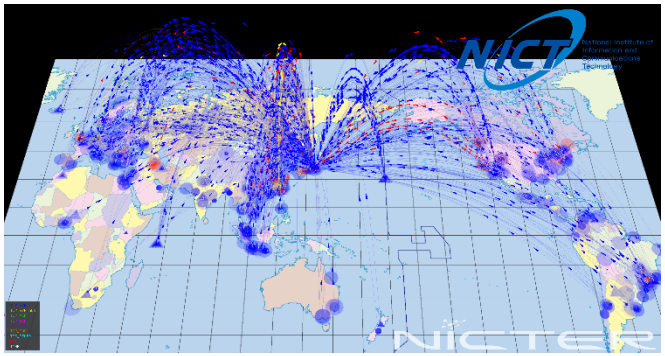
総務省
Ministry of Internal Affairs and Communications

サイバーセキュリティを取り巻く現状と政策について

令和２年２月５日（水）

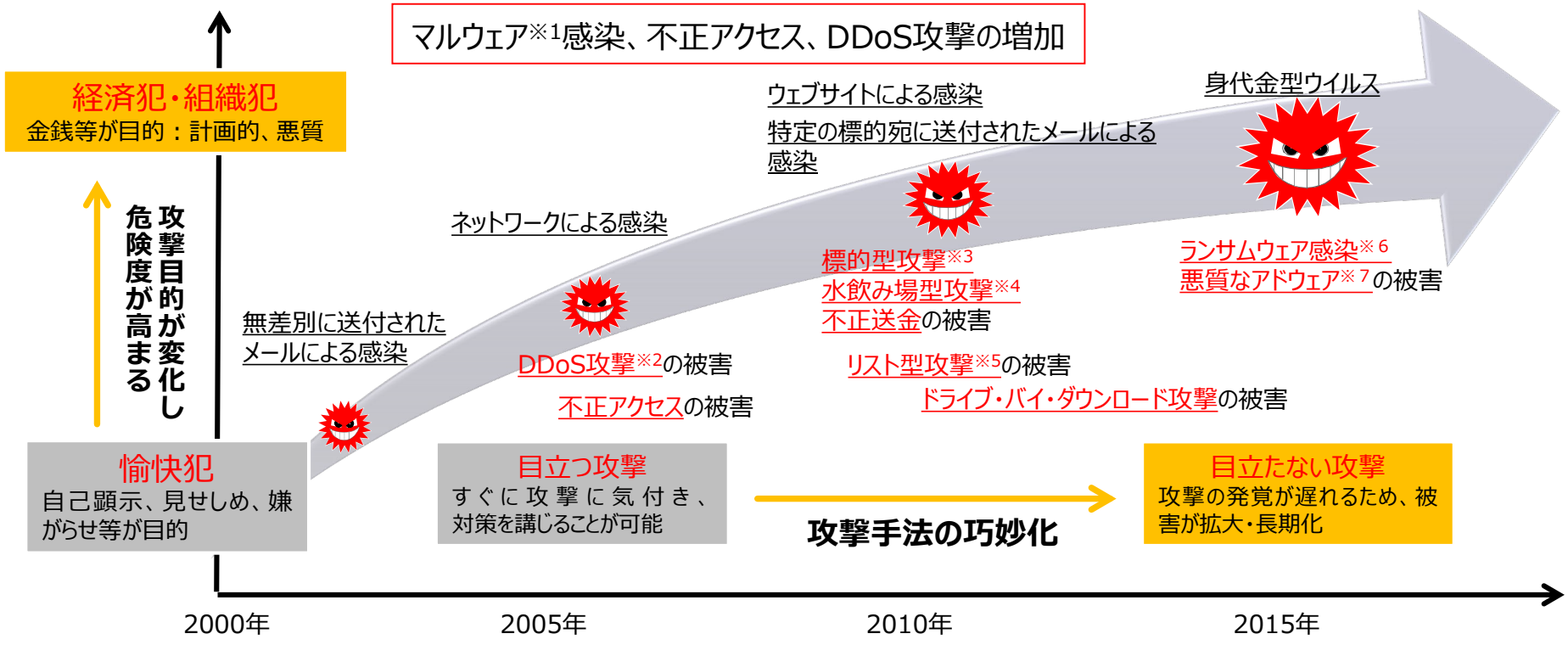
総務省　サイバーセキュリティ統括官室
安井　祥広

昨今のサイバーセキュリティの現状等について



サイバーセキュリティ上の脅威の増大①

■ インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、サイバーセキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。



※1 マルウェア(Malware)　Malicious softwareの短縮語。コンピュータウイルスのような有害なソフトウェアの総称。

※2 DDoS攻撃　分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数の端末から一斉に大量のデータを特定宛先に送りつけ、宛先のサーバ等を動作不能にする攻撃。

※3 標的型攻撃　機密情報等の窃取を目的として、特定の個人や組織を標的として行われる攻撃。

※4 水飲み場型攻撃　標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

※5 リスト型攻撃　不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃。

※6 ランサムウェア(Ransomware)　身代金要求型ウイルスのこと。感染端末上にある文書などのファイルが暗号化され、暗号解除のためには金銭を要求される。

※7 アドウェア(Adware)　広告表示によって収入を得るソフトウエアの総称。狭義には、フリーウエアと共にインストールされ、ブラウザー利用時に広告を自動的に付加するソフト

サイバーセキュリティ上の脅威の増大②

国内事例

2015年６月	日本年金機構の職員が利用する端末がマルウェアに感染し、年金加入者の情報約125万件が流出（標的型攻撃）
2015年10月	金融庁の注意喚起を装ったフィッシングサイトを確認、 国内銀行のセキュリティを向上させるためと称し、口座番号、パスワード、第二認証などの情報を騙し取られる恐れ（フィッシング攻撃）
2015年11月	東京五輪組織委員会のホームページにサイバー攻撃、約12時間閲覧不能（DDoS攻撃）
2016年６月	i.JTB（JTBのグループ会社）の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（標的型攻撃）
2017年５月	**国内（行政、民間企業、病院等）において、WannaCryによる被害が確認。企業内のシステム停止などの障害が発生（ランサムウェア）**
2018年１月	コインチェック社が保有していた暗号資産（仮想通貨）が外部へ送信され、顧客資産が流出（不正アクセス）

海外事例

2015年４月	**フランスのテレビネットワーク TV５ Monde がサイバー攻撃を受け、放送が一時中断（標的型攻撃）**
2015年６月	米国の人事管理局（OPM）が不正にアクセスされ、政府職員の個人情報が流出（不正アクセス）
2015年12月	**ウクライナの電力会社のシステムがマルウェアに感染し、停電が発生（標的型攻撃）**
2016年10月	米国のDyn社のDNSサーバが大規模なDDoS攻撃を受け、同社のDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生（DDoS攻撃）
2017年５月	**世界各国（アメリカ、イギリス、中国、ロシア等）でWannaCryの感染被害が発生。行政、民間企業、医療等の多くの組織に影響（ランサムウェア）**
2017年10月	米Yahoo社で約30億件の個人情報が流出していたことが判明（不正アクセス）
2019年９月	**エクアドルで国民ほぼ全員を含む約2000万人分の個人情報が海外に流出（不正アクセス）**

出典：各種公開資料等より総務省作成

（実被害）サイバー攻撃によるウクライナ停電

サイバー攻撃によりエネルギー供給が停止した初の事例
2015年12月23日　変電所の遮断機切断で最大6時間の停電発生（ウクライナ）
2016年12月17日　変電所の遮断機切断で1時間15分の停電発生（ウクライナ）

2015年
【概　要】
①標的型メール攻撃（ＩＴ系への攻撃）
　　マルウエアを含む添付ファイルをメールで送付
→マルウエアに感染させ、長期間の偵察活動で情報を収集
②ＤＯＳ攻撃で電話システムに支障発生（ＩＴ系への攻撃）
→復旧活動を妨害
③遠隔操作で変電所の遮断機を切断と思われる（OT系への攻撃）
→最大6時間の停電発生（ウクライナ）
※ＵＰＳ（Uninterruptible Power Supply;非常時電源）が動作しないように設定

【被害】 感染した制御システムを使わずに、手動操作で遮断機を操作

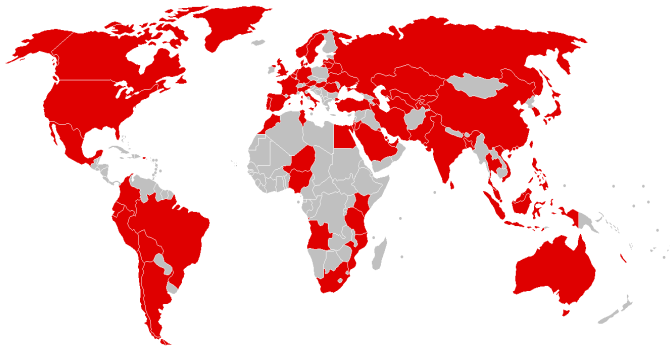
2016年
2015年とほぼ同じ手法だが、複雑化しており、 1時間15分の停電発生

（実被害）大規模サイバー攻撃　WannaCry

2017年5月12日頃より、ランサムウェア（WannaCry）による被害が世界中で多数発生

【感染時の画面イメージ】

【ドイツ鉄道】
行先表示装置がWannaCryに感染
→行先案内表示装置を故障扱い



【被害を受けた国】

【概　要】 150か国30万台以上（国内：600カ所以上2000端末以上）のコンピューターに感染、データを暗号化し、使用不能にする。身代金としてビットコインを要求
【感染ルート】 全容は解析中だが、不審メール開封による感染や、インターネットに接続している端末が感染する場合など、windowsの脆弱性を利用した攻撃
【被害状況】 ルノー（フランス）,Telefonica（スペイン）,FedEx(アメリカ),ドイツ鉄道(ドイツ)など

