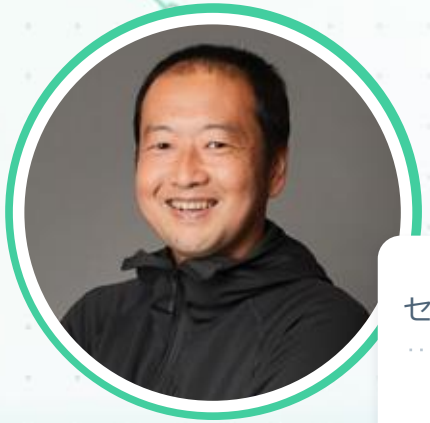
backlog by nulab × nulabpass

企業が今、意識すべきセキュリティ対策

不正アクセスの入口は“アカウント”

入口を固め、情報を集めて守る実践ステップ



株式会社ヌーラボ
セキュリティエンジニア
松山 保

2026年10月19日（月）
13:00〜14:00



株式会社ヌーラボ
プロモーション部
河野 千里

いま、不安に思っていることは？

Zoom投票 ニュースを見て、自社で「まずい」と感じていることを教えてください

A パスワードの使い回しや、
漏えいが心配

B 退職者や委託先のアカウントが、
残っていないか不安

C 情報がメールやチャット、
個人のツールに散らばっている

D 何か起きたとき、
気づけるか・追えるか自信がない

複数選択できます。そのほかの不安は、チャットでお寄せください

自己紹介



河野 千里

Chisato Kouno

株式会社ヌーラボ
プロモーション部

経歴

- 元・請負系システムエンジニア。受託開発の現場で20年以上、開発部門の責任者も担当
- 顧客課題を解決する現場で、個人のスキルより「チームの進め方」が成果を左右することを実感

現在の役割

- プロジェクト管理・チームコラボレーションをテーマにセミナーを担当
- 本日は、現場と管理部門の両方を経験した立場から進行を務めます

自己紹介



松山 保

Tamotsu Matsuyama

株式会社ヌーラボ
セキュリティエンジニア

IPA 情報セキュリティ10大脅威 選考委員

経歴

- 大学時代に学内のUNIXに触れたのがきっかけで、ITの分野に興味を持つ
- Javaプログラマとして、主にWebシステムの開発に20年ほど携わる
- 開発責任者や監査責任者などを経て、徐々にセキュリティの分野へピボット
- 2020年、ヌーラボに一人目のセキュリティエンジニアとして入社

資格・活動

- CISSP（937857）/ CISA
- 情報処理安全確保支援士（第021501号）
- 九州大学SECKUN 第1期生、講師
- IPA情報セキュリティ10大脅威 選考委員
- 九州サイバーセキュリティシンポジウム委員
- 日本シーサート協議会 地区活動委員
- みんなのセキュリティ勉強会 代表
- 一般社団法人 日本セキュリティ心理学会 理事

