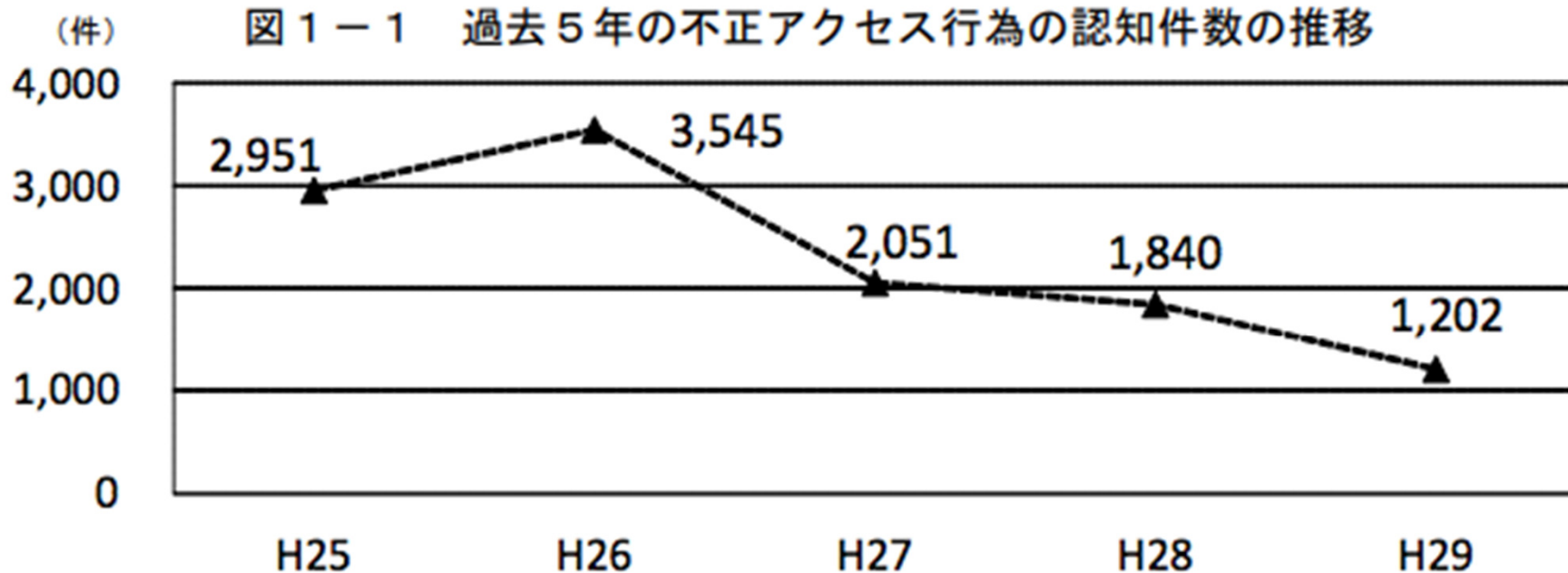


重要インフラに対する サイバー攻撃の脅威と対処方法

2019年2月18日
情報安全保障研究所
首席研究員 山崎 文明

減少傾向にある不正アクセス

平成29年における不正アクセス行為の認知件数^{※1}は1,202件であり、前年と比べ、638件減少した。

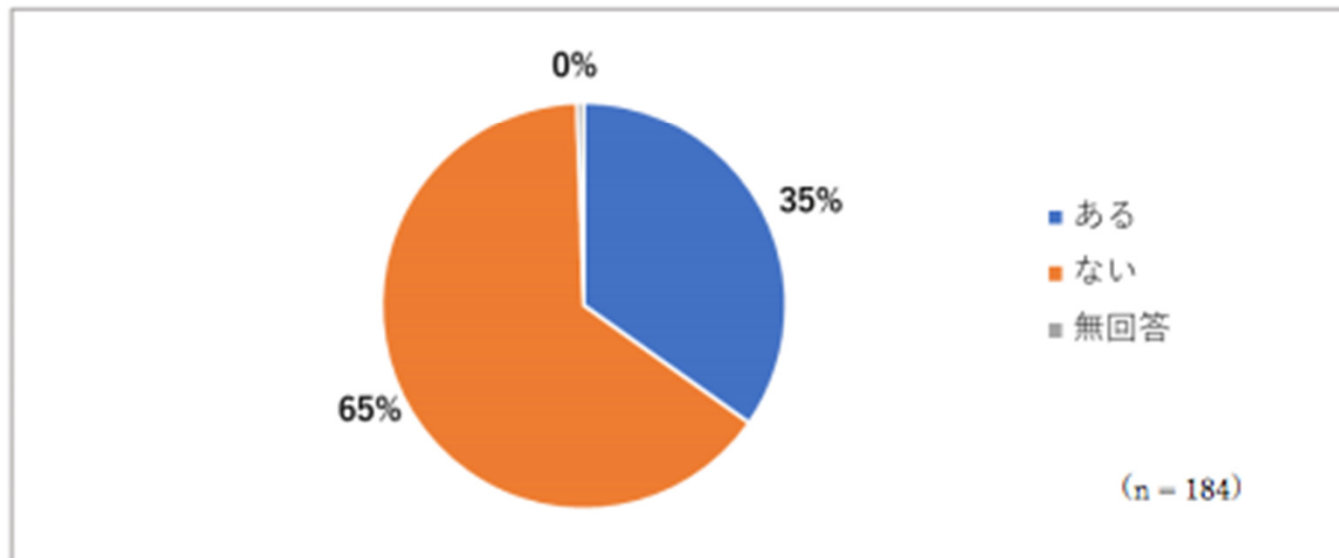


2018年3月22日(平成30年)不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況
国家公安委員会

JPCERT/CCの調査では3社に1社が感染

■ ランサムウェアの被害にあったことはありますか？

調査方法	アンケート調査
調査対象	国内の重要インフラなどの組織
調査期間	2017年9月19日～2017年10月17日
回答組織数	184組織
調査目的	各組織におけるランサムウェアの被害実態や対策などについて状況を把握するために実施



