IPA
Information-technology
Promotion
Agency, Japan

IoTとサイバーセキュリティ

2017年6月2日

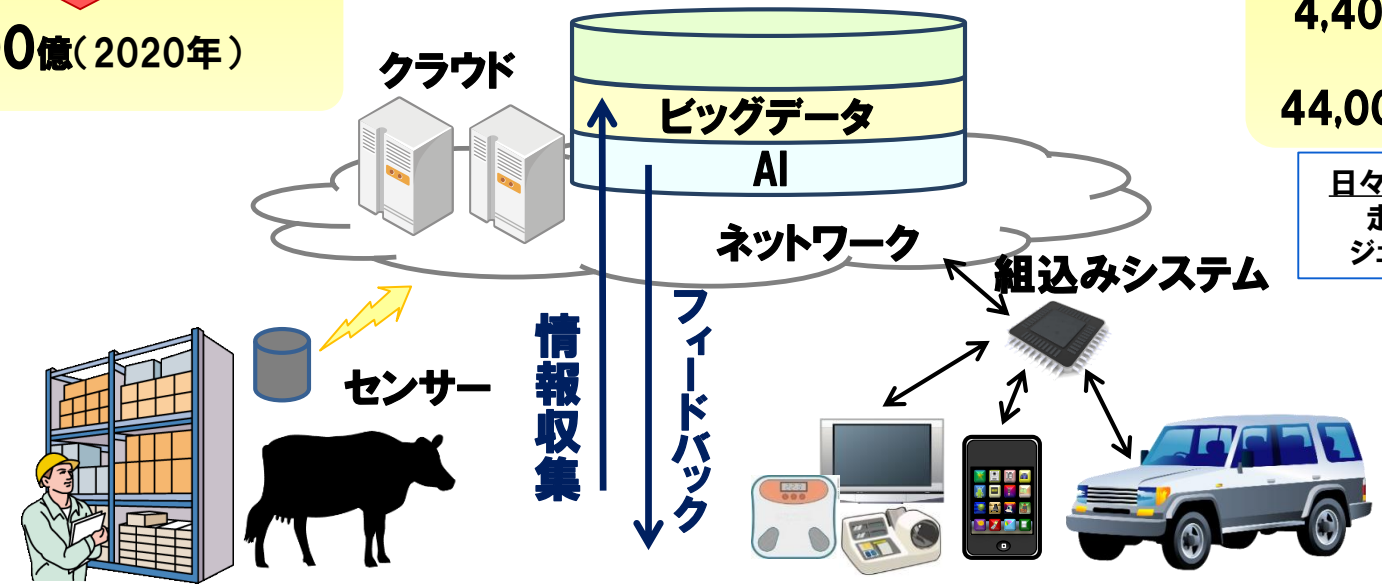
独立行政法人 情報処理推進機構
理事長　富田 達夫

つながる世界の実現

IoTデバイス数〔ガートナー予測〕
25億（2009年）
↓
300億（2020年）

データ量〔IDC予測〕
132EB（2005年）
↓
4,400EB（2013年）
↓
44,000EB（2020年）

日々生み出されるデータ
走行車　3.6TB/時
ジェット機　20TB/時



（参照）IPA「つながる世界の開発指針」

- 膨大な数のセンサーが実世界の情報を収集
- 様々なものがインターネットにつながる
- コンピューティング能力の向上、ディープラーニング等、AIの進化
- 情報が新たな価値を生み出す時代の到来

様々な情報が活用される社会

IPA

INTERNET

…

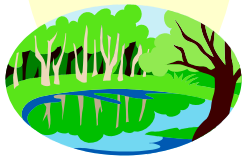
…

…

…

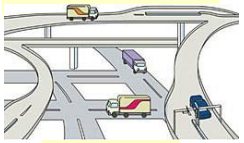
土木

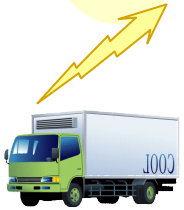
環境センシング
橋梁健全性
地滑り監視



運輸

自動運転





農林

林の監視
農業工場
6次産業

厚生

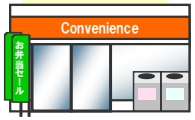
予防医療
遠隔医療
IT診断

金融

フィンテック
電子決済

小売

在庫管理
自動化
リアルタイム
マーケティング



製造

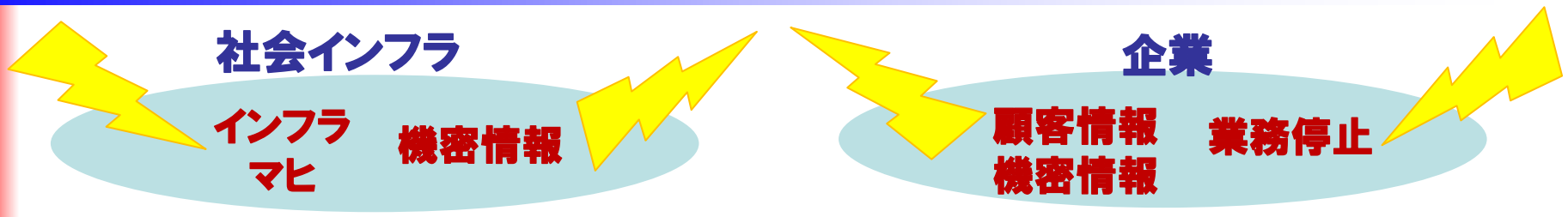
第4次
産業革命

ソフトウェアがドライブ

新たなビジネスの創出

既存ビジネスの破壊

新たな脅威への拡がり



IoTの進展による拡がる脅威

（参照）IPA「つながる世界の開発指針」

- 攻撃対象の増加、被害の深化、手口の巧妙化が進む
- 組織が各自で専門知識を持ち防御を固めることが必要

IPA（情報処理推進機構）のご紹介

- 日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人
- 誰もが安心してITのメリットを実感できる「 **頼れるIT社会** 」を目指しています