本日のゴールと進め方

本日のゴール

不正アクセスの「入口」と「中身」を見直し、明日から自社で動ける状態になる

そのために、本日は3つのステップでお話しします

SECTION 01

不正アクセスは、なぜ起きるのか

4つの原因と、そこに潜む問題・対策を、セキュリティエンジニアの松山と掘り下げます

→ ゴール
原因ごとの対策がわかる

SECTION 02

デモ：Backlog × Nulab Passで備える

ひとつのプロジェクトの始まりから終わりまでで、対策の実際をご覧いただきます

→ ゴール
仕組みでの備え方がわかる

SECTION 03

まとめ・ご案内

4つの対策と明日からできる一歩を振り返り、無料トライアル・個別相談会をご案内します

→ ゴール
明日からの一歩を決められる

ご質問は、Q&Aで随時受け付けています

backlog × nulabpass

SECTION 01

不正アクセスは、なぜ起きるのか

4つの原因と、その問題・対策をセキュリティエンジニアの松山さんと掘り下げます

不正アクセスは、なぜ起きるのか — 4つの原因

入口の問題 — だれが、どうやってログインできるか

① 入口が狙われる

利用者の視点

利用者がID・パスワードを管理しきれていない

② アカウントが把握できていない

管理者の視点

保守用・委託先・退職者のIDや強すぎる権限が残る

中身の問題 — ログインした先で、何ができ、何が残るか

③ 情報が散在し、管理が行き届かない

情報の置き場所の視点

どこに何があるか分からず、漏れても範囲を特定できない

④ 気づけない・追えない

事後の備えの視点

正規ログインに見えるアクセスは検知されにくい

① 入口が狙われる

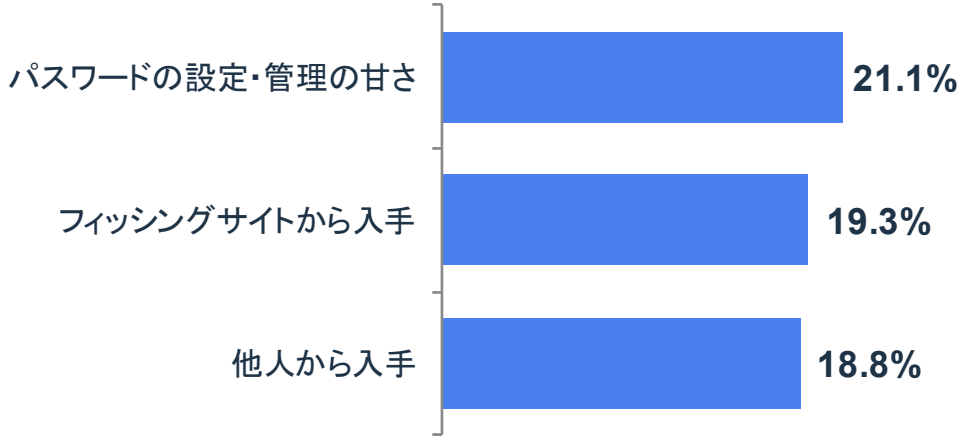
利用者の視点

「パスワードは、知らぬ間に盗まれる」

起きていること

- 利用者がID・パスワードを管理しきれていない
- 使い回し、推測しやすいパスワード、メモやブラウザへの保存
- フィッシングサイトに入力してしまう、端末のマルウェア感染で盗まれる
- 盗まれたID・パスワードで、正規の利用者として入られる

ID・パスワードの入手手口（上位3つ）



事例

日経（Slack）：私物PCのマルウェア感染で認証情報が流出し、不正ログイン（2025年11月公表）

証券口座の乗っ取り：偽サイトでID・パスワードを盗まれ、不正取引5,958件（2025年1～5月、金融庁）

問題は **利用者が管理しきれないことによるパスワードの流出**

出典：警察庁・総務省・経済産業省「不正アクセス行為の発生状況」（令和8年3月12日）検挙された識別符号窃用型399件の内訳

① 入口が狙われる

原因　利用者が管理しきれないパスワードの流出

パスワードが漏れる前提なら、入口はどう守ればいいですか？

出典：警察庁・総務省・経済産業省「不正アクセス行為の発生状況」（令和8年3月12日）

① 入口が狙われる

対策 入口を固める

パスワードだけに頼らず、多要素認証やSSO等の対策を行い入口を守る

1 多要素認証を必須に

パスワードが漏れても、それだけではログインできない状態にする

2 SSOでまとめる

社内の認証基盤でログインを一元化し、認証のルールをそろえる

3 ログインに気づく

ログイン通知機能等を利用して不正アクセスに気づく

4 アクセス元を限定

IP制限で、許可した場所からのアクセスに限定する

明日からできる一歩

- まず管理者アカウントから、多要素認証を設定する
- 業務で使うサービスのログインを、SSOでまとめられないか確認する

デモでお見せします
Nulab Pass
2段階認証の必須化・SSO

② アカウントが把握できていない

管理者の視点

「止めるべきアカウントが、残っている」

起きていること

- 保守用・委託先・退職者のIDが、使われないまま残っている
- 必要以上に強い権限が付いたままになっている
- ツールごとにIDがバラバラ
- 入退社・異動・契約終了のたびに、止め忘れが生まれる

