クラウドの情報セキュリティ

Restoration by cloud computing innovation.

勝ち残りのための情報セキュリティ

株式会社ラック
サイバーリスク総合研究所
最高技術責任者西本 逸郎
itsuro@lac.co.jp
http://www.lac.co.jp/

Copyright ©2010 Little eArth Corporation Co.,Ltd.

株式会社ラック

ITを活用し企業のリスク管理を支援する、次代と経営を拓くセキュリティプランナー

1986年、株式会社ラックは設立されました。”Little eArth Corporation”という社名には、ITの進展で地球が相対的に小さくなっていく中で、ITを基盤に国や企業の発展を支えていこうという理念がこめられています。
独立系セキュリティベンダーとして、15年近くの豊富な実績がお客様の信頼の証です。
JSOC（下記参照）、**サイバーリスク総合研究所**、**サイバー救急センター**の配備が特徴です。

商　号	株式会社ラック LAC：Little eArth Corporation Co., Ltd.
設　立	1986年(昭和61年)9月
資本金	11億5,942万6,500円
株　主	ラックホールディングス株式会社(100%)
代　表	代表取締役社長 執行役員社長 齋藤 理
売上高	5,138百万円(24期：2009年03月期)
	2,342百万円(23期：2008年03月期) ※23期は決算期変更による3ケ月変則決算です。
	7,154百万円(22期：2007年12月期)
決算期	3月末日
従業員数	352名（2010年4月現在）
認定資格	経済産業省情報セキュリティ監査企業登録 情報セキュリティマネジメントシステム (ISO/IEC 27001)認証取得(JSOC) プライバシーマーク認定取得

・本社
〒102-0093　東京都千代田区平河町 2-16-1
平河町森タワー
03-6757-0111(代表)
03-6757-0113（営業窓口）

・名古屋オフィス
〒460-0008　名古屋市中区栄3-15-27
名古屋プラザビル 9F

・米国ニューヨークオフィス USLAC

・韓国ソウル 子会社 CSLAC
Cyber Security LAC Co.,Ltd.

・中国上海 子会社 LAC CHINA
上海楽客網絡技術有限公司

http://www.lac.co.jp/
sales@lac.co.jp
Twitter　@lac_security
YouTube　laccotv

■ JSOC (Japan Security Operation Center)

JSOCは、ラックが運営する情報セキュリティに関するオペレーションセンターです。高度な分析システムや堅牢な設備を誇り、24時間365日運営。高度な分析官とインシデント対応技術者を配置しています。2000年の九州・沖縄サミットの運用・監視を皮切りに、日本の各分野でのトップ企業などを中心に、高レベルのセキュリティが要求されるお客様にその高品質なサービスを提供しています。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

スピーカ

西本 逸郎（にしもと いつろう） CISSP

昭和33年	福岡県北九州市生まれ
昭和59年3月	熊本大学工学部土木工学科中退
昭和59年4月	情報技術開発株式会社入社
昭和61年10月	株式会社ラック入社

通信系ソフトウェアやミドルウェアの開発に従事。1993年ドイツのシーメンスニックスドルフ社と提携し、オープンPOS（WindowsPOS）を世界に先駆け開発・実践投入。2000年よりセキュリティ事業に身を転じ、日本最大級のセキュリティセンターJSOCの構築と立ち上げを行う。
さらなるIT利活用を図る上での新たな脅威への研究や対策に邁進中。

情報セキュリティ対策をテーマに官庁、大学、その他公益法人、企業、各種ITイベント、セミナーなどでの講演、新聞・雑誌などへの寄稿等多数

株式会社ラック　取締役　常務執行役員　最高技術責任者
サイバーリスク総合研究所
サイバー救急センター
特定非営利活動法人 日本ネットワークセキュリティ協会 理事
特定非営利活動法人 日本セキュリティ監査協会 理事
データベースセキュリティコンソーシアム 理事、事務局長

経済産業省 電子商取引等に関する法的問題検討会 委員（2007年～）
IPA セキュリティ＆プログラミングキャンプ実行委員（2007年～）
（財）日本情報処理開発協会 リスク管理統制対応評価検討委員
2009年度情報化月間 総務省情報通信2008年～）国際戦略局長表彰

連載・コラム
西本逸郎のセキュリティー表ウラ
セキュリティー表ウラ 検索
http://it.nikkei.co.jp/security/column/nishimoto_security.aspx

ブログ どらいつ 検索
ツイッター http://twitter.com/dry2

Copyright ©2010 Little eArth Corporation Co.,Ltd.

1. クラウド来る。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

本題の前に

Copyright ©2010 Little eArth Corporation Co.,Ltd.

本題の前に

クラウドを
自社で活用したいと
思っている？

Yes　　No

Copyright ©2010 Little eArth Corporation Co.,Ltd.

本題の前に

クラウドで
ビジネスをしたいと
思っている？

Yes　　No

Copyright ©2010 Little eArth Corporation Co.,Ltd.

本題の前に

クラウドは、

従来のアウトソースや

ASPの一環である。

（課金の単位が異なるだけ？）

（使用技術が異なるだけ？）

Yes　　**No**

Copyright ©2010 Little eArth Corporation Co.,Ltd.

本題の前に

答えは、

そう思えば、**Yes**

そう思わないなら、**No**

Copyright ©2010 Little eArth Corporation Co.,Ltd.

本題の前に

クラウドにより何が変わる？

1. ほとんど変わらない。
2. コストを圧縮・流動化できる。
3. **IT**システムの形態が変わる
4. ビジネススタイルが変わる
5. その他

Copyright ©2010 Little eArth Corporation Co.,Ltd.

本題の前に

本日の本題。

クラウド

実は、、
何がいいのか、よくわからない。

Yes　　**No**

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウドとは。

アマゾン・グーグル・セールスフォース

巨大データセンター

仮想化技術。

オンデマンドで利用が出来る。

所有から利用へ。

ITコストをカット。

最新技術が利用できる。

環境にやさしい。グリーン。エコ。

実態がよくわからない。

ちゃんとやってくれるのだろうか？

Copyright ©2010 Little eArth Corporation Co.,Ltd.

なぜ黒船なのか？

過去に発生した事件をもとに
考えてみたい。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

印象的な事件

「最近、他社に出し抜かれることが多い」

昔、[redacted]、独立。
現在は[redacted]に。社長と元役員との確執。

メールの盗み読み
⇒ ネットワーク・サーバ管理上の問題

Copyright ©2010 Little eArth Corporation Co.,Ltd.

印象的な事件

「提携先の役員から、例のメールの件で」

自分の部下が、[　　]、提携後の事を考慮させるメールを送信。

メールの成りすまし

⇒ メールサーバ監査不足。

ログ取得も不十分。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

印象的な事件

「私のプライベートを知っている人がいる」

自分の[　　]が、自分のメールを盗み読み。

メールの盗み読み
⇒ 上司のPCを管理する部下

Copyright ©2010 Little eArth Corporation Co.,Ltd.

印象的な事件

「業務上の機密が漏れている」

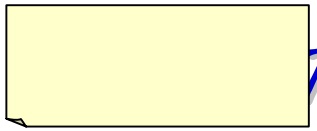
自分の[　　]が、自分のディスクを盗み読み。

リモートでディスクの盗み読み
⇒ 上司のPCを管理する部下

Copyright ©2010 Little eArth Corporation Co.,Ltd.

印象的な事件

「業務上の機密が外部に漏れている」

 から、流出。

関係者であれば誰でも可能であった

⇒ 昔から実施している業務
誰も疑わなかった
時代・環境が変わった

Copyright ©2010 Little eArth Corporation Co.,Ltd.

印象的な事件

「社内情報が漏洩している」

[redacted]社員

当初の開発と運用を任せられていた
⇒ 管理者権限の管理
開発環境・テスト環境・本番環境

Copyright ©2010 Little eArth Corporation Co.,Ltd.

