Internet Week 2018　2018.11.29

実録CSIRT24時！その時なにが起きたか！


原子 拓


まっちゃだいふく


西村 卓也


猪俣 敦夫


齋藤 衡


北村 達也

概要

今回のCSIRTセッションでは、 各業界で活躍されているCSIRT担当の皆さんに登壇いただき、 皆さんが経験された実際のインシデントや業界特有のヒヤリハット事例、CSIRT活動の課題について赤裸々に語っていただきます。発表いただいた事例について各々パネラーの皆さん、 セキュリティ専門家さんとディスカッションをしながらインシデントとインシデント対応、 インシデント予防等の実際を学んでいただきます。 また、最近のIoTやスマートファクトリーなど新たな脅威についてもパネラーの皆さんからコメントをいただきます。

アジェンダ

1. はじめに
2. サイバーセキュリティ動向
3. 事例
   - 事例１　西村卓也さん
   - 事例２　猪俣敦夫先生
   - 事例３　齋藤衛さん
   - 事例４　北村達也さん
4. 新たな脅威に向けて
5. Q&A

アジェンダ

1. はじめに
2. サイバーセキュリティ動向
3. 事例
   - 事例１　西村卓也さん
   - 事例２　猪俣敦夫先生
   - 事例３　齋藤衛さん
   - 事例４　北村達也さん
4. 新たな脅威に向けて
5. Q&A

1．はじめに

■登壇者紹介

①司会、解説

原子 拓

まっちゃだいふく

②パネリストのみなさま

西村 卓也

猪俣 敦夫

齋藤 衡

北村 達也

1．紹介　原子 拓

原子 拓

原子 拓［NCA/ラック］

株式会社ラック
新規事業開発部 事業開発グループ グループマネジャー／日本シーサート協議会 運営委員

1988年 株式会社日立情報ネットワーク入社、日立製作所システム開発研究所にてネットワーク関連の研究開発に従事。
1991年 ヤマハ発動機株式会社入社、情報システム部門にて26年間インフラ・アーキテクチャ全般の企画を担当し、クラウド化、デジタル化を推進。CSIRT構築。
2016年 日本シーサート協議会 運営委員。
2017年 株式会社ラック入社。サイバーセキュリティ関連業務に従事する。

その他、現役消防団員として地域防災活動も行っている。

1．登壇者紹介　まっちゃだいふく

名前：八尾　崇（まっちゃだいふく）
所属：株式会社ラック サイバー・グリッド・ジャパン ICT利用環境啓発支援室
：内閣サイバーセキュリティセンター（NISC）に出向中
経歴：1997年から2008年まで、住友化学システムサービス株式会社に勤務
：　汎用機にて、人事システム設計・構築を担当
：　1万クライアントのインターネット環境構築、ネットワーク再構築の技術担当
：　情報セキュリティの運用・管理・方針策定業務
：　システム技術方針等の部署に所属
：　ERPのバージョンアッププロジェクトにてPMOとして従事
：　2008年から2014年10月までネットエージェントにて、
：　エバンジェリストとして従事
：　営業職として、パートナー営業、プロダクト営業、サービス営業に従事しながら
：　セキュリティコンサルタントとして従事
：2014年11月より、株式会社ラック サイバーグリッド研究所にてリサーチャーとして従事
：2016年04月より、ICT利用環境推進室にて全国で技術系セキュリティ啓発活動を担当
：2017年07月より、京都府警察サイバーセキュリティ戦略アドバイザーを委嘱
：2018年04月より、内閣サイバーセキュリティセンター（NISC）に出向中

1．登壇者紹介　まっちゃだいふく

主な受賞歴：

：Microsoft MVP　12 年連続受賞（2005/10～2018/07 ）
：（ Windows Security -> Consumer – Security -> Cloud and Datacenter Management ）
：Microsoft Insider MVP 2年連続受賞（2016/07～2018/06）
：（ISC）² 6th Information Security Leadership Archivements受賞（2012/07/17）
：CEDEC 2012 ネットワーク部門優秀賞受賞 （共同受賞）（2012/08）
：京都府警生活安全部より、「スマホ時代の子どもを守る 「ALL京都シンポジウム」」協力で感謝状を受賞（2014年）
：京都府警 警察本部長より、京都サイバー犯罪対策研究会の活動で感謝状を受賞（2016年02月）