【対策】
マイクロソフトが3月15日に出したセキュリティ更新プログラム（MS17-010)を適用
セキュリティパッチを適時使用　／　重要データはバックアップ

情報セキュリティ10大脅威 2019

昨年順位	個人	順位	組織	昨年順位
1位	クレジットカード情報の不正利用	1位	**標的型攻撃による被害**	**1位**
1位	フィッシングによる個人情報等の詐取	2位	**ビジネスメール詐欺による被害**	**3位**
4位	不正アプリによるスマートフォン利用者への被害	3位	**ランサムウェアによる被害**	**2位**
NEW	メール等を使った脅迫・詐欺の手口による金銭要求	4位	**サプライチェーンの弱点を悪用した攻撃の高まり**	**NEW**
3位	ネット上の誹謗・中傷・デマ	5位	内部不正による情報漏えい	8位
10位	偽警告によるインターネット詐欺	6位	サービス妨害攻撃によるサービスの停止	9位
1位	インターネットバンキングの不正利用	7位	インターネットサービスからの個人情報の窃取	6位
5位	インターネットサービスへの不正ログイン	8位	IoT機器の脆弱性の顕在化	7位
2位	ランサムウェアによる被害	9位	脆弱性対策情報の公開に伴う悪用増加	4位
9位	IoT 機器の不適切な管理	10位	不注意による情報漏えい	12位

出典：「情報セキュリティ10大脅威 2019」（独立行政法人情報処理推進機構）

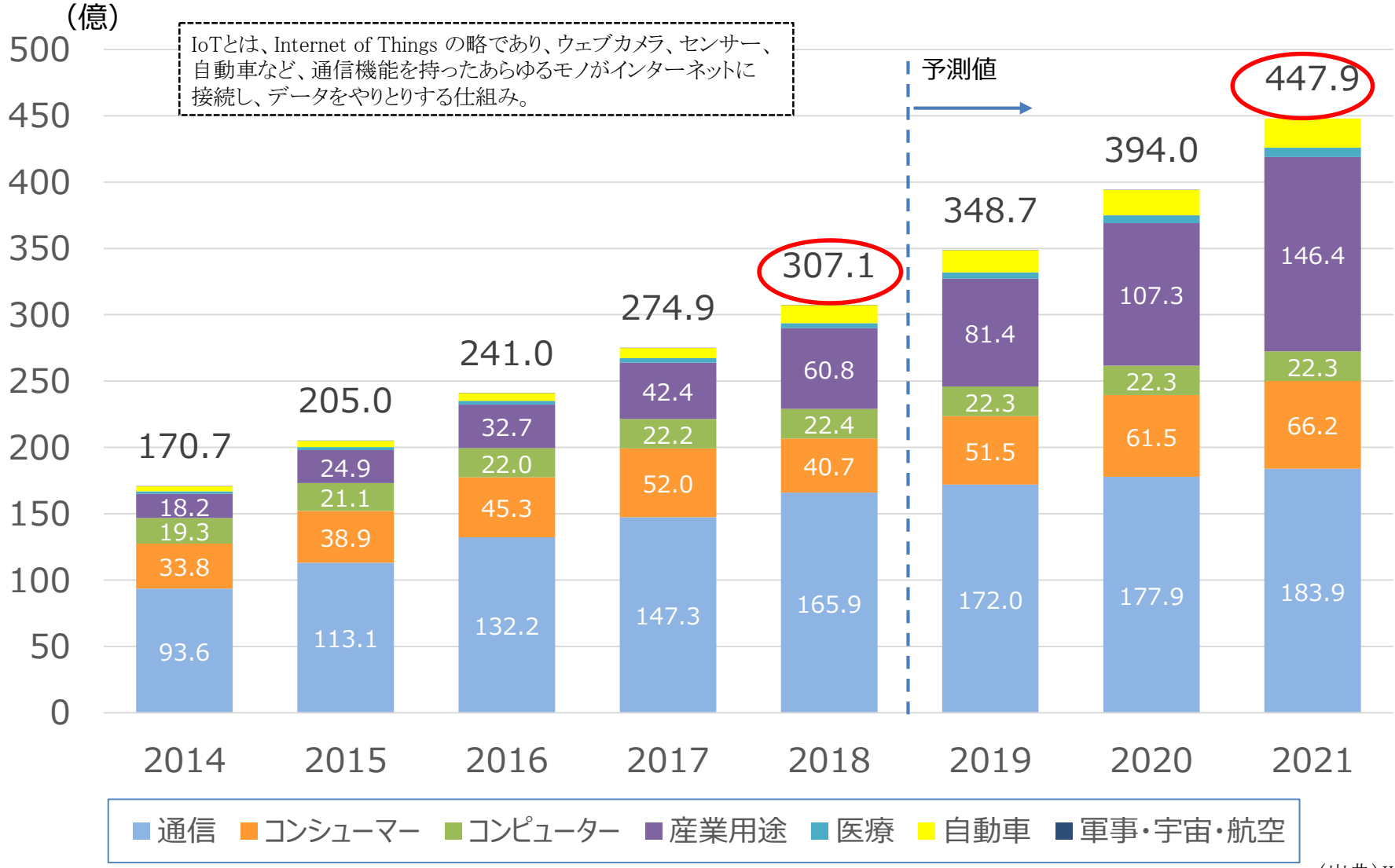
2019 セキュリティ十大ニュース

- 大手コンビニチェーンのキャッシュレス決済、不正アクセス被害を受け一ヶ月でサービス廃止
- 米銀行でクラウドから大量個人情報漏洩
- 米国セキュリティ会社社員がユーザー情報を売却
- フィッシングサイトの月間報告が8,000件を超え過去最多に
- 「内定辞退率」販売問題
- 大手クラウド事業者の大規模障害で多数のサービスに影響
- マルウェア Emotet の感染に関する注意喚起
- 米国企業が量子コンピュータで量子超越性を達成と発表
- IoT機器調査「NOTICE」開始
- 東京五輪にAIを活用した顔認証技術を導入

出典：「2019 セキュリティ十大ニュース」（特定非営利法人日本ネットワークセキュリティ協会）より総務省にて編集

IoT機器の急激な増加

➢ 2018年時点でインターネットにつながるモノ（IoT機器）の数は307億個と推定されており、2021年までに約1.5倍の448億個まで増加する見込み。

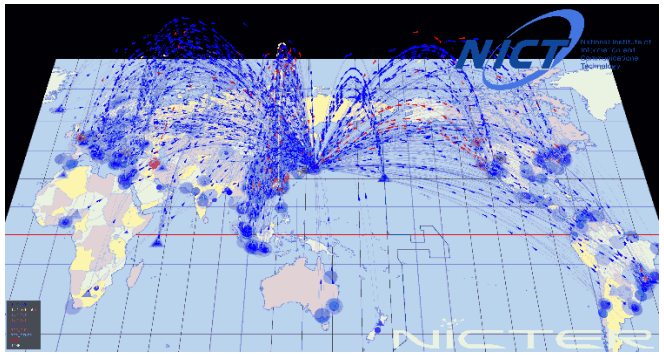


（出典）IHS Technology

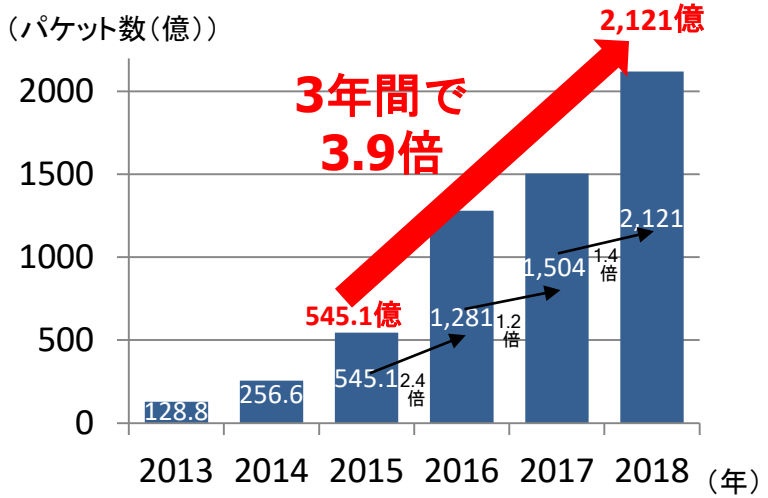
IoT機器を狙った攻撃の急増（NICTERによる観測）

➢ 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。**

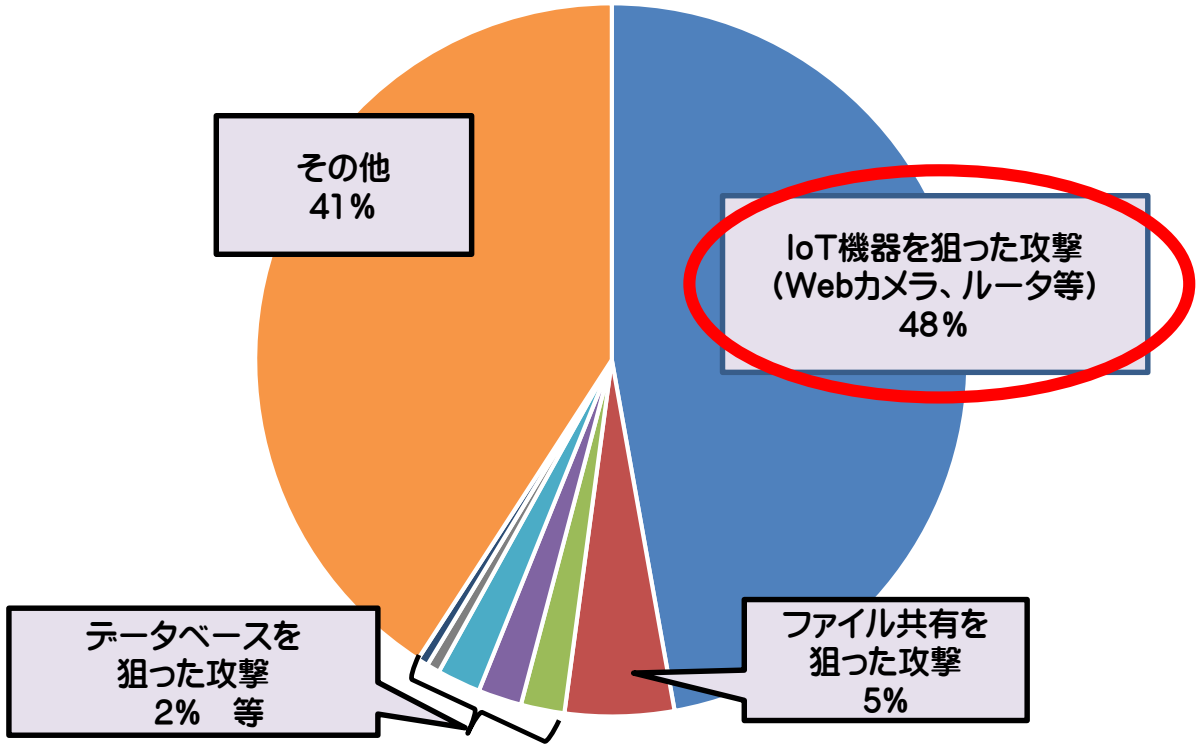
NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測されたサイバー攻撃回数



