Capgemini RESEARCH INSTITUTE

APRIL 2020

サイバーセキュリティの免疫性を高める：現行の在宅勤務シフトにおけるサイバーセキュリティ上のリスクに向き合う

COVID-19パンデミックの影響が深刻化するに連れて、数多くの組織で在宅勤務が「ニューノーマル」となっています。最近の調査によれば、85%の企業が「少なくとも従業員の半数がCOVID-19に伴う在宅勤務をしている」と回答しました。[後注 1]

在宅勤務に基づく事業運営モデルへのシフトは、ITやサイバーセキュリティ面でのかなりの影響と、リスクの拡大を引き起こします。例えばシスコシステムズ社ではここ数週間で、リモート就業者向けセキュリティサポート・リクエスト数が10倍に急増しました。[後注 2] また、国家がスポンサーとなって他国のライフライン・インフラ（医療、救援機関、金融サービス等）に不正アクセスを図ろうとする攻撃のリスクも増大しています。[後注 3] 病院や食品配送サービスを含む重要インフラへまた、国家がスポンサーとなって他国のライフライン・インフラ（医療、救援機関、金融サービス等）に不正アクセスを図ろうとする攻撃のリスクも増大していますの攻撃の高まりも見られます。先日、ヨーロッパのある医療施設がサイバー攻撃に見舞われ、緊急手術の延期や、重篤患者の近隣施設への転院、更にはITネットワーク全体のシャットダウンを強いられる程の、深刻な被害が出ました。[後注 4]

今般の事態では2つの要因がビジネスリーダーにとって重要です。第一に、何故、サイバーセキュリティをCOVID-19危機対応の重点注力分野とすべきなのかを理解すること、第二に、リモート就業者のセキュリティを強化するにはどんなベストプラクティスが有効なのかを理解することです。

