

【報道関係者各位】

AI 攻撃・ランサムウェア攻撃・サーバー攻撃・フィッシング詐欺の無力化につながる

可能性を追求する次世代革新型セキュリティ理論「無数鍵多重時変成立点理論」

「株式会社 Kトラスト」が「越智今治農業協同組合(JA おちいまばり)」と

ライセンス事業推進に関する業務提携

「無数鍵多重時変成立点理論」の普及と社会実装を推進

クラウド・ミュトスの攻撃

最強AI攻撃 vs 次世代究極防衛

クラウド・ミュトスとは？
超高性能AIによる自己進化型攻撃システム

- 自己学習・自己進化
- 全攻撃手法の自動生成
- 人間を超える分析力
- リアルタイム最適化
- 防御の穴を自動発見
- 執続・継続・遠隔攻撃

攻撃の6大能力 (理論最大)

- フィッシング成功率: 極めて高い
- 行動: 人間の完全模倣
- 脆弱性探索の自動化
- システム構造の完全解析
- 攻撃経路の最適化
- 防御資源の動的誘惑

攻撃の流れ (クラウド・ミュトス)

- 偵察・情報収集
- 侵入準備
- 侵入実行
- 内部探索・横断
- 目的達成

攻撃の強み (従来のセキュリティに対して)

- 学習速度: 膨大な情報を瞬時に学習し、最適化を繰り返す
- 適応能力: 防御の変化にリアルタイムで適応
- 網羅性: すべての攻撃手法を網羅し、盲点も狙う
- 持続性: 24時間365日、断続的に攻撃を継続
- 人間超越: 人間の成長速度を超越

攻撃の弱点 (構造の外のみが攻撃対象)

- 人間の心理的弱さ: 管理者の判断ミス、社会工学的攻撃
- 実装ミス・開封: 脆弱API、設定ミス、テスト脆弱性の存在
- 外部依存・供給網: クラウド・SaaS、第三者サービス
- 物理的・環境的脆弱性: 災害、停電など

被害シミュレーション (理論値の一例)

- 攻撃成功率 (侵入まで): 20%
- 横断成功率: 60%
- 被害化成功率: 30%
- 最終被害確率: 約6%

VS

無数鍵多重時変成立点理論

— 侵入されても成立しない世界 —

無数鍵多重時変成立点理論とは？
サーバーに到達するまでの過程を、3段階の動く壁で全段階も設計

- 無数の鍵が毎秒生成・変化
- 成立点が瞬間的 (時変)
- 3段階の多重チェック構造
- AIが常時監視・判断・制御
- 全体監視AIが全レーンを統合
- 侵入されても成立できない構造

3段階の動く壁 (多重成立点)

第1段階 (第1成立点)

- 第1認証API (多要素認証)
- 第1AIチェックAPI (行動・パターン)
- 第1AI監視API (異常検知)

第2段階 (第2成立点)

- 第2認証API (多要素認証)
- 第2AIチェックAPI (行動・パターン)
- 第2AI監視API (異常検知)

第3段階 (第3成立点)

- 第3認証API (多要素認証)
- 第3AIチェックAPI (行動・パターン)
- 第3AI監視API (異常検知)

全体監視AI (グローバル監視層)

- 全レーンの整合性監視
- 予備検出
- リスク相関分析
- 異常パターン検出
- 攻撃検定
- リアルタイム対応

連携・制御エンジン

- 各レーン制御
- 成立点制御
- AIモデル制御
- 自動診断制御
- アラート発行

異常時の即時対応

- 通信遮断
- セッション切断
- 書き換え
- アクセス拒否
- 管理者通知
- 証拠ログ保全

最終サーバー (到達時も継続監視・整合性チェックを実行)

攻撃 vs 防御 比較

クラウド・ミュトスの攻撃	VS	無数鍵多重時変成立点理論
正解を見つけて突破可能 (確率が高い)	突破方法	正解が存在しない (毎秒変化)
可能	突破の可否	極めて困難 (確率が極小)
突破後の検知が中心	検知	不可 (各レーンで再成立必須)
10%~30%以上	被害確率	0.001%~0.05%程度