印象的な事件

「顧客情報を悪用している社員がいる」

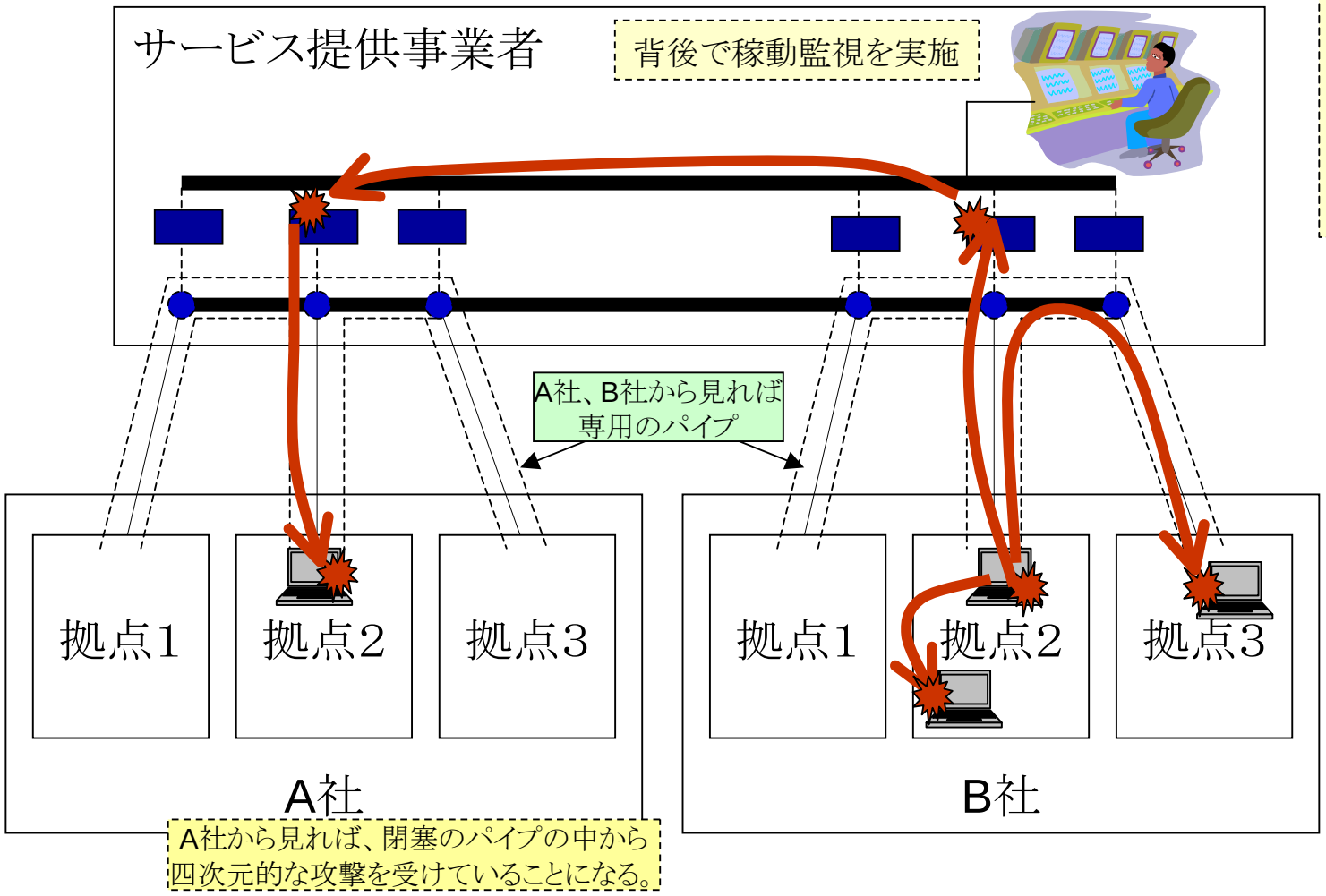
[redacted]の人間

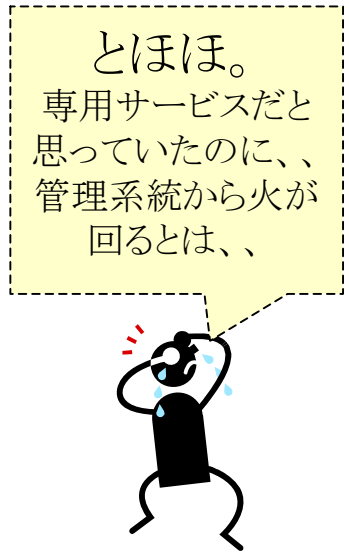
情報システム部であれば可能であった
⇒ アクセス管理はしっかりしているが
ユーザ情報を管理者が閲覧可能
ストーカ行為

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウド社会を想起させる事件

あるサービス会社でのIP-VPNサービスでのウイルス感染事件のイメージ

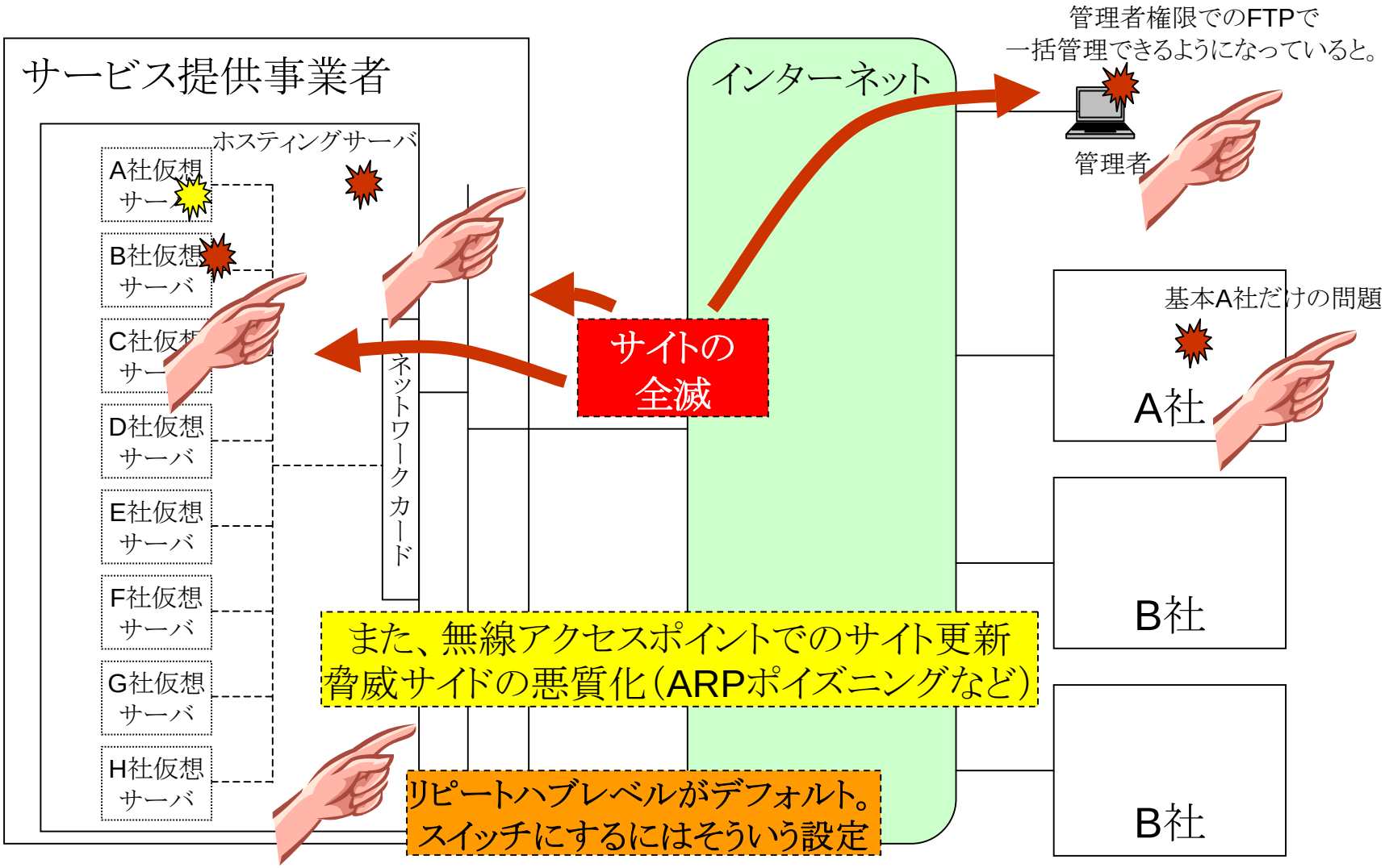




Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウド社会を想起させる事件

あるホスティング会社でのガンブラーウイルス感染事件のイメージ



Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウド社会を想起させる事件

サービス利用の鉄則！

こんなこともあろうかと。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

事件から言えること

外部からの犯罪
1. **Web**改ざん
2. **USB**メモリ
3. 標的型メール

アカウント

内部犯罪
1. 情報システム部門
2. 上司のパソコンの面倒を見ている部下
3. 協力会社(特にオフショア開発・運用)

あと、役員の競合

丸投げ

Copyright ©2010 Little eArth Corporation Co.,Ltd.

