経済産業省
Ministry of Economy, Trade and Industry

最近のサイバー攻撃の状況を踏まえた経営者への注意喚起

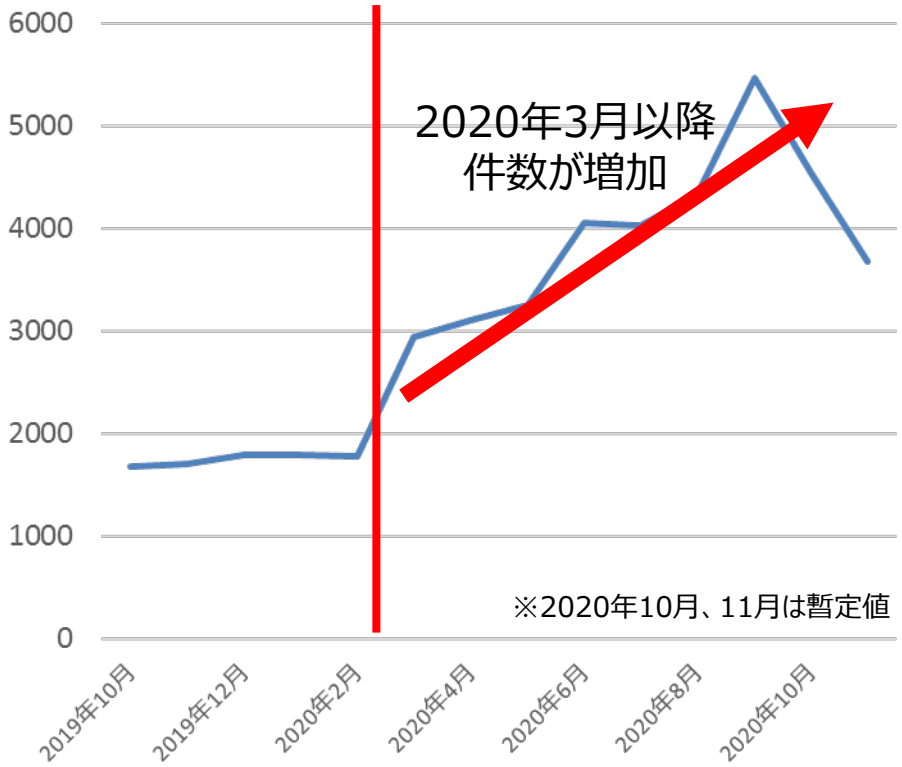
2020年12月18日

経済産業省
商務情報政策局
サイバーセキュリティ課

サイバー攻撃に関する相談窓口の最近の状況

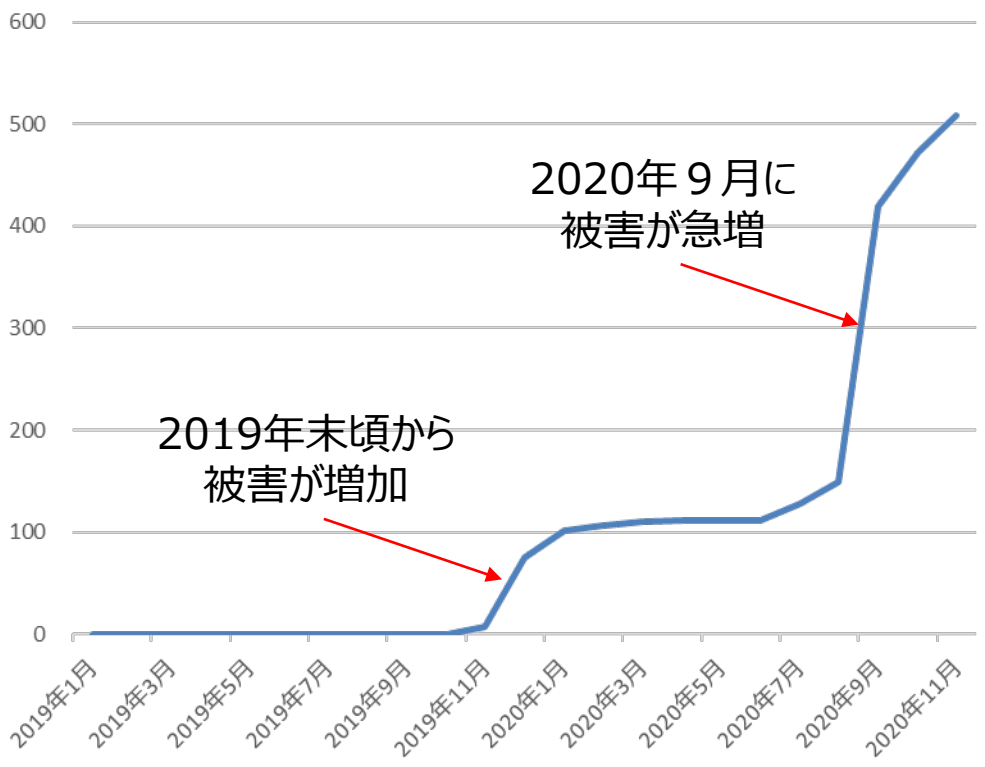
- 新型コロナウイルスの感染が拡大した2020年3月以降、インシデントの相談件数が増加。
- 特に、電子メールを媒介に感染を広げるマルウェア「Emotet※参考１参照」による被害の相談が急増。

