ITセキュリティをゼロから考える

講義の意図

対象者

- 情報システム担当者
- 情報システムの人員を配置していない会社の総務担当者

講義の意図

- セキュリティ対策は時代とともに変化します
- 10年前の考えは今は間違えとされたりします
- 過去のセキュリティ対策の思い込みを捨て、原点回帰する

パスワード

パスワード

- パスワードは何文字に設定していますか？
- 数字だけですか？
- 英字だけですか？
- 英字と数字混ぜてますか？
- 英字と数字と記号を混ぜてますか？

複雑なパスワードにする意味あるの？

→**あるんです**

パスワード

総当たり攻撃でパスワードを探した場合

桁数	6桁	8桁	10桁	12桁	14桁
アルファベット	400ミリ秒	22分	1ヶ月	300年	80万年
アルファベット+数字	1秒	1時間	7か月	2000年	900万年
アルファベット+数字 +記号	19秒	2日	52年	40万年	40億年

パスワード

理想は以下の用のパスワードが良い

3Jgkdsa@#a%q2frGajfg

長所

- 推測されにくい
- 総当たり攻撃でも見つけられない

短所

- 覚えられない
- どこかにメモしなければならず、メモが盗まれたら終わり

パスワード

パスワード設定のコツ

- 推測されにくい
- 覚えやすい
- 総当たり攻撃でも見つけられない

こんな条件のパスワードなんか作れるの？

A.作れます

パスワード

サンドイッチが好きだからパスワードを以下にするとします。

Daisukisandwich　（大好きサンドイッチ）

しかしパスワードが「大好きサンドイッチ」と知られると突破されてしまうので以下のようにします

- aを@,iを1に変更
  D@1suk1s@ndw1ch
- 間に推測つかない記号や文字を入れる
  Daisuki#sand%wich

パスワード

- 一文字置き換え
  i → 1、l → 1、a → @
- 複数の文字の置き換え
  ni → 2,san → 3、Shi →4、Go→5
  例
  SantaMonica → 3taMonica

このようにすれば以下の条件に合うパスワードを作れる

- 覚えやすい
- 推測されにくい
- 記号を含む
- 長いパスワード

パスワード（サーバーシステム）

サーバーシステムのログインパスワードの場合は二段階認証が使えるか確認します。

正式名称は以下の通りですが、日本では二段階認証という名前が普及している。

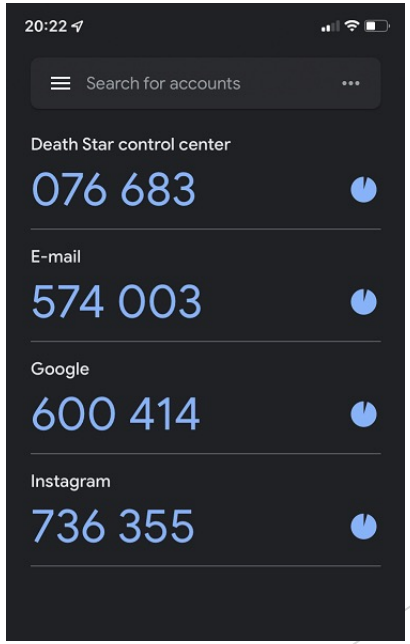
- 多要素認証
- MFA
- Multi Factor Authentication

パスワード（サーバーシステム）

多要素認証には以下のものがあります

電話番号やメールアドレスを登録しパスワード入力後SMSにて６桁の数字の認証キーを送信する

Authenticator アプリもしくは番号を発行するキーホルダーと連動させて１分１回数字発行したものを入力する

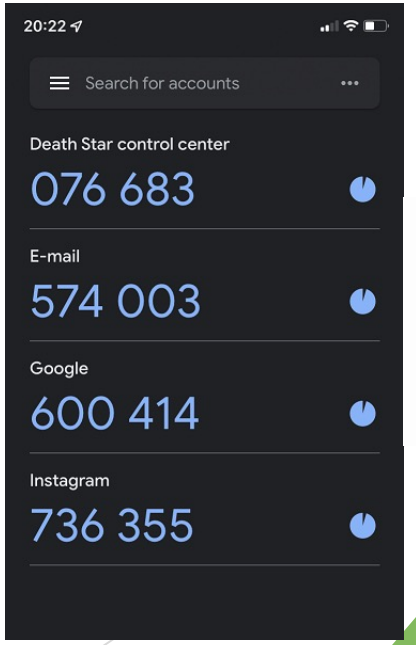


パスワード（サーバーシステム）

多要素認証は１分毎にランダムに生成される番号を入れることでセキュリティが担保される

- サーバーが発行したユニークキーをアプリに登録
- キーホルダーのユニークなシリアル番号を登録
- 電話番号
- メールアドレス

多要素認証があれば多少パスワードを簡素化してもセキュリティレベルは落ちない

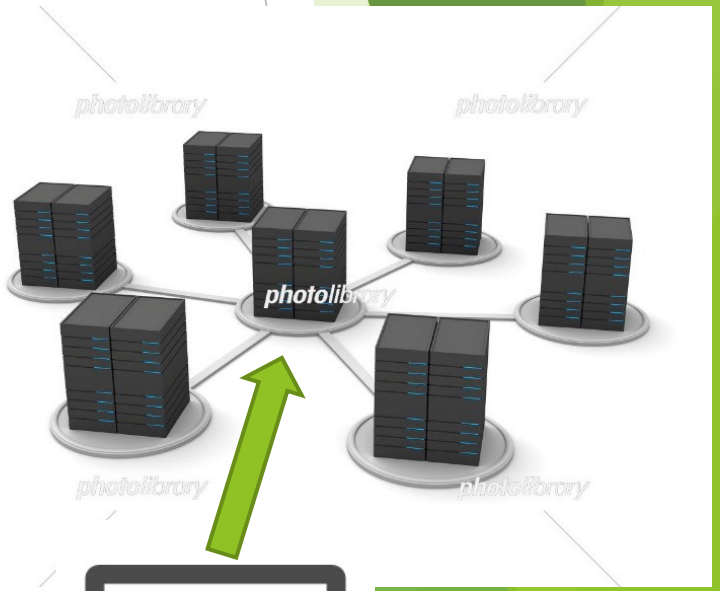


パスワードの入力回数を減らす

管理するサーバー数が多くなるとパスワードを入力する回数が増えて利用者の負担が増えます。

そこで、シングルサインオン(SSO)を導入してパスワード入力の負担を減らします。

１回認証が成功すると SSO サーバーが認証情報を共有してくれるため、他のサーバーはパスワードなしでログインできます。



パスワードを3か月毎に変えるルール？

2000年頃 Microsoft Active Directory が普及し始めたころから始まったルール

- パスワードを３が月に１回変更する
- 過去１０回まで使ったパスワードの使いまわし禁止

このルールってセキュリティ上有効なの？

A.無意味です

2019年4月に Microsoft が公式にセキュリティ上無意味だったと認めてます。負担が増えるだけでなんの意味もないのですぐにやめましょう。

アンチウイルスソフト

コンピューターウイルス

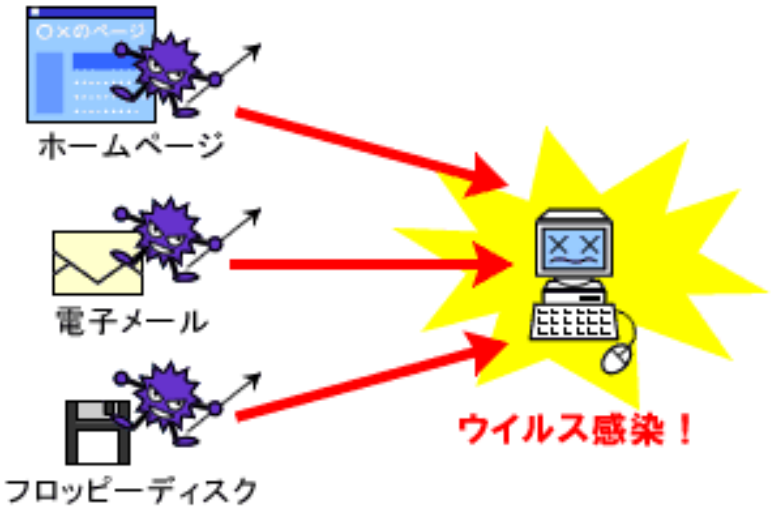
コンピュータに入り込むとコンピュータを本人の意思とは無関係に操るソフトの事を言います。

