「永遠のビギナー及びノーガード戦法」に対して私たちが出来ること

JNSA政策部会 BoF

2008年12月17日

このBoFの表番組　U40（ユーフォ）覆面座談会

役割の異なる組織から精鋭のユーフォーによる座談会らしい、、、
聞いてみたい方は、まだ間に合います！
緊急パッチの話題も出るかも！

さて、

始めましょうか！

永遠のビギナー

現状の対策や課題に関する共通的な事項として、特に、対策実施主体である利用者（個人）について、情報セキュリティ対策に対する意識やスキルが必ずしも高くないと考えられる、いわゆる「永遠のビギナー」に、自らの責任だけで情報セキュリティ対策を全面的に託すことは難しいと考えられるとの指摘が多数なされている。

永遠のビギナーは、年少者や高齢者など、これまでインターネットを利用する機会が少なかった者も幅広くインターネットを利用する環境となっていくことにより増加すると予想されるうえ、現状では何ら問題を感じることなく利用している場合であっても、情報通信機器の高機能化やサービスの多様化により、期せずして、こうした層になってしまう利用者もあると考えられる。

～ 総務省 次世代の情報セキュリティ政策に関する研究会 中間報告書 2008年4月4日

永遠のビギナー

何故問題なのか？

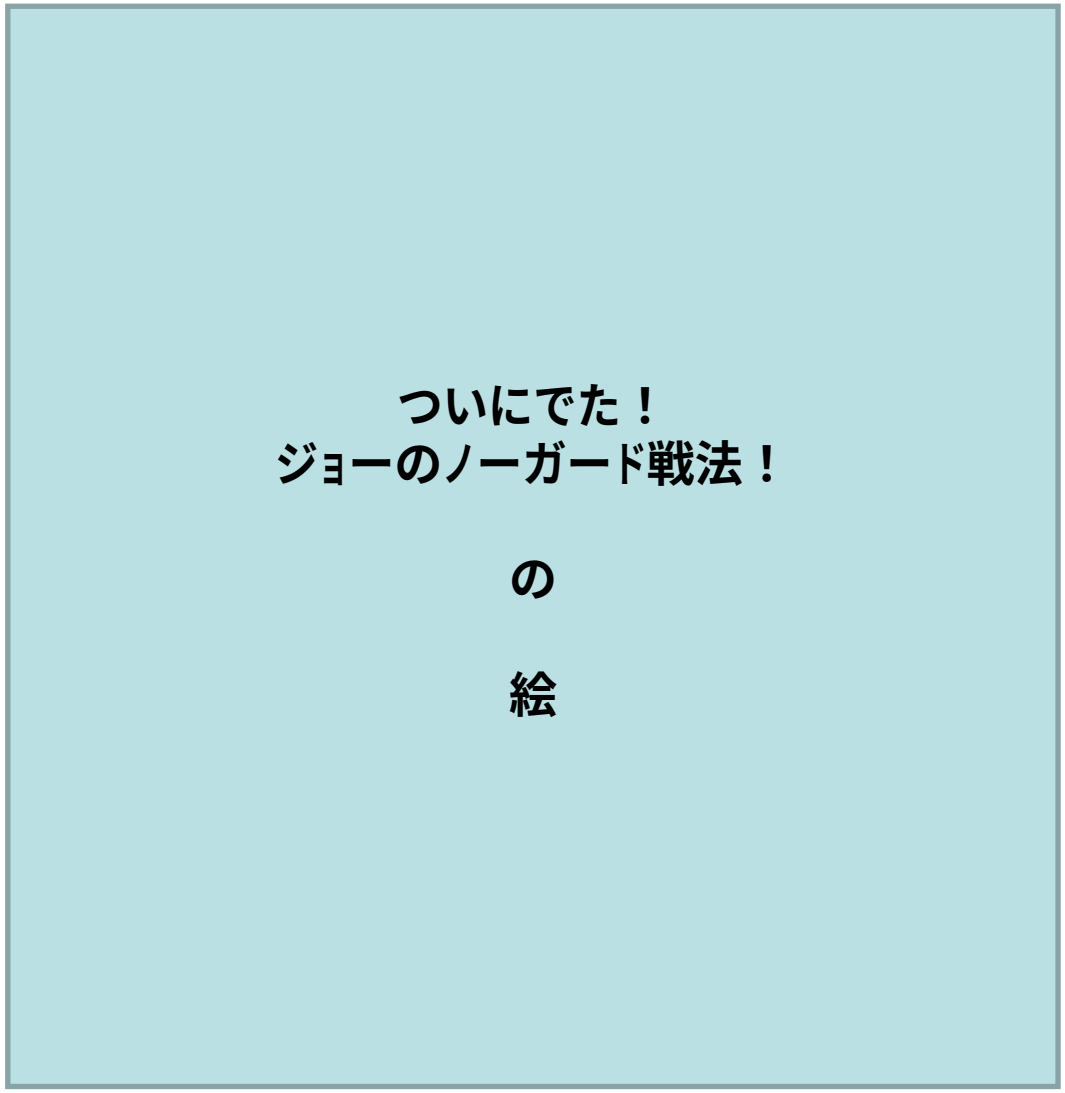
1. 踏み台になり、他者に迷惑をかける。ネット社会の治安を間接的に悪化させる。

2. 自ら被害にあい、ネット社会のコスト増につながる。

3. 被害を想定したり、保障することで、その金額相当分を市場とする犯罪の産業化を促進してしまう。

例:クレジットカード業界の被害見積もり？
インターネットバンキングでの不正被害補償？

ノーガード戦法



ノーガード戦法

サイバー・ノーガード戦法（サイバー・ノーガードせんぽう）とは、コンピュータやそのネットワークに於けるセキュリティ意識に欠ける企業や組織の対応を揶揄する際に用いられる用語。ネット上で生まれた用語であり、実際にこのようなセキュリティ対策が行われているわけではない。