被害シミュレーション (理論値の一例)

- 侵入突破率 (第1レーン): 1%
- 第2レーン突破率: 0.5%
- 第3レーン突破率: 0.2%
- 全体監視突破率: 0.5%
- 被害化成功率: 50%
- 最終被害確率: 約0.0025%

結論: 侵入されても、成立できない構造が勝つ

AIがどれだけ進化しても、構造が変わり続ける限り、攻撃は成立しない

※高精度、精密、緻密、逆算、AIシミュレーション生成画像

株式会社ポイント機構の竹内祐樹(以下、「竹内祐樹」)が発明した「無数鍵多重時変成立点理論」や様々な知的財産権を社会課題の改善や解決の為、「株式会社Kトラスト(以下「Kトラスト」):代表取締役 平川智子/代表取締役 平川和典」が「越智今治農業協同組合(JA おちいまばり):代表理事理事長 渡部浩忠/担当 芥川和豊」と、竹内祐樹が推進する次世代サイバーセキュリティ理論「無数鍵多重時変成立点理論」のライセンス事業推進に関する業務提携を締結いたしました。

本業務提携により、両者は「無数鍵多重時変成立点理論」の普及および社会実装を推進するとともに、AI攻撃、ランサムウェア攻撃、サーバー攻撃、フィッシング詐欺、情報漏えい起因する二次被害・三次被害など、現代社会が直面する様々なサイバーセキュリティ上の課題に対し、その改善および解決に貢献する取り組みを進めてまいります。また、企業、自治体、農業関連団体、金融機関、医療機関、教育機関など幅広い分野へのライセンス事業推進を通じて、地域社会および日本全体のサイバー防御力向上に寄与し、安全・安心なデジタル社会の実現を目指してまいります。



背景

近年、AI 技術の飛躍的な進化に伴い、サイバー攻撃はこれまでにない速度で高度化・自動化しています。

AI を活用した自動攻撃、ランサムウェア攻撃、不正アクセス、マルウェア攻撃、標的型攻撃、フィッシング詐欺などの被害は世界中で拡大しており、多くの企業、自治体、金融機関、医療機関、教育機関が深刻な脅威に直面しています。

国際的なサイバーセキュリティ分野では、固定された境界や入口だけに依存する防御から、継続的な信頼確認や動的な防御の重要性が指摘されています。

また実際のサイバー攻撃では、脆弱性悪用だけではなく、・認証情報窃取/・権限昇格/・横移動/・内部拡散などが組み合わされることで被害が拡大することが知られています。

Kトラストが考える現代サイバー攻撃の本質的課題

Kトラストは、現代のサイバー攻撃における最大級の課題の一つが、「固定された攻撃成立点」にあると考えています。

従来のシステムでは、・固定 ID/・固定パスワード/・固定暗号鍵/・固定 API/・固定管理者権限/・固定セッション/・固定通信経路などが長期間維持される場合があります。

攻撃者はこれらの固定された対象を繰り返し研究し、分析し、AI や自動化ツールを利用して反復攻撃を実施することが可能です。また、脆弱性対策は極めて重要である一方、脆弱性を減らしても、固定された攻撃対象が残る限り、・反復攻撃/・一点集中攻撃/・認証情報窃取/・権限昇格/・ランサムウェアやウイルスの横展開などの脅威は残り続けます。

