福島県警主催「県民をサイバー犯罪被害から守るためのリーダー養成講座」

サイバー攻撃最前線

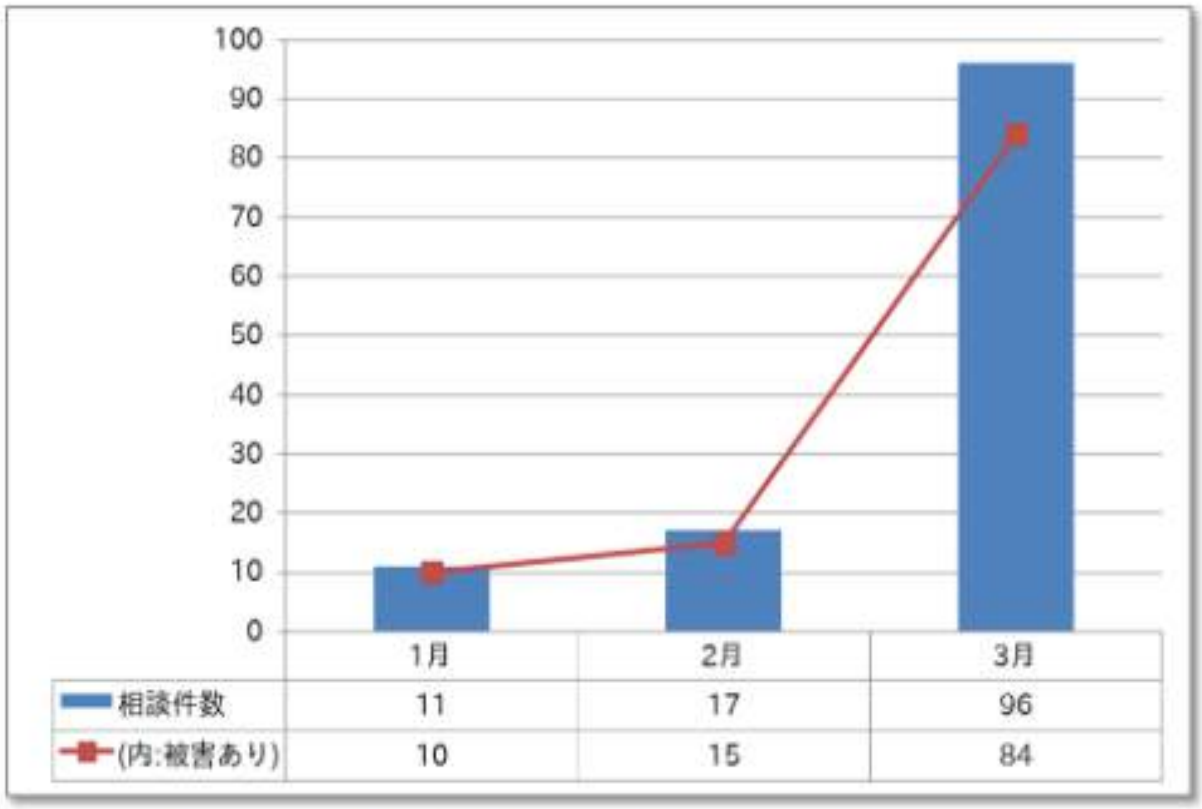
公立大学法人会津大学
特任教授 山崎　文明

ランサムウェア

身代金要求型ウイルス

被害が急増しているランサムウェア

- 2015年FBI被害届2,453件　2,400万ドル（約25億円）
- 日本でも相談件数が急増



	1月	2月	3月
相談件数	11	17	96
(内:被害あり)	10	15	84

図.ランサムウェアに関する相談の月別推移（2016年1月～3月）

【出典】IPA【注意喚起】ランサムウェア感染を狙った攻撃に注意

To Pay or Not to Pay 支払うべきか、支払わざるべきか、それが問題だ！

- 2月5日　米国の病院で電子カルテシステムが使用不能
  - ハリウッド・プレズビテリアン・メディカルセンター（HPMC）
    - ランサムウェア（locky＊1）に感染EMR(電子カルテ)データが暗号化
    - 手書きで対応するも限界
    - 10日後に身代金40ビットコイン（約233万円＊2）を支払って暗号鍵を入手
    - システムの復旧に成功

＊1Locky:Word形式の添付ファイルから感染するランサムウェア

＊21BtcBox=¥58,071換算

CEOの賢明な判断？

- **HPMC病院のCEOの判断**
  - **2016年2月16日声明を発表**
    - 大事なことは患者のケアやその品質に何ら影響を与えなかったことである
    - 我々が最初にこの異変に気づいたのは2月5日の夜である
    - 9,000ビットコインや3百40万ドル支払ったとの事実はない
    - 実際に支払ったのは1万7千ドル相当の40ビットコインである
    - 身代金の支払いは最も迅速で効率的な対応であった
    - 2月１５日の朝にはEMRをすべて正常に復旧させた
    - スタッフの献身的な対応に感謝しています

HOLLYWOOD
PRESBYTERIAN
MEDICAL CENTER

February 17, 2016

I am writing to talk to you about the recent cyber incident which temporarily affected the operation of our enterprise-wide hospital information system.