2000年代に入ってから頻繁にニュースで報じられるようになった日本における個人情報の漏洩事件に絡み、コンピュータセキュリティ筋で同語が用いられる傾向が見られる。

これらは漏洩を発生させた企業内の情報管理に於ける危機管理意識や質が、保護されるべき対象情報・コンピュータの急速な増大に追いついていないために相対的に低下している事とともに、長らく続く平成不況によるコスト削減や技術者の絶対数不足などに起因する技術上の保安措置不足もその要因に挙がっている。

利用されているコンピュータの中には、個人情報などの重要情報が、外部のインターネットから容易に閲覧できるような状態で放置されているような所もしばしば見られ、これを揶揄する形でも同語が使用される。

その一方で、不正アクセス禁止法の制定当初から、セキュリティホールの放置などといった「不正アクセスの誘発」という面を考慮していない同法の制定は、企業のセキュリティ意識の低下を招くおそれがあるといった指摘もされていた。

同語が扱われる局面で重要な点は、企業情報や顧客情報など、その企業にとっては命運すら握る筈の重要情報の管理が杜撰になされている事であり、特にその企業を信頼して個人情報を預託したはずの顧客の個人情報に対する、企業の個人情報保護の責任の放棄とも言える方策である。被害があれば、企業は被害者としての面を強調するが、情報の保護を怠ったことはセキュリティを破ったクラッカーと同程度・またはそれ以上に責任を問う必要があるだろうとする意見が複数セキュリティ関連筋から出ている。これが「同語の（皮肉による）絶賛」という形を生んでいる。

※ サイバー・ノーガード戦法 出典: フリー百科事典『ウィキペディア（Wikipedia）』

ノーガード戦法

1. 専門家としての葛藤

緊急対応現場。経営者談「人並み以上にはやっていると思っていた。」
⇒ そんなことは、常識外と叩き潰すのか？
数十万人の顧客。商売は繁盛（＝必要とされている）
如何に再開させるのか？

