資料2

関係省庁の取組状況について

【総　務　省】

資料２－１　総務省におけるサイバーセキュリティ施策の
取組状況について

【経済産業省】

資料２－２　最近のサイバー攻撃の状況を踏まえた経営者への
注意喚起について

実践的サイバー防御演習（CYDER）

資料２－１

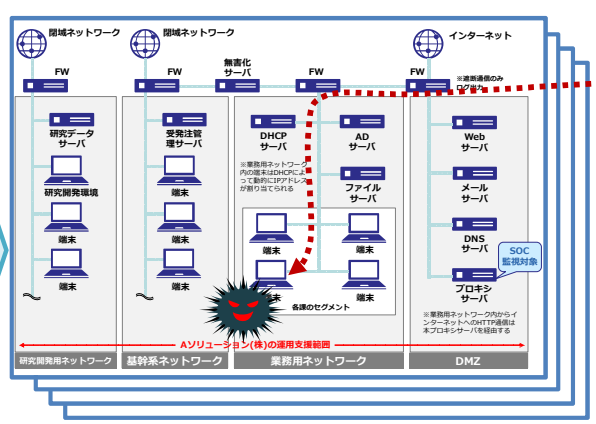
CYDER：CYber Defense Exercise with Recurrence

- 総務省は、情報通信研究機構(NICT)を通じ、**国の機関**、**指定法人**、**独立行政法人**、**地方公共団体**及び**重要インフラ事業者等**の情報システム担当者等を対象とした体験型の**実践的サイバー防御演習**(**CYDER**)を実施。
- 受講者は、**チーム単位で演習に参加。組織のネットワーク環境を模した大規模仮想LAN環境下で、実機の操作を伴って**サイバー攻撃によるインシデントの検知から対応、報告、回復までの**一連の対処方法を体験。**
- **全都道府県**において、年間**100回**・計**3,000名規模**で実施。　参加申込 → https://cyder.nict.go.jp
  ※令和２年度は、74回実施し、2,209名が受講（年和２年末時点）

演習のイメージ

我が国唯一の情報通信に関する公的研究機関である**NICTが有する最新のサイバー攻撃情報を活用**し、実際に起こりうるサイバー攻撃事例を再現した**最新の演習シナリオ**を用意。

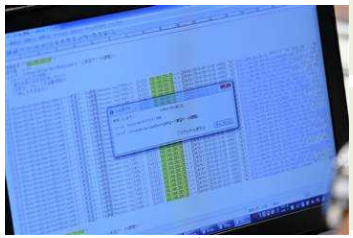
北陸StarBED技術センターの大規模高性能サーバ群を活用



擬似攻撃者

企業・自治体の**社内LANや端末を再現**した環境で演習を実施

受講チームごとに独立した演習環境を**構築**



演習模様 **専門指導員**による補助

チーム内での議論を通じた相互理解

本番同様のデータを使用した演習

インシデント（事案）対処能力の向上

令和３年度の実施計画（予定・調整中）

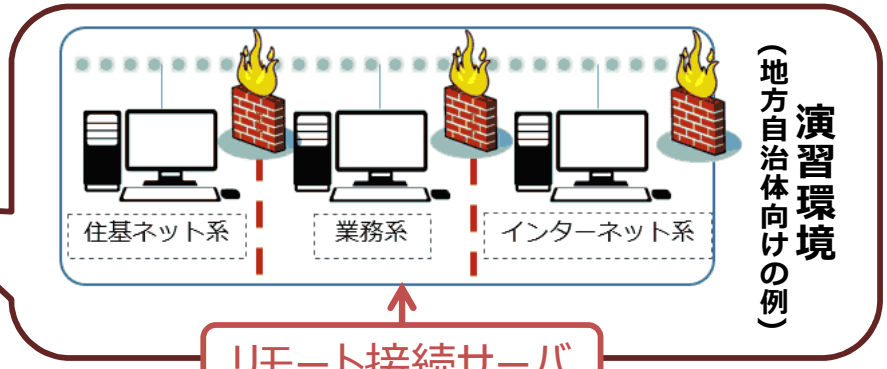
コース名	演習方法	レベル	受講想定者	受講想定組織	開催地	開催回数	実施時期
A	集合演習	初級	システムの運用担当者（システムの利用者レベルを含む）	全組織共通	４７都道府県	６５回	７月～翌年２月
B1		中級	セキュリティ管理業務を主導する立場の者	地方公共団体	全国１１地域	２０回	９月～翌年２月
B2				地方公共団体以外	東京・大阪・名古屋・福岡	１３回	１１月～翌年２月
C		準上級	（詳細調整中）	全組織共通	東京	２回	翌年１月～２月
オンラインA	オンライン演習	初級	システムの運用担当者（システムの利用者レベルを含む）	全組織共通	（受講者職場等）	随時	(調整中)～翌年２月

令和３年度から**新規**開設

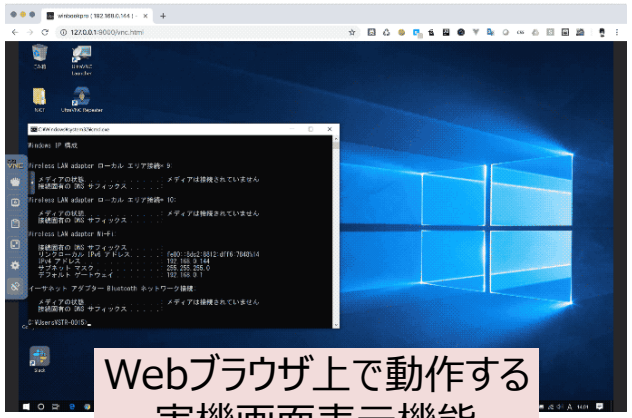
CYDERのオンライン受講

- **感染症拡大防止対策**として、また、**地理的・時間的要因**等によりCYDERが受講できない方への対応として、**オンライン受講環境**を**現在整備中**。
- 令和３年１月から試験提供（クローズβテスト）行い、**令和３年度から本格実施**。
- 自組織のパソコンの**Webブラウザから演習環境に接続**し、**ｅラーニング方式**により演習を**受講**。

