2021.1.14

サイバーセキュリティニュース ＜2020 No.003＞

2020 年におけるサイバー攻撃の実態と対策のポイント
～サイバー攻撃に対する防御の限界、検知・対応の必要性～

【要旨】
■ 2020 年は新型コロナ禍の影響で働き方が大きく変化した。これに合わせて企業の IT 環境も変化したことにより、サイバー攻撃の手法や狙われるポイントも変化した。
■ ウィルス対策ソフトなどの防御だけに頼ったセキュリティ対策では悪意を持ったサイバー攻撃から「守り切る」ことは極めて困難になってきている。
■ 本稿では、2020 年におけるサイバー攻撃の実態と対策のポイントを解説する。

１．サイバー攻撃の実態

2020 年は、新型コロナ禍において不要不急の外出を控えるため、多くの企業でテレワークが推進されるなど、企業の IT 環境が大きく変化した。それに伴い、急速に普及したテレワーク環境、それを利用する人間の隙を突くサイバー攻撃が増加した。IT 環境の変化により利便性が向上する一方で、サイバーリスクが高まっている。以下に、2020 年の特徴的なサイバー攻撃を挙げる。

（１）コロナ禍に便乗したフィッシングメール

新型コロナ禍においてテレワークの導入が進み、従前に比べメールのやり取りが増加した結果、コロナ禍前と比べてメールを利用したサイバー攻撃による被害が発生しやすい状況となっている。例えば、コロナ禍の不安に付け込んだ「COVID-19 のワクチン情報」や、在宅勤務によるオンライン通販の利用増から、宅配業者の不在通知を装ったフィッシングメール等が横行した。

フィッシングメールは、正規サイトを偽装したサイトへ誘導させるような巧妙な文面が用いられており、メール文中の URL をクリックすると、ID、パスワード等の認証情報やクレジットカード番号、勤務先等の個人情報が盗取されてしまう。

（２）テレワーク環境を狙った攻撃

突貫工事でテレワーク環境を構築した企業も少なくなく、導入したネットワーク機器の脆弱性を狙った攻撃が見られた。

VPN 機器等のネットワーク機器は、日々新しい脆弱性が発見され、その修正パッチがリリースされている。攻撃者は、脆弱性を持つ機器の存在をインターネット空間で探査しており、該当する機器を発見した場合に不正アクセスを仕掛けてくる。侵入に成功すると、root 権限[1]を乗っ取ることもあり、保有する個人情報や機密情報の漏えいだけでなく、社外公開ページや基幹システムの停止・遅延等の被害が発生し得る。

（３）Emotet の再流行

2019 年 10 月頃から国内で感染事例が相次いでいた Emotet は、2020 年 2 月以降は大きな動きがなかったが、2020 年 7 月頃から再流行の兆しを見せた。

[1] ほぼすべての操作が可能な権限。すべてのファイルにアクセス可能で、すべてのアカウントのパスワード変更なども可能な強力な権限。

Emotet とは、メールを攻撃の入り口として、エクセルやワード等の不正なコードを含むドキュメントをユーザーに開かせることで感染するマルウェアである。不正なコードを含むドキュメントは、パスワード付き zip ファイルに格納されて送られてくるため、多くのウイルス対策ソフトでは、当該ファイルの中身までウイルスチェック機能が働かない。このため、zip ファイルの中に仕込まれたウイルスを発見できずに侵入を許してしまう例が多く見られた。

Emotet はメール情報の盗取・悪用のほか、新たなマルウェアのダウンロード等を行う特徴があり、攻撃者の C&C サーバー[2]と通信をする際は Windows 標準搭載の「PowerShell[3]」を利用するため、侵入後もウィルス対策ソフトに検知されづらいことが流行した要因の一つであるといえよう。