約半数がIoT機器を狙った攻撃

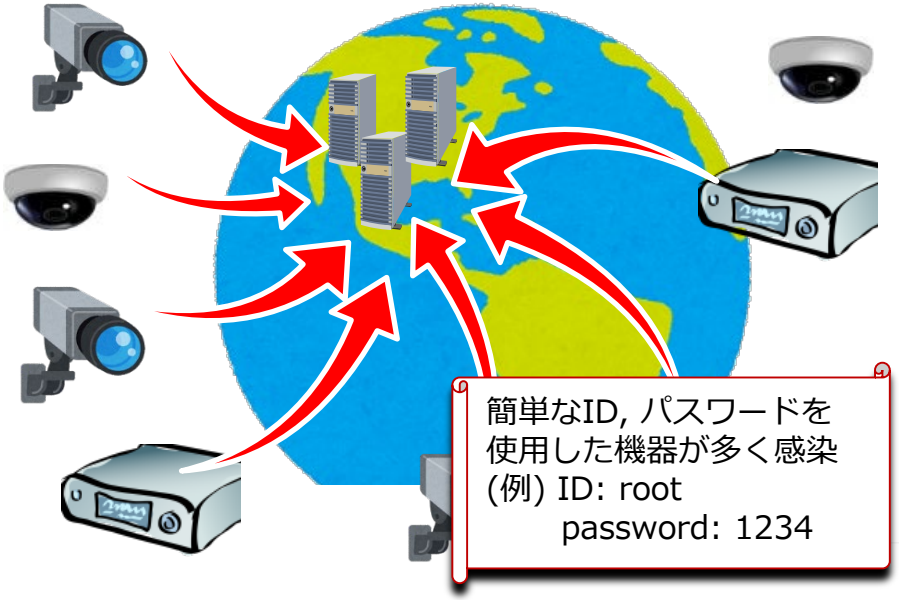


（注１）　NICTERで観測されたパケットのうち、サービスの種類（ポート番号）ごとに割合の多い上位から30位までを分析したもの。

（注２）　IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

IoT機器を踏み台とした大規模DDoS攻撃

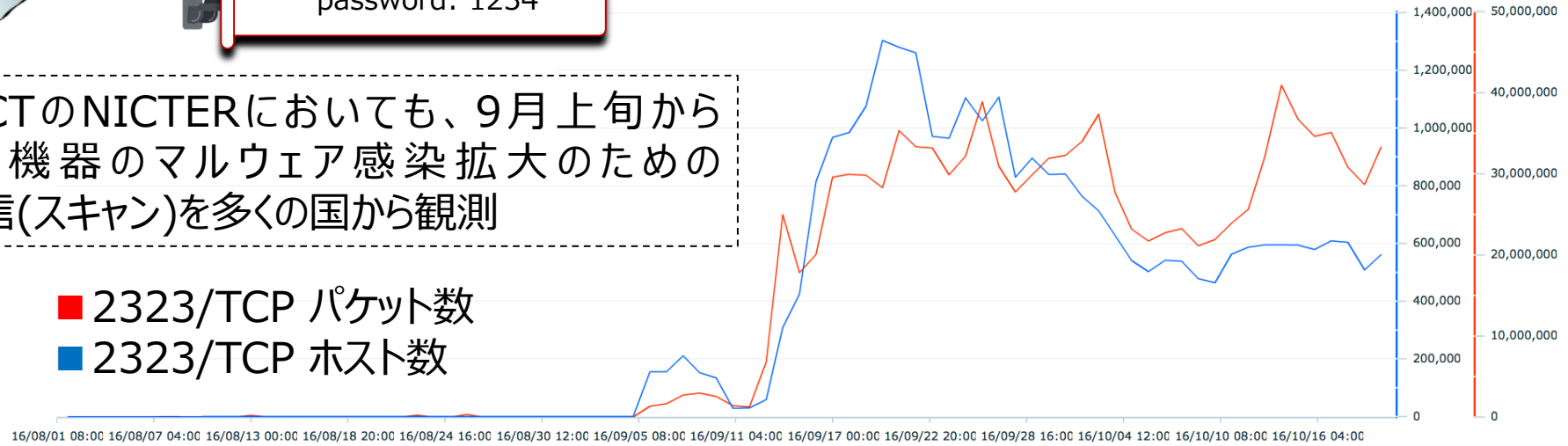
- 2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が２回発生。
- 同社からDNSサービスの提供受けていた企業のサービスにアクセスしにくくなる等の障害が発生。
- サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。



- ✓ マルウェアに感染した10万台を超えるIoT機器からDyn社のシステムに対し大量の通信が発生
- ✓ 最大で1.2Tbpsに達したとの報告もあり。
- ✓ Dyn社のDNSサービスを使用した数多くの大手インターネットサービスやニュースサイトに影響

出典: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

- ✓ NICTのNICTERにおいても、9月上旬からIoT機器のマルウェア感染拡大のための通信(スキャン)を多くの国から観測



マルウェア「Mirai」について

- ボットネットに分類されるマルウェア。
- インターネットからIoT機器をスキャンし、ID/パスワード設定が脆弱な機器に侵入し、ボットネットに追加。
- グローバルIPアドレスによりインターネットから直接アクセスが可能なウェブカメラやルータ等の機器に侵入を試み、次々と乗っ取る。
- 脆弱なIoT機器を次々と乗っ取った上で、攻撃対象に対しDDoS攻撃を実施。

✓ Miraiの作成者：Protraf Solutions LLC社の共同創始者２名。
同社は、DDoS攻撃を沈静化するサービスを提供する企業。

(1) 他の共犯者と共謀し、クリック詐欺（クリック報酬型広告）により多額の広告料を搾取。

(2) また、ボットネット自体をサイバー犯罪者に貸し出し。

2016年9月：KrebsOnSecurity（セキュリティ研究者のサイト）に対するDDoS攻撃
【Miraiボットネットによる最初のDDoS攻撃】
17万台以上のボットネットから、620Gbps超の大量の攻撃パケット。
その数日後、Anna Senpaiと名乗る人物がMiraiボットネットのソースコードを公開。
⇒【Miraiボットネットが拡大。Mirai亜種の拡散。】
⇒ Dyn社の他、英国、仏、独等のISP,金融機関への攻撃

IoT機器がサイバー攻撃の対象として狙われやすい理由

- IoTの進展が企業活動や製品・サービスのイノベーションを加速する一方で、IoT特有の性質と想定されるリスクをもつことから、これらの性質とリスクを踏まえたセキュリティ対策を行うことが必要。

1）脅威の影響範囲・影響度合いが大きい

攻撃を受けると、ネットワークを介してシステム・サービス全体へその影響が波及（自動車・医療等における致命的影響等も存在）

2）IoT機器のライフサイクルが長い

工場の制御機器等をはじめ10年以上の長期にわたって使用され、構築・接続時に適用したセキュリティ対策が危殆化

3）IoT機器に対する監視が行き届きにくい

画面がなく問題の発生がわかりづらい上に、人目が行き届きにくく勝手なネットワーク接続をされかねない

4）IoT機器側とネットワーク側の環境や特性の相互理解が不十分である

IoT機器と接続ネットワークの双方でセキュリティ要件の整合をとらなければ、必要な安全性等をみたせない

5）IoT機器の機能・性能が限られている

適切な暗号等のセキュリティ対策を適用できない場合が存在

6）開発者が想定していなかった接続が行われる可能性がある

これまで外部につながっていなかったモノがネットワークに接続され、当初想定していなかった影響が発生

（出展：IoTセキュリティガイドラインver1.0　平成28年7月　IoT推進コンソーシアム・総務省・経済産業省）

IoT機器における脅威の事例

①ウェブカメラの事例

ネットに接続されるウェブカメラなどの映像や音声がインターネット上で**誰でも閲覧できる設定**となっていることが判明。

②複合機の事例

日本の大学等において、複合機に保存されたデータがインターネット上で**誰でも閲覧できる設定**となっていた。

③水道関連設備

病院等に設置された水道関連設備のデータロガーがインターネット側からアクセス可能なまま運用されており、**動作状況が外部から閲覧可能**な状態であることに加え、**第３者から運転モード(RUN/STOP)の切り替えが可能**な状態になっていた。

④電力監視設備

工場等に設置された電力監視機器システムがインターネット側からアクセス可能なまま運用されており、**警告の閾値の変更、警告の解除、プロキシ設定、再起動等の操作が、第３者が可能**な状態になっていた。

政府の取組について

政府全体のサイバーセキュリティ推進体制

内閣　内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 サイバーセキュリティ基本法により設置）

本部長　内閣官房長官
副本部長　**サイバーセキュリティ戦略本部に関する事務を担当する国務大臣**
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（ＩＴ）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣 ※1
有識者 ※2（８名；10名以下）

閣僚が参画

遠藤　信博	日本電気株式会社取締役会長
小野寺　正	ＫＤＤＩ株式会社相談役
後藤　厚宏	情報セキュリティ大学院大学学長
中谷　和弘	東京大学大学院法学政治学研究科教授
野原佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	日本大学大学院法務研究科教授
宮澤　栄一	株式会社デジタルハーツホールディングス取締役会長
村井　純	慶應義塾大学環境情報学部教授

※1 平成27年７月22日付け内閣総理大臣決定により本部員に指定
※2 令和元年6月25日現在

重要インフラ専門調査会 ／ 研究開発戦略専門調査会 ／ 普及啓発・人材育成専門調査会 ／ サイバーセキュリティ対策推進会議（CISO等連絡会議）

（事務局）

緊密連携

国家安全保障会議（NSC）

我が国の安全保障に関する重要事項を審議

連携

サイバーセキュリティ協議会

官民の多様な主体が相互に連携した、より早期の段階での、サイバーセキュリティの確保に資する情報の迅速な共有等

内閣官房　内閣サイバーセキュリティセンター（2015.1.9 内閣官房組織令により設置）

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
上席サイバーセキュリティ分析官
サイバーセキュリティ参与

政府関係機関・情報セキュリティ横断監視・即応調整チーム（ＧＳＯＣ）
情報セキュリティ緊急支援チーム（CYMAT）

協力

＜重要インフラ所管省庁＞

金融庁（金融機関）
総務省（地方公共団体、情報通信）
厚生労働省（医療、水道）
経済産業省（電力、ガス、化学、クレジット、石油）
国土交通省（鉄道、航空、物流、空港）

