無数鍵多重時変成立点理論

無数鍵多重時変成立点理論による次世代セキュリティ

第 3 世代セキュリティ

ゼロトラスト次世代

99.7% 防御率

ランサムウェア対策

特許取得済み技術

バイタル×音特許

竹内 祐樹 ・株式会社Kトラスト

守る対象が違う ― セキュリティの３世代

第1世代

従来セキュリティ

守る対象 ▶ パスワードを守る

- 社外=危険 / 社内=信頼
- FW・境界防御モデル
- ログイン後は自由
- パスワード漏洩で即侵入

第2世代

ゼロトラスト

守る対象 ▶ 認証を守る

- 社内外すべて不信
- 常時認証・端末認証
- マイクロセグメント
- 侵入は前提の防御

第3世代

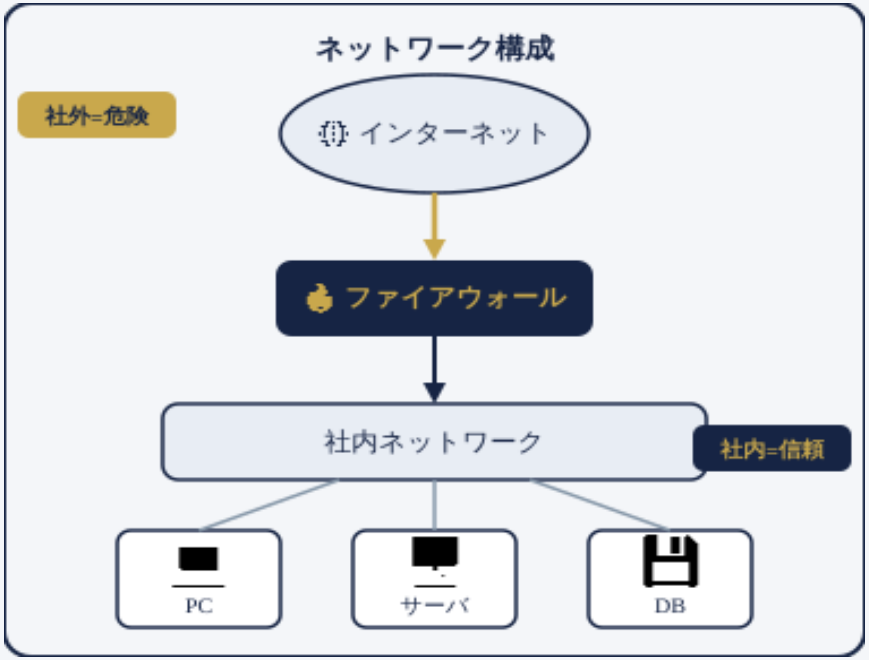
成立点セキュリティ

守る対象 ▶ 成立状態を守る

- 無数鍵多重時変理論
- 成立点トークン生成
- 空間消滅 → 通路が消える
- 99.7%ランサムウェア防御

守る対象が違う ―― ゼロトラスト → 成立点確認

従来セキュリティの構造と弱点



ログイン成功 = 内部自由 ⇨ これがランサムウェア被害の根本原因

ゼロトラストの思想と限界

「誰も信頼しない」思想

社内外すべてを不信とし、端末・ユーザー・ネットワークを多層で認証する。

常時認証・継続監視

一度のログインで終わらない。アクセスのたびに認証を繰り返し監視を続ける。

侵入は「前提」の限界

認証突破後の横展開は依然起きる。攻撃者に経路が見えている点が根本的限界。

ゼロトラスト vs 従来　比較

	従来	ゼロトラスト
認証	ID+PW	常時多層認証
監視	境界内は自由	継続的監視
侵入後	横展開あり	横展開あり
守る対象	パスワード	認証

無数鍵多重時変成立点理論 ― 仕組みの核心

処理フロー

① 条件判定

アクセス条件を
多角的に判定

② 副作用チェック

ウイルス・異常
状態を確認

③ 暗号鍵抽選

無数の鍵から
毎回ランダム選択

④ 成立点生成

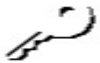
一瞬だけ許可
再利用不可

⑤ 空間消滅

通路が消える
退路ゼロ

鍵の仕組みの違い

従来の鍵



1つのパスワード・固定
繰り返し使用可能

総当たり攻撃が有効

無数鍵多重時変

無数の鍵から毎回抽選
時変 = 二度と同じ鍵なし

総当たり攻撃を根本無効化

特許認証技術

バイタル・音声特許

音声特許
声紋・音響認証

バイタル認証
生体情報で本人確認

見えない通路のセキュリティ ― 攻撃者視点

従来

攻撃者は何度でも試せる。通路は常に開いている。

ゼロトラスト

認証で遅らせるが、侵入後の経路は残存する。

成立点セキュリティ

通路自体が消える。攻撃者は入っても出口がない。

ランサムウェア対策の優位性

防御率比較（推定値）

従来セキュリティ	30%
ゼロトラスト	65%
無数鍵多重時変成立点理論	99.7%

成立点ごとに鍵が変化・空間消滅のため
暗号化成立条件が揃いにくい構造

まとめ ― 成立点セキュリティの本質

従来:「正解を守る仕組み」　　**成立点**:「成立する瞬間だけ作る仕組み」

守る対象が根本的に違う

パスワード → 認証 → 成立状態。対象が変わることで防御概念が根本から変化する。

無数鍵多重時変理論

時変鍵と成立点トークンにより、同一パターンの攻撃を根本から無効化する。

空間消滅 = 通路が消える

操作終了後に通路が消滅。攻撃者は侵入しても出口を見つけることができない。

バイタルセキュリティ・音特許技術

生体認証と音の特許を組み合わせた固有の認証基盤。特許取得済みの独自技術。