Toward
Always evolving forward

Seminar on security defense techniques

知らぬ間に狙われている！？
社会人のためのセキュリティ防衛術

世の中に起きているセキュリティ問題から考えよう

2025年11月10日 管理部

はじめに｜本日の予定

はじめに	セミナーの概要説明		
Session 1	あなたも“もう狙われている”	Session 6	まとめ：意外と知らない“落とし穴”
Session 2	1日あたりの攻撃件数	Session 7	従業員が守るべき5つの基本
Session 3	実例①～③	Session 8	会社としての対策
Session 4	問題の本質：最大の弱点は“人”	Session 9	チェックリスト（今日からできる）
Session 5	セキュリティクイズ	まとめ	便利さと安全はセット

Toward
Always evolving forward

今、世の中で起きている事例を知って
普段の生活や業務の中で気を付けるべきことを 改めて振り返る

本セミナーで学ぶこと

・実際に起きている最新のサイバー攻撃と、個人・企業が直面する現実的なリスク

知る・気づくこと

・技術よりも「人の行動」が狙われているという事実と、自分の業務のどこに危険が潜むか？

とるべきアクション

・今日から実践できるセキュリティ習慣を身につけ、会社と自分の情報を守る

Toward
Always evolving forward

Session 1

あなたも“もう狙われている”

Toward
Always evolving forward

サイバー攻撃は「企業」から「個人」へ　　の時代

金銭的利益・機密情報の入手・システムへの侵入ルートの確保

攻撃者は強固なシステムを直接破るより、Slack・GitHub・ChatGPT
・Google Driveなど、 私たちが日常的に使うツールやクラウドサービス
に潜む“人の油断”を狙う

企業のセキュリティシステムは年々強化されているため、
直接システムを破るよりも、
「人の油断」や「小さな不注意」から侵入する方がはるかに簡単で確実

Toward
Always evolving forward

具体的には？

- フィッシングメールでパスワードを入力させ、社内システムに侵入
- 開発者のGitHubトークンやAPIキーを盗み、サーバーやデータベースへアクセス
- ChatGPTなど外部AIサービス経由で、機密コードや顧客情報を収集
- マルウェアを仕込んだ添付ファイルを開かせ、内部ネットワークに足場を作る

