増え続けるサイバー犯罪、サイバー攻撃から どのように身を守るか

株式会社カスペルスキー
ビジネスディベロップメントマネージャー 松岡正人

WHO‘S WHO?

松岡正人

株式会社カスペルスキー
ビジネスディベロップメントマネージャー

新潟県長岡市出身の元組み込み含むソフトウェア開発者
長岡工業高等学校電気科卒業
元日本ラショナルソフトウェア（日本アイ・ビー・エム）
元日本マイクロソフト
2012年7月より現職

JNSA IoT Security WG リーダー
VEC 制御システムセキュリティ研究分科会 主査
ICST 2017 Tokyo マーケティングチェア
国立東京工業高専 非常勤講師（情報処理）

※TechFactory “組み込み開発視点で見る「IoTの影」” 連載中
(http://techfactory.itmedia.co.jp/tf/articles/1609/16/news001.html)

KASPERSKY

サイバーリスクを知ろう

リスクを知ることはとても重要
まず、事前に配布した２４項目のリストを確認していきましょう

リスクを知ろう　1/3

1. 私はスマートフォンを使っている
2. 私はフラッシュドライブを使っている
3. 私はタブレットまたはノートPCを使っている
4. 携帯電話、フラッシュドライブ、またはタブレットを不注意に放置することがある（机に置いたまましばらく離れる）
5. 私は家または仕事でデスクトップ PC を使っている
6. 私は銀行口座を持っている
7. 私はモバイルまたは家でインターネットアクセスを使っている
8. 私は家で WiFi を使っている

リスクを知ろう　2/3

9. 私はインターネットバンキングまたはモバイルバンキングを利用している
10.私はソーシャルネットワークのアクティブなアカウントを持っている
11.過去 6か月の間にソーシャルネットワークのパスワードを変更していない
12.過去 1か月の間に怪しいメールやスパムメールを開いたことがある
13.私のスマートフォンにはウイルス対策ソフトウェアがインストールされていない
14.過去 1か月の間に何らかの Web サイトの利用登録をした
15.オンラインでの購入に、クレジットカードでの支払いを利用している
16.過去 1か月の間に、自分の PC またはスマートフォンにアプリケーションやプログラムをインストールした

リスクを知ろう　3/3

17. 過去 1週間で公共の Wi-Fi を利用した
18.スマートフォンの自動パスワードロック機能は使っていない
19.ブラウザーで危険を知らせる警告が出た後も Web サイトにアクセスしたことがある
20.Web サイトの利用登録の際に、1234、qwerty のような単純なパスワードを使った
21.過去 1か月の間に携帯電話、タブレット、または PC を他の人にあげた
22.自分の写真を（インターネット上の）クラウドサービスに保管している
23.家での仕事や出張時の仕事のために、仕事関係の文書をフラッシュドライブやハードディスクにコピーしている
24.オフィスのメールやオフィスのネットワークにリモートでアクセスしている

KASPERSKY

このなかで特に重要なのは以下の六つ

4. 携帯電話、フラッシュドライブ、またはタブレットを不注意に放置することがある（机に置いたまましばらく離れる）

9. 過去 1か月の間に怪しいメールやスパムメールを開いたことがある

10.私のスマートフォンにはウイルス対策ソフトウェアがインストールされていない

17.スマートフォンの自動パスワードロック機能は使っていない

18.ブラウザーで危険を知らせる警告が出た後も Web サイトにアクセスしたことがある

19.Web サイトの利用登録の際に、1234、qwerty のような単純なパスワードを使った

サイバーセキュリティってなんのこと？

そもそもサイバーセキュリティってなんのことでしょう？インフォメーションセキュリティなんて言葉もありますが、何が違うのでしょうか？

サイバーと
インフォメーション

- インフォメーションはサイバー以外も含む（紙など）ので幅広い、サイバーはデジタル世界の一部で、ネットワークやインターネットの一部を含む

※ISO/IEC 27032:2012 参照

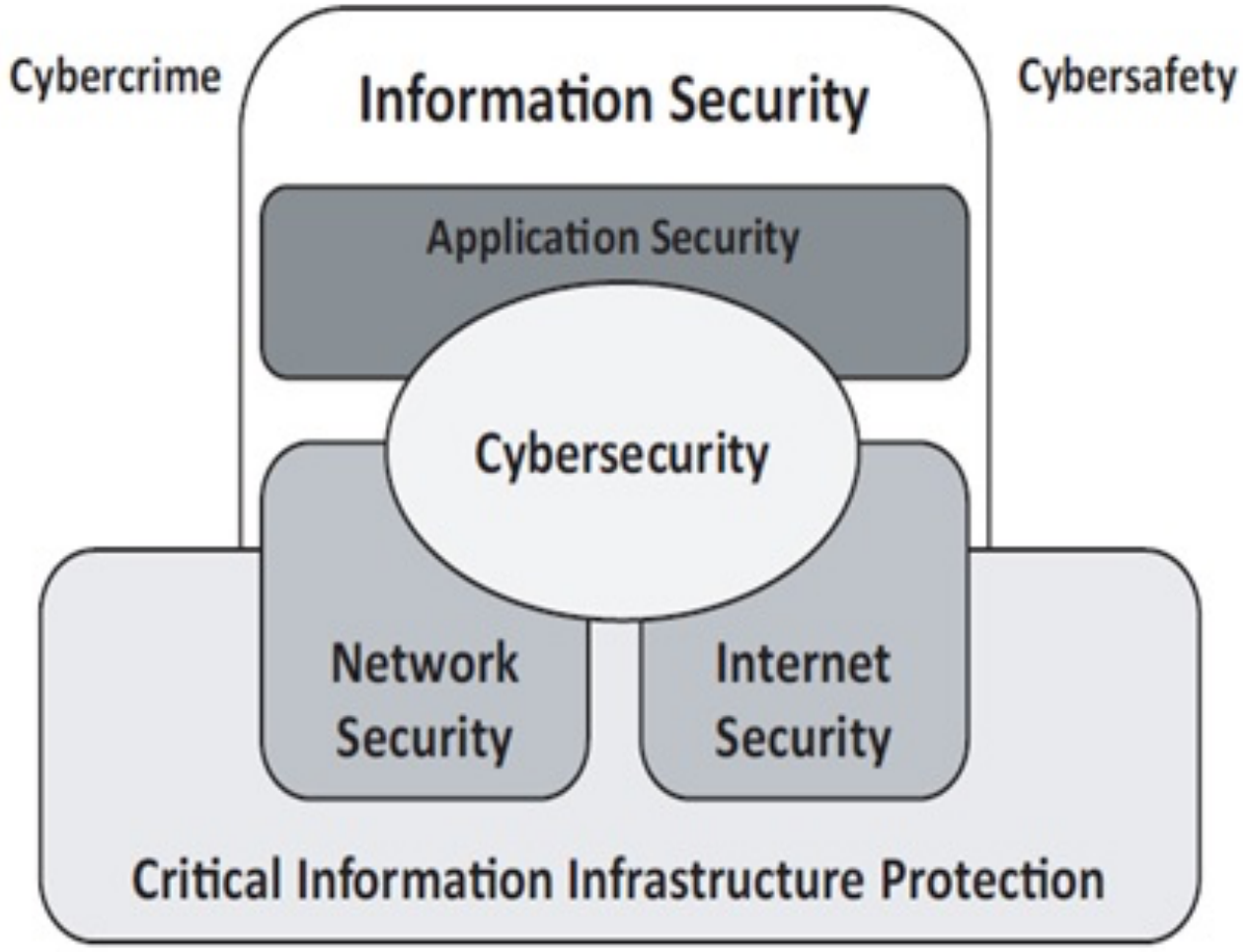


Figure 1 — Relationship between Cybersecurity and other security domains

KASPERSKY

サイバーセキュリティに100万件の求人
平均年収は1000万円超
*2016年

www.forbesjapan.com/articles/detail/10885

KASPERSKY

サイバーセキュリティな仕事を目指す人に
質問：次の言葉は何のこと？

- Wire Tapping（ワイヤータッピング）
- Advanced Persistent Threat（アドバンストパーシステントスレット）
- Ransomware（ランサムウェア）
- Cracking（クラッキング）
- Phishing（フィッシング）

サイバーセキュリティな仕事を目指す人に
質問：次の言葉は何のこと？

- Wire Tapping➔盗聴
- Advanced Persistent Threat➔執拗な標的型攻撃
- Ransomware➔身代金要求マルウェア
- Cracking➔悪意あるハッキング行為
- Phishing➔詐欺

質問：機密情報をやりとりするならどれが安全？

- Line
- Facebook
- Skype
- Twitter
- 電子メール
- TXT（SMS）
- 衛星ネットワーク

KASPERSKY

メールやウェブサイトから侵入しようと試みます

- 偽のメールアカウントからそれらしく送る（スパムです）
- 本物のアカウントを使って送る（激増中）
- 偽の広告
- 偽のウェブサイト（本物と差し替える）
- ファイルに仕込む（メーカーのサイトからダウンロードさせる）
- **最近は携帯電話のSMSやSNSも**

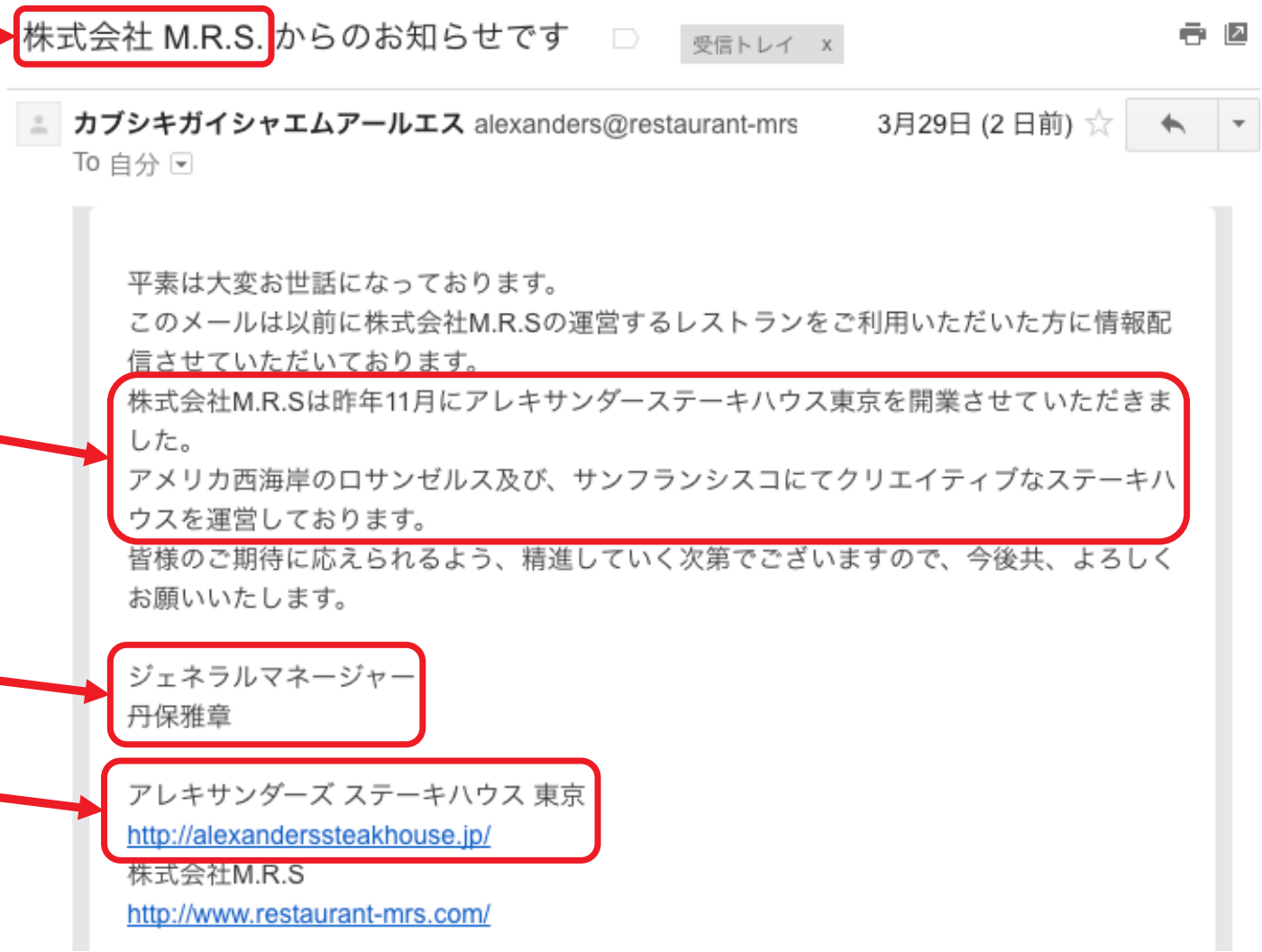
メールをチェックしてみる

こんな会社知らない

ロスもサンフランも行ったけど
シアトルでしか行ってない

誰?

