METEORA SYSTEM

Advanced TCP/IP コンセプト

サイバーテロの時代を終わらせる基盤: サイバーテロリストの自由を劇的に制限する

メテオーラ・システム株式会社（神奈川県伊勢原市，代表渡邊栄治）は，1970 年代から情報理論の研究とその実装技術の開発を進めてきました．今後は，ゼロトラスト・ソリューションを開発されている企業様への技術提供等を模索して参ります．協業，共創に関するお問合せをお待ちしております．

Contents

1. インターネットの約束を継承するために

本ペーパは，サイバーテロに関する最近の話題を引用することに依り，「Advanced TCP/IP」という解決とそのコンセプトを紹介するものです．以下のトピックスを含んでいます．

- 本コンセプトは今の ”Internet Protocol Suit” のアップグレードに位置付けられます．
- 本コンセプトは当社知財から派生した普遍的な技術です．すなわち，数学的防衛技術です．パッチ技術ではありません．
- 本解決はバックドア（ウイルスを含む）と DDoS 攻撃の自由を劇的に制限します．
- サイバー攻撃者がゲートウェイを通ってネットワークに侵入し，Advanced TCP/IP 通信チャネルを自由に移動することは不可能です．

サイバーテロに自由を与えた者は誰でしょうか?インターネットは，何と言っても，開放性と匿名性を特色にしています．なぜなら，開放性と匿名性を約束している技術が Internet Protocol Suit (TCP/IP) だからです．

たとえば，Bill Gates 氏は 1995 年，TCP/IP を OS に含めて開放性，自由，普遍性の約束を世界に実装しました．しかしその約束は，サイバーテロに自由を与えることになりました．Advanced TCP/IP はインターネットの約束を継承しながら，サイバーテロの自由を劇的に制限します．

2. “Yahoo! インシデント” (2000 年 2 月 21 日)

2000 年 2 月から 20 年以上経った今も，サイバーテロは勢いを増す一方です．何故でしょうか？その間，NIST も国際機関も怠けていた訳ではないでしょう．実に多くの標準化活動を行ってきましたが，サイバーテロは勢いを増す一方です．

世界は事件が起きる度に，攻撃を受ける側，つまりターゲットに対策を求めてきました．同じことを今も議論しています．たとえば，この 2021 年 10 月に開催されたオンライン国際会議においても，やはり世界は企業に対策の強化を求めたり，国際的包囲網の構築などを訴えて，いつも「目に見える」 範囲を議論しています．

3. もう少し掘り下げた議論

U.S. Cyber Command は 2020 年，サイバー防衛に関する技術課題をまとめた文書を公開しました．この II 章（モニタリングと可視化）には，重要な指摘があります．

> サイバー侵入者は，ゲートウェイ・ノードを経由してネットワークにアクセスし，その後，何日も，何ヶ月も，あるいは何年もかけてネットワーク内を横方向に移動することがあります．
>
> 侵入者を検知し，その動きを追跡し，ネットワーク全体のリスクを推定し，防御対策を施し，被害や情報公開を評価することは，すべて技術的な課題です．

以上の課題を解決する実装技術が Advanced TCP/IP です．これはパッチ技術でなく，また，NIST 標準を組み合わせたシステムでもありません．C.E.Shannon の数学に基づく防衛技術です．

4. バックドアキラー -証明がなくともバックドアは存在している-

サイバーテロの特性: バックドアは Internet Protocol Suit (TCP/IP) を利用するので，攻撃を受ける側（ターゲット）がどれほどセキュリテイを強化したと主張しても，それは何の効果も持ちません．鍵管理やパスワード管理を強化しても，バックドアには何の係わりもありません．

サイバーテロリストは，いつでも，自らの意思で，予告もなく，作戦を開始することが出来ます．攻撃の予兆が無いということです．バックドアは出荷時や保守時に仕掛けられることが多く，その存在を証明した人は未だ居ません．その理由はなぜでしょうか？

理由は単純です．Internet Protocol Suit (TCP/IP) そのものがバックドアだからです．この気付きによって，当社の発明を活用する Advanced TCP/IP のコンセプトが導かれました．

5. 当社のバックドアキラーに比較対象はない

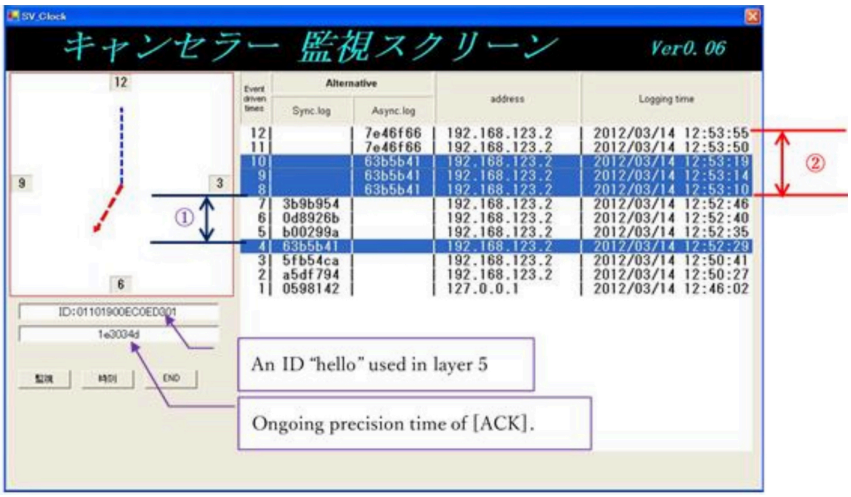
Internet Protocol Suit (TCP/IP) は，IP 層に IP アドレスという識別子を持ち，TCP 層には PORT 番号という識別子を持ちます．識別子はこの二つだけです．OSI 参照モデルの第 5 層はポート間の仮想通信路です．この仮想通信路に第三の識別子を持たせることで，バックドア・キラーが実現します．ですから，比較対象が無いと言えます．