【図 2-3 ランサムウェアの感染被害の有無】

【出典】2018年7月30日 一般社団法人JPCERTコーディネーションセンター

「ランサムウェアの脅威動向および被害実態報告書」

ドイツ鉄道Deutsche BahaがWannaCryに感染

■ 2017年5月

- ✓ 不特定多数を狙った犯行、身代金として\$300を要求
- ✓ ロシアの鉄道会社の感染



日本に向けたウイルスも存在

警告！

71:59:54

あなたの大切なデータは暗号化されてしまいました。
これを修復するためには、\$300相当の支払いが必要です。
制限時間を過ぎると、データは永遠に失われます。

name	location
05月01レポート.doc	C:¥000
05月02レポート.doc	C:¥000
新しいテキスト.txt	C:¥000
201604291230.jpg	C:¥000
課題.xls	C:¥000
課題2.xls	C:¥000

お急ぎ下さい！！

たった\$300でデータは完全に復旧します。
『次へ』から支払い方法を選択して下さい。
制限時間が更新されることはありません。

次へ

奈良県宇陀市立病院でランサムウェアに感染

■ 2018年10月16日午前5時40分頃ウイルス感染

- 医療基幹系システムの初めての感染例

■ 50時間のシステム中断

- 10月18日午前7時復旧

■ 来院患者3,835名の内、1,133名の診療記録が部分的に参照できない事態に

■ 原因はシステム会社の不備により

- 最新のウイルスソフトがインストールされていなかった
- バックアップに必要な磁気テープが装填されていなかった

NHK NEWS WEB

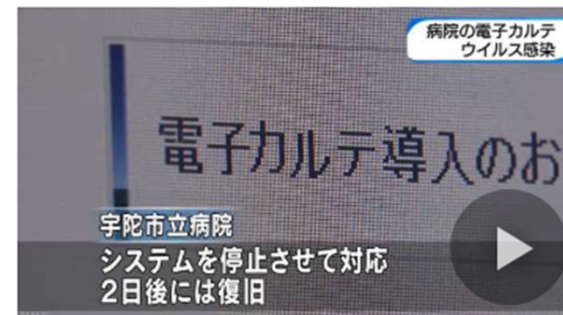
2018年(平成30年)10月24日 水曜日 文字サイズ 小 中 大

関西 NEWS WEB

大阪放送局 トップ

病院の電子カルテ ウイルス感染

10月23日 19時04分



奈良県宇陀市の市立病院で、電子カルテのシステムがコンピューターウイルスに感染し、患者1100人余りの診療記録の一部が開けなくなりました。

病院によりますと、個人情報の流出はなく、現在は平常どおり診療を行っているということです。

宇陀市立病院によりますと、今月16日、電子カルテのシステムが使えなくなったことに職員が気づき、システム会社に連絡したところ、コンピューターウイルスに感染していることがわかったということです。

病院ではシステムを停止させて対応にあたり、2日後には復旧しましたが今月1日から15日までに作成した患者1100人余りの問診でのやり取りの記録に暗号がかけられた状態となっていて開けなくなっているということです。

このトラブルによる個人情報の流出はなく、現在は平常どおり診療を行っているということです。

病院によりますと、システムは今月1日に導入したばかりで、最新のウイルス対策ソフトが入っておらずデータのバックアップも取っていなかったということです。

宇陀市立病院は「市民の皆様にご心配とご迷惑をおかけし大変申し訳なく深くおわび申し上げます」としています。

奈良県宇陀市立病院でランサムウェアに感染

■ GandCrab(ガンドクラブ) V5.02

- ✓ Windows XP、Vista、Windows 7、8、10に感染
- ✓ 頻繁にアップデートを繰り返している
- ✓ 支払いは仮想通貨DUSHで

■ ルーマニアのBitdefender社無償除去ツール公開

- ✓ 10月25日 V1、V4、V5に対応
- ✓ Bitdefender GrandCrab V1,V4,V5 Decryptor
 - <https://labs.bitdefender.com/category/free-tools/>

■ 「無償除去ツール」を騙った有償サイトが多数乱立

- Data Recovery Pro
- GridinSoft Anti-Malware
- Loaris Trojan Remover
- Reimage Repair
- Plumbytes Anti-Malware
- SpyHunter
- WiperSoft

ランサムウェア対策は「データバックアップ」

■ 警視庁はデータのバックアップを推奨

■ ランサムウェアの新しい傾向

- ✓ 復号ツールを使ってもランサムウェアが子供を隠しファイルに作成、しばらくして再暗号化
- ✓ 原則は全システムの上書き

ランサムウェアより恐ろしいドクスウェア

■ doxing(ドクシング)

