大学共同利用機関法人
自然科学研究機構

ゲートウェイでの端末単位の認証から、ユーザー単位の認証でセキュリティを強化 APIを駆使してさまざまな機能を実装し、ネットワーク基盤の「あるべき姿」に向けて前進

大学共同利用機関法人自然科学研究機構（NINS）の岡崎3機関では、クラウドサービス導入を機に「一人一アカウント体制」の整備を進めてきた。そして更改を機に、ユーザー単位の認証を実現し、SAMLでさまざまなリソースと連携しながらアクセス制御を行える新ネットワーク基盤「ORION 2022」を、複数のフォーティネット製品を組み合わせて実現した。

大学共同利用機関法人 自然科学研究機構

自然科学研究機構（NINS）は、宇宙、エネルギー、物質、生命等に係る大学共同利用機関（国立天文台、核融合科学研究所、基礎生物学研究所、生理学研究所、分子科学研究所）を設置・運営することにより、国際的・先端的な研究を推進する自然科学分野の国際的研究拠点として、全国の大学等の研究者に共同利用・共同研究の場を提供している。

大学共同利用機関法人
自然科学研究機構
岡崎情報ネットワーク管理室
大野 人侍氏

大学共同利用機関法人
自然科学研究機構
分子科学研究所
技術推進部
計算情報ユニット
技師
水谷 文保氏

大学共同利用機関法人
自然科学研究機構
分子科学研究所
計算科学研究センター
技術職員
澤 昌孝氏

導入・構築のポイント

（1）以前から整備してきた一人一アカウント体制の上で、機器単位ではなくユーザー単位の強固な認証を次世代ファイアウォールFortiGateで実現

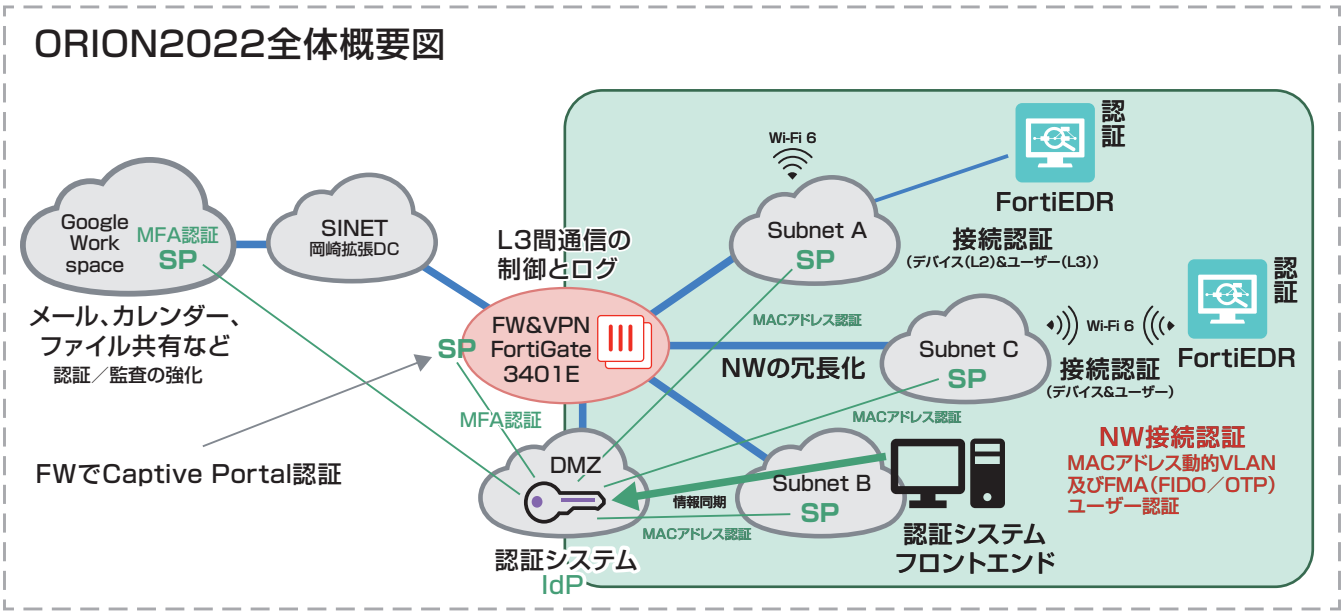
（2）セキュリティ領域の機能をフォーティネット製品でそろえ、運用管理や障害対応の手間を大幅に削減