情報セキュリティ

- ウイルス、不正アクセス等の届出機関
- 情報セキュリティの調査研究、普及啓発活動
- 標的型サイバー攻撃への情報共有・初動対応の実施

情報処理システムの信頼性向上

IT人材育成

- 国家試験「情報処理技術者試験」の実施機関
- IT人材の育成・発掘・スキル明確のとりくみ。若手人材育成。

IPA　検索

1.情報セキュリティの最近の事例
　(1) 情報セキュリティ10大脅威
　(2) ランサムウェアによる被害
　(3) IoT機器の脆弱性の顕在化
2. 情報セキュリティ人材育成への取り組み
3. 安全で安心なIT社会の実現に向けて

情報セキュリティ10大脅威 2017

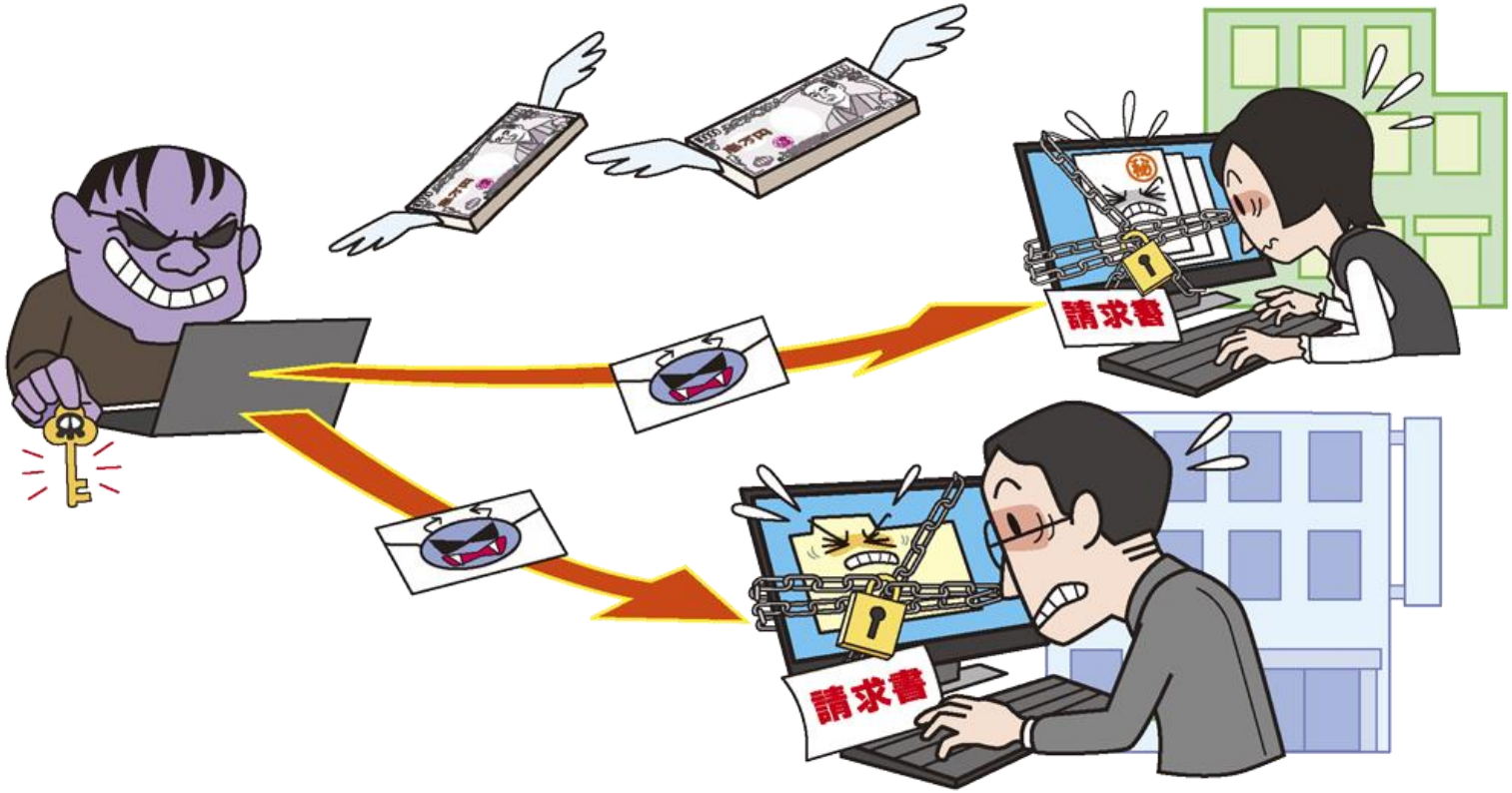
- 10大脅威とは？ https://www.ipa.go.jp/security/vuln/10threats2017.html
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」約100名の投票により、情報システムを取巻く脅威を順位付けして解説

情報セキュリティ10大脅威 2017

IPA

昨年順位	「個人」の10大脅威	順位	「組織」の10大脅威	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル不足に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

ランサムウェアによる被害



- ランサムウェアにより、PC内のファイルが暗号化
  ⇒ファイルの復元に身代金を要求
- 2017年5月、世界中でランサムウェア感染拡大

世界中でランサムウェア感染拡大

世界中で感染が拡大中のランサムウェア"Wanna Cryptor "