It is important to note that this incident did not affect the delivery and quality of the excellent patient care you expect and receive from Hollywood Presbyterian Medical Center ("HPMC"). Patient care has not been compromised in any way. Further, we have no evidence at this time that any patient or employee information was subject to unauthorized access.

On the evening of February 5th, our staff noticed issues accessing the hospital's computer network. Our IT department began an immediate investigation and determined we had been subject to a malware attack. The malware locked access to certain computer systems and prevented us from sharing communications electronically. Law enforcement was immediately notified. Computer experts immediately began assisting us in determining the outside source of the issue and bringing our systems back online.

The reports of the hospital paying 9000 Bitcoins or $3.4 million are false. The amount of ransom requested was 40 Bitcoins, equivalent to approximately $17,000. The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this.

HPMC has restored its electronic medical record system ("EMR") on Monday, February 15th. All clinical operations are utilizing the EMR system. All systems currently in use were cleared of the malware and thoroughly tested. We continue to work with our team of experts to understand more about this event.

I am very proud of the dedication and hard work of our staff who have maintained the highest level of service, compassion and quality of care to our patients throughout this process. I am also thankful for the efforts of the technical staff as the EMR systems were restored, and their continued efforts as other systems are brought back online.

And of course, I want to thank our patients and community for their continued trust in Hollywood Presbyterian Medical Center.

Thank you.

Allen Stefanek, President & CEO
Hollywood Presbyterian Medical Center

- **カンサス・ハート・ホスピタル**
  - **2016年5月18日ウイルス感染**
  - **身代金支払うも増額要求**

- **身代金を支払っても復元できたケースは５０％程度**

マルウェア作者でも不可能な復元

- **Ranscam**
  - 感染した時点で全てファイル削除

ランサムウェア対策は「データバックアップ」

■ 対策は、こまめなバックアップ

音声読み上げ・文字拡大　Multilingual　携帯サイト　警察署一覧　サイトマップ　検索

警視庁

安全な暮らし　交通安全　相談・お悩み　手続き　事件・事故　警視庁について

トップページ → 安全な暮らし → 情報セキュリティ広場 → 注目情報 → 不測の事態に備え、データのバックアップを！

不測の事態に備え、データのバックアップを！

更新日：2016年9月29日

現在、企業はもちろんのこと、一般家庭でも文書や写真、音楽など様々なデータを、パソコンやスマートフォンなどのコンピュータ製品で管理することが多くなりました。しかし、最近、コンピュータがランサムウェア（コンピュータ・ウイルス）に感染し、データが利用できなくなる事案が発生しています。

