

[8]「セキュアで高速なパフォーマンスを実現する FortiGate 次世代ファイアウォール」、フォーティネット、2020 年 4 月 23 日：
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/ja_jp/SB-Secure-Communications.pdf

[9]「Infrastructure as code: The engine at the heart of DevOps」、Christopher Null 氏、TechBeacon、2018 年 11 月 6 日にアクセス時の情報（英語）：
https://techbeacon.com/enterprise-it/infrastructure-code-engine-heart-devops

[10]「Security as Code: Why a Mental Shift is Necessary for Secure DevOps」、Justin Boyer 氏、Simple Programmer、2018 年 3 月 7 日（英語）：
https://simpleprogrammer.com/security-code-secure-devops/

[11]「Assembling your cloud orchestra: A field guide to multicloud management」、IBM、2018 年 10 月（英語）：https://www.ibm.com/downloads/cas/EXLAL23W

[12]「Enterprises are moving SD-WAN beyond pilot stages to deployment」、Andy Patrizio 氏、Network World、2018 年 5 月 7 日（英語）：
https://www.networkworld.com/article/3269858/enterprises-are-moving-sd-wan-beyond-pilot-stages-to-deployment.html

[13]「25% Of Cyberattacks Will Target IoT in 2020」、Retail TouchPoints、2019 年 11 月 6 日にアクセス時の情報（英語）：
https://www.retailtouchpoints.com/resources/type/infographics/25-of-cyberattacks-will-target-iot-in-2020

[14]「Reducing WAN OpEx with High SD-WAN Performance」、Nirav Shah 氏、CSO、2019 年 4 月 9 日（英語）：
https://www.csoonline.com/article/3388026/reducing-wan-opex-with-high-sd-wan-performance.html

[15]「The top five cyber threats for banks—and how to meet them」、Howard Altman 氏、BAI Banking Strategies、2019 年 6 月 26 日（英語）：
https://www.bai.org/banking-strategies/article-detail/the-top-five-cyber-threats-for-banks-and-how-to-meet-them

[16] フォーティネットリサーチがさまざまな立場のユーザーを対象に実施した調査研究に基づく。 調査レポートは近日公開予定。

[17] 同上

[18]「Security Teams Overwhelmed by Rising Volume of Attacks」、Dark Reading、2017 年 5 月 31 日（英語）：
https://www.darkreading.com/security-teams-overwhelmed-by-rising-volume-of-attacks/d/d-id/1329015

[19]「Automation: Moving Security from Human to Machine Speed, and All its Implications」、Dave Barton 氏、Security Magazine、2019 年 5 月 28 日（英語）：
https://www.securitymagazine.com/articles/90285-automation-moving-security-from-human-to-machine-speed-and-all-its-implications

[20]「The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware」、Derek Manky、CSO、2018 年 8 月 29 日（英語）：
https://www.csoonline.com/article/3301148/the-evolving-threat-landscape-swarmbots-hivenets-automation-in-malware.html

[21]「Financial services top cyber attack target」、Warwick Ashford 氏、Computer Weekly、2019 年 7 月 31 日（英語）：
https://www.computerweekly.com/news/252467639/Financial-services-top-cyber-attack-target

[22]「Insider threat: The human element of cyberrisk」、Tucker Bailey 氏他、McKinsey、2018 年 9 月（英語）：
https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

[23]「Threat Spotlight: Advanced polymorphic malware」、Kevin Williams 氏、Smarter MSP、2018 年 6 月 13 日（英語）：
https://smartermsp.com/advanced-polymorphic-malware/

[24]「Challenges and Opportunities to Close the Cybersecurity Gap in the Financial Services Industry」、SecurityIntelligence、2019 年 4 月 18 日（英語）：
https://securityintelligence.com/challenges-and-opportunities-to-close-the-cybersecurity-gap-in-the-financial-services-industry/

[25]「The hidden threat in GDPR’ s encryption push」、Omar Yaacoubi 氏、PrivSec Report、2019 年 1 月 8 日（英語）：
https://gdpr.report/news/2019/01/08/the-hidden-threat-in-gdprs-encryption-push/

[26]「Industry leaders struggle to balance digital innovation and security」、Help Net Security、2018 年 4 月 4 日（英語）：
https://www.helpnetsecurity.com/2018/04/04/balance-digital-innovation-security/

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

WP-Fortinet-Financial-Services-202004-R1