サイバーセキュリティの最前線

櫻井, 幸一
九州大学大学院システム情報科学研究院情報学部門 : 教授

出版情報：九州大学大学院システム情報科学府・研究院先端サマーセミナー. 2014, 2014-08-30
バージョン：
権利関係：

九州大学 公開講座
先端サマーセミナー2014
システム情報科学による安心の社会基盤

サイバーセキュリティの最前線

情報学部門　櫻井 幸一
（システム情報科学研究院 教授）

スライド作成協力：松本 晋一，穴田 啓晃
公益財団法人九州先端科学技術研究所

目次

- ■最近のサイバーセキュリティニュース
  - ●教育/研究の連携
  - ●サイバーインシデント
  - ●対策の動き
- ■Bitcoin, リアルマネートレード
  ～サイバー空間におけるサービスと問題～
  - ●Bitcoin
  - ●リアルマネートレード

第Ⅰ部

最近のサイバー
セキュリティニュース

サイバー攻撃対策 教育/研究の連携(1)

- 米Maryland大と九大のMOU(Memoranda of Understanding)締結(ニュースリリース)
  - 全学生向け教育プログラム開発
  - 専門家要請プログラム開発
  - 先進技術の共同研究

サイバー攻撃研究
九大と米大が連携

【ワシントン山崎健】九州大（福岡市）は24日、サイバー攻撃に備えるサイバーセキュリティー研究で米国有数のメリーランド大と同分野の教育や研究で連携する学術協力覚書に署名した。在米日本大使館によると、この分野で日米の大学が本格的な学術交流の覚書を交わすのは初めて。

首都ワシントン近郊にあるメリーランド州アデルフィの同大システム本部であった署名式には九大の有川節夫学長、メリーランド大のウィリアム・カーワン総長、佐々江賢一郎駐米大使ら約30人が出席した。

有川学長は「サイバーセキュリティーは個人の生活から国の安全保障にまで関係する極めて重要な分野で、最も進んだ米国と協力できるのは画期的だ。すべての学生の必修科目にしていきたい」と強調。今後、九大はメリーランド大とともに①全学生向けの教育プログラム開発②専門家養成のプログラム開発③先進技術の共同研究―を進める。

その上で今秋、理工系学生向けのサイバーセキュリティーの基礎を学ぶ必修科目をスタート。来年からは全学生に広げる。

メリーランド大は米政府の情報機関、米国家安全保障局（NSA）などに多くの人材を輩出。両大学は今後、学生の交流も図る方針で、九大の学生がオンラインでメリーランド大の授業を受けることも目指す。

覚書に署名後、メリーランド大のウィリアム・カーワン総長（左）と握手する九州大の有川節夫学長＝24日、米メリーランド州アデルフィ（共同）

西日本新聞
2014年6月26日
朝刊より

サイバー攻撃対策 教育/研究の連携(2)

- 共同通信社KYODO NEWSの報道(Youtube)より

サイバー攻撃インシデント抜粋

2010年7月 イランの核関連施設がStuxnetによる攻撃を受けたと観測される

2011年4月 大手ゲーム機器メーカへの不正アクセス攻撃。ユーザ情報の流出などにより、一時サービスを中断。

2011年9月 日本の大手重工業メーカへの標的型メール攻撃。サーバ、PC等がウイルスに感染し、情報流出の恐れ。

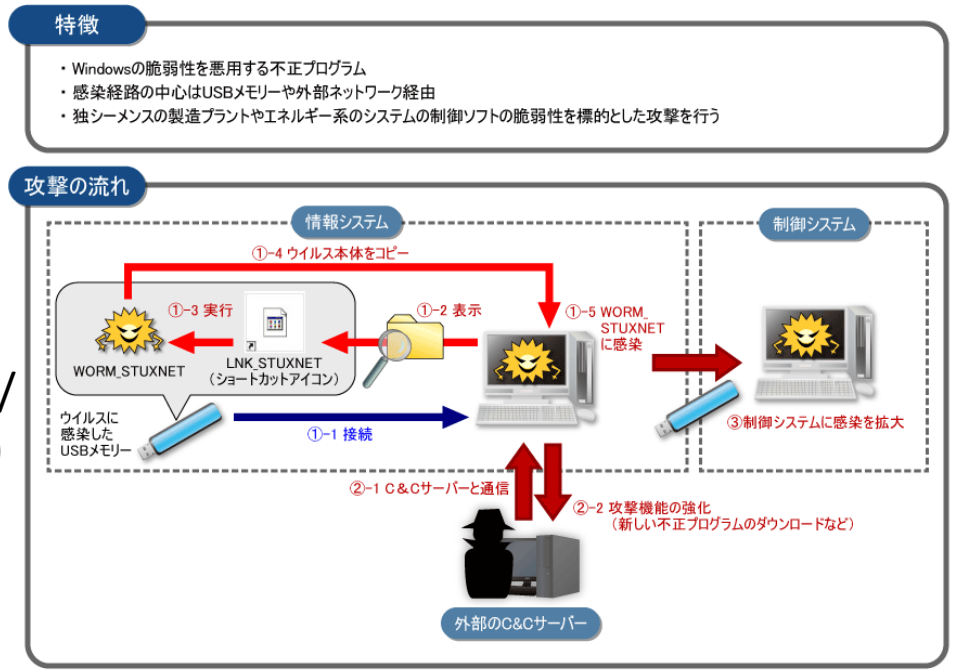
2012年6月 日本の財務省のWEBページや最高裁判所への不正アクセス(WEBページ書換)、民主党、自民党サイトへの攻撃。

2013年3月 韓国の金融機関，テレビ局に対する大規模攻撃。ATM1万6千台が停止など社会的混乱

2014年6月 日本の政府機関等の複数組織がサイバー攻撃を受けたことが発表される

インシデント: Stuxnet(2010年)

- イランの核燃料処理施設の制御コンピュータ(のみ)を狙った不正プログラム
  - ネットワークだけでなくUSBメモリも感染媒体とする
  - 組み込みシステム(SCADA: Sypervisory Control and Data Acquisition)を対象とした攻撃
  - 国家/国家に準ずる組織による攻撃
    - サイバー戦争(Cyber Warfare)/サイバー兵器(Cyber Weapon)



図は制御システムを狙うサイバー攻撃の衝撃 – [1] 原子力発電所の設備を狙う「Stuxnet」：Itproより

インシデント: ゲーム機器メーカ(2011年)

- 大手ゲーム機器メーカのサーバの脆弱性を外部より突いて，ユーザの個人情報が流出
  - サイバー攻撃による個人情報流出としては史上最悪(7700万人分)
  - 利用者からの集団訴訟の和解金として約15億円相当の支払(和解締結2014年6月)
  - メーカの損失は12.5億ドルに上る*1

ソニーの会見：情報流出に対する謝罪－米FBIに捜査依頼：動画

記事 映像　記事を印刷する　記事をメールで送信

シェア　Twitter　チェック　Google　Share　共有/ブックマーク

5月2日（ブルームバーグ）：ソニーの平井一夫副社長は1日の会見で、ゲーム機「プレイステーション」などのネットワークに外部からの不正アクセスが集中し、大量の顧客情報が流出した問題に対し謝罪し、ユーザー約7700万件分の個人情報が流出した可能性が高いことを明らかにしました。　平井氏は「故意の不正侵入により、サイバーテロが行われた」と述べ、米連邦捜査局（FBI）に捜査を依頼したことを明らかにしました。実際に漏えいしたかどうかは不明としながらも、1000万件程度のユーザーのクレジットカード情報が漏えいした可能性があるとも指摘しました。ただ、データベースへのアクセスの形跡や不正利用の報告は「現時点ではない」としています。同社は情報保護の対策を行い、5月中のサービス全面再開を目指すとしています。会見には長谷島眞時業務執行役員と神戸司郎業務執行役員も同席しました。
(Source: Bloomberg)