（3）各製品のAPIと開発者向け情報を活用し、標準では足りない機能を自ら開発してフローを整備

クラウド導入を機に「一人一アカウント」を整備、次期ネットワークで認証強化を視野に

自然科学研究機構（NINS）は、旧岡崎国立共同研究機構から引き継いだ基礎生物学研究所、生理学研究所、分子科学研究所という3つの研究機関（岡崎3機関）に加え、国立天文台、核融合研究所という5つの研究所から構成され、大学共同利用機関法人として、国内外の研究者や大学、共同研究を行う民間企業にさまざまな研究設備を提供してきた。このうち、岡崎3機関や事務センターなどの共通施設群が利用するネットワーク基盤「ORION」の運用やセキュリティ管理を担っているのが、岡崎情報ネットワーク管理室だ。クラウドサービスにおける「責任共有モデル」のように、各研究所の管理者と連携しながら、主に基幹ネットワーク部分の設計や運用保守を行っている。

「トップダウン」が効く民間企業とは異なり、岡崎3機関は基本的に各研究所、各研究室の自主性を尊重する文化が根強い。あくまで「研究ファースト」で、強力な統制を徹底させるのは難しい状況の中、岡崎情報ネットワーク管理室はバランスを取りながらセキュリティポリシーの整備やさまざまな対策を進めてきた。「やりたい対策をすべて実施できる



だけの予算はありません。ですので、必ずやるべき部分にメリハリを付ける形で対策を実施してきました」と、岡崎情報ネットワーク管理室の大野人侍氏は語る。

岡崎3機関ならではの自主性や自由度の高さが端的に現れていたのが、研究者や学生、職員が利用する「アカウント」の管理だった。岡崎3機関では警備やエネルギーセンターなど一部の業務を外注しており、中には業務全体で一つのメールアカウントを共有している部署もあった。このため、人事部のデータベースとネットワークサービス提供のためのレポジトリとで、登録内容が一致していないこともあった。

昨今のクラウド普及を受け、岡崎3機関も2020年からオンプレミスのメールサーバからGoogle Workspaceへの移行を進めることになったが、これと並行してIDの整理整頓を行い、統合認証のための基盤を整えてきた。

この情報整理の結果、ユーザー数は1,000名を超え、端末数は6,000台が存在することが分かった。

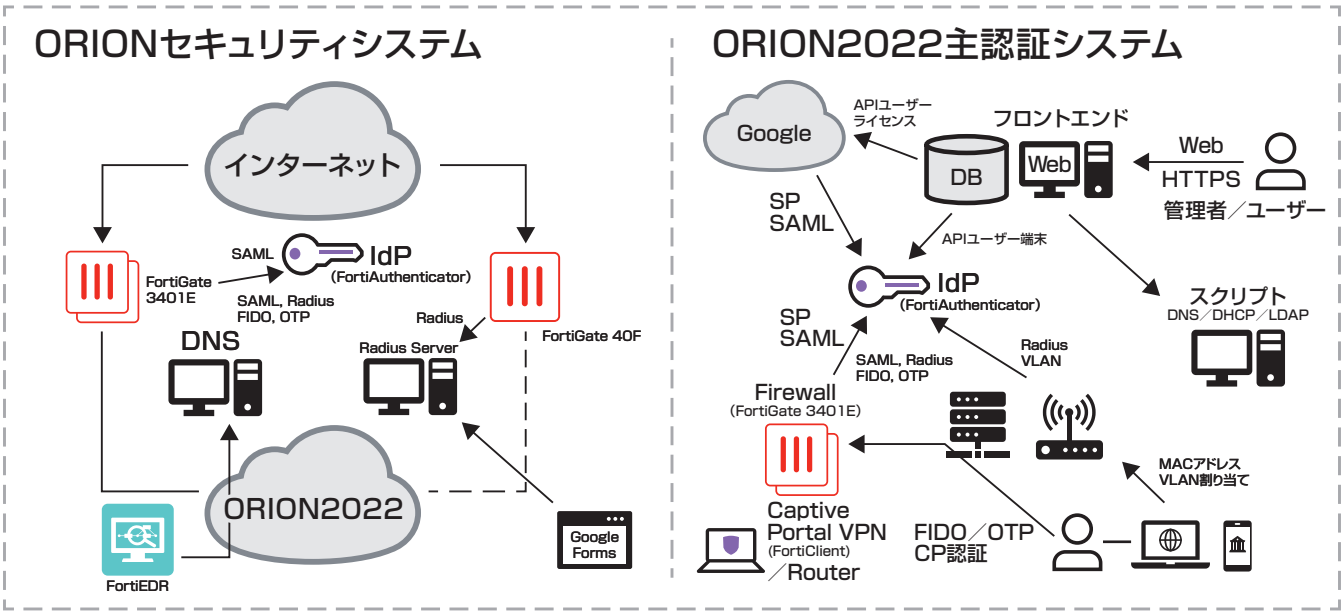
IDの整理に取り組んだ分子科学研究所 技術推進部 計算情報ユニット技師の水谷文保氏は、「この状態を改め、一人一アカウントを発行し、全体に連絡する必要がある時にはグループを組んでそこに通知するという当たり前の形を整えることで、はじめてしっかりとした情報管理ができるようになると考えました」と振り返る。中には逆に、一人で複数のアカウントを使っている研究者もいたが、そうした状態を2〜3年かけて整理し、ようやく「一人一アカウント」体制が整ってきた。