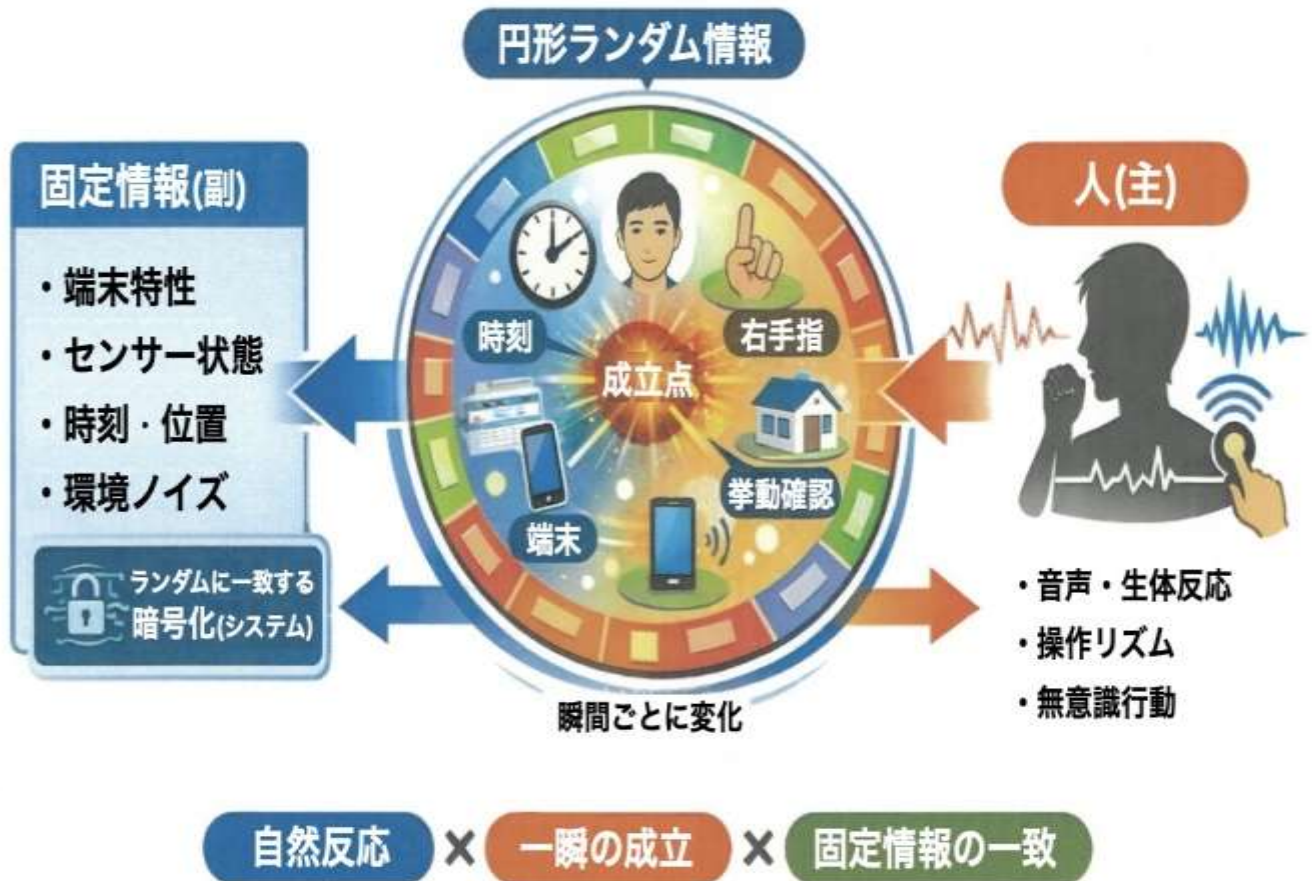
さらに、多くのシステムでは、「アクセス前の防御」には多くの対策が存在する一方、「アクセス後の継続的な成立確認」「アクセス後の異常行動監視」「アクセス後の権限昇格監視」については課題が残る場合があります。

Kトラストは、現代のサイバー攻撃において、「侵入されること」そのもの以上に、「侵入後も成立し続けること」が大きな課題であると考えています。

攻撃者は侵入後に固定された ID、固定された権限、固定された通信経路、固定された API などを利用しながら、・権限昇格/・内部横展開/・情報窃取/・ランサムウェア感染拡大/・顧客情報流出/・フィッシング詐欺のための情報収集などを行う可能性があります。そのため、本理論では、「アクセスできたか」だけではなく、「アクセス後も継続的に成立しているか」を重要視しています。