Running time 01:26:35

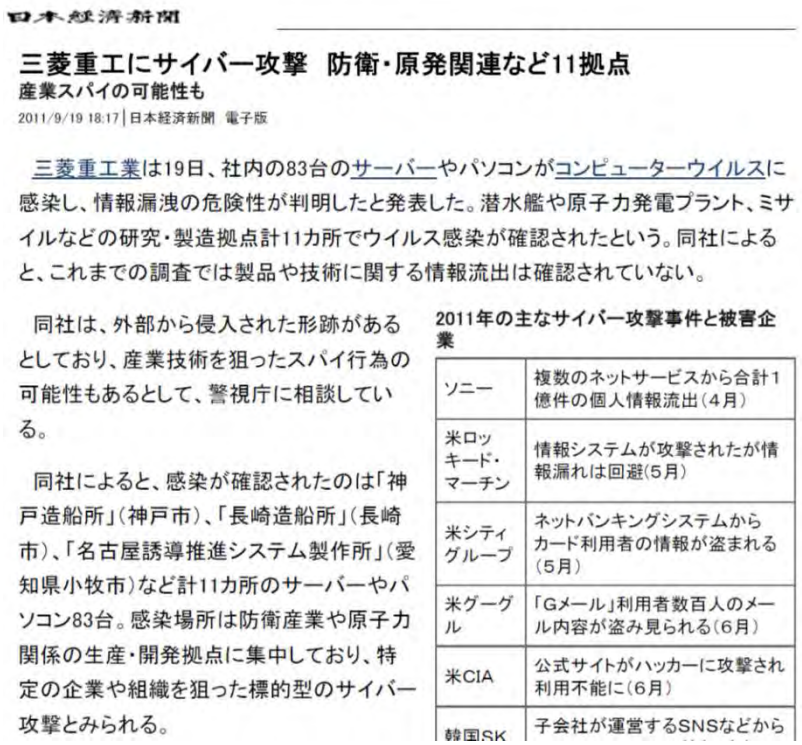
更新日時: 2011/05/02 10:23 JST

BloombergのWebページより
“http://www.bloomberg.co.jp/news/123-LKJNVV1A1I4H01.html”

*1: Wall Street Journal報道”As Sony Counts Hacking Costs, Analysts See Billion-Doller Repair Bill”より

インシデント: 大手重工メーカ(2011年)

- 大手重工メーカのサーバ，PCに対する標的型攻撃(APT: Advanced Persistent Threat)
  - 防衛産業や，原子力に関係する研究・製造拠点を狙った攻撃
  - 企業内の個人に，その関係者(取引先，同僚等)を装ってウイルスを含んだ電子メールを送りつけるなどの攻撃
  - 攻撃の手口の巧妙化・悪質化・長期化



日本経済新聞

三菱重工にサイバー攻撃　防衛・原発関連など11拠点

産業スパイの可能性も

2011/9/19 18:17 | 日本経済新聞 電子版

三菱重工業は19日、社内の83台のサーバーやパソコンがコンピューターウイルスに感染し、情報漏洩の危険性が判明したと発表した。潜水艦や原子力発電プラント、ミサイルなどの研究・製造拠点計11カ所でウイルス感染が確認されたという。同社によると、これまでの調査では製品や技術に関する情報流出は確認されていない。

同社は、外部から侵入された形跡があるとしており、産業技術を狙ったスパイ行為の可能性もあるとして、警視庁に相談している。

同社によると、感染が確認されたのは「神戸造船所」(神戸市)、「長崎造船所」(長崎市)、「名古屋誘導推進システム製作所」(愛知県小牧市)など計11カ所のサーバーやパソコン83台。感染場所は防衛産業や原子力関係の生産・開発拠点に集中しており、特定の企業や組織を狙った標的型のサイバー攻撃とみられる。

2011年の主なサイバー攻撃事件と被害企業

ソニー	複数のネットサービスから合計1億件の個人情報流出(4月)
米ロッキード・マーチン	情報システムが攻撃されたが情報漏れは回避(5月)
米シティグループ	ネットバンキングシステムからカード利用者の情報が盗まれる(5月)
米グーグル	「Gメール」利用者数百人のメール内容が盗み見られる(6月)
米CIA	公式サイトがハッカーに攻撃され利用不能に(6月)
韓国SK	子会社が運営するSNSなどから

日本経済新聞2011年9月19日記事より
http://www.nikkei.com/article/DGXNASDG1900N_Z10C11A9000000/

インシデント: 政府機関(2012年)

- 国内の財務省や，最高裁判所などのホームページの改竄や，サイトへのDDoS(Distributed Denial of Services)攻撃
  - 社会的・政治的な主張(この場合，改正著作権法に対する抗議)をもった集団によるハクティビズム (hacktivism = hacking + activism).

REUTERS ロイター

記事を印刷する | ウィンドウを閉じる

アノニマスが日本にサイバー攻撃か、財務省HPなど被害相次ぐ

2012年 06月 27日 08:19 JST

[27日 ロイター] 国内メディアによると、財務省や最高裁判所など複数の官公庁ホームページ(HP)が26日から27日にかけて、一部書き換えられたり、閲覧できなくなったりした。国際的ハッカー集団「アノニマス」は25日、海賊版ダウンロードへの罰則を盛り込んだ改正著作権法が成立したことに抗議し、日本政府などへのサイバー攻撃を予告していた。

報道によると、財務省は同省HP内にある「国有財産情報公開システム」に不正な情報が書き込まれていたため、26日に同システムを閉鎖した。また、最高裁のサイトでは、全国の裁判所のHPにリンクするページが一時表示できなくなったという。

アノニマスはこのほか、ツイッターで民主党や自民党のHPへの攻撃も表明していた。

REUTER Webページより
http://jp.reuters.com/article/topNews/idJPTYE85P08K20120626

インシデント: 韓国金融機関等(2013年)

- 国外の例．韓国の複数の放送局，金融機関においてシステム停止を引き起こすマルウェア感染．約32,000台のPCが被害を受ける
  - Windowsのパッチ更新サーバを経由しての攻撃
  - Windowsマシンのブートレコードの書き換えにより，起動不能に陥れる
  - 同時多発的な障害発生による社会的な混乱．

日経コンピュータReport 日経コンピュータ

韓国激震、サイバー攻撃が同時多発

パッチ管理システムを突かれる

2013/04/04
浅川 直輝＝日経コンピュータ （筆者執筆記事一覧）

出典：日経コンピュータ　2013年4月4日号p.11
（記事は執筆時の情報に基づいており、現在では異なる場合があります）

記事一覧へ >>

シェア　ツイート　B! ブックマーク

韓国の主要放送局や金融機関が受けた、大規模なサイバー攻撃の波紋が広がっている。日本の企業や官公庁が、同様のサイバー攻撃を受けることは十分に考えられるほか、既に何らかのマルウエアが仕込まれている可能性もゼロではない。サイバー攻撃対策の見直しが急務だ。

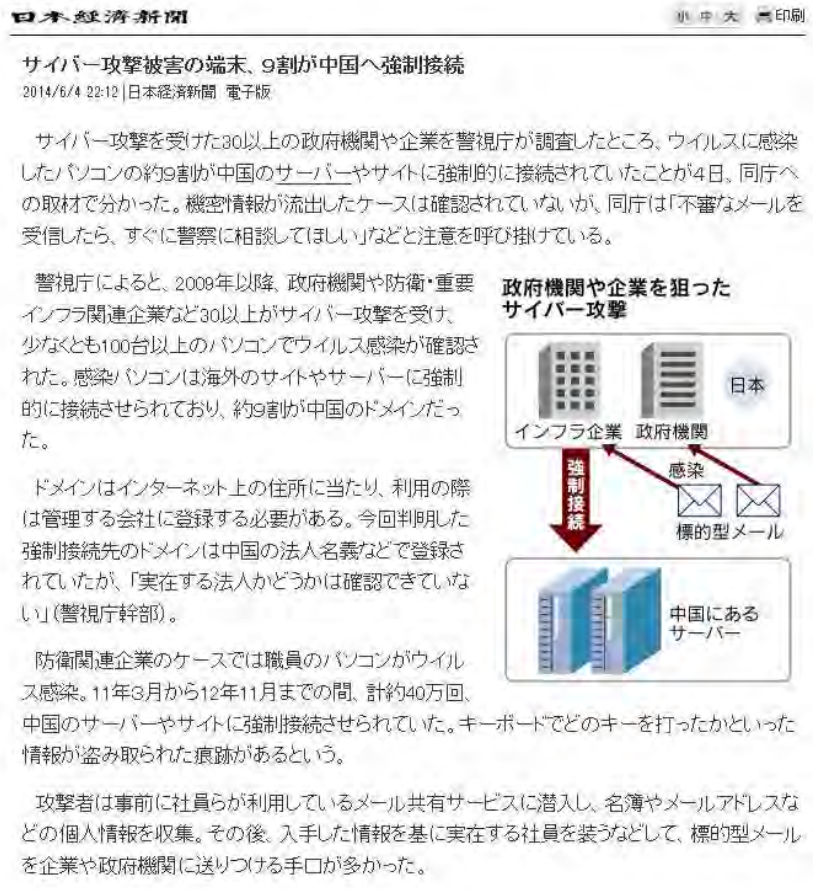
韓国で問題が発生したのは、2013年3月20日14時ごろ。KBSテレビ、MBCテレビ、YTNテレビ、新韓銀行などの社内システムが一斉にダウンし、合計で約3万2000台のPCやサーバーが再起動できないなどの被害を受けた。