主な活動：日本全国において、情報セキュリティに関する勉強会を主催、サポートしており、
若手の育成をサポートにも力を注ぐ
2004年より、情報セキュリティに関する勉強会を主催
現在、年に40回の勉強会に参加、毎年延べ2000人以上の技術者との交流を持つ

1．登壇者紹介　まっちゃだいふく

勉強会名	役職
情報セキュリティワークショップ in 越後湯沢	実行委員
情報セキュリティシンポジウム道後 2012	特別協力者
サイバー犯罪に関する白浜シンポジウム	運営委員
名古屋情報セキュリティ勉強会	代表
東北情報セキュリティ勉強会	代表
北海道情報セキュリティ勉強会	立ち上げ・顧問
まっちゃ１３９勉強会（大阪・京都）	代表
まっちゃ４４５勉強会（東京）	立ち上げ、スタッフ
江戸前セキュリティ勉強会（東京）	代表
静岡ITPRO勉強会	立ち上げ、スタッフ
北陸ITPRO勉強会	立ち上げ・顧問
山陰ITPRO勉強会	立ち上げ・顧問
セキュリティうどん（香川）	立ち上げ・顧問
愛媛情報セキュリティ勉強会	立ち上げ・顧問
電子情報通信学会 情報通信システムセキュリティ研究会	専門委員
京都サイバー犯罪対策研究会（京都府警）2014-2016	メンバー

1．登壇者紹介　西村 卓也

西村 卓也

西村 卓也［KADOKAWA］

株式会社KADOKAWA デジタル戦略推進局 事業技術開発部 部長
／日本シーサート協議会会員

1．登壇者紹介　猪俣 敦夫

猪俣 敦夫

猪俣 敦夫［東京電機大学/大阪大学］

東京電機大学／大阪大学／日本シーサート協議会会員

1．登壇者紹介　齋藤 衛

齋藤 衛

齋藤 衛［インターネットイニシアティブ］

株式会社インターネットイニシアティブ セキュリティ本部 本部長／日本シーサート協議会会員

1．登壇者紹介　北村 達也

北村達也［大成建設］

大成建設株式会社 社長室情報企画部 専任部長／日本シーサート協議会会員

1．日本シーサート協議会（NCA）

1 組織概要

- 設立
  - 2007年3月
- 名称
  - 正式名称：日本コンピュータセキュリティインシデント対応チーム協議会
  - 略称：日本シーサート協議会
  - 英語名：NIPPON CSIRT ASSOCIATION
  - ウェブ： http://www.nca.gr.jp/

CSIRT
日本シーサート協議会

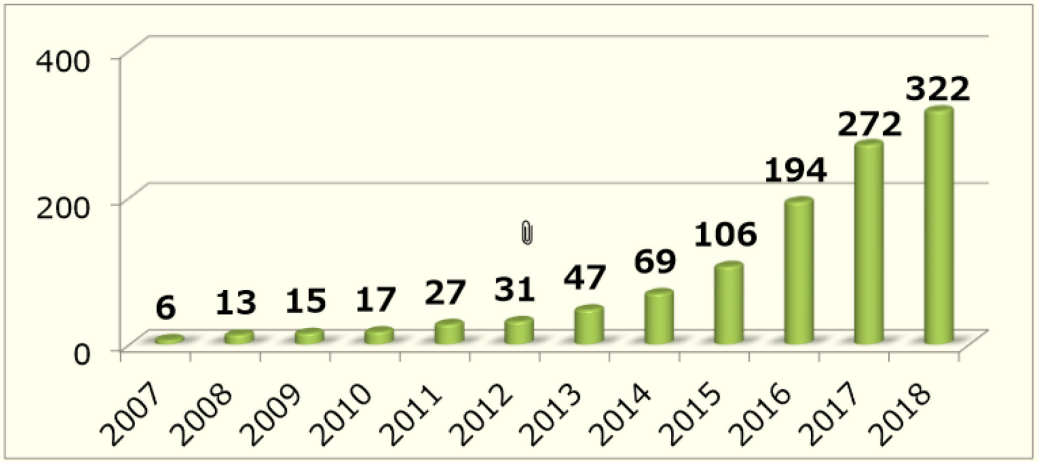
- 使命
  - 本協議会の全会員による緊密な連携体制等の実現を追及することにより、会員間に共通する課題の解決を目指す
  - 社会全体のセキュリティ向上に必要な仕組みづくりの促進を図る