JPCERT/CCへのインシデント相談報告件数（月別）



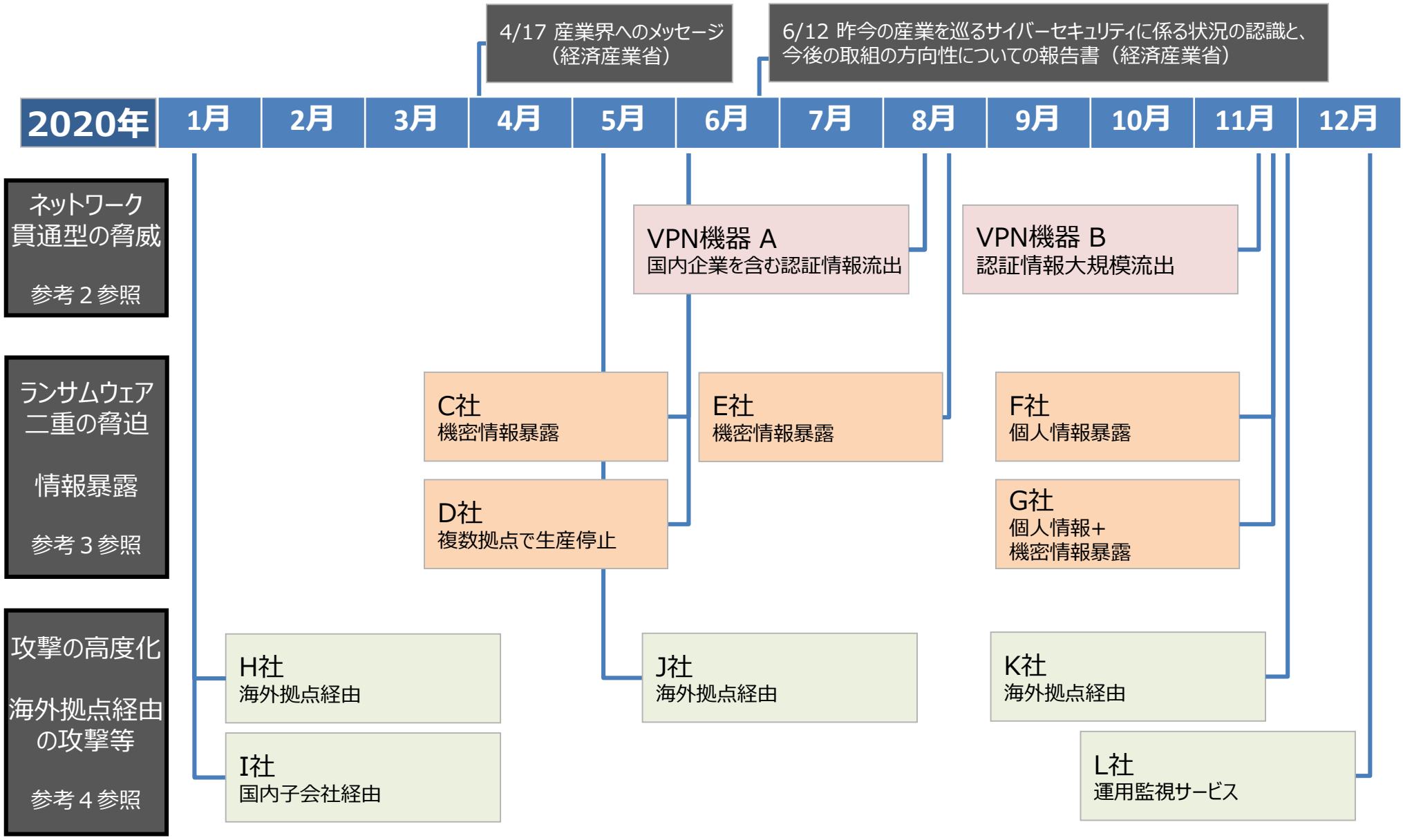
＜（一社）JPCERT/CC＞

IPAへのEmotetに関する相談件数（累積）



＜(独)情報処理推進機構（IPA）＞

2020年の主なサイバー攻撃事案



※攻撃開始時期ではなく、報道・公表された時期等でマッピング

経営者の方々へ

●サイバー攻撃は規模や烈度の増大とともに多様化する傾向にあり、実務者がこれまでの取組を継続するだけでは対応困難になっている。
●アップデート等の基本的な対策の徹底とともに、**改めて経営者のリーダーシップが必要に**。

① 攻撃は格段に高度化し、被害の形態も様々な関係者を巻き込む複雑なものになり、技術的な対策だけではなく関係者との調整や事業継続等の判断が必要に。改めて経営者がリーダーシップを。

② ランサムウェア攻撃による被害への対応は企業の信頼に直結。経営者でなければ判断できない問題。

●「二重の脅迫※」によって、顧客等の情報を露出させることになるリスクに直面。日常的業務の見直しを含む事前対策から情報露出に対応する事後対応まで、経営者でなければ対応の判断が困難。
●金銭支払いは犯罪組織への資金提供とみなされ、制裁を受ける可能性のあるコンプライアンスの問題。

③ 海外拠点とのシステム統合を進める際、サイバーセキュリティを踏まえたグローバルガバナンスの確立を。

●国・地域によってインターネット環境やIT産業の状況、データ管理に係るルール等が異なっており、海外拠点とのシステム統合を通じてセキュリティ上の脆弱性を持ち込んでしまう可能性も。
●拠点のある国・地域の環境をしっかりと評価し、リスクに対応したセグメンテーション等を施したシステム・アーキテクチャの導入や拠点間の情報共有ルールの整備等、グローバルガバナンスの確立が必要。

④ 基本行動指針（高密度な情報共有、機微技術情報の流出懸念時の報告、適切な場合の公表）**の徹底を。**

※攻撃者が、被攻撃企業が保有するデータ等を暗号化して事業妨害をするだけではなく、暗号化する前にあらかじめデータを窃取しておいて支払いに応じない場合には当該データを公開することで、被攻撃企業を金銭の支払いに応じざるをえない状況に追い込む攻撃形態。

相談窓口・注意喚起情報

● 内閣サイバーセキュリティセンター（NISC)

注意喚起情報	URL：https://twitter.com/nisc_forecast
ランサムウェアによるサイバー攻撃について（2020.11.26）	URL：https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf

● （独）情報処理推進機構（IPA）

■一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談

情報セキュリティ安心相談窓口	URL：https://www.ipa.go.jp/security/anshin/index.html 電話：03-5978-7509

■標的型サイバー攻撃を受けた際の相談（専門的知見を有する相談員が対応）

J-CRAT／標的型サイバー攻撃特別相談窓口	URL：https://www.ipa.go.jp/security/tokubetsu/index.html 電話：03-5978-7599

セキュリティ関連情報サイト	URL：https://www.ipa.go.jp/security/index.html
ランサムウェアに関する注意喚起	URL：https://www.ipa.go.jp/security/announce/2020-ransom.html

● （一社）JPCERTコーディネーションセンター（JPCERT/CC）

■インシデントに関する対応依頼

インシデント対応依頼	URL：https://www.jpcert.or.jp/form/

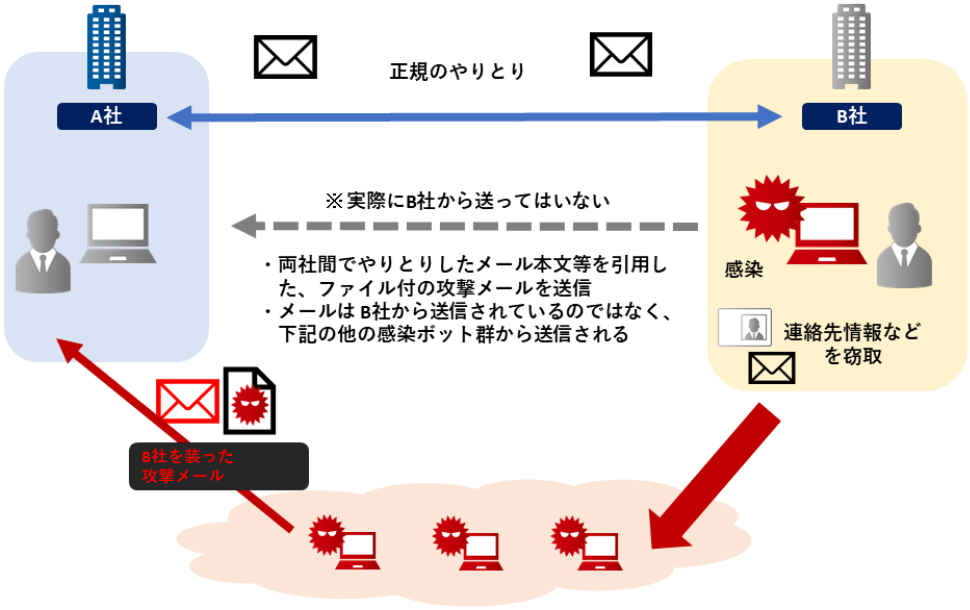
注意喚起情報	URL：https://www.jpcert.or.jp/at/2020.html
マルウェアEmotetへの対応FAQ	URL：https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