- ✓ 個人攻撃のためにその人の個人情報をWeb上で公開するいわゆる「晒し」を意味する英語のインターネットスラングである。日本語では「晒し」。

■ Doxware(ドクスウェア)

- ✓ ランサムウェア(ransomware)の反対語。ランサムウェア攻撃では、マルウェアは被害者のデータを暗号化し、支払いを要求して必要な解読鍵を提供する。ドクスウェア攻撃では、攻撃者またはマルウェアは被害者のデータを盗み、手数料が支払われない限り公開すると脅かす。
- ✓ 医療機関では特に警戒を要す

■ 医療機関から漏えいした65万件のデータWebで販売される

- ✓ 2016年6月28日(米国時間)、データ漏えいが発生したのは米国ミズーリ州ファーミントンの医療機関、米国中央/中央西部の医療機関、米国ジョージア州の医療機関で、それぞれ4万8000人、21万人、39万5000人の患者の医療記録データが漏えいしたとされている。

医療機関は支払を拒否。結果として窃取された医療機関データはダークWebで151ビットコイン(1千万円ほど)から607ビットコイン(4千万円ほど)で売りに出され、すでに一部は売買が成立したようだと指摘がある。

DMARC

**Domain-based Message Authentication,
Reporting and Conformance**

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]
・「インベーションに制度はない！」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！

```
bin/bash .././libtool --tag=CXX --mode=link g++ -L../lib -L../usr/local/lib -o sigfind sigfind.o .././tsk/libtool-ldl -lstdc++  
libtool: link: g++ -g -O2 -pthread -o sigfind sigfind.o .././usr/local/lib/libtsk.a .././usr/local/lib/libewf.so -pthread -lcrypto /usr/lib/x86_64-linux-gnu/libexpat.so -lstdc++ -pthread  
make[2]: Leaving directory /opt/sleuthkit/tools/sorter  
make[2]: Entering directory /opt/sleuthkit/tools/sorter  
make[2]: Leaving directory /opt/sleuthkit/tools/sorter  
make[2]: Entering directory /opt/sleuthkit/tools/sorter  
make[2]: Leaving directory /opt/sleuthkit/tools/sorter
```

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



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。ネット

2013年3月クレジットカード会社からの月次明細

厚生労働省
厚生労働省のホームページ

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ますとともに、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適切な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月公開メールアドレス

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] 『セザンヌEX』を、お得意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

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

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」

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 英子=ニュースフロント (筆者執筆記事一覧)

記事一覧へ>>

9
5 18
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 人事部からのメール

2016年6月 電子チケット

メールアドレスにまつわる問題

■ 公開されているメールアドレス

✓ お問い合わせメールアドレス **info@nenkin.go.jp**

✓ 別ドメインとしていれば感染は広がらなかった

info@nenkin.go.jp → **postmaster@info.nenkin.go.jp**

■ 売買されているメールアドレス

✓ セミナー参加申込者のメールアドレス

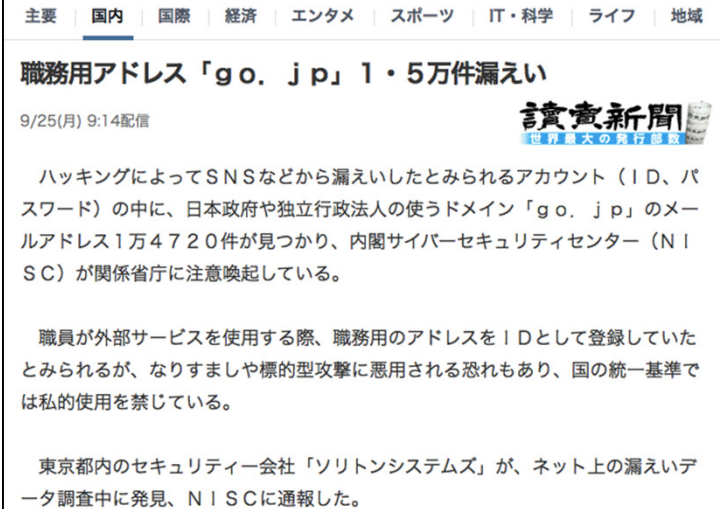
✓ エイリアスの利用

f-yamasaki-seminar@nenkin.go.jp

■ 推測できないメールアドレス体系


✓ **f-yamasaki@nenkin.go.jp**

→ **f-yamasaki89@nenkin.go.jp**



主要 国内 国際 経済 エンタメ スポーツ IT・科学 ライフ 地域

職務用アドレス「go.jp」1・5万件漏えい

9/25(月) 9:14配信 

ハッキングによってSNSなどから漏えいしたとみられるアカウント（ID、パスワード）の中に、日本政府や独立行政法人の使うドメイン「go.jp」のメールアドレス1万4720件が見つかり、内閣サイバーセキュリティセンター（NISC）が関係省庁に注意喚起している。