その頃、以前から運用してきたネットワークインフラ「ORION 2017」も更改の時期を迎えていた。ここで岡崎情報ネットワーク管理室が考えたのが、「ネットワーク接続時に、機器ではなく個人を認証するようにしてセキュリティを強化したい」ということだった。

端末ではなくユーザー単位での認証が鍵ととらえ、エンドポイントでの対策を重視

それまで岡崎3機関のネットワークでは、RADIUSを用いた「主認証システム」が端末のMACアドレスで認証を行い、登録された端末のみが接続できる仕組みを整えていた。だが、「『これはやはり認証ではない』と感じていました。MACアドレスは詐称が可能ですし、そのマシン上で誰が使っているかまでは特定できません。しかし『誰が使っていたか』まで特定できなければ、インシデント発生時の調査などが困難になると感じていました」（大野氏）

「誰が」を特定する認証についても、パスワードだけでなくより強固な認証を行う必要性も感じていた。すでにGoogle Workspace導入のタイ



ミングでGoogle Authenticator等を用いた多要素認証を一部で導入済みで、ユーザーの抵抗感も薄れつつあることを背景に、業界標準である「FIDO」準拠の認証を軸に検討することにした。

暗号化通信の増加に伴ってゲートウェイでのセキュリティ対策が困難になりつつあることも、ユーザー認証の強化、つまりエンドポイント側の対策の強化を求める理由となった。「以前のネットワークではゲートウェイ製品を使っていました。当初は良かったのですが、ネットワークのログを見ているとどんどん暗号化通信が増え、見えない部分が非常に多くなってしまいました」（大野氏）