出典 日本シーサート協議会より

1．日本シーサート協議会（NCA）

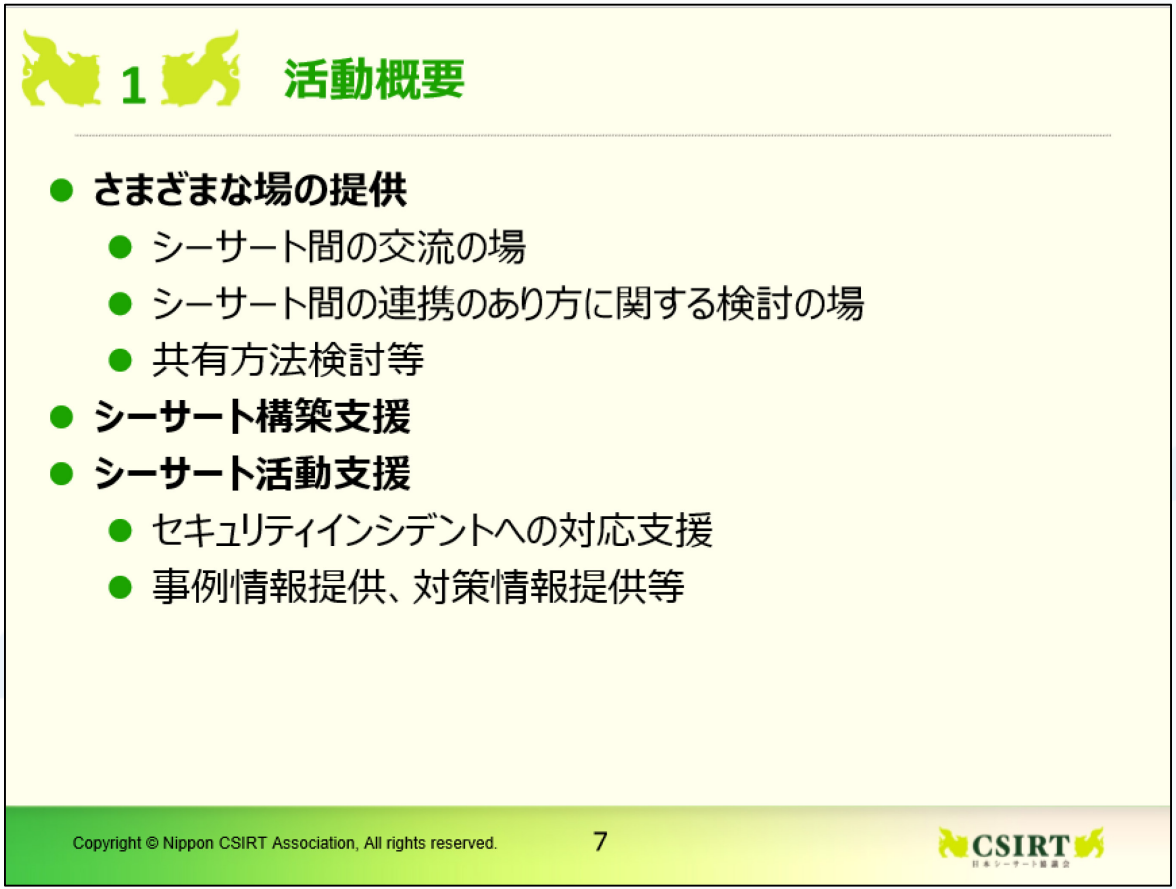
1 日本シーサート協議会加盟数(累積)の推移

- 日本シーサート協議会の加盟チーム数も順調にのび、累積で322チームとなりました(2018年11月現在)



出典 日本シーサート協議会より

1．日本シーサート協議会（NCA）



出典 日本シーサート協議会より

アジェンダ

1. はじめに
2. サイバーセキュリティ動向
3. 事例
   - 事例１　西村卓也さん
   - 事例２　猪俣敦夫先生
   - 事例３　齋藤衛さん
   - 事例４　北村達也さん
4. 新たな脅威に向けて
5. Q&A

サイバーセキュリティ動向

「情報セキュリティ 10大脅威」:2018年版(組織)

