

なぜ日本企業が サイバー攻撃の餌食にされるのか？ —ハッカーからみた日本企業



Enobyte
Data Protection

ミュンヘン日本人会
令和4年6月22日

目次

- 1) はじめに
- 2) LIVE ハッキング
 - パスワードクラッキング(総当り攻撃)
 - なりすましメール
 - 虚偽のウェブサイト&フィッシング
- 3) まとめ
- 4) 質疑応答

はじめに



(日刊スポーツ、2020 年 5 月 30 日、https://www.nikkansports.com/general/nikkan/photonews/photonews_nsinc_202005300000025-0.html)

働き方改革



急速なデジタル化

15%

2021年

サイバー犯罪者にとって日本企業を攻撃することは非常に困難

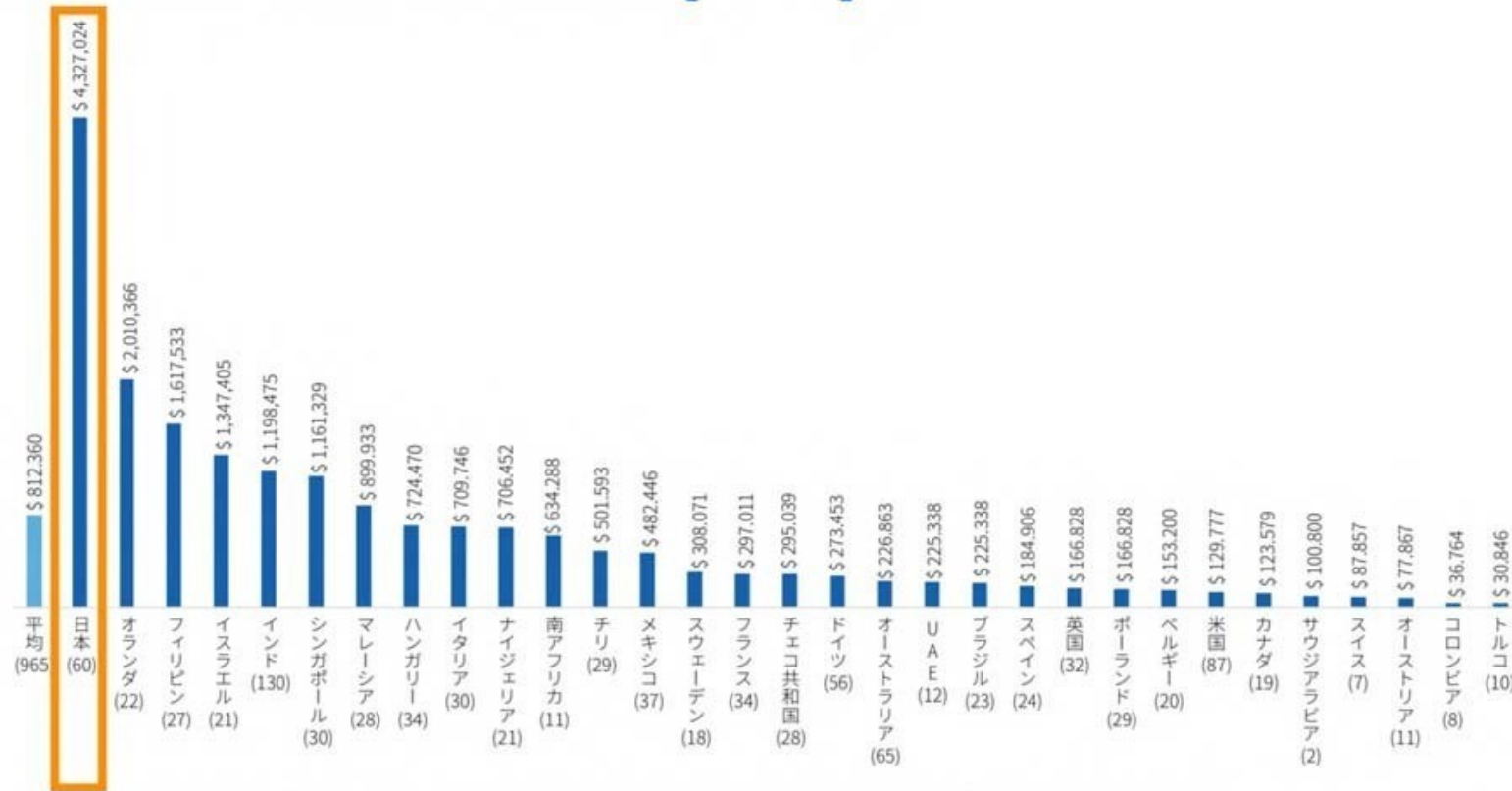
61%

2022年

日本企業への攻撃が急増

ランサムウェアの現状

身代金の平均支払い額（国別）



「最も深刻なランサムウェア攻撃において、支払った身代金はいくらでしたか？」(単位: 米ドル)回答数はグラフ内。「わからない」は除外。

注: 回答数が少ない国に関しては、参考値としてお考えください。

身代金を支払えば解決か？

LIVE ハッキング



これからお見せするハッキングデモは、皆様にサイバー攻撃の手口を紹介し、今後の対策に役立ててもらうことを目的とするものです。

決して真似しないでください。

パスワードクラッキング (総当り攻撃)



