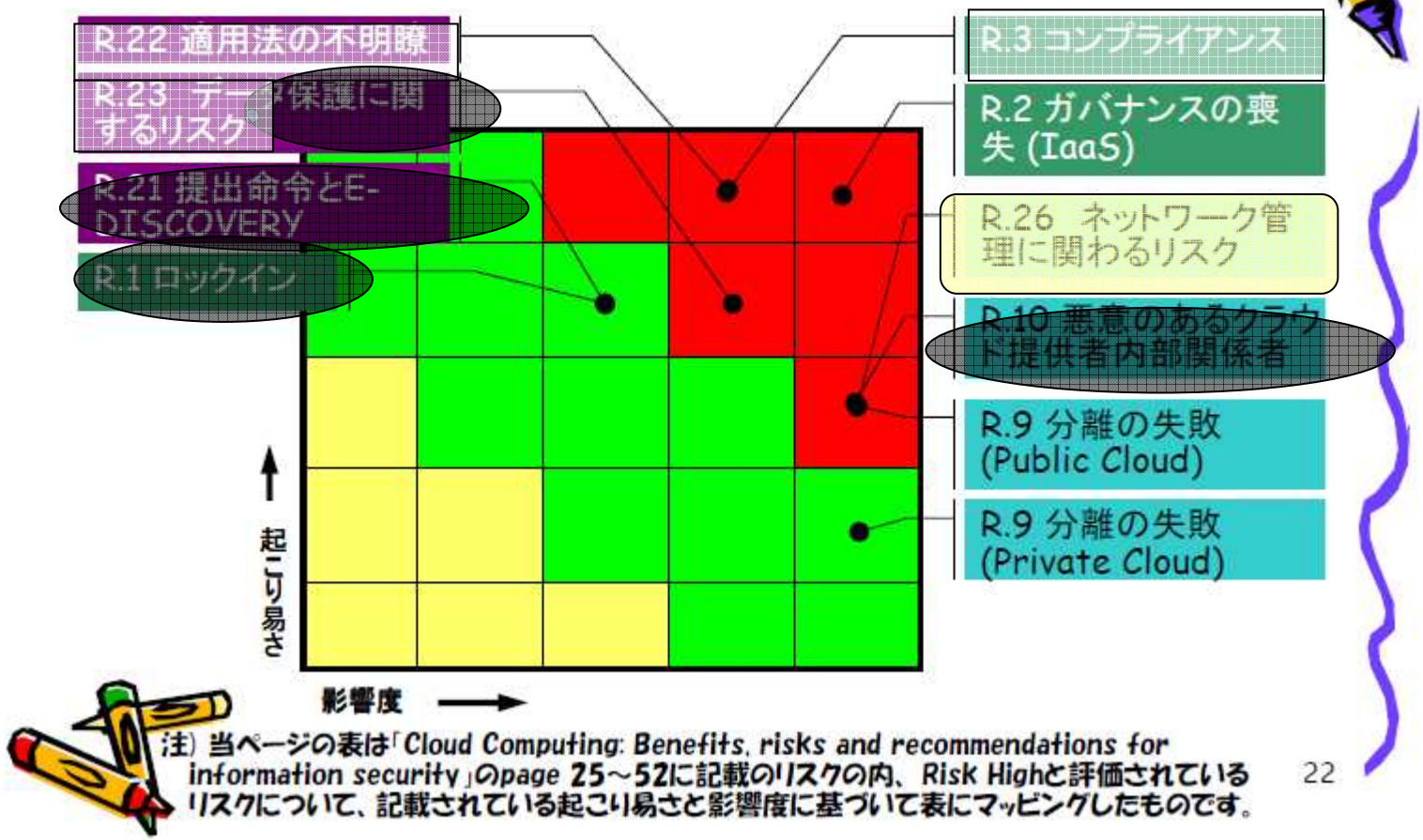
新しいパラダイムでのITリスク

クラウドコンピューティングに対するリスク評価

日本セキュリティ・マネジメント学会 第24回全国大会

ENISAによるリスク評価Highの項目



注) 当ページの表は「Cloud Computing: Benefits, risks and recommendations for information security」のpage 25～52に記載のリスクの内、Risk Highと評価されているリスクについて、記載されている起こり易さと影響度に基づいて表にマッピングしたものです。

22

クラウド時代のリスク

- 従来からの
  自然
- IT時代(I
  ウイ 固定、
  内部犯
- ネットワーク時代にな のリスク
  ネットワークマネージメント、BOT。。。
- クラウド時代になってのリスク
  分離、ガバナンスの喪失

パラダイムの変化

- 従来
  価値は基本的に交換価値で評価される
  価値は使用されれば費消する
- IT（情報データ）の登場
  情報は無限に等価で複製可能
  従来の経済理論崩壊のリスク
- ネットワークの登場で更に距離も自由に
- クラウドの登場
  IT処理自体が無限に増殖する

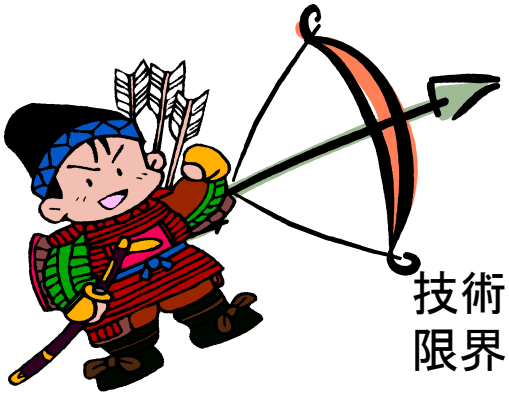
➔このリスクは

ITリスクの限界

	ITでの影響	一般
自然災害	データの滅失 事務処理の停止	死者、負傷者 財産の滅失
テロ	データの滅失 機能の停止	死者、負傷者 財産の滅失
ウイルス	データの滅失 事務処理の停止	死者、身体的影響

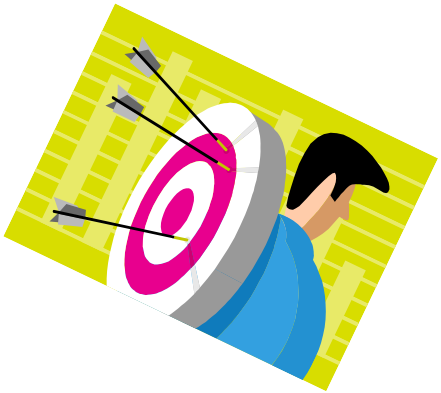
ITにおけるリスクで身体的なリスクは直接的にはありえない

ITリスクの限界



技術的
限界

情報で
身体的
危害は
無理

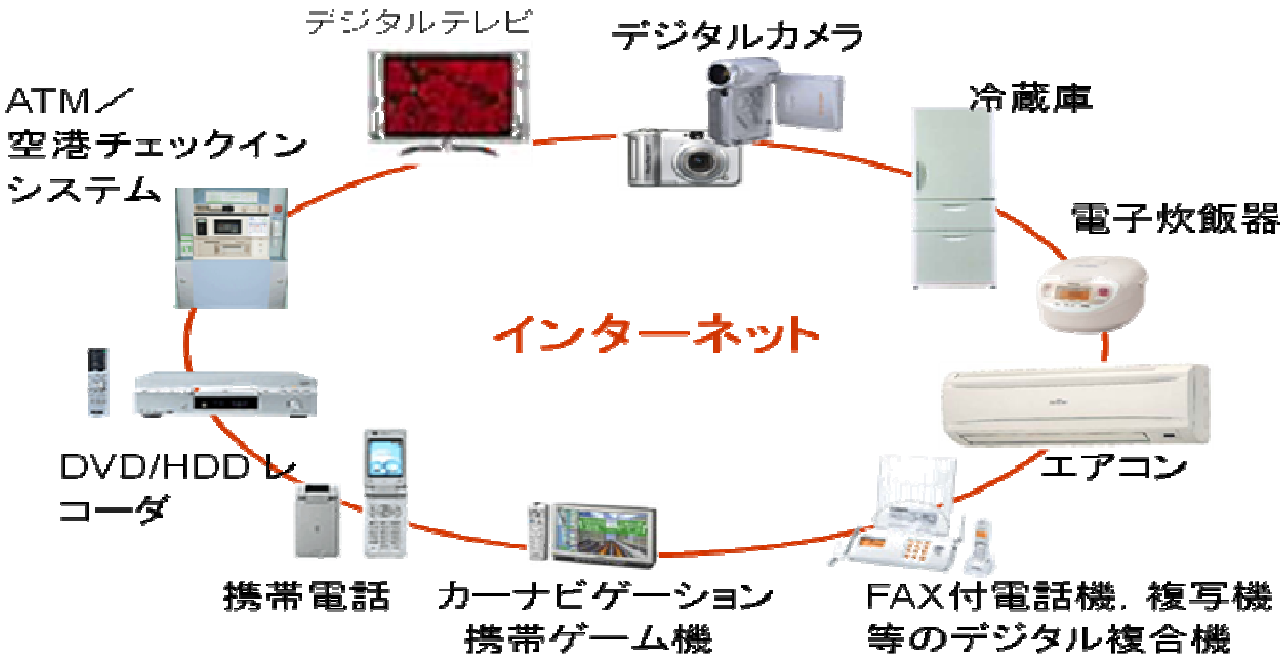


実行者の常識、
良識

ITリスクの限界

- 実行者の常識、良識
  サイバーテロはともかく通常の
  Net参加者はそのモラルが存在
- 情報自体で身体的危害は無理
  あくまでその情報操作による間接的リスク
- 技術自体の限界
  個人の所有するPCではその能力に限界

何でもつながる時代の到来



済賀　宣昭 「組込みシステム用語早わかり」2006年オーム社刊　より

パラダイムの変化

- 実行者の常識、良識
  Net参加者の増大、例えばモラルが確立しない若年者でモラルは崩れないか
- 情報自体で身体的危害は無理
  ITには情報系だけでなく制御系も
- 技術自体の限界
  クラウドで無限の利用が可能に