テレビ局の放送が止まる事態は避けられたが、銀行のATM（現金自動預け払い機）が一部使えなくなるなどの被害が出た。韓国国防省はサイバー防衛の警戒レベルを示す情報作戦防護態勢を、5段階中のレベル4からレベル3へ引き上げるなど緊張が走った。

日経コンピュータWebページより
http://itpro.nikkeibp.co.jp/article/COLUMN/20130328/466648/

インシデント: 日本政府機関 (2014年)

- 国内の中央省庁，独立行政法人，欧州の日本大使館，電力会社，防衛関連企業などへの攻撃が確認される
  - 約9割が中国国内のアドレスに接続
  - 攻撃を受けたことを，長期間に渡って認識していないケース



日本経済新聞

小 中 大 印刷

サイバー攻撃被害の端末、9割が中国へ強制接続

2014/6/4 22:12 | 日本経済新聞 電子版

サイバー攻撃を受けた30以上の政府機関や企業を警視庁が調査したところ、ウイルスに感染したパソコンの約9割が中国のサーバーやサイトに強制的に接続されていたことが4日、同庁への取材で分かった。機密情報が流出したケースは確認されていないが、同庁は「不審なメールを受信したら、すぐに警察に相談してほしい」などと注意を呼び掛けている。

警視庁によると、2009年以降、政府機関や防衛・重要インフラ関連企業など30以上がサイバー攻撃を受け、少なくとも100台以上のパソコンでウイルス感染が確認された。感染パソコンは海外のサイトやサーバーに強制的に接続させられており、約9割が中国のドメインだった。

ドメインはインターネット上の住所に当たり、利用の際は管理する会社に登録する必要がある。今回判明した強制接続先のドメインは中国の法人名義などで登録されていたが、「実在する法人かどうかは確認できていない」(警視庁幹部)。

政府機関や企業を狙ったサイバー攻撃

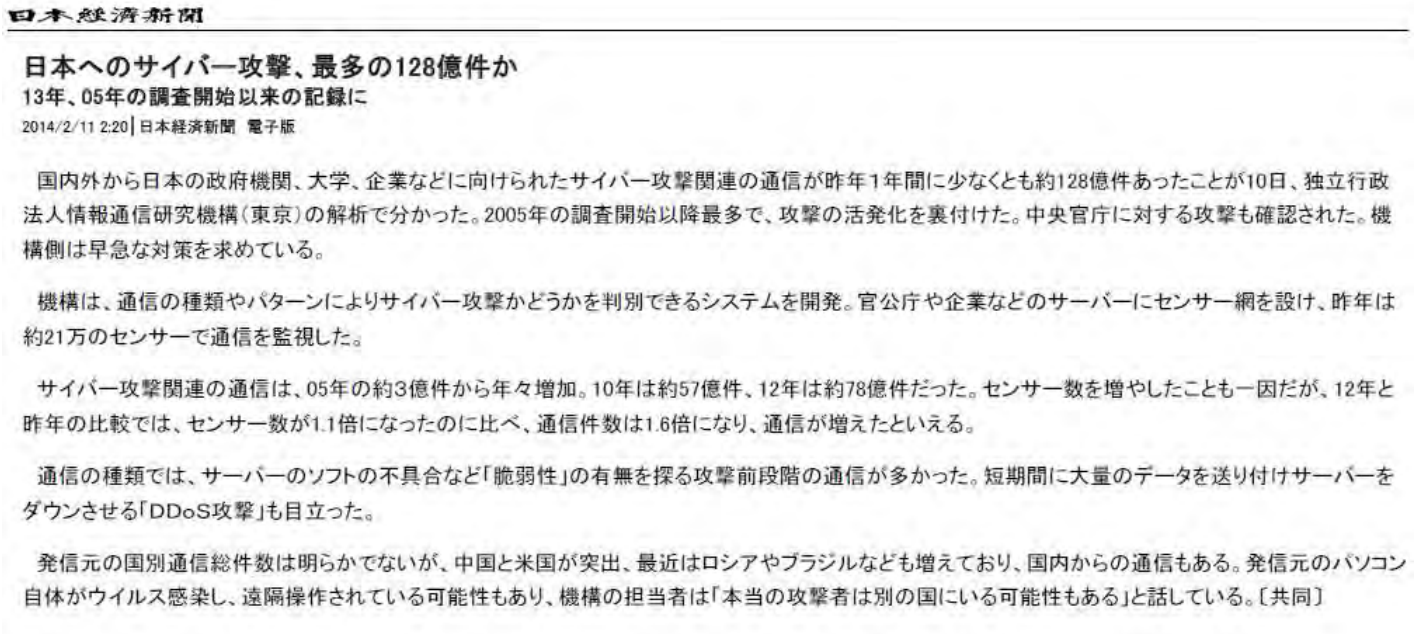
防衛関連企業のケースでは職員のパソコンがウイルス感染。11年3月から12年11月までの間、計約40万回、中国のサーバーやサイトに強制接続させられていた。キーボードでどのキーを打ったかといった情報が盗み取られた痕跡があるという。

攻撃者は事前に社員らが利用しているメール共有サービスに潜入し、名簿やメールアドレスなどの個人情報を収集。その後、入手した情報を基に実在する社員を装うなどして、標的型メールを企業や政府機関に送りつける手口が多かった。

日本経済新聞 2014年6月4日版
http://www.nikkei.com/article/DGXNASDG0403Q_U4A600C1CR8000/

サイバー攻撃統計

- 2013年度，日本の政府機関，大学，企業等を標的としたサイバー攻撃関連通信数は128億件以上(NICT調べ，日経報道)
  - 05年は約3億件，10年は約57億件，12年は約78億件



日本経済新聞

日本へのサイバー攻撃、最多の128億件か

13年、05年の調査開始以来の記録に

2014/2/11 2:20 | 日本経済新聞 電子版

国内外から日本の政府機関、大学、企業などに向けられたサイバー攻撃関連の通信が昨年1年間に少なくとも約128億件あったことが10日、独立行政法人情報通信研究機構（東京）の解析で分かった。2005年の調査開始以降最多で、攻撃の活発化を裏付けた。中央官庁に対する攻撃も確認された。機構側は早急な対策を求めている。

機構は、通信の種類やパターンによりサイバー攻撃かどうかを判別できるシステムを開発。官公庁や企業などのサーバーにセンサー網を設け、昨年は約21万のセンサーで通信を監視した。

サイバー攻撃関連の通信は、05年の約3億件から年々増加。10年は約57億件、12年は約78億件だった。センサー数を増やしたことも一因だが、12年と昨年の比較では、センサー数が1.1倍になったのに比べ、通信件数は1.6倍になり、通信が増えたといえる。

通信の種類では、サーバーのソフトの不具合など「脆弱性」の有無を探る攻撃前段階の通信が多かった。短期間に大量のデータを送り付けサーバーをダウンさせる「DDoS攻撃」も目立った。

発信元の国別通信総件数は明らかでないが、中国と米国が突出、最近はロシアやブラジルなども増えており、国内からの通信もある。発信元のパソコン自体がウイルス感染し、遠隔操作されている可能性もあり、機構の担当者は「本当の攻撃者は別の国にいる可能性もある」と話している。〔共同〕

