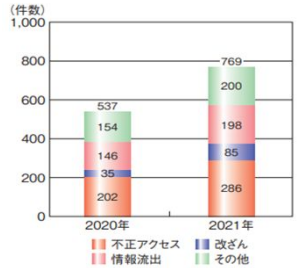
コロナ下サイバー攻撃の実態と対策

ー第7回情報セキュリティ・セミナーー

NPO法人産業クラスター研究会
2022年10月27日
槌谷祐一

目次

1）国内のコロナ下インシデント発生状況



情報セキュリティ種類別インシデント報道件数

・2021年度は前年度の　43%　増

WEBサイト改ざん年度別件数推移

・2021年度は前年の　180%　増加

情報セキュリティ白書2022

年度別フィッシング報告件数

海外含む

・2020年度に比べ　185%　増加

・悪用されたブランド：

・アマゾン・楽天・三井住友カード
JCB・イオンカード等

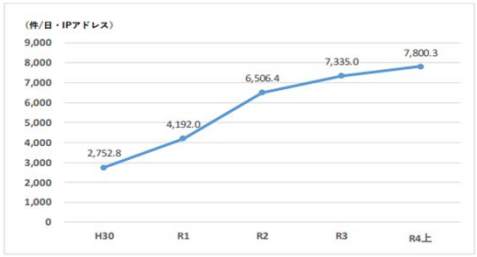
フィッシング月次報告件数（海外含む）

2022年度：2021年度の倍増

フィッシング対策協議会

サイバー空間における脆弱性探索行為状況

センサーで検知したアクセス件数



１日　:IPアドレスあたり　**7800件**　と高水準

IoT機器の普及により攻撃対象が増加、攻撃手法が高度化している。

警察庁　広報資料　令和4年9月15日

2　サイバー攻撃の実態

2022年度10大脅威　IPA資料

「個人」向け脅威	順位	「組織」向け脅威
フィッシングによる個人情報等の詐取	1	ランサムウェアによる被害
ネット上の誹謗・中傷・デマ	2	標的型攻撃による機密情報の窃取
メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	3	サプライチェーンの弱点を悪用した攻撃
クレジットカード情報の不正利用	4	テレワーク等のニューノーマルな働き方を狙った攻撃
スマホ決済の不正利用	5	内部不正による情報漏えい
偽警告によるインターネット詐欺	6	脆弱性対策情報の公開に伴う悪用増加
不正アプリによるスマートフォン利用者への被害	7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
インターネット上のサービスからの個人情報の窃取	8	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	9	予期せぬ IT 基盤の障害に伴う業務停止
インターネット上のサービスへの不正ログイン	10	不注意による情報漏えい等の被害

