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

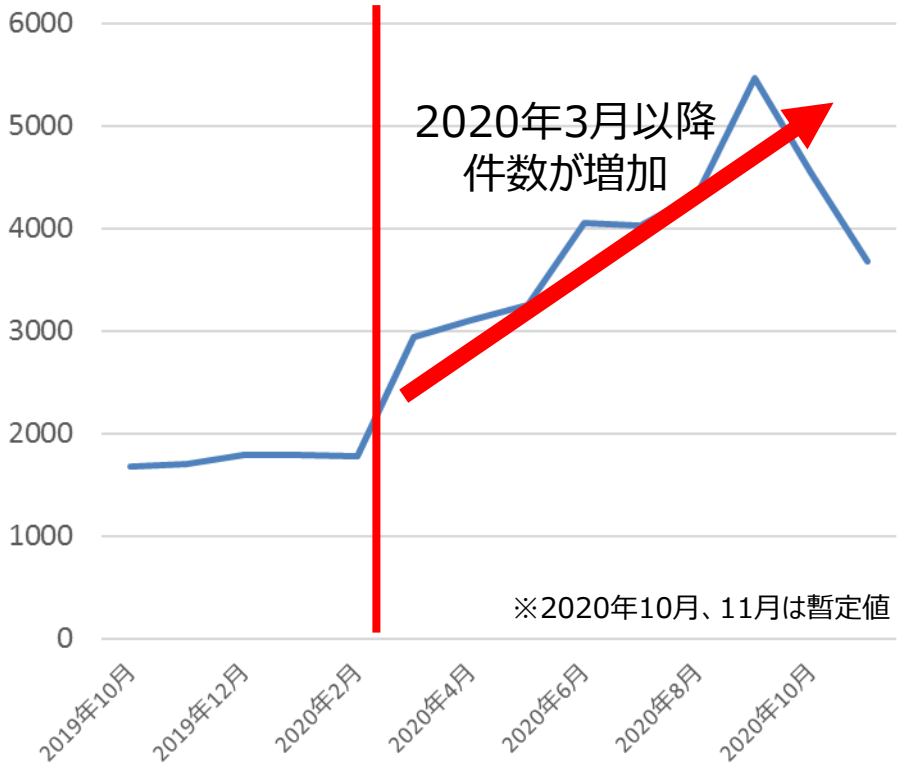
2020年12月18日

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

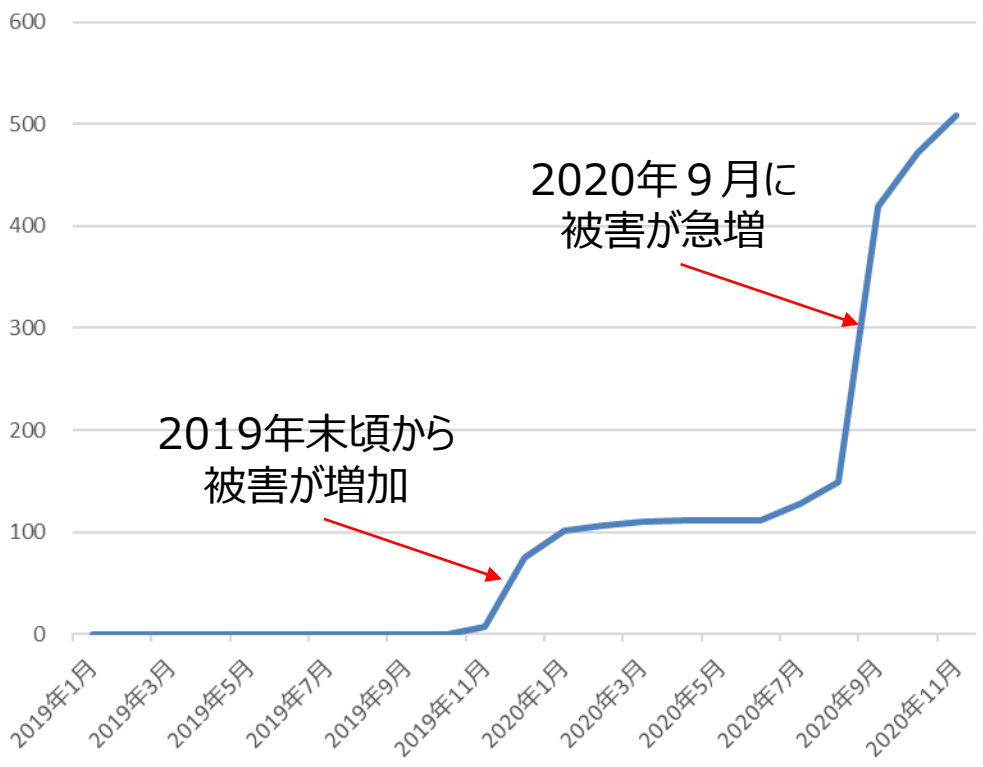
- 新型コロナウイルスの感染が拡大した2020年3月以降、インシデントの相談件数が増加。
- 特に、電子メールを媒介に感染を広げるマルウェア「Emotet※参考１参照」による被害の相談が急増。