日経新聞電子版 2014年2月11日配信より

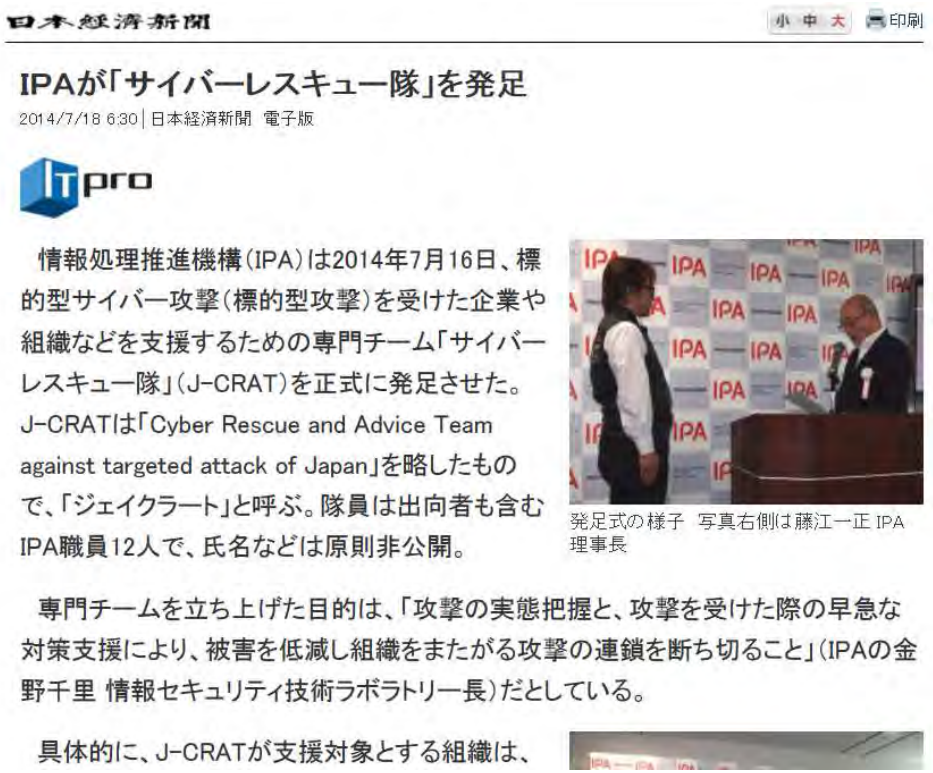
対策の動き(1)

- NECサイバーセキュリティ・ファクトリー
  - サイバーセキュリティサービス支援のためのプラットフォーム
  - 国際刑事警察機構(インターポール)と提携し(2012), サイバー犯罪の調査・分析のための施設(The I OL Glob al Complex for Innovation)設立

※写真はNECのWebページより
http://jpn.nec.com/press/201212/20121218_01.html

対策の動き(2)

- 2014年 7月　情報処理推進機構(IPA),サイバーレスキュー隊 J-CRAT(Cyber Rescure and Advice Team against targeted attack of Japan)設立
  - 攻撃把握と深刻度に関する助言，対策着手のための助言による支援



日本経済新聞　小 中 大 印刷

IPAが「サイバーレスキュー隊」を発足

2014/7/18 6:30 | 日本経済新聞 電子版

ITpro

情報処理推進機構（IPA）は2014年7月16日、標的型サイバー攻撃（標的型攻撃）を受けた企業や組織などを支援するための専門チーム「サイバーレスキュー隊」（J-CRAT）を正式に発足させた。J-CRATは「Cyber Rescue and Advice Team against targeted attack of Japan」を略したもので、「ジェイクラート」と呼ぶ。隊員は出向者も含むIPA職員12人で、氏名などは原則非公開。

発足式の様子　写真右側は藤江一正 IPA理事長

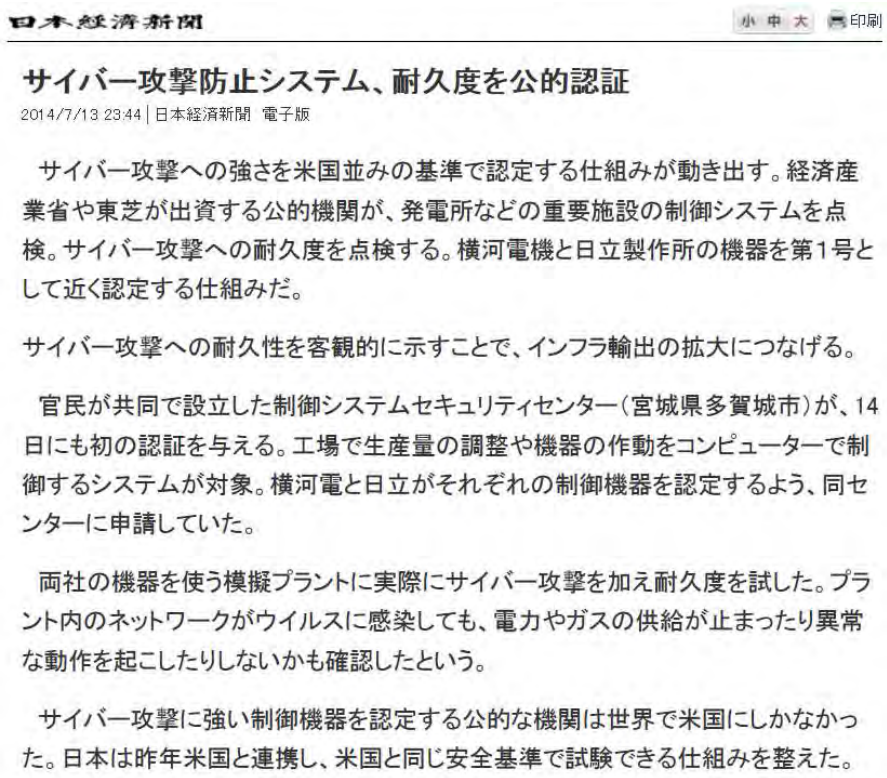
専門チームを立ち上げた目的は、「攻撃の実態把握と、攻撃を受けた際の早急な対策支援により、被害を低減し組織をまたがる攻撃の連鎖を断ち切ること」（IPAの金野千里 情報セキュリティ技術ラボラトリー長）だとしている。

具体的に、J-CRATが支援対象とする組織は、

日経新聞より
http://www.nikkei.com/article/DGXNASFK1702I_X10C14A7000000/

対策の動き(3)

- 重要施設の制御システムのセキュリティ対策の評価
- 宮城県に官民共同による制御システムセキュリティセンター(CSSC)設置
- サイバー攻撃への耐性の認証制度作り



日本経済新聞　小 中 大　印刷

サイバー攻撃防止システム、耐久度を公的認証

2014/7/13 23:44 | 日本経済新聞 電子版

サイバー攻撃への強さを米国並みの基準で認定する仕組みが動き出す。経済産業省や東芝が出資する公的機関が、発電所などの重要施設の制御システムを点検。サイバー攻撃への耐久度を点検する。横河電機と日立製作所の機器を第1号として近く認定する仕組みだ。