個人：第1位　フィッシングによる個人情報搾取

（海外データ含む）

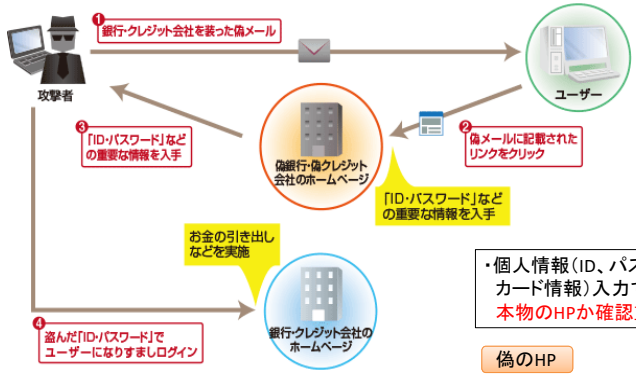
・2022年度：
　2021年度の倍増

・国内：

フィッシング対策協議会　2022年度10月

フィッシング詐欺の手口

・騙しの偽メール注意！
・スパム・メール注意！



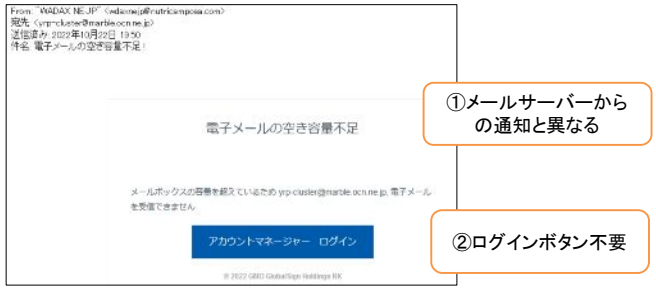
・個人情報（ID、パスワード、カード情報）入力では
　本物のHPか確認重要！

偽のHP

Amazon、楽天・・・
金融機関、カード会社・・

ESET：マルウエア情報局記事

“電子メールの空き容量不足” を通知：フィッシング・メール



- フィッシング　サイトに誘導する手口

9

企業・組織向け：第1位　ランサムウエア被害

IPA

ランサムウエア：身代金を要求ウイルス

PCやサーバーが感染すると端末のロックやデータ暗号化

複旧と引き換えに金銭を要求される。

10

2017.5.12(金)

“WannaCry”

感染原因：
ソフトの脆弱性

2017.5.15（火）

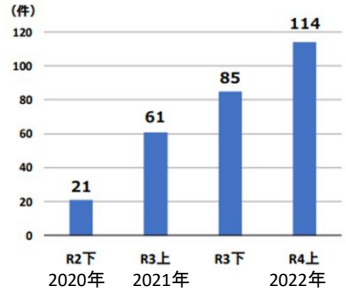
2017.6.29（木）

“NotPetya”

11

企業・団体等に於けるランサムウエア被害

警察庁　令和4年9月15日

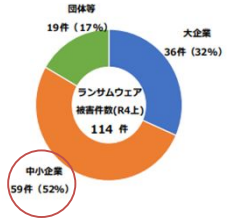


・令和4年上半期に警察庁への
報告件数114件
右肩上がりで増加

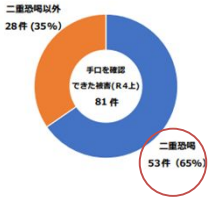
- 従来：暗号化したデータ復元する対価：金銭要求
  最近：データ窃取したうえで、対価払わなければ
  当該データを公開する。二重恐喝の手口。
- 金銭：暗号資産による要求が多い