2. ケースはある。

1）本当に知らないケース
IPAやセキュリティ関係の事件報道など、、（知ってても知っているとは言えないだろうなぁ）

2）確信的
正直、ある時期においては経営的に正しい決断なのか？

ノーガード戦法

何が問題なのか？

1. 利用者はしっかりしてくれていると勘違いしている！？

2. 開き直るのは許せん！？

3. 永遠のビギナーと同様の問題
   踏み台 ⇒ 現在も日々発生している改ざん事件と密かに直す人々

   自己被害により結果コスト増となる

   保護政策により犯罪が産業化する

犯罪の傾向（西本私見）

悪党は本来、銀行などから現金をがっちり頂戴したいと思っている。
⇒ ハイリスク

「アラパス」の動向

サイトから直接SQLインジェクションで抜いていく
サイトにSQLインジェクションで侵入しバックドアを入れて、それ経由で抜いていく
サイトを改ざんし、利用者のPCにボットを潜ませ、抜いていく

当該サイトへの成りすまし（特にカードを登録しているサイト）
同一アカウントを使用してる他サイトへの成りすまし（オークション、バンキング他）
同一アカウントを使用している決済への成りすまし

⇒ セキュリティ対策を行わないサイトや人たちが標的となってきている。

パターナリズム (paternalism：父権主義)

パターナリズム (英: paternalism) とは、強い立場にあるものが、弱い立場にあるものに対して、後者の利益になるとして、その後者の意志に反してでも、その行動に介入・干渉することをいう。日本語では「父権主義」「温情主義」などと訳される。語源はラテン語のpater (パテール、父) で、pattern (パターン) ではない。

社会生活のさまざまな局面において、こうした事例は観察されるが、とくに国家と個人の関係に即していうならば、パターナリズムとは、個人の利益を保護するためであるとして、国家が個人の生活に干渉し、あるいは、その自由・権利に制限を加えることを正当化する原理である。

※ パターナリズム 出典: フリー百科事典『ウィキペディア (Wikipedia)』

パターナリズム (paternalism：父権主義)

パターナリズムの典型例

専門家と素人

専門知識において圧倒的な格差がある専門家と素人のあいだでは、パターナリスティックな介入・干渉が起こりやすい。たとえば、医師（専門家）から見れば、世話を焼かれる立場の患者（素人）は医療に関して無知蒙昧であり、自分で正しい判断を下すことが出来ない。その結果、医療行為に際しては、患者が医師より優位な立場には立てない。そうした状況で患者の自己決定権をどのように確保していくかについては「インフォームド・コンセント」の項を参照（あわせて「尊厳死」の項も参照）。

国家と国民

国家がいわば「親」として「子」である国民を保護する、という国家観にもパターナリスティックな干渉を正当化する傾向がみられる。実際に施行されている事例としては、自動車運転者に対するシートベルトの装着義務化（道路交通法71条の3）、賭博禁止（刑法186条）などが挙げられる。こうした立法措置以外にも、官公庁による行政指導や、市町村における窓口業務などにも同様の傾向がみられる[13]。

※ パターナリズム 出典: フリー百科事典『ウィキペディア（Wikipedia）』

何が出来るのか？

1. 啓発活動

1) 少しでも、減らしてリテラシーを上げる努力。

2) でも、そもそも、興味が無い。

3) ノーガードのほうは確信的に実施。（立ち上がり時から真面目にできない？）

⇒ 立ち上がり時に支援できることはあるのか？ U40ラボが守るぞ？？？

何が出来るのか？

2. 保護活動

1) 余計なお世話がどこまで通用するか？

何が出来るのか？

3. 補償

犯罪の産業化と如何に向き合うか？

⇒ 本来は補償分は犯罪者に与えるのではなく、、、

セキュリティ業界が得ていかなくてはいけないのではないか？

何が出来るのか？

4. さらす

誰が？どこに？

議論！議論！議論！