サイバー攻撃への耐久性を客観的に示すことで、インフラ輸出の拡大につなげる。

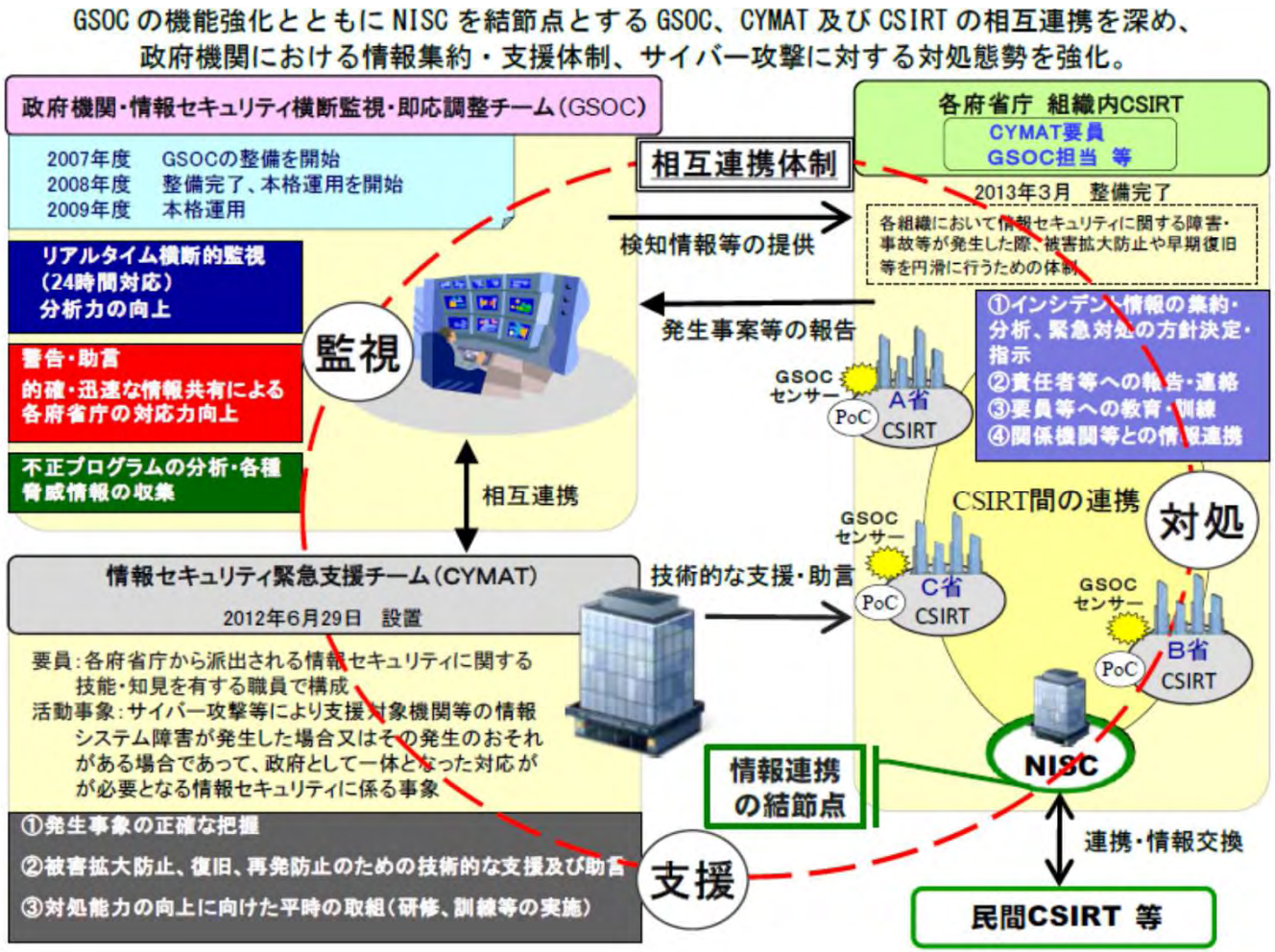
官民が共同で設立した制御システムセキュリティセンター（宮城県多賀城市）が、14日にも初の認証を与える。工場で生産量の調整や機器の作動をコンピューターで制御するシステムが対象。横河電と日立がそれぞれの制御機器を認定するよう、同センターに申請していた。

両社の機器を使う模擬プラントに実際にサイバー攻撃を加え耐久度を試した。プラント内のネットワークがウイルスに感染しても、電力やガスの供給が止まったり異常な動作を起こしたりしないかも確認したという。

サイバー攻撃に強い制御機器を認定する公的な機関は世界で米国にしかなかった。日本は昨年米国と連携し、米国と同じ安全基準で試験できる仕組みを整えた。

日経新聞Webより
http://www.nikkei.com/article/DGXNASDF11H0T_T10C14A7NN1000/?dg=1

日本における
サイバーセキュリティ強化体制



内閣官房情報セキュリティセンター 情報セキュリティ政策会議
「サイバーセキュリティ政策に係る年次報告(2013年度)」 2014年7月10日より

日本の情報セキュリティ研究開発取組

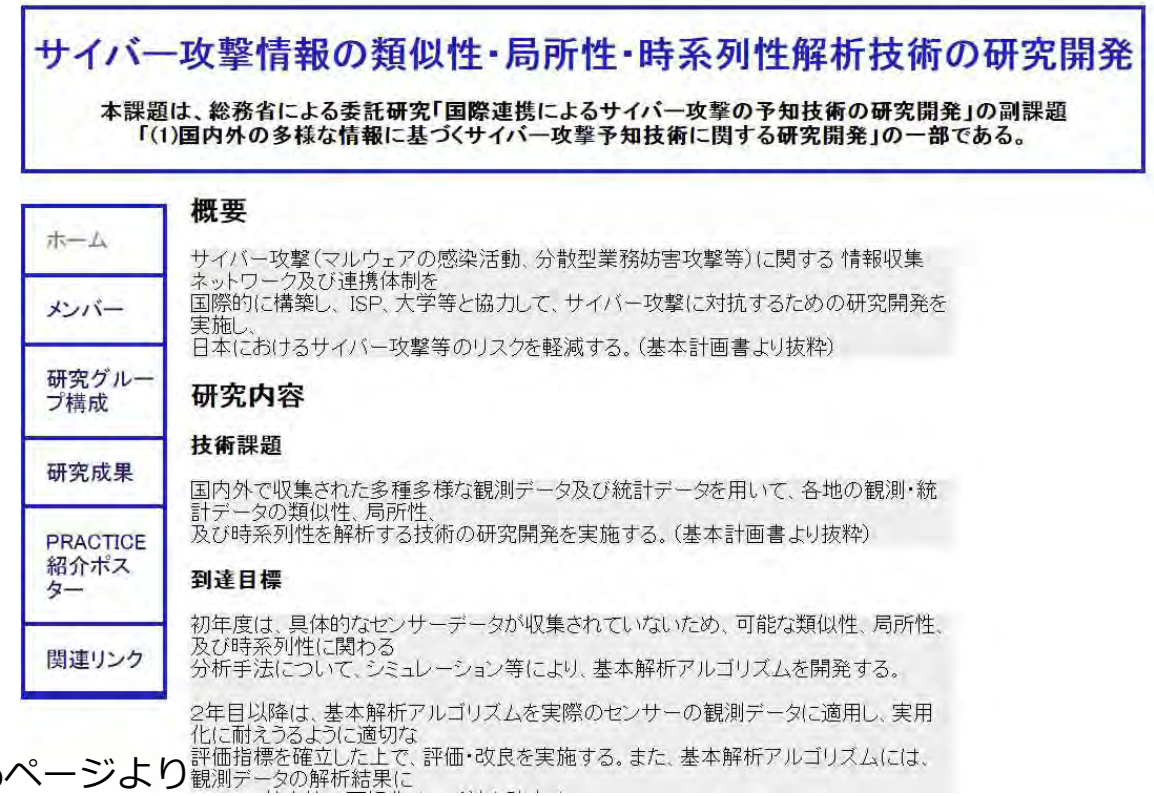
- サイバー攻撃の検知・防御能力の向上
  - 最新の攻撃動向や現状の課題等の情報/データ共有等

- 社会システム等を防護するためのセキュリティ技術の強化
  - 社会の重要インフラを構成する制御システムのセキュリティ対策強化等
- 産業活性化につながる新サービス等におけるセキュリティ研究開発
  - 医療健康，農業，ビッグデータ絵の利活用などに関するセキュリティ研究
- 情報セキュリティのコア技術の保持
  - 暗号(CRYPTREC)技術の研究，評価．IoT時代の認証

※NISC資料「情報セキュリティ研究開発戦略(改訂版)」2014年7月10より

PRACTICE project

- 総務省委託，国際連携による「サイバー攻撃予知･即応技術の研究開発」PRACTICE(Proactive Response Against Cyber-attacks Through International Collaborative Exchange)
  - 一部課題を，九州大を中心とするチームで担務



サイバー攻撃情報の類似性･局所性･時系列性解析技術の研究開発

本課題は、総務省による委託研究「国際連携によるサイバー攻撃の予知技術の研究開発」の副課題
「(1)国内外の多様な情報に基づくサイバー攻撃予知技術に関する研究開発」の一部である。

ホーム
メンバー
研究グループ構成
研究成果
PRACTICE紹介ポスター
関連リンク

概要

サイバー攻撃（マルウェアの感染活動、分散型業務妨害攻撃等）に関する 情報収集ネットワーク及び連携体制を
国際的に構築し、ISP、大学等と協力して、サイバー攻撃に対抗するための研究開発を実施し、
日本におけるサイバー攻撃等のリスクを軽減する。（基本計画書より抜粋）

研究内容

技術課題

国内外で収集された多種多様な観測データ及び統計データを用いて、各地の観測･統計データの類似性、局所性、
及び時系列性を解析する技術の研究開発を実施する。（基本計画書より抜粋）

到達目標

初年度は、具体的なセンサーデータが収集されていないため、可能な類似性、局所性、及び時系列性に関わる
分析手法について、シミュレーション等により、基本解析アルゴリズムを開発する。

2年目以降は、基本解析アルゴリズムを実際のセンサーの観測データに適用し、実用化に耐えうるように適切な
評価指標を確立した上で、評価･改良を実施する。また、基本解析アルゴリズムには、観測データの解析結果に