15.3%

元従業員や知人など、ID・パスワードを知り得る立場にあった人による犯行

調査が示す実態

60.2% 使われていないアカウントが「ある」と答えた情シス担当者

SmartHR調べ（2025年4月、108人）

22.1% 退職日当日にアカウントを止められている企業

ISOプロ調べ（2026年5月、1,019人）

問題は　アカウントの棚卸しができていない

出典：警察庁・総務省・経済産業省「不正アクセス行為の発生状況」（令和8年3月12日）

② アカウントが把握できていない

原因 アカウントの棚卸しができていない

増え続けるアカウントを、
どうすれば把握し続けられますか？

出典：警察庁・総務省・経済産業省「不正アクセス行為の発生状況」（令和8年3月12日）検挙された識別符号窃用型399件の内訳

② アカウントが把握できていない

対策 定期的にアカウントを棚卸しする

入退社や契約と連動させ、アカウントを一か所で把握する

1 止める仕組みと連動させる

入社・異動・退職、委託の開始・終了と、アカウントの停止を連動させる

2 一か所で把握する

「誰が、どこに、どの権限で入れるか」を、ツールごとではなく一か所で把握する

3 権限は必要最低限

「とりあえず管理者」をやめる。強い権限ほど、乗っ取られたときの被害が大きい

明日からできる一歩

- 退職者・委託終了者のアカウントが残っていないか洗い出す
- 管理者権限を持つアカウントを棚卸しする

デモでお見せします

Nulab Pass：アカウント一元管理
Backlog：プロジェクト参加管理

③ 情報が散在し、管理が行き届かない

情報の置き場所の視点

「守るべき場所が、増えすぎている」

起きていること

- 管理すべきものが多すぎる
- メール添付、個人契約のツール、委託先へのデータ持ち出し
- どこに何があるか分からず、権限で守れない
- 漏れたときに、影響範囲を特定できない

事例と調査が示す実態

約307万人分

委託先で、管理者も知らない場所にコピーされていた個人データが漏えい

イセトー（2024年）／個人情報保護委員会（2025年3月公表）

29.6%

会社が承認していないツールの利用が「見受けられる」大企業

ボスコ・テクノロジーズ調べ（2025年3月、108人）

問題は **情報の置き場所が決まっていない**

③ 情報が散在し、管理が行き届かない

原因　情報の置き場所が決まっていない

Q 散らばりがちな情報を、どこにどう置けば守れますか？

③ 情報が散在し、管理が行き届かない

対策 情報の置き場所を決める

置き場所を決めて集め、権限で区切って守る

1 置き場所を決めて集める

業務の情報を管理された場所に集め、守る場所そのものを減らす

2 見せる人を絞る

集めた情報はプロジェクトなどの単位で区切り、必要な人にだけ見せる

3 禁止より受け皿を

禁止だけでは管理外のツールが増える。現場が使いやすい安全な受け皿を用意する

明日からできる一歩

- どこに何があるか把握する
- 重要な情報の置き場所を決める

デモでお見せします
Backlog
情報の集約・プロジェクト権限

④ 気づけない・追えない

事後の備えの視点

「侵入は、正規のログインと区別がつきにくい」

起きていること

- 盗まれたIDでのアクセスは、正規のログインと見分けにくい
- 既存の検知の仕組みをすり抜けてしまう
- 誰が、いつ、何をしたかの記録がないと、影響調査が長引く
- 発覚が遅れるほど、被害と対応コストが膨らむ