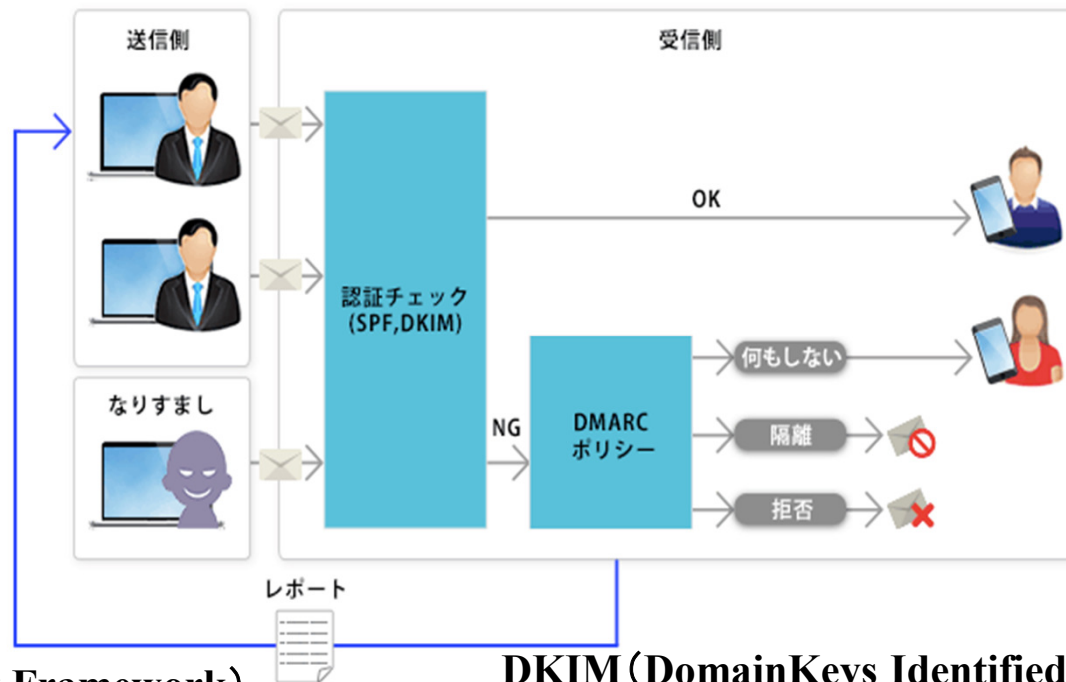
職員が外部サービスを使用する際、職務用のアドレスをIDとして登録していたとみられるが、なりすましや標的型攻撃に悪用される恐れもあり、国の統一基準では私的使用を禁じている。

東京都内のセキュリティ会社「ソリトンシステムズ」が、ネット上の漏えいデータ調査中に発見、NISCに通報した。

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)

- ✓ 2012年1月30日にGoogle、Facebook、Microsoftなどがスパムやフィッシングの脅威撲滅を目的としたワーキンググループ「DMARC.org」を発表
- ✓ 米国や英国を中心に急速に広まっているメールの判別システム



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>

米国や英国では政府主導でDMARC

- 米国の大手クラウドサービス事業者やペイメント事業者が対応済
- 英国政府がサイバー防衛国家戦略として対応済
- DMARCに対応しているか調査できるサイト DMARC Inspector

The image displays several screenshots of the DMARC Inspector website, showing the interface for checking DMARC records for various domains. The interface includes a search bar, a CAPTCHA, and a 'Show Wizard' button. The results for each domain are as follows:

- americanexpress.com**
DMARC record: v=DMARC1;p=reject;fo=1;rua=mailto:dmarc_agg@auth.returnpath.net;ruf=mailto:dmarc_afrr@auth.returnpath.net
- visa.com**
DMARC record: v=DMARC1;p=quarantine;sp=none;fo=1;rua=mailto:dmarc_agg@auth.returnpath.net;ruf=mailto:dmarc_afrr@auth.returnpath.net;rf=afrr;
- gmail.com**
DMARC record: v=DMARC1;p=none;rua=mailto:mailauth-reports@google.com
- gov.uk**
DMARC record: v=DMARC1;p=reject;sp=none;adkim=s;aspf=s;fo=1;rua=mailto:dmarc-rua@dmarc.service.gov.uk;ruf=mailto:dmarc-ruf@dmarc.service.gov.uk
- aol.com**
DMARC record: v=DMARC1;p=reject; pct=100;rua=mailto:d@aol.com;ruf=mailto:d@ruf.aol.com;

BECの被害とDMARCの限界

■ 正規のフリーメールアドレスには無力のDMARC

この企業の社長のメールアドレスから同社の財務担当の幹部に対して送られたものでしたが、日本人同士のメールにも関わらず件名が英語で緊急を意味する「Urgent(ASAP)」となっており、また返信先として指定されているメールアドレスには CEO を想起させる Gmail のアドレスが設定されていました。
このケースでは、社長の正規のメールアドレスから送信されていたため、サイバー犯罪者によって何らかの手法で社長のメールアカウントが乗っ取られていたものと考えられます。 (2017年3月13日トレンドマイクロ)