JPCERT/CCへのインシデント相談報告件数（月別）



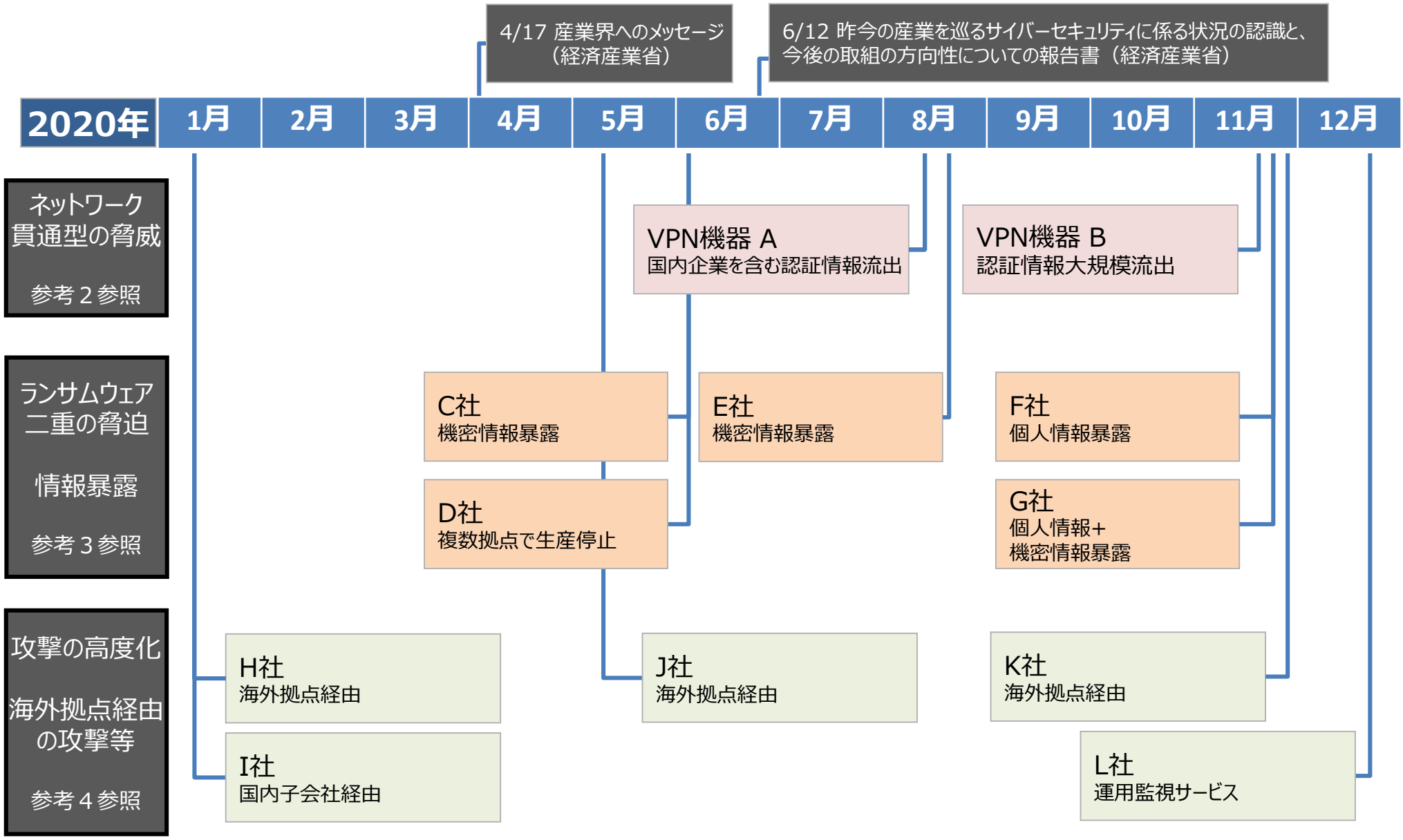
＜（一社）JPCERT/CC＞

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/