パスワードクラッキング

パスワード

ハッシュ値

PASSWORD
JAPANCLUB2022
X7IMhf97f!o
Very_LongSTrinG-ga-iine!! 99.5%secure,sehr gut&stark
CorrectHorseBatteryStaple

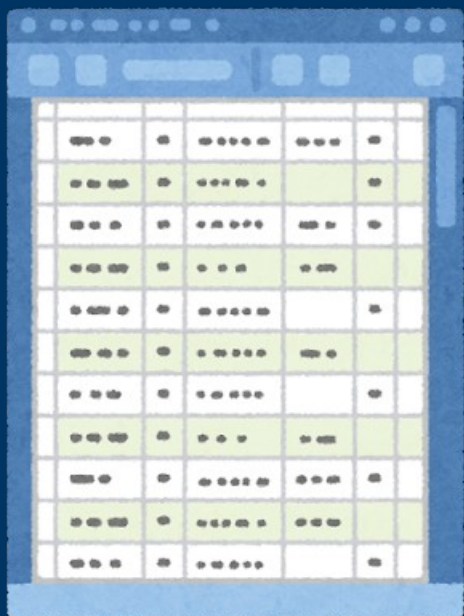
ハッシュ化



一方向性

0be64ae89ddd24e225434de95d501711339baeee1 8f009ba9b4369af27d30d60
1a76540542c919cd3f99eb2c7656a44aa382d84789 41b3f18a8fe930fd4f14e9
1a76540542c919cd3f99eb2c7656a44aa382d84789 41b3f18a8fe930fd4f14e9
1a76540542c919cd3f99eb2c7656a44aa382d84789 41b3f18a8fe930fd4f14e9
7abdae32d3c9fd31959fd66c8c48de11bdff24b1dad 2542f46faa0ebc50329fe

パスワードクラッキング



レインボーテーブル
… ハッシュ化の法則が分かる



- ① 自動的にハッシュ生成
- ② レインボーテーブルと比較
- ③ パスワードを復元

計算が要らないから速い!

〈デモの説明〉

普通の PC と、John というパスワードクラッキングソフトを使って、**7文字のパスワード**を当てていきます。

試すパスワードの数は、**一秒あたり4万個**です。

DEMO

推奨事項(1):

強いパスワードを作る

パスワードクラッキング

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

推奨事項(2):

パスワード付きの ZIP ファイルはメールで送らない・受け取らない

なりすましメール



〈デモの説明〉

info@japanclub-munich.deになりすまして、メールを送ります。

DEMO

推奨事項(1):

怪しいメールの
リンク・ファイルは
クリックしない

推奨事項(2):

デジタル署名
(PGP、S/MIME など)



虚偽のウェブサイト & フィッシング



虚偽のウェブサイト & フィッシング

(本物) <https://www.japanclub-munich.de/>

(偽物) <https://www.japanclub-munich.de/>

虚偽のウェブサイト & フィッシング

(本物) <https://www.japanclub-munich.de/> → 小文字の L

(偽物) [https://www.japancIub-munich.de/](https://www.japanc<u>I</u>ub-munich.de/) → 大文字の I

虚偽のウェブサイト & フィッシング

(本物) <https://www.japanclub-munich.de/> → 小文字の L

(偽物) [https://www.japancIub-munich.de/](https://www.japanc<u>I</u>ub-munich.de/) → 大文字の I

- 未登録のドメイン名であれば、誰でも登録できる
- 費用対効果が高い(年間1,400円程度)

〈デモの説明〉

いかに**短時間**で**ウェブサイトのクローン**ができるのかを紹介します。

本物とそっくりのウェブサイトにユーザーがログインすると、**ログイン情報を含む全てのデータが、攻撃者のもとへ送られます。**

DEMO

推奨事項(1):

偽装されそうなドメイン名は、
予め登録しておく

推奨事項(2):