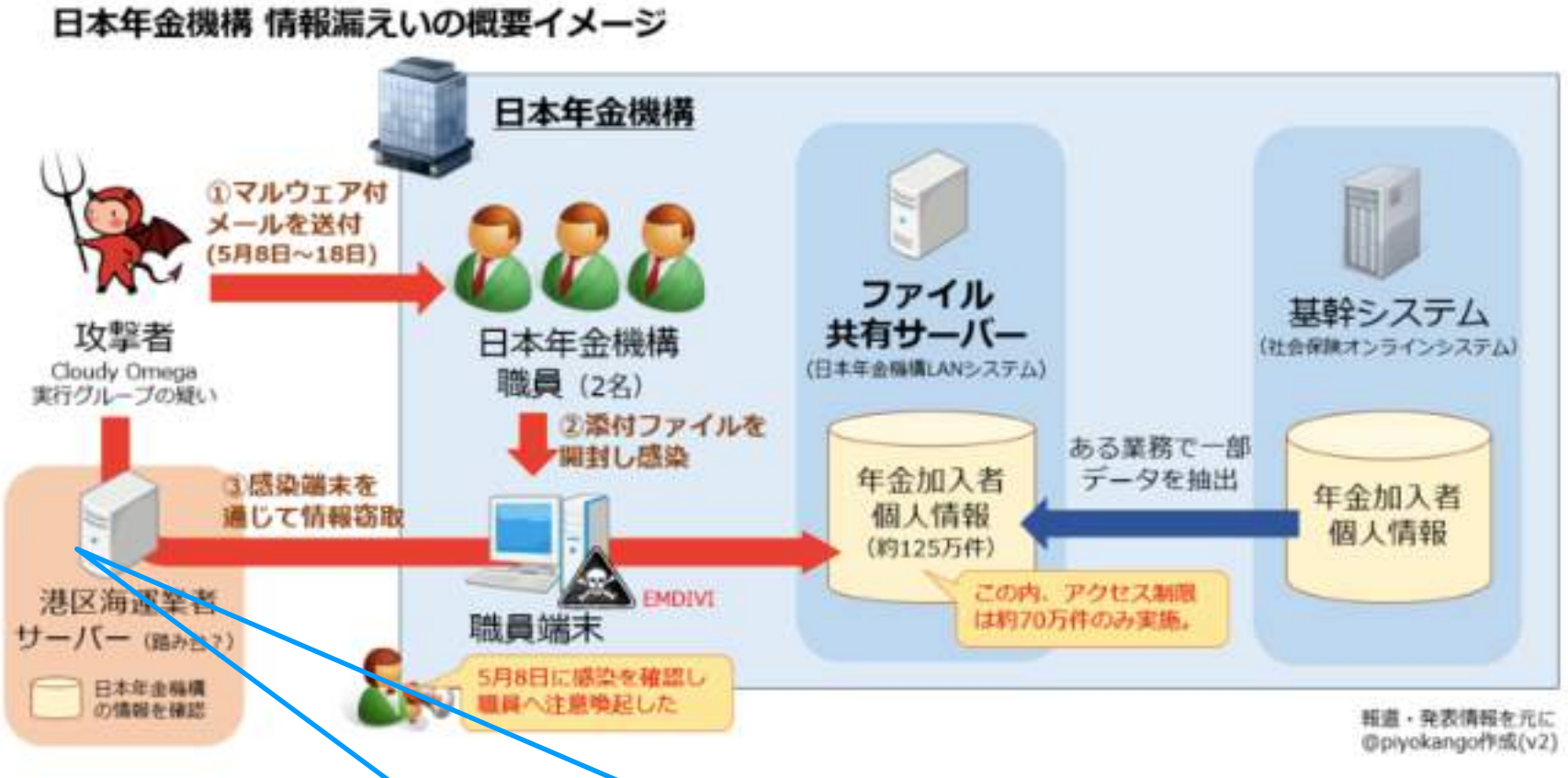
ランサムウェアとは

ランサムウェア（Ransomware）とは、コンピュータ・ウイルスの一種です。ランサムウェアに感染すると、コンピュータ内の画像や文書、場合によっては保存したデータ全てが暗号化され、利用することができなくなってしまいます。この暗号化されたデータは、ランサムウェアを作製した犯人しか元に戻すことができないため、それを盾に犯人は金銭を要求します。この行為が「身代金」を指すRansom（ランサム）の由来となっています

フィシング（偽装）メール

高度な標的型攻撃？

■ **遠隔操作型マルウェア** Backdoor.Emdivi 2012年5月30日



www.summitship.co.jp
125.206.115.79

C&C サーバー（Command & Control Server）

ゼロデイ攻撃（ZERO-day Attack）

■ ゼロデイ攻撃とは

ソフトウェアの脆弱性（セキュリティホール）を標的とした攻撃のうち、脆弱性が発見されてから、開発者によって修正プログラムなどの対策が提供されるまでの時間差を利用して行われる攻撃のことである。

【出典】IT用語辞典

【出典】https://direct.fujixerox.co.jp/ap1/sc/beat/ja/trend/031318.html

一太郎の脆弱性を悪用した不正なプログラム

- **一太郎の脆弱性を悪用した不正なプログラムの実行危険性について**
- 公開日：2014年11月13日
- CVE-2014-7247　CVSS 9.3
- **概要**

  弊社ジャストシステムの一部製品に脆弱性の存在を確認いたしました。この脆弱性が悪用されると任意のコードが実行され、パソコンが不正に操作される危険性があります。この問題の影響を受ける製品と、その対策方法、回避策を以下にご案内いたしますので、ご確認の上、ご対応をお願いいたします。

- **脆弱性の内容**

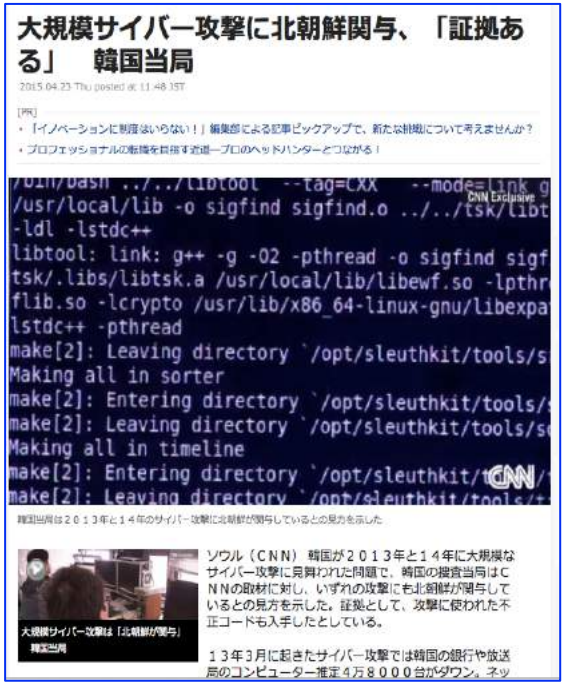
  今回の脆弱性を悪用することを目的に改ざんされた文書ファイルを直接開いた場合、悪意のあるプログラムを実行しようとします。