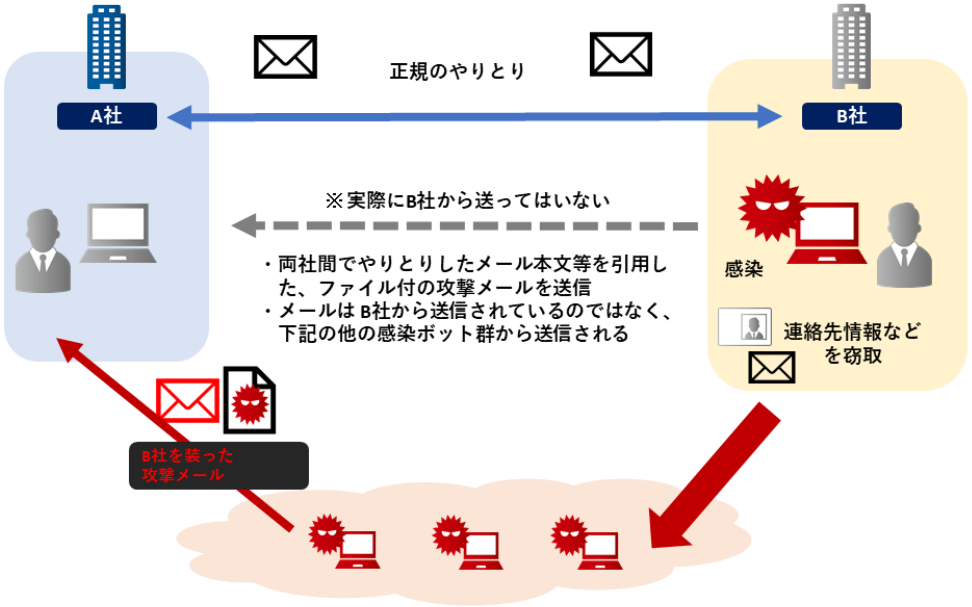
注意喚起情報	URL：https://www.jpcert.or.jp/at/2020.html
マルウェアEmotetへの対応FAQ	URL：https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