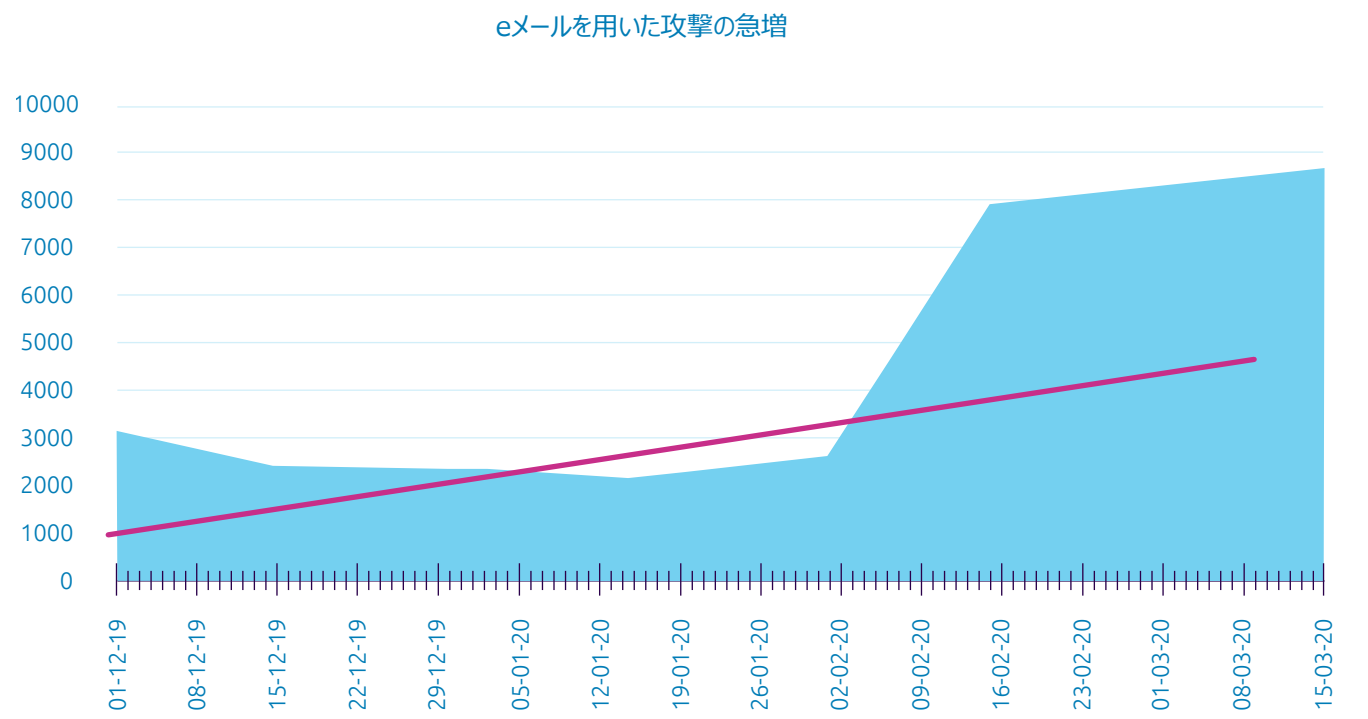
サイバーセキュリティをCOVID-19危機対応の最重点課題とする

コロナ危機は、サイバーセキュリティ上の課題を幾つも提起します。従業員が広く在宅勤務をしている状況は、ハッカーにつけ込む隙をより多く与えることになります（就業環境が変われば攻撃プレーンも変わるという結果を来した）。更にハッカーは、人々がコロナウイルス関連のニュース、ガイダンス、助言等を欲しているという事実につけ入って、偽のウェブサイトやオープンなフィッシングメールにアクセスするよう、従業員や一般大衆を唆しています。この種のサイバーセキュリティ攻撃は、新型コロナウイルスが人々の心に植え付けた恐怖や疑念を悪用して、セキュリティ上の誤った判断をさせようと仕向けます。例えば、ハッカーが仕掛けるサイバー攻撃には、従業員がコロナウイルスに関する最新データをウェブサイトからダウンロードするよう指示したり、政府から給付金を受け取るには組織の内部データを申告するよう促す、といったパターンが見受けられます。

SurveyMonkey社の社長であるトム・ヘイルも、上記の傾向を裏付けるコメントをしています：「コロナ危機に乗じて人々の感情につけ入り、切迫感を煽るようなフィッシング行為の増加が、確実に認められます。」[後注 5]

イタリア（新型コロナウイルスの被害が最も甚大な国の1つ）では、パンデミックの第一波において、異常なメールログインの急増が見られました（図1参照）。

図1： イタリアにおけるサイバーセキュリティ事案の急増



出典: Cynet global threat telemetry data, March 2020 [後注 6]