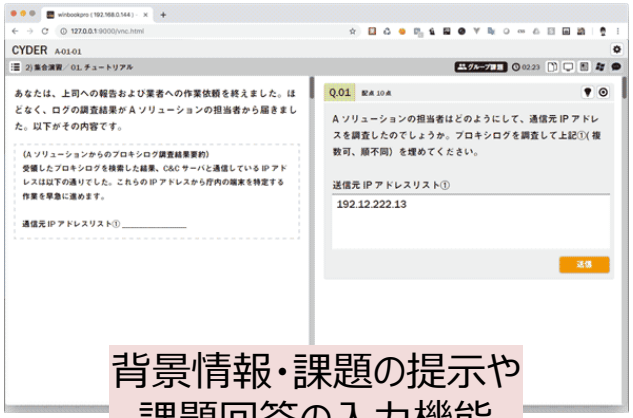
NICT内の大規模計算環境



自身のPC上の**Webブラウザ**において**遠隔受講機能**を利用可能



Webブラウザ上で動作する
実機画面表示機能



背景情報・課題の提示や
課題回答の入力機能

解説表示機能や
チュートリアル表示機能

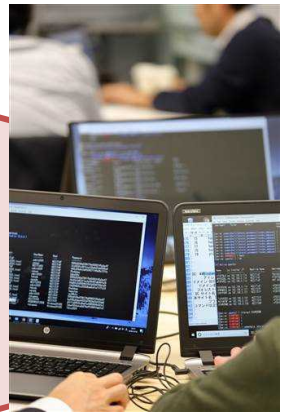
東京大会に向けた実践的サイバー演習（サイバーコロッセオ）

- 高度化・多様化するサイバー攻撃に備え、東京オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象**とした、**高度な攻撃に対処可能な人材の育成**を行う実践的サイバー演習**「サイバーコロッセオ」**を平成30年２月から本格的に実施。
- 大会運営システム等のネットワーク環境を模擬し、**実機演習**により攻撃対処手法を学ぶ**「コロッセオ演習」**に加え、平成30年度からは、**講義演習形式**によりセキュリティ関係の知識や技能を学ぶ**「コロッセオカレッジ」**を実施。
- 令和２年度の事業終了までに、コロッセオ演習で延べ**571名**、コロッセオカレッジで延べ**1,717名**の人材を育成。

サイバーコロッセオ概要

コロッセオ演習

実機演習を伴っての演習
（攻防型演習を含む）



コロッセオカレッジ

講義演習形式により
セキュリティ関係の
知識や技能を学習
（20種の講義科目を開講）

コロッセオ演習の特徴

- 大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を模擬した、演習舞台（仮想ネットワーク環境）を構築。
- 東京大会時に想定されるサイバー攻撃を擬似的に発生させることができるようにし、本格的な攻防型演習等を繰り返し実施。

コロッセオ演習の当日以外でも
学習可能なコンテンツも提供

「**攻防型演習**」とは・・・
受講者が複数チームに分かれ、自組織のネットワークの守備と他チームのネットワークへの攻撃を両方体験することで、攻撃者側の視点をも踏まえたハイレベルな防御手法の検証及び訓練を行う演習

サイバーコロッセオの実施実績

- 実機演習を伴う**コロッセオ演習**は、４年間で33回実施し、**延べ571名**が受講。
- 講義演習形式によりセキュリティ知識等を学ぶ**コロッセオカレッジ**は、 95回実施し、**延べ1,717名**が受講。

サイバーコロッセオ受講人数（括弧内は実施回数）

	2017年度	2018年度	2019年度	2020年度	合計
初級コース		３８名（２回）	７２名（４回）	４２名（２回）	**１５２名**（８回）
中級コース	３４名（１回）	５１名（２回）	６７名（５回）	４６名（３回）	**１９８名**（11回）
準上級コース	４０名（１回）	４８名（２回）	５３名（６回）	８０名（５回）	**２２１名**（14回）
コロッセオ演習　計	**７４名**（２回）	**１３７名**（６回）	**１９２名**（15回）	**１６８名**（10回）	**５７１名**（33回）
初級コース	–	５９名（５回）	２５６名（15回）	８７名（５回）	**４０２名**（25回）
中級コース	–	１１１名（４回）	３７２名（21回）	１５１名（７回）	**６３４名**（32回）
準上級コース	–	１７７名（７回）	３６４名（23回）	１４０名（８回）	**６８１名**（38回）
コロッセオカレッジ　計	**–**	**３４７名**（16回）	**９９２名**（59回）	**３７８名**（20回）	**1,７１７名**（95回）

※受講人数は延べ人数。同一人物がステップアップや習熟のため複数回受講することもある。

サイバーカレッジ カリキュラム

初級コース
- ◇ ☆ セキュリティ基礎
- ◇ ☆ セキュリティツールE
- ◇ ☆ インシデントレスポンス概論
- ◇ ☆ 個人情報保護関係法令
- ◇ ☆ システムアーキテクチャ
- ☆ GDPR

中級コース
- ☆ システムアーキテクチャ
- ◇ ☆ 実践インシデントレスポンス
- ◇ ☆ セキュリティツールM
- ☆ 脆弱性診断実務
- ☆ ペネトレーションテスト実務
- ◇ ☆ 最新セキュリティトレンド
- ◇ ☆ セキュア開発