ゲートウェイを素通しにすることはあり得ないが、「もはや、それだけで守る時代ではない」と判断し、エンドポイントでの対策も強化することにした。

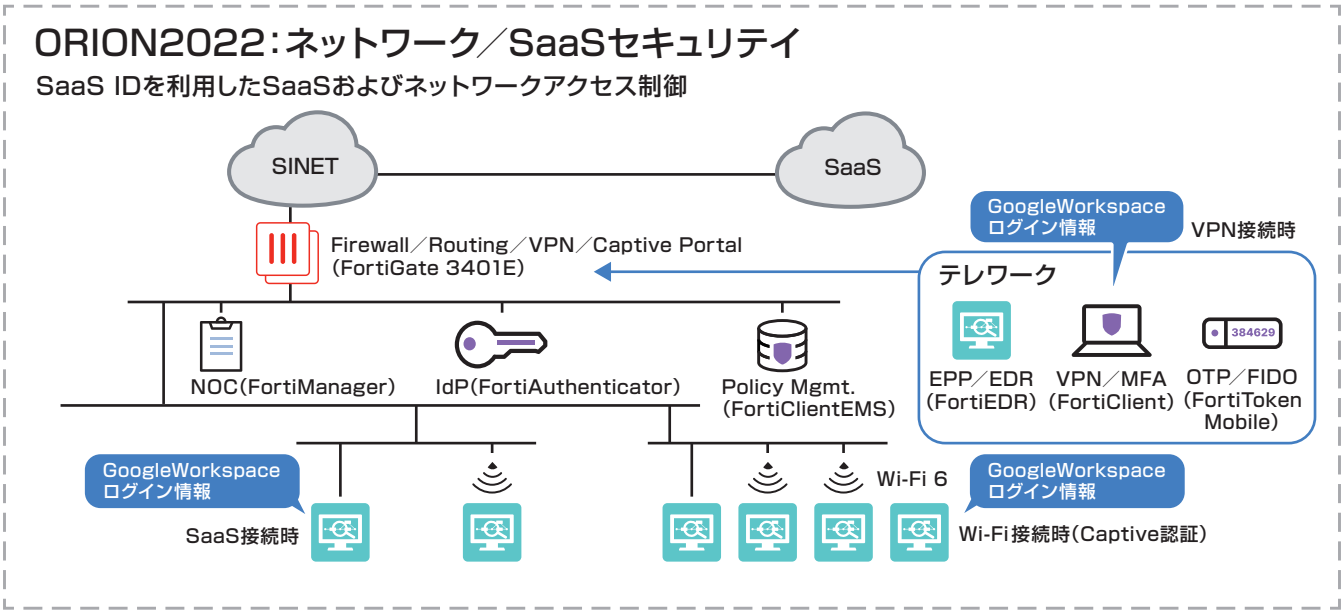
もう一つ重視したのは、機器のメーカーをなるべく統一することだ。それ以前は、さまざまなメーカーから調達した機器を組み合わせ、いわゆるベスト・オブ・ブリードを意識して構築していたが、運用負荷の増大が次第に明らかになっていたという。これまではネットワークとセキュリティだけで10社のベンダーとの契約があったが、ORION2022ではフォーティネットを含む2社にまで集約できた。

主にシステムやネットワークの運用を担っていた分子科学研究所 計算科学研究センター 技術職員の澤 昌孝氏は、「たまにトラブルが起こると、問題を切り分けるためにつながっている他の機器も調べていく必要があります。多種多様な機器で構成されているとそれぞれのベンダーに問合せながら調べていかなければならず、手間がかかっていました」と振り返った。

ORION 2022はこうした要件を踏まえ、FIDOも含めた多要素認証によってユーザー単位で認証を行ってネットワークに接続すると同時に、SAML連携によってGoogle Workspaceや必要なシステムにシームレスにログインできる主認証システムを軸にする形で仕様書をまとめ、入札を実施した。運用保守を楽にするため、できるだけ少ないベンダーの製品で統一することも評価項目として組み入れた。

フォーティネット製品で一連の処理を包括的に実現、足りない部分はAPIを用いて実装

入札の結果、主認証システムのIdPに「FortiAuthenticator」を用い、さらに次世代ファイアウォール兼認証の中核として「FortiGate 3401E」を導入し、エンドポイントに「FortiEDR」「FortiClient」を組み合わせ、キャプティブポータル経由で各種リソースとSAMLで



連携してアクセス制御する提案が選ばれた。

岡崎3機関は学術情報ネットワーク(SINET)へ100Gbps回線で接続している。これだけの帯域をカバーできるリーズナブルなセキュリティ機器となるとFortiGateほぼ一択だっただけでなく、FortiAuthenticatorと連携してFIDO認証が行えることが、岡崎3機関の必須条件を満たしていると判断された。