＜その他関係省庁＞

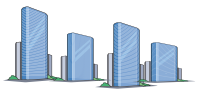
文部科学省（セキュリティ教育）等

協力

閣僚本部員５省庁

警察庁（サイバー犯罪・攻撃の取締り）
総務省（通信・ネットワーク政策）
外務省（外交・安全保障）
経済産業省（情報政策）
防衛省（国の防衛）


重要インフラ事業者等


政府機関（各府省庁）

企業


個人

「サイバーセキュリティ戦略」（平成30年7月27日 閣議決定）の全体概要

中長期的

戦略期間（2018～2021年（3年間））

1 策定の趣旨・背景

1．1． サイバー空間がもたらすパラダイムシフト（サイバー空間では、創意工夫で活動を飛躍的に拡張できる。人類がこれまでに経験したことのないSociety5.0へのパラダイムシフト）

1．2． 2015年以降の状況変化（サイバー空間と実空間の一体化の進展に伴う脅威の深刻化、2020年東京大会等を見据えた新たな戦略の必要性）

2 サイバー空間に係る認識

2．1． サイバー空間がもたらす恩恵

・人工知能（AI）、IoT※などサイバー空間における知見や技術、サービスが社会に定着し、既存構造を覆すイノベーションを牽引。**様々な分野で当然に利用**され、人々に豊かさをもたらしている。

※：Internet of Thingsの略

2．2． サイバー空間における脅威の深刻化

・技術等を**制御できなくなるおそれは常に内在**。IoT、重要インフラ、サプライチェーンを狙った攻撃等により、国家の関与が疑われる事案も含め、多大な経済的・社会的な損失が生ずる可能性は拡大

3 本戦略の目的

3．1． **基本的な立場の堅持**

（1）基本法の目的（2）基本的な理念（「自由、公正かつ安全なサイバー空間」）（3）基本原則（情報の自由な流通の確保、法の支配、開放性、自律性、多様な主体の連携）

3．2． 目指すサイバーセキュリティの基本的な在り方

（1）目指す姿（**持続的発展のためのサイバーセキュリティ（「サイバーセキュリティエコシステム」）の推進**）（2）主な観点（①サービス提供者の**任務保証**、②**リスクマネジメント**、③**参加・連携・協働**）

4 目的達成のための施策

経済社会の活力の向上及び持続的発展

1．新たな価値創出を支えるサイバーセキュリティの推進

＜施策例＞ **経営層の意識改革の促進（「費用」から「投資」へ）**

・投資に向けたインセンティブ創出（情報発信・開示による市場の評価、保険の活用）

・セキュリティ・バイ・デザインに基づくサイバーセキュリティビジネスの強化

2．多様なつながりから価値を生み出すサプライチェーンの実現

＜施策例＞ **中小企業を含めたサプライチェーン（機器・データ・サービス等の供給網）におけるサイバーセキュリティ対策指針の策定**

3．安全なIoTシステムの構築

＜施策例＞ IoTシステムにおけるセキュリティの体系の整備と国際標準化

・**IoT機器の脆弱性対策モデルの構築・国際発信**

等

国民が安全で安心して暮らせる社会の実現

1．国民・社会を守るための取組

＜施策例＞・脅威に対する事前の防御（**積極的サイバー防御**）策の構築

・サイバー犯罪への対策

2．官民一体となった重要インフラの防護

＜施策例＞・安全基準等の改善・浸透（サイバーセキュリティ対策の**関係法令等における保安規制としての位置付け**）

・地方公共団体のセキュリティ強化・充実

3．政府機関等におけるセキュリティ強化・充実

＜施策例＞・**情報システムの状態のリアルタイム管理の強化**

・先端技術の活用による先取り対応への挑戦

4．大学等における安全・安心な教育・研究環境の確保

＜施策例＞・**大学等**の多様性を踏まえた対策の推進

5．2020年東京大会とその後を見据えた取組

＜施策例＞・**サイバーセキュリティ対処調整センターの構築の推進**

・成果のレガシーとしての活用

6．従来の枠を超えた情報共有・連携体制の構築

＜施策例＞・**多様な主体の情報共有・連携の推進**

7．大規模サイバー攻撃事態等への対処態勢の強化

＜施策例＞・**サイバー空間と実空間の双方の危機管理に臨むための大規模サイバー攻撃事態等への対処態勢の強化**

等

国際社会の平和・安定及び我が国の安全保障への寄与

1．自由、公正かつ安全なサイバー空間の堅持

＜施策例＞・**自由、公正かつ安全なサイバー空間**の理念の発信

・サイバー空間における法の支配の推進

2．我が国の防御力・抑止力・状況把握力の強化

＜施策例＞・国家の**強靭性の確保**（①任務保証、②我が国の先端技術・防衛関連技術の防護、③サイバー空間を悪用したテロ組織の活動への対策）

・サイバー攻撃に対する**抑止力の向上**（①実効的な抑止のための対応、②信頼醸成措置）

・サイバー空間の**状況把握の強化**（①関係機関の能力向上、②脅威情報連携）

3．国際協力・連携

＜施策例＞・**知見の共有・政策調整**

・事故対応等に係る国際連携の強化

・能力構築支援

等

横断的施策

人材育成・確保	＜施策例＞**戦略マネジメント層の育成・定着**、実務者層・技術者層の育成（**高度人材**含む）、人材育成基盤の整備、**政府人材**の確保・育成の強化、国際連携の推進
研究開発の推進	＜施策例＞実践的な研究開発の推進（**検知・防御等の能力向上、不正プログラム等の技術的検証**を行うための体制整備）、**AI等**中長期的な技術・社会の進化を視野に入れた対応
全員参加による協働	＜施策例＞サイバーセキュリティの普及啓発に向けた**アクションプランの策定、国民への情報発信**（サイバーセキュリティ月間の充実等）、サイバーセキュリティ教育の推進

5 推進体制

本戦略の実現に向け、サイバーセキュリティ戦略本部の下、**内閣サイバーセキュリティセンターを中心に関係機関の一層の能力強化**を図るとともに、同センターが、各府省庁間の総合調整、産学官民連携の促進の要となる主導的役割を担う。**施策が着実かつ効果的に実施されるよう必要な予算の確保と執行を図る。** 等

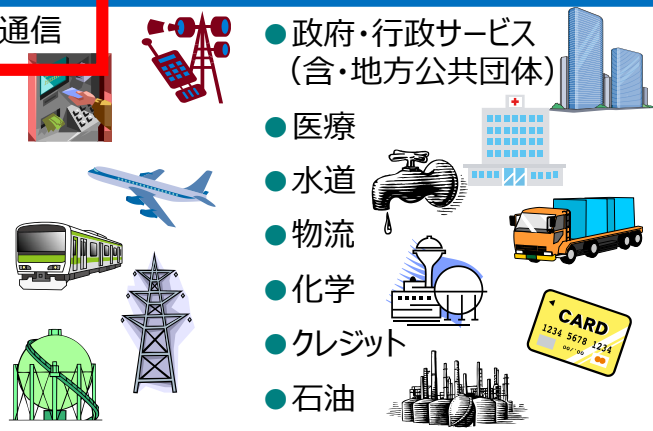
重要インフラの情報セキュリティ対策に係る第４次行動計画

官民連携による重要インフラ防護の推進

重要インフラにおいて、機能保証の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する。

重要インフラ（１４分野）

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油



ＮＩＳＣによる調整・連携

重要インフラ所管省庁（５省庁）

- 金融庁　［金融］
- 総務省　［情報通信、行政］
- 厚生労働省　［医療、水道］
- 経済産業省　［電力、ガス、化学、クレジット、石油］
- 国土交通省　［航空、空港、鉄道、物流］

関係機関等

- 情報セキュリティ関係省庁［総務省、経済産業省等］
- 事案対処省庁［警察庁、防衛省等］
- 防災関係府省庁［内閣府、各省庁等］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］

重要インフラの情報セキュリティ対策に係る第４次行動計画

安全基準等の整備・浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備

リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

出典：内閣官房内閣サイバーセキュリティセンター作成資料

2020年「サイバーセキュリティ月間」（２月１日～３月18日）について

- 重点的かつ効果的にサイバーセキュリティに対する取組を推進するため、2010年より、毎年**2月1日から3月18日**を「**サイバーセキュリティ月間**」に設定。各種啓発主体と連携し、サイバーセキュリティに関する**普及啓発**活動を集中的に実施。
- 「**サイバーセキュリティは全員参加**」をキャッチフレーズに、若年層に認知度の高いコンテンツとタイアップしつつ、SNSにおいてインフルエンサーを起用すること等により、**インターネットを介して全国へ**サイバーセキュリティ月間を伝播させつつ、サイバーセキュリティに対する関心を高めていただく。

今年度実施予定の主な取組

認知度の高いコンテンツとのタイアップ

- 『**ソードアート・オンライン-アリシゼーション-War of Underworld**』とタイアップし、若年層やサイバーセキュリティに関心の薄い層等を含む幅広い層にサイバーセキュリティに対する関心を高めていただく。
- サイバーセキュリティ月間のポスターやWebバナーを産学官民で連携して掲載し、サイバーセキュリティ月間をより多くの国民に知っていただくきっかけをつくる。

情報発信の強化

- **官房長官トップメッセージ**を発信。
- NISCや関係機関のSNSアカウント等において「**＃サイバーセキュリティは全員参加**」をつけた情報発信。
- NISCのWebサイトで、有識者による週替わりコラム「**サイバーセキュリティ　ひとこと言いたい！**」を発信。
- 各種啓発主体の実施する行事を**サイバーセキュリティ月間関連行事**（2020年1月下旬時点で150件）と位置付け、NISCのWebサイトやSNSで案内を行う。
- SNSで**10代を中心に多くのフォロワーを抱えるインフルエンサーを起用**し、サイバーセキュリティを啓発する投稿を行うことで、サイバーセキュリティに関心の薄い層にもサイバーセキュリティに対する関心を高めていただく。

イベント・行事の開催

- **NISC-CTF （2020年2月19日）**（CTF：Capture The Flag、セキュリティ技術の競技）
  各府省庁・独法等の職員がサイバーセキュリティに関する幅広い技術・能力を競う競技会を開催。
- **NISC主催イベントの開催（2020年3月8日）**
  秋葉原駅周辺にて、ステージや展示、来場者参加型イベントを行い、サイバーセキュリティへの意識・理解の醸成を図る。