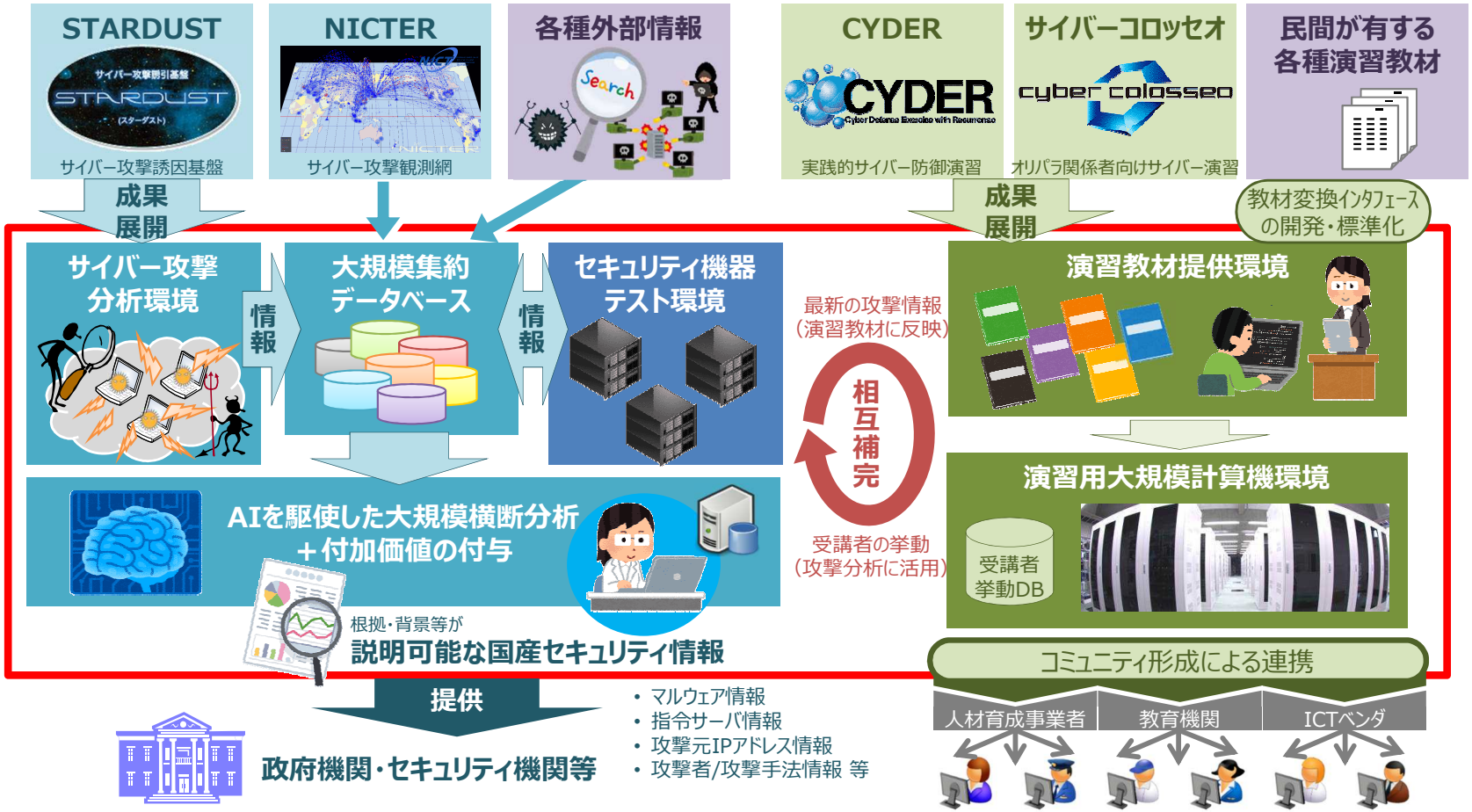
準上級コース
- ☆ セキュリティツールP
- ◇ ☆ ログ・パケット解析実務
- ☆ ログ解析実務
- ◇ ☆ マイクロハードニング
- ◇ ☆ サイバーインテリジェンス
- ◇ ☆ フォレンジック実務
- ◇ ☆ マルウェア解析実務
- ◇ 脆弱性診断実務１
- ◇ 脆弱性診断実務２
- ☆ トラフィック解析実務
- ☆ IRノンテクニカルスキル演習

<凡例>
◇ 2018年度開講
☆ 2019･2020年度開講

※受講は通常１日間。コロッセオ演習の準上級コース及びコロッセオカレッジの準上級コース（IRノンテクニカルスキル演習のみ）は２日間。

サイバーセキュリティ統合知的・人材育成基盤

➢ サイバーセキュリティ情報を**国内で収集・蓄積・分析・提供**するとともに、**社会全体でサイバーセキュリティ人材を育成する**ための共通基盤をNICTに構築し、産学の結節点として開放することで、サイバーセキュリティ対応能力の向上を図る。



次のとおり活用可能な基盤をNICTに構築。

➢ **国産セキュリティ情報の収集・蓄積・分析・提供**
幅広くサイバーセキュリティ情報を収集・蓄積し、AIを駆使して横断的に分析することで、高信頼で即時的なセキュリティ情報を生成し、政府・セキュリティ機関等に提供。

➢ **セキュリティ機器テスト環境**
セキュリティ製品・サービスの開発を推進するため、最新のサイバー攻撃情報を活用し、その対応状況をセキュリティ事業者がテストできる環境を提供。

➢ **高度解析人材の育成**
収集したセキュリティ情報を活用し高度なサイバー攻撃を迅速に検知・分析できる卓越した人材を育成。

➢ **人材育成のための基盤提供**
NICTが有する人材育成に関する環境・知見を民間・教育機関等に開放し、自律的な人材育成を推進。

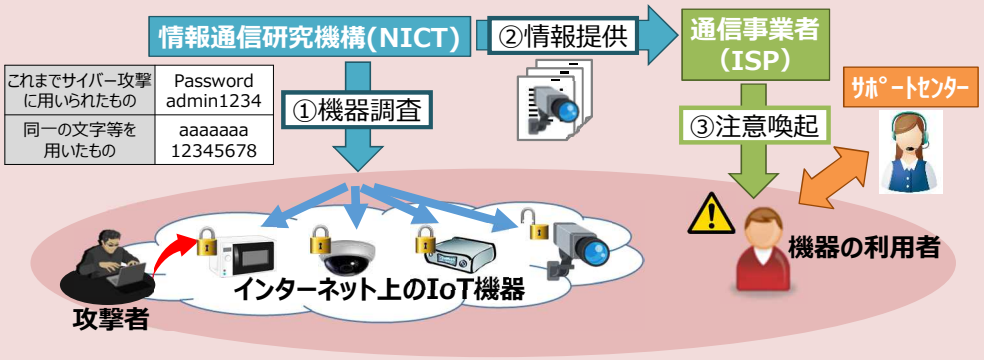
令和２年度三次補正予算案：８５．２億円 ／ 令和３年度当初予算案：７．０億円

IoT機器調査及び利用者への注意喚起

- 情報通信研究機構(NICT)が**サイバー攻撃に悪用されるおそれのあるIoT機器**を調査し、インターネット・サービス・プロバイダ(ISP)を通じた利用者への注意喚起を行う取組「**NOTICE**」を2019年２月より実施。
- NOTICEの取組に加え、**マルウェアに感染しているIoT機器**をNICTの「**NICTER**」プロジェクト※で得られた情報を基に特定し、ISPから利用者へ注意喚起を行う取組を2019年６月より開始。