知らなければならない事実と覚悟

サービスの受け手の意識が変化しないままに、アウトソース ⇒ ASP ⇒ クラウド へと進行し、乖離が進む危険性は大いにある。（茹で蛙現象）

といっても、
自己責任でリテラシーを高め推進する利用者とサービス提供者に過剰な要求をする利用者の混在は、有り得るのか？

クラウドは業者がサービス内容とレベルを決めて利用者はそれを選択する。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウドの定義は様々

どれが正解などは、たぶん存在しない。
組織により生き残り方は異なる。

恐らく、生き残った組織が正しく、
生き残ったクラウドが正しい。

ただ、一般論は存在する。
その組織にとって正しいかどうかは別として。

最初から規制や利用者からの要求でつまらなくならなければ良いが。
あっ！ 所詮、それも自然淘汰か。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウドが着目される理由

クラウドに走る理由（個人的な意見）

0. 短期的には経費カット

1. 経費の流動化
2. 事業の自由度確保
3. トータルコストの削減

成功へのハードルを低く、
機動力を最大限に。
継続的ダメージを最小限に

4. 必然（スマートフォン、タブレット → スマートX）

<u>生き抜いていくこと。</u>

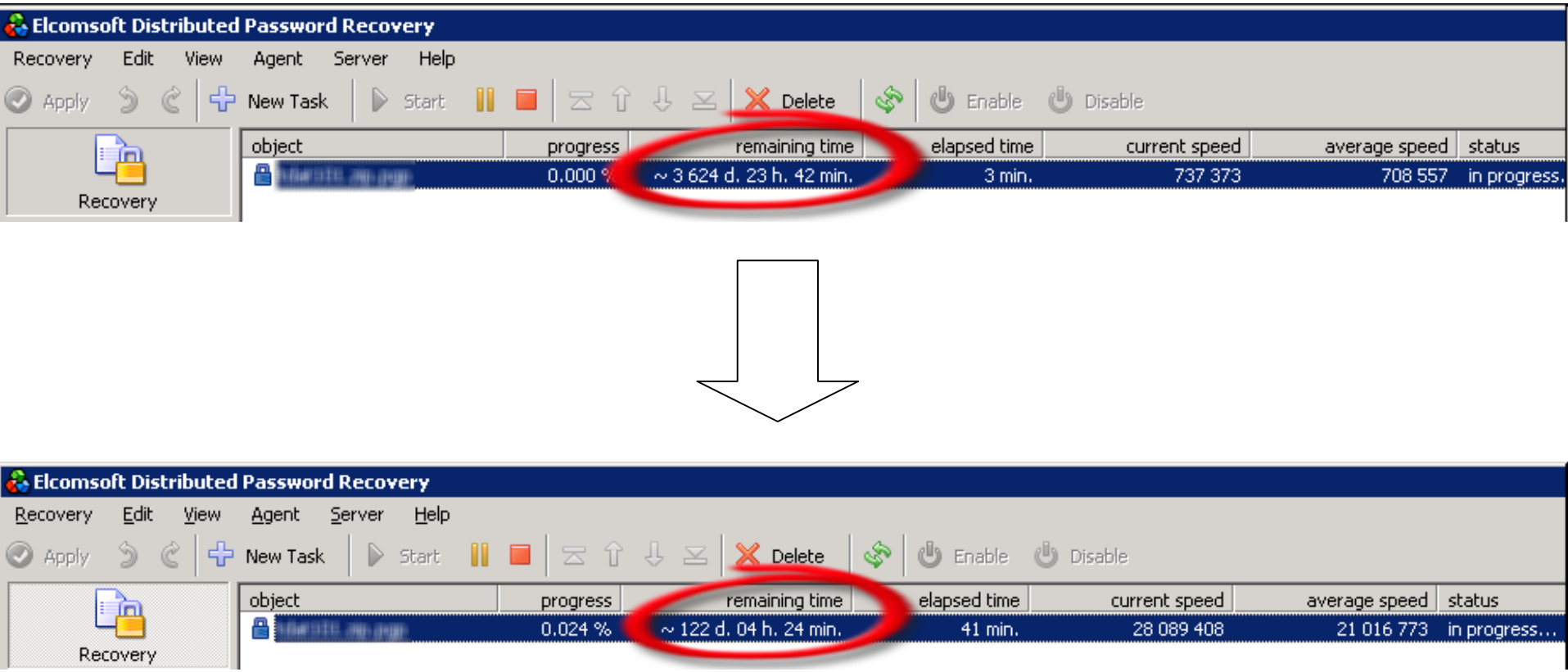
その為には我々は環境適応し続けなければならない。
将来役に立つかもしれないけど、重たい荷物はいらない。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウド活用例

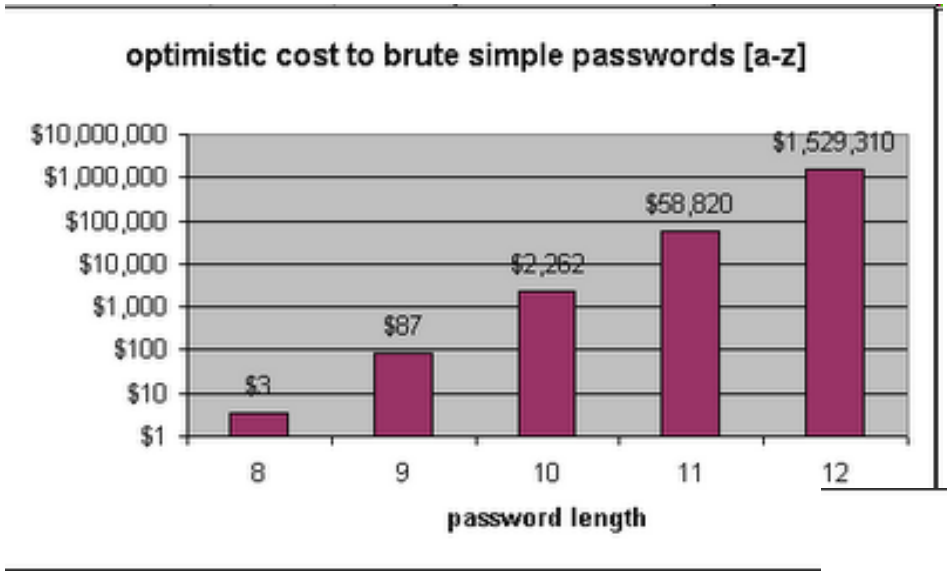
有名なクラウド活用者 ＝ 犯罪者

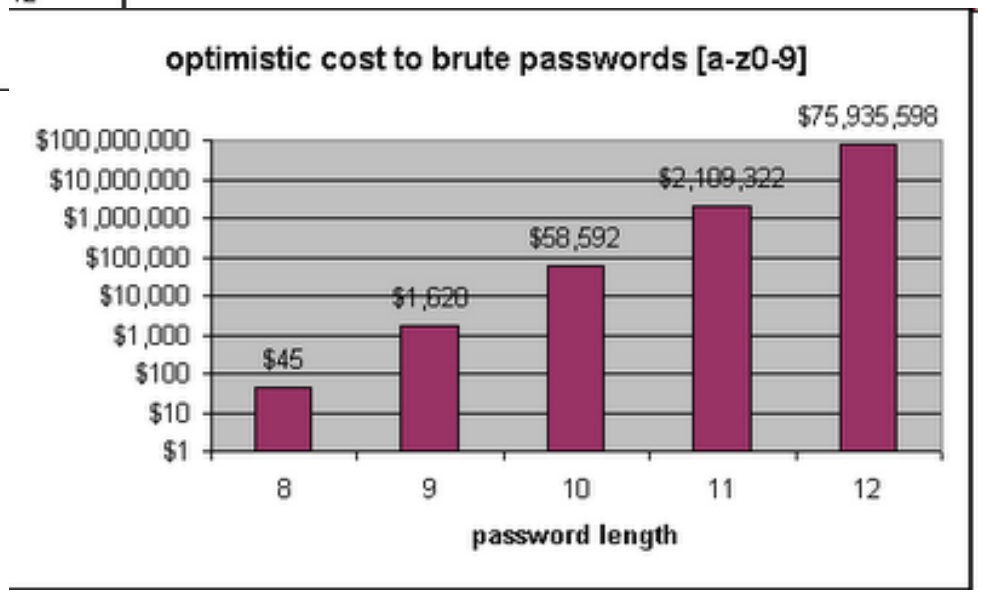
Copyright ©2010 Little eArth Corporation Co.,Ltd.



Copyright ©2010 Little eArth Corporation Co.,Ltd.