継続的な監視、継続的な成立確認、継続的な信頼判定を行うことにより、侵入後の被害拡大を抑制する新たな防御アプローチを目指しています。

無数鍵多重時変成立点理論



※AI 生成画像

情報漏えいが生み出す二次被害・三次被害

現代のサイバー攻撃による被害は、システム停止やデータ暗号化だけに留まりません。

ランサムウェア攻撃や不正アクセスにより流出した情報は、・フィッシング詐欺/・なりすまし/・アカウント乗っ取り/・不正送金/・標的型攻撃などの二次被害・三次被害へ発展する可能性があります。

流出した氏名、メールアドレス、電話番号、所属情報、取引情報などは、より精巧な攻撃の材料として悪用される場合があります。その結果、被害は企業だけでなく、・顧客/・組合員/・取引先/・関係企業/・地域住民へと拡大する可能性があります。

情報流出は、未来のフィッシング攻撃の弾薬供給

日本では年間3,000万人規模の情報流出 → フィッシング詐欺攻撃が急増!

2025年 上場企業公表ベース

約**3,063**万人分の
情報が漏えい

日本人口の約4人に1人規模!



⚠️ 情報流出の本当の危険は、
“次の攻撃の武器になる”
ことです。



現代型サイバー犯罪の流れ



特に危険なのは「本物情報一致」!



年間3,000万人規模の意味



AI時代でさらに危険化



「流出情報 × AI」で、フィッシング攻撃が極端に強化!

現在の本質



無数鍵多重時変成立点理論セキュリティ (強化の方向性)

- 1 鍵固定を減らす (無数鍵・時変)**
鍵が毎回変化。時間・状態・条件で動的に変わるため、盗んでも使えない。
- 2 時変成立 (短命化)**
成立しても数秒〜数十秒で消滅。使い回し・再利用を不可能にする。
- 3 継続成立が必要**
端末・行動・通信・時間などを常時監視。途中で違えば即失効。
- 4 多重成立点 (多層構造)**
L1~L5の多層構造で、1つ突破しても最終到達できない。
- 5 副作用チェック (AI監視)**
操作・通信・挙動の違和感をAIが検知。不正を早期にブロック。
- 6 成立後消滅 (セッション消滅)**
成立後は即消滅。長時間のセッション乗っ取りを防止。