※NICTが、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施。

【NOTICE注意喚起の概要】

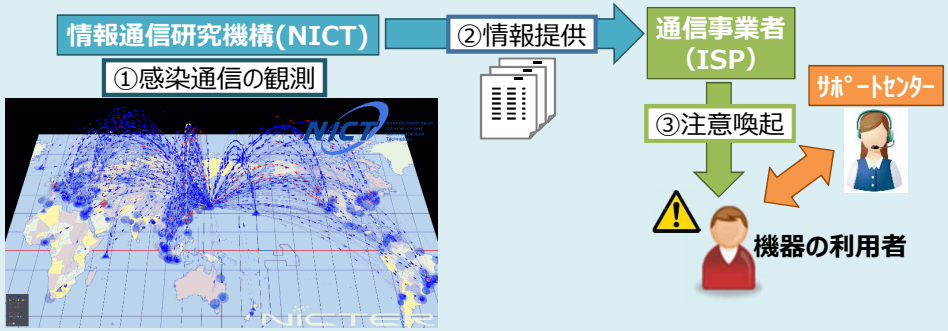


調査対象：パスワード設定等に不備があり、**サイバー攻撃に悪用されるおそれのある**IoT機器

① NICTがインターネット上のIoT機器に、容易に推測されるパスワードを入力するなどして、サイバー攻撃に悪用されるおそれのある機器を特定。
② 当該機器の情報をISPに通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施。

【NICTER注意喚起※の概要】

※マルウェアに感染しているIoT機器の利用者への注意喚起



調査対象：既にMirai等の**マルウェアに感染している**IoT機器

① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。
※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群
② 当該機器の情報をISPに通知。
③ ISPが当該機器の利用者を特定し、注意喚起を実施

実施計画の変更の認可

➢ NOTICEの**実施計画**に記載された事項のうち、特定アクセス行為において**入力する識別符号**、及び特定アクセス行為の**送信元のIPアドレス**について、NICTから**変更**したい旨の申請。

→2020年９月11日付けで**総務大臣認可**　（10月度の調査から適用）

実施計画に記載が必要な事項

総務省令※において規定。

※国立研究開発法人情報通信研究機構法附則第八条第四項第一号に規定する総務省令で定める基準及び第九条に規定する業務の実施に関する計画に関する省令（平成30年総務省令第61号）第2条第2項各号

- ✓ 業務従事者の氏名・所属部署・連絡先
- ✓ 特定アクセス行為の**送信元のIPアドレス**
- ✓ 特定アクセス行為に係る識別符号の方針及び当該方針に基づき**入力する識別符号**
- ✓ 特定アクセス行為の送信先のIPアドレス範囲
- ✓ 特定アクセス行為に関する情報の適正な取扱い
- ✓ ISP等への通知先に求める情報の適正な取扱い
- ✓ その他必要な事項

変更内容

(1) 特定アクセス行為において入力する識別符号（ID・パスワード）の追加

変更前	変更後
約１００通り	**約６００通り**

（追加理由）

継続して新たなIoT機器向けのマルウェアが登場していることを踏まえ当該マルウェアで利用されている識別符号や、機器の初期設定の識別符号等を新たに調査対象とするため。

(2) 特定アクセス行為の送信元のIPアドレスの追加

変更前	変更後
４１アドレス	**５４アドレス**

（追加理由）

(1)により入力する識別符号が増加することから、特定アクセス行為に係る通信量も増加し通信回線を増設するため

IoT機器調査及び利用者への注意喚起の実施状況（2020年12月度）

- 参加手続きが完了している**ISP**（インターネット・サービス・プロバイダ）は**65社**。
  当該ISPの**約1.12億IPアドレス**に対して調査を実施。
- **NOTICE**による注意喚起は、**２,００２件**の**対象を検知**しISPへ通知。
- **NICTER**による注意喚起は、１日平均**１１３件**の**対象を検知**しISPへ通知。

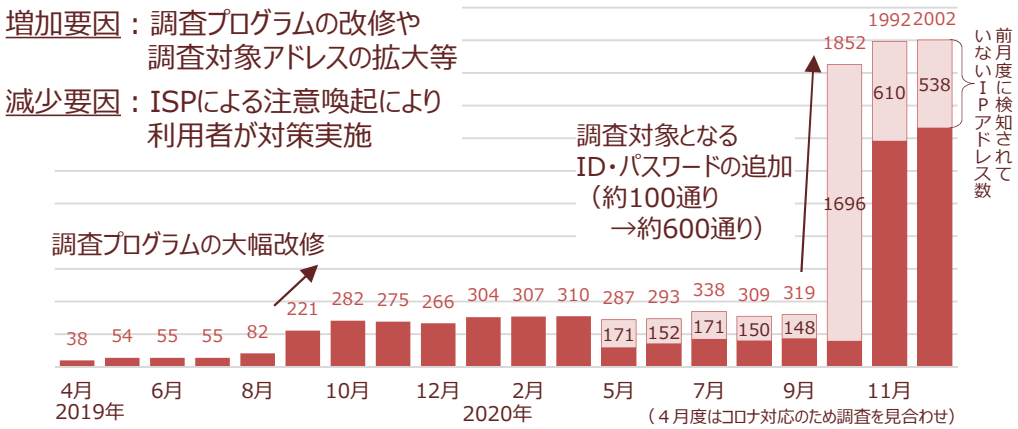
NOTICE注意喚起の取組結果

注意喚起対象としてISPへ通知したもの*

２,００２件（11月度:1,992件）

（参考） 2020年度の累積件数：7,392件（2019年度：2,249件）
ID・パスワードが入力可能だったもの：8.6万件

*) 特定のID・パスワードによりログインできるかという調査をおおむね月に1回実施し、ログインでき、注意喚起対象となったもの（ユニークIPアドレス数）



NICTER注意喚起※の取組結果

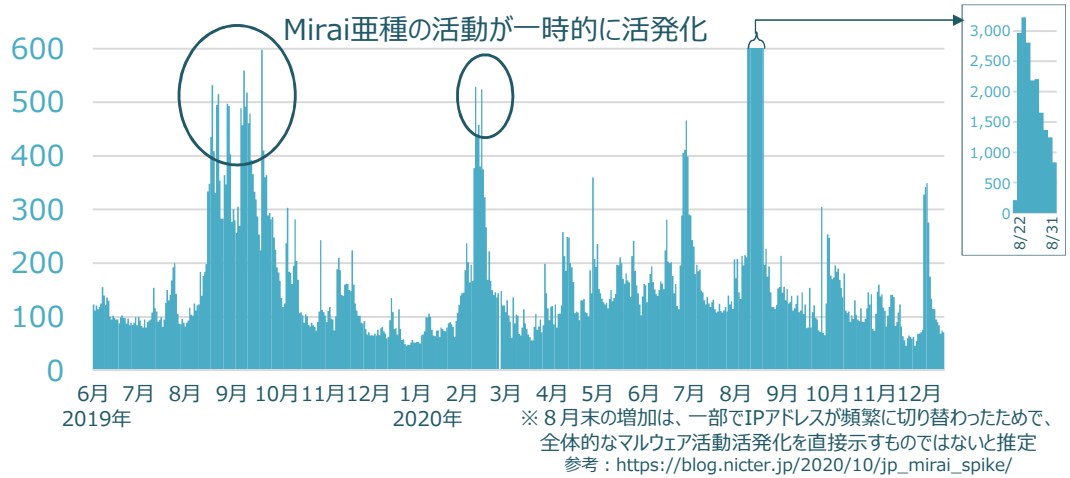
※マルウェアに感染しているIoT機器の利用者への注意喚起

注意喚起対象としてISPへ通知したもの**

１日平均１１３件（11月度:114件）

（参考） 期間全体での値： １日平均187件
最小：46件(2020/12/6等)／最大：3,227件(2020/8/24)