⇒Microsoft製品の脆弱性を悪用

2017年5月14日　「IPA 重要なセキュリティ情報」として緊急告知

2017年5月22日　感染実演デモ公開（IPA安心相談窓口だより）

図：感染した場合に表示される画面の一例

YouTube：ランサムウェア「WannaCry（WannaCryptor）」感染実演デモ

【出展】　IPA安心相談窓口だより　https://www.ipa.go.jp/security/anshin/mgdayori20170515.html

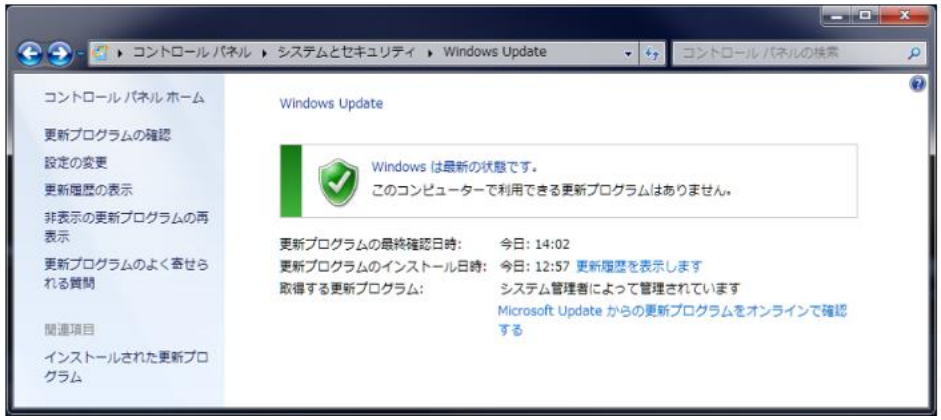
Wanna Cryptorの感染防止のために 今すぐWindows Updateを

Wanna Cryptorは、感染拡大を図る自己増殖型である。

- 脆弱性（Microsoft Windows の脆弱性）を悪用
- ネットワーク上に当該脆弱性が残る端末がないか探索

☒ 至急、下記の対策を実施してください。☒

- ✓ ネットワーク接続をしていない状態で必要なファイルをバックアップ
- ✓ ネットワークに接続し、Windows Updateを実行
- ✓ 更新プログラムが適用されたことを確認



Windows Updateが適用されている（最新の状態となっている）例

【出展】IPA安心相談窓口だより https://www.ipa.go.jp/security/anshin/mgdayori20170515.html

ランサムウェアの手口/影響

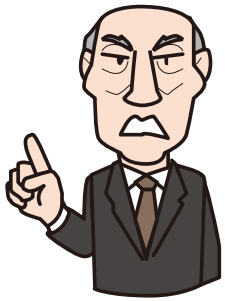
- 手口/影響
  - メールの添付ファイルやリンクからランサムウェア感染
  - ウェブからランサムウェアに感染(脆弱性等を悪用)
  - 感染したPCだけではなく、共有サーバー等別の端末にも影響
- 2016年の事例/傾向
  - ランサムウェアの日本語化・被害拡大
    - 検出されたランサムウェアの件数が2015年の9.8倍※
    - その中には日本語表記のランサムウェアを確認
  - ランサムウェア復号ツールの登場
    - 暗号化されたファイルを復号するツールが登場し、万が一暗号化されてもファイルを復元できる可能性

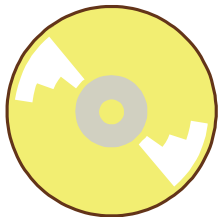
※【出展】トレンドマイクロ　日本と海外の脅威動向を分析した「2016年年間セキュリティラウンドアップ」
国内のランサムウェア検出台数(2015年:6,700台→2016年:65,400台)