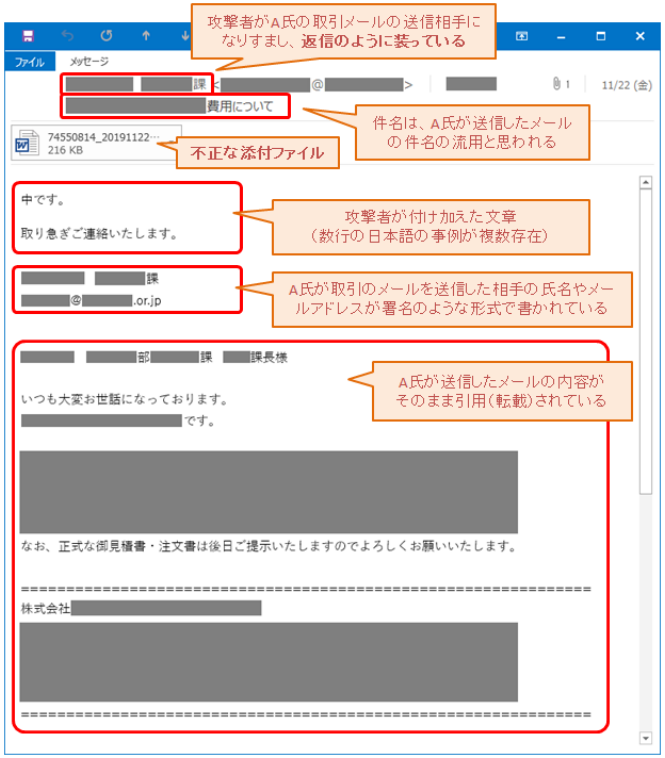
参考資料

Emotet（エモテット）の手口

参考１

- **Emotetとは**
  - Emotetと呼ばれるウイルスへの感染を誘導する高度化した攻撃メールが国内外の組織へ広く着信。
  - 実在の相手の氏名、メールアドレス、メールの内容等の一部を流用して正規のメールへの返信を装っていたり、業務上開封してしまいそうな巧妙な文面となっている場合があり、注意が必要。
- **最近の傾向**
  - 2020年7月末から国内外に向けてEmotetに感染させるメールの配信活動が再び活発化。過去に感染した被害組織から窃取された情報を使ってなりすまされたメールが配信されている状況。
  - Emotetは、情報の窃取等の直接攻撃に悪用されることに加え、他のウイルス等による攻撃の侵入口として悪用されるウイルスでもあり、一度感染すると拡散していく傾向。



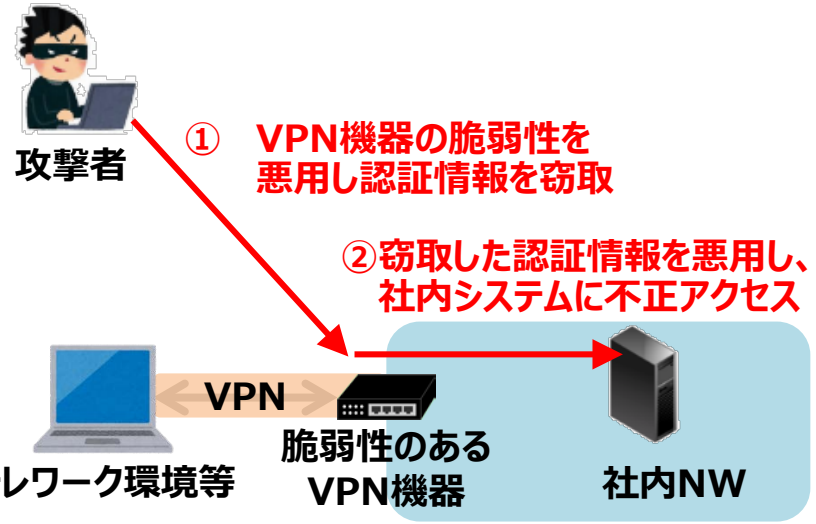


ネットワーク貫通型：VPN機器の脆弱性を悪用したネットワークへの侵入

参考２

- **VPN機器の脆弱性**が相次いで報告され、そうした脆弱性を**悪用するコードが公開**されるなど深刻な状況が発生。**攻撃者はこうした脆弱性を通じて直接的に社内ネットワークへ侵入**し、攻撃を展開。
- 2020年8月、Pulse Secure製VPN機器の脆弱性が悪用され、**国内外900以上の事業者からVPNの認証情報が流出**。2020年11月、Fortinet製品の**VPN機能の脆弱性の影響を受ける約5万台の機器に関する情報が公開。 認証情報等が悪用されることで容易に侵入されるおそれ。**
- **どちらのケースも既に悪用されている可能性**があるため、**機器のアップデートや多要素認証の導入といった事前対策**に加え、事後的措置として**侵害有無の確認や、パスワード変更等の対応**が必要。

VPN機器に対する不正アクセス



Pulse Secure製VPN機器の脆弱性

2019年4月	脆弱性情報公開
2019年8月	脆弱性の悪用を狙ったとみられるスキャンを確認
2019年9月	脆弱性を悪用したとみられる攻撃を確認
2020年8月	国内外900社（国内は38社）の認証情報が公開

Fortinet製FortiOSの脆弱性

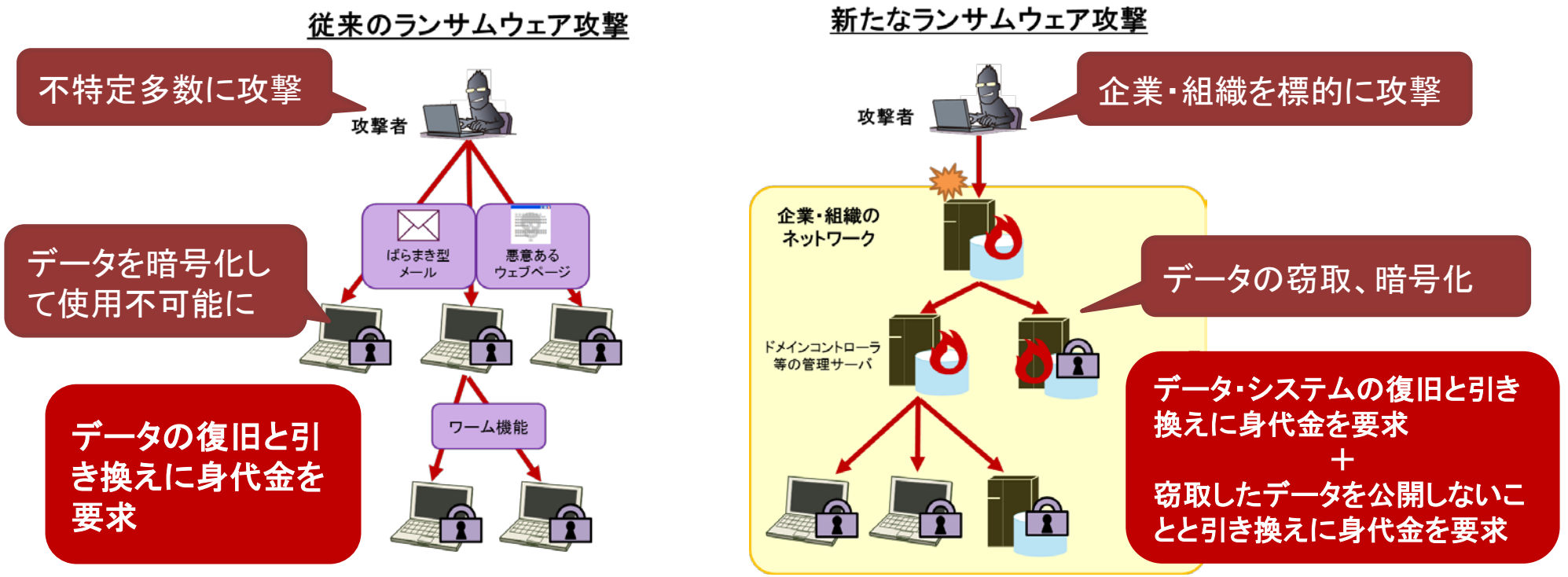
2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等