**) NICTERプロジェクトによりマルウェアに感染していることが検知され、注意喚起対象となったもの（ユニークIPアドレス数）



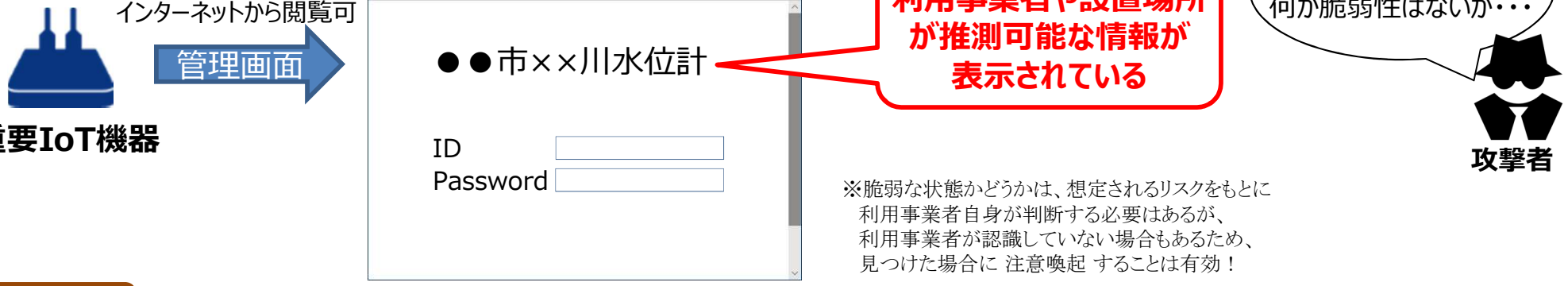
※８月末の増加は、一部でIPアドレスが頻繁に切り替わったためで、全体的なマルウェア活動活発化を直接示すものではないと推定
参考：https://blog.nicter.jp/2020/10/jp_mirai_spike/

NOTICE注意喚起・NICTER注意喚起のいずれについても、前月度から全体として大きな変化はありません。

重要IoT機器のセキュリティ対策

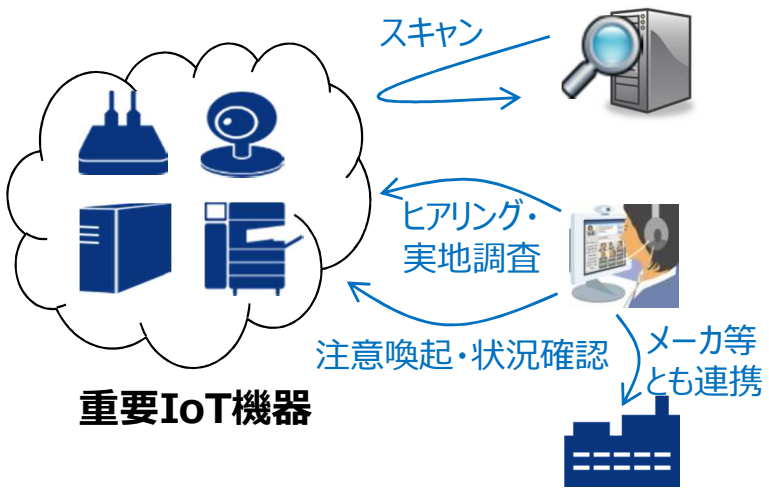
- 重要インフラ等の社会的に影響を及ぼすリスクを伴った使用をしているIoT機器（**重要IoT機器**）について、**公開する必要のない情報が公開されている**など、攻撃を受けやすい**脆弱な状態**にあるものを**検出**する。
- 検出した重要IoT機器について、利用事業者に対して**設定状況等のヒアリング**を行った上で、脆弱な状態を解消するための**注意喚起**や**対策手法の提示**を行い、**対策の完了までのトレース**を行う。

脆弱な状態の例



※脆弱な状態かどうかは、想定されるリスクをもとに利用事業者自身が判断する必要はあるが、利用事業者が認識していない場合もあるため、見つけた場合に 注意喚起 することは有効！

対策スキーム



重要IoT機器探索	重要IoT機器？ Web画面が見える？
利用者特定	画面の事業者名は？
利用環境調査	どのような用途か？ どのような設定・管理をしているか？ どのようなネットワーク環境で使っているか？
注意喚起実施	想定されるリスクはどのようなものか 対策にはどのようなものが有効か
対策状況確認	対策の実施に当たり問題はないか？