1	標的型攻撃による情報流出
2	ランサムウェアによる被害
3	ビジネスメール詐欺
4	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
5	セキュリティ人材の不足
6	ウェブサービスからの個人情報の窃取
7	IoT機器の脆弱性の顕在化
8	内部不正による情報漏えい
9	サービス妨害攻撃によるサービスの停止
10	攻撃のビジネス化（アンダーグラウンドサービス）

～「2018年版 10大脅威 」 https://www.ipa.go.jp/security/vuln/10threats2018.html

サイバー攻撃の目的は？

金銭

不満・怨み

諜報活動

狙われている情報は？

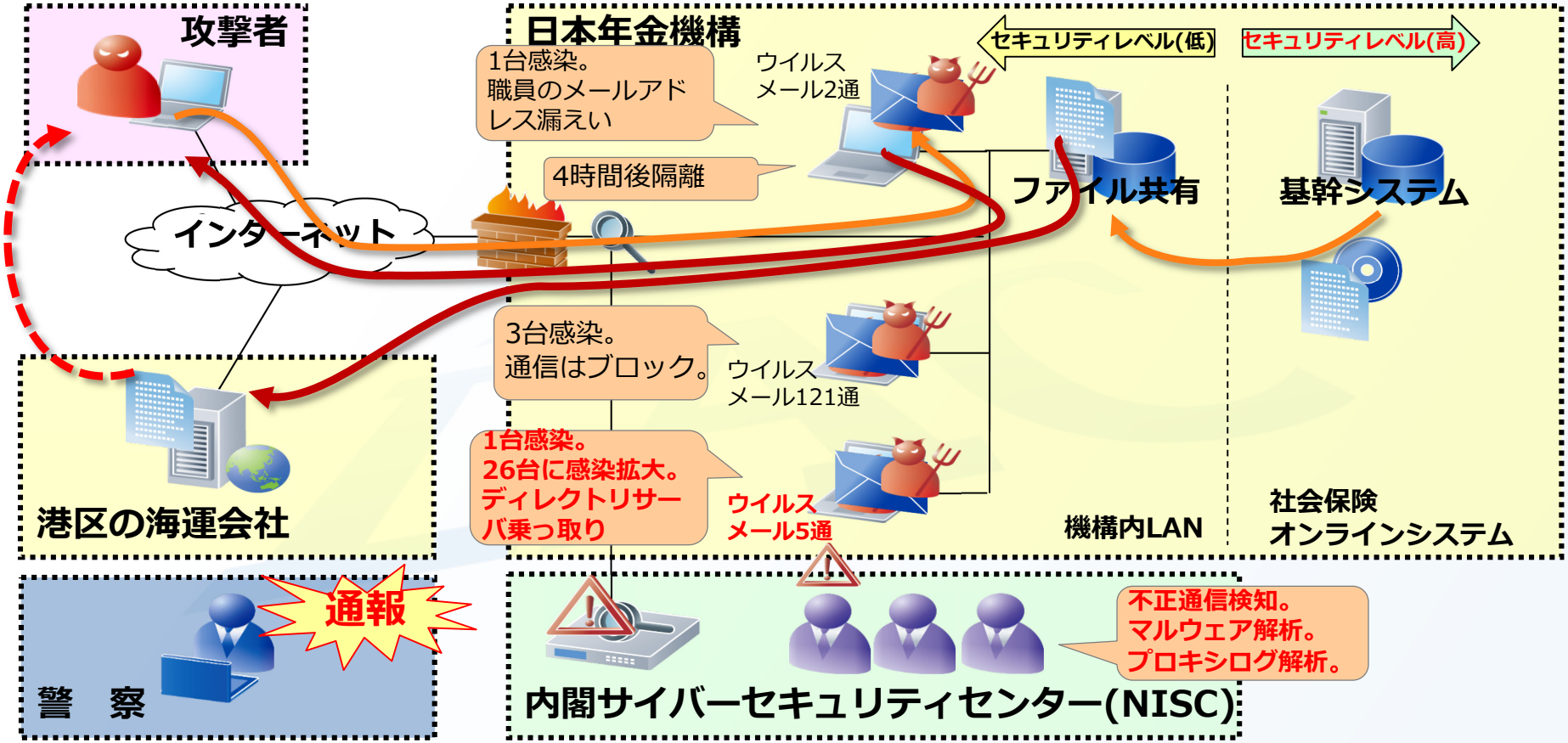
研究

調査

技術

「個人情報」だけが狙われているのではない。外部委託も要注意。

＜事例＞日本年金機構の情報流出事件の流れ



＜事例＞ある組織での「標的型攻撃」の実例

職員Aが、標的型攻撃のメールの添付ファイルを開封。

↓

ウイルスに感染（ウイルス対策ソフトへ検知せず）

↓

PCの中の情報を抜き取られる（メールのアドレスや内容等）

↓

職員Aの名前をかたった標的型攻撃のメールが組織内に送信される

↓

数名が標的型攻撃のメールの添付ファイルを開封。

↓

PCの中の情報を何回かに分けて抜き取られる。（組織の機密情報）

↓

しばらくして、外部からの問い合わせで情報を窃取されたことが発覚。

実は、たった1人の不注意が、きっかけ。

＜事例＞JTBへの標的型攻撃：2016年6月

News & Trend 日経コンピュータ

［詳報］JTBを襲った標的型攻撃

2016/06/15
井上 英明＝日経コンピュータ （筆者執筆記事一覧） 、広田 望＝日経コンピュータ （筆者執筆記事一覧） 、

記事一覧へ

1599 89 128

シェア ブックマーク Pocket ツイート 保存する

ジェイティービー（JTB）が2016年6月14日に公表した、最大で約793万人分の個人情報が流出した可能性がある事案の発端は巧妙に取引先を装った標的型メールだった（関連記事：「流出事実ないがお客様にお詫びする」、793万人の情報流出可能性でJTBの高橋社長が謝罪）。