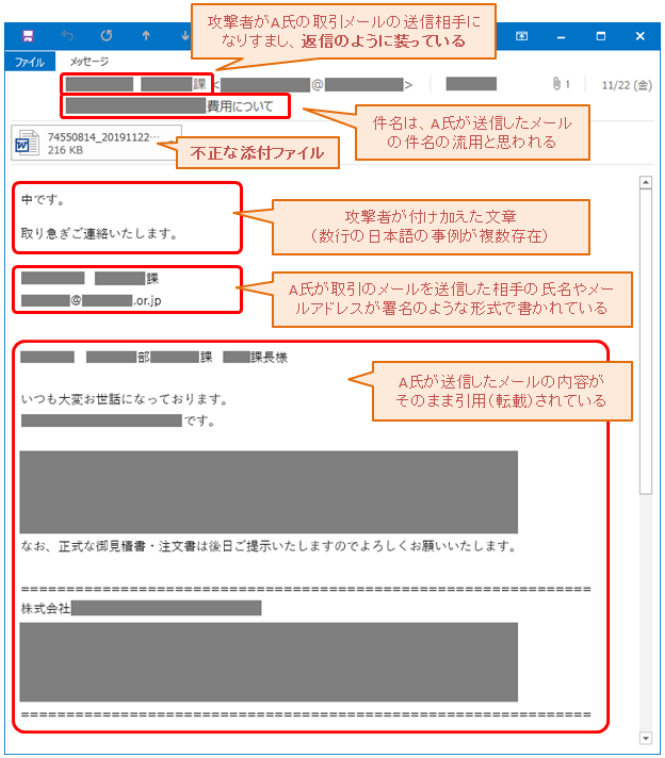
参考資料

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。



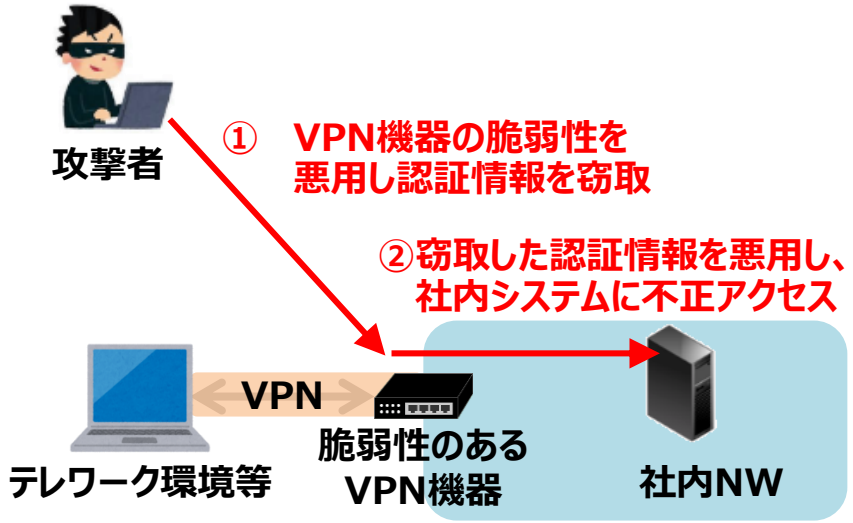


ネットワーク貫通型：VPN機器の脆弱性を悪用したネットワークへの侵入

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

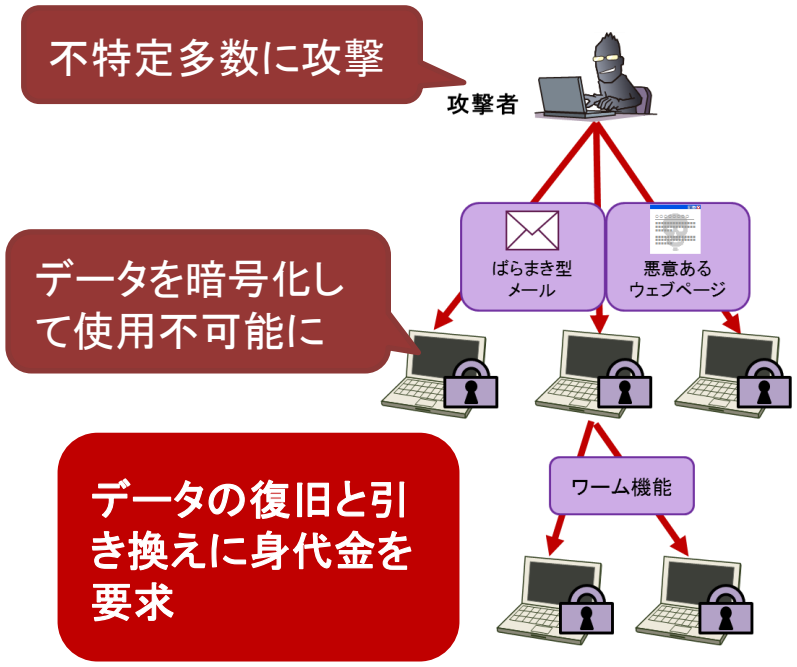
https://www.jpcert.or.jp/newsflash/2020112701.html
https://www.jpcert.or.jp/at/2019/at190033.html