■ 業務命令にフリーメールアドレスは使用しない

- ✓ 業務連絡には正規メールアドレスで
- ✓ 重要な伝達には電話を使用する

■ 内部統制上、複数者の承認を経て振込を行う仕組みとする

■ 社外から送られてきたメールのFromに自己ドメインを含む場合はブロックする

■ 類似ドメイン名はできるだけ取得する

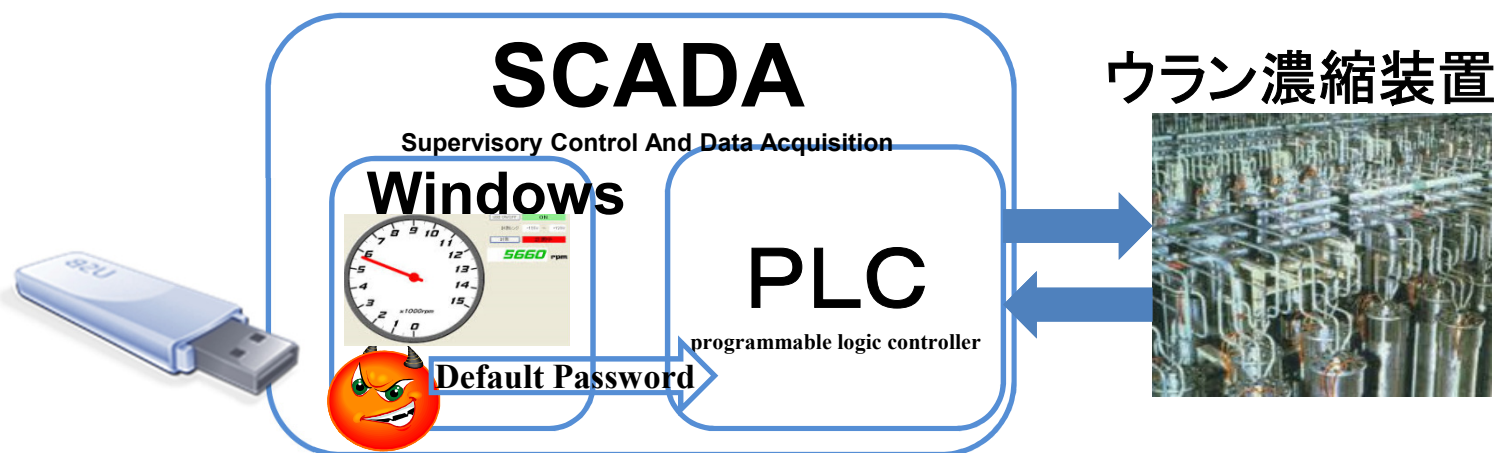
- ✓ yamada@example.co.jp → yamada@example.com yamada@example.net
yamada@exarnple.co.jp yamada@examp1e.co.jp