Webページより
http://itslab.inf.kyushu-u.ac.jp/cyber/jp/index.html

Benesse個人情報漏洩インシデント

- Benesseの持つ顧客情報が外部に漏洩．他社からのDMを受けた顧客からの問い合わせを受けて発覚
  - DMに記載された宛先の住所が，Benesseのみに登録した情報と一致
  - インサイダーの犯行による情報漏洩
  - 個人情報の流通経路が明るみに

ITproまとめ　日経コンピュータ

ベネッセコーポレーション

2014/07/17
斉藤 栄太郎＝日経コンピュータ （筆者執筆記事一覧）

記事一覧へ >>

シェア　ツイート　B! ブックマーク

ベネッセコーポレーションは2014年7月9日、同社の通信教育サービスに関する顧客情報約760万件が外部に漏洩したことを確認したと発表した。漏洩した情報は、保護者および子供の名前、住所、子供の生年月日、性別など。

情報漏洩が発覚したきっかけは、6月26日以降、サービス利用者から「個人情報が漏洩したのでは」という問い合わせが急増したこと。問い合わせがあったユーザーに対し、教育関連事業を運営するITベンダー（後にジャストシステムと判明）からダイレクトメールが届き、記載された宛先住所がベネッセにのみ登録した情報と同一だったケースがあったことなどから、漏洩が強く疑われることとなった。

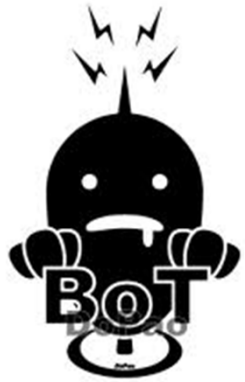
その後、個人情報を不正に持ち出して名簿業者に売った人物として、ベネッセが顧客データベースの管理を委託していた外部企業の派遣SEが浮上。警視庁は15日付けでベネッセから提出された不正競争防止法違反での刑事告訴を受理した。今後、同法違反の疑いで逮捕する見込みだ。親会社のベネッセホールディングスは同日、外部専門家をトップとする「個人情報漏えい事故調査委員会」を発足させている。

日経コンピュータWebページより
http://itpro.nikkeibp.co.jp/atcl/column/14/494329/071600001/?k3

第Ⅱ部

Bitcoin, リアルマネートレード

サイバー空間における
サービスと問題



Bitcoin
(ビットコイン)

Bitcoin とは？

■仮想通貨

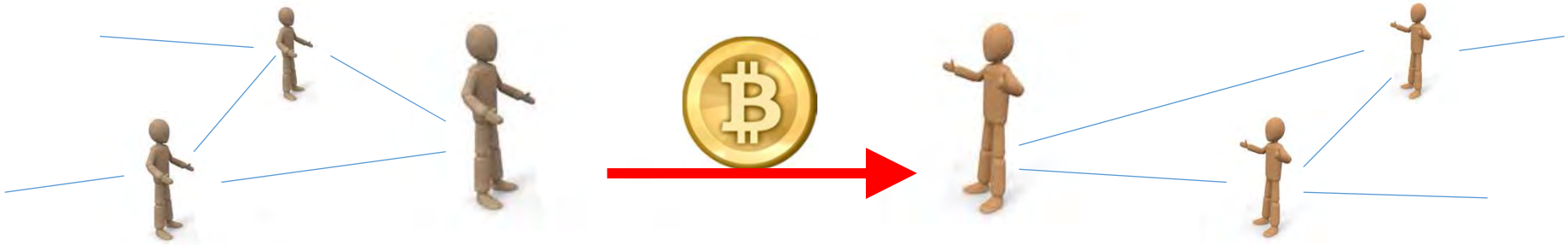
- ●法定通貨でない
- ●デジタルデータ
- ●世界中に認知
- ●合法／非合法

ダイヤモンド社
http://www.diamond.co.jp/book/9784478028445.html

Bitcoin とは？

■ネットワーク分散型メカニズム

●どの２ユーザも直接取引き可（銀行不要）



●取引きの安全性（二重使用や偽造の不可）を次に帰着：

➢解の探索に時間（10分程度）を要する数学問題

➢解けたら直ちにブロードキャストし共有

電子現金・電子通貨の歴史

■第1期
- “PayPal”
- ネット経由でクレジットカード
- インターネット

■第2期
- “Edy” “Suica” “Square”
- 中央管理型電子マネー
- 非接触ICカード

ネット

■第3期
- “Bitcoin”
- 分散型仮想通貨
- スマホ, インターネット

Bitcoinの歴史

- 2008: **Satoshi Nakamoto** 氏（ｶﾘﾌｫﾙﾆｱ州, 60歳前後）が論文をアップロード
  - “Bitcoin: A Peer-to-Peer Electronic Cash System”
- 2009: ｻｰﾋﾞｽ運用開始
- 2011: 広く知られる
- 2013, Apr: 通貨量が100億 米ドル超え
- 2013, July: タイ“非合法”
- 2013, Aug: アメリカ“合法”
- 2013, Aug: ATM 換金運用（米ドル）

Bitcoinに対する法規制

■“Singapore clamps down on Bitcoin exchanges with new regulations”…PC world, Mar. 13, 2014

●シンガポールの政府関係者は，マネーロンダリングやテロリストの金の浄化の目的に使用されるのを防ぐ目的から，Bitcoinの為替取引を規制する計画を発表

http://www.pcworld.com/article/2108421/singapore-clamps-down-on-bitcoin-exchanges-with-new-regulations.html