ランサムウェア（Ransomware）とその手口の変化（二重の脅迫）

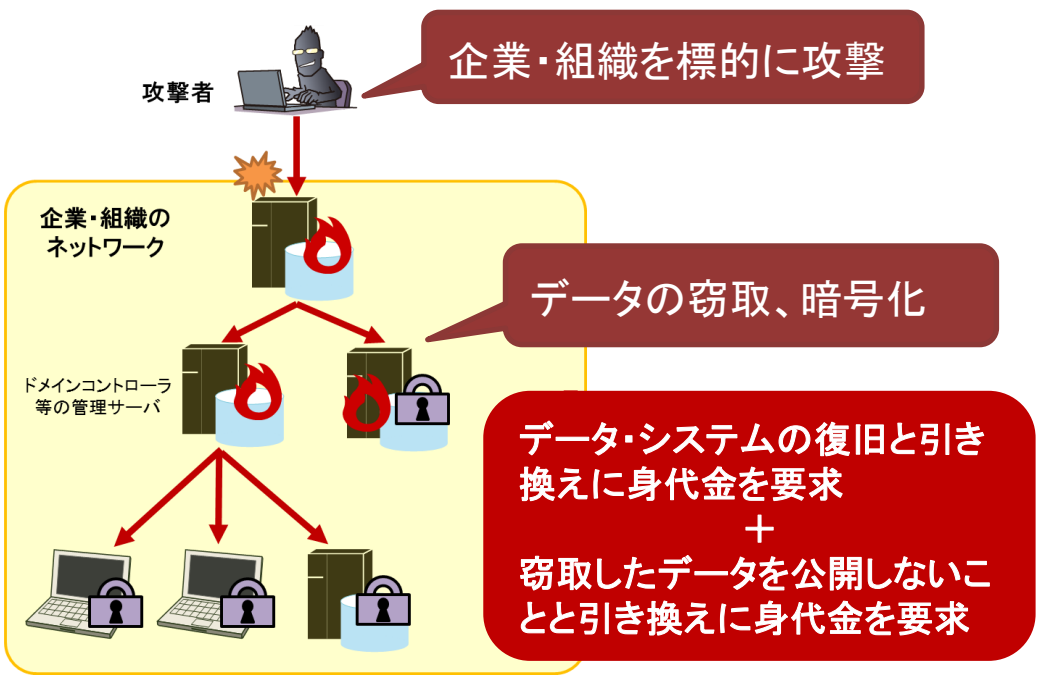
参考３

- **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。

従来のランサムウェア攻撃



新たなランサムウェア攻撃

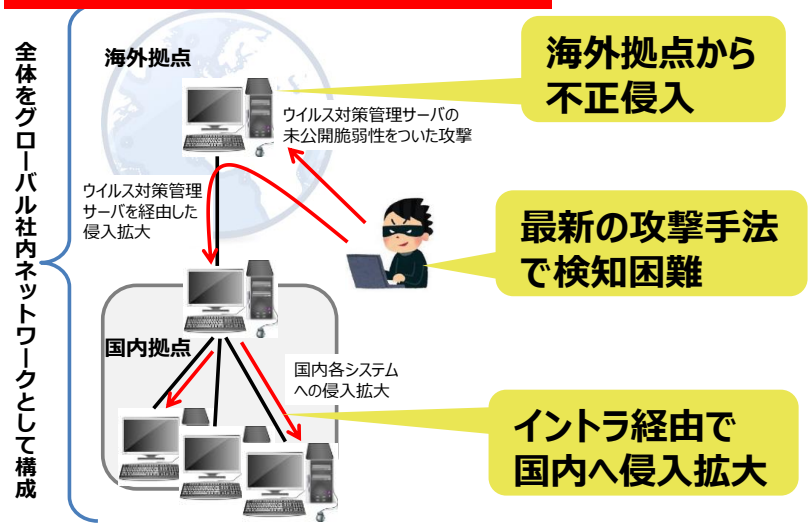


海外拠点経由の攻撃

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