METEORA SYSTEM

当社知財の紹介

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．本リリースでは，情報理論的な数理に基づく 2 つの知財について，下記の通り紹介します．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．

目次

1．はじめに

政府や民間は日々，サイバーテロの脅威と闘っています．これまで，「セキュリティ」や「ソリューション」と名付けられた製品やサービスが次々に生み出されながら，問題は解決されないまま 20 年もの時間が経過しました．この歴史を検証すると判る通り，対策はサイバー防衛を達成していません．これは，「対策技術では問題を根本的に解決できない」という重要な教訓です．対策という言葉に頼らない，騙されない，抜本的なサイバー防衛技術，すなわち問題を「解決」できる技術に，政府や民間のリソースを割くべきではないでしょうか．

当社を例にとれば，既に，問題を解決できる技術を 2 つ完成させました．零細企業でありながら，補助金に頼らず，外部からの資金調達にも頼らず，独力で成し遂げました．このことは，多くの同胞たちが自発的に，リスクを取って協力して下さった証です．当社技術は 2 つとも，概念実証を 2015 年以前に完了しています．しかし，残念ながら，政策担当者にこれを提案する窓口が日本には用意されていません．当社は，当社の技術を活用できる方との出会いを求めています．知財の 1 つは 3-way handshake に関する実装技術，もう 1 つは，ポスト量子暗号

に相当する，暗号学的な鍵の知識分割に関する実装技術です．これらの知財は PoC を経た，情報理論的な数理と実装プロトコル，そして特許を含む，サイバーテロの時代を終わらせる技術です．

1974 年の ”Internetwork Transmission Control Program” は地球規模の文明実験でした．これは第 1 回目の文明実験です．当社は，この 1974 年からのトレンドを ‘サイバーテロの時代’ と定義しています．完璧なサイバー防衛はできない，という常識を破ることが，当社の知財のミッションです．すなわち ‘サイバーテロの時代を終わらせるミッション’ です．当社知財には，その力が論理的に備わっています．これは第 2 回目の文明実験です．

第 2 回目の文明実験を成功させるために，当社には新たな出会いが必要です．1974 年の当時（第 1 回目の文明実験）は，米国の政府機関が主導していました．第 2 回目の文明実験を主導するのはどこか? このように考えると，6 兆ドルとも予測されているランサムウェアの被害額は具体的な指標です．1974 年にはこのような明確な指標はありませんでした．この指標は，‘問題を解決できる技術’ に政府や民間が投資する意義と根拠です．

2. 当社のソリューション

IP 1: バックドアやウイルスの 3-way handshake を即時に検知し，強制的に排除する実装技術

特徴: 不正な通信コネクションの試みが成功する確率 = 0

IP 1 には次のような特色が有ります: バックドアやウイルスの 3-way handshake は，選択的かつ強制的に 「コネクションエラー」を起し，通信路を通れなくなる．たとえば，通信路の識別子を盗めば，通常であれば通信路を乗っ取ることができますが，この技術によってこのような攻撃は「コネクションエラー」を起します．このアルゴリズムとプロトコルは特に，DDoS 攻撃においては攻撃者を麻痺させます．この技術の実証と試験運用は 2011 年以前に終了しました．この時はレイヤー 5 で実施されました．これからは，レイヤー 3 とレイヤー 4 に実装することが期待されます．

特許明細書には， Hyper-fine time stamp（第 3 の識別子）について，あえて触れていません．特許には Hyper-fine time stamp の基礎（初期値の更新）を請求しました．これが何を意味するかを NIST（2012 年当時）は見抜き，「図 4 マトリクス表現」を著作物として登録するよう求すすめ，当社はこれに応じました．先見の明あるベンダーが 2 次製品を商業化し普及させれば，ネットのプライバシーを保障しながら，不正なコネクション確立の試みに自由を与えないネットを実現できます．当社はこれを「CLEANNET」と呼んでいます．

IP 2: 暗号学的な鍵（x1）の知識分割および二重制御の実装技術

特徴: 不正なユーザ権限の乗っ取りが成功する確率 = $1/2^{256}$

通常，ランサムウエアは LAN に侵入した後，パスワードファイルを奪い，ユーザの職務権限を乗っ取り，DB にアクセスします．この動作は，本知財によって無力化されます．この技術は PCI DSS v1.2 が求めた鍵管理（知識分割と二重制御）を実現しています．「職務分離と合意プロセス」と言い換えることができ，これをネットにどう実装するかを，v1.2 は見出せなかったことは周知の通りです．2013 年，当社は一方向関数のペアを発見しました．これが知識分割と二重制御（職務分離と合意プロセス）の実装技術です．現在，実例としてサーバに実装したデモ版を実演，貸出すことができます．因みに，コンセンサスアルゴリズムとしてこれをブロックチェーンに応用

することで，プライバシー，ファイナリティ，スケーラビリティ等のトレードオフを解決することができます．つまり，紙幣と完全に互換のデジタル通貨を創ることも，本知財によって可能になります．

IP 2 の真価は，サービス側がアカウントを管理しないことです．アカウントは従来，サービス側が管理していますが，この実装形態ではアカウントがネットに分散します．ネットはユーザの認証にパスワードファイルを必要とせずに，これまで通りのサービスを継続することができます．たとえば，紙幣は個人情報の登録を求めず，支払い時にパスワード入力を求めず，決済データも記録しません．これは，紙幣と人との間にコンセンサスアルゴリズムがあるからと言えます．つまり，紙幣は，単純で平凡ですが，非可換アルゴリズムのモデルです．2014 年，当社はこの概念実証に成功しました．Adam Back の Hashcash 由来の PoW より格段に優れた，情報理論的なアルゴリズムが実装されています．この知財によって，ウイルス（ランサムウエア）を無力化するネットを創ることもできますし，支払いの署名チェーンとブロックの署名チェーンを創ることもできます．

3. 特許情報

本稿は当社の特許明細より引用，編集した記述を用いて執筆されています．特許番号を含む，詳細情報の開示は，NDAに基づき，具体的な協議の過程で開示します．

4. 本リリースに関するお問合せ

METEORA SYSTEM Co., Ltd

https://www.meteora-system.com