ランサムウェア対策

経営者

- 組織としての対応体制の確立
  - 問題に対応できる体制（CSIRT等）構築
  - 予算の確保
  - セキュリティ対策の指示





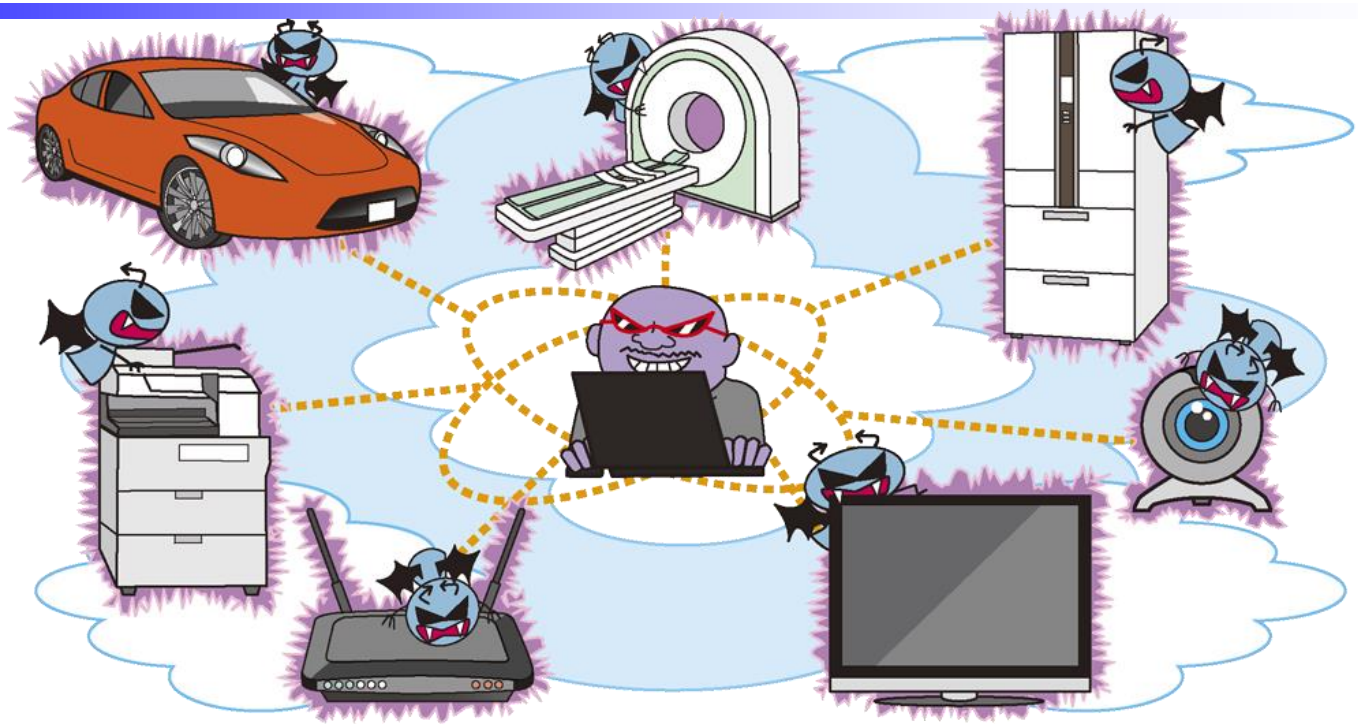
＜対策＞
定期的なバックアップ
脆弱性対策

システム管理者

PC・スマートフォン利用者

- 情報リテラシーの向上
  - 受信メール（添付ファイル・リンク）ウェブサイトの十分な確認
- 被害の予防
  - OS・ソフトウェアの更新
  - セキュリティソフトの導入
  - フィルタリングツールの活用
- 被害を受けた後の対策
  - バックアップからの復旧
    PCだけではなく、共有サーバーも
  - 復元できるかの事前の確認
  - 復元ツール・機能の活用

IoT機器の脆弱性の顕在化



- IoT機器の脆弱性を悪用

  ⇒ウイルス感染や不正利用の被害

- 不正利用されたIoT機器がボット化

  ⇒DDoS攻撃等に悪用されるケース

IoT機器におけるインシデント

IPA

2015年3月 5月	【日本】WebカメラやHEMS(住宅用エネルギー管理システム) 店舗や住宅内に設置されたWebカメラの**映像・音声を第三者が見聞き可能** スマートハウスが管理する情報を見られたり、**家庭内機器を遠隔操作**される可能性
2016年1月	【日本】大学や高等専門学校等 複合機やプリンターの設定不備による情報漏えいの可能性が指摘される

2015年4月	【アメリカ】医療向けのIoT機器メーカー“ホスピーラ社” 薬剤ライブラリや輸液ポンプの設定等を管理する サーバソフトの脆弱性が報告される インターネット越しにサーバ上の**投与する薬や投薬量を改ざん**する事が可能
2016年10月	【アメリカ】インスリンポンプメーカー“Animas社” インスリンポンプに脆弱性、治療情報漏えいや不正操作・妨害 の恐れ
2017年1月	【アメリカ】医療機器大手 “St. Jude Medical社” 心臓ペースメーカーに脆弱性、不正な遠隔操作の恐れ

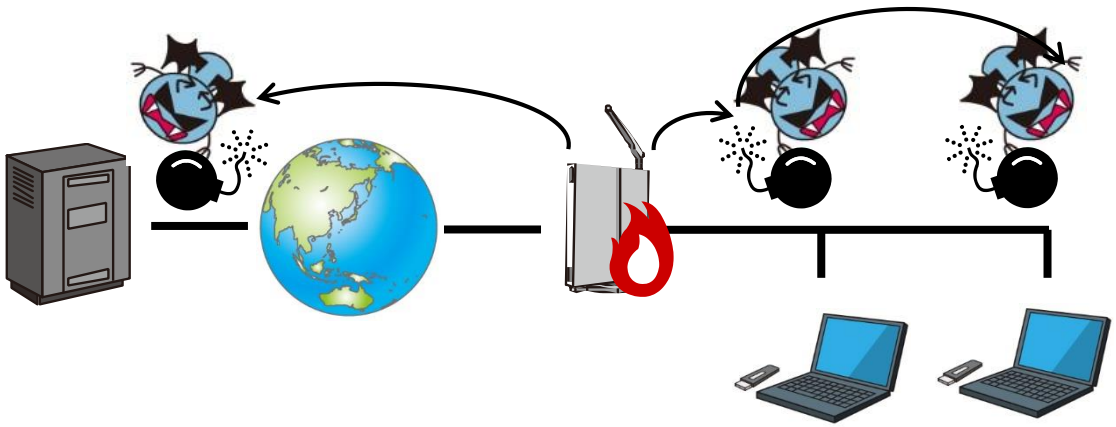
2015年8月	【アメリカ】世界最大級の 2 大ハッカーカンファレンス“Black Hat” “DEF CON” Jeep Cherokeeの脆弱性を攻撃し、遠隔操作を成功させた事例が報告される ファームウェアを改竄した車に対して攻撃コードを送りこむ →**ブレーキ、ステアリング、エアコン等への干渉**が可能
2016年2月	【日本】自動車メーカー 国内電気自動車の専用スマートフォン用アプリに脆弱性、不正遠隔操作の恐れ

IoT機器におけるインシデント

IPA

- IoT機器が乗っ取られ、DDoS攻撃等への悪用が可能になっている
  - 悪用された全てのIoT機器でリモートアクセスが可能
  - ほぼ全てのIoTで初期パスワードを使用
  - LAN内の他の機器にアクセスされる可能性もあり

- 内部だけでなく、外部への攻撃にも悪用される

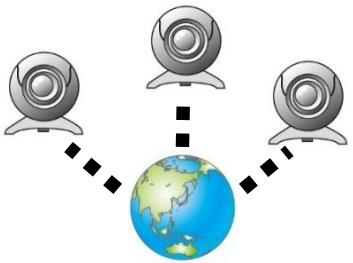


IoT機器におけるインシデント

■ 各国のネットワークカメラが閲覧できるサイト「Insecam」（ロシア）
報道によると利用者の意図しないままにインターネットに公開
設置場所の区市町村が特定され、閲覧できる状態に
⇒日本国内の約4,300台のカメラの映像が公開される
- 医療機関や製造会社に設置された防犯カメラも対象に
- IDやパスワードが設定されていない機器も確認