- **脆弱性がもたらす脅威**

  この脆弱性を悪用した攻撃が「成功」すると、悪意のある第三者によってコンピュータを完全に制御されてしまう可能性があります。これにより、悪意のある第三者は、不正プログラムのインストール、データの変更や削除など、システム管理者の権限でコンピュータを任意に操作できる可能性があります。

一太郎を最新状態にしていれば
この事件は起こらなかった

問題の本質は同根


大規模サイバー攻撃に北朝鮮関与、「証拠ある」　韓国当局

2015.04.23 Thu posted at 11:48 JST

[PR]
・「イノベーションに制度はいらない！」編集部による記事ピックアップで、新たな挑戦について考えませんか？
・プロフェッショナルの転職を目指す近道―プロのヘッドハンターとつながる！

```
/usr/local/lib -o sigfind sigfind.o ../../tsk/libt
-ldl -lstdc++
libtool: link: g++ -g -O2 -pthread -o sigfind sigf
tsk/.libs/libtsk.a /usr/local/lib/libewf.so -lpthr
flib.so -lcrypto /usr/lib/x86_64-linux-gnu/libexpa
lstdc++ -pthread
make[2]: Leaving directory `/opt/sleuthkit/tools/s
Making all in sorter
make[2]: Entering directory `/opt/sleuthkit/tools/
make[2]: Leaving directory `/opt/sleuthkit/tools/s
Making all in timeline
make[2]: Entering directory `/opt/sleuthkit/t
make[2]: Leaving directory `/opt/sleuthkit/tools/t
```

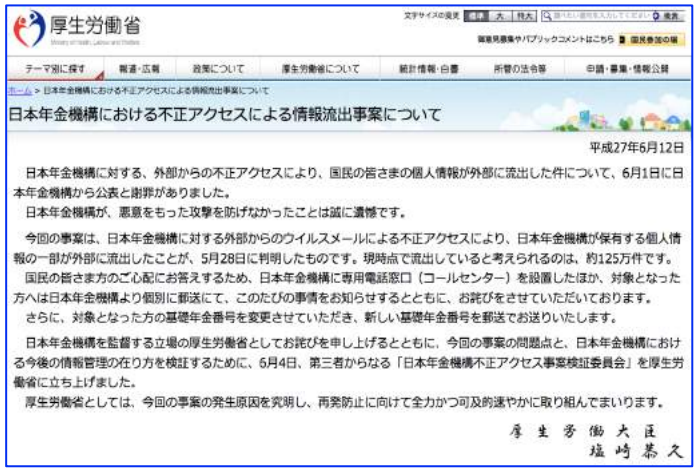
韓国当局は２０１３年と１４年のサイバー攻撃に北朝鮮が関与しているとの見方を示した

大規模サイバー攻撃は「北朝鮮が関与」 韓国当局

ソウル（ＣＮＮ） 韓国が２０１３年と１４年に大規模なサイバー攻撃に見舞われた問題で、韓国の捜査当局はＣＮＮの取材に対し、いずれの攻撃にも北朝鮮が関与しているとの見方を示した。証拠として、攻撃に使われた不正コードも入手したとしている。

１３年３月に起きたサイバー攻撃では韓国の銀行や放送局のコンピューター推定４万８０００台がダウン。ネッ

2013年3月


厚生労働省

日本年金機構における不正アクセスによる情報流出事案について

平成27年6月12日

日本年金機構に対する、外部からの不正アクセスにより、国民の皆さまの個人情報が外部に流出した件について、6月1日に日本年金機構から公表と謝罪がありました。

日本年金機構が、悪意をもった攻撃を防げなかったことは誠に遺憾です。

今回の事案は、日本年金機構に対する外部からのウイルスメールによる不正アクセスにより、日本年金機構が保有する個人情報の一部が外部に流出したことが、5月28日に判明したものです。現時点で流出していると考えられるのは、約125万件です。

国民の皆さま方のご心配にお答えするため、日本年金機構に専用電話窓口（コールセンター）を設置したほか、対象となった方へは日本年金機構より個別に郵送にて、このたびの事情をお知らせするとともに、お詫びをさせていただいております。