最近ではマルウェア(malicious software 悪意のあるソフト)という言葉も使われます。

コンピュータウイルスは３つの特徴と４つの種類に分類されると言われています。

コンピューターウイルスの特徴

- 自己伝染機能
  他のプログラムやシステムに自分の複製をコピーする
- 潜伏機能
  一定時間もしくは特定の条件が揃うまで実行しない
- 発病機能
  ファイルの破壊、異常動作を実行する



コンピューターウイルスの種類

- ワーム型
  増殖機能が強いウイルス。別のデバイスに感染する様子が虫に似てるから名づけられた。不正URLのクリックで感染する。誤動作、情報漏洩等
- トロイの木馬型
  スクリーンセーバーやバックグラウンドに常駐して感染する。情報漏洩や遠隔操作などがあります
  IoT デバイスに感染して DDoS攻撃端末として利用する Mirai などがあります

コンピューターウイルスの種類

- マクロ型
  Microsoft Office 製品のマクロ機能を利用したウイルス。ファイル変更、削除、自己増殖、アプリの設定変更、メール送信等
- ファイル感染型
  exe, com などのプログラム実行ファイルに感染し、プログラムを改ざんする。上書き型、追記型に分かれる。

アンチウイルスソフトの選定

1995年～2000年初期

- TrendMicro　ウイルスバスター
- McAfee　アンチウイルス
- Symantec　アンチウイルス

3大アンチウイルスソフトウェア

アンチウイルスソフトの選定

2005年価格.com サーバー トロイの木馬混入事件

- 価格.comサーバーがハッキングされマルウェアが混入された
- 3大アンチウイルスソフトウェアがこのウイルスを検知できなかった

この事件をきっかけに３大ソフトウェアの優位性が疑問視された

このマルウェアを唯一検知できたソフトとして

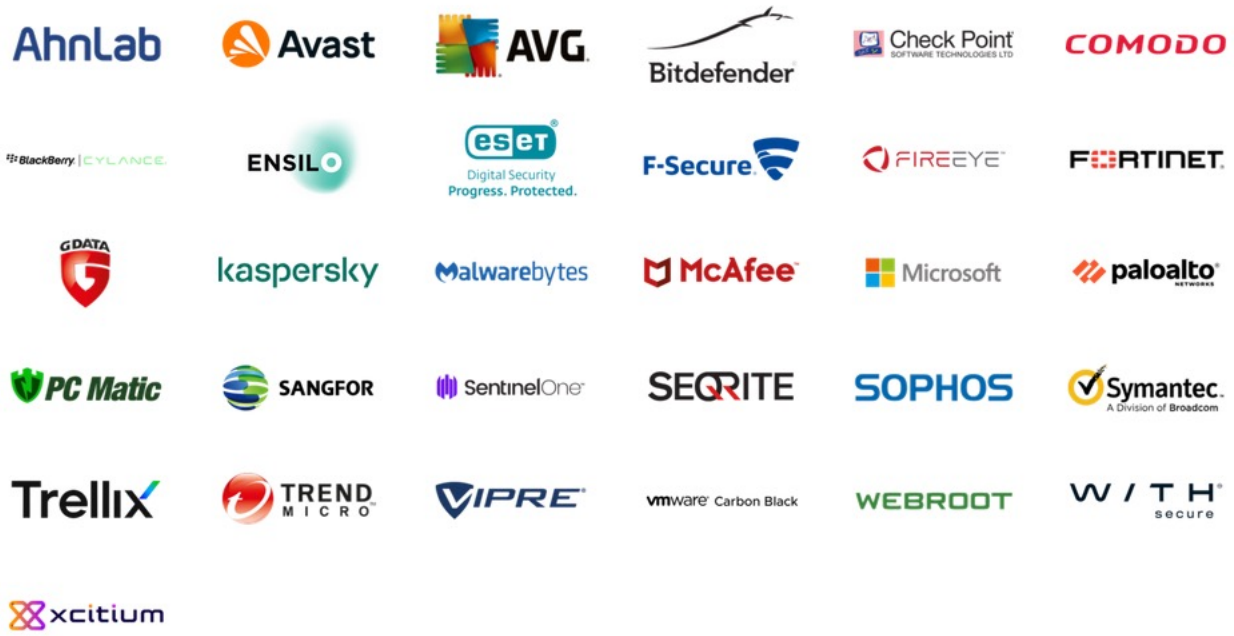
ESET NOD32 に注目が集まる

アンチウイルスソフトの選定

各社から様々なアンチウイルスソフトの製品がリリースされています。そして様々な形で利用を勧められます。

- 販売店の勧め
- 購入したパソコンに付属
- 知人の勧め
- 法人サービス業者の勧め
- 雑誌記事

どれも勧めるソフトの長所しか述べません



アンチウイルスソフトの選定

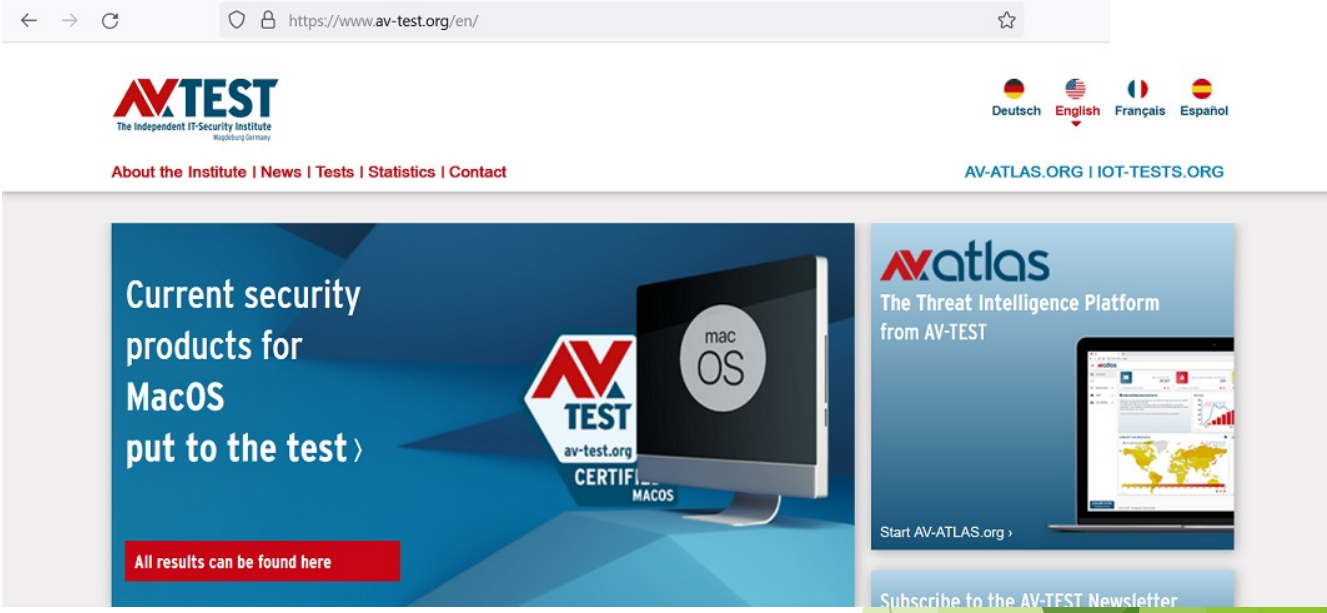
実際はどれがいいの？

正解は時代によって変わるので最新の検査指標を参考にする。

AV-TEST というドイツに本拠地を置くセキュリティソフトウェア調査会社の検査指標がよい。

- システム保護
- パフォーマンス
- 使いやすさ

この３つをテーマに検証しています



https://www.av-test.org/en/

システム保護

ゼロデイマルウェアの保護

ウイルスパターンとして存在しないウイルスを検出できるのか。

ゼロデイ(0 day)…対策が講じられる前に行われるもの

374パターンのサンプルウイルスで検証(2022年)

過去４週間以内に発見されかつ広範囲で確認されているマルウェアの検出の可否

リリースされて間もないが猛威を振るうウイルスを検知できるかを確認する

23,431パターンのサンプルウイルスで検証(2022年)

パフォーマンス

- 人気のあるWebサイトを起動した際の速度低下
  60サイトで検証(2022年)
- よく使われるアプリのダウンロード速度の遅延
  25ダウンロードファイルで検証(2022年)
- 標準ソフトウェアアプリケーションの起動速度
  63パターンのテストケースで検証(2022年)
- 頻繁に利用するアプリケーションのインストール速度
  25種類のアプリケーションで検証(2022年)
- ファイルコピー検証
  9852種類のファイルでコピー検証(2022年)

使いやすさ