【出展】産経ニュース 2016年1月

■ ネットワークカメラがマルウェアに感染
⇒DDoS攻撃
→ Mirai



【参考】Censysに登録されている国内のNetwork Cameraの検索結果：17,599台（2017年5月時点調査）

IoTにおける脅威「Mirai」

2016年、IoTボットネットによる大規模DDoS攻撃の脅威が発生

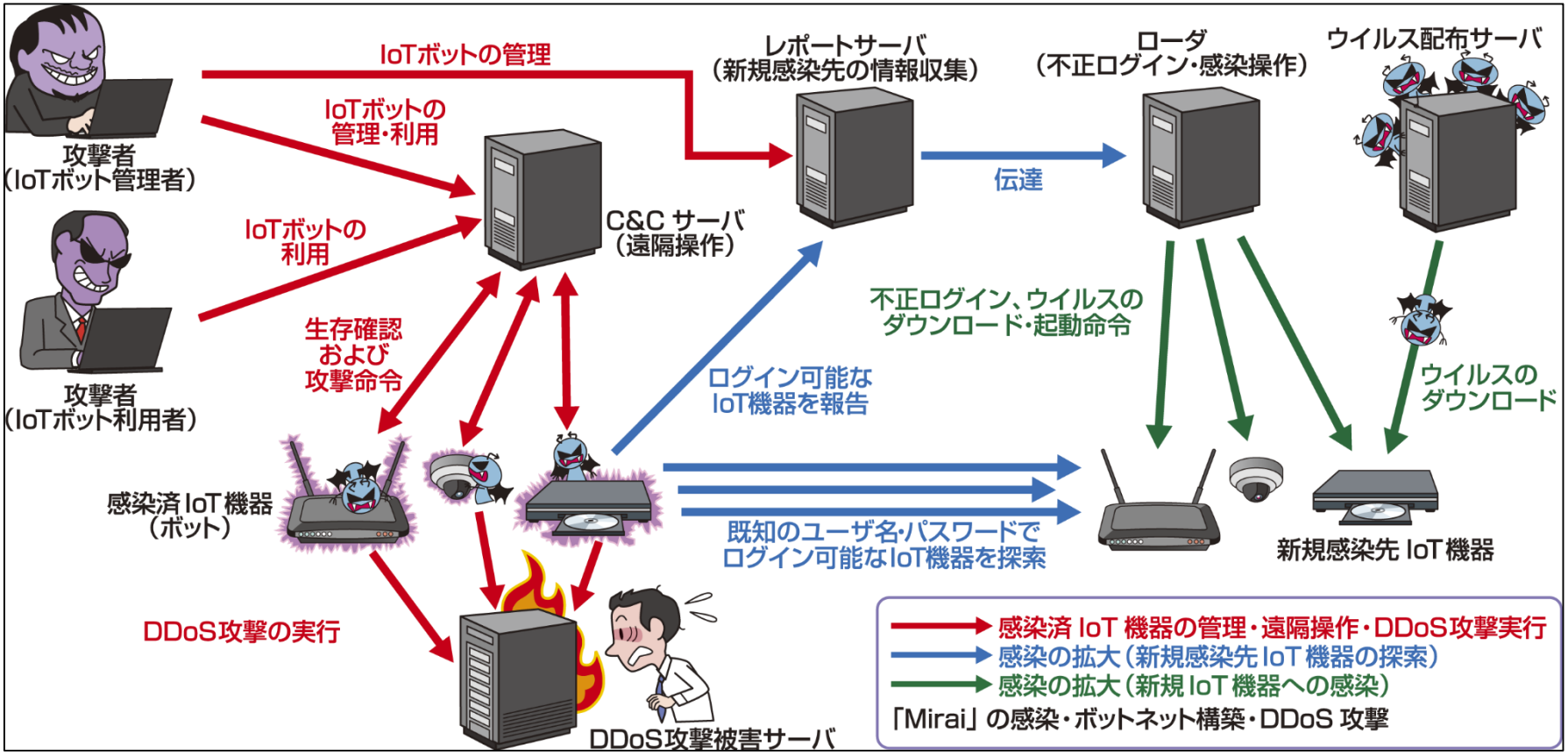
2016年9月	【アメリカ】セキュリティ専門家ブログサイト “Krebs on Security” ・マルウェア「Mirai」に感染したIoT機器で構成されたボットネット ・約620GbpsのDDoS攻撃
2016年9月	【フランス】ホスティングサービス事業者“OVH” ・14万5千台以上のIoT機器からDDoS攻撃 ・ピーク時に1Tbpsを超える攻撃トラフィックを観測
2016年9月	「Mirai」のソースコード公開
2016年10月	【アメリカ】DNSサービス提供会社“Dyn” ・顧客であるTwitter, SoundCloud, Spotify, Reddit 等に影響 ・Dyn社は数千万のIPアドレスが攻撃に参加していたと報告
2016年11月	【ドイツ】ISP“Deutsche Telekom” ・顧客のルータに対するマルウェア感染攻撃(「Mirai」の亜種？) ・4～5%がクラッシュまたは制限状態となり、90万ユーザに影響

「Mirai」の主な挙動（感染・ボットネット構築・DDoS攻撃）とは？

■ 初期設定に使用され易いユーザー名やパスワードを使ったIoT機器

⇒ウイルス「Mirai」に感染（初期設定のままのIoT機器を乗っ取る）

⇒DDoS攻撃（組織のサービスを妨害）



【出典】Level 3 Threat Research Labs の調査結果
http://netformation.com/level-3-pov/how-the-grinch-stole-iot 等をもとに作成

「Mirai」感染の要因

IPA

- **ポート番号23または2323でtelnetが動作している**
  - IoT機器を利用している間、動作している必要があるか否か不明
  - 無効化する管理インタフェースが存在しないIoT機器がある
  - 一部機器では、telnetの動作は利用者に非公開の「バックドア」状態
- **ユーザ名、パスワードが初期値のまま動作していた**
  - IoT機器の利用開始前に、ユーザが変更していない
  - 管理用パスワードがハードコーディングされている
    （ユーザが変更出来ないIoT機器あり）
  - 一部機器でユーザ名やパスワードの存在が利用者に隠蔽