Amazon EC2を使用したパスワードクラック試算



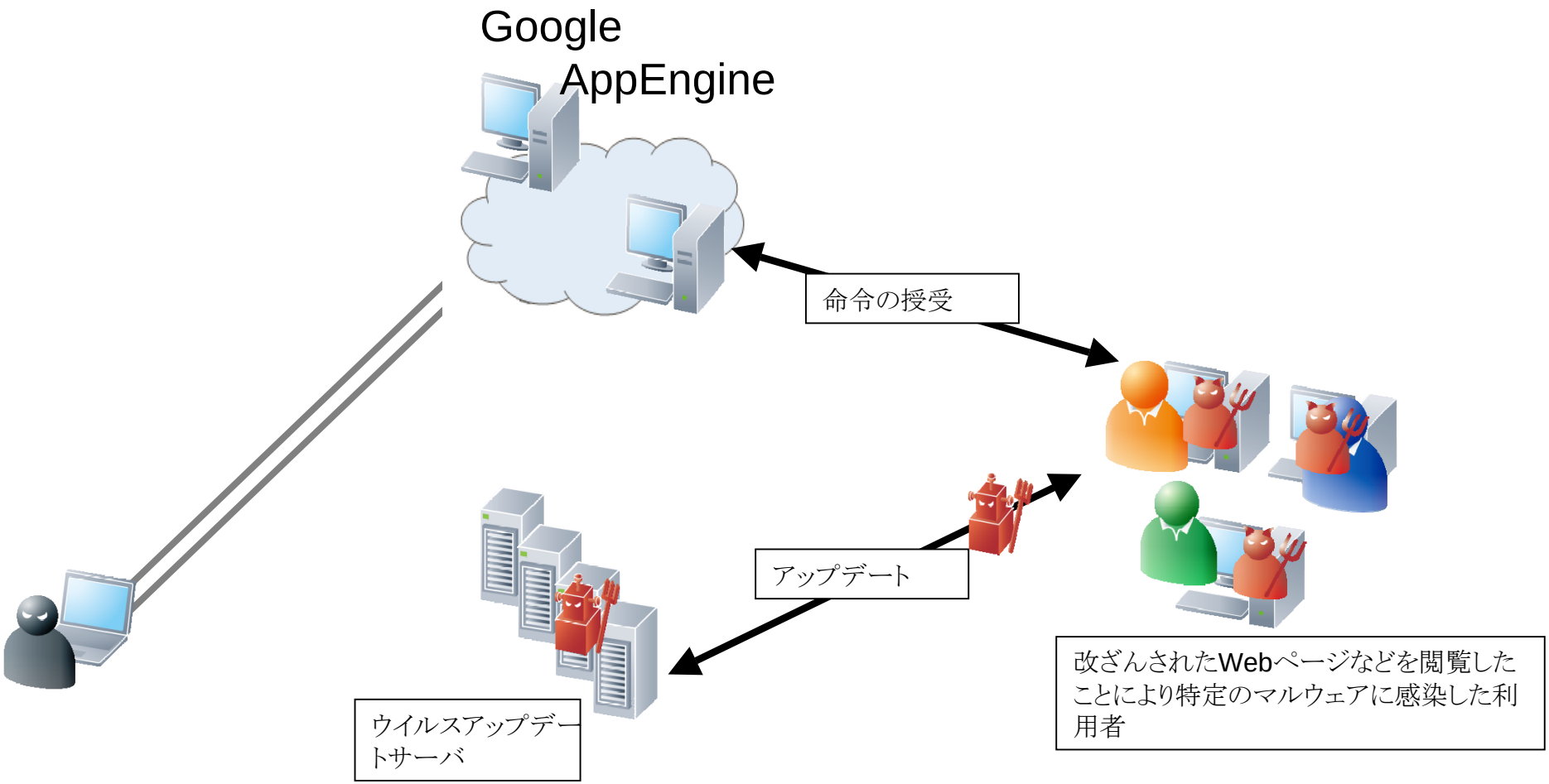


出典:http://news.electricalchemy.net/2009/10/password-cracking-in-cloud-part-5.html

Copyright ©2010 Little eArth Corporation Co.,Ltd.

Google App Engine をCommand & Control サーバに

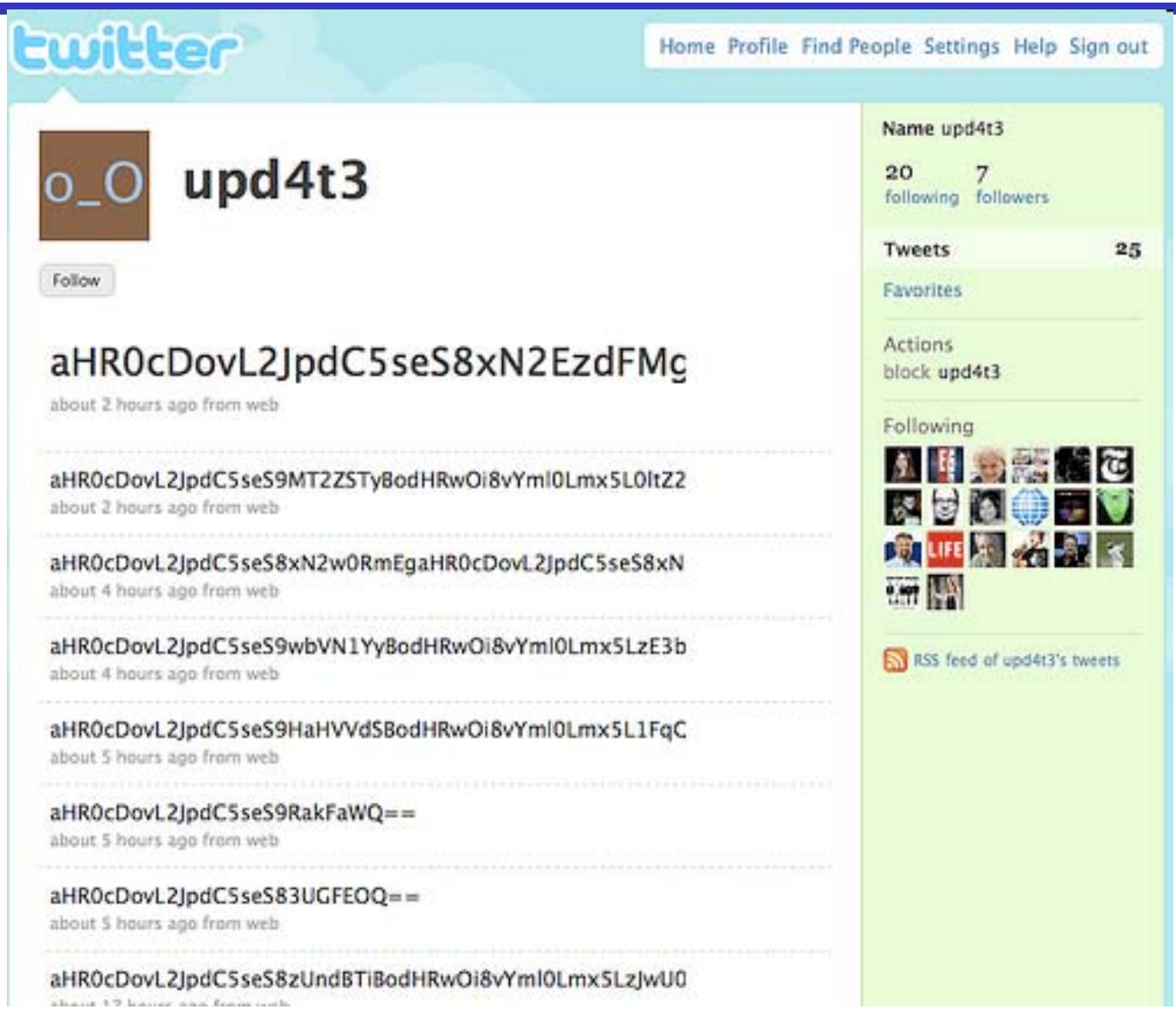
Copyright ©2010 Little eArth Corporation Co.,Ltd.



Copyright ©2010 Little eArth Corporation Co.,Ltd.

Copyright ©2010 Little eArth Corporation Co.Ltd.

Twitter を C&C サーバに



Copyright ©2010 Little eArth Corporation Co.,Ltd.

Let's look at one of the update messages; it's pretty clearly base64 encoded. What does it say?

