

サイバーセキュリティを活用した人工知能

(Saibāsekyuriti o katsuyō shita jinkō chino)

説明: テクノロジーは急速に成長しており、世界は新しいトレンドと機会によって形作られています。人工知能、モノのインターネット、クラウドコンピューティング、拡張現実など、さまざまなテクノロジーでエキサイティングな開発が行われています。これらの新しいテクノロジーには、それぞれ利点と課題があります。では、サイバーセキュリティによってAIがどのように活用されているかを見てみましょう。これらの新しいテクノロジーには、それぞれ利点と課題があります。人工知能がサイバーセキュリティによってどのように強化されているかを見てみましょう。

Setsume: Tekunorojī wa kyūsoku ni seichō shite ori, sekai wa atarashī torendo to kikai ni yotte katachidzukura rete imasu. Jinkō chinō, mono no intānetto, kuraudokonpyūtingu, kakuchō genjitsu nado, samazamana tekunorojī de ekisaitinguna kaihatu ga okonawa rete imasu. Korera no atarashī tekunorojī ni wa, sorezore riten to kadai ga arimasu. Jinkō chinō ga saibāsekyuriti ni yotte dono yō ni kyōka sa rete iru ka o mite mimashou.

サイバーセキュリティ

サイバーセキュリティは、望ましくない攻撃や不正アクセスを保護、防止、検出するためのプロセスです。サイバーセキュリティは、組織がサイバー資産を保護するために使用する人、ポリシー、プロセス、テクノロジーの組み合わせです。サイバーセキュリティは、ビジネス定義のレベルに最適化され、リソース要件と使いやすさ/管理性、およびリスク相殺の程度とのバランスが取れています(ガートナー用語集)。テクノロジーへの依存度と利用度が高まるにつれ、サイバー脅威や攻撃の影響も大きくなります。サイバーセキュリティ対策は、フィッシング、サービス拒否、マルウェア攻撃などの脅威から保護 et. al。それは、社内外のあらゆるビジネススペースで、あるいは個人的なものから生まれます。

Saibāsekyuriti

Saibāsekyuriti wa, nozomashikunai kōgeki ya fusei akusesu o hogo, bōshi, kenshutsu suru tame no purosudesu. Saibāsekyuriti wa, soshiki ga saibā shisan o hogo suru tame ni shiyō suru hito, porishī, purosusu, tekunorojī no kumiawasedesu. Saibāsekyuriti wa, bijinesu teigi no reberu ni saiteki-ka sa re, risōsu yōken to tsukaiyasusa/ kanri-sei, oyobi risuku sōsai no teido to no baransu ga torete imasu (gātonā yōgo-shū). Saibāsekyuriti taisaku wa, fisshingu, sābisu kyohi, maruu~ea kōgeki nado no kyōi kara hogo et. Al. Sore wa, shanaigai no arayuru bijinesusupēsu de, aruiwa kojīn-tekina mono kara umaremasu.

さらに、デジタルマガジンのレポート(2023年)によると、サイバー脅威には次のようなさまざまなカテゴリがあります:

ランサムウェアの脅威: これは、被害者のファイルを暗号化し、復号化キーの支払いを要求するように設計された悪意のあるソフトウェアの一種です。

サプライチェーンの脅威: 組織のコンピュータシステムやデータにアクセスできるサプライヤーやベンダーのネットワークやシステムを標的にしています。これらの脅威は、データの損失、金銭的損失、風評被害につながる可能性があります。

クラウドの脅威: インターネットにアクセスできるサードパーティのサーバー上のデータやアプリケーションの保存、処理、アクセスで構成されるクラウドコンピューティング環境を標的としています。

モバイルの脅威: 機密データを保存し、個人的および専門的な目的で使用されるモバイルデバイスを標的にします。

テクノロジーが進化し、私たちの日常生活に浸透するにつれて、サイバー攻撃の可能性も高まります。その後、技術専門家がサイバー攻撃から身を守る方法を考案しました。これらのサイバーセキュリティソリューションは、ネットワークセキュリティ、データセキュリティ、アプリケーションセキュリティ、クラウドセキュリティ、アクセス管理などの機能に従って分類できます。これらのソリューションは、機密情報を保護すると同時に、データの機密性を維持します。

Sarani, dejitaru magajin no repōto (2023-nen) ni yoru to, saibā kyōi ni wa tsugi no yōna samazamana kategori ga arimasu :

