

コロナ下サイバー攻撃の実態と対策

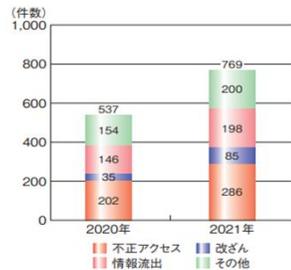
—第7回情報セキュリティ・セミナー—

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

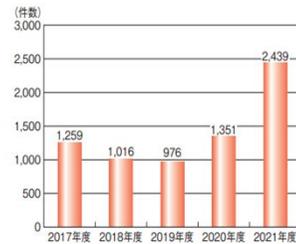
- 1) コロナ下のインシデント発生状況
- 2) サイバー攻撃の実態
 - i) フィッシングによる個人情報の搾取
 - ii) ランサムウェア
 - iii) Emotet
- 3) 対応策
 - i) 個人基本的事項 ii) 企業の基本的注意事項
 - iii) 企業・組織
 - ・セキュリティ・アクション
 - ・企業・組織としての対応

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

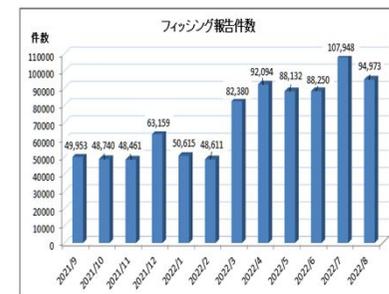


・2020年度に比べ **185%** 増加

・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

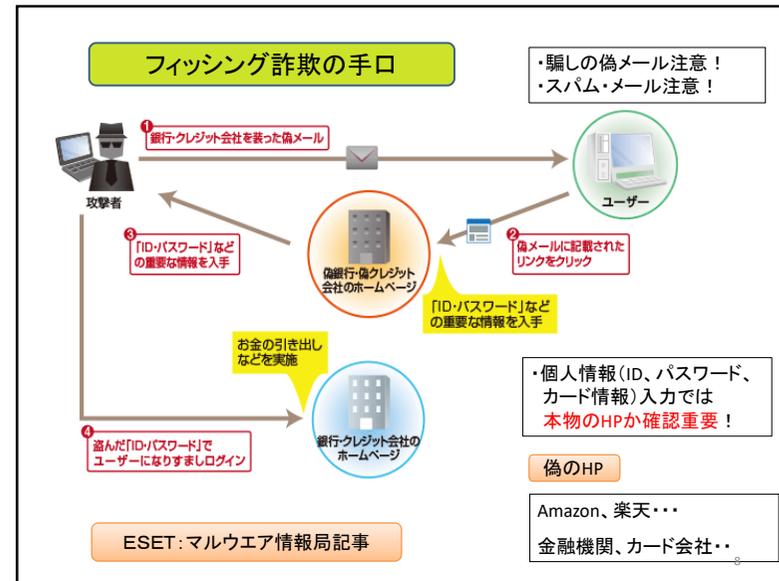
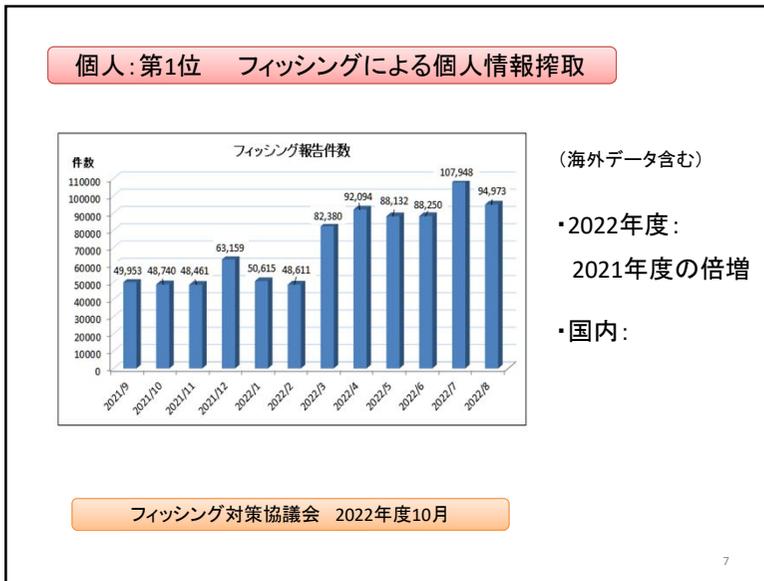
フィッシング対策協議会



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選った攻撃
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



“電子メールの空き容量不足” を通知: フィッシング・メール

From: "WADAX-NE-JP" <wadamj@nutricompos.com>
 宛先: cyrc@kshn@mantle.ocn.ne.jp
 送信日時: 2022年10月22日 13:50
 件名: 電子メールの空き容量不足!