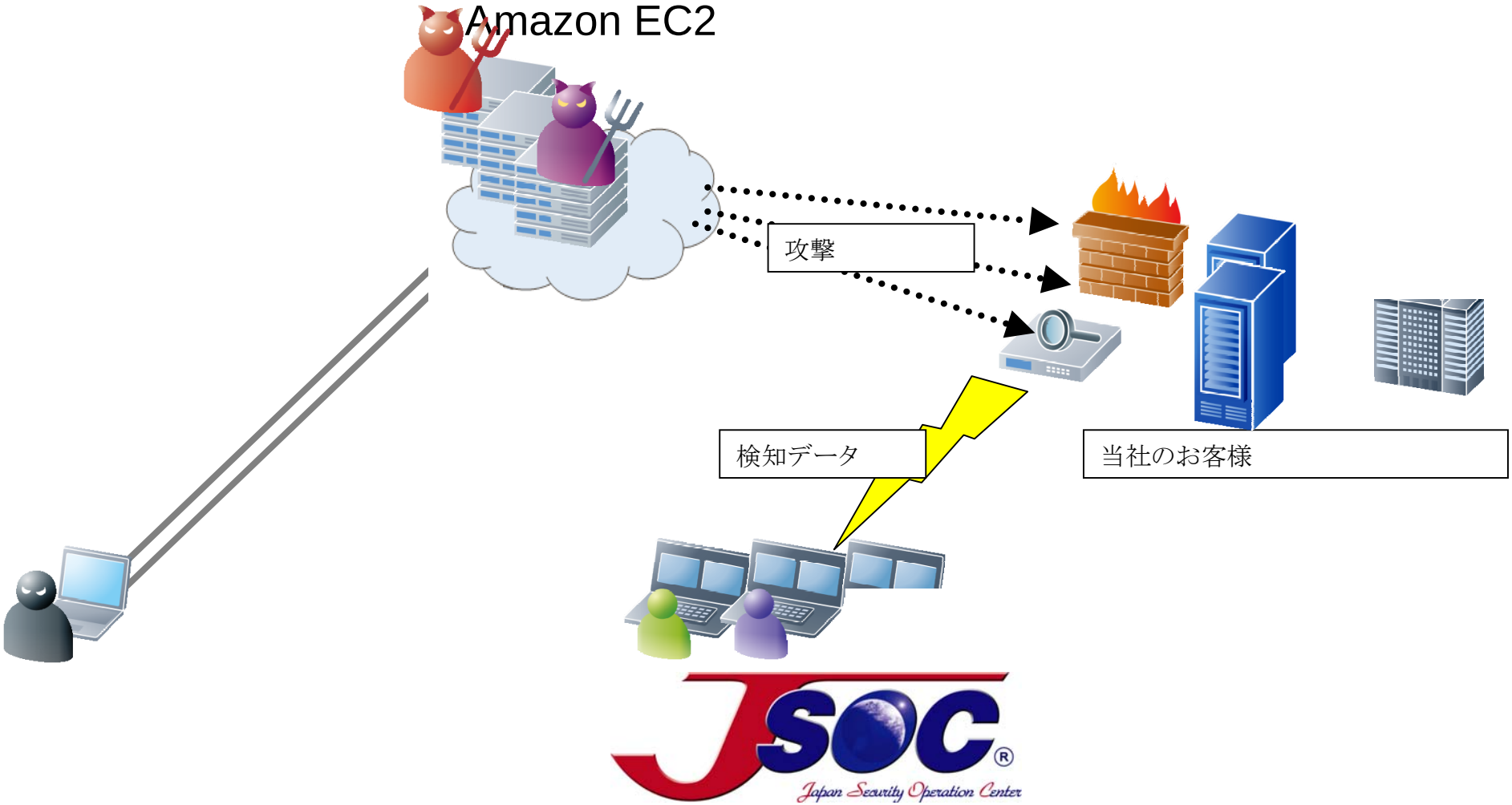
```
$ echo "aHROcDovL2JpdC5seS9SNlNUViAgaHROcDovL2JpdC5seS8yS29Ibw==" |
openssl base64 -d
hxxp://bit.ly/R6STV hxxp://bit.ly/2KoHo
```

OK, a couple of links. One is dead (to a pastebin), one is live.

pastebin.com/pastebin.php?dl=m5222dc70

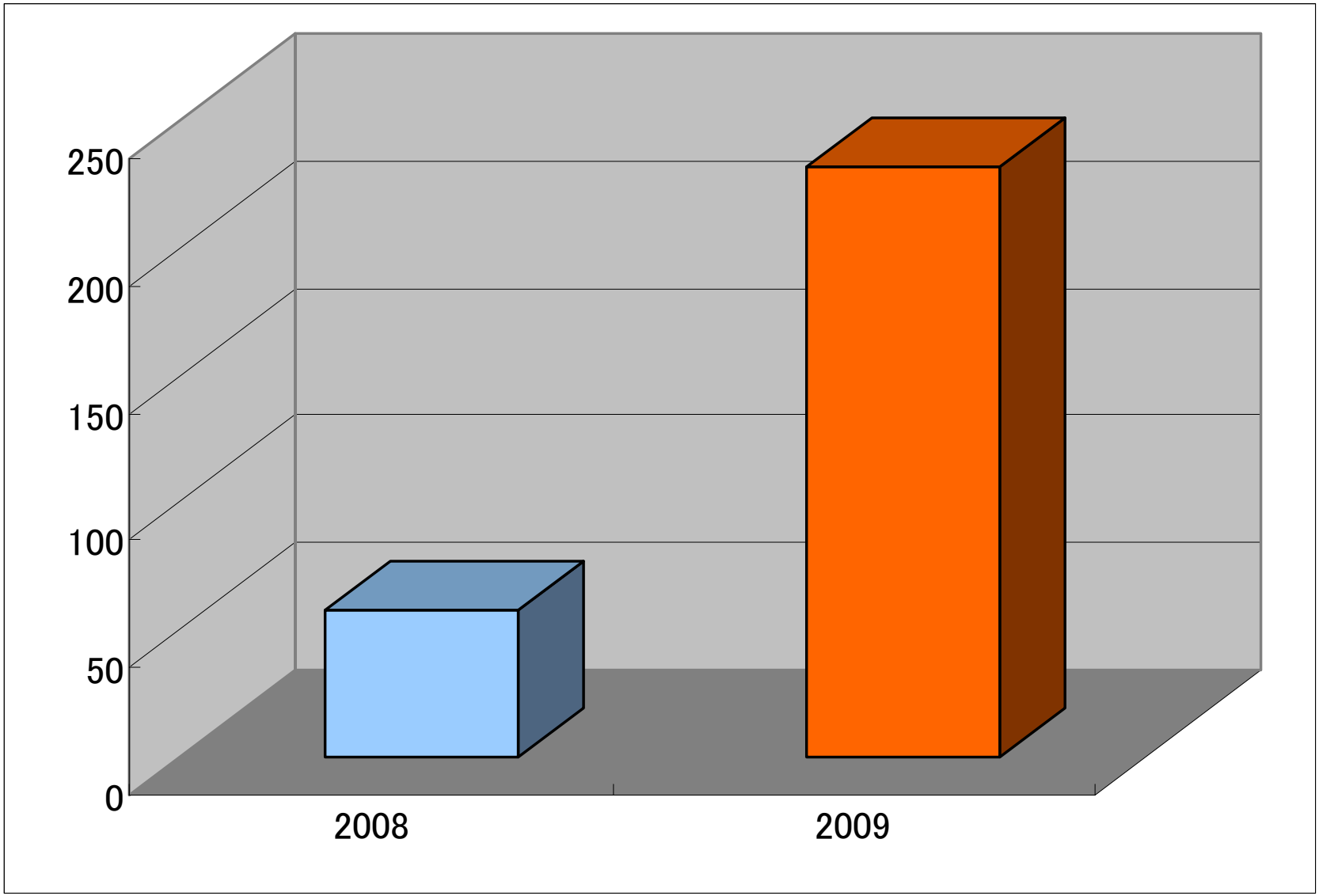
paste.debian.net/43529/download/43529

Copyright ©2010 Little eArth Corporation Co.,Ltd.



Copyright ©2010 Little eArth Corporation Co.,Ltd.

Amazon AWSからの攻撃(LAC JSOC調べ)



Copyright ©2010 Little eArth Corporation Co.,Ltd.

Amazon EC2からの攻撃の特徴

- 2008年にはほとんどなかったが、2009年にはWebアプリケーションの脆弱性を狙う攻撃が内訳として増加した
- 迷惑メールの踏み台利用可能かどうかを調査する活動もみられた

Amazon EC2に関連した情報セキュリティ上の話題

- 世界最大の反迷惑メール組織(Spamhaus)がAmazon EC2をブラックリスト指定

- ファイル共有ソフトShareへの攻撃

Copyright ©2010 Little eArth Corporation Co.,Ltd.

SIPスキャン/総当たり攻撃

VoIP Tech Chat

Patrick and

Amazon EC2 SIP Brute Force Attacks on Rise

12 comments

Update #1: 12 APR 2010. Amazon NOC's response.
Update #2: 12 APR 2010. Amazon Statement.
Update #3: 13 APR 2010. Amazon Response.

Complaints of rampant SIP Brute Force Attacks coming from servers with Amazon EC2 IP Addresses cause many admins to simply drop all Amazon EC2 traffic. Generally, SIP brute force attacks attempt to register various peer names to a system and/or attempt to guess passwords of known/guesses peers or endpoints.

The complaints mentioned this weekend show an excessive amount of traffic; with some providers claiming 6GB of traffic dedicated to such attacks. Since we ourselves received an attack from an Amazon hosted server, we also reported and complained to the Amazon NOC/Abuse depts. ~~As of this posting, no response or acknowledgement has been received from Amazon.~~ The response from Amazon is below.

There are various techniques to assist with minimizing DDoS and Brute Force attacks, such as limiting access via the public internet, using strong passwords, not mapping extension name to peer/endpoint name, limiting simultaneous calls, and aggressively monitoring usage. Automatic blocking of abusive IP's (fail2ban, blockhosts, etc.) can also assist with minimizing damage.