https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

ランサムウェア（Ransomware）とその手口の変化（二重の脅迫）

参考３

- **ランサムウェアとは**
  - 「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語。
  - 感染したパソコンのデータを暗号化するなど使用不可能にし、その**解除と引き換えに金銭を要求**する。
- **新たな（標的型）ランサムウェア攻撃（二重の脅迫）とは**
  - ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを窃取した後に一斉に暗号化してシステムを使用不可能にし、脅迫をするサイバー攻撃。
  - システムの**復旧に対する金銭要求**に加えて、窃取した**データを公開しない見返りの金銭要求**も行うので、**二重の脅迫**と恐れられる。窃取された情報に顧客の情報や機微情報を含む可能性がある場合には、被害組織は**より困難な判断を迫られること**になる。

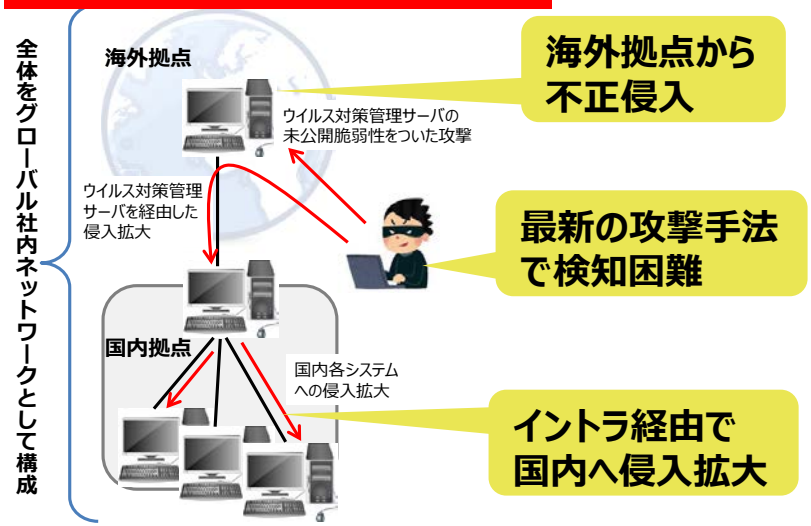


海外拠点経由の攻撃

参考４

- ビジネスのグローバル化に伴って、**海外拠点とのネットワークを国際VPN等によりWAN（広域社内ネットワーク）に取り込んで構築**しているケースが増加。海外とのビジネス効率化に寄与する一方で、**海外拠点への不正侵入によって、即国内ネットワークまで侵入される危険も**伴っている。
- 海外拠点（海外支社の他、関連会社、提携先、取引先等を含む）においては様々な原因により、日本国内と同等なレベルのセキュリティ対策が十分に取れないケースが多い。
  - 安価だが品質管理が不十分なソフトウェアが利用されている（コピー版等の利用により最新の脆弱性管理が適用されない）
  - 本社のガバナンスが行き届かず、システムの脆弱性が放置され、インシデントの監視・対応体制も十分に確保できていない
  - 従業員教育が十分でなく、私用機器やソフトウェアなどが許可なくシステムに接続されている
  - 信頼性の低いプロバイダを利用せざるを得ない　等
- このような国内環境よりも脆弱な**海外拠点において不正侵入を許してしまい、そこを足掛かりに、国内システムの奥深くまで到達されるケースが増加。**

A社事案における攻撃ルート



B社、他数社の事案の概要

- 指定秘密等の重要情報の漏えいは免れたとされている。
- ただし、攻撃者は社内の複数のシステムを渡り歩き、B社事案ではサーバ上の27,445件のファイルが不正アクセスを受けるなど、システム内部にかなりの侵入を許してしまっていた。
- 検知が遅れていれば、さらなる広範なシステムへの侵入を許していた可能性もある。

重要情報に係わるシステム分離、脆弱性対策の迅速なアップデート適用、振る舞い検知など最新の対策導入が重要

最近のサイバー攻撃の状況を踏まえた経営者への注意喚起

2020年12月18日
経済産業省
商務情報政策局
サイバーセキュリティ課

はじめに

2020 年に入ってから、新型コロナウイルスの感染拡大に伴い、テレワークの利用の急拡大など、サイバー空間を巡る環境が大きく変化している。また、サイバー攻撃の攻撃者による攻撃の痕跡の消去などサイバー攻撃の手法の高度化・巧妙化が進むとともに、中小企業等のサプライチェーン上の弱点を起点とする攻撃の拡大が見られる。

こうした変化に対応し、サイバーセキュリティの強化を促進すべく、4 月 17 日に産業サイバーセキュリティ研究会から「産業界へのメッセージ」[1]が発信され、6 月 12 日には経済産業省が「「昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い」に対する報告結果及び「中小企業向けサイバーセキュリティ事後対応支援実証事業（いわゆる「サイバーセキュリティお助け隊」）」の事業報告を踏まえた昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」[2]（以下「昨今の状況認識」という。）を公表し、高度化が進むサイバー攻撃に関する注意喚起を実施してきた。

さらに、攻撃者がサプライチェーンの中で最も脆弱な部分を狙って攻撃起点の構築を図るようになっていることを受け、産業界が一丸となってサプライチェーンのサイバーセキュリティに取り組んでいくため、経済団体が中心となり、11 月 1 日にサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）が発足した。[3]

サイバーセキュリティを強化するためのこうした取組は着実に進められているが、一方で、サイバー攻撃の起点の拡大や烈度の増大は続いており、我が国企業が、規模の大小を問わずサイバー攻撃の被害に遭っている事例が数多く確認されている。

---

[1] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf
[2] https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html
[3] https://www.meti.go.jp/press/2020/10/20201030011/20201030011.html
https://www.ipa.go.jp/security/keihatsu/sme/sc3/index.html

そこで、改めて、最近見られる攻撃の特徴とその攻撃目的を明らかにし、企業やその関係機関等が対応する際に注意する点を整理し、サイバーセキュリティの取組の一層の強化を促すこととした。

１ 今次注意喚起の趣旨

（1） 中小企業を巻き込んだサプライチェーン上での攻撃パターンの急激な拡がり

昨今、中小企業を含む取引先や海外展開を進める企業の海外拠点、さらには新型コロナウイルスの感染拡大に伴うテレワークの増加に起因する隙など、攻撃者が利用するサプライチェーン上の「攻撃起点」がますます拡大している。