「情報を知っていても成立しない」仕組みへ



⚠️ **重要な本質**
情報流出は、単なる漏えい事件ではない。
実際は「未来のフィッシング攻撃の弾薬供給」になっている。

だからこそ
“成立し続けることを不可能化するセキュリティ”が
これからの時代の必須防御です。

※高精度、精密、緻密、逆算、AI シミュレーション生成画像

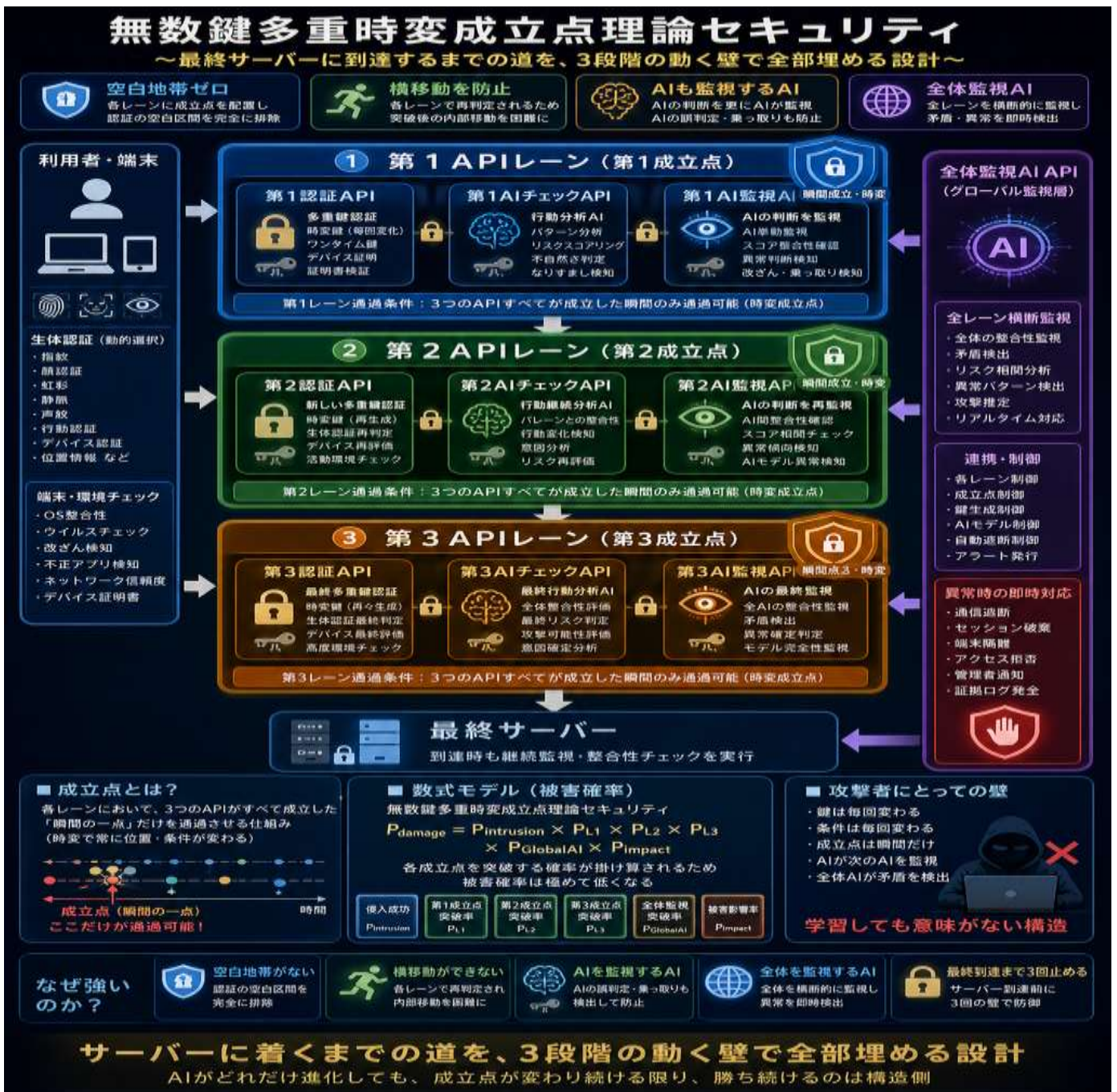
※サイバーセキュリティ・情報漏洩ニュース <https://share.google/xnP7LI0H2CC2tAVgI>

無数鍵多重時変成立点理論とは

無数鍵多重時変成立点理論は、「固定された成立条件を前提としない」という新たな考え方に基づく次世代セキュリティ理論です。

本理論では、・無数鍵化/・多重化/・時変化/・短時間成立/・一回限り成立/・多層成立点制御/・AI監視/・継続的信頼判定を組み合わせることで、固定された攻撃成立点への依存低減を目指します。

本理論の基本思想は、・固定しない/・時変化する/・短命化する/・分散する/・成立後も継続監視する/・異常時には成立を失効させるという方向性にあります。



本理論が目指すもの

無数鍵多重時変成立点理論は、・AI 攻撃/・ランサムウェア攻撃/・サーバー攻撃/・フィッシング詐欺/・認証情報窃取/・不正アクセス/・マルウェア感染/・権限昇格攻撃/・横展開攻撃などの成立を極めて困難化し、それらの無力化につながる可能性を追求する次世代革新型セキュリティ理論です。