調査が示す実態

39.8%

事故に備えて、緊急時の体制や対応手順を準備している中小企業（一部を含む）

IPA調べ（2024年10～11月、4,191件）

約18%

BCP（事業継続計画）を策定していたランサムウェア被害組織

警察庁調べ（2025年の被害組織へのアンケート）

問題は 「起きた後」の備えがない

④ 気づけない・追えない

原因　「起きた後」の備えがない

Q 侵入をゼロにできないなら、何を備えておけばいいですか？

④ 気づけない・追えない

対策　「起きた後」に備える

「誰が、いつ、何をしたか」を追える記録を残しておく

1 気づける状態にする

いつもと違うアクセスに気づける仕組みと、通知を受け取る窓口を用意する

2 ログは「見られる」状態に

取っているだけでなく、重要な操作だけでも普段から確認できるようにする

3 対応の経緯を残す

影響範囲の報告、再発防止、担当者が替わっても引き継げるように記録する

明日からできる一歩

- 主要なツールでログが取れているか、どこで見られるかを確認する
- 不審なログインに気づいたときの連絡先と手順を決めておく

デモでお見せします
Nulab Pass：監査ログ
Backlog：アクセスログ

企業が今、意識すべきセキュリティ対策

原因	対策
1 入口が狙われる	**入口を固める** パスワードだけに頼らず、多要素認証とSSOで入口を守る
2 アカウントを把握できていない	**定期的にアカウントを棚卸しする** 入退社や契約と連動させ、アカウントを一か所で把握する
3 情報が散在し、管理が行き届かない	**情報の置き場所を決める** 置き場所を決めて集め、権限で区切って守る
4 気づけない・追えない	**「起きた後」に備える** 「誰が、いつ、何をしたか」を追える記録を備えておく

backlog × nulabpass

SECTION 02

デモ：Backlog × Nulab Passで備える

ひとつのプロジェクトの始まりから終わりまでで、対策の実際をご覧いただきます

入口はNulab Passで固め、中身はBacklogに集めて守る

nulabpass

① 入口を固める

Backlogで2段階認証の必須化※
NulabPassでSSO
パスワードだけに頼らない

② アカウントを棚卸しする

組織のアカウントを一元管理し、不要なものをすぐ止める

backlog by nulab

③ 情報の置き場所を決める

業務の情報を集約し、プロジェクト単位の権限で見せる人を絞る

④ 「起きた後」に備える

課題の変更履歴とコメントで、対応の経緯を残す（監査ログはNulab Pass）

※ 2段階認証の必須化 は 一部のプランで利用可能。詳細はこちら

では、実際の画面でご覧いただきます

デモ：ひとつのプロジェクトの「始まりから終わりまで」

設定
株式会社サンプル（架空）の情報システム部。社外パートナーと一緒に、新しい開発プロジェクトを進めます

シーン1
プロジェクトを始める

シーン2
情報を集めて進める

シーン3
プロジェクトを終える

シーン4
もしものときに備える

① 入口を固める

nulabpass ／ backlog

社外パートナーを招待し、安全な入口から参加してもらう

③ 情報の置き場所を決める

backlog

情報をプロジェクトに集め、見せる人を絞る

② アカウントを棚卸しする

backlog ／ nulabpass

社外パートナーやメンバーのアカウントを止める

④「起きた後」に備える

backlog ／ nulabpass

不審な操作に気づき、記録をたどって対応する

4つの対策が、プロジェクトのどの場面で効いてくるのかをご覧ください

シーン1　プロジェクトを始める

① 入口を固める

こんな場面

社外パートナーと新しいプロジェクトを始めます。
社員も社外メンバーも、Backlogにログインして一緒に作業します。

デモで見ること

1. **2段階認証を必須にする**
   Backlogのスペース設定で、ログインに2段階認証を必須にする
2. **IP制限を行う**
   許可した場所（IPアドレス）からのアクセスに限定する
3. **社員はSSOでログイン**
   社内の認証基盤（IdP）のアカウントで、そのままBacklogへ
4. **パスワードだけでは入れない**
   2段階認証がなければ、パスワードだけではログインできない

Backlog：2段階認証・IP制限 ／ Nulab Pass：SSO



2段階認証の必須化 → IP制限 → SSOの設定

プラン別の利用可能機能については
Backlogの料金プランページでご確認いただけます

シーン2　情報を集めて進める

③ 情報の置き場所を決める

こんな場面

仕様書、議事録、日々のやり取りが、メールの添付やチャット、個人のツールに散らばりがちです。

デモで見ること

1. **情報をプロジェクトに集める**
   課題・ドキュメント・ファイルを、プロジェクトの中にまとめる
2. **経緯が記録として残る**
   課題のコメントや更新履歴に、決定までの経緯が残る
3. **見せる人を絞る**
   社外パートナーはこのプロジェクトだけに参加。ほかのプロジェクトは見えない