まず、昨年来、取引先との正当なやりとりを装うなど高度化したウイルスメール攻撃である Emotet のように、サプライチェーン上のセキュリティ対策や対策意識の弱い企業を足掛かりとして攻撃を広げる活動が活発化している。実際、中小企業が Emotet に感染した結果、当該中小企業の端末やメールアドレスなどが攻撃に利用され、取引先に対する攻撃の起点になってしまい、攻撃先の企業が更に Emotet に感染するといった悪循環に陥ったケースも多く発生している。企業等の担当者間の信頼関係を悪用する攻撃には、今後も注意が必要である。

攻撃者はこうした活動によって多数の攻撃起点を確保することで、情報の窃取やランサムウェア（マルウェアに感染したサーバ内のデータを暗号化して使用不能とするとともに、データの復元と引き替えに身代金（ランサム）を要求するサイバー攻撃の手法）による金銭取得を狙った二次的な攻撃に入るようになっている。

また、ビジネスメール詐欺（Business Email Compromise：BEC）による金銭取得の被害も国内企業・組織で多く発生している。取引先や、企業の CEO・役員などになりすましたメールを送信することで、正規の取引を装い、攻撃者の偽の口座に振り込みをさせる手口である。なりすましメールの中には過去のメールを引用することで、信頼させるようにするなど、巧妙に細工されているため、取引を行う際には十分な注意が必要である。

次に、グローバル化に伴って海外拠点ネットワークとの密連携のシステム（国際 VPN により社内ネットワークを海外拠点につなげる仕組み）が増加しているが、海外拠点のセキュリティ対策を十分に確保できないこと(技術面、海外側プロバイダの制約、セキュリティリテラシの低い社員等）が原因で、海外拠点に最初に侵入され、その後、拠点間ネットワークを通じ、国内拠点に侵入してくる攻撃手口も増加している。

加えて、世界的な新型コロナウイルスの感染拡大に伴い、日本企業においてもテレワークの利用が急増しているが、テレワークを実現するための VPN 機器の脆弱性

が悪用され、攻撃者が直接的に組織内ネットワークに侵入してくるケース（ネットワーク貫通型の攻撃）が増加している。VPN 機器は、企業内で意識的に管理されるサーバ等と異なり、ネットワークサービスの一部として提供されるケースもあり、運用体制や脆弱性対応の責任が不明瞭なケースも多い。その結果、脆弱性が放置されやすく、攻撃者に侵入起点として悪用されるというサプライチェーン上の問題を抱えている。その他、社員が社外からリモート接続する際に何らかの方法で社員端末に侵入し、社員端末経由で組織内ネットワークに侵入されたという事案も確認している。

このようにサプライチェーン全体において、攻撃パターンの多様化によって攻撃起点が一気に拡がっている状況にある。

（2）大企業・中小企業等を問わないランサムウェアによる被害の急増

新型コロナウイルス感染症の世界的な流行による経済の不安定化などにより、直接的に金銭を求める攻撃が急増している。特に、暗号化したデータを復旧するための身代金の要求に加えて、暗号化する前にあらかじめデータを窃取しておき、身代金を支払わなければデータを公開するなどと脅迫する、いわゆる「二重の脅迫」を行うランサムウェア攻撃の被害が国内でも急増しつつある。以下は、ランサムウェア攻撃の深刻さを伺い知る上で参考になるセキュリティサービス企業による最近の調査結果の抜粋である。

- ある調査[4]では、日本の IT セキュリティ担当者 200 人のうち、半数を超える 52%が、この 1 年間で「ランサムウェア」によるサイバー攻撃を受け、データを暗号化されるなどの被害を受けたと回答。さらに、日本でランサムウェアの被害にあった組織のうち、32%が、暗号化されたデータを復元するためのいわゆる「身代金」を犯行グループに実際に支払ったと回答。支払った額の平均は、110 万米ドル（約 1 億 1,400 万円）。
- 別の調査[5]によれば、ランサムウェアの攻撃を受け、身代金を支払った組織の被害額は平均で 144 万 8,458 米ドル（約 1 億 5,000 万円）。要求に従わなかった組織の被害額は、その約半分の 73 万 2,520 米ドル。
- 日本企業のランサムウェア被害額は世界 2 位。身代金支払いを除く、事業停止によって発生する損失や運用コストなどの損失額で、日本は約 219 万 4,600 米ドル（約 2 億 2,800 万）。
- 2019 年にランサムウェアの被害を受けた企業は日本では 42%と世界平均（51%）よりも低いが、データが暗号化される前に被害の発生を阻止した割合は、世界平均（24%）に対して日本は 5%と調査対象になった国（26 か国）の中では最下位。

---

[4] CrowdStrike,「2020 CrowdStrike Global Security Attitude Survey」

[5] Sophos,「ランサムウェアの現状 2020 年版」

こうしたランサムウェア攻撃の増加の背景としては、RaaS（Ransomware as a Service）とも呼ばれる、マルウェアの開発者と当該マルウェアを使って攻撃を行う攻撃者などで構成される、ランサムウェアの提供や身代金の回収を組織的に行うエコシステムが成立したことにより、高度な技術を持たなくても簡単に攻撃を行えるケースが増えていることなどが挙げられる。

（3）機微性の高い情報の窃取等を目的としたと考えられる海外拠点を経由した攻撃の深刻化

昨今、機微性の高い情報を取り扱う企業においても、ビジネスのグローバル化に伴って海外拠点ネットワークと密連携のシステムを構築するケースが増えている。一方、海外では十分なセキュリティ対策を取れないケースが存在する上、国・地域によっては、その国・地域で広く流通するソフトウェアの品質管理が不十分で脆弱性が修正されないまま放置されていたり、開発過程等でバックドアとして利用可能な脆弱性が混入したまま出荷されていたりするケースも存在する。

このように、海外拠点と日本では、インターネット環境を含め、システムが直面する環境が異なる。しかし、企業によっては、そのことを十分に理解せず、適切な対策を取らないまま、海外のシステムと日本国内のシステムをつなげてしまった結果、海外拠点で侵入経路を構築され、そこから国内に侵入されるリスクを増大させてしまっているケースが存在する。

２ サイバー攻撃の事例

（1）Emotet の事例（攻撃起点の多様化１）

- 事例1（海外地方自治体）
  - 職員が開封したメールのリンクを開いたところ、Emotet に感染。この Emotet により同一ネットワーク内の PC に別のランサムウェア「Ryuk」がインストールされ、PC 内のあらゆるファイルが暗号化された。これにより、合計 16TB のデータがロックされ、ほぼ全てのサーバ・電話・電子メールが使用不能となった。
  - 42 ビットコイン（当時約 50 万米ドル相当）が身代金として犯人に支払われた結果、データを復号できたが、IT 責任者は解雇された。
- 事例2（国内企業）
  - 取引先を装ったメールの添付ファイルを開いたことで社内の PC が Emotet に感染。当該 PC に保存されていた過去のメール送受信履歴が流出し、これに含まれるメールアドレスに対して、同社社員を名乗る不審なメールが送付された。