約4300人分の有効期限中のパスポート番号を含む個人情報が漏洩した可能性のある事案は国内で類がない。同日の記者会見と会見後の取材で分かった経緯を追っていく。

発端は3カ月前の2016年3月15日。旅行商品をインターネット販売する子会社であるi.JTB（アイドットジェイティービー）がWebサイトで公開する、問い合わせを受け付ける代表メールアドレスに、何者かが標的型メールを送り付けた。

2016年3月の標的型攻撃により、約793万件の個人情報が窃取される。

［詳報］JTBを襲った標的型攻撃～日経Itpro,2016年6月15日
http://itpro.nikkeibp.co.jp/atcl/column/14/346926/061500549/

＜事例＞富山大学への標的型攻撃：2016年10月

研究成果や共同研究者ら1492人分の個人情報が流出した可能性。

感染端末は昨年11月～今年6月にかけ、遠隔操作されていた。

富山大学水素同位体科学研究センターに対する標的型サイバー攻撃について
https://www.u-toyama.ac.jp/news/2016/1011.html

ランサムウエア

端末内のファイルの暗号化やロックにより、閲覧・編集・実行をできなくする。その復元や解除のために「身代金(Ransom)」を払うことを要求する機能を持つマルウエア(Malware)

<事例> ランサムウエア被害：2018年7月

2018/07/17 19:04

ニュース

多摩モノレールのランサムウエア被害、データ復旧のめど立たず

岡部 一詩＝日経 xTECH／日経FinTech

日経 xTECH

登録会員限定記事　現在はどなたでも閲覧可能です

多摩都市モノレールは2018年7月13日、社内向け業務システムがサイバー攻撃を受け、ファイルにアクセスできない状態に陥ったと公表した。ランサムウエアに感染したとみられる。7月17日時点でデータ復旧のめどは立っていないという。

被害を受けたのは社内で作成した文書などを管理するファイルサーバーだ。社員の人事情報なども保存しているが、現時点で情報漏洩は確認できていないという。列車の運行管理を担う輸送システムや顧客情報を管理する営業システムなどに被害はなく、サービスへの影響は生じていない。