行った記憶がない



メールをチェックしてみる

Singapore Seafood Republic

シンガポール政府おすすめの名店4店が集まり、各ブランドの味を一店でお楽しみいただけます。活きたまま空輸される貴重なマッドクラブがテーブルに。日本では味わうことのできなかった本場のシンガポール・シーフード料理の数々をご堪能ください。

株式会社 M.R.S

カブシキガイシ

ージャー

ズ ステーキハウス 東京

http://alexandersteakhouse.jp/

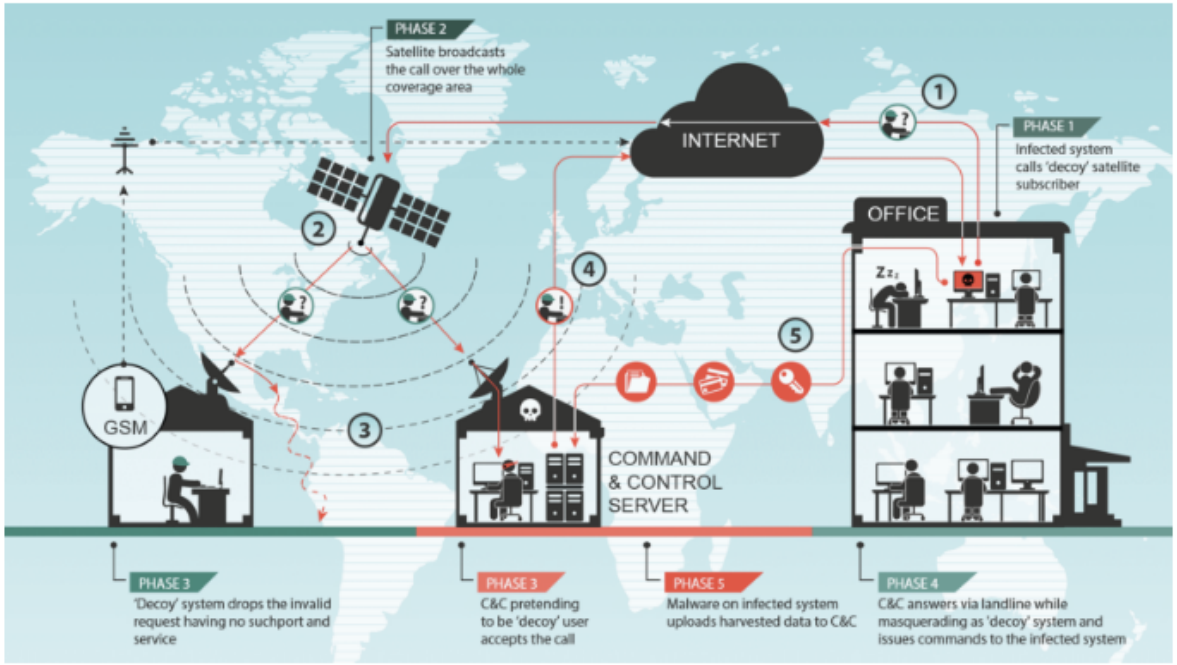
株式会社M.R.S

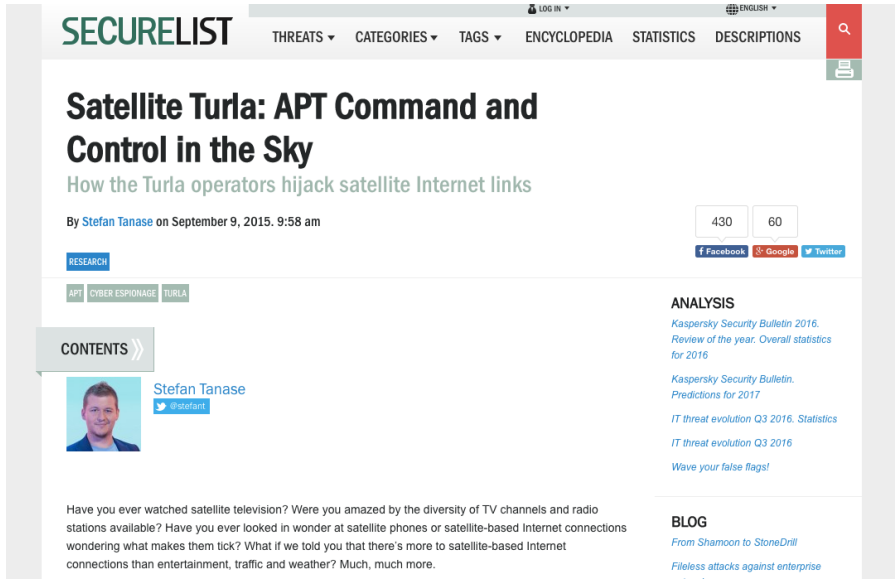
http://www.restaurant-mrs.com/

衛星ネットワークをハイジャック

Turla(2015)

- 衛星通信用チューナーをPCに設置して衛星回線を経由したネットワークに侵入し、攻撃用のサーバーを設置するなど




SECURELIST

THREATS ▾ CATEGORIES ▾ TAGS ▾ ENCYCLOPEDIA STATISTICS DESCRIPTIONS

Satellite Turla: APT Command and Control in the Sky

How the Turla operators hijack satellite Internet links

By Stefan Tanase on September 9, 2015. 9:58 am

430 60

Facebook Google Twitter

RESEARCH

APT CYBER ESPIONAGE TURLA

CONTENTS

Stefan Tanase @stefant

Have you ever watched satellite television? Were you amazed by the diversity of TV channels and radio stations available? Have you ever looked in wonder at satellite phones or satellite-based Internet connections wondering what makes them tick? What if we told you that there's more to satellite-based Internet connections than entertainment, traffic and weather? Much, much more.

ANALYSIS

Kaspersky Security Bulletin 2016. Review of the year. Overall statistics for 2016

Kaspersky Security Bulletin. Predictions for 2017

IT threat evolution Q3 2016. Statistics

IT threat evolution Q3 2016

Wave your false flags!

BLOG

From Shamoon to StoneDrill

Fileless attacks against enterprise

https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/

KASPERSKY

実は、もっと色んなことができます

- スマホのCPUに組み込みました
  http://thehackernews.com/2016/02/mediatek-hacking-mobile.html
- 米軍の兵装にも組み込んでみました
  http://business.nikkeibp.co.jp/article/world/20081015/173843/?rt=nocnt
- USBドライブを使って、強制的にUSBにマルウェアを寄生させます
  http://gigazine.net/news/20141218-usbdriveby/
- これはセキュリティ会社の例、電源アダプターでセキュリティ診断
  http://gigazine.net/news/20120306-little-box-hack-your-network/