■ 関係先を騙ったメールはDMARCで拒否

Data Diode

スタックスネット(Stuxnet)は本当に脅威か

- 原因はデフォルトパスワード

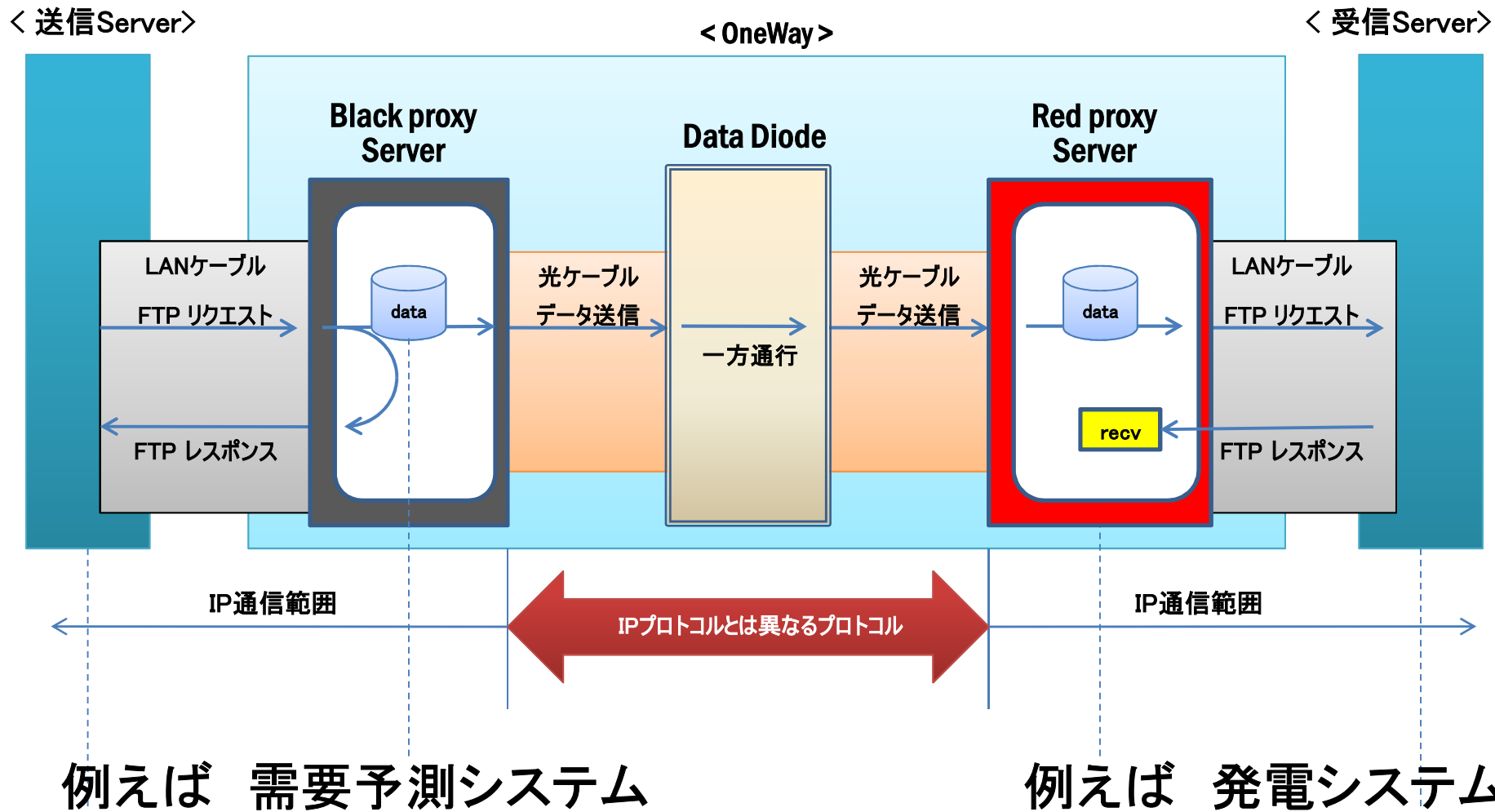


- 真実が語られないウイルスの本質
 - ✓ デフォルトパスワードを使用するウイルス (ワーム: Worm)
 - Voyager Alpha Force/Zotob/My Spooler

普及が望まれるデータダイオード

FTP送信を例にOneWayの構成図

データは左側から右側に一方通行で逆流しないことを保証する高度なセキュリティレベルを実現



【資料提供 SINA】

一方方向ネットワークとデータダイオード



物理切断やファイアウォールよりも合理的なダイオード

■ 確実なセキュリティ

- ✓ 完全な外部ネットワークとの隔離
 - データもコマンドも外部から内部ネットワークに流入することはできない
 - マルウェアのC&C通信も攻撃司令パケット(外部からのAckパケット)が流入できず活動が抑制される
- ✓ 物理的な切断に伴うリスク
 - 情報共有のためにUSBなどの可搬性記録媒体の使用が想定されるが、媒体の盗難、紛失、ウイルス感染などかえってリスクが増加する
- ✓ 設定ミスによる脆弱性誘発がない
 - 設定にミスが発生した場合にも外部から侵入できる脆弱性は発生しない

■ 運用負荷・コスト削減が期待できる

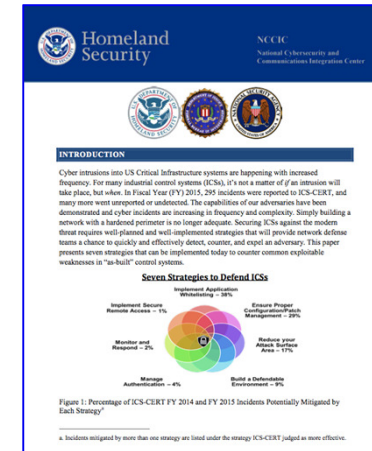
- ✓ アドレス・ポートによるACLやアクセスログ、ユーザアカウントの管理が不要/簡易になることで、運用負荷・コストが軽減される
- ✓ 外部から内部への通信ログが発生しないため、モニタリングの運用負荷・コストが軽減
- ✓ 複雑なファイアウォールの設定がないため、定期的な脆弱性診断コストが軽減される
- ✓ セキュリティドキュメント量を大幅に削減
- ✓ 監査対象の少量化に伴う、外部監査の対応コスト削減

米国連邦政府が推奨するデータダイオード

■ 米国国土安全保障省 制御システムを守る7つの戦略

3. REDUCE YOUR ATTACK SURFACE AREA

Isolate ICS networks from any untrusted networks, especially the Internet.
Lock down all unused ports. Turn off all unused services. Only allow real-time connectivity to external networks if there is a defined business requirement or control function. If one-way communication can accomplish a task, use optical separation (“[data diode](#)”). If bidirectional communication is necessary, then use a single open port over a restricted network path.



■ 米国原子力規制委員会 規制ガイドラインNRC RG5.71

Only one-way data flow is allowed from Level 4 to Level 3 and from Level 3 to Level 2.

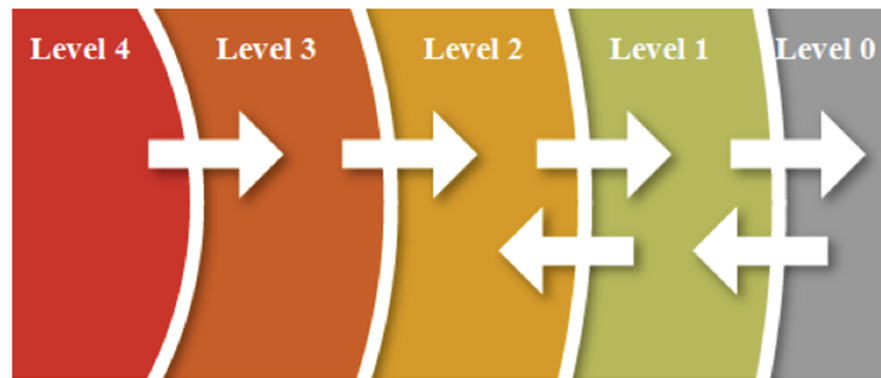
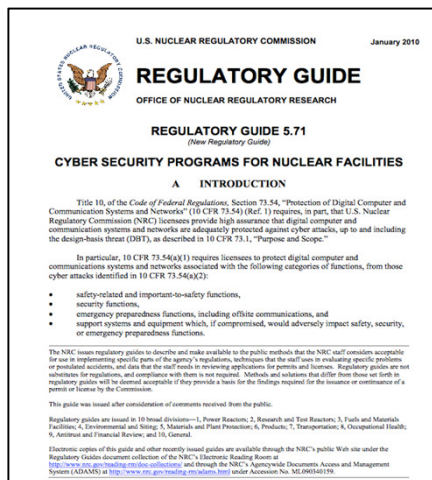