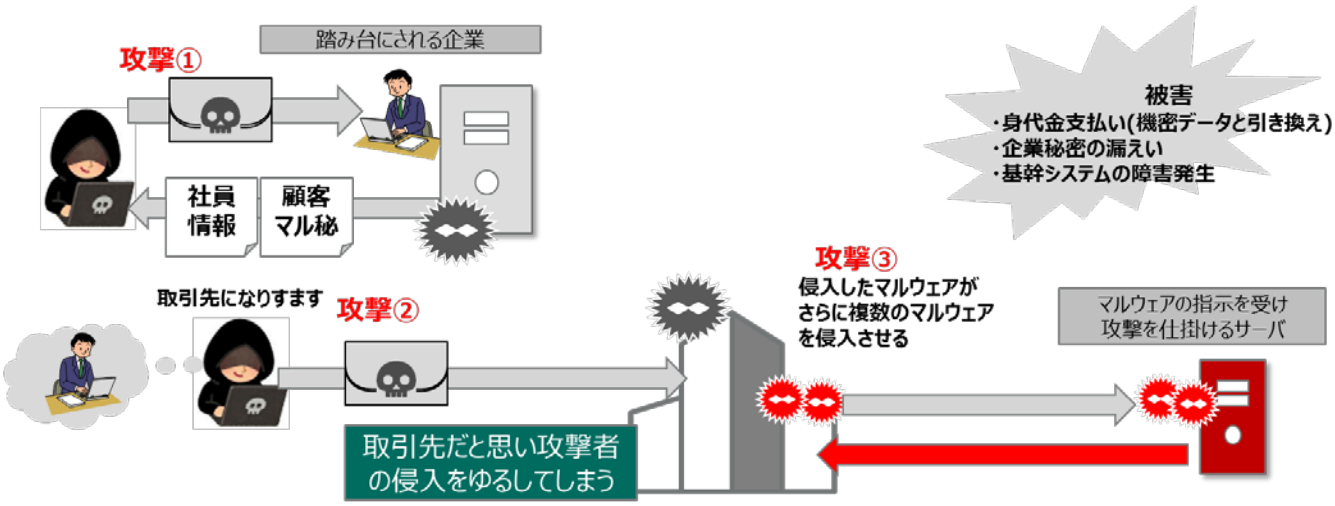
（4）サプライチェーン攻撃

原材料や部品の調達、製造、在庫管理、物流、販売、業務委託先などの一連の商流（サプライチェーン）において、セキュリティ対策が不十分な組織を攻撃の足がかりとして、最終的には大企業を攻撃するケースも見られた。サプライチェーン攻撃と呼ばれるもので、以下に前述の Emotet を用いた攻撃の一例を示す。

攻撃①：最終的な標的である大企業と取引のある企業へマルウェア付きのメールを送り、大企業とのメールのやり取りを盗取する。

攻撃②：取引先の社員になりすまし、大企業へマルウェア付きのメールを送信する。

攻撃③：油断した大企業の社員がメールを開封し、感染した場合、感染したマルウェアがさらに別のマルウェアを感染させる。



【図１】サプライチェーン攻撃の例

（5）ランサムウェアの多様化

従来のランサムウェアは、PC やサーバー内の情報を暗号化することにより、当該情報を参照・使用不能にした後で、元に戻すことと引き換えに「身代金（Ransom）」を要求するものであった。

2020 年は、予め重要情報を盗取した上でその情報を暗号化をし、使用可能な状態に復号することと盗取した情報を第三者に暴露しないことの両方で身代金を要求する「二重の脅迫」がみられた。身代金の支払いを拒否すると、盗取した重要情報をダークウェブ等で暴露される被害が見られた。

