資料36－2

サイバーセキュリティを巡る最近の動向

令和4年3月

サイバーセキュリティタスクフォース事務局

サイバーセキュリティ対策の強化についての注意喚起

○　昨今の情勢を踏まえ、サイバー攻撃事案のリスクは高まっていると考えられることから、総務省では、関係省庁と連携して、電気通信事業者、放送事業者及び地方公共団体等に対して、サイバーセキュリティ対策の強化について、令和4年2月23日及び3月1日に注意喚起を実施。

・「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について」（経済産業省、2月23日）

昨今の情勢を踏まえるとサイバー攻撃事案の潜在的なリスクは高まっていると考えられます。

各企業・団体においては、経営者のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

不審な動きを把握した場合は、早期対処のために速やかに経済産業省やセキュリティ関係機関に御相談ください。

1．リスク低減のための措置

○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。

○IoT機器を含む情報資産の保有状況を把握する。特にVPN装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。　※下記URL参照

○メールの添付ファイルを不用意に開かない、URLを不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

2．インシデントの早期検知

○サーバ等における各種ログを確認する。

○通信の監視・分析やアクセスコントロールを再点検する。

3．インシデント発生時の適切な対処・回復

○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

https://www.meti.go.jp/press/2021/02/20220221003/20220221003.html

・「サイバーセキュリティ対策の強化について」（経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター、3月1日）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

さらに、国外拠点等についても、国内の重要システム等へのサイバー攻撃の足掛かりになることがありますので、国内のシステム等と同様に具体的な支援・指示等によりセキュリティ対策を実施するようお願いいたします。

実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

1．リスク低減のための措置

○パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。

○IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

○メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

2．インシデントの早期検知

○サーバ等における各種ログを確認する。

○通信の監視・分析やアクセスコントロールを再点検する。

3．インシデント発生時の適切な対処・回復

○データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

○インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000470.html

Emotetの感染再拡大

○ マルウェアEmotet（エモテット）は、2019年後半から広く流行した後、2021年１月に欧州においてテイクダウンされ、攻撃・被害が大幅に減少していたが、2021年11月頃から活動の再開が観測されている。

○ 2022年２月には、感染の急速な拡大に伴い、IPA、JPCERT/CCが感染再拡大に関する注意喚起を実施。

✓ IPAでは、正規メールへの返信を装うなどの手口を解説し、身に覚えのないメールの添付ファイルは開かないよう注意喚起

✓ JPCERT/CCでは、Emotet感染確認ツール「EmoCheck」をGitHubで無料公開

○ 2022年３月には、Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の約5倍以上に急増。国内感染組織から国内組織に対するメール配信も増えている状況。

Emotet感染再拡大までの経緯

2019年10月　JPCERT/CCへのEmotet相談増加

2021年1月　欧米8カ国の法執行機関・司法当局によるEmotet攻撃基盤のテイクダウン

2021年2月　海外機関からの提供情報をもとに、Emotetに感染している被害組織に対してJPCERT/CCから個別通知を開始

2021年3月　上記とは別の海外機関から警察庁を経由して提供された国内の過去の感染被害情報をもとに、ISPにおいて利用者単位での注意喚起を実施

2021年4月　Emotet無害化

2021年11月　活動の再開を観測

2022年2月　感染の急速な拡大に伴い、JPCERT/CC、IPAからEmotetの感染再拡大に関する注意喚起

2022年3月　Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数が2020年の感染ピーク時の約5倍以上に急増

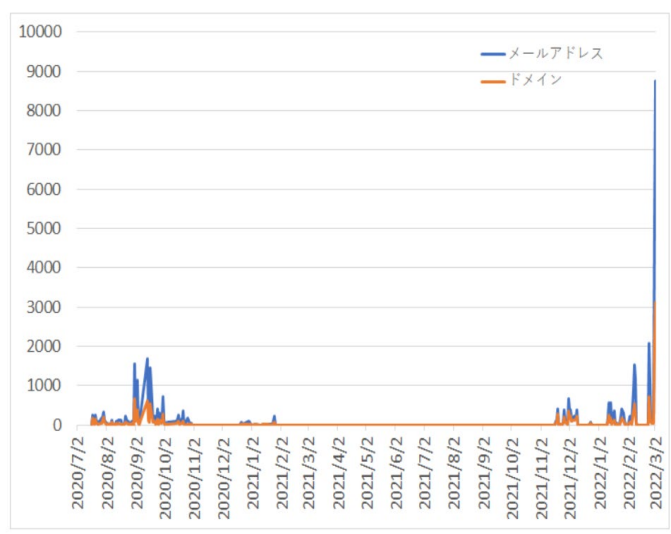
JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」
https://www.jpcert.or.jp/at/2022/at220006.html （2022年3月14日更新）

JPCERT/CC Eyes
「マルウェアEmotetのテイクダウンと感染端末に対する通知」
https://blogs.jpcert.or.jp/ja/2021/02/emotet-notice.html#6（2021年5月25日更新）

IPA「Emotetの攻撃活動の急増（2022年2月9日 追記）」
https://www.ipa.go.jp/security/announce/20191202.html#L18