仮説

クラウドによるパラダイムの変化により

- モラルの確立しない若年ユーザーの手により
- クラウドによって増殖した技術を使って
- Net家電など制御系へのインシデントにより

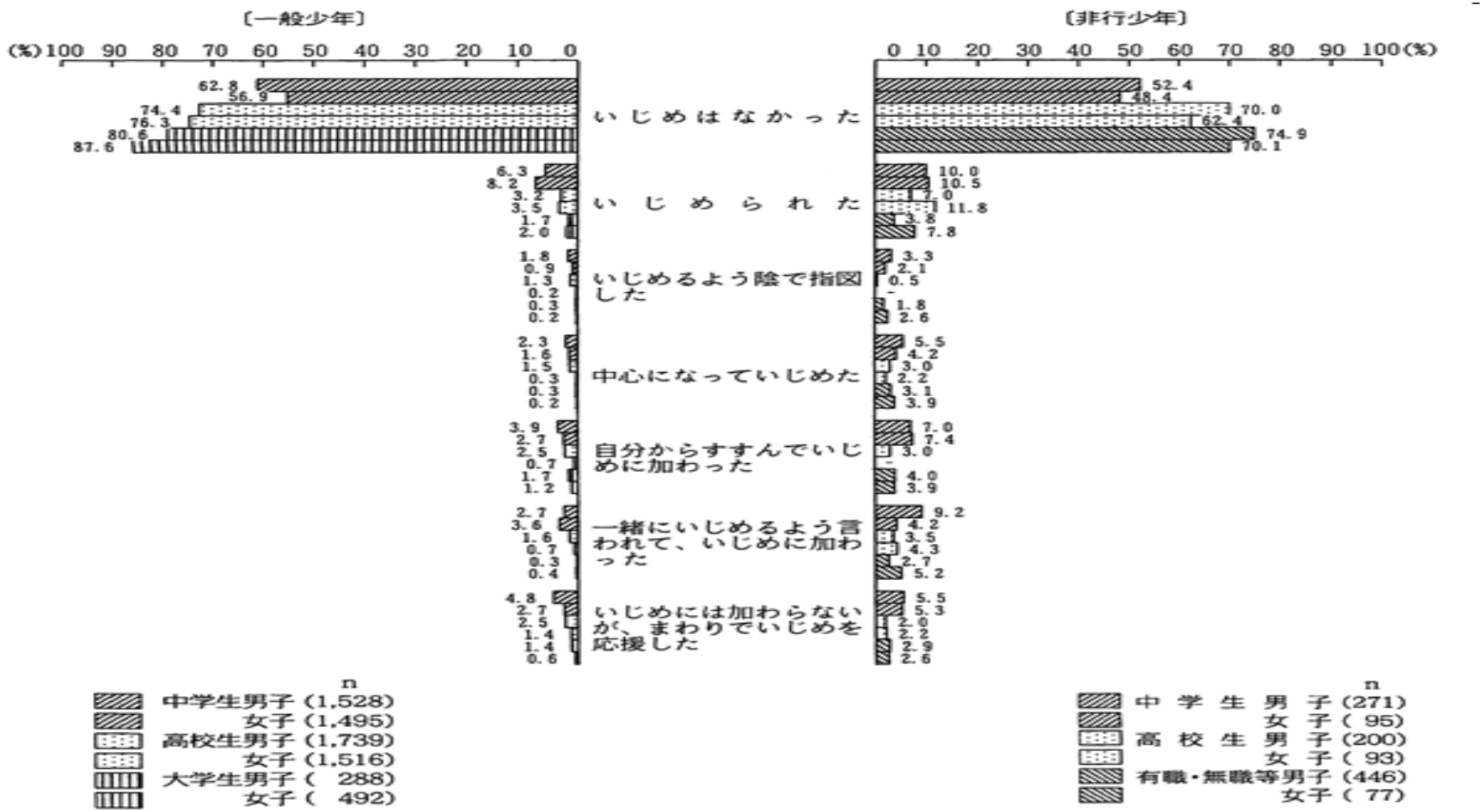
初めて身体への直接的なリスクが発生する

仮説
クラウドによるパラダイムの変化により

- モラルの確立しない若年ユーザーの手により
- クラウドによって増殖した技術を使って
- Net家電など制御系へのインシデントにより

初めて身体への直接的なリスクが発生する

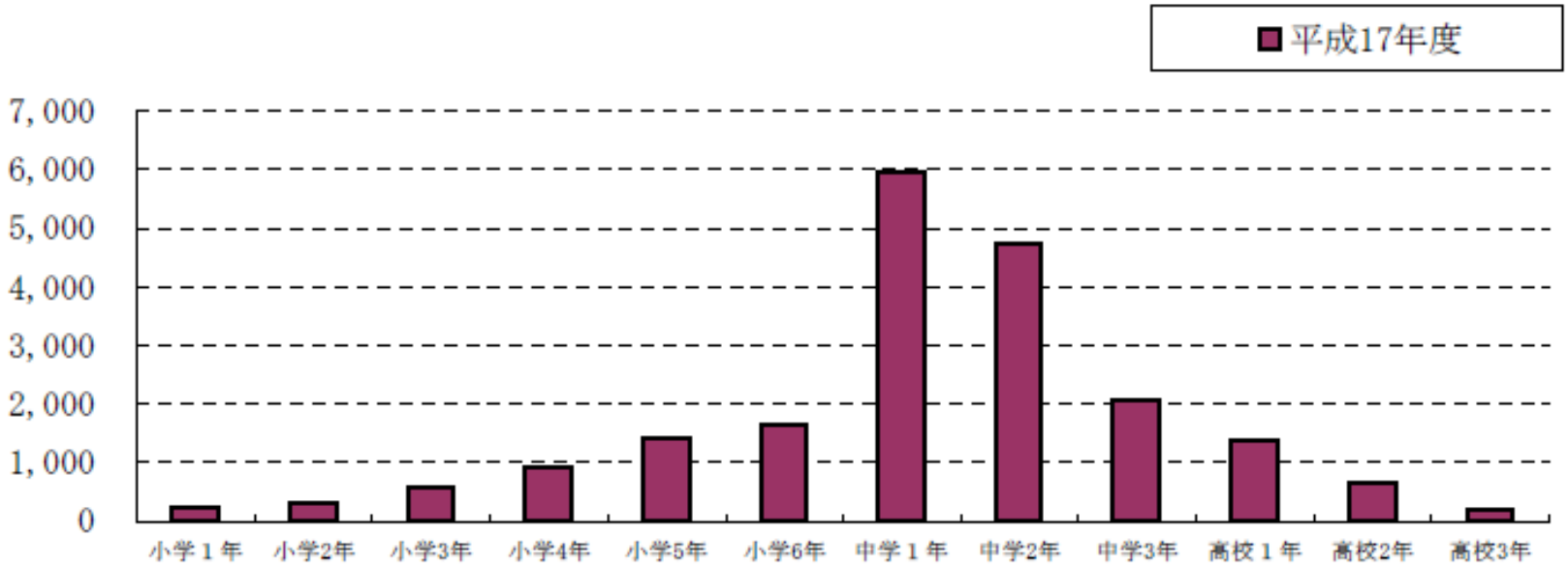
モラルの確立しない若年ユーザー



非行原因に関する総合的研究調査（第3回） 平成11年3月総務庁青少年対策本部

モラルの確立する前の若年

（２－４）　学年別いじめの発生件数



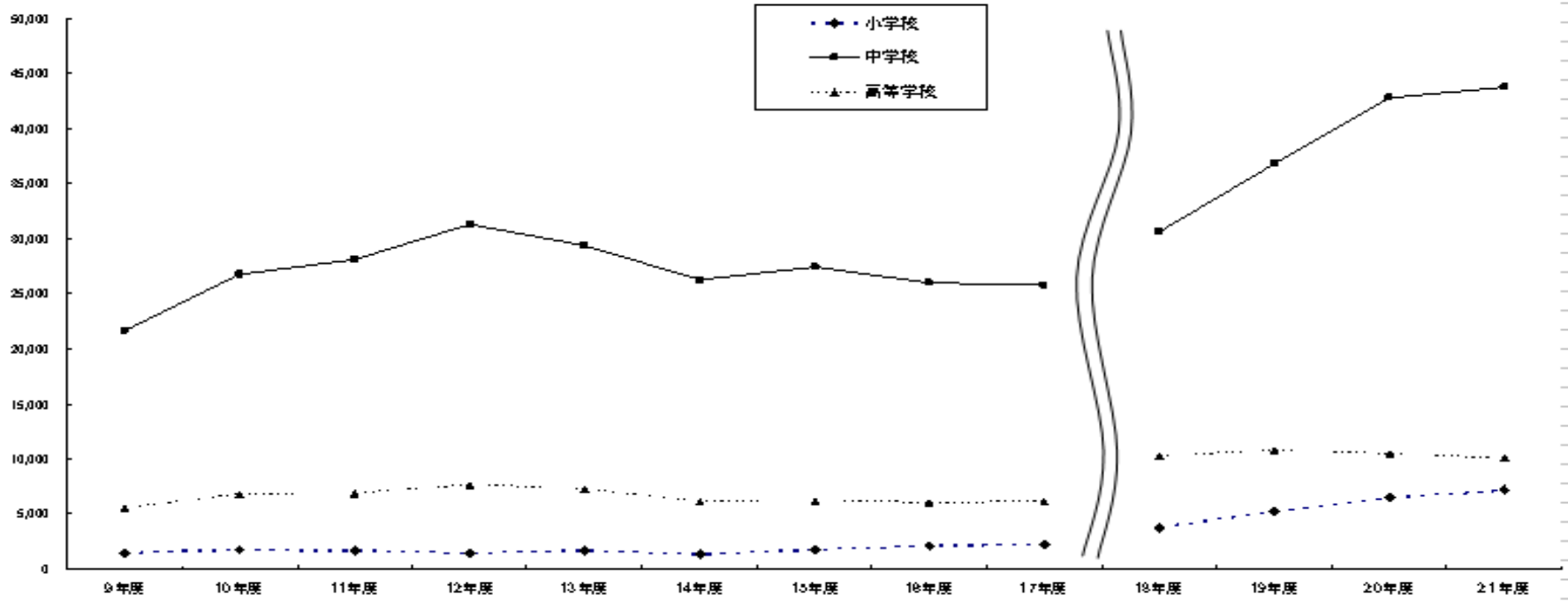
www.mext.go.jp/b_menu/houdou/18/09/06091103/002.pdf