質問：2016年のランサムウェア（身代金を要求するマルウェア）の被害額は全世界でどれくらい？

- 約10億円
- 約1000億円
- 約10兆円

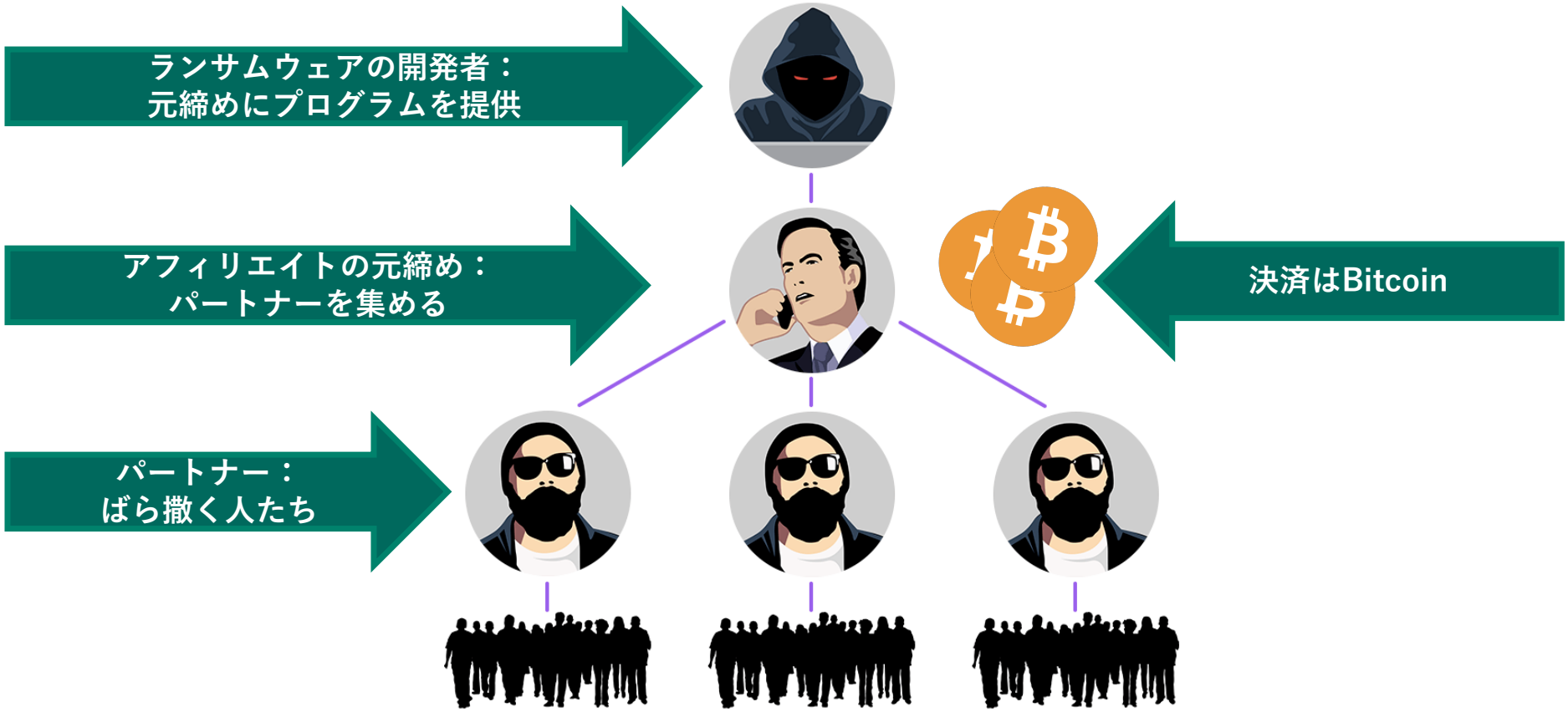
ランサムウェア：パソコンを人質に

- パソコンをロック
- ファイルを暗号化
- 身代金を要求（Bitcoin）

※身代金を支払っても20%は解放されない

https://blog.kaspersky.co.jp/no-no-ransom/13117/

ランサムウェア：言い換えるとネズミ講



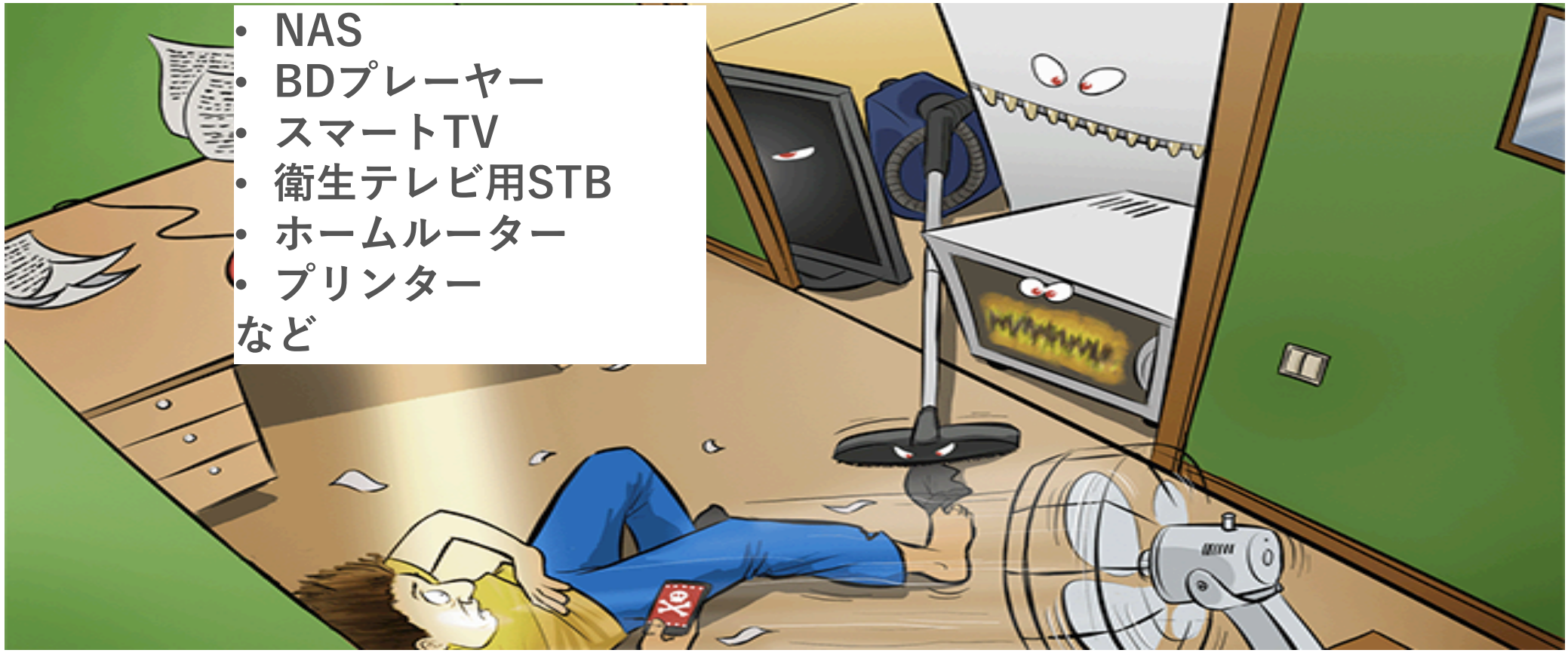
https://blog.kaspersky.co.jp/russian-ransomware/14558/