● 上記条件を満たすIoT機器

■Flashpoint社（アメリカ）調査結果⇒ **世界中に51万5千台以上**

※SHODAN の検索結果をもとに作成される　※https://www.shodan.io/report/aE9jvAXo

・ベトナム	80,499台	・ブラジル	62,359台	・トルコ	39,736台	・台湾	28,624台
・中国	22,528台	・ロシア	21,814台	・韓国	21,059台	・タイ	15,744台
・インド	14,789台	・英国	14,081台	・日本	1,257台		

「Mirai」以外のマルウェアの出現

IPA

- **IoT機器を守ろうとする(？)マルウェア 「Hajime」**
  - ✓ 初期ユーザ名＆パスワードでtelnetで不正ログインして感染
  - ✓ 感染後、ポート番号23, 5538, 5555, 7546の通信を遮断
  - ✓ P2Pネットワーク上に構築(解体が困難、堅牢なボットネット)
  - ✓ ブラジル・イラン・タイ・ロシア等を中心に数万台のIoT機器が感染
  - ✓ 攻撃の踏み台とせず、作成者の善意(？)の警告メッセージを表示
- **IoT機器を使用不能にするマルウェア 「BrickerBot」**
  - ✓ 初期ユーザ名＆パスワードでtelnetで不正ログインして感染
  - ✓ 感染後 → 設定変更、インターネット接続妨害、動作速度低下
    機器上のファイル消去等の致命的な改変
    → 最終的に使用不能に
  - ✓ 作者「Janit0r」の主張
    →「Mirai」を壊滅するため、200万台以上のIoT機器を使用不能状態へ

⇒複数のマルウェアによるIoT機器の陣取り合戦状態に

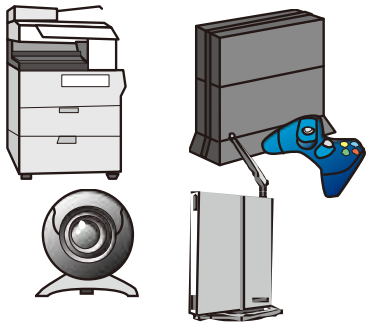
IoT機器の脆弱性対策

IoT機器の利用者

- 情報リテラシーの向上
  - 機器使用前に説明書を確認
- 被害の予防
  - 不要な機能の無効化（telnet等）
  - 外部からの不要なアクセスを制限
  - ソフトウェアの更新（自動化設定含む）

IoT機器の開発者

- 被害の予防
  - セキュアプログラミングの適用
  - 脆弱性の解消
  - ソフトウェア更新手段の自動化
  - 分り易い取扱説明書の作成
  - 迅速なセキュリティパッチの提供
  - 不要な機能の無効化（telnet等）
  - 安全なデフォルト設定
  - 利用者への適切な管理の呼びかけ



利用者は利用しているIoT機器の適切な管理を
開発者は適切な利用者を意識した対策を

顕在化したIoTのセキュリティ脅威とその対策

IPA

開発者・製造者の対策

・設計段階からセキュリティを考慮（セキュリティ・バイ・デザイン）
  - システムの全体構成の明確化
  - 保護すべき情報・機能・資産の明確化
  - 「脅威分析」保護対象に対する脅威の明確化
  - 「対策検討」対策候補の洗い出し、
    脅威・被害・コスト等を考慮した選定

・セキュリティ対策の継続的サポート（脆弱性対応、S/W更新）

「IoT開発におけるセキュリティ設計の手引き」では、
脅威分析・対策検討・脆弱性対応、関連ガイド、
具体的な検討実施例、暗号技術チェックリスト等に
ついて紹介しています。

詳しくは「IoT開発におけるセキュリティ設計の手引き」をご覧ください。
https://www.ipa.go.jp/security/iot/iotguide.html

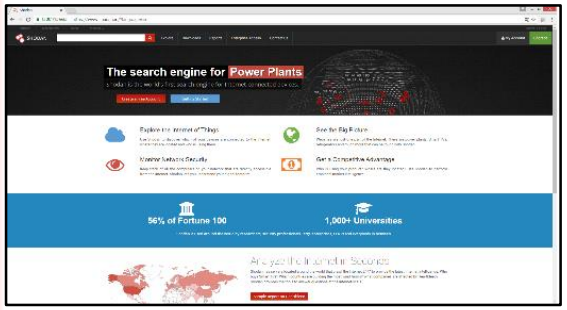
顕在化したIoTのセキュリティ脅威とその対策

IPA

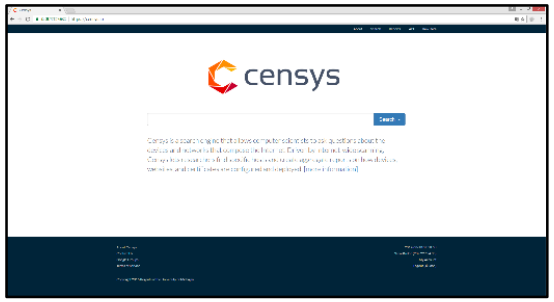
利用者・運用者の対策

- 説明書の熟読、更新ソフトウェアの適用
- ネットワーク保護（ルータ経由でのネットワーク接続等）
- 適切な機器設定（パスワード変更、不要管理機能停止等）

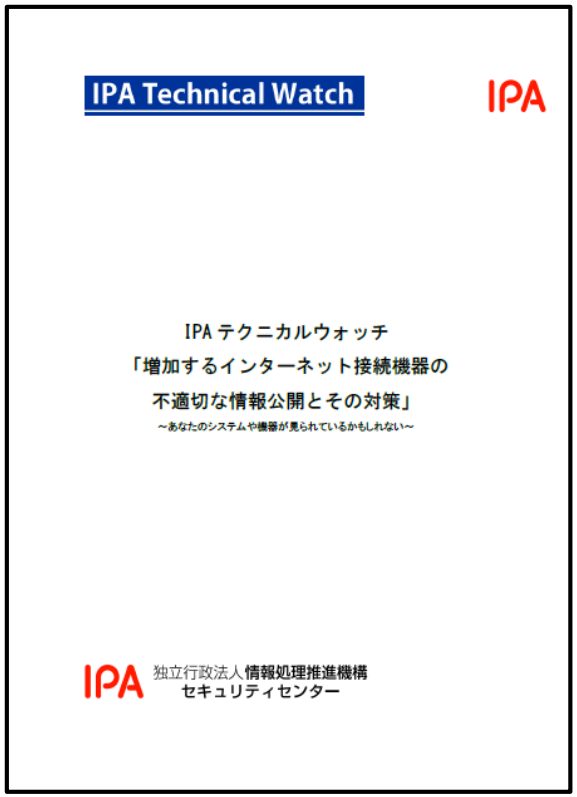
インターネット接続機器検索サービスを活用することで、自社／自分のIoT機器がインターネット上でどの様に見えているか確認することができます。