- 私が担当した6件の事件すべてで加害少年は、理由があれば人に暴力を振るってもいいと思っていたと述べています。さすがに、無差別に誰に対しても暴力をとてもいいとは思ってませんけど、理由があれば、とは言っても、あの野郎気にくわないという程度の理由でもいいのですが、理由があれば人に暴力を振るってもいいと互いにまったく関係のない六件の事件で、まったくおなじように考えていたというのてす。私が付添い人になった3人は目の前で、直接私に話してくれましたし、3件の集団事件については、刑事の記録や民事の法廷で聞き出しました。私はこのことは大変なことだと思います。暴力を加えてはいけないと思っていたが、ついかっとなって、あるいは集団心理で暴力を加えたというのではないのです。人に暴力を加えることを積極的に認めているということなのです。

- いじめられても仕方のない子もいる87%（中1コース）
- むかついた相手に仕返しするは当然63%（中3コース）
- 自分の嫌いな人ならいじめてもよい36%（中2コース）
- 友人に暴力を振るったことがある42%（NHK調査）

（弁護士　　毛　利　正　道
http://www.kodomonoshiten.net/tabikasanarusyonen01.htm）

(参考3)学校内外を合計した暴力行為発生件数の推移



	9年度	10年度	11年度	12年度	13年度	14年度	15年度	16年度	17年度	18年度	19年度	20年度	21年度
小学校	1,432	1,706	1,668	1,483	1,630	1,393	1,777	2,100	2,176	3,803	5,214	6,484	7,115
中学校	21,585	26,783	28,077	31,285	29,388	26,295	27,414	25,984	25,796	30,564	36,803	42,754	43,715
高等学校	5,509	6,743	6,833	7,606	7,213	6,077	6,201	5,938	6,046	10,254	10,739	10,380	10,083
合計	28,526	35,232	36,578	40,374	38,231	33,765	35,392	34,022	34,018	44,621	52,756	59,618	60,913

(注1)平成9年度からは公立小・中・高等学校を対象として、学校外の暴力行為について調査。

(注2)平成18年度からは、公立学校に加え、国・私立学校も調査

インターネットを使う子供が“加害者”となる事件が増加

- 掲示板に「埼玉の小学生の女子を殺害する」などと十数回に渡って書き込み、補導 （千葉県　10歳女子）
『面白半分でやった。こんなに大ごとになるとは思わなかった』
- 18歳男子が自殺。「学校裏サイト」に自殺者の裸の写真を掲載するなどし、逮捕 （兵庫県　17歳男子）
『いじめではなく、罰ゲームだった』
- 同級生のIDとパスワードを使ってオンラインゲームに不正アクセスし、補導（愛知県　12歳の児童3名）
『同級生のキャラクターやアイテムを見たかった』
- 携帯電話から掲示板に「市立中学3校内に爆弾がある」などと爆破予告を書き込み、逮捕 （埼玉県　16歳男子）
『爆破予告が書き込まれた掲示板を見たことがあり、自分もやってみて周りの反応を見たかった』
- 「プロフ」*で仲間が中傷された仕返しに13歳の女子中学生に暴行し、逮捕（東京都　15歳女子ら少年少女計7人）
『書き込みが敬語ではなかった。ケンカを売るような書き込みをされた』

トレンドマイクロサイト
http://is702.jp/special/332/#netiquette-t1　より

目立つ「低年齢化」「放任」
～ 子どものインターネット利用

子どものネット利用は低年齢層に広がっており、しかも子どもは親が把握している以上に奔放にインターネットを利用していることがアンケートなどで明らかになっている。

2006年版「インターネット白書」によると、15歳以下（3～15歳）以下のインターネット利用が増加しており、利用者の約1割は中学生以下だ。ネットで知り合った同士でサッカーチームを作ると、小学生もしくは中学生が1人やって来るというわけだ。（図2）。

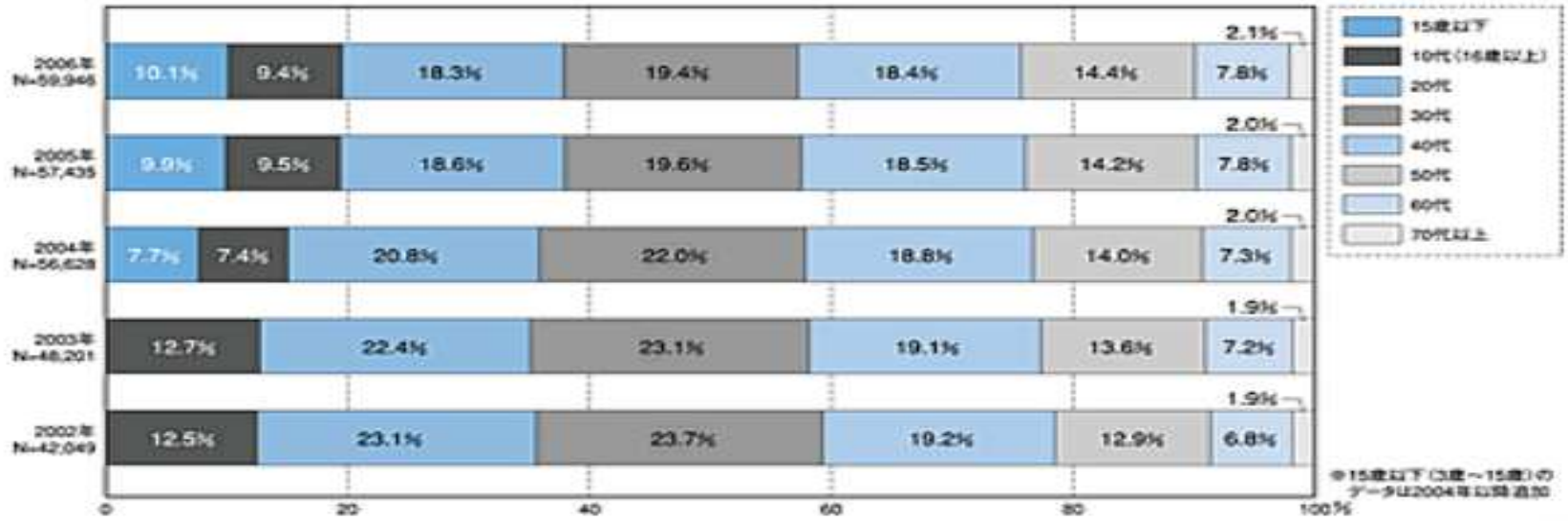


図2 インターネット利用者の年代別構成比推移（インターネット白書2006）

http://www.so-net.ne.jp/security/news/newstopics_200608_02.html

若年ハッカー達

- たった3日間で作ったロシア少年のチャットサイトに36億円の価値
- マサチューセッツ州の少年が、パリス・ヒルトン嬢の携帯電話のアドレス帳がインターネット上で公開された原因となった2005年1月のサイバー攻撃を仕掛けたとして有罪を認めた。
- 教育局のサイトなどを含む666のサイトに侵入してファイルを改ざん、昨年八月に逮捕、起訴された17歳の少年に対して広州花都区人民法院は、被害が軽微だったことから実刑を科さない旨の判決を言いわたしました。
- 中国内外のウェブサイトに不正侵入を繰り返したとして、５月３０日に内モンゴル自治区フフホト（呼和浩特市）で警察に身柄を拘束された１８歳の少年が、「政府の公式サイトへの攻撃は楽だった」などと供述
- サニィーヴのこれまでの経歴をざっと紹介しましょう。
  5歳 ： CorelDRAW(コーレルドロー：ベクトルデータを扱うDTPソフト)、Flash、HTMLの書式をマスター。ペイントショップ、フォトショップを駆使し、画像編集をこなす。
  7歳 ： MCSE(マイクロソフトが認定するシステムエンジニアの最上位資格)試験にパス。
  10歳 ： OCP(Oracle Certified Professional：Oracle社による世界共通の認定資格)およびSJC(Sun Certified java)認定の資格を取得。この頃からプロのプログラマーとして仕事をはじめる。

Security.GS

Security.GSは、2009年10月1日に活動を開始した、学生を中心とした組織

仮説
クラウドによるパラダイムの変化により

- モラルの確立しない若年ユーザーの手により
- クラウドによって増殖した技術を使って
- Net家電など制御系へのインシデントにより

初めて身体への直接的なリスクが発生する

これ知ってますか？

ブラッディマンディより

- 「いま、近所にあるコンピューター1000台に同時にハッキングして、暗号の解析作業をさせています。
これなら、あと5分くらいで暗号が解読できるはずです・・・」

（ネット上の個人ブログ等より引用：三浦クン砂糖クンは公式HPより）

既に総当りに利用している

http://internet.watch.impress.co.jp/docs/news/20091208_334134.html

INTERNET Watch

記事検索

検索

最新ニュース

- Mozilla、Android版「Firefox 4」ベータ版を公開 [2010/10/08]
- Twitterが新検索アーキテクチャー導入、ツイート処理速度が50倍に [2010/10/08]
- 「さくらのVPS」の対応OSが5種・10バージョンに拡充、UbuntuやDebianなども [2010/10/08]
- Operaも、Adobeの「Open Screen Project」へ参加

セキュリティにクラウドの闇、Amazon EC2悪用の総当たり攻撃も

ラックは8日、2009年の情報セキュリティ動向を総括する説明会を開催した。近年、「Amazon EC2」などに代表されるクラウドサービスがサーバーコストの削減につながるとして人気を集めているが、同様のサービスを攻撃者が悪用する例も増えているとして、「クラウドの闇の部分」について解説した。

Amazon EC2活用の総当たり攻撃、8けたのパスワード解読は3ドル

ラックサイバーリスク総合研究所の新井悠氏

ラックサイバーリスク総合研究所の新井悠氏はまず、Amazon.comのサーバーリソースを時間単位で提供するAmazon EC2の持つ演算能力を利用して、文字列の可能な組み合わせをすべて試す「ブルートフォースアタック(総当たり攻撃)」でパスワードを解読するコストを試算した、海外の調査結果を紹介。それによれば、解読コストがかなり軽減されることがわかったという。