アンチウイルスソフトの誤検知は使いやすさに影響を及ぼします。

- Webサイトアクセス時に誤った警告やブロック
  500のサンプルで検証(2022年)
- スキャン時正規のソフトウェアをマルウェアとして誤検知
  1,084,883のサンプルで検証(2022年)
- 正規ソフトインストールおよび特定のアクションの誤警告
  30サンプルで検証(2022年)
- 正規ソフトインストールおよび特定のアクションの誤ブロック
  30サンプルで検証(2022年)

2022年6月度の調査

オール６をはじき出している製品が優秀、他も許容範囲レベル

結論、**どのウイルスソフトもそれほど外れがない…**

AhnLab	V3 Endpoint Security 9.0	6	6	6
Avast	Business Antivirus Pro Plus 22.3 & 22.4	6	6	6
Bitdefender	Endpoint Security (Ultra) 7.5	6	6	6
Bitdefender	Endpoint Security 7.5	6	6	6
eset Digital Security Progress. Protected.	Endpoint Security 9.0	6	6	6
G DATA	Endpoint Protection Business 15.1	6	6	6
kaspersky	Endpoint Security 11.9	6	6	6
kaspersky	Small Office Security 21.3	6	6	6
Malwarebytes	Endpoint Protection 1.2	6	6	5.5
Microsoft	Defender Antivirus 4.18	6	6	6
SECRITE	Endpoint Security 18.00	6	6	6
Symantec. A Division of Broadcom	Endpoint Security Complete 14.3	6	6	5.5
Trellix	Endpoint Security 10.7	6	6	6
TREND MICRO	Apex One 14.0	6	6	6
WITH secure	Elements Endpoint Protection 22.3	6	6	6
SOPHOS	Intercept X Advanced 10.8	6	5.5	5.5
vmware Carbon Black	Carbon Black Cloud 3.8	6	5.5	6
xcitium	Client Security 12	6	5	5.5

パソコンの盗難と廃棄

設置場所からの盗難防止

設置場所及び保管場所からPCの盗難を防ぐ

- ワイヤーロックなどで机に固定する
- 鍵付きロッカーに不使用時のPCを保管

こんなもの誰も取らないだろう…という発想が危険です。取られたら困るものはとられない用心が必要です。

盗難されてしまったら

移動中などでPCが入ったカバンを置き忘れてしまったり、盗まれてしまった場合です。

どんなに複雑なパスワードを設定していたとしても、パソコンの中のディスクを引き抜き、別ディスクとして認識してしまえば、中のデータを見ることができます。

BitLocker の設定

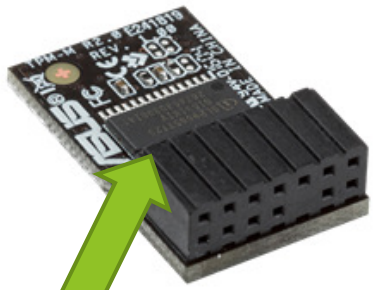
設定条件

- TPM(Trusted Platform Module)チップ搭載
  Windows11が推奨しているのはTPM2
- Windows8 以降のPCに標準搭載

仕組み

チップに入ったハッシュ情報を基にデータ領域を暗号化する。

ディスクを引き抜いて別のパソコンに接続してもマザーボードの**TPMチップが一致しないのでデータが複合できない**



BitLocker が不要な例

- PC端末に重要なデータを保存していない
- 保存する場合が発生したら作業完了後速やかに削除する
- データをすべてクラウド上で管理する
- パソコンはあくまでもサーバーの接続端末としての役目