SHODAN



Censys



詳しくは「増加するインターネット接続機器の不適切な情報公開とその対策」をご覧ください。
https://www.ipa.go.jp/security/technicalwatch/20160531.html

日本国内で接続されているIoT機器数（プロトコル別）

IPA

2017/3/31時点のヒット件数（日本国内）	機器がもつサーバー機能				
	ウェブ機能	ファイル共有機能	メール機能	DNS/NTP機能	telnet機能
機器 ＼ 主要な脅威・リスク	情報漏えい 設定情報の変更	情報漏えい	攻撃の踏み台	攻撃の踏み台	攻撃の踏み台
複合機（プリンター、スキャナー、FAX）	○	○	○		○
ネットワーク対応ハードディスク	○	○	○	○	○
ネットワークカメラ	○	○	○		○
ブロードバンドルーター	○	○		○	○
デジタル液晶テレビ	○				
ブルーレイディスクレコーダー ハードディスクレコーダー	○	○			○
使用プロトコル	HTTP	FTP	SMTP	DNS/NTP	telnet
ポート番号	80, 8080	21	25	53	23, 2323
SHODANに登録されている機器台数	1,812,519	489,453	810,889	292,011	109,734
Censysに登録されている機器台数	2,784,614	493,223	732,059	249,897	136,241