例えば、アルファベットのみで構成される8けたのパスワードを解析する際のコストは3ドル、また、アルファベットと数字で構成される8けたのパスワードでは45ドルだった。新井氏は「攻撃者が通常使う解読ツールを購入するだけでも100ドルはする」と述べ、Amazon EC2のコストパフォーマンスの高さを指摘した。

http://cloud.watch.impress.co.jp/docs/news/20100617_374856.html

クラウド Watch

記事検索

検索

最新ニュース

【 2010/10/8 】

- 「データセンターは寒冷地が適しているという常識を覆す」、Microsoft・リード副社長
- 日本IBM、自動階層化と仮想化に対応したミッドレンジ

東工大、最高性能2.4ペタフロップスを実現するグリーンスパコンを開発開始

今年11月の稼働に向けNECやHPなどの企業連合と協力

東京工業大学は6月16日、学術国際情報センターが中心となり、日本電気株式会社(以下、NEC)と米国ヒューレット・パッカード(以下、HP)などの企業連合と合同で、今年11月に日本初のペタコンとして稼働予定のクラウド型グリーンスーパーコンピュータ「TSUBAME2.0」の開発を開始したと発表した。

また、これを機に、北海道大学および国立情報学研究所とともに、革新的な省エネ型スパコン技術の開発を目指し、大規模実証研究を共同で行うことで合意した。

東京工業大学 理事・副学長の伊澤達夫氏

仮説
クラウドによるパラダイムの変化により

- モラルの確立しない若年ユーザーの手により
- クラウドによって増殖した技術を使って
- Net家電など制御系へのインシデントにより

初めて身体への直接的なリスクが発生する

制御系システムへの攻撃

- **制御システムに対する不正アクセスの危惧**
- **Fear of Illegal Access to Control System**

- クボタシステム開発株式会社　　神　尾　　博
- Kubota Systems Inc.　　Hiroshi KAMIO
- 鳥取環境大学　　安　本　哲之助
- Tottori University of Environmental Studies　Tetsunosuke YASUMOTO

- 要　旨
- 制御システムと情報・通信システムとの融合が、工場，交通，医療，家庭等、社会の様々な分野で急速に進んでいる。たとえばFA分野においては、既に数多くの工場で、メインのコンピュータによる各種自動機械・ロボットの制御や生産情報の収集が行われている。また、HA（Home Automation）分野では、外出先から電話回線を通じての、ビデオの予約や冷暖房の入り切り等をおこなうといったIT家電が具現化し始めた。こうした技術の普及は、生産コストや利便性等で人々に多くの恩恵をもたらす一方、ネットワークを通じての不正アクセスやウイルス等による被害が、制御システムにまで及ぶ可能性も高まってきた。
- 制御システムへの脅威は、電子データのみならず人命や器物に直接的な被害を及ぼしかねないため、サイバーテロリズムにつながる恐れも決して無いとは言い切れない。現時点では、専門エンジニア以外にはあまり中身を知られていないが、近い将来、社会問題となるレベルにまで被害が拡大する可能性も十分にあり得る。現に制御機器の代表格であるPLC（Programmable Logic Controller）への不正アクセスの具体的方法も実演が可能であり、また過去にもPLC以外ではあるが、制御系において小規模ながら被害を与えた事件がいくつか存在する。
- こうした制御系のセキュリティ対策は、ファイアーウォールの設置やパスワードの定期的変更等、従来のビジネス系におけるITセキュリティと同様の内容のみならず、電気信号・メカニズムを加えての検討等、制御システムの特性を十分考慮して行う必要がある。

日本セキュリティ・マネージメント学会誌第17号　2004年9月　発表論文

制御系システムへの攻撃

わが国における制御システムのセキュリティの必要性と取組

Japan's effort to boost activities on Control System Security.

山口英

内閣官房情報セキュリティ補佐官

http://www.jpcert.or.jp/ics/2009/20090219_0940.pdf

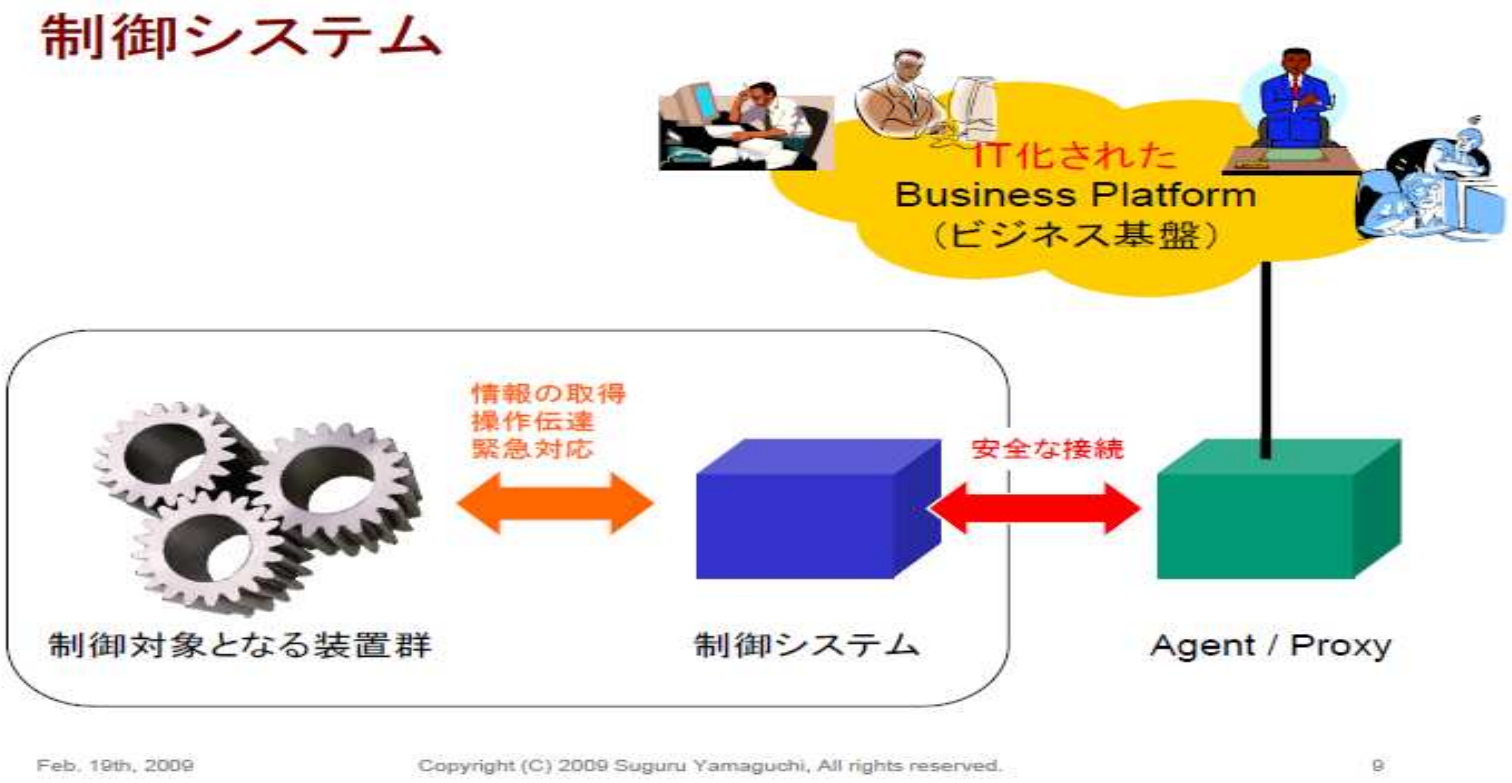
制御系システムへの攻撃

制御システム

- 定義が曖昧？
- 幾つかの特徴は分かっている
  - 我々が日常的に使用するシステムとは違う
  - 装置群と一体的に開発・運用されている
  - 汎用性は低い
  - ライフサイクルは長い
  - 情報系システムとの相互接続は、一般に想定されない
  - 事業に直結した情報処理の実施

http://www.jpcert.or.jp/ics/2009/20090219_0940.pdf

制御系システムへの攻撃



http://www.jpcert.or.jp/ics/2009/20090219_0940.pdf

制御系システムへの攻撃

さらなる挑戦が待っている

- 構成要素の汎用化・共通化
  - OS
  - ネットワーク構成技術とプロトコル
  - ハードウェア
  - SCADA
- リスクの共通化と責任の拡散
- ガラパゴス化は「言い訳」にならない時代
- 新たな役割定義の必要性
  - 事業実施者、システム開発者、構成要素供給者、インテグレータ
  - 事業者団体, 行政機関, 標準化団体, ...
  - ステークホルダの変化

Feb. 19th, 2009 11

http://www.jpcert.or.jp/ics/2009/20090219_0940.pdf

国としての取り組み

- 制御システムセキュリティの信頼性とセキュリティへの取組み強化への提言
- ～「制御システムセキュリティの推進施策に関する調査報告書」の公開～
- 更新日　2010年6月4日
- 掲載日　2010年5月31日
- 独立行政法人 情報処理推進機構
- セキュリティセンター
- IPA（独立行政法人情報処理推進機構、理事長：西垣 浩司）セキュリティセンターは、センサやアクチュエータ、システム等の動作を管理・指示・調整する制御システムのセキュリティに関する欧米等の取組みについて調査を行い、日本での推進施策についてまとめ、「制御システムセキュリティの推進施策に関する調査報告書」として2010年5月31日（月）から、IPAのウェブサイトで公開しました。
- 1. 概要
- IPAセキュリティセンターでは、2008年度から制御システムに対する情報セキュリティ面での脅威と対策について、調査と提言を行っています。2008年度には米国の状況を調査し、制御システムの情報セキュリティのリスクが顕在化していることが明らかになりました。そこで2009年度の調査では、制御システムや情報セキュリティに関わる有識者による検討会「ICS脆弱性低減と普及施策検討会」（委員長：渡辺研司　長岡技術科学大学 准教授）をIPAに設置し、制御システムの脆弱性低減および情報セキュリティ対策の普及施策についての検討を行うと共に、制御システムセキュリティの推進施策に関する調査を行いました。
- 制御システムは以前、独自プロトコルや専用線で構成されていたため、他のシステムとは隔絶されていましたが、昨今は情報システムと同様にコスト削減のため、汎用製品や標準プロトコルの導入、ネットワークを介したシステム接続が進んでいます。水道・ガス・電気などの供給や品質を保証するために機能する重要な制御システムについても、今後高機能な次世代送電網「スマートグリッド」等の新技術が普及すると共に、ネットワークに接続され、一般のパソコン環境と同様に、脆弱性等を悪用した不正アクセス等に備える必要性が高まっています。仮に、これらの制御システムが悪意ある者から攻撃を受け停止した場合、水道・ガス・電気等の供給停止や交通網のまひ等、社会に重大な被害をもたらす可能性があります。

http://www.ipa.go.jp/security/fy21/reports/ics_sec/index.html

The systems that run the Siemens software, called SCADA (supervisory control and data acquisition) systems, are typically not connected to the Internet for security reasons, but this virus spreads when an infected USB stick is inserted into a computer.