資料２－２

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

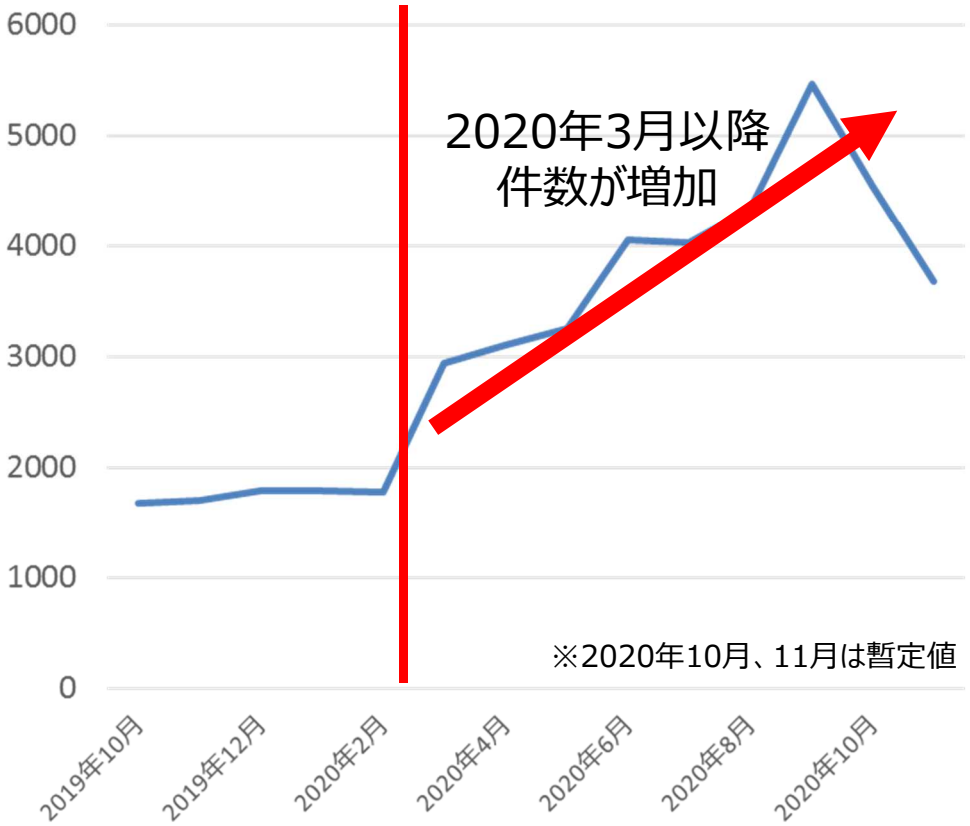
2020年12月18日

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

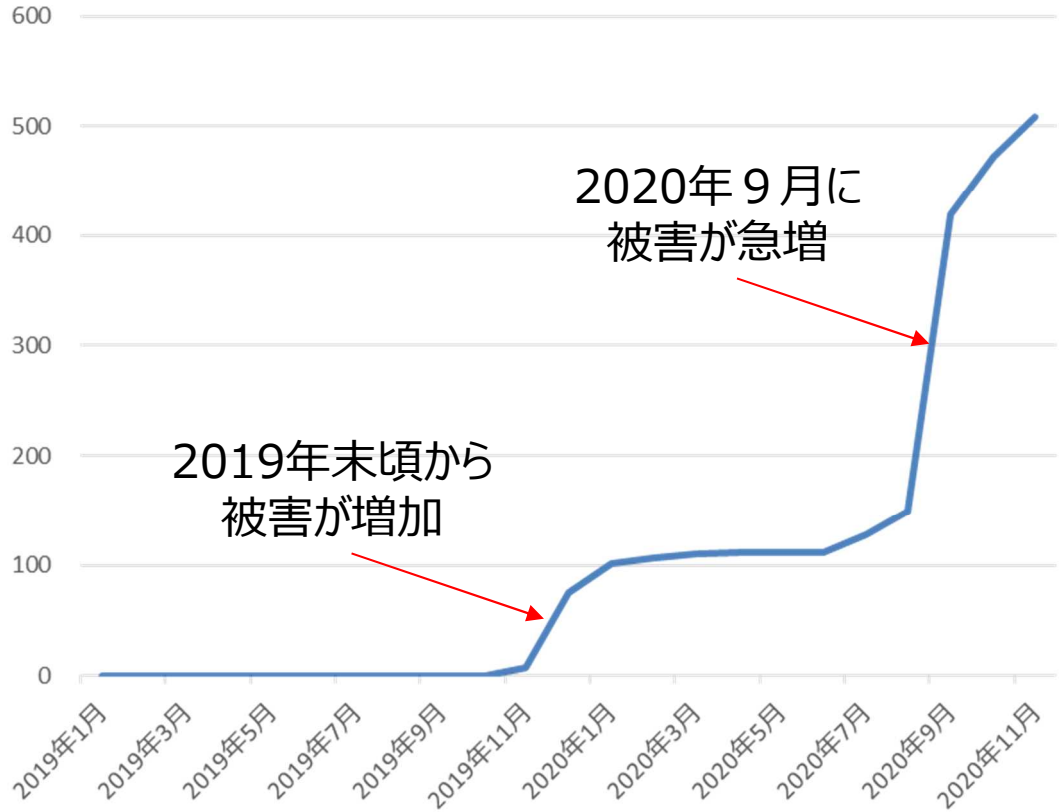
- 新型コロナウイルスの感染が拡大した2020年3月以降、インシデントの相談件数が増加。
- 特に、電子メールを媒介に感染を広げるマルウェア「Emotet※参考１参照」による被害の相談が急増。