『ソードアート・オンライン-アリシゼーション-War of Underworld』

サイバー空間を舞台に、主人公・キリトと仲間たちが、敵の侵攻から仮想世界《Underworld》を守るために立ち上がる物語。若年層のファンを中心に支持を誇る。2020年４月より2ndクールが放送予定。

・『ソードアート・オンライン』シリーズは川原 礫氏による小説作品で、2009年4月の第1巻発売以来、累計発行部数は国内1500万部、全世界で2200万部を突破。
・今回の仮想世界《Underworld》は、AIが人間と同様に育っていく世界を表現している。

NISC　サイバーセキュリティ月間

<2020 年サイバーセキュリティ月間ポスターイラスト>

NISC　サイバーセキュリティ月間報道発表より

総務省の取組について

総務省
Ministry of Internal Affairs and Communications

サイバーセキュリティタスクフォースについて

趣旨

○　2020年東京オリンピック・パラリンピック競技大会を控え、IoT/AI時代を見据えたサイバーセキュリティに係る課題を整理するとともに、情報通信分野において講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、サイバーセキュリティタスクフォースを開催。
○　本タスクフォースは、サイバーセキュリティ統括官の会合として開催。

体制

○　本タスクフォースは座長１名、座長代理１名、委員14名
○　事務局は、サイバーセキュリティ統括官室が行う。

議題

○　IoT/AI時代のサイバーセキュリティを支える基盤・制度　（IoTなど新たな脅威への対応方策等）
○　IoT/AI時代のサイバーセキュリティを担う人材育成　（産学官連携体制の構築等）
○　IoT/AI時代のサイバーセキュリティ確保に向けた国際連携（情報共有、ｾｷｭﾘﾃｨ技術の海外展開等）
○　その他

スケジュール

第１回 2017年1月30日（現状把握、課題整理）
第２回 2017年3月　8日（IoTセキュリティ対策）
第３回 2017年3月27日（IoTセキュリティ対策の取組方針）
第４回 2017年5月15日（情報共有、国際連携）
第５回 2017年5月31日（人材育成、研究開発）
第６回 2017年6月29日（これまでの議論と今後の検討の方向性（案）、リスクマネジメント　等）
第７回 2017年8月　2日（匿名化技術、とりまとめ骨子）
第８回 2017年9月25日（IoTセキュリティ総合対策（案））
第９回 2018年4月11日（IoTセキュリティ総合対策の取組状況、分科会からの報告）
第10回 2018年7月2日（「IoTセキュリティ総合対策 プログレスレポート2018（案）」について）
第11回 2018年11月15日（「国立研究開発法人情報通信研究機構が実施するパスワード設定等に不備のあるIoT機器調査について）
第10回 2018年7月2日（「IoTセキュリティ総合対策 プログレスレポート2018（案）」について）
第11回 2018年11月15日（「国立研究開発法人情報通信研究機構が実施するパスワード設定等に不備のあるIoT機器調査について
第12回 2019年3月26日（「IoTセキュリティ総合対策」の主な取組の進捗　状況等について）
第13回 2019年5月10日（「IoTセキュリティ総合対策」の見直しの方向性）
第14回 2019年6月14日（「IoTセキュリティ総合対策改定版（仮称）（案）」について）
第15回 2019年8月23日（メール審議「IoT・5Gセキュリティ総合対策（案）等について」）～８月28日
第16回2019年11月1日（今後の検討課題等について）
第17回2019年11月22日（今後の検討課題とスケジュールについて）
第18回2019年12月5日（前回までの御議論について）
第19回2019年12月25日（前回までの御議論と今後の進め方等について）
第20回2020年1月27日（我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]（案）について）

※以降、随時開催予定

サイバーセキュリティタスクフォースの構成員

タスクフォース構成員（敬称略）

	鵜飼　裕司	株式会社FFRI　代表取締役社長
	岡村　久道	英知法律事務所 弁護士、京都大学大学院医学研究科　講師
（座長）	後藤　厚宏	情報セキュリティ大学院大学　学長
	斎藤　善昭	株式会社テレビ東京 IT推進局長
	小山　覚	NTTコミュニケーションズ情報セキュリティ部　部長
	篠田　佳奈	株式会社BLUE　代表取締役
	園田　道夫	国立研究開発法人情報通信研究機構（NICT）、ナショナルサイバートレーニングセンター　センター長
	辻　伸弘	ソフトバンク・テクノロジー株式会社　プリンシパルセキュリティリサーチャー
	戸川　望	早稲田大学理工学術院　教授
（座長代理）	徳田　英幸	国立研究開発法人情報通信研究機構（NICT）理事長、慶應義塾大学 名誉教授
	中尾　康二	ICT-ISAC　ステアリングコミッティ委員長、国立研究開発法人情報通信研究機構 主管研究員
	名和　利男	サイバーディフェンス研究所　専務理事/上級分析官
	林　紘一郎	情報セキュリティ大学院大学前学長・名誉教授
	藤本　正代	情報セキュリティ大学院大学　教授
	吉岡　克成	横浜国立大学大学院環境情報研究院/先端科学高等研究院　准教授
	若江　雅子	株式会社読売新聞東京本社　編集委員

タスクフォースオブザーバ

内閣官房内閣サイバーセキュリティセンター、内閣官房IT総合戦略室、経済産業省、地方公共団体情報システム機構

IoT・5Gセキュリティ総合対策について

■ ICTの利活用が一層進展していく中で、5Gのサービスの開始、データ管理・流通の重要性やサプライチェーンリスクへの対応などの必要性が増大していること等を踏まえ、IoT・5G時代にふさわしいサイバーセキュリティ対策の在り方について検討し、総務省として取り組むべき課題を「IoT・5Gセキュリティ総合対策」として策定し令和元年8月に公表（※）。

● 直近で留意すべき事項

1 5Gのサービス開始に伴う新たなリスク

- ✓ 仮想化、ソフトウェア化、モバイルエッジコンピューティング
- ✓ 産業用途でのIoT機器の設置・運用

2 サプライチェーンリスクの管理の重要性

- ✓ ICTの製品・サービスの製造・流通過程でのリスク
- ✓ 委託先が踏み台となって攻撃を受けるケース

3 Society5.0の実現に向けたデータの流通・管理の重要性

- ✓ クラウドサービスやスマートシティなどのセキュリティの確保の重要性
- ✓ トラストサービスの必要性

4 サイバーセキュリティにおけるAI利活用の重要性

- ✓ AIの活用が進展する中で、特にAIを利活用したサイバーセキュリティ対策を促進することが必要

5 大規模な量子コンピュータの実用化の可能性

- ✓ 将来の大規模な量子コンピュータの実用化の可能性を踏まえ、現時点から新たな推奨暗号の在り方について検討の必要性

6 大規模な国際イベント等の開催

- ✓ ラグビーワールドカップや東京オリンピック・パラリンピック大会の円滑な実施、及びその後も見据え、対策の着実な実施が必要

● IoT・5Gセキュリティ総合対策の枠組み

重点的に対応すべき情報通信サービス・ネットワークの個別分野等に関する具体的施策

- ✓ IoT、5G、クラウドサービス、スマートシティのセキュリティ　など
- ✓ トラストサービスの在り方の検討　など

具体的施策間でも連携

連携　連携　連携　連携

研究開発	人材育成 普及啓発	情報共有 情報開示	国際連携
✓ ハードウェア脆弱性 ✓ AI ✓ 暗号 など	✓ 2020東京大会向け人材育成 ✓ 地域の人材育成 など	✓ 情報共有基盤 ✓ 情報開示の促進 など	✓ ASEAN各国との連携 ✓ 国際標準化 など

（※）これに先立ち、2017年（平成29年）には、IoT機器・システムのセキュリティ等の確保を主眼においた「IoTセキュリティ総合対策」を策定・公表

サイバーセキュリティタスクフォースの再開について

■ 2017年１月より開催しているサイバーセキュリティタスクフォースでは、IoT/AI時代を見据えたサイバーセキュリティに係る課題を整理をしつつ、必要な方策の取りまとめを実施。

【過去の実施内容】

2017年10月 「IoTセキュリティ総合対策」を取りまとめ、公表
2018年７月 「IoTセキュリティ総合対策　プログレスレポート2018」を取りまとめ、公表
2019年５月 「IoTセキュリティ総合対策　プログレスレポート2019」を取りまとめ、公表
2019年８月 「IoT・5Gセキュリティ総合対策」を取りまとめ、公表

■ 東京2020大会を控える中、総務省として**短期・中長期で取り組むべき政策課題を検討**するため、2019年11月1日（第16回会合）に再開し、2020年１月27日（第20回会合）までに計5回開催。

主な検討事項

【短期的な検討事項】

①重要インフラ事業者等が設置するIoT機器のセキュリティ確保

②地方公共団体や重要インフラ事業者等の人材育成

③サイバーセキュリティの質の向上のため実効的な情報共有体制

④ Wi-Fiの安全な利用のための周知徹底

⑤重要インフラ事業者等のサイバーセキュリティ対策等の実効性の確保

【中長期な検討事項】

■ 短期的な検討事項での議論を踏まえ、2020年1月28日に『**我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]**』をとりまとめ、公表。

我が国のサイバーセキュリティ強化に向け早期に取り組むべき事項［緊急提言］の概要

■ サイバーセキュリティタスクフォースにおける「IoT・5Gセキュリティ総合対策」の策定・公表後の議論を踏まえ、2020年７月より開催される2020年東京大会に向けた対処として早急に取り組むべき事項を整理したもの。

1 IoT機器のセキュリティ対策の拡充

- ✓ 脆弱な状態にあるIoT機器について注意喚起方法の一層の改善を図ることが必要
- ✓ 重要施設に設置されているIoT機器に対して新たに注意喚起を実施することが必要

2 地方公共団体向け実践的サイバー防御演習（CYDER）の繰り上げ実施等

- ✓ 2020年東京大会前に未受講の地方公共団体を中心としてCYDERの集中的な受講機会を設けることが必要
- ✓ CYDERのオンライン受講を早期に開始することが必要

3 サイバーセキュリティに関する情報共有体制の強化

- ✓ 個人情報などの流出が疑われる時点で、速やかにインシデントに関する情報の公表を検討することが望ましい
- ✓ 類似の被害の拡大を防ぐ観点から、インシデントに関する情報の共有を速やかに行うことが求められる
- ✓ 先行的に始まったISACの知見やノウハウの展開を通じて、重要インフラ分野等におけるISACの立ち上げを促進することが必要