Once the USB device is plugged into the PC, the virus scans for a Siemens WinCC system or another USB device, according to Frank Boldewin, a security analyst with German IT service provider GAD, who has studied the code. It copies itself to any USB device it finds, but if it detects the Siemens software, it immediately tries to log in using a default password. Otherwise it does nothing, he said in an e-mail interview.

That technique may work, because SCADA systems are often badly configured, with default passwords unchanged, Boldewin said.

The virus was discovered last month by researchers with VirusBlokAda, a little-known antivirus firm based in Belarus, and reported Thursday by security blogger Brian Krebs.

制御系システムへの攻撃

ニュース

「Stuxnet」のイラン攻撃説――セキュリティ研究者は懐疑的

イランにおける「Stuxnet」ワームの感染拡大は、同国の原子力施設を狙ったサイバー攻撃なのか。

2010年09月28日 14時13分 更新

産業用インフラシステムを狙った「Stuxnet」ワームの感染がイランで広がり、同国の原子力施設を狙ったサイバー攻撃ではないかとの憶測が浮上している。しかし、英セキュリティ企業Sophosの研究者は、こうした報道は煽りすぎではないかと釘を刺している。

Stuxnetは産業用インフラ管理に使われるSiemensのSCADAシステムを狙ったワームで、Windowsの未解決の脆弱性を次々に悪用するなど高度な仕組みを実装している。

報道によれば、イランは同国内の多数のコンピュータがStuxnetに感染したことを認めたとされる。イスラエルがイランの核施設を攻撃する目的でStuxnetを作成したのではないかとの憶測も飛び交っているようだ。

しかしSophosの研究者 グラハム・クルーリー氏によれば、マルウェアの作者が誰なのかを100%証明することは極めて難しく、ましてや政府、軍、シークレットサービスなどの関与を証明するのはさらに困難だという。また、Stuxnetの感染はイラン以外にも多数の国で確認されており、標的はイランだと言い切ることも難しいとしている。

http://www.itmedia.co.jp/news/articles/1009/28/news064.html

ウイルス、イラン核施設標的説に現実味　米社明らかに

2010年11月20日11時1分　B! チェック ブログに利用する 印刷

【ワシントン＝勝田敏彦】産業制御システムを乗っ取るウイルス「スタクスネット」が、ウラン濃縮などに使われる遠心分離器を誤作動させるのに最適な設計になっていることがわかった。スタクスネットの感染は、イランに集中しており、同国内の核施設が標的との説が現実味を帯びることになる。

米セキュリティーソフト大手シマンテックが公式ブログで明らかにした。同社によると、スタクスネットは、超高速回転するモーターの回転数を制御する装置からの信号を狂わせることで、遠心分離器を誤作動させる設計になっていた。

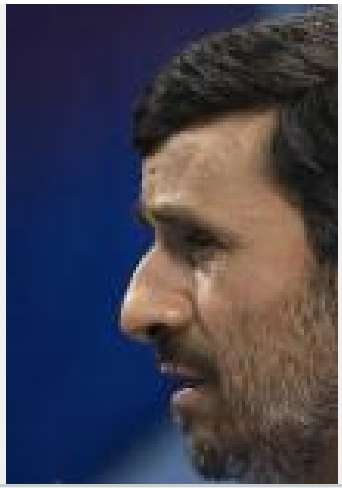
この種の制御装置の用途は、核燃料や核兵器の製造のためのウラン濃縮装置などに限られる。また、スタクスネットは、フィンランドとイランのメーカー2社の製品だけに影響することもわかった。

スタクスネットの感染はイランに集中しており、プログラムにはイランへの警告とも受け取れる旧約聖書の登場人物を暗示する単語が書き込まれていることも判明。イランの核開発を恐れるイスラエルの関与を疑う見方があるが、19日付米紙ニューヨーク・タイムズによると、イスラエル当局者は最近、関与などについて尋ねられると、笑顔を見せているという。

http://www.asahi.com/international/update/1120/TKY201011200104.html

イラン大統領が核施設サイバー攻撃認める、6カ国協議再開も表明

2010年 11月 30日 10:53 JST



1 of 1 [Full Size]

トップニュース

- 10月全世帯の実質消費支出、5カ月ぶりの減少

［テヘラン　29日　ロイター］ イランのアハマディネジャド大統領は29日、同国のウラン濃縮施設の遠心分離機がコンピューターウイルスに感染していたことを明らかにした。この問題は先週、西側外交筋の話として一部メディアが報じていた。

大統領は会見で、感染したウイルスの詳細は明らかにしなかったものの、「何者かがソフトウェアによって一部の遠心分離機に問題を起こした。しかし、問題は既に処理された」と述べ

http://jp.reuters.com/article/topNews/idJPJAPAN-18395820101130

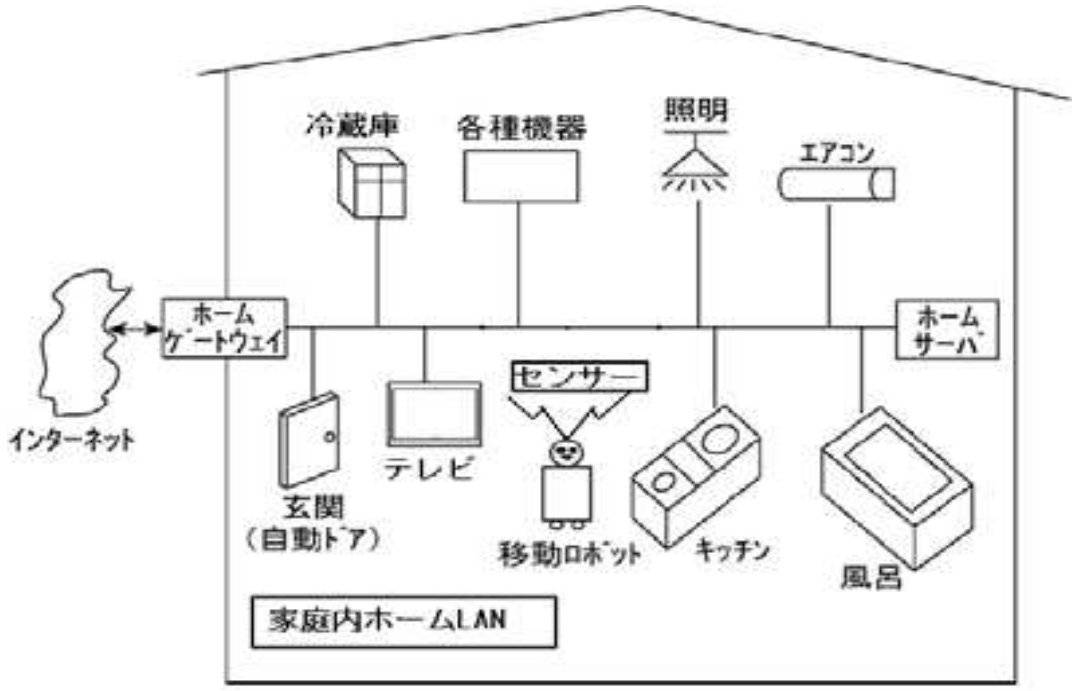
Net家電の想定例

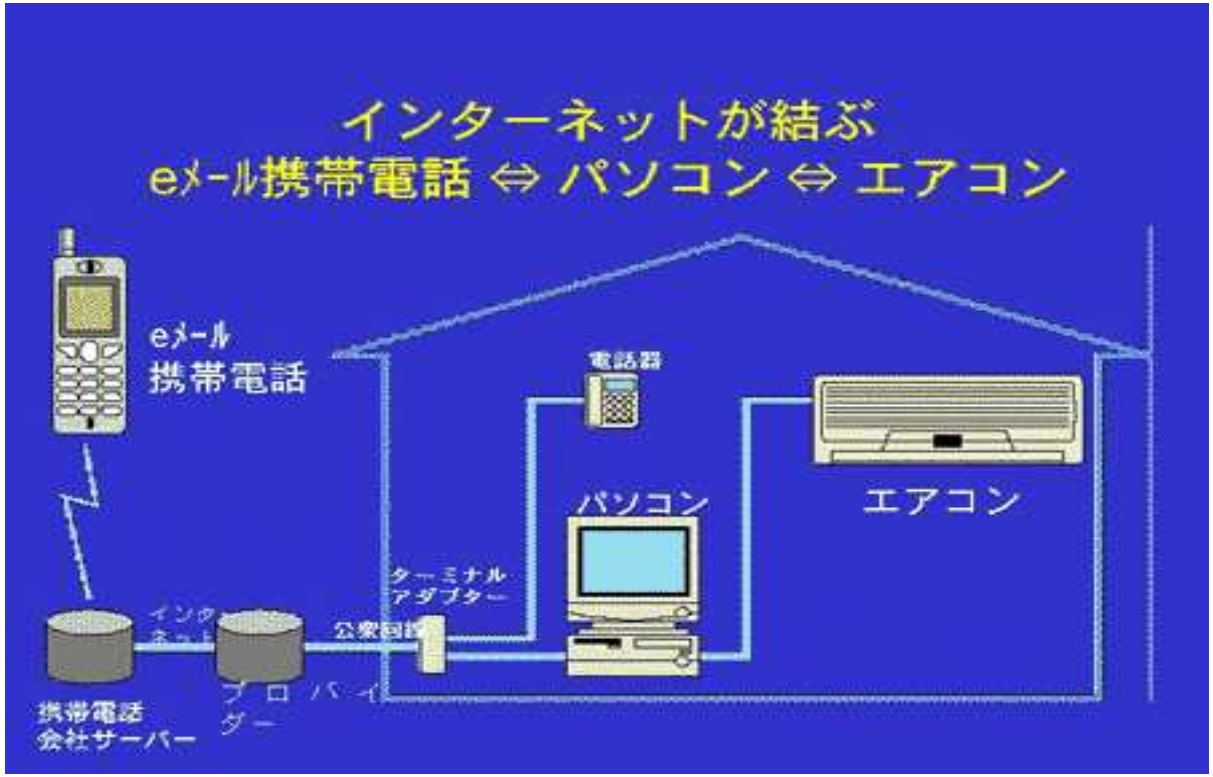
【技術分類】2−1−2　応用技術／端末技術／白物系情報家電
【技術名称】2−1−2−1　インターネット冷蔵庫