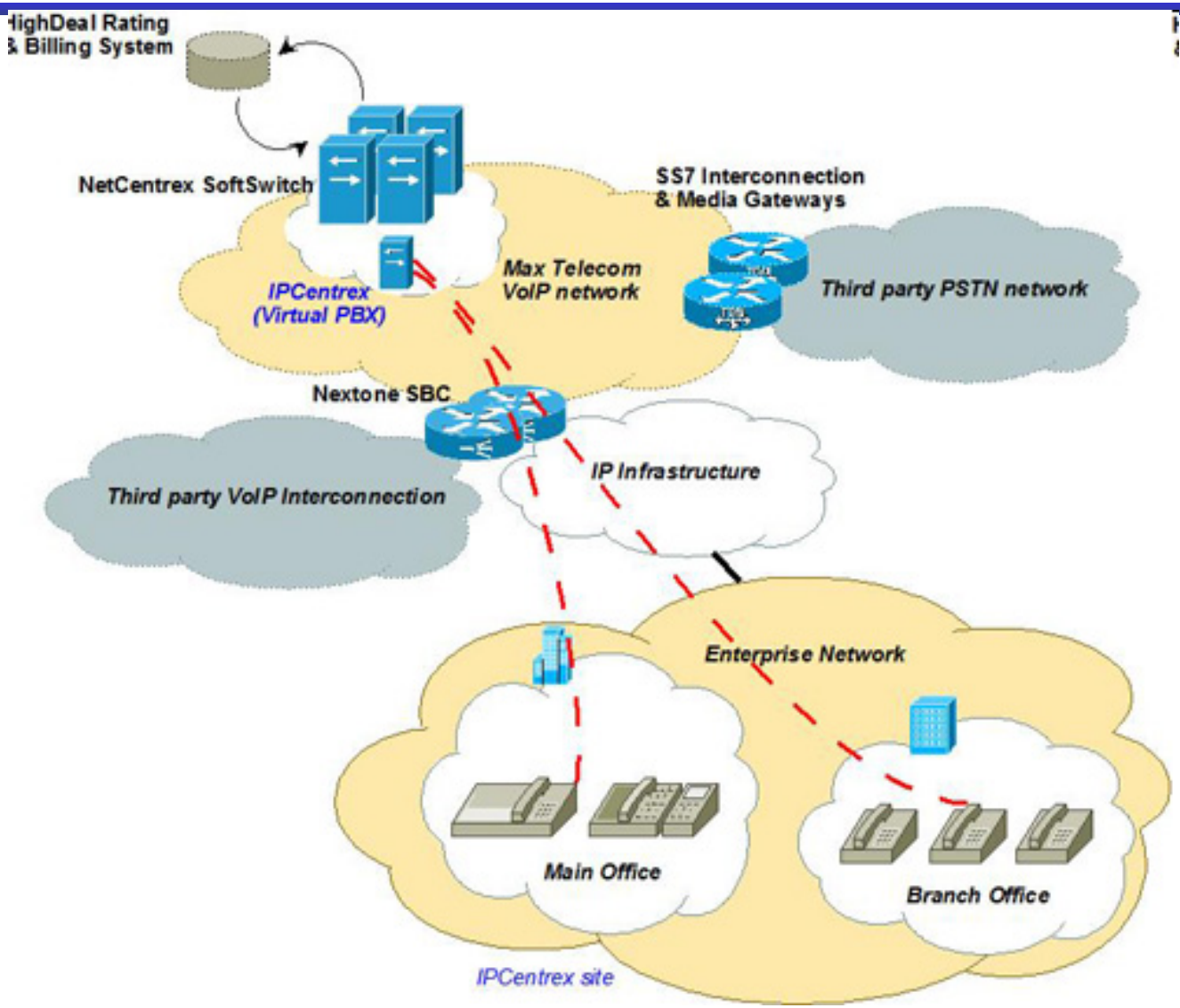
Update #1: 12 APR 2010. "Response" from Amazon's NOC

So when this happened, I submitted a report to Amazon complaining of the attack. The report was sent to their abuse and noc mails and contained the standard abuse report, including their host, my host, the protocol, ports, and description of activity; as well as a sample log.

About 48 hours later, they sent this as a response:

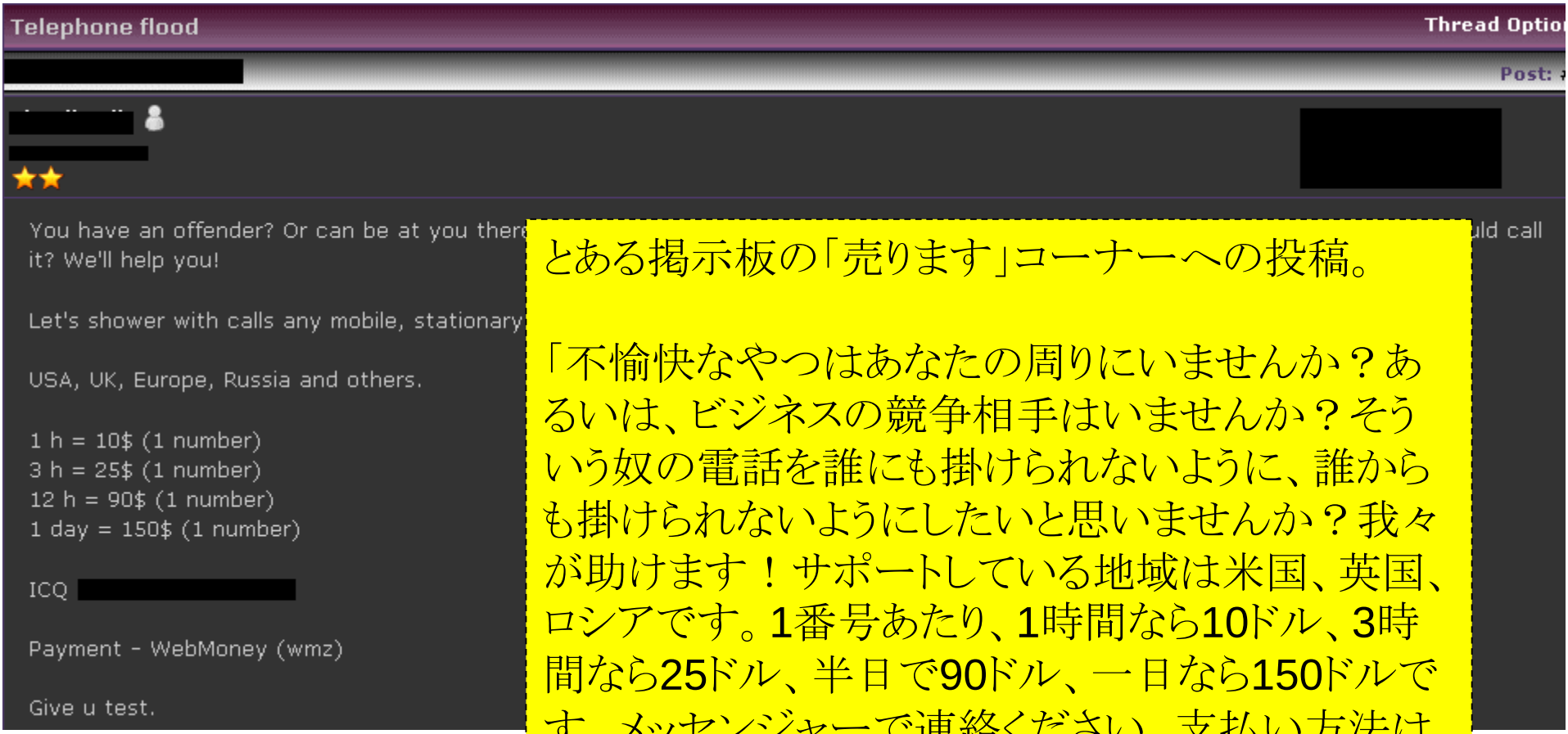
出典:http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/

Copyright ©2010 Little eArth Corporation Co.,Ltd.



出典：http://www.maxtelecom.bg/en/business/vpbx

Copyright ©2010 Little eArth Corporation Co.,Ltd.



とある掲示板の「売ります」コーナーへの投稿。

「不愉快なやつはあなたの周りにいませんか？あるいは、ビジネスの競争相手はいませんか？そういう奴の電話を誰にも掛けられないように、誰からも掛けられないようにしたいと思いませんか？我々が助けます！サポートしている地域は米国、英国、ロシアです。1番号あたり、1時間なら10ドル、3時間なら25ドル、半日で90ドル、一日なら150ドルです。メッセンジャーで連絡ください。支払い方法は電子マネーです。」

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウド活用

一般的なクラウド活用は
個人と中小企業から

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウド活用は個人と中小企業から

すでに、大企業の中でも（勝手に）使用している例も多い

仮想ストレージサービス

無料のものも数多くある

恐らく大半の組織では
違反行為だが、、、

コピー

スマートX

コピー

会社

Copyright ©2010 Little eArth Corporation Co.,Ltd.