Backlog：情報の集約・経緯の記録・参加ユーザー



集める → 経緯が残る → 見せる人を絞る

シーン3 プロジェクトを終える

② アカウントを棚卸しする

こんな場面

プロジェクトが終わり、社外パートナーとの契約も終了。メンバーの1人は異動することになりました。

デモで見ること

1. **プロジェクトから外す**
   Backlogで、社外パートナーをプロジェクトのメンバーから外す
2. **アカウントを棚卸しする**
   Nulab Passのメンバー一覧で、誰がどのチーム・権限かを確認
3. **不要なアカウントを止める**
   止めたいアカウントを選び、「組織から外す」

Backlog：参加ユーザー ／ Nulab Pass：メンバー



プロジェクトから外す → 棚卸し → アカウントを止める

シーン4　もしものときに備える

④「起きた後」に備える

こんな場面

情報システム部に、社員から問い合わせが届きました。

「自分が更新した覚えのない課題の変更が、履歴に残っています。私のアカウントが使われていないか確認してください」

デモで見ること

1. **問い合わせを課題として起票**
   テンプレートで、確認に必要な情報を漏れなく受け付ける
2. **記録をたどる**
   Nulab Pass 監査ログ：誰が・いつ・何を変更したか
   Backlog アクセスログ※：いつ・どこからアクセスしたか
3. **対応の経緯を記録する**
   確認結果と対応を課題に残し、担当が替わっても引き継げるようにする

※アクセスログの対象プランはこちらから

Backlog：課題の起票 ／ Nulab Pass：監査ログ



起票 → 監査ログでたどる → 経緯を記録

デモのまとめ：4つの原因に、仕組みで備える

シーン	原因	使った仕組み	できるようになったこと
シーン1 始める	① 入口が狙われる	nulabpass ／ backlog	2段階認証の必須化・SSO、IP制限で、パスワードだけに頼らない
シーン2 進める	③ 情報が散在し、管理が行き届かない	backlog	情報をプロジェクトに集め、権限で見せる人を絞る
シーン3 終える	② アカウントが把握できていない	nulabpass ／ backlog	アカウントを一か所で把握し、不要なものをすぐ止める
シーン4 備える	④ 気づけない・追えない	nulabpass ／ backlog	監査ログとアクセスログでたどり、対応の経緯を課題に残す

入口はNulab Passで固め、中身はBacklogに集めて守る

backlog by nulab × nulabpass

SECTION 03

まとめ・ご案内・Q&A

明日からできる一歩と、無料トライアル・個別相談会のご案内

まとめ

不正アクセスの入口は「アカウント」。4つの対策で、仕組みとして備える

入口を固める

明日からできる一歩

まず管理者アカウントから、多要素認証を必須にする

仕組みで対策

nulabpass

2段階認証の必須化、SAML認証によるSSO

backlog

IP制限で、許可した場所からのアクセスに限定

アカウントを棚卸しする

明日からできる一歩

退職者・委託終了者のアカウントが残っていないか洗い出す

仕組みで対策

nulabpass

組織のアカウントを一元管理し、不要なものを停止

backlog

プロジェクト単位で、参加メンバーと権限を管理

情報の置き場所を決める

明日からできる一歩

どこに何があるかを把握し、重要な情報の置き場所を決める

仕組みで対策

backlog

課題・ドキュメント・ファイルを一か所に集約し、プロジェクト単位の権限で見せる人を絞る

「起きた後」に備える

明日からできる一歩

主要なツールでログが取れているか、どこで見られるかを確認する

仕組みで対策

nulabpass

監査ログで、誰が・いつ・何を変更したかを確認

backlog

アクセスログ※で、いつ・どこからのアクセスかを確認。対応の経緯は課題に記録

※アクセスログの対象プランはこちらから

次の一歩に、ご活用ください

無料トライアル

Backlogを30日間、無料でお試しいただけます

・まずはひとつのプロジェクトで、権限設定や管理機能を確認

・決済情報の登録は不要

お申込みはこちら

個別相談会

セキュリティ要件や導入について、担当者が個別にお答えします

・自社の基準を満たせるか、設定や運用をご相談いただけます

・Nulab Passの導入・SSO連携のご相談も承ります

お申込みはこちら

backlog by nulab × nulabpass

ご視聴ありがとうございました

アンケートへのご協力をお願いします

今後のセミナーづくりの参考にさせていただきます。



セキュリティエンジニア
松山 保



プロモーション部
河野 千里