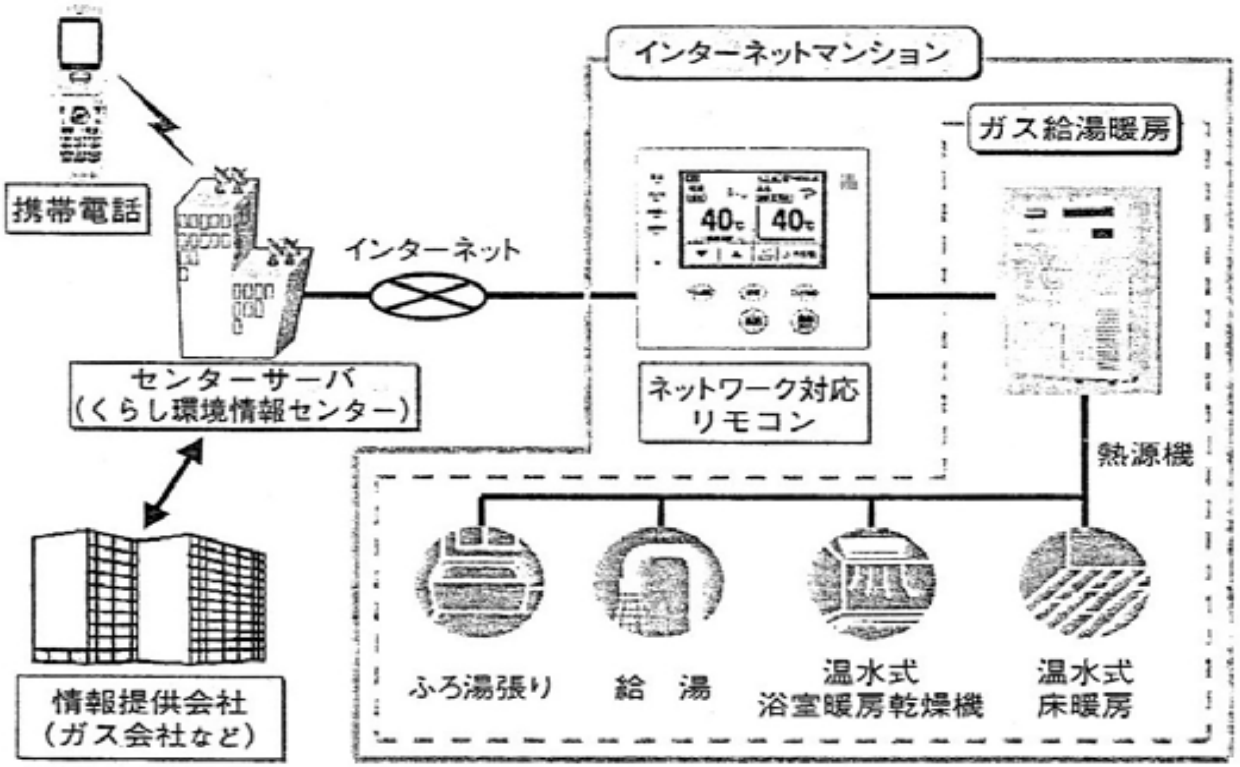
【技術内容】
冷蔵庫には、次の３つの特徴がある。
1. 図１に示すように、扉部分に液晶パネルを収納する広いスペースを持っている。
2. 家の中の生活動線の中心に位置し、家族同士のメッセージなどの情報掲示板として活用できる。
3. ホームサーバ機能に必要な“１日中電気を流しっぱなし”という条件を持っている。

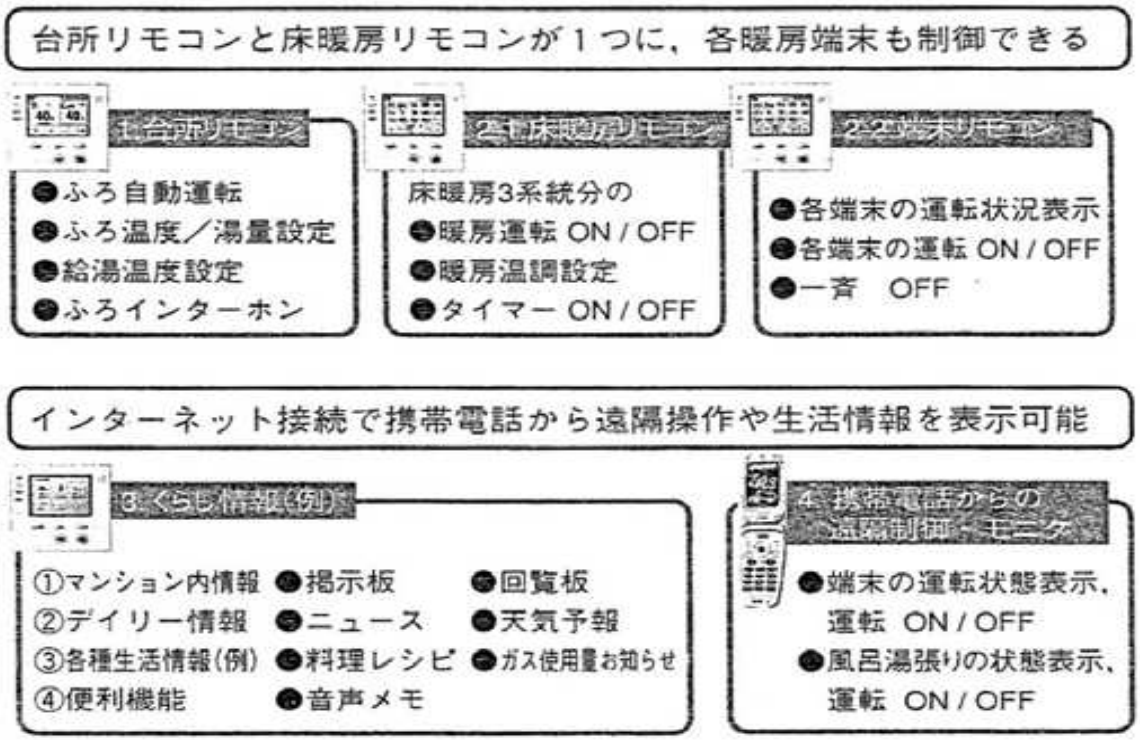
インターネット冷蔵庫の装置としては、上部の扉部分にカラー液晶パネルとマイク、CCD カメラを装備。CPU やモデムなどのコンピュータ部分は冷蔵庫の上部に搭載し、キーボードは使わずタッチパネルや音声によって操作する。家庭内 LAN を利用すれば、あらゆる家電製品を「冷蔵庫」でコントロールできる。さらに、マイクやカメラを使ってボイス・メールやビデオ・メールのやり取りもできる。

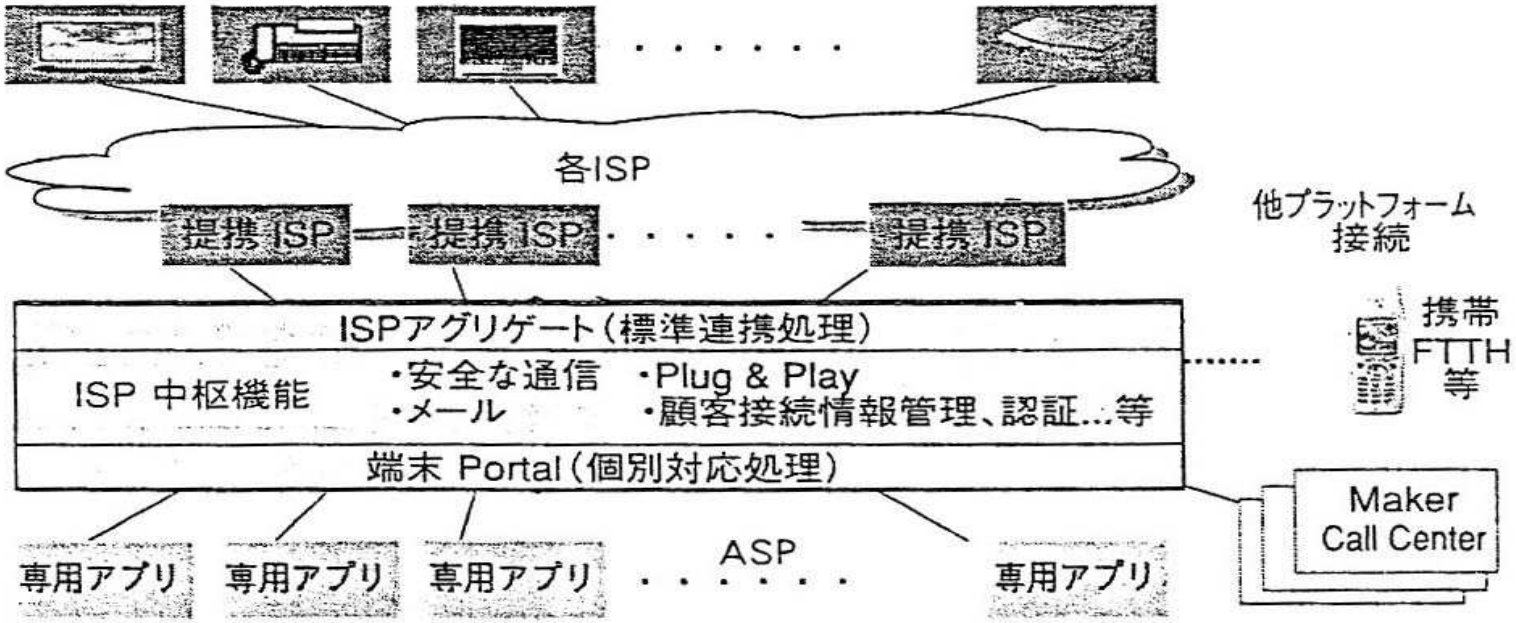
以下　Webベースのインターネット家電
特許庁総務部企画調査課技術動向班　による