4 公衆無線LANのセキュリティ対策

- ✓ 公衆無線LANサービスの利用者及び提供者に対し、公衆無線LANのセキュリティ対策の状況や自ら講じるべきセキュリティ対策の周知を強化するため、ガイドラインを年度内に改定し、ホテル、病院、学校等への周知を強化することが必要

5 制度的枠組みの改善

- ✓ サイバーセキュリティ対策等の法令への位置づけや、官民のガイドラインや基準について周知し、対応の強化を呼びかけていくことが必要
- ✓ 放送設備のサイバーセキュリティ確保に関する省令改正を速やかに実施することが必要
- ✓ 各地方公共団体における情報セキュリティ対策及び緊急時連絡体制の確保等の徹底を図ることが必要

国立研究開発法人情報通信研究機構法の改正について

➢ IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構(NICT)の業務に、**パスワード設定等に不備のあるIoT機器の調査**等を追加（**５年間の時限措置**）する等を内容とする**国立研究開発法人情報通信研究機構法の改正を行い、平成30年11月１日に施行。**

サイバー脅威の深刻化

IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。

※IoT機器を狙った攻撃は全体の３分の２(2016年)

対策の必要性

パスワード設定等に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備

NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進。→ **NOTICE**

情報通信研究機構法の改正

中長期目標･計画

意見聴取

CS戦略本部 ← **総務大臣**

実施計画認可

中長期目標変更･計画認可

これまで送信型対電気通信設備サイバー攻撃のために用いられたもの	password 、admin1234 、supervisor、smcadmin
同一の文字のみ又は連続した文字のみを用いたもの	aaaaaaaa、11111111、abcdefgh、12345678

情報通信研究機構

①機器調査

特定アクセス行為により、パスワード設定等に不備のある機器を（その機器に係るIPアドレス）特定

パスワード設定等に不備のある機器に係るIPアドレス等を提供

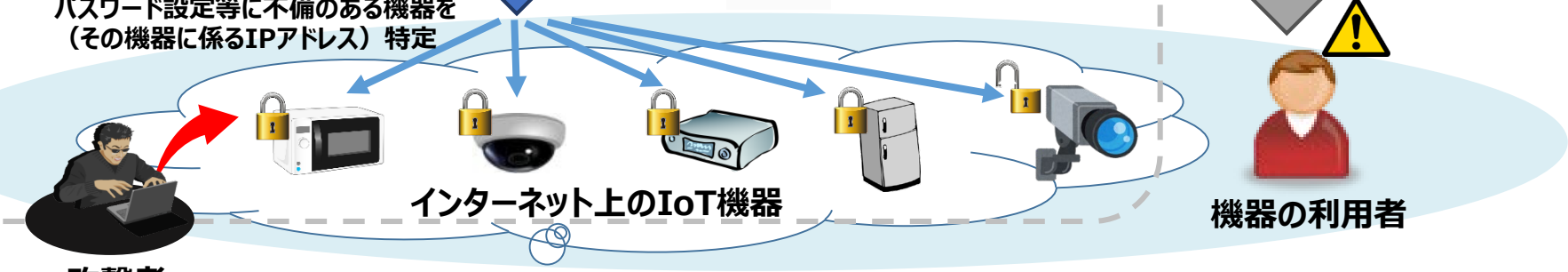
②情報提供

第三者機関

※ 改正後の電気通信事業法に規定する第三者機関に委託

電気通信事業者

③注意喚起



攻撃者

インターネット上のIoT機器

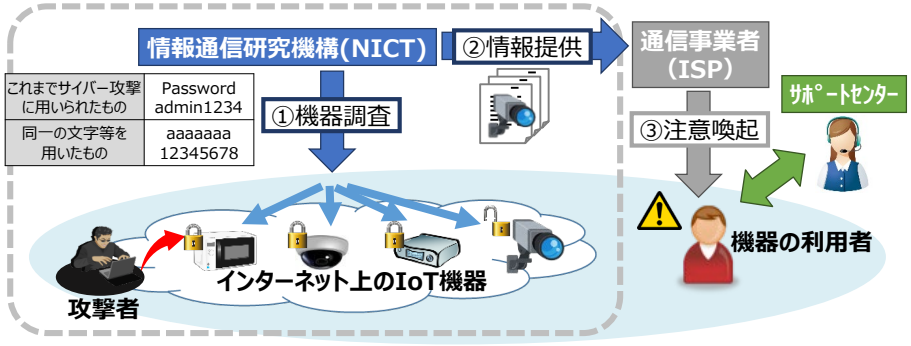
機器の利用者

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。

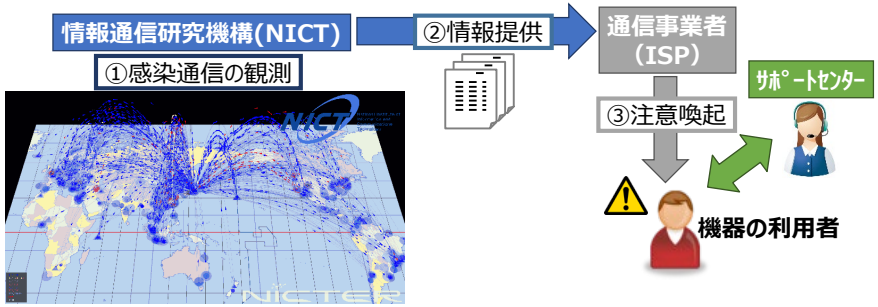
【NOTICEの概要】



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。

【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の取組概要】



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

NOTICEに係る周知広報

- IoT機器のセキュリティ対策の必要性、本取組の内容の広報のため、公共機関等でのポスター掲示に加え、新聞広告、交通広告等を令和元年2月中旬から実施。
- また、本取組の概要を記載したリーフレットを作成し、家電量販店やサイバーセキュリティ関連のセミナー等での配布を実施。

周知ポスター

周知ポスター掲載場所一覧

1．大手家電量販店（計約3000店舗）
　エディオン系列、ケーズデンキ系列、上新電機、
　ビックカメラ系列、ヤマダ電機系列

2．地方自治体（約500団体）

3．東京メトロ駅構内（10駅）

4．電車中吊広告
　東京メトロ全線、JR山手線等

駅構内サイネージ広告

（※全国主要39駅）

新聞広告

IoT機器調査及び利用者への注意喚起結果（2019年12月まで）

➢ 2019年12月までに調査のための手続きが完了しているインターネット・サービス・プロバイダ（ISP）41社に係る約1.1億IPアドレスに対して調査を実施。

【NOTICEの取組結果】

ID・パスワードが入力可能であったもの → 約111,000件（直近での調査）【9月時点：約98,000件】

上記の内、ID・パスワードによりログインでき、注意喚起の対象となったもの → 延べ1,328件【9月時点：延べ505件】

【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の取組結果】

ISPに対する通知の対象となったもの → 60～598件（1日当たり）【9月時点：80～559件】

（参加ISP：計41社） ※下線は2019年度第3四半期の新規参加ISP（7社）

株式会社秋田ケーブルテレビ
諫早ケーブルメディア株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社
株式会社愛媛CATV
近鉄ケーブルネットワーク株式会社
ケーブルテレビ株式会社
山陰ケーブルビジョン株式会社
株式会社ジュピターテレコム（グループ会社計10社）
ソフトバンク株式会社
株式会社TOKAIコミュニケーションズ
ビッグローブ株式会社
株式会社朝日ネット
イッツ・コミュニケーションズ株式会社
株式会社NTTドコモ
株式会社オプテージ
グリーンシティケーブルテレビ株式会社
株式会社ケーブルテレビ品川
GMOインターネット株式会社
株式会社ZTV
株式会社テレビ岸和田
東北インテリジェント通信株式会社
株式会社ベイ・コミュニケーションズ
アルテリア・ネットワークス株式会社
株式会社インターネットイニシアティブ
株式会社NTTぷらら
株式会社Qtnet
KDDI株式会社
株式会社ケーブルネット鈴鹿
株式会社シー・ティー・ワイ
ソニーネットワークコミュニケーションズ株式会社
株式会社TOKAIケーブルネットワーク
ニフティ株式会社

参考　（一社）デジタルライフ推進協会（DLPA）推奨Wi-Fiルータ

- 一般社団法人デジタルライフ推進協会（DLPA）は、出荷時からセキュリティ対策機能が搭載されている家庭用Wi-Fiルーターを「**DLPA推奨Wi-Fiルータ**」として推奨。
- DLPA加盟社のうち４社※がDLPA推奨Wi-Fiルーターを販売中。

※(株)アイ・オー・データ機器、NECプラットフォームズ(株)、エレコム(株)、(株)バッファロー

DLPA推奨Wi-Fiルータ

以下の２つのセキュリティ対策機能を出荷時から搭載。

① ファームウェアの自動更新

② １台ごとに固有の管理画面用ログインID又はパスワードを設定

（出典：DLPAウェブサイト https://dlpa.jp/wifi_support/）

【(一社)デジタルライフ推進協会（DLPA：Digital Life Promotion Association）について】

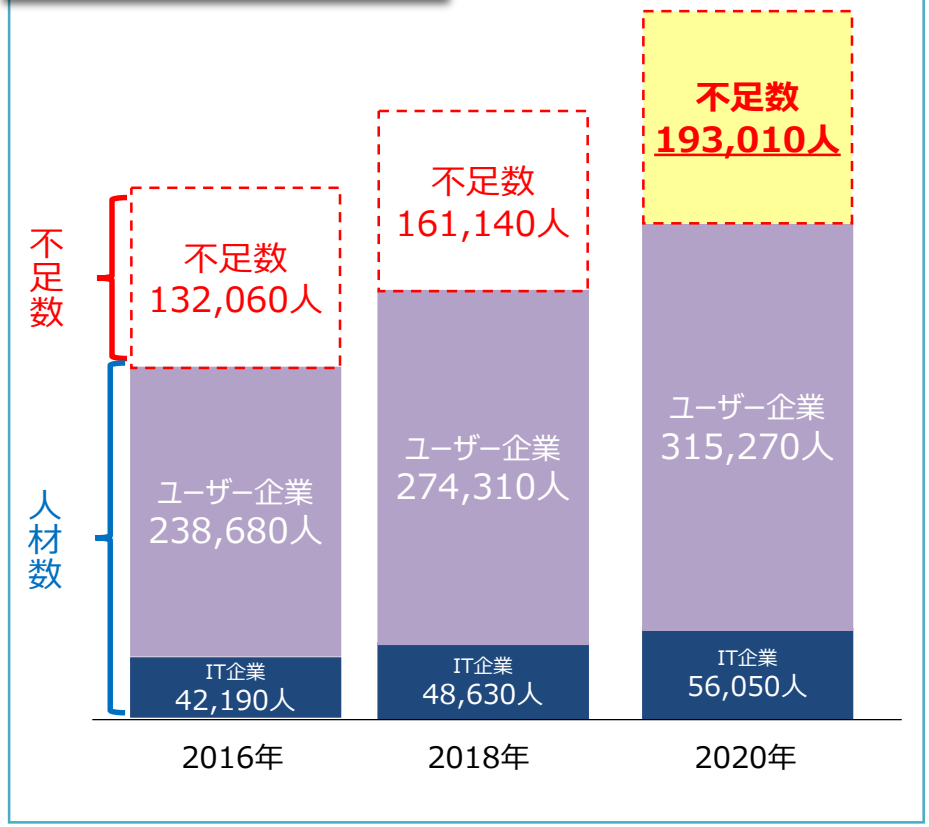
一般社団法人 デジタルライフ推進協会 Digital Life Promotion Association