Figure 5 Simplified cyber security defensive architecture

Supply Chain Problem

Chinese Telecom Provider Says “Goodbye to Cisco Gear”

■ 中国最大手ISPがシスコ製品のリプレースを完了 2012年10月

- ✓ China Unicomが思科製品の脆弱性とバックドア(后门)というセキュリティ上の理由でリプレースを進めてきたプロジェクトが完了
- ✓ バックボーン163、169で中国のインターネットのトラフィックの80%を処理
- ✓ 突然の停止(Kill Switch)を警戒



联通更换思科设备：中国运营商开始重视安全

每日经济新闻 2012-10-26 13:44:41 评论(0)条 随时随地看新闻

核心提示：有业内人士指出，思科的产品漏洞及后门问题，正是引发运营商担忧甚至更换其设备的主要原因

继美国因“安全质疑”封杀华为、中兴后，国内通讯运营商也开始加强保护网络安全。

昨日(10月25日)，《每日经济新闻》记者获悉，中国联通近日已经完成对“China169”骨干网江苏无锡节点的核心集群路由器的搬迁工程，而此次被搬迁的正是思科路由器CRS。

对此，有业内人士指出，思科的产品漏洞及后门问题，正是引发运营商担忧甚至更换其设备的主要原因。

思科存安全隐患

据了解，中国电信(微博)163和中国联通169是中国最重要的两个骨干网络，两者承担着中国互联网80%以上的流量。

资料显示，思科目前在中国骨干网拥有超高的市场份额，其占据着中国电信163骨干网70%以上的份额，同时还把持着其所有的超级节点和绝大部分的普通核心节点；思科占据中国联通169骨干网的份额更是达到了80%以上，把持着所有的超级核心节点、国际交换节点、国际汇聚节点和互联互通节点。

近日，中国联通完成了“China169”骨干网江苏无锡节点的核心集群路由器的搬迁工程，这也是通信业界首个思科CRS集群路由器的搬迁工程。

事实上，随着互联网技术的不断发展，网络安全已经日益成为运营商关注的焦点。此前，思科爆出的安全漏洞曾引发运营商的普遍忧虑。

据外媒报道，一位名叫迈克尔·莱恩(Michael Lynn)的ISS公司分析师公布思科路由器存在安全漏洞。

莱恩公布了思科路由器互联网网络操作系统(IOS)中的一处漏洞，并详细描述了通过该漏洞控制路由器的步骤。他指出，思科的IOS和微软的Windows XP一样，都存在着各种各样的漏洞。莱恩发现了一种关闭思科路由器的方法，可以使路由器无法重新启动。“因为只要有人攻击了路由器，他就可以控制整个网络。”他说。

中華人民共和国国家情報法の制定

- 2017年6月26日制定、翌6月27日施行
- 国の情報活動の基本方針、実施体制、情報機関の職権、法的責任について定める
- 第1条 国の情報活動を強化及び保証し、国の安全と利益を守ることを目的とする
- 第7条 いかなる組織及び個人も法に基づき国の情報活動に協力し、国の情報活動に関する秘密を守る義務を有し、国は情報活動に協力した組織及び個人を保護する
- 第9条 国は、国の情報活動に大きな貢献のあった個人及び組織に対し表彰及び報奨を行う
- 第25条 国の情報活動への支援・協力により財産の損失が生じた個人及び組織に対しては国の関係規定に基づき補償を行う

政府の重要インフラ「安全基準等策定指針」今春改定

- 2019年1月17日専門調査会会合開催

- 国内サーバーでの保管を求める
 - ✓ 国際動向も踏まえた望ましいデータ管理
 - ・ 海外のデータセンターに個人情報情報を保管することを禁じる法律を制定する国が大半
 - ✓ インフラ事業者が持つ重要データについては、サイバー攻撃から保護するため、国内サーバーでの保管を求める規定を設ける方向に

もう一つの戦争 Supply Chain Problem

- 特殊作戦ヘリのユニットや海軍のポセイドン偵察機で、空軍のC-130J輸送機で中国からの偽造電子部品発見される(2012年5月米上院軍事委員会報告)

【総括】

「当軍事委員会は2009年から2010年までの2年間に国防総省に供給された兵器を対象とした調査で、合計1800件の偽造電子部品を発見した。この偽造品は部品の個数にして100万点以上となった。これら偽造品の製造元に関して約100件を追跡調査した結果、70%以上が中国であることが確認された。その他の国としてはイギリスやカナダ、[日本も浮上した](#)が、そもそもの製造国から転売された形跡が濃く、ここでも世界の偽造品大国である中国の影が大きい」