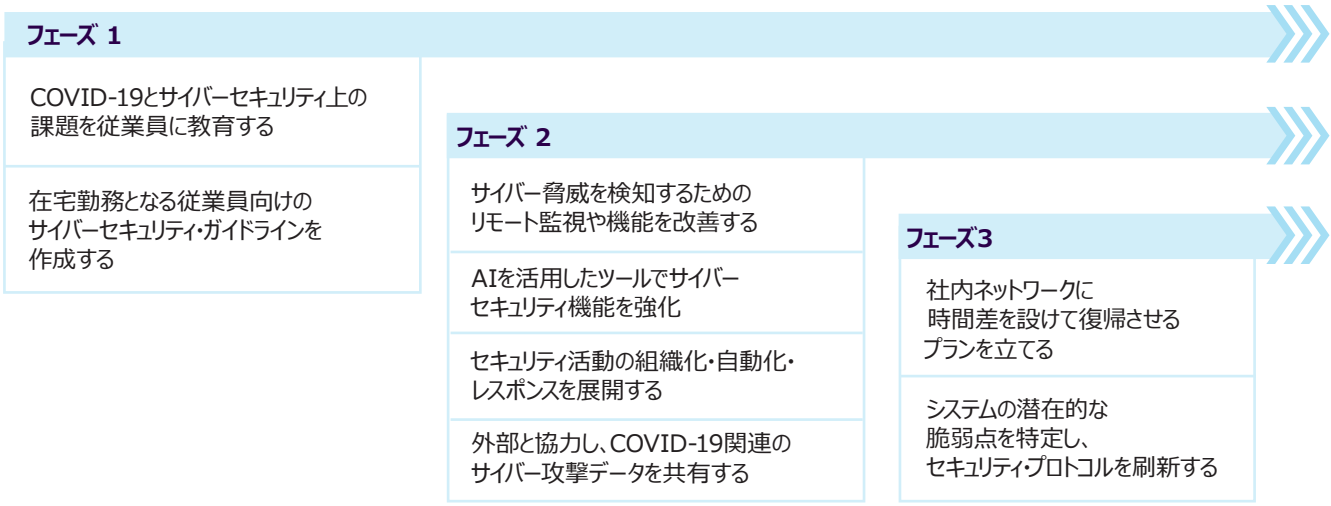
最近、他の国でも同様の現象が見られます。フランスのサイバーセキュリティ関係当局は、地方自治体を標的としたランサムウェア攻撃の警告を発しました。[後注 7] スピアフィッシングメール（特定のユーザーを標的として送られる個人的なメールで、彼らを欺いて要注意情報を漏らすように仕向ける）も、過去3か月間に驚くべきペースで増加しました。例えば、COVID-19関連のスピアフィッシング系メール攻撃は2月末以降、667%増加しています。[後注 8] Okta社（ID/アクセス管理企業）のサイバーセキュリティ戦略担当副社長 兼 Defcon社のセキュリティ責任者であるマーク・ロジャースは次のようにコメントしています：「ここまで大量のフィッシングは見たことがありません。文字通り、世界中の全ての言語でフィッシングメールの存在が認められています。」[後注 9]

リモート就業者のセキュリティを強化する

世界がCOVID-19の甚大な人的被害に対処している一方で、組織もまた、この事態が引き起こすサイバーセキュリティ上のリスクの高まりに、緊急の対応を迫られています。当社の経験では、ベストプラクティス的な対応には、3つの明確なフェーズが含まれます：

667%

2月末以降、COVID-19関連のスピアフィッシング系メールの増加率



フェーズ1：COVID-19とサイバーセキュリティの課題を従業員に教育する

在宅勤務となる従業員向けの包括的なサイバーセキュリティ・ガイドラインを策定し、タイムリーに更新し、遅滞なく周知する必要があります。GreatHorn社（クラウドネイティブのメールセキュリティ企業）のカスタマー・エクスペリエンス担当副社長であるマット・ペトロスキーは、次のように述べています：「企業は、規則が最も順守されるべきケース（例えば、お金がからむ行動や機密情報を求めるメールを受け取った場合）にその働きが強められるような仕組みを作るべきです。そうすればユーザーは、不審なメールに対して何か行動を起こす前に、情報に基づいた判断を下せるようになるでしょう。正しい判断が求められる状況で、規則を思い起こさせるポップアップ・メッセージ等を従業員に提示すれば、企業はリモート就業者に特有のリスクを大幅に低減できるはずです。」[後注 10]

他にも、教育の重要な要素として下記が挙げられます：

- 組織全体を対象に、セキュリティ意識向上キャンペーンを実施する。在宅勤務中に遭遇するであろうサイバーセキュリティ上の課題について、従業員に教育する。
- 従業員は在宅勤務中、安全なVPN経由で社内コミュニケーション用の各チャネルにアクセスすることができない可能性があるため、イントラネットのウェブページは、従業員の教育に相応しい手段ではないかもしれません。そのため、VPNを必要としない代替コミュニケーションチャネルを用意して、全従業員が定期的なサイバーセキュリティのアップデートを確実に受け取れるようにすることが重要です。
- パンデミックにつけ込むメールベースの詐欺やマルウェア等のスキームについて従業員に注意喚起する。例：信頼すべき情報源（疾病予防管理センター（CDC）、世界保健機関（WHO）、官公庁、医療保険会社等）から発信されたように見せかけた偽メール等。オフィスのメールが