- デジタル技術の進歩により可能となる新たなデジタル技術の活用形態＝「デジタルライフ」における利用者の利便性を守り、その健全な発展に寄与することを目的として、2010年に設立
- デジタルライフの普及・啓発活動や業界共通仕様の策定等を実施
- Wi-Fiルータや外付けハードディスク等のデジタル機器のメーカが加盟

セキュリティ人材の不足

■2016年時点で情報セキュリティ人材が13.2万人不足と推計。2020年には、不足数が19.3万人に増加するとも見込まれている。
■中小企業（従業員数５人～99人、100人～299人）では、2016年時点で最大15.6万人不足と推計。

情報セキュリティ人材の不足数推計



うち中小企業

従業員数	業種	セキュリティ人材不足数（専任者のみ）（人）
5～99 人	製造業	18,113.2
	サービス業	67,120.4
	その他	18,795.1
100～299 人	製造業	11,778.5
	サービス業	34,707.6
	その他	6,018.6
	計	156,533.4

※不足数を全て専任者で補う場合のシナリオ

従業員数	業種	セキュリティ人材不足数（専任者のみ）（人）
5～99 人	製造業	1,723.7
	サービス業	6,474.2
	その他	2,022.5
100～299 人	製造業	2,098.3
	サービス業	6,733.2
	その他	1,369.8
	計	20,421.7

※不足数を専任者と兼任者で補う場合のシナリオ

出典：経済産業省「IT人材の最新動向と将来推計に関する調査結果」（平成28年６月）及びみずほ情報総研「ITベンチャー等によるイノベーション促進のための人材育成・確保モデル事業　事業報告書 第２部 今後のIT人材需給推計モデル構築等 編」（平成28年３月）をもとに総務省作成
http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf
http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_fullreport.pdf

セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

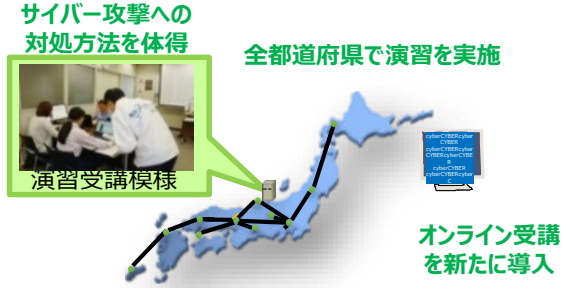
■ 巧妙化・複雑化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月より、情報通信研究機構（NICT）の「ナショナルサイバートレーニングセンター」において、以下の実践的サイバー演習等を積極的に推進。

① 国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等を対象とした実践的サイバー防御演習（CYDER）

② 2020年東京オリンピック・パラリンピック競技大会に向けた大会関連組織のセキュリティ担当者等を対象者とした実践的サイバー演習（サイバーコロッセオ）

③ 若手セキュリティイノベーターの育成（SecHack365）

CYDER



実事案に対処可能な人材育成

新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発

高度な攻撃に対処可能な人材育成

サイバーコロッセオ

ハイレベル層の人材育成

SecHack365

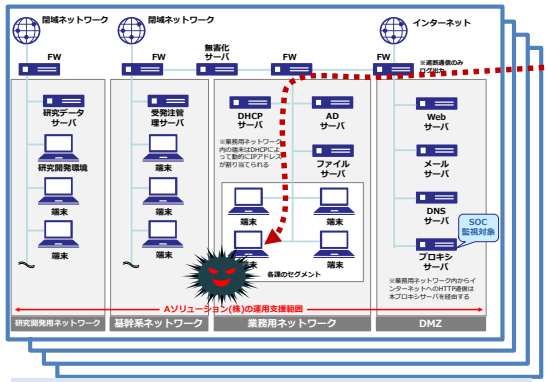
実践的サイバー防御演習（CYDER）

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。
  ※平成29年度は、年間100回・3,009名が受講。平成30年度は、年間107回・2,666名が受講。

演習のイメージ

NICTの有する技術的知見を活用し、サイバー攻撃に係る我が国固有の傾向等を徹底分析し、現実のサイバー攻撃事例を再現した**最新の演習シナリオ**をコースごとに用意。



実際の**大規模LANを模した環境**を、**受講チームごと**に専用環境として**構築**

擬似攻撃者

NICT北陸StarBED技術センターに設置された大規模高性能サーバー群を活用

演習実施模様
専門の指導員による補助

機材・データを使用して**本番同様の作業**を実施

インシデント（事案）対処能力の向上

令和２年度の実施計画（調整中）

コース	受講対象組織	対象者	開催地	開催回数	実施時期
A-1コース（初級）	地方公共団体	システムの運用担当者（システムの利用者レベルを含む）	４７都道府県	２５回	４月下旬～７月
A-2コース（初級）	全組織共通			４０回	７月以降
B-1コース（中級）	地方公共団体	セキュリティ管理業務を主導する立場の者	全国１１地域	２０回	秋以降
B-2コース（中級）	国の機関等、重要インフラ事業者等		東京・大阪・名古屋	１５回	秋以降

CYDERの演習内容例

- 地方公共団体に対してサイバー攻撃が行われ、情報流出事案が発生した状況を実機を使って体験。
- 演習受講者は、仮想の市の情報担当職員として、迅速な調査や的確な報告・情報展開といった情報流出事案の対処方法について、演習を通じて体得。

演習の流れ

実機演習は1日で完結

事前学習（オンライン）

- オンラインで事前学習
- 最新のサイバー攻撃事案紹介
- 攻撃に利用されるツールや技術の紹介
- 演習で利用するネットワーク管理ツールや解析ツール等の説明

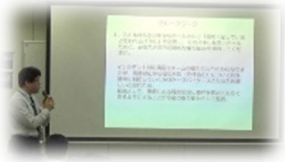
講義

- オンライン事前学習の振り返り
- サイバー攻撃対処の一連の流れの学習

演習

- 異常の検知、職員への注意喚起
- 不審なファイル解析、現状把握
- 状況のエスカレーション
- 内部感染の端末、原因の調査
- 情報漏洩報告

→ これら一連の作業を実機を用いて演習



振り返り

- 演習の振り返り、実機による作業確認
- 管理する際のポイントやベストプラクティス紹介
- 演習で学んだ結果や自組織へのフィードバックについてグループ発表

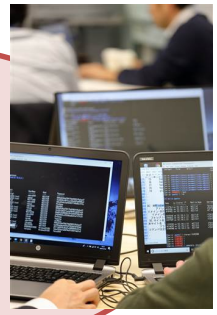
2020年東京大会に向けた実践的サイバー演習（サイバーコロッセオ）

- 近年さらに高度化・多様化するサイバー攻撃に備え、2020年東京オリンピック・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。
- 実機演習を伴う**コロッセオ演習**を補完する形で、演習時以外にも学習可能な**学習コンテンツ**を提供するとともに、**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**を開設。
- **コロッセオ演習**として、**令和元年度は**、初・中級コース各125名、準上級コース150名の**計400名**、**令和２年度は**、大会直前までに初・中級コース各50名、準上級コース75名の**計175名**を予定。（人数は延べ受講定員数）

イメージ図

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）



- 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忠実に再現した、仮想のネットワーク環境を構築。
- 仮想のネットワーク環境上で、東京2020大会時に想定されるサイバー攻撃を擬似的に発生させ、攻撃・防御手法の検証及び訓練を実施。