ボトムアップのクラウド活用に企業は？

どうする？ 選択肢。

1. 禁止する。
   → いたちごっこ。やっても一時的。
2. 黙認する。
   → あり得ない。
3. すべて許可する。(受け入れる)
   → 決断
4. 安全なやり方を用意する。
   → 必然

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウド活用の原則

丸投げを受け止めるクラウドは？

丸投げは通用しない。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

知らなければならない事実と覚悟

仮想は、仮想であり、実物ではない。

VPN、広域イーサ（仮想的イーサ）、VLAN、仮想サーバ、仮想デスクトップ、
仮想ドライブ・ストレージ、仮想アプリ、仮想サイト、など

クラウドを支える基本テクノロジー「仮想化」。

この「仮想」がついたサービスは、四次元的な攻撃や事故が発生しうる。

ある面、サービス提供者は「神様」に成り得るため、その信頼度が極めて重要。→ 重要インフラのサービスがどのようなものか検証してみるのも良いかもしれない。 行政・電気・ガス・水道・金融・通信・航空・鉄道・医療・物流。
SLAの有る無し。法律の縛りの有る無し。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

じゃあクラウドに、と言っても

クラウドの浸透への見方は様々だけど、、

よく言われる、「全て雲へ」というのは、、

さぁ、素晴らしい銀河旅行！みなさんもどうぞ！

実は、まだ地球にいるんだけど。

やっぱり、物事には順番がある。

まず、地球の重力からの離脱。

その後、衛星軌道、太陽系へ、大宇宙へ！

Copyright ©2010 Little eArth Corporation Co.,Ltd.

3. クラウド時代のセキュリティ

Copyright ©2010 Little eArth Corporation Co.,Ltd.

セキュリティとは？

情報セキュリティとは、主体が客体にアクセスする上での
機密性（C）、完全性（I）、可用性（A）を守ることにある。

つまんないなぁ

こういうビジネスマン（会社）はどうですか？

何が秘密か分からない。しかもぺらぺら良くしゃべる。（C）
見積書・請求書は間違いだらけ、納品物も壊れている。（I）
連絡がつかない遅い、肝心なときに遅刻や欠勤する。（A）

実社会においては、
セキュリティの無い
ビジネスは
有り得ないということだ。

⇒ こりゃ最悪だ！

セキュリティとは、ビジネスの信頼基盤

Copyright ©2010 Little eArth Corporation Co.,Ltd.

セキュリティとは？

ちなみに有名な「　　」

4つの行動原則って、ご存知でしょうか？

Copyright ©2010 Little eArth Corporation Co.,Ltd.

セキュリティとは？

よく言われる、C（機密性） I（完全性） A（可用性）

ミスリードしやすい。
覚えやすい語呂合わせが誤解を招く。

1. 可用性（A）
   サービスを提供し続けること。
2. 完全性（I）
   間違いがないこと
3. 機密性（C）
   漏らさない・盗られないこと

Copyright ©2010 Little eArth Corporation Co.,Ltd.

セキュリティとは？

1. 組織で実施するセキュリティ（トップダウン）

① 経営意思やコンプライアンス

宣言する経営意思。
要求されるセキュリティ。例えば、プライバシーマークなど。
種々の基準・規程・ルールなどによる。
→ クラウド型サービス

② システム基盤でのセキュリティ

所謂、システム屋の仕事。
→ クラウド型サービス
システムにより異なるが、より人間をサポートするシステムでは実装は難しくなる。

お金をかける
セキュリティ

2. 人で実施するセキュリティ（ボトムアップ）

モラルの高さ。気づき。カイゼン。

⇒ プロ意識、職場の5S

お金のかからない
セキュリティ

Copyright ©2010 Little eArth Corporation Co.,Ltd.

セキュリティとは？

脆弱性をつぶしすべての脅威への予防をはかるという索は費用対効果が極めて悪い。今後セキュリティサービスを活用するうえで、対策に関して再考しておく必要がある。

セキュリティは何処までやればいいのですか？

脅威のとらえ方

ITリテラシと危険予知能力を高める

Copyright ©2010 Little eArth Corporation Co.,Ltd.

セキュリティ対策はどこまで？

セキュリティは何処までやればいいのですか？

良いリーダーとは？という命題に似ている。

決断力？企画力？統率力？実行力？包容力？・・・・

⇒ このアプローチは限りがない。

素晴らしい人を真似ても所詮、偽物。ものにならない。

⇒ スタイルの欠如！（自分のものになっていない）

そうではなく、最悪を考えてみよう！

最悪のリーダーとは？

優柔不断。手柄の横取り。責任回避。・・・

⇒ この最悪を避けるという具体的アクションから自己スタイルを！

⇒ 最悪の事態 の想定から。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

脅威のとらえ方

枝葉末節にとらわれてはいけない。

どうなるのか？どうなっているのか？を理解すること。

最終的には経営判断。場合によっては 経営者の決断 が必要

にもかかわらず、

セキュリティ上の課題を、経営上の課題に 繋げることの出来る人 が少なすぎる。

我々セキュリティ屋も、セキュリティ家 へ進化しなければならない。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

ITリテラシと危険予知能力を高める

1. セキュリティ対策を過信しない
   プロ意識。職業倫理。
   私たちの仕事の道具は何だ。どういう社会的責任を負っているのか。

2. 不審なメールの見分け方
   簡単なメールの原理、ヘッダの見方。
   クリティカルなお仕事で、オープンなメール を使用するなら 当然 のこと。

3. 信頼をおけないサイトへのアクセス方法とその後
   どんな準備をして アクセスすべきか。アクセス後にどうすべきか。
   サイトだけではなく、ドキュメントも。（どう開けるか？開けてどうするか？）

4. IT環境は、お仕事の重要な道具であり、日本を支えるインフラ。
   自分や社会が依存しているものへの理解。

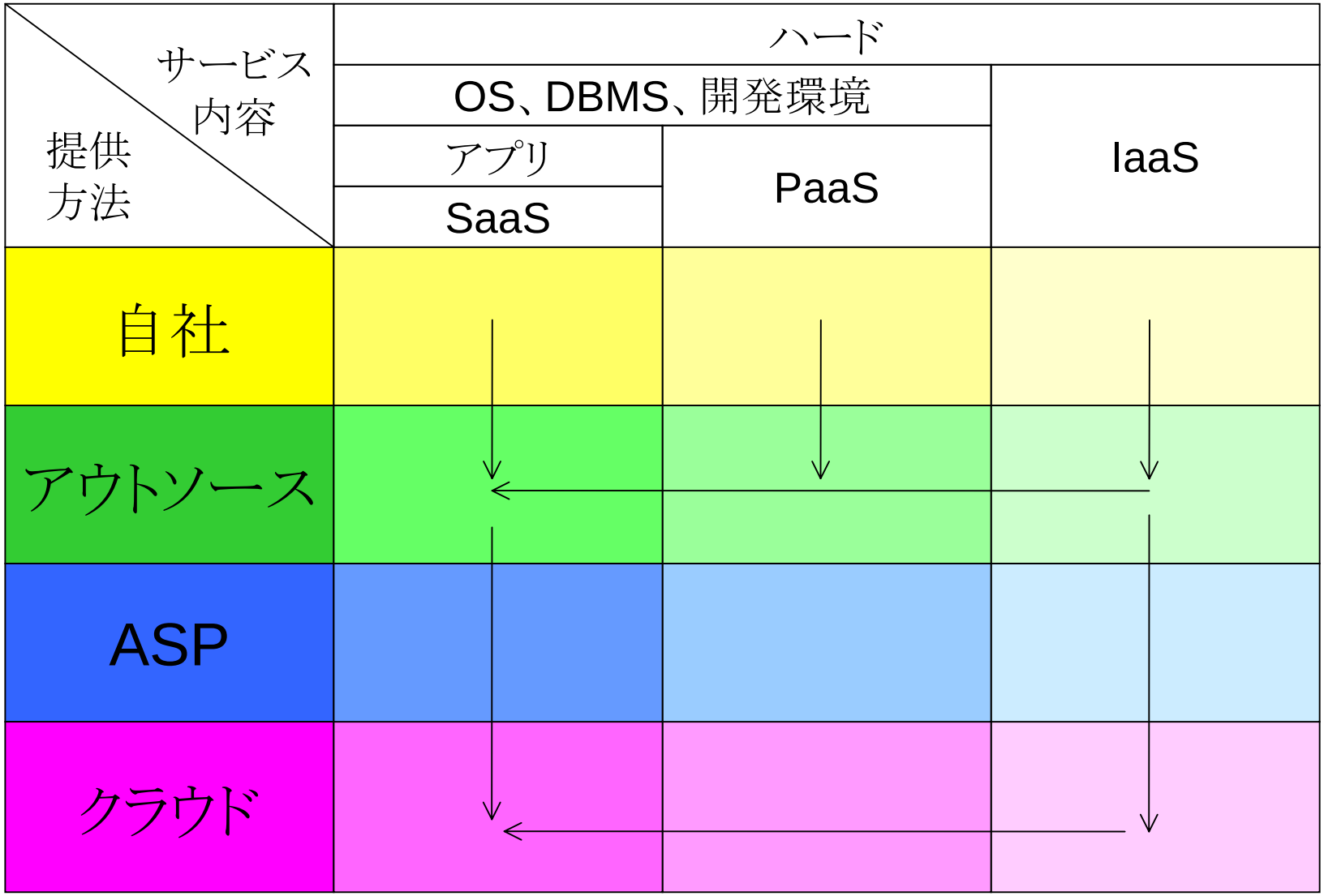
   この志の高さが、我々を救う。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

4. クラウドの形態 とアプローチ

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウド型サービス



Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウドサービスのセキュリティ

1. **IaaS、PaaS** の場合

かなり、コントロールできるはず。

うまく活用すれば、接続部分を除けば、ほとんどハード無しで、**IT**環境を利用することが可能となる。

→ 個人情報保護法の運用上の課題。

個人情報をクラウドに乗せられるのか？

廃棄の部分に課題がある。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

クラウドサービスのセキュリティ

2. **SaaS**の場合

基本的には、コントロールすることはできない。

ベンダーを見極め、評価する必要がある。

→ ちゃんと利用するには、対抗できるリテラシーが必要。

3. いずれの場合も

従量課金。 → 使用量？ 使用期間？
使用量の場合のメリットとリスク。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

4. 心得

Copyright ©2010 Little eArth Corporation Co.,Ltd.