盗難が発覚した瞬間にクラウド上のすべてのパスワードを変更してしまえば、盗難時のパスワードが分かってもデータが盗まれる心配はない

パソコンの廃棄

パソコンの廃棄は産業廃棄物処理業者に任せてれば大丈夫と考えが間違いだったという事件が2019年12月に神奈川県で発生しました。

第三者が廃棄されたディスクの内部のデータの価値を見出し転売する事件が発生しました。

第三者の手に渡る時にはデータが復元できないようにしなければならない

【独自】行政文書が大量流出　納税記録などのＨＤＤ転売

神奈川ＨＤＤ流出

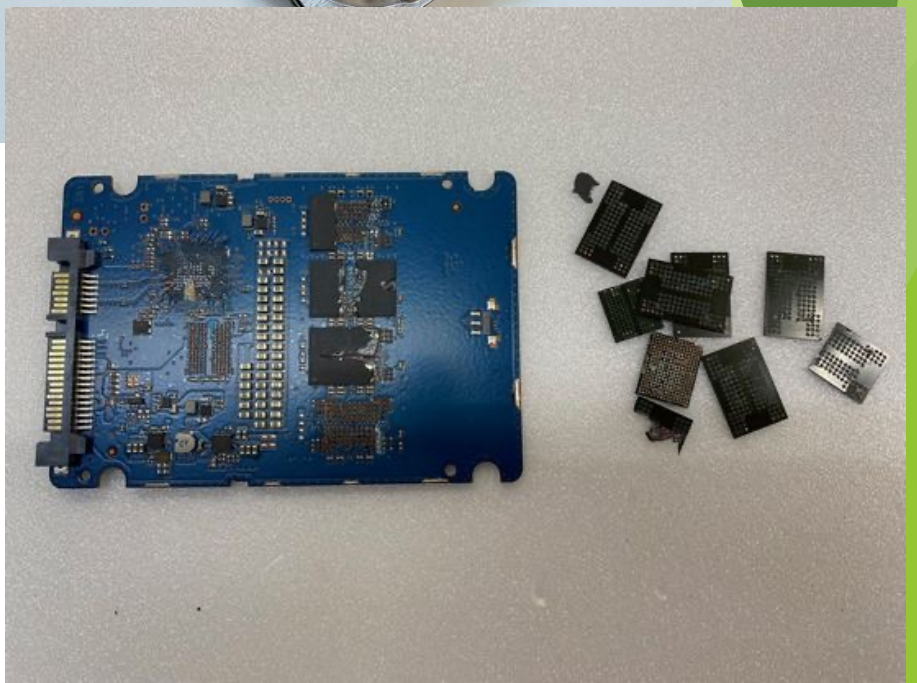
茂木克信　2019年12月6日 5時00分

神奈川県庁＝横浜市中区

納税などに関する大量の個人情報や秘密情報を含む 神奈川県 庁の行政文書が蓄積された ハードディスク （ＨＤＤ）が、ネットオークション を通じて転売され、流出していたことが朝日新聞の取材で分かった。県のサーバーから取り外されたＨＤＤのデータ消去が不十分なまま、中古品として出回っていた。県によると、データの消去から廃棄までを請け負った業者の社

データ領域の物理破壊

- ハードディスク
  円盤に穴をあければOK、円盤が回らないように破壊する
- SSD
  黒いチップにデータが保存されるので黒いチップを破壊したり基盤を真っ二つに折ればOK



長所：短時間で消去できる

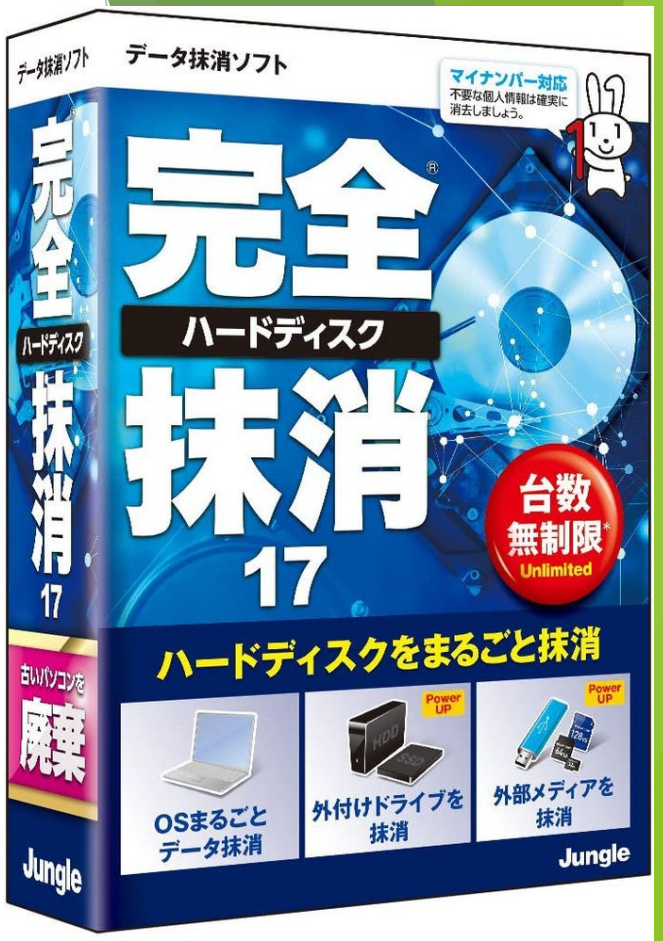
短所：物理作業の手間、価値がなくなる

データ領域の消去処理

市販の消去ソフトもしくはフリーの消去ソフトを使う。

これらのソフトにはハードディスクやSSDのデータを消去するプログラムが入っている。

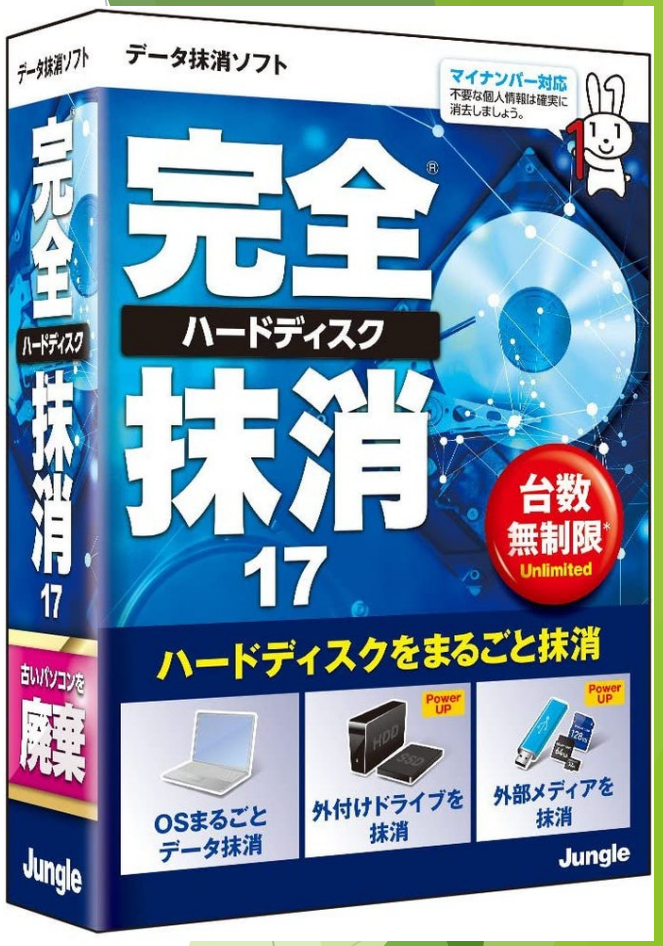
消去レベルのランクがありますが、行っていることは、ダミーデータを書き込んで削除を繰り返します。この回数が多ければ多いほどデータの復元が難しくなります。