12

被害企業・団体規模別

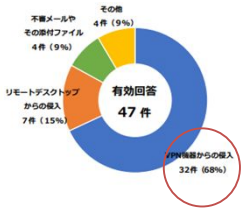


手口：二重恐喝

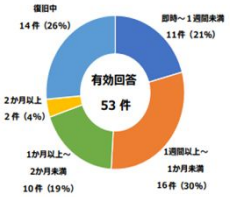


要求金銭

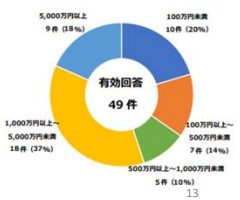
感染経路



複旧に要した期間



調査・複旧の総額



13

（株）日本製粉　サイバー事故

・2021年7月7日：グループ企業で複数のシステムで障害発生

同時多発的にサーバーや端末が暗号化された。
（財務管理・販売管理、11社グループ管理の基幹システム化）

・バックアップ・サーバーも暗号化、復旧に有効な手段なし

・システムの防御：
ファイアーウオール、不正侵入システム、ウイルスソフトupdate

・2021年度3月度四半期決算⇒11月15日に延長

・調査結果の詳細報告なし

接続ネットワーク内感染

14

徳島つるぎ町立半田病院：ランサムウエア攻撃被害

・2021年10月末：ランサムウエア感染（Lockbit　からの犯行声明）

・電子カルテシステムが利用不可、診療報酬システム停止

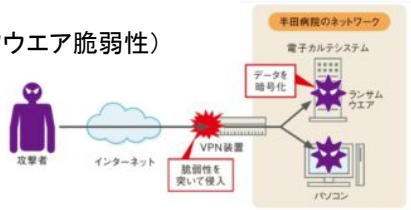
・バックアップ（ネットワーク接続）：暗号化

・侵入箇所：VPN装置（ソフウエア脆弱性）

・複旧：2ケ月

・費用：約2億円

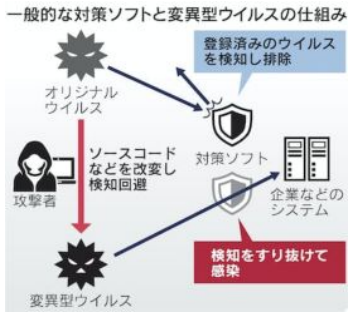
日経XTECH



https://www.handa-hospital.jp/topics/2022/0616/index.html

15

■ ランサムウエア　変異型拡大、1万種確認、被害増加



変異型：
設計図（ソースコード改変）

検知すり抜け

日経新聞電子版20022年9月

■ BCP対策：　侵入前提での対策必要

・バック・アップ　　ネットワークとは切り離す

・重要機密資料：暗号化

16

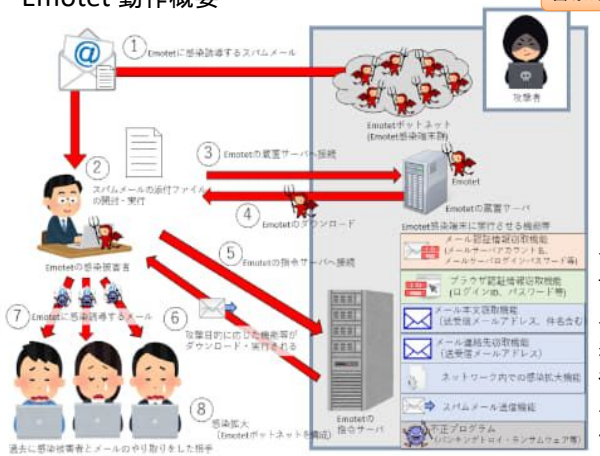
Emotet による被害

- 2014年に現れたウイルス：　再流行のたびに進化
  メールの添付ファイル：　WordやExcelなどに潜む
  開封し、「マクロの有効化」で感染。
- 特徴：端末内の情報をもとにメールを自動で周囲に広げ、データを盗み出すのが特徴、世界中で170万台以上感染
- ランサムウエアなど別のウイルスを招き入れるタイプもある。被害を甚大化