- 事例3（国内企業）
  - 取引先を装ったメールの添付ファイルを開いたことで社内の PC が Emotet に感染。当該 PC からさらに組織内外へウイルスメールが送信され、別の従業員が当該メールの添付ファイルを開いたことで組織内の複数台の PC に感染が拡大した。

（2）ランサムウェアの事例

- 事例1（国内企業）
  - 社内ネットワークの構成や端末の設定等を管理するサーバにランサムウェアが入り込んだことにより、グローバルネットワークに接続している複数拠点の複数の PC が暗号化される被害が発生。社内の情報システムが使用できなくなり、一時操業停止に。
- 事例2（国内企業）
  - ランサムウェアの感染によりデータが窃取、削除されるとともに、システムの一部に障害が発生。攻撃者を名乗るグループがインターネット上に犯行声明を掲載し、窃取した情報の公開停止と引き替えに身代金を要求。実際に情報の一部も公開された。

（3）海外拠点から侵入された標的型攻撃の事例（攻撃起点の多様化２）

- 事例1（国内企業）
  - 中国拠点にあるウイルス対策管理サーバが外部から侵入され、拠点内で感染が拡大。さらに中国拠点から国内拠点にも同様の手法で侵入。検知を遅らせるためと思われるが、正規の Windows アプリ（PowerShell）を用いた痕跡を残さない攻撃手法が使用された。
- 事例2（国内企業）
  - 攻撃者は、顧客向けサービスの監視や障害の切り分けなどを担うシンガポールの運用サーバに侵入。その後、タイなど複数の海外拠点を経由し、国内の運用サーバに入り込み、法人向けクラウドサービスの情報管理サーバのほか、社内セグメントのアクセス権限の管理等を行うサーバやファイルサーバへと侵入。
  - 2 段階認証を導入していたが、攻撃者により無効化され、認証を突破された。
- 事例3（国内企業）
  - 国内企業の海外拠点に設置された VPN 製品の既知の脆弱性を悪用して侵入し、遠隔操作機能を持つバックドアが設置された。バックドアは侵入時点ではウイルス対策ソフトの検知を逃れていたこと、正規プログラムの一部に紛れ込んでいたことから、初期段階での発見は困難だった。

３ 対応

（1）経営者の方々へ

① サイバー攻撃による被害が深刻化し、被害内容も複雑になっており、経営者の一層の関与が必要になっている

経済産業省では、サイバーセキュリティ経営ガイドライン [6]を公表し、経営層のリーダーシップによってサイバーセキュリティ対策を推進していくことを強く求めてきた。当該ガイドラインのダウンロード数は 97，000 件を超える [7]など、サイバーセキュリティの重要性に対する経営者の認識は着実に広まってきていると考えている。

しかしながら、昨今のサイバー攻撃は格段に高度化・複雑化し、被害が発生した場合の事業活動への影響や損害額の規模、社会的評価への影響なども一層深刻なものとなってきており、サイバーセキュリティは今や最大の事業リスクの一つになっていることを改めて認識することが必要である。

また、被害の形態も自社に閉じるものではなく、サプライチェーンを含む様々な関係者を巻き込む複雑なものとなってきており、実務者がこれまでの取組を継続するだけでは対処できなくなっている。

特に、技術的な対策だけでは対応できず、事業運営の方法そのものの見直しを必要とするようなリスクへの対応や、被害が発生した場合に巻き込んでしまった取引先、顧客等の関係者との調整や事業継続に係る判断など、経営者でなければ判断・対応ができないケースが現実に発生するようになっている。

ソフトウェアのアップデートを適切に実施するなどの基本的な対策を徹底するとともに、改めて、経営者のリーダーシップが必要になっているということを深く認識することが、現在直面している激しいサイバー攻撃への対応の第一歩である。

② ランサムウェア攻撃によって発生した被害への対応は企業の信頼に直接関わる重要な問題であり、その事前対策から事後対応まで、経営者のリーダーシップが求められる

ランサムウェアを使った攻撃による被害は世界的規模で深刻化し、被害規模も増大の一途をたどっている。残念ながら、ランサムウェア攻撃は攻撃者が“収益”を上げやすい構造へと変化し、収益性が高い分野と認識されていることから、ランサムウェア攻撃を行うための環境を提供するサービスまで現れるようになっており、ランサム

---

[6] https://www.meti.go.jp/policy/netsecurity/mng_guide.html

[7] 2020 年 11 月末時点

ウェア攻撃は激化していく方向にあることが強く懸念されている。

ランサムウェア攻撃は攻撃環境を含めて日々高度化しているが、最近の攻撃パターンの変化もあり、経営者としては、特に以下の2つの点について、企業の信頼そのものに関わる問題として、自らリーダーシップを発揮して対応を進めることが必要である。

一つは、二重の脅迫という形で、自社で保有するデータ等を単に暗号化して使えなくすることによる事業妨害だけでなく、暗号化する前にあらかじめデータを窃取しておき、支払いに応じない場合には当該データを公開すると脅すことで支払わざるを得ない状況に追い込むようになっていることである。つまり、自社が事業継続上の影響を受けるだけでなく、保有する顧客、取引先等のデータが公開されることによって、自社がランサムウェア攻撃による被害を受けたことで、関係者にまで被害を与えるおそれがあるということである。

したがって、データをバックアップしておくだけでなく、関係者に甚大な被害を与える可能性があるデータは普段から暗号化して管理し、公開されても影響がないように事前に対策を講じておくなどの事前対策を強化しておく必要がある。こうした対策を実行するためには、これまでの日常的な業務運用の変更を伴うことから、経営者のリーダーシップが欠かせない。

もう一つは、金銭の支払いに関する問題である。データ公開の圧力から、攻撃者からの支払い要求に屈しているケースは少なくないとの報告は存在するが、こうした金銭の支払いは犯罪組織に対して支援を行っていることと同義であり、また、金銭を支払うことでデータ公開が止められたり、暗号化されたデータが復号されたりすることが保証されるわけではない。さらに、国によっては、こうした金銭の支払い行為がテロ等の犯罪組織への資金提供であるとみなされ、金銭の支払いを行った企業に対して制裁が課される可能性もある。こうしたランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである。

金銭の支払いに対する対応は、複数の視点から自社への信頼をどのように維持するか、また、犯罪助長行為として支払い行為に対する制裁を用意する国もある中でコンプライアンス上の問題にどう対応するか、ということであり、経営者が判断すべき経営問題そのものであるということを強く認識する必要がある。

③ サイバーセキュリティを踏まえた事業のグローバル・ガバナンスを構築する必要がある：海外拠点をシステム統合する際の留意点

企業がよりスピーディーかつ効果的に事業をグローバル展開していくために、国内と海外拠点のシステムをより深いレベルで連携するようになり、システムを統合する方向へ動きが加速している。こうしたシステム統合によって情報共有の高速化やより広い範囲でのデータ連携などが大きく進む一方、事前に十分なリスク評価を行うこと

なく、インターネット環境やデータ管理に係る規制等が大きく異なる国・地域にあるシステムを、国内にあるシステムに連携させることで、統合されたシステムにセキュリティ上の脆弱性を持ち込んでしまうリスクがある。