データ領域の消去処理

データの消去グレードは３段階に分かれます

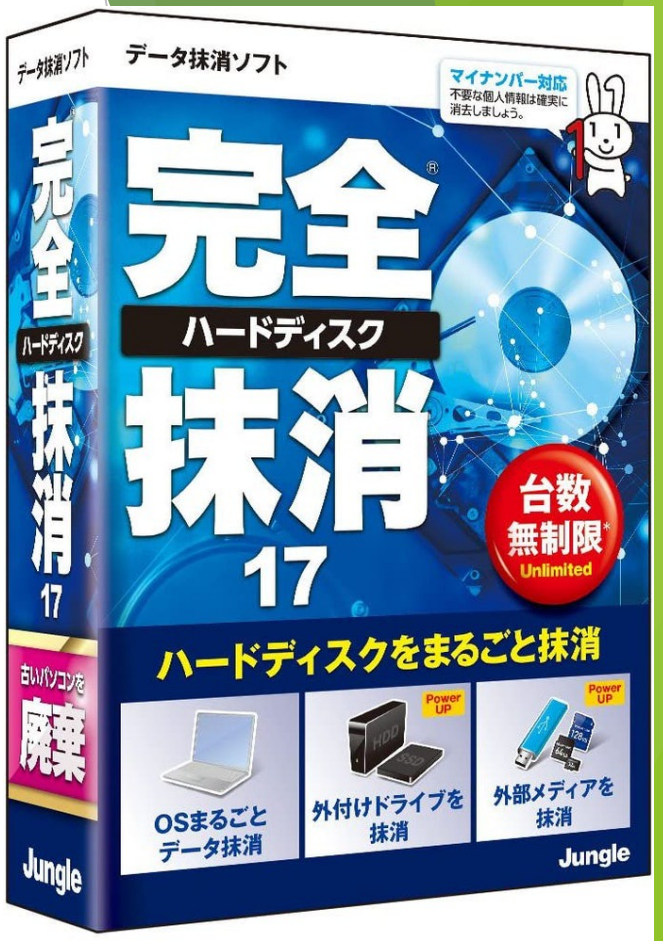
- 個人・企業内再利用PCのデータ消去方式
  - 個人で廃棄する場合
  - 会社内で返却されたPCを消去し他の部署に回す場合
- 機密情報・顧客データの消去方法
  - 廃棄する場合
  - 重要なデータの入ったPCをリース返却する場合
- SSD向け完全消去
  - SSDはハードディスクとデータの保存方法が異なるので SSDに特化したデータの消去方法



個人・企業内再利用PCのデータ消去

- ゼロライト方式
  データ領域ゼロ(0x00)で上書きする。
- ランダムライト方式
  乱数で上書きする
- NIST 800-88方式
  アメリカ国立標準技術研究所(NIST)が推奨する消去方法、ゼロ(0x00)を書き込んだ後、書き込み検証実施
- ランダム&ゼロライト方式
  データ領域を乱数で上書きした後ゼロ(0x00)で上書きする

※この方式は**消去時間が短時間**であるが、いづれも**残留磁気を読み取る装置**を使えば復元される可能性がある。



フォレンジックツール

消去された記憶媒体から残留磁気を読み取る装置があります。

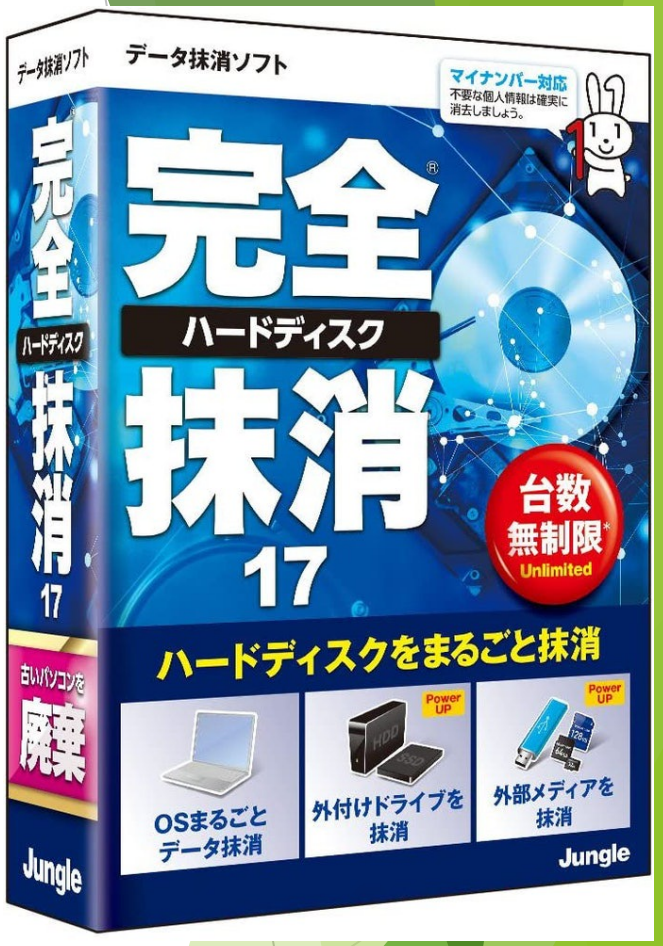
- フォレンジックツール
- 復元処理を「フォレンジック調査」という

事件や事故の調査でデータ消去された携帯電話、パソコンなどからデータを復元して事件解決などに利用される

従業員及び第三者の不正行為が記録されたPCを証拠隠滅などで消去されてしまった場合にこのようなもので復元する

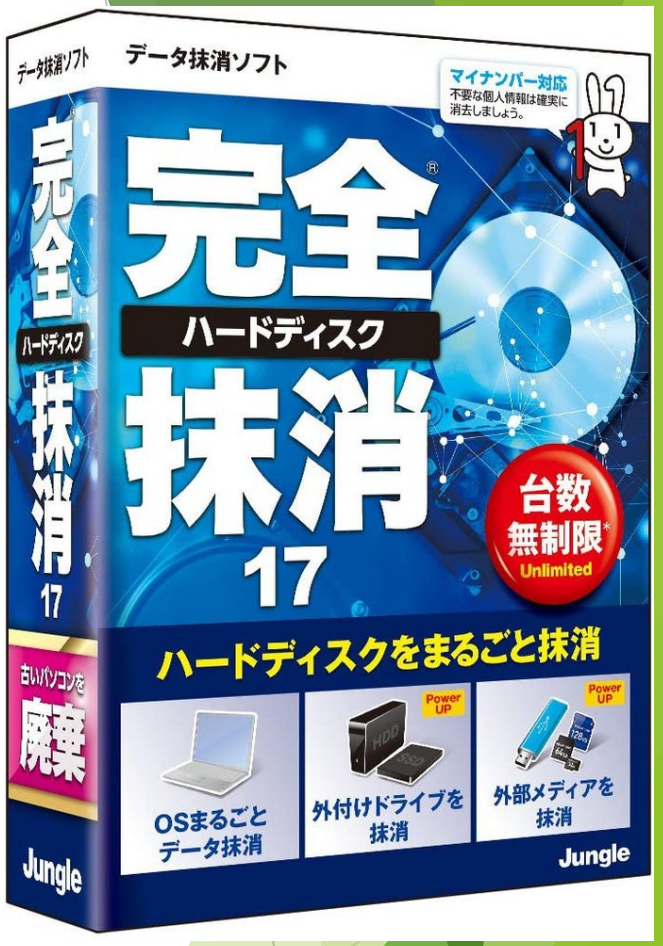
機密情報・顧客データの消去方法

- NIST 800-80 Advanced方式
  アメリカ国立標準技術研究所(NIST)が推奨する NIST800-80に準拠した消去方式
- 現NSA方式(ランダムランダムゼロ)
  ディスク全体を乱数で２回上書きした後ゼロ(0x00)を上書きする
- 米国国防総省準拠方式 DoD5200.28-M
  ディスク全体を固定値(0xff)、ゼロ(0x00)、乱数で上書きする。
- 米国空軍方式 AFSSI5020
  ディスク全体をゼロ(0x00)で上書きした後、固定値(0xff)、ランダム固定値で書き込み最後に検証を実施