冷蔵庫
各種機器
照明
エアコン
ホーム
ゲートウェイ
ホーム
サーバ
インターネット
センサー
テレビ
玄関
(自動ドア)
移動ロボット
キッチン
風呂
家庭内ホームLAN

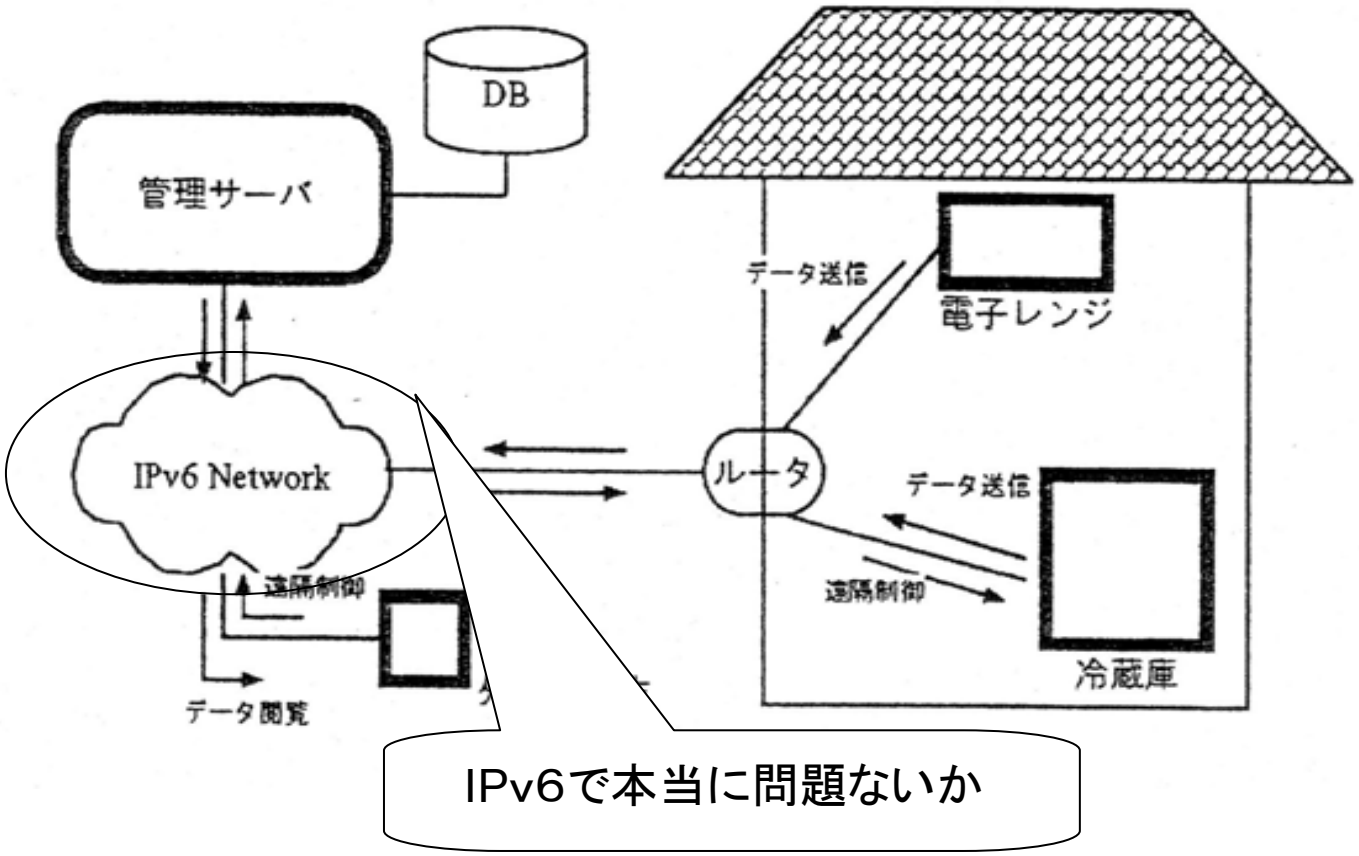

インターネットが結ぶ
eメール携帯電話 ⇔ パソコン ⇔ エアコン
eメール
携帯電話
電話器
パソコン
エアコン
ターミナル
アダプター
公衆回線
携帯電話
会社サーバー
プロバイダー

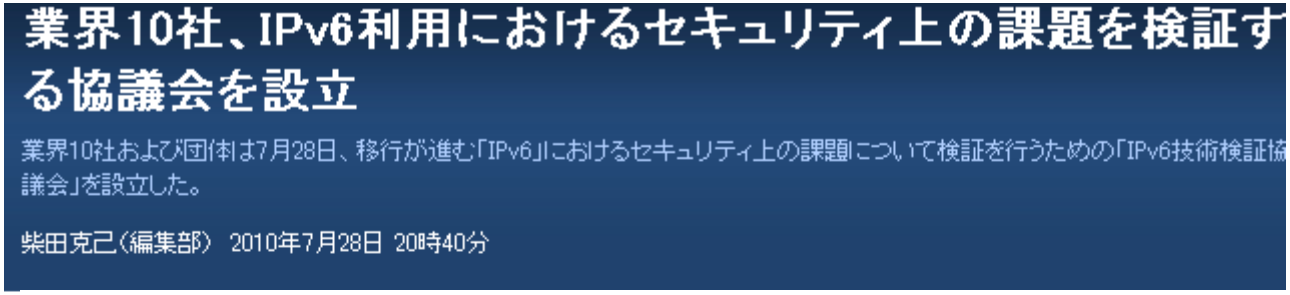

インターネットマンション
ガス給湯暖房
携帯電話
インターネット
40℃
40℃
センターサーバ
(くらし環境情報センター)
ネットワーク対応
リモコン
熱源機
情報提供会社
(ガス会社など)
ふろ湯張り
給　湯
温水式
浴室暖房乾燥機
温水式
床暖房


台所リモコンと床暖房リモコンが１つに、各暖房端末も制御できる
台所リモコン
●ふろ自動運転
●ふろ温度／湯量設定
●給湯温度設定
●ふろインターホン
各暖房リモコン
床暖房3系統分の
●暖房運転 ON / OFF
●暖房温調設定
●タイマー ON / OFF
2分岐ユニット
●各端末の運転状況表示
●各端末の運転 ON / OFF
●一斉　OFF
インターネット接続で携帯電話から遠隔操作や生活情報を表示可能
3.くらし情報(例)
①マンション内情報 ●掲示板 ●回覧板
②デイリー情報 ●ニュース ●天気予報
③各種生活情報(例) ●料理レシピ ●ガス使用量お知らせ
④便利機能 ●音声メモ
4.携帯電話からの遠隔制御・モニタ
●端末の運転状態表示、運転 ON / OFF
●風呂湯張りの状態表示、運転 ON / OFF



(ASP: Application Service Provider, ISP: Internet Service Provider)


DB
管理サーバ
データ送信
電子レンジ
IPv6 Network
ルータ
データ送信
遠隔制御
遠隔制御
データ閲覧
冷蔵庫
IPv6で本当に問題ないか



業界10社、IPv6利用におけるセキュリティ上の課題を検証する協議会を設立

業界10社および団体は7月28日、移行が進む「IPv6」におけるセキュリティ上の課題について検証を行うための「IPv6技術検証協議会」を設立した。

柴田克己（編集部） 2010年7月28日 20時40分

榎並氏は、「IPv6では、一般的に“エンド・ツー・エンドの暗号化および認証”によって、IPv4よりもセキュアになるという定説があるが、一方で実際には自動設定機構に起因する経路詐称やネットワークの境界でブロックするという既存のセキュリティ戦略が通用しなくなるといった課題も内在している」とし、同協議会ではそうした課題の収集と、会員社の持つIPv6対応製品での検証、対策技術の検討と評価を行い、情報公開を行っていくとした。なお、セキュリティ検証のためのテストベッドは、マイクロソフトの大手町テクノロジーセンター内に設置される。

http://japan.zdnet.com/news/nw/story/0,2000056190,20417569,00.htr

自動車も

iPhoneから遠隔操作で車のロック解除やエンジン始動ができるシステム『Viper SmartStart』

ツイートする 0 いいね！ 25 users

米Directed社が、iPhoneのアプリから遠隔操作で車のロックやエンジンをコントロールできるシステムを、**米国のユーザー向けに公開**しています。

通信モジュールを内蔵したアラームを車にインストールし、専用のiPhoneアプリ『Viper SmartStart』を使ってインターネット経由でコマンドを送信。ロックの施錠・解除、エンジンの始動などが行えるようです。

車の盗難や車内の金品を狙った犯罪が日常茶飯事の米国では、自動車向けのセキュリティー・システムが浸透しています。駐車中に振動を感知するとけたたましいアラームを鳴らして犯罪を防ぐ一方で、誤動作することも多く迷惑な存在でもあります。

http://ipodtouchlab.com/2009/10/viper-smartstart-iphone.html

【CEATEC 10】日産 リーフ… スマートフォンで遠隔操作

2010年10月5日(火) 18時27分

CEATEC シーテック 特別編集

- 【CEATEC 10】自然な歌声と表情でうたう女性ロボット
- 【CEATEC 10】既存のナビ市場に影響を与えることはない
- 【CEATEC 10】車載クレードルに各種センサーを内蔵