学習コンテンツ

コロッセオ演習当日以外でも学習可能なコンテンツを提供

コロッセオカレッジ

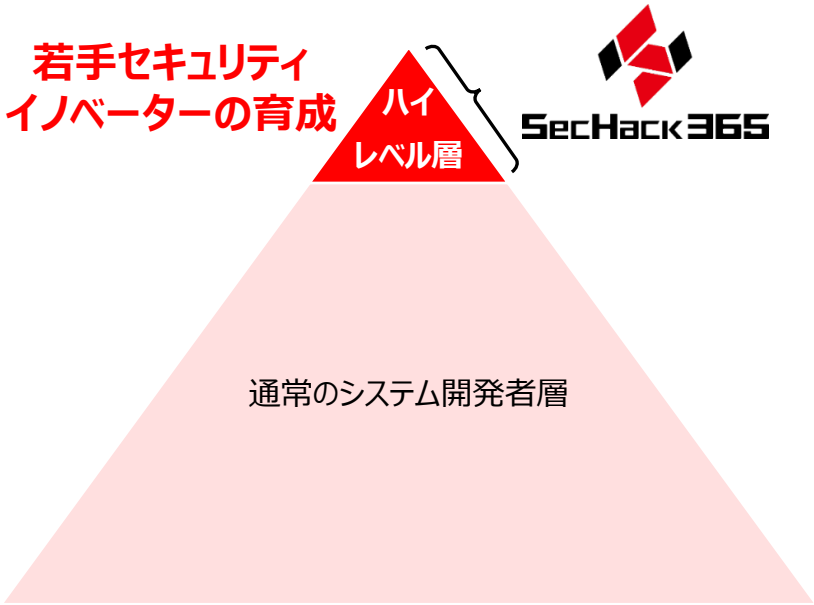
講義演習形式によりセキュリティ関係の知識や技能を学習

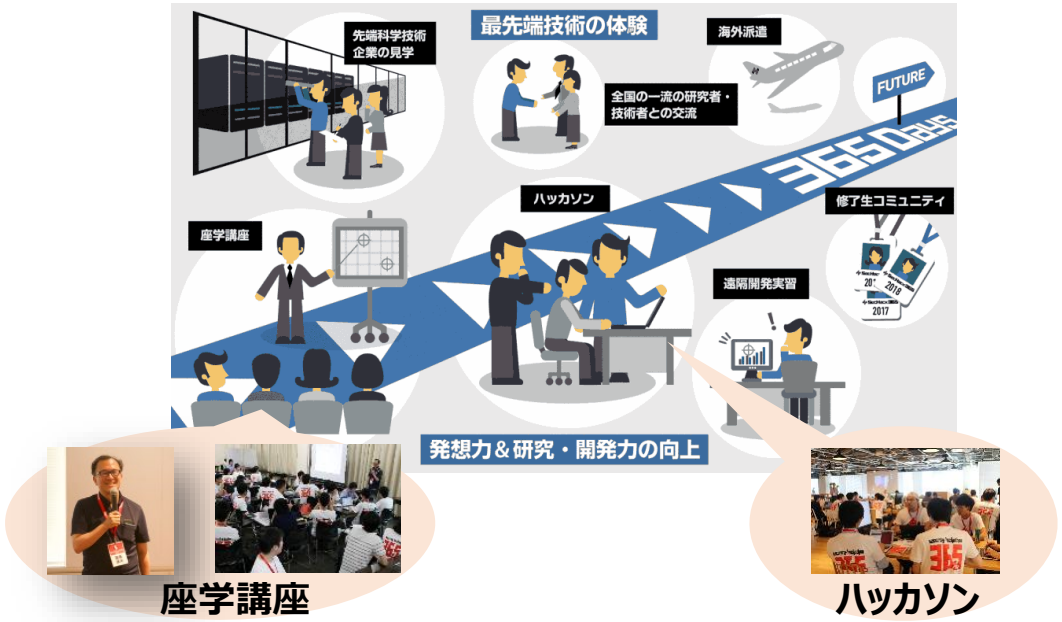
2020年東京オリンピック・パラリンピック競技大会のサイバーセキュリティを確保

SecHack365

- **未来のサイバーセキュリティ研究者・起業家の創出**に向けて、NICTの持つサイバーセキュリティの研究資産を活用し、**若年層のICT人材を対象**に実際のサイバー攻撃関連データに基づいたセキュリティ技術の研究・開発を、**第一線で活躍する研究者・技術者が１年かけて継続的かつ本格的に指導**。
- 対象者は、日本国内に居住する**25歳以下の若手ICT人材**（2017年度は39名、2018年度は46名が修了）。
- 受講者は、NICTの有する遠隔開発環境※を活用し、**年中どこからでも遠隔開発実習が可能**。また、集合イベントとして、**座学講座（研究倫理）**や**ハッカソン等**を実施。

※ NONSTOP（NICTER Open Network Security Test-out Platform）では、NICTの長年にわたるサイバーセキュリティ研究によって得られた膨大なセキュリティ関連データを活用することができ、NONSTOP内に整備された様々な研究開発・解析用ツール類と、他では触れることのできない貴重なデータを用いて研究・開発に取り組むことが可能。

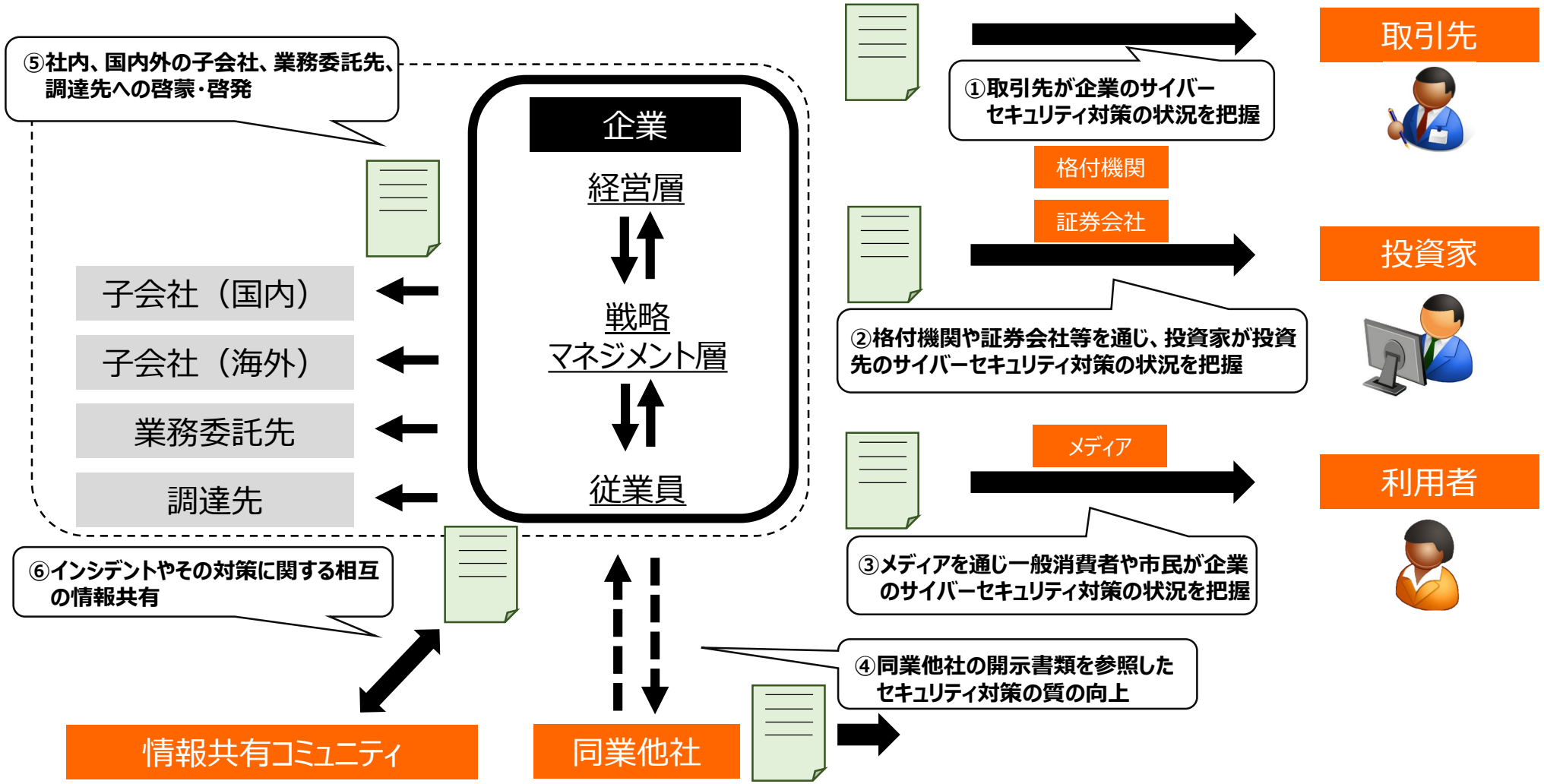




通年の遠隔開発実習＋年６回の集合研修（座学講座・ハッカソン等）の組合せによる総合的な人材育成プログラム

企業をとりまく様々なステークホルダーとサイバーセキュリティ対策の情報開示

- 取引先や投資家、利用者等のステークホルダーへの説明責任を果たすため、サイバーセキュリティ対策の情報開示が重要。
- 同業他社との比較やコミュニティでの情報共有、社内、グループ内、業務委託先、調達先への啓蒙を通じ、サイバーセキュリティ対策の向上に資する。



サイバーセキュリティ対策情報開示の手引きについて

■総務省では、平成29年12月より、サイバーセキュリティタスクフォース（座長：後藤　厚宏 情報セキュリティ大学院大学　学長）の下で「情報開示分科会」（主査：岡村久道　英知法律事務所 弁護士）を開催。
同分科会において、民間企業のサイバーセキュリティ対策の情報開示に関する課題を整理し、民間企業における サイバーセキュリティ対策の情報開示を促進するために必要な方策等について検討。

■今般、検討結果を踏まえ総務省において民間企業にとって参考となり得る情報開示の事例等をまとめた「サイバーセキュリティ対策情報開示の手引き」（案）を作成し、意見公募を経て令和元年6月に公表。

背景

✓ サイバー攻撃が深刻化する中、民間企業においてサイバーセキュリティ対策は重要な経営課題となっているが、企業としての社会的責任を果たしステークホルダーからの信頼を得るためには、**サイバーセキュリティ対策の実施のみならずその内容について適切な情報開示が重要。**

目的

✓ 民間企業による**サイバーセキュリティ対策**やその対策の**情報開示の重要性**の認識を促進。

✓ 民間企業にとって参考になり得るような**既存の情報開示の実例**を**事例集として**示す。

活用主体

✓ **サイバーセキュリティ対策の情報開示**に一定の関心のある民間企業の開示の実務担当者等を想定。

対象とする情報開示

✓ **開示書類**を通じた情報開示を取り扱う。

✓ 開示書類の読み手は、**投資家、融資元、顧客・契約者・取引先、従業員、競合他社等を含む、社会全体の広範なステークホルダー**を想定。

開示にあたってのポイント

①目的適合性	✓ 記載事項の決定にあたっては、ステークホルダーへの説明責任を果たすために開示を行うという目的を踏まえること ✓ 以下の②～⑤を踏まえつつ、ステークホルダーにとって有益と思われる情報を提供すること
②表現真正性	✓ 自社のサイバーセキュリティ対策について、真実を忠実に表現すること ✓ 情報の完全性、中立性、合理性を可能な限り確保すること
③比較可能性	✓ 同業種・同規模間、同じ企業の異時点間等の一定の範囲で比較可能にするための基礎となる情報を提供すること ✓ 定量的な情報や、対策の有無が直接記載の有無につながるような情報など、客観的な評価が可能な情報を記載すること
④理解容易性	✓ 読み手に特別な専門知識がなくても理解できるよう、簡潔かつ明瞭な表現で十分な情報を記載すること ✓ 必要に応じて専門用語に注釈等を付すこと ✓ 概念図や写真等を活用し、読み手に受け入れやすいものとすること
⑤適時公表性	✓ 社会的に大きなインシデント等の発生後や新たな法規制の導入など、ステークホルダーの関心があるタイミングで適切な情報を速やかに公表すること

まずは、セキュリティに関する認証を取得し、開示することが第一歩ではないか。

御静聴ありがとうございました。