例えば、個人情報などのデータの取扱いに関して独自のルールを既に導入している国・地域は少なくないが、こうした場合、データの取扱いに関するルールの違いから、システムを統合してもデータを一方向にしか流通させることができなくなったり、システムを統合していてデータを管理しているサーバが実際には国外にある場合に、国内では制度的に企業秘密として保護されるデータであっても当該サーバが存在する国のルールが適用されて公的機関に提出を求められたりする可能性は存在する。

また、国・地域によってインターネット環境や IT 産業の状況は異なっており、バックドアになる可能性のある脆弱性等の問題が混入したソフトウェアが出荷されたり、脆弱性等の問題に対応するための基盤が整っておらず、広く流通しているソフトウェアの脆弱性が修正されないまま放置され、通信環境全体に攻撃者が利用できる攻撃起点が拡散してしまったりしているようなケースも存在する。

こうしたリスクは、システムの技術的な対応だけでは十分に管理することが難しく、社内における拠点間や部門間における情報共有ルールの設定なども含めて日常的な業務運用で対応することが必要である。

海外拠点を含めたシステムの統合を進めるに当たっては、拠点を展開する国・地域の環境をしっかりと評価し、システムを連携させ、データ等を交換する場合に発生するリスクを最小化するために、各海外拠点のリスク等に応じてセグメンテーションなどを施したシステム・アーキテクチャの導入や情報共有のルール化など、システムの技術的な対応だけでなく、グローバル・ガバナンスの観点から、経営者がシステム統合のメリットとデメリットを踏まえて統合レベルの決定と設定した事業戦略に適した運用体制の構築を主導することが必要である。

④ 改めて「基本行動指針（共有・報告・公表）」に基づいた活動の徹底を

6 月 12 日に公表した「昨今の状況認識」では、サプライチェーンを他の企業とともに構成していることに伴う責任と、企業が負っている社会的な責任を果たしていくために、以下の3つについて実際のアクションとして取り組んでいく必要があることを訴え、6 月 30 日に開催された産業サイバーセキュリティ研究会において、これら3つの項目を「基本行動指針」として提示した。

①サプライチェーンを共有する企業間におけるサイバー事案に関する高密度な情報共有の実施

②機微技術情報の流出懸念がある場合の経済産業省への報告

③情報漏えい等の被害が取引先等不特定多数の関係者に影響するおそれがあ

る場合における関係者の影響緩和の取組促進のための公表の実施

11 月 1 日に発足した SC3 の規約においても、「基本行動指針」の内容が反映されており、産業界が一丸となってサイバーセキュリティの強化に取り組んでいく上での重要な指針となっている。

経営者は、改めて「基本行動指針」に則った事案への対処を進めるよう、担当責任者及び担当部局に指示し、自社に対する社会的な信頼と産業界全体の取組の強化に貢献していく姿勢を明確にすることが求められる。

（2）経営層がセキュリティ担当者に対応状況を確認すべきこと

これまで説明した最近のサイバー攻撃の動向を踏まえて、セキュリティ担当者が特に確認・実施するべき事項について、「サイバーセキュリティ経営ガイドライン Ver.2.0」の指示事項に従って整理する。

① サプライチェーン全体でのセキュリティ対策の重要性

Emotet が起点となり、高度なサイバー攻撃に発展する事例が確認されていることから、取引先等が Emotet 及び類似のマルウェアに感染している状況を認識しながら放置するようなことはせずに、サプライチェーン全体で迅速に脅威に対応していくことが求められている。

また、VPN 機器については、VPN 機器を利用したサービスのサプライチェーンの構造が複雑で責任主体が不明瞭なことが原因で、脆弱性対策が放置される傾向にある。外部委託のサービスを利用する場合であっても、自社へのリスクを正確に把握し対応することが求められている。

- 指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
  - Emotet は取引関係者間などで感染が拡大することから、社会全体での「声がけ」「助け合い」が重要となる。例えば、取引先を装う不審なメールを受信した場合には、取引先が感染に気づいていないケースも想定して、取引先を含めた関係者に状況を共有することが求められる。
  - VPN サービスを利用する場合、VPN 機器については、SIer、インターネット・サービス・プロバイダー（ISP）や運用保守ベンダ等の事業者が設置し運用するケースがあるが、さらに、これらの事業者が VPN 機器を入手する経路が、機器メーカー⇒代理店⇒リセラーと多層のサプライチェーン構造になっているケースが多い。このサプライチェーン構造の中で、メーカー公表の脆弱性情報や注意喚起情報が伝達されず、エンドユーザが修正の必要性に気づかずに放置されている間に攻撃者に侵入されるケースが確認されている。VPN

機器・サービスを利用する場合においては、このようなサプライチェーン構造を正確に把握すると共に、エンドユーザ自らが積極的に最新の脆弱性情報を把握し、対策をしていくことが必要である。

② 攻撃の巧妙化： ランサムウェア攻撃の防御、被害の局所化のために

悪質化するランサムウェア攻撃からの防御、被害の局所化のために確認・実施するべき事項について整理する。なお、ランサムウェアに対する対策については内閣サイバーセキュリティセンター（NISC）[8]からも、2020 年 11 月 26 日に「ランサムウェアによるサイバー攻撃について【注意喚起】[9]」が公表されているので、あわせて参照いただきたい。

- 指示5：サイバーセキュリティリスクに対応するための仕組みの構築
  - 保有資産の守りを固める。
    - ✧ VPN 機器を含め保有資産へのアクセス経路となり得るシステムに対して、最新のセキュリティパッチを当てるなど、脆弱性対策を徹底する。
    - ✧ クラウドサービス等を利用する場合に多要素認証を導入する。
    - ✧ Data Loss Prevention（DLP）などを導入する。
  - 保有資産の「盗む価値」を下げる。
    - ✧ 外部環境では復号できないように、重要な情報を暗号化する。
    - ✧ Information Rights Management（IRM）などを導入する。
- 指示6 サイバーセキュリティ対策における PDCA サイクルの実施
  - ステークホルダとの対話。
    - ✧ 取引先・顧客・株主・社員等とのコミュニケーション、情報開示
      - ✓ 身代金を支払わないことにより、顧客等の情報が漏えいする可能性がある。平常時からリスクに関する情報開示や、セキュリティ対策に関する取組姿勢を伝えておくことにより、緊急時の対応方針について理解を得られるようにしておくことが重要。
      - ✓ ステークホルダの不安を増大させたり、漏えい被害を拡大させたりしてしまうことがないように、事案についての公表時期、公表内容については慎重に検討する必要がある。
- 指示7：インシデント発生時の緊急対応体制の整備
  - 迅速な初動対応
    - ✧ 被害範囲の特定と、被害拡大の防止のためのネットワーク遮断等を実

[8] https://www.nisc.go.jp/
[9] https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf

施する。

- ✧ (独)情報処理推進機構(IPA)、(一社)JPCERT コーディネーションセンター(JPCERT/CC)へ相談する。
- ✧ 犯行グループへの対峙。
  - ✓ 一般論としては、ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むべきものである。
  - ✓ 金銭の支払いに応じてしまった場合、制裁対象(米国財務省外国資産管理室(OFAC)等)になる可能性がある。
  - ✓ 支払いに応じた場合、犯行グループから「支払ってくれる国・業界・企業」として更なる攻撃の対象になりかねず、支払いに応じる組織が存在する限り、攻撃は止まらない。
  - ✓ 支払いに応じたとしても、データが復元される、又はデータが公開されないという保証はない。