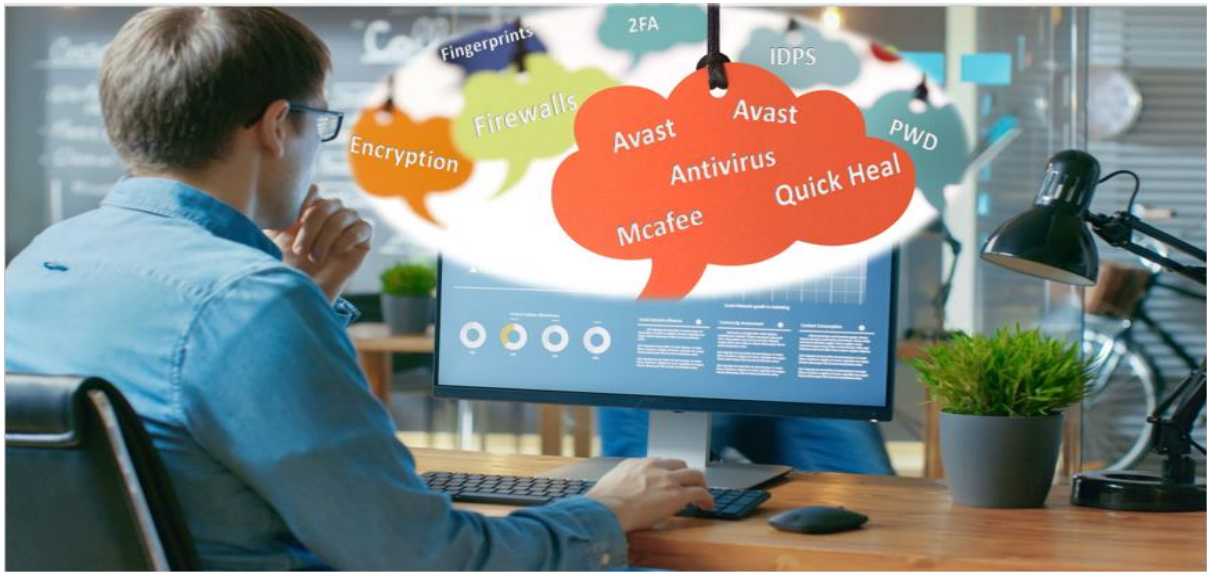
Ransamuu~ea no kyōi: Kore wa, higaisha no fairu o angō-ka shi, fukugō-ka kī no shiharai o yōkyū suru yō ni sekkei sa reta akui no aru sofutō~ea no issitudesu.

Sapuraichēn no kyōi: Soshiki no konpyūtaisutemu ya dēta ni akusesu dekiru sapuraiyā ya bendā no nettowāku ya shisutemu o hyōteki ni shite imasu. Korera no kyōi wa, dēta no sonshitsu, kinsen-teki sonshitsu, fūhyō higai ni tsunagaru kanōsei ga arimasu.

Kura udo no kyōi: Intānetto ni akusesu dekiru sādopāti no sābā-jō no dēta ya apurikēshon no hozon, shori, akusesu de kōsei sa reru kuraudokonpyūtingu kankyō o hyōteki to shite imasu.

Mobairu no kyōi: Kimitsu dēta o hozon shi, kojīn-teki oyobi senmon-tekina mokuteki de shiyō sa reru mobairu debaisu o hyōteki ni shimasu.

Tekunorojī ga shinka shi, watashitachi no nichijō seikatsu ni shintō suru ni tsurete, saibā kōgeki no kanōsei mo takamarimasu. Sonogo, gijutsu senmonka ga saibā kōgeki kara miwomamoru hōhō o kōan shimashita. Korera no saibāsekyuritorisoryūshon wa, nettowākusekyuriti, dētasekyuriti, apurikēshonsekyuriti, kuraudosekyuriti, akusesu kanri nado no kinō ni shitagatte bunrui dekimasu. Korera no soryūshon wa, kimitsu jōhō o hogo suruto dōjini, dēta no kimitsu-sei o iji shimasu.



人工知能

人工知能はパスワードであり、ビジネス、研究、教育のいずれにおいても多くのノイズを生み出しています。国立標準技術研究所の定義によると、人工知能はコンピューターサイエンスの一分野であり、推論、学習、自己改善など、一般的に人間の知能に関連する活動に従事できるデータ処理システムの作成に焦点を。要約すると、知覚ベースの意思決定や自然言語処理など、通常は人間の知性を必要とするタスクを実行するシステムです。例を挙げると、メタ（フェイスブック）に画像をアップロードすると、システムが顔を検出し、画像内の個人を自動的にタグ付けします。このシステムは、機械学習アルゴリズムを使用して利用可能なデータをスキャンし、顔を認識し、パターンを見つけて、顔と人を正確に一致させます。メタ（フェイスブック）は、ディープラーニングアルゴリズムと連携する人工知能駆動の顔認識技術を使用して、人々の顔パターンを認識できるようにします。