電子メールの空き容量不足

メールボックスの容量を超えているため ysp-customer@mantle.ocn.ne.jp 電子メール
 受信できません

アカウントマネージャー ログイン

①メールサーバーからの通知と異なる

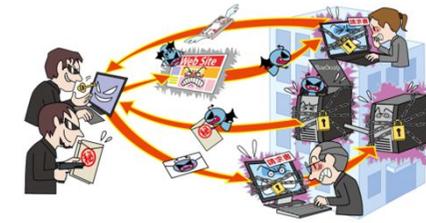
②ログインボタン不要

■ 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 ランサムウェア被害

IPA



ランサムウェア: 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**

復旧と引き換えに**金銭を要求**される。

10

99か国にサイバー攻撃

英病院、手術中止も

被害 7万5000件

2017.5.15(火)

大規模サイバー攻撃再び

被害で被害 10月より感染力強化が

国内感染 週明け続々

2017.6.29(木)

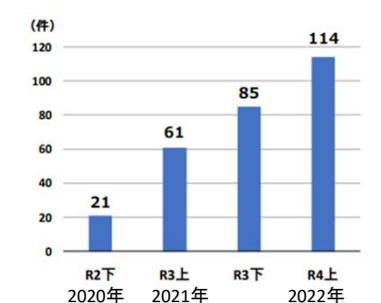
“NotPetya”

感染原因:
ソフトの脆弱性

11

企業・団体等に於けるランサムウェア被害

警察庁 令和4年9月15日

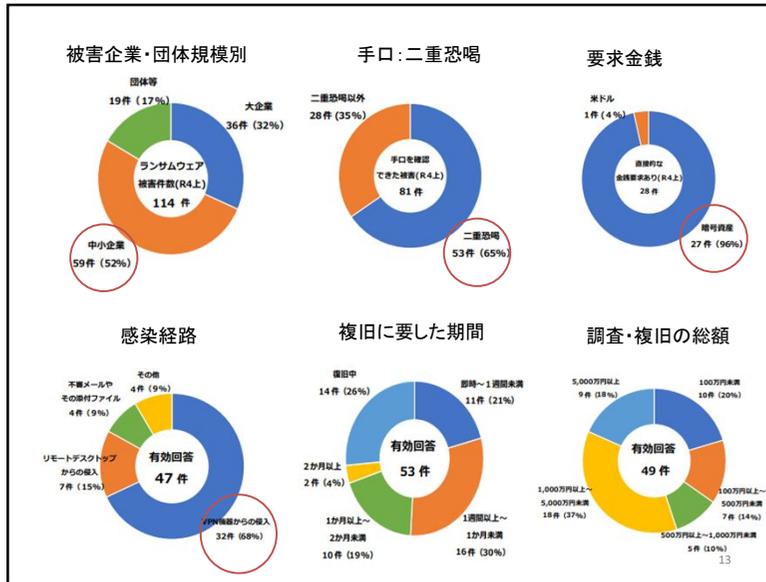


期間	報告件数
R2下 (2020年)	21
R3上 (2021年)	61
R3下	85
R4上 (2022年)	114

・令和4年上半期に警察庁への報告件数114件
 右肩上がり増加

- 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



(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:
ファイアウォール、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

徳島つるぎ町立半田病院:ランサムウェア攻撃被害

- 2021年10月末:ランサムウェア感染(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(ソフトウェア脆弱性)
- 復旧:2ヶ月
- 費用:約2億円

日経 XTECH

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

ランサムウェア 変異型拡大、1万種確認、被害増加

一般的な対策ソフトと変異型ウイルスの仕組み

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

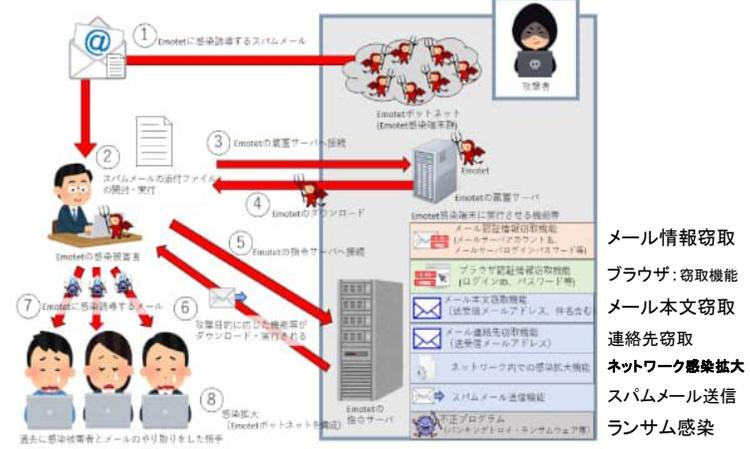
- BCP対策: 侵入前提での対策必要
 - バック・アップ ネットワークとは切り離す
 - 重要機密資料:暗号化

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
- ランサムウェ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

Emotet 動作概要

警察庁 2022年6月



- メール情報窃取
- ブラウザ：窃取機能
- メール本文窃取
- 連絡先窃取
- ネットワーク感染拡大
- スパムメール送信
- ランサム感染

Approval for Tsuchitani
 業務部 山本 <solivo@mundodeportivo-ec.com>
 送信日時: 2019/10/17 (木) 11:17
 宛先: Tsuchitani
 添付ファイル: 20191017_M1191.doc (233 KB) **支援企業先からの返信 Emotet**

2019/10/17(木)11:17

All done.