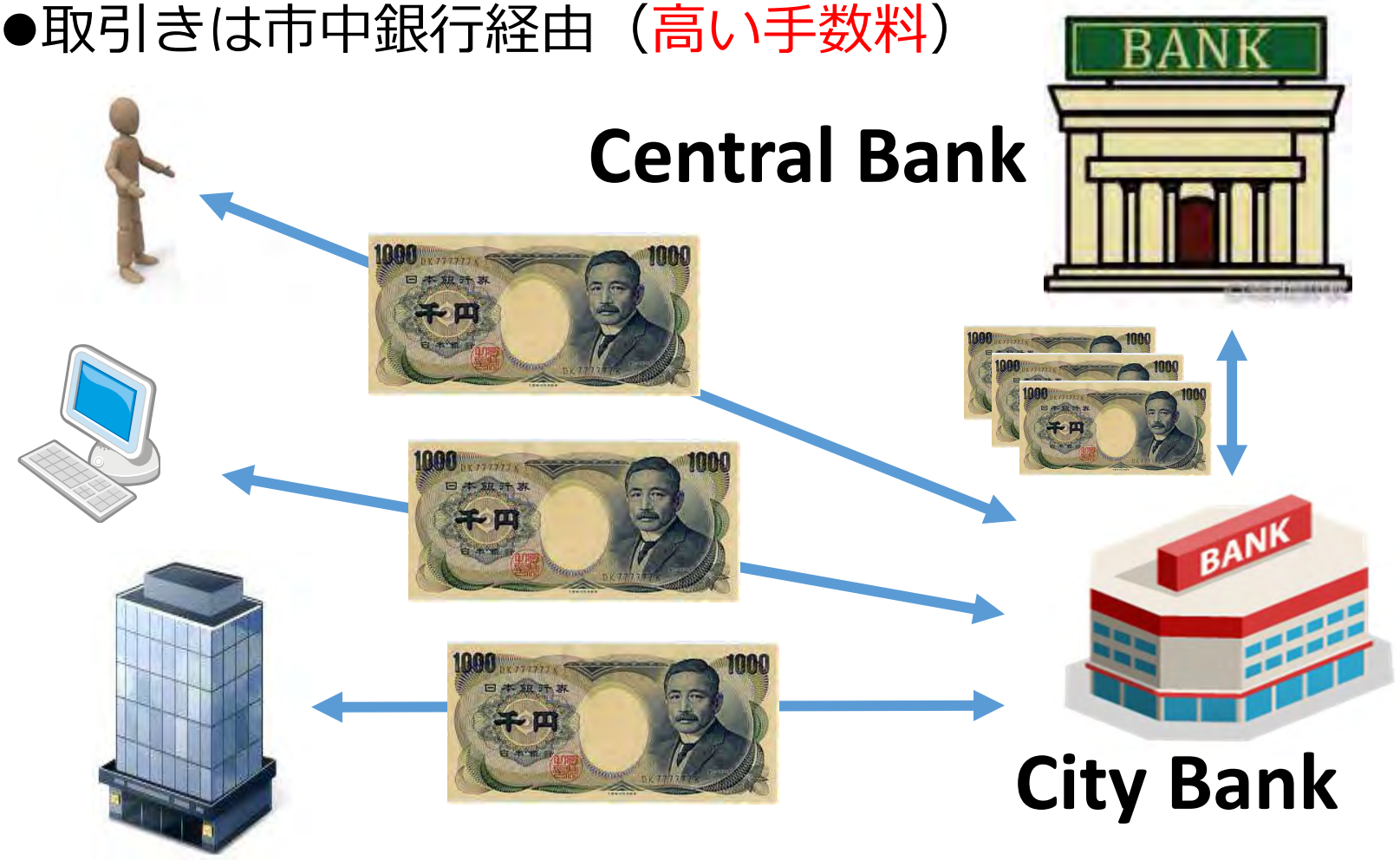
Bitcoinの長所

1. 速い！決済
2. 安い！手数料 ←ビットコインのスピリット
3. 簡単！by スマホ
4. 容易！海外送金
5. 安心！匿名性

現在の現金は中央管理型通貨

■中央銀行は通貨を管理

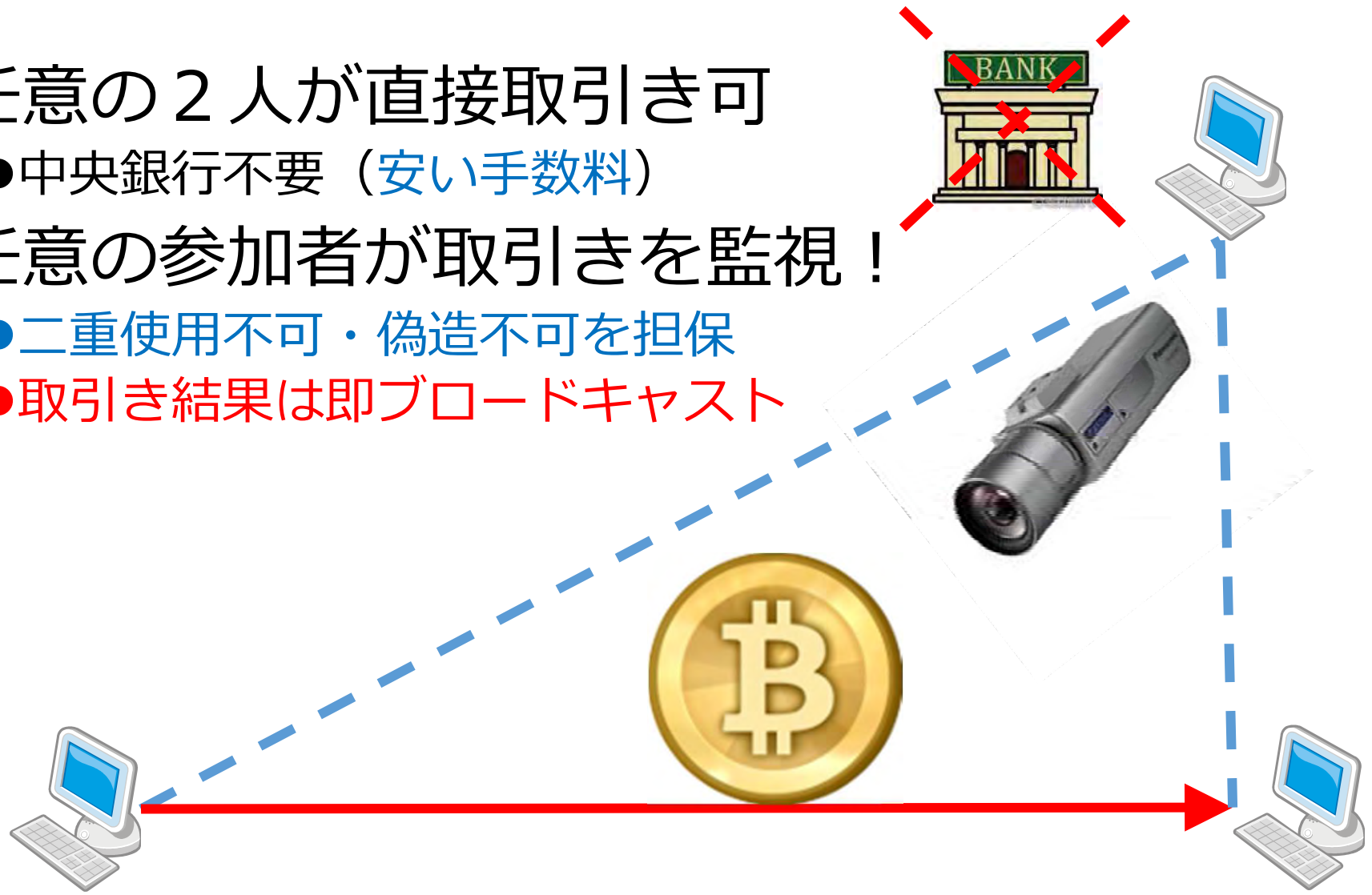
●取引きは市中銀行経由（高い手数料）



Bitcoinは分散型通貨

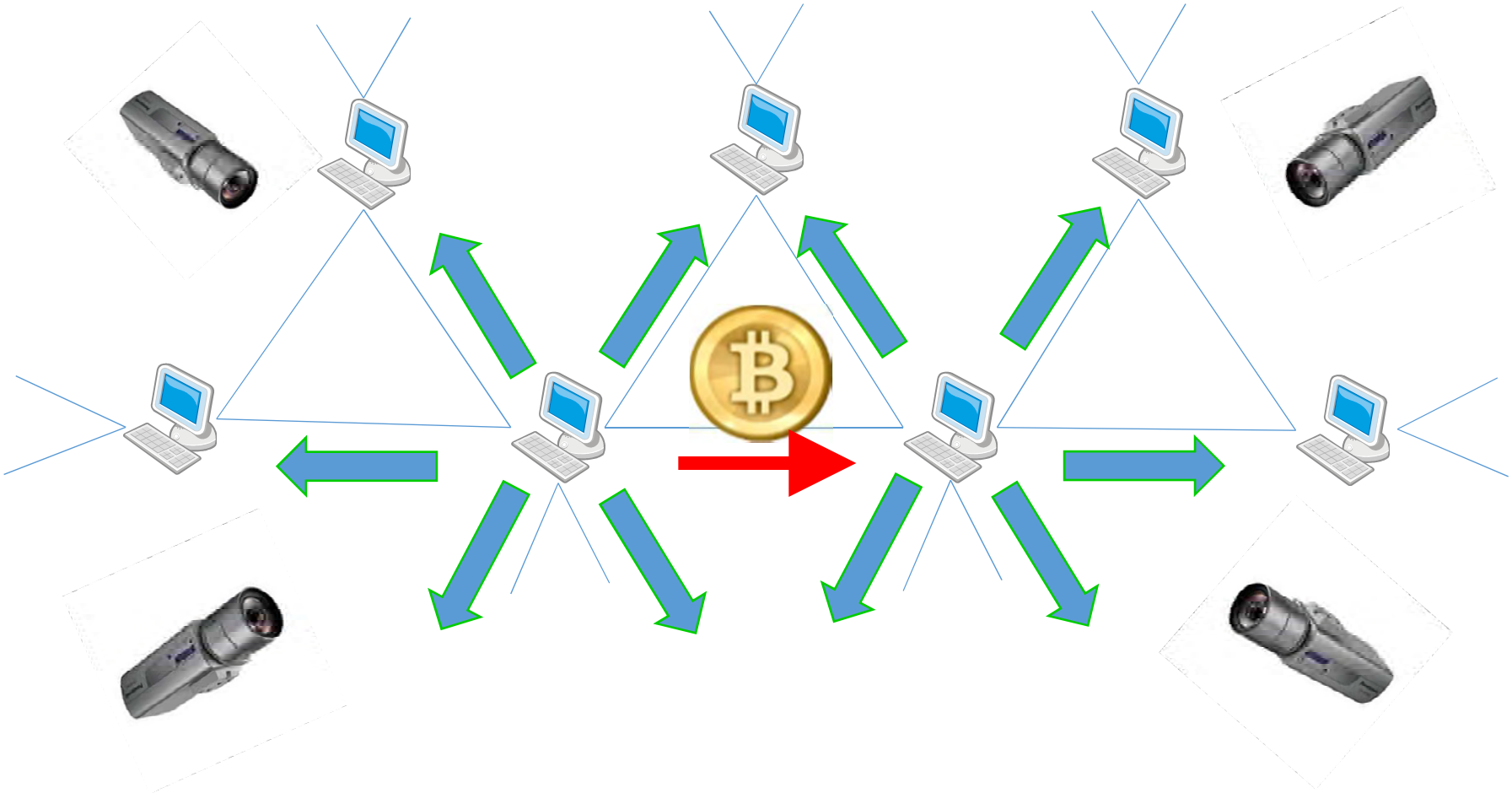
■任意の２人が直接取引き可
- ●中央銀行不要（安い手数料）

■任意の参加者が取引きを監視！
- ●二重使用不可・偽造不可を担保
- ●取引き結果は即ブロードキャスト



取引き結果は即ブロードキャスト

■ネットワーク上の参加者全員が取引きを見届ける



Bitcoinはサイバー空間上の仮想通貨

	カテゴリ	タイプ	Currency-Type	管理者／発行者
	現金	中央管理型	法定通貨	中央銀行／中央銀行
	Bitcoin	分散型	仮想通貨	参加者／採掘者