etc･･･

Toward
Always evolving forward

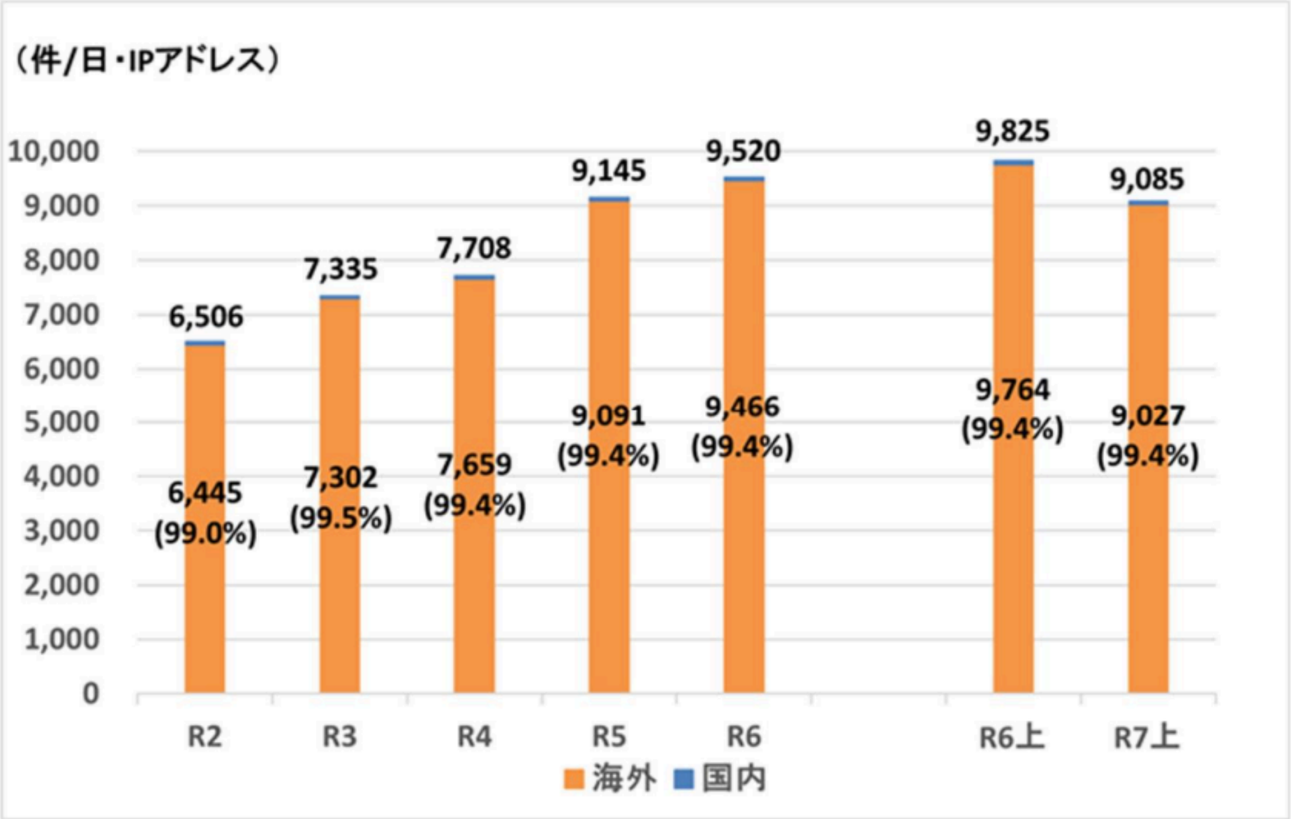
Session 2

1日あたりの攻撃件数

Session 2　1日あたりの攻撃件数

R7年上半期におけるサイバー空間における脅威の情勢等について

【図表１：警察庁が検知した不審なアクセス件数】



参照：警視庁　統計データ

日本国内の不正アクセス件数は
年間数百万件

攻撃の7割以上が
人の操作ミスを狙うもの

海外サーバーを利用してなどの攻撃が増えている

Toward
Always evolving forward

Asahi GROUP

MUJI

LOHACO by ASKUL

Session 3

最近の実例①～③

Always evolving forward

最近の実例①：Asahiグループホールディングス

2025年9月29日、同社は国内システムに障害が発生していると公表。

攻撃はランサムウェア型とされ、後にロシア拠点のハッカー集団 Qilin が犯行を主張。
約27 GB、9,300件超のファイルを窃取したと主張。

情報流出の可能性があるとして「個人情報および取引先・社員データが不正に移転された痕跡を確認」しており、調査中と発表。

財務・契約書類、従業員の個人情報、開発計画などが窃取された可能性が報じられ、被害の規模・影響が今後さらに明らかになる見込み。

Always evolving forward

最近の実例②：GitHubトークン流出事件

2022 年4 月、サードパーティの OAuth アプリ（Heroku／Travis CI）から盗まれたトークンを用い、GitHub 上の複数組織の非公開リポジトリが不正にダウンロードされた。

2025 年3 月～11 月、人気の OSS ツール SpotBugs のワークフローからトークンが盗まれ、関連 GitHub Actions を汚染する“サプライチェーン攻撃”で 200 以上のリポジトリが影響を受けた。

いずれのケースも、技術的な壁を超えるよりも「トークン／人のミス」で入口を作られた点が共通しており、**組織・個人の“アクセストークン管理”が重大なリスク**

Always evolving forward

最近の実例③：進化するフィッシングメール

本物そっくりの送信元・日本語文面（生成AI生成）

以前は、「不自然な日本語」で注意すれば気づけた違和感が
生成AIの進化により、気づきづらくなっている

社内ドメインに酷似した偽メールに注意

一文字だけ変えてある、増やしてあるなど気づきにくくなっている

⇒ 差出人／件名／URLを必ず確認

Toward
Always evolving forward

Session 4

問題の本質：最大の弱点は“人”