KASPERSKY

質問：マルウェア感染の危険性があるのはどれ？

- テレビ
- WiFiルーター
- エアコン
- 自動車

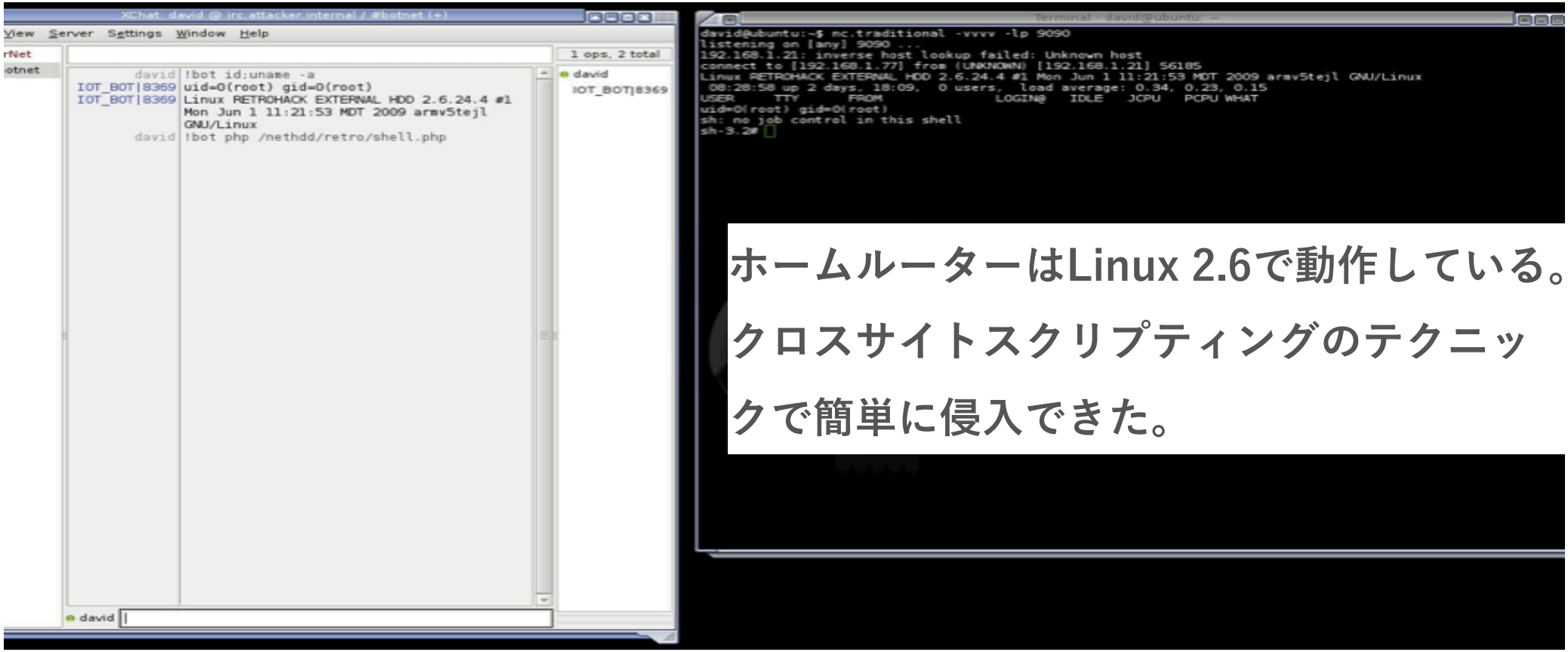
家電は安全なの？



http://blog.kaspersky.co.jp/how-i-hacked-my-home/4617/

KASPERSKY

ルーターに“ボット”を仕込んでみた



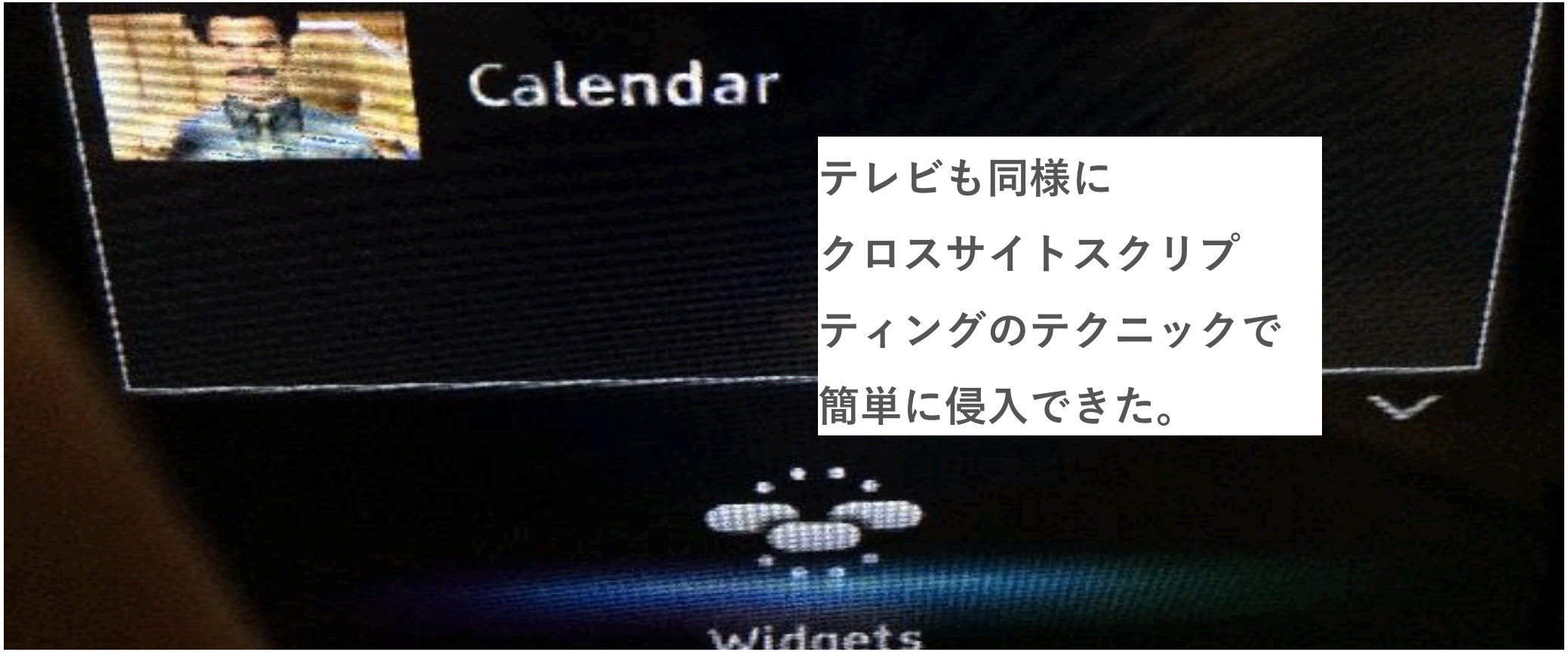
ホームルーターはLinux 2.6で動作している。

クロスサイトスクリプティングのテクニックで簡単に侵入できた。

https://securelist.com/files/2014/08/Hacked_home_8.jpg

KASPERSKY

テレビのアイコンを入れ替えてみた



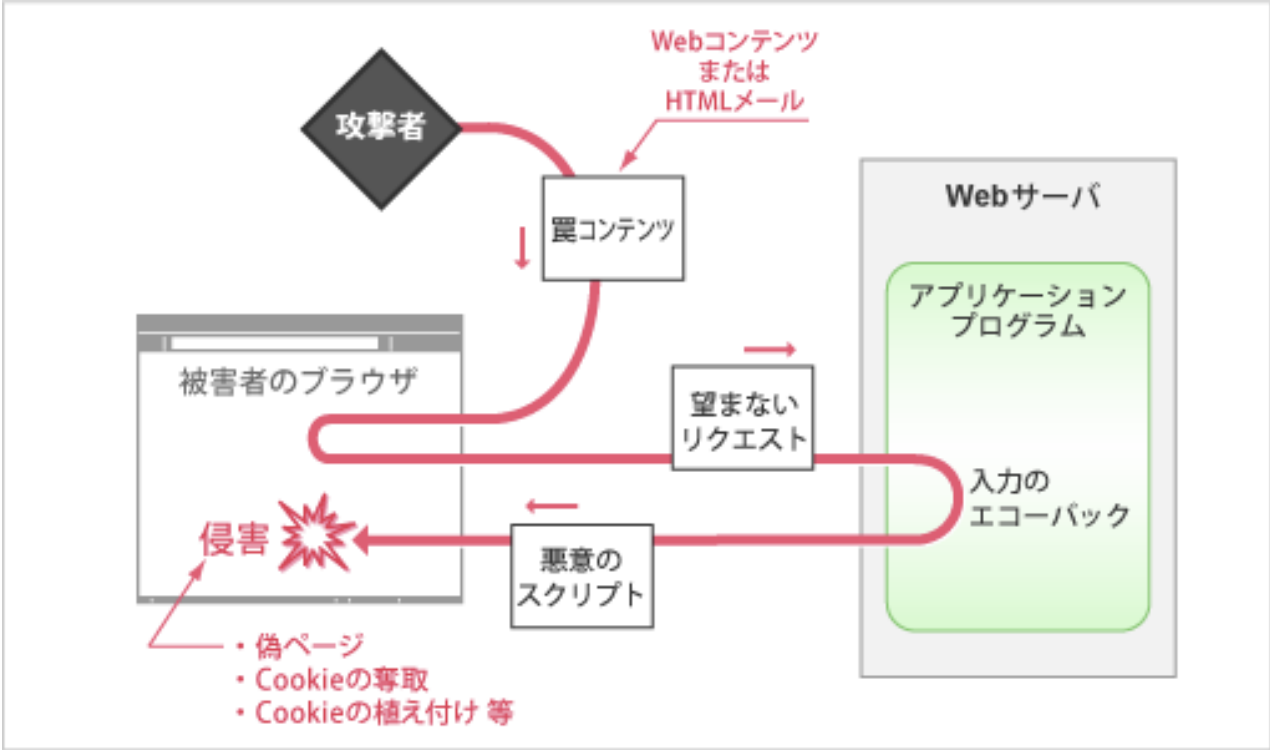
テレビも同様に
クロスサイトスクリプティングのテクニックで
簡単に侵入できた。

https://securelist.com/files/2014/08/Hacked_home_8.jpg

KASPERSKY

XSS（CROSS SITE SCRIPTING）

- これは Webサーバのエコーバック（鸚鵡返し（おうむがえし））のロジックを悪用する攻撃である。もうひとつ、いわゆる「第二攻撃（Second-order XSS）」も挙げられる。 いずれの攻撃においても、スクリプト注入を許してしまうWebサーバは、HTML生成時のスクリプト除染が不備なものである。



https://www.ipa.go.jp/security/awareness/vendor/programmingv2/contents/601.html

KASPERSKY

推奨する対策

- 常にベンダーが提供する最新のパッチを適用する
- デフォルト設定のユーザー名（ID）、パスワードは使用せず、必ず定期的に更新する
- 暗号化（通信およびデータ）
- DMZ/VLANを構成する（設定可能なら）
- たとえハードウェアであってもハッキングされる恐れがあると考える
- ネットワークデバイスは外部からアクセスできないように。ただし、アップデートはダウンロードできるようにしておく

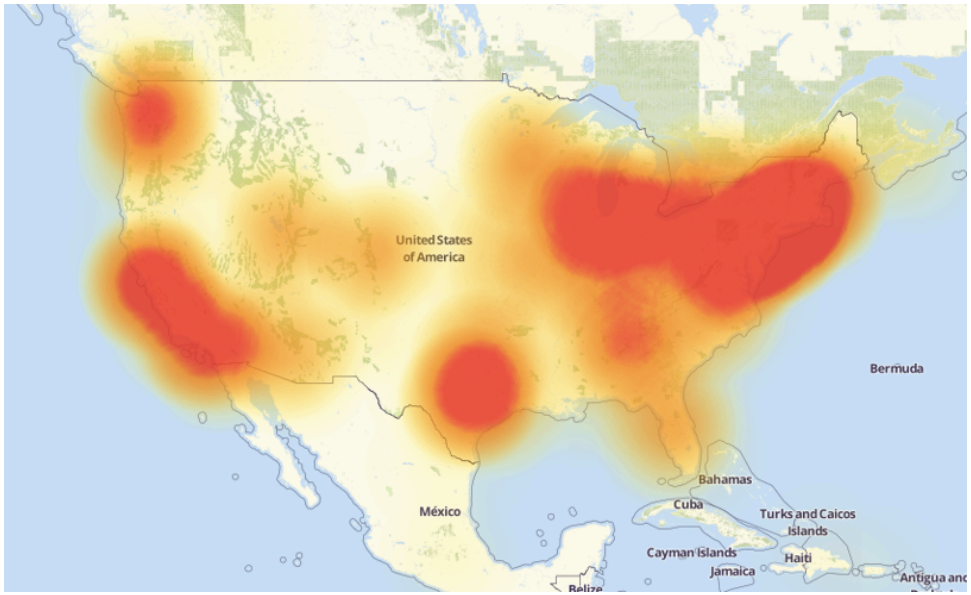
https://securelist.com/files/2014/08/Hacked_home_8.jpg

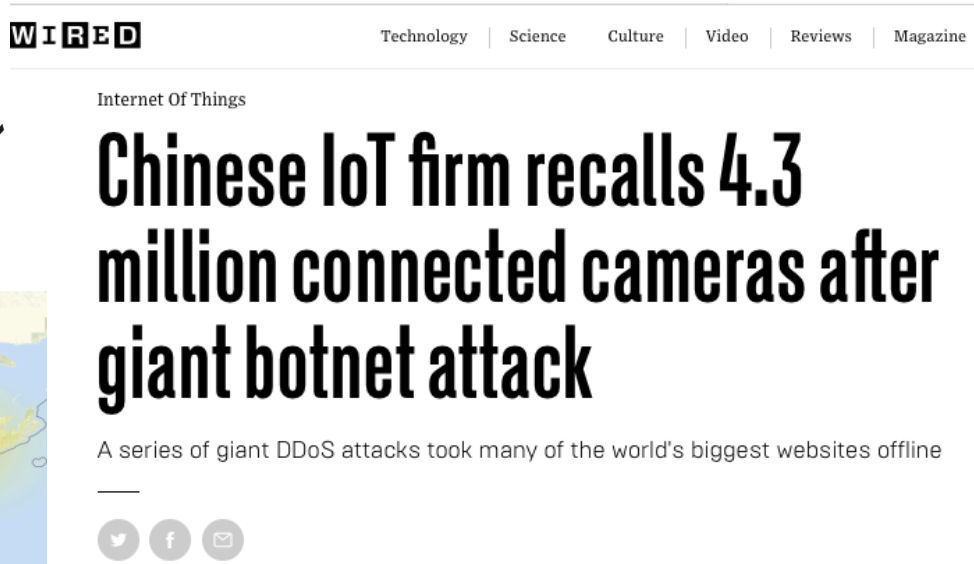
KASPERSKY

家電をハイジャック

SONY PlayStation ネットワーク(Oct 2016)

- 家電をハックして、Dyn社のDNSへのDDoS攻撃でインターネットを麻痺させたことで、他にもTwitter、Netflixなど多くのサービスが利用不能に




WIRED Technology | Science | Culture | Video | Reviews | Magazine

Internet Of Things

Chinese IoT firm recalls 4.3 million connected cameras after giant botnet attack

A series of giant DDoS attacks took many of the world's biggest websites offline

https://blog.kaspersky.co.jp/attack-on-dyn-explained/13047/
http://www.kaspersky.co.jp/about/news/virus/2016/vir09112016
http://wired.jp/2016/10/24/internet-down-dyn-october-2016/

KASPERSKY

いまどきの家電＝「パソコン」

- エアコン：Linux OS搭載
- カーナビ：Windows, Linux OS搭載
- テレビ：Linux OS搭載
- ネットワークカメラ：Linux OS, Windows搭載
- ペッパー：Android OS搭載

車をハイジャック

クライスラー(Jul 2015)

- エンターテインメントシステムの「Uconnect」をセルラーネットワーク経由でハッキング

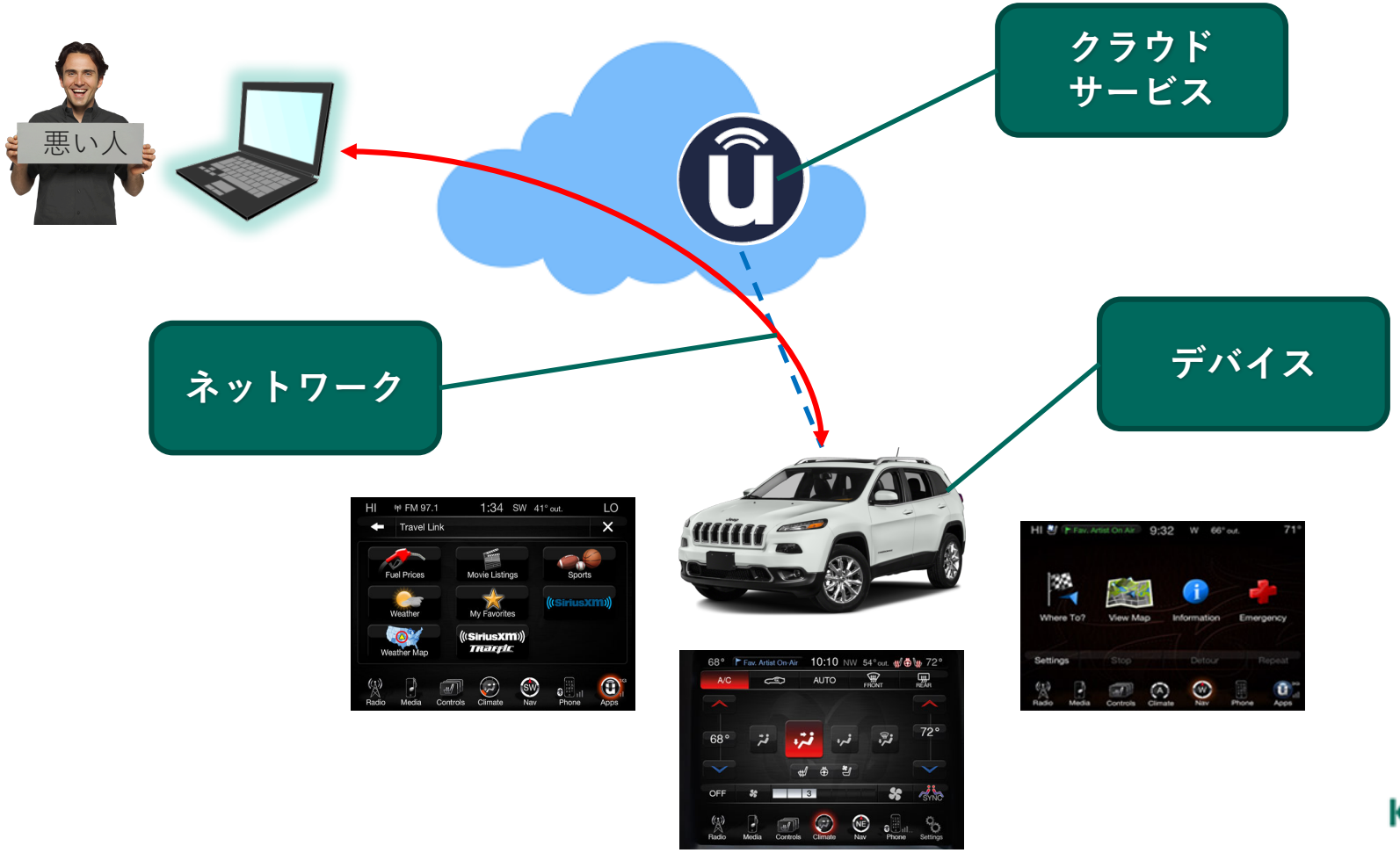
WIRED
@WIRED
Follow

Hackers remotely kill a Jeep on the highway — with me in it
wrd.cm/1HNWxrL
8:44 PM - 21 Jul 2015
2,388 1,118

https://blog.kaspersky.co.jp/remote-car-hack/8332/
https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/
http://www.nikkei.com/article/DGXLASGM25H19_V20C15A7MM0000/