従業員にとって必須の情報源であり、メールにまつわるセキュリティ課題を従業員に教育することが重要です。

- 治療薬・ワクチン・検査キット等を買うための政府からの給付金受け取りに関して、個人データを送信するよう促すメールについて、従業員が警戒するよう徹底する。
- 未許可のストレージシステムを利用することの潜在的なリスクについて、データ盗難の脅威も含めて、従業員に注意喚起する。
- GDPR等の法令に規定されている、個人データの機密性侵害やデータ漏洩にまつわるリスクについて、従業員に注意喚起する。従業員が使う私有デバイスを、その家族の他メンバーも共有して使う可能性があるため。
- 利用を許可している外製コラボレーションツールのリストを、従業員に通知する。一部のコラボツールは、従業員が把握していないセキュリティ上の欠陥を含む可能性があるため。

フェーズ2：サイバー脅威に対するリモート監視と検知の機能を向上させる

多くのリモート就業者がノートPC等、会社支給の機器を使う一方で、私有デバイスの利用も広く行われるでしょう。私有デバイスの利用が増えれば、幾つかのステップが重要になります。

- 要注意データを扱うアプリケーションへは、リモートデスクトップ・アプリケーションを介してアクセスするよう徹底する。
- セキュリティ事案（盗難、紛失等）が発生した場合に、会社支給の機器をリモートで完全データ消去できる機能を確保する。
- 要注意データにアクセスしたり要注意データを扱うために使われるデバイスを、継続的にモニターする仕組みを導入する。

アメリカのFirst Horizon Bankでは以前、在宅勤務できるスタッフは約30%でしたが、COVID-19の感染拡大に伴い、今ではその割合が50%まで上昇しました。この銀行は既にVPNシステムを持っていましたが、在宅勤務のオプションを拡張するために、各種ツール（バーチャルデスクトップ等）を追加しているそうです。同行はまた、複数の防御メカニズムを追加投入し、自社のネットワークを綿密にモニターするなど、サイバーセキュリティに正面から向き合っています。「より多くの従業員をこのリモート勤務モデルに移行させたのに伴い、コントロールされた環境の保全を確保すべく努めています」と、First HorizonのCIOであるブルース・リヴセイは述べています：「こうした状況に便乗しようとあれこれ探っているハッカーが大勢いるのは間違いないですから。」[後注 12]

資格情報を盗んだハッカーは、重要データにアクセスしようと試みるため、ID/アクセス管理（IAM）を強化することが重要です。これは、金融サービスや医療等の規制が厳しいセクターにとって、現下の危機で考慮すべき重要な領域となります。重要なアプリケーションについて多要素認証を確保することと、シングルサインオンをレビューすることが、セキュリティの向上に役立ちます。例えば、ソフトウェア企業のAutodesk社は、パンデミック危機をきっかけに二要素認証の利用を拡大して、同社のテクノロジー・サプライチェーンにおけるリスクを監視しています。[後注 13]

AIを活用したツールでサイバーセキュリティアナリストの機能を強化

セキュリティアナリストは、その仕事の重要性がこれから増大していくでしょう。ここ数週間、幾つもの機器で従業員がログインするようになったため、本物の脅威やアラートを偽陽性（誤検知）から見分けるのは大変になっていきます。もっとも、COVID-19以前でさえ、企業の56%は自社のネットワーク・セキュリティアナリストがパンク寸前だ、と回答していました – 追わねばならないデータポイントと末端デバイスの数が膨大であったためです。[後注 14] その様にリソースが逼迫した環境では、俊敏性が鍵となります。シーメンス社は、リソースを大幅に増員することなく、AIを活用してセキュリティを向上することに成功しました。

> “コロナ危機に乗じて人々の感情につけ入り、切迫感を煽るようなフィッシング行為の増加が、確実に認められます。”
>
> **トム・ヘイル**
> SurveyMonky社 社長