- ➢ 政府関係機関への報告・届出。
  - ✧ 警察、個人情報保護委員会、所管省庁等への報告・届出の実施。特に報告義務のある事案については、正確かつ迅速な報告が求められる。
  - ✧ 事業形態や漏えいしたデータによっては、欧州の GDPR や米国のカリフォルニア州消費者プライバシー法(CCPA)など海外の法制度の報告対象になる場合があることにも留意すること。

- 指示8:インシデントによる被害に備えた復旧体制の整備
  - ➢ 保有資産を破壊されても事業継続できるようにする。
    - ✧ 定期的にデータをバックアップし、バックアップからシステムを復旧できることの確認、訓練を実施する。
    - ✧ システムが復旧するまでの間に業務を止めないための代替手段を整備する。
    - ✧ 再発防止策の実施。
- 指示10:情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供
  - ➢ 情報共有の実施
    - ✧ サイバーセキュリティ協議会、IPA サイバー情報共有イニシアティブ(J-CSIP)、JPCERT/CC、各 ISAC 等への攻撃情報の提供を通じた、社会全体での再発防止への貢献も期待される。

③ 海外拠点経由での侵入防御、被害の局所化のために

海外拠点等経由のサイバー攻撃からの防御、被害の局所化のために確認・実

施するべき事項について整理する。

- 指示4：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
  - 組織における「守るべき資産」について、以下の観点等を参考に確認、見直しを行い、海外拠点（子会社、支店、事務所、研究開発拠点、工場等）等経由で発生し得るサイバーセキュリティリスクについて、把握すること。
    - 海外拠点等を含む IT システム・ネットワーク構成を把握する。
    - 海外拠点等からアクセス可能な国内の IT システム・ネットワークを把握する。
    - 当該 IT システム・ネットワーク上にある「守るべき資産」を把握する。
    - 把握したシステム・ネットワーク等に対する脆弱性対応状況(最新のパッチが適用されているかどうか等)を確認する。
    - 直近では、テレワークの導入増加に伴い、VPN 機器の脆弱性を悪用して侵入される事例や、ドメインコントローラーの深刻な脆弱性（CVE-2020-1472）[通称：Zerologon]を悪用し、組織内で侵害範囲を拡大する事例が多く確認されていることに特に留意する。
    - 安全対策が不十分な状態の端末を用いて、社員が自宅からテレワークのために VPN 接続した際に、マルウェアを持ち込む事例も確認されており、社内のセキュリティ対策が及ばない端末の管理にも注意する必要がある。
    - 守るべき資産を脅かし得るリスクやその発生確率・損害等を検討する。
    - 海外拠点とのシステム統合においては、体力の弱い拠点のセキュリティ対策基準を緩くしてしまいがちであるが、最も弱い拠点が高度な攻撃の侵入起点になることに留意し、リスクを正しく把握する必要がある。
- 指示5：サイバーセキュリティリスクに対応するための仕組みの構築
  - 把握したリスクへの対応策（リスク低減策・回避策・移転策）を検討する。
    - 重要業務を行うITシステム・ネットワーク等の階層化(セグメンテーション)による多層防御を行う。
    - 一部海外子会社の国内ネットワーク・システム等からの切り離し（外部化）を行う。
- 指示9：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
  - システム・ネットワークの監視等を外部委託している場合は、委託先の監視サーバなどの脆弱性対応状況を把握する必要がある。
  - 現地政府等から利用を指定される信頼できないソフトウェアを使用しなけれ

ばならない場合のリスクを把握する必要がある。

④ 改めて恒常的なセキュリティ対策の実施状況の確認を

サイバー攻撃の手法は日々高度化しており、脅威に対抗するためには、セキュリティ対策は一度実施したら終わりではなく、継続的にアップデートし続ける必要がある。本文書に記載の観点だけに限定されることなく、サイバーセキュリティ経営ガイドライン等を参考に、改めて経営層のリーダーシップの下、組織としてセキュリティ態勢の強化に努めていただきたい。

サイバーセキュリティ経営ガイドラインの実践状況を確認するためのツールとして、可視化ツール β版 [10]を公開している。本ツールを利用して、自社の状況を定量的に把握することで、サイバーセキュリティに関する方針の策定、適切なセキュリティ投資の実行等が可能となることを期待している。

(3) セキュリティ担当チームが対処を行うに当たっての参照情報

最新の注意喚起等については以下をご確認いただきたい。

- 内閣サイバーセキュリティセンター(NISC)
  - **注意喚起情報**
    https://twitter.com/nisc_forecast
    - ランサムウェアによるサイバー攻撃について(2020.11.26)
      https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf
- 経済産業省
  - 産業界へのメッセージ (2020.4.17)
    https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/20200417.pdf
  - 昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について (2020.6.12)
    https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html
- (独)情報処理推進機構(IPA)
  - セキュリティ関連情報サイト
    https://www.ipa.go.jp/security/index.html
    - ランサムウェア対策特設ページ:
      https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

[10] https://www.ipa.go.jp/security/economics/checktool/index.html

- ✧ 2020/9/14, テレワークを行う際のセキュリティ上の注意事項
  https://www.ipa.go.jp/security/announce/telework.html

- （一社）JPCERT コーディネーションセンター（JPCERT/CC）
  - ➢ 注意喚起情報
    https://www.jpcert.or.jp/at/
    - ✧ マルウェア Emotet への対応 FAQ：
      https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html
    - ✧ 2020/4/17, Pulse Connect Secure の脆弱性への対策や侵害有無などの確認を
      https://www.jpcert.or.jp/newsflash/2020041701.html
    - ✧ 2020/11/27, Fortinet 社製 FortiOS の SSL VPN 機能の脆弱性（CVE-2018-13379）の影響を受けるホストに関する情報の公開について
      https://www.jpcert.or.jp/newsflash/2020112701.html
    - ✧ 2020/9/25, Netlogon の特権の昇格の脆弱性（CVE-2020-1472）への早急な対応を
      https://www.jpcert.or.jp/newsflash/2020091601.html

4 セキュリティ対策やインシデント対応等に関する相談窓口

セキュリティ対策やインシデント対応でお困りの場合は、以下の相談窓口などをご利用いただきたい。

- IPA
  - ➢ 情報セキュリティ安心相談窓口：
    - ✧ 一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談
    - ✧ https://www.ipa.go.jp/security/anshin/index.html
    - ✧ 電話：03-5978-7509
  - ➢ J-CRAT／標的型サイバー攻撃特別相談窓口：
    - ✧ 標的型サイバー攻撃を受けた際の相談（専門的知見を有する相談員が対応）
    - ✧ https://www.ipa.go.jp/security/tokubetsu/index.html

- ✧ 電話：03-5978-7599

➢ その他（届出・相談・情報提供）窓口：

- ✧ https://www.ipa.go.jp/security/outline/todoke-top-j.html

● JPCERT/CC

➢ インシデント対応依頼：

- ✧ https://www.jpcert.or.jp/form/