KASPERSKY

JEEPのハッキングはどうやったのか？



なぜサイバー攻撃が可能なのか？

- 脆弱性、つまりバグや仕様によって悪用可能なコード（Exploit）がアプリケーションやOSなどに存在するため
- しかし、バグや仕様上の欠陥を見つけ出すことが難しい
- つまり、利用者にとって便利なものは悪いことをしたい人たちにとっても便利になる（多くの場合）

ビジネスにおける新しいリスク

サイバー犯罪やサイバー攻撃のリスク

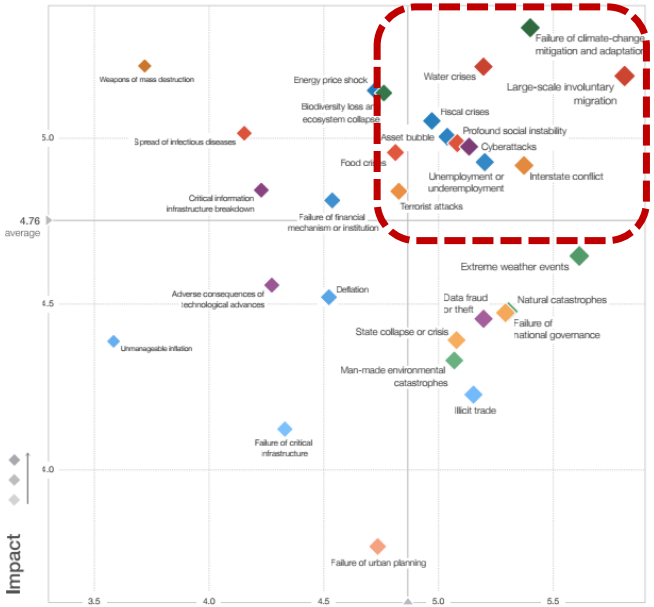
ビジネス上の脅威 – 共通の視点

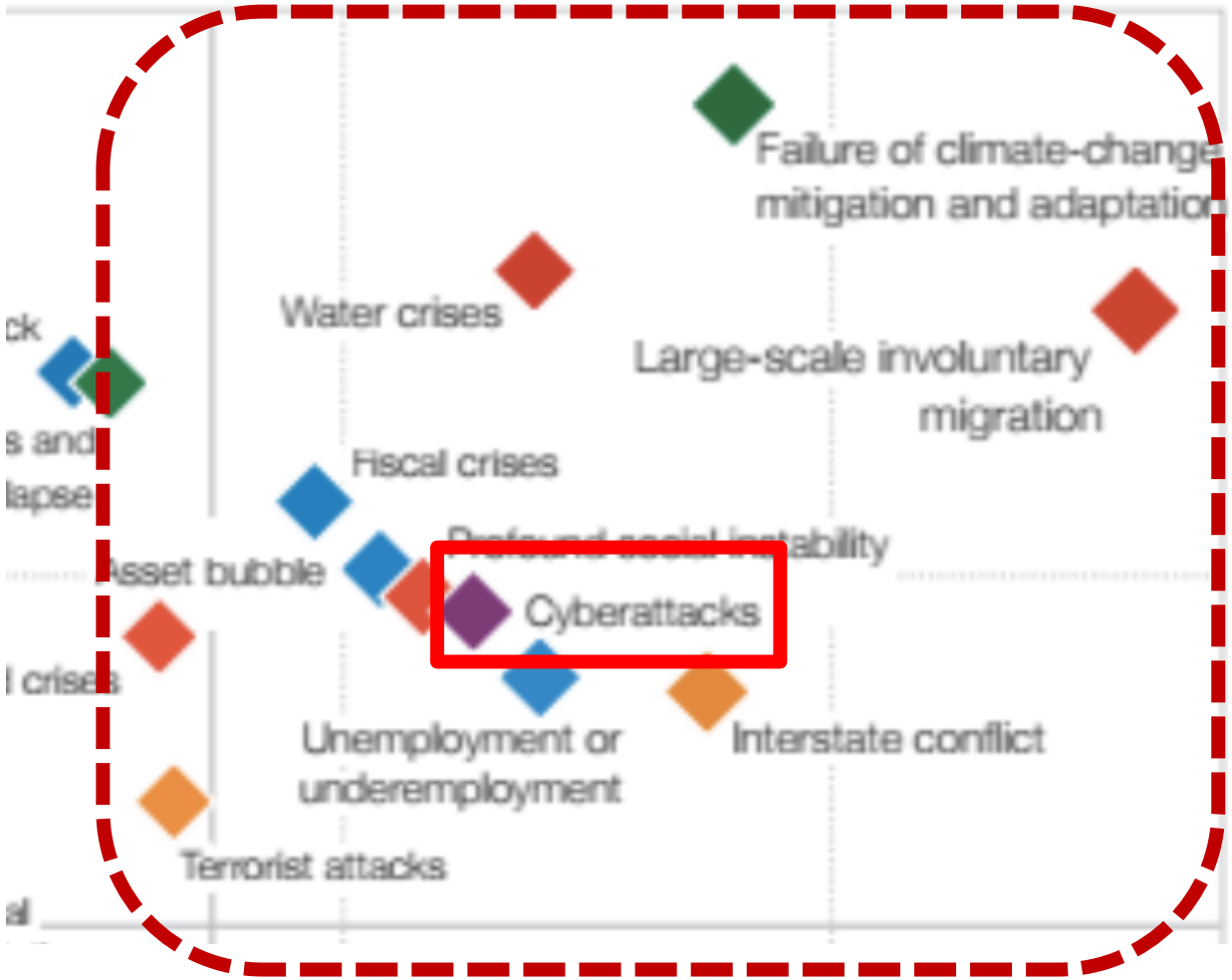
WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