編集部にメッセージを送る

つぶやく

【CEATEC JAPAN 2010(Vol.24)】スマートフォンで遠隔操作できる電気自動車「日産リーフ」

「CEATEC JAPAN 2010」で日産は、通信ユニットTCUを搭載した電気自動車「リーフ」の展示を行っている。「リーフ」はTCUを通じてスマートフォン及びPCからバッテリー状態のチェックやリモート充電、エアコンの設定などの遠隔操作を行うことができる。

展示ブースでは、車の充電完了を知らせるメールの受信や、乗車前に車内の温度を調整する「乗る前エアコン」の作動などがPC上から行われた。また航続距離から到着予想エリアを表示する「到着予想エリアマップ」や、モーター・空調・電装品の電力消費表示機能、充電スポット案内、タイマー充電機能などが利用できる。

http://response.jp/article/2010/10/05/145948.html

例えば

Amazon EC2の持つ演算能力を利用して、文字列の可能な組み合わせをすべて試す「ブルー
フォースアタック（総当たり攻撃）」でパスワードを解読（前述

親のクラウドIDで難なくクラウド接続

千葉
同級
れて
に油
（少年

•同級生のIDとパスワードを使ってオンラインゲームに不正アクセスし、補導（愛知県　12歳の児童3名）

立高校
捕され
した」と
が、すく
いじめ

会社
など）

•風呂の空だきが火災の原因となっています。（住宅防火対策推進協議会）

新しい統制

- 実行者の常識、良識

若年層やテロリストのアクセスを防ぐ意味からも個人認証の強化が必要。もはやモラルには頼れない！

- 情報自体で身体的危害は無理

クリティカルな制御は一般のネットワークから遮断、隠蔽

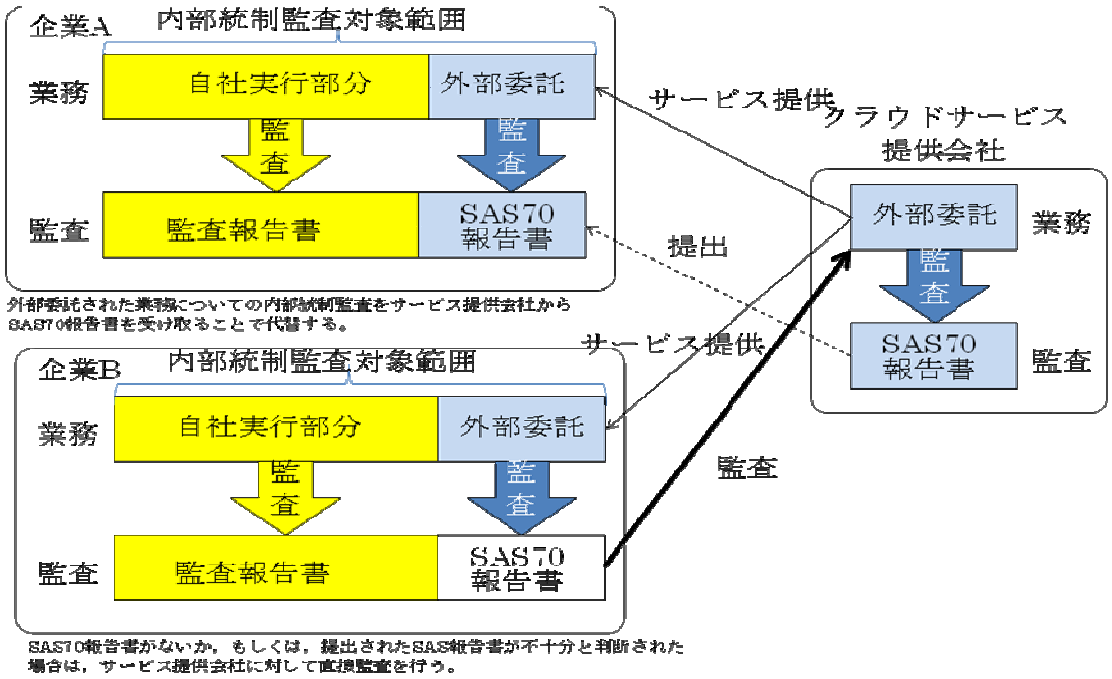
- 技術自体の限界

クラウドの個人認証はより厳しく、また事業者の外部統制もより厳格に。IPV6での経路詐称などへの対応も急務

個人認証の重要性

- 現在，主に用いられている認証技術としては，利便性の高いID・パスワード方式，セキュリティ強度の高いIC カード等を用いたPKI方式などがある。最近では，生体情報を用いた方式も用いられてきている。
- 個人を認識するため，現在，民間においてOpenID[1]やリバティアライアンス[2]プロジェクト等，複数のウェブサイト間で，ID を連携するID管理の取組が進んできている。ID管理とは，ユーザの識別・属性を複数のシステムにまたがって管理することで，このようなID管理をより一層促進してゆくためには，それぞれのウェブサイトで要求する認証に関する本人確認のレベルと認証技術の強度を，ある程度一定に統一しておくことが重要である。例えば，他の機関で行われた本人確認結果が共有可能となることによって，効果的な連携・運用の促進に寄与することができる。また，ID管理とデータ連携が重要になるケースが多いと思われる。
- 本当の脅威はWebサイトが改ざんされることではなく，ID情報が盗まれていることだと再認識すること。それには，まず使用するサービスのSLA（Service Level Agreement）を確認し，課金状態を定期的に（できれば毎日）確認し，一定以上の金額を使用していないかをチェックする必要がある。
- とは言ってもデジタル家電などは，家族間で利用するので，個人認証はできたとしてもヒューマンエラーによるリスクは残る。外出先から制御する場合，想定内のヒューマンエラーについては予め防護ソフトが組み込まれているとしても，想定外の使用法に対する処理は，性善説に立った子供を含む個々の家庭内のセキュリティポリシーを設定・遵守するしかない。

外部統制の必要性



http://www.atmarkit.co.jp/im/cits/serial/soxfw/07/03.html

参考資料

- システムの概念 [編集]

- SCADA という用語は一般に、1つのサイト全体や地理的に分散したシステム群を集中的に監視制御するシステムを指す。制御のほとんどは遠方監視制御装置 (RTU) またはプログラマブルロジックコントローラ (PLC) が自動的に行う。ホストの制御機能は監督的な介入や優先的なものに限られることが多い。例えば、PLCが工業プロセスにおける冷却水の流量を制御する場合、SCADAシステムはオペレータが流量の設定値を変更できるようにしたり、警報発生条件（不正な流量や高温）を変更できるようにしたり、現在の状態をオペレータに対して表示し記録する。フィードバック制御ループはRTUやPLCでほぼ完結しており、SCADAシステムはそれらループの状態を監視する。

http://ja.wikipedia.org/wiki/SCADA

参考資料

- IPv6導入によるメリット [編集]

- 一般に言われているIPv6導入によるメリットとしては以下のようなものがあげられている。
- 事実上無限の数のIPアドレス
- アドレス枯渇を心配しなくてよくなる。実際には有限（2128個）であるが「その辺の石ころにも個別に割り当てることができる」ぐらい有り余っている[2]。同時に、IPマスカレード（NAT/NAPT等）を使わずに済むので、全ノードがグローバルな接続性を持ち、直接接続が可能になる。これによって、P2Pアプリケーション（IP電話、インスタントメッセンジャー及びネットワークゲーム等）の利用が容易になり、またNATの設定等に気を遣わなくて済むようになる。
- 実際にOCNによるIPv6サービスでは、月額300円で/64のネットワークブロックを2ブロック提供するサービスを実施している。このサービスを受けることで、理論的には300円の月額で、一人あたり約43億の2乗(2の64乗、IPv4におけるIPアドレスの総数の2乗)ものアドレス空間をもつネットワークブロックを2つ取得することができる。
- IPsecによるIPレイヤでのend to endセキュリティの確保にあっては、ユーザ認証、パケットの暗号化及びなりすまし防止等がサポートされた。これらはIPv4を使う環境では上位レイヤ (TLS) 等で補完しなければならなかった機能である。
- 一部で「IPv6の実装にはIPSecが必須である」と言われているが、これは規格上(RFC)の話で、IPSecをサポートしないIPv6の実装は多数存在している。
- 管理者に負担をかけないIPアドレスの自動設定
- DHCPサーバがなくても、ホストには自動的にIPアドレスとデフォルト経路が設定される。
- アドレスの集約による基幹ルータでの経路表サイズの抑制
- 新たにIPv6の接続を持つとき、ISPの持っているIPv6アドレス（プリフィックス）を切り出してユーザーに渡す。これによって、新しいIPv6サイトが増えたとしてもバックボーンに対して公告する経路情報は増えず、基幹ルータで保持する経路表の大きさが抑えられる。その一方で、アドレスブロックの可搬性がなくなる、複数のISPと契約した時にどのアドレスをどのように使うかを考慮しなければならない「マルチホーム」問題も発生する。
- 固定長ヘッダ
- IPv6の基本的なヘッダは固定されているため、ルータの負荷を低減できるなどATM等の固定長パケットネットワークに共通な利点を享受しつつ、また拡張性も保つ。
- エラー検出
- IPv4ではレイヤ3 (IP) で各ルータのホップ毎に行われていたエラー検出をIPv6では廃止し、レイヤ4（TCPv6/UDPv6等）以上の上位層で、エンドツーエンド (end-to-end) でエラー検出を行うこととされた。これにより前項と同じくルータの負荷低減等が期待される。

http://ja.wikipedia.org/wiki/IPv6

参考資料

- 一般家庭環境のように，モバイルやクラウド・コンピューティングが普及し，ファイアウォールやプロキシに守られない環境が一般化するときには，セキュリティは特に重要な機能となる。
- 一方では，IPv6では，標準でセキュリティに関する機能が用意される。具体的には，IPv6は端末間の通信をIPSecで守ることが必須であり，認証や暗号化に対しても，認証ヘッダ（Authentication Header：AH）と暗号化ヘッダ（Encapsulated Security Payload：ESP）が，それぞれ拡張ヘッダとして組み込まれている標準プロトコルでもある。しかし，所属セグメントが動的に変わるMobile IPが可能となる仕組みも提供しているが，これは移動端末ゆえの脆弱性となる。