Jinkō chino

Jinkō chinō wa bazuwādodeari, bijinesu, kenkyū, kyōiku no izure ni oite mo ōku no noizu o umidashite imasu. Kokuritsu hyōjun gijutsu kenkyūjo no teigi ni yoru to, jinkō chinō wa konpyūtāsaiensu no ichibun'yadeari, suiron, gakushū, jiko kaizen nado, ippantekini ningen no chinō ni kanren suru katsudō ni jūji dekiru dēta shori shisutemu no sakusei ni shōten o. Yōyaku suru to, chikaku bēsu no ishi kettei ya shizen gengo shori nado, tsūjō wa ningen no chisei o hitsuyō to suru tasuku o jikkō suru shisutemudesu. Reiwoageru to, meta (feisu bukku) ni gazō o appurōdo suru to, shisutemu ga kao o kenshutsu shi, gazō-nai no kojīn o jidōtekini tagudzuke shimasu. Kono shisutemu wa, kikai gakushū arugorizumu o shiyō shite riyō kanōna dēta o sukyan shi,-gao o ninshiki shi, patān o mitsukete,-gao to hito o seikaku ni itchi sa semasu. Meta (feisu bukku) wa, dīpurāninguarugorizumu to renkei suru jinkō chinō kudō no kao ninshiki gijutsu o shiyō shite, hitobito no kao patān o ninshiki dekiru yō ni shimasu.



顔のパターンとタグを識別するアルゴリズム

人工知能はサイバーセキュリティの分野にどのように貢献していますか？

簡単に言うと、人工知能はサイバーセキュリティを実現する要素と言えます。人工知能は、サイバー攻撃を検知、防止、対応し、サイバーセキュリティソリューションの有効性を高める可能性を秘めています。例えば：

- 人工知能アルゴリズムは、データセットを分析し、潜在的なサイバー攻撃を示す傾向を見つけるのに役立ちます。
- また、悪意のあるソフトウェアウイルスの動作パターンを分析し、リスクを評価します。
- 人工知能は、認証手順を改善する可能性を秘めています。
- 人工知能は、起こりうる攻撃への対応を自動化し、対応時間と被害を軽減すると同時に、将来の攻撃を予測することができます。

Jinkō chinō wa saibāsekyuriti no bun'ya ni dono yō ni kōken shite imasu ka?

Kantan ni iu to, jinkō chinō wa saibāsekyuriti o jitsugen suru yōsodearu to imasu. Jinkō chinō wa, saibā kōgeki o kenchi, bōshi, taiō shi, saibāsekyuritisoriyūshon no yūkōsei o takameru kanōsei o himete imasu. Tatoeba:

- Jinkō chinō arugorizumu wa, dētasetto o bunseki shi, senzai-tekina saibā kōgeki o shimesu keikō o mitsukeru no ni yakudachimasu.
- Mata, akui no aru sofutō~ea uirusu no dōsa patān o bunseki shi, risuku o hyōka shimasu.
- Jinkō chinō wa, ninshō tejun o kaizen suru kanōsei o himete imasu.

- Jinkō chinō wa, okori uru kōgeki e no taiō o jidō-ka shi, taiō jikan to higai o keigen suruto dōjini, shōrai no kōgeki o yosoku suru koto ga dekimasu.

一方、ハッカーやサイバー犯罪者も人工知能を使用して攻撃の影響を高めます。サイバー犯罪者は、人工知能を利用した手法を使用して、検出を回避し、コンピューターシステムやネットワークに侵入するための複雑な手法を作成します。

Ippō, hakkā ya saibā hanzai-sha mo jinkō chinō o shiyō shite kōgeki no eikyō o takamemasu. Saibā hanzai-sha wa, jinkō chinō o riyō shita shuhō o shiyō shite, kenshutsu o kaihi shi, konpyūtāshisutemu ya nettowāku ni shin'nyū suru tame no fukuzatsuna shuhō o sakusei shimasu.

一方、サイバー犯罪は、テクノロジーの使用が進むにつれて増加の一途をたどっています。セキュリティ運用アナリストは、潜在的な攻撃を検出するために人工知能に焦点を当てています。さらに、このような攻撃への対応時間を大幅に短縮する独自の特性を組み込むためのカスタマイズにも力を入れています。今のところ、人工知能がサイバーセキュリティソリューションをサポートしていることを理解しています。サイバーセキュリティが人工知能よりも優れているかどうかにかぎらず光を当ててみましょう。

Ippō, saibā hanzai wa, tekunorojī no shiyō ga susumu ni tsurete zōka no ichizu o tadotte imasu. Sekyuriti un'yō anarisuto wa, senzai-tekina kōgeki o kenshutsu suru tame ni jinkō chinō ni shōten o atete imasu. Sarani, kono yōna kōgeki e no taiō jikan o ōhaba ni tanshuku suru dokuji no tokusei o kumikomu tame no kasutamaizu ni mo chikara o irete imasu. Imanotokoro, jinkō chinō ga saibāsekyuritorisoryūshon o sapōto shite iru koto o rikai shite imasu. Saibāsekyuriti ga jinkō chinō yori mo sugurete iru ka dō ka ni hikari o atete mimashou.