緊急時のガイドライン・
メールの文面を
前もって用意しておく

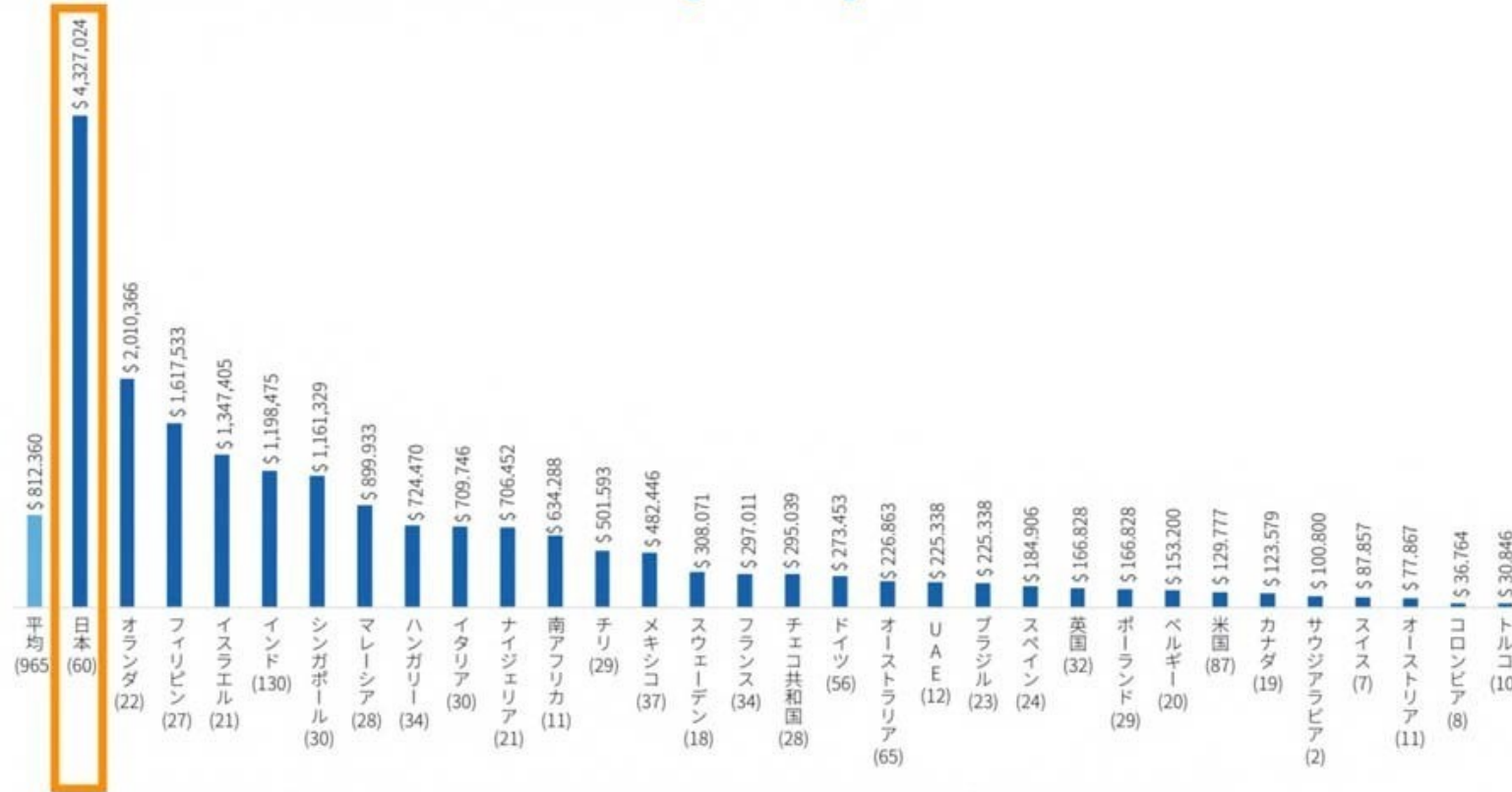
推奨事項(3):

ウェブサイトのログインに
二要素認証を導入する

まとめ

ランサムウェアの現状

身代金の平均支払い額（国別）



「最も深刻なランサムウェア攻撃において、支払った身代金はいくらでしたか？」(単位: 米ドル)回答数はグラフ内。「わからない」は除外。

注: 回答数が少ない国に関しては、参考値としてお考えください。

サイバー保険 = 問題解決 & 安心 ?

サイバー保険 = 問題解決 & 安心 ?

問題の本質:

- ・企業のイメージダウン
- ・顧客・取引先からの信頼を失う
- ・データの紛失による事業停止 等

従業員一人ひとりが
リスクを自覚し、
危機感を持って行動する

質疑応答

ご清聴ありがとうございました。

Enobyte GmbH
Augustenstraße 49
80333 München
089 - 215 4774 - 30
support@enobyte.com
<https://enobyte.com>