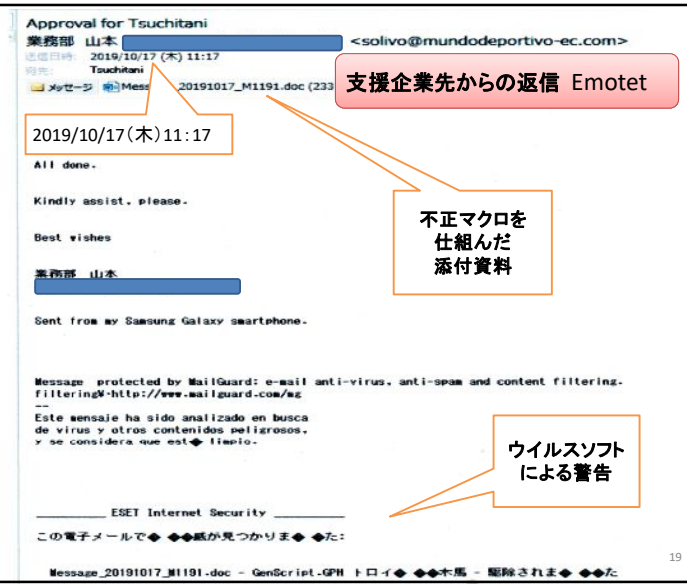
17

Emotet 動作概要

警察庁　2022年6月

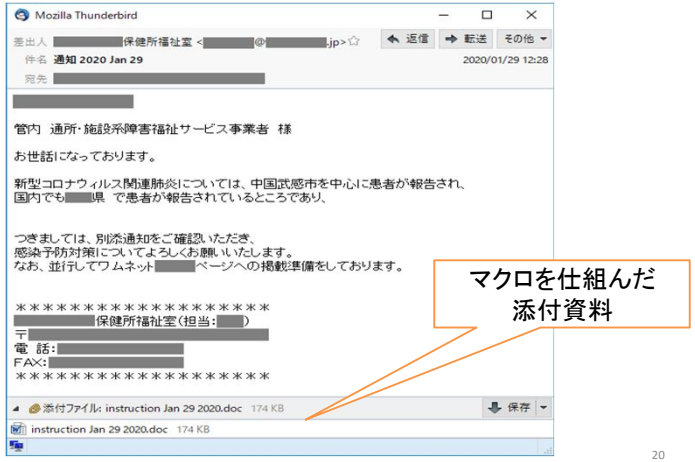


18

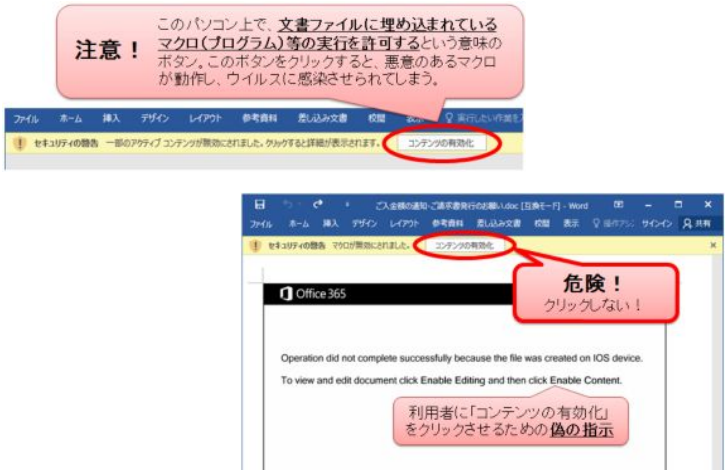


19

新型コロナにかこつけた保健所を語るメール例



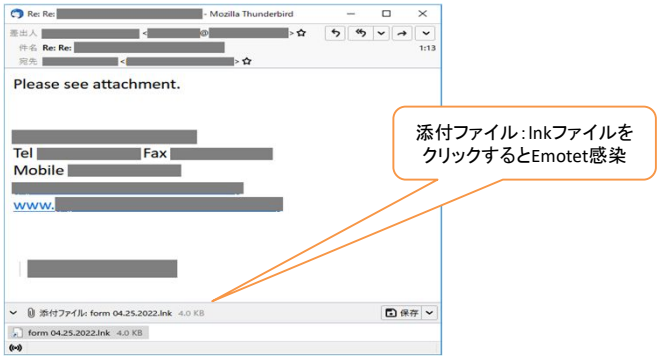
20



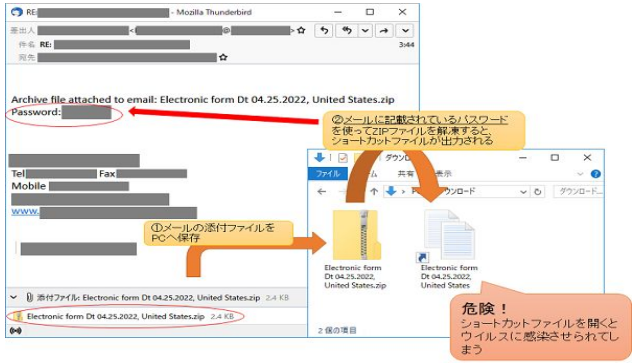
IPA　Emotetに関する記事2020年9月2日

ショートカット・ファイルを悪用した攻撃（2022年4月）

ショートカット・ファイル（lnkファイル）を悪用して Emotet へ感染させる手口



ショートカット・ファイル（lnk）がパスワード付Zipファイルとして添付されている場合



ショートカット・ファイル (lnk) をダブルクリックで開くと、Emotet感染

3） 対応策

3．1　個人PCのウイルス感染防止等の自衛策

①ソフトウエア：　*Update*
　OS（Windows）、各種ソフトに最新バージョン適用

②セキュリティ・ソフト導入：　定義ファイル最新化

③定期的なバックアップの実施

④パスワードの適切な設定と管理

⑤見知らぬ人からのメールや添付資料は開かない。
　スパム・メールのURLは安易にクリックしない

３ ２ 企業内での注意事項

1）見知らぬ人からの添付資料は開かない
　マルウエアの仕掛けの可能性、ウイルスソフトで確認

2）スパム（広告・宣伝等）メールのURL
　安易にクリックしない、ウイルス仕組んだWEB誘導