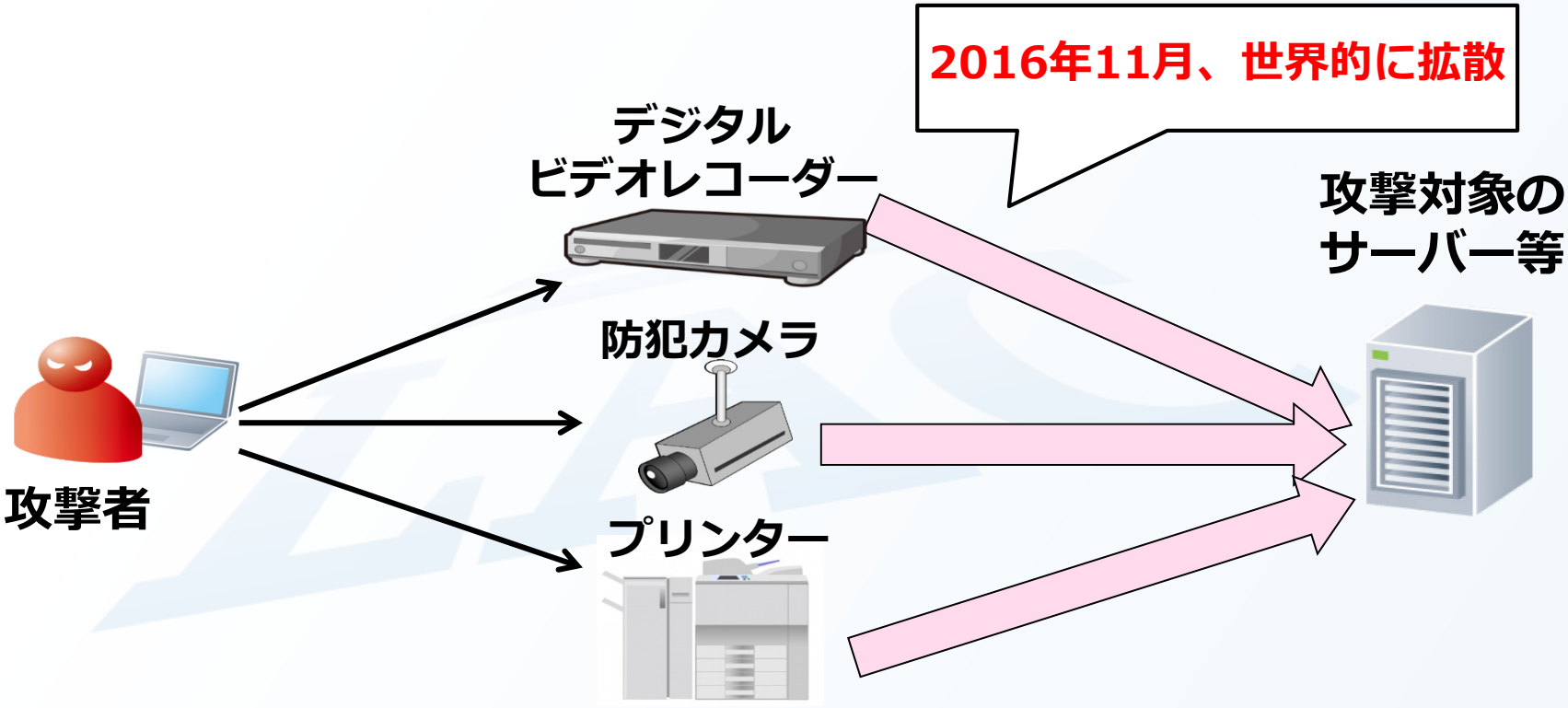
7月9日午後11時ごろ、社員が一部ファイルにアクセスできないことに気付いた。翌10日未明には、同サーバーに格納した全てのファイルにアクセスできなくなった。多摩都市モノレールは9日から10日にかけて、サーバー内のファイルが順次、「ウイルスによって書き換えられた」とみている。

多摩都市モノレールは保守ベンダーを通じて感染経路や詳細な原因を調査しているが、詳細は明らかになっていないという。標的型攻撃による感染も疑われるが、「不審なメールは特になかった」（多摩都市モノレール）という。