Kindly assist. please.

Best wishes

業務部 山本

Sent from my Samsung Galaxy smartphone.

Message protected by MailGuard: e-mail anti-virus, anti-spam and content filtering.
 FilteringV-http://www.mailguard.com/kg

Este mensaje ha sido analizado en busca de virus y otros contenidos peligrosos, y se considera que está limpio.

ESET Internet Security

この電子メールで...
 Message_20191017_M1191.doc - GenScript.GPH トロイ...木馬 - 駆除されま...た

不正マクロを仕組んだ添付資料

ウイルスソフトによる警告

新型コロナにかこつけた保健所を語るメール例

Mozilla Thunderbird

差出人: 保健所福祉室 <...@...>
 件名: 通知 2020 Jan 29
 宛先: ...

管内 通所・施設系障害福祉サービス事業者 様
 お世話になっております。

新型コロナウイルス関連肺炎については、中国武漢市を中心に患者が報告され、国内でも...県で患者が報告されているところであり、

つきましては、別添通知をご確認いただき、感染予防対策についてよろしくお願いたします。なお、並行してワムネット...ページの掲載準備をしております。

 保健所福祉室(担当: ...)
 〒...
 電話: ...
 FAX: ...

添付ファイル: instruction Jan 29 2020.doc 174 KB
 instruction Jan 29 2020.doc 174 KB

マクロを仕組んだ添付資料

注意! このパソコン上で、文書ファイルに埋め込まれているマクロ(プログラム)等の実行を許可するという意味のボタン。このボタンをクリックすると、悪意のあるマクロが動作し、ウイルスに感染させられてしまう。

セキュリティの機能。一部のアクティブコンテンツが無効にされました。クリックすると詳細が表示されます。コンテンツの有効化

Office 365

Operation did not complete successfully because the file was created on iOS device.
To view and edit document click Enable Editing and then click Enable Content.

利用者に「コンテンツの有効化」をクリックさせるための偽の指示

IPA Emotetに関する記事2020年9月2日

21

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(Inkファイル)を悪用して Emotet へ感染させる手口

添付ファイル:InkファイルをクリックするとEmotet感染

22

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

Archive file attached to email: Electronic form Dt 04.25.2022, United States.zip

パスワード: [redacted]

このメールに記載されているパスワードを使ってZIPファイルを解凍するとショートカットファイルが抽出される

①メールの添付ファイルをPCへ保存

危険! ショートカットファイルを開くとウイルスに感染させられてしまう

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

23

3) 対応策

3.1 個人PCのウイルス感染防止等の自衛策

- ①ソフトウェア: 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

24

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
マルウェアの仕掛けの可能性、ウイルスソフトで確認
- 2) スпам(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) ランサムウェア(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!**

25

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ヶ条
に取り組む。



セキュリティ対策自己宣言

** 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

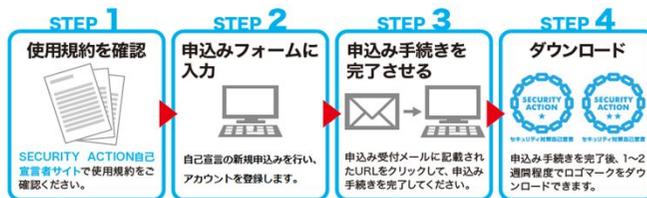


セキュリティ対策自己宣言

26

SECURITY ACTION の手続き手順書

IPA



SECURITY ACTION のメリット:

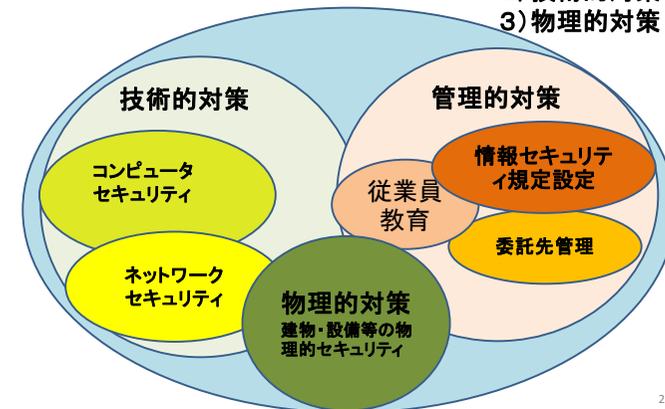
- 1) 企業・従業員の情報セキュリティに関する意識向上
- 2) IT補助金申請要件

27

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



28