従来のように、「侵入を防ぐ」だけではなく、「侵入後も成立しにくい」「攻撃条件そのものを成立しにくくする」「被害の拡大を抑える」という新たな防御アプローチを目指しています。

業務提携の目的

1. ライセンス事業推進→無数鍵多重時変成立点理論のライセンス事業を推進し、企業や団体への普及を図ります。
2. 社会実装推進→実証事業(PoC)の推進を通じて実用化を目指し、社会実装を推進します。
3. 地域社会への貢献→地域社会におけるサイバー防御力向上に取り組めます。
4. 全国展開→企業、自治体、農業団体、金融機関、医療機関、教育機関などへ推進します。

期待される展開→本理論の普及により、・企業情報保護/・顧客情報保護/・組合員情報保護/・地域インフラ保護/・金融情報保護/・重要システム保護/・情報漏えいリスク低減/・情報漏えい後の二次被害抑制/・フィッシング詐欺被害抑制/・なりすまし被害抑制/・ランサムウェア被害拡大抑制/・暗証番号や固定認証情報への依存低減/・AI 時代に対応した新たな本人認証モデルの実現/・AI 時代に対応した新たな防御モデル構築などへの貢献が期待されます。

コメント

株式会社 K トラスト→「AI 時代のサイバー攻撃は、人間による攻撃から AI による自動攻撃へと変化しています。私たちは、固定された成立条件に依存しない新たな防御概念として、無数鍵多重時変成立点理論の普及と社会実装を推進してまいります。今回の業務提携を通じて、地域社会、日本、そして世界のサイバーセキュリティ向上に貢献できるよう取り組んでまいります。」

越智今治農業協同組合 (JA おちいまばり)→「地域社会を支える組織として、情報資産保護の重要性はますます高まっています。今回の業務提携を通じて、新たなサイバーセキュリティの可能性を検証し、地域社会の安全・安心につながる取り組みを推進するとともに、将来的には暗証番号や固定認証情報への依存を低減する未来の実現にも貢献してまいりたいと思います。」

竹内祐樹→「現代、クラウド・ミュトスの出現により、脆弱性について騒がれていますが、本当の脅威は脆弱性よりも AI 攻撃やウイルス攻撃を含め、固定されているセキュリティが存在する事です。固定されているセキュリティは一点集中攻撃が可能であり、攻撃した箇所を認識でき、分析、攻撃手法の変更が可能です。そういった脅威を無くすべく、守れるセキュリティ、安心できるセキュリティの実現を通して社会課題の改善や解決をしてまいります。」

番組出演：<https://youtu.be/W64x53pDf5s?si=ZRzFYfhOI6VGB73S>

YouTube 解説動画など：

<https://youtube.com/channel/UCaw3vYDfrE6nQHMM0RjhQbA?si=YWn4MhIJI59BT2su>

note 一覧：https://note.com/lucky_quokka8752

今後の展望→株式会社 Kトラストが越智今治農業協同組合 (JA おちいまばり) と、無数鍵多重時変成立点理論のライセンス事業推進を通じて、AI 攻撃・ランサムウェア攻撃・サーバー攻撃・フィッシング詐欺などの無力化につながる可能性を追求し、次世代サイバーセキュリティの社会実装と社会課題の改善・解決に取り組んでまいります。

【本件に関するお問い合わせ先】



株式会社 Kトラスト

ライセンス事業推進本部

担当: 平川(ひらかわ)/竹内(たけうち)

TEL: 050-1720-5724

E-mail: k-trust@verda.co.jp

所在地: 愛知県名古屋市守山区下志段味 1 丁目 3313 番地

URL: <http://www.ktrust.info>



越智今治農業協同組合(JA おちいまばり)

担当: 企画管理課 芥川(あくたがわ)

TEL: 0898-34-1802

E-mail: kanri@ja-ochiima.or.jp

所在地: 愛媛県今治市北宝来町 1-1-5

URL: <https://www.ja-ochiima.or.jp>