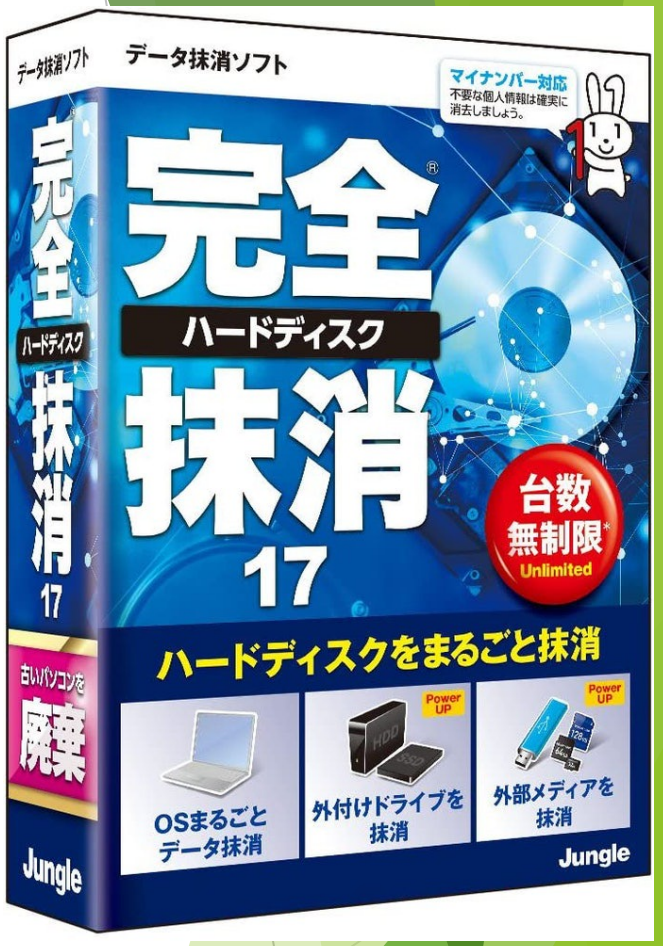
機密情報・顧客データの消去方法

- 米国国防総省準拠方式　DoD5220.22-M
  ディスク全体の領域を最初にゼロ、次に0xff、乱数で上書きし、最後に書き込み検証を行います。国内企業・官公庁で、最も採用されている方式
- 米国海軍方式　NAVSO P-5239-26-MFM
  ディスク全体の領域を固定値（0x01）、固定値（0x7ffffff）、乱数で上書きした後書き込み検証を行う
- 米国海軍方式　NAVSO P-5239-26-RLL
  ディスク全体の領域を固定値（0x01）、固定値（0x7ffffff）、乱数で上書きした後書き込み検証を行う
- 旧NSA方式 Bit Toggle
  ディスク全体の領域をゼロ（0x00）、固定値（0xff）、ゼロ（0x00）、固定値（0xff）の順に計4回の上書きを行います。



機密情報・顧客データの消去方法

- ドイツ標準方式 VSITR
  ディスク全体の領域をゼロ（0x00）と固定値（0xff）のパターンを3回繰り返し上書きし、最後に固定値（0xAA）で上書きする
- グートマン推奨方式
  ディスク全体の領域に対して最初に乱数を4回、その後固定値を27回、最後に乱数を4回、合計35回の上書きを行います。1996年にピーターグートマンによって紹介された方式



選ぶコツ：完全に好み、名前の響き

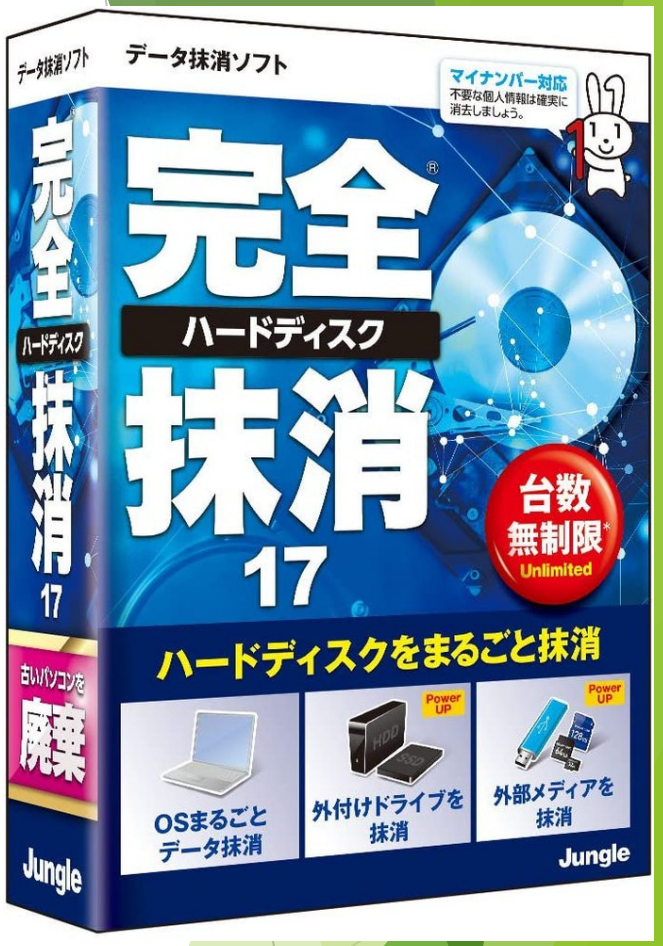
どれも実行するのに１～２日程度かかりますが、フォレンジックツールなどでの復元が不可能

SSD向け完全消去

- Secure Erase方式
  SSDのマッピングテーブルを消去し工場出荷状態に戻す方式。
  SATA/IDE SSDに用意されているコマンドを使用し、高速にデータ消去を実行します。
- 拡張 Secure Erase 方式
  SSD内部に設定された固有の値でデータを消去します。
  SATA/IDE SSDに用意されているコマンドを使用し、高速にデータ消去を実行します。

特徴

SSDに特化して開発された方式の為、消去処理が HDD 向けに作られたものよりも処理が速く復元も不可能



ネットワーク

ネットワーク

現代社会においてネットワークがなければ仕事にならないと言っても過言ではありません。

便利な反面、第三者の悪用も懸念されます。

第三者が出入りせざるを得ない会社の場合は以下を分けます

- 社員向けネットワーク
  - すべてのリソースにアクセスできる
- ゲスト向けネットワーク
  - インターネット接続
  - 社外の人へのアクセスを許したシステムのみアクセス

有線LAN

有線LANは DHCP 設定されているネットワークに接続すればすぐにネットワークにアクセスできます。そのため第三者へのセキュリティ対策を講じる必要があります。

VLAN設定

ゲストネットワークと社内向けネットワークを VLAN で物理的に分断し、エリアを分ける

無線LANの接続方式

- WEP接続、WPA接続
  Wi-Fi初期の暗号化方式、改ざんされやすいため現在は利用を推奨されていない。
  →**同機能しか搭載されていない Wi-Fi AP は廃棄する**
- WPA2(Wi-Fi Protected Access 2)
  802.11i ワイヤレスセキュリティスタンダードと呼ばれるポピュラーな企画
  2017年11月に脆弱性発見→FWアップデートで対応
- WPA3(Wi-Fi Protocted Access 3)
  2018年6月に登場した新しい暗号化企画、WPA2と互換性を持つ
  2019年４月に脆弱性発見→FWアップデートで対応

WPA2, WPA3の脆弱性が見つかるが、FWアップデートで対応できるのでこまめにFWの最新バージョンをチェックする

無線LAN

- ゲスト用 Wi-Fi
  インターネット接続およびゲスト向けに開放したリソースのみ接続許可、VLAN設定
- 社員向けネットワーク
  社内のリソースすべてにアクセスできる。