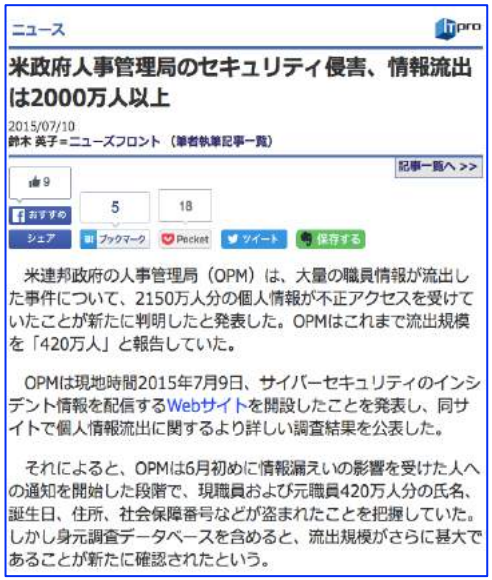
さらに、対象となった方の基礎年金番号を変更させていただき、新しい基礎年金番号を郵送でお送りいたします。

日本年金機構を監督する立場の厚生労働省としてお詫びを申し上げるとともに、今回の事案の問題点と、日本年金機構における今後の情報管理の在り方を検証するために、6月4日、第三者からなる「日本年金機構不正アクセス事案検証委員会」を厚生労働省に立ち上げました。

厚生労働省としては、今回の事案の発生原因を究明し、再発防止に向けて全力かつ可及的速やかに取り組んでまいります。

厚生労働大臣
塩崎恭久

2015年6月


ニュース

米政府人事管理局のセキュリティ侵害、情報流出は2000万人以上

2015/07/10
鈴木 美子＝ニューズフロント（筆者執筆記事一覧）

記事一覧へ >>

9　5　18

おすすめ　シェア　ブックマーク　Pocket　ツイート　保存する

米連邦政府の人事管理局（OPM）は、大量の職員情報が流出した事件について、2150万人分の個人情報が不正アクセスを受けていたことが新たに判明したと発表した。OPMはこれまで流出規模を「420万人」と報告していた。

OPMは現地時間2015年7月9日、サイバーセキュリティのインシデント情報を配信するWebサイトを開設したことを発表し、同サイトで個人情報流出に関するより詳しい調査結果を公表した。

それによると、OPMは6月初めに情報漏えいの影響を受けた人への通知を開始した段階で、現職員および元職員420万人分の氏名、誕生日、住所、社会保障番号などが盗まれたことを把握していた。しかし身元調査データベースを含めると、流出規模がさらに甚大であることが新たに確認されたという。

2015年7月


トップ　社会　政治　経済　国際　サイエンス　スポーツ　オピニオン　カルチャー　ライフ　教育

総合　事件・事故・裁判　気象・地震　話題　皇室　訃報　人事　東日本大震災

[PR]　『セサミンＥＸ』を、お得に試せるモニター募集！

ＪＴＢ情報流出

また「標的型メール」　巧妙偽装、防げず

関連ニュースはこちら

毎日新聞 2016年6月14日　21時55分（最終更新　6月15日　02時58分）

English version

社会　話題　速報

記者会見を終え、頭を下げるＪＴＢの高橋広行社長（中央）ら＝国土交通省で２０１６年６月１４日午後６時１７分、小出洋平撮影

旅行業界最大手で約７９３万人分の情報が流出した恐れが発覚した。流出の可能性がある情報には個人のパスポート番号なども含まれており、客からは不安の声が漏れる。「標的型メール攻撃」と呼ばれる今回の手口は、これまで多くの企業や団体が被害に遭っているが、解決に至らないケースも多く、事件の捜査は難航する可能性がある。