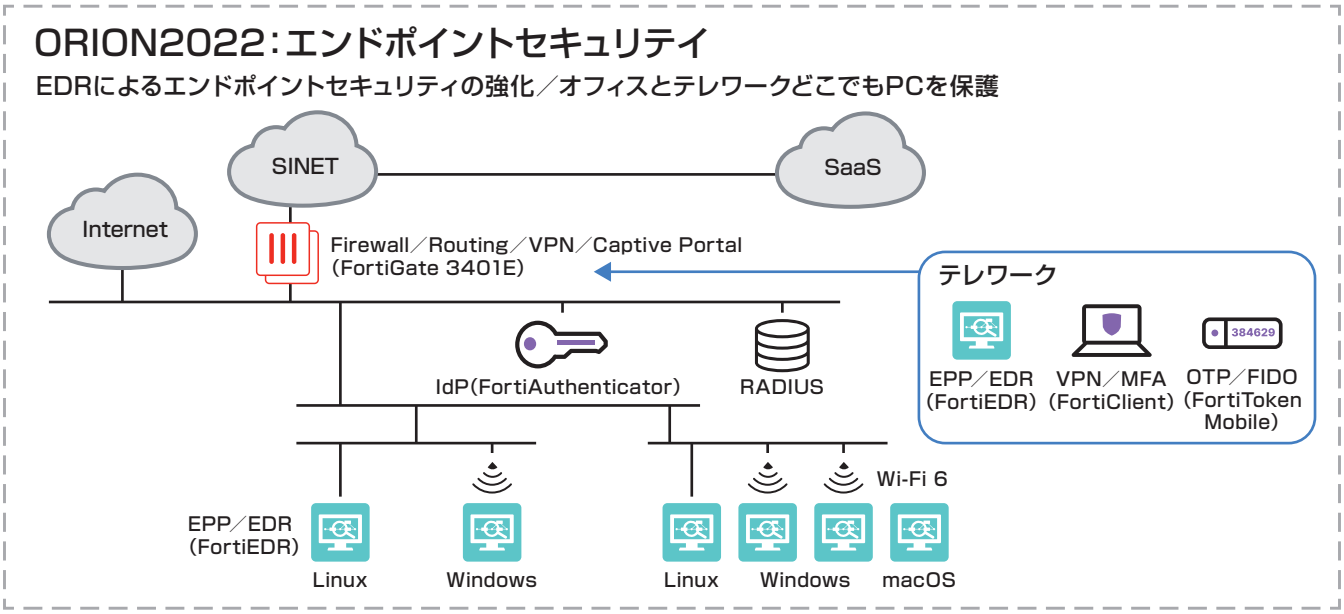
「新ネットワークでは、『誰に』認証をさせるかも検討しました。スイッチやエージェントに担わせる方法もあり得ましたが、認証ポイントとしてFortiGateを利用すれば、セキュリティ周りの機器をフォーティネットの製品でまとめることができ、連携性や保守性、運用性が向上すると期待しました」（大野氏）

こうして運用を開始したORION2022では、以前は別々のデータベースで管理され、煩雑だったユーザーの登録から認証、ネットワーク接続に至るまでの一連の作業を効率化できている。FortiAuthenticatorに登録されているユーザー数は1,000を超え、デバイスも6,000以上登録されているが、FIDO認証については事前にPoCで動作検証を行っていたこともあり問題なく動作している。

「新しい研究者などが加わった時には、岡崎3機関で独自に構築している主認証システムのデータベースに各研究所の担当者が登録を行うと、そこからFortiAuthenticatorに情報が登録され、さらに必要なデータを抽出してGoogleのアカウントを作成したり、各研究所のサービスを利用するためのLDAPサーバへ登録するといった処理が、すべて一連の流れで行えるようになりました」（大野氏）

ユーザーが正しい順番で申請してアカウントを発行し、認証方式をスムーズに切り替えていけるように、申請フローも整備し、途中で詰まらないようにシナリオを整えた。また定期的にアカウントの棚卸しも行い、使われていないアカウントがあれば確認の上で消去処理を行って、引き続き整理整頓を続けていくという。

水谷氏が開発したこの処理をはじめ、岡崎ネットワーク管理室では、フォーティネット製品が提供するAPIを活用し、さまざまな機能を独自に開発して自動化を図っている。たとえばVPN接続時のスプリットトンネリングの接続先をFQDNで管理するため、いったん外側で名前解決を行った上でFortiGateのルールに結果を返すようにしたり、2週間という認証期間が切れる前にキャプティブポータル上で認証期間を確認して自分の都合のいいタイミングで再認証を行う「キャプティブチェッカー」を実装するといった具合に、足りない部分は自ら開発してきた。



「入札時にも『APIを提供すること』を重視して仕様書を策定しました。フォーティネットの製品は基本的にすべてAPIが付いているため、製品単体で実現できない機能でも、APIを使って我々がプログラムすれば実現できる状況になっています」（大野氏）