社員向け SSID とパスワードの公開

- 担当者及び一部の人間のみ共有
  パスワード情報が漏れにくいが管理者に集中し大変
- 全社員に公開
  この場合は第三者に漏れやすくなるので、アクセス制限を行う

無線LANのアクセス制限

MACアドレス
ネットワーク機器に固有に降られる番号
例) 88-D7-F6-7F-5B-73

- 重複しない番号
- この番号で制御すれば固有デバイスの制限ができるのでは？

2000～2010年くらいまで、割と流行ったセキュリティ

無線LANのアクセス制限

仮想環境の登場で揺らぐセキュリティ

VMware 、Xen、KVM などをはじめとした仮想マシン及び仮想マシンをコントロールするハイパーバイザーの登場で事態は一変いしました。

これらのツールは**自由に MAC アドレスを変更できる**のです。

- 登録されているマシンの MAC アドレスを調べる
- そのMACアドレスを仮想環境を持つPC上で割り当てる
- 許可されていないマシンが Wi-Fi アクセスができる

簡単に回避できる

無線LANのアクセス制限

最新OSが持つランダムMACアドレス機能の登場

- Windows
  Windows10以降
- iPhone
  iOS14からデフォルトでON
  ※それ以前も搭載されていたがデフォルトOFF
- Android
  バージョン8以降

昨今の OS にランダム MAC アドレス機能が搭載されています。

MACアドレスが接続するたびに変更されるため、ますます、MACアドレスによる制御設定が難しくなった。

無線LANのアクセス制限

WPA2エンタープライズ接続

- WPA2エンタープライズ対応無線LANアクセスポイント
- WPA2エンタープライズ対応クライアント
- RADIUSサーバー

上記３つの機器があれば構築可能

RADIUS サーバーで以下をユニークに管理できる

- 端末固有の情報
- ユーザー名
- パスワード

※MACアドレス管理を止めて、WPAエンタープライズを導入する

個人利用の場合は WPA2パーソナルで問題ない。

USBメモリ

USBメモリはデータを便利で簡単に持ち出したりできる反面、情報漏洩のリスクが問題視されています。

- 盗難・紛失による情報漏洩
- 利用者のモラル低下による漏洩
- 漏洩事故が発生した場合の漏洩元情報が追えない

特別な場合を除き原則利用を禁止することが望ましい

USBメモリ

代替え案

- メール添付による送信
  容量の制限がある
- ダウンロード用ファイルサーバーの用意
  ファイルサーバーの利用を記録を残す
- USBメモリ貸出申請式
  申請書を提出したら貸し出す
  貸出理由の目的を果たしたら速やかに返却する

→情報漏洩発生時に発生元を追える

情報漏洩事故が発生した時に漏洩元が追えることが大切

スマートフォン

2000年～2012年頃まで会社が携帯電話を支給するケースが多かったのは、携帯電話端末が安かったからですが、スマホ時代になり会社から支給するハードルの高さが問題視されています。

- 端末の価格高騰
  ガラケーの10倍近くする端末を人数分用意するのはハードルが高い
- 電話通話以外の利用の監視
  ガラケー時代は電話の発信先の管理だけよかった
  - 業務に無関係なインターネット接続の監視
  - 業務に無関係なアプリケーションの利用

スマートフォン

これらの問題の回避方法として以下の２つが考えられます

- 個人端末を業務端末として使うことを許可する(BYOD)
  →会社が端末を用意しない
- モバイルデバイス管理システム(MDM)の導入
  →会社が端末を用意する場合

個人端末を業務端末として利用許可

昨今スマートフォンを保有してない人がいないと言っても過言ではありません。

そこで、個人端末を業務端末として使用することを許可してしまう運用方法です。

- メールアプリ(Gmail, Outlook等)
- 電話アプリ（会社の番号・内線で通話可能）
- Authenticator
- 業務チャットアプリ(Slack, Teams等)

すべてクラウド管理なので盗難時、退職時はアカウント停止すればセキュリティ上問題ありません。

モバイルデバイス管理システムの導入

会社としてスマートフォンを支給する場合は、モバイルデバイス管理システム(MDM)を導入して管理するのが望ましいです。

- モバイル端末の紛失・盗難時のリモート制御
- デバイス機能の一元管理
- 各種ポリシー、アプリの一斉配布など

盗難が発覚した後にリモートでスマホのデータを抹消できるため情報漏洩を防げる

メールサーバー

メールサーバー

現代社会においてメールはビジネスにおいて欠かせない存在になっています。

管理方法

- 自社で構築・管理
- 小規模なホスティング管理
- Microsoft 365やGoogle Workspace などのクラウドサービス

自社構築・管理、小規模なホスティング

昔は自社構築・管理が主流でした。Linux やオープンソースが得意なエンジニアがメールサーバーを構築し、管理まで行っていました。私もその一人でしたが現在自社管理のメリットはないと思います。

- 日々発生するセキュリティ問題への対策の熟知
- 通信トラフィック膨大による回線帯域の確保の限界
- スマホ連携の難しさ
- IMAPが主流になりサーバーに膨大なメールを残す
- トラブル発生時の迅速対応の限界
- 高度な知識と強固な監視体制を要求される割に成果が低い

大手メールサービスを利用する

Google Workspace や Microsoft 365 などの世界レベルで可用性を担保しているサービスを利用することが望ましい

- 世界中で冗長構成してるのでシステムがダウンしない
- 膨大な通信トラフィックにも世界トップレベルのバックボーンで対応
- **スマホアプリとの連携の親和性の高さ**
- 世界トップレベルのセキュリティ
- パフォーマンスが低下しない
- 1ユーザー月額300～500円程度で対応可能
- サポートの充実

Microsoft 365　Google Workspace

ホームページ

メールアドレスの開示

自社のホームページにメールアドレスを載せていませんか。これは**第三者のスパムメールの送信対象になるので**すぐ止めましょう。

弊社へのお問い合わせは
info@example.com へ

お問合せ

入力フォームからお問い合わせいただければ、
管理者よりメールでご返答いたします。

お名前：
（必須）
メールアドレス
（必須）
ご質問
（必須）
送信

メール送信フォームを作成します。

こうすることでメールアドレスを開示せず問い合わせのメールを受信することができます。

HTMLのみのフォームはソースにメールアドレスが開示されてるので、**PHPなどのプログラムで作成**する。

ホームページの構成

ホームページをPHPやJSPなどで制作した場合、以下のセキュリティ対策を講じなければならないことは認識していますか。

- SQLインジェクション
- クロスサイトスクリプティング
- CSRF
- ディレクトリトラバーサル
- OSコマンドインジェクション
- セッション管理不備
- HTTPヘッダインジェクション
- HTTPS不適切な利用

ホームページの構成

今挙げた攻撃を理解し対策している人は問題ありませんが、わからない場合はサイトが攻撃にさらされているということです。

対応方法

- 今挙げた攻撃の対策を１つ１つ行う
  →代表的なものを８つ挙げただけで他にもある可能性あり
- CMSの利用
- フレームワークの利用

CMSの利用

Contents Management System の略で、Webサイトのデザインと内容の部分を分離し、内容を簡単に編集できる仕組み。

HTMLを理解してなくてもホームページの内容の編集が行える。

代表的なもの

- WordPress (オープンソース)
- Drupal(オープンソース)
- HeartCore(商用)