3）ランサムウエア（身代金要求ウイルス）
　・個人⇒企業対象　　変異型増加
　・バックアップ　：　　ネットから分離

4）Emotet　マクロ有効化しない、lnk ファイル注意

5）スマホ　ウイルス感染、情報漏洩源とならぬよう！

セキュリティ・アクション

IPA

IPA＊と中小企業関係団体が2017年度に創設した制度で、中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。

IPA＊：独立行政法人情報処理機構

＊ワンスター：

情報セキュリティ　5ケ条
に取り組む。

＊＊ツースター：

「5分でできる自社診断」
実態把握
「情報セキュリティ方針」公表

SECURITY　ACTION　の手続き手順書

IPA

SECURITY　ACTION　のメリット：

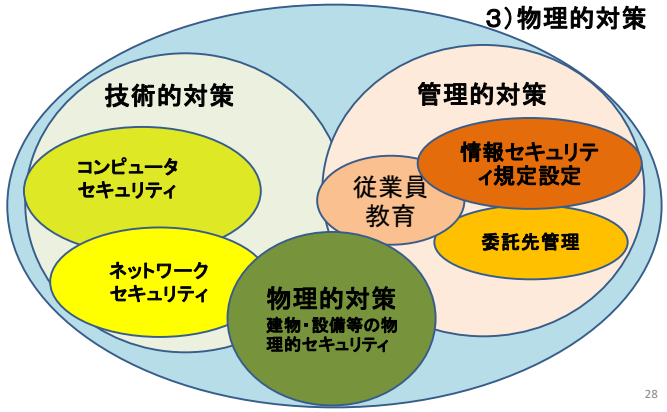
1）企業・従業員の情報セキュリティに関する意識向上

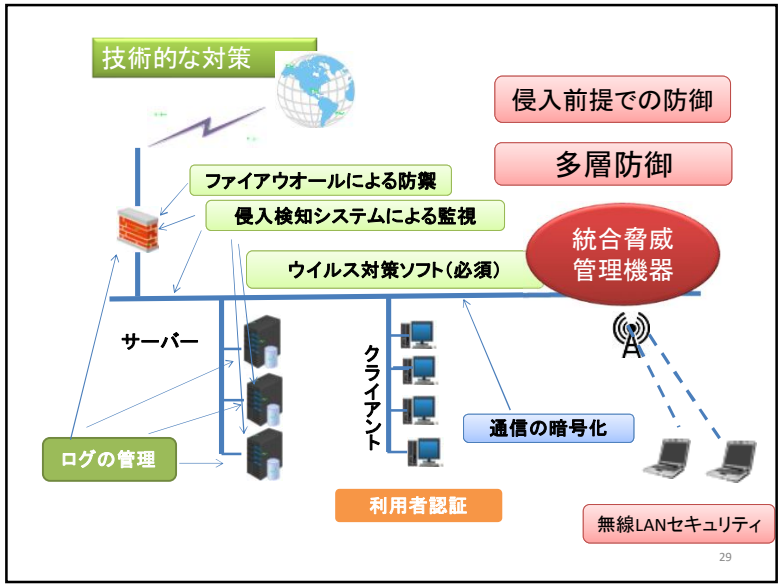
2）IT補助金申請要件

3） 企業・組織・団体での対策

情報セキュリティ・マネジメント・システム構築

1）管理的対策
2）技術的対策
3）物理的対策





管理的対策

1. セキュリティ基本方針
2. 組織のセキュリティ ・・・ 情報セキュリティ管理規定
3. 情報資産の分類及びリスク管理
4. 人的セキュリティ ・・・ 従業員セキュリティ教育
5. 通信及び運用管理 ・・・ 委託先管理
6. アクセス制御
7. 事業継続管理 ・・・ データのバックアップ

物理的管理　建物・設備等の物理的セキュリティ
入退室管理

情報セキュリティ ： 企業存続の保険と考える時代

30