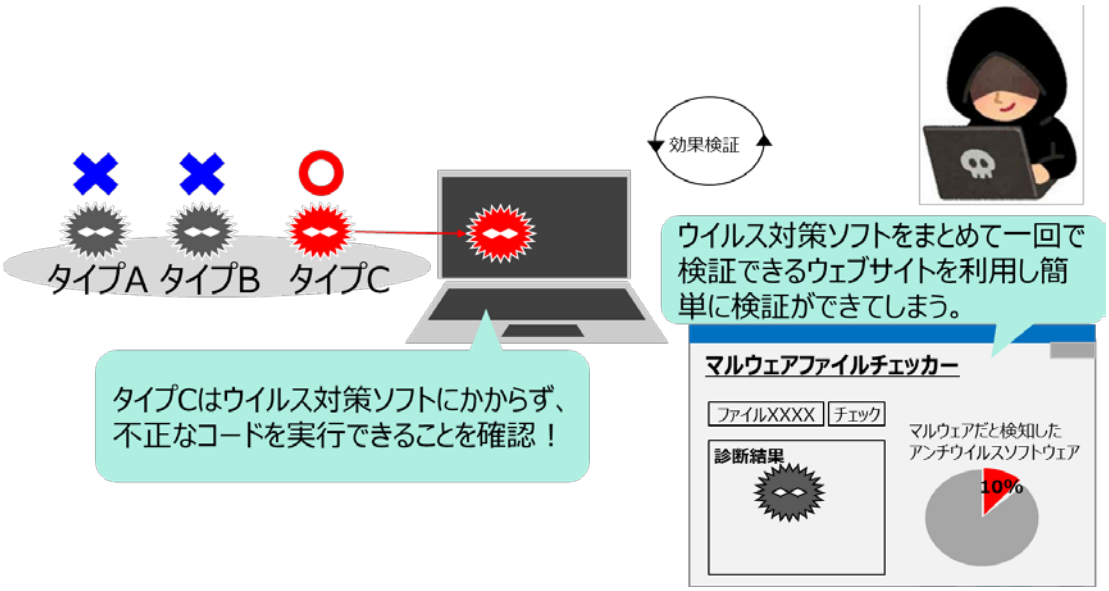
---

[2] Command and Control サーバーの略称。マルウェアに感染した PC をネットワーク経由で操作し、情報の収集や攻撃の命令を出すサーバー。

[3] PowerShell は Windows のほぼ全ての機能を実行可能で、主に遠隔地から PC のメンテナンスを行う場合などに使用される。動作は「プロセス」としてメモリ上で実行され、痕跡が残らない。

（６）ウィルス対策ソフトを突破する攻撃

不審なファイルや URL 等がウィルスに感染していないか、複数のウィルス対策ソフトで同時にスキャンできるサイトが複数のベンダーから提供されており、これを利用することで、単一のウィルス対策ソフトに比べ高精度でウィルスを検出できる。その一方で、攻撃者はこの種のサイトを悪用し、ウィルス対策ソフトで検出されないか確認できるため、ウィルス対策ソフトを突破する攻撃を仕掛けやすくなる。



【図２】ウィルス対策ソフトを突破する攻撃の例

人の心理や IT 環境の隙を突いたり、従前の想定を超える高度かつ巧妙な攻撃手法が増え続ける状況下では、ウィルス対策ソフトなどの防御だけに頼ったセキュリティ対策では悪意を持ったサイバー攻撃から自社を「守り切る」ことは極めて困難になってきている。防御だけではなく、サイバー攻撃を受けることを前提とした「検知・対応」の活動を取り入れることで、「防災」から「減災」を実現することが重要となる。

「検知・対応」は、多層防御の観点から、ネットワークの出入口を監視する「境界防御」と、エンドポイント [4]のセキュリティを確保するための「エンドポイント対策」の両方を実施することが望ましい。