シーメンス社のサイバーディフェンスセンター (CDC) は、1秒当たり60,000もの潜在的に重大な脅威を評価できるよう、AWS (Amazon Web Services) を利用して、AI対応・高速・完全自動化かつ拡張性の高いプラットフォームを構築しました。AIのおかげで、12人に満たないチームでこの機能を実現できました。[後注 15] 私たちの調査によれば、脅威や違反を検知するための総所要時間は、AIを使うと最大12%まで短縮されます。[後注 16]

セキュリティ活動の組織化・自動化・レスポンスを展開してセキュリティ管理を改善する

セキュリティ活動の組織化・自動化・レスポンス (SOAR)[後注 17] は、組織がセキュリティ関連のデータやアラートを各種情報源から収集し、人とマシンのパワーを活用してインシデント分析を行えるようにするテクノロジーです。これはインシデント対応業務の標準化と、その定義付け・優先順位決め・推進に役立ちます。また、測定や報告面での向上と、対応までの時間短縮も図れます。但し、当社の調査では、今日までにそれを導入した企業は36%に留まっています。[後注 18]

外部と協力し、COVID-19関連のサイバー攻撃データを共有する

他の企業との協業による、脅威に関する最新データを共有するためのプラットフォームは、いつの時代も重要ですが、今日のバーチャル就業環境では特に大事です。

- ヨーロッパの大手金融機関 (Mastercard Europe, Banque de France, SWIFT, De Nederlandsche Bank, Euroclearを含む) は、サイバーセキュリティの脅威に関するインテリジェンスを共有するため、ヨーロッパ中央銀行 (ECB) と協力して、サイバー情報・インテリジェンス共有イニシアチブ (CIISI-EU) を立ち上げました。情報はオンラインでのやり取りを介して共有され、新たなサイバー脅威に効果的に対抗するために役立てられます。[後注 19]
- IBM社のX-Force (脅威関連のインテリジェンスを共有するための固有プラットフォーム) が、Emotet攻撃を発見しました。これは日本での新型コロナウイルス蔓延状況に乗じて出現したマルウェアで、障がい者に福祉サービスを提供する事業者からのものと見せかけたフィッシングメールを用いるものです。メールに含まれる文書を開くと、Emotetのダウンロードとインストールを実行します。[後注 20]

但し、上記アプローチの明らかな利点にも拘わらず、多くの企業は連携していません。サイバーセキュリティ、AIについて当社の調査によれば、クラウドソーシング・プラットフォームを介して脅威に関するインテリジェンスを社外と共有している、と答えた幹部社員は2人に1人のみでした。[後注 21]

今や、COVID-19関連のサイバー攻撃に特化したコミュニティが、組織によって生まれつつあります。Automation Anywhere社 (ロボットによる業務自動化 (RPA) のソフトウェア企業) のCIOであるユースフ・カーンは、次のように述べています：「当社では、リアルタイムで問題を特定し解決するため、従業員・パートナー・お客様との間で、オープンなコミュニケーションチャネルを確保しています。COVID-19のような危機は、グローバルの共同体を一体化させ、テクノロジーは巨大な問題を解決するための重要な媒介となる可能性があります」[後注 22]

もう一つのコミュニティはCOVID-19 CTI (サイバー脅威インテリジェンス) リーグで、40カ国に800人超のサイバーセキュリティ専門家を擁しています。このコミュニティは、Microsoft、 Okta、 Amazon、 Clearsky Cyber Security各社の技術担当役員によって運営され、最前線の医療リソースやライフライン・インフラの防御を優先しています。[後注 23]