しかし、一方では、サイバーセキュリティはシステムを保護するためのソリューションや戦略を提供し、人工知能はインテリジェントなパターンを作成して、それらのソリューションを効果的に適用してより良い結果をもたらします。セキュリティと新興技術センターは、サイバー人工知能と呼ばれるプロジェクトに取り組んでいます。このプロジェクトの目的は、人工知能を使用してサイバー操作と防止を自動化することです。

デロイトインサイト の投稿（技術動向、2022年）によると、組織は攻撃者がサイバー人工知能を使用して移動できるよりも迅速に返信できる可能性があります。また、攻撃者の次の動きを予測し、即座に対応できるようにするのも役立ちます。

Shikashi, ippōde wa, saibāsekyuriti wa shisutemu o hogo suru tame no soryūshon ya senryaku o teikyō shi, jinkō chinō wa interijentona patān o sakusei shite, sorera no soryūshon o kōka-teki ni tekiyō shite yoriyoi kekka o motarashimasu. Sekyuriti to shinkō gijutsu sentā wa, saibā jinkō chinō to yoba reru purojekuto ni torikunde imasu. Kono purojekuto no mokuteki wa, jinkō chinō o shiyō shite saibā sōsa to bōshi o jidō-ka suru kotodesu. Deroitoinisaito no tōkō (gijutsu dōkō, 2022-nen) ni yoru to, soshiki wa kōgeki-sha ga saibā jinkō chinō o shiyō shite idō dekuru

yorī mo jinsoku ni henshin dekiru kanōsei ga arimasu. Mata, kōgeki-sha no tsugi no ugoki o yosoku shi, sokuza ni taiō dekiru yō ni surunoni mo yakudachimasu.

サイバー人工知能のツールとテクノロジーは、まだ導入の初期段階にあります。さらに、人工知能は戦力増強剤として機能し、時間のかかるタスクを自動化し、封じ込めと対応を迅速化するために技術専門家を支援することもできると述べています。

Saibā jinkō chinō no tsūru to tekunorojī wa, mada dōnyū no shoki dankai ni arimasu. Sarani, jinkō chinō wa senryoku zōkyō-zai to shite kinō shi, jikan no kakaru tasuku o jidō-ka shi, fūjikome to taiō o jinsoku-ka suru tame ni gijutsu senmonka o shien suru koto mo dekiru to nobete imasu.

サイバーセキュリティの主な目的は、システム、ネットワーク、データなどを保護することであり、人工知能を使用してサイバーセキュリティ防御を強化できます。したがって、サイバーセキュリティと人工知能はどちらも、進化するサイバー脅威を管理するために重要です。

Saibāsekyuriti no omona mokuteki wa, shisutemu, nettowāku, dēta nado o hogo suru kotodeari, jinkō chinō o shiyō shite saibāsekyuriti bōgyo o kyōka dekimasu. Shitagatte, saibāsekyuriti to jinkō chinō wa dochira mo, shinka suru saibā kyōi o kanri suru tame ni jūyōdesu.

参照

CNBCビジネス。(2022年9月13日)。人工知能はサイバーセキュリティにおいてより大きな役割を果たしていますが、最も恩恵を受けるのは悪者かもしれません。 [AI has bigger role in cybersecurity, but hackers may benefit the most \(cnbc.com\)](https://www.cnbc.com)

デロイトインサイト。(2022)。サイバー人工知能:真の防衛。 [The future of cybersecurity and AI | Deloitte Insights](https://www.deloitte.com)

ガートナー用語集, [Definition of Cybersecurity - Gartner Information Technology Glossary](https://www.gartner.com)

NIST 定義 用語集、情報技術研究所、コンピュータセキュリティリソースセンター、情報技術研究所, [CSRC Topics - artificial intelligence | CSRC \(nist.gov\)](https://www.csrc.nist.gov)

PWC 出版。(2021)。パワーと保護のバランスをとる:人工知能におけるサイバーセキュリティとサイバーセキュリティにおける人工知能。 [pwc-balancing-power-protection-ai-cybersecurity.pdf](https://www.pwc.com)

2023 年の脅威予測。(2023)。 [The top 10 cybersecurity threats for 2023 - Atos](https://www.atos.com)