仮想通信路に識別子を持たせた時，何がどう変わるのでしょうか？→バックドアがある日，通信路を確立しようとしても，その識別子のシステムはバックドアの通信路を選択的に切断します．

6. 超微細タイムスタンプ

このスタンプはバックドアの通信路を選択的に切断します．新たな識別子のシステムはコンピュータの TOD (Time of Day) に同期する 256[bit] の乱数です．超微細タイムスタンプの可視化（ログ）を以下に掲載しました．

① の系列「Synch. Log」は，通信路 ハイジャックが無い時刻を表しています．
② の系列「Asynchronous Log」は，通信路ハイジャックが自動的に切断された時刻を表しています．



7. なぜバックドア通信路のみを遮断できるのか?

バックドアのパラメータは出荷や保守の時に設定されます．これらパラメータ群はすべて過去の時制です．仮に，超微細タイムスタンプを盗んだとしても，潜伏している間に時が経過し，バックドアの時制はやはり過去になります．

そして，バックドアがコネクションを確立しようとした時，一つの ID に二つの超微細タムスタンプが存在することになります．それで，バックドアは即座に検知され，その超微細タイムスタンプは ②「Asynchronous Log」に分類されてしまうのです．このようにシステムを設計することができます．

8. DoS 攻撃と DDoS 攻撃

サイバー攻撃，特に DoS 攻撃は，TCP/IP を利用するから，ターゲットがどれほどセキュリティの強化を叫んでも意味はありません．攻撃者は，いつでも，自らの意思で，宣戦布告をすることなく，作戦を開始することがで

きます．宣戦布告が無いが，国内が戦場になるということです．そして，攻撃を受ければ国内ターゲットはまるで魔法にかかったように「しびれる」．

しかし，Advanced TCP/IP は立場を逆転させます．プロトコル・ロジックだけを開示すると，攻撃者がネットに [ACK] を投げても [SYN+ACK] が返って来ない，その間，攻撃者のコンピュータ群は「待ち状態」を強いられる，つまり，攻撃者のコンピュータが「しびれる」というわけです．

9．概念実証は既に終えた

超微細タイムスタンプは第 5 層の仮想通信路のログです．これが Advanced TCP/IP の概念を実証しています．なぜなら，DoS 攻撃者がネットに投げた [ACK] は，②「Asynchronous Log」に分類されてしまい，ネットは [SYN+ACK] を返さないからです．

たとえば，誰にも気づかれないとテロリストが思っても，超微細タイムスタンプは DoS 攻撃の [ACK] に返事を返しません．このように，DoS 攻撃に対抗できるのは今の TCP/IP ではなく，Advanced TCP/IP です．これが，サイバーテロの時代を終わらせる基盤です．

10．民主主義の約束

民主主義の弱みについて考えてみます．アメリカの良さは，外からの脅威が現れれば，党派を超えて団結する点です．アメリカに亡命したウイルス学者イェン・リーモン博士に依れば，CCP は，人種差別などの事件が起きる度に，その対立を煽り，アメリカの分断工作を進めた，「その分断が最高潮に達するのが大統領選，そのタイミングこそ生物兵器を使用する絶好のチャンスだった」と言います（Cited from Magazine “The Liberty” November 2021 No.321）．

テロは，それが戦争だということに我々が気づかないタイミングを狙って実行されます．テロに気付かないほど，我々は何かに熱中しています．そうしてテロに自由を与えます．テロリストは常に次のタイミングを計算しているということです．

11．テロの自由を制限するために

分断ではなく，The CleanNet が必要です．超微細タイムスタンプは CleanNet ID を与えられた者にコネクションの確立を保証します．テロリストが ID を盗んでもサイバーテロに使うことはできません．

このようなプロトコルが今の民主主義には欠如しています．たとえば，Trump 前大統領のアカウントが削除される事件がありました．これは団結ではなく，分断を激しくする行為です．このようなやり方でなく，今のネットを Advanced TCP/IP にアップグレードするべきです．

そうすると，ユーザ一人一人に CleanNet ID が与えられ（このとき，個人情報の登録を求めない），超微細タイムスタンプの刻印されたそのネットは，生き物と考えてみてください．生き物ですから，この CleanNet のアカウントを人が削除することは殺人に値する，そう考えることもできます．

12. 本リリースに関するお問合せ

METEORA SYSTEM Co., Ltd

https://www.meteora-system.com