Bitcoinと金(Gold)

■Bitcoin

- ●総通貨量に上限有り
- ●容易に壊れない
- ●分割・結合可能
- ●Miningにより発行

＝

■Gold

- ●総量に上限有り
- ●容易に壊れない
- ●分割・結合可能
- ●採掘により市場へ

http://gigazine.net

Bitcoinの採掘 (Mining)

■採掘者は一定時間以上の時間を要する数学の問題にトライ

- ●計算能力の高いｺﾝﾋﾟｭｰﾀでも10分程掛かるように自動調整

■解けた者は取引きの完了に寄与すると共に，25+α[BTC]をもらえる

guru8.net

www.cryptocoinsnews.com

Bitcoinのサイバーリスク

■“Bitcoin-mining malware reportedly found on Google Play”… cnet.com, Apr.24, 2014

- スマホの壁紙アプリが
  Miningのボットに！
- ボット：コンピュータに感染し、ネットを通じ外部から操ることを目的として作成されたプログラム

http://www.cnet.com/news/bitcoin-mining-malware-reportedly-discovered-at-google-play/

http://androidfreeware.net/download-beating-heart-live-wallpaper.html

Bitcoin: サイバー空間が違法取引の場に!?

■容易な海外送金

→送金目的を隠ぺいしやすい

■武器

■ドラッグ

等々

kabegami.org “Weapon buying and Selling”

Bitcoinが無くなった！サイバー事件

- “Mt. Gox files for bankruptcy, hit with lawsuit” …
  Reuters, Feb., 28, 2014
  - 日本のBitcoin取引所 “Mt. Gox”が破産を申請

- 約5億ドルの損失

http://www.reuters.com/article/2014/02/28/us-bitcoin-mtgox-bankruptcy-idUSBREA1R0FX20140228

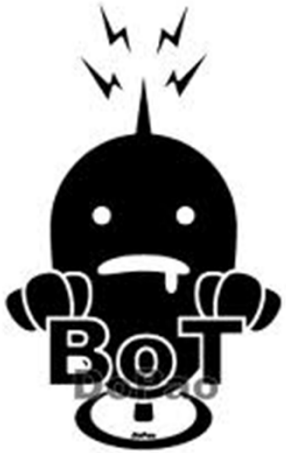
Mt.Gox事件「取引きの展性」

取引き展性攻撃

■支払い処理が完了していないように見せ掛けて二重払いを強いるハッキング手法

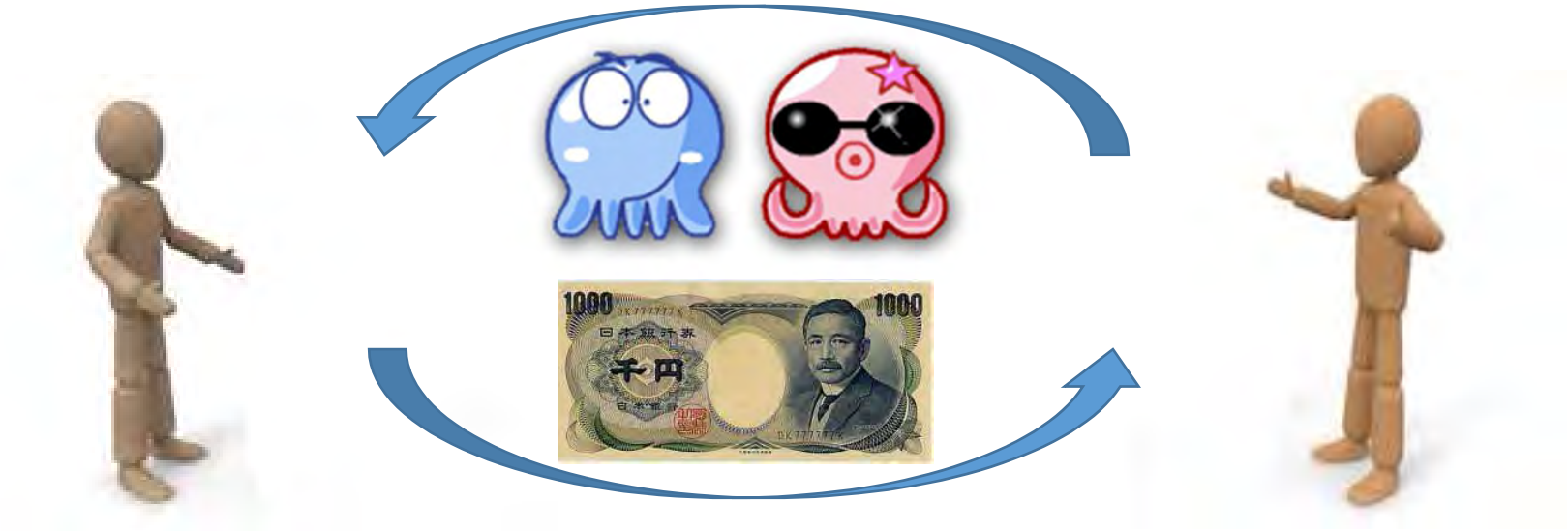
■デジタル署名の正当性を保ったまま，取引きデータが複数通りのハッシュ値を持ちうるようにデータを変化させた（つまり実装上のバグを突いた。。）

リアルマネートレード
(Real Money Trade)



リアルマネートレードとは？ (Real Money Trade，RMT)

■オンラインゲームなどで，ゲーム内で得られた通貨やアイテムなどの架空財産を現実世界で売買すること



リアルマネートレード(RMT)の背景

■オンラインゲームの市場が拡大

●注目を集めているのはMMORPG
（Massively Multiplayer Online Role-Playing Game）

■ゲーム会社：仮想世界の秩序を維持, のはず

ところが…

■ゲームの不正行為の問題が増加

■ゲームを楽しむという本来の目的から外れて
経済的利益の獲得手段に

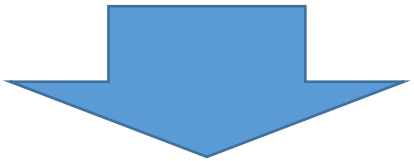
ゲームボット (Game Bot)

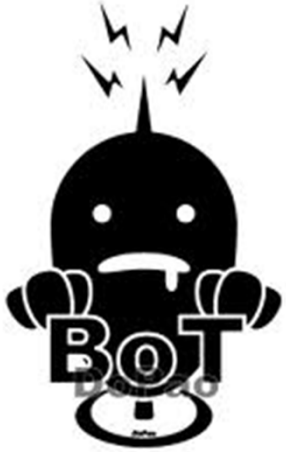
■BOT：キャラクターを自動的に操作するプログラム

■自動的に敵を倒す

■1日24時間働き続ける

- ●レベルを上げる，仮想通貨を稼ぐ，etc.





■結果ものすごい数のアイテムを取得

→RMT; 現金と交換

■ゲーム内のバランスを壊す

■一般プレイヤーにとって邪魔！

- ●ゲーム業者はRMTを規約で禁止している

リアルマネートレード業者

■BOTを製作

■様々な役割のBOT

- ●労働者：仮想世界の中で仮想財産を集める
- ●徴収者：仮想財産を労働者から販売者に転送する
- ●販売者：仮想財産を一般ﾕｰｻﾞに売りお金を稼ぐ

■休みなくキャラクタを動かす

- ●効率よくゲーム内の資産を得る

■多数のゲームアカウントでキャラを育成

収入増