12%
AIを使った場合、
脅威やセキュリティ違反の検知に
要する時間の総削減率

フェーズ3：社内ネットワークに段階的に復帰させるプランを立てる

各種のセキュリティ・コントロールは、企業の社内ネットワークでは効率的に機能するかもしれませんが、在宅勤務環境では必ずしも効率的ではありません。例えばVPNは、多数の従業員が在宅勤務している際に発生する大量のトラフィックを維持できない場合があります。また従業員が一定の期間、企業のVPNに接続せずに就業していると、使用中のノートPCやデスクトップPCは、定期的なアップデートやパッチの適用が遅れてしまうこともあり得ます。「非分散型の企業が用いる各種のセキュリティ・コントロールやツールの多くは、ユーザーがローカルネットワーク上にいることが前提であるため、リモートで行えることは限られます」と、Redox社 (ヘルスケア・テクノロジー企業) の全社セキュリティ統括であるリサ・デイヴィスは語っています：「こうした企業は、機器がローカルネットワーク上にないと、アップデートを配布する・ログをモニターする等の作業がより難しいことに気づきました。従って、従業員が機器を家に持ち帰ると、企業側ではブラックアウト状態なのです。」[後注 24]

事態が平常に戻っても、危機モードの間に従業員のノートPCが何らかの攻撃を受けて、セキュリティの免疫性が低下している可能性があります。デバイスを社内ネットワークに接続させる前に、段階的に機器のスクリーニング検査を行い、ウイルス対策ソフトが最新パッチにアップデートされているか否かを確認することが必須です。

全てのピンチは、それがどんなに陰惨なものであろうと、新たな学びの扉を開いてくれます。今まで在宅勤務のトライアル/テスト経験がなく、制度も整っていなかった企業は、そのことを特に実感するはずです。リモートアプリケーションのボリュームが急増すれば、サイバーセキュリティの免疫性がストレステストに晒されるようなものです。企業はそれを綿密に監視して、サイバーセキュリティ対策の不備を特定することで、自社システムの脆弱箇所を見極め、データへのアクセスや転送等に関するセキュリティ・プロトコルを刷新できるでしょう。

Affinitas Life社 (マーケティングサービス企業) のチーフデジタルオフィサーであるウェイン・サディンは、次のように述べています：「たとえ在宅勤務がフルに機能するようなプランが現時点で全て揃っていなくても、用意できたものをテストして最適化を図るには、今が良いタイミングです。」[後注 25]

結論

COVID-19危機によって、医療システムの健全性からグローバル・サプライチェーンの有効性に至るまで、私たちの社会や世界経済がどこまで耐えられるのか、が試されています。同時に、私たちのサイバーセキュリティと防御力も、その耐性をテストされています。一方で、今日この課題に注力し、投資することは、企業の長期的な競争力の強化につながります。即ち、企業は、最新テクノロジーの進歩を活用し、在宅勤務がますます新しい現実となりつつある世の中で事業運営していくための武器を手に入れることになります。

キャップジェミニ・リサーチ・インスティテュートでは、組織がCOVID-19パンデミックを乗り切るために役立つ実用的な指針を掲載したリサーチノートを連続でリリースしており、本文書はその特別シリーズの一部です。この他にも多くのリサーチノート、ガイダンス、分析などを以下のサイトでお読みいただけます：
https://www.capgemini.com/our-company/covid-19-insights-for-today-and-tomorrow/（英語）
https://www.capgemini.com/jp-jp/our-company/covid-19-insights-for-today-and-tomorrow/（日本語）

著者

Thierry Daumas, Head of Projects & Consulting, CIS and Global Offer Lead (GOL), Cybersecurity; **Steve Wanklin**, Capgemini, Group Chief Cybersecurity Officer; **Geert van der Linden**, Cybersecurity Business Lead; **Sandeep Kumar**, Vice President, Capgemini Invent, UK; **Jerome Buvat**, Global Head of Research and Head of Capgemini Research Institute; **Subrahmanyam KVJ**, Director, Capgemini Research Institute; **Sumit Cherian**, Manager, Capgemini Research Institute; **Gaurav Aggarwal**, Manager, Capgemini Research Institute and **Shahul Nath**, Consultant, Capgemini Research Institute have contributed to this research note.