セキュリティ対策

定期的に CMS の公式サイトをチェックして脆弱性対応があった場合はバージョンアップを行う

フレームワークの利用

CMSは文章の修正程度しか行えず、ある程度自由にプログラムを組んだりする場合には利用できません。

その場合はフレームワークを使います。

- Ruby on Rails(Ruby)
- CakePHP(PHP)
- Synphony(PHP)
- Laravel(PHP)
- Django(Python)
- Spring Framework(Java)

フレームワークの利用

フレームワークは Model, View, Controller の MVC の考え方に基づいて開発します。

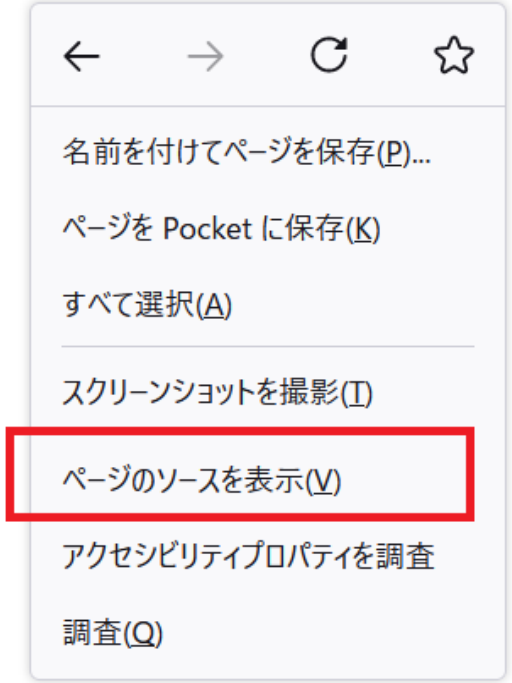
フレームワークが決めたファイル、ルール、記述方法に沿ってページを作成します。

メリット

- 記述するコードが少なくなり記述が統一される
  複雑なコードを１行で表せる文法を用意している
- 同じ記述を繰り返さない
  HTMLだと複数のページに同じ記述がまたがるが、１か所に定義して使いまわす
- **Webセキュリティ対策がフレームワーク事態に対応済み**

WebデザイナーのWebデザイン

Webデザイナーは企業の依頼を基に会社のホームページを修正します。その際に人によりますが、癖で HTML 内部にメモ代わりにコメントを残す人がいます。



ブラウザで開くと見えないからと言って記録した内容が、本来開示してはいけない情報をコメントしてしまってるケースが散見されます。

デザイナーにコメントに情報を載せないよう意識合わせや、掲載前に確認し削除する対応が必要です。

<!-- ここから下の情報は株式上場後に表示する。上場までは隠す -->

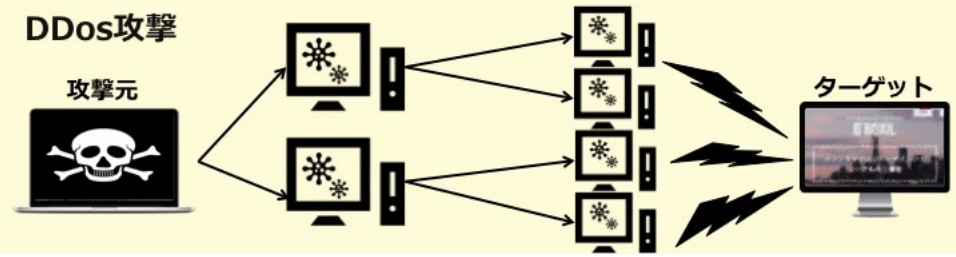
<!- 来期「事業部を〇〇工業に売却する情報を載せる」-->

DoS 攻撃と DDoS 攻撃

DoS攻撃

攻撃元が１台もしくは複数台のコンピュータを使って大量にアクセスすることでWebサーバーを落とす攻撃

→**身元が特定できるので不正アクセス防止法で逮捕も可能**



DDoS攻撃

攻撃元があらかじめマルウェア感染させた一般のサーバーをコントロールして複数台のコンピュータを使って大量にアクセスすることでWebサーバーを落とす攻撃

→**身元が特定できないので対応不可能**

DDoS 攻撃対策

DoS攻撃、DDoS攻撃の対策はただ１つ

ホームページのサーバーを隠しつつホームページを表示する

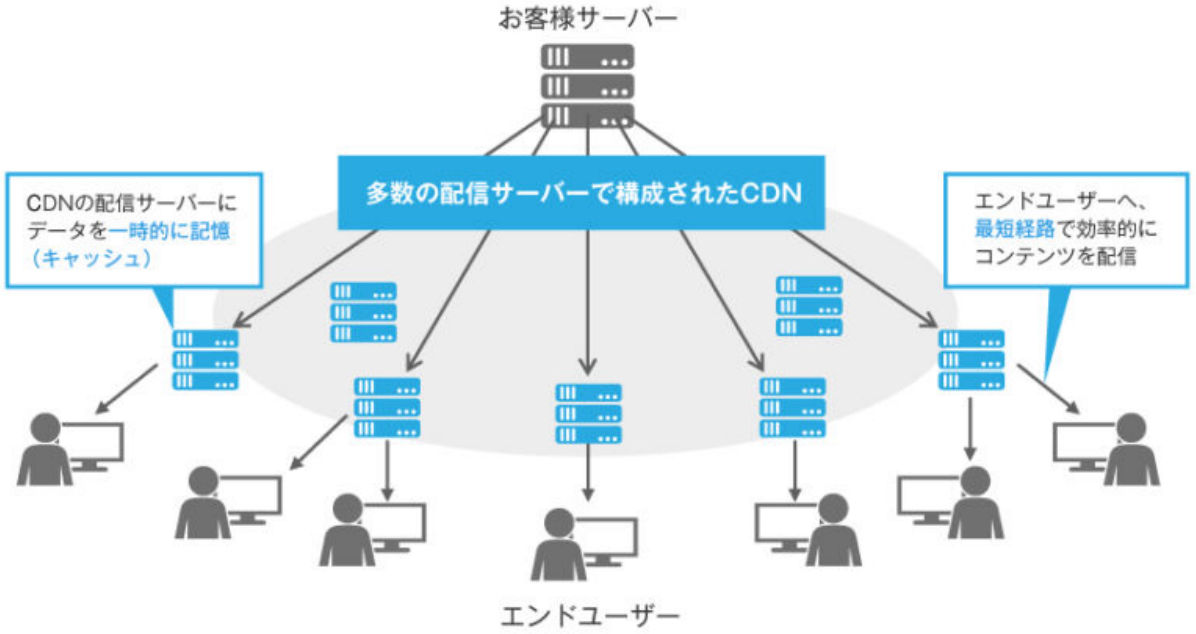
こんなことできるの？

CDNを使えばできます

CDN(Contents Delivery Network)

アクセス数が多すぎて自社でサーバーを賄いきれないサーバーのコンテンツを世界中のサーバーで分散させて表示する仕組みです。

YouTube, NetFlix, AbemaTV



CDNの利用で DDoS攻撃対策

CDNは提供する企業からサービス料金を支払って利用します

- Akamai
- CloudFlare
- Amazon CloudFront(AWS)
- CDNetworks

設定方法

DNSに以下の設定をするだけ

www　CNAME　　xxxxxxxx.cloudflare.com

通常
www A 22.22.22.22

CDN事業者が指定する URL を記載するので**本当のサーバーの情報は外部に公開しない**。

CDN事業者に本当のサーバーのIPアドレスを登録する