JPCERT/CCへのインシデント相談報告件数（月別）



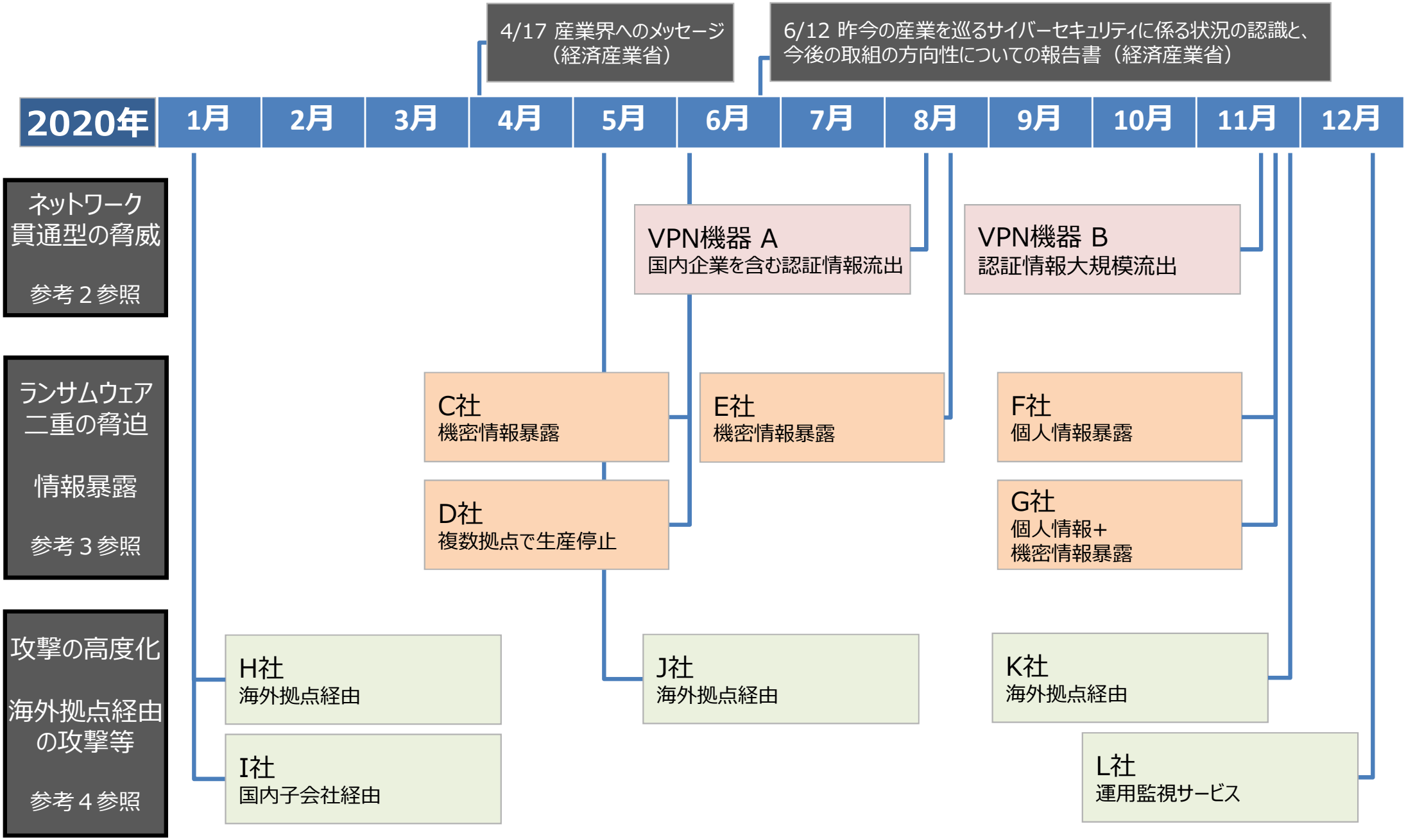
＜（一社）JPCERT/CC＞

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/

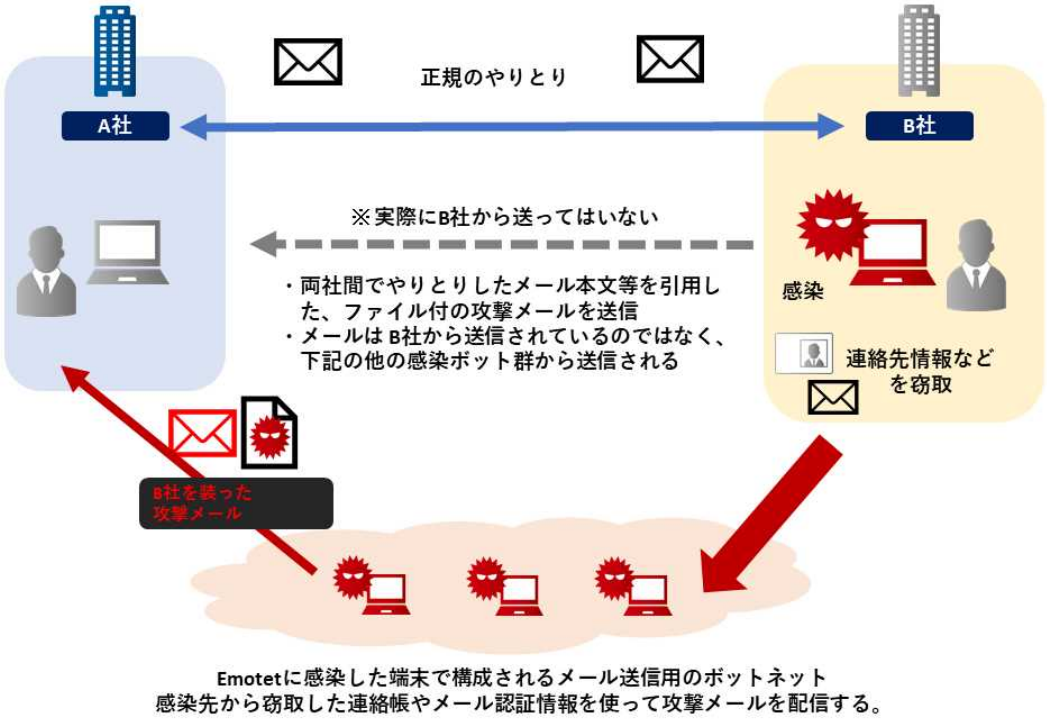
注意喚起情報	URL：https://www.jpcert.or.jp/at/2020.html
マルウェアEmotetへの対応FAQ	URL：https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