Emotetに感染しメール送信に悪用される可能性のある.jpメールアドレス数の新規観測の推移（外部からの提供観測情報）

（2022年3月3日更新）

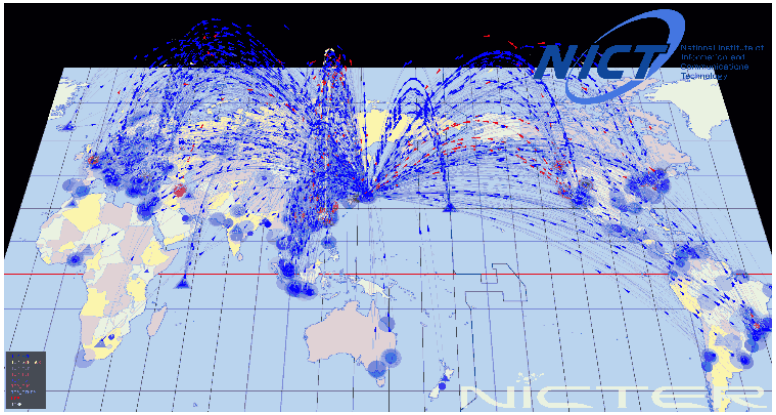


JPCERT/CC「マルウェアEmotetの感染再拡大に関する注意喚起」
https://www.jpcert.or.jp/at/2022/at220006.html
（2022年3月14日更新）

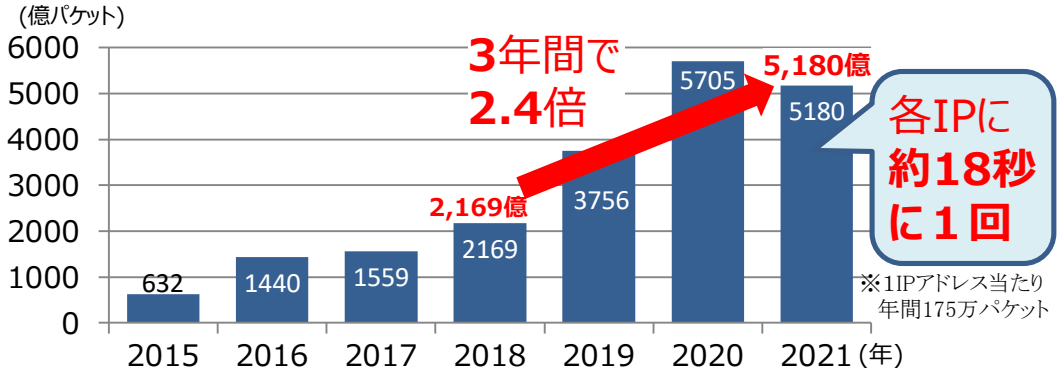
NICTERによるサイバー攻撃の観測（～2021年）

○　国立研究開発法人情報通信研究機構（NICT）では、大規模サイバー攻撃観測網であるNICTERにおいて、未使用のIPアドレス30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測。

NICTERにより観測されるサイバー攻撃の様子



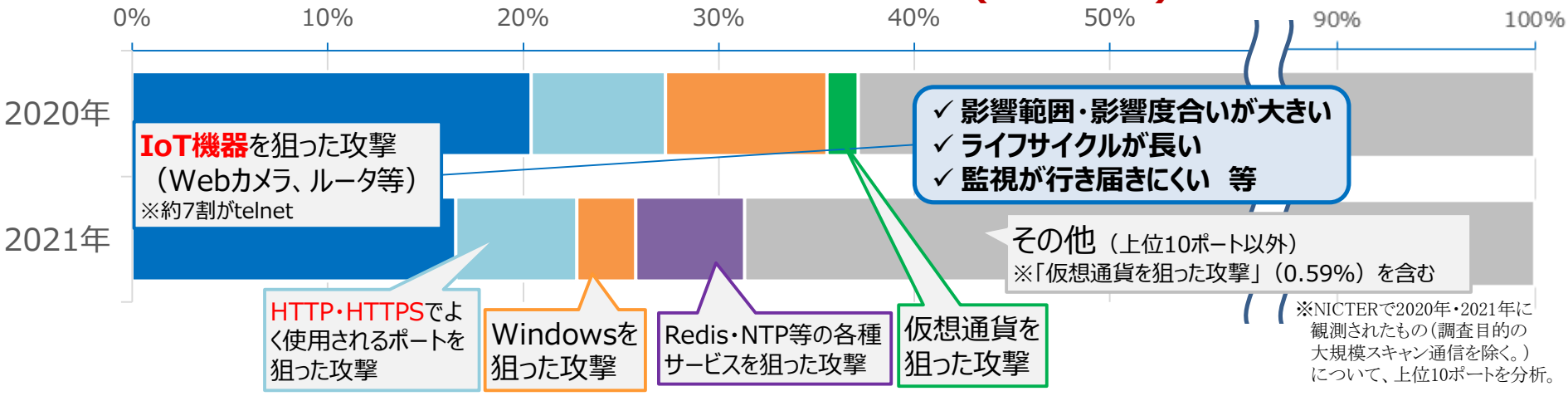
NICTERで１年間に観測されたサイバー攻撃関連の通信数



※2020年は特異的な事象（大規模なバックスキャッタや大量の調査スキャン）が観測されたため、例外的にパケット数が多かったものと推測

NICTERにより観測された通信の内容（上位10ポートの分析）

- ✓ **IoT機器を狙った攻撃が依然としてトップ**
- ✓ **攻撃(対象ポート)が多様化**



※NICTERで2020年・2021年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位10ポートを分析。