The Global Risks Report 2016
11th Edition





* http://www3.weforum.org/docs/Media/TheGlobalRisksReport2016.pdf

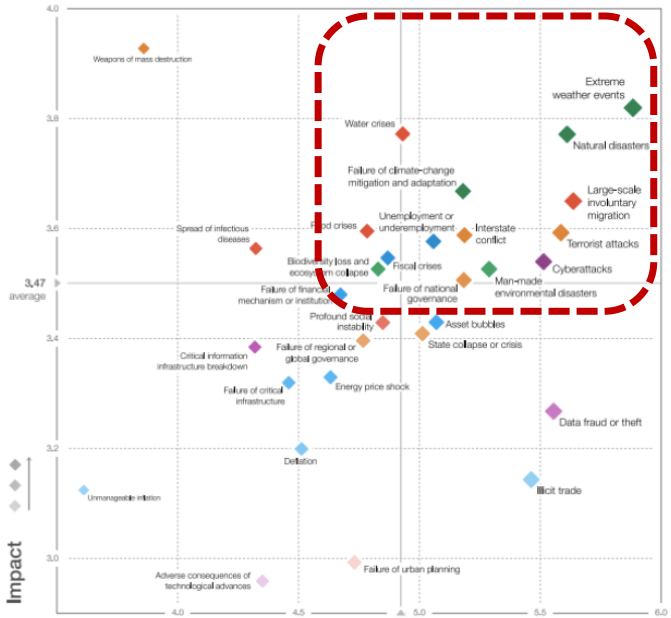
KASPERSKY

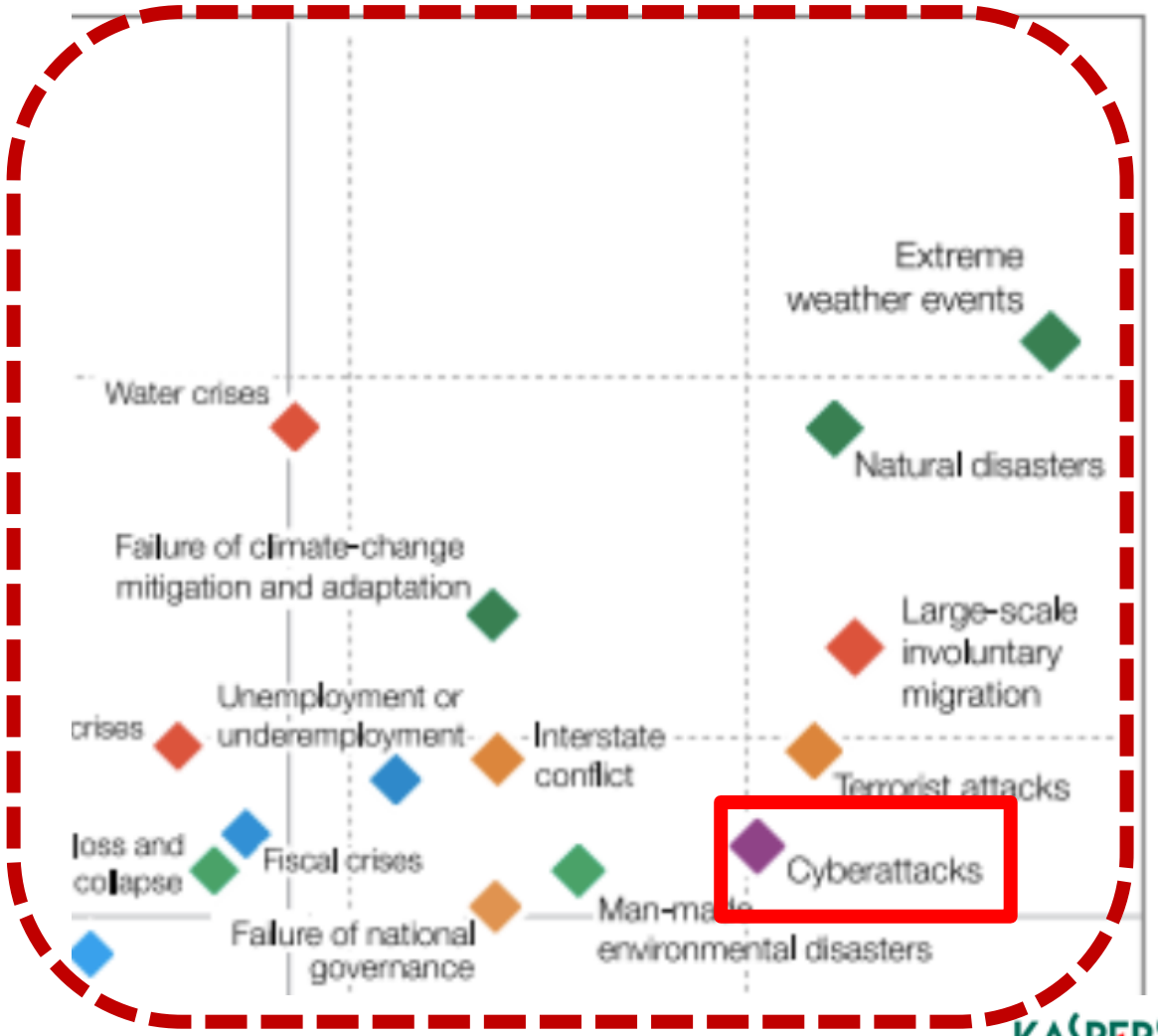
ビジネス上の脅威 – 共通の視点

WORLD ECONOMIC FORUM Agenda Initiatives Reports Events About

The Global Risks Report 2017

Figure 3: The Global Risks Landscape 2017





https://reports.weforum.org/global-risks-2017/global-risks-landscape-2017/

KASPERSKY lab

ビジネスリーダーの10大リスク

ビジネスが止まる

2016 - 3

2015 - 5

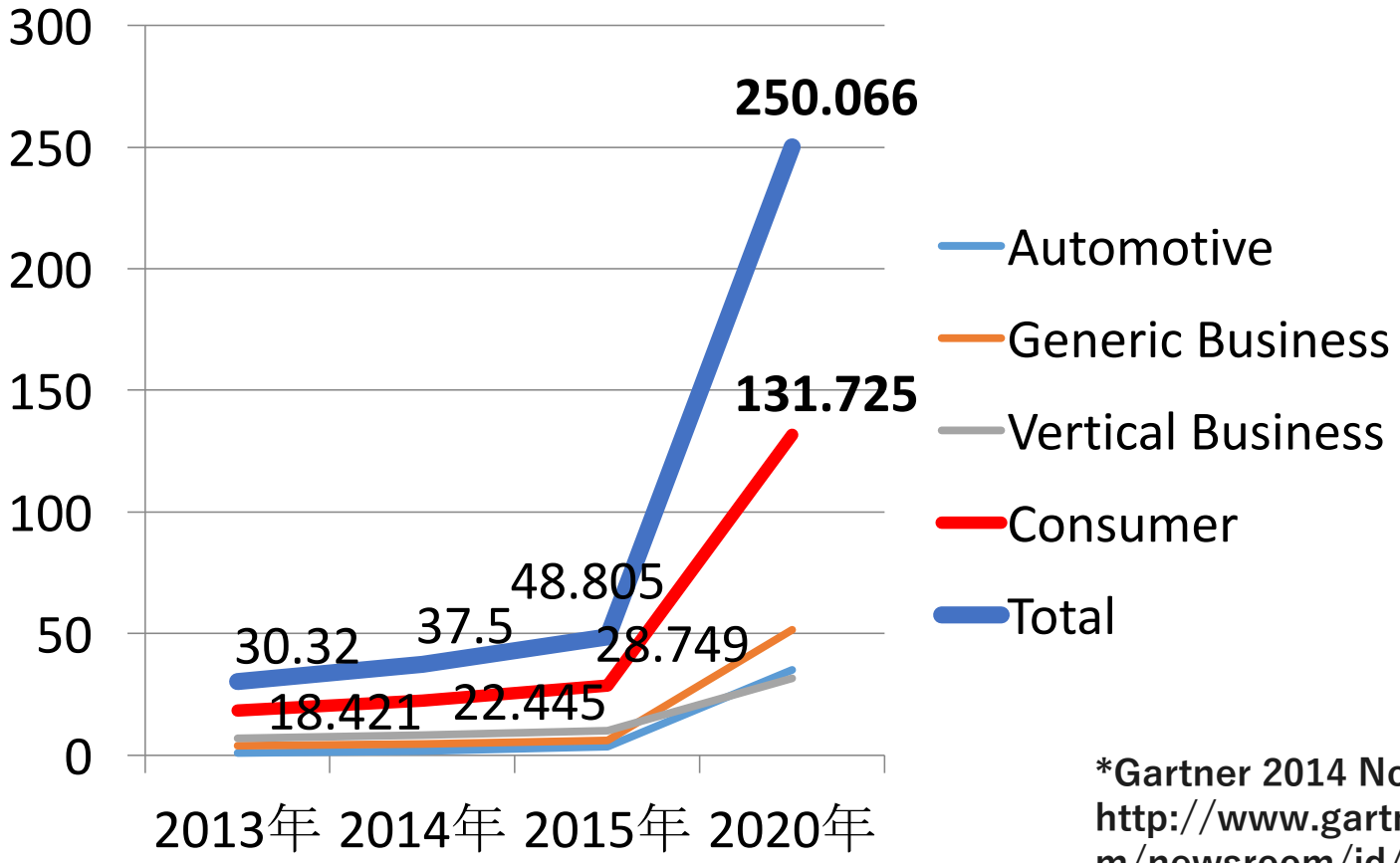
2014 – 8

2013 - 13

ソース: Allianz Risk Barometer 2016

KASPERSKY

2020年までにIOTデバイス数は 250億超
半数超はコンシューマー



*Gartner 2014 Nov.
http://www.gartner.com/newsroom/id/2905717

KASPERSKY

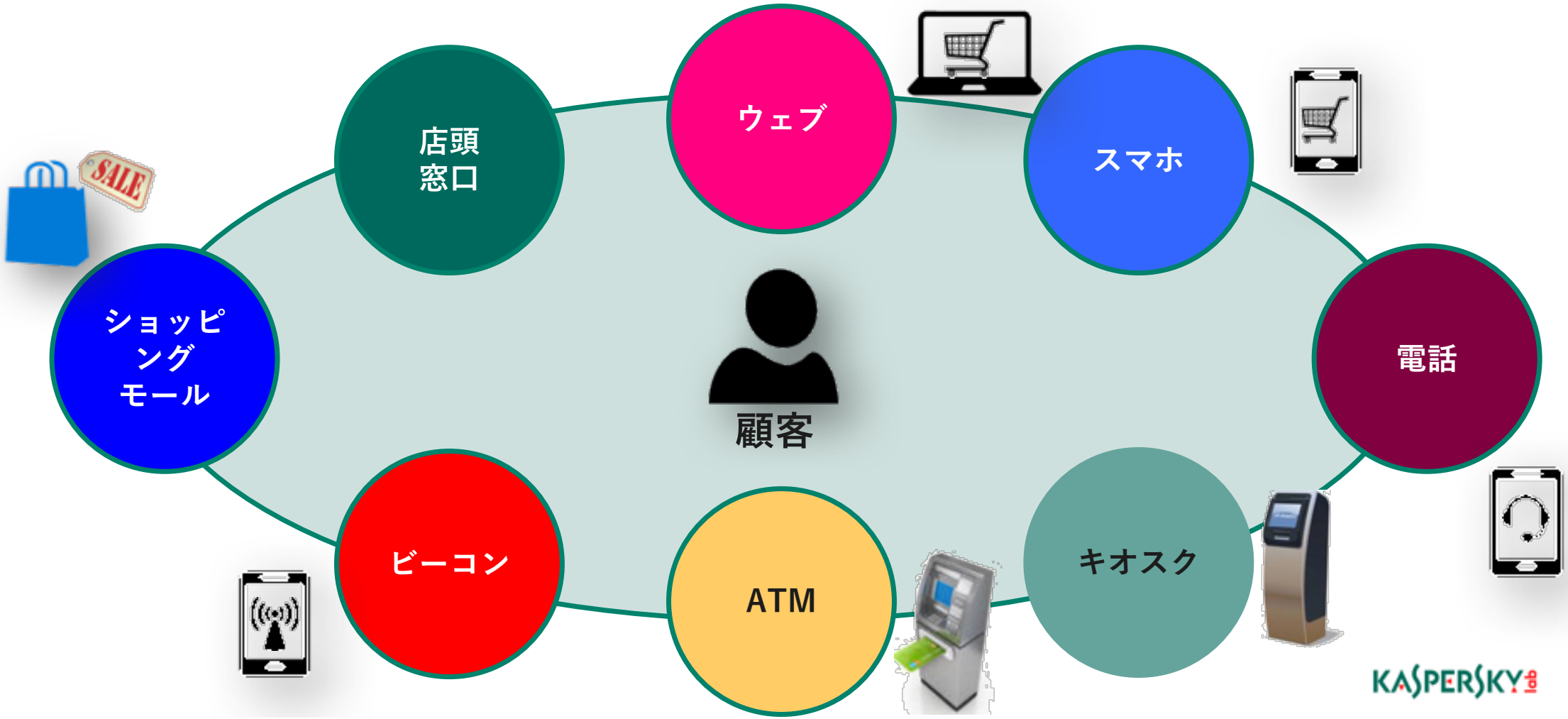
サイバーセキュリティとIOTはお友達

一緒に考えてください、そもそもサイバーセキュリティは「そこ」を安全にするために必要なものなのです

日本のインフラが変わろうとしている
ー ICTに支えられた「IOT」の世界へ ー

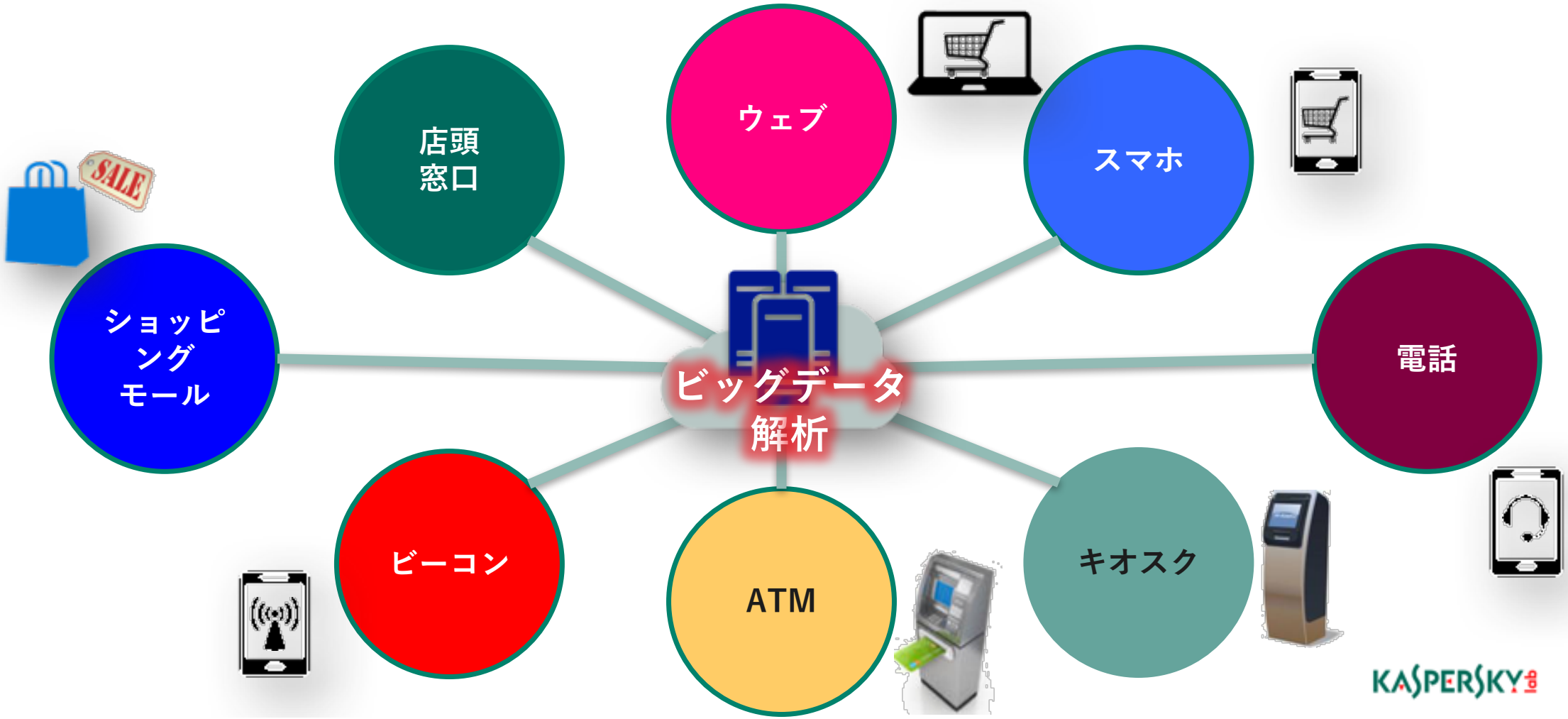
日本のインフラが変わろうとしている
ー ICTに支えられた 「オムニチャネル」 の世界へ ー