- たった10ドルの部品で数百万ドルのミサイルが役立たずになってしまう現実



もう一つの戦争 Supply Chain Problem

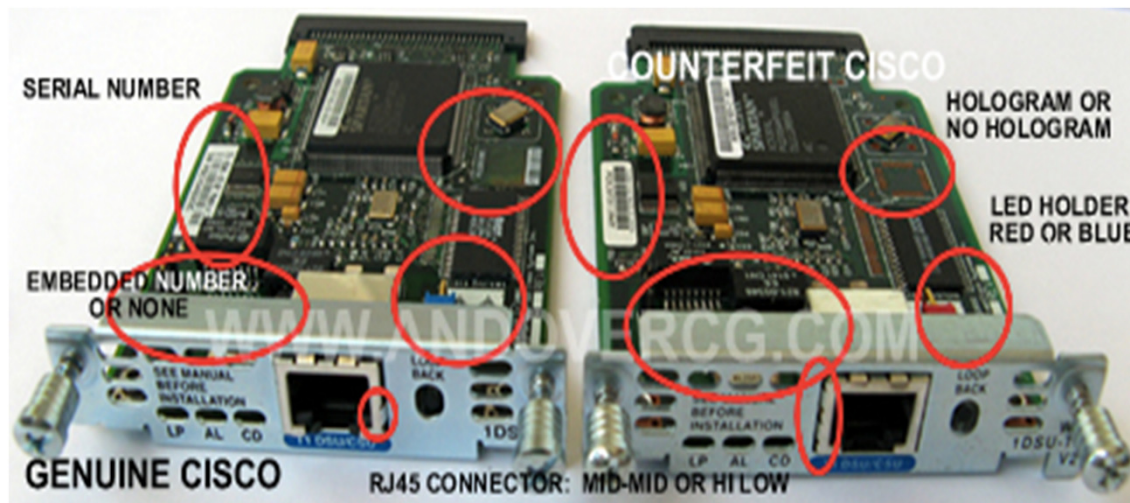
■ 製造・物流にかかわる多くの中国人

✓ 中国国内生産

- 人民解放軍から外資合弁企業へ派遣される社員
- 結成が義務付けられている中国共産党労働組合

✓ 米国国内生産

- 愛国心と金銭による誘惑



Chisco



Michael A. Aisenberg
Principal Cyber
Policy
MITRE

重要インフラ産業の従業員の採用要件

- 米国防総省のクリアランスとポリグラフ検査
 - ✓ Secrete Clearance
 - TS/SCI (Top Secret/Sensitive Compartmented Information)
 - SIGINTや核兵器開発、核開発従事者に求められるクリアランスレベル
 - ✓ ポリグラフ検査
 - 国防総省指令5210.48 国防総省規則5320.48R
 - DoD NSA CIAで義務化

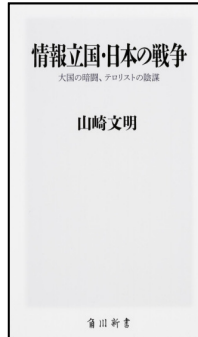


- 我が国でも確立されなければならない民間の採用手続き
 - ✓ 少なくとも複数のリファレンスをとりましょう
 - 大学の複数の教授、ゼミの教授、複数の昔の上司など
- 我が国でも必要なOPSEC教育

求められる経営者の強力なリーダーシップ

- DMARCを国家戦略と位置づけて推進しよう
- データダイオードを普及させよう
- サプライチェーン問題に注意
- 採用手続きに工夫を

自己紹介



山崎 文明(やまさき ふみあき)

情報安全保障研究所 首席研究員

メディカルITセキュリティフォーラム理事

サイバーディフェンス研究会 理事

PCISSC PO Japan 連絡会会長/IT-ADRセンター専門委員

システム監査技術者(経済産業省)/医療情報システム監査技術者/医療情報技師

英国規格協会認定BS7799情報セキュリティ・スペシャリスト/CISM

システム監査、ネットワークセキュリティ、セキュリティポリシーに関する専門家。

【政府関連委員会委員就任歴】

(現任)文部科学賞 教育情報セキュリティ推進チーム 主査

内閣官房情報セキュリティ社会推進協議会 産学官人材育成WG委員

文部科学省「2020年代に向けた教育の情報化に関する懇談会」スマートスクール構想検討WG委員

内閣官房情報セキュリティセンター 情報セキュリティ社会推進協議会産学官人材育成WG委員

内閣官房 安全保障危機管理室 情報セキュリティ対策推進室WG委員

警察庁不正アクセス犯罪等対策専科講師

学校セキュリティ検討委員会委員

経済産業省サイバーテロ実験評価委員

警察庁不正プログラム調査研究委員会委員

警察庁サイバーセキュリティ調査研究委員会委員 他

【加盟学会】

警察政策学会正会員/日本セキュリティ・マネジメント学会正会員/日本安全保障・危機管理学会正会員

【著書】「情報立国・日本の戦争」(角川新書)「PCIデータセキュリティ基準 完全対策」(日経BP社)、「すべてわかる個人情報保護」(日経BP社)、「情報セキュリティハンドブック」(オーム社)、「情報セキュリティと個人情報保護 完全対策」(日経BP社)、「システム監査の方法」(中央経済社)、「コンティンジェンシー・プランニング」(日経BP社)、「セキュリティマネジメント・ハンドブック」(日刊工業新聞社)等。

ADR: Alternative Dispute Resolution 「裁判外紛争解決手続の利用の促進に関する法律」