「お客様や関係者にご迷惑、ご心配をおかけし、おわびします」

2016年6月

アンチウルス技術の変遷と日本の弱点

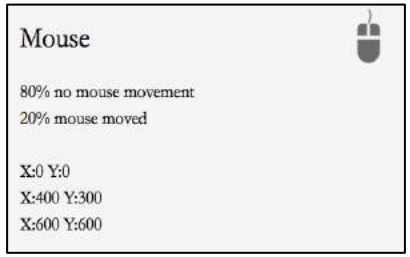
パスワード付きZip
日本の圧縮技術.lzh
サンドボックスOSの言語判定

White List

王道のソリューション
セキュアOS
Data Centric Security

第二世代Sand Box

フルエミュレーション環境



第一世代Sand Box

疑似環境を見破るウイルスの登場
5秒ルール

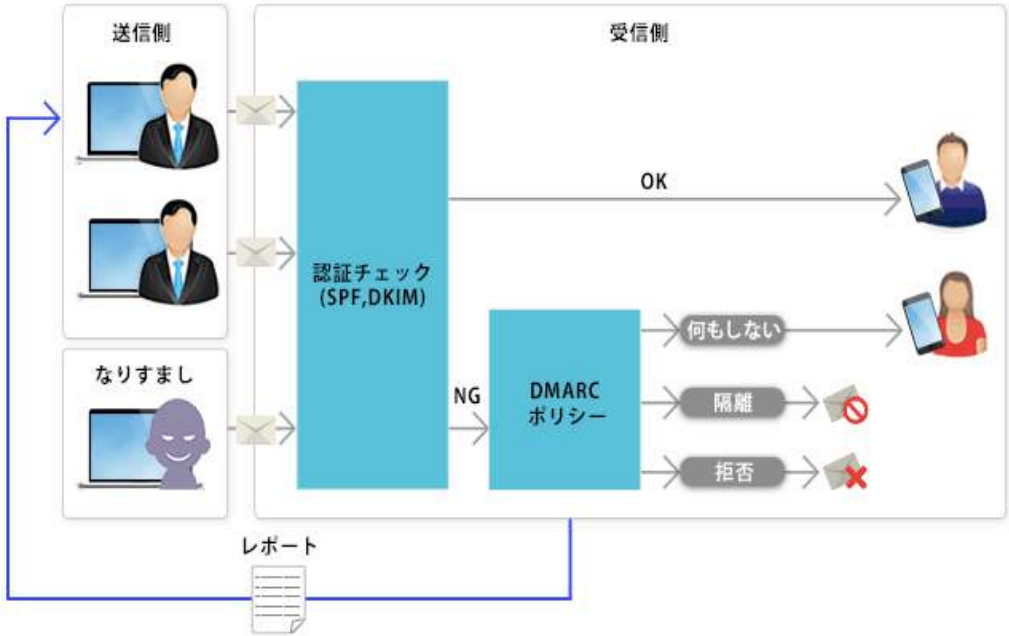
Black List

月間1000万種類の亜種の出現
ブラックリスト方式の限界の露呈

日本国内のC&Cサーバの
IPアドレスはほとんど無視

そもそも偽メールが届かない仕組み構築

- **DMARC（Domain-based Message Authentication, Reporting & Conformance）**
  - 米国を中心に急速に広まっているメールの判別システム
  - 率先導入してその成果を公表しましょう