身近な IOT化：オムニチャネル化
ー タッチポイント多面化、サービス品質と満足度を向上 ー

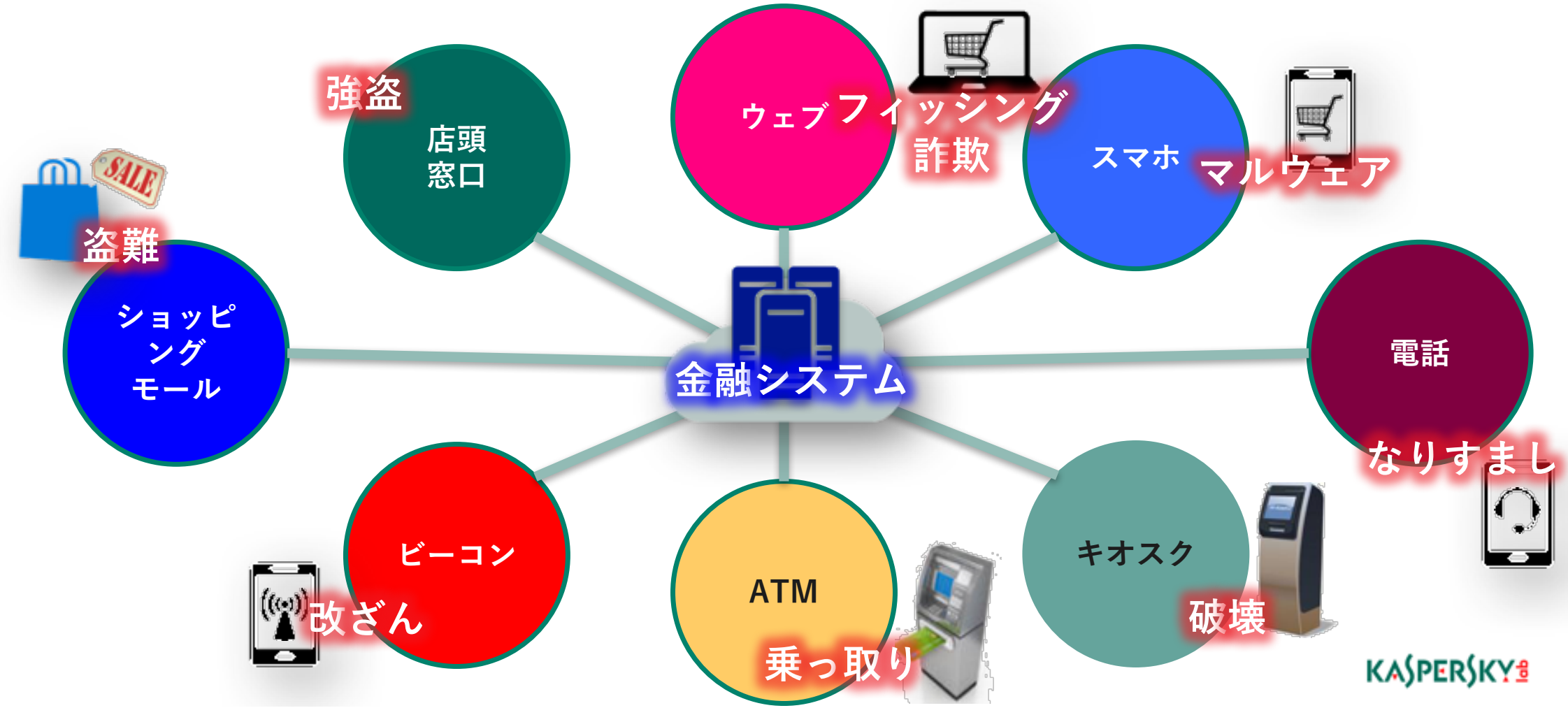


オムニチャネル化：タッチポイントとサービスの拡充

ー 顧客データの多面的な収集と分析により、サービスの革新と向上 ー

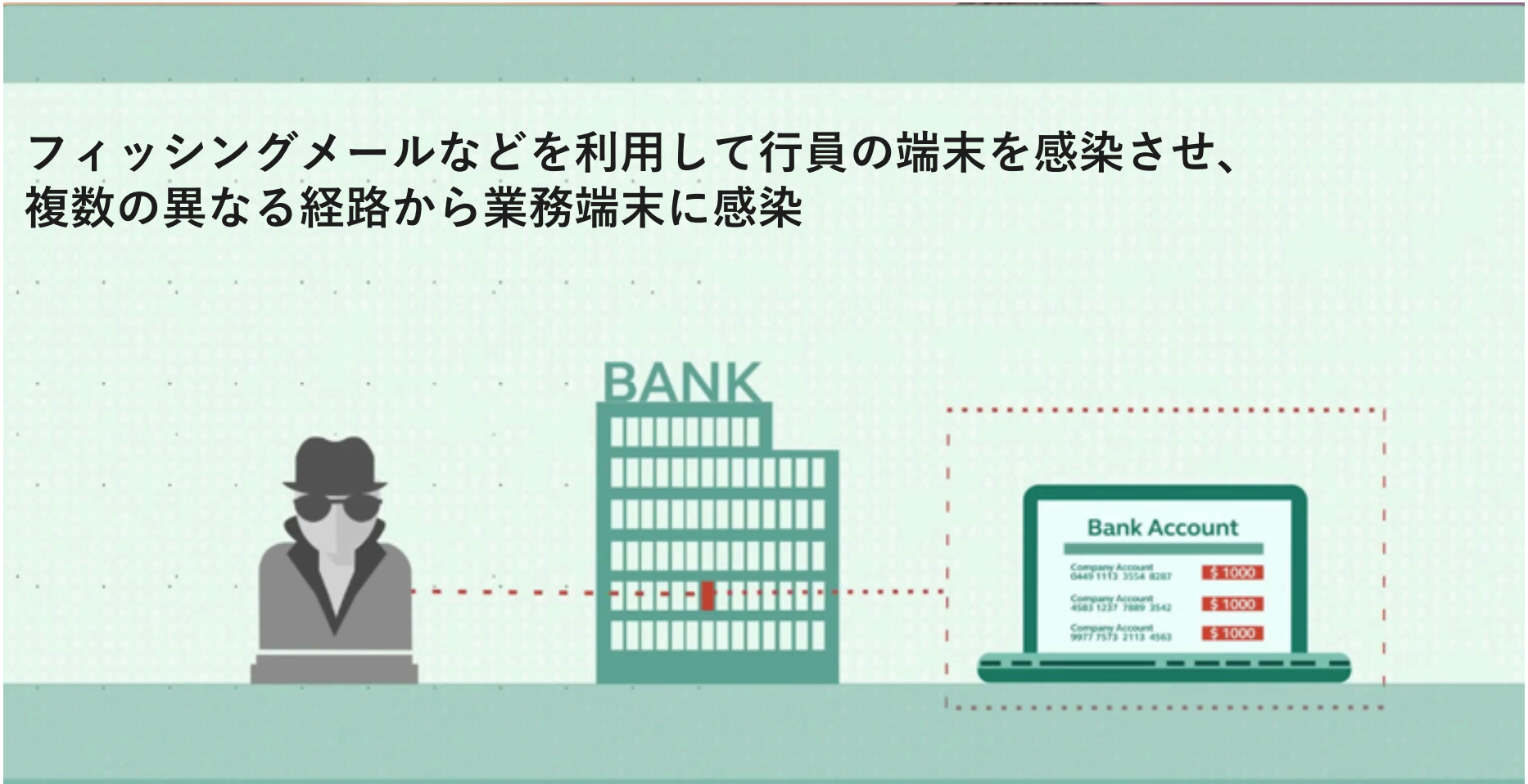


オムニチャネル化：デバイスとネットワークの拡大
ー セキュリティリスクの分析と対策が必要 ー



銀行を狙った最新のインシデント：CARBANAK

フィッシングメールなどを利用して行員の端末を感染させ、
複数の異なる経路から業務端末に感染

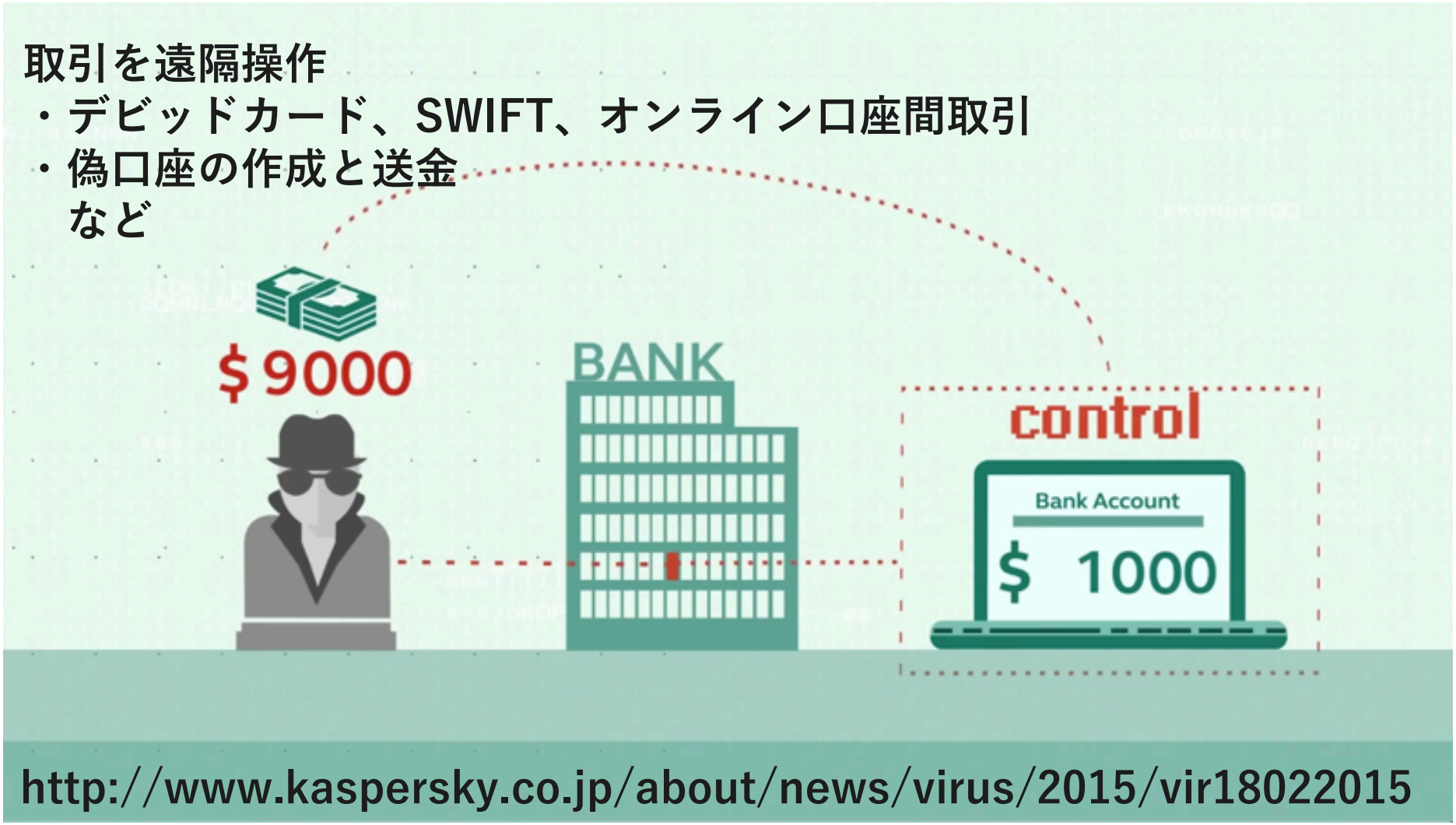


http://www.kaspersky.co.jp/about/news/virus/2015/vir18022015

KASPERSKY

銀行を狙った最新のインシデント：CARBANAK

取引を遠隔操作
・デビッドカード、SWIFT、オンライン口座間取引
・偽口座の作成と送金
など



http://www.kaspersky.co.jp/about/news/virus/2015/vir18022015

銀行を狙った最新のインシデント：CARBANAK

“DARK HOTEL”