大野氏も、将来的にクライアントにFortiEDRの導入を必須化することを視野に入れ、未導入の端末にアラートを表示する機能を開発中だ。「Fortinet Developer Network（FNDN）に行けばマニュアルがあり、実装例も書かれているため、それらを見て『こうやって使えばいいのか』と学びながら実装しています」（大野氏）といい、さらなるAPIの充実やナビゲーションの強化に期待しているという。

また、FortiClientとEnterprise Management Server（EMS）の組み合わせによって、端末にインストールされたOSやソフトウェアの脆弱性を把握することも可能になった。岡崎3機関では年に一回、端末の健全性をチェックして報告する「自己点検」を実施しているが、それを補い、最新の情報に基づいて一日に一回脆弱性の有無を確認することで、リスクの指標として役立てている。

「各部局ごとにIPアドレスレンジを分け、各部局の管理者もEMSのコンソールを閲覧できるようになっているため、自分が担当する部局で目立ってリスクの高い端末があれば注意喚起を行ってもらうよう依頼しています」（大野氏）

岡崎3機関ではマネージドサービスは購入せず、基本的に自力で運用している。FortiEDRについても、各部局の管理者とともに少しずつ運用を回し始めており、不要なアラートもなく従来のアンチウイルスソフト以上の保護機能が得られている。目下の課題は、アウトともセーフとも判断できない疑わしいアラートの調査・対応だ。

また、ファイアウォールのルールについても基本的に各部局に権限を委譲しているが、他ベンダーの別製品を活用してそのルールに穴がないか、適正なフローでポリシーが投入されているかをチェックする仕組みを整備してきた。ゆくゆくはこのフローの中にFortiManagerを組み入れ、FortiManager経由でポリシーのアップデートを行う整備を整えていく計画だ。

フォーティネット製品でセキュリティ関連の機能をほぼ統一することで、運用負荷も軽減できている。「幸いなことに、今のところ大きなトラブルは出ていないので実感する機会も少ないのですが、もしトラブルが起きても、『こういうところに原因があるのではないか』といったノウハ

ウを元に、スムーズに対応できています」（水谷氏）

あるべき姿に向けた「下地作り」が完了したORION 2022、今後も継続して改良を

ORION 2022以前から少しずつIDの整理を進め、さらにインフラを整備したことによって、その先を見据えた「下地作り」ができたと感じている。

「昔に比べて確実にセキュリティの意識は高くなってきています。ただ我々としては、強固な認証を行い、正しい認可を経てネットワークやリソースを使えるようにすることが重要だと思っています。今回の取り組みは、そうしたあるべき姿に慣れてもらうための下地であり、次のネットワークも視野に入れて少しずつ実現していきたいと思っています」と大野氏は語る。

研究機関という性質上、「必ずこの端末を、このツールを入れた状態で使いなさい」と強制することはできない。事実、研究者の中にはWindows利用者もいればMac利用者もおり、タブレット端末を便利に活用したいという具合に多様なニーズがある。その中で完全な統制を目指していては、利用者もネットワーク室も、どちらも不幸な状況に陥ってしまうだろう。

大野氏らは「なるべくおおらかな気持ちで進めています」と、できる限りそんな文化や利用者の意思を尊重しながら、全端末へのFortiEDR導入に向けて少しずつ土壌を整えている。現時点ではワンタイムパスワード認証（FortiToken Mobile）とFIDOキーのいずれかから認証方式を選択する形だが、ゆくゆくはPINコード入力が求められるFIDO2認証やPassKeyなどの採用も検討し、本人確認をさらに強固にしていきたいという。

一方裏側では、まだ一部に、手を動かして処理している部分が残っている。そこで、APIをさらに活用しながら、できる限り自動化していく方針だ。「以前は、シェルスクリプトなどを使ってアドホックに作っていたものを、きちんとAPIを使ってメンテナンスしやすい形で整理していきたいと考えています」（澤氏）

さまざまな利用者が多様な環境から利用するネットワーク基盤のセキュリティを、境界での対策だけに頼るのでは難しい。認証や端末のセキュリティも組み合わせてORION 2022で整備した基盤をベースに、「これからも世の中の動きに追随すべく絶えず情報や技術動向を確認し、変えるべきところは変えていきます。その基礎ができたと思っています」（大野氏）と、これからも足を止めずに改善を続けていく。

FORTINET
フォーティネットジャパン合同会社

〒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