参考資料

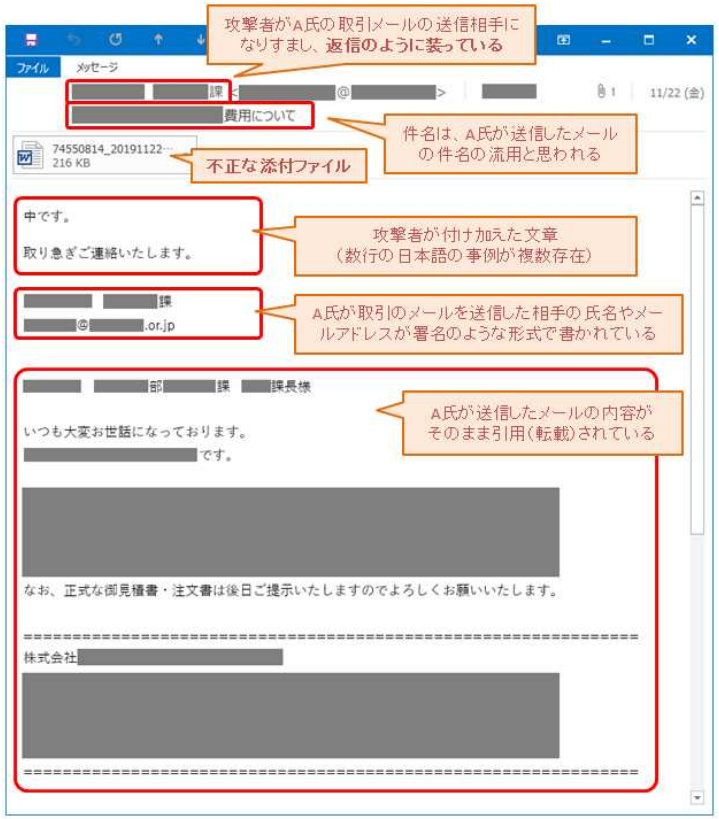
Emotet（エモテット）の手口

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。



Emotetに感染した端末で構成されるメール送信用のボットネット
感染先から窃取した連絡帳やメール認証情報を使って攻撃メールを配信する。

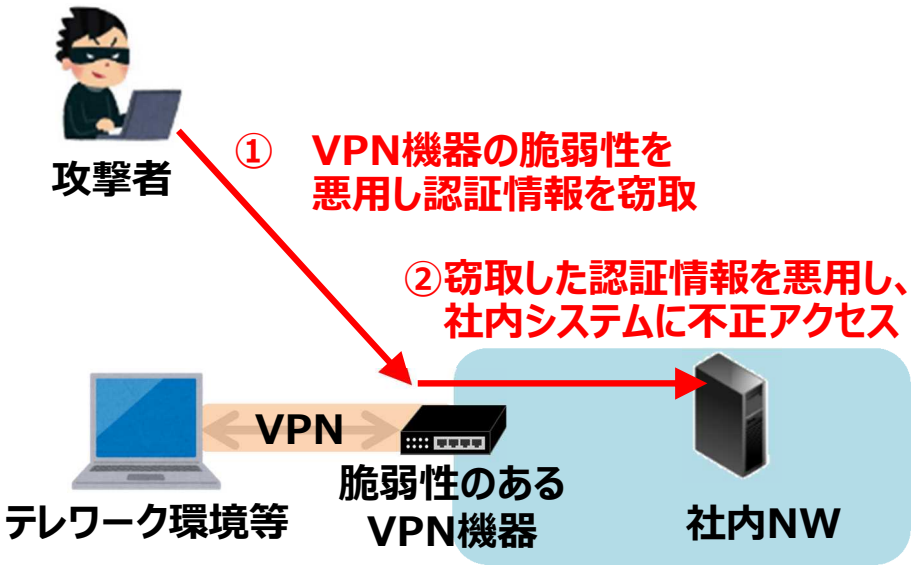


ネットワーク貫通型：VPN機器の脆弱性を悪用したネットワークへの侵入

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

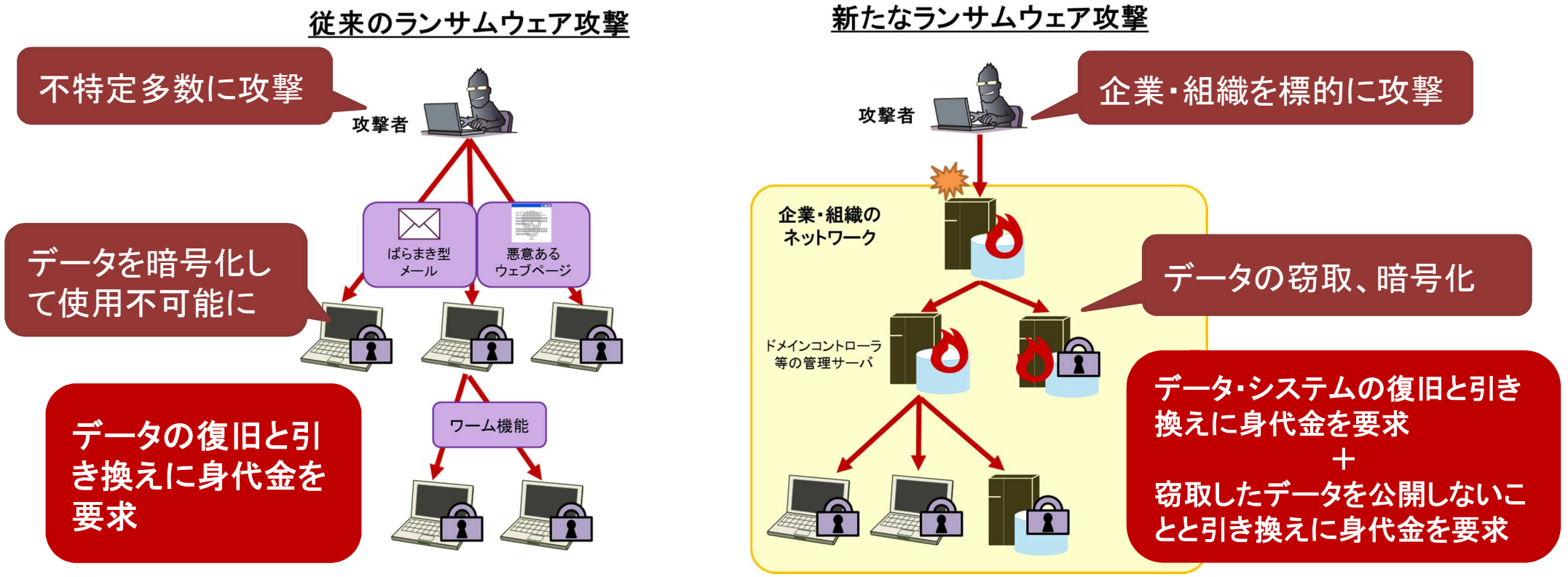
2019年5月	脆弱性情報公開
2019年8月頃	脆弱性の詳細情報公開、悪用やスキャン開始
2020年11月	脆弱性の影響を受ける約5万台の機器情報が公開 IPアドレス、ユーザーアカウント名、平文パスワード等

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。

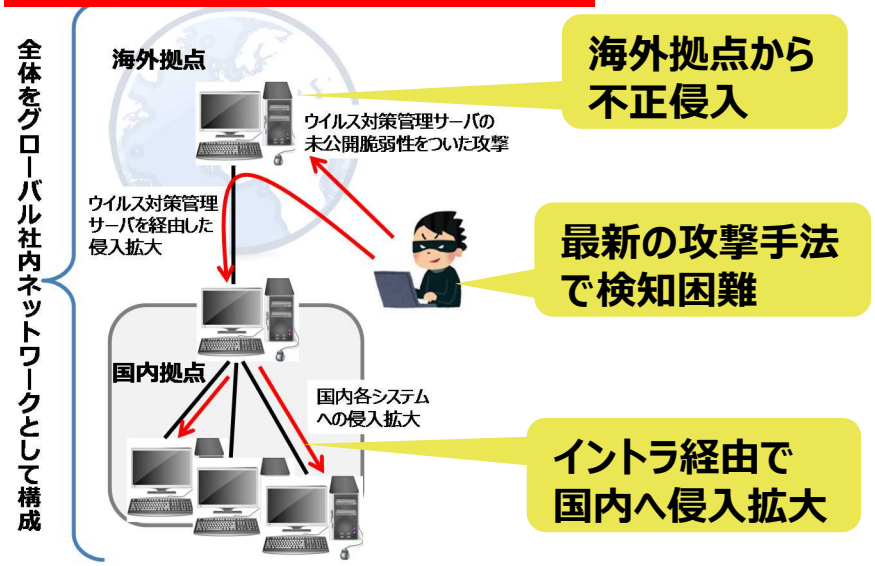


海外拠点経由の攻撃

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