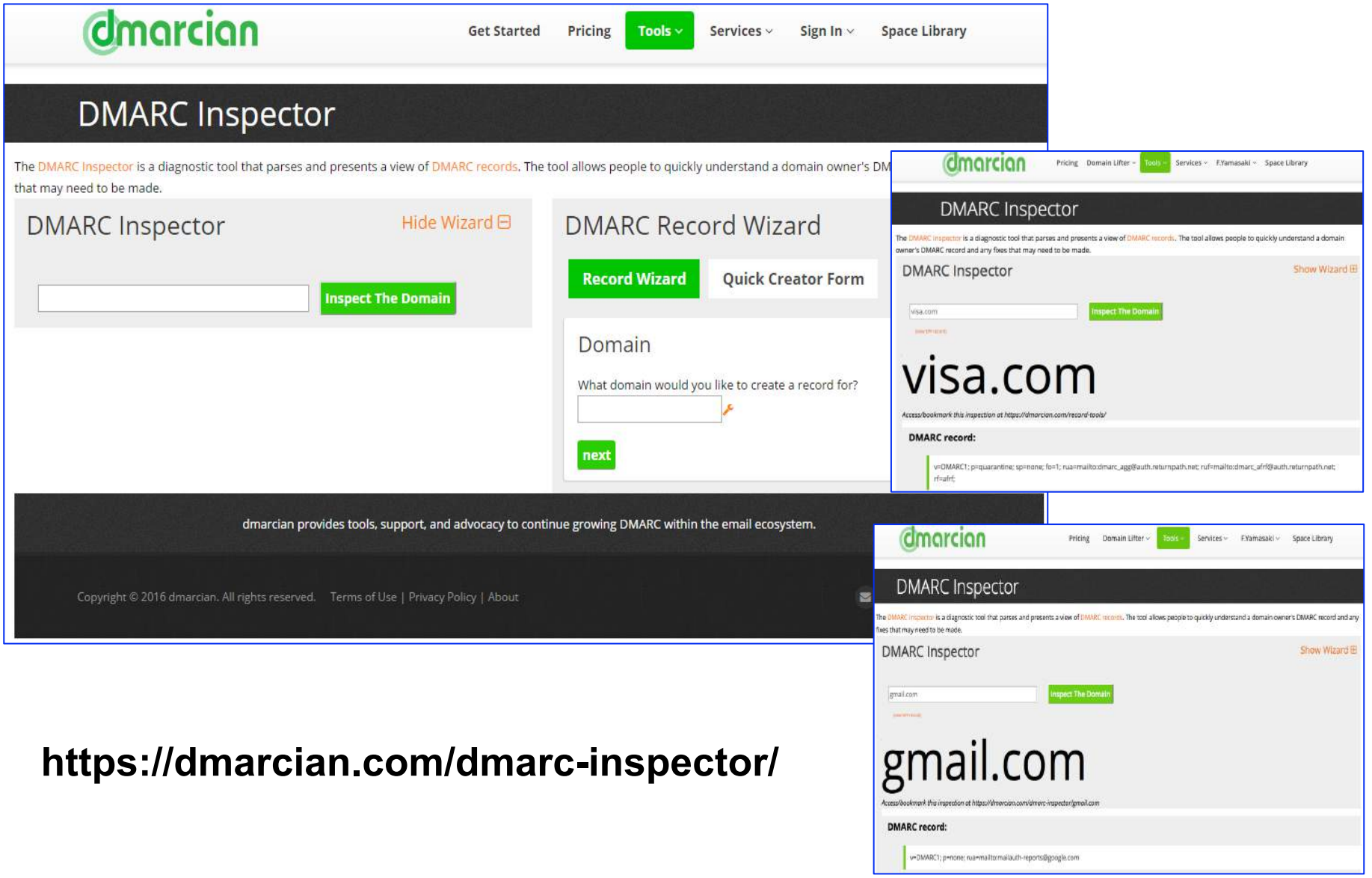


SPF（Sender Policy Framework）
送信元のIPアドレスが送信者名と整合するか確認する仕組み

DKIM（DomainKeys Identified Mail）
電子メールに電子署名を行なって詐称を防止する仕組み

【出典】http://www.cuenote.jp/library/marketing/dmarc.html

DMARC対応しているか調べることができるサイト

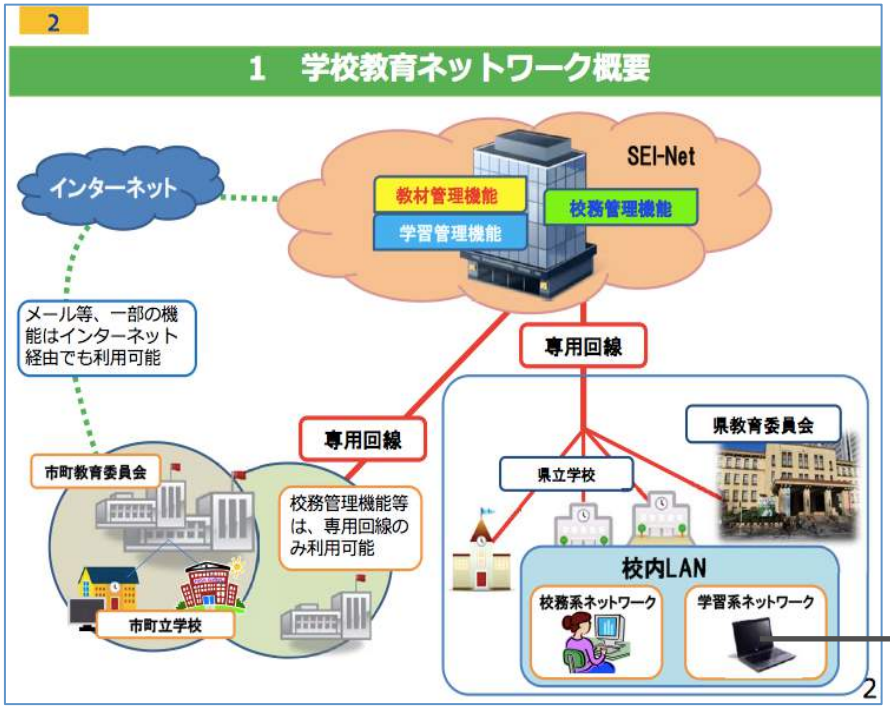


https://dmarcian.com/dmarc-inspector/

内部犯行

佐賀県学校教育ネットワーク侵害事件

- 容疑者は17歳無職少年
  - 複数の在校生と情報交換
  - 動機はセキュリティの脆弱性の指摘、学校への怨嗟



2016年7月28日「2020年代に向けた教育の情報化に関する懇談会」（第5回）
佐賀県提出資料「学校教育ネットワークの不正アクセス事案について」

アクセスポイント　WAP2.0
WAP2.0:Wireless Application Protocol 2.0

-演者補足-

佐賀県学校教育ネットワーク侵害事件

- 17歳無職少年のWiFiへのアクセス
- 在校生による先生へのフィシング
  - パスワードの入力を促すフィシング画面の作成
- 学習用サーバにMACアドレス確認ができる管理者ID、パスワードが蔵置
- 学習用サーバに「kanriID」が存在
- 教職員用テストアカウントが存在
- 学習用サーバへのパスワードから校務用サーバへのパスワードの推測が可能

2015年2月管理者用ID、パスワード盗取

繰り返される類似事件

■　工業高校の個人情報流出問題で校長ら7人を訓告

卒業生304人の進路指導部内のパソコンに保存されていた氏名や成績、進路先、他校の卒業生3人の調査書の内容がインターネット上に流出した。
パソコンには教職員が使うパソコンとLANで接続されていたほか、生徒が使う教育用パソコンともLANで結ばれていた。そのため、生徒も自由に見ることができた。 流出したデータは、自習中の男子生徒が自分のホームページに転送した情報だった。情報管理の責任者である校長と進路指導部の情報管理の責任者である男性教諭を文書による訓告。2人の教頭や総括事務長など5人の教職員を文書や口頭による訓告の処分とした。また、情報を転送した男子生徒に対しては、校長による指導が行われた。