ビジネスエグゼクティブに特化した諜報活動

- 洗練された諜報活動
- 少なくとも 2007年には活動していた
- 90% の感染は日本、台湾、中国、ロシア、韓国そして香港で確認
- もちろんドイツ、米国、インドネシア、インドおよびアイルランドでも確認された
- 主な対象は米国の防衛関連企業
- ユニークな方法でビジネスエグゼクティブを対象に活動

※未知の脆弱性を利用していたことがわかっている

http://www.kaspersky.co.jp/about/news/virus/2014/vir10112014
http://www.kaspersky.co.jp/about/news/virus/2015/vir11082015

KASPERSKY

“DARK HOTEL”

ビジネスエグゼクティブに特化した諜報活動

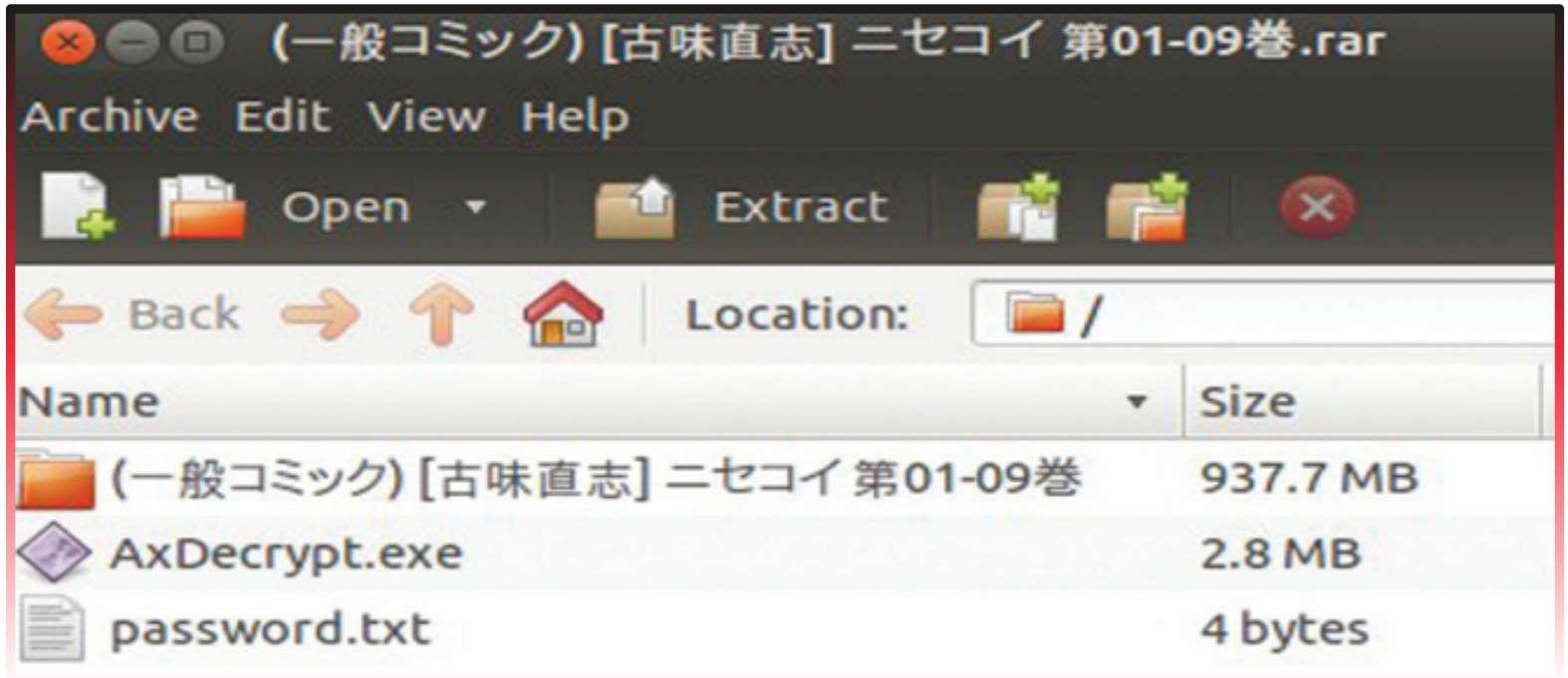
1. 攻撃者がホテルのネットワーク上にDarkhotelを感染
2. 企業の幹部がホテルにチェックイン、WiFiネットワークに接続
3. ログイン画面で名前と部屋番号を入力
4. 攻撃者がソフトウェアの更新を推奨
5. 更新すると、バックドアをインストール
6. 攻撃者はバックドア経由でファイルやパスワード、ログイン情報を入手

http://www.kaspersky.co.jp/about/news/virus/2014/vir10112014
http://www.kaspersky.co.jp/about/news/virus/2015/vir11082015

KASPERSKY

“DARK HOTEL”
ビジネスエグゼクティブに特化した諜報活動

- 行動分析に基づく感染手法の多様化：
  - Torrent ファイル経由での感染



http://www.kaspersky.co.jp/about/news/virus/2014/vir10112014
http://www.kaspersky.co.jp/about/news/virus/2015/vir11082015

KASPERSKY

電力網も危険？

ウクライナ(2015)

- デジタル変電所を攻撃、SCADAなど制御システムをハッキングして5つの地域で6時間に渡って大規模停電

CIO | クラウド | モバイル PC | セキュリティ | ソフトウェア | サーバ | ストレージ | ネットワーク | ミドルウェア | 運用 | マーケティング | ビッデー

ZDNet Japan > セキュリティ

海外コメンタリー

電力会社へのサイバー攻撃で大規模停電--インダストリアルIoTの脆弱性

Charles McLellan （ZDNet UK） 翻訳校正： 編集部 2016年04月05日 06時00分

いいね！ 170 | ツイート | G+1 1 | B! 14 | Pocket 38

印刷 | メール | ダウンロード | クリップ

PR 【コグニティブ時代のオールフラッシュ・ストレージ】無償診断受付中！
PR セキュリティ、コスト、運用管理… 企業ネットワークで優先すべきポイントは？
PR エンジニアは、いかに「事業を創れる技術屋」に進化すべきか？まとめ記事を読む！

旧ソ連圏の国家だったウクライナは、EU加盟を望む市民による抗議活動「ユーロマイダン」、ロシアによるクリミア併合、親ロシア派による反政府活動など、2014年初頭から国際問題の震源地となってきた。

http://www.kaspersky.co.jp/about/news/virus/2016/vir22022016
http://www.itmedia.co.jp/smartjapan/articles/1601/08/news054.html
http://japan.zdnet.com/article/35080555/

KASPERSKY

ICS サイバーセキュリティの現状

2015年 10月
第3回 Kaspersky Industrial Cyber Protection Conference
CTF – Capture The Flag 競技
ゴールは制御システムに潜む脆弱性を見つけ出すこと

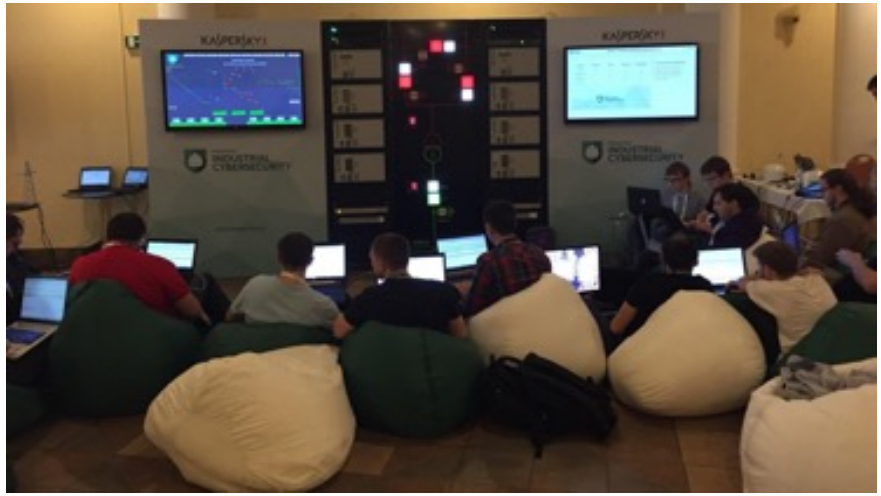
攻撃の手順:

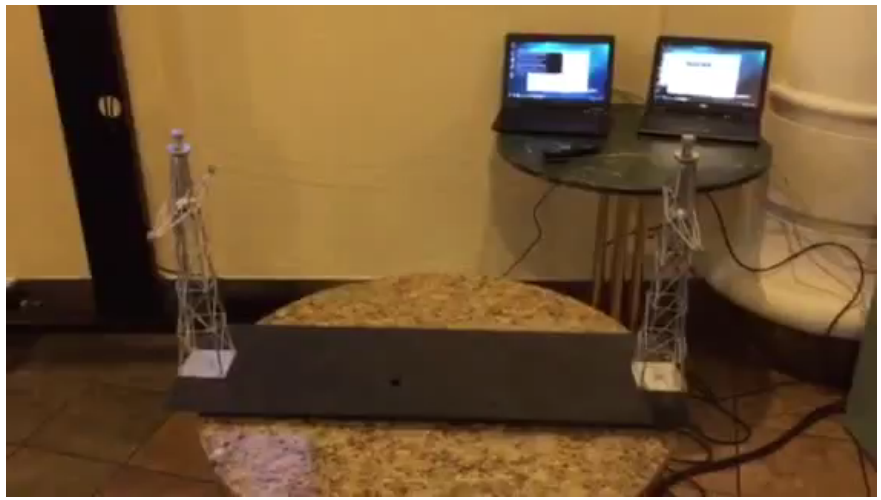
ネットワーク通信を取得

- システムの管理者権限を奪取
- 自動保護を切る
- 電力線モデルをショートさせる

四つのチームのうち三つが競技初日の電力線のショートを引き起こした :

- 電気技術者チーム: 3 時間
- 一般的なハッカーチーム: 5 時間





KASPERSKY

課題：取締りの限界

- サイバー犯罪取締り条約を締結：53カ国/193カ国（国連加盟国数）
- 欧州各国はほぼ施行済み（アイルランド、ロシア、スウェーデン以外）
- 欧州外の施行済み国：オーストラリア、カナダ、ドミニカ、イスラエル、日本、モーリシャス、パナマ、スリランカ、米国

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=zxiSMQok

課題：取締りの限界
“LAZARUS GROUP” 国家レベルでの犯罪

- 北朝鮮が関与するとみられるサイバー犯罪組織
- 2013年、韓国の放送局と金融機関を攻撃し麻痺させる
- 2014年、ソニーピクチャーズを攻撃
- 2016年、世界中の金融機関を攻撃
  8100万ドル（日本円で約90億円）を窃取

https://www.kaspersky.com/about/press-releases/2017_chasing-lazarus-a-hunt-for-the-infamous-hackers-to-prevent-large-bank-robberies

KASPERSKY

ひとりひとりができること

- 最新のセキュリティ更新をインストールする
- セキュリティソフトをインストール（PC/Mac/スマホ）
- 二要素認証などでアカウントを乗っ取られ難くする
- 必要なファイルや情報はこまめにバックアップする
- LineやFBなど友達の振る舞いにも注意、常に疑り深く
- サイバーセキュリティを仕事にしたい人はご連絡ください☺

KASPERSKY

ご静聴ありがとうございました

masato.matsuoka@kaspersky.com

KASPERSKY lab