1.情報セキュリティの最近の事例
（1）情報セキュリティ10大脅威
（2）ランサムウェアによる被害
（3）IoT機器の脆弱性の顕在化

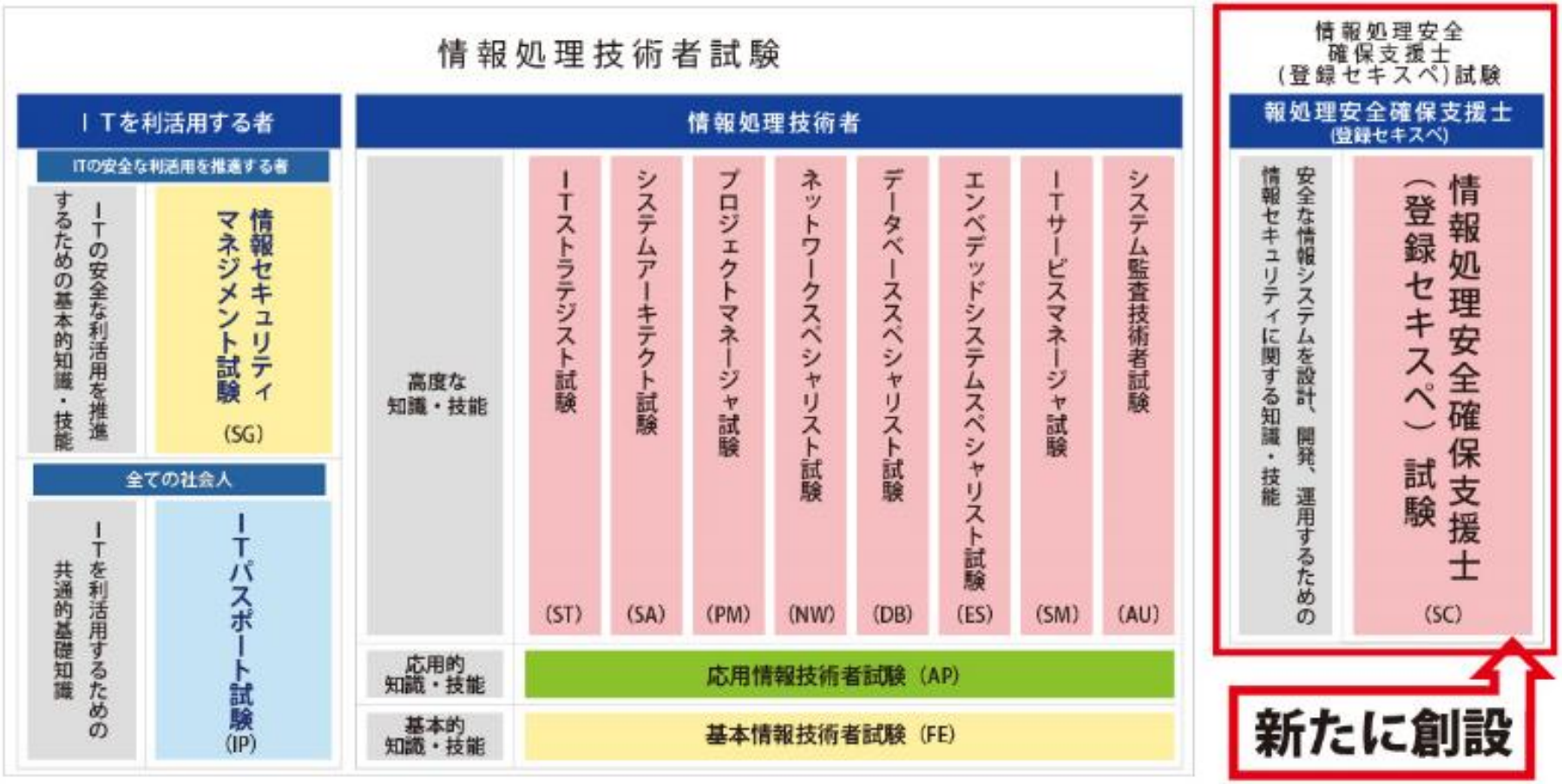
2. 情報セキュリティ人材育成への取り組み

3. 安全で安心なIT社会の実現に向けて

国家試験 情報処理技術者試験

IPA

- 年2回(4月、10月)実施！



- 各種試験を活用して基礎知識から管理能力まで、スキルアップを図ることができます。

2. 情報セキュリティ人材育成への取り組み

国家資格「情報処理安全確保支援士」

IPA

【設立の目的】

サイバーセキュリティに関する実践的な知識・技能を有する専門人材を育成・確保

経過措置
期間限定
現在登録申請受付中

資格試験
2017年春よりスタート

登録簿へ登録
（要申請）

- 講習受講
- 資格名称の使用
- 登録情報の公開

①人材の質の担保

- 「情報セキュリティスペシャリスト試験」をベースとした新たな試験の合格者を登録
- 継続的な講習受講義務により、最新の知識・技能を維持

②人材の見える化

- 資格保持者のみ資格名称を使用
- 登録簿の整備・登録情報の公開（希望しない者を除く）

③人材活用の安心感

- 国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務

【支援士の活動】

企業における安全な情報システムの企画・設計・開発・運用を支援、サイバーセキュリティ対策の指導・助言を実施

■第1回（2017年4月1日）登録者数：4,172名（平均年齢40.5歳）
※経過措置対象者（「情報セキュリティスペシャリスト試験」または「テクニカルエンジニア（情報セキュリティ）」合格者）

■初回試験（2017年4月16日実施）応募者数：25,130名（平均年齢38.5歳）

2020年に登録者3万人が目標

2. 情報セキュリティ人材育成への取り組み

2017年4月に発足「産業サイバーセキュリティセンター」

- **人材・組織強化、技術、ノウハウを結集し、社会インフラ、及び産業基盤のサイバーセキュリティ対策抜本的強化を図るために、3つの事業を柱に推進していく**

人材育成事業

- 自社システムのリスクを認識し、必要なセキュリティ対策を判断できる人材の育成
- 模擬プラントを用いた実践演習による、現場で活きるスキルの醸成
- 国内外の有識者、専門家との連携を促進
- 企業等の経営層へ、サイバーセキュリティ対策の必要性、人材活用についての啓発

制御システムの安全性・信頼性検証事業

- 実際の制御システムの安全性・信頼性に関するリスク評価・対策立案を行う

※IPAセキュリティセンターと連携して実施する事業

中核となる3事業

脅威情報の調査・分析事業

- 脅威情報を収集、新たな攻撃手法など調査・分析

※IPAセキュリティセンターと連携して実施する事業

1.情報セキュリティの最近の事例
（1）情報セキュリティ10大脅威
（2）ランサムウェアによる被害
（3）IoT機器の脆弱性の顕在化
2. 情報セキュリティ人材育成への取り組み
3. 安全で安心なIT社会の実現に向けて

3. 安全で安心なIT社会の実現に向けて

①国民全体の情報セキュリティ意識、リテラシーを高める活動

・IPAはセキュリティ教材、ツール、映像ライブラリーの提供による普及啓発

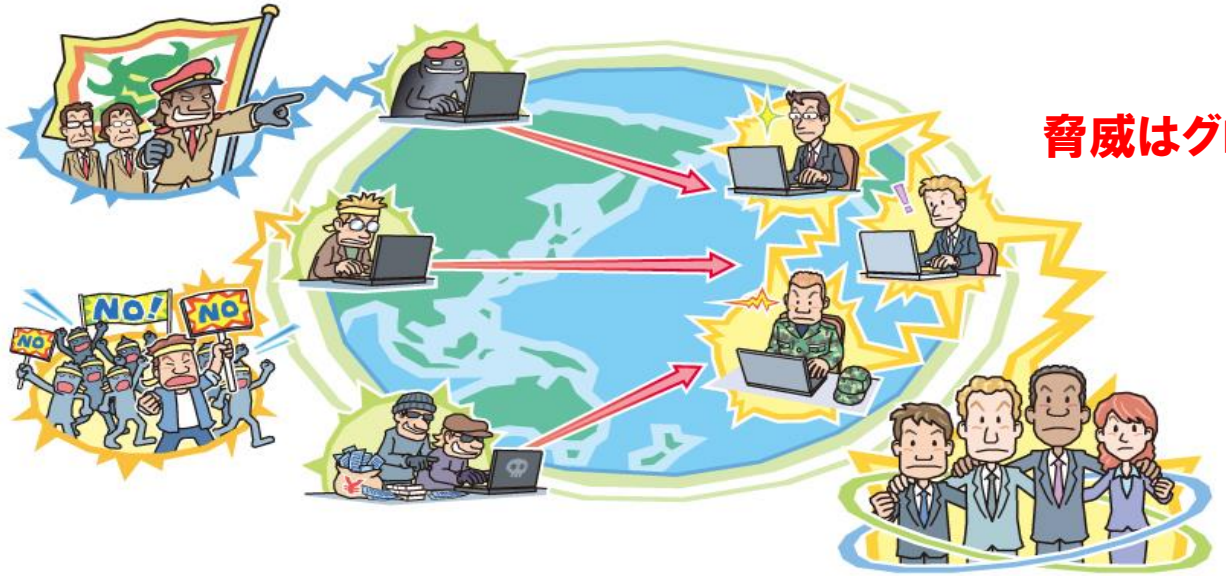
②組織間の連携を強化し、国全体のセキュリティを高める活動

・政府、省庁、セキュリティ関連組織、セキュリティベンダー、産業界等との連携

③官民が連携し、日本のIT社会を活性化

・官民が連携し、セキュリティ産業を活性化

・経済活性化と国の発展をセキュリティの観点から貢献



脅威はグローバル化している

強い連携を！

独立行政法人**情報処理推進機構**
Information-technology Promotion Agency, Japan