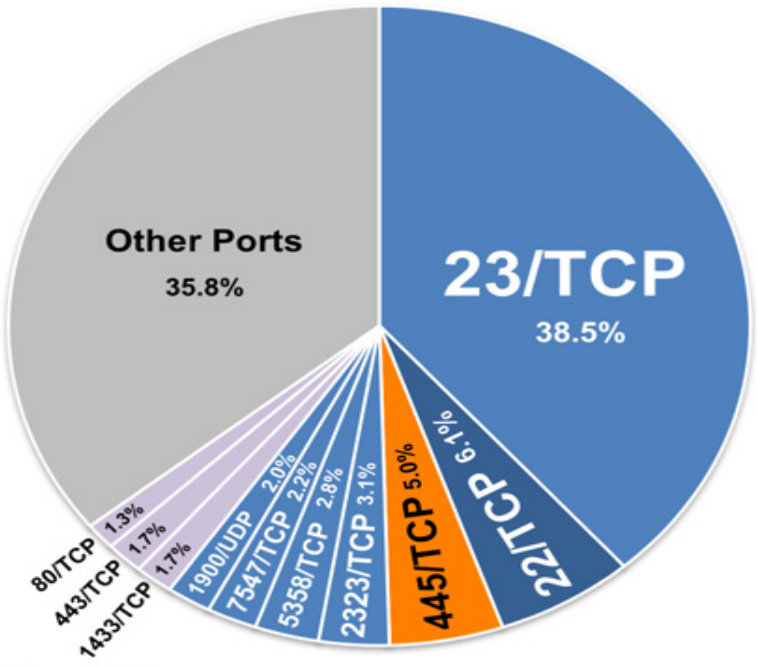
ランサムウエア被害で、多数のファイルが使えず。モノレール運行に影響はなかったものの、復旧に多大な時間を要し、業務に大きな影響。

多摩モノレールのランサムウエア被害、データ復旧のめど立たず
https://tech.nikkeibp.co.jp/atcl/nxt/news/18/01997/

IoT機器への攻撃：IoTウイルス「Mirai」



ますます、狙われるIoT機器



ポート番号	攻撃対象
23/TCP	IoT機器（Webカメラ等）
22/TCP	IoT機器（モバイルルータ等） 認証サーバ（SSH）
445/TCP	Windows（サーバサービス）
2323/TCP	IoT機器（Webカメラ等）
5358/TCP	IoT機器（Webカメラ等）
7547/TCP	IoT機器（Webカメラ等）
1900/UDP	IoT機器（ホームルータ等）
1433/TCP	データベースサーバ（SQL）
443/TCP	Webサーバ（SSL/TLS）
80/TCP	Webサーバ（HTTP）

2017年の攻撃対象への通信TOP10

半数以上がIoT機器をターゲットにした通信。

これらを利用しているのは誰？

「NICTER観測レポート2017の公開」～国立研究開発法人情報通信研究機構、2018年2月27日
http://www.nict.go.jp/press/2018/02/27-1.html

Web改ざん

①「見た目の改ざん」
ページ表記が書き換わる

正規のWebサイト

改ざん

改ざんでマルウエア感染の仕組みを仕掛けている。

②「仕組みの改ざん」
ページ表記は変わらない

＜事例＞学術機関を狙ったWeb改ざん:2017年2月

情報セキュリティ

【注意喚起】学術組織を狙ったウェブサイト改ざんに注意

最終更新日：20
独立行政法人情
技術本部 セ

大学等の学術組織では公式ウェブサイトのほか、研究室やサークル等の単位で独自に開設・運営しているウェブサイトが多数あります。そして、独自ウェブサイトはその役割が終了しても、閉鎖されないことがあります。一方、組織側ではセキュリティ対策の実施体制が十分でなく、個々のウェブサイトを確実に把握・管理できていないと考えられます。

その結果、多くの学術組織において、セキュリティ対策が不十分なウェブサイトが相当数放置されたままであるという状況が、多数のウェブサイト改ざんを招いている主な原因といえます。

学術組織では、研究室単体の情報のみでなく、企業との共同研究などの知的財産といった貴重な情報を保有しています。そのため、ウェブサイトの改ざんを契機に、情報漏えいが一度発生してしまうと、関係組織へのダメージは計り知れません。また、組織の評判に悪影響を及ぼします。

また、ウェブサイトが改ざんされると、閲覧しただけでウイルスに感染させられ、情報漏えいに繋がる可能性もあります(*1)。その他、攻撃のための事前調査と考えられる事例も確認されています(*2)。