２．検知・対応対策のポイント

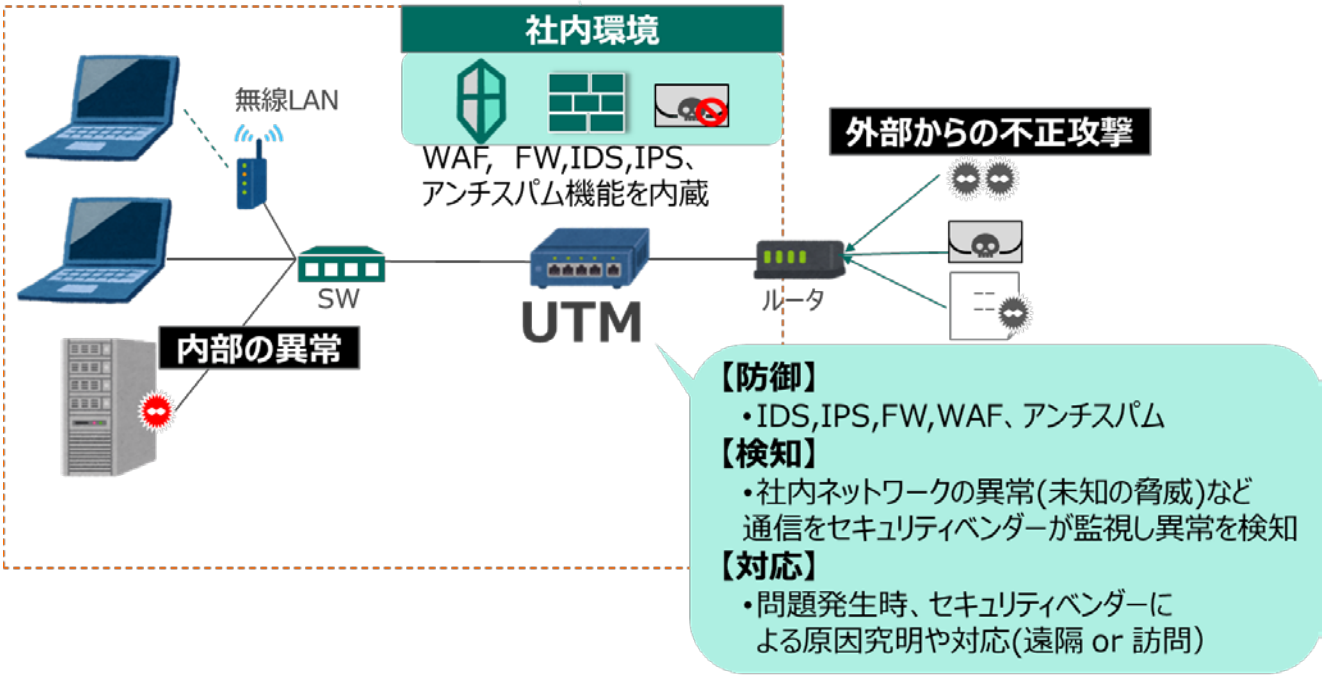
（１）ネットワークの出入口における境界防御

境界防御とは、インターネットと社内環境の出入口を監視し、不正な通信を検知・遮断することでセキュリティを確保することである。ファイアウォールや IPS／IDS、Web フィルタリング [5]、ウィルス対策ソフト等を導入し、社内環境への侵入および社内環境からの情報漏えいを防ぐ。

これらすべての機能を導入することは費用面や運用面での負荷が大きいため、最近では複数の異なる機能を一つのハードウェアに統合し、集中的にネットワーク管理をするセキュリティ装置である

[4] 通信回線やネットワークに接続されている機器のことで、個々の端末やサーバーを指す。
[5] IDS（Intrusion Detection System）：不正侵入を検知するシステム。
IPS（Intrusion Prevention System）：不正侵入を検知し、防止するシステム。
Web フィルタリグ：不適切な Web サイトへのアクセスを遮断するシステム。
WAF（Web Application Firewall）：Web アプリケーションを保護するセキュリティ対策。

UTM（Unified Threat Management（統合脅威管理））の普及が進んでいる。



【図３】ＵＴＭ設置のイメージ

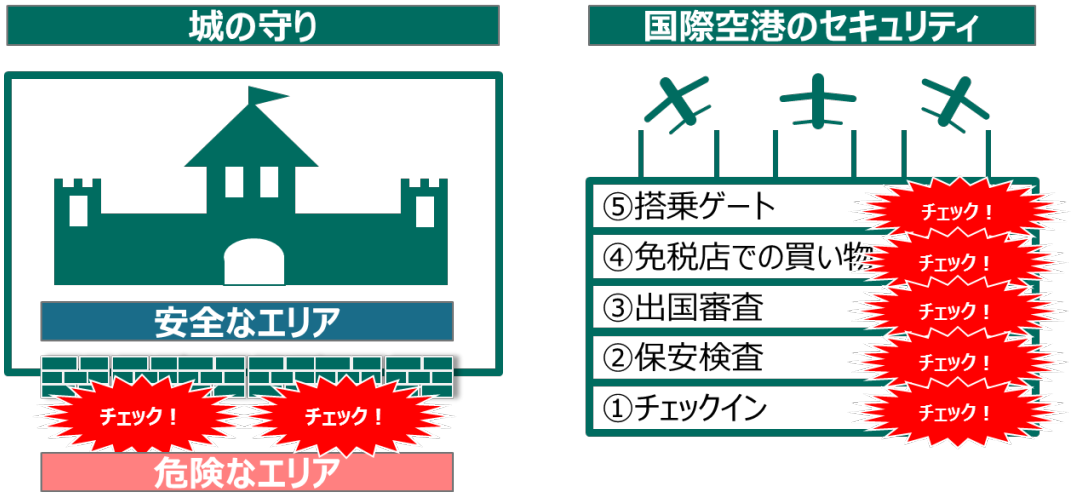
インターネットの通信に対して UTM を挟むことで、不正な通信等のサイバー攻撃を受けた際、素早い検知・対応が可能となる。