Always evolving forward

ファイアウォールよりもヒューマンリスクが多い

エンジニアが犯しやすい行動例

- コードに秘密情報をベタ書き
- 公開リポジトリの誤設定
- ChatGPTに顧客データを貼る
- 同じパスワードを使い回す

Toward
Always evolving forward

Session 5

セキュリティクイズ

Always evolving forward

パスワードは8文字あれば安全だ

Toward
Always evolving forward

こたえ：×

英数字・記号を組み合わせ、12文字以上推奨

生年月日、名前、第三者から推測されにくいもの

使いまわさないこと

Always evolving forward

ChatGPTに機密情報を入れても外に漏れない

Toward
Always evolving forward

こたえ：×

読み込ませてしまうと、情報は外部に漏れます。
ChatGPTから情報漏洩を防ぐには、「チャット履歴とトレーニング」をオフにし、機密情報は入力しないことが重要

Always evolving forward

VPNを使えばどんなWi-Fiでも安全だ

Toward
Always evolving forward

こたえ：×

VPNを使えば公共Wi-Fiなどの通信は暗号化されるため、多くのリスクは低減するが、すべてのWi-Fiを完全に安全にするわけではない。

Toward
Always evolving forward

Session 6

まとめ：意外と知らない“落とし穴”

Toward
Always evolving forward

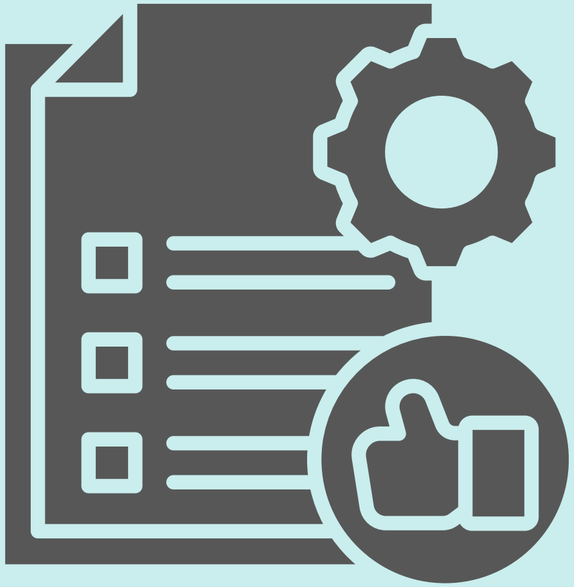
まずは「一歩引いて確認する習慣」を

- 「知っている」と「できている」は違う
- 攻撃は“油断”を狙う

操作の前に立ち止まって、少し冷静に見直す

慌てない
焦らない
ひとりでどうにかしようとしない（誰かに相談）

Toward
Always evolving forward



Session 7

従業員が守るべき5つの基本

Toward
Always evolving forward

最低限　これは気を付けて！

パスワード使い回し禁止・定期更新

機密データをAIや外部サービスに入力しない

リポジトリ権限は最小限に

不審メールは開かず報告

OS・ツールの更新を怠らない

Toward
Always evolving forward

Session 8

会社としての対策

Toward
Always evolving forward

定期脆弱性チェック

インシデント報告・訓練のルール化

セキュリティ教育の定期実施

AI利用ガイドライン整備

今後、社内でAIを活用していくにあたりガイドラインは必要

Always evolving forward

Session 9

チェックリスト（今日からできる）

Session 9　チェックリスト（今日からできる）

- ✓ パスワード管理を見直した
- ✓ 機密情報をクラウドAIに入れていない
- ✓ 不審メールは開かない
- ✓ PCに何か起きてしまったら報告する（ネットワーク切断）
- ✓ VPNを常時ONにしていない状態で業務操作をしていない
- ✓ 開発端末で個人用途のブラウザ拡張機能を入れていない

まとめ

便利さと安全はセット

まとめ

Always evolving forward

「セキュリティ＝信頼を守る力」

新しい技術を使うほど、情報管理の重要性が高まる

小さな意識が大きな防御になる

社会人のための
セキュリティ防衛術

THANK　YOU🧡