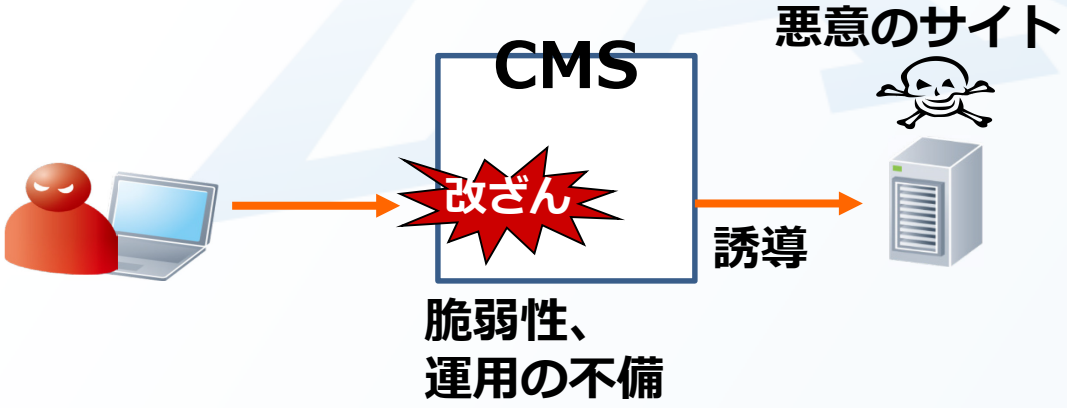
そのため、IPAでは学術組織に向けて、ウェブサイトにおける以下の管理・運用方法を推奨します。

特に、研究室やサークル等が独自に立ち上げたWebサイト。CMSで構築されたものが多数。

https://www.ipa.go.jp/security/announce/academy_website.html#L1

CMSを狙ったWeb改ざん

「CMS(Content Management System)」とは、インターネット上もしくはイントラネット上のWebサイトのコンテンツ(Webページ、テキストや画像など)を統合的に管理し、Webサイトを構築できるシステムのこと。
　運用が簡単なため、Webの知識がなくても利用できる。その運用の不備を突いた改ざんが、近年多発している。



サイバー攻撃被害による影響（手間やコスト）

問い合わせ窓口の設置と運用

原因と影響の調査

ネットワークやシステムの停止による業務効率の低下

代替サービス等の手配

ブランド・イメージの低下

詐欺などによる2次被害

アジェンダ

1. はじめに
2. サイバーセキュリティ動向
3. 事例
   - 事例１　西村卓也さん
   - 事例２　猪俣敦夫先生
   - 事例３　齋藤衛さん
   - 事例４　北村達也さん
4. 新たな脅威に向けて

3．事例

事例１　西村卓也さん

3．事例

事例２　猪俣敦夫先生

3．事例

事例３　齋藤衛さん

3．事例

事例４　北村達也さん

アジェンダ

1. はじめに
2. サイバーセキュリティ動向
3. 事例
   - 事例１　西村卓也さん
   - 事例２　猪俣敦夫先生
   - 事例３　齋藤衛さん
   - 事例４　北村達也さん
4. **新たな脅威に向けて**
5. Q&A

4．新たな脅威にむけて

ディスカッション

アジェンダ

1. はじめに
2. サイバーセキュリティ動向
3. 事例
   - 事例１　西村卓也さん
   - 事例２　猪俣敦夫先生
   - 事例３　齋藤衛さん
   - 事例４　北村達也さん
4. 新たな脅威に向けて
5. Q&A

5．Q&A

ご質問受け付けます

最後に

CSIRT同士の積極的なコミュニケーションを図ることによって、より良いセキュリティ対応を考え、そして、実現していきます。

CSIRT
日本シーサート協議会

http://www.nca.gr.jp/

出典 日本シーサート協議会より

ご清聴ありがとうございました。

LAC
ともに、イキル

昨日の技術は過去のもの。明日の技術は自分の中に。

※ 本資料は2018年11月現在の情報に基づいて作成しており、記載内容は予告なく変更される場合があります。
※ 講演における発言等については、講演者の個人的見解を含んでおり、著作については講演者に帰属します。
※ 本資料に掲載の図は、資料作成用のイメージカットであり、実際とは異なる場合があります。
※ 本資料は、弊社が提供するサービスや製品などの導入検討のためにご利用いただき、他の目的のためには利用しないようご注意ください。
※ LAC、ラック、JSOC、サイバー救急センターは株式会社ラックの登録商標です。
※ その他記載されている会社名、製品名は一般に各社の商標または登録商標です。

株式会社ラック
〒102-0093 東京都千代田区平河町2-16-1
平河町森タワー
Tel 03-6757-0113　Fax 03-6757-0193
sales@lac.co.jp
www.lac.co.jp