1）自己責任

リテラシが高く自己責任で推進する組織は強い。

最終的には、そうであるならば計画的に意識の改革と移行を決断していこう。

これは、経営意思である。どのようにITを活用していくのか、そのために自組織はどうあるべきなのか？

同じレベルで考え一緒に成長できる、パートナ探しなのかもしれない。

リスクが腹に落ちているか？

Copyright ©2010 Little eArth Corporation Co.,Ltd.

2）選択肢の確認

離陸したはいいけど、イザという時には戻れるのか？
危険高度はいつからいつまで？

どこで、シートベルトサインを消灯できる？

選択肢の確認は常に怠らず。場合によっては2社のサービスを同時に受けることも考えて良い。

全体で考えたらそっちの方が安いのかもしれない。

特に、大手やグループ会社などでは相互にうまく連携し、ベンダーを活用する手もある。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

3）IT戦略

自組織のIT環境適応計画・目論見（IT戦略）

1. インターネット関連
2. 基幹系
3. 情報系
3. 社内オフィス系
4. デスクトップ
5. ネットワークインフラ
6. 地域、拠点、組織

仮想化、クラウドへの適応方法

Copyright ©2010 Little eArth Corporation Co.,Ltd.

4）ボトムアップ

トップダウンでの推進が必ずしも良いわけではない。

現実を探りながら推進し、トップダウンとバランスをさせること。

＝最初は「必要な人」がボトムアップで推進し、
　見極めて全社展開

Copyright ©2010 Little eArth Corporation Co.,Ltd.

5)ベンダーの嘘？への対応

どこのベンダーも最初は導入を決めたい。

「対応します。」「やらせます。」「努力します。」

それ、対応して本当にクラウドとしてやっていける？
どこも、枯れたベンダーはない。
早く限界利益を超えたい。

環境に適応できる「嘘」なのか？
どこも、あるボリュームを超えないとペイしない。
あるところまで行き着かないと、
それなりのサービスは出来ないはず。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

6)ベンダーを育てよ

前述の通り、どこもキツイ。

自分自身も成長する中で、付き合うベンダーを決めて「育てる」、相互に発展する信頼モデル。今後は真の意味での**Win-Win**の関係が重要になる。

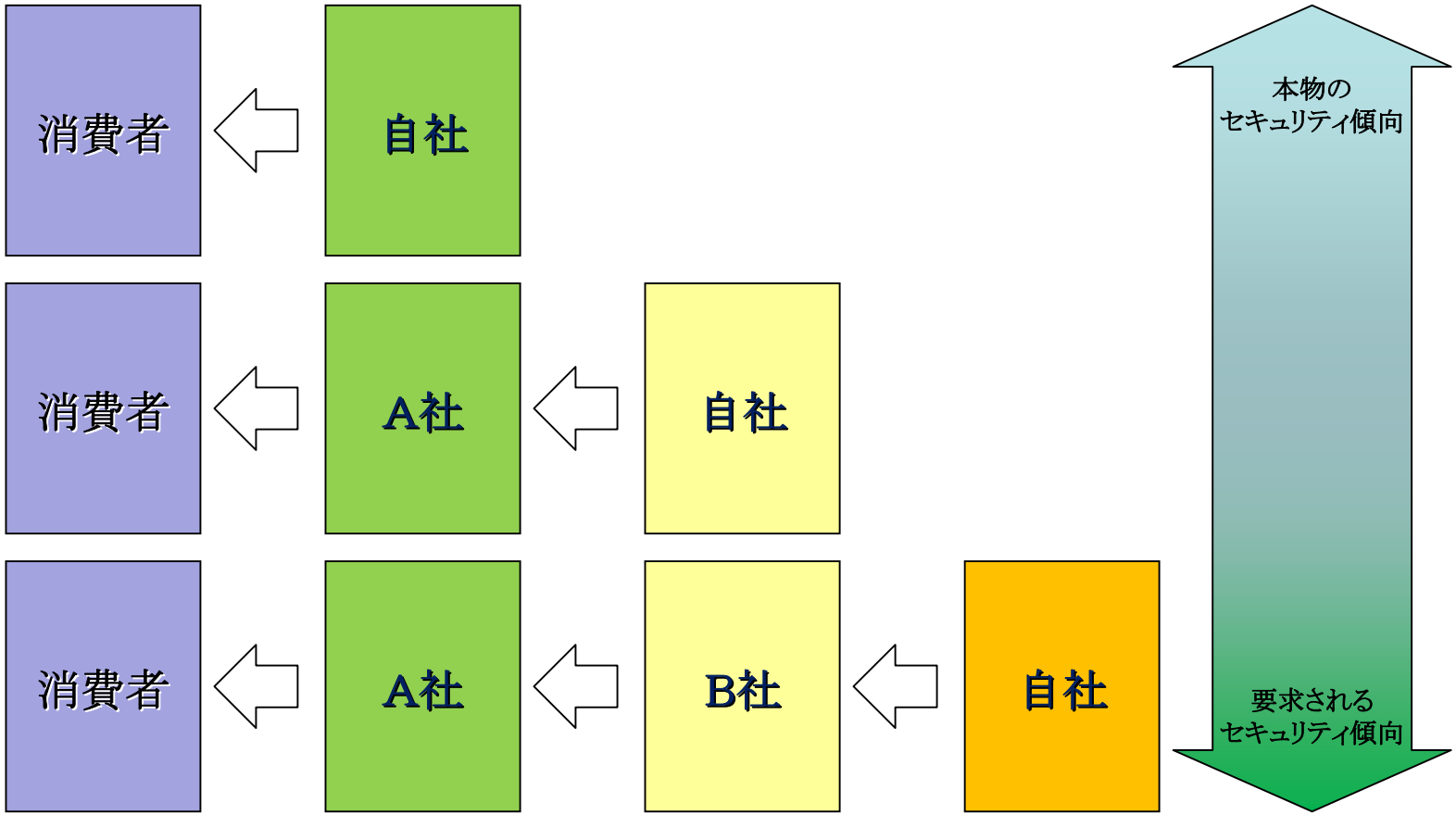
それを自組織の体力に合わせて推進

ベンダーへの過剰なサービス要求は「天に唾」の危険性も。自組織がどこに向かい、どういう運営をしたいのか、考慮した付き合いを戦略的に。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

6）立ち位置を知ろう

中小企業といっても、立ち位置はさまざま。



Copyright ©2010 Little eArth Corporation Co.,Ltd.

最後に

クラウドへの適応は、ある面、

従来の相互依存社会（所謂、ガラパゴス国家）の破壊と、捉えることができる。

どうせやるなら、環境適応をはかりつつ、生き残りを、模索したい。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

最後に

クラウド関係する技術や運用への知見は、枯れているわけではない。

ベンダーはそちらを目指し、活用する組織も多くの期待を寄せ、幻滅し、場合によっては、打ちのめされ、その後、地に足をつけて立ち上がっていくことだろう。

いち早く、その経験を積み、立ち上がっていく必要があると、感じているからこそ、半信半疑でも、幻滅しながらも、雲のかかった峰にチャレンジしているのだと思う。

自己責任の第一歩はITリテラシと
最低限のセキュリティ文化を
身につけるところから。

Copyright ©2010 Little eArth Corporation Co.,Ltd.

最後に

そうは言っても、**中小企業**

セキュリティなんか、
人もいないし、
かまっていられないのですが。

安いセキュリティ。
残念ながら、そういうものは存在し得ない。

→ じゃぁ、どうすれば？
スマートXやクラウドを使い倒しませんか？

Copyright ©2010 Little eArth Corporation Co.,Ltd.

ありがとうございました。

Any question ?

世界トップレベルのセキュリティノウハウで、
日本のスタイルを支える。

LAC
Little eArth Corporation

株式会社ラック
http://www.lac.co.jp/
sales@lac.co.jp