UTM 導入にあたっては、導入後のアラート設定や、セキュリティ事故発生時の復旧対応手順を決めておく等の確実な運用管理を行うこと、そして万が一セキュリティ事故が発生した場合の初動対応を適切に実施することが肝要である。

（２）ゼロトラストの考えに基づくエンドポイント対策

ゼロトラストとは 2010 年に米国 Forrester Research 社の John Kindervag 氏が提唱したセキュリティの概念モデルである。言葉のとおり「何も信頼しない」ということであり、組織の情報システムを構成する各種機器やアプリケーション、ネットワーク、端末、ユーザー等は「いずれも安全ではない可能性がある」という考え方に基づいてセキュリティ対策を行うものである。

境界防御は、城の守りのイメージで、チェックを受けて一度城内に入ると、中では自由に動いてよいというセキュリティになっている。一方で、ゼロトラストには安全なエリアという概念は基本的になくなる。そのため、何か行動する度にシステムの裏側で利用者の本人確認を行い、その情報に触れてよいユーザーかどうかを確認することになる。「城の守り」に対して、国際空港のセキュリティのイメージに近い。空港ではチェックイン後も保安・出国審査、免税店、搭乗ゲートなどさまざまな場所でパスポートや搭乗券の提示が求められる。

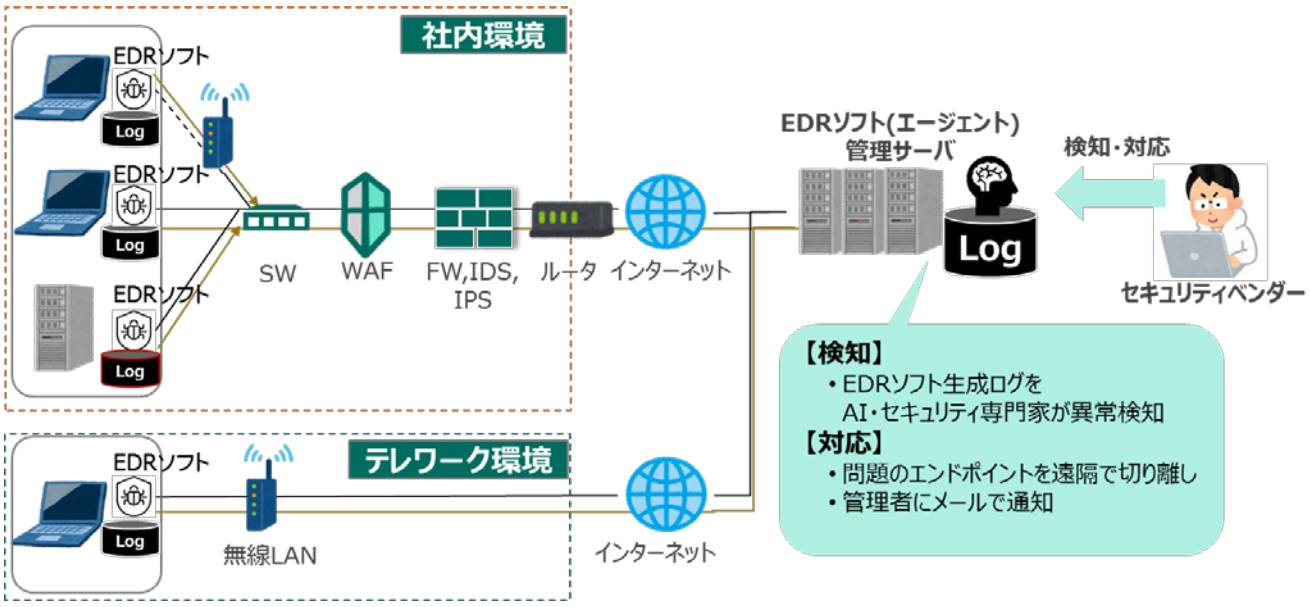


【図４】境界防御とゼロトラストのイメージ

この考えに基づき、国際空港のセキュリティのように、個々のエンドポイントで異常なふるまいやサイバー攻撃を監視し、検知・対応するセキュリティ対策が重要となる。

テレワーク環境の普及等により、自宅やクラウド環境等、社外環境に置かれた端末から社内環境にアクセスし、業務を行う機会が増えている。

境界防御に守られた社内環境であれば、一定のセキュリティ対策がされており、安全な環境のもとで業務が行われる。一方、社外環境に置かれた端末は、セキュリティ対策が適切でないまま外部のネットワークを経由して社内環境へアクセスしている場合があり、サイバーリスクが増大する可能性がある。このため、境界防御だけでなく、エンドポイント自身への対策を併せて行うことが望ましく、EDR（Endpoint Detection and Response）と呼ばれるセキュリティソフトウェアの導入が普及している。