■　中学校で生徒が学内ネットワークに不正アクセス

生徒が学内のパソコンネットワークに不正にアクセスし、同級生ら約200人の名前や成績、住所などの個人情報を入手していた。生徒は学内のパソコンから校務用サーバーに、校長の名前をパスワードに使って侵入できることをみつけ、自分の携帯用音楽プレーヤーを接続してデータをコピー。一部を印刷して教頭に示した。本人は「管理の不十分さを指摘したかった」と話しているという。全教職員にパスワードを変更させたほか、生徒が校務用のサーバーにアクセスできないようにした。校長は「私のパスワード管理の不十分さが原因で、統括する者として責任を痛感している」保護者に陳謝した。

教育情報セキュリティのための緊急提言

- 緊急提言のポイント
  - 校務系、学習系システムの論理的分離
  - 情報の暗号化
  - 二要素認証の導入
  - アクセスログの6ヶ月以上の保管
- 教訓
  - 通用しない「学校だからこの程度で良いだろう」
  - むしろ・・・
    - 機微な個人情報の宝庫
    - 何が起こるか分からない環境

教育情報セキュリティのための緊急提言（案）

各教育委員会・学校において、システムの脆弱性に関する事項を中心に、以下の対応を緊急に行うべきことを提言する。

1．情報セキュリティを確保するため、校務系システムと学習系システムは論理的又は物理的に分離し、児童生徒側から校務用データが見えないようにすることを徹底すること。

2．児童生徒が利用することが前提とされている学習系システムには、個人情報を含む情報の格納は原則禁止とし、個人情報をやむを得ず格納する場合には、暗号化等の保護措置を講じること。

3．各学校において情報セキュリティの専門家を配置することが困難な現状を踏まえれば、重要な個人情報を扱う校務系システムは、教育委員会が管理もしくは委託するセキュリティ要件を満たしたデータセンター（クラウド利用を含む）で一元的に管理すること。

4．校務系ならびに学習系システムにおいても、教職員や児童生徒の負担増にならないよう配慮しつつ、二要素認証の導入など認証の強化を図ること。

5．セキュリティチェックの徹底の観点から、システム構築時及び定期的な監査を実施すること。

6．セキュリティポリシーについて、実効的な内容及び運用となっているか検証を行うこと。その際、アクセスログの６か月以上保存、デフォルトパスワードの変更等について確認すること。

7．教職員の情報セキュリティ意識の向上を図るため、全学校・全教職員に対する実践的な研修を実施すること。

8．情報セキュリティの強化の観点から、教育委員会事務局への情報システムを専門とする課・係の設置や首長部局の情報システム担当との連携強化等、教育委員会事務局の体制を強化すること。

【出典】2016年7月28日「2020年代に向けた教育の情報化に関する懇談会」

これからも起こりえる学校を舞台とした事件

- WiFiの無断使用
  - 児童生徒らによるアクセスポイントへの工作
- IDパスワードの公開
  - 児童生徒らによるIDパスワードの教え合い
  - IDパスワードの売買
- 学校に対する怨嗟
  - 個人情報の公開
  - ランサムウェアを使った校務情報の暗号化
  - データ完全消去による授業妨害
- 技術的好奇心からのハッキング
  - 学校サーバーを踏み台にした攻撃

WiFiエンクロージャーボックス

本気で考えて欲しいセキュリティ対策

- 2要素認証は必須

- 漏えいして困る情報は無価値化
  - 本気で暗号化を考える必要がある現実
    - アンチウイルスの検知率は10%程度まで低下
    - サンドボックスもほぼ役に立たない現実
  - クラウドサービスを使うなら暗号化は必須
    - 外部委託しても委託先管理義務は免れられない
    - 外部委託しても暗号鍵は委託元で管理
  - 暗号鍵はハードウェア(HSM)で管理
    - 暗号化の最大の脅威は暗号鍵の消失

２要素認証（2Factor Authentication)

- **What you know**
  - 本人しか知り得ない情報が提示されることで、本人を確認する方法
  - 固定パスワード、母親の旧姓、好きな都市、

- **What you have**
  - 本人しか持っていないものを提示させることで、本人を確認する方法
  - 電子証明書、ワンタイムパスワード、デバイスDNA、SIMカード

- **What you are**
  - 本人そのものを確認する手法
  - 指紋、声紋、アイリス（虹彩）、静脈など生体認証

まとめ

1. 「高度な標的型攻撃」も対策の本質は変わらない
   - 不要なアプリケーションの削除
   - 確実な更新プログラム（修正パッチ）の適用

2. 偽装メールを不可能にするDMRACの普及

3. ２要素認証の導入

4. データの無価値化
   - トークナイゼーション
   - 暗号化