詳細は、以下にお問い合わせください：

グローバル

Thierry Daumas (ティエリー・ドーマ)
Head of Projects & Consulting, CIS and Global Offer Lead (GOL), Cybersecurity
thierry.daumas@capgemini.com

Geert van der Linden (ヒエルト・ファン・ダ・リンデン)
Cybersecurity Business Lead
geert.vander.linden@capgemini.com

Secure Remote Working and Collaboration Solutions

Cybersecurity Services

参考文献

1. CNBC, “Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems”, March 2020
2. Reuters, “Mass move to work from home in coronavirus crisis creates opening for hackers: cyber experts, March 2020
3. ZDNet, “FBI re-sends alert about supply chain attacks for the third time in three months,” March 2020
4. ZDNeT, “Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak”, March 2020
5. CNBC, “Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems”, March 2020
6. Cynet, “Recent Escalations in Cyberattacks in Italy Prove the Coronavirus Impact on Cybersecurity - Acting as a Warning for CISOs Worldwide”, March 2020
7. Wired, “Hackers are targeting hospitals crippled by coronavirus”, March 2020
8. TechRepublic, “667% spike in email phishing attacks due to coronavirus fears, March 2020
9. CISOMAG, “International Cybersecurity Experts Come Together to Fight COVID-19 Related Cyberthreats”, March 2020
10. SC Magazine, “COVID-19 exposes gaps in cybersecurity safety net as millions work from home”, March 2020
11. US Federal Bureau of Investigation’s public service announcement, “FBI sees rise in fraud schemes related to the coronavirus (COVID-19) pandemic”, March 2020
12. American Banker, “Bank CIOs confront challenge of so many employees working at home”, March 2020
13. Forbes, “CIOs Vs. COVID-19: Tech Leaders Are Key To Companies’ Emergency Plans,” March 2020
14. Capgemini Research Institute, “Reinventing Cybersecurity with Artificial Intelligence”, July 2019 report
15. AWS, “Siemens Handles 60,000 Cyber Threats per Second Using AWS Machine Learning,” April 2019.
16. Capgemini Research Institute, “Reinventing Cybersecurity with Artificial Intelligence”, July 2019 report
17. Gartner, “Preparing Your Security Operations for Orchestration and Automation Tools,” February 2018
18. Capgemini Research Institute, “Reinventing Cybersecurity with Artificial Intelligence”, July 2019 report
19. The Daily Swig, “Europol joins forces with European financial giants to tackle rise in organized cybercrime,” March 2020
20. Capgemini Research Institute, “Reinventing Cybersecurity with Artificial Intelligence”, July 2019 report
21. Barracuda, “Threat Spotlight: Coronavirus-Related Phishing”, March 2020
22. Cmwire, “CIOs Share Business Continuity Plans Amid COVID-19 Pandemic, March 2020
23. GCN, “Cyber experts line up to defend medical community, critical infrastructure”, March 2020
24. SC Magazine, “COVID-19 exposes gaps in cybersecurity safety net as millions work from home”, March 2020
25. CIO, “COVID-19’s impact on the enterprise and remote work,” March 2020

キャップジェミニについて

キャップジェミニは、コンサルティング、デジタルトランスフォーメーション、テクノロジー＆エンジニアリングサービスのグローバルリーダーです。キャップジェミニ・グループはイノベーションの最前線に立ち、進化を続けるクラウド、デジタル及び各種プラットフォーム分野で、顧客のあらゆるビジネス機会に対応致します。キャップジェミニは、50年以上にわたり蓄積してきた優れた実績と業界固有の専門知識を基に、戦略から運用まで、弊社の一連のサービスを通じて、顧客企業が目指すビジネスビジョンの実現をご支援致します。キャップジェミニの信念は、「テクノロジーに関わるビジネス価値は人を通じて具現化される」ことであり、この信念こそが弊社の原動力となっています。キャップジェミニは、世界約50ケ国27万人に及ぶチームメンバーで構成される多文化企業です。Altranを含むグループ全体の2019年度売上は、170億ユーロです。

キャップジェミニについては、以下をご覧ください。

www.capgemini.com

People matter, results count.

MACS_CS_20200401_AP