【図５】ＥＤＲ導入のイメージ

不正な挙動を検知する EDR ソフトをエンドポイントに導入することにより、サーバー上の AI が、EDR ソフトが生成したログを自動解析する。セキュリティベンダーによる監視・分析を加えることで、

攻撃を迅速かつ効率的に検知することができる。

端末毎の監視が可能で、社内環境とテレワーク環境の両方をカバーできることが EDR 導入効果のメリットである。

３． 最後の砦は「人間」

多層防御による「検知」に基づいた素早い「対応」を行うことで、他の端末への感染拡大や、より重要な情報・データにアクセス可能な権限を持つユーザーへの感染などを防ぎ、被害を最小化することができる。その一方で、「悪意のある攻撃」か「正当な処理」かの判断は人間にしか出来ないケースがどうしても残る。

UTM や EDR 等のセキュリティ製品を導入するだけではなく、自社のレベルに合わせた運用を行い、検知結果を人間の目で仕分け、インシデント発生時に適切な初動対応を行うことが重要となる。

【表１】セキュリティ製品の運用レベルの例

	運用レベル	アクション
レベル３	常時監視	日々の運用を監視し、設定を見直す。インシデント発生時はレスキュー対応を実施する。
レベル２	ルールによる脅威の検知	自社に合わせたルールを設定し、インシデント発生時や他部署の要請で検知結果を解析する
レベル１	導入しただけ	導入時の設定から見直していないため、過検知や誤検知、検知漏れが発生する
レベル０	導入していない	セキュリティ対策に穴がある

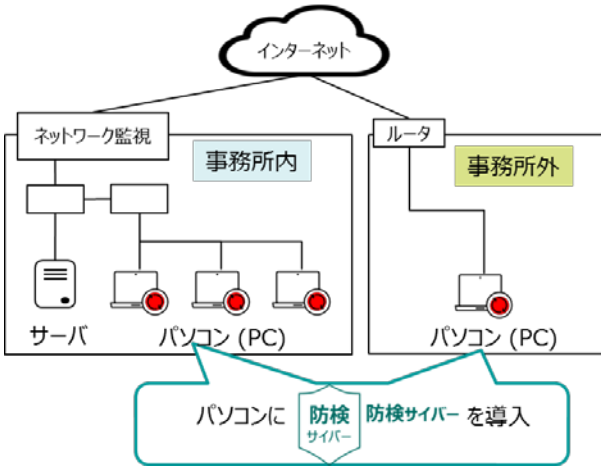
2020 年はビジネス環境の変化により、サイバー攻撃者の攻撃手法や標的となるポイントも変化した。それに合わせて、サイバーセキュリティ対策も定期的な見直しを行い、境界防御やエンドポイント対策を取り入れた多層防御を実現することが望ましい。

本稿が、2020 年の振り返りとともに、「新しい日常」に対応したセキュリティ対策強化の一助となれば幸いである。

ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部 サイバーリスク室
上席コンサルタント　五十嵐　大

ＭＳ＆ＡＤインターリスク総研株式会社では、脅威の侵入を素早く検知し、被害を最小限に止める次世代エンドポイントセキュリティ「EDR」と、24 時間 365 日の監視がパッケージとなったセキュリティサービス「防検サイバー」を提供しています。

本サービスは PC に EDR ソフトを導入し、インターネットを経由して AI やセキュリティアナリストが監視を行います。その為、自宅や外出先でもセキュリティ監視に影響はなく、テレワークを行う企業に適したサービスとなっています。



ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。
サイバーリスク・情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部　サイバーリスク室
千代田区神田淡路町2-105 TEL:03-5296-8961／FAX:03-5296-8941
https://www.irric.co.jp/